インターネットの
安全・安心ハンドブック

NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

×

鳥取県サイバーセキュリティ対策ネットワーク

インターネット安全利用関連資料集

2019

知る・守る・続ける
サイバーセキュリティ普及啓発

ネットワークビギナーのための
情報セキュリティハンドブック Ver 4.00

「インターネット安全・安心ハンドブック（NISC)」
×
鳥取県サイバーセキュリティ対策ネットワーク「インターネット安全利用関連資料集2019」

目 次

インターネットの安全・安心ハンドブック（NISC） ……3～166
URL https://www.nisc.go.jp/security-site/handbook/index.html

専門分科会開催報告（鳥取県サイバーセキュリティ対策ネットワーク事務局） ……167、168

サイバーセキュリティ講演開催報告（鳥取県警察本部サイバー犯罪対策課） ……169～179
URL https://www.pref.tottori.lg.jp/270728.htm

サイバーセキュリティ関連情報（鳥取県警察本部サイバー犯罪対策課） ……180～190
URL https://www.pref.tottori.lg.jp/270729.htm

いまさら聞けない！ソーシャル・ネットワーキング・サービスって何？ ……191～194
株式会社セブンズデザイン代表取締役坂本拓也様寄稿（鳥取法人会）
URL http://www.toriho.com/wp/wp-content/themes/houjinkai/img/pdf/back95.pdf

「電子メディアとの付き合い方ノート（シート)」の活用について ……195～196
【小学校1～3年生向け】電子メディアとの付き合い方学習ノートA ……197～204
【小学校4～6年生向け】電子メディアとの付き合い方学習ノートB ……205～216
【中学生・高校生向け】電子メディアとの付き合い方学習ノートC ……217～220
（以上　鳥取県教育委員会事務局社会教育課）
URL https://www.pref.tottori.lg.jp/277458.htm

リーフレット　小中学生向け　電子メディアとうまくつきあおう ……221～224
リーフレット　高校生向け　　電子メディアとうまくつきあおう ……225、226
（以上　鳥取県教育委員会事務局社会教育課）
URL https://www.pref.tottori.lg.jp/220432.htm

乳幼児保護者向けチラシ「電子メディアが乳幼児期の子どもに及ぼす影響は…？」 ……227、228
（鳥取県教育委員会事務局社会教育課）
URL https://www.pref.tottori.lg.jp/267060.htm

チラシ　みんなですすめよう！「メディア21:00」運動（鳥取県PTA協議会様） ……229、230
URL http://www.tottori-pta.net/publics/index/134/

リーフレット 今すぐ始めよう！！ペアレンタルコントロール ……231～234
（鳥取県福祉保健部子育て王国推進局青少年・家庭課様）
URL https://www.pref.tottori.lg.jp/244415.htm

チラシ スマートフォンのセキュリティ対策のポイント ……235
（鳥取県警察本部サイバー犯罪対策課）
チラシ 情報セキュリティ対策７か条 ……236
（鳥取県サイバーセキュリティ対策ネットワーク）
第14回IPA「ひろげよう情報モラル・セキュリティコンクール」2018優秀賞受賞作品 ……237
（鳥取県警察本部サイバー犯罪対策課）

インターネットの
安全・安心ハンドブック

×

鳥取県サイバーセキュリティ対策ネットワーク

インターネット安全利用関連資料集

2019

サイバーセキュリティ普及啓発

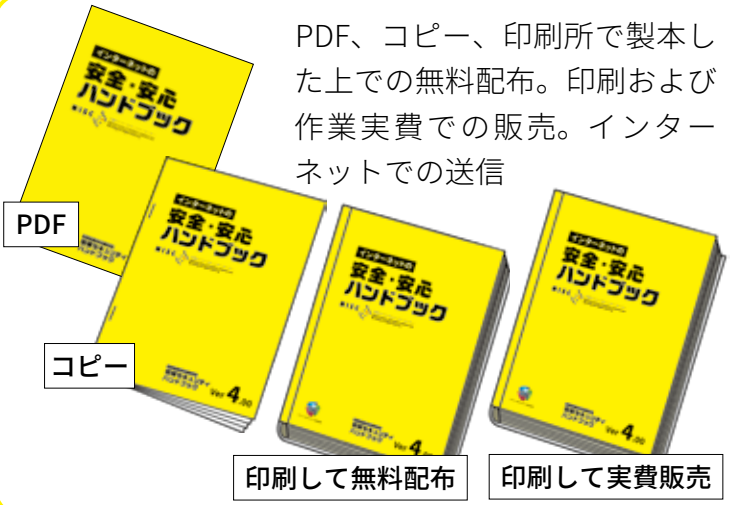
ネットワークビギナーのための
情報セキュリティハンドブック Ver 4.00

NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

「インターネットの安全・安心ハンドブック」
は、下記のようにご活用いただけます。

本冊子の著作権は内閣サイバーセキュリティセンター(NISC)に留保されますが、内容に改変を加えない事を条件に、多様な形でご活用いただく事ができます。

※製本用印刷データが必要な場合は下記までお問い合わせください
security_awareness@cyber.go.jp
※合本やプリンタでの印刷にはNISCホームページ掲載のPDF版をお使いください



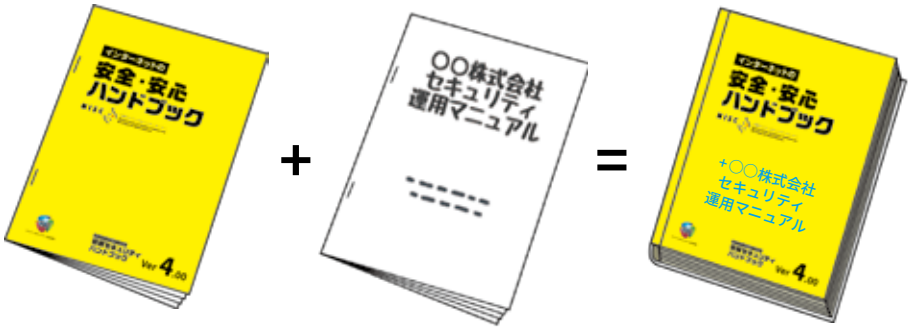
PDF、コピー、印刷所で製本した上での無料配布。印刷および作業実費での販売。インターネットでの送信

ページ単位、イラスト単位での利用、配布(ネット配布含む)

分割して配布、必要部分だけを抜粋して配布

ホームページにダウンロード用サイトのリンクを設置※

使用する団体名を表紙に入れて利用



自団体のセキュリティ資料と合体しての配布

※ダウンロード用サイトURL
https://www.nisc.go.jp/security-site/handbook/index.html

インターネットの安全・安心ハンドブック　活用法

● 学校の授業で

「インターネットの安全・安心ハンドブック」では、まず中高生の方と、その先生方に、この本をセキュリティ意識を高めるための教材として使って頂きたいと思います。

第1章の基本のセキュリティを踏まえつつ、第2章のサイバー攻撃に遭うとどういったことが起こるのか、そして第3章のセキュリティを守る為の各技術をマスターして、さらにそれをご家族にも広めてください。

● ご家庭で

ご家庭でのセキュリティの守り方については各章に記述がありますのでぜひご参照ください。

また第5章では子ども達がSNSを気軽に利用するとどういうったトラブルが発生するのか、SNSをとおして見知らぬ人と友だちになるとどういった事が起こるのか触れていますので、ご家族で一緒になって確認し合ってください。

子ども達だけでなくお年寄りを守る為のテクノロジーの使い方のアイデアも掲載していますのでご活用ください。

● 災害時に備えて

第5章の家族を守るセクションには、災害時に関する記述があります。大規模災害時にどうやって情報を活用して身を守るのか、デジタル世代のサバイバル技術についての知識を得た上で、「もし災害が起こったらどうするか」をご家族で計画を立てて話し合ってみてください。

学校の授業で

P21「第1章．基本のセキュリティ～ステップバイステップでセキュリティを固めよう~」

P41「第2章．サイバー攻撃に遭うとどうなるの？最新の攻撃手口を知ろう」

P51「第3章．パスワード・Wi-Fi・ウェブ・メールのセキュリティを理解して、インターネットを安全に使おう」

P107「第5章．SNSやインターネット関連の犯罪やトラブルから、自分や家族を守ろう。災害に備えよう」

ご家庭で

P108「5-1-1 SNSやネットの楽しみ方と気をつけること」

P118「5-2-1 アニメ・マンガ・音楽の違法なシェア。パクリなどの著作権侵害」

災害時に備えて

P132「5-3-4.大災害やテロに備える」

P135「5-5-4.徒歩帰宅。海外での災害やテロに備えて」

目次

はじめに〜サイバーセキュリティは「公衆衛生」の時代に〜 10
Black Hat the Cracker 12

プロローグ **サイバー攻撃ってなに？** 13

1. サイバー攻撃のイメージ 14
1. サイバー攻撃って誰がやっているの？どうするの？ 14
コラム：攻撃者とハッカーとクラッカー 15
コラム：攻撃者が使う武器「マルウェア」 16
2. サイバー攻撃の例 18
3. サイバー関連の犯罪やトラブル 19
4. 一見サイバー攻撃に見えない「ソーシャルエンジニアリング」攻撃 20

第1章 **基本のセキュリティ〜ステップバイステップでセキュリティを固めよう〜** 21

1. 4つのポイントでセキュリティを守る 22
1. システムを最新に保つ。セキュリティソフトを入れて防ぐ 22
2. 複雑なパスワードと多要素認証で侵入されにくくする 22
3. 攻撃されにくくするには侵入に手間（コスト）がかかるようにする 23
4. 心の隙を作らないようにする（対ソーシャルエンジニアリング） 23

2. 環境を最新に保つ、セキュリティソフトを導入する 24
1. セキュリティソフトを導入して守りを固めよう 24
2. パソコン本体とセキュリティの状態を最新に保とう 25
3. スマホやネットワーク機器も最新に保とう 26
4. ソフトやアプリは原則公式ストアから。権限にも気をつける 27
コラム：必要ならばスマホにはセキュリティパックを検討しよう 28
コラム：パソコンやスマホを最新の状態に保っても防げない攻撃がある。それがゼロデイ攻撃！ 29

3. 複雑で長いパスワードと多要素認証で侵入されにくくする 30
1. パスワードの安全性を高める 30
2. 機器やサービス間でのパスワード使い回しは「絶対に」しない 30
3. パスワードを適切に保管する 31
4. 秘密の質問にはまじめに答えない。多要素や生体認証を使う 32
コラム：パスワードはどうやって漏れるの？どう使われるの？ 33

4. 攻撃されにくくするには、手間（コスト）がかかるようにする 34

5. 心の隙を作らないようにする（対ソーシャルエンジニアリング） 36
コラム：クリックしてはいけない！フィッシング攻撃の傾向 38
コラム：コラム：映画「ザ・ハッカー」にみるソーシャルエンジニアリング 39
コラム：スパムメールとその由来 40

第2章　サイバー攻撃にあうとどうなるの？　最新の攻撃の手口を知ろう 41

1. 攻撃者に乗っ取られるとこんなことが起こる 42
1. 被害に遭わない、そして加害者にならないために 42
2. 盗まれた情報は犯罪に使われる 43
3. 乗っ取られた機器はサイバー攻撃に使われる 44
4. IoTも乗っ取られる。知らずにマルウェアの拡散も… 45
コラム：大きな脅威となっているランサムウェア 46
コラム：仮想通貨の現在地1 47
コラム：QRコード決済サービスで生まれた新たな詐欺 47
コラム：仮想通貨の現在地2 48
コラム：フェイクニュースとサイバープロパガンダ 49
コラム：軍事スパイ、産業スパイに狙われてしまったら 50

第3章　パスワード・Wi-Fi・ウェブ・メールのセキュリティを理解して、インターネットを安全に使おう 51

1. パスワードを守る、パスワードで守る 52
1. パスワードってなに？ 52
2. 3種類の「パスワード」を理解する 52
3. 「PINコード」と「ログインパスワード」に求められる複雑さの違い 52
4. 「暗号キー」に求められる複雑さ 54
5. どちらの「パスワード」か、わかりにくい例 54
6. 総当たり攻撃以外のパスワードを破る攻撃や生体認証を使った防御 55
7. パスワードの定期変更は基本は必要なし。ただし流出時は速やかに変更する 56
8. パスワード流出時の便乗攻撃に注意 56
9. 適切なパスワードの保管 57
10. パスワード情報をクラウドで利用する善し悪し 58
11. ノートやスマホを失くした場合のリカバリ考察 58
12. 注意するべきソーシャルログイン 58
13. 二段階認証を活用する。ただしSMS認証は避ける 59
14. 権限を与えるサービス連携にも注意 60
コラム：暗号化の超簡単説明 60
コラム：パスワードの管理について（2018年の動向まとめ） 62
2. 通信を守る、無線LANを安全に利用する 64
1. それぞれの状況に合わせた暗号化の必要性 64
2. 無線LAN通信（Wi-Fi）の構成要素 64
3. 暗号化なしや、方式が安全ではないものは危険 65
4. 暗号化方式が安全でも「暗号キー」が漏れれば危険 66
5. 家庭内での安全な無線LANの設定（暗号化方式） 66
6. 家庭内での安全な無線LANの設定（その他） 67
7. 公衆無線LAN利用時の注意 68
8. 個別の「暗号キー」を用いる方式の無線LAN 68
9. 公衆無線LANに関して新規に購入したスマホなどで行うこと 69
10. 公衆無線LANが安全ではない場合の利用方法 70
11. 自前の暗号化による盗聴対策 70
12. まとめて暗号化するVPN、現状は過信できないが今後に期待 70
3. ウェブを安全に利用する、暗号化で守る 72
1. 無線LANの暗号化とVPNの守備範囲 72
2. 全ての通信と、その一部であるウェブの通信 72

3. https で始まる暗号化通信にはどんなものがあるか 72
4. より厳格な審査の「EV-SSL 証明書」 74
5. 「EV-SSL 証明書」を持つサイトを見分ける方法 74
6. 有効期限が切れた証明書は拒否する 74
7. 他にも証明書に関する警告が出るサイトは接続しない 74
8. ウェブサービスのログインは二段階認証などを使う 75
9. 二段階認証を破る「中間者攻撃」 76
10. ウェブを使ったサイバー攻撃に対応する 77

4. メールを安全に利用する、暗号化で守る 78

1. メールにおける暗号化 78
2. 送信の暗号化と受信の暗号化 78
3. メールにおける暗号化の守備範囲 78
4. メール本文の暗号化 79
5. 怪しいメールとはなにか 80
6. マルウェア入りの添付ファイルに気をつける 80
7. メールアドレスのウェブサービスなどからの流出 82
8. 流出・スパム対策としての、変更可能メールアドレスの利用 82
9. 通信の安全と永続性を考えた SNS やメールの利用 82

5. データファイルを守る、暗号化で守る 84

コラム：究極の防御手段「ネットにつながない」エアギャップ 86
コラム：「無料」ということの対価は何か 88
コラム：クラウドサービスからのデータ流出。原因は？ 90

第 4 章　スマホ・パソコンのより進んだ使い方やトラブルの対処の仕方を知ろう 91

1. スマホのセキュリティ設定 92

1. スマホにはロックをかけよう。席において離れたり、人に貸したりするのは× 92
2. 情報漏れを防ぐ① 93
3. 情報漏れを防ぐ② 94
4. スムーズな機種変更と、予期せぬデータ流出の防ぎ方 96

2. パソコンのセキュリティ設定 98

1. パソコンを買ったら初期設定などを確実に 98
2. 暗号化機能などでセキュリティレベルを高める 99
3. マルウェア感染に備え、3-2-1 のバックアップ体制を整える 100
4. 売却や廃棄するときはデータを消去する 101
5. 盗難や紛失のとき、スマホとパソコン、どっちが安全？ 102

コラム：ダブルラインでトラブルに備える 103

3. それでも攻撃を受けてしまったときの対処 104

1. 兆候に気をつけて被害が出たら対処 104

コラム：セキュリティの資格取得を目指そう 106

第 5 章　SNS やインターネット関連の犯罪やトラブルから、自分や家族を守ろう。災害に備えよう 107

1. SNS やネットとのつきあい方、守り方 108

1. SNS やネットの楽しみと気をつけること 108
2. SNS やネットの怖さ、こんなことが実際に起こっている 109

3. SNSやネットとのつきあい方の基本 110
4. 存在するデータは流出することがある。流出したら消すことは難しい 111
コラム：子どもにスマホを持たせる時、「スマホ契約書」という提案 112
コラム：GPS、位置情報、ジオタグの管理 113
コラム：SNSやSNSのグループを使ったいじめに備える（いじめ経験者からのアドバイス） 114
コラム：モラルを逸脱すると炎上を生む 115
コラム：屋外でのゲームを安全に楽しむ。ながらスマホは×！ 116

2. サイバー関連でやってはいけないこと 118

1. アニメ・マンガ・音楽の違法なシェア。パクリなどの著作権侵害 118
2. ゲームの不正行為。恋人や家族でもプライバシーは守る 119
3. クラッキングはクールじゃない！ 120
コラム：法律に違反することをしてはいけません。気軽に考えてはダメ 121
コラム：成人年齢18歳引き下げに伴って注意が必要なこと 122
コラム：デジタル遺産相続 123

3. デジタルテクノロジーで家族を守る 124

1. 子ども達を守る 124
2. お年寄りを守る 126

4. 屋外・海外でのネットワーク利用 128

1. 一見なにもないように見えて、危険がいっぱい 128
2. インターネットカフェの利用 129
3. 海外でスマホやタブレットを活用するために 130

5. 大災害やテロに備える 132

1. まずは自分の身の安全を確保する 132
2. 電池をもたす、情報収集をする 133
3. ラジオ、ワンセグを使った情報収集 134
4. 徒歩帰宅。海外での災害やテロに備えて 135
コラム：デマに踊らされない！　ソースを探せ！　確かめよう！ 136
コラム：災害時の情報収集について（本年の振り返り） 137
5. ネットを使わない移動トレーニング（現代版オリエンテーリング） 138

エピローグ **来たるべき新世界へ** 139

1. ネットの「今」と、これからをどう守っていくか 140
2. デジタルネイティブと未来 142
3. バーチャル空間を超えて世界へ 143
4. おわりに 144

用語集 146

情報セキュリティ関連サイト一覧 158

索引 160

※ご注意
本書では初心者の方にサイバーセキュリティ関連の問題を理解してもらうために、実際のケースと比較してわかりやすく簡略化したり、内容を理解しやすいように関連する事項の一部を省略したりして記述している場合があります。ご了承ください。
このハンドブックを読んで、よりサイバーセキュリティに関する理解を深めていきたいと思う方は、ぜひステップアップして、様々な専門誌や最新の記事にチャレンジしていただけると幸いです。
なお、登場する人物および団体は架空のものであり、実在するいかなる人物・団体とも関係はありません。

はじめに～サイバーセキュリティは「公衆衛生」の時代に～

みなさん、はじめまして。私たちは内閣サイバーセキュリティセンター(NISC)です。日本の政府機関で国のサイバーセキュリティ政策を担当しています。

突然ですが、「ウイルス」という言葉をご存じですか？病気の原因としてのウイルスを思い浮かべましたか？それとも「コンピュータウイルス」？

現実の世界ではウイルスに感染して病気にかかった人がいると、病院に行かせたり、場合よっては隔離して適切な治療をし、他の人にうつらないようにもします。そうしないと、家庭や職場の人たちみんなが病気になって、最後は社会全体の活動に大きな問題が発生してしまうからです。

それを知っているから私たちは、マスクをし、手洗いをし、ワクチンを接種し、上下水道を整備し、家の中や町をきれいにして「公衆衛生」に努めるわけです。

※NISC特務第１チームは架空の団体です。

今、日本の街角が綺麗で、病気による大災害が発生しないのも、国民全員が長年取り組んだ「公衆衛生」意識と活動の賜物なのです。

さて、コンピュータやインターネットの世界にも、「ウイルス」が存在します。ウイルスだけで無く細菌や、原虫、寄生虫に相当するトロイの木馬やワームといったものもありますし、また、生活の安全を脅かす、悪意をもった人たちが暗躍しています。それはさながら、社会システムが未発達で公衆衛生意識やなぜそれが必要なのかについての知識も十分ではない、はるか昔の時代のようです。

そしてそのインターネットの世界は、今や私たちの現実の世界と複雑に絡み合っていて、インターネットで発生するトラブルは、現実世界の私たちの生活にまで、多大な影響を及ぼしつつあるのです。

いま私たちに求められているのは、この新しい世界の状況をきちんと理解して、そこを安全に利用し、楽しめる生活空間とするために、インターネットの世界の防犯意識や公衆衛生の意識を確立して、行動に移すことです。

その活動は私たちだけではできません。国民全員参加で初めて成し遂げることができるのです。さぁ、その第一歩を始めましょう。

一人ひとりがサイバーセキュリティを担うことで、安全なネット社会をつくることができます

ネットにいる悪意を持った人たちは、みなさんの手の中にあるスマホや家にあるパソコンを狙ってきます。しかし世の中にあるすべてのスマホやパソコンを守るためには工夫がいります。街の安全が防犯活動や、それによって醸成される防犯意識、あるいは何かあったときに、みんなが助け合うという意志によって守られるように、意思を持ち私たちと一緒にネットを守って下さい。

Black Hat the Cracker

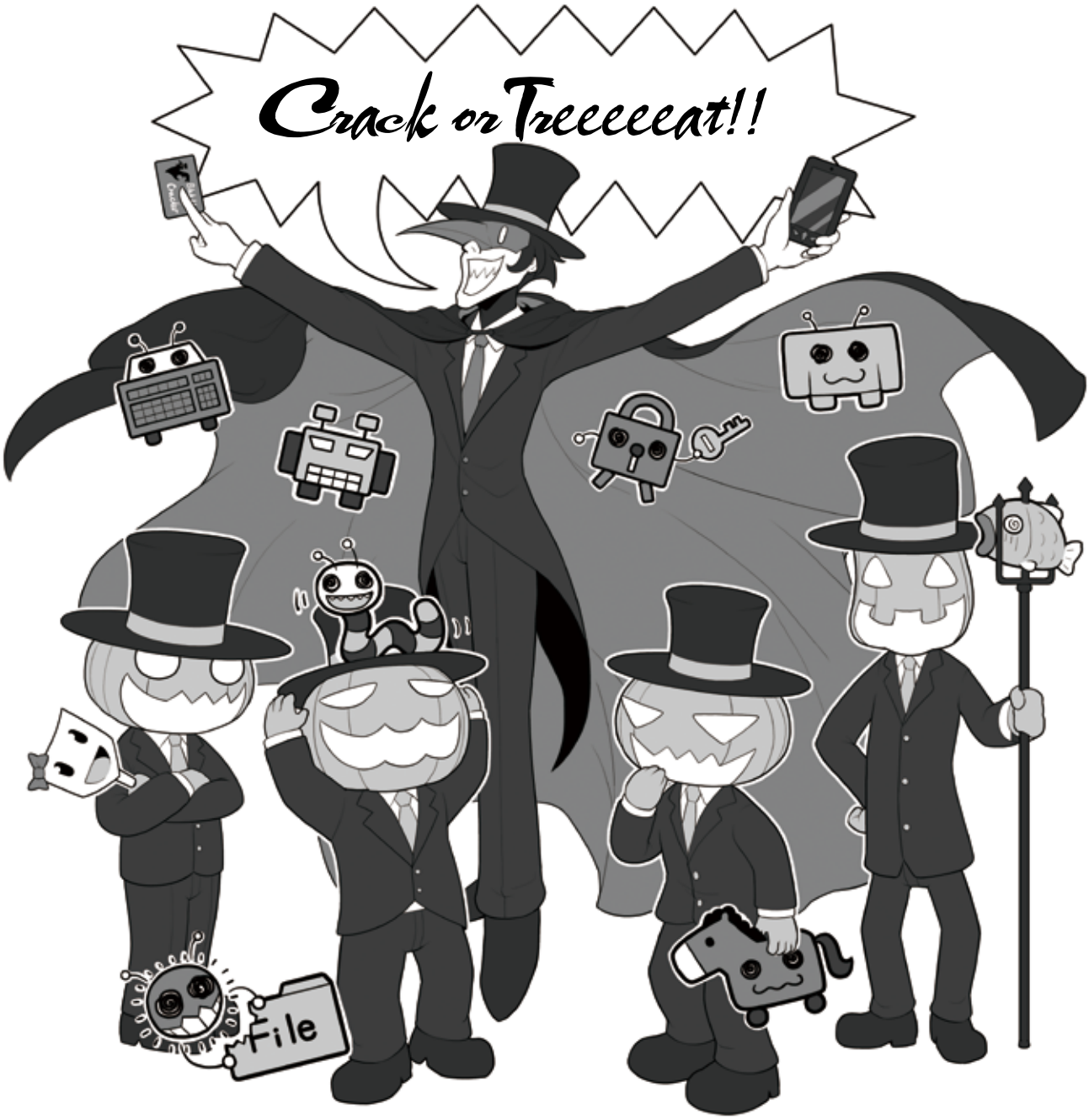
サイバー空間(インターネット)には悪意をもってこれを利用し、自らの利益のためには平気で他人の情報や財産を奪い、またサイバー攻撃を通じて自己誇示するといった、様々な悪事を働くものがいます。

この本ではその者たちの仮の姿として、「ブラックハット・ザ・クラッカー」と、その手下たち「ブラックパンプキン」、そして様々な「マルウェア」が登場します。

また時に、彼らが普通の人の仮面をかぶったり、あるいは普通の人々が彼らの仮面をかぶったりして、悪事を働くこともあります。

解説のイラストでは、そのあたりもきちんと描き分けていきたいと思いますので、ぜひつぶさに見ていて下さいね。

彼(彼女?)の正式名称「ブラックハット・ザ・クラッカー」の由来については、「コラム：攻撃者とハッカーとクラッカー」の項目でお話ししましょう。



プロローグ

サイバー攻撃ってなに？

サイバー攻撃という言葉を聞いて何を思い浮かべますか？
どんなことが起こるの？誰がやっているの？何を狙っているの？
まずサイバー攻撃とは、どのようなものなのか、それを知ってもらいましょう。

悪意を持った人たちは、いったい何を狙っているの？

1 サイバー攻撃のイメージ

1 サイバー攻撃って誰がやっているの？どうするの？

サイバー攻撃はいったい誰が何の目的でやっているのでしょう。

軍事スパイや産業スパイ？ それともハッカー？

いわゆるスパイの目的は軍事機密や先進の研究内容など、自国や企業にとって有益な情報の入手です。それに対し、私たちが普段遭遇するサイバー攻撃は、個人情報や金銭など、主として攻撃する者にとり何らかの利益になるものを目的としています。

スパイは目的の達成が絶対条件なので、ありとあらゆる手段で攻撃を行い、どんなにセキュリティが厳重でも侵入を試みます。それはやっかいな存在で、現状完璧には防ぐことができません。

一方、利益目的のサイバー攻撃は、攻撃する者にとってはビジネスとしての性格を持っています。たとえば「ここはセキュリティがしっかりしているので手間がかかる(≒値段が高い)のでやめよう」「ここなら手間がかからない(≒安い)からこちらに行こう」というように、攻撃しやすい方に流れやすく、機器のセキュリティレベルを高めることで、ある程度攻撃を受けにくくすることができるものです。完璧に防ぐことは難しくても、努力をすれば被害に遭う確率を減らせると考えて良いでしょう。

サイバー攻撃への対処は、ヒーローが登場する勧善懲悪のアニメのように、すっぱりと解決をしたり、あるいはデジタルのようにかっちりと防いだりすることはできません。まずは安全を確保する手段を、地道に積み上げる必要があるのです。

これから私たちが説明していくサイバーセキュリティに関するお話は、この考え方に沿っていることを覚えておいてくださいね。

コラム：攻撃者とハッカーとクラッカー

ハッカー

そもそも「ハッカー」とはコンピュータの知識と技術に精通した人を尊敬して呼ぶ名前で、イコール悪事を働く人という意味ではありません。その用語を自分で使うとき、あるいは報道など見るとき、どのような意味で使われているのかを気にかけましょう。

専門ではない新聞や雑誌、テレビでは、サイバー攻撃を行う者をよく「ハッカー」と称しがちです。しかし実はこの呼び方はあまり正しくありません。

ハッカーとは、もともとはコンピュータに精通しその方面の高い知識と技術を持つ人を指すある種の尊称であり、イコール悪事を行う攻撃者ではありません。そして彼等がその技術を駆使して行う作業を「ハッキング」や単に「ハック」といいますが、これも本来は悪事とイコールではありません。

ただしこういった知識や技術をもって悪事を行う人も存在するため、それらを善意の人と区別する意味で、「ブラックハットハッカー」や「ブラックハッカー」、あるいは防御しているものを割って侵入することを意味する「クラッカー（cracker）」や攻撃者の意味を持つ「アタッカー（attacker）」と呼ぶのです。一方、日本語で「ハッカー」と安易に呼ばない場合は「悪玉ハッカー」や「悪意のハッカー」とも言われます。

また逆に善意に基づいて高い知識や技術を使う人を「ホワイトハットハッカー」や「ホワイトハット」「ホワイトハッカー」といい、日本語では「善玉ハッカー」や「正義のハッカー」と呼びます。

本書ではこの本来の意味に基づいた用語でお話を進めますので、皆さんにもぜひ覚えてもらって、日常の生活でも正しい名称が広く用いられるようご協力ください。

コラム：攻撃者が使う武器「マルウェア」

● どんな種類があるの？

先ほどのハッカーやクラッカーの例と同じように、今ひとつ正しく用いられていないのが、「コンピュータウイルス」や、単に「ウイルス」という用語です。

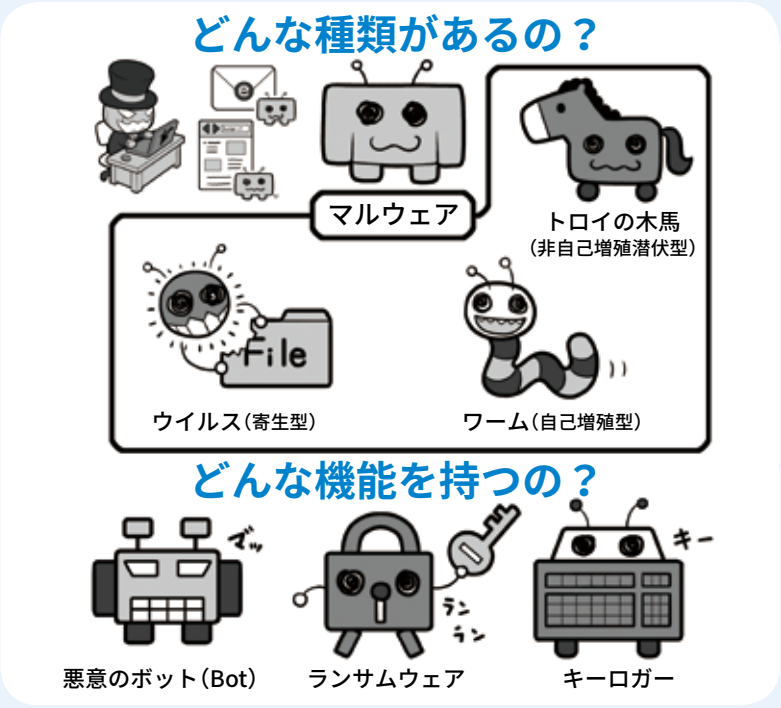
攻撃者がサイバー攻撃を行う場合、相手のコンピュータを何らかの悪意のプログラムに感染させ、これをコントロールする方法がよく用いられます。この攻撃に使われるプログラムをまとめて「ウイルス」と呼びがちです。

しかし攻撃用プログラムは本来「マルウェア」もしくは「不正なプログラム」と呼ぶのが正しく、「ウイルス」とはそのマルウェアの中の一種で、コンピュータ上のファイルが感染し、そのファイルに寄生して活動するタイプのものを指す限定的な名称なのです。

現実世界に例えるなら「マルウェア」とは病気を起こす原因の総称「病原体」にあたり、「病原体」の一種で細胞に寄生しないと増殖できないものを「ウイルス」と呼ぶのと同様です。

そして病原体にはウイルスの他にも、単独で存在することができる細菌、原虫や寄生虫などがあります。マルウェアにも同様に、独立していて非自己増殖型の「トロイの木馬」と呼ばれるものや、独立していてかつ自己増殖型の「ワーム」があります。

また機能による分類としては「ボット」「ランサムウェア」「キーロガー」などの呼び方もあります。これは病原体の行動形態を表す症状の名前のようなものです。



ただ、一般に広がった「ウイルスという言葉がマルウェアと同じ意味で使われる」事実もあるため、その整合性を取るために「広義のウイルス」といった言い方も存在します。

皆さんには、この部分もぜひ覚えていただいて、正しい呼び方を広めてもらうと同時に、新聞、雑誌やテレビで「ウイルス」と使われている時は、それが「広義のウイルス＝マルウェアの意味」なのか「狭義のウイルス＝ファイルに寄生する感染プログラム」なのかを文脈から読み取って、正しく理解してもらえるとうれしく思います。

● どのような機能を持つものがあるの？

マルウェアを機能別に分けるとこのようなものがあります。

- **悪意のボット（Bot）**

ボットとはRobotの略で、悪意のものは感染すると攻撃者にコンピュータが乗っ取られ、別のコンピュータへの攻撃などに使われる。

- **ランサムウェア**

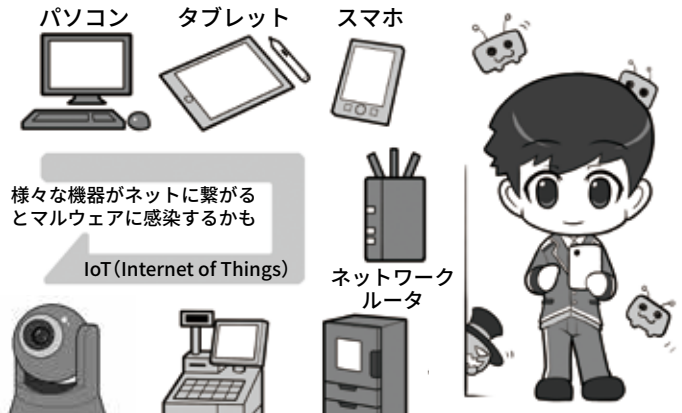
感染すると、コンピュータ上のファイルが暗号化された上で、攻撃者から元に戻すための身代金を要求される。

- **キーロガー**

比較的古いマルウェアで、感染するとキーボードの入力を記録して攻撃者に送信する。攻撃者はこれを利用してパスワードなどを盗む。

またたとえば「トロイの木馬」は、最初にコンピュータに侵入する時は害がないようなふりをして、侵入したらマルウェアの本性を現したり、外部からボットやランサムウェアを呼びこんだりして悪事を働き始める特性を持ちます。これは「トロイアの木馬」という神話から取った名称ですね。

どんなものが感染したり、感染させたり、悪さするようになるのか



● どんなものが感染したり、感染させたり、悪さをするようになるの？

マルウェアに感染するものといえば、おそらく真っ先にパーソナルコンピュータ（以下パソコン）やスマートフォン（以下スマホ）、タブレットなどを想像するでしょう。

「マルウェアはコンピュータが感染する悪意のプログラム」

この表現も間違いありません。しかし実際には、ご家庭で使っている無線LANアクセスルータ、ネットワークにつながるプリンタ、監視カメラやネットワークカメラ、スマートテレビ、スマート冷蔵庫、はてはPOSレジ、変わったところではネットにつながる業務用餅つき機なども感染するそうです。コンピュータではないのに何で感染するのでしょうか。

この「コンピュータが感染する」と「コンピュータじゃないものまで感染している」ことの矛盾を解く鍵は、「現代の電子機器は、コンピュータに見えないものでも、実はコンピュータが内蔵されている」というところにあります。

こういった機器がインターネットにつながりデータをやりとりする以上、マルウェアに感染する可能性があるわけです。

特にIoT（Internet of Things）、「モノのインターネット」の時代が訪れ、私たちの周りに存在するありとあらゆる機器がコンピュータ化し、インターネットにつながるようになると、今より多数の機器が感染する可能性があります。

しかし、こういった悪意の攻撃によってマルウェアに感染してしまうかもしれないことよりも、もっと深刻な問題があります。それは人間の心の隙を突いたサイバー攻撃です。

機器を強制的にマルウェアに感染させるためには、セキュリティホールと呼ばれるプログラム上の弱点が必要です。セキュリティホールがあるということは、家の鍵が壊れているようなものです。しかし日々セキュリティのアップデート＝修正対応が行われ、たいていのセキュリティホールはすぐにふさがれます。

そういった場合でも、持ち主をだまして自らインストールさせれば、外から無理矢理侵入せずとも、簡単に内側から悪事を働くことができてしまいます。

これを実現するのが後ほど説明する「標的型メール」など、人間の心の隙を突くタイプの攻撃です。問題はこの心の隙が、コンピュータのセキュリティホールのように簡単にはふさげないことにあります。セキュリティ意識は、本人が必要性を認識しないと向上しないからです。

どんなにサイバー攻撃に対する防御を固めても、人間をだます攻撃手法はいくつも存在し、こちらはなかなか防げない。このこともよく知ってください。

そして被害者が友人や職場の仲間に次々に感染を広げていって、様々な機器が持ち主の知らぬところで乗っ取られ、勝手に攻撃者によるサイバー攻撃に使われることもあるのです。

そう、被害者であるはずのあなたが、いつの間にか攻撃に参加させられ、時に加害者の立場になることもありうるのです。

まずは防ぐための知識を得て行動をおこしましょう。

2 サイバー攻撃の例

では先ほど紹介したサイバー攻撃が、実際にはどのように行われるのか、いくつかの例を挙げて見てみましょう。

攻撃者はメールにマルウェアを添付してあなたに送ったり、マルウェアを仕込んだサイトに誘導したりして、あなたのパソコンなどをマルウェアに感染させます。その後、IDやパスワードを抜き取ったり、画像や重要情報を気づかれないように裏で送信させたりします。入手したIDとパスワードで勝手に物を購入し、換金できるものはお金に換えたりもします。

また、メールやメッセージで偽の銀行サイトに誘導し、ID・パスワードを盗みお金を不正送金させる、「フィッシング詐欺」などを行うこともあります。

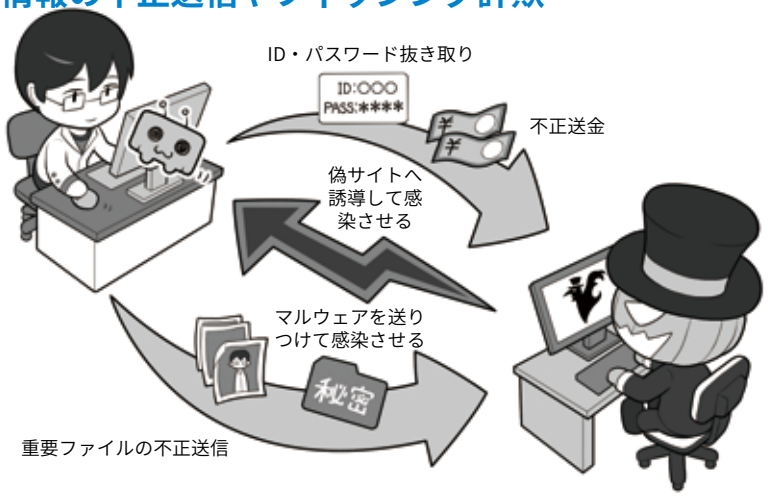
もっと直接的にターゲットにお金を要求する方法もあります。「ランサムウェア」に感染させ、あなたのパソコンなどのデータを勝手に暗号化し、「暗号化を解除してほしければ身代金を払え」と脅迫してお金を要求するのです。

他にも、感染させたパソコンや機器をボットネットと呼ばれる不正な仕組みに勝手に参加させ、所有者が知らないうちに、どこかのウェブサーバに大量のアクセス要求を送って反応できなくする「DDoS攻撃[*1]」などに利用することもあります。持ち主は知らないうちに攻撃に協力してしまうわけです。

攻撃者はこの攻撃用の不正な仕組みを時間制で貸し出して、対価としてお金を稼ぐこともあります。

＊1　DDoS攻撃：Distributed Denial of Service attackの略。多数の機器からサーバなどに攻撃をしかけ通信能力を超えさせ使えない状態にする

情報の不正送信やフィッシング詐欺

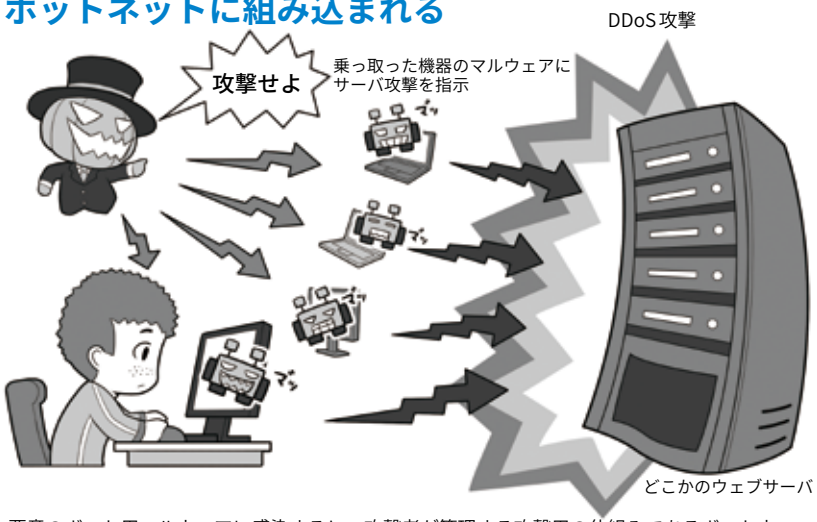


攻撃者はあなたから重要情報やお金を盗むために、マルウェアに感染させて重要ファイルを不正に送信させたり、偽のメールで偽の銀行サイトなどに誘導する「フィッシング詐欺」を行ったりします。どういう方法でだまされてしまうのか、一度調べてみましょう。

ランサムウェアで身代金要求

ランサムウェアに感染すると、パソコンなどのファイルを暗号化され、解除するためには身代金を要求されます。しかし、身代金を払っても解除するキーをもらえるとは限りません。普段からシステムやデータのバックアップを取って、元の状態に戻せるように備えましょう。どうやって侵入されるのか、実例の記事をさがして学んでみましょう。

ボットネットに組み込まれる



悪意のボット用マルウェアに感染すると、攻撃者が管理する攻撃用の仕組みであるボットネットに接続され、あなたが知らないところでサイバー攻撃に参加させられることになります。気づかずに加害者の立場になってしまうかもしれません。

3 サイバー関連の犯罪やトラブル

サイバー攻撃の他にも、ネットを使った犯罪やトラブルはたくさんあります。

たとえば「なりすましや誘拐・略取」。SNSなどで未成年と同じ年齢や性別になりすまして近づき、その上で相手を誘い出して誘拐や略取などに及ぶケース。あるいはSNSで家出などをした子どもの書き込みを見付けて、自宅に連れ込むケースなどもあります。

また同じようにネットで未成年のふりをして近づき、相手の警戒心を和らげて、「私も送るからあなたも送って」と裸の写真を要求して、入手したらその写真を使って相手を脅迫するケースもあります。

このような、子どもたちが自分自身の裸の写真を撮り、交換し合うことによって起こる被害を「自画撮り被害（セクスティング）」と言います。一度自分のスマホなどに記録された写真は、誰かに渡さなくても流出の危険がありますし、相手に渡してしまえばネットに流され、その後ずっと自分を苦しめ続ける可能性があることを考えなくてはいけません。これは子どもに限らず、つきあっていた相手が別れたことの腹いせに、裸の画像をインターネットに流す犯罪「リベンジポルノ」として問題になっています。

その他にもSNSやSNSのグループで誰かの悪口を言ったりする「ネットいじめ」は、やっている本人たちは軽い気持ちでも、時に相手を激しく追い込んで悲劇を招いたりするので、現実世界のいじめ同様、絶対にやってはいけないことです。

なりすましや誘拐・略取（連れ去り）

SNSなどであなたに近寄るために、年齢や性別を偽っている人がいます。同じ歳や性別になりすまし油断させて近づき、誘い出して略取や誘拐に及ぶかもしれません。基本的に実際に会ったことがない人がSNSで近づいてきたら、「そういう人かもしれない」と考え友だちにならないように！

自画撮り被害（セクスティング）

「自画撮り被害（セクスティング）」は裸の写真などを気軽に送り合ってしまうことで起こります。もしその相手が写真をネットで売ったりあなたを脅すためにやっていたりしたらどうでしょう。特に一度ネットに流出した写真は完全に消し去ることもできません。絶対にやってはいけません。

ネットいじめ

現実のいじめはもちろんのこと、ネットを使ったいじめもやってはいけません。ネットはみんなの未来を創るためのものであって、苦しめるためのものにしてはいけないのです。

4 一見サイバー攻撃に見えない「ソーシャルエンジニアリング」攻撃

さて「サイバー攻撃」ではなく一般的な犯罪で、皆さんがよく聞くものには何があるでしょう。たぶん「オレオレ詐欺」「振り込め詐欺」など、人を騙してお金を巻き上げる「特殊詐欺」があげられると思います。

関係機関が常に注意喚起をしていますが、未だに多くの方が被害に遭っています。

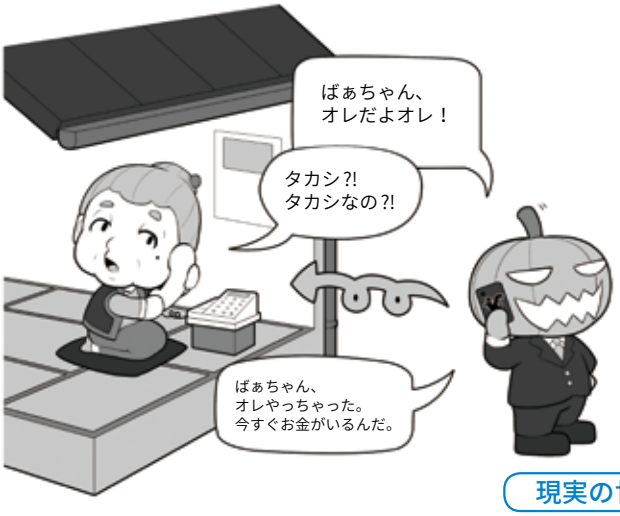
パソコンに例えると、セキュリティホールを必死に埋めようとしているのになかなか埋まらず、目の前で次々とサイバー攻撃が行われてしまっているような状況です。

それが終わらない理由は、人間の「心の隙」というセキュリティホールを突いた攻撃であり、人間のセキュリティホールは対策が難しいためです。そしてサイバー攻撃でも、この人間の心の隙を突いたものがたくさんあります。

たとえば、大企業ですら騙される「ビジネスメール詐欺(BEC)」の発端になる「標的型メール」。送りつける相手をよく調査・分析した上で、本人宛かつあたかも仕事の関係のメールに見える文面に、マルウェア等を添付して送り付け、本人がうっかりファイルを開くと感染させられてしまいます。

こういった攻撃による被害を軽減するためには、多くの人々がサイバーセキュリティに加えて「心の隙」についても詳しくなり、サイバー攻撃だけでなく、こういったハイブリッドな攻撃に関する危機意識が、みんなの心の中に常識として根付くようになることが重要なのです。

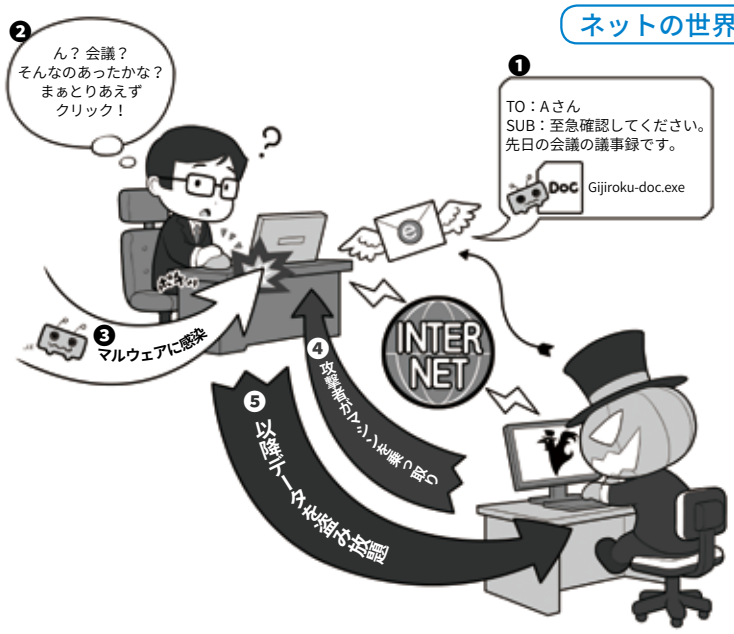
「ソーシャルエンジニアリング」は現実でもネットでも心の隙を突いてだます



現実の世界

この2つの共通点は人間の「心の隙」を突いた点

ネットの世界



振り込め詐欺の場合は、たとえばまず相手に「身内が事故やトラブルを起こして大変だ！」と思い込ませ、電話をかけている人間が誰か確かめるなどの、相手が本来持っている冷静な判断能力を奪います。せかしたり、弁護士や警察官に扮した人物を登場させたり、お金を払えば助かると交換条件を出したりといった心理的な揺さぶりは、古典的なソーシャルエンジニアリングの、「ハリーアップ」「ネームドロップ」「ギブアンドテイク」などに当たるでしょう。

一方、ネットの世界のソーシャルエンジニアリングは、知り合いになりすまして「標的型メール」を送る場合「フレンドシップ」という手法に当てはまります。

現実世界でもネットの世界でも、相手の心の隙を突けばどんなセキュリティでも破ることができます。そのだますテクニックが「ソーシャルエンジニアリング」なのです。ぜひ、そういうテクニックがあることを覚えてください。

この心の隙を突く攻撃は広い意味で「ソーシャルエンジニアリング」と呼ばれます。覚えておいてください。

第1章

基本のセキュリティ

～ステップバイステップでセキュリティを固めよう～

サイバー攻撃を受けにくくするための、簡単なセキュリティの固め方を理解しましょう。
またパスワードの管理の仕方や、攻撃する側が攻撃したくなくなるにはどうすればいいかを学びましょう。
人間の心の隙を突くソーシャルエンジニアリング攻撃などについても勉強しましょう。

1 4つのポイントで セキュリティを守る

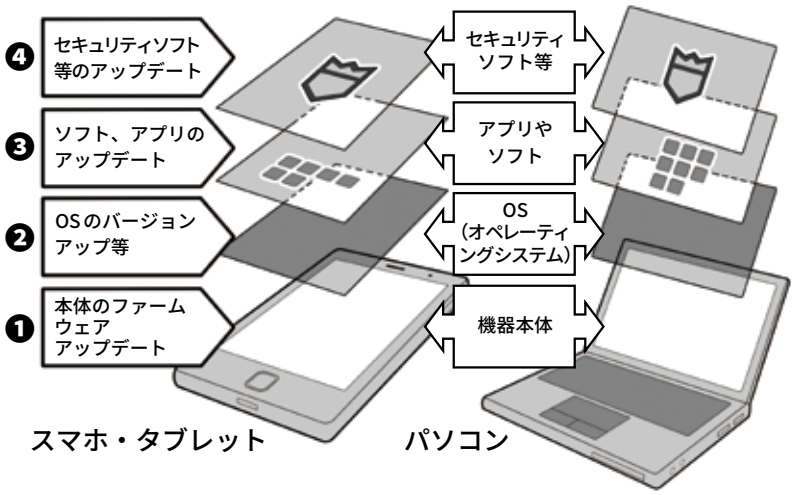
1 システムを最新に保つ。セキュリティソフトを入れて防ぐ

サイバー攻撃を防ぐための第一歩は、システムを最新の状態に保つことです。

まず機器の本体そのものに搭載されている「ファームウェアのアップデート」。次に私たちに操作するインターフェースを提供している「オペレーティングシステム（以下OS）のバージョンアップやアップデート」。そしてセキュリティホールになりやすい「ソフトやアプリのアップデート」を行います。

パソコンの場合それに加えてマルウェア検出などを行う「セキュリティソフトの導入とアップデート」です。なおスマホの場合、導入は必要性に応じてなので、P26を参照してください。これらを常時更新してセキュリティ上の穴をふさぎます。

様々な段階でセキュリティを守る



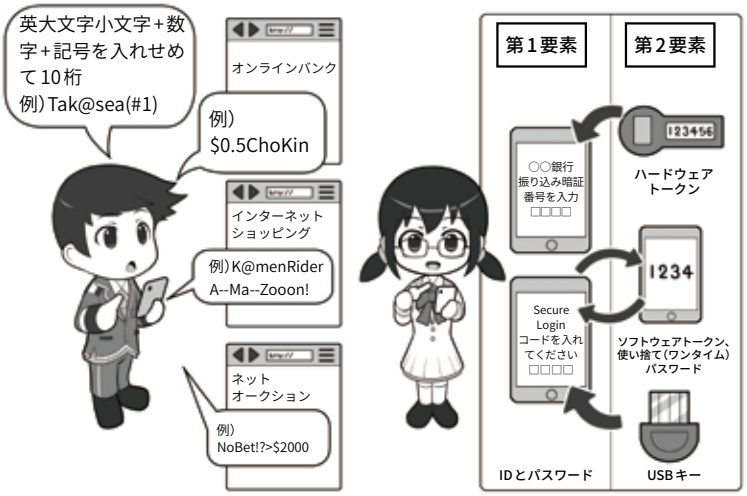
セキュリティソフトには無料のものもありますが、検知機能が有料のものと比べ不十分なものや、セキュリティソフトを騙ってマルウェアのような挙動をするものもあるので注意してください。どれを導入するか迷った場合は、プロバイダなどが提供するセキュリティパックか、信頼できるメーカーのソフトを導入しましょう。多少のコストがかかってもセキュリティ向上は安全への投資なのです。

2 複雑なパスワードと多要素認証で侵入されにくくする

次にサイバー攻撃で的になりやすいのはパスワードです。攻撃者がこれを入手するには「見つけ出す」のと「盗む」攻撃方法があり、まず攻撃でやられないように、購入時に設定されていたパスワードがあるものは必ず変更し、複雑なパスワードをサービスや機器ごとに設定しましょう。設定したパスワードを盗まれないように保管することも重要です。

続いて、仮にパスワードを盗まれても機器やサービスが乗っ取られないように、多要素認証などさらなる防御手段を追加しましょう。

複雑なパスワードや多要素認証でセキュリティを守る



サービスや機器間で使い回しのない英大文字小文字・数字・記号を使った複雑なパスワードを使う

多要素認証の導入や、ネットに流出しない実物としてのキーを利用する

3 攻撃されにくくするには侵入に手間(コスト)がかかるようにする

サイバー攻撃を行う攻撃者も、プロフェッショナルであるスパイを除けば、彼等にとっての効率が重要なので、より手軽に侵入できる状況を選ぶ傾向があります。

警備や戸締まりがしっかりしている場所に泥棒が入らず、鍵がかかっていない留守の家に空き巣が入るのは、その方が危険性(コスト)が低く手軽だからです。

サイバー攻撃でも同じように、侵入するまでに幾重にも防御がしてあると、攻撃者にとっては手間(コスト)がかかって面倒な、あるいはそもそも侵入できない対象となり、攻撃されにくくなります。

そのためには、システムを最新の状態に保ちセキュリティホールをふさぎ、セキュリティソフトを導入し、複雑なパスワードや多要素認証が必要になるわけです。

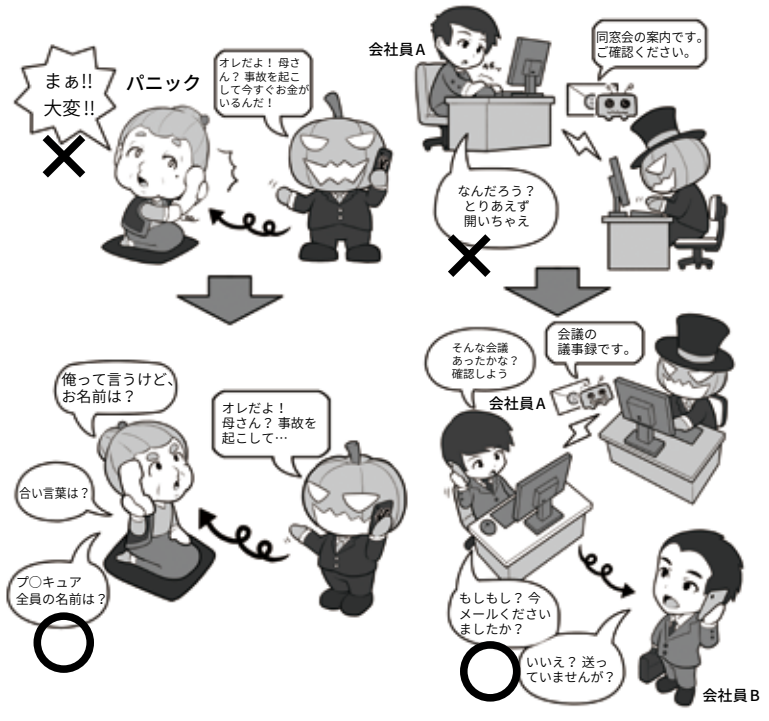
守りを何重にもして侵入されにくくする

4 心の隙を作らないようにする(対ソーシャルエンジニアリング)

しかしそれでも、ソーシャルエンジニアリングなどの手口で、心の隙を突かれて攻撃者に操られ、家の鍵を中から開けるような状況になってしまうことがあります。それを防がなければ、いくらシステム面でセキュリティを高めても意味がありません。システム面でセキュリティを高めることと、心の隙を作らないようにすることは車の両輪なのです。

振り込め詐欺ならば、電話で合い言葉を確認することで防御する。標的型メールなどのサイバー攻撃では、疑わしい通信手段とは別の通信手段で情報を確認するなどの対処法があります。これは項目の2にもあった多要素認証と同じ考え方で、攻撃を防ぐシンプルかつ有効な手段なのです。

心の隙を作らない。攻撃をうけつけない



2 環境を最新に保つ、セキュリティソフトを導入する

1 セキュリティソフトを導入して守りを固めよう

単純なウイルス検知ソフト、あるいは対策ソフトの場合、主としてマルウェアを見つける方法は「手配書」方式になっています。

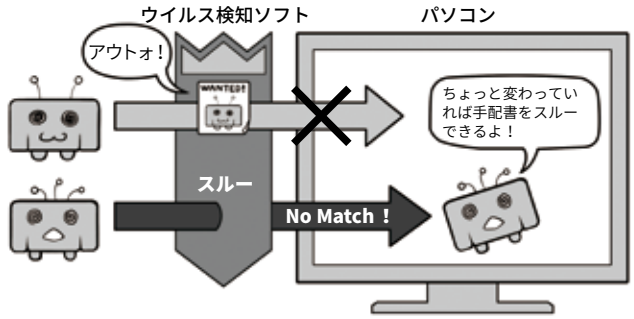
手配書方式とは、あらかじめ検出したいマルウェアの特徴を、販売元からそれぞれのパソコンなどに送信しておき、マッチしたものを駆除する方式です。

しかし現在では攻撃者が、発送先ごとに送信するマルウェアを微妙に変えたり、狙いを定めて専用に作ったりする場合もあるので、この方法では見つけ出すことが難しくなりつつあります。

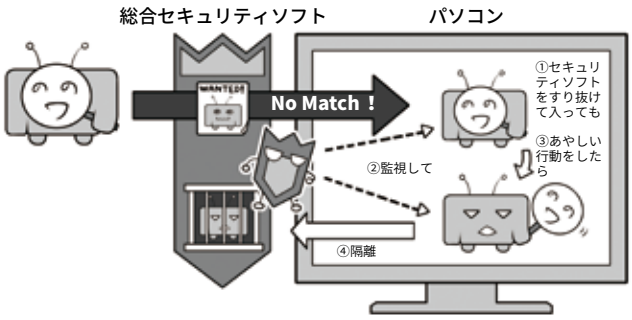
そこで最近の総合セキュリティソフトでは「手配書」方式に加えて、パソコンに入ってしまった後も監視を続け、不審な行動を取れば隔離なり駆除をする、「ふるまい検知」や、機能的に怪しい部分を検出する「ヒューリスティック分析」機能を持つものが出てきています。これにより未知のマルウェアにもある程度は対処できるわけです。

しかし、それでも対処しきれないものもあります。システムのセキュリティホールが発見され、それが修正される前に攻撃する「ゼロデイ攻撃」を行うマルウェアです。この場合は手配書も間に合わないので、現状では決定的に有効な手段がほとんどありません。しかし、そう言ったことを踏まえても総合セキュリティソフトを導入することには多くのメリットがあります。ぜひ導入してパソコンの守りを固めましょう。

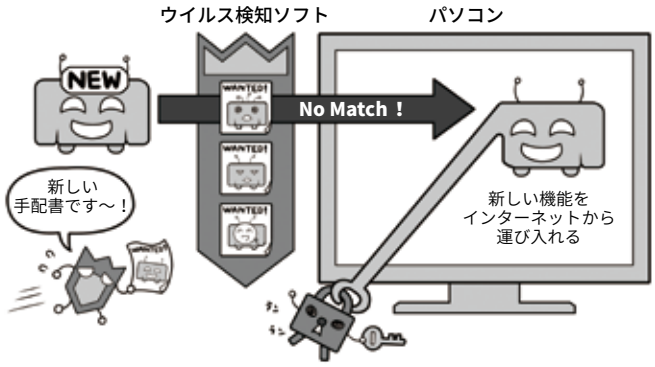
単純なウイルス検知ソフト



進化したセキュリティソフト（総合セキュリティソフト。ふるまい検知、ヒューリスティック分析あり）



手配書が間に合わないゼロデイ攻撃も



2 パソコン本体とセキュリティの状態を最新に保とう

パソコンのセキュリティを最新に保つためには、各種のアップデート処理が不可欠です。

最近の機種ではたいていの場合、OS関連のアップデート処理は自動で行われるか、アップデートを行うよう警告が出るようになっています。ただ、時として重大な脆弱性が発見され、緊急でアップデートを行ったほうがよいこともあります。セキュリティ関連ニュースサイトなどでそういった情報が流れていたら、自主的に更新処理をかけるようにしましょう。Office製品などOSのメーカーが作っている重要なソフトもここで同時にアップデートされます。

次にサイバー攻撃で狙われやすいソフトの更新を重点的に行いましょう。Adobe Flash Player、Adobe Acrobat Reader、Oracle Javaや各種のウェブブラウザはよく使用されるため、攻撃のターゲットになりやすいのです。

また本体機器そのもののプログラムを更新するファームウェアアップデートにも気を配りましょう。こちらの更新通知は、自動で出る機器と出ない機器があるので、自分の機器にファームウェアアップデートがあった場合、どういうようにその情報を入手するべきか、確認して気を配ってください。

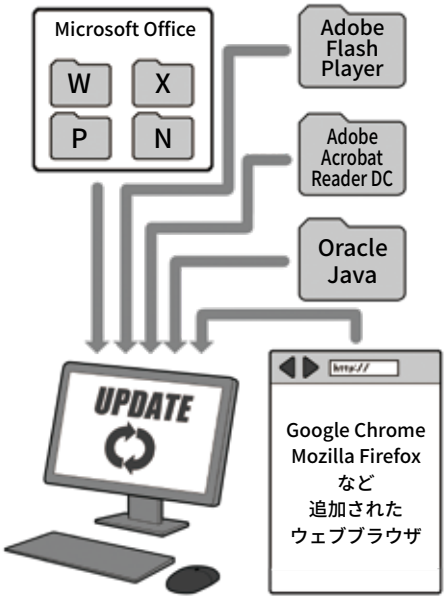
セキュリティソフトも基本的にはインストールすると自動更新されるようになりますが、なるべく日に一度は意識的にセキュリティソフトの画面を見るようにしましょう。これはセキュリティの状態を確認する意味もあります。

本体もOSもセキュリティソフトも重要ソフトもアップデート

本体のファームウェアも更新

OSと基本ソフトの更新

重要ソフトも更新



セキュリティソフトも更新

ここであげられている重要ソフトは、社会で言えば鉄道や電気ガス水道のような社会インフラに相当し、そのためほとんどのパソコンで利用されています。たとえば社会インフラがテロ攻撃などで狙われやすいのは、攻撃者が少ないコストで多大な影響を与えることができるからで、こういった重要ソフトが狙われやすいのも同じ理屈なのです。ですから、利用する側も重要ソフトの更新があったら速やかに適用して、攻撃者が攻撃できないようにしましょう。重要ソフトを使っていない場合は、削除してしまっても良いでしょう。

別項目でも登場したボットネットも攻撃して乗っ取れる機器がなければ成立しないように、穴を作らない一人ひとりの行動が安全なネットを作るのです。

3 スマホやネットワーク機器も最新に保とう

スマホも同様に各種のアップデートが必要です。

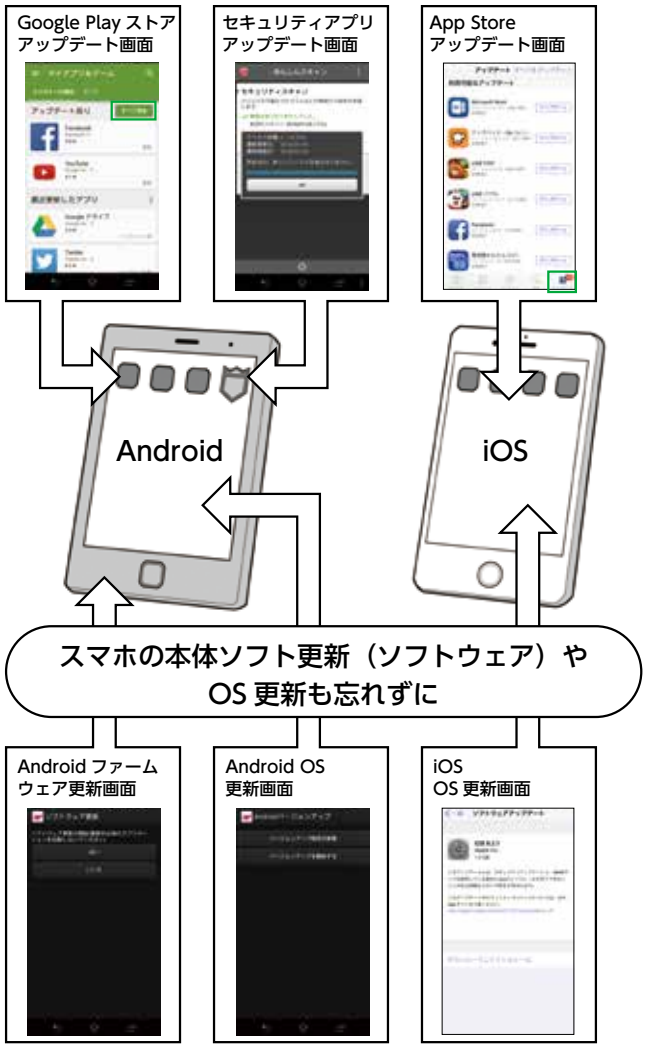
スマホの場合、比較的アップデートの通知がわかりやすくなっており、また自動アップデート機能も充実しています。機器そのもののソフトウェアの更新でもOSのアップデートでも、いつも使用している一般のアプリでも、更新の通知が出たら、マメにアップデートするようにしましょう。

そのためには本体のファームウェア(ソフトウェア更新やシステムアップデート)やOSの更新が、設定メニュー上のどこにあるのか更新手順を確認しておきましょう。またアプリの更新が自動になっているかも確認しましょう。

スマホアプリの自動更新は、設定によっては無線LAN接続時のみ自動で行うことになっている場合もあり、またその設定でも更新時に権限変更で確認が必要な場合は自動更新されないこともあるので、気がついたら更新されていないアプリがたくさんたまっていることもあります。意識してアップデート画面に行き、更新作業をするように心がけましょう。

またネットワークにつながるスマート家電やIoT機器などは、こういった通知がなく、アップデートが公開されても、気づかずセキュリティホールが開いたままになっていることもあります。週1回でも月1回でもアップデートファイルが公開されているかチェックしましょう。特にネットワークカメラなどは適切に管理しないと不正に利用されることがあります。

アプリやセキュリティソフトの更新は基本的に自動にし、まめにチェック



ネットにつながる家電もファームウェア更新や設定ページのID・パスワードの変更をしておくこと

Wi-Fiルータ　ネットワーク対応プリンタ　ネットワークカメラ

スマート家電のファームウェアの更新は、通常はウェブブラウザで本体にアクセスして行います。この時のID・パスワードは必ず購入時から変更しておきましょう。不正アクセスされ、カメラなどでは覗き見される原因になります。

4 ソフトやアプリは原則公式ストアから。権限にも気をつける

本体やシステムを最新の状態に保っても、防ぎにくい攻撃があります。それはまだマルウェアとして認識されていない悪意あるソフトウェアなどの侵入です。

基本的にセキュリティソフトなどがマルウェアを検出するためには、過去に収集されたデータが必要になります。このデータが多ければ多いほどマルウェア検出の精度は高まるのです。現実世界で病気の検体が多ければ、より確実な対応方法を得られるのと同じです。

これとは逆に、セキュリティソフト会社がまだ知らないマルウェア、あるいは検体が充分に収集されていないマルウェアは、検知ソフトなどでの発見が難しくなります。

攻撃者が、チェック体制のしっかりしている公式ストア経由ではなく、私たちをメールなどで誘導し、不審な場所から導入させようとする理由もそのためです。

そのような手に引っかかってマルウェアに感染してしまわないように「ソフトは信頼できる場所から、アプリは公式ストアから導入する」ことが推奨されるわけです。

特にスマホの場合、iOS機器は公式のストア以外からはアプリを導入できない仕組みになっていますが、Android機器の場合は公式ストアやベンダーメーカーのストア以外からもアプリをインストール可能なので、攻撃者がメールなどであなたを誘導して、公式ストアでない場所からインストールさせる、あるいはインストールの過程で「不明なアプリ」と言った言葉を見る方法は避けましょう。

基本的にアプリを公式ストアではない場所からインストールしない。権限付与にも気をつける。

「不明のアプリ」という言葉に注意

・Android
該当の項目や細かい文言は、使用するAndroidのバージョンやスマホメーカーによって異なる場合がありますが、アプリのインストール時に「不明なアプリ」と画面上に表示されたり、設定内の「不明なアプリ」に関する項目を変更させようとするものは、すべてセキュリティ上危険なものと判断して下さい。
アプリは基本的に公式ストアからのみインストールするようにして、その他の場所からは避けましょう。

導入時や起動時の権限付与に注意

・Android、iOS（画面はAndroid）
アプリのインストール時や起動時にさりげなく表示されるため、多くの人が無意識に「承認」や「同意」してしまっていますが、これは「アプリがこれらの情報に自由にアクセスできる許可」を求めている画面です。
個別に却下することができない場合もあるので、その際は導入しないようにしましょう。そしてそもそも不必要な権限を求めるアプリは怪しいと警戒しましょう。

また Android でも iOS でも、アプリのインストール時や初回起動時に、同意を求められる「権限」には充分注意してください。権限とはインストールするアプリに対して、スマホのどの機能の利用を許可するか、という確認です。

単なるカメラアプリなのに住所録にアクセスするものや、撮影する必要がないのにカメラにアクセスするもの、著しく多くの項目にアクセスしようとするものなどは要注意の例です。項目別に許可を却下するか、そうできない場合、そのアプリは導入しないようにしましょう。また最初は無害に見えて、導入後のアップデートで権限の変更の許可を求めるものも、その変更項目に注意してください。

そのほか、アプリ間での機能連携やウェブサービス間で連携して、間接的に権限を奪取するものもあるので「連携」という言葉にも充分注意してください。

コラム：必要ならばスマホには セキュリティパックを検討しよう

スマホの場合、その誕生が比較的最近であることもあり、設計思想自体にセキュリティの概念が盛り込まれていて、パソコンなどと比較して、セキュリティアプリなどが担う役割が大きくはありません。

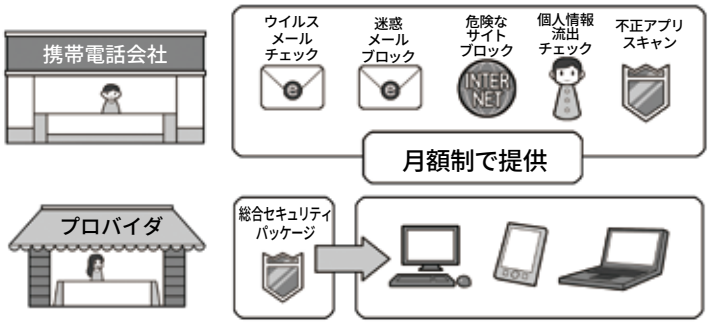
しかしチェックするべき点を見落とし、気づかないうちにインストールされる不正なアプリの検出や、またそういったものの侵入経路になるメール、危険なサイトのブロック、あるいは個人情報の流出チェックなど、セキュリティ全般にかかわる機能を補助的に導入したい場合もあるかもしれません。

そういった場合は、携帯電話会社やプロバイダなどが、セキュリティアプリを含め、セキュリティ機能をまとめて提供するパッケージを、内容を充分に精査した上で導入しても良いでしょう。

なお、メーカーが作ったスマホのセキュリティ思想は、定められた利用方法から外れると、とたんに脆弱になり攻撃されやすくなるので、Android の「root 化」や iOS の「JailBreak」といった改造は絶対にやってはいけません。

また、高機能化するスマート家電など IoT 機器についてもス他と同様にセキュリティ対策が必要になります。103 ページも参照して、万全の対策を講じていきましょう。

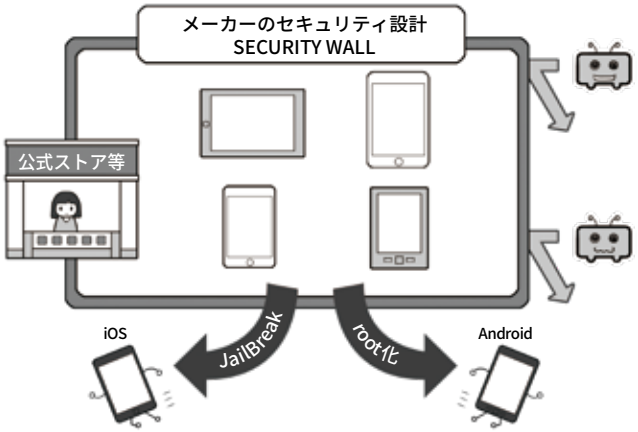
必要性を感じるなら、スマホには セキュリティパック導入を検討しよう



上記のようなサービスをまとめて複数台に月額制で提供

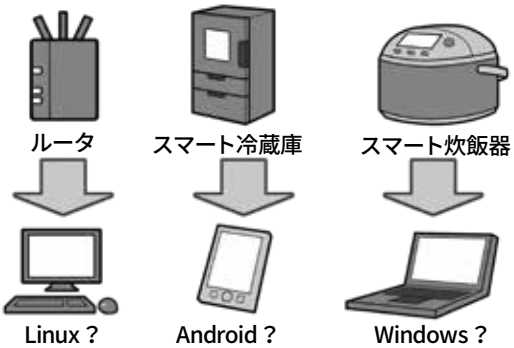
携帯電話会社からはセキュリティ関係の機能がパッケージ化されて提供され、インターネットプロバイダも同様のサービスを提供しています。自分が求める機能があるかを精査して、必要性を感じる場合は導入を検討しましょう。

スマホの改造をしてはいけません



スマホのセキュリティ思想はメーカーが想定する利用方法を守っていることが前提条件です。「root 化」や「JailBreak」といったソフトウェアの改造は、規約違反である場合もあり、セキュリティ上も脆弱になるので非常に危険です。やってはいけません。

スマート家電の中にはパソコンやスマホがある？



スマート家電は一見ただの機械に見えて、実は内部に Linux というコンピュータシステムや、Android、Windows マシンが入っていることがあります。乗っ取られ、サイバー攻撃に利用されるなどの可能性もあるので、セキュリティ対策が必要です。

コラム：パソコンやスマホを最新の状態に保っても防げない攻撃がある。それがゼロデイ攻撃！

一般的にはシステムやソフトにセキュリティホールが見つかると、攻撃者はこの穴を攻撃するためのマルウェアを急いで開発し始めます。メーカーもこの穴に気づけば、アップデート用のセキュリティパッチを開発し公開します。

通常この競争に勝つのは攻撃者で、このようにセキュリティホールが発見されてからメーカーによって修正されるまでの期間を狙って攻撃することを「ゼロデイ（ZERO DAY）攻撃」と言います。

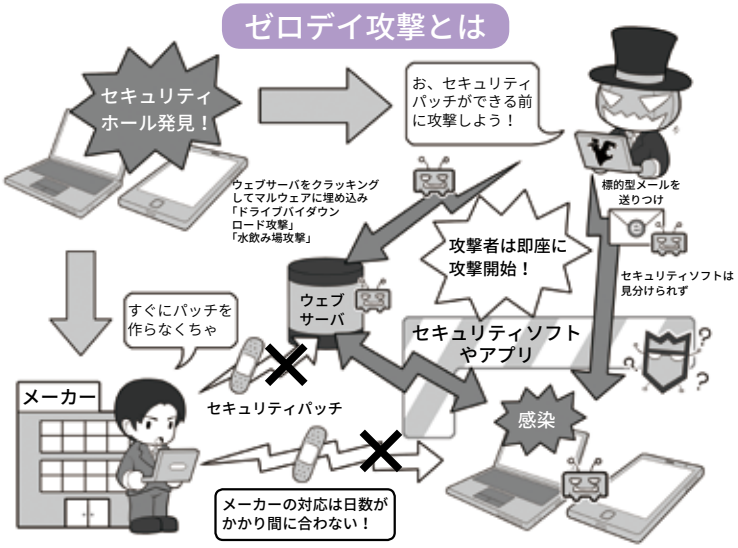
メールで送りつけられるマルウェアは、警戒していればある程度防ぐことができるのですが、動画、ウェブサイトやウェブ広告に仕込まれるマルウェアは、特定のサイトを見ただけで感染することもあり、情報が無いままこの方法でゼロデイ攻撃を受けると実質的に防ぐことができません。

特に最近では攻撃者が、お金を支払ってまで、マルウェアの仕込まれた動画ウェブ広告を大手サイトに出してサイバー攻撃を仕掛けてくるため、その規模も非常に大きくなってきています。これは広告を出すコストが、不正に入手できるお金に見合っているということを意味しています。

被害を少しでも避けるためには、セキュリティ情報サイトやSNS（NISCのtwitter（内閣サイバー（注意・警戒情報））など）をこまめにチェックして、たとえば動画系のマルウェアが登場したら動画の自動再生機能をOFFにする、スマホ用アプリであればセキュリティホールが修正されるまでアンインストールするなどの対応をしましょう。アプリを提供するサービスは、アプリを使用しなくてもウェブブラウザで利用可能なこともあるので、普段からスマホなどでもウェブブラウザ経由での利用に慣れておきましょう。

ゼロデイ攻撃とは？ 対処の例

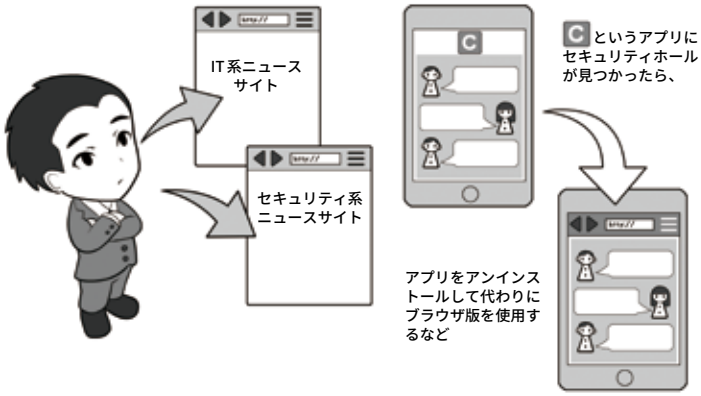
ゼロデイ攻撃とは



ゼロデイ攻撃に対抗するには？

ニュースサイトをこまめに見て情報収集

別の手段でセキュリティホールを避ける



攻撃者とメーカーのゼロデイ攻撃に関する対応競争は、たいていの場合攻撃者が先行します。攻撃者はメーカーが気づいていない情報を入手し、対象の機種どれが一つでも攻撃に成功するなら攻撃を開始できますが、メーカーは情報を入手し精査した上で、対象となっている機種全てで充分な対応をしなくてはいけないからです。

ですから利用者もそれを前提として備え、対処行動をする必要があります。そうすることが結果として自分を守ることになるわけです。

3 複雑で長いパスワードと多要素認証で侵入されにくくする

1 パスワードの安全性を高める

攻撃者のサイバー攻撃には、相手の機器をマルウェアに感染させる方法の他に、なんらかの手段でIDとパスワードを解明し、相手の機器を乗っ取るものもあります。

パスワードは、ウェブサービス等が保管しているものが流出して使われる「リスト型攻撃」、文字の組み合わせを全て試す「総当たり攻撃」、パスワードによく使われる文字列を試す「辞書攻撃」などにより探し当てる方法や、IoT機器購入時のものをそのまま利用していて乗っ取られる場合もあります。

総当たり攻撃を防ぐには、探り当てるまでに膨大な時間がかかるようにするのが一番の防御手段で、それには1桁の文字の種類と桁数による組み合わせを増やします。

たとえば数字だけなら1桁10通りしかありませんが、英字を入れると36通り、英大文字小文字を入れると62通り、これに26文字の記号を入れると88通りになります。これに桁を増やして、累乗で組み合わせを増やすわけです。

総当たり攻撃は、攻撃し続ければ理論上はいつかは成功するのですが「時間がかかり事実上不可能な状態」にして防ぎます。ログイン用パスワードであれば入力ごとに時間がかかるので、英大文字小文字＋数字＋記号混じりで10桁以上を安全圏として推奨します。しかしより長くして安全性を高めるにこしたことはありません。

ログイン用パスワードは英大文字小文字＋数字＋記号で10桁

「ログインに使うパスワードは、英大文字小文字＋数字＋記号で10桁以上」の理由

数字のみだと→100億通り

英大文字小文字＋数字＋記号（26個として）だと→
約2785京97兆6009億通り

数字だけで10桁と、英大文字小文字＋数字＋記号で10桁では雲泥の差がある。
そしてこれほど多量な組み合わせは、機械入力でも事実上突破不可能。

英大文字小文字＋数字＋記号混じりの組み合わせ数

アルファベット（大）＋アルファベット（小）＋数字＋記号（例）
26　＋　26　＋　10　＋26＝88

数字	英大文字	英小文字	記号	合計		5	6	7	8	9	10
10				10	数	100,000	1,000,000	10,000,000	100,000,000	1,000,000,000	10,000,000,000
10	26			36	数英	60,466,176	2,176,782,336	78,364,164,096	2,821,109,907,456	101,559,956,668,416	3,656,158,440,062,976
10	26	26		62	数英大小	916,132,832	56,800,235,584	3,521,614,606,208	218,340,105,584,896	13,537,086,546,263,552	839,299,365,868,340,224
10	26	26	26	88	数英大小記	5,277,319,168	464,404,086,784	40,867,559,636,992	3,596,345,248,055,296	316,478,381,828,866,048	27,850,097,600,940,212,224

2 機器やサービス間でのパスワード使い回しは「絶対に」しない

また複雑なパスワードを使っても、それを複数の機器やサービスで使い回していれば意味がありません。1カ所から漏れれば全てログイン可能になります。また複雑なパスワードを1つ決めて、あとはおしりに数字や規則性のある文字をつけるのも、1つ漏れれば推測されます。それぞれに複雑なパスワードを設定し、使い回しをしないことが大切です。

同じパスワードを使い回さない。似たパスワード、法則性のあるパスワードも×

	白うさ ネットワーク	おさるさん 銀行	三毛猫電気	たこ クレジット	
×使い回し	PASSPPOI	PASSPPOI	PASSPPOI	PASSPPOI	全部同じ
×おしりだけ違う	PASSPPOI1	PASSPPOI2	PASSPPOI3	PASSPPOI4	推測しやすい
×法則性あり	USAGIPPOI	OSARUPPOI	NEKOPPOI	TACOPPOI	法則性がばれたらおしまい

3 パスワードを適切に保管する

使い回しをせず充分な複雑さと長さを持ったパスワードは、総当たり攻撃では突破されにくくなりますが、適切に管理しておかず、別の方法で盗まれてしまってはひとたまりもありません。

たとえばパソコンや壁に貼っていれば、誰かがそれを見て覚えてしまいますし、ファイルにまとめておけばマルウェアに感染した時に流出し、多くのアカウントが一気に乗っ取られるかもしれません。

パソコンでウェブブラウザに覚えさせる「オートコンプリート」機能も要注意です。あなたが席を離れた隙に、誰かがブラウザでサービスを利用してしまうかもしれませんし、ノートパソコンならば本体ごと盗まれることもあります。パスワードは基本的に利用する場所で保管してはいけないのです。

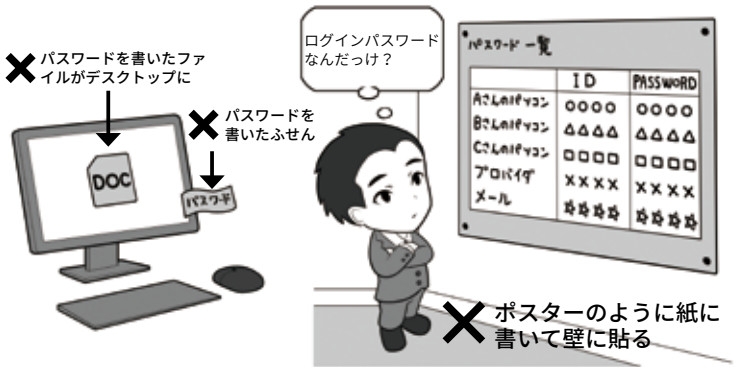
しかし、多くのサービスで複雑なパスワードを設定したら、とても覚えきることはできません。ではどうしたらいいでしょう。

一つはパスワードを管理するノートに書いてパソコンとは別に保管する方法、もう一つはスマホのパスワード管理アプリを利用する方法です。なお後者の場合、クラウドでデータを保管する機能の利用は熟考し、過去に情報流出にまつわるトラブルのあったアプリは避けるようにしましょう。それは他人の手元にIDやパスワードを保管することや、流出の危険が逆に増すことを意味するからです。

利用するところで保管するべきでないなら、スマホでもパスワードを使う場合リスクはありますが、こういったアプリは後述のPINコードや指紋認証＋暗号化で情報がガードされます。盗まれても落としても、簡単に他人が使ったりすることはできません。

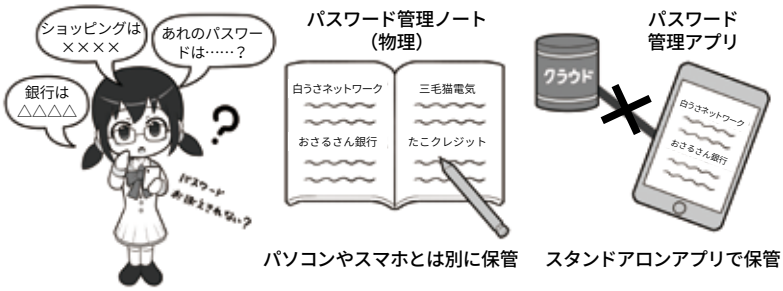
ただ管理しているパスワードは、必ずバックアップするのを忘れないようにしましょう。落としたスマホが戻るとは限りませんから。

パスワードを使用する場所に置かない。パソコンの中も×



オフィスの中ならば外の人は見ないと判断するのは×。出入りの業者が見たり、外から双眼鏡で見たりすることもできるのです。

パスワードはノートに書いて保管するか、パスワード管理アプリで守る

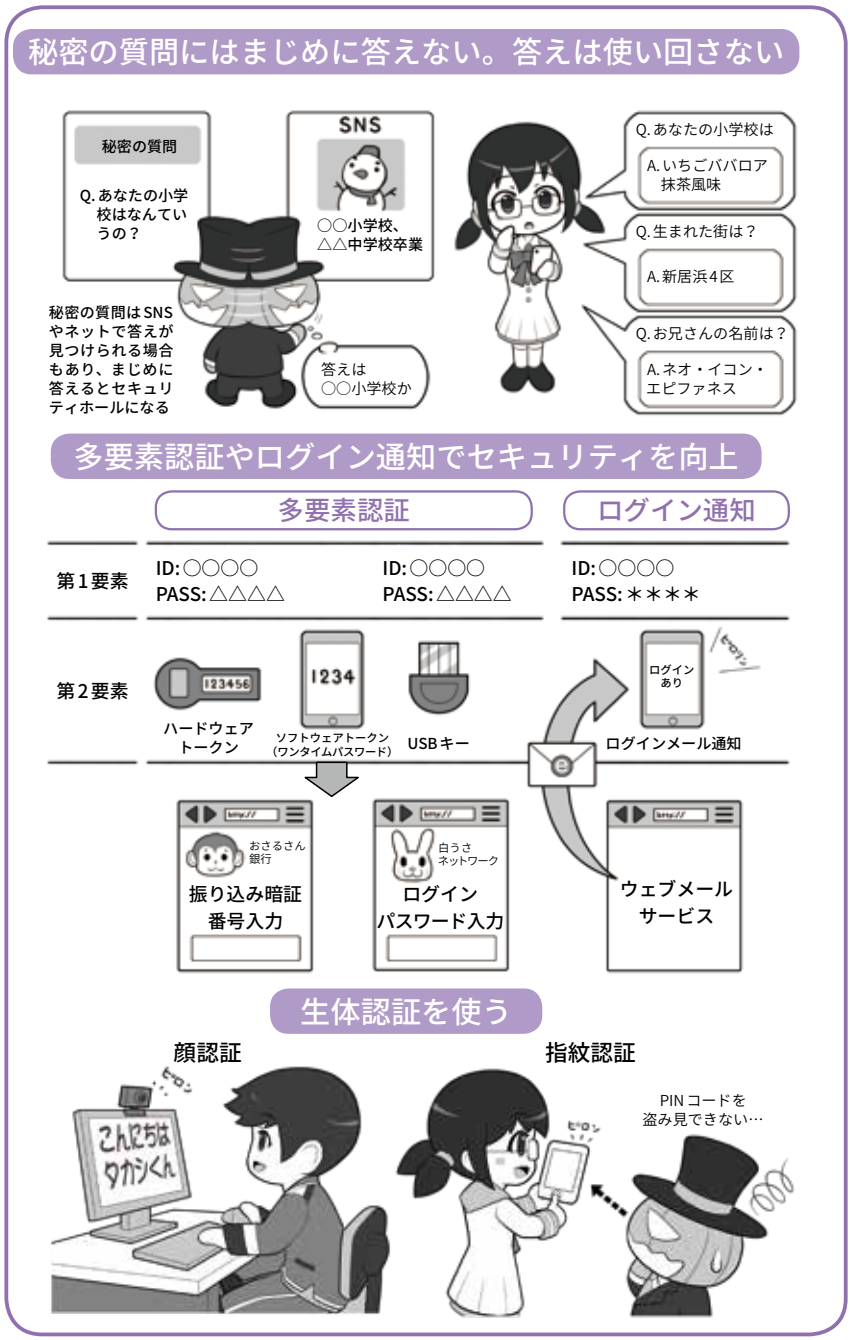


クラウド保管＝ダメというわけではなく、それは利便性との兼ね合いです。アプリの機能や過去のトラブルは、アプリ名＋「トラブル」などで検索します。

ブラウザの自動入力にパスワードを覚えさせない

パスワードなどの自動入力は便利ですが、仕事場などで、あなたがパソコンをロックしないまま席を離れると、各種サービスにログインし放題になります。

4 秘密の質問にはまじめに答えない。多要素や生体認証を使う



各種のウェブサービスには、パスワードを忘れてしまった場合の本人確認、あるいはいつもと違うログインがあった場合の本人確認のために「秘密の質問」と呼ばれる機能があります。これはあらかじめ利用者が、自分しか知らない質問と答えを設定しておいて、合い言葉的にこれに答えるものです。

この秘密の質問には自分で質問を作れるものもありますが、多くは「生まれた市は」とか「ペットの犬の名前は」のように、生活に密着したものからしか選べなくなっています。しかしSNSが普及している今、こういった個人にまつわる情報は簡単にネットで見つけられることもあり、セキュリティ上、安全とは言えなくなっています。

ですから秘密の質問に答えを設定する場合は、まじめに答えず、あえて全く関係ない答えとすることで、SNSなどから推測できないようにし、その上で忘れないように管理アプリ等に保存しましょう。

またサービスへのログインを安全に行うために、複数の要素を使って認証する二段階認証や多要素認証といった方法が提供されていれば必ず設定しましょう。これらの方法では通常のパスワードの他に、その時に一度きり使用する使い捨てパスワードを、ハードウェアトークンや生成アプリで作り、ログイン時に利用者に入力させます。(メール方式で送信方式もありますが、安全面で非推奨です)

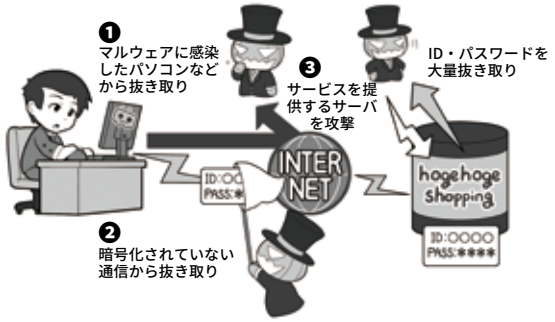
そのほかにもUSB式の鍵(キー)で利用者を確認する方法や、あるいはサービスにログインがあった時に通知をメールで利用者に送ることで不審なログインを検知する機能もあれば活用しましょう。

また最近の機器では3次元の立体的な顔形状や、虹彩や指紋で本人確認をして機器のロック状態を解く生体認証機能もあります。

生体認証は本人のみが使える反面、指紋認証などは寝ている間に勝手にロック解除されることがあるなど善し悪しですが、肩越しの盗み見などよる暗証番号(PINコード)の盗難には強い機能でもあります。なお生体認証はたいていは通常の数字コードの入力の替わりなので、スマホでは失敗すると通常の数字入力に戻ります。本体を盗まれてこの方式でロック解除されないよう、誕生日などの個人情報は使わないようにしましょう。

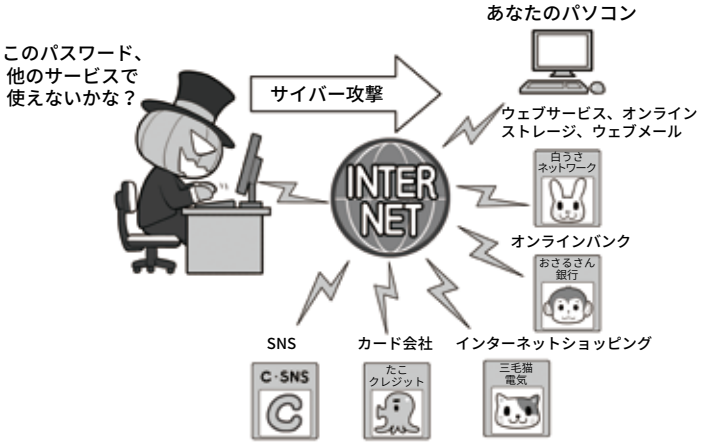
コラム：パスワードはどうやって漏れるの？どう使われるの？

様々なID・パスワードの抜き取り方法



攻撃者にIDとパスワードが抜き取られる方法は、機器がマルウェアに感染したり、自分が通信する過程で抜き取られたりするほかに、利用しているサービス側からも流出する可能性があります。サービス側から流出した場合は、速やかにパスワードを変更するなどの対応を取りましょう。

盗んだID・パスワードを使い、様々なサービスを乗っ取れるか試す



ID・パスワードを何らかの手段で手に入れた攻撃者は、これをどこか別のサービスで使えないか様々な方法で試します(リスト型攻撃)。こういった攻撃を成功させないために、パスワードの使い回しや、似たパスワード、個人情報など推測できるパスワードを利用するのはやめましょう。

私たちがパソコンやスマホ、あるいはSNSやウェブ上のサービスを利用するときに入力するIDやパスワード。サイバー攻撃でこれらの情報を盗まれると、かなり深刻な被害を起こしかねないものですが、では実際はどのように漏れてしまうのでしょう？

一つには、自分のパソコンなどがマルウェアに感染し、そのマルウェアがパスワードを盗み取って攻撃者に送信するケース。次に、ウェブサービスなどにログインするときに、私たちが利用する機器からウェブサービスまでの経路上のどこかで盗み取られてしまうケース。そして、ウェブサービス側でログインを認証するために控えとして持っているIDやパスワードが、攻撃者によって盗み取られるケースなどがあります。

ここで知っておいてほしいのは、自分がマルウェアなどに感染していなくても、漏れてしまうケースがあると言うことです。さらにIDやパスワードを普段入力してしないから安心、とも言い切れません。

そしてIDとパスワードを盗み取った攻撃者は、それでどこか別のウェブサービスなどを乗っ取れないか、様々な所で試します(リスト型攻撃)。

あなたが複数のサービスでIDとパスワードを使い回したり、あるいは似た形のパスワードを使っていると、これらのサービスのアカウントを一気に乗っ取られます。あとはオンラインショッピングで勝手に物を買われてしまったり、現金は送れなくても何らかの送金システムが利用できる場合は、それを使ってお金を奪い取られたりされてしまうわけです。もしパスワード流出が判明したら、まずはすぐに変更しましょう。

4 攻撃されにくくするには、手間(コスト)がかかるようにする

サイバー攻撃をする攻撃者は、軍事や産業スパイ、名をあげることを目的に採算度外視でやる悪意のハッカーなどではない場合、何らかの利益が目的の行動が多いと言うことができるでしょう。

それは彼等にとってのビジネスであり、ビジネスはコストパフォーマンス、つまりいかに手間をかけず大きな利益を生むかが重要です。

そういった攻撃者の視点から見ると、攻撃されにくい環境を作るにはどうしたらいいかが見えてきます。

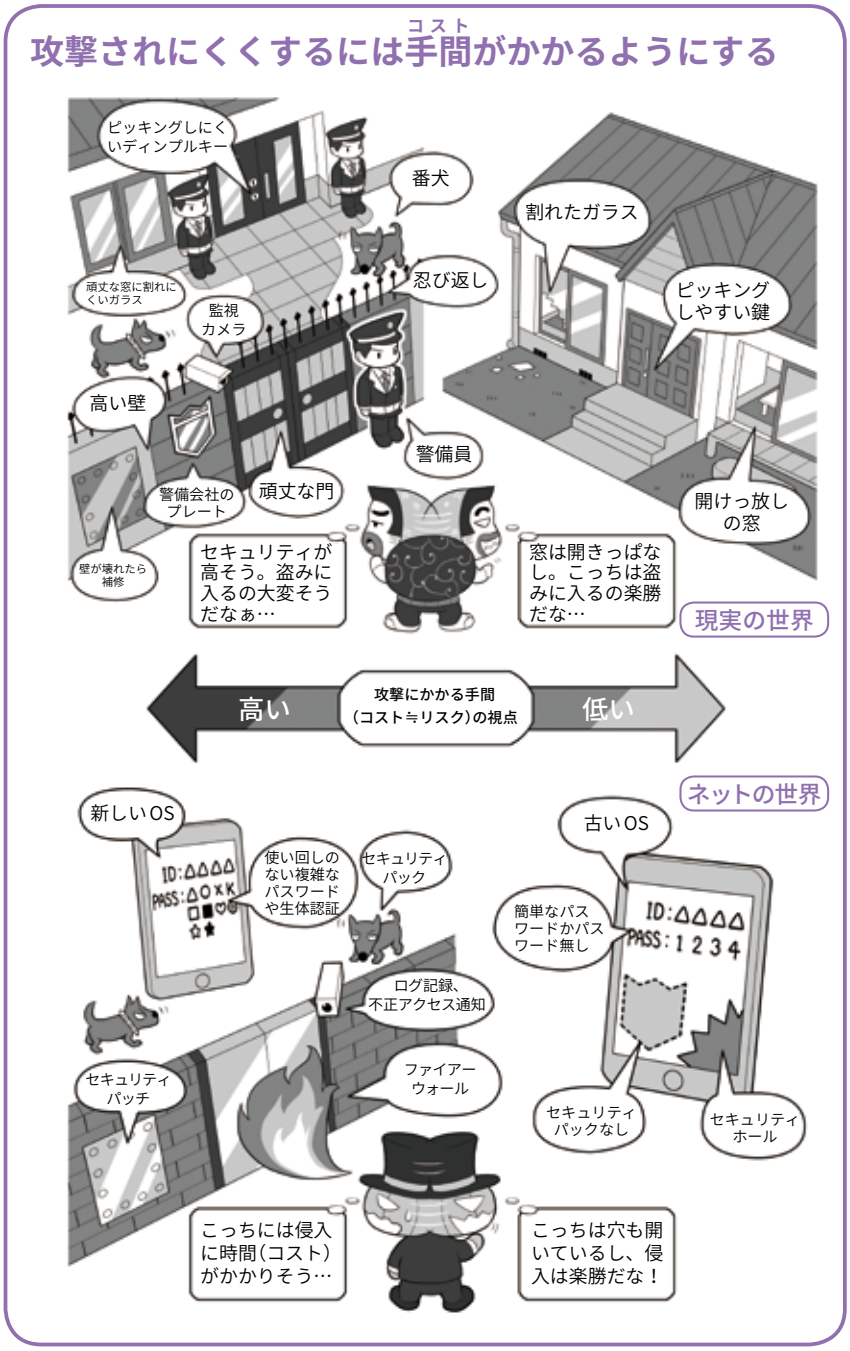
たとえば現実世界では、泥棒は防犯がしっかりしていて警戒が厳重な家よりも、鍵をかけなかったり窓を開けっ放しで外出したりするような家の方に侵入します。その方が彼等にとって安全、つまり手間(コスト)がかからないからです。

これはネットの世界でも同様です。侵入するまでに幾重にも難関があり、侵入を試みたら形跡を記録され(ログ)、場合によってはしかるべき管理者に通知が行き、パスワードを破ろうとしても複雑で突破できない。システムも最新で攻撃するにもセキュリティホールが見あたらない。セキュリティソフトも導入されている。さらにファイルを盗めても複雑な暗号化がされていれば、解読までに何百年もかかってしまい使えない。普通の攻撃者なら敬遠します。

横を見たら、セキュリティホールは放置、パスワードは非常に簡単だったりなしだったり、ファイルそのものも暗号化されておらず、さらにパスワードを使っていても、たくさんのサービスで全部同じものを使い回している。

これならばどっちに行くのがビジネスとしてコストパフォーマンスがいいか明らかですよね。

ですからこういった攻撃者の視点を持ち、侵入することがとても面倒くさく、攻撃したくなくなるような環境を構築するのが安全への近道です。一方単純な利益目的でない場合、すこし対策が変わってきます。



金銭などの利益目的ではない攻撃には、相手そのもの、つまり未成年者略取や、いかがわしい写真の入手などを目的とするものがあります。

現実の世界で面と向かって「いかがわしい写真を撮らせてください」と言ったら、たいていの人は拒否するし逃げ出すでしょう。それがネットの世界だと許容してしまう理由は、攻撃者がネットを利用して警戒心をもたれないような人間になりすまし、相手をうまくだましてしまうからです。

ですからSNSや掲示板などのサービスで知らない人物が近づいてきたら、まず注意し絶対に個人情報は教えないようにしましょう。現実の知り合いでもないのに会おうと誘われた場合は、基本的に会わないか、会う必要がある場合は必ず大人か保護者同伴で行くようにしましょう。

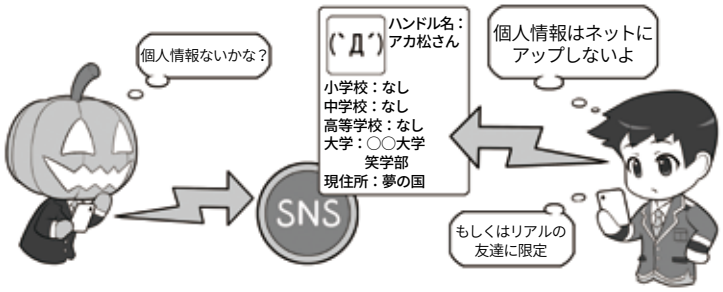
そして少しでも変だなと思ったり、最初と話が違ったりした場合、それは人をだます「心理的な」テクニックかもしれません。警戒し、その場から帰る選択をしましょう。

あまり聞いたことがないかもしれませんが、そういった「人をだます心理的なテクニック(≒ソーシャルエンジニアリング)」は体系化されマニュアルのようになって存在するのです。

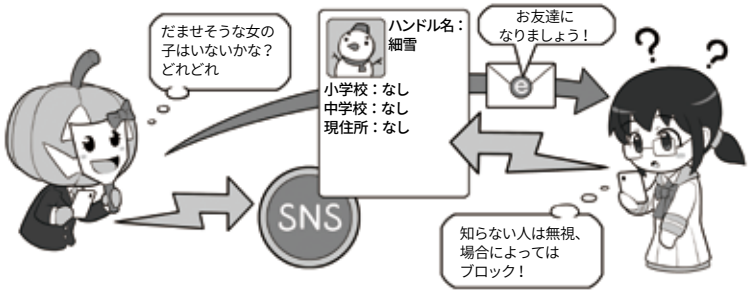
そしてこの人をだますテクニックは、なにも上記のような例だけでなく、私たちも日常生活の様々なシーンで直面しているのです。

たとえば「振り込め詐欺」や「標的型メール」。どんなにセキュリティを固めても、本人がだまされ結果として犯罪者に操られてしまうと、全ては無意味になってしまいます。厳重に注意しましょう。

金銭目的ではない攻撃にも備えよう



個人情報はネットに上げない



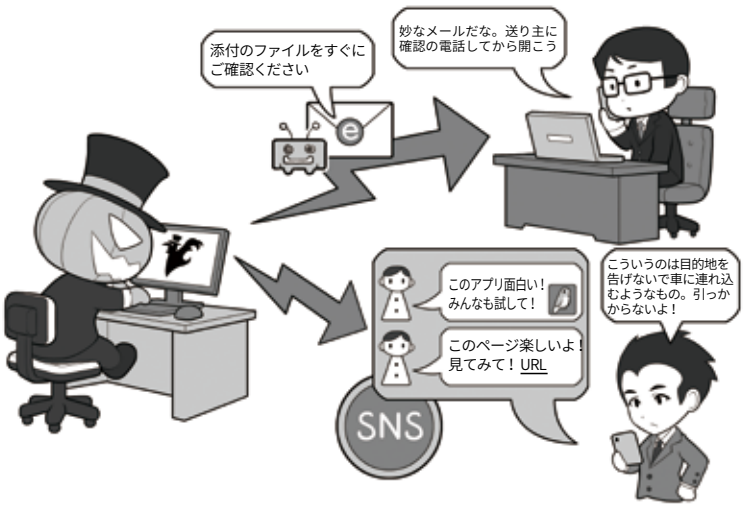
リアルで知り合いじゃない人とは友達にならない

未成年がSNSを利用する場合、写真や自分の個人情報を記載しないようにしましょう。また投稿内容も原則的に一般に公開せず、SNSで友達になった人のみが見られる設定にしましょう。

SNSで知らない人が友達になろうとリクエストを送ってきても、会ったことがない人はスルーするか基本的にお断りしましょう。

それは現実の世界で自分の個人情報を書いた名札をつけて歩いたり、名前もわからない初めて会った人に、ついていったりするのと同じぐらい、たいへん危ないことなのです。

攻撃者に操られて内側から鍵を開けてしまわないように心がまえを持とう



不審なメールに気をつけ、怪しいときは開かず送信者に確認する癖をつけましょう。ネットやSNSの引っかけは、セキュリティ関係のニュースをこまめに見ていると、次第に傾向がわかるようになります。訓練しましょう。

5 心の隙を作らないようにする（対ソーシャルエンジニアリング）

心の隙を突く攻撃、ソーシャルエンジニアリングには、「トラッシング（ゴミ箱あさり）」など相手に直接接触せずにやるものや、「ネームドロップ（権威があるように見せて聞き出す）」「ハリーアップ（急がせて聞き出す）」など、相手が正常に判断できない状況に追い込んで必要な情報を聞き出したり、相手に自分が求める行動を行わせたりするものがあります。

振り込め詐欺をはじめ詐欺全般には、こういった「人間の心の隙を突くソーシャルエンジニアリングの手法がよく用いられている」と言われています。

そしてデジタル世代のソーシャルエンジニアリングもまた人間の心の隙を突くものなのです。

たとえば相手に直接接触せず情報を入手するものとしては、電車で座席に座っている人のスマホ操作を見て「PINコード」やパターンロック形状を盗む「ショルダーハッキング」、カフェなどのテーブルに放置されているスマホの画面に残る指の脂跡からパターンロックを見破る方法などがあります。事前にロック解除の手段を特定してから機会を見てスマホを盗めば、個人情報が丸ごと手に入ります。

またメールで相手の心理的な隙を攻撃するのが「標的型メール」です。詐欺師が詐欺にかける相手をよく調べてから行動するように、標的型メールでは攻撃者が相手の名前、所属、身分、同じような会社でやりとりするメールのパターンなどを入手して、通常の仕事のメールと見分けがつかないほど精緻なものを送ってきます。その結果、会社のネットワークに侵入されたり経営層のふりをして送金を迫るビジネスメール詐欺が行われたりするのです。

精緻な「標的型メール」がライフルによる狙撃のように狙った獲物だけを撃つものだとすると、「スパムメール」は広範囲を攻撃する手法として今でもよく使われます。

スパムメールでの攻撃は引っかかる率が少なくとも、その攻撃の母数を大きく取ることで攻撃者にとっての利益回収のパフォーマンスを上げています。

たとえば「フィッシングメールの例」の画面は、実際にSMS(スマホのメッセージ)に送りつけられた、銀行を名乗るスパムメールでの詐欺メールを模したものです。

これにはフィッシング(=詐欺)メールを疑う手がかりがたくさんあります。まずメールが送りつけられても、口座を持っていない人はリンクを開かないでしょう。表示しているリンクもよく見ると、URLの末尾が日本を示すjpなどではなくgqになっています。しかしこういったものでも一定の割合で引っかかってしまう人がいます。もしその先に詐欺サイトではなく、ゼロデイ攻撃のマルウェアが埋め込まれたウェブサイトならば、それだけで感染してしまうわけです。

またもっとやっかいなのが、攻撃者ではなく、善意でマルウェアを拡散させてしまう人々です。「悪意はないが拡散してしまう例」の画面で、このSNSアカウントが友達のアカウントだった場合、きっと本当にこのアプリが面白いと思って薦めているかもと、あまり不審に思わないでしょう。

しかし本人は知らなくても実際はこのアプリがマルウェア入りだったり、あるいは拡散する間は無害でも、その後権限を拡大して個人情報を抜き取るかもしれません。

まだこれが知らない人の発信ならば警戒できますが、親しい友達や家族だった場合、同じように警戒するでしょうか？

対抗策としては、こういったお薦め系のものは一つの線引きを持って接するようにしましょう。メールの文面など目の前に見ている情報で完結しないものは一律に警戒するのです。動画が面白いとかお金が儲かる方法があるとかだけでなく、リンクでジャンプするとか、知らないアプリをインストールするものは一律に避ける。

それは現実世界で「ちょっと向こうまでつきあってよ」とか「ちょっとこの車乗ってよ」といって連れて行かれるのに等しいと思いましょう。

さらに、「リンクでジャンプしないけど検索エンジンで調べて見る分にはいいよね」、と思っても、攻撃者はそうやって検索エンジンからやってくる人向けに、2段構えでマルウェアを仕込んだウェブサイトを用意していることもある、と覚えておいてください。

標的型メールとフィッシングメールの例

標的型メールの例

フィッシングメールの例
(SMS・ショートメッセージを使った例)

悪意はないが拡散してしまう例

コラム：クリックしてはいけない！フィッシング攻撃の傾向

2018年にフィッシング詐欺の攻撃でもっとも目を引いたのは、宅配業者の不在通知詐欺です。宅配業者を名乗って「配達に行ったが不在だった。下記のリンクから確認して欲しい」というようなSMS（ショートメッセージサービス）を送りつけて、利用者をリンク先の偽サイトに誘導し、そこでID/パスワードなどを詐取するというものです。

実はこの業者は「SMSで不在通知を行うことはない」ということだったのですが、それを知らない人はまんまとだまされてしまったわけです。関係機関で日々「不審なメールに気をつけてください」というアナウンスをしているのですが、SMSとメールは違うものと思われてしまったのかもしれません。

その考え方から言えば、こういったメッセージを使った詐欺には、SMSやメールだけで無く、SNSのメッセージ機能、あるいはゲーム内のメッセージ機能を使った攻撃も考えられるので、同様に注意してください。

他にも地震が発生したときに、気象庁を名乗って津波に関する詐欺メールが送られた例もありました。いずれも私たちが「だまされないぞ」と身構えているのとは違う方向や、災害時で正常な判断が行えない状況を狙っています。

こういった詐欺メッセージは送信元アドレスを確認したり、メッセージ中のリンクのアドレスをよく見ることなどで詐欺を見抜くこともできますが、それらは偽装することも可能なので、確認するだけで安全とは言い切れません。基本は「見るだけで完結しない情報はすべて疑え」です。情報を確認する場合は正規のサイトを見るか正規のアプリから行いましょう。

また日々巧妙になる手口を少しでも知るにはフィッシング対策協議会（https://www.antiphishing.jp/）のWebページや内閣サイバーセキュリティセンターのTwitterをフォローするとよいでしょう。最新の事例をすぐに確認できます。

フィッシング詐欺はいろんな方法がある

SMS（ショートメッセージ）

電話番号宛てに送る

電子メール（eメール）

メールアドレス宛に送る

メッセージ（アプリなど）

アプリのアカウント宛に送る

ゲーム内のメッセージ機能

ゲームのユーザー宛に送る

「怪しいメール」と言われたら「メール」だけでなく似たような機能全般に気をつけましょう。

驚くと人間は警戒心を忘れる

災害時などに人間の警戒心が弱くなった瞬間を狙った攻撃もあります。注意しましょう。

コラム：映画「ザ・ハッカー」にみるソーシャルエンジニアリング

ケビン・ミトニック（左）

ケビン・ミトニックは車で走りながら電話一本で人をだまし、情報を手に入れる段取りをします。

シモムラ・ツトム（右）

シモムラは、当初、後手に回るが、そこから巻き返してミトニックを追い込んでいきます。

「ザ・ハッカー」は1999年に公開された、ハッカー対ハッカーの戦いを描いた実話ベースの映画です。

原作はその登場人物のうちの一人「シモムラ・ツトム」が共著した『Takedown』という小説です。

相手のハッカー「ケビン・ミトニック」にも『欺術（ぎじゅつ）』などの著書があります。

原作ではシモムラがホワイトハット的に、ミトニックがクラッカー的に描かれていますが、映画ではその勧善懲悪的な雰囲気よりも、ハッカーとハッカーの意地とテクニックのぶつかり合いに重点を置いて描かれています。

この映画の注目するべきポイントは「ハッカーの技術」とはなにかという部分であり、特に「凄腕ハッカーは目的のためならデジタルの世界に留まらない」ということに驚愕します。みなさんの中の「ハッカー像」が変わると思います。

ミトニックは劇中で「ソーシャルエンジニアリング」を駆使し、人をだまして情報を手に入れたり、コンピューターセンターに堂々と入り込んで暗号解析をしたりします。

私たちの日常で「要人のメールや個人情報が、電話が原因で盗まれた」といったニュースを目にすると、情報管理が緩いんだなと思ったりしますが、この映画を観れば、人間というものがどれぐらいあっけなくだまされ、どれぐらいあっけなく情報を流出するのかを実感することができます。

見たほとんどの人は「あんなことやられたら、ぜったいに逃げられない」と言います。

残念ながら現在日本では、この作品を販売している会社がありません。中古のDVDを手に入れるか、有料のネット配信サービスで見つけたらぜひご覧になってください。

心の隙への攻撃にポイントを置いたセキュリティの教材にもおすすめです。

ミトニックさんは現在ではホワイトハットとして社会に貢献されています。罪を償って守る側に回ったミトニックさんはかなりクールですよ。

コラム：スパムメールとその由来

スパムおにぎり、スパムの味噌汁、スパムのソテー、スパムのポークオムレツは単品で存在しますが、ホールスパムはないだろ！　ドヤッ！（ホールスパムは執筆担当の夢です）

かつて、メールソフトを開くと、うんざりするほど広告や勧誘、そしてフィッシングなどをする「スパムメール(spam mail)」が送信されてきていて、メールを見るのに滅入る（おっと失礼）時代がありました。

このうんざりする多量のメールを「スパム（spam）」と呼ぶ由来はなにか。諸説ありますが、有力なのはソーセージの中身を缶詰にしたスパム(SPAM)と、これをネタにした英国のコメディ集団「モンティパイソン」のコントでしょう。

実際のコントの内容は文字では表現できないナンセンス系なので、動画サイト検索で探し「考えるより感じろ」で味わってみて下さい。

そしてこのコントの劇中での「スパム推しのウザさ」が当時のスパムメールの「ウザさ」と繋がって、「spam mail」と呼ばれるに至ったのでしょう。

なおSPAMを生産しているホーメルフーズ社は商品を大文字、スパムメールを小文字と表記することで、迷惑メールがスパムメールと呼ばれることを容認しています。

さて、とはいえ日本人にこのうんざり感を説明するのは難しいので、某マンガをリスペクトしつつ日本風にアレンジしたイラストを描きました。「めいる百軒」と書かれた定食屋ののれんをくぐって「おやじ！おまかせ定食！」と注文したら、これが出てきたと思って下さい。滅入るでしょ。

ところでSPAMはすごくおいしいですよ！　姿煮以外は沖縄でお目にかかれます。たださすがの沖縄でも、この完全スパム定食には出くわしたことはありませんけど(^o^)

第2章

サイバー攻撃にあうと、どうなるの？最新の攻撃の手口を知ろう

サイバー攻撃にあうとどんなことが起こるのでしょう。
またサイバー攻撃ではあなたがいつも被害者とは限りません。ときには気づかず加害者になってしまうこともあります。
そうならないように、サイバー攻撃の類型を知ってこれに備えましょう。

1 攻撃者に乗っ取られるとこんなことが起こる

1 被害に遭わない、そして加害者にならないために

攻撃者があなたのパソコンなどにサイバー攻撃を仕掛けるのは、お金や情報を盗むだけでなく、あなたのパソコンなどをサイバー攻撃の道具にする目的もあります。

手順としては、あなたのパソコンなどをマルウェアに感染させるか、流出したID・パスワードを使いパソコンに侵入し、自由にコントロールできるようにします。

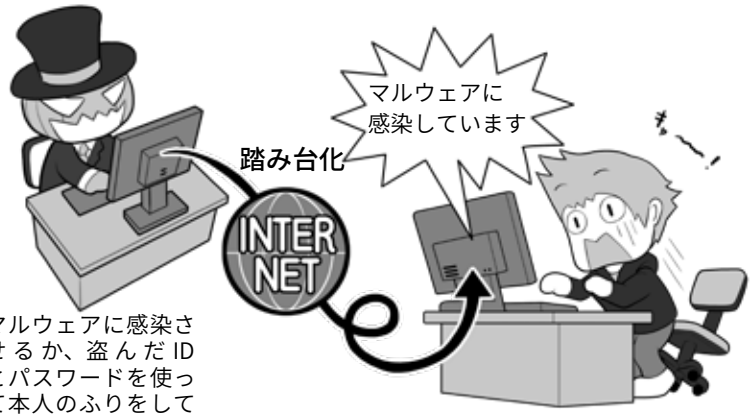
次に別のパソコンやサーバなどに侵入するとき、「踏み台」にしてあなたのパソコンがやっているように見せかけたり、悪意のボットによるボットネットに接続させ、DDoS攻撃を行わせたりします。

こうすることで、万が一サイバー攻撃がばれたとしても、最初にあなたが調べられ、その間に攻撃者は証拠隠滅などをして姿をくらますことができるわけです。

こういった場合でも、入念に調査すれば乗っ取られていた事実が分かるでしょうが、もし攻撃が重要な社会インフラに対して行われ、実際に被害が出てしまったら、あなたは思い悩んでしまうでしょう。

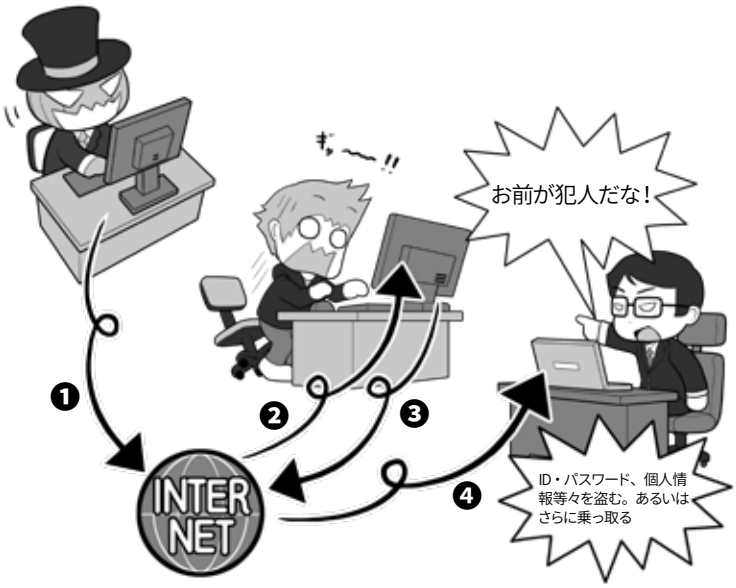
そうならないためにも、パソコンなどのシステムの状態は最新にし、セキュリティを固めましょう。もしセキュリティソフトが、悪意のボットに感染していることを検出したら速やかに駆除します。一方、実害の出ている攻撃に関して、警察などから協力の依頼があった場合は証拠保全を行いましょう。

攻撃者によるパソコンなどの乗っ取り



攻撃者はマルウェアに感染させパソコンなどを乗っ取るほかに、あなたのIDやパスワードがどこかから流出すると、それを利用して（あなたのふりをして）リモートサービスやパソコンにログインを試みて、これを乗っ取ります。マルウェアであればセキュリティソフトで検出されるかもしれませんが、なんらかの正規の方法でログインされ、「本人」としてリモートコントロール用のソフトをインストールされると、その乗っ取りに気づくのは難しくなります。

乗っ取ったパソコンを踏み台にしてサイバー攻撃を行う



攻撃者は、乗っ取ったパソコンなどに対して❶インターネットを通じて、❷乗っ取ったパソコンに指示を出し、❸あなたのパソコンがやっているように見せかけて（踏み台化）、❹他の人のパソコンに攻撃を仕掛けます。攻撃者はこうすることで自分の存在を隠して、安全にサイバー攻撃を行えるわけです。

また乗っ取りだけでなく、あなたのパソコンのメールソフトを使って、フィッシング詐欺のためのスパムメールなどを送信する場合などもあります。

2 盗まれた情報は犯罪に使われる

攻撃者は、あなたのパソコンなどを乗っ取って、個人情報、クレジットカード情報、ウェブサービスやSNSのID・パスワードなどを盗むと、それを犯罪に使います。

たとえば銀行のインターネットバンキングを使った不正送金で、口座からお金を勝手に盗み取るかもしれません。

銀行のインターネットバンキングは多要素認証でガードがされているから大丈夫と思っても抜け道はありますし、あなたの情報を売ってお金を得る手段もあります。

流出したクレジットカードを使いオンラインで勝手に買い物をして、それを受け取り現金化する、と言った事件も起きています。

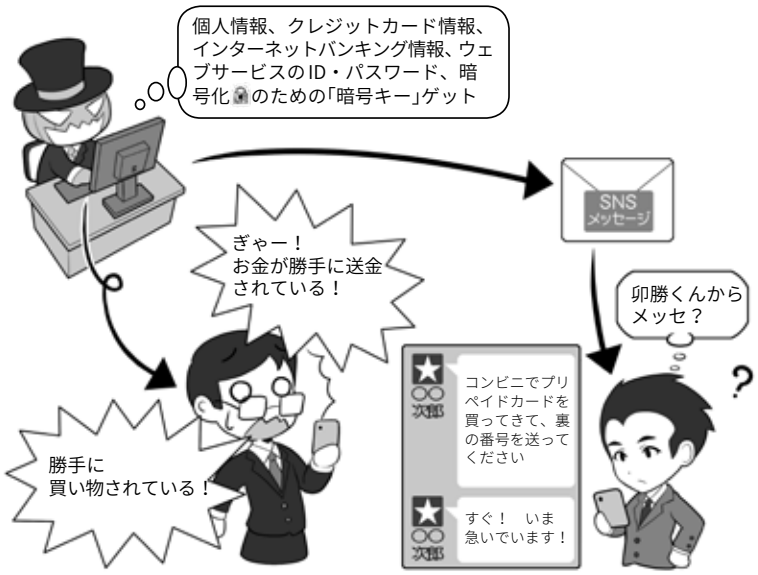
SNSのメッセージであなたになりすまし、友だちに対して「プリペイドカードを買って、アクティベーションコードを送ってくれ」と依頼し、電子マネーをだまし取る場合もあります。

自分が使っているパソコンなどのセキュリティをしっかり固めていても、情報を登録しているウェブサービスなどから、間接的に流出・盗難されることもあります。

この場合でも同じように、攻撃者は盗んだ情報から何らかの手段を用いて、お金を手に入れようとします。あなたに非がなくても流出は起こるのです。自分の環境のセキュリティを固めてもその時は防ぎようがないので、不正使用などの兆候に気をつけてください。

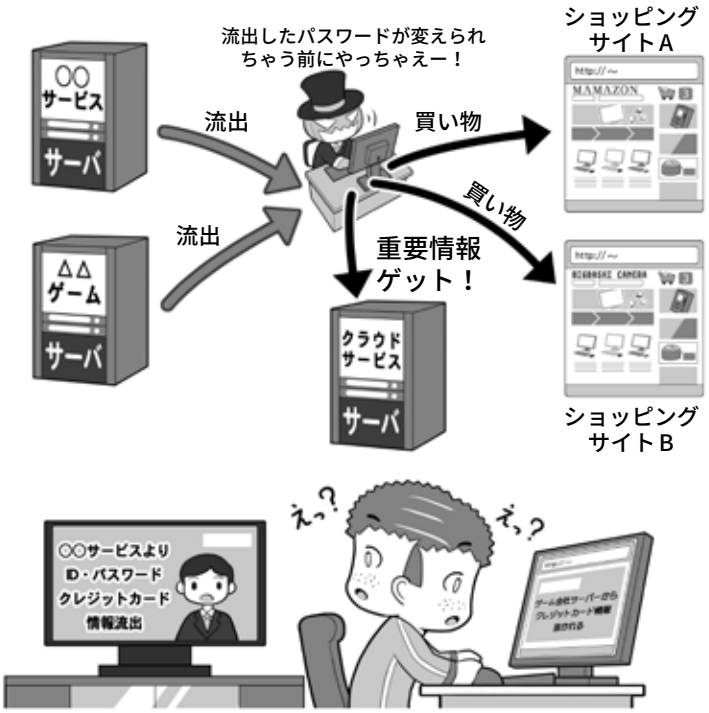
パスワード流出が判明したらパスワードのセオリーに従ってすぐに変更し、クレジットカード情報が流出したらカード会社に連絡してカード番号を変更しましょう。

情報が直接盗難される場合



クレジットカード情報の流出などが起こった場合は、その被害は多岐に及びます。とりあえずカードが不正利用されていないかチェックします。パスワードなどの流出は、各サービスのパスワードの変更を行いましょう。

情報が間接的に盗難される場合



特定のサービスからIDやパスワードが流出しただけならば、ID・パスワードの使い回しをしていない限り、他のサービスへの被害拡大はありませんが、使い回しをしている場合や、クレジットカード情報が漏れた場合、その被害は多岐にわたる可能性があります。楽観的に考えずに迅速に対処しましょう。

3 乗っ取られた機器はサイバー攻撃に使われる

サイバー攻撃で攻撃者に乗っ取られたパソコンなどの機器は、「ゾンビ化」と言い、攻撃者に操られる状態となって、様々なサイバー攻撃に使われることがあります。

サイバー攻撃の「踏み台」に使われるほか、「悪意のボット」に感染した機器は、持ち主の知らないところでボットネットというゾンビ化した機器の集合体に加えられ、攻撃者の命令で特定のサーバに一斉にアクセス要求をするDDoS攻撃などに使われます。

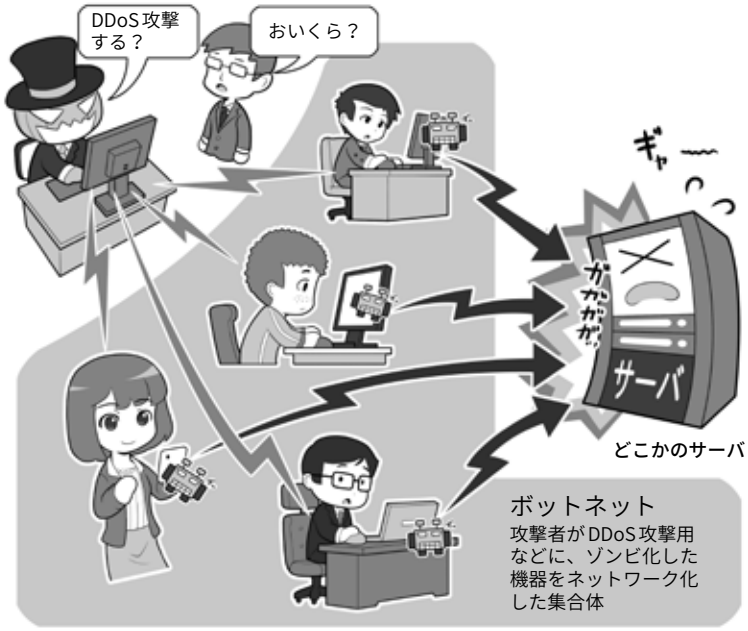
このボットネットによる攻撃は、攻撃者が自分の技術や主張を誇示する行動などにも使われますが、ボットネットを利用して攻撃を行いたい人物に、時間あたりいくらで貸し出されたりもします。攻撃者は乗っ取った人の財産(パソコンなど)を勝手に貸し出し、違法にお金を稼いでいるわけです。

一方、「踏み台」的な攻撃はパソコンなどの乗っ取りによるものだけではありません。

「ウォードライビング」といって、車に乗って、会社や家に設置されている、暗号化されていない、もしくは暗号化や暗号キーの設定の甘い無線LANアクセスポイントを探し、見つけるとこれに侵入する手法があります。

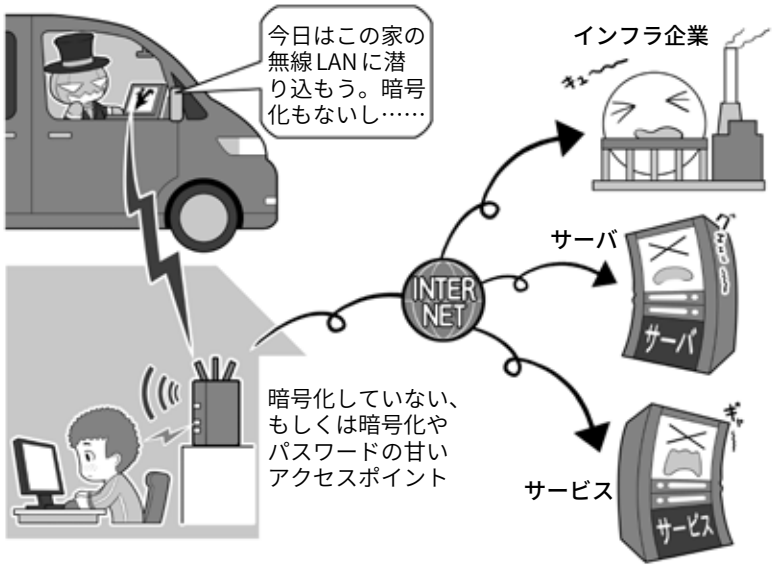
これはアクセスポイントを「踏み台」にし、そこからインターネット上の様々なサーバやインフラ企業に攻撃を仕掛けるためです。攻撃を仕掛けてきているのは「踏み台」がある場所と見せかけて身代わりにし、攻撃がばれたときの追跡を逃れる方法です。

乗っ取られたマシンはボットネットとして貸し出される



攻撃者によって悪意のボットに感染させられ、コントロールされたパソコン(ゾンビPC)などの集合体がボットネットです。攻撃者の命令で、一斉に特定のサーバなどにDDoS攻撃を仕掛け、ダウンさせたり反応不能に陥れたりします。闇サイトで時間あたりいくらという形で貸し出されることもあります。

無線LANに侵入され罪を押しつけられることも



車で街を徘徊して、侵入可能な無線LANアクセスポイントを探すことを「ウォードライビング」といいます。こういった侵入を許し「踏み台」にされないためには、無線LANアクセスポイントのセキュリティ設定をきちんと見直しましょう。それが、自分の身の回りでできるサイバー攻撃阻止の第一歩です。

この場合攻撃者に罪があるのが当然ですが、自分の家からサイバー攻撃が行われ、インフラ企業などで事故が発生したら穏やかではありません。セキュリティを固めて侵入されないようにしましょう。

4 IoTも乗っ取られる。知らずにマルウェアの拡散も…

攻撃者によって乗っ取られるのはパソコンやスマホだけではありません。IoTと呼ばれるネットにつながる電子機器はいずれも、乗っ取られて攻撃の身代わりとなる「踏み台」、DDoS攻撃のボットネットへの接続、マルウェアの拡散など、様々なサイバー攻撃に利用される可能性があります。

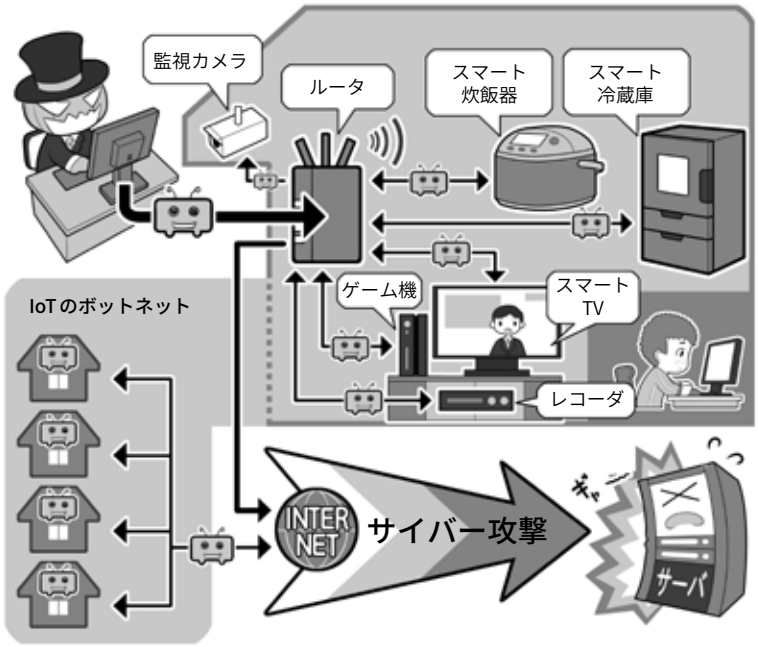
特にIoT機器は監視カメラやスマート家電などのように、普段私たちがあまりセキュリティについて気をつけることがない機器であり、パソコンほどサイバー攻撃への対応能力が高くありません。そして一つの機種で台数が多い＝手間をかけずに多数を攻撃できる。攻撃者にとって「攻撃しやすい条件」が揃っているのです。

最低でも出荷時の「ログインパスワード」はセオリーに従って変更し、システムは最新に保ち、ネットにつなぐ必要がないものはむやみに接続しないようにしましょう。

またサイバー攻撃に協力してしまうのはなにもパソコンやIoT機器だけとは限りません。人間は最大のセキュリティホールとも言われ、マルウェアの拡散元となることもあります。SNSなどで「このサイトが面白いよ」「このアプリ試してみて」といった投稿を考えなしに拡散していると、その先はフィッシングサイトだったり、マルウェアアプリだったりします。

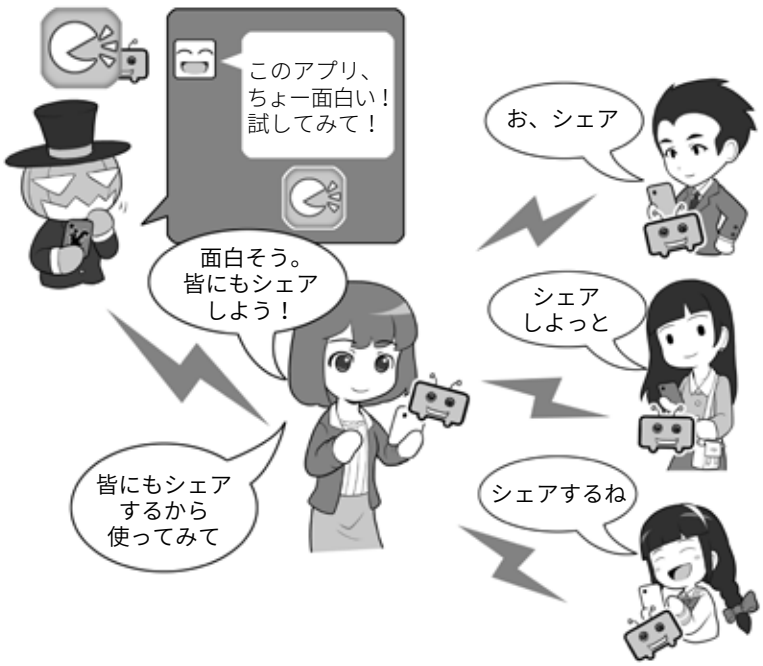
ネットでなにか行動する前には、必ず「それは本当に必要なのか」「そうすることでなにか問題が発生する可能性はないのか」をいつも注意しましょう。

IoT機器も乗っ取られ攻撃に使われる



IoT機器は攻撃者から見ると、乗っ取りやすい要素を多くもっています。攻撃者はそれらを乗っ取って様々なサイバー攻撃に使います。IoT機器は最低でも「初期パスワードの変更」「システムの状態を最新にする」「必要のない機器はネットにつながない」などの対応をしましょう。

知らずにマルウェアの拡散に協力しているかも……



SNSで見た「面白い投稿」や「拡散希望の投稿」を深く考えないで拡散すると、その投稿にあるURLの先にはフィッシングサイト用意されていたり、ゼロデイ攻撃のマルウェアが仕込まれていたり、アプリであればマルウェアが入ったものだったりするかもしれません。拡散する前によく考えて「シェアする必要がないものはシェアをしない」ようにしましょう。そうしないと、あなたが被害者ではなく、サイバー攻撃やマルウェアの拡散者になってしまうかも。

コラム：大きな脅威となっているランサムウェア

パソコンなどのデータを暗号化し使えないようにして、身代金を要求するランサムウェア。その大規模な感染に注目が集まっています。

企業のパソコンやサーバがランサムウェアに感染し、ビジネスに大きな支障が生じている事件が多発しています。

たとえば2017年5月には、「WannaCry」と呼ばれるランサムウェアを使った大規模なサイバー攻撃が実施され、百数十カ国の20万台以上のコンピュータが感染したと言われています。

特にイギリスでは国民に保険サービスを提供するいくつかの団体で端末が利用できなくなり、医療機関において診療ができなくなったり、予定されていた手術が行えなくなったりした事例もありました。

また、ある大手自動車メーカーでは工場内の端末がWannaCryの亜種に感染し、生産が一時止まるといった影響が出ていました。

こういったランサムウェアでは身代金を支払ってもデータの暗号化を解除できないことも多発しています。ランサムウェアのふりをしてデータを破壊することが目的と思われるものもあります。

また最近では、個人のスマートフォンを狙ったランサムウェアも登場しています。最悪の場合は端末を初期化しなければならず、大切なデータが失われることにもなりかねません。

こういった事態を避けるため、システムやアプリは最新の状態を保ち、不審なメールのリンクをクリックしたり、あやしいWebサイトからソフトやアプリをインストールしたりしないこと。データを常にバックアップし、必要に応じてセキュリティソフトを利用するといった対策をしっかり実施しましょう。

ランサムウェア感染はビジネスにも影響

ランサムウェアはパソコン内のファイルを勝手に暗号化するため、感染すれば仕事などをする上で極めて重要なファイルも人質に取られてしまいます。バックアップは常にしておきましょう。

不審なアプリのインストール要求に注意

公式ストアでもマルウェアは発見されていますが、もっとも注意すべきはそれ以外の場所からのインストールです。こういったアプリは不審なメールのリンクや、SNSのお薦めなどでも回ってきます。大きなダメージを被る可能性もありますので、十分に注意しましょう。少なくともアプリのインストールは公式ストアからのみにしましょう！

コラム：仮想通貨の現在地1

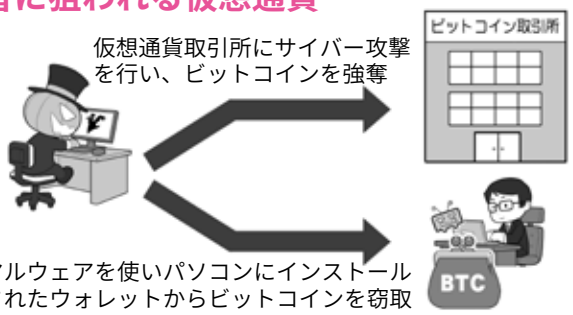
ビットコインなどの仮想通貨が広く流通しつつあります。最近ではビットコインによる現実世界での決済にも使われ始めています。

しかし注意しておきたいのは、こうした仮想通貨の多くは国家の通貨と異なり価値の裏付けを行う者がおらず、最悪の場合突然価値が0になり得るおそれがあります。

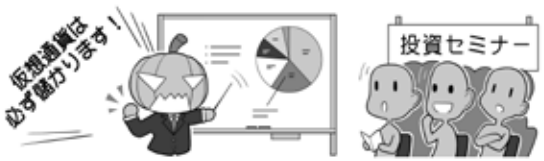
実際、仮想通貨は現実通貨に対する価値が乱高下することがあり、通常の投資対象とするにはリスクが大きいようです。そして、まるで西部劇のようにサイバー攻撃により、仮想通貨を預かる取引所からの大規模な盗難や、個人のお財布(ウォレットという)から仮想通貨が盗まれるケースも伝えられています。

また「仮想通貨は必ず儲かる」といった、投資詐欺も登場しており、その特性や取り巻く環境を理解せずに手を出すことは、非常に危険性が高いと理解しましょう。

犯罪者に狙われる仮想通貨



仮想通貨を巡るサイバー攻撃も続発しています。実際、大手ビットコインの取引所がサイバー攻撃を受け、大きな金銭的被害が生じた事例があるほか、ビットコインの窃取を目的としたマルウェアも登場しています。



仮想通貨をネタにした投資詐欺が増えています。どのようなものであっても「必ず儲かる」という話はありえませんので、くれぐれもご注意を。

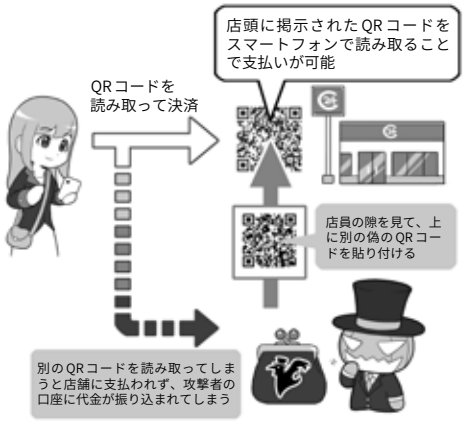
コラム：QRコード決済サービスで生まれた新たな詐欺

ITを活用して金融サービスを実現する、FinTechと呼ばれる取り組みが世界的に広まっています。具体的なFinTechサービスとしては、収入と支出、現預金などをスマートフォンのアプリを使ってすばやく把握できるサービスや、スマートフォンで手軽に送金できるサービスなどがその代表例として挙げられます。

そうしたサービスの1つとして広まる兆しを見せているのが、QRコードを使った決済サービスです。店舗などで商品を購入する際、掲示されたQRコードをスマートフォンで読み取ると代金を支払うことができるというサービスであり、中国などで先行して広く利用されています。

便利なサービスですが、QRコードを別のものに張り替え、代金を横取りする詐欺も発生しています。日本でもQRコードを使った決済サービスは始まっていますが、こうした詐欺行為に巻き込まれる可能性もあるので注意が必要です。

QRコード決済の詐欺の流れ



まず犯罪者が店舗に掲示されたQRコードの上に、別のQRコードを貼り付けます。利用者がそのQRコードを使って決済を行うと、代金は店主ではなく犯罪者の口座に振り込まれてしまうという流れです。

コラム：仮想通貨の現在地2

「仮想通貨の現在地1」の他にも、今年は仮想通貨にまつわる大小さまざまなトラブルが度々発生し、世間を騒がせました。

一つは、ランサムウェアなどでパソコン・スマホのデータを暗号化した上でロックして、そのロックを解いて欲しければ身代金を払えと脅し、支払いをBitcoinなどの仮想通貨で要求するものです。

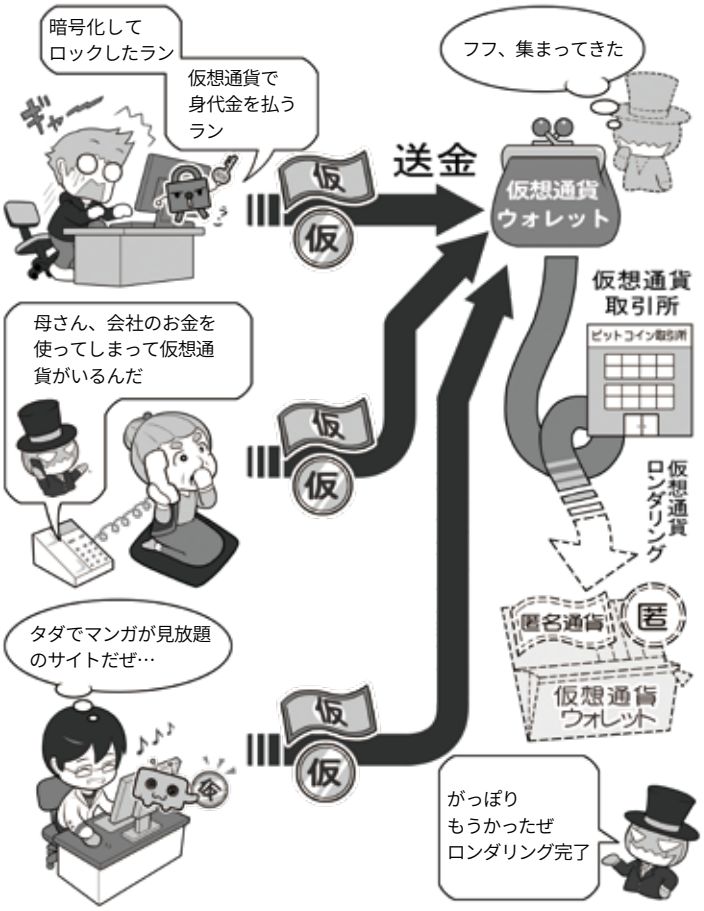
仮想通貨で要求する理由は、仮想通貨が全般的に「匿名性」が高く、不正に入手したり奪取したりしても、その後の追跡が困難だからです。また一般的に知られているBitcoinなどの仮想通貨で要求されても、支払先をばらばらに拡散して追跡し難くし、さらにその上で極めて匿名性の高い仮想通貨に換金(ロンダリング)して、追跡を逃れるなどの手法もあります。

こういった手法は詐欺などで利用されるケースもあるので、「仮想通貨での支払い」ときたら、まず警戒する方が良いでしょう。

仮想通貨を入手するには売買するほかに、自分のパソコンなどで複雑な演算を解いて、その報酬として入手する方法もあります。これを、パソコンなどの保有者に断り無く、勝手に行っているものもあります。不正にマンガなどを閲覧できるサイトに行くと、その裏で勝手に仮想通貨を得る協力をさせられた例がありました。そもそもそういったサイトを見るべきではありませんが、それと同時に、特定のサイトを開いたら突然パソコンの動作が遅くなった、といった場合には注意が必要です。

仮想通貨は最近、全世界における演算による電気消費が中堅国1国分よりも多くなり、規制も厳しくなりつつあることで価値の下落が進んでいます。1項にあった、「必ず儲かる」といった話に引っかからないのと同様に、仮想通貨関連で騙されないように、上記の項目にも注意してください。

著名な仮想通貨を匿名性の高い通貨にロンダリングして逃げる



仮想通貨はもともと匿名性が高いのですが、それをさらに匿名性が高い仮想通貨にロンダリングすることで、追跡を困難にして逃げます。

コラム：フェイクニュースとサイバープロパガンダ

デマと似たようなものとして「フェイクニュース」という言葉が注目されつつあります。

悪意を持った者が何らかの意図を持って、ネット上で偽のニュースを発信するもので、これが拡散され始めるとニュースサイトなどでも真贋不明のまま取り上げられ拡散され、結果的に見た人はそれを真実だと思ってしまうといったことが起きています。

フェイクニュースには意図を持って発信している人の他に、人々が注目するニュースをねつ造することで自分のサイトの閲覧数を増やし、掲載した広告の収入でお金を稼ぐ商売としている人もいて、1つの悪意のビジネスモデルになりつつあります。

検索エンジン企業やSNS企業などはこういった情報がニュースのランキングに登場しないように工夫をしたり、善意の団体と協力して偽の情報の場合は否定するなど処置を行ったりしていますが、いまだ根本的な解決には至っていません。

またこういったフェイクニュースを外国の国家機関が「武器」として使い、他国の選挙における投票行動などに意図的に影響を及ぼす「サイバープロパガンダ」も多く発生しています。

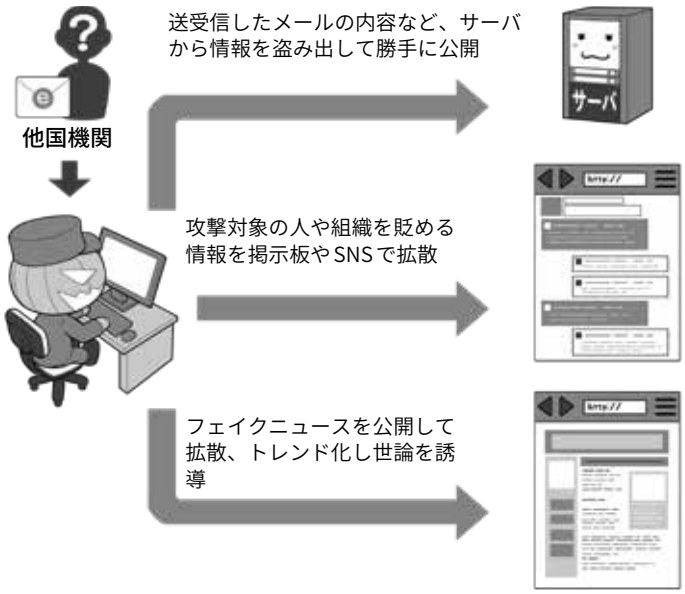
プロパガンダ自体は、古くから国家が自国や他国に対して影響を及ぼすために行われてきた「人を思い通りに動かそうとする情報の悪用法」ですが、これがネットを使うことで高度化かつ目立ちにくくなり、人々が気付かないまま、その考え方が操作される事態が起きているのです。

これを成立させるために、サイバー攻撃によって盗んだ政治家のメールを改ざんした上での暴露、国と密接な関係にあるメディアでの偽ニュースの発信、ボットを使ったSNSでの偽ニュースのトレンド化、政治的な争点になっている事柄の賛否両方にSNS上で広告を打つことで混乱を生み出し国民を分断、そしてSNS上で架空の人格のアカウントを作りインフルエンサーに成長させ、他国の人々を自国に有利になるように扇動するなどといった、様々な手法を総動員してサイバー攻撃が行われているのです。

私たちが希望を持つインターネットには、一方でそういった悪意をもった人々が暗躍しているということを理解し、手元に来た情報をそのまま鵜呑みせず、また短絡的にシェアなどの共有をせず、一呼吸置いてその真贋を見極めたり、本当にシェアなどの拡散をするべきか冷静に判断したりすることが求められています。

何故ならサイバープロパガンダには、私たちが「深く考えず情報を拡散する習性」までもが組み込まれているからです。悪意のある人の駒にならないように気を付けましょう。

サイバープロパガンダが行われた例（米国）



サイバープロパガンダでは、フェイクニュースや盗んだ情報のリークを種として、トロールと呼ばれる情報操作グループと「いいね」や「シェア」を押す自動のボットによりこれをトレンドにのせ、さらにターゲットの国の「自分にマッチした情報を好んでシェアする」人たちのSNS集団（エコーチャンバー）にこれを投げ込み、最終的にその他大勢に、さも「重要なニュースである」というイメージを与え、世論を操作します。

コラム：軍事スパイ、産業スパイに狙われてしまったら

スパイではない攻撃者は、コストパフォーマンスでターゲットを選ぶ傾向がありますが、では逆にスパイはどのように行動するのでしょう。

軍事スパイや産業スパイの場合、入手するべき情報は絶対であり、侵入しにくいからといって別の情報にすることや諦めることはできません。

またこういった攻撃者の場合、活動するための資金は自分でまかなわなくても、国家だったり軍だったり、あるいは産業スパイでも独立して活動して情報を売る者でなく、スポンサーの企業から活動資金を得ている者なら、コストパフォーマンス度外視で攻撃を仕掛けられるわけです。

興味がある方は一般のスパイの教本をお読みになると、目的のためにはどれぐらい容赦ないことをするのか理解できるでしょうし、それが理解できれば、あとはネットの世界のサイバー攻撃に置き換えればいいわけです。

なおネットが全盛になる前のスパイ活動は、相手国の新聞や雑誌など公開されている情報から情報収集するオシント、人間関係を調べたり尾行したり、交友関係を持って情報を聞き出すヒューミント、そして通信を傍受や盗聴して情報を入手するシギントがありました。

ネット社会の現代では、SNSを見ればある程度ヒューミント的な情報は入手できますし交友関係も丸わかりです。またシギントもマルウェアに感染させてメールを盗み見たりファイルを奪取したり、スマホの通話を盗聴できたりもします。

少なくとも相手がSNS好きの人間なら一般人でも楽にヒューミントもオシントもでき、これがサイバー時代のインテリジェンスと言ったところでしょうか。

要職にある方々は、SNSなどに不必要に情報を流さないようにしましょう。あなたの行動のすみずみまで、その情報は誰かに見られていますよ。

第３章

パスワード・Wi-Fi・ウェブ・メールのセキュリティを理解して、インターネットを安全に使おう

私たちの安全なインターネット生活を支えるパスワード、Wi-Fi(無線LAN)・ウェブ・メールの暗号化などのセキュリティについて、理解を深めましょう。
初心者向けとしてはやや難しい項目ですが、なるべく流れを持って平易な言葉で解説していきますので、ぜひ読んでセキュリティへの理解を深めてください。

1 パスワードを守る、パスワードで守る

1 パスワードってなに？

私たちがスマホやパソコンなどのIT機器や、各種のウェブサービスを使う上で、欠かせないのが「パスワード」です。

機器やサービスを利用するときに、正式な利用者や持ち主である自分だけが利用でき、他人が利用できないようにするための鍵の役割を果たすものです。

パスワードはいわば「家の鍵」や「金庫の鍵」。これを適切に守らなければ、家や車、金庫を勝手に開けられてしまうように、パソコンやスマホ、ウェブサービス上にある私たちの個人情報やメール、銀行口座が攻撃者に不正にアクセスされ、情報が流出したり、お金を盗まれたりしてしまいます。

なおこういった役割を担うものには、他に「暗証番号」などや、通信している情報やパソコン・スマホの中のデータを暗号化して、他人や攻撃者が読めないようにする、「暗号化と復号の鍵＝暗号キー」というものもあります。

この3つは性格や役割が異なるのですが、よくまとめて「パスワード」と記述されることがあるのと、暗証番号、パスワードと暗号キーは、等しく攻撃の対象になるために、ここでは一括して扱います。

2 3種類の「パスワード」を理解する

私たちは機器やサービスを利用する時、あるいはファイルを開く時に入力するものを、まとめてパスワードと呼び、同じような役割をするものと思いがちです。しかし、セキュリティ上の性質から、「パスワード」とまとめて呼ばれるものは、大きく3つに分けて理解する必要があります。

1. **銀行のキャッシュカードやクレジットカードの利用時や、スマホのロック解除時に使用し、通常4桁や6桁ぐらいの数字だけで構成されることが多いもの（暗証番号やPIN、PINコード、パスコード。通信事業者のネットワーク暗証番号などを含む）**
2. **パソコンやデジタル機器、ウェブサービスなどの利用時にIDとセットで入力し、英大文字小文字＋数字＋記号混じりで10桁以上など、複雑さと一定以上の長さが推奨されるもの（狭い意味でのパスワード、ログインパスワード）**
3. **パスワードと呼ばれていることもあるけれど、本当はファイルや通信内容を暗号化するための暗号鍵として使われているもの（ZIPファイルのパスワード、WordやExcel、PowerPointの保護パスワード、Wi-Fi機器の暗号化キー、暗号キー、パスフレーズ、セキュリティキー、ネットワークキー）**

一口にパスワードと言っても上記の通り、実に様々なものがあります。28ページでご紹介したのは、上記のうちの2にあたります。

この本では以降、この3つを混同しないように、

1を「PINコード」
2を「ログインパスワード」
3を「暗号キー」

と呼びます。

3 「PINコード」と「ログインパスワード」に求められる複雑さの違い

28ページでは機器やサービスを利用するとき、「ログインパスワード」として、英大文字小文字＋数字＋記号混じりで少なくとも10桁以上を推奨しました。

一方、同様に使う「PINコード」は、メーカーが数字のみの4桁かや6桁で良いとしています。

この2つは両方とも機器やサービスを利用する時に使用するのに、求められる長さや複雑さに差があるのはなぜでしょうか。

そもそもパスワードに「複雑さ」が求められる理由は、攻撃者が制限のない状態でパスワードの文字列を総当たりで試すと、時間はかかるが「いつか必ず探り当てることが可能」だからです。これはどんな複雑な「ログインパスワード」や「暗号キー」でも変わりません。

こうやって力業（ちからわざ）でパスワードを探り当てる攻撃を「総当たり攻撃（ブルートフォース攻撃）」と呼びます。「ログインパスワード」や「暗号キー」を守る第一歩は、いかにこれを成功させないかにあります。

スマホの「PIN コード」の場合は、数回間違うと「入力遅延」と言って一定時間「PIN コード」を入力できないようなり、さらに「10 回間違えば以降 PIN コード入力不可にする（ロック）」「場合によっては機器を初期化する（ワイプ）」ことで「総当たり攻撃」を不可能にし、攻撃者による不正利用を防ぎます。

さらに厳しいキャッシュカードなどでは3回間違うと、以降カードが利用できなくなりますが、これも同じ考え方です。

「PIN コード」では、こういった厳しい制限を設けることで「総当たり攻撃」を不可能にし、4桁から6桁の数字であっても攻撃者から機器やサービスを守れるのです。

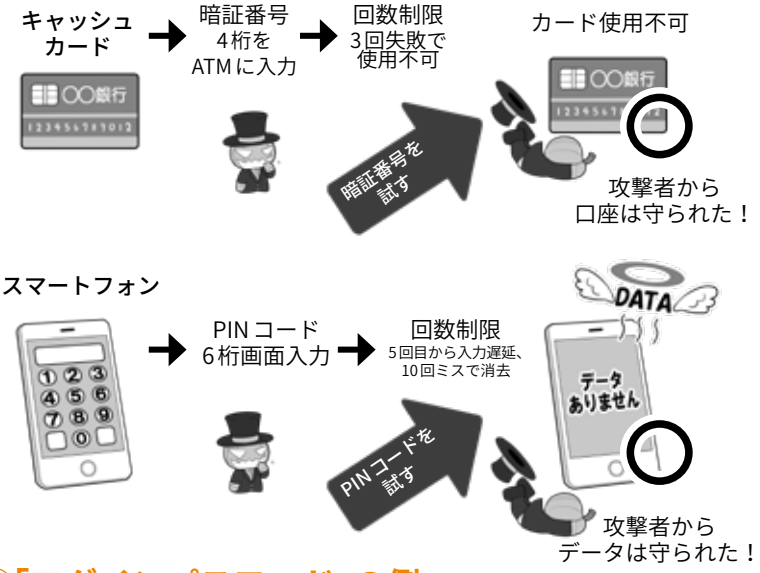
一方「ログインパスワード」は、通常「PIN コード」のようにワイプまでする機能がついていることはほぼありません。数回失敗すると入力間隔が開く、一定時間入力ロックを起こすなどのペナルティを受ける場合もありますが、ペナルティがないものも多いのです。

この「ログインパスワード」は、ウェブサービスのログインページや、パソコンや IoT 機器のログイン画面に入力するもので、こういった入力画面ではネット経由でログインを試みる場合、どう頑張っても 1 秒に数回～数十回程度しか入力することが出来ず、これだけで実質的に高速な攻撃を防ぎます。

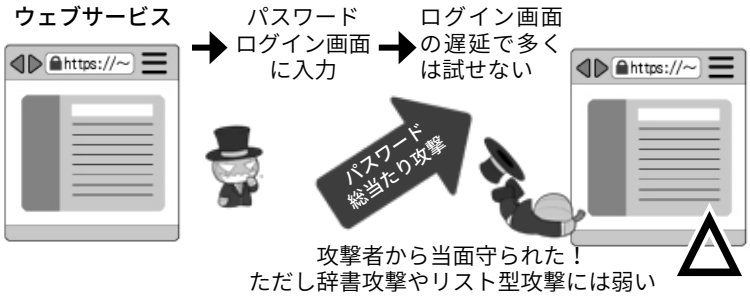
本書の推奨通り英大文字小文字＋数字＋記号 26 種＝88 種類の文字を使い、10 桁のパスワードを作ったとすると、その組み合わせは約 2785 京個（京は兆の上の単位）、1 秒 5 回の制限で「総当たり攻撃」をした場合、全部を試すまでに約 1760 億年かかるわけです。

3 種のパスワードを理解する

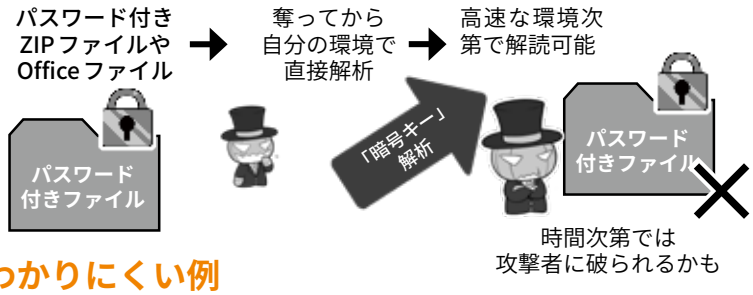
①「PIN コード」の例



②「ログインパスワード」の例



③「暗号キー」の例

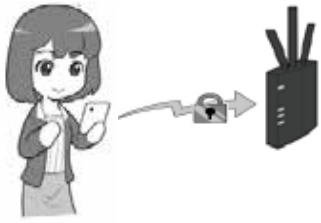


わかりにくい例

「ログインパスワード」か「暗号キー」か分からない例

ハードディスク暗号化の救済に関して、パスワードなのか「暗号キー」なのか分からないものを求められる。そういった場合は「暗号キー」と考える。

無線 LAN アクセス時にパスワードのように入力する文字列



ルータにログインするように見えるが、ログインパスワードでは無い。「暗号キー」を自分の機器に設定してるだけなので、「暗号キー」の基準で設定する。

※この図は一例であり、実際の機器の条件とは異なります。

これならば、100年以内に当てられる確率は非常に小さく、事実上不可能と言えるわけです。

このような攻撃の想定をセキュリティ用語的には「オンラインアタック(攻撃)」と言いますが、ここでは「『ログインパスワード』への攻撃」と呼ぶことにします。

4 「暗号キー」に求められる複雑さ

上記の「ログイン画面」に入力するパスワードとは異なり、「暗号キー」の場合は、攻撃者が暗号化されたデータを盗んで持ち帰り、ログイン作業による遅延などなく、自分のペースで暗号化解除(解読)の攻撃をすることができます。

この攻撃の対象となるのは、「複数のファイルをまとめたパスワード付きZIPファイル」、「パスワードを設定したMicrosoft Officeのファイル」、「暗号化されたUSBメモリ」や「パソコンから取り出された内蔵ディスク」、あるいは暗号化された無線LAN通信などです。

こういったものでは、「パスワード」と思って設定しているものが、実はパスワードではなく、中身を読まれないようにするための暗号化に使われる鍵=「暗号キー」となっている場合が多いのです。

ZIPやMicrosoft Officeのファイルは、パスワードが設定されていると、開く時にパスワード入力画面が出るので、パスワードの総当たり攻撃に対し入力遅延の防御があるように見えますが、実はその画面はZIPやOfficeのプログラムが提供しているもので、ファイルそのものは単なる暗号化されたデータにすぎないのです。

そのため、パスワード入力画面を使わなくても直接ファイルに対して暗号解除の攻撃が可能であり、遅延による防御はありません。

このような暗号化解除は、「暗号キー」が短いと、スーパーコンピュータを使うまでもなく、普通に市販されているゲーム用パソコンの性能で十分可能です。そういったパソコンのグラフィックボードに搭載されているGPUというプロセッサーを駆使すれば、ZIPファイルに対して40億回/秒の暗号化解除の攻撃が可能というデータすらあります。

この場合、先ほどの約2785京個の組み合わせがある場合でも、解読までにかかる期間は78.5万年に短縮、8桁のものになると103年、8桁で記号抜きの62種の文字だと6年、英大文字小文字だけだと2年となり、GPUの性能が向上すればそのうち、数日単位で可能になるでしょう。それはもう「解読可能な領域」と言えます。

そのため本書では、「暗号キー」には、完全にランダムで英大文字小文字＋数字＋記号混じりで15桁以上のものを推奨し、これを基準とします。

ZIPのパスワードに15桁ものランダムな文字列を使うのは、覚えられなくて無理だと思われるでしょうが、8桁程度のパスワードでは破られてしまうので、暗号化したつもりでも攻撃者の前では無力なのです。

なお、このような想定の攻撃をセキュリティ用語的には「オフラインアタック(攻撃)」と呼びますが、ここでは「『暗号キー』への攻撃」と呼ぶことにします。

5 どちらの「パスワード」か、わかりにくい例

以上のように3つカテゴリに分類しましたが、どれに当てはまるかわかりにくい場合もあります。その例を2つ紹介します。

まずは、パソコンの内蔵ディスクの暗号化に関するパスワードのようなものです。

パソコンで内蔵ディスクを暗号化する場合、「暗号キー」が必要になるはずです。

しかし最近の高度なセキュリティシステムの場合、内蔵ディスクの暗号化は自動的に行われ、「暗号キー」もきわめて複雑なものが自動で生成され内部で秘匿されます。そして、起動時に「暗号キー」を開放して内蔵ディスクを利用できるようにするために、「PINコード」や「ログインパスワード」が利用されます。いわば鍵のための鍵のイメージです。

ただし、なんらかの理由で正規の利用手順が使えなかったときに備え、救済用に「復旧キー」や「マスターパスワード」といった、様々な「パスワードのようなもの」を設定する場合もありえます。

これらの「パスワード」のようなものは、「どれがどの分類か」きっちり説明するのは大変手間がかかります。むしろ個別に説明すると、利用者は即座に判断出来ず混乱するかもしれません。

従って以下のようにシンプルに考えましょう。内蔵ディスクの暗号化に関して、「パスワードのようなもの」を求められたら、全て「暗号キー」の基準で、使い回しをしていないものを設定するのです。

もう一つは、無線LANアクセス

ルータに接続するための、「ログインパスワード」のように見える「暗号キー」です。これは、実は機器に接続するためのパスワードではなく、通信するデータの暗号化と復号に必要な「暗号キー」を機器に設定しているのです。

無線LAN通信はネットに接続しているので「オンライン」に思えますが、攻撃者は電波を盗聴して送信内容を持ち帰り、内容を解読することが出来るので、「オンライン攻撃」ではなく「オフライン攻撃」のカテゴリに入ります。従って、「暗号キー」の基準により、これを設定する必要があるわけです。

6 総当たり攻撃以外のパスワードを破る攻撃や生体認証を使った防御

パスワードなどを破る攻撃には「総当たり攻撃」の他にも様々な手法があります。

パスワードでよく使われる言葉などを集めた専用の辞書を利用する「辞書攻撃(ディクショナリアタック)」、ウェブサービスなどから流出した名簿やID・パスワードのリストを入力して試す「リスト型攻撃(アカウントリスト攻撃・パスワードリスト攻撃)」など。

これらに対する防御のためにも、「ログインパスワード」には意味のある単語や、自分に関連の深い語句を使わず、推奨する基準に従い、充分に複雑で、かつ他の機器やサービスで使い回していないものを設定しましょう。

「PINコード」は、入力を間違え続けると「入力遅延」や「ロック」機能があるため、「総当たり攻撃」などの手法が有効ではありません。

パスワードを破る手段は色々

総当たり攻撃(ブルートフォース攻撃)

すべての文字列の組み合わせを試す

辞書攻撃(ディクショナリアタック)

パスワードでよく使われる単語を使って試す

リスト型攻撃
(アカウントリスト/パスワードリスト攻撃)

名前やIDパスワードの流出リストを使う

あくまでも代表的なものの例ですが、簡単なパスワードだったり、使い回しをしていたり、流出したのに放置していると、攻撃者に楽々突破されます。パスワードはしっかり管理しましょう。
(本当は人力でなくプログラムなどで自動的に行われます)

多要素認証の構成要素は?

①知っているもの　②持っているもの　③本人自身に関するもの

多要素認証の組み合わせ例

銀行のキャッシュカードの例

①の暗証番号 ＋ ②のキャッシュカード

スマホからウェブサービスへログインする例

②のスマホの固有情報 ＋ ③の指紋情報

指紋認証が破られることも…

高度なハッキングをしなくても、酔っ払って寝ているあなたの指に押し当てるだけで指紋認証は突破できてしまいます。
指紋認証だから絶対安心と過信しないようにしましょう。
場合によっては機器を再起動したり、わざと数回指紋認証を失敗して、強制的にPINコード入力が必要な状態にしましょう。

しかし、「PIN コード」の強さは「盗み見られたり、推測されたりしないこと」が前提ですので、入力するときは周りに気を配り、また、自分の個人情報など推測しやすいものを使わないようにしましょう。

現にATMでお金を下ろすときに、「暗証番号（PIN コード）」を肩越しに覗き盗み取る手口は、「ショルダーハッキング」としてよく知られています。

「PIN コード」の盗み見などを防ぐためには、指紋認証や顔認証などの「生体認証」を利用するのも一つのアイデアです。それらであれば肩越しに見ても、まねをすることはできないからです。

ただ、指紋認証などの生体認証も100%安全とは言い切れません。どこかで撮影した相手の指の写真から、3D プリンターで偽の指紋を作って認証を突破したり、顔を印刷した紙を加工して、それを使って顔認証を突破したりする実験も行われています。

また、指紋認証が携帯電話に登場したときから、本人が寝ている間に、勝手に指を押し当てて認証を突破するという話があります。最近では親が寝ている間に子どもが勝手に認証し、ゲームに課金して遊んでいたという例もあります。

従って、勝手に認証される可能性がある環境では「PIN コード」入力が必要になるよう、わざと生体認証を数回失敗させて、それ以上勝手に生体認証できない状態にするなどの工夫が必要です。

生体認証はこのほかにも、目の虹彩の模様によって認証する「虹彩認証」、手や指の静脈のパターンで認識する「静脈認証」などがあり日々進化しています。

それぞれの特徴やセキュリティ上のメリットをよく検討して利用すると良いでしょう。

「暗号キー」は攻撃に遅延がないので、「総当たり攻撃」を含め全ての攻撃が有効です。また攻撃されるまでもなく、そもそも「暗号キー」が漏れていれば暗号化された中身が解読され、ひとたまりもありません。この暗号キーが事実上漏れた状態になる話は、62ページ以降で詳しく説明します。

7 パスワードの定期変更は基本は必要なし。ただし流出時は速やかに変更する

利用するサービスによっては、パスワードを定期的に変更することを求められることがあります。しかし、前出のように十分に複雑で使い回しのないパスワードを設定し、実際にパスワードを破られアカウントを乗っ取られたり、サービス側から流出したりした事実がないのならば、基本的にパスワードを変更する必要はありません。

むしろパスワードの基準を定めず、定期的な変更のみを要求することで、パスワードが単純化したり、変更がワンパターン化したり、サービス間で使い回しするようになることの方が問題となります。

ただし、アカウントが乗っ取られたり、流出の事実を知った場合は速やかにパスワードを変更し、その原因も特定しましょう。

原因がマルウェアなどでパソコン側から情報が流出し続けている場合、原因を特定しないまま放置しているなら、パスワードを変更しても意味がありません。

またアカウントが完全に乗っ取られてしまった場合はウェブサービスに連絡して復旧しましょう。

一方、自分の使用機器からではなく、ウェブサービスなどの側からパスワード流出が起きた場合は、速やかにパスワードを変更の上、流出の原因となった点の対策が行われたかを確認しましょう。

サービス側からパスワード強制リセットの通知や、再設定のリクエストが来たら、次項の便乗攻撃に注意しつつ、同様に速やかにパスワードを変更しましょう。

8 パスワード流出時の便乗攻撃に注意

サービス側からパスワード再設定の通知がメールなどで送られて来た場合、まずそれが本当にサービス側から送られてきたものかどうか、該当のサービスのホームページやニュースサイトでチェックし、事実の確認をしましょう。

サービス側を装ったパスワードリセットの通知は、流出事故に便乗したフィッシング詐欺などのよくある攻撃パターンです。パスワードを奪う攻撃者の罠かもしれません。通知のメールにパスワードリセットのリンクなどが貼られていても、うかつにクリックしないよせず、リセットする場合も直接ウェブサイトやアプリからしましょう。

なお、ウェブサービスを利用する時は、パスワードが流出した場合にも簡単にアカウントを乗っ取られないように、必ず二段階認証や多要素認証を設定しておきましょう。これが提供されないサービスは、今日ではセキュリテが低いので、利用は再考しましょう。

9 適切なパスワードの保管

さて、日常的にインターネットを利用していると、IDとパスワードは無限に増えていきます。これはどう管理すれば良いのでしょう。

本書では、「スマホ用のパスワード管理アプリ」と「物理的な紙のノート」の利用を推奨します。

スマホのパスワード管理アプリを導入する場合は、ネットにデータを置く「クラウド連携(バックアップ)機能」を安易に利用せず、まずはスマホ内だけで管理する「スタンドアロン」状態で利用できるものを優先しましょう。

紙と比較した場合、スマホはネットに接続されているので、攻撃者にクラッキングされる可能性は捨てきれませんが、利用規約を守り、システムを最新に保っている限りは、スマホのセキュリティは十分に高い設計となっています。

また、紛失や盗難に遭っても、最新のスマホではデータは暗号化された状態で保存されていますし、管理アプリも独自に暗号化するので2重に暗号化された金庫での保管に等しくなります。加えてスマホは、事前にきちんと設定しておけば、紛失や盗難に遭っても遠隔操作でロックして操作できなくしたり、場合によってはワイプ(消去)して情報流出を避けたりできるという、紛失に対する3重4重のセキュリティが設けられています。

一方、紙のノートを推奨する理由は、あたりまえではありますが、紙のノートはネットに接続できないからです。接続できなければネット経由のサイバー攻撃も不可能です。奪うには現実世界で「盗む」という行動を起こさなければなら

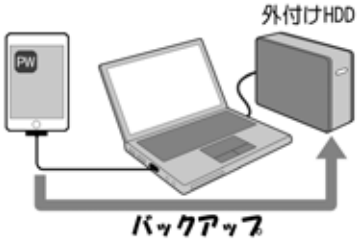
ブラウザにはパスワード保存しない

ブラウザにパスワードを保存すると、席を離れたときに勝手に利用されたり、パソコンをクラッキングされた際に根こそぎ盗まれる可能性があります。

パスワード管理方法の例

一見分かりにくい専用の紙のノートに二重で

管理アプリのデータは、暗号化したディスクにバックアップ



紙のノートに二重に記入したり、スマホのパスワード管理アプリを使って、パソコン経由で暗号化ディスクにバックアップする方法があります。紙のノートは一見内容が分からないようにできる専用のノートも売られています。

パスワード管理方法のメリットデメリット

	利便性	盗まれたときの対策	ネット経由のセキュリティ	データの管理者
紙のノート	△ 持ち歩き可でも落とすと読まれる	× 家にあると盗まれにくいが、盗まれると対応できない	○ 攻撃不可	本人
スマホアプリ	○ ロックしたまま持ち歩き可	○ バックアップがあれば復元可能	△ セキュリティレベルによる	本人
外付けHDDへバックアップ			○ ただし普段は接続しない	本人
クラウドサーバにバックアップ			△ サービス側のセキュリティレベルによる	事業者

パスワードの管理方法とバックアップ方法を一つの表で同列にまとめていますが、一番右列のデータの管理者の項目をよく見て下さい。クラウドサービスを使ったバックアップは便利ではありますが、データの管理者は自分ではなくなります。またクラウドサービスのセキュリティがどのレベルであるのかは、自分では容易に判断出来ません。多少の不便さはあっても、自らの責任において管理するのか、それとも他人の手を借りるのか、クラウドはそれに伴うメリットとデメリットをよく勘案して利用しましょう。

ず、攻撃者が姿を現すリスクがあることが抑止力になるからです。

10 パスワード情報をクラウドで保管する善し悪し

パスワード管理アプリや同様の機能を持つソフトには「クラウド連携機能」やクラウドを用いた「バックアップ機能」があり、これを利用すると複数端末でパスワード情報を共有できたり、明示的にバックアップ処理をしなくても自動でクラウド上にバックアップデータが作られたりします。

この機能を無条件で推奨しない理由は、「重要な情報が複数箇所に存在すれば、流出する可能性はその分増える」からです。

加えてクラウドサービスを利用する場合、他人の手元でデータが保管されますが、利用者には、そのシステムのセキュリティレベルの実態を知ることも管理することもできません。

また、パスワード管理アプリのデータがスマホ上にある限りは「PIN コード」方式で守られますが、クラウドのバックアップデータが流出すれば、それにはマシンパワーにものを言わせた高速な暗号化解除の攻撃が可能になるからです。

銀行の口座からお金が盗まれれば、自分にミスがない限り銀行が補償してくれますが、クラウドから流出した情報は実質的に回収不可能です。これは「お金は補填が可能だが、重要情報の秘密性は戻らない」のです。

11 ノートやスマホを失くした場合のリカバリ考察

スマホも紙のノートも、紛失してしまうとリカバリーするまで困るのは同じです。ただ、スマホの場合、パソコンでスマホのデータを丸ごと暗号化してバックアップをしておけば、紛失しても代替機をパソコンに接続し「復元」を指示するだけで、環境やパスワード管理アプリの内容を含めて、全て元の状態にできるものもあります。

またスマホを丸ごとバックアップしなくても、パスワード管理アプリのデータを、パソコン経由で暗号化された外付けディスクなどにバックアップし、普段は接続せず適切に保管しておけば、盗まれたり流出したりすることもありません。アプリによっては紙に印刷して保管する機能もあります。

なおクラウドサービスのメリットとデメリットを理解した上で、クラウドを使った複数機種での連携機能、自動バックアップやそれに付随するリカバリ機能を利用するのは一つの選択肢と言えます。

紙のノートの場合は、紛失した場合に備え2冊同じ物を作り、一つは金庫に保管するなどのバックアップ手段を取りましょう。

紙のノートによるパスワード管理は、平文で書いてあるものを持ち歩いて紛失してしまった場合、中を見られないような制限はかけられませんので、一見してもパスワードが分からない、専用のノートを利用するのが安全でしょう。

12 注意するべきソーシャルログイン

機器やウェブサービスのパスワードは、使い回しをしないのが絶対です。しかし、膨大な数のパスワードを暗記するのは非現実的なので、必然的にパスワード管理アプリやパスワード管理のノートを使う必要があります。

この手間は、情報漏えい対策のために「パソコンのブラウザにIDやパスワードを覚えさせる機能(＝オートコンプリート)」を使わないならなおさらです。

これを解決する策として「ソーシャルログイン」という方法が用いられて来ました。これはIDとパスワードの管理がしっかりしたウェブサービスのアカウントで、他のサービスを利用するというものです。

しかしこの本を執筆している2018年時点で、最大手SNSサービスからこのソーシャルログインで用いられる身分証明の証(トークン)が流出するトラブルがあったため、本書ではソーシャルログインも非推奨として、基本的にそれぞれのサービスはそれぞれ別々のIDとパスワードを設定する事のみを推奨することとします。

トークンが流出すると、IDとパスワードが流出しなくても、ソーシャルログインを設定していたサービスに根こそぎアクセスしてしまえる可能性があるからです。

一方、それぞれのウェブサービスを利用するときに、別々のIDとパスワードを入力する手間を省くために、パスワード管理アプリが進化し、ウェブサービスやアプリのログイン時に、自動的に入力してくれる機能も登場してきました。二段階認証の使い捨てパスワード入力も楽になっています。

それらを活用することで、サービスの間でパスワードの使い回しをしないというルールを、ストレス無く守るようにしましょう。

13 二段階認証を活用する。ただしSMS認証は避けるる

IDとパスワードでの認証にさらにもう一段階チェック機能を追加するのが二段階認証や多要素認証と呼ばれる機能です。これを利用することで、パスワード流出や乗っ取りなどへの防御をします。

もっとも一般的なものは、何らかの手段で入手する、その場限りの「ワンタイムパスワード」の入力を追加する方法です。

ログインに当たって、サービス提供者から、SMS(ショートメッセージ)、電子メールで送られてくるものを利用する方法や、スマホのアプリを使って生成するソフトウェアトークン、専用の小さな乱数を発生するハードウェアトークンを利用する方法があります。

このうち、SMSは海外で乗っ取りによる成りすましで破られた例があり、電子メールも経路上で奪取される可能性があるので、種類を自分で選択できる場合はトークン形式を選ぶことを推奨します。

ソフトウェアトークンは専用のアプリを利用するものありますが、QRコードを使って情報を読み込むものの場合は、パスワード管理アプリで一括して管理出来るものもあるので、検討しましょう。

またスマートウォッチの中には、スマホのパスワード管理アプリと連携して、手元でIDとパスワードを確認したり、二段階認証用の

現時点で推奨できる二段階認証要素

基本的に推奨できるもの

ソフトウェアトークン
(ワンタイムパスワード生成)

USBキー

生体認証
(指紋認証など)

アプリから認証

推奨できないもの

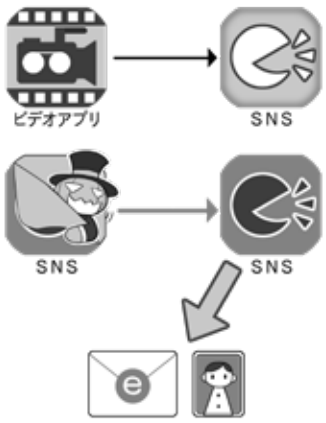
SMS(ショートメッセージ)メール
(ワンタイムパスワード送信)

SMSを使ったワンタイムパスワード受信は、海外でSIMハイジャックという攻撃により破られた例があります。またメールも同様にパスワードを「送信する」をいう点で攻撃の余地が多くなります。

ソーシャルログインとサービス・アプリ連携の違い

ソーシャルログイン

アプリ・サービス連携



アプリの作者が実は攻撃者で、勝手に不正な投稿をされることも

ソーシャルログインは、堅牢なサービスのアカウントを別のサービスの鍵に使え便利ですが、大本のアカウントの認証情報が漏れる事案が発生したため、それぞれのサービスに別々のパスワードを使用する基本対応を推奨します。

アプリなどの連携は定期的に棚卸ししよう

自分が意識的に連携をしていなくても、ネット経由で回ってきた「面白いアプリ」を利用したら、いつの間にか連携されていた、ということもあります。またその時は問題が無くても更新時に権限の拡張を求めてきて、結果的に個人情報を「合法的に」奪うアプリも存在しています。アプリ連携やアプリの権限は定期的に棚卸して、不必要なものや不審なものは連携解除するか、削除するようにしましょう。

パスワードを発生させたりできるので、より快適なパスワード管理を求めるならば利用しましょう。

このほかにも、USB形式の物理的な鍵(キー)や生体認証を用いる方式もあります。またIDとパスワードをネット経由で送信することをそもそも解消する方式も検討検討されています。

より安全な利用のために、アンテナ高く情報収集しましょう。

14 権限を与えるサービス連携にも注意

ソーシャルログインと混同されやすいものに、SNSに関する機能連携として「サービス・アプリ連携」というものがあります。

たとえばAというSNSにBというサービスやアプリから、投稿を認めるといったものです。具体例としては特徴的な機能を持つカメラアプリにSNSへの写真付き投稿を認めるといったものがあります。

これはソーシャルログインとは別の性格の機能ですが、ときに「連携するアプリやサービスに投稿を認める(＝権限を与える)」という部分が、攻撃者による攻撃の手段として利用されることもあります。ソーシャルログインとサービス・アプリ連携の、2つとも利用は避けるようにしましょう。

SNSを利用していると、自分が意識しないうちに誤操作をし、知らずにサービス・アプリ連携していることもあります。

定期的に使用しているSNSアカウントの「連携を確認できる画面」を開いて、知らないアプリや止むを得ず使ったサービス・アプリの連携があれば解除しましょう。

コラム：暗号化の超簡単説明

暗号とは、自分と相手だけが読めて他人が読めないという、セキュリティを保つ技術です。

暗号化というと非常に難しく感じるかも知れませんが、大丈夫、その心配にはあたりません。

ただ暗号化の内容を詳しく書くとそれだけで本になってしまうので、ここではその概念をごく簡単に説明します。

1．暗号化とは「魔法をかけて手紙などの内容を読めないようにする」ことです。

2．暗号化の魔法にはいくつもの系統(方式)があり、魔法をかけるには呪文(「暗号キー」)を決めて使います。

3．魔法の呪文(「暗号キー」)がばれると、魔法が解けて内容が読めてしまいます。

4．古い系統の魔法の中には、その仕組みに不備があり、呪文が分からなくても解けてしまうものがあります。

初歩としてはこのぐらいの理解があれば大丈夫です。

使用する暗号方式が安全かどうかは、魔法研究の専門家に任せましょう。車がどうやって動くのか知らなくても、安全な利用が出来るのと同じです。

大切なのは正しい使用法を知ることと、専門家が「危険が発生した！」という情報を発信したらキャッチし、迅速に避けるように行動する事です。

右のイラストでは、具体的に危険が発生する例を描いていますので、是非覚えておいてください。

まず第一歩は「正しく使う事」からです。

Cipher Disk(シーザー暗号)

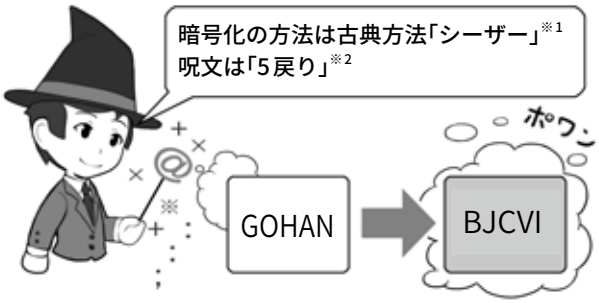
もっとも原始的な暗号はシーザー暗号と言われるものです。文字をずらして記述するだけのシンプルなもので、仕組みさえ分かればアルファベットなら26回試すまでに暗号が解けてしまいます。上の図はその暗号を解きやすくするためのCipher Disk(暗号ディスク)です。現代の暗号は複雑な演算を伴うために、人力での解読はほぼ不可能です。

暗号化ってなに？

平文での通信は読めてしまう

暗号化していないと、攻撃者はどこでも盗んで読み放題

暗号化の魔法は内容を読めなくする



※1：暗号化方式　※2：「暗号キー」

暗号化したものを送れば攻撃者が読めない

※ただし、攻撃者が「シーザー暗号」を読めない場合

事前に決めておいた方法（暗号化方法）と呪文（「暗号キー」）で暗号文を復元（復号）する

暗号が破られる場合

暗号化方法の種類はいろいろ

シーザー暗号化方法
×　古い、危険すぎ

「WEP」方法
×　解読されるからだめ

「WPA」方法
○　呪文が長ければ安全

暗号破られ①　呪文がバレている！

暗号破られ②　方法が古くて解読可能！

暗号破られ③　呪文が簡単すぎて解読される

コラム：パスワードの管理について（2018年の動向まとめ）

ここでは、パスワードの管理に関する最新の動向を踏まえて、本文でも紹介した最新のテクニックを詳しく解説しましょう。攻撃者から身を守るためには、最新の技術で先手を打つのも一つの対策だからです。

パスワードに関して、今年は約16億件のパスワードが流出したというニュースが流れました。また有名ホテルチェーンが顧客情報約5億件を流出させたニュースも報じられました。こうして流出したID/パスワードは必ずと言っていいほど不正アクセスに使われます。そういった攻撃から身を守るには手段は2つ。1つは、万が一流出しても被害を最小限にとどめるため、サービス毎に別々の長くて複雑なパスワードを設定する事。もう一つはそもそもパスワードを盗めないようにしてしまうことです。

● パスワード管理アプリの高度な利用

パスワードに関してNISCでは、「人は必ずヒューマンエラーを起こす」ことを前提に対処方法を考えます。例えばパスワードの管理は数が多くなるほど覚えにくく、使い回しをせずサービス毎に別々のものを考えるのは面倒で、何も対策せずに強要すると、そのうちワンパターン化したり、同じ物の使い回しを始めたりするのではないかと考えます。

これを解決するため、総合的にパスワードを管理する、スマホの「パスワード管理アプリ」を推奨します。パスワード管理アプリは単にパスワードを保管してくれるだけではなく、条件を設定するとそれに合わせた長くて複雑なパスワードを自動的に生成してくれるほか、最近ではWebブラウザでのサービスログイン時に、自動的に起動してID/パスワードを入力したり、アプリ起動時にもID/パスワードを入力してくれたりするように進化しているものもあります。パスワードをいちいち管理アプリを見て入力したり、カット＆ペーストしたりする手間も省きつつ、皆さんの負担を軽減する傾向にあるのです。

またパスワード管理アプリの中には、二段階認証で利用する使い捨てパスワードを発生するためのQRコードを、アプリ内で読み込めるようになっているものもあります。二段階認証で使い捨てパスワードを利用する設定にすると、サービスそれぞれが別々の「ソフトウェアトークンアプリ」をインストールさせるように見えて、実は必要なのはこのQRコードを読み込ませることだけなので、パスワード管理アプリに読み込んで、一括して管理するようにできるのです。

加えて、アプリによってはスマートウォッチとの連携を行っているものもあります。これらのアプリでは、スマートウォッチにインストールされた連携用のパスワード管理アプリ上で、登録しているID/パスワード、二段階認証用の使い捨てパスワードを発生させることもできるので、パソコンでWebサービスへのログインに際して、スマホを立ち上げなくても、手元でログインに必要な情報をすべて確認できます。

これらを使って、楽に個別のパスワードを管理しましょう。どういったアプリが条件を満たすのか評価記事等を参考に検索して、利用する時は責任関係がしっかりとする有料のものを選択しましょう。無料のアプリには情報を抜き取ることを目的とするものも紛れ込んでいるからです。

● パスワードを無くすFIDO

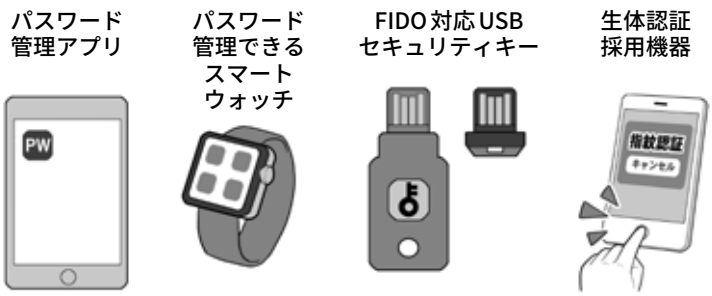
主としてパスワードが流出するのは、サービス側で保管しているID/パスワードを含めた個人情報が、多量にまとめて盗まれるケースです。従って、サービス側に盗むべきパスワードが無い場合は、この攻撃は成功しません。その為にパスワードそのもの無くすことを目指すのがFIDOアライアンス（Googleやマイクロソフト、NTTドコモといった大手IT企業や通信会社、信販会社、通販会社が加盟）が進めるFIDOという方法です。この方法では利用者が「本人」である

という認証をパソコンやスマホなどそれぞれの機器の上で行い、利用するサービスへは「本人だと認証しました」という情報のみをやりとりするのです。本人だと認証する方法は、USB接続等のハードウェアキー、指紋認証・顔認証などの生体認証です。

現在Googleのサービスの一部で利用が始まっている他、正確にはFIDOではありませんが、同じ規格をベースにした、Windowsへのログイン方法であるWindows Helloなどがこれらの方式を採用しています。

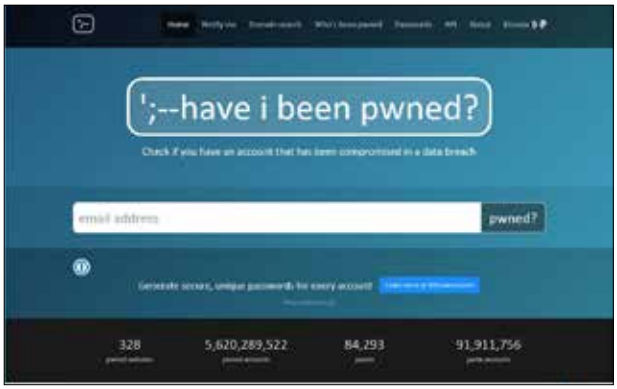
今後これらの方式が普及してきた場合、積極的に選択することも検討しましょう。少なくともGoogleの社内ではUSBのハードウェアキーを採用することで、フィッシング詐欺の被害がゼロになったとのことです。

パスワード管理の新しいルール



ハードウェアメーカーが推奨し、密接に連携するパスワード管理アプリと対応スマートウォッチ。これらの導入がセキュリティの向上に役立ちます。

流出ID/パスワードチェックサイト「Have I Been Pwned?」（私、漏洩してる？）



メールアドレス流出チェックURL：https://haveibeenpwned.com/
パスワード流出チェックURL：https://haveibeenpwned.com/Passwords/

他にもFirefox Monitorなどで、同等の機能が提供されています。実績もありセキュリティ業界において評価は高いですが、あくまでも民間のサービスなので、その点を理解して利用しましょう。

● パスワード流出を能動的に検知する

パスワードの流出は、登録しているサービス側からの流出の事実の通知が行われる他に、流出情報の検索サイトで能動的に調べる事ができます。

セキュリティ識者のトロイ・ハントさんが、流出したID/パスワード情報を収集し検索できるようにした「Have I Been Pwned?」は、オーストラリア・イギリス・スペインなどの政府のメールアドレスのチェックなどにも使われており、サイトで自分のID/パスワードが流出していないかチェックできるほか、事前に登録しておくと流出時に警告のメールが送られてきます。

またパスワードを入力して、そのパスワードが「流出した履歴あり」と出た場合、それはあなたの情報の流出であっても他の人の情報の流出であっても、以降パスワードリスト攻撃の対象になるので変更しておきましょう。

根っこは同じデータベースを用いますが、ブラウザを提供しているFirefoxもFirefox Monitorとして同様のサービスを提供している他、パスワード管理アプリでもパスワードのチェックに採用する動きが見られます。今後こういった流出情報のチェックサービスは増えていくと予測されるので積極的に活用して、攻撃される前に対処するようにしましょう。

2 通信を守る、無線LANを安全に利用する

私たちが日常的にインターネットで送信するIDやパスワード、送受信するメールの文面やウェブサイトで閲覧する内容は、常に攻撃者の盗聴や盗み見の危険にさらされています。

攻撃者はそうした情報を不正に入手して売却したり、様々な手段を駆使して直接お金を手に入れるために利用したりします。それを阻止するためには、通信している情報の暗号化が必要となるのです。

そもそもインターネットはその始まりにおいては、暗号化など全くされておらず、情報をそのままの状態(平文)で送受信するシステムでした。

インターネットは、蜘蛛の巣状に接続し合ったサーバ間で、どこかの経路が遮断されても迂回して通信を続ける、そういう面では先進的ではあったのですが、攻撃者などの悪意の存在を前提に構築してはいなかったからです。

その後インターネットの発展にしたがって、悪意を持ったものが現れ、コンピュータウイルスの登場や、パスワードを破って侵入しての情報の奪取、通信中の情報の盗聴が行われるようになり、それぞれ対策が必要になりました。

コンピュータウイルスにはウイルス対策ソフトが、パスワード破りには複雑なパスワードや二段階認証や多要素認証などが、そして通信中の情報の盗聴には暗号化が、攻撃者への防御として普及していくわけです。

1 それぞれの状況に合わせた暗号化の必要性

一口に通信の暗号化と言っても、様々な状況に合わせた、それぞれの暗号化があります。

私たちが通信する場合、有線LAN、LTEなどの携帯電話回線、Wi-Fiなどの無線LANなど、多様な通信手段があります。

このうち攻撃者にとって、手軽に行いやすい攻撃の一つとして無線LAN通信の盗聴があります。

無線LANではその名の通り通信機器が無線(電波)を使って通信するので、盗聴に際して特に何か工作する必要はありません。通信が暗号化されていなければ、無線LANに対応したパソコンを持って電波が届く範囲に居るだけで、簡単に盗聴することが可能です。

一方、有線通信が暗号化されていなければ、通信経路上のどこかで情報を盗聴することが可能です。

さらに、攻撃者が利用者のふりをしてメールサーバやパソコンに侵入すれば、中にたまったメールや、内蔵ディスクなどの中の情報も盗み見し放題です。

パソコンがマルウェアに感染して、ディスクの中の暗号化されていないファイルが流出し、見放題になるという事件もありました。

そういった状況を避けるためには、仮に盗聴されたり、侵入されたり、流出してしまっても、通信内容や重要なファイルの中身が見られないように、それぞれのシーンに応じた適切な暗号化をする必要があります。

その対策を挙げていくと数え切れないのですが、このセクションでは、まず私たちの生活でもっとも身近な無線LAN通信の暗号化について説明しましょう。

2 無線LAN通信(Wi-Fi)の構成要素

インターネットにつながった無線LANアクセスポイントさえあれば、いちいち機器にLANケーブルをつながなくても、手軽にインターネットを利用できる無線LAN通信(Wi-Fi)。

家庭で利用する無線LANでも、外出時に利用する公衆無線LANでも、セキュリティがしっかりしていなければ、攻撃者にIDやパスワード、通信中のデータ全てを盗まれる危険性があります。

それを理解するために、まずは無線LAN通信を構成する要素を理解しましょう。

最初は無線LAN通信を提供する「無線LANアクセスポイント」になる機器。一般には「無線LANアクセスルータ」「Wi-Fiルータ」あるいはシンプルに「ルータ」などと呼ばれます。

この機器で無線LAN通信を提供する際、最低限以下の3つを設定します。

① 識別名「SSID(Service Set Identifier)」

②通信内容を暗号化するための「暗号化方式」
③その暗号化のための鍵となる「暗号キー」(設定上は暗号化キーと書かれる)

「暗号キー」は利用者が無線LANアクセスポイントに接続するときのパスワードのように使われるほか、通信内容を暗号化する時と、元に戻す復号(元の平文に戻す)の時の鍵として使われます。

ここまでが無線LANアクセスポイントの構成要素です。

スマホやパソコンが無線LANを利用して通信するときは、利用する機器の無線LAN(Wi-Fi)設定で、SSIDを手掛かりに目的の無線LANアクセスポイントを見つけ、必要な場合は暗号化方式を選択し、「暗号キー」を入力して接続します。

なお、災害時や公益目的で、誰でも無線LANを利用できるように、(その安全性は別として)00000JAPANを筆頭に「暗号化なし」で提供されている無線LANアクセスポイントもあります。

この場合は利用時に暗号化方式も「暗号キー」も必要ありません。

次に無線LANの危険要素について説明します。危険なポイントは以下の2つになります。

①「通信が暗号化されていないか、されていても安全ではない場合」
②「暗号化の鍵(「暗号キー」)が公開か漏れている場合」

3 暗号化なしや、方式が安全ではないものは危険

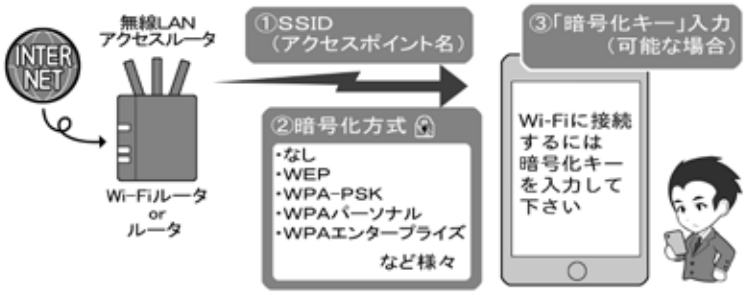
無線LANの利用において、通信

それぞれの状況に合わせた暗号化

通信の暗号化　**ファイルの暗号化**

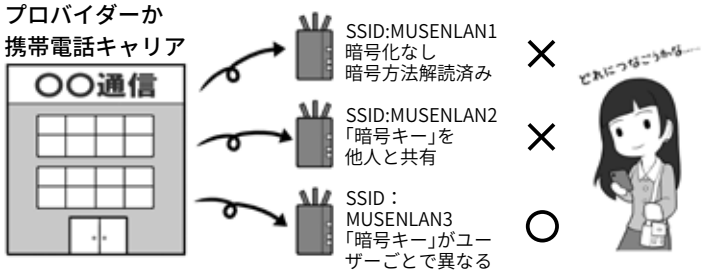
暗号化には、電話、メール、ウェブ閲覧などの「通信の暗号化」と、ファイルやパソコンのハードディスクなどの「ファイルの暗号化」があります。

暗号を使う無線LANの構成要素



暗号化を伴う無線LAN通信には暗号化方式と「暗号キー」の設定が必要となります。「暗号キー」は機器に接続する為のパスワード的にも使われます。

公衆無線LANが安全とは限らない



信頼がおける企業や団体でも、提供しているWi-Fiが安全とは限りません。アクセスの利便性のため暗号化無しで提供される場合もあるからです。

「暗号キー」共有は接続しちゃダメ

暗号化方式が安全でも、「暗号キー」を見知らぬ他人と共用するものは、すべて危険です。こういった方式は、公衆無線LANやホテル、公共機関、インターネットカフェやレストランなどで広く使われています。提供する側が善意で行っていても、攻撃者は善意で行動しません。攻撃出来る環境があると判断するだけです。安全に通信するための自前の暗号化ができなければ利用してはいけません。

が暗号化されていないものは、内容が平文で送受信されているので、別の手段での暗号化を行わないまま使っていると、攻撃者に内容を盗聴されてしまいます。

そのため、まず「暗号化なし」のアクセスポイントは基本的には利用しないようにしましょう。

災害時など例外的に使用する場合は、後述の「10 公衆無線 LAN が安全でない場合の利用方法」を参照してください。安全な利用には最低限、別の手段での暗号化が必要だと覚えておいてください。

暗号化なしの通信は、拡声器で遠くの人と話しているようなもので、耳を傾ければその場にいる誰もが内容を知ることができます。

無線 LAN 通信が暗号化されていても、その暗号化方式がすでに破られていて安全ではない場合、上記と同様に攻撃者は通信を盗聴して、内容を解読することができるので、これも危険です。使用しないようにしましょう。

これは、「英語でしゃべればわからないだろう」と思ったら、周りに居た人も英語が理解でき内容がばれるイメージです。

危険である暗号化方式の具体例としては、「WEP」という名前のものや、方式の名称の中に「TKIP」と含まれるものが該当します。

一方、暗号化方式として安全とされるのは WPA-PSK(AES)、WPA2-PSK(AES)、WPA2-EAP、WPA2- エンタープライズ、IEEE 802.1x、SIM 認証、そして無線 LAN の多くの問題点を解決するために登場しつつある WPA3、それらの記述があるものです。安全な方式の詳細は 69 ページを参照してください。

4 暗号化方式が安全でも「暗号キー」が漏れれば危険

暗号化の方式自体が安全でも通信を暗号化するための「暗号キー」が漏れていると、通信を盗聴した攻撃者が通信内容を復号したり、同じ SSID と「暗号キー」を使って偽の無線 LAN アクセスポイントを作り、本物のアクセスポイントになりすまして通信内容を根こそぎ奪う、中間者(Man-in-the-middle)攻撃を行ったりすることができるようになります。

イメージとしては、破られていない暗号化方式は誰も知らない言語で、「暗号キー」が辞書。しかし辞書が他人の手に渡っていると、たとえ知られていない言語でも解読されてしまうし、その情報をもとに通信する相手になりすますこともできる、というものです。

この至極単純な「暗号キーが漏れていれば、暗号化された通信を復号し解読できる」ということも、よく覚えておいてください。

5 家庭内での安全な無線 LAN の設定(暗号化方式)

家庭内で無線 LAN を使用する場合、先ほど説明した安全な暗号化方式である WPA-PSK(AES)か WPA2-PSK(AES)を利用し、「暗号キー」を基準に従って、完全にランダムで充分に長くして、さらにその「暗号キー」を「家族だけが知っている」状態に保てれば、ほぼ安全に使用することができます。

これを実現する為、無線 LAN 機器設置時には、まず機器を購入したときの初期の「暗号キー」は変更しましょう。上記の通り家族だけしか知らない「暗号キー」に変更しなければなりません。メーカーによっては「暗号キー」が共通だったり、付け方に規則性があるかもしれないからです。

また極端な考え方をすれば、その機種がメーカーから手元につくまでに、初期の「暗号キー」を見たものがいないとも言い切れません。

なお SSID を変更する場合、自分や家族の名前、家族を想起させるものは使わないようにしましょう。あなたが攻撃のターゲットの場合、攻撃するべき無線 LAN を特定させるヒントになるからです。

家庭用無線 LAN アクセスルータは、標準で 2 つ以上の SSID を持てるものが多く、そのうちの一つには、WEP などのもはや安全でない古い暗号化方式が設定されている場合があります。これは主に古いゲーム機などが接続できるようにするためだったりします。

しかし、こういった設定はセキュリティ上の穴となるので、設定を変更し、安全な暗号化方式に変更するか、安全でない暗号化方式の設定はすっぱりと停止しましょう。古いゲーム機など安全でない暗号化方式しか選べない機器の接続は諦めましょう。

同様に、ゲスト用に簡便な「暗号キー」や、問題のある暗号化方式を使った接続設定があれば、これも停止しましょう。ゲストに家族用の SSID に接続させるのも安全ではありません。「暗号キー」が「家族だけが知っている状態」では無くなってしまうからです。

どうしてもゲスト用に一時的にアクセスポイントを開放したい場合は、2 つの SSID の一つをゲスト専用にし、2 つのアクセス設定

の間で、お互いのアクセスポイントに接続した機器が見えないような分離状態に設定しましょう。そしてゲストが帰宅したら、そのSSIDは利用停止しましょう。

6 家庭内での安全な無線LANの設定（その他）

無線LANアクセスルータには、ウェブブラウザを使って本体の設定画面にアクセスするための、機器管理用のIDやパスワードがあります。それは管理者アカウントとも呼ばれます。

こちらのパスワードも必ず購入時のものから変更しましょう。このパスワードはログイン画面から使用するものなので、「ログインパスワード」の基準に従い変更しましょう。

この設定画面が、もし家の中からだけでなくインターネット側からアクセスできるようになっていたら、アクセスできないように変更しましょう。また設定画面が無線LANで接続した機器からアクセスできず、有線LANからのみアクセスできる設定にしましょう。家の外にいる攻撃者が無線LANに接続し、変更できないようにするための予防策です。

無線LANアクセスルータにルータ本体と機器のボタンを押すだけで簡単に接続できる「WPS」「AOSS」「無線LANらくらくスタート」といった名称のもの、もしくは類似の機能がある場合は利用不可にしましょう。この設定をONにしていると、目を離したすきに、利用してほしくない人物が、ボタン一発で手元の機器を無線LANに接続できてしまうからです。

家庭でのWi-Fiの利用

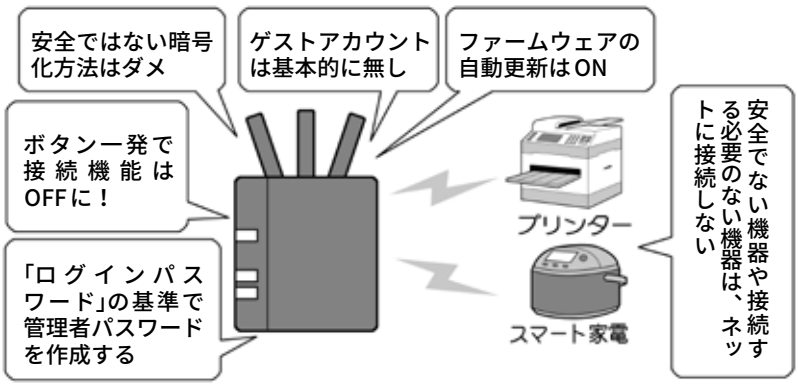
①出荷時の管理者パスワード、「暗号キー」の変更

出荷された機器は、厳密に言えば誰かの手によって梱包されているので、出荷時の「暗号キー」が見られている可能性があります。必ず変更しましょう。

②「暗号キー」は家族のヒミツ

家庭で使える暗号化方式は、「暗号キー」を家族のみの秘密にすることが、安全に使うための絶対条件です。他の人には教えないようにしましょう。

③ルータと機器の安全な運用



家庭で無線LANや有線LANを使用する場合、注意したり設定を変えたりしなければならない点がたくさんあります。必ずチェックして安全な状態を作りましょう。また基本的に接続する必要が無い機器を、むやみに家庭のLANに接続しないようにしましょう。

どうしても利用する場合は、設定画面からそのときだけONにして使用し、設定後はOFFにします。UPnP（Universal Plug and Play）の設定も、不用意に家庭内のLANの機器をインターネット上に公開してしまう可能性があるので、OFFにします。そしてネットに接続する必要のない機器は、無線・有線にかかわらず、そもそもLANに接続しないようにしましょう。

無線LANアクセスルータの設定画面に、本体ファームウェアの自動アップデート機能がある場合はONにしておきましょう。それによりメーカーがルータの不具合（バグ）などを修正した場合、自動で更新が行われセキュリティが最新の状態に保たれます。

もし自動アップデートの設定がない場合は、自分のスマホに定期的な予定を作り、それに従ってファームウェアが更新されていないかチェックし、公開されていれば更新処理を行いましょう。

なお、昔に書かれたセキュリティの解説記事によっては、「SSIDを隠すステルス設定」や、接続できる機器をLAN機器の番号で制限する「MACアドレス規制」を対策として推奨していたりします。

しかし、ステルスになったSSIDも簡単に探し出すことが可能ですし、MACアドレスは盗聴可能かつ詐称可能ですので、これらの対策を行っても安全性は向上せず、むしろ利便性が悪くなるので、設定する意味はないでしょう。

無線LANアクセスルータは、家庭のセキュリティの要です。お使いのルータに上記のようなセキュリティの設定がない場合や、安全な暗号化方式の設定がない古い機器の場合は、速やかに利用を停止し最新のものに買い換えるようにしましょう。

7 公衆無線LAN利用時の注意

公衆無線LANの安全な利用は、家庭用の無線LANの安全な利用と少し事情が異なります。

例えば公衆無線LANで「WPA-PSK（AES）/WPA2-PSK（AES）」の方式の無線LANが提供されていた場合、暗号化方式自体は安全でも、別の危険があります。

上記の名称の中のPSKの部分はPre-Shared Keyの略です。利用にあたり「暗号キー」を事前に共有する方式のことで、この方式では家庭内の利用のときと同様に、複数の人で同じ「暗号キー」を使う事になります。これを公衆無線LANに当てはめると、全く知らない人と、同じ「暗号キー」を一緒に使うことになります。

その設定を使って通信を行うと、「暗号キー」を知っている攻撃者により、通信内容を直接盗聴されたり、なりすまし無線LANアクセスポイント（偽アクセスポイント）を仕掛けられ、盗聴されると言ったことが避けられません。

しかし、この方式を含め安全でない暗号化方式は、街中のカフェやレストラン、ホテル、あるいはインターネットプロバイダーや携帯電話キャリが提供する公衆無線LANでも広く使用されています。これらのアクセスポイントは全て危険ということになります。

こういった危険なアクセスポイントを使用する場合、無線LAN通信の暗号化とは別の暗号化機能で対処する方法もがあります。それについては後述します。一方、安全な暗号化方式の選択で安全を確保する方法もあります。

8 個別の「暗号キー」を用いる方式の無線LAN

公衆無線LANにおいて通信の安全を確保する方法は、危険な暗号化方式などを使わないことは当然として、「暗号キー」を他人と「共有しない」で個別の「暗号キー」を用いる方式を利用することです。

この方法は、公表されている公衆無線LANアクセスポイントの情報の中で「WPA2-EAP、WPA2-エンタープライズ、IEEE 802.1x、SIM認証」といった用語が含まれるものを選択するのです。

携帯電話キャリアなどは、いくつかの異なる暗号化方式の公衆無線LANを提供している場合があり、ウェブサイトなどで、それぞれのSSIDが採用している暗号化方式が、きちんと掲示されている場合があります。

利用前にそこをチェックし、上記の方式名を頼りに、安全な接続ができる公衆無線LANのSSIDを探してから利用しましょう。

「WPA2-EAP、WPA2-エンタープライズ、IEEE 802.1x、SIM認証」などが公衆無線LANとして安全である理由は、これらの方式を使用した無線LANアクセスポイントを利用する場合、公衆無線LANサービスの提供者が、利用する一人ひとりの機器または利用者を識別して個別の認証を行い、個別の「暗号キー」を用いて通信を行うからです。

そのため、他人と同じSSIDに

接続しても、自分用の「暗号キー」を他人に知られることがないのです。

一例を挙げると、「SIM認証」と呼ばれる方式では、それぞれのスマホなどに入っているSIMカードの情報を用いて認証＝接続許可を出すわけです。SIMは1枚1枚別々の情報が入っているので、誰かと「暗号キー」が被ることなく安全な通信が確保されるわけです。

9 公衆無線LANに関して新規に購入したスマホなどで行うこと

新規契約や機種変更、携帯電話会社の乗り換えなどをして、携帯電話キャリアでスマホを新規に手に入れたら、まずやることがあります。

そのスマホには、携帯電話キャリアで提供している様々な方式の公衆無線LAN用の自動接続設定が、安全性に関係なくまとめて導入されていることがあるからです。

購入後、細かい設定をしなくても自動的に公衆無線LANに接続できるので便利と思われがちですが、この状態では、意図せず「安全でない方式の公衆無線LAN」に、接続してしまう可能性があります。

新しいスマホなどを手に入れたら、まず接続される可能性があるアクセスポイントの暗号化方式を調べましょう。安全でない公衆無線LANのアクセスポイントに接続してしまった場合、無線LAN接続を切断して、その接続用のプロファイルも削除し、できれば二度とそのアクセスポイントに自動接続されないようにしましょう。

また知らない公衆無線LANアク

公衆無線LAN通信の表示の意味

①スマホやパソコンの画面から見た無線LAN暗号化

接続	Android	iOS、mac OS	Windows
×（暗号化無し）			
△（暗号化有り）			 ＊1

②詳細な区分けから見た無線LAN暗号化

接続	ネットワークの種類	暗号化キー（「暗号キー」）		解説
×	暗号化なし		なし	暗号化なしは論外
×	WEP		事前入手	解読済み。使用は不適切
×	WPA-PSK WPAパーソナル	（TKIP）	事前入手	TKIPには暗号化にセキュリティ上の不安あり。AESは暗号解読不可能とされているが、「暗号キー」が事前に存在し、利用者は皆同じものを共有するので、暗号解読の可能性あり
△		（AES）	事前入手	
×	WPA2-PSK WPA2パーソナル	（TKIP）	事前入手	
△		（AES）	事前入手	
○	WPA2-EAP＊2 WPA2エンタープライズ	（AES）	SIM認証（端末個別）＊2 個別パスワード、クライアント証明書認証（利用者個別）	SIM認証ではSIMの情報を認証に用い、個別の「暗号キー」が利用されるので通信内容の不正な解読は困難。他にも利用者を個別に認証するEAP-TTLS,EAP-TLSなどの方式もある

上の表は、Android、iOS、mac OS X、Windowsなどで、無線LANアクセスポイントを選択する時の画面に表示されるアイコンの例になります。それぞれ2種類のアイコンしかありません。そしてこのアイコンは、各アクセスポイントが信頼出来るかどうかを表しているのでは無く、単純に「暗号化されているかどうか」だけを表しています。

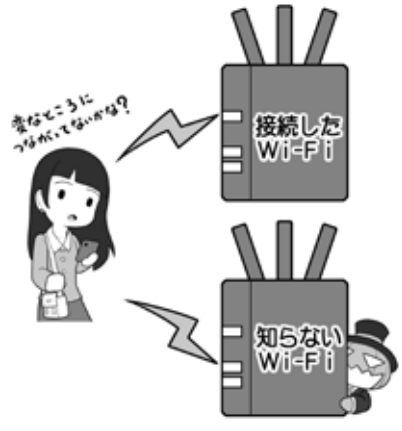
下の表は、暗号化方式のそれぞれの安全性とその理由を書き出したものです。この2つの表を比較すると、すでに暗号化が破られており、利用が推奨されていない「WEP」が、表示アイコン上は暗号化に分類されていることがわかります。アイコンは暗号化の有無を表しているのでこれは正しい表示ですが、アイコンは安全性の担保ではないと認識して下さい。Androidは、接続したアクセスポイントをタップすると「セキュリティ」の項目でネットワークの種類の暗号化方式などを確認できます。Windows、mac OS Xは調べるのに手間がかかります。iOSでは簡単に確認する手段がありません。

なおWPA3が普及すると、これらの問題点のかなりが解消されるようになります。

＊1：Windowsではバージョンによってアイコンに「セキュリティ保護あり」と表示される場合もあります。

＊2：例としてはNTTドコモでアクセスポイントの名称（SSID）が「0001docomo」、auで「au_Wi-Fi2」、ソフトバンクで「0002softbank」のものがWPA2-EAPの方式です。各携帯電話キャリア提供の無線LANアクセスポイントの一部で、自動接続になっているため、意識することはありません。その他の安全性が確保されていないと判断したアクセスポイントに接続されている場合は、接続を切ることが推奨されます。

新しいスマホを購入したら…



携帯電話キャリアなどで購入したスマホには、無料提供されている公衆無線LANの設定が入っています。しかし全ての公衆無線LANが安全とは限りません。それぞれの暗号化方式を調べ、安全で無いものに接続したら切断するようにしましょう。また知らないアクセスポイントに接続した場合も切断しましょう。攻撃者が設置したものだったり潜んだりしている事があります。

セスポイントなどに勝手に接続されてしまった場合は、同様に設定を削除して自動で接続されないようにしましょう。

10 公衆無線LANが安全ではない場合の利用方法

しかし、いつでも安全な状態の公衆無線LANを利用できるとは限りません。先ほど少しだけお話しした、観光目的や災害時に設置される00000JAPANなどの「暗号化なし」の公衆無線LANしか利用できない状況も考えられます。

しかし「暗号化なし」もしくは「危険な状態」で提供されている無線LANアクセスポイントを不用意に利用すると、攻撃者から見れば絶好の獲物が狩り場に飛び込んできた状況になってしまいます。

対策は、「無線LANの暗号化に頼らず、自前で通信を暗号化して盗聴対策をする」ことです。

もしこの言葉の意味が理解できない場合は、ここからはややハードルが上がりますので、無理をせず自前の携帯電話回線、もしくはパソコンならばスマホをルータ代わりに利用する「テザリング」の範囲で、手軽かつ安全にインターネット接続することをおすすめします。

11 自前の暗号化による盗聴対策

自前の暗号化で盗聴対策をする第一歩は、ウェブブラウザでのインターネット閲覧では「https://」から始まるもののみ、メールでは「SSL/TLS」を使った通信設定になっているもののみ、スマホなどのアプリでは暗号通信でサーバに接続するもののみを使用する方法です。

前者2つに関しては、後ほどそれぞれ詳しく説明します。

スマホアプリに関しては、アプリの通信全体を暗号化するトレンドに向かいつつありますが、現状、提供している会社によっては通信を暗号化しているかどうか明確にしていないものも多く、技術者でもない限りは自分で確認することは困難です。

アプリが通信を暗号化しているかどうかは、技術者などによって公開されている情報から確認するか、多くの人が使用していてかつ盗聴や情報流出のトラブルがないもの、という選択しかありません。

もしくは、通信の全暗号化を商品として表明しているアプリに限定して利用することです。

12 まとめて暗号化するVPN、現状は過信できないが今後に期待

こういった個別の面倒な対策ではなく、まとめて一気に対策をする方法もあります。それはVPN（Virtual Private Network：仮想プライベートネットワーク）の個人利用です。

VPNとは元々は、一つの会社の離れた事業所間を、インターネットを使いながら接続する機能です。まるで会社内のLANで接続されているように、秘密を守りつつ互いに通信することができます。VPNはインターネットを使って事業所間を接続してますが、その通信が外部から盗聴できないように暗号化して秘密を守っているのです。

この方式を「事業所から事業所」ではなく、「個人の機器から安全な場所にある出口サーバ」に置き換えて利用するのが、VPNの個人利用です。

この場合、通信は自分のスマホやパソコンから、少なくとも安全な場所にあるとされる出口サーバまで、無条件で全て暗号化されるので、どのようなソフトやアプリでも、またその間の公衆無線LANの暗号化方式が安全でなかったり、そもそも全く暗号化されていなかったりしても、攻撃者に盗聴される心配は少なくなります。

ただ、このVPNの使い方はまだ、一般の利用者が豊富な選択肢の中から選び、ボタン一つで簡単に使える程にはこなれていません。現状は、一部プロバイダーが有料サービスで提供していたり、あるいは有料アプリで提供されていたりする程度で、無料で安全性が高く手軽に使えるものは、自分で設定画面を書き換える必要があるなど、導入にスキルが求められます。

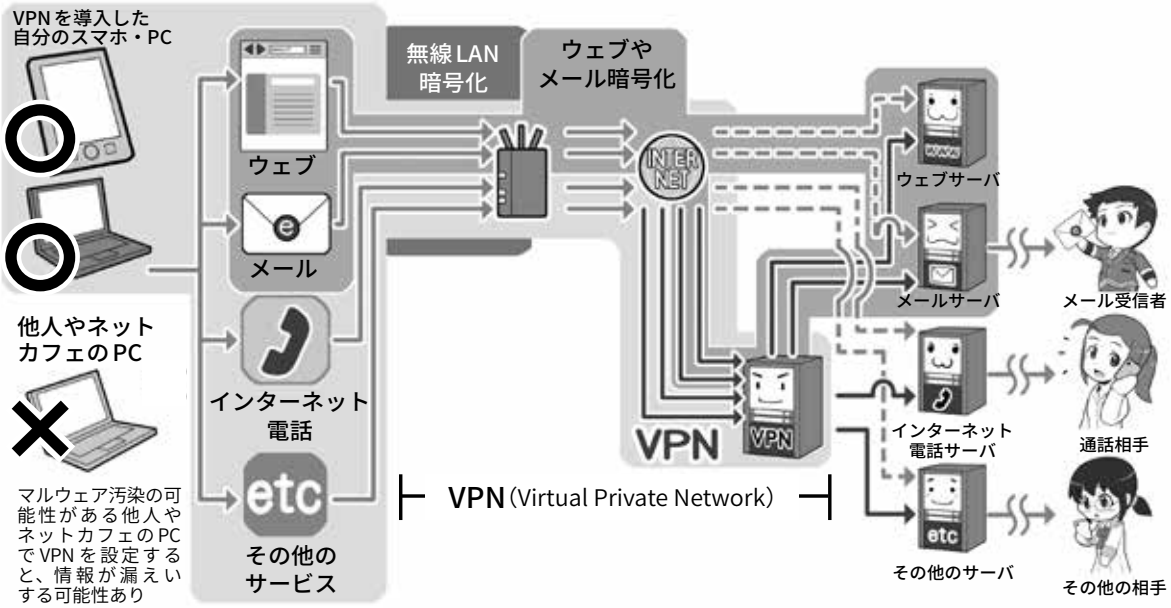
また、利用するVPNのサービスによっては、誤ったアクセスポイントに誘導されたり、VPN接続が切れると暗号化されていない状態で通信を継続したりしてしまうなど、2018年の秋の時点でも、まだ決定的なものがありません。

どうしてもVPNを利用したい場合は、そういった問題点に関する各VPNサービスのテスト結果を公開しているサイトがあるので、そこできちんと問題点に対応しているVPNサービスを探し、導入するようにしましょう。

なお、VPNが通信を暗号化するのは出口サーバまでなので、その先の通信の暗号化は行われない点は注意しましょう。

様々な場所から安全なアクセスを可能にするVPN

①詳細なVPNのイメージ



VPNを図で説明すると、上のように入り組んでよく分からなくなってしまうので、簡単な図を下に用意しました。くじけそうな方はまず下をご覧下さい。上の図では左から右に向かって通信を行う場合、無線LANの暗号化、ウェブやメールの暗号化、VPNとそれぞれ暗号化の守備範囲があることが分かります。無線LANの暗号化は範囲が短く、ウェブやメールの暗号化は文字通り用途が限定されます。VPNは全ての通信を暗号化し、かつ広範囲にカバーしてくれます。しかしその範囲は利用者の機器から安全と思われる場所に設定された出口サーバまで限定なので、その先の目的のサーバまでは暗号化されない区間が残ります。VPNさえあれば全て安全というわけではないのです。

②簡単なVPNのイメージ

VPNを簡単なイメージで説明するとこの図のようになります。スタート地点(自分のパソコンやスマホの中)でデータを護送車に乗せて全部まとめて暗号化、危険地帯を突破し、信頼がおける安全な場所(出口サーバ)に着いたらデータを解放します。VPNは暗号化されていない無線LANを利用するのにも役に立ちますし、危険性があると思われる通信回線の盗聴、検閲や監視がある国からの安全な通信にも役立ちます。また災害時などに利便性を優先して提供される、暗号化なしの公衆無線LANを利用する場合でも役に立ちます。ただし、そもそもだれが運営しているのかよく分からないような無線LANアクセスポイントには、多分に攻撃者が潜んでいる可能性があるので、攻撃の手段は予測できず、VPNを使えたとしても積極的な利用は推奨しません。

3 ウェブを安全に利用する、暗号化で守る

1 無線LANの暗号化とVPNの守備範囲

インターネット通信の基本は「平文」での送受信です。ウェブサイトを見るときに、ウェブブラウザ上部の、アドレスもしくはURLと呼ばれるウェブサイトの住所を入れる欄がhttp://で始まっている、「保護されていない通信」と表示される、先頭に○で囲まれたiとある場合、その通信は平文で送受信されていることを示しています。

平文での通信は、通信の途中、攻撃者によって、いつでも盗聴されたり改ざんされたりして、全てもしくは一部が偽の情報に書き換えられている可能性があります。そうさせないためにはウェブサーバとの通信の暗号化が必要になります。

前項では、通信の暗号化を行うために、無線LAN通信の暗号化と、VPNが登場しました。

利用者が目的のウェブサーバなどと通信するとき、無線LAN通信の暗号化では、利用者の機器から無線LANアクセスポイントまでの、全ての通信が暗号化されます。一方、無線LANアクセスポイントから、目的のウェブサーバまでの通信は、無線LAN通信ではないので暗号化されません。

VPNでは利用者の機器からインターネット上の安全な場所にある出口サーバまで、無線であっても有線であっても全ての通信を暗号化します。しかし、出口サーバから目的のウェブサーバまでの通信は暗号化してくれません。

それぞれの守備範囲があり、攻撃できるポイントが残るわけです。

では無線LANやVPNでは暗号化してくれない区間の通信の暗号化や、前項にあった、何らかの理由で無線LAN通信の暗号化やVPNが使えない状況で安全に通信をしたい場合、どのような対処方法があるのでしょうか。

代表的なものとしては、ウェブサイト閲覧やメール送受信、それぞれ目的の通信に限定して、利用者のそれぞれのソフトやアプリから目的のサーバまでを暗号化するやり方があります。

2 全ての通信と、その一部であるウェブの通信

無線LAN通信の暗号化とVPNでは、暗号化対象を「全ての通信」と書きましたが、ウェブサイトを閲覧するための通信の暗号化は、その「全ての通信」の中の一部分「ウェブサイト閲覧に関する通信」に限定した暗号化になります。

通信にはウェブサイト閲覧やメール送受信の他に、インターネット電話、一部のアプリや特殊な機器など、目的などに応じて多様な通信が存在します。

例えるなら、全ての通信は「テレビの電波放送」という大きなくくり。これに対してウェブサイトを閲覧する通信は、その中の一つのチャンネルにあたります。そして通信には様々なチャンネルが存在するわけです。

インターネットの通信ではこのチャンネルにあたるものを「ポート」と呼び、ウェブサイトの閲覧の通信は、通常「ポート80」「80番ポート」という名称で、文字通り80番のポートを使って通信をします。

80番ポートを使って送受信される通信は、基本的に暗号化されていない平文で、仮にこの状態でIDやパスワード、個人情報などを送信すると、通信を盗聴している攻撃者は特に何の工作をしなくても情報を盗むことができます。また、情報が送受信ともに改ざんされ、偽の情報で取引などをさせられる可能性もあるのです。

それを避けるため、ウェブサイトを安全に閲覧する通信の暗号化が普及しました。それが「SSL(Secure Sockets Layer)/TLS(Transport Layer Security)」(以下SSL/TLS)という暗号化通信です。

通常のウェブサイト閲覧では、URLが「http://」から始まるのに対して、SSL/TLSの通信では「https://」で始まります。後ろに追加されたsは「secure=安全な」の意味のsなのです。

3 httpsで始まる暗号化通信にはどんなものがあるか

先ほどのチャンネルの話に戻ると、httpsは通常ポート443を使用します。つまりテレビのチャン

ネルを443にあわせたら、放送にはモザイクがかかっていて、有料放送契約者だけがモザイクを解除して見ることができる、というイメージです。

https://から始めるサイトにアクセスすると、通信相手が誰であるかが後ほど説明する電子証明書によって証明され、暗号化通信が始まり、ブラウザのURL欄に暗号化を示す鍵マークが表示されます。

この状態になると、「一応は」、IDやパスワードなどを入力しても大丈夫で、「表示される情報も改ざんされていない」ということになります。しかしなぜ「一応は」かというと、鍵マークが表示されていても安全とは限らないからです。

httpsによる通信を行うためには、まず、httpsで通信するサーバを作りたい運営者が、認証局という機関に、自分の会社の情報とサーバのドメイン名を提示して、暗号化通信を行うための電子証明書の発行を求めます。

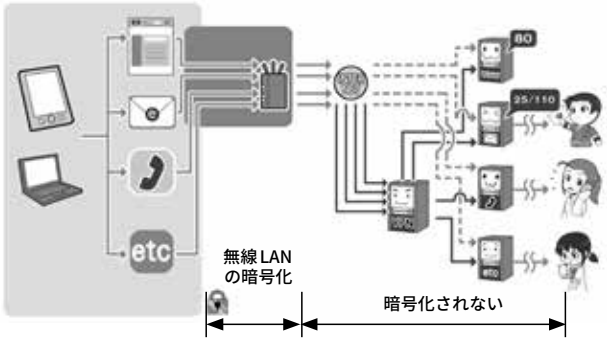
認証局は、審査の上、その会社が実在することを確認できれば、「SSL証明書(SSLサーバ証明書)」という電子証明書を発行します。

「SSL証明書」を取得した会社は、httpsで通信するサーバに「SSL証明書」を設定し、利用者がアクセスしたときに、その「SSL証明書」によって、該当のドメインの運営者であることが証明されることで、安全な暗号化通信が行えるようになります。

しかし、認証局の中には、簡単なオンラインでの確認だけで機械的に「SSL証明書」を発行し、会社名を証明書に記載しないところもあります。そのような「SSL証明書」は誰でも取得出来てしまいます。

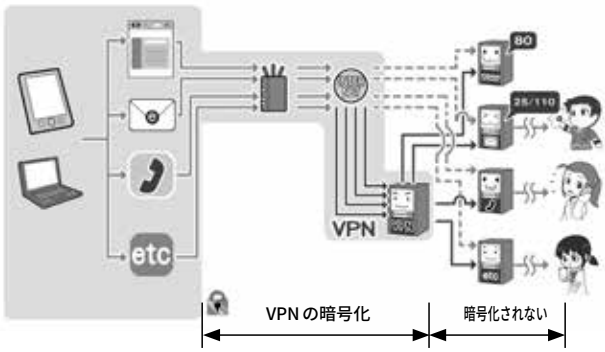
それぞれの暗号化の守備範囲

①無線LANの暗号化



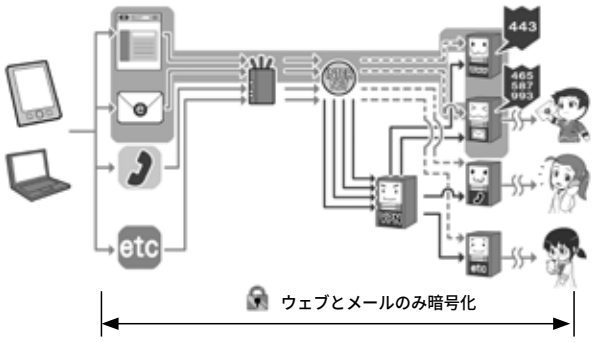
無線LANの暗号化は、利用者の機器から無線LANアクセスポイントまでの全ての通信を暗号化します。

②VPNによる暗号化



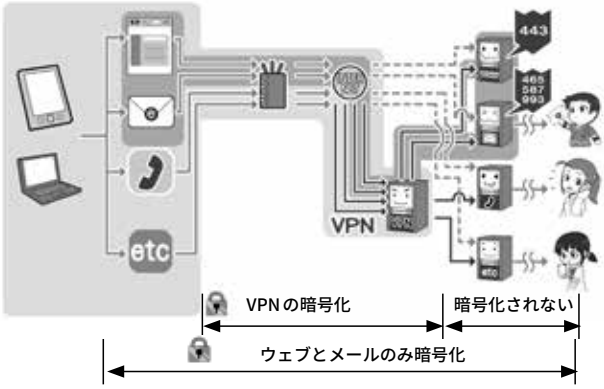
VPNは利用者の機器から、安全とされる「出口サーバ」までの区間で、全ての通信を暗号化します。

③ウェブ、メールの暗号化



ウェブやメールの暗号化は、利用者のブラウザやメールソフトから目的のサーバまでの区間で、ウェブとメールの通信だけを暗号化します。

④VPN＋ウェブメールの暗号化



ウェブやメールの暗号化とVPNを組み合わせて利用する事ももちろん可能です。この場合暗号化される通信範囲は広くなります。

攻撃者はそういった審査の甘い認証局を使って、詐欺サイトのための「SSL証明書」を取得して、httpsからはじまるURLの詐欺サイトを立ち上げます。

そして利用者に、「あ、httpsだから大丈夫」と油断させ、パスワードやクレジットカード番号を盗むという事例が発生するようになったのです。

4 より厳格な審査の「EV-SSL証明書」

そういった問題に直面して、より審査を厳しくした「EV-SSL証明書」が登場しました。

「EV-SSL証明書」の審査では、証明書を発行する認証局も、外部の監査により基準を満たした者に限定して発行権限が与えられ、証明書を受ける側の会社も、法的な存在の証明や、管理責任者や役員など複数人への聴取など、従来よりも厳格に審査が行われます。

これにより、「法的・物理的実在性」と「正当性」、結果としての「安全性」などが担保され、詐欺サイトなどの排除が行えるようになったわけです。

もちろん、「EV-SSL証明書」ではない、「SSL証明書」を使う全てのサイトが詐欺サイトなわけではありません。しかし安全にIDやパスワード、個人情報を入力したり、オンラインショッピングやインターネットバンキングを行ったりする場合は、この「EV-SSL証明書」を持っているサイトを利用する方が、より安心できるといえるでしょう。それは顧客を守ろうという企業のセキュリティ意識の高さの表れでもあるからです。

5 「EV-SSL証明書」を持つサイトを見分ける方法

ウェブブラウザが暗号化通信を行っているかどうかは、URLの欄がhttps://で始まったり鍵マークが付いていたりすることで見分けられますが、では「SSL証明書」と「EV-SSL証明書」の差はどうやって見分けるのでしょう。

「EV-SSL証明書」に対応したパソコンのブラウザでは、該当のサイトに接続すると、https://や鍵マークに加えてURLの欄が緑色になり、URL欄にその「EV-SSL証明書」を取得した会社の名前が表示されます。

さらに、鍵マークをクリックすると、証明書を取得した会社名と発行した認証局名などが表示されますが、「EV-SSL証明書」に対応した一部のブラウザでは、証明書を取得した会社の大まかな所在地まで表示されることもあります。これならば「日本の会社のサイトのはずなのに、所在地が海外になっていておかしい」といったことをチェックすることもできます。

スマホでは、ブラウザによってはURLの表示欄が短いので、暗号化通信をするサイトでもhttps://の表示を行わず、鍵マークのありなしだけで暗号化の有無を表示している場合もあります。

また「SSL証明書」と「EV-SSL証明書」の区別は、URL欄が企業名表示になっているかや、URL欄表示が緑になっているかどうかで見分けるようになっています。ただ、証明書の内容を表示しても会社の所在地が表示されなかったり、そもそも証明書の表示が行えなかったりするものもあるので、パソコンのようには「EV-SSL証明書であることの確認」を行いづらいかもしれません。

6 有効期限が切れた証明書は拒否する

電子証明書には有効期限があり、失効したものは安全ではないと考えるべきです。

有効期限に問題があるなどの理由で、ウェブブラウザやセキュリティソフトが警告を発する場合、そのウェブサイトには接続しないようにしましょう。

きちんとセキュリティに対して必要な手続を行っている会社ならば、証明書の失効前に更新の処理を行い、新しい証明書に差し替えるはずです。

それを行わない企業はセキュリティに対して必要な措置をしていないと判断し、従ってそのサイトは安全に利用できないと考えるべきでしょう。

7 他にも証明書に関する警告が出るサイトは接続しない

証明書が失効している警告以外にも、証明書に関する警告が表示される場合があります。

詳しく分類すると多岐にわたるので、全ては記述しませんが、以下のような例が該当します。

1. 証明書の使い方を間違っている場合
2. 証明書の署名アルゴリズムに問題がある場合
3. 証明書を発行した認証局に何らかの問題がある場合

4.「オレオレ詐欺」のように認証局でないのに認証局と偽って証明書を発行し、それを使っている場合（通称：オレオレ証明書）

いずれの場合も「安全ではない通信」の元凶となります。

証明書の有効期限の問題と同様に、ウェブブラウザやセキュリティソフトが「証明書に関する警告」を発した場合、そのウェブサイトとの通信は安全でないと判断し、利用しないようにしましょう。

さて、ウェブサイトを安全に利用するには、通信面の他にも気をつけるべきポイントがあります。

他のセクションとも重複しますが、ウェブを使うというくくりで少し触れておきましょう。

8 ウェブサービスのログインは二段階認証などを使う

ウェブサービスを安全に利用するには通信の暗号化も大切ですが、ウェブサービスにログインするIDやパスワードの管理と運用も大切です。

通信を暗号化してもスマホやパソコンがマルウェアに感染してしまえば、通信する前の段階で情報が盗まれてしまいますし、ウェブサービスのIDやパスワードが盗まれると、攻撃者がウェブサービスに勝手にログインして、悪さをすることができるからです。

これを避けるため22ページでも触れたように、ウェブサービスへのログインは、二段階認証や多要素認証、使い捨てパスワード（ワンタイムパスワード）を利用して、仮にパスワードが盗まれた場合で

httpsの暗号化通信で情報を守る

個人情報の入力は基本的には……

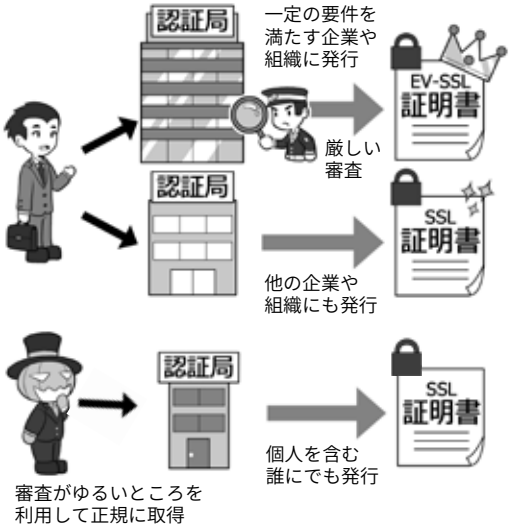
ダメ ✕ 暗号化なし（httpと表示される）

注意 △ SSL（暗号化あり）（httpsと表示される）

OK ○ EV-SSL（暗号化あり）（httpsと表示され、緑色の文字で運営主体名が表示される）

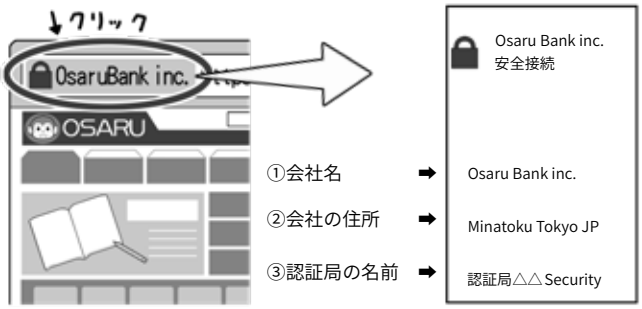
個人情報の入力をする場合、暗号化は必須となります。厳しい認証局の審査を伴うEV-SSLのサイトを利用する場合のみ、安全であると判断しましょう。特にお金関連のサイトはEV-SSLの方がより一層推奨されます。

攻撃者が不正に取得した証明書に注意



SSL証明書には、サイトを運営する企業や組織が実在することを認証局が審査して証明してくれるものと、その機能がないものがあります。SSL証明書は元々、暗号化通信に使うためのもの（中間者攻撃を防ぐために必要）ですので、実在証明がなくても正規の証明書です。これは個人でも取得できるので、攻撃者が攻撃サイト用に取得することもあります。EV-SSLのhttpsサイトはどこの組織が運営しているか確認できますが、ただのhttpsサイトは誰が運営しているかわからないので、要注意です。

証明書の内容をチェックする



パソコンなどの場合は簡単に、証明書の内容をチェックすることが出来ます。会社名や認証局の名前、EV-SSLに対応したブラウザならば会社の大まかな住所も表示されます。また緑の帯や会社名表示はEV-SSL証明書の証でもあるので覚えておきましょう。

も攻撃者が勝手にログインできないようにし、あるいは不正なログインがあった場合にログイン通知を受けとれるものを利用して、これを即座に察知できたりするようにしましょう。

また近年、ウェブサービスへのログインに関して、そもそも「ネットを通じて認証のためにパスワードを送信する」という構造そのものが危険だという考え方も出てきています。パスワードなどによる認証は手元の機器の中で行い、パスワードそのものは送信せず、「本人であることを確認できた」という認証情報だけをサーバに送って、ウェブサービスを利用可能にする、そういった方法も一部で採用が始まっています。

今後の動向に注目して必要に応じて採用するようにしましょう。

9 二段階認証を破る「中間者攻撃」

ウェブサービスの安全な利用のためには、二段階認証や多要素認証を利用するべきと第1章で書きましたが、この方法にも限界があります。

例えば、パソコンから二段階認証に対応したインターネットバンキングを利用する際、銀行のサイトにIDとパスワードでログインするときや送金操作時に、使い捨てのパスワードがスマホに送られて来て、これをパソコンに入力するとしましょう。

このとき、銀行のサイトだと思っていたものが偽サイトだとしたらどうなるでしょう。攻撃者が偽サイトに入力された内容を本物のサイトに中継して、画面の内容をリアルタイムに書き換えていたとしても、利用者は気付かないまま送金の操作をしてしまうでしょう。

さらに攻撃者が通信を中継しながら、送金先を別の銀行口座に差し替えていたら、利用者は自分の操作で知らない銀行口座に送金することになってしまいます。

このような、通信経路の中間で双方の通信を中継しながら裏をかく手口は「中間者攻撃」と呼ばれています。二段階認証ではこの中間者攻撃を防ぐことができません。

結局、偽サイトによる攻撃は、利用者自身で自分がどこのサイトを見ているのか、注意して確認する以外に対策はありません。では、どのように注意すればよいのでしょうか。

本物のサイトが前ページの図にあるようにEV-SSL証明書を使っている場合には、パスワードを入力する直前に、ブラウザ画面のアドレスバーに緑色で自分の利用している会社名や組織名が表示されていることを確認します。

しかし、自分が普段利用しているサイトが元々EV-SSL証明書を使っていないところだと、この方法では確認できません。その場合は、アドレスバーのURLを見て自分が知っているサイトとドメイン名が同じかを確認するしかありません。

「ドメイン名」とは、例えば「https://www.example.co.jp/foo/bar.html」のうち「example.co.jp」の部分のことです。ですが、これを確認するのも簡単ではなく、攻撃者は利用者が見間違うのを狙って、「https://www.example.co.jp.foo/bar.html」というURLで偽サイトをつくることがあります。このURLのドメイン名は「co.jp.foo」であり、全く違うところなのですが、「.」と「/」の違いを見抜かないと気がつきにくいのです。

あるいはアルファベットに似た別の言語の文字を使って偽装する場合もあります。

最近のウェブブラウザでは、URL中のドメイン名部分がどこなのかを強調表示してくれるものや、アドレスバーにドメイン名部分しか表示しないようにしているブラウザもあります（Safariなど）ので、そういうブラウザでは見分けがつきやすいでしょう。

しかし、アドレスバーでサイトを見分けるには、普段から自分の使うサイトのドメイン名を覚えておく必要がありますが、なかにはとても覚えにくいドメイン名で運営されているところもあります。

ドメイン名を覚えられそうにないときは、ブラウザのブックマーク機能を使います。普段利用するサイトの「https」で始まるURLの画面をブックマークに登録しておき、その後はブックマークからそのサイトにアクセスするようにすれば、間違って偽サイトに行ってしまうことはありません。

このほかには、どういったときに偽サイトにアクセスしてしまうのでしょうか。ひとつには、80ページで紹介する「怪しいメール」やSNSのリンクでアクセスを誘導されるものがあります。フィッシング詐欺とも呼ばれる手口で、偽サイトにアクセスさせてIDとパスワードを入力させようとします。

もうひとつは、公衆無線LANを使うときです。安全でないアクセスポイント（69ページの図で接続が×や△になっているもの）に接続している場合には、通信経路が

偽装され、攻撃者によって偽サイトに誘導される危険があるので、利用は避けるようにしましょう。

10 ウェブを使ったサイバー攻撃に対応する

スマホやパソコンがマルウェアに感染したことによる、パスワードなどの情報流出。事態が起こるまでには、マルウェアに感染する経路が必ずあり、その経路がウェブブラウザであることもよくあるケースです。最近ではウェブブラウザでサイトを「見る」だけで感染させる攻撃も発生しています。

攻撃者があなたに、マルウェアを仕込んだウェブサイトのURLをメールやアプリのメッセージで送り、あなたがリンクをクリックして悪意のあるウェブサイトを見てしまう場合（標的型メール攻撃）や、あなたの行動パターンを調べて、よくアクセスするウェブサイトに、事前にマルウェアを仕込んでおく場合（水飲み場攻撃）、さらにわざわざお金を払ってマルウェアが含まれた動画広告などを目的のサイトに出すという方法もあります（マルバタイジング）。攻撃は不特定多数を対象に行われる場合もあります。とくに広告を使うものは、攻撃者は広告費以上のお金を稼がなければならず、攻撃は無差別に不特定多数に対して行われ、被害者も大変多くなります。

この「見る」だけで感染するサイバー攻撃は、未知のセキュリティホールが突然狙われる場合も有るのですが、メーカーなどがセキュリティホールを公表し、そのソフトやアプリを修正するまでの「穴が開いたまま」の期間を狙って攻撃する「ゼロデイ攻撃」で行われる場合も多くあります。

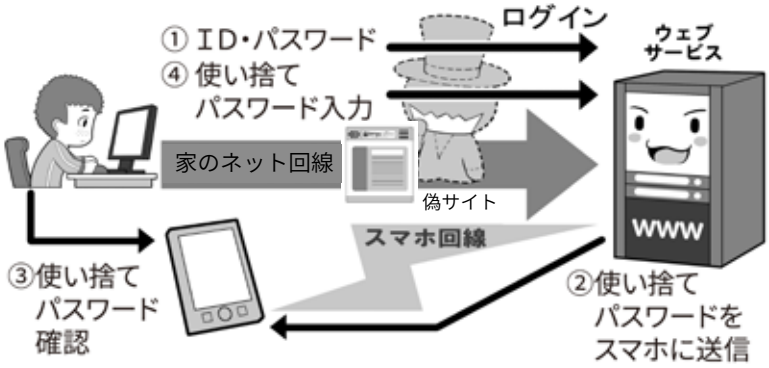
また、見るだけでなく、あなたの心の隙を突き、巧妙に誘導して「自らクリックやインストールさせる」といった攻撃もあり、この場合はセキュリティホールがなくても攻撃ができてしまいます。

なお、セキュリティホールを狙ったサイバー攻撃に対する基本の対処方法は、システムの状態を最新に保つことですが、セキュリティホールの修正など対応が間に合わない場合は、あなたが意識して攻撃を避けるほか対処はありません。

さらに、利用者を巧妙にだましシステムのセキュリティ設定を変えさせて、自らアプリなどをインストールさせる攻撃に至っては、誰にでもある人間の心の隙を、自分が理解しなければ防げません。

そういった場合に備えて、「不審なメール文中のリンクは開かない」「何かをインストールさせようとするものは拒否する」「ニュースなど情報を常時ウォッチして、特定のサイトやアプリを使った攻撃が判明したらそのサイトやアプリに近づかない」「SNSやウェブサービスの動画や広告は自動再生しないように設定する」などの防御策を積み上げて守りましょう。

間に入ってなりすます中間者攻撃



中間者攻撃では利用者とサーバの間に攻撃者の偽サイトが入ります。攻撃を避けるための二段階認証を使っていても、２つの認証が同じ経路使って行われる場合、情報をすり替えられたまま意味をなさないこともあります。

ウェブを使ったサイバー攻撃の例

4 メールを安全に利用する、暗号化で守る

1 メールにおける暗号化

次はメールを安全に使う方法についてです。

「ウェブを安全に利用する」の項目で書いたとおり、メールの送受信も全ての通信の中の一部です。

そして、メールの内容を盗聴されないためには、暗号化の区間が限定される無線LANの暗号化やVPNではなく、メールが送受信中常に暗号化していることが大切です。特にメールはウェブと異なり、殆どが私的な内容になるからです。

メールの送受信では、使用するスマホやパソコンなどのソフトやアプリから、メールサーバまで、送信と受信に別々の通信チャンネルを利用します。

2 送信の暗号化と受信の暗号化

メールは、昔はどちらも暗号化されていない平文で通信が行われており、送信を行うSMTPと呼ばれる通信が25番ポート、受信のうちPOPと呼ばれる通信が110番ポート、IMAPと呼ばれる通信が143番ポートを利用していました。

それが、後になって、平文でのメール送信による盗聴の危険性を回避するため、465番ポートを使って、SSL/TLSによる暗号化を組み合わせてSMTP over SSL(SMTPs)が普及しました。これと併せて、メール受信側の暗号化も普及し、POPがPOP over SSL(POPs：995番ポート)、IMAPがIMAP over SSL(IMAPs：993番ポート)で提供されるようになりました。

現在では多くのプロバイダーメール、携帯電話キャリアメール、フリーメールサービスで、この暗号化によるメール送受信サービスが基本になっています。

設定が「面倒くさくない」ようにスマホなどでは工夫されていて気付きませんが、最近では特に意識しなくても自動的にこの暗号化で通信を行うようになっています。

一方、パソコンのメールソフトでは依然として手動での設定が必要な場合もあるので、パソコンメールを使っている人は一度、自分のメールソフトでメール送受信サーバの設定がきちんと上記の暗号化ポートや類似の方式を利用しているか、もしくはSSL/TLSなどの文字がある設定になっているかをチェックしてみてください。

特に、パソコンで古くからメールを利用し、メールソフトの設定を全然いじっていない場合、暗号化されていない昔の設定のままになっていることもあります。

多くのメールアカウントを持っている人は、一度メールアカウントの棚卸(たなおろし)をし、暗号化されていない設定があれば、暗号化方式に切り替え、暗号化方式がないものしか提供されていないメールサービスは安全でないと考え、安全なメールサービスに乗り換えるようにしましょう。

3 メールにおける暗号化の守備範囲

先ほども少し触れましたが、メール送受信の暗号化は、スマホやパソコンのソフトやアプリなどから、送受信用のメールサーバまでの間を暗号化します。

しかし、目的のウェブサイトの情報を直接閲覧するのと異なり、メールの送受信は自分が利用しているメールサーバから相手のメールサーバまで、複数の中継メールサーバによるバケツリレーのような受け渡しによる送受信が行われる場合があります。

遠方の誰かに手紙を送ると、複数の郵便局を転送された後に、相手に配達されるのに似ています。

そして残念ながら、このバケツリレー中の送信はいまだ平文で行われていることもあるのです。

自分や相手が契約しているメールサーバまでの経路をそれぞれ暗号化しても、その先のバケツリレーの区間で平文での送信が行われていれば、内容を盗聴されてしまったり、改ざんされてしまったりする可能性が残ります。

とはいえ、この転送中の通信の暗号化は、大手メールサービス提供会社の努力により進み、改善されつつあります。

ただ、いくら途中の経路を暗号化しても、それぞれのメールサーバで一旦暗号が解かれますので、バケツリレーの途中のメールサーバに盗聴しようとする者がいたら、

内容を読まれてしまいます。

現代でも外国に郵便を送ると、国や地域によっては手紙が開封されて中を見られてしまったりすることがあり得るのに似ています。通信の秘密が保障されるかは国や地域によるからです。

それを避けたい場合は、安全な国内だけで手紙をやり取りするように、メール送受信を暗号化したサービスの中だけでメールをやり取りする方法もあります。

4 メール本文の暗号化

ところで、メールの暗号化には、送受信の暗号化ではなく、メールの本文そのものを暗号化する手段もあります。

これには、「S/MIME」という方法と「PGP」という方法があります。

これらの方法を使うと、メールのバケツリレーの途中で攻撃者が盗み読もうとしても、本文が暗号化されているため読めません。

メール本文の暗号化には、公開鍵暗号方式の「公開鍵」と「秘密鍵」を使います。この方法を使うときは、事前の準備として、自分用の秘密鍵と公開鍵を作成しておく必要があるのです。

相手が自分の「公開鍵」で暗号化したメールを、受信して復号するには自分の「秘密鍵」を使い、相手にメールを送る際は相手の「公開鍵」で暗号化して、相手は自分の「秘密鍵」で復号して読むのです。

そしてこれを成立させるためには、送り先相手の公開鍵を安全かつ確実な方法で入手しておく必要があります。

特にS/MIMEを使う場合は、お金を払い認証局が発行する証明書

メールの送受信は暗号化されているか

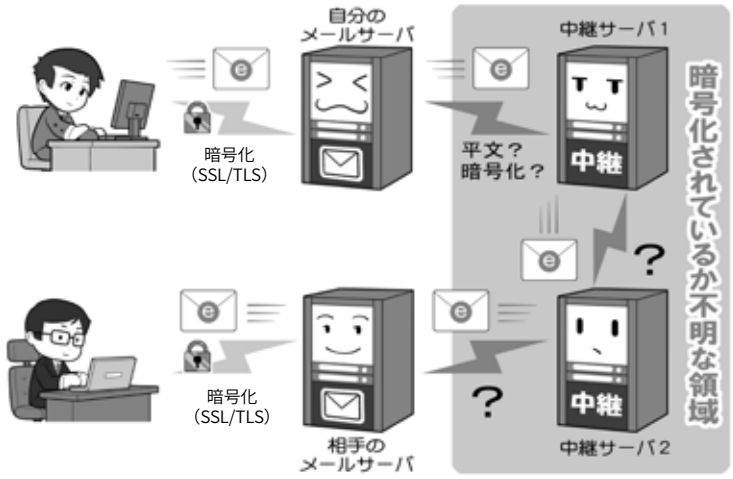
メールソフトやアプリが暗号(SSL/TLS)利用することになっているか？

メールソフトの例

メールアプリの例

メールアカウントが設定された状態で、メールソフトやメールアプリの、サーバの詳細設定画面を開き、暗号化を利用する設定になっているかを確認します。「受信ポート587や993の使用」「送信ポート465の使用」「パラメータとしてSSL使用がON」などになっているかがチェックポイントです。これらは暗号化通信が設定されている目印です。

しかしSSLの通信は自分のサーバまで



メールの暗号化設定は、利用者の機器から契約しているサーバまでの区間のみの暗号化が担保され、メールが送信相手の利用しているサーバに到達するまで、平文で送信される区間がある可能性が残ります。

暗号化している同じサービスを利用する

メールを安全に利用する一つの方法としては、暗号化通信を採用した一つのメールサービスを、送信相手とともに利用する方法があります。通信の秘密が守られる国内だけで手紙をやり取りするのと同じ概念です。

を入手し、自分の公開鍵の正当性を証明する必要があります。事前の準備も必要で、相手も同じ事をする必要があるので負担にもなります。

なお、メールの本文を暗号化しても、メールのヘッダ部分、つまり、件名部分や、宛先と差出人のアドレスなどは、平文で送られることになるので、注意が必要です。

S/MIME や PGP を使うと、盗聴を防ぐことができるだけでなく、仮にメールの本文を改ざんされても、受信者側で改ざんされていないか調べることができるようになります。また、他人がなりすました偽のメールではないかを確認することもできます。これを実現する機能を「デジタル署名」と呼びます。

上記のとおり S/MIME は大変優れた機能なのですが、事前の準備に手間がかかり、また大手のメールソフトが対応してないものもあって、残念ながらあまり利用されていません。詳しい方法の説明はここでは省略しますので、各自で調べてみましょう。

なお、利用者ではなくサービス側で成りすましを防ぐものとして、認証チェックをする SPF、DKIM、そしてこれに引っかかった場合の対処を決める DMARC などがあります。これは送信者の書面上のメールアドレスと実際にメールが発信されたサーバのドメインをつきあわせて、合っていなければメールを受け取らないなどの対応ができるものです。これらを採用したサービスがあれば、積極的に利用を検討しても良いでしょう。それが安全な技術の普及への一助になります。

5 怪しいメールとはなにか

メールを安全に使うために、メールを使ったサイバー攻撃にも触れておきましょう。

サイバーセキュリティの標語などではよく「怪しいメールを不用意に開かないように」といったものを見ます。

これは「標的型メール攻撃」に代表されるフィッシング（詐欺）メールを使った攻撃に関し注意喚起しています。この場合、攻撃者が特定の個人を狙って仕事上のメールを装い、マルウェアの添付や、マルウェアを仕込んだウェブサイトの URL を送り付けるものです。相手が添付ファイルやリンクをうかつに開くと「ゼロデイ攻撃」などを受け、不正なファイルをインストールされたり、パソコンを乗っ取られたりするのです。

実際には、特定の個人を狙った標的型攻撃だけでなく、不特定多数を狙った「スパムメール」でも同様の手口が使われます。誰でも攻撃対象になりうるわけです。

これらの手口は、昨今のセキュリティ環境の向上で「開くだけ」「見るだけ」で感染させることが難しくなったこともあり、少なくとも相手に「感染させるためになにがしかの行動」を起こさせることで感染率を上げています。それが偽装したマルウェアをインストールさせたり、偽装広告をクリックさせたりする方法なのです。

こういった攻撃を避け、マルウェアなどに感染しないようにするためには、まず**「送られてきたメールの文面を見るだけで完結しないものは、全て『怪しいメール』として警戒する」**ことが必要です。

送られてきたメールの差出人が知り合いでも、実は全く違う所から送られて来ていたり、あるいは間違いなく知っている相手から送られてきたメールでも、実は相手のパソコンが乗っ取られていて、そのパソコンから送ってきたりしていることもあります。知り合いからのメールだから安全とはいえないと覚えて下さい。

少なくとも、送られてくることが事前に知らされていない添付ファイルや、「今すぐ確認を！」と言ったように、緊急に文中の URL や添付ファイルを開くことを要求するメールなどは、警戒する必要があります。次項目の偽装添付ファイルにも気をつけてください。

発信者に、送信されてきたメールについて「メールではなく電話などの別通信経路」で問合せをしたり、銀行・行政サービス・インターネットプロバイダ・ウェブサービスなどから送られてきた場合は、文中の URL を直接開くのではなく、公式のウェブサイトに行き、本当に該当の情報が掲載されているか確認し、もし個人情報に関わる問題であれば、ウェブサービス側に電話で問い合わせたりするなどの対応をしましょう。

6 マルウェア入りの添付ファイルに気をつける

「怪しいメール」の一つのパターンであるマルウェア入りの添付ファイルとはどういったものなのでしょう。

例を挙げると、業務を装ったメールに「報告書」などの一見文書ファイルなどに見える形で添付されるものや、ZIP ファイルというファ

イルを圧縮した形で添付されてくる場合などがあります。

そして実際は、こういったファイルは純粋な文書などではなく、何らかのマルウェアを含んだファイルであり、あなたがファイルをクリックして開こうとすると感染する仕掛けになっています。

通常パソコンではファイルはアイコンで表示され、アイコンには文書ファイルであれば文書ファイルを示す画像がつけられます。

しかしこのファイルのアイコンというものは、簡単に変更可能であり、文書ファイルに見せかけたマルウェアを作ることも可能で、事実そういった手法が使われます。

またファイル名は、文書ファイルであれば「文書名.doc」、ZIPファイルであれば「ファイル名.zip」というように、文書の名前の後ろに「拡張子」といって、そのファイルがどういった種類のファイルであるかを示す文字列が付け加えられます。（表示されていない場合は、ファイル拡張子を表示する設定を行ってください）

マルウェアが実行形式ファイル（プログラム）の場合、拡張子は「.exe」となり、exeと表示されれば「実行形式ファイルが送られてくるのはおかしい」と気付く人もいます。

これを隠すために攻撃者はファイルの名前を「houkokusyo.doc.....exe」というような長いファイル名にして、後半が省略され画面上で見えないように細工し、「houkokusyo.doc...」の部分だけが表示されるようにして、その上でアイコンを偽装するといったことを行います。

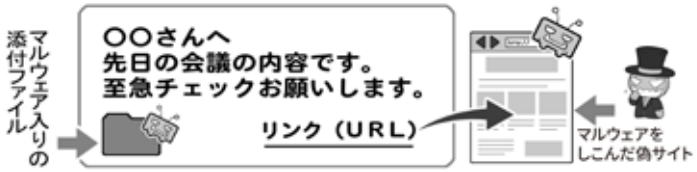
そういった手法に引っかからな

ウェブメールの送受信は暗号化されているか

ウェブブラウザでメールを送受信する場合は、ウェブブラウザの暗号化のチェック項目を参考にしてください。一般的には「SSL証明書」を持ち、暗号化通信を示す鍵マークがついているか、「EV-SSL証明書」を持ち、URLの欄が鍵つきで緑色で、サービス提供主体の名称が表示されているかで、暗号化されているかどうかなどでわかります。確認をした上で「ログインパスワード」を入力します

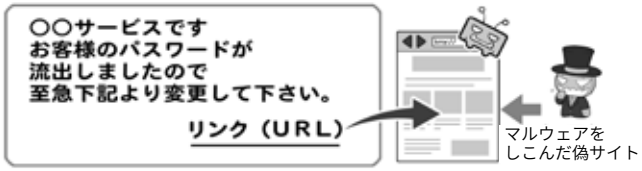
怪しいメールとはなにか

①仕事のメールを装う



サイバー攻撃に使われる怪しいメールとは、まず「見ただけでは終わらない」メールです。リンクをクリックさせたり、ファイルを開かせたり、何かをインストールさせようとしたりします。

②銀行、カード会社、ECサイト、プロバイダ関係を装うメール



また自分が利用しているウェブサービスの名称で、緊急にどこかのサイトを見させるのも、よく使われる手口です。

本当の仕事仲間のメールでも攻撃は来る

自分の知り合いや仕事仲間からのメールと思っても安心は出来ません。名前を名乗っているだけでなく、攻撃者がその人のパソコンを乗っ取って、知り合いや仕事仲間のメールソフトから攻撃を仕掛けてくることもあるからです。

いためにも、繰り返しになりますが、「送られてきたメールの文面を見るだけで完結せず、何か行動させようとするメール」は、全て「怪しいメール」として警戒することを心がけてください。

またこういった攻撃手法は常にブラッシュアップされ進化していくので、定期的に検索エンジンやニュースなどで攻撃の手口を検索をして、最新の攻撃手法の情報を入手してください。

セキュリティソフトメーカーやフィッシング対策協議会、専門機関、識者などのSNSアカウントをフォローすると、最新の情報を入手しやすくなります。

7 メールアドレスのウェブサービスなどからの流出

「標的型メール」や「スパムメール」による攻撃には、送り先となるメールアドレスが必要です。

メールアドレスを無差別に生成し送り付ける方法もありますが、ウェブサービスなどから流出した大量のメールアドレスを使って送られる場合も多くあります。

また会社内で標的型メールによって感染した端末があると、そこから社内のメールアドレスが流出して、さらなる標的となる場合もあります。

こういった情報は、攻撃者によって直接、攻撃メールの送付先として使われるだけではなく、インターネットの闇サイトで名簿として売買されることもあります。

攻撃のメールが送られてきたらもちろん警戒するべきですが、それ以前にもできることがあります。

セキュリティ識者のトロイ・ハント氏が運営する、「Have I been pwned」というサイトなどでは、メールアドレスやパスワードなどの流出情報を、全てではないものの検索できるようになっており、そこで自分の情報が流出した形跡がないかを、ある程度チェックできます。

では流出が判明した場合、速やかに対処するのは当然として、流出に備えてメールアドレスにどのような工夫が出来るのでしょうか。

8 流出・スパム対策としての、変更可能メールアドレスの利用

解決策としては、親しい人とやり取りをする大事なメールアドレスと、ウェブサービスや通信販売サイトなどに登録するメールアドレスを別にし、後者にはメールアドレスを気軽に変更したり、複数のメールアドレスをもらえたりするものを使う方法があります。

これは「メールのサブアドレス」や「使い捨てメールアドレス」「捨てメアド」と呼ばれるもので、ウェブサービスなどからメールアドレスが流出してしまっても、すぐに変更するかメールアドレスごと削除して、攻撃メールが送られてくるのを避けることができます。

思い入れがあり変えられないアドレスと違い、ウェブサービスなどに登録するアドレスはすっぱりと変えたり捨てたりできるものを使いましょう。

一つのサービスからの流出によって他のサービスに登録しているメールアドレスを変更するのが面倒ならば、無限に近いサブアドレスを作れるサービスもあるので、それを利用してサービス毎に別々のアドレスを登録しましょう。

余談ですがこの方式では、攻撃者からスパムメールなどが来たときに、どのサービスから流出したかをチェックすることも出来ます。

なお、親しい人に限定して使っているアドレスでも、相手がマルウェアに感染して流出させる可能性もあります。さすがにそのことまでは対処することができません。

逆に自分が流出させて迷惑をかけてしまう可能性もあるので、セキュリティを固め、まずは自分から流出させないようにしましょう。

9 通信の安全と永続性を考えたSNSやメールの利用

メールの送受信での秘密を確保する手段として、送信者と受信者が「メールの送受信を暗号化している同じサービスを使う」方法について触れましたが、この「閉鎖された空間による安全性の確保」は、「全ての通信の暗号化を宣言しているSNSサービスを使ったメッセージのやり取り」にも当てはまります。

この場合、上記のメールサービスの利用と同じく、サービス全体が一つのセキュリティ方針で守られるので、安全性は確保されます。

ただしSNSの運営企業によっては、全ての通信を暗号化しているかどうかを明確にしていない場合もあり、一般の利用者が自力で暗号化の状況を調べるのは容易ではありません。

現状では、検索エンジンで「自分が利用しているSNSの名前」+「暗号化」などと入力して調べるか、暗号化を明言しているSNSサービ

スを選ぶしか方法がありません。本来であれば全SNSサービスが、セキュリティの向上に対応してほしいところです。

この閉じた空間による安全性の確保は、確かに安全な通信に有効な手段である一方、様々な機器がつながりあって情報をやり取りする、「インターネット」の思想とは逆の発想でもあります。

本来は多様なサーバがつながりあってバケツリレーが行われるメールであっても、全ての過程で暗号化が行われ、安全性が確保されることが理想なのです。

一方、現状では問題が残るメールですが、SNSと比較したメリットもあります。

メールは特定の企業サービスとは紐付かないインターネットの仕様なので、様々なメールソフトを使い、どのメールサーバに接続しても基本的には利用可能なのです。

1社によって提供され、栄枯盛衰（えいこせいすい）によってサービス終了する可能性があるSNSに対して、メールは永続性の点で有利と言えます。

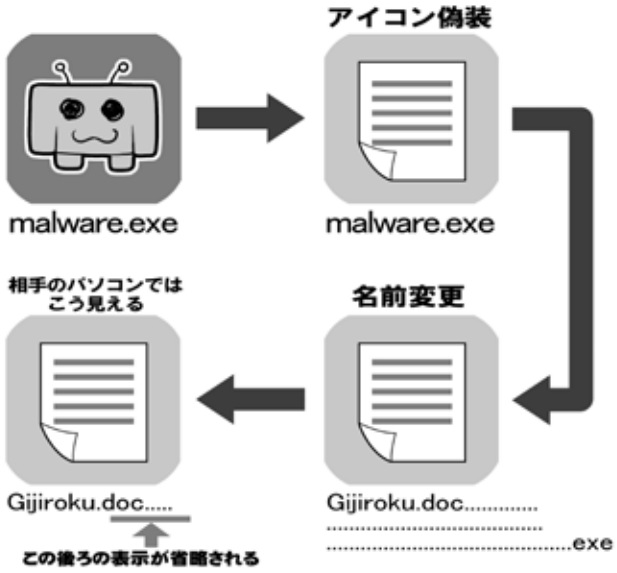
事実、インターネットの初期から様々なOSやメールソフトを乗り継いでも、きちんとメールの内容を引き継ぎ、ごく初期のメールをきちんと見られる状況にしている人が少なからずいます。

SNSや各種通信サービスなどはサービス終了時にデータのエクスポートの対応をすることもありますが、それらは保存されるデータであって、データが生きていた環境はサービス終了とともに終わってしまうわけです。その分、メールにはない、様々な華やかな機能を楽しむ事も出来ます。

SNSとメール、どちらが良いかは人それぞれです。それぞれにメリットとデメリットがあるのでよく機能を理解して、自分に合ったものをうまく利用しましょう。

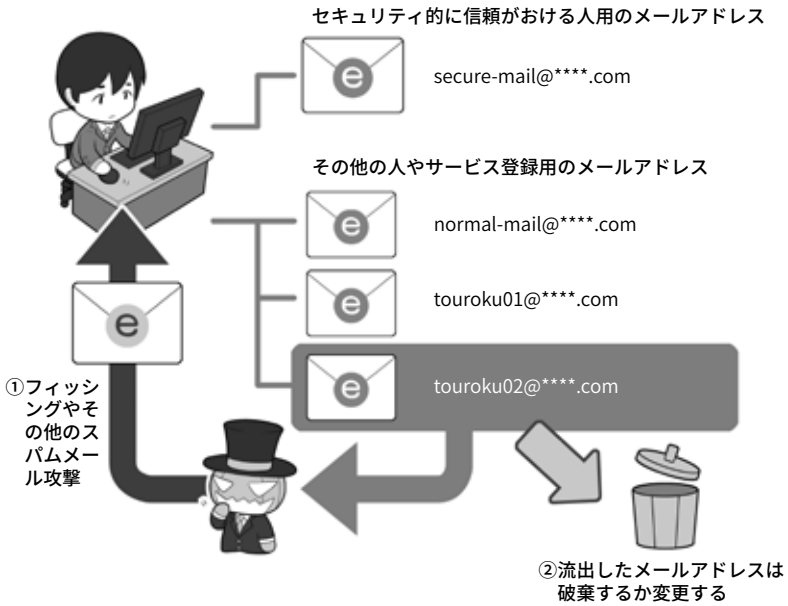
マルウェア入りファイルの偽装

マルウェア入りファイルの偽装



攻撃メールに添付されてくるファイルは、一見するとただの文章ファイルに見える場合もあります。しかし、ファイルのアイコンも名前も偽装したり、別のものに見せかける事は可能なのです

メールアドレスを変えてスパムメールから逃げる



メールアドレスの流出は、ウェブサービス側で管理しているものが攻撃者によって盗まれたり、ウェブサービス側の内部の人間が持ち出して売却したり、セキュリティ意識のない人がマルウェア感染して流出させることなどで起こります。愛着を持って長く使いたいメールアドレスは、むやみに人に教えたりウェブサービスに登録したりしないようにしましょう。流出してしまった場合に備えて変更したり捨ててしまえるメールアドレスを活用しましょう。

5 データファイルを守る、暗号化で守る

もう一つ、通信にまつわる安全で考えなければならないのは「ファイルの暗号化」です。

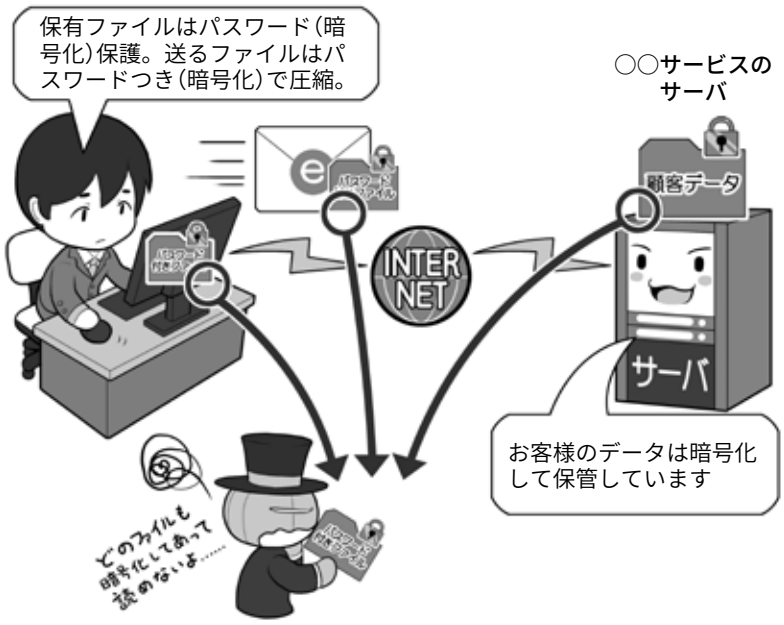
たとえば、メールの添付ファイルが盗聴されたり、保存しているファイルがマルウェアで流出したり、サーバに不正アクセスされて盗まれても、またファイルの入った物理的な記録メディアを紛失しても、確実に適切な方法と鍵（暗号キー）で暗号化してあるならば、攻撃者が解読できなくなり、情報を流出から守ることができます。

ただ、ファイルの暗号化は、攻撃者に盗まれると高速なコンピュータを使って執拗に解読を試みられ続ける可能性があります。従って「暗号キー」の基準に従って、長く複雑なものを設定しなければなりません。

機密情報を持ち運ぶ場合は、ファイル単位の暗号化よりも、ディスク全体の暗号化機能の付いた外付けディスクやUSBメモリの利用を推奨します。可能であれば、高速に暗号処理が可能で様々な攻撃に対策された暗号化チップが内蔵されたものを選択しましょう。そうすることで、ファイル単位の暗号化が不確実になった場合のトラブルも避けられます。

USBメモリの場合、汎用性と安全性を両立した、ハードウェアキーでパスワード認証をするタイプもあります。これらは専用の認証のソフトウェアを必要としないので、利用するOSの依存度が少ないのと、ハードウェアキーの入力が「PINコード」と同じようになっており入力を間違えると「ロック」や「データ消去」の保護機能があるほか、内部の「暗号キー」が十分に長く複

データの暗号化は保険



データを持ち運ぶときは必ず暗号化メディアを使う

ソフトウェア暗号化＋パスワード入力ソフト（機種依存あり）

△ USB HDD

ハードウェア暗号化＋パスワード入力ソフト（機種依存あり）

○ USB HDD

ハードウェア暗号化＋指紋認証 or ハードウェアキー（機種異存が少ない）

◎ USB

＋「強制暗号化」＋「暗号化方式AES256bit以上」
＋「パスワード一定回数入力ミスで完全ロック（アクセス不能）」
あれば…「書き込み時ウイルスチェック（USBメモリ内機能）」

盗まれたメディアはリモートワイプができないので、より高度なセキュリティが求められます。しかし、それよりも重要情報を持ったまま飲酒したり、電車で寝たりすることは言語道断です。本来は暗号化よりもモラルが第一です。

雑なものが自動で生成され、この「暗号キー」の利用に「PIN コード」の入力を求めることで安全性を確保しています。

データの暗号化で重要になってくるのは「暗号キー」の運用です。

「暗号キー」は英大文字小文字＋数字＋記号で、完全にランダムな15桁以上を基準としていますが、完全にランダムな場合、暗記することは困難になりますし、またスマホのパスワード管理ソフトやパスワードノートを見て打ち込むのも一苦労になります。

かといって、パソコン上に保存したり付箋で貼っていたりすると「パスワードを利用場所に保管しない」というセオリーに反します。

現状は単純で楽な解決方法はありません。ただ暗記を前提にするのであれば、自分だけが知っているマイナーな曲の歌詞などからローマ字打ちで15桁よりかなり長くなる部分を抜き出し、独自の方法で一部記号や数字に置き換えるなどが考えられます。

また、暗号化したファイルを誰かとメールで受け渡しする場合、相手と「暗号キー」を共有する方法にも気をつけなければなりません。

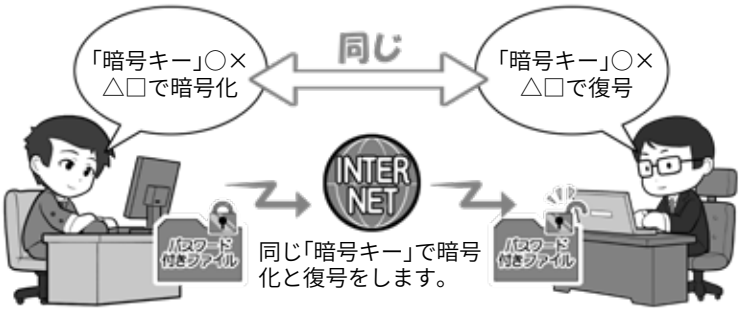
別送信であっても、暗号化ファイルと「暗号キー」を同じメールアドレスに送れば、メールが流出すると２つが揃ってしまいます。

「暗号キー」はメールでは送信せず、現実に会ったときに決めておくか、それができず、出先で突発的に送信が必要になった場合は、電話などで伝達するか、通信が暗号化されている「別系統の送信経路」で送るようにしましょう。

また、「暗号キー」には先ほども少し登場した、対になった２つの暗号キー（公開鍵と秘密鍵）を使ってやりとりする方式（公開鍵暗号方式）があります。この鍵は手で入力するのではなくパソコンが自動的に使うためのものですので、直接目にすることはないかもしれません。

この方式を利用している具体例としては、79ページで紹介した「S/MIME」や「PGP」や、同じように目にすることはありませんが、Wi-Fi通信の暗号化などがあります。

「暗号キー」が１個の方式（共通鍵暗号方式）



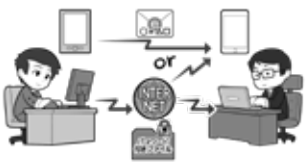
同じ「暗号キー」で暗号化と復号をします。

安全な「暗号キー」の受け渡しの例

電話

直接会ったときに「暗号キー」を渡したり、電話で直接伝えたりします。

別経路のメールアドレス



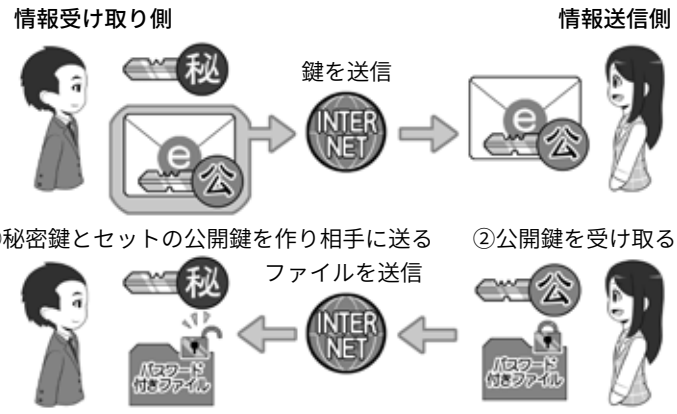
盗聴やマルウェア感染を考え、スマホ対スマホなど別経路で送信します。

古式ゆかしき手紙

アナログだが一つの方法で、銀行などが利用しています。

どの場合であっても「暗号キー」の秘匿が重要です。

「暗号キー」が２個の方式（公開鍵暗号方式）



共通鍵暗号方式と異なり、「暗号キー」を送信しても大丈夫なのがポイントです。この方式では「暗号キー」は手入力では使いません。メール送受信の影で使われていたりします。

コラム：究極の防御手段「ネットにつながない」エアギャップ

小さな会社の仕事などで、業務上どうしても個人情報などの入った顧客データベースを管理しなければならないが、マルウェアによる感染は怖いし、セキュリティを固められているか自信がない。

そんなときは、重要な情報の入ったパソコンを、極力ネットにつながずスタンドアロンパソコンとして使用するという手があります。

このネットにつながっているパソコンとスタンドアロンのパソコンの間、マルウェアが電子的に越えることができない壁を「エアギャップ（空気の隙間）」と呼び、立派な防御方法の一つとなっています。

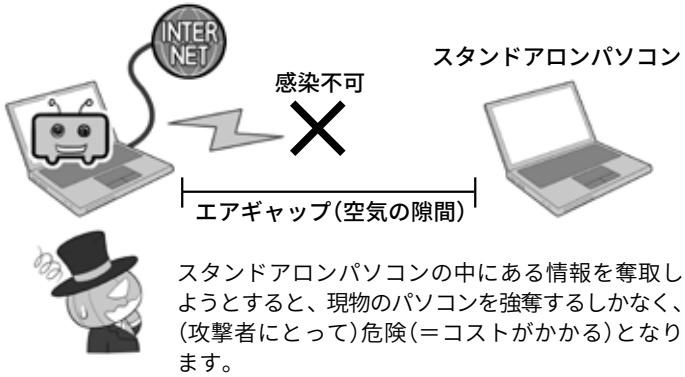
もし攻撃者がこのスタンドアロンのパソコンに入っているデータが欲しければ、物理的に事務所に忍び込まなければならず、それは攻撃者にとって危険でコストがかかることであり、抑止力になるわけです。

ただデータの盗み出しではなく、破壊などが目的のマルウェアの場合は、USBメモリを介して感染させるという手法があります。それらを避けるには、きちんと管理できる人間以外がうかつにUSBメモリを差さないように、パソコン側に鍵つきのUSB端子キャップなどを使いましょう。

余談ですがこの方式の場合、スタンドアロンパソコンが仮に感染しても、外部との通信ができないためデータの持ち出しは困難なのですが、パソコン内でのわかりきった場所にある少量の情報であれば、光るもの（LEDやパソコンのモニタ）、音、消費電圧の上下などを使って、外に向かって信号を送ることは可能であり、攻撃者がこれを観測できれば情報の奪取も可能となります。ようするにこれらのものを使ってモールス信号を打つといわれればイメージがわくでしょうか。

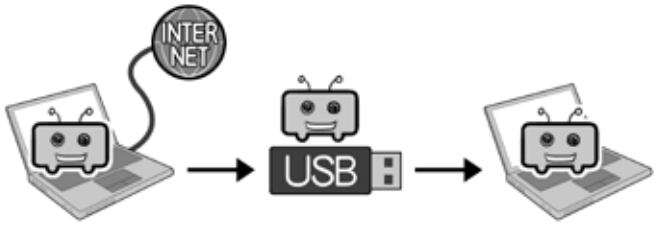
話題を戻してエアギャップをインターネットバンキングの不正送金の例に当てはめて

有線でも無線でも、つながっていないパソコンにはマルウェアは感染しない



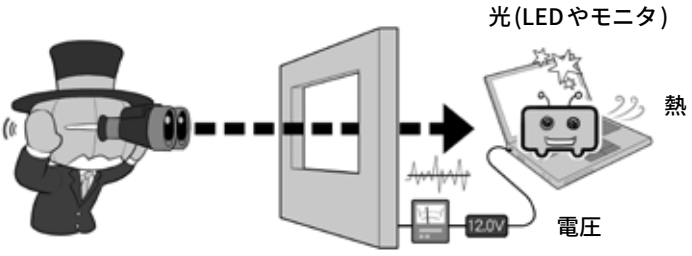
スタンドアロンパソコンの中にある情報を奪取しようとすると、現物のパソコンを強奪するしかなく、（攻撃者にとって）危険（＝コストがかかる）となります。

しかし、USBメモリを介して感染することも



かつて、イランで核燃料施設にあるスタンドアロンパソコンを感染させ、機器を暴走させた手法（Stuxnet型）です。ただし、攻撃者がマルウェアをネット経由で直接操作できないのと、データを抜き出すのは困難。

ネットに接続していなくても、少量のデータであれば盗める



Stuxnet型で感染したパソコンに、あらかじめ特定のデータの内容を、デジタル信号の形で、光、音、電圧差などを使って発信させることは可能です。それを受信することができれば情報の奪取も可能です。ただし通信速度は遅いので大容量のデータを盗み出すことは困難です。

みましょう。

インターネットバンキングのセキュリティの向上と、攻撃者の技術向上はいたちごっこであり、銀行などによって様々なセキュリティ対策が講じられますが、絶対に安全ということはありませんし、今後も難しいでしょう。

それは攻撃者との技術競争的な問題もありますが、セキュリティに人間の心の隙という防御しにくい要素が含まれていることと、攻撃者がネットの闇に姿を潜めていて、現実世界でそこまでたどり着き、相手を捕まえることが簡単ではないからです。

このうち人間の心の隙に関しては一朝一夕に対策を講じることは難しいのですが、攻撃者がネットの闇から出てこなくてはならない方法で防ぐ手段はあります。すごくシンプルな方法でおどろくかもしれませんが、ようは取引をネットで行わなければ良いだけなのです。

インターネットバンキングは確かに便利ですが、現在ではコンビニを含めありとあらゆる所にATMが設置され24時間稼働していますし、24時間送金可能なものもあります。したがって、多量の送金処理を毎日行うのでもなければ、インターネットバンキングを使うのは「便利」ではあっても「必須」ではありません。

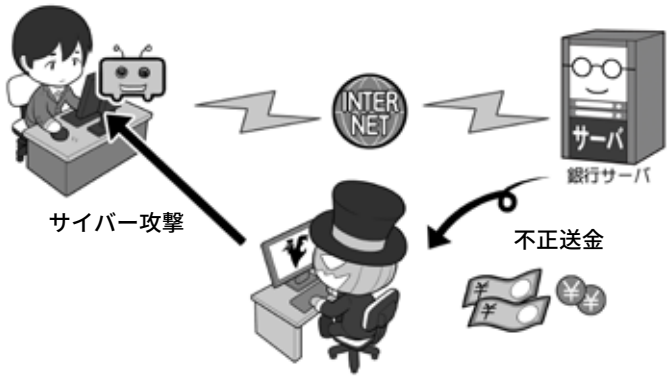
そしてネットを利用しない場合、攻撃者が不正にお金を奪おうと思えば、現実世界でキャッシュカードとあなたの身柄を抑えて、暗証番号を聞き出さなければなりません。

そのようなことをすれば当然のように顔もばれますし、リスク(コスト)も非常に高くなるので、攻撃者としてそういった手段は選びにくくなるでしょう。

このように、ときにはネットにつながない、ネットを利用しないという「ある種のエアギャップ」という選択肢をとることも防御の一つなのです。

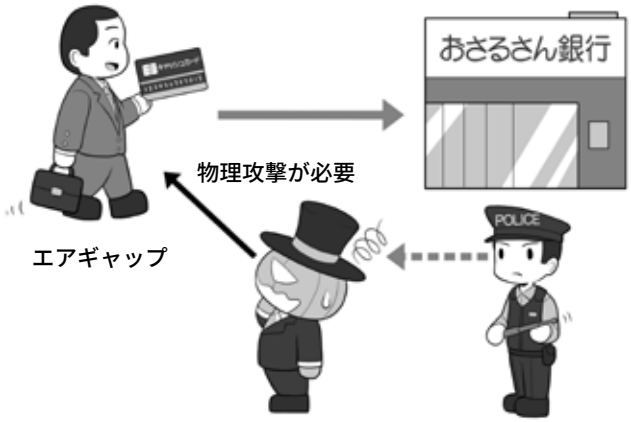
ネットにつなぐのは「便利」の物差しだけで考えるのではなく、「利便性」と「危険性」を天秤の両側に乗せ、総合的に安全な選択肢をとるべきでしょう。

オンラインで銀行口座が狙われるなら



ネットを使って銀行口座から不正送金が行われるのは、そもそも送金処理をネットで行っていることと、攻撃者がネットの闇に潜んでいて、世界のどこにいるかわからず、検挙しにくいこともあります。

インターネットバンキングを止めるという手も



ネット経由ではなく現実世界で送金処理を行うようにすると、当然ネットを使った不正送金はできませんし、お金を引き出す情報や鍵を持っているあなたと攻撃者の間には、エアギャップが存在することになります。無理矢理カードと暗証番号を手に入れようとすると、現実世界で窃盗や強盗をしなければならず、監視カメラなどにも映るので、リスク(コスト)がかかるようになります。このリスクが防御となるわけです。

コラム：「無料」ということの対価は何か

インターネットではよく「無料」という言葉を見かけます。無料のメールサービス、無料のウェブサービス、無料の動画公開サービス、無料のアプリなどなど。

しかしお店などの試食コーナーの図を見てもらうとわかりますが、私たち利用者の側から一見無料に見えても、サービスが提供されるときは必ず「コスト（費用）」がかかっています。そして正常な企業であれば、コストが回収できないビジネスは行いません。そこには何らかの採算が取れるシステムが存在し、私たちが見えないところでお金が回って提供されているわけです。

その方法の一つは広告による収益モデルです。広告主がウェブなどに広告バナーを出し、サービス会社はそれを資金源に運営するわけです。

広告システムがもう少し進むと、ウェブサービス会社が私たちのウェブ上での行動パターンや、趣味や行動などの情報を収集し、一見匿名の情報の形にして、これを広告主に提供、広告主は自社製品にマッチした人物向けに絞り込んで広告を打つなどして、より効果的な宣伝を行います。

このパターンでは、匿名とはいえ平たくいえば「私たちの情報」がサービスの対価として支払われているわけです。

また先行投資といって、当初無料で提供し、サービスに馴染んだら、その後有料化してコストを回収するマネタイズを行う型もあります。

そして最後にもっとも気をつけたいのが善意の無料サービスです。

誰かがウェブサービスやアプリなどを開発し無料で提供

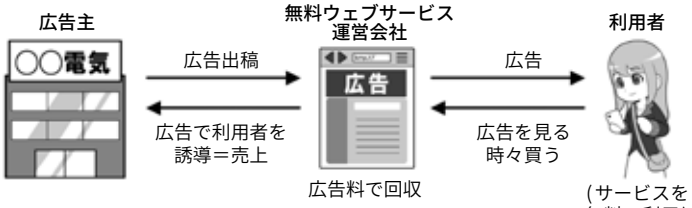
試食サービスのコストの例

（ソーセージを売る場合）

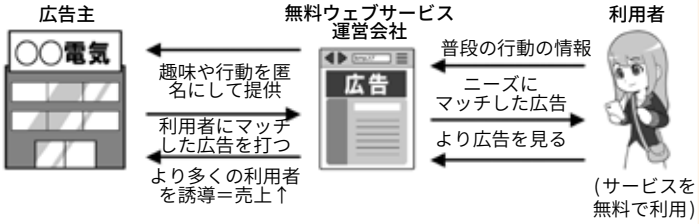
・食べる側は一見無料だが、人件費、光熱費、材料費は必ず発生し、どこかで誰かが必ず支払っている
・お店全体の売上や直接的なソーセージの売上の一部としてなど
・運営主体もしっかりして、コストも回っているので食べても大丈夫

無料ウェブサービスの例

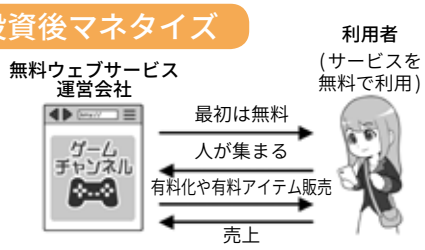
①無差別広告で運営



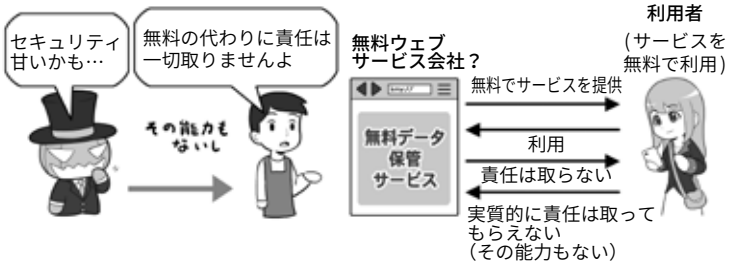
②利用者の情報を利用し、ターゲットに合わせた広告で運営



③先行投資後マネタイズ



④善意の無料サービス（責任能力なし）



するのですが、明示的ではなくても「責任は一切取りませんよ」という状態のものです。この場合コストは提供する側のポケットマネーなどでまかなわれ、ビジネスとしては成立していないので、セキュリティに対して割くべきコストや労力がおろそかになりがちです。そしてここが弱点として攻撃者に狙われ、利用される可能性があるわけです。

公衆無線LANの無料サービスも考えてみましょう。

政府機関・施設や自治体などが提供するものは、運営費とセキュリティの費用が、実は税金でまかなわれています。

携帯電話会社が提供する場合は、支払料金の中からまかなわれているので「追加料金無料」といった方が良いでしょう。

対価を払って利用する場合は、当然その支払料金が運営管理費用やセキュリティ費用にあてられます。

そして今回も問題なのは「善意の無料サービス（ただし責任能力なし）」です。

小さなお店などで無線LANが提供されている場合、それは仕事用のものを開放しているだけかもしれません。そして無料で使っている以上利用者に契約関係もなく、安全性を求める権利もないわけです。

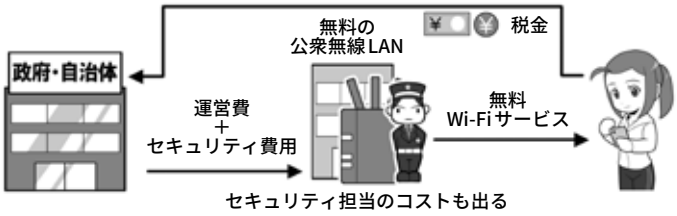
そして攻撃者はこのような所を狙って罠を仕掛けてきます。運営費もセキュリティ費用もないならば、誰も日常的に攻撃者の有無をチェックしないからです。

このような理由があるので、「運営主体がはっきりしていない、責任能力の無い無料の公衆無線LANは使用しない方が良い」というわけです。

無料という言葉には注意。費用の出所がはっきりしない場合、あなたが個人として高いツケを払わされることになるかもしれませんよ。

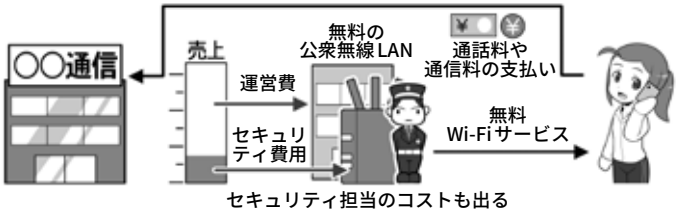
無料の公衆無線LANサービスの例

①一見無料だが税金などでまかなっているから無料



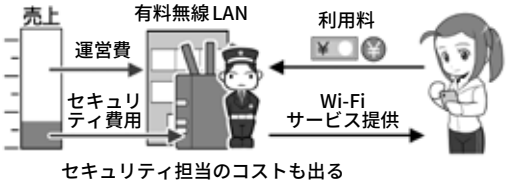
トラブルがあると議会などで取りあげられ問題となることもあります。責任能力もあります。

②企業が収入の中から払っているから無料



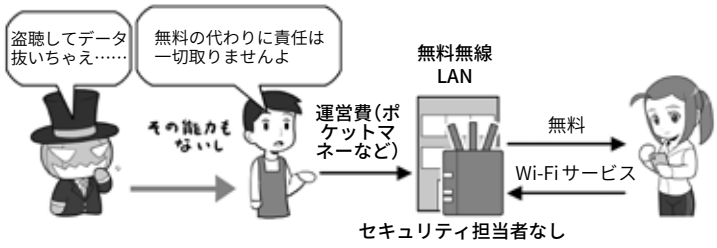
トラブルが起きれば責任問題となり、本業にも影響が出ます。責任能力もあります。

③対価を支払って利用する（有料）



対価をもらったサービスなので、トラブルが起きれば責任問題となります。

④善意の無料サービス（ただし責任能力なし）



対価はもらっていなので、トラブルは自己責任といわれたり、実質的に責任は取ってもらえません（その能力もありません）。

コラム：クラウドサービスからのデータ流出。原因は？

クラウドサービスとは、「従来自分の手元で保存していたデータなどを、インターネット上にどこかに雲のように存在しているサーバに保存し、どの機器からでも意識せず利用できる」サービスで、その雲的なイメージを指してクラウド（cloud）と呼ばれます。

実際にはサーバは雲や霞ではなく、どこかに歴然と存在していますし、概念自体は昔から存在するので、「意識せずに使える」≒「便利である」ことをクラウド（雲）と例えたあたりが、ポピュラーになったポイントでしょう。

最近ではスマホを利用していると、意識しないうちに写真などがクラウドにバックアップされている事もあります。それに、ウェブブラウザがあればどこからでもアクセスできるメールサービスも、クラウドの利用とも言えます。

パスワード管理アプリの記事では、クラウドサービスを利用することに関して厳しく書きましたが、クラウドサービスは、その性格を理解して利用するなら大変便利なものなのです。

一方、問題なのはクラウドサービスからの情報流出です。攻撃者がシステムを攻撃して大規模に情報を奪取することも無いとは言いませんが、ニュースを賑わす話のほとんどは、利用者のパスワードが各種攻撃で破られ、クラウドから情報を抜き取られたケースです。

ここでの攻撃とは、「リスト型攻撃」「辞書攻撃」、そして個人情報からの推測などです。

他のサービスとID・パスワードを使い回ししていて、侵入された場合もありますが、「パスワードは誕生日やニックネームから推測した」という攻撃者の証言もよくあります。

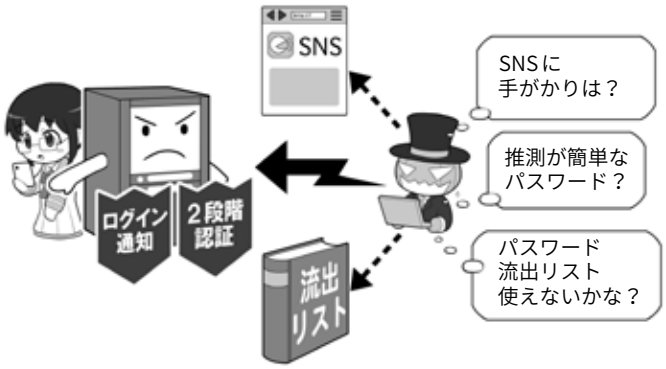
こういった流出事故を起こさないためには、まずID・パスワードを使い回ししないこと。そして、推測されるほど簡単なものにしないこと。二段階認証や、不正なアクセスがあった場合通知されるサービスを利用すること。そして「流出して困る情報はクラウドサービスにアップロードしない・（自動で）されないようにする」ことです。

クラウドは大変便利ですが、きちんとセキュリティを固めなければ攻撃の的になると、理解して利用しましょう。

データはどこに保存されている？

スマホなどを使っていると意識せずにクラウドサーバにデータをバックアップしていることもあります。よく分からない場合は、一度調べてみましょう。「クラウド」という名前ではなく、それぞれのサービス毎の名前をつけられている場合もあります。

パスワードが甘いと流出するかも



攻撃者はクラウドサーバのパスワードを破るために、様々な攻撃を試みます。「ログインパスワード」の基準でパスワードを設定するなど基本を守るとともに、使い回しをせず、二段階認証の設定や不正なログインがあった場合に通知を受け取れる設定を活用しましょう。

第４章

スマホ・パソコンのより進んだ使い方やトラブルの対処の仕方を知ろう

パソコン・スマホの扱い方を中心に、安全を守る手段について勉強しましょう。
どのように情報を守るか、どのように安全にネットを利用するか、セキュリティを守る為の技術を、障害物競走のように楽しめれば、みなさんのスキルアップになるでしょう。

1 スマホのセキュリティ設定

1 スマホにはロックをかけよう。席において離れたり、人に貸したりするのは×

スマホの情報を守る第一歩は、待ち受け画面にロックをかけることです。

ロックにはPINコードによるロック、パターンロック、生体認証によるロック、また最近では特定の機器(普段身につけているスマートウォッチなど)や、GPSに連動して特定の場所(自宅など)で自動的にロックと解除ができる機能もあります。

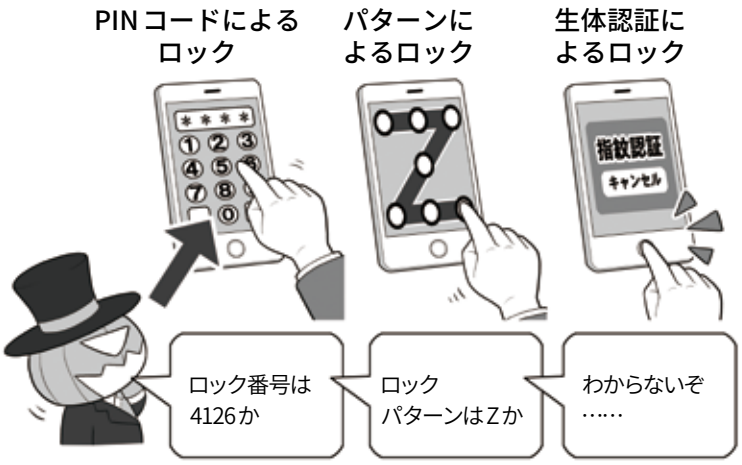
ただ自分が明示的に指示をしないロック解除は、うっかり端末を無防備にすることもあるので、基本的には何らかの動作をして解除する方式にしましょう。そして周りから覗かれPINコードを覚えられる危険性の排除や、入力の面倒くささを省く点からは、生体認証が便利です。

ただ生体認証にも弱点があります。写真から復元した偽の指で指紋認証を破る研究や、「寝ている時に自分の指を勝手に使われ認証突破されてしまう」こともあります。過信しないようにしましょう。

そして各種のロック機能を設定しても、スマホのロックを解除をしたまま置いてその場所を離れたり、ロックを解除して他人に見せたり、あるいは貸してしまったりすれば、一瞬で情報んだり、乗っ取ったりすることは可能です。

スマホは持ち歩く情報の金庫だと思って必ず自分のそばに置き、こまめにロックをかけた状態にし　ましょう。

スマホにはロックをかけよう



席において離れたり、人に貸したりしないようにしよう

スマホを席に置いたままでは、本体も情報も盗まれる恐れがあります(特にロック解除したままの状態で放置)。

スマホを貸すと、プライバシーを覗かれたり、一瞬で盗み見アプリをインストールされたりすることがあります。注意しましょう。

2 情報漏れを防ぐ①

SNS用のアプリなどには、本体のロックとは別にアプリ用のPINコードなど設定できるものもあります。盗難などの際、SNSの内容を見られたくなければ、このアプリPINコードも設定しましょう。守りが二重になります。一部の機種では指紋認証をアプリのロック解除に利用できるものもあるので、セキュリティを向上させても日常的な利用の妨げにはなりません。

一方攻撃する側から見ると、スマホのロックを何らかの方法でパスできたとしても、また別の関門が待ち構えているわけで、手間をかけさせ侵入を諦めさせるというセオリーに沿っているわけです。

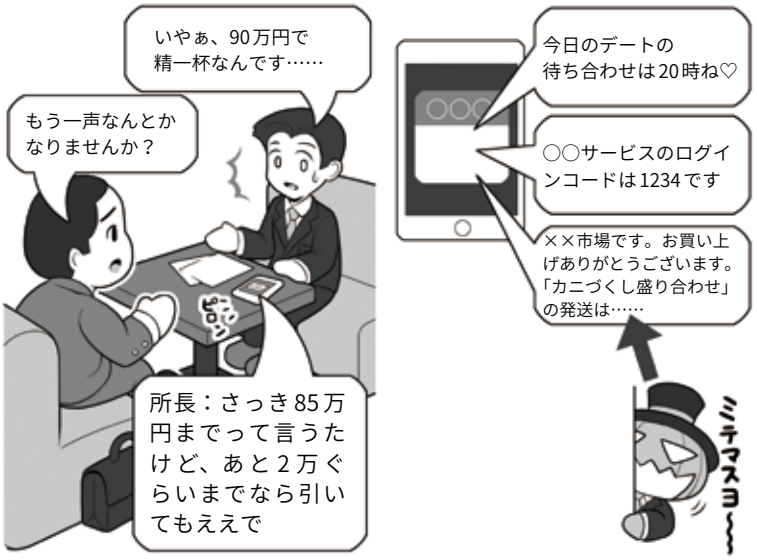
なおアプリのPINコードを使う場合は、スマホロック解除のPINコードと異なるものを設定しましょう。PINコードの使い回しはセキュリティがないのと一緒になってしまいます。PINコードも異なってこそ意味があるのです。

スマホをロックしていても情報漏れが発生することもあります。

たとえば自分だけで使っているときは便利なメールの通知機能。ロック画面にメールの内容を表示していると、誰かと会話中や商談中に、うっかり内部の情報を見られてしまったり、あるいは差出人が分かるだけで、状況によっては知られると問題のある情報を提供してしまうことになります。

また同様にロック画面にメールの内容を表示していると、せっかくセキュリティ向上のために設定した二段階認証の確認メールも見られてしまうことがあり得ます。そうするとIDとパスワード＋ロックのかかったスマホだけでも、「正常に」ウェブサービスのセキュリティをパスできてしまうわけです。

待ち受け画面に表示する通知はよく検討する



ロック画面だけでなく、普段使用している画面に通知ウインドウとして表示される場合でも、同じく情報を見られてしまう原因になります。スマホを使って説明しているときに、不適切なメールの内容が表示されることも……。情報の扱いには気をつけましょう。

アプリごとにパスワードをかけられる場合はかける

本体のロックを解除されても、SNSのアプリに別のパスワードがあれば、流出の危険性は低くなります。ただし、自分が席を離れる時にスマホを残してはいけません。また勝手に人のスマホのロック解除をすることは攻撃です。

3 情報漏れを防ぐ②

直接スマホを盗まれる以外の情報流出のケースには、攻撃者による無線LANを使った盗聴があります。スマホから無線LANのアクセスポイントの間の情報通信を盗聴するわけです。これを防ぐには通信の暗号化が重要です。

暗号化のセクションの繰り返しになりますが、無線LAN利用時のチェックポイントとしては、

1. **無線通信が暗号化されていて、かつその暗号化方式が安全であるか。**
2. **きちんと暗号化されていても、その通信を利用する「暗号キー」が他人に漏れていたり、共用になっていないかどうか。**

などがあります。

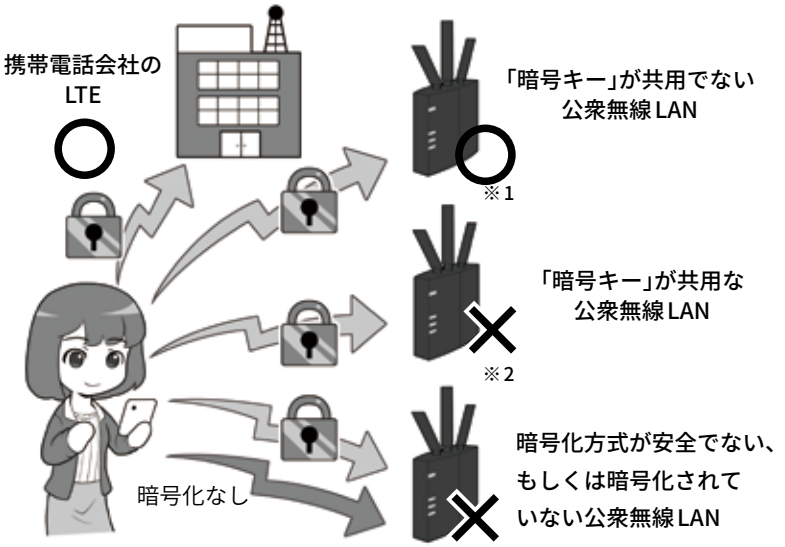
企業によって提供されている公衆無線LANであれば、上記の無線LANの安全性をきちんと理解して提供する能力があるかどうかをチェックしましょう。トラブルを発生させて「謝るだけ」の企業より、情報漏れの芽を摘み「万全の安全性のもとにきちんとサービスを提供する」企業の方が、はるかに優秀で信頼に足るのです。

その点をよく調べた上で利用する公衆無線LANの企業を選択するのも、重要な情報漏れの防御策です。

次に万が一、スマホを落としてしまった場合に、情報流出させない方法も考えましょう。

まずはスマホの中身が暗号化されているかチェックです。古い機種では初期状態で暗号化されていないことがあります。本体と記録メディアいずれも暗号化して、落としてしまっても簡単には利用できないようにしましょう。暗号化は本体のロックとセットとなり、必然的にロック機能もONにする必要があります。

屋外ではむやみに公衆無線LANを使用しない



そもそも自分と「契約関係がない」ものは基本的に使わず、また運営主体がわからない無線LANアクセスポイントは絶対に使用しないようにしましょう。

※1 携帯電話会社やプロバイダが提供していても、「暗号キー」が共用でないとは限りません。きちんとチェックしましょう。

※2 暗号キーが貼り出してあるような公衆無線LANは、「暗号キー」が他人と共有になり危険です。使わないようにしましょう。

無線LAN暗号化などに関するより詳しい説明は、50ページからを参照して下さい。

盗難されたときのために 中を見られないように暗号化しよう

本体もメディアも暗号化。最近では暗号化が標準のものもありますが、必ず確認しましょう。

スマホを落としたときの次の対策としては、リモートロック、位置情報確認やリモートワイプ機能を使える状態にしましょう。

iOSではiCloudの「iPhoneを探す」、Androidでは「Androidデバイスマネージャー」として、それぞれ該当の機能があり、パソコンや同じアカウントを紐付けた他の端末から操作ができるようになっています。無料なので必ず試してマスターしておきましょう。

リモートロックとは遠隔操作でスマホをロックして使えなくする機能です。スマホの所在がわからなくなったら、なによりもまずスマホをロックしましょう。

次に「位置情報」を確認しましょう。事前にこの機能を使ってスマホの位置確認ができるかどうかを試し、確実に使えるように設定しておきましょう。ただし子どもの端末などの監視目的では絶対に使わないようにしましょう。このことの理由は後ほどご説明します。

建物の中などでは明確な場所が特定できない場合もありますが、現在のスマホのおおよそのありかが地図上に表示されます。

見つかった場所が、自分が訪れた場所や、遺失物として届けられた警察などなら連絡をして取り戻す段取りをします。一方そうではない場合は、最後の手段として情報漏れ防止のために「リモートワイプ」機能でスマホの中身を全部消すことも考えましょう。ただし、リモートワイプをすると、位置情報を取ることができなくなりますので、情報を守るための最後の手段になります。

そして、仮にスマホが戻ってこなくても、本体を買い直したらすぐに復旧できるように、スマホの中身は定期的にバックアップしておきましょう。

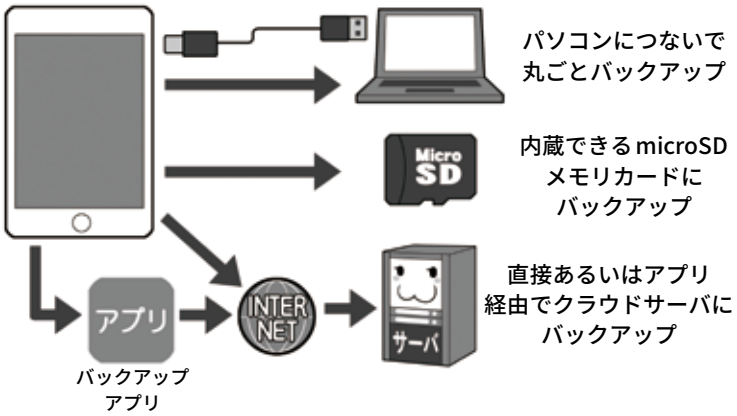
機種によってはパソコンでバックアップすると、新しいスマホをつないでボタン一発指示するだけで復元できるものもあるので、機種選定時に調べておきましょう。

紛失や盗難時のために準備をしておこう

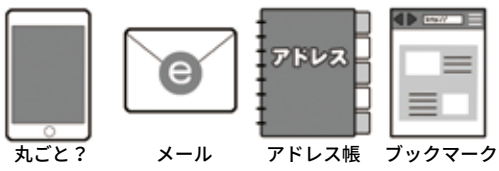
※リモートワイプすると位置情報が確認できなくなるので、リスクが少ないならばロックだけ行い、遺失物として警察に相談するなどの手段をとりましょう。

バックアップは定期的に取ろう

バックアップの方法はいろいろ



なにがバックアップできるか確かめる



なにがバックアップできるのか確かめて、機種やバックアップ方法を選択します。

4 スムーズな機種変更と、予期せぬデータ流出の防ぎ方

スムーズな機種変更を行うためには、その前に機種変更手段を調べておくことが重要になります。

バックアップの項目でも書きましたが「丸ごとバックアップ」「データごとにバックアップ」「アプリを使用してバックアップ」など様々なバックアップ方式があります。このあたりは自分で調べるとともに、実際に機種変更やデータの移行をしたことがある人に聞いたり、記事を見たりしてつつ、どの方法が便利だったり簡単だったか、アドバイスを求めると良いでしょう。

最近ではスマホ自体の中(ローカル)にデータがあるだけでなく、インターネットのどこかに利用者から見て姿が見えない雲のような存在のサーバ(クラウド)に保存されている場合もあり、場合によっては移行のためのバックアップ作業という概念そのものがないものもあります。

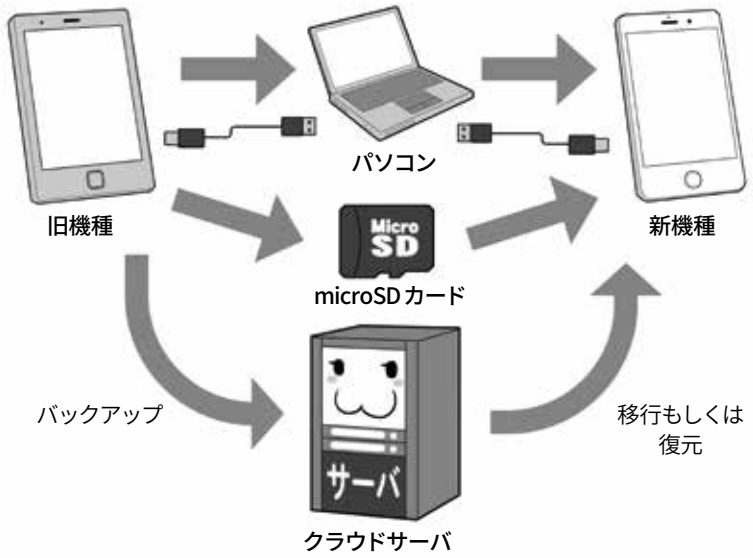
また本体のデータ移行手段とは別に、機種変更に際して、特定の機能の移行処理をしておかなければならないものもあります。

たとえばいわゆる「おサイフケータイ」に関する機能では、一旦スマホから機能を削除して情報をサーバ側に預け、かわりにパスワードを受け取り、その後新しい機種でログインして貰ったパスワードを使って機能を復元する処理が必要があるものもあります。

また一部のSNSでは、旧機種がアクセス可能なまま新機種がアクセス可能になって、複数台から同時アクセスできないように、移行処理の前に一度手続きを踏んで、旧機種からアクセスできないようにしてから、新しい機種でアクセスするための利用開始の手続きをする方式もあります。

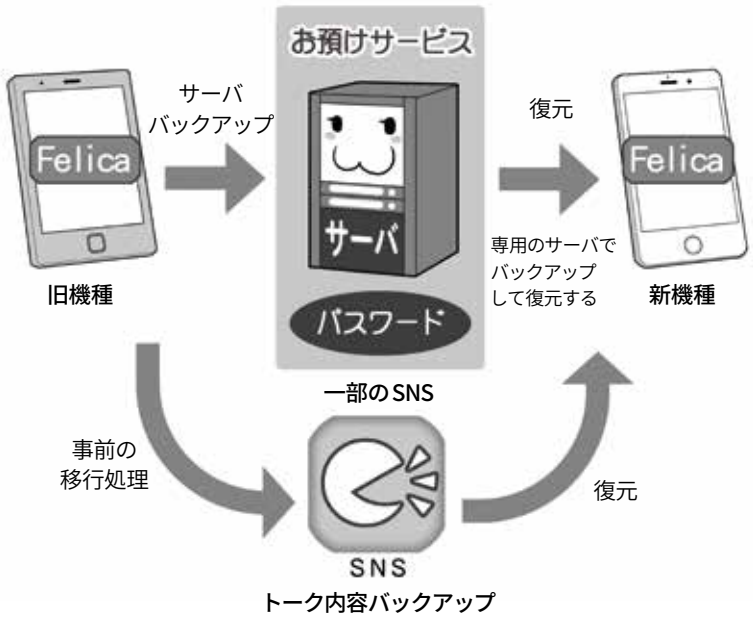
いずれの場合も機種変更の移行処理にあたって、移さなければならない機能を書き出し、それが網羅されているかどうかをチェックしてください。さもないと、電子マネーが旧機種とともに消えてしまって取り戻すのが困難になることもあります。

データの移行は事前に手段を調べる



移行処理は事前に目的の機種でどういった移行手段が使えるのか調べておきます。

おサイフケータイや、SNSデータなどの移行



次は機種変更をした後の情報流出を防ぐ処理です。

機種変更した前のスマホには個人情報である住所録、撮りためた写真、今までやりとりしたメールなど、あなたの情報が全部詰まったままになっています。売却、譲渡や廃棄する場合、データを必ず消去しなければなりません。さもないと、知られたくないメールや写真が流出したり、住所録にある友人宛にフィッシングメールが送られてくるかもしれません。

また修理に出す場合でも、モラルの低い修理会社が、芸能人のスマホから写真を抜き出して流出させた例があるので、必ずデータをすべてバックアップをした上で、本体のデータは消去してから修理に出したほうが安全でしょう。

まず各種サービスはアプリもウェブも全てログアウトします。続いてそれぞれのスマホにある「初期化」や「データ消去機能」を使って内部のデータを消去します。

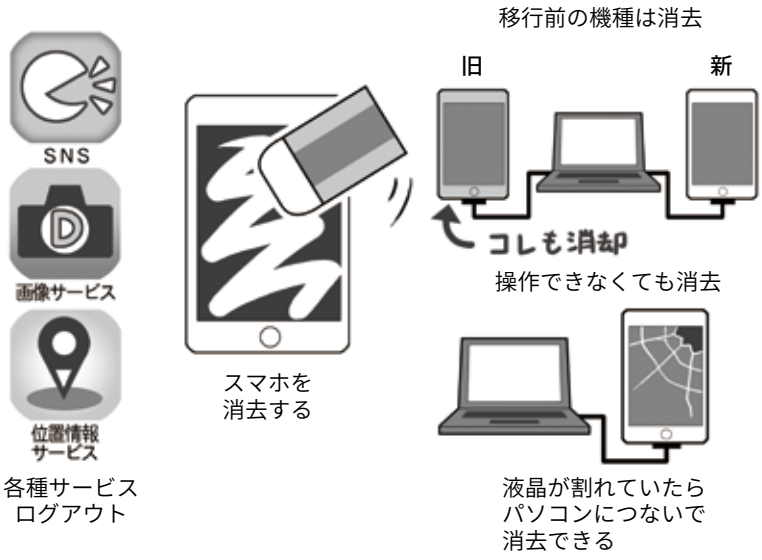
一部のスマホでは、紛失時に探せるように設定した「位置情報を確認するためのサービス」を事前にログアウトしておかないと修理などに出せないものもあるので、消去の前に確認してください。

落としてしまって液晶が割れ、操作ができない場合どうすることもできないと思いがちですが、パソコンに接続することで消去することができますので、あきらめず必ず行いましょう。

業務用に使用しているスマホなどで、万が一にでもデータが復元される可能性を排除したい場合は、各携帯電話会社や家電量販店などで、スマホを物理的に破壊してくれるサービスを利用して、データを読み出せないようにしてしまいましょう。

なお余談ですが、業務用などで情報漏えいのリスクを少しでも排除したいなら、中古品を使ったりしないようにしましょう。中古販売店が良心的でも、プロの組織が仕込むようなマルウェアやバックドアには対処できない可能性があります。それを排除するには信頼できる国で生産された、正規ルートの新品を購入して使いましょう。

転売、譲渡、廃棄のときは必ずデータを消去する



消去する前には、利用しているサービスはログアウトして、サーバなどに情報を預けなければならないもの（おサイフケータイ）などは預ける。SNSで移行処理が必要なものを行う。その後移行処理をして、移行後きちんと復元できたら、前の機種を売却・譲渡や廃棄する場合は、必ずデータを消去する。液晶が割れて操作できなくても、パソコンに繋げば消去することはできる。

業務用のスマホは物理的に破壊する。プロならば新品で情報流出の可能性を排除する

仕事に使うスマホを廃棄する場合は、物理的に破壊する機械がある場所に持ち込んで破壊しましょう。大手携帯電話会社での回収も信頼できます。
一方購入時に、中古品を購入して仮にスパイウェアが仕込まれ、企業の情報が流出しても、販売したものにその責任を取る能力はないでしょう。ましてやオークションでの購入などではなおさらです。残債で購入後使用不能になるケースもあります。業務用に使用するなら情報機器は新品を利用しましょう。

2 パソコンのセキュリティ設定

1 パソコンを買ったら初期設定などを確実に

パソコンを購入したら、まず復旧のときに必要になるリカバリメディアを作成しましょう。

リカバリメディアがDVDなどで付属している場合は必要ありませんが、最近の機種ではコストダウンで添付されないものや、そもそもDVDドライブなどを搭載していないものも多いので、マニュアルなどに従ってDVD-RやUSBメモリで作成します。

またWindowsではリカバリメディアなどを使ったときに「プロダクトキー」が必要になる場合があります。本体の裏側などにシールで貼られているか、付属しているリカバリメディアに貼り付けられているので、スマホなどで写真に撮っておくか、メモに書き写して保管しておきます。

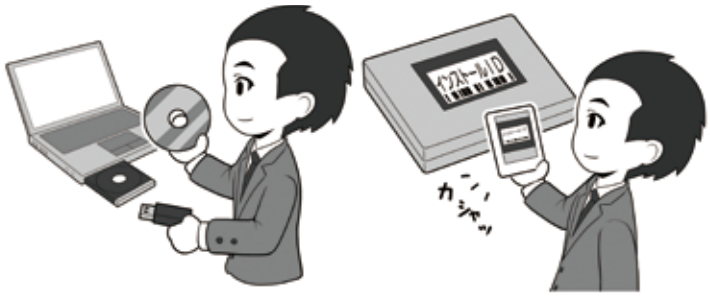
次にセキュリティの設定をします。初期設定時にIDと「ログインパスワード」の設定を必ず行いましょう。また、マニュアルに従って起動用「BIOSパスワード」や「ファームウェアパスワード」といった、電源を入れた段階で入力することを求められるパスワードを設定しましょう。

これを設定しておくと、盗難されてもそもそも電源を入れることができなくなり、盗難時の情報流出をより防ぐことができます。

生体認証を使用する場合は、パスワードのセオリーに従って「ログインパスワード」を設定した上で、生体認証の登録を行い、セキュリティを高めつつログインの手間を省きましょう。

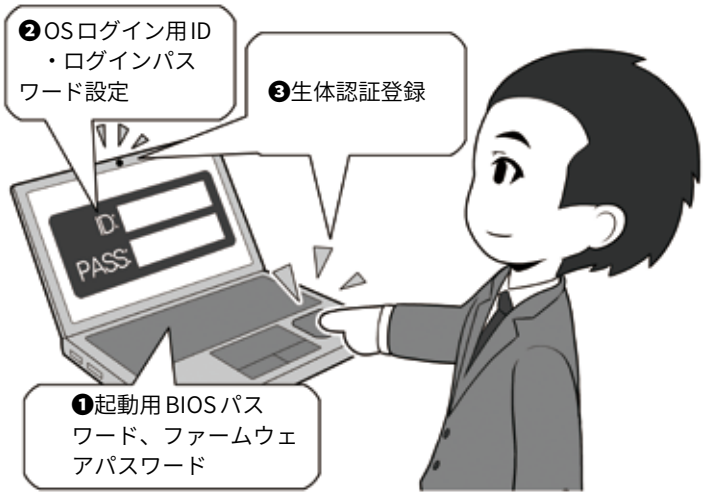
生体認証機能が無い場合はパスワードをしっかり設定しましょう。

パソコンを買ったらまずリカバリメディアを作る



DVD-RやUSBでリカバリメディアを作り、本体裏などにあるプロダクトキーを保存します。メディアは添付されていれば作る必要はありません。

起動用のパスワードや生体認証登録をしよう



「ログインパスワード」はセオリー通り複雑なものを設定し、その上で生体認証を使いログインの手間を省くようにします。起動用パスワードなども設定しましょう。起動用パスワードなどは「ログインパスワード」相当に設定します。

2 暗号化機能などでセキュリティレベルを高める

パソコンを盗まれたときに、情報が流出しないように、攻撃者に嫌がらせ、ではなく、セキュリティレベルを上げましょう。

会社のパソコンは泥棒などが盗んで帰れないように、ワイヤーロックという盗難防止用のワイヤーで、パソコンを移動できないようにしてあります。

こういった場合、攻撃者は情報だけでも入手すべく、パソコンの中のハードディスクやSSDだけを盗む可能性もあります。

そうやって盗んでも情報が漏れないようにするため内蔵ディスクは暗号化処理を行いましょう。

この場合の「暗号キー」は「ログインパスワード」と共用になっているものもあるので、その場合はより複雑な「暗号キー」のセオリーに従い、15桁以上に設定します。

きちんとした複雑さと長さの「暗号キー」で暗号化されたディスクは、盗んで別のパソコンに繋いで暗号化を解除しようとしても、解読が非常に困難であり、情報流出を防ぐ力になります。

またスマホにあるロック機能やリモートワイプも、業務用でかつLTEなどの通信回線を内蔵している一部機種では可能です。

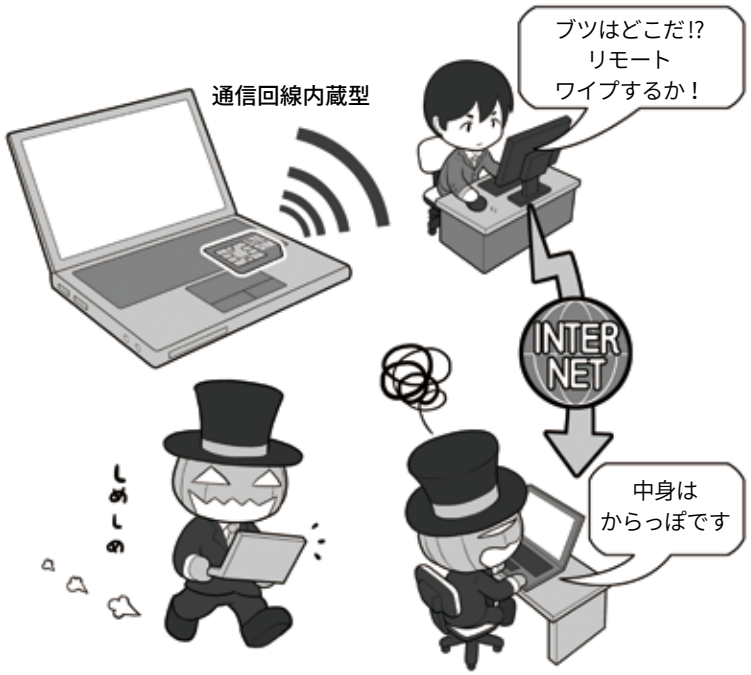
特にこういった用途を前提に開発をされている機種は、相手から電源が入っているように見えない状態でディスクの中身を初期化することもでき、重要情報を持ち出す必要がある場合は有効な防御手段となります。

またスマホほどの精度ではありませんが、こういったパソコンではGPS無しでも盗まれた機器の現在地を探索することができるので、置き忘れのままや届け出られてる場合は取りに行き、盗まれている場合は情報を添えて警察に相談しましょう。

盗難にそなえてのディスクの暗号化

TPMチップで暗号化されているディスクは、「暗号キー」が元の本体のTPMチップ内に残されているので、盗み出しての暗号化解除がさらに困難になります。

パソコンでもリモートワイプはある



業務用の一部機種では、起動をさとられないステルス状態でリモートワイプなどが可能です。盗んだ相手が気づく前に処置することができます。もちろん、そもそも盗まれないようにするのが第一ですが。

3 マルウェア感染に備え、3-2-1のバックアップ体制を整える

マルウェアの感染に負けない環境を整えるにはシステムやソフトウェアを最新の状態に保つこと、セキュリティソフトを導入し同様に最新の状態に保つことが重要です。しかしそれでも感染してしまった時、素早く復旧させる為には、定期的なバックアップが重要です。

バックアップは「3-2-1ルール」と言って、少なくとも3個の複製、2種類の記録メディアで、1個は遠い場所に保管する事を推奨します。具体的には、パソコン＋バックアップディスク＋クラウドサーバといった形です。

メインのバックアップディスクは外付けで、最低でも内蔵ディスクの3〜4倍の容量にして、何世代分かのバックアップを可能にすることが理想です。また昨今顕著になってきた、パソコンの中のファイルを勝手に暗号化し、解除するには身代金を要求するランサムウェアに備える為に「定期的にバックアップをしつつ、普段は本体に接続しておかない」という、やや煩雑な対応が必要です。こうすることでバックアップディスクもろとも暗号化される事を防げます。

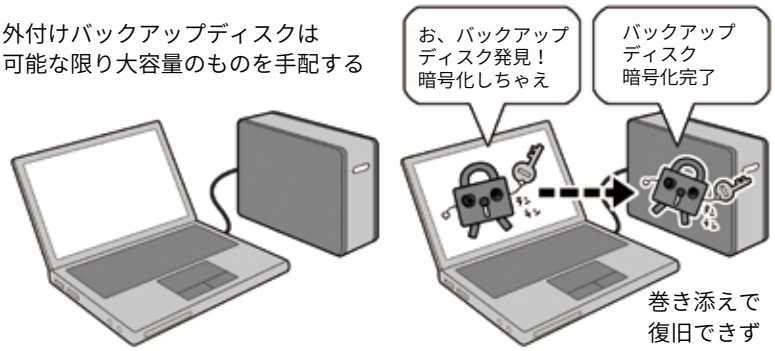
また特に重要なデータは、信頼できるクラウドサーバ上にセキュリティを固めた上でバックアップして、仮に自宅が水害などに遭っても、復旧できるようにしておきましょう。

ランサムウェアをはじめ、こういったマルウェアの感染源はネット経由だけだと思われがちですが、それだけとは限りません。

例えば仕事相手の会社の人から「資料をコピーしてくれ」と渡されたUSBメモリにマルウェアが仕込まれていたり、パーティでプレゼントされたデジタルカメラに仕込まれていたりというケースも実際に存在します。注意しましょう。

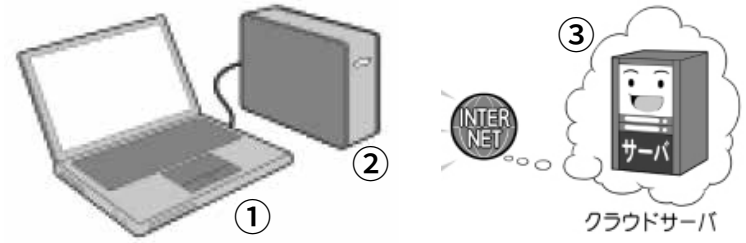
バックアップの体制を整える

外付けバックアップディスクは
可能な限り大容量のものを手配する



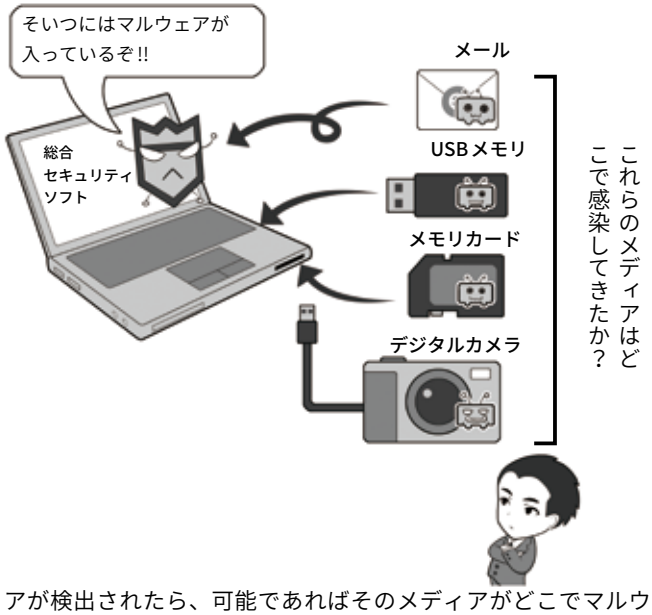
環境を整えたらバックアップを開始します。なにかソフトの導入や、環境を変更したらバックアップします。システムのアップデート後もバックアップします。ただしバックアップディスクを常に接続しておくとランサムウェア感染で巻き添えになって、復旧に使うためのデータも失われてしまいます。

バックアップは3媒体、2種類、1個は遠い場所



本体＋バックアップハードディスク＋クラウドサーバで条件を満たします。クラウドサーバは二段階認証で、攻撃者に乗っ取れないようにしましょう。

様々なマルウェア感染源に注意する



マルウェアが検出されたら、可能であればそのメディアがどこでマルウェアに感染してきたかを追跡して駆除します。

4 売却や廃棄するときはデータを消去する

スマホのセクションでも書きましたが、パソコンの廃棄にあたっても個人情報、メールや写真などの情報流出を防ぐために、内蔵ディスクに含まれるデータを確実に消去しなければなりません。

ハードディスクが正常に読み書きできる状態で、パソコン本体にディスク消去機能があるならそれを使い消去。無い場合は消去用のソフトウェアを利用。裸のディスクで保管していた場合などは本体に接続して消去するか、消去用の機器などを利用しましょう。

データの完全消去はディスク全域に無意味な情報を複数回書き込むことで、記録されていた情報の残留の可能性を消す方法が推奨されます。たとえば米国国防総省や軍などでは、この方式で3〜4回以上の繰り返し上書きによる完全消去が求められます。

なお、SSDはデータの管理方式がハードディスクとは異なるので、この方法では消えず、注意が必要です。専用ソフトや装置を使う必要があります。

一方、故障して正常に読み出せない、あるいはそもそも動作しないディスクの場合は、本体から取り出して物理的に破壊する必要があります。

有料ではありますが、家電量販店などに破壊サービスがあります。これらは自分が見えるところで破壊してくれるので安心です。

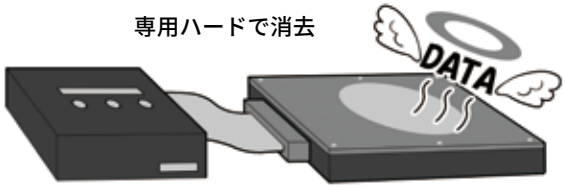
企業などで多量に廃棄する場合は、きちんと安全が確保された環境で、ディスクを読み出し不可能な状態に破壊するか、破壊用の専用機器やハードディスクやSSDでも粉砕出来るシュレッダーの導入も検討しましょう。情報漏洩防止の投資です。

ディスクの中のデータは確実に消去する

内蔵機能で消去

消去ソフトで消去

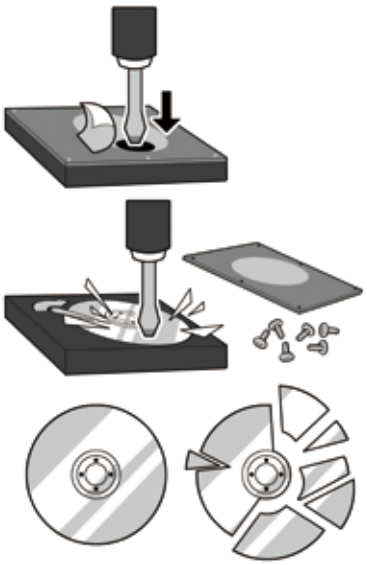
専用ハードで消去



最低3回以上の繰り返し消去(データ上書き)処理をするモードを選択します。

ディスクが読めなければ破壊する

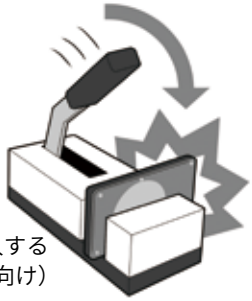
ハードディスクは破壊用の穴を使うか、分解してディスクを取り出し壊す



中のディスクを割るか、穴を開ける

目の前で破壊してくれる店に持ち込む(有料)

破壊用の機器を購入する(企業など向け)



ガラス製のディスクならば割れればOKです。金属製ならばドリルを利用して穴を開け読み出し不能にします。壊れて動かなくても、記録ディスクだけを他に移植して読み出すという手段があるので確実に破壊しましょう。SSDは中のメモリチップを物理的に破壊するのが理想です。

5 盗難や紛失のとき、スマホとパソコン、どっちが安全？

盗難や紛失という視点から見たときに、スマホとノートパソコンとデスクトップパソコン、どれがもっとも安全なのでしょう。

置かれている環境にもよりますが、「盗まれた後」までをその要素に入れて考えてみます。

図の通り、人目に付きやすいスマホは、平たく言えば盗みやすい。その代わり盗難時の不正なロック解除は困難。また基本的に通信機能があり、落とした後の位置情報の確認や盗まれたときのリモートロックやリモートワイプ機能といったセキュリティ機能が標準で備わってます。

ノートパソコンはログインパスワードの試行に制限が無い場合もあり。一方PINコードや指紋認証型もあり。盗難された場合に場所を特定し取り戻すにはLTEなどの「通信機能内蔵」が現実的な最低条件となり、現状ではほとんどの機種で利用できないので、盗難や紛失した後の探知が困難です。

デスクトップパソコンは基本的に屋内にあるので、空き巣に入られるのでもなければ盗まれたり人目についたりすることが少なく、また大きいので目立たないように持ち運びは困難。従って盗まれる機会が少ないで、盗難後の探知機能は必要ないといえばありません。また探知出来なくても代わりに、設置場所の戸締まりや監視カメラの設置で安全性を高められるので、その分は補えるでしょう。

結果として「実質的に盗難紛失時のリカバリ手段のないノートパソコン」が、盗難紛失に最もリスキーといえるかもしれません。

そうなった場合のために、せめてデータを読み出すことができない起動用パスワードやディスク暗号化の手段を講じておきましょう。

要素から安全性のポイントを検証する

	盗まれにくい	人の目につきにくい	ロック解除が困難	LTEなどの内蔵通信機能	GPSを使った位置情報	リモートロック リモートワイプ
スマホ（タブレット） 	×	×	○ 生体認証 PINコード 多数失敗でロック	○	○	○
ノートパソコン 	△	△	△ 失敗しても ロック無しも ○ 生体認証 PINコード	△※1	△※2	△※3
デスクトップパソコン 	○	○	△ 失敗しても ロック無しも	×	×	×

※1　LTEなどの無線WAN通信機能を内蔵しているものが対象
※2　LTEなど内蔵機のみ。ノートパソコンの場合はGPSが内蔵されていなくても、通信基地局を使ったおよその位置確認が可能な場合もある
※3　LTEなど内蔵機のみ。リモートロック、リモートワイプを本体起動していないように見せつつ行うには、専用に設計された機種のみ可能

コラム：ダブルラインでトラブルに備える

インターネットを閲覧していると、突然サーバが無反応になることがあります。そのときどうやって対処するのが良いのでしょう？

使用しているパソコンやスマホが原因なのか、無線LANか、それともウェブサーバ自身がダウンしているのか。それを、特定し別経路でのアクセスを確保するのです。

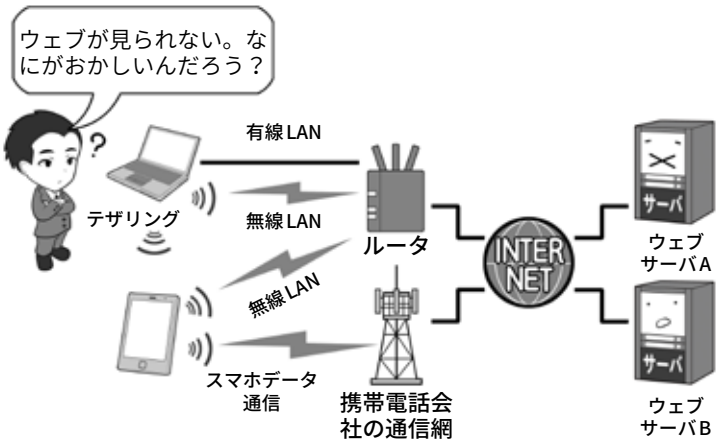
それには主要な機器の二重化(ダブルライン化)が有効です。パソコンで見られないならスマホで確認。無線LANがダメならば有線で。ルータがおかしいならLTEで、Aというサーバがダメならば Bへアクセスして、トラブルが解消した部位の機器を避けるなどの処置をしましょう。

また所有する特定の機器がマルウェアに感染したり、セキュリティホールが明らかになったアプリなどを避けてサービスを利用したりする場合も、同様の考え方になります。

特定の機種へのサイバー攻撃が流行っているなら別機種で、ウェブブラウザにセキュリティホールがあるなら別のブラウザで。問題があるものを避けて利用するわけです。

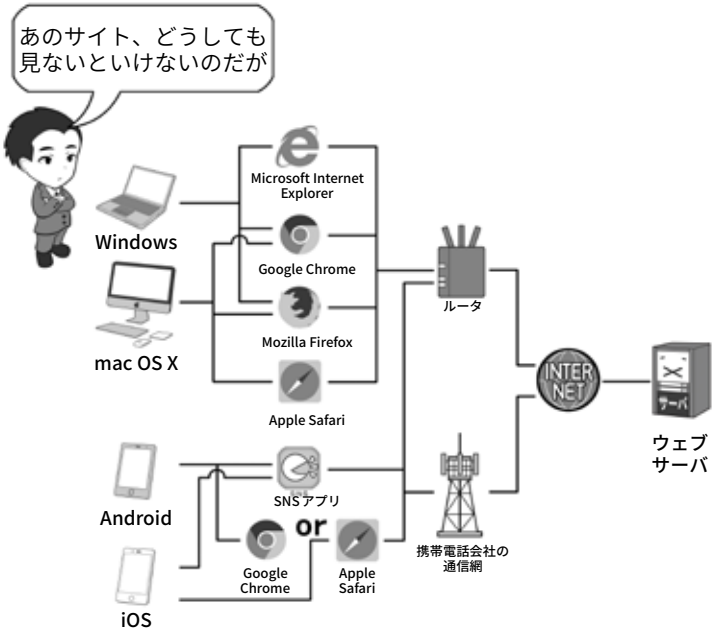
複数台の機材を持つ場合は、機材のタイプを分散することも備えとしては有効でしょう。生物界でも特定の品種に偏った生物は、一つの病気(ウイルスなど)で一気に絶滅に追い込まれる可能性があります。

通信状態がおかしいときに問題点を絞り込む手段



自分から見ると、インターネットのウェブサーバを見る機器、ルータまでの通信方法、インターネットまでの通信方法、そして目的のサーバまで切り替えることで、どの部分にトラブルがあるかを絞り込めます。なお全てを切り替えてもネットが表示されない場合は、しばらく時間をおいて確かめましょう。いずれかの場所で通信が集中し混雑して通信が出来なくなっている可能性があります。

パソコンがマルウェアに感染したり、ブラウザがセキュリティホールで使えないときの回避手段



Windowsにトラブルが発生したらmac OS Xで、特定のブラウザにトラブルが発生したら別のブラウザで、スマホのアプリにトラブルが発生したらウェブブラウザ経由で利用するなどの回避手段を設けるのも、一つの防御手段です。
ここでは簡略化して描いているため、上のイラストを含めインターネットの部分で二重化が収束してしまっているように見えますが、そもそもインターネットは通信経路上にあるサーバが攻撃で破壊されても、迂回して通信が確保されるようになっているので、通信が断絶するトラブルがあった場合、自然と迂回路が形成され通信が確保されるはずです。

雑草のような多様な環境を　作って、力強く備えましょう。

3 それでも攻撃を受けてしまったときの対処

1 兆候に気をつけて被害が出たら対処

ここまでお伝えしてきた内容を的確に実行してもらえれば、定型化されているかなりのサイバー攻撃は防げるでしょう。

しかしそれで安心してはいけません。人間の心の隙を突く攻撃を仕掛けられたり、セキュリティホールの発見に対してパッチなどの提供が間に合わない状態で、ゼロデイ攻撃を仕掛けられたら、防ぐことが難しいからです。

ですから、攻撃を受けたときの兆候を敏感に察知する能力を身につけ、これに対処するスキルを磨きましょう。

攻撃の兆候の中からいくつかの例を挙げてみます。

アカウントの乗っ取りは、知らないログイン通知やログインの履歴、ログインしている機器の一覧に知らないものがあったり、あるいはSNSで自分が知らない投稿やアプリ連携などがあります。

銀行口座関連も、ログイン通知があればそれを受け察知したり、通帳や取引履歴を見てチェック。クレジットカードはたとえ少額の送金であっても検証しましょう。

そしてマシンが乗っ取られている場合などは、動作が普段より遅かったり重かったりすることがあります。

もしマルウェアの感染の疑いや、アカウント乗っ取り、情報の流出や不正送金など、実害が判明した

セキュリティソフトが検知しなくても、兆候に敏感になれ

実被害が出ているときは証拠を保全して通報

LANケーブルは抜き、無線LANは本体もアクセスポイントもOFFにします。被害拡大防止になります。

原因究明までの緊急避難措置

感染したマシンでメールでの連絡や仕事のやりとりは×。感染経路やマルウェアの種類などが判明するまで、同一LAN内、同種の機器の利用も避けます。別の種類の機器、別の種類の回線を使います。家のパソコンが感染したら、スマホなどの通信回線を使用するなどの暫定的な回避策を行いましょう。

ら、とりあえずは有線でも無線でもネットにつながる回線を切断して本体の電源はそのままにして、証拠保全を図りましょう。通信を切断するのは拡散防止のためと外部の攻撃者との連絡を絶つためで、本体の電源を切らない理由はパソコンなどのメモリ上の証拠を消してしまわないためです。

その後、必要に応じて各種サービスに取引を一旦止めてもらう連絡をし、必要に応じて相談窓口などに連絡して対処方法を相談しましょう。実害があれば警察の担当部署に被害を出しましょう。

問題の解明やマルウェアの駆除が終わるまでは、連絡や仕事のやりとりは、感染したと思われる機器とは別種の機器を用いて行いましょう。同種の機種は同じLANに接続していたことで、感染し攻撃を受けている可能性が否定できないからです。

マルウェアが発見されただけで実害が出ていない場合、セキュリティソフトなどで駆除できる場合は駆除します。駆除できない場合は機器を初期化してバックアップから復元し、再びネットに接続して使用し始める前に、まずは感染や乗っ取りの原因と思われるものをクリアにしましょう。

システムやセキュリティソフトは最新の状態にし、不審なメール添付ファイルなどが原因だったならばメールを削除、セキュリティホールになりかねない古いものやサポートが切れたソフトやアプリはアンインストールし、アプリやサービス連携の棚卸(たなおろし)をして、知らないものを解除しましょう。

なおどこかからパスワードが流出した結果、ウェブサービスのアカウントを乗っ取られてパスワードを変えられてしまった場合は、自分で再設定は出来ないので、サービス側に連絡してアカウントを取り戻す処理をしてもらいましょう。

そしてこういったとき、何だかんだで一番頼りになるのが、ITに詳しい友だちだったりします。あなたが困っているときにその友だちが復旧を手伝ってくれたとしたら、いつかはあなたが「ITに詳しい友だち」になって、誰かを助ける番になってください。

一人また一人と、こういったセキュリティに詳しい人が増え、みんなでサイバー攻撃に立ち向かう姿勢が広まることは、きっとネットの安全を守る力になります。

実被害が出ていない場合

マルウェアの駆除

セキュリティソフトなどを最新にしてフルスキャンをかけて駆除します。

バックアップから復元

セキュリティソフトで対処できない場合は、本体を初期化してバックアップから復元します。

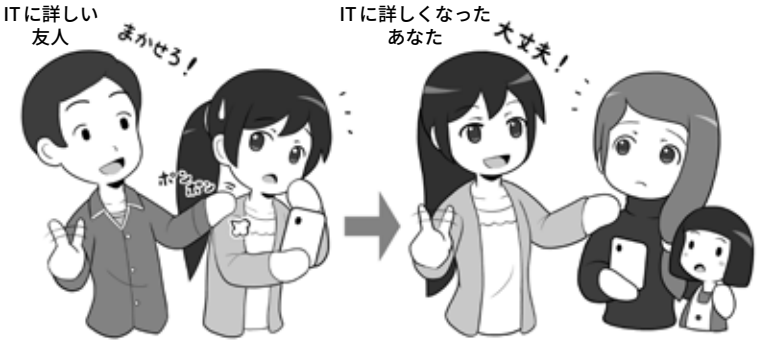
システムチェックする

古いソフト、サポート終了しているソフトおよびアプリは削除します。

サービスやアプリ連携の棚卸(たなおろし)

サービスの連携機能は見直しをします。

そんなとき頼りになるのは……



ITに詳しい友人に対処を手伝ってもらうとともに、一緒に勉強しましょう。その相手が動いてくれる時間には、労力分のお礼をすること忘れずに。
そして次のケースでは、あなたが困っている人に「ITに詳しい友だち」として手を差しのべて、力になってあげてください。

コラム：セキュリティの資格取得を目指そう

セキュリティについて深く知りたい、もっと詳しく学びたいと考えているのであれば、オススメしたいのが資格の取得を目指した勉強です。すでにセキュリティ関連の資格は数多く存在していて、自分自身のレベルや目的に合わせて選択できる環境が整っているほか、資格取得のための勉強を進めることで、体系立てて知識を獲得できるメリットがあります。

そうしたセキュリティ関連の資格として、比較的取り組みやすいものの1つに「情報セキュリティマネジメント試験」があります。これは脅威から継続的に組織を守るための基本的なスキルを認定する試験であり、業務で個人情報を取り扱ったり、情報管理を担当したりするすべての人を対象としています。情報セキュリティについて、基礎知識からバランスよく学習したいと考えているのであれば、まずはここからチャレンジするのも1つの方法です。

さらに高度な試験としては、「情報処理安全確保支援士」やグローバルで普及している「CISSP」(Certified Information Systems Security Professional)などがあります。情報処理安全確保支援士はサイバーセキュリティに関する実践的な知識や技能を有する専門人材の育成や確保を目的とした国家資格制度であり、情報セキュリティに関する高度な知識と技能を持つことを証明することができます。一方、CISSP は(ISC)^2(International Information Systems Security Certification Consortium)が認定を行う、国際的な情報セキュリティのプロフェッショナル認証資格です。これらの資格取得に向けた勉強を積み重ねれば、自身のスキルアップにもつながるでしょう。

数多くあるセキュリティ資格

現在、セキュリティに関する資格試験は数多くあり、自分のレベルや目的に合わせて取得することが可能です。情報セキュリティに特化した試験にチャレンジする前に、ITに関する全般的な知識が問われる「ITパスポート試験」を受けてみてもよいでしょう。そして支援士の「士」は騎士や武士の「士」。現代の騎士や武士としてセキュリティを守りましょう。

セキュリティを網羅的に学ぶことができる

資格取得を目指して勉強する大きなメリットは、その領域に関する知識を段階的かつ網羅的に学べることにあります。また自分の知識レベルを判断する上でも、こうした試験は大いに役立ちます。

第5章

SNSやインターネット関連の犯罪やトラブルから、自分や家族を守ろう。災害に備えよう

SNSやインターネットを使う上で、どんなふうにしたら自分や家族を守れるの？
具体的にどんなことが起こり、そのときどのようにしたら自分や家族を守ることができるのか、一緒に考えてみましょう。
海外での利用の注意点や、災害時に情報を生かしてどうやって身を守るかを知りましょう。

1 SNSやネットとのつきあい方、守り方

1 SNSやネットの楽しみと気をつけること

私たちはインターネットの普及により、「距離の移動に必要な時間が消えた世界」を手に入れることができました。

昔であれば遠い国の人と連絡を取り合うには、手紙を書いて何週間も返事を待ったり、電話をかけるにしても料金が高く気軽にかけられなかったり、あるいは顔を見るために旅行するにしても大変な手間とお金がかかったものです。

しかし今では、まるで隣に座っているかのようにチャットしたり、SNSで写真を送り合ったり、映像つきのインターネット電話を使えば無料で顔を見ながらコミュニケーションができます。

そしてIT技術の進歩は言葉の壁すらも崩しつつあります。まるで世界が一つになったような時代が訪れ、人の意識そのものが変わっていくかもしれません。

一方、あなたが世界中の人にメッセージを発信するとき、それを受け取る人々の中には悪意を持った人がいることも忘れてはなりません。ネットを使ったコミュニケーションは人と人の意識の繋がり合いを容易にしますが、同時に自分の意識の壁の中に、そういった悪意をもった人間がするりと入ってきやすくなることでもあるのです。

私たちはネットの世界をよく知って「この時代に合わせた、新しいつきあい方」を作り上げなければならないでしょう。悪意のあるものを鋭く見分けて、善意のコミュニケーションの世界を作っていくことができるように。

ネットやSNSによるコミュニケーション

ネットやSNSで、距離を超えて世界とつながることができます。そして時間を越えて様々なことを知ることもできるのです。

ネットには落とし穴もある

あなたのなに気ない投稿は、皆の共感を得るかもしれませんが、その「皆」の中には、犯罪に使える手がかりを探している悪意を持った人もいることを知りましょう。どうしたら悪意をかわしつつ、ネットを楽しむことができますか？

2 SNSやネットの怖さ、こんなことが実際に起こっている

ではSNSやネットではどのようなトラブルに遭う可能性があるのでしょう。

SNSなどで実際に会ったことがない同じ年ぐらいの子と友だちになり、どこかで会う約束をしたとします。しかし待ち合わせ場所に行ってみると来たのは本人ではなくて別の人でした。「○○ちゃんが待っているから連れて行ってあげる」と言われ、車に乗せられそうになりました。こんな風に誘拐や略取が行われます。

SNSに家の近くや普段立ち寄る場所、自分の写真などを上げていると、その情報からあなたを特定して、リアルのストーカーがやってくるかもしれません。

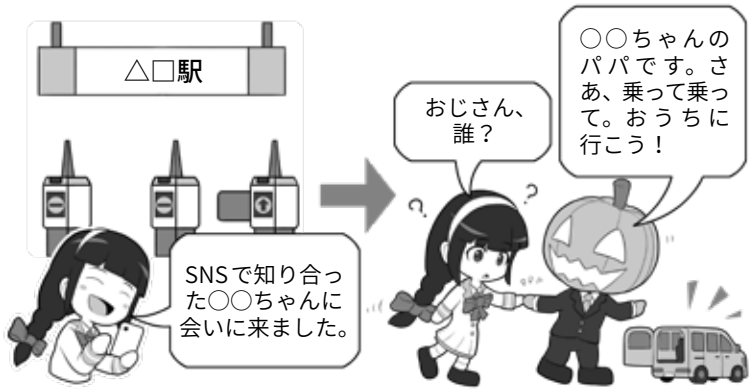
闇サイトなどを興味本位に覗いたりしていると、犯罪勧誘といって、顔も知らない人があなたを犯罪に誘ってくることもあります。

SNSのグループなどで、周りの雰囲気に流され、特定の人物のありもしない書き込みに同調したり、傷つけたり、仲間はずれにしたりする「ネットいじめ」をしたりされたりしてしまうかもしれません。

つきあっている相手が「誰にも渡さないから」とあなたの裸の写真を要求してきて、信頼して渡したら、別れた後にその画像がネットに流出してしまうかも。それは「リベンジポルノ」といって、相手が嫌がらせのために、写真をネットに投稿する行為ですが、他にも相手のスマホがマルウェアに感染して流出してしまうかもしれません。その写真は消えない「デジタルタトゥー」（デジタルの入れ墨）として、以降あなたの人生に、ずっと影を落とし続けることになるかもしれません。

この他にもSNSやネットでは様々なトラブルが発生することがあります。トラブルのことをよく知って、決して巻き込まれないようにしましょう。

誘拐や略取



ストーカー

SNSで得た情報をもとに人物を特定し、リアルの世界でストーカーされる場合もあります。

犯罪勧誘

闇サイトなどと呼ばれる怪しいサイトで、面識がない者同士が集まって、犯罪を行うために仲間を探しています。

ネットいじめ

ノリでいじめに加わった結果、悲しい出来事が起きてしまったら、自分はその時どう思うでしょう。

リベンジポルノ・デジタルタトゥー

元交際相手に、裸の写真をネットに投稿されるかも。ネットに広がった写真は消すことができません。

3 SNSやネットとのつきあい方の基本

自分からネットの怪しげな場所に近づかないなら、日常的に注意しなければならないのは、システムなどを最新の状態に保ちサイバー攻撃を受けないようにすることと、SNSやネットで悪意がある人に個人情報や画像が渡り、あなた自身が狙われたり、攻撃の対象にならないよう、投稿する内容には気をつけることです。

たとえばSNSを利用する場合、個人情報はサービスの規約などで求められるもの以上は記入しないようにしましょう。その上で投稿の標準設定は、友だち限定にしましょう。その他個人情報を守る仕組みが提供されている場合は、それらを有効活用しましょう。

実際に会ったことがない人が突然お友だちになりたいと言ってきても、即座にOKせず家族などに相談しましょう。誰かの友だちならば、実際に会った時の印象や、どういった人かを教えてもらって検討の材料にしましょう。またその人の過去の発言などを良く見て、二面性などを含め判断しましょう。

そして一度も会ったことがないのに、本名や連絡先をたずねたり、いきなり実際に会おうなどと誘ってきたりしたときは、基本的にお断りしましょう。文化活動や物の売買など、何らかのきちんとした理由で会う必要があるときは、大人や保護者同伴で行き、その際でも本名や住所などは極力教えないようにしましょう。

SNSやネットへ投稿をする場合は、普段の立ち回り先や生活のパターンの情報などは避けるようにしましょう。些細なことですが、一枚の写真に写っている背景だけで、自宅を特定される場合もあるので注意しましょう。

個人情報は基本的に公開しない

一度流出した個人情報は絶対にネットから消し去ることができませんし、ときに個人の居場所を特定する情報になります。悪意がある人にとって、手がかりになる情報はネットに載せないようにします。

会ったことがない人とむやみに友だちにならない

会ったことない人が友だちになろうと近づいてくるときは、その中に悪意をもったものがいることを知りましょう。基本的には友だちにならず、必要ならよく吟味したり、相手について調べたりしてから判断しましょう。

現実世界で会おうとする人を警戒する。出会い系に近づかない

実際に会ったことがない人は、プロフィールの年齢や性別が本当なのかわかりませんし、これを偽って近づいてきた人と会い、被害に遭った例もあります。またよく事件が起こる出会い系サイトなどには、絶対に近づかないようにしましょう。

個人が特定される情報はSNSなどに投稿しない

自分自身の写真や日常的な生活圏がわかる情報を投稿しないようにしましょう。友人のみに公開としていても、その人が共有したら一般に公開されることもあります。またデジカメで「位置情報あり」で撮影していると、見えなくても写真に位置情報が記録されるので注意しましょう。

4 存在するデータは流出することがある。流出したら消すことは難しい

個人情報や写真も、スマホなどの中から出さなければ大丈夫じゃないかと思われるかもしれませんが、望まない情報流出の罠は、様々なところに隠れています。

スマホやパソコンの中に存在しているデータは、写真でもメールでも住所録でも、すべてマルウェアの感染などによって流出する可能性があります。

自分がセキュリティについて学んでそういった可能性が少なくなったとしても、現状ではサイバー攻撃を完璧に防ぐことは出来ないので油断してはいけません。

それに、たとえば信頼できる友人に秘密の写真をシェアしたあと、その友人のスマホなどがマルウェアに感染して流出する可能性もあります。

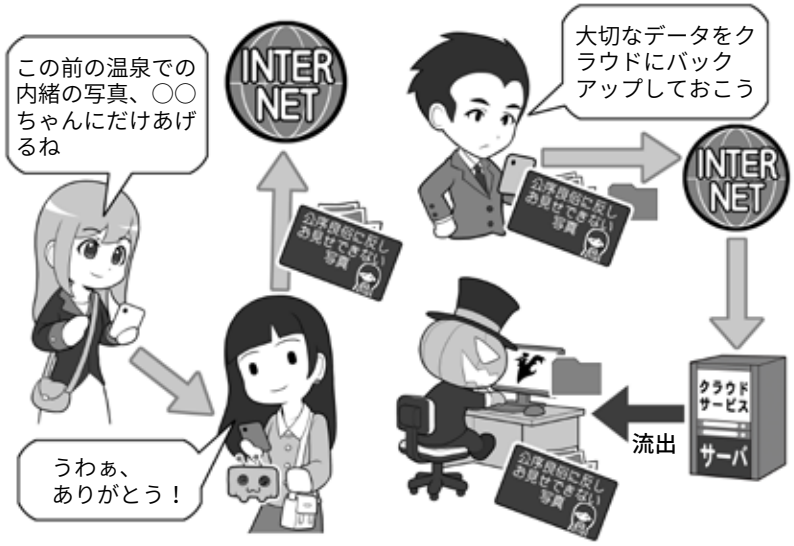
相手が自分と同じレベルのセキュリティ知識を持ち、実践しているとは限らないですし、またそれを強要もできません。

さらに秘密の写真などをクラウドサービスにバックアップした場合、データが自分の手元と他人の管理下に複数存在するため、少なくとも2カ所から流出する可能性が存在するようになります。事実クラウドからセレブの写真が流出する事件も発生しています。

問題がある画像は何かという事に関する意識の差でも問題は起こります。たとえば若気の至りで公序良俗に反することをして、これをその場ののりでSNSに投稿したとします。その写真が大炎上を起こしたとしたら、もしかしたらあなたの人生のあらゆる局面での歩みを妨げるものとなってしまうかもしれません。

流出したら問題になることは、しない、させない、(助長する意味ではなく)撮らない、投稿しないようにしましょう。

存在するデータは必ず流出すると考える



自分が流出させなくても、渡した相手がマルウェアに感染して流出してしまうかもしれません。

パスワードの使い回しなどで、クラウドサービスからデータを抜かれて流出してしまうかもしれません。

投稿したデータは一生ついてまわるかも

上記は極端な例ですが、たとえ若気の至りが少年法によって許されて、その後、裁判所などに申し立ててプロバイダーに情報の削除の依頼をしても、ネットに拡散した情報の全てを消し去ることはできず、人生の節目であなたを苛むかもしれません。まず問題になることはしないことです。そして、(助長する意味ではなく)ネットに投稿するものはよく考えてから投稿しましょう。

コラム：子どもにスマホを持たせる時、「スマホ契約書」という提案

子どもがスマートフォンを使いたいと要望してきたので、人生の課題を設定してそれをクリアしたら契約書付きで提供するようにしたというニュースがありました。

契約書というと物々しいですが、スマホ利用のルールを口頭ではなくきちんと明文化し、それをお互いが確認し合うことで、利用する子ども自身も「それをないがしろにしてはいけない事だ」ということを強く認識するというわけです。厳しいという意見もあると同時に、一歩階段を上り大人として扱われたことを喜ぶ子ども自身の意見もあるようです。

契約書の内容は「家族からの連絡にきちんと返信すること」や、「朝受け取って夜親に返すこと」、「実際に会ったことがない人はアプリで友だちにならないこと」などがあります。

またSNSを使ったトラブルになりそうな「面と向かって言わないことはSNSでも言わないこと」とか、海外の例では「恥ずかしい写真を交換したいと言われてもやってはいけない」といった項目もありました。これはSNS上での炎上の芽を摘んだり、未成年が同年代になりすました人間に裸の写真を要求された上で脅されたり、あるいは同級生同士で交換したものが流出したりする、セクスティングなどを未然に防ぐ意味で重要です。

口約束は忘れてしまいやすい？

ルールは決めても、口約束だけで見返せないと、あやふやになってしまいがちです。結果的に感情的なやりとりを生みます。

契約書を作り、責任ある人として接する

契約書は固いイメージもありますが、ルールを時々見返したり、言った言わないにならないメリットもあります。なにより相手を責任ある人間としてあつかうことで、ルールを自ら決めたことと自律を促しましょう。

それと同時に、インターネット上の情報は必ずしも正しいとは言えず、フェイクニュースやデマが存在すること、情報は裏を取って初めて本当の情報となること、時にスマホを置いて現実の世界へと飛び出し、自然や様々な動物に興味を持つことなどを書いた項目もありました。

些細なことですが、夜になったら親に返し、朝になったら渡してもらうといった項目は、友だちとメッセージをやり取りして眠れない、勝手に眠ると仲間はずれにされるといったことにして、「うちは夜になると親に返さないといけないからごめんね」とスパッと言え、一つの良い対処方法でもあると言えるでしょう。

「スマホ　契約書」で検索して、実際の契約書や記事を見てください。スマホのルール作りの一助になるかもしれません。

コラム：GPS、位置情報、ジオタグの管理

私たちが普段何気なく使っているスマホは、実は相当に高機能で、10数年前ならばすべて別々の機器だったものが、まとまって小さなボディに収まっています。

たとえば電話、音楽プレイヤー、デジカメ、ビデオカメラ、そしてGPSレシーバーなど。

とくに昔はGPS衛星からの電波をキャッチして、緯度経度で構成される位置情報を測るには、ごつい専用のレシーバーが必要でした。今はスマホの地図アプリを開いて「現在地」と押せば、即座に自分がいる場所を示してくれます。

しかし便利になった代わりに、油断すると意図せずこういった情報を公開してしまっていることもあります。

たとえばスマホで写真を撮影するときに位置情報を記録するようにしておくと、撮影場所の情報が「ジオタグ」という形で保存されます。

ジオタグが記録されている写真を写真アプリなどで見返すと、地図上の撮影したポイントに写真を配置してみることができ、時系列順に並んだたくさんの写真からわざわざめくって探さなくても、思い出の場所で撮った写真を即座に見つけることができます。

しかし写真にジオタグをつけたままSNSに投稿すると、SNSによっては撮影場所が公開されてしまうことがあります。たとえばその写真が自宅で撮影したものだったりすると、広く一般に自宅の場所が公開されてしまうわけです。

また位置情報はSNSの投稿時に位置情報を公開する設定にしておくと、文字だけの投稿をしたつもりでも、その投稿を行った場所が公開されてしまいます。

生活圏の位置情報を公開してしまうトラブルは、GPSにまつわるものだけではなく、たとえば普段立ち寄る店の名前を投稿したり、場所が特定できる写真を投稿したりするだけで、いともたやすく「撮影場所が特定される」ことがあります。

そしてこれらの「位置情報」もしくは「位置情報に相当する情報」は、ストーカーにとっては絶好の手がかりになります。

ネットは知らない人と「距離と移動に必要な時間」を超えて知り合える場所ですが、トラブルが発生すればそれは現実世界の我が身に即座に襲いかかってきます。

位置情報を含む個人情報の管理はしっかり行いましょう。

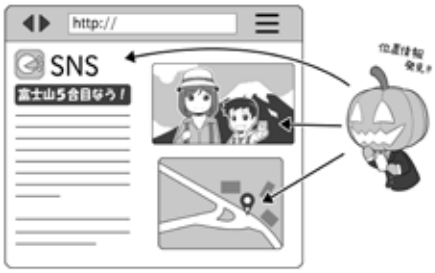
写真には位置情報が含まれることも

スマホによっては購入時の設定で、写真に位置情報を記録するようになっている場合もあります。必要なければ機能をOFFにしましょう。

位置情報は思い出を見返すのに便利

画像アプリによっては地図上に写真がドロップされ、思い出の場所を拡大すると、そこで撮影した写真を見ることができます。写真を一から探さなくて良いので便利です。

位置情報はストーカーの手がかりになる



写真に付加された位置情報、投稿時の位置情報だけでなく、場所の名前や、場所が特定できる写真からはあなたの居場所が分かります。ストーカーにとっては絶好の手がかりになるので、投稿前に必ずチェックしましょう。

コラム：SNSやSNSのグループを使ったいじめに備える（いじめ経験者からのアドバイス）

いじめは公共の目がある場よりも、人々の目が届きにくい比較的閉鎖された空間で起こりやすく、学校はときにその条件に当てはまります。

ネットが普及する以前であれば、コミュニケーションは言葉や暴力など、実際の行動となって現れていたので、それでもまだ目につく可能性がありました。

しかしネットの普及によって、そのいじめの一部がSNS上で匿名で、あるいはSNSの外から見えないグループ内で行われるようになると、いじめの実状を目にする方法が少なくなりました。

また昔であれば学校から離れた別のコミュニティをもつことで、自分が自分らしくいられる場所を確保し、バランスを保つことが出来ました。今はスマホを始終持ち歩くので、学校から離れ別のコミュニティに行き、スイッチを切り替えることも難しくなります。スマホを持っているとそれを通じて四六時中、学校のコミュニティに繋がり続け、その中でのいじめは生活すべてにおいて、その影を落とし続けてしまうからです。

物理的ないじめはもちろん、SNSやネットを使ったいじめを受けているときは親に相談し、画面キャプチャーやコピー、録音などで証拠を集め、それを添えて恐れずに、専門の窓口に相談しましょう。

また学校以外の自分の居場所やコミュニティをもつことで、「学校の中の自分ではない自分」という時間をもち、その中でのアイデンティティを確立しましょう。

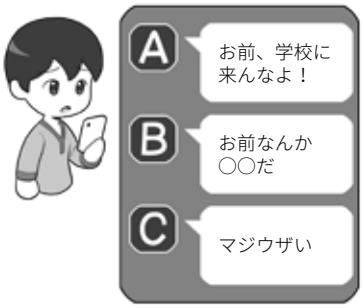
いじめに遭うのは辛いことですが、自分が否定されない別の空間をもつことができれば、心を休める場所と時間をもてます。その場所にいるときは、いっそスマホの電源をOFFにして、目の前に集中して過ごしてみましょう。

（空手道場で生き延びられたNISCのおじさんより）

いじめは閉鎖された場所で起きやすい

公共の空間では人の目がある

ネットも他人から見えにくい



人の目は時に抑止力になりますが、ネットの中は人目が少なく、その分いじめは陰湿でエスカレートしがちです。

証拠を集めて相談しよう

いじめの告発をするときは、きちんと証拠がある方がトラブルの説明がしやすくなります。

自分らしくいられる別の場所をもとう

ネットに関係がない場所を探して、学校以外に自分の居場所を作りましょう。

コラム：モラルを逸脱すると炎上を生む

ネットのニュースなどを見ていると、「炎上」という言葉を良く目にします。

炎上とは特定の人物がSNSなどに投稿した内容が不適切であるとして拡散され、多くの人から集中的に非難を受けることを指します。

たとえば特定のお店に関して言いがかりのような投稿や嘘の書き込みをしたり、飲食店などで働いている人が芸能人のプライベートでの来店を投稿したり、引っ越し業者が業務上知り得た情報で引っ越した女性にアプローチをしたり、あるいは未成年が飲酒ありの大宴会をした投稿をするなどなど。

多くの場合は世間一般の「モラル」に照らし合わせて、おかしいと思われるものに対して炎上は発生します。

問題はその炎上の結果、炎上させた本人が非難されるだけで無く、嫌がらせをされたお店が閉店してしまったり、雇っていた会社が謝罪したりと、周辺に多大なる影響を及ぼしたり、また本人にも損害賠償責任が発生したり、名誉棄損で訴えられたり、内定が取り消しになったりということが起こる点です。

この「炎上」をおこさないためには、投稿する人が「世間とのモラルと自分の意識のギャップを埋める」か、「投稿をしないか」しか解決策はありません。

ネットで炎上を見たらその顛末を見て、どのような書き込みがどのような経緯で炎上を生み、どのような結果を招くか、どこに意識のずれがあったのか調べてみましょう。

またネットの掲示板などを利用して、自分の投稿を多人数のふりをしてはやす「自作自演」や、焚きつけるアオリ行為、誰かのふりをするなりすましの書き込みなども、状況によっては犯罪や名誉棄損の対象となる場合があります。

「こんなことになると思わなかった」という言い訳は昔からよく聞きますが、そう言ったところでもとには戻りません。現実世界とネットでのコミュニケーションの差、SNSの情報拡散の特徴などを、興味を持って調べて、騒がしくない穏やかな生活を送って下さい。

モラルを逸脱することが炎上を生む

自作自演やアオリ行為、嘘の書き込み

コラム：屋外でのゲームを安全に楽しむ。ながらスマホは×！

ここ数年のスマホのパワーアップにより、昔ならば専用ゲーム機が必要だった複雑なゲームでも、スマホで軽く動かせるようになりました。

それに伴い、従来から存在していた「位置情報ゲーム」と呼ばれるジャンルに、リアルタイムの地図情報や動く3Dキャラクター、カメラ映像にAR（拡張現実）を重ねたものも登場してきました。

スマホを持って現実世界に飛び出してモンスターを捕獲したり、様々な場所に行ってご当地でアニメキャラクターと写真を撮ったり、あるいは全国の駅を巡るといったゲームが登場しています。

そういったゲームでは、みんなが安全に楽しく遊び、幸せになるために守らなければならないルールがあります。

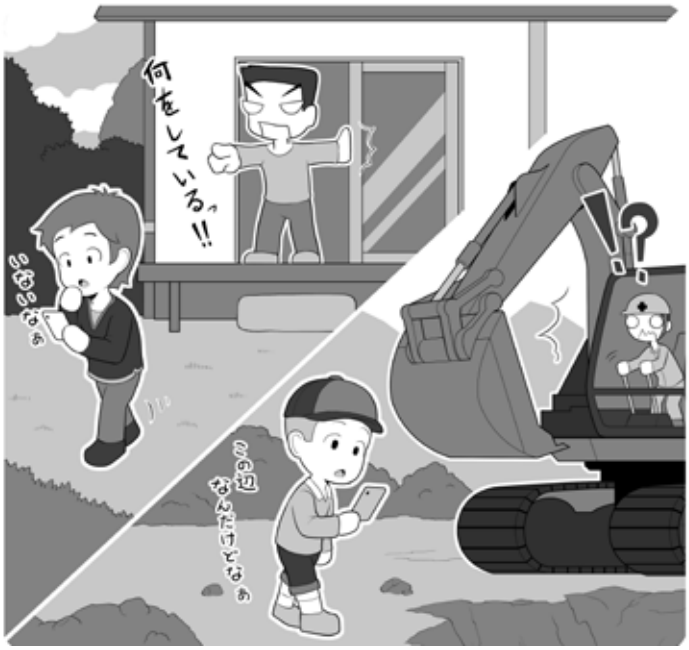
まず、屋外でゲームをするとき「ながらスマホ」をするのは危険です。場所やものを探すゲームでは、ついついスマホの画面を見ながら歩いてしまいますが、わずかの時間スマホを見つめているだけで誰かにぶつかったり、線路に落ちそうになったり、車にはねられそうになったりすることはありえます。また、わざとぶつかってくる「スマホ当たり屋」によって怪我をしたり、難癖をつけられ金銭を要求されるということも起こっています。

移動中は画面を見ずに遊べ

歩きスマホは自分も周りの人も危険

自分は大丈夫と思っていても、歩きスマホは大変危険な行為です。歩いていても車道にでて事故に遭ったり、駅のホームから落下することもあります。また歩きスマホをしている人を避けようとして、自転車や車に乗っている人が事故を起こしてしまう可能性もあります。歩きスマホはやめましょう。

私有地や危険な場所には入らない



スマホを使ったゲームをしてると、それに集中するばかりに、危険な場所に立ち入ったり、他人の家の敷地の中に入ってしまうこともあります。危険な場所での事故や、海外では発砲トラブルも起きています。ゲームはゲーム、命をかけるものではなく、楽しむものです。モラルを持って楽しみましょう。

る方法が提供されていることもあるので、よく調べてみましょう。

また自転車を運転しながらの操作や、当然のことながら自動車を運転中のスマホ操作は論外です。周りをよく見ないで運転する乗り物は、周りからすると命を奪いかねない大変な脅威ですし、条例や法律に違反する場合もあります。

またゲームに熱中していて誰かの家の敷地や私有地に入り込んでしまうと、これは「不法侵入」に当たります。

ただそういった不法行為の問題としてではなく、単純に「自分の家の庭に、知らない人が入ってきたらびっくりするよね」というように、相手の立場に立って考えましょう。そういった考え方ができるようになれば、他のシチュエーションでも生かせるはずです。

自分の街にたくさん人が来て賑わうのはウェルカムですが、迷惑行為があると「もう来なくてよい」となり、誰もハッピーになりません。

また危険な場所に入り込んでケガをすれば、救助する人員や救急車、場合によってはヘリコプターが必要になります。常識的に考えて、その場所が危険であると思われるなら、例えゲームのプレイエリアが設定されていても、近づかないようにしましょう。

こういったモラルや安全を守りながら楽しめるなら、現実世界でプレイするゲームは様々な場所にたくさんの人を呼び、ときには災害に遭った地域の復興支援にも役立つことがあります。

それが成功するかどうかは、みなさんに心持ちひとつにかかっていますよ。

運転中のスマホはダメ。車は凶器になります

運転中のながらスマホは違反です。運転している車はルールを守って使わないと一瞬で人の命を奪う凶器になるということを考えましょう。

位置ゲームを活用すれば、いいこともあるよ

スマホを使った位置ゲームは、上手く使えば地域活性化や復興支援に使える素晴らしいアイテムです。安全に使い、安全に楽しみ、そしてゲームとともに様々な場所を巡って、旅を楽しみましょう。

2 サイバー関連でやってはいけないこと

1 アニメ・マンガ・音楽の違法なシェア。パクリなどの著作権侵害

インターネットは基本的に様々なものを共有する場です。しかし、著作権者の許可を得ずに、ネットにアップロードされた、映画、アニメ、テレビ番組、音楽、マンガなどの作品を、そうと知ってダウンロードするのは違法行為です。

また、同様に上記のような作品を、著作権者の許可を得ずにインターネットサーバにアップロードして配信する行為も違法です。

違法アップロード、ダウンロードは作品が生み出される環境を破壊し、結果として作品が生まれなくなります。許可を得て公開されているものを利用しましょう。

こういった違法行為以外にも、ネットでは「パクリ」といわれるカジュアルな著作権侵害がよく行われています。

たとえば他人がSNSに投稿した写真や文章を、自分のもののふりをして勝手に投稿するのは著作権侵害ですし、SNSによっては利用規約違反になりアカウントを停止される場合もあります。

また他人がウェブで発表した小説や写真などの、一部もしくは全部を自分のもののように偽って公開することも著作権侵害です。

パクリで一瞬だけ注目を集めても、いずれ身元が特定されるなどして「パクった人だ」とネットに記録されてしまうでしょう。

ネットには距離が存在しない分、今まで会うことができなかった人に作品を届られる世界です。誰かの作品ではなく自ら作品を生み出して世界に届けましょう。

違法アップロード、ダウンロードは刑罰の対象にも……

＊1：有料の作品が違法にアップロードされているものと知っていた場合

他人の投稿や作品を盗む「パクリ」

2 ゲームの不正行為。恋人や家族でもプライバシーは守る

ゲームの不正コピーやチート行為もやってはいけないことです。

それ自身、規約違反で場合によっては犯罪として摘発されますし、「自分ひとりぐらいやっていても大丈夫」という人たちが増えていけば、楽しんでいるゲームそのものが生まれてくる環境を破壊してしまうことになります。

ゲームを作る人はゲームを売ることで利益を上げ、生活をし、また新しいゲームを世の中に生み出してくれます。この利益の循環があるからこそ、ゲームを遊ぶ側は楽しい時間を過ごせるのです。

しかし誰かが不正行為でこの「利益の循環」を回らなくしてしまうと、やがてゲームを作る人々は生活できなくなり、結果としてゲームがこの世に生み出されなくなってしまいます。

楽しみのある世界がいいですか？　ない世界がいいですか？　私たちは信頼関係をもって楽しい世界を盛り上げていく人たちが大好きです。

信頼関係は普段の生活でも大切です。例えばプライバシー。あなたが席を立っている間に勝手にスマホの中身を見られてしまったり、あるいは親があなたの部屋に勝手に入り込んで、パソコンに保存している日記を見ていたらどうでしょう。特に「信頼している」人の行為は人を深く傷付けます。

また「信頼関係」の名のもとに自分のプライバシーを守ってほしかったら、自分も誰かにとって、信頼を裏切らない人物にならなければいけません。

ゲームの不正行為は犯罪になることも…

不正コピー、チート行為、RMT（リアルマネートレード）など、ゲームの販売や運営を妨げたりする行為は、場合によっては犯罪として摘発されますが、それよりも積もり積もってゲームを生み出す会社やシステムの崩壊を引き起こしてしまうことが問題です。その結果、皆が楽しめる世界が奪われてしまうのです。利用者を信頼している制作者の人たちを裏切ってはいけません。

恋人や家族の間でも信頼関係は大事、でしょ

たとえば、あなたの恋人や親がスマホの中を勝手に見たり、内緒でパソコンを開いて勝手に日記を見ていたりしたら、信頼関係はなくなってギスギスしてしまうでしょう。それにスマホやパソコンに対する安心感を失ってしまうかもしれません。自分が「信頼」を守ってほしいと考えるなら、相手に対しても守らないとフェアではありません。信頼を守って笑顔の関係を作りましょう。

というようなことを、真顔でいちいち言われるよりも、お互いのことを思い合って、信頼し合い、笑顔で生活できる社会になった方が良いですよね。「いい笑顔」を守りましょう。

3 クラッキングはクールじゃない！

インターネット上には「ダークウェブ」という、通常は見ることがないネットの陰の部分が確かにあります。そこにはアングラなありとあらゆるものを売るマーケットが存在し、悪意のハッカーがクラッキング用のツールを売っていたり、DDoS攻撃のためのゾンビ化した機器群を時間あたりいくらで貸し出したりもしています。

近年、若い子どもたちがここに足を踏み入れ「インターネットは匿名だからばれないだろう」とツールを購入したり入手したりして、ランサムウェアによるサイバー攻撃や不正送金などを行い逮捕された例もあります。

では果たしてそれは本当にばれないのでしょうか。

インターネットは当初悪意が存在することを想定していない空間でした。しかしそこに悪意が芽生え、犯罪に利用されるようになり、各国の捜査機関も日々こういった犯罪に対応する技術力を向上させています。

事実「そういう事件があった」と報道されるのは、匿名でばれないと思った者たちを、捜査機関が地道な解析などで追い詰め、犯人を特定しているからです。

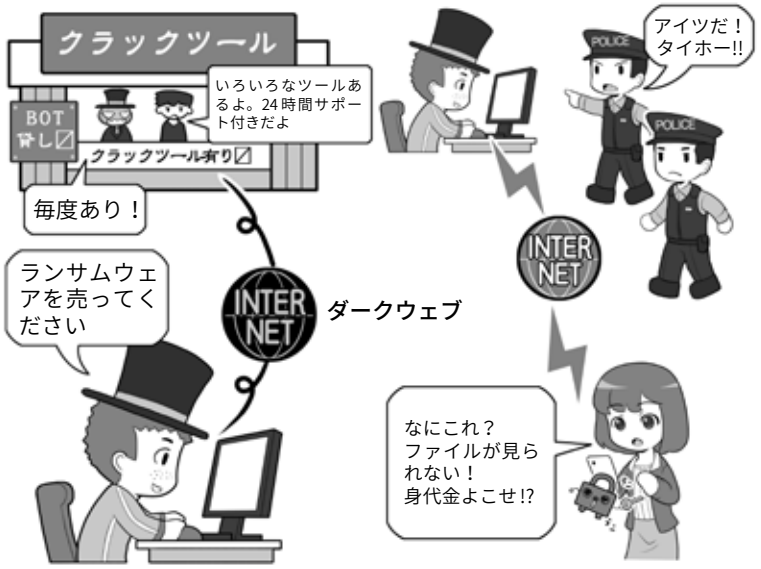
「有名になりたかった」「腕試しをしたかった」「小遣い稼ぎで」

そういう言い訳をしつつクラッキングを行っても、しょせんは自己満足であって、その行為は誰もハッピーにしません。有名になったところで、その悪名がネットに刻まれるだけで誰も尊敬はしてくれません。実名が流出して、その後の人生にずっと影響しつづけることだってあるのです。

それよりも腕と技術力で多くの人々をハッピーにし、ネットの偉人として名前を刻む方が「かっこいい」でしょう？

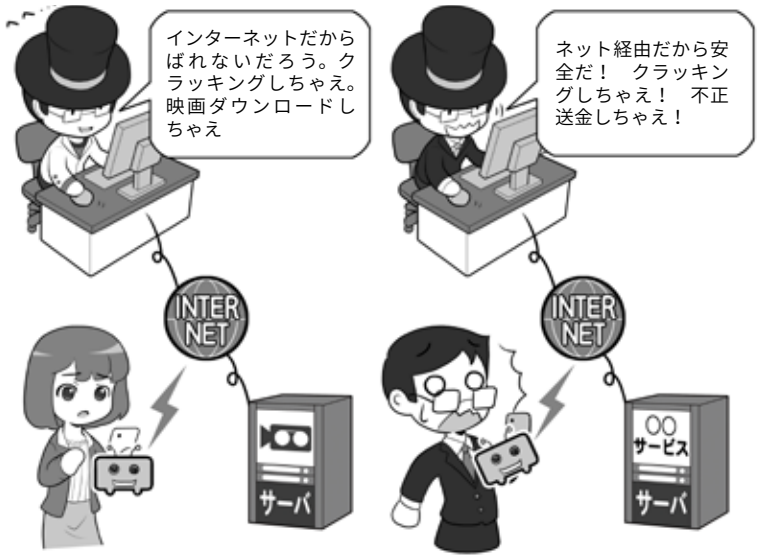
ネットでは現実よりも名前が長く残るかもしれませんよ。

クラッキングツールに手を出さない



現実世界でもネットでも、広く知られている「安全でない場所」や「怪しい場所」は、当然のことながら捜査する側もよく調べ、必要ならば対策を講じています。「匿名性が高い」はずなのに「捕まったこと」が記事になるということは、なにを意味するでしょう？ネットでも危険場所には近づかないようにしましょう。

インターネットだからばれないと思うのは……



本人は軽い気持ちで始めているつもりでも、クラッキングは様々な法律や利用規約に違反します。そして見つからないと思っていても、現実世界に生きる私たちは、現実世界に生きている痕跡を完璧に消すことはできません。

コラム：法律に違反することをしてはいけません。気軽に考えてはダメ

サイバー犯罪というとそれなりの年齢の悪意のハッカーを想像するかもしれませんが、非常に幼い子ども達が行い児童相談所に通告されたり、未成年が書類送検されたりしている事件もあります。

見てはいけないサイト、危険なサイトをフィルタリングするだけでなく、コンピュータやスマホを使う際、どういうことをしてはいけないのか、きちんと家族で話し合っておく必要があります。下記の例などを参考に事例を調べて、共有してみてください。

他人のアカウントへの不正なログインや乗っとりをした場合

不正アクセス禁止法
不正アクセス行為の禁止

第三条、第十一条
→三年以下の懲役又は
百万円以下の罰金

コンピュータウイルスの作成や保管をした場合

刑法
不正指令電磁的記録作成等

（作成、提供、供用）
第百六十八条のニ
→三年以下の懲役又は
五十万円以下の罰金

（取得、保管）
第百六十八条の三
→二年以下の懲役又は
三十万円以下の罰金

児童ポルノの所持・提供をした場合

児童買春、児童ポルノ禁止法
児童ポルノ所持、提供等

（所持）
第七条第一項
→一年以下の懲役又は
百万円以下の罰金

（特定少数者への提供）
第七条第二項
→三年以下の懲役又は
三百万円以下の罰金

● アカウント乗っ取り

2011年　奈良県の小学4年生の女子児童が、会員制の交流サイトでサービス上の通貨の提供を条件に、別の女子中学生のID/パスワードを聞き出し、本人になりすましてログイン、その女子中学生のアカウントを乗っ取ったもの。小学生の女子児童は不正アクセス禁止法違反の容疑で補導され、児童相談所に通告された。

● ウイルス保管と提供

2017年12月、動画サイトなどに掲載されていた動画を参考にコンピュータウイルスを作成、これを保管、提供した等の理由で、大阪に住む小学3年生の男子児童が不正指令電磁的記録提供などの非行内容で児童相談所に通告された。またこれをダウンロードした京都、山梨などに住む児童も不正指令電磁的記録取得の非行内容で児童相談所に通告された。児童は「友だちを驚かせたかった」などと述べた。

● 同級生の少女の裸の画像を拡散

2018年4月、同級生が高校生の少女に裸の画像や動画を撮影させ、これをSNSに投稿することを強要し、そののち拡散した。16歳から17歳の男女4人の児童は、児童買春・児童ポルノ禁止法違反（製造、提供など）の疑いで書類送検された。

コラム：成人年齢18歳引き下げに伴って注意が必要なこと

2018年6月に民法が改正され、約140年ぶりに成人年齢が20歳から18歳に変更されることとなりました。この改正により、2022年4月1日以降は、18歳になると成人になり、またすでに18歳、19歳になっている人は、この日をもって成人となります。

さて成人すると、何が変わるのでしょう。すぐに思いつくのは、飲酒や喫煙、ギャンブルなどがありますが、これらは、成年年齢が変更されても20歳以上のままで変更はありません。最も大きな変化は、「親権者の親権に服さなくなる」ことです。

未成年者は、親権者の同意なく契約行為ができませんが、今回の改正で、18歳になれば成人になりますから、自らの意思で契約行為をすることができます。

例えば携帯電話の購入では、回線の利用契約が必要ですが、保護者が契約した上で、利用者を未成年者としたり、保護者の同意のもと未成年者が契約したりすることになっています。これも施行後は、18歳以上ならば自身で契約できるようになります。また青少年インターネット環境整備法で携帯電話会社に提供が義務付けられているフィルタリングも、その提供が契約事項に含まれているため、これまでは未成年者は親権者の同意がなければ自分の意思で解除をできませんでしたが、施行後は18歳ならばそれも可能になります。

ソーシャルゲーム、オンラインゲームでの課金やオンライン通販などでの購入も契約行為です。親権者の同意のない課金は、未成年者による契約を理由に取り消しを申し出ることが可能でしたが、施行後は18歳になれば成人ですので、未成年であることを理由に取り消しはできません。日頃から課金などをしている場合には、自身で課金額などを確認し、支払える範囲内に収めておくよう心掛けましょう。

さらに高齢者だけでなく成人したばかりの若者をターゲットに、SNSなどで甘い言葉や人間関係を作って勧誘するような手口が国民生活センターからも報告されています。18歳成人化を控えて、従来よりもさらに低年齢層にターゲットが広がるおそれもありますので、日頃からこうした甘い言葉や見知らぬ人からの誘いには注意しておきましょう。

18歳成人化の対象者

対象者	成人になる日	成人年齢
2002年4月1日以前の生まれ	20歳の誕生日	20歳
2002年4月2日～2003年4月1日生まれ	2022年4月1日	19歳
2003年4月2日～2004年4月1日生まれ	2022年4月1日	18歳
2004年4月2日以降の生まれ	18歳の誕生日	18歳

変わるもの・変わらないもの

変わるもの	変わらないもの
・携帯電話の契約 ・ローンを組む ・クレジットカードをつくる ・賃貸契約を結ぶ ・10年有効のパスポート取得 ・結婚　など	・お酒を飲む ・タバコを吸う ・競馬、競輪、オートレース、競艇の投票券(馬券等)を買う ・大型・中型自動車運転免許の取得　など

コラム：デジタル遺産相続

近年、生活の中にIT機器やサービスが深く入り込むにつれ、それぞれで必要となるIDとパスワードの数は増加する一方です。

また、たとえば家族の中でITに詳しい人が一人だったり、あるいは互いになにを利用しているか話していなかったりした場合、その方が亡くなると、資産や負債を含めて、どういったものが残されたのかわからない場合もあります。

特に問題になりやすいのは負の遺産で、FX(外国為替証拠金取引)で取引をしたまま亡くなった場合、取引が継続されていて、その後相場が大きく変動して、知らないうちに莫大な負債(不足)を抱え込んだという例もあります。

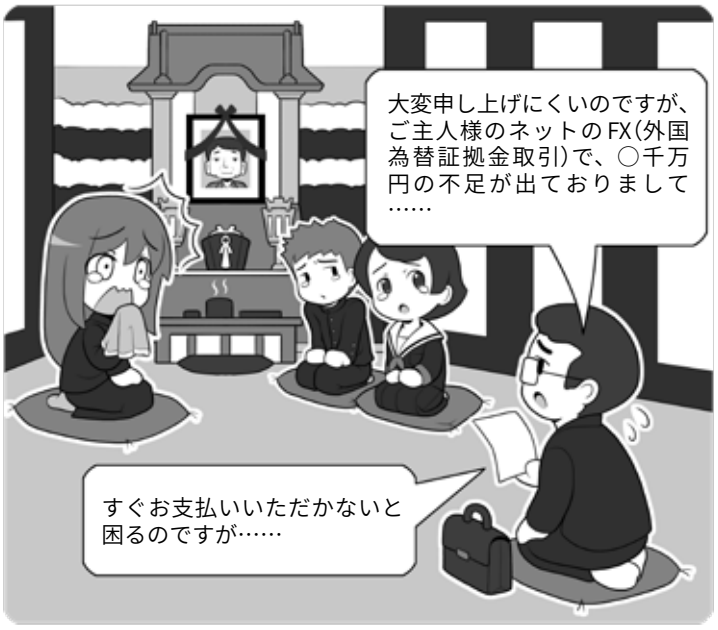
イラストのように極端な話しになるかどうかはさておき、「立つ鳥跡を濁さず」にするためには、残された人が迷わないように、万が一の時に備えて管理情報のありかを残しておきましょう。

どういったサービスを利用していたかの一覧や、もし亡くなったらどのような処理をしたら良いか。IDやパスワードなどをパスワード帳に書き残すか、スマホのパスワード管理アプリを利用している場合は、その解除のためのPINコードなどを、ノートや遺言書に残すか、家族と共有しておきましょう。

SNSのウェブサービスなどは、本人が亡くなった場合、特定の人を管理者に指定できる機能が提供されている場合もあります。調べてみましょう。

残された家族が美しい思い出に浸りながらあなたを偲ぶことができるように、きちんと整理をしておきましょう。

きちんと伝えておかないと、突然負の遺産が現れることも



これは極端なたとえですが、お金のやりとりが発生するサービスをそのままにしておくと、支払いや負債が残された家族にかかってくる場合があります。

何をやっていたかをパスワードを含めて書き残す

お金のやりとりが発生するものは支払いや負債が発生する可能性があり、ブログや電子メールアカウント、デジタル写真サービスは乗っ取られる可能性があります。誰かが相続し管理をするか、きちんと終了させる必要があります。パスワード帳などに書き残すのも一つの方法です。

3 デジタルテクノロジーで家族を守る

1 子ども達を守る

子どもをインターネット関連の犯罪から守るには、理由を述べずにあれもダメこれもダメと頭ごなしに禁止せず、まず可能な限りどういった犯罪がどのように行われるのかを知らせましょう。

子どもたちが犯罪に当たる行為をするとき、本人達はそれが「犯罪になると思っていなかった」という例もあります。知ることが抑止することにも繋がります。

サイバー犯罪に遭うという視点からも、問題点や危険性、またそれによってどれぐらいの範囲にトラブルが広がるのか、きちんと共有することが必要でしょう。

その上でセキュリティソフトやフィルタリングサービス、緊急時のための位置情報共有の必要性を一緒に確認しましょう。

いざというとき子どもを助けに行くためには、位置情報は非常に有効な手段です。一方、子どもたちは過度に位置情報に関することを追求されると、共有を切ってしまうかもしれません。セキュリティ設定の変更などはあっという間にクリアしてしまうこともあります。

ですから、叱ったり、とがめたり、あるいは取引のようにするのではなく、その必要性を共有し、特に位置情報の共有は監視のために使わないことを約束し、そして約束を守りましょう。

また子どもからルールの変更や

本当は怖いインターネット

理由を言わずに禁止するのは命令

ネットでなにが起こるかを一緒に見る

頭ごなしに禁止せず、インターネット関連のトラブルの実例を見ながら、なぜダメなのかを「理解」しあって共通の認識を作ります。子どもだけでは対処できないトラブルがあることを知ることは重要です。

自分だけは大丈夫と思わせない

保護者機能や位置情報を活用する

危ないサイトをフィルタリングサービスでブロック

意識を共有したら実例を示して子どもたちに答えを出してもらいましょう。自分で出した答えは自らのルールとなるからです。

どうしても見たいサイトなどを言い出しやすい雰囲気を作り、それについて一緒に話し合って勉強する姿勢を示しましょう。スマホやIT機器は絆を断絶するためのツールではなく、より太く結ぶためのツールなのです。

スマホが使えないほど幼いお子さん達を守るサービスや機器もいろいろと登場しています。

学校を離れたときや駅を通過したときに親のスマホにメールが送信される見守りメールサービスや、簡単な携帯電話とGPSと防犯ブザーが合体したキッズケータイは、子どもたちが意識しないで使え、あるいはシンプルな操作方法を理解したら、いざというときの強い味方になります。

またある程度スマホの操作をすることができる年代になったら、位置情報を送信したり、必要な情報をメールやSNSを通じてシェアする方法を、一緒に覚えるのも良いでしょう。

幼いお子さんの姿が見えなくなって一番困るのは、迷子になってしまうことです。また親とでもお友だちとでも、待ち合わせ場所などで誰かを探すようなそぶりをしていると、知らない人物から「一緒に探してあげる」というような声をかけられる隙になります。目的の場所に迷わずたどり着け、必要であれば待ち合わせをし、迷わず会うことができるスキルを身につけると役に立つでしょう。

なお、現在は建物の中で迷子になると位置情報や何階にいるかなどの情報は共有できませんが、今後地下街や屋内などにビーコンと呼ばれる機械の設置により、屋内でも位置情報の交換が可能となると考えられます。

その他にも電車やバスの乗り換え案内アプリ、徒歩ナビゲーションの活用などを覚えることで、どこかではぐれても、家に帰り着くスキルを一緒に学びましょう。

見守りメール

見守りメールは、鉄道会社や一部の学校などが提供しているものがあるので、自分が住んでいるエリアでサービスが行われているかを調べてみると良いでしょう。

GPSつきキッズケータイ

連れ去りや変質者に遭遇したときに使用する防犯ブザーと簡単な携帯電話が一体になった機器です。簡単な操作で登録された特定の人物への通話なども可能なものもあります。

位置情報メール

「位置情報を共有」→「メール」などで設定すると、現在地を簡単にメールで送ることができます。これを相手宛に送れば、相手のスマホで地図アプリが起動して位置を確認できます。

位置情報シェアアプリ

本当に親しい友人とは、常時位置情報を確認し合えるアプリを利用するのも良いでしょう。そうすることでいちいちメール送信せずに位置情報を共有できます。

2 お年寄りを守る

離れて暮らしているお年寄りと連絡を取り合うのに、テレビ電話機能に対応したスマートテレビや大きなタブレット、液晶付きスマートスピーカーをプレゼントして、ときどき映像つき電話をして声だけで無く顔を見せるのも良いでしょう。

また一人暮らしのお年寄りの見守りのために、よく相談をした上でウェブカメラの設置をしたり、毎日部屋の中を動いて家電機器やガスを使用しているかをメールで連絡してくれるサービスも存在するので、こちらも相談し、納得してもらった上で利用したりするのも一つの手でしょう。

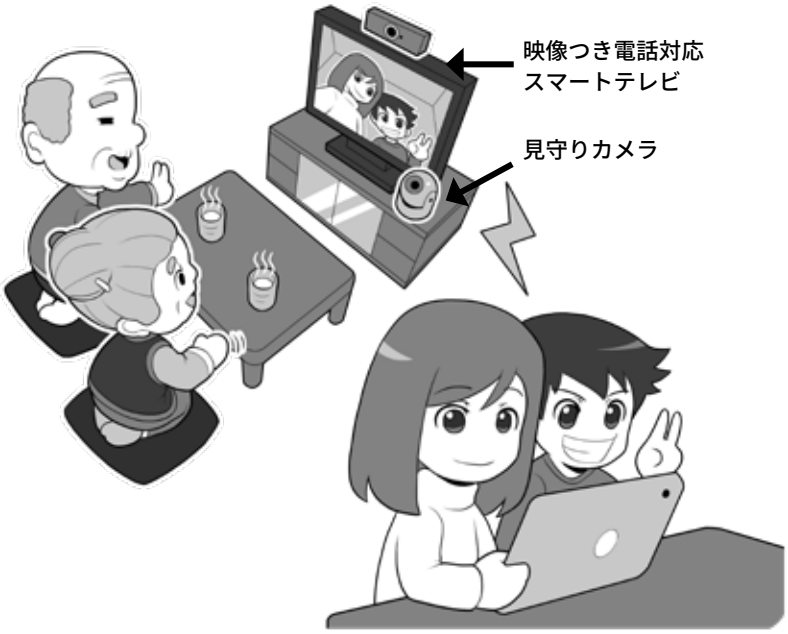
一番良いのは会いに行くことですが、離れて住んでいて頻繁に会えないならば、そういうときこそインターネットの「距離と移動に必要な時間が消えた世界」という能力を生かしましょう。

また、「自分は大丈夫」と思っているお年寄りほど、あっさりと振り込め詐欺などに引っかかってしまうものです。振り込め詐欺は電話で顔が見えない状況で、相手を不安に陥れ正常な判断が出来なくなることを利用しています。

これに対抗するために、たとえばご両親に連絡するときは、通話アプリのTV電話機能を使うと決めておけば、顔が見えない状況で丸め込まれ、だまされることを回避できるかもしれません。

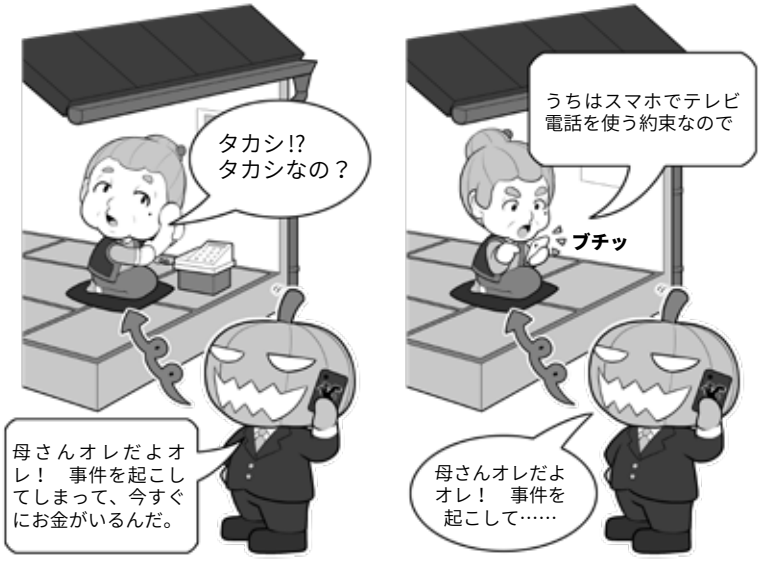
そのテレビ電話機能の為ではありませんが、お年寄りには使いやすい簡単操作のスマホを渡すのも一つのアイデアです。または、いざ操作を勉強する段になって教えてあげやすいように、自分が持っているものと同じ機種を渡しておくのも一つの考え方です。

映像つき電話やITサービスの活用



お年寄りにとって子どもや孫たちの顔を見るのは、なによりの楽しみでしょう。会いに行ってあげるのが一番ではありますが、なかなか訪ねて行けないときは、顔を見てコミュニケーションを取れるツールを活用しましょう。また一人暮らしのお年寄りに万が一のことがあったときのために、日々生活状況を確かめられるサービスも存在しますので、利用を検討しても良いでしょう。

IT機器を使った振り込め詐欺対策



電子機器の操作に不慣れなお年寄りでも、かかってきた電話を受けることはできるものです。子どもや孫から連絡を取るときは必ずTV電話を用いるという方法を使えば、顔が見えない状況で不安に陥れる「振り込め詐欺」などの予防にもなります。同じスマホを渡してあげれば、操作を教えることも簡単です。

ご両親の海外旅行時に、きちんと目的地に着けているか、迷ったりしていないか心配な場合は、事前に相談して位置情報共有サービスや移動履歴が残るサービスを設定して旅に出てもらいましょう。

こうすることで今どこにいるかを確認することができるので、予定通りに旅行しているかもチェックすることができます。

また仮に旅先で迷子になってしまっても現在地がすぐわかれば、どのようにしたら良いかのアドバイスも的確にできるでしょう。

そんなことはあまりあってほしくありませんが、もしスマホを紛失したり盗られたりした場合も、操作するための情報を共有しておけば、スマホをロックしたり所在地を確認することもできます。

認知症を患っているお年寄りは、家族の見ていないときに外に出て徘徊し、事故に遭ってしまうことがあります。

また一緒に外出した後で目を離した隙にいなくなってしまい、本人も自分がどこにいるのかわからず、その結果、行方不明になってしまうケースもあります。

そういった場合に備えて、GPS発信器を使った位置情報サービスを契約したり設定したりしておくと、間をおかず探し出すことができます。

もちろん目を離さないことが重要なのですが、ご自身にリカバリする能力がない状況では、万が一に備えた方が安心でしょう。

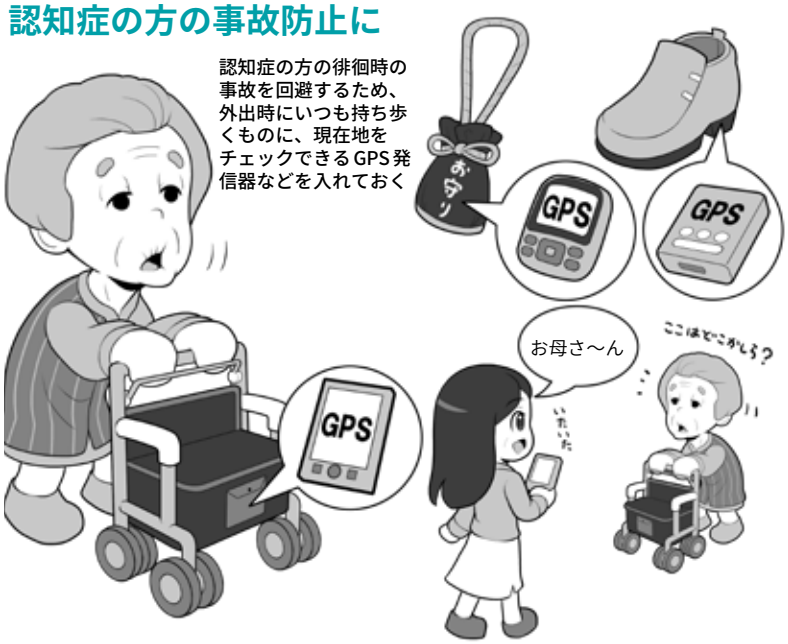
お年寄りによっては、持ち慣れない機器を持つことを嫌がる場合もありますので、機器を入れる場所の工夫は必要ですが、事故などを未然に防げる可能性が少しでも高くなるならば、検討してみると　良いでしょう。

位置情報の共有（安否確認）

スマホの位置情報の共有設定をし、現地でもインターネット接続サービスを利用できるようにしておくと、世界中どこにいても現在地を確認することができます。年輩の方自身が位置情報を使いこなせなくても、電話やSNSのメッセージ機能などを使ってサポートすることができます。

※現地でデータ通信できるようにデータローミングの利用や海外用のSIMを手配する場合は、渡航前に準備や設定を済ませておきましょう。また現地に着いたときに確認するべき事項を紙などに書いて、事前に説明しておきましょう。海外で購入したSIMの使用は最初の設定をしないと、インターネット接続もできない場合がありますので注意が必要です。

認知症の方の事故防止に



普段押して歩くカートや、お守りに入れて持たせたり、そもそも物を持ちたがらないお年寄りには、靴の中に入れられる機器も存在するのでそういったものを利用したりします。しかし、これらはなにかあったときのバックアップの手段で、普段から目を離さないことがなにより大切です。

4 屋外・海外でのネットワーク利用

1 一見なにもないように見えて、危険がいっぱい

たとえば国内でも国外でも、あなたが屋外のカフェでパソコンを開いてウェブを見たりメールをやりとりしたりするとします。カフェには無料の無線LANアクセスポイントがあって快適にネットに接続することができます。うららかな日差し、さえずる鳥の声、実に平和そのものだし、ちょっとお店に入ってケーキでも選んでこようかな？

さぁこのカフェには、どんなサイバーセキュリティ上の危険があると思いますか？

まず日本では、よくスマホで席取りをしてレジに行くのを見かけますが、海外では貴重品は肌身離さず持つことをおすすめします。日本と同じ治安レベルとは限らないので盗難される可能性があります。日本でも油断はなりません。

また席に置きっぱなしにしたパソコンへ目を離した一瞬に、USBメモリを差し込んでマルウェアに感染させることもできます。

所持品が盗まれなくても、肩越しや場合によっては双眼鏡や望遠レンズを使って、スマホやパソコンのロック解除用PINコードを盗み見されるかもしれません。

お店の無線LANアクセスポイントの暗号化は、本当に安全な方式ですか？パスワード(暗号キー)を店内に貼り出していませんか？通信しているデータを盗聴されて、ウェブサービスにログインするIDやパスワードを奪われてしまうかも知れません。それに攻撃者が店のアクセスポイントと全く同じ名前の偽のアクセスポイントを設置して、あなたを待ち構えているかもしれませんよ。

気をつけてくださいね。

2 インターネットカフェの利用

海外旅行に出かけるときになるべく荷物を減らそうとすると、仕事じゃなければパソコンはお留守番になるでしょう。

最近ではスマホもありますし、長いメールを書く必要があるなら、インターネットカフェに行って、ウェブメールを利用すれば、ホテルでもなんでも予約できるし…、なんて思ってはいませんか？

インターネットカフェは国内外を問わず便利ではありますが、これを使ってメールや何らかのウェブサービスのID・パスワードの入力、あるいはクレジットカード情報の入力は、絶対に避けることをおすすめします。

海外のインターネットカフェのパソコンは管理が充分ではないことがあるほか、攻撃者にとっても狙いやすいターゲットでもあります。キーロガーというマルウェアを仕込んで、利用者が入力したIDやパスワードなどの個人情報を抜き取って攻撃者に送信してしまうことがあるのです。

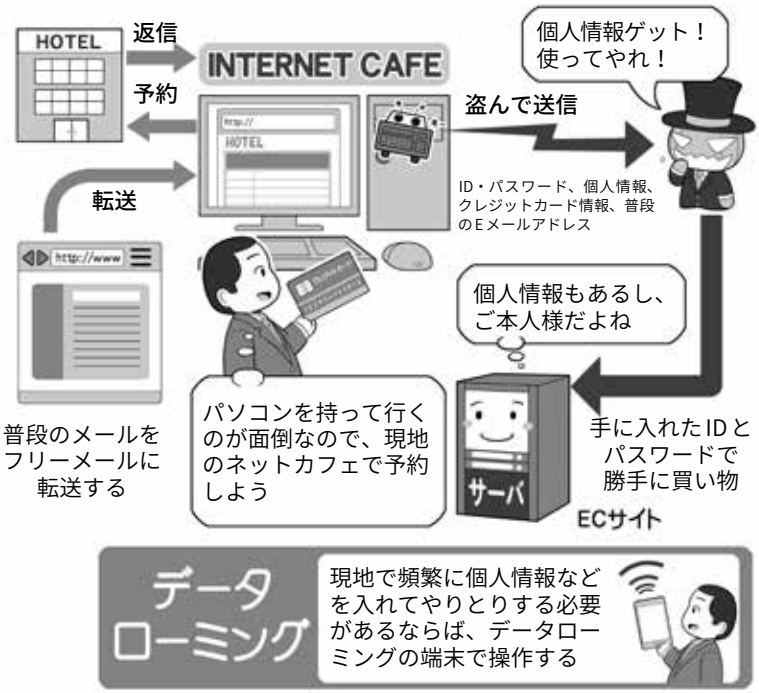
お店の人がシステムを最新に保ち、セキュリティソフトも入れ管理しているから、そんなソフト仕込めないよ、と思ったら甘いのです。キーロガーにはハードウェア版もあり、数秒あればパソコンの本体の後ろ、キーボードのUSB端子と本体の間に装着でき、あとは無線LAN経由でデータを送信できるものもあります。今まで利用したパソコンの後ろをいちいち確認したことはないでしょう？

また自分のパソコンやタブレットを持ち込んで店のWi-Fiを使用する場合は、自前の暗号化が出来ないなら利用はおすすめしません。もし現地で頻繁にデータ通信を利用するならば、データローミングや現地の定額SIM（次頁参照）の使用をおすすめします。

インターネットカフェのマシンには、キーロガーなどが仕込んである前提で利用する

インターネットカフェは基本的に情報を検索するだけに利用します。ID・パスワード、個人情報、クレジットカード情報は絶対に入力しないように。自分の持ち込みパソコンなどを利用する場合は、自前の通信の暗号化ができるならばOKです。

共用のパソコンで重要な情報をやりとりしたら攻撃者に漏れる可能性あり



インターネットカフェで普段利用しているメールを利用するのは危ないと考え、フリーメールアドレスを作成しそこにメールを転送しても、結局予約のやりとりなどを現地で行うことになるのなら、情報流出の危険性はかわりません。現地でそういった情報を入力することが多いのならば、タブレットなどでデータローミングを行うか、自前の暗号化＋公衆無線LANを使うようにしましょう。

3 海外でスマホやタブレットを活用するために

自分のスマホやタブレットを海外旅行にもっていって現地で使う場合、日本で契約している携帯電話会社が提供するローミングサービスを使って、現地の携帯電話回線提供会社と契約せず、データ通信を利用する方法があります。

ローミングサービスは国内よりは割高で、また音声とデータ通信は別々に料金設定されているので、利用した場合いくらかかるのかをよく確かめてから使いましょう。さもないと途轍もない料金請求が届く場合があります。最近は手頃な1日あたり料金定額などのプランも存在します。

また海外では電話を受けただけでも電話料金がかかる会社もあります。着信が無料ではない場合、電話を受けたらいくらかかるのかもチェックしておきましょう。さもないと、不意の長話で高額な請求が来てしまうかもしれません(くどい？)。

データ通信が使えなくも文章のやりとりができる方法にSMS(ショートメッセージ)がありますが、これも利用可能かどうかと、利用できる場合の料金を調べておきましょう。電波整備状況がよくなくデータ通信が使えない場合の文字通信手段になります。

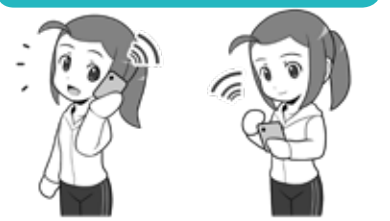
ローミングサービスを電話で利用するメリットは、海外にいても自分の電話番号にかかってきた着信を受けられることです。

もし長期で滞在する場合などで、その間電話番号が変わってもいいならば、現地携帯電話会社のSIMを購入して利用する方法もあります。SIMには目的別に音声のみ、　音声＋データ通信、タブレット用

海外で電話やデータ通信を使う

普段の電話番号で着信できるようにする

電話番号が現地のものになっても良い



現地SIMは現地空港などでも買えるが……

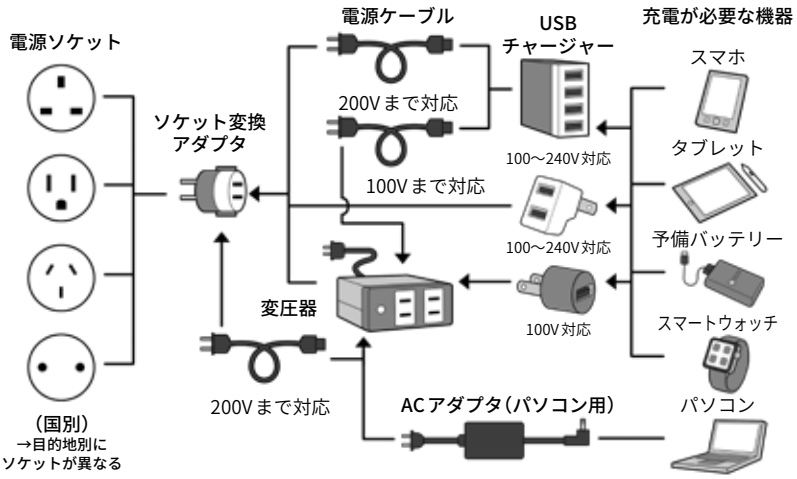
・日本で買えることも(SIMのサイズに注意)
・事前使用設定を済ませておく
・音声の料金、データ通信の上限容量をチェック
・月額料金が発生せず、チャージすれば保存可能なものもある。何回も訪れるなら選択肢に
・料金は従量制か、上限のある定額制か確かめる

外国語が苦手だからメールでやりとりしようと思ったら

海外では意外とデータ通信できず、音声のみのエリアも多いのです。データ通信できても遅い場合もあります。データ通信速度を確保できないことを想定して、地図などは日本で事前にダウンロードしておくことが重要です。

電源・充電方法の確保

ソケットと電源のボルト数はまちまち。理想的には全て100〜240V対応であること



USBチャージャーのUSB端子は、充電する機器の数だけ、差し込み口はあるか。全体の電源容量は足りているか。タブレット用には充電能力は足りしているか。200V系の国へ訪問するときは、ケーブルまでもが200V対応かをチェックします。

にデータ通信のみなどのSIMが存在します。

普段の端末は日本からの着信専用にして、別途SIMフリーの端末を用意し、これに現地のSIMを入れて使用する方法もあります。

海外のSIMを使う場合の注意点は、利用する端末が「SIMフリー」か同様の状態であることを確かめることです。日本の携帯電話会社で販売されてる端末は、その会社のSIMしか使えない設定になっていることが多いからです。ただ多くの端末では、国内では制限があっても海外ではどのSIMでも使える「SIMフリー」相当になっているものもあり、また条件を満たせば携帯電話会社が有料でSIMフリーに改修する「SIMロック解除」を行ってくれる場合もあります。

また忘れがちなのが充電に関することです。充電器の対応電圧と、充電器にケーブルがある場合はこのケーブルの対応電圧が訪問国にあっているか確認して、必要に応じ変圧器を利用し、また現地の様々なタイプの電源ソケットの形状に対応できるソケット変換アダプターを用意していきましょう。

次に、せっかくスマホなどを海外に持っていくのなら、海外で使える機能や役立つ機能を準備していきましょう。

まずは翻訳系です。文字を入力するのではなく、音声で入力、翻訳結果も音読してくれるアプリなどもあります。また逆に相手にしゃべってもらってそれを翻訳することもできるので、音声を使って現地の人と理解を深め合うことができるでしょう。

次は翻訳カメラ。海外で街並みやメニューなどを撮影すると、文字部分を認識し翻訳して表示するものです。こちらもいちいち辞書アプリなどに文字を入力する手間が省けますので、海外の旅をより楽しむことができるでしょう。

地図系のアプリのインストールと、現地の地図のダウンロードも重要です。前述のコラムでも書きましたが、海外では場所によっては日本のように通信網が充実しておらず、データ通信があっても遅いか、場所によっては全く使えないこともしばしばです。そんな中で現在地を確認しなければならない状態になったとき、オフラインでも使えるように、地図を本体にダウンロードできるものを準備しておきましょう。

海外でITを活用する

翻訳アプリ

翻訳カメラ

地図ソフト、GPSナビ

(音声)ローミングの注意点

- 海外では通話を受けても料金がかかる場合もある
- ローミング時の料金はいくらかかるのかチェックしておく
- SMS(ショートメッセージ)が利用できるかどうかと、その料金

データローミングの注意点

- 必要がないなら、データローミングの設定を必ず切る
- つながるからと放置しておくと、莫大な請求金額がくる場合がある

海外利用におけるSIMフリーとは

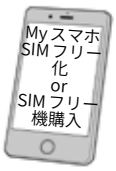
手持ちのスマホなどが海外でも使えるか

- 目的の国でのローミングに対応しているか、実際使用されているか。現地の会社の周波数帯(バンド)に合っているか
- 海外のSIMが使用可能か(≒SIMフリー)

日常使っているスマホなどを、SIMを入れ替えて使う

- ○ 現地SIMなら料金も手頃なものがあり、電話料金も安い
- ✕ 日本から普段の番号につなげない。滞在期間中の電話番号を教えておく必要あり

SIMフリー端末の入手とは



- 日本では特定の会社のSIMのみ利用可能だが、海外ではどれでもOK(海外では「SIMフリー」相当)
- お金を払うと携帯電話会社がSIMフリー状態に改修してくれる(SIMフリー)
- そもそも電気店やメーカーから直接SIMフリーのスマホを買う(SIMフリー)

普段使っていないSIMフリー機を使う

- ○ 手頃なSIMフリー機を入手するか、使わなくなったものをSIMフリー化しておく
  現地SIM使用、料金も手頃
- ○ 普段使用の機種は電話を受けるだけのローミング。日本の電話番号でかけられる
- ✕ 2台持ちは面倒

5 大災害やテロに備える

1 まずは自分の身の安全を確保する

大地震・各種の自然災害・テロなどが発生したり、なんらかの避難勧告が発表されたら、決してその場に留まって写真を撮ったりSNSに投稿したりせず、速やかに安全な場所に避難しましょう。

海や川の近くでの大地震ならば急いでできるだけ高い場所に避難しましょう。昨今の豪雨・水害などの自然災害の例を見ると、避難勧告前に自主的に避難場所に移動するのが有効です。

災害時に現場で写真を撮ったり、実況放送のようにレポートすることは、あなたの仕事ではありません。無事家族の元に帰ることが使命です。それを最優先に考えて、まずは命を守る行動をしましょう。

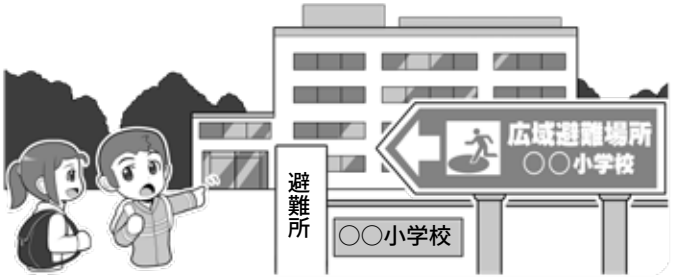
避難場所に到着し、そこが安全であると確認できたら、安否確認の連絡や情報収集をしましょう。

安否確認サービスは様々なものがあるので、家族や友だちと事前にどのサービスを利用するかを決めておきましょう。また災害時はスマホの電話やウェブの閲覧などは混み合ってつながりにくくなります。災害時に通話が優先される公衆電話や、なるべくデータ通信量の少なくてすむ、メールやSNSなどのサービスを使いましょう。

なおスマホアプリの通話機能もメールなどより通信容量を多く使います。譲り合い、少ないデータ通信ですむ手段を利用しましょう。

命を脅かすものから速やかに逃げる

安否の連絡や情報収集は安全な場所に着いてから



自然災害時は避難勧告が出る前でも、自主的な避難が命を守る行動になります。まずは身の安全を確保し、その後、安否の連絡や情報確認を行いましょう。

そして安否連絡や安否確認サービスに登録

安否確認の方法は、複数の候補を事前に家族などで決めておいて、それを利用するようにしましょう。災害時には、スマホを含む一般の電話は通話がつながりにくくなります。電話連絡をする場合は、公衆電話か避難所に設けられる災害時用の電話を利用しましょう。なお、インターネットが使えなくなった場合の避難手順や安否確認方法も検討しておきましょう。

2 電池をもたす、情報収集をする

災害時などにスマホが圏外になったら、それは通信用の基地局が被害にあって壊れている印です。そのまま電源をONにしておくと、スマホはつながらない基地局に接続しようとして貴重な電池を消費してしまいます。

そういったときはスパッとスマホの電源を切るか、スマホの中身を見る場合でもフライトモード（機内モード）にして少しでも電池の消費を抑えましょう。

電波が回復しても、電話よりはデータ通信でメールやSNSを利用しましょう。災害時はその方がつながりやすく、また電池の消費も少なくてすみます。次にいつ充電できるかわからない状況では、とにかく電池の節約を心がけるようにしましょう。モバイルバッテリーを日常的に持ち歩くのも良いでしょう。

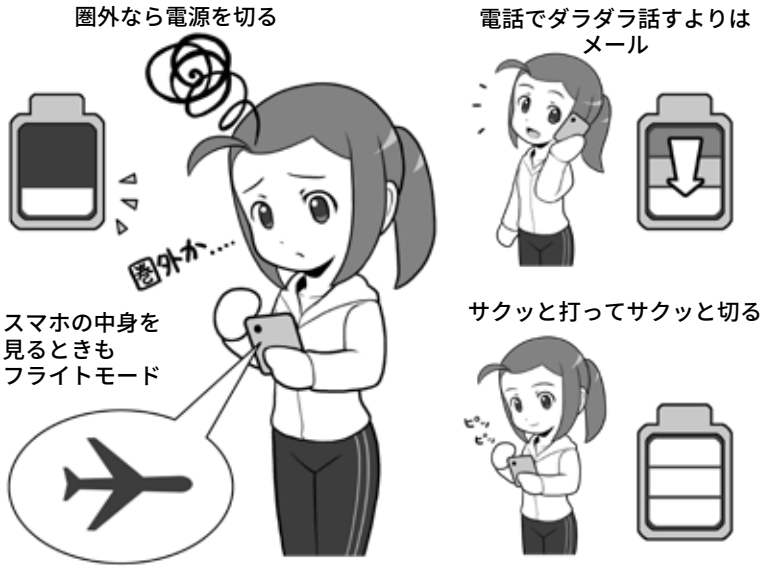
災害直後は情報が錯綜しますが、一定時間が経過すると救援物資や脱出ルートなどの情報がネットに発信され、やがて整然とした情報発信が行われるようになります。

しかし、だらだらとウェブを見て回って情報を収集しても電池を消費するだけなので、メールやSNSで、情報の収集と整理に長けた家族や親しい友人に助けを求め、信憑性や関連性の高い情報、必要としている情報だけを整理して送ってもらうのも良いでしょう。

東日本大震災では旅行で被災地に訪れているときに震災に遭い、帰ることができなくなった方たちが、SNSを通じて被災地から地元に帰るためのルートの確認や車両手配、バスの予約などをしてもらった例もあります。

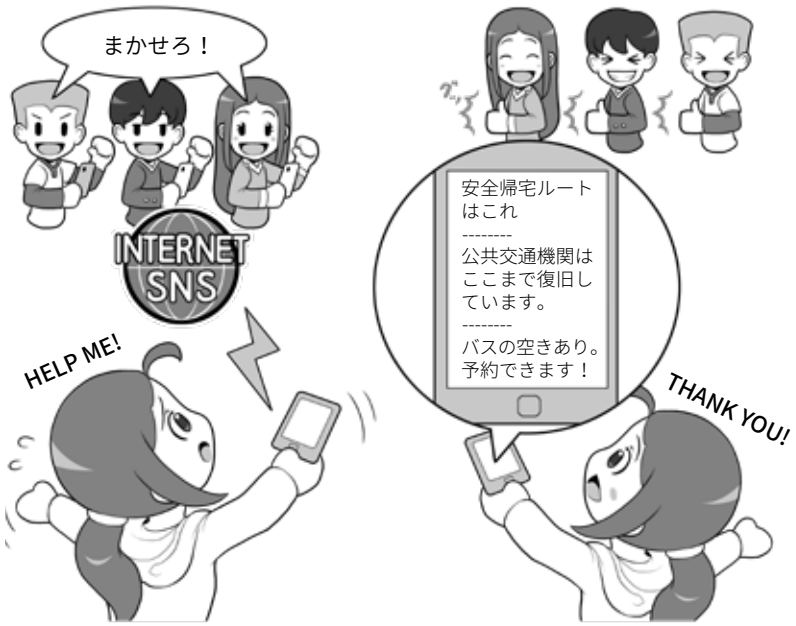
ぜひそういった事例をみんなで話し合って、いざというときにどうするか、ということを相談してみてください。

電池をもたすテクニック



圏外ならば電源を切るか、スマホの内容の閲覧時もフライトモードを利用します。電波が回復したら災害用の超省電力モードがあれば活用してもいいでしょう。電話で長く話すよりも、メールをさくっと打って電源を切った方が電池を消費しません。充電器にもなるモバイルバッテリーを持ち歩くのも役立ちます。

情報収集を協力してもらう



情報収集に長けた家族や友人と相談して、いざというときは情報収集や必要なものの手配をお願い出来るようにしておきましょう。自分一人では気づかない情報も外から見ていると気づく場合もあります。

3 ラジオ、ワンセグを使った情報収集

大災害時に電波がきちんと飛んでいる状態でも、目的のサーバに接続しようとすると、反応が無い場合があります。

それは、サイバー攻撃のDDoS攻撃のように、多くの人が特定のサーバに集中して接続することで、サーバの反応が間に合わなくなり、ギブアップの状況になっている可能性があります。

この問題は災害時には避けがたく、双方向通信のメディア、つまり私たちがサーバに接続してサーバが返信するというプロセスを前提としているインターネットでは、どうすることもできません。

こういったときに力を発揮するのが「片方向通信メディア」である、ワンセグTVやラジオです。これらのメディアは送信局が一方的に情報を発信して私たちが受信するだけなので、アクセスが集中し反応できなくなるということはありえません。

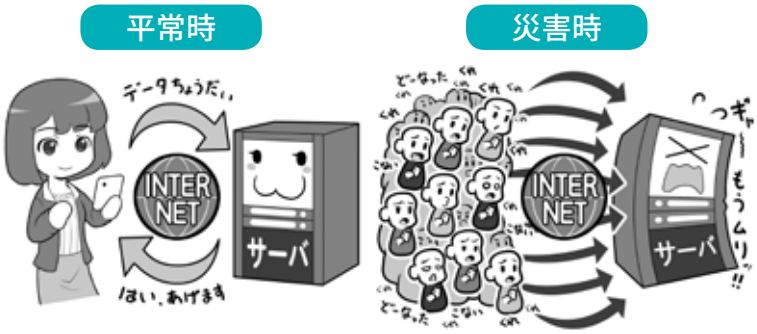
比較的近距離の範囲の放送をするワンセグTVやFMラジオなどは、大震災時などに送信局や送信施設が自分の被災地域に含まれる可能性があります。しかし一局で広範囲に電波を送信できるAMラジオや短波放送ならば、災害時に放送が中断する可能性がワンセグTVやFMと比較して少なくなります。

これが災害用の持ち出し袋にAM放送を受信できるラジオを入れる理由でもあります。

トラブルに対しては複数の手段で備えるのが基本ですから、普段は聴くことがなくても、災害用持ち出し袋にはAMラジオを入れることを検討しましょう。

また自分が持っていなくても、車の中ならAM/FMのラジオ、一部はワンセグTVが受信できます。

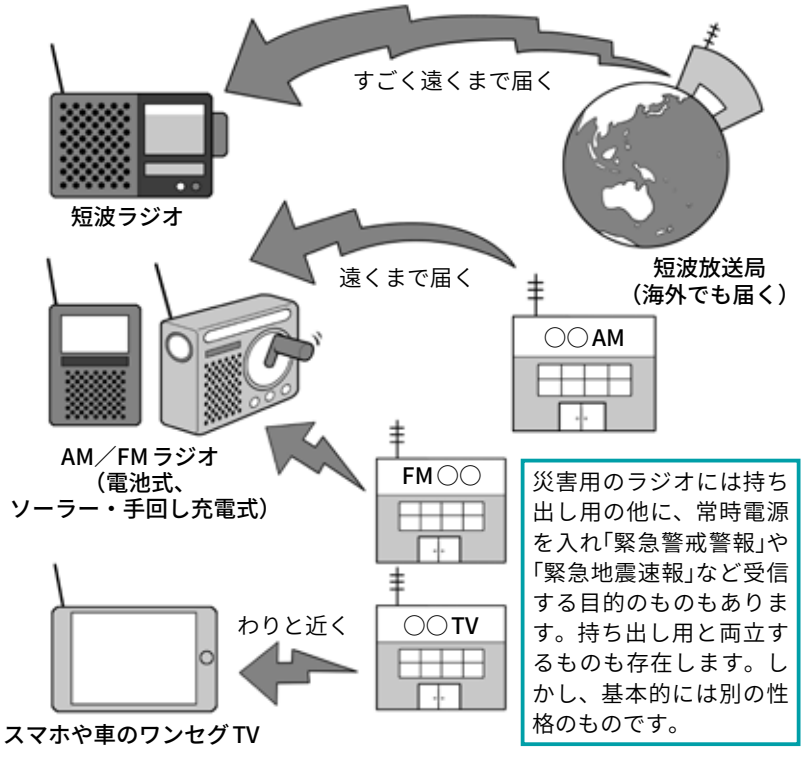
災害時のアクセス集中によるサーバの沈黙(双方向通信)



インターネットでは私たちのリクエストにサーバが答えることで情報が表示可能になります。しかし、一気にリクエストが集中するとサーバの処理能力を超えるため、反応が返ってこなくなります。これがアクセス集中です。

災害時でも沈黙しないラジオやワンセグTV(片方向通信)

ラジオ・TVは一方的に送信できるので大丈夫



災害用のラジオには持ち出し用の他に、常時電源を入れ「緊急警戒警報」や「緊急地震速報」など受信する目的のものもあります。持ち出し用と両立するものも存在します。しかし、基本的には別の性格のものです。

片方向通信の機器は、対応する受信機を持っているすべての人が受信可能です。FMやワンセグTVは放送局も被災して発信できなくなることもありますが、AMではかなり遠くまで届くので別の地域のものを拾うことができる場合もあります。短波にいたっては海外まで届きますが、逆に地域別情報発信には不向きです。ラジオは消費電力が少なく、ソーラー充電や手回し式充電型も実用的です。なおワンセグ搭載のスマホは少なくなりましたが、ワンセグや通常のテレビ受信可能な車のカーナビが増えていることをお忘れ無く。

4 徒歩帰宅。海外での災害やテロに備えて

災害時は原則としては政府や各自治体・消防などの指示に従うという上で、時に徒歩帰宅をするという選択肢を取らざるを得ない場合もあります。スマホには学校や仕事場から自宅までの道中、災害時に役立つ情報を掲載した帰宅支援マップやアプリを入れておくと役立つでしょう。日没時や降雨時の避難場所などもわかります。

またその場合に備え、家族と落ち合う集合場所や、帰宅手順を話し合っておきましょう。長期大規模停電で通信できない状況まで想定して、プランを立てましょう。

また災害時にはスマホの電池が命綱になる場合もあるので、普段からACアダプタ機能付きのモバイルバッテリーや、車の電源を活用できるようにカーチャージャー、ケーブルなどを持ち歩きましょう。

海外での災害やテロに備える場合は、事前に外務省の「海外安全ホームページ」で渡航先の情報を確認し、渡航が推奨されない場所には行かないようにしましょう。

また渡航前に外務省の海外安全情報配信サービス「たびレジ」に登録し、リアルタイムで渡航先の安全状況が把握できるようにしましょう。万が一災害が起こった場合に緊急時の安否確認などがすみやかに行えるように、SMSでメッセージを受け取れるようにしましょう。「海外ではどういう風にデータ通信をするか」を前提に考え、特にデータ通信しない場合でも、いざという時のため、最低限上記のSMSメッセージは必要なんだと覚えておきましょう*1。

災害時に徒歩帰宅をする場合は

帰宅マップ


予備電池


ACアダプタ

USB
カーチャージャー


タブレット対応か
チェックする
（2Aなど）

災害時は政府方針で、最大3日程度現地に待機を求められる場合もあるので、スマホなどの情報機器を使う場合、電池を持たす準備が大切です。ACアダプター機能付きのモバイルバッテリーの携帯や、車で充電できるようにUSB端子のついたカーチャージャーを必要に応じて携帯しましょう。また自分の機器の充電に対応しているかもチェックしておきましょう。条件に合わないと充電できないこともあります（主に2Aや2.1A対応と書かれている給電能力）。

海外での災害やテロに備える場合は

渡航前後に現地の情報を確認する

外務省海外安全
ホームページ
もしくは
外務省海外
安全アプリを
ダウンロード

外務省たびレジに登録する

渡航時は
外務省の
「たびレジ」
ホームページで
登録

緊急時は
SMSで連絡

たびレジ簡易登録にメールアドレスを登録する

渡航予定はなくても、海外安全情報をメールで受け取れる


滞在国の周波数に対応したAM\FM\短波ラジオ

＊1：SMSは基本的には通常の携帯電話回線（インターネット電話ではない）を利用していれば、データ通信を利用していなくてもメッセージを受け取ることができます。

注）「外務省海外安全アプリ」では、約120ページの「海外安全虎の巻」が同梱されていたり、海外安全にかかわる外務省のホームページなどを簡単に分類し、手早くアクセスできるようになっていたりするので、ぜひダウンロードしておきましょう。

コラム：デマに踊らされない！　ソースを探せ！　確かめよう！

昔からデマというものはありました。事件の時に拡散するものや、都市伝説のように長く語り継がれるものなど。

当時は人から人への口伝えですから、自分が聞いた話を再度確かめようと思っても、全て遡って大本の発言者までたどるのは至難の業ですが、その分「うわさ」ということを前提とした「不確かさ」「あやしさ」がありました。

ところがインターネットが普及した現代では、デマは「距離と移動に必要な時間が消えた世界」で、恐ろしいスピードで拡散します。しかも、SNSなどの場合「何人の人がその情報を共有したか」ということが数字としてついて回るので、それが何万人にもなると、デマであっても妙な信憑性があります。その代わり、ネットではソースをたどることができますので、怪しいと思って調べると、元の発言をした人間が、発言を消して逃亡してたなんてこともあります。

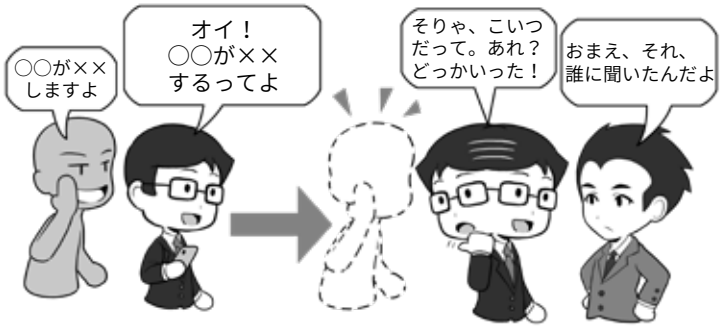
そしてこの構造は「意図的なデマの拡散」にも使われます。デマになりそうな話題を使ったマルウェアへの感染誘導や、フィッシング詐欺を狙った釣りかもしれません。場合によっては、誰かを傷つけ名誉棄損となるものかもしれません。

情報が勢いをつけて手元に飛び込んできても、その勢いに飲まれて拡散に加担せずに、情報の信憑性を確認する余裕を持ってください。

そしてほとんどの場合、後で冷静になって考えると、それはあなたが拡散する必要は、特にないものなのです。

ああ、災害時には本業の人ですら間違った発信をしてしまうミスもあるのでご注意を！

昔から出所が不確かなデマはあった

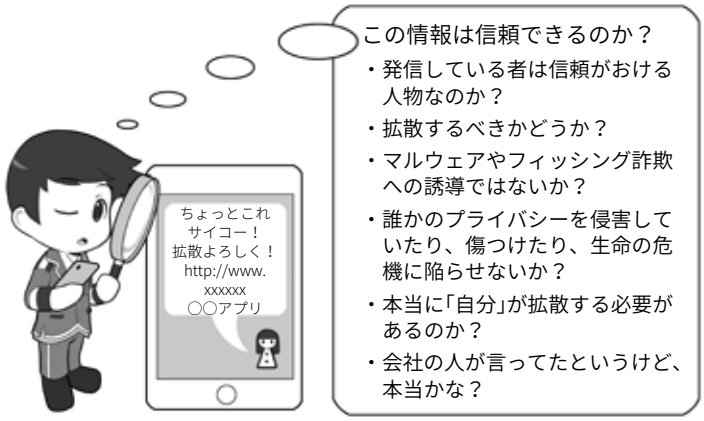


かつてのデマは、人間がしゃべるスピードでしか拡散しませんでしたが……。

ネットでは加速して飛び込んでくるが……

現在は、ネットの特性で「拡散数」を伴って加速して飛び込んできます。しかしその数を真実かどうかの尺度にしてはいけません。元ネタが嘘だったり、意図的に流布してから消して逃げたりすることもあるからです。

情報はよく吟味することが必要



コラム：災害時の情報収集について（本年の振り返り）

今年は様々な自然災害に見舞われ、その中で様々なデマが飛び交い、正確な情報収集の難しさを浮き彫りにしました。悪意のデマではないとしても、不正確な情報の拡散も多く見受けられました。拡散する方々は善意で行っているのですが、情報源（ソース）がはっきりしないものの拡散は状況を混乱させます。物事の正確さ担保するためには、「現場」を知る責任がある方の「公式な情報発信」以外は、むやみに拡散するべきではありません。特に「誰かに聞いた」というものも、たとえそれが「通信会社の人に聞いた」とか「役所が言っていたらしい」というものでも、公式発表ではない場合、「不正確」である可能性が高くなります。特に「伝聞情報」には気をつけて、「本当に拡散するべきか」良く考えてください。

また災害時の救助要請をSNSで行う方法が、広く一般に認識されたことが確認されました。これも本人、もしくや直接依頼された家族などの代理人が行うことは大変有効な手段とも言えますが、上記と同様に伝聞の情報を拡散したり、あるいは本人が救助された後も救助要請が残されたままだったりすると、それが一人でも多く助けようとする方の妨げにもなります。それ以外にもSNSの情報を見て、直接関係が無い人が善意で電話での救助要請を行うなどのケースがあったようです。

こういった情報は、本当に必要な情報収集への「雑音（ノイズ）」となる可能性があるので、十分注意してください。

また、最近は様々な災害時用のアプリが登場し、安否確認の方法も増えてきていますが、これらは連絡を取り合う人と、事前に何を使うか決めておかなければ意味を成しません。きちん事前の確認をしておきましょう。

なお、2018年北海道を襲った地震では、全道が長期間にわたって停電する事態が発生しました。携帯電話網もスマートフォンも使えなくなる可能性が垣間見えた災害でした。そういった場合どういう手段で連絡を取り合うかも確認しておきましょう。

災害時の避難所などでは、自治体や電気通信事業者の取組により、無料で使えるWi-Fi「00000JAPAN」などが立ち上がることがありますが、このWi-Fiは接続しやすさを優先するため、暗号化されていない可能性があることを覚えておき、利用時はID/パスワードの入力を避け、もし利用したい場合は自前で通信を暗号化するVPNの利用知識を得ておきましょう。

災害時の救助要請はわかりやすく確実に

SNSで救助要請をするときは大変な状況だと思いますが場所がわからないとたどりつけません。住所やGPS情報付きの発信をしましょう。

災害時は必要がない情報の拡散はひかえる

平成30年7月（西日本）豪雨時の不要不急拡散TOP3

…災害時に拡散しなくてもよいのでは？

5 ネットを使わない移動トレーニング（現代版オリエンテーリング）

災害時にスマホの電池が切れてしまったり、あるいは旅行先でスマホを落としてしまったり、誰かに盗られてしまったりしたシチュエーションを想定して、スマホを使わずに自力で自宅に帰り着くためのトレーニングを、遠足のような遊びの一環としてチャレンジしてみましょう。

たとえば地図とコンパスやGPS受信機を持って、地図を読んで現在の場所を特定し、ハイキングルートを抜けて駅の場所を目指したり、駅に到着したら鉄道路線図から自宅までの経路を割り出したり、駅に設置されている時刻表から自宅までの電車の時刻を割り出したりしてみます。

こういったことは、実はオリエンテーリングという野外スポーツのアレンジで、慣れると面白いゲームとして取り組むことができます。目的地を自宅ではなく、遠くの親戚の家へ訪問する機会にトライしてみるのも良いかもしれません。

地図が読めるようになると、コンパスがあるだけでも結構なんとかなるものですよ。

さて、最近はスマホになんでも記録できてしまうため、自宅の電話番号や家族の電話番号を覚えていないケースもあります。緊急に連絡を取る必要のある大切な番号は暗記して、公衆電話を見つけてコインやテレホンカードで電話をかける訓練をしてみましょう。公衆電話が見つからない場合は、お店などで聞いて探すところから始めるなど、いろいろなサバイバルを試してみても良いでしょう。

ゲームとして帰宅サバイバルを楽しむ

地図の地形や記号などを読んで、現在地の特定にチャレンジしてみよう

ゲームとしていろいろなことにチャレンジしよう

GPS情報からの現在地の地図の落とし込みや経路探索をしよう

電車の路線図を見て、自宅までの経路を決め、切符を買ってみよう

こういったことを経験しておくと、災害に遭ったときにスムーズに行動にすることができます。

大災害でもそんなことは起こらない？　いえ、こういったことは、どこまで「まさか」と思うことを想定できるかが、サバイバルの鍵になるのです。

エピローグ

来たるべき新世界へ

みんなが守るインターネット、その未来には何があるの？
そのインターネットに新しいテクノロジーが組み合わさって進化を遂げていったとき、私たちはどのような世界を実現し、その先に何を見るのでしょうか。
少しだけ未来を想像してみましょう。

1 ネットの「今」と、これからをどう守っていくか

インターネットというのは今の40歳代以上の大人から考えると「便利な道具」であり、現実世界をサポートする存在といったイメージでしょう。それは逆に今のようにネットが無かった「不便な時代」を知っているから比較ができるからでもあります。

しかし生まれたときからインターネットが存在している環境で育った子どもたちは、インターネットを道具としてではなく、現実世界と一体として感じている場合もあります。

たとえばネットへの接続が高速化して、ものを思い出すのとさほど変わらないスピードで情報端末から目的の情報を引き出させるようになった今、「いつでもネットから引き出せる情報」を、「少し思い出すのに時間がかかる記憶」ぐらいのようにあつかい、あまり脳に記憶することにこだわらないようになっている。そんな風に感じる事はありませんか？機器がさらに進化して考えれば答えが分かるようになれば、その「区別」すら感じなくなるかもしれません。

また現物の本や紙では無い、ネット上のファイルやデータの受け渡しは、もはや「渡す」という概念ですらなく、スマホ一つで共有するだけ。あとは誰がどこからでも遅延無く「リアルタイムで共有」どころか「編集」までできてしまいます。現実世界に軸足をおいた人々にはもはや感覚的にわからない、次元を超えた情報管理です。

ただ、そういったネットのメリットの部分はものすごいスピードで進化していますが、インターネットの世界はまだ生まれてから年数が経っていないため、世界として見たとき、それ以外の、特に安全を守る社会システムのインフラや秩序構築などは充分に確立されていません。

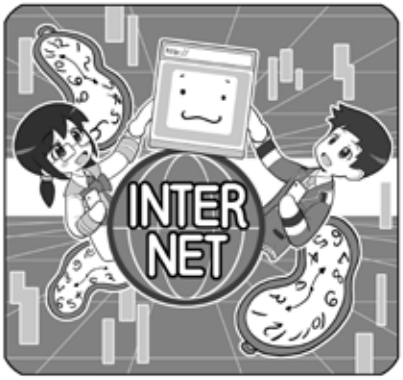
このネットの秩序に関しては、実はネットが生まれたごく初期に、現実世界から積極的にネットに移民してきた開拓意識が旺盛な「ネチズン」と呼ばれた人々により、文章化されていない暗黙のモラルとして存在してた事もありました。

しかしその後ネットが一般化し、様々な人がネットに移り住んできたことによりネットは多様性を帯び、その人たちを含んだ新たな秩

ネットは現実世界のオプションではない

インターネットの中の世界を、現実世界のオプションや便利な道具と捉える人もいますが、実際はそれに留まらない存在です。それは新しい人間の思考を求めます。

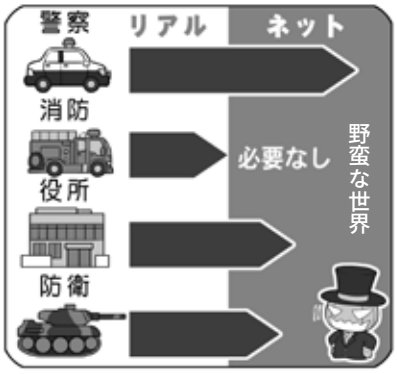
ネットは距離と時間の概念がない世界



ネットには移動という概念がなく、またそれによって消費されていた時間が必要でなくなる新しい世界です。子どもたちはこれを単に「そういうものだ」と自然に捉えて利用しています。

現実世界と同じ「社会インフラ」がまだ整っていない

新世界に人が先に進出して、社会のシステムや秩序の構築が間に合わない状態では「力こそ正義」となりがちです。ある意味「生きぬく能力がない人には危険な世界」といえます。



ネットの世界には消防は必要ありませんが、その他のインフラは必要です。サイバー警察、電子政府、サイバー防衛など次第に整いつつあります。しかし国民全体の協力が必要です。

序の構築が間に合わないまま、現在に至ります。そうして秩序が振り出しに戻ると、ネットの暗部では「強いやつが奪い、奪われるヤツが悪い」という、力こそ正義の、大開拓時代になったのです。

ネットが本当の意味でみんなが安心して使えるようになるには、ネットに必要が無い消防はのぞき、警察や役所、場合によっては防衛などの秩序を作るシステムが対応しなければならず、それにはまだしばらく時間がかかります。

それでも秩序が形作られる片鱗は見えつつあります。

警察組織などは、インターネットの匿名性を悪用して犯罪を行う攻撃者を、地道な努力と解析で追跡し、特定するための技術を磨きつつあります。

私たちが現実世界の住人であり、完全にはネットの中だけで生きていくことができない以上、ネットの闇に隠れても、攻撃者が人であれば、現実世界でのその痕跡を完全に消すことはできないのです。

しかしそういった公的な能力の向上とともに大切なのは、ネットを利用する全ての人たちが、ネットを守ろうという意識を共有し、協力しあうことです。

現実世界の秩序が、警察だけでなく国民一人ひとりの防犯意識や啓発活動の結果、成り立っているように、ネットも、会社や学校の中や、友だちや家族の間で、どうやったら秩序のある世界にしていけるのか、そのためにはなにができるのかを考えることで、初めて「秩序」「防犯意識」「公衆衛生」の概念が醸成され、「社会全体としてセキュリティを向上する」というベクトルを持つことができるのです。

ネット上の社会インフラの構築と皆のセキュリティ意識の向上、それは車の両輪であり、いずれかが欠けてしまっても、安全なネットは成り立ちません。

そうしてネットが安全な「社会」になることができたとき、子どもたちをネットから遠ざける必要がなくなり、もっとネットの世界とともに進化し、より自由な発想で、新しい才能を開花させることができるようになるのでしょう。

そのためにも、ぜひ皆さん一人ひとりが、それぞれの立場でネットの世界のセキュリティを守る知識をもち、これを行う人になってほしいと思います。

匿名の通信は追跡が困難だが…

ネットでは意図的に正体を隠す環境を利用し犯罪が行う者たちがいます。匿名通信するネット、匿名のSNS、防弾サーバ、成りすましの利用などです。

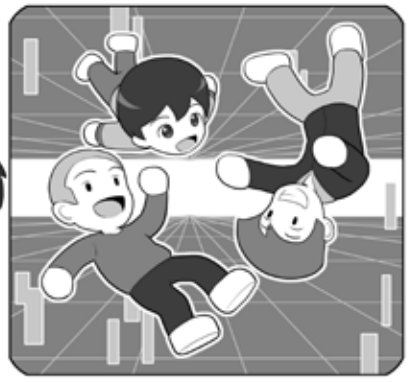
それでも徐々に技術は向上

最近では「バレないと思った」という犯人が捕まえたり、ネットの闇に隠れる攻撃者を追跡する能力が向上しつつあります。

取り締まりは大切だが「防犯意識」醸成も大事

犯罪を起こしたら、きちんと検挙することは抑止力になります。しかし、皆がセキュリティを守ろうという「防犯意識」を醸成することも大切です。

デジタルネイティブの子どもたちに安全な世界を



デジタルネイティブの子たちが犯罪に巻き込まれず、ネットの世界で才能を開花させられるように、ネットの安全を守らなければなりません。

2 デジタルネイティブと未来

パーソナルなコンピュータの歴史が始まってからまだ30年しか経っていないこともあり、世の中にはまだ「パソコン」や「ネットワーク」が存在しなかった時代を知る世代の人がたくさんいます。

これらの人々の一部は、世界にパソコンが生まれ、ネットワークが生まれ、やがて大規模なネットワーク化とインターネットの誕生により「距離と移動に必要な時間が消えた世界」が生まれたときに、その世界に未来を見ました。

やがてその先進的な開拓者たちは、移民のように生活の軸足を新たな世界に移し「デジタルイミグラント(デジタル移民)」と呼ばれるようになりました。

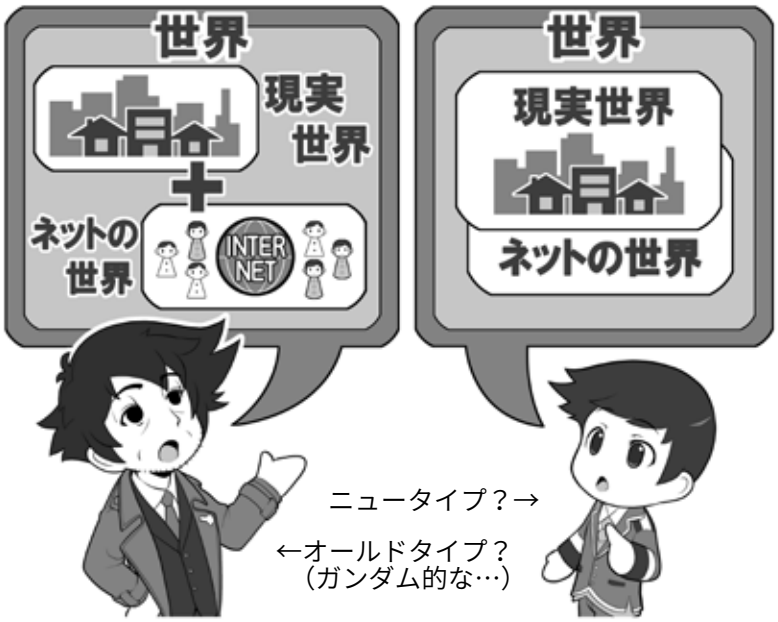
これは現実世界にたとえるならば、旧世界に息苦しさを感じていた人間が、誰も住んでいない新大陸を発見し、夢を描いてそこに移住し、新世界を築き始めたようなものです。

しかしインターネットが一般化したWindows 95から20年、初代スマートフォンと呼べる存在であるiPhoneが誕生から10年の時が過ぎると、多種多様な人々がその世界に移住してきましたし、「距離と移動に必要な時間が消えた世界」にも子ども達が生まれ、ネットを無意識に使いこなす「デジタルネイティブ」と呼ばれる世代が形成されるようになってきました。

そういった世代が社会の中心となると、いままで距離と時間の概念によって形成されていた世界の国の人たちとの意識の壁が、技術に力とともにあっけなく解決されていくかもしれません。

海外で生まれた子ども達が多言語をネイティブのように操り、様々な国の考え方を当然のように理解するように、すべてを楽々と越えていくかもしれません。

デジタルイミグラントとデジタルネイティブ



デジタルイミグラントは手紙に対するメールのように、ネットを現実世界のオプションとして捉えて「便利になった」と考えますが、デジタルネイティブには現実とネットの世界は一体であり、メッセージは一瞬で届く「距離と移動に必要な時間が消費されない」コミュニケーションを当たり前と捉えています。

技術の進化で文化の壁をあっさりと乗り越えていくかも

自動翻訳つきテレビ電話は、すでに一部の言語で始まっています。スマホの翻訳アプリでは、発音した言葉を翻訳してしゃべってくれます。言葉という壁、それに伴う意識の壁も、あっさりと壊される日がくるかもしれません。

3 バーチャル空間を超えて世界へ

デジタル機器の進化は、さらにネットと私たちの融合を進めるかもしれません。

たとえば仮想の3次元空間を目の前に実現するバーチャルリアリティシステムは、驚くべき没入感をもち、まるで自分がその空間に存在しているかのように感じさせてくれます。

さらに仮想空間を使って生活することを前提に考えると、現実の世界でしかできないことは意外に少なく「ご飯を食べる」「おトイレに行く」「お風呂に入る」といった生理現象と清潔さに関するものだけになるかもしれません。

そんな世界が来るはずがないと思うかもしれませんが、実は私たちは毎日「夢」で同じような経験をしています。夢の中の出来事を現実の出来事と混同してしまうことがあるように、「経験」とは必ずしも現実世界だけのものではなく、脳にとっては、どれも等しく同じ経験なのかもしれません。

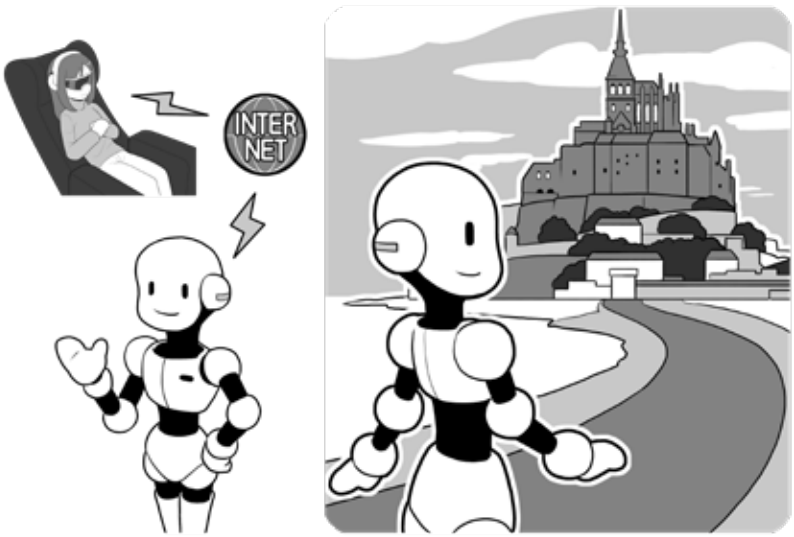
そしてこういった技術がさらに進化を遂げれば、自分の部屋からネット経由でアクセスして、世界各所で「アバターのロボット」をレンタルし、実際にそこに訪れるのと同じように、世界の国々を旅してみたり、その国の人とコミュニケーションをしてみたり、あるいは学校で学ぶことができるようになるかもしれません。

それは体が不自由な人、あるいは病気でベッドから起き上がれない人たちにとっても、社会参加することができるツールにもなるでしょうし、私たちが世界の様々な国の人々との相互に理解しあうこ　とにも役に立つでしょう。

リアルである必要は意外と少ない

ゲームに出てくるような素敵な空間で旅行したり、机を広げて仕事や勉強をしたり、お店があれば買い物をしたりなどバーチャル空間で実現できることはたくさんあります。私たちが夢の世界でやっていることも、現実世界ではないという意味では同じです。一方、ご飯やトイレ、お風呂はバーチャル空間ではできません。残念ながら100%ネットの海に漕ぎ出すことはできません。

バーチャル空間だけでなく、社会参加やネットの向こうの現実世界を旅することも



何らかの事情でベッドから起き上がることができなくても、ネットを通じて「アバター（自分の代わりのロボット）」を使い社会参加し、世界中の様々な国を旅して、コミニュケーションすることができるようになるかもしれません。

4 おわりに

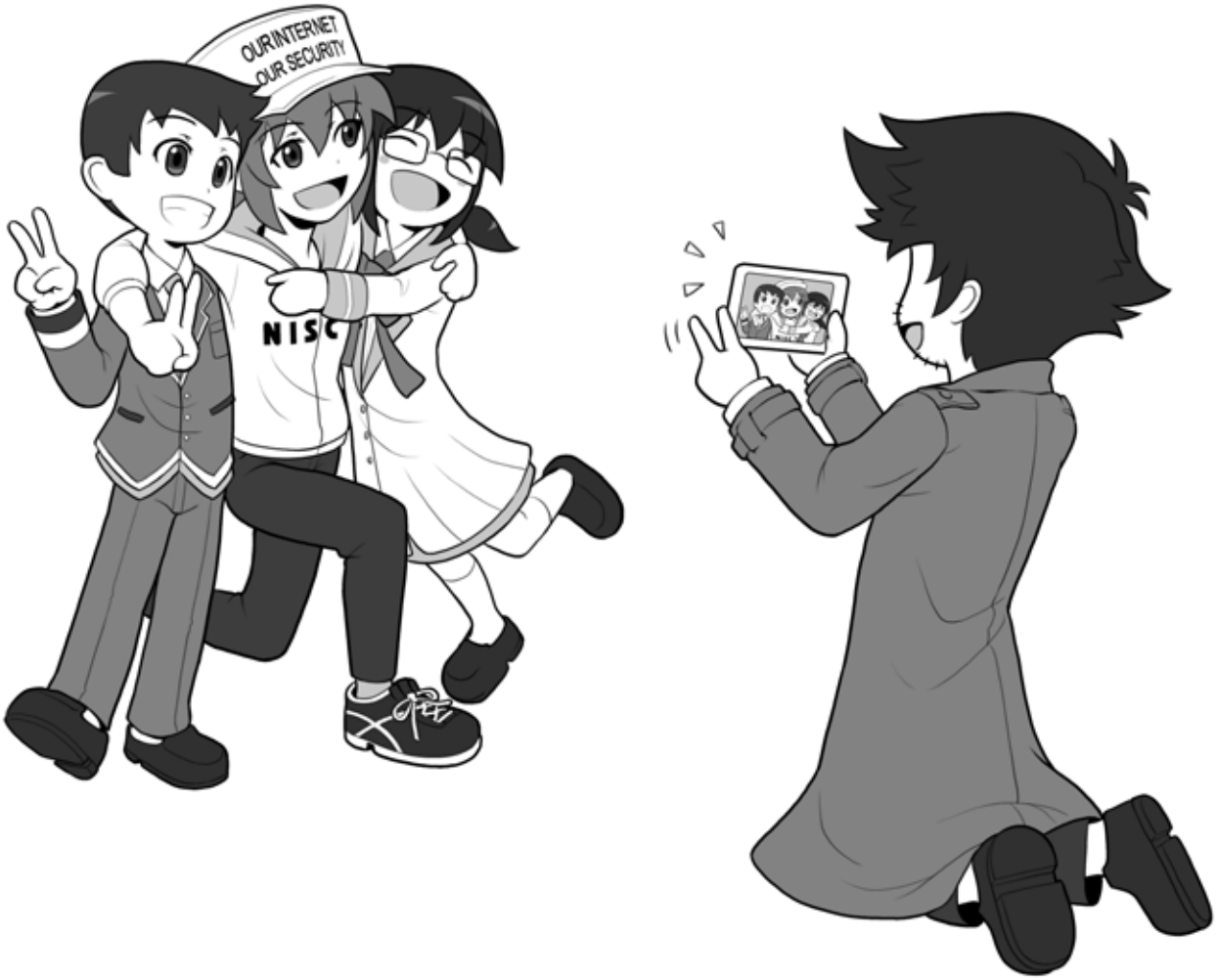
さて少しだけフィクションとして、インターネットとデジタルテクノロジーの進化の果てについて語りました。しかし、これは実現できない未来ではなく、それぞれの要素はすでに種としてこの世界に存在しています。あとはその種の健やかな成長を待つだけです。

しかしこのフィクションには語られなかった部分があります。それはインターネットに潜む影、攻撃者(≒クラッカー)や悪意のハッカーの存在です。

もしあなたがネットの世界でショッピングを楽しんでいるときに悪意のハッカーによる詐欺に遭ったとしたらどうでしょう。買い物はもう嫌となるかも知れません。美しい世界を楽しんでいるときに攻撃者によって怖い仮想空間に引きずり込まれたりしたら、もうそこには近づきたくないと思うかもしれません。

私たちがネットに素晴らしい世界を見出し、ネットの果てに人としての進化があると思ったとしても、それは安全なネット空間があってこそ実現可能なのです。

古来、人は距離とその移動に消費する時間によって、行動する範囲とその可能性を制限されてきました。ほんの少し前までは自分の村から出たことが無いという人も



たくさん存在しました。しかしネットは距離という概念を消失させ、それによって失われていた時間をあなたの可能性に転化します。羽を得て自由になる、それはわくわくしませんか？

それによって生まれる、人間という存在の新たな可能性を見てみたいと思ったならば、ぜひインターネットを安全で安心できる場所にするために、私たちの活動に参加してください。私たちと一緒にネットの未来を守っていきましょう。

さる著名なハッカーが来たるべき未来に「ネットは広大だわ」という意味深い言葉を残しています。

広大なネットは可能性であると同時に、広大であるが故に政府や関連機関、セキュリティ関係企業だけで守り切ることはできるものではありません。

皆さん一人ひとりがネットを守る私たちの仲間となって、私たちともに未来を創ってくれることが必要なのです。

私たちは、皆さんのことを待っていますよ。

可能性の未来でお会いしましょう。

2019年1月

内閣サイバーセキュリティセンター一同

用語集

AES（エー・イー・エス）
暗号化方式の一要素。利用する無線LANの暗号化方式にAESという文字が入っている、WPA-PSK(AES)やWPA2-PSK(AES)という方式は、「暗号キー」を共有しない範囲では安全とされる。また無線LANに限らずファイルやディスクの暗号化方式としても用いられ、数字＋bitで記述される「鍵長」の数字が大きいほど、不正な解読が困難とされる

BIOSパスワード（バイオス・パスワード）
Windowsマシンなどで電源投入時に、OSが立ち上がる前に求められるパスワード

DDoS攻撃（ディードスこうげき）
Distributed Denial of Service Attack。攻撃者などがゾンビ化した多量のパソコンなどから攻撃目標に一斉に多量の問合せなどを行い、攻撃対象の反応が追いつかず利用できない状況にする攻撃。何種類かの類型がある

ECサイト（イーシー・サイト）
Electronic Commerceサイト。インターネット上にある商品販売店舗

EV-SSL証明書
（イーブイ・エスエスエルしょうめいしょ）
Extended Validation証明書。従来のSSL証明書に対して、審査を厳格に行った証明書。証明書を取得した会社名が表示されるため、詐欺サイトではないか、簡単に確認することができる

GPS（ジー・ピー・エス）
Global Positioning System。多数の人工衛星で構成される衛星測位システム。この衛星からの電波を使い計算を行うことで、現在地を測定することができる。主として米国が運用しているが、2018年春より日本版GPS「みちびき」が運用予定

ID（アイ・デイー）
機器やウェブサービスなどを利用する時に、利用者を識別する名称。「ログインパスワード」とセットで、正統な利用者であることを証明する

IMAP（アイマップ）
Internet Message Access Protocol。メールサーバからメールを受信するための通信上のお約束（方法）。POPと異なるのは、メールがサーバ上にメールを残した状態で管理できるので、ウェブブラウザがあればどこからでもアクセス出来るウェブメールなどで使われることが多い。メールソフトでも利用可能。通常はVer.4のIMAP4が使われる

IoT（アイ・オー・ティー）
Internet of Things.。「物のインターネット」とも言われるが、何でもかんでもネットにつなげてしまおうというイメージの考え方。しかし、製造する業者が全てネットワークセキュリティに詳しいとは限らず、攻撃者から見て踏み台にしやすい機器を増やす原因ともなっている

JailBreak（ジェイルブレイク）
AppleのiPhone、iPadなどで規約に反した改造を行い、公式ストアでは認められていないアプリなどをインストールする行為。製造メーカーが設計したセキュリティ思想から逸脱するため、マルウェアへの感染や乗っ取りなどの攻撃に遭う確率が高くなるため、大変危険な行為。やっちゃだめ、絶対

Linux（リナックス）
Windows、macOSとも別の、基本的には「みんなで作る無料のOS」。一般の人も利用可能だが、サーバや工業機器やIoTなど、あまりコンピュータであることを意識しない電子機器でよく使われている。様々な種類のLinuxが存在する他、私たちが普段使っている著名なOSの元になっている場合もある

LTE（エル・ティー・イー）
Long Term Evolution。携帯電話の最近の通信規格。携帯電話回線を提供する会社が個別に名称をつけている場合もあるが、主に４Ｇと呼ばれるタイプのものの総称。高速な無線通信回線ネットワークとしてWANと呼ばれることもある

microSD（マイクロエスディー）
パソコンやスマホなどで使われる、小型のメモリカード。SDカードの超小型版

NISC（ニスク）
National center of Incident readiness and Strategy for Cybersecurity。内閣官房内閣サイバーセキュリティセンターの略称　→内閣サイバーセキュリティセンター。内閣府ではない。

Office製品（オフィスせいひん）
Microsoft Officeなどに代表される、ワープロ、表計算、プレゼン用ソフトなどの総称。

OpenID（オープン・アイ・ディー）
→ソーシャルログイン

OS（オー・エス）
Operating System。
→オペレーティングシステム

「PINコード」（ピンコード）
狭い意味ではスマホなどを利用する時に打ち込む、暗証番号のようなもの。複数回入力を間違うと明示的な入力遅延や入力画面がロックされるなどの規制がかかるものを指す。間違えすぎると強制的にデータを消去する「ワイプ」機能があるものも。本書では機器やサービス利用時に、4〜6桁程度の数字で打ち込むものとして定義

POP（ポップ）
Post Office Protocol。メールサーバからメールを受信するための通信上の規約。IMAPと異なり、基本的にはメールをメールサーバからダウンロードして管理する。ただし、メールソフトの側で「メールサーバ」に残すという設定をした場合は、複数のメールソフトからダウンロードすることも可能。通常はVer.3のPOP3が使われる

POSレジ（ポスレジ）
Point of Salesレジ。販売した段階でその情報が送信され、集中管理されるシステム。内部にはコンピュータが入っており、ネットに接続されているのでマルウェアに感染する事例もある。IoT機器

RMT（リアル・マネー・トレード）
Real Money Trade。ゲームなどで出現したレアな装備を、現実世界の通貨で売買すること。ゲームの規約違反となっていることもある。また販売に関して詐欺や様々なトラブルの発生もしている。レア武器は自力で出しましょう

root化（ルートか）
Androidスマホなどで本来提供されていない、機器の管理者権限を奪取する改造。通常インストール出来ないアプリなどがイントール可能となる。これを行う事はメーカー本来のセキュリティ設計思想を逸脱しサイバー攻撃に弱くなるため、行ってはいけない

SIM（シム）
スマホなどで携帯電話回線を利用するために挿入する小型のカード。電子的なeSIMもある。

SIM認証（シムにんしょう）
公衆無線LANなどで、「暗号キー」を他人と共用しないように、それぞれの利用者によって異なるSIMの情報を使って認証を行う方式

SIMフリー（シムフリー）
スマホなどの端末が、特定の携帯電話会社のSIMだけでなく、どの会社のSIMでも利用できるようになっている状態。使えないように制限されている状態はSIMロックと言う。ただし、SIMフリー端末であっても、どの会社の回線でも利用可能とは限らない。携帯電話会社が提供している周波数とスマホが使える周波数が合っている必要がある。

SMS（ショートメッセージ）
スマホなどで電話番号宛てで送受信できるメッセージ。携帯電話回線契約があればデータ通信契約が無い状態でも送受信出来る。一方、電話番号が無い場合や、データ通信専用SIMでSMSが提供されていない契約では送受信出来ない。SMSがオプションとして提供されている場合もある

SNS（エス・エヌ・エス）
Social Networking Service。会員制のサービスで、メッセージのやりとりやブログ風の発信などを行う。アカウントを作らないと閲覧できないものと、アカウントがなくてもウェブブラウザから閲覧できるものなど、様々な形態がある

SSD（エスエスディー）
Solid State Drive。従来パソコンなどで用いられてきた大容量ディスクであるハードディスク(HDD)に代わり、回転や可動部分がなく、電子的なメモリだけでこれを代替する機器。HDDより小容量で比較的高価だが高速

SSL（エス・エス・エル）
→SSL/TLS

SSL/TLS
（エス・エス・エル／ティー・エル・エス）
Secure Socket Layer / Transport Layer Security。データを暗号化して送受信する方法で、SSLのほうが古く、これを改訂して進化させたものがTLS。SSLがTLSの元になったこともあり、未だにSSLと呼ばれたり、SSL/TLSと書かれたりするが、古い資料やバージョンを明記しているものを除けば同義の意味と考えて良い

SSL証明書
（エス・エス・エルしょうめいしょ）
SSLで通信を行うサーバの身分証明書のようなもの

Stuxnet（スタックスネット）
イランの核燃料施設を攻撃するために用いられたマルウェア。USBメモリを経由しエアギャップを越えて感染するように設計されている。攻撃するだけであれば、人の手を使いエアギャップを越えることは可能であることを示した例

TKIP（ティーキップ）
Temporal Key Integrity Protocol。暗号化方式の一つだが難しく考えないで、無線LANアクセスポイントの暗号化方式にこの文字が入っていたら、危険と考え利用を避ける

TLS（ティ・エル・エス）
→SSL/TLS

TPM（ティー・ピー・エム）
Trusted Platform Module。パソコンなどの内蔵ディスクの暗号化を加速するチップ。「暗号キー」を秘匿し、本体が盗難された場合でも解読を困難にする。内蔵ディスクだけが盗まれた場合は、TPMは本体に残るので「暗号キー」は秘匿され、当然解読が困難になる

UPnP
（ユニバーサル・プラグ・アンド・プレイ）
Universal Plug and Play。ルータに内蔵されている機能で、家や会社のLAN側にある機器を、難しい設定抜きでインターネット側からアクセス可能にする。LAN内の機器がインターネット側からアクセスされ、「踏み台」にされる事もあるので、利用しない方が安全

URL（ユー・アール・エル）
インターネットのウェブサイトの住所を示す文字列

USB（ユー・エス・ビー）
Universal Serial Bus。パソコンなどに周辺機器を簡単に接続する為の規格

USBキー（ユー・エス・ビー・キー）
USB端子に接続して、機器やサービスの正統な利用者である事を証明する物理的な鍵の役割を果たすもの

USBチャージャー（ユー・エス・ビー・チャージャー）
USB経由で機器を充電出来るようにするためのもの。AC電源、乾電池や充電池、車の電源ソケットを利用して充電できるものがある

VPN（ブイ・ピー・エヌ）
Virtual Private Network。仮想プライベートネットワーク。業務用としてはインターネットを利用しながらセキュリティを守りつつ、独立したネットワーク間をLANのように接続する。一般の利用者用には、自分の機器からインターネット上の安全とされる出口サーバまでの区間の通信をすべてまるっと暗号化する

WAN（ワン）
Wide Area Network。LANに対になる言葉で、広域な無線通信回線ネットワークを指す。LTE（4G）やWiMAXがこれに含まれる

WEP（ウェップ）
Wired Equivalent Privacy。暗号化方式の一つだが、容易に解読可能で安全ではない。無線LANアクセスポイントの暗号化方式にこの文字が入っていたら危険と考え利用を絶対に避ける

Wi-Fi（ワイ・ファイ）
→無線LAN

Wi-Fiルータ（ワイ・ファイ・ルータ）
→ルータ

WiMAX（ワイマックス）
高速な無線通信回線ネットワークの一つ。WANと呼ばれることも

WPA（ダブリュー・ピー・エー）
Wi-Fi Protected Access。無線LANの暗号化方式の一つで、WPA-PSK(AES)と書かれたもので、「暗号キー」を他人と共有しない限り安全。TKIPと入っていれば利用を避ける。公衆無線LANでこの方式を採用している場合は、「暗号キー」を他人と共有する場合もあるので注意

WPA2（ダブリュー・ピー・エー・ツー）
Wi-Fi Protected Access 2。WPAをより強力にしたもので、AESが標準となった。「暗号キー」を他人と共有しない範囲では安全とされている。もしTKIPと入っているものがあれば利用は避ける。公衆無線LANでこの方式を採用している場合、「暗号キー」を他人と共有する場合は危険

WPA3（ダブリュー・ピー・エー・スリー）
Wi-Fi Protected Access 3。WPA2で近年発見された特殊な脆弱性や、その他無線LANにまつわる問題点の多くを解消する暗号化方式。

アオリ行為
SNSやブログなどを使って、他人の発言を取り上げ、批判的なコメントをして「炎上」状態にしようとすること

アクセスポイント
無線LANで通信するために、使用している機器を接続する先、およびその機器

アクティベーションコード
ソフトウェアをインストールしたり、コンビニなどで売っている、音楽サービスやゲームなどへのチャージカードを、利用可能にするために用いる。認証処理をするために入力時にネットに接続されている必要がある場合もある。

アタッカー
→攻撃者

アップデート
セキュリティ改善要素が含まれているかどうかは関係なく、ソフトウェアやアプリの更新

アップデートファイル
アップデートを行うためのインストールファイル

アバター
ゲームやSNSなどで自分の代わりの役割を担うキャラクター。あるいは現実世界で代理をになうロボット

アプリ
パソコンやスマホなどで、何らかの機能を実現するプログラム。主にスマホで使われ、一部パソコンでも使われている名称

アプリ連携
複数のアプリ間で機能を連携する事。カメラアプリにSNSアプリの投稿機能を連携し、カメラアプリから直接写真付き投稿を行えるようにするなど。権限を渡すことになるので、攻撃者のサイバー攻撃の手口になるので利用非推奨

アンインストール
インストールしてあるプログラムやアプリを機器から削除すること

暗号化
文章などを正統な利用者以外が読めないように加工すること

暗号化キー
暗号化と復号のために利用する鍵となる文字列。短く複雑でない暗号化キーは総当たりによって探り当てられやすい。また何らかの理由で流出したり、意図せず共有すると、キーを入手したものによって暗号化した内容が復号される。本書では「暗号キー」という

暗号化チップ
暗号化をより高速に行う為の、専用のチップ。≒TPM

暗号化方式
暗号化の方式。一部の古い方式では「暗号キー」がなくても解読出来るものもある。暗号化するときには利用する暗号化方式の安全性に注意が必要

暗号化メディア
暗号化されたメディア。SSDやHDD、USBメモリなどのメディアを暗号化する

「暗号キー」
本書では暗号化と復号に使う鍵の名称として定義

アンダーカバー
潜入調査

インストール
プログラムやアプリを、スマホやパソコンに導入し、使える状態にすること

インターネットバンキング
インターネットを使って銀行の取引を行うサービス

インターフェース
パソコンやスマホを利用する為の操作画面や操作方法

ウイルス定義ファイル
セキュリティソフトがマルウェアを検出するためのファイル。実世界で言えば顔写真付きの手配書のようなもの

ウェブサーバ
ネット上でホームページを表示するためのサーバ

ウェブブラウザ
ネット上で公開されているウェブサーバを閲覧するためのソフトウェアやアプリ

オフラインアタック
攻撃者が暗号化されたデータなどを入手し、制限がない環境で解読攻撃を行うもの。主にネットに接続しないで出来る攻撃なので、オフラインという。＝オフライン攻撃

オペレーティングシステム
パソコンやスマホの機器の上で動作し、利用者に操作用のインターフェースを提供するソフトウェア。Windowsパソコンの Windows。Apple社パソコンの mac OS、Androidスマホの Android OS、iPhone/iPadの iOSなど

オレオレ証明書
本来認証局に申請して発行してもらう証明書を、勝手に発行し暗号化通信を行うために利用するもの。この証明書を利用しているウェブサイトにウェブブラウザでアクセスすると、警告が表示される。接続してはいけない

オンラインアタック
攻撃者がウェブサービスなどに、不正にログインを試みる攻撃など。ネットを経由した攻撃が主なのでオンラインという。＝オンライン攻撃

オンラインストレージ
ネット上に存在するデータ保管用のサーバ

ギブアンドテイク
ソーシャルエンジニアリングの手法で、相手に何かのメリットを与える事で、自分の目的の情報を引き出す手法

クラウドサーバ
インターネット上に存在する、データやアプリなどを保存しておくサーバ。主に「機器のディスクと同等に利用できる」「利用している意識はないが使っている」状態のものを指す。これに対して転送を意識して使用するものは「オンラインストレージ」と呼ばれやすい。スマホなどでは設定をよく確認しないと、知らないうちに、写真などのバックアップに使ってしまっていることもあるので注意

クラッキング
攻撃者が他者のアカウントや機器、サーバなどに不正に侵入すること。セキュリティを割って入るの「割る」の Crack から来ており、クラッキングを行う攻撃者をクラッカーとも呼ぶ

検体
セキュリティ会社などがセキュリティソフトでマルウェアを排除できるように、そのマルウェアを解析するための実物のサンプル

攻撃者
悪意を持ってサイバー攻撃やそれに付随する攻撃を行うもの。悪意のハッカー。ブラックハットハッカー。本書では「ハッカー」の語源が悪意があるかどうかとは関係が無いので、攻撃を行うものとして「攻撃者」とする。＝アタッカー。≒クラッカー

虹彩
目の中にある円盤状の膜で、人によって違っており、生体認証の要素として使われる

公衆無線 LAN
街中や店舗などで、不特定多数に対して インターネット接続環境を提供する無線 LAN のこと

サービス連携
パソコンなどを使って複数のウェブサービスの間で連携をすることをサービス連携と呼ぶ。その中で特にスマホ上でアプリによって連携をすることをアプリ連携と呼ぶ場合があるが、内容は同じ

辞書攻撃
「ログインパスワード」などによく使われる文字列を集めて辞書化したものを使い、不正に他人のアカウントにログイン出来ないかを試みる攻撃

侵入テスト
会社や組織のネットワークに、外部から不正侵入することが出来ないか行うテスト。ペネトレーションテストともいう

スタンドアロン
ネットワーク（繋がっていること）と対になって使われる言葉で、ネットワークに繋がっておらず単独で存在すること。ただし、ネットに繋がっていて、かつ他の機能や機器と連携しないで動作する場合もスタンドアロンと表現する

ステルス状態
パソコンなどが起動していないように見えて、実際は動作している状態

スパムメール
元々はインターネットの初期、不特定多数に対して多量に送られてきた広告メールなどの迷惑メールを指す。攻撃者がこの方法を用いてマルウェア感染などを狙う攻撃をしたり、詐欺サイトに誘導するフィッシングメールなどに利用することもある。この場合はスパムメールでありフィッシングメールでもあることになる。サイバー攻撃に用いられる場合は、特定の誰かを狙った「標的型攻撃（標的型メール）」に対して不特定多数を狙うため「ばらまき型攻撃」と呼ばれることもある

スマートウォッチ
スマホと連動したり、単独でネットに接続して何らかの情報をやり取り出来る腕時計型の機器

スマート家電
単独でネットに接続して、何らかの情報をやり取りしたり、動作の指示を受け付けられる家電機器

セキュリティアプリ
スマホなどのセキュリティを確保することに貢献するアプリ

セキュリティホール
パソコンやスマホのシステム上、攻撃者が不正な侵入などを行える状態になっている「穴」のこと

セキュリティキー
→「暗号キー」

セキュリティソフト
パソコンなどのセキュリティを確保することに貢献するソフトウェア

セキュリティパック
パソコンやスマホなどのセキュリティを向上するために、複数の機能がパッケージになって提供されているもの

セキュリティパッチ
パソコンやスマホのシステム上に開いた、セキュリティの「穴」を塞ぐために、メーカーなどから提供される修正プログラム。パッチワークのパッチから来ている

ゼロデイ攻撃
セキュリティホールが公になってから、メーカーなどがその穴を塞ぐための修正プログラムを提供するまでの期間に行われる攻撃。この期間に攻撃を受けると、防ぐ手段はないため、利用者自身が「避ける手段」を講じる必要がある

総当たり攻撃
攻撃者が「ログインパスワード」や「暗号キー」を破るために、全ての文字などの組み合わせを試す攻撃

ソーシャルログイン
特定のSNSやウェブサービスのIDを使って、他のSNSやウェブサービスを利用可能にする規格。特定の身分証明書で、他のサービスを利用できるイメージ。新しいサービスを利用するためにいちからアカウントを作る手間を省く事ができる。OpenIDとほぼ同義だが、他にもソーシャルログインに見える機能は存在する。本書では非推奨

ソース
「情報ソース」の意味で、発信された情報の発信元。発生した事象そのものを明確に見たり聞いたり体験した上で発信しているものを一次ソースと言う。伝聞などで発信しているものを二次ソース、三次ソースと呼び、次第に信憑性が低くなったり、本来の意味とは別の意味で使われている可能性が高くなる

ソフト
ソフトウェア(≒プログラム)の略。対になる言葉は機器を意味するハード(ハードウェア)

ソフトウェアトークン
二段階認証などで使われる使い捨てパスワード(ワンタイムパスワード)を出力するトークンを、ソフトウェアで実現しているもの。例えばソフトウェアトークンを出力するスマホ用アプリ

多要素認証
サービス利用時に行う利用者認証を、3つの要素(①知っているもの②持っているもの③本人自身に関するもの)のうち、2つ以上の要素を用いて行うもの。3つの要素すべてを使う場合などもあり得る

チート行為
ゲームなどで本来認められた方法ではなく不正な方法によるプレイ。またはそれによって利益を得る行為

通知ウインドウ
パソコンなどで、何らかの通知を出す表示の事

通知機能
エラー発生、メール受信、その他のアラートなどを利用者に通知する機能

使い捨てパスワード
二段階認証などで用いられる、利用するたびに更新されるパスワード。ワンタイムパスワード

ディクショナリアタック
→辞書攻撃

データローミング
ローミングに関して、データ通信のローミングを行う事

テザリング
パソコンなどで、スマホなどを経由してインターネット接続をする方法。スマホをルータとして利用するなど

デジタルイミグラント
現実世界からデジタル世界に、移民のようにその生活の一部を移し、これを使いこなす世代。主にパソコンが普及していない時代に生まれた人が多い

デジタルネイティブ
生まれた時代に既に十分にネットが普及しており、現実世界とデジタル世界を垣根無く一体に使いこなす世代

ドライブバイダウンロード攻撃
いずれかのウェブサイトを訪れただけで、何らかのプログラム(この場合はマルウェア)のインストールが発生する攻撃

トラッシング
ゴミ箱に捨てられた紙などから重要な情報を探し出すソーシャルエンジニアリングのテクニック

内閣サイバーセキュリティセンター
正式名称は「内閣官房内閣サイバーセキュリティセンター」。日本政府のサイバー政策の策定や政府機関へのサイバー攻撃の検知と調査を行っている機関。国民への情報セキュリティ意識の啓発も行う。通称NISC。なお内閣府ではない

二段階認証
利用者認証を2回に分けて行うもの。多要素認証と異なり、同じ認証の要素で2つの段階に分けてもそう呼ぶことがある

認証局
申請に基づきSSL証明書の発行を審査する機関

ネームドロップ
業務上の上司や立場が上の人間を装って要求を実行させるソーシャルエンジニアリングの手法

ネチズン
ネットをよく利用する人物を指す、国内ではやや古い呼称。ネットワーク市民（Network Citizen）の略

ネットワーク暗証番号
通信事業者のサービスを利用する際に、利用者が本人であることを認証するための暗証番号

ネットワークカメラ
主にネットワーク上に設置された監視カメラ。セキュリティ上は主にインターネット上から直接存在が見えるものを指し、サイバー攻撃の対象となりやすい。IPカメラとも呼ばれる。IoT機器

ネットワークキー
無線LANでアクセスポイントへの接続や通信の暗号化に使われる鍵。本書では「暗号キー」に分類している

ネットワークルータ
家庭内や会社内のLANをインターネットに接続するための窓口的役割を担う機器。無線LAN機能を内蔵している場合は「無線LANネットワークルータ」「無線LANアクセスルータ」と呼ばれる

野良Wi-Fi
野良猫のように誰が設置したか分からない無線LANアクセスポイント。主に暗号化されておらず誰でも利用できる状態になっているもの。暗号化されていない時代に設置されてそのままのものもあるが、攻撃者が情報を詐取するために設置しているものもある。災害時や観光目的に、運営主体がはっきりして設置される暗号化無しの無線LANアクセスポイントは別

バージョンアップ
アップデートファイルなどを適用して、ソフトウェアやアプリのバージョンが向上すること。セキュリティ関係の更新が含まれることもあり、積極的に適用するべきもの

バーチャル空間
仮想空間とも呼び、主に3Dなどで利用可能なネット上の世界。ゲームなどが現在の主流。VRメガネなどを利用するもののほか、通常のモニターで見るものを指す場合もある

バーチャルリアリティ
仮想空間をあたかも現実世界のように感じさせる技術

ハードウェアトークン
二段階認証などで用いられる使い捨てパスワードを、専用の物理機器として提供するもの

パスコード
一部のアプリなどでPINコードと同じ役割をするものを指す言葉

パスワード
利用しようとしている人が、その機器やサービスの正規の利用者である事を証明する、合い言葉のようなもの

パスワードリスト攻撃
→リスト型攻撃

パターンロック
スマホをロック解除するときに、画面上に表示される複数の点を、あらかじめ登録したパターンでなぞり、ロックを解除する機能

バックアップディスク
パソコンやスマホの情報を別途保存しておき、機器が故障したり紛失や盗難したりした場合に、復元するためのもの。機器の情報の一括バックアップと、目的のデータ毎のバックアップがある

バックドア
機器やシステムに設けられた、正規のログイン方法ではないアクセス方法。攻撃者がシステムに侵入して、再度侵入するために不正に設置する場合や、システム開発者や管理者が管理の手間を省くために設置し、正規のリリース後をそれをわざと残したり忘れてしまっている場合も

パッチ
≒セキュリティパッチ

パラメータ
機器やソフトウェアの設定上の要素

ハリーアップ
ソーシャルエンジニアリングの手法で、相手を急かすことで正常な判断を出来なくなるようにして、目的の要求を通すこと

秘密の質問
ウェブサービスなどでパスワードを忘れてしまい、再度パスワードを設定し直すときなどに本人である確認をするため、あらかじめ設定しておく質問。ただし質問はサービス側が用意したものが殆どで個人情報にまつわるものが多いため、正直に答えているとSNSなどで探し当てられることも

ヒューミント
スパイの諜報活動で、ターゲットの交友関係を調査すること

ヒューリスティック分析
手配書方式のマルウェア検知方法を避ける攻撃が普及してきたため、マルウェアのプログラム上の特徴ではなく、マルウェアの挙動によって判断する方法。別称「ふるまい検知」

標的型メール
攻撃者がターゲットを定めて、マルウェアなどに感染させるために、個人宛のメールを送り付けてくる攻撃。ターゲットの名前だけで無く、業務上のメールと見分けがつかない内容や、場合によっては業務上のつきあいがある人間の名前、あるいはその人間のメールソフトを乗っ取って送られてくることもある

ファームウェア
利用する機器のソフトウェアやアプリではなく、機器自身を動かすプログラム。ソフトウェアやアプリだけでなく、更新されたら必ずアップデートしなければならないもの

ファームウェアパスワード
パソコンの電源投入時に入力を求められるパスワードの名称の一つ。これを入力しないと、そもそも起動することが出来ない。「起動パスワード」

ファイアウォール
パソコンなどのネット接続部に存在するプログラムで、内部から外部へのアクセスは通し、外部からの不正なアクセスを防ぐ壁の役割をする。また企業などでは専用の機器として存在する

フィッシングメール
攻撃者がターゲットから、お金につながる情報や個人情報を盗み取るための詐欺メール。フィッシング(phishing)は洗練された(sophisticated)＋釣る(fishing)から来ている。嘘の情報を餌にして釣り上げるというイメージ

フィルタリングサービス
青少年がネットにアクセスするに当たって、不適切なサイトを閲覧しないようにするサービス

復号
暗号化されたデータを、暗号キーを使って元に戻すこと

不正アクセス通知
利用しているウェブサービスなどに、不正なアクセスが試みられると、スマホなどに通知が送信されてくるサービス

踏み台
攻撃者がサイバー攻撃を行う際、正体を隠すためにコントロール下においたパソコンなどを一旦経由すること。≒ゾンビ化

フライトモード
スマホなどを飛行機で移動中に使えるように、外部に電波を発しない状態にするモード。それに伴い電池の消費が少なくなるので、災害時の省電力モードとしても利用できる

ブラウザ
→ウェブブラウザ

ブラウザ版
SNSなどで、アプリではなくウェブブラウザを使ってアクセスするために提供されているもの

フリーメール
無料で提供されるメールサービス。広告などが表示されるか、利用者の利用情報を提供する代わりに無料で利用できる

フレンドシップ
ソーシャルエンジニアリングのテクニック。友情を持って接する事で要求を断りにくくする

プロダクトキー
OSなどをインストールするときに、正統な利用者である事を証明するための文字列。パソコンにインストールされた状態で販売されるものは本体にシールで貼ってあり、店頭などで単体で販売される場合はパッケージ内部に封入されている。紛失すると再インストールすることが出来なくなる

プロバイダ
インターネットの接続環境を提供する企業。インターネット回線と提供する企業が同一の場合と、別々の場合がある

ベンダー企業
ソフトウェアやハードウェアなどの製品を販売する企業

ポート
パソコンやスマホがネットを通じて相手とデータを送受信するための窓口。それぞれに数字が振られ、これを「ポート番号」という。また送信するものを「送信ポート」、受信するものを「受信ポート」と呼ぶ

ボット
ロボット(robot)の短縮形。様々な作業を自動化したプログラムのことでTwitterで自動的に呟くものが有名。「悪意のボット」となると、パソコンやIoT機器などを乗っ取ってゾンビ化するためのプログラムを指す

ボットネット
悪意のボットにコントロールされた機器で構成される集合体。パソコンやIoT機器などの機器が、コントロール用のサーバによって管理され、DDoS攻撃などに利用される

マネタイズ
何らかの手段で得たモノや情報、システムをお金に換えること

マルウェア
攻撃者が目的とする機器を攻撃するために利用する不正なプログラム

マルバタイジング
マルウェアを含んだ広告を用いるサイバー攻撃。攻撃者がウェブサイトを閲覧したものを感染させるために広告ネットワークにお金を払って出稿する

水飲み場攻撃
攻撃者が目的とする相手(個人もしくは企業の構成員など)を、マルウェアに感染させるために、あらかじめ訪問しそうなサイトにマルウェアを仕込んで待つこと。砂漠などで動物が水があるところによってくる様子からつけられている

無線LAN
ネットで用いられる通信に、無線の信号を用いるもの。LANはLocal Area Networkの略で、通常は会社や家など小さい単位で用いる。インターネットとはルータを境にネットワーク的には分離されている(データの行き来は可能)。これに対して広範囲を対象とするネットワークはWAN(Wide Area Network)と呼ぶ

無線LANアクセスポイント
無線LANを利用するために、無線LANアクセスルータによって提供される接続環境、もしくはその機器。本書では環境を指している

無線LANアクセスルータ
無線LANアクセスポイントを提供する機器

無線WAN通信機能
WANとはLANのLocal Area NetworkにするWide Area Networkの意味。通信電波の供給範囲が広いものを指し、主に携帯電話のLTEなどによる通信ネットワークなどを指す

ランサムウェア
パソコンやスマホなどのファイルを暗号化したりロックしたりして使えなくし、「解除してほしかったら身代金(ransom)を払え」と要求してくるマルウェア

リカバリメディア
あらかじめOSがインストールされたパソコンで、不具合が起きたときのOS再インストールのため、購入後作成するべきインストール用のメディア

リスト型攻撃
ウェブサービスなどから流出したパスワードのリストなどを使って、他のサービスでログインを試みる攻撃

リモートワイプ
遠隔操作でスマホやパソコンの中身を消去すること

ルータ
インターネットなどを利用するために利用者が接続・経由する機器。会社や家庭で利用する無線LANアクセスルータの他、高速なWANの回線を利用して、主に屋外などでノートパソコンなどを接続して利用するモバイルルータがある。また有線だけで利用する有線ルータもある

ローミング
携帯電話などで、回線提供会社と個別の契約を結ばないで、他の会社の契約をもって音声通話を利用すること

ログ
その機器で行われた活動を記録したデータ。通信に関するものは「通信ログ」という

ログアウト
機器やサービスの利用している状態を終了すること。ウェブサービスの場合、利用していたウェブブラウザを終了してもログイン状態は継続される場合があるので、明示的にログアウトの操作をする必要がある

ログイン
機器やサービスに接続し、パスワードなどを入れる事で利用できる状態にすること

「ログインパスワード」
本書では機器やサービスを利用状態にするために入力するパスワードとして定義

ロック
攻撃者による不正なログインなどが試みられ、機器やウェブサービスへログインできない状態。自分の意志でその状態にすることもある

ロック画面
スマホを他者が勝手に操作できないような状態にした画面

情報セキュリティ関連サイト一覧

情報セキュリティ関連のサイト

● みんなでしっかりサイバーセキュリティ

内閣サイバーセキュリティセンター（NISC）
https://www.nisc.go.jp/security-site/
NISCが運営する、サイバーセキュリティ関連の情報を発信する普及啓発用サイト。本ハンドブックの配布も行っている。

● 国民のための情報セキュリティサイト

総務省
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/
総務省が運営する、情報セキュリティに関する基礎的なことを学べるサイト。企業向けの対策についても触れられている。

● ここからセキュリティ！

独立行政法人情報処理推進機構（IPA）
https://www.ipa.go.jp/security/kokokara/
IPAが運営する情報セキュリティを学べるサイト。様々なサイトのコンテンツを集約して分類されている。ポータルサイト的存在。

● 情報セキュリティ 安心相談窓口

独立行政法人情報処理推進機構（IPA）
https://www.ipa.go.jp/security/anshin/index.html
IPAが国民に向けて開設している、一般的な情報セキュリティ（主にウイルスや不正アクセス）に関する窓口。

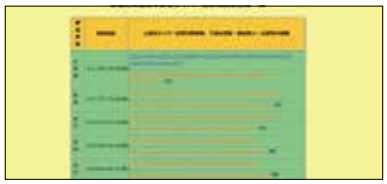
● 情報セキュリティ

独立行政法人情報処理推進機構（IPA）
https://www.ipa.go.jp/security/
IPAが解説するサイトで最新のセキュリティ情報や、情報セキュリティ啓発コンテンツなどを提供している。

● まんが「サイバーセキュリティのひみつ」

独立行政法人情報処理推進機構（IPA）
https://www.ipa.go.jp/security/keihatsu/security-himitsu/
IPAが制作協力をし、学研のマンガひみつ文庫で提供されている。子どもから大人まで楽しめる内容。

● 都道府県警察サイバー犯罪相談窓口



警察庁
https://www.npa.go.jp/cyber/soudan.htm
各都道府県の警察本部のサイバー犯罪の相談窓口と情報発信サイト。

● 消費者ホットライン

消費者庁
http://www.caa.go.jp/policies/policy/local_cooperation/local_consumer_administration/hotline/
消費生活全般の全国共通ダイヤル「１８８（いやや！）」で最寄りの消費生活相談窓口につながります。

NISCのＳＮＳによる情報発信

● Twiter

内閣サイバー（注意・警戒情報）

NISC 内閣サイバーセキュリティセンター 注意警戒情報

@nisc_forecast
フィッシング詐欺・マルウェアなどの注意喚起情報やソフトウェアの更新情報を発信している。

● Twiter

内閣サイバーセキュリティセンター（NISC） 公式アカウント

NISC 内閣サイバーセキュリティセンター

@cas_nisc
NISCの取組やサイバーセキュリティに関連する情報を発信している。

● FaceBook

内閣サイバーセキュリティセンター NISC

NISC 内閣サイバーセキュリティセンター

https://www.facebook.com/nisc.jp/
NISCの活動の紹介や、サイバーセキュリティに関するお役立ち情報を原則1日1回、コラムの形で発信している。

● LINE

内閣サイバーセキュリティセンター（NISC） セキュリティ関連情報

NISC 内閣サイバーセキュリティセンター セキュリティ関連情報

LINEID: @nisc-forecast
原則1日1回、サイバーセキュリティに関するお役立ち情報をコラム形式で発信している。

災害時関連のサイト

● 防災情報のページ

内閣府
http://www.bousai.go.jp/
災害時などに政府発表の情報が逐次公開される。また防災関連会議の情報や、大規模地震対策の計画なども公開されている。

● 防災情報提供センター

国土交通省
http://www.mlit.go.jp/saigai/bosaijoho/
リアルタイムの雨量情報他、ハザードマップ、傘下の気象庁発信の情報や、知識を学べる情報なども提供されている。

● 災害用伝言板（web171）

NTT東日本、NTT西日本
https://www.web171.jp/
災害発生時に設置される「災害用伝言ダイヤル」を、ウェブ経由から利用できるようにしたのがweb171。ウェブ経由でも共有できる。

● 災害・防災情報

国土交通省
http://www.mlit.go.jp/saigai/
災害時の状況や復旧状況を、国土や交通インフラの面から提供。情報は逐次更新され、地震、火山、風水害、雪害時などの状況が発信される。

● 気象庁 ホームページ

気象庁
https://www.jma.go.jp/jma/index.html
天気予報や気象全般に係わる情報、警報注意報、地震・津波・火山などの緊急時の情報、そしてさくらの開花状況まで提供される。

● 安否情報まとめて検索

J-anpi
https://anpi.jp/top
災害時に様々な形で提供される安否確認情報を、横断検索して確認をしやすくするためのシステム。NTTとNHKが提供。

● 公衆電話 設置場所検索

NTT東日本
https://service.geospace.jp/ptd-ntteast/PublicTelSite/TopPage/

● 公衆電話 設置場所検索

NTT西日本
https://www.ntt-west.co.jp/ptd/map/

● 公衆電話インフォメーション：公衆電話の種類と利用方法について

NTT西日本
https://www.ntt-west.co.jp/ptd/mag_public_kind.html

いじめ対策関連

● 子供（こども）のSOSの相談窓口（そうだんまどぐち）

文部科学省
http://www.mext.go.jp/a_menu/shotou/seitoshidou/06112210.htm
子供が自分自身で抱える不安や悩みを相談できる相談窓口を集約してあるサイト。

● インターネット人権相談窓口へようこそ！

法務省
http://www.moj.go.jp/JINKEN/jinken113.html
差別、いじめ、嫌がらせ等人権に関する問題で困っている方が気軽に相談できる窓口を掲載。英語や中国語にも対応。

● ここにもあります！相談できる窓口が。「いじめ」しない させない 見逃さない

政府広報オンライン
https://www.gov-online.go.jp/useful/article/201505/2.html
様々な「いじめ」がある最近の現状と、大人と子どもができる「いじめ」へのかかわり方について解説された記事を掲載。

Twitterアカウント

- 首相官邸（災害・危機管理情報）@Kantei_Saigai
- 内閣府防災　@CAO_BOUSAI
- 総務省消防庁　@FDMA_JAPAN
- 気象庁　@JMA_kishou
- IPA(ICATalerts)　@ICATalerts
- JPCERTコーディネーションセンター @jpcert
- フィッシング対策協議会 @antiphishing_jp
- Twitterライフライン @TwitterLifelin

索引

アルファベット

AES ・・・・・・・・・・・・ 66,68,69,146
BIOS パスワード ・・・・・・・・・ 98,146
DDoS 攻撃 ・・・ 18,42,44,45,120,134,146
EC サイト ・・・・・・・・・・・・ 81,146
EV SSL 証明書 ・・・・・ 74,75,76,81,146
GPS・・・・・・・・・・・・・・・・・・・
92,99,102,113,125,127,131,137,138,146
IMAP ・・・・・・・・・・・・・・ 78,146
IoT ・・・・・・・ 17,26,28,30,45,53,146
JailBreak ・・・・・・・・・・・・ 28,146
microSD・・・・・・・・・・・・・95,96,147
Office 製品 ・・・・・・・・・・・・ 25,147
PIN コード・・・ 32,36,52,53,54,55,56,58,
85,92,93,102,119,147
POP・・・・・・・・・・・・・・・・ 78,147
POS レジ ・・・・・・・・・・・・ 17,147
RMT ・・・・・・・・・・・・・ 119,147
root 化 ・・・・・・・・・・・・・ 28,147
SIM ・・・・・・ ,69,127,129,130,131,147
SIM 認証・・・・・・・・・・ 66,68,69,147
SIM フリー・・・・・・・・・・130,131,147
SMS・・・・・・ 37,38,59,130,131,135,148
SSL 証明書・・・・・・ 73,74,75,76,81,148
Stuxnet ・・・・・・・・・・・・・・・ 86
TKIP ・・・・・・・・・・・・・66,69,148
TPM ・・・・・・・・・・・・・・ 99,148
UPnP ・・・・・・・・・・・・・・ 68,148
USB チャージャー ・・・・・・・ 130,149
VPN・・・・・・・ 70,71,72,73,78,137,149
WEP ・・・・・・・・・・・ 61,66,69,149
Wi-Fi ・・・52,64,65,67,85,89,129,137,149
Wi-iFi ルータ・・・・・・・・・・26,64,149
WPA ・・・・・・・・・・ 61,66,68,69,149
WPA2 ・・・・・・・・・・ 66,68,69,149

あ行

アオリ行為・・・・・・・・・・・ 115,149
悪意のボット・・・・・・・・・ 16,18,42,44
アクセスポイント・・・ 44,64,65,66,67,68,
69,70,71,72,73,76,94,104,128,149
アクティベーションコード・・・・ 43,149
アタッカー・・・・・・・・・・・・ 15,149
アップデートファイル・・・・・・ 26,149
アバター・・・・・・・・・・・・ 143,149
アプリ連携・・・・・・・・ 60,104,105,150
アンインストール・・・・・・・・ 105,150
暗号化キー・・・・・・・・・ 52,65,69,150
インターネットバンキング・・・・・・・
43,74,76,86,87,150
インターフェース・・・・・・・・・ 22,150
ウイルス・・・・・・・・・・・・16,64,121
ウイルス定義ファイル・・・・・・ 25,150
ウェブブラウザ・・・・ 25,26,29,31,67,70,
72,74,75,76,77,81,90,103,150
ウォードライビング・・・・・・・・・ 44
エアギャップ・・・・・・・・・・ 86,87
炎上・・・・・・・・・・・・・111,112,115
オシント・・・・・・・・・・・・・・・ 50
オフラインアタック・・・・・・・・ 54,150
オレオレ証明書・・・・・・・・・ 75,151
オンラインアタック・・・・・・・・ 54,151

か行

キーロガー・・・・・・・・・・・・ 16,129
ギブアンドテイク・・・・・・・・・ 20,151
共通鍵暗号方式・・・・・・・・・・・ 85
クラウドサーバ・・・・・・・ 90,96,100,151
クラッカー・・・・・・・ 15,16,39,144,151
クラッキング・・・・・・・・ 29,57,120,151
検体・・・・・・・・・・・・・・・ 27,151
公開鍵暗号方式・・・・・・・・・・ 79,85
虹彩・・・・・・・・・・・・・・32,56,151
公衆無線 LAN・・・・・・・・・・・・・
64,65,66,68,69,70,71,76,89,94,129,151

さ行

サービス連携・・・・・・・・・ 60,105,151
シギント・・・・・・・・・・・・・・・ 50

辞書攻撃・・・・・・・・・ 30,53,55,90,151
ショルダーハッキング・・・・・・・・・ 36
スタンドアロン・・・・・・・ 31,57,86,151
ステルス状態・・・・・・・・・・・ 99,152
スパムメール・・ 36,37,40,42,46,82,83,152
スマートウォッチ・・・・・・ 59,62,63,152
スマート家電・・・・・・・・・・26,28,152
スマートテレビ・・・・・・・・・・ 17,126
スマート冷蔵庫・・・・・・・・・ 17,28,45
生体認証・・ 32,55,56,58,60,63,92,98,102,
セキュリティアプリ・・・・・・26,28,152
セキュリティホール・・・・・17,20,22,23,
24,26,29,45,77,103,104,105,152
セキュリティキー・・・・・・・52,63,152
セキュリティパック・・・・・・22,28,152
セキュリティパッチ・・・・・・23,29,152
セクスティング・・・・・・・・・・・ 19
ゼロデイ攻撃・・・・・・・ 24,29,37,152
総当たり攻撃・・ 30,31,52,53,54,55,56,152
ソーシャルエンジニアリング・・・・・・
20,23,35,36,39
ソーシャルログイン・・・・・・58.60,152
ソフトウェアトークン・・・ 22,59,62,153
ゾンビ化・・・・・・・・・・・・ 44,120

た行

ダークウェブ・・・・・・・・・・・ 120
多要素認証・・・・・・・・・・・・・・
22,23,32,43,55,56,59,64,75,76,153
チート行為・・・・・・・・・・ 119,153
通知機能・・・・・・・・・・・・ 93,153
使い捨てパスワード・・・・・32,62,75153
ディクショナリアタック・・・・・ 55,153
データローミング・・ 127,129,130,131,153
テザリング・・・・・・・・・ 70,103,153
デジタル遺産相続・・・・・・・・・ 123
デジタルイミグラント・・・・・ 142,153
デジタルタトゥー・・・・・・・・・ 109
デジタルネイティブ・・・・・141,142,153
手配書方式・・・・・・・・・・・・・ 24
ドライブバイダウンロード攻撃・・ 29,153
トラッシング・・・・・・・・・・ 36,153
トロイの木馬・・・・・・・・・・・・ 16

な行

なりすまし・・・ 19,66,68,80,112,115,121
入力遅延・・・・・・・・・・・ 53,54,55
認証局・・・・・・・・・ 73,74,75,79,153
ネームドロップ・・・・・・・・20,36,153
ネチズン・・・・・・・・・・・ 140,154
ネットいじめ・・・・・・・・・・ 19,109
ネットワーク暗証番号・・・・・・ 52,154
ネットワークカメラ・・・・・・17,26,154
ネットワークキー・・・・・・・・ 52,154
ネットワークルータ・・・・・・・ 17,154

は行

バージョンアップ・・・・・・・・ 22,154
バーチャル空間・・・・・・・・ 143,154
バーチャルリアリティ・・・・・ 143,154
ハードウェアトークン・・・・・22,32,154
パスコード・・・・・・・・・・・ 52,154
パスワードリスト攻撃・・・・・55,63,154
パターンロック・・・・・・・・・36,92,154
ハッカー・・・・・・・・・・・・・ 15,39
バックアップディスク・・・・・ 100,154
バックドア・・・・・・・・・・・ 97,154
パッチ・・・・・・・・・・・・・ 104,155
ハリーアップ・・・・・・・・・・20,36,155
秘密の質問・・・・・・・・・・・ 32,155
ヒューミント・・・・・・・・・・ 50,155
ヒューリスティック分析・・・・・ 24,155
標的型メール・・ 17,20,23,29,35,36,37,155
ファームウェア・・・・22,25,26,67,68,155
ファームウェアパスワード・・・・ 98,155
ファイアーウォール・・・・・・23,34,155
フィッシング詐欺・・・・・・・・・・・
18,38,42,56,63,76,136
フィッシングメール・・・・・・37,97,155
復号・・・・・・ 52,55,61,65,66,79,85,155

不正アクセス通知・・・・・・・23,34,155
踏み台・・・・・・・・・・・ 42,44,45,155
フライトモード・・・・・・・・・ 133,156
ブルートフォース攻撃・・・・・・ 52,55
ポート・・・・・・・・・・・・・72,78,156
ボット・・・・・・・・・・・ 16,42,44,156
ボットネット・・・ 17,18,25,42,44,45,156
ホワイトハットハッカー・・・・・・・ 15

ま行

マネタイズ・・・・・・・・・・・ 88,156
マルバタイジング・・・・・・・・ 77,156
水飲み場攻撃・・・・・・・・・・ 77,156
無線LAN・・・・・・・・ 17,26,44,54,55,
64-76,78,88,103,128,157
無線WAN通信機能 ・・・・・・ 102,157

ら行

ランサムウェア・・・16,18,46,100,120,157
リカバリメディア・・・・・・・・ 98,157
リスト型攻撃・・・・・30,33,53,55,90,157
リベンジポルノ・・・・・・・・・ 19,109
リモートワイプ・・・・ 84,95,99,102,157
ルータ・・・・・・・・・・・・・・・・・
17,26,28,53,55,64,66,67,68,103,157
ローミング・・・・・ 127,129,130,131,157
ログ・・・・・・・・・・・・・・・・・ 34
ログアウト・・・・・・・・・・・・ 97,157
ロック画面・・・・・・・・・・・・ 93,157

内閣サイバーセキュリティセンター (NISC)ホームページ：https://www.nisc.go.jp/
NISC「みんなでしっかりサイバーセキュリティ」：https://www.nisc.go.jp/security-site/index.html
内閣サイバーセキュリティセンター 公式Twitter: @cas_nisc
内閣サイバー（注意・警戒情報）Twitter:@nisc_forecast
内閣サイバーセキュリティセンター NISC LINE公式アカウント：@nisc-forecast
NISC facebookページ: https://www.facebook.com/nisc.jp

インターネットの安全(あんぜん)・安心(あんしん)ハンドブック

2019年1月18日　Ver 4.00発行

NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

制作・著作　内閣(ないかく)サイバーセキュリティセンター
イラスト　ＫＯＴＡ

平成30年７月31日

専門分科会開催報告

鳥取県サイバーセキュリティ対策ネットワーク事務局

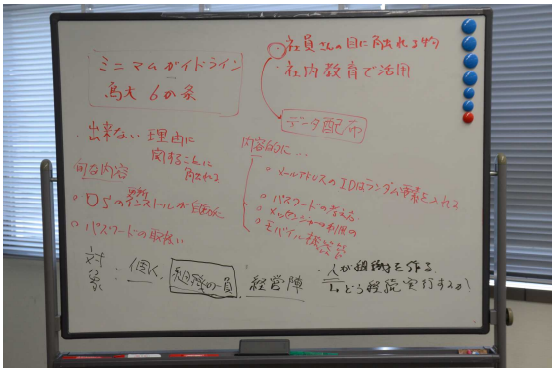
平 成 ３０ 年 度　対 処 能 力 向 上 分 科 会 （ 第 １ 回 目 ）

開催日：平成30年７月27日（金）午後１時30分から午後３時１５分
場　所：鳥取県警察本部３階 第４会議室

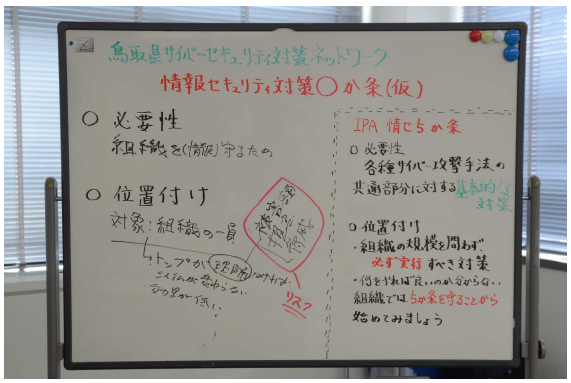
鳥取県サイバーセキュリティ対策ネットワークの専門分科会の内、企業や組織におけるサイバー攻撃などへの対処能力の向上を目指す「対処能力向上分科会」を開催しました。

今年からは、分科会に各会員の関係団体・企業からの推薦員も出席できることとなり、今回は、鳥取県情報産業協会様と鳥取県商工会議所連合会様から推薦された３名の民間企業の方にも出席していただきました。

また、**経営層の方々に情報セキュリティ事故に遭った際のリスクをお伝えする情報の掲載も必要**という意見もあがり、内容に盛り込む方針も決定しました。



今年の対処能力向上分科会では、
「**情報セキュリティ対策簡易ガイドライン**」
の作成を行っています。



新たな対策ツールの完成イメージは、情報セキュリティ対策上、最低限すべき行動や守るべき事項を箇条書きで記載されたポスター形式のものです。

情報セキュリティポリシーが策定されていない組織でも、大切な情報資産を守るための行動がとれるよう、一人ひとりが基本的なことから行動できるよう支援するツールとなります。

【 当ネットワークの制作物が「情報セキュリティ白書2018」に掲載されました！ 】

対処能力向上分科会が制作した「企業と組織のネットトラブル対応マニュアル」が、独立行政法人情報処理推進機構(IPA)刊行の「情報セキュリティ白書２０１８」193ページに「中小企業のための対策支援ツール」として掲載されました。

このマニュアルは、ネットトラブルが発生したとき、まず何をすればよいのかをマンガタッチで解説したものです。

マニュアルのデータは、当ネットワークのホームページで公開していますので、社内教育等でご活用ください。

http://www.pref.tottori.lg.jp/secure/1096988/cybermanual.pdf

事務局：鳥取県警察本部サイバー犯罪対策課

平成30年８月６日

専門分科会開催報告

鳥取県サイバーセキュリティ対策ネットワーク事務局

平 成 ３０ 年 度　啓 発 教 育 分 科 会 （ 第 １ 回 目 ）

開催日：平成30年８月３日（金）午後１時30分から午後３時１５分
場　所：鳥取県警察本部４階 第５会議室

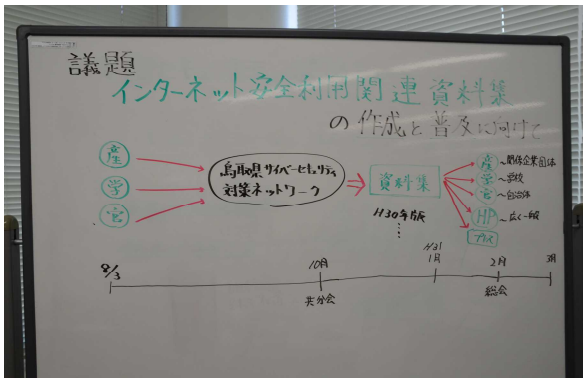
鳥取県サイバーセキュリティ対策ネットワークの専門分科会の内、県民の皆様にインターネットの安全利用を呼び掛ける「啓発教育分科会」を開催しました。

今年の啓発教育分科会では、「**インターネット安全利用関連資料集**」の作成を行っています。

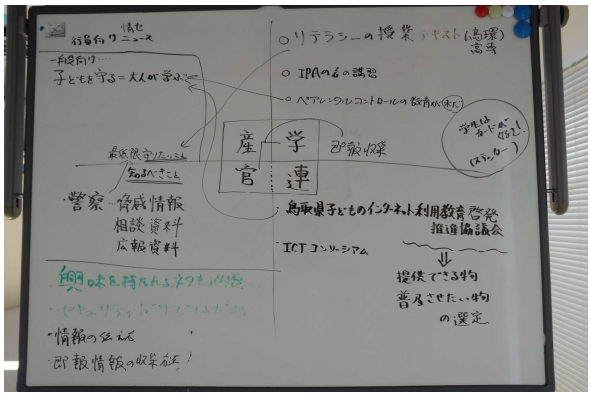
インターネットの安全利用に関する教育や資料の作成は、県内の行政機関、学校、経済団体等でそれぞれ行われています。

資料集の作成は、県内で作成された資料等を収集し、クローズアップしてさらに普及させることで、県民の皆様にとって、有用な教養ツールとなることを目指した取組となります。

警察が発信している、脅威・被害情報や大学・高専でのインターネットリテラシー講義資料、経済団体の会報掲載コラムのほか、教育委員会関係協議会の作成資料などを集約し、年ごとに資料集化する方針が決定しました。



子ども向けから大人向けまで、各方面の優秀な資料を一度に参照できる資料集として、新年度の学校授業や社内教育で活用していただくことを想定しています。



また、「インターネット上の脅威情報は、リアルタイムに共有して警戒を呼び掛ける仕組みが必要」という意見がありました。

今後、会員の皆様が、サイバー攻撃を受けた場合や関連情報を得た場合に事務局へ即報し、会員間で速やかに情報共有できる仕組みをつくります。

【～対処能力向上分科会担当会員の皆様へ～】

資料集の収集に関して、共有できる資料や関連情報などお持ちの場合は、事務局まで情報をお寄せください。

事務局：鳥取県警察本部サイバー犯罪対策課

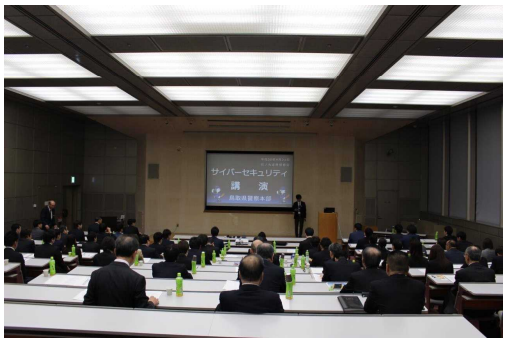
平成30年４月24日

サイバーセキュリティ講演開催報告

鳥取県警察本部サイバー犯罪対策課

大山日ノ丸証券株式会社主催オープン講習会

開催日：平成30年４月21日（土）午後０時50分から午後２時２０分（９０分）
場　所：とりぎん文化会館第１会議室
講　師：鳥取県警察本部サイバー犯罪対策課　警部補　福井　貴



鳥取法人会、鳥取県経済同友会、鳥取商工会議所の会員である大山日ノ丸証券株式会社様からの講演依頼を受け、一般参加可能なオープン講習会におけるサイバーセキュリティ講演を行いました。

講演内容は、

『 サイバーセキュリティ対策　～ネット詐欺の手口 すべて見せます！～ 』

と題し、**ビジネスメール詐欺、フィッシング詐欺、ワンクリック詐欺、サポート詐欺**などの被害防止対策について、具体的な被害事例をアニメーションや動画などを織り交ぜてわかりやすく講演しました。

講習会に参加された皆様は、最新の詐欺手口や新しいインターネット犯罪へのセキュリティ対応策などについて真剣に勉強していただきました。

講演終了後の質疑応答では、振り込んでしまった現金を取り戻す方法や詐欺被害にあいやすい年齢層などについて質問も飛び交うなど、たいへん充実した９０分間となりました。

社員の皆様や鳥取財務事務所職員様など
合計　７８名
の皆様にご聴講していただきました！

ほんとうにありがとうございました。

ご意見・ご要望などございましたら、お気軽にご連絡をお願いします。
鳥取県警察本部サイバー犯罪対策課　TEL 0857-23-0110（内線3424）

平成30年５月15日

サイバーセキュリティ講演開催報告

鳥取県警察本部サイバー犯罪対策課

米子高専においてサイバーセキュリティ講義！！

開催日：平成30年５月10日（木）午後２時30分から午後３時20分（50分）
場　所：米子工業高等専門学校　合同講義室
講　師：鳥取県警察本部サイバー犯罪対策課　警部補　福井　貴

米子工業高等専門学校第３学年の生徒さん（191名）を対象としたサイバーセキュリティ講義を実施しました。今回の講義は、生徒の皆さんが普段、実際に使用しているスマートフォンを使った

ミニハッキングコンテスト

に挑戦してもらった後、ネット犯罪に巻き込まれないための心構えやセキュリティの重要性について学んでいただく、参加・体験・実践型の講義でした。

コンテストは、実際に起こった不正アクセス禁止法違反の事件事例に基づき、アカウントの乗っ取りに挑戦していただくものです。

犯罪者の悪質な犯行手口や**様々なサービスの裏側に潜むセキュリティの脆弱性**を目の当たりにしてもらうことで、そのリスクを肌で感じていただきました。

全国的にもサイバー犯罪に関与した者の低年齢化が問題となっています。
生徒の皆さんにとって、

『犯罪被害にあわない』

そして、

『犯罪者にならない』

ためのリテラシーを身につける貴重な講義となったのではないでしょうか。

鳥取県警察サイバーセキュリティ対策アドバイザーである

米子高専情報教育センター長　松本正己 教授

をはじめ、教職員の皆さまにも、ご協力をいただきました。
本当にありがとうございました！

ご意見・ご要望などございましたら、お気軽にご連絡をお願いします。
鳥取県警察本部サイバー犯罪対策課　TEL 0857-23-0110（内線3424）

平成30年５月23日

サイバーセキュリティ講演開催報告

鳥取県警察本部サイバー犯罪対策課

平成30年度鳥取県・鳥取地区金融機関防犯協議会合同定期総会

開催日：平成30年５月21日（月）午後２時30分から午後３時００分（３０分）
場　所：鳥取銀行本店ビル３階大会議室
講　師：鳥取県警察本部サイバー犯罪対策課管理官 保木本順一、同課長補佐 伊田廣徳

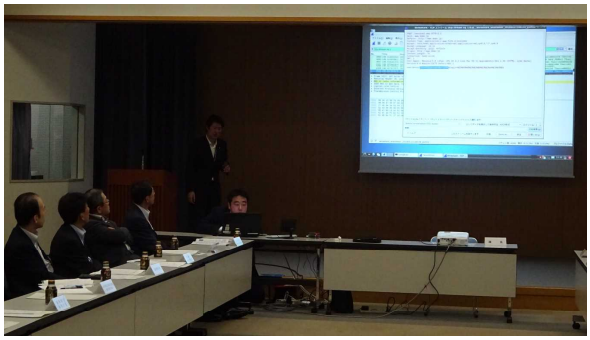
定期総会にご出席の方（24名）を対象としサイバーセキュリティ講演を実施しました。

今回の講演は、「**公衆無線LANの危険性**」をテーマとして、情報漏洩のデモンストレーションを交えながら、危険なWi-Fiアクセスポイントの説明や不正送金の犯行手口の紹介を行いました。

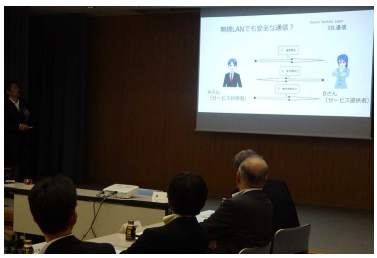
保木本管理官からは、今年度鳥取県警察に新設されたサイバー犯罪対策課の紹介と不正送金被害の発生状況などのサイバー犯罪情勢についての説明をしました。

その後、伊田課長補佐がデモンストレーションと講演を行いました。

デモンストレーションでは、「セキュリティ設定のないWi-Fiアクセスポイント」にスマートフォンで接続し、ウェブサイトのログイン画面で入力したパスワードが第三者に盗み見られる状況を再現しました。



パスワード入力が不要だからと安易にセキュリティ設定の施されていないWi-Fiアクセスポイントを利用すると通信内容が第三者に筒抜けとなる・・・ということを目の当たりにしていただけたことと思います。



また、オラインバンキングなどのサービス提供者側が設定した暗号化通信設定やワンタイムパスワードなどのセキュリティ対策までも無力化してしまう不正送金の犯行手口「中間者攻撃」の仕組みや発生原因について解説を行いました。

公衆無線LANの整備が全国的に進む中、利便性が増す一方で、**正しい使い方を覚え、自らの身を守る**必要があることを感じていただけたことと思います。

ご意見・ご要望などございましたら、お気軽にご連絡をお願いします。
鳥取県警察本部サイバー犯罪対策課　TEL 0857-23-0110（内線3423）

平成30年５月24日

サイバーセキュリティ講演開催報告

鳥取県警察本部サイバー犯罪対策課

鳥取大学の平成30年度全学共通科目において、「インターネットと犯罪」の講義

開催日：平成30年５月21日（月）午後１時から午後２時30分（90分）
場　所：鳥取大学共通教育棟D棟２階D21講義室
講　師：鳥取県警察本部サイバー犯罪対策課長　青木 篤郎、同課係長　福井　貴

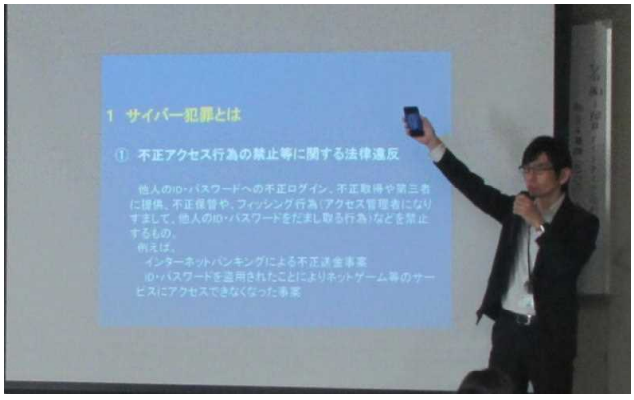
【サイバー犯罪対策課長 青木篤郎】

鳥取大学において「インターネットと犯罪」と題する社会安全政策論の講義を鳥取県警察本部サイバー犯罪対策課長青木篤郎と同課係長福井貴により実施しました。

当日は、39名の大学生と担当教員が聴講しました。

青木課長が、前半、サイバー空間の脅威の現状と対策について、平昌オリンピック公式ホームページに対するサイバー攻撃、ネットバンキング不正送金事案をはじめとするサイバー犯罪など最近の実例に基いて講義しました。

【サイバー犯罪対策課長 青木篤郎】



【サイバー犯罪対策課　サイバー犯罪対策係長　福井　貴】

後半は、福井係長が、サイバー犯罪の検挙状況、相談事例、県警察の取組み事例などを説明したのち、学生と共に実際にスマートフォンを使ったセキュリティ対策を実演しました。

未来を担う若い大学生にとって、サイバーセキュリティ対策がいかに重要であるかを理解していただけたことと思います。

ご意見・ご要望などございましたら、お気軽にご連絡をお願いします。
鳥取県警察本部サイバー犯罪対策課　TEL 0857-23-0110（内線3424）

平成30年６月15日

サイバーセキュリティ講演開催報告

鳥取県警察本部サイバー犯罪対策課

鳥取実業倶楽部勉強会におけるサイバーセキュリティ講演

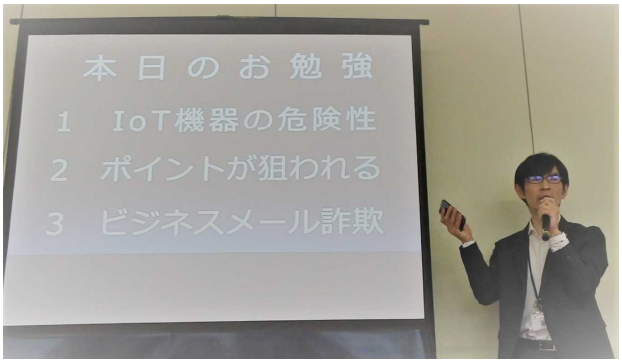
開催日：平成30年６月１２日（火）午前１１時１０分から午後０時１０分（６０分）
場　所：鳥取商工会議所ビル５階大会議室
講　師：鳥取県警察本部サイバー犯罪対策課　警部補　福井　貴

鳥取実業倶楽部様主催の６月勉強会におけるサイバーセキュリティ講演を行いました。

講演内容は、最近、話題のスマートスピーカー、お掃除ロボット、遠隔操作可能な防犯カメラ等のIoT機器のセキュリティ対策、便利なスマホポイントアプリを逆手にとった新手のサイバー犯罪事例とその対策、日本航空（JAL）が巨額の被害を受けたビジネスメール詐欺（BEC）の犯行手口とその対策の３項目についてで、

『サイバーセキュリティ対策～今、IoT機器が、ポイントが、メールが、危ない！～』

と題して講演しました。



勉強会に参加された会員の皆様には、今後、普及していくと思われるIoT機器を取り扱う際にやっておかなければならないセキュリティ対策や企業に対して犯罪者から送信されるメール偽装工作の最新手口やその見破り方などについて、真剣に勉強していただきました。

サイバーセキュリティ分野については、今後、ますます危険性が高まっていくことが予想され、鳥取県においても、産学官が協力してセキュリティ対策を推進していかなければならないことについて、皆様と再度、確認をいたしました。

勉強会に出席された
合計　２３名
の会員の皆様にご聴講していただきました。

本当にありがとうございました。

ご意見・ご要望などございましたら、お気軽にご連絡をお願いします。
鳥取県警察本部サイバー犯罪対策課　TEL 0857-23-0110（内線3424）

平成30年６月29日

サイバーセキュリティ講演開催報告

鳥取県警察本部サイバー犯罪対策課

(公社)倉吉法人会女性部会総会における講演会

開催日：平成30年６月28日（木）午前10時00分から午前11時00分（60分）
場　所：倉吉シティホテル２階
講　師：鳥取県警察本部サイバー犯罪対策課　警部補　福井　貴

公益社団法人倉吉法人会女性部会様からの講演依頼を受けて、サイバーセキュリティ講演会を行いました。

講演内容は、

『サイバーセキュリティ対策』

と題し、スマートフォンから情報流出させないためのセキュリティ対策を中心とした内容でした。

県内におけるスマートフォンを使用した犯罪被害事例等を紹介し、被害防止対策として、講演会に参加された皆様と一緒に実際のスマートフォンを使ったセキュリティ設定について確認を行いました。

また、セキュリティ対策の基本となる**端末ロック設定**や**IDとパスワードの管理**などについても実演しながら説明を行いました。

そのほかにも最新の詐欺手口やサイバー犯罪へのセキュリティ対策について、皆様に真剣に勉強していただきました。

質疑では、強固なパスワードを作る方法やその管理方法についての質問が飛び交うなど充実した60分間となりました。

サイバーセキュリティ講演会には
合計　38名
の皆様にご参加いただきました。

ご清聴いただき、本当にありがとうございました。

ご意見・ご要望などございましたら、お気軽にご連絡をお願いします。
鳥取県警察本部サイバー犯罪対策課　TEL 0857-23-0110（内線3424）

平成30年７月13日

サイバーセキュリティ講演開催報告

鳥取県警察本部サイバー犯罪対策課

米子地区金融機関新入行（職）員等防犯研修会

開催日：平成30年７月11日（水）午後４時１０分から午後４時40分（30分）
場　所：米子警察署３階会議室
講　師：鳥取県警察本部サイバー犯罪対策課　警部補　福井　貴

鳥取県金融機関防犯協議会様からの講師派遣依頼を受けて、サイバーセキュリティ研修を行いました。

研修内容は、

『サイバーセキュリティ対策について』

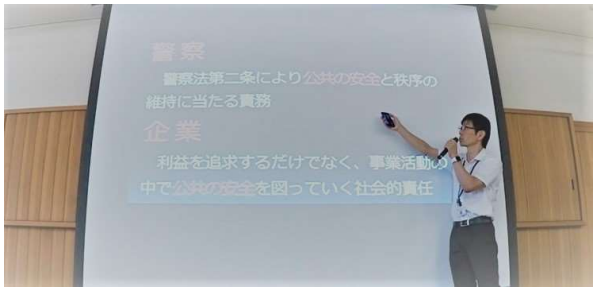
と題し、

スマートフォンのセキュリティ設定

などについて研修しました。

県内におけるスマートフォンを使用した犯罪事例等を紹介しながら、被害を防止するためのセキュリティ対策について、参加していただきました米子地区金融機関職員の皆様方のスマートフォンを実際に使いながら一緒に確認を行いました。

「OS、アプリのアップデート」「セキュリティ（パスコード）ロックの設定」「IDとパスワードの管理」「セキュリティ対策アプリの導入」「公式マーケットからのアプリインストール」の５つのセキュリティ対策の基本を徹底していくことで被害の未然防止を図ることができることを認識していただきました。



また、指紋認証や虹彩認証などの生体認証、強固なパスワードの作成方法についても実演しながら説明するなど高度なセキュリティ対策についても学んでいただきました。

研修会には

合計　49名

の皆様にご参加いただきました。

ありがとうございました。

ご意見・ご要望などございましたら、お気軽にご連絡をお願いします。
鳥取県警察本部サイバー犯罪対策課　TEL 0857-23-0110（内線3424）

平成30年10月19日

サイバーセキュリティ講演開催報告

鳥取県警察本部サイバー犯罪対策課

二十日会ミニセミナーにおけるサイバーセキュリティ講演

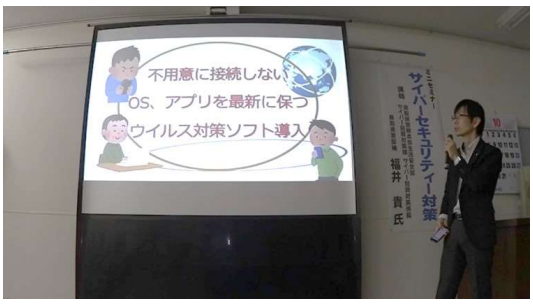
開催日：平成30年10月17日（水）午後０時20分から午後０時50分（30分）
場　所：鳥取卸センター会館２階会議室
講　師：鳥取県警察本部サイバー犯罪対策課　警部補　福井　貴

協同組合鳥取卸センター様主催の二十日会・組合員全体会議において、サイバーセキュリティ講演を行いました。

講演内容は、無線LANのなりすましアクセスポイントによる盗み見事案やセキュリティの甘さを狙った踏み台によるサイバー犯罪事例などを紹介し、正しい無線LANの設定について講義したほか、スマートスピーカー、お掃除ロボット、コネクテッドカーなど通信機能を備えたIoT機器のセキュリティ対策、また、日本航空（JAL）が巨額の被害を受けたビジネスメール詐欺（BEC）の犯行手口とその対策などについて、

『サイバーセキュリティ対策　～サイバー犯罪の被害にあわないために～』

と題して講演しました。



セミナーに参加された会員の皆様には、無線LANルーターやIoT機器を購入した際にやっておかなければならないセキュリティ対策や特定の企業を標的として犯罪者から送信されるメール偽装工作や最新手口とその対処方策などについて、真剣に勉強していただきました。

ビジネスにおけるIT導入がますます加速化していく中で、企業の経営者として、サイバーセキュリティ対策にどのように取り組んでいくべきか、参加された会員の皆様とあらためて確認をいたしました。

会員、同関係者の方
合計　２３名
の皆様にご聴講していただきました。

ご意見・ご要望などございましたら、お気軽にご連絡をお願いします。
鳥取県警察本部サイバー犯罪対策課　TEL 0857-23-0110（内線3424）

平成30年11月21日

サイバーセキュリティ講演開催報告

鳥取県警察本部サイバー犯罪対策課

米子市小・中学校人権教育研修講座におけるサイバーセキュリティ講演

開催日：平成30年11月15日（木）午後３時３０分から午後４時50分（８０分）
場　所：米子市立図書館２階多目的研修室
講　師：鳥取県警察本部サイバー犯罪対策課　警部補　福井　貴

平成30年度米子市小・中学校人権教育研修講座において、サイバーセキュリティ講演を行いました。

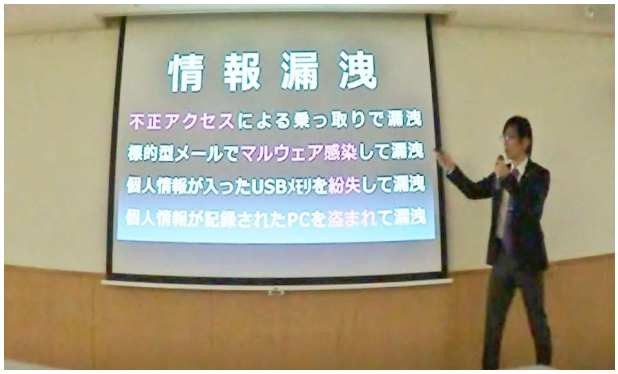
講演内容は、

『サイバーセキュリティ対策　～個人情報漏えい防止対策～』

と題して、パソコンやスマートフォンなどの情報通信機器を利用した個人情報漏えい防止対策について講演しました。

参加された教職員の皆様に対し、パソコンやUSBメモリ等を使用して個人情報などの大切なデータを取扱う際、注意しなければならないポイントについて、実際に発生した全国の様々な情報流出事件を題材として、デモンストレーションを交えながら現状と対策を学んでいただきました。

スマートフォンやSNSの利用が低年齢層にまで普及し、子供たちの情報モラル教育のあり方や必要性が問われるなか、まずは、大人たちがその現状をしっかりと把握し、教育現場だけでなく、地域、関係機関・団体が一体となった効果的な対策を推進していくことの大切さについて、真剣に勉強していただきました。



近年、ICT（情報通信技術）を活用した教育がますます加速していく中で、小・中学校教職員として、今後、サイバーセキュリティ対策にどのように取り組んでいくべきか、研修講座に参加された皆様とあらためて確認をいたしました。

教職員の皆様、教育関係者の方
合計　30名
にご聴講していただきました。

ご意見・ご要望などございましたら、お気軽にご連絡をお願いします。
鳥取県警察本部サイバー犯罪対策課　TEL 0857-23-0110（内線3424）

平成31年２月８日

サイバーセキュリティ講演開催報告

鳥取県警察本部サイバー犯罪対策課

とっとり消費者大学「くらしの経済・法律講座」

開催日：平成31年１月28日（月）午後１時から午後２時30分（90分）
場　所：公立鳥取環境大学本部・講義棟１階　１１講義室
講　師：鳥取県警察本部サイバー犯罪対策課　警部補　福井　貴

平成30年度とっとり消費者大学「くらしの経済・法律講座」における講師派遣依頼を受け、公立鳥取環境大学において、サイバーセキュリティ講座を実施しました。

講座の内容は、

『サイバーセキュリティ対策』～サイバー犯罪に巻き込まれないために～

と題し、治安に関する世論調査結果やサイバー犯罪に関する情勢を踏まえて、サイバー犯罪被害の防止対策などについて講演しました。

内閣府が平成29年９月に行った世論調査において、国民が不安を感じる犯罪として、インターネットを利用した犯罪が、詐欺、窃盗、傷害などの現実空間における犯罪を初めて上回り、サイバー空間における警察活動への要望が年々、増加していることを説明した後、インターネットを利用した最新の犯罪手口などを紹介し、サイバー犯罪に巻き込まれないための対策について説明しました。

本講座は、鳥取県生活環境部くらしの安心局消費生活センターと公立鳥取環境大学が連携し、県民と大学生が一緒に、消費生活に関する様々な分野の高度な知識を習得できるものとなっており、毎年開催されています。

本講座には、
大学生　113名、一般受講者　45名
（合計　158名）
の皆様にご参加いただきました。
ご清聴いただき、ありがとうございました。

ご意見・ご要望などございましたら、お気軽にご連絡をお願いします。
鳥取県警察本部サイバー犯罪対策課　TEL 0857-23-0110（内線3424）

平成31年２月６日

サイバーセキュリティ講演開催報告

鳥取県警察本部サイバー犯罪対策課

米子松蔭高等学校におけるサイバーセキュリティ講話

開催日：平成31年２月４日（月）午前９時55分から午前10時40分（45分）
場　所：学校法人米子永島学園米子松蔭高等学校　第一体育館
講　師：鳥取県警察本部サイバー犯罪対策課　警部補　福井　貴

学校法人米子永島学園米子松蔭高等学校卒業前の第３学年の生徒さんを対象としたサイバーセキュリティ講話を実施しました。

講話の内容は、

スマートフォンのセキュリティ対策、SNSによるストーカー対策

と題し、生徒さんが実際に使用しているスマートフォンを使って、セキュリティ設定の確認を一緒にしながら実演するとともに、インターネット掲示板やSNS等を利用して青少年が犯罪被害に巻き込まれた事例などを紹介して、被害者にも加害者にもならないための対策について講演しました。

２月１日から３月18日までのサイバーセキュリティ月間の期間中であり、春の卒業、進学、就職シーズンに向け、スマートフォンやSNSの安全安心な利用のためのリテラシー向上に重点をおいたタイムリーな講話となり、生徒の皆さん、そして、教職員の方々も含めた実効性のある講演となりました。

サイバーセキュリティ講話には、

生徒　192名、教職員　10名　（合計　202名）

の皆様にご参加いただきました。

ご清聴いただき、ありがとうございました。

ご意見・ご要望などございましたら、お気軽にご連絡をお願いします。
鳥取県警察本部サイバー犯罪対策課　TEL 0857-23-0110（内線3424）

平成30年４月16日

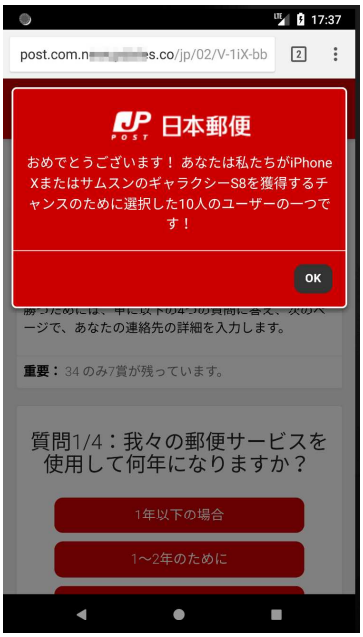
サイバーセキュリティ関連情報（４月号）

鳥取県警察本部サイバー犯罪対策課

○　不正広告で誘導する日本郵便を偽装した当選詐欺サイトを確認

トレンドマイクロは、4月2日前後から日本郵便を偽装する不審サイトを確認したと報じた。この不審サイトは、いわゆる「当選詐欺」サイトであり、最新スマートフォンの当選を理由に最終的に個人情報からクレジットカード情報までを入力させ、詐取することが目的と考えられ、調査の結果、この当選詐欺サイトへの主な誘導経路は不正広告であることも確認したと伝えている。

犯罪者はインターネット利用者の金銭や個人情報を狙い、次々と新しい手口を繰り出しています。これに対し、利用者は今回のようなネット詐欺の最新手口を知り、だまされないようにすることが重要です。



図：今回確認された当選詐欺サイトの表示例（Android からアクセス）
正規サイトと誤解させるよう「post」という単語を入れたり、「.co.jp」と誤解させるよう「.co/jp」という文字列を URL に入れている

出典元URL　http://blog.trendmicro.co.jp/archives/17205

○　不正プログラム感染を確認するためのウェブサイトを公開

JC3（日本サイバー犯罪対策センター）では、不正送金やクレジットカードの不正使用等の犯罪被害につながるインターネットバンキングマルウェアによる感染拡大及びこれによる被害の防止のため、DreamBot又はGozi又はRamnitへの感染状況を確認するためのウェブサイトをホームページ上で公開し、試験運用している。

インターネット利用者は、不正プログラムに感染していないかどうか本チェックサイトで確認するなどにより、犯罪被害の防止を図ってください。

出典元URL　https://www.jc3.or.jp/info/dgcheck.html

平成30年５月11日

サイバーセキュリティ関連情報（５月号）

鳥取県警察本部サイバー犯罪対策課

○ Twitter、パスワードの変更を呼び掛け

Twitterは、2018年5月4日、全ユーザーに向けてパスワードの変更を呼び掛けた。パスワードの設定処理においてバグが存在し、内部ログにパスワードが平文のまま保存されていたが外部漏洩や不正利用の痕跡はないとしている。

今回の問題を受け、内閣サイバーセキュリティセンター（NISC）は、業務で情報発信などにTwitterを使用している府省庁に対し、パスワードを変更するとともに、所管する独立行政法人などの法人や、重要インフラ事業者をはじめ、業界団体などを通じて所管する業界の事業者へ周知を図るよう注意喚起を行った。

Twitterを利用している企業、団体については、パスワードの変更を検討し、2要素認証の活用をお願いします。

【アプリ起動時の告知画面】

Twitter公式ブログの記事
https://blog.twitter.com/official/ja_jp/topics/company/2018/account_secure.html

○ Apple をかたるフィッシングメールが出回る

フィッシング対策協議会によると、2018年5月7日現在、Appleをかたるフィッシングサイトが稼働しているとのことで注意を呼び掛けている。

同協議会は、一般社団法人JPCERTコーディネーションセンターにサイト閉鎖のための調査を依頼中であり、このようなフィッシングサイトでAppleID、パスワード、姓、名、生年月日、郵便番号、都道府県、市区町村、その他住所、電話番号、クレジットカード番号、カードの名義人、有効期限、セキュリティコード、セキュリティ質問、答え等を絶対に入力しないよう注意喚起している。

【フィッシングサイトの表示画面】⇒

出典元URL　フィッシング対策協議会
https://www.antiphishing.jp/news/alert/apple_20180507.html

平成30年６月６日

サイバーセキュリティ関連情報（６月号）

鳥取県警察本部サイバー犯罪対策課

○ フィッシング報告数高水準 -「Apple」関連が約65%

フィッシング対策協議会は、5月中に2701件のフィッシングの報告があり、４月と比較して、804件増加したと発表した。

特に「Apple」をかたるフィッシングが多く、全体の約65%を占めているという。

また、「LINE」や仮想通貨関連サービスを装うフィッシングも報告されている。

同協議会によると、報告件数が2000件を超えたのは、2016年2月以来、27か月ぶりであり、不正メール送信の踏み台やなりすまし、情報漏洩などの被害につながるおそれもあるとして注意を呼び掛けている。

出典元URL　フィッシング対策協議会
http://www.antiphishing.jp/report/monthly/201805.html

○ 森永乳業の通販サイト、最大９万人超の個人情報流出

森永乳業の「健康食品通販サイト」においてクレジットカード情報（以下、カード情報）が流出した可能性がある問題で、同社は調査の結果、カード情報及びカード情報以外の個人情報が流出したと思われる顧客は最大2万9773人、カード情報以外の個人情報のみが流出したと思われる顧客は最大6万3049人とみられることを発表した。

同サイトでは、2017年10月16日にサーバを入れ替えたが、旧サーバに脆弱性が存在し、不正アクセスを受けて顧客情報が流出した可能性があるという。

<table>
<tr><td></td><td colspan="2">2012/1/22　～　2015/1/7　～　2017/10/16
当該サイト開設　旧サーバー閉鎖</td></tr>
<tr><td rowspan="2">当該サイトを利用されたお客さま
（1）+（2）
最大 92,822 名</td><td rowspan="2">（2）最大 63,049 名</td><td>カード利用されたお客さま
（1）　最大 29,773 名</td></tr>
<tr><td></td></tr>
</table>

現在、同サイトについては、不正アクセス攻撃への耐性や脆弱性に問題がないことが確認されているとしているが、クレジットカード決済について、さらなるセキュリティ強化策を行った上で再開する予定としている。

出典元URL　森永乳業
http://www.morinagamilk.co.jp/information2/newsentry-2900.html

平成30年７月10日

サイバーセキュリティ関連情報（７月号）

鳥取県警察本部サイバー犯罪対策課

○ 京都府などの5自治体のウェブサイトで約7500人分情報漏えいの可能性

鳥取県は6月26日、県が民間企業に委託し開設しているウェブサイト「環境家計簿『我が家のエコ録』」がサイバー攻撃を受け、利用者４３６人の氏名やメールアドレスなどが漏えいした可能性があると発表した。

６月25日に都内のITセキュリティー会社から通報があり、委託先の京都市のシステム会社に確認したところ、外部からデータベースを不正操作する「SQLインジェクション」という手法で、同社が管理運営するサーバーが攻撃されていたことを確認した。

また、同社が管理する京都府、埼玉県、滋賀県、東京都小平市のウェブサイトでも同様に攻撃を受けており、約7500人の個人情報が漏洩した可能性があるとしている。

IPAがウェブサイト開発者や運営者が適切なセキュリティを考慮したウェブサイトを作成するための資料「安全なウェブサイトの作り方」を公開しているので参考として下さい。

参考　IPA（独立行政法人情報処理推進機構）ホームページ

https://www.ipa.go.jp/security/vuln/websecurity.html

○ パスワード管理「定期的な変更は不要」と総務省が発表

これまでパスワードの定期的な変更を呼びかけてきた総務省は昨年秋、「定期的な変更は不要」と従来の見解を改めた。

その理由として、定期的な変更をすることでパスワードの作り方がパターン化し簡単なものになるとしており、定期的に変更するよりも、機器やサービスの間で使いまわしのない、固有のパスワードを設定することが求められるとしている。

総務省は、ホームページ上で、パスワードの設定と管理のあり方について、

① 安全なパスワードの設定

② パスワードの保管方法

③ パスワードを複数のサービスで使い回さない（定期的な変更は不要）

の３つの要素を掲げ、アカウントを不正に利用されないための注意喚起を行っている。

パスワードは、名前、生年月日、電話番号など他人から類推されやすいものを避け、他人の目に触れるような場所に貼ったりしないことなどの基本事項を徹底して下さい。

参考　総務省ホームページ

http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/privacy/01-2.html

平成30年８月８日

サイバーセキュリティ関連情報（８月号）

鳥取県警察本部サイバー犯罪対策課

○ 佐川急便を騙る迷惑SMSメールに要注意

佐川急便を騙る迷惑メールについての相談が急増しています。佐川急便では、携帯電話番号を使用したショートメール（SMS）による案内は行っておらず、このようなメールを受信した際には、メール内のリンクを開くことがないようお気をつけ下さい。

リンクをクリックすると、佐川急便の公式サイトにそっくりな偽サイトに誘導され、「貨物追跡」というボタンを押させることで不正なアプリがインストールされるというものです。

もし、リンクを開いてインストールしてしまった場合は、速やかにお使いのキャリアの会社に相談していただき、端末の初期化についてご検討していただきますようお願いします。

参考　http://www2.sagawa-exp.co.jp/whatsnew/detail/721/

○ 仮想通貨を採掘するツール（マイニングツール）に関する注意喚起

警察では、サイバーパトロールの実施等により、閲覧者に気付かれないように仮想通貨を採掘するツール（マイニングツール）が設置されているウェブサイトを確認しております。マイニングツールは、パソコンの処理能力を活用し、仮想通貨を得るためのツールです。マイニングツールを自身のウェブサイトに設置することを検討しているウェブサイトの運営者やインターネット利用者は、以下の点に注意してください。

- **ウェブサイトの管理者**

  マイニングツールを設置していることを閲覧者に明示せずに同ツールを設置した場合、犯罪になる可能性があります。

- **インターネット利用者**

  マイニングツールが設置されたウェブサイトにアクセスするとパソコンの処理能力が意図せずに使用され、パソコンの動作が遅くなるなどの事象が生じる可能性があります。そのような場合、ブラウザを閉じ、同サイトへのアクセスを控えてください。

  なお、ウイルス対策ソフトによっては、この種サイトにアクセスすると、警告画面が表示されるものもあります。

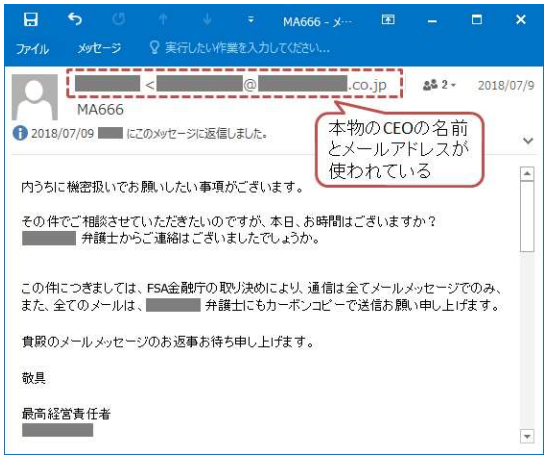
参考　警察庁サイバー犯罪対策プロジェクト
http://www.npa.go.jp/cyber/policy/180614_2.html

平成30年９月11日

サイバーセキュリティ関連情報（９月号）

鳥取県警察本部サイバー犯罪対策課

○ 社長を装う日本語のビジネスメール詐欺を初確認！



日本語で記載された「ビジネスメール詐欺（BEC）」が国内で確認されたとして、情報処理推進機構（IPA）は、類似した手口に注意するよう呼びかけている。

今回確認されたメールは、最高経営責任者（CEO）などとして実際の会社社長の氏名を使用し、差出人の表示において、社長の氏名とメールアドレスを詐称していたほか、「機密扱いでお願いする」「金融庁との取り決めでやり取りはすべてメールで行う」などと受信者に他言させないよう持ちかけていた。

同機構では、今後、国内の企業を標的とした攻撃が強まるおそれがあるとし、注意喚起に利用できるチラシやBECに関するレポート等を提供して活用を呼びかけている。

参考　https://www.ipa.go.jp/security/announce/201808-bec.html

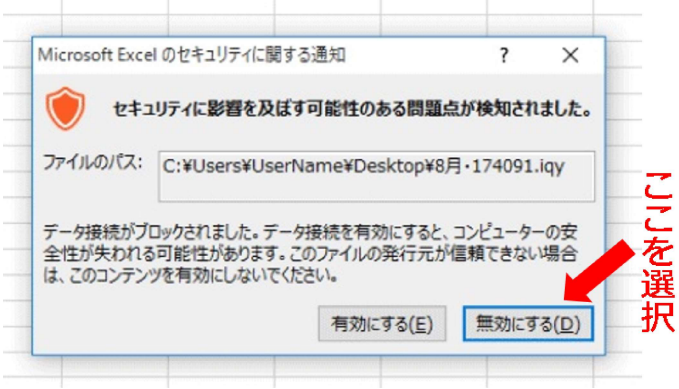
○ 拡張子「iqy」のファイルを使うExcelを悪用した攻撃に注意！

拡張子「.iqy（アイキューワイ）」のファイルを使う攻撃が急増しているとしてトレンドマイクロが注意を呼びかけている。

この攻撃は今年5月に海外で報告され、トレンドマイクロによる観測では、この拡張子のファイルを添付し「お世話になります」「ご確認ください」「写真添付」「写真送付の件」などのさまざまな件名が付けられたメールが流通しているという。

ファイルを開くとMicrosoftExcelが起動し、警告メッセージで「有効にする」を選択すると不正なスクリプトファイルがダウンロードされ、マルウェアに感染する。

被害防止対策として、添付ファイルを開かないこと。仮に開いてしまっても、警告メッセージで必ず「無効にする」を選択するよう呼びかけている。



参考　https://blog.trendmicro.co.jp/archives/19387

平成30年10月10日

サイバーセキュリティ関連情報（10月号）

鳥取県警察本部サイバー犯罪対策課

○ フェイスブック25万人分の個人情報ネット流出

ニューヨークの繁華街のスクリーンに表示されたフェイスブックのロゴ＝3月（AP＝共同）

交流サイト大手フェイスブックの利用者のものと認められる携帯電話番号やメッセージのやりとりなどの個人情報がインターネット上に大量流出していたことがわかった。

サイバー攻撃による漏えいの可能性があり、日本人のものを含む世界各国の利用者25万人分以上に上るとみられる。

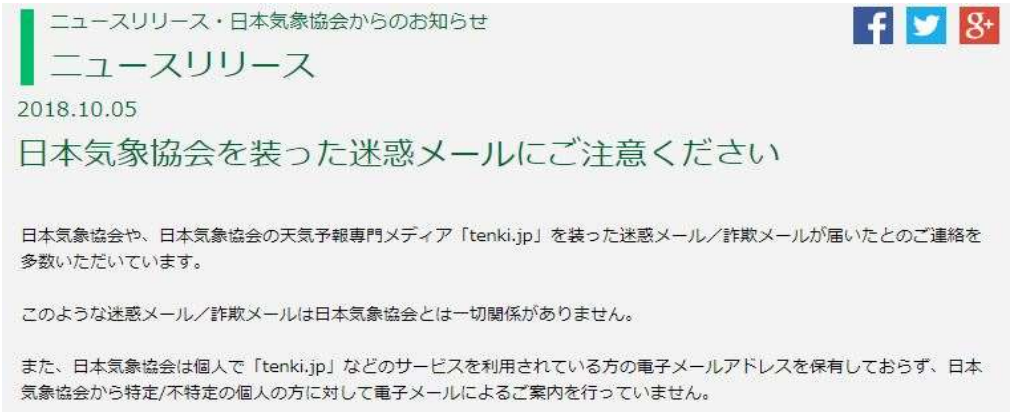
マーク・ザッカーバーグ最高経営責任者は問題を深刻に受け止めセキュリティ対策への投資を続けると説明している。

参考　共同通信社　https://this.kiji.is/421237905324950625

○ 日本気象協会を装う迷惑メールでウイルス感染のおそれ

日本気象協会は、同協会の天気予報専門メディア「tenki.jp」を装った迷惑メールが相次いで送られていると発表した。

同協会によると、「台風は最悪のコースへ」「お住まいの地域が冠水する危険性があります」などの文面で危機感をあおり、リンクされたサイトにアクセスしたり、添付ファイルを開いたりするとコンピューターウイルスに感染するおそれがあるとして、リンク先アドレスを絶対にクリックしないよう注意を呼び掛けている。


ニュースリリース・日本気象協会からのお知らせ

ニュースリリース

2018.10.05

日本気象協会を装った迷惑メールにご注意ください

日本気象協会や、日本気象協会の天気予報専門メディア「tenki.jp」を装った迷惑メール／詐欺メールが届いたとのご連絡を多数いただいています。

このような迷惑メール／詐欺メールは日本気象協会とは一切関係がありません。

また、日本気象協会は個人で「tenki.jp」などのサービスを利用されている方の電子メールアドレスを保有しておらず、日本気象協会から特定/不特定の個人の方に対して電子メールによるご案内を行っていません。

参考　日本気象協会　https://www.jwa.or.jp/news/2018/10/post-001087.html

平成30年11月13日

サイバーセキュリティ関連情報（11月号）

鳥取県警察本部サイバー犯罪対策課

○「アダルトサイトを閲覧している姿を撮影した」などと脅す詐欺メールが急増

平成30年7月以降、「アダルトサイトを閲覧しているあなたの姿をウェブカメラで撮影した。家族や同僚にばらまかれたくなければ仮想通貨で金銭を支払え」等と記載された詐欺メールの相談が急増しています。

メールの内容として、『自分のパスワードが記載されている』『連絡先情報を収集したと脅す』『仮想通貨を要求する』『送信元が自分のアドレスになっている』などの特徴があります。

これらの詐欺メールを受信した場合は、

- **仮想通貨などを絶対に支払わないこと**
- **記載されていたパスワードは変更すること**
- **複数のサイトで同じパスワードを使い回さないこと**

を徹底し、対策を行って下さい。

参考　IPA　https://www.ipa.go.jp/security/anshin/mgdayori20181010.html

○ iPhoneのファイル共有機能を悪用した通称「AirDrop痴漢」に注意！

iPhone、iPad等のApple製の端末同士で行うファイル共有機能「AirDrop（エアドロップ）」を悪用し、電車内で女性にわいせつな画像を送信したなどとして、大阪府警と兵庫県警は、画像送信した男性を迷惑防止条例違反としてそれぞれ逮捕しています。

被害防止対策として、iPhoneなどのApple製の端末を使用している方は、

設定 → 一般 → AirDrop　で**『すべての人』を選択しない**で下さい。

また、相手の端末に本名を表示させないための対策として、

設定 → 一般 → 情報　で表示される名前の部分に**本名を記録しない**で下さい。

設定　一般　AirDrop　情報

引用：Apple社　iPhone（iOS12）　設定画面

平成30年12月３日

サイバーセキュリティ関連情報（12月号）

鳥取県警察本部サイバー犯罪対策課

○ 冬物の「衣服・履物」の詐欺・模倣品サイトに注意！

インターネットの通販サイトで商品を購入したが「商品が届かない」「偽物が届いた」「連絡しても返事がない」などの相談が国民生活センターに多数寄せられています。

特に近年、ダウンジャケット、ブーツなどの冬物の衣服・履物を購入する時期にあわせて、詐欺・模倣品サイトが多く登場し、トラブルが冬季（11月～1月）に集中して発生する傾向があります。

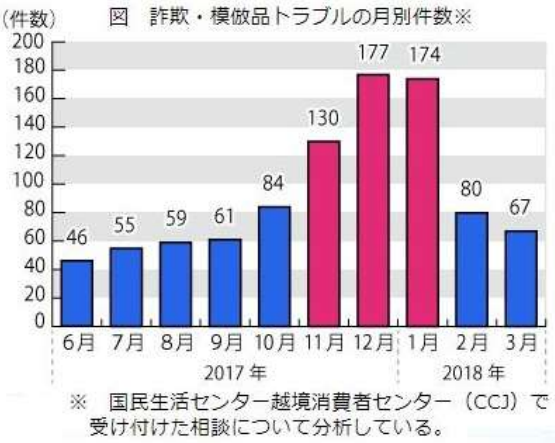


図　詐欺・模倣品トラブルの月別件数※

※　国民生活センター越境消費者センター（CCJ）で受け付けた相談について分析している。

詐欺・模倣品サイトは、

- **日本語の字体、文章表現がおかしい**
- **販売価格が大幅に割引されている**
- **支払方法が銀行振込のみになっている**

などの特徴があります。

普段利用しない通販サイトで商品の購入を検討する場合は十分に注意して下さい。

引用　独立行政法人国民生活センター http://www.kokusen.go.jp/news/data/n-20181023_1.html

○ SNSで見知らぬ外国人からの友達申請に要注意！

インターネット上の交流サイトの友達申請機能などで知り合った外国人から恋人や結婚相手になったかのような言葉巧みなメッセージによって被害者を信用させ、金銭を送金させる詐欺（通称、国際ロマンス詐欺）が発生しています。

金銭要求まで知り合ってから１年以上かけて信用させる場合や、組織で共謀し、友人や弁護士、関税職員などの役を演じて騙すケースもあります。

SNSなどの交流サイトで全く面識のない人物から友達申請された場合、まず詐欺を疑って下さい。

また、年末年始にかけて、様々な手口による特殊詐欺の発生が予想されます。

ご注意をお願いします。

参考　警察庁　特殊詐欺対策

https://www.npa.go.jp/safetylife/seianki31/1_hurikome.htm

平成３１年１月16日

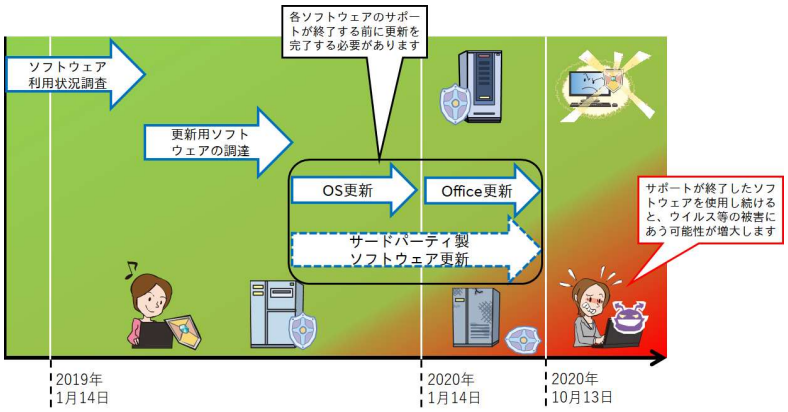
サイバーセキュリティ関連情報（１月号）

鳥取県警察本部サイバー犯罪対策課

○ 「Windows7」「Office2010」などのサポート終了まで、残りあと僅か！

Microsoft社は、「Windows7」「WindowsServer2008」を2020年1月14日に、「Office2010」を2020年10月13日に、それぞれのサポートを終了する。以降、脆弱性が見つかった場合でもアップデートやセキュリティ更新プログラムは提供されなくなる。

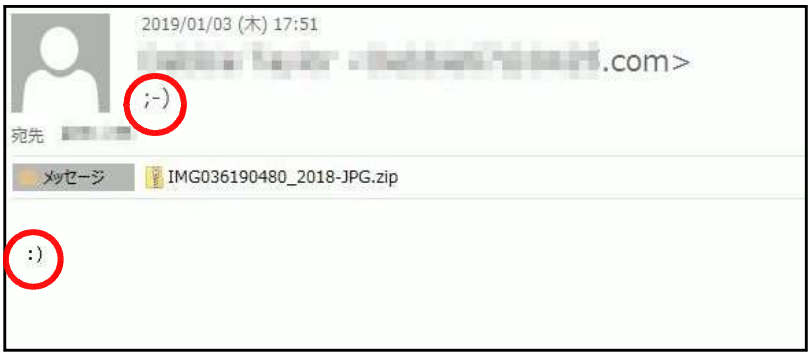
特に「Windows７」などのOS（オペレーティングシステム）のサポート終了は、OSそのものだけでなく、OS上で稼働するブラウザやテキストエディタのほか、他のソフトウェアにも及ぶと指摘されており、メーカー各社は早めのWindows10環境への移行を強く勧めている。



引用　IPA https://www.ipa.go.jp/security/announce/win7_eos.html

○ 新年にランサムウェアの「ばらまき攻撃」が「顔文字メール」で復活

トレンドマイクロによると、件名とメール本文が「：)」、「：D」などのいわゆる「顔文字」のみとなっている特徴的なメールを経由してマルウェアを拡散させる新たな攻撃の発生を確認したと発表した。



顔文字の例（6種）

：D
：-)
;)
; -D
:)
; -)

メールに添付されたファイルを受信者が開いてしまうと、最終的にランサムウェアなどが侵入することを確認しているとのこと。

受信したメールの送信者や内容の正当性をよく確かめ、メールの添付ファイルや本文中のURLを安易に開かないよう注意を呼び掛けている。

引用　トレンドマイクロセキュリティブログ　https://blog.trendmicro.co.jp/archives/20107

平成３１年２月５日

サイバーセキュリティ関連情報（２月号）

鳥取県警察本部サイバー犯罪対策課

○ ２月１日～３月18日は「サイバーセキュリティ月間」！

政府では、サイバーセキュリティに関する普及啓発強化のため、２月１日から３月１８日までを「サイバーセキュリティ月間」としています。国民の皆様にサイバーセキュリティについての関心を高め、理解を深めていただくため、サイバーセキュリティに関する様々な取組を集中的に行っていきます。

内閣サイバーセキュリティセンター（NISC）のホームページでは、身近な話題からサイバーセキュリティに関する基本的な知識を紹介した「インターネットの安全・安心ハンドブックVer4.00」を公開し、様々な形での活用を呼び掛けています。

この機会に、ぜひ、サイバーセキュリティに関する理解を深めていきましょう！

引用　NISC　https://www.nisc.go.jp/security-site/handbook/index.html

○ 「情報セキュリティ10大脅威2019」決定

情報処理推進機構（IPA）は、2018年に発生した社会的に影響があった情報セキュリティにおける脅威事案について、有識者、研究者ら約120名からなる「10大脅威選考会」が選出した「情報セキュリティ10大脅威2019」を発表しました。

なお、IPAは、2月下旬に詳しい解説をウェブサイトで公開するとしています。

■「情報セキュリティ10大脅威 2019」

NEW：初めてランクインした脅威

昨年順位	個人	順位	組織	昨年順位
1位 (*1)	クレジットカード情報の不正利用	1位	標的型攻撃による被害	1位
1位	フィッシングによる個人情報等の詐取	2位	ビジネスメール詐欺による被害	3位
4位	不正アプリによるスマートフォン利用者の被害	3位	ランサムウェアによる被害	2位
NEW	メールやSNSを使った脅迫・詐欺の手口による金銭要求	4位	サプライチェーンの弱点を悪用した攻撃の高まり	NEW
3位	ネット上の誹謗・中傷・デマ	5位	内部不正による情報漏えい	8位
10位	偽警告によるインターネット詐欺	6位	サービス妨害攻撃によるサービスの停止	9位
1位	インターネットバンキングの不正利用	7位	インターネットサービスからの個人情報の窃取	6位
5位	インターネットサービスへの不正ログイン	8位	IoT機器の脆弱性の顕在化	7位
2位	ランサムウェアによる被害	9位	脆弱性対策情報の公開に伴う悪用増加	4位
9位	IoT 機器の不適切な管理	10位	不注意による情報漏えい	12位

引用　IPA　https://www.ipa.go.jp/security/vuln/10threats2019.html

いまさら聞けない！ソーシャル・ネットワーキング。サービスって何？

(株)セブンズデザイン　代表取締役　坂本　拓也

一言で言えば「意思や情報を伝達する道具」です。横文字では「コミュニケーションツール」ですね！

人間は大昔から様々な方法でコミュニケーションをとってきました。文字がない時代では壁や地面や土器に「絵」を書いたり、「文字」ができると紙や壁に書いたり、それを遠くに届けるために人や車や電車や飛行機など様々な手段や方法が発展を遂げてきました。そして今はインターネットの時代です。このインターネットにより大きく世界が変わりました。この変化はとてもスピードが速くて専門分野にいる私たちでさえついていけないくらいすごい勢いで進化しています。その変化についていけない方はたくさんいて当然ですよね。

そして、最近ではスマートフォンがたくさんの人たちに利用されいっぺんに多くの人たちとコミュニケーションがとれるようになりました。

ここが今までと大きな違いだと感じています。これまでは特定の人とのコミュニケーションしかできませんでした。それがこのソーシャル・ネットワーキング・サービスを使うと一度にたくさんの人とコミュニケーションをとることができます。（これからはSNSと言います。）それが現在のSNSの特徴です。

ではどれくらいのSNSがあるのでしょうか。。。

まだまだありますが、ひとまず主要なSNSこんな感じです。結構ありますよね。

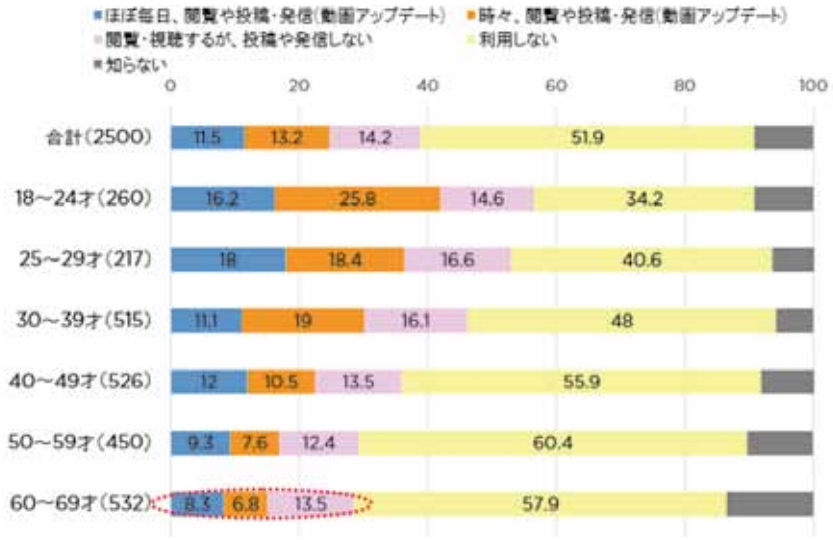
分類すると、情報収集系・写真/動画投稿系、コミュニティ系分類されます。

この会報を読まれてる方は比較的年配者の方が多いと予想してますが、その年配者の方の利用率が最も高いのは「Facebook」ですね。これはある意味驚異的だと思いました。パソコンが苦手な層で若者が比較的やっているであろうネットサービスに年配の方が投稿している。この変化はすごいですね。もちろんされていない方もいるわけですが、それでも周りを見てもおじさんやおばさんがスマホを持って使っています。最近の年配者は若いです！LINEも結構使われてますよね。

ではちょっと最近のSNSの動向ですが、全部紹介することは無理なので「実用的」なSNSを調べてみました。

■Facebook

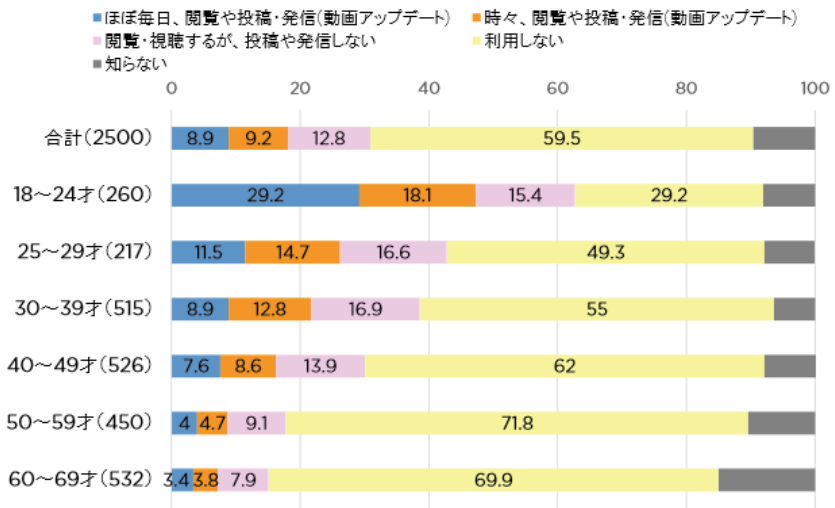
ユーザー数：2，400万人（平成26年11月）
月間アクティブ率：53・1％
【特徴】実名制である。他のSNSユーザー層に比べて年配者の利用が高い。
低年齢層のアクティブ率は下がりつつあるが、Instagramがfacebook上で拡散されるようになると歯止めになるのかもしれない。ただ、相変わらず年配者の利用・アクティブ率が高いのが特徴。また、仕事上利用される経営者も多い。嫉妬する人も多いためSNS疲れも発生している。海外ユーザーともつながりやすい。



また、広告を出稿できる。例えば新しい商品が30代女性をターゲットにしたい場合、これまでの宣伝方法では広く多くの方に宣伝する手法を取られており、特に鳥取という地域を考えると媒体は限られている。Facebookの広告では「鳥取市、30代、女性、化粧関心がある、既婚、学歴」（ユーザー登録内容によって異なる）といった細いところまで絞り込み広告を出すことができる。範囲を絞り無駄なコストを減らすことでこれまでと違うパフォーマンスを得ることができる。

■Twitter

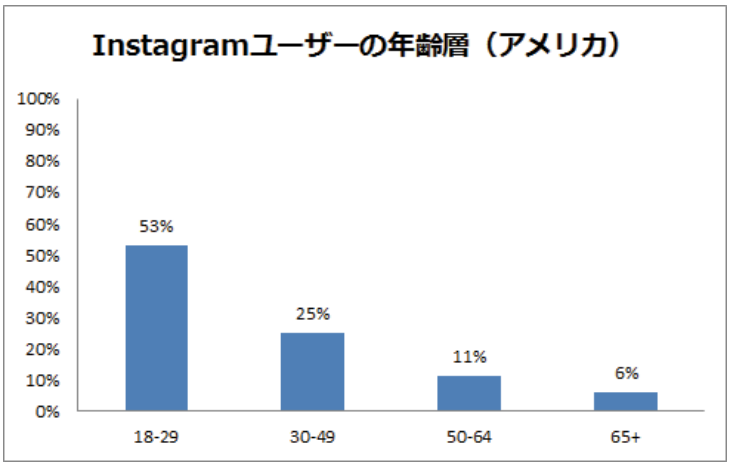
ユーザー数：1，980万人（平成26年6月）
月間アクティブ率：60・5％
【特徴】匿名で利用可能。匿名性のため低年齢層が多くを占めている。自分を知られないので気軽につぶやくことができ、拡散能力も高い。有名人も使っており様々な情報を得ることが可能。気になる専門家を「フォロー」しておくと有利な情報を得ることもできる。低年齢層に情報を拡散したい



時はTwitterが有効。ただしフォロワーを増やす努力が必要になるため決して容易ではない。フォロワーが必要だと思えるような情報を配信したり工夫する必要がある。広告が出稿できる。主なターゲティングは「興味関心、フォロワー、キーワード指定、地域」など絞ることができる。利用層が10代～30代なので若年層の商材であれば有効である。

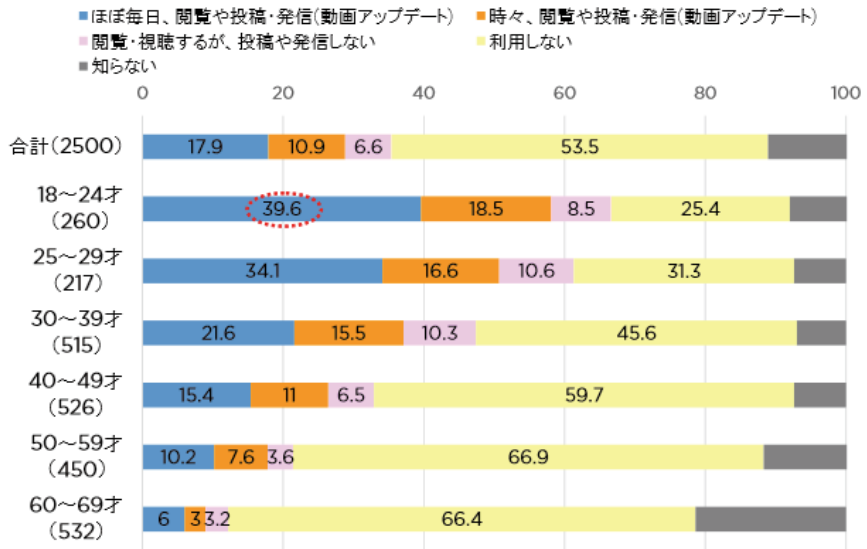
■Instagram（facebookが買収）

ユーザー数：未発表
月間アクティブ率：76・7％
【特徴】匿名で利用可能。これからさらに注目されるSNS。大きな特徴は画像によるコミュニケーションで撮った画像を編集することでクオリティの高い画像を演出することができる。日本においても若年層がメイン利用者である。FacebookやTwitterは文章も含まれており手間だが、画像を撮って編集するだけなので気兼ねなく自分のコレクションなどをアップすることができる。飲食店やファッション系の事業をされている方にはオススメツール。今後広告出稿できる動きもあるため期待できる。



■LINE

国内ユーザー：5，200万人（平成26年7月）
月間アクティブ率：90・6％
【特徴】日本でダントツのコミュニケーションツールである。メールに変わるツールとして利用されており、スタンプというイラストを送ることでコミュニケーションをとることが大きな特徴である。事業に活用するのであればLINE@を利用すると多くのユーザーに宣伝することが可能となるが、難しいのが欲しい情報かどうかになる。Facebookページにも言えることだが、継



続的な情報を受け取ってもらうには「いいね」を押してもらう必要がある。LINE@では「友だち登録」してもらう必要がある。

■まとめ

他にも気になるSNSがありますが、現在「実用的」なSNSとしては上記の4社を活用することをオススメします。ですが情報を配信する際には気をつけることがあります。

・誹謗中傷になるようなコメントや画像は配信しない
・プライベートな部分を出しすぎるとプライバシーが保たれない。
・配信した情報は削除することが困難（操作方法）な為、慎重に投稿する必要がある
・第三者が画像に入っていないか確認する。入っていれば投稿の有無を確認する
・タグ付する際にはしてもいいか確認する

SNSは使い方によってはすごく有効的に作用します。

昔の友人とつながったり、知らない方から友達リクエストがきたり、いろんな情報を調べなくてもわかったり、セルフプロモーションができたりたくさんのメリットがあります。その反面、油断すると間違った情報や間違った風にとられることもあるので気をつける必要があります。それをわかった上で利用すれば安全なツールです。

ぜひ利用してご自身にとっていいか悪いか判断していただければと思います。

特に今後事業に活用する上では、ターゲットをピンポイントに絞った広告出稿ができるため、今後こういったSNSを活用した広告が今後の広告業界を大きく変えていく可能性が十分にあります。当社でも現在ネット広告の出稿依頼が増えてきています。敏感な事業者は動きが早く「先駆者メリット」を得ています。

鳥取においてはまだまだ「ネット集客」を取り入れる事業主は少なくそういった意味では「先駆者メリット」を得ることが可能だと思います。また広告費も費用対効果に応じた設定が可能となり、広告費も抑えつつ最大限のパフォーマンスが得やすくなりました。過去の「ネット集客」はメリットが感じられなかったと思いますが、SNS出現によってそのメリットが大きく変わってきたのは事実です。もちろん紙媒体でしか伝わらない部分もあるので全てではないですが、今後のマーケティングに生かしていく必要があると考えています。「ネット集客」についてご質問があればお気軽にお申し付けください（ちょこっと自社PRです…。）。

教職員の皆様へ

「電子メディアとの付き合い方学習ノート（シート）」の活用について

子どもたちを取り巻く状況

近年、スマートフォン、ゲーム機等電子メディア機器が子どもたちの生活に浸透し、長時間利用による生活習慣の乱れが指摘されています。また、平成27年度に鳥取県教育委員会が実施した「インターネットの利用に関するアンケート」調査の結果から、利用の低年齢化が進んでいること、利用によりトラブルを抱えている子どもたちがいることがわかりました。

電子メディア機器（※）でインターネットを利用している割合　※スマートフォン、携帯ゲーム機、携帯音楽プレーヤー等

○小学生（６年生）80．9%　**○中学生（2年生）**86．2%　**○高校生（2年生）**96．2%

インターネットを利用していて困ったことや嫌なこと（上位4位）

○小学生（6年生）	○中学生（2年生）	○高校生（2年生）
・使いすぎて睡眠不足 ・知らない人からの連絡 ・人間関係のトラブル ・メール等が気になりスマートフォンを手放せない	・使いすぎて睡眠不足 ・人間関係のトラブル ・知らない人からの連絡 ・メール等が気になりスマートフォンを手放せない	・知らない人からの連絡 ・使いすぎて睡眠不足 ・メール等が気になりスマートフォンを手放せない ・人間関係のトラブル

また、家庭でのルールの有無について保護者と児童・生徒には認識に差があることも分かりました。

「家庭で何らかのルールがある」と回答した児童・生徒と保護者の割合の比較

○小学生（6年生）		○中学生（2年生）		○高校生（2年生）	
児童	保護者	生徒	保護者	生徒	保護者
75．0%	94．2%	61．7%	90．3%	37．8%	82．0%
19．2ポイントの差		**28．6ポイントの差**		**44．2ポイントの差**	

鳥取県では、子どもたちが電子メディア機器と適切に接していけるよう、これまで児童・生徒や保護者、地域への啓発活動を行ってきました。平成28年度からは、鳥取県 PTA 協議会の提唱する「メディア21：00」運動を共通ルールとして、児童・生徒が安心・安全にインターネットを利用できる環境づくりを地域全体で進めようと校長会や医師会等の賛同もいただきながら取り組んでいます。

※「メディア21：00」運動とは・・・鳥取県の子どもたちは、21時以降は友だちを巻き込むようなLINEなどのコミュニケーションツールやゲームの利用をやめて、相手の時間を尊重しようという運動。

先生方へお願い

この「電子メディアとの付き合い方学習ノート（シート）」（以下「ノート」という。）は、電子メディア機器（テレビ、スマートフォン、パソコン、ゲーム機、音楽プレーヤー等）との上手な付き合い方を学校や家庭で学習できるようにつくりました。このノートを利用して、児童・生徒自身が電子メディア機器の使い方を振り返ったり、使い方について家の人と話し合ってルールを決めたりできるようになっています。また、ノートには家族で話し合う際の参考にしていただくため「保護者のみなさんへ」のページもあります。シートについては、家族に限らず友だちと話し合うこともできるようにしています。

なお、このノートは、電子メディア機器の利用や購入を推奨するものではありません。今現在利用していない場合でも、想像しながら親子で考え、話し合ってもらうことができます。裏面の活用例を参考にしていただき、保護者への啓発に御活用ください。

【対象学年】

学習ノートＡ：小学校１～３年生、学習ノートＢ：小学校４～６年生、学習シートＣ：中学生・高校生

※学校の実態に合わせて有効に御活用ください。

活用例

※活用例ですので、それぞれの学校の実態に合わせて有効に御活用ください。

学校で…

家庭学習の課題

ショートホームルーム（朝の会、帰りの会など）で記入

情報モラルの学習
・ネット依存
・個人情報の保護
・SNS 等のトラブル
等の学習に活用

学級活動
・基本的な生活習慣の形成
・心身ともに健康で安全な生活態度の形成
等の学習後に記入

道徳
・節度　・礼儀
・思いやり　・社会正義
・規則の尊重
の学習後に記入

家庭で…（学校で…）

家庭（学校）で話し合い、話し合ったことを記入

学校で回収

家庭への啓発

家庭（学校）での話合いの様子を
・学年・学級通信で紹介
・参観日後の学年・学級懇談で活用
していただくと、なお効果が期待できます。

【小学校１～３年生向け】

電子メディアとの付き合い方

学習ノートA

児童の皆さんへ

テレビやゲーム、スマートフォンやパソコンはとても便利で、楽しいものです。このノートは、みなさんがテレビやゲームなどを使いすぎないように、また友だちとのやりとりで思いがけない失敗をしたりしないようにするため、学校や家で学べるようにつくりました。このノートでは、自分の使い方を振り返ったり、友だちやお家の人と話し合ったりできるようになっています。

保護者の皆さんへ

近年、インターネット環境の急速な発達により、スマートフォン等電子メディア機器は生活の中でなくてはならないものとなり、子どもたちの生活の中にも浸透しています。子どもたちにとって、親しみやすく、便利で楽しいものとなっている反面、友人関係のトラブルや生活習慣の乱れなどが深刻化していることから、上手につきあっていくことが求められています。利用に際してトラブルに巻き込まれないよう、家庭で話し合うために、このノートを作成しました。子どもたちが「自分で考え」、家庭で「話し合う」構成になっています。また、家庭で話し合う際の参考にしていただくため「保護者の皆さんへ」のページもあります。

なお、このノートは、電子メディア機器の購入を推奨するものではなく、利用に際して家庭で考え、話し合ってもらうことを目的に作成しています。

学校では

このノートは、子どもたちや各学校の実情に応じて、学校での学習（道徳や学級活動などの情報モラルに関する学習等）や家庭での学習（週末や長期休業での宿題等）で活用できるようになっています。また、このノートをもとに、各家庭で話し合われたことを学級・学年通信等でまとめていただき、保護者の皆さんと情報共有したり、保護者懇談等で活用していただいたりすることも目的の一つとしています。

年　　組　　番

名前

鳥取県子どものインターネット利用教育啓発推進協議会
（事務局：鳥取県教育委員会事務局社会教育課）

「規則正しい生活」

はな子さんは、動物が大すきです。

ある日、学校で友だちが、「インターネットで動物の動画を見ることができる。」と教えてくれました。はな子さんは、家に帰って、さっそく動物の動画を見てみました。かわいい動物が、たくさん出てきました。

画面の横に、動物の出てくる「おすすめ動画」がたくさん出てきました。いくら見ても、あきることがありません。

とても楽しいので、毎日家に帰ると宿題もせず、見てしまうようになりました。次々と見ていると、いつの間にか長い時間がたっています。毎日していたお手伝いも、できなくなりました。夜おそくまで見てしまうので、朝起きることができなくなりました。

【考えてみよう】

① はな子さんの生活で、気になるところはどこですか。

---

② はな子さんは、なぜ動画を見ることをやめることができないのでしょう。

【家の人と話し合ってみましょう】

ゲームやテレビ、インターネットの約束（ルール）を家の人と話し合って決めてみましょう。

★おうちの方へ
話し合う際には次ページの「保護者のみなさんへ」を参考にしてください。

先生の印

保護者のみなさんへ

ポイント

○動画視聴やゲームをやめられなくなり、生活習慣が乱れてしまう事例が多いです。
○ルールをつくる時には、家庭内でしっかり話し合い、具体的なルールをつくる必要があります。
○ルールをつくるときには、「守れなかった時のルール」もつくることが大切です。

動画視聴に熱中するあまり、夜遅くまで起きているため、寝不足になって生活習慣が乱れてしまう児童・生徒が増えています。ひどくなると昼と夜が逆転して学校へ行けなくなる事例もあります。

インターネットでの動画視聴には「次々と関連するおすすめ動画が出てくる」など、やめられなくなる仕組があります。そのため、インターネットでの動画視聴に夢中になってしまい、いつの間にか長時間視聴してしまっていたということがあります。そうならないように家庭で約束（ルール）を決めておきましょう。ルールを決めるときには、家族でよく話し合ってください。

ゲームでも同様の事例があります。ゲームについてもルールを決めておくことが大切です。

知っていますか？　動画再生サイトYouTubeの利用規約について…

※YouTube利用規約より引用

「本サービスは13歳未満の子供による利用を意図していません。あなたが13歳未満の場合、YouTubeウェブサイトを利用しないで下さい。あなたに、より適しているサイトが他にも沢山あります。あなたにそのサイトが適しているか、ご両親に相談してください。」

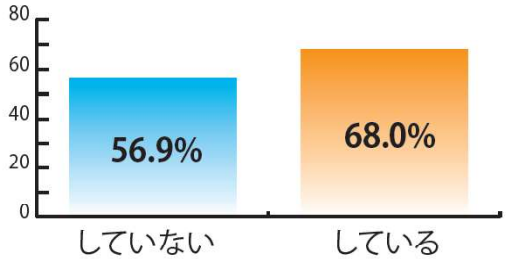
決めておきたいルールの例

- □ 使用時間（１日の使用は○時間以内 など）
- □ 使用場所（自分の部屋では使用しない など）
- □ ルールを守れなかったときは…（○日間使用禁止にする、保護者に返却する など）

生活習慣と学力の関係（平成29年度全国学力・学習状況調査より）

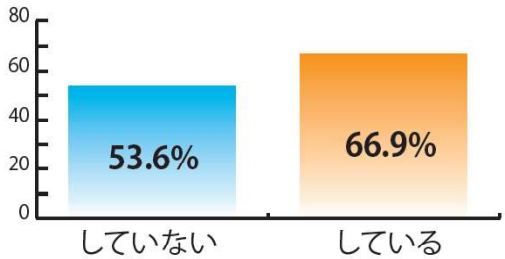
毎日同じくらいの時刻に寝ていますか

＜鳥取県における２教科平均正答率＞



毎日同じくらいの時刻に起きていますか

＜鳥取県における２教科平均正答率＞



⇒ **決まった時間に寝起きしている児童の方が、２教科（国語・算数）の平均正答率が高い傾向が見られます。**

※2教科平均正答率とは、「（どちらかといえば）している」（あるいは「（どちらかといえば）していない」）と回答した児童の国語と算数の正答率の平均

家庭で読むページ（家の人と一緒に読みましょう）

インターネットを安全に使うため、知っておきたいこと

インターネットには、様々な特性やサービスがあります。自分やまわりの人を守るために知っておきましょう。

①世界中に公開されます

インターネットへ載せた文章や写真は世界中に公開されます。「親しい友だちだけだから…」と思っていても、誰かが転送すれば世界中に公開されてしまいます。

②一度載せると取り消すことはできません

インターネット上に一度載せた文章や写真は取り消すことができないことが多く、必ずどこかに記録が残ってしまいます。名前を書かない場合でも誰が発信したかという記録が必ず残ります。将来の自分にとって、マイナスになってしまうこともあります。

③情報をそのまま信用してはいけません

インターネット上には誰でも情報を載せることができるので、信用できない情報も多く、情報を手に入れる時には正しい内容かどうかを確かめる必要があります。

④相手のことを考えながら通信しましょう

インターネットでのやりとりは文字が中心になるため、思いが相手に伝わりにくく、誤解が生じる場合があります。また、同じ情報でも相手によってとらえ方が違う場合もあります。また相手にも事情があり、すぐに返信できないこともあるということを知っておきましょう。

⑤夢中になってやめられなくなるサービスがあります

インターネットのサービスの中には、夢中になるサービスがたくさんあります。使い始めるとなかなかやめられなくなり、依存になる可能性もありますので、使う時間を決めましょう。

「メディア21：00」運動

21時以降は友だちを巻き込むようなLINE（ライン）などのコミュニケーションツールやゲームをやめて相手の時間を尊重しようという運動です。鳥取県PTA協議会が提唱し、様々な団体が賛同し運動を進めています。生活習慣をくずさないようにするためにも「メディア21：00」運動に取り組みましょう。

※電子メディア機器の利用や、購入をすすめるものではありません。

「やくそくしたのに…」

たろうさんは、友だちのじろうさんに、「明日、公園で遊ぶから来てね。」と紙に書いて渡しました。

じろうさんは、「ぼくはいいよ。」と返事を書いて返しました。

それを読んだたろうさんは、次の日「じろうさんが来る」と思って待っていました。

いつまでたっても、じろうさんは来ませんでした。

（本当は「遊べない」という返事でした。）

【考えてみよう】

① なぜ、たろうさんはじろうさんが来てくれると思ったのでしょう。

---

② たろうさん、じろうさんはどうすればよかったのでしょう？

たろうさん：

じろうさん：

【家の人と話し合ってみましょう】

友だちとコミュニケーションをとるとき、どんなことに気をつければよいか、家の人と話し合ってみましょう。

★おうちの方へ
話し合う際には次ページの「保護者のみなさんへ」を参考にしてください。

先生の印

保護者のみなさんへ

ポイント

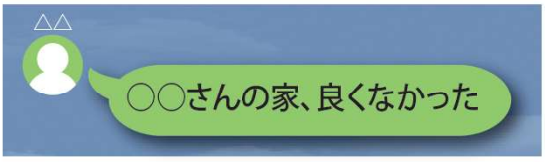
○短い文章でのやりとりは、相手に伝わりにくく、誤解を生みやすいため、トラブルに発展することがあります。
○実際の短い会話でもトラブルになることもあるので、話す側は相手に伝わっているか考えながら話し、聞く側も相手を信頼して悪く受け取らないようにする必要があります。
○普段から、相手を思いやって会話をするようにしなくてはいけません。
⇒スマートフォン等を使った無料通話アプリやメールなどの短い文章でのやりとりで誤解を生み、トラブルが起こりやすくなっています。

【トラブルの例】

①

⇒「遊ばない」「遊ぶ」の２つの意味にとれます

②



⇒「？」をつけ忘れたため、「悪い」という意味になってしまいます

③

⇒「交通手段を尋ねる」「来なくていいのに、何で来るんだ」の２つの意味にとれます

将来大きなトラブルに発展しないために、普段から家族で話し合って気をつけたいこと

- □ 大切なことは実際に会って話す。
- □ 受け取る側は悪い受け取り方をしないようにして、分からないときは真意を確認する。
- □ 普段から、誤解のない表現を心がける。
- □ 何よりも相手を思いやる気持ちを持つ。

困ったときの相談窓口

もしものときや、困ったときは、一人で悩まず、相談しましょう。
親身になって話を聞いてくれます。

インターネットを利用した犯罪にあったら

〔鳥取県警察本部〕
【警察相談専用電話】**#9110**（通常の通話料がかかります。IP電話不可）
0857-27-9110
【サイバー犯罪対策室】**0857-23-0110**（代表）
【電子メール】**k_haiteku@pref.tottori.lg.jp**

架空請求に悩んだり、請求の内容に疑問を感じたら

〔消費者ホットライン〕**188**（局番なし）
〔鳥取県消費生活センター〕
【東部消費生活相談室】**0857-26-7605**（県庁第２庁舎２階）
【中部消費生活相談室】**0858-22-3000**（倉吉交流プラザ２階）
【西部消費生活相談室】**0859-34-2648**（米子コンベンションセンター４階）

ネットいじめに悩んだら

〔相談電話・メール〕
【子どもの相談ダイヤル】**0120-0-78310**（無料・毎日 24時間）
【いじめ相談メール】**ijime@kyoiku-c.torikyo.ed.jp**
【いじめ 110番】**0857-28-8718**（毎日 24時間）
【子どもの人権 110番】**0120-007-110**（平日のみ 8:30 ～ 17:15）（無料・IP電話不可）

【小学校４～６年生向け】

電子メディアとの付き合い方

学習ノートB

児童の皆さんへ

このノートは、電子メディア機器（テレビ、スマートフォン、パソコン、ゲーム機、音楽プレーヤーなど）との上手な付き合い方を学校や家庭で学習できるようにつくりました。このノートを利用して、自分の電子メディア機器の使い方を振り返ったり、友だち同士や家庭で話し合ったりできるようになっています。

保護者の皆さんへ

近年、インターネット環境の急速な発達により、スマートフォン等電子メディア機器は生活の中でなくてはならないものとなり、子どもたちの生活の中にも浸透しています。子どもたちにとって、親しみやすく、便利で楽しいものとなっている反面、友人関係のトラブルや生活習慣の乱れなどが深刻化していることから、上手につきあっていくことが求められています。利用に際してトラブルに巻き込まれないよう、家庭で話し合うために、このノートを作成しました。子どもたちが「自分で考え」、家庭で「話し合う」構成になっています。また、家庭で話し合う際の参考にしていただくため「保護者の皆さんへ」のページもあります。

なお、このノートは、電子メディア機器の購入を推奨するものではなく、利用に際して家庭で考え、話し合ってもらうことを目的に作成しています。

学校では

このノートは、子どもたちや各学校の実情に応じて、学校での学習（道徳や学級活動などの情報モラルに関する学習等）や家庭での学習（週末や長期休業での宿題等）で活用できるようになっています。また、このノートをもとに、各家庭で話し合われたことを学級・学年通信等でまとめていただき、保護者の皆さんと情報共有したり、保護者懇談等で活用していただいたりすることも目的の一つとしています。

年　　組　　番

名前

鳥取県子どものインターネット利用教育啓発推進協議会
（事務局：鳥取県教育委員会事務局社会教育課）

「動画に夢中になると…」

はな子さんは、インターネットでお笑い芸人の動画を見るのが大好きです。

学校にいる間も、帰ってからどんな動画を見ようか考えていると、授業に集中できません。

今日も、家に帰るとすぐにインターネットで動画を見始めました。

「ひとつだけにしよう」と思いましたが、ひとつ動画を見ると、隣におすすめ動画や関連動画が出てきます。

気がつくと、見始めてから２時間が過ぎていました。

夕食の後、宿題をする前に、「もう少しだけ」と思い、動画を見ました。

気がつくと、夜中になっていました。

毎日こんな生活をしているので、朝寝坊をするようになり、宿題もできなくなりました。

【考えてみよう】

① はな子さんの生活で、気になったところはありますか。

② このままの生活を続けていると、はな子さんはどうなると思いますか。

【家の人と話し合ってみましょう】

家の人と話し合い、ゲームやインターネットを使うときの約束（ルール）を決めましょう。

★おうちの方へ
話し合う際には次ページの「保護者のみなさんへ」を参考にしてください。

先生の印

保護者のみなさんへ

ポイント

○動画視聴やゲームをやめられなくなり、生活習慣が乱れてしまう事例が多いです。
○ルールをつくる時には、家庭内でしっかり話し合い、具体的なルールをつくる必要があります。
○ルールをつくるときには、「守れなかった時のルール」もつくることが大切です。

動画視聴に熱中するあまり、夜遅くまで起きているため、寝不足になって生活習慣が乱れてしまう児童・生徒が増えています。ひどくなると昼と夜が逆転して学校へ行けなくなる事例もあります。

インターネットでの動画視聴には「次々と関連するおすすめ動画が出てくる」など、やめられなくなる仕組があります。そのため、インターネットでの動画視聴に夢中になってしまい、いつの間にか長時間視聴してしまっていたということがあります。そうならないように家庭で約束（ルール）を決めておきましょう。ルールを決めるときには、家族でよく話し合ってください。

ゲームでも同様の事例があります。ゲームについてもルールを決めておくことが大切です。

知っていますか？　動画再生サイトYouTubeの利用規約について…

※YouTube利用規約より引用

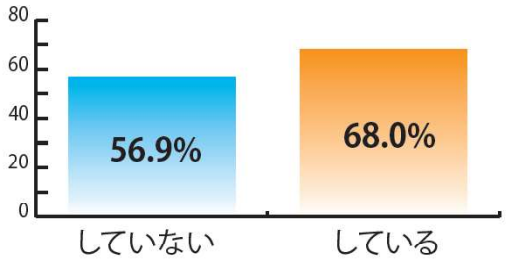
「本サービスは13歳未満の子供による利用を意図していません。あなたが13歳未満の場合、YouTubeウェブサイトを利用しないで下さい。あなたに、より適しているサイトが他にも沢山あります。あなたにそのサイトが適しているか、ご両親に相談してください。」

決めておきたいルールの例

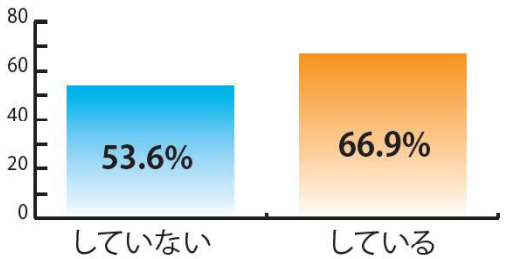
- □ 使用時間（１日の使用は○時間以内 など）
- □ 使用場所（自分の部屋では使用しない など）
- □ ルールを守れなかったときは…（○日間使用禁止にする、保護者に返却する など）

生活習慣と学力の関係（平成29年度全国学力・学習状況調査より）

毎日同じくらいの時刻に寝ていますか
＜鳥取県における２教科平均正答率＞



毎日同じくらいの時刻に起きていますか
＜鳥取県における２教科平均正答率＞



⇒ **決まった時間に寝起きしている児童の方が、２教科（国語・算数）の平均正答率が高い傾向が見られます。**

※2教科平均正答率とは、「（どちらかといえば）している」（あるいは「（どちらかといえば）していない」）と回答した児童の国語と算数の正答率の平均

家庭で読むページ（家の人と一緒に読みましょう）

インターネットを安全に使うため、知っておきたいこと

インターネットには、様々な特性やサービスがあります。自分やまわりの人を守るために知っておきましょう。

①世界中に公開されます

インターネットへ載せた文章や写真は世界中に公開されます。「親しい友だちだけだから…」と思っていても、誰かが転送すれば世界中に公開されてしまいます。

②一度載せると取り消すことはできません

インターネット上に一度載せた文章や写真は取り消すことができないことが多く、必ずどこかに記録が残ってしまいます。名前を書かない場合でも誰が発信したかという記録が必ず残ります。将来の自分にとって、マイナスになってしまうこともあります。

③情報をそのまま信用してはいけません

インターネット上には誰でも情報を載せることができるので、信用できない情報も多く、情報を手に入れる時には正しい内容かどうかを確かめる必要があります。

④相手のことを考えながら通信しましょう

インターネットでのやりとりは文字が中心になるため、思いが相手に伝わりにくく、誤解が生じる場合があります。また、同じ情報でも相手によってとらえ方が違う場合もあります。また相手にも事情があり、すぐに返信できないこともあるということを知っておきましょう。

⑤夢中になってやめられなくなるサービスがあります

インターネットのサービスの中には、夢中になるサービスがたくさんあります。使い始めるとなかなかやめられなくなり、依存になる可能性もありますので、使う時間を決めましょう。

「メディア21：00」運動

21時以降は友だちを巻き込むようなLINE（ライン）などのコミュニケーションツールやゲームをやめて相手の時間を尊重しようという運動です。鳥取県PTA協議会が提唱し、様々な団体が賛同し運動を進めています。生活習慣をくずさないようにするためにも「メディア21：00」運動に取り組みましょう。

※電子メディア機器の利用や、購入をすすめるものではありません。

「どんどんクリックしていくと･･･」

たろうさんは、ゲームの攻略法をいつもインターネットで調べています。

今日も、いつものようにインターネットのサイトを見ていました。ゲームの攻略に役立つ、いろいろな情報が載っていました。

見ていると、ゲームには関係のない、楽しそうなサイトの広告（バナー）や、おもしろそうな動画の情報がたくさん載っていました。

おもしろそうなので、クリックしてみました。

楽しそうな動画の情報がどんどん出てきます。

いろいろなところをクリックしていると、「入場しますか？」と表示されました。

文字の下に「入場する」「入場しない」のボタンがあったので、「入場する」のボタンをクリックしました。

すると、「会員登録完了。登録料３０，０００円」の文字が出てきました。

たろうさんは、困ってしまいました。

【考えてみよう】

① たろうさんの行動で、気になるところはありますか。

---

② たろうさんは、この後どうすればよいでしょう。

【家の人と話し合ってみましょう】

インターネットを利用するとき、たろうさんのようにならないために、どんなことに気をつけなければいけないか家族と話し合ってみましょう。

★おうちの方へ
話し合う際には次ページの「保護者のみなさんへ」を参考にしてください。

先生の印

保護者のみなさんへ

ポイント

○サイトに入ったとたん「登録料」と称して、高額請求を行うサイトがあります。また、「無料」や「プレゼント」の言葉を使い、クレジットカード番号等を聞き出し、詐欺をはたらくサイトがあります。

○個人情報（特にクレジットカード番号や銀行の口座番号など）を入力する場合には必ず保護者に相談することが必要です。

○トラブルに遭ったときは、信頼できる相談窓口（消費生活センターなど）や警察に連絡してください。そのために、保護者のみなさんは相談先を知っておく必要があります。

インターネットを介した詐欺等の例

サイトに入ったとたん「有料サイトの登録完了」の表示とともに、高額の登録料を請求された。

⇒ 表示された連絡先（アドレスや電話番号）に連絡せず、無視をしましょう。
（連絡を取っても解約される保証はなく、かえって個人情報を相手に知らせることになってしまいます。）

本物のショッピングサイトのように見せかけ、クレジットカード番号、パスワードなどを入力させられて、金銭を奪われた。また、実際の金融機関（銀行等）を名乗るメールで、キャッシュカード番号や暗証番号を聞き出され、金銭を引き出された。

⇒ 必ず大人が確認し、「いつもと違う」「何かおかしい」ということがあれば、入力をしないようにしましょう。また、金融機関からメールで暗証番号やクレジットカード番号を聞かれることはないということを知っておきましょう。

トラブルに発展しないために、家族で話し合っておきたいこと

□ むやみに知らないサイトに入らない。（インターネットは安全なサイトばかりではない。）

□ トラブルになったときは、自分で解決しようとはせず、必ず保護者に相談する。（お金を振り込んだり、相手に連絡を取ったりしない。）

□ 個人情報（住所、氏名、電話番号、クレジットカード番号など）を入力する必要がある場合は、必ず保護者に相談する。

□ 個人情報を聞き出すような不自然なメールを受け取った際には、必ず保護者に相談する。

家庭で読むページ（家の人と一緒に読みましょう）

インターネットトラブル事例集 ⚠

ネット依存（インターネット依存）

夜中までインターネットに夢中になり、寝不足になって、勉強等に影響が出ることがあります。ひどくなると昼夜逆転して、健康を害したり、学校に行けなくなったりすることもあります。

■つながり依存

SNSや無料通話アプリ、メールなどインターネット上のつながりに夢中になり、スマートフォンが手放せなくなったり、パソコンの前から動けなくなったりしてしまう人が増えています。

■ゲーム依存

オンラインゲームに没頭してしまい、やめられなくなってしまうこともあります。夜中にプレイすることが多くなるため、睡眠時間が短くなり、勉強や健康等に影響することがあります。

■コンテンツ依存

サイト内の動画や記事などを見続けてしまい、いつの間にか長い時間インターネットを使っていたという人も増えています。

使用する時間や場所などのルールを決めることが大切です。

SNSやネットで知り合った人による犯罪被害

SNSなどネット上で知り合った相手から、優しい言葉をかけられたり、趣味が合ったりすると、自分のことを理解してくれると思ってしまい、実際に会ったことがなくても信頼してしまいます。その結果、実際の友だちや家族に言えないことでも相談したり、悩みを話したりしやすくなります。

しかし、相手の年齢や名前などはもちろん、本当に優しい人かどうか、送ってきた写真が本物かどうかなど、確認することはできません。「自分の写真を送ってしまい、公開されてしまった」ばかりではなく、実際に会う約束をして、生命に関わる犯罪に巻き込まれるといった危険な事例も起きています。

・SNSで知り合った人を簡単に信用してはいけません。
・絶対に実際に会う約束などをしてはいけません。
・絶対に自分や友だちの写真や個人情報を送ってはいけません。

「そんなこと書き込んでも大丈夫？」

はな子さんはインターネットの掲示板に、本当の名前ではなく「めぐみ」という名前で、毎日学校での出来事を書き込んでいます。

読んでくれる人が少ないので、たくさんの人に読んでもらおうと、クラスの友だちの失敗や間違いを、おもしろおかしく書き込んでみました。

すると、読んでくれる人が増えました。

うれしくなったはな子さんは、もっと書き込みをしようと思いましたが、クラスの友だちは毎日失敗や間違いをするわけではありません。

困ったはな子さんは、クラスの友だちが失敗したという「うそ」を書き込み始めました。

ある日、学校で、クラスの友だちが、「誰かがぼくの悪口をインターネットの掲示板に書き込んでいます。」と先生に相談していました。

はな子さんは、「見つかってしまった。」と思いましたが、「本当の名前を出してないからばれないだろう。」と思って、だまっていました。

次の日、はな子さんは先生に呼ばれ、注意されました。

【考えてみよう】

① はな子さんの行動で、気になるところはどこでしょう。

---

② 失敗の書き込みをされたり、うそを書き込まれたりした友だちはどんな気持ちでしょう。

【家の人と話し合ってみましょう】

インターネット上に書き込みをするときに、何に気をつければよいか家の人と話し合ってみましょう。

★おうちの方へ
話し合う際には次ページの「保護者のみなさんへ」を参考にしてください。

先生の印

保護者のみなさんへ

ポイント

○ インターネット上に書き込まれたことは世界中の人が見ることができます。
　⇒書き込まれた内容を誰かが別のところにコピーしてしまうことがあります。
　⇒一度載せると取り消すことができません。
○ 匿名で書き込んでも、誰が書き込んだか突き止めることができます。
○ ネット上でうそや悪口を書くのは、世界中の人にうそや悪口を言っているのと同じことです。
○ 日常生活でやってはいけないことは、インターネット上でもやってはいけません。

インターネットの特性の一つとして、匿名で不特定多数への情報発信が簡単にできることがあげられます。そのため、匿名だからと軽い気持ちでSNSや掲示板に他人の悪口を書き込んだり、写真を掲載したりして、トラブルになる事例が増えています。

また、簡単にコピーできるため、広い範囲に拡散してしまい、取り消すことができなくなります。もとの書き込みを消しても、いつまでも別のところに残っているため、自分や友人の進学や就職等の将来に影響を与えることもあります。

匿名であっても、誰が書き込んだのか調べれば分かります。軽い気持ちで投稿した書き込みが、インターネット上で拡散、炎上し、住所や名前、学校等が突き止められ、個人情報がさらされるという事例もあります。

※後で書き込みを消そうと思っても、書き込みをしたときのIDやパスワード等、登録内容を忘れてしまったため、消すことができないという事例もあります。
　⇒IDやパスワードなどは忘れないようにきちんと管理するよう伝えましょう。

※自分のことが書き込まれているのを見つけたときは、すぐに保護者に相談するよう伝えておきましょう。

トラブルに発展しないために、家族で話し合っておきたいこと

○情報発信には責任を持たないといけない。書き込む前に、書き込んでよい内容かどうか、よく考える。
- 傷つく人がいないか、迷惑をかける人がいないか
- 自分の将来に悪い影響を与えないか

○トラブルになったら、すぐに家族に相談する。

困ったときの相談窓口

もしものときや、困ったときは、一人で悩まず、相談しましょう。
親身になって話を聞いてくれます。

インターネットを利用した犯罪にあったら

〔鳥取県警察本部〕
【警察相談専用電話】**#9110**（通常の通話料がかかります。IP電話不可）
0857-27-9110
【サイバー犯罪対策室】**0857-23-0110**（代表）
【電子メール】**k_haiteku@pref.tottori.lg.jp**

架空請求に悩んだり、請求の内容に疑問を感じたら

〔消費者ホットライン〕**188**（局番なし）
〔鳥取県消費生活センター〕
【東部消費生活相談室】**0857-26-7605**（県庁第２庁舎２階）
【中部消費生活相談室】**0858-22-3000**（倉吉交流プラザ２階）
【西部消費生活相談室】**0859-34-2648**（米子コンベンションセンター４階）

ネットいじめに悩んだら

〔相談電話・メール〕
【子どもの相談ダイヤル】**0120-0-78310**（無料・毎日 24時間）
【いじめ相談メール】**ijime@kyoiku-c.torikyo.ed.jp**
【いじめ 110番】**0857-28-8718**（毎日 24時間）
【子どもの人権 110番】**0120-007-110**（平日のみ 8:30 ～ 17:15）（無料・IP電話不可）

【中学生・高校生向け】

電子メディアとの付き合い方 学習シートC

インターネット依存になっていませんか…

以下の15の各質問について、最もあてはまる回答に○をつけてみましょう。全て回答したら○のついた数字を合計して、自身の依存レベルを確認してみましょう。

依存度チェックリスト

※インターネットとは・・・　サイトの閲覧、メール、SNS、ネットゲーム等

	項　　目	全く あてはまらない	あてはまらない	あてはまる	非常に あてはまる
1	インターネットの使用で、学校の成績（や業務実績）が落ちた。	1	2	3	4
2	インターネットをしている間は、よりいきいきしてくる。	1	2	3	4
3	インターネットができないと、どんなことが起きているのか気になってほかのことができない。	1	2	3	4
4	“ やめなくては”と思いながら、いつもインターネットを続けてしまう。	1	2	3	4
5	インターネットをしているために疲れて授業（や業務）時間に寝る。	1	2	3	4
6	インターネットをしていて、計画したことがまともにできなかったことがある。	1	2	3	4
7	インターネットをすると気分がよくなり、すぐに興奮する。	1	2	3	4
8	インターネットをしているとき、思い通りにならないとイライラしてくる。	1	2	3	4
9	インターネットの使用時間をみずから調節することができる。	4	3	2	1
10	疲れるくらいインターネットをすることはない。	4	3	2	1
11	インターネットができないとそわそわと落ち着かなくなり焦ってくる。	1	2	3	4
12	一度インターネットを始めると、最初に心に決めたよりも長時間インターネットをしてしまう。	1	2	3	4
13	インターネットをしたとしても、計画したことはきちんとおこなう。	4	3	2	1
14	インターネットができなくても、不安ではない。	4	3	2	1
15	インターネットの使用を減らさなければならないといつも考えている。	1	2	3	4
合計		点			
A要因（1，5，6，10，13）		点			
B要因（3，8，11，14）		点			
C要因（4，9，12，15）		点			

判定	総得点および３つの要因別得点のすべてが右にあてはまる場合 インターネットが健全に使用できているか、普段から自己点検を続けてください。	総得点40点以下		
		A要因13点以下	B要因11点以下	C要因11点以下
	総得点または３つの要因別得点のいずれかが右にあてはまる場合 インターネット依存に対する注意が必要です。インターネット依存におちいらないよう節度を持って使用してください。	総得点41点～43点		
		A要因14点以上	B要因12点以上	C要因12点以上
	総得点が該当するか、または、３つの要因別得点のすべてが右にあてはまる場合 インターネット依存傾向が非常に高いです。専門医療機関などにご相談ください。	総得点44点以上		
		A要因15点以上	B要因13点以上	C要因14点以上

「インターネット依存自己評価スケール（青少年用）Kースケール」
開発者：韓国情報化振興院（National Information Society Agency）　翻訳者：久里浜医療センターTIAR

インターネット依存にならないために、以下のような対策が考えられます。

- 利用する時間を決める。（タイマーの機能を使う、「○時以降は通信しない」など友だちとルールを決める。）
- インターネットを使う場所を決める。（自分の部屋では使わない、食事の時は使わない、居間で使うなど）
- 意識してインターネットを使わない日をつくる。など

チェックリストの結果を見て、インターネット依存にならないようにするにはどんなことに気をつければよいか、家族や友だちと話し合ってみましょう。

年　　組　　番　　名前：

H30

鳥取県子どものインターネット利用教育啓発推進協議会
（事務局：鳥取県教育委員会事務局社会教育課）

インターネットを安全に使うため、知っておきたいこと

インターネットには、様々な特性やサービスがあります。自分や周囲の人を守るために知っておきましょう。

①世界中に公開されます

インターネットへ載せた文章や写真は世界中に公開されます。「親しい友だちだけだから・・・」と思っていても、誰かが転送すれば世界中に公開されてしまいます。

②一度載せると取り消すことはできません

インターネット上に一度載せた文章や写真は取り消すことができないことが多く、必ずどこかに記録が残ります。名前を書かない場合でも、将来の自分にとって、マイナスになってしまうこともあります。

③情報をそのまま信用してはいけません

インターネット上には誰でも情報を載せることができるので、信用できない情報も多く、情報を取得するときには正しい内容かどうかを確かめる必要があります。

④相手のことを考えながら通信しましょう

インターネットでのやりとりは文字が中心になるため、思いが相手に伝わりにくく、誤解が生じる場合もあります。また相手にも事情があり、すぐに返信できないこともあるということを承知しておきましょう。

⑤夢中になってやめられなくなるサービスがあります

インターネットのサービスの中には、夢中になるサービスがたくさんあります。使い始めるとなかなかやめられなくなり、依存になる可能性もありますので、使う時間を決めましょう。

「危険です、ながらスマホ（歩きスマホ）」

ながらスマホのトラブル事例

■ 自転車に乗りながらスマホを操作していて・・・

・携帯電話を操作しながら自転車に乗っていた高校生が女性に衝突し、けがを負わせた。その後、裁判所は保護者に５，０００万円の損害賠償の支払を命じた。

・大学生がスマホを見ながら自転車で走行中、高齢の女性に衝突し死亡させたため、警察は「重過失致死罪」の容疑で書類送検した。

■ 歩きながらスマホを操作していて・・・

・スマホを操作しながら歩いていたところ、つまずいて転倒し、顔面を強打した。

・携帯電話を操作しながら歩いていて踏切に進入し、電車にはねられて死亡した。

自転車に乗ったり、歩いたりしながらスマートフォンを操作することは、注意が散漫になったり、片手運転になったりするので、大変危険です。ながらスマホ（歩きスマホ）により、自分が傷ついてしまうだけでなく、相手を傷つけてしまったり、死亡させてしまったりする事故が全国で起こっています。

また、スマートフォン等で通話をしたり、画面を見たりしながら自転車で走行することは法律で禁止されています。（安全運転義務違反となります）

※マナーを守って使いましょう

「公共の場所（図書館、映画館など）、公共の乗り物（電車、バスなど）で通話をしない。マナーモードにする。」「公共の場所で写真や動画を撮るときは他の人が写らないようにする。」「病院やバスなどの優先席の近くでは医療用の電気機器に影響を及ぼす可能性があるため、電源をオフにする。」など、マナーを守って使うことが大切です。

SNSやネットで知り合った人って、友だち？

事例 1

「実際に会おう」と言われて・・・

Aさんはつらいことがあり、SNSにつぶやきました。そのつぶやきに対して気持ちを楽にしてくれるメッセージを返してくれた人がいました。その後も、その人はいろいろな悩みの相談に乗ってくれました。

ある日、「実際に会おう」と言われ、会う約束をしました。

この後、どんな危険があると思いますか。

事例 2

写真を送ってと言われて・・・

BさんはSNSをとおして好きなアイドルのファンで同じ年齢の高校生と知り合いになりました。何度かやりとりをしていると、やりとりがはずみ、とても仲良しになりました。

ある日、高校生の写真が送られてきました。「Bさんの写真も送って」と言われ、自分の写真を送りました。

この後、どんな危険があると思いますか。

ポイント

匿名でのやりとりは、家族や友だちに話せないことも話題にできてしまいます。また、共通の趣味があるとやりとりがとても盛り上がります。

しかし、SNS上だけで優しいふりもできます。また、同じ趣味を装い、話を合わせることもできます。

⇒とても仲良くなったと錯覚してしまうことがあります。

文字のやりとりだけで相手を信用してしまうのは危険です。

⇒実際に会う約束をしたり、個人情報や写真等を送ったりしてしまうことがあります。

危険なことに巻き込まれたり、個人情報が流出したりしてしまいます。

SNSを通してやりとりをしている相手は、顔が見えないため、実際の友だちや家族に言えないことも相談したり、悩みを話したりしやすくなります。また、優しい言葉をかけられたり、趣味が合ったりすると、自分のことを理解してくれると思ってしまい、相手のことをいろいろ知りたくなってくるかもしれません。

SNSによるコミュニケーションは「会って話す」「電話で話す」と同じ感覚かもしれませんが、相手の顔や声、本当に優しい人かどうか、送ってきた写真が本物かどうか、など確認できません。「自分の写真を送ってしまい、公開されてしまった」ばかりではなく、実際に会う約束をして、生命に関わる犯罪に巻き込まれるといった危険な事例も起きています。

※以下のようなことに気をつけましょう

- **SNS等インターネット上で知り合った人を簡単に信用しない。**
  （名前、年齢や性別などを確認できない。）
- **絶対に実際に会わない。**
- **自分の写真や個人情報を送らない。（他人の写真や個人情報も）**
- **困ったときはすぐに家族や先生、同じ学校の友だちに相談する。**
- **周囲に相談できる人がいないときは、警察や専門の窓口に相談する。**

ネット上で知り合った人とやりとりをするときに、どんなことに気をつければよいか、家族や友だちと話し合ってみましょう。

このシートの使い方

生徒の皆さんへ

このシートは、電子メディア機器（テレビ、スマートフォン、パソコン、ゲーム機、音楽プレーヤーなど）との上手な付き合い方を学校や家庭で学習できるようにつくりました。このシートを利用して、自分の電子メディア機器の使い方を振り返ったり、友だち同士や家庭で話し合ったりできるようになっています。

保護者の皆さんへ

近年、インターネット環境の急速な発達により、スマートフォン等電子メディア機器は生活の中でなくてはならないものとなり、子どもたちの生活の中にも浸透しています。子どもたちにとって、親しみやすく、便利で楽しいものとなっている反面、友人関係のトラブルや生活習慣の乱れなどが深刻化していることから、上手につきあっていくことが求められています。利用に際してトラブルに巻き込まれないよう、このシートを作成しました。子どもたちが「自分で考え」、家庭や友だちと「話し合う」構成になっています。

なお、このシートは、電子メディア機器の購入を推奨するものではありません。

学校では

このシートは学校や生徒の実態に合わせて、学校での学習（道徳や学級活動などの情報モラルに関する学習やまとめ、ショートホームルーム等）や家庭学習（週末や長期休業での宿題等）で利用できる構成にしています。また、家庭で話し合われたことを学校でまとめていただき、学級・学年通信、保護者懇談等で活用していただくことも目的の一つとしています。各家庭で話し合われた様子を、保護者の皆さんが情報共有し、家庭でのルールづくりに生かせるように、活用をよろしくお願いします。

困ったときの相談窓口

もしものときや、困ったときは、一人で悩まず、相談しましょう。
親身になって話を聞いてくれます。

インターネットを利用した犯罪にあったら

〔鳥取県警察本部〕
【警察相談専用電話】**#9110**（通常の通話料がかかります。IP電話不可）
0857-27-9110
【サイバー犯罪対策室】**0857-23-0110**（代表）
【電子メール】**k_haiteku@pref.tottori.lg.jp**

架空請求に悩んだり、請求の内容に疑問を感じたら

〔消費者ホットライン〕**188**（局番なし）
〔鳥取県消費生活センター〕
【東部消費生活相談室】**0857-26-7605**（県庁第２庁舎２階）
【中部消費生活相談室】**0858-22-3000**（倉吉交流プラザ２階）
【西部消費生活相談室】**0859-34-2648**（米子コンベンションセンター４階）

ネットいじめに悩んだら

〔相談電話・メール〕
【子どもの相談ダイヤル】**0120-0-78310**（無料・毎日 24時間）
【いじめ相談メール】**ijime@kyoiku-c.torikyo.ed.jp**
【いじめ 110番】**0857-28-8718**（毎日 24時間）
【子どもの人権 110番】**0120-007-110**（平日のみ 8:30 ～ 17:15）（無料・IP電話不可）

「メディア21:00」運動

21時以降は友だちを巻き込むようなLINE（ライン）などのコミュニケーションツールやゲームをやめて相手の時間を尊重しようという運動です。鳥取県PTA協議会が提唱し、様々な団体が賛同し、運動を進めています。生活習慣をくずさないようにするためにも「メディア21:00」運動に取り組みましょう。

※電子メディア機器の利用や購入を推奨するものではありません。

電子メディアとうまくつきあおう

鳥取県の児童・生徒のみなさんへ

スマートフォンやゲーム機、音楽プレーヤーなどでインターネットを使っていると、便利なことや楽しいことがあります。しかし、使い方を間違えると困ったことや怖いことに巻き込まれることがあります。また、進学や就職、結婚などの将来に影響し、後悔する人もいます。

ですから、使う場合には必ず次のことを守りましょう。

スマートフォンやゲーム機、音楽プレーヤーなどを使う場合には、必ず

- 家の人と話し合ってルールを作ろう
- 自分も他の人も傷つけない使い方をしよう
- 夜９時以降は友だちを巻き込むような通信をやめよう

あなたを守るために知っておこうインターネットの４つの特性

1. 一度載せた文章や写真は **世界中に公開されます**
2. 一度載せてしまったら **全てを取り消すことはできません**
3. 名前を隠して発信しても **誰が発信したか必ず分かります**
4. インターネット上でのトラブルが **進学や就職に影響し、後悔する人もいます**

安全に使うためにチェック

- ☑ 顔写真や学校名、連絡先などの個人情報は自分のものも友だちのものも載せない。
- ☑ インターネットでは嘘をついて近づいてくる人もいるので、インターネット上で知り合った人には相談や打ち明け話をしない。会わない。
- ☑ メールなどインターネット上でのやりとりは気持ちが伝わりにくいので、相手のことを思いやる。
- ☑ 困ったことがあったら、すぐに周りの大人に相談する。

鳥取県ケータイ・インターネット教育啓発推進協議会
事務局：鳥取県教育委員会　社会教育課　〒680-8570 鳥取市東町１丁目271番地
TEL 0857-26-7943　FAX 0857-26-8175　E-mail shakaikyouiku@pref.tottori.lg.jp

保護者のみなさんへ

近年、スマートフォンやゲーム機、音楽プレーヤーなどインターネットに接続できる通信機器（インターネット端末）が広く普及し、その利用の低年齢化が進んでいます。平成 27 年度に鳥取県教育委員会が実施したアンケート調査の結果でも、鳥取県の多くの小中学生がインターネット端末を利用していることが分かりました。また、利用に伴い、トラブルに巻き込まれる子どもたちも増えています。

インターネット端末の利用率

小6 80.9%　中2 86.2%　高2 96.2%

利用している子どものうちトラブルを経験したことがある

小6 13.3%　中2 28.4%　高2 38.4%

主な内容
- 睡眠不足
- 知らない人から連絡が来た
- 人間関係のトラブル
- メール等が気になり手放せない など

（H27 鳥取県教育委員会「インターネットの利用に関するアンケート」結果より）

＜インターネットにつながる機器＞

パソコン　スマートフォン　タブレット　ゲーム機　音楽プレーヤー　すえ置き型ゲーム機　テレビ

これからインターネット端末を持たせることをお考えの場合

インターネット端末を持たせないことも選択の一つです。
学校生活には必要ありません。

インターネット端末の利用で、大きなトラブルに巻き込まれる事例が増えています。

ゲーム依存・ネット依存

ひどい場合には昼夜逆転して、健康を害したり、学校に行けなくなったりする「ゲーム依存症・ネット依存症」が増えています。

動画・画像の投稿

面白半分で投稿した動画・画像が、大きなニュースになったり、多くの人に迷惑をかけたりすることがあります。また、一度載せるとどこかに残るため、進学や就職、結婚などの将来に影を落とすこともあります。

個人情報の流出

SNS やブログ・プロフなどに個人情報を載せると悪用される可能性があります。また、知らない人との ID 交換でトラブルにあうケースが増えています。

ながら操作

歩きながらの使用は、周囲の変化に気づかず、つまづいて転倒したり、人にぶつかりケガをさせたりすることもあります。

中傷・悪口

SNS やブログへの書き込みによって、人を傷つけることがあります。

メール等でのトラブル

メール等は短い文章が多いため、誤解も生じやすく、友だち関係が壊れ、いじめにつながるケースもあります。

不当請求

有害サイトやアプリからの架空請求や、詐欺に巻き込まれる被害が増えています。

既にスマートフォン等インターネット端末を使わせている場合

責任を持って家庭のルールを守らせましょう。

使わせるのであれば、子どもと一緒に使用ルールを考えましょう。また、守れなかった時のルールも決めておきましょう。

保護者と子どもとの間には、ルールに関する認識に違いがあります

「家庭で何らかのルールがある」と回答した児童・生徒と保護者の割合の比較

子どもの成長に応じたフィルタリング・機能制限を設定しましょう。

ゲーム機、音楽プレーヤー、スマートフォン、携帯電話などを持たせる（使わせる）前には、「フィルタリング」や「ウイルス対策」などの対応が必要です！！

犯罪の被害に遭った青少年のうち、９割以上がフィルタリング未加入です。

1 電話回線のフィルタリング（スマートフォン、携帯電話など）

電話回線（３G、４G、ＬＴＥ）からのインターネット接続に対するフィルタリングが購入時に設定されているか確認してください。

2 Ｗｉ－Ｆｉ回線のフィルタリング（ゲーム機、音楽プレーヤー、スマートフォンなど）

無線 LAN 回線（Wi-Fi など）からインターネットに接続することができるため、無線 LAN 回線に対するフィルタリングも必要です。

3 アプリケーションへの対策（ゲーム機、音楽プレーヤー、スマートフォンなど）

有害なアプリケーションや子どもたちにふさわしくないアプリケーションのダウンロードを防ぐなどの対策が必要です。

4 ウイルス対策ソフトの導入（ゲーム機、音楽プレーヤー、スマートフォンなど）

パソコン同様コンピュータウイルスに感染する危険性があるのでウイルス対策ソフトの導入が必要です。

Android のフィルタリングについてはこちら

- docomo https://www.nttdocomo.co.jp/service/filtering/index.html
- KDDI http://csmovie.kddi.com/app-service.html?cat_id=MTg=&pid=6
- SoftBank http://www.softbank.jp/corp/csr/internet/instance_01/

ゲーム機等にはペアレンタルコントロール(※)の機能があり、使用制限を設定することができます。

（※ペアレンタルコントロールとは、青少年のインターネットの利用を管理するために保護者が行うべき措置のこと。）

鳥取県民チャンネルコンテンツ協議会の動画コンテンツで設定方法を見ることができます。

下記 QR コードから使用制限の設定方法をご覧いただけます

iOS、ニンテンドー 3DS、Playstation Vita についてはこちら

http://www.tottorikenmin-ch.com/contents/index.html

- ○ゲームソフトの使用制限（年齢制限…レーティング）
- ○インターネットの閲覧権限
- ○コミュニケーション制限（見知らぬ人との出会いを防ぐ）
- ○クレジットカードの利用制限

…> よくわからない時はこのリーフレットを持って販売店にご相談ください。

夜９時以降は通信をやめさせましょう。

鳥取県 PTA 協議会が提唱した「メディア 21:00」運動を全県の共通ルールとして、各家庭や地域で児童･生徒が安心･安全にインターネットを利用できる環境づくりを進めていきましょう。

「メディア 21:00」運動とは…

鳥取県の子どもたちは、21 時以降は友だちを巻き込むような LINE などのコミュニケーションツールやゲームの利用をやめて、相手の時間を尊重しようという運動。

保護者自身が必要な知識を身につけましょう。

学校や地域で開催される研修会へ参加し、スマートフォン等インターネット端末の機能や子どもの使い方・使っているアプリ、困ったときの相談先などについてしっかりと知っておきましょう。

我が家のルール

使用時間
夜〔　　〕時までには使用をやめます
１日の使用は〔　　〕時間以内にします

使用内容
個人情報や悪口は書き込みません
フィルタリングをはずしません

使用場所
必ず〔　　〕で使用します（自分の部屋では使用しません）

利用料金
利用明細で確認します

困ったときは…
すぐに先生か保護者に相談します

ルールを守れなかったときは…
〔　　〕日間使用禁止、保護者に返却するなど

我が家の特別ルール
〔　　〕

★約束した日　　年　　月　　日　署名

ルール作り、フィルタリング等のことをもっと勉強したいという保護者・地域の皆さんに･･･
研修会、親子学習会等に講師としてケータイ・インターネット教育推進員を無料派遣します

専用申込フォーム

申込先 特定非営利活動法人こども未来ネットワーク（県委託）TEL 0858-22-1960 FAX 0858-27-0271
Email media@kodomomirai.kirara.st URL http://www.pref.tottori.lg.jp/67797.htm

困ったときの相談窓口

もしものときや、困ったときは、一人で悩まず、相談しましょう。

インターネットを利用した犯罪にあったら

〔鳥取県警察本部〕
【警察相談専用電話】**#9110**（通常の通話料がかかります。IP電話不可）
0857-27-9110
【サイバー犯罪対策室】**0857-23-0110**（代表）
【電子メール】**k_haiteku@pref.tottori.lg.jp**

架空請求に悩んだり、請求の内容に疑問を感じたら

〔消費者ホットライン〕**188**（局番なし）
〔鳥取県消費生活センター〕
【東部消費生活相談室】**0857-26-7605**（県庁第２庁舎２階）
【中部消費生活相談室】**0858-22-3000**（倉吉交流プラザ２階）
【西部消費生活相談室】**0859-34-2648**（米子コンベンションセンター４階）

ネットいじめに悩んだら

〔相談電話・メール〕
【子どもの相談ダイヤル】**0120-0-78310**（無料・毎日 24時間）
【いじめ相談メール】**ijime@kyoiku-c.torikyo.ed.jp**
【いじめ 110番】**0857-28-8718**（毎日 24時間）
【子どもの人権 110番】**0120-007-110**（平日のみ 8:30 ～ 17:15）（無料・IP電話不可）

H29.3 現在

電子メディアと うまくつきあおう

鳥取県の高校生のみなさんへ

インターネットを利用したＳＮＳやメールには、便利なことや楽しいことがあります。
しかし、使い方を間違えて友だちとトラブルになったり、恐ろしい事件に巻き込まれたりすることがあります。また、進学や就職、結婚などの将来に影響し、後悔する人もいます。
ですから、インターネットの特徴を十分理解して、適切に使いましょう。

あなたを守るために知っておこう～インターネットの４つの特性

1. 一度載せた文章や写真は **世界中に公開されます**
2. 一度載せてしまったら **全てを取り消すことはできません**
3. 名前を隠して発信しても **誰が発信したか必ず分かります**
4. インターネット上での軽はずみな書き込み･投稿が **進学や就職、結婚などの将来に影響し、後悔する人もいます**

安全に使うために必ず守ろう！

- ☑ 顔写真や学校名、連絡先などの個人情報は自分のものも友だちのものも載せない。
- ☑ インターネットでは嘘をついて近づいてくる人もいるので、インターネット上で知り合った人には相談や打ち明け話をしない。会わない。
- ☑ メールなどインターネット上でのやりとりは気持ちが伝わりにくいので、相手のことを思いやる。
- ☑ 困ったことがあったら、すぐに周りの大人に相談する。

鳥取県ケータイ・インターネット教育啓発推進協議会
事務局：鳥取県教育委員会　社会教育課　〒680-8570 鳥取市東町１丁目 271 番地
TEL 0857-26-7943　FAX 0857-26-8175　E-mail shakaikyouiku@pref.tottori.lg.jp

スマートフォンやゲーム機、音楽プレーヤーなどを使う場合には

- 家の人と話し合ってルールを作ろう
- 自分も他の人も傷つけない使い方をしよう
- 夜９時以降は友だちを巻き込むような通信をやめよう

家族や友だちとスマートフォンの使い方のルールを話し合ってみましょう

家族と話し合いたいポイント

- ☑ 本当に必要なのか、利用目的はなにか
- ☑ フィルタリングは外さない
- ☑ 使用する場所と時間を決める
- ☑ ルールを守れなかった時のルールを決める など

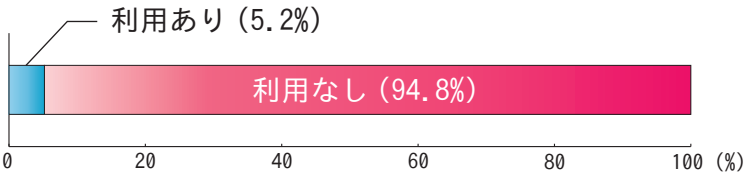
友だちと話し合いたいポイント

- ☑ メールなどの通信は○時まで
- ☑ ながらスマホはやめる
- ☑ 悪口を書き込まない
- ☑ 写真の投稿はしない など

フィルタリングしていますか？

犯罪の被害に遭った青少年のうち、９割以上がフィルタリング未加入です。

コミュニティサイトに起因する事犯の被害児童のフィルタリングの利用状況



警察庁広報資料「平成 27 年における出会い系サイト及びコミュニティサイトに起因する事犯の現状と対策について」より

Android のフィルタリングについてはこちら

- docomo https://www.nttdocomo.co.jp/service/filtering/index.html
- KDDI http://csmovie.kddi.com/app-service.html?cat_id=MTg=&pid=6
- SoftBank http://www.softbank.jp/corp/csr/internet/instance_01/

ゲーム機にはペアレンタルコントロール(※)の機能があり、使用制限を設定することができます。

（※ペアレンタルコントロールとは、青少年のインターネットの利用を管理するために保護者が行うべき措置のこと。）

鳥取県民チャンネルコンテンツ協議会の動画コンテンツで設定方法を見ることができます。

iOS、ニンテンドー 3DS、Playstation Vita についてはこちら

http://www.tottorikenmin-ch.com/contents/index.html

○ゲームソフトの使用制限（年齢制限…レーティング） ○インターネットの閲覧権限
○コミュニケーション制限（見知らぬ人との出会いを防ぐ） ○クレジットカードの利用制限

下記 QR コードから使用制限の設定方法をご覧いただけます

困ったときの相談窓口 もしものときや、困ったときは、一人で悩まず、相談しましょう。

インターネットを利用した犯罪にあったら

〔鳥取県警察本部〕
【警察相談専用電話】**#9110**（通常の通話料がかかります。IP 電話不可）
0857-27-9110
【サイバー犯罪対策室】**0857-23-0110**（代表）
【電子メール】**k_haiteku@pref.tottori.lg.jp**

架空請求に悩んだり、請求の内容に疑問を感じたら

〔消費者ホットライン〕**188**（いやや）（局番なし）
〔鳥取県消費生活センター〕
【東部消費生活相談室】**0857-26-7605**（県庁第２庁舎２階）
【中部消費生活相談室】**0858-22-3000**（倉吉交流プラザ２階）
【西部消費生活相談室】**0859-34-2648**（米子コンベンションセンター４階）

ネットいじめに悩んだら

〔相談電話・メール〕
【子どもの相談ダイヤル】**0120-0-78310**（なやみいおう）（無料・毎日 24 時間）
【いじめ相談メール】**ijime@kyoiku-c.torikyo.ed.jp**
【いじめ 110 番】**0857-28-8718**（毎日 24 時間）
【子どもの人権 110 番】**0120-007-110**（平日のみ 8:30 ～ 17:15）（無料・IP 電話不可）

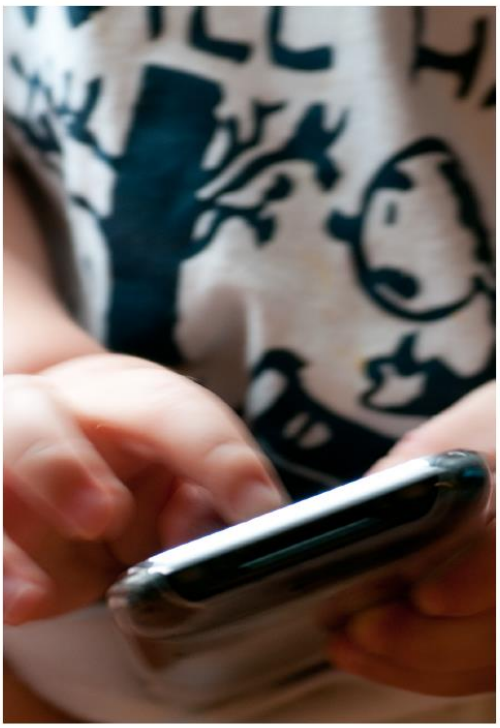
H29.3 現在

電子メディアが乳幼児期の子どもに及ぼす影響は…？

子どもたちは生まれながらにしてたくさんの電子メディアに囲まれて生活しています。電子メディアに子どもたちが触れる機会は、年々、早期化・長時間化の傾向にあります。
乳幼児期は、心とからだの基礎をつくる大切な時期です。電子メディアとの関わり方を振り返ってみましょう。

電子メディアが乳幼児に及ぼす影響は…？

電子メディアとの接触が多くなると、子どもたちが身体を動かす機会が減り、直接人と顔をあわせて遊ぶ時間も減ってしまいます。
また、生活リズムの乱れ、視力低下、依存症など体や心への影響も心配されます。電子メディアによって与えられる情報の質や、その影響を考える必要もあります。



乳幼児にテレビやＤＶＤを見せてはいけないのですか？

赤ちゃんは、音がする方、明るい方、動くものをじっと見つめます。テレビに見入る赤ちゃんを見て、集中していると思いがちですが、コミュニケーションの力を育むには、テレビ視聴のような一方通行ではなく、双方向のやりとりが欠かせません。
また、乳幼児期は視力が発達する重要な時期です。発達を妨げないために、長時間の視聴は控えましょう。

親のスマートフォンやタブレットなどを使いたがるのですが、使わせてもいいのでしょうか？

家庭内には、スマートフォンやタブレットなど子どもの興味を引く道具がたくさんありますが、それらはおもちゃではありません。代わりに、子どもの興味・関心を引くおもちゃを準備し、一緒に遊びましょう。また、スマートフォンなどを大人が使う場合には、子どもの前では使わない、子どもの手に届かないところに置くといった配慮も必要です。

電子メディアと子どもの育ち、乳幼児期のメディアとのよりよい接し方等のことをもっと勉強したいという保護者・子育て関係者の皆さんに…

専用申込フォーム

研修会等に講師としてケータイ・インターネット教育推進員を無料派遣します

申込先 特定非営利活動法人こども未来ネットワーク（県委託） TEL 0858-22-1960 FAX 0858-27-0271
Email media@kodomomirai.kirara.st URL http://www.kodomomirai.kirara.st/

家族で豊かな時間を過ごしましょう

乳幼児期は人格の基礎を培う大切な時期です。短い時間でも一緒に活動することで、体験や楽しさを共有しましょう。

外遊び、体験活動

子どもの体力・運動能力は子どもが体を動かし、自由に遊ぶことで育ちます。いろいろなことを体験することで、「見る」「聞く」「嗅ぐ」「味わう」「触れる」といった五感もバランスよく育ちます。
しっかり遊ぶとよく食べ、よく眠れるようになり、生活リズムも整います。

お手伝い

子どもの成長に応じて、できることをさせましょう。生活能力が養われるだけでなく、感謝を伝えられることで「役に立った」「責任を果たした」という自信が育まれ、自分を大切にする心（自己肯定感）が高まります。

読み聞かせ

子どもたちは、大人に繰り返し絵本を読んでもらい、一緒に楽しむことによってお話の楽しさや愛情を感じています。
親にとっても、子どものすてきな表情を通して、子育ての楽しさを感じることができます。

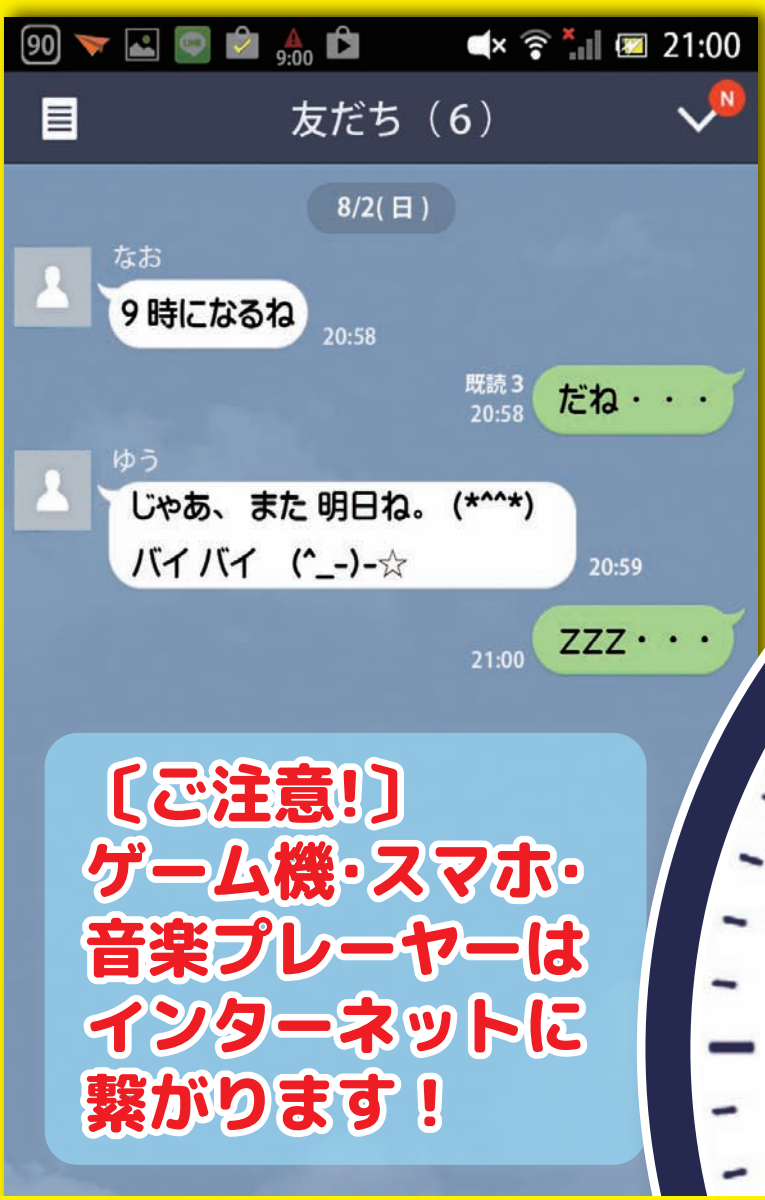
地域行事

地域で様々な年齢の方とふれあう時間から、社会性などたくさんのことを学びます。また、人とふれあうことで、コミュニケーション能力や共感力も育っていきます。保護者の方も一緒に地域行事に参加しましょう。

鳥取県教育委員会社会教育課　TEL 0857-26-7943　FAX 0857-26-8175
鳥取県子どものインターネット利用教育啓発推進協議会　E-mail shakaikyouiku@pref.tottori.lg.jp

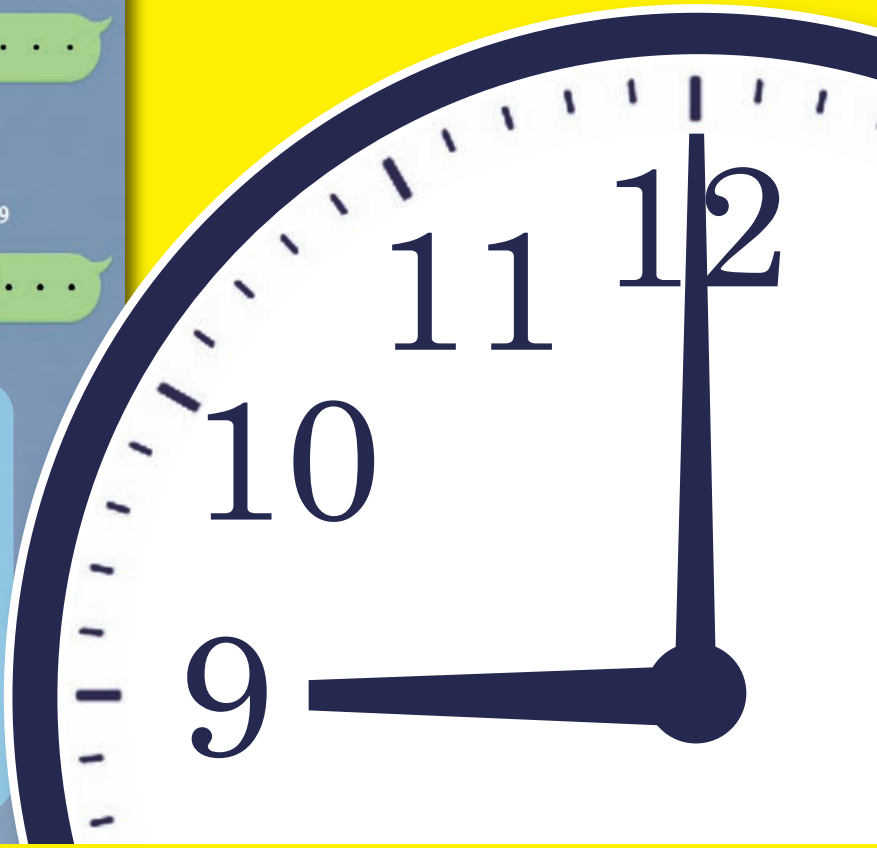
みんなですすめよう！
「メディア21:00（ニジュウイチ）」運動

**21時以降は友だちを巻き込むような
LINE（ライン）やメール、ゲームを
止めて相手の時間を尊重しましょう。**



「我が家のルール」

子どもと話し合って、インターネットやゲームの利用ルールを作りましょう。ケータイやスマホを持たせないことも選択肢のひとつです。



※ケータイやスマホ等の保持を推奨するものではありません。

【提 唱】鳥取県ＰＴＡ協議会

【賛　同】鳥取県教育委員会、多くの市町村教育委員会、PTA団体、各校種校長会、青少年育成鳥取県民会議、公益法人鳥取県医師会など関係団体の皆様に御賛同をいただいております。

【発行元　鳥取県PTA協議会】

ゲーム･インターネットと いい関係を作ってますか？

親子でよく話し合い、ルール作りをしましょう

話し合いたいルールの例

- □１日に使う時間を決める
- □使う場所を決める
- □困ったことがあったら、すぐ家の人に言う
- □ルールを守れなかった時の決まりを決める　など

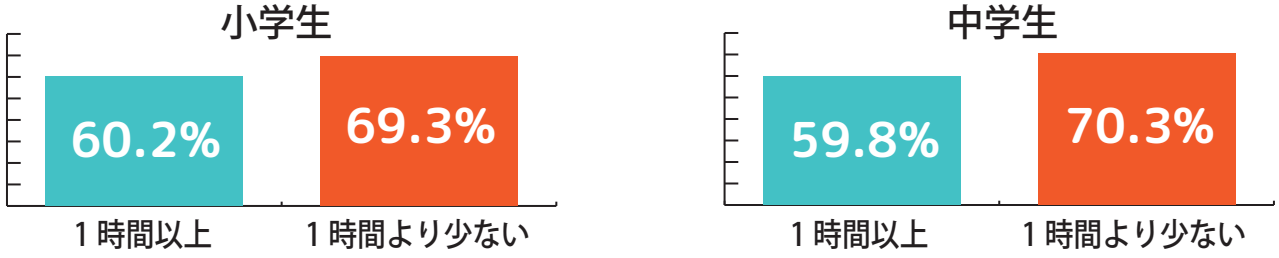
インターネットを長時間使うと、学習効果が失われてしまうという研究結果もあります。

電子メディアの使用と学力の関係

テレビゲーム等の電子メディアに触れる時間が短い児童・生徒のほうが、２教科平均正答率が高い傾向が見られます。

普段（月～金）１日どれくらいの時間、テレビゲーム（コンピュータゲーム、携帯式のゲーム、携帯電話やスマートフォンを使ったゲームも含む）をしますか（平成 28 年度全国学力・学習状況調査より）

鳥取県における２教科（国語、算数（数学））平均正答率



長時間利用のため睡眠不足で困っている児童･生徒が増えています。

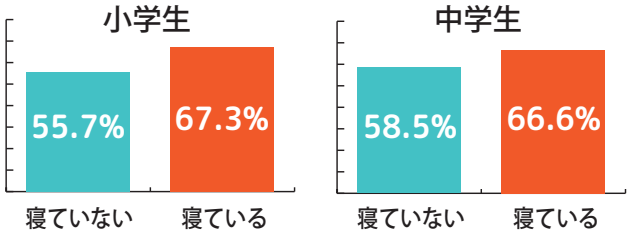
（「平成 27 年度鳥取県インターネットの利用に関するアンケート」より）

基本的生活習慣と学力の関係（平成 28 年度全国学力・学習状況調査より）

決まった時間に寝起きしたり、毎日朝食を食べたりしている児童・生徒のほうが、２教科平均正答率が高い傾向が見られます。

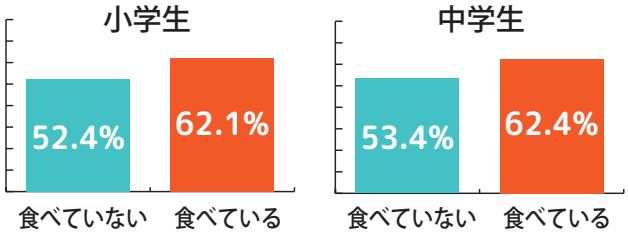
毎日同じぐらいの時刻に寝ている

鳥取県における２教科（国語、算数（数学））平均正答率



朝食を毎日食べている

鳥取県における２教科（国語、算数（数学））平均正答率



基本的生活習慣をくずさないようにするために「メディア 21:00」に取り組みましょう

今すぐ始めよう!!
ペアレンタルコントロール

～インターネットを安全に利用するために～

鳥取県青少年健全育成条例が改正されました。

主な改正内容

◆保護者の方々へ、インターネットの利用について、青少年の年齢等に応じ、ペアレンタルコントロール等の措置を行うよう努力義務を追加しました。

◆販売事業者の方々へ、インターネットが利用出来る機器を販売する際にはペアレンタルコントロール等の説明と書面の交付の義務を追加しました。

平成 26 年 10 月 1 日から施行されました

鳥　取　県

1 保護者は、ペアレンタルコントロール等で青少年のインターネット利用の管理を適切に行いましょう！！

最近のゲーム機や音楽プレーヤーは、Wi-Fi 通信を使ってインターネットに接続することが可能な製品が多くなっています。

青少年が安全に安心してインターネットを利用するためには、保護者自らがインターネットに関する知識や技術等の習得に努めることが大切です。青少年の年齢及びインターネットを適切に活用する能力に応じ、ペアレンタルコントロールを適切に行いましょう。

ペアレンタルコントロール
（青少年のインターネットの利用を管理するために保護者が行うべき措置）

①インターネットを利用できる時間及び場所を制限し、インターネットの利用状況を把握すること。
②保護者が同意した機能に限り、インターネットを利用できるようにすること。
③青少年有害情報フィルタリングソフトウェアを利用して、有害情報の閲覧や視聴を防止すること。
④そのほか、青少年のインターネットの利用を制御することができる措置。

子どもが安心して安全にインターネットを使うため、家庭のルールを子どもと一緒に作りましょう！

★子どもたちがこんな使い方をしていませんか？

◆**保護者の目の届かない場所（コンビニや公共施設など）での無線 LAN回線の利用**

◆**歩きスマホやながら操作**（大怪我をしたり怪我をおわせたりする事故に繋がります。）

◆**保護者のスマートフォンを使って、保護者のクレジットカードでオンラインゲームのアイテムを購入。**（少額でないアイテムもあり高額請求される場合があります。）

2 ゲーム機、音楽プレーヤー、スマートフォン、携帯電話を持たせる前には「フィルタリング」と「ウイルス対策」のペアでセキュリティ対策が必要です！！

① 電話回線のフィルタリング（スマートフォン、携帯電話 など）

電話回線（3G、4G、LTE）からのインターネット接続に対するフィルタリングが購入時に設定されているか確認してください。

※フィルタリング…違法・有害情報（犯罪、アダルト、薬物販売などのサイト）の閲覧を防ぐサービス

※フィルタリングの設定や安易な解除の禁止が、法律や条例で定められています。

② Wi-Fi 回線のフィルタリング（ゲーム機、音楽プレーヤー、スマートフォン など）

ゲーム機、音楽プレーヤー、スマートフォンは、無線 LAN 回線（Wi-Fi など）からインターネットに接続することができます。その場合は①のフィルタリングが適用されない場合があります。必ず無線 LAN 回線（Wi-Fi など）に有効なフィルタリングが必要です。

※機種ごとの設定方法は、このチラシの裏面にある QR コードでご確認ください。（専用の有料ソフトもあります。）

③ アプリケーションへの対策（ゲーム機、音楽プレーヤー、スマートフォン など）

ゲーム機、音楽プレーヤー、スマートフォンは、様々なアプリケーション（アプリ）をダウンロードすることができます。有害なアプリや青少年にふさわしくないアプリのダウンロードを防いだり、起動制限するアプリ用の対策が必要です。

④ ウイルス対策ソフト（ゲーム機、音楽プレーヤー、スマートフォン など）

ゲーム機、音楽プレーヤー、スマートフォンは、パソコン同様コンピューターウイルスに感染する危険性があります。最新のウイルス対策ソフトの導入が必要です。

「フィルタリング」と「ウイルス対策」のペアでセキュリティ対策を行いましょう。

ゲーム機や音楽プレーヤーは、通話機能がないスマートフォン。
子どもたちは保護者が知らないうちに、インターネットの世界へ入り込んでいます。

★ゲーム機にはペアレンタルコントロール機能があり、次の内容について使用制限を設定することができます。

○ゲームソフトの使用制限（年齢制限…レーティング）　○インターネットの閲覧制限
○クレジットカードの利用制限　○コミュニケーション制限（見知らぬ人との出会いを防ぐ）等が可能

3 インターネットに潜む危険性を知っておきましょう！

青少年にとって、携帯電話やスマートフォンは、インターネットを利用する上で便利なものです。加えて最近では、携帯ゲーム機や携帯音楽プレーヤーでもインターネットに接続が可能となっています。インターネットは、大変便利なものですが利用の仕方によっては、次のような危険性があります。

個人情報の流出

ソーシャルネットワーキングサービス（SNS）やブログなどに個人情報を載せると悪用される可能性があります。

写真など一度インターネットに流れた情報は拡散し取りもどすことは不可能です。

ケータイ・スマホ依存

ひどい場合には昼夜逆転して、健康を害したり、学校に行けないこともあります。

このような状態は「ケータイ・スマホ依存症」や「ケータイ・スマホ中毒」です。

ケータイ・スマホに振り回されてしまっては、自分の大切な時間がもったいないよ。

なりすましによる被害

インターネットでのやり取りは顔が見えません。性的な目的で、子どもや同年代の女子（男子）になりすまして近づく大人がいます。

ゲーム機からでも犯罪被害に遭うおそれがあります。

ワンクリック詐欺

有害サイトから架空請求や詐欺に巻き込まれることがあります。

相手にメールや電話で連絡をとることは危険です。支払う必要はないので無視しましょう。

中傷・悪口

SNS やブログへの何気ない書き込みが人を傷つけたり、乱闘などの事件につながることがあります。

誰が書いたか分からないだろう…×
実は書いた人は特定できるんです。

動画・画像の投稿

面白半分や何気ない動画・画像の投稿が、色々な人に迷惑をかけたり、騒動に発展することがあります。

どんな影響があるか投稿する前に考えましょう。

メールでのトラブル

メールは短い文章が多いため、誤解を生じやすく、友達関係がこわれたり、いじめに発展するケースもあります。

メールに頼らず、直接会って話をしましょう！

※この条例で青少年とは 18 歳未満の人（婚姻者は除く）のことです。

◎この条例に関するお問い合わせは…

鳥取県福祉保健部子育て王国推進局
青少年・家庭課
〒680-8570 鳥取市東町一丁目 220
電　　話　0857-26-7076
ファクシミリ　0857-26-7863
電子メール　seisyounen-katei@pref.tottori.jp
ＵＲＬ　http://www.pref.tottori.lg.jp/seishounen-katei/

セキュリティ対策できてますか？

ＯＳやアプリの
アップデートは？

インストール
するアプリは？

ＩＤ・パスワード
の設定は？

セキュリティ
対策アプリの導入は？

セキュリティ
ロックの設定は？

スマートフォンのセキュリティ対策のポイント

1　OSやアプリをアップデートする

アップデートしないまま放置していると、ウイルス感染の危険性が高くなります。スマートフォンのOS（基本ソフト）やアプリの脆弱性(セキュリティ上の弱点)が見つかれば、提供元から修正プログラムが配信されるので、必ずアップデートしましょう。

2　セキュリティ（パスコード）ロックを設定する

端末の画面にセキュリティ（パスコード）ロックを設定していないと、盗難・紛失などの際に大事なデータを悪用される危険性があります。端末を不正に操作されないよう、セキュリティ（パスコード）ロックを設定しましょう。

3　ID、パスワードを適切に設定する

ID、パスワードが悪意のある者に知られると、アカウントが乗っ取られるなどの危険性があります。ID、パスワードは、他人が容易に推測できるようなものは避け、適切に設定しましょう。

4　セキュリティ対策アプリを導入する

パソコンと同じようにスマートフォンもウイルスに感染する危険性があります。スマートフォンを狙ったウイルスも多数存在するため、セキュリティ対策アプリは必ず導入しましょう。

5　アプリは信頼できる場所からインストールする

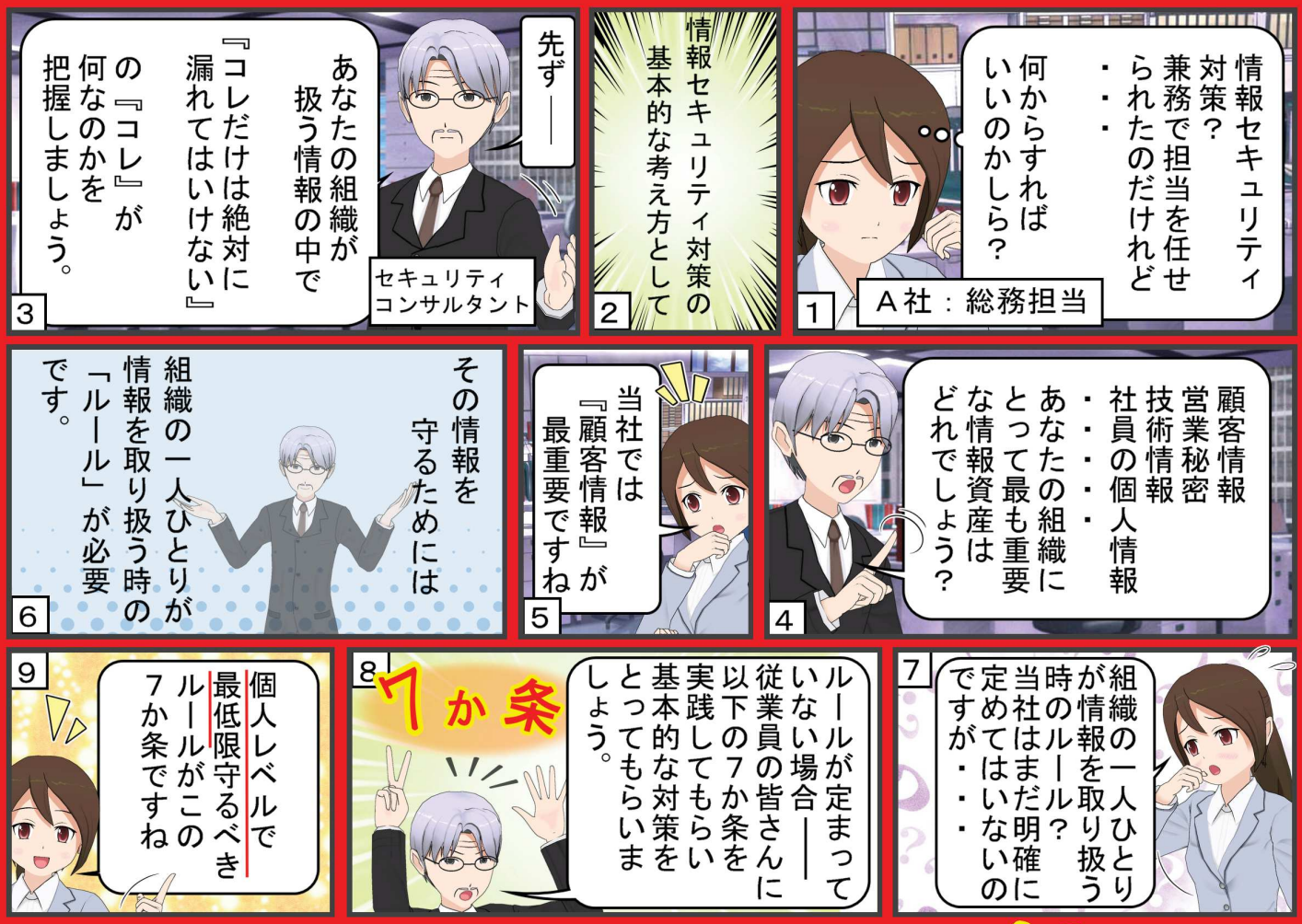
不正なアプリをインストールすると、端末がロックされてお金を要求される、マイクが勝手に起動して通話内容を盗聴されるなどの危険性があります。アプリは、公式マーケットなどの信頼できる場所からインストールしましょう。

**どれだけできているか
チェックしてみよう！**

【鳥取県警察ホームページ】http://www.pref.tottori.lg.jp/police/

鳥取県警察　検索　クリック

組織の一員としての情報セキュリティ対策



情報セキュリティ対策7か条

第 1　システムの更新を忘れず、最新に！

更新を放置しているとウイルスに感染してしまう危険性があるので、更新を忘れずパソコンのＯＳや各種のソフトを最新・安全な状態に保ちましょう。不明な点があれば管理担当者へ確認しましょう。

第 2　ウイルス感染を予防しよう！

ファイルを勝手に暗号化したり、パソコンを乗っ取り、データを盗んだりするウイルスが増えています。ウイルス感染予防のためにウイルス対策ソフトを導入し最新の状態に保ちましょう。

第 3　パスワード設定は長く複雑に！

例）Azn#LbifD3%g

12文字程度で大文字･小文字･数字･記号を含めた長く複雑なパスワードに設定しましょう。
二段階認証を活用し、同じパスワードを複数のサイトで使いまわさないようにしましょう。

第 4　興味を引くメールなどにご用心！

添付ファイルやURLリンクをクリックする前に差出人やメールの内容をよく確認しましょう。業務に関係のある内容を装った偽物のメールや興味を引く内容のメールには用心しましょう。

第 5　異変を感じたら組織内で情報共有を！

不審なメールを受信するなどの異変を認知したら、組織内で情報共有し、被害を最小限に止めましょう。
受信した不審なメールを放置し、別の従業員がそのメールを開きウイルス感染する危険性があります。

第 6　大切なデータはバックアップをとろう！

ウイルス感染や故障のリスクは完全には回避できないと認識し、外付けハードディスクなどへのバックアップを定期的に施し、大切なデータを守りましょう。

第 7　どのような危険があるかを学ぼう！

情報セキュリティ関連サイトなどから、様々なセキュリティに関する事故・事例や犯罪手口などを学び、どのような危険があるかを把握しましょう。

鳥取県サイバーセキュリティ対策ネットワークウェブサイト
https://www.pref.tottori.lg.jp/270729.htm

鳥取県サイバーセキュリティ対策ネットワーク

インターネット、その使い方で大丈夫？

第14回 IPA「ひろげよう情報モラル・セキュリティコンクール」2018 優秀賞受賞作品

コンクール応援隊長
「まもるくん」

【標語部門】

生活安全部長賞

アイコンと
画面の向こうは
違う顔

鳥取西高等学校１年
大呂 夏希さん

サイバー犯罪対策課長賞

あなたの指で
発信しても
あなたの指では
消せない情報

鳥取西高等学校１年
田中 苑希さん

少年課長賞

同じだよ
文字も言葉も
責任を

鳥取西高等学校１年
黒田 澪さん

【ポスター部門】

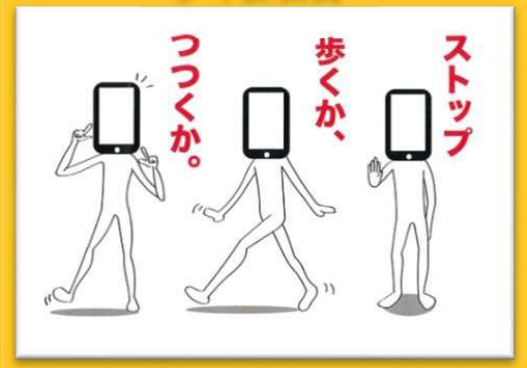
生活安全部長賞

鳥取湖陵高等学校３年
大西 桃夏さん

サイバー犯罪対策課長賞

米子市立福米中学校１年
桑本 美里さん

少年課長賞



鳥取湖陵高等学校３年
浦川 杏菜さん

サイバー犯罪に関する相談窓口（鳥取県警察本部）

- ●警察総合相談窓口　＃9110
- ●サイバー犯罪対策課　0857-23-0110（警察本部代表電話）
- ●電子メール　k_haiteku@pref.tottori.lg.jp
- ●サイバー犯罪対策課ウェブサイト
  https://www.pref.tottori.lg.jp/270444.htm