令和元年8月1日

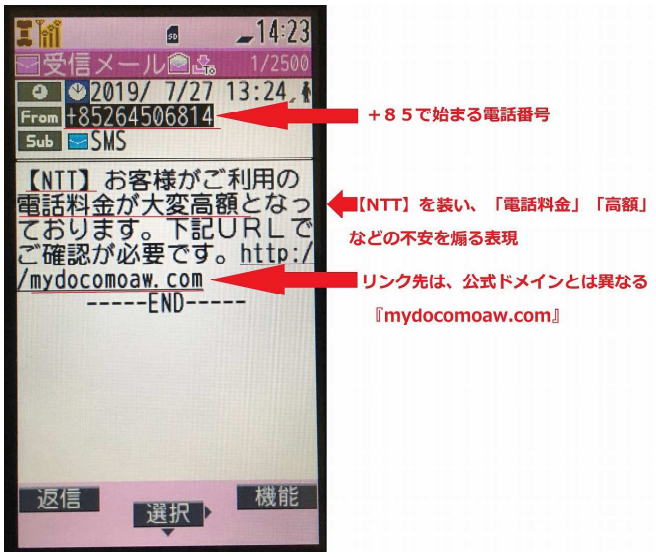
サイバーセキュリティ関連情報（８月号）

鳥取県警察本部サイバー犯罪対策課

○ NTTを装い「電話料金」「高額」などと不安を煽るSMSに注意！

NTTドコモやNTTからのお知らせを装い「高額な料金の発生」や「不正利用の検知」といったフィッシングSMSが届く事例が報告されており、同社では注意を呼びかけている。

送信元は、＋85で始まる電話番号のものが多く、本文にはフィッシングサイトへ繋がるリンク先が記載され、「ｄアカウント」のIDやパスワード、暗証番号、クレジットカード情報などを詐取しようとするケースが確認されている。



※　写真は、実際に当課員が受信したNTTを装う偽SMSの画面

NTTドコモを装った偽SMSについては、前回の７月号でもお伝えしたとおり、公式と同じ「NTT DOCOMO」の文字列を使用し同じスレッド上に表示される事例もあり、あわせて注意が必要です。

NTTドコモ公式サイト　https://www.nttdocomo.co.jp/info/notice/page/190725_01.html

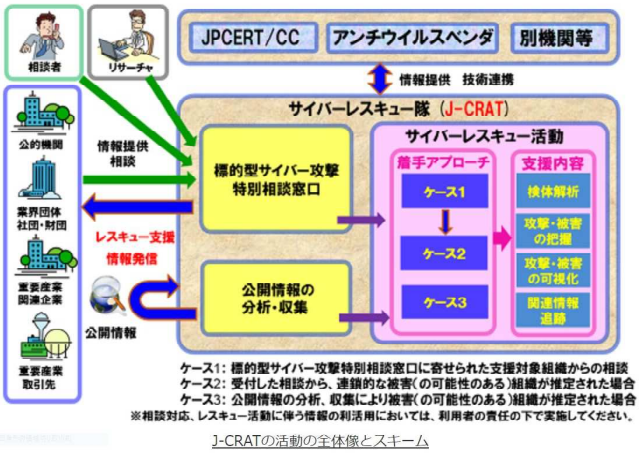
○ J-CRATへの2018年度下半期の標的型攻撃相談は258件

情報処理推進機構（IPA）が標的型攻撃の被害拡大防止に向けて、2014年7月に発足させ、支援活動を行っているサイバーレスキュー隊「J-CRAT」の「標的型サイバー攻撃特別相談窓口」に提供された状況を取りまとめた結果、2018年度下半期の標的型攻撃の相談は258件であり、155件だった2018年度上半期の約1.7倍に増加した。

そのうち、J-CRATのレスキュー支援の対象となったケースは93件で、34件だった2018年度上半期の約3倍近くに跳ね上がった。

標的型サイバー攻撃の侵入段階における手口として、引き続き標的型攻撃メールが用いられた他に、ネットワーク経由で侵入され攻撃活動が開始されたと推定される事例が複数の組織で確認された。

また、外部機関から連絡を受けたことを契機として、3年間以上の長期感染が確認される事例もあり、セキュリティソフトを導入し、OSやアプリケーションの最新化を行っていても検知されないバックドアや侵入ツールが仕掛けられるケースもあった。



J-CRATの活動の全体像とスキーム

引用　IPA　https://www.ipa.go.jp/security/J-CRAT/index.html