令和元年７月2日

サイバーセキュリティ関連情報（７月号）

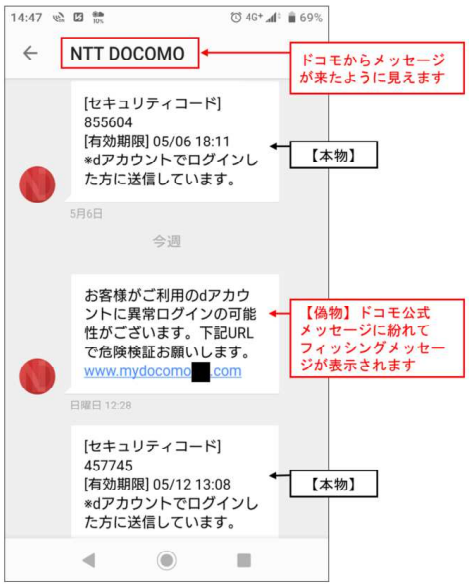
鳥取県警察本部サイバー犯罪対策課

○ NTTドコモを騙る偽ショートメッセージ（SMS）に注意！

本年6月21日、フィッシング対策協議会は、NTTドコモ公式のショートメッセージ（SMS）に紛れ込み、フィッシングサイトへ誘導するショートメッセージの報告を受けていることを発表した。NTTドコモ公式サイトでも、偽のSMSに記載のURLにアクセスすることで、dアカウントのID/パスワードやdカード情報などを詐取され、不正利用された被害が発生していることを公表しており、リンクにアクセスしないよう注意を呼び掛けている。

フィッシングSMSの送信元が、ドコモ公式SMSと全く同じとなっているため、同じスレッドに表示されるとのことで、利用者がフィッシングであると判断することが困難になっている。

被害にあわないためにリンクを開かず、万が一、アクセスしたとしても個人情報は絶対に入力しないで下さい。



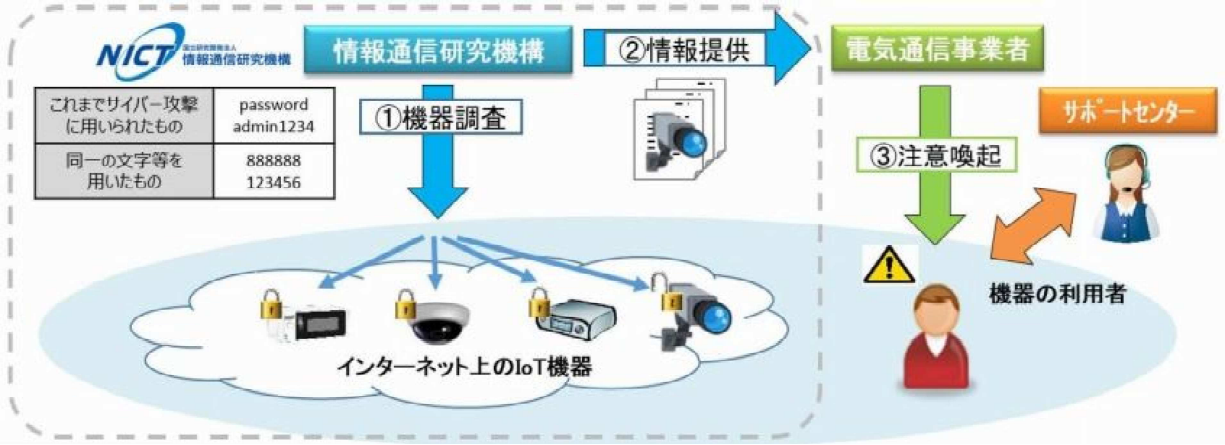
引用　フィッシング対策協議会　https://www.antiphishing.jp/news/alert/docomo_20190621.html
NTTドコモ公式サイト　https://www.nttdocomo.co.jp/info/spam_mail/column/20190617/

○ 「NOTICE」調査結果　注意喚起の対象は、延べ147件！

総務省及び情報通信研究機構（NICT）は、インターネットサービスプロバイダ（ISP）と連携し、本年2月20日から、サイバー攻撃に悪用されるおそれのある脆弱なIoT機器を調査し、注意喚起を行う取組「NOTICE」を実施しているところであるが、本年6月28日、その実施状況を発表した。

調査対象となったIPアドレスのうち、IDとパスワードが入力可能であったものは、約3万1,000件から約4万2,000件で、脆弱なIDとパスワードによりログインでき、注意喚起の対象となったものは、延べ147件であった。

現時点では容易に推測されるID・パスワードを設定している又は既にマルウェアに感染していると判明したIoT機器の数は少ない状況と考えられるものの、今後もマルウェアの感染活動は継続するとして、引き続き、適切なID・パスワードの設定やファームウェアの最新版へのアップデート等のセキュリティ対策の徹底に務めることが重要であると説明している。



引用　総務省　http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00033.html