

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

○ JC3がサイバー犯罪の手口を紹介する動画を公開！

日本サイバー犯罪対策センター（JC3）は、宅配便の不在通知を装うフィッシング攻撃やウェブサイト閲覧中に「マルウェアに感染した」「iPhoneが当選した」などと騙す詐欺の手口を紹介する動画を公開して被害にあわないよう注意を呼びかけています。

フィッシングサイトへ誘導するSMSの被害報告は、全国的に増加しており、動画では、実際のサイトへ誘導され、アプリのインストールを促される様子等が確認できます。スマートフォンによっては挙動が異なることから「iPhone」「Android」のそれぞれの動画が用意されているほか、偽の警告画面を表示して音声を流し、不安を煽るサポート詐欺の手口や商品の当選やプレゼントなどを装って個人情報などを詐取する手口など実際のサイトがどのように動作するかのを具体的に紹介しています。



フィッシング(iPhoneの場合)



サポート詐欺サイト



サイバー犯罪の手口を知っておくことは、被害の未然防止に繋がりますので、ぜひ、ご視聴の上、ご確認をお願いします。

参考：JC3 <https://www.jc3.or.jp/index.html>

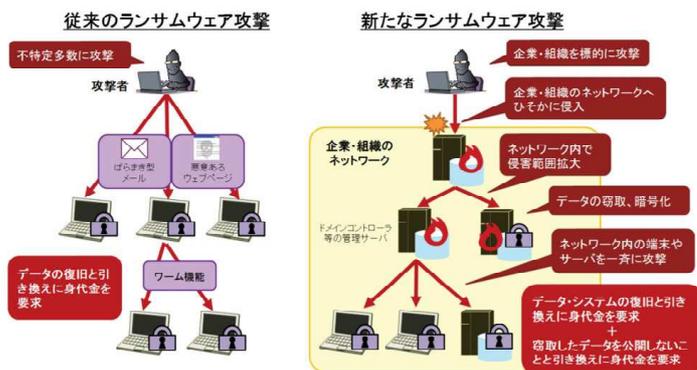
○ IPAが新たなランサムウェア攻撃について注意喚起！

独立行政法人情報処理推進機構（IPA）が「事業継続を脅かす新たなランサムウェア攻撃について」と題する注意喚起およびレポートを公開しました。

ランサムウェアとは、端末上のデータを暗号化するなどして、その復旧と引き換えに金銭を脅し取ろうとするコンピュータウイルスのことですが、レポートでは、近年、企業や組織の事業継続に関わる深刻な脅威として、「人手によるランサムウェア攻撃」と「二重の脅迫」の2つの攻撃方法が使用されていることを挙げ、その被害事例や攻撃手口、推奨される対策などについて詳しく解説しています。

新たなランサムウェア攻撃への対策として、最優先で維持する必要のあるデータ・システム等を見極め、着手できる部分からリスク低減のための多層的な防御策を講じる必要があります。加えて、コロナ禍におけるテレワーク拡大に伴うリモートデスクトップサービスの不用意な露出の停止やVPN（バーチャルプライベートネットワーク）装置の脆弱性の解消、また、データやシステムのバックアップを行うことも引き続き重要な対策であるとしています。ぜひ、レポートの内容をご確認の上、セキュリティ対策の徹底や

被害発生時における適切な対処のための事前体制整備をご検討下さい。



参考：IPA <https://www.ipa.go.jp/security/announce/2020-ransom.html>