2025 年 2 月 3 日
総務課　楢崎

サイバーセキュリティ月間 2025 について

皆さんお疲れ様です。総務課の楢崎です。日々の情報セキュリティ対策にご協力頂きありがとうございます。
さて皆さん、毎年この時期（２月１日～３月１８日）はサイバーセキュリティ月間となっています。

サイバーセキュリティ月間とは何ですか。という感じですが、このサイバーセキュリティ月間とは国が定めたもので、国民におけるセキュリティ意識の向上や理解促進を目的とした啓発活動になります。

今回はこのサイバーセキュリティ月間にちなんで情報セキュリティ 10 大脅威 2024 について紹介させて頂きたいと思います。

この情報セキュリティ 10 大脅威 2024 についてですが、これは 2023 年において社会的に影響が大きかったセキュリティ上の脅威について選考会投票で決まったものになります。（企業と個人で分けて選出されます。）
なお 2025 年版についてはもうちょっとしたら公開されます。（この月曜かいが掲載される頃には出てるはず）

こちらが情報セキュリティ 10 大脅威（個人）の結果になります。

情報セキュリティ 10 大脅威 2024 [個人]

「個人」向け脅威（五十音順）	初選出年	10 大脅威での取り扱い（2016 年以降）
インターネット上のサービスからの個人情報の窃取	2016 年	5 年連続 8 回目
インターネット上のサービスへの不正ログイン	2016 年	9 年連続 9 回目
クレジットカード情報の不正利用	2016 年	9 年連続 9 回目
スマホ決済の不正利用	2020 年	5 年連続 5 回目
偽警告によるインターネット詐欺	2020 年	5 年連続 5 回目
ネット上の誹謗・中傷・デマ	2016 年	9 年連続 9 回目
フィッシングによる個人情報等の詐取	2019 年	6 年連続 6 回目
不正アプリによるスマートフォン利用者への被害	2016 年	9 年連続 9 回目
メールや SMS 等を使った脅迫・詐欺の手口による金銭要求	2019 年	6 年連続 6 回目
ワンクリック請求等の不当請求による金銭被害	2016 年	2 年連続 4 回目

続いてこちらが組織向けのものになります。

情報セキュリティ 10 大脅威 2024 [組織]

順位	「組織」向け脅威	初選出年	10 大脅威での取り扱い（2016 年以降）
1	ランサムウェアによる被害	2016 年	9 年連続 9 回目
2	サプライチェーンの弱点を悪用した攻撃	2019 年	6 年連続 6 回目
3	内部不正による情報漏えい等の被害	2016 年	9 年連続 9 回目
4	標的型攻撃による機密情報の窃取	2016 年	9 年連続 9 回目
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022 年	3 年連続 3 回目
6	不注意による情報漏えい等の被害	2016 年	6 年連続 7 回目
7	脆弱性対策情報の公開に伴う悪用増加	2016 年	4 年連続 7 回目
8	ビジネスメール詐欺による金銭被害	2018 年	7 年連続 7 回目
9	テレワーク等のニューノーマルな働き方を狙った攻撃	2021 年	4 年連続 4 回目
10	犯罪のビジネス化（アンダーグラウンドサービス）	2017 年	2 年連続 4 回目

よくニュースなどで目にする項目が入っていたのではないでしょうか。

ちなみに企業向けには順位が入っていますが、別にこれは下位の項目は影響が少ないので後回しにしてもよいという訳ではないですので悪しからず。（個人向けにそもそも順位が入らず五十音順なのも同じ理由です）

今回は組織向けについてより詳しく見て行こうと思います。

上記のうちすべて紹介するとページがいくらあっても足りないので、順位 1 のランサムウェアについて紹介したいと思います。

ランサムウェアってよく聞きますが、

簡単にいうと見ず知らずの他人が自分のパソコンに侵入してきて、勝手に設定いじられて画面がロックされちゃって、解除して欲しければお金を払え！　をやるコンピューターウィルの一種です。

その上、お金を払ってくれないならパソコンの中のデータをばらまくぞ！と畳みかけてきます。

この感染が家のパソコンで起こった場合はそのパソコンだけの被害だけ（もちろん嫌ですが）ですみますが、会社のパソコンが感染すると、会社のパソコンはネットワークを介して他のパソコンやサーバーに繋がっているので、それらが感染しロックされてしまいます。

つまり、個人のパソコンだけでなく、Karp、パブリックサーバーなどなど様々なものが使えなくなってしまいます。（⇒めっきもできないし出荷もできなくなります）

じゃあその手口は

・脆弱性を悪用した手口

・メールや WEB サイトを悪用した手口　　の大きく分けて 2 つあります。

脆弱性を悪用した手口ですが、
これはソフトウェアの脆弱性を悪用し ウイルスを実行(感染させる)手口ですが、対策としては

1. OS やソフトウェアのアップデートを行い、修正プログラムやセキュリティパッチを適用する
2. サポートが終了したソフトウェアを使用しない

などが有効です。

メールや WEB サイトを悪用した手口については
不正な添付ファイルを開かせる 、メール内のリンクをクリックさせる、ランサムウェアをダウンロードさせるように改ざんした Web サイトへ誘導するなどがあります。

当社でも日々不信なメールは届いています。

メールアカウントが停止（メールが使えなくなる）されたら困ると思って、クリックしたくなりますが
よく見てください。
差出人メールアドレスのドメイン（@より後ろの文字：上記の赤丸部分参照）がおかしい（この場合は@kdp.biglobe.ne.jp）ですよね。
上記のように、やり取りしたことがないドメインや明らかにドメインが変な場合がありますが、パッと見て判断に迷うドメインで来る場合があります。例えば取引先の企業を語って送り付けられる場合に普段は “@会社名.co.jp”で来るのに、来たメールは “@会社名.com” だったなどがあります。

見分けるポイントは他にもありますが、
もし誤ってクリックするとダウンロードが始まったり、ID パスワードの入力を求められ入れてしまったりなど動いているのが分かる場合もありますが、クリックしても何もおこらなかった（よかったよかった）と思わせて実は中で勝手に動いている場合ありますので、
本文中の URL（もしくはここをクリックしてくださいの表示など）をクリックしてしまった場合には
すぐに有線 LAN、無線 LAN をオフにしてください。(もし方法が分からない場合は電波の届かないところまで逃げてください)
⇒その後各部署の情報セキュリティ担当へのご連絡をお願いします。

最後に、当社としましては今後もセキュリティ対策を強化し、業務を止めることがないようにして行きたいと考えておりますので、皆様のご協力をよろしくお願いします。