NET ASSIST
24/7 Guardian Deity

2023.3 #23

NEWS LETTER

TOPICS

＊ TOPICSの各タイトルをクリックすると該当の記事へ飛びます

#1 「情報セキュリティ10大脅威 2023」解説書「組織編」が公開!!

2023年1月25日にIPA（情報処理推進機構）より公開された「情報セキュリティ10大脅威　2023」ですが、2月28日に解説書「組織編」が公開されました。

※IPA（情報処理推進機構）「情報セキュリティ10大脅威 2023」解説書「組織編」 https://www.ipa.go.jp/files/000108838.pdf

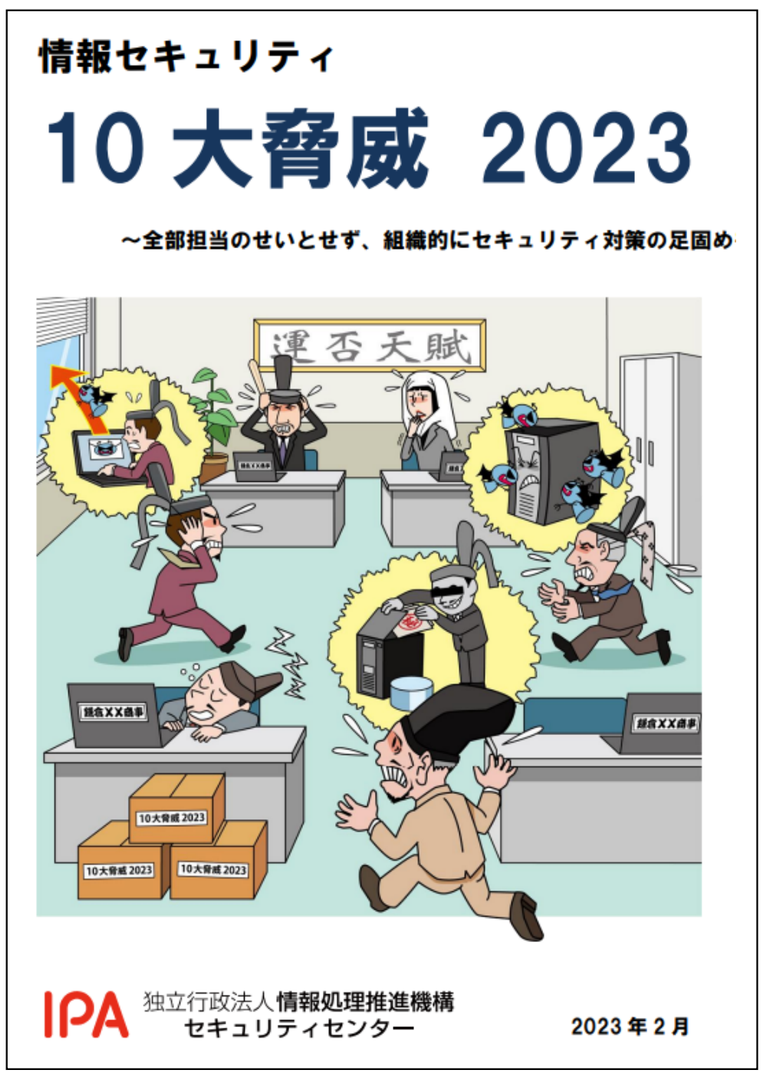


表1.1 情報セキュリティ10大脅威 2023「個人」および「組織」向けの脅威の順位

「個人」向け脅威	順位	「組織」向け脅威
フィッシングによる個人情報等の詐取	1	ランサムウェアによる被害
ネット上の誹謗・中傷・デマ	2	サプライチェーンの弱点を悪用した攻撃
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	3	標的型攻撃による機密情報の窃取
クレジットカード情報の不正利用	4	内部不正による情報漏えい
スマホ決済の不正利用	5	テレワーク等のニューノーマルな働き方を狙った攻撃
不正アプリによるスマートフォン利用者への被害	6	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
偽警告によるインターネット詐欺	7	ビジネスメール詐欺による金銭被害
インターネット上のサービスからの個人情報の窃取	8	脆弱性対策情報の公開に伴う悪用増加
インターネット上のサービスへの不正ログイン	9	不注意による情報漏えい等の被害
ワンクリック請求等の不当請求による金銭被害	10	犯罪のビジネス化（アンダーグラウンドサービス）

今回はその解説書「組織編」の中から、サーバーに関係のある脅威を抜粋してご紹介！
と、その前に、まず気になるのが本書の副題。
「～全部担当のせいとせず、組織的にセキュリティ対策の足固めを～」の部分です。
ことサイバー攻撃に関しては、「被害にあうわけない」「被害にあっても困らない」という意識が働きがちです。
ですが、自社サーバーの脆弱性を足掛かりとされ、関連企業や取引先企業が機密情報を窃取されてしまうなんてことも。。。
10大脅威による被害で共通しているのは、「組織の社会的信用の失墜」「損害賠償による経済的損失」です。
最悪の事態に陥ったときに、とても担当者単位で対処できる話ではないという点について、認識が促されています。
それでは10大脅威「組織編」を一部抜粋してですが、ご紹介して参ります！

1位：ランサムウェアによる被害

■概要

「ランサムウェア」と呼ばれるウイルスに感染させ、PC　やサーバーのデータを暗号化し、業務の継続を困難にした上で、データを復旧することと引き換えに、金銭を要求する手口です。
なお、金銭を支払ったとしても、データの復旧や漏えいした情報の削除が行われないことも。

■手口

・メールへのファイル添付や記載されたリンク先からの感染
・改ざんされたウェブサイトからDLしたことによる感染
・OSやソフトウェアの脆弱性を悪用したインターネット経由の感染

■事例

・中堅Sier：脆弱性をつかれランサムウェアを配置され、社内管理情報や顧客の情報などを窃取される

次ページへ

前ページより

2位：サプライチェーンの弱点を悪用した攻撃

■概要

商品の企画・開発から～調達～製造～在庫管理～物流～販売までの一連のプロセスに関わる組織群の中から、セキュリティ対策が脆弱な組織を最初の標的とし、そこを踏み台として顧客や本命の標的を攻撃する手口です。

■手口

・標的企業のシステム開発元やグループ企業等を攻撃の足掛かりとし、標的が保有する機密情報を狙う

■事例

・大手自動車メーカー：協力企業の子会社がサイバー攻撃被害後、国内全工場の操業が停止

6位：修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

■概要

OSやソフトウェアに脆弱性が存在することが判明し、脆弱性の修正プログラム（パッチ）や回避策がベンダーから提供される前に、その脆弱性を悪用してサイバー攻撃を行う手口です。これをゼロデイ攻撃といいます。

■手口

・ソフトウェアの脆弱性を悪用し各種攻撃を仕掛ける

■事例

・某国サイバー犯罪グループによるInternet Explorer へのゼロデイ攻撃
・Microsoft Exchange Server へのゼロデイ攻撃

8位：脆弱性対策情報の公開に伴う悪用増加

■概要

ゼロデイ攻撃がある一方で、攻撃者は公表されたての脆弱性情報を悪用し、対象製品への脆弱性対策を講じていないシステム（Nデイ脆弱性）を狙って攻撃を行います。近年では脆弱性関連情報の公開後に攻撃コードやツールがダークウェブ上に流通し、攻撃が本格化するまでの時間もますます短くなっています。

■手口

・対策前の脆弱性（Nデイ脆弱性）を悪用
・ダークウェブ上に公開されている攻撃ツールを使用

■事例

・Spring4Shell：PoC（proof of concept:脆弱性を実証するためのプログラム）公開済みの脆弱性を狙った攻撃

共　通　対　策

IPAは解説書「組織編」の中で、10大脅威についての共通対策にも言及しています。
ここでは紙面の関係上、詳細な解説は割愛いたしますが、ぜひリンクよりご一読ください。

①パスワードを適切に運用する

②情報リテラシー、モラルを向上させる

③メールの添付ファイル開封や、メール/SMS のリンク/URL を容易にクリックしない

④適切な報告/連絡/相談を行う

⑤インシデント体制を整備し、対応を行う

⑥サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う

⑦適切なバックアップ運用を行う

※対策の詳細は下記リンクの「情報セキュリティ10大脅威 2023」解説書「組織編」のP30～をご確認ください。
リンク：https://www.ipa.go.jp/files/000108838.pdf

**⑥については、解説の中で、弊社でも取り扱いのあるIDS/IPSやWAFといったセキュリティ製品の導入について言及されています。
気になった方は気軽にお問合せください。**

最 後 に

サイバー攻撃は世界的に増加しており、2022年には企業への攻撃数が2021年と比べて週平均38%増加しているとのデータもあります。犯罪がビジネス化され、より小規模かつ俊敏な犯罪集団が増えたことが増加の背景としてあるようです。

また、攻撃に対する専門知識が無い人でも、ダークウェブ上にあるサービスやツールを利用することで、容易に攻撃を行えるため、今後も攻撃は増加傾向が続く見込みです。

決して対岸の火事とはお考えにならずに、とれる対策を一つ一つ講じていきましょう。

#2 エンジニアコラム～今月注目した話題～

PICK UP!

■AmazonLinux2022→2023 に名称が変わりました

首を長くして待っていたAmazonLinux2022の続報ですが、2023年2月22日付で、AmazonLinux2023に名称が変わり、RC版（RC0）が公開されました。RC版はリリースの準備がほぼ整ったバージョンですが、まだ運用向けではなくテスト段階です。
AmazonLinux2のサポート期間が2025年6月まで延長されたこともあり、2025年以降の後継OSとしてRC版を試しておくのも良いかもしれません。

（AmazonLinux2023 リリースノート更新/3月8日）
https://docs.aws.amazon.com/ja_jp/linux/al2023/release-notes/relnotes-20230308.html

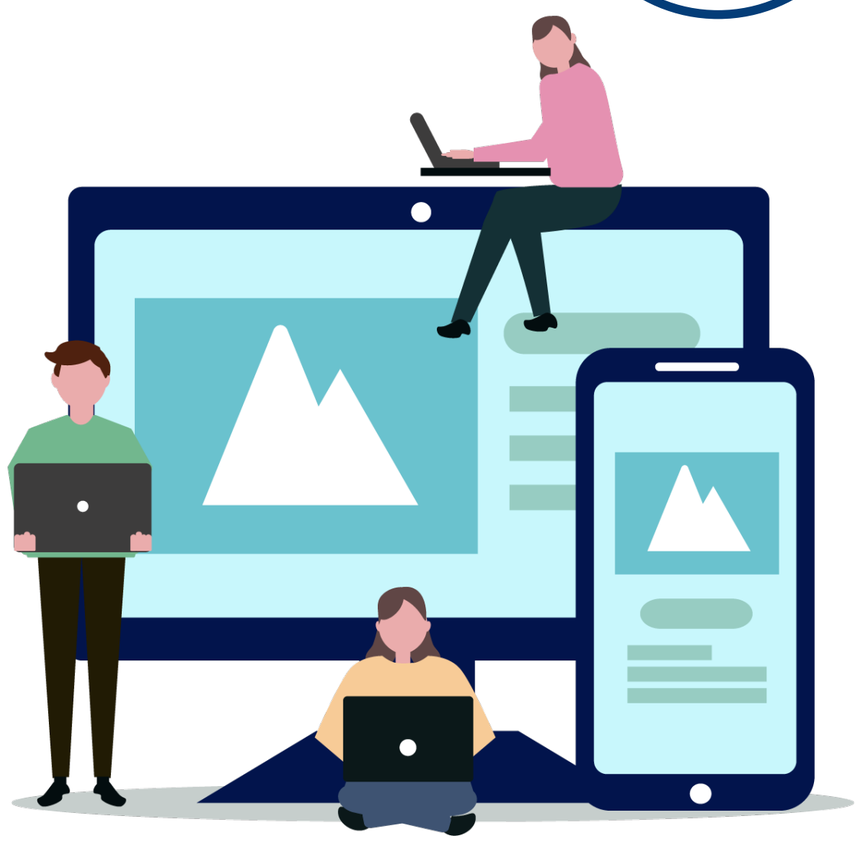
AmazonLinux2022の解説は過去のニュースレターで取り上げています。
よろしければこちらもご確認ください！
https://www.netassist.ne.jp/techblog/23937/

追記：3月16日に正式リリースされたとの情報が発表されました！

PICK UP!

■次世代の通信技術『IOWN（アイオン）』

3月2日、日本電信電話株式会社（NTT）が次世代の光通信『IOWN（アイオン）』を開発したことを発表しました。
今までの光回線だと「光回線は電気信号→光信号にし、光信号→電気信号にする」ことで通信していたのを、電気への変換なしに「直接光→光で通信させる」ことで、通信の遅延が大幅に減るようです。また、従来の回線では光を電気に変換する際に電力を消費し、熱も発生しますが、このエネルギーロスをなくすことができて省電力化も目指せるというメリットがあるそうです。
この『IOWN』は、2030年までの標準化を目指しています。
リモート技術がより発達する、電気の節約やCO2削減につながるなどの期待が高く、今注目しています。



NET ASSIST
24/7 Guardian Deity
株式会社 ネットアシスト

TEL 03-3985-6780
mail sales@netassist.ne.jp
web https://www.netassist.ne.jp