ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

## ●VMware ESXi等の脆弱性を突いてランサムウェアに感染させる攻撃活動に注意喚起

https://news.mynavi.jp/techplus/article/20230207-2584957/
https://www.jpcert.or.jp/newsflash/2023020601.html
https://blogs.vmware.com/security/2023/02/83330.html

### このニュースをザックリ言うと・・・

- 2月3日(現地時間)、フランスのCERT-FRより、VMWare社の仮想マシンソフトウェアの古いバージョンに存在する脆弱性を突き、ランサムウェア感染を仕掛ける攻撃活動「ESXiArgs」が確認されたとして注意喚起が出されています。

- 脆弱性(CVE-2021-21974)は2021年2月に「VMware ESXi」「VMware Cloud Foundation」等において報告され、VMWare社からセキュリティアップデートが提供されていたものです。

- ESXiに対するセキュリティアップデートはサポート対象のバージョン6.5系・6.7系・7.0系に対しリリースされていますが、それよりも前のバージョンにおいても攻撃対象となっているとの報告があるとのことです。

- 2月6日(日本時間)にはVMWare社やJPCERT/CCからも同様の注意喚起が出され、日本国内でもVMware ESXi等が稼働するサーバーが攻撃を受ける恐れがあるとして対策ないし回避策の適用を呼び掛けています。

### AUS便りからの所感等

- 仮想マシンソフトウェアは、一台のホストOS上で通常複数のゲストOSを稼働させる目的で導入されるもので、特にVMware ESXiは、WindowsやLinuxといったOS上ではなく、ホストサーバー上で直接稼働するものとなります。

- 脆弱性はESXiに含まれる一部のサービスに存在し、またホストマシンと同一のLAN上から攻撃を受ける恐れがあるとされ、別途社内ネットワークに侵入した攻撃者から悪用されるケースも考えられます。

- 多数のIoT機器がマルウェアMiraiに感染したのと同様、更新がされているかの確認が行き届いていない機器が相次いでターゲットにされる恐れがありますので、組織内でネットワークに繋がっている機器全てを洗い出し、特にサポート対象外の古いバージョンのESXi等は確実にバージョンアップを実施し、今後もセキュリティアップデートを確実に適用できる体制を整えるとともに、不要なサービスについてもできる限り無効化ないしアクセスの遮断を行うようUTM等も組み合わせた安全なネットワーク構成とすることを強く推奨致します。

TECH+ Powered by マイナビニュース

### VMware ESXi狙うランサムウェア攻撃に警告、JPCERT/CC-日本も標的の恐れ

掲載日 2023/02/07 08:45　　著者：後藤大地

JPCERTコーディネーションセンター(JPCERT/CC: Japan Computer Emergency Response Team Coordination Center)は2月6日、「VMware ESXiを標的としたランサムウェア攻撃について」において、VMware ESXiが稼働するサーバを標的としたランサムウェア攻撃キャンペーンが展開されていると伝えた。日本も標的になる恐れがあることから、注意が呼びかけられている。

サイバー攻撃キャンペーンに関する情報は次のページにまとまっている。

- Campagne d'exploitation d'une vulnérabilité affectant VMware ESXi – CERT-FR

## ●1月フィッシング報告件数は38,269件…1年半ぶりに4万件切る

https://automaton-media.com/articles/newsjp/20230121-234501/
https://twitter.com/itchio/status/1615507107545231360

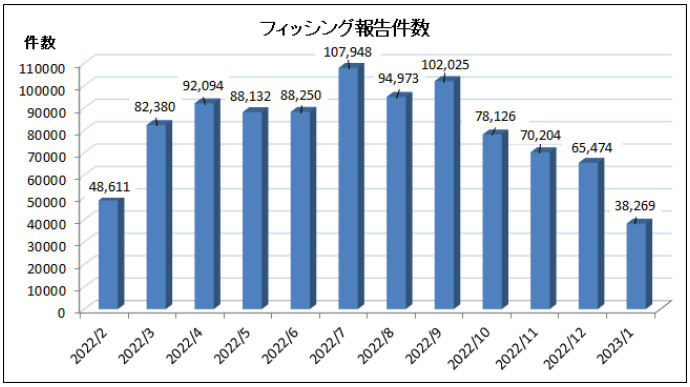
### このニュースをザックリ言うと・・・

- 2月6日(日本時間)、フィッシング対策協議会より、1月に寄せられたフィッシング報告状況が発表されました。
- 1月度の報告件数は38,269件で、12月度(https://www.antiphishing.jp/report/monthly/202212.html )の65,474件から27,205件減少しています。
- フィッシングサイトのURL件数も7,704件と、12月度(13,810件)から6,106件減少、フィッシングに悪用されたブランド数は76件で12月度(78件)から2件減少となっています。
- Amazonを騙るフィッシングは全体の約44.6%と割合は減少(12月度51.7%)、以下ETC利用照会サービス・セゾンカード・PayPayカードを騙るものと合わせて全体の約67.6%を占めたとのことです。

### AUS便りからの所感

- 2022年は3~9月度にかけて月間報告件数が8万件を超える状態が続きましたが、以降は右肩下がりが続き、今回で2021年7月度以来1年半ぶりに4万件を切っています。
- フィッシングメール・サイトの傾向としては、短縮URLやDDNSサービスを悪用するものの報告が全体の約41.1%となった他、QRコードを用いてフィッシングサイトに誘導しようとするものが1,000件以上報告されているとのことです。
- また、フィッシング報告が急増した2020年以降、旧正月の前後は報告が減る一方、翌月は報告が増加する傾向にあるとして、今後再びフィッシングが活発化する可能性に注意を呼び掛けており、引き続きWebブラウザー・アンチウイルス・UTM等のアンチフィッシング機能を有効にするとともに、利用しているWebサイトへのアクセスは事前に登録したブックマークや公式のモバイルアプリからアクセスする、メールなどで通常と異なるサービスサイトへのアクセス、通常と異なる決済方法等を示された場合には周辺での報告等を参考に十分に警戒するといった自衛策を心掛けてください。

フィッシング対策協議会
Council of Anti-Phishing Japan




## ●IPA、「情報セキュリティ10大脅威 2023」公開…個人・組織ともランキングの顔ぶれほぼ同様

- https://www.ipa.go.jp/security/vuln/10threats2023.html

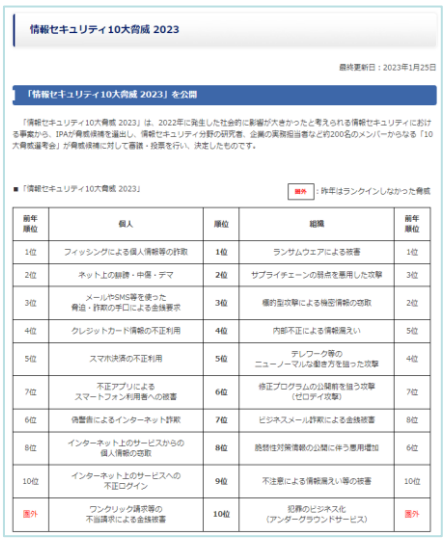
### このニュースをザックリ言うと・・・

- 1月25日(日本時間)、IPAより「情報セキュリティ10大脅威 2022」の概要が発表されました。
- 2022年に発生した、社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、IPAが脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者等約200名によって、個人と組織それぞれのカテゴリーでの10大脅威を決定しています。
- 個人・組織各カテゴリーとも10大脅威はほぼ昨年度と同じ顔ぶれの中で順位が変動しており、個人側は「ワンクリック請求等の不当請求による金銭被害」、組織側は「犯罪のビジネス化（アンダーグラウンドサービス）」が10位に登場しています。

### AUS便りからの所感

IPA

- 今後、2月下旬に10大脅威に関する詳細の解説書が発表される等、追加コンテンツが随時公開される予定となっています。
- 昨年12月にJNSA社が発表した「2022セキュリティ十大ニュース」(AUS便り 2023/1/10号参照)のように、年末年始や半期・四半期において、大手セキュリティベンダーや関連団体等から、各組織の立ち位置・観点等の違いを少なからず反映した年間のセキュリティ関連ニュースのまとめ、あるいは翌年度等における業界の動向予測等がリリースされますので、自分自身や自組織に関連するもの以外であっても各種脅威について知識を得る、あるいは以前に得た知識が正しいかの再確認をし、今後の行動に役立てるのが良いでしょう。



情報セキュリティ10大脅威 2023

最終更新日：2023年1月25日

「情報セキュリティ10大脅威 2023」公開

「情報セキュリティ10大脅威 2023」は、2022年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、IPAが脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者等約200名のメンバーからなる「10大脅威選考会」が脅威候補に対して審議・投票を行い、決定したものです。

■「情報セキュリティ10大脅威 2023」　圏外：昨年はランクインしなかった脅威

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