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。

●1月度フィッシング報告件数は190,500件、3月から再度増加の可能性に警戒を

https://www.antiphishing.jp/report/monthly/202601.html

このニュースをザックリ言うと･･･

- 2月20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202,350件で、12月度(https://www.antiphishing.jp/report/monthly/202512.html)の190,500件から11,850件増加しています。

- 悪用されたブランド件数は108件で12月度(114件)から6件減少、割合が多かったトップ2は3か月連続でAmazon(約17.4%)とApple(約6.5%)、次いで報告されたVISA、Paidy、セゾンカードと合わせて約36.7%、さらに1,000件以上報告された41ブランドまで含めると約95.0%を占めたとのことです。

- フィッシングサイトのURL件数は50,822件で12月度(55,485件)から4,663件減少、使用されるTLD(トップレベルドメイン名)の割合は .cn(約56.4%)、 .com(約29.7%)に加え .cfd(約8.0%)の3つで全体の約94.1%、次いで1,000～10,000件の報告があった .shop(約2.2%)、.info(約1.7%)、.top(約0.8%)、.net(約0.8%)と併せて約99.5%を占めています。

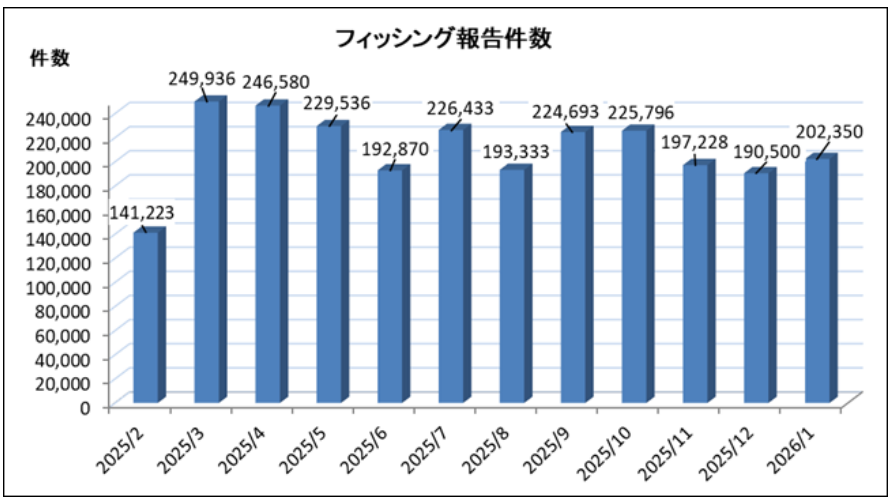
AUS便りからの所感等

- 1月の報告件数について、中旬まで増加、下旬は減少傾向だったとし、同協議会の調査用メールアドレス宛に届いたフィッシングメールも1月26日頃より一部の通信事業者からの配信が急激に減少したことから、「海外におけるレジデンシャルプロキシの無力化(AUS便り 2026/02/06号参照)等の影響の可能性」があったとしている一方、例年通りであれば旧正月が終わる3月から再び急増の可能性があることを指摘しており、継続的な対策と啓発の強化が呼び掛けられています。

- 手元では複数の証券会社による、配当金受取や多要素認証に関する警告を騙るフィッシングメールが多数届いています。

- 他にも日本データ通信協会の迷惑メール相談センターには日々20件以上のフィッシングメールが掲載されており(https://www.dekyo.or.jp/soudan/contents/news/alert.html)、利用しているサービスについて不審なメールを受信した際はこういった情報等と文言が一致するか確認するとともに、本物のサービスのサイトへは事前に登録したブラウザーのブックマークやスマホアプリからアクセスする等、慎重に行動することを日々心掛けましょう。

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



●大学病院患者約1万人個人情報流出…ナースコールシステムにランサムウェア感染

https://www.itmedia.co.jp/news/articles/2602/13/news115.html
https://www.nms.ac.jp/kosugi-h/news/_28830.html

このニュースをザックリ言うと･･･

- 2月13日(日本時間)、日本医科大学武蔵小杉病院より、同院がランサムウェア攻撃を受け、個人情報が流出したと発表されました。
- 被害を受けた個人情報は、同院の患者約1万人分の氏名・性別・住所・電話番号・生年月日等とされています。
- 同9日にナースコールシステムサーバー3台へのランサムウェア感染が確認され、同11日の調査により、サーバーが外部と不正通信を行い、個人情報の窃取を行っていたことが発覚したとしています。
- 発表時点では、外来・入院診察及び救急受け入れは通常通り行っている状態とのことです。

AUS便りからの所感

- ランサムウェア被害は最近も度々報じられており、昨年発生したアサヒグループホールディングスの事例は2月18日に調査報告が行われています。
- 病院関連の感染事案では電子カルテシステム等が停止する事態も発生、また今回も医療機器保守用のVPN装置が侵入経路になったとしていますが、前述のアサヒグループも含め、ことランサムウェア攻撃においてはVPN機器とリモートデスクトップがターゲットとされる傾向が多いです。
- 再発防止策としてVPN(あるいはリモートデスクトップ)の廃止を掲げるケースもありますが、これらを生かしつつ、根本的な対策として、機器のOS・ファームウェアの脆弱性を突かれないよう最新に保つことや、ID・パスワードを破られての侵入の可能性に対し外部から推測されにくいパスワードの設定を行うことも考慮すべきでしょう。

ITmedia NEWS

武蔵小杉病院、ナースコールがランサムウェアの餌食に 患者1万人の個人情報が漏えい

2026年02月13日 18時59分 公開 [松浦立樹，ITmedia]

日本医科大学武蔵小杉病院は2月13日、サイバー攻撃により患者の個人情報が漏えいしたと発表した。ナースコールシステムのサーバがランサムウェア攻撃を受け、患者約1万人の氏名や性別、住所、電話番号、生年月日などが漏えい。なお13日時点では、医療情報システムへの影響はなく、通常通り診療を受け付けている。

9日午前1時50分ごろ、同病院の病棟ナースコール端末が動作不良になった。システムベンダーが調査したところ、サーバがランサムウェア攻撃を受けたことが分かり、このシステムと関連ネットワークを遮断した。その後、厚生労働省から派遣された初動対応チームの調査により、該当のサーバが院外と不正通信を行い、患者の個人情報を窃取していたことを確認した。

現在詳細は調査中としつつも、既にランサムウェアは特定済みで、ウイルス対策ソフトのパターンファイルの作成を依頼中。侵入経路は、医療機器保守用VPN装置からと確認しており、さらなる調査を続けている。

●Visual Studio Code 複数の拡張機能に脆弱性、更新停止のものも

https://www.bleepingcomputer.com/news/security/flaws-in-popular-vscode-extensions-expose-developers-to-attacks/
https://thehackernews.com/2026/02/critical-flaws-found-in-four-vs-code.html
https://www.ox.security/blog/four-vulnerabilities-expose-a-massive-security-blind-spot-in-ide-extensions/

このニュースをザックリ言うと･･･

- 2月17日(現地時間)、OX Security社より、コードエディター「Visual Studio Code(VS Code)」の複数の拡張機能に脆弱点が存在するとして注意喚起が出されています。
- 該当する拡張機能として「Live Server」「Code Runner」「Markdown Preview Enhanced」「Microsoft Live Preview」が挙げられ、悪用により、VS Code上での任意のコードやJavaScriptの実行、情報漏洩等の恐れがあるとしています。
- うちMicrosoft Live Previewについては2025年9月リリースの0.4.16で修正が確認されたものの、他の3つについては未修正としています。

AUS便りからの所感

- 各脆弱点は、設定ファイルに不正なテキストを含める、細工されたMarkdown(md)ファイルを開く等により、それぞれ悪用可能とされています。
- 問題となった拡張機能の中には開発が停滞しているとみられるものもあり、Live Serverは最終更新が2025年1月、Code Runnerに至っては2024年4月と、1～2年近く更新されていないことが確認されています。
- VS Codeの拡張機能は、スマホアプリやWebブラウザーの拡張機能と同様、インストールにより、VS CodeさらにはPC内部やリモート・LAN上の他のサーバー等へのアクセスが可能になり、あるPCで稼働するVS Codeにインストールされた拡張機能が攻撃された場合、LAN上の各PCにまで攻撃が及ぶ可能性も指摘されています。
- また拡張機能の仕様上、現状では細かい権限の制限も特に提供されていないこと、またVS Codeと互換性のあるCursor等のエディターでも影響を受ける可能性が指摘されており、Chrome等と同様必要最低限の拡張機能のみインストール・有効化することが重要です。

Flaws in popular VSCode extensions expose developers to attacks

By Bill Toulas February 17, 2026 04:27 PM 0

Vulnerabilities with high to critical severity ratings affecting popular Visual Studio Code (VSCode) extensions collectively downloaded more than 128 million times could be exploited to steal local files and execute code remotely.

The security issues impact Code Runner (CVE-2025-65715), Markdown Preview Enhanced (CVE-2025-65716), Markdown Preview Enhanced (CVE-2025-65717), and Microsoft Live Preview (no identifier assigned).