— AUS（アルテミス・ユーザ・サポート）便り 2025/12/18号 —
https://www.artemis-jp.com

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。

●閉鎖した「Slashdot Japan」のサイト、ドメイン名の「ドロップキャッチ」で再度表示…アクセスしないよう注意喚起

https://internet.watch.impress.co.jp/docs/yajiuma/2071555.html
https://forest.watch.impress.co.jp/docs/serial/yajiuma/2071523.html
https://togetter.com/li/2639361
https://www.yomiuri.co.jp/local/chubu/news/20251214-GYTNT00022/

このニュースをザックリ言うと･･･

- 12月16日(日本時間)、かつて存在したWebサイト「Slashdot Japan」が、第三者によって不正に復元されたとみられる事象が、インプレス社「やじうまWatch」「やじうまの杜」にて取り上げられています。

- 当該サイトの管理人とみられる人物が同9日にX(旧・Twitter)上で注意喚起していたもので、使用されていたドメイン名を第三者が取得(いわゆる「ドロップキャッチ」)し、Internet Archiveから過去のコンテンツを取得して表示したものと推測されています。

- 現在も当時のURLでサイトが表示されていることが確認されており、かつての当該サイトのアカウント情報を詐取しようとしている可能性もあるとして、サイトにはアクセスしないよう呼び掛けられています。

AUS便りからの所感等

- Slashdot Japan(以下・旧サイト)は2015年5月に「スラド」に改名(ドメイン名も移行)しており、以後旧サイトのURLからはスラドのサイトへリダイレクトする状態となっていました(その後2025年3月にスラドも終了しています)。

- 当該サイトにアカウントを持っており、パスワード管理ツールに現在も情報が登録されている等の場合、(ブラウザーによっては)サイトのログインページへのアクセス時にアカウント情報が自動入力され、ページ上のスクリプトに読み取られる恐れがあることもX上で指摘されています(この他かつてサイトにアクセスしていた際にやり取りしていたCookie情報等も、同じドメイン名で稼働する偽サイトに読み取られる可能性があります)。

- 旧サイトのドメイン名は一旦失効した後12月1日にドロップキャッチされたとみられ、また11月1日にスラドのドメイン名も同様にドロップキャッチされていることから、こちらも偽サイトが立ち上げられる可能性があり、自衛策として、新旧両方のサイトに対し、パスワード管理ツールに登録されているアカウント情報を消去することや、ブラウザー・UTM等のアンチフィッシング機能においてアクセスを遮断するURLに追加すること等を推奨致します。

- ドロップキャッチについては、この他にも12月14日に読売新聞において、愛知県選挙管理委員会が2022年参議院議員選挙の特設サイトで使用したドメイン名がオンラインカジノとみられるサイトに転用されていた事例が挙げられています。

Impress Watch

やじうまの杜

かつての人気サイト「スラッシュドット・ジャパン」に偽物、関係者が警告「絶対ログイン禁止」

何者かがドメインを取得し、過去データを表示、ID・パスワードの盗難に厳重注意

樽井 秀人　2025年12月16日 10:02

かつての人気サイト「スラッシュドット・ジャパン」が復活？……ではなく、第三者による偽物との由

かつて人気だったWebサイト「スラッシュドット・ジャパン」が再びアクセス可能になり、以前のアーカイブを閲覧できるようになっていますが、関係者によると、これは偽サイトとのこと。ドメインが何者かに取得され、「archive.org」に保管されていたコンテンツが使いまわされているようです。

●年末年始における情報セキュリティの注意喚起、IPAより発表

https://www.ipa.go.jp/security/anshin/heads-up/alert20251216.html
https://www.ipa.go.jp/security/measures/vacation.html
https://www.ipa.go.jp/security/measures/everyday.html

このニュースをザックリ言うと・・・

－12月16日(日本時間)、IPAより、年末年始を迎えるにあたっての、情報セキュリティに関する注意喚起が出されました。

－多くの企業・組織において、この時期に従業員等が長期休暇を取得、常駐する人が少なくなる等「いつもとは違う状況」となり、通常時には生じにくい様々な問題が発生し得ることを鑑み、「個人の利用者」「企業や組織の利用者」「企業や組織の管理者」それぞれを対象に、「休暇前」「休暇中」「休暇明け」に行うべき基本的な対策と心得が「長期休暇における情報セキュリティ対策」においてまとめられています。

－IPAでは毎年のゴールデンウィークと夏季・冬季休暇の時期に注意喚起を行っており、また長期休暇に関係なく常時から注意すべき普遍的なものがまとめられた「日常的に実施すべき情報セキュリティ対策」も取り上げられています。

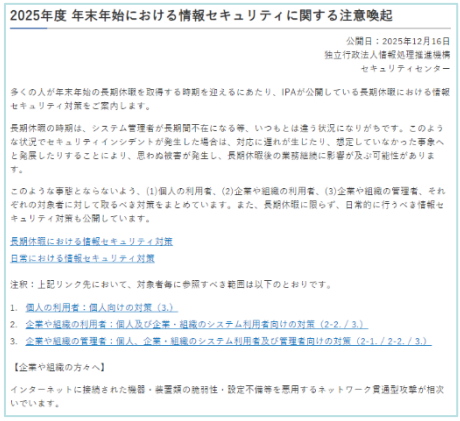
AUS便りからの所感

－注意喚起の内容は、システム管理者が長期間不在になる等により、ウイルス感染や不正アクセス等のインシデント発生に気付きにくく対処が遅れてしまう可能性から、従業員が旅行先等でSNSへの書き込みを行った場合に、最悪関係者にも思わぬ被害が及んでしまう可能性まで、多様なものとなっていますが、「長期休暇における～」「日常的に実施すべき～」いずれも内容は毎回大きく異なるようなものではありません。

－今回のトピックとして、2024～2025年の年末年始においてはIoT機器を中心としたボットネットによるDDoS攻撃が相次ぎ、NISCから注意喚起が出された(AUS便り2025/02/06号参照)ことが取り上げられ、自組織のIoT機器等が不適切に外部に公開されていないか、SHODAN等のサービスも活用して確認するよう呼び掛けられています。

－ともあれ、注意喚起等をいつ確認したかに拘らず、その時点で点検すべきことは様々ですので、以後も、ゴールデンウィークや夏季といった長期休暇に備えて、準備・点検を行うよう意識して頂ければ幸いです。

IPA 独立行政法人 情報処理推進機構


2025年度 年末年始における情報セキュリティに関する注意喚起

公開日：2025年12月16日
独立行政法人情報処理推進機構
セキュリティセンター

多くの人が年末年始の長期休暇を取得する時期を迎えるにあたり、IPAが公開している長期休暇における情報セキュリティ対策をご案内します。

長期休暇の時期は、システム管理者が長期間不在になる等、いつもとは違う状況になりがちです。このような状況でセキュリティインシデントが発生した場合は、対応に遅れが生じたり、想定していなかった事象へと発展したりすることにより、思わぬ被害が発生し、長期休暇後の業務継続に影響が及ぶ可能性があります。

このような事態とならないよう、(1)個人の利用者、(2)企業や組織の利用者、(3)企業や組織の管理者、それぞれの対象者に対して取るべき対策をまとめています。また、長期休暇に限らず、日常的に行うべき情報セキュリティ対策も公開しています。

長期休暇における情報セキュリティ対策
日常における情報セキュリティ対策

注釈：上記リンク先において、対象者毎に参照すべき範囲は以下のとおりです。

1. 個人の利用者：個人向けの対策（3）
2. 企業や組織の利用者：個人及び企業・組織のシステム利用者向けの対策（2-2 / 3）
3. 企業や組織の管理者：個人、企業・組織のシステム利用者及び管理者向けの対策（2-1 / 2-2 / 3）

【企業や組織の方々へ】

インターネットに接続された機器・装置類の脆弱性・設定不備等を悪用するネットワーク貫通型攻撃が相次いでいます。

●「Notepad++」のアップデーターに脆弱性、偽更新ファイルのダウンロードに誘導の恐れ

https://forest.watch.impress.co.jp/docs/news/2070885.html
https://rocket-boys.co.jp/security-measures-lab/notepad-plus-plus-updater-critical-vuln-cve-2023-40031/
https://blackhatnews.tokyo/archives/31085
https://notepad-plus-plus.org/news/v889-released/

このニュースをザックリ言うと・・・

－12月9日(現地時間)、軽量テキストエディター「Notepad++」のアップデート機能に脆弱性があったとして、修正バージョン8.8.9がリリースされています。

－Notepad++に含まれるアップデーター「WinGUp」においてアップデートファイルの検証機能に問題があり、悪意のあるWebサイトに誘導され、偽のアップデートファイルをダウンロードさせられる可能性があったとしています。

－Notepad++のフォーラムでは、10月に古いバージョンのWinGUpが不審なプログラムのダウンロードに悪用されたとみられる事例がユーザーから報告されていた模様です。

AUS便りからの所感

Impress Watch

－自動アップデート機能に関する修正が行われていることもあり、今回の8.8.9へのアップデートに限り、自動アップデート機能を用いず、公式サイトからインストーラーをダウンロードすることが推奨されます。

－フォーラムに報告された事例では、いわゆるDNSスプーフィング攻撃により、偽のサーバーへ誘導された可能性が指摘されており、ブロードバンドルーターや組織で使用するキャッシュDNSサーバーにおいて攻撃が可能となる脆弱性が発生する場合もあり(2024年にはWindowsでも脆弱性が報告された前例があります)、これらに対する攻撃も鑑み、同様にセキュリティアップデートを怠りなく適用することが重要です。

「Notepad++」の自動更新機能にセキュリティ欠陥、偽の更新ファイルにすり替えられる

v8.8.9で修正済み

樽井 秀人　2025年12月12日 16:24

「Notepad++」で用いられている自動アップデートツール「WinGUp」で、トラフィックハイジャックの脆弱性が発見された。アップデートをダウンロードする際に悪意あるサーバーへリダイレクトされ、偽の実行ファイルがダウンロードされることがあったという。

窓の杜からダウンロード

この問題の原因は、アップデーターがダウンロードした更新ファイルの整合性と真正性を検証する処理に弱点があったことにある。攻撃者がアップデーターと「Notepad++」更新サーバーの間の通信を傍受できた場合に、正しい更新ファイルではなく、偽のバイナリをダウンロード・実行できるように促すことができたという。