

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。

●ドメイン名における5つの重要なニュース、JPRSが発表

<https://jprs.jp/related-info/important/2023/231214.html>



このニュースをザックリ言うと…

- 12月14日(日本時間)、[jpドメインを管理するJPRS社](#)より、「[2023年 ドメイン名重要ニュース](#)」として今年のドメイン名に関するニュースから選ばれた5つの大きな話題が発表されました。
- 挙げられたニュースは「[1. ドメイン名廃止後のトラブルやリスクが注目される](#)」「[2. ランダムサブドメイン攻撃の活発化](#)」「[3. インターネット関連の重要な国際会議が日本国内で開催](#)」「[4. .com 3年連続の値上げ](#)」「[5. b.root-servers.netのIPアドレス変更](#)」となっています。

AUS便りからの所感等

- 以下一部の項目について言及しますが、「[1. ドメイン名廃止後のトラブルやリスクが注目される](#)」については、サービス等が終了して使われなくなったドメイン名が十分な期間を経ずに失効した直後に第三者に登録される「[ドロップキャッチ](#)」は今年も時々報じられ、一方で管理ミスで失効したドメイン名がオークションにかけられたものを買い戻した事例も話題となっています(AUS便り 2023/09/27号参照)。
- 「[2. ランダムサブドメイン攻撃の活発化](#)」は[DNSサーバーへのDDoS攻撃](#)、いわゆる「[DNS水責め攻撃](#)」とも呼ばれるものについてですが、[長年問題となっている「オープンリゾルバー\(任意のアクセス元からの再帰問合せを受け付ける脆弱性\) 状態のサーバーやルーター等が悪用されており、これを随時対策していくことなしでは解決しない](#)」でしょう。
- 「[5. b.root-servers.netのIPアドレス変更](#)」は、DNSにおいて通常最初にアクセスされる「[ルートサーバー](#)」の一つに関するもので、他にも複数台のルートサーバーがあることから[影響は低い](#)と思われるものの、ネット上の各種サーバー内あるいはDNSサーバーソフトウェアに組み込まれる形で[ルートサーバーの一覧表が保存されているケース](#)については[可能な限り更新すべき](#)であり、[OSからアプリケーションまで最新バージョンに保つこと](#)はそういう意味合いでも欠かせないものです。



ドメイン名関連情報
2023年 ドメイン名重要ニュース

2023/12/14

2023年の多くのニュースの中から、ドメイン名ニュース担当者が選んだ大きな話題を五つご紹介いたします。

1 ドメイン名廃止後のトラブルやリスクが注目される

2023年は、利用されていたドメイン名の廃止をきっかけとしたトラブルやリスクが、大きく注目されました。行政機関や地方自治体などが利用していたドメイン名が廃止された後、オークションに出品され、第三者に登録されるといった事例が相次いで話題になりました。

ドメイン名を廃止した場合、一定期間が経過した後、第三者がそのドメイン名を登録できるようになります。廃止されたドメイン名がWebサイトのURLとして使われていた場合、他のWebサイトからのリンクや、検索エンジンによるドメイン名の評価が弊り、アクセス数が見込めることなどから、そのドメイン名が関係のない第三者に登録・悪用される可能性があります。

また、廃止されたドメイン名がメールアドレスとして使われていた場合、廃止されたドメイン名を第三者が登録し、メールを送受信できるようにして、悪性を偽ったメールアドレスとして悪用される可能性があります。廃止したドメイン名のメールアドレスをSNSアカウントのログインIDなど、他のサービスで利用していた場合、パスワードの再設定によってそのSNSアカウントを乗っ取られたり、登録している情報を盗み見られたりする可能性があります。

ドメイン名を廃止する場合、該当のWebサイトやメールアドレスを終了することの周知や、そのメールアドレスを利用したアカウントや設定の削除、メールアドレスの変更を事前しておくことをお勧めします。

関連リンク > [ドメイン名の廃止に関する注意\(JPRS\)](#)

2 ランダムサブドメイン攻撃の活発化

2023年3月ごろからDNSを狙った攻撃手法「ランダムサブドメイン攻撃」が活発化し、行政機関や地方自治体などのWebサイトで具体的な被害も発生している旨が、複数の研究者やサービス事業者などから報告されています。

●WordPress最新バージョン6.4.2リリース…脆弱性1件が修正

<https://news.mynavi.jp/techplus/article/20231213-2838379/>
<https://ja.wordpress.org/2023/12/08/wordpress-6-4-2-maintenance-security-release/>



このニュースをザックリ言うと…

- 12月6日(現地時間)、WordPressの開発元より、WordPressの最新バージョン6.4.2がリリースされました。
- バージョン6.4.2では7件のバグの修正の他、プラグインとの組合せおよびマルチサイトでの構築時に深刻な問題となり得るという脆弱性1件が対策されているとのこと。
- WordPress本体では10月にもセキュリティアップデートとして6.3.2が、また4.1系~6.2系の各バージョンでも同様に修正バージョンがリリースされています。

AUS便りからの所感

- 今回は6.3系以前の更新はなく、11月7日リリースにリリースされた6.4系でのみの脆弱性と推測されますが、多くのWordPressを用いたサイトでは6.4系を使用していると思われるため、その場合にはいかなる状況であっても更新を行うようにしましょう。
- WordPressでは本体のみならず各種プラグインでも頻りに脆弱性が報告されるため、決してそれぞれインストールしたまま放置せず、随時管理画面にアクセスし更新機能によって最新に保つよう努めること、またセキュリティを強化するプラグインも多数提供されているため、評判が高いものを導入することが肝要であり、さらに並行して(もしくは本体・プラグインのアップデートが困難な場合を鑑みて)WAFやIDS・IPSの導入についても検討することが望ましいです。



WordPress 6.4.2リリース、リモートコード実行の脆弱性を修正、更新を

掲載日 2023/12/13 14:46

著者: 後藤大地

Automaticはこのほど、「WordPress 6.4.2 Maintenance & Security Release - WordPress News」において、WordPress バージョン6.4.2をリリースしたと伝えた。WordPress バージョン6.4.2では重大なセキュリティ上の不具合が1件、coreの不具合が7件修正されている。

修正されたセキュリティ上の不具合は次のとおり。

- リモートコード実行(RCE: Remote Code Execution)の脆弱性。この脆弱性は直接悪用はできないが、一部のプラグインと組み合わせるとマルチサイトインストールにおいて重大度が高くなる可能性がある

●サポート詐欺の「偽の警告画面」体験サイト、IPA公開

<https://www.itmedia.co.jp/news/articles/2312/19/news153.html>
<https://www.ipa.go.jp/security/anshin/measures/fakealert.html>



このニュースをザックリ言うと…

- 12月19日(日本時間)、IPAより、いわゆる「サポート詐欺」で使用される「偽のセキュリティ警告画面」を体験できるサイトが公開されました。
- 「偽セキュリティ警告画面(サポート詐欺)の閉じ方体験サイト」へのリンクを辿り、アクセス先で「体験サイトを起動」のボタンをクリックすることにより、「画面がフルスクリーンになり簡単に解除できなくなる」「偽のWindowsセキュリティ等多数のウィンドウが表示される」等、多くのサポート詐欺で発生する現象が発生します(音声も再生されるため、体験時には注意してください)。
- 音声再生等でサポート詐欺によくある事例の解説を行っており、ESCキーを一度押しただけで解除できない場合でも一定時間押し続けることで解除できるとしています。

AUS便りからの所感



- ESCキーを一回押して解除できない挙動はChromeおよび同じエンジンを使用しているEdge等のブラウザで有効なものみられ、一方でブラウザからも「全画面表示を終了するにはESCキーを押し続けます」といった表示がなされます(FirefoxではESCキー一回で解除できます)。
- ユーザー側においては現時点で使われている手口がどういふものかを確認する意味でも利用が望まれ、またIPA側でも、サポート詐欺を行う犯罪者の手口が今後変化し、警告画面の形も新しいものとなっていくとして、体験サイトがそれを随時反映した物となることを期待したいものです。

「偽セキュリティ警告体験サイト」IPAが公開 サポート詐欺に注意喚起

© 2023年12月19日 16時41分 公開

[ITmedia]

情報処理推進機構 (IPA) は12月19日、偽の警告によってPCがコンピュータウイルスに感染したかのように見せかけ、対策が必要として不審なソフトをインストールさせたり、金銭を要求したりする「サポート詐欺」が体験できるWebサイトを公開した。サポート詐欺に関する相談件数が増えており、注意喚起のために作成したという。

