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。

●Windows 10のアップデート「KB5034441」で多数のインストール失敗報告…今後の再アップデート待ちを

https://news.mynavi.jp/techplus/article/20240111-2860896/
https://support.microsoft.com/ja-jp/kb/5034441
https://learn.microsoft.com/en-us/windows/release-health/status-windows-10-22h2#3231msgdesc

このニュースをザックリ言うと･･･

- 1月10日(日本時間)にマイクロソフト(以下・MS)からリリースされた月例のセキュリティアップデートのうち、Windows 10向けの「KB5034441」について、「0x80070643」エラーが発生してインストールできないという報告が相次いでいます。
- KB5034441は「Windows回復環境(WinRE)」に対するセキュリティアップデートですが、後日MSが発表した情報によれば、インストールにはPC上に予め作成される回復パーティションに十分な空き容量が必要としています。
- MSではこの問題の解決策に取り組んでおり、今後のリリースで再度アップデートを提供する予定としています。

AUS便りからの所感等

- KB5034441で修正される脆弱性(CVE-2024-20666)は、ディスク暗号化機能(BitLocker)で暗号化されたデータにアクセスされる可能性があるものですが、悪用には攻撃者がPCそのものを直接取り扱う必要があるとされています。
- MSからはKB5034441をインストールするための回避策も提示されていますが、回復パーティションのサイズを変更する等高度な手順をとるものであり、一般のユーザーには実行が難しいものと思われますので、脆弱性を悪用されるシナリオの困難さも鑑み、再度リリースされるであろうアップデートを待つのが無難でしょう。
- PC自体を盗難されたり、第三者に物理的に操作されないよう保護する機構の導入は肝要ですし、またローカルからのみ攻撃可能とされる脆弱性であっても、感染したマルウェアや不正アクセスした攻撃者によって悪用可能になるものもあることから、アンチウイルスやUTMによる防御も欠かさずに行うことは言うまでもありません。

TECH Powered by マイナビニュース

Windows 10で更新プログラムに失敗する現象が発生中

掲載日 2024/01/11 14:28　　著者：杉山貴章

Microsoftは1月9日(現地時間)に月例アップデートとして更新プログラム「KB5034441」をリリースしたが、11日時点で、複数のユーザーからこの更新プログラムのインストールがエラーにより失敗するという現象が報告されている。この問題が発生した場合、Windows Updateの画面にエラーコード「0x80070643」が表示され、アップデートを継続することができない。

更新プログラム「KB5034441」の概要

KB5034441は、WinRE（Windows 回復環境）を使用してBitLockerのセキュリティ機能をバイパスできる脆弱性「CVE-2024-20666」に対処するためのセキュリティ更新プログラム。2024年1月の月例アップデートに含まれているため、自動アップデートが有効な環境ではWindows Updateによって自動的にインストールされる。

Microsoftでは、KB5034441で発生するエラーについて説明するサポートページを開設した。

●島根県が過去に使用したドメイン名が第三者に取得…注意喚起

https://www.itmedia.co.jp/news/articles/2401/16/news101.html
https://www.pref.shimane.lg.jp/life/information/joho/densi_jichitai/domein.html

このニュースをザックリ言うと･･･

- 1月15日(日本時間)、島根県より、県が各種事業等のために登録していたドメイン名が運用終了後に第三者に取得されていたとして注意喚起が出されています。

- 今回の注意喚起で挙げられているのは「島根県新型コロナ対策認証店認証制度(shimane-ninsho.jp)」「スモウルビー・プログラミング甲子園開催事業(smallruby-koshien.jp)」および「しまねものづくり人材育成支援 Navi(shimane-monodukuri.jp)」の3ドメインとなっています。

- 県では当該ドメイン名へのリンクを貼っているWebサイトの管理者に対しリンクを削除するよう呼び掛けるとともに、県民および県庁内へも周知するとしています。

AUS便りからの所感

- 県では2023年10月27日にも、同様に再登録されていたドメイン名として「第71回全国植樹祭しまね(syokujusai-shimane2020.jp)」「Go To Eatキャンペーンしまね(gotoeat-shimane.jp)」および「ご縁の国しまね(shimane-goen.jp)」を挙げており、今回を含め計6つのドメイン名が該当します。

- つい最近まで使用されていたようなドメイン名が十分な期間を経ずに失効してしまい、第三者に登録されてしまう「ドロップキャッチ」については、2023年9月にはNTTドコモが使用していたドメイン名が管理の不手際で失効し、ドメイン名管理業者によるオークションから買い戻したことが報じられています(AUS便り 2023/09/27号参照)。

- ドロップキャッチの発生を想定しての事前事後の対策として、一時的なイベントのために専用のドメイン名を(***.jpや***.com等で)新規に登録するよりも、既存のドメイン名の下にサブドメイン名を作る、または地方自治体であれば「lg.jp」を使う等を検討すること、またイベントやサービスの終了においては、終了の告知ないしサイトの閉鎖後も可能な限り長期間はドメイン名を維持するよう計画すること等が推奨されます。

ITmedia NEWS

島根県が使ったドメイン、第三者が再取得で注意喚起 新型コロナやRuby関連事業など

2024年01月16日 11時32分 公開 [ITmedia]

島根県は1月15日、県が過去に使用したドメインが、運用停止後にオークションサイトで売買されるなどして第三者に再取得されていることが分かったと発表した。各ドメインにリンクを張っているサイトの管理者に対して、リンクの削除を依頼している。

県が使用したドメインの第三者による再取得について

県が過去に使用したドメイン（ホームページアドレス）について、運用停止後にオークションサイトでの売買等により、第三者に再取得されていることを令和５年 10 月 27 日に発表しましたが、新たに３件のドメインが第三者に再取得されていることが判明しました。

これらのホームページに係る事業は既に終了しており、下記ドメインを使用したホームページは、本県とは全く無関係ですので、ご注意ください。

● 12月フィッシング報告件数は90,792件で再度増加、フィッシングサイトURLも急増

https://www.antiphishing.jp/report/monthly/202311.html
https://www.antiphishing.jp/news/alert/smime_20231215.html
https://internet.watch.impress.co.jp/docs/news/1555491.html

このニュースをザックリ言うと･･･

- 1月15日(日本時間)、フィッシング対策協議会より、12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。

- 12月度の報告件数は90,792件で、11月度(https://www.antiphishing.jp/report/monthly/202311.html)の84,348件から6,444件増加しています。

- フィッシングサイトのURL件数は17,172件で11月度(10,678件)から6,494件増加、悪用されたブランド件数も80件で11月度(73件)から7件増加となっています。

- 最も多く報告されたのはETC利用照会サービスを騙るフィッシングで報告数全体に対する約24.3%、次いでそれぞれ1万件超だったAmazon、マイナポイント事務局、三井住友カードと合わせて約69.4%、さらに1,000件以上報告された11ブランドまで含めると約89.7%を占めたとのことです。

AUS便りからの所感

- 同協議会が12月に出した注意喚起の一例として、三井住友カードや三井住友銀行を騙るフィッシングメールに非正規のS/MIME電子署名ファイル(他のメールで作成された署名ファイルを流用した可能性があるとのことです)が添付されているものがあり、署名を検証しないメーラー等でなりすましかどうか判断できないユーザーを誘導する意図があったとされています。

- フィッシングサイトURL件数の急増については、フィッシングサイトへのリダイレクト元として、Cloudflare Workersで付与できるサブドメインを悪用するケースが増加(全体の約37.2%に該当)したためとしています。

- Gmailが発表した、@gmail.com(および @googlemail.com)宛にメールを送信する相手にSPF・DKIM・DMARCの設定等のメールセキュリティ要件を満たすよう要請する「メール送信者のガイドライン(https://support.google.com/mail/answer/81126?hl=ja)」の適用が2月1日に迫っていますが、最大手のメールサービスである以上「対応しなくてよい」ということはほぼ有り得ず、またその他の取引相手をフィッシングから保護する意味でも、全ての組織でドメイン名・メールサーバーにおける対応が必須と言えます。

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