— AUS（アルテミス・ユーザ・サポート）便り 2020/01/20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。

●MSより月例セキュリティパッチ発表…Windows 7は無償サポート終了

https://japan.zdnet.com/article/35147980/
https://gigazine.net/news/20200115-microsoft-patches-nsa-finds-vulnerability/
https://portal.msrc.microsoft.com/ja-jp/security-guidance/releasenotedetail/2020-Jan

このニュースをザックリ言うと・・・

- 1月15日(日本時間)、マイクロソフト(以下、MS)より、今年初めてとなる1月度の月例セキュリティパッチが公開されました。

- OSのみならずOffice・Edge・IE等においても、PCが乗っ取られる恐れのある重大な脆弱性等が修正されており、適用が強く推奨されます。

- Windows 7については今回で無償サポートが終了し、多くのケースで最後のパッチ提供となります。

AUS便りからの所感等

- 今回、Windows 10(およびServer 2016, 2019)の暗号化機能において一部のデジタル署名の偽装が可能となる脆弱性が、米国家安全保障局(NSA)からの報告を受けて修正されており、以前Windowsの脆弱性を悪用するツールが流出した(AUS便り 2017/4/24号参照)こともあるNSAが方針転換を行ったのではとする声も一部では挙がっています。

- Windows 7については今後3年間、Professional等一部エディションで有償サポート(ESU)が提供されますが、これの購入もせずに解決を先送りにしようとするユーザーにより、無対策の状態に置かれるPCが依然多く残るとみられ、マルウェア感染やそれによるボットネットの一部にされる恐れがあります。

- アンチウイルス・UTMによるPC自体の防御を固める、さらには社内外のネットワークから適宜隔離するといった対策をとったとしても、よほどやむを得ぬ事情がある場合でない限り、決してそれでよしとせず速やかなWindows10への移行を計画することが肝要です。

Microsoft

日本 (日本語)

セキュリティ更新プログラム ガイド > リリース ノート

リリース ノート

2020 年 1 月のセキュリティ更新プログラム

リリース日: 1月 14, 2020

1 月のセキュリティ リリースは、次のソフトウェアのセキュリティ更新プログラムで構成されています。

- Microsoft Windows
- Internet Explorer
- Microsoft Office、Microsoft Office Services および Web Apps
- ASP.NET Core
- .NET Core
- .NET Framework
- OneDrive for Android
- Microsoft Dynamics

これらのセキュリティ更新プログラムについて、次の情報に注意してください。

- Windows 10 バージョン 1909 の機能を有効にする方法については、「Windows 10, version 1909 delivery options」(英語情報) を参照してください。Windows 10 バージョン 1903 および 1909 は、同一のシステム ファイル セットを含む共通のコア オペレーティング システムを共有していることに注意してください。また、同じセキュリティ更新プログラムのサポート技術情報も共有しています。
- Windows 10 の更新プログラムは累積的です。今月のセキュリティ リリースには、セキュリティ以外の更新プログラムに加えて、Windows 10 に影響する脆弱性のすべてのセキュリティ修正プログラムが含まれています。これらの更新プログラムは、Microsoft Update カタログから入手できます。
- Windows 10 オペレーティング システムのライフサイクルとサポート期間については、「Windows ライフサイクルのファクト シート」を参照してください。
- 各オペレーティング システムの最新のサービス スタック更新プログラムの一覧については、ADV990001 を参照してください。この一覧は、新しいサービス スタック更新プログラムがリリースされるたびに更新されます。最新のサービス スタック更新プログラムをインストールすることが重要です。
- 2019 年 5 月から、Windows Server 2012 上で Internet Explorer 11 を使用できるようになりました。この構成は、IE の累積パッケージにのみ存在します。
- Windows RT 8.1 および Microsoft Office RT ソフトウェアの更新プログラムは、Windows Update を介してのみ入手できます。
- 脆弱性についてのセキュリティの変更のほか、更新プログラムにはセキュリティ関連機能を改善する多層防御の変更が含まれています。
- 注: Windows 7、Windows Server 2008 R2、および Windows Server 2008 のサポートは、2020 年 1 月 15 日に終了します。詳細については、「ライフサイクルに関する FAQ - 拡張セキュリティ更新プログラム」を参照してください。

次の **CVE** には、追加情報が記載された **FAQ** があります。また、更新プログラムのインストール後に実行する * 追加の手順も記載されている場合があります。この一覧は今回のリリースが対応している **CVE** をすべて掲載しているわけではないことにご注意ください。

●ハードオフネットモールで「リスト型攻撃」による不正ログイン発生…アカウント情報149件被害

https://cybersecurity-jp.com/news/34791
https://www.hardoff.co.jp/news/n649/

このニュースをザックリ言うと・・・

- 1月10日(日本時間)、ハードオフコーポレーションより、同社が運営する通販サイト「ハードオフネットモール」がいわゆる「リスト型アカウントハッキング(リスト型攻撃)」を受けたと発表されました。

- 攻撃は2019年11月29日から今年1月7日まで行われたとされ、同サイトのユーザーアカウント149件が不正ログインの被害を受け、氏名・住所・電話番号・メールアドレス・生年月日・購入履歴等が閲覧された可能性があるとしています。

- クレジットカード情報の一部(カード名義人・有効期限・カード番号下3桁)も同様に閲覧された可能性がありますが、セキュリティコード(CVV)は保存されていないため対象外とのことです。

AUS便りからの所感

- 同社ではさらなる不正ログインの防止のため「他社サービスとは異なるパスワードを設定する」「第三者が容易に推測できるパスワードを使用しない」よう注意喚起、また該当するとみられる以外のユーザーに対しても、他社サービスと同一のユーザID・パスワードを利用している場合は、速やかにパスワードを変更するよう呼び掛けており、リスト型攻撃への対応としては適切なものとみられます。

- 攻撃者が入手したリストに企業等組織のメールアドレスが含まれていた場合、その組織のメールサーバー等がやはりリスト型攻撃のターゲットとされる恐れがありますので、ユーザーにおいてはメールアカウントに設定されたパスワードもやはり他で使い回したりしないよう注意を払う必要があります。

- システム管理者側においてもそのように啓発するとともに、サーバーの設定やUTM等によるIDS・IPS機能を有効にし、不正ログイン試行の兆候を検知・遮断できる体制を整えることを検討するのが良いでしょう。


サイバーセキュリティ.com

セキュリティニュース

ハードオフで不正アクセス、リスト型攻撃でアカウント情報149件流出か

2020.01.14 2020.01.14 事務局 編集部

「リスト型アカウントハッキング（リスト型攻撃）」による弊社ハードオフネットモールへの不正ログインの発生とパスワード変更のお願いについて

2020年1月10日

弊社が運営するオンライン通販サイト(ハードオフネットモール)において、お客様ご本人以外の第三者から「リスト型アカウントハッキング(リスト型攻撃)」による不正なログインがあったことが判明しました。
他社サービスから流出した可能性のあるユーザID・パスワードを利用して、webサービスにログインを試みる手法です。
お客様や関係者の皆様には、ご迷惑とご心配をおかけすることを、深くお詫び申し上げます。

現時点で確認している事実と弊社の対応状況をご報告いたします。

● 2020年の情報セキュリティ十大トレンド、JASAが発表

https://securityblog.jp/news/20200114.html
https://www.jasa.jp/seminar/security_trend_top10.html

このニュースをザックリ言うと・・・

- 1月6日(日本時間)、特定非営利活動法人日本セキュリティ監査協会(JASA)より、同協会認定の情報セキュリティ監査人を対象としたアンケート結果に基づく「2019年 情報セキュリティ十大トレンド」が発表されました。
- ランクインしたトレンド(括弧内は前年度での順位、-はランク外)は以下の通りです。

1(-): 自然災害によるIT被害の拡大
2(10): クラウド・バイ・デフォルト時代の新しい安全性評価制度の開始
3(-): クラウドサービスの障害による大規模なビジネス影響
4(-): DX化の進展によりさらに加速するセキュリティ人材不足
5(5): 働き方改革の推進普及による新たな脅威の発生
6(-): プライバシー保護の国際標準化に乗り遅れる日本企業
7(-): サプライチェーンの透明化で求められるセキュリティ対策の強化
8(8): 標的型ランサムウェアで倒産危機？　システム全てが人質に
9(-): クラウドサービスの管理・設定ミスによる情報漏洩
10 (-): 安易なアジャイル開発によるぜい弱なシステムの氾濫


日立ソリューションズ Information security blog 情報セキュリティブログ

JASAが2020年のセキュリティ十大トレンドを発表

2020年1月14日 0

1月6日、特定非営利活動法人 日本セキュリティ監査協会(JASA)は、「監査人の警鐘 - 2020年 情報セキュリティ十大トレンド」を公開した。これは、同協会より認定を受けた情報セキュリティ監査人約1,800人を対象に実施したアンケートによって選ばれたものだ。

第1位には「自然災害によるIT被害の拡大」が前年のランク外からランクインした。これは、地球温暖化をはじめとする環境変化による災害などにより、情報システムへの影響が拡大することへの懸念を示したもの。

また、第2位、第3位はそれぞれ「クラウド・バイ・デフォルト時代の新しい安全性評価制度の開始」「クラウドサービスの障害による大規模なビジネス影響」がランクインした。政府主導で進むクラウドの活用や、一般化するクラウド利用における潜在的なリスクなど、ビジネスにおけるクラウド活用が進み、その対策に注目が集まる結果となった。

AUS便りからの所感

- 今回のトップ10において、昨年もランクインしていた項目は、根強い脅威として残り続けるランサムウェア等3項目のみと、業界のトレンドが劇的に移り変わっていることを物語っています。
- 1位には2019年に発生した記録的な豪雨・大型台風等を踏まえての自然災害による物理的障害への各種対応、3位にもそういった物理的障害を含めた各種障害に対するデータセンターの分散等の可用性の確保がテーマとして挙げられている他、活用が進むクラウドへの対応に関する項目も複数ランクインしています。
- マカフィーが昨年12月に発表した「10大セキュリティ事件ランキング」(AUS便り 2019/12/23号参照)等、様々なセキュリティベンダーやセキュリティ関連団体等がそれぞれの観点から独自のランキングを挙げており、これらを参考にしつつ、各人が話題となっているセキュリティの脅威について随時情報収集を行い、特にシステム管理者においては、新しい脅威からの被害をも最小限に抑えられるようなシステム・ネットワークの随時見直しに柔軟に対応して頂ければ幸いです。