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。

●2022年6月にWindows10上のIEサポート終了、IPAがブラウザー乗り換え・コンテンツ改修等注意喚起

https://news.mynavi.jp/article/20210819-1950561/
https://www.ipa.go.jp/security/announce/ie_eos.html

このニュースをザックリ言うと・・・

- 8月17日(日本時間)、IPAより、2022年6月16日に一部環境でInternet Explorer(IE)のサポートが終了することに関する注意喚起が出されています。

- この日にサポート終了となるのは、Windows 10 デスクトップ SKU(20H2 以降)・Windows 10 IoT(20H2 以降)上のIE11とされ、当該環境ではIEの代わりにEdgeブラウザーの「IEモード」が起動するようになる(Edgeブラウザーがインストールされていることが条件)とのことです。

- サポート終了後のIEにはセキュリティパッチが提供されなくなること、またEdgeのIEモードも将来(遅くとも2029年)サポート終了予定で、その後はIEのみで動作するよう作成されたコンテンツ(以下・IEコンテンツ)は閲覧できなくなる可能性があること等から、IPAではユーザーに対しEdgeやChrome等のモダンなWebブラウザーの利用を、コンテンツ提供者に対してはコンテンツがモダンなブラウザーで利用可能となるよう改修する(万一間に合わない場合はIEモードで閲覧するよう周知する)ことを呼び掛けています。

AUS便りからの所感等

- マイクロソフトでは、同社が提供する「Microsoft 365」においても、同日IE11(および古いバージョンのEdge)でのサービス利用のサポートを終了させています。

- 前述のWindows 10以外におけるサポート終了日はまちまち(多くはOS自体のサポート終了日と同じ)で、例えばWindows 8.1では2023年1月まで、Windows 10でもエディションによってはさらに先となっているものもありますが、大多数の環境では前述の2022年6月がリミットとなることを考慮するのが良いでしょう。

- モダンなブラウザー向けのWebサービスにおいて、余程入り組んだ作りとしない限り、最も普及しているChromeでしか動かない等ということにはならないと思われますが、特定のブラウザーに依存するサービスは結局IEコンテンツで起こり得ることの繰り返しとなりますので、可能な限りEdge・FirefoxやSafariでも動作する最大公約数の機能を用い、これらのブラウザーでも動作確認することを意識すべきです。

IPA

Microsoft 社 Internet Explorer のサポート終了について

最終更新日：2021年8月18日

概要

2022 年 6 月 16 日（日本時間）に Microsoft 社の Internet Explorer（以下、IE）のサポートが終了します。 サポート終了後に IE を起動しようとすると、Microsoft Edge が起動するよう変更されます(※)。 そのため、IE のみで動作するよう作成されたコンテンツ（以下、IE コンテンツ）を IE で閲覧できなくなります。 IE コンテンツの利用者や提供者は、他のブラウザへの移行やコンテンツの改修等、速やかな対策の実施が求められます。

※ Windows Update が適切に行われている必要があります。

サポート終了の対象ソフトウェア製品は以下の通りです。

- 2022 年 6 月 16 日（日本時間）

Internet Explorer 11 デスクトップアプリケーション（SAC）
Windows 10 デスクトップ SKU（20H2 以降）
Windows 10 IoT（20H2 以降）

●5月発生のProjectWEB不正アクセス、被害は129組織に…富士通より続報

https://xtech.nikkei.com/atcl/nxt/news/18/10982/
https://xtech.nikkei.com/atcl/nxt/column/18/00001/05929/
https://pr.fujitsu.com/jp/news/2021/08/11.html

このニュースをザックリ言うと・・・

- 8月11日(日本時間)、富士通より、同社製プロジェクト情報管理ツール「ProjectWEB」にて5月に発生していた不正アクセス・情報流出(AUS便り 2021/06/01号参照)に関する調査結果が発表されました。

- 同社は5月6日に不正アクセスを認知しており、129のユーザー(組織)がツールに保存していた、組織のシステムに関する情報(構成する機器類等)、プロジェクト運営に関する資料(体制図、打合せメモ、作業項目一覧、進捗管理表、社内事務手続きに関する資料等)といった情報が流出したこと、その一部にユーザーおよび関係者の氏名・メールアドレス等の個人情報が含まれていたことを確認したとのことです。

- また、不正アクセスの際には、第三者が正規のID・パスワードを使用し、ツールの脆弱性を悪用したことにより、正常認証および正常通信によるログインに成功した可能性があるとしています。

AUS便りからの所感

- その後の8月20日付の報道によれば、多要素認証(MFA)が実装されておらず、一部ユーザーについては、「システム構成図・IPアドレス・機器のIDおよびパスワード等の情報」も流出していたとされています。

- また、アカウント情報が流出した経路は特定できていないとしており、別のWebサービス等から流出したパスワードが利用可能だった可能性も、またやはり脆弱性でパスワード含むアカウント情報が奪取された可能性も考えられます(5月時点では「管理者権限アカウントが侵害された」可能性も報じられていましたが、これも確定はしていない模様です)。

- 一般論ではありますが、重要な情報をクラウド上のサーバーに保存するにあたっては、多要素認証が利用可能か等を事前に可能な限り確認し、情報にアクセス可能な管理者から一般ユーザーまで全てのアカウント情報について、不正ログインされないよう管理を徹底する等を強く推奨致します。

- 一方で社内LAN上あるいはデータセンター上の自前のサーバーに保存するオンプレミス方式をとる場合も、決して全ての面でクラウドの利用より安全というわけではなく、システム構成次第ではひとたびの侵入に対し脆弱になる恐れがあることに注意し、UTMの設置等により、サーバー自体への攻撃の防御および情報流出の遮断を意識したネットワーク構成とすること等が重要です。

日経 XTECH

富士通「ProjectWEB」は脆弱性を悪用され情報流出か、被害企業・機関は計129に

鈴木 康太　日経クロステック／日経コンピュータ

2021.08.11

富士通は2021年8月11日、同社のプロジェクト情報共有ツール「ProjectWEB」が不正アクセスを受けた問題について、情報が流出した企業や機関が計129に及んだと発表した。同ツールの脆弱性を悪用されたことでIDとパスワードが流出し、不正アクセスにつながった可能性が高いことも明らかにした。

ProjectWEBはシステム開発などのプロジェクトにおいて、社内外の組織で情報をインターネット上で共有するためのツール。同ツールは富士通のデータセンターで稼働している。情報流出は2021年5月に判明し、これまで内閣官房内閣サイバーセキュリティセンター（NISC）や国土交通省、外務省、成田国際空港会社などが被害を公表していた。

富士通によると、流出した情報は顧客システムの機器に関する情報やプロジェクトの体制図、作業項目、打ち合わせメモ、進捗管理表など。一部には氏名やメールアドレスなどの個人情報が含まれていた。流出した情報の数などについては「非公表」（広報）とした。

●「サイバーセキュリティ経営可視化ツール」IPAより公開

https://www.itmedia.co.jp/news/articles/2108/18/news086.html
https://www.ipa.go.jp/security/economics/checktool/index.html
https://security-shien.ipa.go.jp/diagnosis/

このニュースをザックリ言うと・・・

- 8月17日(日本時間)、IPAより、サイバーセキュリティの実践状況を企業自身のセルフチェックで可視化するWebサービス「サイバーセキュリティ経営可視化ツール」が公開されました。

- 同ツールは、2017年にIPAと経済産業省が発表した「サイバーセキュリティ経営ガイドライン Ver2.0」に基づくもので、自社のサイバーセキュリティ対策状況を定量的に把握し、サイバーセキュリティに関する方針の策定、適切なセキュリティ投資計画の策定等を行うためのものとされています。

- サイバーセキュリティ経営について「経営者がサイバーセキュリティリスクを経営リスクの1つとして認識している」「経営者が、組織全体としてのサイバーセキュリティリスクを考慮した基本方針を策定し、宣言している」等を問う39問を含む、計47問の設問からなっています。

AUS便りからの所感

- 同ツールは2020年3月にExcelファイルによるベータ版が公開され、ユーザーからのリクエストを基に今回Web上からでも利用可能となったものとされています(Excel版も更新が行われ、こちらも引き続き利用可能です)。

- 利用者登録により、過去5回の診断結果を保存することができますので、設問に対し、是非とも組織における現状に基づいた正確な内容を回答し、また改善に努めた結果についても後日改めて回答の上で、比較して頂ければ幸いです。

ITmedia NEWS

IPA、企業のセキュリティ診断ツール無料公開　Webブラウザでセルフチェック

2021年08月18日 11時45分 公開　[荒岡瑛一郎，ITmedia]

印刷　103　Share　B! 4

情報処理推進機構（IPA）は8月17日、情報セキュリティ対策の実施状況を企業がセルフチェックできる無料Webサービス「サイバーセキュリティ経営可視化ツール」を公開した。47問の設問に答えると、対策状況を自動で診断して5段階で評価する。同業種との比較や、改善に向けた参考情報も確認できる。

サイバーセキュリティ経営に関する設問は全39問で、5つの選択肢から答えを選ぶ。設問の内容は「経営者がサイバーセキュリティリスクを経営リスクの一つとして認識している」「重要業務を行う端末・サーバ等には複数の技術的防御策を実施している」など。用語解説や判断基準を載せた「回答のヒント」も用意している。