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。

●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/alert20241217.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17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、今回は特に企業や組織の利用者・管理者への注意喚起として、インターネットに接続された機器・装置類の脆弱性を悪用する「ネットワーク貫通型攻撃」が相次いでいることを挙げています。

AUS便りからの所感等

- 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、毎回の注意喚起で挙げられているセキュリティ対策の内容は大きく異なるようなものではありません。

- ネットワーク貫通型攻撃に関しては、「情報の漏えいや改ざん、ランサムウェアへの感染に加え、不正な通信の中継点とされてしまう」被害も予想されるとしており、こういった攻撃が特に管理者不在とみられる隙を突いて行われる可能性を鑑み、事前の監視体制、あるいは万一間に合わずとも事後のログ監査等の体制を確実に整備すべきでしょう。

- この他、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」についてもやはり内容が頻繁に更新されるものではなく、「長期休暇における情報セキュリティ対策」と同様に各人が目を通し、常日頃において準備・点検を行うよう意識していくこともまた肝要です。

IPA 独立行政法人 情報処理推進機構

2024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：2024年12月17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.）

被害に遭わないためにもこれらの対策の実施をお願いします。

● NTLMv1認証、Windows 11 24H2で削除…v2も6月に非推奨と発表済み

https://forest.watch.impress.co.jp/docs/news/1647735.html
https://forest.watch.impress.co.jp/docs/news/1597143.html
https://learn.microsoft.com/en-us/windows/whats-new/removed-features

このニュースをザックリ言うと・・・

- 12月9日(現地時間)、マイクロソフト(以下・MS)による「Features and functionality removed in Windows client(Windows クライアントで削除された機能と機能)」の情報が更新され、Windowsサーバー・クライアント間のファイル共有で使用されていた古い認証形式であるNTLMv1認証がWindows 11 24H2で削除されたことが記載されています。

- MSは6月3日の時点で、NTLMv1の他、より新しいNTLMv2も含めたNTLM認証全般を「非推奨」とすることを発表しており、NTLMv2も今後削除される可能性があるとして、Kerberos認証の使用を推奨しています。

- NTLMv1認証が導入されたのはWindows NT 3.1、NTLMv2もNT 4.0 SP4(1998年リリース)での導入であり、MSではもはやアクティブな開発が行われていないこと等を非推奨の理由としています。

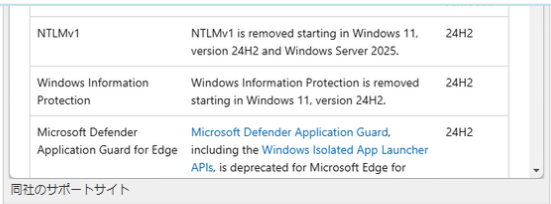
AUS便りからの所感

- 今日一般的な環境でNTLMv2の代わりにNTLMv1が必要となることは皆無であり、今回のNTLMv1の削除自体が大勢に影響しないはずでしたが、Windows 11 24H2へのアップグレードにより、ファイルサーバー等へアクセスできなくなったという報告が散見されており、ID・パスワードが不要なゲストアクセスがデフォルトで制限されたことが原因とされています(ゲストアクセスを可能にする回避策は提示されています)。

- やはりファイル共有で使用されるプロトコルSMBでも、Windows 10において古いSMBv1がセキュリティ上の問題から無効化された際、SMBv1にしか対応していない古いファイルサーバーにアクセスできなくなるトラブルが多く報告された経緯があります(こちらも回避策は公式に提示されています)。

- NTLMから移行が推奨されているKerberos認証はActive Directoryのドメイン環境でのみ利用可能であり、家庭や小規模な組織等のワークグループ環境では利用できないことを鑑み、今後もNTLMv2は削除されずともデフォルトで無効化されることが考えられ、管理者においてはこういった情報や回避策を事前に調査し、あるいはクライアント・サーバー側双方で設定を行うことが求められるでしょう。


「NTLMv1」は削除済み機能に、「Windows 11 バージョン 24H2」「Windows Server 2025」で
全バージョン非推奨、IT管理者は脱「NTLM」を
樽井 秀人　2024年12月17日 06:45



NTLMv1	NTLMv1 is removed starting in Windows 11, version 24H2 and Windows Server 2025.	24H2
Windows Information Protection	Windows Information Protection is removed starting in Windows 11, version 24H2.	24H2
Microsoft Defender Application Guard for Edge	Microsoft Defender Application Guard, including the Windows Isolated App Launcher APIs, is deprecated for Microsoft Edge for	24H2

同社のサポートサイト

今年10月にリリースされた「Windows 11 2024 Update」（バージョン24H2）では、「NTLMv1」が削除されているとのこと。米Microsoftが12月9日、自社のサポートサイトで公開しているWindowsクライアントから削除された機能リストをアップデートした。「Windows Server 2025」にも含まれていない。

● 11月度フィッシング報告件数は178,593件、サイトURL件数共々歴代2位に

https://www.antiphishing.jp/report/monthly/202411.html

このニュースをザックリ言うと・・・

- 12月16日(日本時間)、フィッシング対策協議会より、11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。

- 11月度の報告件数は178,593件で、10月度(https://www.antiphishing.jp/report/monthly/202410.html)の181,443件から2,850件減少しています。

- フィッシングサイトのURL件数は77,109件で10月度(71,367件)から5,742件増加、悪用されたブランド件数は94件で10月度(88件)から6件増加となっています。

- ブランド別で最も多いAmazonを騙るフィッシングの割合は全体の約22.9%と減少、次いで10,000件以上の報告を受けたJCB、マスターカード、えきねっと、PayPayと合わせて約57.1%、さらに1,000件以上報告された24ブランドまで含めると約94.0%を占めたとのことです。

AUS便りからの所感

- 報告件数は、過去最多を更新した10月度に次ぐ歴代2位となり、フィッシングサイトのURL件数も9月度の一時的な減少を経て、こちらも8月度の85,768件に次ぐ歴代2位となっています。

- フィッシングサイトで使用されるTLD(トップレベルドメイン名)の割合は .com(約42.5%)、.cn(約36.4%)が10%超えで2トップの状況が続いており、中華系によるフィッシングが長らく大勢を占めていると推測されます(その他の国のドメイン名が使われるケースも決して見過ごせる規模ではありませんが)。

- DMARC(SPF・DKIMでの検証に失敗したメールの取り扱いの指定)のポリシーがnone(特に指定しない)になっているドメイン名のメールについては、NTTドコモが10月以降、警告を出す措置をとっている(5月22日発表、https://www.docomo.ne.jp/binary/pdf/info/news_release/topics_240522_00.pdf)ことを取り上げており(GMailでは現時点で許容されています)、まだnoneに設定している場合は、自ドメインになりすますメールがどれだけ送られているかをDMARCのレポート機能で把握した上で、quarantine(迷惑メールフォルダー等への隔離)あるいはreject(受信拒否)への移行を計画すべきでしょう。