— AUS（アルテミス・ユーザ・サポート）便り 2024/1/24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。

● Googleが10月に発表した「メール送信者のガイドライン」、2月より適用開始…SPF・DKIM・DMARCその他の適切な設定、運用を

https://support.google.com/mail/answer/81126?hl=ja

このニュースをザックリ言うと・・・

- 2023年10月にGoogleが発表した「メール送信者のガイドライン」について、2月以降適用が開始される予定となっています。

- ガイドラインでは個人のGMailアカウント、即ち@gmail.com(および @googlemail.com)宛に、特に1日あたり5,000通以上のメールを送信する相手に対し「1. 送信メールを認証すること」「2. 未承諾のメールまたは迷惑メールを送信しないようにすること」「3. 受信者がメールの配信登録を容易に解除できるようにすること」を義務付けるとしています。

- 1. についてはSPF(メール送信に使用するサーバー・IPアドレスの申告)・DKIM(メールデータに対する署名)・DMARC(SPF・DKIMでの検証に失敗したメールの取り扱いの指定)等の設定、2. については迷惑メール率を一定の割合未満に抑えること、3. についてはマーケティング目的等のメールについてワンクリックで配信解除できる機構を用意し、メールヘッダーにリンクを記載すること(および解除リクエストは2日以内に処理すること)を挙げています。

- 大手メールサービスでは米Yahoo!も2023年10月に同様のガイドラインを発表し、2024年第一四半期に適用を予定しています(Yahoo! JAPANについてはまだ発表はありません)。

AUS便りからの所感等

- 要件は「1日あたり5,000通以上」の場合とそれに限らないものがあるとはいえ、最大手のメールサービスであり、顧客ユーザーが利用している可能性は決して皆無ではなく、一通りの対応があらゆる組織において必須となるとみられます(これはGmail以外を利用する相手も含め、なりすましメールから保護することに繋がり得ます)。

-メールサーバーを提供するレンタルサーバー・ドメインサービスを契約して運用する組織も多いと思われますが、事業者によって特にDKIM・DMARCの対応状況は依然まちまちであり、1月末に提供が開始されるケースもある等しており、利用しているサービスでの状況や自前で取るべき対応の有無について調査、取りまとめる必要があるでしょう。

- また2. について、自組織ドメイン名での迷惑メール率を上げないためには、マルウェアや不正アクセスによる内部ネットワークからのなりすましメールを送信されないようにすることも考慮が必要であり、個々のPCへのアンチウイルスの導入はもちろん、メールサーバーやUTMによる不審なメールの送信を阻止する機構も検討に値します。

● IPA、「情報セキュリティ10大脅威 2024」公開…個人・組織とも顔ぶれは昨年同様

https://www.ipa.go.jp/security/10threats/10threats2024.html

このニュースをザックリ言うと・・・

- 1月24日(日本時間)、IPAより「情報セキュリティ10大脅威 2024」の概要が発表されました。
- 2023年に発生した、社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、IPAが脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者等約200名によって、個人と組織それぞれのカテゴリーでの10大脅威を決定しています。
- 今回、「順位が高い脅威から優先的に対応し、下位の脅威への対策が疎かになることを懸念」し、個人向け脅威については順位付けは行っておらず、「順位に関わらず自身に関係のある脅威に対して対策を行う」ことを期待しているとのことです。
- 今後、2月下旬に10大脅威に関する詳細の解説書が発表される等、追加コンテンツが随時公開される予定となっています。

AUS便りからの所感

- 個人・組織各カテゴリーとも挙げられた脅威は全て昨年と同様、かつ過去に2回以上登場したものとなっており、組織向け脅威のランキングは1・2位は昨年同様「ランサムウェアによる被害」「サプライチェーンの弱点を悪用した攻撃」、また3・4位は昨年と順位が入れ替わって「内部不正による情報漏えい等の被害」「標的型攻撃による機密情報の窃取」となっています。
- 12月にはJNSAから「2023セキュリティ十大ニュース(https://www.jnsa.org/active/news10/)」も発表されており、年末年始や半期・四半期において、大手セキュリティベンダーや関連団体等から、各組織の立ち位置・観点等の違いを少なからず反映した年間のセキュリティ関連ニュースのまとめ、あるいは翌年度等における業界の動向予測等がリリースされますので、自分自身や自組織に関連するもの以外であっても各種脅威について知識を得る、あるいは以前に得た知識が正しいかの再確認をし、今後の行動に役立てるのが良いでしょう。


情報セキュリティ10大脅威 2024

公開日：2024年1月24日
最終更新日：2024年1月24日

「情報セキュリティ10大脅威 2024」は、2023年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、IPAが脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者など約200名のメンバーからなる「10大脅威選考会」が脅威候補に対して審議・投票を行い、決定したものです。
10大脅威 2024では、個人の10大脅威の順位は掲載せず、五十音順で並べています。これは、順位が高い脅威から優先的に対応し、下位の脅威への対策が疎かになることを懸念してのことです。順位に関わらず自身に関係のある脅威に対して対策を行うことを期待しています。

情報セキュリティ10大脅威 2024 [個人]

「個人」向け脅威（五十音順）	初選出年	10大脅威での取り扱い（2016年以降）
インターネット上のサービスからの個人情報の窃取	2016年	5年連続8回目
インターネット上のサービスへの不正ログイン	2016年	9年連続9回目
クレジットカード情報の不正利用	2016年	9年連続9回目
スマホ決済の不正利用	2020年	5年連続5回目
偽警告によるインターネット詐欺	2020年	5年連続5回目
ネット上の誹謗・中傷・デマ	2016年	9年連続9回目
フィッシングによる個人情報等の詐取	2019年	6年連続6回目

● 「あなたのスマホにウイルスが…」IPA騙る電話に注意喚起

https://www.itmedia.co.jp/news/articles/2401/12/news094.html
https://www.ipa.go.jp/news/2023/announce/ex20240111.html

このニュースをザックリ言うと・・・

- 1月11日(日本時間)、情報処理推進機構(IPA)より、同組織を騙る不審な電話が確認されたとして注意喚起が出されています。
- 注意喚起によれば、電話は「あなたのスマートフォンにウイルスが入っているため情報処理推進機構で解析をしている」といった虚偽の説明を行い、金銭を要求するとされています。
- IPAでは、個人のスマートフォン等を解析したり、それに対し金銭支払いが発生するということは一切ないとしており、不審な電話を受けた場合はIPA情報セキュリティ安心相談窓口や警察署まで連絡するよう呼び掛けています。

AUS便りからの所感

- 挙げられている不審な電話の例としては、この他にも政府機関や弁護士事務所の名前を騙ったり、「個人情報なので誰にも相談しないように」等と口止めを図るものもある模様です。
- フィッシングやサポート詐欺等、金銭や個人情報を詐取しようとする手口はIPAやセキュリティ関係組織等から度々報告されていますが、今回の手口がたとえWeb・メール・SMSを利用しない特殊詐欺(振り込め詐欺)の一種であったとしても決して油断せず、普段からどんな攻撃・詐欺の手口が行われているかの情報収集を行いつつ慎重に行動することが重要です。


「あなたのスマホのウイルスを解析中」IPA装う不審な電話に注意

2024年01月12日 09時31分 公開　[ITmedia]

「あなたのスマートフォンにウイルスが入っているため、情報処理推進機構（IPA）で解析をしている」などとかたり、金銭を要求する不審な電話が確認されているとして、IPAが注意を呼び掛けている。

IPAは「個人の方のスマートフォンなどを解析して金銭支払いが発生するということは一切ない」としている。

情報処理推進機構（IPA）を騙った不審な電話等にご注意ください

公開日：2024年1月11日

「あなたのスマートフォンにウイルスが入っているため情報処理推進機構で解析をしている」等の虚偽の説明を行い、金銭を要求する不審な電話が確認されています。また、その際、政府機関や弁護士事務所の名前をかたり、あたかも国や弁護士が対応しているような虚偽説明を行ったり、「個人情報なので誰にも相談しないように」と言い含めるなど、不安を煽って巧妙にだます手口を確認しています。