

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。

●総務省よりフィッシングメール対策強化要請…生成AIによる巧妙化懸念

<https://www.itmedia.co.jp/news/articles/2509/01/news115.html>
https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000260.html
<https://www.npa.go.jp/bureau/safetylife/sos47/new-topics/250609/01.html>
https://www.antiphishing.jp/report/wg/cert_20250916.html



このニュースをザックリ言うと…

- 9月1日(日本時間)、**総務省**より、**電気通信事業者**に対し**フィッシングメール対策の強化**を行うよう、**4事業者団体**(電気通信事業者協会・テレコムサービス協会・日本インターネットプロバイダー協会・日本ケーブルテレビ連盟)を通じて要請したことが発表されました。
- 4月22日の犯罪対策閣僚会議で決定された「**国民を詐欺から守るための総合対策2.0**」に基づくもので、「詐欺メール、詐欺SMSによる被害防止等のための取組」として「**送信ドメイン認証技術(DMARC等)への更なる対応促進**」を掲げているとしています。
- 証券会社を騙るフィッシングメール等による顧客情報の窃取～不正取引被害の急増、またフィッシングメールにおいては**生成AIによる自然な日本語等の精巧な内容**のものが**大量かつ容易に送付**できるようになっているとし、**より効果的な対策に取り組むことを要請**したとしています。

AUS便りからの所感等

- 要請では、事業者に対し2025年9月～2026年8月末までにおいて、メールの**フィルタリング精度の積極的な向上**・**DMARCの導入**および**隔離(p=quarantine)～拒否(p=reject)ポリシー**の設定・**様々な利用者層に向けた対策サービスの周知啓発**の大きく3点について3ヶ月ごとに取組状況を報告するよう依頼しています。
- 2024年のGMailによる「メール送信者のガイドライン」等を受けてDMARC(およびSPF・DKIM)の導入が進んでおり、9月16日にフィッシング対策協議会から発表された、**国内ISP・CATV・モバイル事業者およびフリーメール事業者におけるSPF・DKIM・DMARC等の対応状況**では、**2024年におけるDMARC導入状況は74.4%**(SPFは99.0%、DKIMは78.5%)とされています。
- DMARC等の送信元チェック機構に留まらないフィルタリング機構についても要請があり、**迷惑メール判定の側においてもAIを活用**すること等が提案されており、今後の展開が注目される一方、**正当なメールを教育した結果が第三者と共有された場合、そこから機密情報が漏洩する恐れがないか、等にも注意が払われるべき**でしょう。



生成AIで巧妙化するフィッシングメール 総務省、DMARC導入など対策強化を業界に要請

© 2025年09月01日 17時01分 公開

[ITmedia]

総務省は9月1日、フィッシングメール対策への対策を強化するよう、IT関連の業界4団体に要請した。フィルタリング精度の向上や送信ドメイン認証(DMARC)の導入などを進め、2026年8月末まで、3カ月ごとに進捗を報告するよう求めている。

総務省は、「生成AIを使って自然な日本語を大量に生成できるようになり、これまで以上に精巧なフィッシングメールの送付が容易となっている」と指摘。ここ最近では、証券会社をかたったフィッシングメールによる不正取引が急増するなど被害が深刻化する中、より効果的な対策を求めた。

要請内容は、AIを活用するなどしてメールフィルタリング精度を向上させ、高度化するフィッシングメールへの対応を目指すことと、送受信ともにDMARCを導入し、適切なポリシーを策定すること、フィッシングメール対策サービスの周知・啓発を行うこと。

(公印及び契印省略)

別紙

総基用第76号
令和7年9月1日

一般社団法人電気通信事業者協会会長 島田 明 殿
一般社団法人テレコムサービス協会会長 是枝 周樹 殿
一般社団法人日本インターネットプロバイダー協会会長 久保 真 殿
一般社団法人日本ケーブルテレビ連盟会長 塩谷 憲司 殿

総務省総合通信基盤局長
湯本 博信

フィッシングメール対策の強化について(要請)

平素より、情報通信行政に御理解と御協力をいただいておりますことに、厚く御礼申し上げます。

フィッシングメール対策について、政府は、「国民を詐欺から守るための総合対策2.0(令和7年4月22日犯罪対策閣僚会議決定)」において、「詐欺メール、詐欺SMSによる被害防止等のための取組」として、「送信ドメイン認証技術(DMARC等)への更なる対応促進」を掲げているところです。

最近では、実在する証券会社を装ったフィッシングメール等から窃取した顧客情報(ログインIDやパスワード等)によるインターネット取引サービスでの不正アクセス・不正取引(第三者による取引)の被害が急増しています。

貴法学会員事業者においても、従前よりフィッシングの被害防止に向けて、送信ドメイン認証技術の導入を含め、様々な対策を推進いただいているものと承知しておりますが、生成AIを用い、自然な日本語を大量に生成できるようになり、これまで以上に精巧なフィッシングメールの送付が容易となっている中、こうしたフィッシングメールへの更なる対策が求められるところです。つきましては、より効果的な対策に取り組んでいただきますよう、下記の3点について、貴法学会員事業者への周知いただきますようお願い申し上げます。

●警察等を騙り「逮捕状」表示…広島県警が注意喚起

<https://www.yomiuri.co.jp/local/kansai/news/20250829-OYO1T50017/>
<https://www.pref.hiroshima.lg.jp/site/police/hayarinoteguchi.html>



このニュースをザックリ言うと…

- 8月29日(日本時間)、読売新聞オンラインにて、**地方の警察本部の偽サイトに誘導する特殊詐欺の事例**が報じられています。
- 記事は**広島県警察本部からの注意喚起**を受けてのものとして、**大阪府警や検察官を騙る電話から府警の偽のWebサイトに誘導、逮捕状の画像を提示**され、800万円を騙し取られたとする4月に発生した事例が取り上げられています。
- 偽の逮捕状を提示する**手口は全国で出現**しているとされ、また広島県警本部のWebサイトでも同様の手口について取り上げており、「**警察はSNSやビデオ通話で絶対に連絡しません**」「**ホームページで逮捕状を公開することはありません**」としています。

AUS便りからの所感

- 記事で取り上げられた手口は、偽の府警がLINEのビデオ通話に誘導した上で**被害者本人の名前が記載された逮捕状**を提示、その後偽の検察官からの電話にかけ直したところさらに**偽の府警サイトに誘導**、検索画面で**生年月日を入力**したところ**再度同様の逮捕状が提示**される、という二段構えで相手を信じ込ませていた模様です。

- このような大掛かりなものでなくとも、詐欺を行われるにあたり**こちらの名前や生年月日を把握**されていることは**心理的動揺を誘うに十分**でしょうが、くれぐれも**世の中で使われる手口の情報を十分に収集し、慎重に行動**することが重要です。

- この手の詐欺では表示される電話番号が+1(アメリカ)、+44(イギリス)等で始まる**国際電話が用いられる頻度が高いもの**、**全てのケースでそうとは限らない**ことにも注意が必要で、不審な相手からかかってきた**電話番号について可能な限りサーチエンジンで検索**し(専用のサイトも複数存在します)、警察を名乗る相手に対しては**その電話番号にかけ直さず**、確認したい場合は**実際の警察の番号を調べ**て**そちらにかけ**る等の自衛策をとるのが良いでしょう。

YOL 読売新聞 オンライン

生年月日を入力すると「あなたの逮捕状」...警察本部の偽ホームページに誘導する新手口

2025/08/29 11:50

📌 保存して後で読む 📱 📧 📺 📻

警察官を名乗ったうえで「逮捕状が出ている」などと脅し、金をだまし取る特殊詐欺事件をめぐり、警察本部のホームページ(H P)とそっくりな偽H Pに誘導して信じ込ませる新たな手口が、広島県内でも確認されている。巧妙な手法に県警は注意を呼びかけている。



発表によると、県内に住む女性の携帯電話に4月、「大阪府警」を名乗る男から国際電話があり「ある男を資金洗浄の疑いで逮捕したところ、あなた名義のキャッシュカードが出てきて、共犯者として名前が挙がっている」と告げられた。LINEのビデオ通話に誘導され、女性の名前が記された「逮捕状」と書かれた画像

が送られてきた。

●Microsoft・Adobe等月例のセキュリティアップデート

<https://forest.watch.impress.co.jp/docs/news/2046104.html>
<https://msrc.microsoft.com/blog/2025/09/202509-security-update/>
<https://forest.watch.impress.co.jp/docs/news/2046107.html>
<https://forest.watch.impress.co.jp/docs/news/2046101.html>
<https://forest.watch.impress.co.jp/docs/news/2046898.html>



このニュースをザックリ言うと…

- 9月10日(日本時間)、**マイクロソフト**(以下・MS)より、**Windows・Office等同社製品**に対する**月例のセキュリティアップデート**がリリースされています。

- Windowsの最新バージョンはWindows 10 22H2 KB5065429(ビルド 19045.6332)、11 23H2 KB5065431(ビルド 22631.5909)および11 24H2 KB5065426(ビルド 26100.6584)等となります。

- その他**Adobe**社より**Acrobat(およびAcrobat Reader)・Premiere Pro等9製品**についてセキュリティアップデートが、**Google**社より**Chrome**ブラウザの**週例アップデート**となるv140.0.7339.127/128(Windows版)がリリースされています。

AUS便りからの所感



- MSの月例アップデートでは**Exchange Server**に関する脆弱性(CVE-2025-33051)が**既に攻撃手法が公知**となっており、Windows・Office・Hyper-V等の脆弱性8件が特に危険度が高い(4段階中最高の「Critical」)と評価されています。

- Chromeの更新で修正された脆弱性は、Edgeブラウザでも同12日にリリースされたv140.0.3485.66で対応されています。

- **10月の「パッチチューズデー」**は日本時間で**15日**、また**22日**にも**Oracle**社から**四半期に一度のパッチリリース**(Java等)がある等、特にシステム管理者においては**リリーススケジュールに基づくアップデート計画**を立てるとともに、パッチの展開・適用完了までに発生し得る攻撃に対し**アンチウイルス・UTM等による防衛**を怠りなく実施することが肝要です。

Microsoft、2025年9月の「Windows Update」を実施 ~深刻度最高の脆弱性は8件

グラフィックス カーネルや「Office」、「Hyper-V」などでリモートコード実行のおそれ

橋井 秀人 2025年9月10日 09:35

米Microsoftは9月9日(現地時間)、すべてのサポート中バージョンのWindowsに対し月例のセキュリティ更新プログラムをリリースした(パッチチューズデー)。現在、「Windows Update」や「Windows Update カタログ」などから入手可能。Windows以外の製品も含め、今月のパッチではCVE番号ベースで80件の脆弱性が新たに対処されている。

このうち、すでに攻撃手法が明らかになっているゼロデイ脆弱性は、以下の1件。

- CVE-2025-33051 : Microsoft Exchange Server の情報漏えいの脆弱性