2025 年 1 月 29 日
デジタルアーツ株式会社

PRESS RELEASE

【セキュリティレポート】国内組織の受信メール添付ファイルを分析
ZIP ファイル割合は 5 年前と比較し半減するも、
調査対象の 2 週間で 6,000 以上のドメインがパスワード付き ZIP を利用

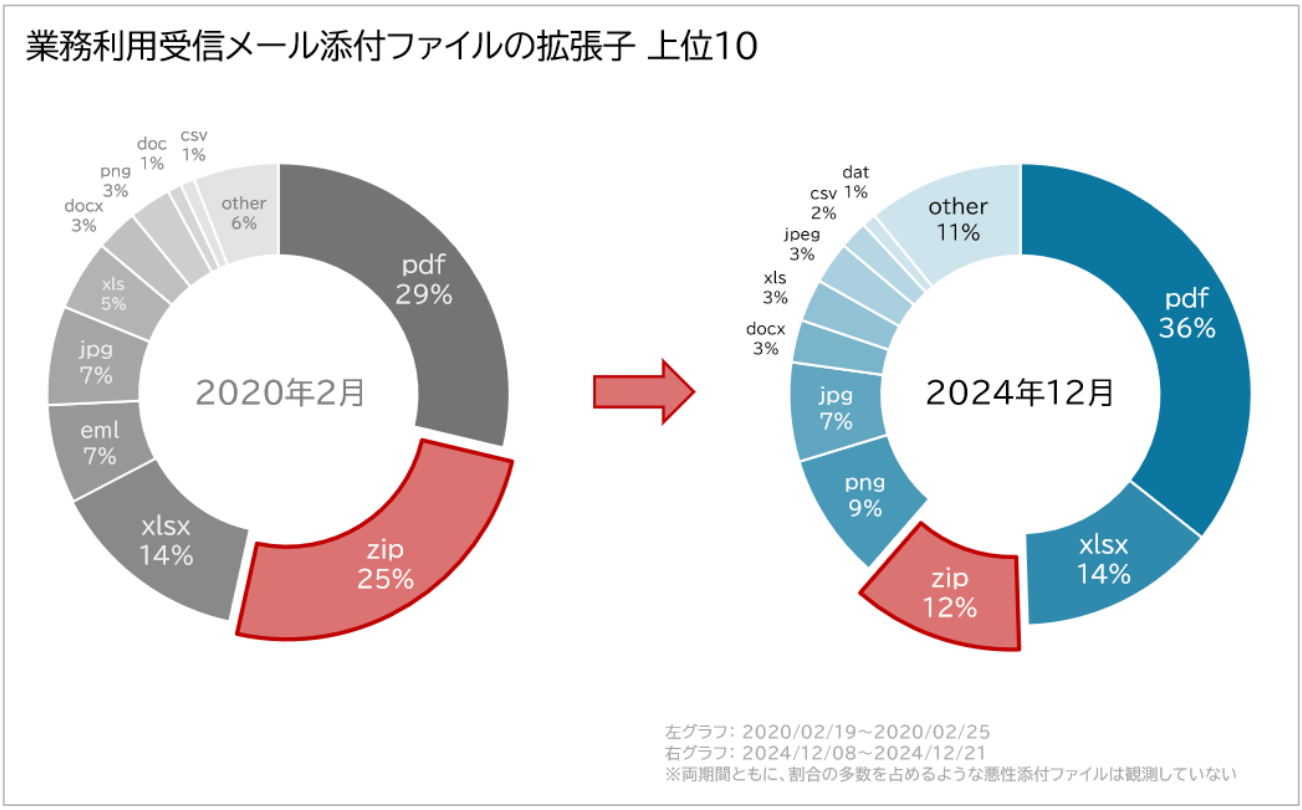
情報セキュリティメーカーのデジタルアーツ株式会社（本社：東京都千代田区、代表取締役社長：道具　登志夫、以下 デジタルアーツ、証券コード 2326）は、国内組織の業務利用受信メールデータを用いて、「何らかのファイルが添付された受信メール」を抽出し、添付ファイルの「拡張子」を集計、分析したセキュリティレポートを公開しました。

国内 2,000 組織、約 300 万通以上のメールを分析

今回の調査※1 は国内の約 2,000 組織を対象とし、「受信メールに何らかのファイルが添付されたもの」に限定し抽出した 300 万通以上の受信メールのデータを基に算出し拡張子の種類を分析しました。その結果、2020 年に集計した同様の調査※2 と比較した際、約 5 年（4 年と 10 か月）で**「ZIP ファイル」の添付割合が半減している**ことがわかりました。

・2020 月　2 月調査…　　25%
・2024 年 12 月調査…　　12%

双方の集計期間において悪性の添付ファイルが多数を占めているといった状況は見られず、業務で利用されている添付ファイルの数と考えられます。



※1 …　調査対象

期間：2024/12/08～2024/12/21

対象：何らかのファイルが添付された受信メール 300 万通以上、2,000 組織以上（組織内メールは含まず）

※2 …　2020 年 2 月「業務利用受信メールの添付ファイル調査（https://www.daj.jp/security_reports/11/）

ZIP ファイル減少、背景には「脱 PPAP」

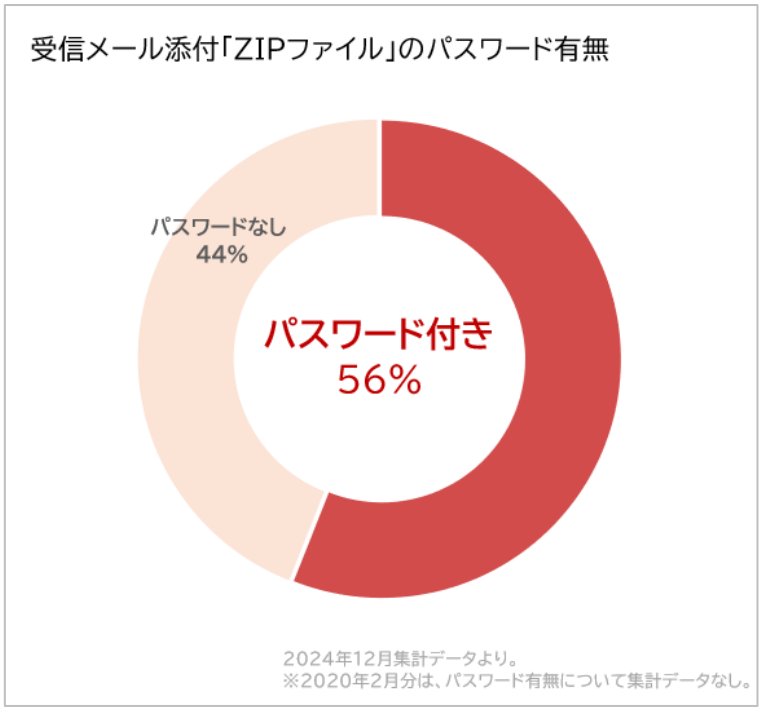
日本国内における多くの企業・団体で、メールファイルを送る際の「ZIP 暗号化」運用（PPAP）は慣例化されたものになっていました。PPAP は大容量、複数ファイルを圧縮し簡易に送信できる一方で、メールの盗聴リスクや ZIP 暗号化ファイルへのウイルスチェック機能の弱さなど、セキュリティリスクが指摘され続けていました。

そのような中で 2020 年、デジタル庁大臣による「中央省庁の職員が文書などのデータをメールで送信する際に使用する『ZIP 暗号化』ファイルを廃止する方針」の発表をきっかけに、その後民間企業においても相次いで廃止の方針を表明するなど、**「脱 PPAP」が日本中に定着していきました。**

現在では多くの企業で脱 PPAP を行い、その代替として、ファイル転送サービスの利用や、クラウドストレージのダウンロードリンクを記載して渡す方法、別のファイル（PDF など）へ変換して内部にダウンロードリンクを記載する方法など、様々な 運用方法へとシフトしており、日本の官民が一体となって推進した「脱 PPAP」の結果、ZIP ファイルのやり取りが減少したと考えられます。

PPAP の現状

今回の受信メール調査で算出された「12%の ZIP ファイル」を「パスワード付き」と「パスワード無し」に分けて分析すると、「パスワード付き ZIP ファイル」の割合は 56%となり、送信元のドメイン数は重複を除くと 6,000 以上存在していました。※3



「送信元ドメイン数」を組織数と仮定した場合、**今回集計した調査だけを見ても 6,000 以上もの組織が PPAP を行ってメールを送信している可能性や、その受信者である取引先がパスワード付き ZIP を受信しなくてはならないという状況が発生している**ことから、PPAP によるリスクを把握しきれていない企業や組織が一定数存在していることが想定されます。

メールセキュリティソフトの多くは「パスワード付き ZIP ファイル」の内部ファイルのウイルス・マルウェア検証まで行う機能を備えておらず、ファイルを開いてウイルスに感染してしまうリスク、受信者組織内で広めてしまうリスクは引き続き存在しています。

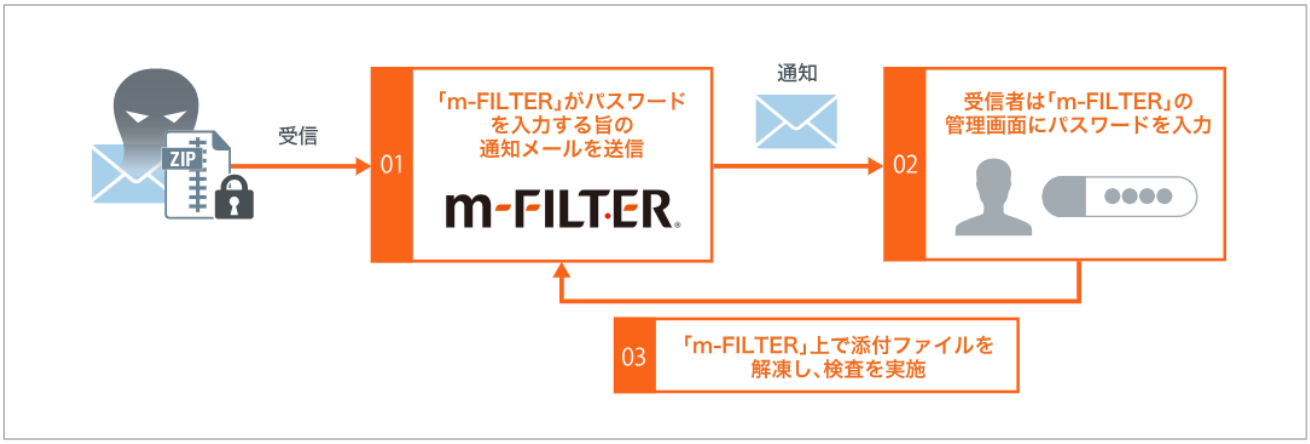
※3 … ZIP ファイルのパスワード有無については、デジタルアーツのメールセキュリティソフト「m-FILTER」の偽装メール対策機能の判定結果を用いて算出。

依然行われる圧縮ファイルを用いた攻撃

パスワード付き ZIP ファイルを用いたマルウェアとして猛威を振るった「Emotet」は 2023 年 3 月末ごろを最後に活動を停止しています。 以降、日本国内に向けたばらまき型攻撃メールについて大規模なものは見受けられないものの、圧縮ファイルを用いたばらまきメール型の攻撃は把握されています。また、このような攻撃手法は続々と新たなものが出てきていることから、送信、受信双方のメールセキュリティが重要になります。

デジタルアーツはこれらの圧縮ファイルを用いた攻撃や「PPAP」運用に対していち早く警鐘を鳴らし、メールセキュリティの「m-FILTER」による対策を提供してきました。メールセキュリティソフトの「m-FILTER」では「PPAP 問題」の抱える受信面、送信面双方の課題への対策が可能です。※4

当社では引き続き、セキュリティを通じて顧客の安全な IT 環境を守るため、新たな脅威への対策や調査研究、製品開発に努め、貢献してまいります。



パスワード付き ZIP の受信対策のイメージ（デジタルアーツ「m-FILTER」）

※4 … デジタルアーツの「脱 ZIP 暗号化」運用について（https://www.daj.jp/bs/lp/ppap/）

詳細のセキュリティレポートはこちら

以下、弊社コーポレートサイト上にて公開しております。詳細はこちらからご覧ください。

URL：https://www.daj.jp/security_reports/43/

■デジタルアーツの「ホワイト運用」

受信したすべてのメールを開け、アクセスしたい Web をクリックできる。情報システム部門の運用負荷も削減できる。デジタルアーツの「ホワイト運用」がセキュアな世界を実現します。全を確認した URL にのみアクセスを許可し未知の悪性 URL をブロックすることができます。

製品ページ：「i-FILTER」Ver.10 ・「m-FILTER」Ver.5 – セキュリティ対策の新定番 ホワイト運用

■参考情報

▶PPAP はなぜ危険？PPAP メールを廃止する理由と代替策

PPAP 運用の問題点を解説し、PPAP 運用を廃止することのメリットや問題点を解決する PPAP 運用の代替案をご紹介します。

URL：https://www.daj.jp/bs/lp/ppap/

▶DLP・ファイル転送サービス「f-FILTER」

重要情報が入ったファイルを確実に選別、セキュアな状態で正しい相手に受け渡しします。

URL：https://www.daj.jp/bs/f-filter/

▶ファイル暗号化ソフト 「FinalCode」(ファイナルコード)

重要ファイルを暗号化して、利用状況を追跡、遠隔削除もできる究極のファイルセキュリティです。ファイル暗号化による情報漏えい対策には、FinalCode をご活用ください。

URL：https://www.finalcode.com/

▶新オプション「Anti-Virus & Sandbox」のご紹介

デジタルアーツが提供する新オプション「Anti-Virus & Sandbox」は安全な Web サイト・メールからの安全なファイルのダウンロード・受信をリアルタイムに実現し、セキュリティレベルを向上させます。

URL：https://www.daj.jp/bs/lp/avsb/

デジタルアーツ株式会社　概要

Web、メール、ファイルなどのセキュリティソフトウェアの提供を核に事業展開する情報セキュリティメーカーです。
1995 年の創業以来、「より便利な、より快適な、より安全なインターネットライフに貢献していく」を企業理念とし、情報漏えい対策や標的型攻撃をはじめとするサイバー攻撃対策を実現する最先端の製品を、企業・官公庁・学校・家庭向けに提供しています。

東京都千代田区大手町 1-5-1 大手町ファーストスクエア　ウエストタワー14F　▶URL: https://www.daj.jp/
＜本リリースに関するお問い合わせ＞
　デジタルアーツ株式会社　広報課　関・宮内　　TEL　: 03-5220-1670／ E-mail : press@daj.co.jp