NTT DATA
Trusted Global Innovator

注目されているセキュリティ事故・事件に関する情報 ＜2020年12月版 (第35号)＞(選り抜き版)

2020年12月24日
ＮＴＴデータ先端技術株式会社
セキュリティ事業本部

今回のサマリー

パスワードで暗号化したファイルをメールで送付する運用を見直そう
2020年7月からマルウェア「Emotet」の感染被害が増加するに伴い、パスワードで暗号化したファイルをメールで送付するという運用は、続けるべきでないという意見が、政府機関、セキュリティ機関、メディアで多く見られるようになっています。Emotetに感染させるための手法の変化とパスワードで暗号化したファイルをメールで送付する運用の問題点について解説します。

パスワードで暗号化したファイルを
メールで送付する運用を見直そう

1. はじめに

　従来、権威あるセキュリティガイドラインなどで効果があるとされ、広く使われてきたセキュリティ対策であっても、その後の技術の進歩、社会状況の変化によって、「効果がない」もしくは「デメリットが大きい」と社会的な評価が変わり、組織のルールを見直す必要が生じることもあります。

　2020年7月よりJPCERT/CCへの相談が増加しているEmotetへの感染において、広く日本で使われている「パスワードで暗号化したファイルをメールで送付する(※1/※2)」というセキュリティ対策に対する社会的な評価が変わり、「効果がない」「見直すべきだ」という意見が政府機関(※3)、セキュリティ機関(※4)、メディアで多く見られるようになっています。

※1.パスワードで暗号化したファイルとは、例えばファイルをZip形式の圧縮ファイルへ変換する際にパスワードを設定し、パスワードが分からないと開くことができないようにしたファイルを指します。
※2.「パスワードで暗号化したファイルをメールで送付する」運用は、「PPAP」と揶揄された表現で呼ばれることがあります。

　P：Password付きファイルをメールで送信
　P：Passwordをメールで送信
　A：An号化（暗号化したつもりになる）
　P：Protocol

　なお名付け親はPPAP総研の大泰司章さんであるとされています。
※3.ITmedia：パスワード付きzip、内閣府と内閣官房で26日から廃止へ　外部ストレージサービス活用　平井デジタル相
　<https://www.itmedia.co.jp/news/articles/2011/24/news097.html>
※4.US-CERT：Alert (AA20-280A) Emotet Malware
　<https://us-cert.cisa.gov/ncas/alerts/aa20-280a>

2. Emotetとは

　Emotetは、第31号の「進化するマルウェア「Emotet」の脅威について」でも解説した通りマルウェアの一種です。
　JPCERT/CCの発表(※)によると、2019年10月から2020年1月まで日本国内での感染事例が相次いでいましたが、2020年2月以降Emotetの感染につながるメールの配布は観測されなくなりました。
　しかし、2020年7月に再度メールの配布が観測され、特に同年8月下旬以降は感染が相次いで報告されています。

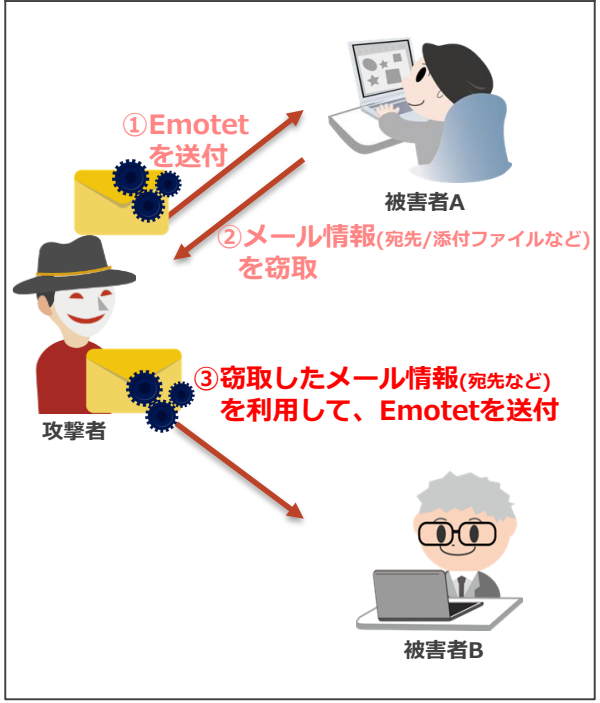
※JPCERT/CC「マルウエア Emotet の感染に繋がるメールの配布活動の再開について（追加情報）」
<https://www.jpcert.or.jp/newsflash/2020072001.html>

3. Emotetに感染させる手法の変化

企業内の啓発活動やウイルス対策ベンダの対応が進んでいるにもかかわらず、Emotetに感染する企業が急増している要因として、感染させる手法の変化(※)が挙げられます。

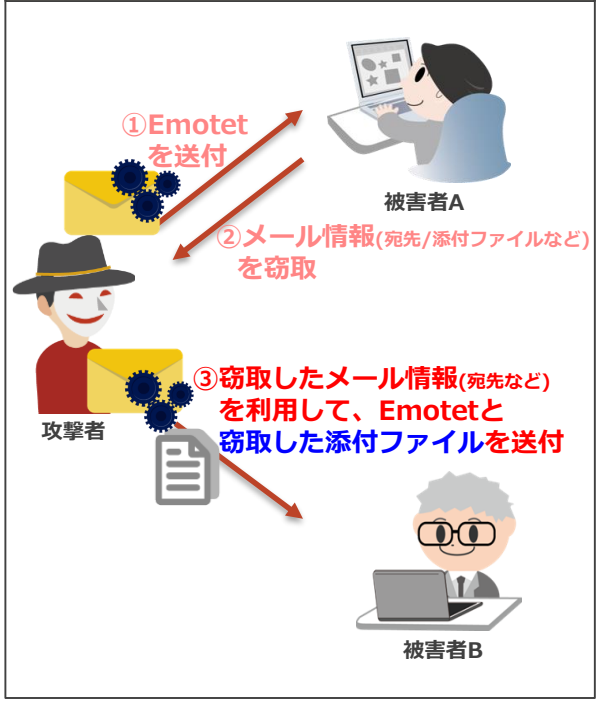
2020年6月以前

従来の手法
(Emotetのみを無加工で送付する手法)



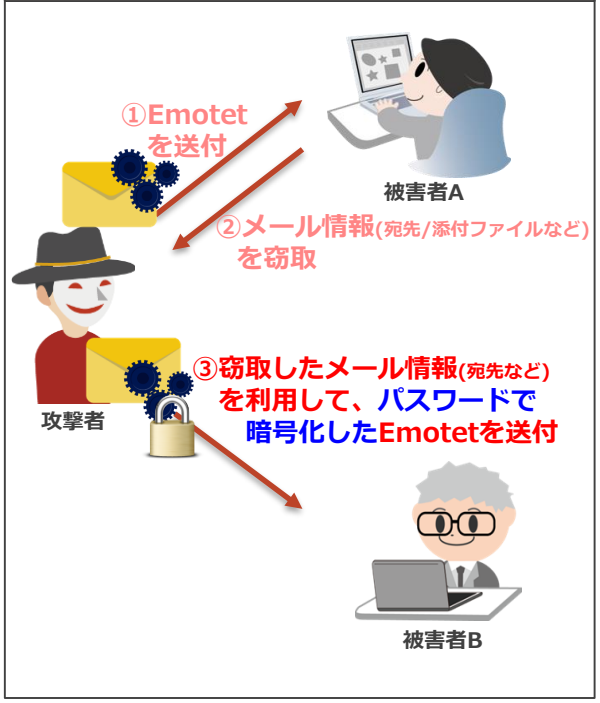
2020年7月~8月中旬

無害なファイルと共に
Emotetを送付する手法



2020年8月下旬以降

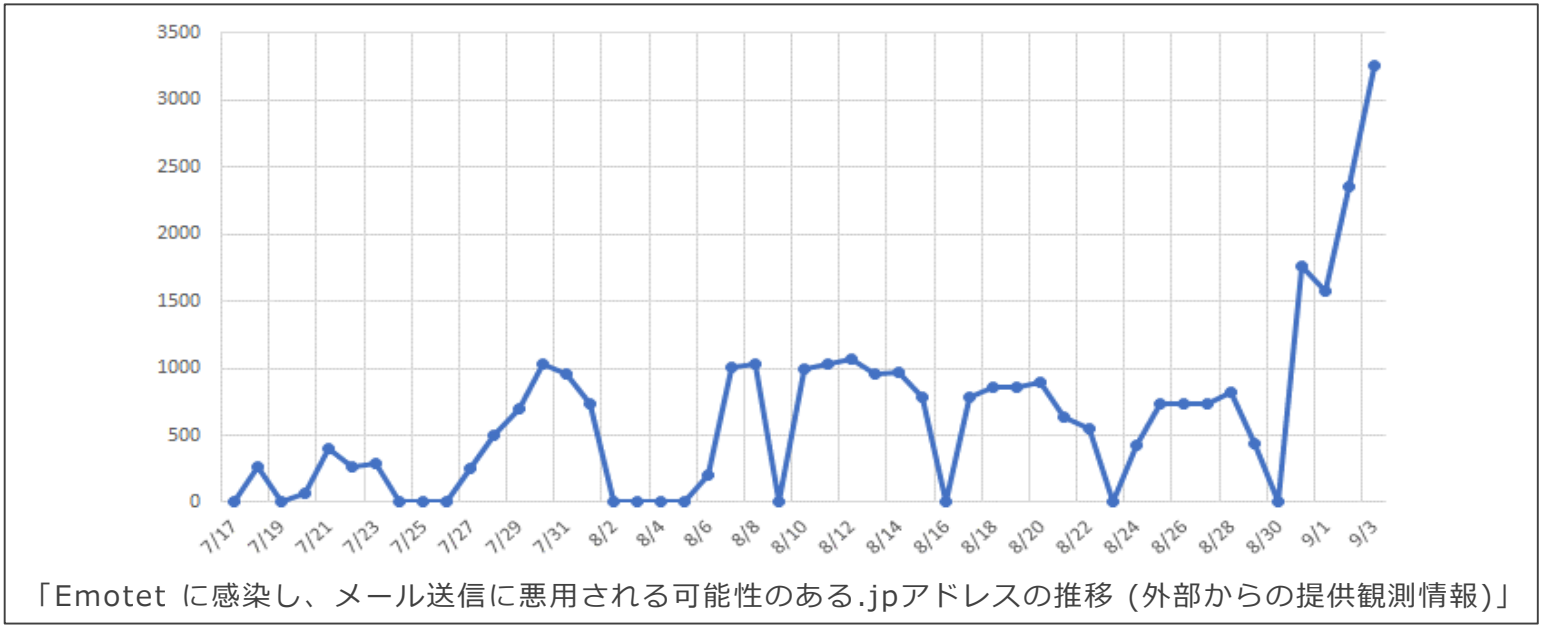
パスワードで暗号化した
Emotetを送付する手法



※変化前の感染手法が用いられなくなったわけではありません

4. Emotetへの感染増加の要因 (1/2)

パスワードで暗号化したEmotetをメールで送付する手法の登場(2020年8月下旬)はJPCERT/CCへの相談件数(※1)が急増したタイミングとリンクしており、この手法が今回の被害増加の要因になったと考えられます。パスワードで暗号化したファイルをメールで送付する運用は、セキュリティ対策として長く運用されてきました。それが、なぜ被害増加の要因となったのでしょうか？

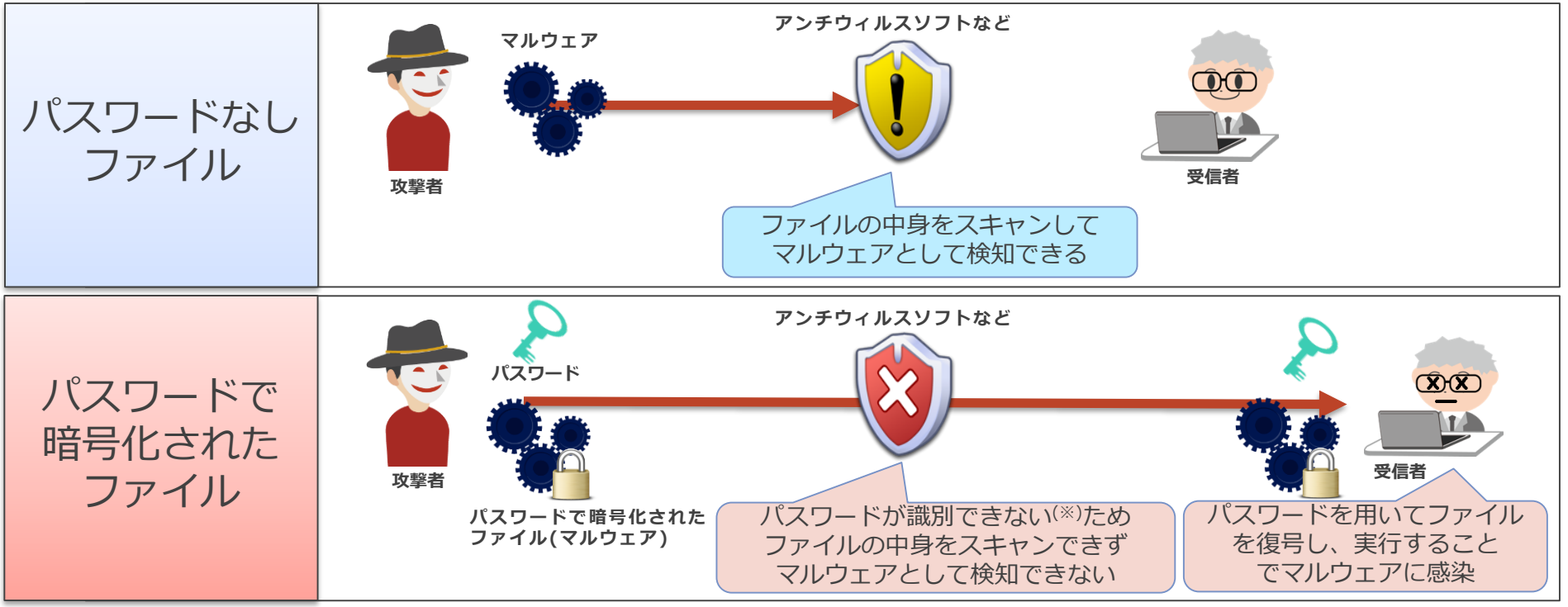


「Emotet に感染し、メール送信に悪用される可能性のある.jpアドレスの推移 (外部からの提供観測情報)」

※1.引用：JPCERT/CC「マルウェア Emotet の感染拡大および新たな攻撃手法について」
<https://www.jpcert.or.jp/newsflash/2020090401.html>
※2.パスワードで暗号化したファイルをメールで送付する手法は、2020年10月より感染が急増しているEmotetとは異なるマルウェアである「IcedID」においても用いられる手法であるとされています。

4. Emotetへの感染増加の要因 (2/2)

　要因として、受信者に「攻撃者はパスワードを掛けたファイルを送ってこない」という先入観や、「パスワードを掛けられた添付ファイルは安全である」という思い込みがあったことが挙げられます。どちらも誤りであり、特に後者については、アンチウィルスソフトはパスワードで暗号化されたファイルの中身をスキャンできず、パスワードで暗号化されたEmotetは検知・検疫されずに受信者に届くため、感染増加に直結する可能性すらある危険な思い込みです。

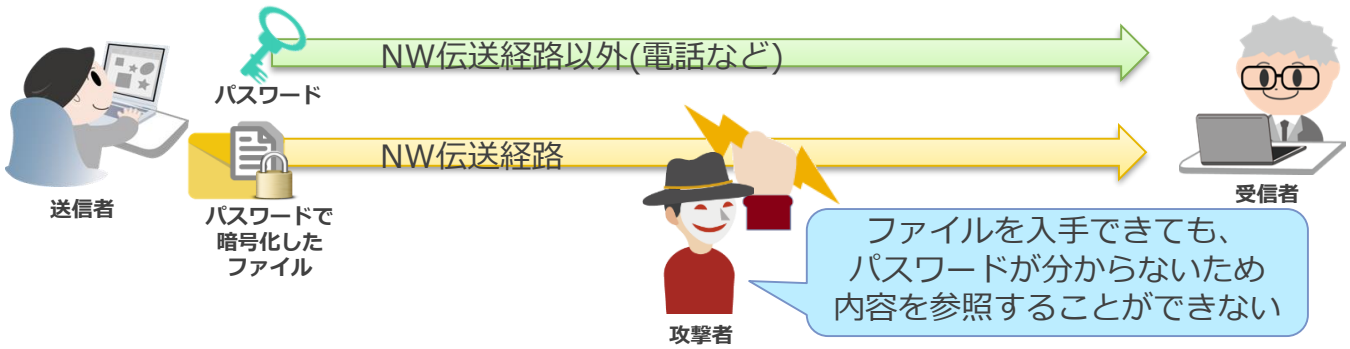
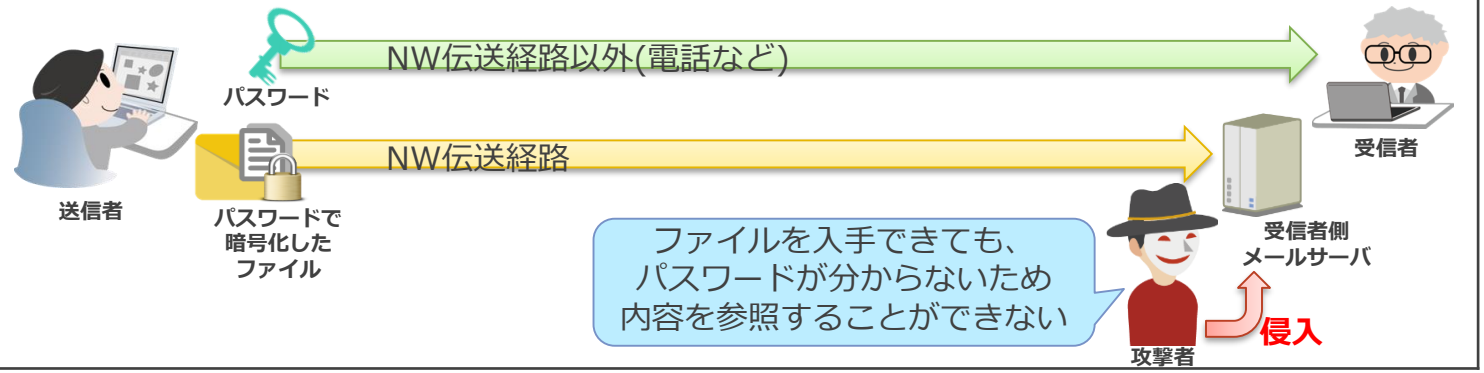


※仮にメール本文中にパスワードが記されていても、多くのアンチウィルスソフトはパスワードとして識別できず、ファイルを復号してのスキャンはできません。

5. パスワードで暗号化したファイルをメールで送付する運用とは (1/3)

そもそもパスワードで暗号化したファイルをメールで送付する運用とは、主に、ファイルを暗号化することで攻撃者に「盗聴されることを防ぐ」目的(※1)で生まれたセキュリティ対策でした。

※1.盗聴可能な箇所は大別して以下の二点が挙げられます。
本記事では、ISO27001(ISMS)において盗聴対策すべき箇所(※2)として言及している「NW伝送経路上」について取り上げます。

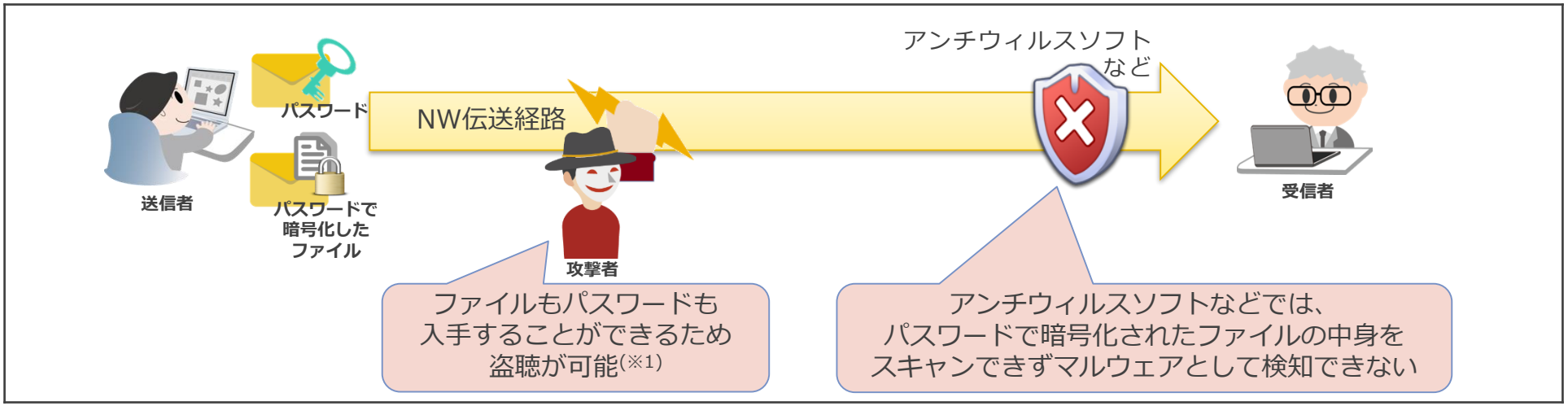
NW伝送経路上	
メールサーバ上	

※2.情報セキュリティ管理基準(平成28年改正版) 13通信のセキュリティ
<https://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Management_Standard_H28.pdf>
※3.上記図では「NW伝送経路上」「メールサーバ上」いずれの場合においても、パスワードとパスワードで暗号化したファイルを異なる手段(NW伝送経路とそれ以外)で送ることで、攻撃者に盗聴されるリスクを低減できることを表しています。

5. パスワードで暗号化したファイルをメールで送付する運用とは (2/3)

「パスワードで暗号化されたファイル」と「パスワード」を異なる手段(例えば、ファイルはメール、パスワードは電話)で伝達すると目的のセキュリティを確保できますが、実際には、この2つを同じ手段(それぞれ別のメール)で伝達する運用が普及しています。

この運用は、メリットである「盗聴防止」の効果(※1)はなく、デメリットである「検知・検疫のすり抜け」というリスクが発生します。



※1.常時接続のインターネットが普及するより以前(2000年前後)は、送信したメールが受信者側のメールサーバに到達するまでに複数組織のメールサーバで中継されていました。しかし、普及以降は大抵の場合において送信者側と受信者側のメールサーバ(MTA:メール転送エージェント)間は中継なしに直接接続されます。また、パスワードで暗号化したファイルをメールで送付する運用が開始された時期(2010年前後)とほぼ同時期に、SMTPS/TLSを利用した通信自体の暗号化も普及しています。そのため、盗聴防止の観点において、ファイルをパスワードで暗号化することのメリットはほとんどないと言えます。

※2.添付ファイル送信時に、添付ファイルを自動で暗号化し、パスワードを別メールで自動送信する製品があることが、添付ファイルとパスワードが同じ手段で伝達される一因となっています。

5. パスワードで暗号化したファイルをメールで送付する運用とは (3/3)

　メールと電話のような異なる手段を用いれば盗聴防止の効果はありますが、メールだけを使う運用が普及しており、また、パスワードで暗号化されたファイルをアンチウィルスソフトが検知できないことを逆手に取った攻撃手法が猛威を振るっている現状などから、伝達の手段が同じか異なるかによらず、パスワードで暗号化したファイルをメールで送付するのは止めるべきであるという意見が多くなっています。

【参考】
プライバシーマーク制度を運営する団体「日本情報経済社会推進協会(JIPDEC)」では、いわゆる誤った運用方法に言及する形で、2020年11月18日に「個人情報を含むファイル等をメールで送信する際に、ファイルをパスワード設定により暗号化して添付し、その**パスワードを別メールで送信する**ことについて、お問合せを多くいただいております。プライバシーマーク制度では**上記の方法による個人情報を含むファイルの送信**は、メールの誤送信等による個人情報の漏洩を防げないこと等から、**従来から推奨しておりません**。」と発表しました。

※JIPDEC「メール添付のファイル送信について」
<https://privacymark.jp/news/system/2020/1118.html>

6. パスワードで暗号化したファイルをメールで送付する運用に代わる運用 (1/3)

パスワードで暗号化したファイルをメールで送付する運用に代わる方法として、どのような運用が考えられるでしょうか？

以下に2つの運用例を示します。

1	公開鍵暗号方式の活用(PGP,S/MIME)	公開鍵暗号方式を活用してメールを暗号化する運用は、パスワードを送付する必要がないうえ、メール本文も暗号化され、復号も受信側のメールクライアントで受信したタイミングとなります。そのため、パスワードで暗号化したファイルをメールで送付する運用よりも「盗聴防止」の目的にかなった運用であると言えます。 なお、公開鍵暗号方式でメールを暗号化する方法自体は2000年以前より存在していましたが、「メールクライアントの設定方法が煩雑である」「費用が発生する」など、様々な理由で長らく普及しませんでした。 しかし2020年8月に代表的なメールクライアントソフトであるThunderbird(※)において、従来アドオンとして提供されていたEnigmailのPGP(OnenPGP)の機能が標準機能として組み込まれました。これはオープンソースソフトウェアのメールクライアントが、PGPがよく使われる機能であると判断したと解釈することができ、今後普及する可能性があります。

※Thunderbird「Thunderbird Release Notes(Version 78.2.0, first offered to channel users on August 25, 2020)」
<https://www.thunderbird.net/en-US/thunderbird/78.2.0/releasenotes/>

6. パスワードで暗号化したファイルをメールで送付する運用に代わる運用 (2/3)

2	Webサービスの活用	Webサービスを活用する運用は、送信者がファイルをWebサービスにアップロードし、受信者がファイルのアップロード先URLの情報をメールで受け取り、そのURLからファイルをダウンロードする流れが一般的です。 プロトコル(ウェブとメール)が異なるうえ、どちらのプロトコルも暗号化されているため、攻撃者に両方を盗聴される可能性は低いと言えます。 なお、この運用は2020年11月に内閣府/内閣官房で採用されることが決定しました。

No.	Who	How	What	Do
①	送信者が	ウェブで	ファイルを	Webサービスにアップロード
②	Webサービスが	メールで	アップロード先URLの情報を	受信者に伝達
③	受信者が	ウェブで	ファイルを	アップロード先URLから入手

※付加機能として、送信者のもとにダウンロードされたことを通知する機能やダウンロード時にパスワードを求める機能などを有するサービスも存在します。

6. パスワードで暗号化したファイルをメールで送付する運用に代わる運用 (3/3)

なお、代替えの運用方法を検討する際は、自社が求める要件を明らかにし、要件を満たす手段を選択する必要があります。

要件の例	
サービス品質保証(SLA)	稼働率、障害から復旧までの時間
セキュリティ	サービスで用いる機器の脆弱性管理有無(※)、 有事の際のログ参照可否、バックアップ取得有無
機能	モバイル端末からのアクセス可否

※前頁で説明したWebサービスの例として、2020年3月にサービスを終了した「宅ファイル便」が挙げられます。「宅ファイル便」は攻撃者にサーバの脆弱性を悪用され個人情報漏えい事故を起こした結果、サービスの停止に追い込まれました。このことから、外部サービスを利用する場合は、外部サービス提供側でセキュリティアップデートを継続するための開発体制が維持されていることを確認することも重要です。

※オージス総研「「宅ふぁいる便」サービスにおける不正アクセスについて　～お客さま情報の漏洩について（お詫びとご報告）～」
<https://www.ogis-ri.co.jp/news/1272165_6734.html>

7. まとめ

従来、権威あるセキュリティガイドラインなどで効果があるとされ、広く使われてきたセキュリティ対策であっても、その後の技術の進歩、社会状況の変化によって、「効果がない」もしくは「デメリットが大きい」と社会的な評価が変わり、組織のルールを見直す必要が生じることもあります。

パスワードで暗号化したファイルをメールで送付する運用は、アンチウィルスソフトによる検知・検疫をする抜けるリスクがありました。更に、これを逆手に取ったEmotetによる被害増加によって、「デメリットが大きい」と評価が変わった実例と言えます。

企業は、対応が後手に回らぬように世の中の流れを掴み、情報をいち早く入手して代替手段を検討・用意する時間を確保し、運用方法の見直しを行っていくことが重要です。

8. 参考URL

- NIST：電子メールのセキュリティに関するガイドライン
  https://www.ipa.go.jp/files/000025332.pdf
- JPCERT/CC：マルウエア Emotet の感染に繋がるメールの配布活動の再開について (追加情報)
  https://www.jpcert.or.jp/newsflash/2020072001.html
- JPCERT/CC：マルウェア Emotet の感染拡大および新たな攻撃手法について
  https://www.jpcert.or.jp/newsflash/2020090401.html
- US-CERT：Alert (AA20-280A) Emotet Malware
  https://us-cert.cisa.gov/ncas/alerts/aa20-280a
- 個人情報保護委員会：個人情報の保護に関する法律についてのガイドライン（通則編）
  https://www.ppc.go.jp/files/pdf/guidelines01.pdf
- JIPDEC：メール添付のファイル送信について
  https://privacymark.jp/news/system/2020/1118.html
- 情報セキュリティ管理基準(平成28年改正版) 13通信のセキュリティ
  https://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Management_Standard_H28.pdf
- Thunderbird：Thunderbird Release Notes(Version 78.2.0, first offered to channel users on August 25, 2020)
  https://www.thunderbird.net/en-US/thunderbird/78.2.0/releasenotes/
- オージス総研：「宅ふぁいる便」サービスにおける不正アクセスについて　～お客さま情報の漏洩について（お詫びとご報告）～
  https://www.ogis-ri.co.jp/news/1272165_6734.html
- ITmedia：パスワード付きzip、内閣府と内閣官房で26日から廃止へ　外部ストレージサービス活用 平井デジタル相
  https://www.itmedia.co.jp/news/articles/2011/24/news097.html

NTT DATA

Trusted Global Innovator