DigitalArts

セキュリティレポート

NewsLetter

2020 12/22

デジタルアーツ株式会社

2020年はメール誤送信による情報漏洩が約2割増加

「PPAP」も疑ってかかれ　メールのセキュリティ対策“再構築”のススメ

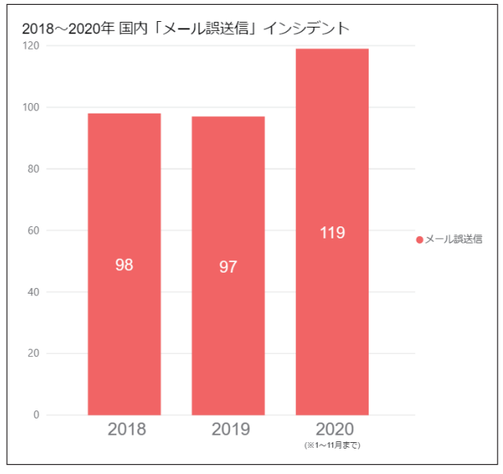
ここ最近、企業や自治体などによるメール誤送信に起因する情報漏洩事故が相次いで報道されました。当社がマスメディアによる報道資料を基に独自に集計した結果、国内セキュリティインシデントは全体的に増加傾向であり、その中でメール誤送信が原因となったインシデントは、2020年1月から11月までで119件、昨年や一昨年から比べると、2割以上増加しています【図1】※1。

2019年時点で、6割以上の企業が誤送信を経験 うち3割以上が社外からの指摘で発覚※2

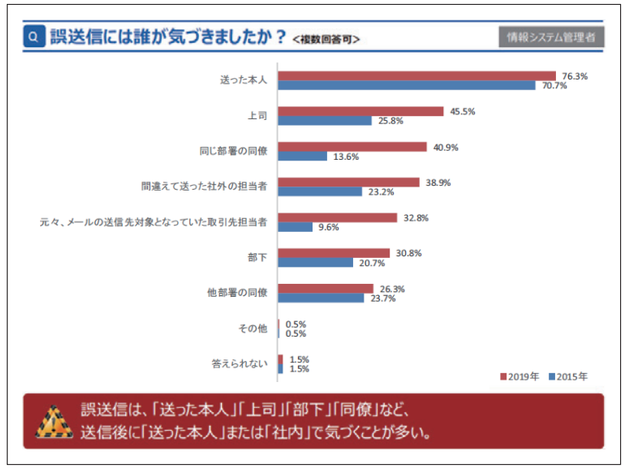
メール誤送信は今に始まったインシデント要因ではありません。当社が2019年に企業を対象に行ったメール誤送信に関する意識調査では、メールを誤送信したことがあると回答した従業員が6割以上、送った本人が誤送信に気付くケースが7割であるものの、3割以上は間違えて送った社外の担当者など、社外からの指摘で発覚したと回答しました【図2】。こうした誤送信から個人情報や重要情報の漏洩が起こってしまい、社会的信用の失墜に繋がります。なぜこれほどまでに誤送信は減らないのでしょうか。

公開されているインシデントの原因としてよくあるケースは、アドレスの記入ミス等によって間違った宛先に送信、公表すべきでないメールアドレスを誤って公表、誤った添付ファイルを添付、といった宛先や添付ファイルの間違いです。

では、こうしたミスは従業員が注意を怠らなければ起きない事故でしょうか。人が注意をしてミスをなくすということには限界があります。必ずミスや間違いは発生してしまうものという前提に立ち、何らかのシステムを用いた誤送信対策はまず不可欠であるといえるでしょう。ポイントとしては、宛先や添付ファイルをシステムで確認する仕組みソリューションを導入していただくことです。



【図1】2018～2020年 国内「メール誤送信」インシデントのみでのグラフ



【図2】メール誤送信の内容（自社調べ）

PPAPにひそむ危険　マルウェア被害のリスクが高まる？

そして、もう一つ、最近話題になっている「PPAP（メールで暗号化ZIPファイルを送信し、後からパスワードをメールで別送する方法）」についても考えていく必要があります。

PPAPは、ファイルを外部に送信する際の機密保持やコンプライアンス遵守の観点から、これまで日本で採用が推進されてきた方法です。しかし、暗号化されたZIPファイルが添付されたメールと、パスワードが別送されるこの手法は、セキュリティとしてはほとんど意味がないとされ、デジタル改革担当の平井卓也大臣が、11月17日の定例会見で中央省庁で使用を廃止する方針であることを明らかにしました。

ここで、PPAPが疑問視されている理由を改めて整理してみます。

■PPAPが、セキュリティ上意味をなさないとされている部分

①悪意の第三者がファイル添付されたメールを見ることができた場合

この場合、パスワードが書かれたメールも見ることができる確率が高く、意味をなさない

②宛先や添付ファイルを間違った場合

ファイルとパスワードのメールどちらかで気づけば防げるが、どちらも間違った宛先に送った場合・どちらのメールでも添付ファイル間違いに気付けない場合、意味をなさない。また、多くの場合パスワードを自動発行・送信するシステムを用いているため、人が気づけるタイミングがなく結局意味をなさない。

こうしたことから、有用性と代替策について現在議論がされています。
加えて最近では、

③「Emotet」や「IcedID」など、パスワード付きZIPファイルを用いた攻撃が横行

パスワード付きZIPファイルがアンチウィルスソフトなどのマルウェア検査を回避してしまうため、このためパスワード付きZIPファイルの受信を廃止すると、いちはやく表明した企業もあるほどです。

PPAP運用の検討とメールセキュリティ対策の再構築を 誤送信は起こりうると想定し確認できるシステムを

では、PPAPをただちに廃止することが必要かというと、その限りではありません。ファイルの暗号化は情報漏洩対策の基本として必要ですし、PPAPに替わる代替対策をただちに講じることが難しい組織もあると思います。

まずは現在の自組織における利用状況と運用ルールを把握することと、上記リスクを把握した上で組織に合致したポリシーを検討することが重要です。

メール誤送信をシステムでチェックする機能を有したメールセキュリティソリューションや、強固でかつ効率的にファイル暗号ができる暗号化ソリューションも出てきています。今一度、メールセキュリティ対策の見直しと“再構築”をされてみてはいかがでしょうか。

（参考）

■セキュリティレポート『国内セキュリティインシデント－メール誤送信は増加傾向－』 https://www.daj.jp/security_reports/201222_1/

■誤送信・内部統制・コンプライアンス強化を備えたメールセキュリティ「m-FILTER」Ver.5 https://www.daj.jp/bs/mf/

■ファイルを暗号化し、利用状況を追跡・遠隔操作できるファイルセキュリティ「FinalCode」 https://www.finalcode.com/jp/

※1 マスメディアによる報道資料をもとにした自社調べ（2020年12月）　※2 自社調べ「勤務先におけるメール誤送信の実態調査」（2019年6月）　https://www.daj.jp/shared/php/downloadset/c/parts.php?page=dl&filename=DigitalArts_mf_1906.pdf

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、有害情報の閲覧を制限するWeb フィルタリングソフトを開発、以来企業・公共・家庭向けに情報セキュリティ製品を提供しております。

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/

本ニュースレターに関するお問い合わせ

※新型コロナウイルス感染症拡大に伴う在宅勤務実施中のため、
お問い合わせ先は下記とさせていただきます
デジタルアーツ株式会社　広報担当 山田
TEL : 090 1555 7254 / E mail : press@daj.co.jp

DigitalArts
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