2022年7月20日

2025年6月5日再公表

公益財団法人 金融情報システムセンター (FISC)

「パスワード付き暗号化ファイル添付電子メール」の課題及び対策に関する FISC 見解

当センターは、2022年7月、「パスワード付き暗号化ファイル添付電子メール」の情報セキュリティ上指摘されている課題について、課題の考察、及びそれを踏まえた対策に関する見解をまとめ、FISC 会員向けに公表した。今般、本書を、一般向けの形として、再公表する。

また、本書の内容について、当センターが策定する「金融機関等コンピュータシステムの安全対策基準・解説書」(最新版は「第13版」)の基準項目(「実138」)に取り込む改訂を、2024年3月に実施している。

1. パスワード付き暗号化ファイル添付電子メールについて報道等において指摘される「課題」

機密性のある情報を含むファイル(文書、計表等)を相手方に送る方法として、①ファイルをパスワードを付す形で暗号化し、②暗号化ファイルを電子メールに添付し送信した後、③パスワードを記載した別途の電子メールを、同じ相手方のアドレス宛に送信し、④受信した相手方が、②の添付ファイルを③のパスワードにより開封する手法、が用いられている。また、送信側における①から③の操作を、システム上、同時・自動的に実施する機能を備えたツール等が提供されており、これらを導入・利用している先もある。

当該手法について、「機密性のある情報をセキュアな形で送る方法として適切でなく、異なる手法を用いるべきである」等の指摘がある。これらの指摘に関して、当該手法の情報セキュリティ面の「課題」として、報道や有識者の発言等において、概ね共通して挙げられている観点は、以下(1)から(3)のとおりである。

なお、「課題」として、情報セキュリティ面とは別途、「受け取った暗号化ファイルを、パスワードを用いてひとつひとつ開封することが、手間を要する」という「操作性」の観点も指摘されることがあるが、ここでは対象としない。

(1) 「マルウェア対策」の観点

パスワードで暗号化されたファイルについては、一般に、メールサーバーや端末に搭載されたセキュリティ対策ソフトによるファイル内容の検証ができないため、マルウェアに感染していても、検知ができない(いわゆる「すり抜ける」)。すなわち、マルウェア検知を阻害する。特に、最近被害事例が急増しているマルウェアである「Emotet」については、パスワード付き暗号化ファイルを添付したメ

ールを使った手口が多く使われているとされ、対策と考えているものが、逆に脅威を増加させている。この点、被害による事業継続へ支障を及ぼす事例がみられることから、特に重視すべきである。

(2) 「誤送信対策」の観点

暗号化ファイルを添付した電子メールを送信した後、パスワードを記載したメールを別途送信することにより、仮に前者のメールを誤った先に送信した場合、後者のメールを送信する手前の時点で気付けば、情報漏洩を回避することが可能である点、誤送信対策とされている。しかしながら、暗号化ファイルを添付したメールを誤送信した後に、宛先を再確認せずに同じ宛先にパスワード通知メールを送ってしまう場合や、ツールにより自動的に同一の相手先アドレスにパスワード通知メールが送信される場合には、誤送信防止対策として意味をなさない。

(3) 「窃取（盗聴・改ざん）対策」の観点

メールサーバー間の通信が暗号化されていない場合には、暗号化ファイルとパスワードを別途のメールで送信したとしても、その両方が同一通信経路でやり取りされているため、当該通信経路上で窃取（盗聴・改ざん）され、暗号化ファイルが開封される可能性がある。サーバー間の通信が暗号化されている場合でも、送受信側双方あるいは片方のサーバー又は端末に脆弱性がある場合には、当該脆弱性を利用した攻撃により、サーバー又は端末から両方のメールが窃取される可能性がある。

2. パスワード付き暗号化ファイル添付電子メールの「課題」に関する FISC の考察

上述（1）～（3）に挙げられる、3つの観点からの「課題」については、各々単独で、サイバー攻撃やオペレーションミス等による情報漏洩のリスクを回避するために、考慮することが必要である。パスワード付き暗号化ファイルとパスワードとを、ともに電子メールで送信する手法に関しては、3つ全ての課題を内包し得るものとして、特にそのリスクを十分に認識することが必要と考えられる。このため、相対的にリスクがより低減されると評価される代替的な手法があれば、そうした手法を用いることが望ましい。

もっとも、代替的な手法を含め、どのような手法を用いる場合でも、「リスクをゼロにする万全な手法は見出しがたい」という認識をあらためて確認し、ファイルの授受を行う双方において、必要な対応を実施することが重要である。具体的には、例えば、上述（1）の観点では、修正プログラムの公開前を狙う攻撃いわゆる「ゼロデイ攻撃」の脅威を鑑みると、「暗号化されていない＝セキュリティ対策ソフトにより検証済み」として、送信元の正当性を何ら確認することなく、不用意に添付ファイルを開封することは適切でない。（2）及び（3）の観点では、添付ファイルの有無に関わらず、誤送信対策としての宛先アドレスの確認や、窃取対策としてのサーバーや端末における脆弱性対応は重要である。また、パスワードを電子メールでない別途の方法により伝達する、ファイルの授受は外部ストレ

ーサービス等を利用しパスワードのみを電子メールで伝達する、といった手法でも、パスワードの管理が緩に流れればパスワードが漏洩する、パスワードが単純で類推しやすいものであれば、「総当たり攻撃」等によりパスワードが特定される、さらに、外部ストレージへの保管が適切に行われない場合には、ファイル流出の可能性がある、といったリスクにつながる。

このほか、リスク管理とは別途の視点で、代替手段を自社で導入することが、システム構成や経営資源等との関係で容易でない、代替手段の活用にファイルの授受を行う相手方が対応することが困難である、といった事情を勘案することが求められる、あるいはそれが制約となる場合もあり得る。

以上のように、複数ある対策及び代替策とされるもの各々について、セキュリティを確保するために優位とされる効果がある一方、別のリスクにつながり得るとする視点からの留意事項がある。すなわち、先述のとおり、リスクをゼロにする万全な手法は見出しがたい。そうした実情のもとで、金融機関等は、業務遂行上取り扱う情報の内容及びその機密性の有無、自社のシステム構成や運用規程及び情報セキュリティ・ルール、また、状況に応じ業務の相手方の事情や相手方との関係等を前提に、ファイルの授受する様々な手法のそれぞれに、得られる効果や内包するリスクがあることを踏まえ、これらを過不足なく評価し、さらに、当該内容及び対応策や運用上の留意事項にかかる認識を、自社内及び相手方の利用者との間で共有したうえで、リスクベースアプローチの考え方¹に基づき、各社が適切と判断する対策を採用することが必要である。

3. パスワード付き暗号化ファイル添付電子メールの「課題」を踏まえた対策

前述の「課題」に関する考察を踏まえ、機密性のある情報を含むファイルをセキュアに授受するための対策としては、以下の例がある。金融機関等においては、リスクベースアプローチの考え方のもと、各先において、以下の例を含め、適切と判断する対策を採用することが望ましい。

(1) ファイル授受の方式

① マルウェア対策

- a. 機密性のないファイルの場合、メールに添付するファイルにパスワードを付す必要はない。
- b. 添付ファイルのあるメールを受信時に、送信元が正しいものか確認する。
- c. ファイル共有サービスを利用する。その際、ファイルにはパスワードを付さないことにより、セキュリティ対策ソフトによるマルウェア検知を可能にする。

② 誤送信対策

- a. パスワードをあらかじめ取り決めたいうで暗号化する。
- b. 別経路でパスワード通知を行う（電話、SMS、ビジネスチャット、郵送等）。

¹ FISC「金融機関等コンピュータシステムの安全対策基準・解説書」において、リスクベースアプローチに関して、次のように示している。

『リスクベースアプローチ』とは、リスク特性の分析結果を安全対策の優先順位など、金融機関等が安全対策を決定するための合理的な意思決定に活用する考え方をいう。この際、金融機関等の経営資源が有限である点を踏まえ、リスクゼロを追求することは必ずしも合理的でないという認識に基づき、安全対策に対する資源配分を経営資源全体の中で調整していくこととなる。』

- c. ファイル共有サービスを利用する場合、当該サービスへのアクセスに当たって認証を行うものや、別経路でパスワード通知を行うものを利用する。
- d. ファイル共有サービスの場合、ファイルの掲載期限を設定する、誤送信判明時にファイルの削除を行う、等の対策を行う。
- e. 暗号化ファイルをメールで送付した後、パスワード通知するためのメール作成時に、宛先を再確認する。

③ 窃取（盗聴・改ざん）対策

- a. メール全体（本文+添付ファイル）を暗号化し、デジタル署名する。
- b. ファイル共有サービスを利用する。その際、端末からファイル共有サービスまでの伝送データの暗号化と、ファイル共有サービス上のデータの暗号化（データベースやストレージ等の暗号化）を行う。
- c. メールサーバー及び端末における脆弱性対応を実施する。
- d. パスワードを類推しにくい、長く複雑なものにする。

（２）利用者との間の認識共有、注意喚起

上記の方式に関わらず、メールを介したサイバー攻撃に関して、自社内及び業務の相手方の利用者との間で、リスクに関する認識及び対処方法を共有し、必要に応じ注意喚起することが重要である。それらの内容としては、以下の例がある。

- ① メールの送信元、添付ファイル、又は本文に記載されているリンク表示について、信頼できるものと判断できない限りは、添付ファイルの開封やリンク先へのアクセスを行わず、確実な手段で送信元へ確認するといった対応を行う。
- ② 不審なメールの添付ファイルを開封した、あるいはリンク先へアクセスした場合は、社内の情報セキュリティ・ルールに従い、直ちに所定の連絡先に連絡する等、必要な対応を行う。

以 上