最新セキュリティマネジメント（第21回）

パスワード付き添付ファイルの送受信リスク

2023.02.24

“PPAP問題”をご存じだろうか。PPAPとは添付ファイル付きのメールを送信する際に、添付ファイルを暗号化したZIPファイルで送信し、別のメールで暗号化したファイルを解凍するパスワードを送るという方法だ。メールでファイルを共有する際にセキュリティを担保するために広まったPPAPだが、セキュリティリスクが大きいと指摘され使用を禁止する企業や組織が増えている。なぜだろうか。

パスワードが盗まれマルウエア感染の恐れ

PPAPはIT用語でよくある英文の頭文字をとって略称にしたものではない。「Password付きZIP暗号化ファイルを送ります」「Passwordを送ります」「Aん号化（暗号化）」「Protocol」のことだ。送信者としては操作が簡単で誤送信防止にもなるため、リスクを減らしてメールでファイルを共有する方法として普及してきた。

広く使われてきたPPAPがなぜ危険なのか。その原因の一つが一通目のパスワード付きファイルを送ったメールと、二通目のパスワードを通知するメールが同じ経路で送信されているからだ。メールはいくつものサーバーをたどって送信されるため、途中で盗み見られる危険がある。一通目を盗み見られた場合、二通目も盗み見られてしまう。これでは暗号化した意味がない。

ファイルを自動で暗号化するPPAPは送信側が手軽にできる一方で、二通目のメールのパスワードでファイルを解凍する必要があるため、受信者側には負担が大きい。なのにセキュリティ上の効果がないのであればやる意味がない、と指摘されるようになった。

さらに大きな問題として浮上したのが、添付ファイルに対してウイルスチェックが効かないという点だ。セキュリティ製品の多くは送られてきたメールをチェックしているが、パスワード付きのZIPファイルの中身はチェックできない。メールが盗み見られてマルウエア付きのファイルにすり替えられても、検知できないことになる。

このような事態は実際に発生していて、独立行政法人情報処理推進機構（IPA）では2020年9月2日に「パスワード付きのZIPファイルを添付したEmotetの攻撃メール」を確認したと報告している。Emotetはこの連載の第18回でも紹介した、悪意を持って作られた代表的なプログラムである。ファイルを開くとデバイスがマルウエアに感染してしまう。

代替手段はクラウドストレージの活用

このようにセキュリティの専門家からセキュリティリスクが大きいと指摘されたPPAPだったが、多くの企業や組織では引き続き使われていた。この流れが変わったのは日本政府がPPAPの廃止を打ち出したからだ。2020年11月に、当時のデジタル庁平井大臣が定例会見で「自動暗号化ZIPファイル」を廃止すると発表したのだ。

この発表を受けてPPAPの利用を禁止する企業や団体は増えている。しかし、PPAPがセキュリティ上の効果がないからとい

って暗号化しないファイルを送信すれば危険は明白だ。より高いセキュリティ効果を期待できる代替案を採用する必要がある。

IPAなどが推奨している方法として、電子メールの暗号化方式S/MIME（エスマイム）の利用が挙げられる。電子証明書を用いてメールの暗号化とメールへの電子署名を行うもので、送信者と受信者が事前に認証局から電子証明書を入手しておく必要があるが、一度設定してしまえば、かなり高いセキュリティが期待できる。

しかし、この方法は電子証明書の入手にコストと手間がかかる、メールソフトの中にはS/MIMEに対応していないものがある、Webメールでは利用できなといった問題があり、現状では利用にハードルがある。

そこで注目されているのが、クラウドストレージサービスの活用だ。送信者は共有したいファイルをクラウドストレージにアップし、クラウドストレージのURLをメールで受信者に伝える形で利用する。ただし、無料のクラウドストレージサービスはアクセス権限の設定がない場合があり、これではセキュリティは担保できない。各クラウドストレージサービスのセキュリティ機能を確認した上での活用をお勧めする。

※NTT西日本グループでは恒常的なウイルス監視を行い、メール送信時は誤送信防止の仕組みを導入しています