いただいた主な質問への回答

回答：パネルディスカッション　登壇メンバー

PPAP総研　大泰司　章　氏
フィッシング対策協議会 証明書普及促進WG　主査
（サイバートラスト株式会社）　田上　利博 氏
フィッシング対策協議会 証明書普及促進WG　副主査
（GMOグローバルサイン株式会社）　稲葉　厚志 氏
九電ビジネスソリューションズ株式会社　ビジネスソリューション事業部
ビジネスソリューション第2部　部長　渡辺　雅久 氏
一般財団法人日本情報経済社会推進協会　セキュリティマネジメント室
主査　　高倉　万記子

【PPAP】

Q1：脱PPAPの最新動向、失敗事例

A：オンラインストレージでの対応が多いです。ただし、ファイルが個別に暗号化された上に、その鍵が相変わらずメールで送られる等、脱PPAPの効果がない上に、かえって受信側の手間を増やすこともあるようです。

まず、最低限、暗号化の必要がないファイルをそのまま暗号化せずに送ることで、受信者の手間を減らすことが大事です。

【S/MIME】

Q2：メーリングリストへの暗号化メールはどうなりますか？

A：一般的なメーリングリストは、S/MIMEの暗号化には対応していません。一方で、PPAPによるファイル暗号化はできますが、その場合の暗号化のメリットはそれほどないと思われます。

【なりすましメール対策】

Q3：なりすましメールが送られた場合の対処法

A：なりすましと思われる不審なメールを受信した場合は、添付ファイルやURLリンクをクリックせず、社内のセキュリティインシデント対応部門や情報システム部門に連絡します。

また、フィッシングメールを受信した場合、フィッシング対策協議会へご報告ください。

https://www.antiphishing.jp/registration.html

Q4：スパマーはどのようにして受信者のアドレスを特定しているのか、それに対する対策はあるのか？
A：スパマーは、入手したアドレスに手当たり次第に送信していることが多いようです。SPF、DKIM、DMARC、S/MIME等のなりすまし対策の普及が望まれます。

Q5：ウイルス感染の経路別割合、メールによる被害はどれぐらいか？
A：参考となりますが、IPAの「情報セキュリティ十大脅威2021」の「組織」向け脅威ランキングによると、組織向け（企業向け）脅威のうち、1位「ランサムウェアによる被害」、2位「標的型攻撃による機密情報の窃取」、5位「ビジネスメール詐欺による金銭被害」の3つの攻撃は、電子メールが起点になっていたり、なりすましメールが関係しています。
※https://www.ipa.go.jp/security/vuln/10threats2021.html

【ファイル送信】
Q６：ファイルの送信、共有にログイン許可した利用者のみ利用可能なオンラインストレージを利用しています。アクセスログや何世代かのファイルの履歴もあり、従来のメール添付がなくなり便利ですが、問題がある場合の対処法を教えてください。
A：セキュアなサービスを選択すれば、問題ないと思います。問題があるとすれば、オンラインストレージへのアクセスが禁止されている企業がまだあるので、そういった企業とのやりとりには使えません。本人認証の仕組みが十分でなかったり、サービス自体のなりすまし対策がされていないこともあるので、その点は注意が必要です。

以　上