【講演レポート】第99回JIPDECセミナー

なりすまし対策
～電子証明書を使った本人確認と電子メールにおける送信元認証～

JIPDEC
セキュリティマネジメント推進室　主査　　高倉　万記子

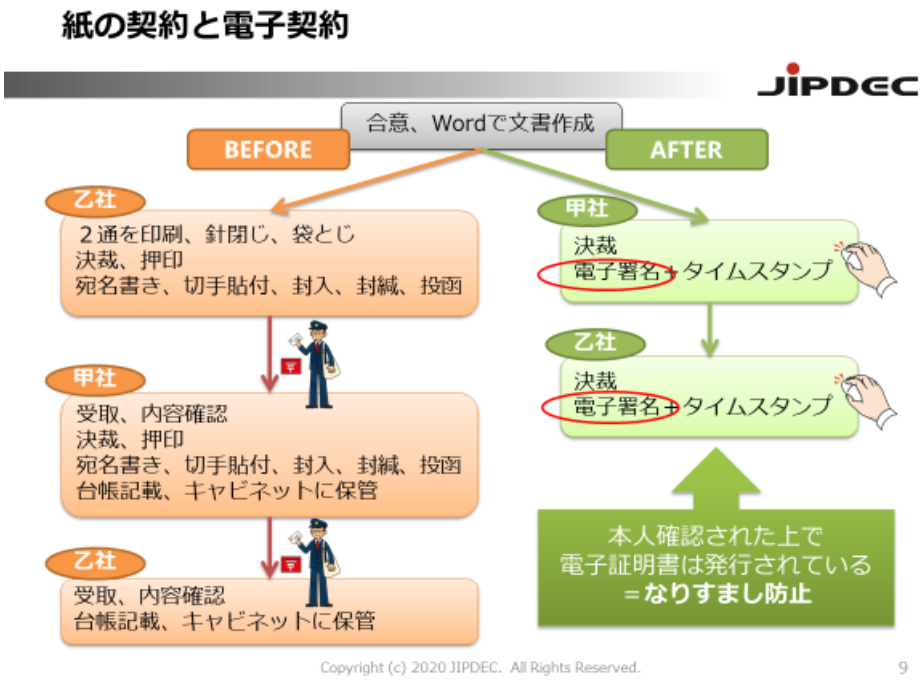
電子証明書とは

今年、マイナンバーカードの電子証明書更新が話題になっていましたが、マイナンバーカードには署名用電子証明書と利用者証明用電子証明書が入っています。紙の世界でペンや印鑑でサイン、押印するのに対し、電子の世界では電子証明書を使って電子署名を行います。

電子証明書を使ったなりすまし対策

電子契約

今年、テレワーク等により電子契約への移行が進んでいますが、この電子契約で電子証明書を使ったなりすまし対策が行われています。電子証明書を使って電子署名を行うことにより、文書が署名後に変更されていないこと、本人が作成したことを確認することができます。また裁判等で電子文書を証拠として提出する場合、電子署名法第3条により「本人による電子署名が行われているときは、真正に成立したものと推定する」とされています。



クライアント認証

JIPDECではなりすまし防止のため、JIPDEC内システムにアクセスする際は本人の電子証明書がインストールされたデバイスでのみアクセスできるようにしています。

メールのなりすまし対策

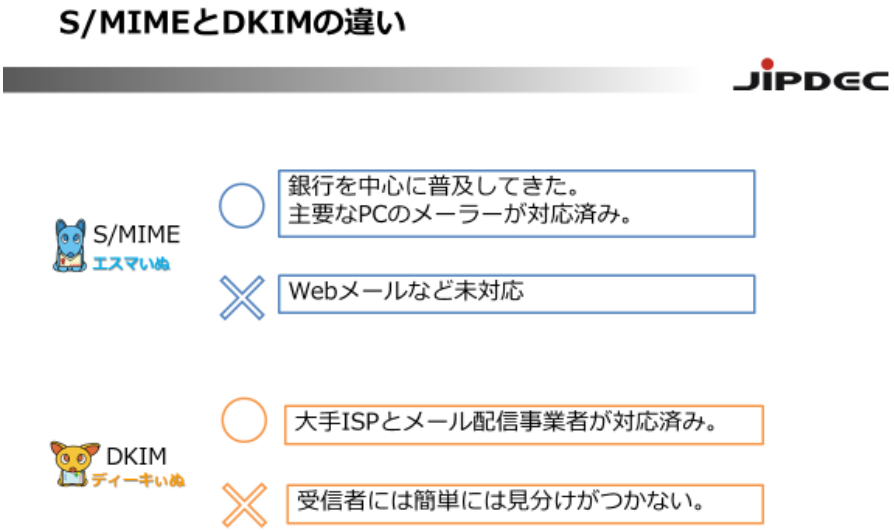
また、JIPDECではメールでも電子証明書を利用してS/MIMEというなりすまし対策を行っています。これによって、例えばOutlookでは真正なJIPDECからのメールには赤いリボンが付くので、付いていないメールは「なりすましの可能性がある」と受信者が気づくことができます。

IPAの資料「情報セキュリティ10大脅威2020」では、第3位にビジネスメール詐欺による金銭被害が挙がっています。この資料の中でも、取引先とメールで重要情報をやり取りする場合、S/MIMEによる電子署名がなりすまし防止策として有効だと紹介されています。

現在、S/MIMEの導入ユーザーは増加しています。昨年6月には九州電力グループが社員14,300名に対しS/MIMEを導入、併せて電子証明書の自動発行・更新・運用管理の仕組みを開発して特許を取得しています。また、今年の4月からは日本クラウドセキュリティアライアンス（CSAジャパン）社において同社から送信されるすべてのメールにS/MIME電子署名を付与しています。さらに、防衛装備庁でも、今年の10月に全職員2,000名でS/MIMEの運用を開始しています。

その他のなりすまし対策

S/MIMEがエンドtoエンドでの対策であるのに対し、DKIMという仕組みがあります。S/MIMEが個々人のメールアドレスに認証をかけるのに対し、DKIMはドメインに対して認証を行います。



この他、DMARCという機能は、送信側が設定した送信ドメイン認証（SPF）またはDKIMを受信側で検証し、認証に失敗した場合にメールをどのように扱うか（何もしない・隔離・拒否）を送信側で設定できるものです。さらに、認証に失敗したメールに関するレポートも届くので、自社ドメインがどの程度なりすましに使用されているかを把握することもできます。

9月に報道された日経平均株価採用企業のDMARC設定状況は23.0%、また10月にJIPDECが公表した防災メールを発信している自治体では14.2%となっています。

海外では、政府機関に対してDMARC設定を強制しているところもあり、企業も5割以上が設定しているとする報道もあります。一方、日本では内閣サイバーセキュリティセンターが公表している「政府機関の情報セキュリティ対策のための統一基準」や、総務省による「地方公共団体における情報セキュリティポリシーに関するガイドライン」等で、メールのなりすまし対策が挙げられています。JIPDECでもLINEスタンプ「なりすまし対策犬」を作って普及啓発活動を行っています。

Emotetと暗号化ZIP

9月2日、IPAが「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」に対する注意喚起を行いました。実際にその後、いくつかの企業が暗号化zipファイルに入ったEmotetによって被害を受けたと発表しています。

また、現在政府が行っているデジタル改革アイデアボックスに寄せられた3,300件のアイデアのうち一番ポイントを集めたアイデアが「暗号化した添付ファイルを送って、その直後にパスワードが来るPPAPをやめる」というもので、その直後にデジタル改革担当大臣の定例会見で「中央省庁の職員がメールを送るときに添付する「パスワード付きZIPファイル」を廃止する」という発言もありました。JIPDECが運営するプライバシーマーク制度においても、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という方法は従来より推奨していないので、この機会にこれまでの安全管理措置を見直し、より実効性の高い対策を行ってください。

JIPDEC
セキュリティマネジメント推進室　主査　　高倉　万記子
JIPDECインターネットトラストセンター兼セキュリティマネジメント推進室主査。トラストサービスやインターネット上のなりすまし対策の普及啓発を行っている。

本内容は、2020年11月20日に開催された第99回JIPDECセミナー「ビジネスモデル変革に伴うなりすましリスク対応－オンライン本人認証となりすまし対策」講演内容を取りまとめたものです。