JIPDEC のなりすましメール対策

JIPDEC　インターネットトラストセンター
企画室　主席研究員　金子　成徳

■はじめに

サイバー犯罪の多発や標的型攻撃が激化する中で、インターネット上での個人、法人、モノ等の実在性確認及びそれらの属性等を証明する仕組みが求められている。こうした背景から、JIPDEC は本年 4 月 1 日にインターネットトラストセンターを設置し、インターネット上の情報の信頼性の確保に向けた活動に取り組んでいる。

インターネットトラストセンターの活動は①電子証明書の市場開拓（JCAN 証明書）、②なりすまし対策（電子メール、Web サイト）、③法人情報基盤の整備（サイバー法人台帳 ROBINS）を柱としているが、本日は②なりすまし対策に焦点を絞ってお話する。

■メールなりすまし対策

「なりすまし」と聞いて受信者（＝潜在的被害者）の立場からはメールフィルタリング、サンドボックス、標的型攻撃メール訓練などの対策を想定すると思うが、JIPDEC はなりすましメールの送信者（＝加害者）とならないための施策、すなわち「正しいメールを正しいと判断できるようにする」方策の普及に力を入れている。具体的には、①電子署名付きメール（S/MIME）、②送信ドメイン認証（DKIM）、さらに DKIM を可視化する「安心マーク」である。また、「正しくないメールを正しくないと判断できるようにする」方策として DMARC の普及に取り組んでいる。

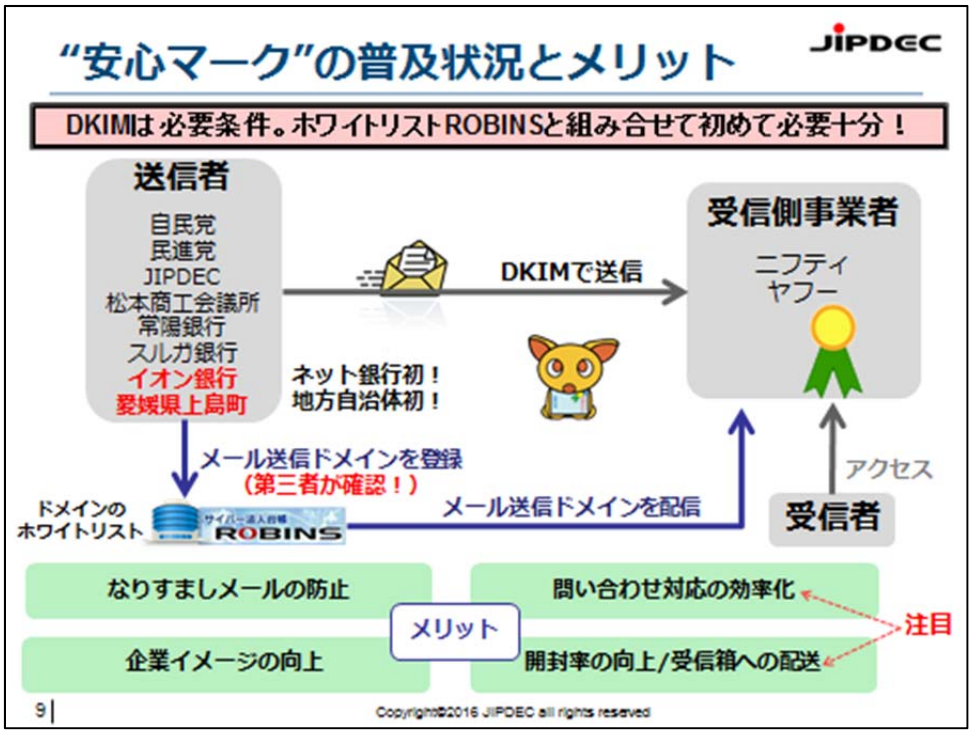
S/MIME と DKIM はともに送信者から送信されたメールが改ざんされていないことを確認するための仕組みだが、公開鍵暗号方式と電子署名の標準規格である S/MIME は送信者と受信者が一対一で改ざんされていないことを確認できる仕組み、電子署名による送信ドメイン認証技術の一つである DKIM はドメイン単位で改ざんされていないことが確認できる仕組みである。

■DKIM 認証の課題を解決する安心マーク

DKIM とは、ドメインに対応する公開鍵を DNS サーバに登録し、送信者は公開鍵に対応した秘密鍵を用いて電子署名を作成・送付、受信者は DNS サーバから受け取った公開鍵によって復号し、改ざんされていないことを確認する仕組みである。しかし、実在する組織のドメインに類似したドメインをなりすまし送信者が取得し、ウイルスメールを送信することを DKIM だけで防ぐことはできない。そこで JIPDEC はメール受信時に認証結果が可視化でき、メール送信者の身元を識別できる仕組みとして「安心マーク」を推進してい

る。

安心マークの仕組みは、JIPDEC が提供する「サイバー法人台帳 ROBINS」にあらかじめ登録された身元が保証されたドメイン情報が受信側事業者（ヤフー、ニフティ）に送られ、DKIM 認証されたメールを受信した際にドメインの突合をし、正しい送信者から送られたことをメールボックス上で表示するものである。この 8 月から地方自治体として初めて愛媛県の上島町にも導入して頂いたが、自民党、民進党、松本商工会議所、常陽銀行、スルガ銀行のほか、10 月からはイオン銀行にも採用頂いている。安心マークは現在 Yahoo! メール、@nifty メールへの対応にとどまっているが、スマホ向けメールソフト、オープンソースウェブメールソフトへの実装などへの拡大を計画するなど、受信環境の整備に取り組んでいる。



■DMARC の仕組み

DMARC は SPF,DKIM といった送信ドメイン認証に成功、失敗したメールの取扱いを送信者が指定し示すもので、送信者はドメイン認証結果を DMARC レポートとして受け取れる。これによって、送信者側の DKIM や SPF の設定状況（実装率や認証成功率）を確認することができ、送信者は自分がなりすまされているかもしれない情報も得られる。

JIPDEC は今年 6 月から DMARC を導入し、効果を最大化するため米 Easy Solutions 社が提供する DMARC Compass を日本で初めて採用した。DMARC Compass は対象ドメインを利用したメールの送信情報、不正メールのコンテンツをリアルタイムに監視するこ

とができ、また、ここで検知した不正サイトを迅速に閉鎖させるオプションもある。

■“安心マーク 2.0”計画

JIPDEC は今後、安心マーク 1.0 を発展させた安心マーク 2.0 の推進を計画している。具体的には、現在の DKIM 認証に制限している安心マークの付与を S/MIME 認証へとプラットフォームを拡大すること、企業ロゴやディスプレイネーム対応も含めた安心マークファミリーの拡充、DMARC 等新技術への取り込み等である。

JIPDEC は今後一層、送信者なりすまし対策の切り札として送信者認証とホワイトリストを組み合わせた“安心マーク”の普及・推進を強化し、安心マーク 2.0 として S/MIME、DKIM、安心マーク、DMARC に加え、企業ロゴやディスプレイネームの対策に取り組んでいく。

また、安心・安全な電子メールを実現するためには多種多様なステークホルダが協力して、エコシステムを構築することが必要だ。JIPDEC はフォーラムの創設等を通じ、インターネット上のセキュリティを向上する仲間を増やす活動を引き続き積極的に行っていく。