# Web なりすまし対策の方向性

一般財団法人日本情報経済社会推進協会（JIPDEC）
インターネットトラストセンター
主席研究員　杉田　修

標的型攻撃等によるサイバー犯罪が激化する中で、JIPDEC は、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を提供するなど、インターネット上の情報の信頼性確保に向けた取り組みを行っている。今回はこのうち、Web サイトのなりすまし対策に関する取り組みについてご紹介する。

## Web なりすましの現状

攻撃者は、検索エンジンの検索結果やなりすましメールなどを使って、なりすまし Web サイトへ利用者を誘導したのち、偽物の商品を送付したり、認証情報（ID・パスワード情報等）を盗んで不正送金を行ったりする。こうした攻撃は、利用者が金銭的被害等に遭うだけではなく、正規サイトを運営する会社等のブランドイメージの失墜にもつながる。フィッシングサイトについては、2015 年では前年と比較し件数は減少傾向にあるものの、被害額は増加している。

## Web なりすまし対策の現状

Web なりすましに対し、Web サイトの運営者側ができる対策として、EV-SSL（EV SSL 証明書）や各種アドオンのほか、Web サイト運営者の実在確認シール（以下、「シール」と略す）などを導入して自社の Web サイトの真正性（本物であること）を利用者に分かるようにすること、また、S/MIME、SPF、DKIM、DMARC などを活用し、自社から発信するメールが本物であることを利用者に分かるようにしたりすることなどがある。

また、Web サイトの利用者側ができる対策としては、Web の検索結果に表示される信頼度のスコアに注意すること、ウイルス対策ソフトの導入やセーフブラウザを利用することのほか、URL フィルタリングの導入などでなりすまし Web サイトや改ざんサイト自体をフィルタリングするといったエンドポイント・ネットワークでの対策が考えられる。

ただし、それぞれの対策には課題もある。EV-SSL に関しては、EV SSL 証明書が今のところさほど認知されておらずまだ広く普及していないことや、スマートフォンで使われている一部のブラウザでは EV SSL 証明書を使っていない https サイトと区別がつかないケースもあること。シールは、クリックをしないとその真正性が分からないこと。また、メールなりすまし対策では、SPF や DKIM などを攻撃者側が利用しているケースがあることや、電子証明書の取り扱いが煩雑であること、またそもそもこうした

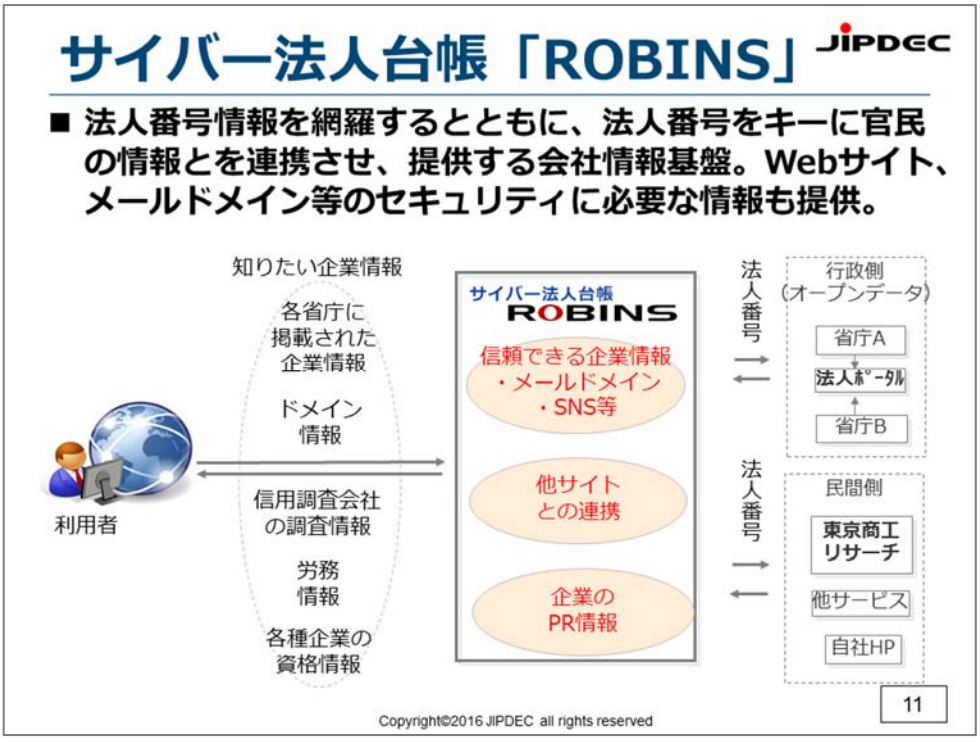
対策の認知度が低いこと。さらに、エンドポイント・ネットワークでの対策は、即時性に欠けていること、スマートフォンでは未成熟であることなどが課題として挙げられる。

### 利用者の自衛策 6 ヶ条

現時点で、オンラインバンキングや EC サイトの利用者ができる対策として考えられるのは、1）ちょっと立ち止まって、考える、2）ブラウジングやメールの送受信には基本的にウイルス対策ソフトを入れた PC を使う、3）広告メール等を読む際は、正しい電子署名が付いていることを確認する、4）Google 等で検索した結果をクリックする前に、リンク先の信頼度を確認する、5）Web サイトにアクセスした際、アドレスバーの部分が緑色（EV-SSL）になっていることを確認し、アドレスバーに表示されている会社名を確認する、6）EV-SSL が実装されていない Web サイトでは、シールをクリックし、そこで表示されるページが EV-SSL になっていることや会社名が正しいことを確認する、といったことである。しかし、これらを行うのは、一般の利用者にとってあまり簡単なことではない。

### JIPDEC の取組みと今後の展望

JIPDEC が運営する「サイバー法人台帳 ROBINS」（以下、ROBINS と略す）は、社会保険労務士や行政書士等の第三者の確認者によって確認された企業情報のほか、法人番号情報を網羅し、法人番号をキーに連携させた官民の情報を提供している（図 1）。




ROBINS には Web サイトやメールドメイン等のセキュリティに必要な情報も登録できるため、JIPDEC は、メールなりすまし対策のひとつとして、これらの情報と DKIM の仕組みを利用し、悪意のない発信者からの本物のメールであることをメールソフト上で示す「安心マーク」というサービスも提供している。また Web サイトのなりすましについては、端末の種類やネットワークに依存せず利用でき、

ROBINS のようなホワイトリストをもとに機能するフィルタリングのような仕組みが有効だろう。

なりすまし Web サイトの発生そのものの抑制や、スマートフォン利用者の保護、一般の利用者による対策負担の軽減など、Web なりすまし対策には課題が残されている。JIPDEC が現在取り組んでいる S/MIME や安心マーク、ROBINS の情報をもとにしたシール（ROBINS シール）の普及だけではなく、これらを活用した新たな仕組みやサービスも、今後検討していきたいと考えている。