なりすましメールの現状と対策

三井物産セキュアディレクション株式会社
営業戦略部　シニアアカウントマネージャ
安元　英行　氏

昨年から今年にかけて、標的型攻撃をきっかけに大量の個人情報が流出する 2 つの事案が発生した。いずれも、発端はなりすましメールの開封である。そこで今回は、標的型攻撃による被害を防ぐ手段としてのなりすましメール対策について考えていきたい。

標的型メールによる被害の事例

今年 6 月、国内大手旅行代理店において約 679 万人分の個人情報が、また昨年 6 月には中央官公庁から約 125 万件の個人情報が漏洩した可能性がある、という事案が発生した。いずれも標的型攻撃によるものであり、送られたメールを開封した事によりマルウェアに感染して PC を乗っ取られた点や、他の PC への二次感染によって拡大した点など、その攻撃手法が共通している。

メールに着目すると、双方の事案とも、攻撃者から送られてきたメールの送信元を詐称されていた可能性が高い。たとえばメール送信元の表示が「山田　太郎＜taro_yamada@example.co.jp＞」であれば、「山田　太郎」が表示アドレス（Display Name）、「taro_yamada」がローカルパート、「@example.co.jp」がドメインパートにあたる。旅行代理店の事案では、オペレータが開いたメールは、ドメインパートは過去に取引があった会社のものだったが、ローカルパートは適切なものでなかったということだ。また当該メールの発信元は海外のレンタルサーバだったため、ドメインは詐称されていた可能性がある。さらに現在、Outlook 等のメールソフトや一部の Web Mail では、受信メール一覧の「送信者」は Display Name が表記されるので、ここも詐称されていたならば、より開封されやすい状況だっただろう。

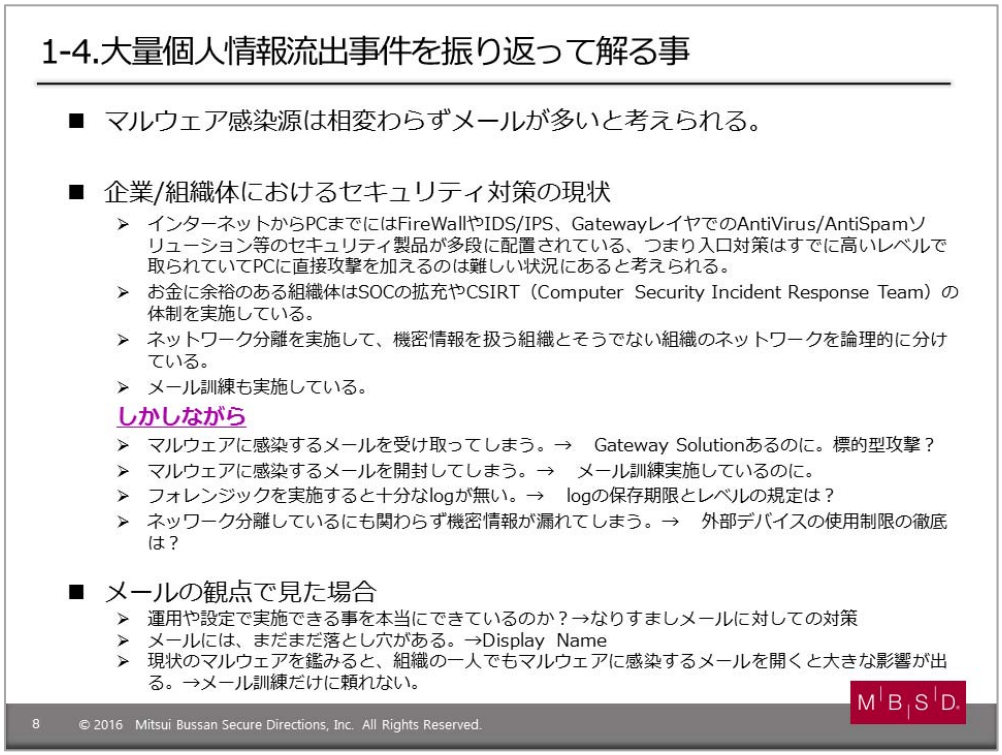
また、中央官公庁における事案では、情報系端末・業務系端末できちんとネットワーク分離を実施していたものの、業務系端末から抽出した個人情報が USB を用いて情報系端末で取扱えるようになっており、標的型メールによってマルウェア感染した情報系端末から、それらの情報にアクセスされたと考えられる。こちらの事案も、なりすましメールがトリガーとなっている。

企業／組織体におけるセキュリティ対策の現状

メールがマルウェア感染源となるケースは、依然として多いと考えられる。最近ではインターネットから PC までのセキュリティ対策、すなわち入口対策を手厚く実施している企業が多いため、PC への直接攻撃は難しくなっているし、ネットワークの適切な運用やメール訓練を行っている企業や、SOC の拡充や CSIRT を構築している企業も少なくない。

しかしこうした対策を講じていても、マルウェアに感染するメールを受け取り開封して実際に感染したり、ネットワーク分離を行っていても外部デバイスの使用制限が徹底されていない等の理由により情報が漏れたりする等の被害が発生してしまう。また被害にあった企業でフォレンジックを実施すると、ログの取得や保管が不十分で、インシデント発生時の影響範囲（流出の有無等）の特定ができないということもある。

被害の発端となるなりすましメールに対する万全の策がとられていないことが多いと推測され、Display Name 詐称への対策や、開封後の出口対策も含め、あらためてこれらの課題に取り組んでいく必要があると考えられる。



なりすましメールの事例分析

なりすましメールは、エンベロープ From と Display Name を詐称しているものが多い。基本的に前者の詐称には送信ドメイン認証（SPF、DKIM、DMARC）が対策として有効だが、なかには認証をパスしてしまうものもある。また、Display Name を詐称されるとユーザーが騙されやすいが、現時点では Display Name 詐称対策として一般化された方法がなく、判定・除去しにくい。

また、送信者認証を行っていないがゆえに、ドメインを攻撃者に使われてしまうというケースもあるので、企業においては、メールに関する設定や運用をきちんと検討し実施すべきである。

対策例と JIPDEC の今後の取組み

攻撃者は、DKIM や SPF、DMARC などの業界標準的な送信者認証に対応していることが多いため、メールなりすましの抜本的な対策には、送信ドメイン認証対応に加えて、別の手段も必要だろう。現在 JIPDEC は、受信メールの安全性を可視化できる「安心マーク」という仕組みを提供しているが、今後はこれに加えて、企業ロゴへの対応と Display Name の識別を進めていくことを検討している。具体的

には、SPF と DMARC への対応を実施すれば、受信メール一覧に企業ロゴを表示させることで安全性を担保する、という仕組みである。また安心マークや企業ロゴがついていないものについては、Display Name ではなくリアルな From メールアドレスを表示させる、といった仕組みも検討していきたい。なお、三井物産セキュアディレクション（MBSD）では、脅威情報との突合を行い、1.マルウェア感染後の悪意あるサイト（C&C サーバ等）へのアクセス防止、2.フィッシングメール等に掲載されている攻撃者サイトの URL へのアクセス防止、3.業務でウェブサーフィンを閲覧する際に攻撃者の用意したサイトへのアクセスを防止するといった、「MBSD Proxy Security Service」という出口対策サービスを提供している。

標的型攻撃による被害をなくすため、送信者ドメイン認証を用いたなりすましメール対策や、多段構成および出口対策等、マルウェア感染を念頭に置いた対策を講じることが重要である。