eRanger

イー・レンジャーのかわら版 (2019 年 2 月第 35 号)

■ メールの乗っ取りと対処について

年があけて**2度**も**セキュリティ関連の事件**がありました。よい事例ですので、そのうちの1つの概要と対策についてご紹介したいと思います。
事件を一言で言うと、**「メールの乗っ取り」**です。以下がその概略図です。

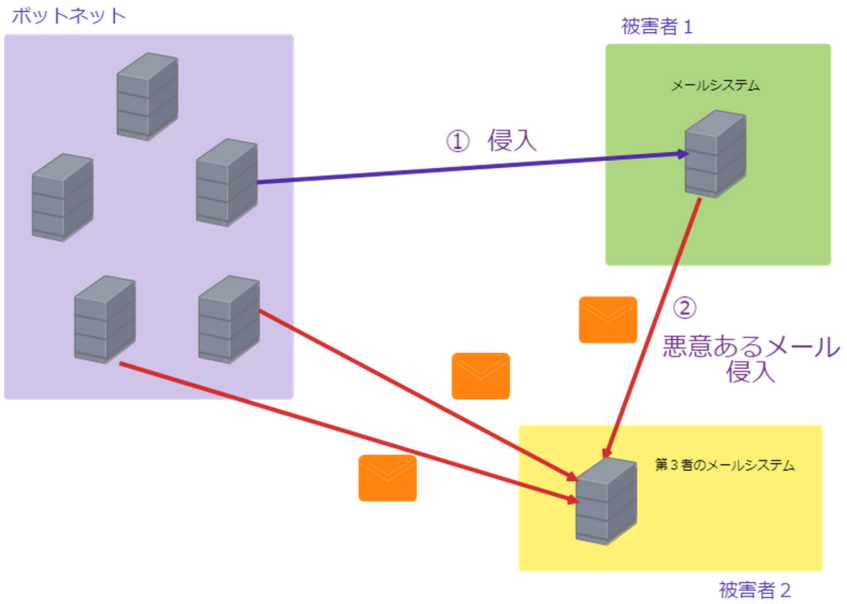

図1：メールの乗っ取りと被害（弊社作成）

弊社のお客様は図右上の「被害者 1」です。お客様のメールが（中国から）夜中に侵入されてしまいました。朝いちばんで電話をいただき、一番最初に懸念したのが「情報の流出」でした。**「お客様の機密情報」、「お客様のお客様の機密情報」が漏れてしまったら**大変なことになります。
お客様は Office365 をご利用になられています。**Office365 にはさまざまなトラッキング機能（監査機能、ログ機能）がついています**ので、これらを利用して調査したところ**情報の流出はないことがわかりました**。
「それではなぜ侵入したのか」という疑問が残ります。調査の結果、**スパムメールを送るための踏み台**とされたことがわかりました。不正に入手された大量のメールアドレス（メールシステム）は「ボットネット」と言われる**「攻撃軍団の兵隊」**として利用されます（図左上）。今回のケースでも、お客様のメールアドレスから数百のスパムメールが世界中にばらまかれていました。被害者から一転加害者になってしまったということです（図中②）。侵入から弊社でメールアドレスをロックするまでに **10 時間程度**を要しました。ばらまかれてしまったものは取り返しがつきませんが、被害は最小限ですんだと考えています。
「なぜ侵入されたか」を正確に知ることは不可能なのですが、今回のケースでは**「推測しやすいパスワード」**を利用していたことが原因と推測しています。攻撃をする側は、（今回のケースでは）お客様を狙い撃ちしたわけではありません。インターネットに公開されているドメイン名やアドレスを入手してメールサーバーを調べて（インターネットの仕組み上公開されています）侵入を試みます。このとき、**社名や社長の名前、創立記念日のようなパスワードを使うと侵入のリスクが高まってしまいます**
一つの目安としては**「ランダムな 10 桁以上のパスワード」**を設定するのが、よい対策となります。また、このような**「事件が発生したときに対処ができるメールシステム」**をお使いになられるべきと思います。