ＮＴＴアドバンステクノロジ
標的型メール耐性診断サービス

標的型メール攻撃に対する社員対応を訓練し企業の情報インシデント耐性を強化します

標的型メールによる情報セキュリティインシデントがあとを絶ちません。
もっとも効果的な対策は、実際の標的型メールを模した訓練を定期的に抜き打ちで行い、社員に体験させることです。
NTTアドバンステクノロジ（以下、NTT-AT）は、実際のインシデント事例とその対策ノウハウを蓄積しており、
実状に即した効果的な耐性診断を提供しています。

特定の企業やユーザを狙った標的型攻撃が急増 巧妙に偽装した標的型メールの被害があとを絶たない

標的型攻撃とは、特定の組織やユーザを狙った攻撃です。そのため、攻撃手法もこれまでのものとは異なり、巧妙になってきています。一例として、攻撃対象とした組織専用の文面や添付ファイル名をつくることで安心させ、「業務に関連する内容だから開封しなければ」という心理をついてきます。事実として近年はこの標的型攻撃が急増しており、2015 年は前年の 2 倍以上となる 3,828 件が確認されています※。そして、攻撃を受けたメールアドレスのうち、89% が公開されていないものでした※。これまでも、公的機関や民間企業など、多数の組織・団体が被害にあっていますが、そのほとんどのケースでウイルス対策は実施済みでした。つまり、標的型攻撃はこれまでのウイルス対策だけでは防ぐことは難しいのです。

標的型攻撃の中でも、標的型メールによる情報セキュリティインシデントがあとを絶ちません（図 1 参照）。実際にインシデントを起こしてしまった人のほとんどは「まさか標的型メールとは思わなかった。」と口をそろえますが、巧妙な偽装が進化し続けているため、対策の講習やマニュアルだけでは防げないのが実状です。その中で効果的な対策は、実際の標的型メールを模した訓練を定期的に抜き打ちで行い、インシデントに至るまでの経緯を、社員に身を持って体験させることです。NTT-AT は、情報セキュリティ分野において扱ってきた実際のインシデント事例とその対策ノウハウを蓄積しており、実情に即した効果的な耐性診断を提供しています。

※警察庁「平成 27 年におけるサイバー空間をめぐる脅威の情勢について」より

耐性診断により社員のセキュリティ意識レベルを可視化して標的型攻撃に必要な対策を見極める

セキュリティ対策にはさまざまなものがありますが、そのすべてを導入するには非常に高いコストが必要となり、多くの場合においては現実的な選択肢とはならないことがあります。限られたコストを有効に活用するためにも、まずは耐性診断を実施し、本当に必要な対策を見極めることが大切です。例えば、耐性診断により下記のような情報を把握することで、より有効と思われるものから順に対策を

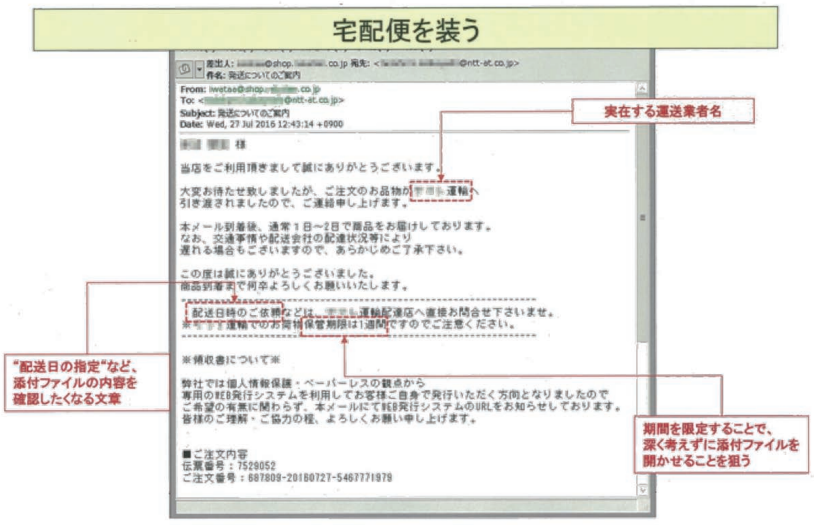

図1　さらに巧妙になる標的型メールの攻撃例

検討することが可能になります。

- ●全社員のセキュリティ意識レベルを可視化して適切な対策を選択
- ●開封しやすい部署や役職をあぶり出すことで対策リソースを集中
- ●メールを開いてしまった後の処置や報告などの事後対応の確認

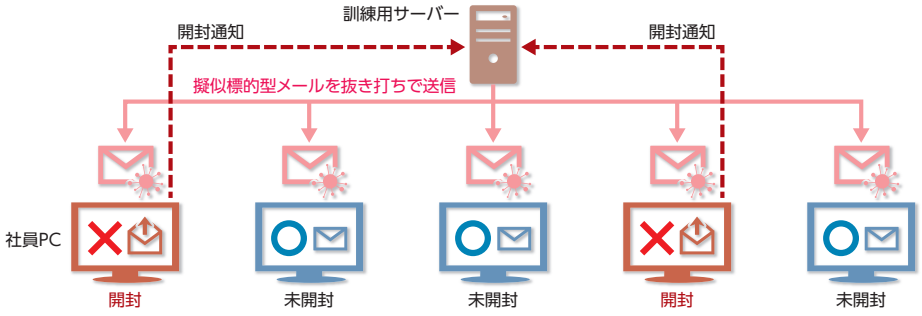

図２ 「標的型メール耐性診断サービス」のサービス概要

この他にも、診断用のテストメールとはいえ、実際の標的型攻撃を模したメールが社員本人に送られることで、「自分には送られてこない」との油断や思い込みを正せたり、標的型攻撃の巧妙さを理解してもらうことなどの効果も期待できます。

最新事例に基づいた訓練サービスを提供 診断後のアフターフォローも充実

標的型攻撃の巧妙さを裏付けるように、実際に標的型メールの被害にあったケースでは、「この内容は一目見ただけでは標的型メールだと判断ができない」、「ファイルを開封した後も指摘されるまで標的型メールだと気がつかなかった」といった声も出ています。最も重要なことは、標的型メールを全社員が見抜けられるようになることです。

NTT-AT が提供している「標的型メール耐性診断」および訓練サービスは、よくありがちな“トレンドから外れた古い内容”や“使い回しの机上の判断テスト”ではありません。普段は標的型攻撃を“防御する側”であり、数々のソリューションや対応実績を持つなど、情報セキュリティ分野において数多くのインシデント事例を扱ってきた NTT-AT だから実施できる“本物と見紛う”擬似標的型メールでの訓練こそが、真のインシデント耐性の強化に大きく貢献することになります。

図２は、NTT-AT が提供する「標的型メール耐性診断サービス」のサービス概要です。本サービスの特徴として次の３つがあげられます。

【１】抜き打ち訓練の効果を高める、リアルかつ自然なメール文面

【２】複雑なシステム変更は不要！ ご依頼後、最短１週間で診断が可能

【３】診断後のアフターフォローが充実

アフターフォローとしては、社員のセキュリティインシデントに対する意識確認するためのアンケートの実施や、開封してしまった社員を対象とした研修・教育コンテンツの提供、効果的な対応策のコンサルティング、具体的なセキュリティ環境の構築など、診断結果に基づいてお客様ごとの課題点に合わせたソリューションを提供（一部オプションでの対応）しています。

標的型攻撃は、我々の心の隙間を巧妙に突いてきます。“ウマいこと考えるなぁ”と感心する程です。NTT-ATのサービスは、最新の“ウマいこと”として考えられた攻撃メールを参考にしていますので、標的型攻撃の巧妙さを体感いただけます。是非、標的型攻撃に騙されないよう、共に頑張っていきましょう。

ＮＴＴアドバンステクノロジ
セキュリティ事業本部　マネージドサービスビジネスユニット
主任技師　**古林 忠史**

お問い合わせ先

NTTアドバンステクノロジ株式会社　商品お問い合わせセンタ
TEL：0120-057-601　E-mail：sales@ml.ntt-at.co.jp

※http://www.bcm.co.jp/でも閲覧できます。