NTT AT

企業向けサイバーセキュリティソリューション

標的型メール耐性診断サービス

全世界に猛威をふるうランサムウェアを防ぐには、社員への“抜き打ち訓練”が必要です！

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。

標的型メール耐性診断サービス

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。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。」と口を揃えますが、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。
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おこない、インシデントに至るまでの過程を、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、実状に即した効果的な耐性診断をご提供します。

標的型メールの“特徴や傾向”をご存知ですか？

悪意を持った標的型メールは、ターゲットが安易に開いてしまうよう仕向けるための特徴や傾向があります。当社では過去のインシデント事例からこれらを分析し、耐性診断に盛り込んでいます。

- 騙されやすい件名は？
- 狙われやすい業種・業態とは？
- 狙われやすい曜日や時間帯がある？
- 開いてしまう人の特徴とは？
- 犯罪者が狙う情報とは？
- 開いてしまったら具体的にどうなる？

私たちは、このような特徴や傾向を数多く把握しています。
明日狙われるのは御社かもしれません。今すぐお問い合わせ下さい！

実際の攻撃事例に基づき、リアリティの高い標的型メールを再現

もっとも重要なことは、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。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来た当社が作成する、“本物と見紛う”擬似標的型メールでの訓練が、御社のインシデント耐性を強化します。

● 標的型メールの文例

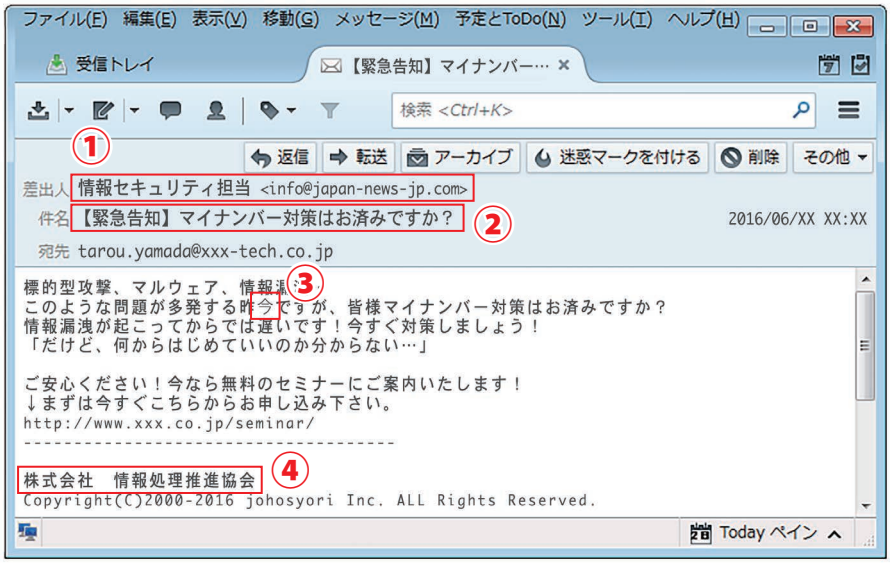
ポイント① 送信者名を偽装

ポイント② 件名が最新の話題

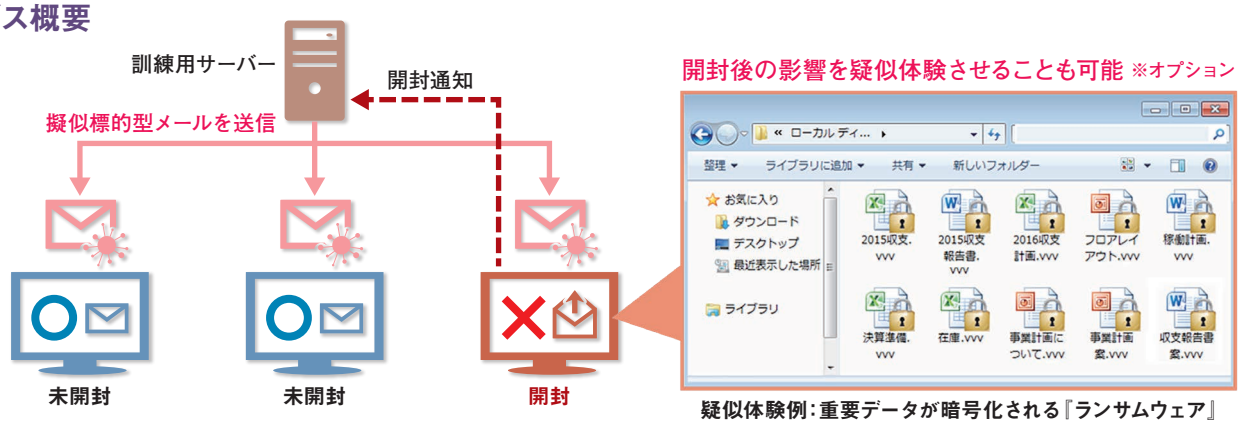
ポイント③ 不自然なフォントや文字化け

ポイント④ 架空の企業・団体名

これは過去の標的型メールの例ですが、最近では巧妙化が更に進んでおり、セキュリティ分野に精通した技術者でも、一見しただけでは通常のメールと見分けがつかなくなって来ています。当社では最新事例に基づいた“リアルな訓練”をご提供します。



● サービス概要



なぜ標的型メール耐性診断が必要なのか？

- 標的型攻撃やランサムウェアを疑似体験させ、セキュリティの重要を意識させる
- 開封しやすい部署や役職をあぶり出して適切な対策を選択
- 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

● 価格

診断対象のメールアドレス数	メール文面数	価格（税抜）
～100	1種	￥200,000
	2種	￥300,000

お問い合わせ先 **http://www.ntt-at.co.jp/product/yarai-taisei/**

NTTアドバンステクノロジ株式会社
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
〒212-0014 神奈川県川崎市幸区大宮町1310 ミューザ川崎セントラルタワー