神奈川県警察からのお知らせ

標的型メール攻撃の脅威

インターネットが、国民生活や社会経済活動に不可欠な社会基盤として定着している中、私たちの生活に密接な関係にある事業者に対するサイバー攻撃が続発し、社会問題となっています。

そこで今回は、サイバー攻撃のうち、“標的型メール攻撃”の手口等について紹介します。

概　況　平成26年中の標的型メール攻撃件数は過去最高

平成26年は、我が国の事業者等からの情報窃取を企図したとみられるサイバー攻撃が多発しました。

警察では、平成26年中、1,723件（前年比＋1,231件）の標的型メール攻撃の発生を把握しました。

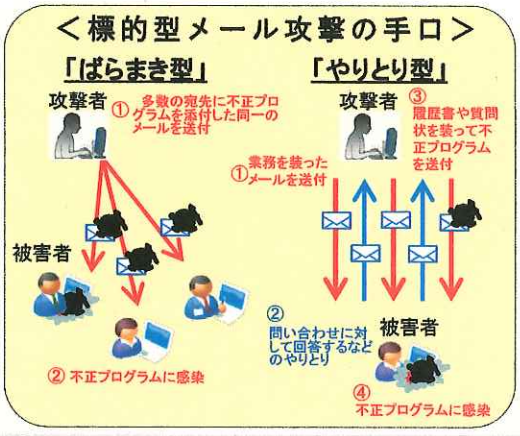
手　口　「ばらまき型」と「やりとり型」

《 ばらまき型 》

多数の宛先に同一の文面及び不正プログラムを添付したメールを一斉に送付する手口

《 やりとり型 》

採用活動や取引等、業務との関連を装った通常のメールのやりとりを何通か行うことにより、添付ファイル付きのメールが送付されても不自然ではない状況を作った上で、不正プログラムを添付したメールを送付する手口



～ 標的型メール攻撃の事例 ～

【事例１】医療費の通知を装った内容の標的型メール攻撃

企業等の健康保険組合からの医療費の通知を装い、受信者が違和感を感じにくい内容のメールを作成して不正プログラムを添付

【事例２】特定分野の研究会等を装った標的型メール攻撃

特定分野の研究者やメーカーが集まる展示会等の、参加申込み方法の通知や参加者名簿の送付を装い、攻撃対象を絞って不正プログラムを添付したメールを送付

巧妙化・多様化するサイバー攻撃

～今、求められている対策とは～

近年、攻撃対象のコンピュータに不正プログラムを感染させる手口が巧妙化しています。

そのため、情報システムの運用・管理に当たっては、基本的な対策（**不審なメールを安易に開封しないこと、ソフトウェアを最新版に保つことなど**）を維持しつつも、それらをすり抜けて侵入する不正プログラム等の脅威があることを前提に、機微な情報の暗号化、機密性に応じたアクセス権の設定、ネットワークの分離等、“リスク・ベース”の防護を複層的に講じることが必要です。