サイバーセキュリティ パートナーシップだより

R7-5

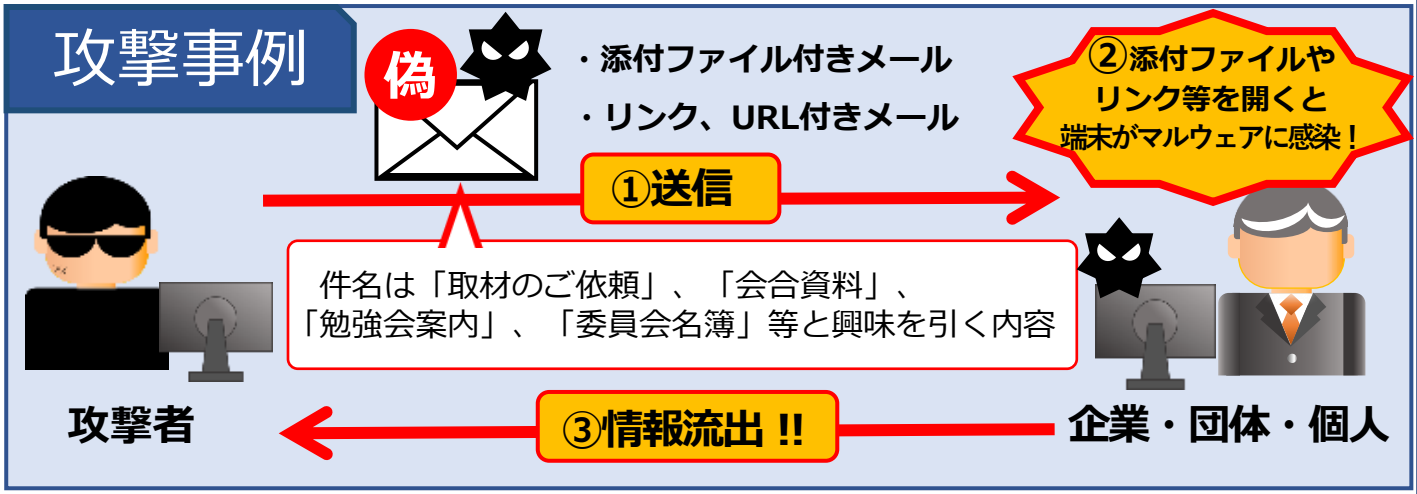
関係者からのメール？ それ本当？

標的型メール攻撃 に注意！！

標的型メールは、取引先や関係者になりすまし、特定の事業者の重要情報を盗むことを目的に不正プログラム（マルウェア）に感染させるメールです。

現在、日本国内の学術、シンクタンク、政治家、マスコミに関係する個人や組織に対し安全保障や先端技術に係る情報を窃取する組織的なサイバー攻撃が行われているため、注意をお願いします。

攻撃事例



被害に遭わないためには？

1 交流相手からのメールでも、普段と異なる状況であれば注意する

一例
- 送信元のメールアドレスが、フリーメールアドレスからの送信
- 第三者のメールアカウントを乗っ取り、なりすましメールを送信

2 違和感があれば不用意に添付ファイルやリンクを開かない

一例
普段はファイルをそのまま添付するやり取りが多いのに、パスワード付きZipファイルで届く場合や、リンクからファイルをダウンロードさせようとする場合　等

3 不審に感じたら、電話など別の方法で送信者へ問い合わせる

送信事実がなければ職場のシステム部門に速報し、組織内で情報共有する

MirrorFaceによるサイバー攻撃について（注意喚起）

https://www.npa.go.jp/bureau/cyber/koho/caution/caution20250108.html

サイバー犯罪相談事例
対処法と対策・相談窓口

県警ホームページにて広報資料や動画を公開中です。
（詳しくはQRコード参照）

警察庁
National Police Agency