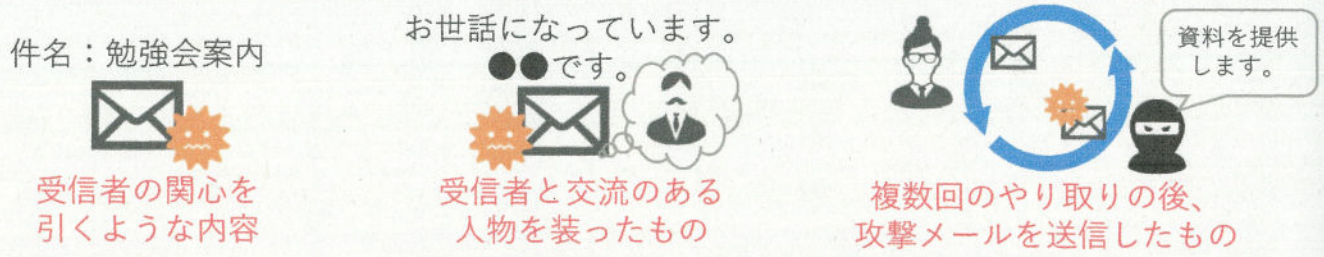
高度なサイバー攻撃にご用心！

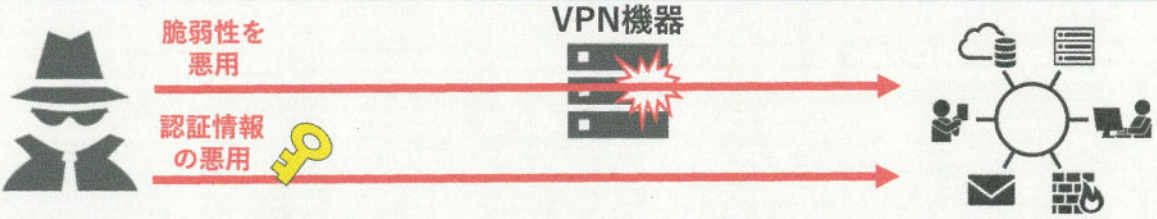
令和７年１月８日、警察庁及び内閣サイバーセキュリティセンターから、「Mirror Face」（ミラーフェイス）と呼ばれるサイバー攻撃グループによるサイバー攻撃について、注意喚起が発出されています。

Mirror Faceによる攻撃事例①



- 攻撃メールは、メール受信者の興味を引く内容であったり、複数回のやり取りの後に送信するなど、受信者が添付ファイルを開いたり、メール本文に記載されたURLへアクセスするよう誘導する事例が確認されています。
- 添付ファイルは、Microsoft WordやMicrosoft Excelなどを使った事例が把握されており、Microsoft Officeファイルのマクロを有効化することによって、マルウェア（悪意のあるソフトウェア）に感染します。

Mirror Faceによる攻撃事例②



- VPN機器の脆弱性や何らかの手段で得た認証情報の悪用により、攻撃対象のネットワークに侵入したとみられる事例が確認されています。

攻撃の検知・緩和策の一例

- 受信したメールに普段と少しでも異なる状況や違和感があれば、添付ファイルを開いたり、リンクをクリックしたりせず、送信者に確認する。
- 添付ファイル等を開いた際に、Microsoft Officeファイルのマクロ「コンテンツの有効化」ボタンをクリックするよう誘導されても、安易にクリックしない。
- ネットワーク機器の脆弱性に関する情報収集を行い、最新のパッチの適用やファームウェアの更新を行う。
- 侵害の原因と範囲の把握に必要不可欠な情報源となるログは、広範囲かつ長期間にわたって保存するようにするとともに、攻撃者によるログの消去を考慮して、可能な限り別のサーバへ集約して保存する。

被害発生時や不審なメールに気がついたときは、通報・ご相談を

盛岡西警察署警備課
019-645-0110