



巧妙化するボイスフィッシングへの対策

昨年発生したボイスフィッシングが、遠隔操作アプリを悪用する手口へと変化しています。

電子証明書の導入などの技術的対策だけでは十分に防止できないことから、下記の事項について関係者への注意喚起及び不審な連絡を受けた際の相談体制の確立をお願いします。

遠隔操作アプリが利用される理由

・ 「電子証明書」をすり抜けるため

正規の利用者の端末を遠隔操作することで、端末に保存された電子クライアント証明書をそのまま利用し、正規利用者として認証を突破します。

・ 銀行の「不正検知システム」を騙すため

遠隔操作により正規利用者の端末から通常どおり操作しているように見せかけることで、不正検知システムによる異常なアクセスや不正送金の検知を回避します。

被害防止対策

1 その場で判断や回答をしない

緊急を要する内容でも、その場で口座番号、暗証番号、ログインID・パスワードなどの重要情報を相手に伝えない。

2 折り返し確認の徹底

銀行を名乗る不審な電話があった場合は、営業店・代表電話に折り返して内容を確認する、インターネットバンキング利用時は公式サイト・アプリからアクセスするといった対応を徹底する。

3 インターネットバンキングへのアクセスの起点限定

銀行を名乗る不審なメール内のリンクにはアクセスせず、必ずブックマーク登録済みの公式URLや公式アプリからアクセスする運用を徹底する。

4 高額送金の複数人承認(ダブルチェック)

送金時の「申請者と承認者を別にする」「高額送金については別の通信手段(対面・内線電話等)での確認を必須とする」といった業務プロセスを設け、認証情報が窃取されても直ちに被害につながりにくくする。

5 着信制限の活用

非通知着信に対するフィルタリングや海外との通話が業務上不要であるならば、国際電話の着信を制限する。

6 PCのソフト制限と保護(システム対策)

業務に必要な指定アプリ以外はPC上で実行できない「許可リスト方式」等を導入する。
不審なツールの起動や不審な挙動をセキュリティシステム(EDR等)で早期に検知・対応できる体制を整える。

被害の発生・疑いがある場合の対応

1 銀行への連絡

金融機関へ至急連絡し、「インターネットバンキングの利用停止」等を依頼する。

2 パスワードの変更と不正送金の有無の確認

安全な端末から、ログインパスワードや暗証番号を直ちに変更し、不正送金の有無を確認。

3 警察への通報

最寄りの警察署、または県警本部サイバー犯罪対策課へ速やかに通報する。