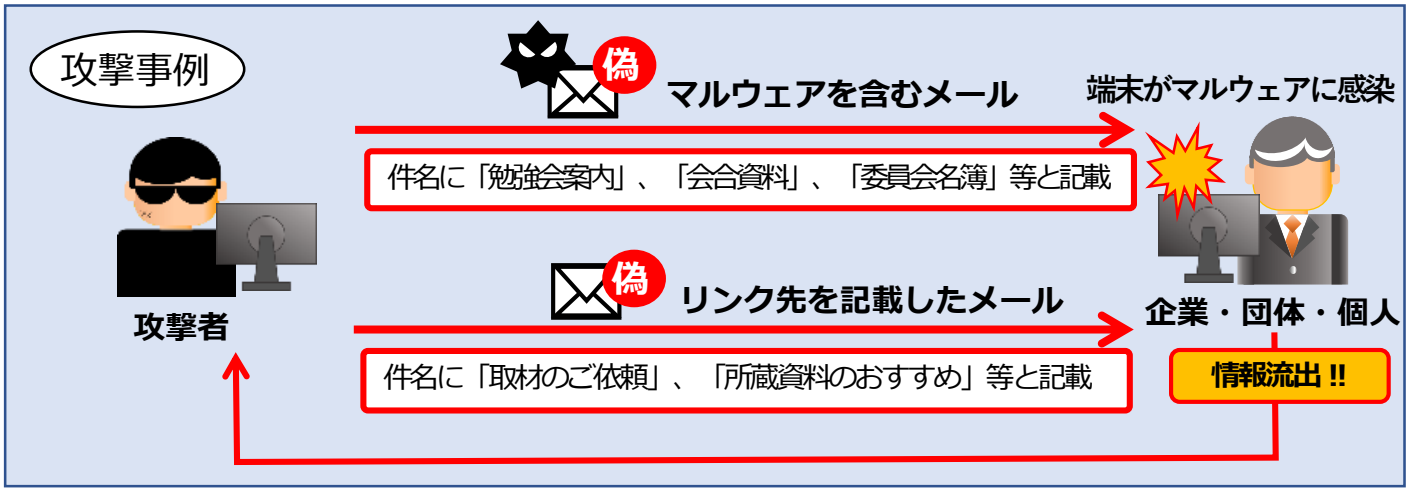
サイバーセキュリティ通信 第16号

令和７年１月
長崎県警察本部
サイバー犯罪対策課

関係者からのメール？それ本当？

もしかしたら、標的型メール攻撃かも？

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て、安全保障や先端技術に係る情報窃取を目的とした組織的なサイバー攻撃が行われています。



被害に遭わないためには？

1　交流相手からのメールであっても普段と異なる状況がないか注意する

例）・最近やり取りがなかったのに突然メールが届いた。
・最近のやり取りの内容と全く脈略のないメールが届いた。
・過去にやり取りをしたことがない相手からメールが届いた。

2　違和感があれば添付ファイルの開封やメール本文にあるリンクをクリックしない

・送信元のメールアドレスを確認する。
・開封等をする前に送信者に対して別の連絡手段でメール送信の事実があるかを確認する。

3　送信ドメイン認証（SPFなど）の機能を利用する

送信元メールアドレスを正規のドメインに詐称したメールが送られてくることがあるため、送信ドメイン認証（SPFなど）の機能を利用して、メールが正しい送信元から送られてきているかどうか確認する。

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

長崎県警察本部サイバー犯罪対策課
公式ＬＩＮＥアカウント

警察庁
National Police Agency