ご注意ください!!
標的型メール攻撃が多発中！

特定の組織や人から機密情報等を窃取することを目的とした標的型メール攻撃が多発しています。この攻撃によりウイルスに感染した場合には、自社の企業情報の流出のみならず、関係企業の情報流出や関係企業への攻撃が発生し、賠償責任による補償など大きな経済的損失が発生する可能性があります。

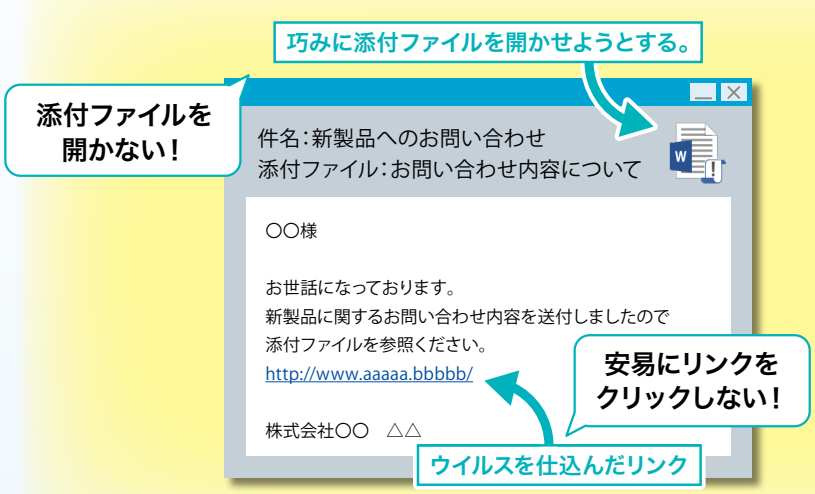
ウイルスの感染経路

- ✓ メールの添付ファイルを開かせる
- ✓ ウイルスを仕込んだリンク先へ誘導

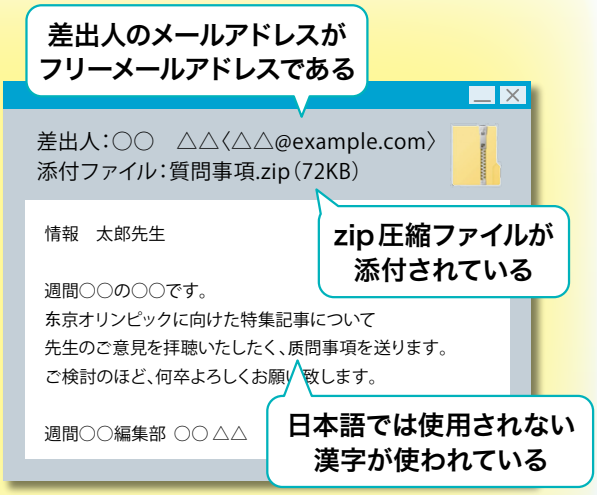
巧みに開封を求める手口

- ✓ 製品やサービスに関する問い合わせ
- ✓ 新聞社などからの取材依頼やアンケート調査
- ✓ 公的機関からのセキュリティー注意喚起
- ✓ 組織内の人事や決済、外部からの配達通知などの案内メール

こんなメールは要注意



【外部からのお問い合わせを装ったメールの例】



【出版社からの取材申し込みを装ったメールの例】

対策

- ✓ 添付ファイル付きのメールは、送信元にかかわらず警戒する
- ✓ 不審に思ったら、開封する前に差出人に確認する
- ✓ 組織内ルールを構築し、不審メールに気付いた場合は速やかに報告する
- ✓ 日常業務を始める前に、アップデートをしてシステムを最新の状態にしてからメールチェックをする

怪しいと思ったら開封前に確認

相談窓口

標的型メール攻撃と思われるメールを受信した場合は

▶ 標的型サイバー攻撃特別相談窓口（IPA）
https://www.ipa.go.jp/security/anshin/

一般的な情報セキュリティ（ウイルスや不正アクセス）に関する技術的な相談は

▶ 情報セキュリティ安心相談窓口（IPA）
https://www.ipa.go.jp/security/tokubetsu/index.html

三重県警察本部生活安全部　サイバー犯罪対策課

対策に関する詳細は、
県警察本部ホームページをご覧ください。▶▶▶