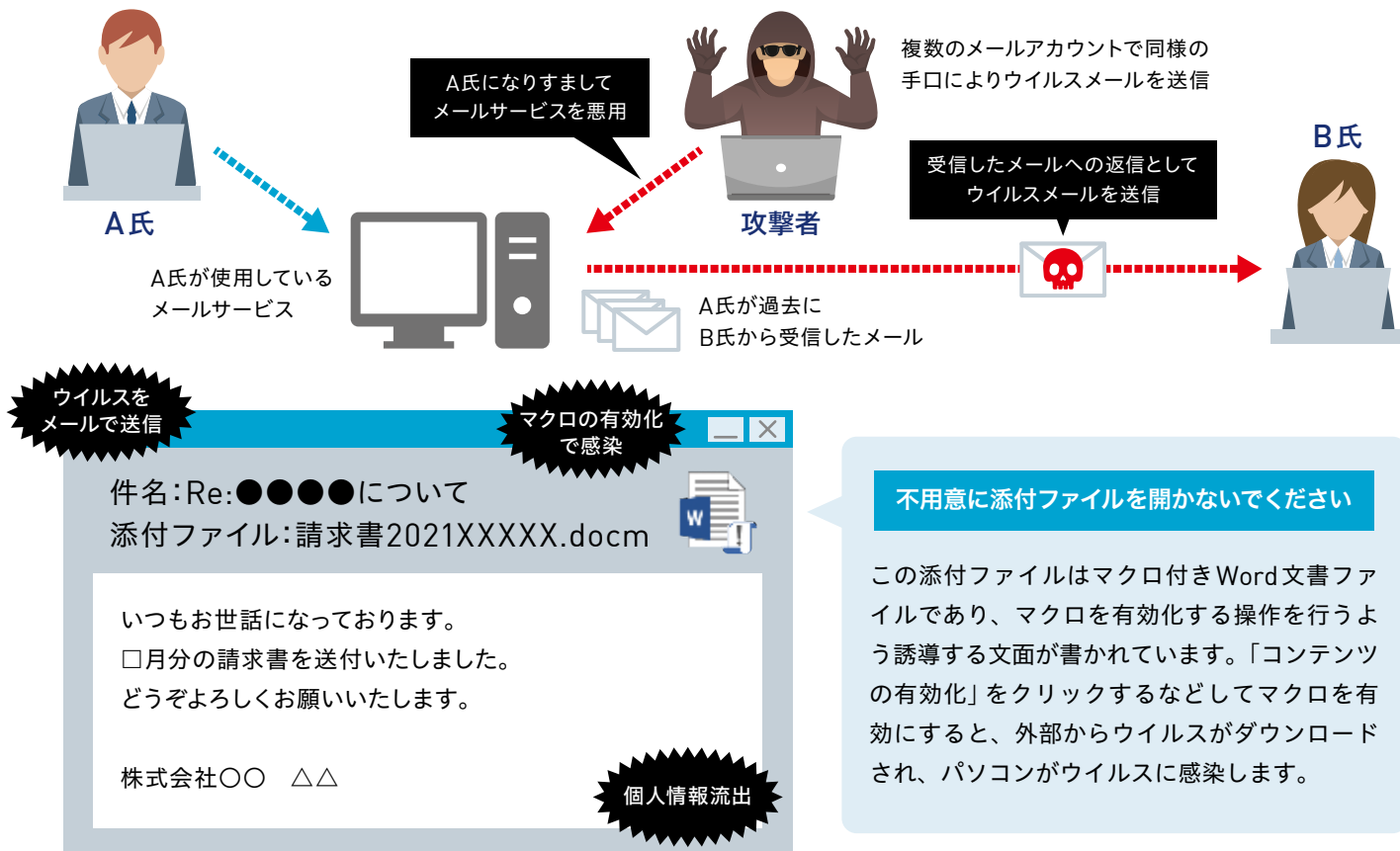


「Emotet」と呼ばれるウイルスを知っていますか？

Emotet [エモテット]とは、受信したメールに添付されたWord形式ファイルを開くことなどにより感染するウイルスです。Emotetに感染すると、感染した端末から連絡先情報などが盗み取られ、さらにその連絡先に対して攻撃メールが送信されるため感染が拡大します。Emotetの攻撃メールには、過去にメールのやり取りをしたことがある人のメールアドレスが送信元に表示されているものや、自分が送ったメールの返信を装っているものなど、受信した人にとって、一見して不審なメールであるか判断しにくいものがあります。知人や取引先からの送信に見えるメールでも、慎重な対応が必要です。

ウイルスメールが送信された状況（推定）



被害防止対策

メールを着信したとき

- メール発信元アドレス・内容をよく確認する
- 不自然な点があれば、差出人に電話するなどして確認する
- 不用意に添付ファイルを開かない

日頃からの対策

- ウイルス対策ソフト、OSを最新の状態に保つ
- WordやExcelなどのマクロを「無効」に設定する

ウイルス感染が疑われる場合

- 感染端末をネットワークから隔離する
- 感染端末で利用していたパスワードを全て変更する
- 過去にメールをやり取りした相手に注意を呼びかける



Emotetに関する情報は、独立行政法人情報処理推進機構（IPA）のウェブサイトでも公開されていますのでご覧ください。
<https://www.ipa.go.jp/security/announce/20191202.html>



三重県警察本部生活安全部サイバー犯罪対策課

協力：三重サイバーセキュリティ・アイザック

