サイバーセキュリティ通信【R4-第1号】

令和４年３月
大分県警察本部生活安全部
サイバー犯罪対策課

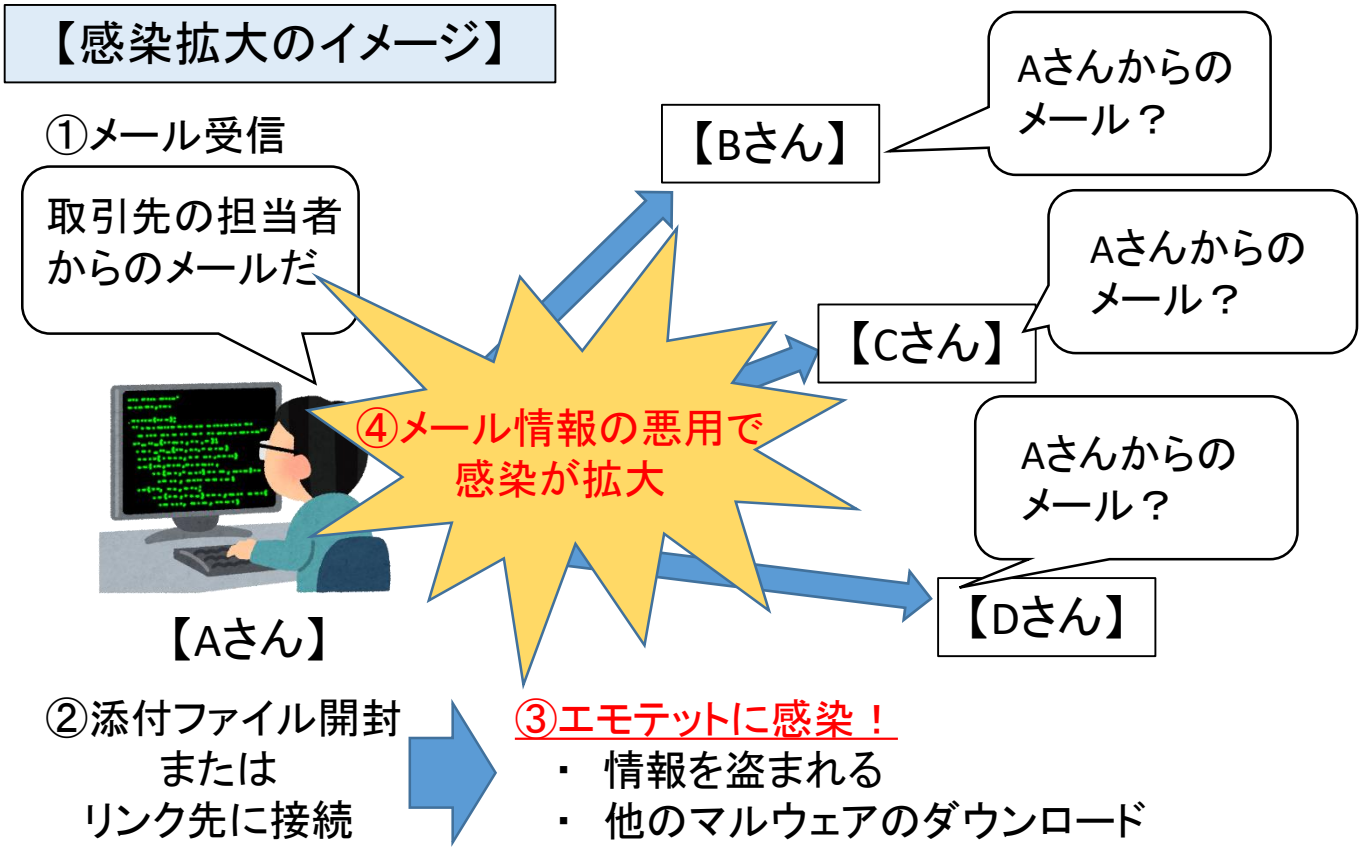
マルウェア「Emotet（エモテット）」に注意！

全国的にEmotetへの感染による被害が拡大しています。

Emotet（エモテット）とは？

・過去にやり取りしたメールへの返信を装ってメールを送信し、添付されたファイルを開封するとエモテットに感染します。
**　感染したパソコンからは、メールアカウント、パスワード、メール本文などの情報が盗まれ、この情報を悪用して感染を拡大させる不正なプログラムです。**

【感染拡大のイメージ】



【最近の事例】

・ 実在の個人名等が記載されているが、メールアドレスや連絡先電話番号等が本物と異なる

・ メールに添付されたファイルの解凍用パスワードが記載されており開封を促す

被害防止対策 知人や取引先からのメールでも要注意!

① ＯＳ、ウイルス対策ソフトなどのソフトウェアを常に最新の状態に更新する

② 不審なメールを受信しても添付のファイルを開封したり、本文中のリンク先にアクセスしない

③ メールの添付ファイルを開いた際、マクロやセキュリティに関する警告が表示された場合は、マクロを有効にしたり、セキュリティ上の警告を無視する様な操作を行わない

④ マクロの自動実行機能を備えたソフトウェアはその機能を無効化する

⑤ 感染が疑われる状況があれば、パソコンをネットワークから隔離する

⑥ ウイルス対策ソフトによるウイルスチェックを行う

・ 不審な内容のメールであれば、開封前に送信者に電話などで事実確認を行いましょう

・ 自らのエモテット感染が疑われる場合は、関係者に電話などで連絡しメールを開封しない様に注意喚起を行いましょう

Emotetに感染した場合や感染が疑われる場合は、最寄りの警察署にご相談ください

あなたの会社や団体で研修の一環として、サイバーセキュリティセミナーを開催しませんか？
小学生から大人まで幅広く対応できます。下記の連絡先にご相談下さい。

大分県警察本部生活安全部サイバー犯罪対策課
企画・指導・サイバーセキュリティ係 Tel:097－536－2131