Ｅｍｏｔｅｔ対策

○　Ｅｍｏｔｅｔとは

Ｅｍｏｔｅｔとは、主にメールの添付ファイルを感染経路としたマルウェア（不正プログラム）です。過去にやり取りしたメールへの返信を装ったメールを送信し、添付ファイルの開封を促します。感染するとパソコンからメールアカウント、パスワード、メール本文等の情報を窃取し、これらの情報を悪用して、感染拡大を目的としたメールを送信します。

（被害例）

- メールソフトやブラウザに記録したパスワード等が窃取される。
- 過去にやり取りしたメールの本文、メールアドレス等が窃取される。
- 窃取されたメール関連の情報が悪用され、感染拡大を目的としたメールが送信される。
- ネットワーク内の他のパソコンに感染が拡大する。
- 他の不正プログラムに感染する（インターネットバンキングの情報の窃取を目的とした不正プログラム等）
- ブラウザに保存されたクレジットカード情報が窃取される。

○　感染が疑われたら

Ｅｍｏｔｅｔの感染の有無は、自分自身で確認することができます。

ＪＰＣＥＲＴコーディネーションセンターのウェブサイトにＥｍｏｔｅｔ専用の感染確認ツール「ＥｍｏＣｈｅｃｋ（エモチェック）」が公開されていますので活用してください。

ＪＰＣＥＲＴコーディネーションセンター「マルウェアＥｍｏｔｅｔへの対応ＦＡＱ」（リンク先：https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html）

○　対処方法

警察への通報・相談の前に

- 感染したパソコンのＬＡＮケーブルを抜くなどしてネットワークから隔離してください。
- 感染したパソコンで使用していたメールのパスワードを変更してください。

警察への通報・相談

資料等を持参して、警察に通報・相談してください。なお、事前に電話で担当者と日時や持参する資料の調整をしていただくと、対応がスムーズに進みます。

サイバー事案に関する相談窓口

（リンク先：https://www.npa.go.jp/bureau/cyber/soudan.html）

○　被害防止対策

被害を防止するためには

- ＯＳやソフトフェアを最新の状態に保つこと。
- ＩＤやパスワードを適切に管理すること。
- ウィルス対策ソフト等を導入すること。

などの一般的なセキュリティ対策に加え、次のような対策を検討してください。

組織内への注意喚起の実施

不審なメールだけではなく、自分が送信したメールへの返信に見えるメールであっても、不自然な点があれば添付ファイルは開かない。メール本文中のＵＲＬリンクはクリックしない。メールに添付された文書ファイルを開いたときに、マクロやセキュリティに関する警告が表示された場合には、マクロを有効にしたり、セキュリティ警告を無視するような操作をしない。

マクロ自動実行機能の無効化

メールセキュリティ製品の導入

不正通信ブロックサービスの導入