令和４年６月１７日
スマート県庁推進課

情報セキュリティ上の注意点について

1. 実在の企業・団体や個人を装った「なりすましメール」

Emotet（エモテット）というマルウェアによる被害が全国的に拡大しています。Emotet は，実在する企業や行政機関等のメールアドレスを送信元として装い，文面もそれらしく巧妙につくられ違和感が少ないため，不審なメールとして判別することが難しいのが特徴です。

✧ Emotet に感染するとどうなるか

次のような危険があります。

- パソコンに保存されている情報が盗み取られる（情報漏えい）。
- パソコンが悪意の第三者からリモート操作される。
- ランサムウェアなどより強力なマルウェアに感染し，パソコンに保存されている情報が読めなくなる（使えなくなる）。
- サイバー攻撃の踏み台として利用される。

✧ 不審なメールへの対処

- 実在する団体や企業を名乗るメールであっても，**不審な点がないか注意**する。
- メールを不審に感じた場合は，**添付ファイルをダウンロードしたり文中の URL をクリックしたりせず**，送信元に電話等で確認する。
- メールに記載された電話番号やメールアドレスは虚偽の可能性があるので，**連絡先は公式ホームページ等で確認**する。
- メールに**添付されたオフィスソフトのファイル**を開いたときにセキュリティ警告が出た場合は，**安易に「コンテンツの有効化」をクリックせず**，送信元に必ず確認すること。

✧ 基本的なセキュリティ対策

- 「Windows Update」などにより，**OS を常に最新の状態**（最新のセキュリティパッチがあたっている状態）にしておくこと。
- Emotet に対応した**ウイルス対策ソフトを利用**すること。
- **ウイルス対策ソフトは常に最新の状態**にしておくこと。
- 利用中の**アプリケーションを常に最新の状態**（最新のセキュリティパッチがあたっている状態）にしておくこと。
- **データのバックアップ**を定期的に行うこと。
- **不審な Web サイトにアクセスしない**こと。

2. アカウントの乗っ取り（主な攻撃手法）

メールアドレスやWebサービスの利用アカウントを乗っ取ることで，虚偽の情報発信や標的とした企業・団体に対し攻撃をしかける足場として利用されたりします。

Emotetなどのマルウェアに感染させる以外にも次のような攻撃方法があります。

✧ 総当たり攻撃

プログラム的にパスワードを生成し，繰り返しログインをリトライする方式。

主な対策

ランダムな英（大小文字）数記号の組み合わせで８桁以上とするなど，**推測しにくいパスワード**とする

✧ パスワードリスト攻撃

脆弱なシステムから窃取したアカウント情報を使って，別のシステムにログインを試す方式。

主な対策

同じ**パスワードを**複数のサービスで**使い回さない**。

✧ フィッシング詐欺

偽サイトに誘導し，巧みにアカウント情報を入力させ盗み取る方式。

主な対策

（１）メール等に貼られている**リンクを安易にクリックせず**，URLをよく確認する，（２）信頼できるサイトからリンクを辿る

✧ ソーシャルエンジニアリング攻撃

ターゲットとなる対象に，電話等により利用者や管理者のフリをしてパスワードを聞き出したり，パスワードの変更を依頼したりする方式。

主な対策

公式の情報から得られる電話番号やメールアドレスを確認して，連絡を改めてし直すなど，**相手を安易に信用しない**。

✧ ショルダーハッキング

アカウント情報を入力する画面を後ろからのぞき見る方式。

主な対策

モバイルワークでPCを利用する場合は，**背後に人が立てない場所を利用**し，**のぞき見防止フィルターをつける**

✧ セキュリティの脆弱なWi-Fiを利用したハッキング

通信が暗号化されていないか，セキュリティ強度の低い暗号化方式を採用している無線通信から内容を読み取る方式。

主な対策

フリーWi-Fiを使って業務をしない，アカウント情報を入力しない。

3. システムやネットワークへの攻撃

一般に，コンピュータ・システムは頻繁に脆弱性が発見されます。またネットワークを構成するハードウェアやソフトウェアについても同様です。

脆弱性が公表された場合対応方法が同時に示されるので，できる限り**迅速に対応する必要があります**。

脆弱性を放置しておくと，**情報の漏えい**やシステムの停止**といった被害を被る**ことがあるほか，攻撃の踏み台に利用された場合，加害行為に荷担することにもなります。

対策として，**セキュリティに詳しい事業者に運用を委託することが必要**です。

半田病院の事例は，このケースに該当します。

4. サプライチェーン攻撃

取引先や委託先を踏み台として狙いを定めたターゲットを攻撃する手法を「サプライチェーン攻撃」といいます。

大手企業や都道府県庁などはセキュリティ対策がしっかりされているので，直接攻撃せず，**セキュリティ対策が十分でない取引先や委託先を足がかりに**します。

トヨタ自動車の主要サプライヤーの 1 社がランサムウェアに感染したことがきっかけで，トヨタ自動車の生産ラインが止まった事例が有名です。

対策は**取引先や委託先にセキュリティ対策の徹底を呼びかけることが基本**となりますが，場合によっては，**県による監査や指導**が必要です。

5. 公的機関や企業等の偽サイト

現在，公的機関，企業・団体等の本物の Web サイトと同じ内容を表示する偽サイトの存在が確認されています。これらの偽サイトのうちには，クリック先が**悪質なサイトへのリンクに置き換えられている**ものがあり，**サイバー犯罪等に用いられる可能性があります**。

対策として，受信メールのリンクをクリックしてサイトを開くなど普段と異なる方法で利用する際は，リンクにポインタを置いたりアドレス欄をよく見る等により，URL の「ドメイン名」を必ず確認してからにしてください。不審な場合には，**安易にアクセスしたり，当該 Web サイト上の何かをクリックしたり絶対にしないで**ください。