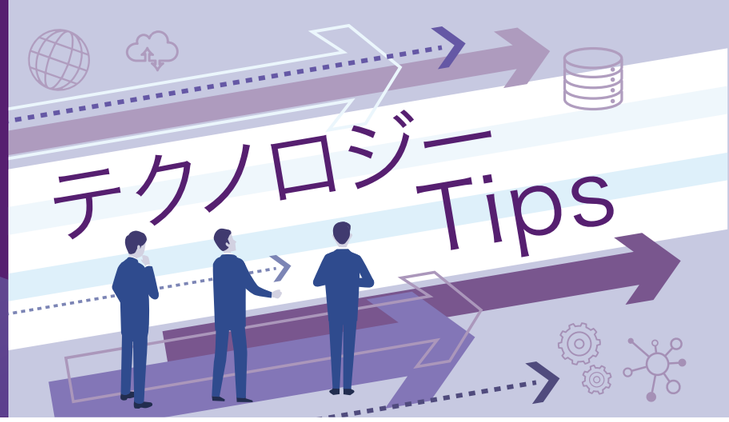
ダイチ通信
今こそ知りたい
＼テクノロジーTips！／
vol.7

DXの基盤構築に必須！

もう一度！セキュリティのポイントを分かりやすくまとめます！社内のセキュリティ水準を向上させましょう！



＼ セキュリティ基本要素のおさらい ／

セキュリティ対策の前提として…

対策を講じる前にやるべきこと、それは保護対象のデータを特定することです！

データの所在や更新状況が不明といった状態で闇雲にセキュリティ対策を打っても、高い効果は期待できません。自社にとって必要な情報とは何かをしっかり見極め、適切な対応をとっていくことがとても重要です。そのために、「データの5S活動」を実践しましょう！データの5S活動については後述します。特定された保護対象のデータは、以下の7要素でしっかりと安全を担保しましょう！セキュリティ基本要素のおさらいです！

セキュリティ基本要素

① 機密性
許可された人だけがデータにアクセスすることができる状態を確保する。

② 完全性
情報が改ざんされておらず、信頼に足る状態が保たれている。

③ 可用性
アクセス権限がある人は、いつでもその情報にアクセスできるということ。
「機密性」の担保が前提。

④ 真正性
署名や認証等(指紋認証やハッシュ等の暗号化技術)により利用者の適正性、データの「完全性」が担保されているということ。

⑤ 責任追及性
各機器から出力されるログおよびログ管理システムにより、いつ何が起こったのかを適切に追跡・追及できるということ。

⑥ 否認防止
タイムスタンプや署名技術を活用し、発生事象や作成されたデータを遡及的に否定されること
(=否認)がないようにすること。

⑦ 信頼性
ハードウェアの冗長化（予備装置の配置）等、システムの安定稼働技術により、適切な情報システム処理、矛盾のない動作が実行されていること。

＼ セキュリティ対策の第一歩！データの5S活動を行いましょう！／

データの5S活動とは…

1	整理	使わないデータや重複データ、最新版以外のデータを削除する。
2	整頓	共通のフォルダを作成し、データの格納場所を決定する。フォルダの階層やファイル名に規則性を持たせる。
3	清掃	データの新たな保管場所を確保する。そこに整理・整頓されたデータを保管し、ファイル名に保管期限などを明記しておくことで、定期的に不要データを削除する。元のデータはバックアップデータとする。
4	しつけ（ルール）	サーバー管理者（または情報管理責任者）を決め、社員に対しデータ保管のルール（ファイル名のつけ方、保管期限など）を徹底させる。
5	清潔	サーバー管理者（または情報管理責任者）が定期的にデータの整理ができているか監視し、「整理」「整頓」「清掃」が維持できる環境を整備する。

＼ セキュリティ関連の基本法とガイドライン ／

TOPIC 01 セキュリティ関連の法律

◎個人情報保護法

2022年4月1日から改正個人情報保護法が施行されました。
個人情報の利用停止・消去等の請求範囲が拡大されるなど、個人の権利利益の保護が強まる一方、特定の個人を識別できないように加工した「仮名加工情報」が新たに創設され、利用目的変更の制限や利用停止請求への対応などの義務を緩和する内容も含まれています。
仮名加工情報は、一定の安全性と有用性を両立でき、マーケティング分析等にも有用です。

◎不正アクセス禁止法

不正アクセス行為や、不正アクセスにつながる識別符号の不正取得・保管行為、不正アクセス行為を助長する行為等を禁止しており、不正アクセスを行った場合には、3年以下の懲役又は100万円以下の罰金に処す等、罰則規定もあります。

- 不正アクセス行為とは… 他人のID・パスワードを入力したり、脆弱性を突いたりなどして、本来は利用権限がないのに、不正に利用できる状態にする行為
- 識別符号とは…… 情報機器やサービスにアクセスする際に使用するIDやパスワード等

（参考：総務省 国民のための情報セキュリティサイト）

◎刑法 ～不正指令電磁的記録に関する罪（コンピューター・ウイルスに関する罪）～

コンピュータ・ウイルスの作成、提供、供用、取得、保管行為が罰せられます。

- ウイルス作成・提供罪/供用罪 → 3年以下の懲役又は50万円以下の罰金
- ウイルスの取得・保管罪 → 2年以下の懲役又は30万円以下の罰金

TOPIC 02 サイバーセキュリティ経営3原則

1. 経営者は、IT活用を推進する中で、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要
2. 自社は勿論のこと、系列企業やサプライチェーンのビジネスパートナー、ITシステム管理の委託先を含めたサイバーセキュリティ対策が必要
3. 平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策、対応に係る情報の開示など、関係者との適切なコミュニケーションが必要

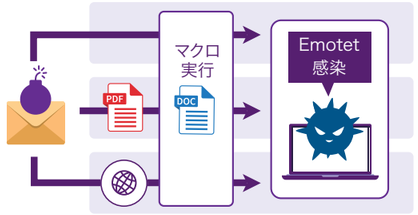
（引用：IPA サイバーセキュリティ経営ガイドライン解説書）

＼ 近年のセキュリティトレンド ／

Emotetの猛威に見る添付ファイルの危険性

Emotetはメール経由で拡散するマルウェアです。
Emotetに感染すると、端末に登録されているアドレス宛にスパムメールが送信されるため、爆発的な感染拡大に結び付きやすく、差出人やメールタイトルの偽装、過去のやり取りを想起させる情報等により真正なメールであると誤認しやすい点も特徴です。不用意に添付ファイルやURLを開かない、不自然な点があれば、送信元に確認するといった対策も重要ですが、そもそもの感染源である「添付ファイル」というものを見直す必要があります。
近年、大手企業や政府機関が次々と「脱PPAP」を表明しています。PPAPとは、パスワードで保護されたファイルの送信から、後で送られてくるパスワードでファイルを解凍するまでのプロセス（P:パスワード付きZIPファイルを送る→P:パスワードを送る→A:暗号化→P:プロトコル）をそれぞれの頭文字で表しており、日本企業特有の対策です。データの盗み見を防止するためのセキュリティ対策として実施されてきましたが、パスワード付きZIPファイルはフィルタをすり抜けてしまうため、Emotetのような添付ファイルを経由するマルウェアに対しては実効性に乏しく、むしろこれがリスクを高める可能性があると指摘されています。PPAPシステムを入れているから大丈夫、といった意識の低下も問題です。
添付ファイルでのデジタル文書のやり取りは、ハイリスクかつ時代遅れの手法となっています。Emotet対策の一環として、見直していくことが必要であると言えるでしょう。

●Emotet感染の仕組み

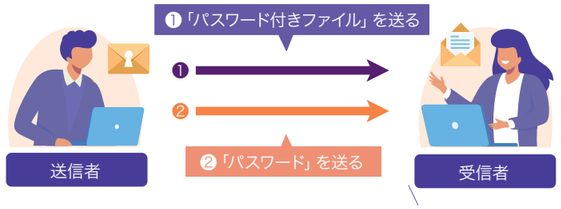


メールに添付されたファイルを通して感染。

Emotet感染対策

- ✓不用意に添付ファイルやURLを開かない
- ✓不自然な点があれば、送信元に確認する

●PPAPの仕組みと問題点



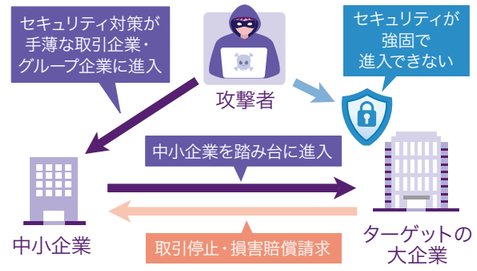
PPAPの問題点

- ✓メール盗聴のリスク
  ファイルとパスワードの送信経路が同じため、盗聴される可能性。
- ✓ウィルスチェックができない
  パスワード付きのZipファイルに対してチェックが働かない可能性。
- ✓ZIPパスワードの脆弱性
  ファイルの暗号は何度でも入力可能なため、突破できる可能性。

サプライチェーン攻撃とは…

組織間の業務上のつながりを悪用した「サプライチェーン攻撃」が注目されています。「中小企業は狙われない」というのは大きな間違いであり、そのような過信こそが危険です。大企業はセキュリティ対策に費やすコストや人員も多く、不正侵入が困難だと考える攻撃者は、セキュリティ対策が手薄な中小企業を狙って攻撃を仕掛けます。
最終ターゲットへの攻撃が成功してしまった場合、踏み台となった会社の経営規模を超えるような莫大な被害が生じる可能性も十分に考えられます。規模の大小に関わらず、セキュリティ対策の徹底が必要です。
侵入させないことが第一ですが、万が一侵入されてしまったとしても、ネットワークにおける挙動監視等、内部活動の迅速な可視化によって早期に対応できる体制を整備していきましょう。

●サプライチェーン攻撃の仕組み



＼ セキュリティレベルの向上のコツ ／

ワクチンソフトの統一と最新化

社内でワクチンソフトは利用しているものの、使用しているソフトやライセンスがバラバラ、といった状況はありませんか？これらを統一することでネットワーク全体としての管理が実現され、セキュリティ効果を高めることにつながります。また、OSのアップデートも重要です。ワクチンソフトは、新生のウイルスには効果が期待できず、その点で万能ではありませんが、最新版へのアップデートを常に行うことによって、効果を最大化することができます。

アクティブディレクトリの導入

アクティブディレクトリはMicrosoft社が提供するWindows Serverに設けられた機能です。Windows2000以降実装されており、標準搭載であるため、特別なソフトをダウンロードすることなくセキュリティレベルを底上げできます。部署や役職など、属性ごとの階層的な管理や一括での権限適用が可能であることからユーザーごと個別に権限設定を行う必要がありません。ソフトウェアの自動インストールや自動更新、ログ管理もアクティブディレクトリの重要な機能であると言えます。管理しなくてはならないIDやパスワードの数が減少したり、確実な更新が実行されるということは効果的なセキュリティ対策の1つです。

セキュリティ意識・知識のアップグレード

こんなシステムを使っているから安心、というのは過信です。いつでもどこでも攻撃を受ける可能性はあり、100%の安全は存在しません。常に脅威に晒されているという意識を持ち、万が一、攻撃を受けた場合の対応マニュアルを整備しておくことなども重要な対策です。また、外部からの攻撃だけでなく、不注意による情報漏えいといった内部的脅威も実は重大です。内外両方の脅威に備えるためにも、セキュリティポリシーの明確化、定期的なセキュリティ教育を行いましょう。また、インターネットに接続しないパソコンであってもUSBメモリ等を通して脅威を取り込んでしまう可能性があります。USBメモリの利用や管理についても注意を徹底する必要があります。
セキュリティの脅威が確実に高度化・多様化しています。ユーザー側もそれに応じて意識や知識のアップグレードをしていかなくてはなりません。最新情報をしっかりと入手し、適切な対応をとっていきましょう。

取扱情報の明確化

社内には個人情報や社員情報、顧客情報、技術情報など多種多様な情報が存在しています。これらを一定の基準に基づいてカテゴライズしましょう。そして万が一、情報漏えいが生じた場合に、どの情報に、どんな被害・損害がどれくらい発生するのか、ということについても予め明確化しておくことが重要です。先述の「5S活動」に取り組みましょう。

大切なデータを守るため、
セキュリティ水準を向上させましょう！
まるっと当社にご相談ください！

Daichi SYSTEM 株式会社 ダイチシステム
〒103-0005 東京都中央区日本橋久松町 12-4
TEL：03-5652-9855　FAX：03-5652-9856
E-mail：info@daichisystem.co.jp
URL https://www.daichisystem.co.jp