

第137回 維持管理研究会 議事録

- 開催日時：2022年12月15日(木) 16:00~17:40
- 場所：Zoomリモート開催
- 出席者(敬称略) 15名参加

小田、井上、上辻、大下、久保、熊澤、越田、坂本、澤田、菅谷、高橋、千葉、柳本、山下、中谷(記)

4. 研究テーマ

今月の研究会は、日本国内におけるサイバー攻撃が激増の一途をたどっており、多くの機密情報を有する大手企業や官公庁関連が攻撃ターゲットの中心でした。しかし最近ではサプライチェーンや中小企業及び医療機関も攻撃の標的になっているのが現状です。

なお今回は、IT専任者ではなくBCやリスク担当者が対応すべき内容を中心に説明しました。

講演資料(抜粋)

サイバー攻撃概要と対策

2022年12月15日

中谷 明男
DRIL 代表取締役
BCAO 幹事兼維持管理研究会会長
RRC 幹事

1. 自然災害との違い

情報漏洩時に発生するコストは、インシデント1件あたり平均億円にも上ることが明らかになっています。

項目	自然災害	サイバー攻撃
対象	不特定	標的型が多い
考慮する視点	従業員の安全確保	業務への影響度把握
被害状況の把握	気づき遅い	気づき難い
復旧開始時期	即時	原因究明後
原因調査部隊	不要	原因調査部隊が必要(原因究明)
法規制の対応	安全記義務、建築基準法など	個人情報保護法、GDPR(EU)

セキュリティ対策の推進・意思決定を行う際は、組織に与える影響を十分に踏まえたうえで、判断していることが重要です。

1-1. 情報セキュリティ脅威の変化

年	脅威	被害額	年	脅威	被害額
18	ランサムウェアによる被害	145	18	ランサムウェアによる被害	145
19	ランサムウェアによる被害	150	19	ランサムウェアによる被害	150
20	ランサムウェアによる被害	160	20	ランサムウェアによる被害	160
21	ランサムウェアによる被害	170	21	ランサムウェアによる被害	170
22	ランサムウェアによる被害	180	22	ランサムウェアによる被害	180

2. マルウェアの種類

マルウェアとは、『悪意のある』ソフトウェアの総称です。
「Malicious(悪意のある)」+「Software(ソフトウェア)」を組み合わせで作られた造語です。

マルウェア	ウイルス
ランサムウェア 情報の暗号化やデータを破壊し、システム稼働に支障を発生させる	ワーム 単独で存在可能で自己増殖する
スパイウェア 秘密にPCにインストールされ情報窃取を行う	トロイの木馬 悪意ある者が侵入し、外部からの命令で動作する
ファイルレスマルウェア メモリ上で動作する	バックドア セキュリティホールを悪用してトロイの木馬などと同様に侵入し、遠隔制御が可能

3. 主なサイバー攻撃

- 標的型メール攻撃(ビジネスメール詐欺)**
金銭や知的財産などの重要情報の不正取得を目的として、組織の従業員・職員をターゲットとして行われるメール等による攻撃です。
- フィッシング詐欺**
クレジットカードやネットバンクなどのサービスになりすまして、そこから偽サイトに誘導しログイン情報や個人情報を入手させることで情報の窃取を行う攻撃手法です。日常生活を行う中で、最も身近で被害を感じるサイバー攻撃である。
- ゼロデイ攻撃(ソフトウェアの脆弱性)**
システムセキュリティに関する脆弱性が発見されてから修正プログラムや対応パッチが適用されるまでの期間に不正に侵入するサイバー攻撃です。
- DoS攻撃/DDoS攻撃**
特定のソフトウェアやサーバに対して、過剰な負荷をかけた脆弱性を突くことでサービスの正常な動作を妨げ、サービス停止状態へと追い込む攻撃です。
- SQLインジェクション**
ブラウザからWebアプリケーションに不正なSQL文を入力することで動作不良を起させ、DBを不正に操作したり、機密情報等を取り出す攻撃です。

4. ネットワークセキュリティ

インターネット、クラウド、VPN、LAN、WAN、モバイルネットワーク

セキュリティ対策の重要性を強調し、各ネットワーク環境での対策を説明する。

5. セキュリティ対策の見直し

既存の境界型セキュリティは「不審」ではなく、「内部は安全」という、今までのセキュリティポリシーから個々のアクセスを評価するポリシー「ゼロトラスト」に向かっていることが重要である。

ゼロトラストの現状調査(参考)

https://www.sipg.jp/secure/research/2022/06/30/3rdRefrSecRpt-5wR2k-2jPMyaXk0000j0000Pw0w0p011yWY1j0r3Q13y74k4RRE

5-1. セキュリティ対策の基本

情報セキュリティ対策を行う上では、最も基本となるルールが「情報セキュリティポリシー」であり、セキュリティレベルを確保するための基本です。

経営者は、テレワーク実施を考慮した情報セキュリティポリシーを定め定期的な監査し、改善を指示する。

管理者は、システム全体を管理する重要な立場であることを自覚し情報セキュリティポリシーに従って、テレワークセキュリティ対策に関する対策を講じると共に定期的に診断する。

従業員は、テレワーク作業中は、利用する情報資産の管理責任があることを自覚し、情報セキュリティポリシーが定める技術的・物理的、及び人的対策の基準に準じて業務を行い、定期的に実施状況を自己点検する。

5-2. 基本的なセキュリティ対策

- 基本的な対応**
 - 定期的なPWの変更、及びウイルス対策ソフトの定期的な更新(毎日更新機能があるOS・API・ウイルスソフトの最新状態を確認)
 - メールの添付ファイル開封やURLには安易にアクセスしない
 - 会社PCでは、フリーWiFiの使用禁止
- 会社PCの使用制限**
 - 会社PCでは、インターネット接続先の制限(ホワイトリスト)
 - 会社PCのHDD(SSD)に重要データ保存を禁止
 - 社内システムには登録PC以外には、ログイン不可
- パスワードやデータの保存**
 - パスワードは他人に推測されにくい複雑なものにする
 - また、PCやスマートフォンには必ずID管理
 - 認証の強化(多要素認証によるID管理)
 - 重要データのバックアップ強化(3-2-1法則)
- 従業員への継続的教育**
 - 基本的な注意事項(盗難・セキュリティ保護)の継続教育
 - 疑わしいメールを定期的に送信し、注意喚起と指導徹底

5-3. 発想の転換が必要

「何威を入れない」対策から「被害を防ぐ」対策へ

100%検出は不可能

EDR(Endpoint Detection and Response)

XDR(Extended Detection and Response)

5-5. インシデント発生時の対応

検知、初動対応、分析調査、通知情報開示、再発防止

一時対応者へ上司・責任者への連絡

ネットワークから遮断、システムの停止

ログ情報や状況の保全・復旧措置

影響範囲の特定、社内(関係者)周知

原因究明、二次被害の防止

被害者へ通知、問合せ対応

監督官庁へ届出・広報(情報開示)

復旧・回復(オフラインバックアップ必須)

再発防止策

事業再開、継続監視

6. 継続的な改善

運用監視・予防検知

設計・防御

訓練・評価・検証

インシデント対応・復旧

継続的な対策や見直しが大変重要である。

5. 意見交換（感想など）

- 自社の重要な課題となっており、大変参考になりました。今後の活動に役立てたい。
- 最近、経営層を中心にハッカーから金銭要求が発生したことを想定に訓練を実施した。
僅々の課題でもあり、熱心に対応方針について議論して頂いたので、今回の資料も含めて参考に今後の対応方針や改善案を検討していきたい。
- BCP 検討メンバーは、総務・人事・リスク部門であったので、IT 部門も検討メンバーに参加させて検討を行っており、全社 B C P の継続戦略や RTO と同期した I T 戦略の検討を開始した。
- I T 部門への確認を継続的に実施する必要性を強く感じました。

<次回予定>

・2023年 1月 19日（木）16:00～17:30

以上