

第115回 維持管理研究会 議事録

1. 開催日時：2021年2月18日(木) 16:00~18:00

2. 場所：Zoomリモート開催

3. 出席者(敬称略) 19名

相原、石綿、井上、葛西、木村、久保、澤田、清水、守護、菅谷、守護、高杉、高橋、藤井、

柳本、柳谷、山下、中谷(記)

ゲスト参加：長谷川(古村代理)

4. 研究テーマ

テレワーク勤務の方が多くなか、世界的にサイバー攻撃が多発しておりますので、今月は全社BC担当者とIT部門の専門家が、BC観点から捉えたセキュリティ対策が検討できることを目標とした。

サイバー攻撃の種類やマルウェアに関する防御策の基本的なことについて、現状の対応状況や今後とすべき対応策や課題などについて、参加者で意見交換を行った。

なお、詳細のセキュリティ対策はIT専門家に任せて、維持管理研究会では全社BC担当者として最低限理解しておくべきことにターゲットを絞り込んで、BCPとして必要なことについて話し合った。

① 現状のセキュリティ対策について

テレワーク勤務の環境下における各社のPC取り扱いや基本的なセキュリティの知識など、各社の対応状況について意見交換を行った。

<h3>1. 情報漏洩が組織に与える影響</h3> <table border="1"> <thead> <tr> <th>影響</th> <th>内容</th> </tr> </thead> <tbody> <tr> <td>損害賠償</td> <td>情報漏えいによって損害が生じた人、組織への損害賠償費用</td> </tr> <tr> <td>対応費用</td> <td>原因調査・再発防止策にかかる費用、謝罪広告などによる広報費用</td> </tr> <tr> <td>機会損失</td> <td>サービス中断、社会的信用失墜による売上低下、取引中止</td> </tr> <tr> <td>法的制裁</td> <td>各国の法令(個人情報保護法、GDPR等)による罰金、入札停止</td> </tr> </tbody> </table> <p>情報漏えい時に発生するコストはインシデント1件あたり平均4億円にもなることが明らかになっています。そのうち、顧客の個人情報漏えいした事例では、発生するコストが最も高い調査結果となっています。</p> <p>セキュリティ対策を推進し意思決定を行う際には、組織に与える影響を踏まえた上で判断していくことが重要です。</p>	影響	内容	損害賠償	情報漏えいによって損害が生じた人、組織への損害賠償費用	対応費用	原因調査・再発防止策にかかる費用、謝罪広告などによる広報費用	機会損失	サービス中断、社会的信用失墜による売上低下、取引中止	法的制裁	各国の法令(個人情報保護法、GDPR等)による罰金、入札停止	<h3>《事例》 自然災害とサイバー攻撃との違い</h3> <table border="1"> <thead> <tr> <th></th> <th>災害 バンデミック</th> <th>サイバー攻撃</th> </tr> </thead> <tbody> <tr> <td>● 標的企業・団体</td> <td>不特定である</td> <td>標的型が多い</td> </tr> <tr> <td>● 考慮する視点</td> <td>被害者視点</td> <td>被害者・加害者視点</td> </tr> <tr> <td>● リスク低減対策</td> <td>リスク低減が困難</td> <td>リスク低減が可能</td> </tr> <tr> <td>● 被害状況把握</td> <td>気づきやすい</td> <td>気づきにくい</td> </tr> <tr> <td>● 復旧開始タイミング</td> <td>即時</td> <td>原因究明後</td> </tr> <tr> <td>● 体制の違い</td> <td>原因調査部隊不備</td> <td>原因調査部隊必要</td> </tr> <tr> <td>● 法規制への対応</td> <td>建築基準法/安全衛生法</td> <td>個人情報保護法/GDPR</td> </tr> </tbody> </table> <p>情報漏洩した個人情報やパスワード等のアカウント情報は、標的型フィッシング攻撃やパスワードリスト型攻撃にも悪用される恐れがあり、それによる二次被害の損害賠償が組織に対して求められるおそれもあると考えられます。</p>		災害 バンデミック	サイバー攻撃	● 標的企業・団体	不特定である	標的型が多い	● 考慮する視点	被害者視点	被害者・加害者視点	● リスク低減対策	リスク低減が困難	リスク低減が可能	● 被害状況把握	気づきやすい	気づきにくい	● 復旧開始タイミング	即時	原因究明後	● 体制の違い	原因調査部隊不備	原因調査部隊必要	● 法規制への対応	建築基準法/安全衛生法	個人情報保護法/GDPR	<h3>2. セキュリティ対策に関する質問</h3> <p>テレワーク勤務用のPCは？</p> <ul style="list-style-type: none"> <input type="checkbox"/>在宅時には会社PCを持ち帰って業務をしているか <input type="checkbox"/>会社用と自宅用の2台のPCを準備しているか <input type="checkbox"/>個人のPCを使用して、社内業務は可能であるか <p>会社PCの使用制限をかけているか？</p> <ul style="list-style-type: none"> <input type="checkbox"/>会社PCは、社内業務以外に使用制限をかけているか(ショッピング等の閲覧・購入禁止、APLダウンロード不可など) <input type="checkbox"/>特に制限をかけていないが、個人使用しないように注意喚起しているか <p>基本的なセキュリティ対策は？</p> <ul style="list-style-type: none"> <input type="checkbox"/>定期的なPWの更新、及びウイルスソフトの更新を指示しているか <input type="checkbox"/>会社PCでフリーWiFi(スポット)の使用を禁止しているか <input type="checkbox"/>自宅からの接続先(会社/DC)までの通信経路は暗号化しているか <p>情報セキュリティの継続的教育は？</p> <ul style="list-style-type: none"> <input type="checkbox"/>基本的な注意事項(盗難・セキュリティ保護)の教育を実施しているか <input type="checkbox"/>疑似メールを定期的に送付し、注意喚起や指導を実施しているか
影響	内容																																			
損害賠償	情報漏えいによって損害が生じた人、組織への損害賠償費用																																			
対応費用	原因調査・再発防止策にかかる費用、謝罪広告などによる広報費用																																			
機会損失	サービス中断、社会的信用失墜による売上低下、取引中止																																			
法的制裁	各国の法令(個人情報保護法、GDPR等)による罰金、入札停止																																			
	災害 バンデミック	サイバー攻撃																																		
● 標的企業・団体	不特定である	標的型が多い																																		
● 考慮する視点	被害者視点	被害者・加害者視点																																		
● リスク低減対策	リスク低減が困難	リスク低減が可能																																		
● 被害状況把握	気づきやすい	気づきにくい																																		
● 復旧開始タイミング	即時	原因究明後																																		
● 体制の違い	原因調査部隊不備	原因調査部隊必要																																		
● 法規制への対応	建築基準法/安全衛生法	個人情報保護法/GDPR																																		

② テレワークにおける脅威とサイバー攻撃について

現状のテレワークにおける脅威やサイバー攻撃の脆弱性について解説を行った。マルウェアとウイルスを混同している方が多くみられたが、明確に違いを理解することができた。

<h3>3. テレワークにおける脅威と脆弱性</h3> <p>脅威</p> <ul style="list-style-type: none"> マルウェア(ウイルス・ワーム) 通信経路 社内システム <p>脆弱性</p> <ul style="list-style-type: none"> マルウェア(ウイルス・ワーム) <ul style="list-style-type: none"> ウイルス対策ソフトの未導入、更新不備 ランサムウェアの未実施 メールの添付ファイルのダウンロード メールに添付されたファイルの開封や実行 リンクのクリック 端末の紛失・盗難 <ul style="list-style-type: none"> 端末の紛失に備えたバックアップの未実施 バックアップの未実施 重要情報の盗難 <ul style="list-style-type: none"> 無線LANの設定不備 後アクセスポイントへの接続 無線LANの盗聴 暗号化せずに送信 盗難による内部不正 不正アクセス <ul style="list-style-type: none"> ファイアウォールなし 脆弱なサービス 脆弱なパスワード 脆弱な設定 脆弱なログ 脆弱なログ 脆弱なログ <p>事故</p> <ul style="list-style-type: none"> 情報漏えい(機密性の喪失) 重要情報の盗失(完全性の喪失) 作業中断(可用性の喪失) 	<h3>4. サイバー攻撃の種類</h3> <ol style="list-style-type: none"> マルウェア 情報窃取などを目的に不正に動作させる悪意あるプログラムの総称です 標的型攻撃 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、組織内の特定の構成員に対して行われる攻撃です ゼロデイ攻撃 システムセキュリティにおけ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実行されるサイバー攻撃です DoS攻撃/DDoS攻撃 特定のネットワークやサーバーに対して、過剰な負荷をかけて脆弱性をつくことでサービス正常な動作を妨害し、サービス停止状態へと追い込むサイバー攻撃です SQLインジェクション ブラウザを介してWebアプリケーションに不正なSQL文を入力することで、動作不良を起こさせデータベースを不正に操作したり個人情報や機密情報を採取する攻撃です バッファオーバーフロー攻撃 パスワードリスト攻撃 セッションハイジャック など 	<h3>5. マルウェアについて</h3> <p>マルウェアとは、『悪意のあるソフトウェアのこと。』 「Malicious」(悪意のある) + 「Software」(ソフトウェア)を組み合わせて作られた造語です。</p> <p>ウイルス 既存プログラムに侵入し一部を改変して自己増殖する</p> <p>ワーム 単独で存在可能で自己増殖する(LoveLetter, CodeRed, Mydoom)</p> <p>トロイの木馬 画面・文書から導入し外部からの命令で自由に振る</p> <p>ランサムウェア 画面・文書等を暗号化し復元に金銭を要求する</p> <p>バックドア セキュリティホールを使ったトロイの木馬をインストールし、設計・開発段階で組み込まれている</p> <p>ボット 別のコンピュータに感染し命令を実行する</p> <p>スパイウェア 盗み取ったデータを外部に送信する</p> <p>主なマルウェア</p>
--	---	--

③ 利用形態とセキュリティ対策

今後は、ゼロトラストセキュリティ（ネットワークを含めた全てのトラフィックを信頼しない）を前提とし、検査やログ取得を徹底し、さまざまなフェーズにおいてセキュリティ対策を実施することが重要である、また P C からの情報漏洩を防ぐ手段として、P C 側にデータを持たせないシンクライアント（VDI など）方式のシステム構築を考えて行くことも検討する必要がある。

6. 個々の利用把握とセキュリティ対策

※内部もしっかりとセキュリティで守れるように、ゼロトラストセキュリティを志向する。

セキュリティセグメント=ネットワークセグメント
機件で認証と許可

セキュリティセグメント=ネットワークセグメント
全ての事業で常に認証と許可

相互に補充しあう関係

注意！
既存の境界型セキュリティは「不要」ではなく、「内訳は安全」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」に向かっていくことが重要なことである。

7. ITのセキュリティ対策

※ゼロトラストセキュリティを志向して、セキュリティの仕組みを検討すること。

《参考》ネットワーク端末の構成例

最近、端末側にシステムやデータを持たないシンクライアント方式が多く利用され始めている。

なお、サイバー攻撃の防御には限界があり、完璧な防御はあり得ないことを前提とした考え方が必要である。すなわち「脅威を入れない対策から実害を防ぐ対策」を「**全社 BC 担当者**」と「**IT 専門化**」が共同で推進することが重要となってきている。

8. 防御策の考え方

- ◆ 防御の強化
- ◆ 侵入の早期検知
- ◆ 迅速な隔離・復旧

【見える化】
・資産管理
・構成管理
・変更管理

【セキュリティ】
・脅威の検知と緩和
・脆弱性の管理
・フォレンジック
(分析・調査)

①システムの個別評価

- ベネレーションテスト (類似攻撃)
- 詳細なリスク分析
- ベースラインアプローチ (セキュリティレベルの到達度調査)

②組織の評価

- 危機対応の体制強化、人材育成
- セキュリティの意識
- サイバー攻撃の対応や復旧計画策定

※セキュリティ対策には、一長一短があり、完全な対策は不可能である。

9. 発想の転換が必要

「脅威を入れない」対策 → 「実害を防ぐ」対策へ

侵入されることを前提にした対応を行う。

<次回開催予定>

2021年 3月18日 (木) 16:00~18:00

Zoom によるリモートで実施

以上