RESOURCES

KnowBe4

Ransomware Attack Response Checklist
ランサムウェア攻撃に対応するためのチェックリスト

ステップ1: 初動調査

- [ ] a. ランサムウェア攻撃なのかを判定する。
- [ ] b. 1デバイス以上が攻撃されたのかを判定し、重大度を確定する。

ランサムウェア攻撃と判定した場合は、ステップ2へ。

ステップ2:ランサムウェア攻撃発生の宣言・インシデント対応の開始

- [ ] a. ランサムウェア攻撃の発生を速やかに表明する(ランサムウェア攻撃の発生を隠蔽しない)。
- [ ] b. サイバー攻撃が発生した場合に従うルールに従って、セキュリティ担当者はあらかじめ設定された代替のコミュニケーション手段を利用することを開始する。
- [ ] c. ランサムウェアインシデントを全セキュリティ担当者へ一斉に連絡し、同時に全部門長および財務部門・法務部門へ重大度とともに情報共有する。

ステップ3:ネットワークスの遮断

- [ ] a. まずは、感染デバイスを即座にネットワークスから遮断し、ネットワーク接続機能を無効化する。
- [ ] b. 感染によってデータを暗号化するワイパー型のマルウェアが疑われる場合、またはデータの暗号化を予見できる場合は、ネットワーク接続を切断して、即座にデバイスをシャットダウンする。

ステップ4:感染範囲の判定

インフラがどの程度侵害されているか、何が暗号化/破損されているか、データおよび/または認証情報が流出していないかどうかを正確に判定する。さらに、通常とは異なる、あるいは説明のつかない新しいプロセス、サービス、デーモンがないかを調査する。また、感染されたデバイスまたは対象に次のコンポーネントが含まれていないかもチェックする。

- [ ] a. 共有デバイス
- [ ] b. クラウドベースのストレージ: DropBox、Googleドライブ、OneDriveなど
- [ ] c. ネットワークストレージデバイス
- [ ] d. 外部ハードデバイス
- [ ] e. USBストレージデバイス (USBメモリー、メモリースティック、接続スマホ／カメラ)
- [ ] f. 他のコンピューターの共有フォルダー

個人情報やログイン認証情報が盗難にあっていないかを特定する

- [ ] a. ログ情報およびDLP(Data Loss Prevention)ソフトをチェックして、データ漏洩が発生していないかを確認する。
- [ ] b. データをコピーするためにステージングファイルとして使用された可能性のある機密データを含む予期せぬ大きなアーカイブファイル(zip、arcなど)がないか確認する。
- [ ] c. データの検索やコピーに使用された可能性のあるマルウェア、ツール、スクリプトがないかを見付ける。
- [ ] d. もちろん、ランサムウェアによるデータ盗難の最も正確な兆候の1つは、個人データや認証情報を盗み出したことを告げるランサムウェアの一団からの通知。

RESOURCES

ランサムウェアの感染経路を特定する

- [ ] a. ランサムウェアの感染経路／タイプは何か？　例えば、Ryuk、Dharma、SamSamなど

ステップ5：被害の極小化

- [ ] a. 検出された被害を初動調査で特定して、止める。または、最小限にとどめて被害を可能な限り軽減する。

ステップ6：セキュリティチーム・関係者を召集、現状を情報共有

- [ ] a. ここでの目的は被害の範囲や程度など、すべての情報をセキュリティ担当者および関係者間で共有し、正しく理解してもらうこと。

ステップ7：対応策の決定

- [ ] a. 身代金を支払う、または支払わないか？
- [ ] b. 修復または再構築？
- [ ] c. フォレンジック調査や被害システムの復旧などを支援してくれる外部のセキュリティスペシャリストを依頼するか？
- [ ] d. 必要に応じて、法的機関、弁護士、保険会社、関係政府機関へ連絡して、被害の状況を連絡する。さらに警察本部のサイバー犯罪相談窓口へ被害を申し立てる。

ステップ8：原状回復

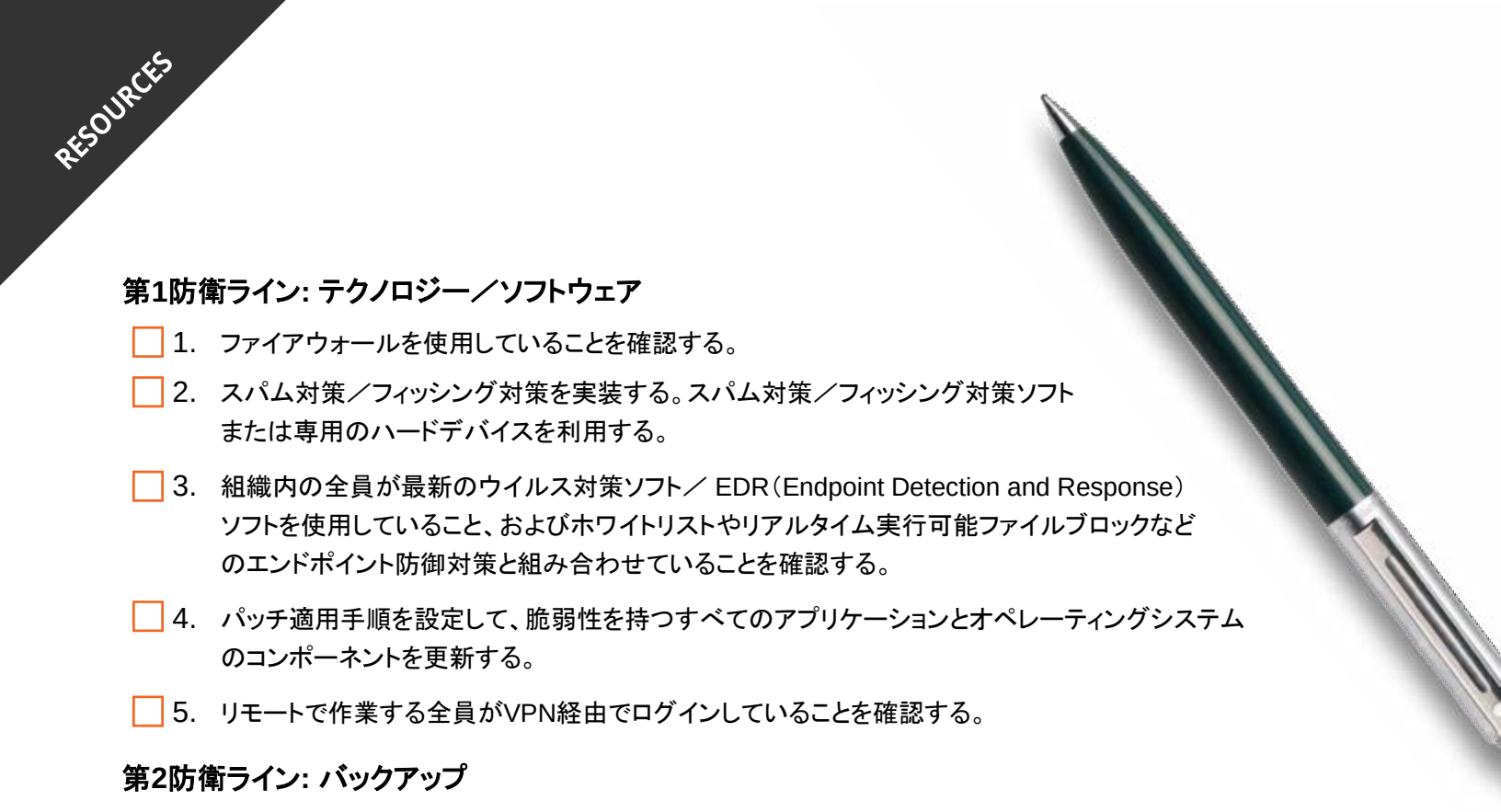
- [ ] a. 修復のみ、または再構築？
- [ ] b. 証拠保全が必要ですか？
- [ ] c. ビジネスインパクト分析により、どのデバイスやシステムを復旧させるか、また、いつ実施するかを決定する。
- [ ] d. まずは、基幹インフラ／基幹システムの原状回復を実施する。

ステップ9：予防措置

ランサムウェア攻撃などのサイバー攻撃は、繰り返さえる。次のサイバー攻撃に備えて、予防措置を講じる。

- [ ] a. セキュリティ意識向上トレーニング／フィッシング攻撃演習など、ソーシャルエンジニアリング攻撃対策を実行する。
- [ ] b. 更新プログラムを欠かさずインストールする。
- [ ] c. 可能な限り、多要素認証（MFA）を実装する。
- [ ] d. アプリケーション毎に強力な異なるパスワードを設定する。
- [ ] e. ウイルス対策ソフト／ EDR（Endpoint Detection & Response）ソフトを利用する。
- [ ] f. スパム対策／フィッシング対策ソフトを利用する。
- [ ] g. DLP（Data Loss Prevention）ソフトを利用する。
- [ ] h. 定期的にバックアップを取り、テストする。

RESOURCES



第1防衛ライン: テクノロジー／ソフトウェア

- ☐ 1. ファイアウォールを使用していることを確認する。
- ☐ 2. スパム対策／フィッシング対策を実装する。スパム対策／フィッシング対策ソフトまたは専用のハードデバイスを利用する。
- ☐ 3. 組織内の全員が最新のウイルス対策ソフト／ EDR（Endpoint Detection and Response）ソフトを使用していること、およびホワイトリストやリアルタイム実行可能ファイルブロックなどのエンドポイント防御対策と組み合わせていることを確認する。
- ☐ 4. パッチ適用手順を設定して、脆弱性を持つすべてのアプリケーションとオペレーティングシステムのコンポーネントを更新する。
- ☐ 5. リモートで作業する全員がVPN経由でログインしていることを確認する。

第2防衛ライン: バックアップ

- ☐ 1. バックアップソリューションを実装する - ソフトウェアベース、ハードウェアベース、またはその両方。
- ☐ 2. モバイル/USBストレージを含む、アクセス・保存が必要なすべてのデータがバックアップされていることを確認する。
- ☐ 3. バックアップによる冗長化によって、データの機密性・完全性 ・可用性が確保されていることを確認する。
- ☐ 4. バックアップ/リストア手順のリカバリー機能を定期的にテストする。物理バックアップのデータ完全性とオンライン/ソフトウェアベースバックアップのデータリカバリーの容易性を、少なくとも過去3～4ヶ月間テストする。サイバー攻撃者は、数ヶ月間ネットワークに潜伏して、バックアップに違法アクセスすることがある。

第3防衛ライン：個人情報データ／ログイン認証情報盗難対策

- ☐ 1. DLP（Data Loss Prevention）ツールを利用する。
- ☐ 2. ファイル・フォルダー・データベースへのアクセス権限を限定する。
- ☐ 3. システムログを有効化して、データの移動をトラッキングする。
- ☐ 4. ネットワークトラフィック分析により、コンピューターやネットワーク上での異常なデータ移動を監視する。
- ☐ 5. データを暗号化し、不正コピーを防止する。

第4防衛ライン：「人」による防御 - ヒューマンファイアウォール

- ☐ 1 新しいスタイルのセキュリティ意識向上トレーニングを実施して、マルウェアなど悪意あるアプリのダウンロードや実行を防ぐために何を注意すべきかをユーザーに教育する。
- ☐ 2 5%～10%の悪意あるメールがメールフィルターをすり抜けている。セキュリティ意識向上トレーニングと並行して、少なくとも毎月1回、フィッシング攻撃演習を実践する。