取締役会レベルのガイド：サイバーセキュリティにおけるリーダーシップ

監督

組織の指導部の最高レベルに当たる取締役会は、サイバーリスクガバナンスに関する究極の説明責任を負うため、この分野における組織の戦略、方針、そして活動を監督する必要がある。取締役会は、特に以下を実施すること：

- 完全な取締役会または特定の取締役会委員会への監督機能の委任を通じて、サイバーリスクおよびレジリエンスに関する究極の責任を負う。
- 組織のサイバーレジリエンス管理能力およびサイバーレジリエンス目標の実装の進捗状況について報告する責任を1人の執行役員に任命する。通常、これには最高情報セキュリティ責任者（CISO）が指名される。この執行役員には、取締役会への定期的なアクセス、十分な権限、主題に関する運用能力、経験、そして当該任務の遂行に必要なリソースが備わっていることを確認する。
- 毎年、組織のリスク許容度を定義して、それが企業戦略とリスク選好度に合致していることを確認する。
- 貴組織のサイバーレジリエンスに関する正式な独立審査が毎年必ず実施されていることを確認する。
- サイバーレジリエンス計画の作成、実装、テスト、そして継続的改善を監督し、組織全体にわたって連携させ、CISO またはアカウンタビリティのあるその他の役員が取締役会に定期的に報告するよう万全を期する。
- 総合的な運用上のリスクにサイバーリスクを完全に統合することを目標に掲げ、組織の総合的な事業戦略、リスク管理、予算編成、そしてリソース配分にサイバーレジリエンスとリスクアセスメントを統合する。第三者リスクを定期的に審査する。
- 上記に関するパフォーマンスを定期的に審査し、継続的な改善を実現できるよう独立した助言を得ることを検討する。

最新情報の入手

取締役会がサイバーリスクを効果的に監督できるかどうかは、主題に関する役員の能力、そして最新情報にかかっている。

- 取締役会に加わる全ての個人が適切かつ最新のスキルと知識を有しており、サイバー脅威が呈するリスクを把握および管理できるよう万全を期する。
- 貴組織の現在および将来的なリスクの露出、関連の規制要件、そしてリスク選好度に関する業界および社会のベンチマークについて、組織の経営陣より定期的な助言を求める。更に、脅威ランドスケープおよび規制環境に関する最新の進展の定期ブリーフィング、サイバーセキュリティにおけるベストプラクティスを実践している同僚およびリーダーとの共同計画および訪問、またガバナンスとレポートに関する取締役会レベルの意見交換に従事する。
- 経営陣には、取締役会議中の常設の議案としてのサイバーリスク、脅威、およびイベントについて、定量化された分かりやすい報告を行う責任を課す。
- サプライチェーンの脆弱性、共通の依存関係、そして情報共有におけるギャップなど、進行中の体系的な課題に関連した進展について経営陣およびその他の関連職員と定期的に確認する。

基調の打ち出し

取締役会は上級管理職と共に、組織のコアバリュー、リスク文化、そしてサイバーレジリエンスに関する期待を設定し、模範となる必要がある。

- あらゆる職位の職員が、各自の重要な責任を認識して、組織のサイバーレジリエンスを確保する組織文化を推進する。模範を示すこと。
- 貴組織のリスク文化の醸成および維持における経営陣の役割を監督する。リスク文化が安全性および健全性に及ぼす影響を考慮した上でその推進、監視、そして評価を行い、必要に応じて変更する。
- 全ての従業員が誠実に行動し、貴組織内外で観察したコンプライアンス違反を速やかにエスカレーションすることを求めている点を明確に伝える。

サイバーリスクガバナンスの基本

以下の質問群に「はい」と回答できることを確認すること：

1. 貴組織は、**関連の法定および規制要件を満たしていますか?**
2. 貴組織は、**サイバーエクスポージャーを定量化して、その財政的レジリエンスをテストしましたか？**
3. 貴組織は、サイバーエクスポージャーが合意済みのリスク選好度内に収まるよう、**改善策**を配備していますか？
4. 取締役会は、経営陣が提供する組織のサイバーレジリエンスに関して簡潔、明晰、かつ実用的な情報の定期的な協議を行っていますか？
5. 貴組織が配備しているインシデントレスポンス計画では、取締役会レベルを含めて最近予行演習を行いましたか？
6. サイバーリスク管理を担当する主要人物の役割は明確であり、3つの防衛線と連携していますか？
7. 貴組織のサイバーリスクポスチャに対する独立検証および保証を取得しましたか？

CEO レベル向けガイド：サイバーセキュリティにおけるリーダーシップ

ガバナンス

貴組織のサイバーセキュリティは、トップマネジメントに始まり、トップマネジメントに終わります。CEO と取締役会はリスクに対する理解を維持し、組織のサイバーセキュリティ活動および職員に関する究極のアカウンタビリティおよび責任を引き受ける必要があります。以下を実施してください：

- 最高情報セキュリティ責任者（CISO）が存在しない場合は、当該責任者を任命する。また、リソースが限定されている場合は、CISO の機能を果たす人物を組織内で任命する。
- CISO またはその他の技術職員との協力の下、国際的、全国的、また業界の基準およびガイドラインを用いて、組織の具体的なサイバーリスクに合わせてカスタマイズされたサイバーセキュリティ戦略およびフレームワークを確立して維持する。
- 組織のサイバーセキュリティの実装および管理を担当する従業員の役割と責任を明確に示す。
  - CISO との協力の下、全ての職位の職員を対象に適正なサイバーセキュリティの役割とアクセス権を特定する。
  - コミュニケーションとコラボレーションを監督し、全体論的なサイバーセキュリティ管理が行われるよう万全を期する。これは特に、サイバーセキュリティに関する責任が組織内の複数の従業員または部署によって共有されている場合に当てはまる（情報セキュリティ、リスク、そしてテクノロジーなどの異種の垂直関係など）。
- CISO には、ご自分と取締役会に対して適宜脅威について伝えることの可能な、明確な直通のコミュニケーションラインが設けられていることを確認する。
- 上級管理職へのブリーフィングを行えるよう、CISO またはその他の技術職員を定期的に招待する。
- 組織のセキュリティポリシー、基準、施行メカニズム、そして手順が全てのチームおよびラインオブビジネスを跨いで統一されていることを確認する。

リスクアセスメントおよび管理

強固なサイバーセキュリティアウェアネスおよびレディネスは、継続的なリスクベース分析によって左右されます。貴組織のサイバーセキュリティを改善するには、以下を実施してください：

- 貴組織の広範なリスク管理およびガバナンスプロセスにおいて、サイバーセキュリティリスクアセスメントおよび管理を確立する。CISO またはその他の技術職員との協力の下、以下を伴うリスクアセスメントの実施計画を立てる：
  - 組織のアセットおよびそれぞれのテクノロジー依存の度合いの解説
  - 組織の成熟度、またアセットのテクノロジー依存度に関連した固有のリスクのアセスメント
  - 組織が希望する成熟度の判断
  - 組織のリスク優先度リストにおけるサイバーセキュリティ脅威の位置づけ
  - サイバーセキュリティの現状と目標とする状態のギャップの特定
  - 成熟度の達成および維持に向けた計画の実装
  - セキュリティへの投資資金の評価および割当て、ならびに既存のギャップへの対処
  - 組織のサイバーセキュリティの成熟度、リスク、目標の継続的な再評価
  - 第三者ペネトレーションテストまたはレッドチームの利用を検討する。
  - サイバー保険の購入といった安全対策の検討
- リスクアセスメントプロセスにおいて従業員の取り組みを主導し、組織全体の時宜を得たレスポンスを促進する。
- 主要ステークホルダーおよび取締役会を含めた経営陣による監督を目的に、リスクアセスメントの結果を分析および提示する。
- 組織において望ましいサイバーセキュリティレディネスを維持または増大させるため、あらゆる変更点を監督する。これには、適切な予算編成の下でサイバーセキュリティの向上を目的に、無理のない、組織のリスクに比例した行動を取ることが含まれる。
- 継続的な監視のパフォーマンスを監督して、進化し続けるサイバーリスクに機敏かつ敏捷に対処する。

組織文化

貴組織のサイバーセキュリティは、一度きりのプロセスでなければ、数人の従業員の仕事でもありません。つまり、あらゆるビジネス上の判断において考慮すべき要因であると共に、全ての従業員が固守するべき慣行なのです。組織内で継続的かつ全体論的なサイバーセキュリティを奨励するには、以下を実施してください：

- リーダーシップチームとサイバーセキュリティに関する協議を始め、サイバーリスク管理を担当する職員と定期的に連絡を取る。
- サイバーセキュリティトレーニングを全ての従業員オンボーディングの一部にして、全員が貴組織のサイバーセキュリティポリシーの最新情報を把握し、これへの遵守に合意した文書に署名すると共に、IT部署またはその他の技術職員はベストプラクティスに関するブリーフィングを受けるよう万全を期する。
- 全ての職員の長期および短期的なセキュリティ面での責任に関して、繰り返し行われるサイバーセキュリティトレーニングを設定する。
- 貴組織が潜在的なベンダーを評価し、第三者とデータを共有する際は、必ずサイバーセキュリティを考慮するよう万全を期する。
- 合併および買収を検討する際は、組織のサイバーセキュリティアセスメントを組込む。
- 毎年、貴組織のサイバーセキュリティポリシーを見直す。
- 組織内および信頼できる取引先において、サイバーセキュリティの脅威およびインシデントに関する自発的な情報共有を推奨する。
- 最初からセキュリティ上の懸念および計画を組み入れたイノベーションを生み出す。

CISO レベル向けガイド：組織を守る

マルウェアによる被害の防止

- ファイアウォールを起動してアクセス制御リスト（ACL）を設定し、ネットワークとインターネット間の緩衝地帯を構築する。特定のIPアドレスまたはサービスをブラックリストに登録するのではなく、ホワイトリスト設定を利用してアクセスを制限する。
- 全てのコンピューターおよびノートパソコンにおいて、アンチウイルスソフトウェアおよびアンチスパイウェアを利用する。分散型ワークフォースを保護するため、セキュリティツールが「在宅勤務」環境においても必ず効率的に運用できるようにする。
- メーカーとベンダーが提供した最新のソフトウェアアップデートを速やかに適用して、全てのソフトウェアおよびファームウェアのパッチを適用する。可能な限り「自動的にアップデート」を利用する。
- 新しいプログラムのインストールは管理者権限を持ったIT職員に制限する。
- 保護／検出ハードウェアまたはソフトウェアによって生成されたアクティビティログを保守・監視する。パスワード保護と暗号化によってログを保護する。
- 全てのホストの内部クロックを同期させる。貴組織のデバイスのクロックの設定に一貫性がない場合、イベント発生時のイベント相関はより困難になる。
- SD カードおよび USB スティックなどのリムーバブルメディアに対するアクセスを制御する。職員には、代わりにメールまたはクラウドストレージ経由でのファイル転送を推奨する。外部ソースを利用するか、自分の USB を他者に引き渡すことのリスクについて職員を指導する。
- 自身のメールサービスにおいて、メールセキュリティとスパムフィルタをセットアップする。
- 顧客対応 Web サイト上の全てのページを暗号化およびその他に利用可能なツールで保護する。
- 組織のアセットおよびシステムのセキュリティを評価するため、ペネトレーションテストサービスの利用を検討する。

従業員の訓練

- 新入社員にはオンボーディングの際に、また既存社員は最低でも年に一度定期的な間隔を空けて、必須のサイバーセキュリティトレーニングを実施する。従業員には以下を義務付けること：
  - 全ての業務デバイスおよびアカウントにおいて強力なパスワードを利用し、プライベートのデバイスでも同様の措置を取ってパスワードマネージャーの利用を奨励する。
  - 在宅勤務用のITインフラストラクチャーを含め、全てのデバイスをまたいだオペレーティングシステム、ソフトウェア、そしてアプリケーションを最新の状態に保つ。
  - 全てのアカウントで二要素認証を用いる。
  - アカウント情報とアクセスカードを安全に保ち、デバイスを離れる際はロックをかける。
  - アカウント情報またはその他の機密データを、暗号化されていないメールまたはその他のオープンな通信経由で共有することを控える。
  - 一方的に送られてきたか、疑わしいメールの添付物またはリンクを直ちに開かないようにする。
  - 個人情報を提供する前に、疑わしいメールまたはポップアップボックスの妥当性を検証して、メールアドレスに細心の注意を払う。
  - 潜在的な内外部のセキュリティインシデント、脅威、データもしくはデバイスの取扱いミスについて、技術職員および／または上級管理職に通報する。

リスクベースの情報セキュリティプログラムの策定

1. 貴組織が保管および利用する情報の種類を特定する

- 貴組織が保管および利用する、あらゆる種類の情報を特定・一覧化する（例：顧客の氏名およびメールアドレス）。

2. 情報の価値を定義する

- 各情報の種類に関して重要な質問をする：
  - この情報が公開された場合はどうなるだろうか？
  - この情報が不正確であった場合、私の事業はどうなるだろうか（例：データの整合性に不正操作があった場合）？
  - 私／顧客がこの情報にアクセスできなかった場合、私の事業はどうなるだろうか？

3. インベントリを開発する

- 特定した情報に触れるテクノロジーは何か記録する。これには、ハードウェア（例：コンピューター）およびソフトウェアアプリケーション（例：ブラウザメール）が含まれる。メーカー、モデル、シリアル番号、またその他の識別子も含める。各製品がどこにあるのか追跡する。ソフトウェアに関しては、そのソフトウェアがどのマシンに搭載されているのか特定する。迅速および／または広範な在宅勤務向けの展開において、こうしたインベントリがどのように変化および拡張するのか理解を構築する。
- 該当する場合は、貴組織の事業以外のテクノロジー（例：クラウド）ならびにファイアウォールなどの保護テクノロジーなどが含まれる。

4. 脅威と脆弱性を理解する

- 金融セクターが直面する脅威および脆弱性について定期的に審議し、貴組織が影響を受ける可能性を判断する。（この情報は、全国的なCERT、FS-ISAC、およびその他の地方自治体の団体より入手可能。）
- 最低でも月に1回、脆弱性のスキャンまたは分析を実施する。
- 企業全体のリスクアセスメントおよびアクセス制御の厳重管理を含む、内部脅威に対する保護計画を開発する。

5. サイバーセキュリティポリシーを作成する

- 貴組織の上級管理職との協力の下、上記リスクに合わせてカスタマイズされ、国際的、全国的、また業界の基準およびガイドラインに基づくサイバーセキュリティ戦略を構築・維持する。NIST フレームワーク、FFIE Cのサイバーセキュリティアセスメントツール、また ISO 27001 はこうしたポリシーの基盤となる。
- ポリシーの詳細について全ての従業員を訓練し、ポリシーを遵守して組織のサイバーセキュリティの継続的な維持に同意する書類への署名を要求する。この書類には、明白かつ周知の「在宅勤務」プロトコルを含めること。

- 偽アカウントからフィッシング形式のメールを送信するシミュレーションなどを通じて、従業員アウェアネスを定期的にテストする。正しく対処できなかった場合でも、懲罰ではなく学習の機会として利用する。

データの保護

- 重要なデータ（例：文書、メール、カレンダー）を定期的にバックアップして、復元可能であることをテストする。クラウドへのバックアップを検討する。
- バックアップを含んだデバイスが、オリジナルのデータを抱えたデバイスに物理的またはローカルネットワーク経由で永続的に接続していないことを確認する。
- サージプロテクターをインストールして発電機を使い、全てのコンピューターおよび重大なネットワークデバイスが無停電電源装置に差し込まれていることを確認する。
- モバイル端末管理（MDM）ソリューションを利用する。

デバイスを安全に保つ

- モバイルデバイスの PIN およびパスワード保護のスイッチをオンにする。デバイスが紛失するか盗難に遭った場合、追跡、遠隔ワイプ、または遠隔ロックが可能となるようデバイスを構成する。
- 可能な場合は「自動的にアップデート」オプションを利用して、デバイス（および全てのインストール済みアプリ）を最新状態に保つ。
- 機密データを送信する際は、公共の Wi-Fi ホットスポットに接続せず、セルラー接続（テザリングおよび Wi-Fi ドングルを含む）またはVPN接続を利用する。
- メーカーサポートが終了したデバイスは、最新の代替品と置き換える。
- 紛失したか盗難にあった機器の通報手順を設定する。

パスワードの利用

- 必ず、全てのコンピューターが、再起動後にパスワード入力を必要とする暗号化製品を利用すること。モバイル端末の PIN またはパスワード保護をオンにする。
- 強力なパスワードを利用すると共に、予測しやすいパスワード（例：passw0rd）や個人を特定可能な情報（家族またはペットの名前）を回避する。同じ対策を全ての従業員に求める。
- 可能な限り二要素認証（2FA）を利用する。
- 職員に配布する前に、ネットワークおよびIoTデバイスを含む、メーカー発行のデフォルトパスワードを全てのデバイスで変更する。
- 職員が容易に各自のパスワードをリセットできるように万全を期する。また、職員が定期的な間隔でパスワードを変更するよう義務付けることも可（例：四半期ごと、半年ごと、または毎年）。
- パスワードマネージャーの利用を検討する。パスワードマネージャーを利用する場合は、「マスター」パスワード（その他全てのパスワードへのアクセスを提供）が強力であることを確認する。

許可の制御

- 必ず、全ての従業員が一意的に識別可能なアカウントを持ち、貴組織のシステムにアクセスする度に認証されるよう万全を期する。
- 管理上の特権は信頼できるIT職員および主要職員のみに付与し、標準ユーザー向けワークステーションにおける管理者特権を破棄する。
- 従業員には職務に必要となる具体的なデータシステムへのアクセス権限のみを付与し、いかなるソフトウェアも許可なくインストールすることのないよう万全を期する。
- コンピューターへの物理的アクセスを制御し、各従業員向けユーザーアカウントを作成する。
- 在宅勤務している職員および管理者向けのアクセスオプションを明確に定義する。

WI-FI ネットワークおよびデバイスのセキュア化

- 職場の Wi-Fi がセキュアであり、WPA2 方式で暗号化されていることを確認する。一般的にルーターの暗号化はオフの状態で届くため、必ずこれをオンにする。ルーターへのアクセスをパスワード保護して、必ず事前設定されたデフォルトパスワードを更新する。あらゆる「遠隔管理」機能をオフにする。
- Wi–Fi ネットワークへのアクセスは、一定の MAC アドレスを備えたデバイスのみに制限する。顧客が Wi-Fi を必要とする場合は、別途の公衆ネットワークをセットアップする。
- ネットワークにアクセスした全てのデバイスを容易に追跡できるよう、ネットワークデバイスで DHCP（動的ホスト構成プロトコル）ロギングを有効にする。
- ルーターのセットアップ後、管理者としてログアウトする。
- ルーターのソフトウェアを最新状態に保つ。ルーターの登録をメーカーで行い、最新情報の取得にサインアップする。

フィッシング攻撃の回避

- 必ず、職員が管理者権限を持ったサーバーまたはアカウントから、Web のブラウジングやメール確認を行うことのないよう万全を期する。
- Web およびメールフィルタをセットアップする。一般的にサイバーセキュリティ脅威と関連付けられている Web サイトに従業員がアクセスする際は、これをブロックすることを検討する。
- 綴りや文法の明らかな誤りや、見覚えのあるロゴの低品質なバージョンなど、フィッシングの分かりやすい痕跡について従業員を指導する。送信元のメールアドレスは正当なアドレスに見えるだろうか？
- フィッシング攻撃を受けたことが疑われる場合は、できる限り早急にマルウェアスキャンを行い、パスワードを変更する。職員がフィッシング攻撃に遭ったとしても、懲罰を与えてはいけない（将来的に通報する気を削ぐことになるため）。

CISO レベル向けガイド：顧客を保護する

アカウントの管理

- 顧客が貴組織のサービスにログインする際は、強力なIDとパスワードを使用するよう義務付ける。他のアカウントと同じパスワードを使うことのないよう助言する。
- インスタント認証、リアルタイム認証、テストデポジット認証、ID認証、および／またはアウトオブウォレット質問を用いて本物の顧客を確認し、詐欺の機会を減らす。
- 顧客があなたのサービスにログインする際は、二要素認証の利用を提案するか義務付ける。
- ユーザーアカウントに詐欺の痕跡がないか、定期的に確認する。

データの保護

- 貴組織がサービスを遂行するにあたって、どの顧客データを収集する必要があるのか検討し、その用途以外の顧客データを収集する際は警戒する。
- データ保持ポリシーを設定して配布する。不要になった顧客データは破棄する。
- 転送および保存中のデータを暗号化する。
- データセキュリティポリシーを配備して、どのデータ転送手段が承認または禁止されているのか明確にして、従業員が顧客データを取扱う際に容認される手段を特定する。こうしたポリシーが全ての従業員を対象に文書化、連絡、施行され、定期的に審査・更新されるよう万全を期する。

公開 WEB アプリケーションのセキュア化

- 組織の顧客対応 Web アプリケーション上で HTTPS を実装し、全ての HTTP トラフィックを HTTPS にリダイレクトする。
- Web サイトでコンテンツセキュリティポリシーを採用し、クロスサイトスクリプティング攻撃、クリックジャッキング、またその他のコードインジェクションを防止する。
- Web サイトで公開キーピニングを有効化し、中間者攻撃を防止する。
- 顧客対応 Web アプリケーションが、極秘または重要な顧客情報（パスワードなど）の保管にクッキーを一切利用せず、クッキーに関して控えめな有効期限（後ではなく近い将来）を設けるよう万全を期する。
- 最低年に一度、顧客対応 Web アプリケーションのセキュリティアセスメントとしてペネトレーションテストサービスの利用を検討する。

金融データを保護するための顧客および従業員向け個別アドバイス

各従業員と顧客が以下のサイバーセキュリティガイドラインに沿った個人的な行動を取り、準備度を高めてサイバー脅威から金融データを保護するよう助言しましょう。

1. デバイス全体にわたって基本的なサイバー衛生慣行を実装する。

- 全ての個人および業務用デバイスで強力なパスワードを利用し、パスワードマネージャーの利用を検討する。
- コンピューターおよびモバイルデバイスにおけるオペレーティングシステムとその他のアプリケーションを常に最新状態に保つ。
- 不正プログラムを防止、検出、そして削除するアンチウイルス、アンチマルウェア、そしてアンチランサムウェアソフトウェアをインストールする。
- ファイアウォールプログラムを利用して、コンピューターへの不正アクセスを防止する。
- 信頼できる会社のセキュリティ製品のみを利用する。コンピューターおよび消費者向け出版物のレビューを読み、コンピューターまたはオペレーティングシステムのメーカーに相談することを検討する。

2. 機密情報の取扱いには注意する。

- 銀行口座のパスワードまたはその他の金融口座に関する機密データを暗号化されていないメールで送信しない。
- 銀行または機密の個人情報が関係するその他の通信のためにインターネット接続を行う場合、いつ、どのようにして利用するのかよく考える。図書館またはホテルのビジネスセンターなどの公衆 Wi-Fi ネットワークおよびコンピューターにはリスクが伴う。

3. フィッシング攻撃に抵抗する。

- 一方的に送られてきたか、疑わしいメールの添付物またはリンクを直ちにクリックしない。Stop. Think. Click.
- 予期せぬ形で誰かがインターネットまたは電話で連絡してきて、個人情報を求めた場合は警戒する。既知のアドレスと通信している場合でも、メール上での個人情報の共有は最小限に留める。
- 金融機関は既にあなたに関する個人情報を保持しているため、機密情報を求めてメールまたは電話で連絡してくることはない点に留意する。
- 一度も口座を開いたことの無い銀行から情報を要求された場合は、詐欺であるものと仮定する。
- 個人情報を提供する前に、疑わしいメールまたはポップアップボックスの妥当性を検証する。メールアドレスに注意を払う。

従業員の訓練

- 従業員に説明責任と戦略を教えて、顧客データの漏洩につながる人的エラーを最小限に留める。つまり、以下の点について助言すること：
    - 顧客データへのアクセスおよびその転送は、各職務権限の遂行のみに必要となるよう最小限に留める。
    - 顧客データを取扱う全てのデバイスおよびアカウントにおいて、強力なパスワード、二要素認証の有効化、ソフトウェアの最新状態の維持、そして疑わしいリンクのクリック回避による強力なセキュリティ慣行を維持する。
    - 潜在的な内部／外部セキュリティインシデント、脅威、またはデータの取扱いミスについて、組織の技術職員および／または上級管理職に通報する。
- 必ず、従業員が組織のデータ保護およびセキュリティポリシーを理解し、これを遵守する書類に署名するよう万全を期する。こうして、ポリシーに違反せず、顧客との対応も円滑にこなし、無防備な方法で顧客とのコミュニケーションを行うことのないようにする。

顧客への通達

- 組織の規制環境に対するアウェアネスを築き、顧客のデータ漏洩を取扱うインシデントが発生した場合も確実に遵守できるようにする。
- 貴組織が顧客の機密情報への不正アクセスによるインシデントを把握した場合、調査を進めて当該情報が悪用されたか、今後悪用される可能性を速やかに判断する。通達に関するベストプラクティスに従い、影響を受けた顧客にできる限り早急に以下の点を伝える：
    - インシデントの基本的な情報および漏洩した情報
    - 更なる情報および支援を提供するための電話番号
    - 今後 12～24 カ月間にわたって「引き続き警戒する」必要があることの確認
    - なりすまし犯罪が疑われるインシデントが発生した場合の迅速な通報の奨励
    - 当該情報を更なる不正アクセスまたは使用から保護するために金融機関が取っているステップの基本的な情報
    - 信用調査機関の連絡先情報
    - 貴組織が遵守するべき規制に基づき義務付けられているその他の情報

CISO レベル向けガイド：第三者との繋がりを守る

第三者を通じたリスクの特定

- 全てのベンダー関係ならびに各関係で晒されるアセットおよびデータを網羅したリストを作成して、継続的に更新する。
- 各ベンダーまたは第三者がアクセス可能なデータを審査して、各アクセスレベルが「最小権限の原則」に従っていることを確認する。
- ベンダーのシステムにデータ漏洩が発生した場合の貴組織への影響に基づき、ベンダーと第三者の関係性を順位付けする（低、中、高）。
- リスクが最も高いベンダーから始めて、各プロバイダーのサイバーセキュリティ性能および関連規格への遵守について評価する。関連規格への遵守は、ふさわしい開始点となる。定期的なセキュリティ評価計画を策定する。最もリスクが高い、および／または顧客データへのアクセス権が最も多いベンダーに関しては、時々オンサイトアセスメントを実施することが望ましい。

第三者のセキュリティの管理

- 徹底したデューディリジェンスを実施する。ベンダーとの提案、契約、事業継続性、インシデントレスポンス、そしてサービスレベル契約に関するあらゆる要求に関して、サイバーセキュリティの期待を設定する。サイバーインシデントが発生した場合の責任および義務について合意する。
    - 貴組織がデータの取引または共有を行う金融機関およびその他のエンティティのサイバーセキュリティ慣行について問い合わせる。貴組織が遵守するべきサイバーセキュリティ要件には、データの共有またはアセットの露出を行うベンダーおよびその他の組織も従う必要がある。
- サイバーセキュリティ規格に対するベンダーのコンプライアンスを監視するため、確立および合意済みの措置を取る。
- 機密データを取扱うベンダーに問い合わせて、貴組織が同ベンダーで抱えているアカウントにおいて二要素認証、暗号化、またはその他のセキュリティ対策を提供しているか確認する。
- 必ず、インストールする全ての第三者ソフトウェアおよびハードウェアにセキュリティ用のハンドシェイクが設定されていることを確認する。これで、ブートプロセスが認証コードによってセキュア化され、コードが認められない限り実行されない。
- 偽物または仕様に一致しないベンダーの製品に遭遇した場合、解決策に向けて交渉するか、出口戦略を見つける。
- 毎年、ベンダーとの契約を見直し、必ず貴組織の戦略的方向性およびデータセキュリティの規制要件を引き続き満たしていることを確認する。契約終了時には、アセットまたはデータの返却、ベンダー側で完全に消去されていることの確認、貴組織のシステムまたはサーバーへの一切のアクセスの無効化に関する規定を含める。

情報の共有

- 貴組織のベンダーおよび取引先にセキュリティの問題について連絡できる、明確な伝達経路と連絡先が存在することを確認する。
- 信頼できる、実践的なサイバーセキュリティ情報を内部および外部ステークホルダー（金融セクター内外のエンティティおよび公的機関を含む）と適宜共有する。
- 他組織が第三者との間で経験している脅威、脆弱性、インシデント、およびレスポンスに関する最新情報を追跡して、組織の防御力を高め、状況認識力を高め、学習の機会を広げる。FS-ISACなどの情報共有組織に加わることで、最新情報を取得しやすくなる。

サイバーセキュリティを念頭に置いたベンダーの選定

潜在的なベンダーに以下の質問群を尋ね、各社のサイバーレディネスおよびアウェアネス、また貴組織のリスクプロファイルに及ぼす影響について測定してください：

1. **経験値はどの程度あるだろうか？** ベンダーがクライアントに提供してきたサービスの履歴を調べること。貴組織に似たクライアントにサービスを提供するにあたってどのような経験があるだろうか？
2. **既知のサイバーセキュリティ規格へのコンプライアンスを文書化しているだろうか**（NISTフレームワークもしくはISO 27001、またはSOC2レポートを提供できるだろうか）？
3. **サービスを履行するために貴組織のどのデータおよび／またはアセットにアクセスする必要があるだろうか？** 不要と思われるアクセスを要求しているだろうか？
4. **保持した貴組織のアセットおよびデータをどのように保護する予定だろうか？**
5. **自社の第三者サイバーリスクをどのように管理しているだろうか？** サプライチェーンセキュリティに関する情報を提供できるだろうか？
6. **貴組織に影響を及ぼすインシデントが発生した場合、どのようなディザスタリカバリおよび事業継続性プランを抱えているだろうか？**
7. **貴組織への最新情報の提供はどのような形で行われるだろうか？** 自社内の動向、脅威、および変化をどのような形で連絡する予定だろうか？

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

THE WORLD BANK IBRD • IDA | WORLD BANK GROUP

SWIFT INSTITUTE

FS-ISAC

Standard Chartered

CYBER READINESS INSTITUTE

GLOBAL CYBER ALLIANCE

ICBA Independent Community Bankers of America

インシデントレスポンスガイド

準備

- 貴組織の上級管理職およびその他の関連職員と協力して、サイバーリスクアセスメントにおいて特定された最も差し迫ったリスクに基づくインシデントレスポンスおよび事業継続性計画を策定する。
  - 貴組織において最も優先度の高いサイバーリスクに関わるインシデントの種類に対応した脅威シナリオを策定する。こうしたシナリオに対応できるキャパシティの構築に焦点を当てること。
  - インシデントレスポンスに関する連絡先リストを特定および記録し、組織内で提供する。
  - 関連する地方自治体および連邦の法執行機関および当局者に関する連絡先情報を特定・記録する。
  - どのような種類のインシデントをいつ、誰に通報する必要があるのかを明記した条項を設ける。
  - インシデントが及ぼす機能および情報面での影響、またそこからの復元可能性などの関連要素に基づき、職員に求められるインシデントレスポンスの速さ、また職員が実行するべき行動を概説した書面上のガイドラインを設ける。
  - 全ての従業員に対し、インシデントが発生した場合は技術チームに連絡するよう伝えておくこと。一般的に、これはITスタッフおよび／または CISO／CIO／その他の同等マネージャーが該当する。
  - ソリューションを展開して、従業員の行動を監視し、内部脅威およびインシデントの特定を可能にする。
  - 事業継続性計画を含めることで、貴組織が業務上の緊急事態に遭遇した際はサプライヤーおよび主要顧客とどのように協働するのか調整する。これには、必要に応じて手動または代替の事業運営の実施方法を含める。
  - 緊急システムの停止および再起動に関する書面上の手順を含める。
  - バックアップデータの回収および復元用のテスト手法を開発する。定期的にバックアップデータをテストして、その妥当性を検証する。
  - 代替の施設／現場で事業活動を行うための確立した合意および手順を用意する。
  - 全ての顧客を対象とした明確な普及チャンネルを配備する。

演習

- 全ての職員または組織の重役、PR／コミュニケーション職員、および法務・コンプライアンスチームを含む、あらゆる職位の代表者と共に小規模な机上演習を編成する。
- 貴組織に関連性のある、業界全土の机上演習を特定して、可能な限り参加する。
- 演習で学んだ教訓を貴組織のサイバーセキュリティ戦略に確実に取り込むための プロセスを設定する。

レスポンス

- 風評被害を含む、事業活動に対する影響を最小限に留めるため、インシデントレスポンス計画の行動を実装する。
- 影響／被害を受けたシステムを特定して、その損害を評価する。
- 影響を受けたアセットを取り除き（接続を解除）、損害を減らす。
- チームがインシデントの発生を疑った時点で、早急にあらゆる情報の記録を開始する。影響を受けたことが特定されたアセットの接続解除／隔離を行いながら、インシデントの証拠保全を試みる（例：影響を受けたログのシステム構成、ネットワーク、侵入検知ログの収集）。
- 適切な内部当事者、第三者ベンダー、および当局に通達して、必要ならば支援を要請する。
- 法規および関連機関のガイダンスに沿った形で顧客への通知および支援活動を開始する。
- FS-ISAC または MISP などの脅威情報共有プラットフォームを利用して、脅威に関して業界に通達する。
- 後日見直すことができるよう、インシデント中に取った全てのステップを文書化する。

復元

- 可能であれば回収したアセットを定期的に「リカバリポイント」で復元して、最後に確認された「良好」ステータスにバックアップデータで復元する。
- 復元したアセットから最新の「クリーン」なバックアップを作成して、重要なアセットの全てのバックアップを物理的および環境的にセキュアなロケーションに確実に保管する。
- 感染したシステムが完全に復元したことをテスト・検証する。 影響を受けたシステムが正常通り機能していることを確認する。

審査

- インシデント発生後は「学んだ教訓」に関するディスカッションを実施する。上級職員、信頼できるアドバイザー、そしてコンピューターサポートベンダーと会い、予想される脆弱性の審査または実装すべき新たなステップの推奨を行う。
- 可能であれば、インシデントを引き起こした脆弱性を特定し（ソフトウェア、ハードウェア、事業活動、または従業員の行動において）、これを緩和する計画を立てる。
- 特定した問題に関連した類似または将来的なインシデントの検出を可能にする監視計画を策定する。
- インシデントの情報および学んだ教訓について、FS-ISACなどの脅威情報共有プラットフォームで共有する。
- 学んだ教訓を貴組織のインシデントレスポンスプロトコルに取り込む。

ランサムウェア：防止および保護

リアルタイム保護

悪意のある行為を行うものがコンピューターシステムを麻痺させ、元に戻すため身代金の支払いを要求することで、マルウェアによる収益化手段を見つけて以降、ランサムウェアの脅威は増大し続けている。効果的に運用させるには長期にわたって隠しておく必要のあるその他のマルウェアとは異なり、ランサムウェアはスピアーフィッシング、不正アクセスを受けた Web サイト、そして破損したダウンロードによって迅速に実行できるようエンジニアリングされている。金融機関は、ランサムウェアの影響を特に受けやすくなっている。これは、魅力的な標的と見なされている以外にも、資金を迅速かつ効率的に動かす能力が脅かされることが原因となっている。しかし、悪意のある行為を行うものは、必ずしも約束を守る訳ではない。身代金の支払いを得ても、マルウェアの除去や機密データへのアクセス制限解除を行わない攻撃者も存在する。

- 新たな脅威インテリジェンスにリアルタイムで適応できるアンチマルウェア保護システムに投資する。
- 機密または必須情報を収容したネットワークに接続した全てのデバイスのセキュリティを評価する。必須ではない全てのシステムを別のネットワークに接続する。
    - 職場にIoTまたは「スマートデバイス」を持ち込む際は、特に注意が必要である。なぜなら、こうしたシステムのセキュリティは脆弱であるか、ほぼ存在しない場合が多いため、必須システムへのアクセスポイントとして標的にされる可能性があるため。
    - リモートワークセットアップのセキュリティを考慮する。セキュリティツールがオフネットワークでも動作し、全ての Web トラフィックを監視できるようにする。
- フィッシング攻撃および強力なパスワード保護の必要性に関して従業員教育を推進する。
- 実行可能であれば、組織全土における多要素認証の実装を検討する。
- 全てのソフトウェアおよびシステムを定期的にアップデートする。可能であれば、自動アップデートに設定を変更する。
- ランサムウェア攻撃および貴重なデータの損失に対処するためのインシデントレスポンスおよび危機管理計画を策定する。
- ランサムウェア攻撃が発生した場合に備えて外部コミュニケーション計画を準備する。

データバックアップ

- データを常に保護する、セキュアかつ定期的にアップデートされるバックアップシステムに投資する。
    - USB またはハードドライブを利用する場合は、バックアップの終了後にネットワークコンピューターからこうしたデバイスの接続を物理的に切断する。
    - クラウドストレージを利用する場合は、サーバーに高レベルな暗号化と多要素認証を配備する。
- 最悪の場合のディザスタリカバリに備えて、総勘定元帳の読み取り専用コピーを作成しておく。
- 自動データリカバリおよび修復を実行するシステムを開発する。
- 重要データおよびビジネスサービスの復元にどの程度の時間を要するか、シナリオを策定する。

規制環境

- 運用環境におけるランサムウェアに関する法規ガイダンスを評価する。
    - 各国ごとのガイダンスを考慮する。変更されたガイダンスの定期的な評価計画を策定する。
    - 金融セクター固有のガイダンスを考慮する。
    - 国際的な法規要件を考慮する。
- 身代金を支払う場合のリスクを評価する。一部のケースでは、身代金の支払いが悪意のある行為を行うものに対して配備された既存の制裁体制への違反となる場合がある。
- 現地法執行機関と連絡を取る。攻撃が発生した場合の迅速な情報共有のつながりを築く。
- ランサムウェアに関するサイバー保険ポリシーのメリットとデメリットを評価する。

組織のランサムウェアに対するレディネスの測定

ランサムウェアの防止および保護対策を策定する際は、以下の質問を検討すること。

1. 貴組織では、**定期的なスケジュールバックアップ**を実施しているだろうか？
    - こうしたバックアップは、クラウドストレージシステムまたはエアギャップされた USB／ハードドライブ経由で接続を遮断されているだろうか？
2. 貴組織のネットワークには、**必須でないデバイス**が接続されているだろうか？
    - こうしたデバイスは、機密データを収容していない他のネットワークに移動できるだろうか？
3. 貴組織は、身代金の支払いに伴う**法規上のリスク**について把握しているだろうか？
    - この点に関する法務ガイダンスは国ごとに異なり、頻繁に更新されている。
4. 貴組織は、ソフトウェアおよびシステムを定期的にアップデートしているだろうか？ こうしたアップデートは**自動化**されているだろうか？
5. 貴組織は、**ランサムウェア攻撃およびデータ損失に対処するための計画**を抱えているだろうか？
6. 貴組織は、**サイバー保険ポリシー**に加入しているだろうか？ ポリシーがある場合、ランサムウェア攻撃はどのように補償されるだろうか？
    - 一部のプランは身代金の支払いを明白に禁止しているほか、中にはポリシーの一環としてこうした支払いを補償するものもある。

ワークフォースの開発

ニーズの特定

- ワークロードの要件を特定する。
  - 貴組織の運用の複雑性ならびに行動の実行スピードを評価する。
  - サージキャパシティのニーズならびに先端テクノロジーが攻撃表面の減少に寄与するかを検討する。
- ワークフォースの要件を特定する。
  - 貴組織のサイバーセキュリティワークフォースのコンピテンシー、柔軟性、また敏捷性を検討する。
  - 理想的なレポート機構を特定して、多機能性が望まれるエリアを強調する。
- サイバーセキュリティワークフォースがサポートするビジネス機能に基づき、必要とされる知識、スキル、能力、そしてコンピテンシーを定義する。
- 組織の既存のサイバーセキュリティワークフォースにおける重大なギャップを特定する。
  - NICE フレームワークなどの既存ツールを利用して、役割と責任に関する内部アセスメントのガイダンスに利用する。

社内研修および能力開発の促進

- サイバーセキュリティワークフォースの昇進コースを強調したキャリアマップを開発する。
- サイバーセキュリティの役割に向けた従業員の再訓練・再配置ルートを組織内で特定する。
  - 関心および能力に基づき、サイバーセキュリティへの従来とは異なるエントリーポイントの可能性を検討する。
  - アップスキルおよび再訓練プログラムを拡張し、組織内の異動を奨励する。
- 社内研修および自主学習を奨励する。
  - 継続学習およびスキル認定の機会を開拓する。
- ワークフォースリテンションに関するデータを追跡する。
  - リテンションデータを定期的に評価して、研修および能力開発プログラムが従業員のニーズを満たしているか明らかにする。

社外登用の改善

- 社内で一貫性ある明白な職務記述書によって求人票の中身を改善する。
  - NICE フレームワークなどの既存ツールを利用して、関連のスキルセットを強調する。
- 応募プロセスを通じて募集に関するデータを収集し、応募者の種類と過去の職務経験に関する情報を取得する。
  - データ収集を体系化して社内全体で共有することで、情報のサイロ化を防止して人材の調達・開発を支援する。
  - 定期的に求人データを評価して、アウトリーチのギャップを特定する。
- 複数の指標を活用して候補者の潜在能力を評価する。
  - 体系的な採用アセスメントの実装を検討する。
  - 関連の学位、認定、そして職務経験を評価する。
  - 採用を決定する際は、特定の測定基準のみに依拠するのを避ける（例：エンジニアリングの修士号）。

基本的アプローチ

サイバーセキュリティワークフォースを開発する際は、以下の戦略的アプローチを検討してください。

1. **新規人材を生み出す 供給パイプライン**を広げる。
   - 大学または専門学校と関わりがありますか？
   - サイバーセキュリティインターンシップおよび実習プログラムを提供していますか？
2. 既存の供給を特定して欠員ポジションと合致させる。
   - 人事部は必要とされるスキルを職務記述書の投稿で効果的に掲載できていますか？
3. **再訓練を通じて 既存の職員**をサイバーワークフォースの一部にする。
   - 貴組織はリソースをサイバーワークフォースに移して既存の人材を活用していますか？
4. **テクノロジーイノベーション**を通じてサイバーワークフォースの**需要を減らす**。
   - 第三者サービスプロバイダーとの間でサージキャパシティを築く合意はありますか？
5. 現行ワークフォースの**リテンションを改善する**。
   - 貴組織は才能あるチームメンバーに投資していますか？
   - 貴組織は関心のある個人がサイバーセキュリティのキャリアを追求できるようにしていますか？