サイバーセキュリティ危機管理計画チェックリスト

ゼットスケーラーのプラットフォームで事業継続を計画し、維持するためのヒント

zscaler™

先行きが不透明な状況で、最高責任者が最優先で取り組まなければならないのは、従業員とコミュニティの健康を守ることです。災害発生時ほど、開発だけでなく運用においても、俊敏性が求められる時はありません。危機によって運用が混乱するかもしれません。しかし、危機によって引き起こされた「ニューノーマル（新たな常識）」に適応できれば、サイバーセキュリティの脅威を食い止めることができます。

緊急事態に直面した際、CISOには迅速かつ決断力を持って行動することが求められます。ゼットスケーラーは、以下の8点が緊急事態におけるCISOの主な戦略的目標であると考えます。

1. 従業員のリモートワークを可能にし、支援する →
2. セキュリティ運用と監視チームのリモートワークを可能にし、支援する →
3. サイバー脅威のリスク、特に危機的状況に乗じた攻撃の増加への対応を計画する →
4. サードパーティベンダがシステムをサポートできることを確認する →
5. ビジネスセキュリティの優先事項を調整する →
6. 予算の調整と精査を計画する →
7. さらに困難になる状況においても、法規制へのコンプライアンスが保証されるようにする →
8. 変化の時に頼れるリーダーとなる →

危機的状況はその都度異なります。
以下のチェックリストを、CISOの危機管理のブループリントとしてご活用ください。

1. 従業員のリモートワークを可能にし、支援する

危機的状況、特にウイルスの大規模発生時には、従業員によるリモートワークを可能にする必要があります。CISOは、以下の点を考慮しなければなりません。

☐ 従業員がリモートワークをすることで、データセンタの運用にどのような影響が起こり得るか？

- 実作業が困難な状況では、パッチやアップデートのワークフローが中断する可能性がある
  - リモートでのシステムのパッチの適用と管理のプロセスを確認し、確立する
- サイバー侵害と侵害されたデバイスをリモートで調査する必要がある
  - サイバー脅威の修復をリモートワークで可能にするための新しいプロセスを作成する
  - リモートワーカーと社外アセットの調査、およびフォレンジックの新しいプロセス生成を実行する
  - トリアージ：調査に優先順位を付け、まず重要なイニシアチブに集中的に取り組む
- オフィスが無人となるため、社内の無線ネットワークがハッカーにとって格好の侵害点になる
  - オンプレミスの無線ネットワークをリモートで保護できること、不要の場合はリモートでシャットダウンできることを確認する

☐ サービスや製品のライセンスはリモートワークに移行しても問題なくサポートされるか？

- エンドポイントのライセンス数がリモートワークの増加に伴って変わるかどうかを判断する
- サイバーセキュリティツール（アンチウイルス、エンドポイントの検知とレスポンス、アイデンティティのアクセスと管理を含む）のライセンス数がリモートワークの増加に伴って変わるかどうかを判断する
- リモートワークのBYODアクセスへの移行がライセンス数に影響するかどうかを判断する

☐ 企業がリモートワークへ移行するに伴い、デバイスのセキュリティ管理はどのように変化するか？

- リモートワークがセキュリティ管理にどう影響するかを判断する
  - インベントリの管理（NIST Cybersecurity Frameworkをガイドとして使用）と分析を実施する
- リモートで正しくコントロールできることを確認する
  - データセンタベースのコントロールは、VPNを使用しない場合に有効ではなくなる可能性がある（リモートアクセスの一時的な急増によって過負荷状態に陥る可能性がある）
  - 必要があれば、それに代わるコントロール（管理による方法や技術的な方法）を特定する
  - DLP（情報漏洩防止）メカニズムに影響するリスクを特定する

- 可視性が失われた場合の対応計画を策定する
  - エンドポイントと通信できなくなる可能性があるため、テレメトリを受信する代替方法を特定する
  - アップデートのデフォルトのメカニズムが有効であることを確認する

☐ マルウェアのクリーンアップをどのように処理するか？

- リモートのエンドポイントをクリーンアップする方法を確立する
  不可能な場合は、従業員によるデバイスの取り扱いのワークフローを確立する

☐ 対面でのコミュニケーションやイベントが不可能な状況でセキュリティに対する意識改革をどのように行うか？

- サイバーセキュリティのベストプラクティスを周知するプロセスを確立する
- 定期的に開催される上級管理職向けコミュニケーションに「セキュリティブリーフ」を追加する

2. セキュリティ運用と監視のチームのリモートワークを可能にし、支援する

データセンタとセキュリティの担当者は、自らも在宅勤務しながら、従業員の在宅勤務を支援することが見込まれます。セキュリティやITのワークフローに影響が出る可能性を考慮しましょう。

☐ ITチームがリモートワーク時、どのように情報を伝えるか？

- メーリングリスト、グループチャット、定期的な（バーチャル）会議の仕組みを確立する
- ZoomやWebExなどの会議ツールを使用する
- Slack、Microsoft Teams、Google Chatなどのコラボレーションツールに投資する

☐ ITチームはどのように自宅からツールや監視にアクセスするか？

- アクセスポリシールールを変更して、リモートでの使用を許可する
- 可能であれば、Webフロントエンドやクライアントアプリケーションをリモートアクセスに使用する

☐ インシデント対応はどのように変わるか？

- リモートのセキュリティインシデントに対応するための計画を確立する
- リモートインシデントの修復計画を策定する

☐ アイデンティティのプロビジョニングと解除をどのように実行するか？

- 従業員のアクセスのリモートでの許可 /取消を可能にする
- 必要があれば、リスク軽減戦略として権限の範囲を少なくする
- SLAM（Starters、Leavers、And Movers：人事異動）プロセスで従業員や役員が実際に立ち会う必要がある場合は、次のような計画を定義する
  - 資産の配布や回収
  - 資産の（物理的および論理的）クリーニング
  - 文書の署名
- 必要に応じて、郵便や宅配システムを利用してトークン・MFAメカニズムを配布できるようにしておく

☐ 在宅勤務はサードパーティのセキュリティサービスにどのように影響するか？

- サードパーティのアクセス要件を決定し、文書化する
- 緊急性に応じてサードパーティのアクセスが優先されるようにする
- サードパーティのアクセスの許可・取消のワークフローを確立する

3. サイバー脅威のリスク、特に、危機的状況に乗じた攻撃の増加への対応を計画する

2020年のCOVID-19の感染拡大のような危機的状況では、多くの場合に「機に乗じた」マルウェア攻撃が増加します。

リモートアクセスにVPNを採用している企業でリモートワークが増えると、MPLSバックホールの距離と脅威対象領域の両方が大きくなります。VPNベースの境界セキュリティモデルは、簡単に拡張してリモートアクセスの増加をサポートすることができないため、一部の従業員がファイアウォールをバイパスしてインターネットに接続しようと考えるようになる恐れがあります。そのような脆弱性にハッカーが不正を働く隙ができます。更には、危機に関連する大量の情報が報道され、セキュリティ意識が低下する可能性があり、危機を伝える重要な情報であるかのように装ってマルウェアを送り込もうと考える犯罪者も現れます。

危機的な状況と情報侵害の増加には関連性があることが、サイバーセキュリティのエキスパート（ゼットスケーラーのThreatLabZチーム）によって確認されています。CISOは、このような危機状況下で発生する新たな脅威リスクに対処する必要があります。

☐ リスクの測定
リモートユーザはフィッシングやその他の策略に対して脆弱か？

- セキュリティポリシーを従業員に繰り返し説明し、危機関連の詐欺について従業員に周知する
- 緊急時であってもセキュリティが重要であることを周知する

4. サードパーティベンダがシステムをサポートできることを確認する

サードパーティのセキュリティベンダは、運用を調整して、危機的状況下での要求にも対応できなければなりません。サードパーティベンダとのコミュニケーションを図り、システムのサポートが環境に影響するような形で変わらないことを確認しましょう。

☐ セキュリティベンダは、危機的状況に合わせて運用の調整およびサポートを提供できるか？

- サードパーティベンダによるサポートの監査：
  - リモートであっても、サードパーティのシステムアクセスが継続されるようにする
  - 各ベンダの事業継続計画（BCP）の準備と危機サービス計画を確認する
  - 特に、MSSP（マネージドセキュリティサービスプロバイダ）は、在宅勤務に対応できない場合がある そのリスクに対してどのように計画できるか？

5. ビジネスセキュリティの優先事項を調整する

危機的状況では、企業は緊急対応に重点的に取り組むことになるため、サイバーセキュリティの対策には優先的に目を向けられない可能性があります。

☐ 状況が変化する中で、どのようにセキュリティを維持するか？

- 必要があれば、会社の資産の許容可能なリスクレベルを調整する
  - 物理、および論理アセットのインベントリを作成する
  - アセットに対するリスクとなる要素を可能な限り可視化する
  - パフォーマンスとセキュリティを比較して評価し、必要に応じてセキュリティ体制を調整する
- リモートワークへの移行を前提にリスク許容度を評価する
- 必要とされる変更やアクションを拒否することなく、セキュリティの支持者であり続ける（セキュリティが長期的な成功にとって重要なことに変わりはない）

☐ 新しいプロセス、導入環境、デバイスが可視化されるか？

- レポート（フィード、ログ、テレメトリ）をリモートで取得、使用、評価するメカニズムを確立する
- 会社の外のシステムからその情報に基づいてアクションを実行するプロセスを確立する

6. 予算の調整と精査を計画する

危機的状況では、緊急対応への支出がセキュリティより優先される可能性があります。プロジェクトに対する予算が不足する、または獲得自体が困難になるケースもあります。緊急の運用上のニーズに対応するために、セキュリティの優先順位が下がることは大いにあり得ます。

☐ 運用や計画の予算に影響するか？

- 重要な計画、デバイス、サービスのインベントリを作成して優先順位を付け、必要に応じて切り分ける
- 必要不可欠でないものを削る準備をする
  （そして、「必要不可欠」が何かという新しい定義を受け入れる）
- 出張、イベント、将来のイニシアチブの予算をセキュリティの優先事項に回す

7. さらなる困難に陥っても、法規制へのコンプライアンスが保証されるようにする

危機的状況においても、企業の法規制へのコンプライアンスは引き続き求められます。

☐ 危機に対応するための運用や構造の変更は、法規制要件に対する組織のコンプライアンスの能力にどのように影響するか？

- 新しいデバイスやプロセスの展開がデータフローやセキュリティ要件にどのように影響するかを判断し、文書化する

☐ データの保存に関する要件に対する組織のコンプライアンスの能力は、危機対応の運用の影響を受けるか？

- データが保存される場所とデータの移動経路がどのように変化するかを判断する
- 新しいデータフローパスにおいてもコンプライアンスが維持されることを確認する
  クラウドやデータセンタの管理の変更が必要になる場合があり、状況によっては、異なる地域への新たなデータの冗長性の追加が必要になる場合もある
- SSLやその他のセキュリティ対策が必要に応じて採用されていること、データプライバシーの適用法を準拠していることを確認する

☐ 危機状況下においては、コンプライアンスのルールが法規制団体や政府によって調整されることになるか？

- コンプライアンス要件に影響する法規制の通達を監視する
- 危機によって生じるコンプライアンス要件の調整にあたっての対応ワークフローを構築する（または、少なくとも構築を計画する）

8. 変化の時に頼れるリーダーとなる

危機的状況では、誰もが十分な情報を入手できない中で動き、事態の対処にあたる必要があります。セキュリティの維持が不可欠であるため、CISOがパニック状態に陥ることがあってはなりません。危機的状況での有効なコミュニケーションには、確かな視点、謙虚さ、率直さ、強い発言力が必要です。具体的な目的もなく過剰なコミュニケーションを取ると、無駄な情報に振り回される結果となりますが、コミュニケーションが不足すると情報の空白が生じてしまいます。明確な行動計画を確立し、適切なコミュニケーションを図ることが大切です。

☐ 誰とコミュニケーションする必要があるか？

- 社内のセキュリティ関係者が、役割、責任、行動、プロセスを十分に理解していることを確認する
- 運用に影響する変更が社外の関係者と顧客に通知されるようにする

☐ どれ位の頻度でコミュニケーションが必要か？

- 重要な変更が発生した場合は直ちに知らせる
- 明確な測定指標と進捗の通過点を使用し、測定と追跡が可能な段階にわけて計画を伝達する
- コミュニケーションが配信されるだけでなく、受信、理解、実行されたことを確認する
  コミュニケーションの有効性を測定するためのワークフローを確立する

☐ 誰とコミュニケーションを調整するか？

- 社内に危機コミュニケーションチームを設立する
- 業界団体に相談して、コミュニケーションのベストプラクティスのベンチマークを実施する
- 関連する（地方自治体や国の）政府機関のリソースを調査する

☐ CISOはどのような形で危機コミュニケーションのリーダーシップを最も発揮できるのか？

- CISOには、セキュリティのプロフェッショナルとしての危機管理の経験があるはずである
  - その経験を活かし、リーダーとして、組織の準備と対応を進める
  - 組織の関係者による緊急時の判断の結果の評価を支援する
- 平常心でリーダーシップを発揮する：

– 知識、理解、準備を活かして、不安、不確実性、パニックに対処する

ゼットスケーラーのクラウドベースのセキュアアクセスサービスエッジプラットフォームは、ローカルインターネットブレイクアウト経由のダイレクト接続を可能にすることで、企業（およびそれらすべての企業のリモートワーカ）が予測できない状況に陥っても前進できるように支援します。

ゼットスケーラーの**事業継続プログラム**は、最も困難な状況下でも
世界最高水準のセキュリティスタンスを維持できるよう
お客様をサポートします。

詳細はこちら

ゼットスケーラーについて

ゼットスケーラーは「アプリケーションがクラウドに移行されるなら、セキュリティもクラウドに移行する必要がある」という、シンプルかつ力強い概念に基づき、2008年に設立されました。ゼットスケーラーは現在、世界中の数千の組織のクラウド対応の運用への移行を支援しています。

zscaler™