株式会社テリロジー

＜White Paper 抄訳版＞

NIST-CSF 基準

サイバーセキュリティリスク管理ガイド | ランサムウェア

Quick Start Guide

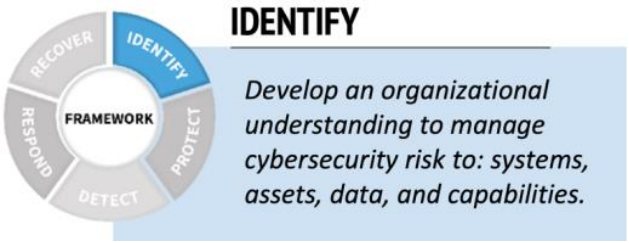
～ランサムウェアの脅威が高まる中、この Quick Start Guide は、
企業が NIST(米国国立標準技術研究所)のランサムウェアリスク管理ガイドを使用するのに役立つ～

はじめに

ランサムウェアに対抗するためのサイバーセキュリティフレームワークプロファイルについて解説します。これは企業がサイバーセキュリティリスクの削減を支援するために広く使用されている自主的なガイダンスで、NIST サイバーセキュリティフレームワークをベースにカスタマイズされたランサムウェアプロファイルは、パートナーやサプライヤーを含む内外の利害関係者間のコミュニケーションとリスクベースのアクションを促進します。

フレームワークは、識別(Identity)、保護(Protect)、検出(Detect)、応答(Response)、および復旧(Recover)の 5 つの主要な機能で構成されています

これら 5 つの項目は、サイバーセキュリティリスクを管理するためのライフサイクルを表示するための包括的なフローのしくみを提供します。各機能にリストされているアクティビティは、サイバーセキュリティの課題に対処するための企業を含め、あらゆるユーザ部門にとって効果的なスターティングポイントを提供します。これらは、企業がランサムウェアのリスク管理の取り組みから最大の価値を引き出せるように優先順位を設定するのに役立ちます。サイバーセキュリティのリスク管理では、現在の企業での運用レベルに大きく依存します。ランサムウェアに対処するために実行できることと実行すべきことは諸々ありますが、すべてを一度に実行する必要はありません。まずスタートすることが、ランサムウェアのリスク管理を含むサイバーセキュリティの重要な鍵です。NIST は、ランサムウェア攻撃を阻止するためにこれら 5 つの手順を実行することが重要です。このアクティビティは一般的にリスクアセスメントのワークフローでよく活用されています。
以下にこの 5 つの主要な機能について詳しく記述します。



➡ハードウェアとソフトウェアのインベントリを保全（資産管理）

企業で使用されているコンピュータのハードウェアとソフトウェアのインベントリを把握することは重要です。これらは、ランサムウェア攻撃に関与する悪意のある攻撃者のエントリポイントになることがよくあります。そして、ランサムウェア攻撃で悪用される可能性のある脆弱性の修正とか復旧に非常に役立ちます。インベントリは、スプレッドシートで整理して単純化することができます。ソフトウェアインベントリは、ソフトウェアの名前とバージョン、現在インストールされているデバイス、最後のパッチの日付、および既知の脆弱性を追跡するのに用います。

➡ドキュメント情報フロー

企業が使用する重要なドキュメント情報を知ることは重要ですが、特に契約や外部パートナーが関与している場合は、データがどこにあり、どこに流れるかを理解することも重要です。情報フローの記録（デバイス/インターネット間の接続など）を作成して、攻撃者が企業内をラテラルムーブメントに移動した場合にどの情報またはどのプロセスが危険にさらされているかを列挙できるようにします。

➡企業が接続する外部システムを特定

ランサムウェアの場合、パートナーとの通信方法を吟味し、外部システムから一時的に切断するための可能なアクションを特定する必要があります。これらの接続を特定することは、セキュリティ制御システム（アクセス権など）を導入し、サードパーティとも共有できる領域をもつのにも役立ちます。

➡重要なインフラプロセスと資産を特定

実行可能なプロセスを絶対に維持しなければならない企業の経営資源とは何か？ これは、ビジネス事業を継続するための Web サイトの保全、顧客情報の安全な保護、または企業が収集するデータへのセキュアなアクセスと正確性の維持を保証することです。これらは、ランサムウェアに対する企業の対策スコープとインパクトレベルを明確にするために不可欠であり、将来のランサムウェア対応、緊急対応、および復旧アクションの緊急時対応計画にも不可欠です。こうした情報を事前に準備しておくと、企業はリソースに優先順位を付けることができます。産業制御システム（ICS）に依存している場合は、こうした施策は必要です。

➡役割と責任を明確にするサイバーセキュリティポリシーを確立

これらは、従業員、請負業者、パートナーを含む企業のサイバーセキュリティ対策がどのように企業情報とシステムインフラを保護し、重要な企業プロセスをサポートするかについて明確に示す必要があります。サイバーセキュリティポリシーは、企業でのリスク管理の考慮事項（財務、評判など）とのリンクが必要です。

➡資産と情報へのアクセスを管理

企業は、物理的およびコンピュータ関連の資産と関連施設へのアクセスを許可されたユーザ、プロセス、およびデバイスを制限し、重要なアクティビティとトランザクションのリスクに関わるアクセスを管理します。まず、従業員毎に一意のアカウントを作成し、ユーザが自分の仕事に必要な情報、コンピュータ、およびアプリケーションにのみアクセスできるようにします。可能な限り、標準のユーザアカウントと管理者権限を持つアカウントを選択する必要があります。 ユーザはそのアクセスする前に、強力なパスワードまたは多要素技術によってユーザ認証します。殆どのランサムウェア攻撃はリモートで実行されるため、悪意のあるコードの挿入やデータの漏えいから保護するために、システムとデータファイルの整合性を維持するためにリモートアクセスを制御することが不可欠です。個人用デバイスからの公式ネットワークへのアクセスは制限します。ラップトップコンピュータであろうと産業用制御システム（ICS）の重要なコンポーネントであろうと、デバイスへの物理的アクセスを厳密に管理および追跡します。大規模とか複雑な企業組織形態では、ネットワークのセグメンテーションまたは分離により、潜在的なターゲットシステム間でマルウェアが拡散するのを防ぐことにより、ランサムウェアの範囲を制限できます。　これは、安全計装システム（SIS）を含む重要な ICS 機能にとって特に重要です。

➡デバイスの脆弱性を管理

コンピュータやその他デバイスの OS とアプリケーションを定期的に更新して攻撃から保護します。これらにパッチを当てておく必要があります。可能であれば、自動更新を有効にします。ランサムウェアサイトへのアクセスをブロックします。ソフトウェアツールを使用してデバイスをスキャンし、追加の脆弱性を検出し、可能性または影響が大きい脆弱性を修正します。変更および更新プロセスを適切にコンフィグすると、マルウェアを含むアクセス管理ポリシーを満たさないコードを置き換えるような不正

行為を思いとどまらせることができます。

➡従業員や他のユーザの人材教育および訓練

すべてのユーザを定期的にトレーニングおよび再トレーニングして、企業のサイバーセキュリティポリシーと手順、および特定の役割と責任を認識していることを確認し、それを雇用の条件にします。ハードウェアとソフトウェアのインストール、構成、およびメンテナンスの責任者をトレーニングすることは重要ですが、同様に重要なのは、すべてのユーザが常にウイルス対策ソフトウェアを使用し、企業によって承認された場合にのみインストールし、確認済みリンクのみにアクセスして安全なネットワークを確保します。ユーザは、個人用デバイスから公式ネットワークへのアクセスが制限されていることを知っておく必要があります。

➡デバイスを安全に保護

ファイアウォールや、エンドポイントセキュリティなどのセキュリティ製品をインストールする必要があります。目的の機能をサポートするために不必要なデバイスサービスまたは機能は無効にします。デバイスを適切にフィルタリングするためのポリシーとしくみを確認する必要があります。これらの対策は、ランサムウェアの侵入を防ぎ、データ漏洩も防ぎます。

➡機密データを保護

企業は機密データを保存または送信する可能性が高いため、情報の機密性、完全性、および可用性を保護するために、リスク戦略と記録（データ）を管理する必要があります。認証チェックメカニズム（デジタル署名など）を使用して、ソフトウェア、ファームウェア、および情報の完全性を検証し、マルウェアの侵入で攻撃される改ざんを検出します。

➡定期的なバックアップを実施

データの可用性を保持することで、ランサムウェアのインパクトを軽減することができます。これには、オフサイトおよびオフラインでのデータバックアップを行う機能、および平均復旧時間(MTTR)とシステムの冗長性をテストする機能が含まれます。多くの OS には、バックアップ機能が組み込まれています。バックアップを自動化するためのソフトウェアおよびクラウドソリューションも利用できます。頻繁にバックアップされるデータセットをオフラインにしておくことは重要です。ランサムウェア攻撃からのタイムリーで比較的損害の少ないリカバリーのためには、定期的なバックアップが不可欠です。セキュアにバックアップし、オフラインにして、ランサムウェアや攻撃者によって破損したり削除されたりしないようにします。

DETECT

Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

➡検出プロセスをテストおよび更新

許可されていないエンティティや、ネットワーク上および物理的環境での人的活動を含むアクションなどの異常な振舞いを検出するためのプロセスと手順を決めテストします。これには、ランサムウェア攻撃への対応と復旧の優先順位を通知できるイベントを判断することが含まれます。大規模で複雑な企業環境では、ネットワークの可視性を向上させ、ランサムウェアの早期検出を支援し、ランサムウェアがネットワークを介してどのように侵入するかの振舞いを検知するのに役立つ複数のソースとセンサーを含むセキュリティ情報およびイベント管理（SIEM）ソリューションをインストールする必要があります。シスログは、コンピュータとアプリケーションの異常を識別するために重要です。システムやアカウントの変更、通信チャネルなどのイベントを記録します。これらのシスログを集約し、予想されるネットワークの振舞いからパターンまたは異常性を探すことができるソフトウェアツールの使用が必要です。

➡スタッフのトレーニング

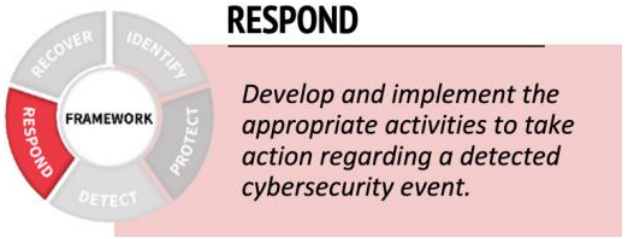
担当者は、社内組織および外部関係者に報告するための役割と責任を認識している必要があります。それにはトレーニングによる人材養成が必要です。

➡予想されるデータフローを把握

企業管理者はデータフローのしくみを知っていると、予期しないことが起こったときに気付く可能性がはるかに高くなります。予期しないデータフローには、内部データベースからエクスポートされて社内ネットワークから外部インタネットに送出される顧客情報が含まれる場合があります。クラウドまたはマネージドサービスプロバイダーに作業を委託している場合は、データフローを追跡し、予期しないイベントを含めてレポートする方法についてプロバイダーと話し合う必要があります。

➡サイバーセキュリティイベントのインパクトをすばやく伝達して判断

ランサムウェア攻撃で損害を被る前に、異常なイベントをタイムリーに発信することは、是正措置を講じるために不可欠です。サイバーセキュリティイベントが検出された場合、企業はそのインパクトの規模レベルを理解するために迅速かつ徹底的に調査を取り組む必要があります。適切な利害関係者や法執行機関とのコミュニケーションは、パートナー、監督機関、その他公的な機関との良好な関係を維持し、ポリシーとプロセスを改善するのに役立ちます。



➡レスポンスプランの策定

ランサムウェアに対するレスポンンスは、内部および外部の利害関係者とのプラン調整から始まります。被害の軽減とランサムウェアイベントの封じ込め、およびそのインパクトの判断手順に焦点を当てます。

➡内部および外部利害関係者との調整

すべての主要な利害関係者と外部サービスプロバイダーや法執行機関、法律顧問、インシデント対応リソースなど、ランサムウェア攻撃の社内外の緊急連絡先の最新リストを維持します。優先事項には、予知メッセージと、誤った情報の拡散を食い止める対策に関する相互の合意が含まれます。

➡レスポンスプランのテスト

レスポンスのテストは、各人がプランを実行する際の自己の役割と責任を確認するのに役立ちます。企業対策の準備が整っているほど、対応はより効果的になる可能性があります。

➡対応プランを更新

対応プランをテストする（そしてインシデント中に実行する）と、必然的に必要な改善が明らかになります。学んだ教訓で対応プランを更新することはベストです。これにより、将来ランサムウェア攻撃による被害の可能性が最小限に抑えられ、利害関係者間の信頼が回復します。

RECOVER

Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber-security event.

➡緊急時対応プランの立案

レスポンスと同様に、企業はシステム機能の復旧と脆弱性の修正をプランする必要があります。ランサムウェアイベントを回復させ、イベントのインパクトレベルを即座に判断し、関係者に通知するための手順に焦点を当てます。

➡内部および外部の利害関係者とのコミュニケーション

復旧は効果的なコミュニケーションにかかっています。復旧プランでは、ランサムウェアイベント情報がさまざまな利害関係者と共有され、すべての利害関係者が必要な情報を受け取るようにする必要があります。

➡広報と協力して企業の評判を管理

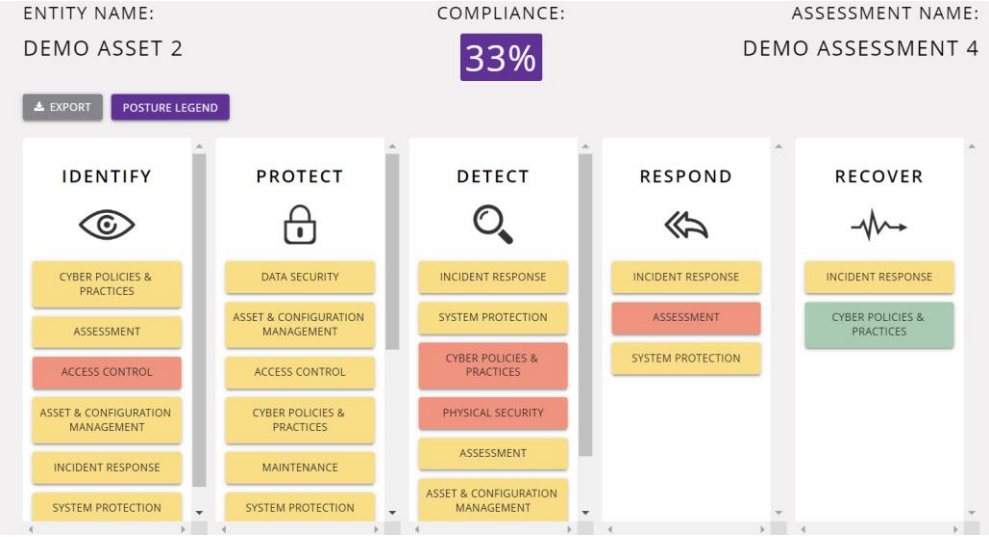
ランサムウェアの復旧計画を立てるときは、情報共有が正確、完全、かつタイムリーであり、反動的にならないように、広報をどのように管理するかを検討すべきです。

➡復旧プランのテストと更新

復旧プランをテストすることで、従業員とパートナーの意識が向上し、改善すべき領域が浮き彫りになります。

おわりに

国内でも今後、NIST 準拠によるサイバーセキュリティガイドが参照されると思われます。
SecurityGate が提供するポスチャマップ機能は、まさに NIST サイバーセキュリティフレームワークの 5 つの機能、つまり、識別、保護、検出、応答、および復旧のステータスを表示します。
Securitygate は、SecurityGate コントロールとさまざまなフレームワークの間のマッピングを絶えず更新して、NIST 機能に関連するサイバーセキュリティの洞察の全体像を提供しています。
そして、エンティティ（人、資産、施設等）およびアセスメントレベルで最新のアセスメントの結果に従って、新しいアセスメントが行われると、ポスチャマップは自動的に更新されます。
以下は SecurityGate に含まれるポスチャマップの一例です。



出典

Getting Started with Cybersecurity Risk Management | Ransomware

https://csrc.nist.gov/csrc/media/Publications/white-paper/2022/02/24/getting-started-with-cybersecurity-risk-management-ransomware/final/documents/quick-start-guide--ransomware.pdf

関連リンク

National Institute of Standards and Technology (NIST)

https://www.nist.gov/

Getting Started with Cybersecurity Risk Management: Ransomware

https://csrc.nist.gov/publications/detail/white-paper/2022/02/24/getting-started-with-cybersecurity-risk-management-ransomware/final

お問い合わせ窓口

株式会社テリロジー

グループ事業推進統括部 OT/IoTセキュリティ事業推進部

SecurityGate 担当 宛

製品に関するお問い合わせは当社のお問い合わせフォームからお寄せください

この資料は、National Institute of Standards and Technology (NIST)が公開しているホワイトペーパーの内容をもとにテリロジーが翻訳したものです。