サイバー回復力のあるデータ復元戦略の構築

目次

はじめに

今日のデジタルファーストの世界においてサイバーセキュリティは不可欠な要素です。サイバーセキュリティに関する最近のブログ記事やホワイトペーパーの多くがランサムウェアを取り上げているのも驚くことではありませんこうした脅威の話題はうんざりするものですが、ランサムウェアはあらゆる規模の組織にとって最大の脅威となっており、最も重要なインフラストラクチャと業界を標的としています。これはいたちごっこであり、新たな脅威が発生すると、セキュリティチームは適応して対応する必要があります。事業運営、政府機能、個人活動のデジタル化が普及したことで、オンラインで保存・送信される機密データの量が飛躍的に増加しています。残念ながら、この変化によりサイバー犯罪者の攻撃対象領域も拡大しており、堅牢なサイバーセキュリティ対策が不可欠となっています。

データ侵害やランサムウェア攻撃から国家による高度なサイバースパイに至るまで、サイバー脅威は、重要なインフラストラクチャの完全性、個人情報のプライバシー、さらには世界経済の安定に重大なリスクをもたらします。したがって、サイバー攻撃、主にランサムウェアの脅威は目の前にある明確な危機であるため、組織のあらゆる戦略の最前線にデータセキュリティを据える必要があります。残念ながら、2022年には85%の組織が少なくとも1回はランサムウェア攻撃を受けています[1]。さらに憂慮すべきは、今日のランサムウェア攻撃は単に組織によるデータへのアクセスを妨げるだけでなく、組織データの盗難、流出、販売、アーカイブも行っているという事実です。

サイバーセキュリティ計画では、こうしたデータに対する悪意のあるアクセスを防止することを最も重要な目標として捉える必要があります。ただし、いかなる組織も、その防御が常に維持されると想定するべきではありません。したがって、データを復元する能力を維持することも同様に重要です。ランサムウェアの影響を受けた組織は平均で15%の本番データを失っており[2]、適切に設計された信頼性の高いデータ復元計画を備えることの重要性を浮き彫りにしています。

効果的なサイバーセキュリティプラクティスとは、データへの不正アクセスから保護し、運用の継続性を確保して、消費者とサービスプロバイダーとの間の信頼を維持するものです。サイバー脅威の複雑さが高まり、その規模が拡大するにつれて、デジタル資産、個人のプライバシー、および国家セキュリティの保護におけるサイバーセキュリティの重要性はますます高くなっています。サイバーセキュリティは今日のデジタル社会のアーキテクチャにおける重要な柱であり、私たちがデジタル世界を安心してナビゲートし、イノベーションを推進してコミュニケーションを円滑に図れることを保証するものです。

NISTサイバーセキュリティフレームワーク（CSF）2.0の最近の更新[3]は、サイバーセキュリティの標準的なアプローチにおいて極めて重要な進化を示すものであり、より複雑化したデジタル脅威が蔓延している世界におけるパラダイムシフトを反映しています。

このホワイトペーパーでは、更新済みのNIST CSFフレームワークについて検証し、このフレームワークの実装においてVeeam Softwareが支援できる領域について説明します。

[1] https://go.veeam.com/wp-data-protection-trends-2024

[2] https://go.veeam.com/wp-data-protection-trends-2024

[3] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

NISTサイバーセキュリティフレームワークの背景

NISTサイバーセキュリティフレームワーク（CSF）は、サイバーセキュリティリスクを管理するための統一されたアプローチに対するニーズの高まりに対応して、2014年に初めて導入されました。このフレームワークは、米国国立標準技術研究所（NIST）が民間およびパブリックセクターの両方の組織と協力して開発し、情報システムの保護に役立つ一連の業界標準を組織に提供することを目的としていました。CSFは組織がサイバーセキュリティにおけるリスク管理について理解して改善できるように支援することを目的としており、これによって重要なインフラストラクチャのセキュリティと回復力も強化されます。

2024年2月にリリースされたNISTサイバーセキュリティフレームワーク（CSF）2.0は以前のバージョンに基づいて構築されており、サイバーセキュリティの状況の進化と、コミュニティから受け取ったフィードバックを反映したいくつかの重要な変更を導入します。

CSF 2.0は、重要なインフラストラクチャセクターだけにとどまらず、規模や種類にかかわらず全ての組織にメリットをもたらすように改定されたことで、より普遍的に適用できるガイドラインとなりました。

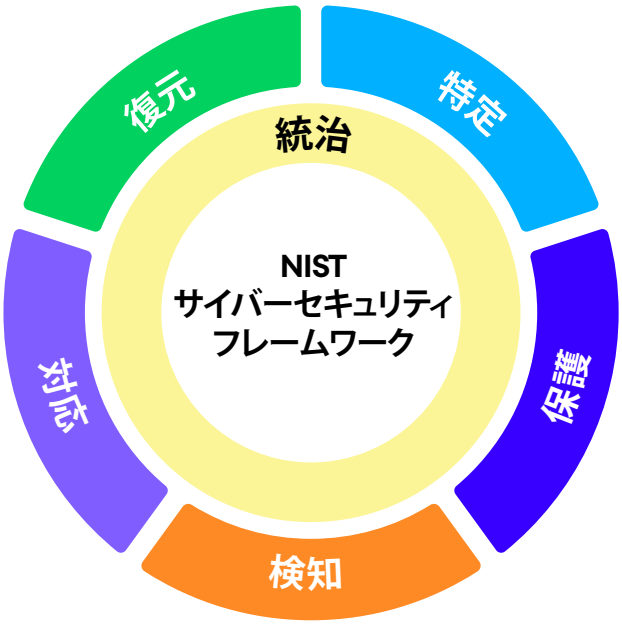

図1 — NISTサイバーセキュリティフレームワーク2.0

CSFの中核は6つの主要な機能を中心に構成されており、これらの機能を組み合わせることで、サイバーセキュリティリスクのライフサイクルに基づいた包括的な推奨事項を得ることができます。

- **特定：**組織のシステム、従業員、資産、データ、および能力に対するサイバーセキュリティリスクを管理するための組織的な理解を深めます。これには、重要なビジネスプロセスと主要な資産、およびそれらの脆弱性と脅威の特定が含まれます。
- **保護：**重要なサービスを確実に提供し、潜在的なサイバーセキュリティインシデントの影響を制限または封じ込めるための適切なセーフガードを導入します。これには、ID管理、アクセス制御、データセキュリティ、および保護テクノロジーが含まれます。
- **検知：**サイバーセキュリティインシデントの発生をタイムリーに特定するための対策を実施します。継続的な監視と脅威の検知がこの機能の重要な要素です。
- **対応：**サイバーセキュリティインシデントが検知された際に行動を起こします。これには、インシデント対応計画、分析、軽減、およびコミュニケーションが含まれます。
- **復元：**サイバーセキュリティインシデントによって損なわれた機能やサービスのリストアと復旧に関する計画を維持します。通常の運用へのタイムリーな復元が目標です。
- **統治（新機能）：**CSF 2.0のこの新機能は、サイバーセキュリティリスクの全体的な管理とガバナンスに焦点を当てています。組織はここで、役割と責任の定義や、エンタープライズリスク管理へのサイバーセキュリティの統合を含む、サイバーセキュリティリスク管理戦略、ポリシー、および監視を確立します。

この新しい「統治」機能は、説明責任と透明性という基本的な目標を高め、組織が他の5つの機能で示されている目標を優先して達成できるよう支援するための「統合力」として機能します。また、サイバーセキュリティが決して単独の懸念事項ではなく、エンタープライズリスクを構成する不可欠な一部であることも強調しています。特に、新機能の監視コンポーネントは、組織がITセキュリティに関する決断を下す上級管理職や取締役会の説明責任の強化を促すSEC規制などの規制フレームワークに準拠するのに役立ちます。

もともとの5つの機能「特定」、「保護」、「検知」、「対応」、「回復」は、明確さと関連性を高め、進化するサイバーセキュリティの脅威と慣行を反映するために保持され、更新されており、組織が動的なデジタル環境においてサイバーセキュリティリスクを効果的に管理し、軽減できるようになっています。ガバナンス関連の要素も、新しく作成された「統治」機能に移行されました。さらに、各機能の主な目的がより明確に述べられるようになりました。これらのタスクが連続的なものではなく、包括的なサイバーセキュリティ戦略における相互依存的な部分であると認識することで、この再編を通じて、よりまとまりのある連携的なサイバーセキュリティ対策が可能になります。

サイバーセキュリティのサプライチェーンリスク管理もますます重視される傾向にあり、組織の全体的なサイバーセキュリティプログラムにサプライチェーンリスク管理を統合することを目的とした新しい制御機能が登場しています。

このフレームワークのユーザーには、ユーザー固有のニーズに合わせてカスタマイズされた導入例[4]とクイックスタートガイド[5]も提供されるようになりました。これには、参照ツールを介してアクセスできる検索可能な参照カタログ[6]が含まれており、組織はこれによってガイダンスを50件以上もの他のサイバーセキュリティ関連文書にマッピングできます。

[4] https://www.nist.gov/document/csf-20-implementations-pdf

[5] https://www.nist.gov/quick-start-guides

[6] https://csrc.nist.gov/projects/olir/informative-reference-catalog#

主な変更点は次のとおりです。

1. CSF 2.0は、重要なインフラストラクチャセクター以外の領域にも適用できるようになりました。今回のフレームワークの改定は、ガイドラインの普遍的な関連性を高めることで、規模や業界に関わらず全ての組織にメリットをもたらすことを目的としています。

2. 「統治」機能の追加は、CSF 2.0における非常に重要な機能強化の一つです。この機能は、説明責任と透明性という中核的な目標を高めるとともに、組織が他の5つの機能で示されている目標を優先して達成できるように支援するための「統合力」として機能します。この機能は、サイバーセキュリティを単独の懸念事項として扱うのではなく、全体的なエンタープライズリスク管理に統合することを強調しています。「統治」機能の監視コンポーネントは、サイバーセキュリティに関連する決断を下す取締役会や上級管理職の説明責任の強化を促すSEC規制などの規制フレームワークを遵守する必要がある組織にとっては特に有用なものです。

3. サプライチェーンのリスク管理への関心の高まりも考慮されています。CSF 2.0は、サプライチェーンにおけるサイバーセキュリティリスクの管理をより重視するものとなっています。また、組織のサイバーセキュリティプログラム全体にサプライチェーンのリスク管理を統合するための新しい制御も導入されています。これは、パートナー、ベンダー、サービスプロバイダーのエコシステム全体を保護することの重要性を認識しています。

NIST CSF 2.0におけるこれらの機能拡張は、組織が複雑なサイバーセキュリティの状況をナビゲートするのに役立つ、より包括的で適応性の高いフレームワークを提供します。CSF 2.0では、範囲を拡大して「統治」機能を導入し、コア機能を更新してサプライチェーンのリスク管理にも焦点を当てることで、サイバーセキュリティ体制を強化して、進化する脅威に対して回復力を高めるために必要なツールとガイダンスを組織に提供します。

このフレームワークのユーザーには、ユーザー固有のニーズに合わせてカスタマイズされた導入例[7]とクイックスタートガイド[8]も提供されるようになりました。これには、参照ツールを介してアクセスできる検索可能な参照カタログ[9]が含まれており、組織はこれによってガイダンスを50件以上もの他のサイバーセキュリティ関連文書にマッピングできます。

[7] https://www.nist.gov/document/csf-20-implementations-pdf

[8] https://www.nist.gov/quick-start-guides

[9] https://csrc.nist.gov/projects/olir/informative-reference-catalog#

信頼性の高いデータの復元基盤

データの復元は、データのアベイラビリティ戦略の一環として、サイバーセキュリティ計画の最後の砦となることが多いため、慎重に検討して計画する必要があります。組織は、「3-2-1-1-0」のデータ保護戦略といったコンセプトを活用し、インフラストラクチャ全体にわたってデータをバックアップして、サイバーインシデント後にデータを健全な状態にリストアできる単一のツールを用意することで、いかなる状況でもデータを復元するための適切な段取りを整えることが可能になります。

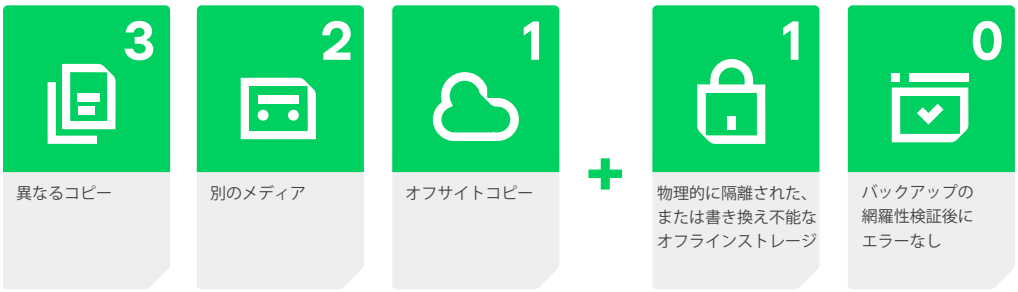

図2 — Veeamの3-2-1-1-0バックアップルール

Veeamのお客様は、Veeam Data Platformを使用することで、適切にオーケストレーションおよび文書化されたセキュアな方法でこの段取りを整えることができます。Veeam Backup & Replication、Veeam ONE、Veeam Recovery Orchestratorを含む完全なスイートにより、お客様はNISTサイバーセキュリティフレームワークのあらゆる段階に対応する、データのバックアップと復元以上のデータセキュリティ目標を達成できます。

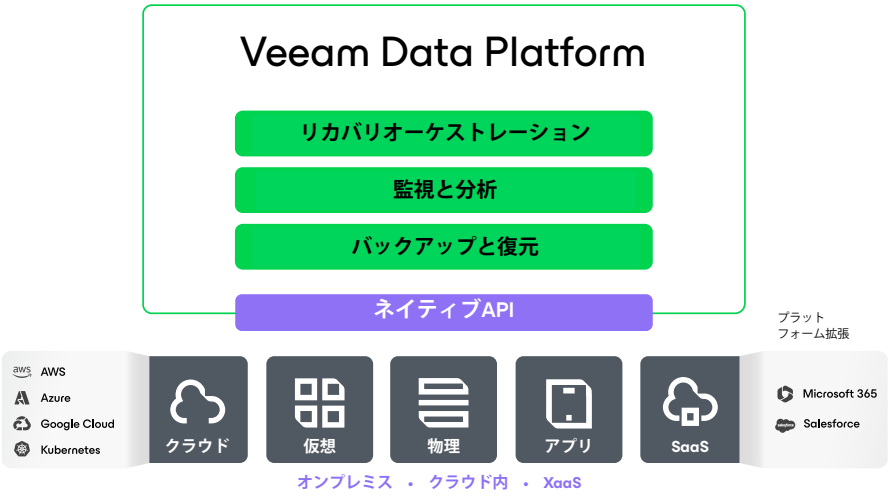

図3 — Veeam Data Platform

本書の残りの部分では、前述のNISTサイバーセキュリティフレームワークを取り上げて、IT組織、セキュリティチーム、意思決定者に、フレームワーク内でVeeam Data Platformを活用するために必要なインサイトと知識を身に付けていただくことを目的としています。また、重要なデータの特定、マルウェアの検知、データの保護、アクティブな脅威への迅速な対応、クリーンデータの迅速な復元に役立つ豊富な情報と機能を、これらの目標を達成するために使用できる主な機能を明らかにしつつ、皆様に提供したいと考えています。

NISTの「特定（ID）」機能

サイバーセキュリティの望ましい成果:

組織の現在のサイバーセキュリティリスクに関する理解。

サイバーセキュリティと従来の災害復旧またはディザスタリカバリ（DR）との間には、「**知らないものは保護できない**」という、核心的な共通する原則が存在します。保護を必要とする資産をカタログ化および分類することは、サイバーセキュリティの脅威に積極的に対抗して対応することに比べれば取るに足らないことのように見えるかもしれませんが、何がリスクにさらされているか、そしてその相対的な優先順位を知ることが第一歩になります。以下の機能を備えたVeeam製品は、重要なデータを**特定**するための多層的な戦略において必要不可欠な役割を担うことが可能です。

重要なシステムとデータのカタログ化

信頼性の高い復元計画を作成するには、ITチームとセキュリティチームが企業と緊密に連携し、組織全体に存在するすべてのワークロードとデータを特定、カタログ化、優先順位付けする必要があります。その起点としては、Veeam ONEで利用可能な各種レポートや、Veeam Backup & Replicationでバックアップされているシステムのカタログが適しています。重要なデータはすべてバックアップすべきであり、Veeamのソリューションでは保護されていない仮想マシン（VM）またはデータの有無を確認することができます。

同様に、セキュリティチームが使用するネットワークツールとセキュリティツールでも環境内のシステムのリストを作成できます。多くの場合、これらのシステムを比較することで、各ツール内でデータが適切に保護されていない場所を浮き彫りにして、保護・復元計画の完全性を可能な限り高めることができます。

タグ付けと分類によるデータの特定と優先順位付け

Veeam Backup & Replicationのタグ付け機能と分類機能を活用することで、既存のワークロード（そのバックアップ）のカタログを用いてタグを適用し、場所や所有者、復元の優先順位などのシステムメタデータを特定できます。こうすることで欠落しているデータを浮き彫りにし、データ保護におけるギャップを特定して、適切なデータ復元計画の構築に必要な主要メタデータを特定できる場合があります。

メタデータが適用されたら、Veeam Recovery Orchestratorのウィザード主導の復元計画立案機能を使用して復元計画を作成し、開発にかかる時間を短縮できます。その後、企業とともに追加の確認作業としてこの計画を見直し、ビジネス上のニーズに関する正確性と完全性を確保します。

自動復元テストを介したギャップと変更の表面化

緊急事態の発生時にバックアップや復元計画を使用する準備ができているかどうかを確認する最善の方法は、それらをテストすることです。Veeam Recovery Orchestratorの自動化されたテスト機能は、インフラストラクチャの一部またはすべてにおいて完全な復元力を確保するうえで大きなメリットをもたらします。テストの復元プロセスを自動化することで、テストの実行時における労力削減という明らかなメリットに加えて、テストの実行頻度を高め、欠陥をより迅速に検出できるようになります。

頻繁なテストを介して特定できる問題点の一つに、バックアップされていないシステム、または計画に含まれているシステムの存在があります。これらのテスト結果を定期的に見直してギャップを修復することで、保護する必要のある対象に関する組織の知識を向上できます。

NISTの「保護（PR）」機能

サイバーセキュリティの望ましい成果:

安全対策を導入して、資産の安全を確保しましょう。

バックアップインフラストラクチャは、あらゆるIT環境にとって特別な場所です。これは、データセキュリティにおける最後のセーフティネットを構成するだけでなく、本番環境で削除された可能性のあるデータなど、すべてのデータの複数のコピーが格納されている場所です（重要なデータであるほどコピーの数は増えます）。このため、バックアップインフラストラクチャは、身代金スキームと脅迫スキームの成功率を上げるためにデータを盗み出し、安全性を損なおうとするサイバー犯罪者の格好の標的となります。これが、バックアップインフラストラクチャ自体を**保護**することが非常に重要である理由です。

誰も信頼しないバックアップインフラストラクチャ

バックアップ保護の第一歩は、バックアップ管理システム自体への不正アクセスを防ぐことです。ゼロトラストの原則（明示的に検証する、侵害を想定する、最小特権アクセスを使用する）を適用して、バックアップインフラストラクチャへのラテラルムーブメント（横移動）をできるだけ困難にする必要があります。

マルチファクター認証（MFA）を使用し、独立した専用のデータ保護IDとアクセス管理（IAM）システムを導入することで、ユーザーとそのログイン情報が適切に検証され、侵害がより困難になります。また、管理者アカウントと運用アカウントを分けるなど、最小特権アクセスを実装することで、意図しないミスを防ぎ、特権昇格を最小限に抑えることができます。最後に、そのほか全てのインフラストラクチャがすでに侵害されていると仮定して、あらゆるものを構成する必要があります。これは、バックアップコンポーネントを分離されたネットワーク上に隔離し、VPNまたはリモート接続を介したVeeam Backup & Replicationコンソールへのアクセスを制限することを意味します。

これらのアプローチをバックアップインフラストラクチャの各レベルに組み込む必要がありますが、それぞれのレベルでアプローチが若干異なる場合があります。つまり、オペレーティング システム、ファイル共有、帯域外管理、およびそれらを管理するために使用されるすべてのアプリケーションも、同様の原則に従う必要があります。

バックアップインフラストラクチャ コンプライアンスの分析

お客様による「ゼロトラスト」原則の正しい適用を支援するために、Veeam Backup & Replicationコンソールには「セキュリティおよびコンプライアンスアナライザー」（旧称ベストプラクティスアナライザー）と呼ばれる組み込みユーティリティが備わっています。これによってVeeamインフラストラクチャが分析され、Veeamの推奨事項に従って導入されていない設定アイテムが報告されます。この分析は定期的に実行し、非準拠の各項目を修正または抑制する必要があります。抑止されたアイテムは、抑止したユーザーと日時とともに記録されます。修復が完了した後、分析を再実行し、結果を文書化する必要があります。

必要時に使えるバックアップの確保

今や、データを復元できないようにバックアップを削除することがランサムウェアの一般的な機能の一つとなっています。したがって、バックアップを変更または削除できないよう徹底することが極めて重要です。

イミュータビリティ（不変性）はコンピューターサイエンスの世界では非常に古くからあるコンセプトですが、最近では、特に保持要件を満たすために変更やエラーなしの状態で存続させる必要があるバックアップのための不可欠な機能となっています。強化リポジトリ、オブジェクトストレージ、サードパーティ 重複排除アプライアンス、テープのいずれを使用する場合も、管理者でさえデータを変更または削除できない状態でVeeamバックアップを保存できます。あらゆるセキュリティシステムの場合と同様に、たいていは対応策が存在するため、こうした対応策がスタック全体（データセンターに至るまでの全て）で排除される、または緊密に制御されるよう徹底することが極めて重要です。

サイバーセキュリティの世界では、最も安全なシステムは、電源をオフにし、ネットワークから切断し、誰もアクセスできない部屋に保存するシステムである、という古いジョークがあります。このジョークは完全に正しいことを言っていますが、実際にはアクセスできないシステムに存在価値はありません。ただし、この格言は、バックアップセキュリティに関しては非常に正しいものです。必要なときにアクセスできるのであれば、オフラインで保存されているバックアップは改ざんされるリスクが最も低くなります。Veeamでは、異なる認証を必要とするオンラインシステムから、究極的なオフラインストレージであるテープに至るまで、バックアップを保存するための物理的に隔離されたアプローチを実現するうえで、複数のオプションを用意しています。

一方で、いかなる計画も絶対に単一層の保護だけに頼るべきではありません。そのため、Veeam Backup & Replicationではバックアップの削除に対してFour-Eyes認証を取り入れています。旧来の「核ミサイルの鍵」アプローチと同様、この設定では、バックアップの削除を認可するために2人の管理者を必要とするため、意図せぬ削除や悪意のある削除からバックアップを保護することができます。

独自のバックアップの暗号化

データを窃取後に不正使用から保護するために、Veeamではバックアップを暗号化して、Veeamインフラストラクチャの外部から誰かがバックアップにアクセスできないよう保護できます。これでデータがランサムウェアを介して取得またはロックされるのを防ぐことはできませんが、データが恐喝スキームの手段として使用される可能性が非常に低くなります。この暗号化は、Veeam内部で管理することも、サードパーティのキー管理システム（KMS）に結び付けて、これらのキーの管理をオフロードして一元化することもできます。

サイドバー：ゼロトラストセキュリティモデル

ゼロトラストの目標は、境界セキュリティ内に従来存在していた本質的な信頼を排除することで、脅威が環境内を簡単に移動する能力を抑えることにあります。「決して信頼せず、常に検証する」というモットーを厳格に採用することで、ファイアウォールがサイバー脅威を必ず阻止するという前提に囚われない、「境界のないセキュリティモデル」を実現できます。このモデルでは、全てのシステムで全ての新しい相互作用を検証する必要があり、それらが安全であるという前提は適用されません。ゼロトラストセキュリティモデルの3つの原則は次のとおりです。

1. **明示的に検証する。**

2. **最小特権アクセスを使用する**

3. **侵害を想定する**

NISTの「検知」機能

サイバーセキュリティの望ましい成果:

サイバーセキュリティイベントを特定するための適切な対策を策定および導入する。

システムとデータの状況を完全に把握したら、これらの資産への侵入を迅速に検知するための計画とシステムを確立する必要があります。迅速な検知により、金銭の損失につながる可能性のある潜伏期間と脅威の影響を大幅に軽減できます。ここでもまた、Veeamはサイバー脅威を**検知**するための多層的な戦略における主要な構成要素となります。

異常な行動に関する注意喚起

マルウェアに対する重要な戦略の一つは、特権昇格を得て環境内を横方向に移動（リテラルムーブメント）しながら検知を回避し、できるだけ多くのシステムに感染することです。これを実現するために、マルウェアでは、ユーザーに気付かれないように一度に小さな変更のみを行います。また、身代金を要求するのに必要なデータを復元する機能を妨害する手口もより巧妙になり、バックアップを削除したり、バックアップ保持時間を短縮したり、バックアップジョブを無効化したりするようにもなりました。Veeamは、Veeam ONEの複数のアラームとレポートを介してこの種の異常な行動を特定し、アラートを通知できます。

バックアップ時のマルウェアのスキャン

Veeam Backup & Replicationでは、インラインマルウェア検知機能を利用することで、Veeamプロキシノードを通過するブロックを分析し、アクティブなマルウェアの主な指標である新しい暗号化の兆候を見つけることができます。バックアップインデックスの検索に基づき、悪意のあるファイル名と署名が検知されて疑わしいものが見つかった場合は、このバックアップは「疑わしいもの」としてフラグが付きます。

バックアップ内のマルウェアの検知

Veeam Backup & ReplicationのSureBackup機能は本来、バックアップのリストアと検証を自動化して、それらがリストア可能であることを確認することを目的として設計されました。エンドポイント保護ソフトウェアは完璧ではなく、バックアップへのマルウェアの侵入につながる可能性があるため、SureBackupには、マルウェアに関してバックアップをチェックできる一連の堅牢な機能も用意されています。

リストア可能性テストの一環として、SureBackupはマルウェアスキャンツールと連携して、リストアした仮想マシン（VM）をスキャンすることもできます。これにより、組織は、検知に対して「信頼するが検証する」というアプローチでセカンダリマルウェア検知ツールを使用できるようになります。付加的なメリットとして、SureBackupのスキャンは、本番ワークロードに影響を及ぼすことなく実行されるため、より全体的なスキャンが可能になる場合があります。また、SureBackupでは、個別のディスクをテストマシンにマウントし、そのマシンでファイルをスキャンすることでマルウェアの存在を確認することもできます。このため、完全なリストアが必要ないときには、より一層高速でリソース効率の高いマルウェアスキャンを実行できます。

これらのスキャンで何か見つかった場合は、疑わしいものとして、その特定のリストアポイントにフラグが付けられます。

侵害を検出するための定期的な復元計画テスト

繰り返しになりますが、復元計画の定期的なテストは、マルウェアによって引き起こされた損失を浮き彫りにするうえで役立ちます。完全な復元計画テスト（アプリケーションの検証を含む）中の障害により、主要なファイルが暗号化された、または設定ファイルが不適切に変更された領域が判明する場合があります。これは、起動シーケンス中に実行されるマルウェアを検出するのに特に役立ちます。

一元的なログレポートの作成と相関関係

ログファイルを外部syslogサービスに送信することで、ログのセカンダリリポジトリを確保し、システム間でのイベントの相関関係を確認可能にする一元化を実現できます。これは、大半のセキュリティチームにとって、セキュリティインシデントおよびイベント管理（SIEM）システムのプライマリ機能となります。SIEMシステムをSyslogターゲットとして設定することで、Veeamが検出した侵害の痕跡をシステム内で直接フラグ付けできるため、対応時間が短縮され、セキュリティアナリストはイベントをより確実に把握できるようになります。

データ保護のための外部統合

インシデントAPIとは、サイバーセキュリティツールが感染をバックアップインフラストラクチャに通知し、バックアップを「疑わしいもの」または「感染しているもの」としてフラグ付けする際に使用できる一連のアプリケーションプログラミングインターフェイス（API）です。Veeam Backup & Recoveryは、この情報に基づいて管理者に注意を喚起するように設定できます。これにより、管理者は、即時バックアップの作成、感染の有無のチェックまたはクリーンファイルの復元のためのSureBackupアクションの実行、フォレンジックを目的としたイミュータブル（書き換え不能）なバックアップコピーの作成などのアクションを介して迅速に確認、検証、対応できるようになります。コアセキュリティツールとデータ保護プラットフォーム間のこのオープンな統合ポイントによりコミュニケーションが大幅に向上し、マルウェアの潜伏期間を短縮して、復元をより迅速かつクリーンに行えるようになる可能性が生まれます。

サイドバー：潜伏期間

潜伏期間（マルウェアが検出されるまでに環境内にとどまる期間）は、マルウェアがプライマリ攻撃を実行せずに環境内に存在する期間です。マルウェアはこの時間を利用して、別のアカウントの侵害、特権昇格、オペレーティングシステム内のより深い場所への侵入または自身の埋め込み、その他のシステムへの横方向の拡散（リテラルムーブメント）、現在または今後の攻撃に利用できるインテリジェンスの収集を行う可能性があります。

NISTの「対応」機能

サイバーセキュリティの望ましい成果:

検知したサイバーセキュリティイベントに適した対応を策定および導入する。

常に100%保護することは不可能であるため、マルウェアを食い止め、できるだけ早く削除することに集中する必要もあります。自然災害からの復元計画のように、あらゆる意思決定において整合性を維持しなければならない主な目標の一つが「目標復旧時間（RTO）」です。サイバーセキュリティイベントに対しても、マルウェアを食い止めて環境から削除し、システムを稼働状態に戻すことができるようにすることに焦点を当てた、非常によく似た目標があります。マルウェアが潜伏してデータを窃取する期間を短縮できれば、クリーンアップにかかる労力を軽減して復旧時間を短縮できます。これが、迅速に**対応**するための準備が極めて重要な理由です。

サイバーフォレンジック用のバックアップの使用

前述のとおり、SureBackupバックアップはバックアップの復元可能性をテストするだけでなく、マルウェアも検知できる機能です。「対応」フェーズの目標の一つに潜伏期間を特定することがあります。リストアポイントでマルウェアが検知されたかどうかや、サードパーティ製ツールで検知されたかを示す、Veeam Backup & Replicationのマルウェアフラグを利用することで、最初の感染ポイントを見つけるための作業が容易になります。

「セキュアなリストア（SecureRestore）」は、完全なリストアを行う前にディスクをマウントしてマルウェアの有無をスキャンできる、Veeam Backup & Replicationの別の機能です。感染していないポイントが発見されるまでこのプロセスを反復すると、指定したシステムでマルウェアが最初に出現した時点を見つけ出すとともに、潜伏中のマルウェアの一部をリストアすることで再感染を回避することがより容易になります。

Veeam Recovery Orchestratorを使用すると、オーケストレーションされた「クリーンルーム」アプローチにより、環境全体でこの「セキュアなリストア」プロセスを実行できます。これにより、クリーンなリストアポイントをチェックするための時間が短縮されるだけでなく、サイバーセキュリティインシデントのデジタルフォレンジックに価値ある情報が迅速に追加されます。

YARAを使用した高度な脅威ハンティング

サイバーセキュリティの脅威ハンターにとって馴染みのあるツールであるYARAは、マルウェアを特定して分類するためのルールベースのアプローチです。SureBackupまたはSecureRestore操作の一環として、マルウェアの初期分類とバックアップ全体にわたるマルウェアの検索の両方において、YARAルールを特定して実行することができます。

ServiceNowを使用したインシデントの追跡

Veeam ONEでは、ServiceNowに直接統合することで、状況の進展に伴って新しいケースの作成や既存のケースの更新を自動的に行うことができるため、異なるチーム間でのより効率的なやり取りを支援したり、インシデント履歴のより自動的な文書化を実現したりできます。

サイドバー：窃取

マルウェアによってデータにアクセスされて改ざんされた場合は、まず最初にそのデータが盗まれていた可能性があります。窃取されたデータとは、被害者の環境からサイバー犯罪者に送信されたデータを指します。こうしたデータは侵害後にサイバー犯罪者によって公開または販売され、企業秘密の漏洩や評判の失墜、個人情報の盗難を引き起こし、さらには将来の詐欺やサイバー攻撃にもつながる可能性があります。

NISTの「復元」機能

サイバーセキュリティの望ましい成果:

サイバーセキュリティイベントから復旧するための適切なアクティビティ（計画、プロセス、人材、テクノロジー）を開発して導入する

サイバーセキュリティインシデントの性質によっては、特にランサムウェアの場合、クリーンデータをリストアすることがサービスをリストアするうえで極めて重要になります。潜伏期間が長い場合は、多くの復元ポイントにマルウェアが侵入している可能性があり、時間を大きく遡ってクリーンなリストアポイントを見つけなければならないことがあります。従来のDRと同様に、データ消失を最小限に抑えた目標、つまり「目標復旧時点（RPO）」に揃えることが重要です。対応フェーズでは感染の開始時期を発見することが重要であるため、これらの作業の多くはデータの**復元**作業と並行して行われます。

バックアップが役立つのはリストア可能である（かつマルウェアを含んでいない）場合のみ

SureBackupやインシデントAPIなどの機能によって、「検知」段階と「対応」段階で疑わしいまたは感染しているリストアポイントにフラグを立てることにより、Veeam Backup & Replicationコンソール内で、それぞれのリストアポイントでマルウェアが検知されたかどうかを容易に特定できるようになります。これは優れた開始点ですが、以前のリストアポイントが完全にクリーンであることが保証されるものではありません。

感染したデータを復元して労力を浪費する可能性を減らすために、復元は対応フェーズで行ったサイバーフォレンジックと組み合わせて行う必要があります。適切なデータをリストアし、マルウェアを再度持ち込まないようにするには、IT部門、セキュリティ部門、ビジネス全体の強力な連携が不可欠です。

SureBackupやセキュアなリストアの一環として最新のマルウェア検知ツールを使用した際に、以前は検知されなかったマルウェアが古いリストアポイントで見つかる可能性があるため、以前のスキャンで設定されたマルウェアフラグのみに頼らないことが重要です。クリーンなリストアポイントが定義済みのRPOよりはるかに前の時点である場合は、ファイルレベルのリストアを使用して、主要データの個々の部分をリストアすると同時に、フルバックアップ内に潜むマルウェアを回避できます。

感染していないデータをいち早くリストア

自動化はシンプルな環境の復元においても重要になる要素ですが、リストアのモードによっても違いが生まれる場合があります。「ストレージアレイ」スナップショットとインスタント復元を利用することで、リストアされたバックアップをほぼ瞬時に使用できるようになります。

Veeam Recovery Orchestratorは、リストアプロセス全体を規定し、ボタンのワンクリックだけで簡単に実行できるように設計されています。Veeamでは、リストア計画と、感染フラグ、セキュアなリストア、ストレージアレイスナップショット、インスタント復元、アプリケーション検証とを組み合わせることで、データを迅速かつ効率的にリストアすると同時に、データをできるだけマルウェアが存在しない状態に保つ機能を組み合わせて提供しています。

I/Oの異常の可視化

場合によっては、トレンドを浮き彫りにするうえで視覚的なグラフより優れたものは存在しません。Veeam Backup & Replicationのユーザーインターフェイスでは、レプリケーションジョブから復元する際に、大規模な暗号化が開始された時点を特定するうえで役立つグラフが提供され、暗号化前の時点を見つけるための労力を削減できます。

サイドバー：サイバーセキュリティの復元のためのバックアップとレプリケーション

レプリケーションはサイバーセキュリティ復元計画の一環である場合がありますが、バックアップと比較したレプリケーションの目標を理解することが重要です。レプリケーションは、データをできるだけ迅速に移動し、最新の優れたレプリカに戻すことに焦点を当てています。バックアップは継続的ではないため、クリーン性とリストア可能性を確保する際により体系的になる可能性があります。サイバーセキュリティの復元を潜伏期間とリストアポイントのクリーン性に基づいて行うことで、バックアップをより一般的なメカニズムにする必要があります。

NISTの「統治」機能

サイバーセキュリティの望ましい成果:

組織のサイバーセキュリティリスク管理戦略、期待事項、ポリシーが確立されて伝達され、監視される。

「統治」機能の導入は、サイバーセキュリティ戦略と監視における重大な進化を表しています。この新しい機能は、組織全体のサイバーセキュリティリスクを管理するうえでのガバナンスの重要性を強調しています。また、組織の全体的な目標とリスク許容度に沿った明確なサイバーセキュリティポリシー、戦略、およびプロセスを確立する必要性も強調しています。NIST CSF 2.0では、「統治」機能を統合することで、組織がサイバーセキュリティに対してより包括的で説明責任のあるアプローチを採用し、サイバーセキュリティ関連の考慮事項が組織の統治構造に織り込まれることを推進しています。これには、サイバーセキュリティの役割と責任の定義、セキュリティ意識の文化の醸成、サイバーセキュリティに関する意思決定が組織の目標と制約に基づいて行われるようにすることが含まれます。この機能の追加は、サイバーセキュリティを単なる技術的な課題としてではなく、ビジネス管理と運用の回復性の重要な要素として認識する傾向にあることを浮き彫りにしています。

データセキュリティの重要な要素であるバックアップインフラストラクチャは、企業や政府の規制に明確に準拠するものである必要があります。適切な「**統治**」には、設定とポリシー、変更の追跡、すべてのテスト結果の文書化など、組織のサイバーセキュリティリスク管理戦略の文書化が含まれます。これにより、期待とポリシーが効果的に伝達され、監視されます。

すべてが文書化されることの確認

監査、サイバー保険、プロセス改善、自己保証のいずれの目的であっても、正確で徹底した頻繁な文書化の重要性を過小評価してはいけません。完全にオーケストレーションされた復元計画の正確性とスピードは管理者とビジネスオーナーにとって最も価値あるものですが、完全実行またはテスト実行のたびに行われる動的な文書化は、セキュリティチームやコンプライアンスチームなど、実際に機能したことの証拠を必要とするあらゆるチームにとってさらに大きな価値をもたらします。

さらに、Veeam ONEから作成できる多数のレポートによって、バックアップインフラストラクチャとその正常性に関する豊富な情報が提供されます。バックアップ頻度の文書化や、バックアップ設定の変更の追跡などは、スケジュール設定または手動で生成し、適切な受信者に自動的に送信できる組み込みのレポートです。

リスクを最小限に抑えるための常時モニタリング

自動化を利用してVeeamの設定やバックアップ環境をチェックし、お使いのデバイスやソフトウェアが安全で最新の状態であることを確認します。Veeamのセキュリティおよびコンプライアンスアナライザーを使用すると、30以上ものセキュリティチェックが自動的に実行され、最新の状態であること、パッチが適用されていること、そして安全でない古いプロトコルが無効になっていることが確認されます。さらに、これらの情報はすべて単一のレポートにまとめられるため、セキュリティチームとITチームは組織のポリシーへの準拠状況を追跡できます。

バックアップ セキュリティ ダッシュボード

多くの場合、サイバーセキュリティは環境全体でパターンを見つけることを意味します。Veeamでは多岐にわたる機能を提供しており、サイバーセキュリティに焦点を当てたさまざまな新機能が含まれています。たとえば、Veeam脅威センターダッシュボードでは、管理者やセキュリティ専門家は、複数のデータソースをVeeam ONEのインターフェイスに集約する統合画面を通じて、バックアップインフラストラクチャ全体を一元管理することができます。

結論

NIST CSF 2.0は、サイバーセキュリティリスク管理の進展と、進化し続ける脅威との闘いにおける重要なマイルストーンを示すものです。CSF 2.0は、CSF 1.1の強固な基盤の上に構築され、「統治」機能やサプライチェーン重視などの主要な機能拡張を導入することにより、刻々と変化するサイバーセキュリティの状況をナビゲートするのに役立つ、より包括的で適応性の高いフレームワークを組織に提供します。

CSF 2.0の範囲が拡大されたことで、あらゆる規模とセクターの組織がCSF 2.0のガイダンスの恩恵を受けることができ、サイバーセキュリティに対するより包括的で協力的なアプローチが促進されます。更新されたこのフレームワークでは、効果的なサイバーセキュリティリスク管理には、上級管理職から最前線の従業員に至るまで、組織全体の利害関係者の積極的な関与とコミットメントが必要であることも示されています。

結局のところ、NIST CSF 2.0の実装が成功するかどうかは、サイバーセキュリティの意識、コラボレーション、説明責任の文化を育むかどうかにかかっています。トレーニングや教育プログラムに投資することで、組織は従業員がサイバーセキュリティリスク管理プロセスに積極的に参加できるように力を与えることができます。責任感と警戒感を共有するには、明確なコミュニケーションとサイバーセキュリティポリシーとベストプラクティスの一貫した強化が不可欠です。

今後、サイバーセキュリティが世界中の組織にとって重要な優先事項であり続けることは明らかです。サイバー脅威の巧妙化と頻度の増加、そしてデジタル技術への依存度の高まりが相まって、NIST CSF 2.0のような堅牢で俊敏なサイバーセキュリティフレームワークの必要性が浮き彫りになっています。この更新されたフレームワークを受け入れ、継続的な実装にコミットすることで、組織は回復力を強化して資産を保護し、進化するサイバーリスクに直面しても利害関係者の信頼を維持できるようになります。

近年、サイバーセキュリティプログラムを構築することは簡単なタスクではありません。脅威は数が非常に多く、犯罪者にとって侵害の価値は潜在的に非常に大きいため、組織は利用可能なツールをすべて使用して階層型のセキュリティを構築し、NISTサイバーセキュリティフレームワークのあらゆる段階で効率を最大限に高めることができるようにする必要があります。VeeamはNISTサイバーセキュリティフレームワークのあらゆる段階に価値を提供し、あらゆる組織のサイバーセキュリティプログラム全体の改善を目指しています。

- 復元計画を作成して定期的にテストすることで、特定フェーズで使用できる貴重なデータを得られる場合があります。これを利用して、重要データを**特定**して確実に保護することができます。
- 文書化されたベストプラクティスとネイティブのセキュリティ機能を導入することで、**保護**フェーズでバックアップとバックアップインフラストラクチャに確実に対処できるようになります。
- バックアップはインフラストラクチャ全体にわたるすべてのデータにかかわるため、**検出**段階でのエンドポイント観測で見逃された可能性があるマルウェアに対するセカンダリチェックとしても機能する場合があります。
- さまざまな時点や仮想の「クリーンルーム」環境への迅速なアクセスは、**対応**フェーズでの情報収集に不可欠な要素です。
- リストア可能でマルウェアが存在しないことが実証されたバックアップが必要な際に利用可能になり、**復元**フェーズをサポートするために、クリーンで使用可能な状態にできるだけ迅速にリストアできるようになります。
- 組織とそのデータの保護には、全員がそれぞれの役割を果たす必要があります。**統治**フェーズでは、組織のサイバーセキュリティ戦略とポリシーを確立して伝達し、監視することが重要です。

ITチームがリストア可能なデータを単に管理するだけの存在ではなく、サイバーセキュリティ計画に積極的に参加するときが来ました。本書のガイダンスを参考にすることで、ITチームはサイバーセキュリティチームやビジネスの利害関係者との建設的な会話を促進できるようになり、Veeamベースのデータ保護プラットフォームをサイバーセキュリティプログラム全体に統合できるようになります。

Veeamが提供する機能の詳細については、弊社までお問い合わせください。

Veeam Softwareについて

Veeamは、データ保護とランサムウェアからの復元におけるNo.1のグローバルマーケットリーダーとして、ハイブリッドクラウド向けのデータセキュリティ、データの復元、データの自由を通じて、あらゆる組織の根源的な回復力の確立と強化をご支援することをミッションに掲げています。米国ワシントン州シアトルに本社を置き、30ヶ国以上に事業拠点を構えるVeeamは世界中で45万社以上のお客様に保護を提供しており、お客様からはビジネス継続性について多大な信頼をお寄せいただいています。詳細については、www.veeam.com/jpをご覧になるか、LinkedIn（@veeam-software）およびX（@veeam）でVeeamをフォローしてください。

→ Veeam Data Platformのデモを見る

→ 30日間無償でお試しください