cpl.thalesgroup.com

THALES
Building a future we can all trust

ランサムウェア攻撃を防ぐタレスソリューション

NISTサイバーセキュリティフレームワークおよびランサムウェア防御ガイダンスに対するタレスソリューション

ランサムウェア攻撃は長年続いている問題ですが、最近では重要インフラから病院や小売業者まであらゆる対象を標的に数千万ドルの身代金を要求するなど、より被害が拡大しています。今日、注目を集めるサミットで世界の首脳がこれらの攻撃について議論しているように、政府機関は、企業や組織が攻撃から身を守れるように、教育やリソースの提供において積極的な役割を果たしています。

ランサムウェア攻撃の防御に関するNISTガイダンス

米国国立標準技術研究所（NIST）の一部であるNational Cybersecurity Center of Excellence（NCCoE）は、ランサムウェアから守るべき資産の特定と保護に関するガイダンスを発表しました。サイバーセキュリティ特別刊行物（SP）1800-25は、資産の保護に関する包括的な戦略を立てるための手順を説明しています。また、ランサムウェアの脅威に対処する特効薬がないことも示しています。

ランサムウェアを防ぐタレスソリューション

ランサムウェアから組織を保護するためにNISTが提唱するサイバーセキュリティフレームワークには、必要不可欠な要素があります。タレスのデータセキュリティおよびアクセス管理ソリューションは、そのいくつかを提供しています。タレスの業界をリードするソリューションは、以下を実現できる機能を組織に提供します。

- 機密データを発見し、リスクに応じて分類する
- 強力なアイデンティティおよびアクセス管理制御を実装する
- 暗号化とトークン化によって保存中および転送中の機密データを保護および制御する
- インテリジェントな修復のためにデータセキュリティを監視する

以下に、タレスソリューションがNISTサイバーセキュリティフレームワークおよびランサムウェアガイダンスにどのように対応するかの概要を示します。

NISTサイバーセキュリティフレームワークおよびランサムウェアガイダンスに対応するタレスソリューション

カテゴリ	要件	タレスソリューション
特定	ID.RA-1: 資産の脆弱性を特定し、文書化している。	**CipherTrust Data Discovery and Classification** は、クラウド、ビッグデータ、従来のデータストア全体にわたり、構造化および非構造化両方の規制対象となる機密データを特定します。「single pane of glass（単一のユーザーインターフェイス）」で機密データとそのリスクを把握できるため、セキュリティギャップの解消、修復アクションの優先順位付け、クラウド変換とサードパーティのデータ共有の保護について、より適切な意思決定が行えます。
リスク評価(ID.RA)	PR.AC-1: 認可されたデバイス、ユーザー、プロセスに対して、アイデンティティとクレデンシャルを発行、管理、検証、無効化、監査している。 PR.AC-3: リモートアクセスを管理している。 PR.AC-4: 最小特権と職務分掌の原則を取り入れて、アクセス許可と認可を管理している。	**SafeNet Trusted Access はアクセス管理の一元化を実現します。そのため**オンプレミス、クラウドベース、仮想化を問わず、幅広いリソースを保護しながら、分散したトークン資産の展開と管理を自動化および簡素化して、プラットフォーム全体で一貫した認証ポリシーを追求できます。 **また、SafeNet Trusted Accessは、商用オフザシェルフの多要素認証により**、幅広い認証方式とフォームファクタを提供します。これにより、クラウドまたはオンプレミスで提供される1 つの認証プラットフォームから管理される一元管理された統合ポリシーによって、多数のユースケース、保証レベル、脅威ベクトルに対応できます。 **CipherTrust Transparent Encryptionは、ビジネスクリティカルなデータに対するきめ細かいアクセス制御**を提供します。特定の保護されたファイル/フォルダにアクセスできるユーザーと、ユーザーが実行できる操作を定義します。 • 管理ユーザーが自分の特権を悪用して機密ファイルやデータベースへの読み取りアクセスを取得するのを防ぎます。 • ックアップアーカイブに関する厳格なアクセス制御ポリシーを設定し、データ漏洩を防ぐためにバックアップを暗号化します。 • データベースユーザーが読み取り/書き込みアクセスを許可されるのに対し、バックアップソフトウェアは同じデータベースへの読み取りアクセスのみを持つように、職務分掌を実装します。

カテゴリ	要件	タレスソリューション
保護 データセキュリティ (PR.DS)	PR.DS-1: 保存データを保護している。	**The CipherTrust Data Security Platform** は、鍵を一元管理し、データの検出、分類、データ保護、そしてこれまでにないきめ細かいアクセス制御をすべて、単一のプラットフォーム上で実現します。これにより、データセキュリティの運用にかかるリソースを削減し、ユビキタスなコンプライアンス管理を実現して、ビジネス全体のリスクを大幅に減少させます。 • **CipherTrust Transparent Encryption** は、既存のアプリケーションに変更を加えることなく、保存データの暗号化、特権ユーザーアクセス制御、詳細なデータアクセス監査ログを提供します。これにより、ポリシーを設定して不正なプロセスや許可されていないユーザーによって機密性の高いデータが暗号化されるのを防止し、機密データの漏洩を防ぐことで、ランサムウェア攻撃から組織を保護します。エージェントは、クラウドおよびビッグデータ環境の物理サーバーと仮想サーバー全体にわたり、Windows、AIX、Linux OS上のファイル、ボリューム、データベースのデータを保護します。 • **CipherTrust Application Data Protection** は、APIによる鍵管理、署名、ハッシュ、暗号化サービスなどの暗号化機能を備えており、アプリケーションサーバーまたはビッグデータノードのデータを容易に保護できます。 • **CipherTrust Tokenization** は、Vaultless（トークンボルトなし）のトークン化とVaulted（トークンボルトあり）の両方が用意されており、PCI DSSなどのデータセキュリティ要件を遵守するコストと複雑さを軽減できます。 • **CipherTrust Database Protection** ソリューションは、データベース内の機密フィールドのデータ暗号化を、安全で一元化された鍵管理と統合します。データベースアプリケーションの変更は不要です。CipherTrust Database Protectionソリューションは、Oracle、Microsoft SQL Server、IBM DB2、Teradataデータベースをサポートしています。 • **CipherTrust Manager は、プラットフォームの中央管理ポイントです。** これにより、暗号鍵を一元管理し、きめ細かなアクセス制御を提供して、セキュリティポリシーを策定することができます。暗号鍵の生成、ローテーション、破棄、インポート、エクスポートなどのライフサイクルタスク管理、暗号鍵とポリシーへの役割ベースのアクセス制御、強力な監査とレポート作成のサポート、さらに開発者にとって使いやすいREST APIを提供します。CipherTrust Managerは、FIPS 140-2（Level 3まで）に準拠した仮想フォーム **Luna Hardware Security Modules** は、機密データや重要なアプリケーションの保護に使用される暗号鍵を生成、保管、保護、管理します。米国サプライチェーンに対する政府の要件を満たす、高保証、耐タンパ性のLuna HSMは、米国で設計、開発、製造、販売、サポートされています。 Thales Luna HSMは、公開鍵基盤（PKI）を含む既存および新興技術の信頼の基点を提供し、コードの整合性を維持するためにコード署名用の鍵を安全に保管します。またタレスは、オンプレミス、クラウドHSMサービス、ハイブリッド環境で利用可能な、Luna HSM、コンテナ、REST APIを基盤とするエンタープライズ向けのカスタム仕様のコード署名ソリューションも提供しています。 **Data Protection on Demand (DPoD)** は、シンプルなオンラインマーケットプレイスを通じて、さまざまなクラウドHSMおよび鍵管理サービスを提供するクラウドベースのプラットフォームです。

カテゴリ	要件	タレスソリューション
保護 データセキュリティ(PR.DS)	PR.DS-2: 転送中データを保護している。	**Thales High Speed Encryptors** 企業や政府機関にとって理想的な、移動中データ(時間が重要となる音声およびビデオストリームを含む)を保護する認定された実証済みのソリューションを提供します。 • CNシリーズのネットワーク暗号化装置は、転送中データのためにネットワーク層に依存しない(レイヤー2、3、4)暗号化を提供するハードウェアネットワークアプライアンスです。これらのハードウェア暗号化装置は、FIPS140-2 Level 3、コモンクライテリア、NATO、DoDIN APLの認定を受けています。 • CVシリーズは、ネットワーク機能仮想化(NFV)を使用して、高速キャリアWANおよびSD-WANリンク全体における、移動中データに対する強力な暗号化を提供する強固な仮想アプライアンスです。
対応(RS) 緩和(RS-MI)	RS.MI-3: 新たに特定された脆弱性に関して、許容できるリスクである場合にはその旨を文書化し、そうでない場合には緩和している。	**CipherTrust Intelligent Remediation** は、リスクベースの機密データ検出とポリシーベースの透過的暗号化を統合して、データ漏洩のリスクを自動的に緩和します。これにより、ビジネスリスクを視覚化し、ランサムウェア攻撃から保護するための修復アクションを自動化できます。 **SafeNet Trusted Access** すべてのシステムへのあらゆるアクセスイベントについて即座に最新の監査証跡を提供することで、組織がランサムウェアのリスクに対応して緩和できるようにします。広範な自動レポートは、アクセスの実施と認証に関するすべての側面を文書化します。さらに、このサービスはログを外部のSIEMシステムに自動的にストリーミングします。

NISTのサイバーセキュリティフレームワークを満たす包括的なソリューションセット

タレスソリューションは、NISTサイバーセキュリティフレームワークで最も重要な機能のいくつかを提供しますが、一つの企業のみでNISTの要件を満たす真に包括的なソリューションセットを提供することはできません。そのためタレスは、世界をリードするテクノロジープロバイダーである400社以上のパートナーと提携して、NISTのサイバーセキュリティフレームワークを満たすための包括的なソリューションと統合セットをお客様に提供しています。ランサムウェアだけでなく、破壊的マルウェア、内部脅威、その他のAPT攻撃を防ぐお手伝いもできます。詳しくは弊社にお問い合わせください。

タレスについて

皆様がプライバシー保護を信頼して任せている相手は、そのデータを保護するためにタレスに頼っています。データセキュリティに関しては、組織が直面する決定的な局面は次々と増え続けています。その局面が暗号化戦略の策定、クラウドへの移行、コンプライアンス要件の順守のいずれであっても、デジタルトランスフォーメーションを保護するためにタレスに頼ることができます。