THALES

cpl.thalesgroup.com

Encrypt Everything

組織が機密データを保護するための実践ガイド

目次

THALES

cpl.thalesgroup.com

概要

エンタープライズデータセキュリティを担うエキスパートは、組織の貴重なデータを保護するために、エンタープライズ規模の暗号化戦略を策定し実施することが求められています。しかし、重要なデータはどこにでも流れています。境界はもはや存在しません。データは運用システムから分析システムへ、オンプレミスからクラウドへ、データベースからデータレイクへと移行しています。データの世界はかつてないスピードで変化しています。ビッグデータやマイクロサービスなどの新しいテクノロジーが同時にさまざまな形で採用されています。

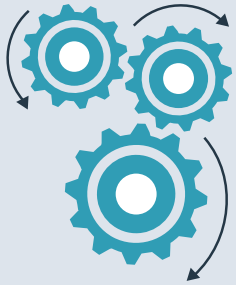
データセキュリティとは、アプリケーションや、データベース、クラウド、データレイク、またはその他の特定のプログラムではなく、データに対するセキュリティです。必要なものは、最も貴重なデータ資産を企業内外のどこにあろうとも守る、広範な保護方法と実施メカニズムの効果的な組み合わせを含めた、包括的なデータセキュリティプラットフォームです。この電子ブックでは、最も重要なデータ資産を保護するためのデータセキュリティポリシーの定義と適用に使用できる方法論とベストプラクティスの概要についてご紹介します。

データセキュリティの課題

データセキュリティの最重要課題は4つあります。

爆発的なデータの増加

新しいコンプライアンス要件



運用の複雑化

急増する脅威

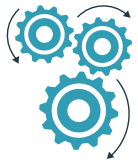
データセキュリティの最重要課題

爆発的なデータ増加

規模や業界を問わず、世界中の企業が、かつてないほど多くのデータを生成しています。同時に、こうした情報へのアクセスに対する要求も高まっています。コストの削減、効率性の向上、新製品の開発、製品の最適化、よりスマートでデータ主導のビジネス上の意思決定のために、ビジネスインテリジェンスチームやマーケティングチームから、パートナーやサードパーティベンダーにいたる誰もが、データに目を向けています。こうした要求を満たすには、データを生成、保存、処理し、より多くの場所で共有して配布する必要があります。

新しいコンプライアンス要件

個人を特定できる情報（PII）を標的とする世界的な脅威の増大により、企業が管理および処理する機密データの保護強化を目的としたコンプライアンス要件が増え続けています。これには、一般データ保護規則（GDPR）、カリフォルニア州消費者プライバシー法（CCPA）、ブラジル個人情報保護法（LGPD）などが含まれています。組織は、これらの規制やPCI DSSなどの業界基準に合わせて特定の要件にどのように対処するか、ガイドを必要としています。



運用の複雑化

クラウド、コンテナ、ビッグデータテクノロジー、さらに複数ベンダーの多様なツールへの移行によって、複雑化はますます進行しています。企業のセキュリティ境界がますます曖昧になるにつれて、分散したITリソースに対して一貫性のある統一したアクセスポリシーを提供して実装し管理することが困難になっています。すべての組織に、レガシープラットフォームと新しいプラットフォームが混在しています。しかし、データはデータなので、問題のあるサイロは関係がなく、損失した機密データはやはり損失した機密データであり、どこにあったかは関係がないのです。

急増する脅威

ビジネスの損失から規制違反による罰金や是正にかかるコストまで、データ侵害は広範囲に影響します。データに対する脅威を防御することは、非常に困難な取り組みです。マルウェア、フィッシング、機械学習、暗号通貨など、多くの新たな進化するデータセキュリティ脅威によって、企業、政府、個人のデータや資産は常に危機に直面しています。

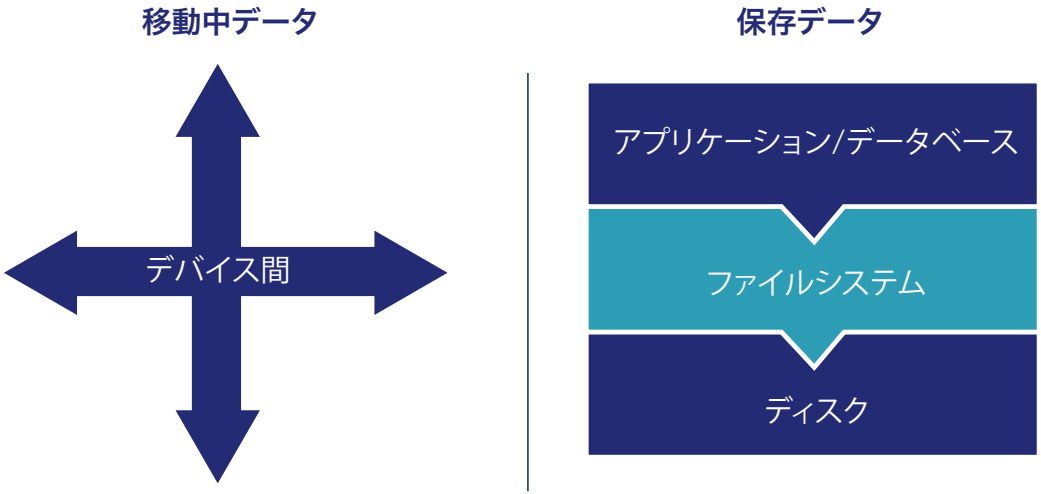
データセキュリティの課題に対処する方法

データ中心のセキュリティアプローチは、事実として、世界中のすべてのデータコンプライアンス規制と標準に不可欠であり、基本的なベストプラクティスです。データ中心セキュリティの特徴は、データの場所に関係なく、データ自体に保護が適用されることです。

残念ながら、ほとんどのデータセキュリティテクノロジーは、データ自体ではなくデータの場所の保護に焦点を当てています。たとえば、特定のノートパソコンまたはサーバーに保存されている全データや、特定のネットワークを通過する全データを保護します。このアプローチの問題点は、データが他の場所に移動するとすぐに、別のソリューションが必要になるか、データが保護されないままになることです。

一方、データ中心セキュリティは、保護すべきもの、すなわち機密情報を含むファイルに焦点を当て、データがどこにあるかに関係なく適切な形式で保護します。この効果を発揮させるには、自動で行われなければならず、機密情報は、組織のITエコシステムに入ったらすぐに特定され、データライフサイクル全体を通して続くポリシーベースの保護によって安全を確保する必要があります。

データは、転送中も保存時もリスクにさらされる可能性があるため、どちらの状態でも保護が必要です。そのため、転送中も保存時もデータを保護する多くのアプローチがあります。暗号化はデータセキュリティにおいて非常に重要な役割を果たしており、転送中も保存時もデータを保護する一般的なツールです。転送中データの保護については、企業は多くの場合、機密データを移動する前に暗号化するか、暗号化装置を使用して転送中データのコンテンツを保護することを選びます。保存データの保護については、企業は機密データをファイルやデータベースに保存する前に暗号化するか、ストレージドライブ自体を暗号化することを選べます。



暗号化技術を使用してデータを保護する場合、エンタープライズセキュリティは暗号鍵とポリシー管理に頼ることになります。ポリシー管理により、関連付けられている機密情報を保護するために、必要に応じて暗号鍵を生成、配布、保存、ローテーション、無効化/破棄できます。暗号化を使用したベストプラクティスのデータセキュリティソリューションには、強力な鍵管理のほか、データ保護を適用するシステムと鍵管理を実行するシステム間の職掌分散などが含まれます。また、優れた鍵管理システムは、鍵の作成と保管にハードウェアベースの信頼のルートを活用する機能を提供します。

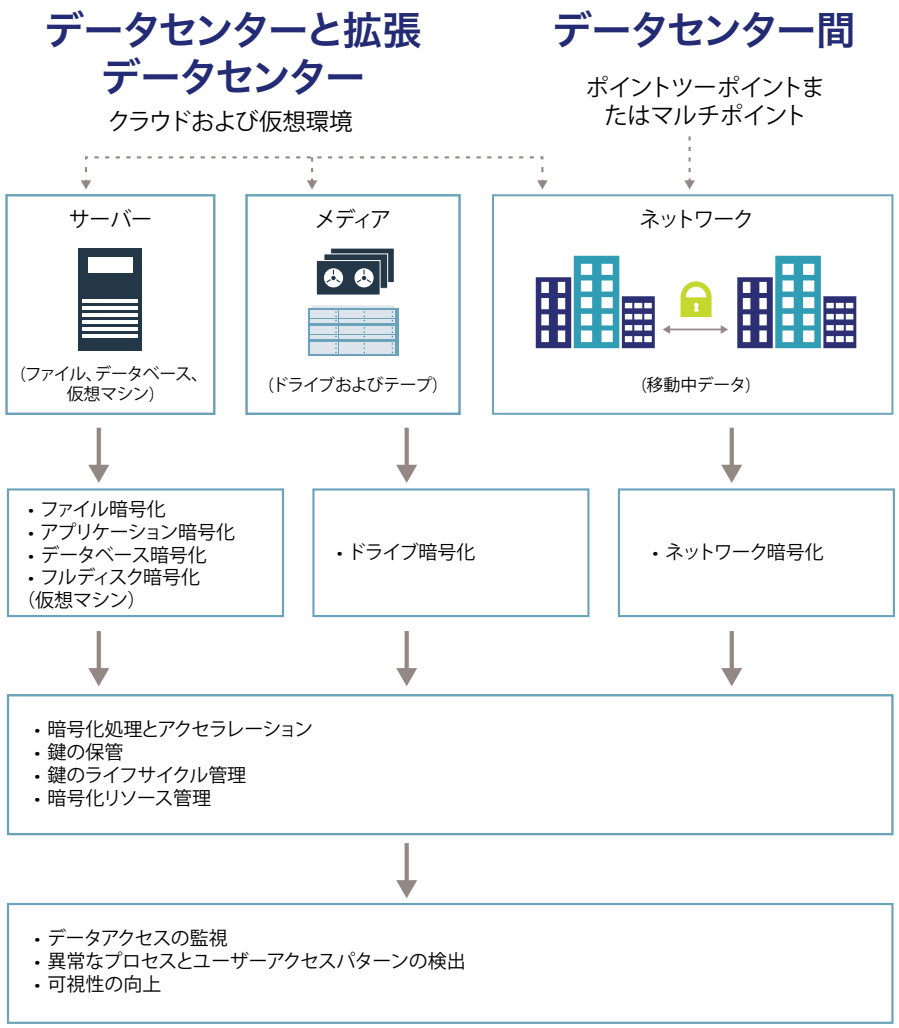
データ中心セキュリティが適切に実装されると、組織は各ファイルやデータベースレコードが作成された瞬間から、機密データを完全に制御できます。保護されたデータへのアクセスはいつでも許可または取消でき、すべてのアクティビティは監査とレポートのためログに記録されます。

データ中心のセキュリティアプローチを適切に実行するには、利用可能な暗号化とデータ保護方法に加えて、要件、保護するアプリケーションまたはデータ、選択した保護方法を適用する理由に注意することが重要です。利用可能な最も広範なソリューションセットと、一元化された鍵管理とポリシー管理を提供するベンダーを選択すると、インストールベースを拡張するときに導入と管理制御が容易になります。

エンタープライズデータ保護に取り組む方法

エンタープライズデータ保護に取り組む際は、従うべき4つの一般的な手順があります。

1. 機密データを特定する
2. 機密データを暗号化する
3. 暗号鍵を管理する
4. アクセスポリシーを実施する



THALES

cpl.thalesgroup.com

まず最も機密性の高いデータ資産がオンプレミスデータセンターのどこにあるかを特定してから、拡張データセンター（クラウドおよび仮想環境）に移動します。ストレージサーバーおよびファイルサーバー、アプリケーション、データベース、仮想マシンを検索します。ネットワーク全体やデータセンター間を流れるトラフィックを見落とさないでください。このデータが組織の境界を越えると、そのデータを制御できなくなります。

次に、データ中心セキュリティソリューションを使用して、データを暗号化します。幸い、データを大規模に、ビジネスの流れを中断させない一元的な方法で暗号化する技術は、今日のエンタープライズ対応ソリューションで実現しています。

そして、鍵を忘れないでください。鍵をデータと切り離して一元的に管理および保管することで、所有権と制御を維持し、監査と制御のために暗号化インフラストラクチャを合理化できます。

効果的なデータセキュリティは、今日のデジタルビジネスにおいて重要な差別化要因となります。データはほぼすべての組織の中核をなしており、データを保護し続けながら、効果的な利用を促進してビジネス価値を向上させることが重要な成功要因になります。

効果的なデータセキュリティとは何か?

最適なデータセキュリティソリューションは、データ保護の過程を通じて、より優れた可視性の獲得、実用的な洞察の活用、リアルタイム管理の実施、コンプライアンスサポートの自動化を実現する、データ保護機能の統合スイートを提供します。重要なデータ保護機能の一部を下図に示します。

データディスカバリ

データディスカバリとは、インタラクティブな視覚分析を使用して、複数のソースからデータのパターンを見つけることにより、実用的な情報を取得するプロセスのことです。この用語は、すべてのデータソースの全体像を得て、データが存在する場所を特定し、機密データや規制対象データを含む可能性のあるネットワーク内のデータベースまたはファイルソースを検出しようと試みる分析の方法を意味します。

データ分類

データ分類とは、広義では、データをより効率的に使用および保護できるように、関連するカテゴリごとにデータを整理するプロセスを指します。検出されたデータソースを解析して、それらに含まれるデータの種類を判別し、定義済みのパターンまたはキーワードのセットと照合します。次に、データタイプに基づいてラベルを割り当て、ポリシーを通知します。データ分類は、リスク管理、コンプライアンス、データセキュリティに関して特に重要です。

データ難読化

データ中心のデータ保護の本質は、データに独自の防御があることです。これには、データを判読不能にして再度判読可能にするにはツールを要すること、またそれらのツールをデータから切り離してツールへのアクセスを慎重に制御することが必要となります。暗号化とトークン化はデータを判読不能にする手段であり、鍵管理はデータを再び判読可能にするために必要なツールを切り離して保護するプロセスです。

鍵管理

暗号鍵管理は、暗号鍵のライフサイクル全体を管理し、鍵を紛失や誤用から保護します。ライフサイクルには、鍵の生成、使用、保管、アーカイブ、削除が含まれます。暗号鍵の保護には、(物理的およびユーザー/ロールアクセスを介した)鍵へのアクセスの制限、複雑な暗号化環境全体での鍵の安全な配布、鍵管理の一元化、データの機密性と準拠(FIPS)を維持するための組織化された安全な鍵管理の実現が含まれます。

暗号化

データ暗号化は、データを別のフォームまたはコードに変換するため、秘密鍵（正式名称は復号鍵）またはパスワードにアクセスできるユーザーのみがデータを読み取ることができます。暗号化されたデータは一般に暗号文と呼ばれ、暗号化されていないデータは平文と呼ばれます。現在、暗号化は、一般的に組織で使用される特に効果的なデータセキュリティ手法の1つとなっています。データ暗号化には主に、公開鍵暗号とも呼ばれる非対称暗号化と、対称暗号化の2種類があります。

トークン化

トークン化とは、アカウント番号などの意味のあるデータを、漏洩しても意味を持たないトークンと呼ばれるランダムな文字列に置き換えるプロセスです。トークンは元データへの参照として機能しますが、それらの値を推測するために使用することはできません。これは、暗号化とは異なり、トークン化では機密情報をトークンに置き換えるための数学的プロセスを使用しないためです。

クラウドセキュリティ

エンタープライズ向け暗号化ソリューションを使用すると、オンプレミスだけでなく、仮想環境、パブリッククラウド環境、ハイブリッド環境にわたってデータと暗号鍵の制御と所有権を維持できます。クラウドセキュリティは、利用するクラウドプロバイダーと展開モデルによって大幅に異なります。大きく分けると、次の3つのオプションがあります。:

- **Bring your own encryption**（独自の暗号化適用）と鍵の一元管理: これにより、ハイブリッド環境全体にわたって機密データを保護し、最大限の制御、可視性、移植性を実現できます。クラウド、ベンダー、場所に依存しないため、運用の容易さとコンプライアンスのためにセキュリティを統一する柔軟性が得られます。
- **Bring Your Own Key**（独自の鍵使用）によるクラウド暗号化サービス: 暗号鍵管理に関するベストプラクティスに準拠するため、ほとんどの主流のIaaS/PaaSプロバイダーが、BYOK（Bring Your Own Key）API（Application Programming Interfaces）やHYOK（Hold Your Own Key）を提供しています。独自のBYOK APIを備えたマルチクラウド環境では、BYOK暗号鍵を管理するために追加ツールが必要になる場合があります。
- **ネイティブ暗号化サービス:** これはクラウドサービスプロバイダーに固有のものであり、プロバイダーが完全に管理します。リスクプロファイルとデータの機密性に応じて、可視性、制御、移植性のためのツールを追加してこれらのサービスを補完する必要があります。

Encrypt Everything戦略

すでに説明したように、情報に対する内外のリスクと脅威は、範囲、量、影響のすべてにおいて増大しています。そのため、組織は競争力を維持して新しい規制に準拠することをますます強く求められるようになっていますが、最終目標は組織のデータを保護することです。デジタルエンタープライズの保護は、サイバー脅威からの保護だけではなく、データの機密性、整合性、可用性も含まれます。

セキュリティ侵害の脅威に影響されない組織はありませんが、データ暗号化の実装は、情報資産と組織の評判を守るための主要な保護手段です。ほとんどの組織は、機密データ、特に保存データを暗号化することは堅実なデータ保護戦略であると同意しています。しかし、そのアプローチには誤りがあります。

まず、かつてないほど膨大なデータが存在し、驚異的なスピードで作成され続けています。多くの場合、暗号化は手間のかかる取り組みであると推定されるため、暗号化は最も価値のある情報資産のみに制限されています。これは、データ分類の問題につながります。データを分類しないと、その機密データがどこにあり、何と相互作用し、価値とリスクに関して組織にとってどのような意味を持つのかがわかりません。しかし、「機密」とされるものは何でしょうか？　「機密」の意味に全員が同意するわけではないため、組織は「機密」の意味を定義するために時間とエネルギーを費やす必要があります。このため、実装には多くの時間とリソースが必要です。

これはもはや事実とは異なります。これまで、一般的な暗号化は、非常に時間がかかり、計算要件、スペース要件、運用効率、管理や全体的な使いやすさが大きな足かせとなって、ほとんど放棄されていました。こうした技術的課題により、機密データのみを暗号化することにつながっていました。しかし、これらの障壁のほとんどは解消されました。CSOのために、Encrypt Everything戦略をよりシンプルで費用対効果の高いものにする道が開かれたのです。

すべてのデータを暗号化することで、組織内やオンプレミスとクラウド間であっても、データの移動時に各種の規制基準や要件に常に準拠することが保証されます。同様に重要なこととして、Encrypt Everythingアプローチは、組織のブランドと評判を保護できます。ほぼすべての組織が、いつかはデータ侵害に苦しむことに、ほとんどの専門家が同意しています。これは、攻撃された「場合」ではなく、攻撃された「とき」の問題です。組織から流出したデータは暗号化されているため、データを盗んだサイバー犯罪者にとって価値がないことが分かっている安心感（およびリスク低減）を想像してください。ほとんどのコンプライアンス基準では、データが暗号化されている場合、侵害されたデータを公に報告する必要はないとされています。機密データのみの暗号化アプローチに固執する同業他社は、侵害されたデータが機密情報であるかどうか、暗号化されていたかどうかを判断するサイクルに時間を費やす必要があります。暗号化されていなければ、侵害を公に報告する必要があります。その損害は、顧客、パートナー、潜在従業員、その他ステークホルダーの目から見た会社のブランドと評判にまで及びます。

非常に優秀な企業の非常に優秀な人々は、データの大半を暗号化することが、リスクを軽減して顧客の不安を和らげるためにできる最善策の1つであるという結論に達しました。どの企業やCEOもデータ侵害についての話し合いを望んでいませんが、データ保護を優先するための広範な戦略を持つことは、セキュリティとマーケティングの両方の観点から重要です。

Encrypt Everything戦略により、すべてのデータが暗号化され強力なアクセス制御によって保護され、業務上そのデータを必要とする人物のみが目的のデータにのみアクセスできるようになります。特権ユーザーは、メタデータにのみアクセスでき、企業データを見ることはできないため、データ分類が不要になります。また、CSOは、まったく新しい別の方法でデータへのアクセスを維持、モデリング、提供することにより、リスクを異なる方法で評価できます。

THALES

cpl.thalesgroup.com

タレスがデータを保護できる理由

タレスは、データ侵害が発生した場合でも、機密の保存データと移動中データを安全に保つために必要なソリューションを提供します。タレスのソリューションを使えば、ビジネス固有のニーズに応じて、データ保護を必要な場所で、必要なときに必要な方法で適用できます。

企業、政府、組織が、タレスを信頼して、最も機密性の高いデータの保護を任せています。タレスの高度なデータ暗号化、鍵管理、トークン化、ハードウェアセキュリティモジュールソリューションにより、デジタル決済の安全確保、コンプライアンスの達成、クラウド、データセンター、ネットワーク、ハイブリッドIT環境全体の場所を問わないデータ保護、制御の維持を実現できます。

このように、Encrypt Everything戦略を展開するために使用できる手段と方法は多数あります。「お決まりの」手法があるわけではありませんが、単一の統一プラットフォームで利用可能なオプションがあると、現在および将来のデータの保護が容易になります。

タレスの業界をリードするデータセキュリティソリューション

タレスの保存データセキュリティソリューションは比類のない保護を提供し、オンプレミス、クラウド、仮想環境のデータベース、アプリケーション、ファイルサーバー、ストレージを保護します。タレスのCipherTrust Data Security Platform（CDSP：データセキュリティプラットフォーム）を使用すると、組織全体で保存データのセキュリティを簡単かつ効率的に管理できます。拡張可能なインフラストラクチャ上に構築されたこのプラットフォームは、高度な暗号化、トークン化、鍵の一元管理を実現する、個別にでも組み合わせても導入可能な複数のデータセキュリティ製品を備えています。このデータセキュリティソリューションにより、最小のTCOで次なるセキュリティ課題と新しいコンプライアンス要件に対応できる準備が整います。

鍵を保護するために、タレスの業界をリードするクラウドHSM（ハードウェアセキュリティモジュール）、汎用HSM、決済用HSMは、世界で最もセキュリティ意識の高い各種組織の暗号化機能とインフラストラクチャを保護する、信頼のルートを提供します。

保存データセキュリティソリューションのほか、タレスは、最大10 Gbpsの速度でネットワーク上を移動する機密データを保護する、広範なSafeNet高速ネットワーク暗号化を提供しています。

この包括的なアプローチにより、現在のデータ保護ニーズにすぐに応えられるとともに、堅牢なセキュリティ、拡張するエコシステム、将来の信頼できるフレームワークの構築に必要なスケーラビリティを提供するソリューションへの投資にもなります。

まとめ

このデジタルトランスフォーメーションの時代に生き残って繁栄することを望む組織は、最高の人材、最高の戦略、そしてもちろん最高のテクノロジーといった、あらゆる優位性の獲得が必要となります。テクノロジーは、結局のところ、商取引の高速化、透明化、効率化に寄与しています。ビッグデータ、クラウドコンピューティング、「IoT（モノのインターネット）」、ロボティクス、ボット、およびその他の形式の人工知能はすべて、まだ使用していなくても、おそらく組織が検討または検証しているであろうテクノロジーです。

これらのテクノロジーは、従来のエンタープライズの境界を曖昧にしたり排除したりするため、サイバー攻撃の新たな経路を生み出しています。また同時に、攻撃者の手口は巧妙化しています。私たちは、マルウェア、ランサムウェア、スピアフィッシング、インサイダー脅威、国家攻撃、APT、SQLインジェクション、ソーシャルエンジニアリングの世界に住んでいます。

この現実から保護するための「特効薬」はありません。しかしCSOとCISOは、「お金の流れを追って真実を見出し（follow the money）」、データ保護に対してEncrypt Everythingアプローチに焦点を合わせることで、ステークホルダーから委託されたデータや組織の評判と財務の健全性を保護しつつ、新しいビジネスやテクノロジーの使用を実現できます。

タレスのデータセキュリティソリューションを使用すれば、組織全体にわたって保存データと移動中データのセキュリティを低コストかつ効率的に管理できます。

タレスDIS CPLジャパン株式会社
〒108-0075 東京都港区港南1-6-31 品川東急ビル5階 | Tel: 03-6744-0221
Fax: 03-3474-8162 | E-mail: cpl.jpsales@thalesgroup.com

> cpl.thalesgroup.com <