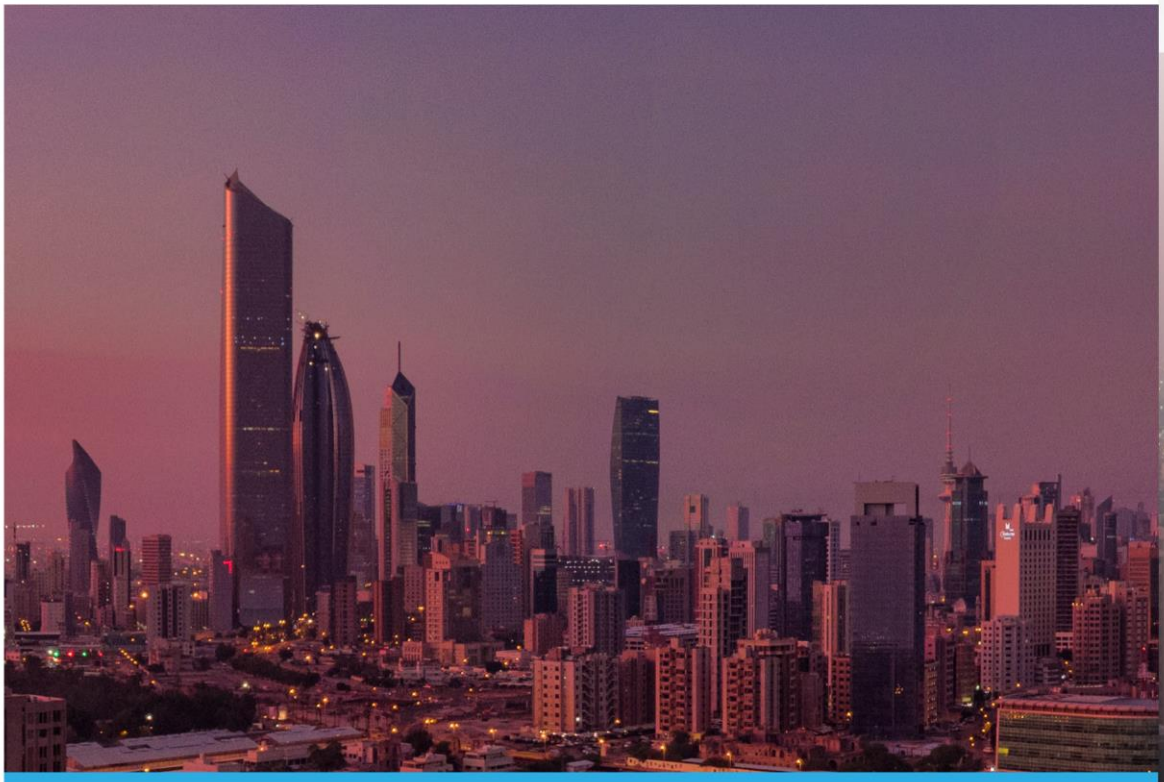
スポンサーコンテンツ| ホワイトペーパー

サイバーセキュリティ

# HSM：企業向けサイバーセキュリティ戦略における重要な要素



CSO

スポンサー ENTRUST

サイバーセキュリティ

**現在、企業にとって、シームレスな業務運営、顧客満足度の向上、将来のビジネス成長を実現するには、データが最も重要です。**一方で、サイバーセキュリティの脅威が日々増大しています。企業がマルチクラウドソリューションを追求する現在の分散環境では、データ保護がこれまで以上に重要になっています。多くの企業は、暗号鍵を使用してデータを暗号化しています。しかし、これらの鍵を適切に保護できていない企業が非常に多く、データが内外の脅威に対して脆弱な状態になってしまいます。暗号鍵を保護し、重要なデータを確実に保護する最善の方法は、暗号鍵の保護と管理を目的として特別に設計されたハードウェアセキュリティモジュール (HSM) を使用することです。

## 重要なデータを保護する上での問題

企業は現在、ビジネスを拡大し、競争力を維持し、市場や顧客に関するより深い洞察を得るために、より多くのデータを使用するようになっています。

これには、個人識別データ、企業財務データ、顧客販売情報、人事および販売データ、知的財産などが含まれます。これらはすべて、社内外からの脅威に対して攻撃を受けやすい状態である可能性があります。特に、データが明確な境界内に保存されなくなった現在の分散環境においては、こうした懸念が高まっています。多くの企業では、データをクラウドやデータセンターに保存しているのです。

「もはやセキュリティの境界線など存在しません。非常に曖昧な領域なのです」と、Entrust の製品ソリューションおよびパートナーマーケティング担当ディレクターであるフアン・アセンホ氏は述べています。「分散環境は攻撃の対象を増やし、より多くの脅威を生み出します。そして、悪意のある第三者がこうした状況を悪用しようとし、リスクが増大しているのです」こうした脅威には、外部からの脅威（データや鍵を盗んだり、インフラにマルウェアやトロイの木馬を注入するハッカーなど）や、仕事に不満を抱くスタッフによる内部からの脅威が含まれます。また、ヒューマンエラーによってもデータが危険にさらされる可能性があります。さらに、ソーシャルエンジニアリング、賄賂、汚職、強要などを通じて脅威がもたらされる可能性もあります。

その一方で、企業に対するプライバシーやデータ保護への期待は高まっています。データを保護できない企業は、知的財産や顧客の信頼を失うリスクに直面します。また、株式市場での損失、多額の改善費用、訴訟費用、さらには罰金が発生する可能性もあります。

サイバーセキュリティ

ほとんどの企業は、自社や業務内容を定義する重要なデータ資産を保護する必要があることを十分に認識しています。そのため、このような脅威からデータを保護するために、多くの企業が数学的アルゴリズムを使用して、データへの不正アクセスを防止する暗号化に頼るようになってきました。暗号化はデータの安全性を確保し、インターネット取引の安全性も確保します。暗号化アルゴリズムは、暗号鍵を使用してデータのロックとロック解除を行います。

2022 年の Ponemon Institute Global Encryption Trends Study（2022 年 ポネモン研究所 グローバル暗号化動向調査）によると、暗号化を使用する主な理由のトップ 5 は次の通りです：

- **顧客の個人情報の保護**
- **特定の脅威から情報の保護**
- **企業の知的財産の保護**
- **外部のプライバシーまたはデータセキュリティに関する規制や要件への準拠**
- **違反や不注意による情報漏洩に対する責任の制限**

しかし、暗号化の安全性は暗号鍵の保護機能に左右されます。アセンホ氏は、これを家の玄関の鍵と鍵の保管場所に例えて説明しています。「玄関の鍵の安全性は、鍵をどこに保管するかによって決まります。玄関マットの下に鍵を置いておけば、簡単に発見されてしまい、保護効果は期待できません」と彼は述べています。

残念ながら、暗号鍵をどこに保管しているのか把握していない、あるいはソフトウェアに保管している企業があまりにも多く、その場合、サーバーのファイルシステムに鍵がはっきりと残るため、ハッカーの攻撃対象とされやすくなってしまいます。この脆弱性は、企業内外の悪意ある行為者にまで広がります。

また、アセンホ氏によると、企業が暗号化のための暗号化機能を備えたデータベースセキュリティソリューションを導入することはよくあるそうですが、その場合、企業はアプリケーションが稼働しているのと同じソフトウェアレベルで鍵を保存してしまっているようです。

この状況を「玄関のウェルカムマットの下に置いているようなものです。鍵をそれ以上のレベルで保護しなければ、暗号化メカニズムを適切に確保できません。

暗号鍵を保護することは、情報と企業の整合性を確保する上で最も重要です」と彼は説明しています。

## 暗号鍵管理の包括的ソリューション

企業は、暗号鍵のライフサイクル全体（作成、使用、保存から削除、交換まで）にわたって管理する方法を必要としています。

特に、機密性の高い重要なデータに関しては、企業は機密性、完全性、可用性を確保しなければなりません。暗号化を実装した後も、対応を継続する必要があり、その中心となるのが HSM です。

HSM（ハードウェアセキュリティモジュール）は、サポートするアプリケーションとは別に暗号鍵を生成および管理ためにデザインされた専用デバイスです。「鍵を意図的に別の場所、つまりハードウェアである保管庫に置くのです」とアセンホ氏は言います。HSM には、鍵が意図されたアプリケーションでのみ使用され、権限のある個人およびアプリケーションのみがアクセスできるようにするメカニズムが組み込まれています。

さらに、HSM は、チェックアンドバランスと二重制御なしに、暗号鍵の使用ポリシーが個人または企業によって変更されることがないようにします。銀行の貸金庫を開けるには顧客と銀行員の両方が必要であるように、HSM では、企業の鍵の変更は複数の人物によって承認されなければなりません。

脅威が増加し、さらに高度化してきている現在の環境において、HSM は企業のサイバーセキュリティ戦略にとって不可欠な要素であるとアセンホ氏は述べています。HSM は、暗号鍵の生成、使用、管理に安全な環境を提供し、データと鍵を徹底的に防御することで、侵入を試みる悪意のある行為を阻止します。

HSM は、セキュリティ対策のベストプラクティスも維持します。企業にセキュリティの安心感を提供し、より高度な管理を可能にします。また、汎用性が高く、公開鍵基盤 (PKI)、クラウド、IoT、デジタル決済、ブロックチェーン、コード署名など、幅広いアプリケーションで利用できます。

HSM の主な特徴には、以下のものが含まれます。

- **セキュリティの強化**
- **暗号鍵の保護**
- **強靭な鍵ストレージの提供**
- **ハッカーの侵入阻止**
- **規制順守の促進**

## 認証 HSM は安心感を提供

Entrust nShield HSM のような認証 HSM は、企業に強化された保護を提供します。

認定 HSM は、連邦情報処理標準(FIPS)やコモンクライテリアなど、世界的に認められた暗号の堅牢性に関する基準を満たしています。「デバイスが認定されていることは重要です。第三者機関による承認の証しですから」とアセンホ氏は言います。

Entrust の nShield HSM は、認証されたハードウェア環境を提供するように特別にデザインされており、アプライアン

ス、組み込みカード、または USB デバイスとして提供されます。アプライアンスは、オンプレミスのデータセンターに導入することも、ブスクリプションモデル (nShield as a Service) を通じて利用することもできます。

nShield HSM は、強固なアクセス制御メカニズムを採用する暗号境界内で、企業が鍵を安全に保護することを可能にします。これにより、鍵が承認された目的でのみ使用されます。また、nShield HSM は、高度な鍵管理、保存、および冗長機能により、鍵が必要なときにアプリケーションが常に利用できるようにします。その結果、要求の厳しいアプリケーションやトランザクションレートをサポートする高いパフォーマンスを実現します。

フォームファクタや導入オプションに関係なく、Entrust の nShield HSM は、機密データやトランザクションを保護するために、デジタル署名と暗号化用の強固な鍵生成を提供します。Entrust の nShield HSM は、以下の特長を備えています。

- **アプリケーションおよびソフトウェア環境から鍵を分離**
- **ユーザー認証を強化し、職務の分離を実現**
- **FIPS セキュリティ境界内でカスタムアプリケーションの実装に対応**
- **セキュアな鍵のバックアップを簡素化し、ポリシーの順守を徹底**

「nShield のもう一つの特徴は、Security World と呼ばれる包括的な管理アーキテクチャです」とアセンホ氏が主張。Security World は鍵を個別のコンポーネントに分割します。これらのコンポーネントは異なる場所に保管され、HSM 内でしか再構成できません。「それによって、安全性と回復力が向上します」とアセンホ氏が説明します。

Entrust の顧客は、nShield の導入により、機密データの保護を強化することができました。その実際の例は Novacoast です。名前や電話番号などの顧客データを収集し、他の企業のデジタルセキュリティを管理する Novacoast 社。リスクの回避と軽減を優先しており、セキュリティのベストプラクティスを実践するために nShield を導入しました。nShield を導入することで、暗号鍵の保護に成功し、アプリケーション間で安全にデータをやり取りできるようになりました。

その他に、ハンガリーの認定トラストサービスプロバイダーである Microsec は、ドイツの高速道路運営会社である Autobahn GmbH des Bundes とそのインフラの高度道路交通システム(C-ITS)向けに、Entrust HSM を利用したメッセージセキュリティサービスを提供しました。

nShield のおかげで、ヨーロッパの道路約 6000 キロが C-ITS に対応できるようになりました。車両、道路利用者、サービスプロバイダ、道路運営者はすべてネットワークに接続しており、お互いに匿

名化されたデータを安全に交換することができるようになりました。

その結果、完全にデジタルで接続かつ自動化された交通システムが構築され、ドライバー、乗客、保守作業員にとって交通安全が向上しました。

ビジネスの世界が進化し、より多くの企業が分散環境で事業を展開し、マルチクラウドソリューションに移行するにつれて、鍵管理における新たな問題が発生しているとアセンホ氏が指摘します。企業は、それに対応できるように準備をしなければなりません。

「異なる暗号化メカニズムを使用するクラウド環境がある場合、そのすべてをどのようにまとめるのか。包括的な理解が必要で、一貫した方法でセキュリティ管理を適用する必要があります。そこで、nShield は、暗号鍵を支える信頼性の基盤を提供し、企業に一貫性をもたらします」とまたアセンホ氏が述べています。◆

**Entrust nShield HSM の詳細については、こちらからクリックしてください。**