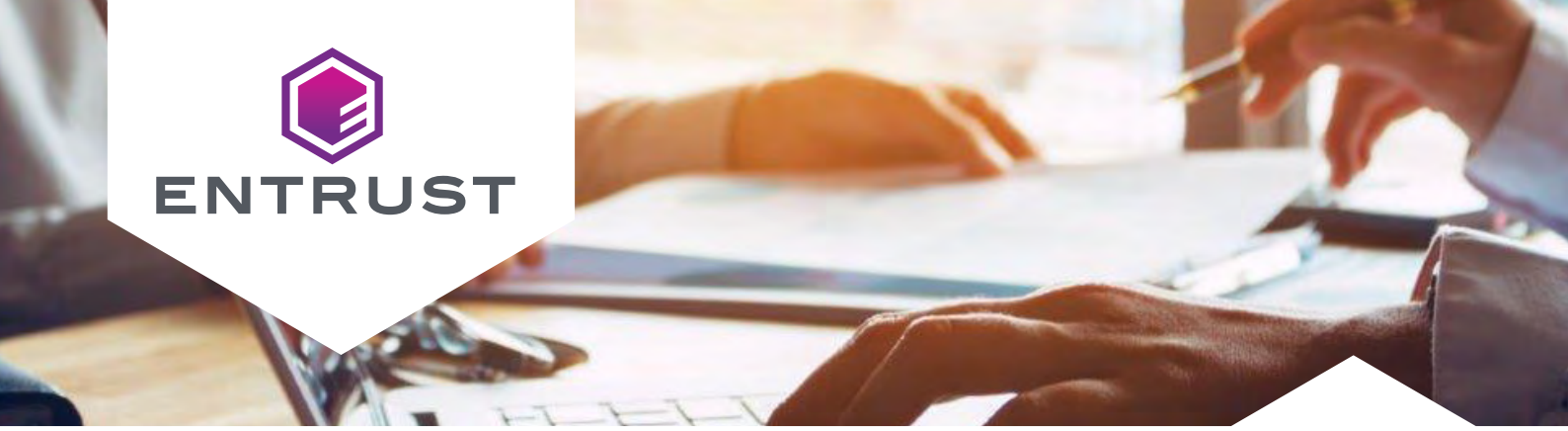


Entrustと大手トークン化プロバイダーが企業向けデータセキュリティとコンプライアンスを強化

NFINITY STRATEGIC TECHNOLOGY PARTNER PROGRAM

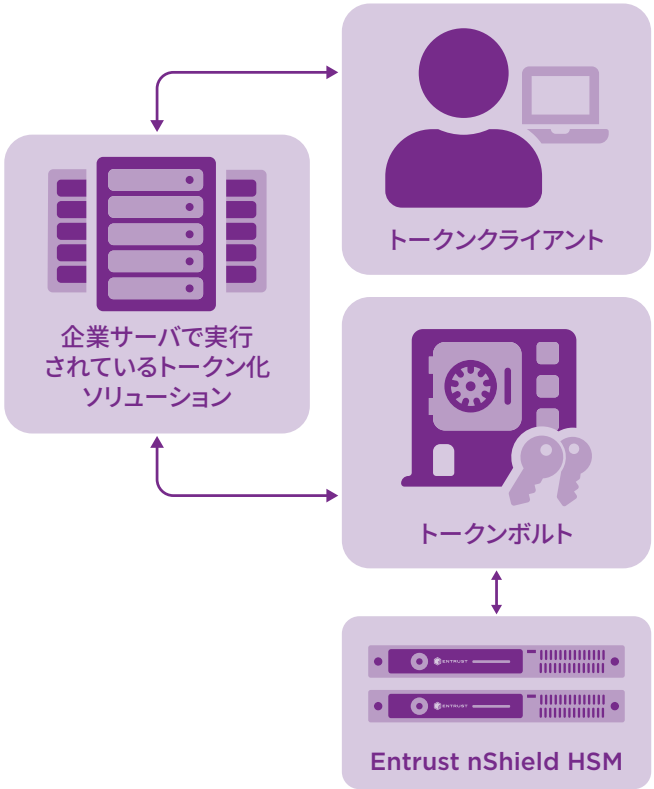
Entrust nShieldハードウェア・セキュリティ・モジュール（HSM）でトークン化とコンプライアンスの強化を実現

ハイライト

- 保存中、使用中、移動中の機密データを保護
- コンプライアンス監査の範囲を縮小しコストを削減
- フォーマット保持トークン化を使用して、アプリケーションの中断を回避
- FIPS 140-2レベル3認証を受けた耐タンパ性セキュリティモジュールで暗号鍵を保護
- 規格に準拠したエントロピーソースを使用して乱数を生成

課題：

さまざまな業界において企業は、機密性の高い情報をかつてないほど大量に保存および送信するようになっており、個人データの悪用によって収益を得ようとするサイバー犯罪者が攻撃を仕掛けてくる可能性が高まっています。個人データの流通市場が存在することで、個人を特定できる情報、決済用カード番号、医療記録が特に危険にさらされています。



Entrust nShield HSMはトークン化機能のマスタールート鍵をホストし、また、CodeSafeセキュアコードを使用して、安全な境界内で重要な機能を実行する場合があります。

詳細はこちらをご覧ください：ENTRUST.COM/ja/HSM

データセキュリティとコンプライアンスを強化

企業はこの状況への対応策として、データ漏洩のリスクを軽減するためにトークン化を利用しています。トークン化では、元のデータと同じフォーマットとタイプを維持しながら、実際の値をランダムなトークンに置き換えます。これにより、既存のアプリケーションとデータベースは、元の情報と同じ方法でトークンを認識して処理することができます。例えば、カスタマーサービス担当者が顧客の記録に情報を追加する際、特定のフィールドが即座にトークン化されるようにすることで、不正アクセスを防ぐことができます。アーキテクチャに応じて、実際の値が暗号化され別のボルトに保存されるか、ボルトレスアプローチを使用する場合は、トークンがアルゴリズムを介して生成されるため、実際の情報を保存する必要がなくなります。

トークン化によってデータの価値が下がることでセキュリティが向上し、データ盗難のリスクが軽減します。また、PCIデータセキュリティ基準では、規格に準拠したトークン化システムを使用することで、PCI DSS監査の範囲を効果的に縮小できると規定しており、トークン化によって、同基準などの規則への準拠を強化できます。

企業はトークン化システムを実装するにあたり、トークンが逆転し、データが明らかになることがないよう設計されたシステムを採用する必要があります。これは、企業が機密データの安全性を維持し、データプライバシーに関する規則を常に遵守する上で不可欠です。

ソリューション：Entrust nShield HSMを統合したトークン化

強力なトークン化ソリューションは、トークンの生成プロセスから始まります。最も効率的にトークンを生成するためには、ランダムなトークン化または暗号化によるトークン化と、暗号鍵の安全な保存が必要であるとされます。PCIのトークン化ガイドラインでは、「PCI DSS要件に従って、暗号鍵を管理および保護する必要がある。したがって、トークンの生成と解除に使用される暗号鍵が、安全なトークン化システム外にあるアプリケーション、システム、ユーザ、プロセスによって使用できないようにする必要がある」と明記しています。[1]

Entrust nShield® HSMは、主要なトークン化ソリューションと統合されています。これらは、トークンの生成プロセスで使用される、非常にランダムかつ安全性の高い暗号鍵の参照テーブルを確立します。nShieldの乱数ジェネレーターは、FIPSに準拠したエントロピーソースとして認定されています。企業はこの乱数ジェネレーターを使用することで、承認されていないユーザは元に戻すことができない、安全性の高いトークンを生成することができます。また、nShield HSMは、参照テーブルの暗号化に使用される鍵を生成し保護します。

トークン化アーキテクチャに、元のデータ用の個別のボルトが組み込まれている場合、ボルト内のデータの保護をサポートする暗号鍵は、nShield HSMによって生成および保護されます。

1. https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf

データセキュリティとコンプライアンスを強化

Entrust nShieldの特異点

Entrust nShield HSMは、認定された耐タンパ環境で暗号鍵を保護します。nShield HSMの暗号境界外で処理される鍵は、攻撃に対して非常に脆弱であり、機密情報の漏洩につながる可能性があります。HSMは、暗号化された重要なデータを保護することが実証され、かつ監査が可能な唯一の方法です。nShield HSMは次の機能をもたらします。

- 慎重に設計された暗号境界内で鍵と証明書を保護
- 堅牢なアクセス制御メカニズムを使用し、鍵が許可された目的にのみ使用されることを保証
- 高度な鍵管理、保管、冗長性機能を使用して可用性を確保し、必要なときに鍵にいつでもアクセスできることを保証
- 高い性能を発揮して大量のトークン化をサポート
- 金融サービス、小売業、その他の業界を管理する規制要件と規則に準拠

詳細

Entrust nShield HSMの詳細については、**entrust.com/ja/HSM**をご覧ください。ID、アクセス、通信、データに関するEntrustのデジタルセキュリティソリューションの詳細については、**entrust.com/ja**をご覧ください。

MICRO FOCUS Voltage

PrimeFactors™ — APPLIED DATA PROTECTION —

Entrust nShield
HSMの詳細はこちら：

HSMinfo@entrust.com

entrust.com/ja/HSM

ENTRUST社について

Entrust は信頼できる認証、支払い、データ保護を実現することで、動き続ける世界をセキュアにしています。今日、支払いや国際取引、電子政府サービスへのアクセス、そして企業ネットワークへの認証において世界中でより安全で円滑なユーザ体験が求められています。Entrust はこうしたインタラクションの要となり、他にはない多様なデジタルセキュリティと認証発行ソリューションを提供しています。2,500人を超える従業員、グローバルパートナーネットワーク、そして150カ国以上におよぶ顧客に支えられ、世界で最も信頼されている組織から信頼されています。

詳細はこちらでチェック：
entrust.com/ja/HSM

お問い合わせ：
HSMinfo@entrust.com