強化されたセキュリティ：Red Hat証明書システムのためのEntrustの高保証鍵保護

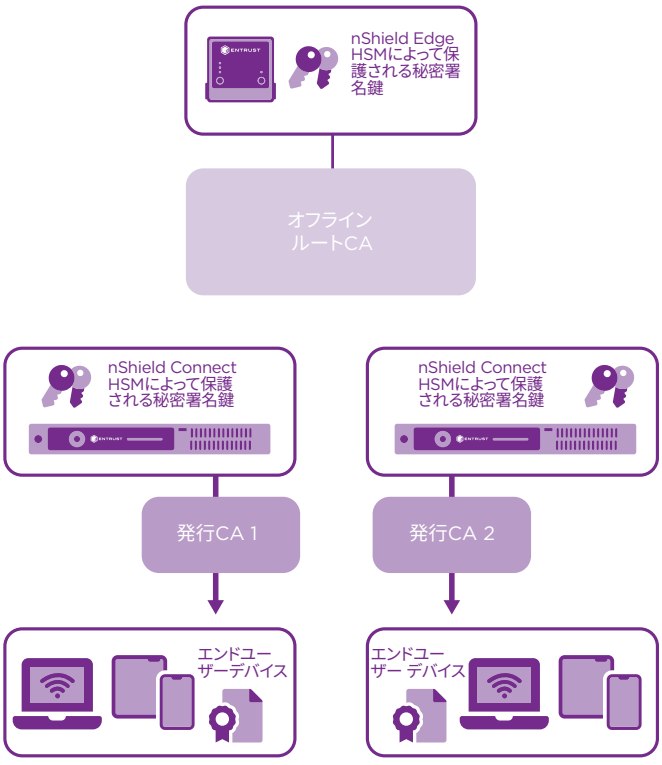
公開鍵基盤（PKI）に対する信頼の構築

ハイライト

- クラシファイド向けNSA商用ソリューション（CSfC）アプリケーションのRed Hat証明書システムのセキュリティを拡張する
- ユーザーIDを管理し、通信をプライベートに保つセキュリティフレームワークを強化する
- トランザクションとPKI対応アプリケーションを保護します
- NIST FIPS 140-2認定のEntrust nShield®ハードウェアセキュリティモジュール（HSM）を使用する

問題：組織のPKIは、増え続けるビジネスアプリケーションに対応するために拡張される

データ侵害がより高度になるにつれて、組織は重要なアプリケーションや機密データへのアクセスを保護かつ制御するためにPKIに注目しています。PKI内で、認証局（CA）は電子資格情報を発行して、オンラインIDを検証し、アクセス制御を実施します。使用されるデジタル証明書の数、それがサポートするアプリケーションの重要性と価値、アプリケーションが政府または業界の規制コンプライアンスのために高レベルの精査の対象となるかどうかを分析することは、PKIが増大する需要に対応できるようにするための重要な要素です。



nShield HSMは、Red Hat証明書システムで使用される秘密鍵を保護します。

詳細をチェック：ENTRUST.COM/ja/HSM

Red Hat証明書システムのための高保証鍵保護

課題：IDとアクセス制御の信頼の基点を確立する

PKIを支えるCAの整合性とセキュリティを保護することは、ビジネスアプリケーションとそれが保護するデータへの信頼を確保するために非常に重要です。PKIがモバイルを含むユーザーアクセストポロジの変更をさらにサポートし、独自のデバイスを持ち込む（BYOD）につれて、組織は秘密暗号化鍵が信頼できる方法で保護かつ管理されるようにする必要があります。

ソリューション：Red HatとEntrustはともに、デジタルIDの堅牢な保護を提供する

Red Hat 証明書システムは、個人、デバイス、サービスを対応する秘密鍵にバインドするために使用されるデジタルIDを発行、管理、検証します。発行された各証明書の有効性は、IDを発行するCA鍵の保護に依存します。ファイルにローカルに保存されている鍵を使用してサーバ上で発行プロセスが実行されると、その鍵は複製、変更、置換に対して脆弱になる可能性があります。現在、ほとんどのCAは、組織内で使用する証明書の発行に使用されています。証明書は組織内では通常、有線および無線認証、セキュアソケットレイヤー／トランスポートレイヤーセキュリティ（SSL ／TLS）接続、仮想プライベートネットワーク（VPN）認証の実行のために使用されます。拡張するアプリケーションにはPKIのサービスが必要であるため、CAに対する要求と、強化されたセキュリティの必要性が最も重要です。

Entrust nShield HSMは、プライベートルートを保護し、CA鍵に署名することにより、PKIの保証レベルを向上させます。nShield HSMは、発行、管理、検証のプロセスを保護し、組織がIDおよびアクセスソリューションを強化できるようにします。nShield HSMは、標準の暗号化アプリケーションプログラミングインターフェイス（CAPI）を使用して、Red Hat 証明書システムと簡単に統合できます。Entrust nShield HSMが使用される場合、すべての証明書の発行と検証の処理は、HSMの保護された範囲内で行われます。プライベートルート鍵と署名鍵は、HSMの外部でアクセスしたり、読み取り可能な形式でアクセスすることはできません。nShield HSMは、バックアップ、アーカイブ、リカバリプロセス中であっても、秘密鍵が操作や侵害の影響を受けないようにします。

Red Hat証明書システムのための高保証鍵保護

Entrust HSMをRed Hat証明書システムと併せて使用する理由は？

侵害の特定、回復、緊急時対応計画は、PKIのセキュリティを強化するために実行できる重要な手順です。強化された高保証PKIは、セキュリティが重要な鍵を盗難や誤用から保護する環境を提供します。Entrust nShield HSMを使用したIDチェックと承認へ証明書発行をバインドすることは、過去のCAのセキュリティ侵害から学んだ重要な教訓に基づいています。

FIPS140-2レベル3およびコモンクライテリアEAL4 + nShield HSMを含む厳格なセキュリティ標準の認定を受けています。

- 安全で改ざんされにくい環境で、デジタル証明書の署名および発行を行うための鍵を保存する
- スマートカードベースのポリシーと2要素認証を使用して、管理者アクセスを管理する
- 公共部門、金融サービス、企業の規制要件に準拠する

Entrust HSM

Entrust nShield HSMは、最高の性能と安全性を備え、簡単に統合できるHSMソリューションの1つであり、規制コンプライアンスを促進すると同時に、企業、金融機関、政府機関に最高レベルのデータセキュリティとアプリケーションセキュリティを提供します。当社独自のSecurity World鍵管理アーキテクチャは、鍵へのアクセスおよび鍵の使用を厳重かつきめ細かく制御します。

Red Hat

Red Hatは、企業向けのオープンソースソリューションにおいて業界をリードするプロバイダーです。Red Hat証明書システムに加えて、ソリューションには、幅広い管理とサービスの中で、Red Hat Enterprise Linux、Red Hat OpenStack、Red Hat OpenShiftプラットフォームが含まれます。Entrust nShield HSMは、RedHat証明書システムで認定されています。**www.redhat.com**

詳細

Entrust nShield HSMの詳細については、**entrust.com/ja/HSM**をご覧ください。アイデンティティ、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。

Entrust nShield
HSMの詳細はこちら：

HSMinfo@entrust.com
entrust.com/ja/HSM

ENTRUST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 はこれらの要となる部分において、他に類を見ない幅広いデジタルセキュリティとID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。

詳細は下記URLをご覧ください。
entrust.com/ja/HSM

ENTRUST

お問い合わせ：
HSMinfo@entrust.com