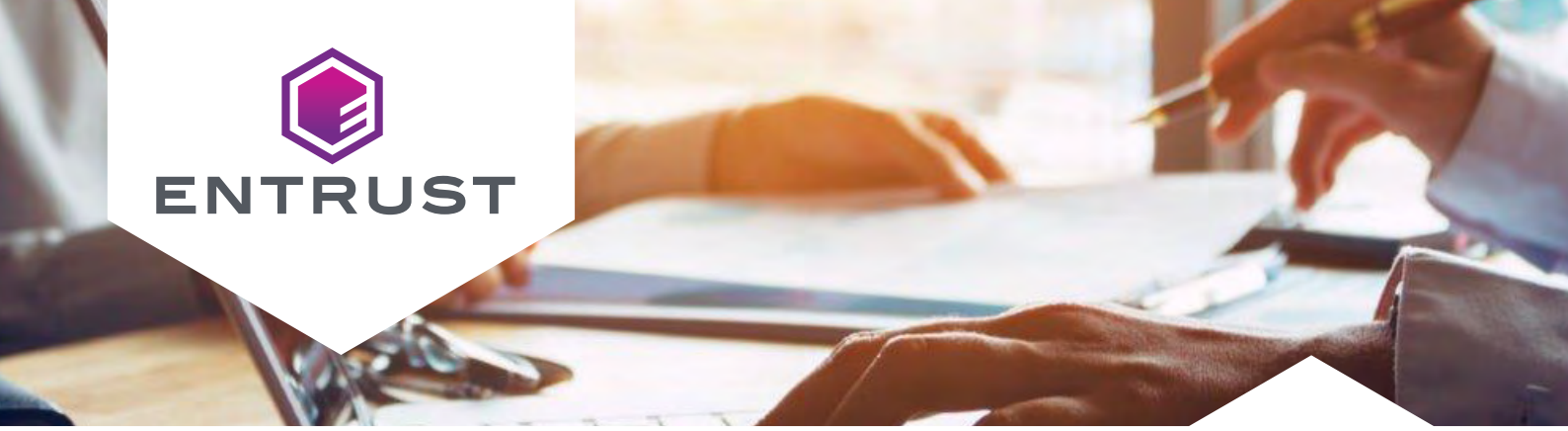
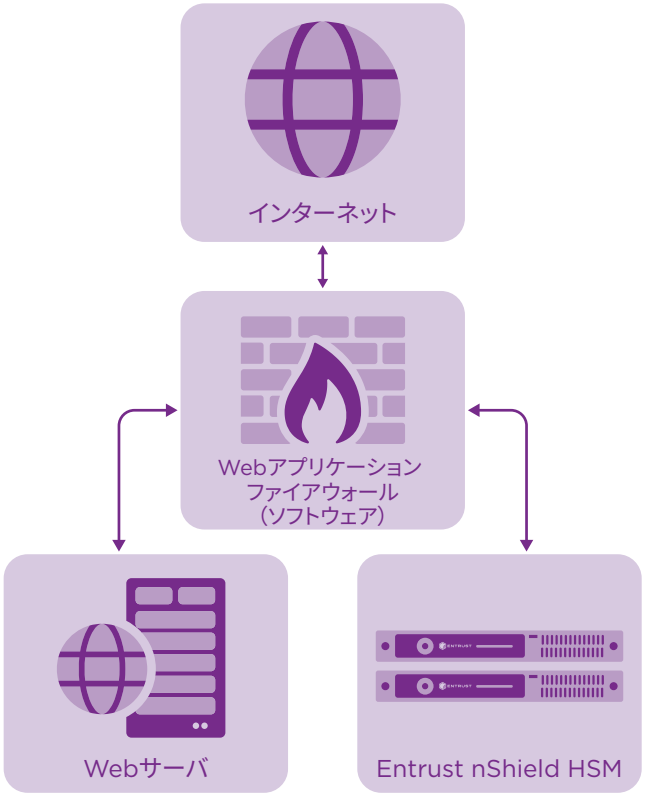


Entrust nShieldハードウェア・セキュリティ・モジュール（HSM）によりWebアプリケーションファイアウォールのセキュリティを強化

マスター鍵に対する高保証の保護を実現

ハイライト

- 詐欺、データ盗難、その他のサイバー攻撃からWebサイトとアプリケーションを保護
- 堅牢なアクセス制御メカニズムを用いて慎重に設計された暗号境界内で鍵と証明書を保護し、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
- 要求が高まるトランザクションレートをサポートすべく優れた性能を発揮
- 監査とデータセキュリティ規則の遵守を推進



主要なWebアプリケーションファイアウォールがnShield HSMを使用して、秘密鍵とパスワードの暗号化に使用されるマスター鍵を保護

詳細はこちらをご覧ください：ENTRUST.COM/ja/HSM

nShield HSMによりWebアプリケーションファイアウォールのセキュリティを強化

課題：接続性の向上が新たな攻撃につながっている

Webアプリケーションとクラウドベースのサービスは、今日の企業にとって不可欠なツールですが、同時に、データセキュリティに関するさらなるリスクも生み出しています。企業はリスクに対応するために、Webアプリケーションファイアウォール（WAF）を導入しており、これにより、トラフィックをフィルタリングおよび監視し、クロスサイトスクリプティング、SQLインジェクション、ゼロデイエクスプロイト、マルウェア感染、なりすまし、その他の脅威による攻撃を検出、ブロック、そして防止することができます。

WAFは暗号化を使用して検証済みの接続を確保し、データの機密性と整合性を保護しますが、これには、暗号鍵の強力な保護を組み合わせる必要があります。暗号鍵を暗号境界外に保存すると、組織が攻撃に対して脆弱になると同時に、誤った安心感が生まれる恐れがあります。

また、PCI DSSや国内の重要なインフラストラクチャ規制といった多くのコンプライアンス要件により、暗号鍵の強力な保護が求められています。鍵を保護するためにハードウェア・セキュリティ・モジュール（HSM）を使用することで、コンプライアンス要件を満たすだけでなく、セキュリティ業界で認められているベストプラクティスを実行することができます。

ソリューション：nShield HSMと統合したWebアプリケーションファイアウォール

次世代のWebアプリケーションファイアウォールは、企業が攻撃をブロックして検出し、防止するだけでなく、コンテンツを暗号化して、検証済みの接続と機密データの保護を保証できるようサポートします。Entrustハードウェア・セキュリティ・モジュール（HSM）は、主要なWebアプリケーションファイアウォールと統合して、すべての秘密鍵とパスワードの暗号化に使用されるマスター鍵、およびSSL/TLS暗号化に使用される秘密鍵を保護し、信頼の基点を提供して、ネットワークセキュリティを強化します。nShield® HSMシリーズは、FIPS140-2およびコモンクライテリア認証を取得しており、Webアプリケーションファイアウォール環境がコンプライアンス要件を満たしていることを保証します。

nShield HSMによりWebアプリケーションファイアウォールのセキュリティを強化

nShield HSMの特異点

Entrust nShield HSMは、専用の強化された環境内で特権アカウント向けの鍵とパスワードを保護します。認定された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済みで監査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のセキュリティを保護
- 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に保証
- 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
- 要求が高まるトランザクションレートをサポートすべく優れた性能を発揮
- 重要なインフラストラクチャ、政府、銀行、その他の業界に関連する規則への準拠をサポート

Entrustは、ソリューションおよびアプリケーションプロバイダーと数十年にわたって協力し、次のようなデータ保護に関連するさまざまなビジネス課題に取り組んできました。

- モノのインターネット向けのデバイス資格情報
- クラウドコンピューティング、ビッグデータ、およびアプリケーションのセキュリティ
- 法令と業界における規則の遵守
- 知的財産の保護
- 安全な資格情報の発行

nFinityパートナー

Palo Alto Networks® 次世代ファイアウォールはnShield Connect HSMと統合して、秘密鍵とパスワードの暗号化に使用されるマスター鍵のセキュリティを強化します。また同HSMは、SSL/TLS復号化プロセスで使用される秘密鍵を保護および管理し、完全なネットワークセキュリティ体制を強化する信頼の基点を提供します。

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。

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