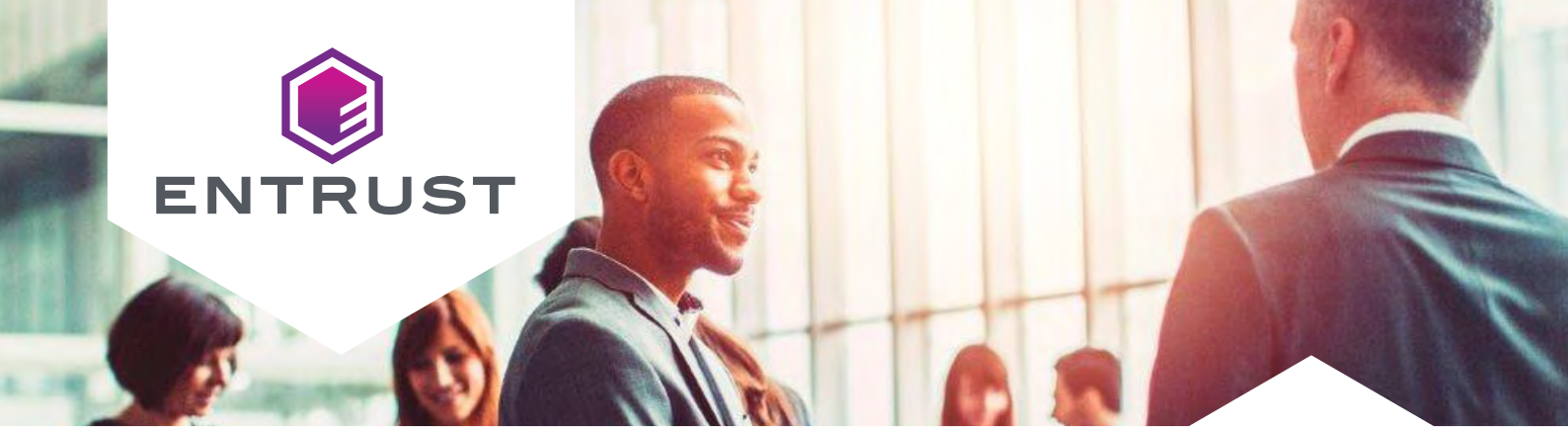


Entrustは、企業固有のセキュリティニーズに対応する、自己管理型PKIソリューションを提供します

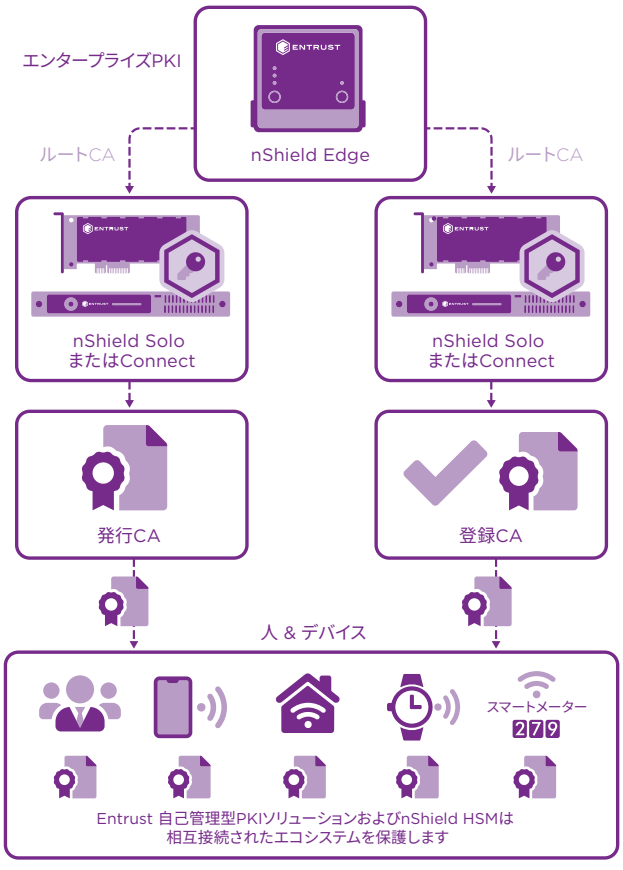
Entrustサービスとハードウェアセキュリティモジュールを使用して、セキュリティで保護されたID管理ソリューションを展開および維持します

ハイライト

- 個人とデバイスのIDの保護
- 適切なプロセスと手順の開発
- 既存のPKI展開の状態の評価
- 高まる需要に対応するためのPKIの移行
- セキュリティ監査とコンプライアンスの促進

問題：相互接続されたテクノロジーの採用の増加により、既存の公開鍵基盤（PKI）の機能が限界まで使用されているため、新しいものを立ち上げる必要性が求められている。

暗号化対応アプリケーションの使用の増加とモノのインターネット（IoT）の影響により、PKIに前例のない新しい需要が生まれています。資格情報の要件の拡大と、デバイスやセンサーの緊密なネットワークエコシステムへの安全な接続方法を管理する必要性により、企業は既存のPKIの状態を再評価することが求められています。変化するセキュリティ標準と組み合わせて、企業はPKI実装戦略を再検討、または再設計したり、また新しい、より堅牢な展開に移行しています。



詳細をチェック：ENTRUST.COM/ja/HSM

企業固有のセキュリティニーズに対応する、自己管理型PKIソリューション

課題：セキュリティをさらに重視するアプリケーションの運用上の要求を満たす、エンタープライズPKI全体で、強力な信頼の基点を維持する

PKIを使用するセキュリティを重視するアプリケーションでは、秘密鍵を支えるセキュリティが必要です。2020 Ponemon Institute PKI動向調査によると、デジタル証明書を使用する上位3つのアプリケーションには、公開Webサイト用のSSL / TLS、パブリッククラウドベースのアプリケーション、エンタープライズユーザー認証が含まれます。デジタル証明書により、アプリケーションとデバイスの識別、および信頼できるエコシステムへの認証が可能になります。これには、自動化された信頼できる方法で、増加する秘密鍵の保護と管理が必要です。

ソリューション：Entrustの自己管理型PKI製品は、コンサルティングサービスと適切なセキュリティハードウェアを組み合わせて、要件の定義から展開およびトレーニングまで、顧客を支援します。

エンタープライズPKI要件は、通常、ビジネス、クライアント、サポートするアプリケーションに応じて固有のものです。Entrustの自己管理型PKI製品は、組織のPKIの設計と実装に関する技術的専門知識と、システムに堅牢な信頼の基点を提供するために必要なセキュリティハードウェアを提供します。サービスには、初期要件の評価とプロセスおよび手順の開発、顧客が現在および将来の要件を満たすPKIを展開できるようにするために必要なインフラストラクチャの設計と実装が含まれます。コンサルタントは、高可用性と冗長性を必要する運用設定、または顧客による独自のPKIスキルセットの開発を支援するラボ環境をサポートできます。PKIを初めて展開する顧客向けに、サポートするセキュリティハードウェアと組み合わせた文書と展開サービスが提供されます。既存および拡大中のPKI展開を持つ顧客けには、ヘルスチェック、およびセキュリティハードウェアとともにSHA移行サービスが提供されます。

Entrust nShield® ハードウェアセキュリティモジュール（HSM）は、PKI展開の保証レベルを向上させます。Entrust nShield HSMは、認定された分離環境で基盤となる秘密鍵を保護・管理することを目的とし、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、Microsoft、Red Hat、Entrust、RSA、InstaのPKIをサポートします。

企業固有のセキュリティニーズに対応する、自己管理型PKIソリューション

Entrust HSMを自己管理型PKIと併せて使用する理由は？

セキュリティがより重視されたアプリケーションと接続されたデバイスの展開により、PKIに対する需要が高まり、ドメイン間で発行された個人証明書とデバイス証明書のルート認証局（CA）の秘密鍵だけでなく、それらの登録も保護されることが期待されています。秘密鍵を保護するためにHSMを使用していない組織のPKIは、混乱に対して脆弱なままであり、深刻な結果を招く可能性があります。HSMは、セキュリティが重要な鍵を盗難や不正使用から保護し、フェイルオーバーをサポートすることで、ライフサイクル全体の管理を可能にする強化された環境を提供します。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、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 + Entrust 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。

- ルートCAと登録鍵を安全で改ざん防止環境に保存する
- 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

Entrust nShield HSMは、仮想化環境を含む企業全体のID資格情報の管理を簡素化し、組織がペイメントカード業界データセキュリティ基準（PCI DSS）やペイメントサービス指令（PSD2）などの監査およびコンプライアンス要件を満たすのに役立ちます。nShield HSMは、特定の顧客のニーズを満たすために、次のモデルで利用できます。

- nShield Edge HSM：オフラインルートCAおよび開発者アプリケーション用のポータブルUSB接続HSM
- nShield Solo / Solo+ / Solo XC HSM：サーバ用の組み込みPCIExpress高性能HSM
- nShield Connect / Connect+ / Connect XC HSM：データセンター用のネットワーク接続された高性能HSM

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

お問い合わせ:
HSMinfo@entrust.com