世界10大銀行の1つがEntrust nShield HSMを導入し、信頼性の高いWebサービスを顧客とパートナー企業に提供

ビジネスにおけるチャレンジ

顧客向けのオンラインサイトを持つ企業は、ユーザがサービスを利用する際にユーザ認証を行っており、世界の主要銀行も例外ではありません。インターネットとオンライントランザクションの拡大に伴い、オンラインやクラウドでやり取りされる機密データはますます攻撃の対象になっています。

オンラインサービスは、ログインメカニズムを使用してエンドユーザーのブラウザをWebサーバに接続しており、これらの接続は、インターネット上のデータ暗号化技術Secure Sockets Layer（SSL）によって保護されています。SSL標準（ブラウザの南京錠マークが示すトランスポート層セキュリティ（TLS）技術）は、あらゆるインターネット通信に対する事実上の保護基準です。

« インターネットトラフィックが増加し続け、HeartbleedなどのSSLベースのマルウェア攻撃が多発する中で、この大手銀行は、SSLトラフィックを安全に検査する機能を強化し、システムに感染し得るウイルスやマルウェアが隠れていないことを確認する必要がありました。 »

世界の大手銀行

信頼性の高いWebサービスをユーザに提供するため、企業はサービスによって処理されるデータの機密性、整合性、そして可用性を保証する必要があります。インターネットトラフィックが増加し続け、HeartbleedなどのSSLベースのマルウェア攻撃が多発する中で、この大手銀行は、SSLトラフィックを安全に検査する機能を強化し、システムに感染し得るウイルスやマルウェアが隠れていないことを確認する必要がありました。このプロジェクトでは、具体的に同銀行のパートナー企業、グループ会社、従業員が生成するトラフィックの検査に重点が置かれました。

技術的チャレンジ

ネットワークを通過する暗号化されたトラフィックの量が増加すると、悪意のあるコードが隠れて検出されない可能性があるため、SSLが攻撃の媒介となる恐れもあります。SSLインスペクションは、暗号化されたコンテンツ内に隠れている潜在的な危険要素を除外するために使用されます。

これには、Webサイトのトラフィックのインターセプト、復号化、検査、および最終デスティネーションへの再暗号化が含まれます。

ハードウェア・セキュリティ・モジュール（HSM）は、復号化と再暗号化処理に伴い使用量が増加するSSL鍵に対して、さらなるセキュリティレイヤーを提供します。トラフィックを検査し（再び復号化して）Webサーバ上に戻すためのトラフィックの復号化、検査、再暗号化の過程で、このプロセスに必要な鍵がより頻繁に取得されることになります。一般的に、使用されるすべての鍵が同じではないため、より強力な保護が必要となります。

HSMは信頼の基点を提供し、すべての重要な接続を保護するだけでなく、その信頼性を保証します。同銀行のセキュリティアーキテクトによると、HSMがなくてもインターネットのトラフィックフローを検査することは可能ですが、非常に危険です。

世界の大手銀行

そのため、Webトラフィックの復号化技術を保護する、つまり、復号鍵を安全に保護する必要があります。まさにこれこそがHSMの役割です。

ソリューション

同銀行はEntrust nShield Connect HSMを導入し、約10km離れた2か所のデータセンターで「アクティブ・アクティブ」構成を採用しました。このHSMは、現在45台のプロキシサーバのセキュリティ要件を満たし、十分に拡張可能な容量を提供しています。

結果

Entrust nShield HSMは、レガシーシステムの少なくとも5倍の容量を達成すると見込まれています。これにより、企業は、潜在的な悪意のあるコードが隠されていないかインターネットトラフィックを検査し、システムの成長に合わせてセキュリティを確保できます。

10年以上にわたってEntrustと協力関係にあるこの世界的な大手銀行は、テクノロジーに関するEntrustの豊富な経験とセキュリティ問題への対応力を評価し、Entrustを事実上のHSMプロバイダーとして選択しました。Entrustの専門サービスチームは、HSMのインストールと、同銀行の行員を対象にしたHSMの使用方法に関する研修にも採用されました。

世界の大手銀行

ビジネスニーズ

- 信頼性の高いWebサービスをユーザーに提供

技術的ニーズ

- 増加する内部インターネットトラフィックを監視し、監視技術を保護
- 組織の包括的なITインフラストラクチャを保護

ソリューション

- 「アクティブ・アクティブ」構成を採用するEntrust nShield Connect HSMでSSL鍵を管理・保護

結果

- FIPS 140-2レベル3およびコモンクライテリアEAL4+認定のセキュリティ
- レガシーシステムの5倍の容量
- 将来のニーズに合わせて簡単に拡張可能

ENTRUSTについて

Entrust は信頼される認証、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、国境を越えた移動、買い物、電子政府サービスへのアクセス、企業ネットワークへのログインといったさまざまな場面で、シームレスで安全なユーザー体験がこれまで以上に求められています。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のネットワーク、150か国以上に顧客を擁するEntrustは、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