cpl.thalesgroup.com

THALES
Building a future we can all trust

IoTにセキュリティ（S）をプラスする「IoSTプラットフォーム」の「信頼の基点」として活躍するタレス ProtectServer HSM

サマリ

IoT（Internet of Things）、モノのインターネットが急速に進展しています。IoTデバイス数は、2022年には世界で300億台を超えました[1]。

それに伴い、IoTデバイスをターゲットにした攻撃は増大するばかりです。企業が「IoTシフト」によって新たなビジネスモデルを創造していくためには、適切なセキュリティ要件を満たす必要があります。その一つとして、データ暗号化や認証などに利用される暗号鍵の適切な管理が求められますが、そのためには暗号鍵に関する技術とノウハウが必要となります。

そこで、大日本印刷株式会社（以下、「DNP」と略記）が提供するのが、顧客のIoTシステムに暗号鍵管理機能を簡易に組み込むことが可能なIoST（Internet of Secure Things）プラットフォームです。

IoSTプラットフォームは、暗号鍵をあらかじめ埋め込んだSAM[2]をIoTデバイスに実装し、SAMに格納された暗号鍵を使ってIoTデバイスとクラウドが暗号化と復号を行いながら情報をやりとりすることで、IoT環境におけるEnd to Endの安全な情報流通を実現します。SAMはIoTデバイスの信頼性を保証するためのRoot of Trust（信頼の基点）として使用され、トランスアンカーとなる情報を格納しています。しかし、これをシステムとして利用するためには、IoTデバイスにSAMを実装するだけでなく、クラウド側にもトラストアンカーを管理するシステムが必要になります。

このトラストアンカーの管理システムにおいて重要なの役割を担うのが、タレスのHSMです。タレス ProtectServer HSMは、強固な耐タンパ性を備えたHSMハードウェア内で暗号処理を完結させて、IoSTクラウド側での暗号鍵管理に高い信頼性をもたらしています。

選定のポイント

DNPは1876年の創業以来、約150年の長きにわたって、印刷会社の事業の根幹として情報セキュリティの三大要素である機密性・完全性・可用性を自ら実現し、顧客から預かった重要情報を大切に守り続けてきました。

さらに、1981年からICカードを開発しており、国内外のクレジットカードブランド認定やISO/IEC 15408 (Common Criteria) 認証取得などを通じ、ハイレベルなセキュリティ技術とノウハウを蓄積してきました。

IoSTプラットフォームのシステム構築にあたっても、セキュリティの要となる暗号鍵管理には、顧客満足のため高いレベルの技術要件を設定しました。

タレスのHSM、特にそのラインナップの中からタレス ProtectServer HSMを採用した理由はファンクションモジュールというツールキットが提供され、複雑な暗号処理を行う独自ファームウェアを開発しやすい柔軟性、カスタマイズ性を持つことが挙げられます。また、金融等の重要情報を取り扱う業界で求められる物理的な耐タンパ性を持つFIPS 140-2 Level 3取得製品であること、楕円曲線暗号 (ECC) に対応していることや、スワップ可能なAC二重化電源を採用し、障害機を自動的に切り離せるなど、可用性の高い冗長構成を構築できる点も評価しました。

すでに開発経験のある他社製品とも比較しましたが、1台あたりの価格差が大きく、冗長構成を考える上で選定する大きな要素になりました。その結果、厳しい技術要件を満たしたうえで、圧倒的なコスト優位性を誇るタレス ProtectServer HSMを採用しました。

ソリューション

IoSTプラットフォームの開発において、最初はセットアップやファームウェア開発が手探り状態だったものの、開発環境構築からその後の実開発までタレスのSEがサポートに入ったことで、予定通りのスケジュールで本番商用サービスを開始できました。

DNPのIoSTプラットフォームは、HSMを用いて安全な暗号鍵管理が行えるため、耐タンパデバイスの使用が求められることが多い金融業界や自動車業界で評価され、導入が進んでいます。

その一例が、金融機関店舗に設置した入出金機、出納機のセキュア遠隔保守サービスです。従来、金融機関は外部とのネットワーク通信を避けてきましたが、SAMを埋め込んだセキュアIoTゲートウェイを用いた認証と暗号化通信を行うことで、インターネット経由の高セキュリティな情報収集が可能になり、遠隔保守のための外部通信が行えるようになりました。

クレジットカード決済端末においては、実装したSAMでカード情報と決済電文を暗号化し、IoSTプラットフォーム経由で決済インフラへ送信することで、クレジットカード業界の情報セキュリティ規格であるPCI DSS対応を実現しています。

また、自動車のデジタルキープラットフォームも支えています。スマートフォンアプリに組み込んだソフトウェアSAMを用い、スマートフォンへデジタルキーを安全に配信・保管し、堅牢化によりアプリのハッキングと電子鍵の搾取を防ぎます。

タレスのHSMは高セキュリティを求められるさまざまな分野で用いられていて知名度が高く、顧客への説明責任を容易に果たせるのも導入効果のひとつです。FIPS 140-3、耐量子計算機暗号など、最新の暗号技術へ確実に対応していく将来性も安心感につながります。

IoSTプラットフォームは、IoTデバイスの企画設計段階からセキュリティ対策を施す「セキュリティ・バイ・デザイン」を実現するための環境を顧客に提供して、IoTビジネスの拡大を支援していきます。

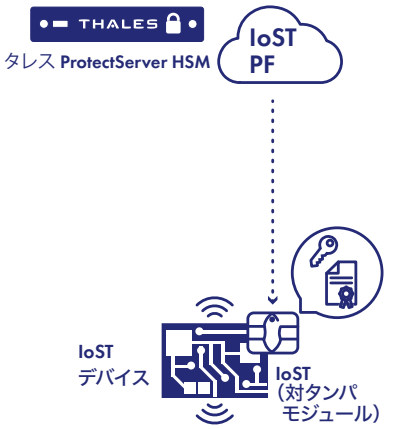
1 出典：総務省 情報通信白書（令和4年版）

2 SAM：Secure Application Module。ICチップなどのセキュアエレメント上に、暗号鍵保護やデータ暗号化など、サーバと安全にデータのやりとりをする機能を搭載した耐タンパモジュール。セキュアエレメントを組み込むことが出来ないデバイスには、ソフトウェアで耐タンパ暗号モジュールを提供する。

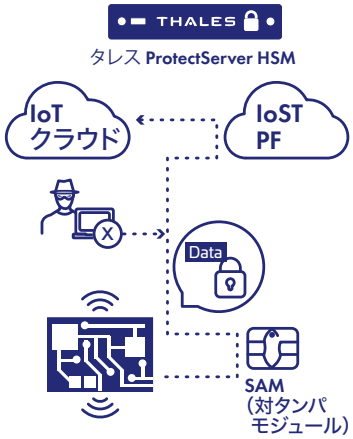
IoSTプラットフォーム 3つの機能

機能

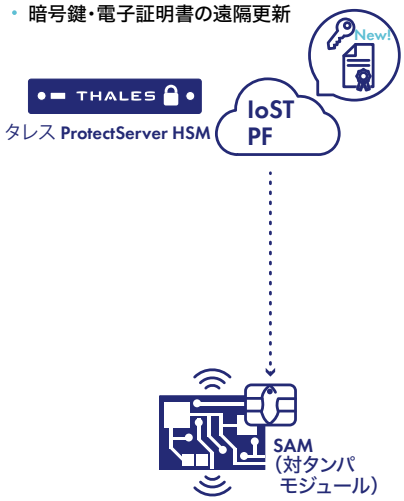
- デバイス認証用の個別データ生成・管理



- IoTデータに対する暗号化/復号



- 暗号鍵・電子証明書の遠隔更新



導入効果

- 耐タンパデバイスによる安全なデバイスIDや暗号鍵の保護
- セキュリティ・バイ・デザインの実現

採用事例

- 金融機器 遠隔監視サービス
- 決済端末 遠隔保守サービス
- デジタルキープラットフォーム

課題

- IoTサービスに「セキュリティ」を付加するプラットフォームを構築するにあたり、クラウド側の暗号鍵管理には、最高レベルの耐タンパ性を保証する「専用ハードウェア」が必須と判断した
- 「FIPS 140-2 Level 3以上」が技術要件の大前提
- 複雑な暗号処理を実行させるため、カスタマイズ性の高いHSMを求めた

ソリューション

- FIPS 140-2 Level 3、およびECCに対応し、冗長構成を組みやすいタレスのHSMを選定
- タレスのラインナップから、独自ファームウェアの開発・実装がしやすく、低コストであるThales Protect Server HSMを採用

メリット

- すべての暗号鍵処理は、侵入に強く耐タンパ性を備えたFIPS認証取得済みのハードウェア内で行われ、セキュアな暗号基盤を実現
- 高セキュリティが要求されるさまざまな分野で実績あるタレスのHSMをクラウド側のRoot-of-Trustに据えることで、顧客に安心感を与え、信頼を獲得
- ファンクションモジュールなどのツールキット充実により、独自ファームウェアを開発・実装しやすかった。稼働開始後のファームウェア修正も容易だった
- スワップ可能なAC二重化電源、障害機を自動的に切り離す機能などを活用して、可用性の高い冗長構成を構築
- FIPS 140-3、耐量子計算機暗号など、最新技術への対応が保証されており、顧客のビジネスを将来にわたって確実に支えるプラットフォームを構築できた

「IoSTプラットフォームは今後、欧米で重要インフラ分野の実質的なセキュリティガイドラインになりつつあるIEC62443や医療機器のサイバーセキュリティガイダンスであるIMDRFなどのさまざまな規格、ガイドラインへの対応を目指し、産業機器・産業ロボット、医療分野にも展開していく計画です。ゆくゆくはサプライチェーン全体をカバーする社会インフラへと拡張していくことも考えていますので、タレスには、より幅広い領域での協業を期待しています。」

– 大日本印刷株式会社 情報イノベーション事業部
PFサービスセンター IoSTプラットフォーム本部
サービス開発第1部 企画販促グループ
主幹企画員
大野 毅氏

DNP
大日本印刷

タレスのProtect Server HSMについて

タレス ProtectServer HSM（ハードウェアセキュリティモジュール）は、暗号化、署名、認証サービスを提供しながら、暗号鍵を保護します。

ユーザーと開発者は、暗号化とHSMを多数のサードパーティソリューションやカスタムアプリケーションにシームレスに統合することができます。カスタマイズ用ソフトウェア開発キット（SDK）により、HSMの安全な境界内でカスタム固有の機能モジュールを開発、ダウンロード、保存できます。

ProtectServer HSMには、安全な暗号化処理を高保証で実行するため、FIPS140-2レベル3検証済みの暗号化モジュールが含まれています。業界標準のセキュリティアプリケーション向けに構築されたProtectServer HSMは、改ざんから保護された境界内で機能し、気密性の高い情報、暗号鍵、PIN、データ用の安全なストレージを提供します。

タレスについて

皆様がプライバシー保護を信頼して任せている相手は、そのデータを保護するためにタレスに頼っています。データセキュリティに関しては、組織が直面する決定的な局面は次々と増え続けています。その局面が暗号化戦略の策定、クラウドへの移行、コンプライアンス要件の順守のいずれであっても、デジタルトランスフォーメーションを保護するためにタレスに頼ることができます。

決断の瞬間のための、確実なテクノロジー。

> cpl.thalesgroup.com/ja <

お問い合わせ先 – cpl.jpsales@thalesgroup.com すべてのオフィスの所在地と連絡先情報につきましては 、cpl.thalesgroup.com/ja/contact-usをご覧ください。