yubico

世界最小のハードウェア・セキュリティモジュール（HSM）で暗号鍵を保護

YubiHSM 2は、FIPS 140-2認証取得済みのLevel 3のソリューションまたはFIPS認証未取得のソリューションのいずれかをお選びいただけます。いずれも同じ機能が装備されており、どちらをお選びになっても、従来型のHSMよりもはるかに小さく、安価なコストで、アプリケーション、サーバー、コンピューティングデバイスの暗号鍵をハードウェアで確実に保護できます。

ソフトウェア内に保存する暗号鍵は脅威に対して脆弱

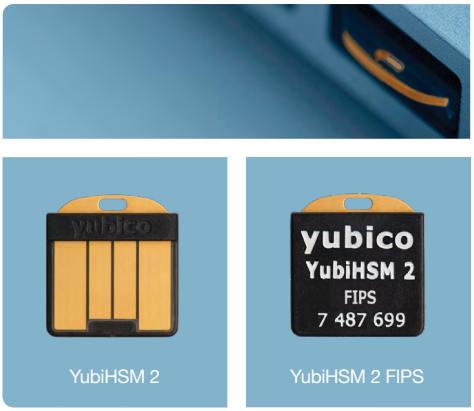
サイバー犯罪による被害額は2015年の3兆ドルからはるかに増加し、2021年には全世界で6兆ドルとなることが予測されています[1]。攻撃が洗練されてきているため、ソフトウェアに保存したサーバー用の暗号鍵の脆弱性が増しています。例えば、証明書認証局（CA）から秘密鍵を盗んだ攻撃者は、対象のウェブサイトになりすますことができます。

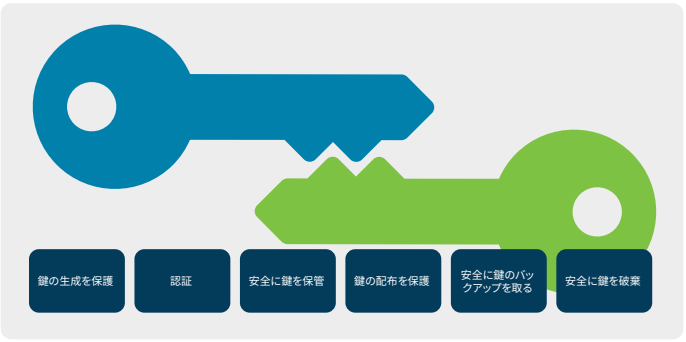
鍵のセキュリティを別次元に高めるYubiHSM 2およびYubiHSM 2 FIPS

従来型のハードウェア・セキュリティモジュール（HSM）の複雑でコストが大きいという問題を排除しつつ、ハードウェアに保存されたアプリケーション、サーバー、コンピューティングデバイス用の暗号鍵の保管とオペレーションを確実に保護します。不正利用を防止するYubicoのHSMソリューションを使用すれば、ポータブルな「ナノ」フォームファクターにより、さまざまなデバイスと場所を柔軟に保護できるため、低コストで高いセキュリティ対策を実現し、高い費用対効果を達成できます。YubiHSM 2とYubiHSM 2 FIPSを導入すれば、組織は、攻撃者、マルウェア、悪意のある内部関係者が暗号鍵を複製するのを防止できます。企業はオープンソースのSDK 2.0を使用して、YubiHSM 2またはYubiHSM 2 FIPSいずれかのHSMオプションを素早く統合できます。

暗号鍵のハードウェア保護を強化

ソフトウェアに保存した暗号鍵は複製可能なだけでなく、意図せぬ配布や遠隔地からの盗難に対して脆弱です。厳格な手続きがない場合、管理者や悪意のある内部関係者は、バックアップを取る目的で暗号鍵を簡単に複製し、USBメモリに保存することや、FTPで転送すること、クラウドストレージ・サービス経由で他の人物と共有することができます。さらに、高度な攻撃者は、管理者アクセスを掌握するか、もしくはサーバーにプログラムをインストールさせ、暗号鍵を検索するトロイの木馬を侵入させ、鍵をコピーしてAlphabayなどのダークウェブのサイトで販売・配布することができます。





暗号鍵のライフサイクルを保護

ハードウェアベースのHSMソリューションは、鍵の意図せぬ複製や配布と保存された鍵の遠隔地からの盗難を防止し、安全な鍵の保管とオペレーションを可能にします。

- 監査ログを使用し、不正利用を防止するハードウェアで安全な鍵の保管とオペレーションを実現。
- ハッシュ化、鍵ラッピング、非対称署名、復号化、認証など幅広い暗号機能。

柔軟に使える革新的な設計

従来型のラックマウント型、カードベースのHSMの場合、HSMのサイズの問題と導入が複雑という問題があるため、多くの組織にとって現実的な選択肢になりません。さらに、共有データセンターのラック・スペースには多くの場合、物理サーバーの筐体があり、アクセスを制限することを目的とした金属製のメッシュドアが設置されているため、利用できるスペースが限られています。

YubicoのHSMソリューションを使用することで、組織はさまざまな環境に速やかかつ柔軟に導入できるポータブルな「ナノ」フォームファクターを使用して簡単にサーバー、アプリケーション、データベース、組み立てライン、IoTデバイス、暗号通貨の取引などの安全を確保できます。

YubiHSM 2とYubiHSM 2 FIPSは、USBスロットにほぼ平らな状態で容易にフィットするため、物理的なセキュリティ用の筐体を妨害せず導入できます。

- さまざまなデバイスと場所での柔軟な導入と使用を可能にする「ナノ」フォームファクター
- USB-Aポートに完全に収まるHSM
- ネットワーク共有できるため、他のサーバー上のアプリケーションによる使用が可能

[1]Cybersecurity Ventures

低コストで高いセキュリティ対策を実現し、高い費用対効果を達成

ソフトウェアに保存した暗号鍵は、ハッカーやマルウェアによる攻撃に脆弱です。また従来型のHSMは導入にコストがかかります。

YubicoのHSMソリューションを使用することで、組織は従来のHSMにかかるコストをかけることなく、エンタープライズクラスの暗号鍵セキュリティとオペレーションを実現できます。

- 設備投資を大幅に削減：従来のHSMより最大90%安価
- 使用電力量が少なく企業のエネルギー消費量の削減が可能

導入に時間がかからず&管理が簡単

開発者はYubiHSM 2 SDKを使用することで、キーの生成とインポート、署名・検証、データの暗号化・復号化などの各種機能と共に、YubiHSM 2またはYubiHSM 2 FIPSのサポートを業務で利用する製品やアプリケーションに速やかに実装できます。また開発者は、業界標準のPKCS#11を介してこれらの機能を利用できるようにすることが可能です。

- オープンソースのライブラリを使用してのカスタムアプリケーションサポート。YubiHSM KSP、PKCS#11、およびネイティブライブラリ経由でのインターフェース
- 遠隔管理で管理の複雑さを軽減し、管理コストを削減

既存のユースケース、将来のユースケースに対応

暗号通貨の取引を保護： 暗号通貨の市場は急速に成長しており、新たに生じるセキュリティ・リスクに対する保護を要するアセットの量も増えています。セキュリティが侵害された取引もありましたが、ハードウェア・セキュリティモジュールを使用するセキュリティ・アプローチのベストプラクティスに従っていれば、それらのセキュリティ侵害はすべて防止することができたはずです。暗号通貨の取引を行うソリューションを開発している開発者は、YubiHSM 2 SDKを使用することで、YubicoのHSMを素早く統合して暗号鍵を保護し、センシティブな金融情報を保護できます。

モノのインターネット(IoT)の環境を保護： モノのインターネット(IoT)は急速に成長している分野であり、この分野ではシステムを厳しい環境[2]で使用することが多くあります。十分なセキュリティを確保しないまま暗号鍵を使用しているIoTアプリケーションが無数にあります。これまでは暗号鍵を保護してIoTゲートウェイやプロキシに証明書を登録する作業が複雑であり、コネクテッドカーのような特定のIoT環境では従来型のHSMが大きすぎて扱いにくかった、ということがその一因として挙げられます。IoTアプリケーションを開発している開発者は、オープンソースのSDKを使用することで携帯性に極めて優れたYubiHSM 2またはYubiHSM 2 FIPSを素早く統合し、暗号鍵を保護して重要なIoT環境を悪意のある攻撃者による乗っ取りから保護できます。

クラウドサービスを保護： 組織はクラウド上のデータを確実に保護しなければならないため、クラウド環境のための強固なセキュリティが不可欠です。YubicoのHSMは、データセンターに導入してクラウド・インフラのコンポーネントとして実行できます。使用中のクラウドホスティング・サービスがその一部としてYubiHSM 2またはYubiHSM 2 FIPSを実行していれば、組織は安心できます。

Microsoft Active Directoryの証明書サービスを保護： YubicoのHSMソリューションにより、ハードウェアを利用する鍵を、組織のMicrosoftベースのPKI実装に導入することができます。YubicoのHSMをMicrosoft Active Directoryの証明書サービスに導入することで、証明書認証局の秘密鍵だけでなく、秘密鍵を使用するすべての署名・検証サービスも保護できます。[3]

最後に

YubiHSM 2およびYubiHSM 2 FIPSを使用することで、あらゆる規模の組織がライフサイクル全体にかけて暗号鍵のセキュリティを強化し、リスクを減らして規制に対するコンプライアンスを確保することができます。組織はオープンソースで利用できるYubiHSM SDK 2.0を使用することで、安全なHSMのサポートを素早く簡単に多彩なプラットフォームやシステムに導入し、強固なセキュリティがこれまで以上に求められている中、既存のユースケースや将来のユースケースに対応できます

[2] https://www.smartcard-hsm.com/2017/02/14/IoT_Devices_with_SmartCard-HSM.html

[3] 備考：Microsoft Active Directoryの証明書サービスで使用するKey Storage Provider（KSP）を除き、すべてのYubiHSM 2 SDK 2.0の要素をオープンソースとして利用できます。

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
スウェーデン

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301米国
844-205-6787（フリーダイヤル）
650-285-0088