

HSM (Hardware Security Module) の機能と有効性

HSM って何？

何するものなの？セキュリティの世界にいておぼろげながらわかる方、専門の方、初めて HSM という言葉に触れる方色々です。出来るだけ判りやすい言葉と表現で HSM に関するお話をしたいと思います。PKI に精通されている方は本分を読む必要は無かろうと思います。飛ばしてください。

HSM は暗号器です。また、サーバーに繋ぐことにより暗号化に使用される鍵を作成し、サーバーの負担を大幅に軽減するアクセラレータでもあります。何故、アクセラレータが必要かという、暗号化するには暗号化鍵が必要です。この鍵は簡単に解読されないように出来る限り複雑なランダムな基本数の組合せで出来ている必要があります。その計算には高度な数学的計算が必要ですがサーバーの負荷が大きくその他の機能に影響することがあります。その機能を補完するのに HSM が使用されると、作成した鍵を安全に保存するのに使用されます。



鍵って何？

暗号化には暗号アルゴリズムという暗号化する場合の計算方式があります。その計算の元となる情報が鍵と呼ばれるもので、高度な数学的計算をして真似の出来ない鍵を作るには相当な負荷が掛かりますので、その部分を専門の HSM にやらせようということで HSM の存在意義の一つがあります。同じ暗号アルゴリズムを使っても強い、弱いがありますがこれは鍵の精度によるものです。

その鍵で暗号化して、復号化しますが二つの鍵を使い、一つは暗号化、もう一つは復号化する方法があります。この二つの鍵(公開鍵/秘密鍵)を使用するのが PKI = 公開鍵基盤という仕組みで現在使用されるもっとも信頼できる情報セキュリティの仕組みです。

鍵が解読されたり、使用されてしまうと暗号化された情報が解読されたり流出する可能性があり、またネットワークアクセス認証が簡単に行われてしまいます。そのため“電子”の金庫 HSM に保管する必要があります。流出すると暗号メール等は暗号メールではなくなり、人事情報などが解読されることとなります。知らないうちにデータは全くの他人、悪意のある人に平文で読まれる可能性があります。

鍵は HSM を使用しない場合、サーバーで作られこの鍵も暗号化されていますが鍵の保管はサーバー上では色々な方法で保護されディスク上に保管されます。サーバーの不具合、ハードディスクのクラッシュには同時にこれら鍵を失うこととなります。更に高度なセキュリティを確保するのに HSM が使用されています。

HSM の使い方

先の述べましたように HSM は暗号化の性能向上と、鍵の安全を確保するためのハードウェアで出来たデバイスです。通常の PC サーバーを HSM として使用されるものや、専用 ASIC でハードウェアを構成するものがあります。HSM は二種あり、HSM 本体 (HSM ボックスと呼ばれる場合もあります。) とスマートカードや USB デバイスです。これらを総称して HSM と言います。スマートカードや USB デバイスはボックスで作成した鍵や、証明書を保存しておくのに使用されます。

両方使用するのが一般的ですがどちらか一方を使用してもある程度のセキュリティは確保できます。経済性とセキュリティポリシーにより選択されます。



専用 ASIC 型 HSM

* AEP Networks, Inc. Spyrus, Inc.



各社 PC サーバー型 HSM

各製品の機能は細部において仕様の違いがありますが基本的には鍵の生成と、保管及び証明書の確認署名です。また、処理速度に違いがあり、規模、用途により選択肢があります。価格も其々ですが凡そサーバー型は1台250 - 400万円、専用型も同様ですが処理速度が速いようです。専用 ASIC で同時に6個の鍵を生成できるものもあります。右上の写真は現在最小の ASIC 型 HSM で価格は20万円と ASIC の更なる集積化で、小型で廉価になっています。各社 RSA4096ビット鍵長に対応しています。また、最強の ECC (楕円曲線暗号) を採用し今後の長鍵時代を高速処理できるよう対応しているものもあります。鍵長とは鍵を生成する時に 256, 1024, 2048, 4096 ビットのようにビット数が大きければそれだけ解読が困難なため、現在は 4096 ビットも視野に入れて各社対応しています。

ネットワーク型とサーバー接続型

上記の殆どはネットワーク型で PKI サーバーのあるネットワーク上に設置し、サーバーのリクエストに応じて鍵の生成、証明書の検証を行うようになっています。先の USB 接続型は例えばマイクロソフトPKIサーバー (Microsoft Certificate Server) のUSBポートに接続しサーバーの補助暗号化アクセラレータとして使用されます。簡単に PKI 構成が設定できる製品です。価格も15 - 20万円と非常に廉価です。



J-SOX や電子文書法、電子署名法などのコンプライアンスには文書、データの暗号化や完全性 (変更がされておらず信頼に足りるもの) が要求されております。これら文書へのアクセス、変更権限、データ保全に欠かせない、必要な仕組みを提供できる仕組みがPKIです。以下の世界標準がPKIを指定しています。

CobiT、 Process Control & Management
 COSO、 Process Enterprise Risk Management
 ITIL、 IT Service Process
 ISO17799, IT Security Program Guidance
 NIST SP800 for FIPS

日本では J - SOX と呼ばれる金融商品取引法に準じてポリシーを作成する必要があります。その適用を受けるのはアメリカの SOX 法に習い“上場会社”ということになりますが、その連結決算を行う会社にも必要です。また、時間差があると思われませんが密接な関係にある協力会社もそれに準じて対応が要求されるでしょう。

例えば社内に配布する文書の流出防止に公開鍵で暗号化し、特定の社員にのみしか解読できないようにして配布し、変更が出来ないように設定することも可能です。商法では10年間の法定文書の保管義務がありますが、2004年の電子文書法で電子的に保管された文書でも、商法の定めを満足する条件を満たせば有効であるとされました。条件とは改ざん防止の仕組みを付すること、つまり文書の完全性 (変更がされていない信頼できる) が要求されています。簡単に申しますとPKIがこの要求事項です。

文書の真実性の確保

真実性とは、紙文書を適切かつ確実にスキャンし、電子化した文書とオリジナルを比較して、異なっていないことを証明できることです。つまり、電子データの内容が改変されたり、記録自体の消去や差し替えが行われたりした場合に、そのことを証明できる仕組みを導入することが求められています。真実性を確保するための技術要件としては、主に「電子署名」と「タイムスタンプ」があり、電子署名は電子データの作成者と変更がないことを証明する機能を有し、タイムスタンプは作成時刻と非改ざんを証明する機能が要求されます。

電子署名は、入力単位ごとに入力業務を行う人、またはその人を直接監督する人の電子署名を付け、一連の書類がある場合は各書類単位で電子署名が必要です。また、署名に用いる電子証明書は「電子署名及び認証業務に関する法律(電子署名法)」に規定されているいわゆる「特定認証業務」の認定を取得している認証局が発行するものを用いる必要があります。このような認証局は2005年5月時点では政府認定の17局がサービスを行っています。タイムスタンプは、日本データ通信協会による「タイムビジネス信頼・安心認定制度」の認定を取得したタイムスタンプ局の発行するものを利用することになっています。

セキュリティと電子文書、企業情報防衛は連動して動いています。電子文書関連の法律から始まる業務の電子化とセキュリティはすでに法制化されており、改正の必要な部分も技術の進歩で出てくると可能性はありますが、J-SOXは本会計年度から適用され、電子文書法は2004年から、電子署名法は2005年から施行されています。

ICHはそのような時代に必要で機密保持、文書の暗号化、真実性が確保できるPKIシステムを15万円から始まるHSMから大企業向けHSMとPKIシステムを提供しております。

以上