情報を強固に守る仕組みを内蔵したIBMのハードウェア・セキュリティー・モジュール

高い安全性を認証されたIBMハードウェア暗号化機構とその有効活用

IBMのハードウェア暗号化機構には、データ暗号化／復号のための暗号鍵をハードウェア暗号化機構の外に持ち出せない仕組みを実装した「ハードウェア・セキュリティー・モジュール」があります。個人情報漏洩に対する社会の目が厳しさを増す今、ハードウェア・セキュリティー・モジュールは、個人情報や機密情報を守るための手段として注目を集めています。

本稿では、ハードウェア・セキュリティー・モジュールの仕組みとIBM製品の特徴、有効活用場面について解説します。

1. IBMの暗号処理への取り組み

IBMの暗号処理研究は1960年代に始まり、1971年には「Lucifer」という暗号方式を開発・商用化しました。1970年代後半には、Luciferの改良版である「DES（Data Encryption Standard）」を米国標準暗号方式の候補として米国規格基準局に提案し採用されました[1]。現在DESそのものは、コンピューター処理スピードの向上に伴い暗号強度不足と判断されて使われることが少なくなりましたが、DESを3重に施して暗号強度を向上した「Triple DES（3DES-EDE）」は、後継の標準暗号方式の「AES（Advanced Encryption Standard）」とともに、業界標準として現在もさまざまな場面で利用されています。

また、IBMでは、DES標準化とほぼ同時に、DESに特化したハードウェア暗号化機構「IBM 3845」「IBM3848」の提供も開始しました[2]。以来、IBMは継続的にハードウェア暗号化機構を提供し続けており、現在ではIBM z SystemsプロセッサーやIBM Power Systemsプロセッサーに内蔵できる、さまざまな標準暗号方式に対応したハードウェア暗号化機構を提供しています。

2. ハードウェア・セキュリティー・モジュール（HSM）とは

どのような暗号であっても、暗号鍵が分かってしまえばデータが解読できるため、暗号鍵は厳重に管理・秘匿する必要があります。暗号化処理はソフトウェアでも実装可能ですが、ソフトウェア処理ではオペレーティング・システムのメモリー上に暗号鍵が平文で露出してしまいます。このため、電子署名に使う秘密鍵やデータベース暗号化の暗号鍵のように、一定期間変更が行われないことを前提とした暗号鍵を扱う場合には、暗号化／復号処理を物理的に守られたパッケージの中でのみ行う「ハードウェア暗号化機構」が使われます（**図1**）。これは、暗号

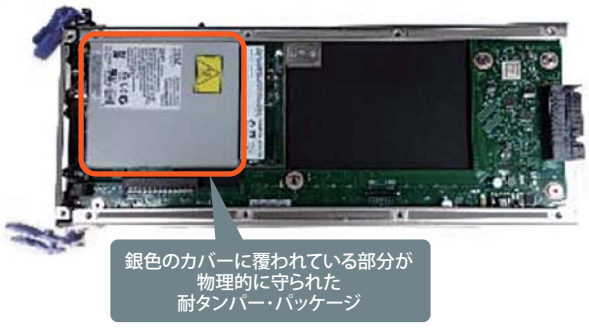

図1. IBM z13のCrypto Express5S

鍵が漏洩してしまうことによる、成りすましや大規模な情報漏洩を防ぐためです。

このようなハードウェア暗号化機構では、暗号鍵自体は暗号化機構の外部で管理・保管しますが、物理的に守られたパッケージの外にはマスター鍵と呼ばれる別の鍵で暗号化した形でしか取り出せない仕組みになっています。オペレーティング・システムのメモリー・ダンプを取得しても暗号鍵は平文では露出せず、データを復号できません(**図2**)。

さらに、ハードウェア暗号化機構は、内部の平文の暗号鍵を奪取しようとするなどの攻撃を検知すると、その痕跡を残したり、暗号鍵を含む内部保持データを消去したりする仕組み「耐タンパー機構」(「タンパー」とは「開封、改ざん」の意味)を有しています。例えば、**図1**の「Crypto Express5S」は、銀色のカバーを開封しようと傷つけたり、端子に解析装置などを取り付けてデータを解析しようとすると、それを検知して内部保持データをゼロクリアします。

このような耐タンパー機構を持つハードウェア暗号化機構を、「ハードウェア・セキュリティー・モジュール」(以下、HSM)と呼びます。

3.「FIPS 140-2」規格で最高レベルの耐タンパー性認証を取得したIBMのHSM

現在IBMは、HSMとして以下を提供しています。

- IBM z13用Crypto Express5S(IBM 4767 PCIe暗号処理コプロセッサー搭載)
- IBM zEnterprise EC12/BC12用Crypto Express4S(IBM 4765 PCIe暗号処理コプロセッサー搭載)
- IBM Power Systems用IBM 4765 PCIe暗号処理コプロセッサー

これらのIBMのHSMは、耐タンパー性に関して米国標準技術研究所(NIST)が定めるFIPS 140-2規格[3]で最高のレベル4の第三者認証を取得しています[4][5]。レベル3までの要件である、暗号方式が正しく実装されていること、HSMを開封するなどの物理的な攻撃の証跡を残すこと、攻撃を検知したらデータ消去などの対応を実行することに加えて、レベル4では、HSMの温度や電圧を変化させてタンパー検出を回避するなどのいかなる物理的な攻撃にも対応するため、温度や電圧などの環境条件が規定外となったときにもデータ消去などを行うことが要求されます。

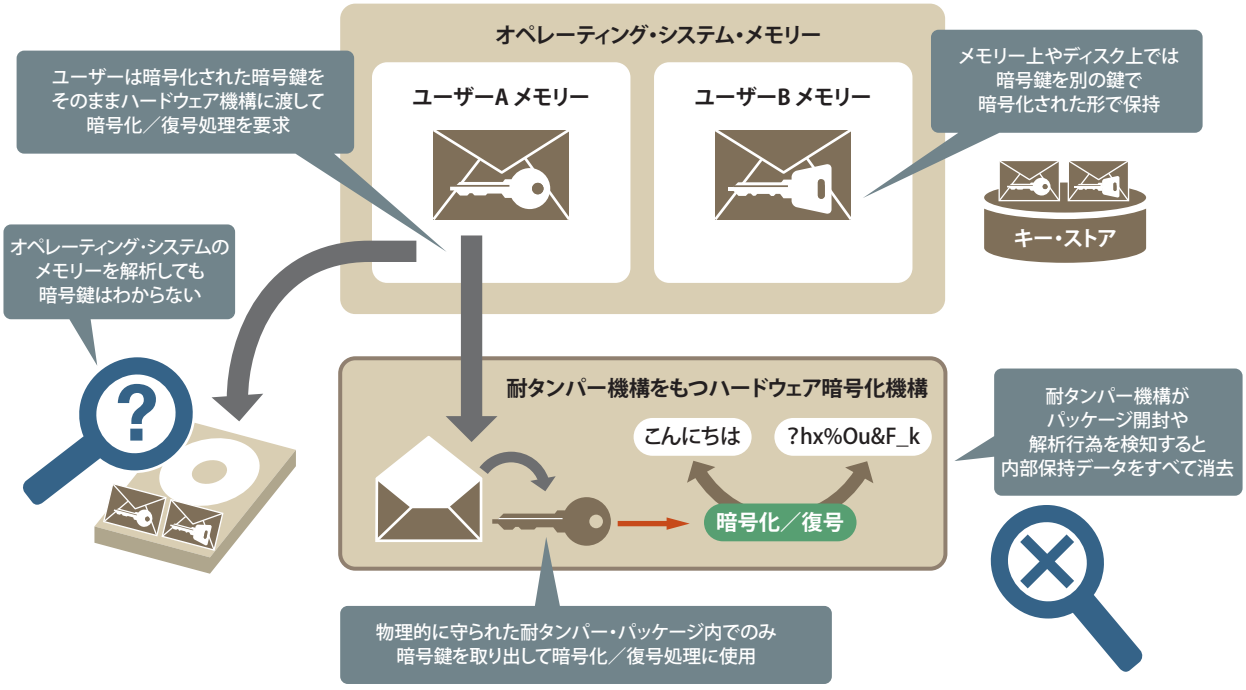

図2. HSMの仕組み

FIPS 140-2の第三者認証に申請されたもののうち、約50%にセキュリティー上の欠陥が、25%以上に暗号方式の欠陥が見つかったという事実[6]があります。認証を取得しているということは、こうした欠陥がないことが確認され、安全性が担保されていることの証です。つまり、FIPS 140-2認証を取得しているIBMのHSMは、機密情報や個人情報などの重要なデータを安全に保護できるということです。

4. HSMの活用場面とソリューション

前述のような特性を持つHSMを活用することで、企業や官公庁におけるセキュリティー対策に大きな効果が期待できます。

以下では、現在多くの企業や官公庁が直面しているセキュリティー事故のうち、可能な限り速やかな対応が求められている「標的型攻撃」や「内部漏洩」を取り上げ、HSMの有用性を説明します（**図3**）。

4-1. 標的型攻撃への対策

Wikipediaによると、標的型攻撃とは、「特定の組織内の情報を狙って行われるサイバー攻撃の一種で、その組織の構成員宛てにコンピューター・ウイルスが添付された電子メールを送ることなどによって開始される。（中略）対象とされる組織は、政府／公共サービス機関、製造業が多く、価値の高い知的財産を保有している組織が対象になっている」と解説されています[7]。

価値の高い知的財産を攻撃から守るためには、

①攻撃を受けないように防御する

②攻撃によって仕込まれたウイルスが発症し、価値の高い知的財産や個人情報が格納されたファイルなどの資源がハッカーに奪われた場合にも内容が判読できないようにする

という2つの方法が考えられます。このうち、HSMが大きく寄与するのは②への対策です。②への対策は、秘匿すべき情報を暗号化するとともに、復号に必要な暗号鍵をいかなる場合においてもハッカーに奪取されない環境を構築することです。現在、暗号方式としてAESを、鍵長として256ビットを用いた場合、30年以上の安全性が確保できる（解読不可能）と言われていますが、情報を暗号化し安全に保っても、鍵が盗まれた場合その安全性は担保されません。HSMは前章で解説したように、暗号化／復号の鍵をHSMハードウェア内に保持し、決してHSM外に持ち出せない仕組みを搭載しています。つまり、標的型攻撃で仕掛けられたウイルスによって暗号化された情報が奪取されたとしても、HSMで管理された鍵を用いて暗号化を施しているため解読不能な状態を保つことができます。よって、奪取され解読されてしまえば大きな損害につながる「価値の高い知的財産」や「個人情

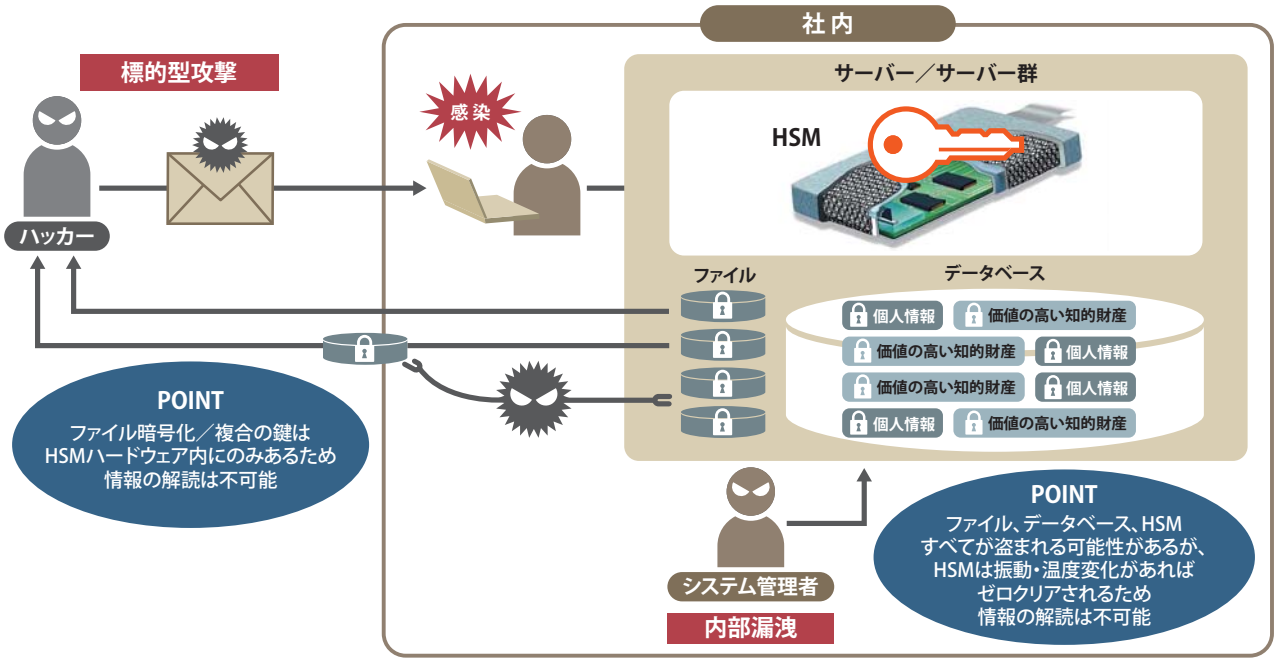

図3. 標的型攻撃と内部漏洩

報」を守る対策として、HSMは非常に有効だと言えます。

4-2. 内部漏洩への対策

内部漏洩への対策は、2014年に発覚した大量の顧客の個人情報をシステム管理者が外部に流出させ販売した事件をきっかけに必要性が叫ばれ始めました。この後、多くの企業や官公庁で内部漏洩対策が求められていますが、一つの方策だけで万全という内部漏洩対策はなかなか存在しません。

システム管理者は、システムの正常稼働のために必要なさまざまな運営に関わる作業を行うため、オールマイティーに近い権限を有していないと作業実施に支障をきたすことも稀ではありません。特にデータベースのように多くの個人情報を格納している資源の管理者は、通常時でもバックアップの取得やログのアーカイブなどの作業が必要です。また、非常時（異常時）には、バックアップ・データのリストアやログからのリカバリーによるデータの最新化やその確認など、個人情報の実体に触れなくては成しえない作業もあります。

そこで、「価値の高い知的財産」や「個人情報」を扱うシステム管理者による内部漏洩への対策として、

①情報を流出できないような対策を講じる

②その情報が漏洩した場合にも「価値の高い知的財産」や「個人情報」として意味を成さないように強度の高い鍵を用いて暗号化し復号不可状態に保つ

という2つの方法が考えられます。ただし、情報を奪取するのは、標的型攻撃の場合と異なりシステム管理者であり、情報の奪取と同時に復号に必要なHSM装置を奪取できる立場にあります。こうした場合でも、FIPS 140-2の対応レベルが高いHSMは、HSMを盗み出す際に発生する振動や温度変化などを検知して鍵をゼロクリアする耐タンパー性を実現する仕組みが実装されているため、外部侵入者より多くのシステムの資源にアクセスを許されているシステム管理者が万が一悪意を持ったとしても「価値の高い知的財産」や「個人情報を」を守る内部漏洩対策として有効です。

4-3. HSMを利用した最新ソリューション

2015年10月5日から開始されたマイナンバー制度の中でも、「価値の高い知的財産」や「個人情報」を個人番号と共に扱う、また今後扱う必要があるシステムが少なくありません。このような特定個人情報を取り扱うソリューションとして、IBMを含め多くのITベンダーからHSMを使用した「マイナンバー・ソリューション」が発表・発売されています。お客様・従業員から取得したマイナンバーを漏洩した場合には実刑を伴う罰則が適用される場合もあることから、多くのマイナンバー・ソリューションでは、マイナンバーや個人情報をHSMで暗号化して保管し、標的型攻撃や内部漏洩から情報を守る対策を施しています。このように、「価値の高い知的財産」や「機密性の高い個人情報」を安全に保管するソリューションとして、HSMの利用は拡大の兆しを呈しています。

[参考文献]

[1] IBM：世界をつなぐ暗号化技術, IBM100年の軌跡, http://www.ibm.com/ibm/history/ibm100/jp/ja/icons/cryptography/

[2] Arnold, T.W. and VanDoorn, L.P.：The IBM PCIXCC: A new cryptographic coprocessor for the IBM eServer, IBM Journal of Research & Development, vol.48, no.3/4（2004）

[3] NIST：FIPS PUB 140-2 - Effective 15-Nov-2001, http://csrc.nist.gov/groups/STM/cmvp/standards.html

[4] NIST:Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules, http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

[5] NIST：Cryptographic Module Validation Program FIPS 140-1 and FIPS 140-2 Modules In Process List, http://csrc.nist.gov/groups/STM/cmvp/inprocess.html ※Crypto Express5SはIBM 4767 として検証中

[6] NIST：Frequently Asked Questions for the Cryptographic Module Validation Program, http://csrc.nist.gov/groups/STM/cmvp/documents/CMVPFAQ.pdf

[7] Wikipedia：標的型攻撃, https://ja.wikipedia.org/wiki/%E6%A8%99%E7%9A%84%E5%9E%8B%E6%94%BB%E6%92%83（2015年10月11日）

日本アイ・ビー・エム株式会社
システムズ・ハードウェア事業本部ソリューション事業部
システムズ・ラボサービス サーバー・ソリューション
アドバイザリーITスペシャリスト

鎌田 瑞穂
Mizuho Kamata

ITスペシャリストとして、一貫してメインフレームのz Systemsハードウェアとオペレーティング・システムz/OSを担当。近年ではお客様のセキュリティー意識・関心の向上に伴い、暗号化機構やz/OS RACFなどのセキュリティー関連製品のテクノロジー普及と実装を推進。

日本アイ・ビー・エム株式会社
テクニカル・リーダーシップ
技術理事

長島 哲也
Tetsuya Nagashima

アーキテクトとして、メインフレームからPCまでの技術を担当。特に、e-Business、Enterprise Architecture（EA）、Service Oriented Architec-ture（SOA）分野のエバンジェリストとして広くIT業界に先端テクノロジーや手法の認知・普及に努める。現在は公共分野におけるテクノロジーの顔としてCTO（チーフ・テクノロジー・オフィサー）の役割を任命され、政府や官公庁・地方自治体に新テクノロジーの普及を推進している。