魅惑のHSM

-ハードウェアセキュリティモジュール導入のススメ-

JANOG30@Kurashiki

Tomofumi Okubo
Cryptographic Key Manager, IANA / DNS Operations
Internet Corporation for Assigned Names and Number

HSMの概要

HSMの概要 Cont'd

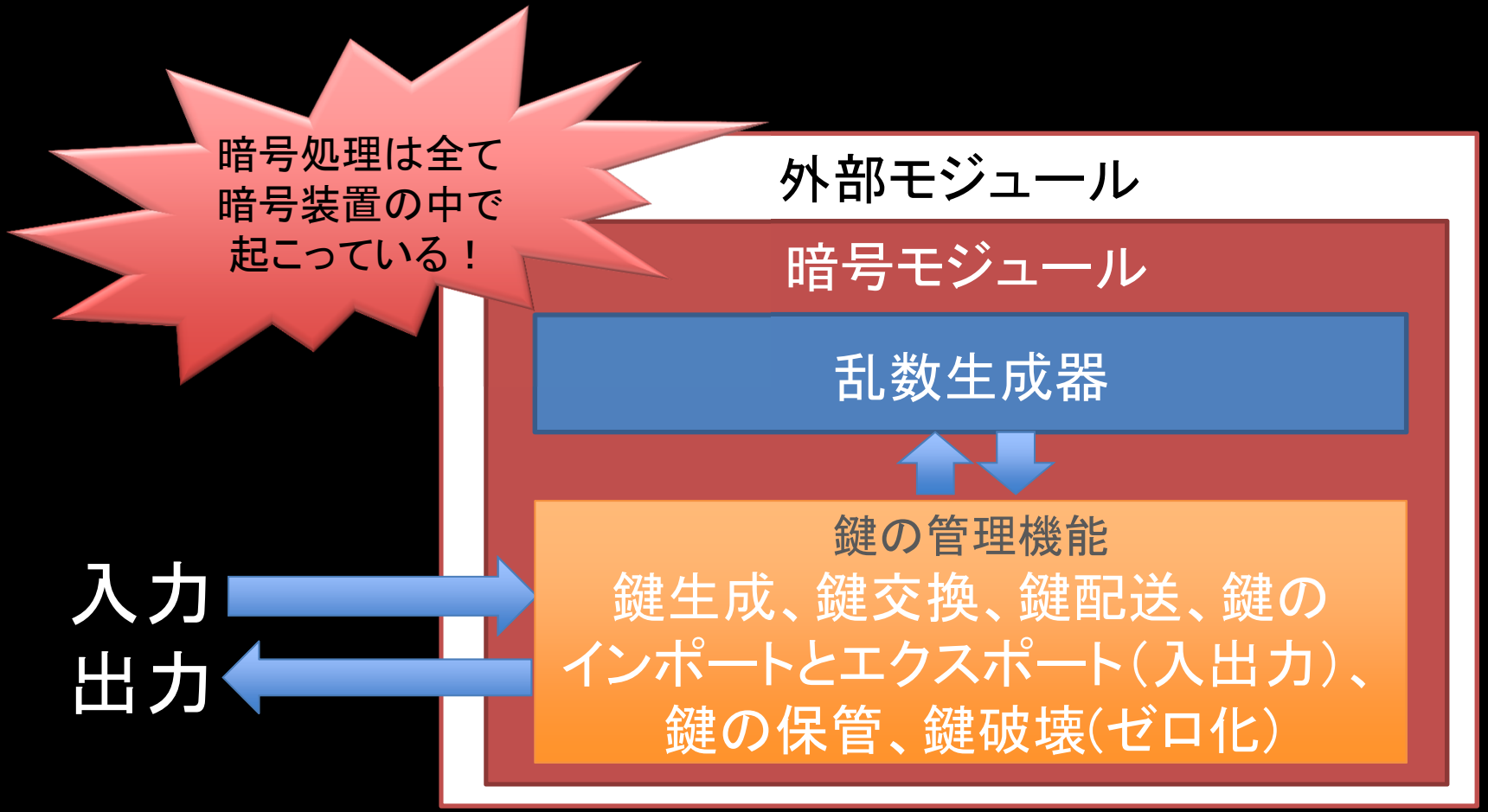
Hardware Security Module ＝ 暗号鍵の管理を安全に行う装置。

HSMの概要 Cont'd

暗号鍵のセキュアな
生成、**使用**、**保存**、
破壊などを行います。

HSMの概要 Cont'd

図解！3秒くらいで分かるかもしれない一般的なHSM



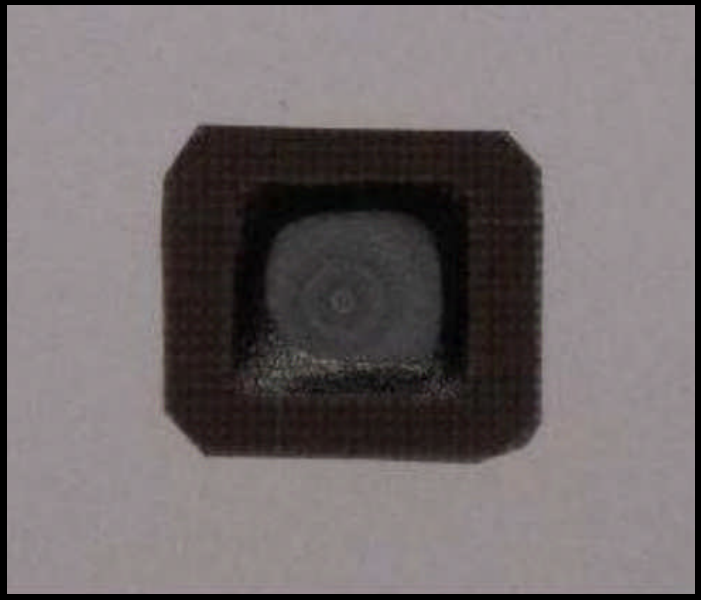
HSMの概要 Cont'd

HSMの暗号モジュールの例、その1

外部モジュール(外身)

Athena ID protect

暗号モジュール(中身)



Athena ID protect chip

HSMの概要 Cont'd

HSMの暗号モジュールの例、その2

外部モジュール(外身)　　暗号モジュール(中身)

Imation Ironkey

Imation Secure Flash Drive
Cryptographic Module

HSMの概要 Cont'd

HSMの暗号モジュールの例、その3

外部モジュール(外身)

AEP Keyper Series K

暗号モジュール(中身)

ACCE

HSMの概要 Cont'd

HSMの暗号モジュールの例、その4

外部モジュール(外身)

Thales nShield Edge

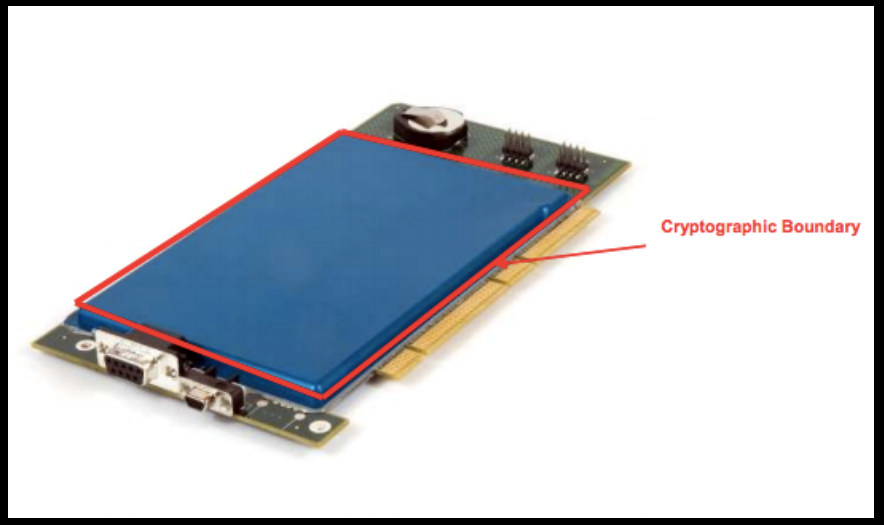
暗号モジュール(中身)

Mini HSM

HSMの概要 Cont'd

HSMの暗号モジュールの例、その5

外部モジュール(外身)　　暗号モジュール(中身)



Luna SA

Luna PCI

HSMの概要 Cont'd

高リスクまたは
高価値なサービスを
運用している場合

HSMの概要 Cont'd

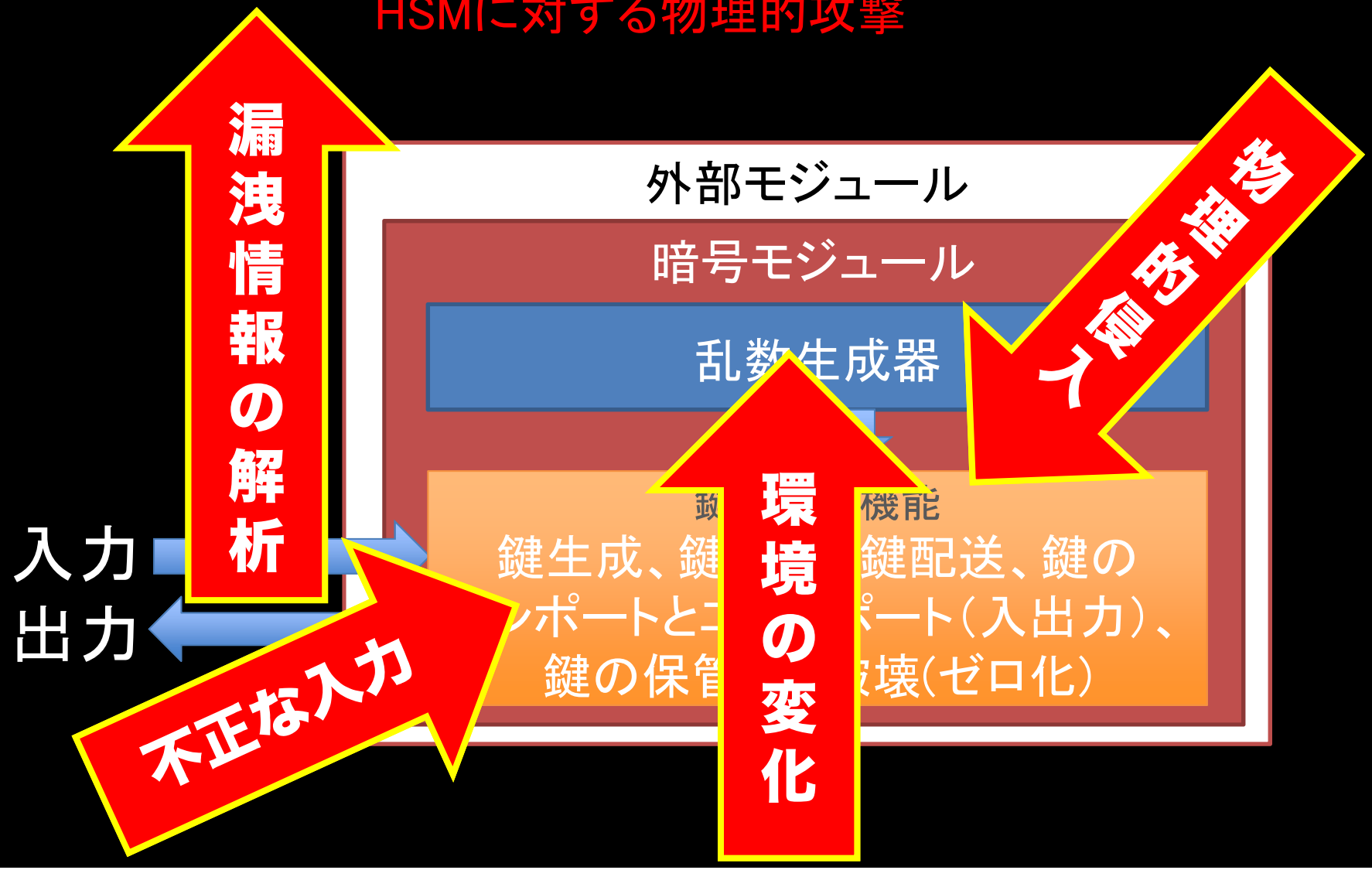
政府機関
認証局
金融機関など

HSMの導入効果

HSMの導入効果 Cont'd

1. 暗号鍵に高度な物理セキュリティを提供
2. 監査性と追跡性の確保
3. 暗号処理の拡張性とサーバの負荷軽減
4. 論理セキュリティの強制
5. 品質の優れた暗号処理

HSMの導入効果 Cont'd



HSMの導入効果 Cont'd

例: MofN、業務分掌、カウント制限、時間制限など

HSMの導入効果 Cont'd

例: 乱数生成器

Ron was wrong, Whitt is right

http://eprint.iacr.org/2012/064.pdf

FIPS140とコモンクライテリア

FIPS140とコモンクライテリア

1. FIPS140とは何か？

FIPS140とコモンクライテリア Cont'd

米国標準技術局(NIST)が発行している規格で、暗号モジュールのセキュリティ要件を規定している文書。

FIPS140とコモンクライテリア Cont'd

2. FIPS140-2のレベル定義

FIPS140とコモンクライテリア Cont'd

Security Level 1＝

暗号モジュールとしての基本的なセキュリティ要求事項のみが充足されることが求められる。
物理的要件は特に無い

Security Level 2＝

レベル1に加え、タンパー証跡を残す

Role Based Access Controlの実装

Security Level 3＝

レベル2に加え、タンパー検知とタンパー応答

Identity Based Access Controlの実装

Security Level 4＝

レベル3に加え、環境変動、環境状況に対応した保護

FIPS140とコモンクライテリア Cont'd

認定では、
規定されている
セキュリティ要件に
適合しているか
確認をする。

FIPS140とコモンクライテリア Cont'd

3. コモンクライテリアとは何か？

FIPS140とコモンクライテリア Cont'd

情報技術セキュリティ評価のための共通基準。
ISO/IEC15408に規定されている。

FIPS140とコモンクライテリア Cont'd

4. コモンクライテリアのレベル定義

FIPS140とコモンクライテリア Cont'd

EAL1＝機能テスト
EAL2＝構造化テスト
EAL3＝方式的テスト、およびチェック
EAL4＝方式的設計、テストおよびレビュー
EAL5＝準形式的設計、およびテスト
EAL6＝準形式的検証済み設計、およびテスト
EAL7＝形式的検証済み設計、およびテスト

FIPS140とコモンクライテリア Cont'd

Evaluation Agreement Level (EAL)=評価保証レベル

FIPS140とコモンクライテリア Cont'd

認定は製品の評価を保証する
程度を示すもので、
セキュリティ強度を
示すものでは無い。

FIPS140とコモンクライテリア Cont'd

セキュリティ性能の高い製品を
選ぶという観点からは、
政府調達でない限り
コモンクライテリアは
スルーをしていい。

HSMの
いる組織、
いらない組織

HSMのいる組織、いらない組織

1. HSMの
いらない組織

HSMのいる組織、いらない組織 Cont'd

A. 少々粗相をしても、訴訟や批判を受けそうにない組織

HSMのいる組織、いらない組織 Cont'd

B. あまり価値の無いサービスを提供している組織

HSMのいる組織、いらない組織 Cont'd

年間損失予測(ALE)

＜

セキュリティの年間運用費

HSMのいる組織、いらない組織 Cont'd

年間損失予測(ALE)の計上方法

HSMのいる組織、いらない組織 Cont'd

脅威によって起こる
損失の割合(EF)×
資産価値(AV)＝
単一損失予測(SLE)

HSMのいる組織、いらない組織 Cont'd

単一損失予測(SLE)×年次発生率(ARO)=年間損失予測(ALE)

HSMのいる組織、いらない組織 Cont'd

年間損失予測(ALE)＝
セキュリティに
かけられるコストの指標

HSMのいる組織、いらない組織 Cont'd

例

財布を無くした場合の損失のパーセンテージ＝
１００％、資産価値は３０００円＝
単一損失予測は３０００円。
一年にだいたい５回財布（５００％）を
なくしているとすると、
３０００円×５００％＝１５０００円。
財布をなくさないための対策費用は、
年間１５０００円までであれば妥当である。

HSMのいる組織、いらない組織 Cont'd

こんな計算面倒くさい。思った運用者に朗報！

HSMのいる組織、いらない組織 Cont'd

御社セキュリティか事業継続計画の担当者がすでに計算しているはず！

HSMのいる組織、いらない組織 Cont'd

2. HSMの導入を考えるべき組織は？

HSMのいる組織、いらない組織 Cont'd

A. いらない組織の特徴に当てはまらない組織

HSMのいる組織、いらない組織 Cont'd

B. 本当は必要な気がするけど、今まで鍵管理について考えたことが無い組織

HSMのいる組織、いらない組織 Cont'd

Due Careと Due Diligence と日本の安全神話

HSMの選択

HSMの選び方

1. HSMの探し方

HSMの選び方 Cont'd

FIPS140-2 認定のページに一覧があり⊠。

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

HSMの選び方 Cont'd

HSMを提供しているベンダーの例

HSMの選び方 Cont'd

認定を受けた暗号モジュールの数
（140-1と140-2混合）

	レベル1	レベル2	レベル3	レベル4	合計
ハードウェア	142	703	318	19	1182件
ソフトウェア	434	59	0	0	493件
ファームウエア	47	7	3	0	57件
ソフトウェアハイブリッド	15	0	0	0	15件
ファームウェアハイブリッド	1	0	0	0	1件
合計	639件	769件	321件	19件	

HSMの選び方 Cont'd

ベンダー名　暗号モジュール名　種別　認定日　セキュリティレベル

1747	OpenSSL Software Foundation 1829 Mount Ephraim Road Adamstown, MD 21710 USA -Steve Marquess TEL: 800-673-6775 **CST Lab:** NVLAP 100432-0	**OpenSSL FIPS Object Module** (Software Version: 2.0) *(When built, installed, protected and initialized as assumed by the Crypto Officer role and as specified in the provided Security Policy. Appendix A of the provided Security Policy specifies the actual distribution tar file containing the source code of this module. There shall be no additions, deletions or alterations to the tar file contents as used during module build. The distribution tar file shall be verified as specified in Appendix A of the provided Security Policy. Installation and protection shall be completed as specified in Appendix A of the provided Security Policy. Initialization shall be invoked as per Section 4 of the provided Security Policy. Any deviation from specified verification, protection, installation and initialization procedures will result in a non FIPS 140-2 compliant module.)* Validated to FIPS 140-2 Security Policy Consolidated Validation Certificate	Software	06/27/2012	***Overall Level:* 1** -Roles, Services, and Authentication: Level 2 -Design Assurance: Level 3 -Operational Environment: Tested as meeting Level 1 with Android 2.2 (gcc Compiler Version 4.4.0); Android 2.2 running on Qualcom QSD8250 (ARMv7) with NEON (gcc Compiler Version 4.4.0); Microsoft Windows 7 (32 bit) (Microsoft 32 bit C/C++ Optimizing Compiler Version 16.00); uCLinux 0.9.29 (gcc Compiler Version 4.2.1); Fedora 14 running on Intel Core i5 with AES-NI (gcc Compiler Version 4.5.1); HP-UX 11i (32 bit) (HP C/aC++ B3910B); HP-UX 11i (64 bit) (HP C/aC++ B3910B); Ubuntu 10.04 (32 bit) (gcc Compiler Version 4.1.3); Ubuntu 10.04 (64 bit) (gcc Compiler Version 4.1.3); Android 3.0 (gcc Compiler Version 4.4.0); Linux 2.6.27 (gcc Compiler Version 4.2.4); Microsoft Windows 7 (64 bit) (Microsoft C/C++ Optimizing Compiler Version 16.00); Ubuntu 10.04 running on Intel Core i5 with AES-NI (32 bit) (gcc Compiler Version 4.1.3); Linux 2.6.33 (gcc Compiler Version 4.1.0); Android 2.2 running on OMAP 3530 (ARMv7) with NEON (gcc Compiler Version 4.1.0); VxWorks 6.8 (gcc Compiler Version 4.1.2); Linux 2.6 (gcc Compiler Version 4.3.2); Linux 2.6.32 (gcc Compiler Version 4.3.2); Oracle Solaris 10 (32 bit) (gcc Compiler Version 3.4.3); Oracle Solaris 10 (64 bit) (gcc Compiler Version 3.4.3); Oracle Solaris 11 (32 bit) (gcc Compiler Version 4.5.2); Oracle Solaris 11 (64 bit) (gcc Compiler Version 4.5.2); Oracle Solaris 11 running on Intel Xeon 5675 with AES-NI (32 bit) (gcc Compiler Version 4.5.2); Oracle Solaris 11 running on Intel Xeon 5675 with AES-NI (64 bit) (gcc Compiler Version 4.5.2); Oracle Linux 5 (64

証明書ダウンロード

セキュリティポリシーダウンロード

HSMの選び方 Cont'd

セキュリティポリシー

11項目の達成度の一番低いものが全体レベルとなる。そのため、
全体レベルが低いからセキュリティが劣った製品とは限らない。

1 Introduction

This document is the non-proprietary security policy for the OpenSSL FIPS Object Module, hereafter referred to as the Module.

The Module is a software library providing a C-language application program interface (API) for use by other processes that require cryptographic functionality. The Module is classified by FIPS 140-2 as a software module, multi-chip standalone module embodiment. The physical cryptographic boundary is the general purpose computer on which the module is installed. The logical cryptographic boundary of the Module is the fipscanister object module, a single object module file named *fipscanister.o* (Linux[®1]/Unix[®2] and Vxworks[®3]) or *fipscanister.lib* (Microsoft Windows[®4]). The Module performs no communications other than with the calling application (the process that invokes the Module services).

The FIPS 140-2 security levels for the Module are as follows:

Security Requirement	Security Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	2
Finite State Model	1
Physical Security	NA
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	NA

Table 1 – Security Level of Security Requirements

The Module's software version for this validation is 2.0, replacing the previous OpenSSL FIPS Object Module v1.2. The 2.0 Module incorporates changes from the v1.2 module to support the

HSMの選び方 Cont'd

HSMの価格

- 数千円のものから数万円
  - スマートカード型、オンボード型
- 数十万円から数百万円
  - 外付け型、内蔵型
- 数百万円から数千万円
  - アプライアンス型

HSMの選び方 Cont'd

図解！HSMの分類はこんな具合だ！

HSMの選び方 Cont'd

2. HSMの評価をする

HSMの選び方 Cont'd

- 組織の鍵管理方針への適性を確認する
- ベンターのサポート対応を見る
- 製品の品質を見る
- EOL/EOSを確認する
- MTBFを確認する
- 技術的な要件を見る
- 供給プロセスの確認

HSMの選び方 Cont'd

3. HSMの導入コスト、運用コストの試算

HSMの選び方 Cont'd

4. セキュリティの担当部署への ウィッシュリストを華麗に送りつける!

- サービスの定量的リスク、定性的リスクの分析
- 鍵管理の運用をデザイン
- セキュリティ関連の文書整備
- 鍵管理の運用に必要なリソースの確保
- HSMの評価（暗号はセキュリティ担当者の必修科目です）

など

結局タイトルの
魅惑って一体
何だったのか？

HSMの導入効果 Cont'd

HSMの魅惑その1

HSMの導入効果 Cont'd

お客様にセキュリティに対する意識の高さをアピールできる。

HSMの導入効果 Cont'd

HSMの魅惑その２

HSMの導入効果 Cont'd

ソフトウェアでは
実装が困難な機能が
そろっている。

HSMの導入効果 Cont'd

HSMの魅惑その３

HSMの導入効果 Cont'd

ソフトウェア環境では担保できない高度なセキュリティ機能を安価に導入できる。

HSMの導入効果 Cont'd

HSMの魅惑その４

HSMの導入効果 Cont'd

**HSMは、
セキュリティ部署を
巻き込むことで
案外簡単に導入できる
キタ―(゜∀゜)―!**

HSMのトレンド(おまけ)

- Key Management Interoperability Protocol

https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip

- FIPS140-3

http://csrc.nist.gov/groups/ST/FIPS140_3/

- DNSSECやRPKIなどの普及

ご清聴
ありがとうございました。

ご質問、ご要望、苦情はこちらへ↓

tomofumi.okubo@icann.org