鍵管理に関する
2つの第三者認証制度

JNSA 鍵管理勉強会
2010.11.22
小川　博久

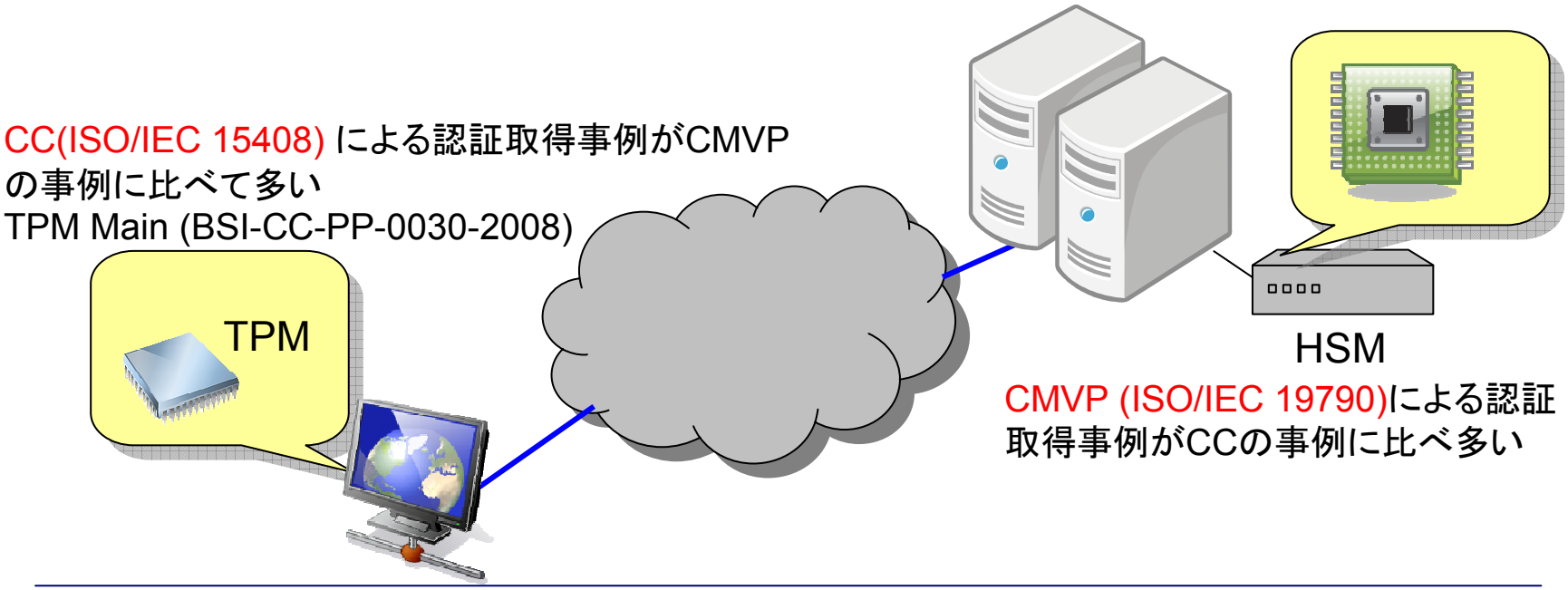
みずほ情報総研

内容

1. 鍵管理の評価はCMVPか？CCか？
2. 鍵移行(更新)の整理

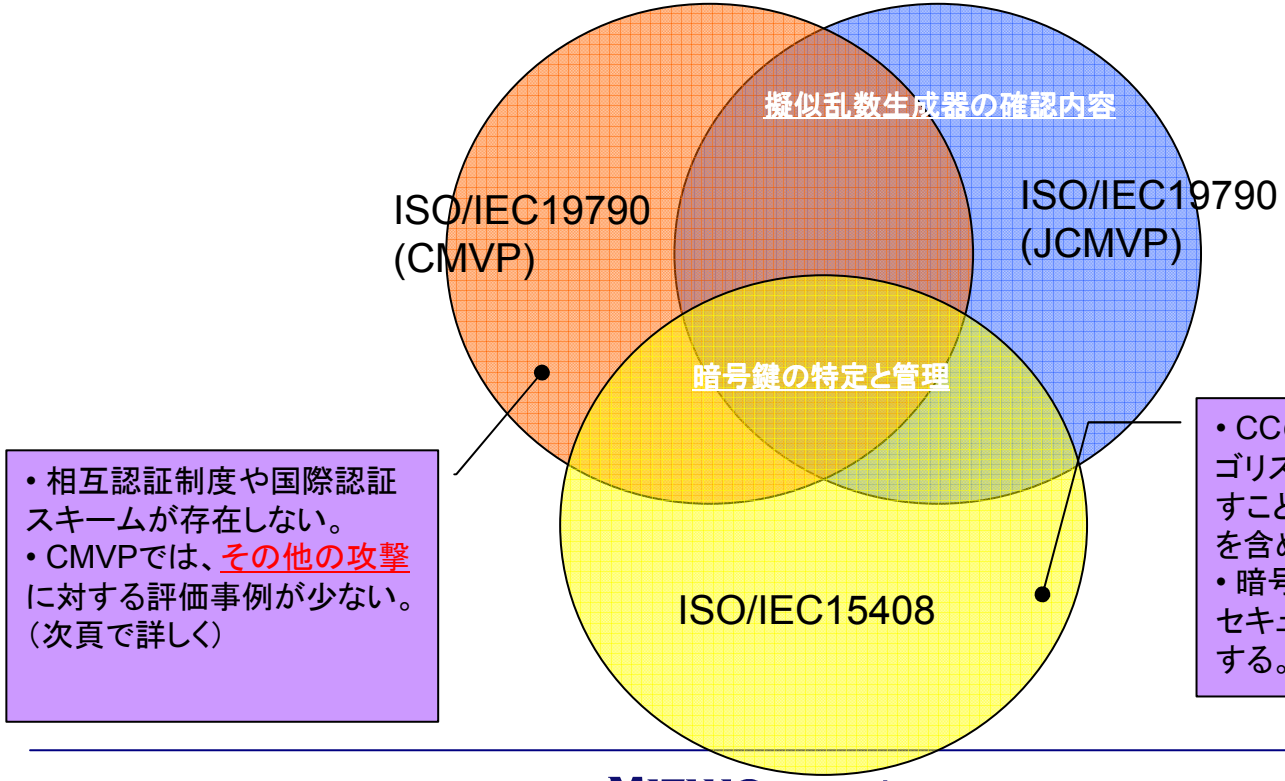
Trust chainの各エンティティの暗号モジュールは、どちらの規格で評価する？

- 現状、クラウド環境のセキュリティで最も重要となる暗号モジュール（耐タンパな製品）に関する第三者評価は、ISO/IEC15408とISO/IEC19790の両制度が混在している。
- 事例では、サーバの鍵保管（HSM）はISO/IEC19790で評価し、クライアントの鍵保管（TPM）はISO/IEC15408で評価されている。
- 異なる規格で評価された暗号モジュールによるTrust chainで問題はないのだろうか？



2つの評価制度で差分(気になる部分)はないのか？

- 異なる規格で評価された暗号モジュールによるTrust chainで問題ないことを確認するためには、各規格を確認する必要がある。



• 相互認証制度や国際認証スキームが存在しない。
• CMVPでは、その他の攻撃に対する評価事例が少ない。(次頁で詳しく)

• CCの評価では、正しい暗号アルゴリズムの実装を確認した結果を示すことができない。(擬似乱数生成を含め)
• 暗号鍵のライフサイクルに対するセキュリティ要件は、開発者が規定する。

Mitigation of other attacks
（FIPS140-3 1st Draft の時代）

■ NIST FIPS140-3 Draft

	TA	SPA/DPA	EME
Level 1, 2	—	—	—
Level 3	Y	—	—
Level 4	Y	Y	—
Level 5	Y	Y	Y

TA : Timing Analysis
SPA : Simple Power Analysis
DPA : Differential Power Analysis
EME : Electro-magnetic Emanation
SEMA : Simple Electromagnetic Analysis
DEMA : Differential Electromagnetic Analysis
FI : Fault Induction

■ CRYPTREC/INSTAC Comment

	TA	SPA	DPA	EME		FI
				SEMA	DEMA	
Level 1, 2	—	—	—	—	—	—
Level 3	Y	Y	—	Y	—	—
Level 4	Y	Y	Y	Y	Y	Y
Level 5	Y	Y	Y	Y	Y	Y

古い情報なので、気をつけてください。。
耐タンパー性評価基準の標準化に関する調査研究成果報告書, 財団法人 日本規格協会, 情報技術標準化研究センター, 平成20年3月.

Mitigation of other attacks
（最近の事例）

Cert#	Vendor	Cryptographic Module	Module Type	Val. Date	Level / Description
1450	Gemalto Avenue du Jujubier Z.I Athelia IV La Ciotat, 13705 France -Arnaud Lotigier TEL: +33 4 42 36 0 74 FAX: +33 4 42 36 55 45	**TOP DL V2 (Hardware Version: A1023378; Firmware Version: Build#11 - M1005011+ Softmask V03)** **Validated to FIPS 140-2 Security Policy Certificate**	Hardware	11/15/2010	***Overall Level: 3*** ***-FIPS-approved algorithms: AES (Cert. #1363); ECDSA (Cert. #172); RNG (Cert. #749); RSA (Cert. #664); SHS (Cert. #1243); Triple-DES (Cert. #938)*** ***-Other algorithms: N/A*** ***Single-chip*** ***"This module is based on a Java Card platform (TOP DL V2) with 128K EEPROM memory available. The Cryptographic Module provides dual interfaces (i.e. contact and contact-less) where the same security level is achieved."***

Security Policy を見てみると…↓

12 Mitigation of other attacks

The TOP DL V2 has been designed to mitigate the following attacks:

- Timing Attacks,
- Differential Power Analysis,
- Simple Power Analysis,
- Electromagnetic Analysis,
- Fault Attack.
- Card Tearing

A separate and proprietary document describes the mitigation of attacks policy provided by the TOP DL V2 platform.

※これは、Java Cardの事例だがCMVPだからMitigation of other attacksが、記載されていない。ということではない。

1.『CMVPか？CCか？』のまとめ

- 暗号モジュールの利用者は、以下を踏まえて、選定しないといけない。
  - TPM/HSMは、メーカーの“活動している国”によって、評価制度の対応が変わるようだ。
  - 攻撃耐性への対応は、メーカーや評価制度に関係なく、製品分類によって変わるようだ。

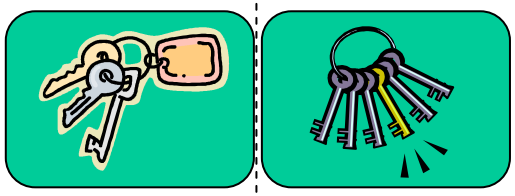
（CMVPがいい/CCがいいとは言えないが、
両制度で評価されている内容を理解する必要はある。）

鍵の移行(更新)について

- 鍵を考えるためには、鍵の移行(更新)が重要。
- 鍵の移行(更新)は、鍵のライフサイクルを複数、同時に行うこと。
  - 鍵生成
  - (鍵配送、鍵合意、鍵包装)
  - 鍵保管
  - 鍵活性化
  - 鍵利用
  - 鍵廃棄(ゼロ化)
- これらをある程度、整理できないだろうか?

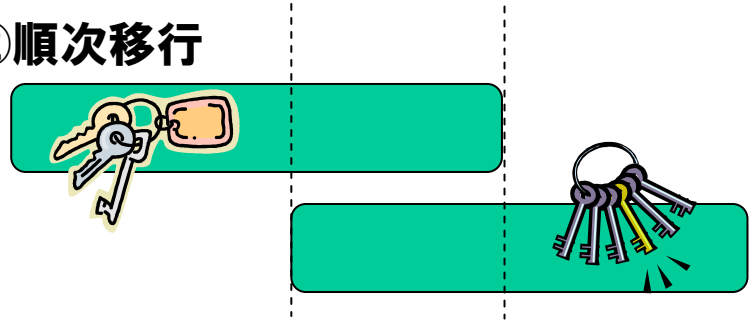
鍵の移行には、
どのようなパターンがあるのだろうか？

①完全移行



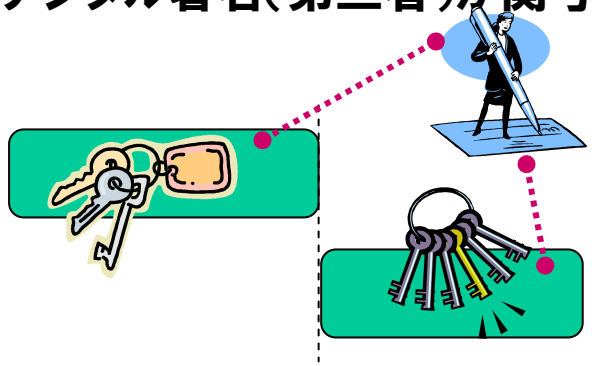
企業内の小規模システムならあるかもしれない。

②順次移行



一般的なシステムでは、システム全体としては、
順次鍵が更新される。

③デジタル署名（第三者）が関与する場合



デジタル署名が絡むと信頼点も考慮する必要
がある。

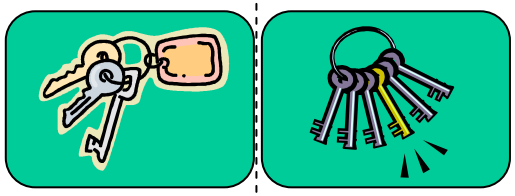
さらに、もっと細かく考えると．．．
（検討事例）

- 5.1.3 Hardware Security Module
  - Hardware security module (HSM) is the trusted computing base of a vehicle. The purpose of an HSM is to provide a physically protected environment for the storage of private keys (long-term and short-term keys), the execution of cryptographic operations (message signing and decryption of encrypted anonymous certificates) and key management functions [60].
  - . . . For practical purposes, an HSM implementation somewhere between high-end and low-end devices is needed.

Performance Analysis of Authentication Protocols in Vehicular Ad Hoc Networks (VANET), Abdul Kalam Kunnel Aboobaker, Technical Report, RHUL-MA-2010-02, 31st March 2010.

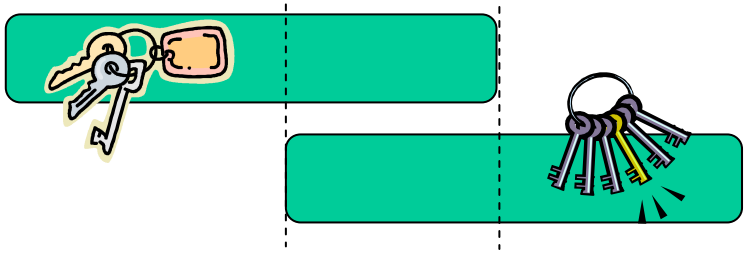
鍵の移行のパターンについて
（追加：Key及びDevicesの長短・高低）

①完全移行



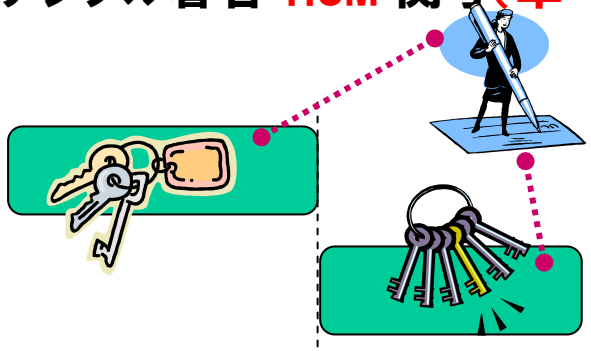
企業内の小規模システムならあるかもしれない。

②順次移行

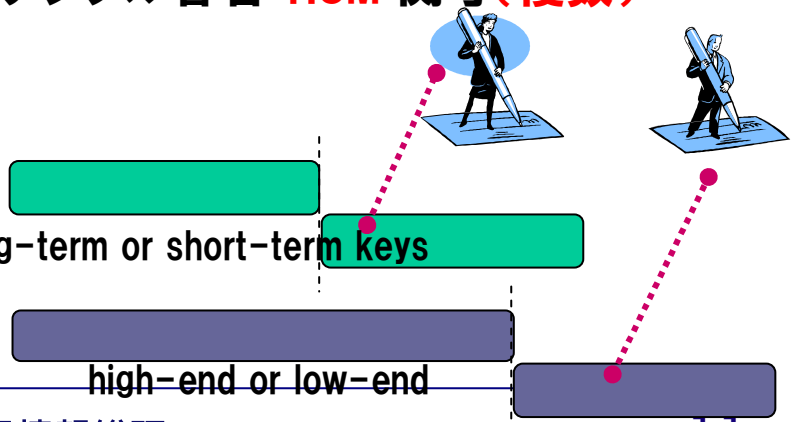


一般的なシステムでは、システム全体としては、
順次鍵が更新される。

③デジタル署名・HSM 関与（単一）



④デジタル署名・HSM 関与（複数）



2.『鍵の移行』のまとめ

- 開発者は、鍵の移行(更新)について、以下を踏まえて、設計しないといけない。
  - 移行するその鍵の信頼性を担保・確認するために、HSM(又はTTP等)は関与する必要はないのか？
  - 移行するそのKeyは、long-term か？ short-term か？
  - 移行するそのDevicesは、high-end か？ low-end か？

（各社の Mitigation of other attacks が、進化することを考えると、
long-term Key（又は high-end Devices）と short-term Key（又は low-end Devices）で要求する”運用時の”攻撃耐性を定めて、必要に応じて監視する必要はあるのかもしれない。）