IT製品の調達における
セキュリティ要件リストに関する
情報セキュリティ認定制度勉強会

ベンダ視点の発表

gemalto
security to be free

2014年9月29日
ジェムアルト株式会社　セキュリティ　相原 敬雄 (tim.aihara@gemalto.com)

ジェムアルトのご紹介

ジェムアルトについて(Euronext: GTO)

- **Gemalto は2006年に、Gemplus International S.A.とAxalto Holdings N.V.との対等合併により設立**
- **ICカードの発明から1983年世界初の商用利用に深く関与し、デジタルセキュリティのリーダ**

会社概要

- 2013年決算
  - 売上高24億ユーロ（約3,360億円）
  - 利益（PFO)3.5億ユーロ（約490億円）
- 技術革新に対する投資
  - 25箇所のR&D拠点
  - 2,000人の技術者
  - 2013年に110以上の特許申請、投資額1.4億ユーロ(約196億円)
- グローバルネットワーク
  - 85箇所のオフィス
  - 34箇所のパーソ/データセンター
  - 15箇所の生産拠点
- 社員
  - 従業員数:約12,000+人
  - 110+カ国の国籍
  - 44カ国に配置
- 190ヶ国に顧客
  - 450以上のMNO
  - 3,000以上の金融機関
  - 80以上の公共プロジェクト

日本法人

- 会社名：ジェムアルト株式会社
- 所在地:東京都港区高輪3-25-23 京急第2ビル 6F
- 設立
  - 1990年代にジェムプラスおよびシュルンベルジェ*は日本でICカードの営業を行っていた
  - 2003年アクサルト株式会社として設立
  - 2007年アクサルト株式会社からジェムアルト株式会社に商号変更
- 従業員数：約50名

*Axaltoはシュルンベルジェの ICカード部門がスピンアウトし設立された

実績

- #1
  - チップ付きペイメントカード
  - M2M
  - SIM/UICCカード
  - オンラインバンキング
  - 電子ドキュメント

gemalto
security to be free

OS、アプリケーション開発からICチップ、カード製造、デバイス製造、発行、その他サービス・ソリューション提供まで

ジェムアルトは、半導体メーカー各社と協力して最適なプラットフォームを製造（ウエハーのみ製造委託）、
自社でモジュール化します。また、搭載するOS・アプリケーション開発も行い、徹底した品質管理のもと
カード製造・発行まで手掛けています。
さらにデジタルセキュリティをリードする各種OTPデバイスや、サービス・ソリューションの提供も行っています。

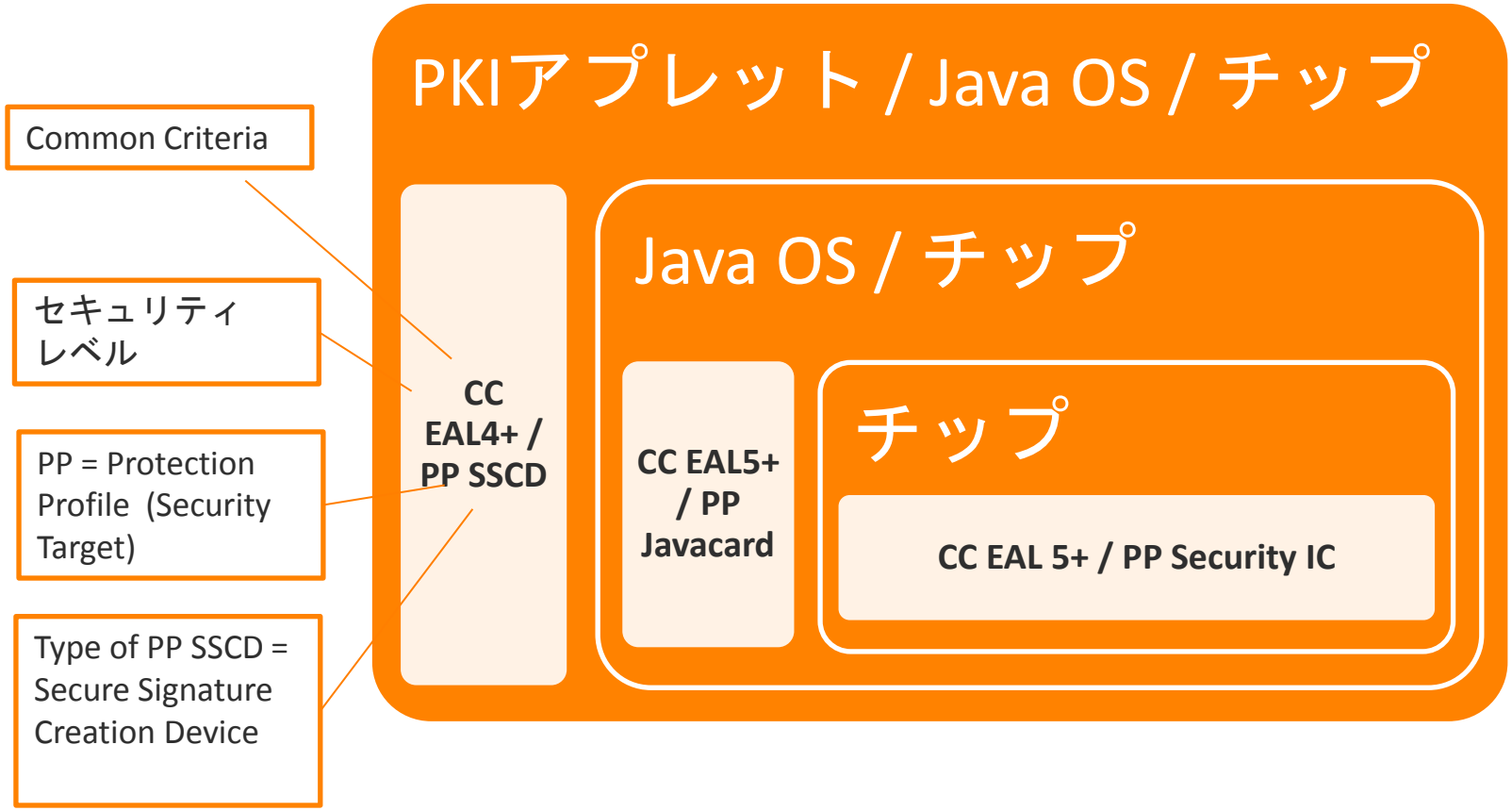
gemalto
security to be free

ICカードのセキュリティ認証に関して

gemalto
security to be free

コモンクライテリア（CC）セキュリティ認証

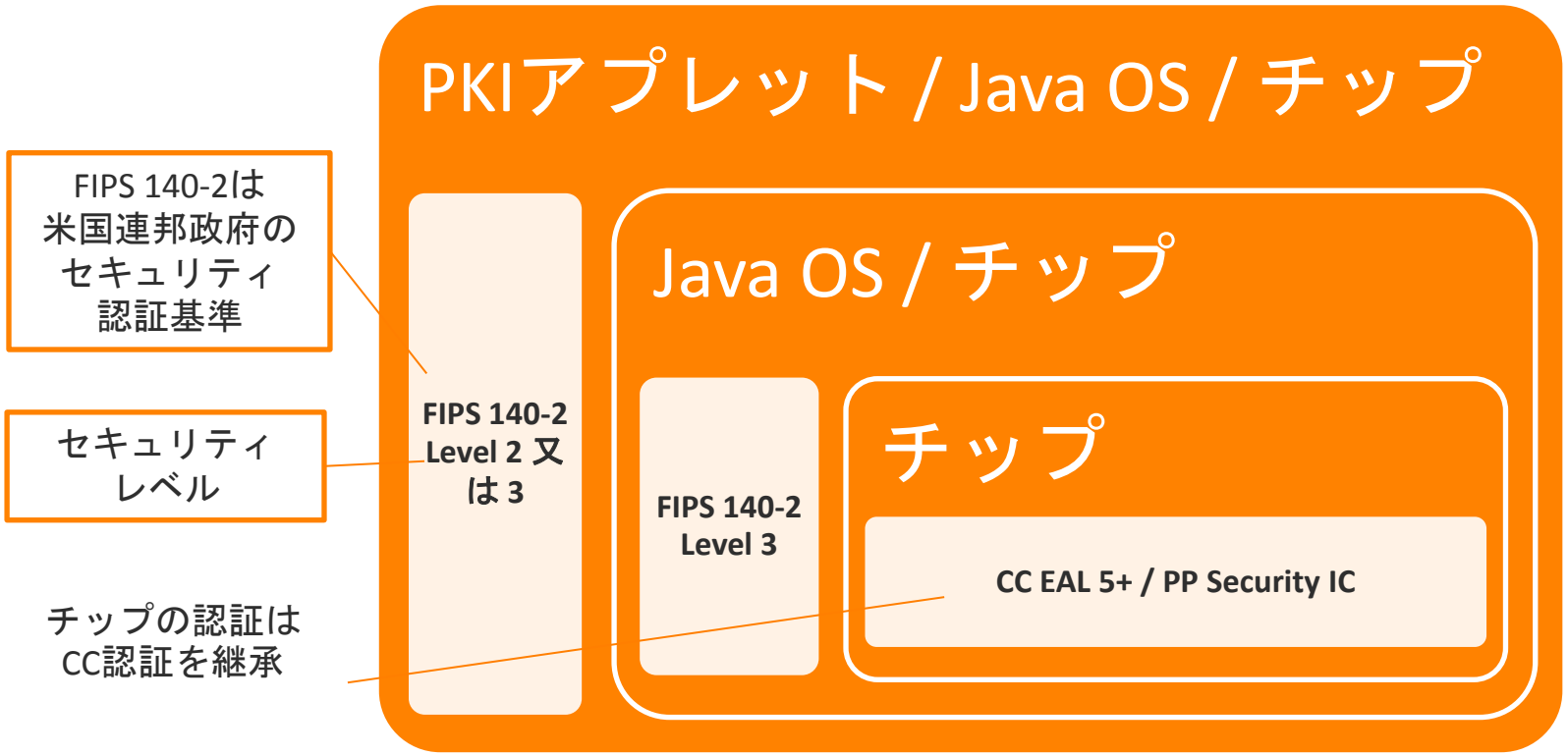
- 欧州および政府系調達条件



gemalto
security to be free

FIPSセキュリティ認証

•米国連邦政府調達条件、国内でも一般企業が要求



注: FIPS 201はセキュリティ認証ではなくPIVカードの規格

gemalto
security to be free

認証制度について

gemalto
security to be free

認証制度は良い事か?

- 当然Yes!

  But…

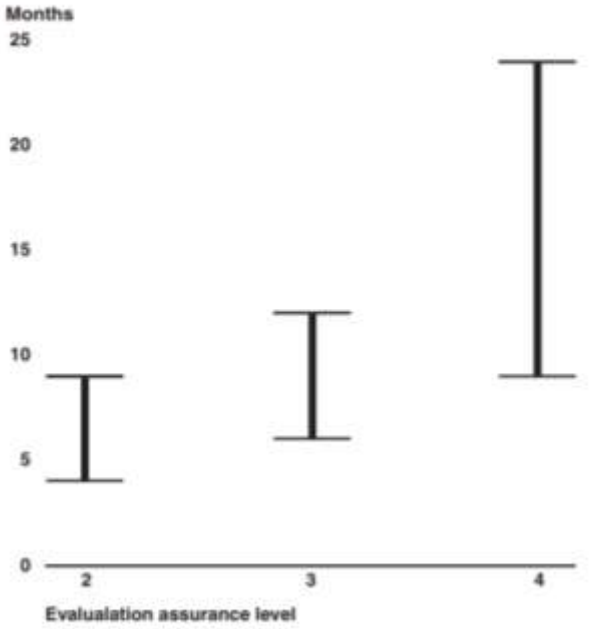
- 認定コストと期間
  - 増加傾向
  - ハードウェア→オペレーティングシステム→アプリケーション
- FIPSとCCの非整合性
  - 例Javaカードでは両方を同じ設定では取得できない
  - PKIに関しては各国の電子署名法関連認定もあり、より複雑
- FIPSは完成品の認定
  - ICカードリーダを内蔵したノートパソコンでは
    内部のモジュールが同じであっても毎モデル取得する必要あり
- 認定されても本当に安全か?

gemalto
security to be free

認定取得に掛かる期間とコスト

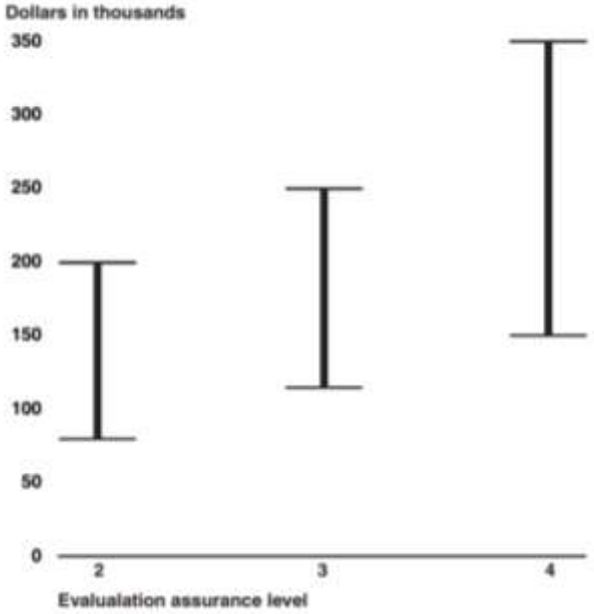
http://www.gao.gov/new.items/d06392.pdf

Figure 2: Range of Sample Cost of NIAP Evaluations to Vendors by Evaluation Assurance Level



Source: GAO analysis of data provided by laboratories.

Figure 4: Range of Time Required for Completing Product Evaluations at Various Evaluation Assurance Levels



Source: GAO analysis of data provided by laboratories.

gemalto
security to be free

IDPrimeシリーズ比較

主な機能	IDPrime .NET 510	IDPrime .NET 5500	IDPrime MD 3810	IDPrime MD 830	IDPrime MD 3840	IDPrime MD 840
Base CSP	✓	✓	✓	✓	✓	✓
PKCS#11	✓		✓	✓	✓	✓
RSA	✓	✓	✓	✓	✓	✓
On board PIN Policy	✓	✓	✓	✓	✓	✓
Multi PIN support	✓	✓	✓	✓	✓	✓
Biometry support		✓				
Dual interface (contact / contactless & **NFC** support)			✓		✓	
FIPS 140 -2 Level 3 certif. (platform + PKI applet) **FIPS 140-2 Level 2 certif** (platform + PKI , OTP & MPCOS app)	*チップのみ*		*チップのみ*	✓		
CC EAL5+ / Javacard & **CC EAL5+ / PP SSCD** (Java+applet)					✓	✓
Elliptic Curves			✓	✓	✓	✓
OTP OATH option	✓		✓	✓	✓	✓
MPCOS applet option			✓	✓	✓	✓

gemalto
security to be free

FIPS 140-2 Level 2 Certified USB Memory Stick Cracked

https://www.schneier.com/blog/archives/2010/01/fips_140-2_leve.html

Kind of a dumb mistake:

> The USB drives in question encrypt the stored data via the practically uncrackable AES 256-bit hardware encryption system. Therefore, the main point of attack for accessing the plain text data stored on the drive is the password entry mechanism. When analysing the relevant Windows program, the SySS security experts found a rather blatant flaw that has quite obviously slipped through testers' nets. During a successful authorisation procedure the program will, irrespective of the password, always send the same character string to the drive after performing various crypto operations -- and this is the case for all USB Flash drives of this type. Cracking the drives is therefore quite simple. The SySS experts wrote a small tool for the active password entry program's RAM which always made sure that the appropriate string was sent to the drive, irrespective of the password entered and as a result gained immediate access to all the data on the drive. The vulnerable devices include the Kingston DataTraveler BlackBox, the SanDisk Cruzer Enterprise FIPS Edition and the Verbatim Corporate Secure FIPS Edition.

Nice piece of analysis work.

The article goes on to question the value of the FIPS certification:

> The real question, however, remains unanswered - how could USB Flash drives that exhibit such a serious security hole be given one of the highest certificates for crypto devices? Even more importantly, perhaps - what is the value of a certification that fails to detect such holes?
>
> The problem is that no one really understands what a FIPS 140-2 certification means. Instead, they think something like: "This crypto thingy is certified, so it must be secure." In fact, FIPS 140-2 Level 2 certification only means that certain good algorithms are used, and that there is some level of tamper resistance and tamper evidence. Marketing departments of security take advantage of this confusion -- it's not only FIPS 140, it's all the security standards -- and encourage their customers to equate conformance to the standard with security.

So when that equivalence is demonstrated to be false, people are surprised.

gemalto
security to be free

セキュリティデバイスの必要性は増している（1）

- **RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis**
- **Q1: What information is leaked?**
  - This depends on the specific computer hardware. We have tested numerous laptops, and several desktops.
    - In almost all machines, it is possible to distinguish an idle CPU (x86 "HLT") from a busy CPU.
    - On many machines, it is moreover possible to distinguish different patterns of CPU operations and different programs.
    - Using GnuPG as our study case, we can, on some machines:
      - distinguish between the acoustic signature of different RSA secret keys (signing or decryption), and
      - **fully extract decryption keys, by measuring the sound the machine makes during decryption of chosen ciphertexts.**
- **Q2: What is making the noise?**
- The acoustic signal of interest is generated by vibration of electronic components (capacitors and coils) in the voltage regulation circuit, as it struggles to supply constant voltage to the CPU despite the large fluctuations in power consumption caused by different patterns of CPU operations. The relevant signal is *not* caused by mechanical components such as the fan or hard disk, nor by the laptop's internal speaker.
- 出典： http://www.tau.ac.il/~tromer/acoustic/

gemalto
security to be free

セキュリティデバイスの必要性は増している（2）

- BadUSB: Big, bad USB security problems ahead
  - http://www.zdnet.com/badusb-big-bad-usb-security-problems-ahead-7000032211/

Nohl and Lell have discovered that USB controller chips' firmware offer no protection from reprogramming. Using a set of proof-of-concept tools they call BadUSB, they claim that an ordinary USB device, even a thumb drive, can be used to compromise computers in the following ways:

- A device can emulate a keyboard and issue commands on behalf of the logged-in user, for example to exfiltrate files or install malware. Such malware, in turn, can infect the controller chips of other USB devices connected to the computer.
- The device can also spoof a network card and change the computer’s DNS setting to redirect traffic.
- A modified thumb drive or external hard disk can — when it detects that the computer is starting up — boot a small virus, which infects the computer’s operating system prior to boot.

gemalto
security to be free

最後に…

- 製品評価に認証を参考にするのは良い
  - しかし、FIPSとCCは直接比較できない
  - レベルが高い=開発コストも高い=製品コストに反映

- セキュリティベンダの選定
  - 製品の認証だけで選ぶことは危険
  - 独自のセキュリティ対策
  - 20年後を考えたい策を行っているか
  - 実績
    - 認証製品の数
    - 過去に取消、事件等が無いか

gemalto
security to be free

ご静聴、ありがとうございました