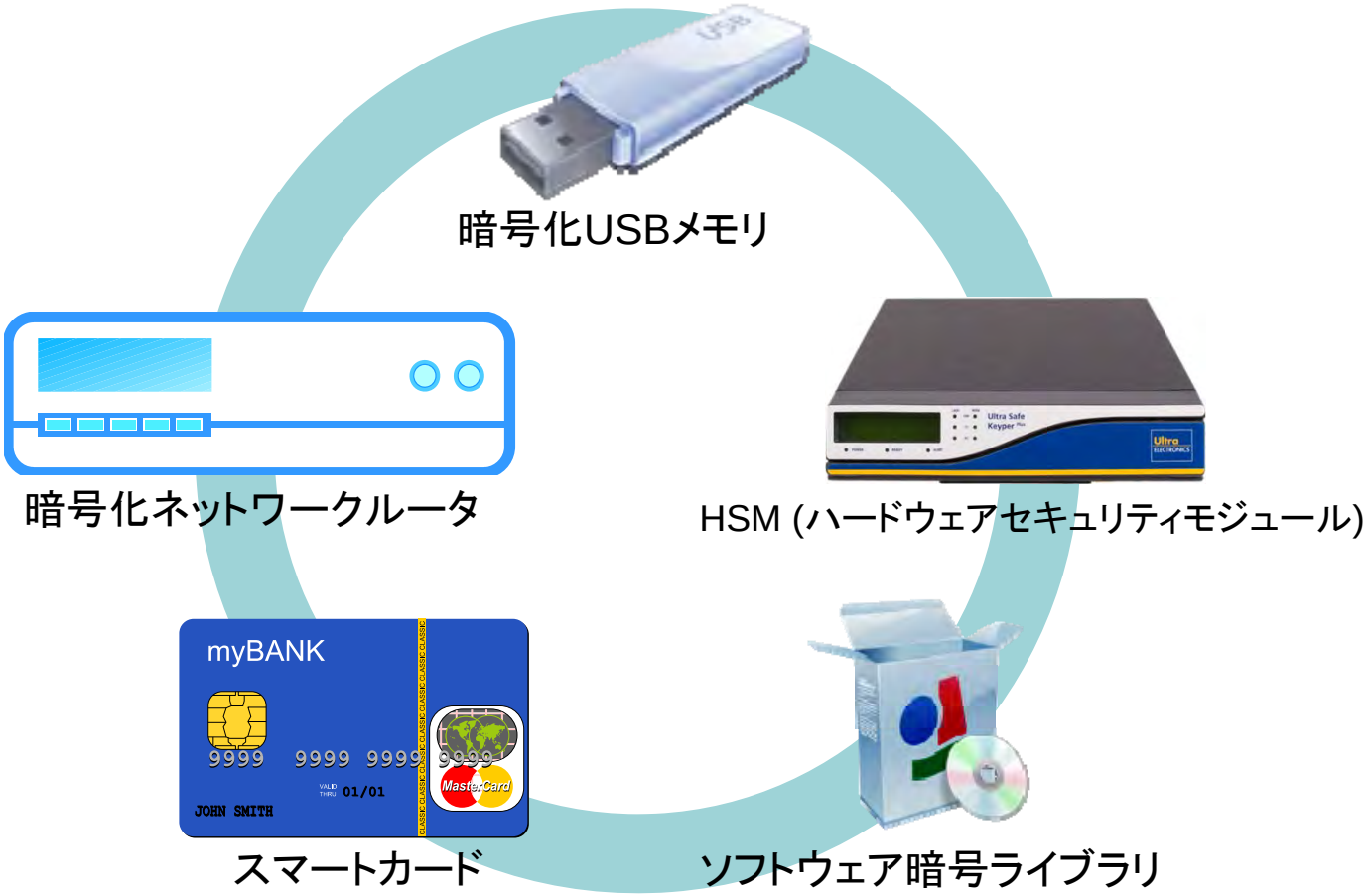
IPA Better Life with IT

Japan Cryptographic Module Validation Program ®
JCMVP

その暗号モジュールは大丈夫?

～安心して使える暗号モジュールとは～

暗号モジュールとは何か

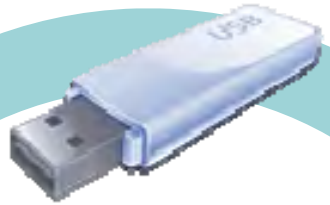


「承認されたセキュリティ機能」をソフトウエア/ファームウエア/ハードウエアで実装したものである。

承認されたセキュリティ機能: 電子政府推奨暗号リスト等に記載され安全性の確認されたセキュリティ機能

安心して使用できる暗号モジュール?

暗号アルゴリズム
の強度は十分?



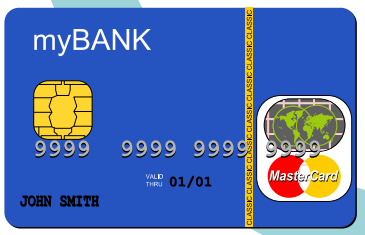
暗号化USBメモリ

暗号アルゴリズム
の実装は正しい?

暗号化ネットワークルータ

HSM (ハードウェアセキュリティモジュール)

鍵管理は
大丈夫?



スマートカード

ソフトウェア暗号ライブラリ

生成した鍵は
安全?

安心して使用できる暗号モジュールであるかどうかは、さまざまな視点で検証する必要がある

セキュリティ機能

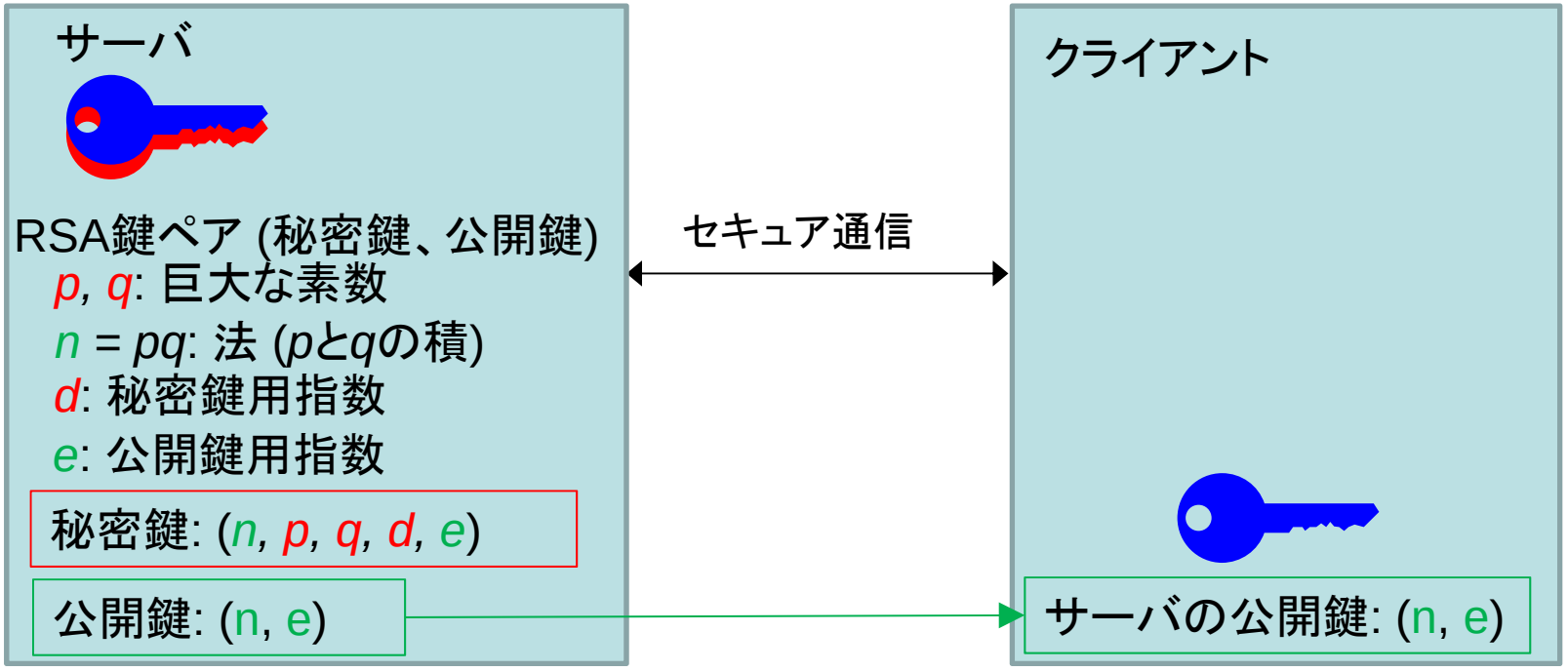
- 暗号化/復号
- 署名生成/署名検証
- 乱数生成器
- ハッシュ関数
- 鍵確立
- メッセージ認証

事例紹介

暗号の実装や使い方が不適切であったために、十分なセキュリティが得られなかった例

事例紹介
SSL/TLS, SSH

- 公開鍵暗号でセキュリティを確保
  - 主にRSA暗号が使用されている



疑問: この鍵はどうやって作った?

RSA暗号の原理

- *p, q:* 巨大な素数
- *n (=pq):* 巨大な素数の積
- *e*: 公開鍵用指数, *d*: 秘密鍵用指数
- 秘密鍵: (*n, e, d, p, q*)
- 公開鍵: (*n, e*)
- 暗号化: $c \equiv m^e \pmod{n}$, 復号: $m \equiv c^d \pmod{n}$
- 署名: $s \equiv m^d \pmod{n}$, 署名検証: $m \equiv s^e \pmod{n}$

巨大な数の素因数分解の計算量的困難性が安全性のよりどころ
鍵長(*n*のビット数)が十分であれば、

- *n*を知っていても、*p*と*q*を知ることは計算量的に困難
- *n*と*e*を知っていても、*p*と*q*を知らない限り、*d*を知ることは計算量的に困難

RSAの鍵生成

- 素数pをランダムに生成
  - 乱数生成→素数判定→素数が得られるまで繰り返し
- 素数qをランダムに生成
  - pの生成と同様
- $n = pq$ を計算 (容易に計算できる)
- 公開鍵用指数eを生成 (ランダムあるいは固定値)
- $de \equiv 1 \bmod \phi(n)$ となるdを計算し、秘密鍵用指数とする
  (pとqを知っていれば容易に計算できる)

鍵生成には、乱数生成器を使用する
鍵は予測不可能でなければならないので、
乱数生成器の質は重要

事例紹介
RSA鍵における素因数の共有

- RSA公開鍵の法(modulus) $n=pq$
- Nが素因数分解できると、秘密鍵が判明する
- 巨大な数の素因数分解は困難である

- しかし、もしも、2個のRSA公開鍵が、素因数を共有していたら…

$$n_1=pq_1 \ , n_2=pq_2$$

- 最大公約数 $p=\gcd(n_1, n_2)$ は容易に計算できる

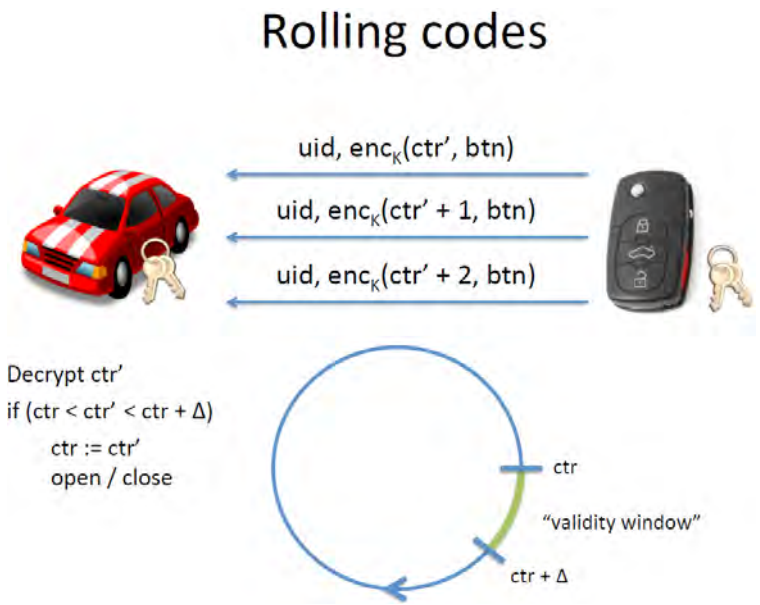
- SSL証明書・SSHホスト鍵から多数のRSA公開鍵を取得
- 同じ素因数を共有している公開鍵の組が見つかった!

鍵生成時の乱数生成に問題があったと考えられる

https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/heninger

事例紹介
自動車の開錠リモコン

- replay攻撃を防ぐため、インクリメンタルカウンタと暗号を使用して正当な開錠要求かどうかを判定するようにしている



ある車種において、全世界のすべての車で同一の暗号鍵を使用していた!

事例紹介
欧州「オイスターカード」

- 2008年6月、オランダの研究者が、欧州で**1,700万枚発行されている「オイスターカード」**を複製できることを英国ロンドンの地下鉄で実証した。
- 破られた理由としては次のようなものが挙げられている。
  - このカードはNXPセミコンダクタ社製のMIFARE Classicと言われる古い製品であり、搭載されている**暗号アルゴリズムはNXP社独自**のCRYPTO1と言われるものでアルゴリズムは非公開だった。
  - **暗号鍵長は48ビット**しかなく、全数探索しても数時間で探索可能であり現在では明らかに強度が不足している。
  - **通信プロトコルや乱数生成アルゴリズムにも脆弱性**があり、これらを利用されると極めて短時間に**暗号鍵**を盗まれてしまう。

安全性の弱い暗号アルゴリズムを使用していたためにセキュリティが守られていなかった

「隠蔽によるセキュリティ」は通用しない

IPA

安心して使える暗号モジュールとは?

暗号モジュール試験及び認証制度 (JCMVP)の紹介

暗号モジュール試験及び認証制度とは

- 「暗号モジュール試験及び認証制度」
  (**JCMVP**: Japan Cryptographic Module Validation Program)とは、

1. 暗号の実装が正しく、
2. それが正しく実行され、
3. 重要情報が適切に保護されていること

を担保する制度。

- この制度を利用すると、次の事項を確認できます。
  - 「電子政府推奨暗号リスト」に記載された暗号化及び電子署名のアルゴリズムを、正しく実装していること。
  - 暗号鍵管理が適切に行われること。
- 米国・カナダのCMVP (Cryptographic Module Validation Program) 制度と同等の制度

JCMVPで承認されたセキュリティ機能

技術分類		暗号名称
公開鍵暗号	署名	DSA、ECDSA、RSASSA-PKCS1-v1_5、RSASSA-PSS
	守秘	RSA-OAEP
	鍵確立	DH, ECDH, MQV, ECMQV, NIST SP800-56B
共通鍵暗号	64ビットブロック暗号	3-key Triple DES
	128ビットブロック暗号	AES, Camellia
	ブロック暗号利用モード	ECB, CBC, CFB, CTR, XTS
	ストリーム暗号	KCipher-2
その他	ハッシュ関数	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA512/224, SHA512/256
	メッセージ認証	CCM, CMAC, GCM/GMAC, HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, HMAC-SHA-512/224, HMAC-SHA-512/256
	擬似乱数生成系	NIST SP800-90A (Hash_DRBG, HMAC_DRBG, CTR_DRBG)

注： CMVPで承認されたセキュリティ機能は青字で表示。

暗号モジュール試験及び認証制度の概要
第三者による評価の有効性

- 北米CMVP (Cryptographic Module Validation Program)では、暗号モジュール試験において、ほぼ半数の製品で問題が発覚している。
  北米CMVP試験機関の調査結果として、2013年秋~2014年夏まで、セキュリティレベル1・2の平均で

57%程度の不適合事例

暗号モジュール試験及び認証制度の概要
政府の調達要件における位置づけ

- 府省庁対策基準策定のためのガイドライン (平成28年8月31日)
  http://www.nisc.go.jp/active/general/pdf/guide28.pdf
  - 6.1.5 暗号・電子署名
    基本対策事項 (1)-1

情報システムセキュリティ責任者は、**暗号化**又は**電子署名を行う情報システム**において、以下を例とする措置を講ずること。
a) 情報システムのコンポーネント（部品）として、暗号モジュールを交換することが可能な構成とする。
b)複数のアルゴリズム及びそれに基づいた安全なプロトコルを選択することが可能な構成とする。
c)選択したアルゴリズムがソフトウェア及びハードウェアへ適切に実装されており、かつ、暗号化された情報の復号又は電子署名の付与に用いる鍵及びそれに対応する主体認証情報等が安全に保護されることを確実にするため、**「暗号モジュール試験及び認証制度」に基づく認証を取得している製品を選択する**。
d) 暗号化された情報の復号又は電子署名の付与に用いる鍵については、耐タンパ性を有する暗号モジュールへ格納する。
e) 機微な情報のやり取りを行う情報システムを新規に構築する場合は、安全性に実績のある暗号プロトコルを選択し、長期的な秘匿性を保証する観点を考慮する。

統一基準の遵守事項を満たすために採られるべき基本的な対策事項として位置づけられています。

暗号モジュール試験及び認証制度の概要
個人情報の保護に関連して

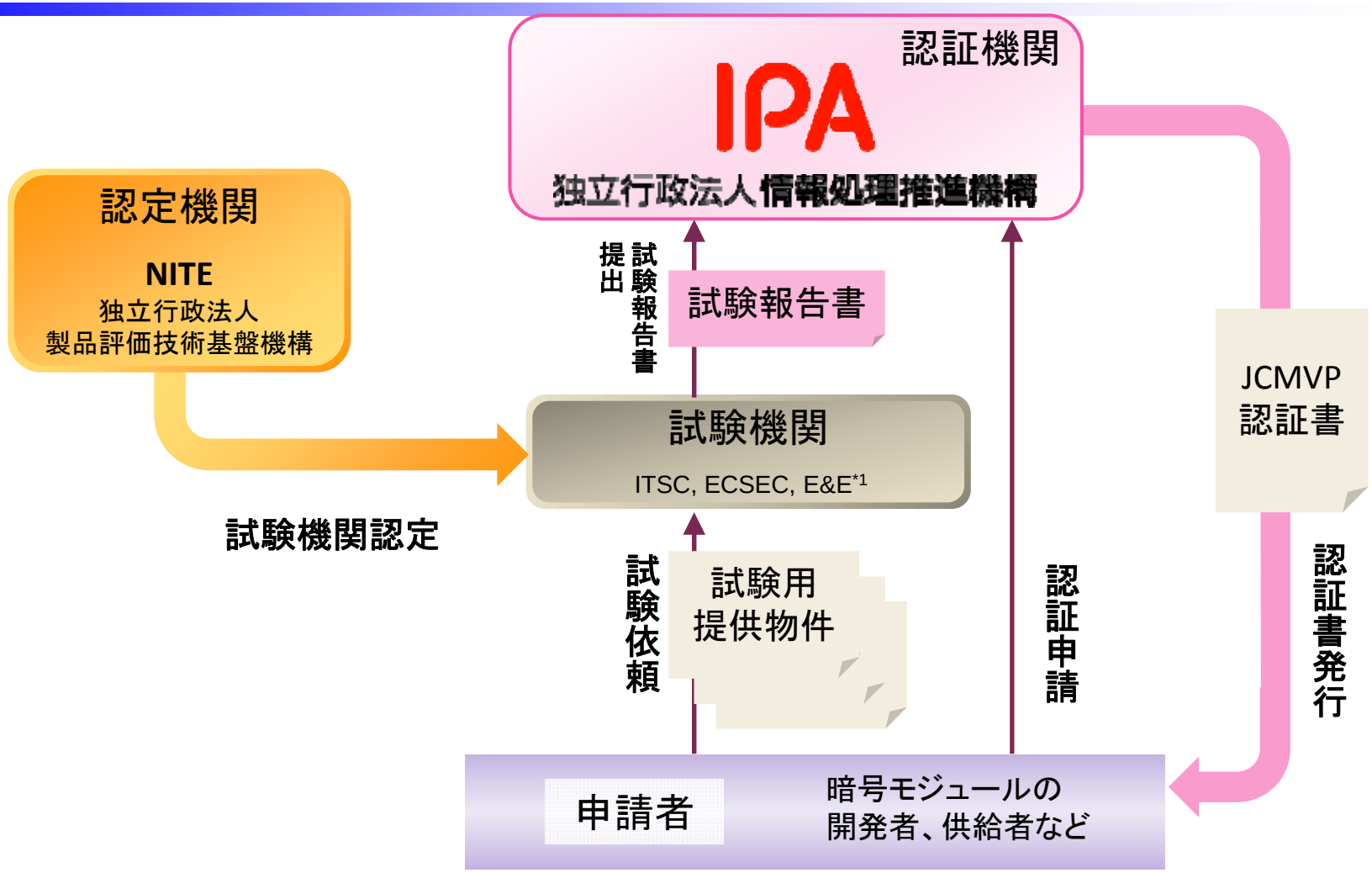
- 個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン (平成28年12月28日)
  http://www.meti.go.jp/policy/it_policy/privacy/downloadfiles/161228kojoguideline.pdf
  - 2-2-3-2.安全管理措置
    - 組織的安全管理措置
      - ⑤事故又は違反への対処
        - » (カ)事実関係、再発防止策等の公表

二次被害の防止、類似事案の発生回避等の観点から、個人データの漏えい等の事案が発生した場合は、可能な限り事実関係、再発防止策等を公表することが重要である。
ただし、例えば、以下のように、二次被害の防止の観点から公表の必要性がない場合には、事実関係等の公表を省略しても構わないものと考えられる。
(省略)
・**高度な暗号化等の秘匿化**が施されている場合(ただし、(オ)に定める報告の際、高度な暗号化等の秘匿化として施していた措置内容を具体的に報告すること。)

高度な暗号化等の秘匿化が施されている場合とは、例えば、**電子政府推奨暗号リスト**又はISO/IEC18033に掲げられている暗号アルゴリズムによって個人データを適切に暗号化し、**かつ、**復号(平文化)のための**かぎ(鍵)が適切に管理されている**と認められる場合など、十分な秘匿性が確保されている場合
http://www.meti.go.jp/policy/it_policy/privacy/downloadfiles/1212qa.pdf

暗号モジュール試験及び認証制度で認証された製品を使って、高度な暗号化等の秘匿化を実現できます。

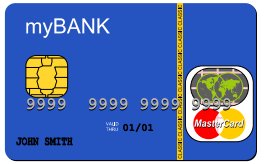
JCMVP制度の全体像

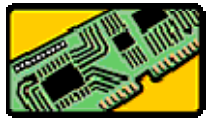


*2 ITSC: 一般社団法人 ITセキュリティセンター 評価部
ECSEC: 株式会社ECSEC Laboratory 評価センター
E&E: Epoche & Espri

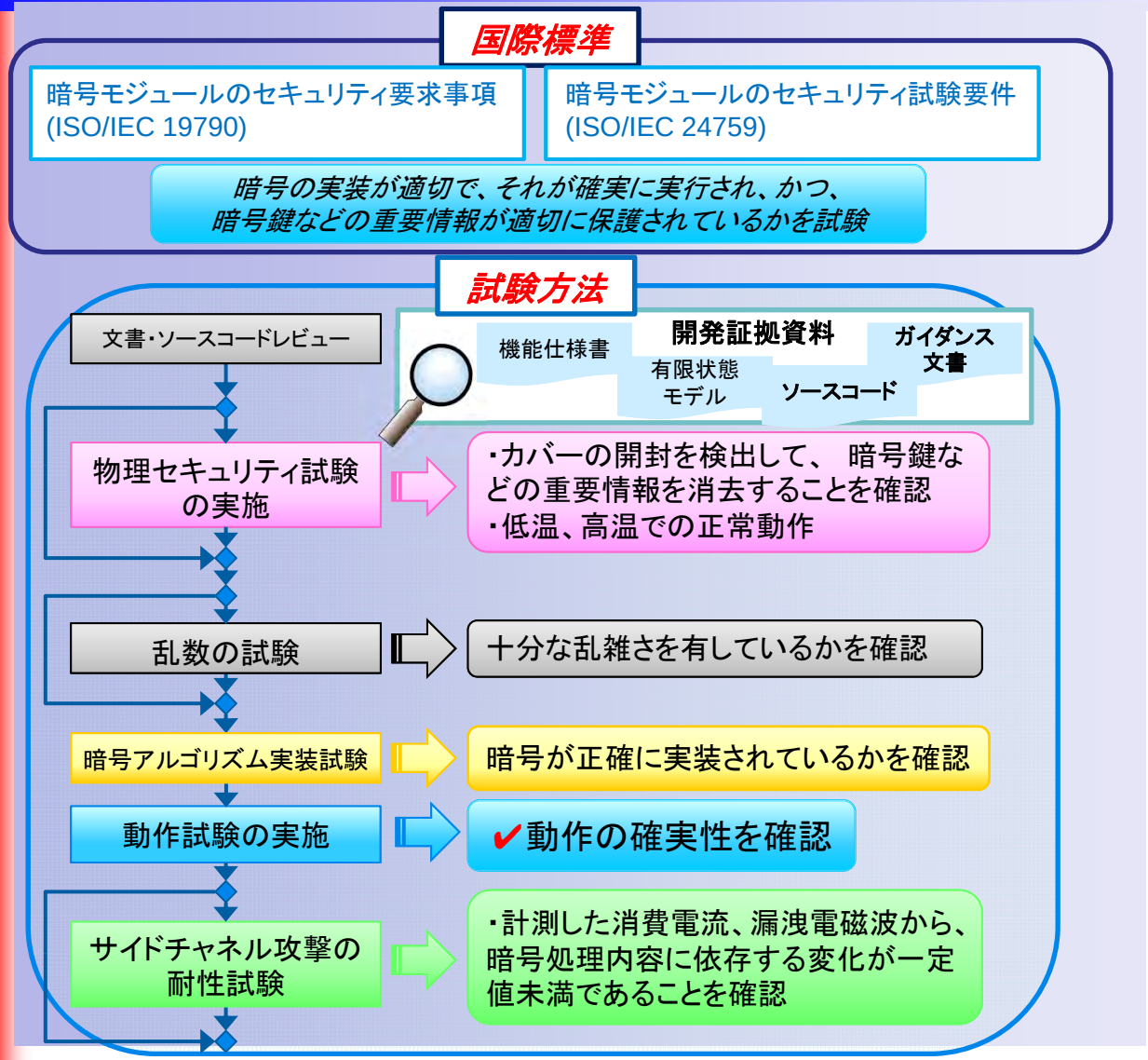
JCMVP認証適用可能な製品例

- スマートカード
- 暗号化記憶装置
- PCIカード
- HSM
  (ハードウェアセキュリティモジュール)
- ルータ
- ソフトウェア暗号ライブラリ
- ファイル暗号化ソフトウェア　等





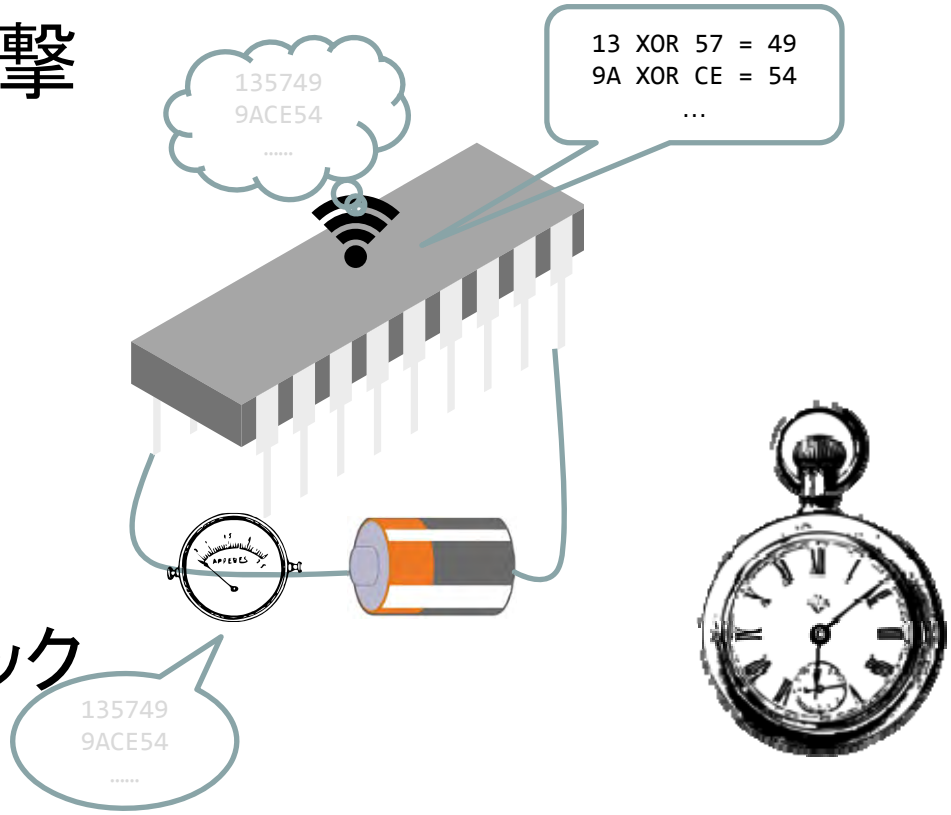
暗号モジュール試験及び認証制度の概要
暗号モジュール試験の流れ



※ ウォーターフォールである必要はない。

サイドチャネル情報
動作するICから漏れる情報

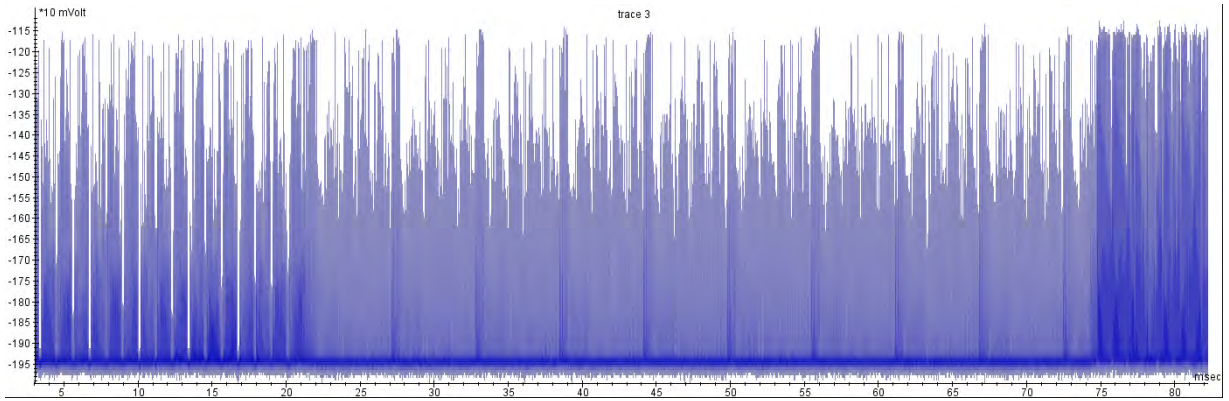
- ICの動作時には、消費電力や発散する電磁場などを通してある程度情報が漏れている
- サイドチャネル攻撃
  - 消費電力
    →電力解析
  - 電磁場
    →電磁解析
  - 処理時間
    →タイミングアタック



サイドチャネル情報
共通鍵暗号の消費電力の例

AES-128の消費電力波形の例

消費電力



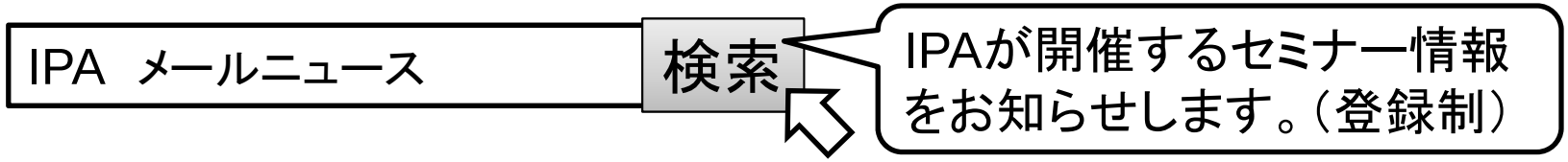
時刻

AESの繰り返し構造を反映した消費電力

ブースにて、サイドチャネル攻撃の実演動画公開中

まとめ

- 暗号モジュール試験及び認証制度は、
  - ベンダにとっては、安心して使用できる暗号モジュールであることのアピールに有効
  - 調達者にとっては、安心して使用できる暗号モジュールであるかどうかの判断材料となる
- 本日の内容をより詳細に解説するセミナーを定期的に開催しています。



情報セキュリティマネジメント試験 IPA

IT利用部門の情報セキュリティ管理の向上に役立つ国家試験
あらゆる部門で必要な、情報セキュリティ管理の知識を
体系的に習得できます。

◆受験をお勧めする方◆

- 個人情報を扱う全ての方
- 業務部門・管理部門で
  情報管理を担当する全ての方

◆試験実施日◆

年2回実施（春期・秋期）

春期：　4月第三日曜日

秋期：10月第三日曜日

ITパスポート試験

「ｉパス」は、ITを利活用する

すべての社会人・学生

が備えておくべきITに関する基礎的な知識が証明できる**国家試験**です。

試験の主なメリット

戦略、財務等幅広い出題	セキュリティを積極出題	エントリーシート等活用
▼	▼	▼
仕事に役立つ	**セキュリティに強くなる**	**就職に役立つ**

IPA 公式キャラクター

上峰 亜衣（うえみね あい）

パソコンを利用して受験するCBT方式なので、都合の良いときに受験可能！お申込みはｉパスWebサイトで常時受付中！


IPA
Better Life
with IT