

暗号モジュール試験及び認証制度

～安心して使える暗号モジュールとは～

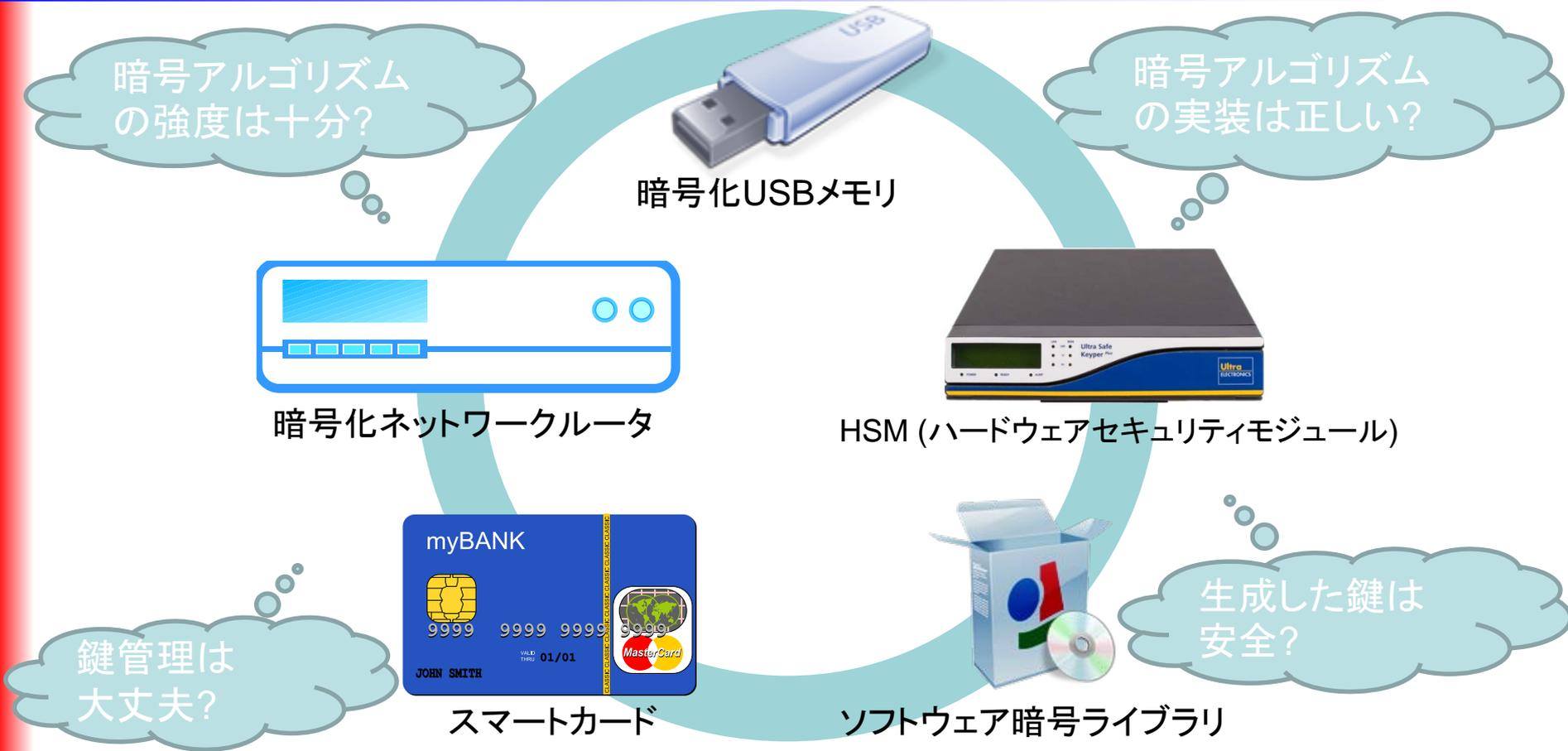
暗号モジュールとは何か



「承認されたセキュリティ機能」をソフトウェア/ファームウェア/ハードウェ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？



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

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

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 $p=\text{gcd}(N_1, N_2)$ 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

スマートメーター

- セキュリティ欠陥の例
 - *GCHQ intervened to change the original designs and save the £11bn nationwide system of smart energy meters against hackers on discovery of a fault, which meant all of the meters were given the same encryption key.*

<http://www.powerengineeringint.com/articles/2016/03/intervention-saves-11bn-uk-smart-meter-system-from-potential-mass-hack.html>

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： JCMVP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26年5月19日)
– 6.1.5 暗号・電子署名 <http://www.nisc.go.jp/active/general/pdf/guide26.pdf>
 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た製品であって、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ひも付く主体認証情報等が安全に保護される製品を利用することを前提とするため、**「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

個人情報保護に関連して

- 個人情報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26年12月12日)
http://www.meti.go.jp/policy/it_policy/privacy/downloadfiles/1212guideline.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)

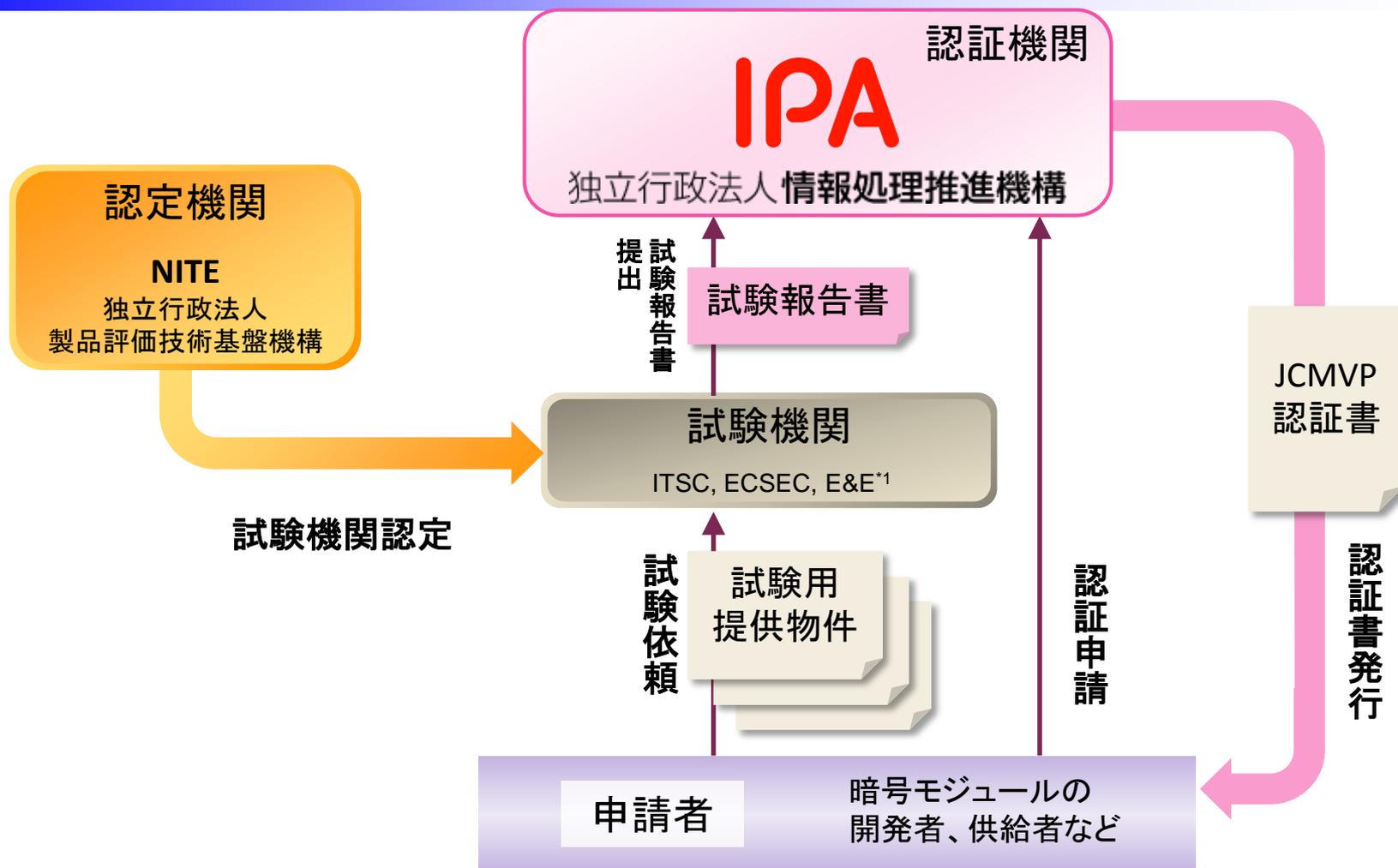
・ **高度な暗号化等の秘匿化**が施されている場合(ただし、(オ)に定める報告の際、高度な暗号化等の秘匿化として施していた措置内容を具体的に報告すること。)

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

国際標準

暗号モジュールのセキュリティ要求事項
(ISO/IEC 19790)

暗号モジュールのセキュリティ試験要件
(ISO/IEC 24759)

暗号の実装が適切で、それが確実に実行され、かつ、暗号鍵などの重要情報が適切に保護されているかを試験

試験方法

文書・ソースコードレビュー

機能仕様書

開発証拠資料

ガイダンス
文書

有限状態
モデル

ソースコード

物理セキュリティ試験
の実施

・カバーの開封を検出して、暗号鍵などの重要情報を消去することを確認
・低温、高温での正常動作

乱数の試験

十分な乱雑さを有しているかを確認

暗号アルゴリズム実装試験

暗号が正確に実装されているかを確認

動作試験の実施

✓ 動作の確実性を確認

サイドチャネル攻撃の
耐性試験

・計測した消費電流、漏洩電磁波から、暗号処理内容に依存する変化が一定値未満であることを確認

※ ウォーターフォールである必要はない。

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概要

- 文書レビュー
 - セキュリティポリシーの確認
 - 有限状態モデル (FSM)
 - 設計資料の確認
 - VEDキュメント (ベンダ情報要件の説明／参照先指定)
- ソースコードレビュー
 - FSM・設計資料とソースコードの一致
- 物理セキュリティ試験 (セキュリティレベル2以上)
- 暗号アルゴリズム実装試験
 - 暗号アルゴリズム実装試験ツール (JCATT) を用いたセキュリティ機能のブラックボックステスト
- 動作試験 (オペレーションテスト)
 - FSMとの一致 (エラー状態を含む)
 - ガイダンス文書との一致

FSM: Finite State Model (有限状態モデル)

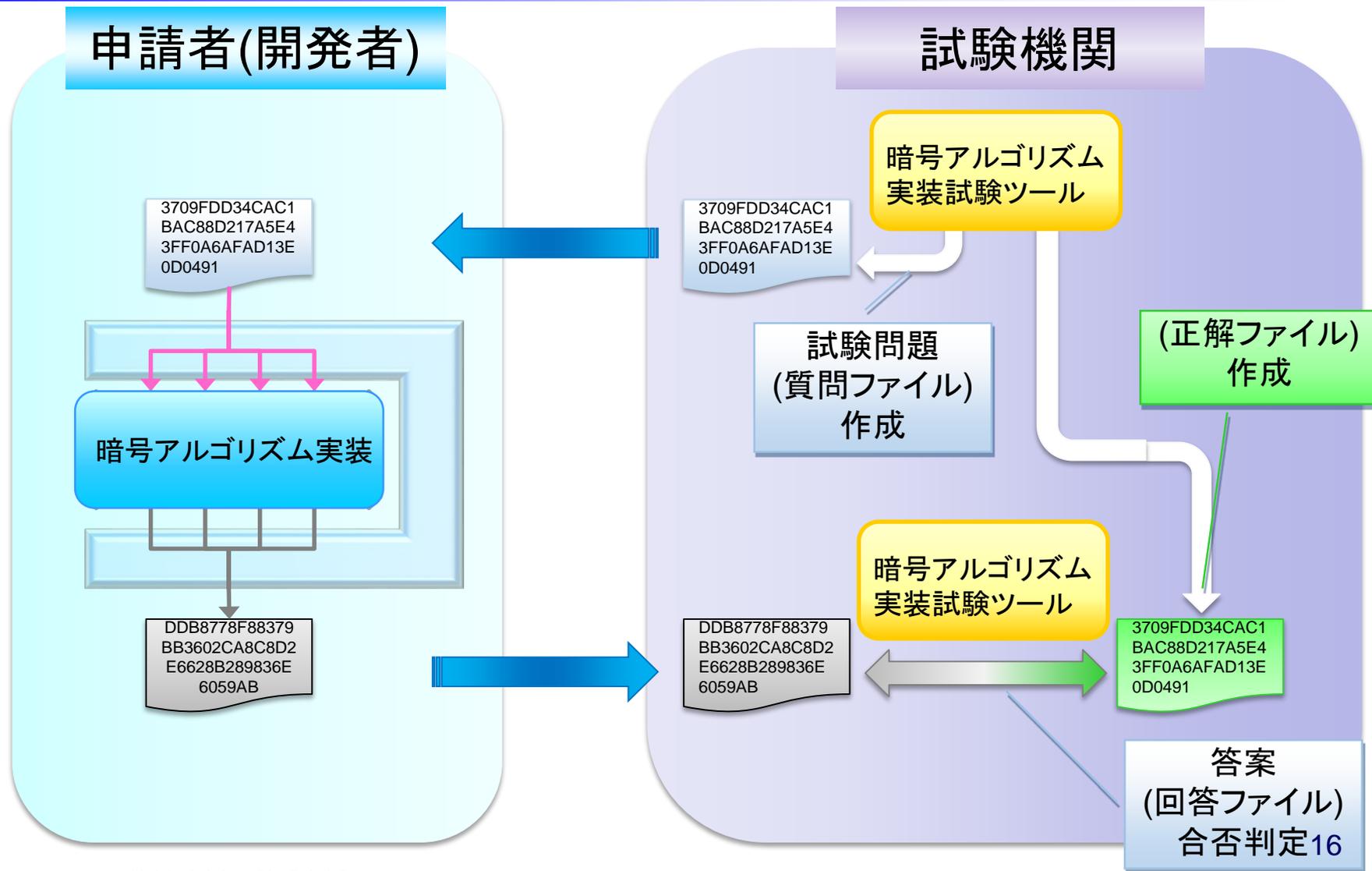
VE: Vendor Evidence (ベンダ証拠資料)

・試験要件の中でVEで識別された要件に対応

暗号モジュール試験及び認証制度の概要

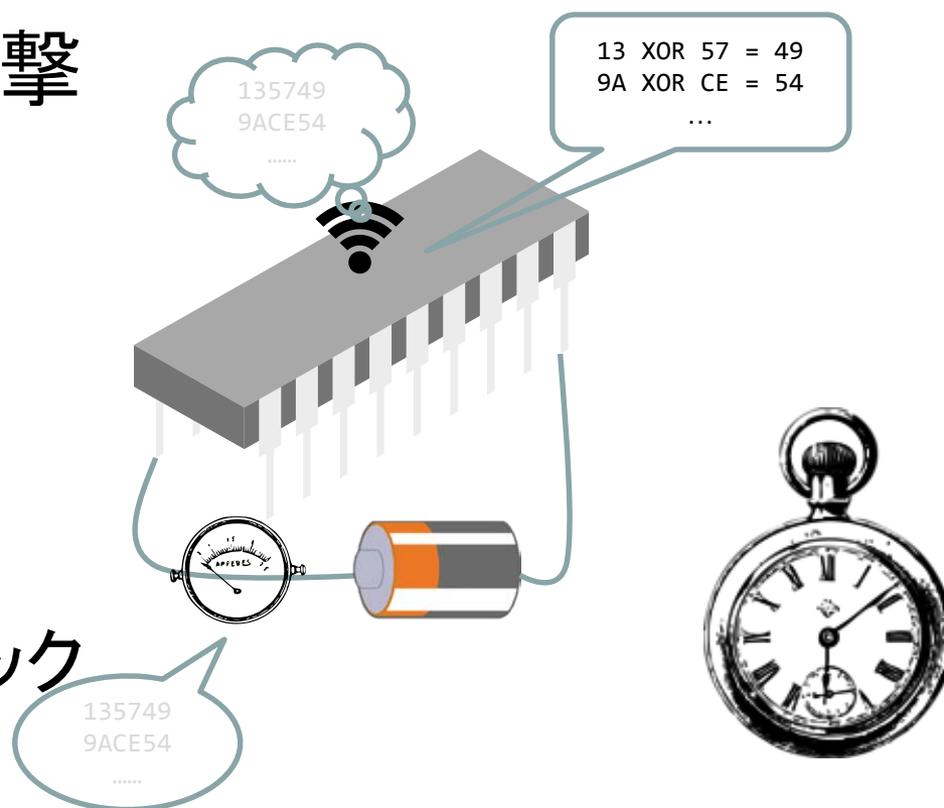
暗号モジュール試験概要

暗号アルゴリズム実装試験



サイドチャネル情報 動作するICから漏れる情報

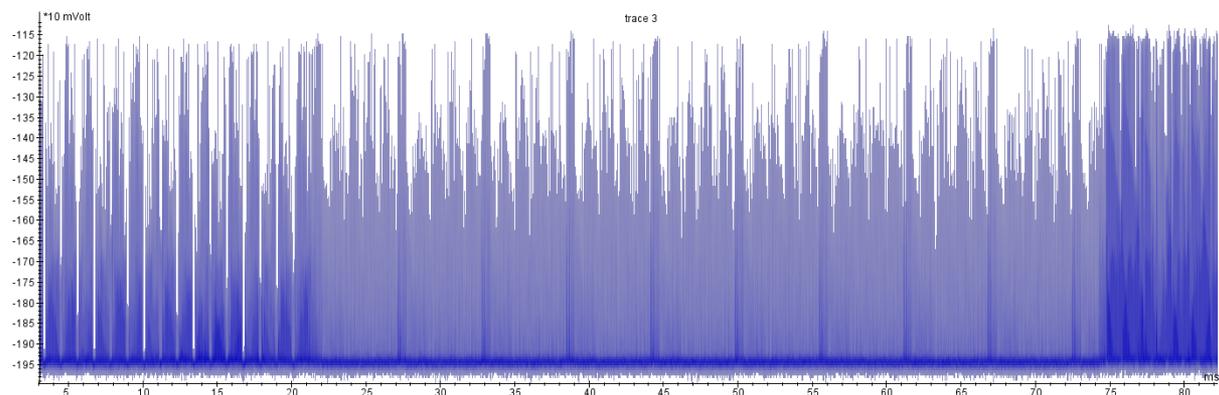
- ICの動作時には、消費電力や発散する電磁場などを通してある程度情報が漏れている
- サイドチャネル攻撃
 - 消費電力
→ 電力解析
 - 電磁場
→ 電磁解析
 - 処理時間
→ タイミングアタック



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
的に開催しています。

「暗号モジュール試験及び認証制度に関する説明会」
6月30日(木)開催予定

IPA メールニュース

検索

IPAが開催するセミナー情報
をお知らせします。(登録制)

新試験はじまる！ 情報セキュリティマネジメント試験

IPA

情報セキュリティの基礎知識から管理能力まで、
組織の情報セキュリティ確保に貢献し、脅威から
継続的に組織を守るための基本的スキルを認定する試験

国家試験 平成28年度春期開始
情報セキュリティマネジメント試験



初回応募者
約2万3千人！！

◆受験をお勧めする方◆

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

◆28年度秋期試験実施時期◆

- ・実施日 2016年10月16日(日)
- ・申込受付 2016年7月11日(月)から

パス ITパスポート試験

あなたのIT力を証明する国家試験



ITパスポート公式キャラクター
上峰亜衣(うえみねあい)

【プロフィール: マンガ】 <https://www3.jitec.ipa.go.jp/JitesCbt/html/uemine/profile.html>

「iパス」は、ITを活用する**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。

IPA

**Better Life
with IT**