暗号モジュール試験及び認証制度のご紹介

2016年3月29日

独立行政法人　情報処理推進機構
技術本部 セキュリティセンター

目次

- 暗号モジュール試験及び認証制度の概要
- 本制度における暗号アルゴリズムの移行
- ISO/IEC 19790:2012の紹介
- 関連する最新情報

目次

- 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
  - 第三者によって評価された製品を使うメリット
  - 暗号モジュール試験及び認証制度とは
    - 政府の調達要件における位置づけ
    - 個人情報の保護に関連して
  - 制度の全体像
  - 認証適用可能な製品例
  - 承認されたセキュリティ機能
  - 採用している標準
  - 暗号モジュール試験概要
  - 暗号モジュール認証の実績
- 本制度における暗号アルゴリズムの移行
- ISO/IEC 19790:2012の紹介
- 関連する最新情報

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(1)

- 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.*

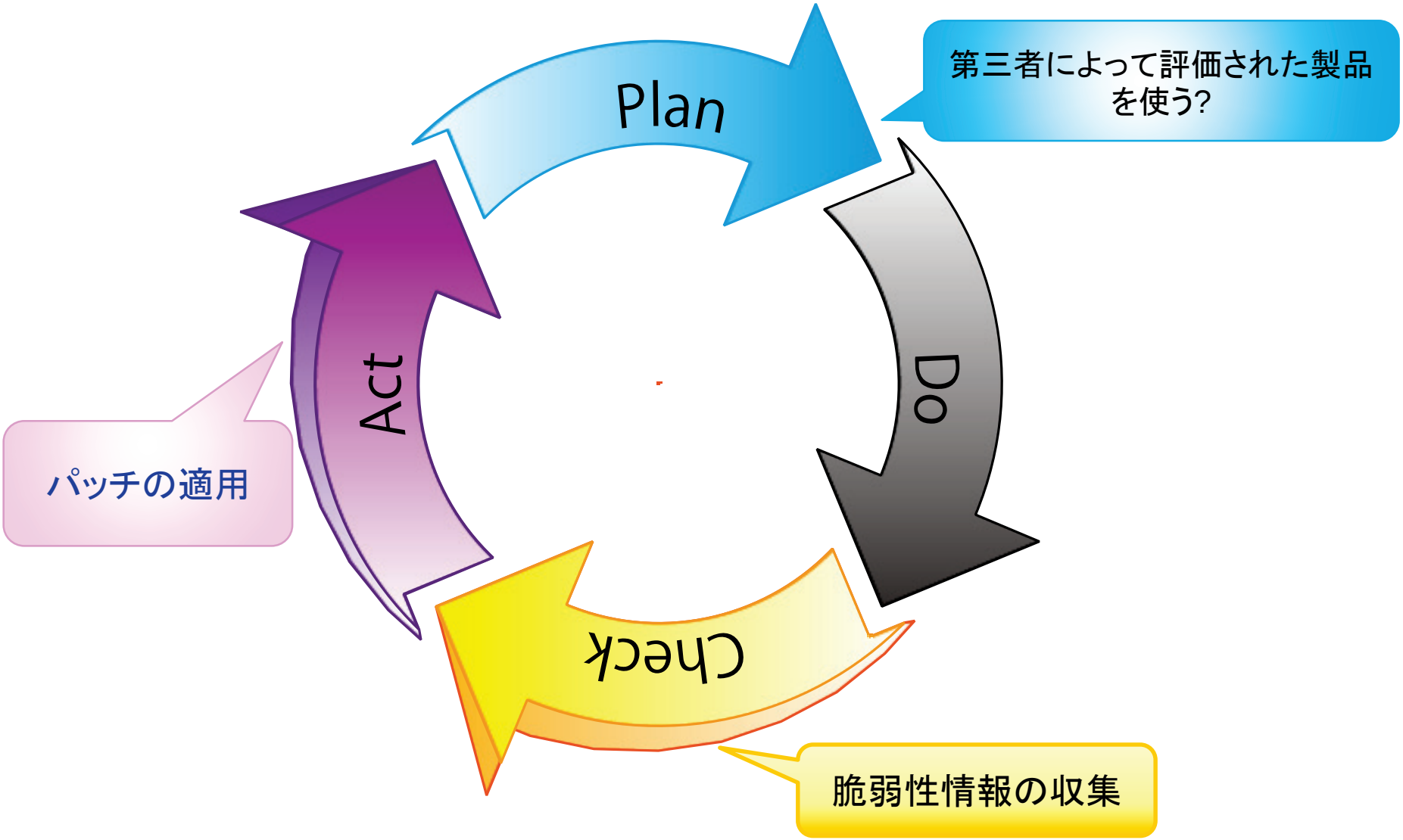
http://www.powerengineeringint.com/articles/2016/03/intervention-saves-11bn-uk-smart-meter-system-from-potential-mass-hack.html

暗号モジュール試験及び認証制度の概要
第三者による評価の有効性(2)

- 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
第三者によって評価された製品を使うメリット
― PDCAの観点から ―



目次

- 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
  - 第三者によって評価された製品を使うメリット
  - 暗号モジュール試験及び認証制度とは
    - 政府の調達要件における位置づけ
    - 個人情報の保護に関連して
  - 制度の全体像
  - 認証適用可能な製品例
  - 承認されたセキュリティ機能
  - 採用している標準
  - 暗号モジュール試験概要
  - 暗号モジュール認証の実績
- 本制度における暗号アルゴリズムの移行
- ISO/IEC 19790:2012の紹介
- 関連する最新情報

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

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
    基本対策事項 (1)-1

http://www.nisc.go.jp/active/general/pdf/guide26.pdf

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

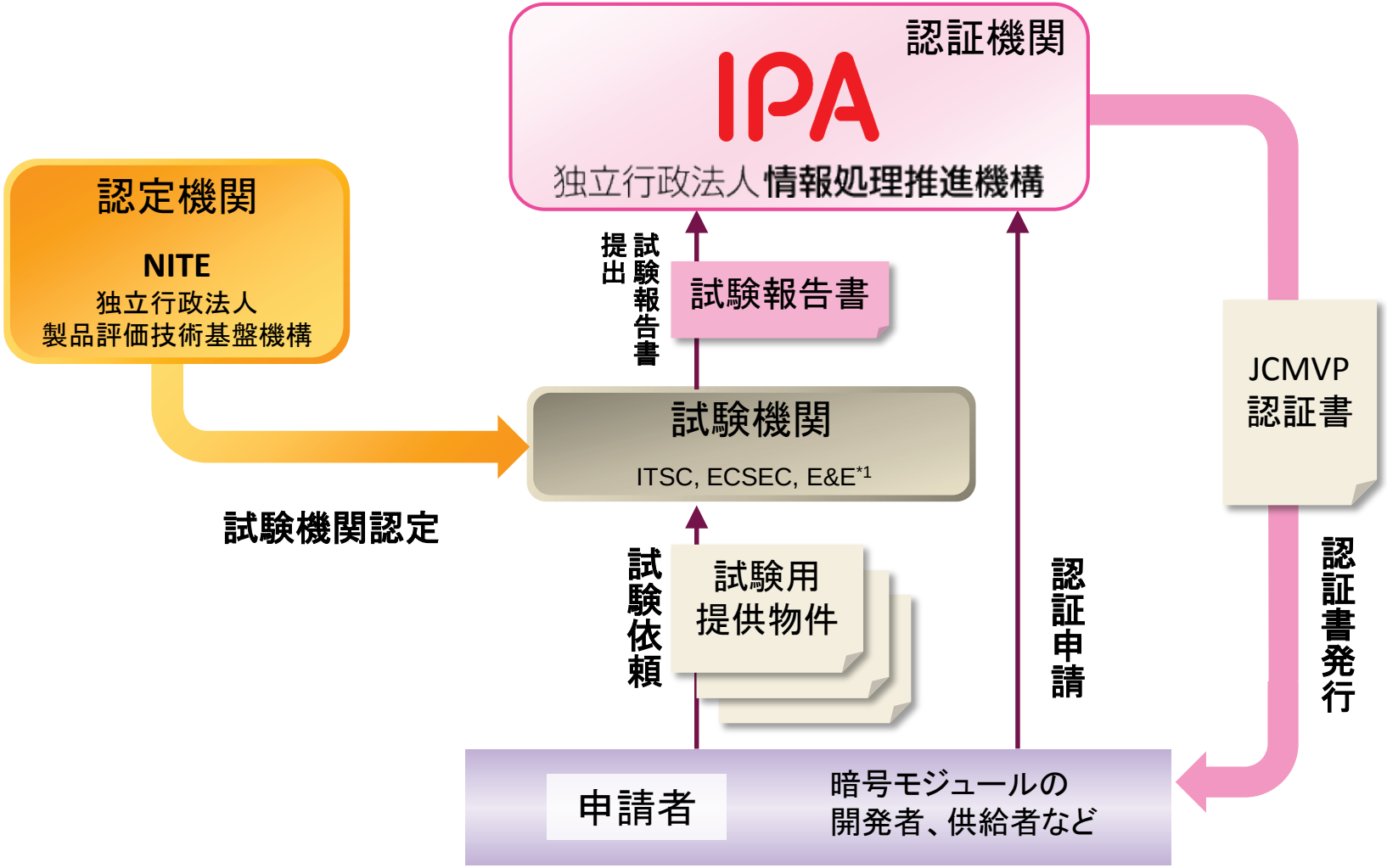
http://www.meti.go.jp/policy/it_policy/privacy/downloadfiles/1212qa.pdf

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。

目次

- 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
  - 第三者によって評価された製品を使うメリット
  - 暗号モジュール試験及び認証制度とは
    - 政府の調達要件における位置づけ
    - 個人情報の保護に関連して
  - 制度の全体像
  - 認証適用可能な製品例
  - 承認されたセキュリティ機能
  - 採用している標準
  - 暗号モジュール試験概要
  - 暗号モジュール認証の実績
- 本制度における暗号アルゴリズムの移行
- ISO/IEC 19790:2012の紹介
- 関連する最新情報

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
- 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

JCMVPとCMVPの差異
― 承認されたセキュリティ機能 ―

JCMVP制度で承認されたセキュリティ機能

RSA-OAEP
Camellia
KCipher-2

Approved Security Functions for FIPS 140-2

RSASSA-PKCS1-v1_5, RSASSA-PSS
DSA, ECDSA
AES, 3-key Triple DES
SHA-256,SHA-384,SHA-512,
HMAC-SHA-256, HMAC-SHA-384,
HMAC-SHA-512
CMAC, CCM, GCM/GMAC
SHA-1, SHA-224,
SHA-512/224, SHA-512/256,
HMAC-SHA-1, HMAC-SHA-224
HMAC-SHA-512/224, HMAC-SHA-512/256,
XTS

Random bit generators
・SP800-90A
(Hash_DRBG, CTR_DRBG, HMAC_DRBG)

SP800-56B
KDF(SP800-108,
SP800-132,
SP800-135 rev.1)

・FIPS 202
(SHA3-224, SHA3-256,
SHA3-384, SHA3-512,
SHAKE-128, SHAKE-256)

共通のセキュリティ機能

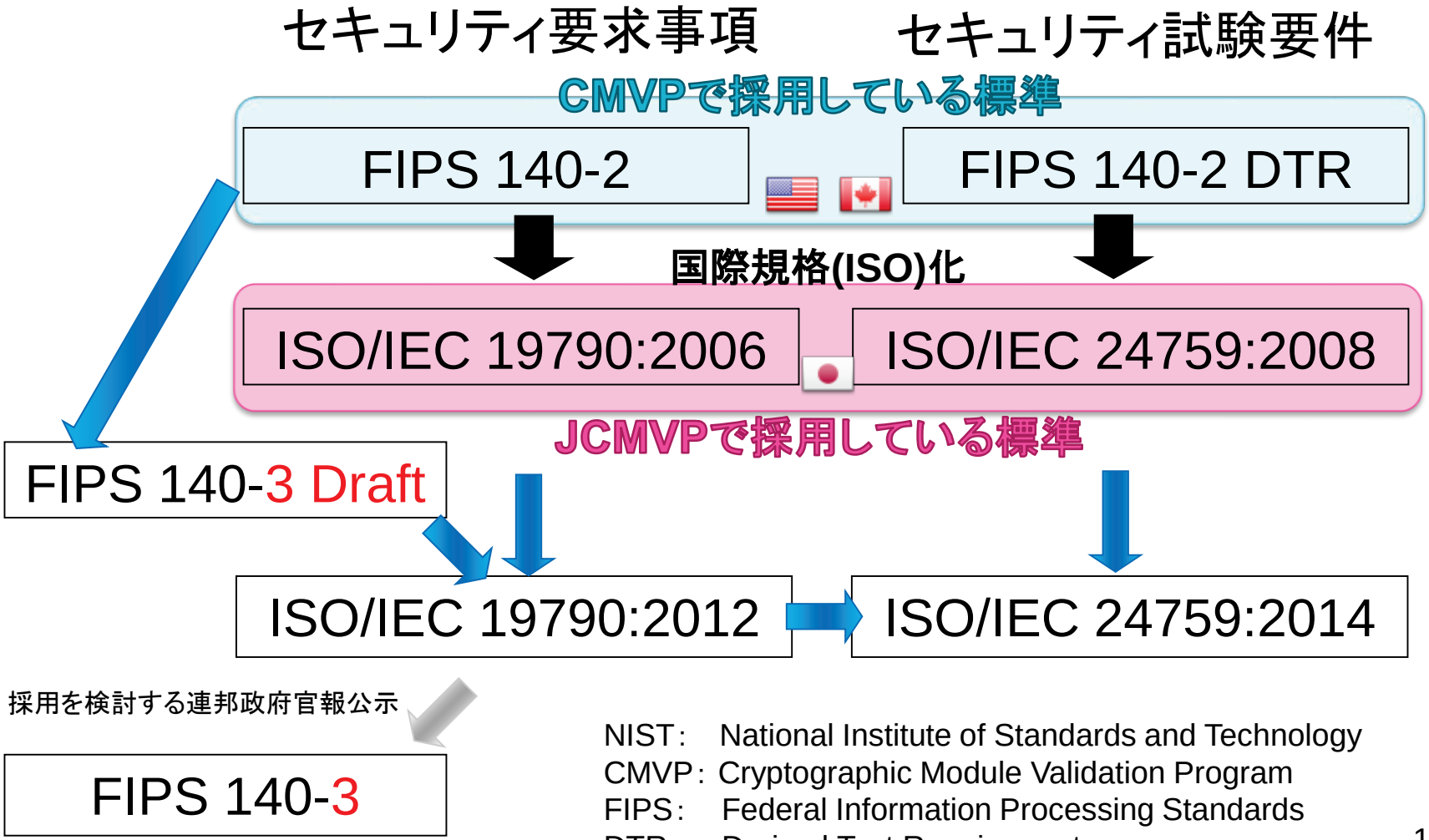
青字:
電子政府推奨暗号リスト

目次

- 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
  - 第三者によって評価された製品を使うメリット
  - 暗号モジュール試験及び認証制度とは
    - 政府の調達要件における位置づけ
    - 個人情報の保護に関連して
  - 制度の全体像
  - 認証適用可能な製品例
  - 承認されたセキュリティ機能
  - 採用している標準
  - 暗号モジュール試験概要
  - 暗号モジュール認証の実績
- 本制度における暗号アルゴリズムの移行
- ISO/IEC 19790:2012の紹介
- 関連する最新情報

JCMVPとCMVPが採用している標準(1)

- 米国・カナダのCMVPで採用している標準との関係



NIST： National Institute of Standards and Technology
CMVP： Cryptographic Module Validation Program
FIPS： Federal Information Processing Standards
DTR： Derived Test Requirements

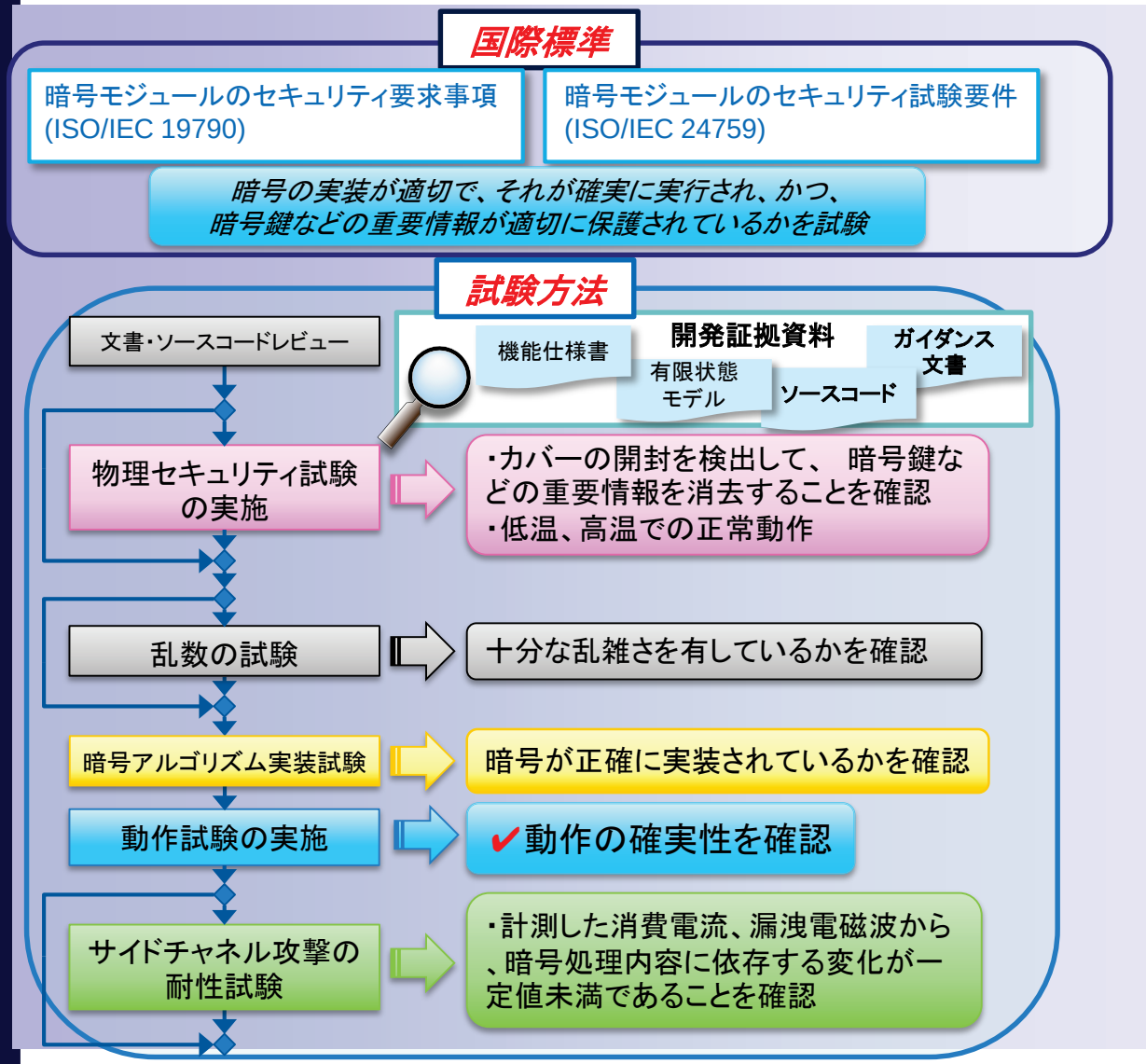
JCMVPとCMVPが採用している標準(2)
米国の動向

- ISO/IEC 19790:2012の採用を米国でも検討 (2015/8/12)

目次

- 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
  - 第三者によって評価された製品を使うメリット
  - 暗号モジュール試験及び認証制度とは
    - 政府の調達要件における位置づけ
    - 個人情報の保護に関連して
  - 制度の全体像
  - 認証適用可能な製品例
  - 承認されたセキュリティ機能
  - 採用している標準
  - 暗号モジュール試験概要
  - 暗号モジュール認証の実績
- 本制度における暗号アルゴリズムの移行
- ISO/IEC 19790:2012の紹介
- 関連する最新情報

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。

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の確認
  - 有限状態モデル (FSM)
  - 設計資料の確認
  - VEドキュメント (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

セキュリティポリシとは

- 暗号モジュールが従わなければならないセキュリティ規則を定めたもの
  - 満たすべき標準 (ISO/IEC 19790) の要求事項に基づくセキュリティ規則

公開用セキュリティポリシには最低限、次の項目について記述が必要。

a) 識別認証ポリシ
全ての役割及び認証のタイプ (IDベース、役割ベース等)
認証に必要なデータ (パスワード等)

b) アクセス制御ポリシ
役割において認可されたサービス、アクセスできる情報等

c) 物理セキュリティのポリシ

d) その他の攻撃への対処のポリシ

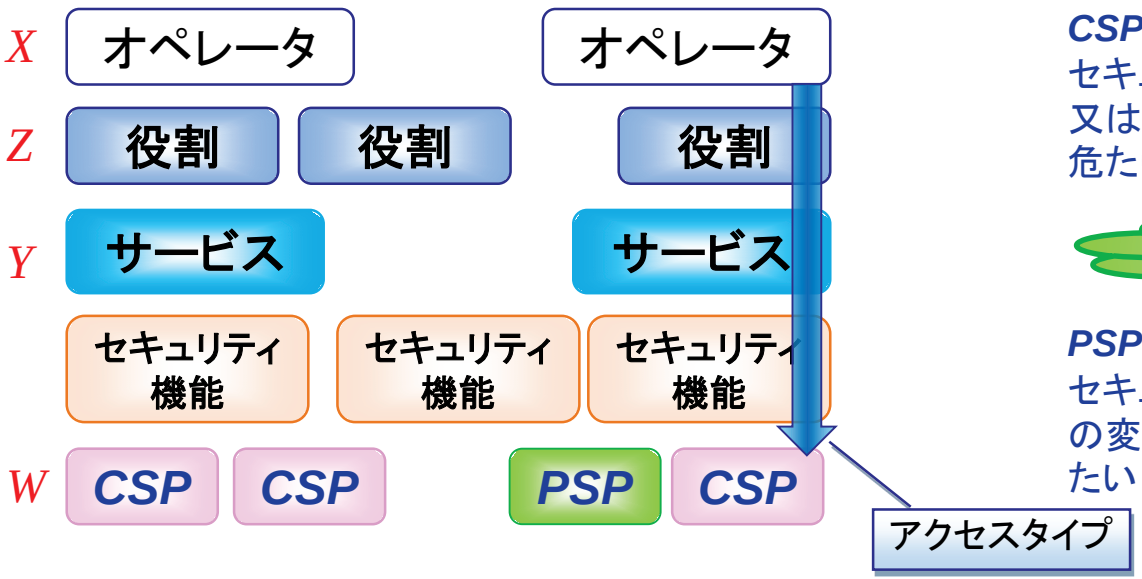
暗号モジュール試験及び認証制度の概要
暗号モジュール試験概要
セキュリティポリシにおける— アクセス制御ポリシ —

IPA

- ISO/IEC 19790の要求事項

セキュリティポリシは、次の質問に十分答えられるように詳述する必要がある。

「暗号モジュールに含まれるすべての役割，サービス及びセキュリティに関連するデータに対して，役割Zを担ってサービスYを実行しているオペレータXは，セキュリティに関連するデータ項目Wへのどのようなアクセスを行うか？」



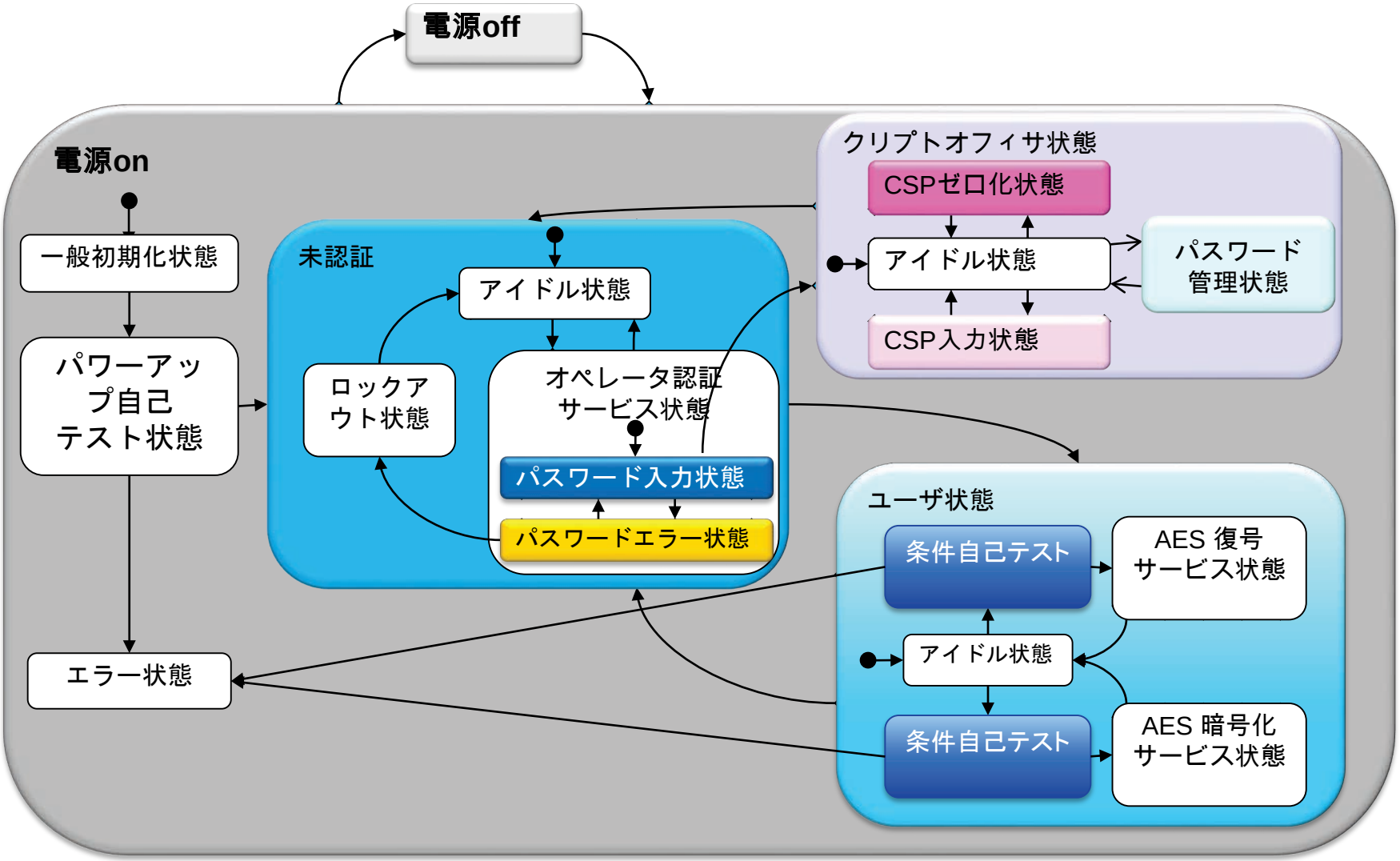
秘密鍵、認証データ等

CSP :Critical Security Parameter
セキュリティに関する情報であって，その開示又は変更が，暗号モジュールのセキュリティを危たい（殆）化し得るもの

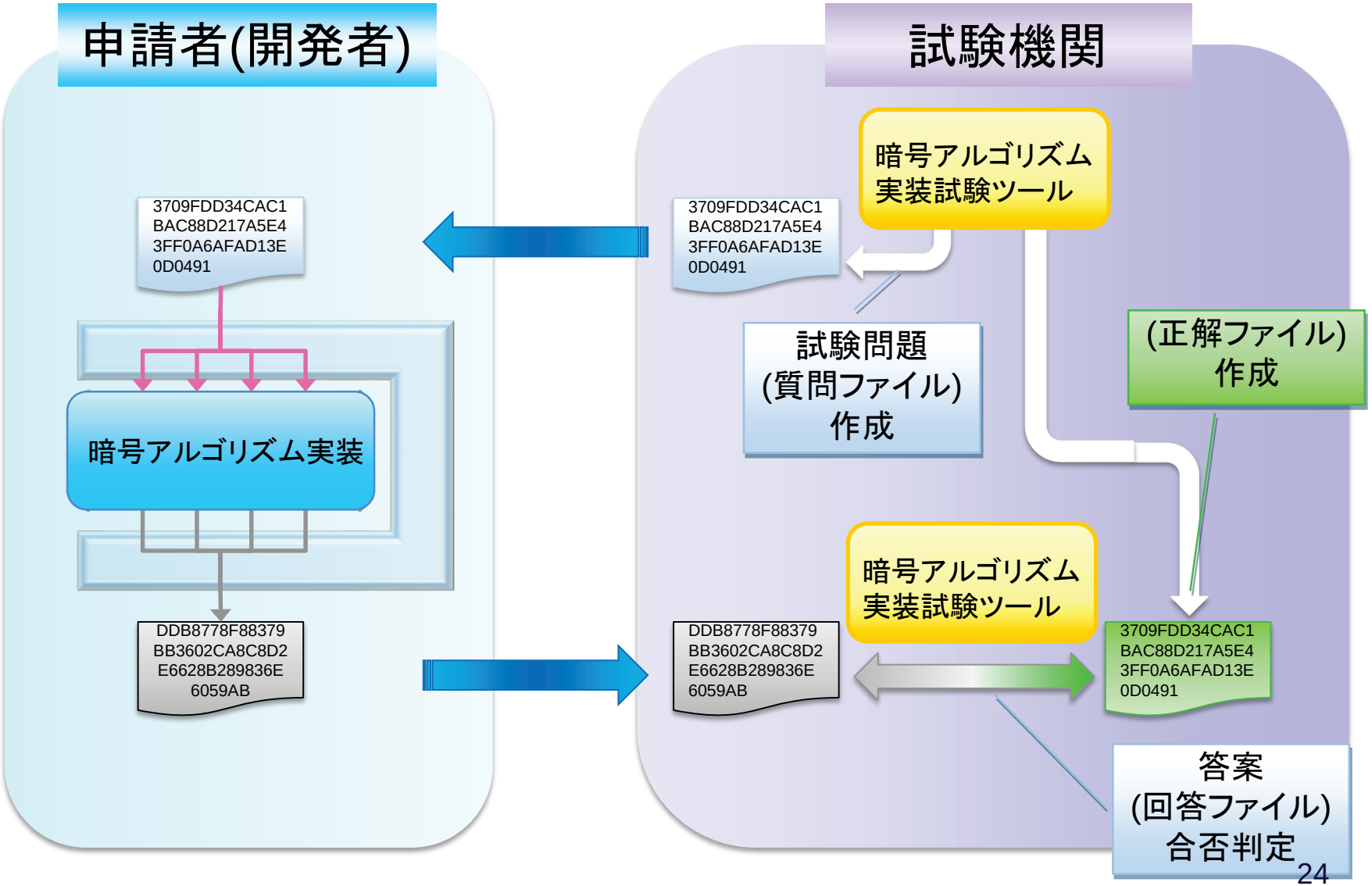
公開鍵、ドメインパラメタ等

PSP :Public Security Parameter
セキュリティに関連する公開情報であって，その変更が，暗号モジュールのセキュリティを危たい（殆）化し得るもの

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
有限状態モデルの参考（状態遷移図の例）



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

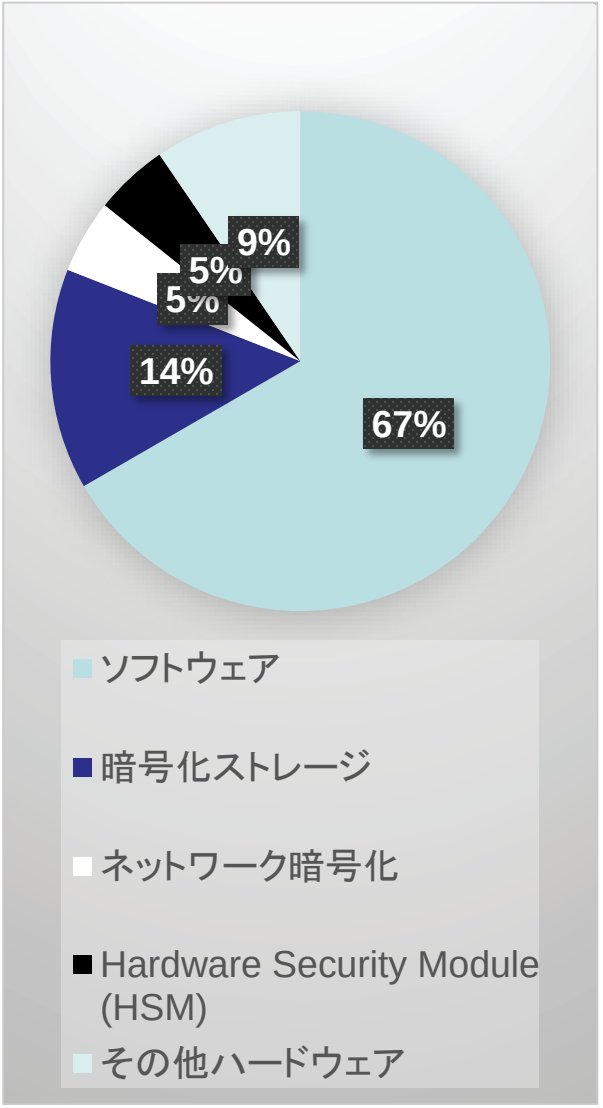


目次

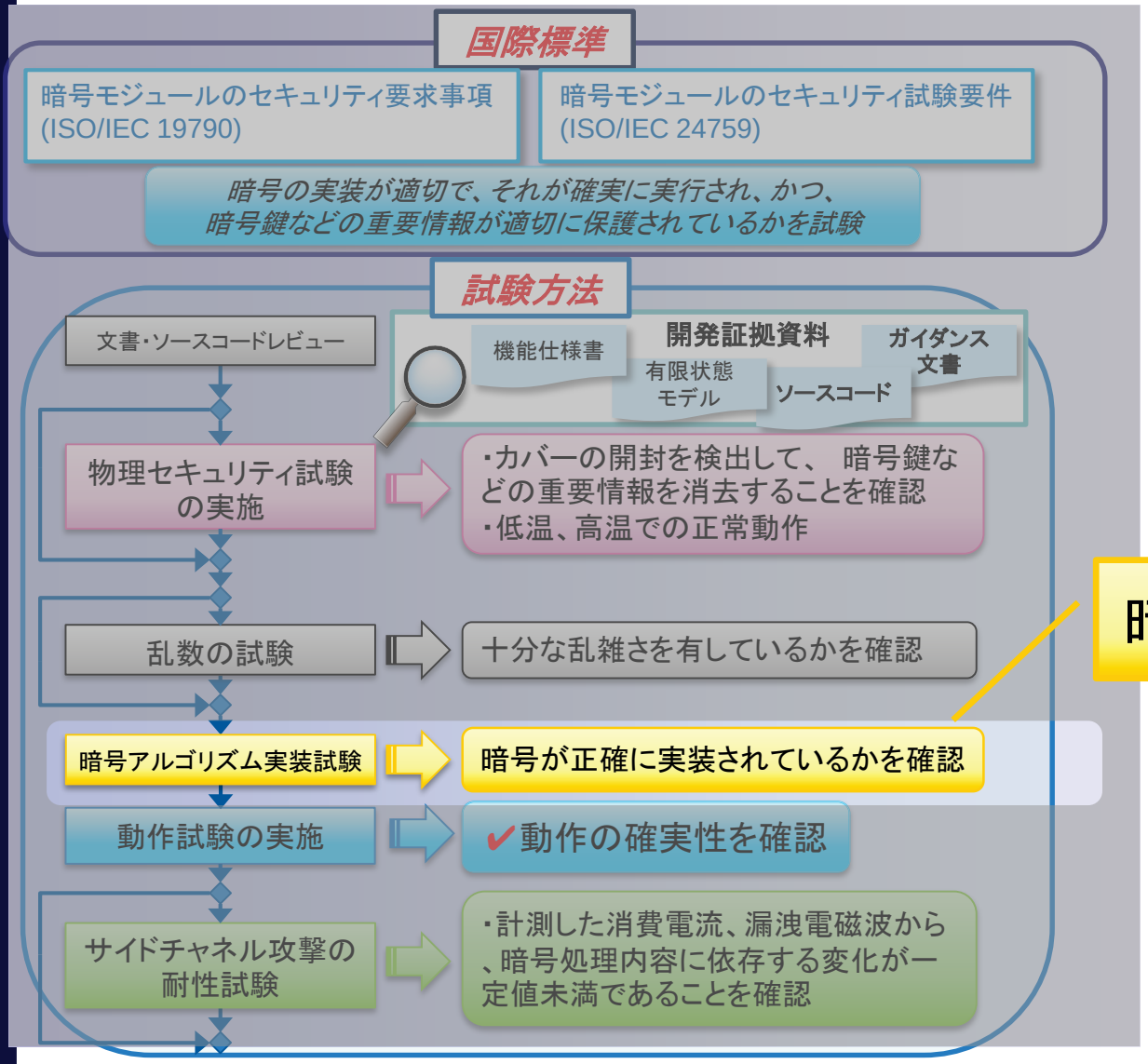
- 暗号モジュール試験及び認証制度の概要
  - 第三者による評価の有効性
  - 第三者によって評価された製品を使うメリット
  - 暗号モジュール試験及び認証制度とは
    - 政府の調達要件における位置づけ
    - 個人情報の保護に関連して
  - 制度の全体像
  - 認証適用可能な製品例
  - 承認されたセキュリティ機能
  - 採用している標準
  - 暗号モジュール試験概要
  - 暗号モジュール認証の実績
- 本制度における暗号アルゴリズムの移行
- ISO/IEC 19790:2012の紹介
- 関連する最新情報

暗号モジュール試験及び認証制度の概要
暗号モジュール認証の実績

JCMVP Cert. No	CMVP Cert. No	Vendor Name	Module Type	Overall Level
F0001		Toshiba Solutions Corporation	Software	1
F0002		Canon Inc.	Software	1
F0003		Tohoku University & AIST	Hardware	1
F0004		Canon Inc.	Software	1
J0005		Hitachi, Ltd.	Software	1
J0006		Toshiba Corporation	Hardware	1
J0007		Hitachi, Ltd.	Software	1
J0008		NEC Corporation	Software	1
F0009		NTT Electronics Corporation	Hardware	2
F0010		Canon Inc.	Software	1
F0011		PGP Corporation	Software	1
J0014		AIST	Hardware	1
J0015	1696	Hitachi Solutions, Ltd	Software	1
J0016	1697	Hitachi Solutions, Ltd	Software	1
J0017	1698	Hitachi Solutions, Ltd	Software	1
F0018	1269	Imation Corporation Japan	Hardware	3
J0019		NTT Electronics Corporation	Hardware	3
J0020	1962	ACES	Software	2
J0021	2350	Canon Inc.	Hardware	2

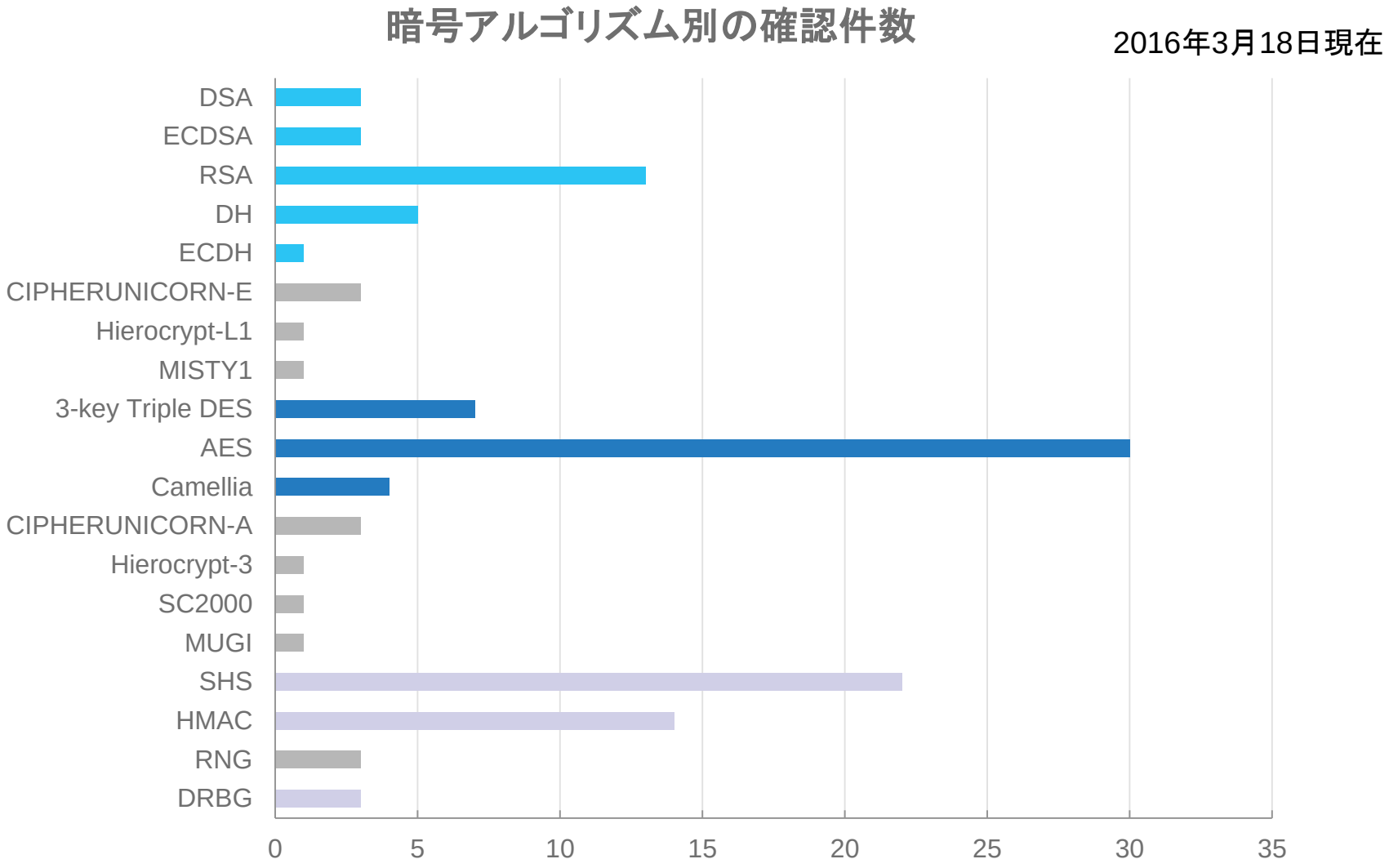


暗号モジュール試験及び認証制度の概要
暗号アルゴリズム実装試験と暗号アルゴリズム確認



暗号アルゴリズム確認

暗号モジュール試験及び認証制度の概要
暗号アルゴリズム確認の実績



暗号モジュール認証と暗号アルゴリズム確認

	暗号モジュール認証	暗号アルゴリズム確認
ベンダ提出物	認証申請書　、セキュリティポリシ、有限状態モデル、各種設計文書、ソースコード、VEドキュメント、マニュアル、回答ファイル	確認申請書、回答ファイル
試験期間	2ヶ月～	1週間程度
申請手数料 （試験費用を除く）	レベル1: 270,000円 レベル2: 385,700円 レベル3: 540,000円 レベル4: 756,000円	21,600円 （セキュリティ機能の数に制限はありません。）
暗号アルゴリズム確認書の交付	○	○
暗号モジュール認証書の交付	○	ー
認証マークの使用	○	×

目次

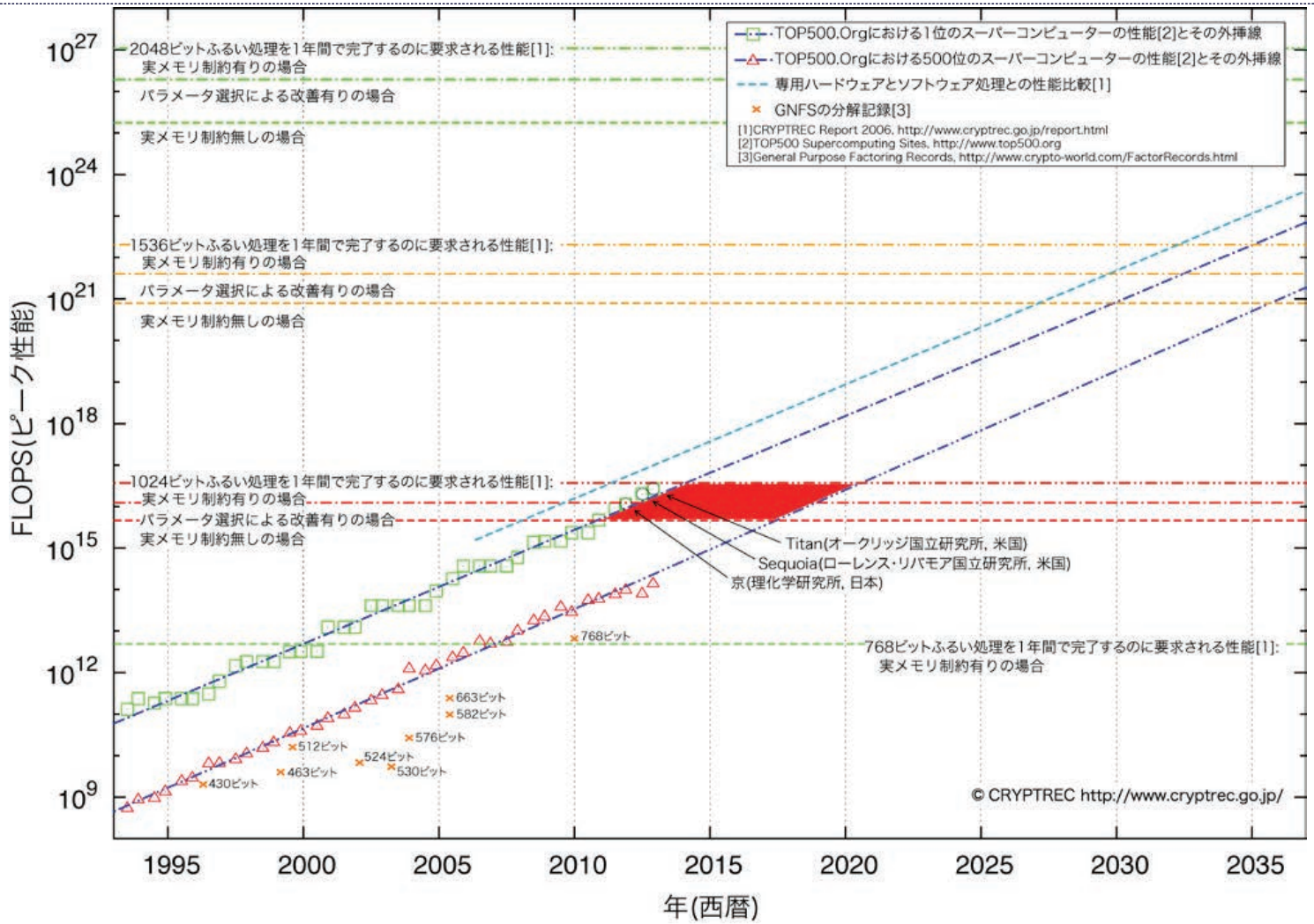
- 暗号モジュール試験及び認証制度の概要
- 本制度における暗号アルゴリズムの移行
  - 暗号の世代交代の必要性
  - 基本移行方針
  - 承認されたセキュリティ機能の変更点
    - 公開鍵暗号
    - 共通鍵暗号、ハッシュ関数
    - メッセージ認証、乱数生成器
    - 鍵確立
- ISO/IEC 19790:2012の紹介
- 関連する最新情報

暗号の世代交代の必要性

- 計算機の性能向上により、今まで安全とされていたアルゴリズムや鍵長が、十分安全とはいえなくなりつつある。
  - 例
    - 2009年に、RSA-768が素因数分解された
    - 1024ビットRSAは、次第に十分安全とはいえなくなりつつある

T. Kleinjung, et. al. *Factorization of a 768-Bit RSA Modulus*, Advances in Cryptography – CRYPTO 2010, LNCS Volume 6223, 2010, pp 333-350

素因数分解の解読推移と予測



1年でふるい処理を完了するのに要求される処理能力の予測(2013年2月更新)

CRYPTRECシンポジウム2013 (http://www.cryptrec.go.jp/symposium/20130326_cryptrec-cpe.pdf)

目次

- 暗号モジュール試験及び認証制度の概要
- 本制度における暗号アルゴリズムの移行
  - 暗号の世代交代の必要性
  - 基本移行方針
  - 承認されたセキュリティ機能の変更点
    - 公開鍵暗号
    - 共通鍵暗号、ハッシュ関数
    - メッセージ認証、乱数生成器
    - 鍵確立
- ISO/IEC 19790:2012の紹介
- 関連する最新情報

本制度における暗号アルゴリズムの移行
承認されたセキュリティ機能の基本移行方針

- NISTやCRYPTRECの動きを参考に、JCMVPでは以下の方針を選択
  - 方針1:
    112-bit未満の強度の暗号アルゴリズムは、2014年3月末を以て承認を取り消す。
    - 但し、互換性の目的で112-bit未満の強度の暗号を次の用途に使用することは認める。
      - 既に生成された電子署名の検証
        - » SHA-1はこの理由により署名検証用途に使用することは認める。
      - 既に生成された暗号文の復号
  - 方針2:
    電子政府推奨暗号リストから外れた暗号アルゴリズムについては2014年3月末を以て承認を取り消す。推奨候補暗号リストのアルゴリズムについては、暗号アルゴリズム確認対象の非承認暗号アルゴリズムとする。
  - 方針3:
    NIST SP800-90A以外の”legacy”な乱数生成アルゴリズムは、2015年12月末を以て承認を取り消す。

目次

- 暗号モジュール試験及び認証制度の概要
- 本制度における暗号アルゴリズムの移行
  - 暗号の世代交代の必要性
  - 基本移行方針
  - 承認されたセキュリティ機能の変更点
    - 公開鍵暗号
    - 共通鍵暗号、ハッシュ関数
    - メッセージ認証、乱数生成器
    - 鍵確立
- ISO/IEC 19790:2012の紹介
- 関連する最新情報

本制度における暗号アルゴリズムの移行
JCMVPで承認されたセキュリティ機能の変更点 (公開鍵暗号)

技術分類		暗号名称
公開鍵暗号	署名	DSA(*1), ECDSA(*2), RSASSA-PKCS1-v1.5(*3), RSASSA-PSS(*3)
	守秘	RSA-OAEP(*4), ~~RSA-PKCS-v1.5~~

*1: |p|が2048ビット未満あるいは|q|が224ビット未満のものは署名検証のみ許可。
|p|が2048ビット以上かつ|q|が224ビット以上のものは今後も使用可
*2: |n|が224ビット未満のものは署名検証のみ許可。
|n|が224ビット以上の場合は今後も使用可。
*3: |n|が2048ビット未満のものは署名検証のみ許可。
|n|が2048ビット以上のものは今後も使用可。
*4: |n|が2048ビット未満のものは復号のみ許可。
|n|が2048ビット以上のものは今後も使用可。

本制度における暗号アルゴリズムの移行
JCMVPで承認されたセキュリティ機能の変更点 (共通鍵暗号, ハッシュ関数)

技術分類		暗号名称
共通鍵暗号	64ビットブロック暗号	~~CIPHERUNICORN-E, Hierocrypt-L1, MISTY1,~~ 3-key Triple DES
	128ビットブロック暗号	AES, Camellia, ~~CIPHERUNICORN-A, Hierocrypt-3, SC2000~~
	ストリーム暗号	~~MUGI, MULTI-S01, 128-bit RC4,~~KCipher-2
	ブロック暗号利用モード	ECB, CBC, CFB , OFB, CTR, XTS
ハッシュ関数		~~RIPEMD160,~~ SHA-1(*5), SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256

*5: 署名生成の用途には使用不可。署名検証の用途には使用可。
その他の用途には使用可。

本制度における暗号アルゴリズムの移行
JCMVPで承認されたセキュリティ機能の変更点 (メッセージ認証, 乱数生成器)

技術分類	暗号名称
メッセージ認証	HMAC(*6), CMAC, CCM, GCM
乱数生成器	Hash_DRBG, HMAC_DRBG and CTR_DRBG in NIST SP800-90A ~~PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1,~~ ~~PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1,~~ ~~RNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1,~~ ~~NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms~~

*6: 鍵長80ビット以上112ビット未満は検証のみ使用可。
鍵長112ビット以上は今後も使用可

CMVPにおける暗号アルゴリズムの移行と関連する事項

- 乱数生成器(Random Number Generator)の移行
  - Active Validation Lists
    - 古い乱数生成器を使わず、認証日から5年以内の暗号モジュール
  - Historical List
    - 古い乱数生成器を使う暗号モジュールを含めて掲載

本制度における暗号アルゴリズムの移行
JCMVPで承認されたセキュリティ機能の変更点 (鍵確立)

技術分類		暗号名称
鍵確立		DH(*8), ECDH(*9)(*10),MQV(*8),ECMQV(*9), NIST SP800-56B(*11), ~~PSEC-KEM~~
	KDF	NIST SP800-56C, NIST SP800-108, NIST SP800-132, NIST SP800-135 Revision 1 (TPMに基づくKDFは除く)

*8: |p|が2048ビット未満かつ|q|が224ビット未満のものは不許可。
|p|が2048ビット以上かつ|q|が224ビット以上のものは今後も使用可。
*9: |n|が224ビット未満のものは使用不可。
|n|が224ビット以上の場合は今後も使用可。
*10: SP800-56Aに基づかないもの(SEC1)は非推奨。
*11: |n|が1024ビットのものは使用不可。
|n|が2048ビットのものは今後も使用可。

目次

- 暗号モジュール試験及び認証制度の概要
- 本制度における暗号アルゴリズムの移行
- ISO/IEC 19790:2012の紹介
  - 暗号モジュールのセキュリティ要求事項の要約
  - ISO/IEC 19790:2006との比較
    - 機能に関する改訂された要求事項
    - 保証に関する改訂された要求事項
  - ISO/IEC 19790:2012に関連するIPAの取り組み
    - 国際標準化
    - JIS原案作成
- 関連する最新情報

ISO/IEC 19790:2012
暗号モジュールのセキュリティ要求事項

- ISO/IEC 19790:2012とは
  - コンピュータ及び通信システムにおける取扱いに慎重さを要する情報を保護するセキュリティシステムの中で使用される暗号モジュールに対するセキュリティ要求事項を規定する。

- 経緯
  - 次の文書をベースにして国際標準化された
    - FIPS 140-2を国際標準化したISO/IEC 19790:2006
    - FIPS 140-2 Implementation Guidanceの一部
    - FIPS 140-3 Draft
  - 2012年8月発行
  - 2015年12月訂正再発行

- 用途(国際標準の観点から)
  - ストレージセキュリティ
    - ISO/IEC 27040:2015
  - モバイルバンキング
    - ISO/DIS 12812-2
  - ホーム エレクトロニクス システム(HES)
    - ISO/IEC 14543-5-1:2010

ISO/IEC 19790:2012
暗号モジュールのセキュリティ要求事項

- セキュリティ要求事項は11分野(側面)に分類
  - 暗号モジュールの仕様
  - 暗号モジュールのインタフェース
  - 役割, サービス及び認証
  - ソフトウェア・ファームウェアセキュリティ
  - 動作環境
  - 物理セキュリティ
  - 非侵襲セキュリティ
  - Sensitive Security Parameter管理
  - 自己テスト
  - ライフサイクル保証
  - その他の攻撃への対処
- 1～4のセキュリティレベルを定義
  - セキュリティレベルの数値が大きいほど、より多くの要求事項を満たす必要がある。

ISO/IEC 19790:2012
暗号モジュールのセキュリティ要求事項の要約(1)

	セキュリティレベル1	セキュリティレベル2	セキュリティレベル3	セキュリティレベル4
暗号モジュールの仕様	暗号モジュールの仕様　暗号境界　承認されたセキュリティ機能　通常動作モード、縮退動作モード　すべてのハードウェア、ソフトウェア及びファームウェア構成要素を含む暗号モジュールの記述　すべてのサービスについて、承認された暗号アルゴリズム、セキュリティ機能又はプロセスをサービスが承認された方法で使用していることを表す状態表示			
暗号モジュール インタフェース	必須及び追加のインタフェース　すべてのインタフェース、すべての入出力データパスの仕様		高信頼チャネル	
役割、サービス・認証	必須及び追加の役割 並びに サービスの論理的分離	役割ベース又はIDベースのオペレータ認証	IDベースのオペレータ認証	多要素認証
ソフトウェア/ ファームウェア セキュリティ	承認された完全性技術 定義されたSFMI, HFMI及びHSMI	承認されたデジタル署名又はメッセージ認証子に基づく完全性テスト	承認されたデジタル署名に基づく完全性テスト	
動作環境	変更不可、限定又は変更可能な動作環境 SSPの管理	変更可能な動作環境		
物理セキュリティ	製品グレードの構成要素	タンパー証跡 不透明なカバー又は筐体	カバー及びドアに対してのタンパー検出及びタンパー応答 強固な囲い又はコーティング　EFP 又は EFT	タンパー検出及びタンパー応答包被　EFP　故障誘導対策
非侵襲セキュリティ	Annex Fに規定された非侵襲攻撃に対処するよう設計			
	Annex Fに規定された対策技術の有効性の文書化		対策技術のテスト	対策技術のテスト

DIS : Draft International Standard
(IS : International Standard(国際標準)の2歩手前)

ISO/IEC 19790:2012
暗号モジュールのセキュリティ要求事項の要約(2)

		セキュリティレベル1	セキュリティレベル2	セキュリティレベル3	セキュリティレベル4
Sensitive Security Parameter 管理		乱数ビット生成器　SSPの生成、確立、入出力、格納及びゼロ化			
		自動化されたSSPの転送方法 又は 承認された方法を用いたSSPの確立			
		手動で確立されるSSPは、平文で入出力されても良い		手動で確立されるSSPは、暗号化された形式又は知識分散法を使って入出力	
自己テスト		動作前自己テスト:ソフトウェア/ファームウェア完全性テスト、バイパステスト、重要機能テスト			
		条件自己テスト:暗号アルゴリズムテスト、鍵ペア整合性テスト、ソフトウェア/ファームウェアロードテスト、手動鍵入力テスト、条件バイパステスト 及び 重要機能テスト			
ライフサイクル保証	構成管理	暗号モジュール、構成要素及び文書に対する構成管理システム ライフサイクルを通じて各々の構成要素が一意に識別され追跡可能		自動化された構成管理システム	
	設計	すべてのセキュリティ関連サービスのテストを可能にするような設計			
	FSM	有限状態モデル			
	開発	コメント付けされたソースコード、回路図又はHDL	高級言語の使用		事前条件、 事後条件の文書化
	ベンダ試験	機能試験		詳細試験	
	配付及び運用	初期化手順	配付手順		ベンダ提供認証情報に基づくオペレータ認証
	ガイダンス	管理者 及び 非管理者ガイダンス			
その他の攻撃への対処		現在、試験要件が整備されていないような攻撃への対処技術の仕様			試験要件と攻撃への対処の仕様

ISO/IEC 19790:2012
ISO/IEC 19790:2006との比較(1)

- 機能に関する改訂された要求事項
  - 縮退動作(degraded operation)
    - 耐障害性を実現したいというニーズに対応
      → 条件自己テストに失敗しても、継続動作を許容。
  - 暗号出力の自動開始機能
    - VPNルータのようなデバイスが、再起動時に管理者不在であっても暗号化通信を開始できる。

ISO/IEC 19790:2012 ISO/IEC 19790:2006との比較(2)

- 機能に関する改訂された要求事項
  - 自己テスト
    - 起動時に行う自己テストの項目削減
      → 非接触スマートカードの応答時間の短縮
    - 暗号アルゴリズムの仕様で定められた、暗号アルゴリズム特有の自己テストを実施しなければならない。
    - 連続乱数生成器テストの削除
      → SP800-90B(Draft)で代替自己テストの記述あり
      (乱数生成器の素性に応じた自己テスト設計)

ISO/IEC 19790:2012 ISO/IEC 19790:2006との比較(3)

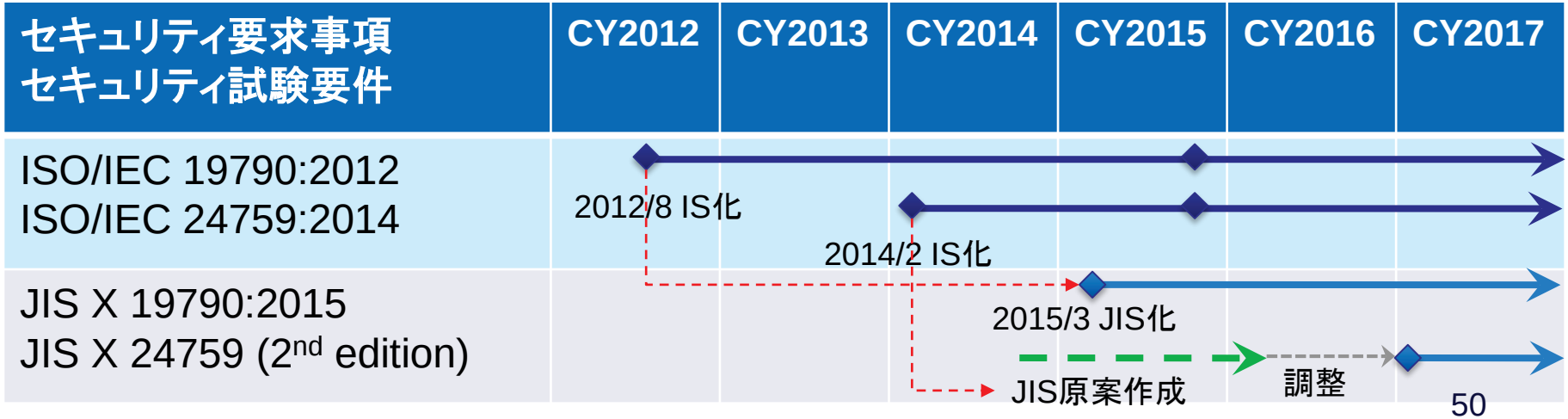
- 保証に関する改訂された要求事項
  - 入出力フォーマットの規定
    - ソフトウェア・ファームウェアのセキュリティの重視
  - 特権昇格しないことの確認
  - サイドチャネル解析
    - サイドチャネル解析対策を行っている場合
  - ベンダーによる試験
    - レベル1,2
      - 機能試験
    - レベル3, 4
      - 詳細試験

ISO/IEC 19790:2012に関連するIPAの取り組み
国際標準化

2009/5	ISO/IEC 19790 (2nd edition)の早期改訂に参加
2011/4	ISO/IEC 24759 (1st edition)の早期改訂に参加
2012/8	ISO/IEC 19790:2012の発行.
2013/1	JIS X 19790 (2nd edition)の原案作成開始
2014/2	JIS X 19790 (2nd edition)の原案作成完了
2014/2	ISO/IEC 24759:2014の発行.
2014/3	ISO/IEC 19790:2012の欠陥報告の提出
2014/11	JIS X 24759 (2nd edition)の原案作成開始
2015/3	JIS X 19790:2015の発行
2015/10	ISO/IEC 19790:2012 及び ISO/IEC 24759:2014の**正誤表の発行**
2015/12	ISO/IEC 19790:2012 及び ISO/IEC 24759:2014の**訂正再発行**
2016/3	JIS X 24759 (2nd edition)の原案作成完了予定

ISO/IEC 19790:2012に関連するIPAの取り組み
JIS原案作成

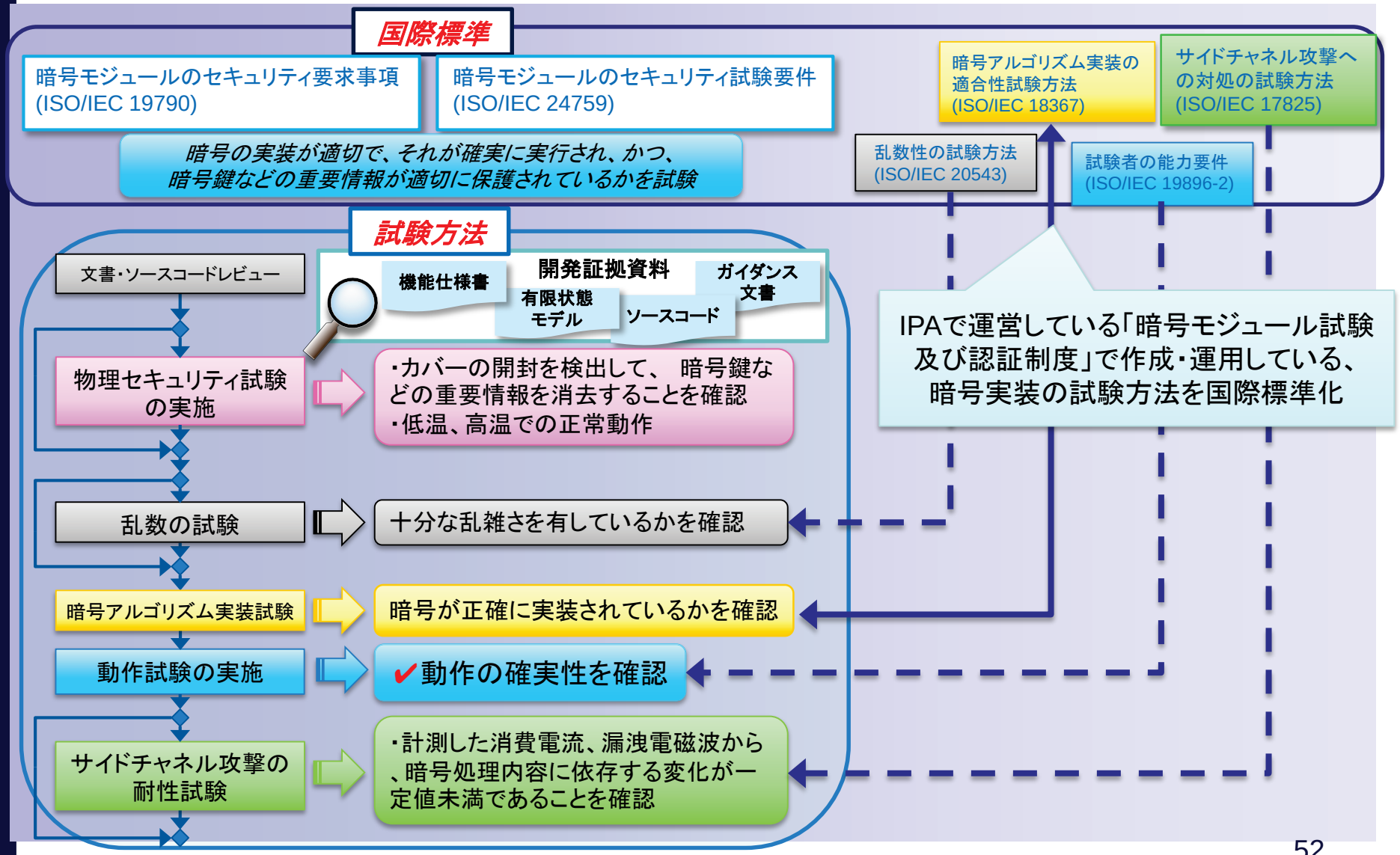
- JIS X 19790:2015
  - ISO/IEC 19790の国際一致規格
  - 2015/3/20 発行
- JIS X 24759:201X
  - ISO/IEC 24759の国際一致規格
  - 2016/3/29 原案作成完了予定



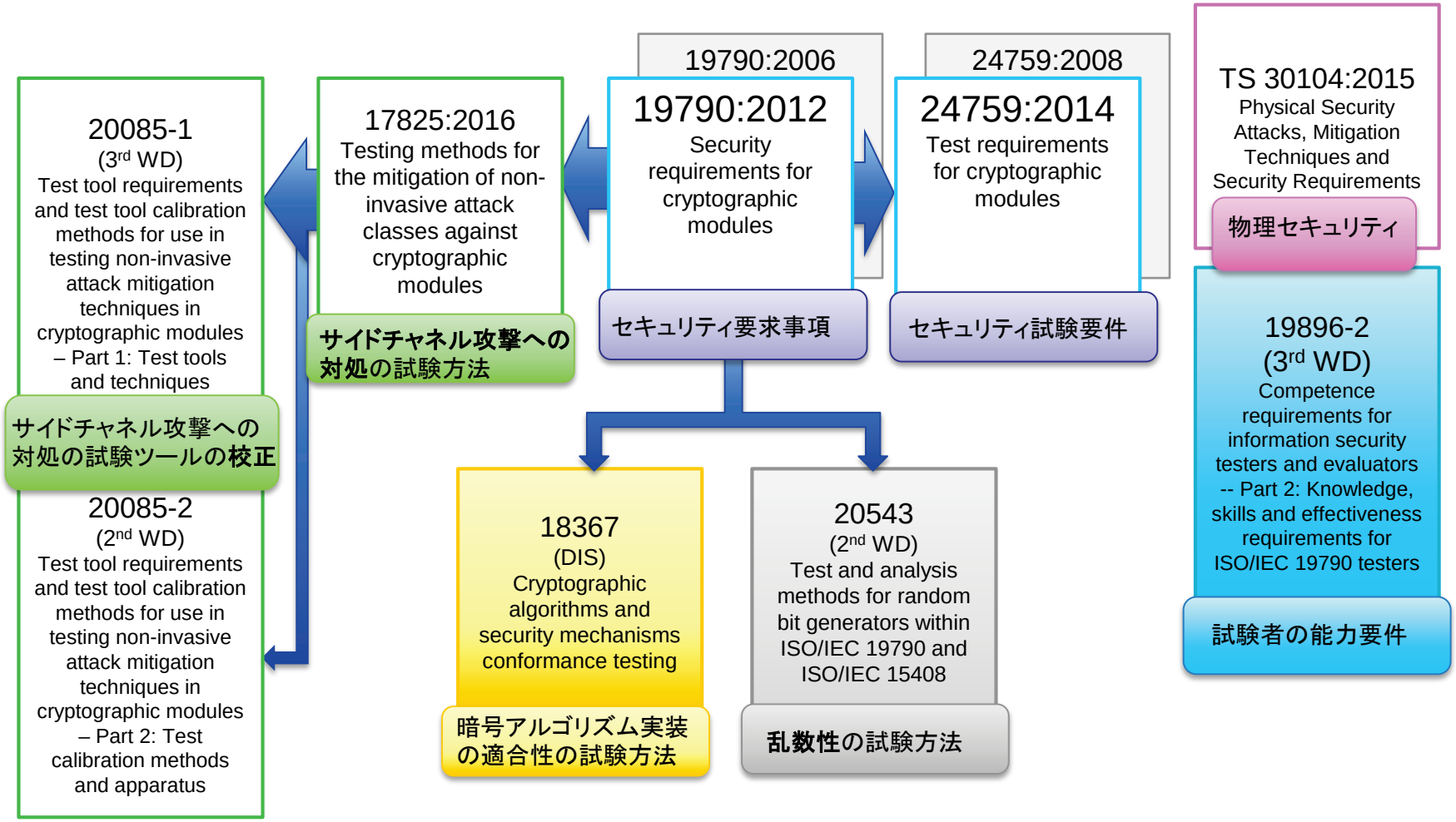
目次

- 暗号モジュール試験及び認証制度の概要
- 本制度における暗号アルゴリズムの移行
- ISO/IEC 19790:2012の紹介
- 関連する最新情報
  - 国際標準化
    - ISO/IEC 17825
  - 暗号アルゴリズム実装試験ツールの整備
    - SHA-3
  - 乱数源に関するセキュリティ要求事項 - SP800-90B
    - Health tests
  - CMVPの動向
  - collaborative Protection Profileの翻訳

関連する最新情報
国際標準化(1)
暗号モジュール試験の流れと国際標準

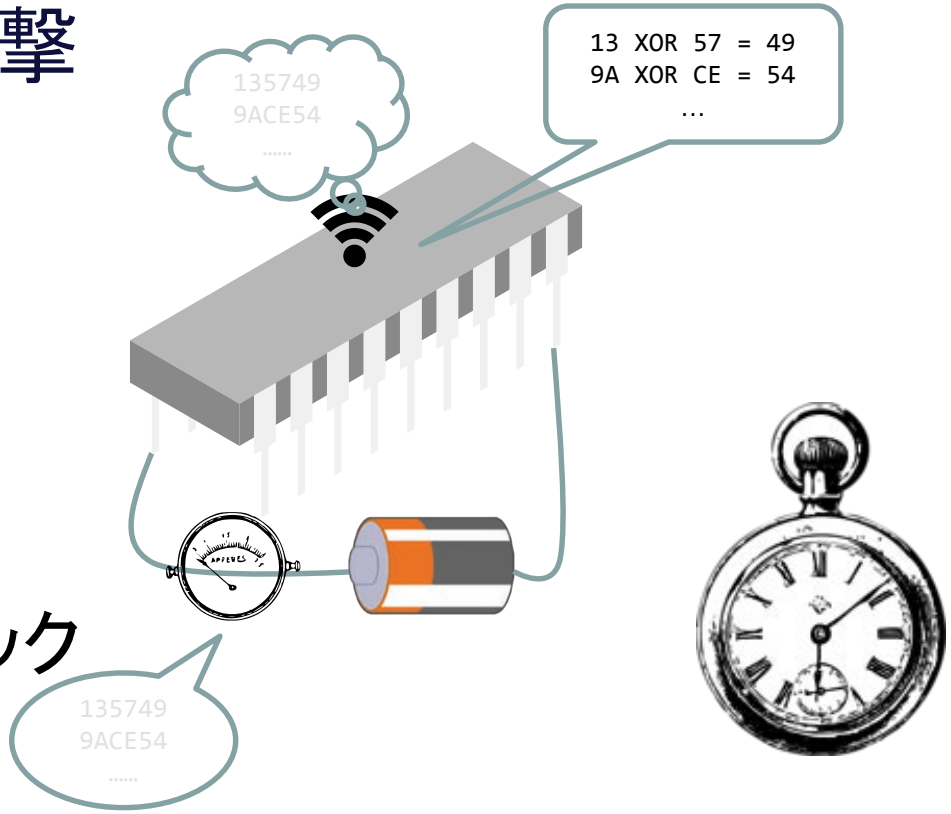


関連する最新情報
国際標準化(2)
関連する国際標準への展開



関連する最新情報
国際標準化(3)
サイドチャネル情報＝ 動作するICから漏れる情報

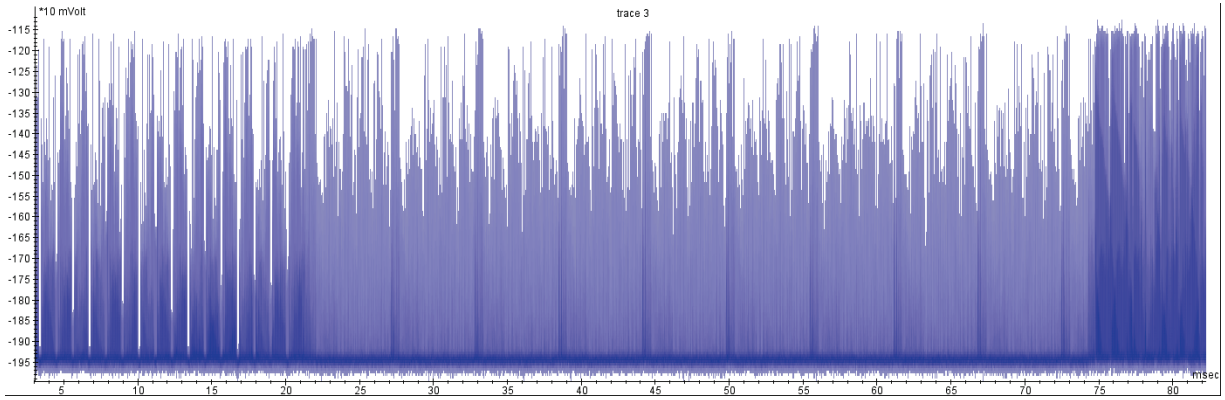
- ICの動作時には、消費電力や発散する電磁場などを通してある程度情報が漏れている
- サイドチャネル攻撃
  - 消費電力
    →電力解析
  - 電磁場
    →電磁解析
  - 処理時間
    →タイミングアタック



関連する最新情報
国際標準化(4)
サイドチャネル情報　共通鍵暗号の消費電流の例

AES-128の消費電流波形の例

消費電流

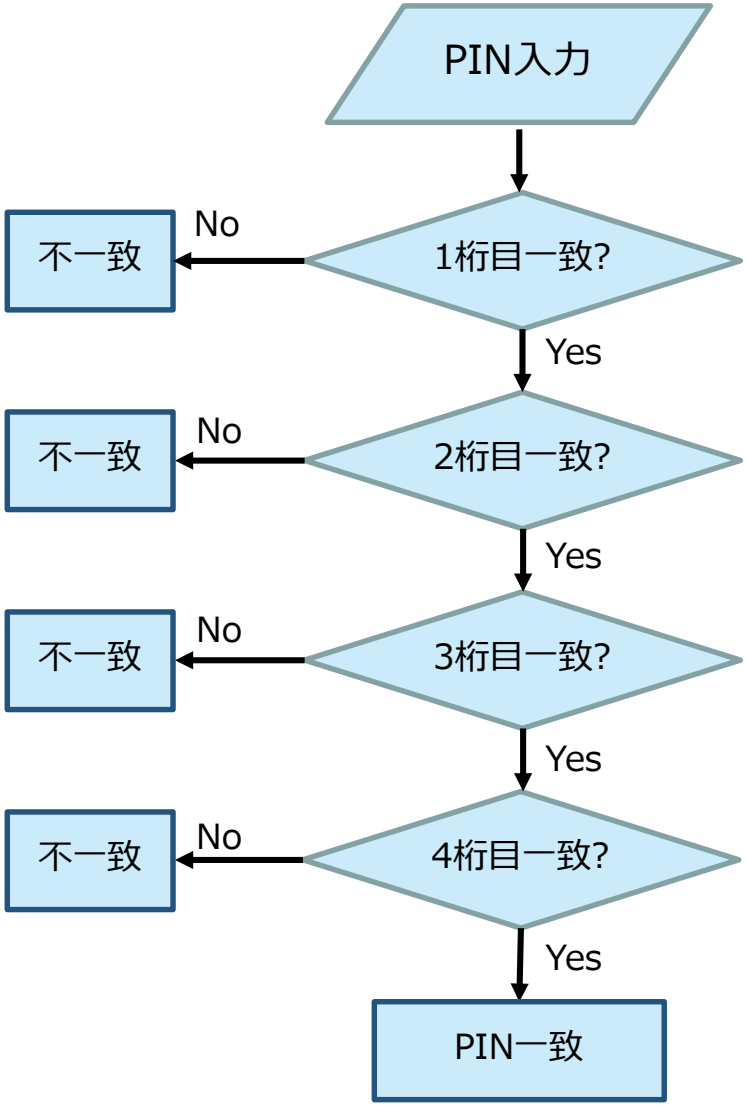


時刻

AESの繰り返し構造を反映した消費電流

関連する最新情報
国際標準化(5)
サイドチャネル情報 暗証番号の照合の例

- 4桁の暗証番号
  - 番号の組み合わせは10x10x10x10の10000通りだが、
  - 右の実装だと不一致判定の時間で各桁毎に推定可能。10+10+10+10の40通りになる。
  - 最後に判定する等、時間差が出ないように実装する必要がある。



関連する最新情報
国際標準化(6)
ISO/IEC 17825 (1)

- *“Test methods for the mitigation of non-invasive attack classes against cryptographic modules”*
  - 2016/1/4 発行
  - 対象
    - 非侵襲攻撃(non-invasive attack)へ対処する暗号モジュールであって、ISO/IEC 19790のセキュリティレベル3又は4を主張する暗号モジュール
  - 方針
    - できる限り「**押しボタン式**」でサイドチャネル情報の漏洩の程度を**判別したい**
    - 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
- 適用対象
  - 例
    - USBメモリ
    - Self Encryption Drive

関連する最新情報
国際標準化(7)
ISO/IEC 17825 (2) —暗号アルゴリズムと適用する試験方法—

セキュリティ機能		非侵襲攻撃の方法		
		SPA/SEMA	DPA/DEMA	TA
共通鍵	AES	A	A	A
	Triple-DES	A	A	A
公開鍵	Plain RSA	A	A	A
	RSA PKCS#1 v1.5	A	A	A
	RSA PKCS#1 v2.1	NA	NA	A
	DSA	A	A	A
	ECDSA	A	A	A
ハッシュ関数	SHA	A	NA	NA
メッセージ認証	HMAC	A	A	NA
鍵確立	DLC	A	NA	NA
	IFC	A	NA	NA

SPA :Simple Power Analysis

SEMA :Simple Electromagnetic Analysis

DPA :Differential Power Analysis

DEMA :Differential Electromagnetic Analysis

TA :Timing Analysis

A:Applicable, NA: Not Applicable

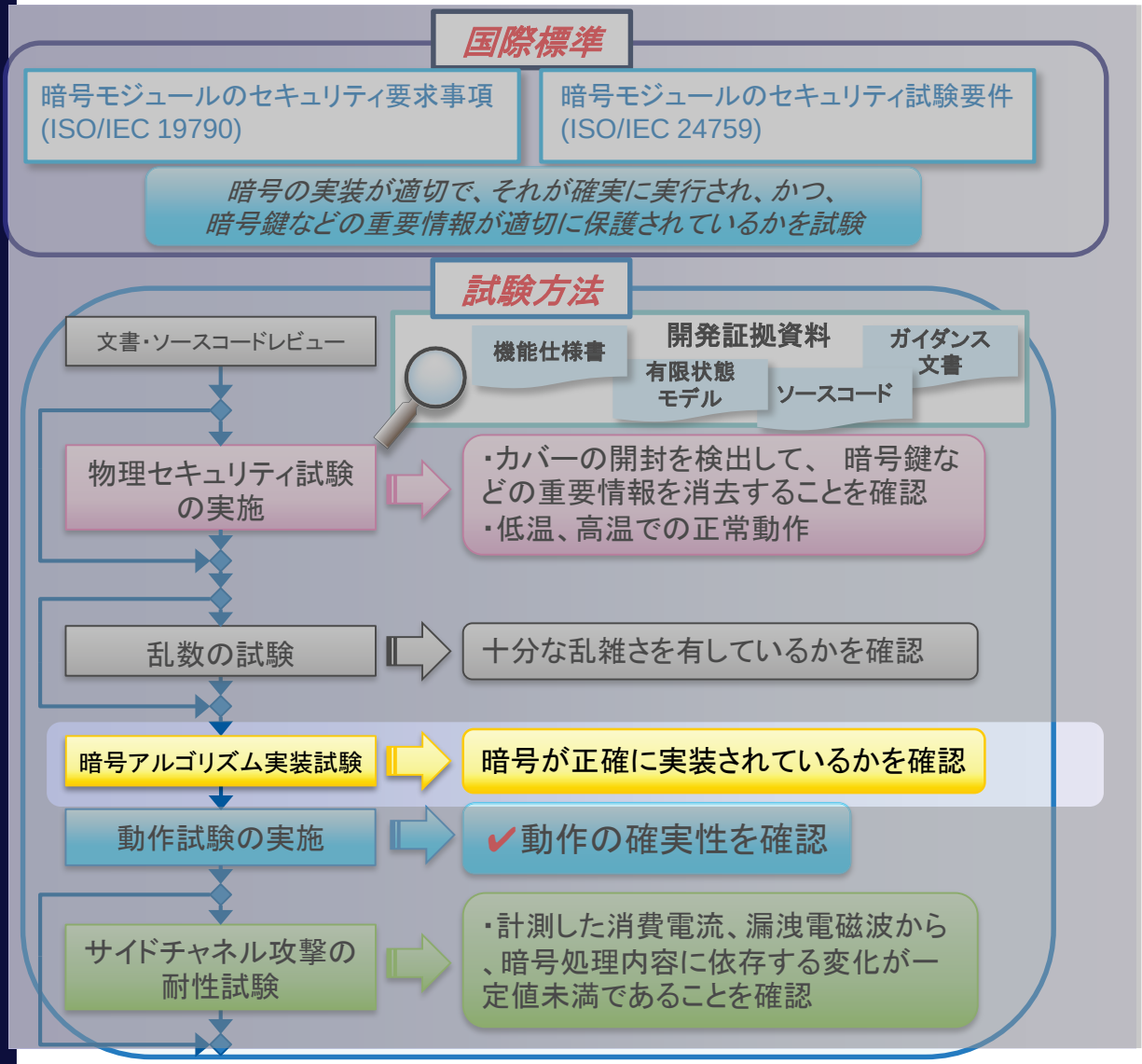
関連する最新情報
国際標準化(8)
ISO/IEC 15408とISO/IEC 17825のアプローチ

- ISO/IEC 15408のアプローチ
  - 脆弱性が悪用できないことを、
  - 専門知識を有する人が、
  - 時間をかけて(～3ヶ月)、評価する。
  - 結果的にコストが高い。
- ISO/IEC 17825のアプローチ
  - 脆弱性が明らかかどうかを判別することに注目して、
  - 専門知識の代わりに統計テストを用い、
  - 相対的に短い時間で(～2週間)、評価する。

目次

- 暗号モジュール試験及び認証制度の概要
- 本制度における暗号アルゴリズムの移行
- ISO/IEC 19790:2012の紹介
- 関連する最新情報
  - 国際標準化
    - ISO/IEC 17825
  - 暗号アルゴリズム実装試験ツールの整備
    - SHA-3
  - 乱数源に関するセキュリティ要求事項 - SP800-90B
    - Health tests
  - CMVPの動向
  - collaborative Protection Profileの翻訳

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



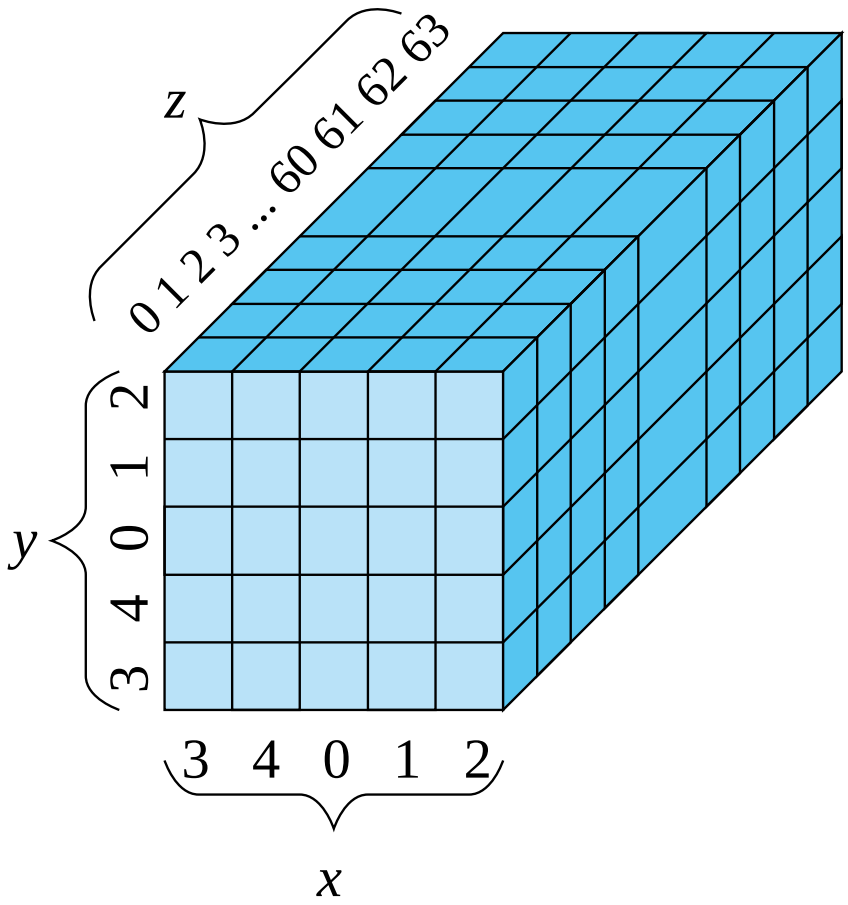
関連する最新情報
暗号アルゴリズム実装試験ツールの整備

- 公開鍵暗号
  - FIPS 186-4
    - RSA鍵ペア生成
      - CAVPのテストベクタの誤りを見つける
    - FFCドメインパラメータ生成・検証
- ストリーム暗号
  - KCipher-2
- ハッシュ関数
  - SHA-3
    - CAVPのベータテストに協力
- 鍵導出関数
  - NIST SP800-56C

新しいハッシュ関数 SHA-3 (1)

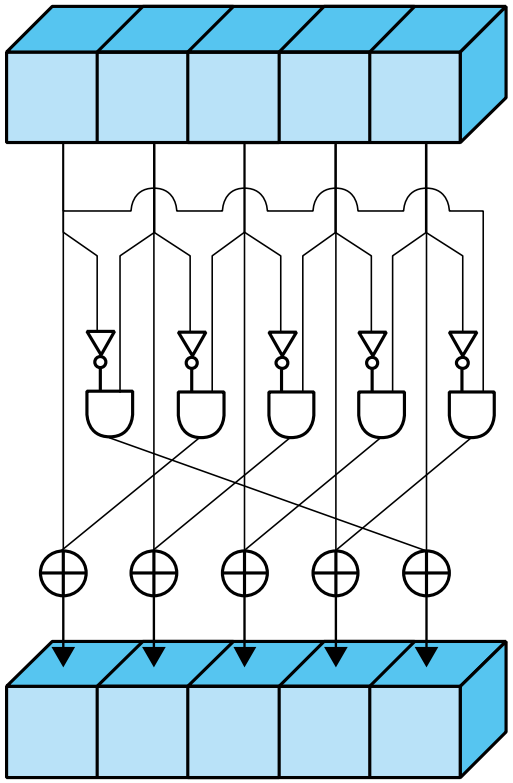
- ハッシュ関数
  - SHA3-224
  - SHA3-256
  - SHA3-384
  - SHA3-512
- 可変長出力関数 (extendable output function:XOF)
  - SHAKE-128
  - SHAKE-256
- 用途
  - ハッシュ関数
    - SHA-2と同様に使用できる。
  - 可変長出力関数
    - 別途NIST SP800シリーズの文書で、承認された使用方法について規定する。

暗号アルゴリズム実装試験ツールの整備
新しいハッシュ関数 SHA-3 (2)
State Array



- 1600ビットの配列
  “State Array”

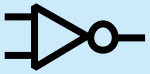
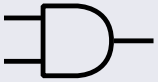
暗号アルゴリズム実装試験ツールの整備
新しいハッシュ関数 SHA-3 (3)
State Arrayの更新



- 非線形(FIPS 202, 3.2.4)

$$A'[x,y,z] = A[x,y,z] \oplus ((A[(x+1) \bmod 5, y, z] \otimes 1) \bullet A[(x+2) \bmod 5, y, z])$$

- メリット
  - サイドチャネルのリークを少なくするのに都合が良い設計。

記号	
	NOT
	AND

暗号アルゴリズム実装試験ツールの整備
新しいハッシュ関数 SHA-3 (4)
暗号アルゴリズム実装試験

- SHA3VS　**IPAが協力して開発**
  - Short Message Test
    - 次の長さのメッセージの処理の試験

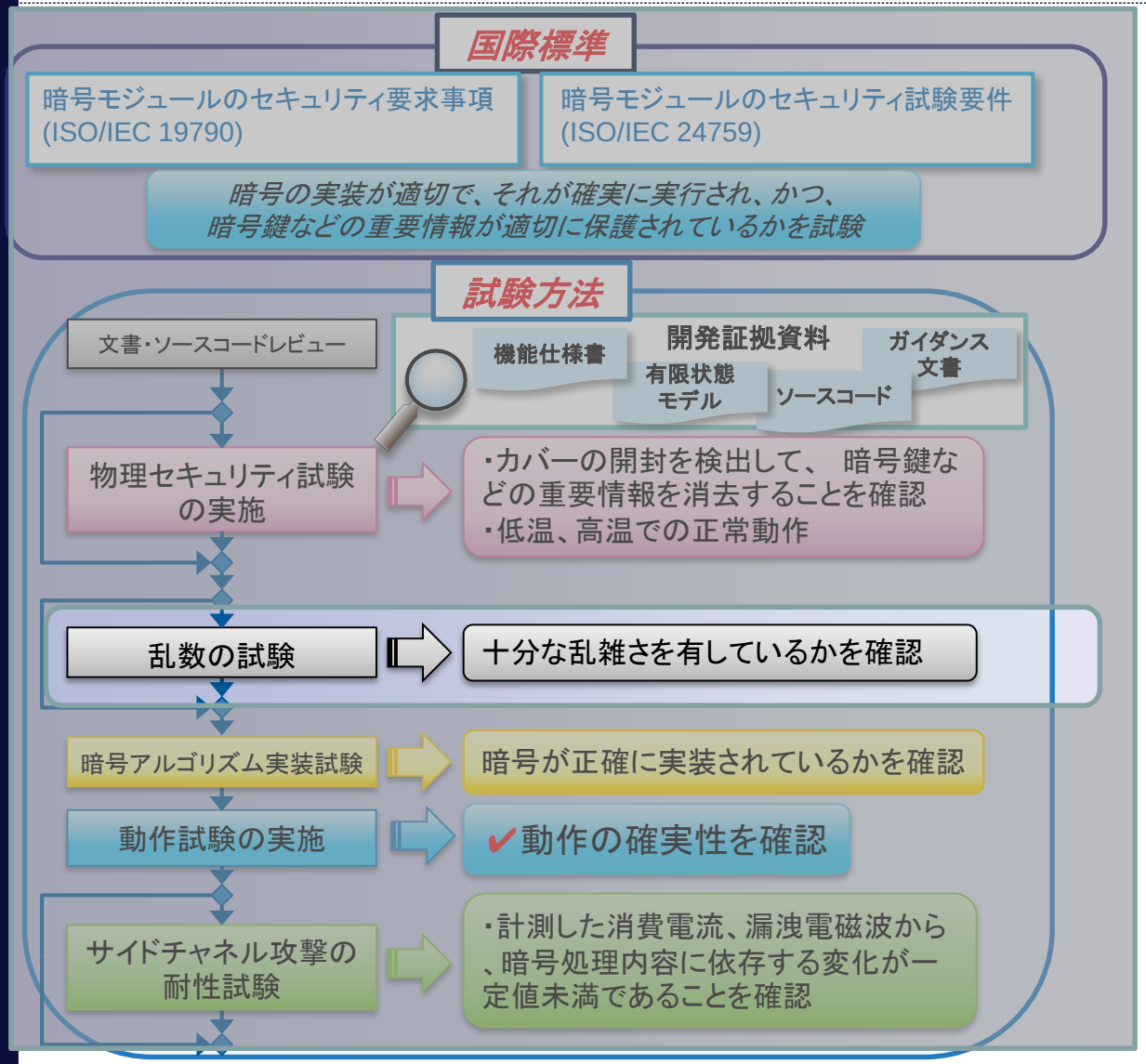
ハッシュ関数	メッセージ長(ビット)	
	bit-oriented	byte-oriented
SHA3-224	{0, 1, 2, …, 1152}	{0, 8, 16, …, 1152}
SHA3-256	{0, 1, 2, …, 1088}	{0, 8, 16, …, 1088}
SHA3-384	{0, 1, 2, …, 832}	{0, 8, 16, …, 832}
SHA3-512	{0, 1, 2, …, 576}	{0, 8, 16, …, 576}

  - Long Message Test
    - Short Message Testに使うメッセージより、長いメッセージの処理の試験
  - Monte Carlo Test
    - 制御された入力では検出できないようなやり方で実装を動作させて、欠陥を洗い出そうとする試験
  - Variable Output Test
    - SHAKE-128及びSHAKE-256専用の可変長出力の試験

目次

- 暗号モジュール試験及び認証制度の概要
- 本制度における暗号アルゴリズムの移行
- ISO/IEC 19790:2012の紹介
- 関連する最新情報
  - 国際標準化
    - ISO/IEC 17825
  - 暗号アルゴリズム実装試験ツールの整備
    - SHA-3
  - 乱数源に関するセキュリティ要求事項 - SP800-90B
    - Health tests
  - CMVPの動向
  - collaborative Protection Profileの翻訳

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



NIST SP800-90B(2nd Draft)

Recommendation for the Entropy Sources Used for Random Bit Generation

- Scope
  - エントロピー源の設計と試験
    - Entropy source validation
      - 開発証拠資料/テストに基づくエントロピー源の適切性の検査
    - Health tests
      - 自己テストに基づく実行時のエントロピー源の適切性

- Health tests (自己テスト)
  - 動機
    - 実行時にエントロピー源が故障するかもしれない。
    - エントロピー源が正しく動いているという確信が欲しい。
  - 方針
    - エントロピー源が故障していないことを、実行時に簡単な自己テストを行って確認する。
  - 自己テストが実施される頻度及び条件
    - 電源投入、継続的に、オンデマンド
    - 既知、疑われる故障モード
    - Continuous health tests
      - » Repetition count test
      - » Adaptive proportion test

4.4.1 Repetition count test (1)

- 背景
  - 連続乱数生成器テスト
    (Continuous random number generator test)
    - 乱数生成器から出力が定常値にならないことを確認するためのテスト
      - 実際には次の出力ブロックが異なることを確認する。
        - » 前に生成されたブロック
        - » 今生成されたブロック
    - 2つのブロックが一致して、テストが失敗となる場合、暗号モジュールはエラー状態になり、暗号モジュールからの出力を禁止しなければならない。
- 課題
  - 偶然に一致した場合は、必ずしも乱数生成器・エントロピー源の故障ではない場合が考えられる。

4.4.1 Repetition count test (2)

- 考え方
  - ある値を観測する頻度が一定以上になった場合、エラーにする。 (min-entropyに着目しているため、「ある値」に注目したテストである。)
    - n個連続して同じ値を観測する確率の最大値

$$P = 2^{-H(n-1)}$$

(H: min-entropy)

    - 式変形して

$$n = 1 + \frac{-\log_2 P}{H}$$

    - Pに誤検出率αを代入して、α対応する回数をカットオフ回数とする。

$$C = \left\lceil 1 + \frac{-\log_2 \alpha}{H} \right\rceil$$

α: 許容可能な誤検出率

C: カットオフ回数

テストの設計として、C回以上、有る値を観測したらエラーにする。

4.4.2 Adaptive proportion test

- 考え方
  - ある値を観測する頻度が一定以上になった場合、エラーにする。
  - 具体的には、あるWindow(W)の中に、C個以上の同じ値が観測される確率をαとおく。
    - 例：Binary(0又は1)を出力するノイズ源だと、Window(W)の中に出現する、0又は1の個数がC以上の場合、エラーとする。

Binaryを出力するノイズ源を想定しており、偏りが一定以上になった場合にエラーにするといったことができる。電源投入時や環境変動などによる偏りを検出することに用いることができる。

目次

- 暗号モジュール試験及び認証制度の概要
- 本制度における暗号アルゴリズムの移行
- ISO/IEC 19790:2012の紹介
- 関連する最新情報
  - 国際標準化
    - ISO/IEC 17825
  - 暗号アルゴリズム実装試験ツールの整備
    - SHA-3
  - 乱数源に関するセキュリティ要求事項 - SP800-90B
    - Health tests
  - CMVPの動向
  - collaborative Protection Profileの翻訳

関連する最新情報
CMVPの動向

- 乱数生成器(Random Number Generator)の移行
  - Active Validation Lists
  - Historical List
- Validation Sunsetting Policy
  - 5年間が認証の有効期限
- Approved Protection Profileの見直し
  - Mobile Device Fundamentalsも対象に
- Extended Cost Recovery
  - Complexity
    - 認証手数料の従量制
      - 1件で多数の暗号モジュールを対象とする場合

関連する最新情報

cPP: collaborative Protection Profileの翻訳

ネットワークデバイス	ネットワークデバイスのコラボラティブプロテクションプロファイル、2015/2/27、バージョン1.0 [翻訳暫定第0.2版]	
	https://www.ipa.go.jp/files/000050182.pdf	
	サポート文書（必須技術文書）、ネットワークデバイスcPPの評価アクティビティ、2015年2月 、バージョン1.0 [翻訳暫定第0.2版]	
	https://www.ipa.go.jp/files/000050183.pdf	
	ステートフルトラフィックフィルタファイアウォールのコラボラティブプロテクションプロファイル、2015/2/27、バージョン1.0 [翻訳暫定第0.2版]	
	https://www.ipa.go.jp/files/000050184.pdf	
	サポート文書（必須技術文書）、ステートフルトラフィックフィルタファイアウォールcPPの評価アクティビティ、2015年2月 、バージョン1.0 [翻訳暫定第0.2版]	
	https://www.ipa.go.jp/files/000050185.pdf	
ドライブ全体暗号化	ドライブ全体暗号化のコラボラティブ プロテクションプロファイル－許可取得、2015/1/26、バージョン1.0 [翻訳暫定第0.4版]	
	https://www.ipa.go.jp/files/000050186.pdf	
	サポート文書（必須技術文書）、ドライブ全体暗号化：許可取得、2015年1月 、バージョン1.0 [翻訳暫定第0.2版]	
	https://www.ipa.go.jp/files/000050187.pdf	
	ドライブ全体暗号化のコラボラティブ プロテクションプロファイル－暗号エンジン、2015/1/26、バージョン1.0 [翻訳暫定第0.3版]	
	https://www.ipa.go.jp/files/000050188.pdf	
	サポート文書（必須技術文書）、ドライブ全体暗号化: 暗号エンジン、2015年1月 、バージョン1.0 [翻訳暫定第0.2版]	
	https://www.ipa.go.jp/files/000050189.pdf	

JCMVPやCAVPで採用しているブラックボックス・テストが使えます。

ご清聴有難うございました。

JCMVPホームページ

http://www.ipa.go.jp/security/jcmvp/

お問い合わせ先

jcmvp-info@ipa.go.jp