IPA Better Life with IT

暗号モジュール試験及び認証制度の動向

2014年9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
- Hardware Security Module
  - 関連する事例・最近の研究
    - OpenSSL Heartbleed
    - RSA鍵ペア生成
    - 暗号鍵のゼロ化
- ISO/IEC 19790 (2nd edition)
  - 暗号モジュールのセキュリティ要求事項11分野
  - 要求事項の抜粋
    - 暗号モジュールのインタフェース
    - Sensitive Security Parameter管理
    - ライフサイクル保証
- 暗号の危殆化と移行
  - NIST SP 800-131A "*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*"
  - NIST SP 800-52 rev.1 "*Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*"

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

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

SSP :Sensitive Security Parameter
クリティカルセキュリティパラメタ（CSP）及び公開セキュリティパラメタ（PSP）の総称

暗号モジュール試験及び認証制度の概要

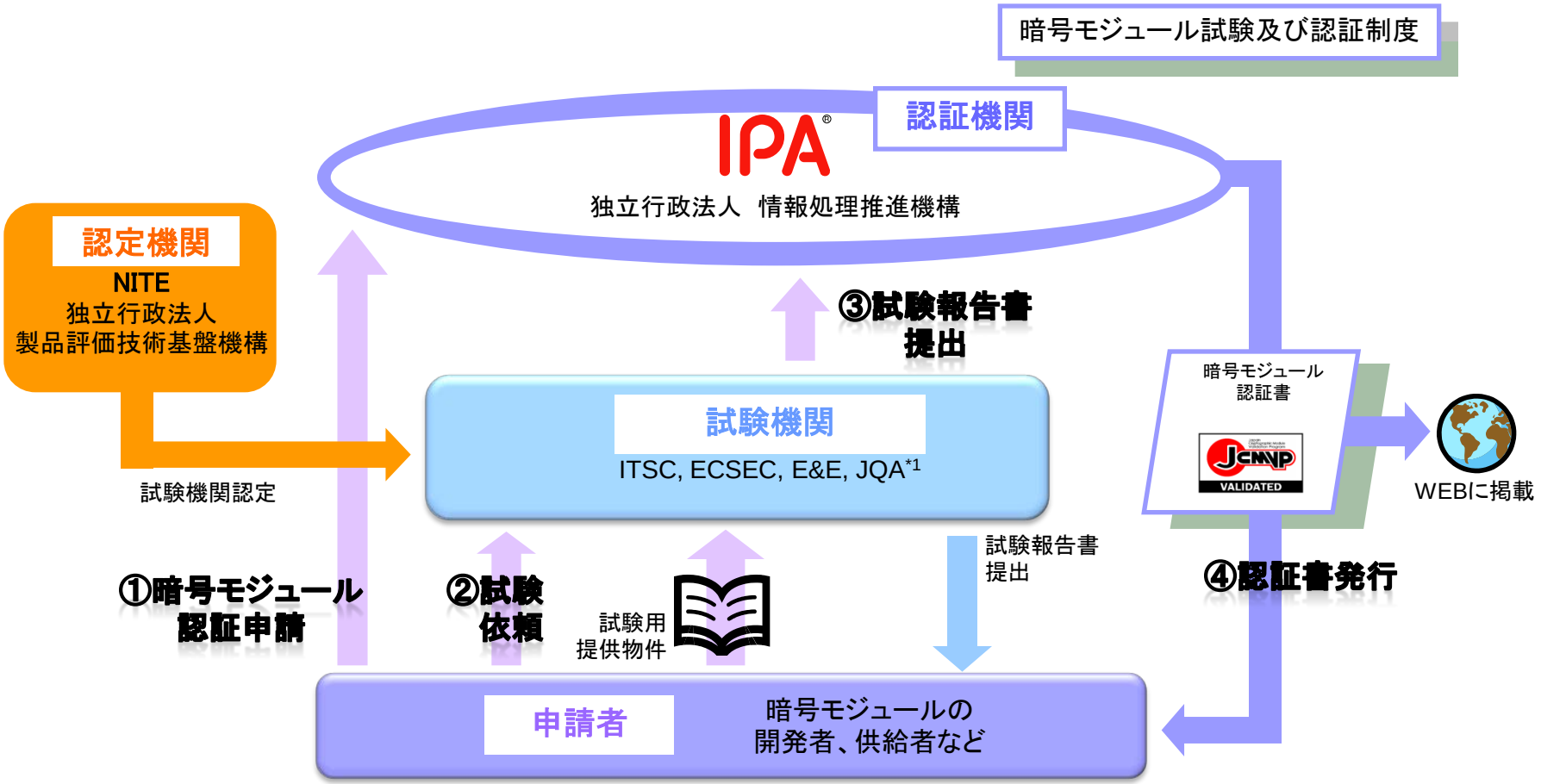
- 「暗号モジュール試験及び認証制度」
  (**JCMVP**：Japan Cryptographic Module Validation Program) とは、

  暗号モジュールに暗号アルゴリズムが適切に実装され、その鍵やパスワードといった重要情報が攻撃者から保護されるとともに、許可された者がいつでもその機能を確実に利用できることを、暗号モジュールのユーザが客観的に把握できるように設けられた**第三者適合性評価制度**。

- 暗号モジュールとは
  「**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。

- 米国・カナダのCMVP (Cryptographic Module Validation Program) 制度と同等の制度

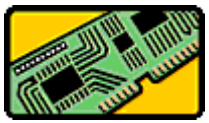
暗号モジュール試験及び認証制度の概要
JCMVP制度の全体像



*1 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
JQA: 一般財団法人 日本品質保証機構 関西試験センター

暗号モジュール試験及び認証制度の概要
JCMVP認証適用可能な製品例

- 暗号化記憶装置
- Hardware Security Module
- ルータ
- ソフトウェア暗号ライブラリ　等

目次

- 暗号モジュール試験及び認証制度の概要
- Hardware Security Module
  - 関連する事例・最近の研究
    - OpenSSL Heartbleed
    - RSA鍵ペア生成
    - 暗号鍵のゼロ化
- ISO/IEC 19790 (2nd edition)
  - 暗号モジュールのセキュリティ要求事項11分野
  - 要求事項の抜粋
    - 暗号モジュールのインタフェース
    - Sensitive Security Parameter管理
    - ライフサイクル保証
- 暗号の危殆化と移行
  - NIST SP 800-131A "*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*"
  - NIST SP 800-52 rev.1 "*Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*"

Hardware Security Module

- 用途
  - 暗号鍵の物理的・論理的保護
    - タンパー検出・応答、そしてゼロ化
    - 環境故障試験・環境故障保護
    - アクセス制御
  - 暗号鍵(公開鍵ペア)の生成
    - エントロピー
  - 署名生成・検証
- 運用側面
  - 長期間の使用　←→**暗号の危殆化**

Hardware Security Module 関連する事例 (1) OpenSSL

- OpenSSL Heartbleed
  - Heartbeat: TLSプロトコルの拡張機能
  - 暗号鍵を含む重要情報が、Heartbeatの応答として返される

- 教訓
  - 暗号モジュールの「インターフェース・サービス」の重要性
  - 重要機能・重要データ(暗号鍵)の、データ出力からの適切な分離

Hardware Security Module
関連する事例(2) RSA鍵ペア生成

- 同じ秘密鍵を共有するTLS/SSLの鍵
  - N. Heninger, et al. "*Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices*", Usenix Security 2012. https://factorable.net/weakkeys12.extended.pdf

- 教訓
  - 乱数生成器、エントロピーの重要性

Hardware Security Module
関連する事例(3) 暗号鍵のゼロ化

- タイミング
  - オペレータがいない時
  - 暗号モジュールを廃棄する時
  - 敵の手に渡りそうな時
- 要求
  - 暗号鍵を、短時間で確実に、最優先で消去したい
- 検討課題
  - 暗号鍵のコピーがたくさんあったら…
    (RAM上、キャッシュ上、レジスタ上)
  - 平文の暗号鍵がたくさんあったら…
  - デッドロックでゼロ化できなかったら…

目次

- 暗号モジュール試験及び認証制度の概要
- Hardware Security Module
  - 関連する事例・最近の研究
    - OpenSSL Heartbleed
    - RSA鍵ペア生成
    - 暗号鍵のゼロ化
- ISO/IEC 19790 (2nd edition)
  - 暗号モジュールのセキュリティ要求事項11分野
  - 要求事項の抜粋
    - 暗号モジュールのインタフェース
    - Sensitive Security Parameter管理
    - ライフサイクル保証
- 暗号の危殆化と移行
  - NIST SP 800-131A "*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*"
  - NIST SP 800-52 rev.1 "*Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*"

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

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

SSP :Sensitive Security Parameter
クリティカルセキュリティパラメタ（CSP）及び公開セキュリティパラメタ（PSP）の総称

ISO/IEC 19790 (2nd edition) 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
→入力パラメータ・フォーマットの検査
♦役割, サービス及び認証
→サービスの確認
♦ソフトウェア・ファームウェアセキュリティ
♦動作環境
♦物理的セキュリティ
♦非侵襲セキュリティ
♦Sensitive Security Parameter管理
→エントロピーの試験
→ゼロ化の試験
♦自己テスト
♦ライフサイクル保証
→自動化されたセキュリティ診断ツールを使ったソフトウェア・ファームウェア構成要素の検査
♦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

ISO/IEC 19790 (2nd edition)

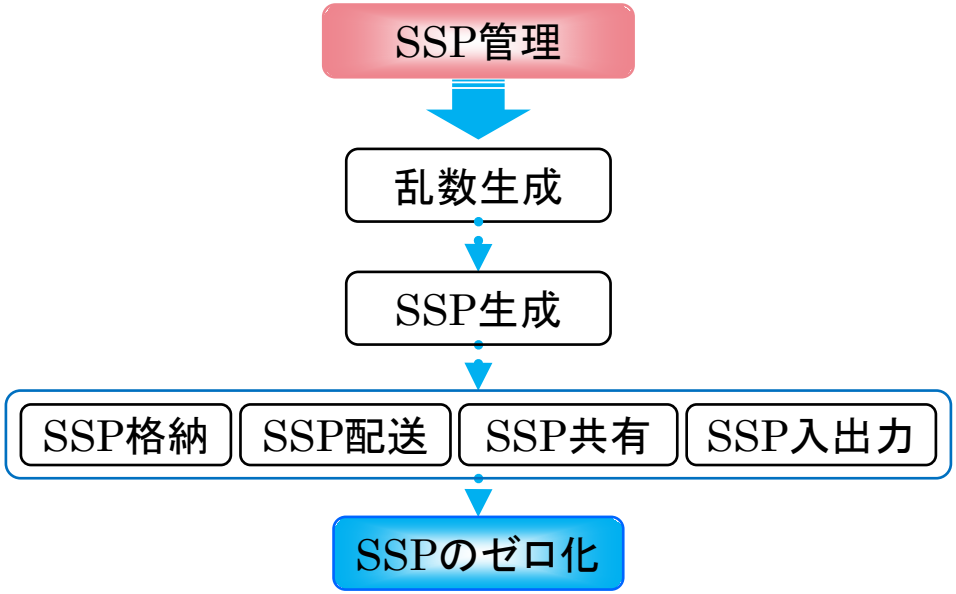
暗号モジュールのインタフェース

- セキュリティレベル1, 2, 3及び4
  - 暗号モジュールの仕様は，入力データ及び制御情報のフォーマットを，全ての可変長入力の長さ制限を含めて，明確に規定しなければならない。

ISO/IEC 19790 (2nd edition)

Sensitive Security Parameter管理 –その1 –

- SSP : CSPとPSPの総称
  - CSP : critical security parameter
    秘密鍵、パスワード等の重要情報
  - PSP : public security parameter
    公開暗号鍵など



- 乱数生成は、SSP管理の起点
- SSPのゼロ化は、SSP管理の終点

ISO/IEC 19790 (2nd edition)

SSP管理 –その2 –

- 乱数生成
  - 暗号鍵を生成することを見越して、SSPに必要なエントロピーを収集できるか
- SSP生成
  - 共通鍵
  - 公開鍵
  - 認証データ
    (例：チャレンジ)
- SSP共有
  - SSP共有方法の理論的強度と共有されるSSPの強度
    (see SP 800-57)
- SSP入出力
  - SSPとエンティティとの関連付け
- SSP格納
  - SSPとエンティティとの関連付け
  - 格納形式(平文、暗号化)

ISO/IEC 19790 (2nd edition)

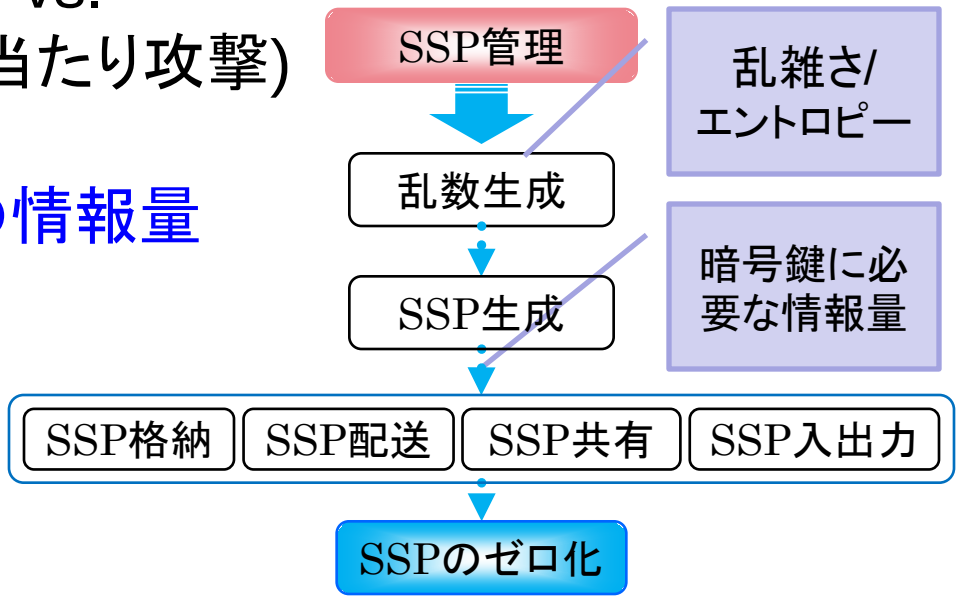
SSP管理 –その3 乱数生成 —

•乱数生成の”乱雑さ”が、SSP生成(暗号鍵生成)といった、暗号モジュールの重要機能に影響を与える。

- 攻撃者の視点
  - 乱数生成の乱数を推定 vs.
    暗号鍵の全数探索(総当たり攻撃)

    ↓

    乱数には暗号鍵以上の情報量(エントロピー)が必要



ISO/IEC 19790 (2nd edition)

SSP管理 –その4 SSP生成(1) —

- セキュリティレベル1, 2, 3及び4
  - 承認されたRBGの出力を利用するSSP生成方法のセキュリティの危たい（殆）化（例えば，決定論的RBGを初期化するためのシード値の推定）は，最低限，生成されたSSPの値を決定するのと同じだけの操作が必要でなければならない。

参考) NIST SP 800-90B (Draft)

Independent and Identically Distributed (IID)

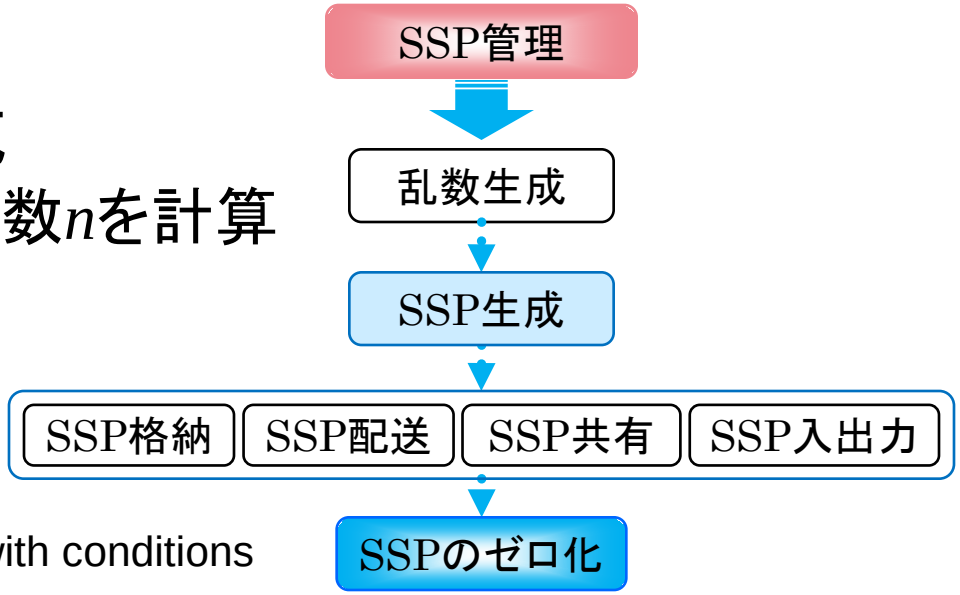
乱数の系列であって、その系列の各要素が他の要素と同じ確率分布に従い、全ての値が相互独立であるようなもの。

Non-IID

ISO/IEC 19790 (2nd edition)

SSP管理 –その4 SSP生成(2) —

- SSP生成
  - 例) RSA鍵ペア生成
    素数p, qを生成し、合成数nを計算
    - 鍵ペア生成方法
      - FIPS 186-4
        - » Provably Primes
        - » Probably Primes
        - » Provable Primes with conditions
        - » Probable Primes with conditions
    - 素数生成
      - FIPS 186-4
        - » Miller-Rabin Probabilistic Primality Test
        - » Enhanced Miller-Rabin Probabilistic Primality Test
        - » Shawe-Taylor random prime routine
        - » …



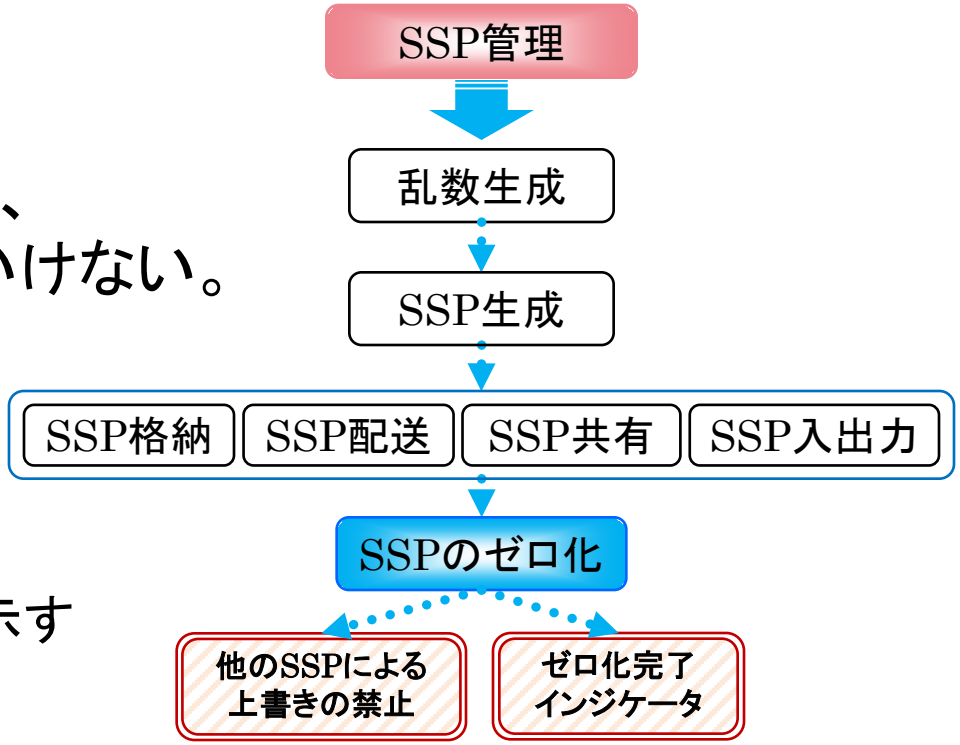
ISO/IEC 19790 (2nd edition)

SSP管理 –その5 SSPのゼロ化(1) –

- SSPのゼロ化

→重要情報であるSSPのデータ復元等を防止したい

- 保護されていないSSP及び鍵要素をゼロ化する方法を提供しなければならない。
- ゼロ化されたSSPは、取り出せてもいけないし、再利用可能であってもいけない。
- セキュリティレベル2, 3
  - SSPを他のSSPで上書きすることは、禁止。
  - ゼロ化が完了したことを示す状態出力が必要。



ISO/IEC 19790 (2nd edition)

SSP管理 –その5 SSPのゼロ化(2) –

- SSPのゼロ化
  - セキュリティレベル4
    - ゼロ化は，直ちに実行され，かつ，中断不可能でなければならず，さらに，ゼロ化は，その開始時刻から完了時刻までの間にセンシティブデータが復元されることを防ぐために，十分短い時間で行われなければならない。
    - 全てのSSPは，平文であっても，暗号的に保護されていても，ゼロ化されなければならない。その結果，暗号モジュールは工場出荷状態に戻る。

ISO/IEC 19790 (2nd edition)
ライフサイクル保証 –開発-

- セキュリティレベル1
  - 暗号モジュールがソフトウェア又はファームウェアを含む場合には，ソースコード，言語リファレンス，コンパイラ，コンパイラバージョン及びコンパイラオプション，リンカ及びリンカオプション，ランタイムライブラリ及びランタイムライブラリの設定，構成の設定，ビルドの手順及びビルド方法，ビルドオプション，環境変数，並びにソースコードを実行可能形式にコンパイル及びリンクするために用いられるその他の全てのリソースが，構成管理システムを用いて追跡されなければならない
- セキュリティレベル2及び3
  - ソフトウェアモジュール又はファームウェアモジュールは，暗号モジュールの機能及び実行に不必要なコード，パラメタ又は記号の使用を避けるように，設計かつ実装されなければならない。

ISO/IEC 19790 (2nd edition)
ライフサイクル保証 –ベンダ試験-

- セキュリティレベル1及び2
  - ソフトウェアモジュール若しくはファームウェアモジュール，又はハイブリッドモジュールのソフトウェア構成要素若しくはファームウェア構成要素に対して，ベンダは，（例えば，バッファオーバーフロー検知する）自動化されたセキュリティ診断ツールを用いなければならない。

目次

- 暗号モジュール試験及び認証制度の概要
- Hardware Security Module
  - 関連する事例・最近の研究
    - OpenSSL Heartbleed
    - RSA鍵ペア生成
    - 暗号鍵のゼロ化
- ISO/IEC 19790 (2nd edition)
  - 暗号モジュールのセキュリティ要求事項11分野
  - 要求事項の抜粋
    - 暗号モジュールのインタフェース
    - Sensitive Security Parameter管理
    - ライフサイクル保証
- 暗号の危殆化と移行
  - NIST SP 800-131A "*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*"
  - NIST SP 800-52 rev.1 "*Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*"

暗号の危殆化と移行
セキュリティ強度

Bits of security	対称鍵暗号アルゴリズム	FFC	IFC	ECC
80	2TDEA	L=1024 N=160	k=1024	f=160-223
112	3TDEA	L=2048 N=224	k=2048	f=224-255
128	AES-128	L=3072 N=256	k=3072	f=256-383
192	AES-192	L=7680 N=384	k=7680	f=384-511
256	AES-256	L=15360 N=512	k=15360	f=512+

SP800-57 Part 1 Table 2

- 2TDEA: 2-key Triple DES Algorithm
- 3TDEA: 3-key Triple DES Algorithm
- FFC: Finite Field Cryptography
- IFC: Integer Factorization Cryptography
- ECC: Elliptic Curve Cryptography

L: FFCドメインパラメータの一部である素数pのビット長　k: RSAの法nのビット長

N: FFCドメインパラメータの一部であるqのビット長　f: 楕円曲線の部分群の位数

暗号の危殆化と移行
米国の動き

- NIST SP800-131A “*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*”
  - NISTが制定した暗号アルゴリズムの移行計画
  - 112ビット以上のセキュリティ強度へ移行する
  - 112ビット未満の強度の暗号については、”legacy use”のみ認める
    - 既に暗号化されたデータの復号
    - 既に署名されたデータの検証
  - 乱数生成器については、legacyなものからSP800-90Aベースのものに移行

暗号の危殆化と移行
SP800-131Aの移行スケジュール

	セキュリティ強度	CY 2010	CY 2011	CY 2012	CY 2013	CY 2014	CY 2015	CY 2016
暗号化/署名生成/MAC生成	112ビット未満	→						
	112ビット以上	→						→
復号/署名検証/MAC検証	112ビット未満	→						→
	112ビット以上	→						→
乱数生成器	SP800-90A	→						→
	それ以外	→						

- Acceptable (許容): 承認されており、使用に際してのセキュリティリスクは知られていない
- Deprecated (非推奨): 承認されてはいるが、使用に際してユーザがリスクを受容しなければならない
- Legacy-use (レガシー): 暗号アルゴリズムを用いて既に保護された情報を処理するために使用しても良いが、その保護のための暗号アルゴリズム又は鍵長の使用は、現時点で、Deprecated、Restricted又は非承認となったもの。