NIST SP 800-57，SP 800-130ドラフト とそのコメントから鍵管理の全体像を見る

2010年11月22日

筑波大学 金岡 晃

筑波大学
University of Tsukuba

NISTの鍵管理（Key Management）に関する動向

文書

	Title	Year
SP 800-57	Recommendation for Key Management	2007 (Part1)
SP 800-108	Recommendation for Key Derivation Using Pseudorandom Functions	2009
SP 800-130 DRAFT	A Framework for Designing Cryptographic Key Management Systems	2010
SP 800-132 DRAFT	Recommendation for Password-Based Key Derivation - Part 1: Storage Applications	2010
SP 800-135 DRAFT	Recommendation for Existing Application-Specific Key Derivation Functions	2010

ワークショップ

Cryptographic Key Management Workshop
2009年と2010年の2回開催

NIST SP 800-57

- 暗号鍵（Cryptographic Key）の管理に関するガイダンス
- 3部構成
  - Part 1: General
    - 暗号鍵の一般的ガイダンスとベストプラクティス
  - Part 2: Best Practices for Key Management Organization
    - 米国政府組織向けのポリシ・セキュリティ企画の要件
  - Part 3: Application-Specific Key Management Guidance
    - 現行システムでの暗号利用

NIST SP 800-130

- まだドラフト
- A Framework for Designing Cryptographic Key Management System
- “Cryptographic Key Management System (CKMS)” とは？
  - 暗号鍵へのセキュリティを、コスト面で効果的に提供するための技術と標準
  - 暗号鍵の管理に関する機能を実現するオブジェクトのグループとしてシステムが構成される。
  - システムを作り上げるコンポーネントの記述を行うのがフレームワークであり、SP 800-130はそれを与えるもの
- プロファイル
  - フレームワークからシステムに必要なコンポーネントを選択する
- SP 800-57は「鍵管理」に焦点を置いているが、800-130は「鍵管理システム」
  - 鍵に付随するメタデータとその管理
  - システムのテスト、標準、国際法や国内法・ルールなどの検討
  - 災害復旧
  - セキュリティ監査

鍵管理（Key Management）の全体像

鍵の種類と情報

- 鍵の種類
- メタデータ

利用されるサービス

- 機密性、完全性、認証…

鍵の管理

※ここで言う「鍵」は「鍵発行用データ（Keying Material）」を含んでいます。

- 鍵の用途
- 鍵管理のフェーズ
- 鍵の危殆化
- 鍵の有効期間
- 鍵の状態と遷移
- 鍵のアーカイブ
- 暗号アルゴリズムと鍵サイズ
- 鍵とメタデータの関連付け
- 鍵のバックアップ
- 鍵の保証
- 鍵の確立
- 鍵の保護
- 相互運用性と移行

鍵管理の運用

- 運用フェーズ
- 災害復旧
- システムテスト
- 監査

鍵の種類

署名用プライベート鍵（Private Signature Key）	鍵配送用プライベート鍵（Private Key Transport Key）
署名検証用公開鍵（Public Signature Verification Key）	鍵配送用公開鍵（Public Key Transport Key）
認証用共通鍵（Symmetric Authentication Key）	鍵共有用共通鍵（Symmetric Key Agreement Key）
認証用プライベート鍵（Private Authentication Key）	鍵共有用プライベート静的鍵（Private Static Key Agreement Key）
認証用公開鍵（Public Authentication Key）	鍵共有用公開静的鍵（Public Static Key Agreement Key）
データ暗号化用共通鍵（Symmetric Data Encryption Key）	鍵共有用プライベート短期鍵（Private Ephemeral Key Agreement Key）
暗号鍵暗号化用共通鍵（Symmetric Key Wrapping Key）	鍵共有用公開短期鍵（Public Ephemeral Key Agreement Key）
乱数生成用共通/非対称鍵（Symmetric and Asymmetric Random Number Genration Keys）	認可用共通鍵（Symmetric Authorization Key）
マスター共通鍵（Symmetric Master Key）	認可用プライベート鍵（Private Authorization Key）
	認可用公開鍵（Public Authorization Key）

鍵のメタデータ

鍵ラベル	鍵長	鍵の保護
鍵識別子	鍵強度	メタデータ保護
鍵ライフサイクル状態	鍵の適切なアプリケーション	メタデータ紐付の保護
鍵フォーマット明細	鍵に適用可能なセキュリティポリシー	日時
鍵生成に利用される製品	所有鍵識別子	失効理由
鍵を利用する暗号アルゴリズム	鍵アクセス管理リスト（ACL）	
運用モード	バージョン番号	
鍵のパラメータ	親鍵	

SP 800-130にはメタデータと鍵の紐付（Binding）や、
メタデータの保護、メタデータと鍵の紐付自体の保護など
メタデータ関連の管理が記載されていますが、本資料では割愛します

鍵の有効期間（Cryptoperios）（１）

鍵の種類	鍵作者（Originator）利用期間（OUP）	鍵受領者（Recipient）利用期間
署名用プライベート鍵	1-3年	
署名検証用公開鍵	複数年（鍵サイズに依存）	
認証用共通鍵	2年以内	（OUP＋3年）以内
認証用プライベート鍵	1-2年	
認証用公開鍵	1-2年	
データ暗号化用共通鍵	2年以内	（OUP＋3年）以内
暗号鍵暗号化用共通鍵	2年以内	（OUP＋3年）以内
乱数生成用共通/非対称鍵	Seedが再生成されるまで	
マスター共通鍵	大体1年	
鍵配送用プライベート鍵	2年以内	
鍵配送用公開鍵	1-2年	

鍵の有効期間（Cryptoperios）（２）

鍵の種類	鍵作者（Originator）利用期間（OUP）	鍵受領者（Recipient）利用期間
鍵共有用共通鍵	1-2年	
鍵共有用プライベート静的鍵	1-2年	
鍵共有用公開静的鍵	1-2年	
鍵共有用プライベート短期鍵	1回の鍵共有トランザクション	
鍵共有用公開短期鍵	1回の鍵共有トランザクション	
認可用共通鍵	2年以内	
認可用プライベート鍵	2年以内	
認可用公開鍵	2年以内	

鍵とその他の鍵発行用データ（Keyiing Material）の危殆化

- 非認可の開示（漏えい）
- 鍵の完全性（改変、差し替え）
- 用途やアプリケーションの変更
- 鍵所有者の変更
- 関連情報の変更

暗号アルゴリズムと鍵サイズ

ビット (Bits of Security)	対称鍵	FFC （有限体）	IFC （素因数分解）	ECC （楕円曲線）
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

暗号アルゴリズムと鍵サイズ（ハッシュ関数）

ビット (Bits of Security)	電子署名、ハッシュ専用アプリ	HMAC	鍵導出関数	乱数生成器	その他
80	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	
112	SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	
128	SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	
192	SHA-384 SHA-512	SHA-224 SHA-256 SHA-384 SHA-512	SHA-224 SHA-256 SHA-384 SHA-512	SHA-224 SHA-256 SHA-384 SHA-512	
256	SHA-512	SHA-256 SHA-384 SHA-512	SHA-256 SHA-384 SHA-512	SHA-224 SHA-256 SHA-384 SHA-512	

暗号アルゴリズムと鍵サイズ

アルゴリズムセキュリティ存続期間	対称鍵アルゴリズム（暗号化、MAC）	FFC（有限体：DSA、DH）	IFC（素因数分解：RSA）	ECC（楕円曲線：ECDSA）
2010年まで	2TDEA，3TDEA AES128,192,256	Min: L=1024 N=160	Min: k=1024	Min: f=160
2030年まで	3TDEA, AES128,192,256	Min: L=2048 N=224	Min: k=2048	Min: f=224
2030年より先	AES- 128,192,256	Min: L=3072 N=256	Min: k=3072	Min: f=256

※「まで」はその年を含む

暗号情報の保護要件
(Protection Requirements for Cryptographic Information)

鍵タイプ	サービス	保護対象	関連保護対象	必要とされる保証	保護期間
署名用プライベート鍵	認証、完全性、否認防止	完全性、機密性	アプリ/用途、ドメインパラメータ、公開鍵署名検証鍵	所持	生成から有効期間の終わりまで
署名検証用公開鍵	認証、完全性、否認防止	アーカイブ、完全性	アプリ/用途、鍵ペア所持者、ドメインパラメータ、公開鍵署名検証鍵	正当性 (Validity)	生成から保護データの検証必要性がなくなるまで
認証用共通鍵	認証、完全性	アーカイブ、完全性、機密性	アプリ/用途、他認証エンティティ、認証データ		生成から保護データの検証必要性がなくなるまで
認証用プライベート鍵	認証、完全性	完全性、機密性	アプリ/用途、認証用公開鍵、ドメインパラメータ	所持	生成から有効期間のおわりまで
認証用公開鍵	認証、完全性	アーカイブ、完全性	アプリ/用途、鍵ペア所持者、認証データ、認証用プライベート鍵、ドメインパラメータ	正当性	生成から保護データの認証必要性がなくなるまで
データ暗号化用共通鍵	機密性	アーカイブ、完全性、機密性	アプリ/用途、他認可エンティティ、平文/暗号文データ		生成から、データの有効期間の終わりまたは暗号有効期間の終わりまでの遅いほう

暗号情報の保護要件（２）
(Protection Requirements for Cryptographic Information)

鍵タイプ	サービス	保護対象	関連保護対象	必要とされる保証	保護期間
暗号鍵暗号化用共通鍵	サポート	アーカイブ、完全性、機密性	アプリ/用途、他認可エンティティ、暗号化された鍵		生成から、暗号有効期間の終わりまたは暗号化された鍵の必要性がなくなるまで、の遅いほう
乱数生成用共通/非対称鍵	サポート	完全性、機密性	アプリ/用途	プライベート乱数生成系の保持（可能ならば）	生成から置き換えまで
マスター共通鍵	サポート	アーカイブ、完全性、機密性	アプリ/用途、他認可エンティティ、導出された鍵		生成から、暗号有効期間の終わりまたは導出された鍵の期限切れまで、の遅いほう
鍵配送用プライベート鍵	サポート	アーカイブ、完全性、機密性	アプリ/用途、暗号化された鍵、鍵配送用公開鍵	所持	生成から配送された全ての鍵の保護期間の終わりまで
鍵配送用公開鍵	サポート	完全性	アプリ/用途、鍵ペア所有者、鍵配送用プライベート鍵	正当性	生成から暗号有効期間の終わりまで

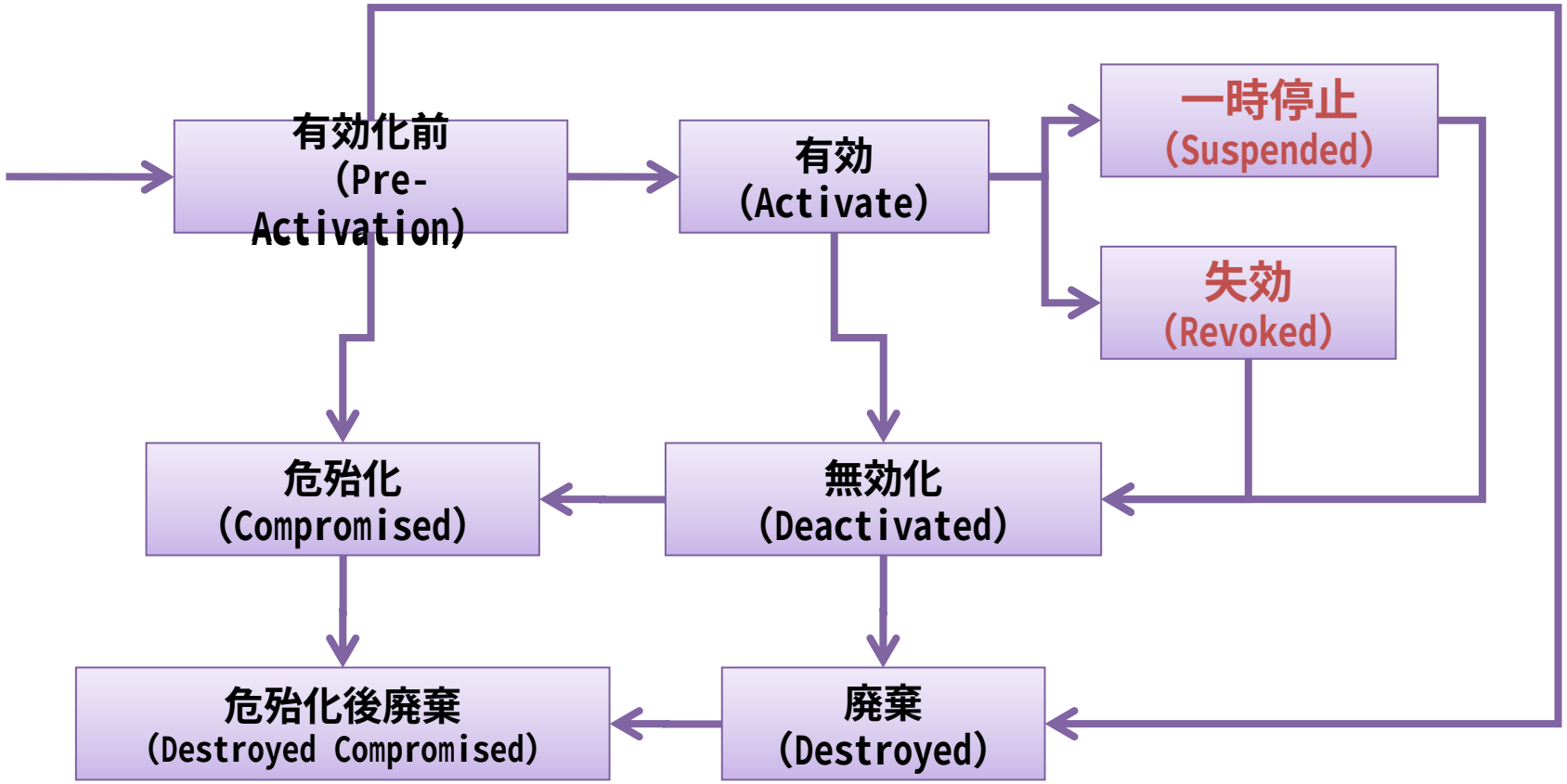
暗号情報の保護要件（３）
(Protection Requirements for Cryptographic Information)

鍵タイプ	サービス	保護対象	関連保護対象	必要とされる保証	保護期間
鍵共有用共通鍵	サポート	アーカイブ、完全性、機密性	アプリ/用途、他の認可エンティティ		生成から、暗号有効期間の終わりまた共有された鍵の必要性がなくなるまで、の遅いほう
鍵共有用プライベート静的鍵	サポート	アーカイブ、完全性、機密性	アプリ/用途、ドメインパラメータ、鍵共有用公開静的鍵	所持	生成から、暗号有効期間の終わりまた共有された鍵の必要性がなくなるまで、の遅いほう
鍵共有用公開静的鍵	サポート	アーカイブ、完全性	アプリ/用途、鍵ペア所有者、ドメインパラメータ、鍵共有用プライベート静的鍵	正当性	生成から、暗号有効期間の終わりまた共有された鍵の必要性がなくなるまで、の遅いほう
鍵共有用プライベート短期鍵	サポート	完全性、機密性	アプリ/用途、鍵共有用公開短期鍵、ドメインパラメータ		生成から、鍵共有プロセスの終了まで。プロセス後は鍵は廃棄されるべき。

暗号情報の保護要件（４）
(Protection Requirements for Cryptographic Information)

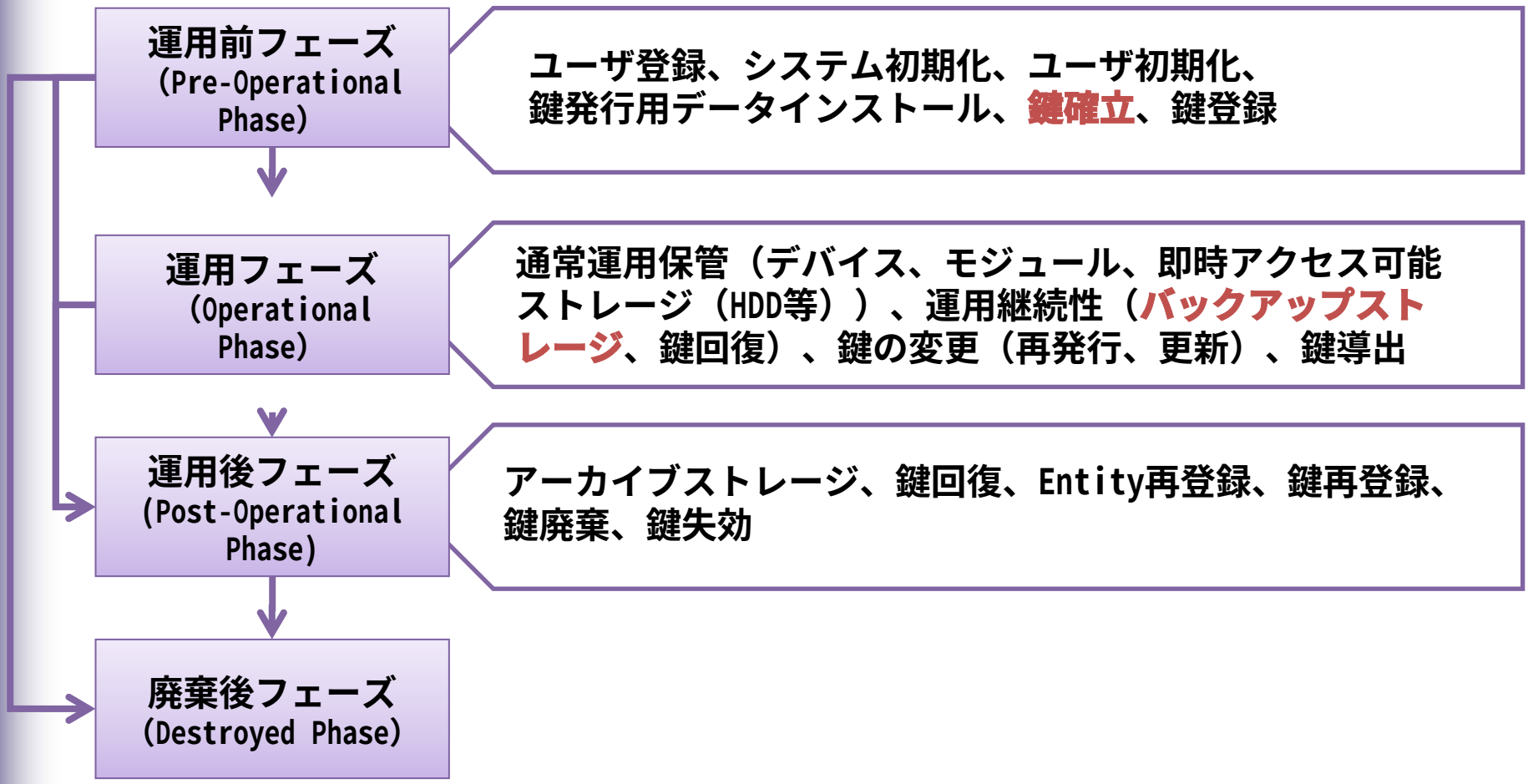
鍵タイプ	サービス	保護対象	関連保護対象	必要とされる保証	保護期間
鍵共有用公開短期鍵	サポート	完全性	アプリ/用途、鍵ペア所有者、鍵共有プライベート短期鍵、ドメインパラメータ	正当性	生成から鍵共有プロセスの終了まで
認可用共通鍵	認可	完全性、機密性	アプリ/用途、他認可エンティティ		生成から暗号有効期間の終わりまで
認可用プライベート鍵	認可	完全性、機密性	アプリ/用途、認可用公開鍵、ドメインパラメータ	所持	生成から暗号有効期間の終わりまで
認可用公開鍵	認可	完全性	アプリ/用途、鍵ペア所有者、認可用プライベート鍵、ドメインパラメータ	正当性	生成から暗号有効期間の終わりまで

鍵の状態と遷移
(Key States and Transitions)



※「一時停止」と「失効」はSP 800-57にはなく 800-130に登場

鍵管理フェーズとそれぞれの機能



鍵確立（Key Establishment）

- 非対称鍵の生成と配布
  - 公開静的鍵の配布
    - トラストアンカ公開鍵の配布
    - RAやCAへ送る（Submission）
    - 一般的な配布
  - 公開短期鍵の配布
  - センターで生成された（Centrally Generated）鍵ペアの配布
- 対称鍵の生成と配布
  - 鍵生成、鍵配布（マニュアル、電子的）、鍵共有（Key Agreement）
- 他の鍵生成用データ（Keying Material）の生成
  - ドメインパラメータ、初期化ベクトル、乱数生成器のシード、Intermediate Result（？）

鍵のバックアップ

署名用プライベート鍵（Private Signature Key）	（一般的に）不可。CAの署名用プライベート鍵の場合、必要であれば所有者の制御のもとで保管される
署名検証用公開鍵（Public Signature Verification Key）	可
認証用共通鍵（Symmetric Authentication Key）	可
認証用プライベート鍵（Private Authentication Key）	可
認証用公開鍵（Public Authentication Key）	可
データ暗号化用共通鍵（Symmetric Data Encryption Key）	可
暗号鍵暗号化用共通鍵（Symmetric Key Wrapping Key）	可
乱数生成用共通/非対称鍵（Symmetric and Asymmetric Random Number Genration Keys）	必要ないし、望ましくない（アプリケーション依存）
マスター共通鍵（Symmetric Master Key）	可

鍵のバックアップ（2）

鍵配送用プライベート鍵 (Private Key Transport Key)	可
鍵配送用公開鍵 (Public Key Transport Key)	可
鍵共有用共通鍵 (Symmetric Key Agreement Key)	可
鍵共有用プライベート静的鍵 (Private Static Key Agreement Key)	不可（鍵回復で再構成が必要とされるまで）。
鍵共有用公開静的鍵 (Public Static Key Agreement Key)	可
鍵共有用プライベート短期鍵 (Private Ephemeral Key Agreement Key)	不可
鍵共有用公開短期鍵 (Public Ephemeral Key Agreement Key)	可
認可用共通鍵 (Symmetric Authorization Key)	可
認可用プライベート鍵 (Private Authorization Key)	可
認可用公開鍵 (Public Authorization Key)	可

鍵管理（Key Management）の全体像（再掲）

鍵の種類と情報

- 鍵の種類
- メタデータ

利用されるサービス

- 機密性、完全性、認証…

鍵の管理

※ここで言う「鍵」は「鍵発行用データ（Keying Material）」を含んでいます。

- 鍵の用途
- 鍵管理のフェーズ
- 鍵の危殆化
- 鍵の有効期間
- 鍵の状態と遷移
- 鍵のアーカイブ
- 暗号アルゴリズムと鍵サイズ
- 鍵とメタデータの関連付け
- 鍵のバックアップ
- 鍵の保証
- 鍵の確立
- 鍵の保護
- 相互運用性と移行

鍵管理の運用

- 運用フェーズ
- 災害復旧
- システムテスト
- 監査

最後に宣伝

- IPA 情報セキュリティ技術動向調査タスクグループ
  - http://www.ipa.go.jp/security/outline/committee/isec_tech1.html
  - 半期に1回、委員がそれぞれ情報セキュリティ分野の調査報告をする
  - 私も委員
  - 下期は「鍵管理」に焦点を当てる予定
    - 来年4月にWeb公開
  - ちなみに上期は「楕円曲線暗号の整備動向」を報告しました。
- ご静聴ありがとうございました
  - Contact: kanaoka@cs.tsukuba.ac.jp