暗号鍵管理に必要な仕組み

IPA/セコム株式会社
伊藤　忠彦

伊藤　忠彦

- IPA セキュリティセンター　暗号グループ
- セコム株式会社　IS研究所　暗号・認証基盤グループ
- セキュアオープンアーキテクチャ・エッジ基盤技術研究組合（TRASIO）

専門　：　暗号鍵管理、暗号システムの設計・運用・ポリシ管理

- 今までの行った鍵管理に関わる業務
  - 鍵管理ガイドライン執筆
  - ルート認証局構築
  - 特定の暗号システムの、（長期の）ライフサイクル管理指針提案、運用設計、ファシリティ設計etc..
  - CA/BForum（認証局関係の国際団体）でポリシの国際標準化活動
  - IETF等で標準化活動（主にメカニズムの国際標準化、7月にRFC8813が公開されました）
  - 量子コンピュータ登場を見据えた、長期間の鍵管理の検討
  - IoT機器のセキュリティ（消費電力分析、L2暗号化、乱数）

目次

- 背景
  - ポリシとメカニズム（仕組み）について
  - 今回の活動の位置づけ

- どのような考え方でメカニズムを使うべきか
  - 今回のガイドラインの使い方
  - ポリシとしての要求を、既存のメカニズムで解決する例

ポリシ（指針）とは

- What need to do、どんなことをしないといけないのか。
- 神田さんの発表は、主にこれについて

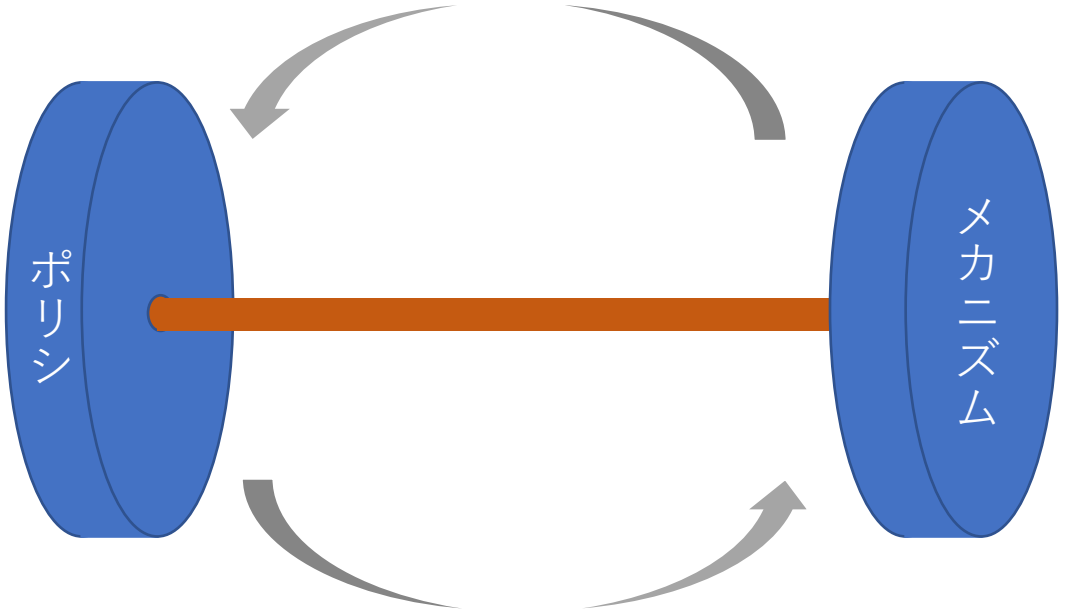
Howを示すのは、メカニズム（仕組み）。

- 次のスライドでは、ポリシとメカニズムの関係について
- 舟木さんの発表は、主にこれについて

今回の公開した指針は、「ポリシ」を作るためのもの

Policy とMechanismは車の両輪

ポリシを実施（Enforce）するためにはメカニズム（Mechanisms、複数形）が必要



メカニズムが正常に動作するにはポリシ（Policies、複数形）が必要

ポリシとメカニズムの例

- ポリシ：Aという作業をする場合は、必ず2人以上でやる事。
  - メカニズムA：作業が発生する場所に信用できる人物を常に配置し、1人で作業しようとした場合は排除する
  - メカニズムB：2つの鍵が必要な金庫に、作業に必要な機器を格納して、鍵は別々の人が保管
  - メカニズムC：ICカードによる秘密分散して、ICカードは別々の人が保管
  - メカニズムD：メカニズムAにおいて、ビデオで監視でできるようにし、さらにAIを利用して信用している人物が不正をしないかも監視
  - Etc…

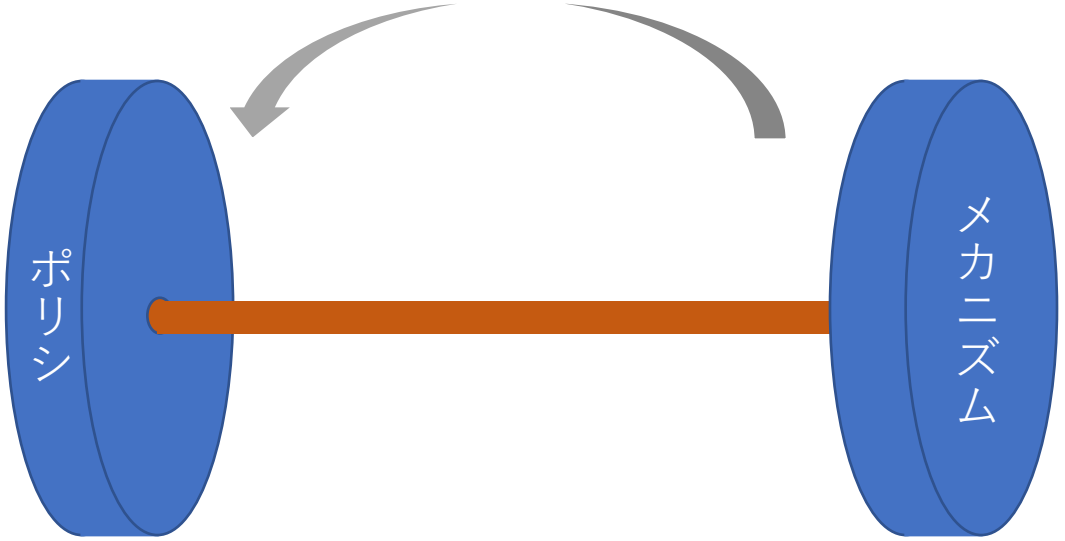
- 全てをヒューマンオペレーションで解決というアプローチは非効率
  - 【課題】監査可能性、死活監視、透明性、長期間の継続可能性、etc…

- 効率的なメカニズムを利用して、ポリシを実現する必要がある
  - 効率的なメカニズムは時代とともに変わる可能性があるため、ポリシで上手いこと吸収し、それにも対応できる事が望ましい。
  - 例：Aは非効率と思っていたら、AIの発達でAの延長たるDの方がBより効率的になるという事もあり得る。

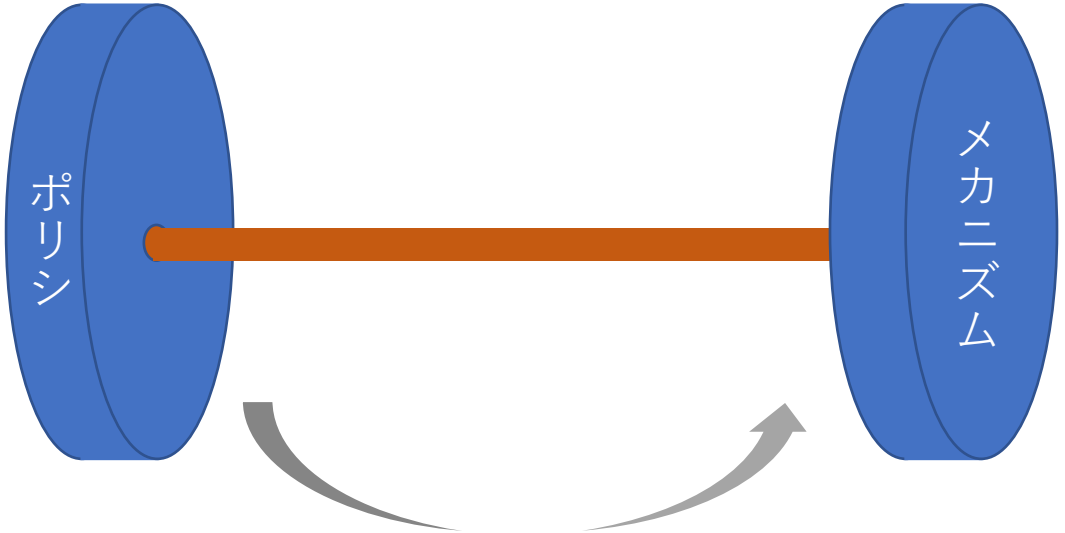
Policy とMechanismの関係

※仮に、必ず2人以上で作業するために、
メカニズムC（ICカードによる秘密分散）を利用したとして話を進めます

作業に対するポリシ（2人以上）を実施（Enforce）するためには、
何らかのメカニズム（ここではICカード）が必要



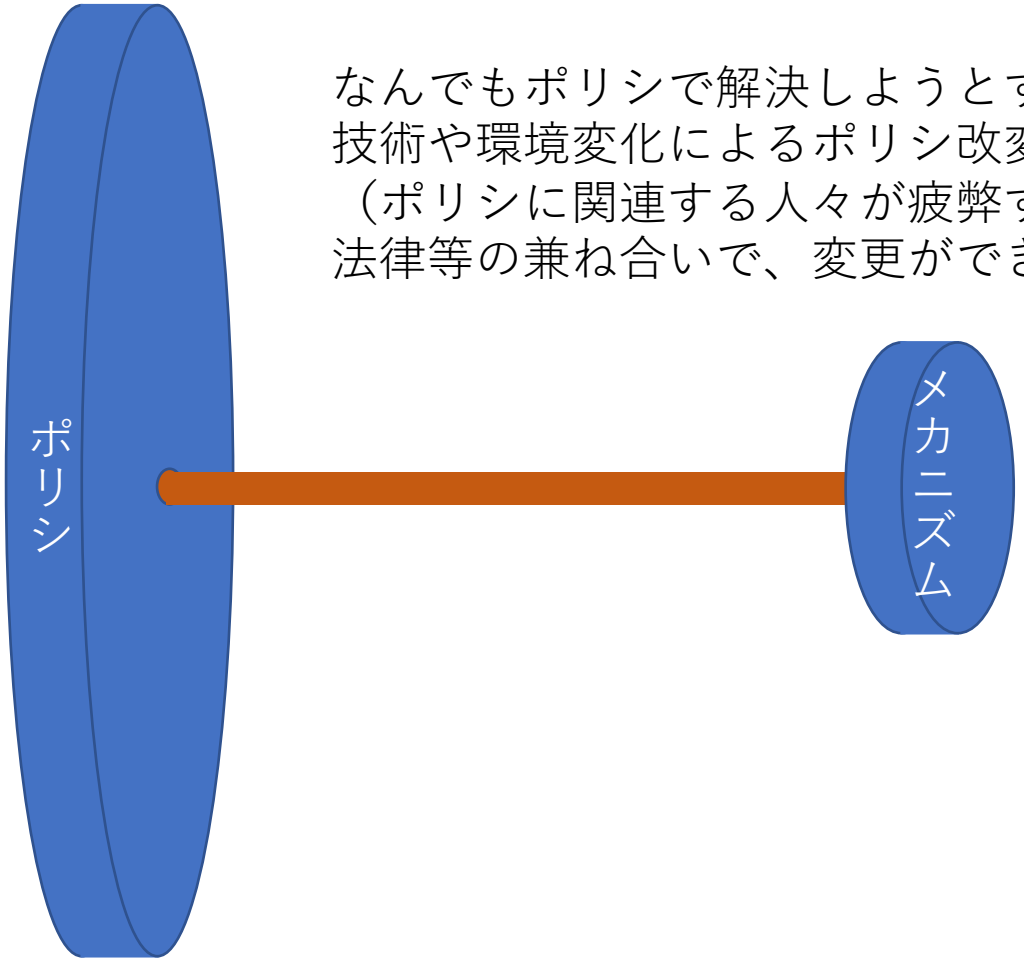
Policy とMechanismの関係



ICカードによる秘密分散メカニズムが正常に動作するには、
ICカード登録・運用・利用等のポリシが必要

※ループが続かないようにするためには、モジュール化する事が望ましい（後述）

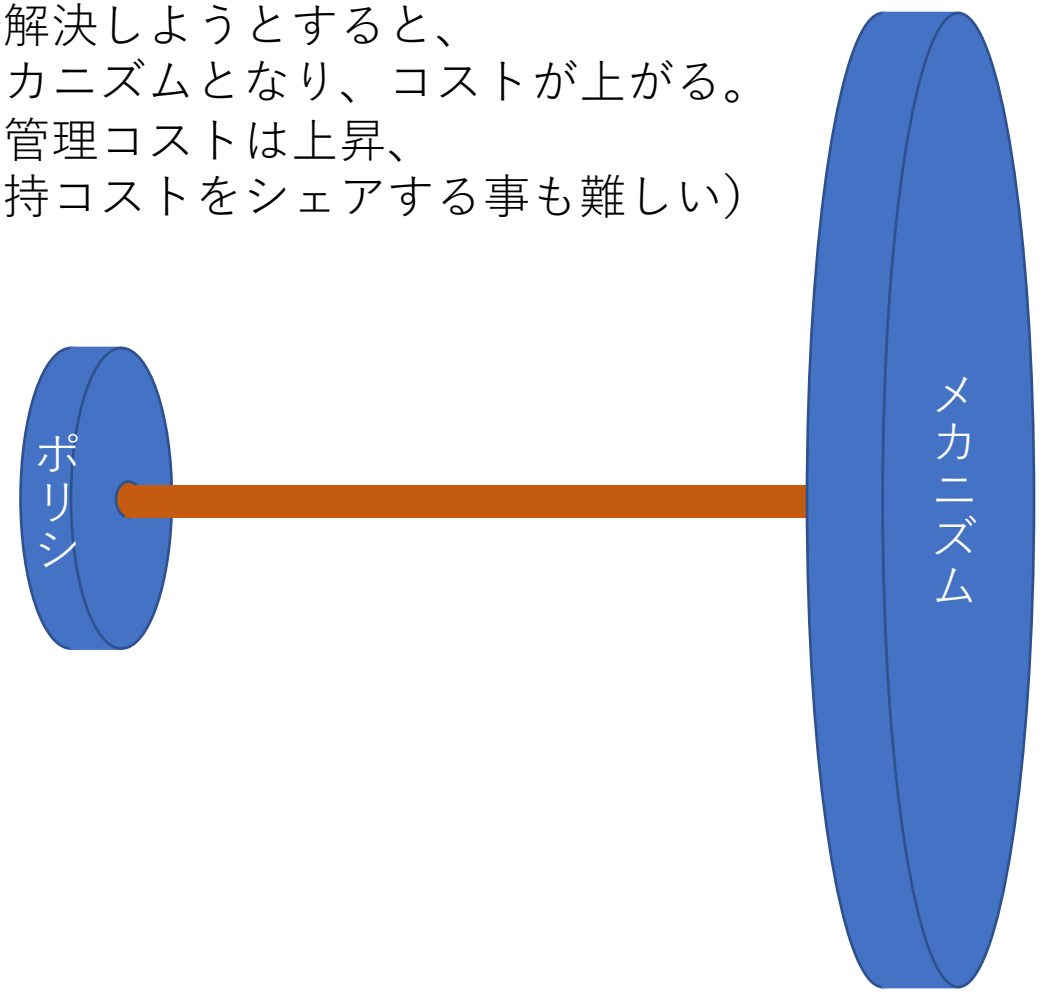
Policy とMechanismの関係



なんでもポリシで解決しようとすると、
技術や環境変化によるポリシ改変が頻繁に発生しうる。
（ポリシに関連する人々が疲弊する。
法律等の兼ね合いで、変更ができないこともある）

Policy とMechanismの関係

なんでもメカニズムで解決しようとすると、
特定用途に特化したメカニズムとなり、コストが上がる。
（メカニズムの維持・管理コストは上昇、
使う人が少ないので維持コストをシェアする事も難しい）



以上を踏まえて…

鍵管理を効率的・効果的に行うために望まれる事

鍵管理ポリシと鍵管理メカニズムを、ある程度分離

- 特定の業界に特化しない鍵管理メカニズムが発達し、調達コストが下がる
- 移行や環境の変化にも対応できる
- 業界によっては、既にできている？

適切な鍵管理メカニズムの提供

- 汎用的なメカニズムである事が望ましい
- JCMVPとか、CCとか、（既に日本でもやっている）

適切なポリシとは何かを示す

- 今回のドキュメントの位置づけ

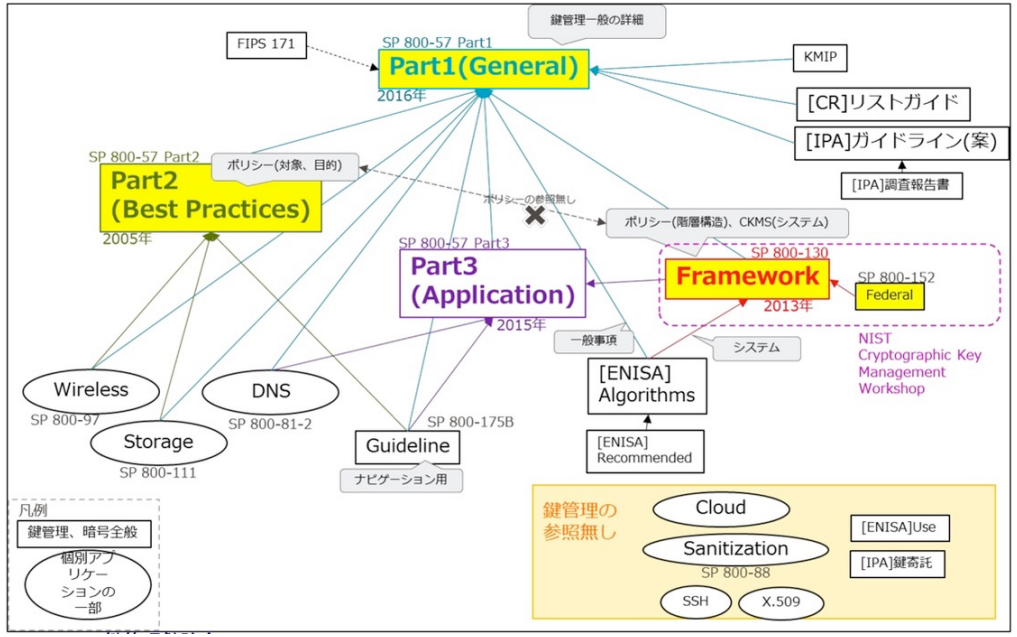
今回のガイドラインの使い方について

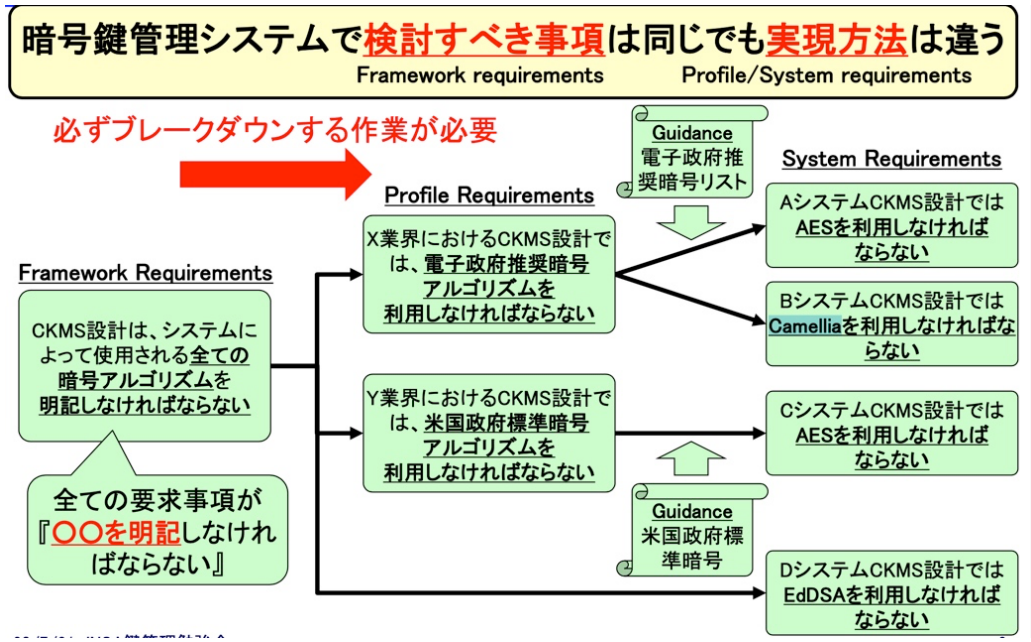
自社向けの鍵管理ポリシとメカニズムを決定するために必要な事（ポリシの検討 1/3）

- 保護対象のデータの価値の検討（冒頭の神田さんの守衛室とドアのぶのロックの話。 また１００万円のものと１００億円の物では必要な仕組みは違う）
- 暗号鍵が消えた時の影響の度合い検討（自社のみ？人の生命への影響は？社会的影響度は？）
- どのような不正に備える必要があるか検討（外部不正？内部不正？）
- どのような災害に備える必要があるか検討
- どの程度の期間その暗号鍵を使うのか検討（5年？10年？30年？100年？）
- 暗号鍵を管理する為にさけるリソースの検討
- 暗号鍵を管理する人員は、どのような属性を持つ人を想定するか検討
- 上位ポリシやメカニズムとして何があるか把握
- 既存の仕組みとの相互運用性が必要か把握
- サポート対象の国や地域を把握（日本のみ？インターネット？）
- etc.

自社向けの鍵管理ポリシとメカニズムを決定するために必要な事（ポリシとメカニズムの決定　2/3）

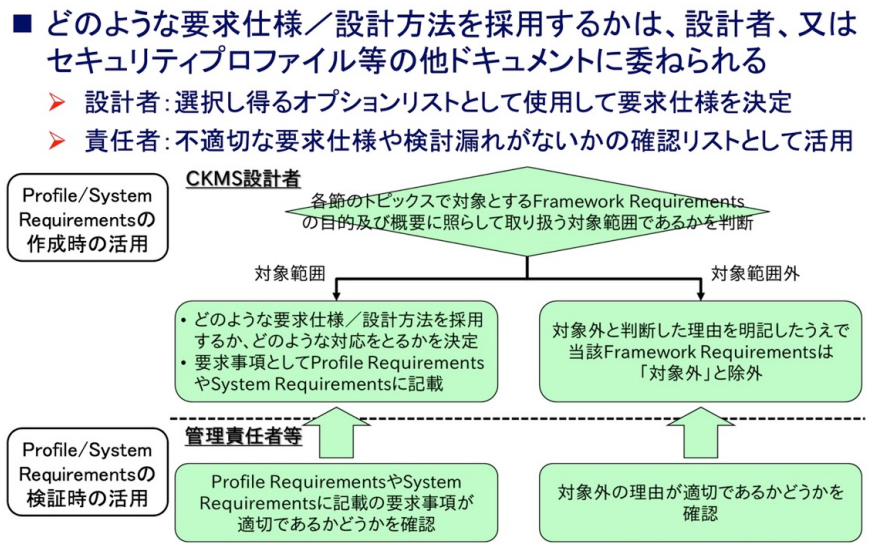
- **要求を満たすポリシを設計する**
- **既存のポリシやメカニズムを利用する場合は、参照/利用するものを決める**





自社向けの鍵管理ポリシとメカニズムを決定するために必要な事（適切であるか確認 3/3）

- 設計者により要求仕様が決定される
- 管理責任者により適切であるか確認される
- なお、採用メカニズムのために別のポリシを採用する必要があれば、採用



ポリシとしての要求を既存のメカニズムで解決する例

幾つかは、なんらかのメカニズムを利用する事で、効率的に達成できる。

メカニズムをうまく使う事が重要

鍵管理設計指針には２５６項目の要求事項があるわけですが。。。

（例）ポリシとしての要求を、メカニズムで解決

- 対象
  - D.1-10（メタデータについて）、
  - E8-11（メタデータと鍵の保護）、
  - etc..
- メタデータ保護（メタデータと暗号鍵の結びつきの保護）をオペレーションで解決するのは大変だが、
- 電子証明書を利用する事で、大きく効率化できる。

E.08	FR6.58	CKMS 設計は、どのように、どのような状況で鍵情報（暗号鍵及びメタデータ）が暗号モジュールに入力されるか、入力される形式、及び入力に用いられる手段を明記しなければならない。	6.4.19 節
E.09	FR6.59	CKMS 設計は、（必要ならば）どのように入力された鍵とメタデータの完全性及び機密性が入力時に保護され検証されるかを明記しなければならない。	6.4.19 節
E.10	FR6.60	CKMS 設計は、どのように、どのような状況で鍵情報（暗号鍵及びメタデータ）が暗号モジュールから出力されるか、及び出力される形式を明記しなければならない。	6.4.20 節
E.11	FR6.61	CKMS 設計は、どのように出力された鍵とメタデータの機密性及び完全性が暗号モジュールの外部で保護されるかを明記しなければならない。	6.4.20 節

検討番号	FR 番号	Framework Requirements の内容	SP800-130 参照章
D.01	FR6.1	CKMS 設計は、使用されているそれぞれの鍵タイプを明記及び定義しなければならない。	6.1 節
D.02	FR6.2	システムで使用されているそれぞれの鍵タイプに対して、CKMS 設計は、信頼関係のために選択される全てのメタデータ要素、メタデータ要素が作成され鍵との関連付けが満たされている状況、及び関連付けの手段（すなわち、暗号メカニズム又は信頼プロセス）を明記しなければならない。	6.2.1 節
D.03	FR6.13	それぞれの鍵タイプに対して、CKMS 設計は、暗号鍵及びメタデータ要素に関する以下の情報を明記しなければならない： a) 鍵タイプ b) 暗号鍵有効期間（cryptoperiod）（静的鍵（static key）に対して） c) 生成手段 i. 使用した乱数生成器（RNG） ii. 鍵生成の仕様（例えば、署名鍵については［FIPS 186］、Diffie-Hellman 鍵確立鍵（key establishment key）については［SP800-56A］） d) それぞれのメタデータ要素に対して、以下を含める i. メタデータのソース ii. メタデータの検証方法 e) 鍵確立（key establishment）の手段 i. 鍵配送スキーム（使用されている場合） ii. 鍵合意スキーム（使用されている場合） iii. プロトコル名（名称があるプロトコルが使用されている場合） f) 暴露に対する保護（例えば、鍵の機密性、物理セキュリティ） g) 改ざんに対する保護（例えば、MAC 又はデジタル署名） h) 鍵を使用し得るアプリケーション（例えば、TLS、EFS、S/MIME、IPSec、PKINIT、SSH、等）	6.2.2 節
		i) 鍵の使用が許可されないアプリケーション j) 鍵保証（key assurances） i. 対称鍵保証（Symmetric key assurances）（例えば、フォーマットチェック） • 誰が保証を得るか • 保証が得られる状況 • どのように保証を得るか ii. 非対称鍵保証（Asymmetric key assurances）（例えば、所有と有効性の保証） • 誰が保証を得るか • 保証が得られる状況 • どのように保証を得るか iii. ドメインパラメタ有効性チェック • 誰が有効性チェックを実行するか • チェックが実行される状況 • どのようにドメインパラメタの有効性の保証を得るか	
D.04	FR6.14	CKMS 設計は、CKMS によって生成、保管、伝送、処理、及びその他管理される全ての鍵タイプ及びメタデータについて、全てのシンタックス、セマンティクス、及びフォーマットを明記しなければならない。	6.2.2 節

公開鍵利用における RFC5280証明書

多くの典型的なメタデータを、
既にサポートしている。

この仕組みを適切に使えれば、メタデータ管理がすごく楽になる。

表 7-2　典型的なメタデータ要素一覧

●	a) 鍵ラベル（Key Label）
●	b) 鍵識別子（Key Identifier）
●	c) 所有者識別子（Owner Identifier）
●	d) 鍵ライフサイクル状態（Key Lifecycle State）
●	e) 鍵フォーマット指定子（Key Format Specifier）
	f) 鍵生成に使用した製品（Product used to create the Key）
●	g) 鍵を使用する暗号アルゴリズム（Cryptographic Algorithm using the Key）
●	h) スキーム又は暗号利用モード（Scheme or Modes of Operation）
●	i) 鍵パラメタ（Parameters for the Key）
●	j) 鍵長（Length of the Key）
○	k) 鍵／アルゴリズム組のセキュリティ強度（Security Strength of the Key/Algorithm Pair）
●	l) 鍵タイプ（Key Type）
○	m) 鍵に対する適切なアプリケーション（Appropriate Applications for the Key）
●	n) 鍵セキュリティポリシー識別子（Key Security Policy Identifier）
	o) 鍵アクセスコントロールリスト（Key Access Control List（ACL））
	p) 鍵使用カウント（Key Usage Count）
	q) 親鍵（Parent Key）
	r) 鍵機微性（Key Sensitivity）
	s) 鍵保護（Key Protections）
○	t) メタデータ保護（Metadata Protections）
●	u) 信頼関係保護（Trusted Association Protections）
●	v) 日時（Date Times）
●	w) 失効理由（Revocation Reason）

モジュール化したメカニズムを使えば、広い範囲を効率的にカバーできる。

- **Cryptographic Module（暗号モジュール）**というメカニズムがある
  - 【FIP Sの定義】A cryptographic module shall be a set of hardware, software, firmware, or some combination thereof that implements cryptographic functions or processes, including cryptographic algorithms and, optionally, key generation, and is contained within a defined cryptographic boundary.
  - 【意訳】うまいこと暗号処理をしてくれるメカニズム

- 加えて
  - そのメカニズム（暗号モジュール）に対する認証制度がある　（NISTのCMVP（Cryptographic Module Validation Program）など）
  - そのメカニズム（暗号モジュール）が正常に動作しているか確認する仕組みも検討されている（Attestation）

汎用的な暗号モジュールは、多くの鍵管理ポリシをカバーできるメカニズムたりえる？

検討番号	FR番号	Framework Requirements の内容	SP800-130参照章
B.01	FR2.4	CKMS 設計は、以下を含む CKMS システムの高レベルの概要を明記しなければならない： a) 利用するそれぞれの鍵タイプ b) 鍵が生成される場所と手段 c) それぞれの鍵タイプとの信頼関係で使用されるメタデータ要素（7.1 節表 7-2 参照） d) 鍵情報（暗号鍵やメタデータ）が存在しているそれぞれのエンティティのストレージにおける、鍵情報（暗号鍵やメタデータ）の保護方法 e) 配送時の鍵情報（暗号鍵やメタデータ）の保護方法 f) 鍵情報（暗号鍵やメタデータ）が配送され得る先となるエンティティの種類（例えば、ユーザ、ユーザデバイス、ネットワークデバイス）	2.5 節

- 汎用的な暗号モジュールとして、HSMとか、クラウドHSMというものがあります。
  - 詳細は舟木さんから
- HSMの利用で、沢山の検討番号が簡単にクリアできる
  - 例：B01とか

【急遽追加】時間管理は面倒。

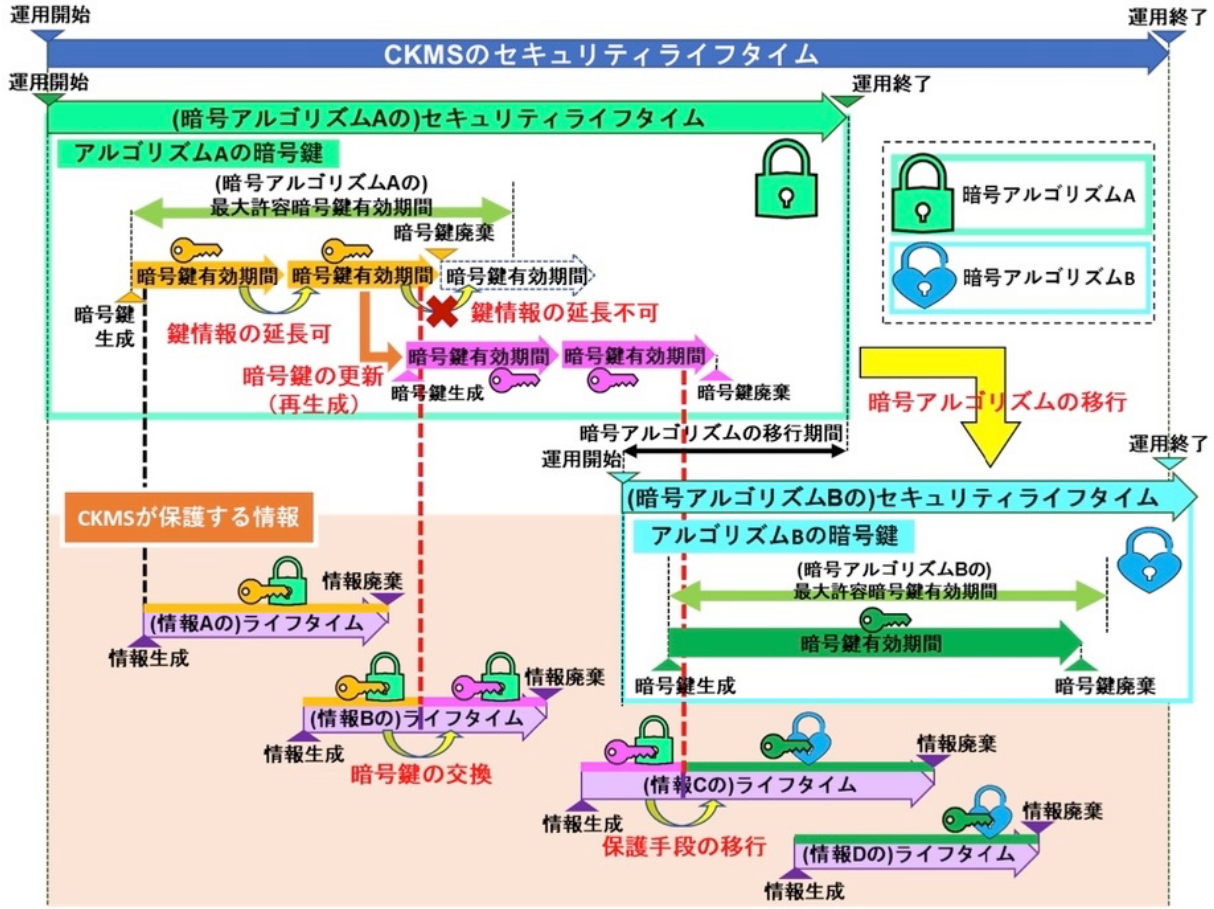


図 2-6　暗号鍵管理における時間管理の概念図

最後に

- 今回のドキュメントは、適切な暗号鍵管理メカニズムを設計するためのポリシ（指針）
  - どんな事をやらなければいけないか（ポリシ）であって、How（メカニズム）ではない
  - 適切なメカニズムは、業界や団体によって変わりうる

- 今後も増加し続ける大量のデータを、効率よく管理するために、暗号鍵管理メカニズムを効果的に使いこなす事が望まれる
  - 適切な暗号鍵管理メカニズムとポリシは、国・業界・サービス等により大きく異なる。
  - メカニズムの効果的な採用をするためには、鍵管理ポリシとメカニズムを、ある程度分離して考える事が望ましい。

- 技術の選択方法は現状設計者に委ねられているが、それを助ける仕組みが望まれる？
  - 自分がやった事が正しいかを判断する方法が望まれる？
  - 判断を助ける仕組みが望まれる？

補助資料

例えば：住居の鍵管理

課題

- 居住性のために、窓は欲しい。だが居ない時のためのセキュリティも欲しい。

解決策

- 錠と鍵なしで物件を守るのであれば、信用できる人を配置したりする必要がある。
- 窓やドアを鍵付きにして、全ての鍵を閉めて無人で守るというアプローチは効率的
- 窓は鍵無し錠で内側からロックし、入り口だけ鍵付きにすると、さらに効率的

- 昔から人々は、色々な種類の錠前や鍵を使い、鍵を管理し、色々なものを守ってきた。
- 今は、暗合鍵管理システム等を利用してデータも守っている。
- 暗号鍵管理においても、既存の鍵管理と同じように、既存の仕組みをうまく利用し、組み合わせる事が効率的
- だか、どのような組み合わせが効果的かの判断が難しかった。