2007 情財第 872 号

IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

安全な暗号鍵の
ライフサイクルマネージメントに関する調査

鍵管理ガイドライン（案）

2008 年 7 月

独立行政法人　情報処理推進機構

目次

1. はじめに

1.1. 本ガイドラインの目的

情報システムの構築・運用にあたっては、セキュリティ確保のために随所で暗号技術が活用されている。暗号の利用で必要となる暗号鍵の管理は、システムのセキュリティ要素である機密性・可用性・完全性を維持するために重要な役割を担っており、暗号鍵の管理が疎かであればシステムのセキュリティを大きく損なう可能性がある。そのため暗号鍵の生成から廃棄までのライフサイクルを考慮した管理手法を策定・確立することは、情報セキュリティシステムを維持するために必要不可欠である。

暗号鍵の管理については参照すべき日本語資料は少なく、実際に暗号を利用する情報セキュリティシステムの構築・運用において活用可能な、あるべき暗号鍵管理を示す文書の提示は強く望まれている。

本資料は、暗号鍵管理について特に鍵のライフサイクルに注目し一般的にその要点を示す。作成にあたっては米国国立標準技術研究所（NIST）の発行する SP800-57 part 1（鍵管理に関する推奨事項、改訂版）を参考とした。
本資料は完成版ではなく、今後の議論を受けた改訂を続け、内容の充実をはかることを意図している。

1.2. 想定読者

主な想定読者は、情報システムの調達／運用の担当者、およびこれらから依頼・指示されシステムの構築・運用を行う者とする。

1.3. 本ガイドラインの構成

本ガイドラインは以下の構成である。
2 章では、鍵管理に関する全般的な記述を行う。3 章では鍵情報のライフサイクルと、各段階の概要、鍵情報のリスクと対策について一般論を示す。
4 章ではより具体的な暗号利用場面における暗号鍵管理を示す。PKI を取り上げ、想定したシステムモデルにおける鍵管理について、管理上の脅威と対策の方向性を示す。

2. 暗号の利用と暗号鍵管理

2.1. 暗号鍵に係る脅威

安全とされる暗号を選び利用しているにも係らずセキュリティ上の問題が生じ暗号の効果が得られない場合、その原因の多くは、暗号鍵の運用上の不備、暗号実装上の問題に起因した暗号鍵の取り扱いの不備にある。

暗号鍵の管理上の不備に基づく脅威の例を以下に挙げる。

- 同一の暗号鍵を適切な利用期間を超えて使用し続ける。
  → ミスや故意により暗号鍵が漏えいする機会が増加し続ける。結果的に暗号鍵の入手が容易なものとなってしまう。
- 秘密鍵（共通鍵やプライベート鍵）を暗号化されていない状態で人間が読み出してコピーできる状態におく。あるいは、秘密鍵を誰でもアクセス可能な記録媒体に記録する。
  → 暗号鍵が漏えいする機会が増加する。鍵へのアクセスへの制限が極めて緩い状態で放置しているため、誰がいつ暗号鍵を入手したかが判らなくなる。
- 暗号鍵自体や、暗号化した情報（秘匿や署名の対象となる情報）と暗号鍵との関連付けに関する情報を失くしてしまう。
  → 暗号化の対象の情報について後で復号化して利用することや署名を検証することができない。
- 漏えい等の問題が疑われる暗号鍵を使い続け、新たな暗号化や署名を行ってしまう。
  → 被害範囲の更なる拡大を招く。漏洩した暗号鍵で施された暗号化を行うことにより保護されるはずの情報は漏洩可能性を持つ情報となる。

これらの脅威に対して、適切な対策を講じるためには、暗号鍵の体系的な管理を確立する必要がある。

暗号鍵の取扱いにおける、より具体的な脅威については、以後の章において述べる。

2.2. 暗号の用途と暗号鍵

2.2.1. 暗号の利用場面

さまざまな電子システムにおいてセキュリティ確保のために暗号技術が活用されているが、暗号鍵は、システム内部に組み込まれ自動的に処理され、管理者やエンドユーザの目に触れることなく用いられることも多いが、一方で、パスワード、IC カードやトークン、電子的なデータといった形態でより直接的に取り扱われ、人による管理を必要とする場合もある。

以下に、暗号の利用場面の例を、特にエンドユーザやシステム管理者が直接的に暗号鍵の管理運用に係る場合に注目して説明する。

(1)PKI

PKI 利用システムにおいては、公開鍵証明書以外にも通信路の機密性確保のため等の用途で複数の箇所で多様な暗号鍵が用いられている。運用についてもっとも考慮すべき暗号鍵としては、認証局および加入者（エンドユーザ）の鍵ペアが挙げられる。これらの鍵ペアのうち、特にプライベート鍵は高い機密性を要求されるため生成、保管、廃棄等の取り扱いに注意が必要となる。

本文書では、署名用途で用いられる PKI システムについて利用モデルを作成し、鍵管理上の考慮すべき事項について整理を行った。検討の結果を4章に後述する。

(2)蓄積データの暗号化

ファイル、ディスクなど暗号化を行う単位はさまざまある。暗号化製品でも組織的な暗号鍵管理に対応できる製品は比較的少なく、電子的な鍵情報や鍵に対応するパスワードの管理がエンドユーザに任せられている場合も多い。

組織に属するエンドユーザが個人的に電子的な暗号化鍵情報やパスワードを管理した場合には様々な問題が置きうる。以下にその例を挙げる。

- 暗号鍵情報が紛失する。エンドユーザ本人が忘却してしまう可能性、エンドユーザの異動等により失われる可能性がある。
- 暗号鍵へのアクセスが限定される保証がないため、暗号化された情報へのアクセスが制限されていることが保証できない。暗号鍵がコピーされ

ていない等を確実にする必要がある。

- 問題がある鍵情報やパスワードで暗号化が行われる可能性がある。同一の鍵情報で多数の暗号化が行われている場合や、弱いパスワードが使われる場合など。
- 暗号化された情報と暗号鍵の対応関係についての情報が失われやすい。鍵情報を頻繁に更新・再設定した場合に、どの鍵がどの暗号化情報と対応するかが不明確となる

このような問題がもととなり、暗号化した情報が後に復号できない事態が生じうる。

データの暗号化においては、主に共通鍵暗号方式の暗号が用いられる。一般に、共通鍵暗号方式の暗号鍵管理については、実装や管理手法の実態が公開されている事例は少ない。

(3)通信路の機密性確保

通信路の機密性確保を実現するために多用される手法としては SSL/TLS による暗号通信を挙げることができる。

(4)電子文書の長期保存

電子文書の典型例としては e 文書法の対象となる文書（契約書、設計図、仕様書）があげられる。

電子文書への署名に用いられる鍵の管理については、電子文書のライフサイクルとの対応を考慮する必要がある。管理上の課題としては、暗号鍵の有効期間についての考慮、暗号鍵と署名対象文書との対応付けの記録が上げられる。

(5)パスワード管理

暗号を用いる上では暗号鍵の代わりにパスワードが用いられる場合も多くある。ユーザにより生成、更新（破棄）される場合には注意が必要である。

2.2.2. 暗号鍵の分類

一般に暗号の用途とは、暗号の利用により実現される基本的なサービスのことをさす。用途には、機密性、完全性、認証、認可、否認防止がある。

暗号鍵は、暗号アルゴリズムの大分類、利用目的（用途）に応じ、管理内容や利用する期間等が異なる。これらを基にして、暗号鍵を分類することができる。NIST SP800-57part1 に示された暗号鍵の分類のうち、主要なものを下表に示す。[1]

表： 暗号鍵の分類（主要用途に関連するもののみ）

分類	説明	使用目的
署名生成鍵 (Private signature key)	デジタル署名の生成に用いられる、公開鍵暗号アルゴリズムのプライベート鍵	認証 データ完全性 否認防止
署名検証鍵 (Public signature verification key)	デジタル署名の検証に用いられる、公開鍵暗号アルゴリズムの公開鍵	認証 データ完全性 否認防止
認証用秘密鍵 (Symmetric authentication key)	メッセージやデータの認証に用いられる共通鍵暗号アルゴリズムの秘密鍵	認証 データ完全性
認証用プライベート鍵 (Private authentication key)	データの完全性と作成者についての保証を提供するために用いられる、公開鍵暗号アルゴリズムのプライベート鍵	認証 データ完全性
認証用公開鍵 (Public authentication key)	データの完全性と作成者の確認のために用いられる、公開鍵暗号アルゴリズムの公開鍵	認証 データ完全性
データ暗号化／復号用秘密鍵 （Symmetric data encryption key）	データの機密性を確保するために用いられる共通鍵暗号アルゴリズムの秘密鍵	機密性

各分類についての詳細を以下に示す。

[1] NIST SP800-57 part1 においては暗号鍵の分類として 19 のカテゴリが示されている。ここでは利用目的に機密性、認証、データの完全性、否認防止が明示される 6 カテゴリを特に重要な暗号鍵とみなして取り上げることとした。

(1)署名生成鍵 (Private signature key)

公開鍵暗号アルゴリズムの鍵ペアのプライベート鍵。

比較的長期間の有効性を持つデジタル署名の生成に用いられる。

管理を必要とする期間は、設定された鍵の有効期間、または破棄されるまでの間。

一般に､否認不可性を確保するため署名生成鍵のバックアップは作成しない。（ただし、認証局の署名生成鍵のようにバックアップが必要とされる場合もある。署名生成鍵のバックアップを作成する場合には、バックアップは所有者自身の管理下に置くべきである。）

(2)署名検証鍵 (Public signature verification key)

公開鍵暗号アルゴリズムの鍵ペアの公開鍵。

デジタル署名を検証するために用いられる。

管理を必要とする期間は、署名データの検証の必要が無くなるまでの間。

公開鍵証明書として複数の鍵のバックアップが作成されて用いられる。

(3)認証用秘密鍵 (Symmetric authentication key)

共通鍵（対称鍵）暗号方式アルゴリズムの秘密鍵。

メッセージ、通信時のセッション、保存データを認証する（完全性および発信元を保証する）ために用いられる。

管理を必要とする期間は、認証が必要となる期間、または破棄されるまでの間。

鍵のバックアップを作成して用いることも可能である。

(4)認証用プライベート鍵 (Private authentication key)

公開鍵暗号アルゴリズムの鍵ペアのプライベート鍵。

データの完全性、発信側エンティティ（人あるいはデバイス）の身元、メッセージ／セッション／保存データの出典について保証を提供するために用いられる。

管理を必要とする期間は、設定された鍵の有効期間、または破棄されるまでの間。

アプリケーションで必要とされる場合には鍵のバックアップが作成される。

(5)認証用公開鍵 (Public authentication key)

公開鍵暗号アルゴリズムの鍵ペアの公開鍵。

データの完全性、発信側エンティティ（人あるいはデバイス）の身元、メッセージ／セッション／保存データの出典について確認するために用いられる。

管理期間は対象データの認証の必要がなくなるまでの間。

公開鍵証明書として複数の鍵のバックアップが作成されて用いられる。

(6)データ暗号化／復号用秘密鍵 (Symmetric data encryption key)

共通鍵暗号アルゴリズムの秘密鍵

データの機密性を確保するために用いられる。

管理期間は、鍵の有効期間またはデータの有効期間のうちいずれか長い間、もしくは鍵が破棄されるまでの間。

バックアップを作成して用いることも可能である。

2.3. 暗号鍵の管理

2.3.1. 暗号鍵のライフサイクル

暗号鍵一般についての管理段階（状態）およびそのライフサイクルについて下図に示す。

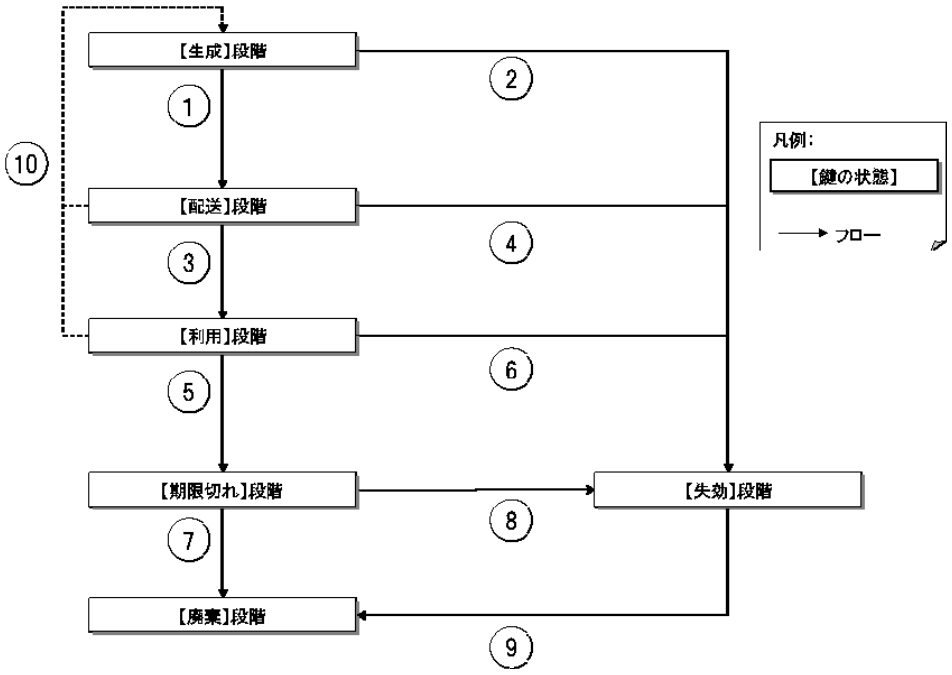

図 2-1　鍵のライフサイクル

ここでは暗号鍵の管理段階(状態)は、【生成】、【送付】、【利用】、【期限切れ】、【失効】、【廃棄】からなるものと定義している。
段階間の遷移の条件を以下に示す。

① 生成され初期登録が済まされた鍵は、【生成】段階から【送付】段階に移行する。
② 【生成】段階において完全性、機密性が疑わしくなった鍵は【失効】段階に移行する。
③ 実際に利用される地点まで配送され使用可能な状態となった鍵は【送付】段階から【利用】段階に移行する。

④ 【送付】状態において完全性、機密性が疑わしくなった鍵は【失効】段階に移行する。
⑤ 有効期間が経過し、新規の署名生成や暗号化等の処理に利用しなくなった鍵は【利用】段階から【期限切れ】段階に移行する。
⑥ 【利用】段階において完全性、機密性が疑わしくなった鍵は【失効】段階に移行する。
⑦ 期限切れとなった鍵に基づいて作られた全データの利用期限が過ぎ、鍵が不要となった時点で【期限切れ】段階から【廃棄】段階に移行する。
⑧ 【期限切れ】段階において完全性、機密性が疑わしいことが明らかとなった鍵は【失効】段階に移行する。
⑨ 取消された鍵に基づいて作られた全データを利用しなくなり、鍵が不要となった時点で、鍵は【失効】段階から【廃棄】段階に移行する。データとしての鍵を完全に消し去ることができる。
⑩ 【送付】段階あるいは【利用】段階において鍵を【失効】した場合、または【利用】段階において鍵が【期限切れ】となった場合には、旧い鍵に変わる新たな鍵を生成する。新たな鍵は【生成】段階からライフサイクルを開始する。

各管理段階における鍵に関する機能については3章に述べる。また、具体的事例として PKI システムにおける暗号鍵の管理について4章に述べる。

2.3.2. 鍵の有効期間設定

暗号鍵の有効期間とは、特定の鍵について、その鍵を扱う正当なエンティティ（人間やデバイス）による鍵の利用が許されている期間のことを指す。

一般に同一の暗号鍵を長期間にわたって利用するとセキュリティ上のリスクは高まる。以下にそれらのリスクを示す。

- 鍵の利用期間が長いほど、秘密鍵の漏洩の可能性が高まる。ミスや事故による漏えいの機会が増えるだけでなく、物理的・論理的に鍵を保護する機構を攻撃者が不正アクセスや脆弱性の攻略により破ろうと試みる機会（時間）も増える。
- 暗号鍵を入手しようとする攻撃の機会が増え、攻撃可能な時間も延びる。
- 同一の鍵を利用し続ければ、鍵が漏洩／解読された場合の影響範囲が拡大する。
- ある暗号鍵に対して数学的手法で解読を試みる時間が長く取れるように

なる。また、同じ鍵に基づく情報がより多く作成されるため解読に有用な情報を大量に入手し易くなる。

これらを避けるために、暗号鍵には有効期間を設定し、同一の鍵の利用を制限する必要がある。

有効期間の設定には次のような副次的なメリットも期待できる。

- 管理対象とする暗号鍵、暗号処理の対象とするデータ・メッセージの総量に制限を行うこととなり、管理の実効性が高まる。
- 鍵更新の必要性が明確化され、鍵危殆化時の対応や新たな暗号アルゴリズムの切り替えを考慮したシステム構築も容易になる。

暗号を用いるシステムにおいては、有効期間に達した暗号鍵が利用されることを想定し、鍵、鍵に付随する情報、あるいは鍵から作成された情報を基に、鍵が期限切れで既に無効なものであることを検出可能とする必要がある。

鍵の有効期間をより短く設定すると、鍵の更新を頻繁に行う必要が生じる。現実的には更新に伴う手作業等を通じて鍵が漏洩するリスクが高まる可能性がある。更新頻度を上げる前提として適切な鍵更新プロセスの実現が必要となる。

暗号鍵の有効期間設定には、解読の可能性だけでなく、暗号鍵を使用して作成されるデータ（文書）の有効期間、暗号鍵およびそれらのデータを使用するユーザが権限を持つ期間（在任期間）、システムの改変・更新の計画等の考慮が伴う。

鍵が復号の対象とする暗号文や、検証対象とする署名が付された情報の有効期間がより長期にわたる場合には、有効期間に達した鍵をアーカイブする場合もある。（3.5.1項参照）

鍵により生成された情報が全て破棄され、以後鍵が全く使われないことが明確になった時点で鍵は破棄される（3.5.3項参照）。

2.3.3. 鍵危殆化の想定

- 秘密鍵、プライベート鍵が漏洩した場合には、その鍵で保護されている全ての情報について、漏えい、改ざん、偽造等が起きている可能性がある。
- 速やかに鍵情報を失効させ、影響を受けうる者に通知し、実際の影響範囲の特定と復旧作業（新たな鍵の発行等）を行う。
- 失効させる事態となる可能性が高く、影響範囲が比較的小さい鍵（例：各ユーザの鍵）については、事前に対処の方法（機能やルール）を備えておくことが有効である。

・ 影響範囲が広い鍵（例：CA の署名鍵、システムで共有している暗号化や鍵配送のための秘密鍵）については、速やかに通知するとともに、システム全体としての鍵情報の再設定・交換を行う。

3. 暗号鍵ライフサイクル管理

3.1. 鍵の生成

3.1.1. 一般

- 暗号鍵は適切な暗号モジュールの内部で生成することが望ましい。
- 利用者の手元で暗号鍵を生成する場合には、利用者以外が入手できないことを確実とするような手法による生成が望ましい。
- 秘密鍵／プライベート鍵は、その値を推定することが至難であるような乱数／擬似乱数処理を通じて生成されることが望ましい。
- 平文の秘密鍵／プライベート鍵への直接的なアクセスはできないことが望ましい。

3.1.2. 公開鍵暗号方式の鍵ペアの場合

- 公開鍵暗号方式の鍵ペアは、その所有者（秘密鍵を利用するエンティティ）、認証局（CA）等の機関、あるいはこれらが協力する処理により生成される。
- プライベート鍵は人間が理解できない形式（可読性がない形式）で生成する。
- プライベート鍵の生成に用いたシードは（鍵回復を考慮しない場合には）生成後にすみやかに消去する。
- 鍵ペアの所有者が、所有者自身の否認防止に鍵ペアを用いる場合には自身で署名用途の鍵ペアを生成する必要がある。
- ユーザが鍵ペアを生成する場合には、真にそのユーザが鍵ペアを所有することを示す情報を認証機関（CA）に提供し、その情報に基づいて CA は検証を行わなければならない。（これを POP: proof of possession という）
- CA 等で集中して生成される署名用途の鍵ペアは、個々のユーザの否認防止には用いることができない。組織の認証局がある組織に属するユーザのために鍵ペアを生成する場合には、その組織としての否認防止は確保される。

3.1.3. 共通鍵暗号方式の秘密鍵の場合

- 共通鍵暗号方式の秘密鍵は適切な乱数生成、鍵更新、マスタ鍵からの生成により鍵生成が行われなければならない。
- 再現困難な鍵を生成する処理としては、乱数生成／擬似乱数生成があげられる。あるひとつの鍵から再現可能な処理を通じて複数の鍵を生成する処理は鍵変形（key transformation）、鍵導出（key derivation）と呼ばれる。これらの処理は初期鍵が鍵空間において予測不可能な値であれば、以後生成される全ての鍵が予測不可能であるという性質を持つことが望ましい。また、あるこの手法で作られたひとつの鍵が漏洩した際に、他の鍵を逆に導くことが不可能である性質も求められる。

3.2. 鍵の配送

3.2.1. 一般

- 秘密鍵を配送する際には、配送先を確実なものとする必要がある。例えば、利用者へのプライベート鍵の配送の処理には何らかの利用者の本人確認が含まれる。
- 配送される鍵（および送付中に一時的に保存される鍵）は適切に保護されなければならない。
- 保護される対象としては、暗号サービスを確立するために配送中の鍵材料（例；機密性の提供に用いられる鍵の確立）、復旧に備えバックアップまたは記録保存される暗号化情報などがある。
- 鍵の配送は、手動（例：郵送／宅配便事業者等による配達）、自動（例：プロトコルに基づいた電子的通信）、あるいは手動と自動の組み合わせにより行われる。プロトコルによっては保護を提供する場合もある。
- 鍵材料への保護メカニズムの適用は発信側エンティティが行う。保護された状態からの鍵材料の復元・検査は受信者側エンティティが行う。
- 配送後の暗号鍵の可用性は、通信時に伝送誤り、改ざん、破壊の可能性があるため暗号学的手法を適用しても保証はできない。しかしながら経路の多重化、誤り訂正符号等の暗号以外のメカニズムによるサポートは可能である。
- 配送における暗号鍵の完全性は、改ざん防止と改ざん検出の両方に係る。配送中の鍵情報の完全性は、物理的保護が提供されるもとでの手動処理あるい

は通信プロトコルに則った電子的な配送処理において、ひとつ以上の保護手法を用いて保護される。情報に対する CRC（手動のみ）、MAC、デジタル署名の適用により検出する手法、あるいは、鍵材料は目的が明確な暗号処理で用いられる際に、受信した情報で目的通りの暗号化ができない場合に鍵材料が壊れている可能性を検出する手法がある。配送後の暗号鍵の完全性に関する不具合が検出された際の対応は、暗号鍵の利用環境により異なる。不具合の処理を適切に行い、攻撃の機会としないことが必要である。この対応についてはセキュリティ方針で定義を行う。

- 配送における暗号鍵の機密性については、鍵材料の暗号化、知識分割（split knowledge）に基づく鍵材料の分割を適用することで確保する。郵送事業者等が提供する適切な物理的・手続き的な保護といった手法を 1 つ以上用いることにより保護される。
- 暗号鍵は、デバイスの変更やすり替え、受け取り先のなり済まし等の不正が行われていないと確認された際にのみ受け渡されるべきである。

3.2.2. 公開鍵暗号方式の鍵ペアの場合

- 署名生成に用いられるプライベート鍵は、その所有者以外のエンティティに配送されてはならない。
- 公開鍵の配送においては、受信者に鍵ペアの所有者が既知であることが保証されるべきである。さらに以下についても保証されるべきである。
    - 鍵の目的／用途が判っていること
    - 公開鍵と関係するパラメタが分かっていること
    - 公開鍵が有効であること
    - 所有者が公開鍵に対応するプライベート鍵を所有すること
- CA 等で集中的に鍵ペアを生成する場合には、鍵ペアは暗号モジュール内で生成した後で、その鍵ペアの所有者だけに対して機密性を保ちつつ鍵を配送しなければならない。

3.2.3. 共通鍵暗号方式の秘密鍵の場合

- 共通鍵暗号方式の秘密鍵は、以下のいずれかの方法で生成・配送される。
    - 生成に続けた、手動による配送、あるいは、電子的な鍵配送（事前に配布した鍵暗号化鍵による配送等）。
    - 鍵共有方式の適用による鍵の確立
    - 鍵更新処理による鍵の決定

- マスタ鍵からの導出

・ 全ての鍵は適切な保護を与える暗号モジュール内で生成されるべきである。
・ 手動での鍵の配送について
  - 鍵は暗号化されるか、適切な物理的セキュリティ手段により保護された上で輸送される。
  - 手動での鍵の配送については以下が保証されなければならない：正式に認められた発信者から鍵が発送されていること。正式に認められた受信者に鍵が受け取られること。鍵を生成するエンティティおよび鍵を受け取るエンティティの両方が信頼するエンティティがから鍵を配送すること。配送時に鍵が適切な方法に従い保護されること。
  - 鍵を暗号化して配送する場合には、鍵は、専用の鍵ラッピング鍵を用いる適切な鍵ラッピングスキーム、あるいは、受信者が持つ鍵配送用公開鍵を用いる鍵配送スキームで暗号化されなければならない。
  - 秘密分散の手法を用いる際には、各鍵コンポーネントは、各個人への輸送のために、暗号化されるか、セキュアな経路を通じて個別に配送されなければならない。機密性を要する情報として個々の鍵コンポーネントに対して適切な物理的セキュリティ手順が用いられなければならない。
・ 電子的な手法での鍵の配送について
  - 鍵の配送に先立ち適切に生成され配布された、鍵暗号化鍵または鍵配送用公開鍵が必要となる。
  - 適切な鍵暗号化鍵あるいは鍵配送スキームのみを使わなければならない。これらのスキームは、鍵暗号化鍵および配送される鍵が秘密にされており改ざんされていないこと、適切に保護されていることの保証を与える。加えて、受信者が正しい鍵を得ることを保証する必要がある。
・ 平文の鍵は手動で取り扱わないことが望ましい。耐タンパー性を持つハードウェアセキュリティモジュール等の適切な手段で保護した上で配送する。
・ 鍵材料については、二重制御（dual control）と知識分割（split knowledge）により処理する。
・ 暗号化された鍵は通信路を介して電子的に配送されうる。鍵のすり替え、改ざんに対する防護が必要となる。
・ 鍵を保護するデバイスへの鍵の配送やロードを行う際には適切な手段をお用いる。（例：手動でキーパッド等から鍵材料を直接入力する。デバイス間を有線で直接接続してのロード）

3.3. 鍵の利用

- 通常、暗号鍵は有効期間中、常に利用可能な状態におかれる（運用の連続性が確保される）。
- 有効期間中の暗号鍵はストレージ中で適切に保護されなければならない。鍵の保管については3.4.1項に述べる
- 暗号鍵へのアクセスを限定し、取り扱うことが許された者のみが鍵を利用できるような手段で実装する。例えば利用に先立つユーザ確認機能を用意する。
- 暗号鍵は運用の連続性を確保するために、有効期間中に紛失や消去等で利用できなくなった場合に復元可能であることが要求される。鍵の復元（key recovery）はバックアップあるいは鍵導出（key derivation）に基づく。
- 以下に、鍵の運用の連続性を確保する手段として、鍵の変更および鍵導出について述べる。

3.3.1. 鍵の変更

- 暗号鍵の有効期間が終了した後も運用を継承する場合は、古い鍵と新たな鍵を交換する。この交換は、暗号鍵の有効期間の継続性を維持するために、有効期間の終了が近づき、期間が終わる前に行われる。
- 新たな鍵は鍵変更（key change）の手法により入手される。鍵の変更には鍵再作成（re-keying）および鍵更新（key update）の 2 つの手法がある。以下にそれらの手法について述べる。
- 古い鍵は適切に破棄されなければならない。必要でなくなった秘密鍵は漏洩するリスクを最小とするために直ちに破壊されるべきである。鍵の廃棄については3.5節に述べる

(1) 鍵再作成

- 鍵再作成（re-keying）とは、以前の鍵の値とは全く無関係に新しい鍵を生成する手法を指す。
- 鍵の再作成は鍵確立方式を用いて行われる。古い鍵を共有していたエンティティ間で情報の交換が必要となる。
- 鍵再作成は鍵が危殆化した際（ただし鍵確立方式が危殆化していない場合に限られる）あるいは暗号鍵の有効期間の終了が近づいている際に行われる。

(2) 鍵更新

- 鍵更新（key update）とは、古い鍵の値に基づいて、新しい鍵を作る手法である。
- 鍵更新では､古い鍵に不可逆関数を適用して新しい鍵を得る手法が用いられる。古い鍵を共有していたエンティティ間での情報の交換は不要である。
- 古い鍵が危殆化した場合には鍵更新を用いてはならない。
- 新たに作られた鍵が危殆化した場合でも（不可逆関数が用いられるため）以前の鍵は危殆化せず保護される。

3.3.2. 鍵の導出

- 鍵導出（key derivation）とは、マスタ鍵と呼ばれる秘密の値から秘密鍵（共通鍵暗号アルゴリズムの共通鍵あるいは公開鍵暗号アルゴリズムのプライベート鍵）を導出する手法である。導出された秘密鍵は導出鍵と呼ばれる。
- 鍵導出では､秘密値を不可逆関数(導出関数)に入力して導出鍵を生成する。導出関数は他の導出鍵から導出鍵を推定できるものであってはならない｡導出鍵の強度は導出に用いられるアルゴリズムやマスタ鍵の強度よりも大きくはならない。

3.4. 鍵の保管／バックアップ

3.4.1. 鍵の保管

- 転送中ではない暗号鍵は何らかのデバイスか記録媒体に保管される(転送中の暗号鍵のコピーの場合も同様である)。保管時には適切な保護を適用しなければならない。
- 暗号鍵は、それを用いるデバイスあるいはモジュール、あるいは即座にアクセス可能な記録媒体に保存される｡必要とされた際に暗号鍵がデバイスあるいはモジュールのアクティブなメモリ上に存在しない場合にはアクセス可能な記録媒体から取得される。
- 暗号鍵はアプリケーションで即座に利用可能なように保存されることがある（例：ローカルなハードディスクやサーバ)。典型的な例としては暗号モジュールや即座にアクセス可能な記憶領域(例:ローカルなハードドライブ)に置かれる鍵材料がある。
- 鍵材料は、リムーバブルメディア（例：CD-ROM）上に電子的な形態で記

録される場合、リモートアクセス可能な場所に置かれる場合、紙媒体にハードコピーされ安全な場所に保管される場合がある。これらはバックアップやアーカイブの際にしばしば行われる。

- データが暗号鍵を用いて保護されている間は、暗号鍵を即座に利用可能にしておく必要がある。この保護を提供する一般的な手法としては、1 つ以上のコピーを作成して異なる地点に保管しておく方法がある。
- 暗号鍵の有効期間の間は、長期間にわたり可用性を必要とする鍵材料は運用とバックアップの各記憶装置のそれぞれに保管されるべきである。
- 全ての鍵情報には完全性の保護が必要である。改ざんからの保護、改ざんの検知、改ざんからの回復が取られる。これらは物理的な隔離手法（例：アクセス制御機能を持つ暗号モジュールや OS、他システムから独立したシステムやメディア、金庫等）、暗号学的手法（例：MAC やデジタル署名、意図された暗号処理の実行結果による確認）、それらの組み合わせにより実現される。
- 改ざんや誤りが検出された際に鍵情報を回復させる場合には、物理的に異なる場所に鍵情報のコピーを作成し保管しておく手法をとるべきである。これらのコピーの完全性についても定期的に確認を行なうべきである。
- 秘密鍵やプライベート鍵の機密性を確保するためには、鍵暗号化、暗号モジュール、アクセスが管理されたセキュアな保管庫のいずれかが用いられる。鍵暗号化鍵の回復はその鍵で暗号化された鍵の回復よりも困難とすべきである。

3.4.2. 鍵のバックアップ

- 運用に用いられるストレージに置かれている現在利用可能な鍵情報のコピーを保管するためにバックアップは行われる。
- 独立したセキュアな保管用メディアへの鍵材料のバックアップは鍵回復（key recovery）のためのソースとなる。鍵回復については3.6節に後述する。
- 鍵情報が漏洩する危険性を下げるためには厳格なバックアップの運用が求められる。
- 全ての鍵がバックアップを必要とするわけではない。鍵の分類とバックアップの必要性については2.2.2項に示した通りである。
- 組織の認証局等が鍵のバックアップを行う場合には、ユーザ個人の否認防止は実現が困難となる点に注意が必要である。

3.5. 鍵の期限切れ／失効／廃棄

- 鍵の有効期間の終了時、あるいは鍵が危殆化した際には、運用されている鍵は適切な手段で取り除かれる必要がある。必要が無くなった暗号鍵を速やかに破棄する機構を用意する。
- 以下では、有効ではなくなった鍵が取り除かれる際の流れに沿って、有効期限を過ぎた鍵の扱い、鍵の失効、鍵の廃棄について説明する。

3.5.1. 鍵の期限切れ

- 有効期間が過ぎた鍵は使用を停止される。処理・運用が続けられる場合は、古い鍵に変わる新たな鍵が用いられる（3.3.1項参照）。
- 暗号鍵のアーカイブが必要となる場合は、鍵の有効期間が終わる前にアーカイブすることが望ましい。

3.5.2. 鍵の失効

- 秘密鍵の漏洩による鍵の危殆化や、暗号鍵の利用者が組織から離れることに伴う登録抹消等により、有効期間が終わる前の暗号鍵について以後の利用を停止する必要が生じうる。これを鍵の失効（key revocation）という。
- 暗号鍵の失効は、共通鍵暗号アルゴリズムの共通鍵や公開鍵暗号アルゴリズムの公開鍵が無効であることを明示するために行われる。公開鍵が無効とされた場合には対応するプライベート鍵も無効となる。
- 暗号鍵の失効は、その鍵の以後の使用が継続されないことの通知により実現される。これは関係する全エンティティへの通知を送信する機構、あるいはエンティティからの通知要求に応じる機構を伴う。
- 同じ鍵のコピーが存在する場合、バックアップが存在する場合、鍵がペアで使われる場合等を考慮し、いずれの地点に対しても通知が行われ、失効した鍵の取扱いが適切なものとする必要がある。

3.5.3. 鍵の廃棄

- 不要となった暗号鍵の記録は消去される。特に秘密鍵（共通鍵およびプライベート鍵）は有効期間終了後に確実に消去される仕組みが必要となる。公開鍵は、保持されたままであっても消去されても良い。
- ただし、監査の目的で暗号鍵および暗号鍵に関連する情報が保持され、後に

鍵の変更や危殆化を追跡するために用いられる場合もある。

- 鍵のコピーが存在する場合は、鍵危殆化の可能性を最小とするために、鍵が不要となった時点で全てのコピーを消去しなくてはならない。（アーカイブあるいは鍵回復に備えてコピーがとられている場合も同様に考慮が必要となる）
- 暗号化されていない暗号鍵を記録された媒体から消去する際には適切な物理的・電磁気学的な消去方策を講じる必要がある。通常のデータを消去する場合と同様の手法で削除しただけでは情報が完全に抹消されない可能性がある。（例えば長期間暗号鍵が記録されていた磁性体には暗号鍵のビットが焼き付けられている可能性がある）

3.6. 鍵の回復

- 多くの場合、紛失した古い鍵は失効させて新たな鍵を発行しなおすが、以前暗号化された情報や署名が付された情報の扱いが問題となる。
- 暗号鍵の紛失等により鍵を利用不可能となる事態に対処するために、バックアップを取り、鍵の回復（key recovery）を行う。鍵の回復は、暗号化された情報の復号、データの完全性の検証のために次のような事態になった際に行われる。
  - 暗号鍵の有効期間が過ぎ、ストレージ中に暗号鍵がなくなっている。
  - 暗号鍵が、システムのクラッシュや改ざんにより破損している。
  - 暗号鍵の所有者が所属する組織が、その暗号鍵の利用を求めた際に所有者が求めに応じられない。
- 暗号鍵の回復に際しては、暗号鍵自体をバックアップあるいはアーカイブから取得しデバイス、モジュール等に配送する場合、鍵導出の手法を用いて、改めて暗号鍵を再構築する場合がある。
- 鍵の回復に備えたバックアップやアーカイブの作成の有無についてはシステム個別に決定される。決定にあたっては以下の考慮が必要となる。
  - 暗号鍵の分類に基づく種別
  - 暗号鍵が用いられるアプリケーションの種別
  - 暗号鍵が保持される形態と保持者
  - 暗号鍵を用いた通信におけるエンティティの役割
  - 暗号鍵が用いられるアルゴリズムおよび計算
  - 暗号鍵により保護される情報の価値と鍵喪失時の被害の大きさ
- 暗号鍵の回復を実現するためには鍵回復に関する方針に従い、セキュアな鍵復元のシステムを確立する必要がある。このシステムは、暗号鍵の保存・復

元に関する技術と設備、システム管理の手順、システムオペレータで構成される。

- 暗号鍵の回復については運用方針を事前に策定しておく必要がある。以下に関して考慮し明確化しておく。
    - 保管しておくべき暗号鍵
    - 暗号鍵を保管する手法および場所
    - 鍵回復に関連する情報の取扱い責任者
    - 鍵回復を要請可能な者および回復の条件
    - 鍵回復の方針を変更する条件および変更可能な者
    - 適切に鍵回復が行われたことを示すための監査機能
    - 長期間を経た暗号鍵とその破壊に関する対処
    - 暗号鍵が回復された際に通知を行う対象者および条件
    - 鍵回復のためのデータが危殆化された際に従うべき手順

4. PKI システムにおける暗号鍵ライフサイクル管理

本章では、ライフサイクルを考慮した暗号鍵管理の実際を具体的に示す一例として PKI における公開鍵証明書の管理とセキュリティ対策について示す。

想定する PKI の用途モデルを下の 2 つの図に示す。この例ではユーザ証明書を利用者における署名生成と検証に用いることを想定し、ユーザ証明書に係る鍵ペア、認証局（CA）の自己署名証明書に係る鍵ペアを中心に証明書の利用を示している。このモデルはあるひとつの構築手法を例示するものであり利用者は実際に利用するシステムがどの様に構成されているかイメージして検討することが好ましい。。

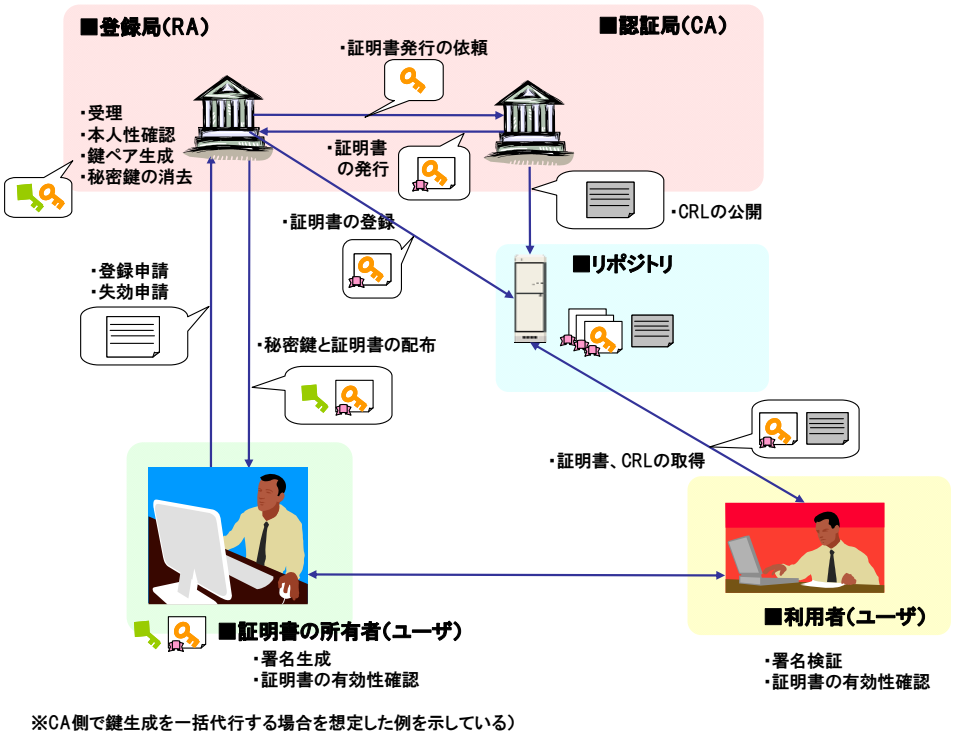

図 4-1 用途モデル（署名用途に用いられるユーザ証明書の鍵ペア）

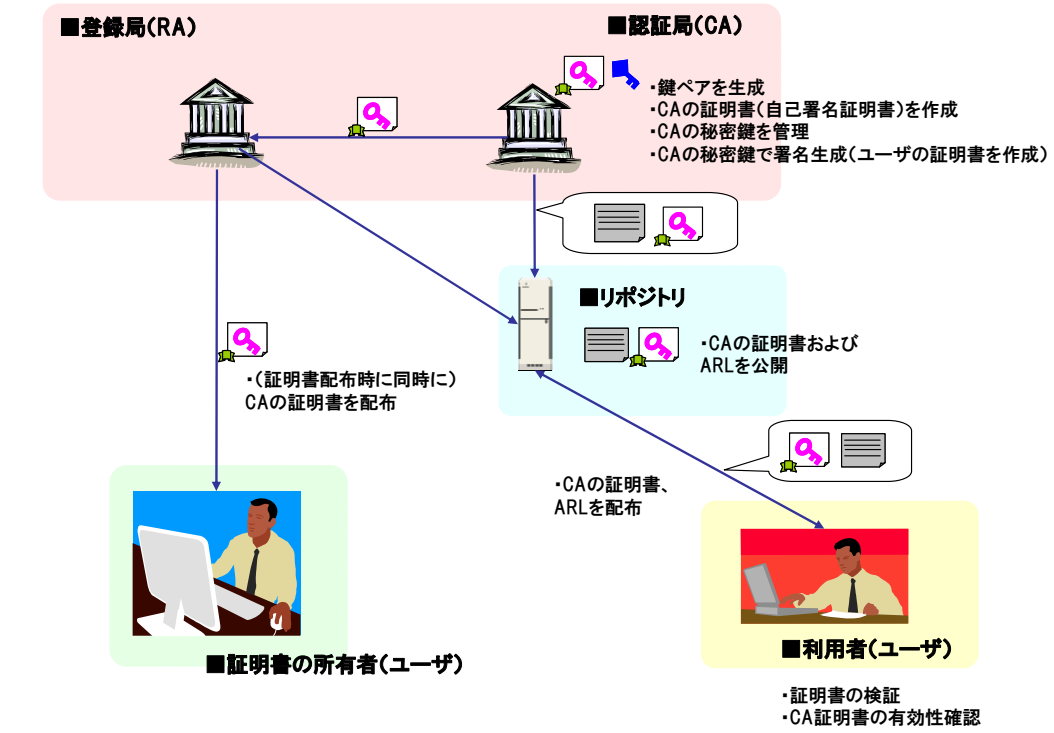

図 4-2　用途モデル（CA の自己証明書の鍵ペア）

PKI システムの全体を通じて重要な要件としては、特定のエンティティとプライベート鍵が対応付けられ、そのエンティティのみがプライベート鍵にアクセス可能である性質が確保されることがあげられる。プライベート鍵は唯一存在し、適切に管理され、他のエンティティによって決して用いられないことを確実にしなければならない。

以下では、このモデルに基づいて、利用者のプライベート鍵に係る鍵管理を段階毎に 4 つに分けて記述する。

4.1. 利用者のプライベート鍵の管理

以下では、利用者のプライベート鍵の管理について、脅威と対策の方向性をライフサイクルに沿って記述する。下図に利用者のプライベート鍵のライフサイクルを示す。

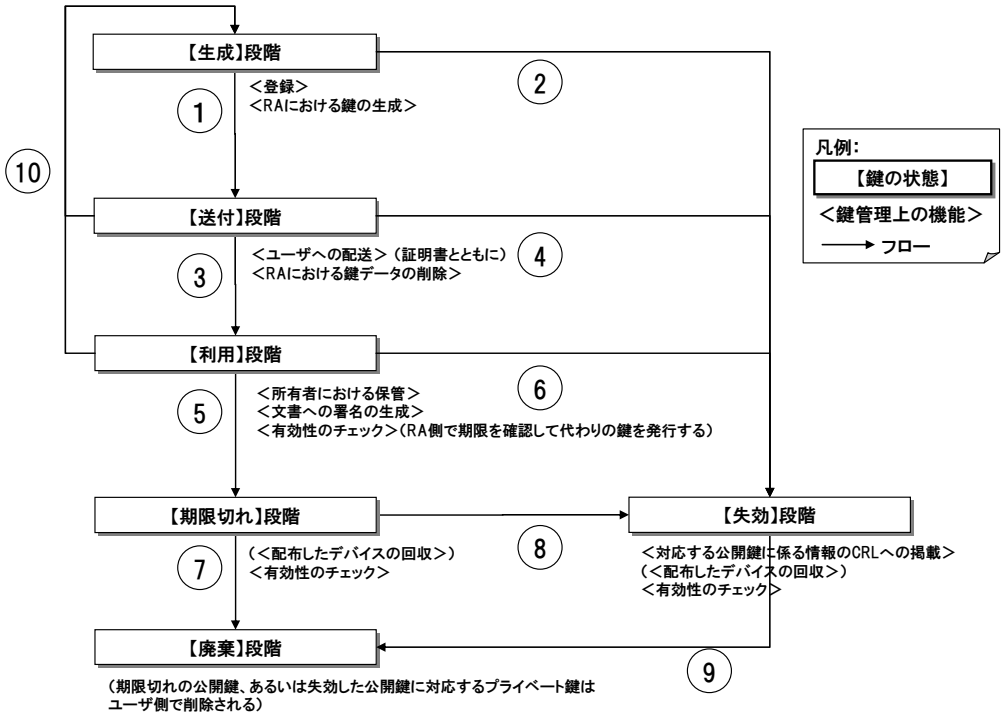

図 4-3　利用者のプライベート鍵のライフサイクル

4.1.1. 生成段階

(1)発行申請とエンティティ登録

(a)処理の内容

利用者は登録局（RA）に赴いて登録申請を行う。RA は登録申請を受理し、申請内容に基づいて利用者の資格および本人性の審査（確認）を行う。

関連する情報資産	種別	ロケーション
登録申請、本人確認のための情報（登録申請情報）	データ	RA
証明書に記載する利用者情報（利用者情報）	データ	RA
登録申請／本人確認ツール	ソフトウェア	RA
RA のオペレータ	エンティティ	RA
利用者	エンティティ	利用者

(b)想定される脅威

脅威（故意）	種別
登録後に登録申請情報を不正に入手される	情報の漏洩
登録後に登録申請情報が改ざんされる（あるいは削除される）	情報の改ざん
登録後に利用者情報が第三者に漏洩する	情報の漏洩
登録後に利用者情報が改ざんされる（あるいは削除される）	情報の改ざん
登録申請／本人確認ツールが改ざんされる（例：情報を漏洩する機能の追加）	ソフトウェアの改ざん・破壊
利用者になりすまされ虚偽の申請をされる	なりすまし

脅威（過失）	種別
登録時に登録申請情報が誤入力される	情報の誤入力
登録後に登録申請情報が消失する	情報の亡失
登録後に登録申請情報を漏洩する	情報の漏洩

(c)対策の方針

- 厳密な本人確認を行う。
- 利用者資格に関する審査を厳密に行う。

(d) 対策手法の例

・ 本人との対面を含む手続きで登録を行う。
・ 利用者資格について証明する手段を用いる

(2)登録局（RA）における鍵の生成

(a)処理の内容

このモデルでは認証局サイドの登録局（RA）で利用者の鍵ペアを生成するものとしている。[2]

関連する情報資産	種別	ロケーション
鍵ペア	データ	RA
鍵のシード	データ	鍵ペア生成用ツール内
鍵ペア生成用ツール	ソフトウェア	RA
鍵ペア/証明書保管ツール	ソフトウェア	RA
RA のオペレータ	エンティティ	RA

(b)想定される脅威

脅威（故意）	種別
鍵ペアを不正に入手される	情報の漏洩
鍵ペアが別の鍵ペアにすりかえられる	情報の改ざん
鍵ペア生成ツールが改ざんされる （例：別の鍵ペアへのすりかえ、鍵ペアを漏洩する機能の追加）	ソフトウェアの改ざん・破壊
鍵シードがすりかえられる	情報の改ざん

脅威（過失）	種別
鍵ペアが消失する	情報の亡失
鍵ペアを漏洩する	情報の漏洩
問題のある鍵シードが使用される	デザイン・運用上のミス

(c)対策の方針

- 鍵の生成に関するオペレータの不正を監視する
- 暗号学的な強度の観点からみて適切な鍵シードを用いる。

(d)対策手法の例

- 鍵ペアおよびプライベート鍵にアクセスする際に必要とする PIN コードは、複数のオペレータが安全な環境下で相互にチェックを行いながら協同作業により生成する。
- 鍵ペアおよび PIN コードは、オペレータがその内容を知らないようにして生成する。
- 鍵ペアおよび PIN コードは IC カード等の配布媒体に記録した後、生成時

に関連する他の全ての機器上から、ただちに完全に消去する。

- 鍵のシードとして物理乱数生成装置を用いる。
- 動作が検証されたツールをセキュアな実行環境上で用いて鍵ペアを生成し保持する。
- 鍵の生成と一時的な保存に関する一連の処理を自動化する。

[2] IC カード上で鍵生成を行い、外部に出力しない手法がある。

4.1.2. 送付段階

(a)処理の内容

登録局（RA）は利用者に、利用者の秘密鍵を証明書とともに配送する。

利用者は登録局（RA）より得たプライベート鍵を、利用者の環境において保管する。

関連する情報資産	種別	ロケーション
プライベート鍵	データ	RA、RA—利用者間、利用者
利用者の証明書	データ	RA、RA—利用者間、利用者
IC カード検証ツール	ソフトウェア	RA
一時保管用ツール	ソフトウェア	RA
利用者	エンティティ	利用者
RA のオペレータ	エンティティ	RA
RA—IC カード間	通信路	—
RA—利用者間	通信路	—

(b)想定される脅威

脅威（故意）	種別
配送の途中でプライベート鍵が不正に入手される	情報の漏洩
異なるプライベート鍵と証明書、あるいは偽のプライベート鍵と証明書が IC カードに格納される。	情報の改ざん
検証ツールが改ざんされ、すりかえられた不正な IC カードにプライベート鍵、証明書が格納される。	ソフトウェアの改ざん

脅威（過失）	種別
プライベート鍵を消失する	情報の亡失
プライベート鍵が誤入力される	情報の誤入力
プライベート鍵を漏洩する	情報の漏洩

(c)対策の方針

- 利用者はプライベート鍵およびその使用に係る情報の盗難、紛失、不正利用に対して十分な注意を払う。
- プライベート鍵を誤って紛失、消去しないように適切な媒体上に記録する
- プライベート鍵は利用者のみが活性化できるようにする。
- 安全な経路を用いて利用者にプライベート鍵を送付する。

(d) 対策手法の例

- プライベート鍵を可読性のあるデータとして取り扱わない。
- プライベート鍵を耐タンパー性を持つ暗号モジュールである IC カード内に格納する。IC カードに格納後は外部に直接プライベート鍵を出力できないようにする。
- プライベート鍵は、利用者が PIN を用いて活性化する。プライベート鍵および PIN コードの 2 つの情報を利用者が合わせて用いた際にのみ鍵を使用可能とする。
- プライベート鍵と PIN を利用者に異なる送付方法（経路）で送る。

4.1.3. 利用段階

(1)利用者によるプライベート鍵の保管

(a)処理の内容

利用者はプライベート鍵を保管する。

関連する情報資産	種別	ロケーション
プライベート鍵	データ	利用者
利用者	エンティティ	利用者

(b)想定される脅威

脅威（故意）	種別
プライベート鍵を他者に知られる	情報の漏洩
プライベート鍵を他者に改ざんされる	情報の改ざん
署名アプリケーションを改ざんされ処理を妨害される（例：偽のプライベート鍵で署名をつける。誤った署名を出力する）	ソフトウェアの改ざん

脅威（過失）	種別
利用者がプライベート鍵を漏洩する（例：プライベート鍵を記録したディスクを不用意に他者に渡してしまう）	情報の漏洩
利用者がプライベート鍵を紛失する（例：暗号化して保存しているプライベート鍵のパスワードを忘れてしまう。）	情報の亡失
利用者がプライベート鍵を誤って消去する（例：ハードディスクを壊しプライベート鍵を読み出せない）	情報の亡失

(c)対策の方針

- プライベート鍵を利用者のみがアクセス可能とする。
- 利用者がプライベート鍵を誤って紛失、消去を未然に防止する。

(d)対策手法の例

- プライベート鍵を耐タンパー性を持つ暗号モジュールであるICカード内に保管し、格納後はプライベート鍵は外部に出力しない。
- ICカード上のプライベート鍵は利用者がPINを用いて活性化する。
- ICカード上のプライベート鍵は利用者がログアウトするか、ICカードを取

り外すことで非活性化する。

(2)署名の作成

(a)処理の内容

利用者はプライベート鍵を用いてデジタル署名を作成する。

期限切れあるいは失効している秘密鍵では署名を行わない。

関連する情報資産	種別	ロケーション
プライベート鍵	データ	利用者
署名アプリケーション	ソフトウェア	利用者
利用者	エンティティ	利用者

(b)想定される脅威

脅威（故意）	種別
プライベート鍵を他者に知られる	情報の漏洩
プライベート鍵を他者に改ざんされる	情報の改ざん
署名アプリケーションを改ざんされ処理を妨害される（例：偽のプライベート鍵で署名をつける。誤った署名を出力する）	ソフトウェアの改ざん

脅威（過失）	種別
利用者がプライベート鍵を漏洩する（例：プライベート鍵を記録したディスクを不用意に他者に渡してしまう）	情報の漏洩
利用者がプライベート鍵を紛失する（例：暗号化して保存しているプライベート鍵のパスワードを忘れてしまう。）	情報の亡失
利用者がプライベート鍵を誤って消去する（例：ハードディスクを壊しプライベート鍵を読み出せない）	情報の亡失

(c)対策の方針

・ プライベート鍵を利用者以外にはアクセスできないよう管理可能な媒体に記録する

(d)対策手法の例

・ プライベート鍵を IC カード内に保管し、IC カードの外部には出力しない。

・ 署名アプリケーションは、署名生成時に IC カード内の機能を呼び出す。

(3) 失効状況の確認

(a) 処理の内容

失効したプライベート鍵を用いた署名は行わない。

期限のチェックについては、署名の際にプライベート鍵の有効期間（＝証明書の有効期間）を確認する

失効状況のチェックについては、署名の際にプライベート鍵の失効状況（＝証明書の失効状況）を CRL に照らし合わせて確認する。

関連する情報資産	種別	ロケーション
プライベート鍵	データ	利用者
署名アプリケーション	ソフトウェア	利用者
利用者自身の証明書	データ	利用者
CA の証明書	データ	利用者
現在の時刻に関する情報	データ	利用者
CRL	データ	リポジトリ、リポジトリ—利用者間、利用者
証明書有効性検証ツール	ソフトウェア	利用者
ディレクトリ・ソフトウェア	ソフトウェア	リポジトリ
利用者	エンティティ	利用者
利用者—リポジトリ間	通信路	—

(b) 想定される脅威

脅威（故意）	種別
プライベート鍵を他者に知られる	情報の漏洩
プライベート鍵を他者に改ざんされる	情報の改ざん
署名アプリケーションを改ざんされ処理を妨害される（例：偽のプライベート鍵で署名をつける。誤った署名を出力する）	ソフトウェアの改ざん
現在の時刻に関する情報を改ざんする	情報の改ざん
証明書有効性検証ツールを改ざんし、証明書の有効・無効について誤った判断をさせる（例：改ざんされた署名をパスさせる、期限切れの証明書をパスさせる）	ソフトウェアの改ざん

脅威（過失）	種別
利用者がプライベート鍵を漏洩する（例：プライベート鍵を記録したディスクを不用意に他者に渡してしまう）	情報の漏洩
利用者がプライベート鍵を紛失する（例：暗号化して保存しているプライベート鍵のパスワードを忘れてしまう。）	情報の亡失

利用者がプライベート鍵を誤って消去する（例：ハードディスクを壊しプライベート鍵を読み出せない）	情報の亡失
CRL を誤って消去する	情報の亡失
本来有効な証明書を誤って CRL に載せる	情報の誤入力・誤更新

(c) 対策の方針

- 時刻情報の改ざんを防止する
- 古い証明書の有効期限が切れる前に証明書の更新を申請する。（利用期間が重複していても構わない。）
- 証明書を利用する際にソフトウェアで有効期限を確認し、当該公開鍵が利用可能かを自動的に判断する。

(d) 対策手法の例

- 署名アプリケーションを改ざん困難／検出可能な実行環境上で実行する。
- 失効した鍵について、迅速かつ信頼のおける手段で周知可能とするための機構（取り消された鍵のリストを含む）を整備する。

4.1.4. 期限切れ段階

利用期限が切れたプライベート鍵は新たな署名を作成するために使われることはない。プライベート鍵はすみやかに破棄される。

(a) 処理の内容

関連する情報資産	種別	ロケーション
プライベート鍵	データ	利用者
現在の時刻に関する情報	データ	利用者
署名アプリケーション	ソフトウェア	利用者
利用者	エンティティ	利用者

(b) 想定される脅威

脅威（故意）	種別
期限切れのプライベート鍵を用いて新たな署名を作成する	その他
期限切れのプライベート鍵を他者に知られる	情報の漏洩

脅威（過失）	種別
期限切れのプライベート鍵を用いて新たな署名が作成される	その他

(c) 対策の方針

- 有効期間が過ぎたプライベート鍵については更新を期間が切れる前に行い、すみやかに破棄する。
- 有効期間について確認をした上で有効な鍵のみで署名を行う。

(d) 対策手法の例

- 署名アプリケーションにおける有効期間確認および鍵更新機能を実装する
- 登録局側から鍵更新を促すような手順を実装する

4.1.5. 取消し段階

失効したプライベート鍵は新たな署名を作成するために使われることはない。プライベート鍵はすみやかに破棄される。

(a) 処理の内容

関連する情報資産	種別	ロケーション
プライベート鍵	データ	利用者
利用者自身の証明書	データ	利用者
CRL	データ	リポジトリ、リポジトリ—利用者間、利用者
署名アプリケーション	ソフトウェア	利用者
証明書有効性検証ツール	ソフトウェア	利用者
ディレクトリ・ソフトウェア	ソフトウェア	リポジトリ
利用者	エンティティ	利用者
利用者—リポジトリ間	通信路	—

(b) 想定される脅威

脅威（故意）	種別
失効したプライベート鍵を用いて新たな署名を作成する	その他
失効したプライベート鍵を他者に知られる	情報の漏洩

脅威（過失）	種別
失効したプライベート鍵を用いて新たな署名が作成される	その他

(c) 対策の方針

- 失効したプライベート鍵については更新を期間が切れる前に行い、すみやかに破棄する。
- 失効状況について確認をした上で有効な鍵のみで署名を行う。

(d) 対策手法の例

- 署名アプリケーションにおける失効状況の確認および鍵更新機能の実装
- 登録局側から失効後に鍵更新を促すような手順の実装

4.1.6. 破棄段階

有効期間が過ぎたプライベート鍵および失効したプライベート鍵は記録した媒体から消去される。

(a) 処理の内容

関連する情報資産	種別	ロケーション
プライベート鍵	データ	利用者
利用者	エンティティ	利用者

(b) 想定される脅威

脅威（故意）	種別
古いプライベート鍵を用いて新たな署名を作成する	その他
古いプライベート鍵を他者に知られる（例：プライベート鍵の消去が不十分で他者が入手してしまう）	情報の漏洩

脅威（過失）	種別
古いプライベート鍵を用いて新たな署名が作成される	その他

(c) 対策の方針

・ 使用しなくなった古いプライベート鍵はコピーを含めて確実に破棄する。

(d) 対策手法の例

・ 鍵データを論理的・電磁気学的に確実に消去する。（例：記録媒体上に焼付けられた場合を考慮し、0、1、ランダムなビットの上書きを複数回繰り返す。

4.2. ユーザおよび認証局の鍵ペアに係るその他の鍵の管理

4.2.1. 認証局のプライベート鍵の管理

認証局のプライベート鍵の管理について、鍵ライフサイクルを下図に示す。

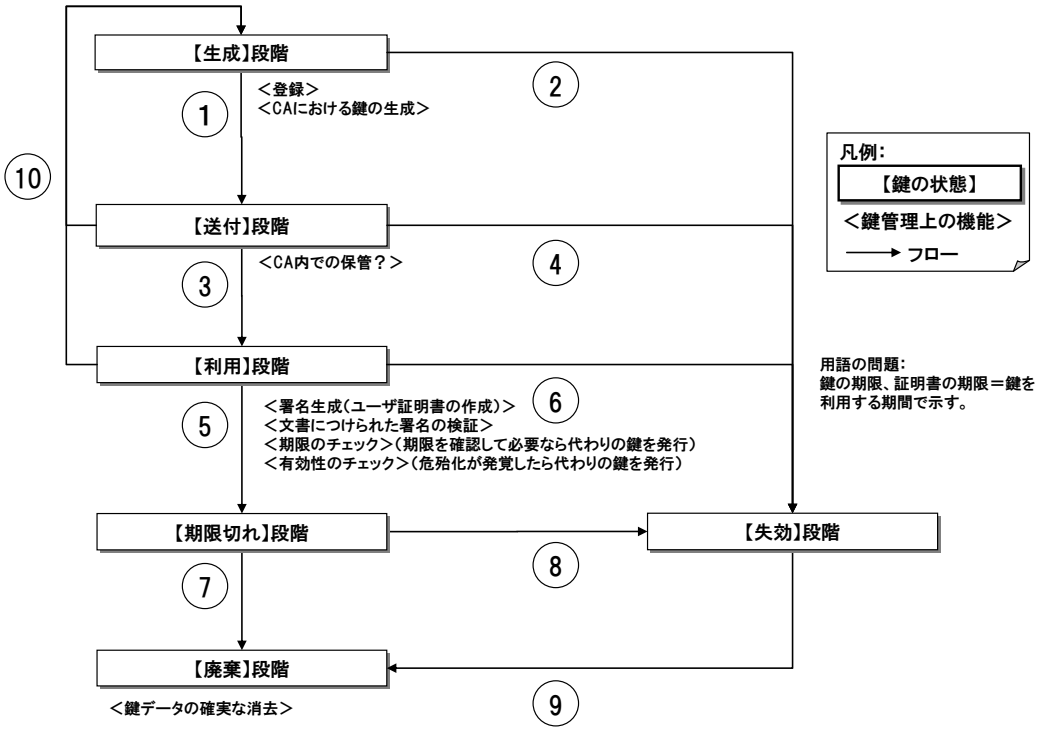

図 4-4　CA の自己署名証明書に係るプライベート鍵のライフサイクル

4.2.2. 利用者の公開鍵の管理

利用者の公開鍵の管理について、鍵のライフサイクルを下図に示す。

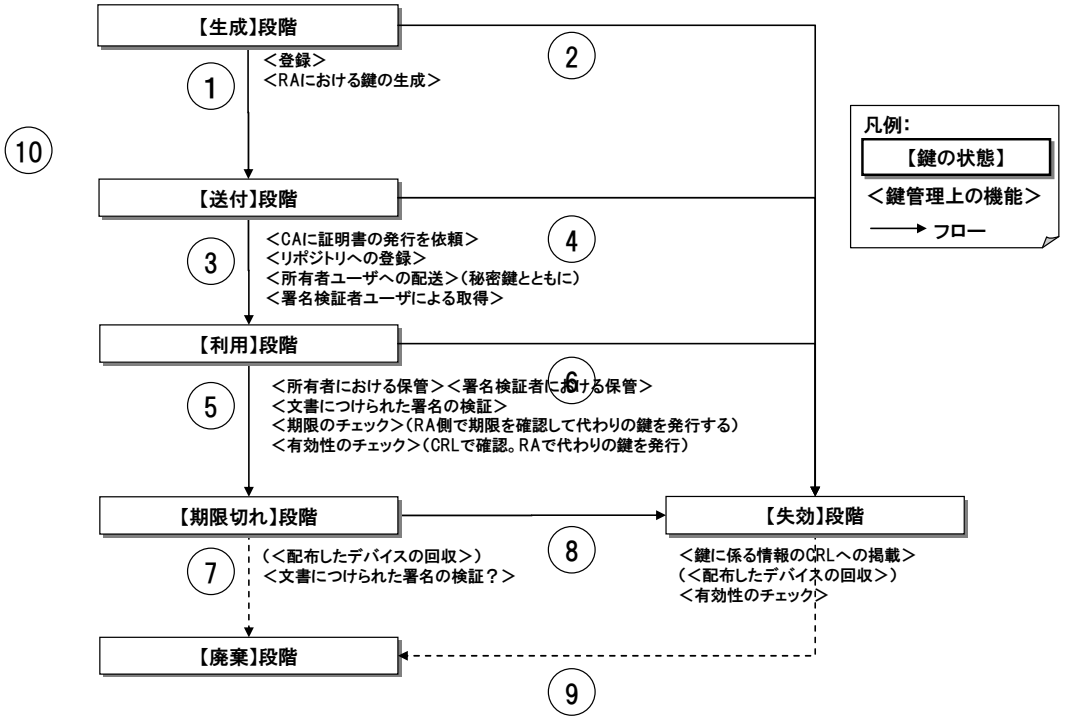

図 4-5　利用者の公開鍵のライフサイクル

4.2.3. 認証局の公開鍵の管理

認証局の公開鍵の管理について、鍵ライフサイクルを下図に示す。

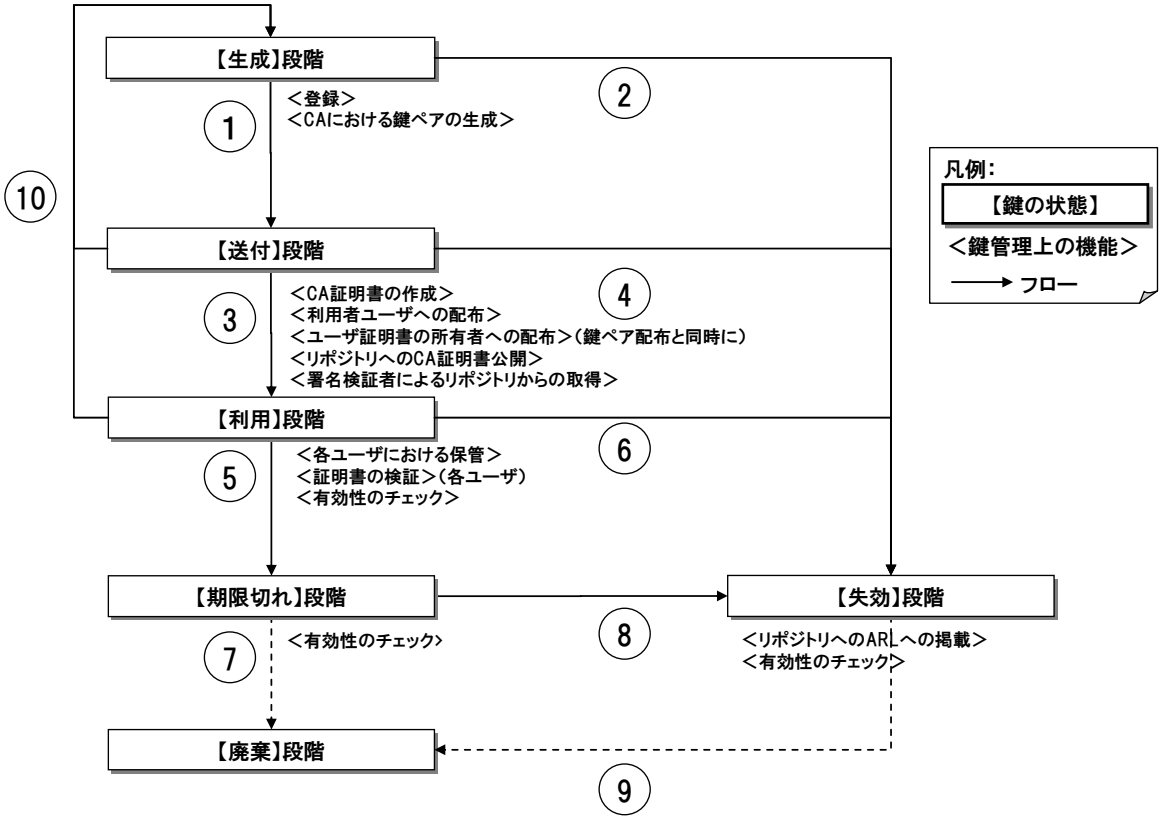

図 4-6　自己署名証明書に係る公開鍵のライフサイクル