2010年度版　リストガイド（鍵管理）

CRYPTREC

2011年06月30日

目 次

1 本文書の位置づけ 1
1.1 文書の目的 . . . 1
1.2 対象とする利用目的 . . . 1
1.3 本文書の構成 . . . 2

2 定義 3

3 公開鍵暗号技術の鍵管理 10
3.1 技術の利用モデル . . . 10
3.2 鍵の生成手順 . . . 10
3.2.1 PKI におけるトラストアンカーの公開鍵の配送 . . . 11
3.2.2 登録局 RA および認証局 CA への申請 . . . 12
3.2.3 一般的な公開鍵の配送 . . . 14
3.2.4 中央サーバ等で生成された鍵ペアの配送 . . . 15
3.3 個別暗号鍵の有効期間の設計指針 . . . 16
3.4 暗号鍵の更新手順 . . . 16
3.4.1 鍵の回復 . . . 16
3.4.2 鍵の変更 . . . 17
3.5 鍵の廃棄手順 . . . 18
3.5.1 鍵の廃棄 . . . 18
3.5.2 鍵の失効 . . . 19
3.6 鍵が漏洩した場合のリスクを低減する方法 . . . 19
3.7 鍵の保存手順 . . . 21
3.7.1 有効期間内の鍵の保存手順 . . . 21
3.7.2 有効期間終了後の鍵の保存手順 . . . 22

4 共通鍵暗号技術の鍵管理 25
4.1 技術の利用モデル . . . 25
4.2 鍵の生成手順 . . . 25
4.2.1 鍵の生成 . . . 25
4.2.2 鍵導出 . . . 26
4.2.3 鍵の配送 . . . 27
4.3 個別鍵の有効期間の設計指針 . . . 28
4.4 暗号鍵の更新手順 . . . 28
4.4.1 鍵の回復 . . . 28
4.4.2 鍵の変更 . . . 29
4.5 個別鍵の廃棄手順 . . . 30
4.5.1 鍵の廃棄 . . . 30
4.5.2 鍵の失効 . . . 30

4.6 鍵が漏洩した場合のリスクを低減する方法 32
4.7 鍵の保存手順 33
4.7.1 有効期間内の鍵の保存手順 33
4.7.2 有効期間終了後の鍵の保存手順 35

5 共通項目 **38**
5.1 鍵を転送する場合の鍵の保護 38
5.1.1 可用性 38
5.1.2 完全性 38
5.1.3 守秘性 39
5.1.4 用途またはアプリケーションとの関係性 40
5.1.5 その他のエンティティとの関係性 40
5.1.6 その他関連情報との関係性 40
5.2 ストレージ上での鍵の保護 40
5.2.1 可用性 40
5.2.2 完全性 41
5.2.3 守秘性 41
5.2.4 用途またはアプリケーションとの関係性 42
5.2.5 その他のエンティティとの関係性 42
5.2.6 その他関連情報との関係性 42

1　本文書の位置づけ

1.1　文書の目的

電子政府推奨暗号[1] とは、総務省及び経済産業省が共同で開催する暗号技術検討会において暗号技術を公募の上、客観的に評価された暗号であり、電子政府における調達の際に推奨される暗号である。各府省庁は情報システムの構築に当たり暗号を利用する場合は、可能な限り、電子政府推奨暗号リストに掲載された暗号の利用を促進することとなっている[2]。

CRYPTREC では、2007 年度以降、「電子政府推奨暗号の利用方法に関するガイドブック」および「リストガイド」を作成し、電子政府推奨暗号リストの適切な利用方法の解説を行っている。リストガイドでは、「電子署名」、「メッセージ認証コード」、「秘匿の暗号利用モード」および「擬似乱数生成器」について、実装レベルの推奨仕様を作成し、公開している。CRYPTREC では、今後もリストガイドを作成・追加していく予定である。

暗号を安全かつ適切に利用するためには、セキュリティパラメータの設定やソフトウェアの設定等を含む、暗号運用上の暗号鍵管理の指針が必要である。米国 NIST においては、SP 800-57 を中心に暗号鍵の管理に関する推奨が規定され、連邦政府内での暗号鍵管理における安全性向上を推進しているところである。我が国でも、「政府機関の情報セキュリティ対策のための統一基準（第 4 版）」（以下、統一基準）において、暗号鍵の『生成』、『有効期限』、『廃棄』、『更新』、『鍵が露呈した場合の対処』の各手順等を具体的に定めることが求められている [統一基準]。

かかる状況を鑑み、統一基準 1.5.2.4 項で策定が求められている暗号鍵の管理手順の各フェーズ（『生成』、『有効期限』、『廃棄』、『更新』、『鍵が露呈した場合の対処』の各手順）について、CRYPTREC の活動内容および米国 NIST800-57 等の情報を集約し、リストガイド（鍵管理）として取り纏めることにより、政府機関内における暗号鍵管理手順の策定の一助となることを目的とする。

1.2　対象とする利用目的

本書の想定読者は、政府機関において電子政府システムの調達を行う政府職員、ならびに、電子政府システムの構築、運用を行う情報システムの開発者および運用者を対象とする。

本書で想定する利用目的は、我が国の政府機関における電子政府システムの調達、ならびに、運用において、暗号鍵の管理に係る『生成』、『有効期限』、『廃棄』、『更新』、『鍵が露呈した場合の対処』等の各手順に関する推奨される考え方ならびに関連する情報提供を行うことを目的とする。

---

[1] 電子政府推奨暗号リスト：http://www.cryptrec.go.jp/images/cryptrec_01.pdf

[2] 各府省の情報システム調達における暗号の利用方針、平成 15 年 2 月 28 日、行政情報システム関係課長連絡会議了承 http://www.cryptrec.go.jp/images/cryptrec_02.pdf

1.3　本文書の構成

本文書では、利用する暗号方式に応じて参照しやすいように公開鍵暗号技術 (3 章) と共通鍵暗号技術 (4 章) に分けて、鍵管理の方法を分けて記述した。第 2 章で、本リストガイドで用いる用語の定義について述べ、第 5 章において、公開鍵暗号及び共通鍵暗号で共通する鍵の管理・保護策について述べている。

2　定義

本書で用いる用語ならびに記号、記法についての定義を述べる。

表 1: 用語の定義

用語	定義
アイデンティティ	個人またはエンティティの特性や個性。個人やエンティティの人物と資格を区別するために用いる。
暗号アルゴリズム	暗号鍵を含む変数を入力として、暗号文を出力するまでの過程を明確に定めた計算方法。
暗号アルゴリズムの利用可能期間	データの暗号化を行うエンティティによって、ある特定の暗号アルゴリズムを利用してもよい期間。
暗号化	ある暗号アルゴリズムおよび鍵を用いて、平文を暗号文に変える処理。
暗号解析	１．データ保護に利用している鍵に関する知識を用いずに、暗号の保護機能を破るために実施する処理。 ２．暗号技術及び暗号技術で保護された情報システムのセキュリティを破ることを試みる数学的な技術の研究。あるアルゴリズムの実装またはそのアルゴリズム自体についてのエラーまたは弱点を探す処理を含む。
暗号鍵（鍵）	暗号アルゴリズムと共に用いるパラメータであり、このパラメータを指定することで暗号処理の方法が決定する。鍵に関する知識を有するエンティティは、この処理を再現したり、逆変換を行うことができるが、鍵を知らないエンティティはこれを行うことができない。例えば、以下のような処理ががこれに該当する。 1. 平文のデータを暗号文に変換する処理。 2. 暗号文のデータを平文に変換する処理。 3. あるデータの電子署名を計算する処理。 4. 電子署名の検証を行う処理。 5. メッセージ認証コードを計算する処理。 5. メッセージ認証コードの検証を行う処理。 7. 鍵および関連パラメータを導出するために用いる共有秘密情報を計算する処理。 単に“ 鍵 ”と表記する場合もある。
暗号鍵および関連パラメータ	鍵に関連して、生成、共有および保持する必要のあるデータ（例えば、鍵や IV など）。
暗号鍵の有効期間	ある特定の鍵の利用権限が与えられている期間、またはあるシステムやアプリケーションの鍵が有効な期間。

表 1: 用語の定義

用語	定義
暗号鍵要素	暗号鍵として同等のセキュリティを有する、少なくとも 2 つ以上のパラメータのうちの 1 つ。これらのパラメータは、利用前に組み合わせて、平文形式の暗号鍵に変換する。
暗号文	暗号化された形のデータ。
暗号モジュール	認定済みの暗号アルゴリズムおよび鍵生成を含む、暗号機能を実現するハードウェア、ソフトウェア、および、ファームウェアの集合体。
安全な通信プロトコル	適切な守秘性、認証およびコンテンツの完全性の保護機能を提供する通信プロトコル。
アーカイブ	アプリケーションで必要とされる期間が終了したのち、長期保管用のストレージにその情報を保管すること。
エンティティ	ある個人、組織、デバイスまたは処理など、行動を行う主体。
解読コスト	ある暗号を解読するために要する計算量。例えば、12MIPS years は、1 秒当たり 100 万命令を処理する能力を有する 1 台のコンピュータで、12 年要することを示す。同じ処理量は、十分な並列化を行えたと仮定すると、同様のコンピュータ 12 台を用いて 1 年で計算できる。
鍵管理実施規定	鍵管理実施規定は、組織構成、責任ある役割（所掌）、および、鍵管理ポリシーに規定される機能における組織の鍵管理に関するルールを詳細に記載した文書または文書群である。
鍵管理ポリシー	鍵管理ポリシーは、組織の鍵管理に関する規程であり、上位組織、責務、標準および推奨に関する管理、組織的な依存関係およびセキュリティポリシーを規定する。
鍵管理用アーカイブ	重要な鍵および関連パラメータを保管するリポジトリ。
鍵導出	1 つ以上の鍵を、共有秘密情報およびその他の情報から導出する処理。
鍵の共有	2 者以上のエンティティで、暗号に関する処理を実施するための鍵を共有する処理。
鍵の移送	正当なエンティティに対して、鍵および関連パラメータを電子的な手段で転送する、または、メディア等に記録して運搬する処理。
鍵の回復	正当なエンティティが、鍵のバックアップまたはアーカイブから、鍵および関連パラメータを取得できるようにする機構または処理。

表 1: 用語の定義

用語	定義
鍵の更新	これまでに利用していた古い鍵を用いて、新たな鍵を生成する処理。
鍵の再生成	これまでに利用していた古い鍵が漏洩する、有効期間が迫る等により、信頼のおけない状態になった場合に、古い鍵の値とは独立した新たな鍵を生成する処理。
鍵の失効	鍵の有効期限が来る前に、鍵および関連パラメータを通常の利用から取り除くように、関係するエンティティに通知する処理。
鍵の廃棄	鍵（および関連パラメータ）を復元が困難な状態にする処理。
鍵の配送	鍵およびその他のパラメータを、当該鍵を所有する、または、生成したエンティティから、その鍵を使用することを意図する別のエンティティへ転送する処理。
鍵の変更	これまで利用していた鍵と同等の機能を発揮するように、別の異なる鍵と置き換える処理。
鍵の保有期間	ある鍵およびその他関連する情報をアーカイブで保有する最低限の時間。
鍵の有効期間	特定の鍵について、その利用が許可されている、または、システムまたはアプリケーションの中で効力を有している期間。
鍵ペア	ある公開鍵と当該公開鍵に対応する秘密鍵のペア。鍵ペアは公開鍵暗号アルゴリズムで用いる。
確定的乱数生成器（DRBG）	シードと呼ばれる初期値によって決定されるビット列を生成するアルゴリズム。DRBG の出力は、統計的に乱数の値と識別不可能である。暗号の DRBG は、シードが既知でない場合に、出力を予測できないという追加の特性を持つ。DRBG は、擬似乱数生成器（PRNG）とも呼ばれる。 確定的擬似乱数生成器または擬似乱数生成器を利用する場合には、2009 年度版リストガイド 6 章を参考に選択することが望ましい。
完全性	不当に情報が改変または消去されていないことを示す特性。データが生成、移送、蓄積されて以後、許可されていない方法で当該データが変更されていないことを示す。
共通鍵暗号アルゴリズム	暗号化および復号の各処理で同じ鍵を用いる暗号アルゴリズム。

表 1: 用語の定義

用語	定義
（共通鍵暗号の）共通鍵	共通鍵暗号アルゴリズムで用いられる暗号鍵で、1つ以上のエンティティと関連付けられており、公開されない鍵。
共有秘密情報	鍵導出関数への入力値として、および、鍵共有方式に利用されて計算される秘密の値。
公開鍵暗号アルゴリズム	公開鍵とそれに対応する秘密鍵を用いる暗号アルゴリズム。公開鍵から秘密鍵を計算することは、計算量的に困難であるという性質を持っている。
公開鍵基盤（PKI）	公開鍵証明書の発行、維持、失効を管理するフレームワーク。
公開鍵証明書	あるエンティティを唯一に識別するデータの集合。そのエンティティの公開鍵、および、エンティティに関するその他の情報を含む場合もある。信頼のおける第三者により署名され、当該エンティティと関連付けられる。証明書に記載される付加的な情報により、その鍵の利用方法と有効期間が規定される。 証明書と略記する場合もある。
（公開鍵ペアの）公開鍵	公開鍵暗号方式とともに用いる暗号鍵。あるエンティティに唯一に関連付けられており、公開される。公開鍵暗号方式では、公開鍵はある秘密鍵に関連付けられている。アルゴリズムに依存して、以下の処理に用いられる。 1. 対応する秘密鍵で署名された電子署名を検証する。 2. データの暗号化を行う。暗号化されたデータは、当該の公開鍵に対応する秘密鍵によって復号する。 3. 共有されたデータの一部を保護する。
（公開鍵ペアの）秘密鍵	公開鍵暗号アルゴリズムとともに用いる鍵。あるエンティティと唯一に関連付けられており、公開されない。公開鍵暗号技術においては、ある公開鍵と秘密鍵は関連付けられている。アルゴリズムによって、秘密鍵は以下に示す処理に用いられる。 1. 対応する公開鍵を算出する。 2. 対応する公開鍵で検証できる電子署名を算出する。 3. 対応する公開鍵で暗号化されたデータを復号する。 4. その他の情報と一緒に用いることで、一般に共有されているデータの一部を保護する。

表 1: 用語の定義

用語	定義
識別子	ある個人、デバイス、組織に関連づけられたビット列。アプリケーションに応じて識別名称や、より抽象的なもの（例えば、IP アドレスやタイムスタンプで構成される文字列）になる。
自己署名証明書	トラストアンカーと呼ばれる信頼の基点となる認証局が発行する証明書。自らの公開鍵に対して、当該公開鍵に対応する署名生成鍵で署名した特別な証明書。自己署名証明書に関する署名は、データの完全性を保護するが、情報の信憑性を保証するものではない。自己署名証明書の信頼性は、それらを配布するために用いられる方法に依存する。
証明書の失効	公開鍵証明書の有効期間が満了する、署名生成鍵が漏洩する等を原因として、公開鍵証明書の信頼性が低下した場合に、当該公開鍵証明書を証明書失効リスト（CRL）等に掲載することにより、当該公開鍵証明書が無効となったことを関係者に通知すること。
署名検証	電子署名を検証するために、電子署名アルゴリズムと署名検証鍵を用いる処理。
署名生成	あるデータに関する電子署名を生成するために、電子署名アルゴリズムおよび署名生成鍵を用いる処理。
所有者	公開鍵暗号方式において、秘密鍵を利用する権限を有するエンティティを示す。
所有証明（POP）	あるエンティティが、公開鍵に関連する秘密鍵を実際に所有することを証明する検証処理。所有者は、定められた方法で秘密鍵を利用することで、秘密鍵を所有していることを示す。
知識分散	暗号鍵を、元の暗号鍵の知識を複数の鍵要素に分割するプロセス。個々の鍵要素は、別々のエンティティによって暗号モジュールに入出力され、元の暗号鍵を再構成するために組み合わされる。
電子署名	公開鍵暗号アルゴリズムにおいて、適切に管理された秘密鍵を用いて電子データに施される署名。以下のサービスを提供する。 1. 発信元の認証 2. データの完全性 3. 署名生成者の否認防止

表 1: 用語の定義

用語	定義
トラストアンカー	証明書の系列において、最上位として検証される認証局の名称および公開鍵。トラストアンカーの公開鍵は、トラストアンカーとなる認証局が発行する証明書を検証することに用いられる。検証処理の安全性は、トラストアンカーの完全性および信憑性に依存する。トラストアンカーは自己署名証明書の形態で配布されることがある。
登録局 (RA)	公開鍵基盤（PKI）において、利用者の真偽確認等を行い、登録を行う機関。RA は、利用者の真偽確認を行った後、認証局に対して証明書の発行を依頼する。
ハッシュ関数	任意長のビット列を固定長のビット列に写像する関数。認定済みハッシュ関数は以下の特性を満たす。 1.（一方向性）特定の出力値に写像される任意の入力値を見つけることが、計算量的に困難であること。 2.（衝突困難性）同じ出力値に写像される任意の異なる 2 つの入力値を見つけることが、計算量的に困難であること。 ハッシュ関数を利用する場合には、電子政府推奨暗号リストから選択することが強く求められる。
ハッシュ値	あるデータ（情報）に対して、ハッシュ関数を適用して得られた値（データ）。
バックアップ	必要に応じて、暗号鍵の有効期期間内に、鍵の回復を可能とするために複製された情報。
（秘密鍵の）保有保証	あるエンティティが公開鍵暗号技術の秘密鍵、および、当該秘密鍵に関連する情報を保有していることの保証。
否認防止	報の完全性と当該本人の行為であることを、第三者が確認できるようにすることで、行為を行った当該本人による否認の脅威を防ぐものである。当該本人のみが知る鍵ペアの秘密鍵を署名生成鍵として使用する電子署名技術により、当該本人の行為であることが証明される。
平文	意味を有し、復号を行わなくてもそのまま理解できるデータ。
不当開示	その情報にアクセスすることを許されていないエンティティに対して、当該情報が開示されることを含むイベント。
認定済み	ある暗号アルゴリズムを用いる場合、以下のいずれか、または、両方を満たす技術または製品を用いること。 1. 暗号アルゴリズムは電子政府推奨暗号を用いること。

表 1: 用語の定義

用語	定義
	2. 暗号モジュールを利用する場合、ISO/IEC 19790 に準拠した認証を受けていること。 なお、ISO/IEC 19790 は国際標準規格であり、米国 NIST における FIPS 140-2(CMVP) などが含まれる。日本においては、Japan Cryptographic Module Validation Program (JCMVP) において、電子政府推奨暗号リスト等に記載される暗号化機能、ハッシュ関数等を実装したハードウェア、ソフトウェアなどで構成される暗号モジュールの第三者認証を行っている。 本文書では、「ISO/IEC 19790 に準拠した認定を取得した」等の表現を用いる場合、FIPS 140-2 等に準拠した認定を受けた場合も含むものとする。
認証	情報の発信元を確認する、または、エンティティの識別情報を決定する処理。
認証局 (CA)	公開鍵基盤（PKI）において、公開鍵証明書の発行および PKI ポリシーを遵守することに責任をもつエンティティ。
復号	ある暗号アルゴリズムおよび鍵を用いて、暗号文を平文に変換する処理。
メッセージ認証コード（MAC）	偶発的または意図的なデータの改変を検知するために、共通鍵暗号方式またはハッシュ関数を用いてデータに付加する暗号的なチェックサム。
乱数シード	確定的乱数生成器（DRBG）を初期化するために用いる秘密の値。
X.509 公開鍵証明書	ユーザ（またはデバイス）の公開鍵およびユーザ（またはデバイス）の名前を、いくつかの他の情報とともに、認証局の電子署名によって偽造できないようにして、ISO/ITU-T の X.509 標準で定義されるフォーマットで符号化された証明書。
X.509 証明書	ISO および ITU-T の X.509 で標準的に定義された 2 つのタイプの証明書。X.509 公開鍵証明書および X.509 属性証明書である。一般的には、X.509 証明書は X.509 公開鍵証明書のことを示す。

3　公開鍵暗号技術の鍵管理

公開鍵暗号技術を利用する場合の鍵の管理について述べる。公開鍵暗号技術を利用する場合には、電子政府推奨暗号リストに記載される公開鍵暗号のカテゴリの中から選択することが強く求めれられる。

3.1　技術の利用モデル

公開鍵暗号技術の用途として、主に以下を挙げることができる。

- 署名
  公開鍵暗号アルゴリズムの鍵ペアの秘密鍵を用いて任意のメッセージに関する電子署名を作成し、対となる公開鍵暗号方式鍵ペアの公開鍵を用いて当該電子署名とメッセージの検証を行う。メッセージに改ざんがなされている場合、これを検知できる。署名用途に用いる秘密鍵は署名生成鍵と呼ばれ、他者に鍵情報を知られないように鍵ペアの所有者が管理する。一方、署名の検証に用いる公開鍵は署名検証鍵と呼ばれ、公開する。

- 認証
  認証とは、情報のやりとりを始めるにあたり、システムを利用するユーザ、または、システムそのものが確かな正当性を持つことを確認する仕組みである。認証を行うことにより、不正侵入やなりすましの脅威を防ぐ。

- 否認防止
  否認防止は、情報の完全性と当該本人の行為であることを、第三者が確認できるようにすることで、行為を行った当該本人による否認の脅威を防ぐものである。当該本人のみが知る鍵ペアの秘密鍵を署名生成鍵として使用する電子署名技術により、当該本人の行為であることが証明される。

3.2　鍵の生成手順

全ての公開鍵ペアは、ISO/IEC 19790 に準拠した認定[3] を受けた暗号モジュール内部、または、予め定められた方法により、生成する必要がある。政府機関においては、使用する電子政府推奨暗号の仕様に基づき、鍵の生成を行う必要がある。

公開鍵暗号方式の鍵および関連パラメータは、電子的方法または手動の方法により配送されてくるか、ローカルに生成される。いずれの場合も 5 章に示す適切な方法を用いて保護する必要がある。

[3]FIPS 140-2 に基づき NIST（米国）が実施する CMVP や、独立行政法人情報処理推進機構が実施する JCMVP などが ISO/IEC 19790 に準拠した暗号モジュールの認定を実施している。両者はそれぞれ、これまでに認定した暗号モジュールのリストを提供している。

個人利用を目的として公開鍵ペア生成した場合、生成された秘密鍵および関連パラメータは、所有者自身以外のサブエンティティに配付されることはなく、5.2 節に示す適切な方法を用いて保護する必要がある。

生成した鍵および関連パラメータを他者又は特定コミュニティ内へ配付する際には、5.1 節に示す方法を用いて保護する必要がある。また、公開鍵暗号方式鍵ペアの秘密鍵を配送する場合には、5.1 節に示す方法を必ず講じる必要がある。

移送により共有された公開鍵ペアの秘密鍵は、5.2 節に示す方法を用いて保護する必要がある。

比較的長期間にわたり利用する公開鍵ペアを生成する場合、これを利用する所有者が生成するか、3.2.4 節に示す方法で中央サーバ等で生成するか、この両者の共同作業により生成するかの、いずれかで行う必要がある。

鍵ペアを生成したエンティティは、秘密鍵を他のエンティティに渡さないようにする必要がある。そして本人による行為の証明及び否認防止をより確実にするために、他者が生成した鍵ペアの秘密鍵ではなく、自身で生成した鍵ペアの秘密鍵を用いる必要がある。

公開鍵（署名検証鍵）とそれに対応する秘密鍵 (署名生成鍵) の場合、鍵の所有者自身が鍵および関連パラメータを生成することが望ましい。これにより、否認防止をより確実なものとする。

生成された鍵ペアは 5.2 節に示す方法に従い、保護する必要がある。

3.2.1 PKI におけるトラストアンカーの公開鍵の配送

認証局の公開鍵は公開鍵認証基盤によるセキュリティの根幹となるものである。トラストアンカー自体は秘密情報ではなく、トラストアンカーが真正であることが PKI の極めて重要な前提条件となる。

1. トラストアンカーの配付は、エンティティが RA または CA に対して証明書発行を要求する際に行うことが望ましい。一般的にトラストアンカーの X.509 公開鍵証明書は自己署名されている。証明書に記された署名検証鍵に対応する署名生成鍵で署名されているため、証明書の型式としては正しくても、トラストアンカーの実在性・真正性は自己署名証明書では担保されない。

2. 自己署名証明書では担保されないトラストアンカーの実在性等の情報をエンティティに提供する必要がある場合、RA または CA はエンティティが証明書発行のために自己の公開鍵を RA 又は CA へ安全に提供する仕組みを用いるなどにより、当該情報を安全に配送することが望ましい。エンティティがユーザ登録を行う際に PIN（個人識別番号）やパスワード等が設定されているのであれば、エンティティからの証明書発行要求時にトラストアンカー情報を提供してもよい。

3.2.2 登録局 RA および認証局 CA への申請

CA から証明書発行を受けるために公開鍵を RA 又は CA へ提供する過程で、RA または CA は、下記の情報が正しいことを鍵の所有者、またはファイアウォール等デバイス向けの場合は、当該機器の管理者から確認する必要がある。また RA 又は CA はこれらエンティティの実在性も確認する必要がある。

1. 鍵の利用目的
2. 公開鍵に紐づいた証明書に記載される諸情報
3. 既知の数学的方式により生成された適切な公開鍵であること
4. 鍵の所有者による当該公開鍵に対応する秘密鍵の確実な保有（所有証明）

一般的に鍵所有者はユーザ登録の過程で特定され、鍵に紐付く正確な諸情報及び正しい鍵を確実に保有することで、鍵を適切に利用することを認識する。実名でない公開鍵所有者名の使用を認め、RA が仮名 (pseudonym) を作成して利用者に割り当てる際には、当該証明書が誰に割り当てられたかを一意に特定できる様にしておく必要がある。

所有証明は、通常、署名検証鍵の登録時に、鍵の所有者が対になる署名生成鍵を所有することの証明を、CA に与えるために用いる。所有証明は、鍵ペアの所有者と考えられるエンティティによって提供される必要がある。所有証明がない場合、CA は、本来の鍵の所有者とは異なるエンティティを公開鍵に結びつける可能性がある。

鍵の所有者であると考えられるエンティティは、指定された鍵の用途を満たす公開鍵ペアの秘密鍵を用いた処理を行うことで、所有証明を提供する必要がある。例えば、鍵ペアが鍵の移送をサポートすることを意図して作成されていたとき、CA は所有者の公開鍵を用いて鍵を暗号化して所有者に渡し、鍵の所有者は自身が所有する秘密鍵で復号を試みる。鍵の所有者が適切に暗号化された鍵データを復号できた場合、鍵データを適切に復号できたということが所有証明となる。この処理を任意のタイミングで実行することにより、鍵の所有者は所有証明を示すことができる。

鍵の共有を行うために用いた鍵ペアの秘密鍵は、証明書発行後の署名生成に用いないようにする必要がある。

ユーザ登録に関して、システムの安全性は、RA または CA への鍵の移送に用いる方法に依存する。様々な方法があり、用途に応じてそれぞれ適切な方法が異なる。いくつかの一般的な方法を以下に例示する。

1. 以下に示す情報と共に公開鍵ペアの公開鍵を公開鍵ペアの秘密鍵の所有者または所有者に承認された代理人により、RA または CA に提供する。
   (a) 鍵の利用目的
   (b) 公開鍵に紐づいた証明書に記載される諸情報
   (c) 既知の数学的方式により生成された適切な公開鍵であること

(d) 鍵の所有者による当該公開鍵に対応する秘密鍵の確実な保有（所有証明）

2. 公開鍵ペアの所有者のアイデンティティは、ユーザ登録の処理の際に、本人が直接、または、代理人によって、CA または RA において確立する。認証コードまたは暗号鍵のような唯一で予期できない情報は、秘密の値として、RA または CA から、このタイミングで所有者に提供される。CA または RA から提供される秘密の値は、証明書の生成に成功したことの確認を受け付けた時点で、3.5 節に示す方法で廃棄する必要がある。RA および CA は、この秘密の値を監査のために廃棄しないで保持する場合、アイデンティティを証明するためにこの秘密の値を利用しないことが強く望まれる。

   署名検証鍵および識別子を登録するために、鍵の所有者の定められたリストを事前に認証する場合には、所有者の識別子が大量に生成される可能性がある。この場合、この秘密の値を維持して保護することは非常に重要となる。この秘密の値の有効期間は制限されるが、公開鍵ペアの秘密鍵の所有者が RA または CA に対して提示できなければならない。RA または CA に対してこの秘密の値を鍵の所有者が提示するには幾分時間がかかるため、2 週間または 3 週間程度の期限を設けることがおそらく合理的である。

   公開鍵ペアの所有者が事前に承認されていない場合、RA または CA は、ユーザが存在することを仮定して識別子を生成する必要がある。この場合、公開鍵ペアの所有者は自身の鍵を生成して、RA または CA に提出するので、秘密の値の有効期間は、より厳しく制限されるだろう。この場合、秘密の値の有効期間は 24 時間程度が合理的だろう。

3. 組織内での運用を除き、オープンなネットワーク上で PKI を利用する場合、公開鍵ペアの秘密鍵の所有者のアイデンティティは、以前に決定された公開鍵ペアの秘密鍵の所有者のアイデンティティを用いて、RA または CA において立証することが望ましい。この行為は、以前に認証された電子署名の署名生成鍵と署名検証鍵のペアに対して、新たな公開鍵証明書のチェーンをつなぐことを要求することにより達成される。例えば、新たな公開鍵証明書を取得するための要求には、認証を受けるべき公開鍵（署名検証鍵）と対になる署名検証鍵の所有者が署名を施す。この要求に対して署名を行う際に用いられる署名生成鍵は、この新たな署名検証鍵を認証する同一の CA によって認証された署名検証鍵に関連付けられていることが望まれる。加えて、この CA は、公開鍵の正当性と、この公開鍵ペアの署名検証鍵の所有者が対応する署名生成鍵を確かに保有しているという保証を得ることが望まれる。

4. 公開鍵およびその用途、利用するパラメータ、またそれらの妥当性を保証する情報、および公開鍵に対応する秘密鍵を確かに所有者が保有しているという保証（保有証明）は、申請に必要な申請者のアイデンティティとともに、RA または CA に提供される。RA または CA は公開鍵ペアの秘密鍵の所有者に関するアイデンティティの検証を信頼できる方法で行う。（例えば、電子署名法

で定められた認定基準を満たす認証事業者への申し込みでは、認証事業者は、住民票の写しや印鑑登録証明書等の利用者申込書類に基づいて厳正な真偽確認を行う)。CA または RA は、証明書発行要求を受け付けたら、固有の予期できない情報を生成し、信頼できる処理を利用して、申請者に送付する。RA または CA から提供された情報を申請者が受け取る前に、この信頼できる処理の中で申請者のアイデンティティの検証を行う（例えば、電子署名法で定められた認定基準を満たす認証事業者への申し込みでは、認証事業者が申請者の秘密鍵を生成する場合、安全性を確保した環境および運用（複数人）でこれを生成し、IC カード等に格納して、電子証明書を利用可能にするための活性化 PIN（パスワード等）とともに、本人限定受取郵便等で送付する。この場合、本人限定受取郵便が信頼できる処理に相当する)。アイデンティティの検証に成功したことを証明するために、公開鍵ペアの秘密鍵の所有者はメッセージ認証コードや暗号鍵などの情報を利用する（同じ例では、利用者は送付された電子証明書を PIN によって活性化し、内容等を確認する)。そして、公開鍵ペアの秘密鍵の所有者に証明書を配送する。信頼できる処理がこの検証に成功したことを証明するために用いた情報は、生成された証明書を受け取った時点で、3.5 節に規定される方法で公開鍵ペアの秘密鍵の所有者によって廃棄する必要がある。(RA または CA は監査目的のために認証子や暗号鍵といった情報を維持するが、アイデンティティの証明のために固有の識別子の利用することを認めないことが強く望まれる)。

RA を含む場合、要求を行っているエンティティから必要となる全ての情報を受信したら、RA は関連する情報を CA に配送する。RA および CA は共に、証明書を発行する前に、署名検証鍵を用いるアルゴリズムを用いて申請された当該署名検証鍵の検査を行う必要がある。CA は公開鍵の検証または検査が終了したことを提示することが強く望まれる。証明書生成後、CA が定める認証局運用規定 (Certificate Practice Statement: CPS) に基づいて、手動または電子的に、RA、公開鍵ペアの秘密鍵の所有者または証明書のリポジトリに証明書を配送する。

3.2.3 一般的な公開鍵の配送

登録局 RA および認証局 CA 以外のエンティティへの鍵の配送には、複数の方法がある。この鍵の配送方法には、以下の事項が含まれる。

1. 公開鍵所有者による公開鍵の手動による配送（例えば、対面による配送など）の場合には、公開鍵を利用する前に、(公開）鍵の利用目的および使用方法、関連パラメータ情報、公開鍵の妥当性、また、受領した公開鍵に対応する秘密鍵を鍵の所有者が所有していること（所有証明)、に関する保証を、鍵の受信者に提供する必要がある。

2. メール等を用いた手動の方法、または、電子的な方法により、公開鍵ペアの秘密鍵の所有者、CA、証明書のリポジトリから配送する場合には、公開鍵を利

用する前に、受信者側で（公開）鍵の利用目的および使用方法、関連パラメータ情報、公開鍵の妥当性、また、受領した公開鍵に対応する秘密鍵を鍵の所有者が所有していること（所有証明）について、確認する必要がある。

3. 認証およびコンテンツの完全性を確認できる通信プロトコルを用いて、公開鍵を配送する場合には、配送される公開鍵は保護される。公開鍵を利用する前に、受信者側で（公開）鍵の利用目的および使用方法、関連パラメータ情報、公開鍵の妥当性、また、受領した公開鍵に対応する秘密鍵を鍵の所有者が所有していること（所有証明）について、確認する必要がある。

3.2.4 中央サーバ等で生成された鍵ペアの配送

公開鍵暗号方式の鍵ペアを組織単位で生成する際は、ISO/IEC 19790 に準拠した認証を取得した暗号モジュール内部で行うか、または、鍵ペアの所有を許可された者への移送を規定した組織の鍵管理に関する規定、または、政府統一基準 1.3.1.4 項 [統一基準] に基づき実施する必要がある[4]。

中央サーバ等で生成された鍵ペアを組織内の申請者に配付する方法では、申請者個々の強固な否認防止実現はできない。申請者個々の否認防止が必要な場合は、各々の申請者が個別に鍵ペアを生成するか、中央サーバ等で鍵ペアを生成し適切な認証または本人確認を行った上で秘密鍵を当該本人に配送することが強く望まれる。

中央のサーバ等で生成した公開鍵ペアの秘密鍵は、その秘密鍵の所有者として指定されたエンティティに対してだけ、配送される必要がある。この秘密鍵を守秘性により保護する必要があり、また、その配送方法の中で、この秘密鍵の受信者を認証する手続きを行う必要がある。

目的とする秘密鍵の所有者に対する鍵ペアの配付は、メールや郵便といったマニュアルの方法または安全な通信プロトコルを用いて行われるだろう。この配送される秘密鍵は、配送過程において、5.1 節に示す方法により、保護する必要がある。

公開鍵ペアの秘密鍵を知識分散を行って配送する場合には、この秘密鍵は、元の秘密鍵と同程度の安全性（ランダム性）を有する複数の鍵要素に分割される必要がある。個々の鍵要素からは、分割される前の秘密鍵に関するいかなる情報も得らないようにする必要がある（例えば、個々の鍵要素は全くランダムに生成されてように見える必要がある）。

秘密鍵と公開鍵のペアを受信したら、その所有者はただちにその公開鍵の妥当性を確認する必要がある。また、所有者は受信した秘密鍵と公開鍵のペアが正しく対応していることを確認する必要がある。

[4]政府統一基準関連項目
1.3.1.4 情報の移送
1.5.2.4(1) 暗号と電子署名に係る規定の整備

3.3 個別暗号鍵の有効期間の設計指針

個別の暗号鍵の有効期間の設計は、鍵の種類、用途、運用環境、利用している暗号アルゴリズムなど、様々な要因によって左右される。表 2 は、[SP 800-57,part1] に示されている個別の暗号鍵の有効期間を示すとともに我が国の電子署名に関連した法制度における証明書の有効期間を示したものである。鍵の種類、用途、運用環境、利用している暗号アルゴリズムに関する攻撃に関する情報などを参考に、システムごとに修正等行う必要がある。

表 2: 公開鍵暗号に関する鍵用途別の有効期間

鍵の種類	用途	SP 800-57 鍵の有効期間	証明書有効期間		
			施行規則 *1	施行令 *2	公的個人 *3
署名生成鍵	署名生成 否認防止	1〜3 年	5 年	1 年	3 年
署名検証鍵	署名検証 否認防止検証	複数年 (鍵サイズに依存)			
認証用秘密鍵	署名を用いた認証	1〜2 年	-	-	-
認証検証用公開鍵	署名を用いた認証の検証	1〜2 年	-	-	-

∗1:電子署名及び認証業務に関する法律施行規則（平成 13 年 3 月 27 日）第 5 条 2 項
http://www.meti.go.jp/policy/netsecurity/digit-sekoukisoku.htm
∗2:電子署名及び認証業務に関する法律施行令（平成 13 年政令第 41 号）第一条
http://www.meti.go.jp/policy/netsecurity/digitalsign-seirei.htm
∗3:公的個人認証ポータルサイト http://www.jpki.go.jp/procedure/period.html

政府機関内の情報システムにおいては、2008 年 4 月に情報セキュリティ政策会議において、「政府機関の情報システムに使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」[5] （以下、移行指針）が決定され、2013 年度末までに移行を完了することとなっている。

3.4 暗号鍵の更新手順

3.4.1 鍵の回復

メモリ上に存在する、または、PC 等のハードディスクに保持された鍵および関連パラメータが、システムクラッシュや電圧の変動等で、紛失または棄損することがある。鍵および関連パラメータの中には、オペレーションを継続するために必要で、簡単に置き換えができない場合がある。何らかのイベントが発生した後に、可能な限り復元できるように、どの鍵をバックアップするのか、分析を行う必要がある。

[5]http://www.nisc.go.jp/active/general/pdf/crypto_pl.pdf

どの鍵を回復する必要があるかの意思決定は、ケースバイケースで行うことが強く望まれる。その意思決定は、以下に基づいて行われることが強く望まれる。

1. 鍵の種類（署名生成鍵、署名検証鍵、認証用秘密鍵、認証用公開鍵）
2. 鍵を利用するアプリケーション (署名生成または検証、認証など)
3. 鍵の所有者 (公開鍵ペアの秘密鍵のように特定のエンティティが所有しているか、公開鍵のように複数のエンティティが所有しているか、など)
4. 通信におけるエンティティの役割 (送信者/受信者、署名生成者/署名検証者など)
5. 当該鍵を入力とする暗号アルゴリズム

暗号鍵の回復に関する意思決定に必要となる要因は、注意深く検討することが強く望まれる。業務の継続性と鍵および関連パラメータが露見するリスクの間には、トレードオフの関係が存在する。現在利用されている公開鍵ペアの秘密鍵が有効期間内にあり、その秘密鍵を回復する必要がある場合には、鍵の変更を行う (3.4.2 節参照)。この操作により、その秘密鍵を用いて保護しているデータが漏洩した場合の範囲を抑制することが可能となる。

3.4.2 鍵の変更

鍵の変更によって、ある鍵を別の鍵に置き換えることで、もともとの鍵と同じ機能を実現する。以下に示すように、いくつかの理由で鍵の変更が必要となる。

1. ある特定の鍵が既に漏洩している場合
2. ある特定の鍵の有効期間が間もなく切れ、失効する場合
3. 任意の与えれた鍵で保護されるデータの数または量を制限したい場合

公開鍵暗号技術では、鍵の変更は、鍵の再生成によって行う。

3.4.2.1 鍵の再生成

古い鍵の値とはまったく関係ない新しい鍵を生成する処理は、鍵の再生成と呼ばれる。鍵の再生成による鍵の変更は、公開鍵ペアを利用する用途やアプリケーションに応じて、3.2 節に示される方法を用いて行う必要がある。鍵の再生成は、ある鍵が漏洩しているが与えられた鍵の再生成の方法が十分な安全性を有している場合に、または、鍵の有効期間が間もなく切れる場合に利用する。

3.5 鍵の廃棄手順

3.5.1 鍵の廃棄

暗号の鍵がコピーされている場合、最終的な廃棄処理に関する注意が必要である。鍵のリスクを最小化するために、公開鍵ペアの秘密鍵の全てのコピーを不要となった時点で消去する必要がある。守秘性による保護が必要であるが暗号化されていない鍵および関連パラメータが記録されているメディアは、物理的または電子的な方法のいずれかを用いて、鍵が復元されないように鍵および関連パラメータに関する全ての痕跡を消去する必要がある。公開鍵ペアの公開鍵は、必要に応じて、保持または廃棄する。

公開鍵暗号の秘密鍵（署名生成鍵および認証用秘密鍵など）を記録した記憶装置毎の廃棄に係る指針を表 3 に示す。

表 3: 公開鍵ペアの秘密鍵の廃棄方法の方針

分類	例	秘密鍵の廃棄方法	記憶媒体の廃棄方法
内蔵電磁的記憶媒体	サーバに内蔵されたハードディスク クライアント PC 内蔵のハードディスク	■ ハードディスク上に保持されている秘密鍵データを抹消する ■ 鍵データが抹消されていることを確認する	■ 内蔵電磁的記憶媒体に格納されている全ての秘密鍵データを抹消する ■ レンタル等、貸与を受けている場合には、電磁的記憶媒体に格納されている全てのデータが抹消されていることを確認後、返却する
外部電磁的記憶媒体	CD-R/DVD-R	■ 記憶媒体を一元管理し、不要となった時点で復元が困難な状態にする ■ 鍵を記憶した記憶媒体が復元困難な状態となったことを確認する	
	CD-RW, DVD/DVD-RW, USB メモリ、メモリカード、外付けハードディスク	■ 記憶媒体を一元管理し、秘密鍵が不要となった時点で、秘密鍵データの復元が困難な状態にする	■ 記憶媒体を一元管理し、不要となった時点で復元が困難な状態にする ■ 鍵を記憶した記憶媒体が復元困難な状態となったことを確認する

3.5.2 鍵の失効

エンティティが組織から離脱した場合や、公開鍵ペアの秘密鍵が漏洩した等の理由により、通常の鍵の有効期間が切れるより前に、鍵および関連パラメータの利用を停止する必要が生じるときがある。この処理は、鍵の失効と呼ばれ、明示的に公開鍵ペアの公開鍵を失効する。失効された公開鍵と対応する秘密鍵も失効する。

鍵の失効は、ある鍵および関連パラメータについて、これ以上の継続的な利用を推奨できないことを利用者に通知することにより実現する。鍵の失効に関する通知は、利用停止されている鍵および関連パラメータ、または、その識別子を、失効対象となる鍵を利用する可能性のある全てのエンティティに通知するか、または、エンティティの方から鍵の有効性を確認させる（Push または Pull）ことにより行われる。この鍵の失効の通知内容には、対象となる鍵および関連パラメータを特定する情報、当該鍵が失効された日時およびその理由を合わせ含むことが強く求められる。

PKI など共通的な基盤 (infrastructure) に鍵が登録されているような場合には、その鍵を利用するエンティティの鍵が失効したとしても、その鍵に関連するエンティティに鍵が失効されたことを直接知らせることが常にできるわけではない。代わりに、鍵を失効したエンティティは、共通的な基盤に鍵を失効されたことを通知する必要がある。共通的な基盤 (infrastructure) は、その鍵および関連パラメータを登録解除する必要がある。

3.6 鍵が漏洩した場合のリスクを低減する方法

暗号を用いて保護された情報は、使用している暗号アルゴリズムが十分な強度を持ち、かつ、鍵が不正に流出していない場合に限り、安全に保護される。鍵の不正な流出は、鍵の保護機構が機能しなくなり、鍵がもはや信頼できなくなった場合に発生する。ある鍵が不正に流出した場合、その鍵の利用の一切を停止し、失効する必要がある。加えて、その流出した鍵を失効する必要がある。不正に流出した鍵を継続して利用することは、その鍵で保護されている情報を処理することに限定される必要がある。この場合、その情報を利用するエンティティは、危険性を十分に認識する必要がある。鍵の有効期間を限定することは、鍵が不正に流出した場合に、その鍵で保護されている情報の量を制限する。単一の鍵で保護する情報の量を制限することと同様に用途ごとに異なる鍵を利用することも、鍵が不正に流出した場合に影響を受ける情報の量を制限することとなる。

公開鍵ペアの秘密鍵が漏洩する確率や、その結果の影響を最小化するために、下記のようないくつかの手段が採られる。

- 公開鍵暗号の秘密鍵が平文の状態である期間を制限する。
- 公開鍵暗号の秘密鍵を平文の状態では人間の目に触れないようにする。
- 公開鍵暗号の秘密鍵が平文の状態であるのを、物理的な容器内など、安全な格納場所に限定する。この物理的な容器とは、秘密鍵を配送するための特別なデバイス、暗号モジュールなどである。

- 秘密鍵およびその関連情報との対応関係が損なわれることを防ぐために、秘密鍵の完全性を保証するための検査を行う。例えば、秘密鍵を暗号化しておくことで、不正な改変や本来対応するべき情報とは別の情報との対応関係を検知することができる。
- 公開鍵暗号の秘密鍵へのアクセスを記録するシステムを構築する。
- MAC や電子署名などの暗号技術を用いて、鍵の完全性を確認する。
- 信頼できるタイムスタンプを利用して、署名付きデータへの信頼性を高める。
- 不要となった時点で、即刻秘密鍵を廃棄する。

漏洩最悪な状況の中には、秘密鍵の漏洩を検知できないという事象がある。このようなケースにおいても対策がないわけではない。鍵管理システムは、一つの鍵が漏洩した際の影響を最小限にとどめるように設計する必要がある。すなわち、流出した鍵によって影響を受ける鍵を可能な限り少なくなるように、システムを設計する必要がある。例えば、単一の秘密鍵を、多数のユーザではなく、例えば、単一の秘密鍵を、多数のユーザではなく、単一のユーザまたは限られた数のユーザだけが利用するように設計することなどがあげられる。大切なのは、致命的な弱点を有するシステム構築を避けることである。

秘密鍵の漏洩に関する再構築プランは、秘密鍵の不正流出といったイベントが発生した際に、イベント発生以前の状態に復旧するためのものである。秘密鍵の漏洩に関する再構築プランを文書化し、組織内の人間が簡単に閲覧できるようにしておくことが強く望まれる。この計画は、鍵管理実施規定に記載されるか、鍵の漏洩に関する再構築プランを単独で作成し、組織の鍵管理実施規定から参照することが強く望まれる。

秘密鍵の漏洩に関する復旧作業は主に組織内の対応作業となるが、単一の秘密鍵の漏洩に関する影響は、そのシステムまたは施設の利用者全体に及ぶ。従って、この復旧作業に係る一連の手続きは、組織内だけでなく利用者も含むことが強く望まれる。例えば、ルート CA の署名生成鍵が漏洩した場合の復旧の場合、その基盤上の全てのユーザは新たなトラストアンカーを取得してインストールする必要がある。

多くの場合、この復旧作業には人手と費用がかかる。これを回避するためにも入念な復旧プランを検討しておくことが必要である。

秘密鍵の漏洩に関する再構築プランには、以下の項目を明確に規定することが強く望まれる。

1. 秘密鍵の漏洩を知らせる担当者（または要員）
2. 回復作業を行う担当者（または要員）
3. 鍵の再生成の方法
4. その他、復旧に係る手順

(a) 装置の実機検査方法

(b) インシデント発生により影響を受ける情報の特定

(c) 署名生成鍵が漏洩したことにより、影響を受ける署名データの特定

(d) 必要であれば、新たな秘密鍵および関連パラメータの配送方法

3.7 鍵の保存手順

3.7.1 有効期間内の鍵の保存手順

有効期間内にある鍵および関連パラメータは、必要に応じてアクセスの行いやすい記憶装置に保持される。このような記憶装置内に存在する間、鍵および関連パラメータは、5.2 節に示される方法で保護する必要がある。

通常、モジュールやデバイス、または、容易にアクセスが可能な記憶装置やメディアに鍵および関連パラメータが記録されている。デバイスまたはモジュールのメモリにロードされていない場合、鍵および関連パラメータは、即座にアクセス可能な記憶装置からロードする。

有効期間内において秘密鍵および関連パラメータを失効する場合（即ち、紛失、または、漏洩等が疑われる場合)、オペレーションの継続性を担保するために、鍵および関連パラメータが即座に復元可能となっていることが求められる。システムのオペレーション分析の結果、鍵および関連パラメータを、何かのインシデントの際に復元可能となるようにする必要があると判断されたなら、鍵および関連パラメータを 3.7.1.2 節に示される方法でバックアップするか、鍵および関連パラメータの再構築が可能となるようにシステムを設計する必要がある。

鍵の有効期間の終了時に、オペレーションを継続するために、鍵の再生成 (3.4.2.1 節参照) を行い、利用可能な状態にする必要がある。古い鍵は、漏洩のリスクを低減するために不要となった時点で 3.5 節に示される方法に基づき即座に破棄することが強く望まれる。

3.7.1.1 ストレージ上での鍵の取扱い

秘密鍵を管理する目的は、標準的な暗号の利用に関して鍵および関連パラメータのオペレーション上の可用性を促進することである。秘密鍵の有効期間内では、鍵および関連パラメータは、デバイスまたはモジュール内（RAM)、および、即座にアクセス可能なストレージ（ハードディスク）で保持されて利用される。

秘密鍵がハードディスクなどのストレージに保持されている場合、5.2 に示す方法で保護する必要がある。

3.7.1.2 バックアップ

公開鍵暗号の鍵および関連パラメータは、ハードウェアの故障、プログラムまたはデータファイルの欠損、システムポリシーやコンフィギュレーションの変更等により、紛失や利用不可能となることがある。オペレーションの継続性を担保するた

めに、ユーザまたはシステム管理者の一方または両方が、鍵および関連パラメータをバックアップ装置から復元できるようにする必要がある。しかしながら、鍵の再生成などを用いることで鍵および関連パラメータのバックアップが行う必要がない場合や、鍵および関連パラメータを保存することなく再構成が可能な場合には、鍵および関連パラメータの漏洩の可能性や関係する情報の漏洩の可能性を減少させるために、これらを保存しないことが望ましいだろう。

公開鍵暗号技術の秘密鍵および関連パラメータの漏洩は、オペレーションの継続性に影響を与える。鍵および関連パラメータが漏洩した事態を想定し、オペレーションの継続性を維持するために、全ての鍵および関連パラメータを再度生成および配付する必要があるかを検討すると共に、どの鍵および関連パラメータが影響を受け、交換しなければならないかを評価する必要がある。他のシステムとは独立しており、安全なストレージメディアによる公開鍵暗号技術の鍵および関連パラメータのバックアップは、鍵の回復 (3.4.1 節参照) を可能とする。バックアップに用いる記憶装置は、通常利用する記憶装置（暗号モジュールやハードディスクなど）に保持されている有効期間内の鍵のコピーを保存する。全ての鍵についてバックアップを行う必要があるわけではない。鍵および関連パラメータをバックアップするストレージには、5.2 節に示される保護が可能なものを用いる。

表 4 に、[SP 800-57,part1] に示される公開鍵暗号技術に関する鍵の種別ごとのバックアップのガイダンスを示す。”可”は、ストレージへのバックアップを許容できることを示しており、必ずしも要求条件を示すわけではない。バックアップに関する最終判断は、鍵および関連パラメータを利用するアプリケーションに基づいてなされることが強く求められる。

少なくとも同じ鍵および関連パラメータが通常用途で利用される間、当該の鍵および関連パラメータのバックアップを行い、これを維持することが強く求められる。暗号鍵および関連パラメータが不要となった場合には、バックアップ用のストレージから削除することが強く求められる。バックアップ用のストレージから鍵および関連パラメータを削除する場合には、3.5 節に示す廃棄手順に基づき、実施する必要がある。

3.7.2 有効期間終了後の鍵の保存手順

公開鍵暗号技術に関連する鍵および関連パラメータの有効期間が終了した後、アーカイブ用の記憶装置に保存されている場合、このアーカイブストレージから鍵および関連パラメータを入手することにより、回復することができる。復元した鍵および関連パラメータは、処理終了後ただちに消去し手元におかずアーカイブストレージにのみ保管される状態を維持する。

公開鍵暗号技術に関連する鍵および関連パラメータのアーカイブは、情報の完全性およびアクセスコントロールを目的として行われる必要がある。情報の完全性は、不当な改変、削除および挿入からアーカイブされた情報を保護するために必要となる。アクセスコントロールは、不当な情報の開示を防ぐために必要となる。アーカイブされた情報は、5.2 節に示される方法で保護される必要がある。公開鍵暗号技術

表 4: 公開鍵暗号技術の鍵の種別ごとのバックアップの可否

鍵の種別	バックアップの可否
署名生成鍵	一般的には不可。認証局 CA の署名鍵などのようにバックアップを許可されるケースもある。バックアップが必要となるケースでは、バックアップする署名鍵は鍵の所有者のコントロール下に置かれている必要がある
署名検証鍵	可。利用可能な公開鍵証明書がいずれかの場所に存在すれば十分である
認証用秘密鍵	アプリケーションで必要とするなら可
認証用公開鍵	可。利用可能な公開鍵証明書がいずれかの場所に存在すれば十分である

に関連する鍵および鍵に関連パラメータがアーカイブとして保管された場合、アーカイブされた日時が判別できるように、しばしばタイムスタンプを用いる。タイムスタンプを用いることで、鍵および関連パラメータが不当に改変された場合には、これを検知することができる。

有効期間が終了したのち、公開鍵暗号技術に関連する鍵および関連パラメータを回復できるようにする必要がある場合、鍵および関連パラメータをアーカイブする必要がある。

公開鍵暗号技術の鍵管理用のアーカイブは、鍵および関連パラメータおよびその他関連する情報の履歴を含むリポジトリである。全ての鍵および関連パラメータが、アーカイブされる必要があるとは限らない。組織のセキュリティプランは、アーカイブする情報のタイプを指定することが強く求められる。

ストレージ内において、アーカイブされた情報は、変更されることがない静的な情報となっているか、新たなアーカイブを暗号化するための鍵を用いて再暗号化する必要がある。アーカイブされたデータは、オペレーションで利用するデータとは区別して保持することが強く望まれる。また、アーカイブされた公開鍵暗号技術の処理に関連する情報の複数のコピーは、物理的に分離された場所に保管することが強く望まれる。アーカイブ用の暗号化鍵で暗号化した重要な情報に対して、アーカイブ用の暗号化鍵をバックアップし、また、アーカイブ用の暗号化鍵の複数のコピーを異なるロケーションで保持する必要があるだろう。

アーカイブを行う際には、公開鍵暗号技術に関連する鍵および関連パラメータは、当該の鍵の有効期間が切れていないことを確認して、アーカイブを行うことが強く望まれる。不要となった鍵は、3.5 節に従い、廃棄する必要がある。

アーカイブされた暗号に関する情報は、5.2 節に示す方法で保護する必要がある。守秘性は、アーカイブ用の暗号化鍵および、別のアーカイブされた鍵、または、アーカイブされた鍵から算出される鍵により、提供される。アーカイブ用の暗号化鍵を用いて暗号化を行う場合、暗号化される鍵および関連パラメータは、古いアーカイブ用の暗号化鍵の有効期間が切れる際に、任意の新たなアーカイブ用の暗号化鍵を

用いて再暗号化する必要がある。鍵および関連パラメータを再暗号化する場合、鍵および関連パラメータの完全性を保持するための値を再計算する必要がある。このことは、多大な負荷となるため、暗号アルゴリズムの強度は、再暗号化の必要性を最小限にするように選択する必要がある。

同様に完全性についても、アーカイブに用いられる完全性保持のための鍵 (アーカイブ専用に用いられる 1 つ以上の認証用秘密鍵、または、署名生成鍵)、または、アーカイブされている別の鍵によって提供される。守秘性による保護は、アーカイブに用いる守秘性保持のための鍵の有効期間が終了する場合には、古い鍵を適用してアーカイブされている情報に関して、新たな完全生を保証するための値を計算する必要がある。

アーカイブ用の鍵は共通鍵、または、公開鍵ペアのいずれかである。単一の鍵で守秘性と完全性の両方を提供できるように特別に設計されている暗号アルゴリズムの場合を除いて、守秘性のために用いる鍵と完全性のために用いる鍵は別々となる必要がある。また、それぞれの鍵は、5.2 節に示す方法に従い、保護する必要がある。

表 9 に、[SP 800-57,part1] に示されている鍵の種別ごとのアーカイブの可否について示す。「アーカイブの可否」における”可”は、アーカイブを行うことが許されることを示す。「保有期間」は、鍵および関連する情報がアーカイブの中に保有されなければならない最低限の時間を示す。

表 5: 鍵の種別ごとのアーカイブの可否

鍵のタイプ	アーカイブの可否	保有期間
署名生成鍵	不可	
署名検証鍵	可	関連する署名生成鍵を用いて署名されたデータの検証が必要でなくなるまで
認証用秘密鍵	不可	
認証用公開鍵	可	対応する認証用秘密鍵でデータの信憑性を検証する必要がなくなるまで

有効期間が切れたのち、公開鍵暗号技術で用いる鍵および関連パラメータは、アーカイブ用のストレージから削除される。

アーカイブされた鍵および関連パラメータから行う鍵の回復は、暗号により保護されているアーカイブデータの復号とチェック (電子署名の検証や MAC の検証) を行う必要がある。鍵の回復により、アーカイブ用のストレージから所望の鍵および関連パラメータを得る。鍵の回復の処理が終了した後すぐに、鍵および関連パラメータは暗号に関連する処理から消去する必要がある。

4　共通鍵暗号技術の鍵管理

共通鍵暗号を利用する場合の鍵の管理について述べる。共通鍵暗号を利用する場合には、電子政府推奨暗号リストに記載される共通鍵暗号のカテゴリの中から選択することが強く求めれられる。

4.1　技術の利用モデル

共通鍵暗号技術の用途として、主に以下を挙げることができる。

- 暗号化
  送信者と受信者で同じ鍵を事前に共有し、その鍵を用いて、送信者はメッセージを暗号化して受信者に送り、受信者は暗号化されたメッセージの復号を行う。

- メッセージ認証コード (MAC:Message Authentication Code)
  送信者と受信者で同じ鍵を事前に共有し、その鍵を用いて、メッセージの偽造、改ざん、破損等を検知し、メッセージの生成元が確かであること、および、データの完全性を保証する。

4.2　鍵の生成手順

データや鍵の暗号化／復号、およびメッセージ認証コードの計算に用いる共通鍵暗号技術の共通鍵は、定められた仕様により決定する必要があり、5 章に示す方法を用いて保護する必要がある。

共通鍵暗号技術の共通鍵の生成および配送については、以下のいずれかで実施する必要がある。

1. 生成した共通鍵を手動で配送する場合には、鍵ペアの公開鍵と同様の方法を用いるか、鍵暗号化鍵を事前に配送または共有する。

2. 鍵共有方式 (生成と配送が 1 つのプロセスで完了) を用いる。

3. **鍵の更新方法**により決定する (4.4 節参照)。

4. マスター鍵から導出する。

4.2.1　鍵の生成

共通鍵暗号技術に用いる個別の共通鍵は、以下のいずれかの方法で生成する必要がある。

- 電子政府推奨暗号リストに掲載される擬似乱数生成器[6] を用いて生成する。

[6]電子政府推奨暗号の仕様書：http://www.cryptrec.go.jp/method.html
2009 年度版　リストガイド　第 6 章：http://www.cryptrec.go.jp/report/c09_guide_final.pdf

- 定められた鍵更新の方法に基づいて、直前の共通鍵から生成する。
- 安全な鍵導出関数[7] を用いてマスター鍵から生成する。

知識分散に関する方法を用いて共通鍵暗号技術に用いる個別の共通鍵を生成する場合、その共通鍵は、複数の鍵要素の形で存在する必要がある。鍵および関連パラメータは、生成後、複数の鍵要素に分割されるか、または、最初から分割された鍵要素として生成される。個々の鍵要素から、鍵要素に分割される前の共通鍵に関して、いかなる情報も得られないようにする必要がある (即ち、個々の鍵要素は、ランダムに生成されたように見えなければならない)。本来の共通鍵を構成するために、n 個のうち k 個 ($k \leq n$) の鍵要素を必要とする場合、どの $k-1$ 個の鍵要素の組み合わせからも、本来の共通鍵に関する推定長以外のいかなる情報も得られないようにする必要がある (例えば、80 ビットの共通鍵を 2 つの 40 ビットの鍵要素に分割するような、単純に共通鍵を数ビットずつ分割するような方法では不十分である)。

全ての鍵は ISO/IEC 19790 に準拠した認定を受けた暗号モジュール内、または、利用する電子政府推奨暗号の仕様に基づき、生成する必要がある。

4.2.2 鍵導出

共通鍵暗号技術の共通鍵は、異なる別の秘密の値から導出される。この秘密の値は、マスター鍵と呼ばれることがある。鍵導出関数は、この秘密の値およびその他の補助情報を入力とし、1 つ以上の鍵を出力する。鍵の変更とは異なり、鍵導出は新たな鍵の利用目的のために使用される。鍵導出関数は、出力された鍵から入力となった秘密の値を求めることができないように、一方向性関数として構成されている必要がある。加えて、出力された複数の鍵のうちの 1 つから、他の鍵の値を導出ができないようにする必要がある。以下に、鍵導出の 4 つのケースについて述べる。

1. 両者が共有している秘密から、共通の鍵を生成するケース
   この方法の安全性は、共有する秘密情報と利用する鍵導出関数に依存する。

2. マスター鍵から個別エンティティの鍵を生成するケース
   マスター鍵、ユーザ ID、および、その他の既知の情報を入力として、エンティティの個別の共通鍵を生成する鍵導出関数を用いて実現する。この処理の安全性は、マスター鍵および鍵導出関数の安全性に依存する。エンティティの中の一つのエンティティがマスター鍵を知った場合、全てのエンティティの共通鍵が生成可能となる。従って、マスター鍵を用いた鍵の導出は、マスター鍵自身と同程度の安全性しかもちえない。マスター鍵が秘密に保持されている限りは、生成される個別の共通鍵は、ランダムに生成された鍵と同じように扱うことができる。

[7] 電子政府推奨暗号の利用方法に関するガイドブック 9 章
http://www.cryptrec.go.jp/report/c07_guide_final_v3.pdf

3. 保有するマスター鍵とエンティティのパスワードから個別エンティティの鍵を生成するケース
   秘密情報であるマスター鍵およびパスワードは、既知である他の情報と共に鍵導出関数に入力し、エンティティ毎に共通鍵が生成される。出力されるエンティティ個別の鍵の安全性は、マスター鍵の安全性、パスワードの安全性、および、鍵導出関数の安全性の強度に依存する。この形態の鍵導出は、しばしば鍵導出に加えてエンティティ認証を行う場合に用いられる。マスター鍵やパスワードが秘密に保たれている限りは、生成される個別の共通鍵はランダムに生成された鍵と同じように扱うことができる。認証サービスの安全性は、パスワードと同程度の安全性である。

4. エンティティのパスワードから個別エンティティの鍵を生成するケース
   この方法は、パスワード、エンティティの ID、およびその他の既知の情報を入力とする鍵導出関数を用いて実現される。この方法は、上述の保有するマスター鍵とパスワードから個別エンティティの鍵を生成するケースとは、マスター鍵を用いないという点で異なる。従って、この処理の安全性は、単純にパスワードと鍵導出関数の処理の安全性に依存する。エンティティのパスワードが知られる、または、推測できる場合には、対応するエンティティの個別鍵を生成することが可能となる。個人が利用可能なパスワードの数は、鍵のバリエーションの数よりも非常に少ないため、この方法で生成される鍵は、ランダムに生成された鍵の安全性よりも低いと考えられる。このケースで生成する鍵は認証を目的として利用し、一般の暗号化に利用しないようにする必要がある。

4.2.3 鍵の配送

4.2.3.1 手動による鍵の配送

手動で共通鍵の配送を行う場合 (つまり、電子的な鍵の転送プロトコルを利用する場合以外)、配送過程を通して、配送される共通鍵を保護する必要がある。配送される共通鍵は、配送過程の全てにおいて暗号化された状態としておくか、物理的な安全策を講じた適切な方法を用いて配送を行う必要がある。もし、多人数で 1 つの共通鍵をコントロールする必要がある場合、知識分散に関する方法を用いてもよい。手動による共通鍵の配送では、以下の事項に関して保証する必要がある。

1. 共通鍵の配送は、認証された送信元からのものであること

2. 平文のままの共通鍵を配送するどのエンティティも、共通鍵を生成したエンティティ、および、共通鍵を受信するエンティティの両方から信頼されているエンティティであること

3. 配送される共通鍵は 5.1 節に示される方法を用いて保護されていること

4. 配送された共通鍵は、認証された受信先が受け取ること

共通鍵暗号技術の共通鍵を暗号化して配送する場合、事前に共有した鍵配送用の共通鍵を用いて暗号化するか、受信者の公開鍵を用いて暗号化する。

知識分散に関する方法を用いる場合、個々の鍵要素を暗号化して配送するか、安全な通信路を用いて別々に配送する必要がある。個々の鍵要素を慎重に取扱うべき情報として、適切な物理的安全策を講じた方法を用いて保護する必要がある。

適切な物理的安全策を講じた方法は、手動による鍵の配送の全てに対して利用することができる。特に配送対象となる個別鍵が平文の形式で配送される場合には、適切な物理的安全策を講じることが重要である。

配送された鍵については、5.2 節に示す方法により、保護する必要がある。

4.2.3.2 電子的な手段による方法

電子的な手段による共通鍵の配送または転送は、インターネットなどの通信路を介して、共通鍵の配送を行う場合に利用する。電子メールなどを用いて共通鍵の配送を行う場合には、予め上述 4.2.3.1 節に示す方法で、共通鍵を暗号化して配送する必要がある。それ以外の場合は、電子政府推奨暗号の鍵共有を用いることが強く求められる。

配送された鍵については、5.2 節に示す方法により、保護する必要がある。

4.3 個別鍵の有効期間の設計指針

個別の暗号鍵の有効期間の設計は、鍵の種類、用途、運用環境、利用している暗号アルゴリズムなど、様々な要因によって左右される。表 6 は、[SP 800-57,part1] に示されている個別の暗号鍵の有効期間を示したものである。鍵の種類、用途、運用環境、利用している暗号アルゴリズムに関する攻撃に関する情報などを参考に、システムごとに修正等行う必要がある。

表 6: 共通鍵暗号技術の個別鍵に関する有効期間

鍵の種類	用途	所有者利用期間 (OUP)	受信者利用期間
認証用共通鍵	MAC	2 年以下	OUP+3 年
暗号化用共通鍵	データ暗号化	2 年以下	OUP+3 年

4.4 暗号鍵の更新手順

4.4.1 鍵の回復

メモリ上に存在する、または、通常の用途に利用するストレージに保持されている共通鍵暗号技術の鍵および関連パラメータは、システムクラッシュや電圧の変動等で、紛失または棄損することがある。共通鍵暗号技術の暗号鍵および関連パラメータの中には、オペレーションを継続するために必要で、簡単に置き換えができない

ものがある。後になって可能な限り回復できるように、どの暗号鍵および関連パラメータをバックアップするのか、検討を行う必要がある。

どの鍵を回復する必要があるかの意思決定は、以下の項目を基にケースバイケースで行う必要がある。

1. 暗号鍵の種類 (データ暗号化用共通鍵など)。
2. 暗号鍵を利用するアプリケーション (インタラクティブな通信、ファイルストレージの暗号化など)。
3. 暗号鍵の所有者 (データ暗号化用共通鍵のように共有されているか、など)
4. 通信におけるエンティティの役割 (送信者、または、受信者)。
5. 暗号鍵が利用されるときに必要なアルゴリズムおよび計算方法。すなわち、鍵の再計算に必要な情報。

鍵の回復に関する意思決定に含まれる要因については、注意深く評価すること必要である。オペレーションの継続性と暗号鍵および関連パラメータが露見するリスクの間にはトレードオフが存在する。ある鍵を回復する必要があると判断し、その鍵がアクティブである (鍵の有効期間内である) 場合には、その鍵で保護しているデータがそれ以上漏洩することを防止するために、鍵の変更を行う (4.4.2)。

4.4.2 鍵の変更

鍵の変更は、元の鍵を、同じ機能を持った別の鍵で置き換えることで同じ機能を実現する。以下に示すように、いくつかの理由で鍵の変更を行う必要性が生じる。

1. ある特定の鍵が既に漏洩している場合
2. ある特定の鍵の有効期間が間もなく失効する場合
3. 任意の与えられた鍵で保護されるデータの量を制限したい場合

鍵の変更は、鍵の再生成、または、鍵の更新を用いて行う。

4.4.2.1 鍵の再生成

古い鍵の値とは完全に独立した新しい鍵を生成する処理は、鍵の再生成と呼ばれる。鍵の再生成による鍵の変更は、4.2 節に示した鍵生成の方法の中の 1 つを用いて行う必要がある。鍵の再生成は、ある鍵が不正に流出しているが、与えられた鍵の再生成の方法が十分に安全と考えられる場合、もしくは、鍵の有効期間が間もなく失効する場合に利用する。

4.4.2.2　鍵の更新

新たな鍵の値が、古い鍵の値に依存している鍵を生成する処理が鍵の更新である。鍵の更新は、一方向性を有する関数を用いて、実現する必要がある。鍵の再生成とは異なり、鍵の更新では、古い鍵を共有するエンティティ間で、新たな情報を交換する必要はない。しかし、将来生成される新たな鍵は保護されていないため、あらかじめ定められた鍵の更新回数を実施した後は、鍵の再生成を用いて新たな鍵を生成する必要がある。鍵の更新は、しばしば、単一の鍵で保護されるデータの量を制限するために用いる。しかし、鍵の更新の処理を漏洩した鍵の変更のために用いてはならない。

4.5　個別鍵の廃棄手順

4.5.1　鍵の廃棄

共通鍵暗号の共通鍵のコピーが作成されている場合、最終的な廃棄処理に関する注意が必要である。漏洩リスクを最小化するために、共通鍵の全てのコピーを、不要となった時点で消去する必要がある。守秘性による保護が必要で暗号化されていない共通鍵暗号技術の鍵および関連するパラメータが記録されているメディアは、物理的または電子的な方法を用いて、鍵が回復できないように全ての痕跡を消去する必要がある。

共通鍵暗号技術の共通鍵を記録した記憶装置毎の廃棄に係る指針を表 7 に示す。

4.5.2　鍵の失効

エンティティが組織から離脱する場合や、共通鍵の漏洩などの理由により、通常の鍵の有効期間が切れるより前に、鍵および関連するパラメータの利用を停止する必要が生じるときがある。この処理は、鍵の失効と呼ばれ、明示的に共通鍵を無効にする。

鍵の失効は、ある鍵および関連パラメータについて、これ以上の継続的な利用を推奨できないことを通知する処理である。鍵の失効では、利用停止の対象となる鍵および関連するパラメータを利用していると考えられる全てのエンティティに通知することにより、または、エンティティが利用している鍵および関連するパラメータの状態 (有効か、無効かなど) を問い合わせることにより、実現する。鍵の失効の通知内容には、鍵および関連するパラメータの完全な識別子、鍵の失効日時およびその理由を含めることが強く望まれる。

鍵の失効に関する詳細は、個別鍵のライフサイクルに関してよく検討することが強く望まれる。もし、2 つのエンティティ間の安全なセッションを通じて通信を行

表 7: 共通鍵暗号技術の共通鍵の廃棄方法の方針

分類	例	共通鍵の廃棄方法	記憶媒体の廃棄方法
内蔵電磁的記憶媒体	サーバに内蔵されたハードディスク クライアントPC内蔵のハードディスク	■ ハードディスク上に保持されている共通鍵データを抹消する ■ 共通鍵データが抹消されていることを確認する	■ 内蔵電磁的記憶媒体に格納されている全ての共通鍵データを抹消する ■ レンタル等、貸与を受けている場合には、電磁的記憶媒体に格納されている全てのデータが抹消されていることを確認後、返却する
外部電磁的記憶媒体	CD-R/DVD-R	■ 記憶媒体を一元管理し、不要となった時点で復元が困難な状態にする ■ 共通鍵を記憶した記憶媒体が復元困難な状態となったことを確認する	
	CD-RW, DVD/DVD-RW, USB メモリ、メモリカード、外付けハードディスク	■ 記憶媒体を一元管理し、共通鍵が不要となった時点で、共通鍵データの復元が困難な状態にする	■ 記憶媒体を一元管理し、不要となった時点で復元が困難な状態にする ■ 共通鍵を記憶した記憶媒体が復元困難な状態となったことを確認する

うように、1 つの鍵を 1 対のペアが共有して利用するような状況では、片方のエンティティが利用している鍵を失効した場合、もう一方のエンティティにそのことを知らせる必要がある。

4.6 鍵が漏洩した場合のリスクを低減する方法

暗号を用いて保護された情報は、使用している暗号アルゴリズムが十分な強度を持ち、かつ、鍵が漏洩していない場合に限り、安全に保護される。鍵の漏洩は、鍵の保護機構が機能しなくなり、もはや信頼できなくなった場合に発生する。ある鍵が漏洩した場合、その鍵の利用の一切を中止する必要がある。加えて、その漏洩した鍵を失効する必要がある。しかしながら、特別に管理された状態で復号や MAC 検証を行うために漏洩した鍵を継続して利用することは、その鍵を利用することで発生するリスクおよび組織のポリシーに基づいて、許容される。漏洩した鍵を継続して利用することは、その鍵で保護されている情報を処理することに限定される必要がある。この場合、鍵を利用するエンティティは、危険性を十分に認識する必要がある。鍵の有効期間を限定することは、鍵が漏洩した場合に、その鍵で保護されている対象を制限する。単一の鍵で保護する情報の量を制限することと同様に用途ごとに異なる鍵を利用することも、鍵が漏洩した場合に影響を受ける情報の量を制限することとなる。

共通鍵の漏洩の発生確率や、その結果の影響を最小化するために、一般に以下のような保護手段を採用する。

- 共通鍵暗号技術の共通鍵が平文の形式である期間を制限する。
- 平文の共通鍵を人間の目に触れないようにする。
- 平文の共通鍵を物理的な容器内に制限する。この物理的な容器とは、鍵の移送用デバイス、暗号モジュールなどである。
- 共通鍵の完全性を保証するための検査、または、当該の共通鍵との関係性が危殆化していない別のデータとの対応関係の検査を行う。例えば、鍵を暗号化しておくことで、暗号化された鍵や関連性の不正な改変を検知し得る。
- 平文形式の共通鍵へのアクセスを記録するシステムを構築する。
- MAC や電子署名を用いて、鍵の完全性を確認するための暗号技術を利用する。
- 不要となった時点で、即刻鍵を廃棄する。

共通鍵の漏洩において最悪の状況の 1 つは、それを検知できないことである。しかし、このようなケースにおいても対策をとることができる。単一の鍵の漏洩が他に与える悪影響を緩和するように鍵管理システム (Key Management System:KMS) を設計することが強く望まれる。すなわち、漏洩漏洩した単一の共通鍵によって影

響を受けるその他の鍵を可能な限り少なくなるように鍵管理システムを設計することが強く望まれる。例えば、単一の共通鍵を、多数のユーザではなく、単一のユーザまたは限られた数のユーザの利用に制限することがあげられる。多くの場合、エンティティ間の認証を行う通信において、単に鍵の保有だけに依拠しないような代替手段をシステムは有している。この目的は、致命的な弱点を有するシステム構築を避けるためである。

鍵の漏洩に関する再構築プランは、鍵漏洩が発生した際に、暗号に係るセキュリティサービスの回復において不可欠な要素である。鍵の漏洩に関する再構築プランを理解しやすいように文書化しておくことが強く望まれる。このプランは、鍵管理実施規定に記載されることになるだろう。もしそうでない場合、鍵管理実施規定において、鍵の漏洩に関する再構築プランを参照していることが強く望まれる。

鍵の漏洩に関する復旧作業は主にローカルな作業であるが、単一の鍵の漏洩に関する影響はそのシステムまたは施設を利用する利用者全体で共有されることになる。従って、この復旧に係る一連の手続きは、関係者全体を含むことが強く望まれる。典型的には、実施することに非常にコストのかかる物理的手段も含まれる。このような高価な手段を避けるために、漏洩を防止するための綿密な予防措置をとるのが望ましい。

鍵の漏洩に関する再構築プランには以下の項目を含めることが強く望まれる。

1. 共通鍵の漏洩を通知すべき担当者（または要員）
2. 回復作業を行う担当者（または要員）
3. 鍵の再生成の方法
4. その他、再構築に係る手続き
   (a) 装置に関する物理的な検査方法
   (b) インシデントが発生した場合に影響を受ける全ての情報の特定
   (c) 単一の署名鍵が漏洩したために MAC の検証をパスするであろう全ての署名データの識別
   (d) 必要であれば、新たな暗号鍵および関連するパラメータの配送方法

4.7 鍵の保存手順

4.7.1 有効期間内の鍵の保存手順

有効期間内に利用される暗号鍵および関連パラメータは、多くの場合、必要に応じて参照して利用できるように準備されている。ストレージ上では、暗号鍵および関連パラメータは、5.2 節に示される方法で保護される必要がある。

通常利用の場合、モジュールやデバイス、または、容易にアクセスが可能なメディアに共通鍵暗号技術の暗号鍵および関連パラメータを保持する。デバイスまたはモ

ジュールのアクティブメモリにロードされていない場合、暗号鍵および関連パラメータは、即座にアクセス可能なストレージからロードする。

有効期間内において、暗号鍵および関連パラメータを利用不可能とする場合（即ち、紛失、または、漏洩等が疑われる場合など)、オペレーションの継続性を担保するために、暗号鍵および関連パラメータが、回復可能であることが求められる。もし、システムのオペレーション分析の結果、暗号鍵および関連パラメータを回復可能とすることが必要と判断されたなら、暗号鍵および関連パラメータを 4.7.1.2 節に示される方法でバックアップするか、暗号鍵および関連パラメータの再構築が可能となるようにシステムを設計する必要がある (4.4 節参照)。

鍵の有効期間の終了時に、オペレーションを継続するために、古い鍵を新しい鍵に置き換えて、利用可能な状態にする必要がある。この処理は、鍵の再生成、鍵の更新、鍵の導出により、実現する。古い鍵は、漏洩のリスクを低減するために、不要となった時点で、即座に、4.5.1 節に示される方法に基づき破棄することが強く望まれる。

4.7.1.1　ストレージ上での鍵の取扱い

鍵管理の目的は、標準的な暗号の利用に関して暗号鍵および関連パラメータの可用性を高めることである。鍵の有効期間内では、暗号鍵および関連パラメータは、デバイスまたはモジュール内（RAM)、および、即座にアクセス可能なストレージ（ハードディスク）で利用できる。

暗号鍵および関連パラメータは、デバイスまたはモジュールに保持され、暗号を用いて情報の保護を行う。通常時は、暗号鍵および関連パラメータを保存するストレージは、または ISO/IEC 19790 に準拠したレベルで保護されなければならない。

暗号鍵および関連パラメータは、鍵の有効期間内では、ローカルハードディスクなどのメディアに保持される。この場合、5.2 節に示す保護策を鍵および関連パラメータに適用する必要がある。

暗号鍵および関連パラメータは、ハードウェアの故障、プログラムまたはデータファイルの欠損、システムポリシーやコンフィギュレーションの変更等により、紛失や利用不可能となることがある。オペレーションの継続性を担保するために、ユーザまたはシステム管理者の一方または両方が、暗号鍵および関連パラメータがバックアップ装置から回復できるようにする必要がある。しかしながら、鍵の再生成などを用いることで暗号鍵および関連パラメータのバックアップが必要でない場合や、保存することなく鍵の回復が可能な場合には、暗号鍵および関連パラメータの漏洩の可能性や暗号処理に関連する情報が漏洩する可能性を低減させるために、暗号鍵および関連パラメータを保存しないことが望ましいかもしれない。

暗号鍵および関連パラメータの漏洩は、オペレーションの継続性に影響を与える。暗号鍵および関連パラメータが漏洩した場合、オペレーションの継続性のために、全ての暗号鍵および関連パラメータを再度生成して共有する必要があるか検討し、その後、どの暗号鍵が影響を受け、変更しなければならないかを検討する。

4.7.1.2　バックアップ

暗号鍵および関連パラメータを独立していて安全なストレージメディアにバックアップすることにより、鍵の回復を可能とする (4.4.1 節参照)。バックアップに用いるストレージは、ある鍵の有効期間内で、通常利用するストレージ（暗号デバイスやモジュール、ハードディスクなど）に記録されている情報のコピーを保存する。全ての鍵がバックアップを行う必要があるわけではない。バックアップを行う暗号鍵および関連パラメータは 5.2 節に示される方法で保護する必要がある。

表 8 に、[SP 800-57,part1] に示される暗号鍵および関連パラメータの種別ごとのバックアップの指針を提示する。”可”は、ストレージへのバックアップを許容できることを示しており、必ずしもバックアップは必須ではない。バックアップの最終判断は、暗号鍵および関連パラメータを利用するアプリケーションに基づいてなされることが強く望まれる。

少なくとも同じ暗号鍵および関連パラメータが通常用途で利用される期間、バックアップにより維持されることが強く望まれる。通常用途で暗号鍵および関連パラメータが不要となった場合には、バックアップ用のストレージから削除することが強く求められる。バックアップ用のストレージから暗号鍵および関連パラメータを削除する場合には、4.5.1 節に示す手順に基づき、廃棄する必要がある。

表 8: 鍵の種別ごとのバックアップの可否 [SP 800-57,part1]

鍵の種別	バックアップの可否
認証用共通鍵	可
暗号化用共通鍵	可
マスター鍵	可

4.7.2　有効期間終了後の鍵の保存手順

通常の暗号鍵および関連パラメータの利用が終了した場合でも、当該の暗号鍵および関連パラメータへのアクセスが求められる場合がある。

暗号鍵および関連パラメータのアーカイブには、情報の完全性およびアクセスコントロールが必要である。情報の完全性は、許可されない改変、削除および挿入からアーカイブされた情報を保護するために必要となる。アクセスコントロールは、許可されない情報の開示を防ぐために必要となる。アーカイブされた情報は、5.2 節に規定される方法で保護される必要がある。鍵および関連パラメータがアーカイブとして保管された場合、保管の日時が記録されるように、しばしばタイムスタンプを用いる。タイムスタンプを用いることで、鍵および関連パラメータが不当に改変された場合には、これを検知することができる。

暗号鍵の有効期間が終了したのち、暗号鍵および関連パラメータを再構成可能なようにする必要がある場合、暗号鍵および関連パラメータをアーカイブするか、再導出できるようにシステムを設計する必要がある。これらの処理は、一般的に鍵の回復として知られる。

鍵管理用のアーカイブは、暗号鍵および関連パラメータおよびその他関連する履歴情報を含むリポジトリである。全ての暗号鍵および関連パラメータが、アーカイブされる必要があるとは限らない。組織のセキュリティプランは、アーカイブする情報の種別を指定する必要がある。

ストレージ内において、アーカイブされた情報は、変更されることがない静的な情報となっているか、新たなアーカイブを暗号化するための鍵を用いて再暗号化される必要がある。アーカイブされたデータは、オペレーションで利用するデータとは区別して保持される必要がある。また、アーカイブされた暗号処理に関連する情報の複数のコピーは、物理的に分離された領域に保管されることが強く望まれる。即ち、暗号鍵管理のアーカイブはバックアップで行う必要がある。アーカイブ用の暗号化鍵で暗号化された重要な情報に対して、アーカイブ用の暗号化鍵をバックアップする必要があり、また、アーカイブ用の暗号化鍵の複数のコピーは異なる場所で保持する必要があるだろう。

アーカイブを行う際には暗号鍵および関連パラメータは、当該の鍵の有効期間が切れるより前に、アーカイブを行う必要がある。不要となった鍵は、4.5.1 節に示す方法に従い、廃棄する必要がある。

アーカイブされた暗号処理に関する情報は、5.2 節に示される方法で保護する必要がある。

守秘性は、アーカイブ用の暗号化鍵および、別のアーカイブされた鍵、または、アーカイブされた鍵から算出される鍵による。アーカイブ用の暗号化鍵を用いて暗号化を行う場合、暗号化対象となる鍵および関連するパラメータは、古いアーカイブ用の暗号化鍵の有効期間が切れる際に、任意の新たなアーカイブ用の暗号化鍵を用いて再暗号化する必要がある。鍵および関連するパラメータを再暗号化する場合、鍵および関連するパラメータの完全性を保持するための値（MAC や電子署名など）は、再計算する必要がある。このことは、著しい負担となるため、暗号アルゴリズムの強度は、再暗号化の必要性を最小限にするように選択する必要がある。

同様に完全性についても、アーカイブに用いる完全性保持のための鍵 (アーカイブ専用に用いられる 1 つ以上の認証用、または、署名用の鍵)、または、アーカイブされている別の鍵によって提供されるだろう。アーカイブに用いる守秘性保持のための鍵の有効期間が終了する場合には、古い鍵を適用してアーカイブされている情報に関して、新たな完全性を保証するための値を計算する必要がある。

アーカイブ用の鍵は共通鍵、または、公開鍵ペアのいずれかである。単一の鍵で守秘性と完全性の両方を提供できるように特別に設計されている暗号アルゴリズムの場合を除いて、守秘性のために用いる鍵と完全性のために用いる鍵は異なる必要がある。また、それぞれの鍵は、5.2 節に示す方法に従い、保護する必要がある。

表 9 に、[SP 800-57,part1] に示されている鍵の種別ごとのアーカイブの可否について示す。「アーカイブの可否」における”可”は、アーカイブを行うことが許されることを示し、アーカイブは必須ではない。「保有期間」は、鍵および関連する情報がアーカイブの中に保有されなければならない最低限の期間を示す。

鍵の有効期間が切れたのち、暗号鍵および関連パラメータは、アーカイブ用のストレージから削除する。また、別の方法では、鍵管理システムが適切に設計されて

表 9: 鍵の種別ごとのアーカイブの可否 [SP 800-57,part1]

鍵の種別	アーカイブの可否	保有期間
認証用共通鍵	可	対象となるデータの認証が不要となるまで
暗号化用の共通鍵	可	暗号化に用いた共通鍵を用いて復号を行う必要がなくなるまで
共通鍵のマスター鍵	可。アーカイブデータに対して別の鍵を生成する必要がある場合。	他の鍵を算出する必要がなくなるまで

いる場合、暗号鍵および関連パラメータを回復することができる。

アーカイブされた暗号鍵および関連パラメータから行う鍵の回復は、暗号により保護されているアーカイブデータの復号とチェック (つまり、電子署名の検証や MAC の検証) を行う必要がある。鍵の回復により、アーカイブ用のストレージから所望の暗号鍵および関連パラメータを得る。鍵の回復の処理が終了した後すぐに、暗号鍵および関連パラメータは暗号に関連する処理から消去する必要がある。

5　共通項目

暗号鍵の有効期間内では、鍵と関連パラメータは、正当な利用者に対して配送処理の中に存在するか、ストレージに保管されているか、のいずれかの状態にある。鍵がいずれの状態にある場合でも、保護方法にはいくつかの選択肢があり、注意深く選択することが強く望まれる。以下に示す鍵の保護方法の実装および関連する鍵の管理によって、実現可能な攻撃が成功しないように十分な安全性を提供しなければならない。

5.1　鍵を転送する場合の鍵の保護

鍵および関連パラメータは、暗号の機能を利用するため、または、バックアップやアーカイブするために配送される。鍵および関連パラメータの転送では、信頼できるエンティティを利用して手動の方法を用いる場合と、通信プロトコルを用いて電子的に転送される場合と、手動および電子的な方法を組み合わて行う場合がある。いくつかの電子的な通信プロトコルでは、プロトコル自体に保護機能を有するものがある。このような保護機能を有するプロトコルを利用する以外の場合、鍵および関連パラメータに関する保護を直接行う。漏洩この保護は、鍵を生成したエンティティの責任により行い、鍵および関連パラメータの保護を取り外すこと、または確認を行うことは、受信者の責任において行う。

5.1.1　可用性

通信においては、ノイズ等の影響や、意図的な改変および紛失などの影響を受ける可能性があり、配送後の鍵および関連パラメータ等の暗号に関連する情報に関する可用性を、暗号技術を利用した方法で保証することはできない。しかしながら、冗長性を有する通信路や複数の通信路、受信を確認したのち情報を削除するシステム、誤り訂正符号、およびその他の暗号に依存しない方法により可用性をサポートすることが可能である。再転送は、フォールバック機構としてだけ利用することが強く望まれる。

5.1.2　完全性

情報の完全性を維持することは、当該情報の改変を検知すること、および、これを防止すること、の両方を含んでいる。改変が検知された場合、当該情報を改変されていない状態に回復する対策を行う。暗号技術を用いた対策は、不当な改変を検知することによく用いられる。情報の配送過程では、鍵および関連パラメータ等を含む情報に対して完全性を与えるために、手動で鍵を配送する場合と通信プロトコルを用いて電子的に配送する場合で、以下に示す異なる方法を用いる必要がある。

1. 手動で鍵を配送する場合：
   鍵および関連パラメータ等を含む情報に巡回符号やMAC、電子署名等を付し、これを受信者に渡す。
   物理的な保護手段を用いて意図的な改変等への対策を行う場合には、MACや電子署名の代わりに巡回符号を用いる。

2. 通信プロトコルを介して電子的に配送する場合:
   鍵および関連パラメータ等を含む情報にMAC、電子署名等を付し、これを受信者に渡す。
   巡回符号を用いるのは適切ではない。

完全性の検証をパスしなかった場合の対応は、その環境ごとに異なる。不適切なエラー処理は、サイドチャネル攻撃といった攻撃を可能とするかもしれない。従って、このようなイベントが発生した場合の対応についてセキュリティポリシーなどに記載する必要がある。例えば、エラーが見つかった場合の対応について、以下のような事項をセキュリティポリシーに記載する。

- その情報を利用しないことが強く望まれる。
- 受信者から、その情報の再送を要求される可能性があるため、予め定められた回数だけ再送を行うように制限することが強く望まれる。
- インシデントに関連した情報をログとして記録し、事後にエラーの発生原因の特定を行う。

5.1.3 守秘性

暗号鍵および関連パラメータを、その配送過程において、秘匿による保護を必要とする場合がある。鍵および関連パラメータに対して、秘匿による保護を行う場合、手動で鍵を配送する場合と通信プロトコルを介して電子的に配送する場合とで、それぞれ異なる方法を用いる必要がある。手動で鍵を配送する場合には、(a)、(b)、(c)のうち、最低1つの方法を用いる必要がある。

1. 手動で鍵を配送する場合

   (a) 鍵および関連パラメータを暗号化する。
   (b) 鍵および関連パラメータを複数の鍵要素に分割する。分割した鍵要素は知識分散に関する方法を用いるため、個々人が全ての鍵要素にアクセスすることができなくなる。
   (c) 適切な物理的、手続き的な保護手段を用いる（例えば、高セキュリティな郵送サービスなど)。

2. 通信プロトコルを介して電子的に配送する場合

   (a) 鍵および関連パラメータを暗号化する。

5.1.4　用途またはアプリケーションとの関係性

暗号鍵および関連パラメータと、その用途またはアプリケーションとの関係性（つまり、どの用途またはどのアプリケーションで当該の鍵を利用するか）について、移送過程において、明確に区別できるようにする。例えば、アプリケーションに入力フォーマットで規定することによって、暗黙のうちに、この関係性を定義するなどの方法を用いる。

5.1.5　その他のエンティティとの関係性

暗号鍵および関連パラメータと正当なエンティティとの関係性について、配送過程において明確に区別できるようにする（例えば、署名の場合は公開鍵証明書等を用いるなど)、または、アプリケーションを用いることによって暗黙のうちに定義する必要がある。

5.1.6　その他関連情報との関係性

暗号鍵と、当該暗号鍵と関連する情報（暗号化鍵または復号鍵と暗号処理に利用する情報）との関係性についても、移送過程において明確に区別できるようにする、または、アプリケーションを用いることによって暗黙のうちに定義する必要がある。

5.2　ストレージ上での鍵の保護

暗号鍵および関連パラメータを、暗号モジュールやハードディスクといったデバイスに蓄積することは、一般的なことである。また、鍵および関連パラメータを、CD-ROM 等の補助記憶装置から読み出すことや、リモートアクセスで呼び出すこと、印刷物といった形態から読み込むこと、などがあるが、これらはバックアップやアーカイブなどでは一般的なことである。

5.2.1　可用性

長期間利用する鍵および関連パラメータは、有効期間内において、ハードディスクなどの記憶装置に保持するとともにバックアップストレージにも記録することが強く望まれる。有効期間が切れた鍵および関連パラメータは、アーカイブ用の記憶装置に保持しておくことが強く望まれる。バックアップ用の記憶装置とアーカイブ用の記憶装置として同じ記憶媒体を用いてもよいし、別々のものを用いてもよい。

5.2.2 完全性

完全性による情報の保護は、その情報が正しいことを保証することと関連する。不当な改変に対する絶対的な保護は不可能である。これを達成する最も良い方法は、改変を防止することができ、改変が行われたことを非常に高い確率で検知することができる対策を講じるとともに、改変が行われたことを検知した場合に、その情報の改変されていない元のデータを再読み込みすることができるようにすることである。

暗号処理に係る全ての情報に対しては、完全性に係る保護策を講じる必要がある。完全性に係る保護策を講じるには、物理的な方法と暗号を用いた方法のいずれか、または両方を用いる必要がある。以下に示す5つの保護策の中から1つ以上の方法を用いる必要がある。

- 物理的保護策
    1. 認定を受けた暗号モジュールまたはオペレーティングシステムを用いて、内部に記録された情報へのアクセスを制限すること。
    2. コンピュータシステムまたは記憶装置を他のシステムと接続しないこと。
    3. コンピュータシステムの外側に物理的に安全な環境（アクセス制限区域など）を構築し、適切なアクセスコントロールを行うこと。
- 暗号技術を用いた保護策
    1. MACや電子署名といった暗号技術を用いた完全性を提供する機構を用いて、蓄積されている情報（暗号鍵および関連パラメータなど）を利用する際に、完全性についての検証を行う。
    2. 所与の暗号処理を行う。受信した情報が正しくない場合には、鍵および関連パラメータが破損、または、改ざん等されている可能性を示している。

エラーが検知された場合には暗号処理に係る情報（鍵および関連パラメータ等）の復元が必要になることに備えて、これらの情報の複数のコピーをバックアップ用の記憶装置やアーカイブ用の記憶装置などに保管し、物理的に隔離された場所で維持管理することが強く望まれる。個々のコピーの完全性を定期的に検査することが強く望まれる。

5.2.3 守秘性

記憶装置に保管されている、公開鍵ペアの秘密鍵や共通鍵暗号の共通鍵などの鍵および関連パラメータに対して、以下に示す方法のいずれかを用いて、保護する必要がある。

1. ISO/IEC 19790に準拠した認定を受けた暗号モジュール内で、電子政府推奨暗号を用いて暗号化する。この場合、暗号化した鍵を復号するコストと暗号化に用いた鍵を入手するコストとを比べて、同程度のコストを要するか、後者の方がコストがかかるようにする必要がある。

2. ISO/IEC 19790 レベル 2 以上の認定を受けた暗号モジュールを用いる。

3. アクセスコントロールの可能なセキュアストレージを用いる。

5.2.4 用途またはアプリケーションとの関係性

暗号鍵および関連パラメータを含む暗号処理に用いる情報は、電子署名や鍵の共有といった所与の暗号的な処理や、特定のアプリケーションと共に用いられる。これらの情報が間違って利用されないという保証を与えるために、保護方策を提供する必要がある。(例えば、鍵および関連パラメータと、その用途またはアプリケーションとの関係性だけでなく、その関係性の完全性を維持するための方策を用いる)。暗号鍵および関連パラメータと、用途およびアプリケーションとの関係性を維持する方法として、暗号処理に用いる情報と、暗号処理を行うモジュールやアプリケーションを分離して管理し、適切なラベル付けなどを用いて、利用時に参照するようにするなどの方法がある。

5.2.5 その他のエンティティとの関係性

暗号鍵および関連パラメータを含む暗号処理に用いる情報の中には別のエンティティ（例えば、鍵の生成を行ったエンティティなど）との正確な関係性を必要とするものがあり、そのような場合、この関係性の完全性を維持管理する必要がある。例えば、情報の暗号化に用いる共通鍵暗号のデータ暗号化用共通鍵や MAC の生成や検証に用いる認証用共通鍵、その共通鍵を共有している、その他のエンティティと関連付けて管理する必要がある。公開鍵暗号の場合、公開鍵証明書などを用いて、鍵ペアの所有者と鍵ペアを正確に関連づける。

鍵および関連パラメータを含む暗号処理に用いる情報は、記憶装置内に存在する間、エンティティまたはアプリケーションと分離して、または、適切なラベル付けを行うことによって、その他エンティティの関連性を保持するようにする必要がある。

5.2.6 その他関連情報との関係性

保護対象である情報とその情報を保護する鍵および関連パラメータ間の関係は維持管理される必要がある。加えて、鍵とその他のパラメータとの関係性も同様に関係性を維持管理する。

これらの関係性の維持管理は、一緒に保管するか、情報間のポインタやリンクを残すというという形によって、実現される。典型的には、鍵と情報とのリンクは、鍵の識別子を基に行い、識別情報やラベルと共に鍵と識別子を保管し、保護対象の情報と鍵の識別子を一緒に記録することで実現できる。これらの関係性は、保護対象となる情報を利用する必要がある限りにおいて、維持管理する必要がある。

参考文献

[FIPS 140-2] National Institute of Standards and Technology, “Security Requirements for Cryptographic Modules,” May, 2001.

[SP 800-57,part1] National Institute of Standards and Technology, “Recommendation for Key Management - Part1:General(Revised),” March, 2007.

[SP 800-56A] National Institute of Standards and Technology, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography,” March, 2007.

[統一基準] 内閣官房情報セキュリティセンター, “政府機関の情報セキュリティ対策のための統一基準（第４版）,” 2009 年 2 月.

[FIPS 186-3] National Institute of Standards and Technology, “Digital Signature Standard,” June, 2009.

[SP 800-56B] National Institute of Standards and Technology, “Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography,” August, 2009.

発行日　2011 年 6 月 30 日　第 1 版第 1 刷
発行者

・〒184-8795
東京都小金井市貫井北四丁目 2 番 1 号
独立行政法人 情報通信研究機構
（ネットワークセキュリティ研究所　セキュリティアーキテクチャ研究室、
セキュリティ基盤研究室）
NATIONAL INSTITUTE OF
INFORMATION AND COMMUNICATIONS TECHNOLOGY
4-2-1 NUKUI-KITAMACHI,KOGANEI
TOKYO,184-8795 JAPAN

・〒113-6591
東京都文京区本駒込二丁目 28 番 8 号
独立行政法人 情報処理推進機構
（セキュリティセンター 暗号グループ）
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
2-28-8 HONKOMAGOME,BUNKYO-KU
TOKYO,113-6591 JAPAN