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
調査報告書

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

電子政府や電子商取引等において、暗号は、セキュリティ上の重要な基盤をなすものである。我が国においては、2003 年に CRYPTREC（Cryptography Research and Evaluation Committees：電子政府推奨暗号の安全性を評価・監視し、暗号モジュール評価基準等の策定を検討するプロジェクト）によって電子政府推奨暗号リストが策定された。また、米国においても NIST（National Institute of Standards and Technology）が、AES（Advanced Encryption Standard：FIPS（Federal Information Processing Standards Publication） 197）をはじめとして、連邦政府で使用する暗号アルゴリズムの仕様を決定している。

他方、暗号アルゴリズムの多くでは、暗号化または復号や署名データ生成等を行うためには秘密の鍵が必要であり、その漏洩によりデータの漏洩や改ざんの可能性が高くなるとともに、紛失によりシステムの可用性に問題が生ずる可能性もある。従って、情報システムやデータの機密性、完全性、可用性等を保証するためには、暗号鍵の管理が重要である。

しかし、米国では NIST SP（Special Publications） 800-57 において暗号鍵の管理ガイドラインが示されているが、我が国においては暗号鍵の管理方法についてのガイドライン等の制定は行われておらず、暗号鍵の管理の重要性が社会に認識されるには至っていない状況にある。

このような状況を鑑み、本調査においては、暗号鍵の管理に対するニーズを把握すると共に、暗号の鍵管理に関する技術動向並びに海外の政策動向等および鍵管理の実態を把握した上で、暗号鍵の具体的な取扱方法を提示する。

2. 暗号の鍵管理に係わる技術動向

暗号鍵の確立・共有に関する研究は、Diffie-Hellman 鍵共有方式が提案されてから盛んに検討され、現在ではパスワードベース鍵交換方式の安全性評価や ID ベース暗号、グループ鍵共有方式など、ユーザにおける鍵管理の簡略化を目指す方式の検討が進んでいる。これらの方式が実用化されるためには、安全性の検討など更なる研究の深化が求められる。また、鍵の更新機能を含む暗号技術としては、Bellare らが提案した Forward Secure Public Key Crytpography などがあるが、鍵の無効化・廃棄についてはほぼ検討がなされていないといえる。

2.1. パスワードベース鍵交換プロトコル

2.1.1. 概要

パスワードベース鍵交換プロトコルは、クライアントおよびサーバの 2 者間で暗号通信を行う際のセッション鍵を共有するために、パスワードを用いてセッション鍵を共有するためのプロトコルである。ここでパスワードは、人間が記憶可能であること等の理由から、比較的少ないパスワード候補（辞書）の中から選ばれることとなるため、クライアントおよびサーバ間でプロトコルが実行されていない状態（オフライン）でも、攻撃者はこの辞書に含まれるすべてのパスワード候補をしらみつぶしに入力していくことで、なりすましが可能であるところにポイントがある。ここで、クライアントとサーバ間でプロトコルが実行されている際（オンライン）には、攻撃者は通信されている情報等を取得できると考えるため、オフラインのときよりも多くの情報を攻撃に利用することができる。このとき、オンラインでの攻撃者の優位性がオフラインのときと比較して同程度となるプロトコルを安全と考える。

2.1.2. 研究動向

パスワードベース鍵交換プロトコルでは、Bellare らが 2000 年に発表したモデル[1]の上で安全性を証明したプロトコルが多数発表されている。特に安全性証明においては、プロトコルを等価なゲームに変換し、各ゲームでの安全性の確率的変化を変化を比較するゲーム変換証明が用いたものがおおい[2,3,4,5,6]。また、これらの安全性証明では、ランダムオラク

[1] Mihir Bellare, David Pointcheval, Phillip Rogaway, “Authenticated Key Exchange Secure Against Dictionary Attacks”, Advances in Cryptology—Eurocrypt ’00, LNCS 1807, Springer-Verlag, 2000.
[2] Jonathan Katz and Rafail Ostrovsky and Moti Yung, “Efficient Password-Authenticated Key Exchange Using Human-Memorable Passwords”, Advances in Cryptology -- EUROCRYPT-2001, LNCS 2045, 2001.
[3] Michel Abdalla and David Pointcheval, "Simple Password-Based Encrypted Key Exchange Protocols", Topics in Cryptology -CT-RSA 2005, LNCS 3376, 2005.
[4] Michel Abdalla and Oliver Chevassut and David Pointcheval, "One-time Verifier-based Encrypted Key Exchange", PKC2005, LNCS 3386, 2005.

ルモデルやイデアルサイファーモデル等、理想的な仮定をおいた証明も多い。

また、パスワードベース鍵交換プロトコルにおいて匿名性を有する方式も提案されている[7,8]、その分析論文も公表されている[9]。

2.2. グループ鍵共有プロトコル

2.2.1. 概要

グループ鍵共有プロトコルとは、三者間以上のパーティで秘密の通信を行うなどの目的のために、秘密の値(セッション鍵) を共有するためのプロトコルである。特に二者間の場合と異なるのは、鍵交換を行おうとするグループの中に不正者が存在するかも知れないと考える点、および、グループの参加者が通信の途中で参加してきたり退場したりする動的なケースを考える点が異なる。

グループ鍵共有のアプリケーションとしては、ビデオ会議等をあげることができる。

2.2.2. 研究動向

Bresson、Chevassut, Pointcheval、Quisuater は、グループ鍵共有プロトコルにおいて、識別困難性(indistinguishability)に基づくモデルを提案し、Diffie-Hellman ベースの認証機能付の鍵交換プロトコルを提案した[10]。

Bresson, Chevassut, Pointcheval は、鍵共有を行う参加者が、いつでもグループに加わったり、グループから退場したりできる動的なケースを踏まえたプロトコルを提案した[11,12,13]。

---

[5] Emmanuel Bresson and Olivier Chevassut and David Pointcheval, "New security results on encrypted key exchange", PKC2004: 7th International Workshop on Theory and Practice in Public Key Cryptography, LNCS 2947, 2004.

[6] Dario Catalano and David Pointcheval and Thomas Porin, "Trapdoor Hard-to-Invert Group Isomorphisms and Their Application to Password-based Authentication", Journal of Cryptology, vol.20, no. 1, 2007.

[7] D. Q. Viet, A. Yamamura, and H. Tanaka. Anonymous Password-Based Authenticated Key Exchange. In Proc. of INDOCRYPT 2005, LNCS 3797, pages 244-257. Springer-Verlag, 2005.

[8] D. Q. Viet, A. Yamamura, and H. Tanaka. Anonymous Password-Based Authenticated Key Exchange.In Proc. of the 2006 Symposium on Cryptography and Information Security (SCIS2006), 3D3-4, January 2006.

[9] SeongHan Shin, Kazukuni Kobara, Hideki Imai, A Secure Threshold Anonymous Password-Authenticated Key Exchange Protocol, In Proc. of the 2007 Symposium on Cryptography and Information Security (SCIS2007), 2D3-1, January 2007.

[10] E.Bresson, O.Chevassut, D.Pointcheval and J.J.Quisquater, “Provably authenticated group Diffie-Hellman key exchange”, Proc. 8th ACM Conference on Computer and Communication Security, pp.255-264, ACM Press, November 2001.

[11] E.Presson, O.Chevassut and D.Pointcheval, “Provably authenticated group Diffie-Hellman key exchange – The dynamic case”, In Advances in Cryptology – ASIACRYPT 2001, LNCS 2248, pp.290-390, Springer-Verlag, December 2002.

[12] E.Bresson, O.chevassut and D.Pointcheval, “Dynamic group Diffie-Hellman key exchange under standard assumptions”, In Advances in Cryptology—EUROCRYPT 2002, LNCS 2332, pp.321—336, Springer-Verlag, April/May 2002.

グループ鍵共有について、UC フレームワーク上での定式化を Katz、Shin が行っている[14]。Katz らが与えた定式化では、グループ内部の不正者の成りすましを定義し、これにより、これまで提案されてきた内部不正者が行う攻撃を網羅的に定義した。また、認証機能付鍵交換(Atuhetnicated Key Exchange : AKE)を、UC 安全を満たすグループ鍵交換プロトコルに変換するコンパイラも同時に提案している。

Ota, Yoneyama, Kiyomoto, Tanaka, Ohta は、デジタル署名を利用せず、MAC（Message Authentication Code, メッセージ識別子）を用いた、動的ケースを考慮したグループ鍵共有プロトコルを提案している[15]。

清藤、二井、四方、松本は、信頼できる第三者機関（Trusted Authority: TA）を仮定することなく、Multirender Atuhentication code（MRA-code）のモデルの下で情報理論的安全性を保有し、メンバーの中の特定の検証者の秘密鍵を無効化できる方式を提案している[16]。

---

[13] E.Bresson, O.Chevassut and D.Pointcheval, “Provably secure authenticated group Diffie-Hellman key exchange”, ACM Transaction on Information and System Security, vol.10, no.3, ACM Press, July 2007.

[14] Jonathan Katz and Ji Sun Shin, Modeling Insider Attacks on Group Key-Exchange Protocols, ACM CCCS 2005.

[15] Haruki Ota, Kazuki Yoneyama, Shinsaku Kiyomoto, Toshiaki Tanaka, Kazuo Ohta, “Provably Secure Authenticated Group Key Exchange without PKI”, SCIS2008, 1E1-3, January 2008.

[16] 清藤武暢、二井将太、四方順司、松本勉、“メンバーの秘密鍵を無効化できる情報理論的に安全な認証方式について”、SCIS2008、1E1-5、January 2008。

2.3. プロキシ暗号[17, 18]

2.3.1. 概要

プロキシ暗号は、Alice が Charley の公開鍵で暗号化したメッセージを、Charley の秘密鍵ではなく、Bob の秘密鍵で復号できるようにプロキシが変換するプロトコルである。この際、プロキシは、Charley の公開鍵と Bob の公開鍵から生成されるプロキシ鍵を持ち、暗号文の変換を行うのみで、Charley および Bob の秘密鍵を所有することなく、また、復号することもできない（図 2-1）。

このプロキシ暗号は、署名にも拡張される。プロキシは、Alice の署名検証鍵と Bob の署名検証鍵から生成されたプロキシ鍵で、Bob が生成した署名を Alice の署名に変換する。この際、プロキシは、Bob の署名を Alice の署名に変換する（または、Alice の署名を Bob の署名に変換する）のみで、他の人の署名に変換することはできない（図 2-2）。

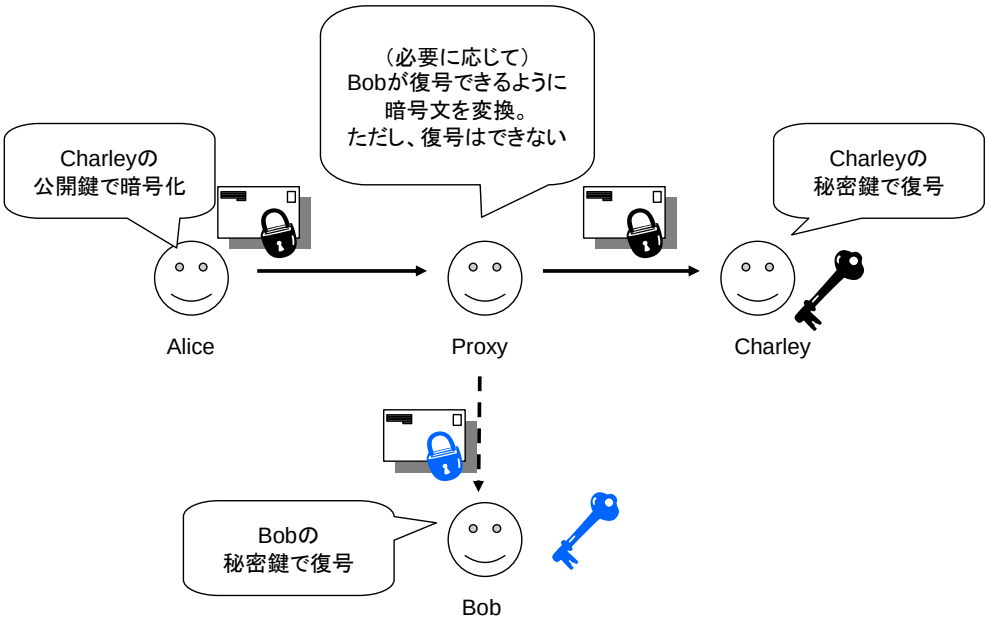


図 2-1 プロキシ暗号（暗号化）

[17] Y. dodis, and A. Ivan, “Proxy cryptography revisited.” In Proceedings of the Tenth Network and Distributed System Security Symposium, February 2003

[18] G, Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage” full version accepted to appear in ACM Transaction on Information and System Security(TISSEC) Also in Cryptology eprint Archive, Report 2005/028

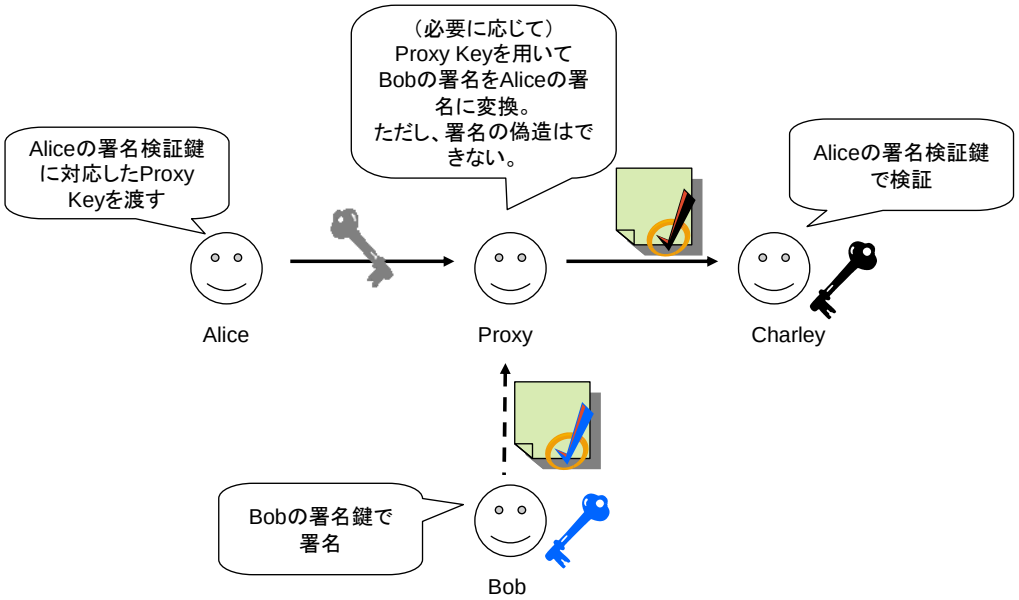


図 2-2 プロキシ暗号（署名）

プロキシ暗号のアプリケーションとしては以下をあげることができる。

- 鍵供託
- 復号鍵の紛失対策
- 代理署名

2.3.2. 研究動向

プロキシ暗号化の概念は Blaz、Strauss により提案された[19]。これに続き、Ivan、Dodis によりプロキシ暗号化の概念の拡張が行われ、識別困難性（indistinguishability）および偽造困難性（unforgeability）を保証するプロキシ暗号化方式が提案された[20]。Ivan、Dodis の提案では、El Gamal 暗号方式、RSA 暗号方式、ID ベース暗号（2.4節参照）、RSA-Hash 署名方式を利用した方式が示されている。

[19] Matt Braze, Martin Strauss, “Atomic Proxy Cryptography”, Eurocrypt 98, 1998.
[20] Anca Ivan, Yevgeniy Dodis, “Proxy Cryptography Revised”, Network and Distributed System Security Symposium (NDSS), February 2003.

2.4. ID ベース暗号

2.4.1. 概要

ID ベース暗号（Identity-Based Encryption:IBE）は、暗号鍵として任意の文字列を用いることができるため、ユーザ ID 等を暗号化鍵として利用可能な暗号システムである。

ID ベース暗号では、Bob の秘密鍵を生成するためのマスターキーをもつ PKG（Private Key Generator）が存在する。Alice は ID などの任意の文字列を用いてメッセージを暗号化し、Bob に送付する。Bob は ID を用いて PKG に問い合わせを行い、PKG から秘密鍵を受け取る。Bob は、受信した暗号文を、PKG から受領した秘密鍵を用いて復号する（図 2-3）。

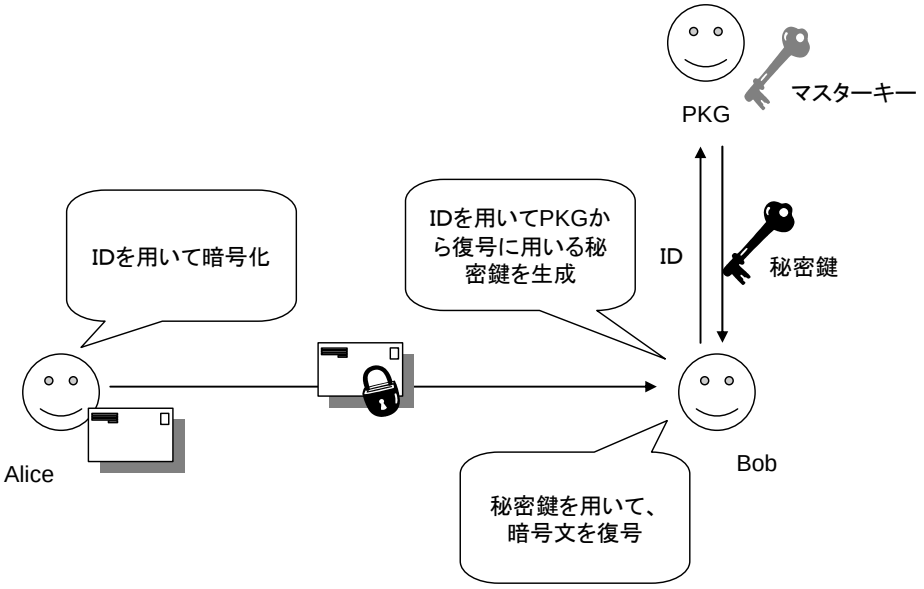


図 2-3 ID ベース暗号

ID ベース暗号は電子署名としても利用できる。署名を生成する Bob は、ID を用いて PKG から秘密鍵を得たのち、ID を公開する。Bob は秘密鍵を用いてメッセージに対応する署名を生成する。Alice は、署名付メッセージを取得した後、公開されている ID を用いて、書名の検証を行う（図 2-4）。ID ベースの署名では、ID 等に失効情報等を含めることが可能であるため、PKI における証明書の管理が軽減できるという利点がある。

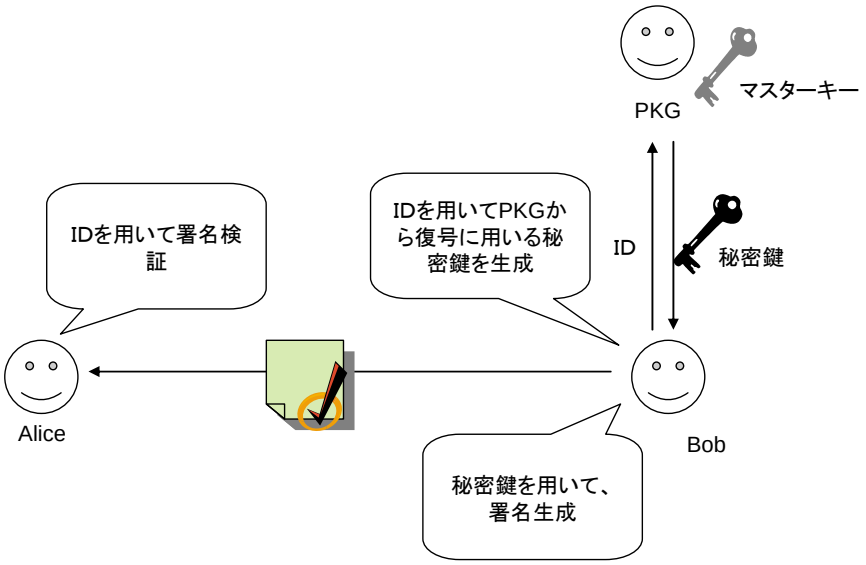


図 2-4　ID ベース署名

ID ベース暗号のアプリケーションとして、以下をあげることができる

- 有効期間情報を含めた公開鍵の管理
- 鍵供託
- 鍵の紛失対策

2.4.2. 研究動向

ID ベース暗号に関する概念は、1984 年に Shamir が提案したのがはじめである[21]。

楕円曲線上での Weil Paring を用いた ID ベースの暗号方式は、Boneh、Franklin によって提案された[22]。また、Cocks によって素因数分解の困難さに依拠した問題の下で、安全性が証明されたスキームも提案された[23]。しかし、これらのスキームは、ランダムオラクルモデルを仮定した下での証明となっていたため、以後ランダムオラクルモデルを仮定しない方式が提案されている。Canetti, Halevi, Katz は従来の ID ベース暗号の安全性を緩めることで、ランダムオラクルモデルを仮定しないで安全性が証明可能な方式を提案している[24]。また、Boneh and Boyen は、ランダムオラクルモデルを仮定せず、selective-ID

[21] Adi Ahamir, “Identity-based cryptosystems and signature schmes”, in Advances in Cryptology—Crypto ’84, LNCS 196, Springer-Verlag, pp.47—53, 1984.
[22] Dan Boneh and Matthew Franklin, “Identity-Based Encryption from Weil Pairing”, SIAM Journal of Computing, vol.32, No.3, pp.586—615, 2003.
[23] Clifford Cocks, “An identity based encryption scheme based on quadratic residues”, In Proceeding of the 8th IMA International Conference on Cryptography and Coding, 2001.
[24] Ran Canetti, Shai Halevi and Jonathan Katz, “A forward-secure public-key encryption scheme”, In Advances in Cryptology—EUROCRYPT 2003, LNCS 2656, Springer-Verlag, 2003.

の安全性証明を持つ２つの方式を提案している[25]。また、Boyen and Waters は、ランダムオラクルモデルを用いないで安全性証明を持つ匿名階層型 ID ベース暗号方式を提案している[26]。

2.5. まとめ

パスワードベース鍵共有、グループ鍵共有、ID ベース暗号、プロキシ暗号について調査した。

暗号鍵の管理に関する新たな技術が実用化されると、暗号の利便性は向上するといえる。しかし、これらの技術が実用化されるためには、十分な安全性の検討が必要である。また、鍵の更新や廃棄といったフェーズに関する研究はあまり進んでいないといえる。

従って、今後も学会等の動向を調査すると共に、ID ベース暗号等の新技術の研究の深化をはかるべきである。

[25] Dan Boneh and Xavier Boyen, “Effiecient selective-ID secure identity based encryption without random oracles”, In Advances in Cryptology—EUROCRYPT 2004, LNCS 3027, pp.223—238, Springer-Verlag, 2004.

[26] Xavier Boyen, Brent Waters, “Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles)”, CRYPTO 2006, LNCS 4117, Springer-Verlag, 2006.

3. 暗号の鍵管理に係わる海外動向

3. 1. 米国 NIST

3. 1. 1. SP 800-21 Guideline for Implementing Cryptography In Federal Government (Second Edition)[27]

米国政府内部において、重要性が高いが、機密扱いにはされていない情報の保護を目的とした暗号の選択について述べられている。特に、FIPS（Federal Information Processing statndards）、SP（Special Publication）シリーズを中心に、暗号の選択に関してそのガイドとなるように構成されている。

鍵管理に関して、以下のガイドラインが述べられている（同様の記述は SP 800-57 Section 3.6 にもある）。

- 暗号鍵を安全に取り扱うことの重要性をユーザ自身が理解し、その責任を負うこと
- 危殆化（または鍵の漏洩）についての準備を行うこと
- 認定または認証された暗号アルゴリズムおよび暗号モジュールを使用すること
- 米国政府システムにおいては、米国政府職員によって集中的に、暗号鍵の記録、システムコンポーネントの制御が実施されること
- SP 800-57 に基づく鍵管理が実施されること

[27] http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf

3.1.2. SP 800-56A Recommendation for Pair-wise Key Establishment Schemes Using Discrete Logarithm Crytpography[28]

本推奨事項では、*Accredited Standards Committee (ASC) X9, Inc.*が開発した標準、*ANS X9.42 (Agreement of Symmetric Keys Using Discrete Logarithm Cryptography)*と *ANS X9.63 (Key Agreement and Key Transport Using Elliptic Curve Cryptography)* に基づく、離散対数暗号を使用した鍵確立方法を規定する。SP 800-57 とともに使用するとともに、FIPS 140-2 検証済みモジュールの非対称アルゴリズムを使用して鍵確立するのに十分な情報を提供する目的とし、鍵確立に関連した様々なプロセス（ドメインパラメータの生成プロセス、共有秘密から秘密鍵関連情報を取得するプロセスを含む）を規定する。

[28] Elaine Barker, Don Johnson, and Miles Smid, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)”, NIST Special Publication 800-56A, March 2007.

3. 1. 3. SP 800-57 Recommendation for Key Management[29]

暗号メカニズムを選択し、使用する際に適切な判断ができるように、背景となる情報を提供し、その枠組みを構築するために、基本的なガイダンスらその内容を拡大したものである。

本推奨書は、3 部から構成される暗号鍵管理のガイダンスである。第 1 部は、暗号鍵材料管理の総合的なガイダンスと適切な事例について記載する。第 2 部では、米国政府機関の方針に関するガイダンスおよびセキュリティ計画の要件について記載する。最後に第 3 部は、現行システムの暗号機能使用する際のガイダンスとなる。

以下に NIST SP 800-57 part 1 に示された鍵の分類を示す。

表 3-1 SP 800-57 における暗号鍵の分類

分類	説明	使用目的（鍵が提供するサービス）
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
認証用共通鍵 (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共通鍵。	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／復号用共通鍵 （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共通鍵。	機密性
鍵暗号化用共通鍵 （Symmetric key wrapping key）	他の暗号鍵を暗号化するために用いられる共通鍵暗号アルゴリズムの共通鍵。	鍵管理のサポート
乱数生成用鍵 （Symmetric and asymmetric	乱数を生成するために用いられる鍵。	鍵管理のサポート

[29] Elaine Barker, William Barker, William Burr, William Polk, and Miles Smid, “Recommendation for Key Management-Part1:General(Rivised)”, NIST Special Publication 800-57, March 2007. http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf

RNG key）		
マスター共通鍵 （Symmetric master key）	他の共通鍵を派生するために用いられる共通鍵暗号アルゴリズムの共通鍵。 （データ暗号化用共通鍵、鍵暗号化用共通鍵、あるいは認証用共通鍵が作られる）	鍵管理のサポート
鍵配送用プライベート鍵 （Private key transport key）	対になる鍵配送用公開鍵により暗号化された鍵(*1)を復号するために用いられる公開鍵暗号方式のプライベート鍵。	鍵管理のサポート
鍵配送用公開鍵 （Public key transport key）	鍵を暗号化して配送するために用いられる公開鍵暗号方式の公開鍵。対になる鍵配送用プライベート鍵で復号する。	鍵管理のサポート
鍵共有用鍵 （Symmetric key agreement key）	鍵(*1)を確立するために用いられる共通鍵暗号方式の共通鍵。	鍵管理のサポート
鍵共有用固定プライベート鍵 （Private static key agreement key）	鍵(*1)を確立するために用いられる公開鍵暗号方式のプライベート鍵。	鍵管理のサポート
鍵共有用固定公開鍵 （Public static key agreement key）	鍵(*1)を確立するために用いられる公開鍵暗号方式の公開鍵。	鍵管理のサポート
鍵共有用一時プライベート鍵 （Private epehemeral key agreement key）	1 つあるいは複数の鍵(*1)を確立ためにただ一度のみ使われる、公開鍵暗号方式のプライベート鍵。	鍵管理のサポート
鍵共有用一時公開鍵 （Public epehemeral key agreement key）	1 つ、または複数の鍵を確立するために、鍵確立のプロセスで一度だけ用いられる公開鍵。必要に応じてその他のセキュリティパラメータを確立するために用いられる。	鍵管理のサポート
認可用共通鍵 （Symmetric authorization key）	共通鍵暗号方式を用いてエンティティに対して権限を付与する際に用いる鍵。	鍵管理のサポート
認可用プライベート鍵 （Private authorization key）	公開鍵暗号方式を用いてエンティティに対して権限を付与する際に用いる公開鍵方式のプライベート鍵。	鍵管理のサポート
認可用公開鍵 （Public authorization key）	公開鍵暗号方式を用いて、エンティティに対して権限を付与する際に用いる公開鍵暗号方式の公開鍵。	鍵管理のサポート

(*1) 確立される鍵には、鍵暗号化用鍵、データ暗号化用鍵、MAC の鍵がある。

また、SP 800-57 に示される一般的な鍵のライフサイクルを以下に示す。

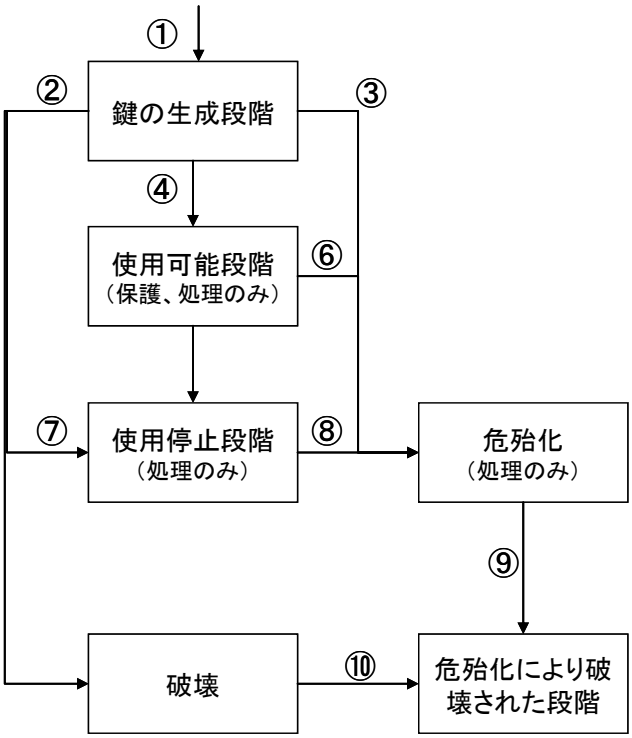


図 3-1 SP 800-57 鍵のライフサイクル

表 3-2 SP 800-57 鍵のライフサイクルとその概要

ライフサイクル	概要
鍵の生成	鍵は生成されたが、まだ使用の許可を受けていない。この状態にある鍵は、所有の証明、または鍵確認を実行するためにのみ用いられる。
使用可能	鍵は、情報を暗号化によって保護するために、あるいは、あらかじめ保護されている情報を暗号化によって処理する（例えば、暗号文の復号、またはデジタル署名の検証）ために、またはその双方に、用いられる。
使用停止	暗号化が有効な期間は終了したが、暗号化による処理がまだ必要な鍵は、破壊されるまで鍵の使用停止段階にある。使用停止段階にある鍵は、情報を新たに暗号化する等の保護を適用するためには用いられないが、既に暗号化された情報を復号する等に用いられる。
鍵の破壊	その存在に関する全ての記録が、削除されることがある。しかし、監査の目的で、ある特定の鍵属性を保持しなくてはならないことがある。
危殆化	鍵は、許可されていないエンティティに公開されたり、発見された場合には、危殆化する。鍵の完全性または秘密（情報）が疑われる場合、危殆化した鍵は廃棄される。
危殆化による	危殆化した鍵は破壊されるか、あるいは、鍵が破壊された後に、危殆化が見つ

ライフサイクル	概要
鍵の破壊	かる。破壊された段階とは異なり、この段階にある鍵は、危殆化していることが知れているか、または疑われている時点で、既に危殆化によって破壊されている状態を指す

表 3-3　SP 800-57 ライフサイクルの移行

鍵の移行	概要
移行①	生成された鍵は、鍵の生成段階にある。
移行②	全く使用されない鍵は、鍵の生成段階から、直接鍵の破壊段階に移行することがある。この場合、機密性の保護を要求する鍵の完全性、または機密性は、信用できると見なされるが、鍵そのものは今後必要ないと判断されている。
移行③	全く使用されない鍵は、鍵の完全性、または、機密性保護を要求する鍵の機密性が、最初の使用前に疑わしくなった場合、始動前状態から、危殆化状態に移行することがある。
移行④	鍵は、使用可能な状態になったら、始動前状態からアクティブ状態に移行する。この移行は、起動日に達した後、または、外的事象によって誘発される。
移行⑤	アクティブな鍵は、鍵の完全性、または、機密性保護を要求する鍵の機密性が疑わしくなった場合、アクティブ状態から危殆化状態に移行することがある。
移行⑥	アクティブな鍵は、データに暗号保護を適用するために使用されなくなった場合、または、保護データを暗号処理するために使用することが意図されなくなった場合、動作停止状態に移行することがある。
移行⑦	鍵が動作停止状態中に危殆化していないと判定されたと仮定した場合、鍵は、動作停止状態から破壊された状態に移行することがある。
移行⑧	鍵の完全性、または機密性保護を要求する鍵の機密性が疑われる場合、動作停止中の鍵は、動作停止状態から危殆化状態に移行する。
移行⑨	危殆化状態の鍵は、データの処理に必要なくなった場合、破壊された危殆化状態に移行することがある。
移行⑩	破壊された鍵は、鍵が以前に危殆化していたと判定された場合、破壊された危殆化状態に移行することがある。

3. 1. 4. SP 800-63 Electronic Authentication Guide

米国政府において、電子的な認証機構を実装する際のガイドラインである。特に、リモートのオープンなネットワーク上でのユーザ認証についてもカバーする。ユーザ識別子の証明、登録、トークン、認証プロトコルについて述べられている。

3. 1. 5. SP 800-73 Interfaces for Personal Identity Verification

米国政府職員ならびに請負業者の身元証明（Identity Credential）をおこなう PIV

（Personal Identity Verification）[30]カードのインターフェースについての推奨が述べられている。

SP 800-73 は以下の 3 部構成となっている。

- 一般的なデータモデルとマイグレーション
- カードの移行に関するインターフェース
- PIV カードおよびクライアントのプログラミングインタフェース

3.1.6. SP 800-77 Guide to IPsec VPNs

IPsec を実装および配置する際のガイドラインである。以下のフェーズに分けて解説を行っている。

- Identity Needs
- Design the Solution
- Implement and Test a Prototype
- Deploy a Solution
- Manage the Solution

3.1.7. SP 800-78 Cryptographic Algorithms and Key Size for Personal Identity Verification

FIPS 201 に関連する文書であり、PIV システムのための暗号アルゴリズムおよび鍵のサイズを規定している。

3.1.8. SP 800-85A PIV Card Application and Middleware Interface Test Guidelines (SP 800-73 Compliance)

「PIV ミドルウェア」および「PIV カードアプリケーション」という 2 つの PIV 構成要素について、NIST SP 800-73 への遵守／適合性の検証に使用できる試験要件および試験アサーションを提供することである。

3.1.9. SP 800-89 Recommendation for Obtaining Assurances for Digital Signature Applications

適切な電子署名の確認に必要な電子署名手法を規定する。特に、ドメインパラメータ、公開鍵の確認、プライベート鍵の所有者が執り行うべきプロセスと鍵所有者の識別を含む。

[30] PIV カードの仕様については FIPS 201 に述べられている。

3.1.10. SP 800-90 Recommndation for Random Number Generation Using Determinisic Random Bit Generators (Revised)

ハッシュ関数、ブロック暗号を用いた擬似乱数生成器についての推奨を述べている。

3.1.11. SP 800-97 Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11.i

このガイドの目的は、各組織が、最も一般的に利用されている WLAN の標準ファミリである IEEE（Institute of Electrical and Electronics Engineers：米電気電子技術者協会）802.11 を、IEEE 802.11i amendment（IEEE 802.11i 修正案）で導入されたセキュリティ強化策を中心としてより深く理解できるように支援することである。

3.1.12. SP 800-104 A Scheme for PIV Visual Card Topography

政府職員の所属ごとの PIV カードのカラーコーディングの指定についての追加的推奨を与える。

3.1.13. SP 800-111 Guide to Storage Encryption Techlogies for End User Devices (Draft)

許可されたものだけがストレージに蓄積されている情報にアクセスまたは利用ができるようにするに関するストレージセキュリティについての基本的説明と、フルディスク暗号化、ヴォリュームおよびヴァーチャルディスク暗号化、ファイルおよびフォルダ暗号化の技術について説明されている。また、ストレージ暗号化におけるユースケースも含んでいる。

ストレージ暗号化について以下の推奨を与えている。

- ストレージ暗号化技術を選択する際には、既存システムの特徴およびインフラストラクチャーを考慮したソリューションを検討すること。
- 使用されているストレージ暗号化についてすべてを集中管理し、スタンドアローンでの仕様や小規模での仕様を避けること。
- ストレージ暗号化に用いるすべての暗号鍵は、利用しているソリューションに適合した適切な管理を実施すること。
- ストレージ暗号化において適切なユーザ認証を実施すること
- エンドユーザデバイス向けに適切なストレージ暗号化およびそのサポートを行うための手段を実装すること。

3.1.14. SP 800-113 Guide to SSL VPNs (Draft)

SSL についての基本技術と特徴、および、SSL の配置の助けとなるプランニングと実装をフェーズアプローチで示している。

SSL VPN の利用に関して以下の推奨を与えている。

- 米国政府機関においては、FIPS に適合した暗号アルゴリズム、暗号スイート、バージョンを用いて SSL VPN を配置しなければならない。
- 組織にあった製品を選定するために、要求事項を明確化し、複数の製品を評価すること。
- SSL VPN のプランニングと実装にはフェーズド・アプローチを用いること。
- SSL VPN 技術の限界について精通すること。
- FIPS に適合した SSL VPN 実装またはサポートに関する、現状以外の方法も考慮すること。

3.2. 国際標準化機構 ISO

3.2.1. ISO 13491 Secure cryptographic devices (retail)[31]

金融のリテール向けサービス用の暗号モジュール（Secure Cryptographic Device:SCD）に関する物理的論理的特性と管理方法について述べている。

Part1 では、SCD に関するコンセプト、要求事項、評価方法について述べ、Part2 では、チェックリストを記述している。

3.2.2. ISO 11568 Banking - Key management (retail)

金融のリテール向けサービス向けの鍵管理標準を定めている。３部構成である。

(1) Part1: Principles

共通項目として、暗号鍵の管理に関する原則とライフステージを定義する。

[31] ISO 13491：Banking-Secure cryptographic devices(retail) Part 1:Concepts, requirements and evaluation methodssecond editon, ISO/TC 68/SC2, June 2007.

ISO 11568 における鍵管理の原則

a) 鍵は ISO 11568 で規定されている形態でのみ存在するべき

b) 平文の秘密/プライベート鍵には誰もアクセスしたり突き止められるべき

c) システムは、これまでにデータを保護していたり将来データを保護する秘密/プライベート鍵が暴かれることを防ぐべき

d) 秘密/プライベート鍵は、可能な全ての結果の値以外には結果の値を予測したり推定できないような処理を通じて生成されるべき

e) システムは、秘密/プライベート鍵を暴く試みや、秘密/プライベート鍵の意図されない目的での使用を検出できるべき

f) システムは、S/P 鍵あるいはその一部の目的外の使用、任意の鍵の事故や不正使用による変更、利用、代用、削除、挿入を防ぐか検出できるべき。

g) 鍵は、古い鍵を特定可能とみなせるだけの時間までに新しい鍵に換えられるべき

h) 鍵は、古い鍵で暗号化されたデータへの辞書攻撃が成功するとみなせるだけの時間までに新しい鍵に換えられるべき

i) 鍵は、その危殆化が知られるか疑われたら使用を止められるべきである。

j) あるひとつのグループにおいて共有される危殆化した鍵は、他の集団により共有される複数の鍵を危殆化しないようすべき

k) 危殆化した鍵はその代替鍵を特定可能な情報を与えないようすべき

l) 鍵は、合理的に、デバイスが不正な変更やすり替えがおこなわれておらずセキュアだと確認されるときだけデバイスにロードされるべき

ISO 11568 における鍵のライフサイクル

1. 生成（Generation）
2. 保管（Storage）
3. バックアップ（Backup）
4. 配送とロード（Distribution and loading）
5. 利用（Use）
6. 置換（Replacement）
7. 破棄（Destruction）
   使い終わった鍵のあるインスタンスをその場から無くす。後で再構築可能
8. 削除（Deletion）
   使い終わった鍵の全インスタンスをその場から無くす。後で再構築もできない
9. アーカイヴ（Archive）
10. 終了（Termination）
    使い終わった鍵の全インスタンスをあらゆる場から無くす。後で再構築もできない

(2) Part2: Symmetric ciphers, their key management and life cycle[32]

共通鍵暗号方式を用いる場合の暗号鍵のライフサイクルと、それぞれのライフステージにおけるオペレーションを定義する。

[32] ISO 11568-2: Banking—Key management (retail)—Part2: Symmetric ciphers, their key management and life cycle, Second edition, October 2005.

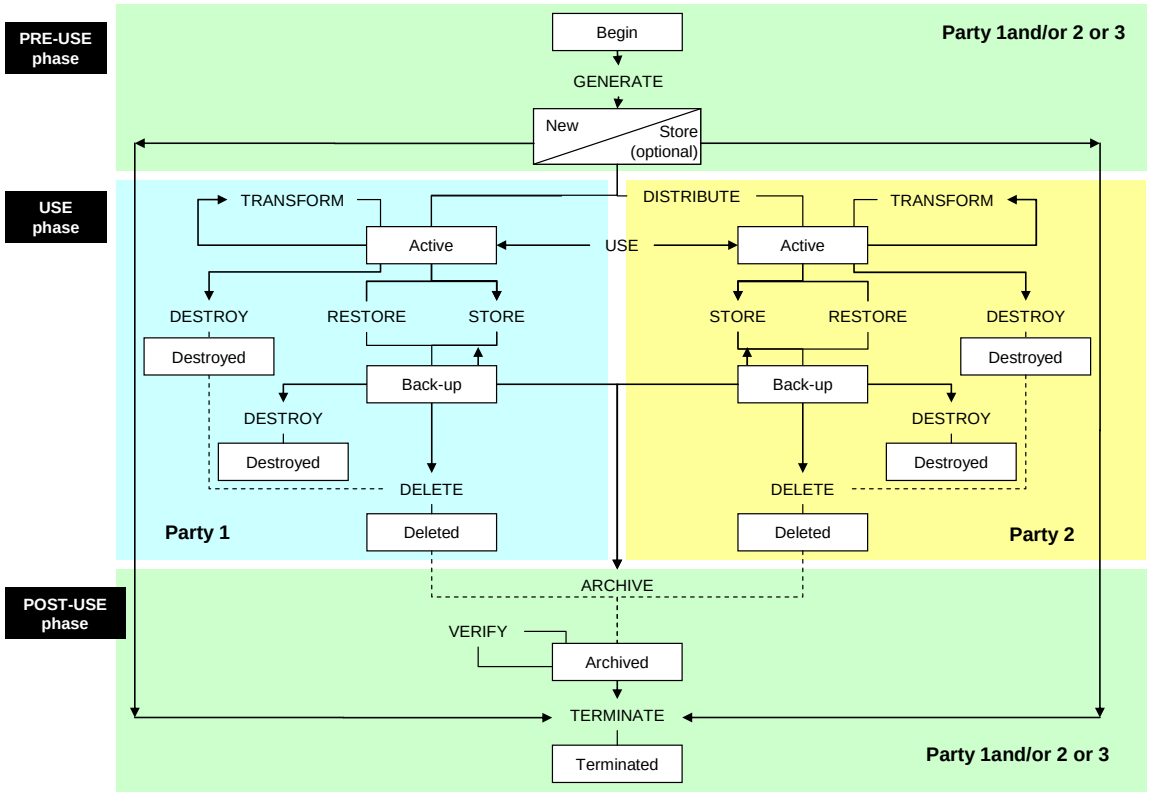


図 3-2 ISO11568-2：共通鍵暗号方式における暗号鍵のライフサイクル

表 3-4　ISO11568-2：共通鍵暗号方式における各ライフステージのオペレーション

ライフサイクルステージ	オペレーション
Key generation	・鍵および鍵コンポーネントは以下のいずれかの方法で生成されるべきである（詳細は4.3.に記載）: a）再現不可能な鍵生成手法 1）乱数処理（random process） 2）擬似乱数処理（pseudo-random process） b）再現可能な鍵生成手法 1）鍵変形（key transformation） 2）鍵導出（key derivation）

Key storage	・鍵はいずれかの保存形態の適切な実装により保護されるべきである(4.7.2 参照) a) 平文 (plaintext key) – 鍵の危殆化が複数の集団(party)に影響する場合: SCD で保護されるべき – 鍵の危殆化が単一の集団(party)に影響する場合: SCD で保護、あるいは物理的にセキュアな環境で b) 鍵コンポーネント (key components) – 2 つ以上の鍵コンポーネントの形態の鍵は知識の分割や二重制御のテクニックで保護されるべき – 鍵コンポーネントは必要な人間に最低期間だけアクセス可能にすべき – 人間が認識できる形態とする際には、ある時点である人間のみに知らせるべきで、 SCD に入力するまで – 2 つ以上の鍵コンポーネントを同一人物がアクセスできないようにすべき c) 鍵暗号化鍵で暗号化された形態(enciphered key) – SCD 内で暗号化を行う ・鍵の置換についてはプロシージャの実行が必要とされる(6.3.3 参照) ・鍵の形態に合わせた保存方法 ・鍵のすり替え(unauthorized key substition) と回復
バックアップからの鍵の回復 Key restoration from back-up	・Plaintext keys (SCD で保持) (-> 4.9 参照) a) 鍵配送プロセスでは平文の鍵のいかなる部分も明かされない。 b) 平文の鍵を移すデバイスはタンパーされていない。 c) SCD 間の通信は盗聴されていない。 d) SCD は平文の鍵を少なくとも権限を持つ 2 名が認証されたときのみ通信する。 e) 鍵生成デバイスから利用デバイスへと移す際に用いるデバイスは SCD であること。移した後は鍵を明かしうるいかなる情報も保持しないこと ・Key components (a～c は、ほぼ plaintext keys と同様) d) Dual control と split knowledge に則って処理する ・Enciphered key – 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(modification)に対する防護が必要 (ISO 11770-2 を参照) ・SCD への配送やロードは以下のテクニックのいずれかに則って行われるべきである。 a) 手動。例:キーパッドからの鍵コンポーネントの直接入力。 b) 直接的な電子的ローディング。例:生成デバイスあるいは鍵転送デバイスからケーブルで直接注入 c) ネットワークによる配送とロード。例:ネットワークによる遠隔鍵配送

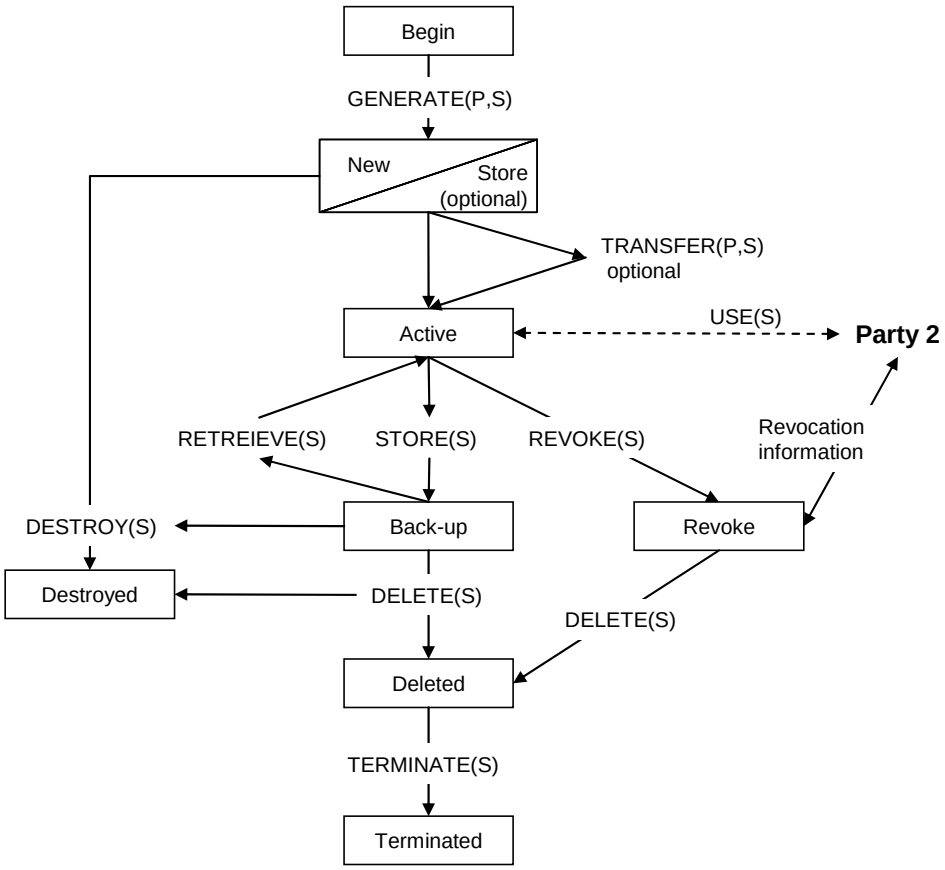
鍵の使用 Key use	・権限のないものによる鍵の使用を防ぐ ・鍵は意図した機能と、意図した場所でのみ用いられる(しかしながら鍵の variant は異なる機能に用いられうる) ・鍵は単一の機能のみに用いる ・鍵は効果的なシステム運用に最低限必要とされる場所にのみ存在する。通信に用いられるデバイスに存在する鍵は他のデバイスには存在してはいけない。 ・鍵を適切に隔離しておくために使われるべきテクニック（4.7.4 参照） a) 物理的および手順により鍵保管区域への許可しないアクセスを防止する b) 意図する利用に応じた機能として暗号化し鍵を保存する c) 平文と鍵暗号化鍵により暗号化された暗号文の両方で鍵を得られないようにする ・1 つの鍵は通信を行う少なくとも 2 つのパーティにより共有されるべきである ・危殆化が疑われる鍵の使用は防止されるべきである。これは以下の要件を含みうる: a) 全ての運用の場から当該鍵を削除(delete)すること b) 当該鍵を入手する手段を止めること
鍵の置換 Key replacement	・鍵は、鍵の危殆化あるいはすり替えが疑われる際には置換される。鍵暗号化鍵が疑われる場合には、その影響下にある全ての鍵が置換される ・鍵は、辞書攻撃あるいはブルートフォースアタックに成功するのに十分な時間が経つまでに置換される ・鍵は、その鍵が存在する全ての場所で置き換える ・置き換えられた鍵は、再び利用しない。 ・鍵の置換の手法 - 新しい鍵の配送 - 現在の鍵の不可逆な変換 ・鍵の危殆化が疑われる場合には、新しい鍵を配送する。 ・鍵の置換の際には、古い鍵を破棄する

鍵の破棄、消去、アーカイブ、終了 Key destruction, deletion, archive and termination	・鍵を消去するためのテクニック(key erasure techniques) – メディアを物理的に破壊することを含めた説明(省略) ・鍵の破棄(Key destruction) – あるひとつの鍵のインスタンスが不要になった際には破棄する。 – SCD をシステムから取り除く際には内の全ての鍵を破棄する – 鍵のあるひとつのインスタンスについて上述のテクニックを用いること ・鍵の消去(Key deletion) – ある 1 つの鍵がある場所(location)で不要になった際に消去する。 – その場所のその鍵の全インスタンスについて上述のテクニックを用いること ・鍵のアーカイヴ(Key archive) (4.7 も参照) – アーカイブされた鍵は、アーカイブ以前の Transaction の正当性を検証する際に用いる。 – アーカイブされた鍵は通常の運用には利用されない – アーカイブされた鍵は、その鍵で暗号化された全ての鍵やデータの寿命の間セキュアに保管される – 鍵は使用中の鍵が暴露されるリスクを高めないような手段でアーカイブされなければならない – アーカイブされた鍵は以下のいずれかの形態である a) セキュアな暗号デバイス内の平文(plaintext keys) b) 少なくとも 2 つの隔離された鍵コンポーネントの形態(key components) c) 鍵暗号化鍵で暗号化された形態(enciphered keys) ・鍵の終了(Key termination) – 全ての場所において鍵が削除された場合に、鍵は終了する。 – 鍵を終了する際には、鍵を再構築可能な情報は存在しないようにすべき – 鍵を用いる全ての場所(location)において上述のテクニックを用いること

(3) Part4: Asymmetric cryptosystems -- Key management and life cycle[33]

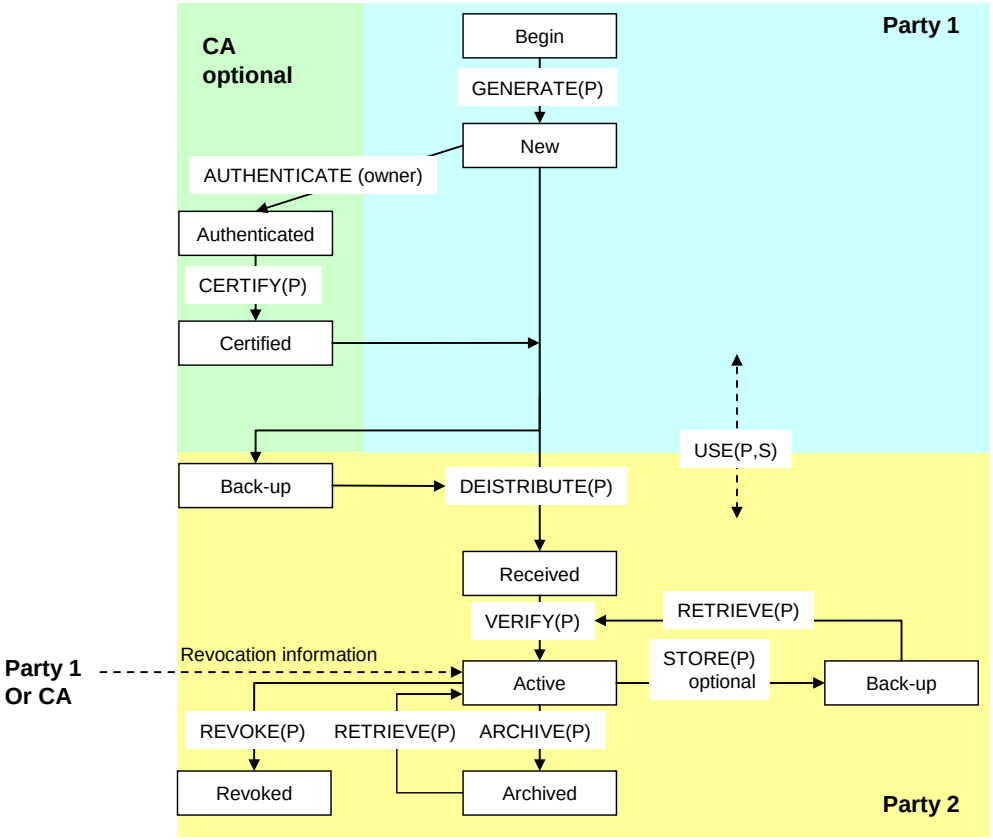
公開鍵暗号方式における秘密鍵および公開鍵のライフサイクルと、各ライフステージにおけるオペレーションを示す。

[33] ISO 11568-4:Banking—Key Management (retail) –Part4:Asymmetric cryptosystem—Key management and life cycle, Second Edition, July 2007.



ISO11568-4:2007 Banking—Key management(retail)– Part4: Asymmetric cryptosystems– Key management and life Cycle, Figure.1

図 3-3 ISO11568-4 公開鍵暗号：秘密鍵のライフサイクル



ISO11568-4:2007 Banking—Key management(retail)– Part4: Asymmetric cryptosystems– Key management and life Cycle, Figure.2

図 3-4 ISO11568-4 公開鍵暗号：公開鍵のライフサイクル

表 3-5 ISO11568-4：公開鍵暗号方式における各ライフステージにおけるオペレーション

<table>
<tr><th>ライフサイクルステージ</th><th>秘密鍵</th><th>公開鍵</th></tr>
<tr><td>Generation</td><td colspan="2">・唯一の party が秘密鍵 S および公開鍵 P の鍵ペアを生成する。
＜CA が生成する場合＞
・SCD 内部で鍵ペアを生成し、Key Pair Owner に転送する。
＜Key Pair Owner が生成する場合＞
・SCD 内部で鍵ペアを生成し、同一の SCD 内部に保管するか、その他利用する SCD に安全に転送する。
＜Third Party が生成する場合＞
・SCD 内部で鍵ペアを生成し、Key Pair Owner に転送する。</td></tr>
<tr><td></td><td>・秘密鍵 S は人間が理解できない形式とする。
・秘密鍵 S およびその生成に用いた Seed は、転送後速やかに消去する
・秘密鍵 S の integrity を確保する。</td><td></td></tr>
<tr><td>Storage</td><td>・Secrecy, Integrity を確保する
・以下の 3 つのうちどれかを採用する
a) SCD 内部で平文の形式
b) Key Share（秘密分散法を用いた鍵を分割）
c) 鍵暗号化鍵を用いて暗号化</td><td>・Authenticity、Integrity を確保する
・以下のいずれかを用いて保管する
a) 不正な Replacement を検知する SCD 内部に保管
b) Key Verification Technique(5.5)を利用する
・置き換え攻撃に対応する場合には、以下のうち 1 つ以上の方法を用いること
a) Key Storage Are への不正なアクセスを防ぐ
物理的および機能的機構を導入する
b) 鍵暗号化鍵で暗号化する
c) 公開鍵証明書
・不正な公開鍵の置き換えを検知した場合は、update を行う</td></tr>
<tr><td>Backup</td><td colspan="2">・Storage と同じ方針で行う。</td></tr>
</table>

Distribution and Loading		・Storage と同じ方針で行う
Asymmetric Key Pair Transfer	[Key Pair Owner への Key Pair の転送に使用] ・Key Pair Owner が鍵生成の能力がない場合に使用する ・Key Pair Owner を認証する ・ISO11770-3 に示す方式で転送を行う	

	＜Plaintext Private Key＞ ・Transfer Process では confidentiality と Integrity を確保する。 ・Transfer および Loading プロセスは Dual Control、Split Knowledge に従って実施する。 ・Transfer を行う際は、少なくとも二人以上の人間が SCD に認証されている場合に限る。 ・SCD へのロードは、SCD がこれまでにタンパリングされていない場合に限る。 ・SCD 間の Transfer では、インターフェース部分でのタッピングがない場合に限る。 ・Transfer 用デバイスは SCD に限り、転送後は秘密鍵 S に関する情報が何も残らないこと。 ＜Key Share＞ ・秘密鍵 S の一部の情報が認証されていない人に漏れてはならない。 ・Key Share の Transfer は、転送先のデバイスがタンパリングされていないことが保証されている場合に限る。 ・Key Share の SCD への転送は、インターフェース部分で 、タッピングが行われていない、または、パッシブタッピングであることが確保されている場合に限る。 ・Transfer は Dual Control, Split Knowledge の理念に従って実行する。 ・秘密鍵 S を再構成するための定足数は、Key Share の保持者によって個別に決定される。 ＜Enciphered Private Key＞ ・5.2 節に示す方法に従うこと	・公開鍵 P を転送する前に、Key Pair の検証を行う。 ・Key Pair の検証は SCD 内部で実施する。 ・Key Pair の検証プロセスで発生した中間値およびその結果は破棄すること
Use	・許可されていない利用は禁止 ・最適なオペレーションに矛盾しない最低のロケーションで利用する。 ・SCD の外で利用しない	・使用する前に証明書の確認（5.3 節）を行うか、Key Verification Technique (ISO 11609）で、公開鍵 P の Authenticity、Integrity を確認する

	・１つの Key Pair は、１つの目的（Authenticity または Confidentiality）に利用する。なお、署名および鍵暗号化(encipherment）の場合はこの限りではない。 ・意図した目的、意図したロケーションで利用する。 ・物理的および論理的に許可されていない鍵の利用を防止するメカニズムを搭載する。 ・Cryptoperiod または秘密鍵 S が漏洩した場合または予測される場合には、その鍵ペアの利用は今後行わない。 ・鍵の漏洩が疑われる場合には、以下のいずれかを行うこと a）全ての作業領域から鍵を削除すること b）鍵が導出されないようにブロックする手段を講じること	
Public Key Revocation		・公開鍵 P の利用者は revocation notify がなされた場合、P の利用を即座にやめる。 ・revocation notification は公開鍵 P の全ての利用者にブロードキャストするか、利用者がアクセス可能な DB に公開する。
Replacement	・鍵ペアが失効または revoke した場合に実施する ・Key Generation, Transfer, Loading の各プロセスを再度実行する。 ・古い鍵（ペア）は破棄する。	
Destruction	・古い秘密鍵データは消去する ・作業領域に残るものは新しい秘密鍵をリストアする。 ・破棄する秘密鍵に対応する公開鍵は通信相手に渡さない。すでに公開鍵が渡されている場合には、破棄するように通知する。 ・サービスから SCD が削除された場合には、当該デバイスに記憶されている秘密鍵は全て破棄する。 ・秘密鍵の廃棄は、新たな秘密鍵または無関係なデータで上書きするか、鍵ストレージメディアを ISO9564-1 に示される方法で破壊する。	
Deletion	・秘密鍵 S が Destruction された場合に実施する。 ・全ての形態の秘密鍵 S を消去する ・鍵コンポーネントがメディアに記録されている場合には、燃やす等の方法で廃棄する。	

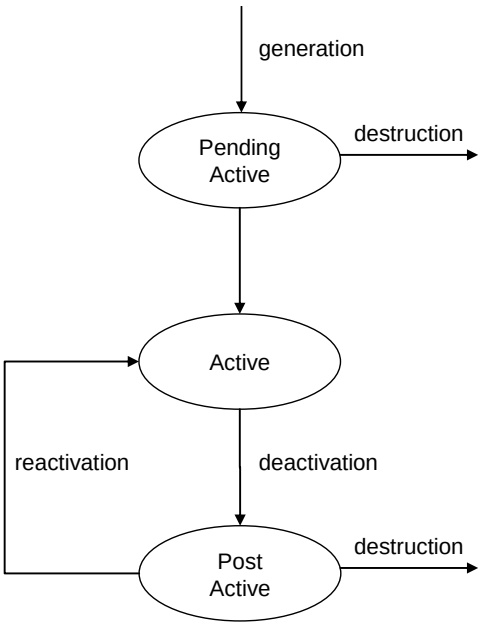
Archive		・Key Revocation に先立って、署名検証に公開鍵 P を利用する場合に実施し、使用後は破棄する。 ・データ検証に用いるため、安全に保管する。 ・Active Key 等と区別するために Key tagging（5.4 節）の手法を利用する。
Termination	・鍵の Deletion が実行された後のステージ。 ・消去された鍵に関する情報は何もなく、再構成できない。	
Public Key Certification（option）		・Third Party のプロセス ・Key Pair Owner と公開鍵を関連付ける
Key Retrieval（option）	・バックアップデータから取得する場合 ・Key Distribution and Loading に示す手法が一つの実現方法	

3. 2. 3. ISO/IEC 11770 Information technology -- Security techniques -- Key management

ISO 11568 が銀行におけるリテール向けの暗号鍵のライフサイクルを提示するのに対して、ISO/IEC 11770 は一般的な暗号鍵のライフサイクルを示している。

(1) Part1: Framework[34]

ISO/IEC 11770-1 に示される一般的な鍵のライフサイクルモデルを下図に示す。



ISO/IEC 11770-1 Figure 1 より

図 3-5 ISO/IEC 11770-1 Key Life Cycle

鍵の管理状態	概要
Pending Active	鍵は生成されたが、まだ使用されていない状態
Active	鍵が暗号機能に利用された状態
Post Active	鍵が復号、または、検証のみに利用されるために待機している状態

鍵管理の状態遷移	概要
Generation	鍵の生成 あらかじめ決められた生成方法で鍵を生成する。また、所定の方法で鍵が生成されたかどうかの試験を含む場合もある。

[34] ISO/IEC 11770-1, Information Technology –Security techniques –Key management – Part1: Framework, First Edition, 1996-12-15.

Activation	鍵が、暗号機能の入力として適切となるようにする。
Deactivation	鍵の利用を制限する。 特に、鍵の失効やリボークされることにより発生する。
Reactivation	Post Active の状態の鍵を利用するときの遷移。
Destruction	鍵のライフサイクルが終了する。 論理的および物理的な鍵の破壊を意味する。

(2) Part2: Mechanisms using symmetric techniques[35]

共通鍵暗号を用いた鍵確立の 13 の方法を規定する。

(3) Part2: Mechanisms using asymmetric techniques[36]

公開鍵暗号方式を用いた鍵確立の 16 の方法（Key agreement 7, Key transport 6, Public key transport 3）を規定する。

(4) Part4: Mechanisms based on weak secrets[37]

パスワード等をはじめとする人間が記憶可能で、比較的小規模な集合の中から選択されることが予測される秘密に基づく鍵確立の方法を規定する。

[35] ISO/IEC 11770-2, Information technology –Security techniques –Key management –Part2: Mechanisms using symmetric techniques, First Edition, 1996-04-15.
[36] ISO/IEC 11770-3, Information technology –Security techiniques –Key management –Part3: Mechanisms using asymmetric techniques, Fist Edition, 1999-11-01.
[37] ISO/IEC 11770-4, Information technology –Security techniques –Key management –Part4: Mechanisms based on weak secrets, First Edition, 2006-05-01.

3.3. Internet Engineering Task Force （IETF）

3.3.1. RFC 2408 Diffie-Helman USM Key Management Information Base and Textual Convention[38]

ネットワークマネージメントプロトコル向けの Management Information Base(MIB)の一部を規定する。

3.3.2. RFC 2786 Internet Security Association and Key Management Protocol (ISAKMP)[39]

インターネット環境におけるセキュリティアソシエーション（SA）の確立と鍵管理に必要なセキュリティコンセプトを利用するプロトコル（ISAKMP）を示す。ISAKMP では、ピア間の認証、SA の生成と管理、鍵生成、およびサービス負荷攻撃やリプレイ攻撃等の脅威の軽減を目的とした手順を提供する。

3.3.3. RFC 2792 DSA and RSA Key and Signature Encoding for the Keynote Trust Management System[40]

KeyNote Trust Management System Version 2 における RSA および DSA の鍵および署名のエンコーディングについて。

3.3.4. RFC 3766 Determining Strengths For Public Keys Used For Exchange Symmetric Keys[41]

システム等で利用する公開鍵暗号方式の鍵長を決める際のガイドラインである。実現すべき安全性のレベルを共通鍵暗号方式の鍵長とし、これと対比することで、利用する公開鍵暗号方式の鍵長を決定する。また、公開鍵方式でよく利用される大きな整数値（法、べき指数等）について、鍵交換に利用する際の変更時期についても言及している。

---

[38] M.St.Johns, “Diffie-Helman USM Key Management Information Base and Textural Convention”, RFC2786, March 2000.
[39] D.Manghan, M.Schertler, M.Schneider, J.Turner, “Internet Security Association and Key Management Protocol (ISAKMP)”, RFC2408, November 1998.
[40] M.Blaze, J.Ionnidis, A.Keromytis, “DSA and RSA Key and Signature Encoding for the Keynote Trust Management System”, RFC2792, 2000.
[41] H.Orman, P.Hoffman, “Determining Strengths For Public Keys Used For Exchanging Symmetric keys”, RFC 3766, April 2004.

3. 3. 5. RFC 4107 Guideline for Cryptographic Key Management[42]

鍵管理について、自動または手動の選択を行う際の判断基準を与えるガイドラインであるが、可能な限り自動化を行うことを指針としている。

3. 3. 6. RFC 4306 Internet Key Exchange (IKEv2) Protocol[43]

IKE のバージョン２のプロトコルについて述べる。

3. 3. 7. RFC 4962 Guidance for Authentication, Authorization, and Accunting (AAA) Key Management[44]

RADIUS[RFC2865]および Diameter[RFC3588]を含む Authentication, Authorization and Accounting (AAA)の鍵管理プロトコル（AAA Key Management Protocol）に関するデザイナー向けのガイダンスである。本ガイドラインで示される鍵管理におけるよう旧条件は以下である。

1. 暗号アルゴリズムに独立であること
2. セッションキーに関しては、十分な鍵長を選択し、更新を行うこと
3. 鍵に関連するセキュリティパラメータに関して、ユーザの権限に応じたアクセスコントロールを行うこと
4. リプレイ攻撃対策を行うこと
5. 個々のユーザが通信相手から認証されること
6. ピアおよび Authenticator は認証を行うこと
7. 鍵データの機密性および完全性を維持すること
8. ロールバック攻撃を検知するために、暗号スイートの確認を行うこと
9. 鍵データの参照名を唯一にすること
10. あるピア（または Authenticator）の鍵の漏洩が他のピア（または Authenticator）の鍵の漏洩につながらないように実装すること
11. 鍵をコンテキスト（鍵の利用方法、鍵を生成するためのセキュリティパラメータの有効期限等）と関連付けること

3. 4. まとめ

NIST SP、ISO、RFC 等において、鍵管理に関する標準化やガイドラインについて文献調査を行った。これらの NIST SP800-57 や ISO/IEC 11770、ISO 11568 では、鍵のライフサイクルおよび有効期間（Cryptoperiod）を規定し、それぞれのステージにおける管理方針を示している。また、NIST SP 800-57 や ISO/IEC 11770 は、暗号アプリケーションにとらわれない汎用的な鍵管理のガイドラインとなっている。ただし、PDCA(Plan Do

[42] S.Bellovin, R.Housley, “Guideline for Cryptographic Key Management”, RFC4107, June 2005.
[43] C.Kaufman, Ed., “Internet Key Exchange (IKEv2) Protocol”, RFC4107, December 2005.
[44] R.Housley, B.Aboba, “Guidance for Authentication, Authorization, Accounting (AAA) Key Management”, RFC4962, July 2007.

Check Action)のような、鍵管理に関わる運用状況等の確認と改善といったプロセスは含まれていないようである。

他方、NIST SP では、無線 LAN や SSL VPN、PKI といった個別の暗号アプリケーションごとに、実装方針等を含むガイドラインを提示している。

わが国における暗号鍵管理に関わるガイドラインにおいては、これらの文献を参考として、ライフサイクルマネージメントをベースとし、各ライフサイクルでの PDCA 等による確認と改善のプロセスを含むガイドラインを作成することが望ましい。

4. 暗号の鍵管理に係わる国内実態

情報セキュリティ関連事業者、PKI 事業者等へのヒアリングに基づき、国内の暗号を利用する情報システムにおける暗号鍵管理に関する実態、特に電子政府システムにおける実態について示す。

4.1. 国内における暗号鍵管理の現状

現在のところ、国内においては暗号鍵管理の技術面・運用面のいずれについて公開された文書は殆ど無く、概論や教科書として参照可能な文書や、最低限満たすべき基準等の整備は遅れている。個別のシステムにおける暗号鍵の運用については、具体的な取扱い方法がシステム運用に関するマニュアル等に記載されており、これらは基本的に関係者以外には非公開の文書である。

国内の暗号を利用するシステム、特に電子政府における暗号鍵管理の方法および状況について、ヒアリングおよび文献調査により得られた情報を以下に示す。

- 政府の情報システム管理および構築の担当者においては暗号および暗号鍵への関心は低く、管理の不備に関する問題意識も薄い。
- 鍵管理も含めてシステム・ベンダが仕様書や試験項目を作っている。鍵管理に関連する記述はチェック項目のみである。
- 運用そのものをアウトソーシングしており担当者が関与する部分はない。
- SET 等を扱った際の VISA や Master が示した要求仕様をおそらくベンダも引き継いで参考にしている。また、暗号鍵の管理上の脅威は示されておらずチェック項目のみである。
- ユーザに必要な利用マニュアルについては作られており、パスワード管理や IC カード管理等が記載されている。
- PKI においては認証局の鍵管理手法は既に確立しており、他の暗号用途と比べても手法が公開される部分も多い。署名・認証用途の鍵の管理についてはプラクティスが確立している。一方で、暗号（秘匿）用途の鍵管理については確立しているとは言い難い。
- PKI の導入に関しては認定基準がありコンサルタント事業を企業が行っている。特定認証業務の事業者相手のコンサル（運用側のコンサル）は既にビジネスとして展開されている。

また、銀行をはじめとする金融業界における暗号の利用状況ならびに鍵管理の実態について、ヒアリング調査により以下の情報を得た。

- 銀行では長期署名は使われていない。
- SSL を使う場合は多い。自前でなく民間のサービスを利用している。鍵管理についてもそれらのサービスに則って行っている。

- 全銀協は、全銀協 PKI を運営し、IC キャッシュカード仕様を定めている。デビッドカード、IC カードが使える仕様。MAC 等で認証をしているようだが、仕組み上は電子署名を使っている。全銀協が各銀行に証明書を発行し、IC カードとの認証に利用している。
- インターネットバンキングでは SSL を用いている。民間のサービスを利用している。
- 暗号利用システムの運用担当者には開発ベンダが鍵管理に係る文書（マニュアル）を作っている。担当者の理解度は高くはない。
- 暗号のシステム、鍵の管理についてはベンダが仕様書や試験項目を作成している。
- ベンダから管理者にはミニマムの情報を渡して管理意識を持ってもらうようお願いしなければならない。
- ユーザの利用マニュアルは作っている。パスワード管理や IC カード管理等。
- 運用そのものをアウトソーシングしており担当者が何かする部分はない。
- SET 等を扱った際の VISA や Master が示した要求仕様をおそらくベンダも引き継いで参考にしている。脅威は示されておらずチェック項目のみ。

ヒアリングでは、このような現状を踏まえ、ガイドラインとして知識を整理しても活用の場があるかについては疑問があるとの意見もあった。

4.2. 暗号鍵管理に関する課題・問題

運用されているシステムにおいて明らかになっている暗号鍵管理に関する現在あるいは将来の課題・問題について、ヒアリングにより得られた情報を以下に示す。

- 暗号自体はフリーで入手可能であり、方式が破られることは殆ど無い。問題が起きるとすれば鍵管理である。
- 実際は鍵管理で不適切な実装も多く、鍵情報が漏洩してしまう場合もある。
- 実装手法や技術詳細はビジネスとして各社が工夫のしどころとして任せられているポイントである。
- システム・ベンダでは、システム管理者にはミニマムの情報を渡して管理意識を持つようお願いしている。
- ライフサイクルについても概念整理と理解は必要である。実際には面倒なので考慮されていない。鍵長や方式の移行を考慮するためにも必要な概念ではある。
- 現在の鍵管理の概念は公開鍵と共通鍵で大きく異なる。共通鍵のライフサイクル管理はプラクティスが外部に出ないので整理は難しい。おそらく方法を示すことで安全性が失われる（弱点が明らかになる）性質があるため、非公開にして安全性を保っている部分もあるだろう。
- システム上では鍵の復元が必要であるが、キーリカバリ、キーエスクロへの批判があったために研究が止まっており進捗がない。
- 鍵管理のガイドラインは必要である。使用している暗号と暗号鍵管理のバランスを欠くシステムが多い。
- 公開鍵と共通鍵の使い分けが理解されにくい。ソリューションとしても説明されていないので、この部分について十分な解説等が望まれる。
- 電子署名については政府関係者の理解は比較的進んでいるが、暗号化については進んでいない。
- 共通鍵暗号に関する理解は特に知識が少なく理解の範囲から抜けている。電子私書箱で

も共通鍵暗号を利用する動きがあるため、PKI よりもそちらの方が重要ではないか。
- 実用的な問題としてキーリカバリの必要もあるのではないか。

4.3. 暗号鍵ガイドラインへの要望

事業者の視点から寄せる暗号鍵ガイドラインへの要望について、ヒアリングにより得られた情報を以下に示す。

- 鍵の期限切れについての記述は重要である。
- エンドユーザが自分の問題として認識できることが重要である。問題発生シナリオなどの情報が必要である。
- 読み易くする工夫が必要である。できるだけテクニカルタームを使わず、薄い冊子にすると良い。
- PKI を用いていない組織も多くある。他のモデルも提示の要望はある。
- 最終的なまとめ方としては最低限やってほしいことをチェックリストとして、理由を解説で示すとわかりやすい。
- 網羅性は策定段階の作業手順で必要である。
- 読者は、チェックリストを満たせば十分であると考えるので注意したほうがよい。
- 府省担当者が漏れや矛盾を見つけると信頼性を損なうので注意したい。
- 構築上の要件はあまり読まないため、運用要件に関する記述もあったほうがよい。特に府省関係者はそちらを重視する。
- 用途モデルは一例にすぎないことを明示すべきである。違いを理解してもらえず、絶対的に捉えられる可能性がある。
- 省庁担当者にいくつかモデルを示さないと理解してもらえない。
- 「必須対策」「推奨対策」ではなく、「要件」「対策の実装手法の例」のように示したほうがよい。必須とするには強制力の根拠が必要。
- 脅威を多く書き、鍵管理と対策の重要性を示してほしい。
- 鍵管理の理解を進めるためには個々の項目について解説が必要。
- 公開鍵暗号方式（プライベート鍵と秘密鍵）、共通鍵暗号方式それぞれでどのようなステップを踏むかの図が最初に欲しい。現在のものではよくわからない。

4.4. まとめ

暗号鍵の管理に関する実態および、今後作成予定の暗号鍵管理に関するガイドラインへの要望について、情報セキュリティ関連事業者、PKI 事業者等へのヒアリング調査を行った。

情報システム管理者および構築担当者は、概ね暗号および暗号の鍵管理についての認識は低いこと、一部ではユーザに対して鍵管理に関わるチェック項目が提供されていることが、システム構築において不適切な実装がなされるケースも散見されることが判明した。また、PKI システムについてはマニュアルの整備が進んでおり、システムコンサルや SIer がビジネスとして展開するレベルに達していることが判明した。

このため、暗号鍵の管理に関しては、組織の情報システム担当者の普及啓発活動をはか

ると共に、それぞれのアプリケーションについて適用可能で理解しやすいガイドラインにすることで、意識の醸成をはかることが望まれる。

5. 暗号鍵管理ガイドライン（案）

暗号技術が提供するセキュリティ上の効果を十分に得るためには、暗号の鍵の管理を適切に行う必要がある。しかし、我が国においては、これまでのところ、米国 NIST の SP 800-57 のような暗号の鍵管理に関する一般的な指針は示されていない(第3章参照)。また、システム開発ベンダ等が個別システムごとに暗号の鍵管理に関する最低限の情報をシステム管理者に提供する程度であり、システム開発ベンダやシステム管理者においても、暗号の鍵管理に関わる意識は総じて高いとはいえないようである（第4章参照)。従って、暗号の鍵管理に関するガイドラインを作成し、普及啓発を行うことが求められているといえる。

本年度は、暗号の鍵管理に関する典型的な利用用途を検討したうえで、NIST SP 800-57 および ISO13491 を参考にこれらを統合的に扱うための一般的な鍵管理のライフサイクルを検討した。そして、暗号の典型的なアプリケーションである PKI における CA の秘密鍵の鍵管理をベースに検討を進め、ガイドライン（案）としてまとめた（別添参照)。

5.1. 暗号利用用途

ここでは、代表的な暗号の利用用途として、PKI、機密文書管理、通信路の暗号化、電子文書の長期保存、パスワード管理についてまとめる。

(1) PKI

公開鍵認証基盤（PKI : Public Key Infrastracture）は、GPKI および LGPKI をはじめとした電子政府の基盤システムとしても稼動する、暗号の応用システムの代表事例である。

PKI では、認証局（CA : Cartification Autority）が、利用者に対してデジタル証明書を発行し、利用者の秘密鍵と対になる公開鍵の証明書とする。ある利用者 A のデジタル署名を検証するためには、A の公開鍵証明書を CA の公開鍵証明書に附属する公開鍵を用いて検証することで行われる。

PKI システムの安全性は、公開鍵証明書に用いられる公開鍵暗号アルゴリズムの強度と、CA の秘密鍵の管理に大別されると考えられる。

(2) 機密文書管理

情報漏えい等の対策を目的として、組織内で作成されたドキュメント等の内容に応じて管理レベルを決定して管理が行われる。その管理方法は、組織によって決定される管理方針に準じて行われる。特に機密性が高い文書においては、暗号化や電子署名を付与し、機密情報の漏洩や改ざんを防止した上で、予め定められた文書保存期間、保管管理されることになる。電子政府においては、文書データの内容に応じて機密性や可用性といったレベルを決定し、文書管理規則に則ってそのデータの管理が行われる。

機密文書管理では、ある一定期間（例えば、1 年以上）ドキュメントの管理を行う必要があるため、暗号を利用した場合にはその暗号化／復号鍵や署名生成／検証鍵もその期間管理する必要がある。このため、当該組織で定められた文書管理方針に則した暗号化／復号鍵の管理を行う必要がある。

(3)通信路の暗号化

電子政府における電子申請／届出システムや電子商取引では、サービス提供者と利用者の間の通信に暗号が利用され、カード番号や個人情報、申請内容等の情報の漏洩を防止する。通信路の暗号化でよく利用されるパッケージとして SSL／TLS が用いられる。

通信路の暗号化は主にパッケージソフトウェアやシステムとして提供されることが多く、暗号の鍵の管理においては、そのパッケージやシステムにおける実装方針に大きく影響されるといえる。

(4)電子文書の長期保存

契約書や仕様書など、長期的に電子文書の改ざん等の防止することためにタイムスタンプ等を用いる。電子文書の長期保存では、特に長期のもでは 10 年以上といった長期間の保管を想定するものがある。このため、タイムスタンプ等で利用する鍵の更新をはじめとして、利用している署名アルゴリズムの危殆化やシステム更新等を考慮する必要がある。

(5)パスワード管理

PC や携帯電話、社内システム、電子商取引等、IT システムを利用するためにパスワードによる個人認証が多く用いられている。特に、システムごとにパスワードを設定することが多く、1 個人が管理するパスワードの数は増加傾向にある。また、安全なパスワード設定のためには複雑なパスワード（例えば、半角英数字 16 文字以上など）を設定することを求められることもあり、パスワードの記憶自体が困難なものになりつつある。このため、複数のシステムで同一のパスワードを利用することや、テキストファイルなどに ID とパスワードを記録しそのままの状態で保管されることがある。従って、パスワード管理では、このような状況を考慮して、個人が所有する ID 及びパスワードの適切な管理方針を定める必要がある。

5.2.一般的な暗号鍵管理方針

5.2.1.暗号鍵に関する運用要件

(1)暗号鍵の機密性

暗号の鍵やデジタル署名の署名生成鍵が秘密に管理されることを前提として、暗号技術の機能は発揮される。このため、暗号の鍵や署名生成鍵が漏洩することは、運用上で第 1 に考慮すべきことであるといえる。

(2)暗号鍵の完全性

暗号の鍵および暗号鍵に関連する情報が改ざん等されることにより暗号文の復号ができなくなることや、デジタル署名等の検証が行えなくなる。このため、暗号鍵を保管する、USB メモリ等に記録して持ち運ぶ等の際には、改ざん防止技術や誤り訂正等により完全性を保つことが求められる。

(3)暗号鍵の可用性

暗号の鍵や署名検証鍵が、紛失等により必要なときに利用できない場合、当然暗号文の復号や署名の検証が行えない。このため、暗号の鍵や署名検証鍵が必要なときに利用できる世必要がある。

5.2.2.暗号鍵の運用要件を満たすための対策

(1)暗号鍵の機密性保持のための対策

暗号鍵はその用いられる範囲を明確かつ限定されたものとしておき、漏えいや紛失等の問題が発生した際に影響を受ける範囲に制限をかける。より具体的には、以下の項目に関する設定が対策に含まれる。

- 暗号鍵の特定可能な利用者を設定する。
- 暗号鍵に有効期間を設定する。
- 鍵情報の利用目的はひとつに限定する（例：暗号化と署名に使われる公開鍵暗号）
- 暗号鍵を蓄積する機器、媒体、ソフトウェアに保護機能を備える。

特に暗号化されていない状態の秘密鍵（共通鍵やプライベート鍵）の扱いについては注意が必要となる。以下に例を示す。

- 秘密鍵が存在する時間を制限する
- 暗号モジュール（hardware security module, HSM）内でのみ鍵を利用されるように用いられる範囲を限定する。
- 秘密鍵を人間が読み取ることや書き写すことを困難にする（可読性を与えない）。
- 暗号化されていない状態の秘密鍵へのアクセス履歴を保管する機能を用意する。

(2)暗号鍵の完全性保持のための対策

暗号鍵の記憶（または記録）方針を明確にする。特に暗号の鍵は、人間が記憶することが難しい長いビット列(共通鍵暗号では 64 ビット以上、公開鍵暗号では 1024 ビット以上)であることから、ファイル等に記録されるケースが想定される。具体的には以下の処置を講じることなどがあげられる。

- 複数の鍵を記録したファイルを暗号化し、そのマスター鍵を USB や HSM 等で管理する。
- 組織等においては、組織内で利用する暗号の鍵を管理する管理簿を設定し、管理簿を暗号化して管理する。特にマスター鍵の管理においては、組織の責任者が管理することとする。
- 暗号鍵等を管理する管理簿を設定する場合には、デジタル署名等の技術を適用することにより、改ざん等を防止する。

(3)暗号鍵の可用性保持のための対策

暗号鍵等の紛失などが発生しないように管理簿等のバックアップ等の処置を講じる。なお、バックアップデータに関しても、機密性や完全性保持の観点からマスター鍵を用いた暗号化が望まれる。

5.2.3. 暗号鍵のライフサイクル

上記、暗号鍵の運用要件を満たすための対策を包括的に実施するためには、暗号の有効期限に基づくライフサイクルを定義し、それぞれのライフステージにおいて、具体的な運用方針を明確化することがあげられる。

以下では､暗号鍵全般についての一般化された暗号鍵ライフサイクルについて説明する。その後、よりなじみ深い、共通鍵暗号方式の共通鍵、公開鍵暗号方式のプライベート鍵、公開鍵暗号方式の公開鍵のそれぞれについての暗号鍵ライフサイクルを示し、簡潔な注釈を加える。

5.2.4. 暗号鍵ライフサイクル（一般）

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。

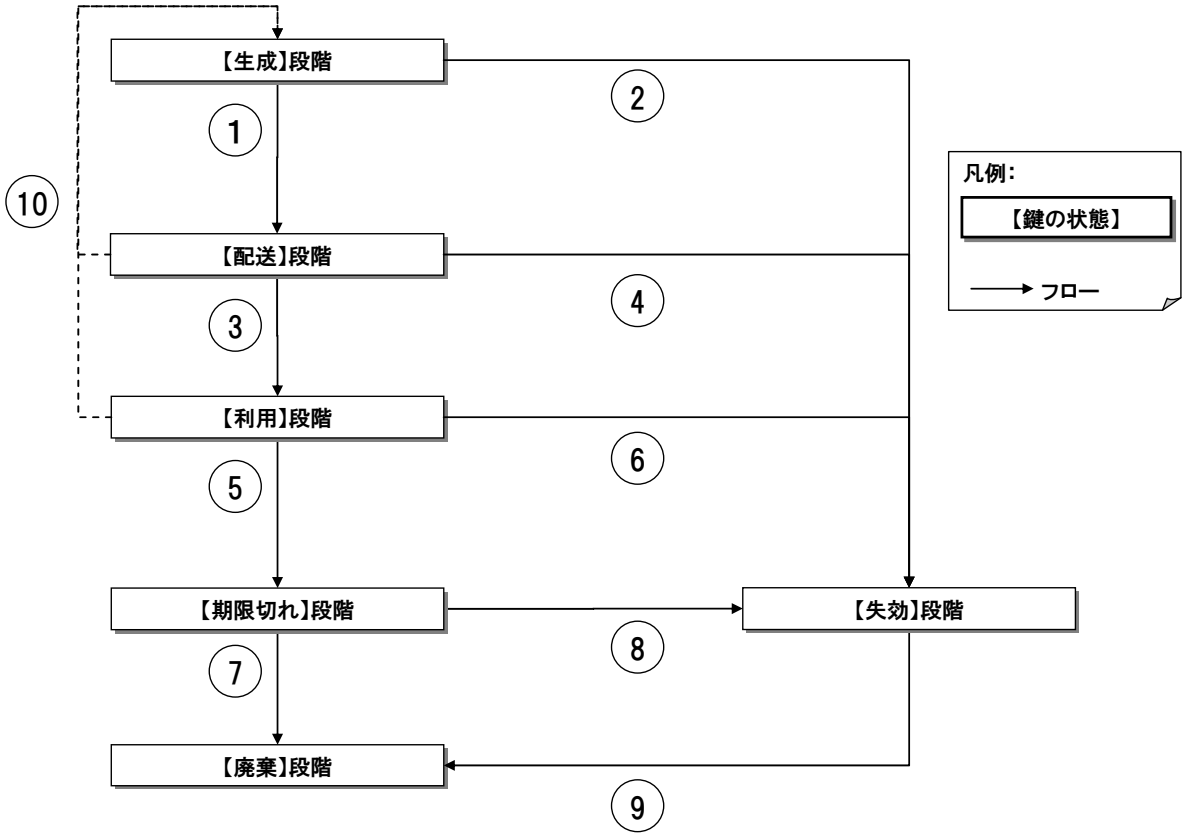


図 5-1 暗号鍵のライフサイクル

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。

5.2.5.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。

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。

5.2.6. 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。

5.2.7. PKI の CA 鍵管理に関するガイドライン（案）の作成

以上の検討内容を基に、ガイドライン（案）を作成した。特に一般的な項目を PKI における CA 鍵の管理について詳細化を行った（別添参照）。

5.3. まとめ

暗号の利用用途（PKI、機密文書管理、暗号通信、電子文書の長期保存、パスワード）を挙げ、一般的な暗号鍵の管理方針について検討を行った。暗号の鍵管理方針については、暗号鍵のライフサイクルの一般的なモデルを提示し、PKI における CA 鍵の管理について詳細化し、ガイドラインとして示した。暗号の鍵を管理する際には、DB やファイル等を用いることを想定し、マスター鍵による暗号化を行うこととした。

今後は、PKI 以外の応用用途に対してガイドラインを詳細化するとともに、一般的な管理方針について修正を行っていく必要がある。また、暗号の鍵管理はシステム用途、実装形態および運用状況により変化するといえる。このため、PDCA 等の確認と改善プロセスを含むようにガイドラインを修正していくことが望まれる。

6. 提言

今回の調査では、暗号の鍵管理に関する技術動向、標準化動向を調査した。また、暗号の鍵管理の実態についてヒアリング調査を実施した。さらに、暗号鍵のライフサイクルマネージメントに基づく暗号鍵管理のガイドライン（案）を作成した。

暗号の鍵管理に関する技術は、近年 ID ベース暗号等の新技術が盛んに検討されるようになってきている。これらの研究動向をウォッチするとともに、NIST SP や ISO 等の標準化団体の動向に関する情報収集を行い、電子政府推奨暗号リスト等へ反映するよう活動を進めるべきである。また、IPA においては、これら新技術の実用を推進し、電子政府や民間での利用を促進すべきである。

また、今回作成した暗号鍵管理のガイドライン（案）においては、PKI の CA 鍵管理に関するものであったが、今後はこのガイドライン（案）の更新を行うとともに、機密文書管理、暗号化通信、電子文書の長期保存、パスワード管理についてもガイドラインを作成していくことが課題である。そして、内閣官房情報セキュリティセンター（NISC）等と連携し、作成したガイドライン（案）を用いて、暗号の鍵管理について電子政府を中心として普及啓発活動を進めるべきである。また、IPA においては、一般のエンドユーザや企業等に対しても普及啓発を進めるべきである。

今後更新および作成を進めるガイドライン（案）においては、共通的な項目として、暗号鍵を記録する DB やファイル等を想定して、マスター鍵を用いた暗号化を行うとともに、マスター鍵の管理者の設置と管理方針を検討すること、ならびに、PDCA 等の確認および改善のプロセスを導入することが挙げられる。

以上まとめると、以下のようになる。

提言内容

- CRYPTREC 及び IPA は、暗号の鍵管理に関する研究動向および標準化動向を調査し、電子政府推奨暗号リストの見直しに資する情報収集を行なう。
- IPA は、ID ベース暗号等の新技術の実用化の促進を図るべきである。
- CRYPTREC として、PKI のみならず、暗号の応用用途（機密文書管理、通信路暗号化、電子文書の長期保存およびパスワード管理）それぞれに関してガイドラインを作成し、NISC 等と連携の上、電子政府の情報システム担当者および電子政府システムのエンドユーザを念頭において、普及啓発をはかる。
- IPA 殿においては、企業ならびに一般のエンドユーザ向け普及啓発活動に取り組む。
- また、それぞれのガイドラインにおいては、共通的に以下の事項を含むように記述することが望ましい。
  - システム構成を把握するとともに、システム内における暗号の使用部分を明確にする。
  - 利用している全ての秘密鍵またはパスワードを DB 等で管理する。
  - 秘密鍵またはパスワード等を管理する DB 等においては、暗号利用用途に応じたライフサイクルマネージメント機能を搭載したものが望ましい。
  - 秘密鍵またはパスワードを記録する DB は暗号化機能を有するものとし、記録データ（暗号化／復号鍵、パスワード）を暗号化する。
  - DB 等を暗号化した鍵（マスター鍵）は、組織の責任者が管理する。
  - マスター鍵は、必要に応じて IC カード等の耐タンパー性を有するハードウェアに保管する。
  - 鍵管理におけるライフステージにおいて、PDCA 等の確認と改善プロセスを導入する。

以上。