NIST Special Publication 800-175B
Revision 1

米国連邦政府での暗号標準利用のためのガイドライン：

暗号メカニズム

Elaine Barker

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-175Br1

コンピュータ セキュリティ

National Institute of Standards and Technology
U.S. Department of Commerce

この文書は以下の団体によって翻訳監修されています

IPA 独立行政法人 情報処理推進機構
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

NIST Special Publication 800-175B

Revision 1

米国連邦政府での暗号標準利用のためのガイドライン：

暗号メカニズム

Elaine Barker
コンピュータセキュリティ部門
情報技術研究所

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-175Br1

March 2020

米国商務省
Wilbur L. Ross, Jr.、長官

米国国立標準技術研究所
Walter Copan、NIST 標準技術局長兼商務次官

発行機関

本文書は、米国国立標準技術研究所（NIST：National Institute of Standards and Technology）によって、2014 年連邦情報セキュリティ近代化法（Federal Information Security Modernization Act (FISMA) of 2014）、合衆国法典（U.S. Code）第 44 編第 3541 条等、公法（P.L.）113-283 に基づく法的責任を推進するために策定された。NIST は、連邦情報システムの最小限の要求事項を含め情報セキュリティ標準及びガイドラインを開発する責務があるが、これらの標準及びガイドラインは、国家安全保障システムについての政策的権限を有する適切な連邦機関の明示的な承認を得ることなしには、国家安全保障システムに適用されてはならない。このガイドラインは、行政管理予算局（OMB：Office of Management and Budget）による通達（Circular）A-130 の要求事項に一致している。

本出版物における一切は、商務長官が法的権威に基づき連邦政府に対して義務及び拘束力を与えた標準及びガイドラインを否定するものではない。また、これらのガイドラインは、商務長官、行政管理予算局長、又は他の全ての連邦政府当局者の既存の権威に変更を加えたり、これらに取って代わったりするものと解釈すべきではない。本出版物は、非政府組織が自由意思で使用することもでき、米国における著作権の制約はないが、NIST に帰属する。

National Institute of Standards and Technology Special Publication 800-175B Revision 1
Natl. Inst. Stand. Technol. Spec. Publ. 800-175B Rev. 1, 91 pages (March 2020)
CODEN: NSPUE2

本出版物は、以下から無料で利用可能である：
https://doi.org/10.6028/NIST.SP.800-175Br1

本文書中で特定される商業的組織、装置、又は資料は、実験手順又は概念を適切に説明するためのものである。このような特定は、NIST による推奨又は同意を意味するものではなく、これらの組織、資料、又は装置が、その目的のために利用可能な最善なものであることを意味しているわけでもない。

与えられた法的責任に従い、NIST によって現在作成中のその他の文書への参照が本文書にあるかもしれない。本文書におけるその情報は、概念及び方法論を含め、このような関連文書の完成前であっても連邦政府機関によって利用されるかもしれない。したがって、それぞれの文書が完成されるまで、現在の要求事項、ガイドライン、及び手順が、存在する限り、運用の効力を有する。計画及び移行目的に関して、連邦政府機関は、NIST によるこれらの新しい文書の開発に密接に従うことを希望するかもしれない。

組織は、パブリックコメント期間中の全てのドラフト文書をレビューし、NIST へフィードバックを提供するよう奨励する。上記以外の多くの NIST サイバーセキュリティ文書は、http://csrc.nist.gov/publications から入手可能である。

本出版物へのコメントは以下で受け付ける：

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive（Mail Stop 8930）Gaithersburg, MD 20899-8930
Email: SP800-175@nist.gov

全てのコメントは、連邦情報公開法（FOIA）の下での公開対象である。

コンピュータシステムの技術に関する報告書

米国国立標準技術研究所（NIST：National Institute of Standards and Technology）情報技術研究所（ITL：Information Technology Laboratory）は、国家の計測及び標準に関する基盤において技術的リーダーシップを提供することにより、米国の経済及び社会福祉に貢献している。ITL は、テスト、テスト技法、参照データ、概念実証及び技術的分析の開発を通じて、情報技術の開発と生産的利用の発展に努めている。ITL の責務は、連邦政府の情報システムにおいて、国家安全保障に関連する情報以外の情報に対する費用対効果の高いセキュリティとプライバシーを実現するための、管理面、運用面、技術面及び物理面での標準及びガイドラインを策定することを含んでいる。本 Special Publication 800 シリーズは、情報システムセキュリティに関する ITL の調査、ガイドライン及び普及活動、ならびに産業界、政府機関及び学術機関との共同活動について報告する。

要旨

本文書は、デジタル化された機密ではない機微情報を送信中及び保管中に保護するために暗号技術及び NIST の暗号標準を使用する際のガイダンスを連邦政府に提供する。使用される暗号方法及びサービスについて説明する。

キーワード

非対称鍵アルゴリズム； ID 認証； 機密性； デジタル署名； 暗号化； 完全性； 鍵確立；メッセージ認証； 乱数ビット生成； 対称鍵アルゴリズム

謝辞

本文書の元となった NIST Special Publication (SP) 800-21[1]の著者である Annabelle Lee 氏と William C. Barker 氏をはじめ、本文書のドラフトをレビューし、その開発に貢献してくれた同僚（Lily Chen 氏、Kerry McKay 氏、NSA の Lydia Zieglar 氏）に感謝したい。また、公的機関ならびに民間の方々による、本刊行物の品質及び有用性を向上させる思慮深く建設的なコメントをいただいたことにも深く感謝の意を表する。

特許公開の通知

通知：情報技術研究所（ITL）は、本書のガイダンスや要件に準拠するために使用が必要となる可能性のある特許請求項の所有者に対し、その特許請求項を ITL に開示するよう要請している。しかし、特許保有者は ITL の特許募集に応じる義務はなく、ITL は本書に適用される特許があるとしても、それを特定するための特許調査を行っていない。

本書を発行し、本書のガイダンスや要件に準拠するために使用が必要となる可能性のある特許請求項を特定するための呼びかけを行った時点で、ITL はそのような特許請求項を特定していない。

ITL は、本書の使用において特許侵害を回避するためのライセンスが必要ないことを表明又は暗示するものではない。

---

[1] SP 800-21, *Guideline for Implementing Cryptography in the Federal Government*.

本文書は、原典に沿ってできるだけ忠実に翻訳するよう努めていますが、完全性、正確性を保証するものではありません。翻訳監修主体は、本文書に記載されている情報より生じる損失又は損害に対して、いかなる人物あるいは団体についても責任を負うものではありません。

目次

1 はじめに

1.1 概要と目的

今日の環境では、オープンで相互接続されたシステムやネットワークやモバイル端末の使用が日に日に増えている状況で、ネットワークとデータのセキュリティは IT を最も安全に使用するうえで非常に重要になっている。機微であり、価値が高い、もしくは伝送・保管時の無認可開示又は検知できない改ざんに脆弱なデータの保護のために暗号技術の使用を検討するべきである。

暗号は数学の一分野で、データ変換に基づいており、複数のセキュリティサービスを実現する手段である：機密性、ID 認証、データ完全性認証、情報源認証、及び否認防止のサポート

- *機密性*は、機微情報が認可されていないエンティティに開示されない特性のことである。機密性は、*暗号化*と呼ばれる暗号処理によって実現される。
- *データ完全性認証*（*完全性検証*とも呼ばれる）は、データが生成、伝送、もしくは保管された時点以降、認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確認するために使われる手段のことである。
- *ID 認証*は、システムとやり取りするエンティティの身元を保証するために使われる。
- *情報源認証*は、受信エンティティに対して情報源（すなわち、情報源のエンティティの身元）を保証するために使われる。情報源認証の特殊な形態に否認防止がある。これは情報源が正しいことを保証するためのサポートを第三者に提供するためのものである。

本文書は、機微だが機密ではないデジタル化された情報を伝送中又は保存中に暗号技術を用いて保護するためのガイダンスを連邦政府に提供することを目的とした一連の文書群の一部である。以下、“機微“という用語はこのクラスの情報を示す際に用いる。連邦政府以外の機関が自発的に本文書を使用することを歓迎する。以下は初版の SP 800-175 シリーズである。将来的に追加文書が発行される可能性もありうる。

- SP800-175A[2]では、暗号を利用する際の要求事項を満たすためのガイダンスを提供する。これには、連邦政府の機微情報を保護するために求められる法令や規則、保護対象の特定及び当該情報の最適な保護手法の判断するためのリスク評価の実施ガイダンス、及び要求されるセキュリティ関連文書（各種ポリシ、実践文書など）の解説が含まれる。
- SP800-175B（本文書）では、連邦政府の機微情報を保護するために利用可能な暗号化手法及びサービスを解説し、NIST 暗号標準の概要を紹介する。

1.2 対象読者

本文書は、連邦政府職員及び指定されたセキュリティ要求事項を満たす必要のある暗号サービスを提供又は利用することに責任を持つ者を対象としている。本文書は下記の者によって使用される：

- プログラムマネージャ：システムに暗号化手法を選定し組み込む責任を持つ者
- 技術スペシャリスト：特定の要求事項を満たす一つ以上の暗号化手法／暗号技術を選定することが求められる者

---

[2] SP 800-175A, *Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies.*

- 購買担当スペシャリスト：セキュリティ機能を実行するための暗号化手法を必要とするシステム、ネットワークもしくはサービスの要件を規定する者
- 暗号サービス利用者：

目的は、利用者一人一人に対して十分な情報を提供することで、システムやネットワークで伝送されたり保管されたりしているデータの機密性と完全性を保護し、その信頼性を保証するための特定の要件に合致する暗号化手法について十分な情報に基づいた決定ができるようにすることである。

本文書は、連邦政府の調達プロセスに関する情報、又は暗号技術もしくは暗号アルゴリズムの数学的な技術的考察を提供することを目的としたものではない。

1.3 範囲

本文書は、暗号化手法の範囲を、連邦情報処理標準（FIPS）と NIST 特別刊行物（SP）に準拠する、本文書で NIST“標準”と総称されている内容に限定する。連邦政府においては、適用可能な場合にはこれらの標準を使用することが求められ、産業界、国内標準化団体及び国際標準化団体もこれらの暗号化手法を採用している。

本文書は、新規システムもしくは既存システムにおいて暗号技術の選択及び使用に関する情報を示している。

1.4 背景

暗号の利用は 2 つの基本コンポーネントからなる：*アルゴリズム*と*鍵*である。アルゴリズムは数学的な関数で、鍵は暗号化処理の際に利用されるパラメータである。アルゴリズムと鍵は、データを暗号化保護（例：データを暗号化、もしくはデジタル署名を生成）する場合、及び保護を解除又は確認（例：暗号化されたデータを復号、もしくはデジタル署名を確認）する場合に一緒に用いられる。暗号化保護の安全性は鍵の機密性に依存する。安全性はアルゴリズムの機密性に左右されるべきではない。なぜならば、アルゴリズム仕様は公に利用可能なものであることもある。

暗号アルゴリズムを利用するには、全ての必要な暗号鍵が“所定の場所”になければならない（すなわち、鍵は暗号を使用しようとしているエンティティの間で確立されなければならない）。鍵は手動（例：信頼できる送付手段を使って）もしくは自動化された方法を使って確立することができる。しかし、自動化された方法が使われる場合は、参加エンティティに対して、確立された信頼基盤（例えば公開鍵基盤（PKI）、もしくは手動で配付された認証鍵）を活用した情報源認証が必須である。

一般的に、ある目的（例：デジタル署名生成）に使用された鍵は別の目的（例：鍵確立）に使用してはならない。なぜなら、2 つの異なる暗号化処理に同一鍵を利用すると、片方もしくは両方の処理の安全性を弱めることにつながることがあるからである。詳細については、SP 800-57 Part1[3]の 5.2 節を参照。

[3] SP 800-57 Part 1, *Recommendation for Key Management: General Guideline.*

1.5 用語及び定義

以下の用語及びその定義が本文書で使用される。通常、これらの定義は FIPS 及び NIST 特別刊行物から引用している。

Algorithm アルゴリズム	計算のために明確に指定された数学的プロセス；実行されればあらかじめ定められたとおりの結果を導き出すルール群のこと
Approved 承認	FIPS 承認や NIST 推奨のこと。アルゴリズム又は技法で、1）FIPS 又は NIST 推奨に記されているもの、もしくは 2）他の文書で規定されていて FIPS 又は NIST 推奨の参考文献に採用されているもの
Asymmetric-key algorithm 非対称鍵アルゴリズム	公開鍵アルゴリズムを参照
Authentication 認証	伝送又は保存された情報の情報源及び完全性の保証、もしくはシステムとやり取りをするエンティティの ID の保証を提供するプロセス。 一般的な用例では、“認証”という用語は情報源認証又は ID 認証の意味でしか使われないことに注意されたい。本文書では、必要に応じて、情報源認証、ID 認証、もしくは完全性認証という用語によって複数の使い分けをする
Bit string ビット列	0 と 1 から成る一続きの列
Block cipher algorithm ブロック暗号アルゴリズム	暗号鍵によってパラメータ化される関数及び逆関数の対であって、固定長のビット列を同じ長さのビット列に変換する関数
Certificate (or public key certificate) 証明書（もしくは公開鍵証明書）	エンティティを一意に識別する一連のデータで、エンティティの公開鍵及び他の情報を含み、信頼される組織によりデジタル署名され、その結果、公開鍵を証明書で特定されるエンティティに結合する。証明書の追加情報として、鍵用途と証明書の有効期間を規定できる
Certificate Revocation List (CRL) 証明書失効リスト（CRL）	認証局から発行された、期限切れ前に失効した証明書のリスト
Certification Authority (CA) 認証局（CA）	公開鍵基盤（PKI）の中のエンティティであって、証明書サブジェクトに証明書を発行し、PKI ポリシーに厳密に準拠する責任を担う
Ciphertext 暗号文	暗号化された形式のデータ
Compromise 危殆化	機微データ（例：秘密鍵、プライベート鍵、又は秘密メタデータ）の認可されない開示、改ざん、置換又は利用
Confidentiality 機密性	機微情報が認可されないエンティティへ開示されない性質（すなわち、鍵情報の機密性が確保されている）

Cross-certify
相互認証

2 つの認証局（CA）間で、互いの証明書の公開鍵の署名を通じて信頼関係が確立されること。“相互証明”とも呼ばれる

Cryptographic algorithm
暗号アルゴリズム

暗号鍵（存在する場合）を含む可変の入力を伴い、出力を生成するような、明確に定義された計算手順

Cryptographic boundary
暗号境界

暗号モジュールの物理的境界を定め、暗号モジュールの全てのハードウェアやソフトウェア、ファームウェアのコンポーネントを含む、明確に定義された連続する境界線

Cryptographic checksum
暗号チェックサム

暗号アルゴリズムを使用して生成される数学的な値であって、データに割り付けられ、後に当該データが変更されていないことを確認する際に使用するものである

Cryptographic hash function
暗号学的ハッシュ関数

任意の長さのビット列を固定長ビット列に写像する関数。**承認された**ハッシュ関数は以下の特性を満たす：

1. （一方向性）任意のあらかじめ指定された出力に写像する入力を見つけることが計算上実行不可能である。
2. （衝突困難性）同一の出力に写像される 2 つの別個の入力を見つけることが計算上実行不可能である。

Cryptographic key
暗号鍵

暗号アルゴリズムと共に用いられるパラメータであって、鍵の知識を持つエンティティが操作を再現又は逆演算できるが、鍵の知識を持たないエンティティはそれらができないような方法で、その処理を決定するもの。以下の例が含まれる：

1. 平文データから暗号文データへの変換
2. 暗号文データから平文データへの変換
3. データからのデジタル署名の計算
4. デジタル署名の検証
5. データからのメッセージ認証子（MAC）の計算
6. データと一緒に受信した MAC の検証
7. 鍵材料の導出に使用される共有秘密の計算

Cryptographic module
暗号モジュール

（暗号アルゴリズムと鍵生成を含む）**承認された**セキュリティ機能が実装されたハードウェアやソフトウェア、ファームウェアの集合であり、それは暗号境界内に含まれている

Cryptographic primitive
暗号プリミティブ

より高レベルの暗号アルゴリズムを作るための基本構成ブロックとして利用される低レベルの暗号アルゴリズム

Cryptography
暗号

機密性、データ完全性、情報源認証及び否認防止を含む情報セキュリティを実現する原理、手段、及び手法を体現する学問分野

Cryptoperiod
暗号利用期間

特定の鍵の使用が認可されている期間、もしくは特定のシステムにおいて鍵の有効性が残存している期間

Data integrity データ完全性	作成、伝送、又は保管された以降、認可されていない方法でデータが変更されていないことを示す特性
Data integrity authentication データ完全性認証	データの完全性を確認するプロセス。完全性認証や完全性検証とも呼ばれる
Decryption 復号	暗号アルゴリズムと鍵を用いて、暗号文を平文に変換するプロセス
Digital signature デジタル署名	データの暗号学的変換の結果であり、適切に実現された時、以下のサービスを提供する： 1. 情報源認証 2. データ完全性 3. 署名者の否認防止のサポート
Digital Signature Algorithm (DSA) デジタル署名アルゴリズム（DSA）	デジタル署名の生成と検証を行うために使用する公開鍵アルゴリズム
Domain parameters ドメインパラメータ	暗号アルゴリズムと共に、ユーザのドメインに共通して使用されるパラメータ
Elliptic Curve Digital Signature Algorithm (ECDSA) 楕円曲線デジタル署名アルゴリズム（ECDSA）	DSA と類似した、楕円曲線を使用するデジタル署名アルゴリズム
Encryption 暗号化	暗号アルゴリズムを用いて、セキュリティやプライバシーの目的のために平文を暗号文に変換するプロセス
Entity エンティティ	個人（人）、組織、デバイス、又はプロセス
Ephemeral key pair 一時的鍵ペア	公開鍵（非対称鍵）アルゴリズムと共に利用する短期の鍵ペアで、必要に応じて生成される。一時的鍵ペアの公開鍵は公開鍵証明書で提供されず、静的公開鍵がしばしば証明書に含まれるのとは異なる
Function 関数	本文書では、アルゴリズムの意味で用いる
Hash function ハッシュ関数	暗号学的ハッシュ関数を参照
Hash value ハッシュ値	情報にハッシュ関数を適用した結果；メッセージダイジェストとも呼ばれる
Identity authentication ID 認証	システムとやり取りをするエンティティの ID を保証するプロセス；情報源認証も参照
Initialization Vector (IV) 初期ベクトル（IV）	暗号プロセスの開始点を定義する際に使用するベクトル

Integrity 完全性	データが不正かつ検出されない方法で変更又は消去されていないことを示す特性
Integrity authentication (integrity verification) 完全性認証（完全性検証）	データの完全性を確認するプロセス。データ完全性認証とも呼ばれる
Interoperability 相互接続性	エンティティが他のエンティティと通信可能なこと
Key 鍵	暗号鍵を参照
Key agreement 鍵合意	二者の関係者が寄与した情報から秘密の鍵材料を生成する鍵確立手続きであって、他方の関係者の寄与なしに一方の関係者が秘密の鍵材料の値を予測することができないようになっている。鍵配送と対比されたい
Key confirmation 鍵確認	ある関係者に対して、他方の関係者が実際に同じ鍵材料や共有秘密を保有していることを、保証するために使用される手順
Key derivation 鍵導出	事前共有鍵又は鍵合意スキームで生成された共有秘密のいずれかから、その他の情報と共に鍵材料を導出するプロセス
Key establishment 鍵確立	複数のエンティティで共有する鍵材料をもたらすためのプロセス
Key information 鍵情報	鍵に関する情報であって、当該鍵に付随する鍵材料及び関連メタデータを含んでいる
Key management 鍵管理	鍵の生成，保管，確立、入力、出力、使用及び破棄を含む鍵のライフサイクル全体にわたり、暗号鍵及びその他の関連するセキュリティパラメータ（例：IV やカウンタ）の取扱いを含む行為
Key pair 鍵ペア	公開鍵及びその鍵に対応するプライベート鍵；鍵ペアは公開鍵（非対称鍵）アルゴリズムとともに用いる
Key transport 鍵配送	ある当事者（送信者）が秘密の鍵材料の値を選択した後、安全に他方の当事者（受信者）にその値を配付する鍵確立手順。鍵合意と対比されたい
Key wrapping 鍵ラッピング	対称鍵アルゴリズムを用いて鍵の機密性と完全性を暗号学的に保護する手法
Key-wrapping key 鍵ラッピング鍵	他の鍵の機密性と完全性を保護するために用いる対称鍵
Keying material 鍵材料	暗号アルゴリズムで使用される暗号鍵及びその他のパラメータ（例：IV やドメインパラメータ）。

	鍵材料が SP 800-56C[4]及び SP 800-108[5]で定義したとおりの方法で導出された場合、データは次のようなビット列で表現される：ビット列のどの部分であっても重複しないで抜き取る限り、任意長のビット列は秘密鍵、秘密初期化ベクトル、及び他の秘密パラメータとして使用できる
Keying relationship, cryptographic 鍵関係（暗号）	少なくとも 1 つの暗号鍵を共有している 2 つのエンティティ間に存在する状態
Message Authentication Code (MAC) メッセージ認証コード（MAC）	データの偶然及び意図的な改変の両方を検出するために**承認された**セキュリティ関数及び対称鍵を使用した、データに対する暗号学的チェックサム
Message digest メッセージダイジェスト	ハッシュ値を参照
Metadata メタデータ	鍵に付随している情報で、具体的な特性、制約条件、受入れ可能な用途、所有者等について記述したもの。鍵属性と呼ばれることもある
Mode of operation 暗号利用モード	ブロック暗号アルゴリズムを暗号化プリミティブとして使用し、機密性や認証などの暗号サービスを提供するアルゴリズム
NIST standard NIST 標準	連邦政府情報処理標準（FIPS）や特別刊行物（SP）
Non-repudiation 否認防止	あるメッセージが所与のエンティティにより実際に署名されたかどうかの判断を支援するために使用されるデジタル署名を用いるサービス
Owner of a certificate 証明書の所有者	必要な場合に、証明書の要求、交換、及び失効を行うことを含む証明書の管理に責任を持つエンティティ。証明書の所有者は、必ずしも証明書の公開鍵に関連するサブジェクトエンティティ（すなわち、鍵ペア所有者）であるとは限らない
Owner of a key or key pair 鍵又は鍵ペアの所有者	対称鍵又は鍵ペアのプライベート鍵を使用することが認められた一つ以上のエンティティ
Plaintext 平文	暗号化されていないデータ。意味を持っており、復号の適用なしに理解可能な、分かりやすいデータ
Pre-shared key 事前共有鍵	安全な方法（例：安全な手動配付プロセスや自動鍵確立スキーム）を用いて、利用を認可された当事者間で事前に確立された秘密鍵
Primitive プリミティブ	暗号プリミティブを参照
Private key プライベート鍵	公開鍵暗号アルゴリズムで使用され、一意にエンティティに関連付けられ、公開されない暗号鍵。非対称（公開鍵）暗号系で

[4] SP 800-56C, *Recommendation for Key Derivation through Extraction-then-Expansion.*
[5] SP 800-108, *Recommendation for Key Derivation Using Pseudorandom Functions.*

	は、プライベート鍵は公開鍵と対応する。アルゴリズムに依存するが、プライベート鍵は、以下のように利用される： 1. 対応する公開鍵を算出する 2. 対応する公開鍵によって検証されるデジタル署名を作成する 3. 対応する公開鍵によって暗号化されたデータを復号する 4. 鍵合意プロセスにおいて共有秘密を計算する
Protocol プロトコル	2 つ以上の通信エンティティが用いる一連のルールで、それらのエンティティ間で交換する情報のメッセージ順序及びデータ構造を規定する
Public key 公開鍵	公開鍵（非対称鍵）暗号アルゴリズムで使用され、一意にエンティティに関連付けられ、公開される暗号鍵。非対称鍵（公開鍵）暗号系では、公開鍵はプライベート鍵に対応する。公開鍵は誰でも知らされ得るもので、アルゴリズムに依存するが、以下のように利用される： 1. 対応するプライベート鍵により署名されたデジタル署名を検証する 2. 対応するプライベート鍵を用いて復号可能なデータに暗号化する 3. 鍵合意プロセスにおいて共有秘密を計算する
Public key (asymmetric-key) cryptographic algorithm 公開鍵（非対称鍵）暗号アルゴリズム	公開鍵及びプライベート鍵の 2 つの関連する鍵を使う暗号アルゴリズム。2 つの鍵には、公開鍵からプライベート鍵を求めることが計算上実行不可能であるという特性を有する
Public Key Infrastructure (PKI) 公開鍵基盤（PKI）	公開鍵証明書を発行し、維持し、かつ失効するために確立されるフレームワーク
Random bit generator (RBG) 乱数ビット生成器（RBG）	統計的に独立で、偏りが表れていないビット列を出力するデバイス又はアルゴリズム
Relying party 依拠者	証明書及び証明書を発行する CA に依存するエンティティ。その証明書を使って、当該証明書の所有者の身元と、当該証明書内の公開鍵、関連するアルゴリズム及びその他関係するパラメータの有効性、並びに当該証明書の所有者が対応するプライベート鍵を所持していることを検証する
RSA RSA	鍵確立、及びデジタル署名の生成と検証に用いる公開鍵アルゴリズム
Scheme スキーム	適切に実装され、維持されている場合に、(暗号) サービス（例：鍵確立）を提供する明確に規定された一連の変換方法。スキームは、プリミティブより上位、かつプロトコルよりも下位の構造体である

Secret key 秘密鍵	対称（秘密鍵）暗号アルゴリズムで使用され、公開されない（すなわち、秘密に保たれる）単一の暗号鍵。秘密鍵は対称鍵とも呼ばれる。 この文脈での“秘密”という用語の使用は、格付けレベルを意味するのではなく、暴露から鍵を保護する必要性を示している。 公開鍵（非対称鍵）アルゴリズムで使用するプライベート鍵と対比されたい
Secret-key (symmetric) cryptographic algorithm 秘密鍵（対称）暗号アルゴリズム	対称（秘密鍵）アルゴリズムを参照
Sensitive (information) 機微（情報）	機微だが機密ではない情報
Security function セキュリティ機能	暗号アルゴリズム及び暗号利用モード（該当する場合）のこと；例えば、ブロック暗号アルゴリズム、デジタル署名アルゴリズム、非対称鍵確立アルゴリズム、メッセージ認証コード、ハッシュ関数、もしくは乱数ビット生成器。FIPS 140[6]を参照
Security strength セキュリティ強度	暗号アルゴリズム又はシステムを破るために必要とされる作業量（すなわち、操作数）に関連する数値
Server サーバ	ネットワーク上のコンピュータ又はデバイスであり、ネットワークリソースを管理する。例えば、ファイルサーバ（ファイルを保管する）、プリンタサーバ（一つ以上のプリンタを管理する）、ネットワークサーバ（ネットワークトラフィックを管理する）、及びデータベースサーバ（データベースへの検索を処理する）が含まれる
Shall ～しなければならない	この用語は、本推奨への適合性を主張するために満たすことが必要な要件を示す際に用いる。「**～しなければならない**」は否定形で示されることもあり、その場合は「**～してはならない**」になることに留意されたい
Shared secret 共有秘密	（ペア間の）鍵合意処理中に計算される秘密の値であり、鍵導出方法を使って鍵を導出するための入力として使用される
Should ～すべきである	**太字**で示されているときには、この用語は重要な推奨を表すために使われる。この推奨を無視すると好ましくない結果を招く可能性がある。「**～すべきである**」は否定形で示されることもあり、その場合は「**～すべきでない**」になることに留意されたい
Signature generation 署名生成	デジタル署名アルゴリズムとプライベート鍵を用いて、データに対するデジタル署名を作成する
Signature verification 署名検証	デジタル署名アルゴリズムと公開鍵を用いて、データに対するデジタル署名を検証する

[6] FIPS 140, *Security Requirements for Cryptographic Modules.*

Source authentication 情報源認証	情報源についての保証を提供するプロセス。データ作成者認証と呼ばれることもある。ID 認証と比較されたい
Static key pair 静的鍵ペア	しばしば公開鍵証明書で公開鍵として提供される、長期の鍵ペア
Symmetric key 対称鍵	対称（秘密鍵）アルゴリズムで使用される単一の暗号鍵であり、一意に一つ以上のエンティティに関連付けられ、公開されない（すなわち、当該鍵は秘密に保たれる）；対称鍵はよく秘密鍵とも呼ばれる
Symmetric-key (secret-key) algorithm 対称鍵（秘密鍵）アルゴリズム	ある処理とその逆処理（例：暗号化と復号）に同じ秘密鍵を使用する暗号アルゴリズム。鍵は秘密に保たれ、秘密鍵もしくは対称鍵と呼ばれる

1.6 頭字語

AES	Advanced Encryption Standard；FIPS 197[7]で規定されている
ANS	American National Standard（米国標準規格）
ANSI	American National Standard Institute（米国規格協会）
ASC	Accredited Standards Committee（認定標準委員会）
CA	Certification Authority（認証局）
CBC	Cipher Block Chaining mode；SP 800-38A[8]で規定されている
CFB	Cipher Feedback mode；SP 800-38A で規定されている
CKMS	Cryptographic Key Management System（暗号鍵管理システム）
CP	Certificate Policy（証明書ポリシー）
CPS	Certification Practice Statement（証明書実践ステートメント）
CRL	Certificate Revocation List（証明書失効リスト）
CTR	Counter Mode；SP 800-38A で規定されている
DES	Data Encryption Standard；元々は FIPS 46 で規定されていたが、現在では SP 800-67[9]で規定されている
DH	Diffie−Hellman アルゴリズム
DNSSEC	Domain Name System Security Extensions（ドメインネームシステムセキュリティ拡張）

---

7 FIPS 197, *Advanced Encryption Standard (AES).*
8 SP 800-38A, *Recommendation for Block Cipher Modes of Operation: Methods and Techniques.*
9 SP 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher.*

DRBG	Deterministic Random Bit Generator（決定論的乱数ビット生成器）；SP 800-90A[10]で規定されている
DSA	Digital Signature Algorithm（デジタル署名アルゴリズム）；FIPS 186[11]で規定されている
ECB	Electronic Codebook mode；SP 800-38A で規定されている
ECDSA	Elliptic Curve Digital Signature Algorithm（楕円曲線デジタル署名アルゴリズム）+
EMC	Electromagnetic Compatibility（電磁環境適合性）
FCKMS	Federal Cryptographic Key Management System（連邦政府暗号鍵管理システム）
FIPS	Federal Information Processing Standard（連邦情報処理基準）
FISMA	Federal Information Security Management Act（連邦情報セキュリティ管理法）
GCM	Galois Counter Mode；SP 800-38D[12]で規定されている
HMAC	Keyed-Hash Message Authentication Code（鍵付きハッシュメッセージ認証コード）；FIPS 198[13]で規定されている
IEC	International Electrotechnical Commission（国際電気標準会議）
IEEE	Institute of Electrical and Electronics Engineers（米国電気電子学会）
IETF	Internet Engineering Task Force（インターネットエンジニアリングタスクフォース）
EMI	Electromagnetic Interference（電磁干渉）
INCITS	International Committee for Information Technology Standards（情報技術規格国際委員会）
IPSEC	Internet Protocol Security
ISO	International Organization for Standardization（国際標準化機構）
IT	Information Technology（情報技術）
KMAC	KECCAK Message Authentication Code（KECCAK メッセージ認証コード）；SP 800-185[14]で規定されている
MAC	Message Authentication Code（メッセージ認証コード）

[10] SP 800-90A, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators.*
[11] FIPS 186, *Digital Signature Standard (DSS).*
[12] SP 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.*
[13] FIPS 198, *Keyed-Hash Message Authentication Code (HMAC).*
[14] SP 800-185, *SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash and ParallelHash.*

MQV	Menezes–Qu–Vanstone アルゴリズム；SP 800-56A[15]で規定されている
NRBG	Non-deterministic Random Bit Generator（非決定論的乱数ビット生成器）
NIST	National Institute of Standards and Technology（国立標準技術研究所）
OFB	Output Feedback mode；SP 800-38A で規定されている
OMB	Office of Management and Budget（行政予算管理局）
OTAR	Over-the-Air-Rekeying
PKI	Public Key Infrastructure（公開鍵基盤）
RA	Registration Authority（登録局）
RBG	Random Bit Generator（乱数ビット生成器）
RFC	Request for Comment
RSA	Rivest、Shamir、Adleman に由来する公開鍵アルゴリズム
ROTs	Roots of Trust（信頼起点）
SHA	Secure Hash Algorithm
SP	Special Publication（特別刊行物）
SSH	Secure Shell protocol
TCG	Trusted Computing Group
TDEA	Triple Data Encryption Algorithm；SP 800-67 で規定されている
TLS	Transport Layer Security
TPM	Trusted Platform Module

1.7 文書構成

本文書は、以下の節で構成される：

- 1 節では、SP 800-175 シリーズの出版物、特に本文書の紹介を行い、用語集と頭字語リストを提供する
- 2 節では、暗号に関連する標準の重要性、及び国内と国際標準化団体について述べる。
- 3 節では、暗号化、デジタル署名、及び鍵確立に関する承認されたアルゴリズムを紹介する。また、セキュリティ強度とアルゴリズムの寿命に関する議論を提供する。
- 4 節では、暗号が提供する以下のサービスについて述べる：例えば、データ機密性、データ完全性認証、ID 認証、情報源認証、及び否認防止のサポート、など。

---

[15] SP 800-56A, *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography.*

- 5 節では、暗号を使用する際に求められる鍵管理について述べ、鍵管理システム、鍵確立メカニズム及び乱数ビット生成に関する一般的なガイダンスと議論を紹介する。
- 6 節では、暗号の利用に関連する追加の課題について述べる。
- 参考文献の節では、適用可能な連邦情報処理標準、NIST 推奨及びガイドラインのリストを示す。
- Appendix A では、本文書の初版以降の更新履歴を示す。

2 標準及びガイドライン

2.1 標準化のメリット

標準は共通的な実践、手法、測定、及び評価基準を定めている。標準はそれぞれの分野の専門家により評価され、公開レビューを経て、その結果、多くのユーザコミュニティに受け入れられたソリューションを提示している。標準を使うことで、組織はコストを削減し、技術への投資を保護することができる。

標準は、以下のメリットを提供する：

- **相互接続性**。特定の標準に準拠した製品は、同じ標準に準拠した他の製品との相互接続性を提供するために使うことができる。例えば、同じ暗号アルゴリズムを使っていれば、A 社の製品を使って暗号化したデータを B 社の製品で復号することができる。製品の相互接続性を保証するには、同じ標準に準拠した暗号アルゴリズムを使うことは必要であるが十分ではない。他の標準、例えば通信プロトコル標準なども共通していることが必要な場合もある。

  標準化により異なるベンダの製品間の相互接続性を保証することで、組織は利用可能な様々な製品から選択して最も費用対効果の高いソリューションを見つけることができるようになる。

- **セキュリティ**。標準は共通のセキュリティレベルを保つために使用される。例えば、機関の管理者のほとんどは暗号セキュリティ専門家ではない。しかし、**承認された**暗号アルゴリズムと鍵長を使うことで、当該アルゴリズムが政府の機微情報の保護に適しており、十分な期間にわたって公開された解析とコメントの対象となってきたことを管理者は認識することができる。

- **品質**。標準を使うことで、製品の品質を確保することができる。標準は、以下のようなことを実現できる：

  - どのように機能を実装したらよいか規定する。
  - 製品が正しく機能し続けていることを保証するための自己テストを要求する。
  - 適切な実装及び製品変更管理を保証するために具体的な文書を要求する。

  NIST 標準の多くは関連する適合性テストが用意されており、適合性要件が規定されている。適合性テストは NIST が認定した試験機関で実施され、NIST 標準が正しく実装されていることの認証を提供することができる。

- **共通形式のリファレンス**。NIST 標準は共通形式のリファレンスとして、ベンダ製品の試験又は評価を行う際に利用する。例えば、FIPS 140 には、暗号処理を実装するあらゆる暗号モジュールに求められるセキュリティと完全性の要求事項を含んでいる。

- **コスト削減**。標準が提供されていて、共通して受け入れられた仕様に準拠した実装を使うことでコストを抑制することができる。標準がないと、ユーザは調達を検討する全ての IT 製品の専門家になる必要があるかもしれない。また、標準なしには、その製品は他のユーザが購入した他の製品との間で相互接続できないかもしれない。このことは巨額な浪費を生むか、もしくは IT ソリューションの導入の遅延につながる可能性がある。

2.2 連邦情報処理標準及び特別刊行物

2.2.1 FIPS 及び SP の利用

連邦政府には、機微情報を保護するために連邦政府機関が連邦情報処理標準（FIPS）に定められている機能類を求める場合にはいつでも、FIPS の利用が*義務付け*られている [16]。例えば、FIPS 197 には AES アルゴリズムについての具体的な技術的セキュリティ要件群が含まれている。機関が AES を利用する際にはいつでも、FIPS 197 に準拠するように実装及び利用しなければならない。FIPS は商務長官により**承認されて**いる。

NIST 特別刊行物（SP）は FIPS に類似しているものの、特定の政府機関（例えば行政管理予算局（OMB））がこれを義務付けした場合を除いて、必須ではない。SP は商務長官の承認を必要としない。

FIPS と SP の使用に関する要件は異なっているが、両方の文書とも連邦政府機関によるレビュー及びパブリックレビューのプロセスを同じように受ける。FIPS の承認プロセスの方が SP のそれより正式なものであることから、最初の承認及び改訂版の承認にはより時間を要する。NIST 標準及びガイドラインの完全な制定プロセスに関しては、NIST 7977[17]を参照されたい。

連邦政府機関が暗号の使用（例：暗号化）を求める場合、**承認された**アルゴリズムを使用しなければならない。承認されたものであることは、FIPS 又は SP に記されることによって示される。例えば、AES（FIPS 197 に定義されている）は**承認された**アルゴリズムである。連邦政府機関が機微情報の保護のために暗号化を使用する場合、**承認された**暗号アルゴリズムを指定されたとおりに実装して使用しなければならない。**承認された**アルゴリズムを使うだけでなく、連邦政府機関は、当該アルゴリズムの実装が認証され、かつ認証された暗号モジュールに含まれているものだけを利用することが要求される（詳細は 5.4.5 節を参照）。

暗号メカニズム又は暗号サービスの選択にあたっての仕様又は基準を定めるとき、利用可能な場合には、FIPS 及び SP で定められた暗号アルゴリズムを利用しなければならない。一部のガイドライン（例：FIPS 199[18]や SP 800-53[19]）では、アルゴリズムが実行する機能を規定するために利用されることがある。他の NIST 標準では、具体的な種類のアルゴリズム（例：AES や ECDSA）の処理と利用、及びセキュリティ環境の種類に要求される独立した試験のレベル（例：FIPS 140）を規定する。

付録 A には、連邦政府による暗号技術の実装に適用される FIPS 及び SP のリストが含まれる。"FIPS が改訂されると、一般に資料番号の後に改訂回数を表す版番号が付加されることに留意されたい（例：“FIPS 186-4”という記述は FIPS 186 の第 4 版のことを示すために使われる）。SP が改訂されると、資料番号の後に更新状態の表示（すなわち、Rev. 1）が付加される。この表記法は本文書の本体では利用されないので、読者は正式に**承認された** FIPS 又は SP の最新版を参照しなければならない（http://csrc.nist.gov/publications/を参照。なお、このサイトには明確にマークされたドラフト版も含まれていることに注意されたい）。

2.2.2 NIST 組織間／内部レポート

NIST が作成するもう一つの出版物が NIST 組織間／内部レポート（NISTIR）である。これは、NIST（内部）で、又は他の機関と共同（組織間）で作成する公開文書である。NISTIR は、しばしば、今後

---

[16] FISMA 2002 を改正した FISMA 2014 及び行政管理予算局（OMB）回覧（Circular）A-130, Appendix III による。また、公法 107-347 を拡張した公法 113-283 も参照されたい。

[17] NIST 7977, *NIST Cryptographic Standards and Guidelines Development Process.*

[18] FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems.*

[19] SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations.*

の FIPS 及び SP をサポートする研究状況を紹介するために用いられる。ただし、これらの文書類での論点は、本文書（すなわち、SP 800-175B）の対象外とする。

2.2.3 FIPS 除外規定

過去に、機関によっては FIPS の利用を要求しないことを示すために、当該機関が除外規定を発行することが時々あった。しかしながら、2002 年連邦情報セキュリティ管理法（FISMA of 2002 (P.L. 107-347)）により、過去に認められた FIPS 除外規定の根拠条項が削除された。除外規定の禁止（大統領によるものを除く）は、その後のサイバーセキュリティに関する法的措置に対しても適用されている（法的必須要件や行政指令に関しての説明は SP 800-175A を参照）。

2.3 他の標準化組織

NIST は、セキュリティ製品、コンポーネント及びモジュールを開発しているベンダが活用する標準やガイドラインを制定する。それらの製品は、連邦政府機関が調達し、使用する。さらに、NIST 以外にも標準を制定し公開する団体もある。以下にそれらの組織の概略を記す。

2.3.1 米国規格協会[20]（ANSI）

米国規格協会（ANSI）は、米国の民間の自主的な標準化システムの管理及び調整を行う組織である。ANSI は米国の国内規格そのものを制定するわけではない；むしろ、資格を持つグループ間でのコンセンサスを確立することによって標準の開発を促進している。

ANSI の複数の委員会で暗号を利用した標準を制定しているが、暗号アルゴリズムそのものの標準を制定する主な委員会は認定標準委員会（ASC）X9[21]であり、金融業界の委員会である。

ASC X9 が制定した多くの標準が NIST 標準に採用されている（例：米国国内標準 X9.62[22]で規定された楕円曲線デジタル署名アルゴリズムは FIPS 186 で採用された）。同様に、ASC X9 は、ASC X9 以外を源とする承認された標準の登録簿によって NIST 標準の利用を承認している（例：FIPS 197 に規定されている AES）。

いくつかの ASC X9 標準は、他の標準化団体の標準にも組み入れられている。例えば、国際標準化機構（ISO）（2.3.4 節を参照）があり、情報技術標準国際委員会（INCITS）と呼ばれる技術諮問グループ（TAG）を通して実現している。INCITS は、米国標準（例：NIST が制定した標準と ASC X9 が制定した標準の両方）が ISO 標準に組み入れられるように請け負う責任がある。

2.3.2 米国電気電子学会（IEEE）標準化協会[23]

IEEE は国際的な専門家学会であり、技術革新と卓越した技術の発展に貢献している。IEEE の技術的目的は、電気・電子・コンピュータ工学、及びコンピュータサイエンスの理論と実践を発展させることに焦点を当てている。IEEE は、最先端の電気技術を含む、コンセンサスに基づいた産業標準を自主

---

[20] 詳細は ANSI のウェブサイトを参照：www.ansi.org

[21] 詳細は ANSI X9 のウェブサイトを参照：x9.org

[22] ANS X9.62, *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).*

[23] 詳細は IEEE-SA のウェブサイトを参照：standards.ieee.org

的に制定し、普及させている。IEEE は国際標準化を支援しており、世界的に受け入れられる標準の制定を奨励している。

米国電気電子学会標準化協会（IEEE-SA）は、国際標準を開発するための IEEE 内の組織である。1,000 以上の活動中の標準規格があり、そのうちのいくつかは暗号と関連している。

IEEE 1363[24]は暗号に焦点を当てた唯一の IEEE 標準であり、公開鍵暗号に関する一連の標準が含まれている。IEEE 1363 は、ASC X9（2.3.1 節を参照）が制定した ANSI 公開鍵暗号標準の多くと同時期に制定された。

- IEEE 1363 標準の初版は 2000 年に発行され、2004 年に改訂され IEEE 1363a[25]となった。これは、基本的な公開鍵暗号スキーム、例えば RSA 暗号、デジタル署名、デジタル署名アルゴリズム（DSA）、及び有限体上と楕円曲線上の Diffie-Hellman（DH）並びに Menezes-Qu-Vanstone（MQV）を利用した鍵確立などを含んでいる。
- IEEE 1363.1[26]は 2008 年に発行され、NTRU 暗号スキームと NTRU 署名スキームを規定している。
- IEEE 1363.2[27]も 2008 年に発行された。これはパスワード認証鍵合意スキーム及びパスワード認証鍵回復スキームを規定している。

IEEE 1363.1 及び 1363.2 にて規定されたスキームは NIST 標準には含まれていない。

暗号スキームは他のアプリケーションのための IEEE 標準に使用されている。特筆すべきものの一つは IEEE 802 LAN/MAN[28]標準群であり、これらは有線ネットワーク（イーサネット）及び無線ネットワーク（IEEE 802.11[29]）の両方のコンピュータネットワーク標準として広く使用されている。暗号アルゴリズムは無線通信を保護するために使用されている。認証と機密性のために SP 800-38C[30]で規定された CCM モードは、IEEE 802.11 から採用されたものである。他の AES 暗号利用モード（例：SP 800-38D で規定されている GCM）も、IEEE 802 標準で使われている。IEEE 802 標準はまた、FIPS 180[31]で規定されているハッシュ関数 SHA-1 と SHA-2 ファミリーを、FIPS 198 で規定されている HMAC の中で使用している。

XTS は SP 800-38E[32]で規定されたブロック暗号利用モードであり、IEEE 1619[33]から採用されたものである。

---

[24] IEEE 1363, *Standard Specifications for Public-Key Cryptography.*
[25] IEEE 1363a, *Standard Specifications for Public Key Cryptography - Amendment 1: Additional Techniques.*
[26] IEEE 1363.1, *Public-Key Cryptographic Techniques Based on Hard Problems over Lattices.*
[27] IEEE 1363.2, *Password-Based Public-Key Cryptography.*
[28] LAN/MAN: Local Area Network (LAN) and Metropolitan Area Network (MAN)
[29] IEEE 802.11, *Wireless Local Area Networks.*
[30] SP 800-38C, *Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality.*
[31] FIPS 180, *Secure Hash Standard (SHS).*
[32] SP 800-38E, *Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices.*
[33] IEEE 1619, *Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices.*

2.3.3 インターネットエンジニアリングタスクフォース[34]（IETF）

インターネットエンジニアリングタスクフォース（IETF）は、インターネットアーキテクチャとその技術やプロトコルに関連しているネットワーク設計者、オペレータ、ベンダ、研究者、及び技術者で構成される国際団体である。IETF の公式技術仕様又は推奨は、Request for Comments （RFC）と呼ばれる。

IETF の技術的作業はワーキンググループ内で行われ、それらはトピックごとに、ルーティング、トランスポート、セキュリティなどのいくつかの分野に分かれて組織される。セキュリティ分野では、セキュリティプロトコルやアプリケーションのために異なるセキュリティメカニズムを開発する必要があるときには、別のワーキンググループが構成される。例えば：

1. PKIX（公開鍵基盤 X.509）ワーキンググループ（PKIX-WG）は、X.509 プロトコルに基づく公開鍵基盤をサポートするための技術仕様及び推奨を制定した[35]。これは信頼及び認証のサービス基盤を構築するために利用する。
2. IPSEC（インターネットプロトコルセキュリティ）ワーキンググループは、ネットワークデバイス間の安全なルーティングに関するプロトコル及びその他の技術推奨を制定した。
3. TLS（トランスポート層セキュリティ）ワーキンググループは、サーバ・クライアント間の通信におけるセキュリティサービスを提供するための通信プロトコル及び技術推奨を規定した。

NIST 承認暗号アルゴリズム（ブロック暗号利用モード、ハッシュ関数、鍵確立スキーム、デジタル署名など）は、様々な IETF プロトコルに使用されている。例えば、RFC 5288[36]では、TLS 用に SP 800-38D に基づいた AES Galois Counter Mode（GCM）暗号スイートを規定している。

2.3.4 国際標準化機構[37]（ISO）

ISO は非政府組織であり、各国の標準化団体からなる世界的な連合体である。そのミッションは、国際標準規格を制定することで、産業をより効率的かつ効果的にすることの支援を行うことである。ISO 標準は、食品安全からコンピュータ、また農業からヘルスケアまで、技術及びビジネスのほぼすべての分野にわたりカバーしている。世界中から集まった専門家が、それぞれの出身国やリエゾン組織が要求する標準を、コンセンサスプロセスを通して制定していく。

ISO/IEC JTC 1 は、国際標準化機構（ISO）と国際電気標準会議（IEC）の合同技術委員会である。ISO/ITC JTC1 SC27 は、IT セキュリティに関連する小委員会である。ワーキンググループ 2（WG2）は、暗号とセキュリティメカニズムの標準を制定するグループである。通常 20 以上のプロジェクトが実行されており、既存標準の改訂や新しい標準の制定を進めている。各標準規格は複数のパートから構成されていて、それぞれのパートは複数のアルゴリズムやメカニズムが含まれる。

FIPS 及び SP の暗号アルゴリズムとスキームは、通常、他の国が提案した数多くのアルゴリズムとともに ISO/IEC 標準に含まれる。以下の ISO/IEC 標準リストは、NIST 標準に規定された暗号アルゴリズム及びスキームを含んでいるものである。

---

[34] 詳細は IETF のウェブサイトを参照：https://www.ietf.org/

[35] X.509, *Information technology - Open Systems Interconnection -The Directory: Public-key and attribute certificate frameworks.*

[36] RFC 5288, *AES Galois Counter Mode (GCM) Cipher Suites for TLS.*

[37] 詳細は ISO のウェブサイトを参照：https://www.iso.org/

1. ISO/IEC 9797-1、*情報技術－セキュリティ技術－メッセージ認証コード（MAC）－第 1 部：ブロック暗号を用いたメカニズム*
2. ISO/IEC 9797-2、*情報技術－セキュリティ技術－メッセージ認証コード（MAC）－第 2 部：専用ハッシュ関数を用いたメカニズム*
3. ISO/IEC 10116、*情報技術－セキュリティ技術－n ビットブロック暗号の暗号利用モード*
4. ISO/IEC 10118-3、*情報技術－セキュリティ技術－ハッシュ関数－第 3 部：専用ハッシュ関数*
5. ISO/IEC 11770-3、*情報技術－セキュリティ技術－鍵管理－第 3 部：非対称技術を用いたメカニズム*
6. ISO/IEC 11770-6、*情報技術－セキュリティ技術－鍵管理－第 6 部：鍵導出*
7. ISO/IEC 14888-2、*情報技術－セキュリティ技術－アペンディクス付きデジタル署名－第 2 部：整数因数分解に基づくメカニズム*
8. ISO/IEC CD 14888-3、*情報技術－セキュリティ技術－アペンディクス付き電子署名－第 3 部：離散対数に基づくメカニズム*
9. ISO/IEC 18033-3、*情報技術－セキュリティ技術－暗号アルゴリズム－第 3 部：ブロック暗号*
10. ISO/IEC 19772、*情報技術－セキュリティ技術－認証暗号*

2.3.5 トラステッドコンピューティンググループ（TCG）

トラステッドコンピューティンググループ（TCG）は、信頼起点を構築する一連の産業標準を制定し推進している。信頼起点（RoT）は、ハードウェア、ファームウェア、及びソフトウェアコンポーネントであり、特定の極めて重要で欠かせないセキュリティ機能を実行するために本質的に信頼されるものである。なぜなら RoT による不正行為は検知されない可能性があるので、それらは設計上安全でなければならない。RoT が信頼できて改ざんに対する耐性があることを確実にするために、RoT はハードウェアに実装されているか、又はハードウェアによって保護されていることが多い。

TCG で制定された産業標準は、信頼起点の一連の基本となる能力を定義しており、それら信頼起点を様々なアーキテクチャ及びユースケースでどのように使用するかを示している。TCG 技術及び仕様がサポートするユースケースの多くは、以下の 1 つ以上の分野に注力している：1）デバイス個体識別、2）暗号鍵又は資格情報の保管、3）システム状態の証明

TCG が制定した標準を支える技術は、企業レベルでのクライアントとサーバ、ストレージデバイス、組込システム、及び仮想デバイスとして展開される。TCG に関連する標準及び仕様群には以下のものがある：

- Trusted Platform Modules（TPM）：TPM は暗号化モジュールであり、他の機能の中でも、デバイス個体識別をプラットフォーム内に確立し、鍵と資格情報の安全な保管を提供し、かつシステム状態の計測や報告をサポートすることができる機能を持っている。TPM 2.0 ライブラリ仕様は、TPM の標準的なアーキテクチャ及びコマンドセットを提供するとともに、特定のシステムクラスでどのように TPM を実装したらよいかを扱ったプラットフォーム特化仕様も提供している。ISO/IEC JTC 1 では、TPM ライブラリ仕様を ISO/IEC 11889:2015 Part 1-4[38]として承認している。

[38] ISO/IEC 11889:2015 Parts 1-4, *Trusted Platform Module; Part 1: Architecture, Part 2: Structures, Part 3: Commands, and Part 4: Supporting Routines.*

- Trusted Network Connect（TNC）: TCG TNC ワーキンググループは、ネットワーク管理者がネットワークに接続されているデバイスのエンドポイント完全性に関するポリシーを強制することを可能にする仕様を定めている。これらの仕様は、IETF Network Endpoint Assessment（NEA）ワーキンググループでの多くの作業の基礎となっており、IETF Security Automation and Continuous Monitoring（SACM）ワーキンググループが進めている作業との強い補完的関係になっている。
- ストレージ : TCG ストレージワーキンググループは、ストレージデバイス上のデータを保護するための標準ベースのメカニズムを利用可能にし、当該デバイス及び機能を管理する仕様を定めている。TCG ストレージ仕様では、共通基本仕様から 2 つのセキュリティサブシステムクラス（SSC）を準備している : Opal SSC はクライアントデバイス（例 : タブレット、ノート PC、デスクトップ PC）を対象としており、Enterprise SSC はハイパフォーマンスストレージ装置（例 : サーバ）を対象としている。

3 暗号アルゴリズム

本文書は 3 種類の暗号アルゴリズムを紹介する：暗号学的ハッシュ関数、対称鍵アルゴリズム、及び非対称鍵アルゴリズムで、それぞれ 3.1 節、3.2 節、及び 3.3 節に記す。本節で紹介する他のトピックとして、アルゴリズムのセキュリティ強度及びアルゴリズムライフタイムの概念について述べる（3.4 節、3.5 節をそれぞれ参照のこと）。

3.1 暗号学的ハッシュ関数

ハッシュ関数（ハッシュアルゴリズムとも呼ばれる）は暗号学的プリミティブアルゴリズムで、入力（例：メッセージ）の凝縮した表記を生成する。ハッシュ関数は任意長の入力を取り、あらかじめ決められた長さの値を出力する。ハッシュ関数の出力の一般的な名称には、*ハッシュ値*及び*メッセージダイジェスト*がある。

暗号学的ハッシュ関数は一方向関数で、逆計算は非常に困難である。つまり、ハッシュ値から入力値に戻す逆プロセスを実行することは非現実的である。

図 1 はハッシュ値の生成方法と検証方法を示す。

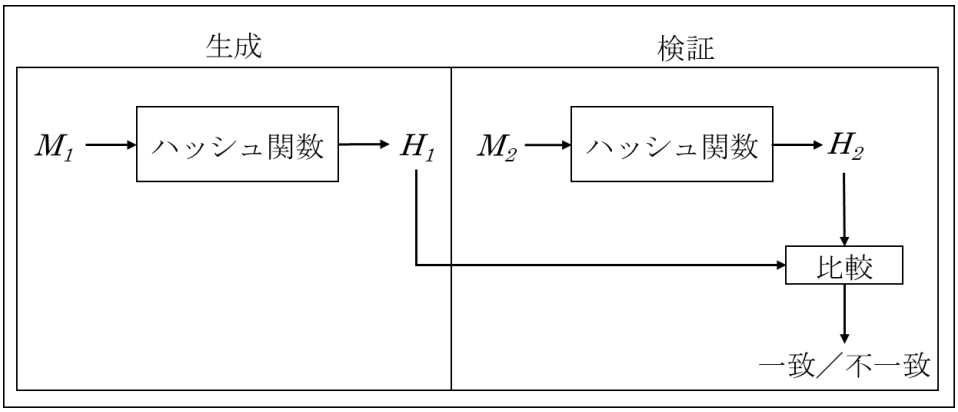

図 1：ハッシュ関数の生成と検証

ハッシュ関数の使用方法は以下のとおりである：

- ハッシュ生成：
  1. ハッシュ値（H_1）がハッシュ関数を利用してデータ（M_1）から生成される
  2. その後、M_1 と H_1 を保存もしくは伝送する
- ハッシュ検証：
  1. H_1 を生成した時と同じハッシュ関数を使って、受信又は読み取ったデータ（M_2）からハッシュ値（H_2）を生成する
  2. H_1 と H_2 を比較する。$H_1=H_2$ であれば、M_1 は保管又は伝送中に変更されていないと考えてよい。

上述の説明はハッシュ関数の最も単純な利用時のものである。ハッシュ関数は、通常、以下のようなよりハイレベルなアルゴリズムの中で利用される：

- 鍵付きハッシュメッセージ認証コードアルゴリズム（3.2.2 節及び 4.2.2.2 節）

- デジタル署名アルゴリズム（4.2.3 節）
- 鍵導出関数（例：鍵確立用）（5.3.2 節）
- 乱数ビット生成器（4.4 節）

連邦政府が利用するための**承認**ハッシュ関数は、FIPS 180、FIPS 202[39]、及び SP 800-185 に規定されている。

- FIPS 180 には、SHA-1 ハッシュ関数、及び SHA-2 ハッシュ関数群（SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 及び SHA-512/256）が規定されている。これらのハッシュ関数を利用するための追加ガイダンスは、SP 800-106[40]及び SP 800-107[41]に記されている。

  SHA-1 をデジタル署名の生成に使用した場合、当初の想定より弱いセキュリティになることを示した SHA-1 への攻撃手法があることに注意されたい（4.2.3 節を参照）。従って、デジタル署名生成の目的で SHA-1 を用いることは今では禁止されている。しかし、SHA-1 はそれ以外のほとんどのハッシュ関数アプリケーションで利用継続することができる。その中には、過去にハッシュ関数に SHA-1 を用いて署名されたデジタル署名の検証も含む（SP 800-131A[42]を参照）。

- FIPS 202 は、SHA-3 ハッシュ関数群（SHA3-224, SHA3-256, SHA3-384 及び SHA3-512）を規定している。この FIPS は、2 つの出力拡張可能関数（SHAKE128 及び SHAKE256）も規定しているが、これらの関数はこれ自体のみではハッシュ関数と見なされない。SP 800-185 は、SHAKE128 及び SHAKE256 の**承認された**使用方法を規定している。

それぞれのハッシュ関数の名称に使用されている数字はハッシュ関数の出力長を示す（例 : SHA-1 は 160 ビットの出力を生成する一方、SHA-XXX 及び SHA3-XXX は XXX で示される長さの出力を生成する）。

- SP 800-185 は、TupleHash 関数及び ParallelHash 関数を規定する。どちらの関数も可変長出力を生成することができる。TupleHash は、複数の入力をハッシュするように設計されている。ParallelHash は、非常に長いメッセージの連続した重複しないブロックを並列にハッシュ処理することのできる可変長ハッシュ関数である。

3.2 対称鍵アルゴリズム

対称鍵アルゴリズム（秘密鍵アルゴリズムと呼ばれることもある）は、暗号保護を行う際と、保護解除又は保護検証を行う際の両方で単一の鍵を用いる（すなわち、同じ鍵を暗号化処理とその逆処理に用いる）。例えば、データを暗号化（つまり、保護を適用）する際に用いる鍵は暗号化されたデータを復号（つまり、保護を解除）する際にも用いられる。暗号化の場合、元のデータを平文と呼び、暗号化された形のデータを暗号文と呼ぶ。データが保護され続ける必要がある場合には、鍵は秘匿され続けなければならない。

---

[39] FIPS 202, SHA-3 *Standard: Permutation-Based Hash and Extendable Output Functions.*
[40] SP 800-106, *Randomized Hashing for Digital Signatures.*
[41] SP 800-107, *Recommendations for Applications Using Approved Hash Algorithms.*
[42] SP 800-131A, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths.*

対称鍵アルゴリズムの複数の種類が承認されている。ブロック暗号アルゴリズム（例：AES）に基づくもの、及びハッシュ関数の利用に基づくもの（例：SHA-1 ベースの鍵付きハッシュメッセージ認証コード）である。

対称鍵アルゴリズムは、以下のために利用される：

- データの機密性を提供するための暗号化（4.1 節を参照）
- データの完全性及び情報源を確認するための認証（4.2 節を参照）
- 鍵導出（5.3.2 節を参照）
- 鍵ラッピング（5.3.5 節を参照）
- 乱数ビット生成（4.4 節を参照）

対称鍵アルゴリズムを使用する際、暗号関係 [43]ごと及び目的ごと（例：暗号化、データ完全性認証、鍵ラッピング）に単一の鍵の生成が必要である。技術的には、アルゴリズムが同じであれば、同じ鍵を複数の目的に使うことが可能である。しかしこのやり方は通常推奨しない。なぜなら、同じ鍵を 2 つの異なる暗号処理（例：同じハッシュ関数を用いた HMAC と鍵導出）に使用した場合、どちらか一方もしくは両方の処理でのセキュリティを弱くすることにつながることがあるためである。しかしながら、このルールの例外として承認されたものがある（4.3 節を参照）。

対称鍵アルゴリズムを使用する際に必要な鍵の数の例として、4 つのエンティティ（A、B、C 及び D）で暗号通信が必要であり、それぞれのエンティティペアで異なる暗号鍵を使うと想定する。6 つのペア関係（A-B、A-C、A-D、B-C、B-D 及び C-D）がありうるので、少なくとも 6 つの鍵が必要となる [44]。代わりに、もし 1,000 エンティティが互いに通信しようとする場合、499,500 個のペア関係が考えられ、それぞれのペアに対して少なくとも 1 つの一意の鍵が必要となる。もし、複数のアルゴリズム、鍵長、又は目的（例：暗号化と鍵ラッピングの両方）をサポートする場合、追加の鍵が必要となる。各エンティティは、全ての当該エンティティの対称鍵を秘密に保ち、その完全性を保護しなければならない。大量の鍵関係の必要性は大きな問題であり、この問題を軽減する手法が 5 節で紹介されている。

機微データの保護のために、NIST により複数の対称鍵アルゴリズムが**承認されている**。ただし、それらのアルゴリズムのうちのいくつかはすでに暗号保護への適用（例：暗号化）は承認されていないが、既に保護されている情報への処理（例：復号）は、そうすることのリスクが許容できる（例：鍵が危殆化されていないと信じるに足る理由がある）ことを条件に、継続してよい。暗号アルゴリズムごとの利用許容性についてのより詳細な情報は、SP 800-57 Part1 及び SP 800-131A を参照されたい。

3.2.1 ブロック暗号アルゴリズム

ブロック暗号アルゴリズムは、単一の鍵とともに**承認された**暗号利用モードで、暗号保護への適用（例：暗号化)及び後の保護された情報の処理（例：復号）の両方に利用される。複数のブロック暗号アルゴリズムが暗号プリミティブとして NIST から承認されているが、そのうちのいくつかはすでに暗号保護への適用は承認されていない。しかしながら、それらは過去に保護された情報の処理のために必要とされる場合もある（例：過去に暗号化された情報を復号するために必要とされる場合がある)。

---

[43] 暗号関係は、2 つ以上の当事者が同じ鍵とアルゴリズムを使用して通信できる場合に存在する。関係は 1 対 1 の場合もあれば、1 対多の場合もある（例えば、放送）

[44] この例では、6 つの暗号関係のみを使用しているが、プロトコルによっては、通信方向ごとに異なる鍵が必要となる場合がある（つまり、A から B への通信には、B から A への通信に使用する鍵とは異なる鍵が必要となる場合がある）

ブロック暗号アルゴリズムについては 3.2.1.1 節から 3.2.1.4 節で説明する。**承認された**暗号利用モードについては 3.2.1.5 節で説明する。

3.2.1.1 Data Encryption Standard（DES）

Data Encryption Standard（DES）は 1977 年 7 月に承認された、最初の NIST **承認**暗号アルゴリズムである。何度か再承認されてきたが、コンピュータの能力と処理速度が向上したことにより、連邦政府の情報を適切に保護する目的には DES の強度はもはや不十分になってきた。そのため、DES は 2005 年に**承認**アルゴリズムから廃止された（つまり、もはや DES は暗号化やその他の暗号保護に適用する手法として承認されない）。しかし、DES“暗号化エンジン”は、TDEA のコンポーネント関数として継続的に利用される（次節を参照）

3.2.1.2 Triple Data Encryption Algorithm（TDEA）

Triple Data Encryption Algorithm（TDEA）は、トリプル DES とも呼ばれ、データを変換するために DES 暗号エンジンを 3 回施す（SP 800-67 参照）。TDEA は、鍵束として定義した 3 つの鍵を用いて 64 ビットのブロックでデータを暗号化する。TDEA には 2 つの手法が規定されている：一つは 1 つ目と 3 つ目に同じ鍵を使う 2 鍵 TDEA（2TDEA）、もう一つは 3 つとも異なる（つまり、別個の）鍵を用いる 3 鍵 TDEA（3TDEA）である。

TDEA のセキュリティ寿命がほぼ終わりに近づいていることを示す複数の TDEA への攻撃が公表されている。そのため、NIST は、連邦政府のアプリケーションでの TDEA 使用の承認を打ち切る計画を発表した [45]。そのスケジュールは SP 800-131A に示されている。

2TDEA は、暗号保護（例：平文の暗号化）への適用が**認められていない**。しかし、ユーザは時間がたつとともにリスクが増しているということを受容しなければならないものの、すでに保護された情報への処理（例：暗号文の復号）に 2TDEA を使用することは継続できる。例えば、そのアルゴリズムがまだ安全だと想定されていた時期にデータが暗号化され公衆ネットワークで伝送されていた場合、その時点で（敵対者によって）暗号文が取得されて、後に当該アルゴリズムが安全ではないとみなされるようになった時点でその敵対者によって復号される可能性がある；このように、データの機密性はもはや保証されなくなる。

3TDEA を暗号保護（例：暗号化）に適用することは**推奨されておらず**、他の**承認**ブロック暗号を選択する（つまり、ユーザはこのアルゴリズムを保護に適用する際にはリスクを受け入れなければならない）。さらに、SP 800-67 では、一組の 3 鍵セットで保護するデータ量に制約を設けている。連邦政府のアプリケーションでは、TDEA を暗号保護に適用する際にはいつでも、必ず 3 つの異なる鍵を用い**なければならない**。2023 年 12 月 31 日以降、3TDEA を暗号保護に適用することは**認められない**。しかし、繰り返しになるが、ユーザは一定のセキュリティリスクがあることを受け入れなければならないという条件のもとで、すでに保護された情報処理への使用が継続できる。

3.2.1.3 SKIPJACK

SKIPJACK は FIPS 185[46]で参照されており、機密文書にて規定されている。SKIPJACK はすでに連邦政府情報の保護には適さなくなったと判定され、FIPS から廃止された。暗号保護（例：暗号化）への

---

[45] https://csrc.nist.gov/news/2017/update-to-current-use-and-deprecation-of-tdea を参照

[46] FIPS 185, *Escrowed Encryption Standard.*

適用に SKIPJACK を利用することは**認められていない**が、情報を復号するためにこのアルゴリズムを利用することは認められている。

3.2.1.4 Advanced Encryption Standard（AES）

Advanced Encryption Standard（AES）は DES 及び TDEA の代替として開発され、新しい製品で推奨されるブロック暗号アルゴリズムである。AES は FIPS 197 に規定されている。AES は 128 ビットのデータブロックを扱い、128、192、又は 256 ビットの鍵を使う。異なる鍵長の AES の命名法は AES-x と表記し、x は鍵長を示す（つまり、AES-128、AES-192 及び AES-256）。鍵長は AES を使用する際の要素になりうる（3.4 節を参照）が、全ての AES アプリケーションで AES の使用は容認される（つまり、安全とみなされる）。

3.2.1.5 暗号利用モード

対称鍵ブロック暗号アルゴリズムでは、同じ鍵を使う場合、同じ入力のブロックからは同じ出力のブロックが常に生成される。もし標準的なメッセージの複数のブロックが別々に暗号化された場合、敵対者は個々のブロックをほとんど検知されることなく容易に取り替えることができる。また、ブロックの繰り返しなど、平文にある種のデータパターンがあると、暗号文にも同じように出現する。これらの特性に対処するため、ブロック暗号アルゴリズムを使用するための暗号利用モードが規定されている。

これらのモードは、暗号プリミティブアルゴリズムと対称鍵及び可変の初期値（一般に初期化ベクトルと呼ばれる）を組み合わせて暗号サービスを提供する（例：メッセージの暗号化、メッセージ認証コードの生成）。ブロック暗号アルゴリズムへの**承認された**モードは SP 800-38 シリーズの文書に規定されており、以下が含まれる：

- 暗号化：SP 800-38A、SP 800-38E 及び SP 800-38G[47]で規定される（4.1 節を参照）
- 認証：SP 800-38B[48]で規定される（4.2.2.1 節を参照）
- 認証暗号：SP 800-38C 及び SP 800-38D で規定される（4.3 節を参照）
- 鍵ラッピング：SP 800-38F で規定される（5.3.5 節を参照）

3.2.2 ハッシュ関数を用いた対称鍵アルゴリズム

ハッシュ関数を用いた対称鍵アルゴリズムは、メッセージ認証コード（MAC）生成のための FIPS 198 に規定されている。HMAC として知られるこのアルゴリズムは、FIPS 180 か FIPS 202 にて規定された**承認**ハッシュ関数のいずれかと一緒に使用することで**承認されている**。HMAC のための FIPS 180 に規定されているハッシュ関数の使用に関するガイダンスは、SP 800-107 に記されている。

SP 800-185 は追加された MAC アルゴリズム（KMAC として知られている）を規定している。これは、FIPS 202 で規定されている拡張可能な出力関数をベースにしたものである。KMAC は 2 つのバリエーション（KMAC128 と KMAC256）がある。

---

[47] SP 800-38G, *Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption.*

[48] SP 800-38B, *Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication.*

3.3 非対称鍵アルゴリズム

非対称鍵アルゴリズム（一般的に公開鍵アルゴリズムと呼ばれる）は 1 対の鍵（つまり、鍵ペア）を使用する。それらの鍵ペアは公開鍵とプライベート鍵であり、互いに数学的に関連がある。公開鍵は公開してもプロセスの安全性を損なうことはない。一方で、プライベート鍵は、暗号保護をし続けたい場合においては秘密に保ち続けなければならない。両鍵に関連はあるものの、公開鍵の知識から効率的にプライベート鍵を特定することはできない。

鍵ペアのうちの一つの鍵は暗号保護を適用するために用い、もう片方の鍵は保護を解除もしくは検証するために用いる。使用する鍵は、使用するアルゴリズム及び提供されるサービスによって異なる。例えば、デジタル署名はプライベート鍵を用いて算出され、その署名は公開鍵を使って検証される（つまり、プライベート鍵を用いて保護が適用され、対応する公開鍵を用いて検証される）。暗号化も使用できる非対称鍵アルゴリズム[49]については、暗号化の際は公開鍵を使って行われ、復号はプライベート鍵を使って行う（つまり、公開鍵を用いて保護が適用され、プライベート鍵を用いて解除される）。

非対称鍵アルゴリズムは以下のように使用される：

1. ID 認証サービス、完全性認証サービス、及び情報源認証サービスをデジタル署名の形で提供する（3.3.1 節及び 4.2.3 節を参照）
2. 鍵合意アルゴリズムや鍵配送アルゴリズムを用いて暗号鍵材料を確立する（3.3.2 節及び 5.3 節を参照）。

これらのアルゴリズムは対称鍵アルゴリズムに比べて格段に遅い傾向があるので、大量のデータを扱う際には使用されない。しかしながら、鍵確立（5 節を参照）に用いる際には、対称鍵アルゴリズムと非対称鍵アルゴリズムを組み合わせて使う方法がある。これは、非対称鍵アルゴリズムのみを使う場合よりも効率よくすることができ、かつ対称鍵アルゴリズムのみを使う場合よりも必要な鍵の数を減らすことができる。

非対称鍵アルゴリズムの鍵ペアは目的ごと（例：デジタル署名の生成及び検証に用いる鍵ペアと鍵確立に用いる鍵ベアは異なる）に生成**すべきである**。技術的には、同じ鍵ペアを複数の目的に使いまわすことも可能である場合もあるが、この方法は推奨しない。なぜなら、2 つの異なる暗号目的（例：デジタル署名と鍵確立）に同一の鍵ペアを用いることは、片方もしくは両方のプロセスが提供する安全性を弱めることにつながることがある。

非対称鍵アルゴリズムを使う場合、対称鍵アルゴリズムを使う場合に比べて数少ない初期鍵の確立で済む。例えば、あるエンティティがデジタル署名を生成し、かつ当該エンティティ自身の鍵ペアを用いて鍵確立プロセス[50]に関与したいと仮定する。その時、それぞれの目的に対して鍵ペアを生成する必要がある。もし 6 つのエンティティがデジタル署名を生成し、かつ鍵確立プロセスに関与する意図がある場合、デジタル署名生成用に 6 鍵ペア、鍵確立用に別の 6 鍵ペアの合計 12 鍵ペアが必要になる。1,000 エンティティであれば、それぞれの目的に 1,000 鍵ペア、合計 2,000 鍵ペアが必要になる。各々の関係に対して一意の鍵ペアを生成する必要はない。対称鍵アルゴリズムにおいては各々の関係に対して一意の鍵を生成する必要があることを想起されたい（3.2 節を参照）。もしいずれかのプロセスで複数の公開鍵アルゴリズム又は鍵長を用いる場合には、さらに追加で鍵ペアを用意する必要がある。

---

[49] 全ての公開鍵アルゴリズムが複数の機能（例えば、暗号化と復号の両方、及びデジタル署名の生成と検証）を備えているわけではない

[50] 鍵確立方式の中には、全ての当事者が鍵ペアを持っている必要がない方式もあり、その場合は鍵確立のために鍵ペアを必要としない当事者がいることに注意されたい

プライベート鍵は、鍵ペアを“所有”するエンティティによって保持され、利用される。その鍵は秘密に保持され、完全性も守らなければならない。公開鍵は通常他のエンティティに配付され、完全性の保護が必要であるが、機密性保護は必要としない。5.2.3 節で紹介しているように、公開鍵証明書を使うことで配付が実現されることが多い。公開鍵証明書を使用する場合、証明書によって公開鍵の完全性保護が提供される。従って、各エンティティによる鍵保護にかかる負担は当該エンティティが所有するプライベート鍵のみに限定される。

いくつかの非対称鍵アルゴリズムはドメインパラメータを使用する。これは、当該暗号アルゴリズムを用いる際に追加で必要となる値である。これらの値は、相互に、また利用する鍵とも数学的に関連性がある。ドメインパラメータは通常公開されており、ユーザコミュニティ内で相当程度の期間継続して用いられる。これらのドメインパラメータは、公開鍵を含む公開鍵証明書内に含まれていたり、証明書によって参照されていたりする。

非対称鍵アルゴリズムが安全に使用できるかは、以下の点での一定の保証をユーザが得ているかに依存する：

- ドメインパラメータの有効性保証（ドメインパラメータを使用するアルゴリズムの場合）により、ドメインパラメータが数学的に正確であるという信頼を得る
- 公開鍵の有効性保証により、公開鍵が適切な鍵であるという信頼を得る
- プライベート鍵所有の保証により、プライベート鍵の所有者とされるエンティティが本当に当該鍵を持っているという信頼を得る

重要な注意：大規模量子コンピュータが利用可能になった場合、**承認された**非対称鍵アルゴリズムの安全性を脅威にさらすことになる。特にデジタル署名スキーム、Diffie-Hellman 及び MQV を利用 [51]した鍵合意スキーム、及び RSA を利用した鍵合意スキームと鍵配送スキームは、量子コンピュータに耐性のある（もしくは“耐量子計算機”）安全なものに変更する必要があるかもしれない。SP 800-175B の本版が発行される時点では、NIST は標準化に向けて耐量子計算機暗号アルゴリズムの選定プロセスを進めている段階である。このプロセスは数年がかりのプロジェクトである；新しい標準が利用可能となった時点で、本文書は適切に改訂される予定である。このプロジェクトの進捗状況は https://csrc.nist.gov/Topics/Security-and-Privacy/cryptography/post-quantum-cryptography を参照されたい。

3.3.1 デジタル署名アルゴリズム

デジタル署名は、ID 認証、完全性認証、情報源認証、及び否認防止のサポートを提供するために使用される。デジタル署名はハッシュ関数とともに用いられ、（ハッシュ関数によって規定された上限までの）任意長のデータに対して計算される。FIPS 186 はデジタル署名の計算のために**承認されている**アルゴリズムを規定している [52]。ここでは、デジタル署名アルゴリズム（DSA）及び楕円曲線デジタル署名アルゴリズム（ECDSA）を規定し、さらに RFC 8017[53]及び PKCS 1[54]（version 1.5 以上）で規定さ

---

[51] 有限体と楕円曲線の両方のバージョン

[52] デジタル署名方式には、2 つの一般的なタイプがある：アペンディクス付きデジタル署名とメッセージ復元型デジタル署名。FIPS 186 は、アペンディクス付きデジタル署名のアルゴリズムを規定しており、本推奨で取り上げているデジタル署名方式である。

[53] RFC 8017, *RSA Cryptography Specifications Version 2.2.*

[54] PKCS 1, *RSA Cryptographic Standard 1.*

れている RSA アルゴリズム並びに RFC 8032[55]で規定されているエドワード曲線デジタル署名アルゴリズム（EdDSA）を採用している。

FIPS 186 は、さらにこれらのアルゴリズムの各々で**承認されている**複数の鍵長も規定しており、デジタル署名の生成及び検証に必要なアルゴリズムの鍵ペアと他の様々なパラメータの生成方法も含んでいる。ただし、ECDSA 及び EdDSA に使用する推奨楕円曲線は、SP 800-186（新しい文書）に記載されている。

デジタル署名の生成は、FIPS 186 に規定されている鍵長を満たすか、もしくはより長いサイズの鍵であって、かつ FIPS 186 に準拠した方法で生成した鍵ペアを使って行わ**なければならない**。より短い鍵長のものは、それら短い長さの鍵を使用して生成されたデジタル署名を検証する際にしか使用**してはならない**。SP 800-131A を参照されたい（旧システム（レガシーシステム）では、現在の FIPS 186 で承認されているよりも短いサイズの鍵を使用していた）。

3.3.1.1 DSA

デジタル署名アルゴリズム（DSA）は FIPS 186 に規定されており、本文書の発行時点では承認されている。このアルゴリズムは有限体を利用したデジタル署名の生成及び検証に利用する。FIPS 186 は DSA ドメインパラメータ及び鍵ペアを生成する方法を定義し、安全に相互接続するために使われる鍵長とデジタル署名の生成と検証で使うアルゴリズムを規定している。

最新の FIPS 186 ドラフト（つまり、FIPS 186-5）では、DSA を標準から除外することを提案している。もしこの提案が採択されれば、今後 DSA の使用は**認められなくなる**。本文書の読者は、DSA を使用する前に FIPS 186-5 の状況を確認**すべきである**。

3.3.1.2 ECDSA

楕円曲線デジタル署名アルゴリズム（ECDSA）は FIPS 186 にて**承認され**、規定されている。基本的な署名と検証のアルゴリズムは DSA で使っているのと同じであるが、算術的には有限体の代わりに楕円曲線の利用を根拠にしている。FIPS 186 は連邦政府内で ECDSA を使用する際のガイダンスを記しており、SP 800-186 は ECDSA で用いるべき楕円曲線を含んでいる。DSA や RSA の代わりに ECDSA を使うことの利点は、鍵長が格段に短いことである。そのため、必要な保管場所及び伝送バンド幅が削減され、また一般的に DSA と RSA よりもアルゴリズムの実行速度が速い。

FIPS 186 は、ECDSA ドメインパラメータ及び鍵ペアの生成のための仕様、さらにはデジタル署名の生成及び検証のためのアルゴリズムの仕様を含んでいる；また、安全な相互接続のために利用する鍵長を定義する；及び鍵ペアを生成する際に使用する乱数ビット生成器の追加ガイダンスについて記している。

3.3.1.3 EdDSA

EdDSA は FIPS 186 にて採用され、RFC 8032 に規定されている。それには、RFC に記載されている Ed25519 曲線及び Ed488 曲線に対する推奨パラメータを含んでいる。これらの曲線は SP 800-186 にも含まれている。ECDSA（及び DSA）署名では署名を生成するたびにランダムな（一意の）値を使用することが求められるが、EdDSA 署名は決定的である：一意の値はプライベート鍵及び署名するメ

---

[55] RFC 8032, *Edwards-Curve Digital Signature Algorithm (EdDSA).*

ッセージを使って算出される（つまり、この値を生成するために乱数ビット生成器は不要であり、乱数ビット生成器を含まない実装も許容される）。

3.3.1.4 RSA

RSA アルゴリズムは、デジタル署名の生成及び検証が FIPS 186 にて**承認され**、PKCS 1 及び RFC 8017 で規定されている。FIPS 186 には、RSA をデジタル署名生成に使用する際の制約条件と RSA 鍵ペアを生成する方法を含み、また安全な相互接続のために使用すべき鍵長が定義されている。RSA 鍵ペア生成に関する追加情報は SP 800-56B[56]に記載されている。

3.3.2 鍵確立スキーム

非対称鍵確立スキームは、通信エンティティ間で使用する鍵を設定する際に使用する。スキームは、暗号サービス（今回のケースでは鍵確立サービス）を提供する変換方法の集合（つまり、暗号処理）である。このスキームは、鍵確立プロセスに必要な通信に実際に行うプロトコルで使用される。

数学的未解決問題を基にしている非対称スキームの 2 つのクラスが**承認されている**：離散対数ベースのスキームと素因数分解スキームである。

3.3.2.1 Diffie-Hellman 及び MQV

SP 800-56A は、離散対数ベースのアルゴリズムを使った鍵確立スキームを規定している。これらのスキームは有限体算術（ほとんどの人が使用する数学の形式）又は楕円曲線算術のいずれかを使用して規定される。

鍵合意用に 2 つのアルゴリズムが承認されている：Diffie-Hellman（DH）及び MQV[57]である。これらのアルゴリズムを鍵合意に使用する方法は SP 800-56A に規定されており、5.3.3 節に紹介されている。

有限体の DH 及び MQV に関して、SP 800-56A は、ドメインパラメータを SP 800-56A でリスト化されているドメインパラメータ群 [58]の一つから選ぶか、もしくは DSA でのドメインパラメータと同じ方式で生成すること（FIPS 186 を参照）と規定している。リスト化されている群をドメインパラメータとして利用するほうが望ましい。鍵ペアは DSA と同じ方式で生成される（FIPS 186 を参照）。

楕円曲線の DH 及び MQV に関して、鍵ペアの生成法は FIPS 186 に規定されており、ECDSA の鍵ペア生成と同じ方法を利用する。DH と MQV の鍵確立での推奨楕円曲線は SP 800-186 に記載されており、新しい曲線の生成に関する仕様も合わせて記されている。

3.3.2.2 RSA

RSA は、鍵確立だけでなく、デジタル署名の生成や検証にも使用できる。鍵確立への利用法は、SP 800-56B に規定されている。その文書には、鍵合意及び鍵配送の両方に対して**承認された**手法を規定している（鍵確立、鍵合意及び鍵配送に関するより詳しい解説は 5.3 節を参照）。

---

[56] SP 800-56B, *Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography.*

[57] Menezes–Qu–Vanstone.

[58] これらの群は、RFC3526 と RFC7919 で規定されている

RSA が鍵確立とデジタル署名生成の両方に利用可能なことから、両方の目的に同じ鍵を用いないことが重要である（鍵使用法に関する説明は SP 800-57 Part1 の 5.2 節を参照）。

3.4 アルゴリズムのセキュリティ強度

暗号アルゴリズムのセキュリティ強度は、攻撃者がアルゴリズムを破ることの難易度で測定される。暗号アルゴリズムを破ることは、アルゴリズムが提供することを意図した保護機能のある部分を破ることであると定義できる。例えば、データの機密性を保護するために使われるブロック暗号アルゴリズムが破られたというのは、許容できる作業量で、鍵の値を特定すること、又は鍵を知らなくても暗号文から平文に戻すことが可能であることである。

SP 800-57 Part1 では、**承認された**暗号アルゴリズムが提供できる現時点でのセキュリティ強度の推定値を記している。これらの強度は、特定の鍵長の観点で定めている。

連邦政府アプリケーションで**承認されている**セキュリティ強度は、112、128、192 及び 256 ビットである。以前は 80 ビットのセキュリティ強度も承認されていたこともあることに注意されたい。もはや保護強度が十分ではないとみなされたため、80 ビットのセキュリティ強度を提供するアルゴリズム及び鍵の利用は、暗号保護（例：データ暗号化）への適用が**認められなくなった**。しかしながら、80 ビットのセキュリティ強度を提供するアルゴリズム及び鍵は、すでにその強度で保護されているデータへの処理（例：復号）に利用できる。ただし、一定のリスクを許容しなければならない。

これらのセキュリティ強度を実際に実現するためには、アルゴリズム、鍵長、鍵生成と取扱い方法を適切に使用することが必要である。

3.5 アルゴリズムの寿命

時間とともに、アルゴリズムへの攻撃が成功し、そのアルゴリズムが望まれる保護強度を提供できなくなる場合がある；DES 及び TDEA[59]はそういったアルゴリズムの事例である（それぞれ 3.2.1.1 節及び 3.2.1.2 節を参照）。攻撃はアルゴリズムそのものに対して、又は特定の鍵長を使うアルゴリズムに対して行われる。後者の場合、DES や TDEA 以外のアルゴリズムでは、より長い鍵を使用することで、攻撃の成功を防ぐか、少なくとも一定の期間攻撃成功を遅らせることができる。

アプリケーションに使うアルゴリズム及び鍵長を選ぶ際、データを保護しておくのに必要な時間を考慮**すべきであり**、それに応じた適切なアルゴリズム及び鍵長を使用する。SP 800-57 Part1 は、**承認されている**アルゴリズム及び鍵長が安全であると考えられる期間の現時点での推定値を提供している。暗号保護に使用するアルゴリズム及び鍵長は、推定された期間内に収まると必要がある。しかし、これらの推定値は単なる推定でしかない。その期間の終了日前に、技術（例：量子コンピュータとアルゴリズムの使用）や暗号解読の進展が起きることもありうる。たいていの場合、これらの技術進化の初期のころは、現実的に使用できないものであったり、脅威が限定的であったりする。各組織において、こういった問題が起きた時に対処するための移行戦略を定めておくことを推奨する。これには、組織のデータの危殆化リスクを評価し、必要であれば新しいアルゴリズムや鍵長に移行することが含まれる。

[59] DES と TDEA は、鍵の長さが 1 つしか定義されてない

4 暗号サービス

全ての機微情報には完全性保護が必要であり、機密性保護も同様に求められる場合がある。本節では、鍵以外の機微データを保護するために提供できる暗号サービスについて述べる。これらのサービスには、データ機密性、データ完全性認証、ID 認証、情報源認証及び否認防止のサポートが含まれる。これらの暗号サービスを提供するために利用する鍵の保護及び管理に関しては、5 節で述べる。

理想的には、暗号サービスはできるだけ数の少ないアルゴリズムで提供されるのが望ましい。例えば、AES は機密性（4.1 節）、データ完全性認証（4.2 節）、鍵ラッピング（5.3.5 節）、及び乱数ビット生成器（4.4 節を参照）の基本演算を提供するために使うことができる。しかしながら、このことは最初に記載したほど実用的ではないかもしれない。なぜならば、別のアプリケーションで必要になったり他のセキュリティ特性を提供したりする他のアルゴリズムも同様に利用可能であるかもしれないためである。

1 つのブロック暗号利用モードで機密性と認証を組み合わせることに関しては、4.3 節で述べる。

4.1 データ機密性

データ機密性を提供するために暗号化を使用する。保護されていない形式のデータを平文と呼ぶ。暗号化は平文データを暗号文に変換し、暗号文は復号することで平文に戻すことができる。一般的にデータの暗号化と復号は対称鍵ブロック暗号アルゴリズムを使用して提供される。AES は、3 つの鍵長すべてを使うデータ暗号化手法として**承認されている**（3.2.1.4 節を参照）。3-key TDEA は現在でも暗号化の使用に認められているものの、その利用は推奨されていない（3.2.1.2 節及び SP 800-131A 参照）。

暗号文の復号は、平文を暗号化した時に使ったアルゴリズムと鍵を用いて行う。暗号アルゴリズムを知っているが正しい鍵を持っていない不正な暗号文受信者は、暗号文を復号することができないようにすべきである。しかしながら、鍵と暗号アルゴリズムを保有しているものは誰でも、暗号文を簡単に復号し、元の平文を手にすることができる。

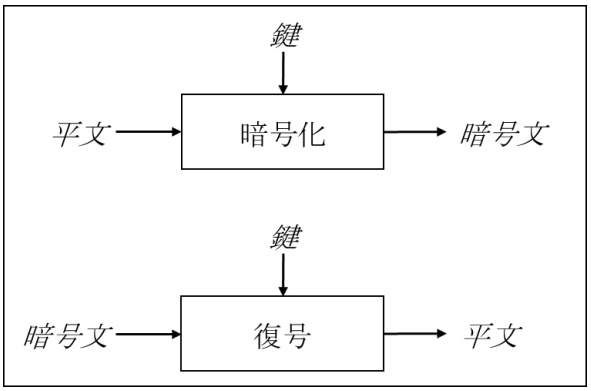

図 2：暗号化と復号

図 2 は暗号化と復号のプロセスを示す。平文と鍵を用いて暗号化プロセスを実行して暗号文を生成する。復号は、暗号文と同じ鍵を用いて復号プロセスを実行して平文データに復元する。

データの暗号化と復号に非対称鍵アルゴリズムを用いることもできるが、これらのアルゴリズムはブロック暗号アルゴリズムに比べて遅いため、一般のデータの暗号化や復号に通常は用いられないことに留意されたい。しかし、鍵自体を保護する際には用いられることもあり、そのことに関しては 5 節で述べる。

3.2.1.5 節で述べたとおり、データ暗号化はブロック暗号アルゴリズムと暗号利用モードを用いて実行される。暗号化のための**承認された**暗号利用モードは以下のように規定されている：

- SP800-38A（AES 及び TDEA 向け）: Electronic Codebook（ECB）モード、Cipher Block Chaining（CBC）モード、Cipher Feedback（CFB）モード、Counter（CTR）モード、及び Output Feedback（OFB）モード
- SP800-38E（AES 向け）: XTS-AES モード（ストレージデバイス上でのデータの機密性を保護する場合のみに限定）
- SP800-38G（AES 向け）: Format Preserving Encryption（FPE）のための FF1 モード及び FF3 モード

機密性と認証（4.2 節を参照）の両方を提供する追加のモードについては 4.3 節にて述べる。

4.2 データ完全性、ID 認証、及び情報源認証

データ完全性（単に*完全性*と呼ぶことも多い）は、特定の 2 つの時点（例えば、データが生成や保存、伝送された時点と、そのデータが取り出されたり受信されたりした時点）においてデータに変更が加えられたか否かに関係している。データ完全性を保証することは不可能だが、データ完全性コードを用いることでデータが変更されたことを高い確率で検出する手段を提供する。データ完全性コードは、データが生成された時に、保存又は伝送される前にデータに対して実行され、またデータが取り出し又は受信されたときに再度実行される。これらの演算結果が合致することを検証することで、データ完全性を保証する方法として提供される。暗号関連書籍では、このプロセスのことを*メッセージ（もしくはデータ）認証*と呼んでおり、完全性コードのことを MAC 又はデジタル署名と呼んでいることが多い。

ID 認証（単に*認証*と呼ぶ場合も多い）は、システムとやり取りをするエンティティの ID を保証するために用いられる。認証プロセスには、通常、エンティティがその身元を保証するための何らかの証拠（例：トークン、指紋、PIN やそれらの組み合わせを使って）を生成することが、データやリソースにアクセスすることが許諾される前に求められる。

情報源認証は、伝送もしくは保存された情報の情報源を保証するために用いられるプロセスである。使用する手法によっては、情報源認証は否認防止をサポートすることも可能である（すなわち、情報源が誰であるかについて、第三者、例えば司法エンティティが確信できるか否か[60]）。

暗号はこれらのサービスを提供するために利用することが可能であるが、単一のアルゴリズムだけではこれらすべてのサービスを提供することはできない。4.2.1 節で述べるハッシュ関数はある種のデータ完全性を保証するために使うことができる。4.2.2 節で述べるメッセージ認証コード（MAC）アルゴリズムは、データ完全性サービスと情報源認証サービスの両方を提供できる。デジタル署名アルゴリズムは、より高い性能コストが必要だが、データ完全性認証と ID 認証、情報源認証のサービス、さらに否認防止のサポートも提供することもできる（4.2.3 節を参照）

[60] 否認防止の実際の決定は、考慮すべき多くの側面を持つ法的な決定である。暗号メカニズムは、この決定における一つの要素としてのみ使用することができる（すなわち、デジタル署名は、否認防止の決定をサポートするためにのみ使用することができる）

4.2.1　ハッシュ関数

ハッシュ関数は、ハッシュ値が生成されたデータの完全性をある程度保証できるハッシュ値を計算するために用いる。しかしながら、ハッシュ関数が単独で使用された（例えば、HMAC やデジタル署名生成とセットで必要とされるような秘密鍵を使用しない）場合、敵対者によってデータに変更が加えられておらず、新たに計算されたハッシュ値ではないという保証はない。従って、完全性保護を提供するためにハッシュ関数を単独利用することは、リスクが非常に低い場合（例えば、データが信頼できる情報源から与えられ、ハッシュ値が伝送手段の劣化により発生する可能性がある変化を判断するためにのみ使用される場合）を除いて、推奨されない

4.2.2　メッセージ認証コードアルゴリズム

メッセージ認証コードアルゴリズムと暗号鍵は、メッセージ認証コード（MAC）を生成するために用いられる。MAC は、データの完全性と情報源認証を保証するために利用できる。MAC はデータに対する暗号学的チェックサムであり、データが保存もしくは伝送されてから変化又は変更されていないことを保証することができる。データの MAC をあるエンティティ（エンティティ A という）が生成した場合、MAC を生成するのに使ったその鍵を知っているエンティティなら誰でも、当該データの完全性を検証することができる。データが MAC とともに保管されていて、鍵がエンティティ A、B 及び C に知られている場合、A、B、C のいずれもがデータと MAC をストレージから読み出し、その完全性を確認（つまり、データが保存されている間に変更されていないことを検証）することができる。

もしエンティティ A が鍵を知っている他のエンティティ（エンティティ B）にデータと MAC を送ると、受信者（B）は伝送中にデータが変更されなかったことを確認できる。もし、A と B のみが鍵を知っている場合、エンティティ B（受信者）は、エンティティ A のみがデータを送れる（すなわち、エンティティ A がデータの情報源である）ことも知っている。しかしながら、データと MAC が複数のエンティティ（つまり、エンティティ B と C など、複数の受信者が鍵を知っている）に送られたとすると、各受信者は受信データの完全性は確認できるものの情報源保証を得ることはできない（例えば、受信者エンティティ C＜※誤植＞の観点からは、エンティティ A もしくはエンティティ B のいずれかが情報源になる。なぜなら、両者とも鍵を知っているためである)。このことは用途によっては許容できる場合もあることに留意されたい。

MAC は、最初に MAC が生成された時と、受信もしくは読み出された MAC が検証された時との間に発生するデータの変更を検知するために使用される。これらは、MAC が最初に生成される前に発生したエラーは検知できない。データ完全性と情報源認証を提供するための MAC の使用は、MAC を生成する当事者とそれを取得又は受信することを意図した当事者のみに限定された秘密鍵の知識に依存する。MAC 鍵自体はユーザコミュニティ内（例：二人以上の当事者）で共有されるもので、当該鍵を共有している当事者のみが所与のデータに対する正しい MAC を計算することができる。

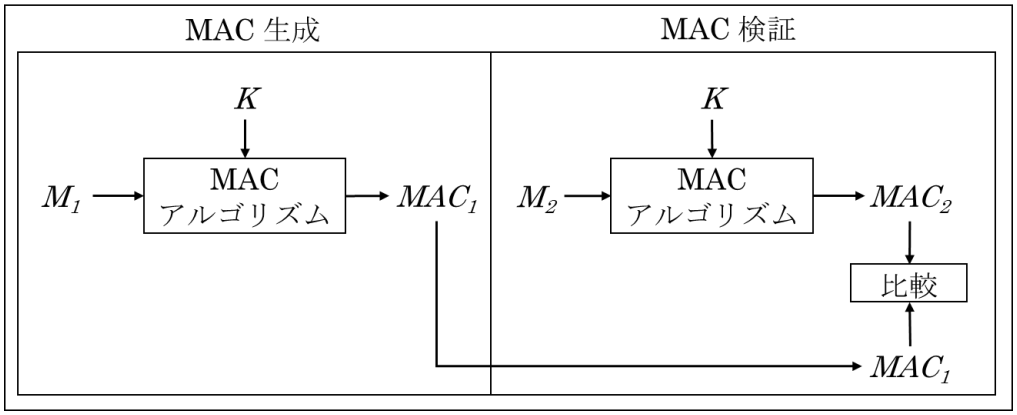

図 3：メッセージ認証と検証

図 3 はメッセージ認証コードの使い方を示す。

- メッセージ認証コード（MAC_1 ）はデータ（M_1 ）から鍵（K）を用いて計算される。その後、M_1 と MAC_1 は保存もしくは伝送される。
- しかる後に、保存又は受信されたデータの完全性をチェックする。保存又は受信されたデータを M_2、保存又は受信された認証コードを MAC_1 とする。
- M_2 に対して同じ鍵（K）を用いてメッセージ認証コードを計算する。その時のメッセージ認証コードを MAC_2 とラベル付けする。
- $MAC_1 = MAC_2$ であれば、M_2（保存又は受信されたデータ）は、MAC_1 を計算した際のデータ（M_1 ）と同じであると見なすことができる（すなわち、$M_1 = M_2$ ）。

データ完全性保証は、エラー検出コードとして知られている非暗号学的手法を使って提供されることも多い。しかしながら、これらのコードは、敵対者によって、敵対者の有利なように改ざんすることができる。MAC のような**承認された**暗号メカニズムを使うことによってこの問題に対応することができる。つまり、MAC によって提供される完全性の保証は、暗号鍵を知らない人は誰でも正しい MAC を生成できないという前提に基づいている。鍵を知らない敵対者は、データを改変して、当該改変データに対する検証可能な MAC を生成することはできない。従って、MAC 鍵を秘密に保護することは極めて重要である。

MAC を算出するための 2 つのタイプのアルゴリズムが、連邦政府での利用に**承認されている**：対称鍵ブロック暗号アルゴリズムベースの MAC アルゴリズムと、ハッシュ関数もしくはハッシュ関連関数ベースの MAC アルゴリズムである。

4.2.2.1 ブロック暗号アルゴリズムベースの MAC

SP 800-38 シリーズの文献では、MAC 生成のモードを記載している。

- SP 800-38B は、CMAC モードを定義している。これは AES と TDEA（ブロック暗号アルゴリズム）を使用して MAC を算出する方法である；TDEA の非推奨とされる使用法に関しては 3.2.1.2 節を参照。
- SP 800-32D は、GMAC モードを定義している。これは AES を使用して MAC を算出する方法である。
- 機密性（すなわち暗号化）と認証（すなわち MAC 算出）の両方を 1 回の処理で提供するモードも定義されている（4.3 節を参照）。

4.2.2.2 ハッシュ関数ベースの MAC

FIPS 198 は、MAC（HMAC）を定義しており、これは暗号学的ハッシュ関数を秘密鍵と組み合わせて使う。HMAC は、**承認された**暗号学的ハッシュ関数（4.2.1 節を参照）で使用しなければならない。HMAC を使用した際の安全性に関しては SP 800-107[61]に記されている。

---

[61] SP 800-107, *Recommendation for Applications Using Approved Hash Algorithms.*

SP 800-185 は、別の MAC アルゴリズム（KMAC）を定義しており、これは FIPS 202 に規定されている拡張出力関数をベースにしている。KMAC には 2 つのバリエーション（KMAC128 と KMAC256）が規定されている。それぞれの安全性に関しては SP 800-185 に記されている。

4.2.3 デジタル署名アルゴリズム

デジタル署名アルゴリズムは、一対の鍵ペア（プライベート鍵と公開鍵）を使用して、デジタル署名の生成と検証を行う。プライベート鍵は署名生成の際に用いられ、署名者（鍵ペアの所有者）のみが知っているようにしなければならない；公開鍵は署名検証に使われる。アルゴリズムの設計及び鍵ペアの生成方法のため、公開鍵を効率よく使ってプライベート鍵を決定することはできない。2 つの鍵が生成プロセスと検証プロセスのために必要なことから、デジタル署名アルゴリズムは非対称鍵アルゴリズムに分類される。

デジタル署名はコンピュータ上ではビット列として表現され、公開鍵にアクセスできる人であれば誰でも検証できる手書き署名の電子的な類似物である。署名は、データ完全性認証と ID 認証、情報源認証の提供、及び否認防止のサポートに利用可能である。

各署名者はプライベート鍵と公開鍵のペアを保有する。署名生成（検証可能なデジタル署名の）は、プライベート鍵にアクセス権を持つ当事者にしか実行出来ない。公開鍵を知っている人は誰でも、関連する公開鍵を使って署名を検証することができる。デジタル署名システムの安全性は、署名者のプライベート鍵の機密性を維持することに依存する。したがって、署名者は、自分のプライベート鍵を認可されていない開示から守らなければならない。

デジタル署名は、代替の署名方法では得られない保護を実現することができる。そのような代替法の一つが、デジタル化された署名である。デジタル化された署名は、手書き署名の視覚的形状を電子イメージ（例えば、スキャナーで PC に取り込むことによって）に変換することで生成される。デジタル化された署名は、印字した時に手書き署名に似たものになるが、デジタル署名と同じレベルの保護を提供しない。デジタル化された署名は偽造や複製の可能性があり、さらに他の電子データに付加することができる；また、デジタル化された署名は、署名された後に情報が変更されたかどうかを判断するために利用することもできない。しかしながら、デジタル署名は、各メッセージに対して署名者だけが知っているプライベート鍵を利用して計算される。署名者が署名した異なるメッセージごとに、異なるデジタル署名を持つことになる。メッセージにほんの少しの変化しかない場合でも、署名は異なるものになる。敵対者がプライベート鍵を知らない場合、敵対者は有効な署名（すなわち、署名生成時に使用したプライベート鍵に対応した公開鍵を使って検証可能な署名）を生成することはできない。

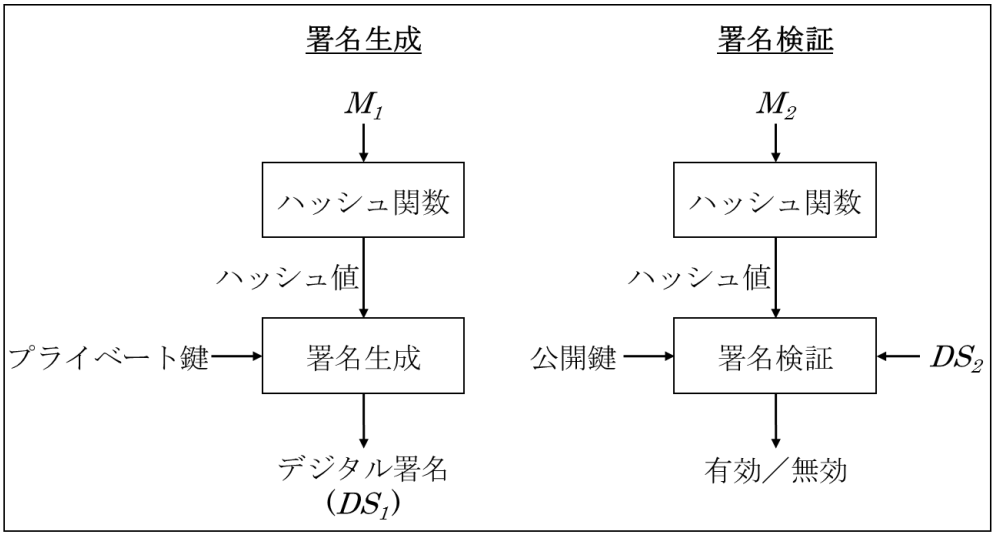

図 4：デジタル署名の生成と検証

図 4 は、デジタル署名の生成と確認を図示する。デジタル署名アルゴリズムは、署名生成プロセスと署名検証プロセスを含む。

a. 署名生成：

   1. 署名生成プロセスの中で、ハッシュ関数（3.1 節を参照）を使用してハッシュ値を得る。それは、署名されるデータを凝縮したもの（つまり、図 4 の署名生成で M_1 と示される）である。

   2. ハッシュ値は、その後、署名生成プロセスへの入力となり、プライベート鍵と合わせてデジタル署名を生成する（図 4 で DS_1 と示される)。

   3. デジタル署名（DS_1 ）は、署名されたデータ（M_1 ）と共に検証者に提供される（すなわち、DS_1 と M_1 は、意図した受信者に伝送されるか、又は後の読み出しのために保管される)。

b. 署名検証 : 伝送されたデータと署名の受信者（又はストレージからデータと署名を読みだしたエンティティ）は、以下のように署名を検証する。

   1. 受信したデータ／読み出したデータ[62]（M_2 ）に署名生成時に使用したのと同じハッシュ関数を用いて、別のハッシュ値を計算する。（もしデータが伝送もしくは保存された間に変更されていれば、新しく計算されたハッシュ値は、署名生成時（Step a.1 での）に計算されたハッシュ値とは同じ値にならないことに注意されたい。）

   2. 新たに算出されたハッシュ値と受信した署名／読み出された署名[63]（DS_2 ）は、署名者の公開鍵とともに、署名検証プロセスの入力となる。このプロセスの出力は、受信したデータ／読み出されたデータ（M_2 ）の署名が有効か無効かを示すものである。

FIPS 186 は、非対称（公開鍵）暗号を用いたデジタル署名の生成方法及び検証方法を規定している。4 つのデジタル署名アルゴリズムが、FIPS 186-4 に記されている：

- デジタル署名アルゴリズム（DSA）（3.3.1.1 節を参照）
- 楕円曲線デジタル署名アルゴリズム（ECDSA）（3.3.1.2 節を参照）
- エドワード曲線デジタル署名アルゴリズム（EdDSA）（3.3.1.3 節を参照）
- RSA（3.3.1.4 節を参照）

デジタル署名アルゴリズムは、FIPS 180、FIPS 202 及び SP 800-185 に規定されているハッシュ関数とともに利用される。これらのアルゴリズムはそれぞれ、使用するドメインパラメータや鍵の保証を得ることが求められる。これについては 3.3 節で述べる ; SP 800-89[64]では、デジタル署名を使用するために必要なこれらの保証を得るための手法を提供している。

---

[62] 送信時／保存時にエラーが発生したり、悪意のある敵対者が送信中／保存中にデータを改ざんしたりする可能性があるため、受信データ／取得データは、署名生成時にハッシュされたデータとは異なる可能性がある（ステップ a.1 を参照)。そのため、受信データ／取得データは、M_1 ではなく M_2 と呼ばれる

[63] 署名もまた送信中／保存中に変更される可能性がある。そのため、DS_1（ステップ a.2（※補足）で生成された署名）ではなく、DS_2 が使用される

[64] SP 800-89, *Recommendation for Obtaining Assurances for Digital Signature Applications.*

多くの場合、デジタル署名がいつ生成されたか判断することが重要である。例えば、特定の日付より前に署名された文書であるかどうか（例えば、遺言が 2 つ存在する場合、遺言者の亡くなる日付よりも前で、かつ、より近い日のものに署名されたのはどちらか）を判断することが重要な場合がある。SP 800-102[65]は、デジタル署名がいつ生成されたかを立証するためのガイダンスを提供する。

4.3 ブロック暗号の暗号利用モードにおける機密性と認証の組合せ

機密性と認証は、2 つの異なるブロック暗号アルゴリズム（例えば、暗号化は AES の CBC モード、認証は HMAC）を使うか、又は単一のブロック暗号の暗号利用モードを使うかのいずれかによって提供することができる。ここでの説明では、認証とは、データ完全性と暗号学的に保護されたデータの情報源の両方の保証を得るために使うことに注意されたい。

暗号化と認証が 2 つの異なる処理で実行される（それぞれ 4.1 節と 4.2 節を参照）場合、2 つの異なる鍵を必要とする。これらの処理を実行する際に注意を払わないと（例えば、正しい手順で処理を実行するなど）、攻撃を許すような脆弱性をはらむ可能性がある。暗号化と認証を別々に行う場合には、よく吟味され標準化されたプロトコルと構成を用いる**べきである**。

別の方法として、暗号化と認証の両方を単一の鍵を使って単一の処理で実行するモードを使うことである；このようなモードのことを“認証暗号”モードと呼ぶ。そのようなモードを利用すると、2 つの別々の処理を使う場合よりも、鍵の数が少なくて済み、一般的に処理速度が速くなる。AES には 2 つの認証暗号モードが定義されている（TDEA ではこのようなモードは定義されていない）。

- SP 800-38C では CCM モードが規定されている。
- SP 800-38D では Galois/Counter（GCM）モードが定義されている。

4.4 乱数ビット生成

暗号やセキュリティのアプリケーションは、非常に多くの乱数と乱数ビットを使用する。暗号では、暗号鍵を生成するために乱数の値が必要である。“エントロピー”とは、ある値のランダム性の度合いを表すために用いられる用語で、エントロピー量でその値を推測する難しさを示している。

乱数ビット生成器（RBG）には 2 つのクラスがある：非決定論的乱数ビット生成器（NRBG）で真正乱数（ビット）生成器とも呼ばれるものと、決定論的乱数ビット生成器（DRBG）で擬似乱数（ビット）生成器とも呼ばれるものである。各 RBG は、エントロピー源の使用に依存して、人が制御できない予測不能なビットを提供する。これらのビットは、ある物理的ソース（熱雑音、リング・オシレータ、ハードディスクのシークタイムなど）から得ることができる。NRBG は、NRBG 出力ごとにエントロピー源が生成する新しい未使用のエントロピービットを利用できるかに依存する。DRBG は、エントロピー源によって、又はエントロピー源（例：NRBG）に依存する**承認された**方法を使って生成されるエントロピーで最初に“シード化”される；アプリケーションによっては、DRBG は、処理中に（例えば、再シード化されることによって）追加のエントロピーを受け取る場合もそうでない場合もある。

乱数ビット生成について、複数の文書が開発されているか、現在開発中である。

- SP 800-90A では、ハッシュ関数とブロック暗号アルゴリズムの利用をベースにした**承認された** DRBG アルゴリズムを規定している；DRBG は、当該 DRBG がサポートするセキュリティ強度に十分なエントロピーを提供するランダム源（例：エントロピー源もしくは NRBG）で初期化されなければならない。

---

[65] SP 800-102, *Recommendation for Digital Signature Timeliness.*

- SP 800-90B[66]では、エントロピー源について記述する。それには、エントロピー源が故障していないことを判断するために必要な健全性テストや、認定された試験機関によるエントロピー源の認証試験などを含む。
- SP 800-90C[67]では、SP 800-90A でのアルゴリズムと SP 800-90B に従って設計されたエントロピー源を用いた NRBG と DRBG の設計と実装に関する説明を提供する。NRBG は、SP 800-90A での DRBG アルゴリズムを含むように構成されており、エントロピー源の故障が直ちに検出されない場合にフォールバック機能を提供することに注意されたい。
- SP800-22[68]では、乱数生成器と擬似乱数生成器を選定し試験する際の様々な側面を記述している。本文書には、適切な生成器を特徴づけ、選定するためのいくつかの基準が含まれており、統計的検定と暗号解読との関係について説明し、推奨される統計的検定をいくつか提供している。これらのテストは、ある生成器が特定の暗号アプリケーションに対して適しているかどうかを判断するための最初のステップとして有用である。しかしながら、連邦政府のアプリケーションでは、FIPS 140 及び SP 800-90 の該当部分に準拠していると認証された RBG でなければならない。

4.5 対称暗号対非対称暗号

3.2 節と 3.3 節で述べた通り、非常に多くの暗号関係が求められる時、必要な初期対称鍵の数は、必要な公開鍵／プライベート鍵の鍵ペアの数に比べて非常に多くなる可能性がある。

しかし、対称鍵暗号の第一の利点は処理速度である。対称鍵アルゴリズムは、通常、非対称鍵アルゴリズムに比べて圧倒的に高速であり、同じセキュリティ強度であれば鍵長も短くて済む；鍵長は、鍵を保存するためのメモリーや鍵を配送するためのバンド幅が制限されているときに重要な考慮点になりうる。さらに、暗号解読や計算効率の向上によって、公開鍵暗号によって提供される保護レベルは、対称鍵暗号によって提供される保護レベルに比べて急速に低下する傾向にある。また、潜在的な耐量子世界では、現時点で承認されている非対称鍵アルゴリズムは十分な保護を提供しなくなる。

非対称鍵（すなわち、公開鍵）暗号は全体的に少ない数の鍵しか必要とせず、また対称鍵暗号が圧倒的に高速であることから、しばしばハイブリッド方式が使用される。ここでは、非対称鍵アルゴリズムがデジタル署名の生成と検証及び最初の鍵確立のために使用される。その一方、対称鍵アルゴリズムはその他の全ての目的（例：暗号化）のために用いられ、特に大量のデータの保護を伴う場合や、エンティティが既に確立された（例えば、手動配付方式もしくは非対称鍵確立方式を使って確立された）対称鍵を共有しているときに鍵配付を行う場合に使われる。例えば、非対称鍵システムは対称鍵を鍵合意プロセス又は鍵配送プロセス（それぞれ 5.3.3 節、5.3.4 節を参照）を用いて確立するために利用し、その後、当該対称鍵をファイルやメッセージの暗号化や他の鍵の配付のために使用する。

状況によっては、非対称鍵暗号は不要であり、対称鍵暗号のみで十分な場合もある。これには、エンティティ間で既に共有されている対称鍵を使用して安全な対称鍵の確立を行うことができる環境、単一の権限者が全ての鍵を知っていて管理する環境、及び単独ユーザ環境などが含まれる。

一般的に、非対称鍵暗号はオープンなマルチユーザの環境に最も適している。しかしながら、量子コンピュータの利用可能性が迫ってきているため、現在の非対称アルゴリズムは攻撃に対して脆弱になる（3.3 節を参照）。

---

66 SP 800-90B, *Recommendation for the Entropy Sources Used for Random Bit Generation.*
67 SP 800-90C, *Recommendation for Random Bit Generator (RBG) Constructions.*
68 SP 800-22, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications.*

5 鍵管理

暗号鍵の正しい管理は、セキュリティのために暗号を効果的に使用する際に不可欠である。鍵は金庫の暗証番号と類似している。もし金庫の暗証番号が敵対者に知られたら、その金庫はその敵対者による侵入に対してセキュリティを提供しない。同様に、鍵管理がおろそかであれば、強固なアルゴリズムも簡単に危殆化する可能性がある。究極的には、暗号により保護された情報の安全性は、鍵の強度、当該鍵に関連するメカニズムとプロトコルの有効性、及び全ての鍵情報（すなわち、鍵材料及びその鍵材料に関連する全ての情報（つまり、鍵のメタデータ））に提供される保護に直接依存する。適切と思われるメタデータの提案リストについて、SP800-57 Part 1 を参照されたい。

全ての鍵情報は、変更に対して保護される必要がある（つまり、完全性が保たれることが必要である）。また、秘密鍵とプライベート鍵（つまり、対称アルゴリズムと非対称アルゴリズムそれぞれで使用される鍵）及び全ての秘密メタデータは、認可されない開示から保護される必要がある（つまり、それらの機密性は保たれる必要がある）。

鍵管理は、鍵の安全な生成、保管、配付／確立、利用、及び破棄の基盤を提供するものであり、鍵ライフサイクルの全てのフェーズが重要である。もし強力なアルゴリズムを利用して適切に生成された鍵を使ってデータを暗号化した場合、その後のデータの保護は、鍵情報を保護することだけに縮退させることができる（つまり、暗号によって保護された情報のセキュリティは鍵情報に提供される保護に直接依存する）。従って、鍵とその鍵に付随する情報の管理のために、暗号鍵管理システム（CKMS）が必要となる。

5.1 一般的な鍵管理ガイダンス

一般的な鍵管理におけるガイダンスのために複数の文書が発行されている：SP 800-57（5.1.1 節を参照）、FIPS 140（5.1.2 節を参照）、及び SP 800-131A（5.1.3 節を参照）である。

5.1.1 鍵管理にかかわる推奨事項

SP 800-57 は、暗号鍵及び関連情報を管理（鍵の生成、利用、及び最終的な破棄）するうえでの一般的なガイダンスを示している。関連トピック（例えば、アルゴリズム選択、適切な鍵長、暗号化ポリシー）も SP 800-57 に含まれており、3 つのパートで構成されている：

1. SP 800-57 Part 1“*一般ガイダンス*”には、以下のような基本的な鍵管理ガイダンスを含んでいる：
    - 鍵材料に必要な保護
    - 鍵ライフサイクルの責任
    - 鍵のバックアップ、アーカイブ及び復元
    - 鍵の変更
    - 暗号利用期間（すなわち、その鍵を使用するのに適切な期間）
    - 説明責任及び監査
    - 鍵の棚卸
    - 緊急時対応計画
    - 鍵危殆化復旧（新しい鍵を生成するなど）

連邦政府機関は、暗号保護を必要とすると判断した様々な情報を保有しているが、情報の機微度や保護が必要な期間も様々である。このため、NIST は情報保護のために 4 段階のセキュリティ強度[69]（112、128、192 及び 256 ビット）を設定している。これらのセキュリティ強度は**承認された**暗号アルゴリズム及び鍵長に割り付けられており、当該アルゴリズムと鍵長の使用が安全であると予想されている期間が提示されている。より詳しい情報は、SP 800-131A（5.1.3 節で紹介する）を参照されたい。

機関は、適切なセキュリティ強度を持ったアルゴリズムと鍵長を決める前に、暗号保護が必要な時間の長さを決定する必要がある。

SP 800-57 Part 1 は、その中で提供されるガイダンスがもはや有効でなくなった（例えば、あるアルゴリズムが適切なセキュリティを提供できなくなる）場合は、いつでも更新されることに留意されたい。

2. SP800-57 Part 2 "*鍵管理組織のベストプラクティス*" では、以下のことを行う：
   - 対称鍵及び非対称鍵の管理のための効果的なシステムに共通する概念、機能、及び要素を特定する
   - 効果的な組織の鍵管理に必要なセキュリティ計画の要件と文書を特定する
   - 鍵管理仕様の要件を記述する
   - 暗号を使用する組織に必要な暗号鍵管理ポリシー文書を作成する
   - 鍵管理実践ステートメントの要件を記述する

3. SP800-57 Part 3 "*アプリケーションに特化した鍵管理ガイダンス*" では、以下のような現時点で利用可能な暗号メカニズムに付随する鍵管理の課題を対処する。例えば、公開鍵基盤（PKI）、インターネットプロトコルセキュリティ（IPsec）、Secure/Multipart Internet Mail Extensions（S/MIME）、Kerberos、Over-the-Air Rekeying（OTAR）、ドメインネームシステムセキュリティ拡張（DNSSEC）、暗号化ファイルシステム（EFS）、Secure Shell（SSH）プロトコル、など。

   以下のようなことについて、具体的なガイダンスが提供されている：
   - 推奨や許容されるアルゴリズムスイート及び鍵長
   - 現時点でのメカニズムを利用して連邦政府の情報を保護するための推奨事項
   - 鍵管理プロセス及びその鍵管理プロセスによって生成・管理される鍵を使った暗号メカニズムの有効性に影響を与える可能性があるセキュリティ上の考慮事項

[69] 2014 年以前は、暗号保護（暗号化など）を適用する場合、5 番目のセキュリティ強度（80 ビットセキュリティ）が許容されていた。しかし、この強度はもはや適切ではない

Transport Layer Security (TLS) プロトコルは本文書の初期バージョンには含まれていたが、現バージョンの Part 3 では TLS（SP 800-52[70]参照）を説明する別文書を参照する形をとっていることに注意されたい。

新しい鍵管理技法とメカニズムが次々と開発されており、既存の鍵管理メカニズムと技法は常に改良されている。Part 3 に記されているセキュリティガイダンス情報は、メカニズムと技法が改良されるに従って更新されるが、新しい商品や技術仕様が現バージョンの文書に反映されていないことは常にあり得る。したがって、与えられるコンテキストには、ステータス情報（最後に文書が改定された時点でのバージョン番号や実装状況など）を含んでいることがある。

5.1.2 暗号モジュールのセキュリティ要件

FIPS 140 は、連邦政府情報システムでの暗号を組込んだりサポートしたりする暗号モジュールに求められる最低限のセキュリティ要求を示す。暗号モジュールは、機微情報を保護するセキュリティシステムでの暗号計算を実際に実行する。セキュリティ要件は、以下のようなモジュール仕様を含む、暗号モジュールのセキュリティ設計と実装に関連する領域を包含する。例えば、暗号モジュールのポートやインタフェース；役割、サービス、及び認証；有限状態モデル；物理的セキュリティ；運用環境；暗号鍵管理；電磁干渉／電磁環境適合性（EMI/EMC）；自己診断；設計保証；攻撃に対する緩和策、など。

FIPS 140 は、コンピュータ及び電気通信システムで機微情報を保護するために暗号を利用する全ての連邦政府機関に適用可能である。FIPS 140 及び暗号モジュール認証に関する詳細な情報は、https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program に掲載されている。

5.1.3 新しい暗号アルゴリズム及び鍵長への移行

SP800-57 Part 1 の作成と公開に際して、NIST は新しい暗号アルゴリズム及び鍵長への移行に関する推奨事項を提供している。これは、アルゴリズムが破られることや、より強力なコンピュータを用いて暗号鍵の効率的な探索を行える可能性があることが理由である。SP 800-131A は、このような移行のためのより具体的なガイダンスを提供するために作成された。アルゴリズムやサービスごとに SP 800-131A で扱われており、それぞれの使用について、使用可能[71]（Acceptable）、非推奨[72]（deprecated）、既存アプリケーションでのみ使用可能[73]（Allowed only for legacy applications）、禁止（disallowed）のどれであるかが記されている。

SP 800-131A は、必要に応じて更新されることに注意されたい（例えば、適切なセキュリティが提供されなくなったアルゴリズムの移行スケジュールを提供するため）。

---

[70] SP 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations.

[71] 現状では、セキュリティリスクが知られていない

[72] 当該アルゴリズムや鍵長の使用は容認されているが、ユーザは何らかのリスクを受容しなければならない

[73] 当該アルゴリズムや鍵長は、すでに保護されている情報を処理するために使用されることがあるが、そうすることに対してリスクがある場合がある

5.2 暗号鍵管理システム

鍵管理システムの開発のため、複数の文書が用意されている：SP 800-130[74]（5.2.1 節を参照）、SP 800-152[75]（5.2.2 節を参照）、及び非対称鍵暗号に利用される公開鍵基盤に関する文書（5.2.3 節を参照）である。

暗号鍵管理システム（CKMS）には、ポリシー、手順、コンポーネント及びデバイスが含まれており、これらを利用して鍵情報の保護、管理、及び配付を行う。CKMS には、鍵もしくは鍵に付随する他の情報にアクセスできる全てのデバイスもしくはサブシステムを含む。デバイスは、コンピュータ、携帯電話、タブレット、又はその他のスマートデバイス（自動車、警報システム、冷蔵庫など）である可能性がある。

5.2.1 鍵管理フレームワーク

SP 800-130 には、CKMS の設計者が CKMS 設計仕様を開発する際に考慮**すべき**トピックが含まれている。トピックには、セキュリティポリシー、暗号鍵及びメタデータ、相互運用性及び移行、セキュリティコントロール、テスト及びシステム保証、災害復旧、及びセキュリティアセスメントを含んでいる。

それぞれのトピックについて、SP 800-130 では、設計者が対応する必要がある 1 つ以上の文書化要件を指定している。

- CKMS 設計の定義で、重要な CKMS の性能の仕様を要求すること
- CKMS 設計者が、包括的な CKMS に必要な要素を考慮することを奨励すること
- 異なる CKMS やその能力を論理的に比較すること
- 実装されたりサポートされたりした CKMS 機能の仕様を要求して、セキュリティアセスメントを実行すること
- 組織で使用する CKMS の特定の要件を指定するプロファイルを開発するための基礎を作ること

5.2.2 鍵管理システムプロファイル

SP 800-152 には、米国連邦政府組織とその請負業者による CKMS の設計、実装、調達、設置、構成設定、管理、運用及び使用についての要件が含まれている。プロファイルは SP800-130（5.2.1 節を参照）に基づいている。SP 800-152 は、要件を規定し、特別なセキュリティ要求があってベースとなるセキュリティサービスと鍵管理サービスの強化を希望する連邦政府組織への推奨事項を示し、さらに実装したり使用したりすることが望ましいと思われる追加機能を提案している。

CKMS 設計に組み込まれるべき設計要件を提供するのに加えて、SP 800-152 は連邦政府 CKMS（FCKMS）に対する要件も記している。なお、FCKMS はサービスプロバイダによって運営され、それには連邦政府機関自身、もしくは 1 つ以上の連邦政府機関と請負業者との契約の下で FCKMS を運用する第三者がなる可能性がある。

このプロファイルは、以下のことを目的としている：

---

[74] SP 800-130, *A Framework for Designing Cryptographic Key Management Systems.*
[75] SP 800-152, *A Profile for U. S. Federal Cryptographic Key Management Systems (CKMS).*

- CKMS 設計者及び実装者が、適切な暗号アルゴリズムと鍵をサポートし、鍵に付随するメタデータを選定し、機微な米国連邦政府のコンピューティングアプリケーションとデータを保護するプロトコルを選定することを支援する
- FCKMS のテスト、調達、設置、構成設定、管理、運用、メンテナンス及び使用に関する要件を確立する
- CKMS の設計や実装を分析することで、ある CKMS と別の CKMS との容易な比較を促進し、それぞれがフレームワーク（すなわち、SP 800-130）とプロファイル（SP 800-152 など）の要件をどのように満たしているかを理解する
- 米国連邦政府機関とその請負業者が取得、処理、保管及び利用する機微で価値のある情報を保護するために使う鍵情報を管理する FCKMS を評価、調達、設置、構成設定、管理、運用及び使用するに必要なものが何かを理解することを支援する

5.2.3 公開鍵基盤

PKI は、セキュリティ基盤であり、公開鍵証明書を生成・管理する。これにより、公開鍵（つまり、非対称鍵）暗号の利用を容易にする。この目的を実現するために、PKI は以下の 2 つの基本的役割を実行する必要がある：

1. 公開鍵証明書を生成し、提供する。その公開鍵証明書は、結び付けるべき情報の正確性を検証した*後に*、公開鍵を対応するプライベート鍵の所有者に関連する識別子[76]及びその他に必要な情報と結びつける。
2. 期限切れ前に失効した証明書のための証明書ステータス情報を維持し提供する

2 つのタイプの証明書が一般的に利用される：デジタル署名を検証するために使用される公開鍵を提供するために使われる証明書、及び鍵確立のために使用される公開鍵を提供するために使われる証明書である。デジタル署名に関連する各証明書は、FIPS 186 で承認されたデジタル署名アルゴリズム（DSA、ECDSA、EdDSA 又は RSA（3.3 節を参照））のいずれか一つの公開鍵を提供する。鍵確立に使用される公開鍵を伝える証明書は、以下の 2 タイプがある：鍵合意公開鍵を提供するもの（5.3.3 節を参照）、及び鍵配送公開鍵を提供するもの（5.3.4 節を参照）である。証明書内の鍵使用ビットは、その公開鍵が意図した使用目的を示す。

3.3 節で述べたとおり、公開鍵は誰にでも利用可能である。しかし、プライベート鍵は秘密に保たれなければならず、当該プライベート鍵を所有し、使うことを認可されたエンティティだけが使えるようにしなければならない。エンティティは、人、組織、デバイス又はプロセスであり、例えばネットワークサーバも含まれる。人ではないエンティティ（デバイスやプロセスなど）の場合、その鍵情報を管理するために一人以上の人が当該エンティティの代理者又は保証人として指名される。その代理人又は保証人は、一度システムに入力された全ての秘密鍵情報へのアクセス権を持つ**べきではない**。この場合、プライベート鍵の保有者（デバイスやプロセスなど）は、証明書の所有者（すなわち、人である代理者又は保証人）と同じではない。

依拠当事者は、証明書及び当該証明書を発行した CA（認証局）に依存するエンティティのことであり、証明書の所有者の ID、証明書内の公開鍵と関連アルゴリズム、全ての関連パラメータの有効性、並びに対応するプライベート鍵に対する当該プライベート鍵所有者の所持証明を検証する。

---

[76] 識別子は、所有者に関連する公知の識別子（所有者の個人名など）や、所有者を表すために使用される別名や仮名である可能性がある

プライベート鍵の紛失、もしくは危殆化した場合は、以下のような影響を及ぼす：

- デジタル署名の生成に使用するプライベート鍵を紛失した場合、所有者はデジタル署名を生成できなくなる。ポリシーによっては、運用継続のためにプライベート鍵のバックアップコピーを持つことを許可している場合があるが、この方法は推奨できない。つまり、代替策は、単純に新しい鍵ペアと証明書を生成することである。
- デジタル署名の生成に使用するプライベート鍵が危殆化した場合、依拠当事者は当該プライベート鍵を使って生成されたデジタル署名を信用できなくなる（例えば、誰かが偽情報を提供するために署名を使用している可能性がある）。
- 鍵確立に使用するプライベート鍵（例えば、鍵配送もしくは鍵合意に使われる鍵）を紛失した場合、当該鍵を復元するか交換するまで、それ以上の鍵確立プロセスを行うことはできない。もし鍵によって保護されたデータを復元するためにその鍵が必要であれば、当該鍵が復元できない限りその保護されたデータは失われる。例えば、鍵が暗号化されたデータの復号鍵を配送するために使われていたとして、その鍵を紛失した場合、暗号化されたデータを復号することはできない。重要なデータへのアクセスが失われないことを確実にするために、PKI では、復元の可能性のためにプライベート鍵－確立鍵をバックアップすることも多い。
- 鍵確立に使用するプライベート鍵が危殆化した場合、当該鍵を利用した全てのトランザクションが信用できなくなる（例えば、プライベート鍵の本当の所有者ではない誰かが、不正な目的のために“安全な”と思われているトランザクションに入ろうとしている可能性がある）

5.2.3.1 PKI コンポーネント、依拠当事者、及びその責任

拡張性を持たせるため、PKI は通常、補完的コンポーネント一式で実装され、それらのコンポーネントは各々PKI プロセスでの特定の側面に焦点を当てている。PKI の主要なタスクは、以下の論理コンポーネントに割り当てられている；その他のコンポーネントも PKI をサポートするために使われるが、ここでは述べない（詳しくは SP 800-32[77]を参照）。

- *認証局*（CA）が証明書と認証書ステータス情報を生成する。
- *登録局*（RA）では証明書[78]を申請したユーザの身元を確認し、証明書に含むべきその他の情報を認証する。

一般的に、PKI は以下のように動作する：

1. 証明書の申請書を RA に提出する
2. RA は以下のことを行う
    a) 申請者の ID と証明書を得ようとする申請者の権限を確認する
    b) 証明書に挿入される情報を確認する
    c) 申請者が、証明書に含まれる公開鍵に対応するプライベート鍵を所持していることを確認する

    この情報の正確性が、証明書を利用する際のセキュリティの要となるものである。

---

[77] SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure.*
[78] 証明書は、ユーザ用、又は証明書取得が認可されたユーザのデバイス用の場合がある

3. Step 2 で RA が実施した確認により証明書に挿入される情報が有効であることが示され、申請者の ID と権限が確認できた場合、RA は公開鍵とその他の関連情報を CA に送り、証明書の発行を要求する。
4. 証明書生成プロセスのセキュリティは、CA は信頼できる RA に対してのみ証明書を生成することを必要とする。信頼された RA から証明書要求を受けると、CA がデジタル証明書を作成し、その RA や申請者が当該証明書を利用できるようにし、レポジトリに当該証明書を預ける。RA 又は CA は、全ての証明書の棚卸リストも作るべきである。
5. 依拠当事者が公開鍵証明書を持っている他のエンティティとやり取りをする場合、依拠当事者は、他のエンティティの証明書を当該エンティティから直接入手するか、又は保管されているリポジトリから入手する必要がある。証明書を入手したのち、依拠当事者は証明書の署名を検証する。証明書が“良好”であった場合、依拠当事者は公開鍵所有者とのやり取りを安全に進めることができる。

証明書の使用が関係するほとんどのやり取りは、ユーザ（すなわち依拠当事者）には透過的である。しかしながら、ユーザ又はシステム管理者は、証明書を入手してインストールすることに責任を負う場合がある。その後、アプリケーション（例：ブラウザ）が他のエンティティとやり取りをするために証明書を使用し、ユーザはこれらの動作に気が付かない場合がある。例外として、証明書の有効期限が切れていたり失効したりした時に、この状態を示すメッセージが表示されることがある。

証明書は、あらかじめ定められた時に有効期限が切れる。多くの場合、証明書が有効期限切れになるとサービスを拒否する。証明書棚卸リストを用いることで有効期限が近づいている証明書を特定することができ、有効期限切れになる前に当該証明書を交換する時間を設けることができ、結果的にサービスの停止を避けることができる。また、証明書棚卸リストを使うことで、安全でなくなったアルゴリズムや鍵長を使用していることを検出したり、暗号インシデント（例：CA 危殆化）に対応したり、証明書のメンテナンスのための連絡先（例：証明書所有者）を変更したりすることができる。

証明書は、有効期限になる前に失効する場合がある（例えば、失効した証明書を識別する証明書失効リストを用いる）。証明書は、様々な理由で失効する可能性がある。例えば、証明書の公開鍵に対応するプライベート鍵の危殆化、証明書所有者が組織を離れたことによるものなどがある。証明書が失効すると、システムは多くの場合証明書の失効メッセージを表示し、失効理由を含めることもある。アプリケーションの実装方法や失効理由に応じて、アプリケーションは、それ以降の処理を禁止することもあるし、警告を無視して処理を続行するか単に処理を中止するかをユーザ（すなわち、依拠当事者）が指示することを許容することもある。この警告を軽視してはならない。警告を無視することは、ユーザがそうすることで直面するリスクを受け入れることを意味する。例えば、もし警告がデジタル署名証明書の危殆化を示していれば、証明書の所有者と名乗っている人以外の者が実際に公開鍵に対応するプライベート鍵を使ってデータに署名している可能性がある。データによっては、警告を無視することが注意深い行動であるとは言えないことがあるかもしれない。この警告への対応をどうするかを決定するために、ユーザは所属する組織に相談**すべきである**。

5.2.3.2 証明書検証プロセス

PKI は、図 5 に示すように、少なくとも一つの CA 及びその登録者で構成される。各登録者（User 1、User 2、及び User 3）は、自分の公開鍵とその他の情報を含む証明書を取得する。その証明書は CA によって署名される。CA の全ての登録者には、当該 CA の公開鍵が提供される。

これがどのように機能するかの基本的な例として、User 3 がある文書に署名し、署名された文書を User 1 に送信したとする。また、User 1 は署名された文書の内容と情報源を検証する必要があるとする。これは、以下のようにして達成される：

1. User 1 は、文書に署名した際に使用したプライベート鍵に対応する公開鍵を含む証明書を入手する（つまり、User 1 が User 3 の証明書を入手する）。User 3 がその証明書を提供するか、もしくは他の提供先（例えば CA）から証明書を入手する。
2. User 1 は User 3 の証明書を CA の公開鍵を使って検証する。
3. その後、User 1 は User 3 の証明書の公開鍵を使って、User 3 から受信した署名された文書の署名を検証する。もし署名が正しく検証されれば、User 1 は、User 3 が署名を生成し、署名が生成された後に認可されていない変更が文書に加えられていないことを知ることができる。

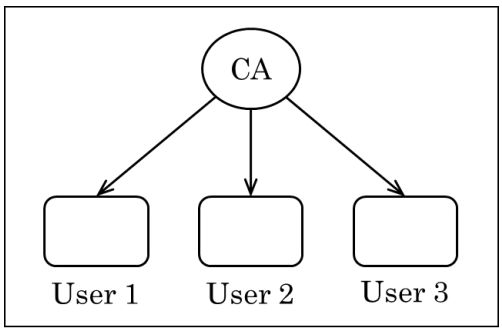

図 5：基本的な証明書の検証例

もっと複雑な別のシナリオが存在する。例えば、異なる CA に登録しているユーザが、互いの証明書に署名することによって相互認証された CA を使って、やり取りする必要がある場合などである。相互認証は、“クロス証明書”と呼ばれる証明書の互いの公開鍵に署名することにより、2 つの CA 間の信頼関係を確立することである。クロス証明書は、単一の信頼できるルート CA から複数の他の CA への信頼連鎖を構築するための手段を提供する。これによって、ある CA ドメインの登録者が、他の CA ドメインの登録者との間で安全にやり取りすることができる（例えば、ある CA ドメインの登録者が、他のドメインの登録者の ID の保証、及び証明書によって提供される他の情報の正確性の保証を得る）。

5.2.3.3 CA 証明書ポリシーと証明書実践ステートメント

各 CA は、証明書ポリシーと証明書実践ステートメントを定めている。ITU[79] Recommendation X.509 で定義されているように、証明書ポリシー（CP）は “名前付きのルール群であり、共通のセキュリティ要件を持つ特定のコミュニティやアプリケーションのクラスに対する証明書の適応性を表すものである”。CP は、当該ポリシーを使う CA が発行する証明書を信頼する依拠当事者コミュニティの期待及び要件を定義する。CP は、鍵の生成や保管などに関する課題に対処する；例えば、証明書生成；鍵預託[80]及び鍵復元；証明書失効リスト（CRL）の生成と配付を含む証明書ステータスサービス；セキュリティ監査、構成設定管理、アーカイブなどのシステム管理機能などである。

証明書実践ステートメント（CPS）は、特定の CA が公開鍵証明書を発行し、管理する方法を記述している。CPS は、CA に登録しているコミュニティやアプリケーションに適用可能な CP から導き出される。

連邦政府公開鍵基盤（FPKI）は、連邦政府が利用するために確立されている（詳細については 5.2.3.4 節を参照）。

---

[79] International Telecommunication Union.

[80] 必要に応じて（紛失や破損などの理由で）鍵を復元できるようにするため、鍵又は鍵を再構成できる情報を保存すること

NISTIR 7924[81]のドラフトは、証明書の安全な発行をサポートするためのセキュリティコントロールと実践のベースライン一式を特定している。NISTIR 7924 は、特定のコミュニティ向けの CP 又は特定の CA 向けの CPS を作成するためのテンプレートとガイドとして利用できるように設計されている。

5.2.3.4 連邦政府公開鍵基盤

連邦政府公開鍵基盤（FPKI）は、デジタル証明書と公開－プライベート鍵ペアの管理するための共通インフラを連邦政府に提供している。FPKI のネットワークに関連する部分（通常、“ブリッジ”と呼ばれる）は、様々な機関が指定する“主要 CA”で構成される。ブリッジ内の各 CA は、ブリッジ内の他の全ての CA と相互認証されており、したがって FPKI 内の全ての CA 間で信頼関係のルートが確立される。各主要 CA は、また、ブリッジの一部ではない他の CA と関連していてもよい。FPKI の証明書ポリシーや証明書実践ステートメントを含む FPKI の詳細については、https://www.idmanagement.gov/topics/fpki/を参照されたい。

5.3 鍵確立

鍵確立は、鍵を生成して、当該鍵の使用を認可されたエンティティに提供するための手段である。鍵確立を実行するシナリオには、以下のようなものがある。

- 一つのエンティティが鍵を生成（5.3.1 節を参照）し、他のエンティティに当該鍵を提供することなく使用する（例えば、ローカルに保存するデータを保護するために）。
- 鍵が、2 つ以上のエンティティ間で既に共有している鍵から導出される（5.3.2 節を参照）。
- 2 つのエンティティが、鍵合意スキーム（5.3.3 節を参照）を組込んだ自動プロトコルを使用した各エンティティからの貢献（すなわち、データ）を使って鍵を生成する。
- 一つのエンティティが鍵を生成して、当該鍵を他の一つ以上のエンティティに提供する。その際、手動の方法（印刷物で又はフラッシュメモリーなどに保管された電子形式で鍵を宅配便や面談時に渡す）か、又は鍵配送スキームを組込んだ自動プロトコルを使うかのどちらかで提供する（5.3.4 節と 5.3.5 節を参照）。

5.3.1 鍵生成

暗号鍵は、ほとんどの暗号アルゴリズムで必要であるが、他の暗号プロセスの構成部品（例：HMAC）として使用されていないハッシュ関数は例外である。SP 800-133[82]は、**承認された**暗号アルゴリズムで使用する鍵の生成法について述べている。

全ての鍵は、**承認された**乱数ビット生成器（RBG）の出力に直接的又は間接的に基づいていなければならず、FIPS 140 認証暗号モジュール内で生成されなければならない（FIPS 140 参照）。モジュールが要求する全ての乱数値は、暗号モジュール内で生成されたものでなければならない。

SP800-133 は、RBG から直接鍵を生成するためのガイダンスを示し、特定のアルゴリズムの鍵生成に必要な追加情報について別の文書を参照している。

- FIPS 186 は、デジタル署名生成で使う鍵ペアを生成するためのルールを記している。

---

[81] NISTIR 7924, *Reference Certificate Policy (Second Draft).*

[82] SP 800-133, *Recommendation for Cryptographic Key Generation.*

- SP 800-108 は、事前共有鍵から鍵を生成する方法を記している（以下の 5.3.2 節も参照）。
- SP 800-56A は、Diffie-Hellman 及び MQV 鍵合意スキームでの鍵ペアを生成するためのルールを規定している（以下の 5.3.3 節も参照）。
- SP 800-56B は、RSA 鍵合意スキーム及び RSA 鍵配送スキームでの鍵ペアを生成するためのルールを規定している（以下の 5.3.3 節及び 5.3.4 節も参照）。
- SP 800-132[83]は、パスワードから鍵を生成するためのルールを規定している。

5.3.2 鍵導出

鍵導出は、秘密情報から鍵を生成することに関係しているが、生成プロセスでは秘密でない情報もまた秘密情報に追加して使用することがある。典型的に、秘密情報は、その後のやり取りのために同一の鍵を導出することが必要なエンティティ間で共有される。秘密情報とは、エンティティ間で既に共有されている鍵（つまり、事前共有鍵）か、又は鍵合意スキーム（5.3.3 節を参照）で導出された共有秘密である。

SP 800-108 では、事前共有鍵を使用する鍵導出関数をいくつか規定している。事前共有鍵は、以下のようなものである：

- あるエンティティによって生成され、一つ以上の他のエンティティに手動の手段（例：宅配便又は面談）で提供される。
- 自動鍵合意スキーム（5.3.3 節を参照）を使用してエンティティ間で合意される。
- あるエンティティによって生成され、自動鍵配送スキーム（5.3.4 節及び 5.3.5 節を参照）を用いて他のエンティティに提供される。

SP 800-56C と SP 800-135[84]は、鍵合意（5.3.3 節を参照）の際に生成される共有秘密から鍵を導出する方法を示す。

5.3.3 鍵合意

鍵合意は鍵確立手順のことであり、その中で結果として得られる鍵材料は鍵合意プロセスへの全ての参加者から提供された情報の関数になっている。つまり、どの参加者も、他の参加者の貢献なしに結果として得られる鍵材料の値を予測することができない。鍵合意は、通常、自動化プロトコルを用いて実行される。

SP 800-56A と SP 800-56B は、複数の自動化された二者間鍵合意スキーム（つまり、2 つの当事者が関係する鍵合意スキーム）を紹介している。それぞれのスキームでは、共有秘密を生成し、その共有秘密から SP 800-56C で規定された又は承認された鍵導出手法を使用して鍵材料が導出される。

SP 800-56A と SP 800-56B には、使用する鍵の数や、鍵が長期な値（すなわち静的）か一時的な値（ノンス、短期鍵ペアなど）かどうかによって異なる鍵合意スキームのバリエーションを含んでいる。鍵合意スキームには、2 つの参加エンティティ（イニシエータとレスポンダ）がいる。

---

[83] SP 800-132, *Recommendation for Password-Based Key Derivation, Part 1: Storage Applications.*
[84] SP 800-135, *Recommendation for Existing Application-Specific Key Derivation Functions.*

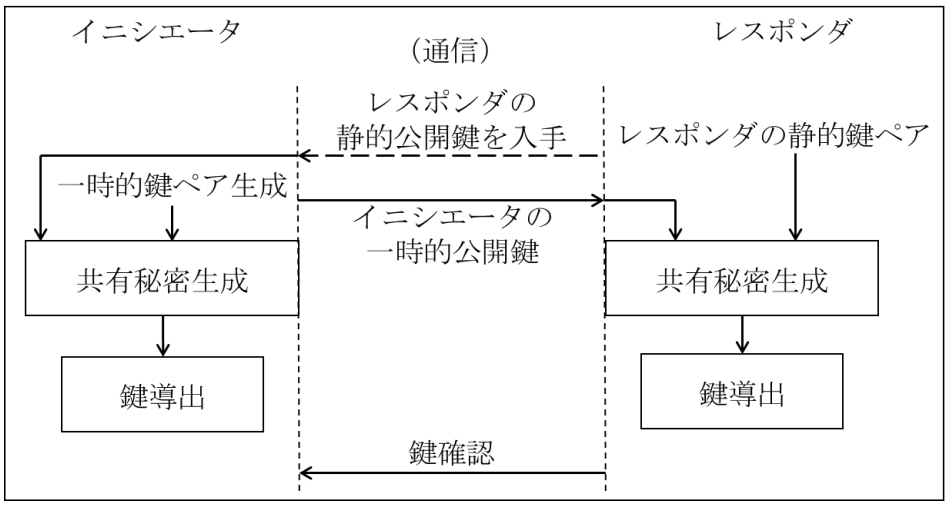

図 6：鍵合意の例

図 6 は鍵合意スキームの例を示している。ここでは、スキーム中にレスポンダは静的鍵ペアを使用し、イニシエータは一時的鍵ペアを使用している。他の鍵合意スキームでは、異なるアレンジをした鍵ペアが使われる場合もあることに注意されたい（例えば、各々の当事者が静的鍵ペアを使ってもよいし、一時的鍵ペアを使ってもよい）。上述の図で示している例では、レスポンダのプライベート鍵はレスポンダ（当該鍵ペアの所有者）が保持するが、レスポンダの公開鍵は誰に提供されてもよい。この例では、公開鍵はイニシエータに提供される。

1. イニシエータは、レスポンダの公開鍵を入手する（例えば、CA 経由、又はレスポンダから直接）; このスキームでは、この公開鍵は、鍵合意プロセスへのレスポンダの貢献ということになる。
2. イニシエータは、その後、短期鍵ペア（つまり、一時的鍵ペア）を生成し、一時的公開鍵をレスポンダに送信し、一時的プライベート鍵は自分自身のために保持する。一時的公開鍵は、このスキームでの鍵合意プロセスへのイニシエータの貢献ということになる。
3. 両当事者は、自身の鍵ペアと相手の公開鍵を使って共有秘密を生成する。
4. そして、両当事者は、共有秘密のコピーを使用して（おそらく）同一となる鍵を 1 つ以上導出する。

鍵確認は、オプションであるが強く推奨されるステップであり、両当事者がこの時点で同じ（同一の）鍵を保有していることの保証が得られる。イニシエータがレスポンダから鍵確認を受信するケースを図 6 に示す。詳細については、SP 800-56A と SP 800-56B を参照されたい。

SP 800-56A は、共有秘密を生成するために有限体又は楕円曲線の計算と非対称鍵ペアを使った Diffie-Hellman（DH）と MQV 鍵合意スキーム規定している（上述の 3.3.2.1 節を参照）。また、SP 800-58B は、2 つの RSA 鍵合意スキームを規定している（上述の 3.3.2.2 節を参照）SP 800-56A と SP 800-56B は、各鍵合意スキームが提供するセキュリティ特性の分析も提示している。

5.3.4 鍵配送／鍵配付

鍵配送とは、ある当事者（送信者）が鍵を生成し、それを他の一人以上の当事者（受信者)に配付する手段のことである。鍵配送は、手動の手段（低：宅配便）を使って達成するか、又は自動化プロトコルを使って実行する。SP 800-56B には、RSA を用いて自動化された二者間鍵配送スキームと各鍵配送ス

キームが提供するセキュリティ特性の分析を記述している（5.3.4.1 節を参照）。SP 800-71[85]は、対称鍵ブロック暗号アルゴリズム（例：AES）が保護する鍵材料を配付するスキームを提供している（5.3.4.2 節を参照）。

5.3.4.1 SP 800-56B 鍵配送

SP 800-56B では、送信者が受信者の公開鍵を用いて受信者に鍵材料を安全に配送する鍵配送方法を規定している。

図 7 は、SP 800-56B で示している鍵配送手法の簡略化した例を示している。受信者は、鍵配送トランザクションで使用される鍵ペアを持たなければならない。鍵配送は、以下のように実行される。

送信者：

1. 意図する受信者の公開鍵を入手する
2. 配送する対称鍵を生成する
3. 受信者の公開鍵を用いて対称鍵を暗号化する
4. 得られた暗号化された対称鍵を受信者に送信する

受信者：

5. プライベート鍵を使って暗号化された対称鍵を復号し、元の平文の対称鍵を得る
6. オプションで鍵確認を行う。このステップはオプションだが、両当事者がこの時点で同じ対称鍵を持っていることを保証するために強く推奨される。

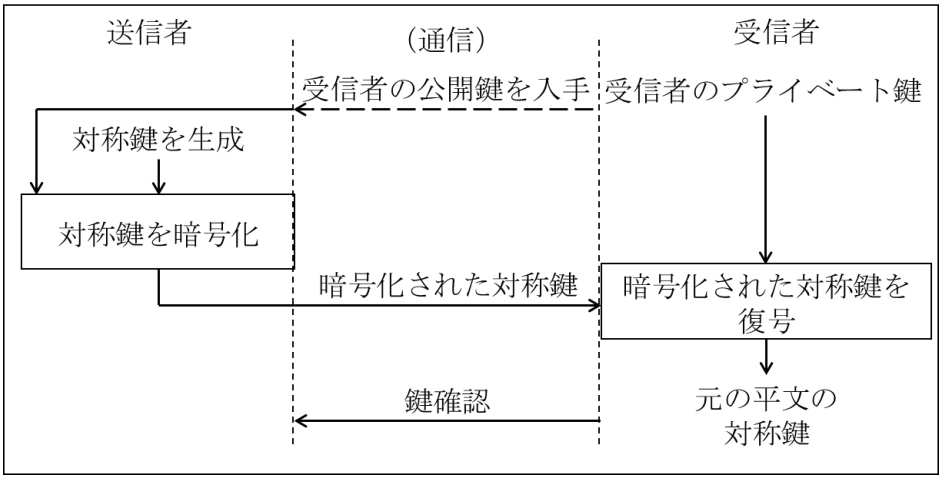

図 7：SP 800-56B 鍵配送の例

[85] SP 800-71, *Recommendation for Key Establishment Using Symmetric Block Ciphers.*

5.3.4.2 SP 800-71 鍵配付

SP 800-71 では、対称鍵暗号を使う鍵配付における鍵材料の保護を取り扱う。**承認された**鍵ラッピング手法（5.3.5 節を参照）を用い、鍵のラッピング（つまり、完全性保護した鍵の暗号化）、当該鍵へのメタデータの関連付け、及び配付される鍵情報の完全性の保護のための技術を説明している。

複数の鍵配付アーキテクチャが記されている。これらには以下のものが含まれる。

- 鍵ラッピング鍵を共有している通信グループ間（例：エンティティのペア）での鍵配付
- 鍵生成・配付センタによる登録者への鍵配付
- 一人以上の登録者に配付するためにある登録者が生成した鍵を保護して配布するために鍵変換センタを利用する方法
- 組織ドメイン間での鍵配付のために複数のセンタを設ける環境

SP 800-71 では、鍵配付のプロトコルを規定しないが、鍵配付プロトコルに加**えるべき**鍵配付通信のオプションとトランザクション内容について提案している。

5.3.5 鍵ラッピング

鍵ラッピングは、鍵（及び場合によっては他の情報）の機密性と完全性の保護を提供するために使う手法であり、対称鍵ブロック暗号アルゴリズムと送信者と受信者の両方が知っている対称鍵ラッピング鍵を使う。従って、ラッピングされた鍵材料を安全に保管、もしくは送信（つまり、配付）することができる。

鍵材料のラッピングを解くには、元のラッピングプロセスで使われたものと同じアルゴリズムと鍵ラッピング鍵を使うことが必要である。

鍵ラッピングは単純な暗号化とは異なっており、ラッピングプロセスには暗号化と完全性保護の両方を含んでいる。ラッピングを解くプロセスでは、ラッピングされた鍵材料への偶発的又は意図的な変更を検知するために完全性検証の手段を利用する。

SP 800-38F[86]では、3 通りの鍵ラッピング手法を規定し、また SP 800-38 の他のモード（もしくはモードの組合せ）を承認している。手法やモードによって、AES もしくは TDEA のどちらかを用いることができる。

5.3.6 パスワードからの鍵導出

鍵は、パスワードから導出することができる。ほとんどのパスワードは簡単に推測されることから、この方法で導出された鍵はほとんどのアプリケーションに適していない。しかしながら、SP 800-132 では、電子保管アプリケーション用（例えば、ディスクドライブ全体を暗号化する場合）にパスワード[87]から鍵材料を導出するのに使うことができる関数群を規定している。

---

[86] SP 800-38F, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping.*

[87] 本文書ではパスフレーズや PIN（暗証番号）をパスワードであるとみなしていることに注意されたい

5.4 鍵管理の課題

CKMS を選定して使用する際には、いくつもの課題に取り組む必要がある。

5.4.1 手動鍵確立 vs 自動鍵確立

5.3 節で紹介したとおり、鍵は手動もしくは自動化手法の利用のいずれかによってエンティティ間で確立することができる。多くの場合、ハイブリッドアプローチが使われており、あるエンティティが一つ以上の鍵を生成して他のエンティティに手動で配付し、その後はこれらの鍵を使って他の鍵を確立する（SP 800-56A、SP 800-56B 及び SP 800-71 参照）。

手動で配付される鍵の数は、使用する暗号のタイプ（すなわち、対称方式か非対称方式か）に依存し、CKMS に求められる機能を選択する際に考慮されなければならない。

5.4.2 CKMS の選択と運用

CKMS は、利用する組織によって設計、実装、運用される可能性がある。組織は、ベンダから調達した CKMS を運用することもできるし、ベンダから CKMS を調達した第三者のサービスを調達することもできる。どのような選択をするにしても、組織は、利用する CKMS が当該組織の情報が必要とする保護を提供することを確認する必要がある。SP 800-130 と SP 800-152 では、連邦政府組織が対処する必要がある考慮事項を述べている。これには、CKMS のスケーラビリティ、鍵に付随させるべきメタデータなどが含まれる。

5.4.3 鍵の保管と保護

鍵は、様々な場所に保管し、様々な方法で保護することができる。鍵は、金庫に保管することもできる。鍵は、認証された暗号モジュール内にのみ存在することもできる。その場合、設計に依存するが、そのモジュール自体が適切に鍵を保護できる。鍵は、電子メディア（フラッシュドライブなど）に保管することもできる。その場合、鍵はラッピングされる（つまり、暗号化と完全性保護が行われる）か、鍵コンポーネントに分割して一人では鍵を特定できないようにする必要があるかもしれない。これらの課題は、運用中の鍵に対して対処する必要がある。

ある種の鍵はバックアップを取る必要がある場合がある。なぜなら、運用中の鍵が不注意で紛失したり変更されたりした場合に復元して処理を再開することができるようにするためである。また、鍵によっては長期保管のためにアーカイブする必要のある場合もある（例えば、法的要求がある場合やアーカイブされたデータを復号する場合など）。鍵をバックアップしたりアーカイブしたりした場合はいつでも鍵復元機能が必要になる。この機能は、許容できる時間内に復元することの認可を受けたエンティティによってのみ鍵を復元できるように設計する必要がある；鍵バックアップ、鍵アーカイブ、及びバックアップやアーカイブされた鍵の復元に関する詳細については、SP800-57 Part 1 を参照されたい。

5.4.4 暗号利用期間

暗号利用期間は、特定の鍵の使用が認可されている期間のことである。鍵の暗号利用期間は、いくつかの理由により指定される。例えば、鍵が危殆化したときに暗号化されたデータの漏えい量を制限することなどである。暗号利用期間は、通常、熟慮して決めた期間、又はその鍵によって保護されるデータの最大量によって指定される。暗号利用期間を定めるのに関連するトレードオフとして、漏えいのリスクと結果が影響する。SP800-57 Part 1 の 5.3 節では、暗号利用期間の設定の必要性、適切な暗号利用

期間を定める際に考慮すべき要素、及び暗号利用期間の長さに関するいくつかの提案について、より詳細な説明を提供している。

5.4.5　認証暗号アルゴリズム及び認証暗号モジュールの使用

暗号アルゴリズムは認証されていなければならず、かつ FIPS 140 認証暗号モジュールに実装されていなければならない。暗号機能を持つほとんどの IT 製品では、その製品の機能性や提供されるセキュリティについて表明している。機微データを保護する際、それらの製品の FIPS 140 認証暗号モジュールを使うことで、当該製品に記載されているセキュリティの主張が有効であることの最低限の保証をすることができる。

暗号サービスを提供する全ての製品の中核をなすのは、暗号モジュールである。暗号モジュールには暗号アルゴリズムが含まれており、製品やシステムがセキュリティサービス（機密性、完全性、認証など）を提供する際に使用される。暗号はセキュリティを提供するために使用するが、貧弱な設計や弱いアルゴリズムなどの欠点は、製品が安全でない状態にし、機微情報を大きなリスクにさらすことになる可能性がある。暗号モジュール及びその基礎となる暗号アルゴリズムについて、確立された標準に沿って適切にテストし認証することは、セキュリティを保証するうえで不可欠である。

NIST は、**承認された**暗号アルゴリズムの実装及びそれらが使われている暗号モジュールを認証するためのプログラムを確立している：暗号アルゴリズム認証プログラム [88]（CAVP）と暗号モジュール認証プログラム [89]（CMVP）である。

暗号モジュールのセキュリティ要件の説明については、本文書の 5.1.2 節を参照されたい。

5.4.6　鍵材料のコントロール

鍵へのアクセスは、コントロールされる必要がある。鍵へのアクセスは、認可されたエンティティに対してのみ、かつ認可された目的のためだけに認める**べきである**。例えば、鍵配送用に指定された鍵は、デジタル署名の生成や認証のために用いてはならない。

鍵の拡散についてもコントロールする必要がある。鍵のコピーを作ることは便利なことが多いが、これら余分なコピーの必要性を説明する必要がある。鍵が危殆化した場合、その後の不正使用を防ぐために、当該鍵と全てのコピーを破棄する必要があるかもしれない。例えば、デジタル署名の生成に使われるプライベート鍵が危殆化して、元のコピーが破棄された後にも当該鍵のコピーが残っていた場合、後々そのコピーを使って不正なデジタル署名が作成される可能性がある。

ユーザには責任と責務の一覧を提供しなければならず、各ユーザは、鍵を受け取る前にこれらの事項を認める誓約書に署名**するべきである**。ユーザは、各自の責任を認識しなければならない。とりわけ、鍵の危殆化や紛失の重大性についてはそうである。ユーザは、自分の秘密鍵やプライベート鍵を安全に保管できなければならない。なぜなら、侵入者がそれらにアクセスできないようにしなければならないが、合法的な利用の際には当該鍵が容易にアクセスできるようにしなければならないからである。

5.4.7　危殆化

鍵が危殆化した、又は危殆化が疑われる場合の対応計画を持つことは必須である。とりわけ、中心となるサイトで使用・管理されている鍵（例えば、CA が証明書に署名するために使う鍵）はそうである。

---

[88] CAVP についての情報は https://csrc.nist.gov/projects/cavp を参照

[89] CMVP についての情報は https://csrc.nist.gov/projects/cmvp を参照

危殆化復旧計画は、システムが運用に入る前に策定されるべきであり、危殆化したシステムのソフトウェアやハードウェア、CA 鍵、ユーザ鍵、以前に生成された署名、暗号化データなどについてどのような措置を取るのかを取り扱っておくべきである。SP800-57 Part 1 では、鍵危殆化による影響、鍵危殆化の可能性や影響を最小化するための対策、及び危殆化復旧計画を策定する際に考慮するべき事項についての説明を含んでいる。

誰かのプライベート鍵又は秘密鍵が紛失もしくは危殆化したならば、他のユーザにそのことを知らせなければならない。なぜなら、それ以降、その危殆化した鍵を使用してデータの保護を開始したり、危殆化した鍵を使って保護されたデータについて受け入れることのリスクを評価して受容すると判断することなしにそのデータを受け入れたりすることがないようにするためである。この通知は、CRL もしくは危殆化鍵リスト（CKL）を使って行われることが多い；この説明は、SP 800-57 Part 1 を参照されたい。

場合によっては、鍵及びその鍵の全てのコピーは、当該鍵の危殆化が発覚した時点で直ちに破棄すべきである。例えば、デジタル署名の生成に使用されているプライベート鍵なら、直ちに破棄すべきである。しかしながら、以前に危殆化したプライベート鍵を使って生成された署名を検証するために、対応する公開鍵は利用可能な状態を維持しておく必要があるかもしない。これらの署名を受け入れることは一定のリスクを伴うことに注意されたい。

5.4.8 説明責任と棚卸リスト管理

説明責任には、ライフサイクルを通じて、暗号鍵または証明書へのアクセス権またはコントロール権を持つエンティティを識別することが含まれる。説明責任は、以下のことを支援するのに有効なツールになり得る。例えば、鍵の危殆化を防ぐ、危殆化が検知された際にその影響を軽減する、危殆化が発生した際に関与した可能性がある個人を特定する、鍵へアクセスしたことが知られるとユーザが理解することで鍵を危殆化させることを思いとどませる、鍵が使われた場所及び危殆化した鍵で保護された（つまり、同時に危殆化したかもしれない）データやその他の鍵の内容を判断する、などである。公開鍵証明書を利用する際、説明責任は、証明書の管理（例えば、証明書の有効期限が切れたりプライベート鍵が危殆化した際に証明書を交換すること）に関して責任を負う人が誰なのかを判断するために使われる

鍵又は証明書の棚卸リストは、説明責任を補助するツールとして利用できる。棚卸リスト管理とは、鍵や証明書の棚卸リストを作成して維持することに関係する；例えば、所有者、代理人もしくは保証人を指定し追跡すること（例えば、所有者、代理人もしくは保証人が誰（もしくは何）であり、どこにいて、どのように連絡が取れるか、など）；鍵と証明書の棚卸リストへの登録を自動化すること；鍵と証明書のステータスを監視すること（例えば、有効期限や鍵が危殆化したかどうか、など）；必要に応じて、是正措置のために、適切な責任者にステータスを報告すること、がある。SP800-57 Part 1 では、鍵と証明書の両方の棚卸リスト管理に関する説明を記載している。

5.4.9 監査

監査は、鍵の危殆化に対する予防、検知及び復旧のために使われるメカニズムである。適切な鍵管理を保証するためには、いくつかのタイプの監査を実施する必要がある：

- 適合性監査は、組織が規制ガイドラインを遵守しているかどうかの包括的なレビューのことである。適合性監査人は、セキュリティポリシー（例：鍵管理ポリシー）、及びユーザのアクセスコントロールとリスク管理手順をレビューして、これらのコントロールや手順がポリシーをサポートしているかどうかを判断する。
- 採用されている保護メカニズム（例えば、利用している暗号アルゴリズムや鍵長）に対する監査が必要であり、現在提供されているセキュリティレベル、及び将来的に必要とされ、提供される

と期待されるセキュリティレベルを再評価する。このことは、そのメカニズムが正しく、かつ効果的に適切なポリシー（例えば、鍵管理ポリシー）をサポートしているかどうかを判断するために必要である。新しい技術の開発や新しい攻撃手法を考慮に入れる必要がある。

- 鍵管理システムの利用、運用及び維持にかかわる担当者の行動に対する監査が必要であり、その担当者が確立されたセキュリティ手順を継続的に遵守しているかを検証する。極めて異常なイベントについては留意し、システムへの攻撃試行などの可能性指標としてレビューされる。

6 その他の課題

暗号の利用は、徹底したリスク分析、保護すべき情報の機微度及び利用するセキュリティコントロールの決定なしには実施**すべきではない**（FIPS 199、SP 800-175A、SP 800-53 を参照）。リスク評価を行って保護すべき情報の機微度（低、中、高）及び利用するセキュリティコントロールを決定したら、暗号を正しく利用することを確実にするために、いくつもの課題に対応する必要がある。

本節では、アプリケーションに暗号が必要であると判断した後に対応すべき課題を特定する。

6.1 必要なセキュリティ強度

最低限必要なセキュリティ強度は、情報の機微度（FIPS 199 を参照）によって定まる。SP 800-152 は、低インパクトの情報保護には最低 112 ビット、中インパクトの情報には最低 128 ビット、高インパクトの情報には最低 192 ビットのセキュリティ強度を要求している。これによって、要求されるセキュリティ強度は、使用するアルゴリズムと鍵長を決定するために使用することができる。SP 800-57 Part 1 の 5.6 節は、適切なアルゴリズムと鍵長を選定する際の表を提供している。

多くのアプリケーションは、異なる複数の暗号アルゴリズムを使用する必要がある。理想的には、これらのアルゴリズムが全て同じセキュリティ強度を提供することだが、パフォーマンスや可用性、相互運用性の理由により、その限りではない。データ保護のために強度の異なる複数のアルゴリズムを同時に利用した場合、アルゴリズムの組み合わせで得られるセキュリティは、最も弱いセキュリティ強度をもつアルゴリズムに関連付けられた強度になる（SP 800-57 Part 1 の 5.6 節を参照）。例えば、2048 ビットの RSA は 112 ビットセキュリティ強度をサポートしているが、128 ビットセキュリティ強度をサポートしている SHA-256 との組み合わせて使われることがよくある。この組み合わせを使ってデジタル署名を生成した場合、その署名は 112 ビットセキュリティ強度しか提供できない。つまり、これは 2 つのアルゴリズムが提供する強度の弱い方にあたる。

承認されたアルゴリズムの組み合わせ（暗号スイートと呼ばれる）がいくつかのプロトコルで提供されており、SP 800-57 Part 3（S/MIME 向け）と SP 800-52（TLS 向け）に示されている。

6.2 相互運用性

相互運用性は、あるエンティティが別のエンティティと通信する能力のことである。ここでのエンティティは、人、デバイス、もしくはプロセスであるかどうかにかかわらない。通信するために、エンティティは以下のことを備えなければならない：

1. 通信チャネル（例：インターネット）及び同じ通信プロトコル（例：TLS）
2. エンティティ同士での通信を容認するポリシー

安全に通信できるためには、当該エンティティはまた以下のことも備えなければならない：

3. 各エンティティは、それぞれの独自のポリシーを実施しているという信頼がある
4. 4 節で述べた相互運用可能な暗号機能がある
5. 安全に確立された適切な鍵材料を共有している（5.3 節を参照）

例えば、エンティティ A と B が 2 つの異なる組織に所属しており、かつ

- それぞれの組織で、エンティティが通信することを容認するポリシーがある
- 各エンティティは、相手のエンティティが独自のポリシーを実施していると信頼している
- 通信に利用できる TLS 機能がある
- 各エンティティは、128 ビットの AES を使って情報の暗号化と復号ができ、3072 ビットの RSA 鍵配送（5.3.4.1 節を参照）を使って鍵確立ができる、そして
- 一方のエンティティが AES の 128 ビット鍵を生成できて鍵配送スキームの送信者として動作することができ、もう一方のエンティティが 3072 ビットの RSA 鍵ペアを持っており受信者として動作することができる場合に、

その 2 つのエンティティは、128 ビット鍵を確立して AES を利用した情報の暗号化が行うことができる安全で相互運用可能な通信チャネルを持っていることになる。この場合、AES を利用した暗号処理で得られるセキュリティ強度は 128 ビットである。なぜならば、3072 ビット RSA と 128 ビット AES（AES-128）の両方ともセキュリティ強度 128 ビットと格付けされているからである（6.1 節を参照）。

6.3 アルゴリズムが承認されなくなった場合

あるアルゴリズムが適切な保護を提供できず**承認されなくなった**場合（例えば、そのアルゴリズムが破られた可能性がある）、リスク評価を実施して、セキュリティで保護されるべき残りの期間の情報保護のために**承認されている**アルゴリズムと鍵長を使用して再保護化すべきであるかどうか決める必要がある。詳細な説明は、SP 800-57 Part 1 の 5.6.4 節を参照されたい。

参考文献

NIST 刊行物

以下の FIPS 及び NIST 特別刊行物（SP）が、連邦政府における暗号の使用に適用される。

FIPS 140 National Institute of Standards and Technology (2019) Security Requirements for Cryptographic Modules. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 140-3. https://doi.org/10.6028/NIST.FIPS.140-3

FIPS 140-3 は、米国政府情報を保護する暗号モジュールが満たさなければならない要件を規定する。この標準では、4 段階の質的レベルのセキュリティを提供しています。セキュリティ要件は、暗号モジュールの安全な設計と実装に関連する領域をカバーしている。

FIPS 180 National Institute of Standards and Technology (2015) Secure Hash Standard (SHS). (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 180-4. https://doi.org/10.6028/NIST.FIPS.180-4

FIPS 180-4 では、7 つの暗号学的ハッシュアルゴリズムが規定されている：SHA-1、SHA-224、SHA-256、SHA-384、SHA-512、SHA-512/224、及び SHA-512/256 である。

FIPS 185 National Institute of Standards and Technology (1994), Escrowed Encryption Standard, (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 185. Withdrawn October 19, 2015. https://csrc.nist.gov/CSRC/media/Publications/fips/185/archive/1994-02-09/documents/fips185.pdf

FIPS 185 では、電子デバイスに実装され、必要な時に政府の電気通信を保護するために利用する暗号化／復号アルゴリズムの使用及び法的執行アクセスフィールド（LEAF）の作成方法が規定されている。アルゴリズムと LEAF の作成方法を機密である。LEAF は、電気通信へのアクセスが合法的に認可された場合に、電気通信の復号のために提供されるキーエスクローシステムで使用することを目的としていた。

FIPS 186 National Institute of Standards and Technology (2013) Digital Signature Standard (DSS). (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 186-4. https://doi.org/10.6028/NIST.FIPS.186-4

National Institute of Standards and Technology (2019 Draft) Digital Signature Standard (DSS). (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 186-5. https://doi.org/10.6028/NIST.FIPS.186-5-draft

FIPS 186 は、デジタル署名を生成するために使用できるアルゴリズム一式を規定している。デジタル署名は、データへの不正な変更を検出し、署名者の身元を認証するために使用される。さらに、署名されたデータの受領者は、証拠としてデジタル署名を使用し、署名が実際に主張する署名者によって生成されたものであることを第三者

に証明することができる。これは、否認防止として知られており、署名者が後で簡単に当該署名を否認することができないからである。

FIPS 197 National Institute of Standards and Technology (2001) Advanced Encryption Standard (AES). (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 197. https://doi.org/10.6028/NIST.FIPS.197

FIPS 197 は、対称鍵ブロック暗号アルゴリズムを規定している。この標準は、128、192、256 ビットの鍵長と 128 ビットのブロック長をサポートする。

FIPS 198 National Institute of Standards and Technology (2008) The KeyedHash Message Authentication Code (HMAC). (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 198-1. https://doi.org/10.6028/NIST.FIPS.198-1

FIPS 198-1 では、メッセージ認証コード（MAC）を定義しており、MAC の計算と検証に秘密鍵と組み合わせて暗号学的ハッシュ関数を使用する。

FIPS 199 National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 199. https://doi.org/10.6028/NIST.FIPS.199

FIPS 199 は、情報及び情報システムの両方に対するセキュリティ分類を設定している。セキュリティ分類は、あるイベントが発生した場合の組織への潜在的なインパクトに基づくものである。そのようなイベントとは、割り当てられたミッションを達成し、資産を保護し、法的責任を果たし、日々の機能を維持し、個人を保護するために組織が必要とする情報及び情報システムを危険にさらすような事象のことである。

FIPS 202 National Institute of Standards and Technology (2015) SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 202. https://doi.org/10.6028/NIST.FIPS.202

FIPS 202 では、SHA3-224、SHA3-256、SHA3-384、及び SHA3-512 を規定している。この FIPS はまた、2 つの拡張可能出力関数（SHAKE128 と SHAKE256）を規定しているが、これらはそれ自体ではハッシュ関数とは見なされない。

SP 800-21 Barker EB, Barker WC, Lee A (2005) Guideline for Implementing Cryptography in the Federal Government. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-21 2nd edition. Withdrawn August 27, 2016. https://doi.org/10.6028/NIST.SP.800-21e2

NIST SP 800-21 は、連邦情報システムにおける暗号保護メカニズムの選択、指定、採用、及び評価のための構造化された柔軟性のあるガイドライン一式を提供している。

SP 800-22 Bassham LE III, Rukhin A, Soto J, Nechvatal JR, Smid ME, Barker EB, Leigh SD, Levenson M, Vangel M, Banks D, Heckert NA, Dray JF, Jr. (2010) A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. (National Institute of Standards and Technology, Gaithersburg, MD),

NIST Special Publication (SP) 800-22, Rev. 1a.
https://doi.org/10.6028/NIST.SP.800-22r1a

SP 800-22 では、真にランダムな出力と区別がつかない乱数を提供するための乱数発生器及び擬似乱数発生器の選択及びテストのいくつかの側面について説明している。

SP 800-32 Kuhn R, Hu VC, Polk T, Chang S-jH (2001) Introduction to Public Key Technology and the Federal PKI Infrastructure. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-32.
https://doi.org/10.6028/NIST.SP.800-32

SP 800-32 は、機関の意思決定者が、PKI が機関にとって適切かどうかを判断し、連邦政府機関内で PKI サービスを最も効果的に展開する方法を支援するために開発された。PKI 機能とそのアプリケーションの概要を提供することを目的としている。

SP 800-38 ブロック暗号アルゴリズムの暗号利用モードを規定した一連の出版物（以下を参照）。

SP 800-38A Dworkin MJ (2001) Recommendation for Block Cipher Modes of Operation: Methods and Techniques. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-38A.
https://doi.org/10.6028/NIST.SP.800-38A

*SP 800-38A では、基本となる対称鍵ブロック暗号アルゴリズムで使用するための 5 つの機密性の暗号利用モードを定義している：Electronic Codebook（ECB）、Cipher Block Chaining（CBC）、Cipher Feedback（CFB）、Output Feedback（OFB）、及び Counter（CTR）である。**承認された**基本となるブロック暗号アルゴリズム（すなわち AES 又は TDEA）と一緒に使用する場合、これらのモードは機微なコンピュータデータに暗号保護を提供することができる。*

SP 800-38B Dworkin MJ (2005) Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-38B, Includes updates as of October 6, 2016.
https://doi.org/10.6028/NIST.SP.800-38B

SP 800-38B では、対称鍵ブロック暗号（すなわち、AES 又は TDEA）を基礎とするメッセージ認証コード（MAC）アルゴリズムを規定している。CMAC と呼ばれる、このブロック暗号ベースの MAC アルゴリズムは、バイナリデータの情報源と完全性の保証を提供するために使用することができる。

SP 800-38C Dworkin MJ (2004) Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-38C, Includes updates as of July 20, 2007.
https://doi.org/10.6028/NIST.SP.800-38C

*SP 800-38C では、128 ビットのブロック長を持つ対称鍵ブロック暗号アルゴリズム（すなわち、AES）の CCM と呼ばれる暗号利用モードを定義している。CCM は、コンピュータデータの機密性と完全性を保証するために使用することができ、SP 800-38A で規定されている Counter（CTR）モードと Cipher Block Chaining-Message Authentication Code（CBC-MAC）アルゴリズム（SP 800-90B で規定されているが、今は汎用目的では承認**されていない**）を組み合わせて実現する。*

SP 800-38D Dworkin MJ (2007) Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. (National Institute of Standards and

Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-38D. https://doi.org/10.6028/NIST.SP.800-38D

*SP 800-38D は、関連付けられたデータの認証暗号アルゴリズムである Galois/Counter Mode（GCM）、及び暗号化されていないデータのメッセージ認証コード（MAC）を生成するための特化版である GMAC を規定している。GCM と GMAC は、128 ビットのブロック長を持つ**承認された**対称鍵ブロック暗号（すなわち、AES）を基礎とした暗号利用モードである。*

SP 800-38E Dworkin MJ (2010) Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-38E. https://doi.org/10.6028/NIST.SP.800-38E

SP 800-38E では、IEEE 1619 を参照して AES アルゴリズムの XTS-AES モードを承認している。これは、ストレージデバイス上のデータの機密性を保護するためのオプションとして追加されて要件であるこのモードは、データやその情報源の認証を提供しない。

SP 800-38F Dworkin MJ (2012) Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-38F. https://doi.org/10.6028/NIST.SP.800-38F

SP 800-38F は、鍵ラッピングとして承認されている暗号化方式を記述している。既存の方式の承認に加えて、本刊行物では、Advanced Encryption Standard（AES）アルゴリズムの 2 つの新しい決定論的な認証暗号モード（AES Key Wrap（KW）モード及び AES Key Wrap with Padding（KWP）モード）を規定している。Triple Data Encryption Algorithm（TDEA）を基礎のブロック暗号とする類似モード（TKW と呼ばれる）も、レガシーアプリケーションをサポートするために規定されている。

SP 800-38G Dworkin MJ (2019) Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Special Publication (SP) 800-38G Revision 1. https://doi.org/10.6028/NIST.SP.800-38Gr1-draft

*SP 800-38G は、フォーマット保存暗号化のために FF1 と FF3 と呼ばれる 2 つの方法を規定している。これらの方法はいずれもが、**承認された**対称鍵ブロック暗号アルゴリズムを基礎とする暗号利用モードである。*

SP 800-52 McKay KA, Cooper DA (2019) Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-52, Rev. 2. https://doi.org/10.6028/NIST.SP.800-52r2

Transport Layer Security（TLS）は、インターネット上での電子配信中にデータを保護するためのメカニズムを提供する。SP 800-52 は、FIPS 及び NIST 推奨の暗号アルゴリズムを効果的に利用する、TLS プロトコル実装の選択と設定に関するガイダンスを提供する。これは、FIPS ベースの暗号スイートを設定した TLS 1.2 を全ての政府機関の TLS サーバ及びクライアントでサポートすることを要求し、かつ 2024 年 1

月 1 日までに TLS 1.3 をサポートすることを要求している。また、本刊行物では、セキュリティに影響を与える証明書と TLS 拡張についてのガイダンスも提供している。

SP 800-53

Joint Task Force Transformation Initiative (2017) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Special Publication (SP) 800-53, Rev. 5.
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft

SP 800-53 は、連邦情報システム及び組織のセキュリティ及びプライバシー管理のカタログを提供し、さらに組織運営（ミッション、機能、イメージ、評判などを含む）、組織資産、個人、他の組織、及び国家を、多様な脅威（例えば、敵対的なサイバー攻撃、自然災害、構造的障害、ヒューマンエラーなど）から保護するための管理を選択するためのプロセスを提供する。

SP 800-56A

Barker EB, Chen L, Roginsky A, Vassilev A, Davis R (2018) Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-56A, Rev. 3.
https://doi.org/10.6028/NIST.SP.800-56Ar3

SP 800-56A では、Diffie-Hellman と Menezes-Qu-Vanstone（MQV）鍵確立スキームのいくつかのバリエーションを含む、有限体と楕円曲線上の離散対数問題に基づく鍵確立スキームを規定している。

SP 800-56B

Barker EB, Chen L, Roginsky A, Vassilev A, Davis R, Simon S (2019) Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-56B, Rev. 2.
https://doi.org/10.6028/NIST.SP.800-56Br2

SP 800-56B では、素因数分解型暗号（RSA）を用いた鍵確立スキームを規定している。鍵配送と鍵合意の両方のスキームが規定されている。

SP 800-56C

Barker EB, Chen L, Davis R (2018) Recommendation for KeyDerivation Methods in Key-Establishment Schemes. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-56C, Rev. 1.
https://doi.org/10.6028/NIST.SP.800-56Cr1

SP 800-56C では、SP 800-56A 又は SP 800-56B で定義された鍵確立スキームで確立された共有秘密から鍵材料を導出する技術を規定している。

SP 800-57, Part 1

Barker EB (2019) Recommendation for Key Management: Part 1 – General. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Special Publication (SP) 800-57 Part 1, Rev. 5.
https://doi.org/10.6028/NIST.SP.800-57pt1r5-draft

SP 800-57 Part 1 では、暗号鍵材料の管理に関する一般的なガイダンスとベストプラクティスを提供しており、暗号を使用する際に提供される可能性のあるセキュリティサービス及び採用される可能性のあるアルゴリズムと鍵の種類の定義、鍵やその他の暗号情報の種類ごとに要求される保護の仕様及びその保護を提供する方法、鍵管理に関わる機能についての説明、及び暗号を使用する際に対処すべき様々な鍵管理の問題についての説明を含んでいる。

SP 800-57, Part 2

Barker EB, Barker WC (2019) Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-57 Part 2, Rev. 1. https://doi.org/10.6028/NIST.SP.800-57pt2r1

SP 800-57 part 2 では、米国政府機関のポリシー及びセキュリティ計画要件に関するガイダンスを提供している。SP 800-57 の本パートには、一般的な鍵管理基盤、組織的な鍵管理ポリシーステートメント及び鍵管理実践ステートメントの作成のためのガイダンス、一般的なサポートシステム及び暗号を採用する主要なアプリケーションのセキュリティ計画に組み込む必要がある鍵管理情報の特定、及び暗号を使用する全ての連邦政府のアプリケーションについて文書化する必要がある鍵管理情報の特定が含まれている。

SP 800-57, Part 3

Barker EB, Dang QH (2015) Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-57 Part 3, Rev. 1. https://doi.org/10.6028/NIST.SP.800-57pt3r1

SP 800-57 part 3 では、現在利用可能な暗号メカニズムに関連した鍵管理の問題を取り上げている。例えば、公開鍵基盤（PKI）、Internet Protocol Security（IPsec）、Secure/Multipart Internet Mail Extensions（S/MIME）、Kerberos、Over-the-Air Rekeying（OTAR）、ドメインネームシステムセキュリティ拡張（DNSSEC）、暗号化ファイルシステム、Secure Shell（SSH）プロトコルなどである。

SP 800-67

Barker EB, Mouha N (2017) Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-67, Rev. 2. https://doi.org/10.6028/NIST.SP.800-67r2

SP 800-67 では、Triple Data Encryption Algorithm（TDEA）を規定しており、その主要な構成要素の暗号化エンジンは Data Encryption Algorithm（DEA）である。

SP 800-71

Barker EB, Barker WC (2018), Recommendation for Key Establishment Using Symmetric Block Ciphers. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Special Publication (SP) 800-71. https://csrc.nist.gov/publications/detail/sp/800-71/draft

SP 800-71 では、鍵配付に対称鍵暗号を使用する鍵確立時の対称鍵材料の保護を取り扱う。また、本推奨は、鍵配付プロセス中に検出可能なエラーが発生した場合の復元についても対処する。ラッピングメカニズムが規定されており、鍵を暗号化し、当該鍵に鍵管理情報を結合し、この情報の完全性を保護する。

SP 800-89

Barker EB (2006) Recommendation for Obtaining Assurances for Digital Signature Applications. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 80089. https://doi.org/10.6028/NIST.SP.800-89

デジタル署名の生成又は検証に参加するエンティティは、当該プロセスの真正性に依存する。SP 800-89 は、有効なデジタル署名に必要な保証を得るための方法を規定している。それは、ドメインパラメータの有効性の保証、公開鍵の有効性の保証、鍵ペ

アの所有者が実際にプライベート鍵を所有していることの保証、及び鍵ペアの所有者の身元の保証である。

SP 800-90A

Barker EB, Kelsey JM (2015) Recommendation for Random Number Generation Using Deterministic Random Bit Generators. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-90A, Rev. 1. https://doi.org/10.6028/NIST.SP.800-90Ar1

SP 800-90A では、決定論的手法を用いた乱数ビット生成のための DRBG メカニズムを規定している。提供される手法は、ハッシュ関数又はブロック暗号アルゴリズムのいずれかに基づいており、選択されたセキュリティ強度をサポートするように設計される。DRBG は、DRBG がサポートするセキュリティ強度に対して十分なエントロピーを提供するランダム性のソースで初期化されなければならない。

SP 800-90B

Sönmez Turan M, Barker EB, Kelsey JM, McKay KA, Baish ML, Boyle M (2018) Recommendation for the Entropy Sources Used for Random Bit Generation. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-90B. https://doi.org/10.6028/NIST.SP.800-90B

SP 800-90B では、乱数ビット生成器で使用されるエントロピー源の設計原理及び要件を規定しており、それにはエントロピー源が故障していないことを判断するための健全性テストやエントロピー源の有効性を確認するためのテストを含んでいる。

SP 800-90C

Barker EB, Kelsey JM (2016), Recommendation for Random Bit Generator (RBG) Constructions. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Special Publication (SP) 800-90C. https://csrc.nist.gov/publications/detail/sp/800-90c/draft

SP 800-90C では、乱数ビット生成器（RBG）の実装のための構成を規定している。RBG は、決定論的乱数ビット生成器（DRBG）であっても非決定論的乱数ビット生成器（NRBG）であってもよい。そのように構成された RBG は、SP 800-90A で規定されているような DRBG メカニズムと SP 800-90B で規定されているようなエントロピー源とから構成される。

SP 800-102

Barker EB (2009) Recommendation for Digital Signature Timeliness. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-102. https://doi.org/10.6028/NIST.SP.800-102

デジタル署名が生成された時刻を確立することは、しばしば重要な考慮事項である。署名（したと主張する）時刻を含む署名メッセージは、時刻の正確性が信頼できない限り、 その時刻にプライベート鍵を使ってメッセージに署名したことを保証するものではない。信頼できるタイムスタンプ機関からのデジタル署名ベースのタイムスタンプや署名メッセージに含まれる検証者が提供したデータを適切に使用することで、署名者はメッセージが署名された時刻についてある程度の保証を提供することができる。

SP 800-106

Dang QH (2009) Randomized Hashing for Digital Signatures. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-106. https://doi.org/10.6028/NIST.SP.800-106

NIST 承認デジタル署名アルゴリズムでは、署名の生成と検証で承認された暗号学的ハッシュ関数の使用を必要とする。SP 800-106 では、署名されるメッセージをランダム化することにより、デジタル署名アプリケーションで使用される暗号学的ハッシュ関数のセキュリティを強化する方法を規定している。

SP 800-107 Dang QH (2012) Recommendation for Applications Using Approved Hash Algorithms. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-107, Rev. 1. https://doi.org/10.6028/NIST.SP.800-107r1

任意長のメッセージから固定長のメッセージダイジェストを計算するハッシュ関数は、情報セキュリティの多くの目的で広く利用されている。SP 800-107 では、FIPS 180 で規定されている承認されたハッシュ関数を採用する暗号アプリケーションに必要な、又は所望のセキュリティ強度を達成するためのセキュリティガイドラインを提供している。これには、デジタル署名と鍵付きハッシュメッセージ認証コード（HMAC）の生成と検証、及びハッシュベースの鍵導出関数（ハッシュベース KDF）の使用が含まれる。

SP 800-108 Chen L (2009) Recommendation for Key Derivation Using Pseudorandom Functions (Revised). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-108, Revised. https://doi.org/10.6028/NIST.SP.800-108

SP 800-108 では、事前に共有された秘密鍵（すなわち、鍵導出鍵）から擬似乱数関数を使用して追加の鍵材料を導出するための技術を規定している。鍵生成鍵は、鍵生成スキームによって確立されたものであってもよいし、他の方法で共有されたものであってもよい(例えば、手動での鍵配布)。

SP 800-130 Barker EB, Smid ME, Branstad DK, Chokhani S (2013) A Framework for Designing Cryptographic Key Management Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-130. https://doi.org/10.6028/NIST.SP.800-130

SP 800-130 には、CKMS 設計仕様を開発する際に、CKMS 設計者が考慮すべきトピックが含まれている。トピックには、セキュリティポリシー、暗号鍵及びメタデータ、相互接続性と移行性、セキュリティコントロール、テストとシステムの保証、災害復旧、及びセキュリティ評価が含まれる。

SP 800-131A Barker EB, Roginsky A (2019) Transitioning the Use of Cryptographic Algorithms and Key Lengths. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-131A, Rev. 2. https://doi.org/10.6028/NIST.SP.800-131Ar2

SP 800-57 Part 1 の 5.6.4 節では、アルゴリズムが破られた場合や、暗号鍵を効率的に探索するために使用できるより強力なコンピュータが利用可能になった場合に、新しい暗号アルゴリズム及び鍵長に移行するための推奨事項を提供している。SP 800-131A は、このような移行のためのより具体的なガイダンスを提供している。アルゴリズムとサービスごとに SP 800-131A で扱われ、その使用が許容されるか、非推奨と

されるか、制限されるか、レガシーアプリケーションでのみ許可される[90]か、又は禁止されるかを示している。

SP 800-132 Sönmez Turan M, Barker EB, Burr WE, Chen L (2010) Recommendation for Password-Based Key Derivation: Part 1: Storage Applications. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-132.
https://doi.org/10.6028/NIST.SP.800-132

SP 800-133 では、承認された暗号アルゴリズムで管理・使用される鍵の生成について説明している。

SP 800-133 Barker EB, Roginsky A (2019) Recommendation for Cryptographic Key Generation. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-133 Revision 1.
https://doi.org/10.6028/NIST.SP.800-133r1

*SP 800-133 では、**承認された**暗号アルゴリズムで管理・使用される鍵の生成について説明している。*

SP 800-135 Dang QH (2011) Recommendation for Existing Application-Specific Key Derivation Functions. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800135, Rev. 1.
https://doi.org/10.6028/NIST.SP.800-135r1

広く使用されている多くのインターネットセキュリティプロトコルには、独自のアプリケーション固有の鍵導出関数（KDF）があり、暗号機能に必要な暗号鍵を生成するために使用される。SP 800-135 では、それらの KDF に対するセキュリティ要件を提供している。

SP 800-152 Barker EB, Branstad DK, Smid ME (2015) A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-152.
https://doi.org/10.6028/NIST.SP.800-152

SP 800-152 には、米国連邦機関及びその請負業者による、又は米国連邦機関及びその請負業者のための CKMS の設計、実装、調達、設置、構成、管理、運用、及び使用に関する要求事項が含まれる。このプロファイルは、SP 800-130 に基づく。

SP 800-175A Barker EB, Barker WC (2016) Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates, and Policies. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-175A.
https://doi.org/10.6028/NIST.SP.800-175A

SP 800-175A では、暗号を使用するための要件の決定に関するガイダンスを提供する。これには、連邦政府の機密情報の保護に関する法規制の概要、何を保護する必要がありその情報をどのように保護するのが最善かを判断するためのリスクアセスメントの実施に関するガイダンス、及び関連するセキュリティ関連文書（各種のポリシー文書や実践文書など）についての説明が含まれている。

---

90 当該アルゴリズムや鍵長は、すでに保護されている情報を処理するために使用されることがあるが、そうすることに対してリスクがある場合がある

SP 800-185 Kelsey JM, Chang S-j, Perlner RA (2016) SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-185. https://doi.org/10.6028/NIST.SP.800-185

本推奨では、4 種類の SHA-3 由来の関数（cSHAKE、KMAC、TupleHash、ParallelHash）を規定している。それらはいずれも 128 ビット及び 256 ビットセキュリティ用に定義されている。cSHAKE は、FIPS 202 で定義されている SHAKE 関数のカスタマイズ可能な変形版である。KMAC（KECCAK Message Authentication Code）は、KECCAK をベースにした可変長メッセージ認証コードアルゴリズムである。これは、また擬似乱数関数としても利用可能である。TupleHash は、明らかな衝突なしに複数の入力文字列をハッシュするように設計された可変長ハッシュ関数である。ParallelHash は、非常に長いメッセージを並列にハッシュすることができる可変長ハッシュ関数である。

SP 800-186 Chen L, Moody D, Regenscheid A (2019) Recommendation for Discrete-Logarithm Based Cryptography: Elliptic Curve Domain Parameters. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Special Publication (SP) 800-186. https://doi.org/10.6028/NIST.SP.800-186-draft

本推奨では、以前からの素体及びバイナリ体で定義された推奨 Weierstrass 曲線に加えて、新たに 2 つの具体的なモンゴメリ曲線を含んでいる、これらは、従来の曲線と比較して、性能向上、サイドチャンネル耐性強化、及び実装の簡素化を実現するとされている。また、本推奨では、実装の柔軟性を高めるために、これら新しい曲線の代替表現も規定している。新しい曲線は、Internet Engineering Task Force（IETF）の Crypto Forum Research Group（CFRG）が規定したものと相互接続可能である。

NISTIR 7924 Booth H, Regenscheid A (2014) Reference Certificate Policy. (National Institute of Standards and Technology, Gaithersburg, MD), Second Draft NIST Interagency or Internal Report (IR) 7924. Available at https://csrc.nist.gov/publications/detail/nistir/7924/draft

NISTIR 7924 は、証明書の安全な発行をサポートするための一連のセキュリティコントロール及び実践を特定することを目的としている。これは、証明書ポリシー（CP）の形式で書かれており、認証局（CA）が発行した証明書を信頼する依拠当事者コミュニティの期待及び要件を定義するための標準フォーマットである。

NISTIR 7977 Cryptographic Technology Group (2016) NIST Cryptographic Standards and Guidelines Development Process. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7977. https://doi.org/10.6028/NIST.IR.7977

NISTIR 7977 では、NIST による暗号技術の標準化及びガイドライン開発の取り組みを推進するための原則、プロセス、及び手順を記述している。

NIST 以外の刊行物

IEEE 802.11 Institute of Electrical and Electronics Engineers (2016) *IEEE 802.11-2016 – IEEE Standard for Information technology-Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements - Part 11: Wireless LAN Medium Access*

Control (MAC) and Physical Layer (PHY) Specifications (IEEE, Piscataway, NJ). Available at https://standards.ieee.org/content/ieee-standards/en/standard/802_112016.html

IEEE 1363 — Institute of Electrical and Electronics Engineers (2000) *IEEE 13632000 – IEEE Standard Specifications for Public-Key Cryptography* (IEEE, Piscataway, NJ). Available at https://standards.ieee.org/standard/1363-2000.html

IEEE 1363a — Institute of Electrical and Electronics Engineers (2004) *IEEE 1363a2004 – IEEE Standard Specifications for Public Key Cryptography – Amendment 1: Additional Techniques* (IEEE, Piscataway, NJ). Available at https://standards.ieee.org/standard/1363a-2004.html

IEEE 1363.1 — Institute of Electrical and Electronics Engineers (2008) *IEEE 1363.12008 – IEEE Standard Specification for Public Key Cryptographic Techniques Based on Hard Problems over Lattices* (IEEE, Piscataway, NJ). Available at https://standards.ieee.org/standard/1363_1-2008.html

IEEE 1363.2 — Institute of Electrical and Electronics Engineers (2008) *IEEE 1363.22008 – IEEE Standard Specification for Password-Based Public-Key Cryptography* (IEEE, Piscataway, NJ). Available at https://standards.ieee.org/standard/1363_2-2008.html

IEEE 1619 — Institute of Electrical and Electronics Engineers, *Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices*, IEEE 1619, (multiple parts), 2008 (IEEE, Piscataway, NJ). Available at https://standards.ieee.org/content/ieee-standards/en/standard/16192018.html

ISO/IEC 9594-8 — International Organization for Standardization/International Electrotechnical Commission (2017) *ISO/IEC 9594-8:2017 – Information technology – Open Systems Interconnection – The Directory – Part 8: Public-key and attribute certificate frameworks* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/72557.html

本仕様は、以下でも発行されている。International Telecommunications Union (2019) ITU-T X.509 (10/2019) – Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks (ITU, Geneva, Switzerland). Available at https://www.itu.int/itu-t/recommendations/rec.aspx?rec=X.509

ISO/IEC 9797-1 — International Organization for Standardization/International Electrotechnical Commission (2011) *ISO/IEC 9797-1:2011 – Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/50375.html

本標準には、SP 800-38B で規定されている CMAC が含まれている。

ISO/IEC 9797-2 — International Organization for Standardization/International Electrotechnical Commission (2011) *ISO/IEC 9797-2:2011 – Information*

technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/51618.html

本標準には、FIPS 198 で規定されている HMAC が含まれている。

ISO/IEC 10116 International Organization for Standardization/International Electrotechnical Commission (2017) *ISO/IEC 10116:2017 – Information technology – Security techniques – Modes of operation for an n-bit block cipher* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/64575.html

本標準には、SP 800-38A で規定されている全てのモードが含まれている。

ISO/IEC 10118-3 International Organization for Standardization/International Electrotechnical Commission (2018) *ISO/IEC 10118-3:2018 – Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/67116.html

本標準には、FIPS 180 で規定されている SHA-1 及び SHA-2 ファミリーのハッシュ関数が含まれている。ISO/IEC 10118-3 の改訂版には、FIPS 202 で規定されている SHA-3 関数が含まれる予定である。

ISO/IEC 11770-3 International Organization for Standardization/International Electrotechnical Commission (2015) *ISO/IEC 11770-3:2015 – Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/60237.html

本標準は、鍵確立メカニズムを規定しており、SP 800-56A 及び SP 800-56B で規定されている鍵確立スキームで例示化できる。

ISO/IEC 11770-6 International Organization for Standardization/International Electrotechnical Commission (2016) *ISO/IEC 11770-6:2016 – Information technology – Security techniques – Key management – Part 6: Key derivation* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/65275.html

本標準ドラフトには、SP 800-108 で規定されている全ての鍵導出関数と、SP 800-56C で規定されている 2 段階の鍵導出方法が含まれる。

ISO/IEC 11889 この複数パートの標準には、以下のものが含まれている：

International Organization for Standardization/International Electrotechnical Commission (2015) *ISO/IEC 11889-1:2015 – Information technology – Trusted Platform Module Library – Part 1: Architecture* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/66510.html

International Organization for Standardization/International Electrotechnical Commission (2015) *ISO/IEC 11889-2:2015 – Information technology – Trusted Platform Module Library – Part 2: Structures* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/66511.html

International Organization for Standardization/International Electrotechnical Commission (2015) *ISO/IEC 11889-3:2015 – Information technology – Trusted Platform Module Library – Part 3: Commands* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/66512.html

International Organization for Standardization/International Electrotechnical Commission (2015) *ISO/IEC 11889-4:2015 – Information technology – Trusted Platform Module Library – Part 4: Supporting Routines* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/66513.html

ISO/IEC 14888-2 International Organization for Standardization/International Electrotechnical Commission (2008) *ISO/IEC 14888-2:2008 – Information technology – Security techniques – Digital signatures with appendix – Part 2: Integer factorization-based mechanisms* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/44227.html

本標準には、FIPS 186 で規定されている RSA 署名が含まれている。

ISO/IEC 14888-3 International Organization for Standardization/International Electrotechnical Commission (2018) *ISO/IEC 14888-3:2018 – Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm-based mechanisms* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/76382.html

本標準には、FIPS 186 での有限体及び楕円曲線で規定されている DSA が含まれている。

ISO/IEC 18033-3 International Organization for Standardization/International Electrotechnical Commission (2010) *ISO/IEC 18033-3:2010 – Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/54531.html

本標準には、64 ビットブロック暗号（TDEA など）と 128 ビットブロック暗号（AES など）が含まれている。TDEA は SP 800-67 で規定され、AES は FIPS 197 で規定されていることに注意されたい。

ISO/IEC 19772 International Organization for Standardization/International Electrotechnical Commission (2009) *ISO/IEC 19772:2009 – Information technology – Security techniques – Authenticated encryption* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/46345.html

本標準では、CCM（SP 800-38C で規定）、GCM（SP 800-38D で規定）、及び鍵ラッピング（SP 800-38E で規定）が含まれている。

PKCS 1 Moriarty K (ed.), Kaliski B, Jonsson J, Rusch A (2016) PKCS #1: RSA Cryptography Specifications Version 2.2. (Internet Engineering Task Force (IETF)), IETF Request for Comments (RFC) 8017. https://doi.org/10.17487/RFC8017

PKCS 1 は、RSA アルゴリズムに基づく公開鍵暗号の実装のための推奨事項を提供しており、暗号化プリミティブ、暗号化スキーム、アペンディックス付き署名スキーム、及び鍵の表現とスキームの識別のための ASN.1 構文をカバーしている。

RFC 3526 Kivinen T, Kojo M (2003) More Modular Exponential (MODP) Diffie-Hellman Groups for Internet Key Exchange (IKE). (Internet Engineering Task Force (IETF) Network Working Group), IETF Request for Comments (RFC) 3526. https://doi.org/10.17487/RFC3526

本文書は、インターネット鍵交換（IKE）プロトコルでの新しいモジュラ指数（MODP）グループを定義する。

RFC 5288 Salowey J, Choudhury A, McGrew D (2008) AES Galois Counter Mode (GCM) Cipher Suites for TLS. (Internet Engineering Task Force (IETF) Network Working Group), IETF Request for Comments (RFC) 5288. https://doi.org/10.17487/RFC5288

本 RFC は、Transport Layer Security（TLS）認証暗号の処理として、GCM（Galois/Counter Mode）における Advanced Encryption Standard（AES）の使用について記述している。

RFC 7919 Gillmor D (2016) Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS). (Internet Engineering Task Force (IETF)), IETF Request for Comments (RFC) 7919. https://doi.org/10.17487/RFC7919

本文書は、既知の構造を持つ有限体 DH パラメータを確立する。

RFC 8017 *RSA Cryptography Specifications Version 2.2*, Internet Engineering Task Force, Network Working Group, Informational RFC 8017, The Internet Society; November 2016. https://tools.ietf.org/html/rfc8017

本文書は、RSA アルゴリズムに基づく公開鍵暗号の実装のための推奨事項を提供しており、暗号化プリミティブ、暗号化スキーム、アペンディックス付き署名スキーム、及び鍵の表現とスキームの識別のための ASN.1 構文をカバーしている。

RFC 8032 Josefsson S, Liusvaara I (2017) Edwards Curve Digital Signature Algorithm (EdDSA). (Internet Research Task Force (IRTF)), Request for Comments (RFC) 8032. https://doi.org/10.17487/RFC8032

本ドキュメントでは、Edwards-curve Digital Signature Algorithm（EdDSA）について記述している。

X9.62 Accredited Standards Committee X9 (2005) *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).* (American National Standards Institute), American National Standard for Financial Services (ANS) X9.62-2005. Available at https://webstore.ansi.org/SDO/X9

ANS X9.62 では、楕円曲線デジタル署名アルゴリズム（ECDSA）を使用して、メッセージとデータを保護するためのデジタル署名（署名）の生成と検証の方法を定義している。

付録 A：改訂履歴

2020 年版では、本文書の初版（2015 年版）から以下の変更を行った。

1. 1. 1.1 節：箇条書き 1 に“完全性検証”という代替用語を追加し、“ID 認証”の箇条書きを追加した。
2. 1.5 節 : 以下の用語について変更を行った : 認証、危殆化、機密性、鍵材料、暗号利用モード、平文、秘密鍵、情報源認証、対称鍵、対称鍵（秘密）アルゴリズム。

   以下の用語を追加した : データ完全性認証、ドメインパラメータ、ID 認証、完全性認証、鍵確認、鍵情報、鍵ラッピング、メタデータ、証明書の所有者、鍵又は鍵ペアの所有者、事前共有鍵、プロトコル、スキーム、セキュリティ機能、サーバ。
3. 1.6 節：以下の頭字語を追加した：KMAC、OMB、ROTs、TPM
4. 1.7 節：4 節の概要を変更した。
5. 2.2.3 節：除外規定の禁止についての文章を追加した。
6. 2.3.4 節：ISO 標準一覧の日付を削除した。
7. 3.1 節：SP 800-185 を承認されたハッシュ関数を含む文書のリストに追加した。SHA 関数の命名法及び SP 800-185 の箇条書きを説明するための文章を追加した。
8. 3.2.1.2 節 : 本節は、2-key 及び 3-key TDEA の使用を非推奨や禁止する戦略に合致するように改訂された。
9. 3.2.1.4 節：AES で使われる命名法及びその許容性を説明するための文章を追加した。
10. 3.2.1.5 節：第 1 段落を修正し、暗号利用モードが必要な理由を説明した。
11. 3.2.2 節：SP 800-185 についての段落を追加した。
12. 3.3 節：非対称鍵アルゴリズムの使用についての文章を改訂し、耐量子アルゴリズムと将来的になぜそれが必要なのかについての注釈を追加した。
13. 3.3.1 節：デジタル署名アルゴリズムの一般的な説明を追加した。
14. 3.3.1.1 節：DSA の承認に関して FIPS 186-5 に提案されていることを示す文章を追加した。
15. 3.3.1.2 節：楕円曲線が、FIPS 186 ではなく SP 800-186 で提供されることを示す文章を挿入した。FIPS 186 の改訂内容についての最後の段落を変更した。
16. 3.3.1.3 節：最新の FIPS 186 改訂版で規定されている EdDSA について、新たな節を追加した。
17. 3.3.1.4 節 : 本節は、デジタル署名の RSA について説明し、FIPS 186-5 との整合性を図るために改訂された。
18. 3.3.2 節：鍵確立スキームに関する入門的な資料を追加した。
19. 3.3.2.1 節 : 本節は、ドメインパラメータの使用に関する追加ガイダンスを含むように改訂された。
20. 3.3.2.2 節：前バージョンの 3.3.3 節の資料を追加し、鍵確立に RSA を使用することの具体的な説明を追加した。
21. 3.4 節 : 第 3 段落の最後に、80 ビットのセキュリティしか提供しない鍵を使用することのリスクを受け入れることについての文章を追加した。

22. 4.1 節：第 1 段落の最後に、3-key TDEA が非推奨となることを警告する文章を追加した。
23. 4.2 節 : 第 1 段落の最後に完全性コードの使用に関する文章を追加した。ID 認証に関する段落を挿入し、情報源認証に関する段落を修正した。
24. 4.2.2 節：MAC アルゴリズムに関する本節を修正し、再構成した。
25. 4.2.2.2 節：SP 800-185 についての段落を追加した。
26. 4.2.3 節 : デジタル署名の生成と検証を記述するステップを修正した（理解しやすくするため）。FIPS 186-5 で提供されるアルゴリズムのリストに EdDSA を追加した。
27. 4.3.2 節の第 2 段落を改訂し、十分に検証されたプロトコル及び構造を使用することを推奨した。
28. 4.4 節：SP 800-90B の記述を修正した。
29. 4.5 節：第 3 段落を改訂し、鍵配付について説明した。最後の段落の最後に、量子コンピューティングの出現についての警告文を追加した。
30. 5.0 節：本文書で使用されている“鍵情報”という用語の説明を追加した。
31. 5.1.1 節：SP 800-57 part 2 の内容の説明を修正した。TLS が SP 800-52 で説明されるようになったことの注釈を追記した。
32. 5.1.2 節：CMVP への新しいリンクを追加した。
33. 5.2.3 節 : EdDSA が承認されたデジタル署名アルゴリズムのリストに追加された。公開鍵の使用、依拠当事者など（上述される箇条書きの項目）についての説明を修正した。
34. 5.2.3.1 節項目 4 : 全ての証明書の棚卸リストに対する推奨を追加した。証明書の有効期限の説明を拡張した。
35. 5.3.2 節：最終段落を修正し、以前は SP 800-56A 及び SP 800-56B にあった KDF について、今は全て SP 800-56C に記載されていることを示した。
36. 5.3.2.2 節：SP 800-175B 初版の 6.5 節での内容は、本節に挿入された。
37. 5.3.3 節第 2 段落 : 以前は SP 800-56A 及び SP 800-56B にあった全ての鍵導出手法について、今は SP 800-56C に記載されていることを示す文章を追加した。
38. 5.3.4 節：SP 800-56B の記述を変更し、SP 800-71 への参照を追加した。
39. 5.3.4.1 節：第 1 段落を短縮した。
40. 5.3.4.2 節：SP 800-71 についての新しい節である。
41. 5.4.1 節：SP 800-71 への参照が追加された。
42. 5.4.5 節：CAVP 及び CMVP へのリンクを更新した。
43. 5.4.8 節 : 本節は、説明責任と鍵及び証明書の棚卸リスト管理の両方を含むように改訂された。
44. 5.4.9 節：異なる種類の監査に関する新しい節である。
45. 6.4 節及び 6.5 節は削除された。
46. 参照文献は更新された。