SSL/TLS 暗号設定ガイドライン改訂及び
鍵管理ガイドライン作成のための調査・検討
― 調査報告書 別紙 3 ―
鍵管理 文献のトピック一覧

2018 年 6 月

IPA 独立行政法人 情報処理推進機構
技術本部 セキュリティセンター

鍵管理　文献のトピック一覧

SP800130とほぼ同じなので
マッピングは省略

No	1	1	2	3	7	8	9	13
文献	SP 800-57 Part1	SP 800-57 Part1	SP 800-57 Part2	SP 800-57 Part3	SP 800-130	SP 800-152	SP 800-175B	ENISA
文献名		Recommendation for Key Management, Part 1: General Revision 4	Recommendation for Key Management – Part 2: Best Practices for Key Management Organization	Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance	A Framework for Designing Cryptographic Key Management Systems	A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS)	Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms	Algorithms, key size and parameters Report.2014
略称	Part 1 (General)	Part 1 (General)	Part 2 (Best Practices)	Part 3 (Application)	Framework	Federal	Guideline	[ENISA]Algorithms
概要	[読者] ・開発者、システム管理者→"ベストプラクティス"について助言 ・暗号モジュール開発者→具体的なアプリの支援に必要となる鍵管理の理解 ・プロトコル開発者→アルゴリズムの具体的なスイートの特徴を識別 ・システム管理者→構成設定の最適な決定		[読者] システム所有者と管理者 [目的] ・連邦政府のための**ポリシーと安全性計画**のガイド。 ・組織の鍵管理の確立を支援するためのフレームワークと一般的なガイダンス。 ・連邦政府組織の法的および方針としてのセキュリティ計画の鍵管理の要求事項を満たすための基礎を提供	[目的] ・セキュリティガイダンスの背景を提供することを意図した検討中のシステムの簡潔な説明 ・推奨アルゴリズムスイートと鍵サイズおよび関連するセキュリティおよび適合性の問題 ・連邦政府情報の保護のための現在の形のメカニズムの使用に関する推奨事項 ・鍵管理処理のセキュリティの有効性に影響する可能性のあるセキュリティ上の考慮事項 ・調達決定者、システムインストーラ、システム管理者およびエンドユーザへの一般推奨事項 [トピック] PKI、IPsec、TLS、S/MIME、ケルベロス ・無線の鍵更新（OTAR）鍵管理message（KMM）、DNSSEC、EFS、SSH	[読者]CKMS設計書の作成者 [概要] 各節で、FR:The CKMS design shall specify～が定義されていて、CKMS設計書者が各項目で何を指定すべきかの要件が書かれている。	・US連邦組織で使われるための設計、実装、調達、導入、設定、管理、操作の要件 [読者] CKMSの設計者、実装者：機能を選択するアシスト 連邦組織の人：調達、導入、設定、管理、操作	[目的] ・連邦政府の機密情報を保護する方法の議論と、NISTの暗号標準の概要を提供。 [読者] ・システムに暗号システムを構築する時に選択するプログラムマネージャー ・要件に合う暗号方式を選択する技術者 ・暗号サービスの利用者	[対象トピック]暗号アルゴリズムと鍵サイズ [目的] ①レガシーシステム：ふさわしくない場合、置換するためのアドバイス ②将来のシステム [概要] ・暗号プリミティブ内の各方式をFutureとRegacyに分けて説明。 [読者]暗号ソリューションの設計と実装の決定者と専門家。 [鍵管理の部分] KeyDerivationFunctions 6.3 Key Life Cycle Management
他文献との関連			・ポリシーの詳細はPart1を参照している			・ベースの文書：SP800-130(A Framework～) ・扱っているトピックは、800-130とほぼ同じ。	SP800-57 Part1,2,3、 SP800-130、SP800-152 など、多数の文献を参照している	・2013版のアップデート ①SP800-57を参照 ②SP800-130(Framework)を参照
年月	2016/1/28		2005/8/25 (12年も前)	2015/1/22	2013/8/15	2015/10/28	2016/8/22	2014/11
1	**3 セキュリティサービス** 3.1 機密性 3.2 データ完全性 3.3 認証 3.4 権限付与 3.5 否認防止 3.6 支援サービス 3.7 結合サービス	**3 Security Services** 3.1 Confidentiality 3.2 Data Integrity 3.3 Authentication 3.4 Authorization 3.5 Non-repudiation 3.6 Support Services 3.7 Combining Services						
1	**4 暗号アルゴリズム** 4.1 暗号アルゴリズムのクラス 4.2 暗号アルゴリズムの機能 4.2.1 ハッシュ関数 4.2.2 暗号化および復号で使用される対称鍵アルゴリズム 4.2.3 メッセージ認証コード（MAC） 4.2.4 ディジタル署名アルゴリズム 4.2.5 鍵確立スキーム 4.2.6 鍵確立プロトコル 4.2.7 乱数ビット生成	**4 Cryptographic Algorithms** 4.1 Classes of Cryptographic Algorithms 4.2 Cryptographic Algorithm Functionality 4.2.1 Hash Functions 4.2.2 Symmetric-Key Algorithms used for Encryption and Decryption 4.2.3 Message Authentication Codes (MACs) 4.2.4 Digital Signature Algorithms 4.2.5 Key Establishment Schemes 4.2.6 Key Establishment Protocols 4.2.7 Random Bit Generation					**SECTION 3: CRYPTOGRAPHIC ALGORITHMS** 3.1 Cryptographic Hash Functions 3.2 Symmetric-Key Algorithms 3.3 Asymmetric-Key Algorithms 3.4 Algorithm Security Strength 3.5 Algorithm Lifetime **SECTION 4: CRYPTOGRAPHIC SERVICES** 4.1 Data Confidentiality 4.2 Data Integrity and Source Authentication 4.2.1 Hash Functions 4.2.2 Message Authentication Code Algorithms 4.2.3 Digital Signature Algorithms 4.3 Combining Confidentiality and Authentication in a Block-Cipher Mode of Operation 4.4 Random Bit Generation 4.5 Symmetric vs. Asymmetric Cryptography	**3 Primitives** 3.1 Comparison 3.2 Block Ciphers 3.3 Hash Functions 3.4 Stream Ciphers 3.5 Public Key Primitives 3.6 Key Size Analysis **4 Basic Cryptographic Schemes** 4.1 Block Cipher Basic Modes of Operation 4.2 Message Authentication Codes 4.3 Authenticated Encryption (with Associated Data) 4.4 Key Derivation Functions 4.5 Generalities on Public Key Schemes 4.6 Public Key Encryption 4.7 Hybrid Encryption 4.8 Public Key Signatures **5 Advanced Cryptographic Schemes** 5.1 Password-Based Key Derivation 5.2 Key Wrap Algorithms 5.3 Encrypted Storage 5.4 Identity Based Encryption/KEMs
1	**5 一般的な鍵管理ガイダンス**	**5 General Key Management Guidance**						
1	**5. 1 鍵種別とその他の情報** 5.1.1 暗号鍵 5.1.2 その他の暗号学的または関連する情報	**5.1 Key Types and Other Information** 5.1.1 Cryptographic Keys 5.1.2 Other Cryptographic or Related Information			6.1 Key Types　鍵の種類（共通鍵、公開鍵、署名鍵など）			
1	5.2 鍵使用法	5.2 Key Usage						
1	**5.3 暗号期間** 5.3.1 暗号期間に影響するリスク要因 5.3.2 暗号期間に影響する帰結要因 5.3.3 暗号期間に影響するその他の要因 5.3.4 非対称鍵の使用期間と暗号期間 5.3.5 対称鍵の使用期間と暗号期間 5.3.6 鍵種別に固有の暗号期間に関する推奨事項 5.3.7 その他の暗号学的または関連する情報についての推奨事項	**5.3 Cryptoperiods** 5.3.1 Risk Factors Affecting Cryptoperiods 5.3.2 Consequence Factors Affecting Cryptoperiods 5.3.3 Other Factors Affecting Cryptoperiods 5.3.4 Asymmetric Key Usage Periods and Cryptoperiods 5.3.5 Symmetric Key Usage Periods and Cryptoperiods 5.3.6 Cryptoperiod Recommendations for Specific Key Types 5.3.7 Recommendations for Other Cryptographic or Related Information	3.2.2.7 Establishment of Cryptoperiods　鍵の期間の設定				5.4.4 Cryptoperiods　暗号の期間	

No	1	1	2	3	7	8	9	13
文献	SP 800-57 Part1	SP 800-57 Part1	SP 800-57 Part2	SP 800-57 Part3	SP 800-130	SP 800-152	SP 800-175B	ENISA
文献名		Recommendation for Key Management, Part 1: General Revision 4	Recommendation for Key Management – Part 2: Best Practices for Key Management Organization	Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance	A Framework for Designing Cryptographic Key Management Systems	A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS)	Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms	Algorithms, key size and parameters Report,2014
略称	Part 1 (General)	Part 1 (General)	Part 2 (Best Practices)	Part 3 (Application)	Framework	Federal	Guideline	[ENISA]Algorithms
1	5.4 保証 5.4.1 完全性の保証(完全性の保護) 5.4.2 ドメインパラメータ有効性の保証 5.4.3 公開鍵有効性の保証 5.4.4 プライベート鍵所持の保証 5.5 鍵およびその他の鍵材料の危殆化	5.4 Assurances 5.4.1 Assurance of Integrity (Integrity Protection) 5.4.2 Assurance of Domain Parameter Validity 5.4.3 Assurance of Public-Key Validity 5.4.4 Assurance of Private-Key Possession 5.5 Compromise of Keys and other Keying Material						
1	**5.6 暗号アルゴリズムと鍵サイズの選択についてのガイダンス** 5.6.1 アルゴリズムの同等強度 5.6.2 適切なアルゴリズムスイートの定義 5.6.3 アルゴリズムスイートの利用 5.6.4 新しいアルゴリズムおよび鍵サイズへの移行 5.6.5 セキュリティ強度の減少	**5.6 Guidance for Cryptographic Algorithm and Key-Size Selection** 5.6.1 Comparable Algorithm Strengths 5.6.2 Defining Appropriate Algorithm Suites 5.6.3 Using Algorithm Suites 5.6.4 Transitioning to New Algorithms and Key Sizes 5.6.5 Security Strength Reduction					6.1 Required Security Strength　セキュリティ長の要件	
1	**6 暗号学的情報の保護要件**	**6 Protection Requirements for Cryptographic Information**						
1	6.1 保護および保証要件	6.1 Protection and Assurance Requirements						
1	6.1.1 暗号鍵の保護および保証要件の要約	6.1.1 Summary of Protection and Assurance Requirements for Cryptographic Keys						
1	6.1.2 その他の暗号学的情報や関連情報に対する保護要件の要約	6.1.2 Summary of Protection Requirements for Other Cryptographic or Related Information						
1	6.2 保護メカニズム	6.2 Protection Mechanisms						
1	6.2.1 送信中の暗号学的情報の保護メカニズム 6.2.1.1 可用性 6.2.1.2 完全性 6.2.1.3 機密性 6.2.1.4 用途やアプリケーションとの関連付け 6.2.1.5 その他のエンティティとの関連付け 6.2.1.6 その他の関連情報との関連付け	6.2.1 Protection Mechanisms for Cryptographic Information in Transit						
1	6.2.2 保管情報の保護メカニズム 6.2.2.1 可用性 6.2.2.2 完全性 6.2.2.3 機密性 6.2.2.4 用途やアプリケーションとの関連付け 6.2.2.5 その他のエンティティとの関連付け 6.2.2.6 その他の関連情報との関連付け	6.2.2 Protection Mechanisms for Information in Storage						
1	6.2.3 暗号学的情報に関連付けされるメタデータ 識別子、期間、種別、状態　など [SP800-152]はメタデータの使用についての追加の情報を提供する。	6.2.3 Metadata Associated with Cryptographic Information			6.2 Key Metadata メタデータ （鍵レベル、鍵識別、所有者識別、ライフサイクル、鍵フォーマット、暗号アルゴリズム、操作モード、パラメタ、鍵長、ACL、無効など）			
1	**7 鍵の状態と遷移** 7.1 活性化前状態 7.2 活性化状態 7.3 一時停止状態 7.4 不活性化状態 7.5 危殆化状態 7.6 破棄状態	**7 Key States and Transitions** 7.1 Pre-activation State 7.2 Active State 7.3 Suspended State 7.4 Deactivated State 7.5 Compromised State 7.6 Destroyed State			6.4.1 Generate Key　鍵生成 6.4.3 Activate Key　有効化 6.4.4 Deactivate Key　無効化			

No	1	1	2	3	7	8	9	13
文献	SP 800-57 Part1	SP 800-57 Part1	SP 800-57 Part2	SP 800-57 Part3	SP 800-130	SP 800-152	SP 800-175B	ENISA
文献名		Recommendation for Key Management, Part 1: General Revision 4	Recommendation for Key Management – Part 2: Best Practices for Key Management Organization	Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance	A Framework for Designing Cryptographic Key Management Systems	A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS)	Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms	Algorithms, key size and parameters Report,2014
略称	Part 1 (General)	Part 1 (General)	Part 2 (Best Practices)	Part 3 (Application)	Framework	Federal	Guideline	[ENISA]Algorithms
1	**8 鍵管理のフェーズと機能** **8.1 運用前フェーズ** 8.1.1 利用者登録機能 8.1.2 システム初期化機能 8.1.3 利用者初期化機能 8.1.4 鍵材料インストール機能 8.1.5 鍵確立機能 8.1.6 鍵登録機能 **8.2 運用フェーズ** 8.2.1 正常な運用中のストレージ機能 8.2.2 運用機能の継続 8.2.3 鍵の変更機能 8.2.4 鍵導出方法 **8.3 運用後フェーズ** 8.3.1 アーカイブストレージと鍵回復の機能 8.3.2 エンティティ登録抹消機能 8.3.3 鍵登録抹消機能 8.3.4 鍵破棄機能 8.3.5 鍵失効機能 8.4 破棄フェーズ	**8 Key-Management Phases and Functions** **8.1 Pre-operational Phase** 8.1.1 User Registration Function 8.1.2 System Initialization Function 8.1.3 User Initialization Function 8.1.4 Keying-Material Installation Function 8.1.5 Key Establishment Function 8.1.6 Key Registration Function **8.2 Operational Phase** 8.2.1 Normal Operational Storage Function 8.2.2 Continuity of Operations Function 8.2.3 Key Change Function 8.2.4 Key Derivation Methods **8.3 Post-Operational Phase** 8.3.1 Archive Storage and Key Recovery Functions 8.3.2 Entity De-registration Function 8.3.3 Key De-registration Function 8.3.4 Key Destruction Function 8.3.5 Key Revocation Function 8.4 Destroyed Phase	**3. 2 Key Management Practices Statement (KMPS)** 鍵管理実施ステートメント 3.2.1 Alternative KMPS Formats フォーマットの変更 3.2.2 Common KMPS Content 共通 ※詳細はPart1を参照している 3.2.2.1 Association of KMPS with the KMP 3.2.2.2 Identification of Responsible Entities and Contact Information 3.2.2.3 Key Generation or Acquisition 鍵生成、獲得 3.2.2.4 Key Agreement 鍵共有 3.2.2.5 Cross Certification Agreements クロス証明 PKI公開鍵証明書の階層について 3.2.2.6 Key Distribution and Revocation Structures 鍵配布と失効 3.2.2.7 Establishment of Cryptoperiods 鍵の期間の設定 3.2.2.8 Tracking of and Accounting for Keying Material 鍵素材の追跡 3.2.2.9 Protection of Keying Material 鍵素材の保護 3.2.2.10 Emergency and Routine Revocation of Keying Material 鍵素材の失効 3.2.2.11 Auditing 監査 3.2.2.12 Keying Material Destruction 鍵素材の破棄 3.2.2.13 Key Backup and Recovery 鍵のバックアップと回復 3.2.2.14 Compromise Recovery 漏洩の回復 3.2.2.15 Policy Violation Consequences ポリシー違反 3.2.2.16 Documentation 文書		6.4.2 Register Owner 所有者登録 6.6 Cryptographic Key and Metadata Security: During Key Establishment --- 6.4.6 Suspend and Re-Activate a Key 停止/再有効化 6.4.7 Renew a Public Key 公開鍵の更新 6.4.8 Key Derivation or Key Update 更新 --- 6.5 Cryptographic Key and/or Metadata Security: In Storage 保管されている鍵の保護(アクセスコントロールなど) 6.4.5 Revoke Key 失効		5.3 Key Establishment 鍵構築 5.3.1 Key Generation 生成 5.3.2 Key Derivation 抽出 5.3.3 Key Agreement 共有 5.3.4 Key Transport 転送 5.3.5 Key Wrapping 鍵ラッピング 5.3.6 Derivation of a Key from a Password パスワードからの鍵の生成	**6.3 Key Life Cycle Management** Key Generation Key Registration/Certi cation Key Distribution and Installation Key Use Key Storage Revocation/Validation Key Archive/Destruction
1	**9 責任追跡性、監査、および抗たん性**	**9 Accountability, Audit, and Survivability**						
1	9.1 責任追跡性	9.1 Accountability						
1	9.2 監査	9.2 Audit					5.4.8 Accountability and Auditing 監査	
1	9.3 鍵管理システムの抗たん性	9.3 Key Management System Survivability						
1	9.3.1 バックアップ鍵	9.3.1 Backup Keys						
1	9.3.2 鍵回復	9.3.2 Key Recovery						
1	9.3.3 システムの冗長性／緊急時対応計画の立案	9.3.3 System Redundancy/Contingency	**5.3 Key Management Planning Information Requirements 鍵管理計画の要件** 5.3.5 Access Control アクセス制御 5.3.6 Accounting 製品等のログやアクセス制御を使う 5.3.7 Compromise Management and Recovery 漏洩管理と回復 5.3.8 Key Recovery 鍵回復					
1	9.3.4 危殆化からの回復	9.3.4 Compromise Recovery			**6.8 Compromise Recovery 危殆化回復** 6.8.1 Key Compromise 鍵危殆化 6.8.2 Metadata Compromise 6.8.3 Key and Metadata Revocation 6.8.4 Cryptographic Module Compromise 6.8.5 Computer System Compromise Recovery 6.8.6 Network Security Controls and Compromise Recovery 6.8.7 Personnel Security Compromise Recovery 6.8.8 Physical Security Compromise Recovery		5.4.7 Compromises 危殆化	
1	**10 暗号デバイスやアプリケーションの鍵管理仕様**	**10 Key Management Specifications for Cryptographic Devices or Applications**						
1	10.1 鍵管理仕様説明／目的	10.1 Key Management Specification Description/Purpose					**5.4 Key Management Issues 鍵管理の問題** 5.4.1 Manual vs. Automated Key Establishment マニュアルか自動か 5.4.2 Selecting and Operating a CKMS 選択と操作 5.4.3 Storing and Protecting Keys 鍵の保管と保護 5.4.5 Use Validated Algorithms and Cryptographic Modules 有効なアルゴリズムとモジュールの使用 5.4.6 Control of Keying Material 鍵素材の管理 **SECTION 6: OTHER ISSUES** 6.3 When Algorithms are No Longer Approved アルゴリズムが承認されなくなったら 6.4 Registration Authorities (RAs) 6.5 Cross Certification クロス証明	
1	10.2 鍵管理仕様の内容	10.2 Content of the Key Management Specification						
1	10.2.1 暗号アプリケーション	10.2.1 Cryptographic Application						
1	10.2.2 通信環境	10.2.2 Communications						
1	10.2.3 鍵管理構成要素の要求事項	10.2.3 Key Management Component Requirements						
1	10.2.4 鍵管理構成要素の生成	10.2.4 Key Management Component Generation						
1	10.2.5 鍵管理構成要素の配付	10.2.5 Key Management Component Distribution						
1	10.2.6 鍵材料保管	10.2.6 Keying Material Storage						
1	10.2.7 アクセス制御	10.2.7 Access Control						
1	10.2.8 責任追跡性	10.2.8 Accounting						
1	10.2.9 危殆化の管理と回復	10.2.9 Compromise Management and Recovery						
1	10.2.10 鍵回復	10.2.10 Key Recovery						
1								
1	**附属書A:暗号学的および非暗号学的な完全性と情報源認証メカニズム**	**APPENDIX A**: Cryptographic and Non-cryptographic Integrity and Source Authentication Mechanisms						

No	1	1	2	3	7	8	9	13
文献	SP 800-57 Part1	SP 800-57 Part1	SP 800-57 Part2	SP 800-57 Part3	SP 800-130	SP 800-152	SP 800-175B	ENISA
文献名		Recommendation for Key Management, Part 1: General Revision 4	Recommendation for Key Management – Part 2: Best Practices for Key Management Organization	Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance	A Framework for Designing Cryptographic Key Management Systems	A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS)	Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms	Algorithms, key size and parameters Report,2014
略称	Part 1 (General)	Part 1 (General)	Part 2 (Best Practices)	Part 3 (Application)	Framework	Federal	Guideline	[ENISA]Algorithms
1	**附属書B: 鍵回復** B.1 保管された鍵材料からの回復 B.2 鍵材料の復元による回復 B.3 鍵材料が回復可能である必要があるような条件 B.4 鍵回復システム B.5 鍵回復方針	**APPENDIX B: Key Recovery** B.1 Recovery from Stored Keying Material B.2 Recovery by Reconstruction of Keying Material B.3 Conditions Under Which Keying Material Needs to be Recoverable B.4 Key Recovery Systems B.5 Key Recovery Policy						
7					**2. Framework Basics** 2.1 Rationale for Cryptographic Key Management 2.2 Keys, Metadata, Trusted Associations, and Bindings 2.3 CKMS Applications 2.4 Framework Topics and Requirements 2.5 CKMS Design 2.6 CKMS Profiles 2.7 CKMS Framework and Derived Profile 2.8 Differences between a Framework and a Profile 2.9 Example of a Distributed CKMS Supporting a Secure E-Mail Application 2.10 CKMS Framework Components and Devices **3. Goals** 3.1 Providing Key Management to Networks, Applications, and Users 3.2 Maximize the Use of COTS in a CKMS 3.3 Conformance to Standards 3.4 Ease-of-use 3.4.1 Accommodate User Ability and Preferences 3.4.2 Design Principles of the User Interface 3.5 Performance and Scalability		5.2.1 Key Management Framework フレームワーク 5.2.2 Key Management System Profile プロファイル	
7,2			**3 Key Management Policy and Practices 鍵管理ポリシーと実施** 3.1 Key Management Policy (KMP) 鍵管理ポリシー 3.1.2 Policy Content 3.1.2.1 General Policy Content Requirements 一般的な要件 3.1.2.1.1 Security Objectives 保護する対象 3.1.2.1.2 Organizational Responsibilities 組織の責任 組織、役割の説明 3.1.2.1.3 Sample KMP Format 鍵管理ポリシーのサンプルフォーマット 3.1.3 Policy Enforcement ポリシーの施行		**4. Security Policies セキュリティ ポリシー(方針)** 4.1 Information Management Policy 情報管理ポリシー 4.2 Information Security Policy 情報安全性ポリシー 4.3 CKMS Security Policy CKMSのポリシー 4.4 Other Related Security Policies 4.5 Interrelationships among Policies ポリシー間の相互関係 4.6 Personal Accountability 個人説明責任 4.7 Anonymity, Unlinkability, and Unobservability 匿名性、アンリンカビリティ、観測不可能性 4.8 Laws, Rules, and Regulations 法律、規則、規制 4.9 Security Domains セキュリティドメイン 4.9.1 Conditions for Data Exchange データ交換条件 4.9.2 Assurance of Protection 保護の保証 4.9.3 Equivalence of Domain Security Policies 4.9.4 Third-Party Sharing 共有 4.9.5 Multi-level Security Domains 複数レベル 4.9.6 Upgrading and Downgrading 4.9.7 Changing Domain Security Policies 変更			
7			**2 Key Management Infrastructure 鍵管理の基盤** 2.1 Central Oversight Author 中央監視権限 2.2 Key Processing Facility(ies) 鍵保有機関 2.3 Service Agents サービス提供者 2.4 Client Nodes クライアントノード 3.1.2.1.2 Organizational Responsibilities 組織の責任 組織、役割の説明		**5. Roles and Responsibilities 役割と責任** 管理者、鍵保有者、CKMS使用者など			
7					**6. Cryptographic Keys and Metadata** **メタデータの管理** 6.4.9 Destroy Key and Metadata 6.4.10 Associate a Key with its Metadata 6.4.11 Modify Metadata 6.4.12 Delete Metadata 6.4.13 List Key Metadata 6.4.14 Store Operational Key and Metadata 6.4.15 Backup of a Key and its Metadata 6.4.16 Archive Key and/or Metadata 6.4.17 Recover Key and/or Metadata 6.4.18 Establish Key 6.4.19 Enter a Key and Associated Metadata into a Cryptographic Module 6.4.20 Output a Key and Associated Metadata from a Cryptographic Module			
7					**鍵の検証** 6.4.21 Validate Public Key Domain Parameters 公開鍵のパラメタ 6.4.22 Validate Public Key 公開鍵の検証 6.4.23 Validate Public Key Certification Path PK証明書検証パス 6.4.24 Validate Symmetric Key 共通鍵の検証 6.4.25 Validate Private Key (or Key Pair) 6.4.26 Validate the Possession of a Private Key 共通鍵の所有の検証			

No	1	1	2	3	7	8	9	13
文献	SP 800-57 Part1	SP 800-57 Part1	SP 800-57 Part2	SP 800-57 Part3	SP 800-130	SP 800-152	SP 800-175B	ENISA
文献名		Recommendation for Key Management, Part 1: General Revision 4	Recommendation for Key Management – Part 2: Best Practices for Key Management Organization	Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance	A Framework for Designing Cryptographic Key Management Systems	A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS)	Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms	Algorithms, key size and parameters Report,2014
略称	Part 1 (General)	Part 1 (General)	Part 2 (Best Practices)	Part 3 (Application)	Framework	Federal	Guideline	[ENISA]Algorithms
7					**ACS** 6.7 Restricting Access to Key and Metadata Management Functions 鍵へのアクセス制限 6.7.1 The Access Control System (ACS) 6.7.2 Restricting Cryptographic-Module Entry and Output of Plaintext Keys 6.7.3 Controlling Human Input 6.7.4 Multiparty Control 6.7.5 Key Splitting			
7					**7. Interoperability and Transitioning CKMSの相互運用と移行**		6.2 Interoperability 相互運用	
7					**8. Security Controls 安全性の管理** 8.1 Physical Security Controls 物理安全性 8.2 Operating System and Device Security Controls 操作とデバイス 8.2.1 Operating System Security OS 8.2.2 Individual CKMS Device Security デバイス 8.2.3 Malware Protection マルウェア保護 8.2.4 Auditing and Remote Monitoring 監査/モニタリング 8.3 Network Security Control Mechanisms ネットワーク 8.4 Cryptographic Module Controls 暗号モジュール			
7					**9. Testing and System Assurances テストと保証**			
7					**10. Disaster Recovery 災害時の回復** 10.1 Facility Damage 10.2 Utility Service Outage 10.3 Communication and Computation Outage 10.4 System Hardware Failure 10.5 System Software Failure 10.6 Cryptographic Module Failure 10.7 Corruption of Keys and Metadata			
7					**11. Security Assessment 安全性の評価** 11.1 Full Security Assessment 11.2 Periodic Security Review 11.3 Incremental Security Assessment 11.4 Security Maintenance			
12								
12,13								**6 General Comments** 6.1 Side-channels 6.2 Random Number Generation **6.3 Key Life Cycle Management** **6.3.1 Key Management Systems** **800-130(Framework)を参照しているだけ。**
2			**4 Information Technology Systems Security Plans 情報技術システム安全性計画** 4.1 General Support System 一般的なシステム 4.2 Major Application Security Plans 主要なアプリケーションの安全性の計画 4.3 Key Management Additions to System Security Plans 安全性計画への鍵管理の追加 4.4 Documentation Required for Security Evaluation 安全性評価のための文書要件					

No	1	1	2	3	7	8	9	13
文献	SP 800-57 Part1	SP 800-57 Part1	SP 800-57 Part2	SP 800-57 Part3	SP 800-130	SP 800-152	SP 800-175B	ENISA
文献名		Recommendation for Key Management, Part 1: General Revision 4	Recommendation for Key Management – Part 2: Best Practices for Key Management Organization	Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance	A Framework for Designing Cryptographic Key Management Systems	A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS)	Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms	Algorithms, key size and parameters Report,2014
略称	Part 1 (General)	Part 1 (General)	Part 2 (Best Practices)	Part 3 (Application)	Framework	Federal	Guideline	[ENISA]Algorithms
2			**5 Key Management Planning for Cryptographic Components 暗号部品への鍵管理計画** 5.1 Key Management Planning Documents 鍵管理計画の文書 5.2 Key Management Planning Process 鍵管理計画のプロセス 5.3 Key Management Planning Information Requirements 鍵管理計画の要件 5.3.1 Key Management Products and Services Requirements 製品とサービスの要件 5.3.2 Key Management Products and Services Ordering 製品とサービスのオーダー 5.3.3 Keying Material Distribution 鍵素材の分配 5.3.4 Keying Material Storage 鍵素材の保管 5.3.5 Access Control アクセス制御 5.3.6 Accounting 製品等のログやアクセス制御を使う 5.3.7 Compromise Management and Recovery 漏洩管理と回復 5.3.8 Key Recovery 鍵回復 5.3.9 KMI Enhancements Requirements (optional) 強化要件					
2			**A.2 Representative Encryption Key Lifecy 鍵のライフサイクル** A.2.1 Example of Distribution of Symmetric Keys 共通鍵の配布の例 A.2.2 Example of Distribution of Asymmetric Keys 公開鍵の配布の例					
2			**APPENDIX B: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework** **公開鍵基盤**					
3,16,19				2 公開鍵基盤(PKI)			**5.2.3 Public Key Infrastructure PKI基盤** 5.2.3.1 PKI Components, Relying Parties and Their Responsibilities パーティと信頼性 5.2.3.2 Basic Certificate Verification Process 検証プロセス 5.2.3.3 CA Certificate Policies and Certificate Practice Statements 認証局ポリシー 5.2.3.4 Federal Public Key Infrastructure 連邦政府PKI	
3				3 インターネットプロトコルセキュリティ(IPsec)				
3				4 トランスポート層セキュリティ(TLS)				
3				5 セキュア／多目的インターネットメール拡張(S/MIME)				
3				6 ケルベロス(Kerberos)				
3				7 無線回線経由の鍵更新(OTAR)鍵管理メッセージ(KMM)				
3				8ドメインネームシステム セキュリティ拡張(DNSSEC)				
3				9 暗号化ファイルシステム(EFS)				
3				10 セキュアシェル(SSH)				
3								
14								

No	1	1	2	3	7	8	9	13
文献	SP 800-57 Part1	SP 800-57 Part1	SP 800-57 Part2	SP 800-57 Part3	SP 800-130	SP 800-152	SP 800-175B	ENISA
文献名		Recommendation for Key Management, Part 1: General Revision 4	Recommendation for Key Management – Part 2: Best Practices for Key Management Organization	Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance	A Framework for Designing Cryptographic Key Management Systems	A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS)	Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms	Algorithms, key size and parameters Report,2014
略称	Part 1 (General)	Part 1 (General)	Part 2 (Best Practices)	Part 3 (Application)	Framework	Federal	Guideline	[ENISA]Algorithms
調査14,18,21								
9							**SECTION 2: STANDARDS AND GUIDELINES** 2.1 Benefits of Standards 2.2 Federal Information Processing Standards and Special Publications 2.2.1 The Use of FIPS and SPs 2.2.2 FIPS Waivers 2.3 Other Standards Organizations 2.3.1 American National Standards Institute (ANSI) 2.3.2 Institute of Electrical and Electronics Engineers (IEEE) Standards Association 2.3.3 Internet Engineering Task Force (IETF) 2.3.4 International Organization for Standardization (ISO) 2.3.5 Trusted Computing Group (TCG)	

鍵管理　文献のトピック一覧

No	1	12	14	15	16	17	18	19	21
文献	SP 800-57 Part1	ENISA	ENISA	OASIS	RFC3647	CR2010GK	IPA2008R	IPA2008G	IPA2013
文献名		Recommended cryptographic measures	Study on the use of cryptographic techniques in Europe	KMIP Specification V1.3 (OASIS Standard) Key Management Interoperability Protocol Specification Version 1.3 OASIS Standard	インターネット X.509 PKI：証明書ポリシーと認証実施フレームワーク	2010年度版　リストガイド（鍵管理） CRYPTREC	安全な暗号鍵のライフサイクルマネージメントに関する調査　調査報告書	安全な暗号鍵のライフサイクルマネージメントに関する調査　鍵管理ガイドライン（案）	暗号鍵の適切な運用・管理に係る課題調査 調査報告書
略称	Part 1 (General)	[ENISA]Recommended	[ENISA]Use	KMIP	X.509	[CR]リストガイド	[IPA]調査報告書	[IPA]鍵管理ガイドライン（案）	[IPA]鍵寄託(Escrow)
概要	[読者] ・開発者、システム管理者→"ベストプラクティス"について助言 ・暗号モジュール開発者→具体的なアプリの支援に必要となる鍵管理の理解 ・プロトコル開発者→アルゴリズムの具体的なスイートの特徴を識別 ・システム管理者→構成設定の最適な決定		[概要] ・EU Member States(MS)において、各暗号方式が使用されている割合がグラフで示されている。 ・電子政府が保存/通信する未分類情報に関してEU MSが定義した暗号仕様を検査した研究。 ・電子政府のための仕様と推奨を示す。 [読者]国家や部門の暗号文書を定義するポリシー策定者、電子政府部門担当者。	[概要] 相互運用のプロトコルの詳細 [目次] 2 Objects 3 Attributes 4 Client-to-Server Operations 5 Server-to-Client Operations 6 Message Contents 7 Message Format 8 Authentication 9 Message Encoding 10 Transport 11 Error Handling 12 KMIP Server and Client Implementation Conformance	[目的] 証明書ポリシーもしくは認証実施フレームワークを書く人を支援するためのフレームワークを提供	[読者] 政府機関において電子政府システムの調達を行う政府職員、 ならびに、電子政府システムの構築、運用を行う情報システムの開発者および運用者 [目的] 日本政府機関の電子政府システムの調達/運用において、鍵管理の『生成』、『有効期限』、『廃棄』、『更新』、『鍵が露呈した場合の対処』等の各手順に関する推奨される考え方と関連する情報提供を行うこと	[目的] ・暗号鍵の管理に対するニーズを把握する ・暗号の鍵管理に関する技術動向並びに海外の政策動向等および鍵管理の実態を把握した上で、暗号鍵の具体的な取扱方法を提示する。	[目的] 暗号鍵管理について特に鍵のライフサイクルに注目し一般的にその要点を示す。 [読者] 情報システムの調達／運用の担当者、およびこれらから依頼・指示されシステムの構築・運用を行う者	・本調査は、米国や国際社会における**鍵寄託・鍵回復**に関する歴史的な動向を振り返 ・当時の日本政府の対応や、通産省・IPAが実施した鍵回復試作システムの内容を概観した上で、現代的な視点での鍵回復システムの必要性や課題などをまとめるものである。
他文献との関連		・ENISAの2013版Algorithms, key size and parameters Report.の一部 ・鍵管理は「Algorithms, key size and parameters Report.2014」と同じ記載	単独	単独		CRYPTREC の活動内容と NIST800-57 等の情報を集約		"SP800-57 Part 1（鍵管理に関する推奨事項、改訂版）を参考とした。"	単独
年月	2016/1/28	2013/9	2011/12	2016/12/27	2003/11 (14年も前)	2011/6	2008/7	2008/7	2013/2
1	**3 セキュリティサービス** 3.1 機密性 3.2 データ完全性 3.3 認証 3.4 権限付与 3.5 否認防止 3.6 支援サービス 3.7 結合サービス	**3.2. Security Requirements** 3.2.1. Confidentiality 3.2.2. Integrity 3.2.3. Availability　可用性 3.2.4. Forward confidentiality 3.2.5. Non-repudiation　否認防止							
1	**4 暗号アルゴリズム** 4.1 暗号アルゴリズムのクラス 4.2 暗号アルゴリズムの機能 4.2.1 ハッシュ関数 4.2.2 暗号化および復号で使用される対称鍵アルゴリズム 4.2.3 メッセージ認証コード（MAC） 4.2.4 ディジタル署名アルゴリズム 4.2.5 鍵確立スキーム 4.2.6 鍵確立プロトコル 4.2.7 乱数ビット生成	**4. Basic cryptographic techniques** 4.1. Encryption 4.2. Data authentication 4.3. Hashing 4.4. Digital signing **5. Cryptographic primitives** 5.1. Symmetric primitives 5.1.1. Block cipher 5.1.2. Stream cipher 5.1.3. Hash function 5.1.4. Message Authentication Code 5.2. Asymmetric primitives 5.2.1. Factoring/RSA problem 5.2.2. Discrete logarithm 5.2.3. Pairing 5.3. Strength of cryptographic primitives 5.3.1. Key sizes 5.3.2. Shortcut attacks							
1	**5 一般的な鍵管理ガイダンス**								
1	**5. 1 鍵種別とその他の情報** 5.1.1 暗号鍵 5.1.2 その他の暗号学的または関連する情報							2.2.2. 暗号鍵の分類	
1	5.2 鍵使用法								
1	**5.3 暗号期間** 5.3.1 暗号期間に影響するリスク要因 5.3.2 暗号期間に影響する帰結要因 5.3.3 暗号期間に影響するその他の要因 5.3.4 非対称鍵の使用期間と暗号期間 5.3.5 対称鍵の使用期間と暗号期間 5.3.6 鍵種別に固有の暗号期間に関する推奨事項 5.3.7 その他の暗号学的または関連する情報についての推奨事項					公開鍵 3.3 個別暗号鍵の有効期間の設計指針 共通鍵 4.3 個別鍵の有効期間の設計指針 sp800-57 part1の期間と日本の期間の表		2.3.2. 鍵の有効期間設定	

No	1	12	14	15	16	17	18	19	21
文献	SP 800-57 Part1	ENISA	ENISA	OASIS	RFC3647	CR2010GK	IPA2008R	IPA2008G	IPA2013
文献名		Recommended cryptographic measures	Study on the use of cryptographic techniques in Europe	KMIP Specification V1.3 (OASIS Standard) Key Management Interoperability Protocol Specification Version 1.3 OASIS Standard	インターネット X.509 PKI：証明書ポリシーと認証実施フレームワーク	2010年度版 リストガイド(鍵管理) CRYPTREC	安全な暗号鍵のライフサイクルマネージメントに関する調査 調査報告書	安全な暗号鍵のライフサイクルマネージメントに関する調査 鍵管理ガイドライン(案)	暗号鍵の適切な運用・管理に係る課題調査 調査報告書
略称	Part 1 (General)	[ENISA]Recommended	[ENISA]Use	KMIP	X.509	[CR]リストガイド	[IPA]調査報告書	[IPA]鍵管理ガイドライン(案)	[IPA]鍵寄託(Escrow)
1	5.4 保証 5.4.1 完全性の保証(完全性の保護) 5.4.2 ドメインパラメータ有効性の保証 5.4.3 公開鍵有効性の保証 5.4.4 プライベート鍵所持の保証 5.5 鍵およびその他の鍵材料の危殆化								
1	**5.6 暗号アルゴリズムと鍵サイズの選択についてのガイダンス** 5.6.1 アルゴリズムの同等強度 5.6.2 適切なアルゴリズムスイートの定義 5.6.3 アルゴリズムスイートの利用 5.6.4 新しいアルゴリズムおよび鍵サイズへの移行 5.6.5 セキュリティ強度の減少								
1	**6 暗号学的情報の保護要件**								
1	6.1 保護および保証要件								
1	6.1.1 暗号鍵の保護および保証要件の要約								
1	6.1.2 その他の暗号学的情報や関連情報に対する保護要件の要約								
1	6.2 保護メカニズム								
1	6.2.1 送信中の暗号学的情報の保護メカニズム 6.2.1.1 可用性 6.2.1.2 完全性 6.2.1.3 機密性 6.2.1.4 用途やアプリケーションとの関連付け 6.2.1.5 その他のエンティティとの関連付け 6.2.1.6 その他の関連情報との関連付け					**共通項目** **5.1 鍵を転送する場合の鍵の保護** 5.1.1 可用性 5.1.2 完全性 5.1.3 守秘性 5.1.4 用途またはアプリケーションとの関係性 5.1.5 その他のエンティティとの関係性 5.1.6 その他関連情報との関係性 ※SP800-57 part1と類似			
1	6.2.2 保管情報の保護メカニズム 6.2.2.1 可用性 6.2.2.2 完全性 6.2.2.3 機密性 6.2.2.4 用途やアプリケーションとの関連付け 6.2.2.5 その他のエンティティとの関連付け 6.2.2.6 その他の関連情報との関連付け					**共通項目** **5.2 ストレージ上での鍵の保護** 5.2.1 可用性 5.2.2 完全性 5.2.3 守秘性 5.2.4 用途またはアプリケーションとの関係性 5.2.5 その他のエンティティとの関係性 5.2.6 その他関連情報との関係性 ※SP800-57 part1と類似			
1	6.2.3 暗号学的情報に関連付けされるメタデータ 識別子、期間、種別、状態 など [SP800-152]はメタデータの使用についての追加の情報を提供する。								
1	**7 鍵の状態と遷移** 7.1 活性化前状態 7.2 活性化状態 7.3 一時停止状態 7.4 不活性化状態 7.5 危殆化状態 7.6 破棄状態				4.6.4. アクティベーションデータ アクティベーションデータの防護				

No	1	12	14	15	16	17	18	19	21
文献	SP 800-57 Part1	ENISA	ENISA	OASIS	RFC3647	CR2010GK	IPA2008R	IPA2008G	IPA2013
文献名		Recommended cryptographic measures	Study on the use of cryptographic techniques in Europe	KMIP Specification V1.3 (OASIS Standard) Key Management Interoperability Protocol Specification Version 1.3 OASIS Standard	インターネット X.509 PKI：証明書ポリシーと認証実施フレームワーク	2010年度版 リストガイド（鍵管理）CRYPTREC	安全な暗号鍵のライフサイクルマネージメントに関する調査 調査報告書	安全な暗号鍵のライフサイクルマネージメントに関する調査 鍵管理ガイドライン（案）	暗号鍵の適切な運用・管理に係る課題調査 調査報告書
略称	Part 1 (General)	[ENISA]Recommended	[ENISA]Use	KMIP	X.509	[CR]リストガイド	[IPA]調査報告書	[IPA]鍵管理ガイドライン（案）	[IPA]鍵寄託(Escrow)
1	**8 鍵管理のフェーズと機能** **8.1 運用前フェーズ** 8.1.1 利用者登録機能 8.1.2 システム初期化機能 8.1.3 利用者初期化機能 8.1.4 鍵材料インストール機能 8.1.5 鍵確立機能 8.1.6 鍵登録機能 **8.2 運用フェーズ** 8.2.1 正常な運用中のストレージ機能 8.2.2 運用機能の継続 8.2.3 鍵の変更機能 8.2.4 鍵導出方法 **8.3 運用後フェーズ** 8.3.1 アーカイブストレージと鍵回復の機能 8.3.2 エンティティ登録抹消機能 8.3.3 鍵登録抹消機能 8.3.4 鍵破棄機能 8.3.5 鍵失効機能 8.4 破棄フェーズ	**5.4. Key management** 5.4.1. Secret keys and public/private key pairs 5.4.2. Objectives of key management 5.4.3. Key generation 5.4.4. Key registration/certificatio 5.4.5. Key distribution & installation 5.4.6. Key use 5.4.7. Key storage 5.4.8. Revocation/validation 5.4.9. Key destruction 「Algorithms, keysize and parameters report 2014 」の6.3 Key Life Cycle Managementと同じ			4.4.7. 証明書の鍵の再生成 新しい鍵ペアを生成して、(新しい公開鍵を認定する)新しい証明書が発行されることについて 4.4.9. 証明書の失効と一時保留 プライベート鍵危殆化の懸念 4.4.12. 鍵寄託と復旧 4.5.6. 鍵 Changeover 4.6.1. 鍵ペアの生成と導入 4.6.2. プライベート鍵の防護と暗号モジュールエンジニアリングのコントロール	公開鍵 3.4 暗号鍵の更新手順 3.4.1 鍵の回復 3.4.2 鍵の変更 3.5 鍵の廃棄手順 3.5.1 鍵の廃棄 3.5.2 鍵の失効 3.7 鍵の保存手順 3.7.1 有効期間内の鍵の保存手順 3.7.2 有効期間終了後の鍵の保存手順 （アーカイブの説明が詳しい） 共通鍵 4.4 暗号鍵の更新手順 4.4.1 鍵の回復 4.4.2 鍵の変更 4.5 個別鍵の廃棄手順 4.5.1 鍵の廃棄 4.5.2 鍵の失効 4.7 鍵の保存手順 4.7.1 有効期間内の鍵の保存手順 4.7.2 有効期間終了後の鍵の保存手順		**3. 暗号鍵ライフサイクル管理** 3.1. 鍵の生成 3.1.1. 一般 3.1.2. 公開鍵暗号方式の鍵ペアの場合 3.1.3. 共通鍵暗号方式の秘密鍵の場合 3.2. 鍵の配送 3.2.1. 一般 3.2.2. 公開鍵暗号方式の鍵ペアの場合 3.2.3. 共通鍵暗号方式の秘密鍵の場合 3.3. 鍵の利用 3.3.1. 鍵の変更 3.3.2. 鍵の導出 3.4. 鍵の保管／バックアップ 3.4.1. 鍵の保管 3.4.2. 鍵のバックアップ 3.5. 鍵の期限切れ／失効／廃棄 3.5.1. 鍵の期限切れ 3.5.2. 鍵の失効 3.5.3. 鍵の廃棄 3.6. 鍵の回復	
1	**9 責任追跡性、監査、および抗たん性**								
1	9.1 責任追跡性								
1	9.2 監査								
1	9.3 鍵管理システムの抗たん性								
1	9.3.1 バックアップ鍵								
1	9.3.2 鍵回復								
1	9.3.3 システムの冗長性／緊急時対応計画の立案					公開鍵 3.6 鍵が漏洩した場合のリスクを低減する方法 秘密鍵 4.6 鍵が漏洩した場合のリスクを低減する方法			
1	9.3.4 危殆化からの回復							2.3.3. 鍵危殆化の想定	
1	**10 暗号デバイスやアプリケーションの鍵管理仕様**								
1	10.1 鍵管理仕様説明／目的								
1	10.2 鍵管理仕様の内容								
1	10.2.1 暗号アプリケーション								
1	10.2.2 通信環境								
1	10.2.3 鍵管理構成要素の要求事項								
1	10.2.4 鍵管理構成要素の生成								
1	10.2.5 鍵管理構成要素の配付								
1	10.2.6 鍵材料保管								
1	10.2.7 アクセス制御								
1	10.2.8 責任追跡性								
1	10.2.9 危殆化の管理と回復								
1	10.2.10 鍵回復								
1									
1	**附属書A:暗号学的および非暗号学的な完全性と情報源認証メカニズム**								

No	1	12	14	15	16	17	18	19	21
文献	SP 800-57 Part1	ENISA	ENISA	OASIS	RFC3647	CR2010GK	IPA2008R	IPA2008G	IPA2013
文献名		Recommended cryptographic measures	Study on the use of cryptographic techniques in Europe	KMIP Specification V1.3 (OASIS Standard) Key Management Interoperability Protocol Specification Version 1.3 OASIS Standard	インターネット X.509 PKI：証明書ポリシーと認証実施フレームワーク	2010年度版 リストガイド(鍵管理) CRYPTREC	安全な暗号鍵のライフサイクルマネージメントに関する調査 調査報告書	安全な暗号鍵のライフサイクルマネージメントに関する調査 鍵管理ガイドライン(案)	暗号鍵の適切な運用・管理に係る課題調査 調査報告書
略称	Part 1 (General)	[ENISA]Recommended	[ENISA]Use	KMIP	X.509	[CR]リストガイド	[IPA]調査報告書	[IPA]鍵管理ガイドライン(案)	[IPA]鍵寄託(Escrow)
1	**<u>附属書B: 鍵回復</u>** B.1 保管された鍵材料からの回復 B.2 鍵材料の復元による回復 B.3 鍵材料が回復可能である必要があるような条件 B.4 鍵回復システム B.5 鍵回復方針								
7									
7,2									
7									
7									
7									

No	1	12	14	15	16	17	18	19	21
文献	SP 800-57 Part1	ENISA	ENISA	OASIS	RFC3647	CR2010GK	IPA2008R	IPA2008G	IPA2013
文献名		Recommended cryptographic measures	Study on the use of cryptographic techniques in Europe	KMIP Specification V1.3 (OASIS Standard) Key Management Interoperability Protocol Specification Version 1.3 OASIS Standard	インターネット X.509 PKI：証明書ポリシーと認証実施フレームワーク	2010年度版 リストガイド(鍵管理) CRYPTREC	安全な暗号鍵のライフサイクルマネージメントに関する調査 調査報告書	安全な暗号鍵のライフサイクルマネージメントに関する調査 鍵管理ガイドライン(案)	暗号鍵の適切な運用・管理に係る課題調査 調査報告書
略称	Part 1 (General)	[ENISA]Recommended	[ENISA]Use	KMIP	X.509	[CR]リストガイド	[IPA]調査報告書	[IPA]鍵管理ガイドライン(案)	[IPA]鍵寄託(Escrow)
7									
7				相互運用プロトコル					
7									
7									
7									
7									
12		<u>6. Case study. Protective</u> measures 6.1. Classification 6.1.1. Type 0: hashed-data-only leak 6.1.2. Type 1: logical leakage 6.1.3. Type 2: hardware leakage 6.1.4. Type 3: break-in on live device 6.1.5. Type 4: full user impersonation 6.2. Countermeasures 対策 6.2.1. Secure deletion of files 6.2.2. Authenticated encryption 6.2.3. Secure hardware 6.2.4. Key architecture 6.2.5. Access control system							
12,13									
2									

No	1	12	14	15	16	17	18	19	21
文献	SP 800-57 Part1	ENISA	ENISA	OASIS	RFC3647	CR2010GK	IPA2008R	IPA2008G	IPA2013
文献名		Recommended cryptographic measures	Study on the use of cryptographic techniques in Europe	KMIP Specification V1.3 (OASIS Standard) Key Management Interoperability Protocol Specification Version 1.3 OASIS Standard	インターネット X.509 PKI：証明書ポリシーと認証実施フレームワーク	2010年度版　リストガイド（鍵管理） CRYPTREC	安全な暗号鍵のライフサイクルマネージメントに関する調査　調査報告書	安全な暗号鍵のライフサイクルマネージメントに関する調査　鍵管理ガイドライン（案）	暗号鍵の適切な運用・管理に係る課題調査 調査報告書
略称	Part 1 (General)	[ENISA]Recommended	[ENISA]Use	KMIP	X.509	[CR]リストガイド	[IPA]調査報告書	[IPA]鍵管理ガイドライン（案）	[IPA]鍵寄託(Escrow)
2									
2									
2									
3,16,19					証明書、PKI全般を記載	**3.2 鍵の生成手順(公開鍵)** 3.2.1 PKI におけるトラストアンカーの公開鍵の配送 3.2.2 登録局RA および認証局CA への申請 3.2.3 一般的な公開鍵の配送 3.2.4 中央サーバ等で生成された鍵ペアの配送		**4. PKI システムにおける暗号鍵ライフサイクル管理** 4.1. 利用者のプライベート鍵の管理 4.2. ユーザおよび認証局の鍵ペアに係るその他の鍵の管理 4.2.1. 認証局のプライベート鍵の管理 4.2.2. 利用者の公開鍵の管理 4.2.3. 認証局の公開鍵の管理	
3									
3									
3									
3									
3									
3									
3									
3									
3									
14			3 Survey results 3.1 Availability of cryptographic policies 3.2 Surveyed cryptographic policies (by type of application) 3.3 Data recommended to be encrypted 3.4 Encryption of data between the citizens and e-government services 3.5 Encryption of data shared between government systems 3.6 Protection of data at rest 3.7 Recommended cryptographic techniques 3.7.1 Key exchange algorithms 3.7.2 Signature schemes 3.7.3 Data encryption algorithms 3.7.4 Hash functions 3.8 Consistency of cryptography specifications 3.9 Key management 3.10 Auditing 3.11 Maintaining policies and guidelines 3.12 Information resources used for defining recommendations and policies 3.13 Perceptions of the IT industry 3.13.1 General level of expertise and knowledge of specific standards 3.13.2 How cryptographic parameters are selected 3.13.3 Common errors in the configuration of cryptography 3.13.4 What should European governments do to improve the deployment of cryptography?					

No	1	12	14	15	16	17	18	19	21
文献	SP 800-57 Part1	ENISA	ENISA	OASIS	RFC3647	CR2010GK	IPA2008R	IPA2008G	IPA2013
文献名		Recommended cryptographic measures	Study on the use of cryptographic techniques in Europe	KMIP Specification V1.3 (OASIS Standard) Key Management Interoperability Protocol Specification Version 1.3 OASIS Standard	インターネット X.509 PKI：証明書ポリシーと認証実施フレームワーク	2010年度版 リストガイド(鍵管理) CRYPTREC	安全な暗号鍵のライフサイクルマネージメントに関する調査 調査報告書	安全な暗号鍵のライフサイクルマネージメントに関する調査 鍵管理ガイドライン(案)	暗号鍵の適切な運用・管理に係る課題調査 調査報告書
略称	Part 1 (General)	[ENISA]Recommended	[ENISA]Use	KMIP	X.509	[CR]リストガイド	[IPA]調査報告書	[IPA]鍵管理ガイドライン(案)	[IPA]鍵寄託(Escrow)
調査14,18,21			4 Cryptographic specifications beyond MS borders 4.1 Cryptographic specifications in USA and Japan 4.1.1 USA and NIST standards 4.1.2 Japan and CRYPTREC IPA research project 4.2 EU-funded initiatives related to the use of cryptographic techniques 4.2.1 ECRYPT 4.2.2 NESSIE 4.2.3 Action Plan on e-signatures and e-identification and ESI				2. 暗号の鍵管理に係わる技術動向 2.1. パスワードベース鍵交換プロトコル 2.2. グループ鍵共有プロトコル 2.3. プロキシ暗号, 2.4. ID ベース暗号 2.5. まとめ 3. 暗号の鍵管理に係わる海外動向 3.1. 米国NIST 3.2. 国際標準化機構ISO 3.3. Internet Engineering Task Force (IETF) 3.4. まとめ 4. 暗号の鍵管理に係わる国内実態 4.1. 国内における暗号鍵管理の現状 4.2. 暗号鍵管理に関する課題・問題 4.3. 暗号鍵ガイドラインへの要望 4.4. まとめ 5. 暗号鍵管理ガイドライン第1 版 5.1. 暗号利用用途 5.2. 一般的な暗号鍵管理方針 5.3. まとめ 6. 提言		1. はじめに 2. 米国の暗号政策 2.1 CLIPPER政策以前 2.2 CLIPPER政策 2.3 米国の対外政策と暗号輸出規制の緩和 3. 米国以外の国および国際機関の動き 3.1 欧州諸国の動き 3.2 OECDの動き 3.3 G8の動き 3.4 ワッセナー・アレンジメントの動き 3.5 ISOの動き 4. 鍵寄託・鍵回復システムの民間利用 4.1 民間企業における鍵回復機能の必要性 4.2 鍵回復制御 5. 日本の暗号政策と鍵寄託・鍵回復システムへの対応 5.1 日本の暗号政策 5.2 鍵寄託・鍵回復システムの試作 6. 現代的視点での鍵回復システム 6.1 現代的視点での鍵回復システムの目的と要件 6.2 今後の課題
9			5 Concluding remarks 6 List of recommendations						