暗号に関する国内外のガイドラインの実態調査

― 調査報告書 ―

2018 年 1 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**

目 次

1. はじめに

1.1 調査背景・目的

近年、暗号は情報セキュリティの基盤技術として、情報システムの中で広く利用されている。組織の IT 担当者は、情報システムを安全に運用するために、暗号を適切に利用することが求められる。しかしながら、一般の IT 担当者が暗号について知見を持ち、自らの判断で適切に設定してシステムを運用することは容易ではない。

独立行政法人情報処理推進機構（以下「IPA」という。）が、2014 年に実施した「暗号利用環境に関する動向調査」においては、米国 NIST[1]が SP800 シリーズ の中でガイドライン等を整備していることや、欧州の ENISA[2]においても暗号に関する文書の作成を行っていることなどが取りまとめられている。

本調査は、国内の IT 担当者向けにアンケート調査を実施し暗号の利活用に関する課題やニーズを明らかにするとともに、国内外におけるガイドライン等の整備状況とあわせて総合的に分析することで、今後作成を検討すべきガイドラインの対象を明確化することを目的に実施した。

1.2 調査の実施概要

本調査では、国内の暗号の利活用に関する課題やニーズの把握、国内外における暗号の利活用にガイドライン等の整備状況を整理・分析し、今後作成を検討すべきガイドラインの対象を明確化することを目的に以下の調査を実施し、その結果を報告書として取りまとめた。

表 1-1　本調査の概要

調査項目	概要
暗号の利活用に関するアンケート調査（2 章）	・ 国内企業の情報システムまたは情報セキュリティに関与する者を対象としたアンケート ・ 暗号の利活用状況・ガイドラインニーズ等について調査を実施
国内外における暗号の利活用に関する文書の調査（3 章）	・ IPA 等の国内機関、NIST、ENISA、IETF[3]の暗号利活用に関する文書を対象に調査を実施
ヒアリング調査（4 章）	・ アンケート・文書調査の分析結果をもとに、企業・有識者にヒアリング調査を実施

[1] National Institute of Standards and Technology の略で、米国国立標準技術研究所のこと。

[2] European Network and Information Security Agency の略で、欧州ネットワーク情報セキュリティ庁のこと。

[3] Internet Engineering Task Force の略。

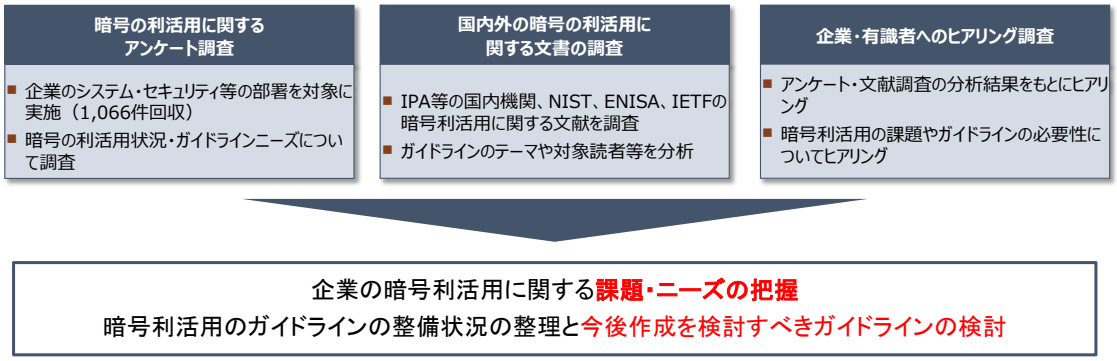

暗号の利活用に関する
アンケート調査
企業のシステム・セキュリティ等の部署を対象に実施（1,066件回収）
暗号の利活用状況・ガイドラインニーズについて調査
国内外の暗号の利活用に
関する文書の調査
IPA等の国内機関、NIST、ENISA、IETFの暗号利活用に関する文献を調査
ガイドラインのテーマや対象読者等を分析
企業・有識者へのヒアリング調査
アンケート・文献調査の分析結果をもとにヒアリング
暗号利活用の課題やガイドラインの必要性についてヒアリング
企業の暗号利活用に関する課題・ニーズの把握
暗号利活用のガイドラインの整備状況の整理と今後作成を検討すべきガイドラインの検討

図 1-1　本調査の概要

2. 暗号の利活用に関するアンケート調査

2.1 調査概要

企業の暗号利活用の状況や課題、暗号利活用に関するガイドラインのニーズ等を把握することを目的にアンケート調査を実施した。

調査は国内企業の、情報システムまたは情報セキュリティに関与する立場のものを対象に実施した。アンケート調査の概要は表 2-1 の通りである。また、アンケート調査票を設計する際に検討した調査仮説は表 2-2 の通りである。

表 2-1　アンケート調査概要

調査目的	国内企業の暗号利活用の状況や課題、暗号利活用に関するガイドラインのニーズ等を把握し、今後作成を検討すべきガイドラインの対象等の検討材料とする。
調査対象	所属する企業で情報システムまたは情報セキュリティに関与する立場の者とし、本調査では以下を対象とした。 ・ 情報システム担当部門の責任者または担当者 ・ 情報セキュリティ担当部門の責任者または担当者 ・ システム・サービス製品の開発責任者または担当者
調査期間	2017 年 5 月下旬から 2017 年 6 月上旬
調査方法	ウェブアンケート調査
回収数	1,066 件
調査項目	・ 回答企業の基本情報 ・ 回答企業における暗号利活用状況 ・ 暗号利活用に関する情報源 ・ 暗号利活用に関するガイドラインのニーズ ・ 暗号に関する組織・制度・新技術の認知度
データ精査	アンケートデータの精度向上を目的に、以下の設問の回答及び回答時間の条件に該当する回収データを除外した。 ・ 問 4 で「暗号技術を利用していない」を選択した回答のうち、以下の条件に該当する回答 ➢ 問 3 で「暗号化製品」を選択 ➢ 問 5 で「暗号技術の利用・適用基準を検討している」を選択 ➢ 問 8 で「暗号技術の利用・運用基準がある」を選択 ➢ 問 12 で「情報セキュリティリスク分析を実施し、情報セキュリティ対策として暗号技術は適切と判断し利用している」または「情報セキュリティリスク分析は実施していないが、暗号技術を利用している」または「情報セキュリティリスク分析を実施しているかわからないが、暗号技術は利用している」を選択 ・ 回答時間 120 秒未満の回答

表 2-2　アンケート調査仮説

暗号利活用の現状に関する仮説	・ 組織的に暗号の導入や管理、運用を行う体制が構築されていないのではないか。 ・ 暗号製品の選定・導入・開発・利用・運用に関して、暗号技術に関する基準が整備されていないのではないか。 ・ 暗号の設定方法や留意事項がわからないまま運用している企業が多いのではないか。 ・ 暗号の詳細を理解し適切に運用できる担当者が不足しているのではないか。 ・ 鍵管理の重要性を理解し、対策を実施している企業は少ないのではないか。
ガイドラインに関する仮説	・ 暗号利活用に関するガイドラインが十分整備されていないため、ガイドラインに対するニーズがあるのではないか。 ・ 企業は暗号の技術的仕様に比べ、暗号利活用に焦点をあてたガイドラインを求めているのではないか。 ・ 求められるガイドラインの種類・テーマ・内容は、システム・セキュリティ担当者と開発担当者で異なるのではないか。 ・ 求められるガイドラインの種類・テーマ・内容は、業務経験年数により異なるのではないか。
暗号に関連する制度・新技術の認知度に関する仮説	・ CRYPTREC[4]・CRYPTREC 暗号リスト・JCMVP[5]の認知度は低いのではないか。 ・ 新技術（耐量子計算機暗号及び軽量暗号）の認知度は低いのではないか。

アンケート回答者の基本情報は、図 2-1 から図 2-5 の通りである。

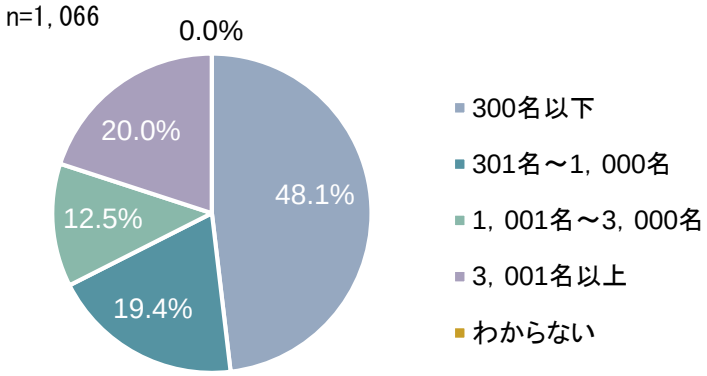


図 2-1　従業員数

[4] Cryptography Research and Evaluation Committees の略。

[5] Japan Cryptographic Module Validation Program の略で、暗号モジュール試験及び認証制度のこと。

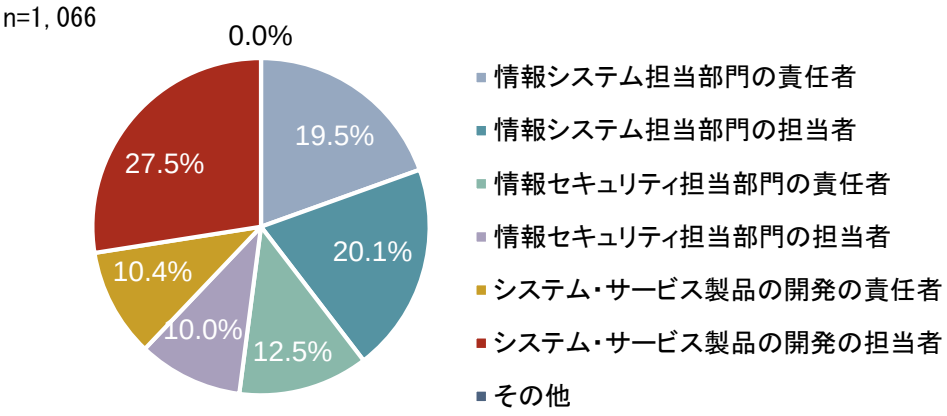


図 2-2　回答者役職

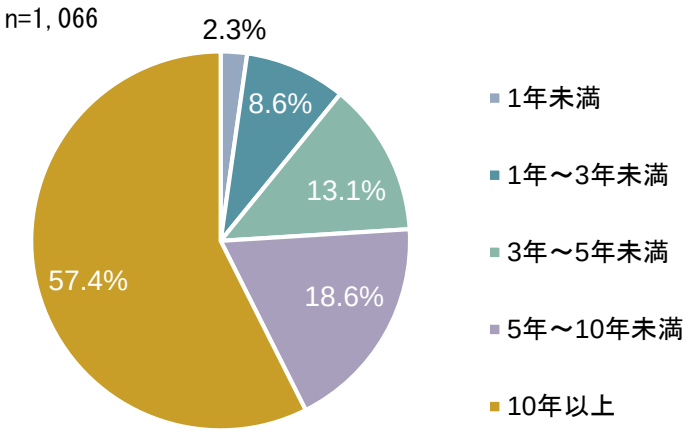


図 2-3　現在の役職での業務経験年数

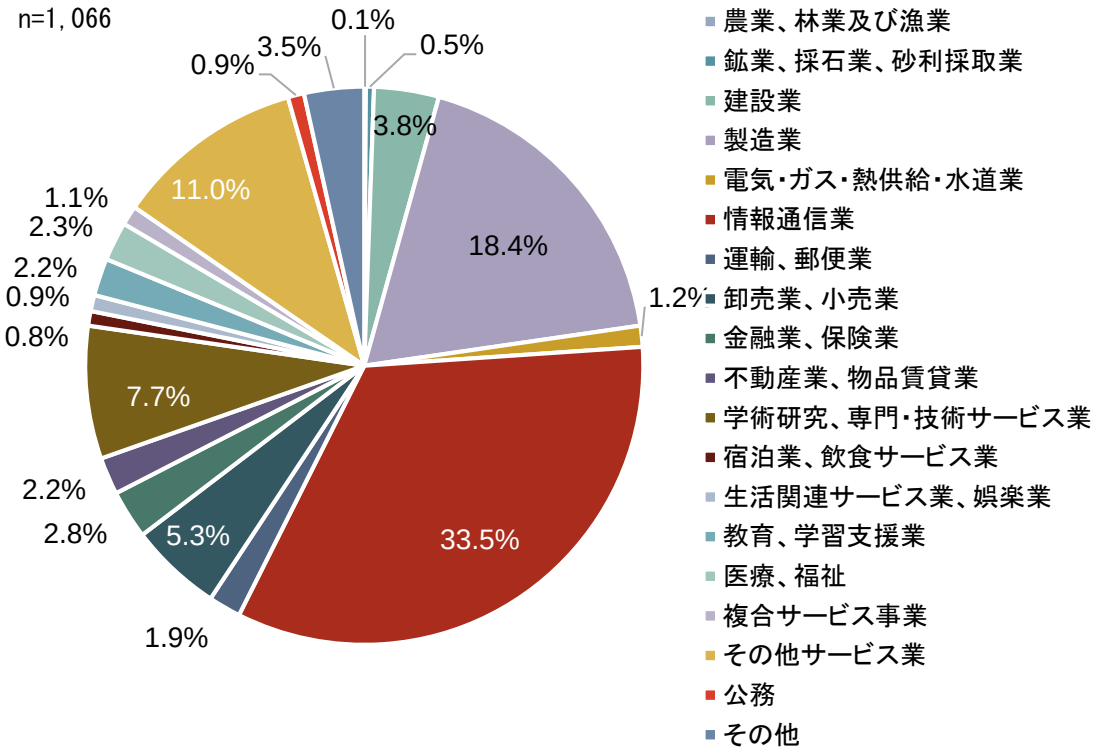

n=1, 066
0.1%
0.5%
3.5%
0.9%
3.8%
18.4%
1.2%
33.5%
1.9%
5.3%
2.8%
2.2%
7.7%
0.8%
0.9%
2.2%
2.3%
1.1%
11.0%
農業、林業及び漁業
鉱業、採石業、砂利採取業
建設業
製造業
電気・ガス・熱供給・水道業
情報通信業
運輸、郵便業
卸売業、小売業
金融業、保険業
不動産業、物品賃貸業
学術研究、専門・技術サービス業
宿泊業、飲食サービス業
生活関連サービス業、娯楽業
教育、学習支援業
医療、福祉
複合サービス事業
その他サービス業
公務
その他

図 2-4　業種

表 2-3　業種

業種	割合（%）
農業、林業及び漁業	0.1
鉱業、採石業、砂利採取業	0.5
建設業	3.8
製造業	18.4
電気・ガス・熱供給・水道業	1.2
情報通信業	33.5
運輸、郵便業	1.9
卸売業、小売業	5.3
金融業、保険業	2.8
不動産業、物品賃貸業	2.2
学術研究、専門・技術サービス業	7.7
宿泊業、飲食サービス業	0.8
生活関連サービス業、娯楽業	0.9
教育、学習支援業	2.2
医療、福祉	2.3
複合サービス事業	1.1
その他サービス業	11.0
公務	0.9
その他	3.5

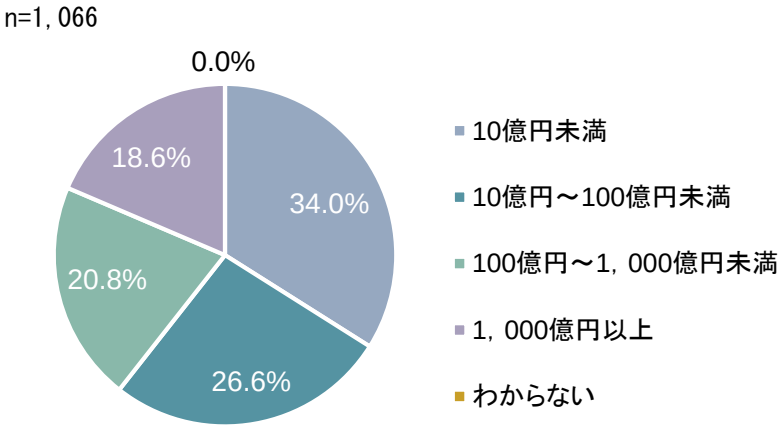


図 2-5　売上高

2.2 調査結果 [6]

本節では、アンケート調査の主な分析結果について説明する。なお、アンケート結果の詳細については、「付録 1　アンケート調査結果詳細」にまとめた。

2.2.1 暗号利用状況

導入している情報セキュリティ対策製品について回答全体をみると、「コンテンツセキュリティ対策製品（ウイルス対策ソフト、ウェブフィルタリングソフト、DLP（情報漏えい対策製品）等）」（82.3%）が最も高く、「暗号化製品（メール、ファイル、外部記録媒体等を暗号化する製品）」は 45.7%となっている。

企業規模別にみると、各種情報セキュリティ対策製品の導入状況は大企業のほうが高く、暗号化製品に関しては、大企業（301 名以上）が 62.0%であるのに対し、中小企業（300 名以下）では 28.1%となっている。

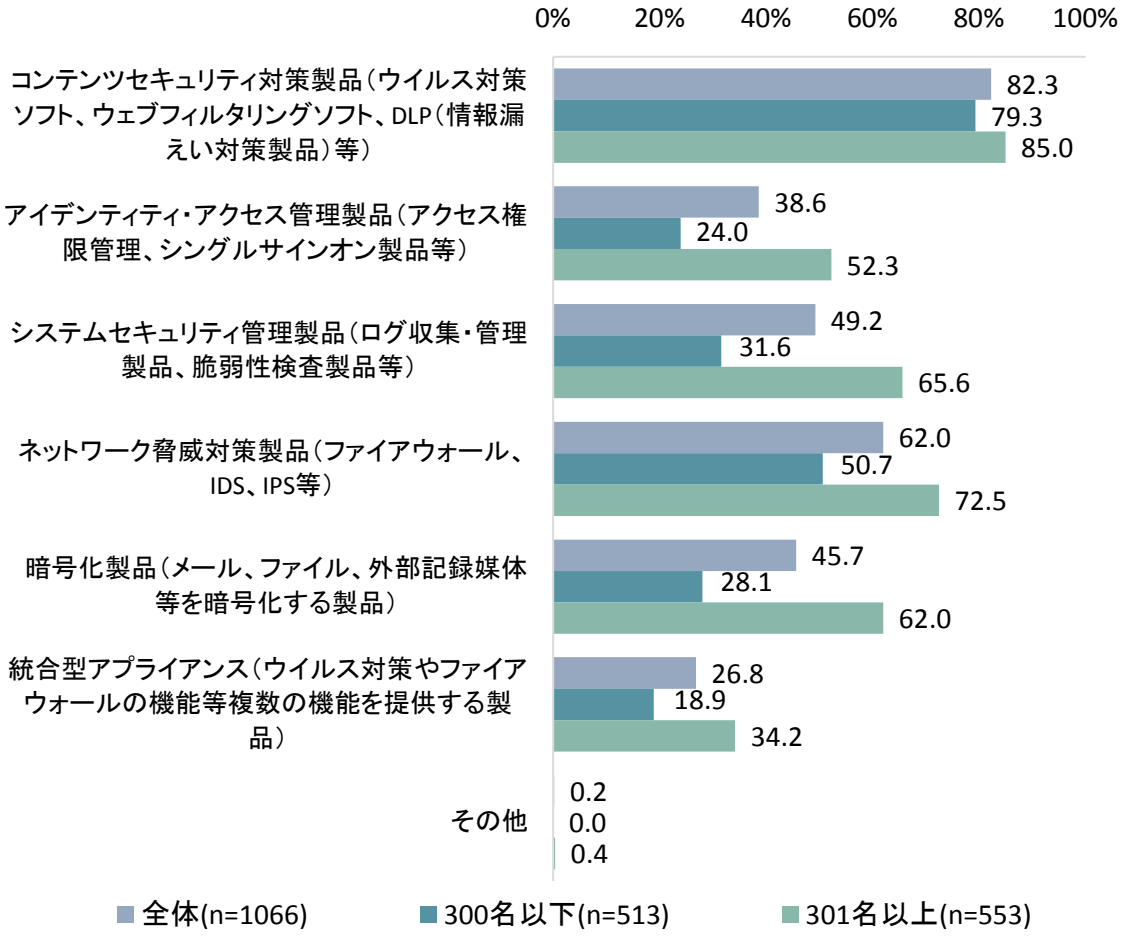


図 2-6　導入している情報セキュリティ対策製品（複数回答）

[6] 本調査では、中小企業を従業員数 300 名以下、大企業を従業員数 301 名以上と定義し分析した。

暗号技術[7]の利活用場面について全体をみると、「インターネット通信の暗号化（SSL や VPN 等）」（65.6%）が最も高く、以下「電子メールの暗号化（メッセージや添付ファイルの暗号化等）」（50.8%）、「ファイルの暗号化」（39.4%）の順となっている。

企業規模別にみると、大企業（301 名以上）では中小企業（300 名以下）に比べ、インターネット通信の暗号化等多くの場面で暗号を利用している。また、中小企業（300 名以下）では、「暗号技術を利用していない」との回答が 28.3%となっている。

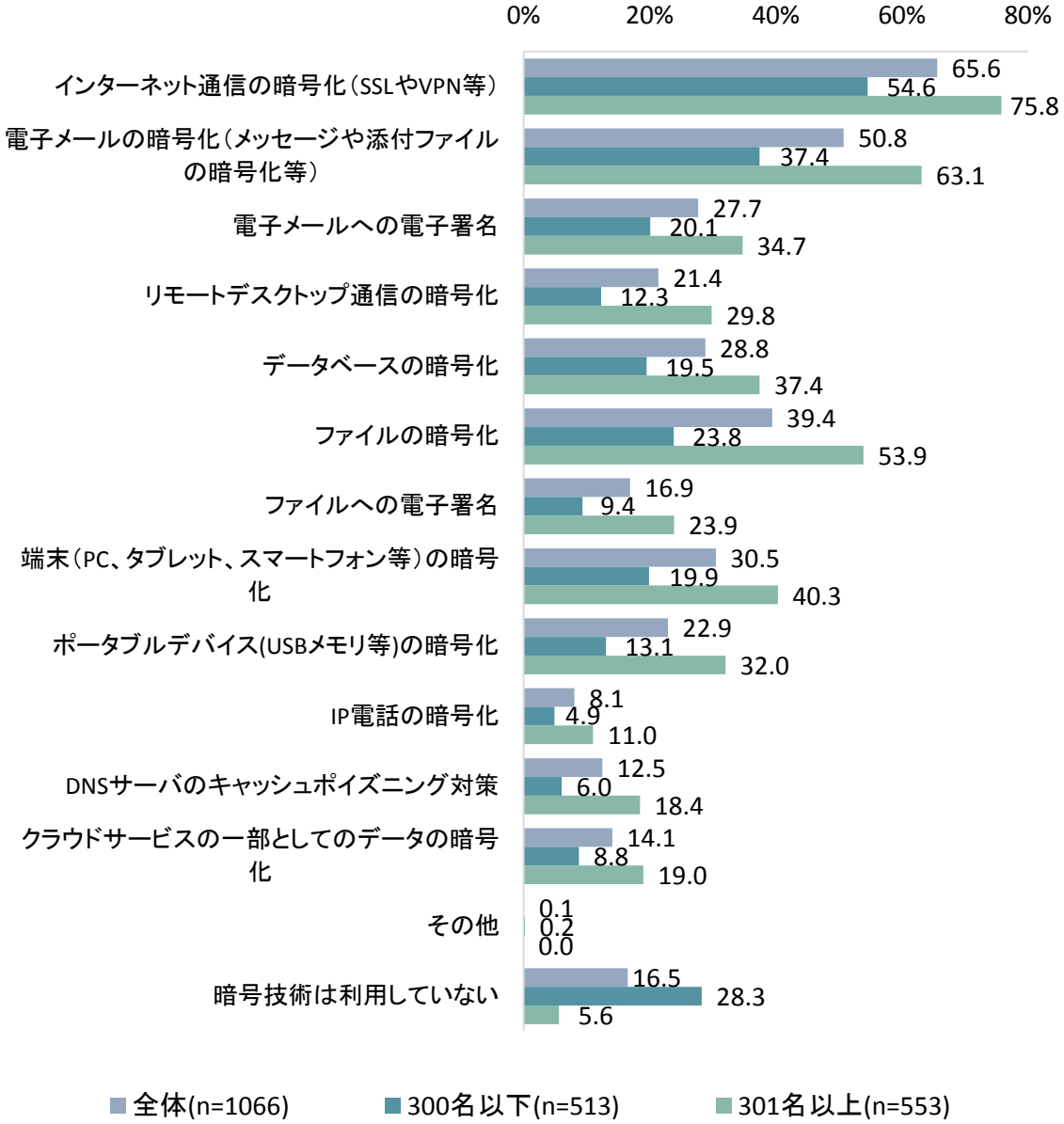


図 2-7　暗号技術の利活用場面（複数回答）

[7] 本調査では暗号技術を「公開鍵暗号や共通鍵暗号等の暗号に加え、周辺関連技術（電子署名、ハッシュ関数等）も含まれるもの」と定義した。

2.2.2 システム関連製品の選定・導入・開発時の暗号技術に関する基準・課題

システム関連製品の選定・導入時の暗号技術に関する基準の有無について、「暗号技術の利用・適用に関する基準がある」との回答は 23.1%で、基準が整備されている企業の割合は低い。

企業規模別にみると、「暗号技術の利用・適用に関する基準がある」との回答は大企業（301 名以上）で 33.8%、中小企業（300 名以下）で 11.5%となり、大企業のほうが基準の整備が進んでいる。特に中小企業（300 名以下）では、「暗号技術の利用・適用に関する基準はなく個別に判断している」と回答する割合が高い。

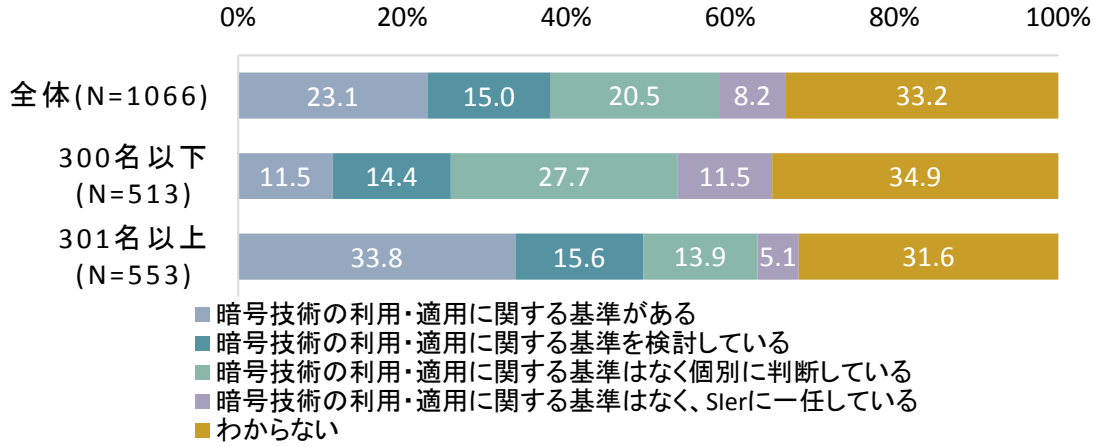


図 2-8　暗号技術に関する基準の有無（選定・導入時）

システム関連製品の開発時の暗号技術に関する基準の有無について、「暗号技術の利用・適用に関する基準がある」は 17.9%で、選定・導入と比べると基準がある割合はやや低下している。

企業規模別にみると、「暗号技術の利用・適用に関する基準がある」は大企業で 26.6%、中小企業で 8.6%となっており、選定・導入と同様大企業のほうが基準の整備が進んでいる。

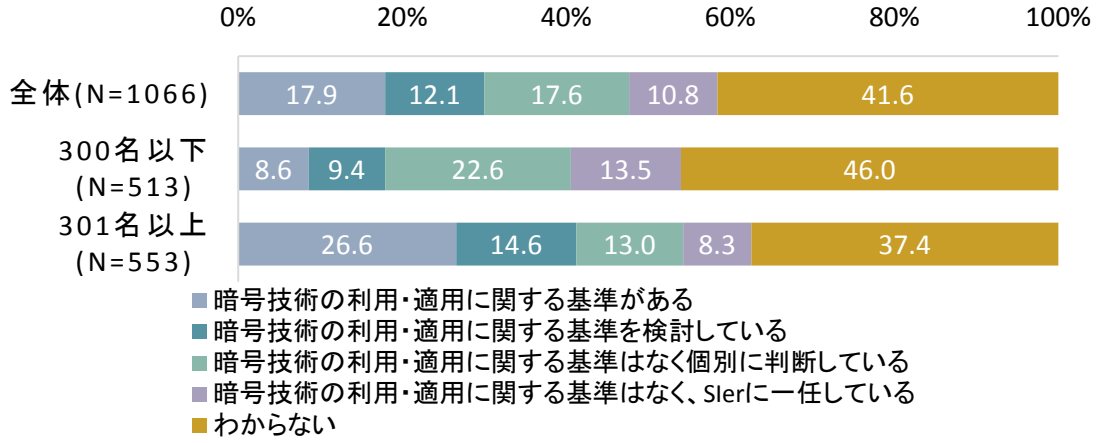


図 2-9　暗号技術に関する基準の有無（開発時）

システム関連製品を選定・導入する際の暗号技術に関する課題について確認したところ、企業規模に関係なく、「導入・維持管理コストが高い」を課題とする割合が高く、次に「どの製品が安全で導入してよいものであるのかがわからない」・「正しくかつセキュアな暗号処理が行われているか、確信が持てない」を課題としてあげる割合が高い。

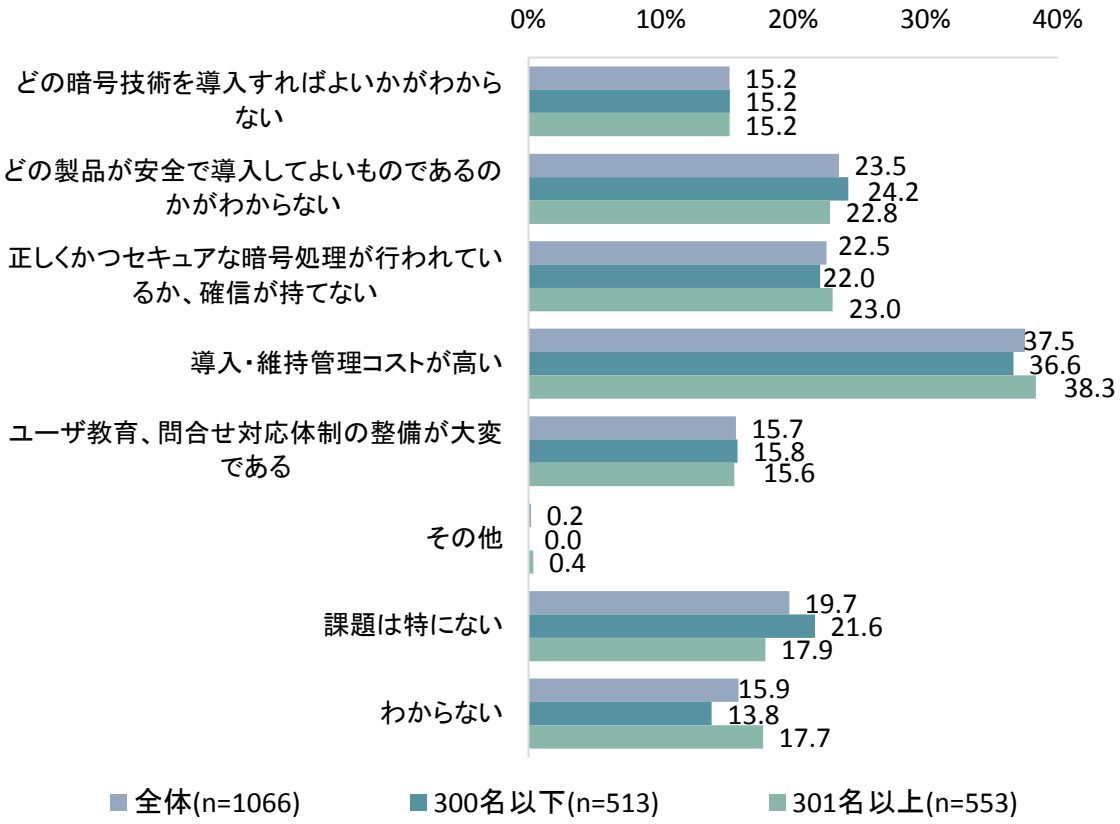


図 2-10　システム関連製品を選定・導入時の暗号技術に関する課題（複数回答）

2.2.3 暗号技術の利用・運用時の基準・課題

暗号技術を利用・運用する際の基準の有無について全体をみると、「暗号技術の利用・運用基準はなく、個別に判断している」（26.5%）が最も高く、次に「暗号技術の利用・運用基準がある」（25.6%）となっている。システム関連製品の選定・導入・開発時の暗号技術に関する基準の有無と比較すると、利用・運用に関しては個別に判断している企業の割合が高い。

企業規模別にみると、「暗号技術の利用・運用基準がある」との回答は、大企業（301 名以上）で 38.0%、中小企業（300 名以下）で 12.3%となっており、システム関連製品の選定・導入・開発時の暗号技術に関する基準と同様、大企業のほうが基準の整備が進んでいる。

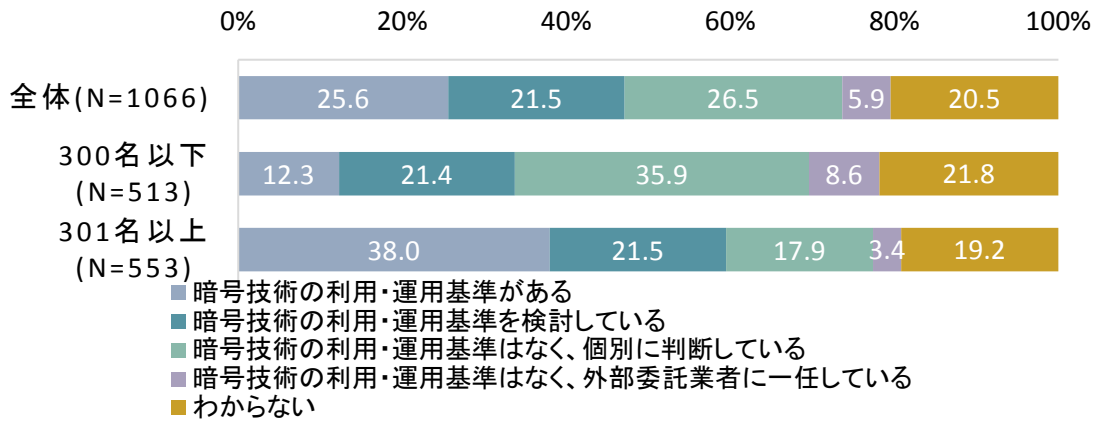


図 2-11　暗号技術の利用・運用に関する基準の有無

暗号技術を利用・運用する際の課題は、企業規模に関係なく「情報システムの暗号に関する部分を適切に運用できる人材がいない」・「ユーザの利便性と暗号技術の導入によるセキュリティ対策のバランスをとるのが難しい」・「暗号鍵の管理が難しい」等が課題としてあげられている。

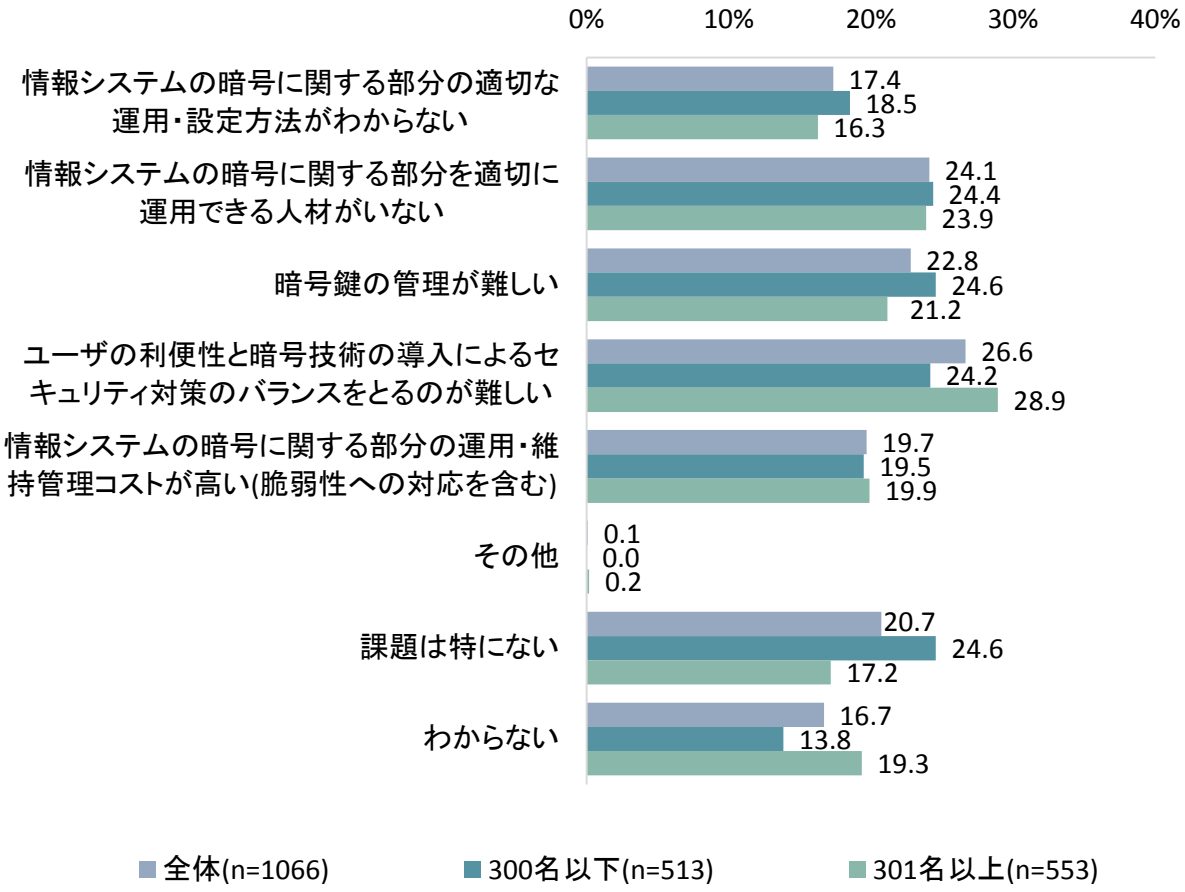


図 2-12　暗号技術を利用･運用する際の課題（複数回答）

2.2.4 暗号鍵管理

暗号鍵管理の必要性について確認したところ、全体の約 7 割が暗号鍵管理の必要性を認識しているが、「暗号鍵を適切に管理する必要があると考えており、対策も実施している」との回答は 27.2%で、鍵管理の必要性の認識はあるものの、対策まで実施できている割合は低い。

企業規模別にみると、大企業（301 名以上）は中小企業（300 名以下）に比べ、鍵管理の必要性を認識しており、対策を実施している割合も高い。

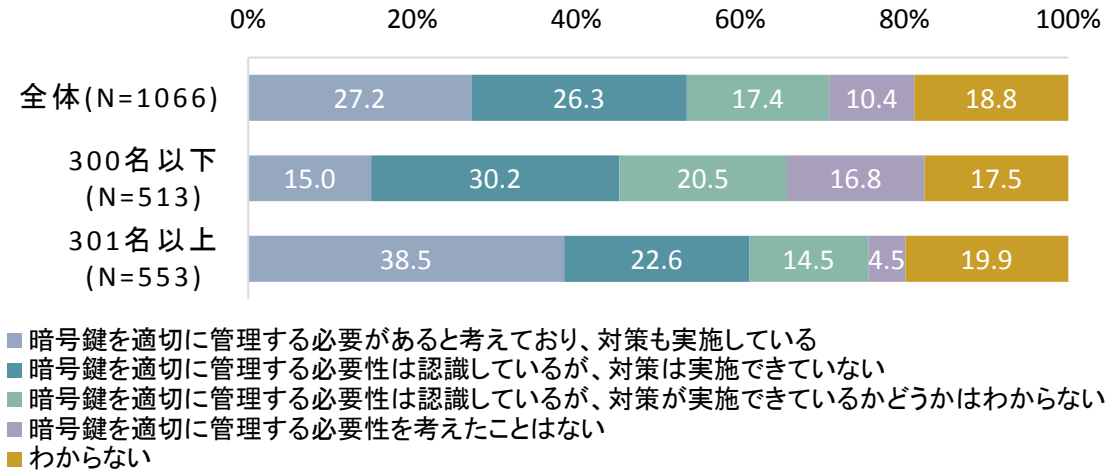


図 2-13　暗号鍵管理の必要性認識と対策状況

2.2.5 暗号技術に関する情報源

暗号技術を利用する際に参照する情報について確認したところ、全体では「自社で利用している製品ベンダからの情報」が 32.1%、「IPA からの情報」が 31.2%、「国内の情報セキュリティ関連組織（政府関係機関除く）からの情報」が 28.0%となっている。

企業規模別にみると、大企業（301 名以上）では「IPA からの情報」が最も高く、次いで「自社で利用している製品ベンダからの情報」が高い。一方中小企業（300 名以下）では、「特に参照していない」との回答が 4 割を超えているものの、情報源としては、「自社で利用している製品ベンダからの情報」が最も高い。

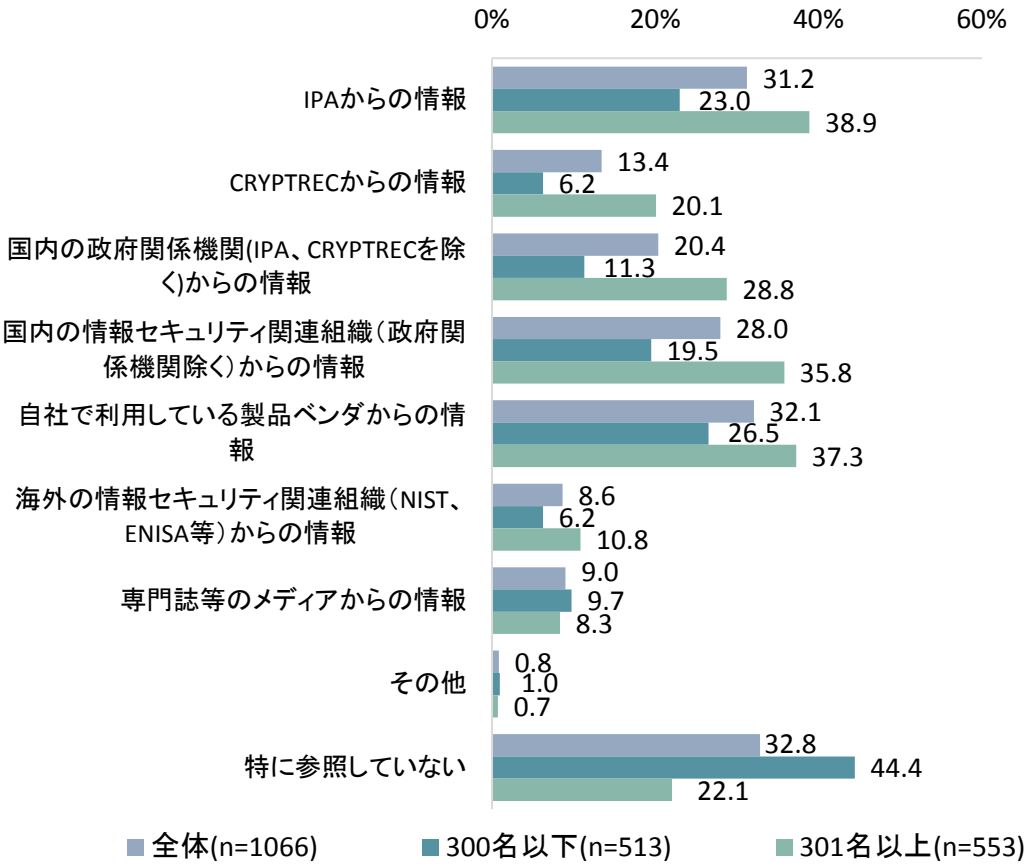


図 2-14　暗号技術を利用する際に参照する情報（複数回答）

暗号技術に関する人材の状況について確認したところ、大企業（301 名以上）では「暗号技術に特化した専門家がいる」・「暗号技術には特化していないが、セキュリティの専門家がいる」割合が 5 割程度で、大企業では暗号技術に関する人材がある程度いる。一方中小企業（300 名以下）では、「特に暗号技術に詳しい人材はいない（疑問がある場合は担当者が随時調査）」との回答が 50.5%で、大企業に比べ暗号技術に関する人材は確保されていない。

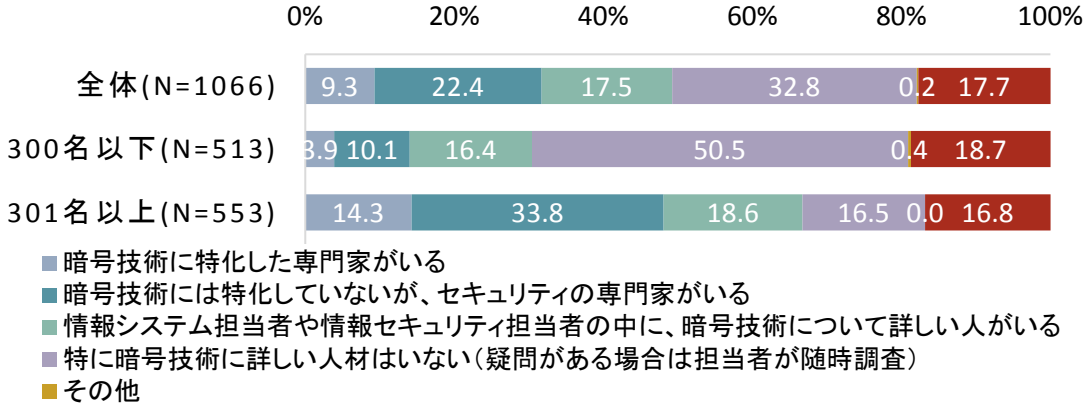


図 2-15　暗号技術に関する人材

2.2.6 暗号技術の利活用に関するガイドライン

暗号技術の利活用に関するガイドラインの必要性について、約 7 割（「公的機関（政府機関）が発行する内容がまとまったガイドラインが必要」と「内容がまとまったガイドラインが必要（公的機関発行でなくてもよい）」の合計）がガイドラインを必要と回答している。特に、大企業（301 名以上）では約 8 割が必要と回答している。このことから、暗号技術の利活用に関するガイドラインに対するニーズはあると考えられる。

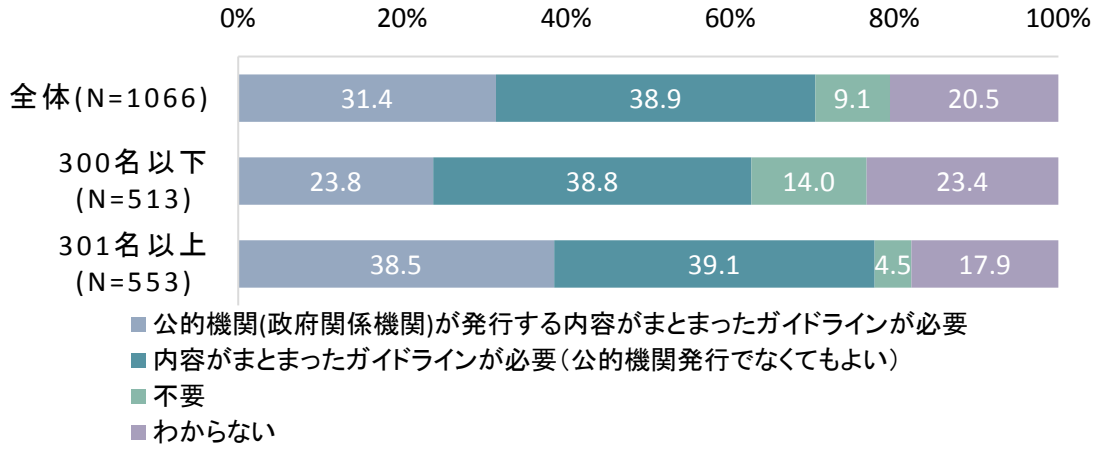


図 2-16　暗号技術の利活用に関するガイドラインの必要性

ガイドラインを必要とする理由は、企業規模による差はほとんどなく、「信頼できる機関の情報を参考にしたい」が最も高く、次に「暗号技術に関してまとまった情報がほしい」があげられている。

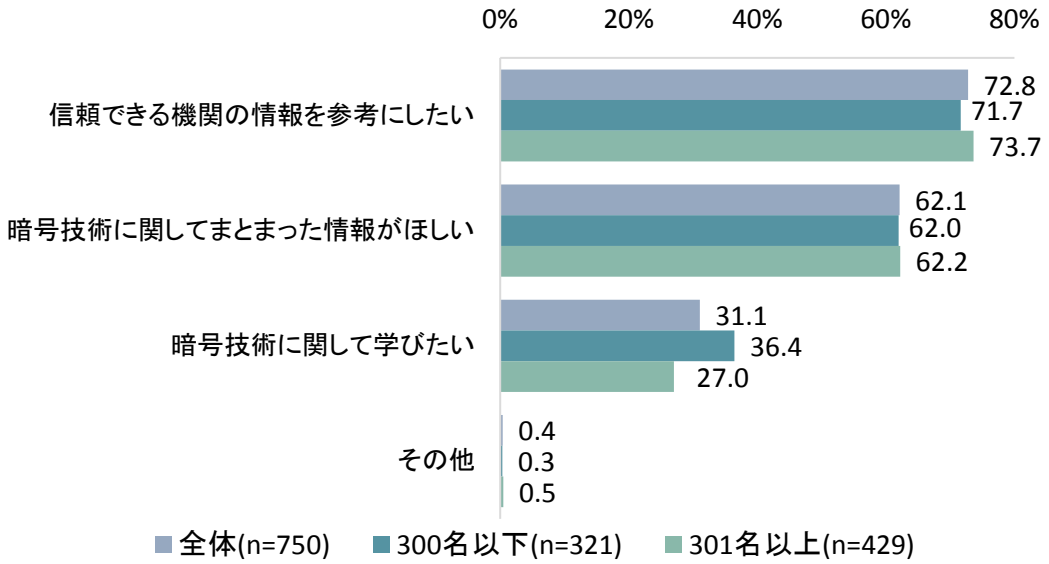


図 2-17　ガイドラインを必要とする理由（複数回答）

暗号技術に関するガイドラインを策定する場合どのような種類のガイドラインがあるとよいか確認したところ、大企業・中小企業ともに「暗号技術を利用した製品（暗号製品）や情報システムにおける暗号技術の設定や運用に関するガイドライン」をあげる割合が最も高く、設定・運用に関するガイドラインに対するニーズがあると考えられる。

また、大企業では「暗号技術を利用した製品（暗号製品）や情報システムにおける暗号技術の開発や実装に関するガイドライン」をあげる割合が高い。

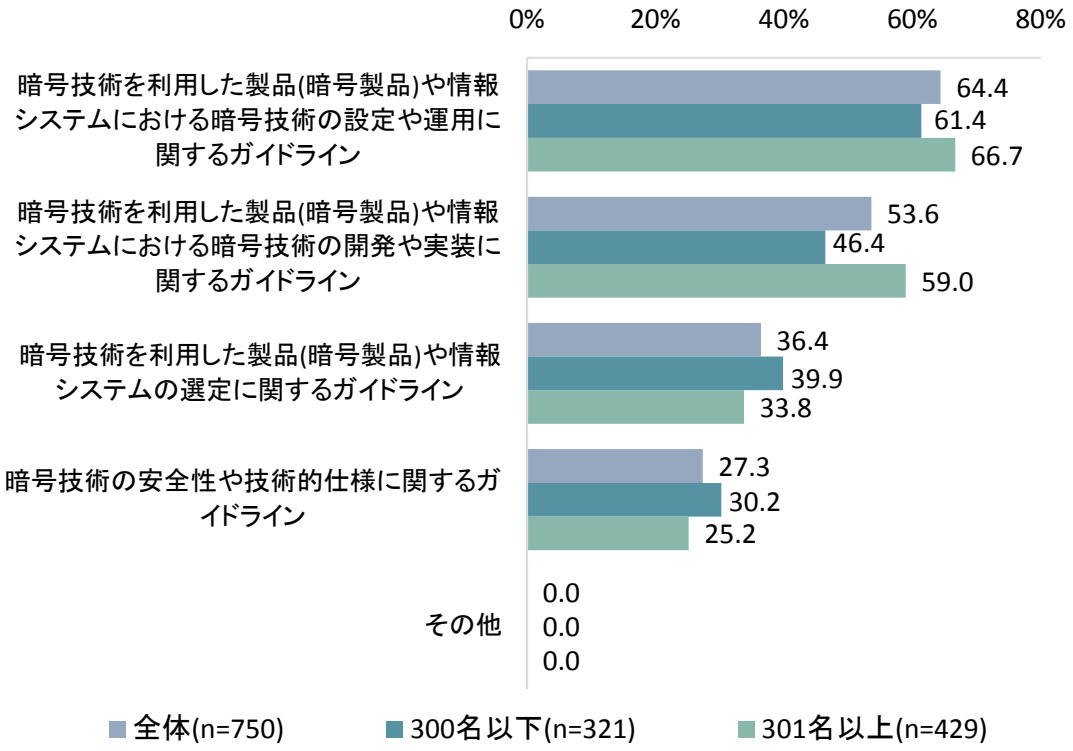


図 2-18　暗号技術に関するガイドラインの種類（複数回答）

ガイドラインの種類について回答者の役職別[8]にみると、「暗号技術を利用した製品（暗号製品）や情報システムにおける暗号技術の設定や運用に関するガイドライン」の割合が何れの役職でも高く、特にシステム・サービス製品開発部門でその割合が高い。

同様の設問について業務経験年数別でみると、「暗号技術を利用した製品（暗号製品）や情報システムにおける暗号技術の開発や実装に関するガイドライン」のニーズは業務経験年数が 5 年～10 年未満で高い。

[8] 役職別のクロス集計について、情報システム部門は「情報システム担当部門の責任者」と「情報システム担当部門の担当者」の回答を合計したものである。情報セキュリティ担当部門、システム・サービス製品の開発も情報システム部門と同様、責任者と担当者の回答を合計している。

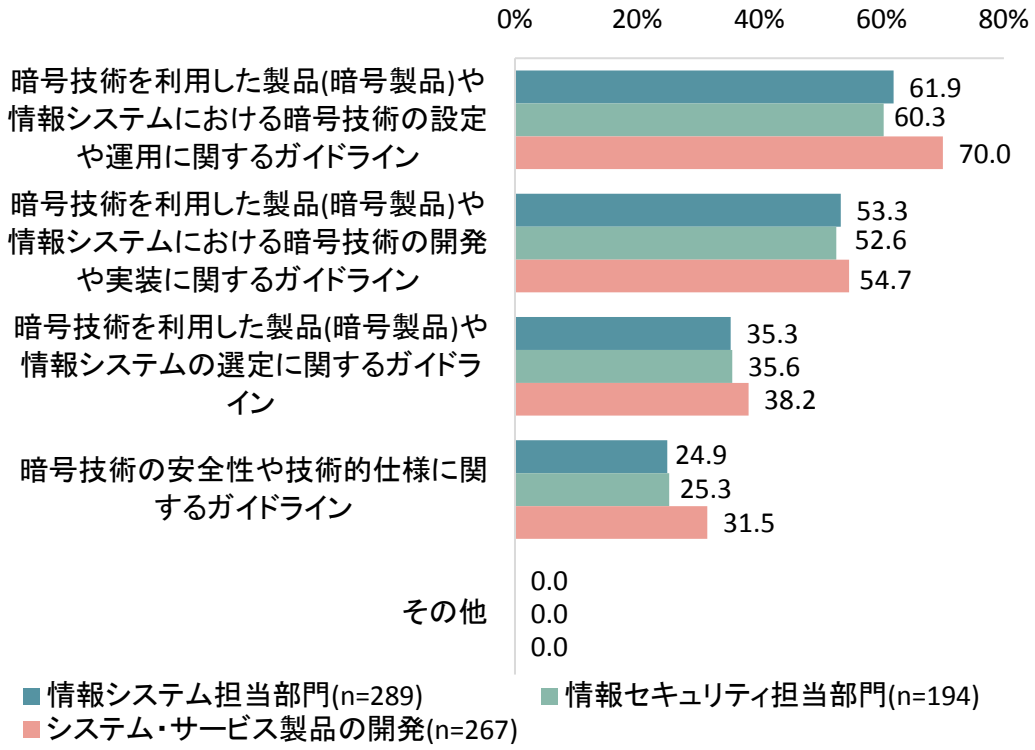


図 2-19 暗号技術に関するガイドラインの種類（役職別・複数回答）

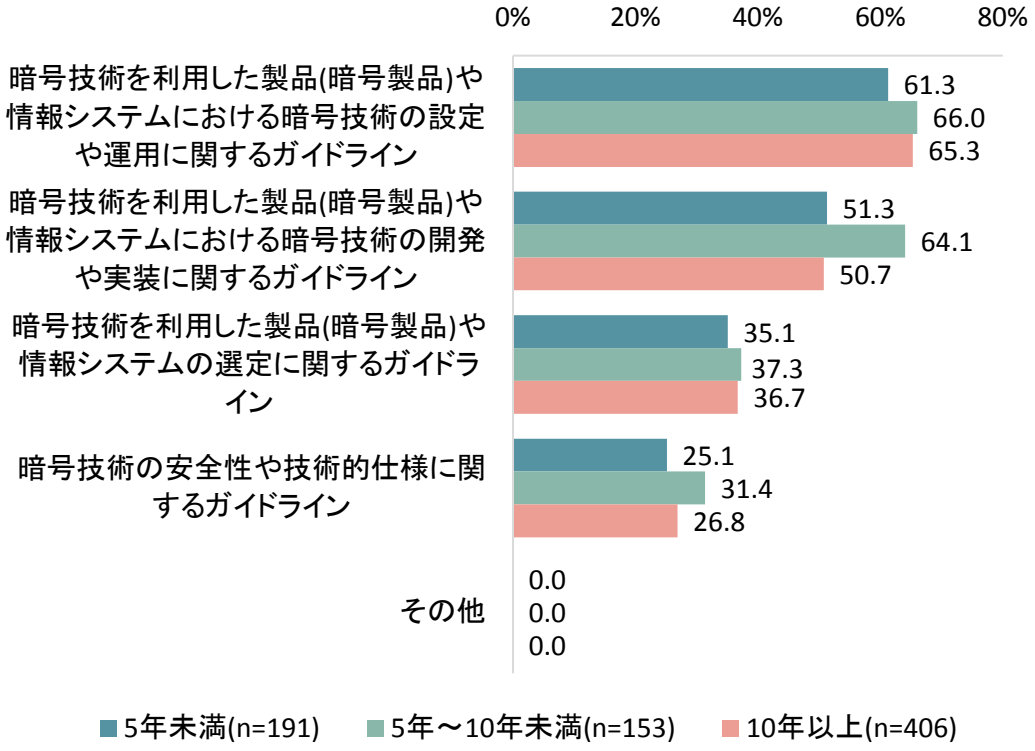


図 2-20　暗号技術に関するガイドラインの種類（業務経験年数別・複数回答）

暗号技術に関するガイドラインを策定する場合、どのようなテーマ（対象）のガイドラインがあるとよいかを確認したところ、大企業（301 名以上）・中小企業（300 名以下）ともに「暗号技術を利用するために必須な暗号鍵の管理（生成・保管・廃棄）」が最も高く、次いで「暗号技術を利用したドキュメントやデータの管理（生成・保管・廃棄）」、「暗号技術を利用したプロトコル（暗号プロトコル　例：SSL/TLS）」の順となっている。

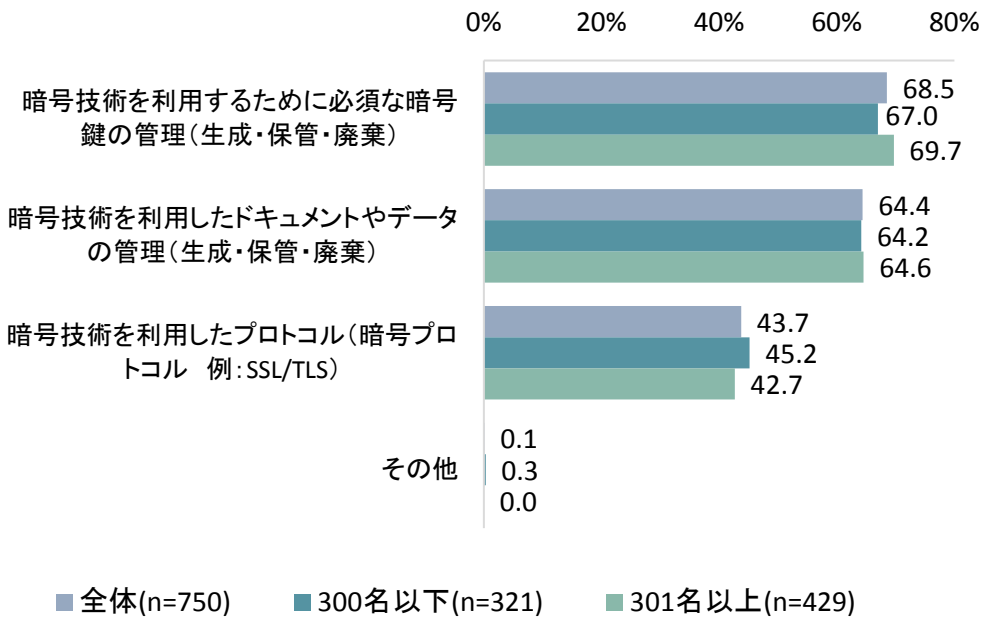


図 2-21　暗号技術に関するガイドラインのテーマ（複数回答）

ガイドラインのテーマについて回答者の役職別・業務経験年数別で回答を比較すると、回答者の役職や業務経験年数による差はあまりない。

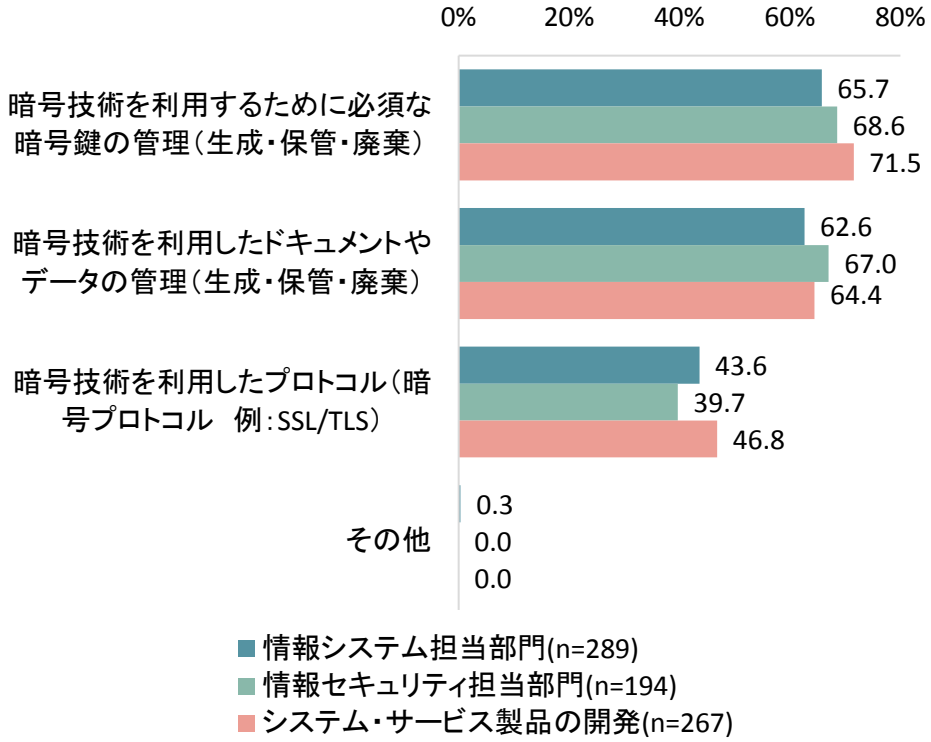


図 2-22　暗号技術に関するガイドラインのテーマ（役職別・複数回答）

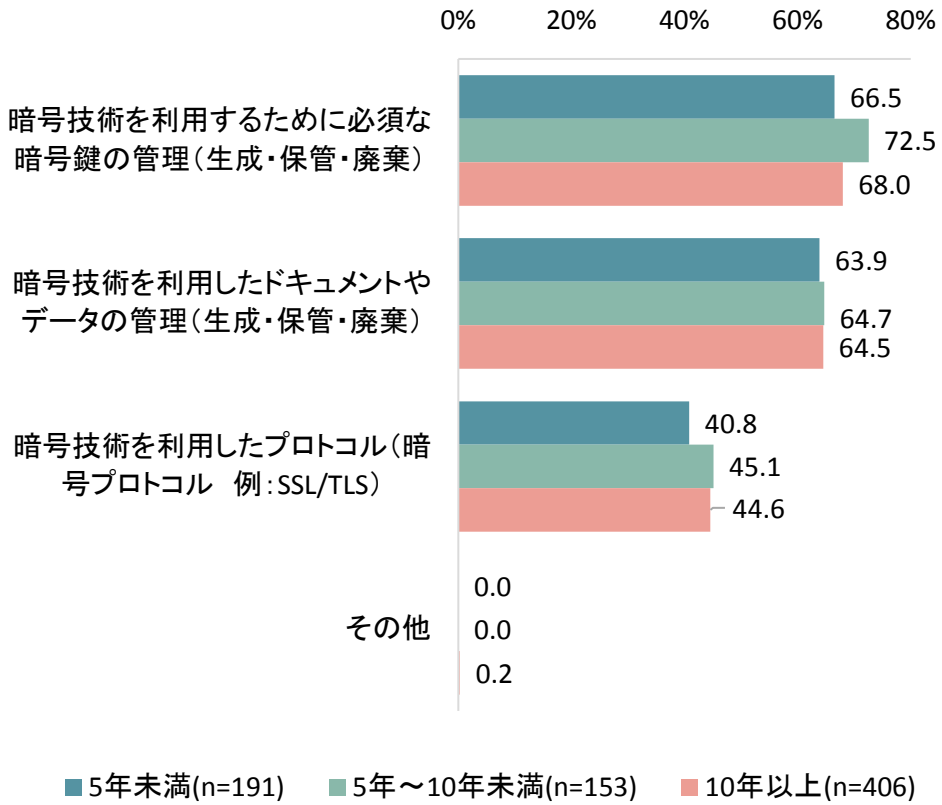


図 2-23　暗号技術に関するガイドラインのテーマ（業務経験年数別・複数回答）

ガイドラインを策定する場合、どのような内容を盛込むとよいか確認したところ、全体では「暗号技術の設定基準や設定方法」（61.6%）が最も高く、「暗号技術の設定に役立つチェックリスト」（56.1%）、「暗号技術の設定基準や設定方法の背景や理由」（45.2%）の順となっている。

企業規模別にみると、中小企業では「暗号技術の設定に役立つチェックリスト」・「暗号技術を利用した具体的な情報システム」・「暗号技術の入門的解説書」を回答する割合が大企業に比べやや高い。また、大企業では、「暗号技術の設定基準や設定方法の背景や理由」を回答する割合が中小企業に比べやや高く、中小企業ではチェックリストや具体的な情報システムの設定方法の例示等、現場で活用しやすい内容が求められていると考えられる。

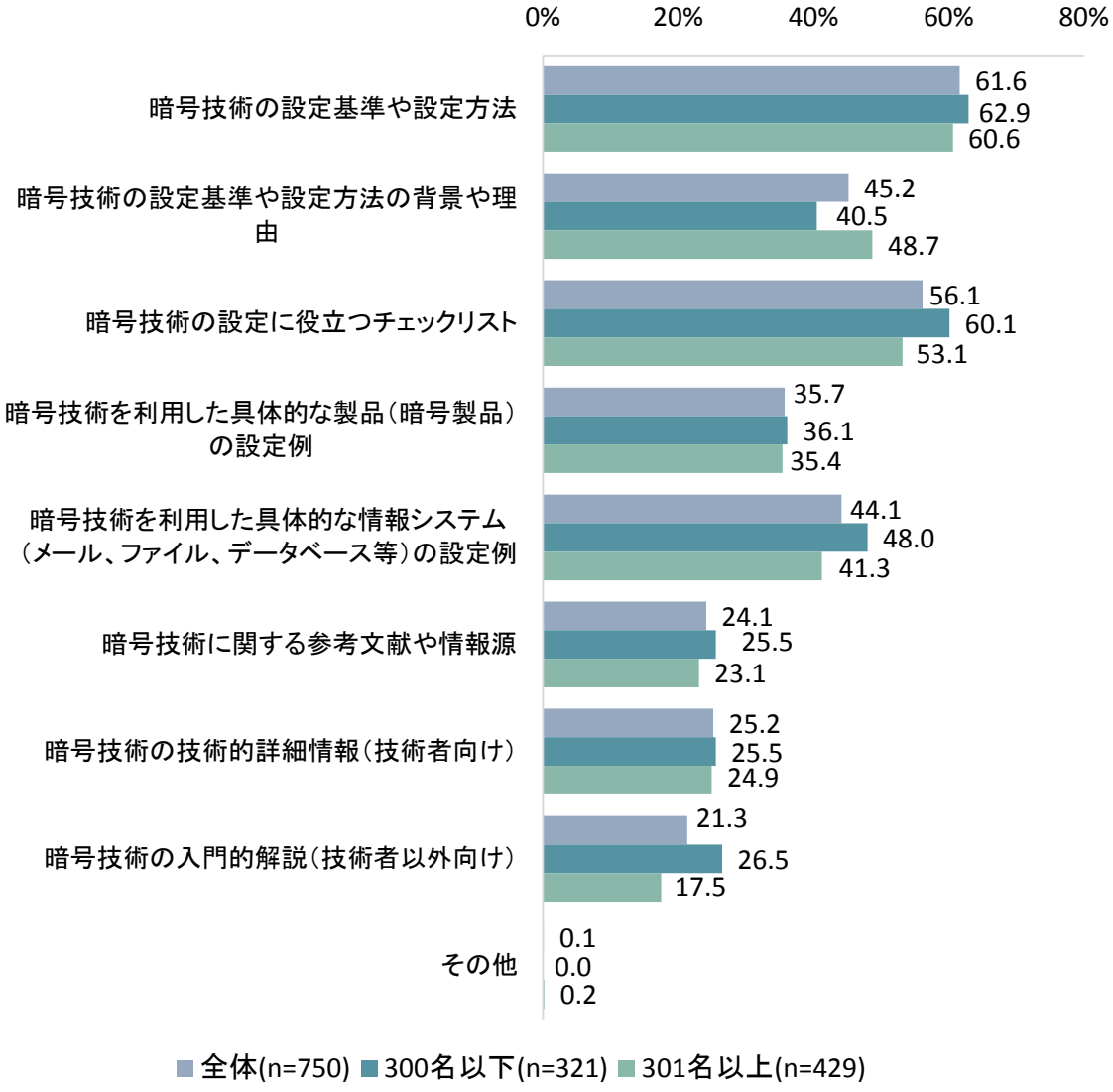


図 2-24　暗号技術に関するガイドラインの内容（複数回答）

同様の設問について役職別にみると、何れの役職でも「暗号技術の設定基準や設定方法」が最も高い。システム・サービス製品の開発部門では、「暗号技術の設定に役立つチェックリスト」や「暗号技術の技術的詳細情報（技術者向け）」が役立つとする回答が他の役職に比べやや高い。

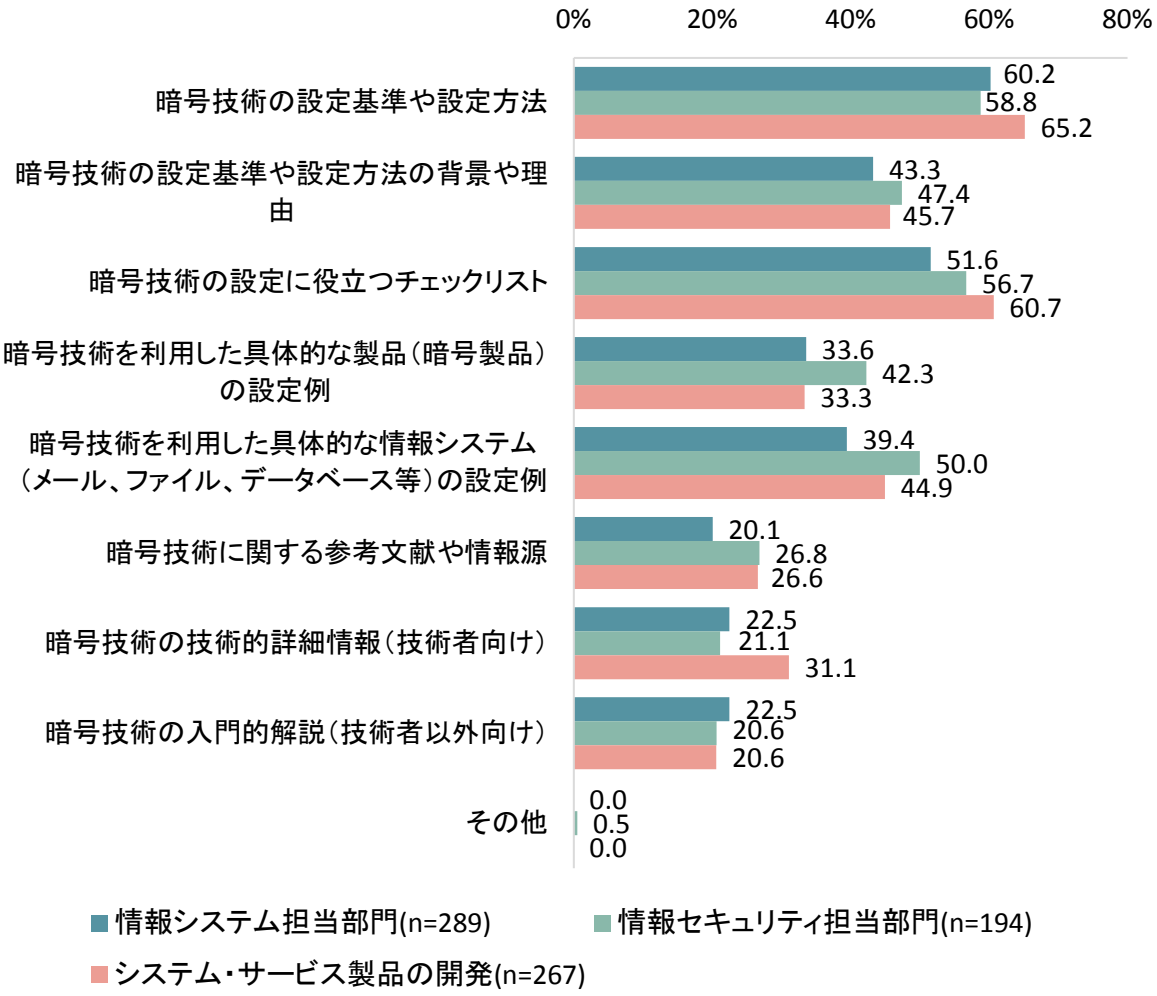


図 2-25　暗号技術に関するガイドラインの内容（役職別・複数回答）

同様の設問について回答者の業務経験年数別にみると、業務経験年数が 5 年以上では「暗号技術の設定基準や設定方法」の割合が高いが、他の項目に関しては業務経験年数により大きな差はなく、業務経験年数で求めるガイドラインの内容に差はない。

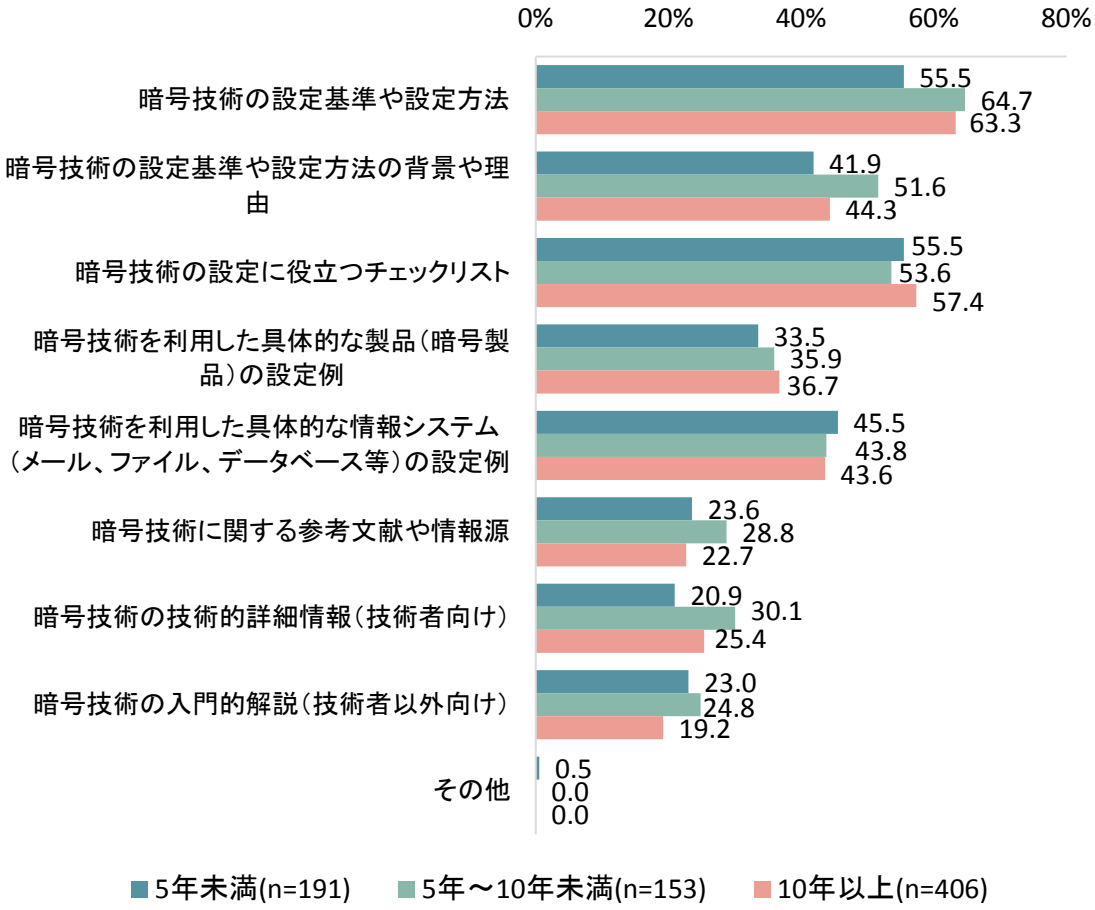


図 2-26　暗号技術に関するガイドラインの内容（業務経験年数別・複数回答）

2.2.7 暗号に関する組織・制度の認知度

暗号に関連する組織・制度である「CRYPTREC」・「CRYPTREC 暗号リスト」・「JCMVP」の認知度を確認したところ、何れも中小企業（300 名以下）に比べ大企業（301 名以上）のほうが認知度は高い。

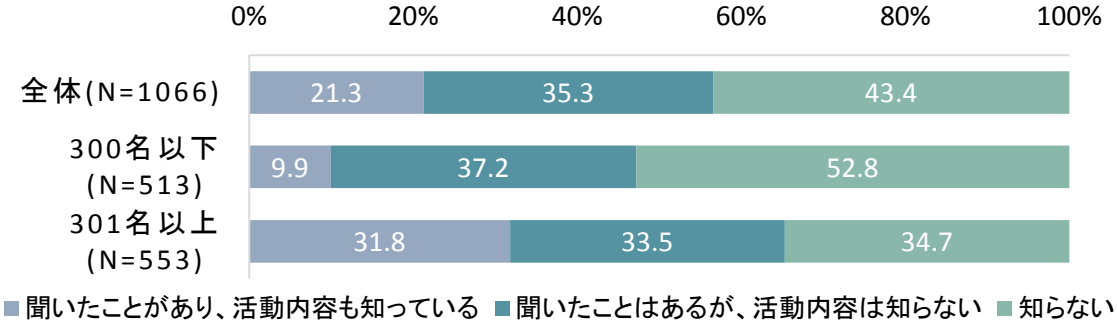


図 2-27　CRYPTREC の認知度

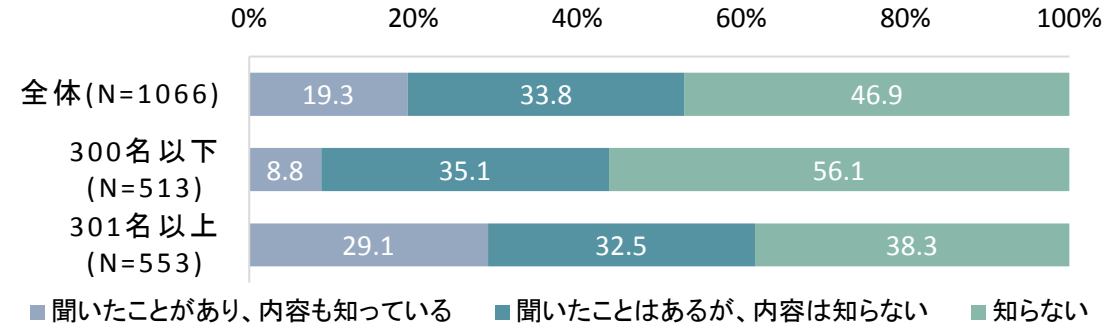


図 2-28　CRYPTREC 暗号リストの認知度

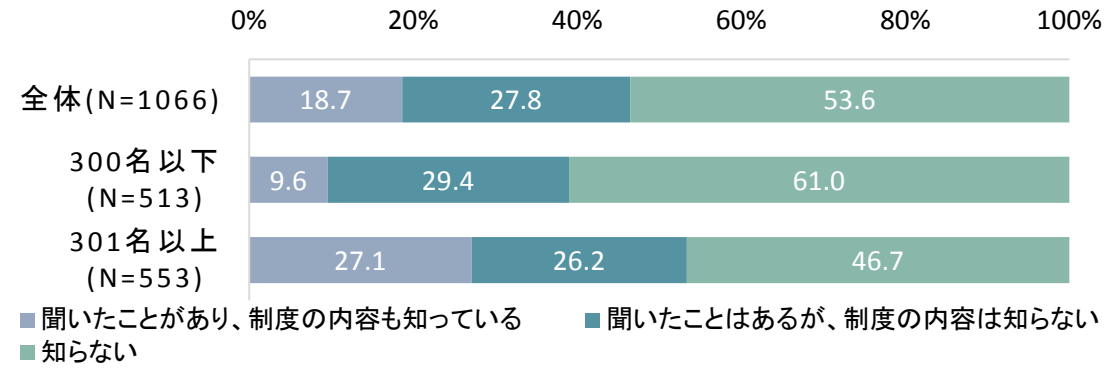


図 2-29　JCMVP の認知度

2.2.8 暗号に関する新技術の認知度

暗号に関する新技術である、「軽量暗号」と「耐量子計算機暗号」の認知度を確認したところ、軽量暗号・耐量子計算機暗号の認知度（「内容は知っており、必要と思う」・「内容を知っているが、必要とは思わない」・「内容は知っているが、必要性についてはわからない」の合計）はともに 3 割程度で、中小企業（300 名以下）に比べ大企業（301 名以上）のほうが認知度は高い。

また、新技術の必要性については、軽量暗号・耐量子計算機暗号ともに 5 割程度が必要（「内容を知っており、必要と思う」と「内容は知らないが、必要と思う」の合計）と回答している。

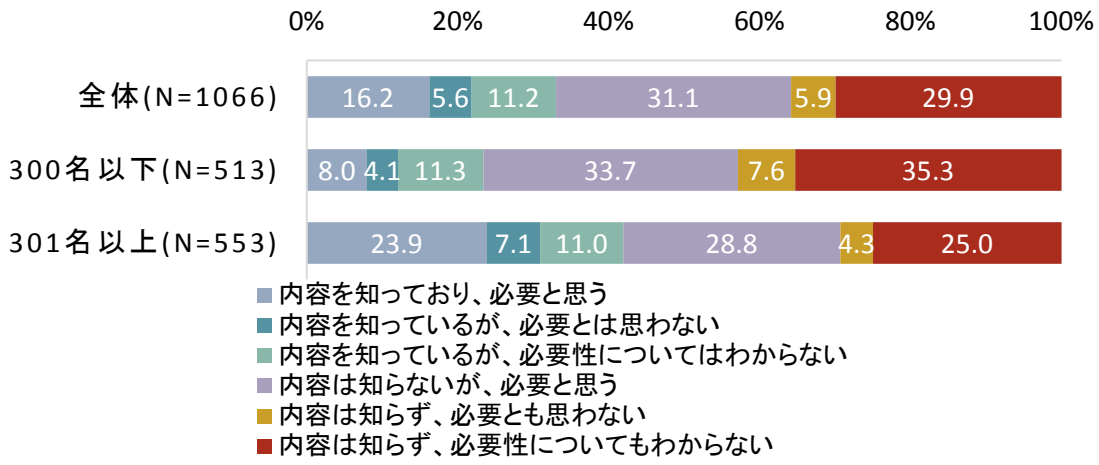


図 2-30　軽量暗号の認知度と必要性

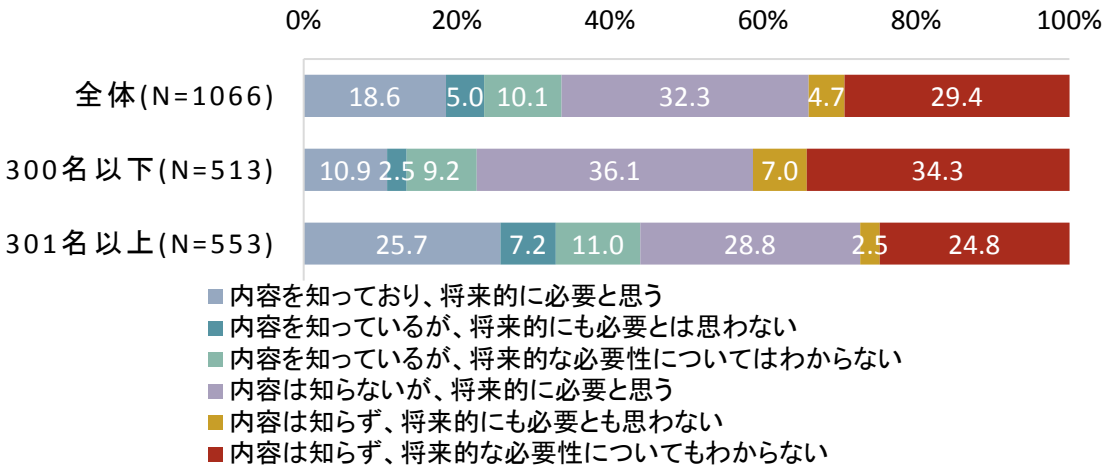


図 2-31　耐量子計算機暗号の認知度と必要性

2.3 考察

アンケート調査より得られた主な分析結果は以下の通りである。

(1) 暗号技術の利活用状況

アンケート調査結果から、中小企業に比べ大企業のほうが暗号製品・技術の利用が進んでいる。そして、大企業ではシステム関連製品の選定・導入・開発時の暗号技術に関する基準や暗号技術の利用・運用基準の整備が中小企業に比べ進んでおり、大企業では暗号技術の利用や基準の整備が進んでいる。

一方で、暗号技術を利用したシステム関連製品の選定・導入時や利用・運用時の課題については企業規模による差はほとんどない。選定・導入時の課題としては、コストをあげる割合が高いが、「どの製品が安全で導入してよいものであるのかがわからない」や「正しくかつセキュアな暗号処理が行われているか、確信が持てない」を課題とする割合も高く、企業の担当者が暗号技術を適切に評価し、導入することを課題として捉えていると考えられる。また、利用・運用時の課題では、「ユーザの利便性と暗号技術の導入によるセキュリティ対策のバランスをとるのが難しい」や「情報システムの暗号に関する部分を適切に運用できる人材がいない」等が課題としてあげられており、暗号の適切な運用が課題となっていると考えられる。

暗号鍵管理に関しては、7 割程度の企業でその必要性は認識されているものの、具体的な対策まで実施している企業は、大企業で約 4 割、中小企業では 15%となっており、特に中小企業での対策が遅れている。また、暗号鍵管理の具体的な方策としては、大企業・中小企業ともに「暗号鍵自体のパスワード等による保護（認証/暗号化）」をあげる割合が高い。

多くの企業で暗号製品・技術が利用されているものの、基準等の体制面の整備は十分に進んでいない。企業の担当者が暗号製品や技術を適切に利活用できるように、暗号利活用に関するガイドライン等を整備し、普及啓発していく必要があると考えられる。

(2) 暗号利活用に関するガイドライン

暗号の利活用に関するガイドラインに関しては、約 7 割が必要と回答しており、ガイドラインに対するニーズはある。

ガイドラインのテーマや内容に関しては、暗号技術の技術的仕様ではなく、暗号製品や技術の設定方法や運用、暗号鍵の管理や暗号技術を利用しドキュメントやデータの管理等、暗号技術の設定基準や設定法等、暗号の利活用に関した内容を求める割合が高い。また、この傾向は、企業規模や回答者の役職、業務経験年数による差はほとんどないことから、企業規模や回答者の属性に関係なく共通のニーズであると考えられる。

今回のアンケート調査結果から、暗号の利活用に関するガイドラインの策定が今後必要になると考えられる。また、ガイドラインに関しては中小企業ではチェックリストや具体的な設定方法、システム・サービスの開発担当者ではチェックリストや技術的詳細情報を求める意見もあり、チェックリスト等企業の担当者が活用しやすいガイドラインの策定を検討する必要があると考えられる。

さらに、暗号技術を利用する際の情報源としては、大企業では政府系機関や情報セキュリティ関連団体、中小企業では IPA の情報を参照している割合が高い。このことから、暗号利活用に関する普及啓発を考えた場合、これらの団体から発信することでより高い効果が得られると考えられる。

(3) 暗号に関連した組織・制度・技術の認知度

暗号に関連した組織・制度である、「CRYPTREC」・「CRYPTREC 暗号リスト」・「JCMVP」の認知度について調査した結果、中小企業に比べ大企業のほうが認知度は高かったが、活動内容まで知っている割合はそれぞれ全体で 2 割程度で認知度は十分ではない。

また、暗号に関する新技術である「軽量暗号」・「耐量子計算機暗号」の認知度は中小企業で 2 割程度、大企業で 4 割程度であった。これら技術の必要性については、5 割程度が必要と回答しており、認知度はまだ低いものの今後必要になると考えられている。

3. 国内外における暗号の利活用に関する文書の調査

3.1 調査概要

以下の事項を明らかにすることを目的に、国内外の組織が作成した暗号の利活用に関する文書の調査を実施した。

- 暗号の利活用の文書に関して国外にあり日本にはない種類（テーマ）の有無
- 暗号の利活用に関する文書間の関係性
- 今後整備すべきガイドラインの対象

3.1.1 調査対象文献の選定

国内外における暗号の利活用に関する文書の調査の実施にあたり、対象とする文書の選定を行った。

本調査で対象とする文書は、日本国内の組織、NIST、ENISA、IETF が発行する暗号の利活用に関する文書とした。なお、本調査における暗号の利活用に関する文書は、暗号に関するフレームワーク、ガイドライン、推奨事項もしくはベストプラクティスについて記載されているものとした。

調査対象となる文書の選定にあたっては、以下の点を考慮した。

- 組織間で横並びに分析することを念頭におき、他組織で列挙した文書と類似するテーマの文書を中心に選定（ハッシュ関数、乱数生成、メッセージ認証、電子署名、鍵管理、IPsec、SSL/TLS）
- アンケート結果との比較分析を念頭におき、IT 担当者を想定読者とした文書を選定

調査対象とした文書の件数を表 3-1 で示す。

表 3-1　調査文書の件数

発行組織	調査件数・選定基準
日本国内の組織	暗号の利活用に関する文書 14 件
NIST	SP800 シリーズ及び SP1800 シリーズの中から暗号技術が関係する文書 30 件
ENISA	暗号の利活用に関する文書 5 件
IETF	RFC の中から暗号の利活用に関する文書 10 件 特に暗号プロトコル、暗号アルゴリズム、鍵長等の選択に関する文書を含む

調査対象とした文書の一覧を表 3-2、表 3-3、表 3-4、表 3-5 で示す。

選定した文書の中には、IT 担当者向け以外の文書も含まれるが、暗号技術の使用方法・選択方法等が記載されており、IT 担当者にも参考になると考えられる。

表 3-2　日本国内の組織が発行する文書

発行組織	タイトル
IPA/CRYPTREC	SSL/TLS 暗号設定ガイドライン
IPA	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）
IPA	情報漏えいを防ぐためのモバイルデバイス等設定マニュアル～安心・安全のための暗号利用法～
CRYPTREC	CRYPTREC 暗号技術ガイドライン(SHA-1)
CRYPTREC	2008 年度版リストガイド（秘匿の暗号利用モード）
CRYPTREC	2008 年度版リストガイド（メッセージ認証コード）
CRYPTREC	2008 年度版リストガイド（電子署名）
CRYPTREC	2010 年度版リストガイド（鍵管理）
CRYPTREC	2011 年度版リストガイド（SSL/TLS）
CRYPTREC	2011 年度版リストガイド（IPsec）
CRYPTREC	2011 年度版リストガイド（DNSSEC）
日本コンピュータセキュリティインシデント対応チーム協議会	SSH サーバセキュリティ設定ガイド
データベース・セキュリティ・コンソーシアム	データベース暗号化ガイドライン
JEITA	テープストレージの暗号化機能に関するチェックリスト

表 3-3　NIST が発行する文書

発行組織	番号	タイトル
NIST	SP 800-22 Rev. 1a	A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications
NIST	SP 800-52 Rev. 1	Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
NIST	SP 800-57 Part 1 Rev. 4	Recommendation for Key Management, Part 1: General
NIST	SP 800-57 Part 2	Recommendation for Key Management, Part 2: Best Practices for Key Management Organization
NIST	SP 800-57 Part 3 Rev. 1	Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance
NIST	SP 800-63-3	Digital Identity Guidelines
NIST	SP 800-63B	Digital Identity Guidelines: Authentication and Lifecycle Management
NIST	SP 800-77	Guide to IPsec VPNs

発行組織	番号	タイトル
NIST	SP 800-78-4	Cryptographic Algorithms and Key Sizes for Personal Identity Verification
NIST	SP 800-81-2	Secure Domain Name System (DNS) Deployment Guide
NIST	SP 800-88 Rev. 1	Guidelines for Media Sanitization
NIST	SP 800-89	Recommendation for Obtaining Assurances for Digital Signature Applications
NIST	SP 800-90A Rev. 1	Recommendation for Random Number Generation Using Deterministic Random Bit Generators
NIST	SP 800-90B (Draft)	Recommendation for the Entropy Sources Used for Random Bit Generation
NIST	SP 800-90C (Draft)	Recommendation for Random Bit Generator (RBG) Constructions
NIST	SP 800-97	Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i
NIST	SP 800-102	Recommendation for Digital Signature Timeliness
NIST	SP 800-106	Randomized Hashing for Digital Signatures
NIST	SP 800-111	Guide to Storage Encryption Technologies for End User Devices
NIST	SP 800-113	Guide to SSL VPNs
NIST	SP 800-130	A Framework for Designing Cryptographic Key Management Systems
NIST	SP 800-131A Rev. 1	Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths
NIST	SP 800-132	Recommendation for Password-Based Key Derivation: Part 1: Storage Applications
NIST	SP 800-133	Recommendation for Cryptographic Key Generation
NIST	SP 800-135 Rev. 1	Recommendation for Existing Application-Specific Key Derivation Functions
NIST	SP 800-152	A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS)
NIST	SP 800-175A	Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies
NIST	SP 800-175B	Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
NIST	SP 800-177	Trustworthy Email
NIST	SP 1800-6B (Draft)	Domain Name Systems-Based Electronic Mail Security: Approach, Architecture, and Security Characteristics

表 3-4　ENISA が発行する文書

発行組織	タイトル
ENISA	Algorithms, key size and parameters report 2014
ENISA	The Use of Cryptographic Techniques in Europe
ENISA	Recommended cryptographic measures - Securing personal data
ENISA	Study on cryptographic protocols
ENISA	Standardisation in the field of Electronic Identities and Trust Service Providers

表 3-5　IETF が発行する文書

発行組織	番号	タイトル
IETF	RFC2504	Users' Security Handbook
IETF	RFC4086	Randomness Requirements for Security
IETF	RFC4107	Guidelines for Cryptographic Key Management
IETF	RFC4513	Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms
IETF	RFC4641	DNSSEC Operational Practices
IETF	RFC4894	Use of Hash Algorithms in Internet Key Exchange (IKE) and IPsec
IETF	RFC4962	Guidance for Authentication, Authorization, and Accounting (AAA) Key Management
IETF	RFC6518	Keying and Authentication for Routing Protocols (KARP) Design Guidelines
IETF	RFC7520	Examples of Protecting Content Using JSON Object Signing and Encryption (JOSE)
IETF	RFC7525	Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)

3.1.2 個別文献調査の方針

選定したそれぞれの文書に関し、以下の観点で精査を行い、概要をまとめた。

- 発行年、文書のバージョン番号
- 発行機関
- 対象読者
- 文書の位置づけ（法的な遵守義務があるかなどを含む）
- 文書の種類及びテーマ
- 他の文書との関係

なお、本調査では文書の種類を以下の通り分類分けした。

- 暗号の開発実装に関連する文書
- 暗号に関して運用・設定に関する文書（特に暗号プロトコルに関するもの）
- 暗号に関して運用・設定に関する文書（暗号プロトコル以外に関するもの）
- 暗号を利用したシステムの運用もしくはマネジメントに関する文書
- 特定の製品・サービスの利用に関する文書

3.1.3 文書の比較分析方針

個別に内容を精査した後、以下の観点から各々の文書について分析を実施した。

(1) 文書の種類の傾向

組織ごとに文書の種類（3.1.2 で示す 5 つの分類）の傾向を分析。

(2) 類似するテーマの文書間の関係性

同一組織内において類似するテーマの文書がある場合、類似するテーマの文書間の関係性・違いを分析。

(3) 国外と比較したガイドラインの整備状況

国外の各組織間と国内におけるガイドラインの整備状況について分析し、結果を取りまとめることで暗号の利活用の文書に関して国外にあって日本にはない種類・テーマの有無を明らかにした。

比較分析にあたっては、縦軸をテーマ、横軸を組織名とした星取表を作成し、国外と日本におけるガイドラインの整備状況の違いを分析した。

(4) ユーザのニーズと現在のガイドライン等の文書整備状況を比較

アンケート結果と文献調査結果について、ユーザのニーズと現在のガイドライン等の文書整備状況を比較し、分析を実施した。この観点については 5 まとめに結果を記述する。

3.2 調査結果

3.2.1 個別文献調査

個別文献調査では、選定した 59 件の文書を調査し、各々の文書について要旨を 1 ページ以内にまとめた。各文書の調査結果については、付録 2　国内外における暗号の利活用に関する文書の調査結果詳細にまとめた。

文献調査結果の例として、IPA/CRYPTREC 発行「SSL/TLS 暗号設定ガイドライン」、NIST 発行 SP 800-52 Rev. 1 “Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations”、IETF 発行“Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)”をそれぞれ表 3-6、表 3-7、表 3-8 に示す。

表 3-6　IPA/CRYPTREC 発行「SSL/TLS 暗号設定ガイドライン」

題名	SSL/TLS 暗号設定ガイドライン
対象読者	SSL/TLS サーバを実際に構築するにあたって具体的な設定を行うサーバ構築者、実際のサーバ管理やサービス提供に責任を持つことになるサーバ管理者、並びに SSL/TLS サーバの構築を発注するシステム担当者
策定年・ 文書のバージョン番号	2015 年 8 月 Ver.1.1
発行機関	CRYPTREC (Cryptography Research and Evaluation Committees)・IPA（情報処理推進機構）
言語	日本語
文書の種類・テーマ	暗号に関して運用・設定する文書（特に暗号プロトコルに関するもの） 対象読者が適切なセキュリティを考慮した暗号設定ができるようにするためのガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	IPA 発行「安全なウェブサイトの作り方」とともに適切な暗号設定をする資料の 1 つとして使用することができる。 NISC 発行「政府機関等の情報セキュリティ対策のための統一基準群」で参照するように求められている。
概要	SSL/TLS 通信での安全性と可用性（相互接続性）のバランスを踏まえた SSL/TLS サーバの設定方法を説明したガイドライン。 「暗号技術以外の様々な利用上の判断材料も加味した合理的な根拠」を重視し、実現すべき安全性と必要となる相互接続性とのトレードオフを踏まえたうえで、実際に設定すべき「要求設定項目」として 3 つの設定基準（「高セキュリティ型」「推

	奨セキュリティ型」「セキュリティ例外型」）を提示。 第 1 章と第 2 章において、本ガイドラインの目的や SSL/TLS についての技術的な基礎知識をまとめたうえで、第 3 章で SSL/TLS サーバに要求される設定基準の概要について説明。 第 4 章から第 6 章では、第 3 章で定めた設定基準に基づき、プロトコルバージョン、サーバ証明書、暗号スイートについての具体的な SSL/TLS サーバの要求設定項目について示している。付録には、4 章から 6 章までの設定状況を確認するためのチェックリストが掲載されており、「選択した設定基準に対応した要求設定項目の設定忘れの防止」と「サーバ構築の作業受託先が適切に要求設定項目を設定したことの確認」を行うために利用できるように作られている。
目次	1. はじめに 2. 本ガイドラインの理解を助ける技術的な基礎知識 3. サーバ構築における設定要求項目について 4. プロトコルバージョンの設定 5. サーバ証明書の設定 6. 暗号スイートの設定 7. SSL/TLS を安全に使うために考慮すべきこと 8. ブラウザを利用する際に注意すべきポイント 9. その他のポイント 付録（チェックリスト、サーバ設定編、暗号スイートの設定例、ルート CA 証明書の取扱い）
URL	https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html

表 3-7　NIST 発行「SP 800-52 Rev. 1“Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations”」

題名	SP 800-52 Rev. 1 “Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations”
対象読者	主に連邦政府利用者及びシステム管理者
策定年・ 文書のバージョン番号	2014 年 4 月 Rev. 1
発行機関	NIST (National Institute of Standards and Technology)
言語	英語
文書の種類・テーマ	暗号に関して運用・設定する文書（暗号プロトコルに関するもの） TLS 実装の選択、設定及び使用のためのガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	TLS 実装には公開鍵証明書を生成する公開鍵基盤の存在を必要としており、これに関して SP 800-32 “Introduction to Public Key Technology and the Federal PKI Infrastructure”を参照すべきとし、RSA などの鍵生成に関するガイダンスについては SP 800-56A Rev.1 “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”を参照するよう書かれている。また、クライアント公開鍵証明書で提示される鍵長に関しては、SP 800-131A Rev1 “Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths” で提供される鍵長ガイドラインを使用しなければならないとしている。
概要	承認された暗号運用とアルゴリズムを効果的に使用する際の TLS 実装の選択及び設定について、サーバとクライアント別に要求事項をまとめたガイドライン。 TLS1.1 を最低限適切なセキュアトランスポートプロトコルとし、承認された運用とアルゴリズムを用いた暗号スイートを設定することを要求。さらに、2015 年 1 月 1 日までに TLS1.2 への移行計画を政府機関が策定することも推奨している。 TLS サーバの最小限要求事項については、「サーバ選択の推奨事項」・「サーバのインストール設定のための推奨事項（バージョンサポート、証明書、暗号サポート、拡張、クライアント認証、セッション再開、圧縮方法、運用上の検討事項）」・「サーバシステム管理者のための推奨事項（バージョンサポート、証明書、暗号サポート、クライアント認証、運用上の検討事項）」の 3 分類で各分類における要求事項・推奨事項を整理している。

	第 4 章では TLS クライアントの最小限要求事項について、「クライアント選択の推奨事項」・「クライアントのインストールと設定のための推奨事項（バージョンサポート、証明書、暗号サポート、拡張、サーバ認証、セッション再開、圧縮モード）」・「クライアントシステム管理者のための推奨事項（バージョンサポート、証明書、サーバ認証、運用上の検討事項）」・「エンドユーザのための推奨事項」の 4 分類で各分類における要求事項・推奨事項を整理している。 同ガイドラインの要求事項を満たすことにより、以下の内容が促進されるとしている： 1. インターネット上の情報配送保護のための、認証、機密性及び完全性のより一貫した使用 2. NIST 承認されたアルゴリズム及び公開標準を含む推奨暗号スイートの一貫した使用 3. TLS プロトコル上の既知及び想定される攻撃に対する保護 4. トランスポート層のセキュリティ実装の統合におけるシステム管理者や管理者（マネージャー）による十分な情報を得たうえでの決定
目次	1. 序説 2. TLS 概要 3. TLS サーバの最小限要求事項 4. TLS クライアントの最小限要求事項 付録 A 略語 付録 B 暗号スイート名の解釈 付録 C 事前共有鍵 付録 D 将来の機能 付録 E 参考文献
URL	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf https://www.ipa.go.jp/files/000057084.pdf （IPA による翻訳版）

表 3-8　IETF 発行「RFC7525” Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)”」

題名	RFC7525” Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)”
対象読者	TLS/DTLS 通信における認証（片方向もしくは相互）、機密性、データ完全性の保護を行いたいと考えているシステム開発者
策定年・ 文献のバージョン番号	2015 年 5 月 初版
発行機関	IETF (Internet Engineering Task Force)
言語	英語
文書の種類・テーマ	暗号の開発実装に関連する文書、及び暗号に関して運用・設定に関する文書（特に暗号プロトコルに関するもの） TLS と DTLS のセキュリティを改善する推奨事項を提供するガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	RFC 7457 “ Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS)”は本文書の付随文書で、TLS と DTLS に対する攻撃の理解と、本文書の推奨事項の根拠を理解するための文書。 暗号アルゴリズムに関する推奨事項は RFC 7465“ Prohibiting RC4 Cipher Suites”、RFC 3766“ Determining Strengths For Public Keys Used For Exchanging Symmetric Keys”を参照。
概要	TLS と DTLS を使用する際の推奨事項を明記した文書。本文書はベストカレントプラクティスで、TLS1.3 の仕様では、この文書に記載されている多くの脆弱性が解決される予定であるとしている。 第 3 章では、プロトコルのバージョン、 HTTP Strict Transport Security (HSTS)、データ圧縮、TLS セッション再開、TLS 再ネゴシエーション、サーバ名表示（SNI）といった TLS の仕様に関する一般的な推奨事項が示されている。各事項は、「必須」、「禁止」、「推奨」、「非推奨」、「任意」に分類され、その根拠が明記されている。 第 4 章では暗号スイートに関する推奨事項について述べており、使用を禁止する暗号スイート、使用を推奨する暗号スイートとその実装方法、推奨される暗号鍵長を説明している。 第 5 章では、本文書の推奨事項がどのようなシステムやサービスにおいて適用されるべきかが明記されており、第 6 章では、TLS に関連したより幅広いセキュリティの考慮事項が説明されている。

目次	1. 序説 2. 用語 3. 一般的な推奨事項 4. 暗号スイートに関する推奨事項 5. 適用性事項 6. セキュリティに関する考慮事項 7. 参考文献
URL	https://tools.ietf.org/html/rfc7525

3.2.2 文献の比較分析

(1) 文書の種類の傾向

本調査で対象とした文書のうち、各組織が発行する種類ごとの文書数を表 3-9 で示す。

表 3-9 をみると本調査の範囲内では、日本国内の組織が発行する文書としては「暗号に関して運用・設定に関する文書（特に暗号プロトコルに関するもの）」が 14 件中 5 件と多い。また、NIST が発行する文書では「暗号に関して運用・設定に関する文書（暗号プロトコル以外に関するもの）」が 30 件中 15 件となっている。

ENISA が発行する文書に関しては「暗号に関して運用・設定に関する文書（暗号プロトコル以外に関するもの）」が多い。ただし、「暗号に関して運用・設定に関する文書（暗号プロトコル以外に関するもの）」の文書 4 件のうち 2 件は「暗号を利用したシステムの運用もしくはマネジメントに関する文書」にも分類され、比較的運用・マネジメントを目的とした文書である。また、IETF が発行する文書は「暗号の開発実装に関連する文書」が 10 件中 6 件となっている。

表 3-9　各組織が発行する種類ごとの文書数

	日本国内の組織 全 14 件	NIST 全 30 件	ENISA 全 5 件	IETF 全 10 件
暗号の開発実装に関連する文書	3 件	12 件	0 件	6 件(1)
暗号に関して運用・設定に関する文書（特に暗号プロトコルに関するもの）	5 件	8 件(6)	1 件	4 件(3)
暗号に関して運用・設定に関する文書（暗号プロトコル以外に関するもの）	3 件	15 件(7)	4 件(2)	1 件(1)
暗号を利用したシステムの運用もしくはマネジメントに関する文書	3 件(1)	6 件(5)	2 件(2)	2 件(1)
特定の製品・サービスの利用に関する文書	1 件(1)	4 件(3)	0 件	0 件

※括弧内は 2 種類以上の分類にあてはまる文書の数

(2) 類似するテーマの文書間の関係性

同一組織が発行する類似テーマの文書に関して、文書間の関係性・違いを以下で説明する。

1) NIST 発行「鍵管理」に関する文書

NIST が発行する「鍵管理」に関する文書は、本調査の対象文書内で計 14 件あった。

鍵管理に関する文書について、その内容を表 3-10 に示す。

表 3-10　NIST が発行する「鍵管理」に関する文書間の関係性

番号	タイトル	内容
SP 800-57 Part 1 Rev. 4	Recommendation for Key Management, Part 1: General	基本的な鍵管理に関する推奨事項を提供する文書。鍵の生成、使用、及び最終的な破棄について解説。
SP 800-57 Part 2	Recommendation for Key Management, Part 2: Best Practices for Key Management Organization	米国政府機関向けの方針及びセキュリティ計画の要求事項に関するガイドライン。セキュリティプランの要件、一般のセキュリティ方針と鍵管理に関する施策の必要性を明示。
SP 800-57 Part 3 Rev. 1	Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance	システムの暗号機能を使用する際の推奨事項を提供。公開鍵基盤及びプロトコル、アプリケーションにおける鍵管理について解説。
SP 800-81-2	Secure Domain Name System (DNS) Deployment Guide	DNSSEC の機能の 1 つとして鍵管理に関する推奨事項を記載。
SP 800-89	Recommendation for Obtaining Assurances for Digital Signature Applications	電子署名に必要な保証を得る方法として鍵管理に関する推奨事項を記載。
SP 800-97	Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i	IEEE 802.11i を実装する際の鍵管理について推奨事項を記載。
SP 800-111	Guide to Storage Encryption Technologies for End User Devices	エンドユーザ端末のストレージ暗号化について計画・実装及び保守を支援するための文書。ストレージ暗号化に関連して鍵管理について解説。
SP 800-130	A Framework for Designing Cryptographic Key Management Systems	暗号鍵管理システムを設計するためのフレームワークに関する文書。
SP 800-131A Rev. 1	Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths	SP 800-57 に基づき、2010 年頃の暗号解読に関する研究の進展状況を踏まえ、詳細な移行計画を示す文書。
SP 800-133	Recommendation for Cryptographic Key Generation	暗号鍵の生成手順・アルゴリズムについて説明した文書。
SP 800-152	A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS)	鍵管理システムの設計者及び実装者が、「製品」で提供される機能を選択することを支援するため、また、連邦機関とその請負業者が連邦鍵管理システムを調達、インストール、設定、運用及び使用することを支援するための文書。

番号	タイトル	内容
SP 800-175B	Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms	連邦政府の機密情報保護に利用できる暗号手法とサービス、NIST の暗号標準の概要を説明したガイドライン。暗号アルゴリズムを紹介したうえでそれらのアルゴリズムを使用する際の暗号鍵の保護と管理について説明し、鍵生成・導出・共有・伝送といった鍵確立メカニズムに関しても解説。
SP 1800-6B (Draft)	Domain Name Systems-Based Electronic Mail Security: Approach, Architecture, and Security Characteristics	DNS システムベースの E メールのセキュリティ設定に関するガイドライン。証明書に基づく鍵管理について解説。

表 3-10 で整理した NIST が発行する「鍵管理」に関する 14 件の文書を、内容ごとに分類したものが図 3-1 である。

鍵管理に特化した文書と、鍵管理以外の技術についても記載する文書に分かれ、鍵管理に特化した文書の中でも、運用面のガイドラインとシステム面のガイドラインが存在する。また、鍵管理以外の技術についても記載する文書は、一般技術における鍵管理の応用について説明する文書と、暗号技術の 1 つとして鍵管理の機能について触れる文書が存在し、NIST では様々な視点から鍵管理に関する文書を発行している。

図 3-1 NIST が発行する「鍵管理」に関する文書間の関係性

2) NIST 発行「電子署名」に関する文書

NIST が発行する「電子書名」に関する文書は、本調査の対象文書内で計 9 件あった。電子署名に関する文書について、文書の内容を表 3-11 に示す。

表 3-11　NIST が発行する「電子書名」に関する文書間の関係性

番号	タイトル	内容
SP 800-81-2	Secure Domain Name System (DNS) Deployment Guide	DNS のセキュリティを保護するための文書。DNSSEC の機能の 1 つとして電子署名アルゴリズムに関する推奨事項を記載。

番号	タイトル	内容
SP 800-89	Recommendation for Obtaining Assurances for Digital Signature Applications	有効な電子署名に必要な保証を得る方法について推奨事項を記載。
SP 800-102	Recommendation for Digital Signature Timeliness	電子署名が生成された時刻を保証するための方法を記載した文書。
SP 800-106	Randomized Hashing for Digital Signatures	電子署名を生成する際に、メッセージをランダム化する手法を提供する文書。
SP 800-131A Rev. 1	Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths	SP 800-57 に基づき、2010 年頃の暗号解読に関する研究の進展状況を踏まえて詳細な移行計画を示す文書。電子署名のアルゴリズムについて強度を評価。
SP 800-133	Recommendation for Cryptographic Key Generation	暗号鍵の生成手順・アルゴリズムについて説明した文書。電子署名を利用する場合の鍵の生成に関する考慮すべき事項を記載。
SP 800-175B	Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms	連邦政府の機密情報保護に利用できる暗号手法とサービス、NIST の暗号標準の概要を説明したガイドライン。電子署名に使用されるべき暗号アルゴリズムを説明。
SP 800-177	Trustworthy Email	E メールの信頼性を向上させるためのプロトコルや技術の推奨事項の概要を記載。推奨事項の 1 つに電子署名を含む。
SP 1800-6B (Draft)	Domain Name Systems-Based Electronic Mail Security: Approach, Architecture, and Security Characteristics	DNS システムベースの E メールのセキュリティ設定に関するガイドライン。設定要素の 1 つに電子署名を示す。

表 3-10 で整理した NIST が発行する「電子署名」に関する 14 件の文書を、内容ごとに分類したものが図 3-2 である。

電子署名に特化した文書と、電子署名以外の技術についても記載する文書に分かれている。電子署名に特化した文書は、運用面のガイドラインとなっており、保証内容で文書が分かれている。また、電子署名以外の技術についても記載する文書は、一般技術における電子署名の応用について述べる文書と、電子署名の基礎技術について述べる文書、暗号技術の 1 つとして電子署名について説明する文書が存在する。NIST では様々な視点から電子署名に関する文書を発行している。

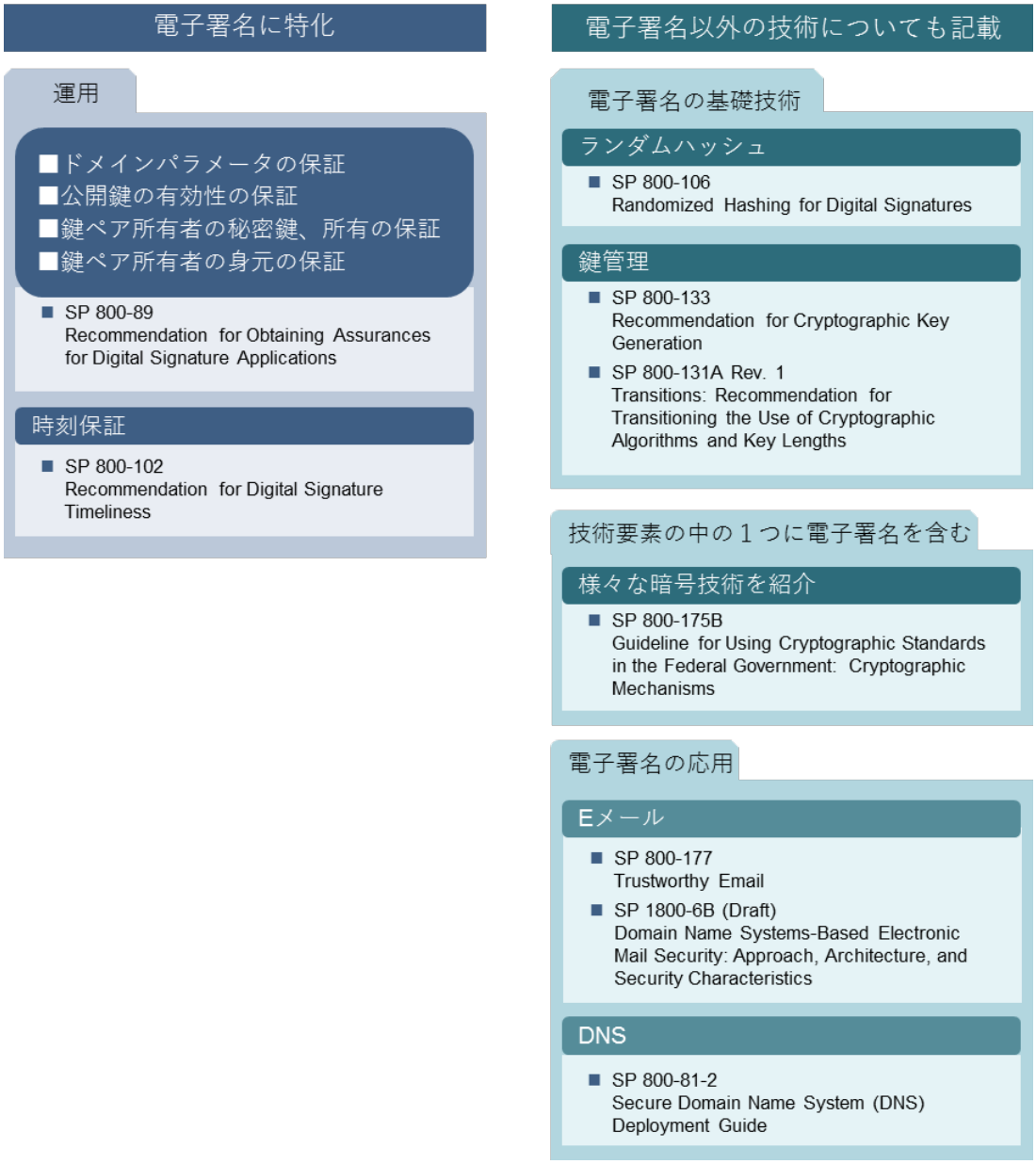


図 3-2 NIST が発行する「電子書名」に関する文書間の関係性

(3) 国外と比較したガイドラインの整備状況

国外の各組織間と国内における暗号利活用の文書の整備状況について整理し、国外にあって日本にはない種類・テーマの有無を明らかにするために、縦軸をテーマ、横軸を組織とする星取表を作成した。

表 3-12　各組織における文書の整備状況

	発行組織	日本国内の組織	NIST	ENISA	IETF
暗号技術（分類）	共通鍵暗号	△	○	○	△
	公開鍵暗号	△	○	○	△
	ハッシュ関数	○	○	○	△
	利用モード	○		○	
	鍵導出関数		○	○	
	乱数生成		○	○	○
署名・認証	メッセージ認証	○	○	○	△
	電子署名	○	○	○	△
	電子認証		○		
	送信ドメイン認証		△		
	トラストサービス			○	
	公開鍵基盤（PKI）		○		
暗号の利用方法	鍵管理	○	○	○	○
	鍵ラップ		○	○	□
	鍵のサイズ	△	○	○	△
	鍵共有	△	○	□	□
暗号プロトコル等	IPsec	○	○	○	○
	SSL/TLS	○	○	○	○
	SSH	○	□	○	△
	Kerberos		□	○	□
	SRTP		□		
	DNSSEC	○	○		○
	認証プロトコル		△	○	
	鍵交換プロトコル			○	
	無線 LAN		○	○	
	E メールで使われる暗号化プロトコル（S/MIME・PGP 等）		△		△
その他	サニタイズ		○		
	データ暗号化	○	○		○
	通信経路の暗号化	○			○

	暗号化ファイルシステム（EFS）		□		
	無線回線経由の鍵更新（OTAR）		□		
暗号利用に関するポリシー	リスクアセスメント		○		
	ポリシーの策定		○	□	
	リスクマネジメント		○		

○はメインテーマとして取りあげられている文書が発行されている
△はメインテーマを構成する機能として取りあげられている文書が発行されている
□はメインテーマが適用されるもの・応用先としてのみ取りあげている文書が発行されている
は国外の組織でメインテーマとして文書が発行されているが、日本国内で発行されていない文書
は国外の組織でテーマの一部として文書が発行されているが、日本国内で発行されていない文書

日本国内の組織がメインテーマとして取りあげているテーマは 11 種類、NIST がメインテーマとして取りあげているテーマは 22 種類、ENISA がメインテーマとして取りあげているテーマは 19 種類、IETF がメインテーマとして取りあげているテーマは 7 種類で、NIST が多岐にわたるテーマに関して文書を整備している状況がわかる。また、ENISA 発行の“The Use of Cryptographic Techniques in Europe”では、NIST や日本の IPA・CRYPTREC における暗号技術の使用に関する文書の整備状況を説明したうえで、欧州では同様の取り組みがあまり行われていないことを言及している。

国内外のガイドライン整備状況を比較した結果をもとに、国内の文献で取りあげられていないテーマを以下に示す。

1) 暗号利用のポリシーに関する文書

暗号利用のポリシーに関する文書の整備状況は表 3-13 の通りである。

表 3-13　暗号利用に関するポリシーに関する文書の整備状況

組織	該当文書	内容
日本国内の組織	なし	
NIST	SP 800-175A Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies	連邦政府における暗号及び NIST が定める暗号基準を使用する際の基礎的なガイドライン。暗号を利用する際の要求事項を決定するためのガイダンスを提供。連邦政府が扱う機微情報保護に関連する法律や指令、保護すべき資産を特定するためのリスクアセスメント方法等について解説。

組織	該当文書	内容
ENISA	The Use of Cryptographic Techniques in Europe	暗号に関するガイドライン等を作成する政策立案者や電子政府所管組織の関係者を対象読者として、電子政府において用いられる暗号化手法に関して、EU 加盟国におけるアンケート調査結果及び推奨事項を記した文書。調査結果として、以下の推奨事項が述べられている： 1. 保護すべきデータと適切なセキュリティ対策の実施 2. 適切な暗号ポリシーの策定 3. 優れたセキュリティプラクティスに従ってソリューションを展開する 4. 暗号ポリシーの読者を理解する 5. 監査の実施 6. 暗号プロセスの開発に関する明確なガイダンスを作成する 7. 長寿命なソリューションを構築し、最新のリスクに対応する 8. 暗号政策の策定、最小要件の評価・推奨を EU 全体で行う
IETF	なし	

NIST 発行の“SP 800-175A Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies”は主に連邦政府機関職員を対象として、暗号を利用する際の要求事項を読者自身で決定できるようにするための文書であり、どの法律・文書を参照すべきかまとめ、暗号の観点からリスクアセスメント方法について解説している。また、より詳細な暗号（暗号プロトコル等）を使用する際の要件を決定する方法については、連邦政府機関職員及び暗号化サービスの提供と使用に関する担当者、プログラム管理者、システムの調達担当等を対象読者として、“SP 800-175B Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms”で示している。

ENISA 発行の“The Use of Cryptographic Techniques in Europe”は政策立案者や電子政府所管組織の関係者を対象読者として、電子政府において用いられる暗号化手法に関して、EU 加盟国におけるアンケート調査結果及び推奨事項を記した文書である。詳細な推奨事項は記していないが、アンケート結果として暗号プロセスの開発に関する明確なガイダンスを作成することを推奨している。

また、日本国内の組織、NIST、ENISA、IETF 共に、企業の責任者・担当者を対象読者とした暗号利用に関するポリシーに関する文書は今回の調査範囲ではなかった。

2) 様々な暗号技術に関して言及する文書

暗号メカニズムの選択と使用には様々な暗号技術を一通り理解する必要がある。様々な暗号技術について 1 つの文書内で言及する文書の整備状況は以下の通りである。ここでは表 3-12 に示したテーマについて、1 つの文書の中で 10 テーマ以上言及されているものを取りあげている。

表 3-14　様々な暗号技術について 1 つの文書内で言及する文書の整備状況

組織	タイトル	内容
日本国内の組織	なし	
NIST	SP 800-175B Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms	連邦政府の機密情報保護に利用できる暗号方法とサービス、NIST の暗号標準の概要を説明したガイドライン。
ENISA	Algorithms, key size and parameters report 2014	組織における意思決定者及び暗号ソリューションを設計し実装する専門家を対象読者として、暗号アルゴリズムと暗号鍵サイズ及びパラメータに関する一連の推奨事項を記した文書。
IETF	なし	

NIST や ENISA は、様々な暗号技術に関して推奨事項や技術内容を示した文書を発行しているが、日本や IETF は技術ごとのガイドラインを発行している傾向がある。

3) 目的を細分化し、一部の内容に特化した文書

a. 鍵管理

鍵管理に関する文書の整備状況は以下に示す通りである。

表 3-15　鍵管理に関する文書の整備状況

組織	件数
日本国内の組織	5 件(4)
NIST	13 件(10)
ENISA	4 件(2)
IETF	5 件(3)

※括弧内は主題として鍵管理があげられているもの

表 3-15 をみると NIST では様々な視点から鍵管理に関する文書を発行している。それぞれの文書間の関係性については「3.2.2(2)1)NIST 発行「鍵管理」に関する文書」に示す通り

であるが、“SP 800-130 A Framework for Designing Cryptographic Key Management Systems”では暗号鍵管理システムに特化し“SP 800-133 Recommendation for Cryptographic Key Generation”は鍵生成に特化している。また、鍵管理には含まれないが、“SP 800-132 Recommendation for Password-Based Key Derivation: Part 1: Storage Applications”や“SP 800-135 Rev.1 Recommendation for Existing Application-Specific Key Derivation Functions”では鍵導出関数に特化し、推奨事項を記載している。

一方、日本国内の組織が発行した鍵管理に関する文書は IPA 発行の「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）」、IPA/CRYPTREC「2010 年度版リストガイド（鍵管理）」、日本コンピュータセキュリティインシデント対応チーム協議会「SSH サーバセキュリティ設定ガイド」があげられるが、前者 2 つに関しては鍵管理全体に関して言及されており、最後の 1 つは SSH サーバのセキュリティのために鍵管理の要求事項が掲載されている。

b. サニタイズ

NIST“SP 800-88 Rev.1 Guidelines for Media Sanitization”において、連邦政府機関、企業におけるサニタイズ やメディア廃棄の担当者や意思決定者を対象読者として、暗号化消去について考慮事項を記載している。一方、今回調査した範囲では、日本国内の組織が発行した文書で、暗号化によるサニタイズについて言及されている文書はない。

c. 乱数生成

NIST “SP 800-22 Rev.1a A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications”において、乱数生成器と擬似乱数発生器の選択とテストについて解説し、“SP 800-90 シリーズ”において、乱数生成の実装要件について記載している。また、NIST 発行の“SP 800-175B Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms”や ENISA 発行の“Algorithms, key size and parameters report 2014”では、暗号技術に関する一連の推奨事項の 1 つとして乱数生成について言及している。IETF は“RFC4086 Randomness Requirements for Security”において乱数生成の要件を記載している。

一方で、今回調査した範囲では、日本国内の組織は乱数生成に特化した文書を発行していない。

d. 電子認証

NIST は SP 800-63-3 シリーズ“Digital Identity Guidelines”において、電子認証を使用する際のリスク評価手法と一般的なフレームワークの概要を提供している。一方、今回調査した範囲では、日本国内の組織が発行した文書で、電子認証について言及されている文書はない。

3.3 考察

本調査では、日本国内の組織が発行した文書 14 件、NIST が発行した文書 30 件、ENISA が発行した文書 5 件、IETF が発行した文書 10 件を調査した。

その結果、日本国内の組織が発行する文書としては「暗号に関して運用・設定に関する文書（特に暗号プロトコルに関するもの）」が多く、NIST が発行する文書としては「暗号に関して運用・設定に関する文書（暗号プロトコル以外に関するもの）」が多い。また ENISA が発行する文書としては「暗号に関して運用・設定に関する文書（暗号プロトコル以外に関するもの）」が多く、IETF が発行する文書は「暗号の開発実装に関連する文書」が多い。この結果は、今後ガイドラインを策定する場合、策定するガイドラインの目的により参考とすべき組織の選定の参考になると考えられる。

また、暗号の利活用の文書に関して国外にあって日本にはない種類（テーマ）としては、以下があげられる。

- 政府システム利用時の暗号利用に関するポリシーに関する文書
  - ✓ どの文書を参照すべきかまとめた文書
  - ✓ 暗号の観点からリスクアセスメント方法についてまとめた文書
- 様々な暗号技術に関して言及する文書
  - ✓ 詳細な暗号（暗号プロトコル等）使用の際の要件を決定することを支援する文書
- 目的を細分化し、一部の内容に特化した文書
  - ✓ 鍵生成に特化した文書
  - ✓ 暗号鍵管理システムに特化した文書
  - ✓ 鍵導出関数に関する文書
  - ✓ 暗号化によるサニタイズに関する文書
  - ✓ 乱数生成に関する文書
  - ✓ 電子認証に関する文書

ただし、暗号利用に関するポリシーに関する文書に関しては、日本国内の組織、NIST、ENISA、IETF 共に、企業の責任者・担当者を対象読者とした文書は発行していない。

2017 年 7 月現在のところ、上記内容のテーマに関しては日本国内の組織より発行されていないため、該当テーマに関する文書を策定すべきか検討する必要があると考えられる。

4. ヒアリング調査

4.1 調査概要

アンケート及び文書調査の分析結果をもとに、暗号の利活用に関する知見を持つ有識者及び暗号を利用したシステムを運用した経験を持つ企業を対象にヒアリング調査を実施した。調査は、専門家の視点を踏まえ、今後優先的に作成していくべきテーマや文書の種類を含め、整備すべきガイドラインの対象を明らかにすることを目的として実施した。

ヒアリング調査の概要は下表の通りである。

表 4-1　ヒアリング調査概要

調査目的	アンケート及び文書調査の分析結果をもとに、今後優先的に作成していくべきテーマや文書の種類を含め、整備すべきガイドラインの対象について、専門家の視点から意見を伺う。
調査対象	ヒアリングは以下を対象に 3 件実施した。 ・ 暗号の利活用に関する知見を持つ有識者（1 件） ・ 暗号を利用したシステムを運用した経験を持つ企業（2 件）
ヒアリング項目	・ アンケート調査・分析結果及び国内外ガイドラインの調査・分析結果について ・ 暗号の利活用に関する課題について ・ 今後策定すべき暗号利活用に関するガイドラインについて

4.2 調査結果

ヒアリング調査で得られた主な意見を以下に示す。

(1) 暗号利活用に関する課題

暗号利活用に関する課題としては、企業の暗号利用に対する理解度が不足していることや企業が海外に事業展開する際の各国規制への対応等が課題として指摘された。また、今後 IoT 等の利活用が進んだ場合、IoT 機器は長期間の利用となるケースが多いため、セキュリティ対策や暗号鍵の管理等が課題になるとの指摘もあった。

（有識者）
- 暗号技術の輸出規制への対応が複雑である。ビジネスとして暗号技術自体を輸出することがなくても、企業のグローバル化は進んでおり、セキュリティに関する各国の制度に対応する必要がある。
- クラウド上のセキュリティ・暗号技術の利用についてのガイドラインは整備されておらず、対策基準が曖昧となっている。
- 企業等の暗号技術は、システム等の外注時に外注先に判断を委ねているのが現状である。調達側が自ら暗号要件について決定する必要があるのではないか。

・ 日本のブランド名で販売しているが、実際の製造は海外で行っている製品もある。過去にそのような製品の脆弱性が見つかったが、調達要件に暗号・セキュリティに関する要求事項がなかったために製造側は対応が必要ないと考えた事例があった。

（暗号を利用したシステムを運用した経験を持つ企業）

・ 暗号利用に関しては啓発が不足している。
・ 攻撃者のほうが暗号をうまく活用している。ネットワークの経路の暗号化による匿名化等を行っており、守る側よりも攻撃する側のほうが暗号を活用しているのが現状ではないか。
・ 暗号に関してはワッセナーアレジメントの制約がある。海外の現地法人に製品を展開したいと考えても制限を受けることがある。
・ 暗号を活用した製品やサービスを顧客に提案する際に、暗号の選定で問題になることはほぼない。
・ S/MIME やデータベースの暗号化、モバイルデバイスの暗号化は重要であると考えているが、利用するプラットフォームが対応していない等の理由で導入が進んでいないのではないか
・ HDD の暗号化を自社の標準 PC で実施しているが、鍵管理をユーザに任せている部分があり、システムによる自動化等の対応ができていない。課題として認識している。
・ 暗号を利用する際は、多くの製品で採用されている標準的なものを利用している。標準以外のものを利用する場合追加コストが発生する。
・ 社内標準 PC の Windows10 への移行を進めているが、Windows7 で利用できていた暗号化ツールが Windows10 で利用できない事象が発生している。HDD の暗号化と Windows10 の問題はこれから注目されると考えている。ガイドラインでなくとも、参考になる資料があるとよい。
・ 自社は複数事業を展開しており、事業により暗号利活用に対する認識や理解度は異なる。
・ IoT はコンシューマ向けとインダストリー向けの 2 つがある。インダストリー系はこれまでの IT ベンダではなく製造業が中心となるため、暗号に関する知識が不足しているのではないか。
・ 自動運転の登場により、自動車のセキュリティ対策が今後重要になると考えられるが、セキュリティに対する意識はまだ十分ではない。自動運転において暗号は基盤技術になる。
・ 自動車の耐用年数を考えると、鍵管理が長期間となるため、鍵管理が課題となるのではないか。
・ Society5.0 はマルチステークホルダーの世界である。サプライチェーンの管理も重要となるが、暗号技術も重要な要素となる。
・ 暗号技術をセキュリティのための技術と考えないほうがよい。イノベーションのためであり、産業競争力の観点から暗号を考えたほうがよい。

(2) 今後策定すべき暗号利活用に関するガイドラインについて

今後策定を検討すべき暗号に関するガイドラインとしては、利用者の観点からガイドライン読者が実際に活用できるガイドラインや運用や実装等利活用に焦点をあてたガイドラ

イン、暗号技術の全体像がわかるもの、利用目的や対象読者別に既存の暗号に関する文書が整理されたインデックスのようなものがあるとよい等の意見があった。

（有識者）
- 暗号技術の全体像・アーキテクチャがわかるようなインデックスのような文書があるとよい。
- ガイドラインの発行の有無に関わらず、読者が実際に利用できるものを作る必要がある。利用者側の目線に立った文書は少ないのではないか。
- ガイドラインの策定は技術者が行うことが多く、わかりにくいものが多い。利用者の立場に立って文書を記述できる人を策定者側に巻き込む必要があるのではないか。
- 担当者向けに実務的な面を支援するガイドラインも必要だが、経営者等のトップ層向けに環境整備を促す啓発用資料が必要ではないか。
- 諸外国におけるセキュリティ・暗号技術の制度・規制を調べたものがあるとよい。
- クラウド上における暗号技術に関するガイドラインが必要ではないか。例として、クラウド上の鍵管理があげられる。
- 委託先管理の観点から、委託先に提示する最低限やるべき対策を示したガイドラインなども必要ではないか。
- 高機能暗号について、どのように利用できるかを紹介するようなガイドラインも必要ではないか。あるいは必要かどうか検討すべきではないか。

（暗号を利用したシステムを運用した経験を持つ企業）
- 有識者やサービス提供事業者、大企業、中小企業それぞれの立場により意見は異なるのではないか。対象読者によりメッセージが異なる。
- アルゴリズムより運用や実装に関するガイドラインのほうが必要である。
- アルゴリズムのような技術的情報よりも、ユーザが暗号を利用した製品等を容易に導入できるガイドラインのほうがニーズはあるのではないか。
- 技術的詳細の資料は参考としてあると助かるが、優先度は高くない。
- 暗号は基盤技術であるため、システムの開発者や製品担当者向けのガイドラインは必要である。
- データベースにパスワードを保存する際の暗号設定等具体的なユースケースで、どうすればよいのか、適切な方法は何か等が整理されると参考になる。
- システム開発者・製品担当者向けに暗号利活用教育をするのであれば、IPA で実施しているセキュアコーディング等の開発者向け教育の一環で実施するとよいのではないか。
- モバイル端末等のデバイスで使用されている暗号やその安全性について解説すれば、BYOD 等で企業がデバイスを活用する際の参考になるのではないか。
- どの文章を参照すればよいかがわかるインデックスがあるとよい。利用シーンや利用目的、対象読者等の基準で分類されるとよい。
- 鍵管理に関しては、利用する側と利用してもらう側の両方のガイドラインがあるとよい。
- 暗号がよく利用されるケースに限定してガイドラインを策定する方法も考えられる。ガイドラインとせず、啓発資料としてもよいのではないか。
- 一般ユーザに普及啓発するためには、企業の情報システム部門に啓発するのが効果的である。情報システム部門にインプットすることで、担当者から一般ユーザへの展開が容易

になる。
・ 鍵管理をガイドラインとしてまとめるのは難しいのではないか。NIST でも検討は進められているが、うまくまとめられていない印象である。
・ CRYPTREC のガイドラインはシーズ指向であるが、Society5.0 はサービス視点から必要となる暗号を検討しており、視点が異なる。サービスの観点からの検討も必要になるのではないか。
・ 製造業等対象者を絞った暗号に関する読み物があるとよいのではないか。
・ 暗号移行や鍵長等に関するロードマップがあるとよい。CRYPTREC では今後 10 年間を対象に検討しているが、暗号のライフサイクルから考えると期間が短い。
・ 高機能暗号に関しても検討する必要があるのではないか。
・ 鍵管理はビジネスモデルの話でもある。つながる世界ではステークホルダーが多数となるため、誰が鍵管理や更新を実施するかを整理し、ガイドラインを検討するとよいのではないか。

5. まとめ

暗号の利活用に関するアンケート調査・国内外における暗号の利活用に関する文書の調査・ヒアリング調査の結果をもとに、今後策定を検討する必要があると考えられるガイドラインを以下の 4 つの観点から整理した。

- 対象読者にあわせたテーマ別ガイドラインの検討
- 活用しやすさを考慮したガイドラインの検討
- 既存ガイドラインの普及方策・内容更新の検討
- 暗号利用環境の変化にあわせたガイドラインの検討

5.1 対象読者にあわせたテーマ別ガイドラインの検討

今回の調査結果から、管理者向けと現場の担当者向けでは、ガイドラインで必要となる内容が異なるとの指摘が有識者等からあった。そこで、対象者別にガイドラインの内容等を検討する必要があると考えられる。

以下に対象読者別に今後検討が必要になると考えられるガイドラインの例を示す。また、図 5-1 にガイドラインの対象読者とテーマの関係を示す。

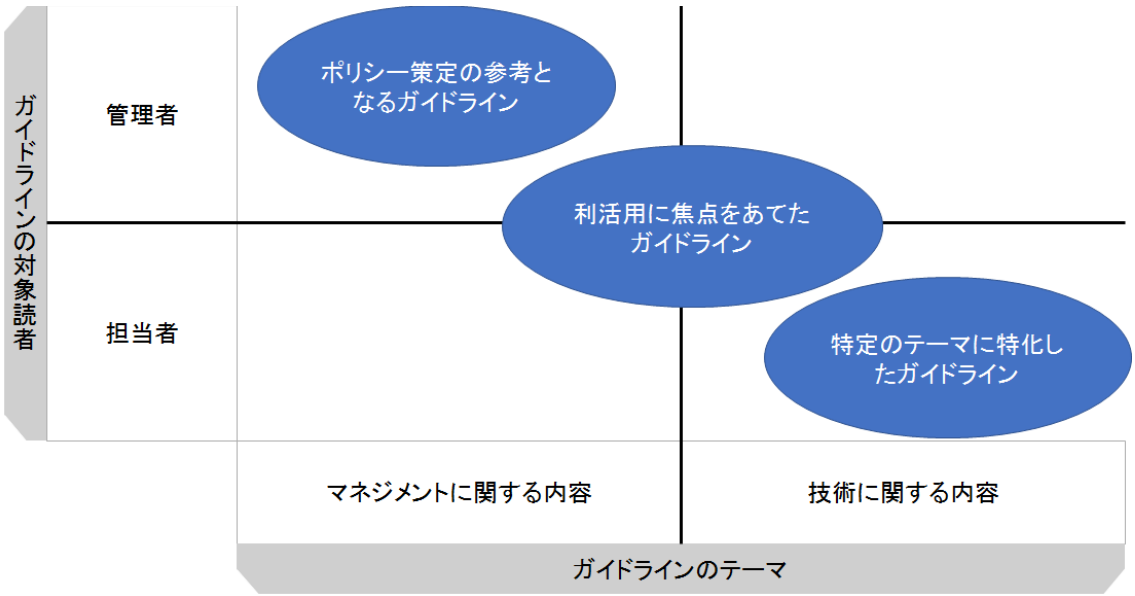


図 5-1　ガイドラインの対象読者とテーマ

(1) 暗号利用に関するポリシー策定の参考となるガイドライン（管理者向け）

文書調査の結果から、海外では NIST の SP800-175A のように、暗号を利用する際にどの法律や文章を参照すべきか、暗号利用の観点からリスクマネジメントについて体系的にまとめた文書があった。また、ヒアリング調査でも、暗号を利活用する際にどのような文書を参照すべきかを利用シーンや利用目的別にまとめたインデックスがあると活用しやすいとの意見があった。

暗号利用に関して参照すべき文書や暗号利用の観点からのリスクマネジメントについて解説したガイドラインは、企業の情報システムや情報セキュリティ部門の管理者が暗号利用に関するポリシーを検討する際に参考になると考えられる。アンケート調査結果から、多くの企業では暗号利用に関する基準は現状整備されていない。このようなガイドラインを整備することにより、企業の適切な暗号利用を促進する可能性があると考えられる。

(2) 暗号技術の利活用に焦点をあてたガイドライン（管理者・担当者向け）

アンケート調査結果から、暗号技術を利用したシステム関連製品の選定・導入・利用・運用時の課題として「どの製品が安全で導入してよいものであるかがわからない」、「正しくかつセキュアな暗号処理が行われているか、確信が持てない」、「ユーザの利便性と暗号技術の導入によるセキュリティ対策のバランスをとるのが難しい」等、企業担当者が暗号技術を適切に評価し製品を導入することや暗号の適切な利用・運用が課題になっていると考えられる。ガイドラインの内容に関しても、暗号技術の技術的な仕様ではなく、暗号製品や技術の設定方法や運用、暗号鍵の管理等、暗号技術の利活用に関する回答割合が高かった。また、ヒアリング調査でも暗号アルゴリズム等の技術的内容よりも運用や実装等に関する内容が必要との意見があった。

これらの結果から、暗号の技術的詳細に関するガイドラインよりも設定や運用等暗号技術の利活用に焦点をあてたガイドラインの検討が必要になると考えられる。

(3) 特定のテーマを深堀したガイドライン（担当者向け）

文書調査の結果から、海外では一部の内容に特化した文書があった。

例えば、今回の調査した範囲では国内外ともに鍵管理全体をカバーしたガイドラインは整備されていたが、鍵管理に関連した要素である、鍵生成に関する NIST SP800-133 や鍵導出に関する NIST SP800-132、NIST SP800-135 のように鍵管理の中でも特定のテーマに特化した文書が海外では整備されていた。他にもサニタイズ（NIST SP800-88 Rev.1）や乱数生成（NIST SP800-22 Rev.1a や IETF RFC4086 等）に特化した文書もあった。

今後ガイドライン策定にあたっては、現時点で国内では策定されていないテーマについても検討する必要があると考えられる。また、これら特定のテーマに特化したガイドラインに関しては、導入や運用等を実際に担当する担当者を想定読者として検討する必要があると考えられる。

5.2 活用しやすさを考慮したガイドラインの検討

アンケート調査の結果から、ガイドラインの内容についてチェックリストや具体的な製品等の設定方法等を求める回答があり、企業の担当者は活用しやすいガイドラインを求めていると考えられる。

ヒアリング調査でも、ガイドラインの読者が実際に利用できるよう、利用者側の目線にたったガイドラインの必要性や、具体的に暗号が利用されるケース別等、ガイドライン利用者がより活用しやすいガイドラインを求める意見もあった。

これらの結果から、ガイドラインの検討にあたっては、ガイドライン利用者の活用しやすさを考慮する必要があると考えられる。具体的には、アンケートでもニーズがあったチェックリストや具体的な製品設定方法の例等を示す方法が考えられる。

5.3 既存ガイドラインの普及方策・内容更新の検討

今回の調査結果から、既にガイドラインが策定されているものの、十分に活用されていないと考えられるものがあった。

例えば、今回のアンケート調査では、7 割程度の企業が鍵管理の重要性を認識しているものの、具体的な対策まで実施できている企業は多くなかった。鍵管理に関しては IPA より、「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）」が公開されているが、ヒアリング調査で有識者等から、企業の担当者に十分に活用されていない可能性があるとの指摘を受けた。

鍵管理に関しては、ガイドラインが整備されているものの、十分認知・利用されていない可能性や企業が求める内容と異なり企業の課題解決につながっていない可能性がある。このような状況は、鍵管理以外の分野でも存在する可能性がある。

既にガイドラインが整備されている分野に関しては、既存のガイドラインの普及方策や企業の担当者が活用しやすいように内容の更新等を検討する必要があると考えられる。

5.4 暗号利用環境の変化にあわせたガイドラインの検討

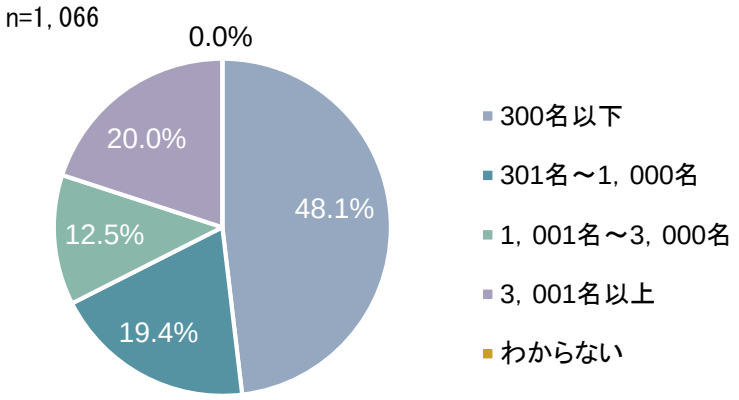
今回のヒアリング調査で、現時点で国内外でガイドラインがないが、今後ガイドラインの策定を検討したほうがよいテーマとして、クラウド環境での暗号利用や高機能暗号等があげられた。また、企業が海外に事業展開する際に、セキュリティに関する各国制度の対応が必要となるため、各国の制度等をまとめた情報があるとよいとの意見もあった。

暗号利用環境の変化や新規技術の登場に合わせて、新たなテーマに関するガイドラインの検討も今後考慮する必要があると考えられる。また、クラウドや IoT に関しては、既存のセキュリティに関するガイドラインがあるため、そのガイドラインの中に暗号利活用に関する考慮事項等を記載する方法も考えられる。

付録１　アンケート調査結果詳細

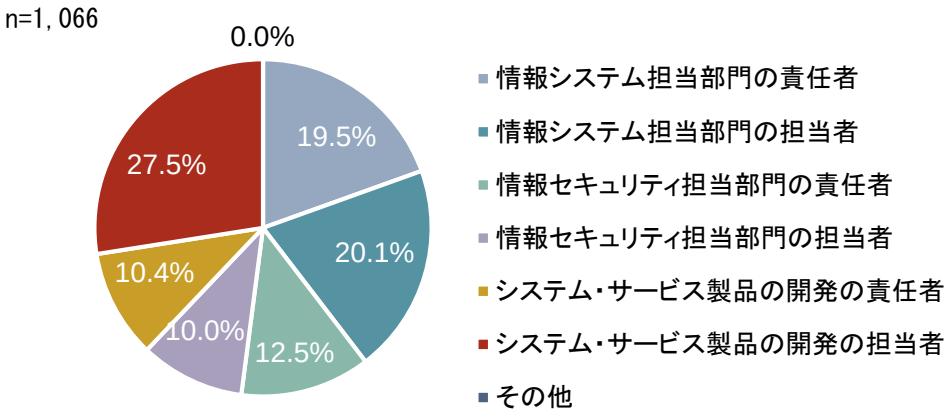
付録 1.1　属性情報

S1. お勤め先の会社（以下、貴社）の総従業員数（有給役員，正社員・正職員，準社員・準職員，アルバイト等を含む）について、直近の会計年度の人数をお答えください。



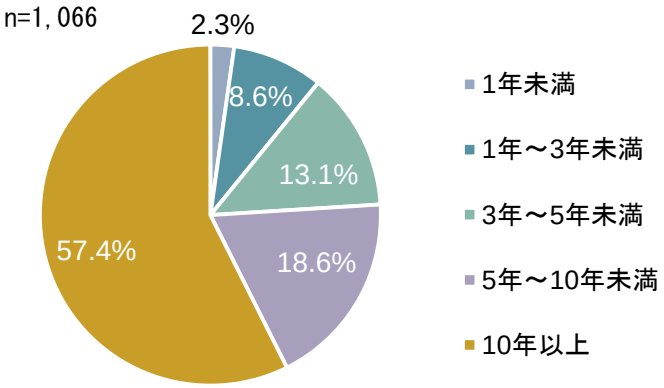
付録 1-1 従業員数

S2. 貴社におけるあなたの役割として一番近いものをお答えください。



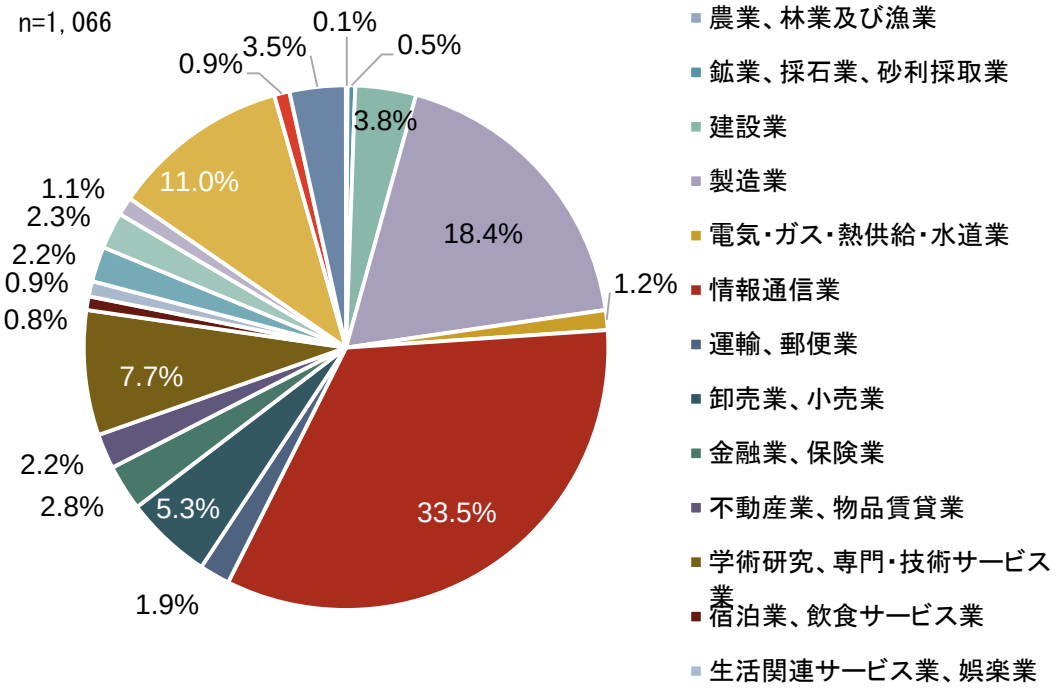
付録 1-2 回答者役職

S3. 前問で回答した役割での業務経験年数について、お答えください。



付録 1-3 現在の役職での業務経験年数

S4. 貴社の主な業種をお選びください。

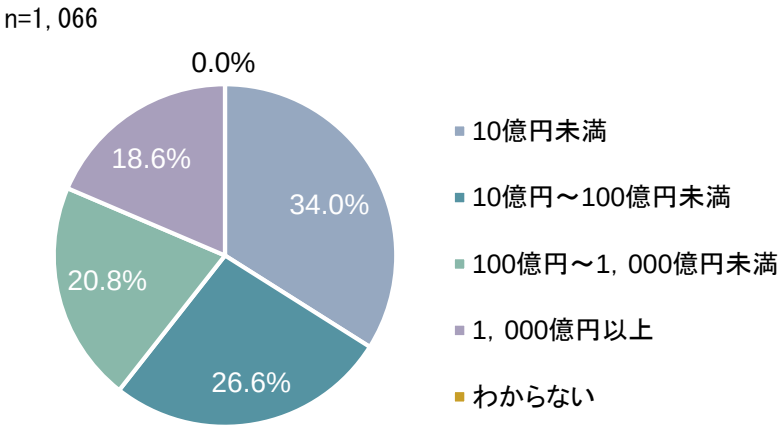


付録 1-4 業種

付録 1-5 業種

業種	割合（%）
農業、林業及び漁業	0.1
鉱業、採石業、砂利採取業	0.5
建設業	3.8
製造業	18.4
電気・ガス・熱供給・水道業	1.2
情報通信業	33.5
運輸、郵便業	1.9
卸売業、小売業	5.3
金融業、保険業	2.8
不動産業、物品賃貸業	2.2
学術研究、専門・技術サービス業	7.7
宿泊業、飲食サービス業	0.8
生活関連サービス業、娯楽業	0.9
教育、学習支援業	2.2
医療、福祉	2.3
複合サービス事業	1.1
その他サービス業	11.0
公務	0.9
その他	3.5

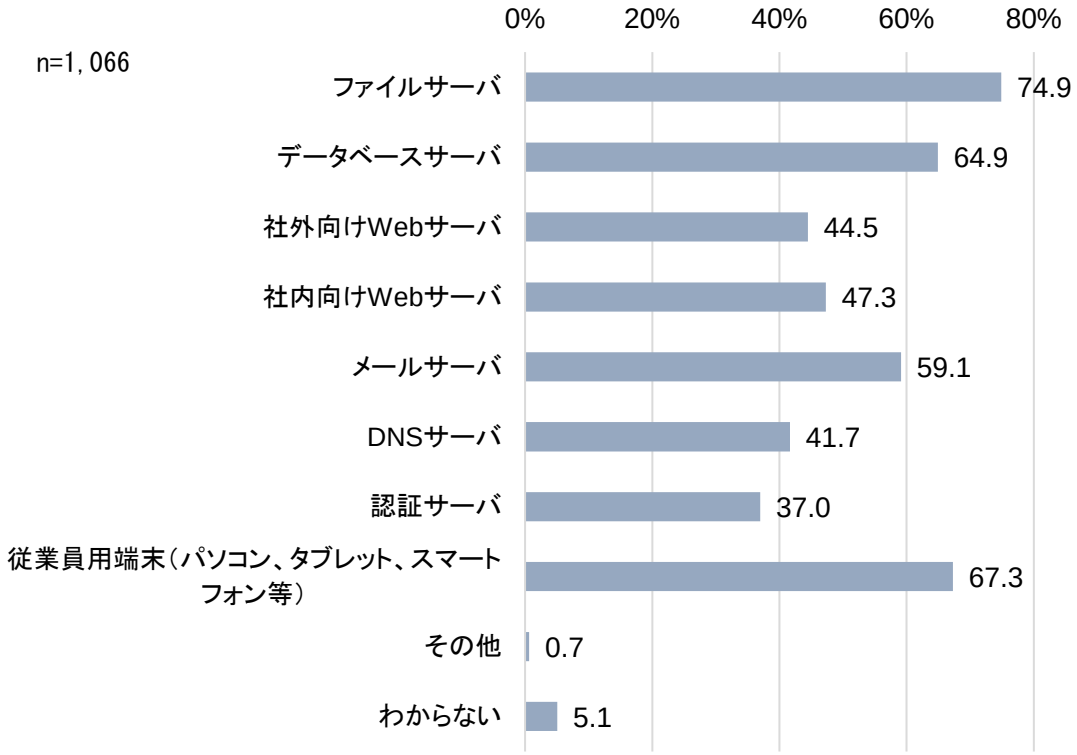
S5. 貴社の総売上高について、直近の会計年度の金額をお答えください。



付録 1-6 売上高

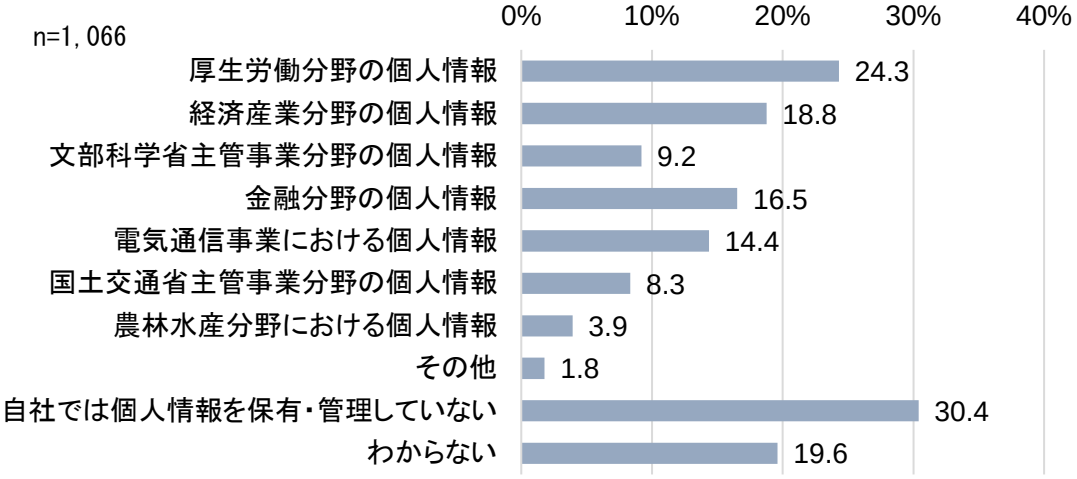
付録 1.2　基本情報

問 1.　貴社で保有・管理している情報システムを構成しているものについて、あてはまるものを全てお選びください。



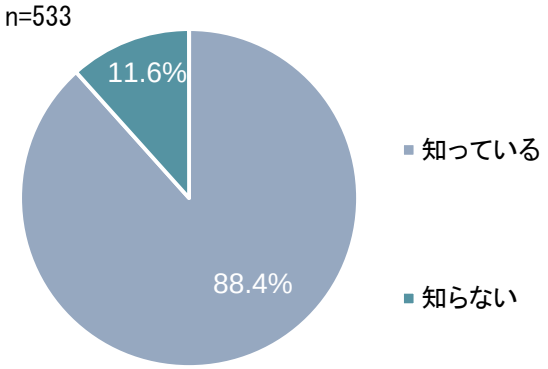
付録 1-7 保有・管理している情報システム（複数回答）

問 2-1.　貴社で保有・管理している個人情報（貴社で直接収集または委託されたもの）の種類について、個人情報保護法に基づき、あてはまるものを全てお選びください。



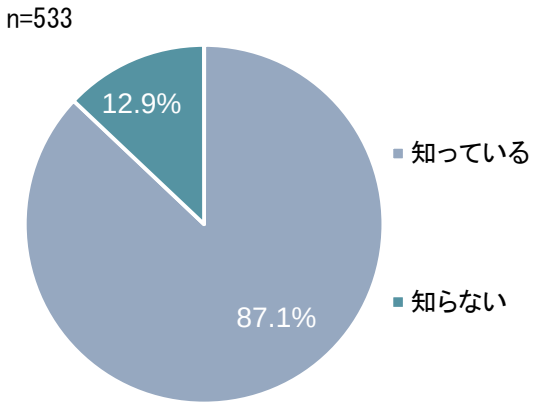
付録 1-8 保有・管理している個人情報（直接収集または委託されたもの）種類（複数回答）

問 2-2. 選択した分野の個人情報保護に関するガイドラインについて知っていますか。



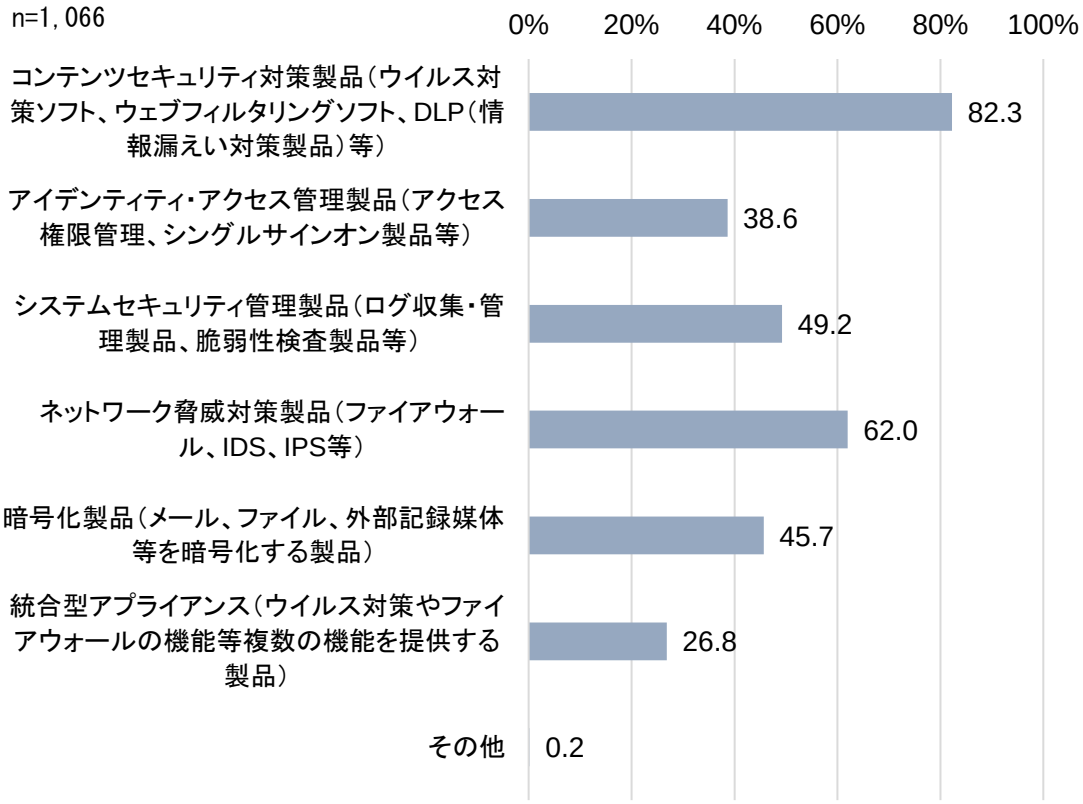
付録 1-9 選択した分野の個人情報保護に関するガイドラインの認知度

問 2-3. 個人情報保護法が定める「特定個人情報の適正な取扱いに関するガイドライン」について知っていますか。



付録 1-10 「特定個人情報の適正な取扱いに関するガイドライン」の認知度

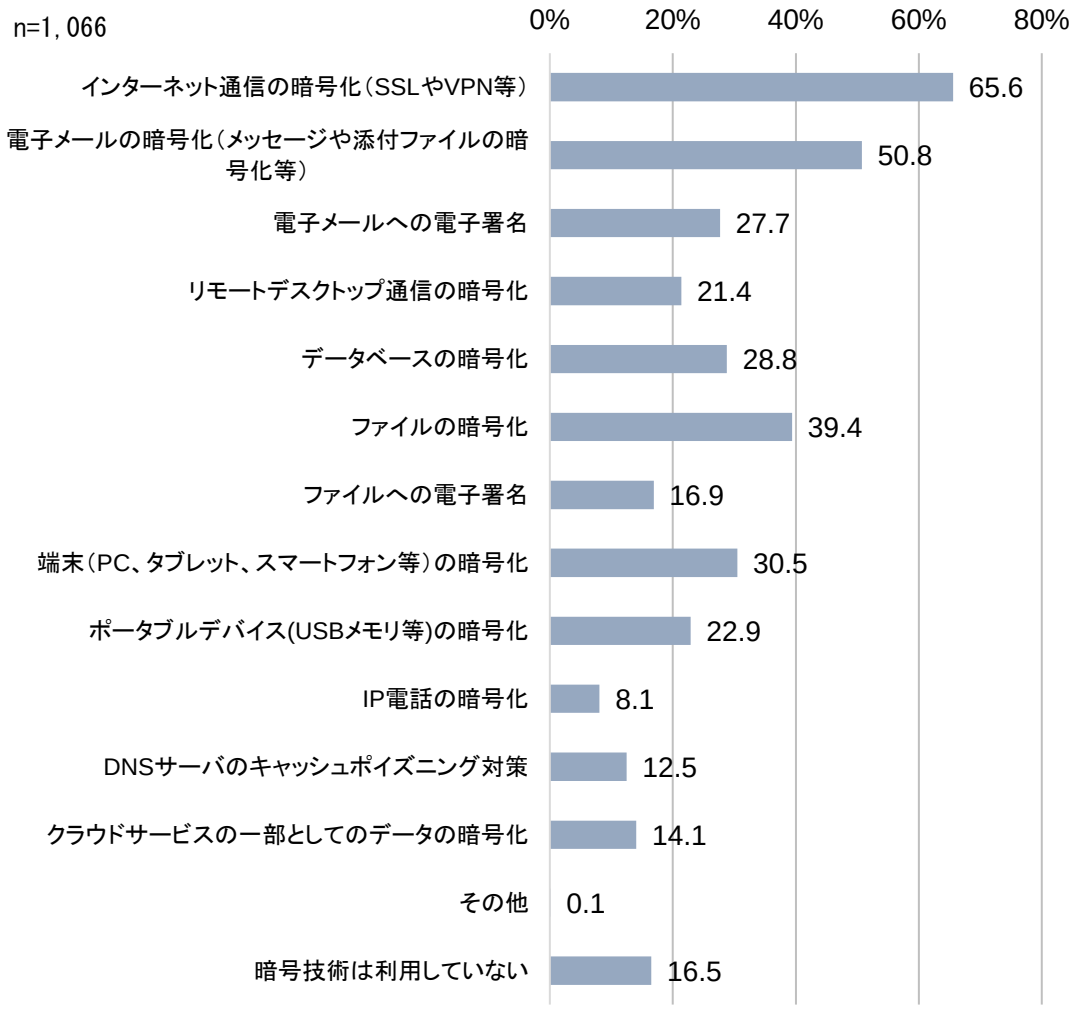
問 3. 貴社で導入している情報セキュリティ対策製品について、あてはまるものを全てお選びください。



付録 1-11 導入している情報セキュリティ対策製品（複数回答）

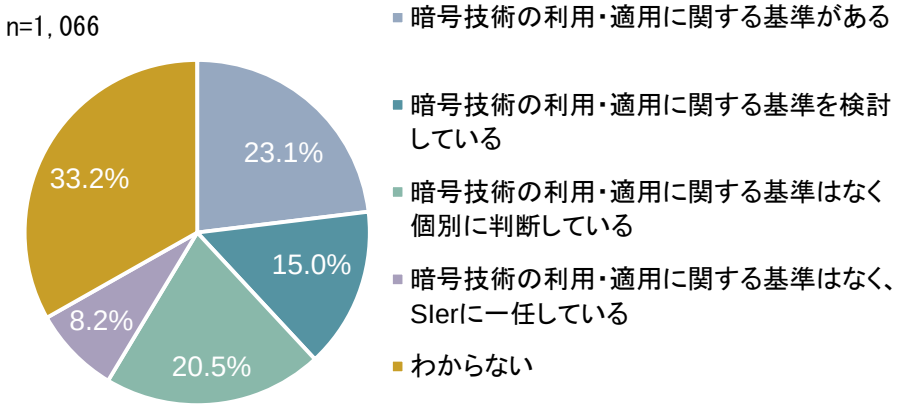
付録 1.3　暗号利活用状況

問 4. 貴社では、どのような場面で暗号技術を利用していますか。あてはまるものを全てお選びください。

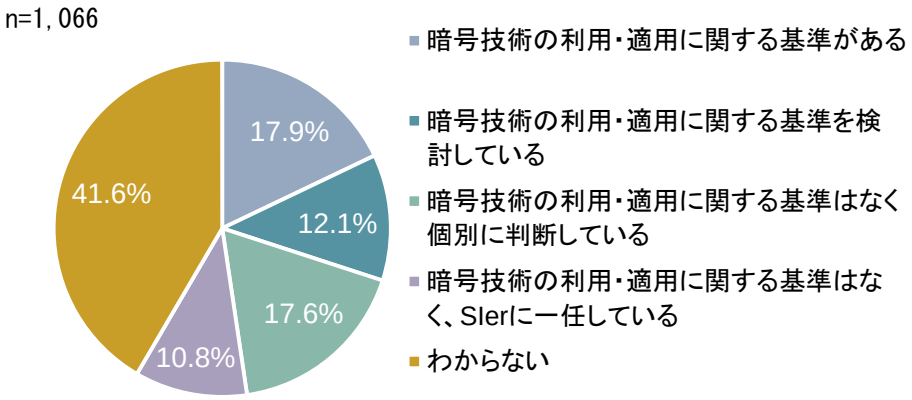


付録 1-12 暗号技術の利用場面（複数回答）

問 5-1. 貴社では、システム関連製品を選定・導入・開発する際に、暗号技術に関する基準を設けていますか。-選定・導入

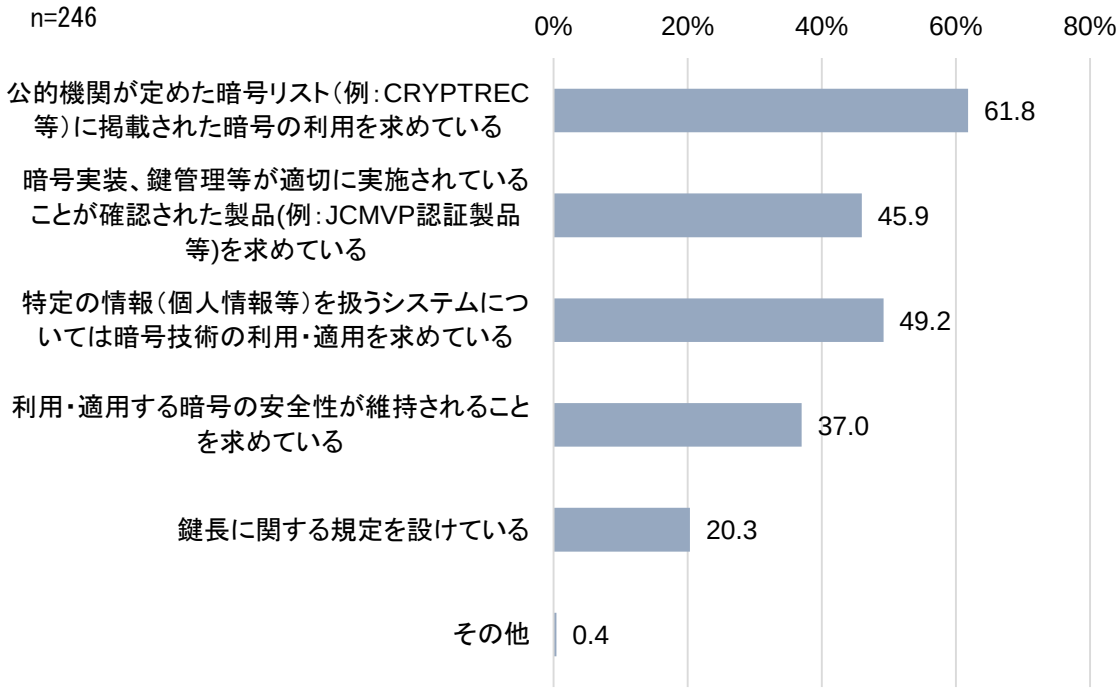


付録 1-13 暗号技術に関する基準の有無（選定・導入時）

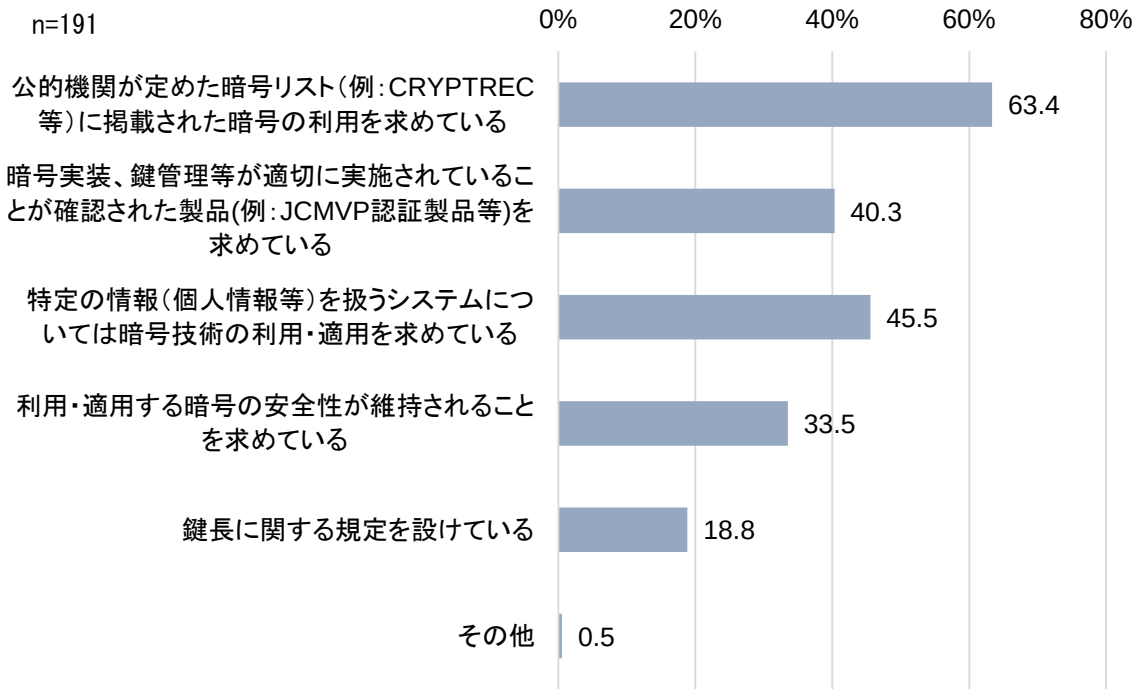


付録 1-14 暗号技術に関する基準の有無（開発時）

問 5-2. 貴社でシステム関連製品を選定・導入・開発する際に、暗号技術に関する基準として、あてはまるものを全てお選びください。

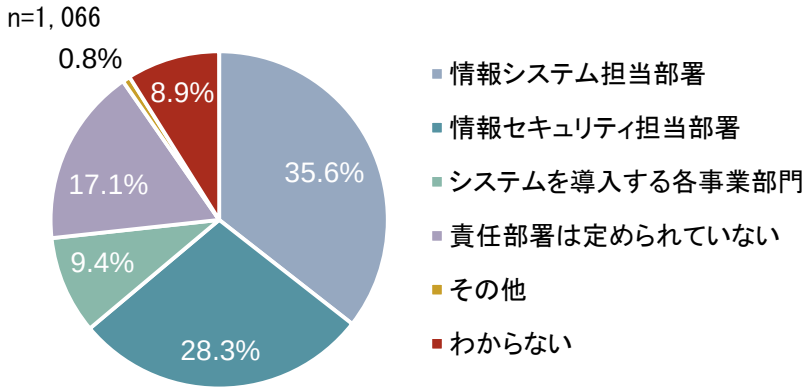


付録 1-15 暗号技術に関する基準（選定・導入時）（複数回答）



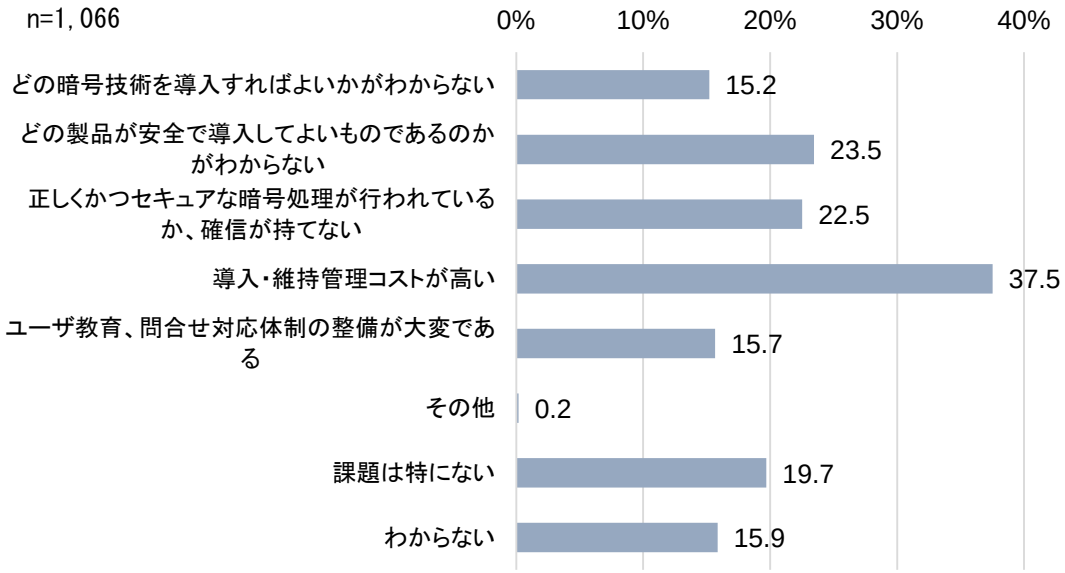
付録 1-16 暗号技術に関する基準（開発時）（複数回答）

問 6. 貴社で暗号技術を利用した製品を導入する際、導入に関して責任を持つ部署はどこですか。



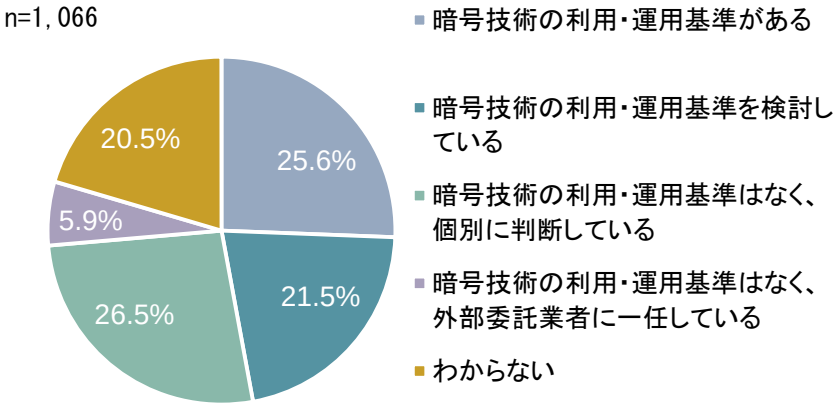
付録 1-17 暗号技術を利用した製品の導入に関する責任部署

問 7. 貴社でシステム関連製品を選定・導入する際に、暗号技術に関する課題として、あてはまるものを全てお選びください。



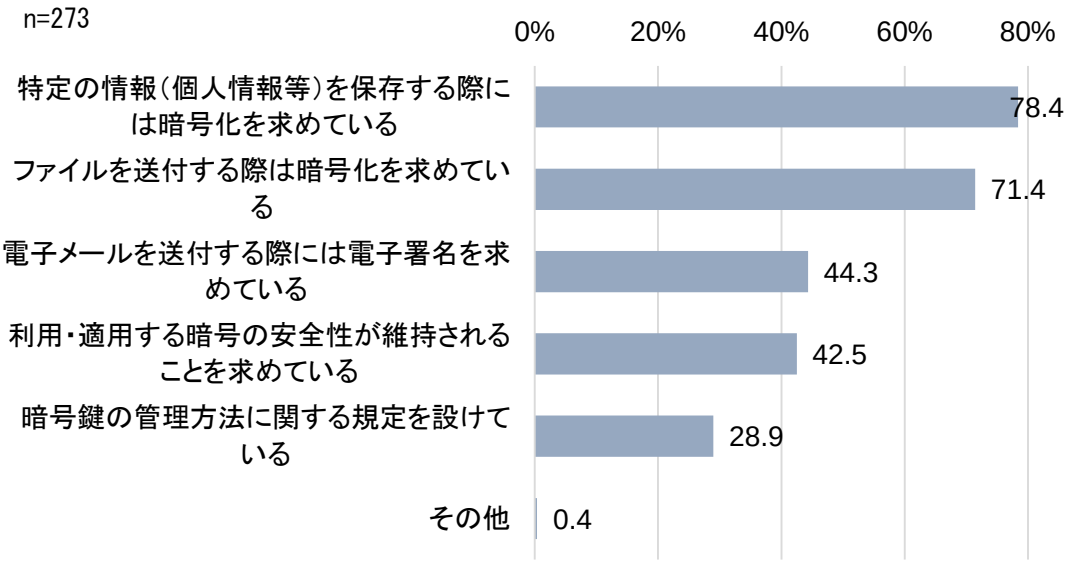
付録 1-18 システム関連製品を選定・導入時の暗号技術に関する課題（複数回答）

問 8-1. 貴社では、暗号技術の利用・運用に関する基準はありますか。



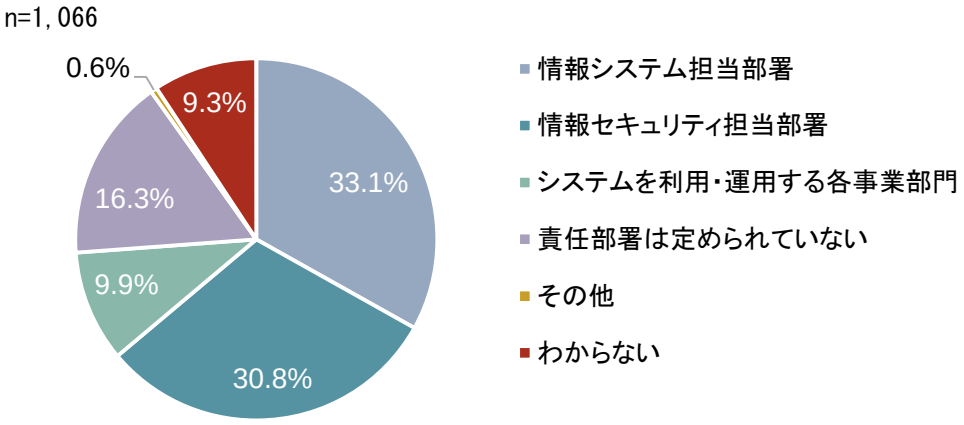
付録 1-19 暗号技術の利用・運用に関する基準の有無

問 8-2. 貴社の暗号技術の利用・運用基準の内容として、あてはまるものを全てお選びください。



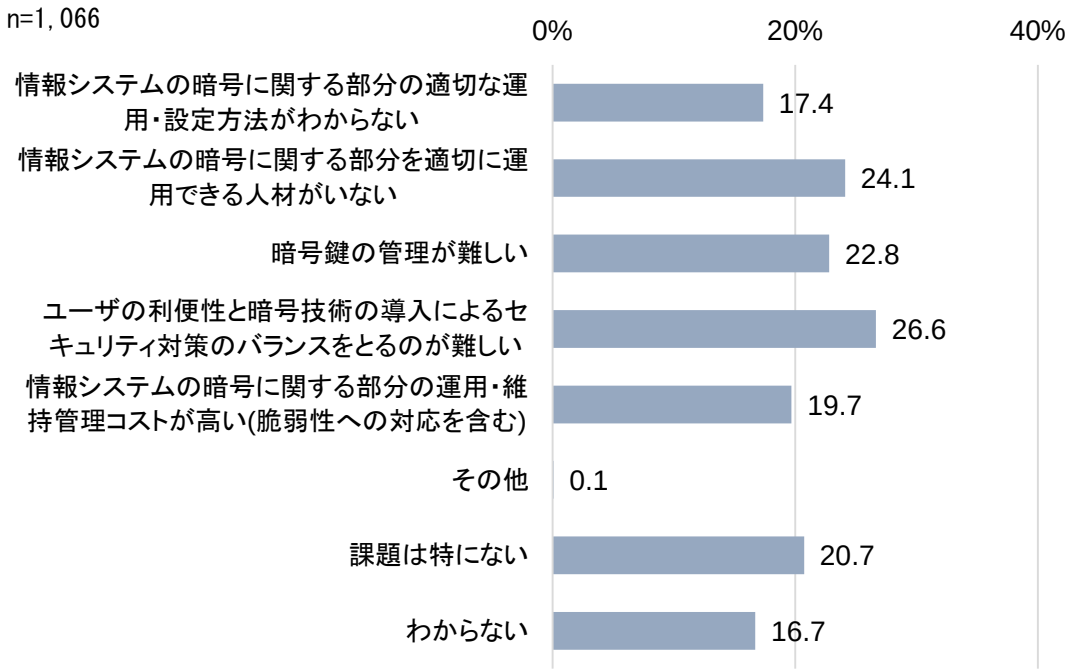
付録 1-20 暗号技術の利用・運用基準の内容（複数回答）

問 9. 貴社で暗号技術を利用・運用する際に責任を持つ部署はどこですか。



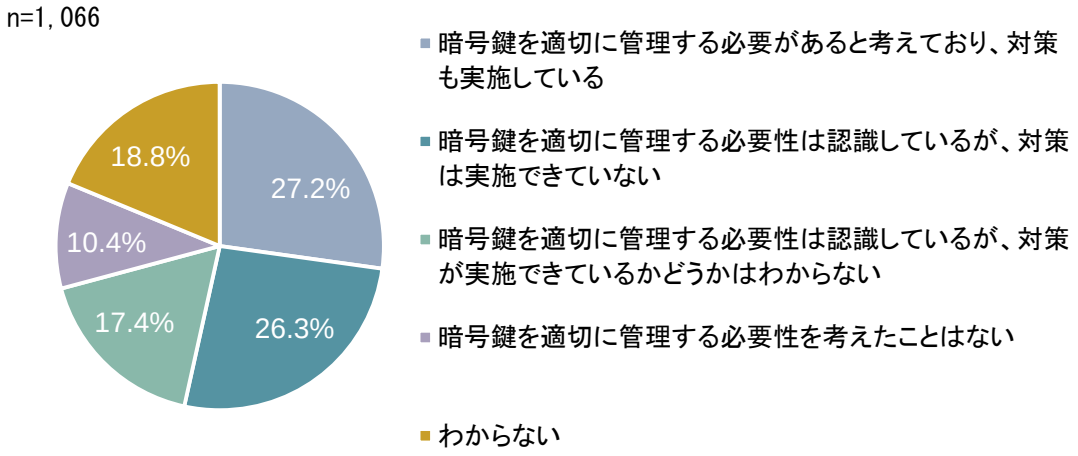
付録 1-21 暗号技術を利用・運用に関する責任部署

問 10. 貴社で暗号技術を利用・運用する際の課題として、あてはまるものを全てお選びください。



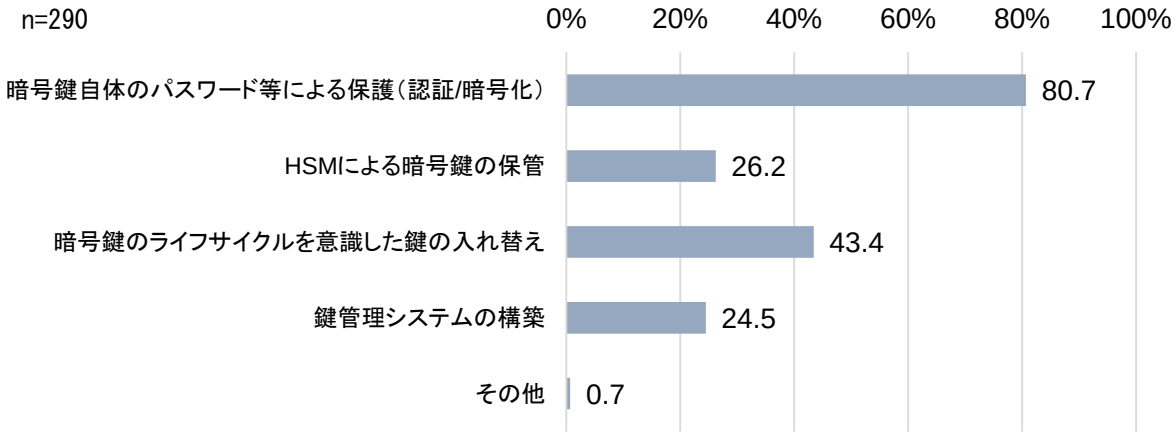
付録 1-22 暗号技術を利用・運用する際の課題（複数回答）

問 11-1. 貴社では、暗号鍵の管理についてどのように考えていますか。



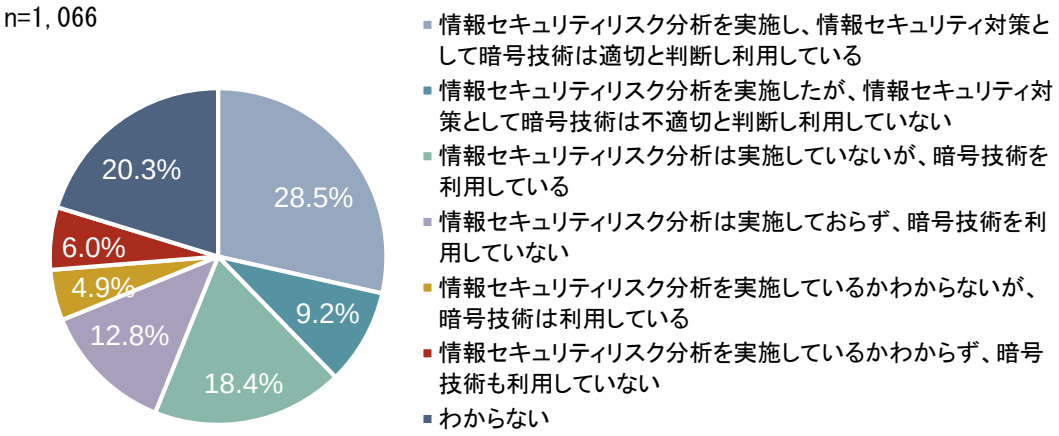
付録 1-23 暗号鍵管理の必要性認識と対策状況

問 11-2. 暗号鍵をどのように管理（セキュリティ対策）していますか。あてはまるものを全てお選びください。



付録 1-24 暗号鍵の管理方法（複数回答）

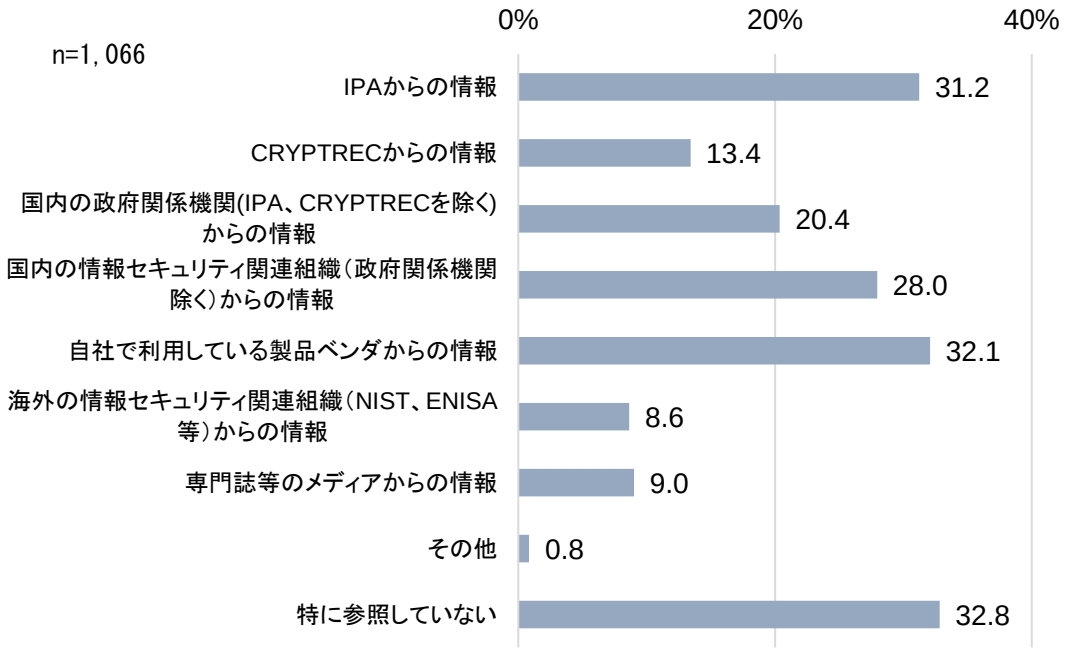
問 12. 貴社では、情報セキュリティリスク分析を実施したうえで、暗号技術を利用していますか。



付録 1-25 情報セキュリティリスク分析実施状況及び暗号技術利用状況

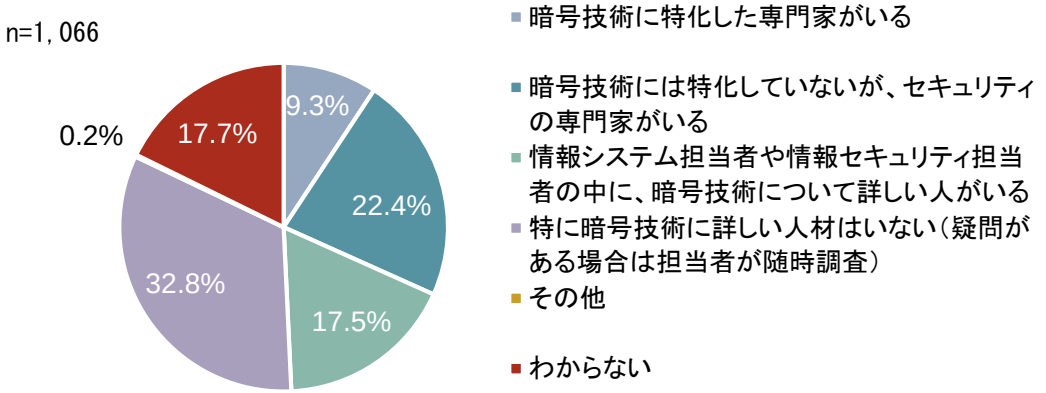
付録 1.4　暗号利活用に関する情報源

問 13.　貴社で暗号技術を利用する際に参照する情報としてあてはまるものを全てお選びください。



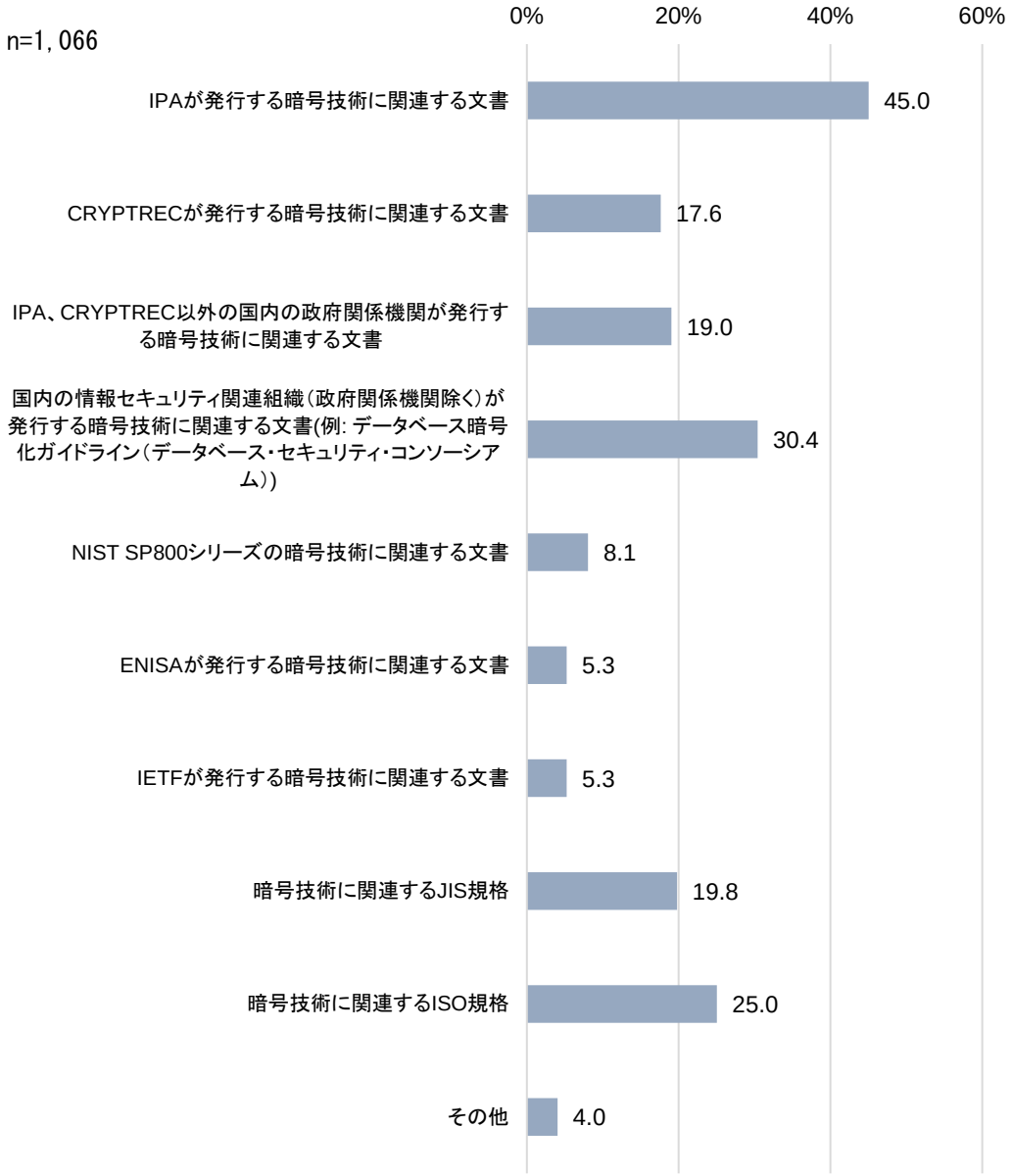
付録 1-26 暗号技術を利用する際に参照する情報（複数回答）

問 14.　貴社には暗号技術に詳しい人材（暗号や暗号技術について疑問があれば質問できるような人材）がいますか（回答者自身を含む）。



付録 1-27 暗号技術に関する人材

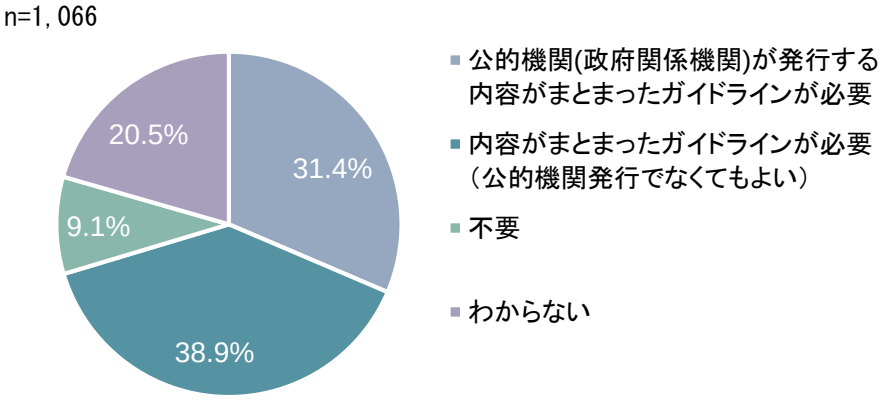
問 15. 貴社で暗号技術を利活用する際に参照しているガイドライン・文献としてあてはまるものを全てお選びください。



付録 1-28 暗号技術を利活用する際に参照するガイドライン・文献（複数回答）

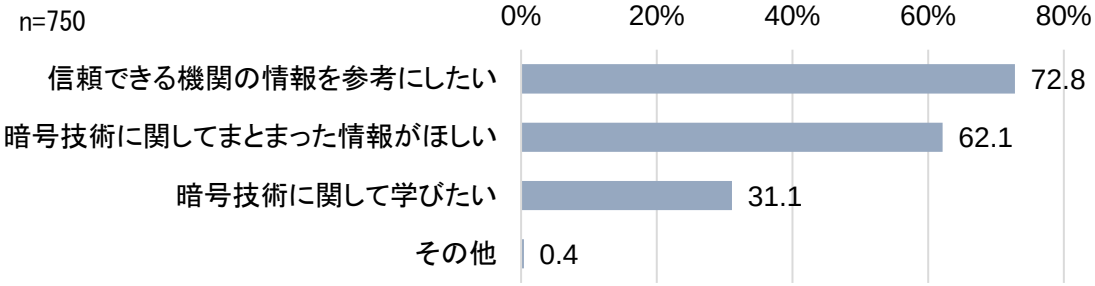
付録 1.5　暗号に関するガイドラインに対するニーズ

問 16-1. あなたは、暗号技術の利活用に関するガイドラインが必要と考えますか。



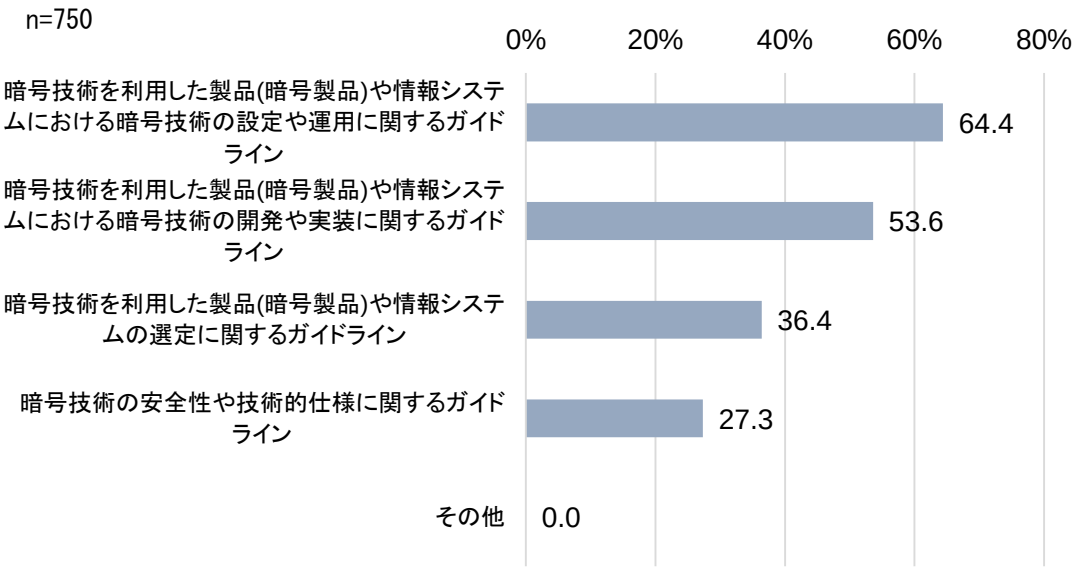
付録 1-29 暗号技術の利活用に関するガイドラインの必要性

問 16-2. ガイドラインを必要とする理由として、あてはまるものを全てお選びください。



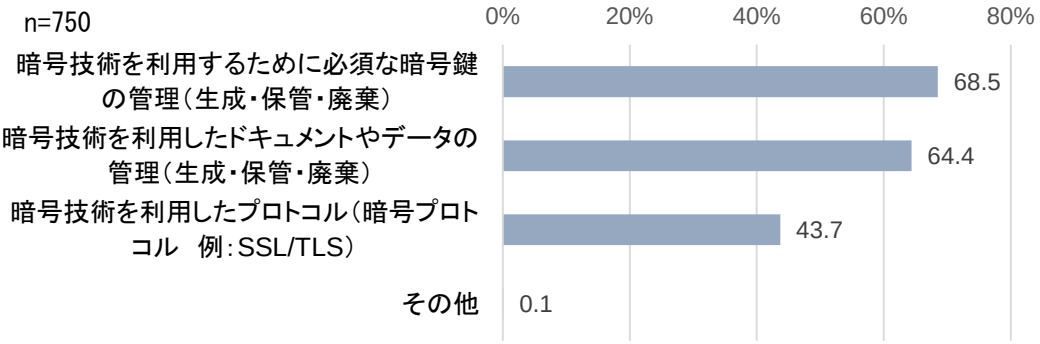
付録 1-30 ガイドラインを必要とする理由（複数回答）

問 17. あなたは、暗号技術に関するガイドラインを公的機関等が策定するとした場合、どのような種類のガイドラインがあるとよいと考えますか。あてはまるものを全てお選びください。



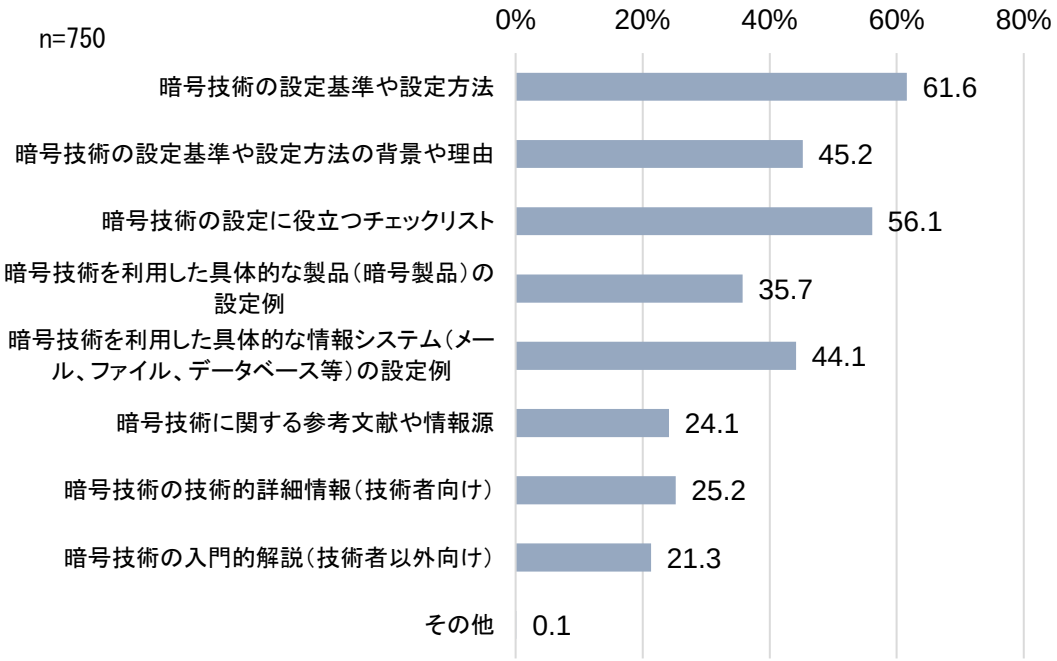
付録 1-31 暗号技術に関するガイドラインの種類（複数回答）

問 18. あなたは、暗号技術に関するガイドラインを公的機関等が策定するとした場合、どのようなテーマ（対象）のガイドラインがあるとよいと考えますか。あてはまるものを全てお選びください。



付録 1-32 暗号技術に関するガイドラインのテーマ（対象）（複数回答）

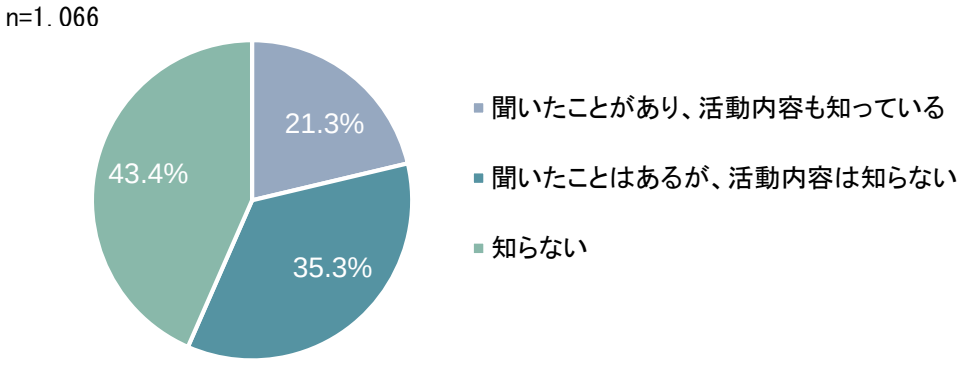
問 19. あなたは、暗号技術に関するガイドラインを公的機関等が策定するとした場合、どのような内容を盛り込んだガイドラインがあると役立つと考えますか。あてはまるものを全てお選びください。



付録 1-33 暗号技術に関するガイドラインの内容（複数回答）

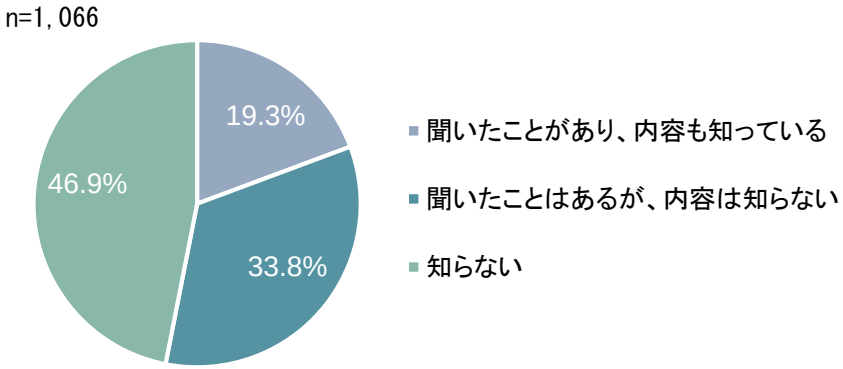
付録 1.6　暗号に関する組織・制度・技術の認知度

問 20.　あなたは、CRYPTREC について知っていますか。



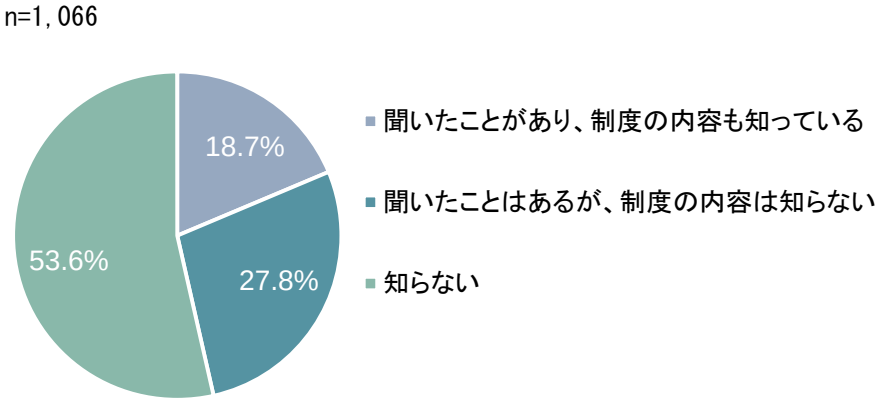
付録 1-34 CRYPTREC の認知度

問 21.　あなたは、CRYPTREC 暗号リストについて知っていますか。



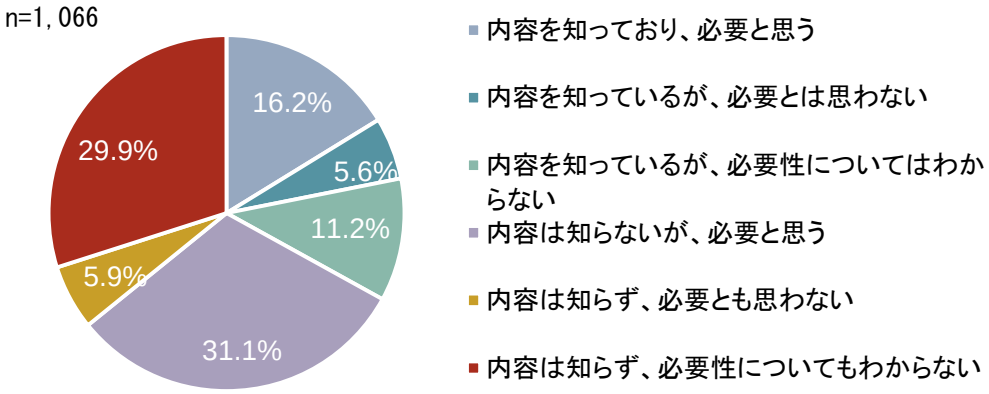
付録 1-35 CRYPTREC 暗号リストの認知度

問 22. あなたは、JCMVP（暗号モジュール試験及び認証制度）について知っていますか。



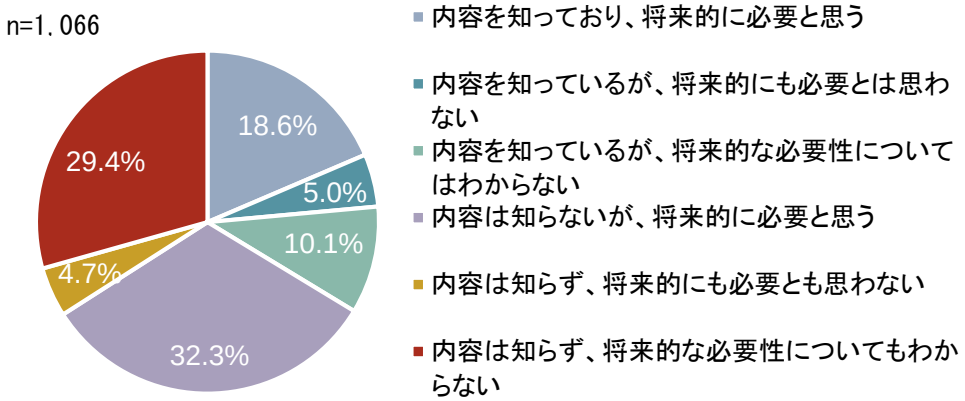
付録 1-36 JCMVP の認知度

問 23-1. あなたは軽量暗号について知っていますか。また、必要だと思いますか。



付録 1-37 軽量暗号の認知度と必要性

問 23-2. あなたは耐量子計算機暗号について知っていますか。また、将来的に必要だと思いますか。



付録 1-38 耐量子計算機暗号の認知度と必要性

付録２　国内外における暗号の利活用に関する文書の調査結果詳細

付録 2-1 SSL/TLS 暗号設定ガイドライン

題名	SSL/TLS 暗号設定ガイドライン
対象読者	SSL/TLS サーバを実際に構築するにあたって具体的な設定を行うサーバ構築者、実際のサーバ管理やサービス提供に責任を持つことになるサーバ管理者、並びに SSL/TLS サーバの構築を発注するシステム担当者
策定年・ 文書のバージョン番号	2015 年 5 月（初版）、2015 年 8 月（Ver.1.1） Ver.1.1
発行機関	CRYPTREC (Cryptography Research and Evaluation Committees)・IPA（情報処理推進機構）
言語	日本語
文書の種類・テーマ	対象読者が適切なセキュリティを考慮した暗号設定ができるようにするためのガイドライン 暗号に関して運用・設定する文書（特に暗号プロトコルに関するもの）
文書の位置づけ	法的義務はない
他の文書との関係	IPA 発行「安全なウェブサイトの作り方」とともに適切な暗号設定をする資料の 1 つとして使用することができる。 NISC 発行「政府機関等の情報セキュリティ対策のための統一基準群」で参照するように求められている。
概要	SSL/TLS 通信での安全性と可用性（相互接続性）のバランスを踏まえた SSL/TLS サーバの設定方法を説明したガイドライン。 「暗号技術以外の様々な利用上の判断材料も加味した合理的な根拠」を重視し、実現すべき安全性と必要となる相互接続性とのトレードオフを踏まえたうえで、実際に設定すべき「要求設定項目」として 3 つの設定基準（「高セキュリティ型」「推奨セキュリティ型」「セキュリティ例外型」）を提示。 第 1 章と第 2 章において、本ガイドラインの目的や SSL/TLS についての技術的な基礎知識をまとめたうえで、第 3 章で SSL/TLS サーバに要求される設定基準の概要について説明。 第 4 章から第 6 章では、第 3 章で定めた設定基準に基づき、プロトコルバージョン、サーバ証明書、暗号スイートについての具体的な SSL/TLS サーバの要求設定項目について示している。付録には、4 章から 6 章までの設定状況を確認するためのチェックリストが掲載されており、「選択した設定基準に対応した要求設定項目の設定忘れの防止」と「サーバ構築の作業受託先が適切に要求設定項目を設定したことの確認」を行うために利用できるように作られている。
目次	1. はじめに 2. 本ガイドラインの理解を助ける技術的な基礎知識 3. サーバ構築における設定要求項目について 4. プロトコルバージョンの設定 5. サーバ証明書の設定 6. 暗号スイートの設定 7. SSL/TLS を安全に使うために考慮すべきこと 8. ブラウザを利用する際に注意すべきポイント 9. その他のポイント 付録（チェックリスト、サーバ設定編、暗号スイートの設定例、ルート CA 証明書の取扱い）
URL	https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html

付録 2-2 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）

題名	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）
対象読者	情報システムの調達・運用の担当者、及びこれから依頼・指示されシステムの構築・運用を行う者
策定年・ 文書のバージョン番号	2008 年 7 月 初版
発行機関	IPA（独立行政法人情報処理推進機構）
言語	日本語
文書の種類・テーマ	暗号に関して運用・設定する文書（暗号プロトコル以外に関するもの） 暗号鍵管理に関するガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	米国 NIST SP 800-57 part 1 を参考とし作成した文書。
概要	本文書は、情報セキュリティシステムを維持するための暗号鍵の管理について生成から廃棄までのライフサイクルを考慮した管理手法を策定・確立することを目的とし、米国 NIST SP 800-57 part 1 を参照したうえで作成したものである。 第 2 章では鍵管理に関する全般的な記述を行い、第 3 章では鍵情報のライフサイクルと、各段階の概要、鍵情報のリスクと対策について一般論を示し、第 4 章では具体的な暗号利用場面における暗号鍵管理を示している。特に公開鍵技術を取りあげ、想定したシステムモデルにおける鍵管理について、管理上の脅威と対策の方向性を示す。 第 2 章「暗号の利用と鍵管理」では、暗号鍵の管理上の不備に基づく脅威事例を例示し、暗号の利用場面（PKI や蓄積データの暗号化、通信路の機密性確保、電子文書の長期保存、パスワード管理など）や暗号鍵の分類（署名生成鍵、署名検証鍵等）を説明している。また、暗号鍵の管理について、暗号鍵のライフサイクル（①生成②送付③利用④期限切れ⑤失効⑥廃棄）や鍵の有効期間設定、鍵危殆化の想定について解説。 第 3 章「暗号鍵ライフサイクル管理」では、①鍵の生成②鍵の配送③鍵の利用④鍵の保管／バックアップ⑤鍵の期限切れ／失効／廃棄⑥鍵の回復、のフェーズごとに考慮すべき事項を説明している。 第 4 章「PKI システムにおける暗号鍵ライフサイクル管理」は、ライフサイクルを考慮した暗号鍵管理の実際を具体的に示す例として PKI における公開鍵証明書の管理とセキュリティ対策について示している。
目次	1. はじめに 2. 暗号の利用と暗号鍵管理 3. 暗号鍵ライフサイクル管理 4. PKI システムにおける暗号鍵ライフサイクル管理
URL	https://www.ipa.go.jp/security/fy19/reports/Key_Management/index.html

付録 2-3 情報漏えいを防ぐためのモバイルデバイス等設定マニュアル
～安心・安全のための暗号利用法～

題名	情報漏えいを防ぐためのモバイルデバイス等設定マニュアル～安心・安全のための暗号利用法～
対象読者	セキュリティ対策実施の責任者・担当者に加え企業・組織の全従業員、個人
策定年・ 文書のバージョン番号	2013 年 4 月 初版
発行機関	独立行政法人情報処理推進機構
言語	日本語
文書の種類・テーマ	暗号を利用したシステムの運用もしくはマネジメントに関する文書、及び特定の製品・サービスの利用に関する文書 情報漏えい対策としての暗号利用について具体的な対策等を解説した文書
文書の位置づけ	法的義務はない
他の文書との関係	
概要	モバイルデバイスの紛失等による情報漏えいトラブルの回避策を利用者が自ら行えるよう、情報の重要度にあわせた対策と、端末や可搬媒体ごとの対策を示したもの。「解説編」と「実践編」の 2 部で構成。 「解説編」では、暗号製品が情報漏えい対策として正しく機能するために最低限知る必要がある事項として、暗号化の必要性や暗号化の仕組み、暗号を利用する際の注意事項（暗号アルゴリズムの脆弱性、正規の利用者へのなりすまし等）、暗号化が正しく安全に機能するための必要事項（電子政府推奨暗号リストの利用や認証等）について解説。さらに、情報価値レベルと端末・可搬媒体別に求められる対策レベルを説明。 「実践編」では、端末ロックやファイルの暗号化等に関して具体的に実施すべき対策を示している。また、情報漏えいの 3 つのユースケースに基づき、想定すべきリスクと実施すべき対策の例を示している。さらに、広く利用されている代表的な製品（Windows7、Windows8、iOS6 等）について、具体的な情報漏えい対策の設定方法を示している。
目次	解説編 1. はじめに 2. 情報漏えい対策が正しく機能するために知っておくべきこと 3. 暗号化による情報漏えい対策の実施方法～ベースライン対策～ 対策編 実践編Ⅰ 情報保護対策の具体的手法例 実践編Ⅱ ユースケースと対策例 実践編Ⅲ 代表的な製品の具体的な設定方法の実例
URL	https://www.ipa.go.jp/security/ipg/documents/dev_setting_crypt.html

付録 2-4 CRYPTREC 暗号技術ガイドライン (SHA-1)

題名	CRYPTREC 暗号技術ガイドライン (SHA-1)
対象読者	電子政府のシステム調達者及び電子政府システムを構築する関係者
策定年・ 文書のバージョン番号	2014 年 3 月 初版
発行機関	CRYPTREC (Cryptography Research and Evaluation Committees)・NICT（情報通信研究機構）・IPA（情報処理推進機構）
言語	日本語
文書の種類・テーマ	CRYPTREC 暗号リストの運用監視暗号リストに記載されているハッシュ関数 SHA-1 を利用する際に必要となる情報を示したガイドライン 暗号の運用・設定に関する文書（暗号プロトコル以外に関するもの）
文書の位置づけ	法的義務はない
他の文書との関係	本書は、内閣官房情報セキュリティセンター（現：内閣官房内閣サイバーセキュリティセンター）が公表した「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」に基づいて作成されている。また、CRYPTREC は暗号技術ガイドラインとして「SSL/TLS における近年の攻撃への対応」に関する暗号技術ガイドラインも発行しており、CRYPTREC 発行「SSL/TLS 暗号設定ガイドライン」では、本書を参照している。 なお、NIST SP 800-131A「暗号アルゴリズムと鍵長の使用移行にかんする推奨事項」においては、デジタル署名生成の SHA-1 の使用は 2013 年以降許容されないことが述べられている。
概要	CRYPTREC 暗号リストの運用監視暗号リストに記載されているハッシュ関数 SHA-1 を利用する際に必要となる情報を示す文書。SHA-1 の利用範囲に関して、非推奨及び推奨事項を第 2 章で説明。 SHA-1 の利用について、「電子署名における署名作成」に関しては SHA-1 の利用は非推奨とし、許容される利用範囲としては「電子署名における署名検証」、「メッセージ認証のための鍵付ハッシング（HMAC）」「鍵導出関数（KDF）」「擬似乱数生成系」「パスワード・ハッシングやチェックサムの計算としての利用(hash-only applications)」の 5 分野をあげている。 第 3 章では、第 2 章で述べられた利用範囲に関する参考情報を NIST SP800 から引用し、記載。
目次	1. 本書の位置づけ 2. ハッシュ関数 SHA-1 の利用について 3. 参考情報 4. 参考文献
URL	http://www.cryptrec.go.jp/report/c13_kentou_gjji02_r3.pdf

付録 2-5 2008 年度版リストガイド（秘匿の暗号利用モード）

題名	2008 年度版リストガイド（秘匿の暗号利用モード）
対象読者	（記載なし）
策定年・ 文書のバージョン番号	2009 年 3 月 初版
発行機関	CRYPTREC (Cryptography Research and Evaluation Committees)、独立行政法人情報通信研究機構、独立行政法人情報処理推進機構
言語	日本語
文書の種類・テーマ	暗号の開発実装に関連する文書 共通鍵ブロック暗号アルゴリズムとともに用いるべき利用モードを示すガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	本文書で示した利用モードとともに用いるべきブロック暗号に関しては、CRYPTREC が定めた電子政府推奨暗号リストを参照するよう求めている。
概要	本文書では、共通鍵ブロック暗号アルゴリズムとともに用いるべき利用モードとして、以下の 5 つの利用モードについて技術内容・利用時の推奨事項の解説及び仕様の定義を行っている。 ・ Cipher Block Chaining (CBC) ・ Cipher Feedback(CFB) ・ Counter (CTR) ・ Electronic Codebook (ECB) ・ Output Feedback (OFB) 本技術では、暗号化処理により元の情報 (平文と呼ぶ) から暗号文を生成することで、情報の秘匿を実現する。 1.2 節で用語や記法、数学的記述などを示し、1.3 節で扱う技術について以下の順で解説。 ・ 暗号技術の利用モデル（一般的な枠組みとしてどのようなモデルで利用するか） ・ 技術の基本的構成（関連する他の技術やその運用） ・ 評価観点と比較（本文書で扱う 5 つのモードの違いや選択の方法を解説） ・ そして、1.4 節にて個々のモードの仕様を記述し、1.5 節では動作をより正確に理解するための具体的なデータ例 (テストベクトル) を示している。
目次	1. 秘匿の暗号利用モード 1.1. 本文書の位置づけ 1.2. 定義 1.3. 技術概要 1.4. 実装仕様 1.5. テストベクトル
URL	http://www.cryptrec.go.jp/report/c08_listguide2008_mode_v7.pdf

付録 2-6 2008 年度版リストガイド（メッセージ認証コード）

題名	2008 年度版リストガイド（メッセージ認証コード）
対象読者	（記載なし）
策定年・ 文書のバージョン番号	2009 年 3 月 初版
発行機関	CRYPTREC (Cryptography Research and Evaluation Committees)、独立行政法人情報通信研究機構、独立行政法人情報処理推進機構
言語	日本語
文書の種類・テーマ	暗号の開発実装に関連する文書 ハッシュ関数ベースのメッセージ認証コードである HMAC、ブロック暗号ベースのメッセージ認証コードである CBC-MAC 及び CMAC の技術概要及び実装仕様を記述するガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	HMAC 内で使用するハッシュ関数として、電子政府推奨暗号リストに記載されたハッシュ関数の使用を推奨。 1 つの鍵で MAC 生成を行うメッセージ数の選択基準として、NIST の SP800-38B" Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication" の付録 B に記載されている指針を参考にすることを推奨。
概要	本文書は、ハッシュ関数ベースのメッセージ認証コードである HMAC、ブロック暗号ベースのメッセージ認証コードである CBC-MAC 及び CMAC の技術概要及び実装仕様について解説したもの。 1.3 節でメッセージ認証コードの利用モデルやメッセージ認証コード技術の基本的構成（MAC 生成アルゴリズム及び MAC 検証アルゴリズム）について解説。さらにメッセージ認証コードである、HMAC・CBC-MAC・CMAC について、技術概要及び主な特徴を示し比較。 1.4 節で HMAC, CBC-MAC,CMAC それぞれについて実装仕様を解説。
目次	1. メッセージ認証コード 1.1. 本文書の位置づけ 1.2. 定義 1.3. 技術概要 1.4. 実装仕様
URL	http://www.cryptrec.go.jp/report/c08_listguide2008_mac_v7.pdf

付録 2-7 2008 年度版リストガイド（電子署名）

題名	2008 年度版リストガイド（電子署名）
対象読者	（記載なし）
策定年・ 文書のバージョン番号	2009 年 3 月 初版
発行機関	CRYPTREC (Cryptography Research and Evaluation Committees)、独立行政法人情報通信研究機構、独立行政法人情報処理推進機構
言語	日本語
文書の種類・テーマ	暗号の開発実装に関連する文書 FIPS 186-3 Draft 記載の (楕円) 離散対数問題ベースの電子署名技術である DSA, ECDSA、及び RSA PKCS#1 v.2.1 記載の素因数分解問題 (RSA 問題) ベースの RSASSA-PKCS1-v1 5, RSASSA-PSS の技術概要、及び実装仕様を記述するガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	電子署名技術「DSA」については、NIST FIPS 186-3 Draft の推奨事項をベースに記述されている。 電子署名技術「ECDSA」については、FIPS 186-3 Draft をベースに説明を行い、必要に応じて ANS X9.62 版との違いを説明。
概要	本文書では、FIPS 186-3 Draft 記載の (楕円) 離散対数問題ベースの電子署名技術である DSA, ECDSA、及び RSA PKCS#1 v.2.1 記載の素因数分解問題 (RSA 問題) ベースの RSASSA-PKCS1-v1 5, RSASSA-PSS の技術概要、及び実装仕様について解説。 1.3 節では、電子署名に関する暗号技術の利用モデル及び技術の基本的構成（鍵生成（アルゴリズム）・署名生成（アルゴリズム）・署名検証（アルゴリズム））について解説。また、本文書で解説する電子署名技術である「DSA」、「ECDSA」、「RSASSA-PKCS1-v1 5」、「RSASSA-PSS」の概要と安全性について説明。 1.4 節では、「DSA」、「ECDSA」、「RSASSA-PKCS1-v1 5」、「RSASSA-PSS」の実装仕様を説明。
目次	1. 電子署名 1.1. 本文書の位置づけ 1.2. 用語及び略語 1.3. 技術概要 1.4. 実装仕様
URL	http://www.cryptrec.go.jp/report/c08_listguide2008_signature_v7.pdf

付録 2-8 2010 年度版リストガイド（鍵管理）

題名	2010 年度版リストガイド（鍵管理）
対象読者	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、並びに、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及び運用者
策定年・ 文書のバージョン番号	2011 年 6 月 初版
発行機関	CRYPTREC (Cryptography Research and Evaluation Committees)
言語	日本語
文書の種類・テーマ	暗号に関して運用・設定する文書（暗号プロトコル以外に関するもの） 暗号鍵の管理に係る「生成」、「有効期限」、「廃棄」、「更新」、「鍵が露呈した場合の対処」等の各手順に関する推奨される考え方並びに関連する情報提供を行うためのガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	「政府機関の情報セキュリティ対策のための統一基準（第 4 版）」で策定が求められている暗号鍵の管理手順の各フェーズについて、取りまとめたもの。 CRYPTREC の活動内容及び NIST SP 800-57 等の情報を集約。
概要	電子政府推奨暗号リストに掲載された暗号の利用を促進し、暗号を安全かつ適切に利用するための暗号鍵管理の指針を提供することを目的とした文書。「政府機関の情報セキュリティ対策のための統一基準（第 4 版）」に基づき、CRYPTREC の活動内容及び米国 NIST SP 800-57 等を参照し作成。 本文書では、暗号鍵の管理に係わる「生成」、「有効期限」、「廃棄」、「更新」、「鍵が露呈した場合の対処」等について、利用する暗号方式に応じて「公開鍵暗号技術」（第 3 章）と「共通鍵暗号技術」（第 4 章）に分けて、手順や推奨事項等を説明。公開鍵暗号技術・共通鍵暗号技術の利用にあたっては、電子政府推奨暗号リストに記載されている暗号の選択を強く求めている。 公開鍵暗号技術・共通鍵暗号技術それぞれについて具体的な指針や運用例を、「利用モデル（公開鍵暗号技術に関しては署名・認証・否認防止、共通鍵暗号技術に関しては暗号化・メッセージ認証コードを例示）」、「鍵の生成手順」、「鍵の有効期間の設計指針」、「鍵の更新手順」、「鍵の廃棄手順」、「鍵が漏えいした場合のリスクを低減する方法」、「鍵の保存手順」の各項目について解説している。 また、公開鍵暗号及び共通鍵暗号で共通する鍵の管理・保護策については第 5 章で、「鍵を転送する場合の鍵の保護」と「ストレージ上での鍵の保護」の 2 つの観点から解説。 「鍵を転送する場合の鍵の保護」については、「手動で鍵を配送する場合」と「通信プロトコルを介して電子的に配送する場合」を想定し、①可用性②完全性③守秘性④用途またはアプリケーションとの関係性⑤他のエンティティとの関係性⑥他の関連情報との関係性、の 6 つの観点から考慮すべき事項等を整理している。 「ストレージ上での鍵の保護」についても上記①～⑥の観点で考慮すべき事項等を整理。
目次	1. 本文書の位置づけ 2. 定義 3. 公開鍵暗号技術の鍵管理 4. 共通鍵暗号技術の鍵管理 5. 共通項目
URL	http://www.cryptrec.go.jp/report/c10_guide2010_keymanagement_final.pdf

付録 2-9 2011 年度版リストガイド（SSL/TLS）

題名	2011 年度版リストガイド(SSL/TLS)
対象読者	電子政府のシステム調達者及び電子政府システムを構築する開発者
策定年・ 文書のバージョン番号	2012 年 3 月 初版
発行機関	CRYPTREC (Cryptography Research and Evaluation Committees)・NICT（情報通信研究機構）・IPA（情報処理推進機構）
言語	日本語
文書の種類・テーマ	暗号に関して運用・設定する文書（特に暗号プロトコルに関するもの） SSL/TLS を利用する際に必要となる情報並びに推奨事項を示したリストガイド
文書の位置づけ	法的義務はない
他の文書との関係	リストガイドは 3 つのプロトコル（DNSSEC, IPsec, SSL/TLS）に関してそれぞれ発行されており、本文書はそのうち SSL/TLS に関する文書である。
概要	電子政府をはじめとしてよく利用されている SSL/TLS について、その利用方法並びに選択すべき暗号アルゴリズムについて情報提供を行う文書。 電子政府において利用可能な暗号スイートを選定するために必要な情報を 2.2 章では示しており、利用を推奨する暗号スイートの一覧が示されている。 推奨する暗号スイートを適切に利用する場合は、TLS 1.1/1.2 の利用が望ましいとし、最新の OS の導入を進め、各種ブラウザの TLS 1.1/1.2 への対応にあわせて、適切にバージョンアップを行える OS 環境に移行することが望ましいとしている。 付録では 2012 年 3 月現在での、Windows 環境下での各ブラウザ（IE, Firefox, Google Chrome, Safari）における SSL/TLS の利用可能性を整理。
目次	1. 本文書の位置づけ 2. SSL/TLS に関する推奨 付録 A SSL/TLS の実行環境ごとの利用可能性
URL	http://www.cryptrec.go.jp/report/c11_guide2011_TLS-f3.pdf

付録 2-10　2011 年度版リストガイド（IPsec）

題名	2011 年度版リストガイド（IPsec）
対象読者	電子政府のシステム調達者及び電子政府システムを構築する開発者
策定年・ 文書のバージョン番号	2012 年 3 月 初版
発行機関	CRYPTREC (Cryptography Research and Evaluation Committees)、独立行政法人情報通信研究機構、独立行政法人情報処理推進機構
言語	日本語
文書の種類・テーマ	暗号に関して運用・設定する文書（特に暗号プロトコルに関するもの） IPsec を利用する際に必要となる情報並びに推奨事項を示したリストガイド
文書の位置づけ	法的義務はない
他の文書との関係	推奨する暗号スイートに関しては、「電子政府推奨暗号リスト」を前提としている。 IPsec に関連した標準として、RFC 及び NIST の文章を参照。
概要	電子政府をはじめとして、よく利用されている IPsec に関して、その利用方法並びに選択すべき暗号アルゴリズムについて情報提供を行う文章。本文書で推奨する暗号スイートは、電子政府推奨暗号リストに記載されている暗号アルゴリズムの利用を前提としている。 IPsec に関する推奨事項として各種標準で規定されている暗号スイートについて説明。RFC に関しては IPsec 用暗号スイートの RFC4308”Cryptographic Suites for IPsec”、IPsec 用 Suite B 暗号スイートに関しては RFC6379” Suite B Cryptographic Suites for IPsec”を参照している。他にも、IANA 暗号アルゴリズム ID 及び NIST SP800-57,Part3”Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance”を参照。 電子政府において利用される暗号スイートの中で、IPsec の利用を推奨するものとして、以下に関してリストをあげている。 ・ AH 及び ESP の認証アルゴリズムの推奨暗号スイート ・ ESP 暗号化 推奨暗号スイート ・ IKEv1 推奨暗号スイート ・ IKEv1 ハッシュアルゴリズム ・ IKEv1 認証アルゴリズム ・ IKEv2 推奨暗号スイート
目次	本文書の位置づけ 1. 定義と表記 2. IPsec に関する推奨
URL	http://www.cryptrec.go.jp/report/c11_guide2011_IPsec.pdf

付録 2-11　2011 年度版リストガイド（DNSSEC）

題名	2011 年度版リストガイド（DNSSEC）
対象読者	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、並びに、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及び運用者
策定年・ 文書のバージョン番号	2012 年 3 月 初版
発行機関	CRYPTREC (Cryptography Research and Evaluation Committees)、独立行政法人情報通信研究機構、独立行政法人情報処理推進機構
言語	日本語
文書の種類・テーマ	暗号に関して運用・設定する文書（特に暗号プロトコルに関するもの） DNSSEC を運用する際に選択すべき暗号アルゴリズムについて情報提供を行うリストガイド
文書の位置づけ	法的義務はない
他の文書との関係	推奨する暗号スイートに関しては、「電子政府推奨暗号リスト」を前提としている。 ゾーン署名で利用できる暗号アルゴリズムに関しては IETF の RFC を参照（RFC4034、2539 等）。 また、KSK（Key Signing Key:署名検証鍵）と ZSK(Zone Signing Key:ゾーン署名鍵) に関しては、IETF の RFC 及び NIST の文章を参照。
概要	政府機関における電子政府システムの調達、並びに、運用において、DNSSEC 利用時の鍵生成に必要となる暗号鍵のアルゴリズムと鍵長に関する推奨事項並びに関連する情報提供を行うことを目的とした文書。電子政府で利用する DNSSEC における暗号スイートを示している。 3.1 節では、ネームサーバのソフトウェア・バージョンによる制約として、①DNSSEC で利用できる暗号アルゴリズム、②DNSSEC における不在証明（存在しないドメイン名が偽造されるのを防ぐための証明）の必要、③ネームサーバごとの制約、を説明。ネームサーバごとの制約に関する説明としては、BIND9、NSD、Unbound を例に、各ネームサーバで利用できる暗号スイートを示す。 3.2 節では、関連する RFC や NIST の文章を紹介する形で、KSK (Key Signing Key:署名検証鍵) 及び ZSK (Zone Signing Key:ゾーン署名鍵) に対する推奨事項を説明し、電子政府で利用する DNSSEC における推奨暗号スイートのリスト及び KSK と ZSK の鍵長を示している。
目次	1. 本文書の位置づけ 2. 定義と表記 3. DNSSEC に関する推奨
URL	http://www.cryptrec.go.jp/report/c11_guide2011_DNSSEC.pdf

付録 2-12 SSH サーバセキュリティ設定ガイド

題名	SSH サーバセキュリティ設定ガイド
対象読者	企業･個人を問わず、SSH サーバの構築･運用に関わる者で、TCP/IP 等のネットワークの基本的な仕組みを理解している者
策定年・ 文書のバージョン番号	2015 年 3 月（初版）、2015 年 3 月（1.0 版 Rev.1） 1.0 版 Rev.1
発行機関	日本コンピュータセキュリティインシデント対応チーム協議会（日本シーサート協議会）
言語	日本語
文書の種類・テーマ	暗号に関して運用・設定する文書（特に暗号プロトコルに関するもの） SSH サーバをサイバー攻撃から守るためのセキュリティ設定について解説するガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	―
概要	本文書は、サーバのリモート保守やファイル転送などで利用される SSH サービスについて、SSH サーバをサイバー攻撃から守るためのセキュリティ設定について解説したもの。 主な推奨事項は第 4 章に記載されており、「ネットワークサービス」、「SSH サービス」、「鍵管理」について、①設定方法（設定はどのようにすればよいのか）、②確認方法（設定をどのように確認すればよいのか）、③参考情報から構成されている。また、4 章の推奨事項を一覧化したチェックリストが第 3 章にある。 ネットワークの推奨事項として、以下の項目があげられている。 ・ 不要なサービスを停止／無効化する ・ 特定のホストからの接続だけを許可する SSH サービスの推奨事項として、以下の項目があげられている。 ・ SSH プロトコルのバージョン 2 のみを許可する ・ 公開鍵認証を使用する（パスワード認証を無効化する） ・ ポートフォワードを止める ・ SSH サービスを 22/TCP 以外で稼働させる ・ known_hosts ファイルをハッシュ化する 鍵管理の推奨事項として、以下の項目があげられている。 ・ ユーザ秘密鍵ファイルにパスフレーズをつけること ・ SSH サーバ上にユーザ秘密鍵ファイルを置かない
目次	1. はじめに 2. 前提条件 3. チェックリスト 4. SSH サーバの要塞化 付録 A 利用形態別ガイド . 付録 B SSH 関連コマンド 付録 C クラウドでのセキュリティ設定 .ブラウザを利用する際に注意すべきポイント 付録 D WINDOWS 環境での SSH-AGENT 利用
URL	http://www.nca.gr.jp/imgs/nca_ssh_server_config_v01.pdf

付録 2-13 データベース暗号化ガイドライン（1.0 版）

題名	データベース暗号化ガイドライン（1.0 版）
対象読者	データベース・セキュリティに携わる責任者
策定年・ 文書のバージョン番号	2011 年 9 月（第 0.9 版）、2011 年 11 月（第 1.0 版） 第 1.0 版
発行機関	データベース・セキュリティ・コンソーシアム
言語	日本語
文書のテーマ・種類	暗号を利用したシステムの運用もしくはマネジメントに関する文書 データベース（DB）における暗号化を実装するうえで必要となる事象について言及したガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	データベース・セキュリティ・コンソーシアムの「DB 内部不正対策ガイドライン」で参照するよう求められている。
概要	DB の暗号化対策として、データそのものの暗号化だけでなく、「暗号鍵の管理」、「通信経路の暗号化」も含めたものを DB 全体の暗号対策として定義し、それぞれの対策度合いに応じて、各脅威に対する対応レベルを設けている。 DB の暗号化については、「HDD 暗号化」、「DB テーブル暗号化」、「DB カラム暗号化」及び「バックアップテープ暗号化」に分類し、各暗号化導入の概要とそのメリット・デメリット、そして導入に際する必須事項・推奨事項を明記。 暗号鍵の管理については、「ファイルとしての暗号鍵管理」、「専用ハードウェアでの暗号鍵管理」、「暗号鍵のアクセス制御」、「鍵の世代管理」に分類し、各項目の概要とそのメリット・デメリット、そして導入に際する必須事項・推奨事項を明記。 通信経路の暗号化については、その経路を「DB-アプリケーション間」、「DB-管理者端末間」、「DB-鍵管理デバイス間」の 3 つに分類し、それぞれの経路に関して、同様に概要とそのメリット・デメリット、そして導入に際する必須事項・推奨事項を明記。 第 6 章では、実際の DB 暗号化導入事例を示している。
目次	1. はじめに 2. DB 暗号化概略 3. DB の暗号化 4. 暗号鍵管理 5. 通信経路の暗号化 6. DB 暗号化導入事例 7. DB 暗号化ガイドライン執筆者
URL	http://www.db-security.org/report/dbsc_cg_ver1.0.pdf

付録 2-14 テープストレージの暗号化機能に関するチェックリスト

題名	情報漏えいを防ぐためのモバイルデバイス等設定マニュアル～安心・安全のための暗号利用法～
対象読者	IT システムの統括者・構築者・運用者
策定年・ 文書のバージョン番号	2013 年 5 月 初版
発行機関	JEITA（一般社団法人電子情報技術産業協会） テープストレージ専門委員会
言語	日本語
文書の種類・テーマ	暗号を利用したシステムの運用もしくはマネジメントに関する文書 情報漏えい対策としての暗号利用について具体的な対策等を解説した文書
文書の位置づけ	法的義務はない
他の文書との関係	―
概要	テープストレージにデータを保管する際のデータ暗号化を対象として作成されたチェックリスト。ユーザの求めるセキュリティレベルごとやシステムに対するユーザの立場（統括者、構築者、運用者）ごとにどのようなチェック項目があるかをまとめている。チェックリストにより、データ暗号化システムを構築・運用・廃棄する際に考慮すべき事項、適切なシステム環境となっているかを判断することを可能としている。 第 3 章では、データ暗号化に対する社会的要請の高まりや各種法規制（個人情報保護法、会社法、米国 SOX 法等）、データ漏えい時の影響等について説明している。 第 4 章では、テープストレージの優位性について解説している。 第 5 章ではデータ暗号化技術に関して、基本的な暗号化方式（共通鍵暗号方式・公開鍵暗号化方式）、鍵長と安全性、鍵管理の重要性について説明している。 第 7 章では、「検討／計画」・「設計／構築」・「運用」・「障害／災害」・「データ移行」・「終了／停止」の各フェーズにおける検討すべき事項や具体的な実装方法等について解説し、各フェーズで解説された検討事項等は付録のチェックリストとしてまとめられている。
目次	1. はじめに 2. 本チェックリストの対象者 3. 社会的動向によるデータ暗号化への要請 4. テープストレージの優位性 5. データ暗号化技術 6. 達成したい機密性・厳密性 7. 各フェーズにおけるチェック項目 付録 テープストレージの暗号化機能に関するチェックリスト
URL	http://home.jeita.or.jp/upload_file/20130924142250_Va5Ube6RwL.pdf

付録 2-15 SP 800-22 Rev. 1a “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications”

題名	SP 800-22 Rev. 1a “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications”
対象読者	組織における擬似乱数生成器のテスト担当者
策定年・ 文書のバージョン番号	2010 年 4 月（Rev. 1a） Rev. 1a
発行機関	NIST (National Institute of Standards and Technology)
言語	英語
文書の種類・テーマ	暗号に関して運用・設定に関する文書（暗号プロトコル以外に関するもの） 乱数生成器と擬似乱数発生器の選択と検定について解説した文書
文書の位置づけ	法的義務はない
他の文書との関係	擬似乱数生成器の選択の際には、FIPS 180「安全なハッシュの基準」で規定されているセキュアハッシュアルゴリズムとデータ暗号化規格を使用する必要があると述べている。 初版では、「Lempel-Ziv 圧縮検定」を含む計 16 個の検定項目があげられていたが、改訂版ではこの検定項目が削除されている。
概要	暗号鍵の生成などに用いられる乱数発生器と擬似乱数発生器に関する、選択と検定等について解説したガイドライン。特に、これらの生成器のランダム性検定について説明。 第 2 章では、15 個の検定項目で構成される NIST 乱数検定スイートのそれぞれに関して、そのテストの概要を説明し、第 3 章では、各検定の数学的背景と技術的な詳細を提供。 具体的な 15 個の検定項目は以下の通り: 1. 頻度検定（The Frequency (Monobit) Test） 2. ブロック単位の頻度検定（Frequency Test within a Block） 3. 連検定（The Runs Test） 4. ブロック単位の最長連検定（Tests for the Longest-Run-of-Ones in a Block） 5. 2 値行列ランク検定（The Binary Matrix Rank Test） 6. 離散フーリエ変換検定（The Discrete Fourier Transform (Spectral) Test） 7. 重なりのないテンプレート適合検定（The Non-overlapping Template Matching Test） 8. 重なりのあるテンプレート適合検定（The Overlapping Template Matching Test） 9. Maurer のユニバーサル統計量検定（Maurer's "Universal Statistical" Test） 10. 線形複雑度検定（The Linear Complexity Test） 11. 系列検定（The Serial Test） 12. 近似エントロピー検定（The Approximate Entropy Test） 13. 累積和検定（The Cumulative Sums (Cusums) Test） 14. ランダム回遊検定（The Random Excursions Test） 15. 変形ランダム回遊検定（The Random Excursions Variant Test） 第 4 章では、検定戦略、検定結果の解釈方法と、一般的な推奨事項について説明し、第 5 章では、NIST の擬似乱数評価ツールの検定の設定と、実行のためのユーザガイドを提供。
目次	1. 乱数検定の概要 2. 乱数生成テスト 3. 検定の技術的説明 4. 検定戦略と結果の解釈 5. ユーザガイド 付録 A ソースコード 付録 B サンプルデータの実証結果 付録 C 検定スイートの拡張 付録 D 参照擬似乱数発生器の説明 付録 E 数値アルゴリズムの問題 付録 F サポートソフトウェア 付録 G 参考文献
URL	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf

付録 2-16 SP 800-52 Rev. 1 “Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations”

題名	SP 800-52 Rev. 1 “Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations”
対象読者	主に連邦政府利用者及びシステム管理者
策定年・ 文書のバージョン番号	2014 年 4 月 (Rev. 1) Rev. 1
発行機関	NIST (National Institute of Standards and Technology)
言語	英語
文書の種類・テーマ	暗号に関して運用・設定する文書（暗号プロトコルに関するもの） TLS 実装の選択、設定及び使用のためのガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	TLS 実装には公開鍵証明書 を生成する公開鍵基盤の存在を必要としており、これに関して SP 800-32 ”Introduction to Public Key Technology and the Federal PKI Infrastructure”を参照すべきとし、RSA などの鍵生成に関するガイダンスについては SP 800-56A Rev.2 “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”を参照するよう書かれている。また、クライアント公開鍵証明書で提示される鍵長に関しては、SP 800-131A ” Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths”で提供される鍵長ガイドラインを使用しなければならないとしている。
概要	承認された暗号運用とアルゴリズムを効果的に使用する際の TLS 実装の選択及び設定について、サーバとクライアント別に要求事項をまとめたガイドライン。 TLS1.1 を最低限適切なセキュアトランスポートプロトコルとし、承認された運用とアルゴリズムを用いた暗号スイートを設定することを要求。さらに、2015 年 1 月 1 日までに TLS1.2 への移行計画を政府機関が策定することも推奨している。 TLS サーバの最小限要求事項については、「サーバ選択の推奨事項」・「サーバのインストール設定のための推奨事項（バージョンサポート、証明書、暗号サポート、拡張、クライアント認証、セッション再開、圧縮方法、運用上の検討事項）」・「サーバシステム管理者のための推奨事項（バージョンサポート、証明書、暗号サポート、クライアント認証、運用上の検討事項）」の 3 分類で各分類における要求事項・推奨事項を整理している。 第 4 章では TLS クライアントの最小限要求事項について、「クライアント選択の推奨事項」・「クライアントのインストールと設定のための推奨事項（バージョンサポート、証明書、暗号サポート、拡張、サーバ認証、セッション再開、圧縮モード）」・「クライアントシステム管理者のための推奨事項（バージョンサポート、証明書、サーバ認証、運用上の検討事項）」・「エンドユーザのための推奨事項」の 4 分類で各分類における要求事項・推奨事項を整理している。 同ガイドラインの要求事項を満たすことにより、以下の内容が促進されるとしている: 1. インターネット上の情報配送保護のための、認証、機密性及び完全性のより一貫した使用 2. NIST 承認されたアルゴリズム及び公開標準を含む推奨暗号スイートの一貫した使用 3. TLS プロトコル上の既知及び想定される攻撃に対する保護 4. トランスポート層のセキュリティ実装の統合におけるシステム管理者や管理者（マネージャー）による十分な情報を得たうえでの決定
目次	1. 序説 2. TLS 概要 3. TLS サーバの最小限要求事項 4. TLS クライアントの最小限要求事項 付録 A 略語 付録 B 暗号スイート名の解釈 付録 C 事前共有鍵 付録 D 将来の機能 付録 E 参考文献
URL	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf https://www.ipa.go.jp/files/000057084.pdf （IPA による日本語翻訳版）

付録 2-17 SP 800-57 Part 1 Rev. 4 “Recommendation for Key Management, Part 1: General”

題名	SP 800-57 Part 1 Rev. 4 “Recommendation for Key Management, Part 1: General”
対象読者	システムまたはアプリケーションの所有者や管理者、暗号モジュール 開発者、プロトコル開発者、及びシステム管理者
策定年・ 文書のバージョン番号	2015 年 1 月（Rev. 4） Rev. 4
発行機関	NIST (National Institute of Standards and Technology)
言語	英語
文書の種類・テーマ	暗号に関して運用・設定する文書（暗号プロトコル以外に関するもの） 暗号鍵管理に関するガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	SP 800-57 シリーズは 3 部で構成され、本文書は第 1 部。第 2 部は、米国政府機関向けの方針及びセキュリティ計画の要求事項に関するガイダンスを提供。第 3 部は、システムの暗号機能を使用する際のガイダンスを提供。 暗号技術の基本的知識は、公開鍵基盤（PKI）への入門書である SP800-32 “ Introduction to Public Key Technology and the Federal PKI Infrastructure”を参照することを推奨。 暗号モジュールの実装の詳細については、FIPS 140 ”Security Requirements for Cryptographic Modules” を参照。
概要	システム開発者とシステム管理者に対して、鍵管理に関連するベストプラクティスについて助言することを目的として、基本的な鍵管理に関する推奨事項を提供する文書。鍵の生成、使用、及び最終的な破棄に焦点をあてる。関連話題として、アルゴリズムの選択や適切な鍵サイズ、暗号方針、及び暗号モジュール選択等についても、推奨事項に含まれる。 第 1 章では本文書の目的と適用範囲を定め、第 2 章から第 4 章までは本文書内で使用される用語の説明及び暗号の利用場面及び基本的な暗号アルゴリズムを説明。第 5 章では、用途によって異なる種別の鍵及び他の暗号技術情報を分類し、個々の鍵種別についての適切な暗号期間、他の鍵材料についての推奨事項と要求事項を提供。また、ドメインパラメータや公開鍵有効性の保証を導入し、鍵材料の危殆化の意味するところを議論し、暗号アルゴリズム強度選択の実装と置換えについてのガイダンスを提供。第 6 章では、暗号学的情報の保護要件や保護メカニズムについて解説し、第 7 章では暗号鍵のライフサイクルの各状態における推奨事項を説明。第 8 章では、鍵管理の各フェーズ（運用前・運用・運用後・廃棄）において考慮すべき事項等を説明。第 9 章では、鍵材料を保護するために使用される 3 つの管理原則（責任追跡性・監査・鍵管理システムの抗たん性）について説明。第 10 章では、鍵管理仕様の内容と要求事項を規定し、通信環境や構成要素の要求事項、鍵材料保管、アクセス制御、アカウント管理及び危殆化時回復策について説明。
目次	1. 序説 2. 用語と略語の解説 3. セキュリティサービス 4. 暗号アルゴリズム 5. 一般的な鍵管理ガイダンス 6. 暗号学的情報の保護要件 7. 鍵の状態と遷移 8. 鍵管理のフェーズと機能 9. 責任追跡性、監査、及び抗たん性 10. 暗号デバイスやアプリケーションの鍵管理仕様 付属 A 暗号学的及び非暗号学的な完全性と情報源認証メカニズム 付属 B 鍵回復 付属 C 参考文献 付属 D 改訂
URL	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf https://www.ipa.go.jp/files/000055490.pdf （IPA による日本語翻訳版）

付録 2-18 SP 800-57 Part 2 “Recommendation for Key Management, Part 2: Best Practices for Key Management Organization”

題名	SP 800-57 Part 2 “Recommendation for Key Management, Part 2: Best Practices for Key Management Organization”
対象読者	システムの所有者または管理者、鍵管理システムの実行者または管理者
策定年・ 文書のバージョン番号	2005 年 8 月 初版
発行機関	NIST (National Institute of Standards and Technology)
言語	英語
文書の種類・テーマ	暗号に関して運用・設定に関する文書（暗号プロトコル以外に関するもの） 暗号鍵管理に関するガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	SP 800-57 は 3 部で構成される暗号鍵管理ガイドラインである。Part 2 は米国政府機関における方針とセキュリティプランの要件を提供することを目的とした文書。
概要	本文書は、暗号鍵の管理及び手順策定、法律や連邦政府機関のセキュリティポリシー要求事項に適合した鍵管理のインフラを構築するうえで参考となるフレームワーク及び一般的なガイダンスの提供を目的としたもの。 第 2 章「鍵管理基盤（KMI）」では、鍵管理基盤を構成する要素として①中央監視局（Central Oversight Authority）、②鍵処理所（Key Processing Facility）、③サービス・エージェント（Service Agent）、④クライアント・ノート（Client Node）を示し、それぞれの役割等について説明。 第 3 章「鍵管理方針と施策」は、鍵管理方針（Key Management Policy）と鍵管理プラクティス（Key Management Practices Statement）について説明。鍵管理方針は暗号鍵材料の生成、配布、計量、保管、使用、及び失効に適用される権限、保護目的及び制約に関する原則を示す文書である。鍵管理プラクティスは、鍵管理基盤の信頼ルートを確立し、鍵管理施策を実施するために鍵管理手続きと手法を規範的かつ具体的に明示する文書で、鍵管理施策状況（KMPS）の内容は組織の違いによって大きく変わるところがあるので、本文書では作成する際に指針となるフォーマットと共通内容を示している。 第 4 章「情報技術システムのセキュリティプラン」は、OMB Circular A-130 と NIST SP 800-18 Rev. 1 “Guide for Developing Security Plans for Federal Information Systems”に従い、①一般のサポートシステム（LAN、バックボーン、データ処理センター等のような相互接続情報源）と②特別監査が必要となるシステム（重要情報を扱うといった主要のアプリケーション）に対するセキュリティプランを説明。そしてシステムを識別する情報以外の追加事項を列挙している。 第 5 章「各暗号構成要素に対する鍵管理プラン」は、大規模または複雑なシステムにおいて提案された鍵管理製品及びサービスが適切に運用できるよう、鍵管理プランを作成する際の注意事項を説明。鍵管理プランには、プロセスと情報要件（①鍵管理製品とサービス要件、②特注の鍵管理製品とサービス、③鍵素材の配布、④鍵素材保存、⑤アクセス権⑥記録、⑦危殆化の管理と回復、⑧鍵回復、⑨拡張機能の要件）を含む必要があるとしている。
目次	1. 導入 2. 鍵管理基盤（KMI） 3. 鍵管理方針と施策 4. 情報技術システムのセキュリティプラン 5. 各暗号要素に対する鍵管理プラン 付録 A 概念的鍵管理基盤（KMI） 付録 B インターネット X. 509 の公開鍵基盤認証方針と施策認証構造 付録 C 評価者向けチェックリスト 付録 D セキュリティ計画に鍵管理を追加する際のテンプレート 付録 E 暗号製品開発者向け鍵管理チェックリスト 付録 F 参考文献
URL	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-57p2.pdf

付録 2-19 SP 800-57 Part 3 Rev.1 “Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance”

題名	SP 800-57 Part 3 Rev.1 “Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance”
対象読者	システムの調達者及び管理者、エンドユーザ
策定年・ 文書のバージョン番号	2015 年 1 月（Rev. 1） Rev. 1
発行機関	NIST (National Institute of Standards and Technology)
言語	英語
文書の種類・テーマ	暗号に関して運用・設定する文書（特に暗号プロトコルに関するもの）、及び暗号に関して運用・設定する文書（暗号プロトコル以外に関するもの） 暗号鍵管理に関するガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	SP 800-57 は 3 部で構成されるガイドラインで、Part 3 は現在利用または今後利用される鍵管理基盤及びプロトコル、アプリケーションについて、鍵管理に関するガイダンスを提供することを目的とした文書。 第 4 章トランスポート層セキュリティ（TLS）に関しては、本書では詳細を解説せず、SP800-52 Rev.1 ”Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations”を参照するよう求めている。
概要	本文書は現在利用または今後利用される鍵管理基盤及びプロトコル、アプリケーションについて、鍵管理に関する推奨事項等を提供するガイダンス。 本文書で説明される鍵管理基盤・プロトコル・アプリケーションは、①公開鍵暗号基盤（PKI）、②インターネットプロトコルセキュリティ（IPsec）、③トランスポート層セキュリティ（TLS）、④セキュア/多目的インターネットメール拡張（S/MIME）、⑤ケルベロス（Kerberos）、⑥無線回線経由の鍵更新（OTAR）、⑦ドメインネームシステムセキュリティ拡張（DNSSEC）、⑧暗号化ファイルシステム（EFS）、⑨セキュアシェル（SSH）で、各項目について提供される内容は以下の通りである。 ・ 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及び関連するセキュリティ及び適合性の問題 ・ 連邦政府情報保護のための現在のメカニズムの仕様に関する推奨事項 ・ 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、システム管理者及びエンドユーザへの一般推奨事項
目次	1. 序説 2. 公開鍵基盤（PKI） 3. インターネットプロトコルセキュリティ（IPsec） 4. トランスポート層セキュリティ（TLS） 5. セキュア／多目的インターネットメール拡張（S/MIME） 6. ケルベロス（Kerberos） 7. 無線回線経由の鍵更新（OTAR）鍵管理メッセージ（KMM） 8. ドメインネームシステムセキュリティ拡張（DNSSEC） 9. 暗号化ファイルシステム（EFS） 10. セキュアシェル（SSH） 付録 A 用語 付録 B 略語 付録 C 初心者エンドユーザへの言葉 付録 D 参考文献 付録 E 改訂履歴
URL	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf https://www.ipa.go.jp/files/000055491.pdf （IPA による日本語翻訳版）

付録 2-20 SP 800-63-3 “Digital Identity Guidelines”

題名	SP 800-63-3 “Digital Identity Guidelines”
対象読者	デジタルアイデンティティ サービスを実装する連邦政府機関
策定年・ 文書のバージョン番号	2017 年 6 月（第 3 版） 第 3 版
発行機関	NIST (National Institute of Standards and Technology)
言語	英語
文書の種類・テーマ	暗号を利用したシステムの運用もしくはマネジメントに関する文書及び暗号に関して運用・設定に関する文書（暗号プロトコル以外に関するもの） デジタルシステムでデジタルアイデンティティを使用する際のリスク評価手法と一般的なフレームワークの概要を提供する文書。
文書の位置づけ	法的義務はない
他の文書との関係	SP 800-63-2 を大幅に更新した文書で、SP800-63-2 からは、Token（トークン）と呼ばれていた、認証要求者が所持し管理している情報（通常は鍵またはパスワード）が、Authenticator（認証器）と呼ばれる等、用語や要求事項が変更されている。また、SP 800-63-2 までは単一の文書であったが、本文書は本文書と SP 800-63A,SP800-63B、SP 800-63C の 4 部で構成される。 暗号鍵に関する要件は、NIST SP 800-57 Part 1“Recommendation for Key Management, Part 1: General”の最小要件を満たすこと、デジタルアイデンティティにおけるリスクマネジメントに関しては SP 800-30 Rev. 1 “Guide for Conducting Risk Assessments”の参照を求めている。
概要	デジタルアイデンティティを利用したシステムにおける、一般的な認証フレームワーク及び情報システムにおける認証器（Authenticator）、クレデンシャル（Credential）、アサーション（Assertion）の利用について概説した文書。本文書では、OMB M-04-04 で決められていた 4 つのアイデンティティ保証レベル(LoA)を以下の 3 つの要素に分解し、それぞれのレベルで 3 つの保証レベルを定義し、各保証レベルの選択方法について述べられている： ・ Identity Assurance Level(IAL)：アイデンティティ証明の強度を示す保証レベル ・ Authenticator Assurance Level(AAL)：認証プロセス自体の強度を示す保証レベル ・ Federation Assurance Level(FAL)：フェデレーション 環境における保証レベル 第 4 章では、デジタルアイデンティティモデルの概要を示し、詳細な要件に関しては、SP 800-63A、SP800-63B、SP 800-63C で示されている。第 5 章では、NIST のリスクマネジメントフレームワーク（RMF）を補完する形で、デジタルアイデンティティリスクマネジメントについて説明し、3 つの保証要素（IAL、AAL.FAL）における保証レベルの概要を概説。第 6 章では、リスクに基づいた適切な IAL、AAL 及び FAL の各保証レベルを選択する際に参考となるフローチャートを提供。
目次	1. 目的 2. 序論 3. 定義と略語 4. デジタルアイデンティティモデル 5. デジタルアイデンティティリスクマネジメント 6. 保証レベルの選択 7. フェデレーションにおける考慮事項 8. 参考文献 付録 A 定義と略語
URL	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

付録 2-21 SP 800-63B “Digital Identity Guidelines: Authentication and Lifecycle Management”

題名	SP 800-63B “Digital Identity Guidelines: Authentication and Lifecycle Management”
対象読者	デジタルアイデンティティサービスを実装する連邦政府機関
策定年・ 文書のバージョン番号	2017 年 6 月 初版
発行機関	NIST (National Institute of Standards and Technology)
言語	英語
文書の種類・テーマ	暗号を利用したシステムの運用もしくはマネジメントに関する文書及び暗号に関して運用・設定に関する文書（暗号プロトコル以外に関するもの） 認証器保証レベル（Authenticator Assurance Level, AAL）で使用できる認証プロバイダの選択肢など、認証プロセスの種類に関する推奨事項を示したガイドライン。
文書の位置づけ	法的義務はない
他の文書との関係	SP 800-63-3 で分類された 3 つのアイデンティティ保証レベルのうち AAL に関する文書で、アイデンティティ保証レベル（Identity Assurance Level, IAL）は SP 800-63A、フェデレーション保証レベル（Federation Assurance Level, FAL）は SP 800-63C でガイドラインが提供。 また、CSP は SP 800-53「連邦政府情報システム及び連邦組織のためのセキュリティ管理策とプライバシー管理策」であげられているセキュリティ管理策を採用すべきとしている。
概要	SP 800-63-3 で分類された 3 つのアイデンティティ保証レベルのうち、AAL に関して述べた文書で、認証器の選択、認証プロセスの種別から、認証器のライフサイクルに関する指針を提供するもの。認証トランザクションの強度はこの AAL によって特徴付けられ、より高度な AAL では、攻撃者が認証を達成するために高度なリソースが必要となる。AAL は AAL1 から AAL3 の 3 段階に分類され、AAL3 ほど高いレベルの保証がされる。 第 4 章では、AAL の各保証レベルにおいて求められる、認証器の種類や再認証、セキュリティ管理策の要求事項等について説明。第 5 章では、パスワード等の認証器及び検証器 に対する要件の詳細について、第 6 章では認証器のライフサイクルマネジメントについて説明。第 7 章では各 AAL における検証器の再認証などのセッション管理に関する推奨事項があげられている。第 8 章から第 10 章では、それぞれ検証器に対する脅威やその脅威を緩和する戦略、認証器のプライバシーとユーザビリティに関する考慮事項がまとめられている。
目次	1. 目的 2. 序論 3. 定義と略語 4. 認証器保証レベル(AAL) 5. 認証器と検証器の要件 6. 認証器のライフサイクルマネジメント 7. セッション管理 8. 脅威とセキュリティに関する考慮事項 9. プライバシーに関する考慮事項 10. ユーザビリティに関する考慮事項 11. 参考文献 付録 A 記憶秘匿性の強度
URL	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

付録 2-22 SP 800-77 “Guide to IPsec VPNs”

題名	SP 800-77 “Guide to IPsec VPNs”
対象読者	ネットワークインフラを運用、管理するネットワーク管理者、セキュリティスタッフ、テクニカルサポートスタッフ及びコンピュータセキュリティプログラム管理者
策定年・ 文書のバージョン番号	2005 年 12 月 初版
発行機関	NIST (National Institute of Standards and Technology)
言語	英語
文書の種類・テーマ	暗号の開発実装に関連する文書、及び暗号に関して運用・設定に関する文書（特に暗号プロトコルに関するもの） IPsec 技術を理解し、設計・実装・保護・監視及び保守を支援するガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	SSL VPN に関しては SP 800-113 “Guide to SSL VPNs”が提供されている。VPN の利用に関しては、FIPS140 で指定された暗号アルゴリズムを使用する必要があるとし、IPsec VPN の公開鍵認証基盤に関しては、SP 800-32「公開鍵基盤の導入と連邦におけるインフラストラクチャ」を参照すべきとしている。
概要	IPsec に基づき VPN を実装する組織に対して、実用的なガイダンスを提供することにより、組織がネットワークを介して機密情報を送信することに伴うリスクの軽減を支援することを目的とした文書。 第2章ではネットワーク層 セキュリティの必要性について説明し、VPN 技術の概念を紹介し、第 3 章では、「暗号ペイロード（ESP）」、「IP 認証ヘッダ（AH）」、「インターネット鍵交換（IKE）」、「IP ペイロード圧縮プロトコル（IPComp）」にといった IPsec の基礎概念を説明。 第 4 章では、IPsec の計画と実装のステップと、その際に考慮すべき事項について、①要件の特定②ソリューション設計③プロトタイプの実装とテスト④ソリューション展開⑤ソリューション管理のステップごとに解説。 第 5 章では、IPsec の代替案として、データ層・トランスポート層・アプリケーション層の VPN プロトコルを説明し、これら代替策の適用が適切な場合があることについて説明。 第 6 章では、IPsec の利用についてケーススタディを用いて紹介している。具体的には、2 つのローカルエリアネットワーク（メインオフィスとリモートオフィス）間の通信保護、小規模オフィスとホームオフィス環境でのワイヤレス通信の保護、メインオフィスと遠隔ユーザ（在宅勤務者など）間の通信保護の 3 つのシナリオに関して、上記の 5 つのステップに沿った IPsec の計画と実装を説明。 第 7 章では、IPsec の今後の方向性について簡単に紹介。
目次	1. 序説 2. ネットワーク層のセキュリティ 3. IPsec の基本 4. IPsec の計画と実装 5. IPsec の代替案 6. 計画と実装に関するケーススタディ 7. 将来の指針 付録 A 政策に関する考慮事項 付録 B ケーススタディ構成ファイル 付録 C 用語 付録 D 略語 付録 E 参考文献 付録 F 索引
URL	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-77.pdf

付録 2-23 SP 800-78-4 “Cryptographic Algorithms and Key Sizes for Personal Identity Verification”

題名	SP 800-78-4 “Cryptographic Algorithms and Key Sizes for Personal Identity Verification”
対象読者	暗号化と PKI 技術に関する実務知識を有する、連邦政府機関及び PIV システム実装者
策定年・ 文書のバージョン番号	2015 年 5 月 初版
発行機関	NIST (National Institute of Standards and Technology)
言語	英語
文書の種類・テーマ	暗号の開発実装に関連する文書 PIV のための暗号アルゴリズムと鍵サイズに関する文書
文書の位置づけ	法的義務はない
他の文書との関係	本文書は、ID 証明、登録、PIV カードの発行、PIV カードの使用など、PIV のライフサイクル活動の要件を定義した FIPS 201-2 の内容を補足する文書である。PIV に関連する文章として、NISTSP800-73”Interfaces for Personal Identity Verification” 、 SP800-76” Biometric Specifications for Personal Identity Verification”
概要	本文書は、PIV システムの暗号アルゴリズム及び鍵長、FIPS 201-2”Personal Identity Verification (PIV) of Federal Employees and Contractors”の内容を補足することを目的とした文書。 本文書の推奨事項の範囲は、PIV カード及び PIV カードを発行・管理を補助するインフラの構成要素、セキュリティサービスを提供するために PIV カードのクレデンシャル情報を活用するアプリケーションとなっている。推奨事項では、対称/非対称暗号化アルゴリズム、デジタル署名アルゴリズム、鍵確立スキーム、メッセージダイジェストアルゴリズム、PIV 鍵またはデジタル署名により構成される特定のメカニズムについてまとめられている PIV 暗号鍵として設定が求められているものは、①PIV 認証キー②非対称カード認証キー③対称カード認証キー④電子署名キー⑤鍵管理キー⑥安全なメッセージングのセッションキーを確立するための非対称キーの 6 種類で、それぞれ求められる暗号アルゴリズム・鍵長について説明。また、PIV カードに格納されているオブジェクトの中で、電子署名が求められるものは、①X.509 公開鍵証明書②セキュアメッセージングカード検証可能証明書（CVC）③中間 CVC④電子署名された CHUID（Card Holder Unique Identifier）⑤バイオメトリック情報（例えば、指紋）の 5 種類としている。 第 4 章では、PKI 認証機関及びオンライン証明書ステータス確認プロトコルの応答者によって生成される、ステータス情報の暗号化要件について、X.509 CRL 及び OCSP について説明。 第 5 章では、PIV カードに格納された情報を管理するための暗号要件として、PIV カードアプリケーション管理キーの暗号アルゴリズムと鍵長について説明。 第 6 章では、SP800-73 “Interfaces for Personal Identity Verification”で定義されたアプリケーションプログラミングインタフェースとカードコマンドのための鍵の参照値とアルゴリズム識別子について、第 7 章では、サポートする鍵とアルゴリズムごとに PIV カードで実行する必要のある暗号アルゴリズム検証テストについて説明。
目次	1. 序説 2. FIPS 201-2 における暗号の適用 3. カードの暗号化要件 4. 証明書ステータス情報 5. PIV カード申請管理キー 6. PIV カードインタフェースの識別 7. 暗号アルゴリズム検証テストの要件 付録 A 用語 付録 B 参考文献
URL	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-78-4.pdf

付録 2-24 SP 800-81-2 “Secure Domain Name System (DNS) Development Guide”

題名	SP 800-81-2 “Secure Domain Name System (DNS) Development Guide”
対象読者	DNS 導入の管理者及び DNS 関連業務に関して責任を持つコンピュータセキュリティ担当者とシステム管理者
策定年・ 文書のバージョン番号	2006 年 5 月（初版）、2013 年 9 月（第 2 版） 第 2 版
発行機関	NIST (National Institute of Standards and Technology)
言語	英語
文書の種類・テーマ	暗号に関して運用・設定に関する文書（特に暗号プロトコルに関するもの） DNS のセキュリティを保護するための導入ガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	2006 年 5 月に発行された初版より暗号化パラメータの推奨事項を更新。この推奨事項は SP 800-57 “Recommendation for Key Management”や FIPS 186「デジタル署名基準」、FIPS 180「安全なハッシュの基準」に基づいている。
概要	組織における DNS サービスの安全な導入について理解を深められるよう、組織を支援することを目的とした文書。DNS の各種側面のセキュリティ保護について、運用環境及び関連する脅威の分析結果に基づく実践的な指針を示している。 第 2 章では、DNS 及び DNS インフラストラクチャの概要、セキュリティ目標を説明し、第 3 章では DNS を構成するゾーンやリゾルバ などの基本的な構成要素を説明。第 4 章では各種の DNS トランザクションを明確に定めている。第 5 章・第 6 章では、DNS ホスティング環境と DNS トランザクションについて、脅威、セキュリティ目標及び保護策について説明。 第 7 章以降では、DNS を構成するホスティング環境やトランザクションのセキュリティ保護のためのガイドラインを具体的に説明。暗号技術の観点からは、DNS クエリ/レスポンスの脅威に対する保護策として DNSSEC を示し、DNSSEC におけるゾーン署名鍵、鍵署名鍵に関する推奨事項として、各鍵におけるデジタル署名アルゴリズムスイート、鍵サイズ、鍵ロールオーバについて述べられている。他の推奨事項として、鍵署名鍵を使った署名の生成には、オフラインに保存されている鍵署名鍵の秘密鍵を用いて、オフラインで行うことや、権威ネームサーバが動的に更新されない場合は、ゾーン証明鍵・鍵署名鍵の両方に対応する秘密鍵をネームサーバに保存しないことをあげている。
目次	1. 序説 2. DNS のセキュリティ保護 3. DNS データと DNS ソフトウェア 4. DNS トランザクション 5. DNS ホスティング環境—脅威、セキュリティ目標、保護策 6. DNS トランザクション—脅威、セキュリティ目標、保護策 7. DNS ホスティング環境のセキュリティ保護のためのガイドライン 8. DNS トランザクションのセキュリティ保護のためのガイドライン 9. DNS クエリ/レスポンスのセキュリティ保護のためのガイドライン 10. DNS 内容制御を通じて情報露出を最小限に抑えるためのガイドライン 11. DNS のセキュリティ管理業務ガイドライン 12. キャッシュサーバとスタブリゾルバのセキュリティ保護のためのガイドライン 13. 検証リゾルバのセキュリティ保護のためのガイドライン 付録 A 重要な用語の定義 付録 B ベンダによるチェックリスト項目の特定手順 付録 C 略語 付録 D 参考文献
URL	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf https://www.ipa.go.jp/files/000025348.pdf（IPA による日本語翻訳版（初版））

付録 2-25 SP 800-88 Rev. 1 “Guidelines for Media Sanitization”

題名	SP 800-88 Rev. 1 “Guidelines for Media Sanitization”
対象読者	連邦政府機関、企業におけるサニタイズやメディア廃棄の担当者や意思決定者
策定年・ 文書のバージョン番号	2006 年 9 月（初版）、2014 年 12 月（Rev. 1） Rev. 1
発行機関	NIST (National Institute of Standards and Technology)
言語	英語
文書の種類・テーマ	特定の製品・サービスの利用に関する文書 サニタイズと廃棄に関する意思決定を支援するガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	システムの機密性分類については、FIPS 199「連邦政府の情報及び情報システムに対するセキュリティ分類規格」及び SP 800-60“Guide for Mapping Types of Information and Information Systems to Security Categories”を参照し、機密性分類は組織がサニタイズの意思決定を行う際に要求すべき保証レベルに影響するとしている。 また、FIPS 200「連邦政府の情報及び情報システムに対する最低限のセキュリティ要求事項」には、サニタイズプログラムを用意することを求めるセキュリティ要件の基礎が設定されており、SP 800-53 “Security and Privacy Controls for Federal Information Systems and Organizations”には、連邦政府システムの全体的なセキュリティ分類に基づく、（サニタイズを含んだ）最低限の推奨セキュリティ管理策が示されているため、参照を推奨。 ストレージの暗号化やセキュリティに関しては、SP 800-111 “Guide to Storage Encryption Technologies for End User Devices”及び SP 800-122 “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)”を参照すべきとしている。
概要	組織やシステムオーナーが情報の機密性レベルに基づいて、サニタイズに関する意思決定を行えるよう支援するガイドライン。暗号技術の高度化により、組織の機密情報にアクセスすることが困難となったが、攻撃者は媒体から削除されたはずのデータを復元する攻撃を行う可能性があるため、サニタイズを適切に行うことでこのような攻撃を阻止できるとしている。 第 2 章では、サニタイズに対するニーズやサニタイズ及び媒体の基本的な種類の概要を示しており、第 3 章では、サニタイズの意思決定に影響を与える、CIO や情報システム管理者等の関係者ごとに役割と責任について説明。 第 4 章では、サニタイズの意思決定を行うプロセス（システムライフサイクル、機密性の区分、メディア再利用、メディア管理、文書化等）別に、考慮すべき事項等を説明。 第 5 章ではいくつかのサニタイズ技法の要約が示されている。 暗号に関しては、暗号化消去（Cryptographic Erase：CE）と呼ばれる、暗号化されたデータの暗号鍵をサニタイズすることで、目的データの復号を不可能にする技術があげられ、CE を行う際の考慮事項も明記されている。CE を使用する場合は FIPS 140-2 認定を満たすような、有効性が確認された強力な暗号モジュールの使用を推奨。
目次	1. 序論 2. 背景 3. 役割及び責務 4. 情報のサニタイズと処分に関する意思決定 5. サニタイズ技法の要約 付録 A データを含む媒体のサニタイズに関する最小限推奨事項 付録 B 用語 付録 C ツールと資料 付録 D 暗号的消去デバイスのガイドライン 付録 E デバイス固有の特徴 付録 F 参考文献 付録 G サニタイズ証明の書式例
URL	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf https://www.ipa.go.jp/files/000025355.pdf （IPA による日本語翻訳版（初版））

付録 2-26 SP 800-89 “Recommendation for Obtaining Assurances for Digital Signature Applications”

題名	SP 800-89 “Recommendation for Obtaining Assurances for Digital Signature Applications”
対象読者	連邦政府機関のシステム実装者と運用者
策定年・ 文書のバージョン番号	2006 年 11 月 初版
発行機関	NIST (National Institute of Standards and Technology)
言語	英語
文書の種類・テーマ	暗号に関して運用・設定する文書（暗号プロトコル以外に関するもの） 電子署名アプリケーションの保証取得に関する推奨事項を記述した文書
文書の位置づけ	法的義務はない
他の文書との関係	本文書は FISMA に基づく法的責任を促進するために NIST によって開発された。
概要	本文書は有効な電子署名に必要な保証を得る方法として、「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」、「鍵ペア所有者の秘密鍵所有の保証」、「鍵ペア所有者の身元の保証」に関する推奨事項を説明したもの。 第 4 章では、電子署名の各プロセスに関わる当事者がとるべき、ドメインパラメータの有効性の保証方法について説明している。電子署名に関わる当事者としては、署名者、署名者に鍵を生成する TTP、署名者に証明書を発行する認証局、検証者、ドメインパラメータのユーザを示し、各当事者は、以下の方法の少なくとも 1 つを使用して、ドメインパラメータが有効であるという保証を得る必要があるとしている。 ・ 指定された要件（DSA の場合は FIPS 186-3、ECDSA の場合は米国標準規格（ANS）X9.62 を参照）に従ってドメインパラメータを生成 ・ 明示的なドメインパラメータの検証を行い、妥当性の兆候を取得 ・ ドメインパラメータを TTP に生成してもらうか、または明示的なドメインパラメータ検証を TTP に行ってもらい、ドメインパラメータが生成された時点で有効であったことの保証を TTP から獲得 第 5 章では、電子署名の各プロセスに関わる当事者（署名者、検証者、署名者に証明書を発行する認証局）がとるべき、公開鍵の有効性の保証方法を説明。
目次	1. 序説 2. 権限 3. 定義及び略語 4. ドメインパラメータの有効性の保証 5. 公開鍵の有効性の保証 6. 秘密鍵保有の保証 7. 身元の保証 付録 A RFC 4211 証明書要求メッセージでインスタンス化された保証メッセージ 付録 B 参考文献
URL	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-89.pdf

付録 2-27 NIST SP 800-90A “Recommendation for Random Number Generation Using Deterministic Random Bit Generators”

題名	SP 800-90A “Recommendation for Random Number Generation Using Deterministic Random Bit Generators”
対象読者	連邦政府機関関係者
策定年・ 文書のバージョン番号	2012 年 1 月（初版）、2015 年 6 月（Rev. 1） Rev. 1
発行機関	NIST (National Institute of Standards and Technology)
言語	英語
文書の種類・テーマ	暗号の開発実装に関する文書 確定的ランダムビット発生器を用いた乱数発生のための勧告
文書の位置づけ	法的義務はない
他の文書との関係	SP 800-90B では、エントロピー源の設計と検証に関するガイダンスが提供されている。 SP 800-90C では、エントロピー入力ソースからの RBG の構築と、本勧告（SP 800-90A）の承認された DRBG メカニズムに関するガイダンスを提供する。FIPS180 ではハッシュ関数、FIPS197 及び SP 800-67 “Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher”（それぞれ AES 及び TDEA）ではブロック暗号アルゴリズムについて述べられている。
概要	本文書は決定論的方法を用いてランダムビットを生成するためのメカニズムに関する勧告をまとめたものである。扱われている手法は、ハッシュ関数、ブロック暗号アルゴリズム、または数論的問題のいずれかに基づいている。 勧告には以下が含まれる： 1. DRBG メカニズムの使用要件 2. ハッシュ関数、ブロック暗号及び数論的問題を使用する DRBG メカニズムの仕様 3. 実装上の問題 4. 保証の考慮事項 勧告は、勧告公表時点で許容可能なセキュリティレベルにある、いくつかの DRBG メカニズムを規定している。仮に特定の DRBG メカニズムへの新しい攻撃が見つかった場合でも、承認されたメカニズムの多様性により、他の DRBG メカニズムへのタイムリーな移行が可能である。乱数生成は、2 つのエンティティ間の相互運用性を必要としないため、各エンティティは、アプリケーションに適した単一の DRBG メカニズムを選択することができる。
目次	1. 導入 2. 適合テスト 3. 範囲 4. 用語と定義 5. 記号と省略用語 6. 文書構成 7. DRBG の機能モデル 8. DRBG メカニズムの概念と一般要件 9. DRGB メカニズム関数 10. DRGB アルゴリズムの詳細 11. 保証 付属 A（規定）変換及び補助ルーチン 付属 B（参考）各 DRBG メカニズムの擬似コードの例 付属 C（参考）DRBG メカニズムの選択 付属 D（参考）参考文献 付属 E（参考）改訂
URL	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf

付録 2-28 SP 800-90B (Draft) “Recommendation for the Entropy Sources Used for Random Bit Generation”

題名	SP 800-90B Recommendation for the Entropy Sources Used for Random Bit Generation
対象読者	主に連邦政府所有者及び非政府協会利用者
策定年・ 文書のバージョン番号	2012 年 8 月(Draft) (Draft)
発行機関	NIST (National Institute of Standards and Technology)
言語	英語
文書の種類・テーマ	暗号の開発実装に関連する文書 乱数ビット生成のうえで使用するエントロピー源のガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	SP800-90A では、エントロピー源を使用する DRBG のメカニズムについて説明している。SP800-90C では、RBG の作成について説明されている。FIPS 198 では HMAC についての説明がされている。FIPS 180 ではハッシュ関数について説明されている。さらに FIPS197 ではブロック暗号アルゴリズムについて触れられている。
概要	本勧告は、ランダムビットを生成するためのエントロピー源について規定。具体的には、SP800-90A で規定された決定論的ランダム・ビット・ジェネレータ（DRBG）で用いられるエントロピー源が満たすべき特性と、エントロピー源の品質を検証するためのテストについて規定している。
目次	1. はじめに 2. 用語と説明 3. 記号と略語 4. 一般協議 5. 概念に対するインタフェース 6. エントロピー源生成の必要事項 7. 批准データと書類のための必要事項 8. エントロピー源の実験方法 9. エントロピー源によって生成されたエントロピーを判断方法 10. 機能テスト確認：同等の機能のテスト
URL	http://csrc.nist.gov/publications/drafts/800-90/sp800-90b_second_draft.pdf

付録 2-29 SP 800-90C (Draft) “Recommendation for Random Bit Generator (RBG) Constructions”

題名	SP 800-90C (Draft) “Recommendation for Random Bit Generator (RBG) Constructions”
対象読者	連邦政府機関
策定年・ 文書のバージョン番号	2012 年 8 月(Draft) (Draft)
発行機関	NIST (National Institute of Standards and Technology)
言語	英語
文書の種類・テーマ	暗号の開発実装に関する文書 ランダムビット生成器(RBG)の構築に対する勧告
文書の位置づけ	法的義務はない
他の文書との関係	DRBG メカニズムの議論と詳細については SP 800-90A を参照。 エントロピー源などの非決定出力源については SP 800-90B を参照。RBG の構成の規定については American National Standard（ANS）X9.82 Part4 を参照。
概要	この勧告は、 SP 800-90A で規定された DRBG メカニズムと SP 800-90B で規定されたエントロピー源を使用した RBG の構成を規定している。具体的には、SP 800-90C は、American National Standard（ANS）X9.82、Part 4 に基づいており、RBG の構成と、これらの RBG 構成内で使用される構成要素を規定している。ソース（SEI）、及びエントロピーソース出力の外部調整のために使用される、DRBG の Get_entropy_input コールを実装するための構造
目次	1. 範囲 2. 用語と定義 3. 記号と略語 4. 一般議論 5. RBG の概念 6. RBG インタフェース 7. SEI 8. DRBG の構築 9. NRBG の構築 10. 追加の構築 11. 試験 付録A 基本 RBG 設定の図 付録B SP 800-90C の要求への適合 付録C RBG 出力の事前処理
URL	http://csrc.nist.gov/publications/drafts/800-90/sp800_90c_second_draft.pdf

付録 2-30 SP 800-97 “Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i”

題名	SP 800-97 “Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i”
対象読者	組織における、無線 LAN のセキュリティを確保する責任を負う担当者、IEEE 802.11i 実装の設計、実装、保守及び維持を担当するネットワークエンジニアやセキュリティエンジニア及び管理者
策定年・ 文書のバージョン番号	2007 年 2 月 初版
発行機関	NIST (National Institute of Standards and Technology)
言語	英語
文書の種類・テーマ	暗号に関して運用・設定に関する文書（特に暗号プロトコルに関するもの）、暗号を利用したシステムの運用もしくはマネジメントに関する文書、及び特定の製品・サービスの利用に関する文書 IEEE 802.11i に基づいた技術の理解、選択、実装を支援するガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	SP 800-48 “Guide to Securing Legacy IEEE 802.11 Wireless Networks”、Bluetooth と携帯端末」は、IEEE 802.11 の実装を保護するための具体的な推奨事項が含まれているため、参照することを推奨。暗号鍵の生成に関しては、SP 800-90 “Recommendation for Random Number Generation Using Deterministic Random Bit Generators”、暗号鍵管理に関しては、SP 800-57 “Recommendation for Key Management”の一般的なガイダンスとベストプラクティスの推奨事項を参照することを推奨。
概要	IEEE 802.11 で利用されていた Wired Equivalent Privacy(WEP)方式のセキュリティ問題点を克服するために設計された IEE802.11i について、新たなセキュリティ機能の理解と実装、保守を支援することを目的とした文書。ロバストセキュリティネットワーク（RSN）のフレームワークを通じて、IEEE 802.11i に関連するセキュリティ機能と能力を解説し、RSN の計画と展開に関する広範なガイダンスを提供。 第 2 章では、IEEE 802.11 の無線 LAN 規格に焦点をあて、基本構成要素とアーキテクチャモデルについて説明し、第 3 章では、IEEE 802.11 のセキュリティ機能の概要を説明し、IEEE 802.11i で定義される主要なセキュリティ関連構成要素を解説。第 4 章では、RSN とロバストセキュリティネットワークアソシエーション（RSNA）の概念を説明し、RSN のデータ機密性と完全性のプロトコル及びこれらのプロトコルで作成及び使用される暗号化キーについて説明。 第 5 章では RSN 通信中に発生する 5 つのフェーズ（発見・認証・鍵生成と配布・データ移転保護・接続終了）について説明。第 6 章では、RSN の展開に必要な拡張認証プロトコル（EAP）の実装計画について説明し、組織が環境に適した EAP メソッドの選択とセキュリティ考慮事項 EAP アーキテクチャモデルと関連するサポート要件を照会する方法について解説。 第 7 章では、IEEE 802.11 無線ネットワークに適用される FIPS140-2 認証、第 8 章では無線 LAN セキュリティに関連するベストプラクティスの推奨事項を示している。第 9 章では、異なるシナリオで組織が RSN を計画、設計、実装する方法を示す 3 つのケーススタディが紹介されている。第 10 章では、文書の第 2 章から第 8 章で示された主要な概念と推奨事項がまとめられている。暗号の観点からは、EAP 認証を行う際に組織はアクセスポイントを使用する必要があるが、その際に PKI を使用する必要があると述べ、暗号モジュールは FIPS 準拠の暗号アルゴリズムを使用するべきとしている。最後に第 11 章では、開発中の IEEE 802.11i に関する拡張性について概要を説明。
目次	1. 序論 2. 無線ネットワークの概要 3. IEEE 802.11 セキュリティの概要 4. ロバストセキュリティネットワークのセキュリティフレームワーク 5. ロバストセキュリティネットワークの動作原理 6. 拡張認証プロトコル（EAP） 7. FIPS 及び WLAN 製品の認証 8. WLAN セキュリティに関するベストプラクティス 9. ケーススタディ 10. コンセプトの要約と推奨事項 11. 今後の方針 付録 A 略語 付録 B 参考文献 付録 C オンラインの資料
URL	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-97.pdf

付録 2-31 SP 800-102 “Recommendation for Digital Signature Timeliness”

題名	SP 800-102 “Recommendation for Digital Signature Timeliness”
対象読者	連邦政府機関のシステム実装者と運用者
策定年・ 文書のバージョン番号	2009 年 9 月 初版
発行機関	NIST (National Institute of Standards and Technology)
言語	英語
文書の種類・テーマ	暗号の開発実装に関連する文書、及び暗号に関して運用・設定に関する文書（暗号プロトコル以外に関するもの） 電子署名の適時性に関する推奨事項に関する文書
文書の位置づけ	法的義務はない
他の文書との関係	本勧告は Trusted Timestamp Authority (TTA)の設立と管理については、この文書の範囲外であるとし、TTA の詳細については、 ・ ”Request for Comment 3161, Internet X.509 Public Key Infrastructure Time-Stamp Protocol”（2001） ・ ”Information Technology – Security Techniques – Time-stamping Services”(2002) ・ ”Trusted Timestamp Management and Security”(2005) を参照するように求めている。 また、本文書は管理予算システム（OMB）の Securing Agency Information Systems (Circular A-130, Section 8b) の要件と一致している。
概要	本勧告は、TTA 等を用いて電子署名が生成された時刻を保証するための方法を規定したもの。署名付きメッセージに含まれている TTA の検証署名付きのタイムスタンプ及び/または検証者提供のデータを適切に使用することを推奨している。本勧告は連邦政府機関が秘密鍵や電子署名を正しく使用するために準備されたもの。 第 4 章では、TTA からのタイムスタンプを使用する際、異なる電子署名ベースのタイムスタンプスキームを使用した場合に、保証が得られるかどうかの判断に役立つよう、複数のスキームのケースについて説明。 第５章では、TTA からのタイムスタンプを用いるのとは別の方法で、署名の適時性の証拠を検証者に提供する方法について、複数のスキームのケースについて説明。
目次	1. 序説 2. 権限 3. 定義及び略語 4. TTA からのタイムスタンプの使用 5. 検証者が提供するデータを使用した適時性の証拠 付録 A 参考文献
URL	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-102.pdf

付録 2-32 SP 800-106 “Randomized Hashing for Digital Signatures”

題名	SP 800-106 “Randomized Hashing for Digital Signatures”
対象読者	連邦政府機関、電子署名の運用者
策定年・ 文書のバージョン番号	2009 年 2 月 初版
発行機関	NIST (National Institute of Standards and Technology)
言語	英語
文書の種類・テーマ	暗号の開発実装に関連する文書、及び暗号に関して運用・設定に関する文書（暗号プロトコル以外に関するもの） 電子署名を生成する際に、メッセージをランダム化する手法を提供する文書
文書の位置づけ	法的義務はない
他の文書との関係	連邦政府での使用が認められたハッシュ関数は、FIPS (Federal Information Processing Standard) 180-3 “the Secure Hash Standard (SHS)”で規定されている。 デジタル署名は FIPS 186-3 “the Digital Signature Standard”で規定されている。 ランダム化されたハッシュ実装の適合性テストは、NIST とカナダ政府の通信セキュリティ設立の共同作業である暗号モジュール検証プログラム（CMVP）の枠組みの中で実施されるとしている。
概要	本文書は DSA (Digital Signature Algorithm)、ECDSA (Elliptic Curve Digital Signature Algorithm) 及び RSA を使用した電子署名を生成する際に、ハッシュ関数に入力してメッセージをランダム化する手法について記述している。 第 2 章では、ランダムハッシュの特徴及び適用の必要性について示している。ランダムハッシュは衝突可能性がある場合でも、電子署名の生成段階において、最終的に同じハッシュ値を生成する可能性を低減することによって、署名者に追加の保護を提供することができる。また、プロトコルとアプリケーションの設計者は必ずしもランダムハッシュを適用する必要はなく、メッセージ署名者が署名するメッセージの全部または一部を、別人のメッセージ作成者が生成する状況においてランダムハッシュの使用の検討が推奨されている。 第 3 章では、ハッシングの前段階におけるメッセージのランダム化の手法について記述している。 第 4 章では、電子署名の生成及び検証段階におけるメッセージのランダム化に対応するための追加の操作について記述している。
目次	1. 序説 2. ランダムハッシュの適用範囲と適用可能性 3. ランダムハッシュ 4. ランダムハッシュを使用した電子署名 5. 参考文献 付録 RV_LENGTH_INDICATOR GENERATION
URL	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-106.pdf

付録 2-33 SP 800-111 “Guide to Storage Encryption Technologies for End User Devices”

題名	SP 800-111 “Guide to Storage Encryption Technologies for End User Devices”
対象読者	エンドユーザデバイスのストレージ暗号化技術を選択・管理・保守を行う情報セキュリティプログラムの管理者及びスタッフ、システム管理者
策定年・ 文書のバージョン番号	2007 年 11 月 初版
発行機関	NIST (National Institute of Standards and Technology)
言語	英語
文書の種類・テーマ	暗号の開発実装に関する文書、及び暗号を利用したシステムの運用もしくはマネジメントに関する文書 エンドユーザデバイスにおけるストレージ暗号技術のガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	SP 800-53 “Security and Privacy Controls for Federal Information Systems and Organizations”を本書とあわせて使用することが推奨されている。 SP 800-124 Rev. 1 “Guidelines for Managing the Security of Mobile Devices in the Enterprise”では、モバイルデバイスの暗号化管理に関して本書を参照することが求められている。
概要	組織がエンドユーザデバイスのストレージ暗号化技術を理解し、ストレージ暗号に関する計画・実装及び保守を支援するための文書。 本ガイドラインで扱うエンドユーザデバイスは、パーソナルコンピュータ（デスクトップ及びラップトップ）、コンシューマデバイス（スマートフォン等）、リムーバブルメディア（USB や外部 HDD 等）が含まれる。 また、本ガイドラインが対象とするストレージの暗号化手法は、「フルディスク暗号化」・「仮想ディスクの暗号化」・「ファイル・フォルダ暗号化」の 3 種類で、各暗号化手法の特徴や導入・実装する際の推奨事項やユースケース等を解説。また、暗号鍵の管理方法などの重要なセキュリティ要素についても解説。 ストレージ暗号化技術の実装計画及び実装に関しては、段階的なアプローチで対応する必要があるとし、以下のステップごとに考慮すべき事項等を解説。 1. 要件の特定（ストレージ暗号化が必要なデバイス、保護すべきデータ関連する要求事項等の特定） 2. ソリューション設計（アーキテクチャの考慮事項、認証方法、暗号化ポリシー等） 3. プロトタイプの実装及びテスト 4. ソリューションの展開 5. ソリューションの管理
目次	1. 序説 2. ストレージセキュリティの概要 3. ストレージ暗号化技術 4. ストレージ暗号化技術の計画と実装 付録 A エンドユーザデバイス上のストレージ暗号化に関する代替案 付録 B 用語 付録 C 略語 付録 D ツールとリソース
URL	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf

付録 2-34 SP 800-113 “Guide to SSL VPNs”

題名	SP 800-113 “Guide to SSL VPNs”
対象読者	システム・ネットワーク・アプリケーション管理者やセキュリティスタッフ。SSL VPN の導入を検討している組織及び IPsec VPN を既に導入している組織
策定年・ 文書のバージョン番号	2008 年 7 月 初版
発行機関	NIST (National Institute of Standards and Technology)
言語	英語
文書の種類・テーマ	暗号の開発実装に関連する文書、及び暗号に関して運用・設定に関する文書（特に暗号プロトコルに関するもの） SSL VPN 技術を理解し、設計・実装・保護・監視及び保守を支援するガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	SSL/TLS の理解のために SP 800-52 “Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations”を参照することを推奨。また、暗号アルゴリズムに関しては SP 800-56 “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”や FIPS140 で指定された暗号アルゴリズムの使用を推奨。SP 800-53 “Security and Privacy Controls for Federal Information Systems and Organizations”における「リモートアクセス」や「伝送される情報の機密性と完全性」のセキュリティ管理策として本文書を参照するよう求めている。 また、本書第 5 章では SP 800-64 “Security Considerations in the System Development Life Cycle”のライフサイクルモデルに基づいて、組織が行うべき SSL VPN 推奨プラクティスが明記。
概要	本文書は、 組織が SSL VPN 技術を理解し、SSL VPN の設計・実装・保護・監視及び保守を支援することを目的としたガイドライン。SSL VPN と類似技術である、IPsec VPN やその他の VPN ソリューションとの比較も実施。 SSL VPN の計画と実装にあたっては、以下に示す段階的アプローチを推奨し、各段階における考慮事項等については 4 章で解説。 1. 要件を特定する 2. ソリューションを設計する 3. プロトタイプを実装しテストする 4. ソリューションを配備する 5. ソリューションを管理する 第 5 章では、組織が行うべき SSL VPN の推奨プラクティスを SP 800-64 のライフサイクルモデルに基づき整理し、第 6 章では、他の種類の VPN のほうがより良いソリューションを提供する場合もあるとし、SSL VPN の代替案として使用されるいくつかの VPN プロトコルを説明。第 7 章では、実際のセキュリティ要件に基づく SSL VPN ソリューションの計画と実装の事例をケーススタディとして紹介。 また、本文書で示された以下の推奨事項を実施することで SSL VPN の使用を効率的かつ効果的に促進するとしている。 1. FIPS 準拠の暗号アルゴリズム、暗号スイート及び SSL バージョンのみを許可 2. 要件を特定して定義し、複数の製品を評価して適合度を判定 3. SSL VPN の計画と実装に対する段階的なアプローチを使用 4. SSL VPN 技術の限界を知る 5. SSL VPN 実装をサポートし補完する他の手段を実装
目次	1. 序説 2. ネットワーク/トランスポート層におけるセキュリティ 3. SSL VPN の基本 4. SSL VPN の計画と実装 5. SSL VPN の推奨プラクティス 6. SSL VPN の代替案 7. ケーススタディ 付録 A 用語 付録 B 略語
URL	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-113.pdf

付録 2-35 SP 800-130 “A Framework for Designing Cryptographic Key Management Systems”

題名	SP 800-130 “A Framework for Designing Cryptographic Key Management Systems”
対象読者	暗号鍵管理システムの設計者、セキュリティアナリスト、調達担当者、実装者、インテグレータ、オペレータ、及び責任者
策定年・ 文書のバージョン番号	2013 年 8 月 初版
発行機関	NIST (National Institute of Standards and Technology)
言語	英語
文書の種類・テーマ	暗号の開発実装に関連する文書 暗号鍵管理システムを設計するためのフレームワークに関する文書
文書の位置づけ	法的義務はない
他の文書との関係	鍵管理に関する基礎的知識については、SP800-57” Recommendation for Key Management, Part 1: General”の参照を求めている。
概要	本文書は、暗号鍵管理システム（Cryptographic Key Management Systems ,CKMS）を設計する際に、CKMS の設計者等が検討すべき項目や推奨事項について示したもの。CKMS の設計者は本文書で示されたフレームワークの要求事項を満たすように、ポリシーやプロシージャ、構成要素（ハードウェア、ソフトウェア、ファームウェア）、デバイスを選択し CKMS を設計する必要があるとしている。 本フレームワークにおいて、CKMS 設計者が検討すべき項目は大きく分けて以下の通りである。 ・ 暗号鍵とメタデータ ・ 相互運用性と移行 ・ セキュリティ管理 ・ テストとシステムの保証 ・ 災害からの回復 ・ セキュリティ評価 特に第５章では、暗号鍵とメタデータについて説明しており、これが CKMS の最も重要なテーマとし、以下の観点から考慮すべき事項を説明。 ・ 主要ライフサイクルの状態と遷移 ・ キーとメタデータの管理機能 ・ 暗号鍵及び/またはメタデータセキュリティ ・ キー及びメタデータ管理機能へのアクセスの制限 ・ 復旧
目次	1. 序説 2. フレームワークの基礎 3. 目的 4. セキュリティポリシー 5. 役割と責任 6. 暗号鍵とメタデータ 7. 相互運用性と移行 8. セキュリティ管理策 9. テストとシステム保証 10. 災害からの回復 11. セキュリティ評価 12. 技術的課題 付録 A 参考文献 付録 B 用語 付録 C 略語
URL	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-130.pdf

付録 2-36 SP 800-131A Rev. 1 “Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths”

題名	SP 800-131A Rev. 1 “Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths”
対象読者	システムの所有者や管理者、システム移行を計画・実行する者
策定年・ 文書のバージョン番号	2011 年 1 月（初版）、2015 年 11 月（Rev. 1） Rev. 1
発行機関	NIST (National Institute of Standards and Technology)
言語	英語
文書の種類・テーマ	暗号に関して運用・設定する文書（暗号プロトコル以外に関するもの） 暗号鍵管理（特に移行）に関するガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	2011 年 1 月に発行された SP 800-131A の改訂版。 SP 800-57 に基づき、鍵移行に関してより具体的な情報の提供を目的とする文書。
概要	鍵管理に関する SP 800-57 “Recommendation for Key Management”のうち、鍵移行に関する詳細をまとめたもの。暗号アルゴリズム及び鍵長に関する、推奨事項を説明。 ユースケースごとに利用する暗号アルゴリズムまたは鍵長について、セキュリティの強度に応じて、推奨（Approved）、容認（Acceptable）、推奨しない（Deprecated）、制限（Restricted）、推奨から除外（Legacy-use）、容認できない（Disallowed）に分けて定義。 各ユースケース及び評価されているアルゴリズムは以下の通り。 ① ブロック暗号アルゴリズムによる暗号化と復号：TDEA、SKIPJACK、AES ② 電子署名：DSA、ECDSA、RSA ③ 乱数生成：HASH_DRBG、HMAC_DRBG、CTR_DRBG ④ Diffie-Hellman 鍵共有と MQV 鍵共有 ： DH（Diffie-Hellman）、MQV（Menezes-Qu-Vanstone） ⑤ RSA 暗号方式の鍵共有と鍵配送：SP 800-56B RSA、Non-56B-compliant RSA ⑥ 鍵ラップ：AES、Two-key TDEA、three-key TDEA ⑦ 鍵導出：HMAC-based KDF、CMAC-based KDF ⑧ ハッシュ関数：SHA-1、SHA-2、SHA-3 ⑨ メッセージ認証コード（MAC）：HMAC、CMAC、GMAC
目次	1. 序論 2. ブロック暗号アルゴリズムによる暗号化と復号 3. 電子署名 4. 乱数生成 5. Diffie-Hellman 鍵共有と MQV 鍵共有 6. RSA 暗号方式の鍵共有と鍵配送 7. 鍵ラップ 8. 暗号鍵からの鍵導出 9. ハッシュ関数 10. メッセージ認証コード（MACs） 付録A レガシーユースでのアルゴリズム及び鍵を利用する際のリスク低減策 付録B 参照文献 付録C SP 800-131A からの改定箇所
URL	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf

付録 2-37 SP 800-132 “Recommendation for Password-Based Key Derivation: Part 1: Storage Applications”

題名	SP 800-132 “Recommendation for Password-Based Key Derivation: Part 1: Storage Applications”
対象読者	連邦情報システムの開発者及び使用者、各端末の使用、実装、インストール及び設定する者
策定年・ 文書のバージョン番号	2010 年 12 月 初版
発行機関	NIST (National Institute of Standards and Technology)
言語	英語
文書の種類・テーマ	暗号に関して運用・設定に関する文書（暗号プロトコル以外に関するもの） パスワードベース鍵導出関数の技術・仕様を明記する文書である。
文書の位置づけ	法的義務はない
他の文書との関係	2002 年に制定された連邦情報セキュリティマネジメント法（FISMA）で定めた NIST の義務を促進するための文書である。
概要	本文書は、電子的に保管されたデータまたはデータ保護鍵を保護するために、パスワードやパスフレーズから暗号鍵を導出する、パスワードベース鍵導出関数（password-based key derivation functions）について解説したもの。暗号鍵のランダム性はセキュリティの安全性を大きく左右する。ただし、アプリケーションの使用者が直接入力したパスワードのランダム性が足りないので、直接暗号鍵として使えない。本文書は、使用者が入力したパスワードに基づき、暗号鍵を生成する技術・仕様を詳しく説明する文書である。 第 4 章の一般論では、パスワードやパスフレーズから導出された鍵材料であるマスター鍵の使用目的について、データ保護鍵の生成とデータ保護鍵を保護する中間鍵を生成の 2 点に制限し、それ以外の目的への使用は禁止するとしている。 第 5 章は利用者が選択したパスワードを直接暗号鍵として使う危険性について説明し、パスワードベース鍵導出関数について詳細に解説。PBKDF は擬似ランダム関数及び反復回数、パスワード、ソルト、マスター鍵の鍵長で構成され、各構成要素について解説。マスター鍵の長さは 112 ビット以上にする必要があるとし、ソルトは FIPS または NIST に認証された乱数生成器によって生成される 128 ビット以上の列である必要があるとしている。反復回数はマスター鍵を生成する際に擬似ランダム関数を実行する回数で、回数が多いほどよいが、計算時間がかかるため、情報の機密性と機器の性能によって設定（最低でも 1000 回以上、重要な鍵や効能のよいシステムであれば、1000 万回以上）必要があるとしている。
目次	1. 概要 2. 発行官庁・機関 3. 定義、略語、記号 4. 一般論 5. パスワードベース鍵導出関数（PBKDF） 6. 参考文献 付録 A セキュリティ考慮事項 付録 B テスト不可能要件の適用
URL	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132.pdf

付録 2-38SP 800-133 “Recommendation for Cryptographic Key Generation”

題名	SP 800-133 “Recommendation for Cryptographic Key Generation”
対象読者	米国連邦政府またはシステムを設計、実行、使用する者
策定年・ 文書のバージョン番号	2012 年 12 月 初版
発行機関	NIST (National Institute of Standards and Technology)
言語	英語
文書の種類・テーマ	暗号に関して運用・設定に関する文書（暗号プロトコル以外に関するもの） 暗号鍵の生成手順・アルゴリズムについて説明した文書。
文書の位置づけ	法的義務はない
他の文書との関係	技術的詳細に関しては、FIPS または他の SP800 シリーズ文書を参照。
概要	認証された暗号アルゴリズムを利用した鍵生成に関する推奨事項をまとめた文章。暗号鍵生成に関連する内容を説明し、詳細については他の SP800 シリーズや FIPS シリーズを参考文献として示している。 第 4 章は鍵生成の一般論について説明し、鍵生成の種類として、「ランダムビット生成器による生成」や「他の鍵からの鍵導出」、「パスワードからの鍵導出」、「認証された鍵共有スキームを利用した鍵共有」を例示し、鍵生成は認証されたランダムビット生成器に基づき直接的または間接的に生成すべきとしている。 第 5 章ランダムビット生成器の利用では、公開鍵暗号方式・共通鍵暗号方式ともに認証されたランダムビット生成器を使用すべきとし、認証されたランダムビット生成器の詳細に関しては、SP 800-90 “Recommendation for Random Number Generation Using Deterministic Random Bit Generators”等を参照。 第 6 章公開鍵暗号方式における鍵ペアの生成では、利用する鍵ペアの生成は、鍵ペアの所有者または信頼できる機関から生成すべきとし、①電子署名、②鍵共有・配送、③鍵配布の各利用シーンでの考慮事項を説明し、参考文献を示している。 第 7 章共通鍵暗号方式における鍵生成では、共通鍵生成時の考慮事項について、①共通鍵の「直接生成法」、②生成した共通鍵の配布、③鍵共有スキームを利用した共通鍵生成、④事前に共有された鍵からの共通鍵導出、⑤パスワードからの共通鍵導出、⑥複数の鍵及び他のデータを組み合せた共通鍵導出、⑦共通鍵の置換の 7 ケースで説明。
目次	1. 概要 2. 発行官庁・機関 3. 定義、略語、記号 4. 一般論 5. ランダムビット生成器 6. 公開鍵暗号方式における鍵ペアの生成 7. 共通鍵暗号方式における鍵生成 付録A 参考文献
URL	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133.pdf

付録 2-39 SP 800-135 Rev.1 “Recommendation for Existing Application-Specific Key Derivation Functions”

題名	SP 800-135 Rev. 1 “Recommendation for Existing Application-Specific Key Derivation Functions”
対象読者	米国連邦政府またはシステムを設計、実行、使用する者
策定年・ 文書のバージョン番号	2010 年 12 月（初版）、2011 年 12 月（Rev. 1） Rev. 1
発行機関	NIST (National Institute of Standards and Technology)
言語	英語
文書の種類・テーマ	暗号に関して運用・設定に関する文書（特に暗号プロトコルに関するもの）、及び暗号に関して運用・設定に関する文書（暗号プロトコル以外に関するもの） 既存のアプリケーションに内包される鍵導出関数のセキュリティ要件に関する文書。
文書の位置づけ	法的義務はない
他の文書との関係	技術的詳細は FIPS または他の SP800 シリーズ、RFC を参照。
概要	一般的に利用されるインターネット・セキュリティ・プロトコルに含まれる独自の鍵導出関数について、セキュリティ要件を提供することを目的とした文章。 本文書でセキュリティ要件を示す鍵導出関数は下記の通りである。 ・ 米国国家標準（ANS）X9.42-2001-金融サービス業界における公開鍵暗号：離散対数暗号を使用した共通鍵暗号：ANS X9.42、RFC 2631 ・ 米国国家標準（ANS）X9.63-2001-金融サービス業界における公開鍵暗号：楕円曲線暗号を使用した鍵共有と鍵転送：ANS X9.63、RFC 3278 ・ インターネット鍵交換（バージョン 1（RFC 2409）及びバージョン 2（RFC 4306）） ・ セキュアシェル（SSH）（RFC 4251） ・ TLSv1.0（RFC 2246）、TLSv1.1（RFC 4346）、TLSv1.2（RFC 5246） ・ セキュア・リアルタイム転送プロトコル（SRTP）（RFC 3711） ・ SNMP 第 3 版に関するユーザベースセキュリティモデル（USM）（RFC 2574） ・ TPM（Trusted Platform Module）（TPM の原理（Part 1）、TPM の構造（Part 2）、TPM コマンド（Part 3））
目次	1. 概要 2. 発行官庁・機関 3. 用語、略語、数学記号 4. E-E （Extraction-then-Expansion） 鍵導出プロセス 5. 他の既存鍵導出関数 6. 参考文献 付録A 変更履歴
URL	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-135r1.pdf

付録 2-40 SP 800-152 “A Profile for U.S. Federal Cryptographic Key Management Systems”

題名	SP 800-152 “A Profile for U.S. Federal Cryptographic Key Management Systems”
対象読者	CKMS 設計者及び実装者、FCKMS 調達者、インストーラ、構成担当者、管理者、オペレータ、及びユーザを対象。ユーザとしては、連邦従業員及び連邦請負業者などを想定。
策定年・ 文書のバージョン番号	2015 年 10 月 初版
発行機関	NIST (National Institute of Standards and Technology)
言語	英語
文書の種類・テーマ	暗号の開発実装に関連する文書 連邦暗号鍵管理システムのプロファイルに関する文書
文書の位置づけ	法的義務はない
他の文書との関係	本文書は、NIST Special Publication（SP）800-130、”A Framework for Designing Cryptographic Key Management Systems”に基づく。
概要	本文書は、暗号鍵管理システムの設計と実装について示した NISTSP800-130 に基づき作成されたもので、連邦政府機関向けの暗号鍵管理システムの設計に関して、より詳細な要求事項を提供するもの。本文書で提供されるプロファイルは、暗号鍵管理システム設計者及び実装者が、適切なセキュリティサービスや鍵管理機能を選択すること、連邦鍵管理システムの調達者や管理者、サービス提供・利用組織が、適切な鍵管理システムまたは鍵管理サービスを選択できることを支援するものである。 本プロファイルで扱う、CKMS の設計者及び実装者が検討すべき項目は大きく分けて以下の通りである。 ・ 暗号鍵とメタデータ ・ 相互運用性と移行 ・ セキュリティ管理 ・ テストとシステムの保証 ・ 危機からの回復 ・ セキュリティ評価
目次	1. 序説 2. プロファイルの基礎 3. 連邦 CKMS の目的 4. セキュリティポリシー 5. 役割と責任 6. 暗号鍵とメタデータ 7. 相互運用性と移行 8. セキュリティ管理策 9. テストとシステム保証 10. 危機からの回復 11. セキュリティ評価 12. 技術的課題 付録A 参考文献 付録B 用語
URL	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-152.pdf

付録 2-41 SP 800-175A “Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies”

題名	SP 800-175A “Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies”
対象読者	主に連邦政府職員
策定年・ 文書のバージョン番号	2016 年 8 月 初版
発行機関	NIST (National Institute of Standards and Technology)
言語	英語
文書の種類・テーマ	暗号を利用したシステムの運用もしくはマネジメントに関する文書 連邦政府において暗号を使用するための要件決定に関するガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	SP800-175B の関連文書。 ポリシー策定に関しては SP 800-130 “A Framework for Designing Cryptographic Key Management System”と SP 800-152 “A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS)”「米国連邦暗号鍵管理システムのプロファイル」の参照することが求められている。また、暗号鍵管理ポリシーの必要事項に関しては SP 800-57 Part 2 “Recommendation for Key Management, Part 2: Best Practices for Key Management Organization”を参照することが求められている。
概要	連邦政府における暗号及び NIST が定める暗号基準を使用する際の基礎的なガイドライン。本文書は暗号を利用する際の要求事項を決定するためのガイダンスを提供。連邦政府が扱う機微情報保護に関連する法律や指令、保護すべき資産を特定するためのリスクアセスメント方法等について解説。 第 2 章では、NIST が発行または策定に関与した暗号標準やガイドラインに関連する法令（Cybersecurity Enhancement Act of 2014 等）を説明し、第 3 章では、 NIST が発行した暗号標準やガイドラインに関連する EOP（米国大統領行政府）からの指令について説明している。具体的には「HSPD-7：重大インフラの識別、優先順位付け及び保護」や「EO13636: 重大インフラのサイバーセキュリティ向上」などの 11 の大統領指令や大統領令などを説明。 第 4 章では、連邦政府組織が策定する必要があるポリシーとして、情報管理ポリシー、情報セキュリティポリシー、暗号鍵管理ポリシーの 3 つを示し、それぞれのポリシーの役割等を解説。 第 5 章では、セキュリティ管理要件を決定するリスクマネジメントプロセスについて、情報及び情報システムの分類、セキュリティ管理策の選択について解説。
目次	1. 序説 2. 適用される公法 3. EOP（米国大統領行政府）指令 4. 組織の方針 5. リスクマネジメントプロセス 付録 A 参考文献
URL	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175A.pdf

付録 2-42 SP 800-175B “Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms”

題名	SP 800-175B “Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms”
対象読者	連邦職員及び暗号化サービスの提供と仕様に関する担当者、プログラム管理者、技術専門家、システムの調達担当、暗号サービス利用者
策定年・ 文書のバージョン番号	2016 年 8 月 初版
発行機関	NIST (National Institute of Standards and Technology)
言語	英語
文書の種類・テーマ	暗号に関して運用・設定に関する文書（暗号プロトコル以外に関するもの） 新規・既存システムの暗号メカニズムの選択と使用に関するガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	ブロック暗号方式に関しては、SP 800-38 “Recommendation for Block Cipher Modes of Operation”を参照。 デジタル署名に関しては SP 800-102 “Recommendation for Digital Signature Timeliness”、乱数生成に関しては SP 800-90A “Recommendation for Random Number Generation Using Deterministic Random Bit Generators”を参照。 鍵管理に関しては SP 800-57 “Recommendation for Key Management”、特に暗号鍵管理システムの設計者は SP 800-130 “A Framework for Designing Cryptographic Key Management Systems”を参照すべきとし、承認された暗号アルゴリズムに関しては SP 800-133 “Recommendation for Cryptographic Key Generation”を参照。 鍵生成・鍵導出・鍵共有・鍵伝送に関しては、SP 800-108 “Recommendation for Key Derivation Using Pseudorandom Functions (Revised)”、SP 800-56 “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”、等を参照。
概要	連邦政府の機密情報保護に利用できる暗号方法とサービス、NIST の暗号標準の概要を説明したガイドライン。 第 2 章では、暗号標準の重要性並びに暗号に関する米国及び国際的な標準化機関の重要性とその役割について説明し、第 3 章では、暗号化、デジタル署名、暗号鍵生成に使用されるべき承認されたアルゴリズムを紹介。具体的には、暗号化ハッシュ関数、公開鍵暗号方式、共通鍵暗号方式のそれぞれのメカニズムに関して、NIST によって承認されたアルゴリズムを紹介。また、必要なセキュリティ強度とアルゴリズムの存続期間に関しても NIST の承認要件が記されている。 第 4 章では、データ機密性、データ完全性と送信元認証、ブロック暗号における機密性と認証の組み合わせ、乱数生成といった、機密データを保護するために推奨される暗号化サービスについて説明。 第 5 章では、これらの暗号化サービスが提供される際に使用される暗号鍵の保護と管理について説明し、鍵生成・導出・共有・伝送といった鍵確立メカニズムに関しても解説。
目次	1. 序説 2. 標準とガイドライン 3. 暗号アルゴリズム 4. 暗号サービス 5. 鍵管理 6. その他の課題 付録 A 参考文献
URL	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175B.pdf

付録 2-43 SP 800-177 “Trustworthy Email”

題名	SP 800-177 ”Trustworthy Email”
対象読者	連邦政府及び企業のメール管理者、情報セキュリティの専門家、ネットワーク管理者
策定年・ 文書のバージョン番号	2016 年 3 月 初版
発行機関	NIST (National Institute of Standards and Technology)
言語	英語
文書のテーマ・種類	暗号を利用したシステムの運用もしくはマネジメントに関する文書、及び特定の製品・サービスの利用に関する文書 信頼性のある E メールのためのガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	本文書は SP800-45“Guidelines on Electronic Mail Security”を補足するものであり、最新の証明書や暗号化技術を推奨するもの。ウェブサービスとしてのメールサービスにおけるセキュリティは SP800-95“Guide to Secure Web Services”を参照し、鍵管理等については SP800-57part1”Recommendation for Key Management, Part 1: General”を参照。また、メールサーバでのセキュリティを考慮した保存の仕方については SP800-111”Guide to Storage Encryption Technologies for End User Devices”と重なる部分があるとしている。
概要	本文書は電子メールのセキュリティを向上させるために使用するプロトコルや技術に関して推奨を提供するもの。 第 2 章で E メールシステムの概要について、メールの主要構成要素（MUA,MTA 等）やプロトコル（SMTP、POP3 等）、暗号化メールフォーマット（S/MIME、PGP 等）等について解説。 第 3 章では組織の電子メールサービスに対する脅威について完全性・機密性・可用性に分類し、攻撃の種類とその対策について解説。 第 4 章では送信ドメインと個々のメールの認証について解説。具体的には、SPF、DKIM、DMARC、電子署名によるメールメッセージの認証について概要とセキュリティ上の推奨事項について説明。 第 5 章では電子メール機密性保護に関して、電子メール送受信時と電子メールの内容保護の 2 つに分けて解説。電子メール送受信時におけるセキュリティの確保については TLS、X.509、STARTTLS、DEEP（Deployable Enhanced Email Security）、DANE についてその概要とセキュリティ推奨事項について説明。電子メールの内容保護に関しては、S/MIME、SMIMEA、OpenPGP についてその概要とセキュリティ推奨事項について説明。 第 6 章では迷惑メール減少させる方法について、承認/未承認送信者リストやドメインベースの認証、コンテンツフィルタリング、ユーザ教育の必要性について説明。 第 7 章ではローカルメールサーバと E メールクライアントの電子メールのセキュリティについて解説。
目次	1. 導入 2. 電子メールの要素 3. 電子メールサービスのセキュリティ上の脅威 4. 送信ドメインとメールメッセージの認証 5. 電子メールの機密性の保護 6. 迷惑メールの削減 7. エンドユーザの電子メールセキュリティ 付録A 略語 付録B 参考文献
URL	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177.pdf

付録 2-44 SP 1800-6B (Draft)“Domain Name Systems-Based Electronic Mail Security”

題名	SP 1800-6B (Draft) “Domain Name Systems-Based Electronic Mail Security”
対象読者	情報責任者、セキュリティ責任者、及びセキュリティ管理者
策定年・ 文書のバージョン	2016 年 11 月 (Draft)
発行機関	NIST (National Institute of Standards and Technology)
言語	英語
文書の種類・テーマ	暗号に関して運用・設定する文書（暗号プロトコルとそれ以外に関するものを両方含む）及び特定の製品・サービスの利用に関する文書 DNS システムベースの E メールのセキュリティに関するガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	SP 800-177“Trustworthy Email”の推奨事項を実装するためのプラクティスガイド。DNS システムの保護機能は、SP 800-81-2 “Secure Domain Name System (DNS) Deployment Guide.”を参照。
概要	本文書は、E メールを利用し、証明書ベースの暗号鍵と DNSSEC を利用する企業を対象に、DNS ベースの電子メールセキュリティプラットフォームの説明と必要なサービスのインストールと使用のためのガイドラインである。 第 4 章では DNS-Based Electronic Mail Security プロジェクトの詳細とリスクアセスメントの方法、電子メールへの脅威（データの盗聴や破壊、改ざん等）、プラットフォームのためのテクノロジーと要素について記載されている。リスクアセスメントとして以下の要素を考慮する。 第 5 章ではプロジェクトセキュリティプラットフォームの利用について以下の 2 つのシナリオに基づき解説。 ・ 典型的な電子メール利用:2 つの企業間の電子メールサーバが STARTTLS 拡張の TLS で通信する。 ・ エンドツーエンド署名電子メール:異なる企業のユーザ間の電子メール伝送で TLS に保護されたチャネルを使用し、署名に使われたアーティファクトが S/MIME と TLS 認証にも用いられる 第 6 章ではセキュリティプラットフォーム導入による、ユーザの使用感の変化とシステム管理者の使用感の変化について、具体的な製品を例示し解説。 第 7 章ではセキュリティプラットフォームの分析評価結果について述べている。MTA を送信するための TLS 保護チャネルを確立した。攻撃シナリオでは悪意あるユーザが転送を遮断するとした。全てのテストで送信 MUA はメッセージに署名し、受信 MUA は署名を確認した。送信 MTA は DNSSEC 認証により全ての DNS レスポンスの正確性を確認した。
目次	1. 概要 2. このガイドの使用法 3. 導入 4. アプローチ 5. アーキテクチャ 6. 結果 7. 評価 8. 今後の検討事項 付録A 略語 付録B 参考文献 付録C DNS-Based Email Security プロジェクトのフレームワークコアと参考引用への関連付け
URL	https://nccoe.nist.gov/sites/default/files/library/sp1800/dns-secure-email-sp1800-6b-draft.pdf

付録 2-45 Algorithms, key size and parameters report 2014

題名	Algorithms, key size and parameters report 2014
対象読者	組織における意思決定者及び暗号ソリューションを設計し実装する専門家
策定年・ 文書のバージョン番号	2014 年 11 月 初版
発行機関	ENISA (European union agency for Network and Information Security)
言語	英語
文書の種類・テーマ	暗号に関して運用・設定する文書（暗号プロトコル以外に関するもの）暗号アルゴリズムと暗号鍵サイズ及びパラメータに関する一連の推奨事項を記したガイドライン 暗号アルゴリズムと暗号鍵サイズ及びパラメータに関する一連の推奨事項を記したガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	本文書は、“Algorithms, key size and parameters report – 2013 recommendations”の内容を更新したもの。2013 年版から主に第 6 章の内容が追記され、暗号プロトコルの一部が拡張されている。 ECRYPT と ECRYPT II による年次報告書「アルゴリズムと鍵サイズに関する年次報告書」と強く関連しており、ECRYPT は一般的な枠組みや要約を提供している反面、本文書は暗号アルゴリズムに関する明示的な提案を行うことを目的としている。 鍵導出関数に関しては NISTSP800-108 等を参照。
概要	暗号プリミティブ、暗号スキーム、そして暗号鍵サイズに関する文書であり、現在一般的に使用されているアルゴリズムを分析し、将来のシステムにおけるアルゴリズムの決定方法に関して、最先端の提言を行うことを目標としている。 本文章では、暗号ユーザにとって重要となる、「暗号プリミティブ・暗号スキーム・暗号鍵サイズが使用可能であるかの判定」と「暗号プリミティブ・暗号スキーム・暗号鍵サイズが、新規システム・将来のシステムに適しているかの判定」の 2 つに焦点をあてている。本文書では多くの暗号プロトコルの概要を説明しているが、ある程度実用化されたもののみを扱い、学術的に先端的メカニズムは対象外としている。 第 3 章では、ブロック暗号、ハッシュ関数、ストリーム暗号などの基本的な公開鍵暗号方式の暗号プリミティブについて説明し、第 4 章では、「ブロック暗号利用モード」、「メッセージ認証符号（MAC）」、「認証付き暗号」、「鍵導出関数（KDF）」、「ハイブリッド暗号方式」等の基本的な暗号スキームについて説明。第 5 章では、より高度な暗号スキームとして、「パスワードベースの鍵導出」、「鍵ラップアルゴリズム」、「暗号化ストレージ」、「ID ベース暗号 /鍵カプセル化メカニズム」について説明。 第 6 章では、暗号プリミティブ・暗号スキームに関連した一般的な問題について説明している。具体的には、ハードウェア及びソフトウェアに対するサイドチャネル攻撃とその対策、乱数生成方法とその際のセキュリティ要件、及び暗号鍵のライフサイクル管理を説明。
目次	1. エグゼクティブサマリー 2. 本文書の読み方 3. 暗号プリミティブ 4. 基本的暗号スキーム 5. 発展的暗号スキーム 6. 一般的なコメント 参考文献
URL	https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014/at_download/fullReport

付録 2-46 The Use of Cryptographic Techniques in Europe

題名	The Use of Cryptographic Techniques in Europe
対象読者	暗号に関するガイドライン等を作成する政策立案者や電子政府所管組織の関係者
策定年・ 文書のバージョン番号	2011 年 12 月 初版
発行機関	ENISA (European union agency for Network and Information Security)
言語	英語
文書の種類・テーマ	暗号に関して運用・設定に関する文書（暗号プロトコル以外に関するもの）、暗号を利用したシステムの運用もしくはマネジメントに関する文書 電子政府において用いられる暗号化手法に関して、EU 加盟国におけるアンケート調査結果及び推奨事項を記したガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	本調査結果をもとに、EU 加盟国における基本的な暗号アルゴリズムの導入が不完全であったため、“ Recommended Cryptographic measures – Securing personal data”では暗号アルゴリズムの基本的な仕組みと推奨事項を説明。
概要	政府が保護する「秘密区分に指定されていない情報（unclassified）」を保護するために利用される、暗号仕様と推奨事項について調査した報告書。秘密区分に分類された情報を保護するための暗号については調査対象外としている。 調査は、13 の EU 加盟国を対象に実施したアンケート回答をもとに、それらの国が定義・使用している暗号のガイドライン、要件、仕様を分析し、各調査項目に対して提言をまとめている（提言に関しては 6 章でリスト化）。さらに、諸外国の暗号仕様について述べられており、米国の NIST や日本の IPA や CRYPTREC の取組が説明されている。また、暗号技術に関連する EU の取組として ECRYPT や NESSIE 等が紹介されている。 第 5 章では調査結果として、以下の推奨事項が述べられている: 1. 保護すべきデータと適切なセキュリティ対策の実施 2. 適切な暗号ポリシーの策定 3. 優れたセキュリティプラクティスに従ってソリューションを展開する 4. 暗号ポリシーの読者を理解する 5. 監査の実施 6. 暗号プロセスの開発に関する明確なガイダンスを作成する 7. 長寿命なソリューションを構築し、最新のリスクに対応する 8. 暗号政策の策定、最小要件の評価・推奨を EU 全体で行う
目次	1. エグゼクティブサマリー 2. 序説 3. 調査結果 4. 加盟国以外の暗号仕様 5. まとめ 6. 推奨リスト 7. 参考文献 付録 A 暗号仕様と推奨基準 付録 B 簡略化されたリストと質問 付録 C 背景情報 付録 D 用語と略語
URL	https://www.enisa.europa.eu/publications/the-use-of-cryptographic-techniques-in-europe/at_download/fullReport

付録 2-47 Recommended Cryptographic measures – Securing personal data

題名	Recommended Cryptographic measures – Securing personal data
対象読者	組織の意思決定者及び暗号ソリューションを設計し実装の専門家
策定年・ 文書のバージョン番号	2013 年 9 月 初版
発行機関	ENISA (European union agency for Network and Information Security)
言語	英語
文書の種類・テーマ	暗号に関して運用・設定に関する文書（暗号プロトコル以外に関するもの） 機密データ及び個人データ保護策を記したガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	本文書は、ENISA の“Algorithms, key size and parameters report – 2013 recommendations”の一部で、アルゴリズム、暗号鍵サイズ、暗号パラメータ、暗号化プロトコルの推奨事項を補完するもの。実際に暗号メカニズム使用する場合、望ましいセキュリティレベルを達成するために、上記文書の詳細情報の参照を求めている。 また本稿で紹介される防護措置は、欧州委員会規則（EC） No. 611/2013「欧州議会及び理事会の指令 2002/58/EC に基づく個人データ侵害の通達に適用される措置」を背景としている。
概要	個人データや機密データの保護措置に関する文書。暗号化、認証、ハッシュや電子署名等の個人情報を保護する基本的な暗号メカニズムに焦点をあてており、EU 加盟国における暗号化に関する最低レベルのセキュリティ要件を示したもの。 第 2 章では、情報（個人情報を含む）の保護が必要となる政策的背景や必要な措置（リスクアセスメントの実施や物理的なセキュリティ、アクセス制御やウイルス対策のような論理セキュリティ対策）等が述べられている。第 3 章では個人データのライフサイクルについて説明したうえで、ライフサイクルに応じたセキュリティ対策の概要とセキュリティ要件について述べられている。データ保護に関しては、情報の CIA（機密性、完全性、可用性）に加え、より安全性を高める方法として Forward secrecy（前方秘匿性）等について説明。 第 4 章では基本的な暗号技術として、データの暗号化・復元化手法、データ認証、ハッシングと電子署名の簡単な解説が記されている。第 5 章では基本的な暗号プリミティブとして、ブロック暗号、ストリーム暗号、ハッシュ関数、メッセージ認証符号（MAC）、RSA 問題、離散対数問題、ペアリング暗号の簡単な解説が示されている他、これらのプリミティブを強化する方法や暗号鍵管理方法についても述べられている。第 6 章では、データ侵害につながる可能性のあるいくつかの攻撃に対する保護対策を、ケーススタディとして提供。
目次	1. エグゼクティブサマリー 2. 序説 3. セキュリティ要件の特定 4. 基本的な暗号技術 5. 暗号プリミティブ 6. ケーススタディ: 保護対策 7. まとめ 8. 付録: データ最小化 9. 参考文献
URL	https://www.enisa.europa.eu/publications/recommended-cryptographic-measures-securing-personal-data/at_download/fullReport

付録 2-48 Study on cryptographic protocols

題名	“Study on cryptographic protocols”
対象読者	法人や政府の意思決定者、暗号プロトコルの分野の研究者と資金提供者、新しいプロトコルを開発している組織
策定年・ 文書のバージョン番号	2014 年 11 月 初版
発行機関	ENISA (European Union Agency for Network and Information Security)
言語	英語
文書の種類・テーマ	暗号に関して運用・設定する文書（特に暗号プロトコルに関するもの）暗号プロトコルの研究
文書の位置づけ	法的義務はない
他の文書との関係	暗号プリミティブとスキームについては姉妹レポートである、”Algorithms, key size and parameters report”で議論。 2013 年の ENISA アルゴリズム報告書では、いくつかのプロトコルについて議論が行われた。本文書では、より多くのカテゴリのプロトコルをカバーするために、2013 年報告書を拡張している。
概要	本文書の目的は、法人や政府の意思決定者が、非公開にする必要がある個人データを含む、オンライン通信を保護するために使用するプロトコルを決定することを支援することである。この目的のため本文書は、多くのカテゴリのプロトコルについて議論している。暗号プリミティブとスキームが安全であるとみなされても、プロトコル内でそれらを使用した場合、安全なはずのデータを公開してしまうような脆弱性が生じる可能性がある。 本文書のもう 1 つの目的は、標準プロトコルがセキュリティ目標を満たしていることを証明する作業の不足を指摘することである。 本文書では、プロトコルを 4 種類に分類して議論している。 ・ 一般的なプロトコル：一般的なセキュリティ要件を満たすように設計され、多数のアプリケーションで使用できるプロトコル。これらは、一般に、「参照」実装または展開がない単純なスタンドアロンのプロトコルである。例として、一般的な鍵の共有等があげられる。 ・ 特殊なプロトコル：細かく定義されたセキュリティ要件を実装することが多いプロトコル。これらのプロトコルは、利用される特定の環境に応じて、様々なアプリケーションサービスを提供するために使用されるプロトコルである。例として TLS、Kerberos、IPsec、SSH があげられる。 ・ アプリケーション固有のプロトコル：厳密に定義された特定のアプリケーション用に設計されたプロトコル。例として、UMTS / LTE、WEP / WPA、ZigBee などがあげられる。 ・ アプリケーション分野：様々なプロトコルが適用される分野であり、この文書では、クラウドコンピューティングの分野に焦点をあてている。
目次	1. 序説 2. 一般的なプロトコル 3. 特殊なプロトコル 4. アプリケーション固有のプロトコル 5. 適用分野 付録 参考文献
URL	https://www.enisa.europa.eu/publications/study-on-cryptographic-protocols

付録 2-49 Standardisation in the field of Electronic Identities and Trust Service Providers

題名	Standardisation in the field of Electronic Identities and Trust Service Providers
対象読者	セキュリティ分野の標準化に関心のある専門家
策定年・ 文書のバージョン番号	2014 年 12 月（Ver 1.0） Ver 1.0
発行機関	ENISA (European union agency for Network and Information Security)
言語	英語
文書の種類・テーマ	暗号を利用したシステムの運用もしくはマネジメントに関する文書、及び暗号に関して運用・設定に関する文書（暗号プロトコル以外に関するもの） 電子署名とトラストサービス（電子シール、電子配信サービス、電子文書、タイムスタンピングサービス及びウェブサイト認証）の分野におけるサイバーセキュリティの標準化についてまとめた報告書
文書の位置づけ	法的義務はない
他の文書との関係	暗号アルゴリズムに関しては ENISA の” Algorithms, key size and parameters report”を参照し、望ましいセキュリティレベル等を選択することを求めている。
概要	電子署名とトラストサービスプロバイダの分野におけるサイバーセキュリティ標準の重要性を説明したガイドライン。標準が必要な理由を説明し、電子 ID ベース暗号とトラストサービスプロバイダに関連する具体的な標準化活動についても議論する。 第 2 章では、一般的な情報セキュリティにおける標準の重要性について説明し、第 3 章では国際的な標準化に関する現在までの取り組みと、これを達成する際の課題を説明している。 第 4 章では、 欧州委員会が発行した「EU のサイバーセキュリティ戦略」をもとに、EU におけるサイバーセキュリティの戦略が述べられている。 第 5 章では、CEN、CENELEC、ETSI I の 3 つの標準化機関により設立された「サイバーセキュリティ調整機関（CSCG）」の役割が説明されている。CSCG は IT セキュリティ、ネットワーク・情報セキュリティ、サイバーセキュリティの分野での戦略的な助言を行う。 第 6 章では ICT 分野における EU の標準化戦略の現在のアプローチを説明している。第 7 章では、eIDAS 規則が適用される分野における標準化活動を一覧として示している。 第 8 章では、ESTI TS 119 312「電子署名とインフラストラクチャ：暗号スイート」に関連する電子署名及びインフラのための暗号スイートに関する標準の提案がなされ、付録 1 では、電子署名とトラストサービスの分野における標準化を支援するために、TS 119 312 に対してコメントを行い、新たな標準の提案を行っている。具体的には、望ましいセキュリティレベル、推奨されるハッシュ関数、使用すべき暗号スイート、RSA 暗号・楕円曲線暗号における鍵生成の際のパラメータに関してである。
目次	1. 序説 2. 情報セキュリティ分野における標準の重要性 3. サイバーセキュリティ分野における標準化の課題 4. EU のサイバーセキュリティ戦略 5. サイバーセキュリティ調整機関（CSCG） 6. 標準化オプションへの戦略 7. 電子署名及びトラストサービスプロバイダ分野における標準化活動 8. ETSI TS 119 312 の代替案の提案 付録 1 ETSI TS 119 312 の代替案の提案 付録 2 参考文献
URL	https://www.enisa.europa.eu/publications/standards-eidas/at_download/fullReport

付録 2-50 RFC2504 “User’s Security Handbook”

題名	RFC2504 “User’s Security Handbook
対象読者	システム及びネットワークの管理者、エンドユーザ
策定年・ 文書のバージョン番号	1999 年 2 月 初版
発行機関	IETF (Internet Engineering Task Force)
言語	英語
文書の種類・テーマ	暗号を利用したシステムの運用もしくはマネジメントに関する文書 ネットワークやコンピュータを利用する際のセキュリティリスクと対応策を解説
文書の位置づけ	法的義務はない
他の文書との関係	本文書は、RFC2196”Site Security Handbook”の副読本。システム・ネットワーク管理者が本文書を読む場合は、RFC2196 を参照すべきとしている。
概要	ネットワークやシステムをセキュアに保つことを補助するために、エンドユーザを対象に必要な情報を提供することを目的としたハンドブック。 インターネットやコンピュータを利用する際のセキュリティ上のリスクやその対応策等について、「集中管理されたネットワークにおけるエンドユーザ」と自身でネットワークを管理するケースのような「ネットワーク化されたコンピュータのエンドユーザによる自己管理」の 2 つのケースに分けて解説。 インターネットやコンピュータを利用する際のセキュリティリスクとして、安全ではないソフトウェア等のダウンロード、偽のウェブサイト閲覧、ウイルス感染等をあげており、それぞれに対して必要な対策等を解説。 暗号に関しては、ファイルや電子メールの暗号化の実施をあげており、適切な暗号化が実施されない場合、機密情報の窃取や盗聴のリスクがあるとしている。暗号化プログラムの例としてPGP（Pretty Good Privacy）を示し、適切な暗号化ソフトウェアの利用を推奨している。また、暗号化を利用する際には暗号化に使用するパスワード、鍵の管理を適切に実施することを求めている。 さらに、リモートログインを利用する際には、ワンタイムパスワードや SSH、SSL 等のセキュアな通信方法を利用することを推奨。
目次	1. はじめに 2. 集中管理されたネットワークにおけるエンドユーザ 3. ネットワーク化されたコンピュータのエンドユーザによる自己管理 付録 セキュリティ用語
URL	https://tools.ietf.org/html/rfc2504 https://www.ipa.go.jp/security/rfc/RFC2504JA.html （IPA による日本語翻訳版）

付録 2-51 RFC 4086 “Randomness Requirements for Security”

題名	RFC 4086 “Randomness Requirements for Security”
対象読者	設計のプロ及びアマチュア
策定年・ 文献のバージョン番号	2005 年 6 月 初版
発行機関	IETF (Internet Engineering Task Force)
言語	英語
文書の種類・テーマ	暗号の開発実装に関連する文書 パスワード、暗号鍵、IV、シーケンス番号及び同様のセキュリティアプリケーションに使う、推測不能な「乱数」を生成するためのテクニックと推奨事項に関する文書
文書の位置づけ	法的義務はない
他の文書との関係	NIST の電子署名標準の付録 3 において、プライベート鍵等として使うための擬似乱数 160 bit のシーケンスを作成するための手法を提供している。
概要	本文書は、エントロピーが乏しいソースや、従前の擬似乱数生成テクニックを使う際の多くの落とし穴を指摘し、真に乱雑なハードウェアテクニックの利用を推奨。 第 2 章では、一般化した場合の乱雑性に関する要件を提供する。 第 3 章では、エントロピー生成にかかる予測困難性等の条件を示し、エントロピー生成の方法を記載する。 第 4 章では、乱数を平滑化するための簡単な技術を紹介する。 第 5 章では、攪拌関数の仕組みについて説明し、より強固な攪拌を実施するにあたり、米国政府の AES（Advanced Encryption Standard）や、「S ボックス（substitution box）」として知られているモジュールや Diffie-Hellman 鍵交換を紹介している。また、攪拌関数の選択の方法についても提供する。 第 6 章では、擬似乱数生成をする際のセキュリティ的に悪い例をあげ、暗号技術的に強い乱数生成のテクニックを記述する。また、ここでは、アマチュアは擬似乱数生成アルゴリズムの設計を行うべきではないとしている。 第 7 章では、3 つの標準的な乱数生成器と 3 つの擬似乱数生成器（X9.82 擬似乱数生成、X9.17 鍵生成、DSS 擬似乱数生成）の手法を提供する。 第 8 章では、パスワード生成及び極めて高いセキュリティの暗号鍵を例にとり、必要とされる乱雑性について指摘する。
目次	1. 導入と概要 2. 一般的な要件 3. エントロピーのソース 4. 平滑化 5. 攪拌 6. 擬似乱数生成器 7. 乱雑性生成の例及び標準 8. 要求される乱雑性の例示 9. 結論 10. セキュリティについての考慮事項 11. 謝辞 付録 RFC1750 からの変更点
URL	https://tools.ietf.org/html/rfc4086

付録 2-52 RFC 4107 “Guidelines for Cryptographic Key Management”

題名	RFC 4107 “Guidelines for Cryptographic Key Management”
対象読者	IETF のワーキンググループ参加者とプロトコルの開発者、または鍵管理の仕方について意思決定をする者
策定年・ 文書のバージョン番号	2005 年 6 月 初版
発行機関	IETF (Internet Engineering Task Force)
言語	英語
文書の種類・テーマ	暗号に関して運用・設定する文書（暗号プロトコルとそれ以外に関するものを両方含む） 暗号鍵管理に関するガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	要求水準については RFC 2119 にある定義に基づく。
概要	本文書はシステムの鍵管理について、「自動化された鍵管理」または「マニュアルによる鍵管理」を選択する際の指針の提供を目的としたガイドライン。 一般的に、自動化された鍵管理が推奨されるが、マニュアルによる鍵管理のほうが合理的である場合もあるとし、マニュアル鍵管理を利用する際に考慮すべきセキュリティの重要事項を説明。 自動化された鍵管理が行われなければならない状況としては以下の条件を示している。 ・ N の 2 乗の鍵を管理する場合（N が大きい場合） ・ ストリーム暗号（RC4、AES-CTR、AES-CCM）を使用する場合 ・ IV（Initialization Vector）が再利用される場合 ・ 大量のデータが短期間に暗号化される必要があり、頻繁な短期セッション鍵の変更をもたらす場合 ・ 長期セッション鍵が 2 者以上で利用される場合 マニュアルによる鍵管理については以下の状況では合理的なアプローチであるとしている。 ・ 利用可能な帯域の制限や高いラウンドトリップがある環境 ・ 保護されている情報の価値が低い場合 ・ 長期セッション鍵のライフタイムのうち総トラフィックのボリュームが非常に低い場合 ・ 展開の範囲が非常に制限されている場合
目次	1. 概要 2. ガイドライン 3. セキュリティにおける考慮事項 4. 参考書目
URL	https://tools.ietf.org/html/rfc4107 http://www.ipa.go.jp/security/rfc/RFC4107JA.html（IPA による日本語翻訳版）

付録 2-53 RFC 4513 “Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms”

題名	RFC4513 “Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms”
対象読者	システムの運用管理者
策定年・ 文書のバージョン番号	2006 年 6 月 初版
発行機関	IETF (Internet Engineering Task Force)
言語	英語
文書の種類・テーマ	暗号に関して運用・設定に関する文書（特に暗号プロトコルに関するもの）、及び暗号を利用したシステムの運用もしくはマネジメントに関する文書 LDAP の認証方法・セキュリティメカニズムについて解説した文書
文書の位置づけ	法的義務はない
他の文書との関係	LDAP に関する技術詳細をまとめた RFC4510“Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map”に関連する文書の 1 つ。LDAP に関しては他に、RFC4511、RFC4512 がある。 RFC2251、RFC2829、RFC2830 からの変更点は付録 B にまとめられている。
概要	本文書は、LDAP の認証方法及びセキュリティメカニズム及び、StartTLS を利用した TLS の設定に関する詳細をまとめたもの。 LDAP が提供するセキュリティメカニズムとして以下を示している。 ・ バインド操作による認証 ・ ベンダ固有のアクセスコントロール機能のサポート ・ TLS または SASL メカニズムのセキュリティ層のデータ完全性 ・ TLS または SASL メカニズムのセキュリティ層のデータ機密性 ・ サーバ管理者によるサーバ資源の利用制限 ・ TLS プロトコルまたは SASL メカニズムによるサーバ認証 StartTLS の運用については、TLS の確立手順、認証状態における TLS の影響、TLS の暗号スイートについて解説。暗号スイートの選択に関しては、トランスポート層を介したデータ転送等について適切な保護ができること、保護するデータの機密性レベルに適しているか等を考慮事項としてあげている。 バインドオペレーションに関しては、シンプルな認証方法、SASL 認証方法について解説している。 セキュリティ考慮事項としては、一般的な LDAP、StartTLS、バインドオペレーション、SASL 等のセキュリティに関する事項について解説。
目次	1. はじめに 2. 実装要件 3. StartTLS の運用 4. 承認状態 5. バインドオペレーション 6. セキュリティ考慮事項 7. IANA に関する考慮事項 8. 謝辞 9. 規範的な参考文献 10. 参考情報 付録 A 認証と認可のコンセプト 付録 B 変更の概要
URL	https://tools.ietf.org/html/rfc4513

付録 2-54 RFC 4641 “DNSSEC Operational Practices”

題名	RFC 4641 “DNSSEC Operational Practices”
対象読者	DNSsec を展開するゾーン管理者及び DNSsec を導入したいと考えている事業者
策定年・ 文書のバージョン番号	2006 年 9 月 初版
発行機関	IETF (Internet Engineering Task Force)
言語	英語
文書の種類・テーマ	暗号に関して運用・設定する文書（特に暗号プロトコルに関するもの）DNSsec を運用する方法を示した文書
文書の位置づけ	法的義務はない
他の文書との関係	DNS に関する文書である RFC 1034“Domain Names – Concept and Facilities”と RFC 1035“Domain Names – Implementation and Specification”と、DNSsec に関して記した RFC4033“DNS Security Introduction and Requirements”に記載されている知識を前提として書かれている。 この文書は、従来文書である RFC 2541“ DNS Security Operational Considerations”を廃止し、DNSsec プロトコルの進化を反映した新たな文書となっている。
概要	DNSsec を利用して DNS を運用する一連の方法を説明した文書で、DNSsec の暗号鍵と電子署名における、暗号鍵生成・保管、電子署名生成、鍵ロールオーバ（更新）及びこれらに関連する政策に関して主に説明。 第 2 章では「信頼の連鎖」を損なうことの重大性について議論し、第 3 章では秘密鍵の生成と保管について説明している。具体的には、DNS サーバにおけるゾーン署名鍵や鍵署名鍵、鍵生成、鍵の有効期間、鍵アルゴリズム、望ましい鍵サイズ、そして鍵の保管に関して解説。 第 4 章では公開鍵に関連した事項として、DNSsec の署名の有効期限に関する考慮事項、鍵ロールオーバ、緊急時の鍵ロールオーバ計画、そして関連する政策について解説している。付録 B ではゾーン署名鍵ロールオーバ方法を 4 つのステップ（準備、有効期限の決定、鍵の利用、鍵更新）で説明している。
目次	1. 序説 2. 「信頼の連鎖」の保持 3. 鍵生成と保管 4. 署名生成、鍵ロールオーバと関連する政策 5. セキュリティ考慮事項 6. 謝辞 7. 参考文献 付録 A 用語 付録 B ゾーン署名鍵ロールオーバのハウツー 付録 C 表記規則
URL	https://tools.ietf.org/html/rfc4641

付録 2-55 RFC 4894 “Use of Hash Algorithms in Internet Key Exchange (IKE) and IPsec”

題名	RFC 4894 “Use of Hash Algorithms in Internet Key Exchange (IKE) and IPsec”
対象読者	プロトコルの実装者
策定年・ 文書のバージョン番号	2007 年 5 月 初版
発行機関	IETF (Internet Engineering Task)
言語	英語
文書の種類・テーマ	暗号の開発実装に関連する文書 IKE（Internet Key Exchange）及び IPsec におけるハッシュアルゴリズムの使用に関する文書
文書の位置づけ	法的義務はない
他の文書との関係	SP 800-119 “Guidelines for the Secure Deployment of IPv6”で参照されている。 IKEv2 と IPsec の必須アルゴリズムと推奨アルゴリズムは、RFC 4307 と RFC 4305 を参照するように求めている。
概要	本文書は、IKEv1 と IKEv2、 IPsec プロトコルがどのようにハッシュ機能を使うかについて記述しており、また、2008 年頃に相次いで発表されたハッシュ関数の脆弱性が発見された経緯を踏まえ、 MD5 及び SHA-1 アルゴリズムの劣化した衝突耐性について、こうしたプロトコルの脆弱性がどのような水準にあるのかについても説明している。 第 2 章から第 4 章では、IKEv1, IKEv2, IPsec におけるハッシュ関数の脆弱性の影響について指摘。 第 5 章では、暗号関数の選択について、複数の暗号関数が選択できるプロトコルであること、複数の暗号関数が利用できる際に、どの関数が主要なプロトコルで使用されるかについて合意する方法を持つこと、公開鍵証明書で使用すべき暗号関数を指定すること、を推奨している。 第 6 章では、ハッシュ関数の脆弱性受けて、プロトコル自体の機能の変更に関する推奨事項、及び実装者に対するプロトコル適用の変更に関する推奨事項を記載。プロトコル自体の機能の変更としては、PKIX 証明書に MD5 を利用する場合、ターゲットコリジョン攻撃が可能であるため、PKIX の WG に対し、PKIX の変更を求めている。また、実装者に対するプロトコル適用の変更に関する推奨事項としては、IKE と IPsec 自体は、ハッシュ関数に対する既知の衝突軽減攻撃の影響を受けないため、MD5 または SHA-1 の使用を禁止するなどの変更を行う必要はないとしている。一方で、認証に PKIX 証明書を使用する IKEv1 及び IKEv2 の実装は、PKIX の弱点に基づく攻撃の影響を受けやすい可能性があるため、SHA-256、SHA-384、及び SHA-512 ハッシュアルゴリズムで署名された証明書の使用を強く考慮する必要があるとしている。
目次	1. はじめに 2. IKEv1 と IKEv2 におけるハッシュ関数 3. IPsec におけるハッシュ関数 4. IKEv1 及び IKEv2 における PKIX 証明書 5. 暗号関数の選択 6. 変更推奨事項 7. セキュリティについての考慮事項 8. 参考文献 付録 謝辞
URL	https://tools.ietf.org/html/rfc4086

付録 2-56 RFC 4962 “Guidance for Authentication, Authorization, and Accounting (AAA) Key Management”

題名	RFC 4962 “Guidance for Authentication, Authorization, and Accounting (AAA) Key Management”
対象読者	認証、認可、アカウンティングの鍵管理プロトコルを含むシステム及びソリューションの設計者。 EAP メソッド設計者。セキュリティアソシエーションプロトコル設計者
策定年・ 文書のバージョン番号	2007 年 7 月 初版
発行機関	IETF (Internet Engineering Task Force)
言語	英語
文書の種類・テーマ	暗号の開発実装に関連する文書 認証、認可、及びアカウンティング（AAA）キー管理のガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	2003 年 3 月、IETF 56 AAA ワーキンググループセッションで、Russ Housley が「AAA における鍵管理」を発表しており、本文書はその発表で示された要求事項をカバーしている。
概要	本文書は、認証、認可、アカウンティング（Authentication, Authorization, and Accounting (AAA)）の鍵管理プロトコルのアーキテクチャについて解説したもの。 第 3 章では、AAA 鍵管理の要件として、以下の項目について整理している。 ・ 暗号アルゴリズムとの独立性 ・ 強力で新しいセッションキー ・ 鍵の範囲制限 ・ リプレイ検出メカニズム ・ 全ての関係者の認証 ・ ピア及びオーセンティケータの承認 ・ 鍵材料の機密性と完全性 ・ 暗号スイートの選択の確認 ・ 一意の名前付き鍵 ・ ドミノ効果の防止 ・ 利用環境にあわせた鍵のバインド 第 4 章では、AAA 鍵管理の推奨事項として以下の項目について説明している。 ・ アイデンティティの機密性 ・ 承認制限
目次	1. 序説 2. AAA の環境に関する考慮事項 3. AAA の鍵管理に関する要求事項 4. AAA の鍵管理に関する推奨事項 5. セキュリティ考慮事項 6. 引用規格 7. 参考文献 付録 鍵管理の歴史 謝辞
URL	https://tools.ietf.org/html/rfc4962

付録 2-57 RFC 6518 “Keying and Authentication for Routing Protocols (KARP) Design Guidelines”

題名	RFC6518 “Keying and Authentication for Routing Protocols (KARP) Design Guidelines”
対象読者	KMP のシステム実装者
策定年・ 文書のバージョン番号	2012 年 2 月 初版
発行機関	IETF (Internet Engineering Task Force)
言語	英語
文書の種類・テーマ	暗号の開発実装に関連する文書 ルーティングプロトコルの鍵と認証の設計に関するガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	本 RFC は、RFC 4948” Report from the IAB workshop on Unwanted Traffic March 9-10, 2006”で示されたルーティングインフラストラクチャのセキュリティを強化するための 4 つのステップの 1 つである「ルーティングプロトコルの通信されたパケットを保護する」ステップを扱っている。
概要	本文書は、ルーティングプロトコルにおけるメッセージ認証に、最新の暗号化メカニズムとアルゴリズムを適用するためのプロトコルの仕様化作業のロードマップを定義したもの。特に本文書では、セッションキーを生成・管理するために使用される主要な管理プロトコルのフレームワークを定義する。 KARP では、ルーティングプロトコル、オペレータ、及び自動鍵管理の間のインタフェースについて記述する鍵情報の概念化に焦点をあてる。 KARP の機能としては、 ①鍵テーブル抽象化、鍵管理プロトコルとルーティングプロトコル間のインタフェースを設計する。 ②各ルーティングプロトコルについて、KARP は、プロトコルがキーマテリアルをどのように表現するかと、プロトコルに依存しない鍵テーブルの概念化との間のマッピングを定義する。 ③対称鍵とグループ鍵の自動鍵管理を設計する場合、①で設計した概念化を使用して、自動鍵管理プロトコルとルーティングプロトコル間で通信する。 第 6 章では、新たなルーティングプロトコル認証メカニズムをネットワーク全体に即座に導入することは現実的ではないとし、設計者に対し、ルーティングプロトコルの認証メカニズムに関して互換性を持たせることを推奨している。 第 7 章では、KARP を設計する際の DoS 攻撃に関する注意事項を示す。 第 8 章では、ギャップ分析に関して、参考すべき文献をあげ、分析の流れを示す。
目次	1. 序説 2. ルーティングプロトコルの分類 3. 鍵管理プロトコルの将来のあり方に関する考察 4. ロードマップ 5. カテゴリ内のルーティングプロトコル 6. 少しずつの配備 7. DoS 攻撃 8. ギャップ分析 9. セキュリティの考慮事項 10. 謝辞 11. 参考文献
URL	https://tools.ietf.org/html/rfc6518

付録 2-58 RFC 7520 “Examples of Protecting Content Using JSON Object Signing and Encryption (JOSE)”

題名	RFC 7520 Examples of Protecting Content Using JSON Object Signing and Encryption (JOSE)
対象読者	JOSE 実装を行う開発者
策定年・ 文献のバージョン	2015 年 5 月 初版
発行機関	IETF (Internet Engineering Task Force)
言語	英語
文書の種類・テーマ	暗号の開発実装に関する文書 JSON 形式で署名や暗号化されたデータを表現するための仕様のサンプルリスト
文書の位置づけ	法的義務はない
他の文書との関係	”RFC7515 JSON Web Signature (JWS)”、”RFC7516 JSON Web Encryption (JWE)”、”RFC7517 JSON Web Key (JWK)”、”RFC7518 JSON Web Algorithms (JWA)”と同時に IETF JOSE WG が発行。 ”RFC7515 JSON Web Signature (JWS)”は JSON 形式で署名付きのデータを表現するための仕様を示す。 ”RFC7516 JSON Web Encryption (JWE)”は JSON 形式で暗号化されたデータを表現するための仕様を示す。 ”RFC7517 JSON Web Key (JWK)”は JSON 形式で JWS や JWE などで利用する鍵を表現するための仕様を示す。 ”RFC7518 JSON Web Algorithms (JWA)”は JWS 等で利用されるアルゴリズム等を示す。
概要	本文書は JOSE を用いた署名、暗号化の用例を示す。 JOSE は、様々なアルゴリズムを用いてコンテンツに一括して暗号化及び署名を施すことができる。 第 3 章では①楕円曲線暗号、②RSA 暗号、③メッセージ認証コードと暗号化に用いる共通鍵暗号を例に JWK のオブジェクト生成方法を示している。 第 4 章では①RSA v1.5 署名、②RSA-PSS 署名、③楕円曲線 DSA 署名、④HMAC-SHA2 整合性保護、⑤デタッチされるコンテンツの署名、⑥特殊ヘッダフィールドの保護、⑦コンテンツの保護、⑧多重署名を例に JWS のオブジェクト生成方法を示している。 第 5 章では、鍵の暗号化や鍵ラップ、鍵の共有、コンテンツの圧縮等を例に、JWE のオブジェクト生成方法を示している。 第 6 章では JWS 及び JWE の入れ子構造を示している。
目次	1. 序説 2. 用語と略語の解説 3. JSON ウェブ鍵の例 4. JSON ウェブ署名の例 5. JSON ウェブ暗号化の例 6. 署名・暗号化の入れ子構造 7. セキュリティに関する注意事項 8. 参考文献
URL	https://tools.ietf.org/html/rfc7520

付録 2-59 RFC 7525 “Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)”

題名	RFC 7525 Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)
対象読者	TLS/DTLS 通信における認証（片方向もしくは相互）、機密性、データ完全性の保護を行いたいと考えているシステム開発者
策定年・ 文献のバージョン番号	2015 年 5 月 初版
発行機関	IETF (Internet Engineering Task Force)
言語	英語
文書の種類・テーマ	暗号の開発実装に関連する文書、及び暗号に関して運用・設定に関する文書（特に暗号プロトコルに関するもの） TLS と DTLS のセキュリティを改善する推奨事項を提供するガイドライン
文書の位置づけ	法的義務はない
他の文書との関係	RFC 7457 “ Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS)”は本文書の付随文書で、TLS と DTLS に対する攻撃の理解と、本文書の推奨事項の根拠を理解するための文書。 暗号アルゴリズムに関する推奨事項は RFC 7465“ Prohibiting RC4 Cipher Suites”、RFC 3766“ Determining Strengths For Public Keys Used For Exchanging Symmetric Keys”を参照。
概要	TLS と DTLS を使用する際の推奨事項を明記した文書。本文書はベストカレントプラクティスで、TLS1.3 の仕様では、この文書に記載されている多くの脆弱性が解決される予定であるとしている。 第 3 章では、プロトコルのバージョン、 HTTP Strict Transport Security（HSTS）、データ圧縮、TLS セッション再開、TLS 再ネゴシエーション、サーバ名表示（SNI）といった TLS の仕様に関する一般的な推奨事項が示されている。各事項は、「必須」、「禁止」、「推奨」、「非推奨」、「任意」に分類され、その根拠が明記されている。 第 4 章では暗号スイートに関する推奨事項について述べており、使用を禁止する暗号スイート、使用を推奨する暗号スイートとその実装方法、推奨される暗号鍵長を説明している。 第 5 章では、本文書の推奨事項がどのようなシステムやサービスにおいて適用されるべきかが明記されており、第 6 章では、TLS に関連したより幅広いセキュリティの考慮事項が説明されている。
目次	1. 序説 2. 用語 3. 一般的な推奨事項 4. 暗号スイートに関する推奨事項 5. 適用性事項 6. セキュリティに関する考慮事項 7. 参考文献
URL	https://tools.ietf.org/html/rfc7525

付録３　用語集・略語集

用語集

用語	説明
AH	Authentication Header IPsec を構成するプロトコルの 1 つで、認証のためのメカニズムを提供するもの。
BIND	Berkeley Internet Name Domain/named DNSSEC に対応する権威 DNS サーバ兼キャッシュ DNS サーバであり、鍵の生成から署名まで DNSSEC 運用に必要なツール群を提供するもの。
CKMS	Cryptographic Key Management Systems 暗号鍵管理システムのこと。
CSP	Credential Service Provider 加入者の発行または登録を行い、クレデンシャルを加入者に対して発行する機関のこと。
DANE	DNS-Based Authentication of Named Entities 認証に関する情報を DNS を用いて通信するための仕組みのこと。
DKIM	DomainKeys Identified Mail 送信ドメイン認証方式のこと。
DMARC	Domain-based Message Authentication and Reporting Conformance SPF や DKIM 認証技術を利用して、認証の通らないメールの受信側での扱い方を定める仕組みのこと。
DNS	Domain Name System ドメイン名を管理し、ドメイン名と IP アドレスの変換を行うシステムのこと。
DNSSEC	Domain Name System Security Extensions DNS について、データ作成元の認証やデータ完全性を確認できるよう仕様を拡張したもの。
DTLS	Datagram Transport Layer Security データグラム（通信ネットワークにおいて情報が付加された情報の小さなまとまり。パケットと異なり再送制御などが行われない単純なデータの送受信単位）プロトコルのための暗号化プロトコルで、TLS に基づくもの。
EAP	PPP Extensible Authentication Protocol 認証プロトコルの 1 つ。各種の拡張認証方式を利用するための手続きをまとめたもの。
eIDAS 規則	Electronic identification and electronic Trust Services 電子署名とトラストサービスについての EU における取り組みをまとめた規則（Regulation）。国境を超えた電子取引を安全かつシームレスに実現させることが目的としている。

用語	説明
ESP	Encapsulated Security Payload IPsec を構成するプロトコルの 1 つで、暗号化及び認証機能を提供するもの。
HMAC	Hash-based Message Authentication Code ハッシュ関数を使用してメッセージ認証を行う仕組み。SHA-1 などのハッシュ関数を共通鍵と組み合わせて使用するため、暗号強度はこのハッシュ関数に依存する。
HSTS	HTTP Strict Transport Security ウェブサーバがクライアントに対し、現在接続しているアクセスを次回以降 HTTP の代わりに HTTPS を使うように伝達するセキュリティ機構のこと。
IEEE 802.11	IEEE（米国電気電子学会）により策定された、無線 LAN 関連規格の 1 つ。
IKE	Internet Key Exchange IPsec における SA（Security Association ゲートウェイ間でのコネクションのこと）を自動的に生成・管理するプロトコルのこと。
IPComp	IP Payload Compression Protocol IP ペイロード圧縮プロトコル。データグラムを圧縮するプロトコルのこと。
IPsec	IP security protocol インターネットプロトコル（IP）を用いて通信される全てのデータを秘密鍵暗号方式で暗号化するプロトコルのこと。
KDF	Key Derivation Function 鍵導出関数のこと。暗号鍵または他の秘密のデータを入力として、鍵材料と呼ばれるビット列を生成する関数。
MAC	Message Authentication Code メッセージ認証符号のこと。ネットワークを通じて伝送されたメッセージが途中で改ざんされてないかを確認するためにメッセージに付加される短いデータ。
MIME	Multipurpose Internet Mail Extensions 様々な書式が使えるようにした E メールの規格のこと。
MTA	Mail Transfer Agent E メールの送受信を行うサーバ。
MUA	Mail User Agent 電子メールの送受信や管理を行うアプリケーションソフトウェアのこと。
NSD	Name Server Daemon DNSSEC に対応する権威 DNS サーバのこと。
OCSP	Online Certificate Status Protocol デジタル証明書の有効性をリアルタイムで確認するための通信プロトコルのこと。

用語	説明
OpenPGP	Open Pretty Good Privacy データを暗号化してやりとりするためのソフトウェアの暗号化方式、手順のこと。
PGP	Pretty Good Privacy 公開鍵暗号を使用した暗号、署名のためのソフトウェアのこと。
PIV	Personal Identity Verification 個人識別情報検証。連邦政府における政府職員の身分証明用の IC カードの調達に関する施策のこと。
PKI	Public Key Infrastructure 公開鍵暗号基盤。公開鍵と秘密鍵のキーペアからなる公開鍵暗号方式を利用し、インターネット上で安全に情報のやりとりを行うセキュリティの基盤のこと。
POP3	Post Office Protocol version 3 E メールを受信する際に使用するプロトコルのこと。
RSA	Rivest-Shamir-Adleman cryptosystem 公開鍵暗号方式の 1 つで、桁数の非常に大きな数値の素因数分解が困難であることを利用した方式のこと。
RSNA	Robust security network association 様々な暗号技術を使用した、無線 LAN セキュリティの脅威に対して中程度から高いレベルの保証を提供する無線ネットワーク機能のこと。
S/MIME	Secure Multipurpose Internet Mail Extensions MIME の E メールでの公開鍵を利用した暗号化とデジタル署名についての規格。
SHA-1	Secure Hash Algorithm 1 任意の原文をもとに 160 ビットの値を生成するハッシュ関数の 1 つ。NIST により標準化されている。
SMTP	Simple Mail Transfer Protocol 簡易的な E メール送信用のプロトコルのこと。
SNI	Server Name Indication SSL/TLS の拡張仕様の 1 つで、サーバネーム表示 1 台のウェブサーバで異なる SSL 証明書を使い分けることを可能とする技術のこと。
SPF	Sender Policy Framework SMTP における送信者の偽証を防ぐ送信ドメイン認証方式のこと。
SSL/TLS	Secure Sockets Layer/Transport Layer Security セッション層に位置するセキュアプロトコル。通信の暗号化、データ完全性の確保とサーバの認証を行う。暗号通信を始めるに先立ち、ハンドシェイクと呼ばれるウェブブラウザとウェブサーバ間で確実にデータが転送されたかを確認する通信方式。
STARTTLS	TLS 接続を開始するときに使われる標準的な方式のこと。
TTA	Trusted Timestamp Authority 正確な時刻情報を提供するために信頼されているエンティティのこと。

用語	説明
TTP	Trusted Third Party 電子認証で電子証明書の発行等をおこなう、信頼性を持った第三者機関のこと。
VPN	Virtual Private Network インターネット回線上に専用線を仮想的に作る技術で、企業内のプライベートネットワーク接続などに利用される。
WEP	Wired Equivalent Privacy IEEE802.11 無線ネットワークセキュリティのためのアルゴリズム。
X.509	PKI（公開鍵基盤）における規格。S/MIME で採用されている。
暗号スイート	SSL 通信で使用される暗号化アルゴリズムの組み合わせのこと。具体的には鍵交換方式・鍵認証方式・暗号化通信方式・メッセージ認証符号方式の組み合わせを意味する。
暗号スキーム	暗号プリミティブとその他の要素（ハッシュ関数や擬似乱数等）を組み合わせてセキュリティ機能を実現する方式のこと。
暗号プリミティブ	素因数分解問題や離散対数問題等の数学的に定義される暗号の基本演算アルゴリズムのこと。
暗号モジュール	暗号機能を有するソフトウェア・ファームウェア・ハードウェア、もしくはその組み合わせのこと。
暗号利用モード	ブロック暗号を利用してブロック長よりも長いメッセージを暗号化するメカニズムのこと。
鍵ペア	公開鍵とそれに対応する秘密鍵のこと。
鍵署名鍵	鍵を署名し、ゾーン間での鍵の信頼の連鎖を形成するための鍵のこと。
クレデンシャル情報	ユーザ認証に用いられる情報のこと。
検証器	認証要求者が認証器を所持していることを、認証プロトコルを用いて確認することにより、認証要求者のアイデンティティを検証するエンティティのこと。
公開鍵	非対称（公開鍵）暗号アルゴリズムと共に使用され、秘密鍵に関連付けられた暗号鍵のこと。
公開鍵証明書	公開鍵とその所有者の情報とを結びつける証明書のこと。デジタル証明書とも呼ばれる。
再ネゴシエーション	SSL/TLS 通信のクライアント、ウェブサーバ双方から暗号化のパラメータの更新を行うこと。
サイドチャネル攻撃	暗号処理装置が発する電磁波や熱、処理時間等の違いを物理的手段で観察することにより、暗号解読の手がかりを得ようと試みるサイバー攻撃の 1 つ。
サニタイズ	データを簡単に取り出したり再現したりできないという合理的な保証を得るために記憶媒体からデータを削除するプロセスのこと。
サーバ証明書	通信先のサーバ運営組織が実在することを証明し、ウェブブラウザとウェブサーバ間で暗号化通信を行うための電子証明書のこと。

用語	説明
信頼の連鎖	公開鍵の正当性を担保する仕組みのこと。公開鍵のハッシュ値（DS)を権威 DNS サーバに送信し、DS が正しい場合、権威 DNS サーバの秘密鍵で署名することにより正当性を担保。
ストリーム暗号	共通鍵暗号の一種で、1 ビットずつあるいは数ビットずつ逐次処理する暗号方式のこと。
ゾーン	1 つの権威 DNS サーバが管理する範囲のこと。
タイムスタンプ	適時性の保証を提供するために使用される情報のパケットのこと。タイムスタンプには､時間を含むタイムスタンプ付きデータと､TTA によって生成された署名が含まれる。
楕円曲線 DSA	Digital Signature Algorithm について楕円曲線暗号を用いたもの。同じセキュリティ強度を実現するための鍵長が短くて済む。
デジタルアイデンティティ	Digital Identity 人やデバイス、サービスを含めた属性情報を管理する主体の属性情報の集合であるアイデンティティをデジタルで表現したもの。
ドメインパラメータ	公開鍵暗号アルゴリズムと共に鍵ペア生成、電子署名生成、鍵材料の確立に使用されるパラメータのこと。
ハイブリッド暗号方式	共通鍵暗号方式と公開鍵暗号方式を組みあわせた暗号方式のこと。
フェデレーション	複数の組織間で、相互に信頼関係を結びアイデンティティ情報を交換できる仕組みのこと。
ブロック暗号	共通鍵暗号の一種で、情報をブロックと呼ばれる一定長のまとまりに分割して処理する暗号方式のこと。
ペアリング暗号	Pairing-based cryptography 公開鍵暗号方式の一種で、離散対数問題に基づく暗号方式のこと。ペアリングと呼ばれる数式を利用する。
離散対数暗号	離散対数問題を扱った公開鍵暗号方式のこと。ElGamal 暗号などがある。
リゾルバ	ネームサーバにホスト名を通知して IP アドレスの検索を依頼したり、その逆を依頼したりするプログラムのこと。
ルーティングプロトコル	ルーター同士がネットワーク上の任意の 2 ノード間の経路を選択するための情報をやりとりする通信プロトコルのこと。
ルート CA 証明書	電子証明書を発行する認証局（CertificationAuthority）のうち最高位に位置する認証局（ルート CA）が発行する電子証明書のこと。

略語集

略語	正式名称
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CRYPTREC	Cryptography Research and Evaluation Committees
ENISA	European Union Agency for Network and Information Security
ETSI	The European Telecommunications Standards Institute

略語	正式名称
ETSI TS	ETSI Technical Specification
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act of 2002
HSPD	Homeland Security Presidential Directive
IANA	Internet Assigned Number Authority
IETF	Internet Engineering Task Force
NISC	National center of Incident readiness and Strategyfor Cybersecurity
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
RFC	Request for Comments