独立行政法人**情報処理推進機構**

〒113-6591
東京都文京区本駒込2-28-8　文京グリーンコートセンターオフィス16階
http://www.ipa.go.jp/

暗号アルゴリズムの利用実績に関する調査報告書

令和５年３月１日

This page is intentionally left blank

目次構成

1. 調査業務の背景と目的

1.1. 背景

独立行政法人情報処理推進機構（以下「IPA」という。）が、総務省、経済産業省、国立研究開発法人情報通信研究機構（以下「NICT」という。）と共同で運営している暗号技術評価プロジェクト CRYPTREC では、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討しており、その成果の一環として CRYPTREC 暗号リストを公表している。

同リストは、内閣サイバーセキュリティセンターが公表している「政府機関の情報セキュリティ対策のための統一基準」において、暗号・電子署名に係る規定での遵守事項として参照することが求められている。

現行の CRYPTREC 暗号リストが改定から 10 年が経過することを考慮し、CRYPTREC では、2022 年度末の再改定に向けた検討を行っているところである。その際、推奨候補暗号リストから電子政府推奨暗号リストへの昇格は、「製品化、利用実績等」の観点を踏まえて判断することが決められている。

1.2. 目的

本調査では、CRYPTREC 暗号リスト、特に推奨候補暗号リストに掲載されている暗号アルゴリズムについて電子政府推奨暗号リストへの昇格是非を判断するための重要な判断指標となる「暗号アルゴリズムの製品化、利用実績」についてアンケートを中心とした調査を行い、対象となる個々の暗号アルゴリズムが、どの程度の製品やシステム等に搭載されているか、またどの程度の標準規格等に採用されているか、について明らかにする。

本調査結果は、2022 年度末の CRYPTEREC 暗号リスト改定における重要な情報として、総務省、経済産業省、NICT 及び CRYPTREC 検討会・各委員会とで共有し、リスト改定作業に活用する。併せて、概要については、CRYPTREC Report 2022 や CRYPTREC シンポジウム 2023 を通じ、一般に公開する。

1.3. 実施作業内容

本調査は、以下の５つの調査により構成される。

①応募暗号アルゴリズムの応募者に対するアンケート調査
②暗号アルゴリズムを搭載している市販製品に対する調査
③日本の政府機関等に対する調査
④国際標準規格・民間規格等に対する調査
⑤オープンソースソフトウェアでの利用実績調査

上記①～⑤の調査については、報告書中では以下のように表記する。

表 1.1 報告書中での表記

調査	報告書中での表記
①応募暗号アルゴリズムの応募者に対するアンケート調査	応募者調査（調査A）
②暗号アルゴリズムを搭載している市販製品に対する調査	市販製品調査（調査B）
③日本の政府機関等に対する調査	政府系情報システム・情報システム規格調査（調査C）
④国際標準規格・民間規格等に対する調査	標準規格・民間規格・特定団体規格調査（調査D）
⑤オープンソースソフトウェアでの利用実績調査	オープンソースソフトウェア調査（調査E）

本調査における実施作業の概要図を以下に示す。

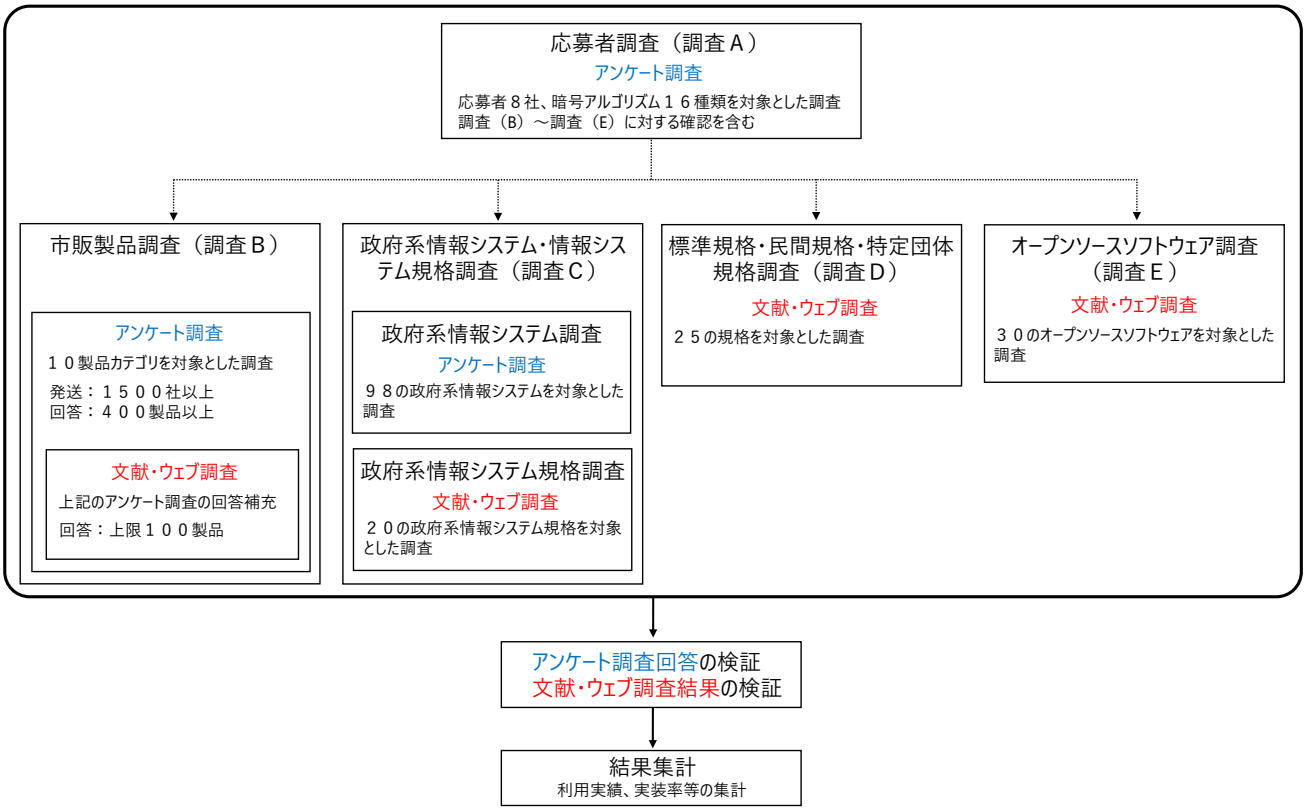

図 1.1 実施作業概要図

1.4. 実施スケジュール

各調査の実施スケジュールを以下に示す。

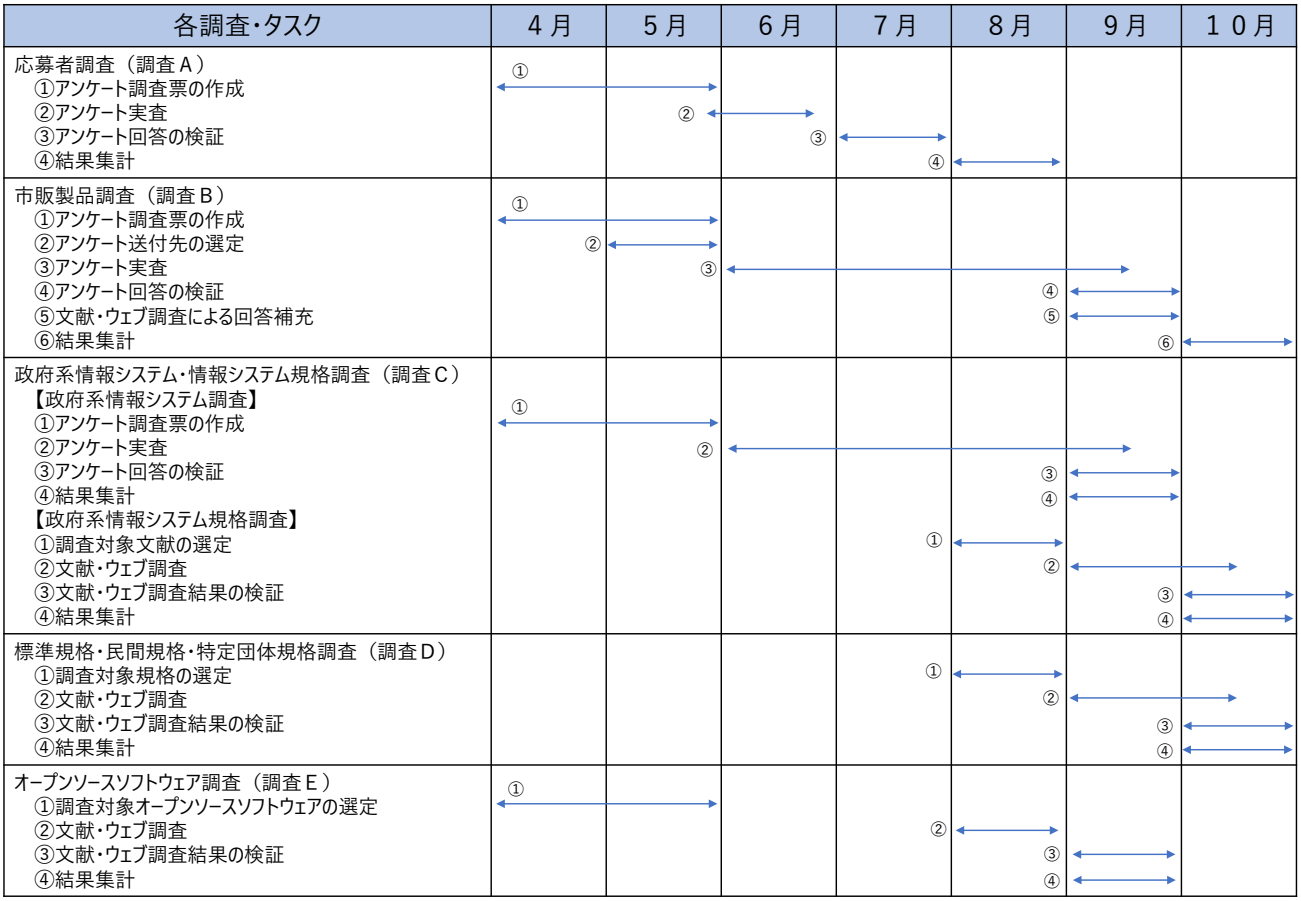

図 1.2 実施スケジュール概要図

2. 調査・集計方法

2.1. 応募者調査（調査A）

電子政府推奨暗号アルゴリズムの応募者８社に対して、2001 年度及び 2009 年度の CRYPTREC の公募に当該会社が応募した暗号アルゴリズムの製品化、利用実績についてのアンケート調査を実施した。以下に調査Ａの概要を示す。

表 2.1 調査A概要

No	項目	内容
1	調査期間	2022 年 5 月 25 日（水）から 2022 年 6 月 24 日（金）までの１か月間
2	調査方法	アンケート調査 ・CRYPTREC 暗号リスト掲載暗号技術の問合せ先として登録されている担当者や問い合わせ窓口のメールアドレス宛にアンケート調査への協力を依頼
3	調査対象	電子政府推奨暗号アルゴリズムの応募者８社
4	調査項目	１．電子政府推奨暗号アルゴリズムに関する情報 ２．暗号アルゴリズムを利用した製品・システムに関する情報
5	集計・活用方法	１．電子政府推奨暗号アルゴリズムに関する情報 ・調査Ｃ、調査Ｄ、調査Ｅの調査対象・範囲を検討する際に活用 ２．暗号アルゴリズムを利用した製品・システムに関する情報 ・本情報の集計結果を検証したうえで調査Ｂの集計結果に追加

2.1.1. アンケート調査

調査Ａのアンケート調査の対象企業と対象の暗号アルゴリズムの種類及びアンケート調査項目の概要を以下に示す。また、実際に使用した調査票は、６．付録一覧の１．調査票（Ａ）を参照。

（１）アンケート調査対象（調査Ａ）

調査Ａのアンケート調査の対象である電子政府推奨暗号アルゴリズムの応募者８社と 16 種類の暗号アルゴリズムを以下に示す。

表 2.2 アンケート調査対象詳細（調査Ａ）

No	企業名	No	対象暗号アルゴリズム
1	ソニー株式会社	①	CLEFIA
2	株式会社日立製作所	②	Enocoro-128v2
		③	MUGI

		④	MULTI-S01
3	KDDI 株式会社	⑤	KCipher-2
4	日本電気株式会社	⑥	CIPHERUNICORN-E
		⑦	CIPHERUNICORN-A
		⑧	PC-MAC-AES
5	富士通株式会社	⑨	ECDSA
		⑩	ECDH
		⑪	SC2000
6	日本電信電話株式会社	⑫	PSEC-KEM
		⑬	Camellia
7	株式会社東芝	⑭	Hierocrypt-L1
		⑮	Hierocrypt-3
8	三菱電機株式会社	⑯	MISTY1

（2）アンケート調査項目（調査A）

調査Aのアンケート調査項目の概要を以下に示す。

表 2.3 アンケート調査項目概要（調査A）

No	設問
1	電子政府推奨暗号に提案している暗号アルゴリズム名称
2	上記の暗号アルゴリズムが採択されている国際標準規格
3	上記の暗号アルゴリズムを指定している国際的な民間規格（プロトコル規格を含む）等
4	上記の暗号アルゴリズムを指定または推奨している、政府機関が利用する法令・ガイドライン等
5	上記の暗号アルゴリズムを指定または推奨している業界団体規格
6	上記の暗号アルゴリズムが実装されているオープンソースソフトウェア
7	上記の暗号アルゴリズムの利用状況（①市販製品・システム、②官公庁・地方自治体・公共機関等への納入システム、③その他有益と考えられる情報等）

※上記の No.3～No.6 の詳細は、後述の 2.2. 市販製品調査（調査 B）の 2.2.1. アンケート調査を参照

（3）アンケート調査項目（国際標準規格）

アンケート調査対象の国際標準規格を以下に示す。

表 2.4 アンケート調査項目（国際標準規格）

No	国際標準規格
1	ISO/IEC 9796 (Digital signature schemes giving message recovery)
2	ISO/IEC 9797 (Message Authentication Codes (MACs))
3	ISO/IEC 10116 (Modes of operation for an n-bit block cipher)
4	ISO/IEC 10118 (Hash-functions)
5	ISO/IEC 14888 (Digital signatures with appendix)
6	ISO/IEC 18033 (Encryption algorithms)
7	ISO/IEC 19772 (Authenticated encryption)
8	ISO/IEC 29192 (Lightweight cryptography)
9	ISO/IEC 7816 (Identification cards - Integrated circuit cards -)
10	ITU-T Y.SecMechanisms (NGN Security Mechanisms)
11	ITU-T H.233 / H.234 (audiovisual services)
12	ITU-T H.235 (Multimedia systems)
13	ICAO Doc 9303 (Machine readable travel documents)
14	その他（対象団体：ISO/IEC、ITU-T、ICAO）

2.2. 市販製品調査(調査 B)

IPA より提示された調査対象の製品カテゴリ（表 2.6 参照）を取り扱う代表的な業界団体の会員企業や、公開情報により当該製品カテゴリの製品を販売していることが確認された企業で、かつコンタクトポイントを持つ企業などを対象に、当該会社の市販製品にどの暗号アルゴリズムが搭載されているか等について、アンケート調査を実施した。

表 2.5 調査Ｂ概要

No	項目	内容
1	調査期間	2022 年 6 月～9 月
2	調査方法	１．調査対象の製品カテゴリを取り扱う代表的な業界団体の会員企業を対象としたアンケート調査（以下「業界団体調査」という。） ・当該業界団体に対して、アンケート調査への協力を依頼 ２．公開情報により当該製品カテゴリの製品を販売していることが確認された企業で、かつコンタクトポイントを持つ企業を対象としたアンケート調査（以下「個別企業調査」という。） ・当該企業に対して、個別にアンケート調査への協力を依頼 ３．電子政府推奨暗号アルゴリズムの応募者を対象としたアンケート調査（以下「応募者」という。） ・当該応募者に対して、個別にアンケート調査への協力を依頼 ４．弊社が提供しているインターネットアンケート事業（TrueNavi）が抱える調査パネルのうち、技術系（ソフトウェア、ネットワーク）及び技術系（電気、電子、機械）の職種のパネルを対象としたアンケート調査（以下「インターネットアンケート調査」という。） ・当該インターネットアンケート事業（TrueNavi）が持つインターネットアンケートシステムを活用して、アンケート調査を実施 ５．文献・ウェブ調査 ・アンケート調査回答の補充のため実施
3	調査対象	１．業界団体調査 ・業界団体 14 団体、会員企業総数 2,535 社 ２．個別企業調査 ・個別企業 108 社 ３．応募者調査 ・電子政府推奨暗号アルゴリズムの応募者８社 ４．インターネットアンケート調査 ・調査パネル 23,747 名 ５．文献・ウェブ調査 ・JISEC（IPA）による公開情報等をもとにした上限 100 製品
4	調査項目	・暗号アルゴリズムを利用した製品・システムに関する情報

5	集計・活用方法	・業界団体調査、応募者調査、文献・ウェブ調査については、回答全件を有効回答として扱う ・個別調査については、調査票にて回答があったものについては、有効回答として扱う。調査票での回答が得られなかったものについては、ヒアリングを実施し、有効回答とは分離して、今後の調査に向けた課題分析の材料として扱う ・インターネットアンケート調査については、回答内容を精査し、信頼に足ると判断された回答については、有効回答として扱う。それ以外の回答については、今後の調査に向けた課題分析の材料として扱う ・有効回答について、同一会社の製品・システムは最大5製品・システムまでとする制限や製品・システムの重複を確認して集計

調査対象の製品カテゴリを以下に示す。

表 2.6 アンケート調査項目（製品カテゴリ）

No	製品カテゴリ	代表例（例示）
1	暗号化ツールキット/ライブラリ	暗号化ツールキット、ライブラリ
2	アプリケーションソフトウェア	暗号化メール関連ソフトウェア、ファイル暗号化ソフトウェア（除外：暗号化ツールキット）、ブラウザ、オンラインバンキングソフトウェア、オンライントレードソフトウェア、金融系ソフトウェア、その他ソフトウェア全般
3	ネットワーク装置（無線含む）	ルータ・スイッチ、イーサネット暗号化装置、VPN 装置、ネットワークシステム、その他ネットワーク関連機器、ネットワークソフトウェア
4	ストレージ／外部記憶装置	ストレージ関連機器、データベース、USB メモリ／SD メモリカード／ハードディスク
5	サーバー／端末	サーバー関連機器、PC 本体、周辺機器（ソフトウェアを除く）、スマートフォン／携帯電話、ハンディターミナル／POS／ATM
6	カード／IC チップ	IC カード／SIM カード／関連ソフトウェア、カードリーダライタ／関連ソフトウェア、汎用 IC、特定用途 IC、IC 組込用ソフトウェア
7	ハードウェアセキュリティモジュール	HSM、TPM
8	IoT 機器	ネットワーク制御型家電／関連ソフトウェア、デジタルカメラ／Web カメラ、カーナビ／車載機器／関連ソフトウェア、ゲーム機、スマートメータ、監視カメラ、RFID/タグ、センサー

		（センサーチップ）、NFC セキュリティ製品（除外：カード）
9	システム	シンクライアントシステム、情報漏洩対策システム、テレビ会議システム、電話・無線・音声システム、シネマコンテンツ配信システム、オンライン教育システム、見守りシステム、DRM／著作権保護システム
10	サービス	データ預かりサービス、クラウドサービス、大容量データ転送サービス、電子認証局サービス、ユーザ認証サービス、タイムスタンプサービス、署名生成サービス
11	その他	上記に該当しない

2.2.1. アンケート調査

市販製品調査（調査 B）におけるアンケート調査対象の詳細やアンケート調査項目の概要を以下に示す。

（1）アンケート調査対象（調査Ｂ）

前述した業界団体調査の調査対象として設定した業界団体とその会員企業数、全 14 業界団体、2,535 社を対象に実施した。

（2）アンケート調査項目（調査Ｂ）

アンケート調査の設問項目を以下に示す。

表 2.7 アンケート調査項目概要（調査Ｂ）

No	設問項目
1	暗号アルゴリズムを組込んだ製品・システム等の名称
2	上記の製品・システム等の発売／提供時期 （①発売／提供開始時期、②発売／提供予定時期、③納入時期、④納入予定時期）
3	上記の製品・システム等の製品カテゴリ
4	上記の製品・システム等に関する製造・販売及び OEM 等 （①暗号アルゴリズムを含め自らが製品・システムを開発／製造している、②暗号アルゴリズム部分は他社の暗号製品を利用し、上位の製品・システムを開発／製造している、③製品・システムを販売している）
5	上記の製品・システム等が利用しているオープンソースソフトウェア
6	上記の製品・システム等が実装している暗号アルゴリズム（暗号アルゴリズム名称）及び鍵長
7	上記の製品・システム等が実装しているエンティティ認証の仕様及び対応している規格

8	上記の製品・システム等で利用している国際的な民間規格（プロトコル規格を含む）等
9	上記の製品・システム等で準拠している業界団体規格
10	上記の製品・システム等が暗号アルゴリズムを実装していることを明示的に読み取れる情報及び情報の提供条件（入手可能な条件）
11	上記の製品・システム等に関する第三者評価・試験及び認証制度の取得状況及び検討状況（①認証取得済み、②評価・試験・認証中、③認証取得検討中、④検討していない）
12	上記の製品・システム等において、今後、組込みを検討・計画している暗号アルゴリズム（暗号アルゴリズム名称）及び鍵長

（3）アンケート調査項目（暗号アルゴリズム）

アンケート調査では、ストリーム暗号と認証暗号、暗号利用モードとメッセージ認証コード、守秘と鍵交換をそれぞれ一体として扱い、①共通鍵暗号（64 ビットブロック暗号）、②共通鍵暗号（128 ビットブロック暗号）、③共通鍵暗号（ストリーム暗号・認証暗号）、④暗号利用モード／メッセージ認証コード、⑤公開鍵暗号（署名）、⑥公開鍵暗号（守秘・鍵交換）、⑦ハッシュ関数の 7 種類に分類して、調査対象製品・システム等での表 2.8 に記載の暗号アルゴリズムの利用実績調査を実施した。

表 2.8 アンケート調査項目（暗号アルゴリズム）

分類	小分類	暗号アルゴリズム	分類	小分類	暗号アルゴリズム
共通鍵暗号	64 ビットブロック暗号	CAST-128	暗号利用モード／メッセージ認証コード		GCM
		CIPHERUNICORN-E			GMAC
		Hierocrypt-L1			HMAC
		HIGHT			OFB
		MISTY1			PC-MAC-AES
		Triple DES			XTS
	128 ビットブロック暗号	AES			その他
		ARIA	公開鍵暗号	署名	DSA
		Camellia			ECDSA
		CIPHERUNICORN-A			KC-DSA
		CLEFIA			RSA-PSS
		Hierocrypt-3			RSASSA-PKCS1-v1_5 (RSA 署名)
		GOST			
		SC2000			SM2
		SEED		守秘・鍵交換	DH
		SMS4			ECDH
	ストリーム暗号・認証暗号	ChaCha20-Poly1305			PSEC-KEM
		Decim v2			RSAES-PKCS1-v1_5 (RSA 暗号)
		Enocoro-128v2			
		KCipher-2			RSA-OAEP
		MUGI		その他	
		MULTI-S01	ハッシュ関数		RIPEMD-160
		RC4			SHA-1
		Rabbit			SHA-224
		SNOW			SHA-256
	その他				SHA-384
暗号利用モード／メッセージ認証コード		CBC			SHA-512
		CBC-MAC			SHA-512/256
		CCM			SHA3-256
		CFB			SHA3-384
		CMAC			SHA3-512
		CTR			SHAKE128
		CTS			SHAKE256
		ECB			SM3
					その他

（4）アンケート調査項目（エンティティ認証の仕様）

アンケート調査対象のエンティティ認証の仕様を表 2.9 に示す。調査対象製品・システム等での表 2.9 に記載のエンティティ認証の利用実績調査を実施した。

表 2.9 アンケート調査項目（エンティティ認証の仕様）

No	エンティティ認証の仕様
1	ISO/IEC 9798-2
2	ISO/IEC 9798-3
3	ISO/IEC 9798-4
4	その他

（5）アンケート調査項目（国際的な民間規格（プロトコル規格を含む））

アンケート調査対象の国際的な民間規格（プロトコル規格を含む）を表 2.10 に示す。調査対象製品・システム等での表 2.10 に記載の規格の利用実績調査を実施した。

表 2.10 アンケート調査項目（国際的な民間規格（プロトコル規格を含む））

No	国際的な民間規格（プロトコル規格を含む）
1	IETF TLS
2	IETF IPsec
3	IETF S/MIME
4	IETF PGP
5	IETF OAuth
6	IETF SSH
7	IETF X.509
8	IETF DNSSec
9	IETF Kerberos
10	IEEE802.1
11	IEEE802.11
12	IEEE802.15
13	IEEE802.16
14	IEEE802.21
15	IEEE P1619
16	その他（対象団体例：IETF, IEEE 等）

（6）アンケート調査項目（業界団体規格（業界団体名））

アンケート調査対象の業界団体規格（業界団体名）を表 2.11 に示す。調査対象製品・システム等での表 2.11 に記載の規格の利用実績調査を実施した。

表 2.11 アンケート調査項目（業界団体規格（業界団体名））

No	業界団体規格（業界団体名）
1	Bluetooth SIG, Inc
2	Wi-Fi Alliance
3	Association of Radio Industries and Broadcast (ARIB)
4	IPTV フォーラム
5	Advanced Access Content System (AACS)
6	一般財団法人日本データ通信協会タイムビジネス認定センター
7	Europay 、MasterCard、Visa (EMV)
8	3rd Generation Partnership Project (3GPP)
9	Trusted Computing Group (TCG)
10	FIDO Alliance
11	その他

（7）アンケート調査項目（第三者評価・試験及び認証制度）

アンケート調査対象の第三者評価・試験及び認証制度を表 2.12 に示す。調査対象製品・システム等での表 2.12 に記載の認証制度の利用実績調査を実施した。

表 2.12 アンケート調査項目（第三者評価・試験及び認証制度）

No	第三者評価・試験及び認証制度
1	IT セキュリティ評価及び認証制度（JISEC）
2	JISEC 以外での ISO/IEC 15408（Common Criteria）認証
3	日本の暗号モジュール試験及び認証制度（JCMVP）
4	北米の暗号モジュール試験及び 認証制度（CMVP/FIPS140）
5	その他のセキュリティ製品認証制度

（8）アンケート調査項目（オープンソースソフトウェア）

アンケート調査対象のオープンソースソフトウェアを表 2.13 に示す。調査対象

製品・システム等での表 2.13 に記載のオープンソースソフトウェアの利用実績調査を実施した。

表 2.13 アンケート調査項目（オープンソースソフトウェア）

分類	オープンソースソフトウェア名称	分類	オープンソースソフトウェア名称
言語等	Java	暗号化ライブラリ	OpenSSL
	PHP		Network Security Service (NSS)
	python		GnuPG
開発環境	Gitlab		Mcrypt
	Redmine		BouncyCastle
	Eclipse		libsodium
ブラウザ	Webkit	圧縮ツール	7-zip
	Chrome	OS	Linux
Web サーバー	Apache		FreeBSD
	Nginx		Debian
ファイルサーバー	samba		Android
	MySQL		mbedOS
	PostgreSQL		Ubuntu
	Redis	認証	Keycloak
アプリケーション	OpenOffice	コンテナ	Docker
		その他	上記の分類に関係なく

2.3. 政府系情報システム・情報システム規格調査（調査C）

デジタル庁及びIPAの協力のもと政府機関で利用する情報システムにおいて、表2.8に記載の暗号アルゴリズムごとの利用実績の集計を行った。また、法省令・ガイドライン・政府系情報システム規格において採用されている暗号アルゴリズムについて公開情報ベースでの調査を行った。公開情報の調査対象は、暗号を利用していると想定される法省令・ガイドライン・政府系情報システム規格から、IPAと相談のうえ決定した。

表2.14 調査C概要

No	項目	内容
1	調査期間	2022年6月～10月
2	調査方法	1．アンケート調査 ・アンケート調査票の送付・回収はデジタル庁及びIPAが実施した。また、政府系情報システムの匿名処理後の集計は野村総合研究所が実施した 2．公開情報調査 ・文献・ウェブ等の公開情報をもとに調査を実施した
3	調査対象	1．アンケート調査対象 ・政府機関で利用する情報システム　98システム 2．公開情報調査対象 ・IPAと相談のうえ決定した公開されている各種政府系規格（法省令・ガイドライン・政府系情報システム規格等）
4	調査項目	1．アンケート調査 ・政府系情報システムにおける暗号アルゴリズムの利用実態 2．公開情報調査 ・政府系規格（法省令・ガイドライン・政府系情報システム規格等）における暗号アルゴリズムの採用実績
5	集計・活用方法	1．アンケート調査 ・政府機関で利用する情報システム98システムに関する回答を集計 2．公開情報調査 ・調査対象の政府系規格（法省令・ガイドライン・政府系情報システム規格等）において明示的に読み取れる調査対象暗号アルゴリズムを集計

2.3.1. アンケート調査

政府系情報システムに関するアンケート調査では、デジタル庁及び IPA がアンケート送付と回収を行い、野村総合研究所が集計を行った。政府系情報システムの調査項目概要を表 2.15 に示す。

（1）アンケート調査項目（調査C：政府系情報システム）

アンケート調査の設問項目を以下に示す。

表 2.15 アンケート調査項目概要（調査C：政府系情報システム）

No	設問項目
1	暗号アルゴリズムを組込んだシステム等の名称または識別子
2	上記のシステム等が利用しているオープンソースソフトウェア
3	上記のシステム等が実装している暗号アルゴリズム（暗号アルゴリズム名称）及び鍵長
4	上記のシステム等が実装しているエンティティ認証の仕様及び対応している規格
5	上記のシステム等で利用している国際的な民間規格（プロトコル規格を含む）等
6	上記のシステム等で準拠している業界団体規格
7	上記のシステム等における第三者評価・試験及び認証制度の取得製品の利用状況

2.3.2. 公開情報調査

日本の政府機関等に対する調査では、政府系規格（法省令・ガイドライン・政府系情報システム規格等）において採用されている暗号アルゴリズムについて調査を実施した。

表 2.16 に調査対象の政府系規格の文書入手先 URL を示す。

表 2.16 調査C：政府系規格 公開情報調査対象詳細

No	政府系規格名	文書入手先 URL（最終調査日）
1	電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針 [2020 年版]	http://www.meti.go.jp/policy/netsecurity/docs/esig/sisin.pdf（2022 年 9 月 27 日）
2	公的個人認証サービス 利用者証明用認証局 運用規程 第 2.1 版（2021 年 9 月 1 日）	https://www.jpki.go.jp/ca/pdf/auth_cps.pdf（2022 年 9 月 27 日）
3	商業登記認証局「電子証明書の方式等に関する件(告示)」（2019 年 11 月 29 日変更)	https://www.moj.go.jp/ONLINE/CERTIFICATION/SYSTEM/system.html（2022 年 10 月 13 日）
4	政府認証基盤(GPKI) 政府認証基盤相互運用性仕様書 2021 年版	https://www.gpki.go.jp/session/CompatibilitySpecifications.pdf（2022 年 9 月 27 日）
5	住民基本台帳法(昭和 42 年法律第 81 号)	https://www.ipa.go.jp/security/jisec/certified_pps/c0284/c0284_it0312.ht

	住民基本台帳カード Version 2 組込みソフトウェア プロテクションプロファイル [2011 年 1 月 21 日]	ml（2022 年 9 月 27 日）
6	標準テレビジョン放送等のうちデジタル放送に関する送信の標準方式第八条第一号及び第二号の規定に基づくスクランブルの方式 平成 26 年 7 月 3 日 総務省告示第 235 号 （平成 27 年 3 月 20 日施行)	https://www.tele.soumu.go.jp/horei/law_honbun/72ab4145.html（2022 年 9 月 27 日）
7	政府認証基盤(GPKI)ブリッジ認証局（BCA）との相互認証業務に関する CP/CPS（Ver. 5.0）[令和元年 11 月 29 日]	https://www.moj.go.jp/content/001307027.pdf
8	LGPKI 組織認証局 R2 CPCPS - 地方公共団体組織認証基盤(LGPKI) [2020]	https://www.lgpki.go.jp/doc/C-6-3-6_CPCPS_OCA_20220214.pdf
9	LGPKI 技術仕様書 [20190520]	https://www.lgpki.go.jp/doc/C-6-4-5_LG_tech_LGPKI_spec_20190520.pdf
10	認証業務及びこれに附帯する業務の実施に関する技術的基準 [令和三年二月十五日]	https://www.soumu.go.jp/main_content/000392344.pdf
11	商業登記認証局「電子証明書の方式等に関する件（告示）[2019. 11. 29] 付録 1 電磁的記録への記録方式（ASN. 1 構造とオブジェクト識別子）	https://www.moj.go.jp/content/001216068.pdf
12	オンライン請求ネットワーク関連システム 共通認証局運用規程 [令和 2 年 9 月]	https://www.ssk.or.jp/seikyushiharai/online/index.files/claimsys21_2.pdf
13	総務省告示第七百六号 電子署名に係る地方公共団体の認証業務 [平成十五年十二月三日]	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/d12bde7e-a950-493b-987c-0f8d4bbd1b6b/20211228_notice_article_10.pdf
14	医療情報システムの安全管理に関するガイドライン 第 5.2 版（令和 4 年 3 月）	https://www.mhlw.go.jp/stf/shingi/0000516275_00002.html (2022 年 10 月 4 日）
15	クレジットカード・セキュリティガイドライン 3.0 版 (2022 年 3 月)	https://www.meti.go.jp/press/2021/03/20220309003/20220309003.html (2022 年 10 月 20 日）
16	【鉄道事業者用】情報セキュリティ対策チェックリスト（令和３年４月 第２版）	https://www.mlit.go.jp/common/001401615.pdf (2022 年 10 月 20 日）
17	【空港・空港ビル事業者用】情報セキュリティ対策チェックリスト（令和３年４月）	https://www.mlit.go.jp/common/001401613.pdf (2022 年 10 月 20 日）

重要インフラ規格については、金融、電力等、業種ごとにセキュリティガイドラインが作成されているものの、どのような暗号アルゴリズムを使用するかについて記載しているガイドラインは少なく、今回調査した中で、使用する暗号アルゴリズムについて記載しているガイドラインは、表 2.16 に記載したガイドライン(チェックリスト)に留まる。今回調査した重要インフラ規格の中で、使用する暗号アルゴリズムについての記載がないガイドラインを以下に示す。

- ✓ 金融分野におけるサイバーセキュリティ強化に向けた取組方針（2022）
- ✓ 医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン（2020）
- ✓ クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン第１版
- ✓ 医療情報を受託管理する情報処理事業者向けガイドライン
- ✓ 鉄道分野における情報セキュリティ確保に係る安全ガイドライン 第４版（平成 31 年 3 月 29 日改訂）
- ✓ 物流分野における情報セキュリティ確保に係る安全ガイドライン 第４版（平成 31 年 3 月 29 日改訂）
- ✓ 航空分野における情報セキュリティ確保に係る安全ガイドライン 第５版（平成 31 年 3 月 29 日改訂）
- ✓ 空港分野における情報セキュリティ確保に係る安全ガイドライン 第２版（平成 31 年 3 月 29 日制定）
- ✓ 水道分野における情報セキュリティガイドライン（第 4 版）（平成 31 年 3 月）
- ✓ 電気通信分野における情報セキュリティ確保に係る安全基準（第 4 2 版）[令和 3 年 12 月 10 日]
- ✓ 電力制御システムセキュリティガイドライン（2016）
- ✓ スマートメーターシステムセキュリティガイドライン（2016）
- ✓ スマートシティセキュリティガイドライン(第 2.0 版)（2021 年 6 月）

2.4. 標準規格・民間規格・特定団体規格調査（調査D）

標準規格・民間規格・特定団体規格の調査では、国際的な標準規格団体である IETF が策定する RFC および、米国の民間規格団体である IEEE が策定する標準規格において採用されている暗号アルゴリズムの調査を実施した。調査概要を表 2.17 に示す。

表 2.17 調査D概要

No	項目	内容
1	調査期間	2022 年 9 月～10 月
2	調査区分	公開情報調査
3	調査対象	IPA が指定した国際的な民間規格（IETF が策定する RFC および IEEE が策定する規格（詳細参照：表 2.18））
4	調査方法	IPA と合意した国際的な民間規格において調査対象暗号アルゴリズムを調査
5	集計方法	・IPA と合意した国際的な民間規格において、調査対象暗号アルゴリズムを検索 ・検索結果について、内容を確認した上で、暗号アルゴリズムの記載が参考情報扱いでないものについて暗号アルゴリズムを実装されていると見なす ・検索結果について、内容を確認した上で、暗号アルゴリズムの記載が参考情報扱いであるものについて暗号アルゴリズムを実装されていないと見なす

2.4.1. 公開情報調査

表 2.18 に、調査対象とした国際的な民間規格の名称と文書入手先 URL を示す。

表 2.18 公開情報調査対象詳細（調査D：国際的な民間規格）

No	国際的な民間規格名	文書入手先 URL
1	RFC 6043 MIKEY-TICKET Ticket-Based Modes of Key Distribution in Multimedia Internet KEYing (MIKEY) [March 2011]	https://datatracker.ietf.org/doc/html/rfc6043
2	RFC 6476 Using Message Authentication Code (MAC) Encryption in the Cryptographic Message Syntax (CMS) [January 2012]	https://datatracker.ietf.org/doc/html/rfc6476
3	RFC 6637 Elliptic Curve Cryptography (ECC) in OpenPGP [June 2012]	https://datatracker.ietf.org/doc/rfc6637/
4	RFC 6781 DNSSEC Operational Practices, Version 2 [June 2012]	https://datatracker.ietf.org/doc/rfc6781/
5	RFC 8645 Re-keying Mechanisms for Symmetric Keys	https://datatracker.ietf.org/doc/rfc8645/
6	RFC 8702 Use of the SHAKE One-Way	https://datatracker.ietf.org/doc/html/rfc8702

	Hash Functions in the Cryptographic Message Syntax (CMS)	
7	RFC 8708 Use of the HSS/LMS Hash-Based Signature Algorithm in the Cryptographic Message Syntax (CMS)	https://datatracker.ietf.org/doc/html/rfc8708
8	RFC 8723 Double Encryption Procedures for the Secure Real-Time Transport Protocol (SRTP)	https://datatracker.ietf.org/doc/rfc8723/
9	RFC 8725 JSON Web Token Best Current Practices	https://datatracker.ietf.org/doc/html/rfc8725
10	RFC 8732 Generic Security Service Application Program Interface (GSS-API) Key Exchange with SHA-2	https://datatracker.ietf.org/doc/html/rfc8732
11	RFC 8778 Use of the HSS/LMS Hash-Based Signature Algorithm with CBOR Object Signing and Encryption (COSE)	https://datatracker.ietf.org/doc/html/rfc8778
12	RFC 8812 CBOR Object Signing and Encryption (COSE) and JSON Object Signing and Encryption (JOSE) Registrations for Web Authentication (WebAuthn) Algorithms	https://datatracker.ietf.org/doc/html/rfc8812
13	RFC 8871 A Solution Framework for Private Media in Privacy-Enhanced RTP Conferencing (PERC)	https://datatracker.ietf.org/doc/html/rfc8871
14	RFC 8915 Network Time Security for the Network Time Protocol	https://datatracker.ietf.org/doc/html/rfc8915
15	RFC 9021 Use of the Walnut Digital Signature Algorithm with CBOR Object Signing and Encryption (COSE)	https://datatracker.ietf.org/doc/html/rfc9021
16	RFC 9048 Improved Extensible Authentication Protocol Method for 3GPP Mobile Network Authentication and Key Agreement (EAP-AKA')	https://datatracker.ietf.org/doc/rfc9048/
17	RFC 9115 An Automatic Certificate Management Environment (ACME) Profile for Generating Delegated Certificates	https://datatracker.ietf.org/doc/rfc9115/
18	RFC 9132 istributed Denial-of-Service	https://datatracker.ietf.org/doc/rfc9132/

	Open Threat Signaling (DOTS) Signal Channel Specification	
19	RFC 9140 Nimble Out-of-Band Authentication for EAP (EAP-NOOB)	https://datatracker.ietf.org/doc/html/rfc9140
20	RFC 9145 Integrity Protection for the Network Service Header (NSH) and Encryption of Sensitive Context Headers	https://datatracker.ietf.org/doc/rfc9145/
21	IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices	IEEE より購入
22	IEEE Standard for Ethernet	IEEE より購入
23	IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages	IEEE より購入
24	IEEE Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications	IEEE より購入
25	IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks	IEEE より購入

2.5. オープンソースソフトウェア調査（調査E）

オープンソースプロジェクトの調査では、オープンソースプロジェクト（例：OpenSSL、Linux、Android、Chrome）が提供するオープンソースソフトウェアにおいて採用されている暗号アルゴリズムの調査を実施した。調査概要を表 2.19 に示す。

表 2.19 調査E概要

No,	項目	内容
1	調査期間	2022 年 7 月～10 月
2	調査区分	公開情報調査
3	調査対象	IPA が指定したオープンソースプロジェクト（詳細参照：表 2.20）
4	調査方法	・ IPA と合意したソースコードにおいて調査対象暗号アルゴリズムを調査 ・ 上記調査対象暗号アルゴリズムは、表 2.8 アンケート調査項目（暗号アルゴリ

		ズム）に 64 ビットブロック暗号の DES、Blowfish、GOST 28147、IDEA、128 ビットブロック暗号の Twofish、Serpent、守秘・鍵交換の RSA-KEM、EC-MQV、ハッシュ関数の Tiger、HAS-160、MD5 を追加したもの ・ 標準的なパッケージに含まれない追加モジュールは除外
5	集計方法	・ IPA と合意したソースコードにおいて、調査対象暗号アルゴリズムを検索 ・ 検索結果に表示される暗号アルゴリズムを実装されていると見なす ・ 検索結果に表示されない暗号アルゴリズムを実装されていないと見なす

2.5.1. 公開情報調査

オープンソースプロジェクトの調査対象は、IPA に指定されたオープンソースプロジェクトとし、IPA と合意したソースコードを検索することで調査を実施した。表 2.20 に調査対象のオープンソースプロジェクト及びソースコードの URL を示す。

表 2.20 公開情報調査対象詳細（調査Ｅ：オープンソースソフトウェア）

No,	オープンソースプロジェクト名	ソースコード URL（最終調査日）
1	Java	https://github.com/openjdk/（2022 年 9 月 27 日）
2	PHP	https://github.com/php/php-src（2022 年 9 月 27 日）
3	Python	https://github.com/python/cpython（2022 年 10 月 13 日）
4	Gitlab	https://gitlab.com/gitlab-org/gitlab（2022 年 9 月 27 日）
5	Redmine	https://github.com/redmine/redmine（2022 年 9 月 27 日） http://svn.redmine.org/redmine/（2022 年 9 月 27 日）
6	Eclipse	https://github.com/eclipse（2022 年 9 月 27 日）
7	Apache	https://github.com/apache/httpd（2022 年 9 月 27 日） https://dlcdn.apache.org/httpd/（2022 年 9 月 27 日）
8	Nginx	https://github.com/nginx/nginx（2022 年 9 月 27 日） http://hg.nginx.org/nginx/（2022 年 9 月 27 日）
9	Samba	https://github.com/samba-team/samba（2022 年 9 月 27 日） https://git.samba.org/samba.git/（2022 年 9 月 27 日）
10	MySQL	https://github.com/mysql/mysql-server（2022 年 9 月 27 日） https://dev.mysql.com/downloads/mysql/（2022 年 9 月 27 日）
11	PostgreSQL	https://github.com/postgres/postgres（2022 年 9 月 27 日） https://www.postgresql.org/ftp/source/（2022 年 9 月 27 日）
12	Redis	https://github.com/redis/redis（2022 年 9 月 27 日） https://redis.io/download/#redis-downloads（2022 年 9 月 27 日）
13	Linux	https://github.com/torvalds/linux（2022 年 9 月 27 日） https://www.kernel.org/（2022 年 9 月 27 日）

14	FreeBSD	https://github.com/freebsd/freebsd-src（2022 年 9 月 27 日） https://cgit.freebsd.org/src/（2022 年 9 月 27 日）
15	Debian	https://github.com/Debian（2022 年 10 月 13 日） https://sources.debian.org/（2022 年 10 月 13 日）
16	Android	https://github.com/aosp-mirror（2022 年 9 月 27 日） https://android.googlesource.com/（2022 年 9 月 27 日）
17	mbedOS	https://github.com/ARMmbed/mbed-os（2022 年 9 月 27 日）
18	Ubuntu	https://github.com/ubuntu（2022 年 9 月 27 日） https://kernel.ubuntu.com/git/（2022 年 9 月 27 日）
19	Docker	https://github.com/docker（2022 年 9 月 27 日）
20	Webkit	https://github.com/WebKit/WebKit（2022 年 9 月 27 日）
21	Chrome	https://github.com/chromium/chromium（2022 年 10 月 13 日） https://source.chromium.org/chromium（2022 年 10 月 13 日）
22	OpenOffice	https://github.com/apache/openoffice（2022 年 9 月 27 日） https://gitbox.apache.org/repos/asf/openoffice.git（2022 年 9 月 27 日）
23	OpenSSL	https://github.com/openssl/openssl（2022 年 9 月 27 日） https://git.openssl.org/（2022 年 9 月 27 日）
24	Network Security Service (NSS)	https://github.com/nss-dev/nss（2022 年 9 月 27 日） https://hg.mozilla.org/projects/nspr（2022 年 9 月 27 日）
25	GnuPG	https://github.com/gpg/gnupg（2022 年 9 月 27 日） https://git.gnupg.org/cgi-bin/gitweb.cgi?p=gnupg.git（2022 年 9 月 27 日）
26	Mcrypt	http://mcrypt.cvs.sourceforge.net/（2022 年 9 月 27 日）
27	Bouncy Castle	https://github.com/bcgit（2022 年 9 月 27 日）
28	libsodium	https://github.com/jedisct1/libsodium（2022 年 9 月 27 日）
29	7-zip	https://sevenzip.osdn.jp/download.html（2022 年 9 月 27 日）
30	Keycloak	https://github.com/keycloak/keycloak（2022 年 9 月 27 日）

3. 調査結果

応募者調査結果（調査Ａ結果）を 3.1.節に、市販製品調査結果（調査Ｂ結果）を 3.2.節に、政府系情報システム・情報システム規格調査結果（調査Ｃ結果）を 3.3.節に、標準規格・民間規格・特定団体規格調査結果（調査Ｄ結果）を 3.4.節に、オープンソースソフトウェア調査結果（調査Ｅ結果）を 3.5.節にまとめる。

3.1. 応募者調査結果（調査A結果）

各対象暗号アルゴリズムが採択されている国際標準規格や、各対象暗号アルゴリズムを指定している国際的な民間規格（プロトコル規格を含む）、各対象暗号アルゴリズムを指定または推奨している政府機関が利用する法令・ガイドライン等、各対象暗号アルゴリズムを指定または推奨している業界団体規格（業界団体名）、各対象暗号アルゴリズムが実装されているオープンソースソフトウェアについて、該当数を以下に示す。

表 3.1 応募者調査結果（調査Ａ結果）概要

企業名	対象暗号アルゴリズム	対象暗号アルゴリズムの利用実績（注１）	製品情報（注２）	該当数（注３）				
				国際標準規格	国際的な民間規格（プロトコル規格を含む）	政府機関が利用する法令・ガイドライン等	業界団体規格（業界団体名）	オープンソースソフトウェア
ソニー株式会社	CLEFIA	○	○	1	1	0	0	0
株式会社日立製作所	Enocoro-128v2	○	×	1	0	0	0	0
	MUGI	○	×	1	0	0	0	0
	MULTI-S01	○	○	1	0	0	0	0
KDDI 株式会社	KCipher-2	○	○	1	1	1	0	1
日本電気株式会社	CIPHERUNICORN-E	×	×	0	0	0	0	0
	CIPHERUNICORN-A	×	×	0	0	0	0	0
	PC-MAC-AES	×	×	0	0	0	0	0
富士通株式会社	ECDSA	○	×	3	4	0	8	23
	ECDH	○	×	3	3	0	6	21
	SC2000	×	×	0	0	0	0	0
日本電信電話株式会社	PSEC-KEM	○	×	1	1	0	0	0
	Camellia	○	×	2	7	0	2	15
株式会社東芝	Hierocrypt-L1	○	○	0	0	0	0	0
	Hierocrypt-3	×	×	0	0	0	0	0
三菱電機株式会社	MISTY1	○	×	1	0	0	1	0

注１：対象暗号アルゴリズムの利用実績では、国際標準規格、国際的な民間規格（プロトコル規格を含む)、政府機関が利用する法令・ガイドライン等、業界団体規格（業界団体名)、オープンソースソフトウェア、応募者から提供された製品情報の中で、対象暗号アルゴリズムが採用されているものが１つでもあれば○とした。

注２：製品情報では、応募者調査（調査Ａ）の中で、応募者から対象暗号アルゴリズムを組込んだ製品・システムに関する情報が提供されたものを○とした。

注３：該当数とは、応募者から提供された国際標準規格、国際的な民間規格（プロトコル規格を含む)、政府機関が利用する法令・ガイドライン等、業界団体規格（業界団体名)、オープンソースソフトウェアの情報の中で、項目ごとに該当する規格、法令・ガイドライン等、ソフトウェアの合計数を示す。なお、これらの値は参考情報であり、その一部は各調査（調査Ｂ、Ｃ、Ｄ、Ｅ）にて調査対象として含める場合がある。

各対象暗号アルゴリズムにおいて該当のあった国際標準規格や国際的な民間規格（プロトコル規格を含む)、政府機関が利用する法令・ガイドライン等、業界団体規格（業界団体名)、オープンソースソフトウェアの名称について、以下に示す。

表 3.2 応募者調査結果（調査Ａ結果）概要

対象暗号アルゴリズム	規格・法令・ガイドライン・オープンソースソフトウェアの名称
CLEFIA	【国際標準規格】 ISO/IEC 29192 (Lightweight cryptography) 【国際的な民間規格（プロトコル規格を含む）】 IETF RFC 6114
Enocoro-128v2	【国際標準規格】 ISO/IEC 29192 (Lightweight cryptography)
MUGI	【国際標準規格】 ISO/IEC 18033 (Encryption algorithms)
MULTI-S01	【国際標準規格】 ISO/IEC 18033 (Encryption algorithms)
KCipher-2	【国際標準規格】 ISO/IEC 18033 (Encryption algorithms) 【国際的な民間規格（プロトコル規格を含む）】 IETF RFC 7008 【政府機関が利用する法令・ガイドライン等】 標準テレビジョン放送等のうちデジタル放送に関する送信の標準方式第八条第一号及び第二号の規定に基づくスクランブルの方式 平成 23 年 06 月 29 日総務省告示第 302 号 【オープンソースソフトウェア】 Go implementation of KCipher-2 stream cipher

ECDSA	【国際標準規格】 ISO/IEC 14888 (Digital signatures with appendix) ICAO Doc 9303 (Machine readable travel documents) ISO/IEC 29167、ISO/IEC 19823、ISO/IEC/IEEE 8802-1AR:2020、ISO/IEC 15946　等 【国際的な民間規格（プロトコル規格を含む）】 IETF TLS、IETF IPsec、IETF S/MIME、IETF PGP 【業界団体規格（業界団体名）】 Wi-Fi Alliance、Association of Radio Industries and Broadcast （ARIB）、Advanced Access Content System（AACS）、一般財団法人日本データ通信協会タイムビジネス認定センター、Europay 、MasterCard、Visa （EMV）、3rd Generation Partnership Project （3GPP）、Trusted Computing Group（TCG）、FIDO Alliance 【オープンソースソフトウェア】 Java、PHP、python、Gitlab、Redmine、Webkit、Chrome、Apache、Nginx、PostgreSQL、OpenSSL、Network Security Service（NSS)、GnuPG、Mcrypt、BouncyCastle、libsodium、Linux、FreeBSD、Debian、Android、mbedOS、Ubuntu、Keycloak
ECDH	【国際標準規格】 ITU-T Y.SecMechanisms（NGN Security Mechanisms） ICAO Doc 9303 (Machine readable travel documents) ISO/IEC 29167、ISO/IEC 19823、ISO/IEC 13157、ISO/IEC 18013、ISO 22510:2019、ISO/IEC 15946　等 【国際的な民間規格（プロトコル規格を含む）】 IETF TLS、IETF IPsec、IETF S/MIME 【業界団体規格（業界団体名）】 Bluetooth SIG, Inc 、Wi-Fi Alliance、一般財団法人日本データ通信協会タイムビジネス認定センター、Europay 、MasterCard、Visa （EMV）、Trusted Computing Group（TCG）、FIDO Alliance 【オープンソースソフトウェア】 Java、PHP、python、Webkit、Chrome、Apache、Nginx、PostgreSQL、OpenSSL、Network Security Service（NSS)、GnuPG、Mcrypt、BouncyCastle、libsodium、Linux、FreeBSD、Debian、Android、mbedOS、Ubuntu、Keycloak
PSEC-KEM	【国際標準規格】 ISO/IEC 18033 (Encryption algorithms) 【国際的な民間規格（プロトコル規格を含む）】 IETF RFC 6931

Camellia	【国際標準規格】 ISO/IEC 18033 (Encryption algorithms) ITU-T Y.SecMechanisms (NGN Security Mechanisms) 【国際的な民間規格（プロトコル規格を含む）】 IETF TLS、IETF IPsec、IETF S/MIME、IETF PGP、IETF Kerberos、IEEE802.15、IETF RFC 3713、IETF RFC 5528、IETF RFC 6931 、IETF RFC 6030、IETF RFC 5990 【業界団体規格（業界団体名）】 Association of Radio Industries and Broadcast (ARIB) 、Trusted Computing Group (TCG) 【オープンソースソフトウェア】 Java、PHP、python、Apache、Nginx、OpenSSL、Network Security Service (NSS)、GnuPG、BouncyCastle、Linux、FreeBSD、Debian、mbedOS、Ubuntu、WolfSSL、WolfSSH、WolfCrypt、CycloneSSH Embedded SSH SFTP SCP Library for STM32、Veracrypt、pyca/cryptography (Python)
MISTY1	【国際標準規格】 ISO/IEC 18033 (Encryption algorithms) 【業界団体規格（業界団体名）】 3rd Generation Partnership Project (3GPP)

対象暗号アルゴリズムを利用した製品・システムに関する情報については、ソニー株式会社（CLEFIA)、株式会社日立製作所（MULTI-S01)、KDDI 株式会社（KCipher-2)、株式会社東芝（Hierocrypt-L1）の４社から回答があり、市販製品調査（調査Ｂ）に含めて集計を行った。

3.2. 市販製品調査結果（調査B結果）

業界団体調査では、14 の業界団体、会員企業総数 2,535 社にアンケート回答を依頼し、65 社から 114 製品・システムの回答数を得た。また、個別企業調査では、108 社の個別企業にアンケート回答を依頼し、28 社から 37 製品・システムの回答数を得た。さらに、応募者調査では、電子政府推奨暗号アルゴリズムの応募者８社にアンケート回答を依頼し、４社から４製品・システムの回収数を得た。また、インターネットアンケート調査では、調査パネル 23,747 名にアンケート回答を依頼し、146 名（114 社）から 146 製品・システムの回答数を得た。以上より、合計 211 社、301 製品・システムに関する暗号アルゴリズムの利用状況の調査結果を確保した。

その中から以下の方法により、合計 82 社、128 製品・システムに関する暗号アルゴリズムの利用実績の有効回答数を選定した。

○１社につき、５製品・システムまでの回答を有効回答とした。１社につき、６製品以上の回答があった場合は、IPA と相談のうえ有効回答を選定した。

○個別企業調査の回答には、アンケート調査への協力を辞退する旨の回答が含まれており、それらを対象から除外した。

○応募者調査やインターネットアンケート調査の回答には、企業名や製品・システム名が不明瞭なものが多く含まれており、ウェブ調査にて特定できないものについては対象から除外した。

以下に上記の合計 82 社、128 製品・システムについて、11 種類の製品カテゴリごとの割合を示す。

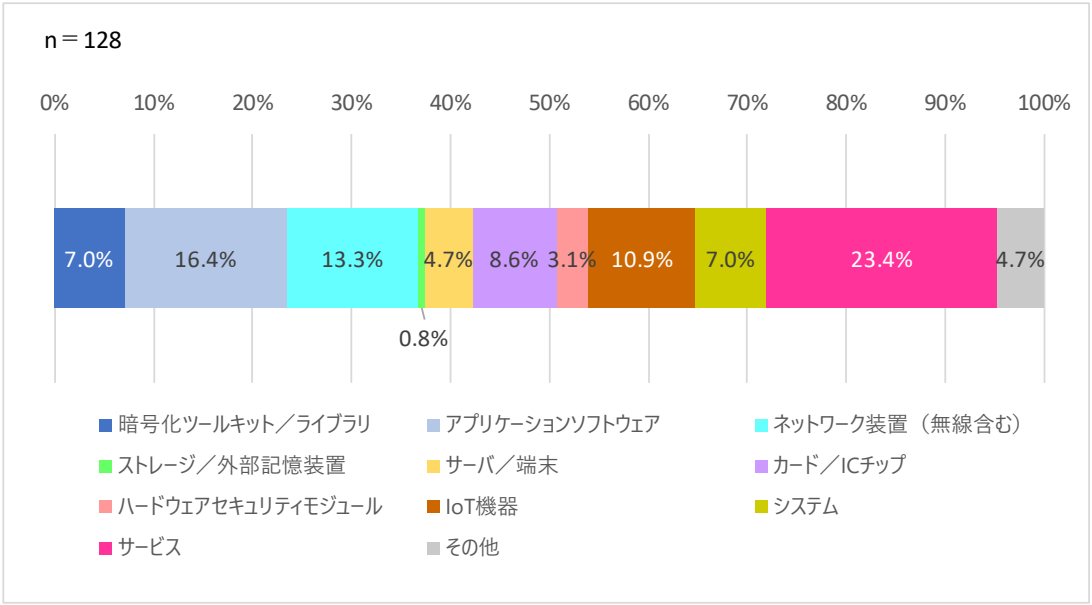

図 3.1 アンケート調査による市販製品調査結果（調査Ｂ結果）概要

製品・システムに実装されている暗号アルゴリズムの集計結果については、上記の合計 82 社、128 製品・システムに関する暗号アルゴリズムの利用状況のアンケート調査結果のうち、実装している暗号アルゴリズムが分からないと回答した調査結果を除いたものに、41 社、100 製品・システムの公開情報調査の結果を合算して、暗号アルゴリズムの記載のある 101 社、209 製品・システムを対象に市販製品の集計を行った。

以下に公開情報調査対象の 41 社、100 製品・システムについて、11 種類の製品カテゴリごとの割合を示す。

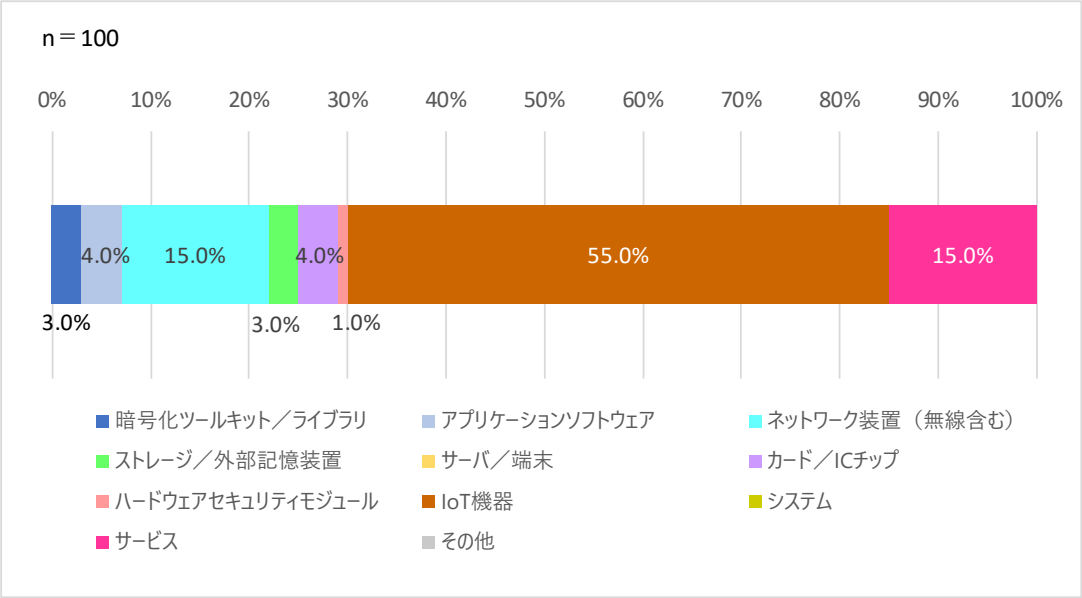

図 3.2 公開情報調査による市販製品調査結果（調査Ｂ結果）概要

3.2.1. 市販製品

市販製品の集計結果を以下に報告する。なお、グラフの記法は以下のとおりである。

以下の（１）市販製品（共通鍵暗号（64 ビットブロック暗号））から（７）市販製品（ハッシュ関数）においては、暗号アルゴリズムを次の７つに分類し、各分類の該当総数を n 値として、アンケート回答総数に n 値が占める割合を記載した。

○共通鍵暗号（64 ビットブロック暗号）
○共通鍵暗号（128 ビットブロック暗号）
○共通鍵暗号（ストリーム暗号・認証暗号）
○暗号利用モード／メッセージ認証コード
○公開鍵暗号（署名）
○公開鍵暗号（守秘・鍵共有）
○ハッシュ関数

例：アンケート回答総数 100、共通鍵暗号（64 ビットブロック暗号）のいずれかを選択した回答数（該当総数）10 の場合
（表記方法）n=10，10%

また、該当暗号アルゴリズムの回答数が該当総数に占める割合をグラフ中に記載した。

例：上記の例で共通鍵暗号（64 ビットブロック暗号）の Triple DES の回答数が 3 の場合
（表記方法）30%

また、以下の（８）市販製品（エンティティ認証）から（１３）市販製品（今後、組込みを検討及び計画している暗号アルゴリズム）においては、各調査項目で、実装・利用・準拠しているアンケート回答総数を n 値として記載した。

例：アンケート回答総数 100、エンティティ認証を実装していないと選択した回答数（該当総数）60、エンティティ認証のいずれかを選択した回答数（該当総数）40 の場合
（表記方法）n=40

（１）市販製品（共通鍵暗号（64 ビットブロック暗号）

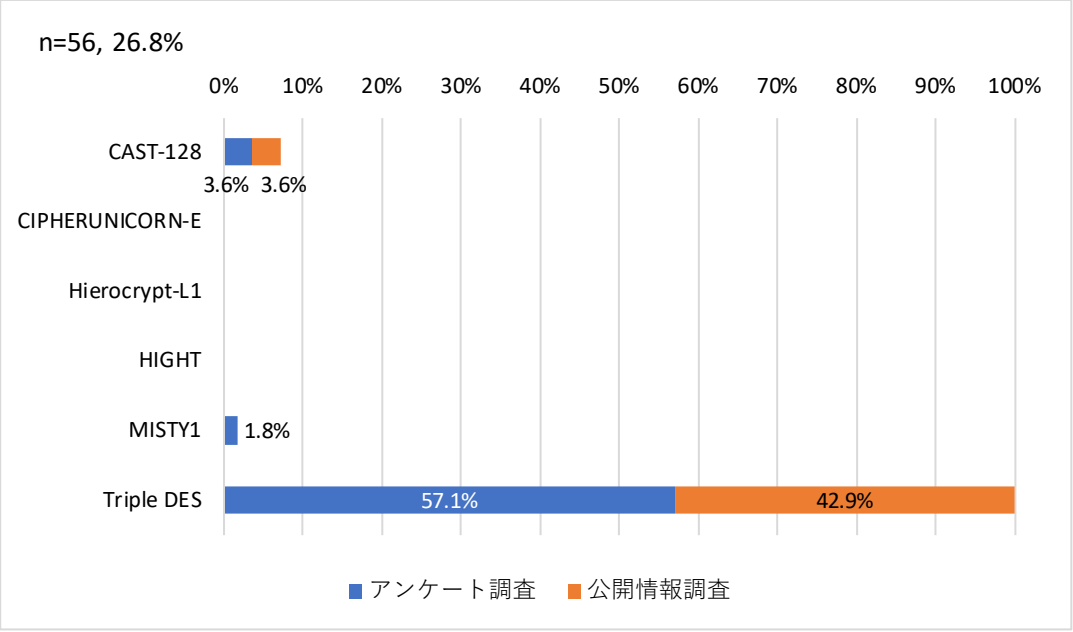

図 3.3 市販製品（共通鍵暗号（64 ビットブロック暗号））

（２）市販製品（共通鍵暗号（128 ビットブロック暗号）

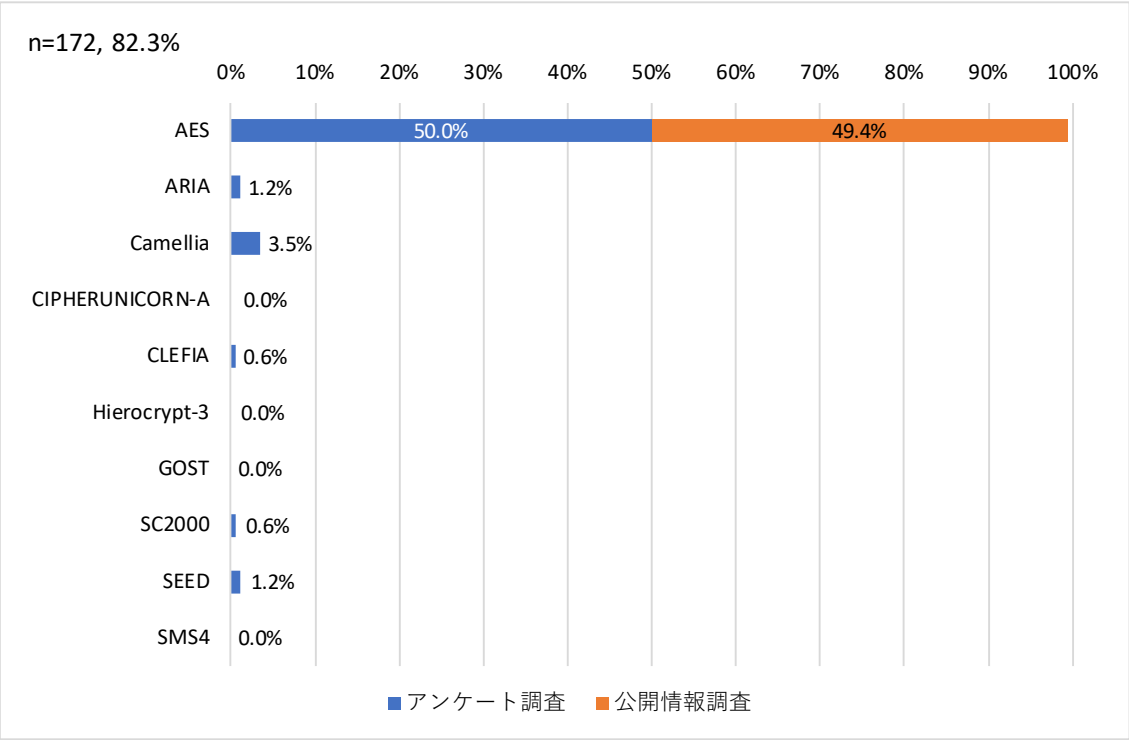

図 3.4 市販製品（共通鍵暗号（128 ビットブロック暗号））

（３）市販製品（共通鍵暗号（ストリーム暗号・認証暗号）

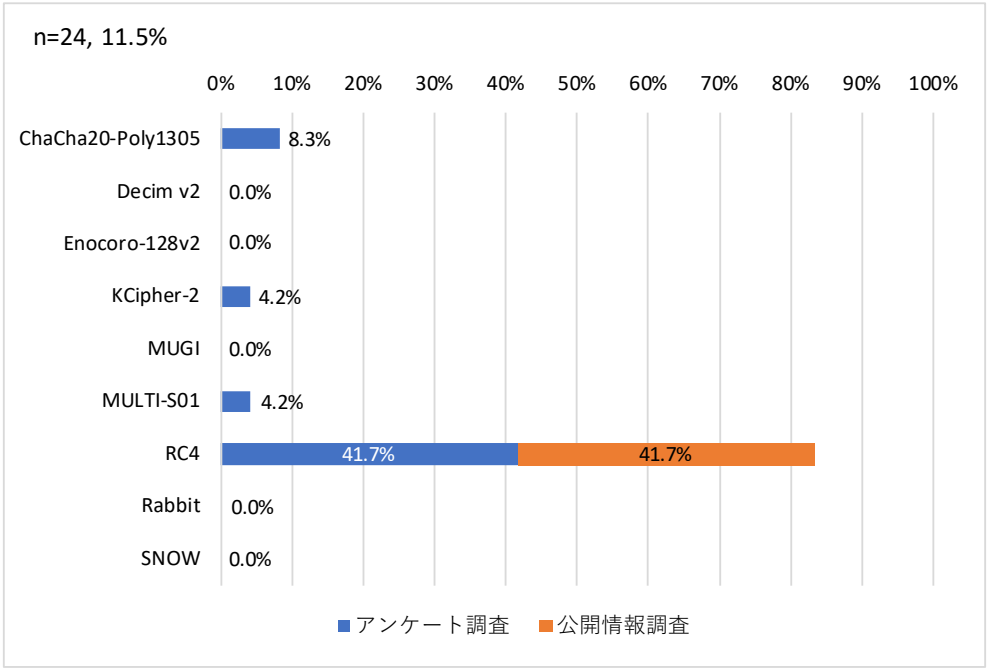

図 3.5 市販製品（共通鍵暗号（ストリーム暗号・認証暗号））

（４）市販製品（暗号利用モード／メッセージ認証コード）

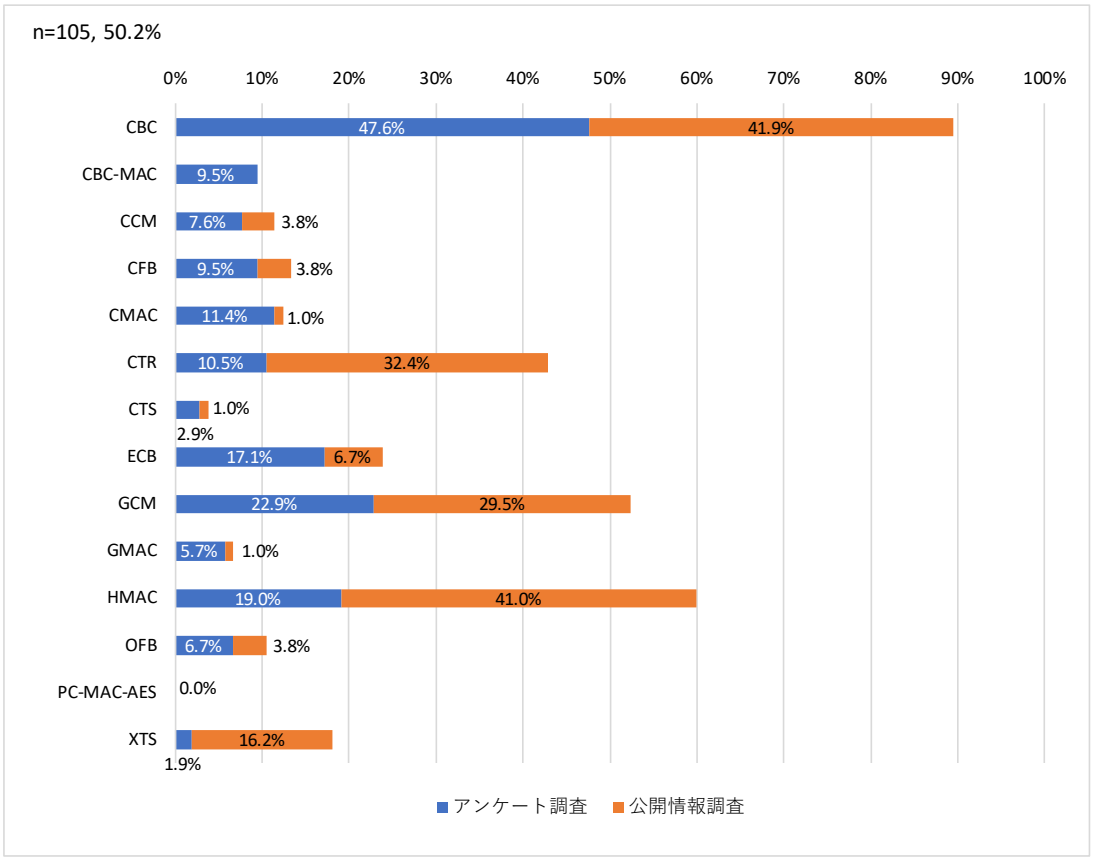

図 3.6 市販製品（暗号利用モード／メッセージ認証コード）

（５）市販製品（公開鍵暗号（署名））

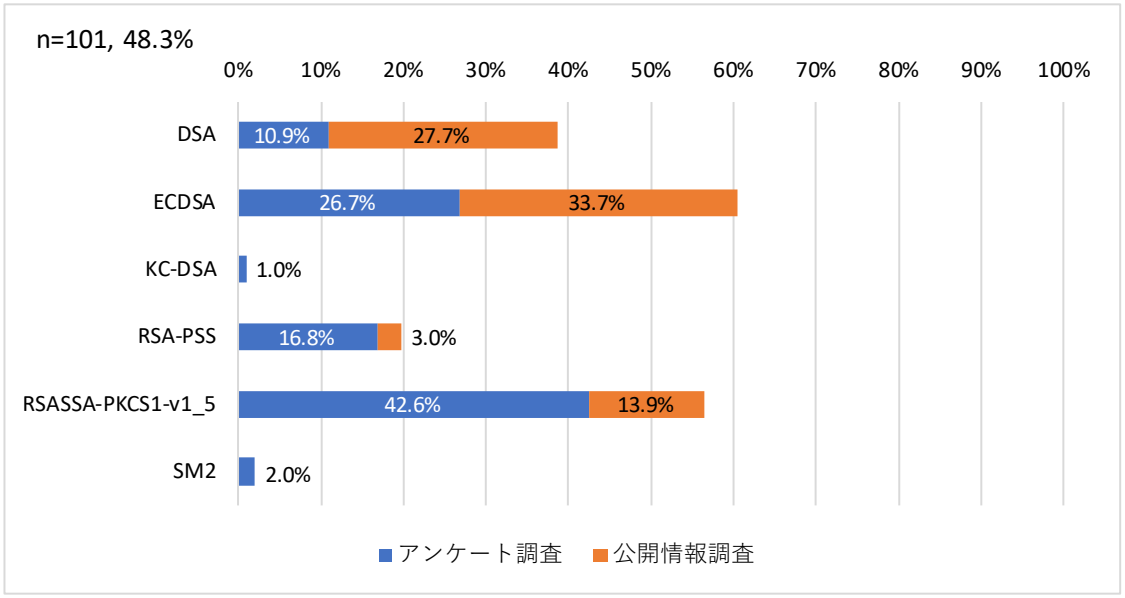

図 3.7 市販製品（公開鍵暗号（署名））

（６）市販製品（公開鍵暗号（守秘・鍵共有））

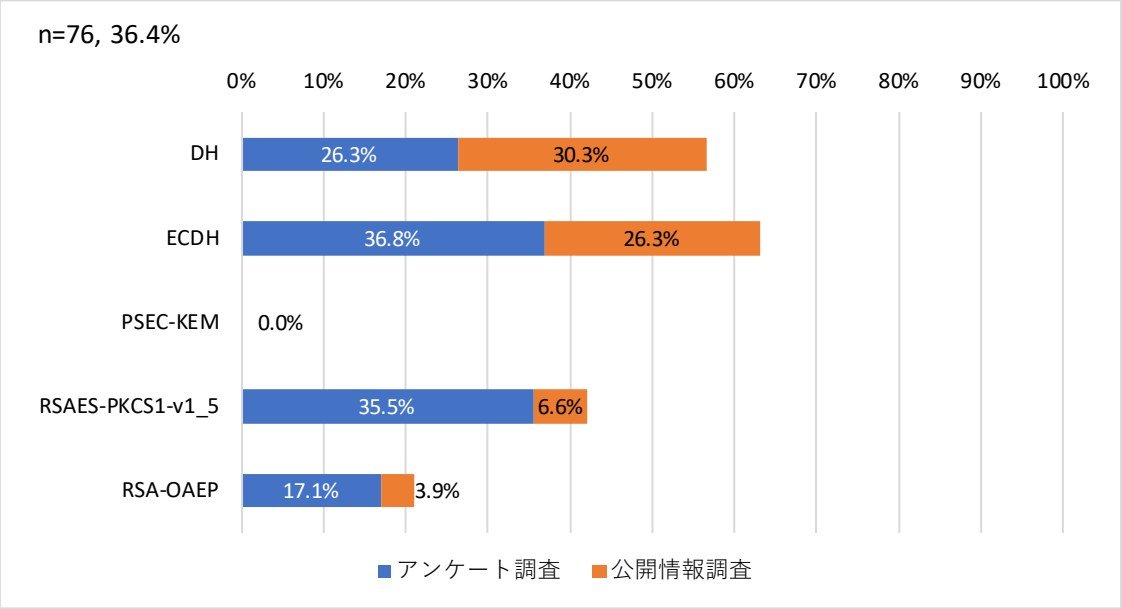

図 3.8 市販製品（公開鍵暗号（守秘・鍵共有））

（７）市販製品（ハッシュ関数）

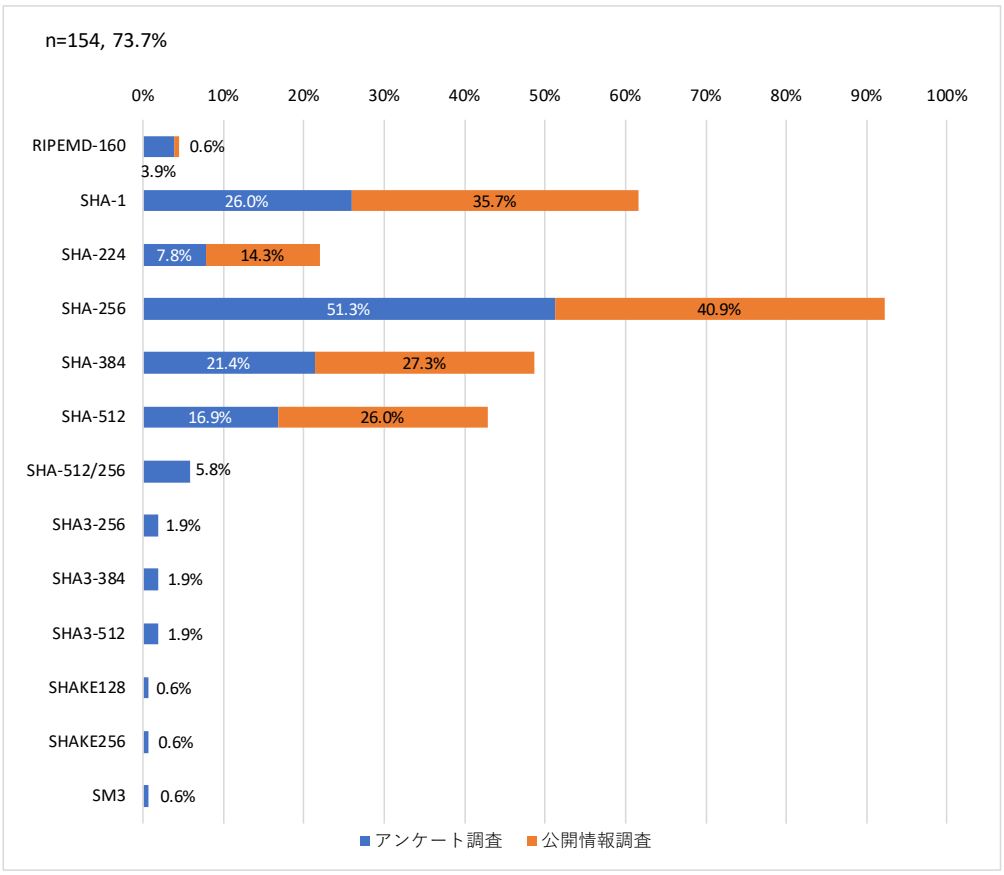

図 3.9 市販製品（ハッシュ関数）

（８）市販製品（エンティティ認証）

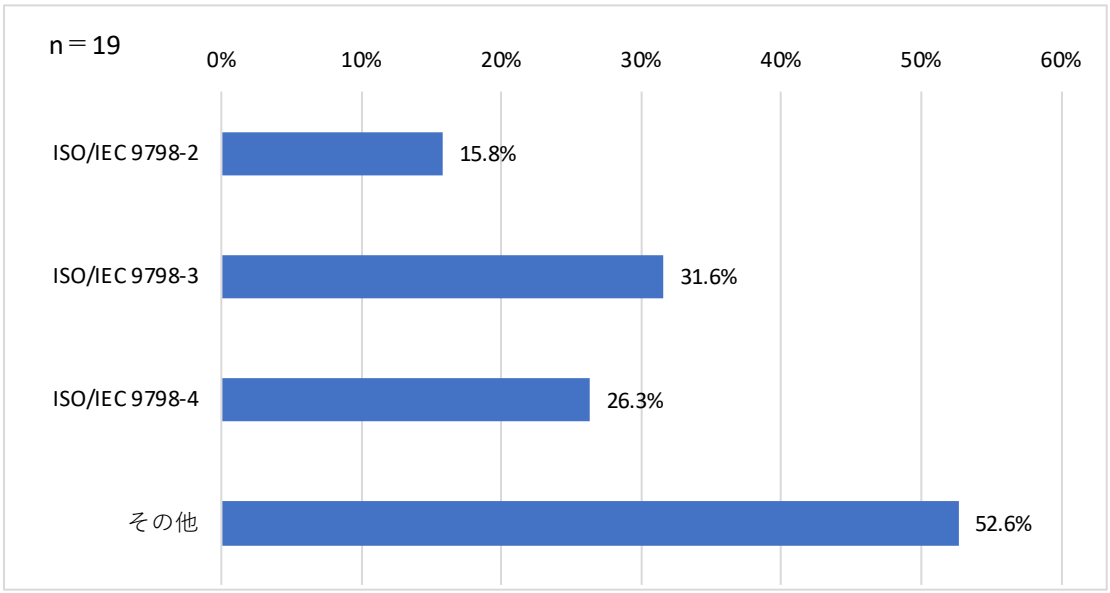

図 3.10 市販製品（エンティティ認証）

（９）市販製品（利用している国際的な民間規格（プロトコル規格を含む））

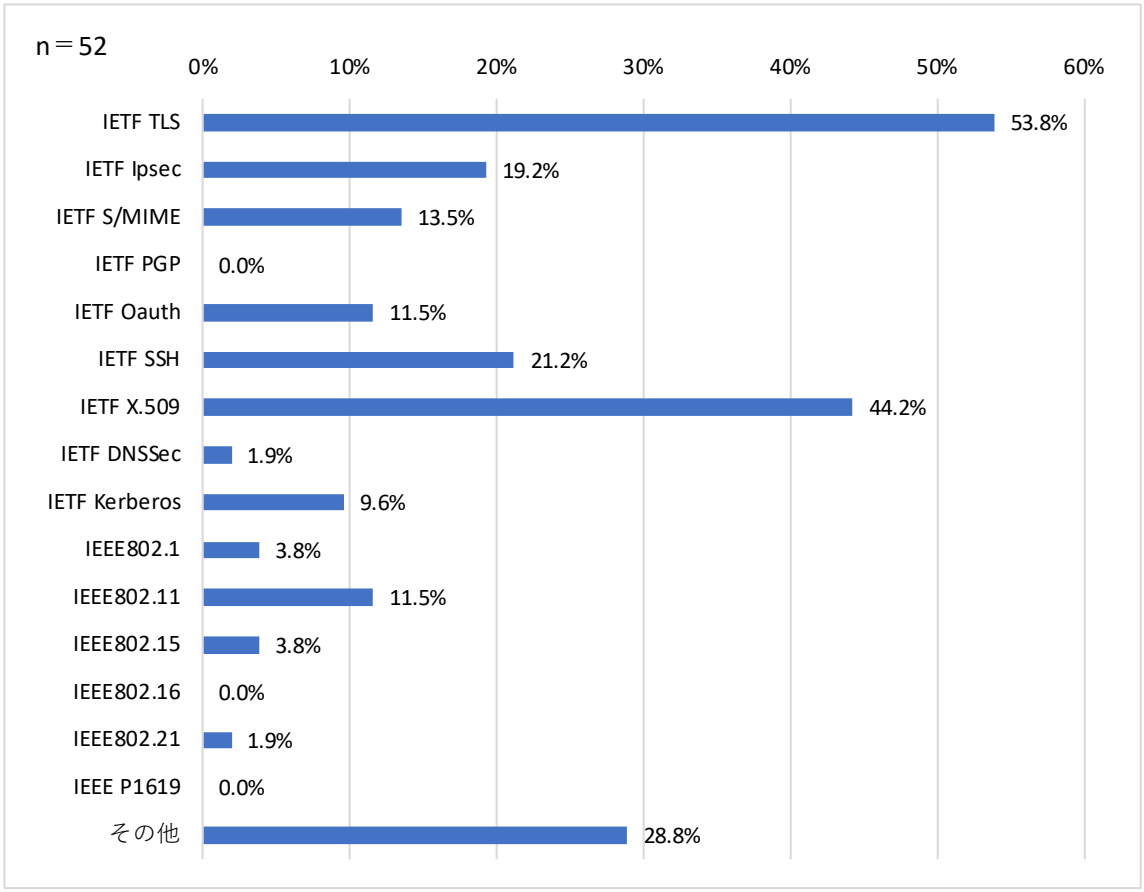

図 3.11 市販製品（利用している国際的な民間規格（プロトコル規格を含む））

（１０）市販製品（準拠している業界団体規格（業界団体名））

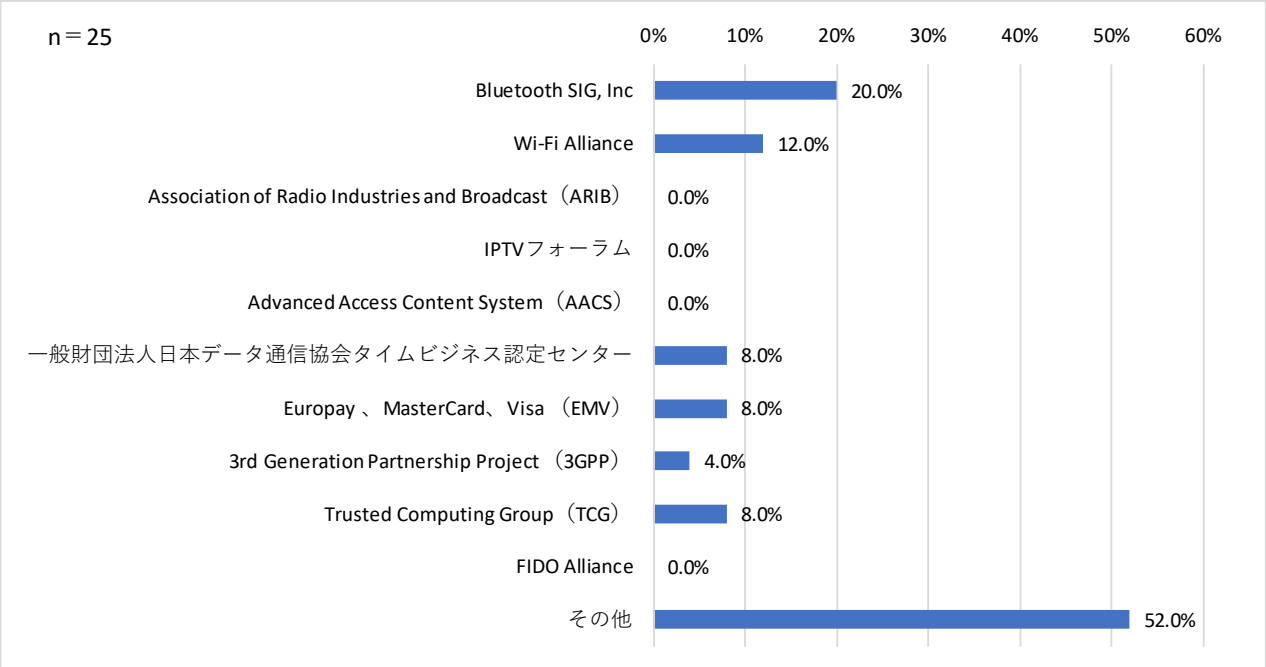

図 3.12 市販製品（準拠している業界団体規格（業界団体名））

（１１）市販製品（第三者評価・試験及び認証制度の取得状況及び検討状況）

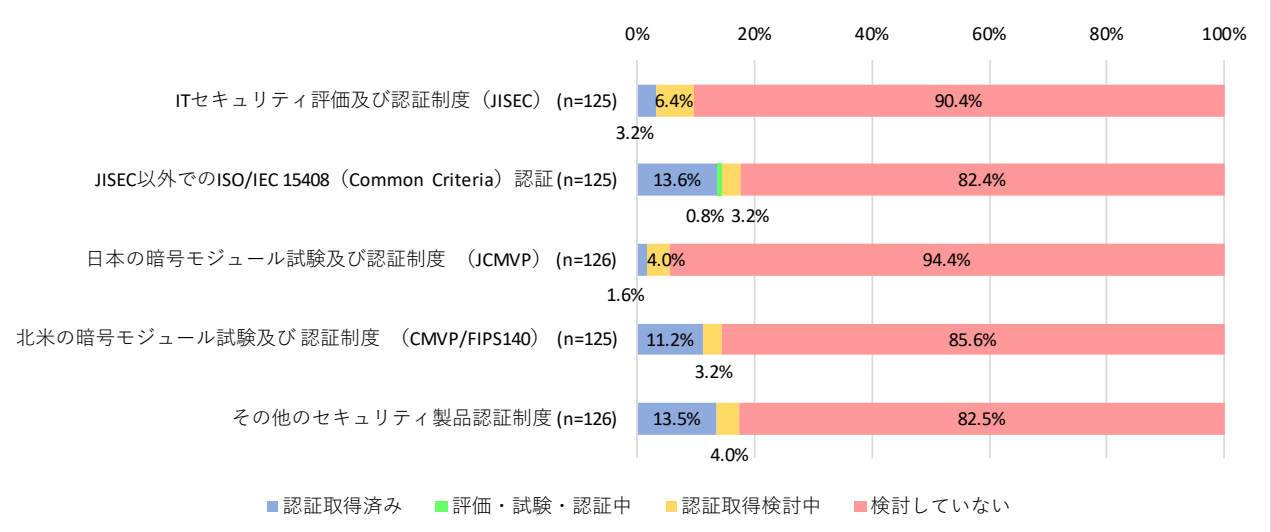

図 3.13 市販製品（第三者評価・試験及び認証制度の取得状況及び検討状況）

（１２）市販製品（利用しているオープンソースソフトウェア）

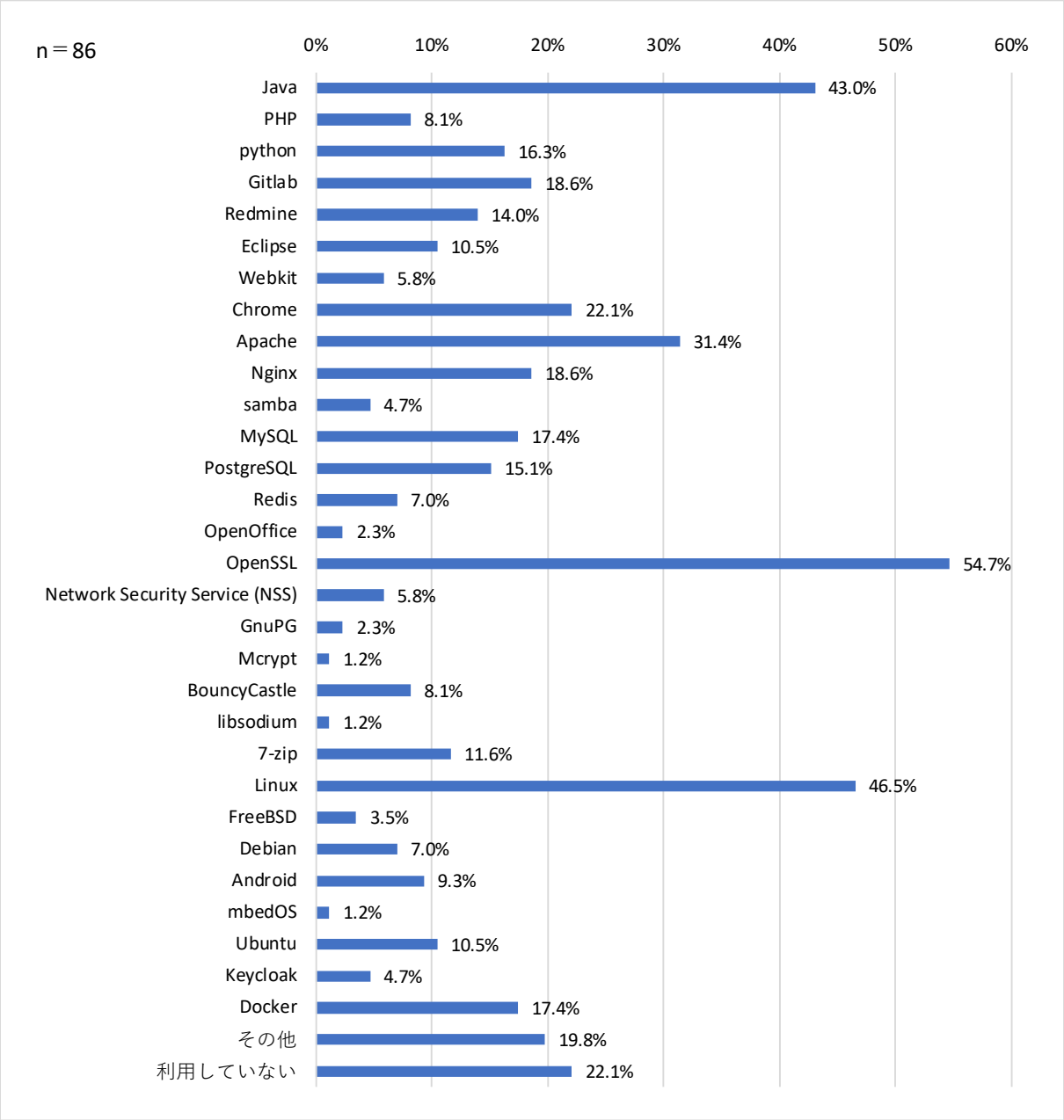

図 3. 14 市販製品（利用しているオープンソースソフトウェア）

（１３）市販製品（今後、組込みを検討及び計画している暗号アルゴリズム）

①共通鍵暗号（64 ビットブロック暗号）

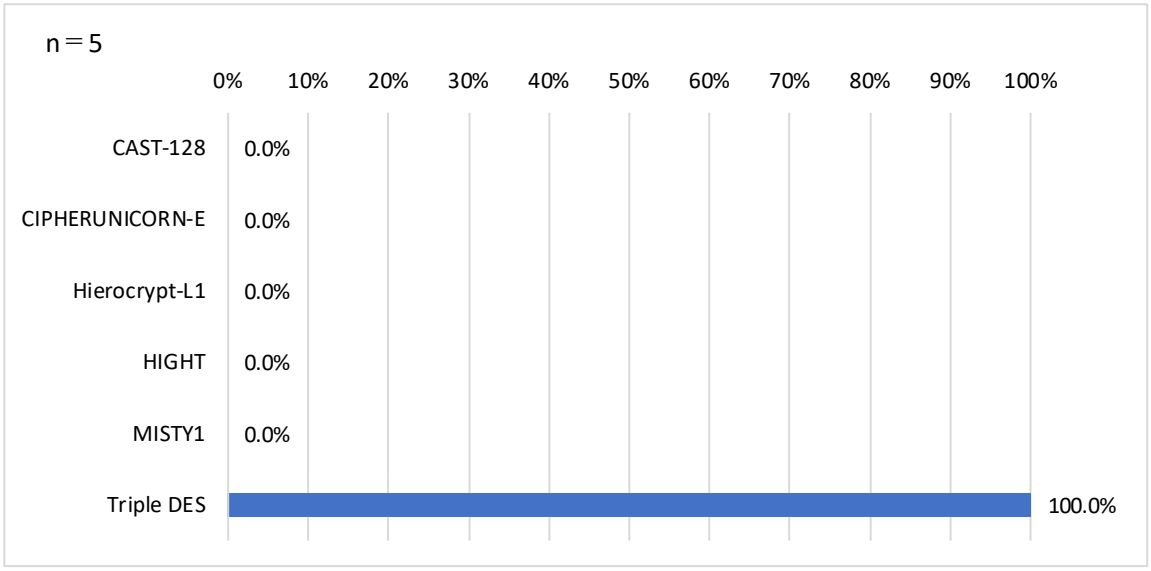

図 3.15 市販製品（今後、組込みを検討及び計画している暗号アルゴリズム（共通鍵暗号（64 ビットブロック暗号）））

②共通鍵暗号（128 ビットブロック暗号）

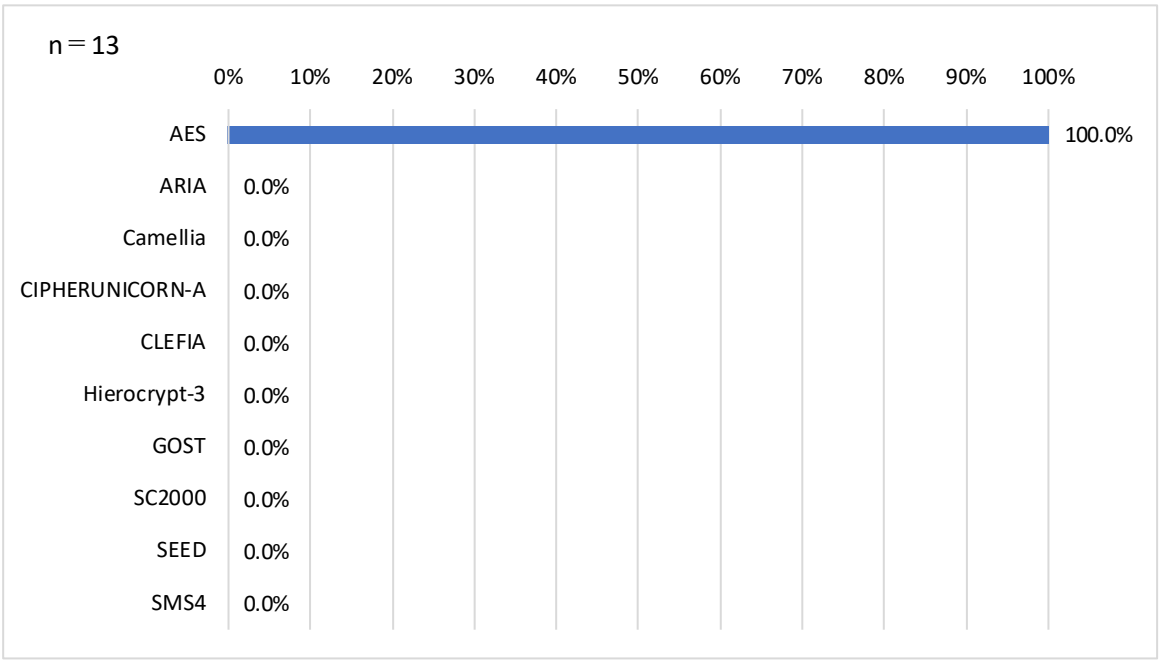

図 3.16 市販製品（今後、組込みを検討及び計画している暗号アルゴリズム（共通鍵暗号（128 ビットブロック暗号）））

③共通鍵暗号（ストリーム暗号・認証暗号）

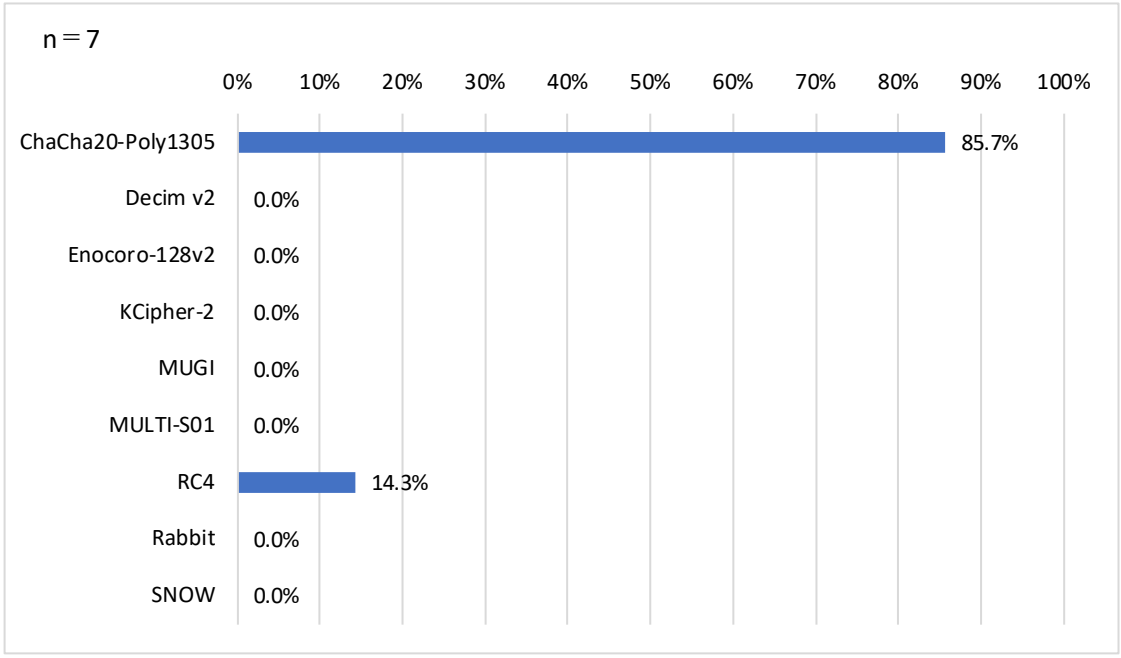

図 3.17 市販製品（今後、組込みを検討及び計画している暗号アルゴリズム（共通鍵暗号（ストリーム暗号・認証暗号）））

④暗号利用モード／メッセージ認証コード

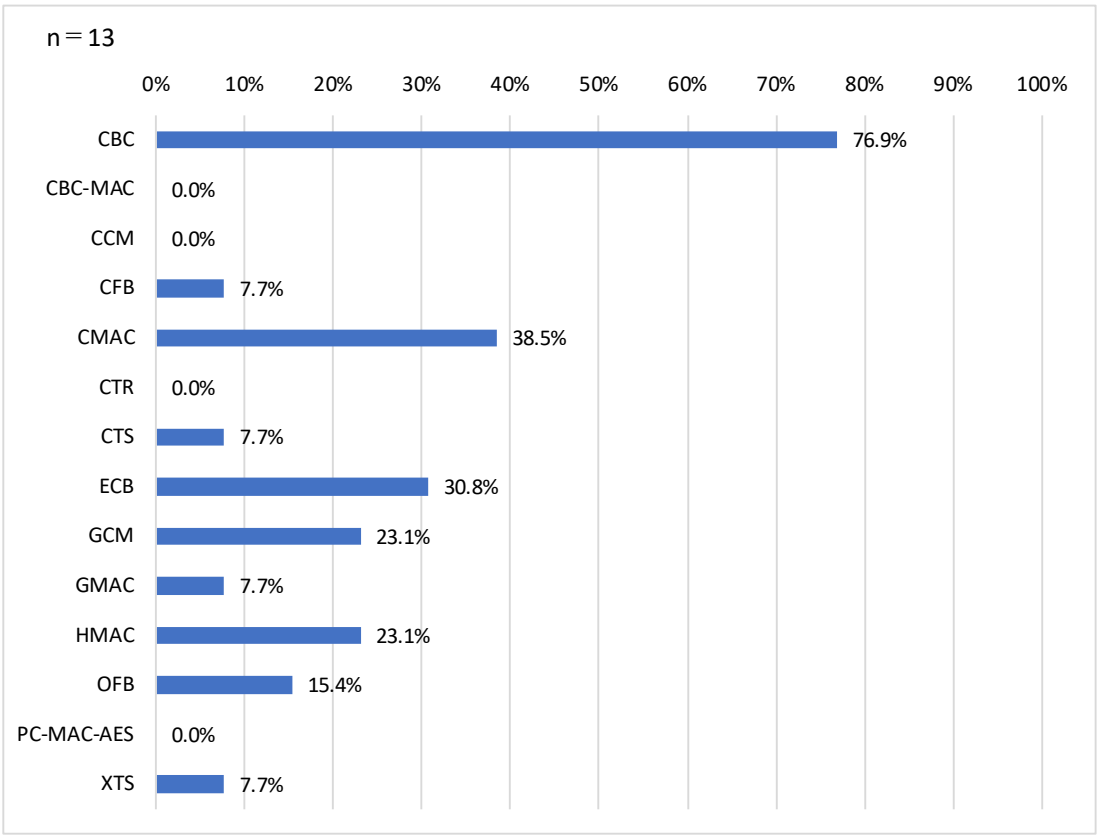

図 3. 18 市販製品（今後、組込みを検討及び計画している暗号アルゴリズム（暗号利用モード／メッセージ認証コード）

⑤公開鍵暗号（署名）

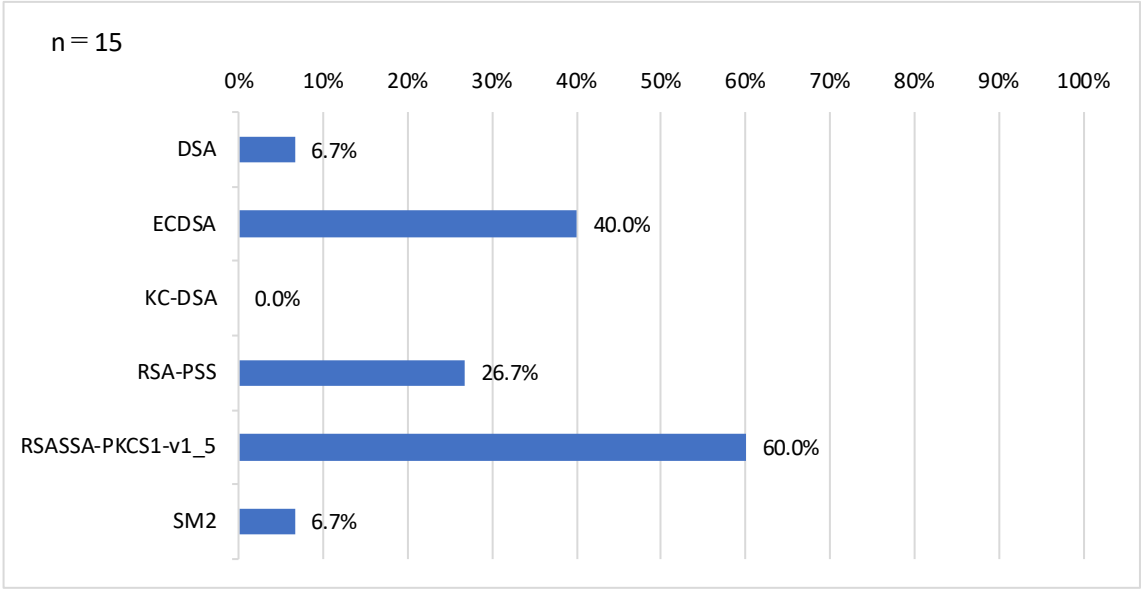

図 3. 19 市販製品（今後、組込みを検討及び計画している暗号アルゴリズム（公開鍵暗号（署名））

⑥公開鍵暗号（守秘・鍵共有）

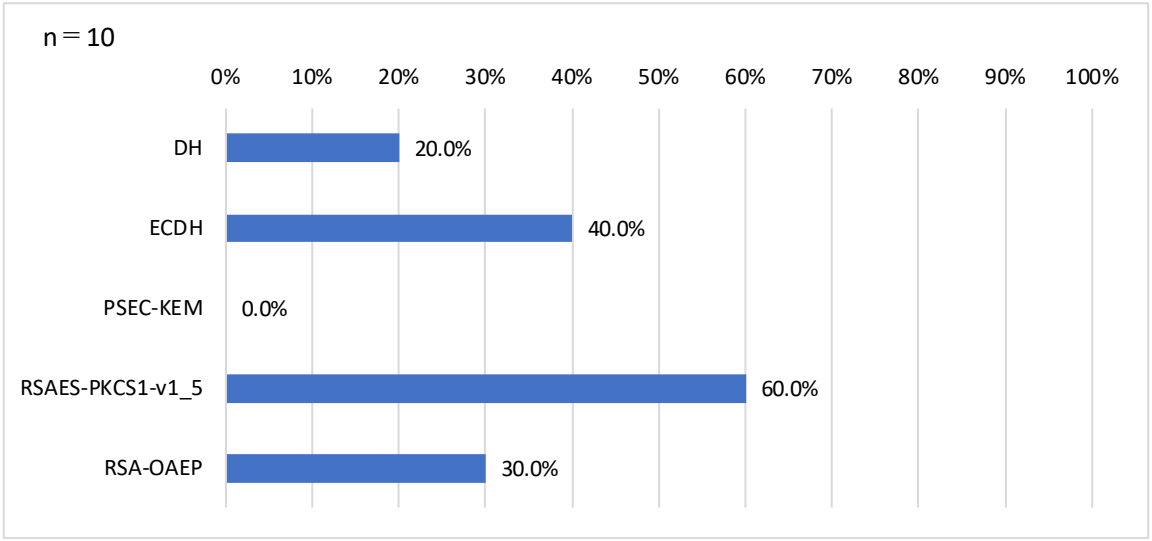

図 3.20 市販製品（今後、組込みを検討及び計画している暗号アルゴリズム（公開鍵暗号（守秘・鍵共有））

⑦公開鍵暗号（守秘・鍵共有）

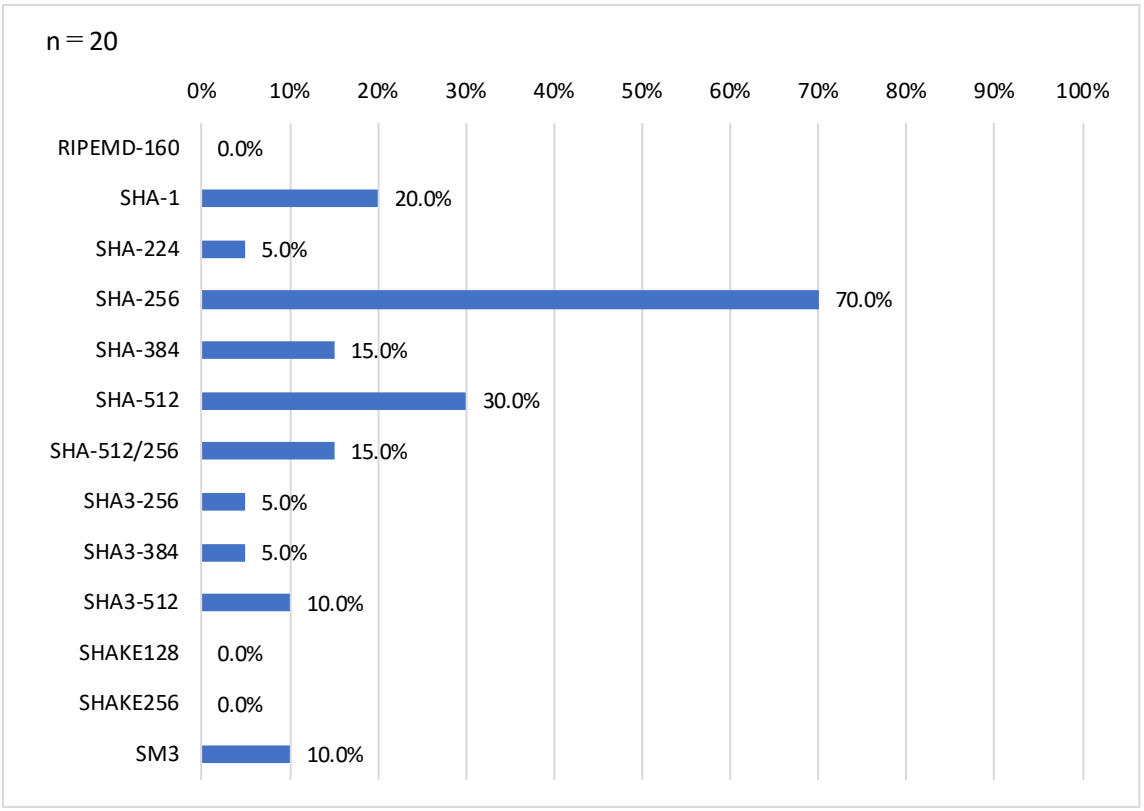

図 3.21 市販製品（今後、組込みを検討及び計画している暗号アルゴリズム（ハッシュ関数）

3.2.2. 個別企業調査結果

個別企業調査では、108 社にアンケート調査への協力を依頼した。その結果、10 社よりアンケート調査に協力してもよいという回答があり、19 製品・システムの回答数を得た。

アンケート調査への協力依頼に対する回答結果の内訳を図 3.22 に示す。

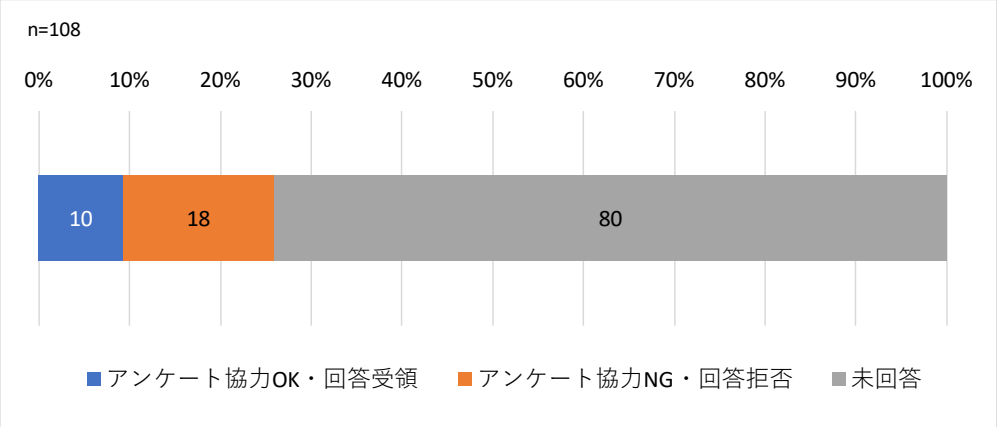

図 3.22 アンケート調査への協力依頼に対する回答結果の内訳

アンケート協力 NG・回答拒否の理由として最も多いのが、開示できない情報が含まれており、社内の法務部門の承認を得ることが難しいという回答であった。その他にも、暗号技術が最初から調達する製品に組み込まれており、かつ使いやすくなっているため、暗号技術の知識を持ち合わせている技術者が社内にほとんどおらず、回答が難しいという回答や、アンケート内容が細かすぎて、すべてに正確に回答しようとすると相当の時間と労力を要することが予想されるため協力が難しいという回答があった。アンケート協力 NG・回答拒否理由の内訳を図 3.23 に示す。

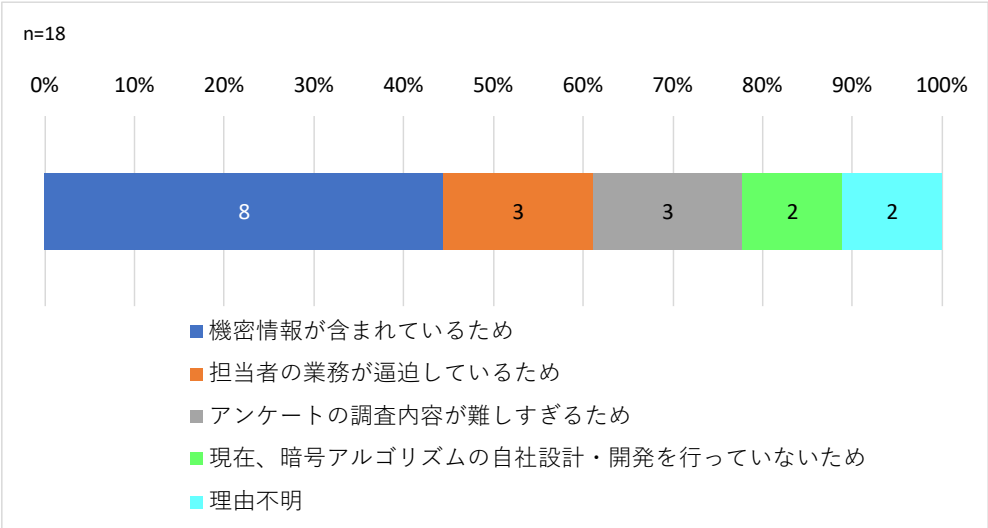

図 3.23 アンケート協力 NG・回答拒否理由の内訳

このように、個別企業調査においては、10 年前に実施した同様の調査と比べて、アンケート調査への協力が得られにくいという厳しい結果となった。その理由として、以下の２つの理由が考えられる。

（１）暗号技術に精通する技術者の減少

（２）技術情報を社外に公開する障壁の高さ

上記（１）については、調達する部品やモジュールに予め暗号技術が組み込まれており、自社側で暗号技術に関わる設計や開発を行う必要がなくなってきている結果、暗号技術に精通し、アンケート調査票に回答できる技術者が少なくなってきているという状況が見られる。

また上記（２）については、企業を取り巻く経営環境として、インシデントの発生が後を絶たない状況がある中で、企業におけるセキュリティポリシー、コンプライアンスポリシー、ビジネスポリシーの遵守に係るスタンスがより厳格な運用となっており、技術情報（暗号技術情報）の公開の足かせとなってきている状況が見られる。

今後、同様の調査を実施するにあたっては、このような状況を考慮した調査の設計が求められる。

3.2.3. インターネットアンケート調査結果

インターネットアンケート調査では、146 名（114 社）から 146 製品・システムの回答を得たが、暗号アルゴリズムの利用実態に関して信頼性の低い回答が多く含まれていたため、選択された複数の暗号アルゴリズムの組み合わせ等を考慮し、IPA と相談のうえ有効回答を選定した。

回答結果の内訳を図 3.24 に示す。

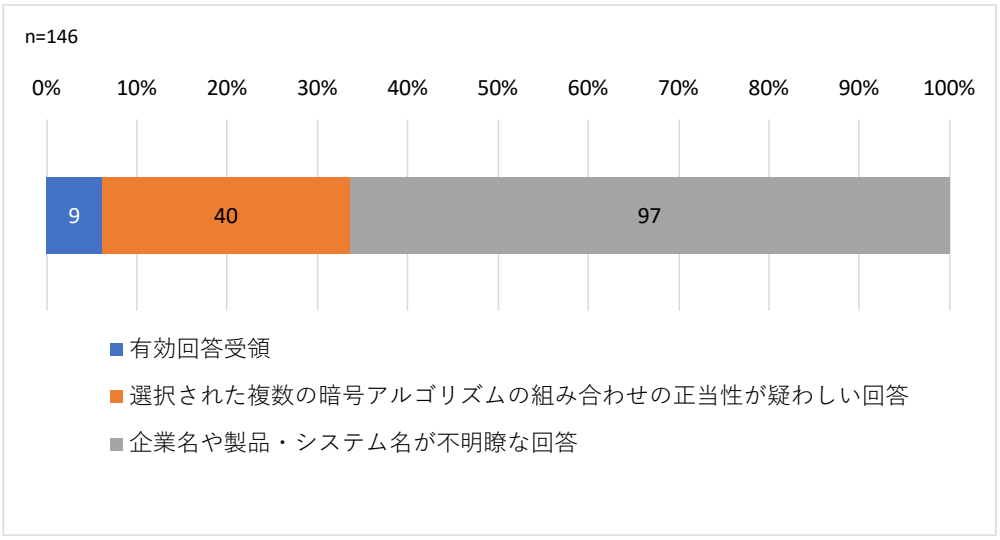

図 3.24 インターネットアンケート調査回答結果の内訳

このうち、選択された複数の暗号アルゴリズムの組み合わせの正当性が疑わしい回答には、以下のような回答が含まれる。

・企業名からみて、利用しているとは非常に想定しにくい暗号アルゴリズムが選択されている回答
・すべてのカテゴリについて、暗号強度に関わりなく、選択肢の１番目の暗号アルゴリズムだけが選択されている回答
・選択肢のほとんどの暗号アルゴリズムが選択されている回答
・多くの国産暗号アルゴリズムばかりが不自然に選択されている回答

このように、インターネットアンケート調査においては、以下のような事前調査を行い、調査対象者を絞り込んだにもかかわらず、信頼性の低い回答が多く含まれる結果となった。

【事前調査の設問項目】

問１　あなたは、現在、IT 分野の製品・サービス・システムの開発・構築に携わっていますか。
問２　あなたが開発・構築に携わっている IT 分野の製品・サービス・システムにおいては、暗号技術が使われていますか。
問３　あなたは、問２の暗号技術に関して、IT 分野の製品・サービス・システムで使用している具体的な暗号アルゴリズム名まで御存知ですか。
問４　暗号技術の利用状況の調査を実施する場合に、あなたは、所属している企業名や提供されている IT 分野の製品・サービス・システム名を明らかにしたうえで、調査に回答できますか。

その理由には、①モニターがアンケート調査に回答するとポイントがもらえる仕組みであること、②それゆえ、ポイント目当てのモニターが情報を偽って、調査対象条件に当てはまらないにもかかわらず、アンケート調査に無理に回答しようとすること、といったインターネットアンケート調査が抱える構造的な問題が大きく影響していると見られる。

また、通常のインターネットアンケート調査で扱うような調査項目とは大きく異なり、暗号技術全般についての専門的な深い知識を必要とする調査項目が多数あったことから、正確に回答する意思があったとしても、知識が不十分であったり、認識に誤りがあったりするなどの理由で適切な回答ができなかった可能性もある。

このように、暗号技術全般についてのかなり深い知識を必要とする調査項目を対象とするような調査をインターネットアンケート調査で行うことは、信頼性の低い回答が多く含まれることが避けられない状況である。実際、今回の調査では、23,747 名のアンケート依頼に対して最終的に集計対象とした有効回答数はわずか９名、有効回答率にして 0.04％にすぎず、効果的な調査方法ではないと判断される。

3.3. 政府系情報システム・規格調査結果（調査C結果）

デジタル庁及び IPA の協力のもと、政府系情報システムの回答数 98 を得た。また、政府系情報システム規格（法省令・ガイドライン・政府系情報システム規格等）の公開情報をもとに、表 2.16 で示す 17 の政府系規格において、暗号アルゴリズムについての記載があった。

政府系情報システムのアンケート回答総数 98 件、政府系規格の公開情報調査 17 件についての集計結果を以下に報告する。なお、グラフの記法は以下のとおりである。

以下の（１）政府系情報システム・規格（共通鍵暗号（64 ビットブロック暗号））から（７）政府系情報システム・規格（ハッシュ関数）においては、暗号アルゴリズムを次の７つに分類し、各分類の該当総数を n 値として、アンケート回答総数に n 値が占める割合を記載した。

○共通鍵暗号（64 ビットブロック暗号）
○共通鍵暗号（128 ビットブロック暗号）
○共通鍵暗号（ストリーム暗号）
○暗号利用モード／メッセージ認証コード
○公開鍵暗号（署名）
○公開鍵暗号（守秘・鍵共有）
○ハッシュ関数

例：アンケート回答総数 100、共通鍵暗号（64 ビットブロック暗号）のいずれかを選択した回答数（該当総数）10 の場合
（表記方法）n=10, 10%

また、該当暗号アルゴリズムの回答数が該当総数に占める割合をグラフ中に記載した。

例：上記の例で共通鍵暗号（64 ビットブロック暗号）の Triple DES の回答数が 3 の場合
（表記方法）30%

また、以下の（８）政府系情報システム（エンティティ認証）から（１２）政府系情報システム（利用しているオープンソースソフトウェア）については、政府系情報システムのアンケート回答のみの調査結果となる。各調査項目で、実装・利用・準拠しているアンケート回答総数を n 値として記載した。

例：アンケート回答総数 100、エンティティ認証を実装していないと選択した回答数（該当総数）60、エンティティ認証のいずれかを選択した回答数（該当総数）40 の場合
（表記方法）n=40

（１）政府系情報システム・規格（共通鍵暗号（64 ビットブロック暗号）

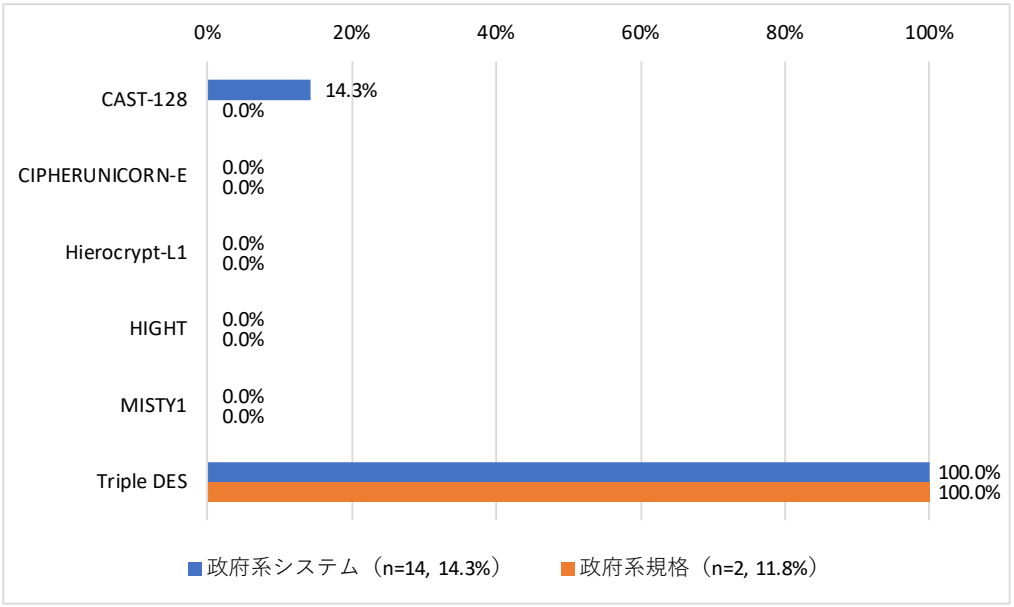

図 3.25 政府系情報システム・規格（共通鍵暗号（64 ビットブロック暗号））

（２）政府系情報システム・規格（共通鍵暗号（128 ビットブロック暗号）

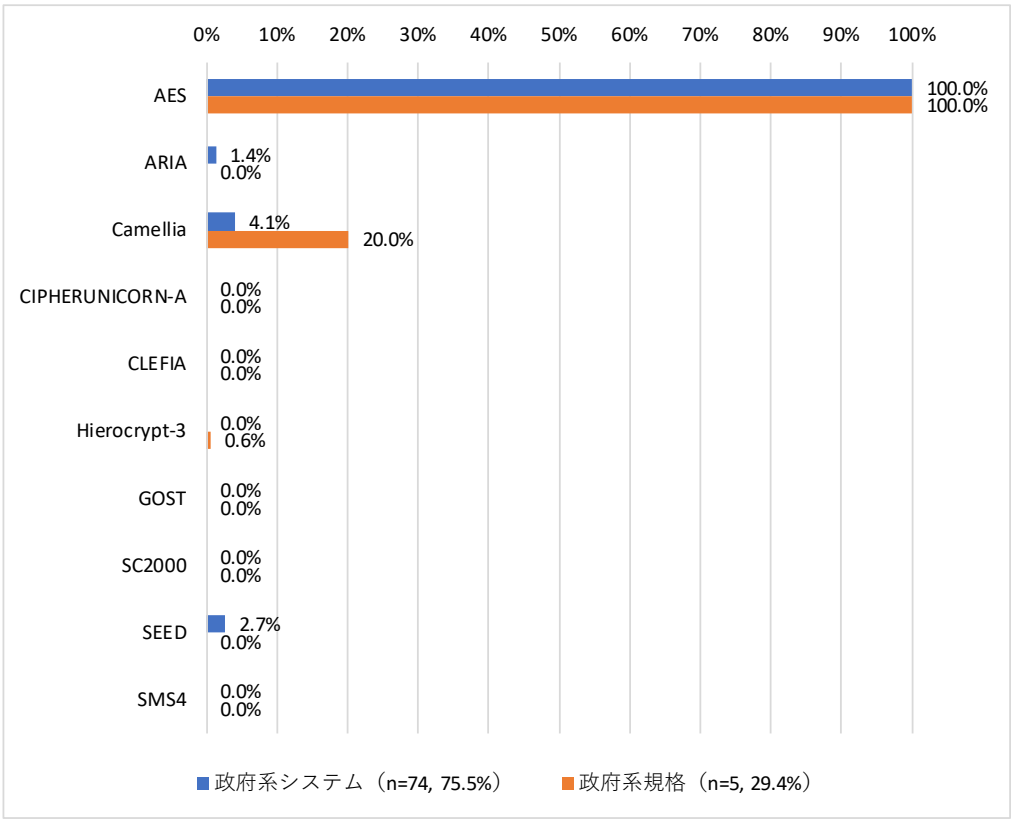

図 3.26 政府系情報システム・規格（共通鍵暗号（128 ビットブロック暗号））

（３）政府系情報システム・規格（共通鍵暗号（ストリーム暗号・認証暗号））

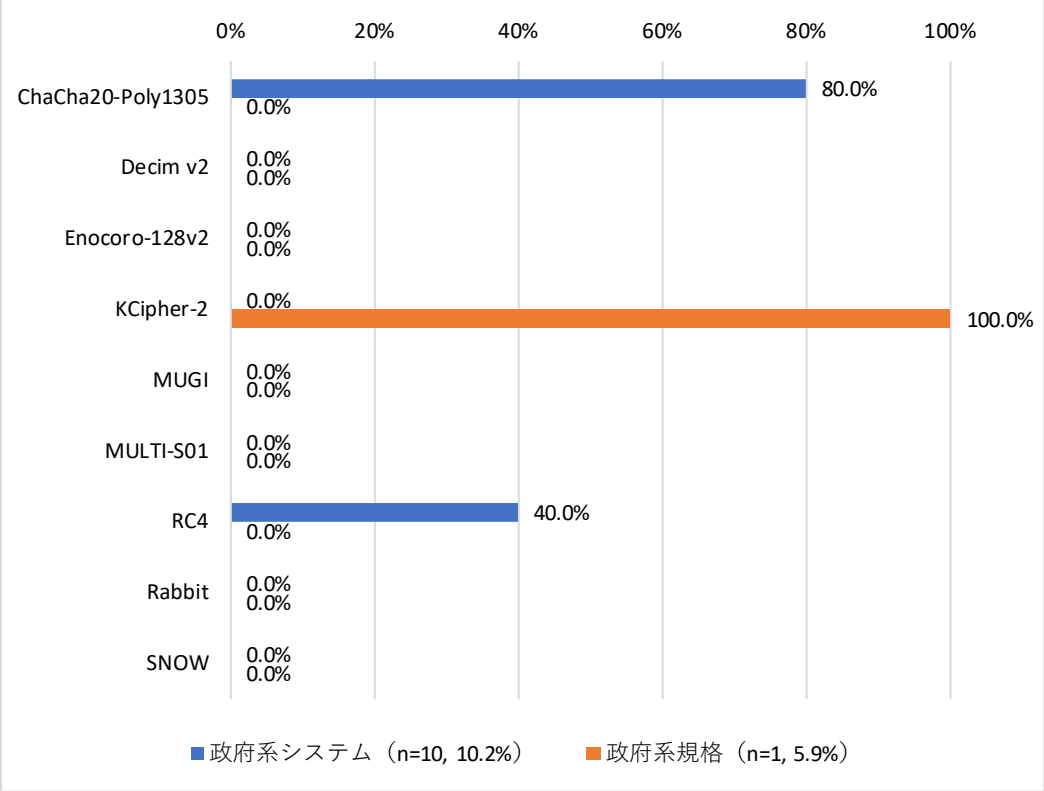

図 3.27 政府系情報システム・規格（共通鍵暗号（ストリーム暗号・認証暗号））

（4）政府系情報システム・規格（暗号利用モード／メッセージ認証コード）

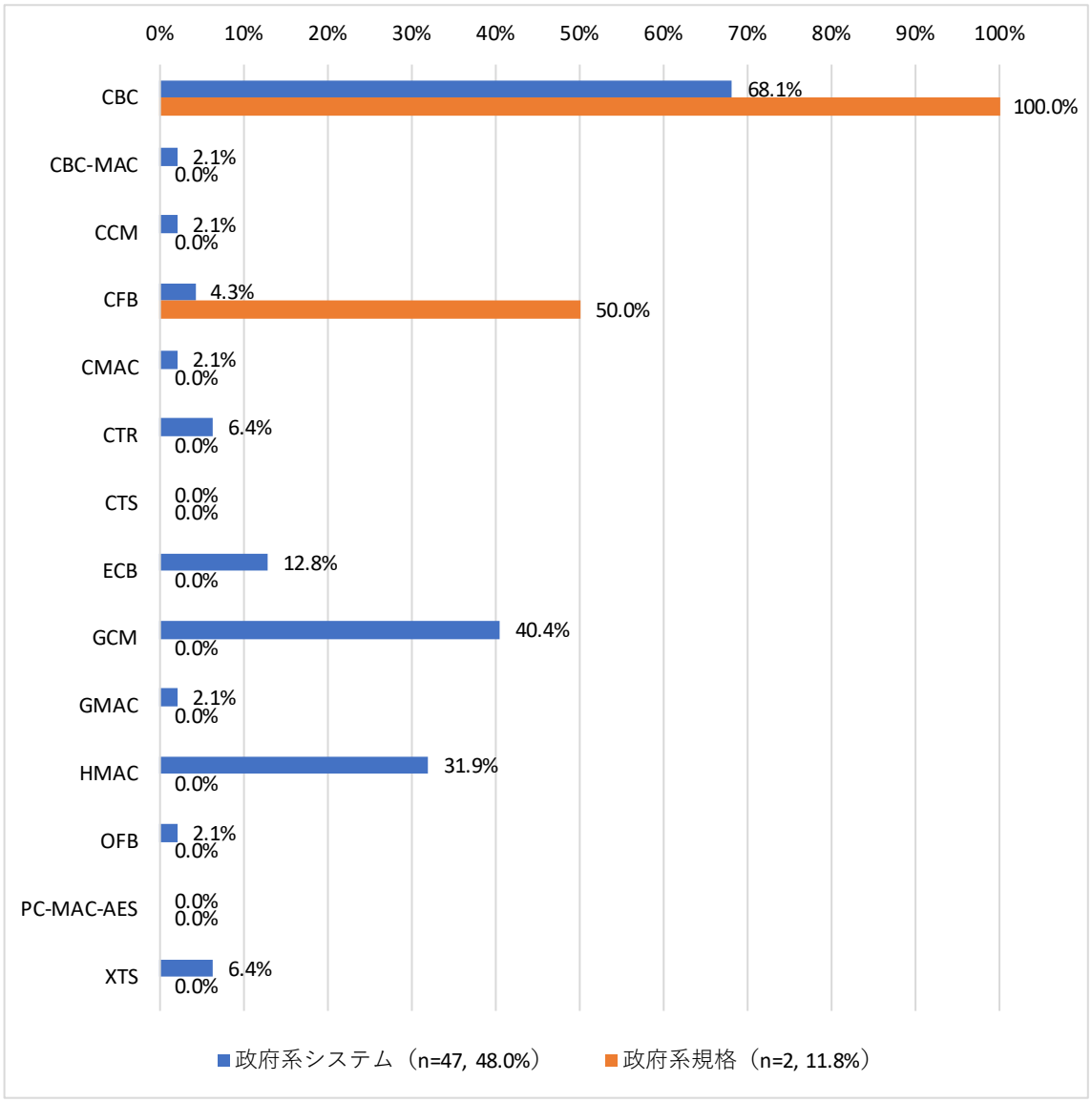

図 3.28 政府系情報システム・規格（暗号利用モード／メッセージ認証コード）

（５）政府系情報システム・規格（公開鍵暗号（署名））

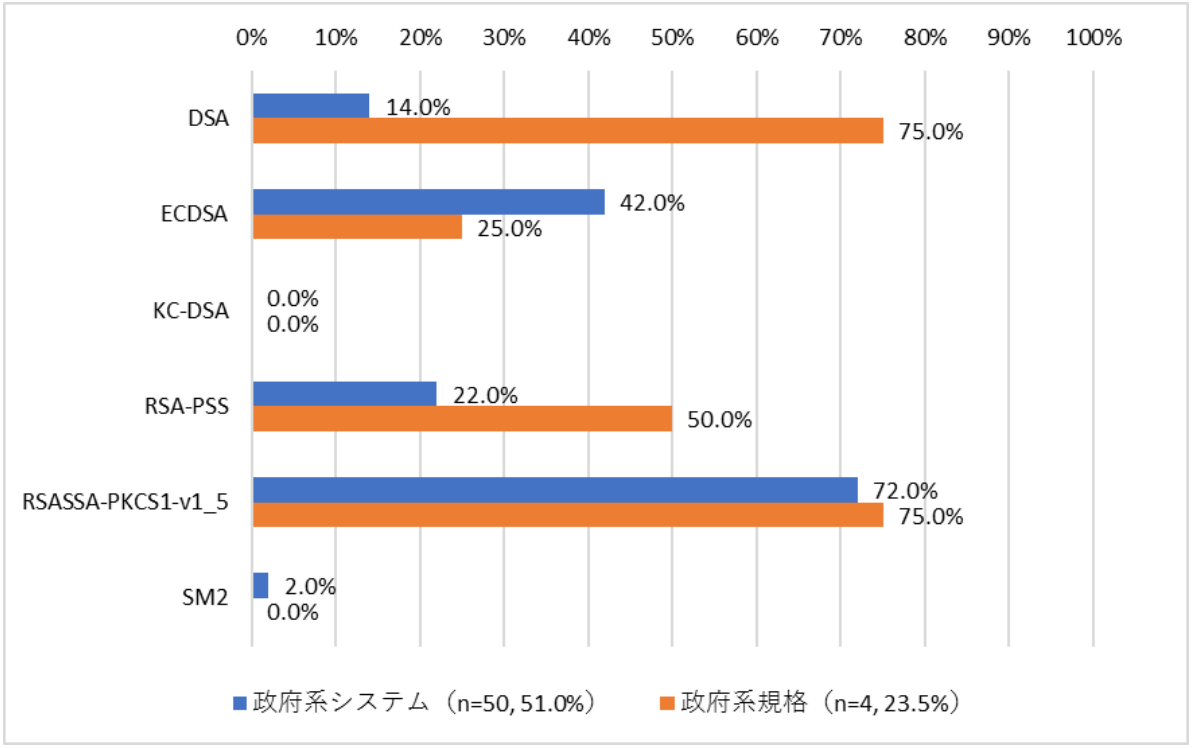

図 3.29 政府系情報システム・規格（公開鍵暗号（署名））

（６）政府系情報システム・規格（公開鍵暗号（守秘・鍵共有））

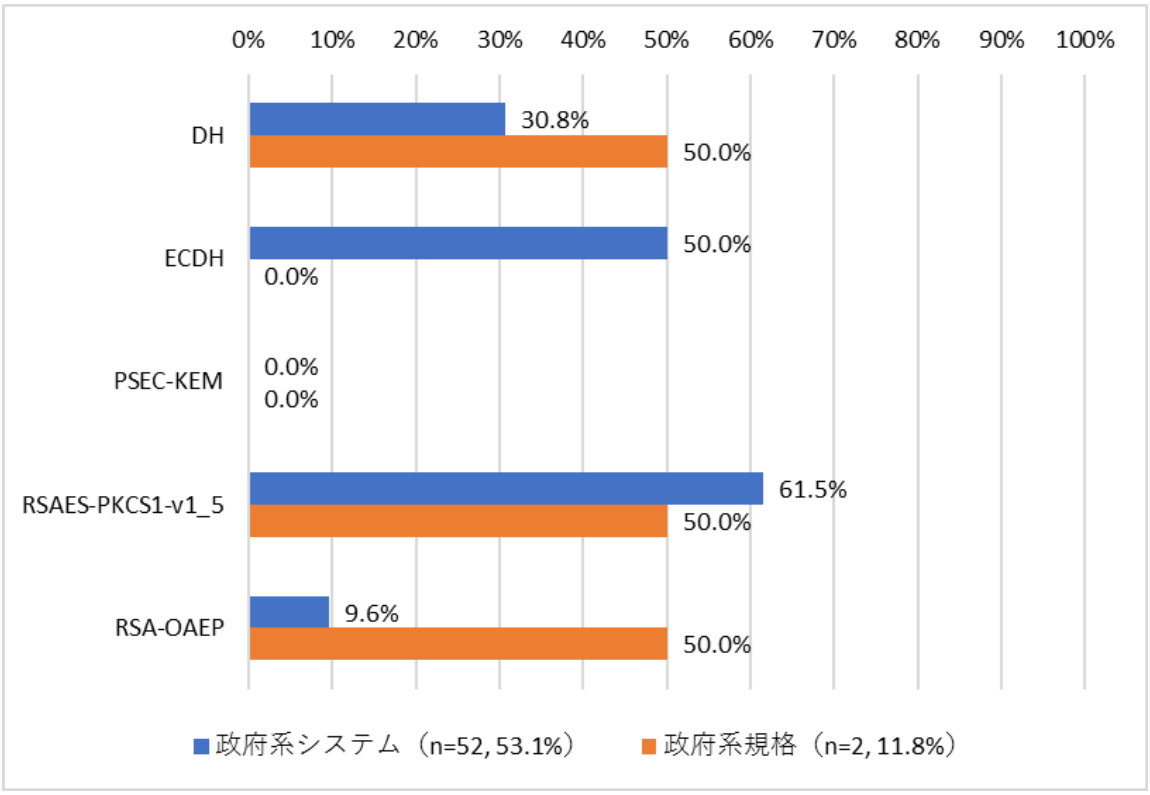

図 3.30 政府系情報システム・規格（公開鍵暗号（守秘・鍵共有））

（７）政府系情報システム・規格（ハッシュ関数）

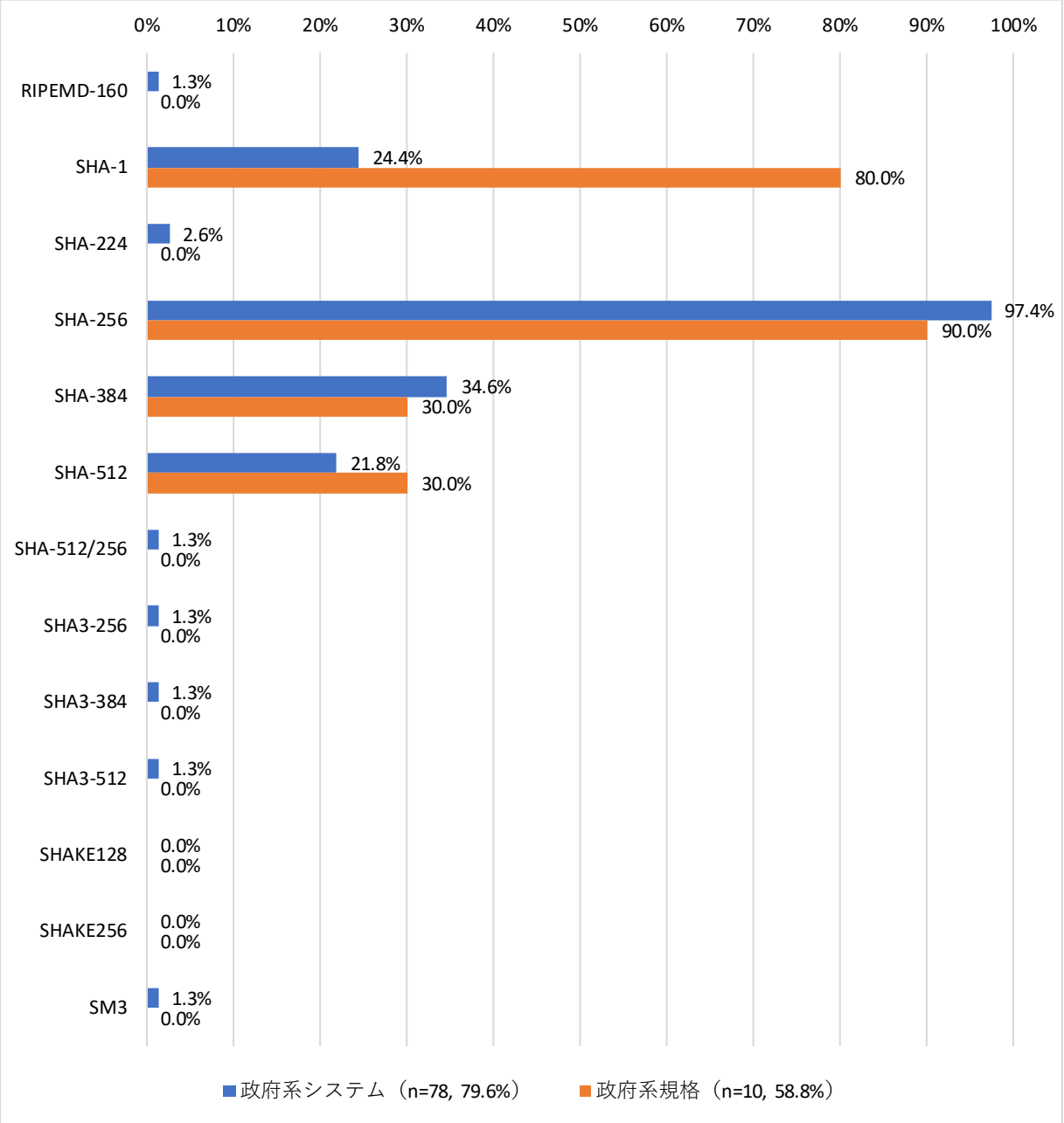

図 3.31 政府系情報システム・規格（ハッシュ関数）

（８）政府系情報システム（エンティティ認証）

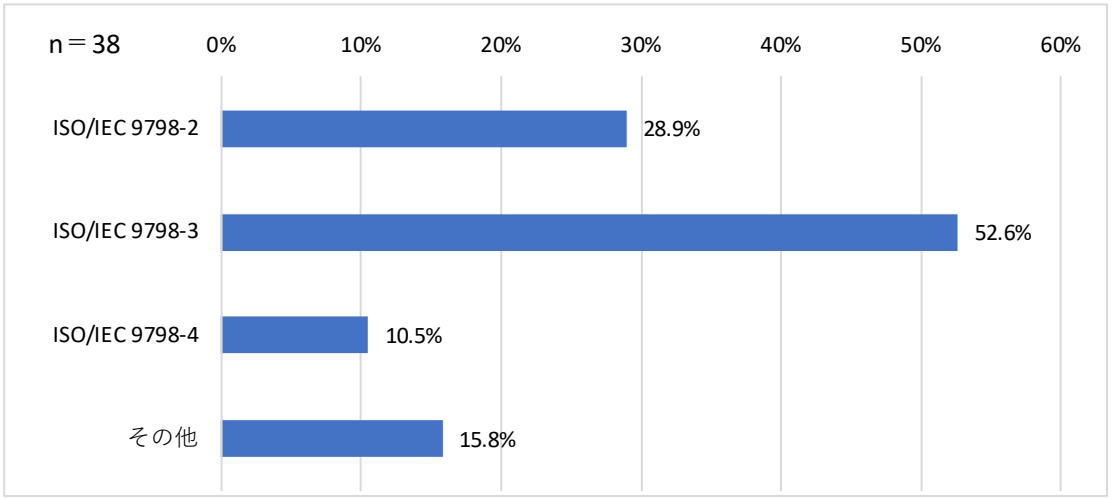

図 3.32 政府系情報システム（エンティティ認証）

（９）政府系情報システム（利用している国際的な民間規格（プロトコル規格を含む））

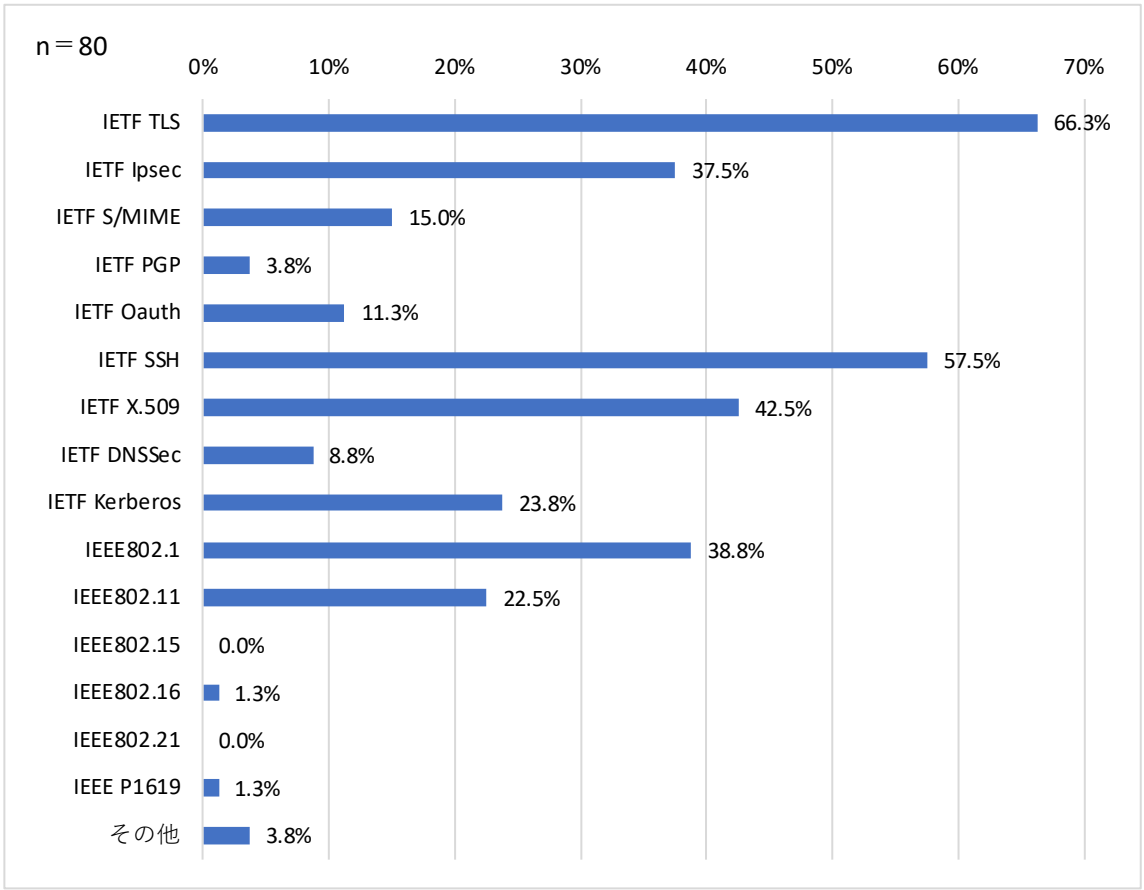

図 3.33 政府系情報システム（利用している国際的な民間規格（プロトコル規格を含む））

（１０）政府系情報システム（準拠している業界団体規格（業界団体名））

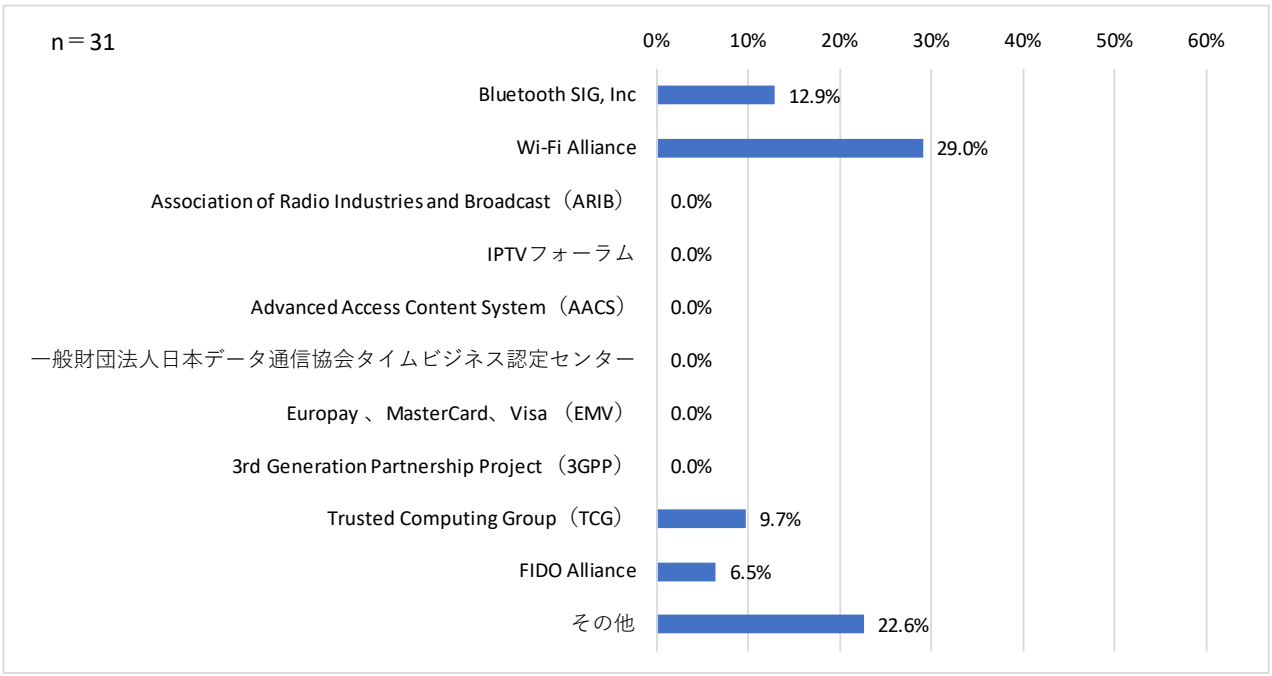

図 3.34 政府系情報システム（準拠している業界団体規格（業界団体名））

（１１）政府系情報システム（第三者評価・試験及び認証制度の取得製品の利用状況）

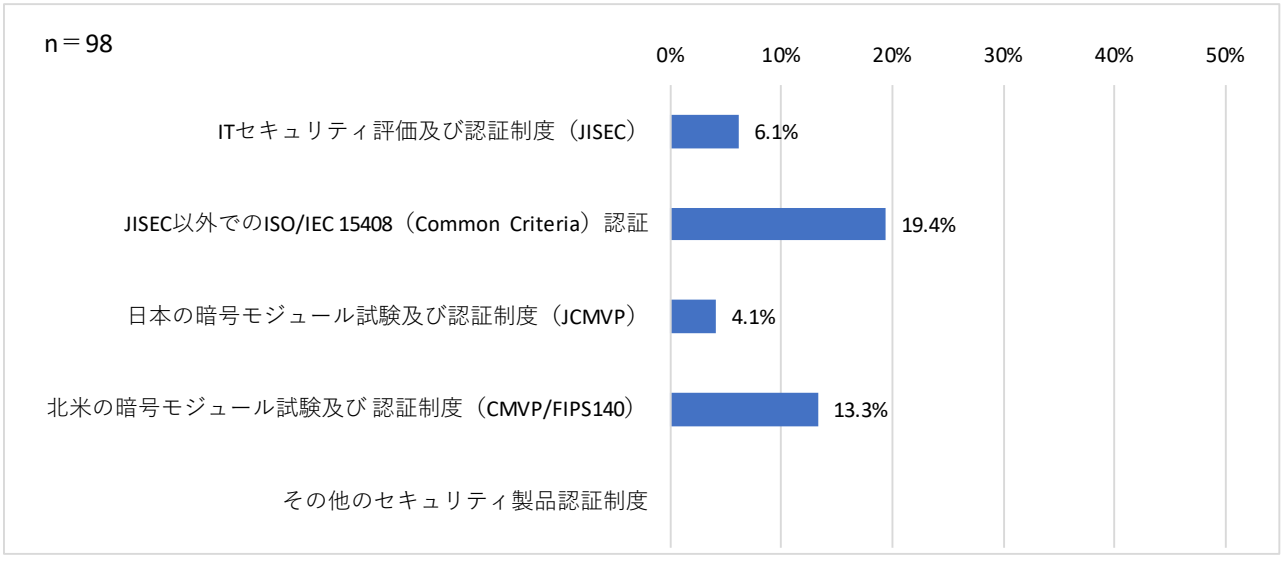

図 3.35 政府系情報システム（第三者評価・試験及び認証制度の取得製品の利用状況）

（１２）政府系情報システム（利用しているオープンソースソフトウェア）

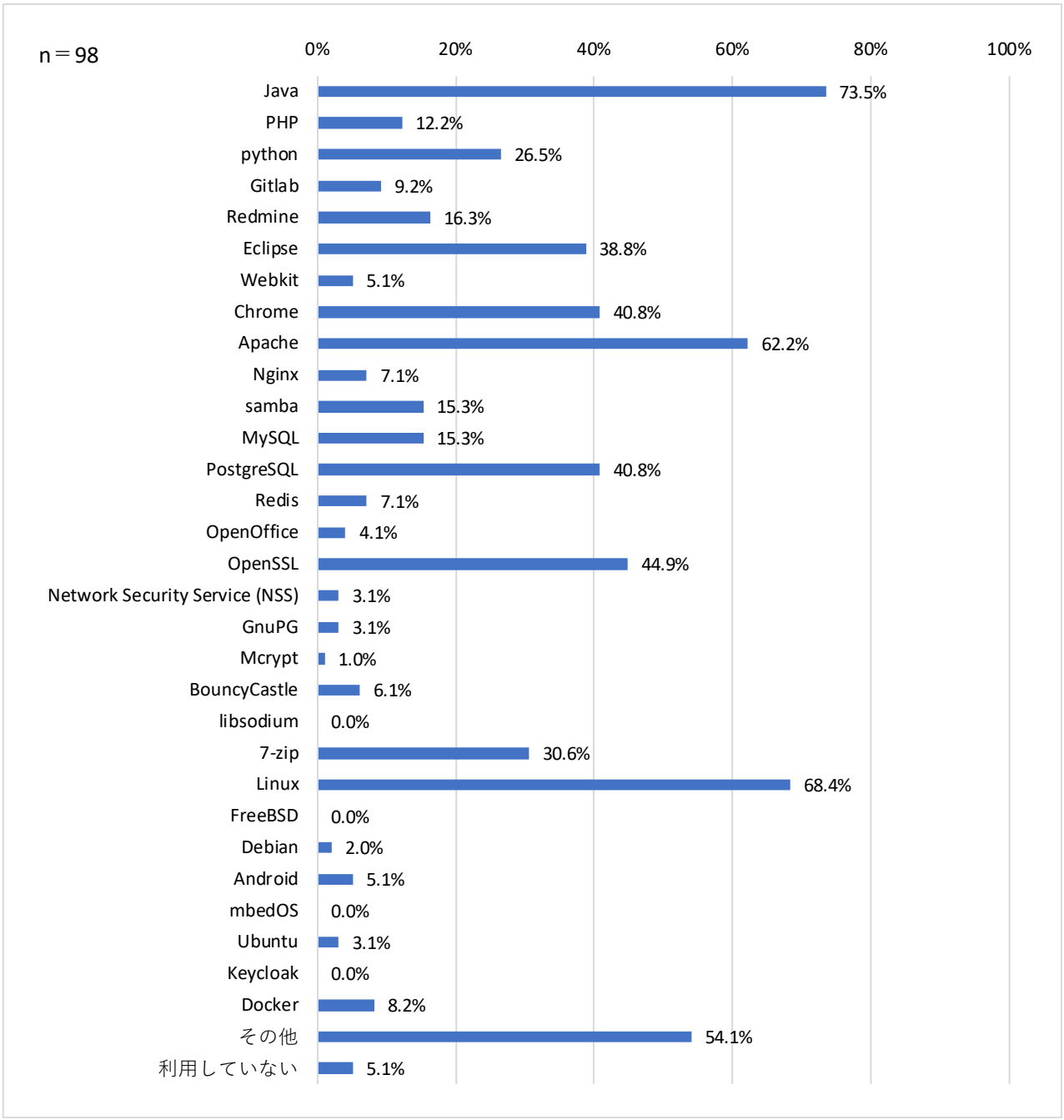

図 3.36 政府系情報システム（利用しているオープンソースソフトウェア）

3.4. 標準規格・民間規格・特定団体規格調査結果（調査D結果）

表 2.18 に記載の国際的な民間規格の集計結果を以下に報告する。

（1）標準規格・民間規格（共通鍵暗号（64 ビットブロック暗号）

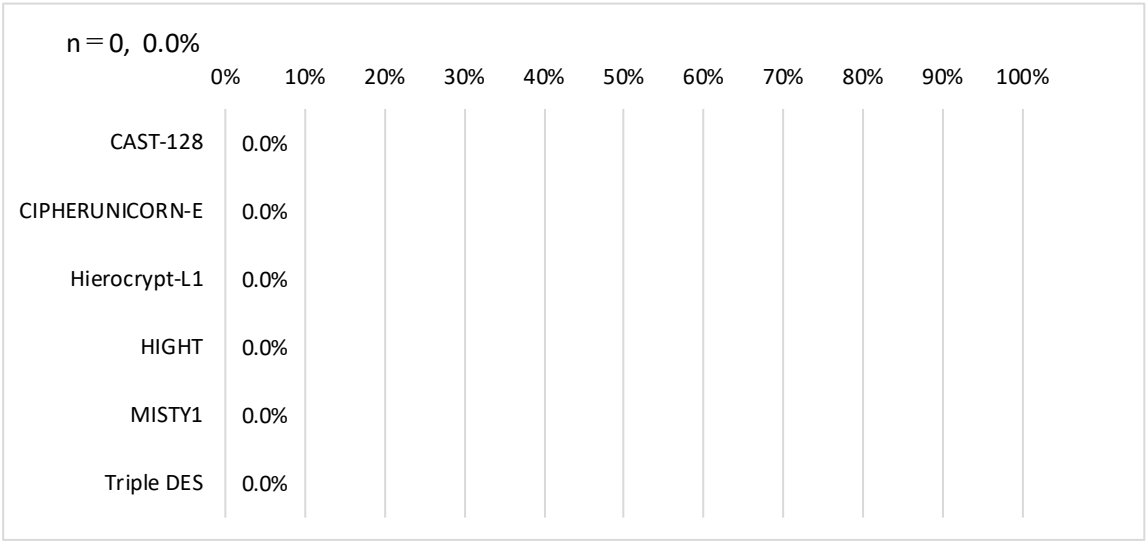

図 3.37 標準規格・民間規格（共通鍵暗号（64 ビットブロック暗号））

（2）標準規格・民間規格（共通鍵暗号（128 ビットブロック暗号）

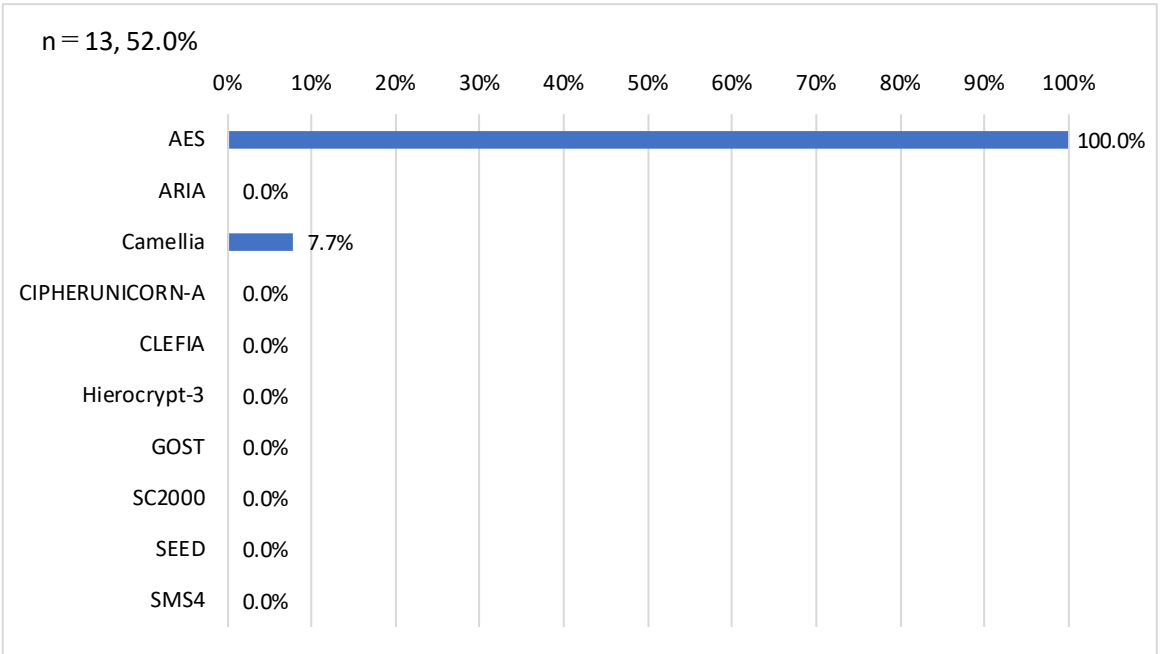

図 3.38 標準規格・民間規格（共通鍵暗号（128 ビットブロック暗号））

（３）標準規格・民間規格（共通鍵暗号（ストリーム暗号・認証暗号）

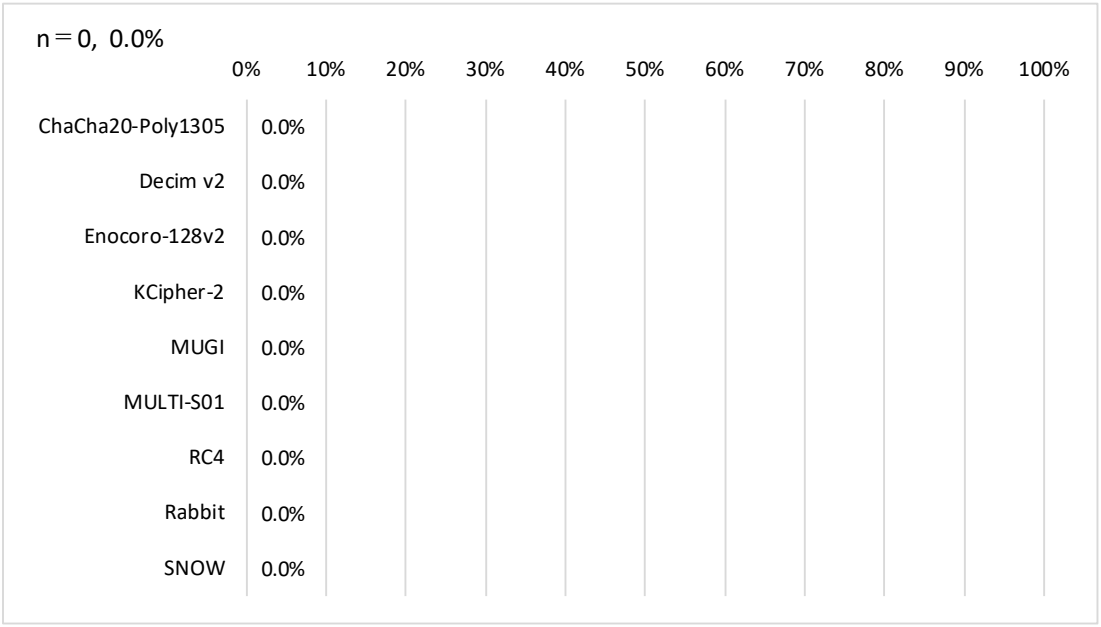

図 3.39 標準規格・民間規格（共通鍵暗号（ストリーム暗号・認証暗号））

（４）標準規格・民間規格（暗号利用モード／メッセージ認証コード）

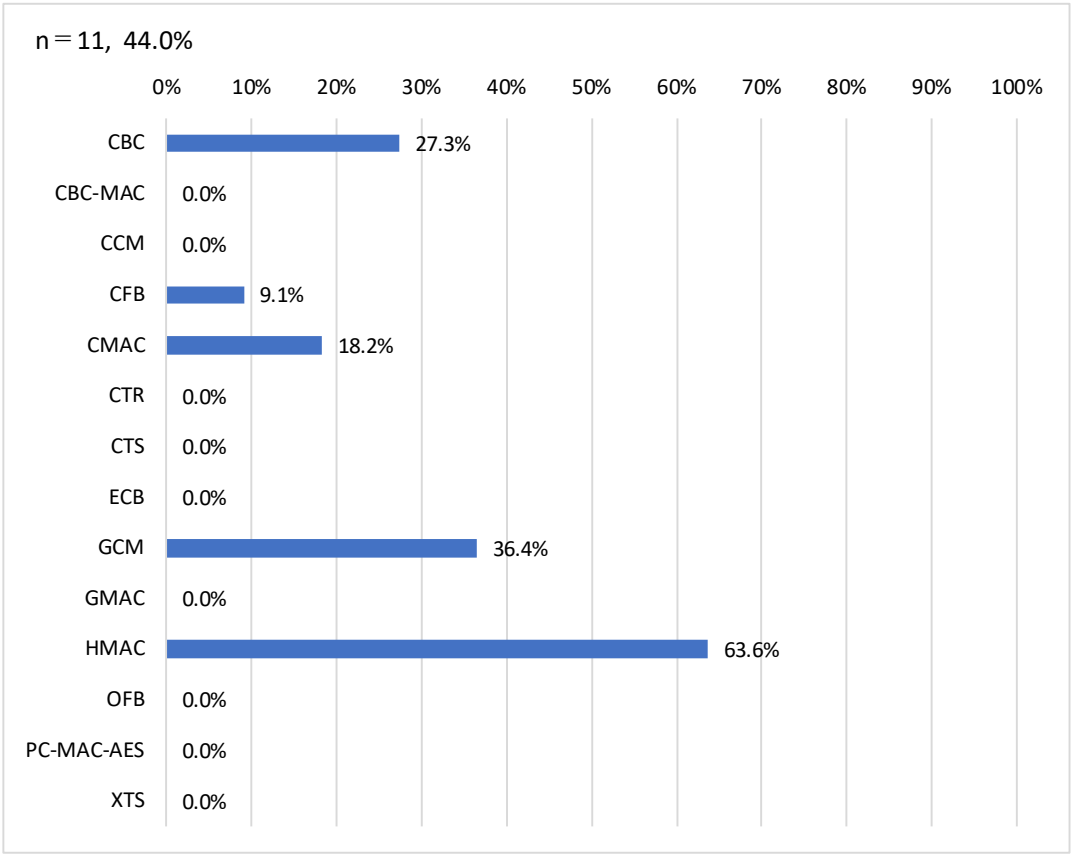

図 3.40 標準規格・民間規格（暗号利用モード／メッセージ認証コード）

（５）標準規格・民間規格（公開鍵暗号（署名））

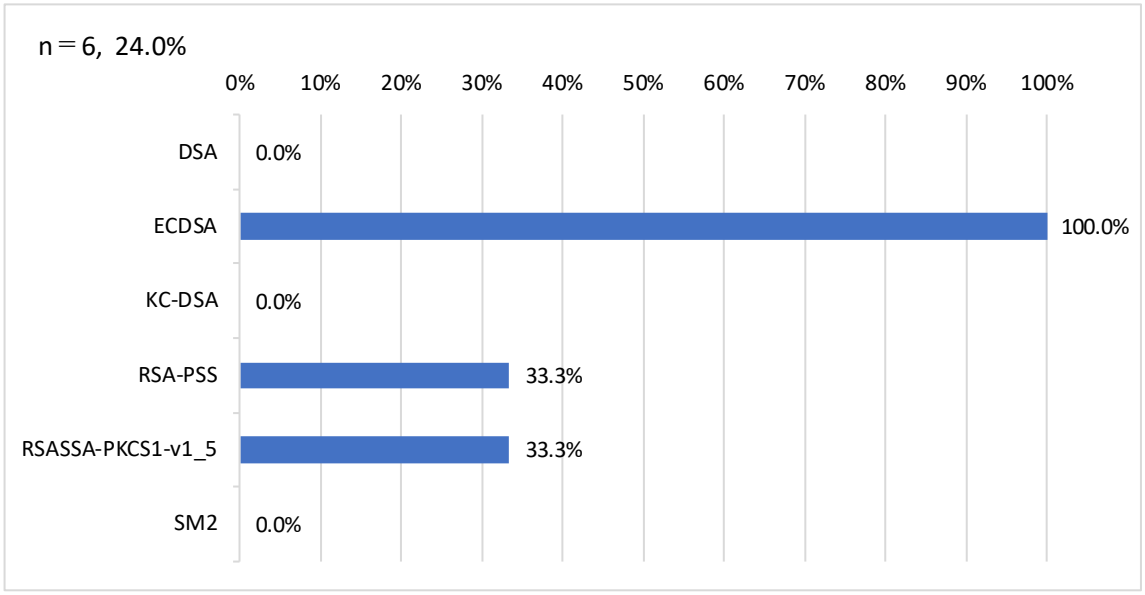

図 3.41 標準規格・民間規格（公開鍵暗号（署名））

（６）標準規格・民間規格（公開鍵暗号（守秘・鍵共有））

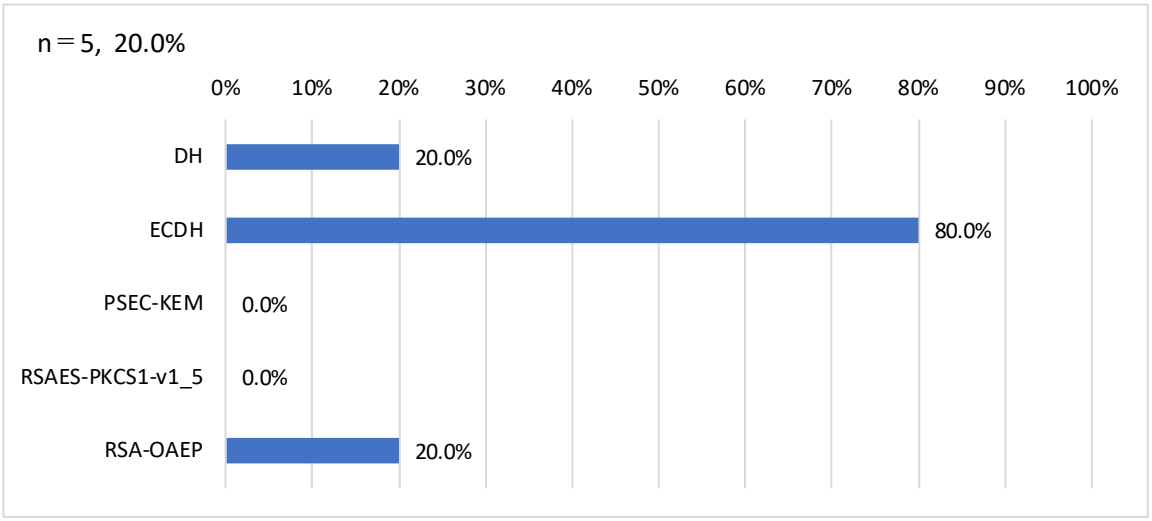

図 3.42 標準規格・民間規格（公開鍵暗号（守秘・鍵共有））

（７）標準規格・民間規格（ハッシュ関数）

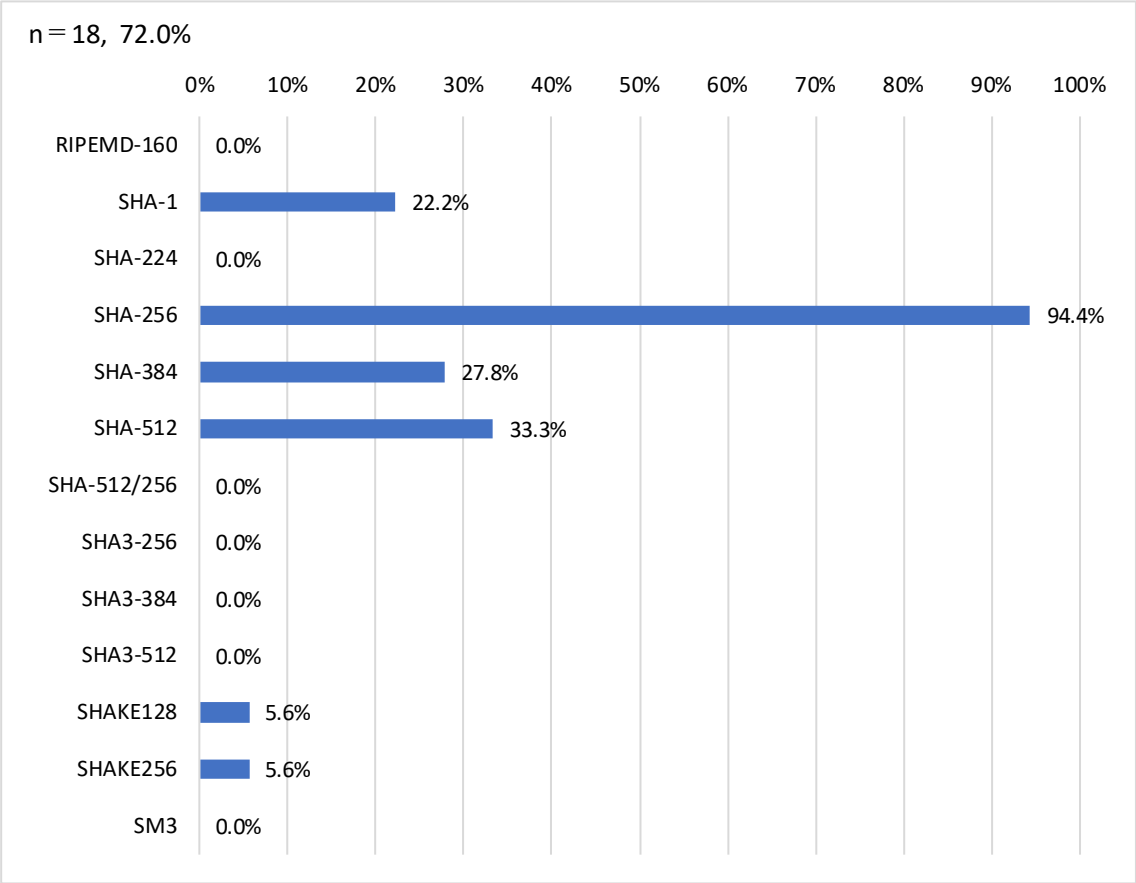

図 3.43 標準規格・民間規格（ハッシュ関数）

3.5. オープンソースソフトウェア調査結果（調査E結果）

オープンソースプロジェクト調査では、表 2.20 で示す計 30 のプロジェクトについて、調査対象暗号アルゴリズムに関する実装調査を行った。以下に集計結果を報告する。

（1）オープンソースソフトウェア（共通鍵暗号（64 ビットブロック暗号））

調査対象のオープンソースのうち、共通鍵暗号（64 ビットブロック暗号）の区分に該当する暗号アルゴリズムを搭載しているオープンソースは 26 個である。それらのオープンソースに対する個々の暗号アルゴリズムの搭載率としては、DES（96.2%）が最も高く、次いで Triple DES（92.3%）、Blowfish（76.9%）となった。

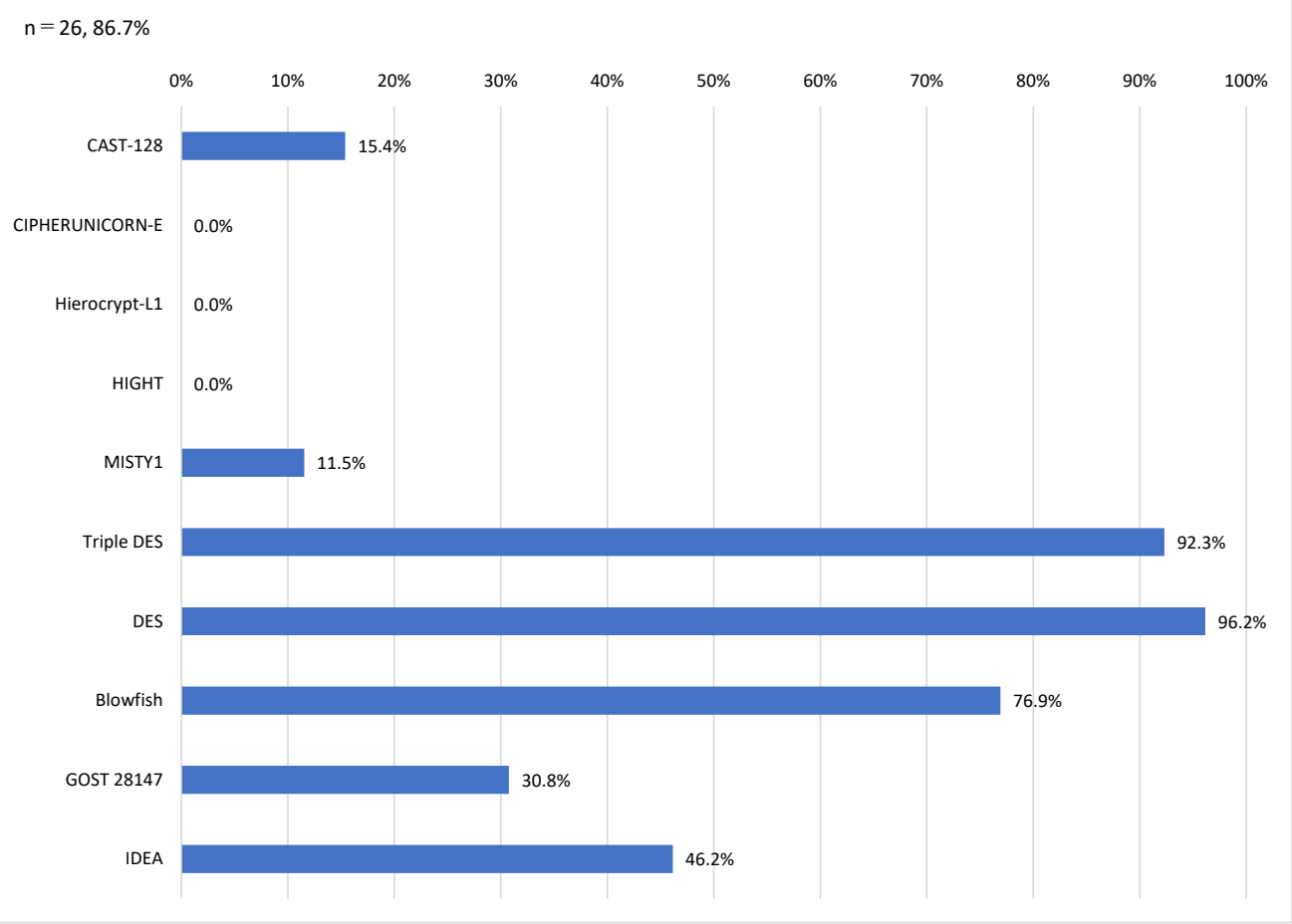

図 3.44 オープンソースソフトウェア（共通鍵暗号（64 ビットブロック暗号））

（２）オープンソースソフトウェア（共通鍵暗号（128 ビットブロック暗号））

調査対象のオープンソースのうち、共通鍵暗号（128 ビットブロック暗号）の区分に該当する暗号アルゴリズムを搭載しているオープンソースは 29 個である。それらのオープンソースに対する個々の暗号アルゴリズムの搭載率としては、AES（100.0%）が最も高く、次いで Camellia（51.7%）、SEED（48.3%）、Twofish（48.3%）となった。

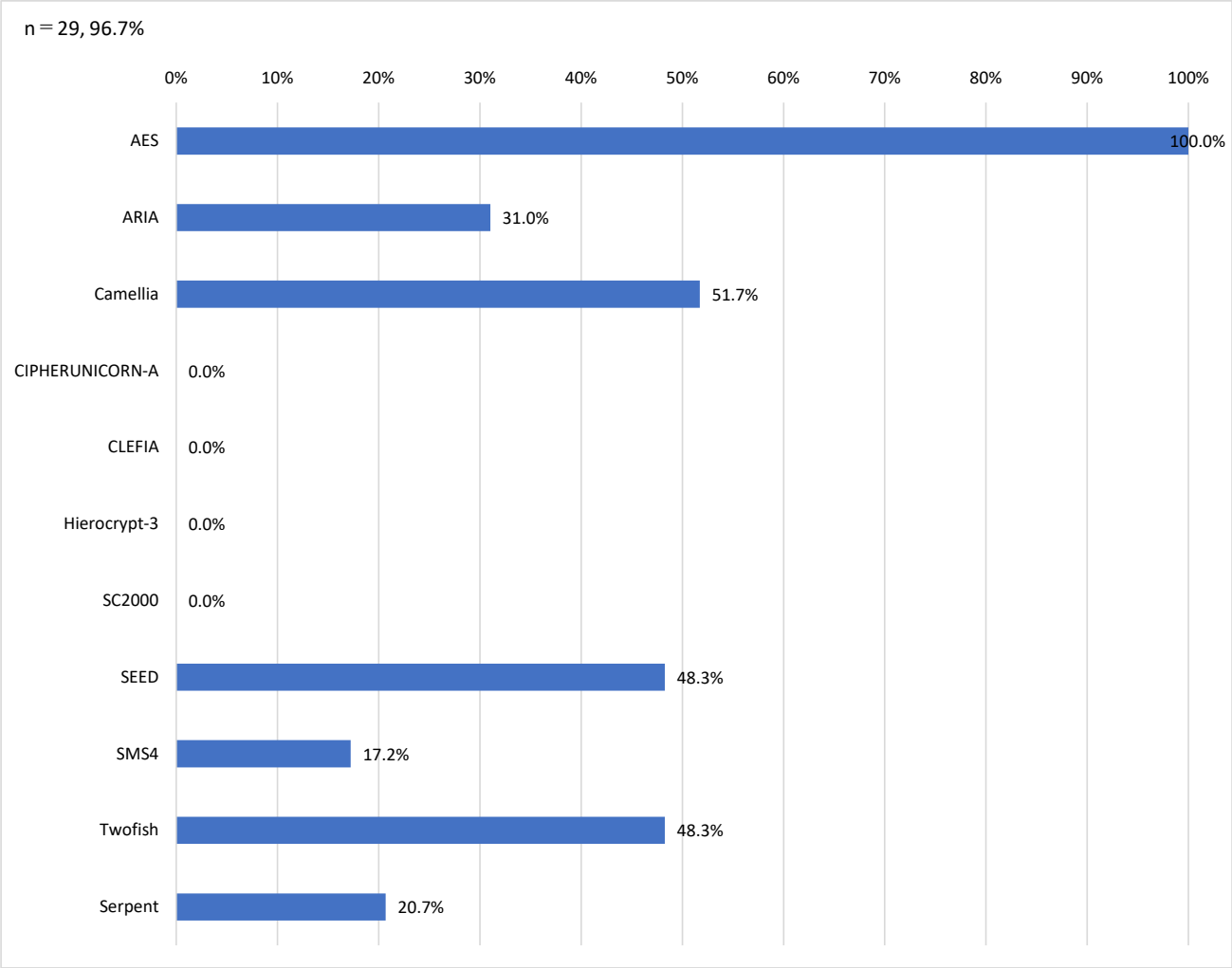

図 3.45 オープンソースソフトウェア（共通鍵暗号（128 ビットブロック暗号））

（３）オープンソースソフトウェア（共通鍵暗号（ストリーム暗号・認証符号））

調査対象のオープンソースのうち、共通鍵暗号（ストリーム暗号・認証符号）の区分に該当する暗号アルゴリズムを搭載しているオープンソースは 25 個である。それらのオープンソースに対する個々の暗号アルゴリズムの搭載率としては、RC4（88.0%）が最も高く、次いで ChaCha20（76.0%）、SNOW（12.0%）となった。

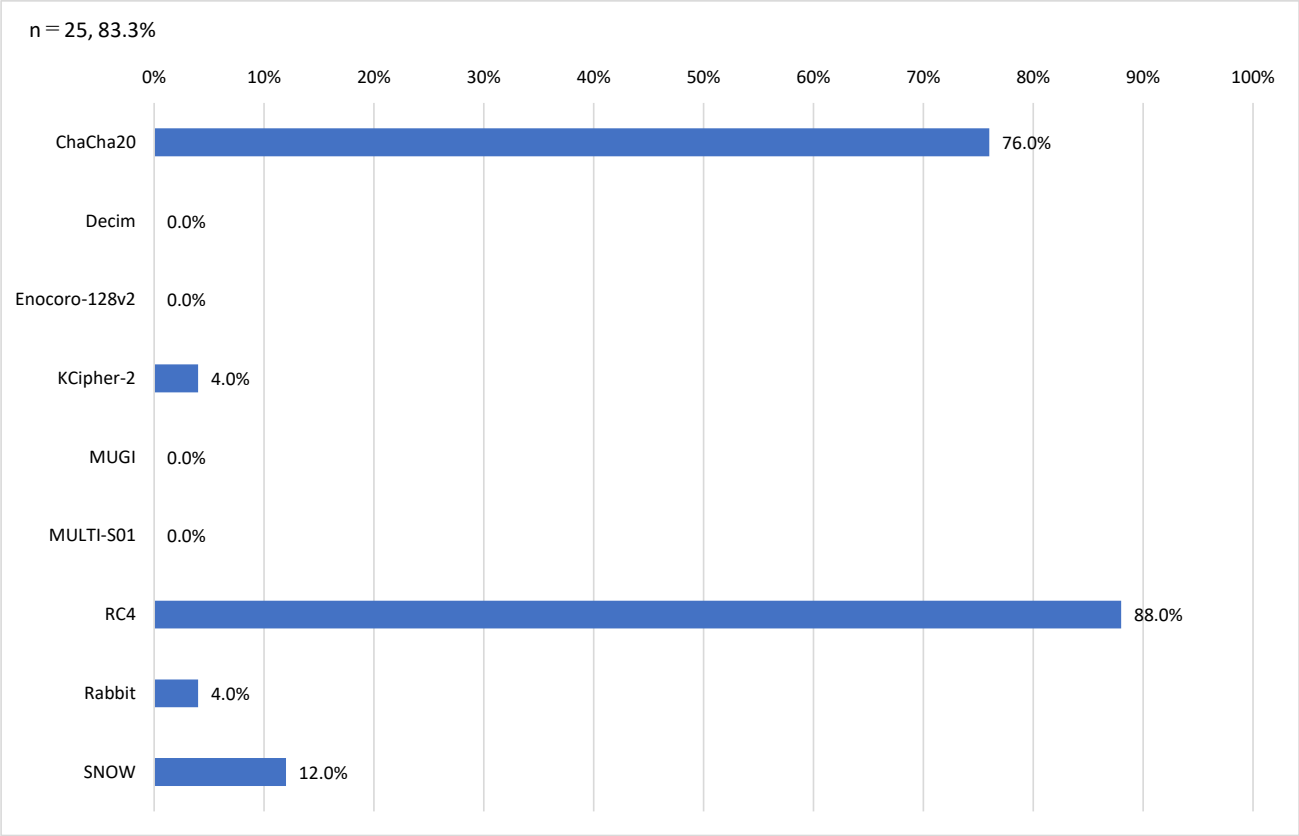

図 3.46 オープンソースソフトウェア（共通鍵暗号（ストリーム暗号・認証符号））

（4）オープンソースソフトウェア（暗号利用モード／メッセージ認証コード）

調査対象のオープンソースのうち、暗号利用モード／メッセージ認証コードの区分に該当する暗号アルゴリズムを搭載しているオープンソースは 29 個である。それらのオープンソースに対する個々の暗号アルゴリズムの搭載率としては、HMAC（100.0%）が最も高く、次いで CBC（93.1%）、GCM（86.2%）となった。

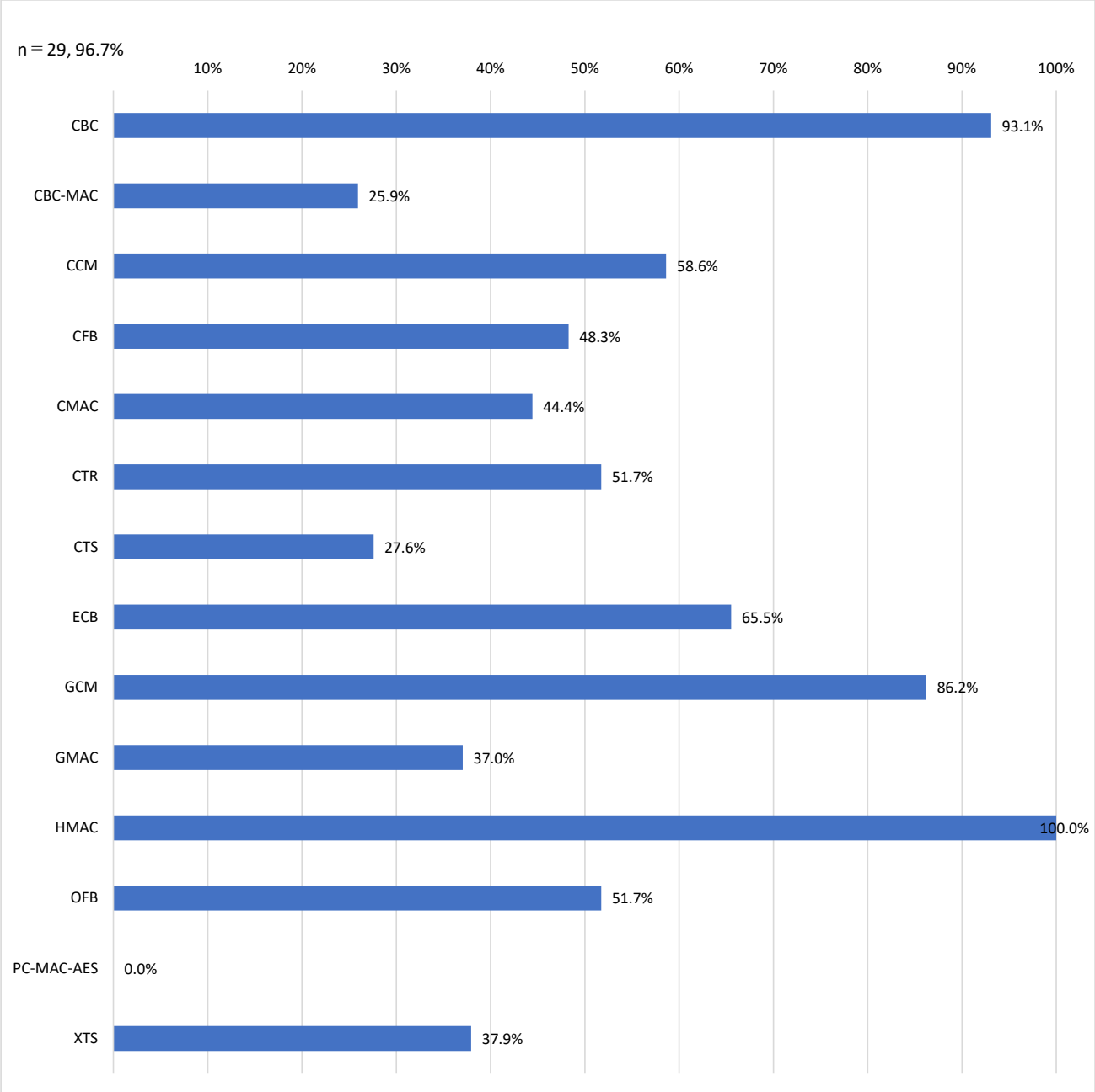

図 3.47 オープンソースソフトウェア（暗号利用モード／メッセージ認証コード）

（５）オープンソースソフトウェア（公開鍵暗号（署名））

調査対象のオープンソースのうち公開鍵暗号（署名）の区分に該当する暗号アルゴリズムを搭載しているオープンソースは 29 個である。それらのオープンソースに対する個々の暗号アルゴリズムの搭載率としては、DSA（89.7%）が最も高く、次いで ECDSA（82.8%）、RSASSA-PKCS1-v1_5（65.5%）となった。

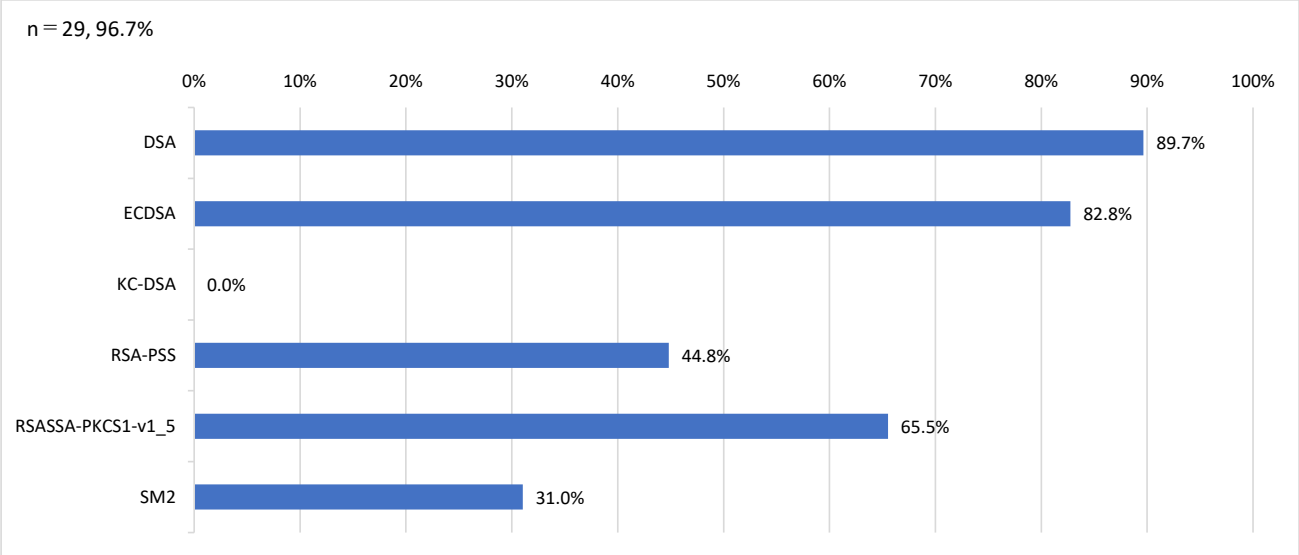

図 3.48 オープンソースソフトウェア（公開鍵暗号（署名））

（６）オープンソースソフトウェア（公開鍵暗号（守秘・鍵交換））

調査対象のオープンソースのうち公開鍵暗号（守秘・鍵交換）の区分に該当する暗号アルゴリズムを搭載しているオープンソースは 25 個である。それらのオープンソースに対する個々の暗号アルゴリズムの搭載率としては、DH（100.0%）が最も高く、次いで ECDH（96.0%）、RSAES-PKCS1-v1_5（68.0%）となった。

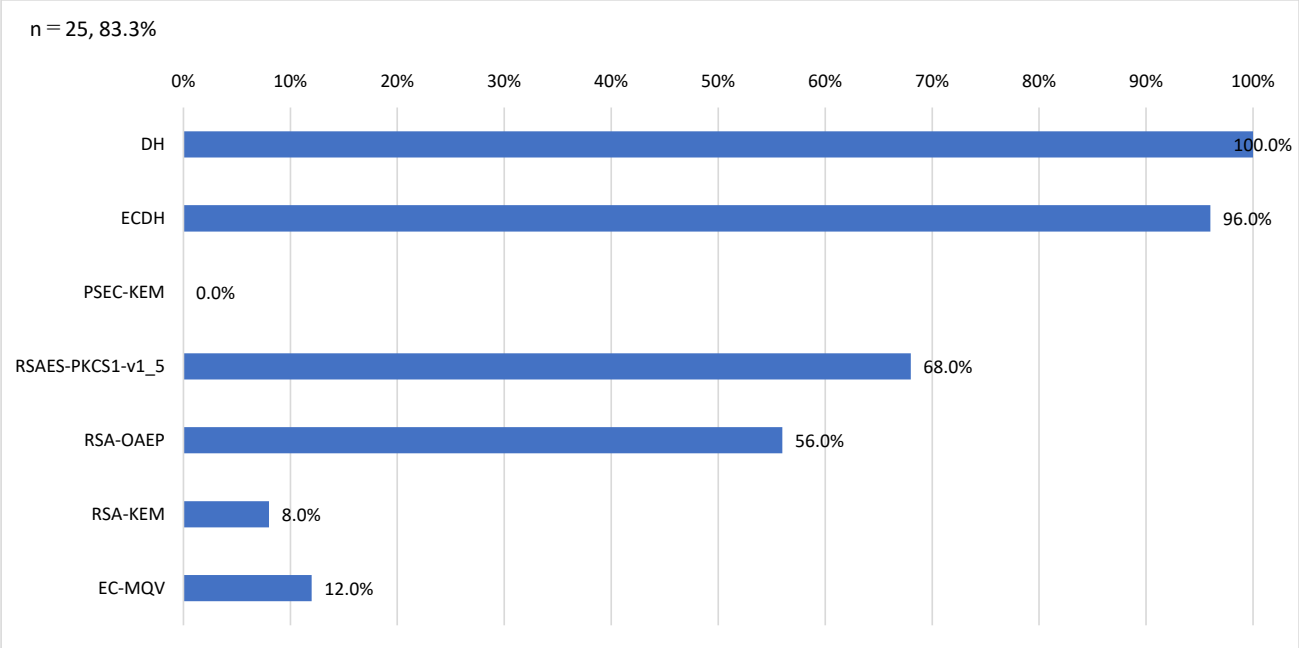

図 3.49 オープンソースソフトウェア（公開鍵暗号（守秘・鍵交換））

（7）オープンソースソフトウェア（ハッシュ関数）

調査対象のオープンソースのうちハッシュ関数の区分に該当する暗号アルゴリズムを搭載しているオープンソースは 30 個である。それらのオープンソースに対する個々の暗号アルゴリズムの搭載率としては、SHA-256（96.7%）が最も高く、次いで MD5（93.3%）、SHA-1（86.7%）、SHA-512（86.7%）となった。

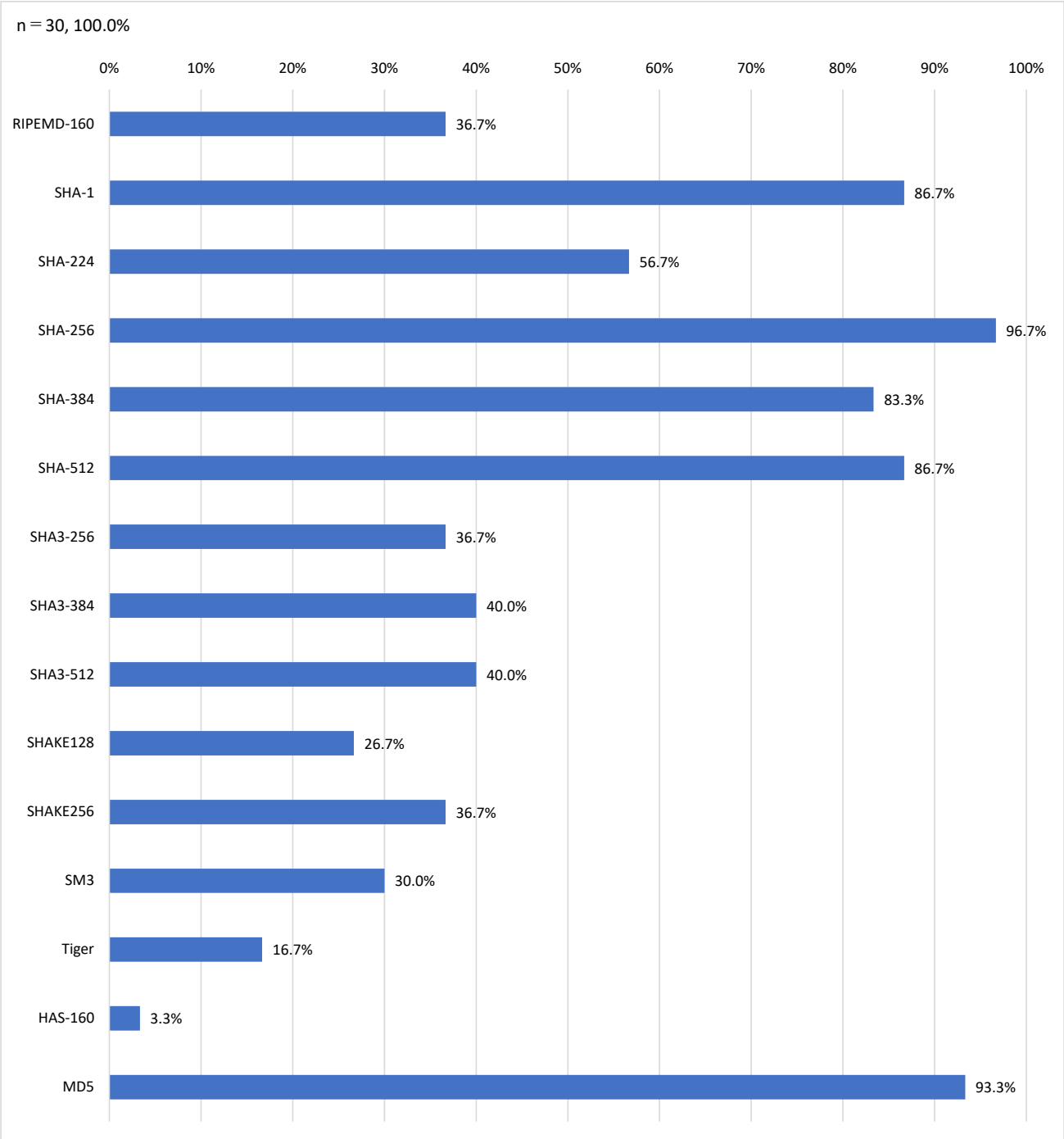

図 3.50 オープンソースソフトウェア（ハッシュ関数）

4. まとめ

本調査では、次期電子政府推奨暗号リスト掲載の対象となる暗号アルゴリズムの製品化、利用実績及び国際標準規格等の調査を行った。

○調査Ａでは、８社の応募者について提案暗号アルゴリズムに関するアンケート調査を実施した。

○調査Ｂでは、14 の業界団体、会員企業総数 2,535 社にアンケート回答を依頼し、65 社から 114 製品・システムの回答数を得た。また、個別企業調査では、108 社の個別企業にアンケート回答を依頼し、28 社から 37 製品・システムの回答数を得た。さらに、応募者調査では、電子政府推奨暗号アルゴリズムの応募者８社にアンケート回答を依頼し、４社から４製品・システムの回収数を得た。また、インターネットアンケート調査では、調査パネル 23,747 名にアンケート回答を依頼し、146 名（114 社）から 146 製品・システムの回答数を得た。以上より、合計 211 社、301 製品・システムに関する暗号アルゴリズムの利用状況の調査結果を確保した。その中から、合計 82 社、128 製品・システムに関する暗号アルゴリズムの利用実績の有効回答数を選定した。製品・システムに実装されている暗号アルゴリズムの集計結果については、上記の合計 82 社、128 製品・システムに関する暗号アルゴリズムの利用状況のアンケート調査結果のうち、実装している暗号アルゴリズムが分からないと回答した調査結果を除いたものに、41 社、100 製品・システムの公開情報調査の結果を合算して、暗号アルゴリズムの記載のある 101 社、209 製品・システムを対象に市販製品の集計を行った。

○調査Ｃでは、政府系情報システムでの利用実績に関するアンケート調査で 98 件、政府系情報システム規格（法省令・ガイドライン・政府系情報システム規格等）での採用実績に関する公開情報調査で 17 件について調査を実施した。

○調査Ｄでは、国際的な民間規格での採用実績に関する公開情報調査で 25 件について調査を実施した。

○調査Ｅでは、30 件のオープンソースソフトウェアでの利用実績について調査を実施した。

以下に、各項目について採用実績の高い上位３位までの暗号アルゴリズムを報告する。

（１）共通鍵暗号（64 ビットブロック暗号）の結果

共通鍵暗号（64 ビットブロック暗号）での採用実績の高い上位３位までの暗号アルゴリズムを以下に示す。

表 4.1 共通鍵暗号（64 ビットブロック暗号）の結果

調査分類	詳細	第１位		第２位		第３位	
市販製品調査結果（調査Ｂ結果）	―	Triple DES	100.0%	CAST-128	7.1%	MISTY1	1.8%
政府系情報システム・情報システム規格調査結果（調査Ｃ結果）	システム	Triple DES	100.0%	CAST-128	14.3%	―	―
	規格	Triple DES	100.0%	―	―	―	―
標準規格・民間規格・特定団体規格調査結果（調査Ｄ結果）	国際的な民間規格	―	―	―	―	―	―
オープンソースソフトウェア調査結果（調査Ｅ結果）	―	DES	96.2%	Triple DES	92.3%	Blowfish	76.9%

（２）共通鍵暗号（128 ビットブロック暗号）の結果

共通鍵暗号（128 ビットブロック暗号）での採用実績の高い上位３位までの暗号アルゴリズムを以下に示す。

表 4.2 共通鍵暗号（128 ビットブロック暗号）の結果

調査分類	詳細	第１位		第２位		第３位	
市販製品調査結果（調査Ｂ結果）	―	AES	99.4%	Camellia	3.5%	ARIA SEED	1.2% 1.2%
政府系情報システム・情報システム規格調査結果（調査Ｃ結果）	システム	AES	100.0%	Camellia	4.1%	SEED	2.7%
	規格	AES	100.0%	Camellia	20.0%	Hierocrypt-3	0.6%
標準規格・民間規格・特定団体規格調査結果(調査Ｄ結果)	国際的な民間規格	AES	100.0%	Camellia	7.7%	―	―
オープンソースソフトウェア調査結果(調査Ｅ結果)	―	AES	100.0%	Camellia	51.7%	SEED Twofish	48.3% 48.3%

（３）共通鍵暗号（ストリーム暗号）の結果

共通鍵暗号（ストリーム暗号）での採用実績の高い上位３位までの暗号アルゴリズムを以下に示す。

表 4.3 共通鍵暗号（ストリーム暗号）の結果

調査分類	詳細	第１位		第２位		第３位	
市販製品調査結果（調査Ｂ結果）	—	RC4	83.3%	ChaCha20-Poly1305	8.3%	KCipher-2 MULTI-S01	4.2% 4.2%
政府系情報システム・情報システム規格調査結果（調査Ｃ結果）	システム	ChaCha20-Poly1305	80.0%	RC4	40.0%	—	—
	規格	KCipher-2	100.0%	—	—	—	—
標準規格・民間規格・特定団体規格調査結果（調査Ｄ結果）	国際的な民間規格	—	—	—	—	—	—
オープンソースソフトウェア調査結果（調査Ｅ結果）	—	RC4	88.0%	ChaCha20-Poly1305	76.0%	SNOW	12.0%

（４）暗号利用モード／メッセージ認証コードの結果

暗号利用モード／メッセージ認証コードでの採用実績の高い上位３位までの暗号アルゴリズムを以下に示す。

表 4.4 暗号利用モード／メッセージ認証コードの結果

調査分類	詳細	第１位		第２位		第３位	
市販製品調査結果（調査Ｂ結果）	—	CBC	89.5%	HMAC	60.0%	GCM	52.4%
政府系情報システム・情報システム規格調査結果（調査Ｃ結果）	システム	CBC	68.1%	GCM	40.4%	HMAC	31.9%
	規格	CBC	100.0%	CFB	50.0%	—	—
標準規格・民間規格・特定団体規格調査結果（調査Ｄ結果）	国際的な民間規格	HMAC	63.6%	GCM	36.4%	CBC	27.3%
オープンソースソフトウェア調査結果（調査Ｅ結果）	—	HMAC	100.0%	CBC	93.1%	GCM	86.2%

（５）公開鍵暗号（署名）の結果

公開鍵暗号（署名）での採用実績の高い上位３位までの暗号アルゴリズムを以下に示す。

表 4.5 公開鍵暗号（署名）の結果

調査分類	詳細	第１位		第２位		第３位	
市販製品調査結果（調査Ｂ結果）	―	ECDSA	60.4%	RSASSA-PKCS1-V1_5	56.4%	DSA	38.6%
政府系情報システム・情報システム規格調査結果（調査Ｃ結果）	システム	RSASSA-PKCS1-V1_5	72.0%	ECDSA	42.0%	RSA-PSS	22.0%
	規格	DSA	100.0%	RSA-PSS	66.7%	ECDSA RSASSA-PKCS1-V1_5	33.3% 33.3%
標準規格・民間規格・特定団体規格調査結果（調査Ｄ結果）	国際的な民間規格	ECDSA	100.0%	RSA-PSS RSASSA-PKCS1-V1_5	33.3% 33.3%	―	―
オープンソースソフトウェア調査結果（調査Ｅ結果）	―	DSA	89.7%	ECDSA	82.8%	RSASSA-PKCS1-V1_5	65.5%

（６）公開鍵暗号（守秘・鍵共有）

公開鍵暗号（守秘・鍵共有）での採用実績の高い上位３位までの暗号アルゴリズムを以下に示す。

表 4.6 公開鍵暗号（守秘・鍵共有）の結果

調査分類	詳細	第１位		第２位		第３位	
市販製品調査結果（調査Ｂ結果）	―	ECDH	63.2%	DH	56.6%	RSAES-PKCS1-V1_5	42.1%
政府系情報システム・情報システム規格調査結果（調査Ｃ結果）	システム	RSAES-PKCS1-V1_5	61.5%	ECDH	50.0%	DH	30.8%
	規格	DH RSA-OAEP	50.0% 50.0%	―	―	―	―
標準規格・民間規格・特定団体規格調査結果（調査Ｄ結果）	国際的な民間規格	ECDH	80.0%	DH RSA-OAEP	20.0% 20.0%	―	―
オープンソースソフトウェア調査結果（調査Ｅ結果）	―	DH	100.0%	ECDH	96.0%	RSAES-PKCS1-V1_5	68.0%

（７）ハッシュ関数の結果

ハッシュ関数での採用実績の高い上位３位までの暗号アルゴリズムを以下に示

す。

表 4.7 ハッシュ関数の結果

調査分類	詳細	第１位		第２位		第３位	
市販製品調査結果（調査Ｂ結果）	―	SHA-256	92.2%	SHA-1	61.7%	SHA-384	48.7%
政府系情報システム・情報システム規格調査結果（調査Ｃ結果）	システム	SHA-256	97.4%	SHA-384	34.6%	SHA-1	24.4%
	規格	SHA-256	90.0%	SHA-1	80.0%	SHA-384 SHA-512	30.0% 30.0%
標準規格・民間規格・特定団体規格調査結果（調査Ｄ結果）	国際的な民間規格	SHA-256	94.4%	SHA-512	33.3%	SHA-384	27.8%
オープンソースソフトウェア調査結果（調査Ｅ結果）	―	SHA-256	96.7%	MD5	93.3%	SHA-1 SHA-512	86.7% 86.7%

5. 参考文献

［1］ IPA,「暗号アルゴリズムの利用実績に関する調査報告書」, 2012 年 12 月
https://www.ipa.go.jp/security/fy24/reports/cryptrec/crypto-algorithm/index.html

［2］ 情報通信研究機構(NICT), IPA,「CRYPTREC Report 2020」, 令和 3 年 3 月
https://www.cryptrec.go.jp/topics/cryptrec_20211012_c20report.html

6. 付録一覧

１．調査票（Ａ）
２．調査票（Ｂ）
３．調査票（Ｃ）
４．調査結果表（調査Ｂ）
５．調査結果表（調査Ｃ）政府系情報システム版
６．調査結果表（調査Ｃ）政府系規格版
７．調査結果表（調査Ｄ）
８．調査結果表（調査Ｅ）