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

２０１２年１２月

目 次

1. 調査業務の背景・目的

1.1 背景

CRYPTREC で実施している 2012 年度末の電子政府推奨暗号リスト[1] [5] の改訂（以下「次期リスト」という。）では、現在の「電子政府推奨暗号リスト」の単一リスト体系から、「電子政府推奨暗号リスト」「推奨候補暗号リスト」「運用監視暗号リスト」から構成される三リスト体系に移行する。

次期リスト掲載の対象となる暗号アルゴリズムは、政府等による調達等を容易にすることを目的として、「安全性」及び「実装性」の観点に加え、「製品化、利用実績等」の観点も踏まえて、いずれかのリストに分類・登録される。このため、次期リスト改訂にあたって、次期リスト掲載の対象となる暗号アルゴリズムの製品化、利用実績等についても明らかにする必要がある。[2] [3] [4] [6]

CRYPTREC 内の暗号運用委員会では、具体的に、次期リスト策定における暗号アルゴリズムに対する製品化・利用実績等の評価について評価手法の検討を行い、さらに、電子政府推奨暗号と国際標準技術との整合性も検討することとなっている。

1.2 目的

次期リスト掲載の対象となる暗号アルゴリズムの製品化・利用実績等の評価を担当する CRYPTREC 暗号運用委員会の指示のもと、次期リスト、特に次期電子政府推奨暗号リストに掲載する暗号アルゴリズムを選定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」について調査を行う。具体的には、次期リスト掲載の対象となっている暗号アルゴリズムを中心に、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化や規格化に採用されているか、について明らかにする。

1.3 実施作業内容

実施作業の概要図を以下に示す。

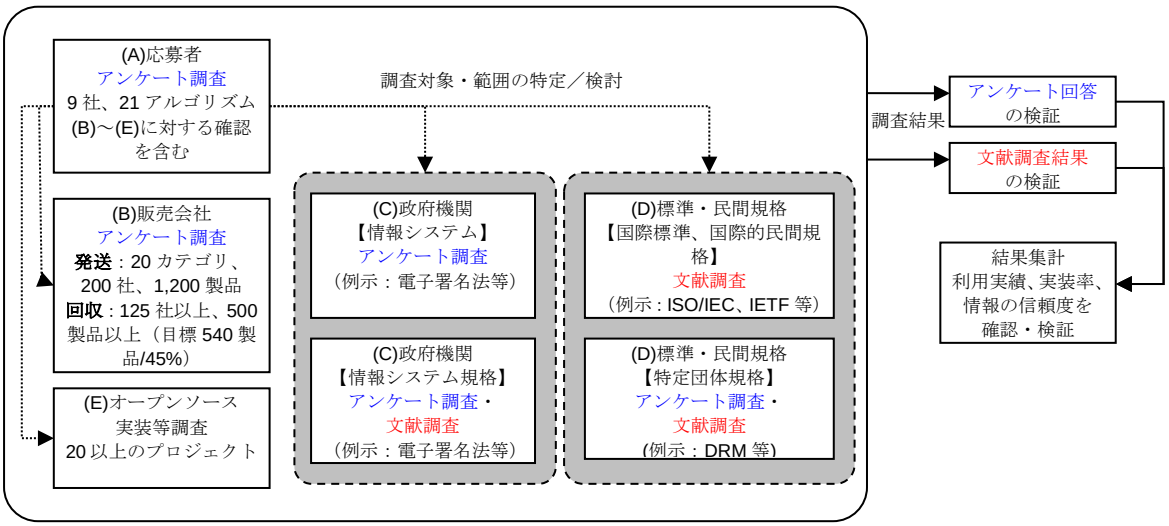

図 1 実施作業概要図

1.4　実施スケジュール

実施スケジュールを以下に示す。

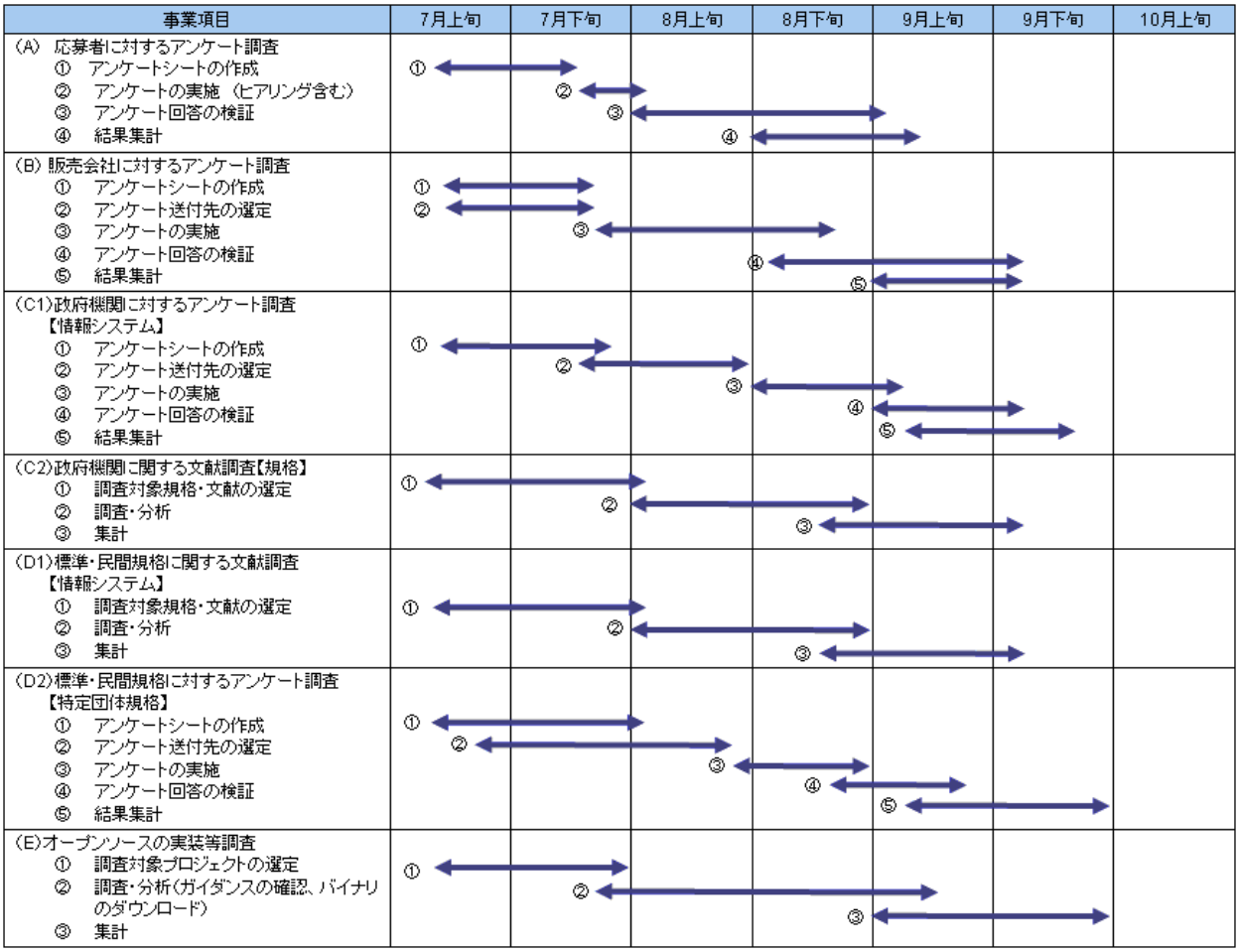

図 2 実施スケジュール概要図

2. 調査・集計方法

以下に各調査項目別の調査概要を示す。

2.1 応募者調査（調査 A）

2001 年度の CRYPTREC の公募に当該会社が応募し現在の電子政府推奨暗号リストに掲載されている暗号アルゴリズム（旧応募暗号）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（現応募暗号）（総計 21 個）の製品化、利用実績についての応募者に対してアンケート調査を実施し、情報収集調査を行った。以下に調査 A の概要を示す。

表 1 調査 A 概要

No,	項目	内容
1	調査期間	2012 年 7 月～9 月
2	調査方法	アンケート調査
3	調査対象	電子政府推奨暗号アルゴリズム応募者:9 社（詳細参照:表 2）
4	調査項目	1.電子政府推奨応募暗号アルゴリズム情報（詳細参照:表 3） 2.暗号アルゴリズムを利用した製品・システム情報（調査 B と共通、詳細参照:表 5）
5	集計方法	1. 電子政府推奨応募暗号アルゴリズム情報 ・ 政府系システム・規格の設問（表 3 内の設問 4）に関しては、調査 C の補足情報とし、調査 C の調査対象外の情報については『応募者情報』として集計 ・ 国際標準規格、国際的な民間規格及び特定団体規格の設問（表 3 内の設問 2、3、5）に関しては、調査 D の補足情報とし、調査 D の調査対象外の情報については『応募者情報』として集計 ・ オープンソースプロジェクトの設問（表 3 内の設問 7）に関しては、調査 E の補足情報として、調査 E の調査対象外の情報については『応募者情報』として集計 2. 暗号アルゴリズムを利用した製品・システム情報 ・ 応募者以外の製品・システムについては、調査 B のアンケート調査対象の追加 ・ 調査 B のアンケート調査対象の追加検討（製造・販売元及び、製品・システムの公開情報調査）の結果、提案暗号以外の暗号アルゴリズムの実装を確認・検証できなかった製品については、『応募者情報（製品）』として集計 ・ 提案暗号を実装したトライアル製品については、『応募者情報（トライアル）』として集計

2.1.1 アンケート調査

調査 A のアンケート調査項目の調査対象と対象アルゴリズム、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、付録 1.調査票(A)を参照。なお、調査 B と共通である暗号アルゴリズムを利用した製品・システムに関するアンケート調査の詳細については、2.2節を参照。

(1) アンケート調査対象（調査 A）

表 2 アンケート調査対象詳細(調査 A)

No,	企業名	対象アルゴリズム
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	EMC ジャパン株式会社	12) RSASSA-PKCS1-v1_5 13) RSAES-PKCS1-v1_5 14) RC4 15) RSA-PSS 16) RSA-OAEP
7	日本電信電話株式会社	17) Camellia 18) PSEC-KEM
8	株式会社東芝	19) Hierocrypt-L1 20) Hierocrypt-3
9	三菱電機株式会社	21) MISTY1

(2) アンケート調査項目（調査 A）

表 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 （上記、表 2 に記載の暗号アルゴリズムのいずれか）
2	採択されている国際標準規格 （ISO/IEC, ITU-T, ICAO の規格であり、調査 D の参考とした設問であるため、詳細は２．４．２(1)を参照）
3	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） （IETF, IEEE 等の規格であり、調査 D の参考とした設問であるため、詳細は２．４．２(2)を参照）
4	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 （電子署名法，公的個人認証，政府認証基盤（GPKI）等であり、調査 C の参考とした設問であるため、詳細は２．３．２(1)を参照）
5	暗号アルゴリズムを指定または推奨している特定団体規格 （Marline Joint Development Association 等であり、調査 D の参考とした設問）
6	上記 2、3、4、5 のいずれにも該当しない情報、もしくはどれに該当するかわからない情報で、本調査において有益だと思われる情報
7	暗号アルゴリズムが実装されているオープンソースプロジェクトについて （Linux, FreeeBSD, Debian 等であり、調査 E の参考とした設問であるため、詳細は２．５(1)を参照）
8	暗号アルゴリズムが実装されている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特注品・SI システム、④その他有益と考えられる情報

※すべて回答必須の設問ではなく、任意回答の設問とした。

2.2 市販製品調査（調査 B）

暗号製品についての市場調査報告書等において売上高調査に協力している企業や、暗号製品を販売している企業であってインターネットにて「企業情報」または「会社情報」を公開している企業などを対象に、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を調査し、表 6 に記載の暗号アルゴリズムごとの製品化、利用実績を明らかにする。

表 4 調査 B 概要

No,	項目	内容
1	調査期間	2012 年 7 月～9 月
2	調査方法	1. アンケート調査 2. 公開情報調査
3	調査対象	1.アンケート調査対象（アンケート配布社数:1,849、総数:2,444） ・ JNSA 会員企業 ・ その他の暗号を利用した製品・システムを情報公開している企業 2.公開情報調査対象（以下、情報源） ・ JISEC（IPA）による公開情報 ・ JCMVP（IPA）による公開情報 ・ CMVP（NIST）による公開情報
4	調査項目	1.アンケート調査 ・ 暗号アルゴリズムを利用した製品・システム情報の実態（詳細参照:表 5） 2.公開情報調査 ・ 暗号アルゴリズムを利用した製品・システム情報の実態（詳細参照:表 5 の項目 2, 3, 4, 8）
5	集計方法	1.アンケート調査については以下を確認し集計（回答有効回答社数 127: 総数:443） ・ 日本国内販売（アンケート調査により説明） ・ アンケート情報はすべて匿名化処理し集計（表 5 の設問 1） ・ 調査対象期間である 2010 年 6 月 30 日時点での発売/提供予定等を確認（表 5 の設問 3） ・ 重複した製品・システムについては、製造元または販売元のいずれかを集計（表 5 の設問 2、5） ・ 製品・システムが暗号アルゴリズム等を実装していることを明示的に読み取れる情報によって情報の信頼度別に集計（表 5 の設問 12、詳細参照:表 8） 2.公開情報調査（調査対象社数:35 総数:90） ・ 調査対象製品・システムの公開情報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 ※表 7 で示した製品カテゴリ全体を「市販製品総合」、製品カテゴリ 1, 2, 11, 12, 13 を合わせたものを「市販暗号モジュール」として集計

2.2.1 アンケート調査

以下に市販製品の詳細なアンケート調査の項目を示す。また、実際に使用した調査票は、付録 2.調査票（B）、付録 3.調査票（B）簡易版を参照。調査票（B）簡易版は、表 5 のオプション調査項目がないものである。

(1) アンケート調査項目（調査 B）

アンケート設問の構成は、本調査を行なううえで必須となる設問を必須項目、本調査において補足的に情報を収集する設問をオプション項目として設定し、アンケート調査の回収率を向上させるために、少なくとも必須項目の回答を得るようなアンケート設問を設定した。アンケート設問の概要を以下に示す。

表 5 アンケート調査項目概要（調査 B）

No	設問項目	必須 調査項目	オプション 調査項目
1	回答内容に関する情報非公表の指定	○	－
2	暗号アルゴリズムを組込んだ製品・システム等の名称	○	－
3	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）	○	－
4	暗号アルゴリズムを組込んだ製品・システム等の製品カテゴリ （詳細参照：表 7）	○	－
5	製品・システムに関する製造・販売及び OEM 等	○	－
6	製品・システムに組み込まれているオープンソースプロジェクトや、機能を提供するうえで必要となるまたはオプション等として利用しているその他の製品・システム（製品カテゴリについては詳細参照：表 7 と同様）	－	○
7	製品・システム等が実装している暗号アルゴリズム （詳細参照：表 6）	○	－
8	製品・システム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（詳細参照：表 9）	○	－
9	製品・システムが実装している擬似乱数生成器の仕様及び対応している規格（詳細参照：表 10）	○	－
10	製品・システムが利用している国際的な民間規格（プロトコル規格を含む）及び準拠している特定団体規格等	○	－
11	製品・システムが暗号アルゴリズム等を実装していることを明示的に読み取れる情報、また、その情報を入手可能な前提条件 （詳細参照：表 8）	○	－
12	製品・システム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	－	○
13	製品・システムの直近 1 年間の販売・出荷数の概算	－	○
14	製品・システム等で今後、組込みを検討及び計画している暗号アルゴリズム（詳細参照：表 6 と同様）	－	○

(2) 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、公開鍵暗号の守秘と鍵共有を一体として扱い、①公開鍵暗号（署名）、②公開鍵暗号（守秘・鍵共有）、③共通鍵暗号（64 ビットブロック暗号）、④共通鍵暗号（128 ビットブロック暗号）、⑤共通鍵暗号（ストリーム暗号）、⑥暗号利用モード、⑦ハッシュ関数、⑧メッセージ認証コードの8種類に分類し調査を実施した。詳細の暗号アルゴリズムを以下に示す。

表 6 アンケート調査項目（暗号アルゴリズム）

アルゴリズム名等		
共通鍵暗号	64ビットブロック暗号	Blowfish
		CAST-128
		CIPHERUNICORN-E
		DES
		GOST
		Hierocrypt-L1
		IDEA
		MISTY1
		Triple DES
	128ビットブロック暗号	AES
		ARIA
		Camellia
		CIPHERUNICORN-A
		CLEFIA
		Hierocrypt-3
		SC2000
		SEED
		Serpent
		SMS4
		Twofish
	ストリーム暗号	Enocoro-128v2
		KCipher-2
		MUGI
		MULTI-S01
		RC4
	その他	

アルゴリズム名等	
暗号利用モード	CBC
	CCM
	CFB
	CTR
	CTS
	GCM
	OFB
	XTS
	その他
メッセージ認証コード	CBC-MAC
	CMAC
	GMAC
	HMAC
	PC-MAC-AES
	その他

アルゴリズム名等		
公開鍵暗号	署名	DSA
		ECDSA
		KC-DSA
		RSA-PSS
		RSASSA-PKCS1-v1_5(RSA署名)
		SM2
	守秘・鍵共有	DH
		ECDH
		EC-MQV
		PSEC-KEM
		RSAES-PKCS1-v1_5(RSA暗号)
		RSA-KEM
		RSA-OAEP
	その他	
ハッシュ関数		HAS-160
		MD5
		RIPEMD-160
		SHA-1
		SHA-224
		SHA-256
		SHA-384
		SHA-512
		SM3
		Tiger
		その他

(3) アンケート調査項目（製品カテゴリ）

表 7アンケート調査項目（製品カテゴリ）

区分番号	カテゴリ	代表例（例示）
1	オペレーティングシステム	汎用 OS、携帯端末用 OS、VM
2	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
3	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：OS、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
4	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、ソフトウェア
5	サーバ	サーバ関連機器/ソフトウェア、電子認証局サーバ関連機器/ソフトウェア、ユーザ認証サーバ関連機器/ソフトウェア、タイムスタンプサーバ関連機器/ソフトウェア、（電子メール用）署名生成サーバ関連機器/ソフトウェア、業務支援ソフトウェア
6	ストレージ	ストレージ関連機器/ソフトウェア、データベースソフトウェア
7	端末	PC 本体（CPU/MPU）、周辺機器（ソフトウェアを除く）、PDA/スマートフォン/携帯電話、ハンディターミナル/POS/ATM/関連ソフトウェア
8	外部記憶装置	USB メモリ／SD メモリカード／ハードディスク／関連ソフトウェア
9	認証機器	認証デバイス関連機器
10	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
11	カード	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
12	IC チップ	汎用 IC、特定用途 IC（除外：IC カード、SIM カード、CPU、HSM、TPM、センサーチップ、消耗品認証用チップ等）、IC 組込用ソフトウェア
13	ハードウェアセキュリティモジュール	HSM、TPM
14	複合機・プリンタ	複合機／プリンタ関連機器／関連ソフトウェア
15	情報家電・生活用品	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／関連ソフトウェア、カーナビ／車載機器／関連ソフトウェア、ゲーム機
16	センサー	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）/関連ソフトウェア
17	消耗品認証	インクカートリッジ認証、消耗品認証、機器認証
18	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
19	特注品・SI システム	顧客仕様に基づいて製造され、納入された特注品、SI システム（一般へ販売はしていない）
20	その他	上記のいずれにも該当しないもの

(4) アンケート調査集計のレベル（調査 B）

表 8 アンケート調査集計のレベル(調査 B)

レベル	内容
Level.1 （以下 Lev.1）	公開情報等（URL 等）により回答内容が暗号アルゴリズムの利用・実装が確認できた情報
Level.2 （以下 Lev.2）	要求があれば、回答内容を検証できる情報を提供してもよいとの回答があった情報
Level.3 （以下 Lev.3）	NDA を締結すれば、回答内容を検証できる情報を提供してもよいとの回答があった情報
Level.4 （以下 Lev.4）	回答内容を検証できる情報はあるが、提供はできないとの回答があった情報
Level.5 （以下 Lev.5）	回答内容を検証できる情報があるかどうか判明しなかった情報

(5) アンケート調査項目（エンティティ認証の仕様）

表 9 アンケート調査項目（エンティティ認証の仕様）

エンティティ認証の仕様
1. ISO/IEC9798-2
2. ISO/IEC9798-3
3. ISO/IEC9798-4
4. その他

(6) アンケート調査項目（擬似乱数生成器の仕様）

表 10 アンケート調査項目（擬似乱数生成器の仕様）

擬似乱数生成器の仕様
1. PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1
2. PRNG based on SHA-1 for general purpose in FIPS 186-2(+ change notice 1) Appendix 3.1
3. PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1
4. ANSI X9.31 Appendix A.2.4 Using 3-Key Triple DES
5. ANSI X9.31 Appendix A.2.4 Using AES
6. Hash_DRBG, HMAC_DRBG and CTR_DRBG in NIST SP800-90
7. ISO/IEC18031
8. その他

2.3 政府系情報システム・情報システム規格調査（調査 C）

総務省及び経済産業省と協議して決定した、政府機関で利用する情報システムにおいて、どの暗号アルゴリズムが搭載されているかを調査し、表 6 に記載の暗号アルゴリズムごとの利用実績を明らかにする。また、法省令・ガイドライン・政府系システム規格（例：電子署名法、住民基本台帳法）において採用されている暗号アルゴリズムを調査する。また、文献調査対象先は、法省令・ガイドライン・政府系システム規格等の公開情報であって、暗号アルゴリズムの選択に関わるものとし、貴機構と相談の上、決定した。

表 11 調査 C 概要

No,	項目	内容
1	調査期間	2012 年 7 月～9 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・回収は経済産業省及び IPA が実施、匿名処理後の集計を調査者が実施） 2.公開情報調査
3	調査対象	1.アンケート調査対象 ・ 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 ・ 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 2.公開情報調査対象 ・ 貴機構と相談のうえ決定した公開されている各種の規格（CRYPTREC 暗号運用委員会委員会によって承認された規格を含む）（詳細参照：表 14）
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（詳細参照：表 12） ・ 政府系情報システム規格における暗号アルゴリズムの採用実績（詳細参照：表 13） 2.公開情報調査 ・ 調査対象規格における暗号アルゴリズムの採用実績（詳細参照：表 12 の項目 1）
5	集計方法	1.アンケート調査 ・ 政府系情報システム及び政府系規格のプロトコル規格（表 12、表 13 の設問 2）選択肢において TLS または IPSec を選択している場合は、利用している暗号アルゴリズムの選択肢と当該プロトコルの必須暗号アルゴリズムとの整合性を確認のうえ、集計（集計表では、Lev.A と表記） ○TLS の必須暗号アルゴリズム ・ RFC5246 から、RSAES-PKCS1-v1_5(RSA 暗号)、RSASSA-PKCS1-v1_5 (RSA 署名)、AES、CBC、SHA-1 ・ RFC2246 から、DH、DSA、Triple DES ○IPSec の必須暗号アルゴリズム ・ RFC4835（ESP、AH）及び RFC4307（IKE）から、Triple DES、AES、CBC、HMAC、DH、SHA-1 2.公開情報調査 ・ 調査対象規格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（集計表では、Lev.B と表記）

2.3.1 アンケート調査

政府系情報システム及び政府系情報システム規格に関するアンケート調査では、経済産業省及び IPA がアンケート送付と回収を行い、みずほ情報総研が集計を行なった。政府系情報システムの調査項目概要を表 12 に、政府系情報システム規格の調査項目概要を表 13 に示す。また、実際に使用した調査票は、付録 4.調査票（C）政府系システム版、付録 5.調査票（C）政府系システム規格版を参照。

(1) アンケート調査項目（調査 C：政府系情報システム）

表 12 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	必須 調査項	オプション 調査項目
1	システムで実装・利用している暗号アルゴリズム名	○	－
2	システムで実装・利用しているプロトコル規格等	○	－
3	システムで実装・利用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	○	－

(2) アンケート調査項目（調査 C：政府系情報システム規格）

表 13 アンケート調査項目概要（調査 C：政府系情報システム規格）

No,	設問	必須 調査項	オプション 調査項目
1	規格で推奨・参照している暗号アルゴリズム名	○	－
2	規格で推奨・参照しているプロトコル規格等	○	－
3	規格で推奨・参照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	○	－

2.3.2 公開情報調査

政府系規格に関する公開情報調査では、貴機構と相談のうえ決定した 7 規格（CRYPTREC 暗号運用委員会委員会によって承認された規格を含む）について調査を実施した。調査対象の規格を表 14 に示す。

(1) 公開情報調査対象（調査 C：政府系規格等）

表 14 公開情報調査（調査 C：政府系規格等）

No,	対象区分	規定（指針・ガイドライン等を含む）
1	電子署名法	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 http://www.meti.go.jp/policy/netsecurity/digitalsign-kokuzi-sisin.htm
2	公的個人認証	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 http://www.jpki.go.jp/jpkiguide/lawindex_pdf/jpki_guide_law6.pdf
3	商業登記認証局	「電子証明書の方式等に関する件（告示）」 http://www.moj.go.jp/content/000011343.pdf
4	医療情報システムの安全管理に関するガイドライン	医療情報システムの安全管理に関するガイドライン 第 4.1 版 http://www.mhlw.go.jp/shingi/2010/02/dl/s0202-4a.pdf
5	政府認証基盤（GPKI）	政府認証基盤（GPKI）政府認証基盤相互運用性仕様書 平成 13 年 4 月 25 日　平成 24 年 3 月 23 日改定 http://www.gpki.go.jp/session/CompatibilitySpecifications.pdf
6	住民基本台帳法（昭和 42 年法律第 81 号）	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 http://www.ipa.go.jp/security/jisec/certified_pps/c0284/c0284_pp.pdf
7	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	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　総務省告示第三百二号 http://www.tele.soumu.go.jp/horei/reiki_honbun/a72ab21451.html

2.4 標準規格・民間規格・特定団体規格調査（調査 D）

国際標準規格（例：ISO/IEC, ITU-T, ICAO）、国際的な民間規格（例：IETF, IEEE 等）、並びに特定団体規格（例：DRM, Bluetooth, ZigBee, Wi-Fi 等）において採用されている暗号アルゴリズムを調査する。

貴機構と相談の上、以下の条件をすべて満たす規格を選定した。

- 国際標準規格（ISO/IEC, ITU-T, ICAO）：3 機関が策定した標準化のうち、暗号アルゴリズムに関する規格について、合計で 10 個以上の規格番号（例：ISO/IEC9796, ISO/IEC18033）を対象とした。
- 国際的な民間規格（例：IETF, IEEE 等）：インターネット、電子機器、金融、携帯電話等で国際的に利用される規格を策定している団体であって、かつ当該団体が策定している暗号アルゴリズムに関する規格が公開されているものについて、合計で 10 個以上のプロトコルまたはシステム（例：TLS, IPsec）に関する規格を対象とした。
- 特定団体規格（例：DRM, Bluetooth, ZigBee, Wi-Fi 等）：日常生活において使われているサービスやシステムで利用される規格を策定している団体・コンソーシアムであって、かつ当該サービスやシステムで暗号アルゴリズムが採用されているものについて、15 団体・コンソーシアム以上を対象とした。原則として、日本に本部、支部、もしくは問い合わせ窓口がある団体・コンソーシアムを対象とする。（但し、対象はアンケート送付先である。）

表 15 調査 D 概要

No,	項目	内容
1	調査期間	2012 年 7 月～9 月
2	調査方法	1.アンケート調査 2.公開情報調査
3	調査対象	1.アンケート調査対象（アンケート発送数：16 団体） ・ 特定団体規格（例：DRM、放送・通信、情報通信基盤（時刻情報）等） 但し、日本に本部、支部、もしくは問い合わせ窓口がある団体・コンソーシアムを対象とする。 2.公開情報調査対象 ・ 国際標準規格（ISO/IEC、ITU-T、ICAO、詳細参照：表 17） ・ 国際的な民間規格（例：IETF、IEEE 等、詳細参照：表 18） ・ 特定団体規格（例：DRM、Bluetooth、ZigBee、Wi-Fi 等、詳細参照：表 19）
4	調査項目	1.アンケート調査対象 ・ 特定団体規格（DRM、放送・通信、情報通信基盤（時刻情報）等）における暗号アルゴリズムの採用実績 2.公開情報調査対象 ・ 国際標準規格（ISO/IEC、ITU-T、ICAO）における暗号アルゴリズムの採用実績 ・ 国際的な民間規格（IETF、IEEE 等）における暗号アルゴリズムの採用実績 ・ 特定団体規格（例：DRM、Bluetooth、ZigBee、Wi-Fi 等）における暗号アルゴリズムの採用実績
5	集計方法	1.アンケート調査 ・ 製品・システムが暗号アルゴリズム等を実装していることを明示的に読み取れる情報によって情報の信頼度別に集計（詳細参照：表 8） 2.公開情報調査 ・ 調査対象規格の公開情報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 ・ 原則として最新版のみを調査対象にする ・ 国際標準規格 ➢ 規格番号単位で規格数をカウント（枝番は考慮しない） ・ 国際的民間規格 ➢ 同一種類に対する複数規格は規格数でカウント ただし、TLS に関しては、現状の利用環境を鑑み、廃止された RFC2246 を追加 ➢ プロトコルに関連する規格のみ対象 ➢ Additional RFC は、メインプロトコルを調査した規格のみ対象

No,	項目	内容
		・特定団体規格 ➢ 同一団体による複数規格は規格数でカウントを実施

2.4.1 アンケート調査

調査Ｄ概要に示した内容に基づき、16団体・コンソーシアムにアンケートを送付した。アンケート調査項目の概要を表 16 に示す。回答を拒否された対象については、その後の調査を中止する。また、実際に使用した調査票は、付録 6.調査票(D)を参照。

(1) アンケート調査（調査 D：特定団体規格等）

表 16 アンケート調査項目概要（調査 D：特定団体規格）

No	設問項目	必須 調査項目	オプション 調査項目
1	暗号アルゴリズムを記載している規格・ガイドラインの名称	○	－
2	規格で推奨・参照している暗号アルゴリズム名	○	－
3	製品・システムが暗号アルゴリズム等を実装していることを明示的に読み取れる情報、また、その情報を入手可能な前提条件 （詳細参照：表 8）	○	－
4	規格で推奨・参照している国際標準規格、国際的な民間規格等	○	－
5	製品・システムに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	○	－
6	製品・システムに実装している擬似乱数生成器の仕様及び対応している規格	－	○

2.4.2 公開情報調査

調査Ｄ概要に示した内容に基づき、国際標準規格及び国際的な民間規格、特定団体規格の公開情報について調査を実施した。調査対象の国際標準規格を表 17 に、国際的な民間規格を表 18 に、特定団体規格を表 19 に示す。

(1) 公開情報調査対象（調査 D：国際標準規格等）

表 17 公開情報調査（調査 D：国際標準規格等）

No,	識別	名称	詳細(バージョン等)
1	ISO/IEC9796	Digital signature schemes giving message recovery	2:2010, 3:2006
2	ISO/IEC9797	Message Authentication Codes (MACs)	1:2011, 2:2011, 3:2011
3	ISO/IEC10116	Modes of operation for an n-bit block cipher	2006, Cor 1:2008
4	ISO/IEC10118	Hash-functions	1:2000, 2:2010, 2:Cor 1:2011, 3:2004, 3:Amd 1:2006, 3:Cor 1:2011, 4:1998
5	ISO/IEC14888	Digital signatures with appendix	1:2008, 2:2008, 3:2006, 3:Amd 1:2010, 3:Cor 1:2007, 3:Cor 2:2009, 3:Amd 2:2012

No,	識別	名称	詳細（バージョン等）
6	ISO/IEC18033	Encryption algorithms	1:2005, 1:Amd 1:2011, 2:2006, 3:2010, 4:2011
7	ISO/IEC19772	Authenticated encryption	2009
8	ISO/IEC29192	Lightweight cryptography	1:2012, 2:2012, 3, 4
9	ISO/IEC7816	Identification cards — Integrated circuit cards —	1:2011, 2:2007, 3:2006, DIS 4:2005, 4:Amd 1:2008, 5:2004, 6:2004, 6:Cor 1:2006, 7:1999, 8:2004, 9:2004, 10:1999, 11:2004, 12:2005, 13:2007, 13:CD Cor 1, 15:2004, 15:Amd 1:2007, 15:Cor 1:2004, 15:Amd 2:2008
10	ITU-TY.2704	Security mechanisms and procedures for NGN	01/2010
11	ITU-TH.233/ ITU-TH.234	Confidentiality system for audiovisual services, Encryption key management and authentication system for audiovisual services	11/2002, 11/2002
12	ICAODoc9303	Machine Readable Travel Documents	Part 1Machine Readable Passports Volume 1Sixth Edition - 2006, Part 1Machine Readable Passports Volume 2Sixth Edition - 2006, Part 2 Machine Readable VisasThird Edition - 2005, Part 3 Machine Readable Official Travel Documents Volume 1Third Edition - 2008, Part 3 Machine Readable Official Travel Documents Volume 2Third Edition - 2008

(2) 公開情報調査対象（調査 D：国際的民間規格等）

表 18 公開情報調査（調査 D：国際的民間規格等）

No,	名称	調査文献一覧	調査数
1	IETF TLS	RFC2246, RFC2712, RFC4162, RFC4492, RFC4785, RFC5246, RFC5288, RFC5289, RFC5469, RFC5487, RFC5489, RFC5932, RFC4680, RFC4681, RFC5746, RFC5878, RFC6066, RFC6176, RFC6460, RFC6367	20
2	IETF IPsec	RFC2403, RFC2405, RFC2410, RFC2451, RFC2857, RFC3526, RFC3566, RFC3602, RFC3686, RFC3948, RFC4106, RFC4196, RFC4301, RFC4302, RFC4303, RFC4307, RFC4308, RFC4309, RFC4312, RFC4478, RFC4494, RFC4543, RFC4615, RFC4621, RFC4806, RFC4809, RFC4835, RFC4868, RFC5282, RFC5529, RFC5996, RFC5998, RFC6040, RFC6379	34
3	IETF S/MIME CMS	RFC2311, RFC2312, RFC3565, RFC3657, RFC3853, RFC4056, RFC5083, RFC5652, RFC5750, RFC5751, RFC5752, RFC5753, RFC5754, RFC5990, RFC3560	15
4	IETF PGP	RFC3156, RFC4880, RFC5581	3
5	IEEE802.11i	IEEE 802.11i-2004: Amendment 6: Medium Access Control (MAC) Security Enhancements	1
6	RSA PKCS#11	PKCS #11 Mechanisms v2.30: Cryptoki – Draft 7 29 July 2009 RSA Laboratories	1
7	EMV	EMV 4.3 Book 1 - Application Independent ICC to Terminal Interface Requirements November 2011 Vsersion 4.3 EMV 4.3 Book 2 -Security and Key Management Version 4.3 November 2011	2
8	3GPP	TS 33.105 3G Security; Cryptographic algorithm requirements Vers10.0.0. TS 35.202 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms;Document 2:	2
9	3GPP2	TSG-S S.S0053-0 v2.0 Common Cryptographic Algorithms 2009/05 TSG-S S.S0054-0 v1.0 Interface Specification for Common Cryptographic	3

No,	名称	調査文献一覧	調査数
		Algorithms 2002/01 TSG-S S.S0055-A v4.0 Enhanced Cryptographic Algorithms 2008/01	
10	OMA	DRM Specification V2.0 Candidate Version 2.0 – 10 December 2004	1
11	IETF DNSSec	RFC3110, RFC4033, RFC4034, RFC4035, RFC4431, RFC4470, RFC4509, RFC5074, RFC5702, RFC6014	10
12	IETF Kerberos	RFC3962, RFC4120, RFC4537, RFC5021, RFC5896, RFC6111, RFC6112, RFC6113, RFC6649	9
13	IEEE1619	IEEE Std 1619-2007 IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices	1
14	Trusted Computing Group	Trusted Computing Group TPM Main Specification Version 1.2 Revision 116 -Part 1 Design Principles, -Part 1 Design Principles, -Part 2 TPM Structures, -Part 3 Commands	3
15	その他	RFC6272, RFC4055	2

(3) 公開情報調査対象（調査 D：特定団体規格等）

表 19 調査対象（調査 D：特定団体規格等）

No,	団体名	詳細
1	ZigBee SIG-Japan	ZigBee 和訳仕様書 （ZigBee Specification Document 053474r17 January 17, 2008） http://www.zbsigj.org/download/085224r00ZB_MG-ZigBee-Specification-053474r17_Japanese_08120.pdf
2	Bluetooth SIG, Inc	Bluetooth 仕様書 （BLUETOOTH SPECIFICATION Version 4.0 [Vol 0]） http://www.bluetooth.org/Technical/Specifications/adopted.htm
3	Wi-Fi Alliance	WiFi 仕様書 （Wi-Fi Simple Configuration Technical Specification Version 2.0.2） https://www.wi-fi.org/knowledge-center/published-specifications
4	IPTV フォーラム	デジタルテレビ ネットワーク(デジタルテレビ情報化研究会/ IPTV Forum Japan) IPTVFJ STD-0001～0009 https://www.iptvforum.jp/standard/about.html
5	Digital Cinema Initiatives, LLC	デジタルシネマシステム仕様 第 1 版 2005 年 7 月 20 日 Digital Cinema System Specification Version 1.2 March 07, 2008 http://www.dcimovies.com/specification/
6	AACS（Advanced Access Content System）	AACS 仕様書 1）Elements Book 2）Blu-ray Disc 3）HD DVD and DVD） http://www.aacsla.com/specifications/

2.5 オープンソースプロジェクト調査（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, Mozilla, Linux, Android）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 20 に示す。

表 20 調査 E 概要

No,	項目	内容
1	調査期間	2012 年 7 月～9 月
2	調査方法	公開情報調査
3	調査対象	貴機構に指定されたオープンソースプロジェクト（CRYPTREC 暗号運用委員会委員会によって指定されたオープンソースプロジェクトを含む）（詳細参照：表 21）
4	調査方法	・ 最新安定バージョンの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 ・ 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	・ 調査対象オープンソースプロジェクト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 ・ Linux 及び Debian は、両方に実装されている場合でも 1 と集計（表 21 の青色） ・ Thunderbird、Firefox、及び NSS は、それらのうちの複数に実装されている場合でも 1 と集計（表 21 の黄色） ・ Qmail 及び OpenSSL は、両方に実装されている場合でも 1 と集計（表 21 の赤色） ・ 応募者からの情報があっても、本調査で調査者が確認できなかったものは当該ソースコードについて対象外とする ・ 重複集計を避けるため、他オープンソースプロジェクト管理のソースコードが組み込まれていた場合、当該ソースコードについては対象外とする ➢ 例えば、Android では、以下のメイン(/libcore/luni/src/main/)ではない、external 直下のフォルダに Camellia が存在するが、Android については Camellia が搭載されているとは認めない。 「/external/bouncycastle/, /external/ipsec-tools/, /external/openssl/crypto/evp/」 ・ 搭載検討中になっているソースコードは対象外とする ・ エンティティ認証は、ISO/IEC9798 等の明示がないため、対象外とする ・ オープンソースプロジェクト全体を「OSS 総合」、Linux, Debian, FreeBSD, Android, NSS, OpenSSL, GnuPG, Mcrypt を「OSS 暗号モジュール」として集計

(1) 公開情報調査対象（調査 E：オープンソースプロジェクト）

オープンソースプロジェクトの調査対象は、貴機構に指定されたオープンソースプロジェクト（CRYPTREC 暗号運用委員会委員会によって指定されたオープンソースプロジェクトを含む）とし、調査時点で最新安定バージョンを特定し、調査を実施した。表 21 に調査対象のオープンソースプロジェクト及びバージョンを示す。

表 21 公開情報調査（調査 E：オープンソースプロジェクト）

	ツール名	バージョン
1	Linux	3.4.7
2	Debian	6.0.5
3	FreeeBSD	9
4	Android	4
5	Java	SE 7
6	Bouncy Castle	(jdk15-17)1.47
7	PHP	5.4.5
8	Subversion	1.7.6
9	Eclipse	4.2

	ツール名	バージョン
10	Samba	3.6.6
11	Tomcat	7.0.29
12	Apache	2.4.2 (released 2012-04-17)
13	Webkit	r125966
14	Thunderbird	14
15	Firefox	14.0.1
16	NSS	3.13.5
17	Qmail	1.06
18	OpenSSL	1.0.1c
19	GnuPG	20 (2.0.19)
20	Mcrypt	2.6.8
21	MySQL	5.5.25a
22	PostgreSQL	9.1.4
23	OpenOffice	3.4.0
24	7-zip	9.2

3. 調査結果

応募者情報調査結果を3.1節に、市販製品調査結果を3.2節に、政府系利用実績調査結果を3.3節に、標準規格等調査結果を3.4節に、オープンソースプロジェクト調査結果3.5節に報告する。

3.1 応募者情報調査結果（調査 A 結果）

応募者情報調査では、応募者 9 社に対して、調査対象暗号アルゴリズム数 21 についてアンケート調査を実施した。アンケート調査としては、①対象暗号アルゴリズムの利用実績、②対象暗号アルゴリズムを利用した製品情報を確認した。①対象暗号アルゴリズムの利用実績としては、RSASSA-PKCS1-v1_5、RSAES-PKCS1-v1_5、RC4 以外の回答を得た。また、②対象暗号アルゴリズムを利用した製品情報については、各社のグループ企業及び関連企業を含め情報を得たものについては、市販製品調査（調査 B）に含めて集計を行った。結果概要を表 22 に示す。

表 22 応募者情報調査（調査 A）結果概要

企業名	対象アルゴリズム	対象アルゴリズムの利用実績	製品情報	応募者の参考情報(※)			
				製品	トライアル	規格	OSS
ソニー株式会社	1) CLEFIA	○	○	0	0	1	0
株式会社日立製作所	2) Enocoro-128v2	○	○	0	0	0	0
	3) MUGI	○	○	0	0	0	0
	4) MULTI-S01	○	○	0	0	0	0
KDDI 株式会社	5) KCipher-2	○	○	2	3	0	0
日本電気株式会社	6) CIPHERUNICORN-E	○	○	0	0	0	0
	7) CIPHERUNICORN-A	○	○	0	0	0	0
富士通株式会社	8) ECDSA	○	○	0	0	0	1
	9) ECDH	○	○	0	0	0	1
	10) SC2000	○	○	0	0	0	0
EMC ジャパン株式会社	12) RSASSA-PKCS1-v1_5	×	○	0	0	0	0
	13) RSAES-PKCS1-v1_5	×	○	0	0	0	0
	14) RC4	×	○	0	0	0	0
	15) RSA-PSS	○	○	1	0	1	0
	16) RSA-OAEP	○	○	3	0	3	0
日本電信電話株式会社	17) Camellia	○	○	14	0	6	21
	18) PSEC-KEM	○	○	1	0	1	0
株式会社東芝	19) Hierocrypt-L1	○	○	0	0	0	0
	20) Hierocrypt-3	○	○	0	0	0	0
三菱電機株式会社	21) MISTY1	○	○	0	0	1	0

※応募者から提供された製品、トライアル（製品）、規格、OSS の情報の中で、調査対象外、一般に公開されていない、内容を確認できない、該当暗号アルゴリズムの名称が明示的に読み取れないものの合計数を示す。なお、これらの値は参考情報であり、各調査（調査 B、C、D、E）の集計結果には含まれない。

上記の応募者情報調査の結果、調査対象外の規格及び一般に公開されていない規格等、規定内容を確認できない情報、または規格に該当暗号アルゴリズムの名称が明示的に読み取れなかった規格（上記表内「応募者の参考情報：規格」）の規格名称等を以下に報告する。

表 23 応募者情報調査（調査 A)結果概要

暗号アルゴリズム名	応募者情報（詳細規格名・団体名）
MISTY1	国内で広く使われている非公開規格
Camellia	-TV-Anytime Forum: TV-Anytime Rights Management and Protection Information for Broadcast Applications, IETF: RFC3713, IETF: RFC5528, IETF: RFC4051, IETF: RFC6030, ISDB-Tmm
CLEFIA	IETF: RFC6114
RSA-PSS	IEEE1363A
PSEC-KEM	IETF: RFC4051
RSA-OAEP	IEEE1363, W3C XML Encryption Syntax and Processing, SET（Secure Electronic Transaction）

3.2　市販製品調査結果（調査 B 結果）

市販製品調査では、1,849 社にアンケートを配布し、127 社から 443 製品・システムの有効回答数を得た。また、35 社、90 製品の公開情報調査を実施し、合計 156 社、533 製品・システムに関する暗号アルゴリズムの利用状況を調査した。以下に、各製品カテゴリの集計結果を報告する。下図では、回答情報の検証可能性を考慮した信頼度ごとに、Lev1 から Lev5 までを分け、各レベルにおける 20 種類の製品カテゴリの回答数を Lev1～Lev3（図中、上段）、Lev1～Lev4（図中、中段）、Lev1～Lev5（図中、下段）に記している。

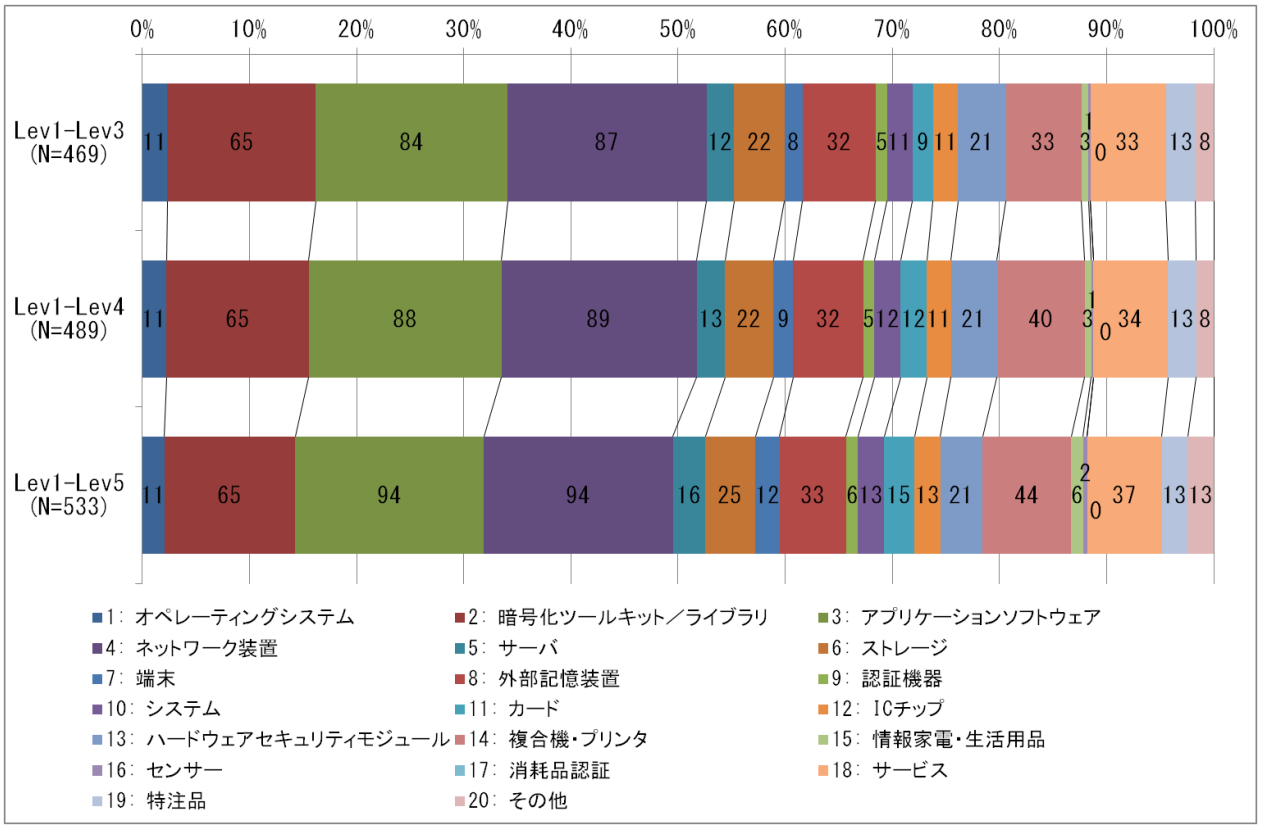

図 3 市販製品調査（調査 B）結果概要図

製品カテゴリ全体を「市販製品総合」とし、その集計結果を3.2.1に、製品カテゴリ 1, 2, 11, 12, 13 を合わせたものを「市販暗号モジュール」とし、その集計結果を3.2.2に報告する。また、アンケートのオプション設問の集計結果を3.2.3に報告する。なお、各暗号アルゴリズム、各製品カテゴリの実数は、付録 7.調査結果表（B）を参照。調査結果表(B)には、調査 A で対象となっている暗号アルゴリズムを開発した企業以外で、同暗号アルゴリズムの利用企業を示す「他社利用」の項目を設けており、応募者・グループ会社[1]・関係会社[2]以外の利用の有無を「○」「×」で表記をしている。

1 応募者と同じ社名・略称が含まれている企業はグループ会社とみなす。

2 資本関係等、応募者と関係があると広く知られている企業は関係会社とみなす。

3.2.1 市販製品総合

市販製品総合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通りである。

凡例

- 『公開鍵暗号(署名)』等の該当総数をＮ値とし、アンケート回答総数にＮ値が占める割合を記載。
- 例)アンケート回答総数:100、公開鍵暗号(署名)のいずれかを選択した回答数(該当総数):10
- 例示の場合の表記:凡例(N=10, 10%)

各暗号アルゴリズムのデータ値

- 該当総数に該当暗号アルゴリズムが占める割合を記載。
- 例)上記の例示で暗号アルゴリズムＡを選択した回答数:5
- 例示の場合の暗号アルゴリズムＡの表記:50%

(1) 市販製品・総合（公開鍵暗号（署名））

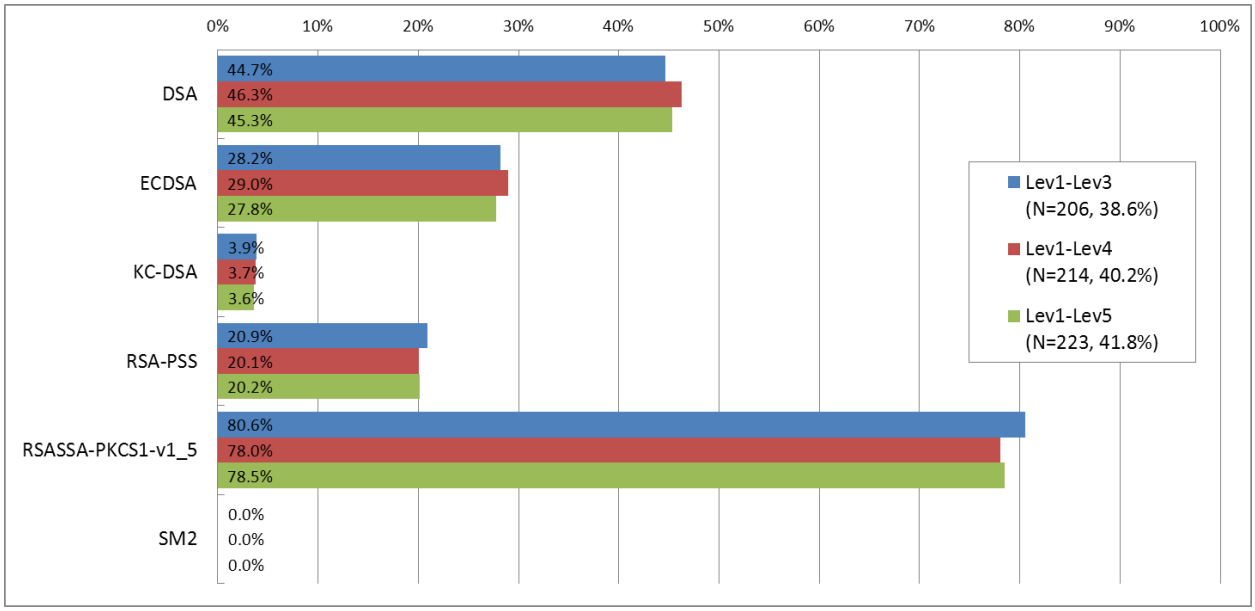

図 4 市販製品・総合（公開鍵暗号（署名））

(2) 市販製品・総合（公開鍵暗号（守秘・鍵共有））

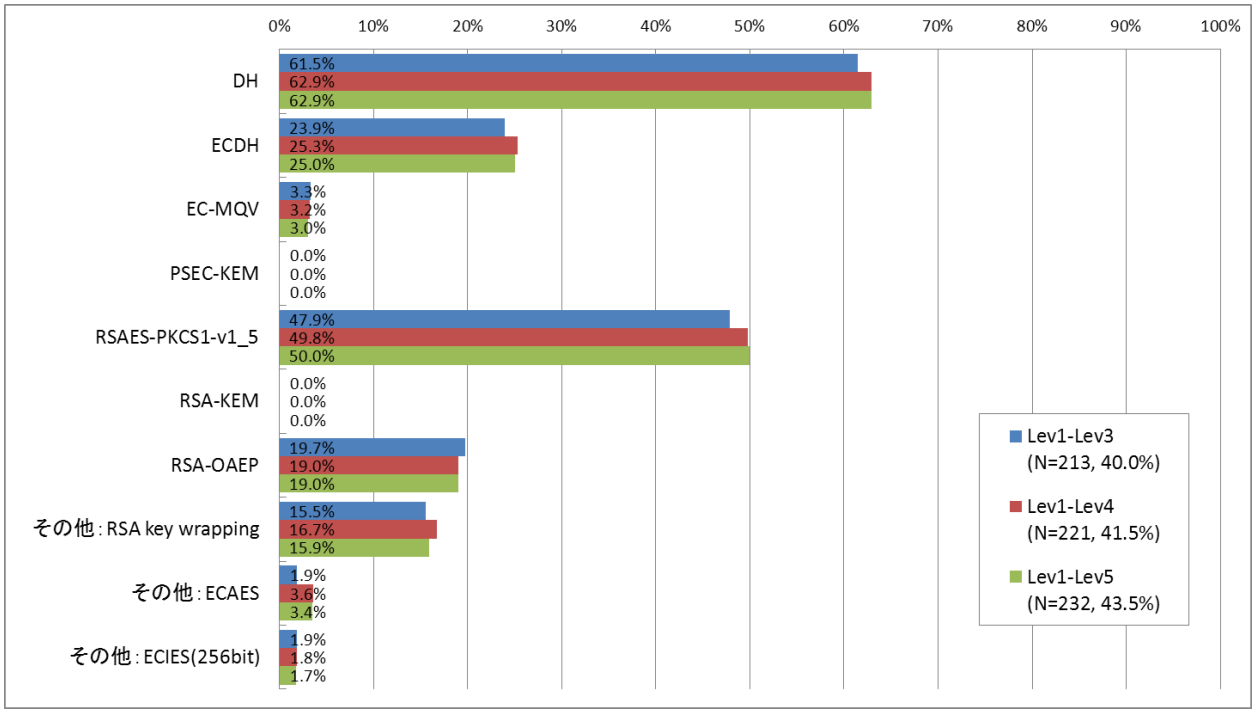

図 5 市販製品・総合（公開鍵暗号（守秘・鍵共有））

(3) 市販製品・総合（共通鍵暗号（64 ビットブロック暗号））

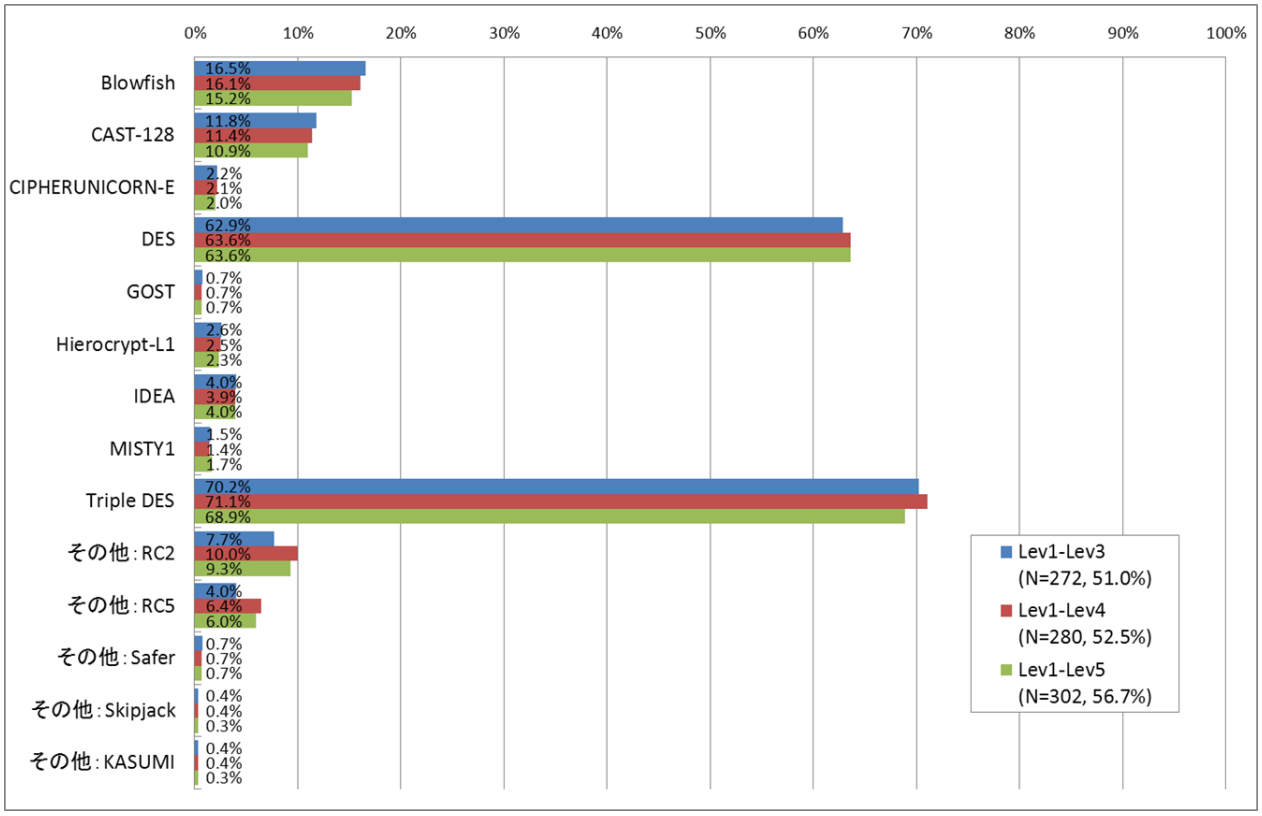

図 6 市販製品・総合（共通鍵暗号（64 ビットブロック暗号））

(4) 市販製品・総合（共通鍵暗号（128 ビットブロック暗号））

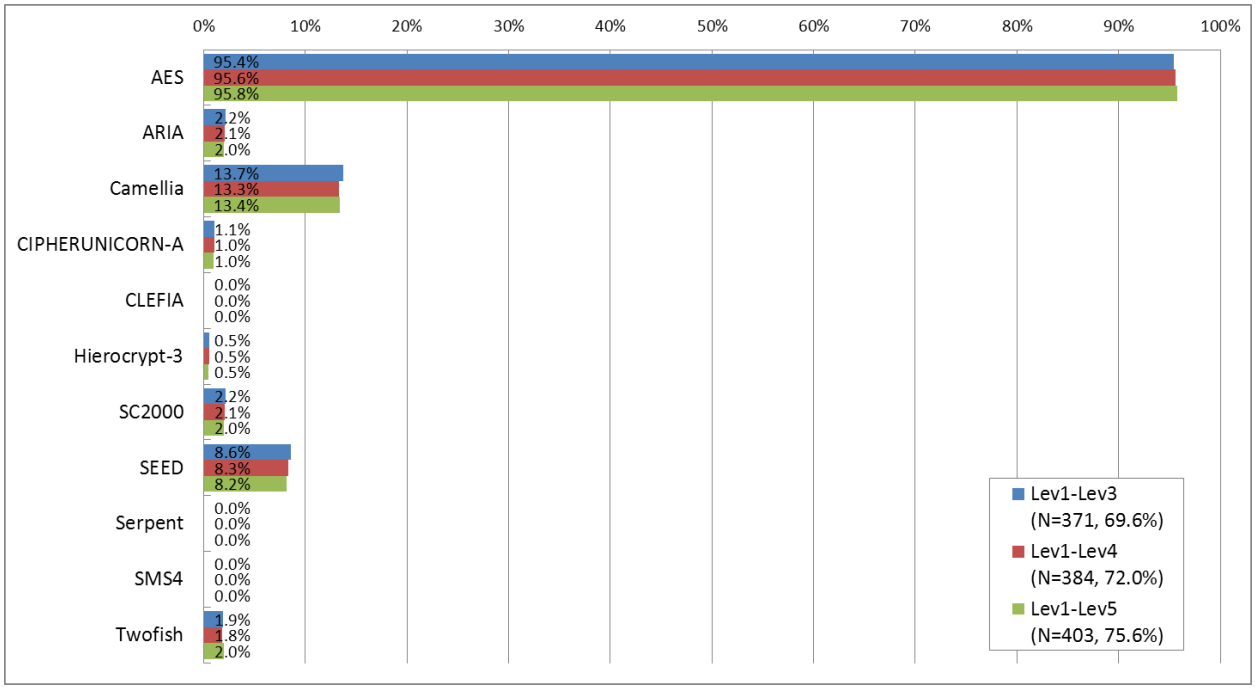

図 7 市販製品・総合（共通鍵暗号（128 ビットブロック暗号））

(5) 市販製品・総合（共通鍵暗号（ストリーム暗号））

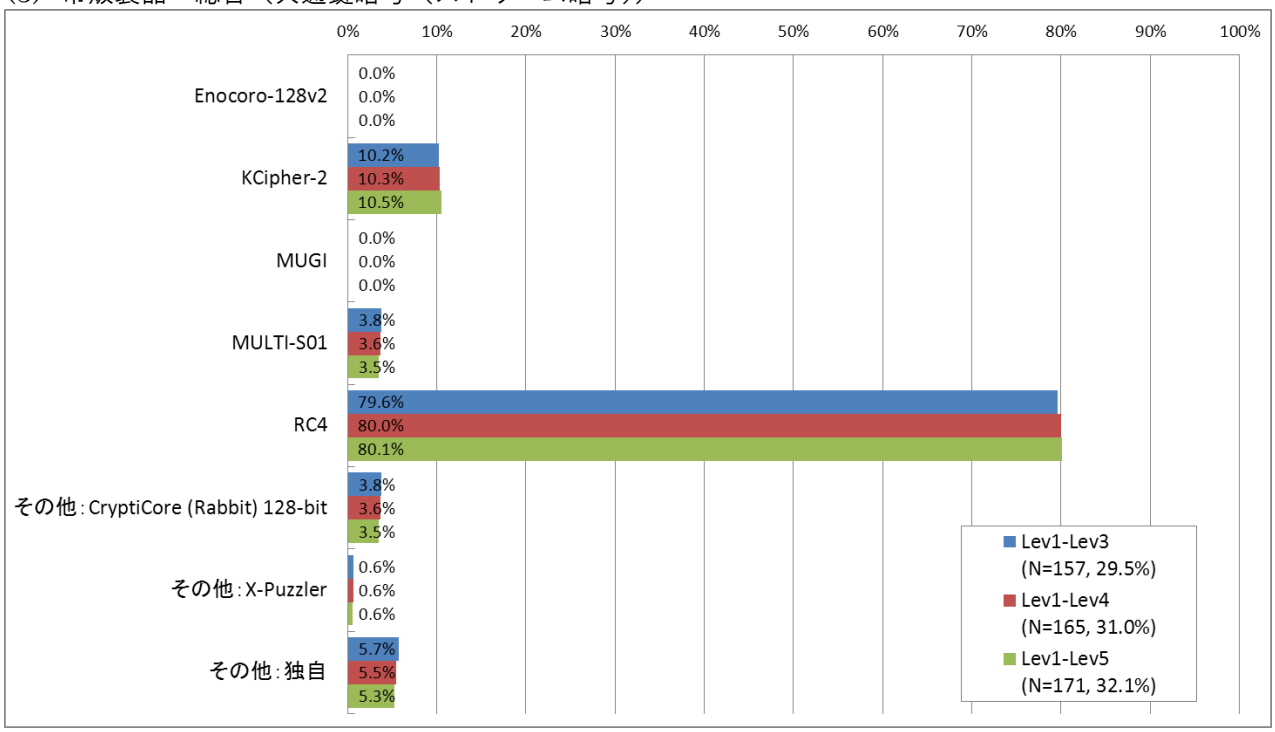

図 8 市販製品・総合（共通鍵暗号（ストリーム暗号））

(6) 市販製品・総合（ハッシュ関数）

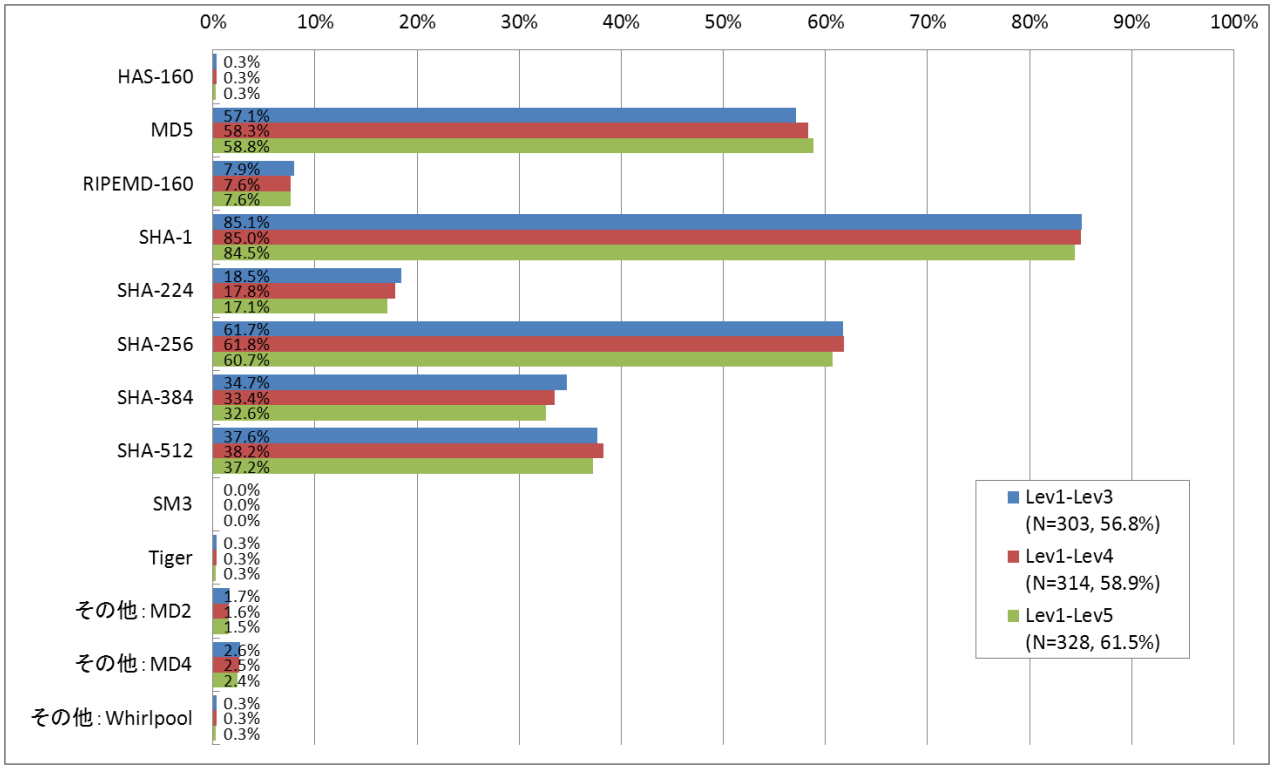

図 9 市販製品・総合（ハッシュ関数）

(7) 市販製品・総合（暗号利用モード）

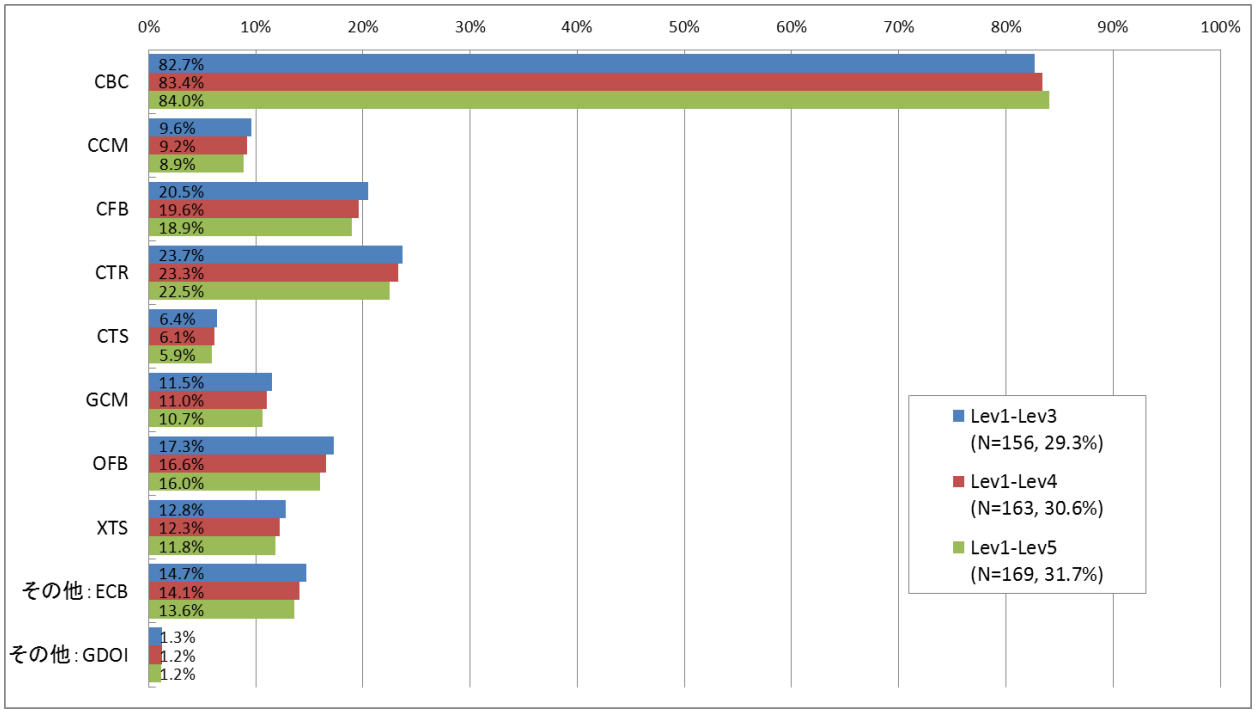

図 10 市販製品・総合（暗号利用モード）

(8) 市販製品・総合（メッセージ認証コード）

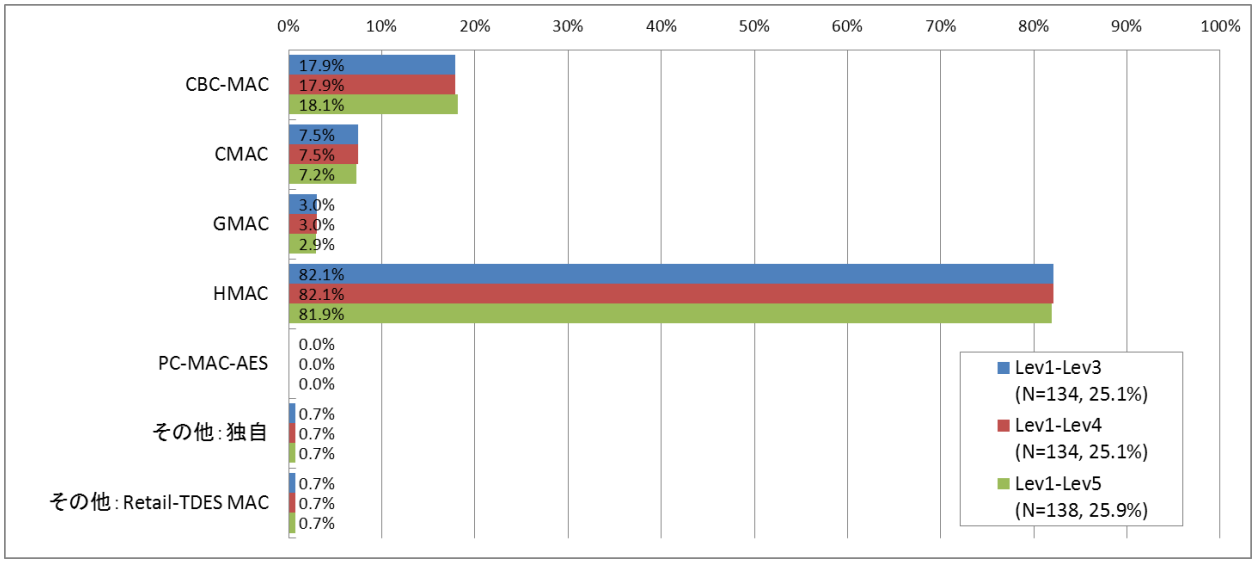

図 11 市販製品・総合（メッセージ認証コード）

(9) 市販製品・総合（エンティティ認証）

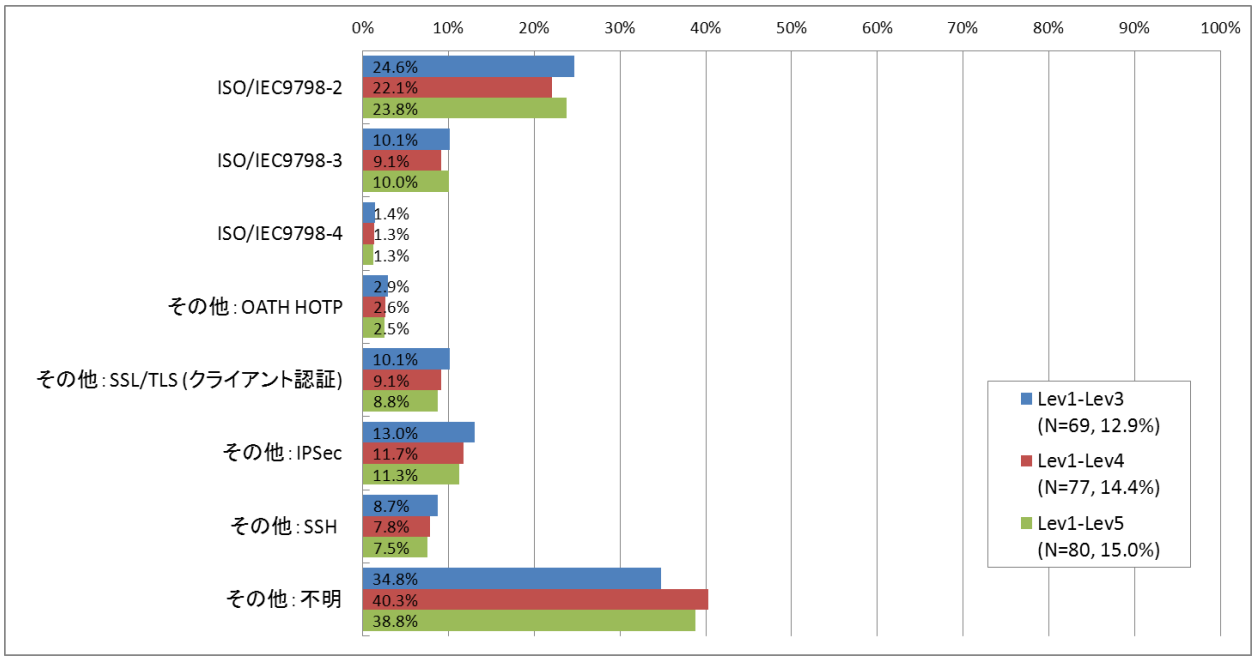

図 12 市販製品・総合（エンティティ認証）

(10)　市販製品・総合（擬似乱数生成器）

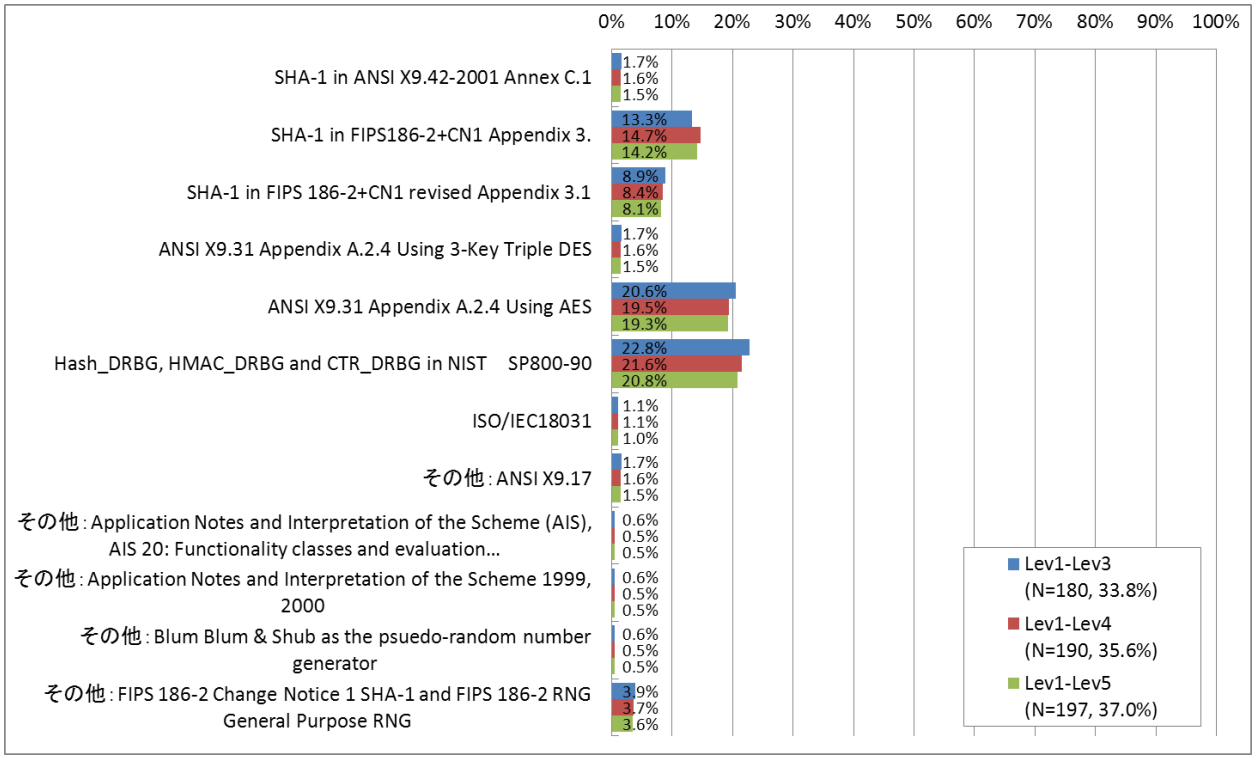

図 13 市販製品･総合(擬似乱数生成器(1))

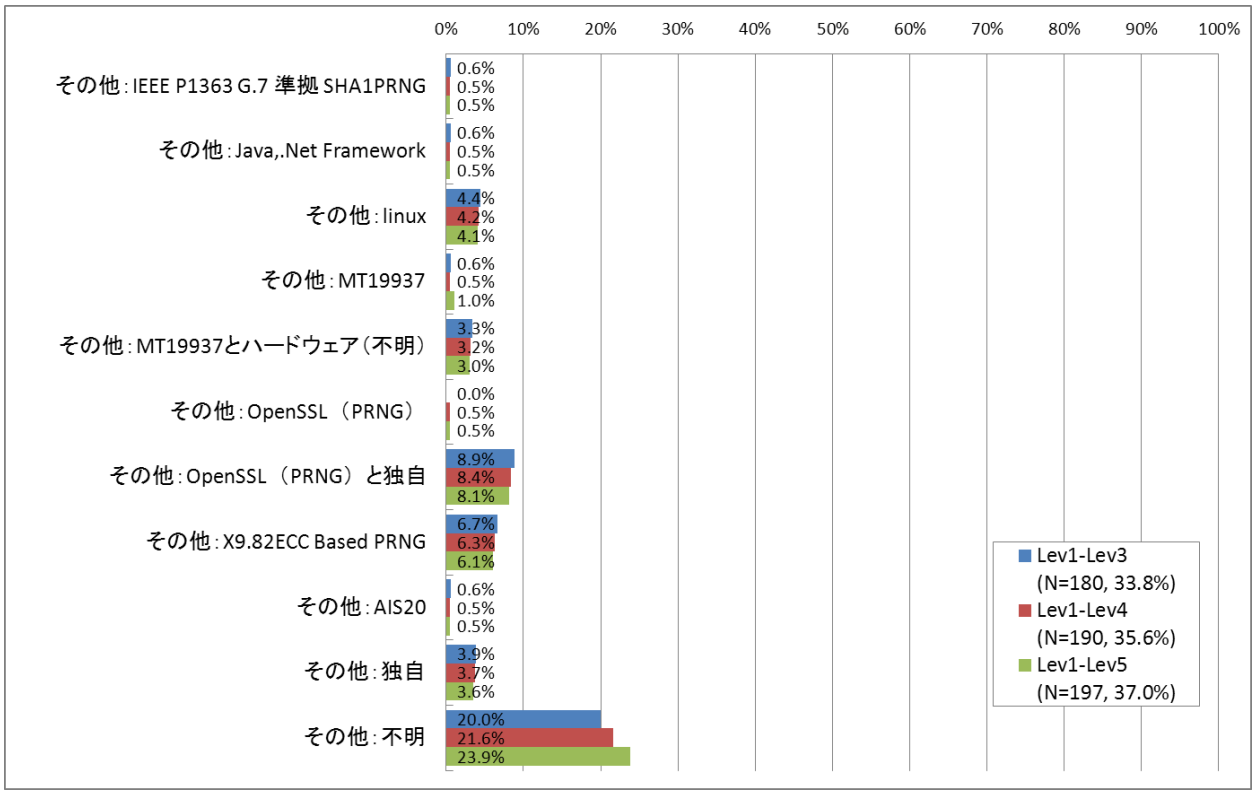

図 14 市販製品･総合(擬似乱数生成器(2))

(11)　市販製品・総合（利用・準拠している国際的な民間規格）

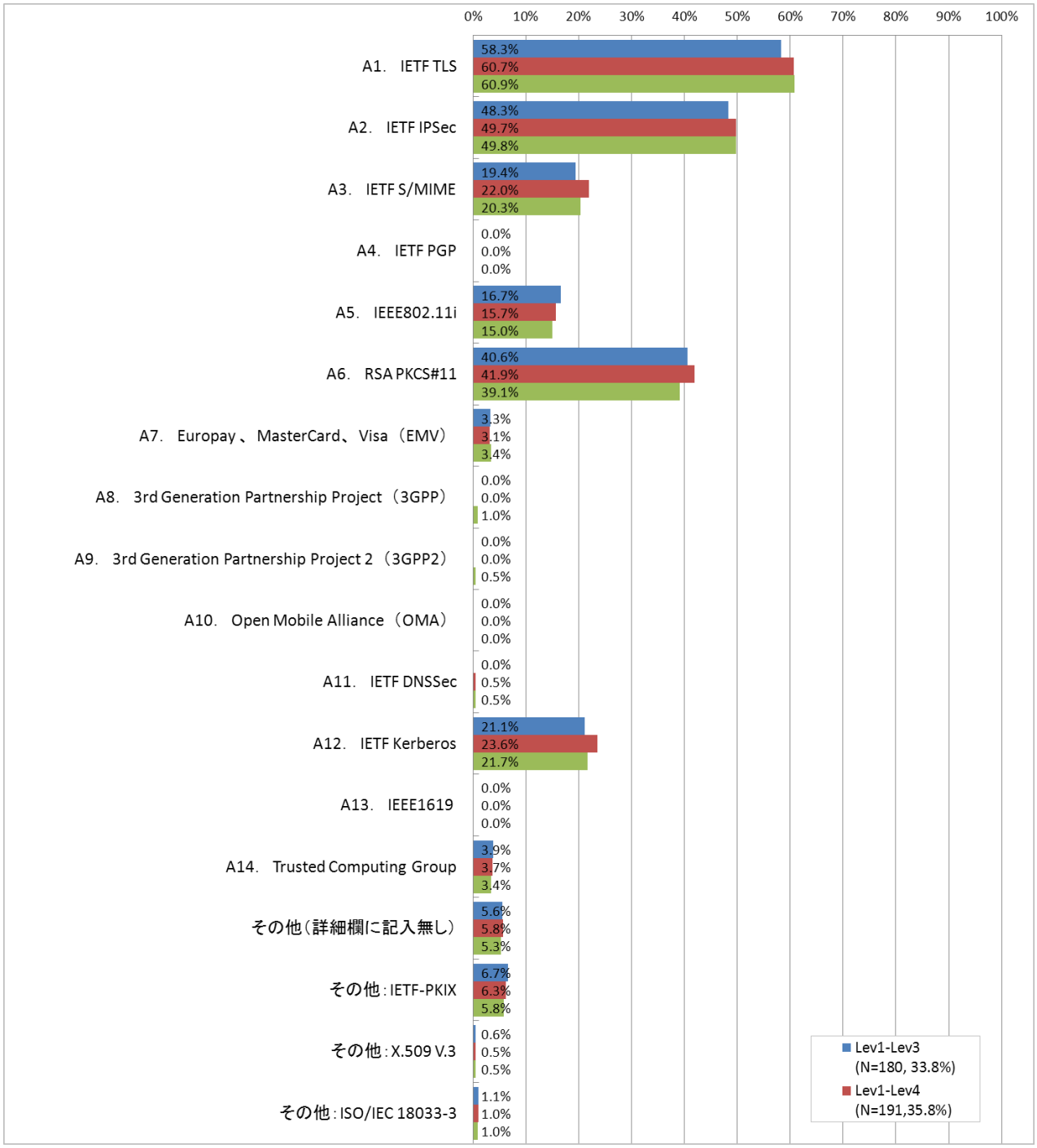

図 15 市販製品･総合（利用･準拠している国際的な民間規格(1)）

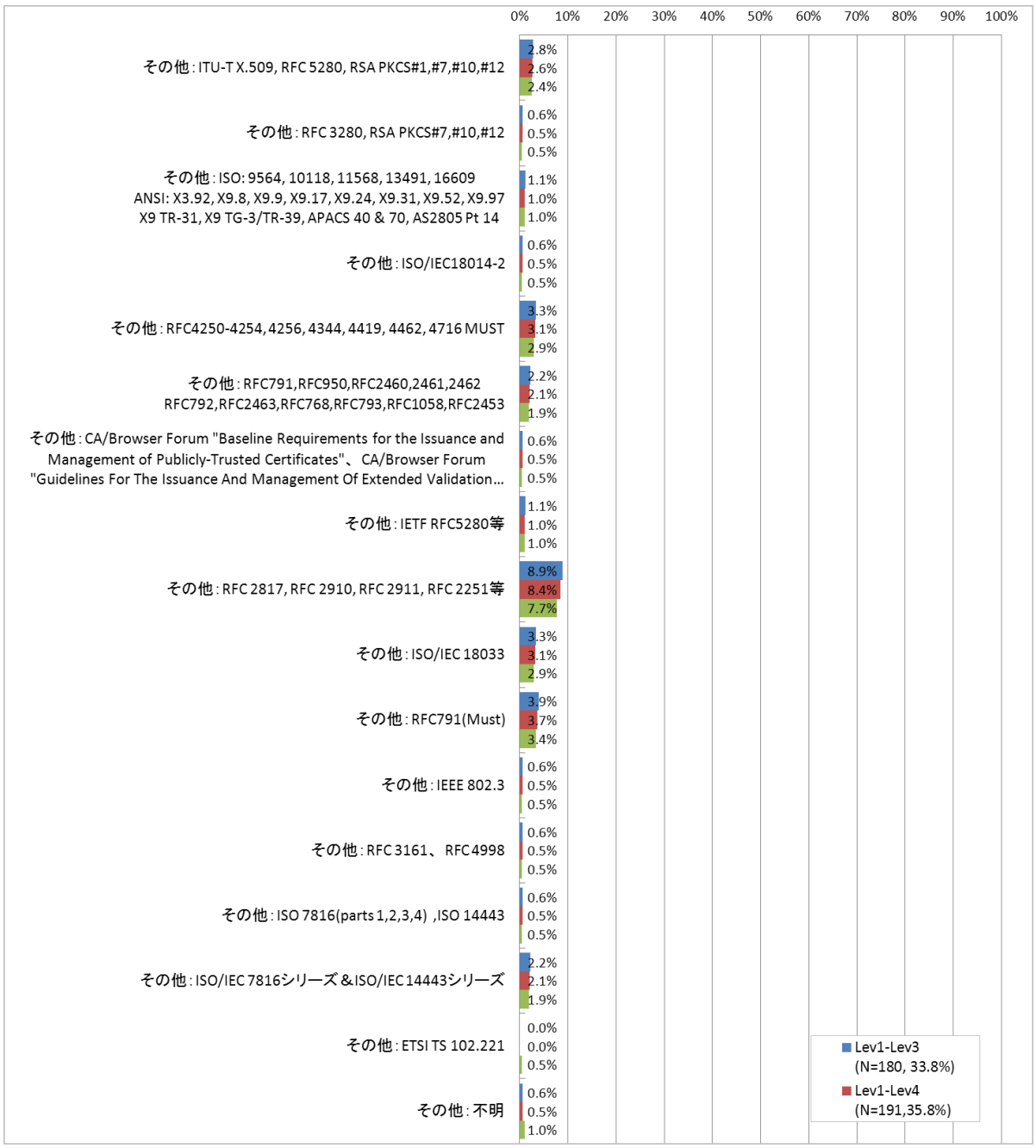

図 16 市販製品・総合（利用・準拠している国際的な民間規格(2)）

(12)　市販製品・総合（利用・準拠している特定団体）

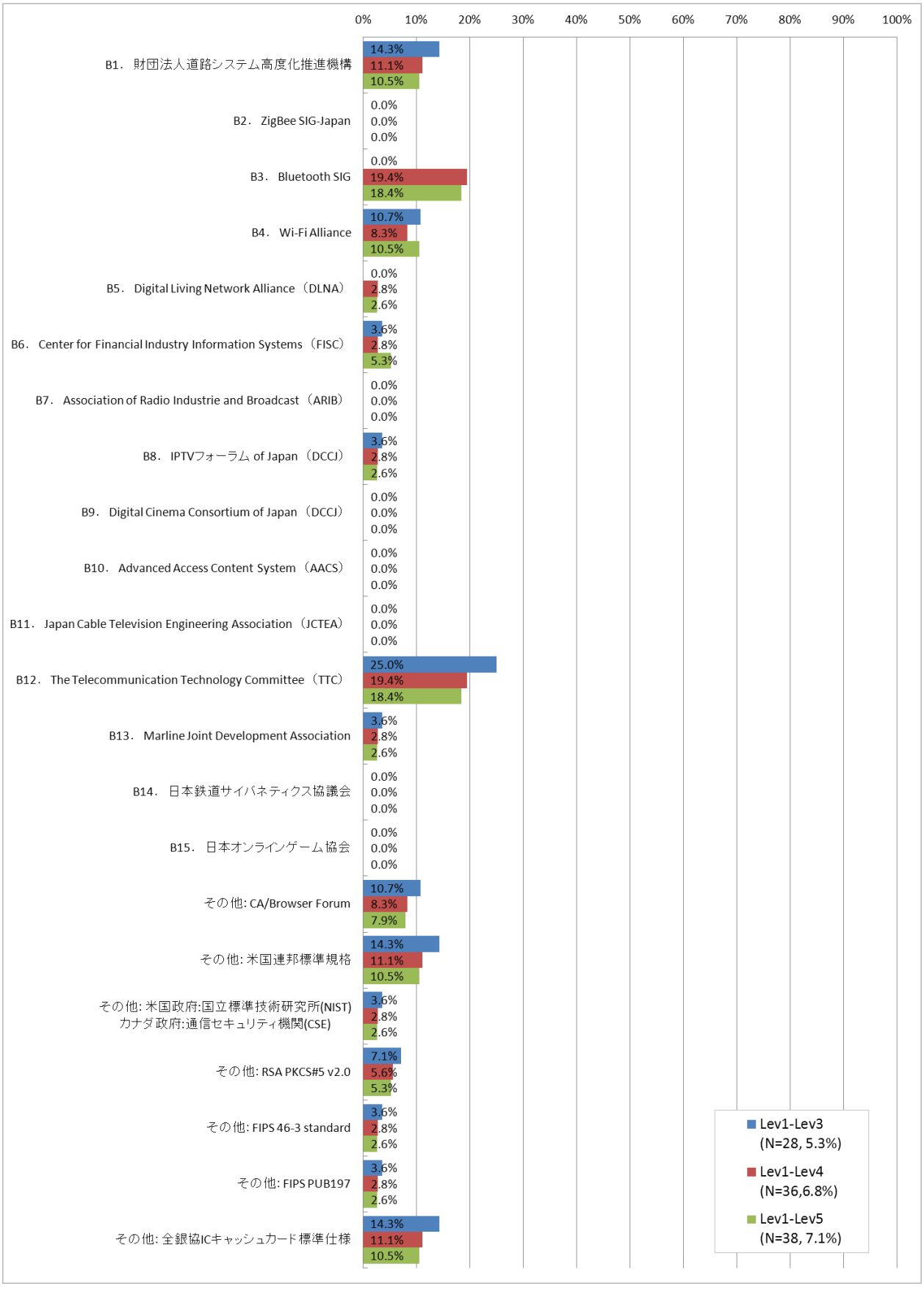

図 17 市販製品･総合（利用･準拠している特定団体）

3.2.2 市販暗号モジュール

市販暗号モジュールは、製品カテゴリの1:オペレーティングシステム、2:暗号ツールライブラリ/ライブラリ、11:カード、12:IC チップ、13:ハードウェアセキュリティモジュールである。以下に集計結果を報告する。

(1) 市販暗号モジュール（公開鍵暗号（署名））

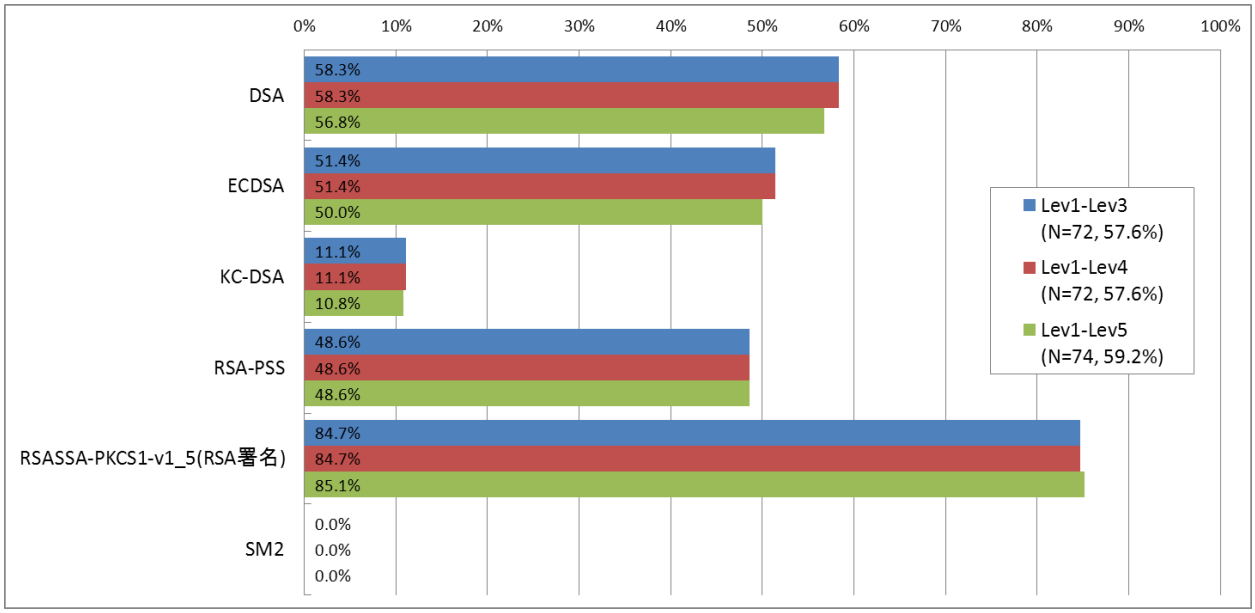

図 18 市販暗号モジュール(公開鍵暗号（署名))

(2) 市販暗号モジュール（公開鍵暗号（守秘・鍵共有））

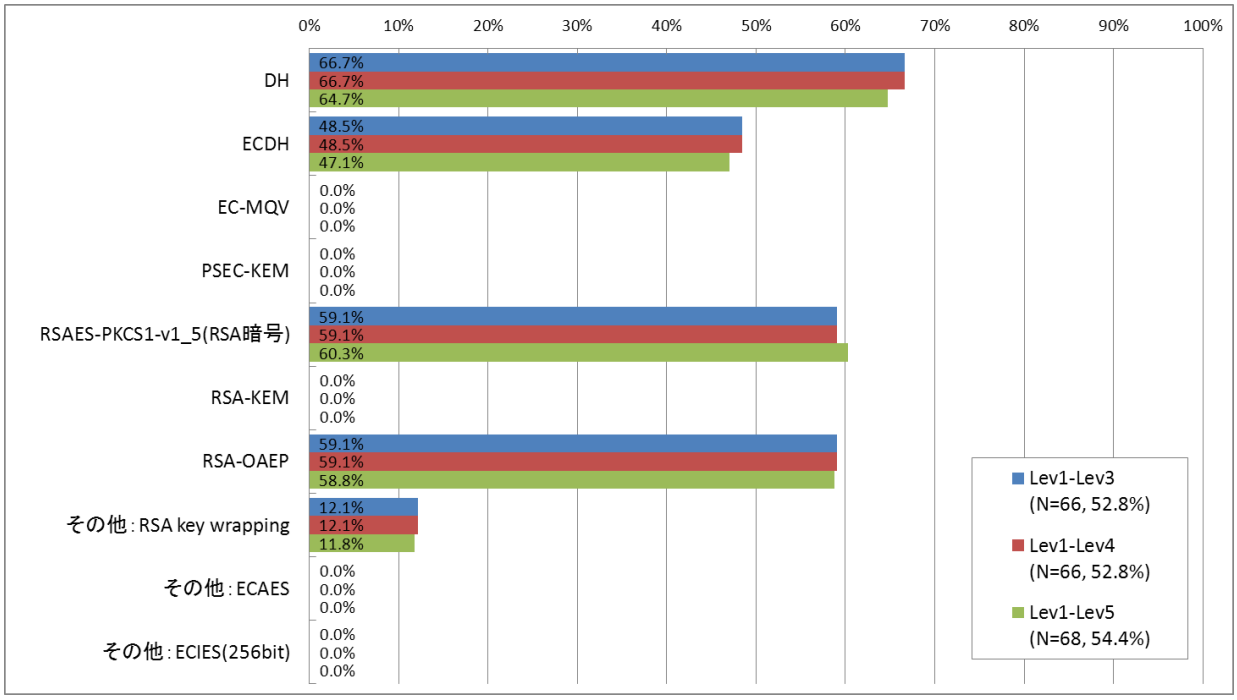

図 19 市販暗号モジュール(公開鍵暗号（守秘・鍵共有))

(3) 市販暗号モジュール（共通鍵暗号（64 ビットブロック暗号））

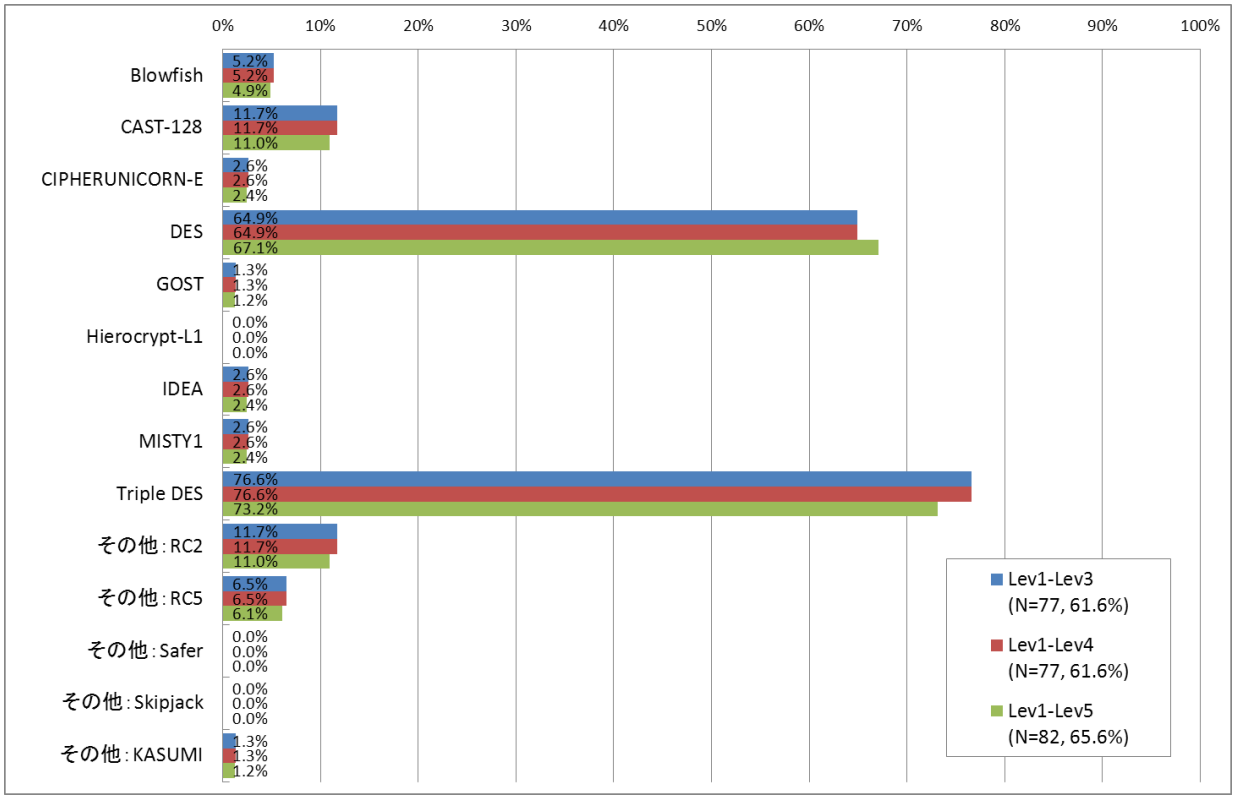

図 20 市販暗号モジュール(共通鍵暗号（64 ビットブロック暗号))

(4) 市販暗号モジュール（共通鍵暗号（128 ビットブロック暗号））

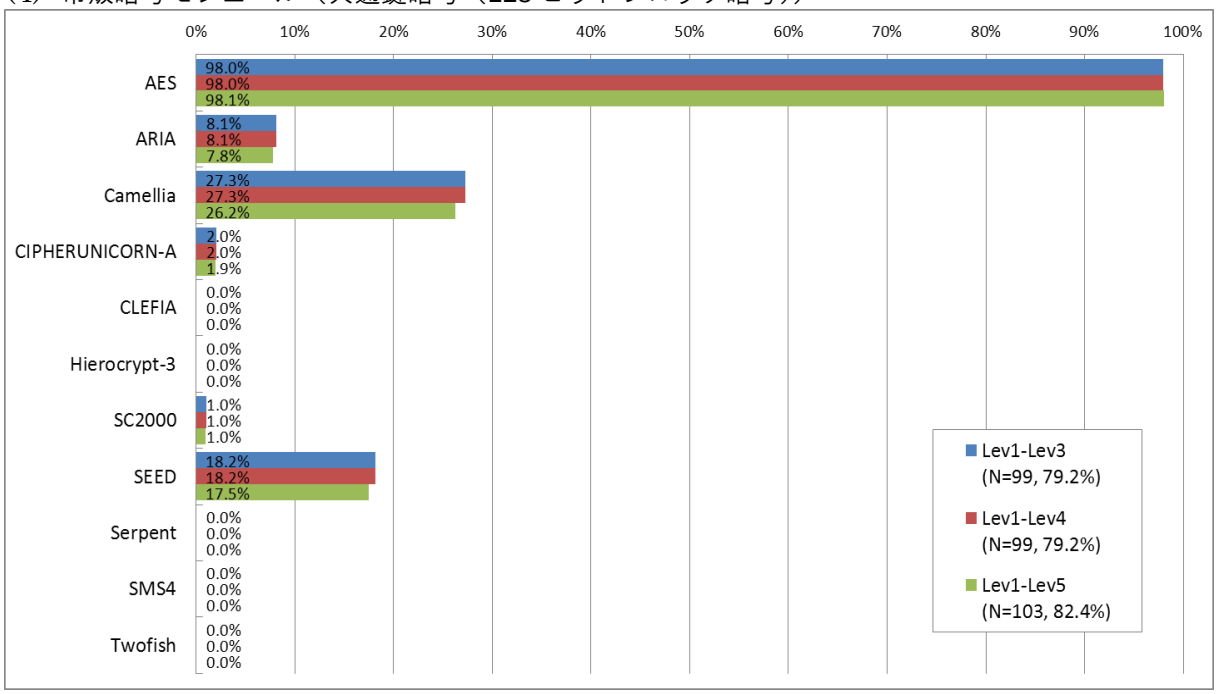

図 21 市販暗号モジュール(共通鍵暗号（128 ビットブロック暗号))

(5) 市販暗号モジュール（共通鍵暗号（ストリーム暗号））

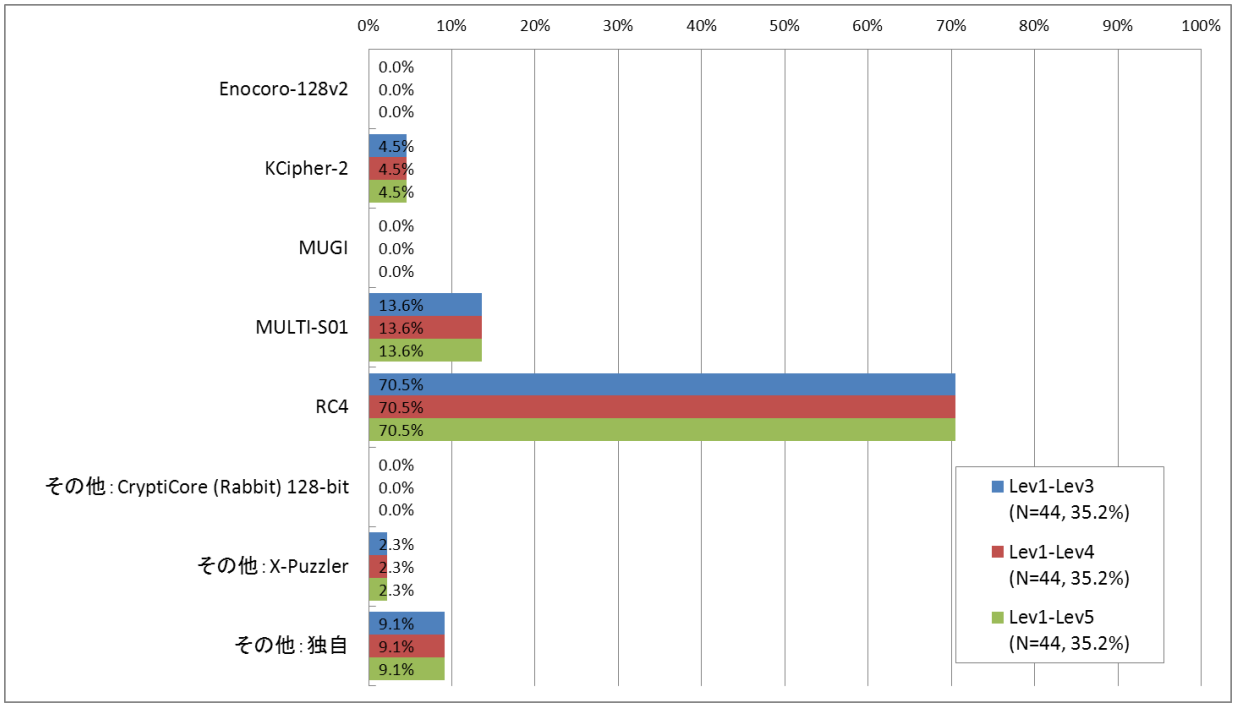

図 22 市販暗号モジュール(共通鍵暗号（ストリーム暗号))

(6) 市販暗号モジュール（ハッシュ関数）

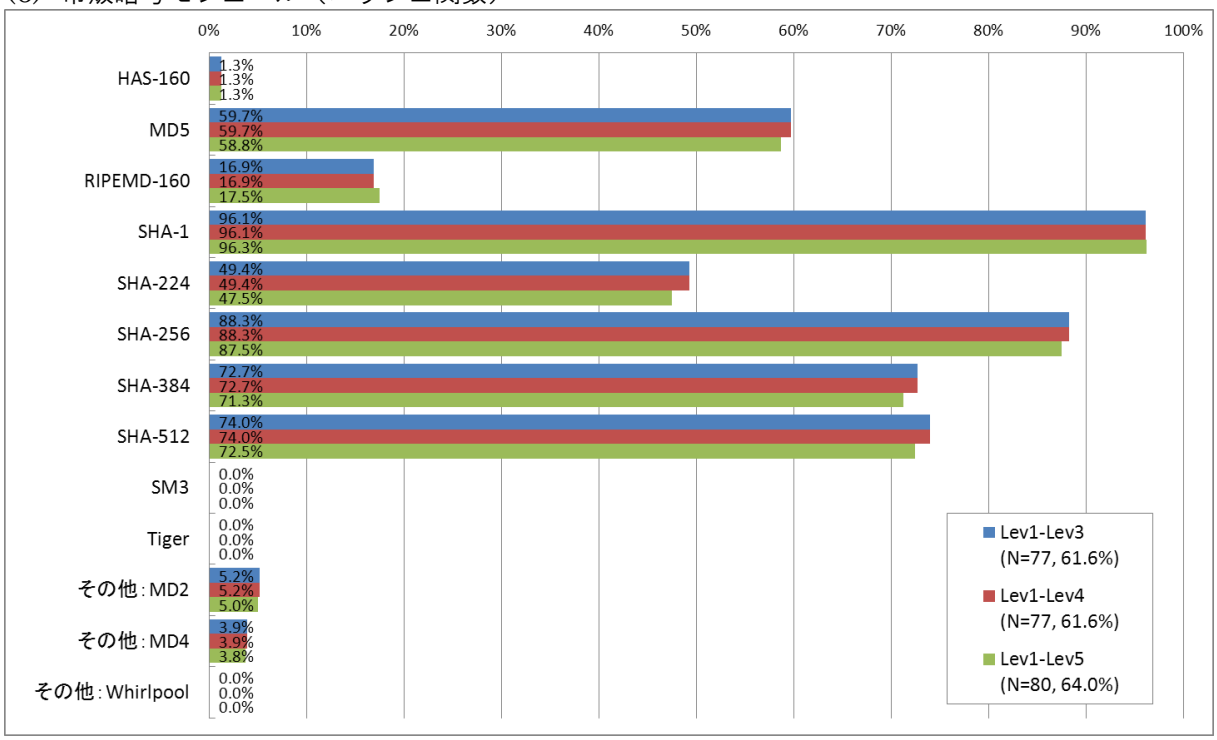

図 23 市販暗号モジュール（ハッシュ関数）

(7) 市販暗号モジュール（暗号利用モード）

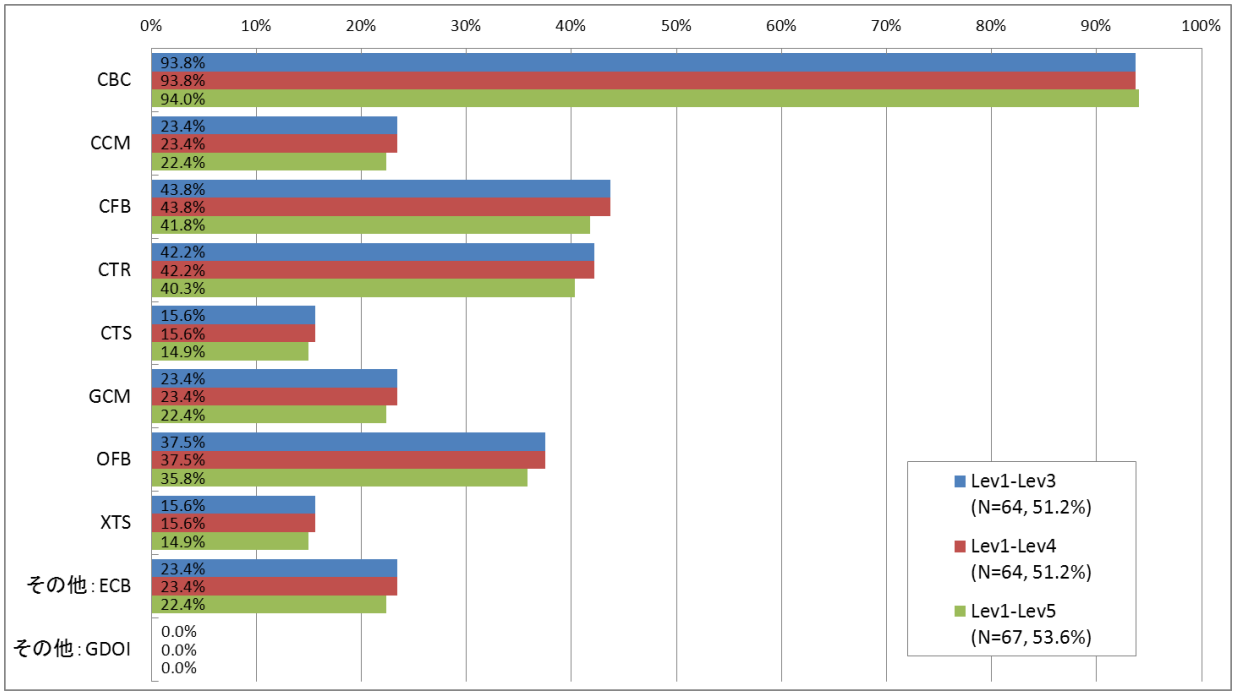

図 24 市販暗号モジュール（暗号利用モード）

(8) 市販暗号モジュール（メッセージ認証コード）

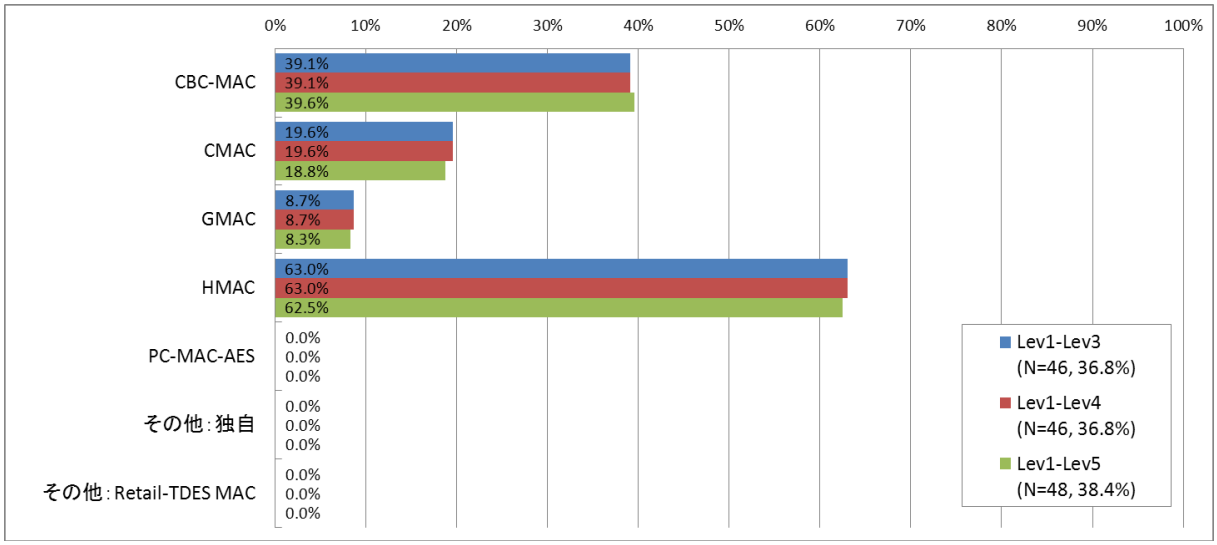

図 25 市販暗号モジュール（メッセージ認証コード）

(9) 市販暗号モジュール（エンティティ認証）

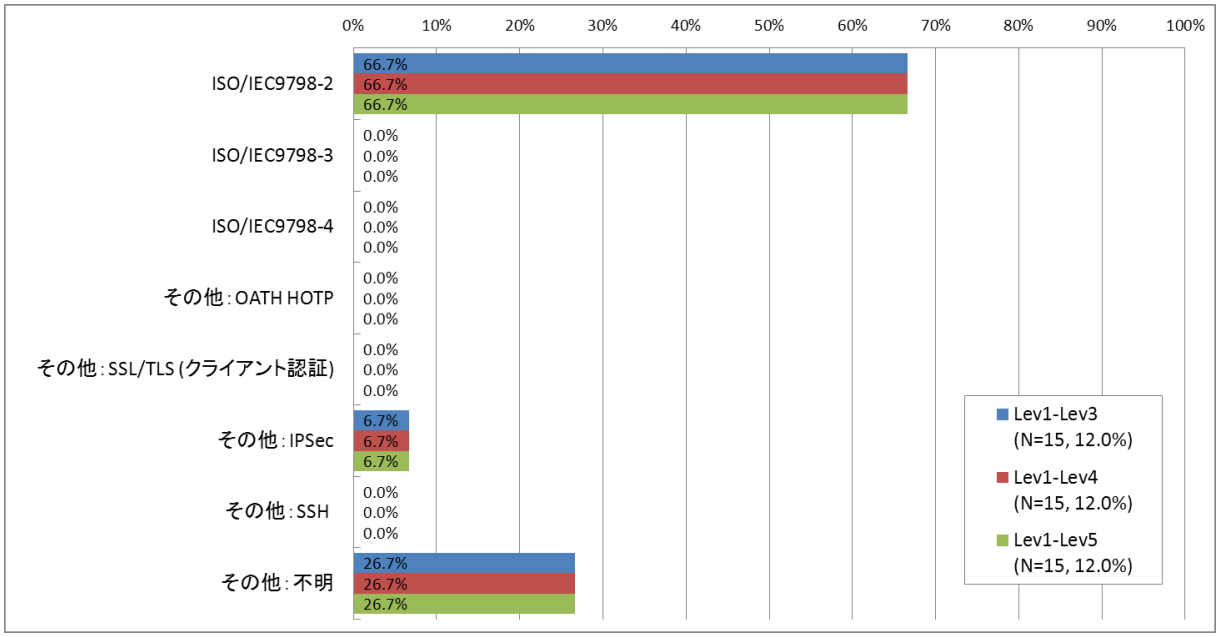

図 26 市販暗号モジュール（エンティティ認証）

(10) 市販暗号モジュール（擬似乱数生成器）

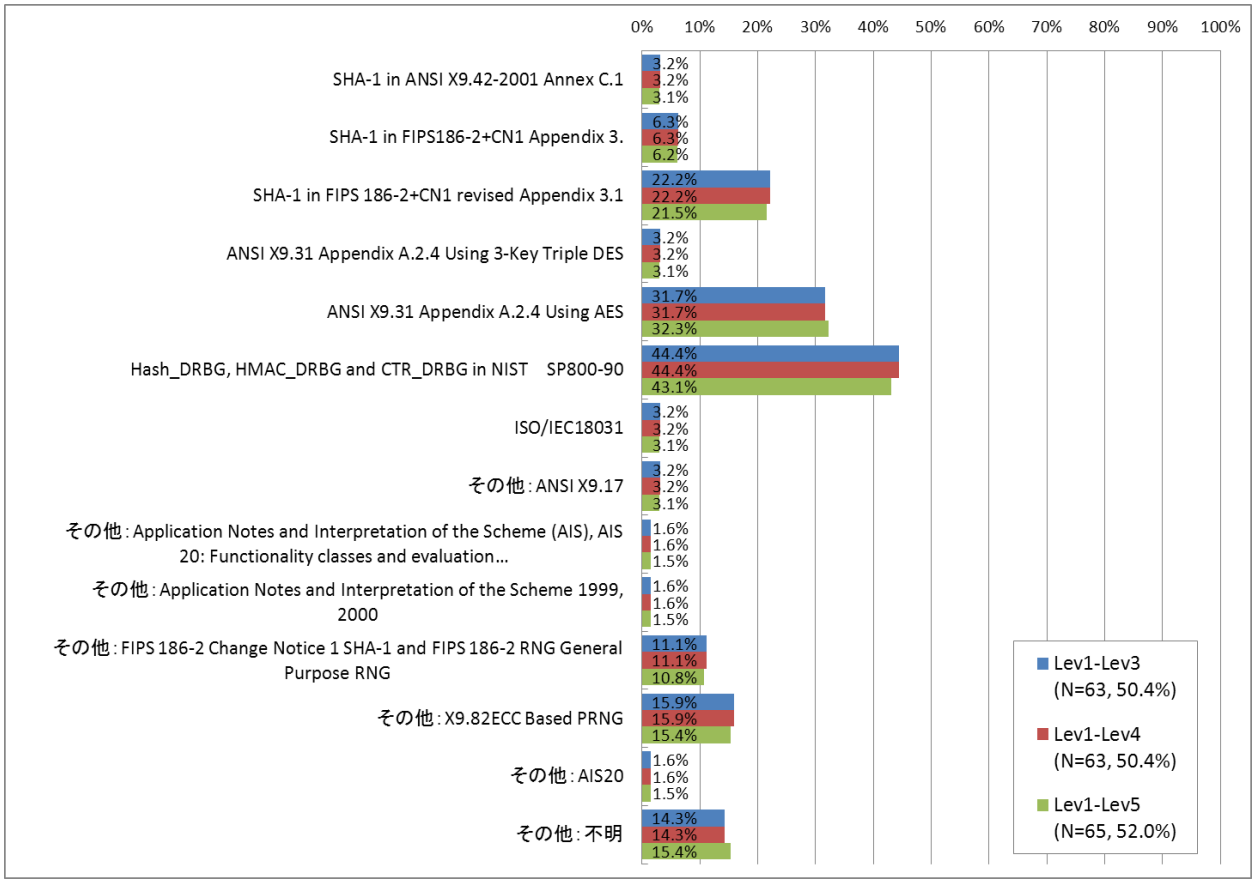

図 27 市販暗号モジュール（擬似乱数生成器）

(11)　市販暗号モジュール（利用・準拠している国際的な民間規格）

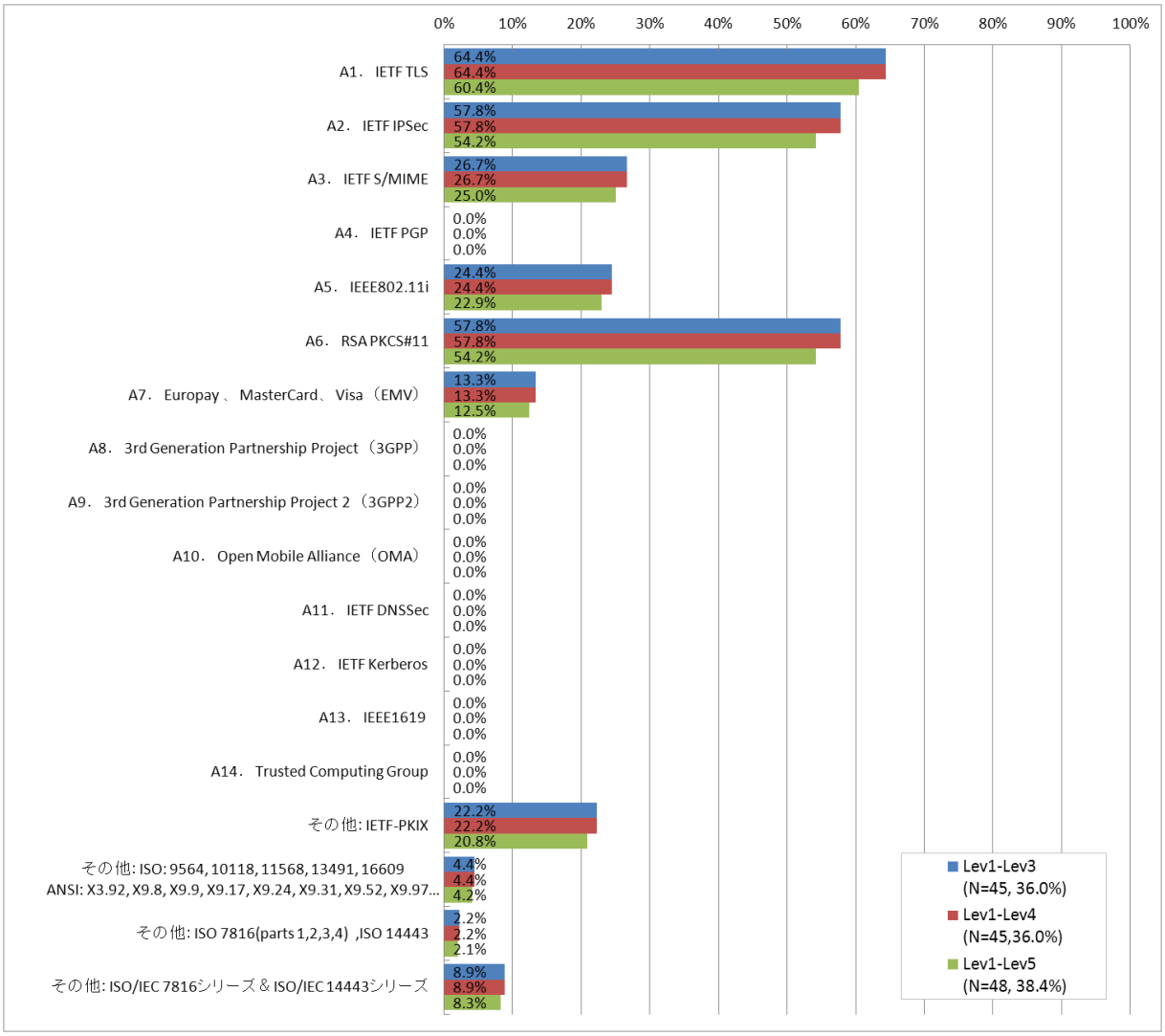

図 28 市販暗号モジュール（利用・準拠している国際的な民間規格）

(12)　市販製暗号モジュール（利用・準拠している特定団体）

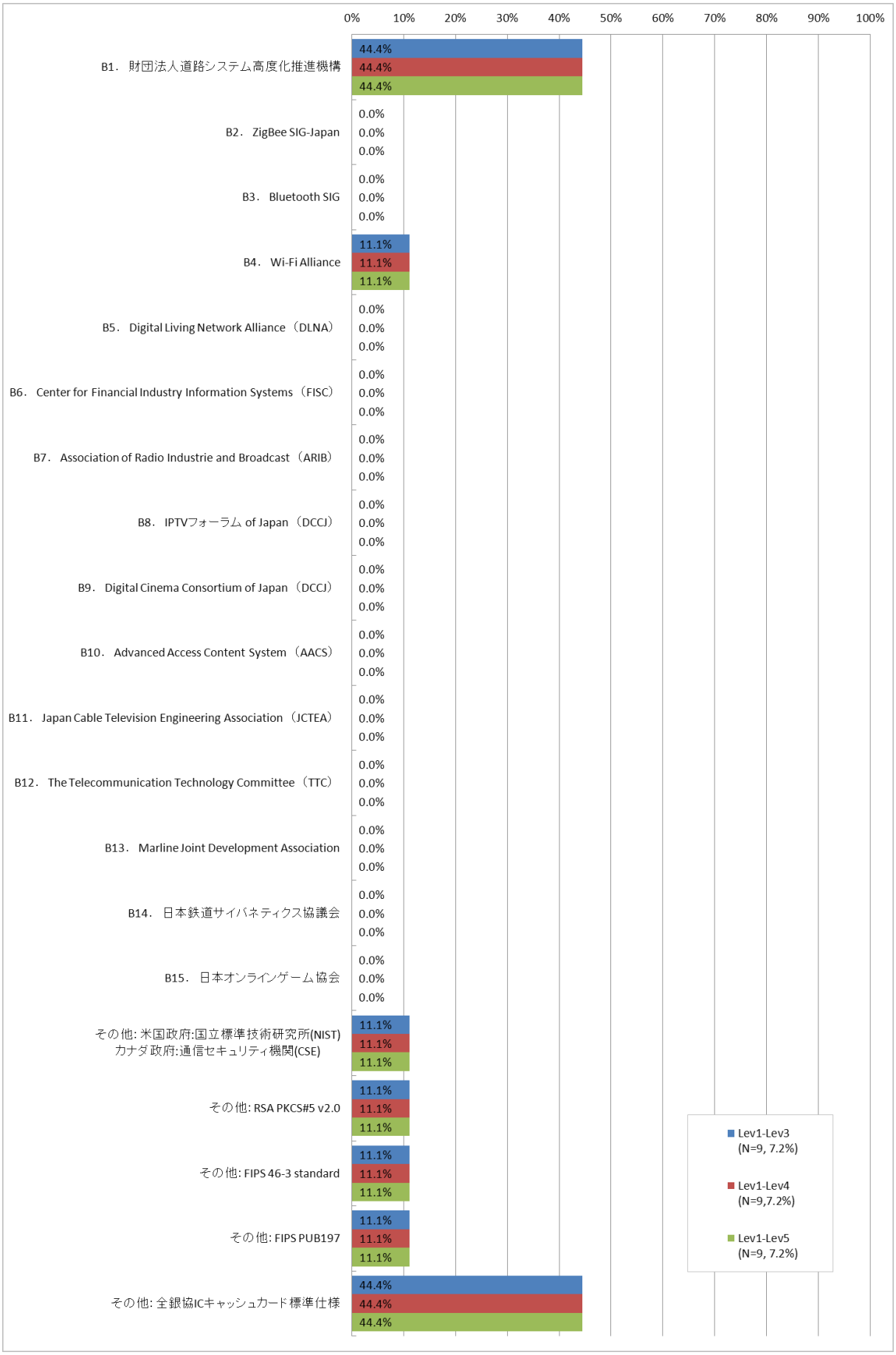

図 29 市販暗号モジュール（利用・準拠している特定団体）

3.2.3　オプション設問等の集計結果について

オプション設問については、本調査の補足情報を収集することを目的として調査を実施した。オプション設問の回答情報は、製品・システムが利用しているオープンソースプロジェクトや今後組込みを検討している暗号アルゴリズムなど回答者にとっては、他の情報と関連付けを避けたい内容も含まれており、企業名や製品名、及び製品カテゴリ等についても、その他の回答内容と関連付けないことを前提として回答を得たものも存在する。そのため、他の情報とは関連付けない形式として単純集計の結果を以下に報告する。

(1) 利用しているオープンソースプロジェクト

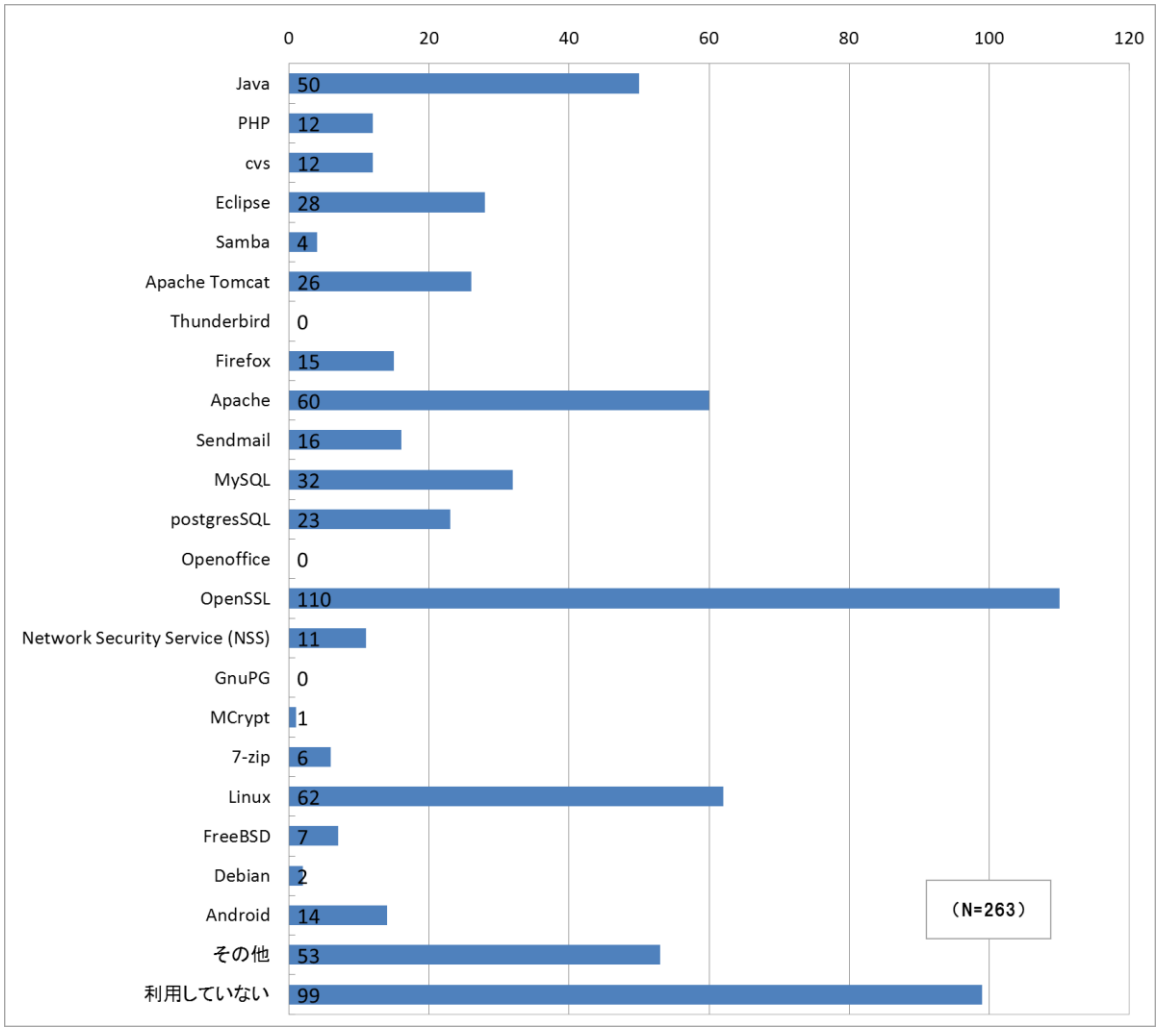

図 30 利用しているオープンソースプロジェクト

(2) 利用している製品・システムのカテゴリ

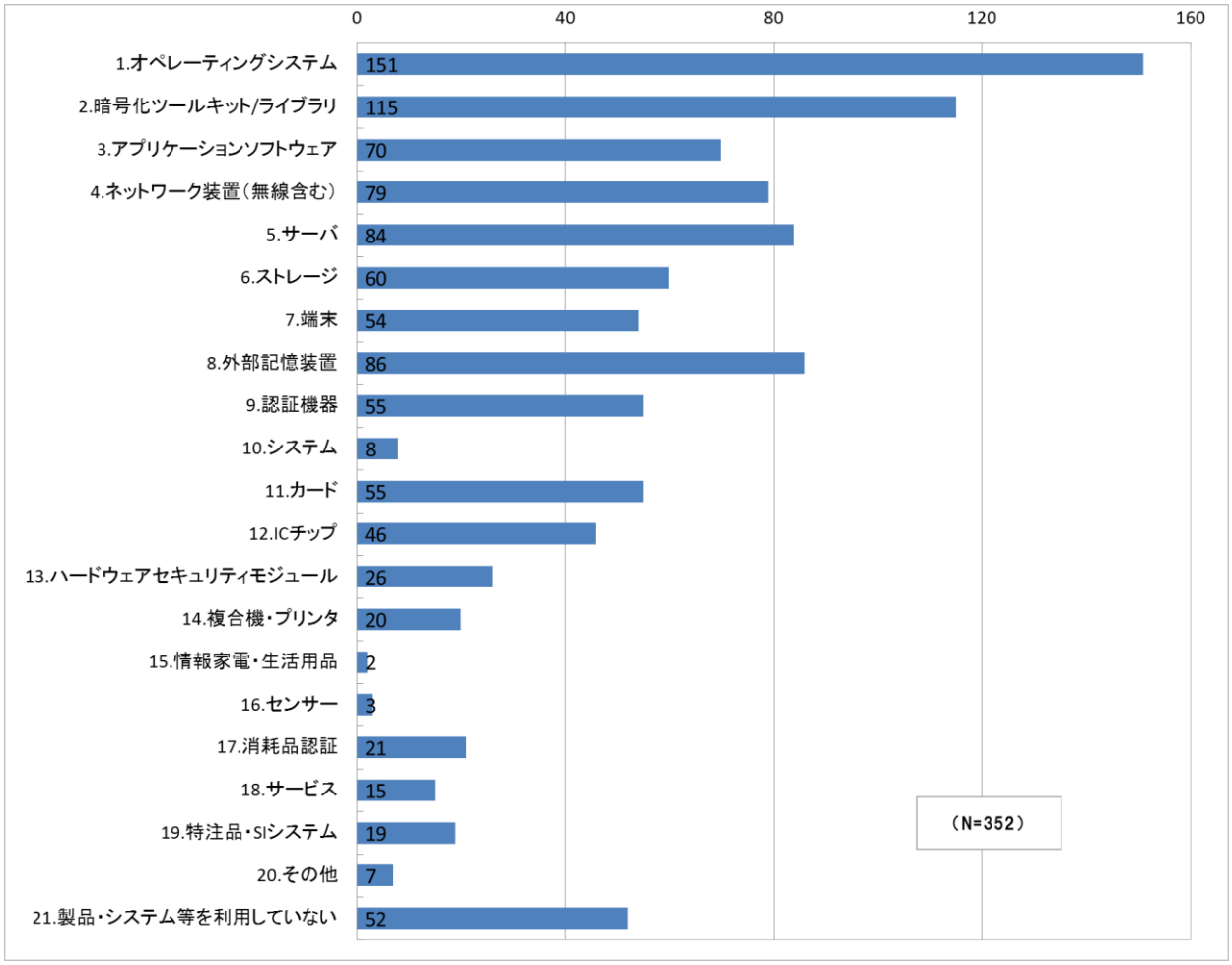

図 31 利用している製品・システムのカテゴリ

(3) 今後、組込みを検討及び計画している暗号アルゴリズム

A) 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））

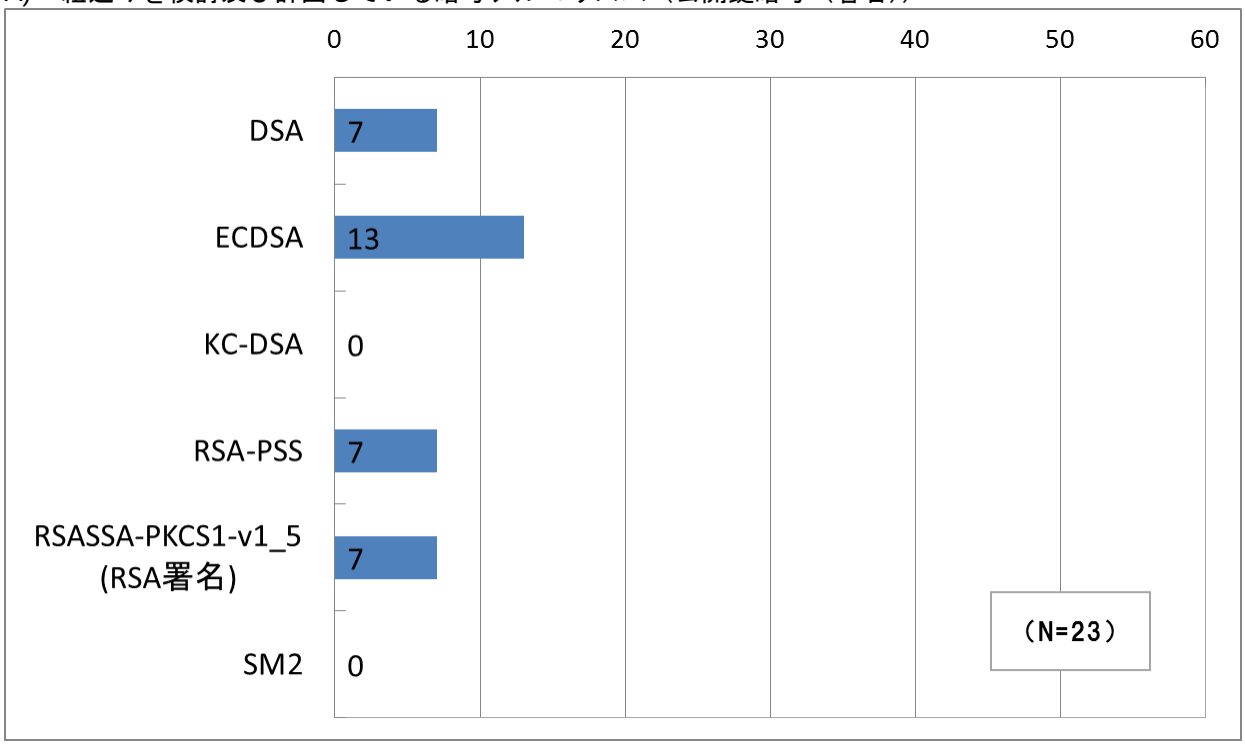

図 32 組込みを検討及び計画している暗号アルゴリズム（公開鍵暗号（署名））

B) 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））

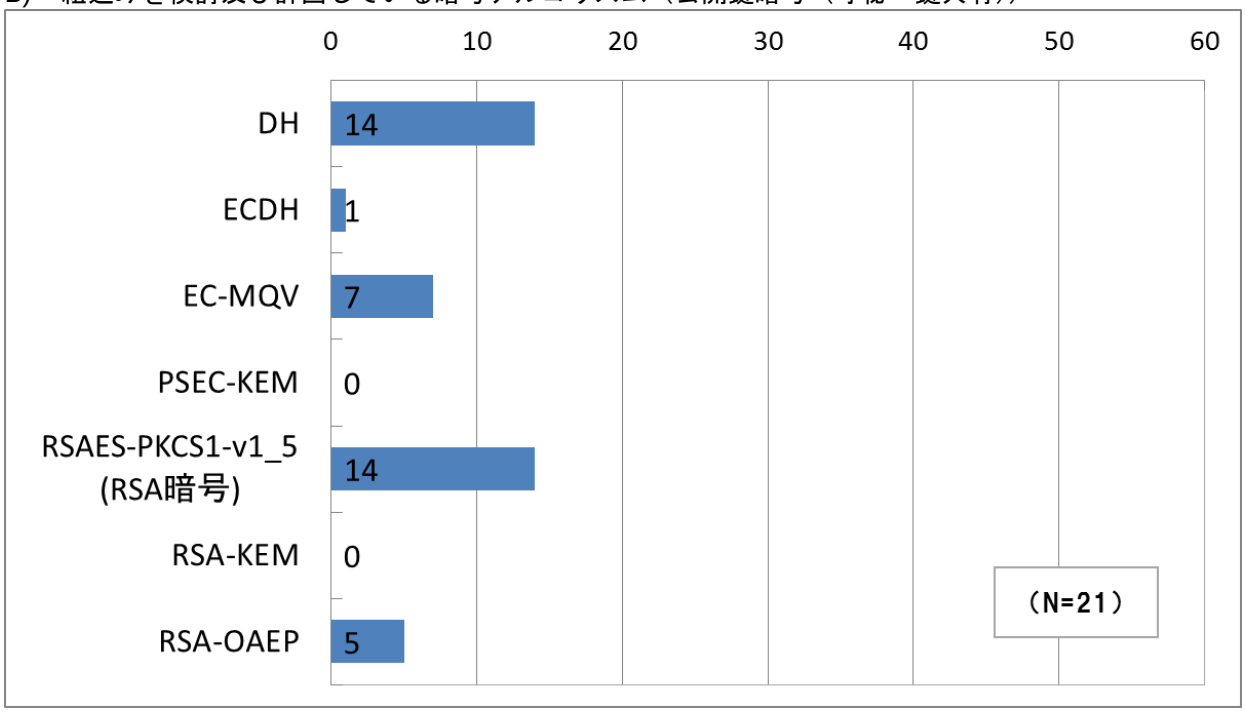

図 33 調査結果：組込みを検討している暗号アルゴリズム（公開鍵暗号（守秘・鍵共有））

C)　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））

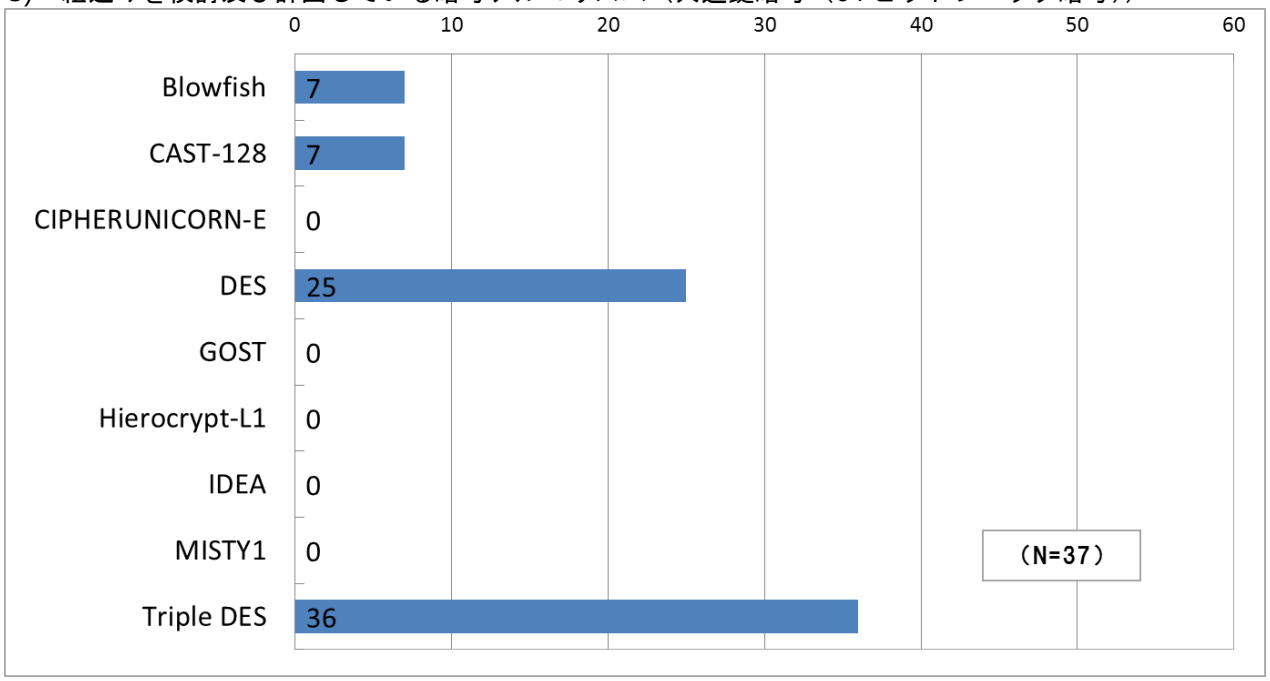

図 34 組込みを検討及び計画している暗号アルゴリズム（共通鍵暗号（64 ビットブロック暗号））

D)　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））

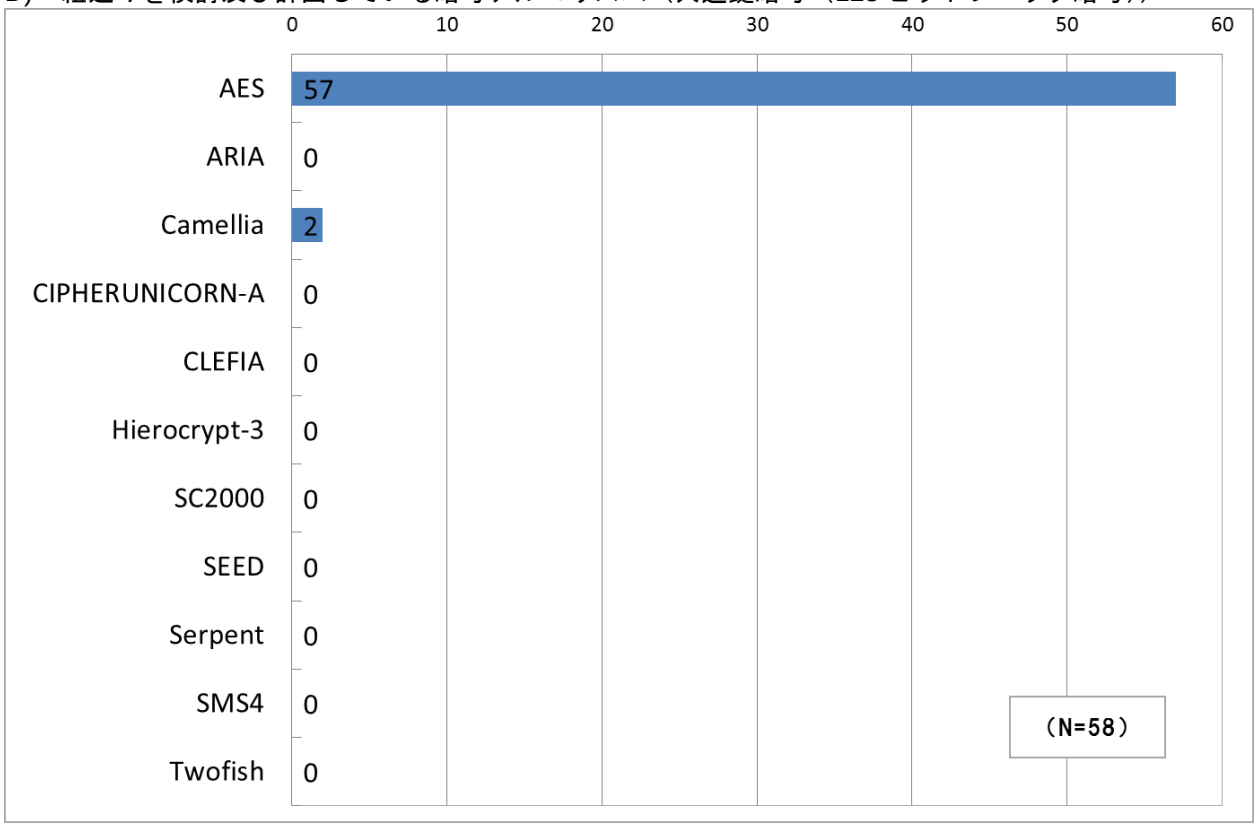

図 35 組込みを検討及び計画している暗号アルゴリズム（共通鍵暗号（128 ビットブロック暗号））

E)　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））

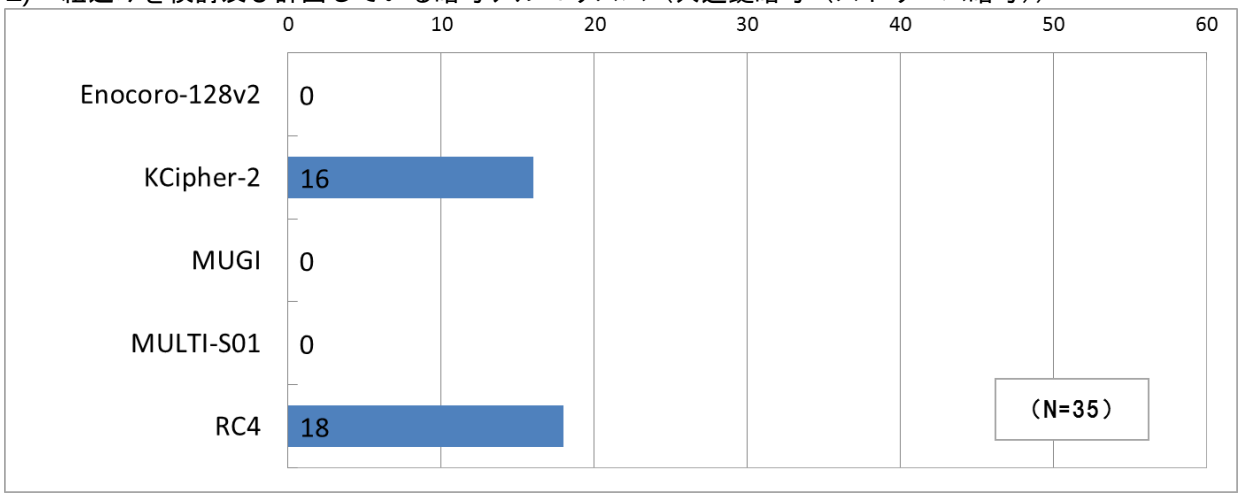

図 36 組込みを検討及び計画している暗号アルゴリズム（共通鍵暗号（ストリーム暗号））

F)　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）

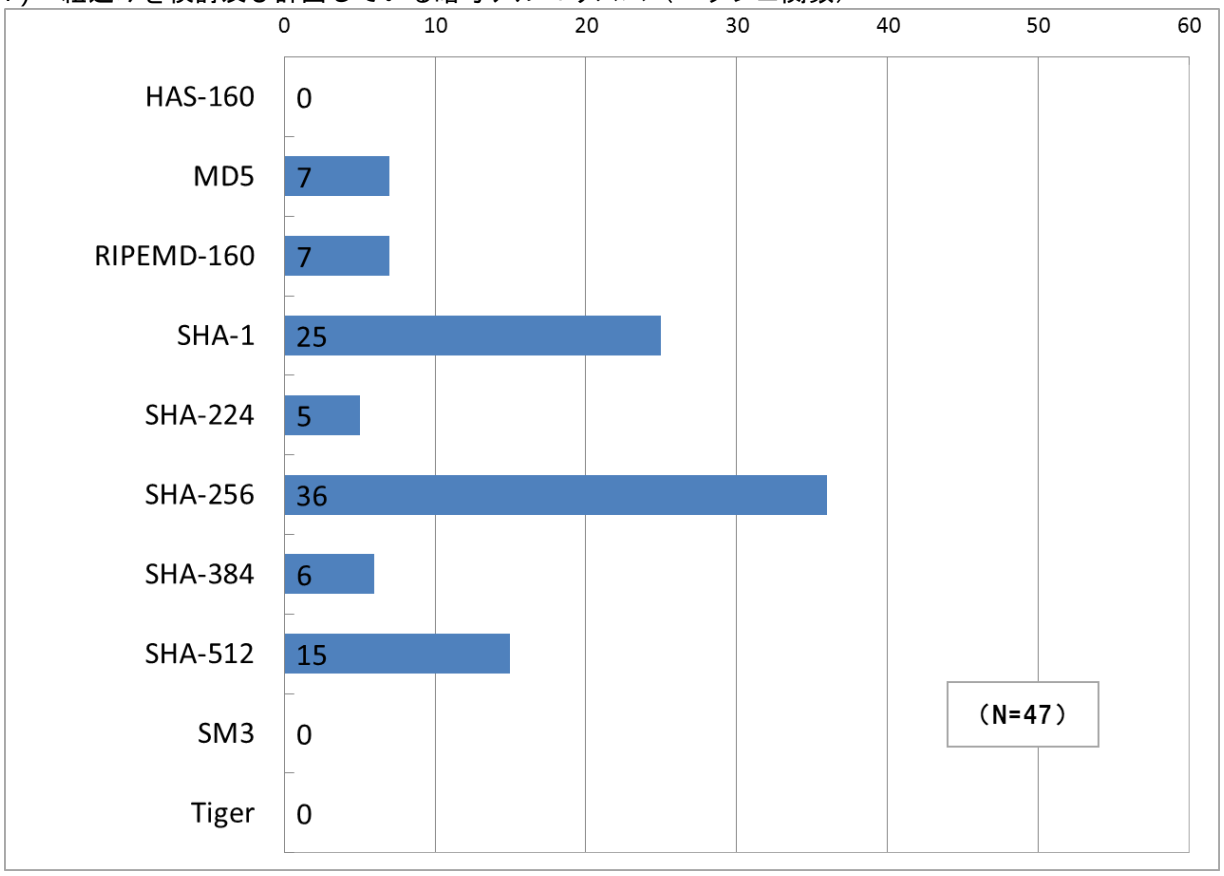

図 37 組込みを検討及び計画している暗号アルゴリズム（ハッシュ関数）

G)　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）

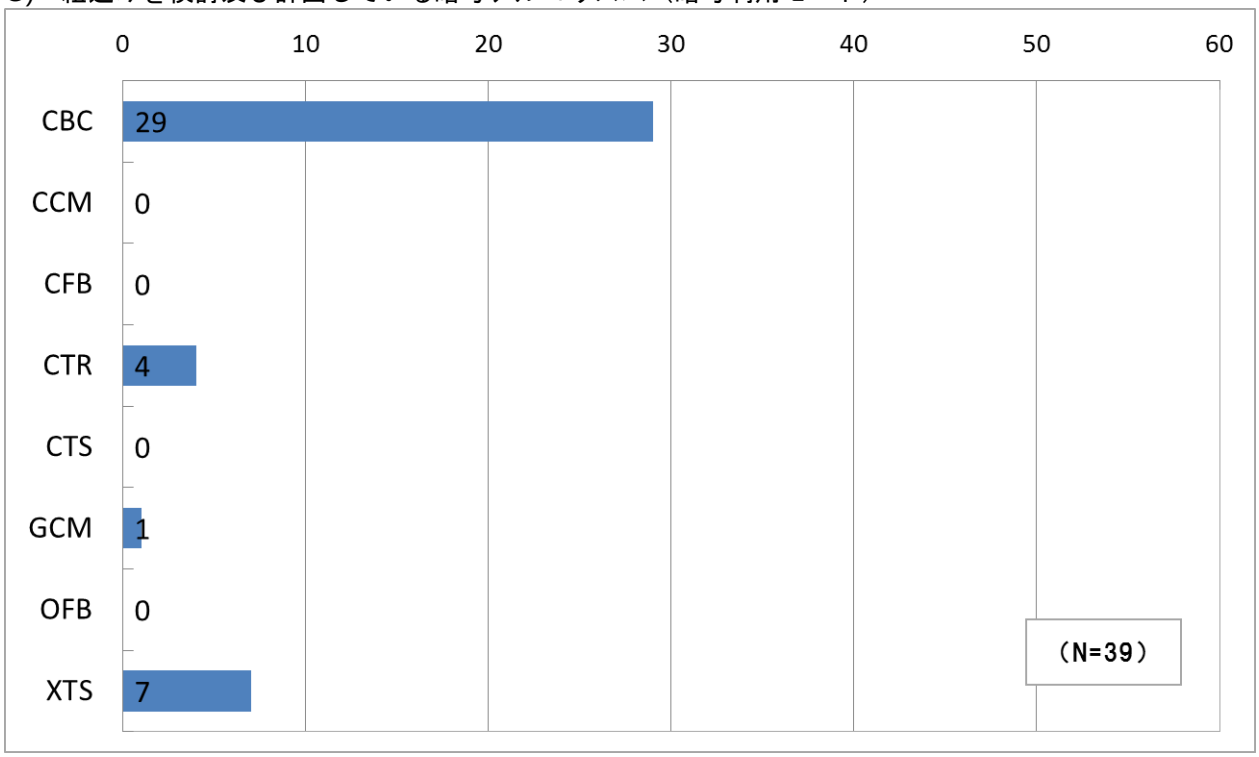

図 38 組込みを検討及び計画している暗号アルゴリズム（暗号利用モード）

H)　組込みを検討及び計画している暗号アルゴリズム（メッセージ認証コード）

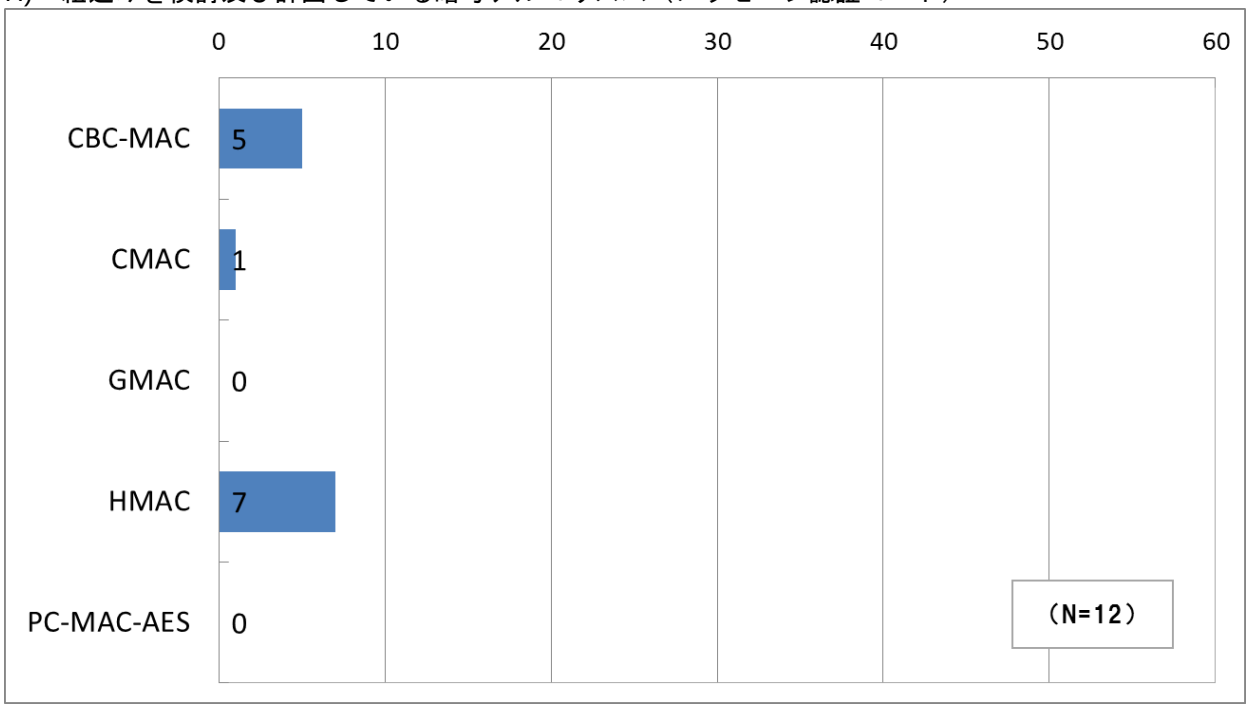

図 39 組込みを検討及び計画している暗号アルゴリズム（メッセージ認証コード）

(4) 第三者評価・試験及び認証制度の取得状況及び検討状況

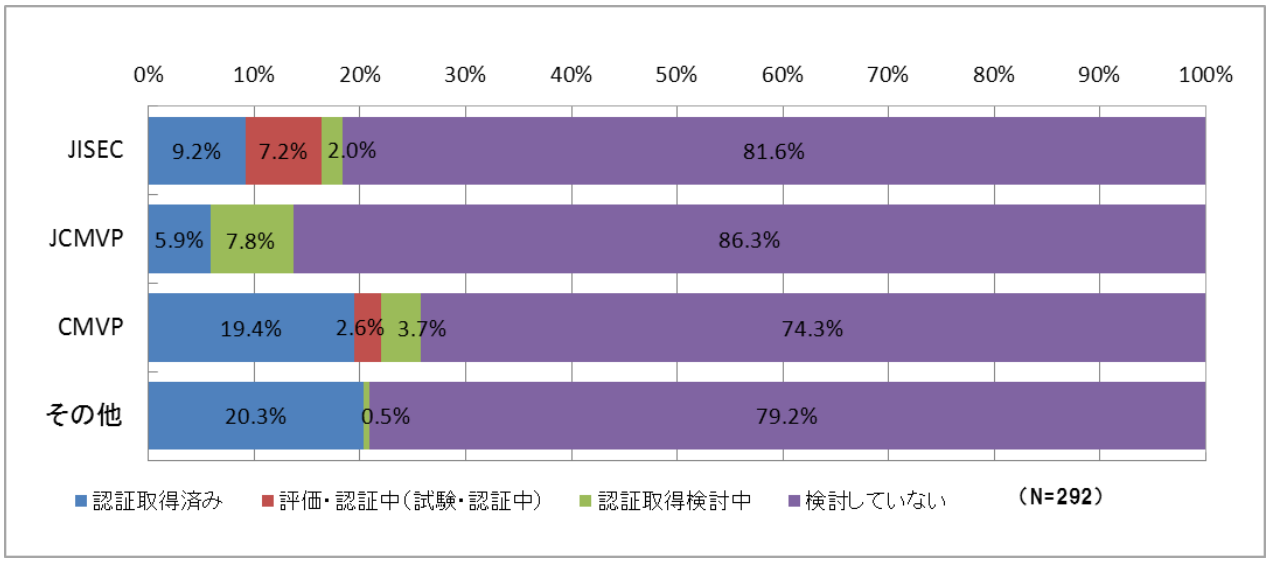

図 40 第三者評価・試験及び認証制度の取得・検討状況

(5) 直近 1 年間の総出荷台数

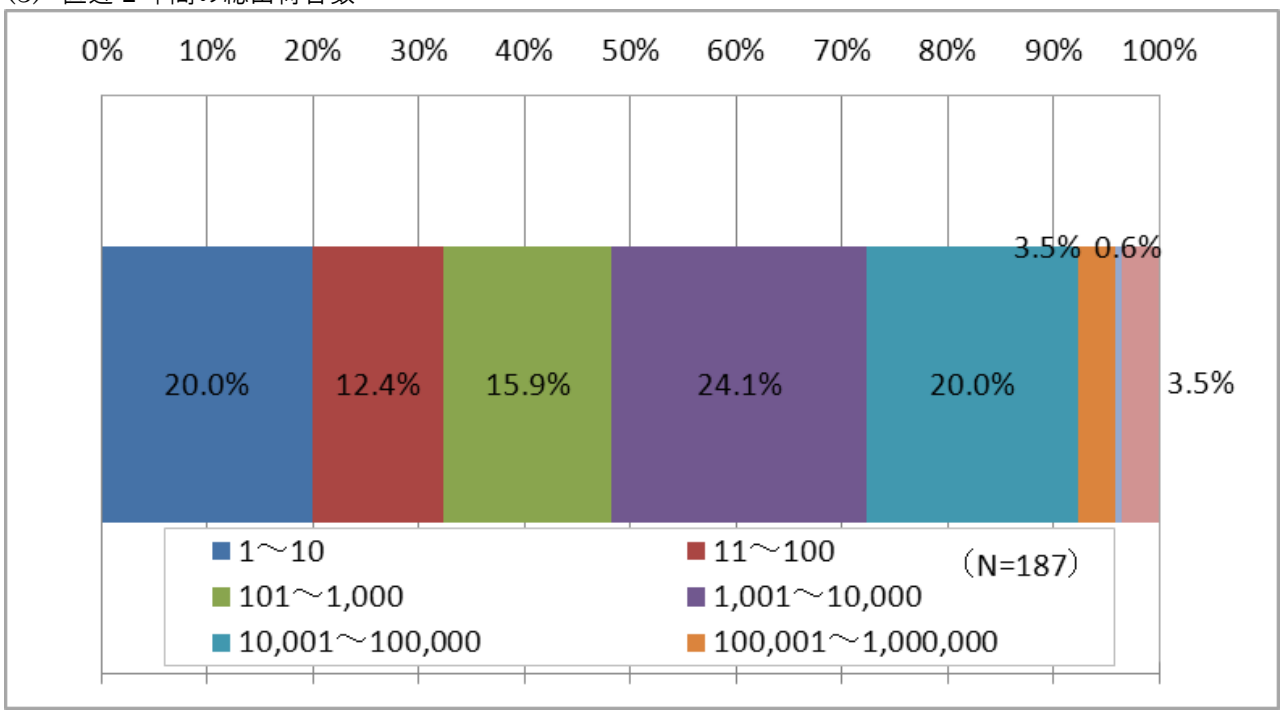

図 41 直近 1 年間の総出荷台数

3.3　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）

経済産業省及び IPA の協力の下、8 府省庁から政府系情報システムの回答数 77、政府系情報システム規格の回答数 5 を得た。また、政府系情報システム規格の公開情報を基に、表 14 で示す 7 規格の調査を実施した。政府系情報システム及び政府系情報システム規格の調査結果を以下に示す。下表では、政府系情報システム及び政府系情報システム規格のアンケート回答の集計結果を Lev.A、政府系情報システム規格の公開情報調査の集計結果を Lev.B で記す。なお、各暗号アルゴリズムの実数は、付録 8.調査結果表（C）を参照。

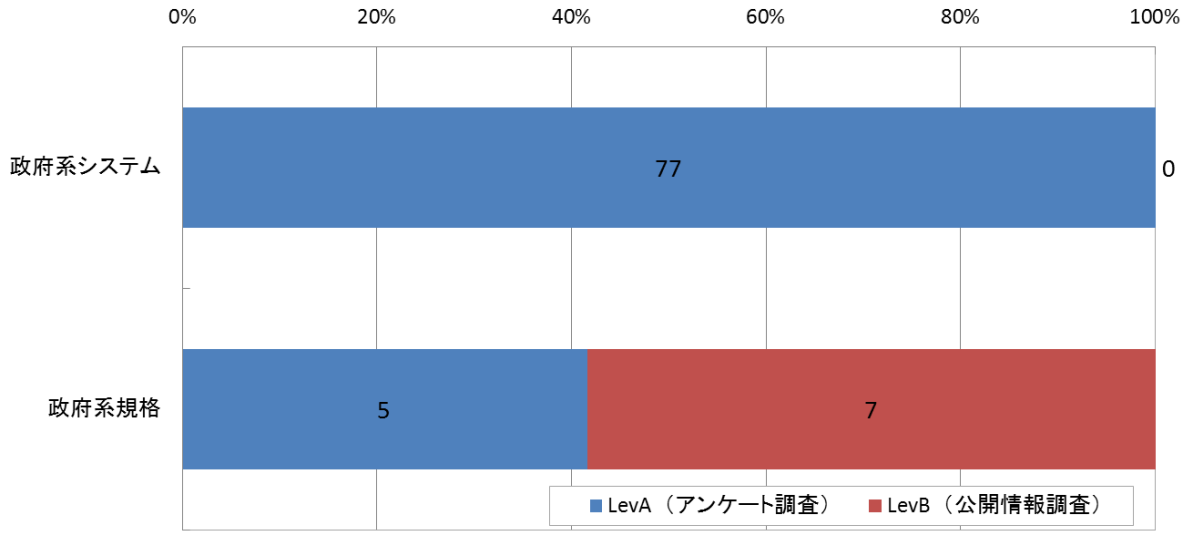

図 42 調査結果概要（調査 C）

政府系情報システムのアンケート回答総数 77 件、政府系情報システム規格のアンケート回答総数 5 件、政府系情報システム規格の公開情報調査 7 件についての集計結果を報告する。

(1) 政府系システム・規格（公開鍵暗号（署名））

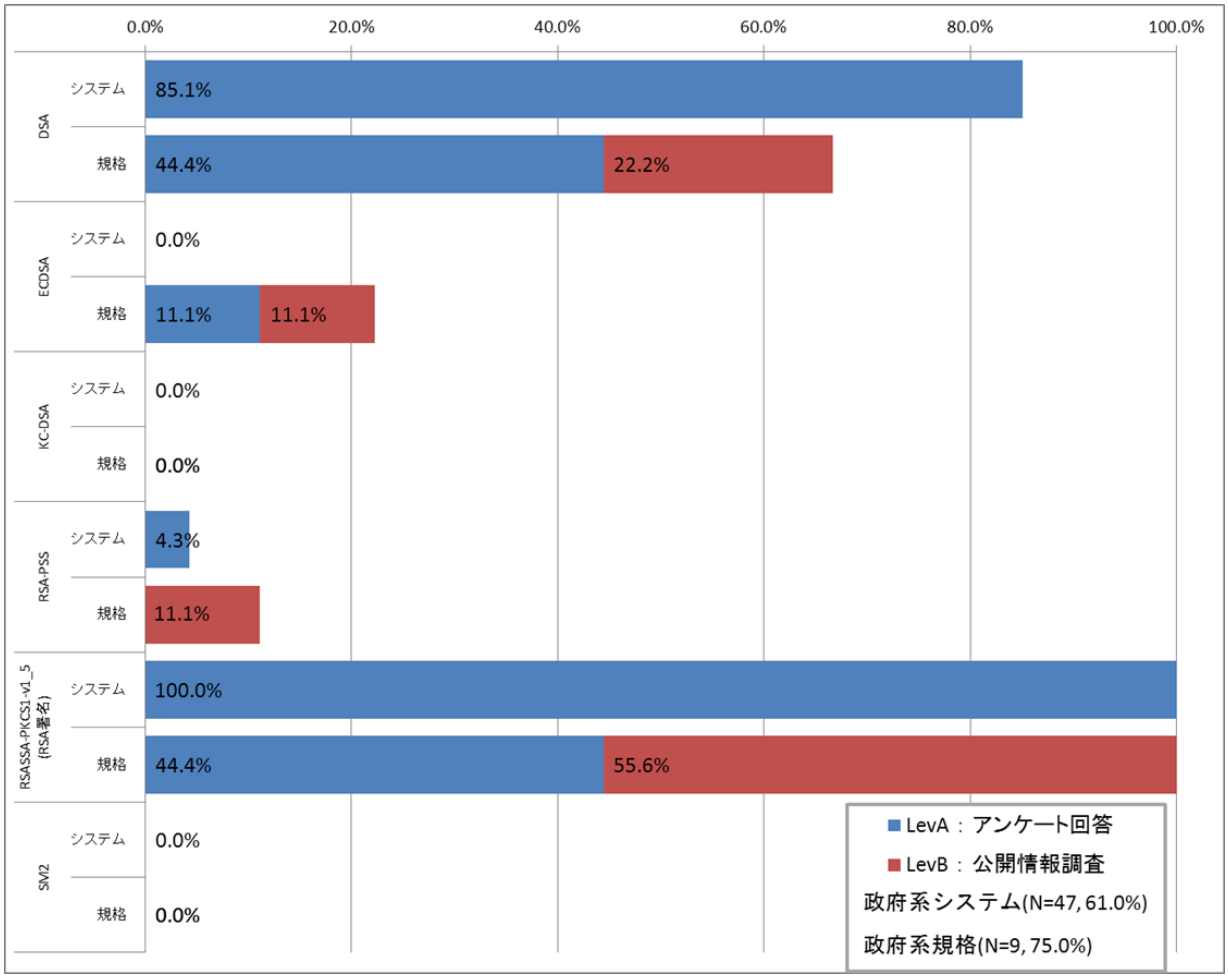

図 43 政府系システム・規格（公開鍵暗号（署名））

(2) 政府系システム・規格（公開鍵暗号（守秘・鍵共有））

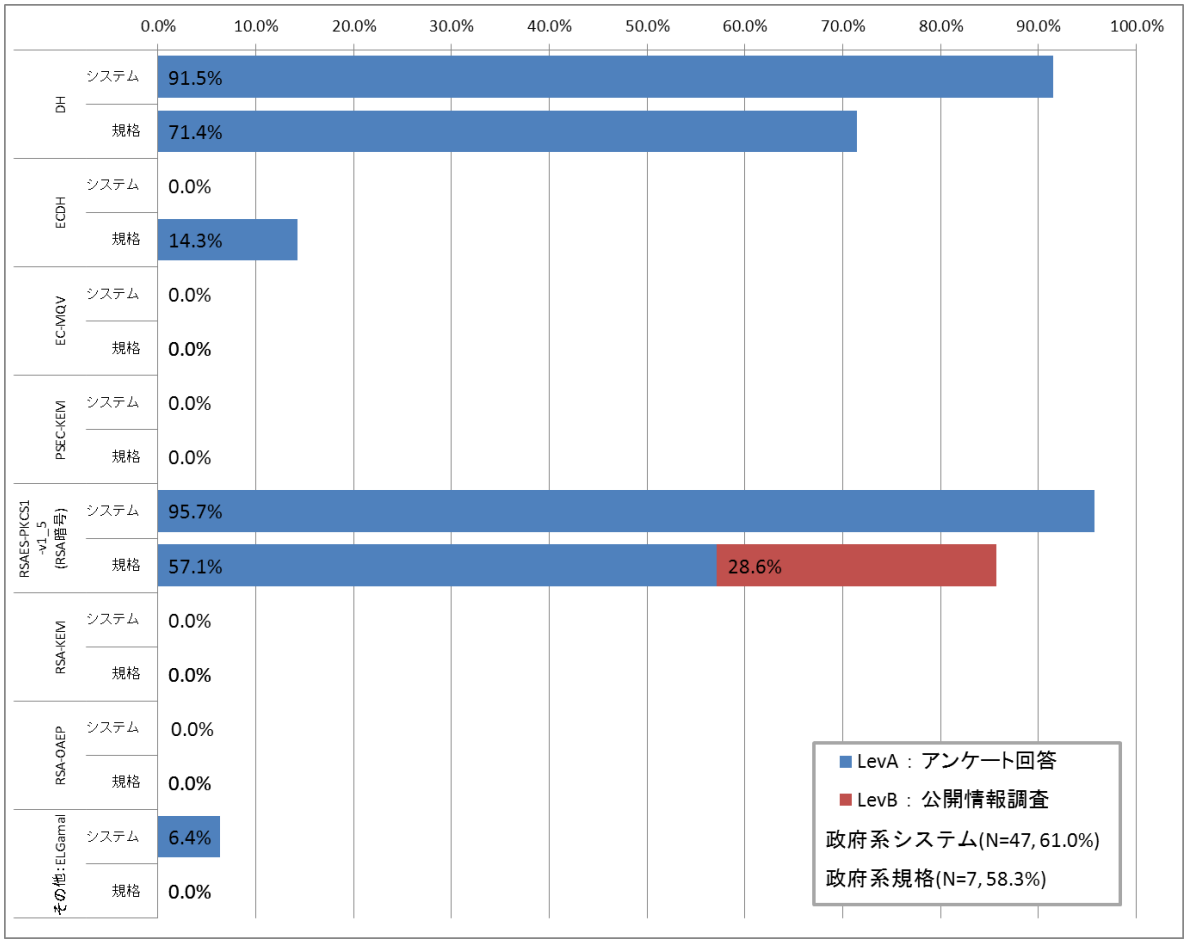

図 44 政府系システム･規格(公開鍵暗号(守秘･鍵共有))

(3) 政府系システム・規格（共通鍵暗号（64 ビットブロック暗号）

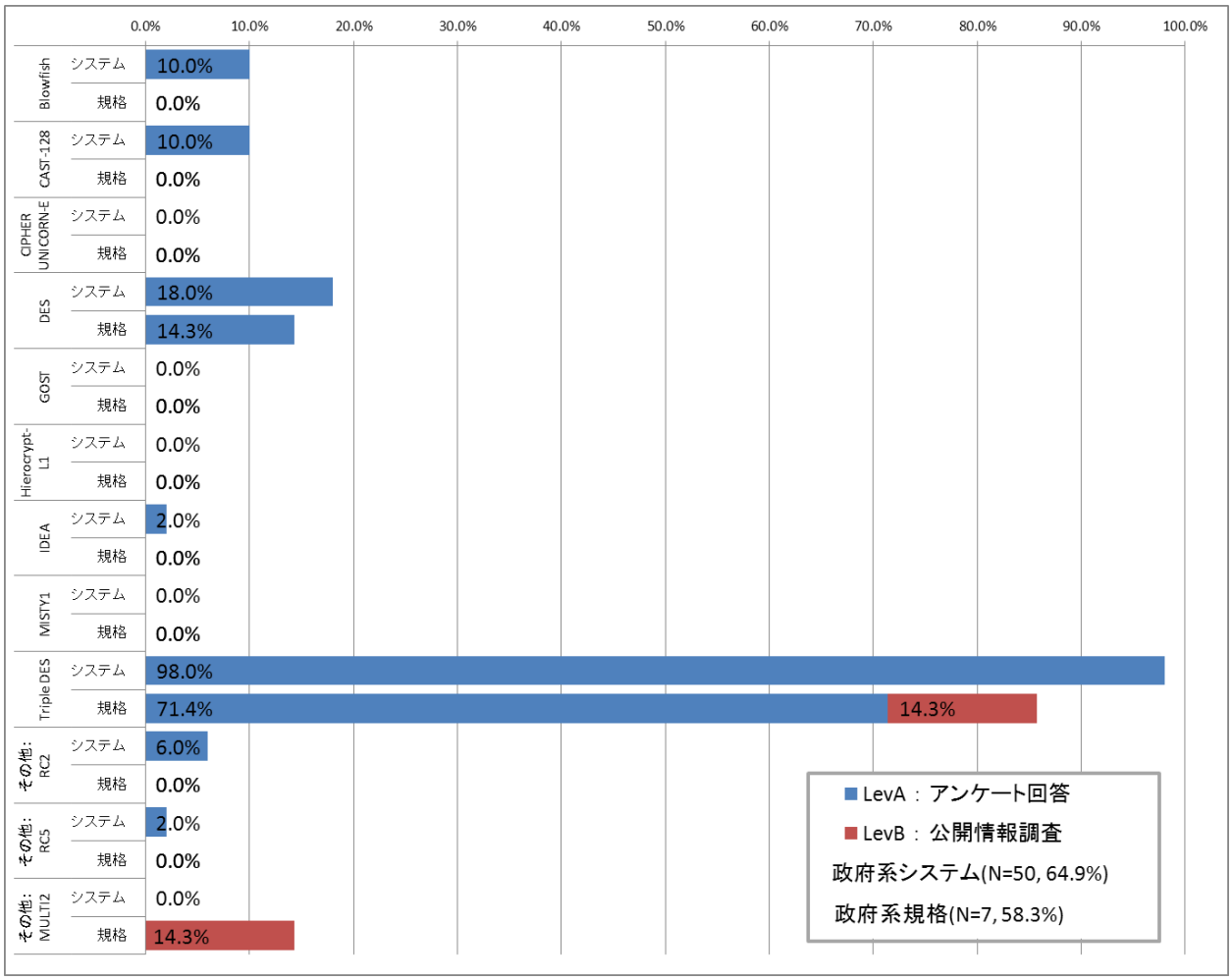

図 45 政府系システム･規格(共通鍵暗号(64 ビットブロック暗号))

(4) 政府系システム・規格（共通鍵暗号（128 ビットブロック暗号））

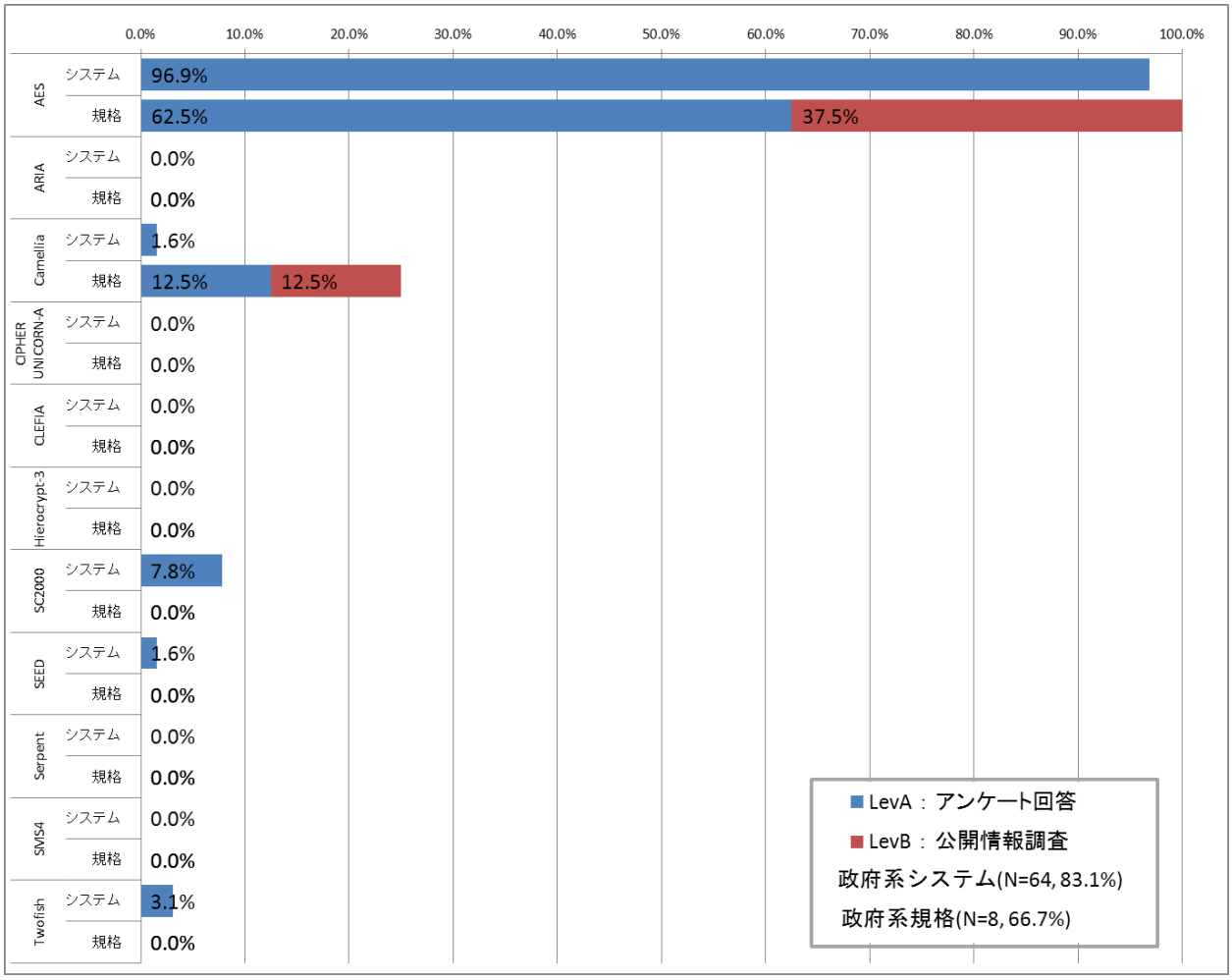

図 46 政府系システム･規格（共通鍵暗号（128 ビットブロック暗号））

(5) 政府系システム・規格（共通鍵暗号（ストリーム暗号））

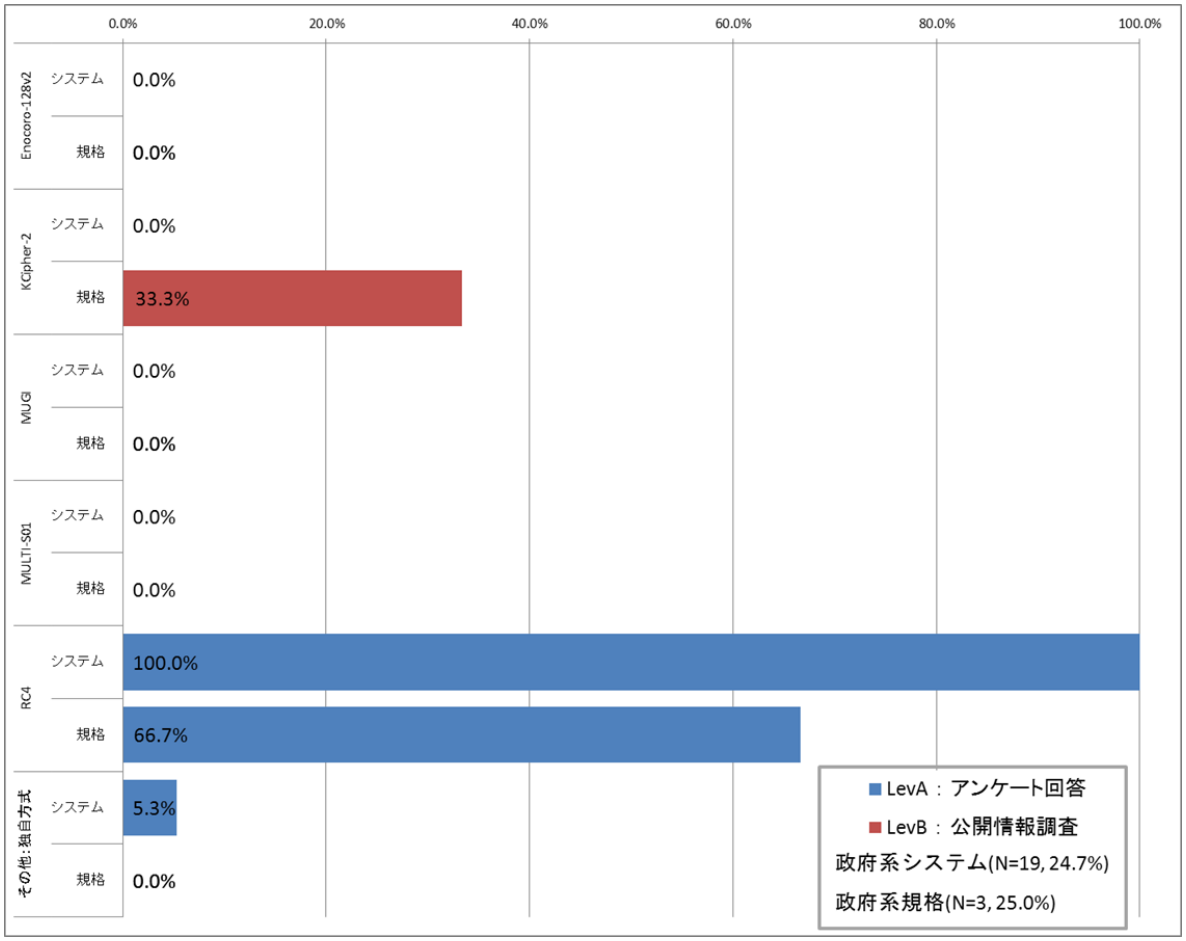

図 47 政府系システム・規格（共通鍵暗号（ストリーム暗号））

(6) 政府系システム・規格（ハッシュ関数）

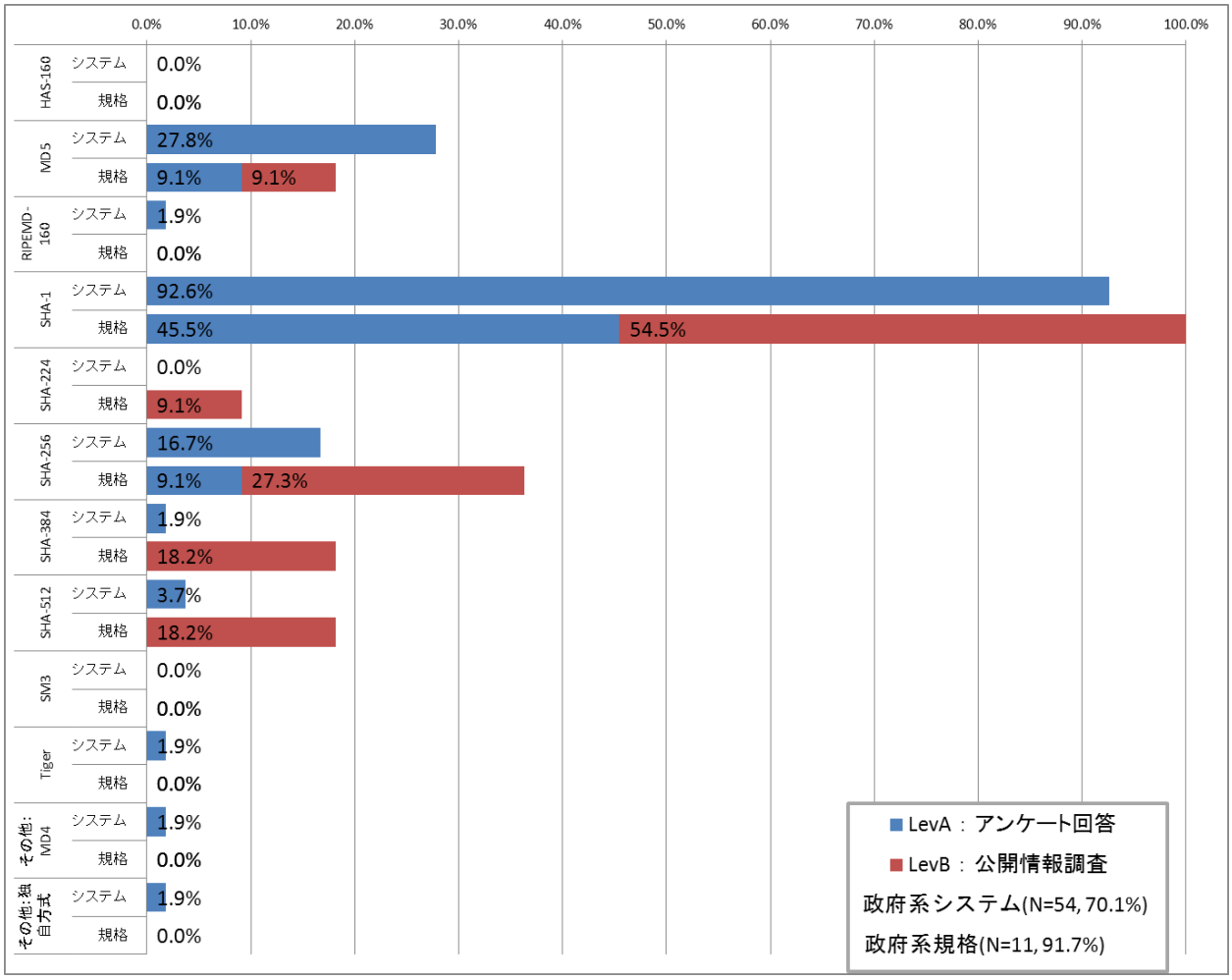

図 48 政府系システム・規格（ハッシュ関数）

(7) 政府系システム・規格（暗号利用モード）

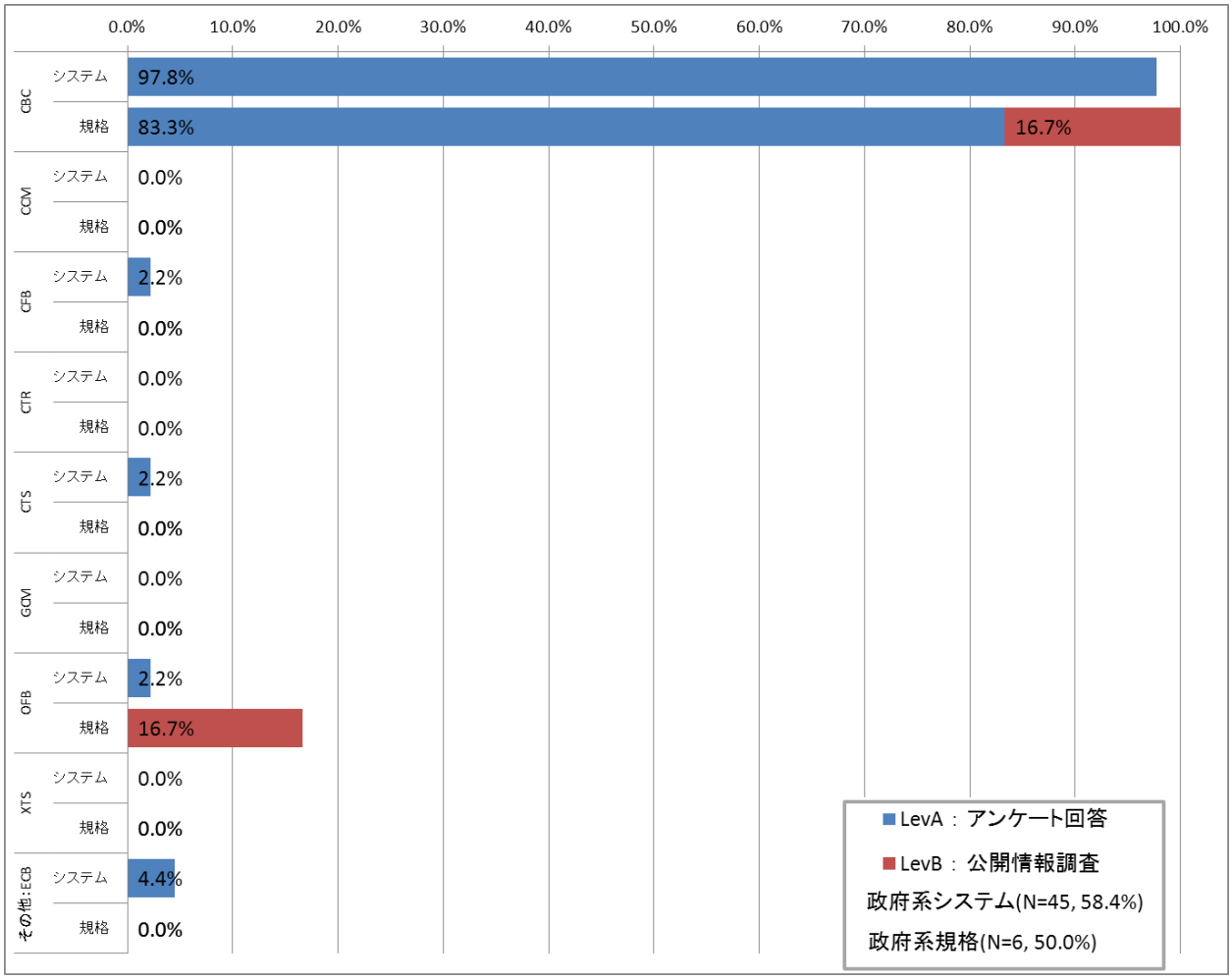

図 49 政府系システム･規格(暗号利用モード)

(8) 政府系システム・規格（メッセージ認証コード）

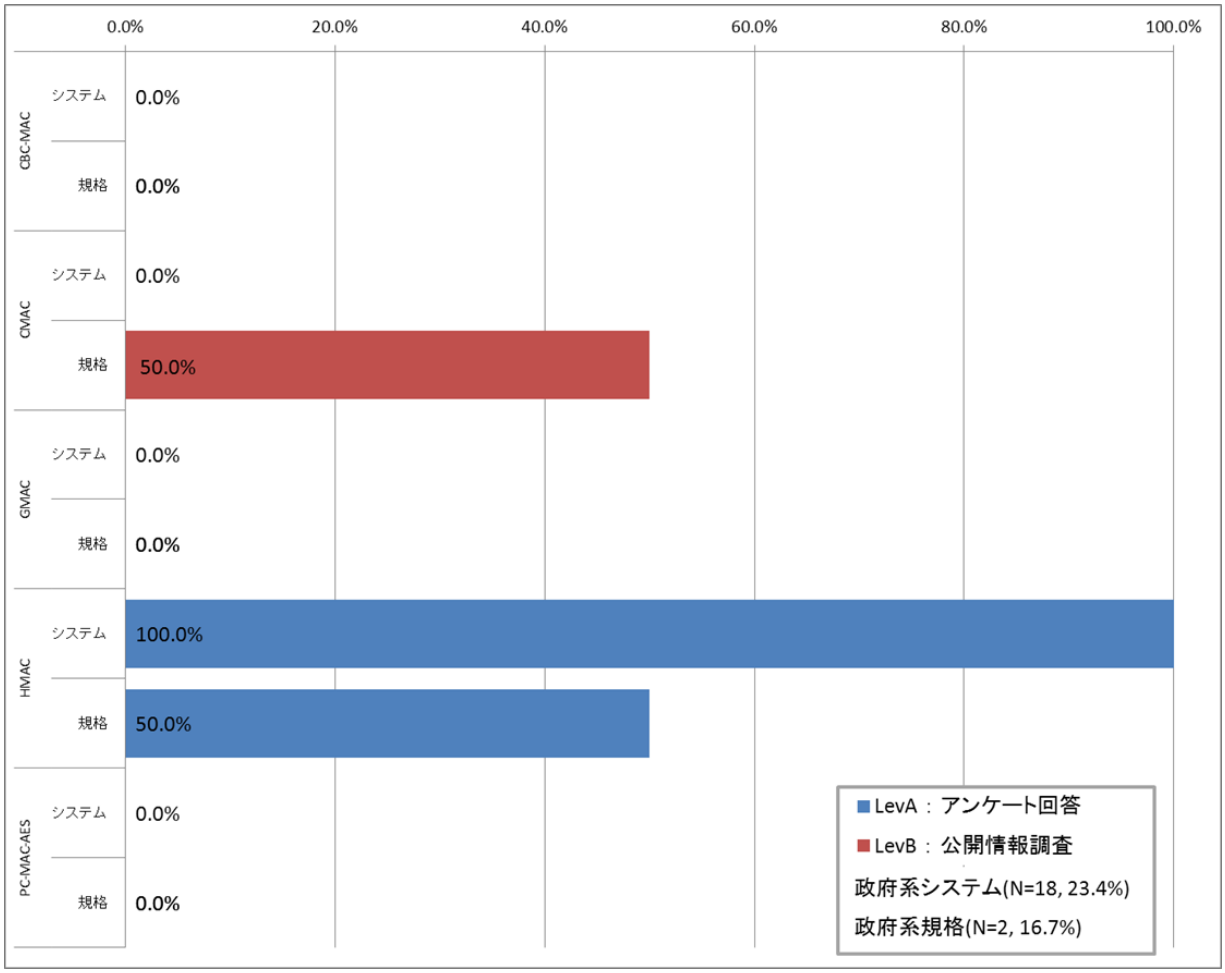

図 50 政府系システム･規格(メッセージ認証コード)

(9) 政府系システム・規格（エンティティ認証）

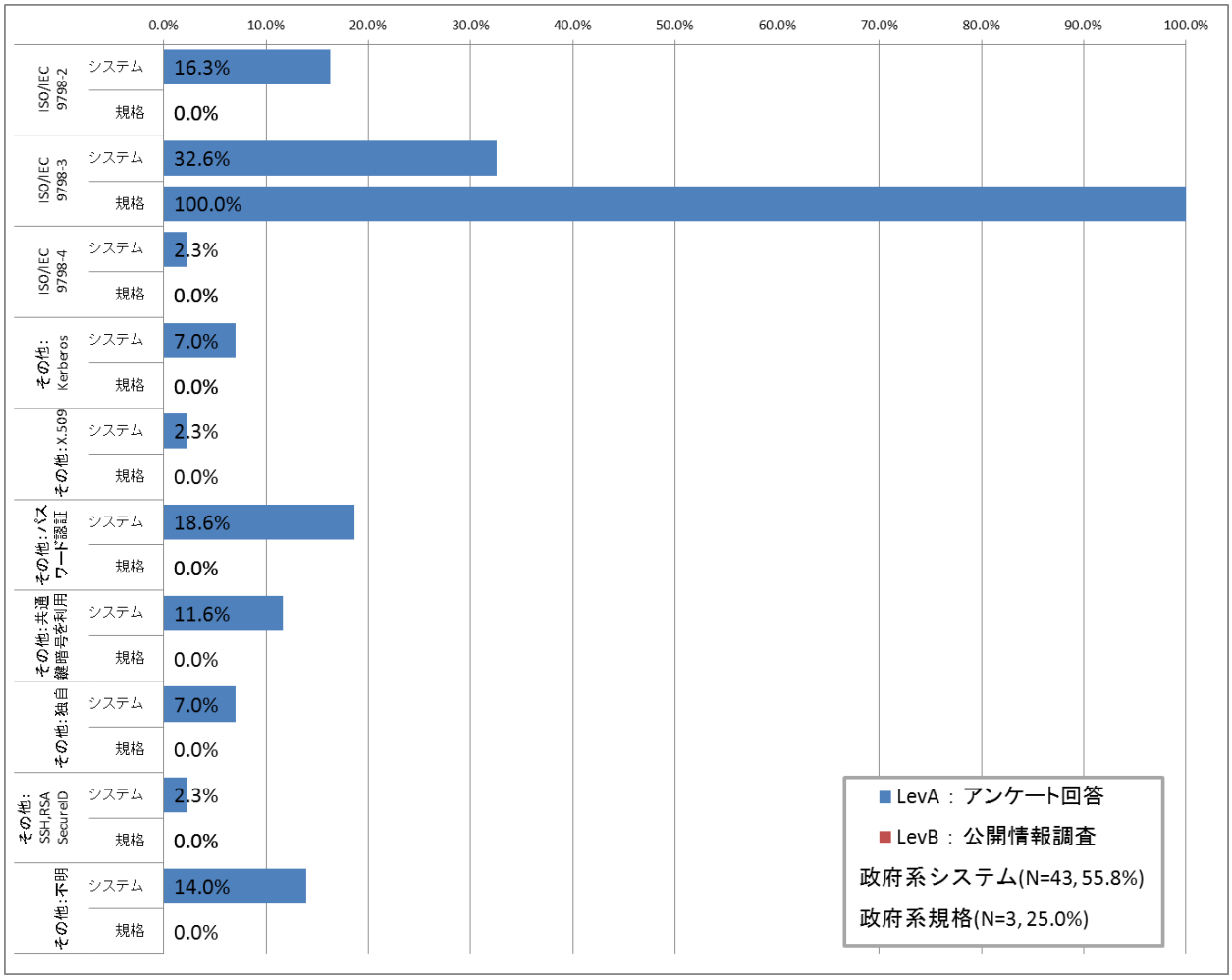

図 51 政府系システム・規格（エンティティ認証）

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）

標準規格等の調査では、国際標準規格数 12 件、国際的な民間規格数 107 件、特定団体規格数 24 件を調査した。特定団体規格数 24 件のうち、アンケート回答を得たものが 16 件、特定団体規格の公開情報調査が 8 件（6 団体）である。アンケート調査の結果、一般社団法人 電波産業会、Marlin Developer Community LLC、タイムビジネス部タイムビジネス認定センターの３団体から合計 16 規格の回答を得た（アンケート回答を得た規格は表 24 を参照）。

表 24 特定団体規格に関するアンケート回答結果（調査 D）

団体名	No	正式名称
一般社団法人 電波産業会	1	ARIB STD-T63 IMT-2000 DS-CDMA and TDD-CDMA System
	2	ARIB STD-T64 IMT-2000 MC-CDMA System （S.S0053-0: Common Cryptographic Algorithms）
	3	ARIB STD-T64 IMT-2000 MC-CDMA System （S.S0055-A: Enhanced Cryptgraphic Algorithms）
	4	ARIB STD-T64 IMT-2000 MC-CDMA System （S.S0078-B: Common Security Algorithms）
	5	ARIB STD-T94 OFDMA Broadband Mobile Wireless （Access System (WiMAXTM applied in Japan)）
	6	ARIB STD-T105 WirelessMAN-Advanced System
	7	携帯電話加入者証明書プロファイル
	8	モバイル属性証明書プロファイル
	9	暗号アルゴリズム移行におけるオペレータ認証基盤の運用ガイドライン
	10	デジタル放送におけるアクセス制御方式 ARIB STD-B25 2.2 版
	11	デジタル放送におけるダウンロード方式 ARIB STD-B45 2.2 版
	12	Forward Link Only Transport Specification ARIB STD-B48 1.1 版
	13	Forward Link Only Open Conditional Access (OpenCA) Specification ARIB STD-B50 1.1 版
Marlin Developer Community LLC	14	Marlin IPTV End-point Service System
	15	Marlin Broadband Delivery System
タイムビジネス部タイムビジネス認定センター	16	タイムビジネス信頼・安心認定制度認定基準

以下に国際標準規格、国際的な民間規格及び特定団体規格の公開情報の調査結果と特定団体規格のアンケート調査結果について報告する。なお、各暗号アルゴリズムの実数は、付録 9.調査結果表（D）を参照。

国際標準規格、国際的な民間規格及び特定団体規格の集計結果を以下に報告する。なお、国際標準規格は表 17 を、国際的な民間規格は表 18 を、特定団体規格は表 19 と表 24 を調査した結果である。下表では、特定団体規格のアンケート回答の集計結果を Lev.A、国際標準規格、国際的な民間規格、特定団体規格の公開情報調査の集計結果を Lev.B で記す。

(1) 標準規格・民間規格（公開鍵暗号（署名））

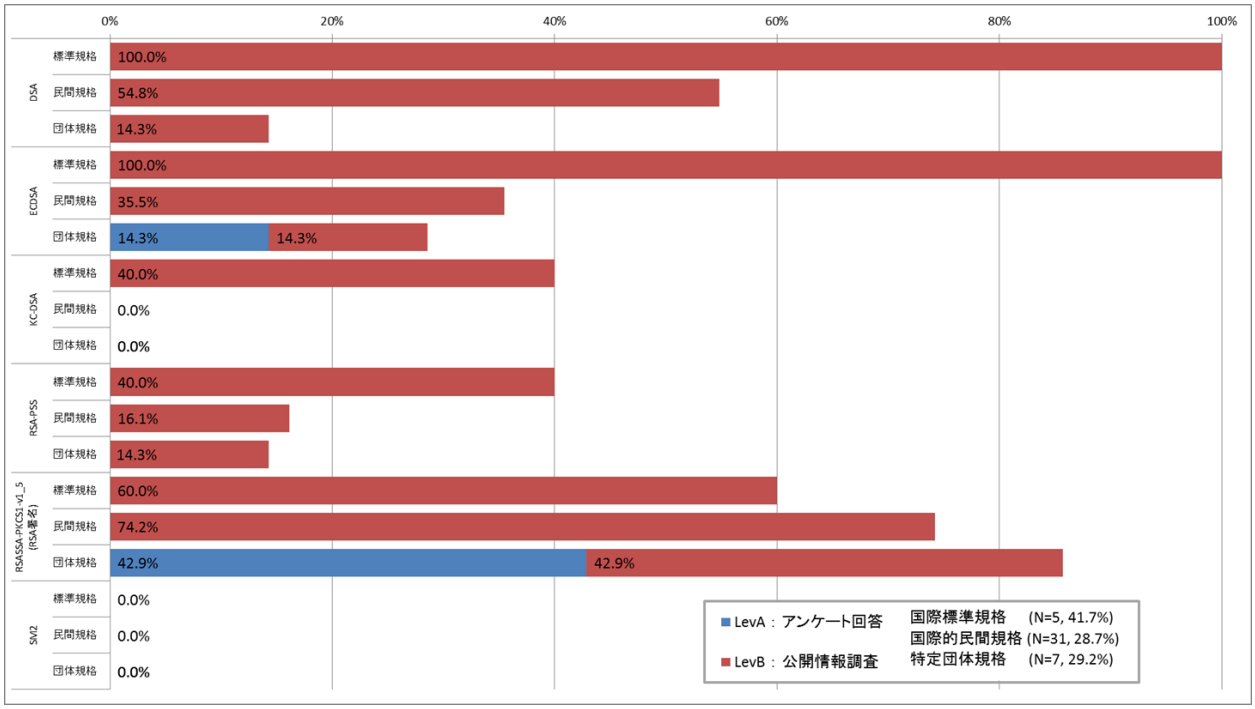

図 52 標準規格・民間規格（公開鍵暗号(署名)）

(2) 標準規格・民間規格（公開鍵暗号（守秘・鍵共有））

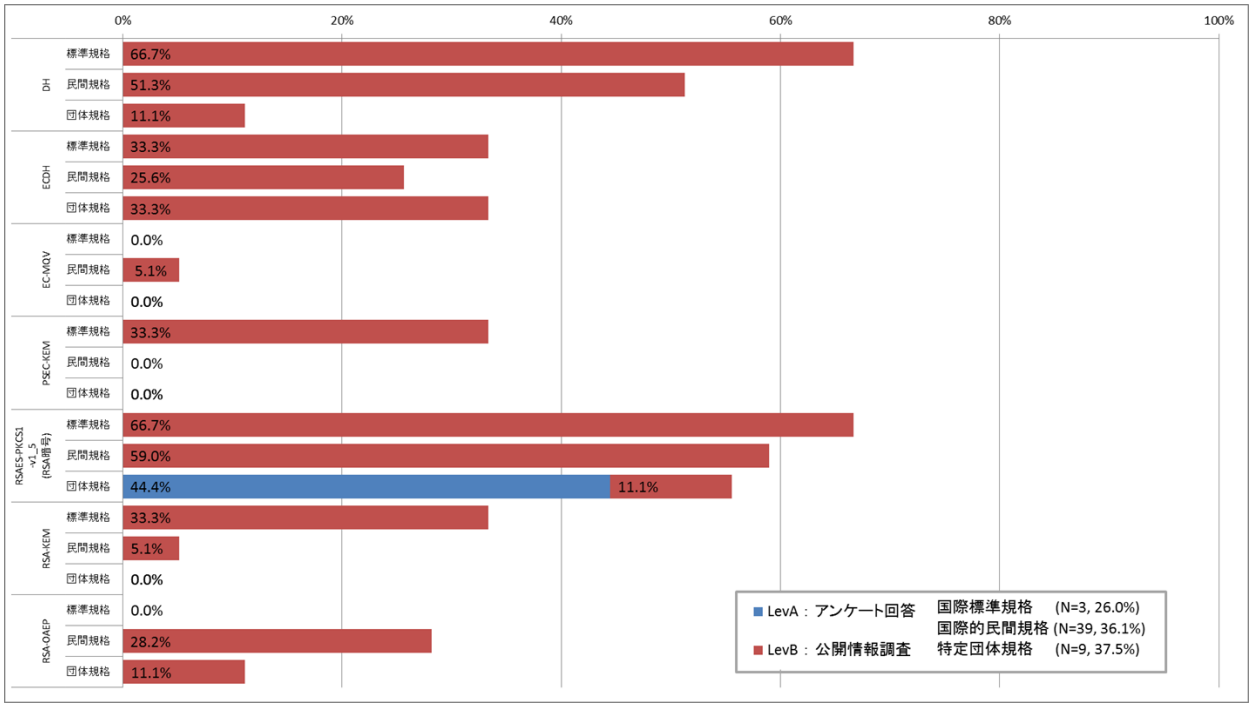

図 53 標準規格・民間規格（公開鍵暗号(守秘･鍵共有)）

(3) 標準規格・民間規格（共通鍵暗号（64 ビットブロック暗号））

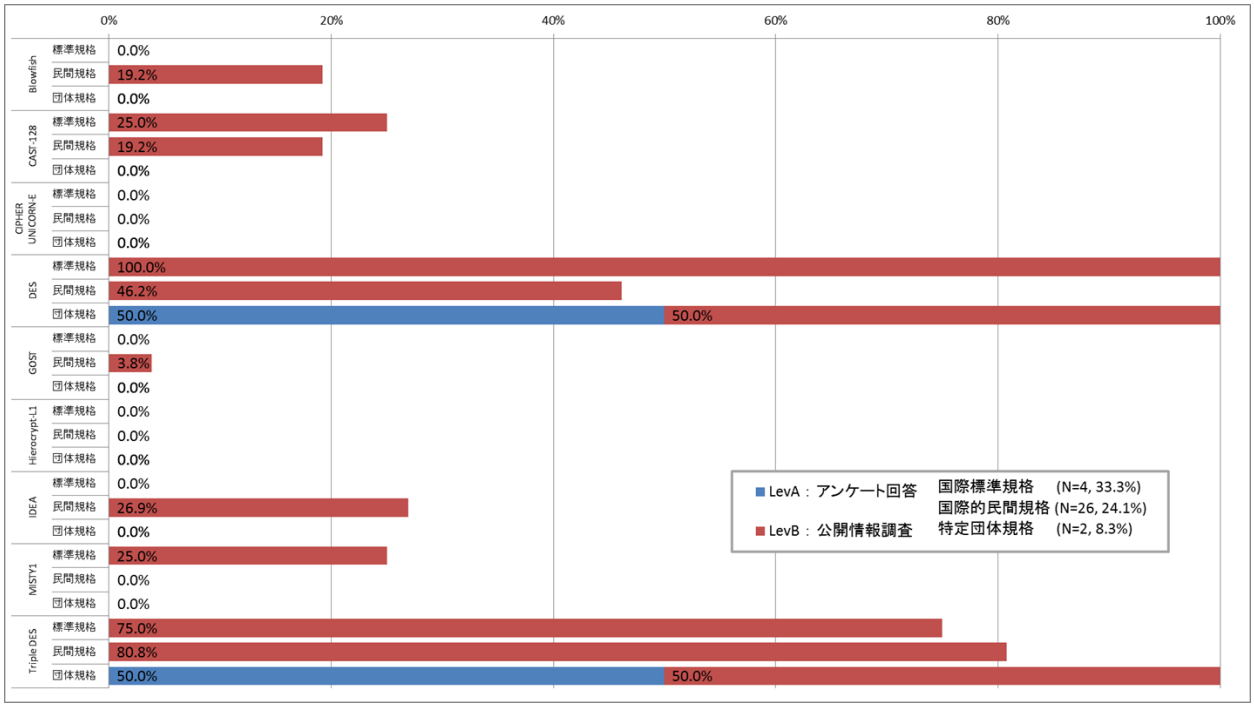

図 54 標準規格・民間規格（共通鍵暗号(64 ビットブロック暗号)）

(4) 標準規格・民間規格（共通鍵暗号（128 ビットブロック暗号））

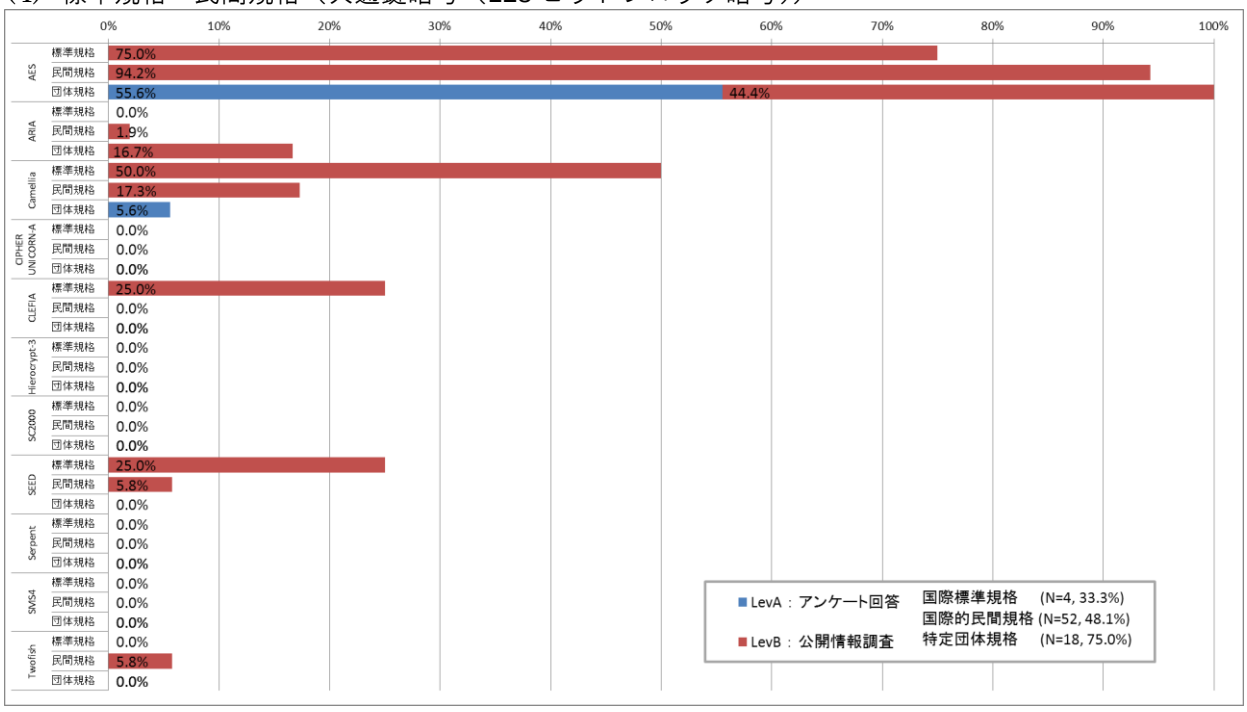

図 55 標準規格・民間規格（共通鍵暗号(128 ビットブロック暗号)）

(5) 標準規格・民間規格（共通鍵暗号（ストリーム暗号））

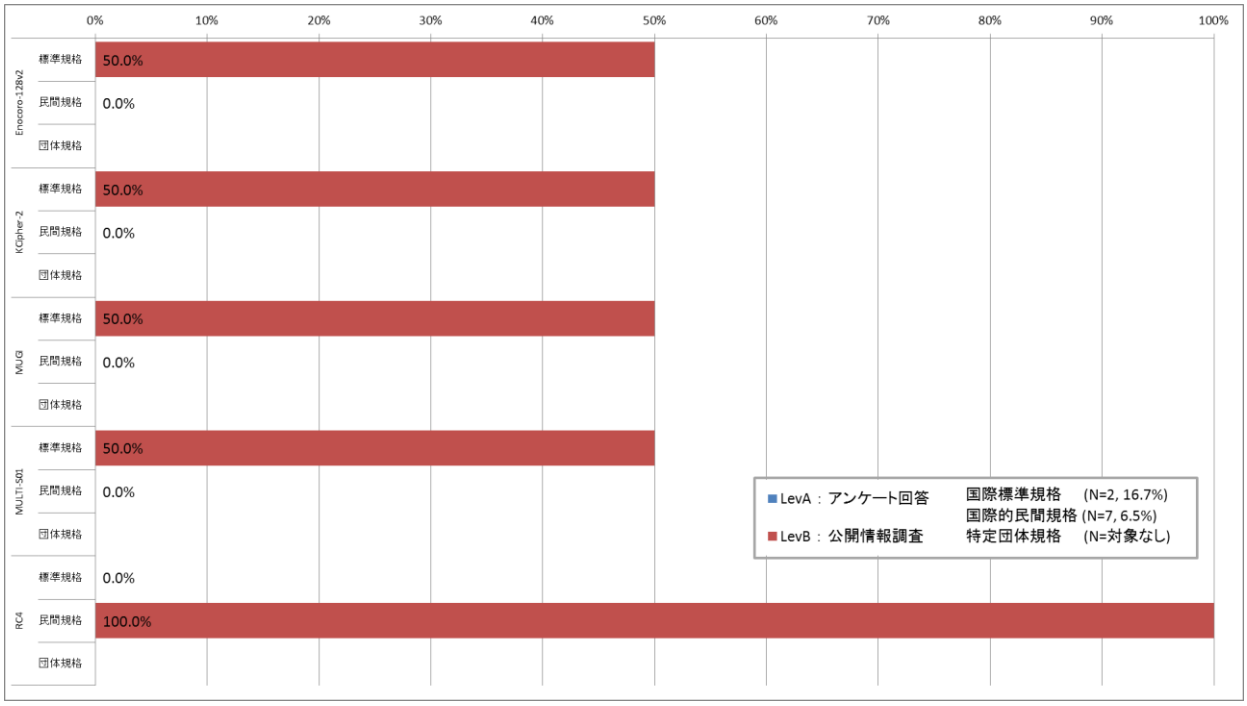

図 56 標準規格・民間規格（共通鍵暗号(ストリーム暗号)）

(6) 標準規格・民間規格（ハッシュ関数）

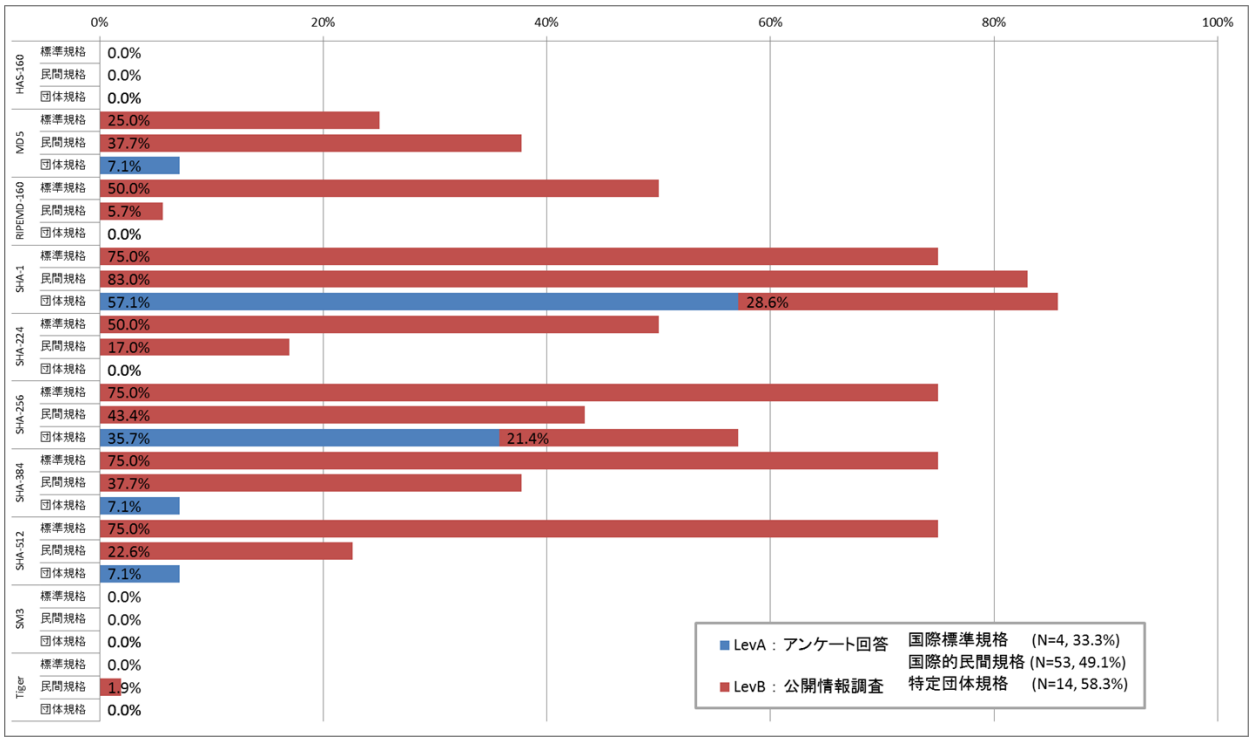

図 57 標準規格・民間規格（ハッシュ関数）

(7) 標準規格・民間規格（暗号利用モード）

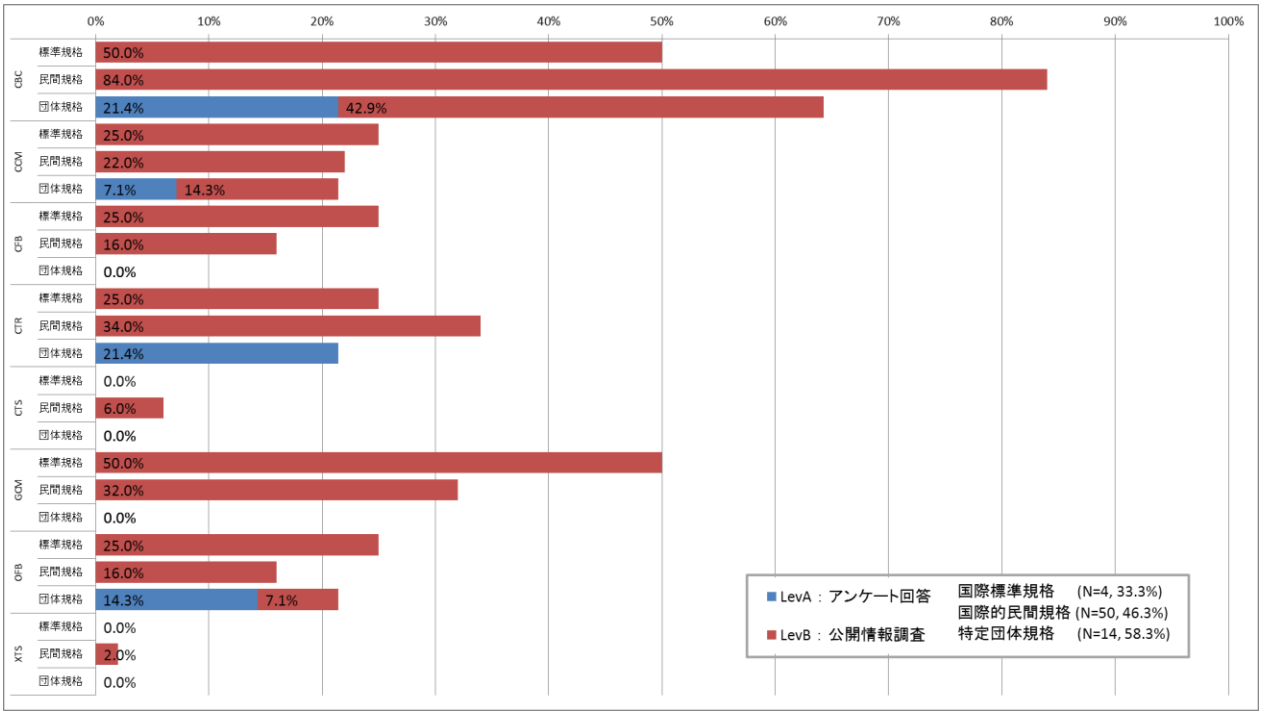

図 58 標準規格・民間規格（暗号利用モード）

(8) 標準規格・民間規格（メッセージ認証コード）

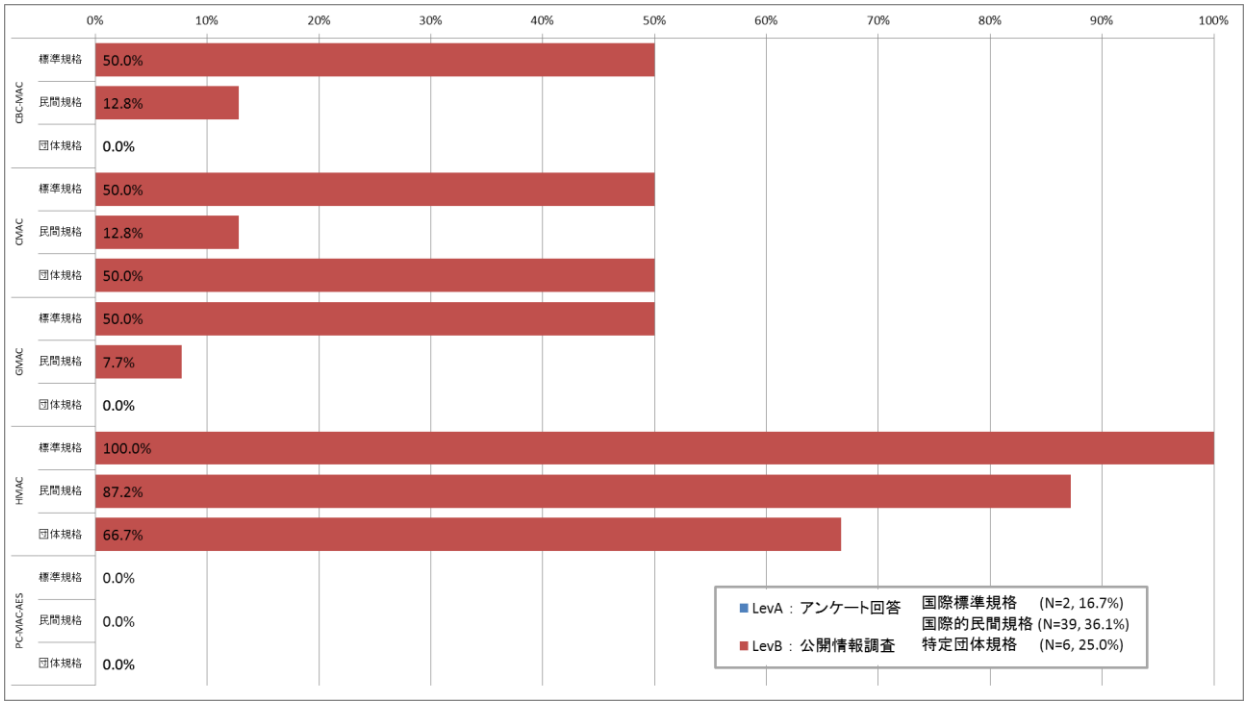

図 59 標準規格・民間規格（メッセージ認証コード）

(9) 標準規格・民間規格（エンティティ認証）

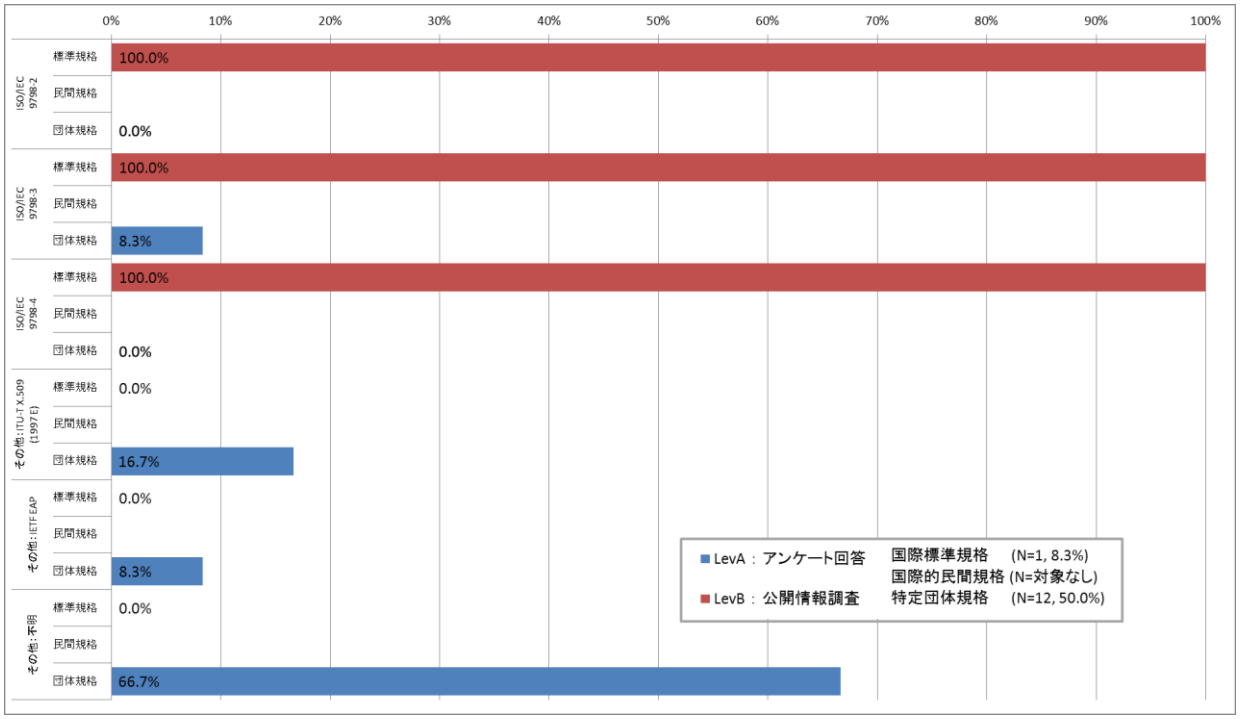

図 60 標準規格・民間規格（エンティティ認証）

3.5　オープンソースプロジェクト調査結果（調査 E 結果）

オープンソースプロジェクト調査では、表 21 で示す合計 24 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なった。以下に集計結果を報告する。

なお、オープンソースプロジェクト全体を「OSS 総合」、Linux, Debian, FreeBSD, Android, NSS, OpenSSL, GnuPG, Mcrypt を「OSS 暗号モジュール」として集計した。ただし、集計に際し、以下の項目を考慮する。また、各暗号アルゴリズムの実数は、付録 10.調査結果表(E)を参照。

- Linux 及び Debian は、両方に実装されている場合でも 1 と集計
- Thunderbird、Firefox、及び NSS は、それらのうちの複数に実装されている場合でも 1 と集計
- Qmail 及び OpenSSL は、両方に実装されている場合でも 1 と集計
- 応募者からの情報があっても、本調査で調査者が確認できなかったものは当該ソースコードについて対象外とする
- 重複集計を避けるため、他オープンソースプロジェクト管理のソースコードが組み込まれていた場合、当該ソースコードについては対象外とする
  例えば、Android では、以下のメイン(/libcore/luni/src/main/)ではない、external 直下のフォルダに Camellia が存在するが、Android については Camellia が搭載されているとは認めない。
  「/external/bouncycastle/, /external/ipsec-tools/, /external/openssl/crypto/evp/」
- 搭載検討中になっているソースコードは対象外とする
- エンティティ認証は、ISO/IEC9798 等の明示がないため、対象外とする

(1) オープンソースプロジェクト(公開鍵暗号（署名))

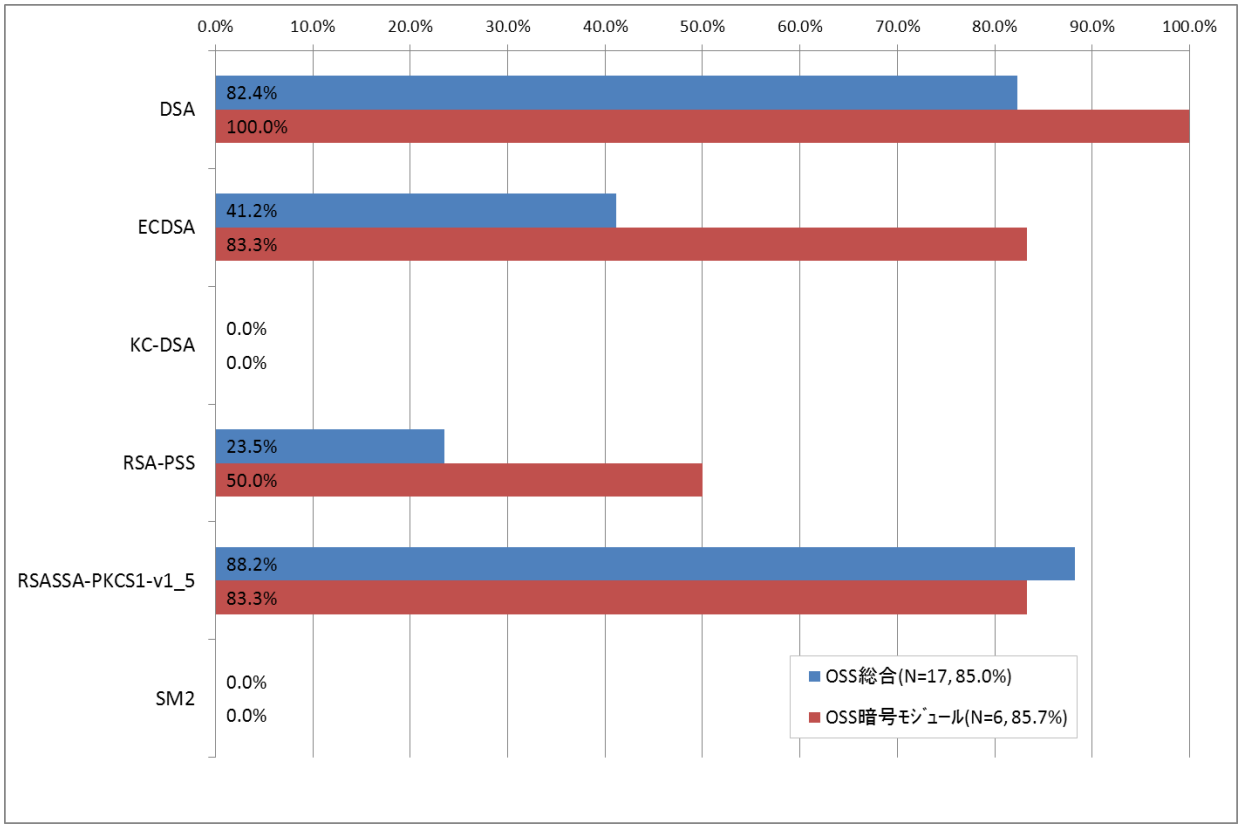

図 61 オープンソースプロジェクト（公開鍵暗号(署名)）

(2) オープンソースプロジェクト(公開鍵暗号（守秘・鍵共有))

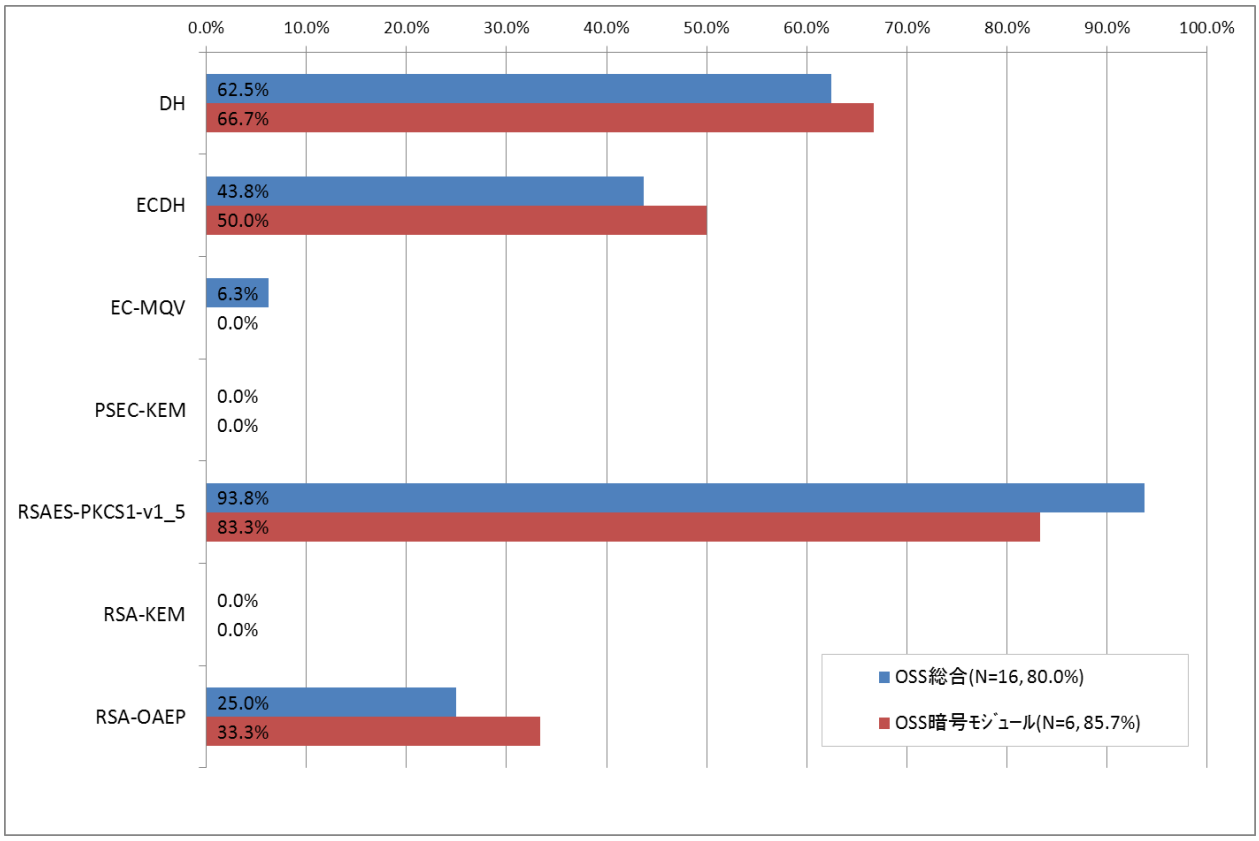

図 62 オープンソースプロジェクト（公開鍵暗号(守秘･鍵共有))

(3) オープンソースプロジェクト(共通鍵暗号（64 ビットブロック暗号))

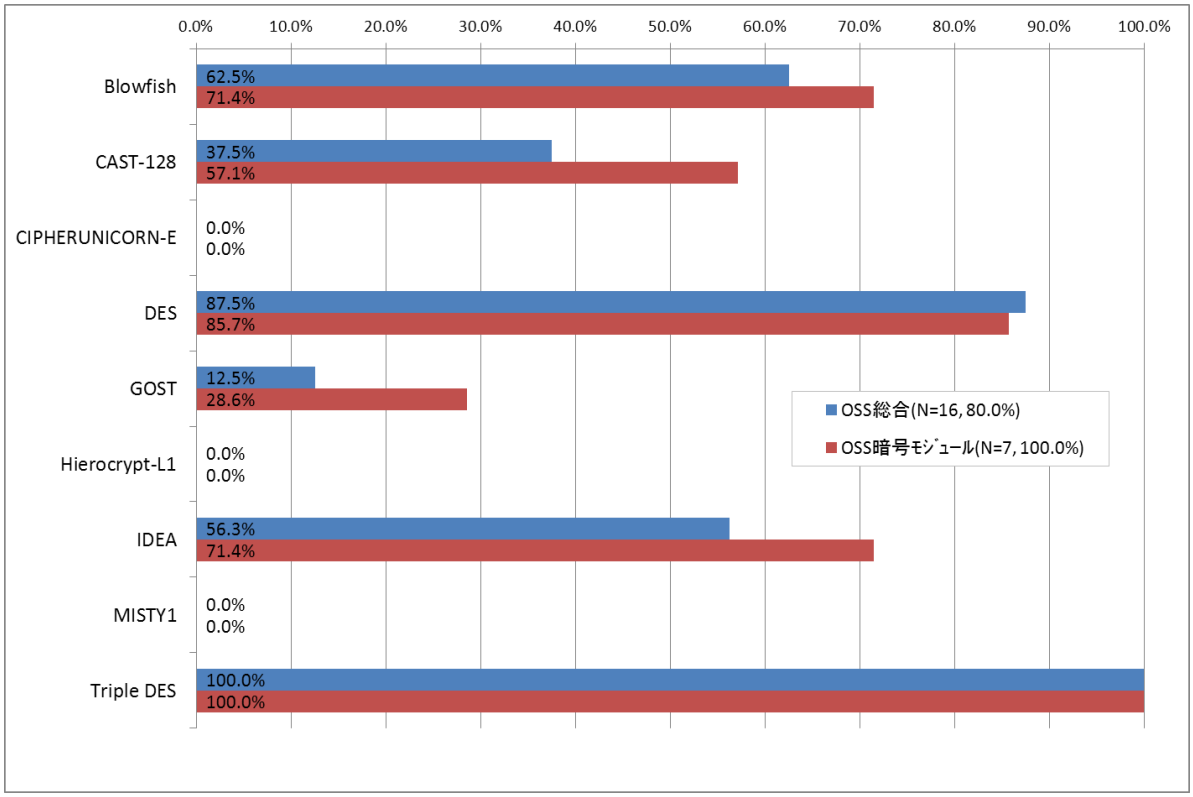

図 63 オープンソースプロジェクト（共通鍵暗号(64 ビットブロック暗号))

(4) オープンソースプロジェクト(共通鍵暗号（128 ビットブロック暗号))

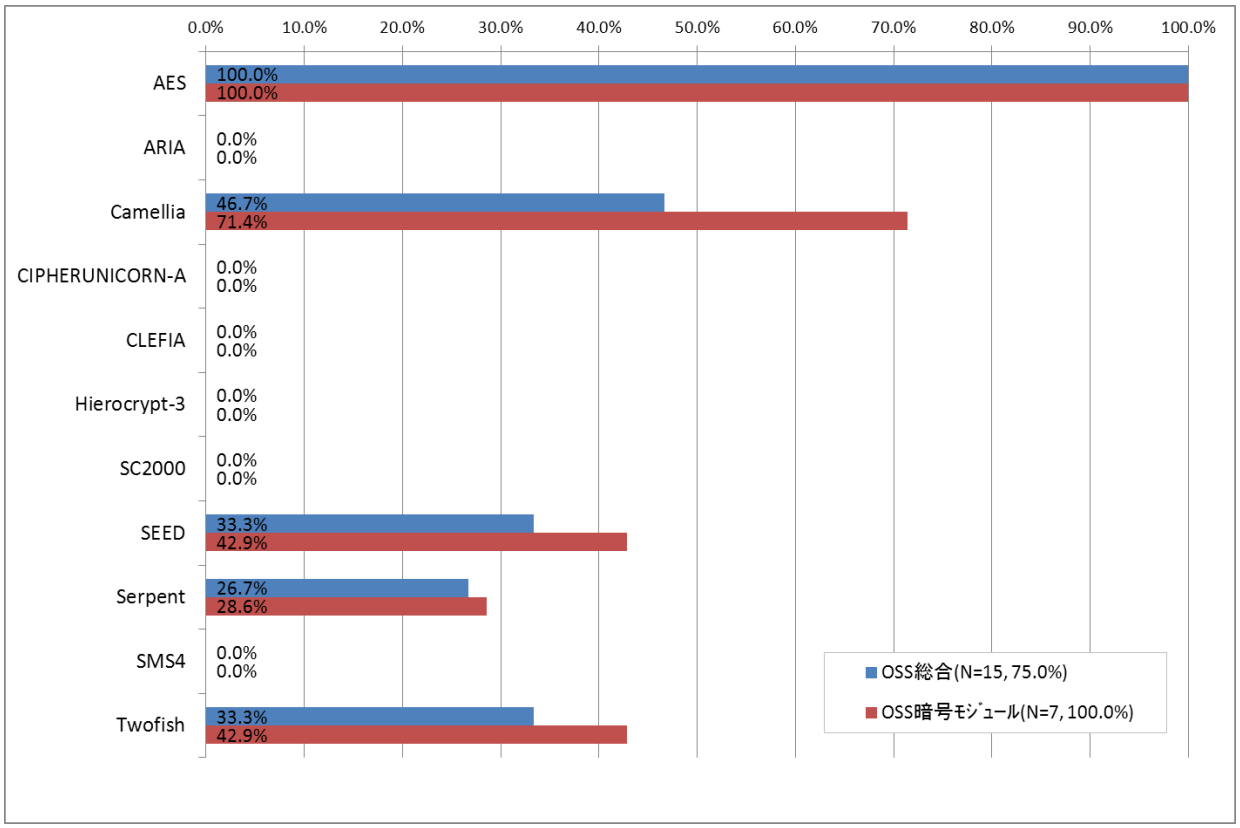

図 64 オープンソースプロジェクト（共通鍵暗号(128 ビットブロック暗号))

(5) オープンソースプロジェクト(共通鍵暗号（ストリーム暗号))

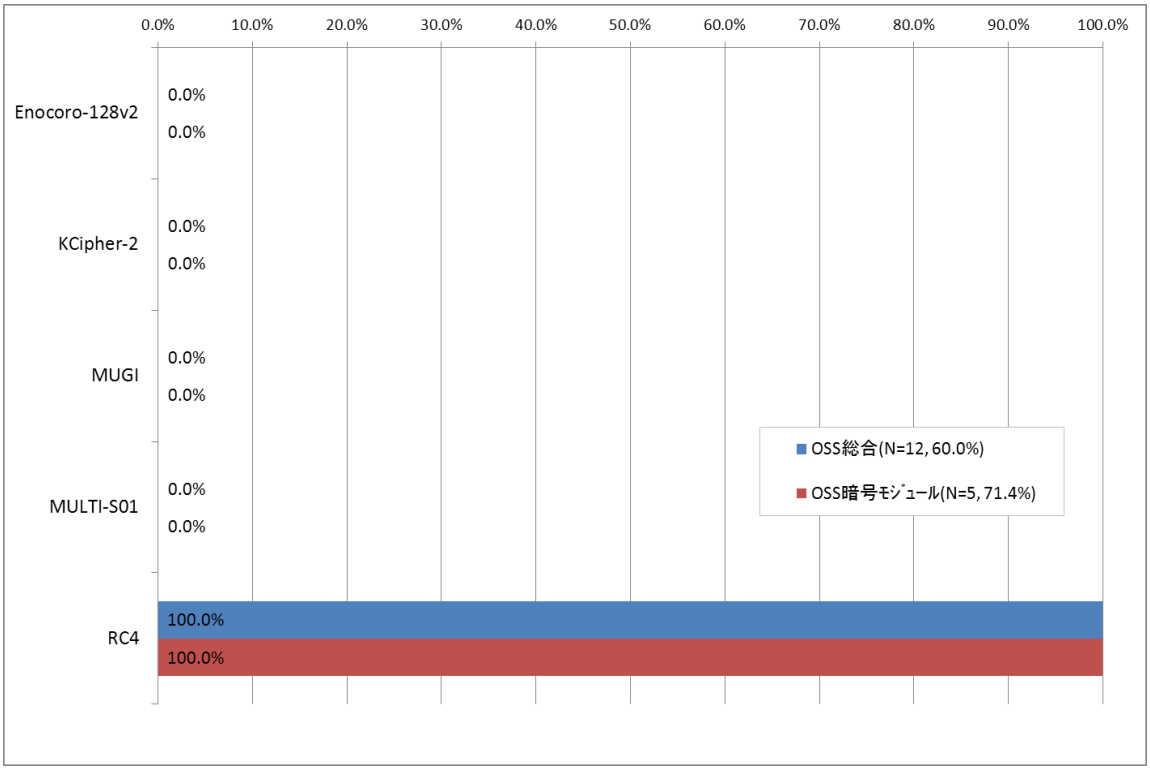

図 65 オープンソースプロジェクト（共通鍵暗号(ストリーム暗号))

(6) オープンソースプロジェクト(ハッシュ関数)

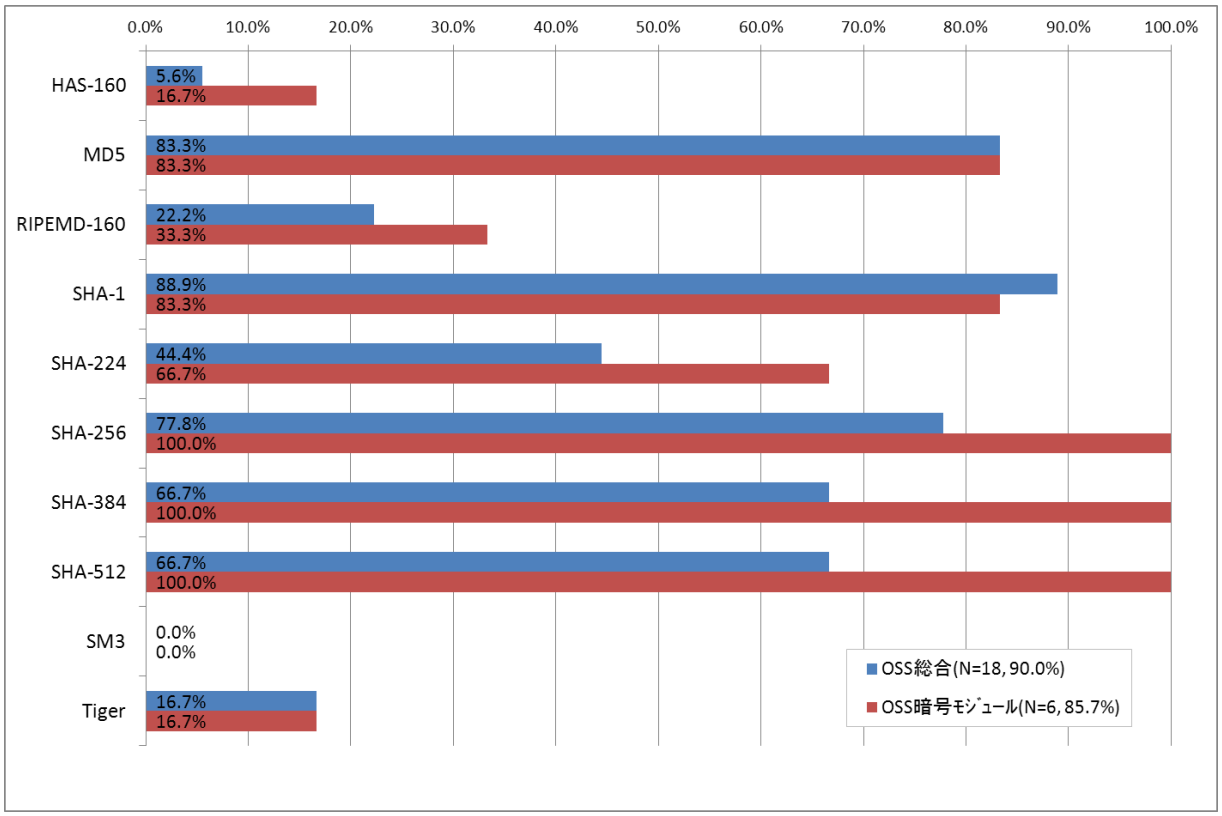

図 66 オープンソースプロジェクト (ハッシュ関数)

(7) オープンソースプロジェクト(暗号利用モード)

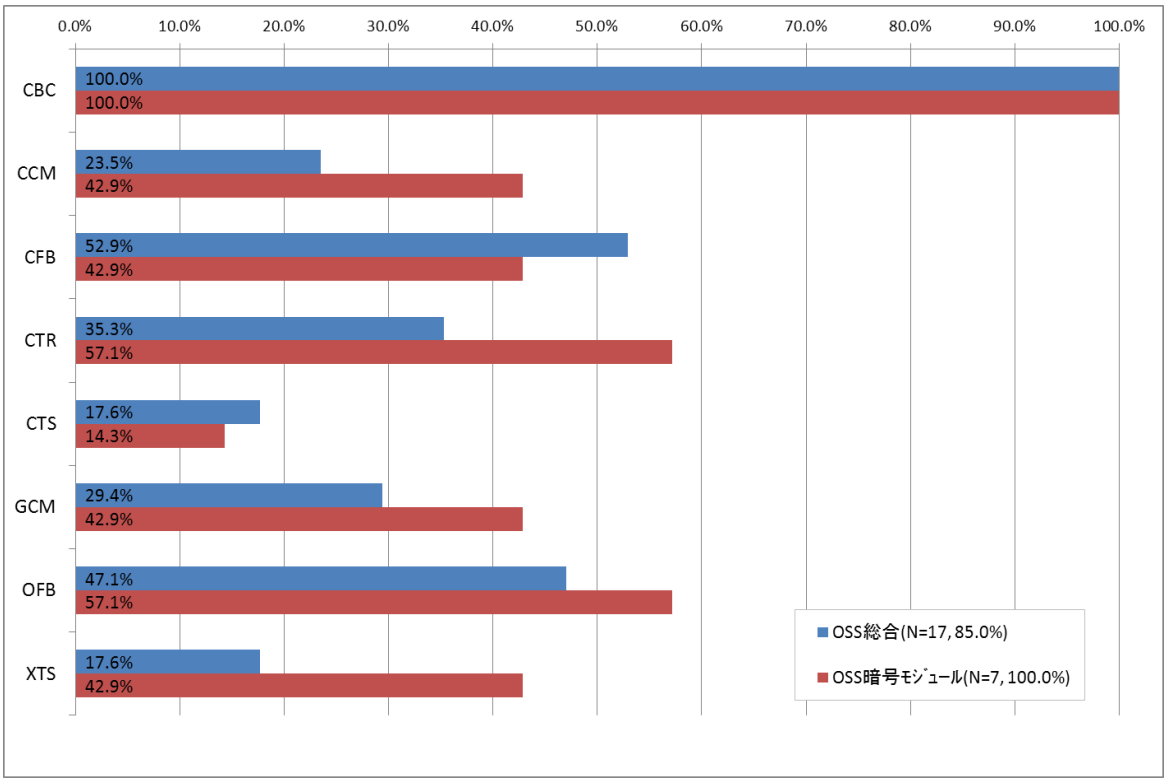

図 67 オープンソースプロジェクト (暗号利用モード)

(8) オープンソースプロジェクト(メッセージ認証コード)

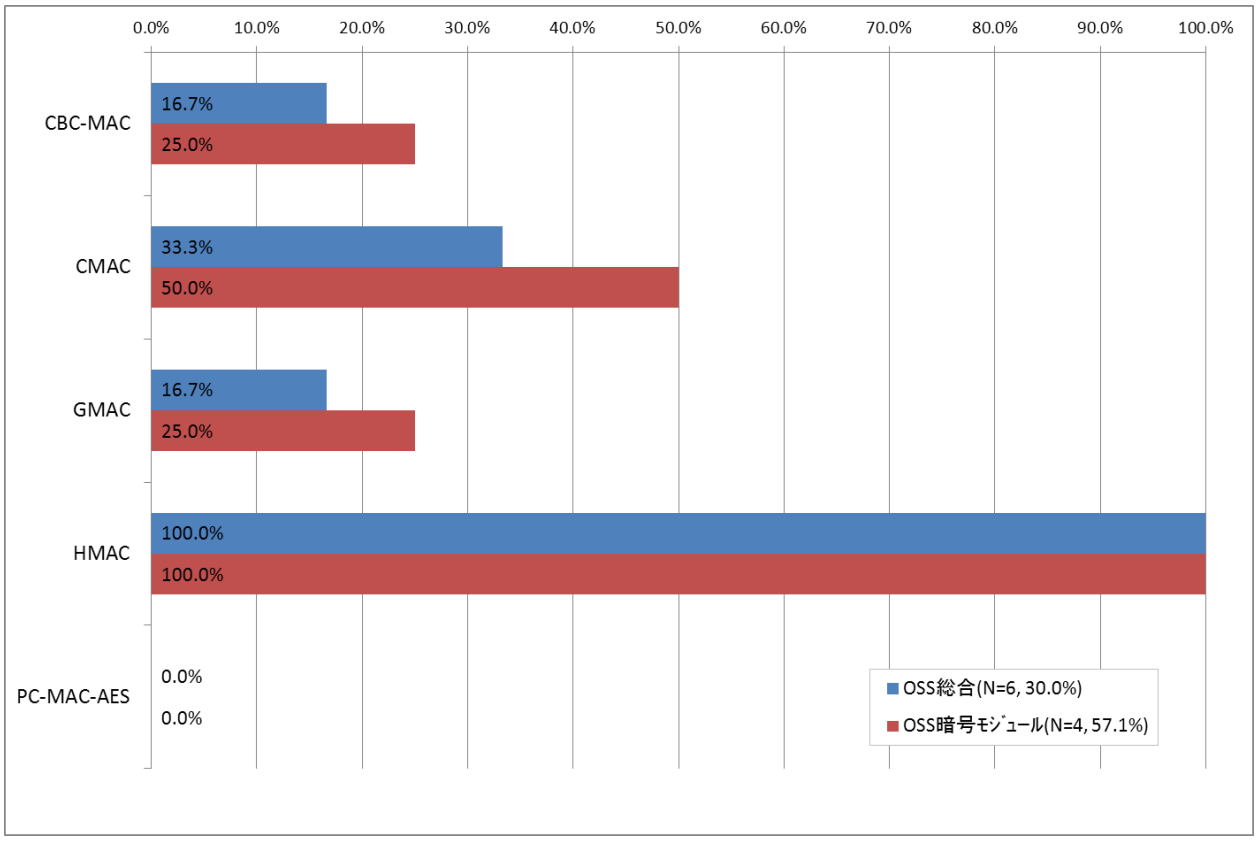

図 68 オープンソースプロジェクト（メッセージ認証コード）

4. まとめ

本調査では、次期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、9 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、市販製品のアンケート調査として、1,849 社にアンケート配布し、うち有効回答社数：127 社から得た 443 製品・システムについて調査を実施した。また、公開情報調査では、35 社、90 製品について調査を実施した。アンケート調査と公開情報調査を含め、合計 156 社、533 製品・システムの利用実績を調査した。
- 調査 C では、政府系情報システムでの利用実績はアンケート調査で 77 件、政府系情報システム規格の利用・推奨実績はアンケート調査で 5 件、公開情報調査で 7 件について調査を実施した。
- 調査 D では、国際標準規格の調査件数 12 件、国際的な民間規格は 107 件、特定団体規格のアンケート調査では 3 団体から 16 件、及び公開情報調査件数 8 件（6 団体）について調査を実施した。
- 調査 E では、オープンソースプロジェクトについては、24 件のオープンソースプロジェクト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が高い上位、3 位までの暗号アルゴリズムを報告する。なお、応募暗号については下線で示す。

(1) 公開鍵暗号（署名）の結果

表 25 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）	総合	RSASSA-PKCS_v1_5	80.6%	DSA	44.7%	ECDSA	28.2%
	暗号モジュール	RSASSA-PKCS_v1_5	84.7%	DSA	58.3%	ECDSA	51.4%
政府系情報システム調査結果（調査C）	システム	RSASSA-PKCS_v1_5	100.0%	DSA	85.1%	RSA-PSS	4.3%
	規格	RSASSA-PKCS_v1_5	100.0%	DSA	66.6%	ECDSA	22.2%
標準規格等調査結果（調査D）	国際標準	DSA, ECDSA	100.0%	RSASSA-PKCS_v1_5	60.0%	–	–
	国際的民間規格	RSASSA-PKCS_v1_5	74.2%	DSA	54.8%	ECDSA	35.5%
	特定団体規格	RSASSA-PKCS_v1_5	42.9%	ECDSA	28.6%	DSA, RSA-PSS	14.3%
OSS調査結果（調査E）	総合	RSASSA-PKCS_v1_5	88.2%	DSA	82.4%	ECDSA	41.2%
	暗号モジュール	DSA	100.0%	ECDSA, RSASSA-PKCS_v1_5	83.3%	–	–

(2) 公開鍵暗号（守秘・鍵共有）の結果

表 26 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）	総合	DH	61.5%	RSAES-PKCS_v1_5	47.9%	RSA-OAEP	15.5%
	暗号モジュール	DH	66.5%	RSAES-PKCS_v1_5, RSA-OAEP	59.1%	–	–
政府系情報システム調査結果（調査C）	システム	RSAES-PKCS_v1_5	95.7%	DH	91.5%	その他: ElGamal	6.4%
	規格	RSAES-PKCS_v1_5	85.7%	DH	71.4%	ECDH	14.3%
標準規格等調査結果（調査D）	国際標準	RSAES-PKCS_v1_5, DH	66.7%	ECDH, PSEC-KEM, RSA-KEM	33.3%	–	–
	国際的民間規格	RSAES-PKCS_v1_5	59.0%	DH	51.3%	RSA-OAEP	28.2%
	特定団体規格	RSAES-PKCS_v1_5	44.4%	ECDH	33.3%	DH, RSA-OAEP	11.1%
OSS調査結果（調査E）	総合	RSAES-PKCS_v1_5	93.8%	DH	62.5%	ECDH	43.8%
	暗号モジュール	RSAES-PKCS_v1_5	83.3%	DH	66.7%	ECDH	50.0%

(3) 共通鍵暗号（64 ビットブロック暗号）の結果

表 27 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）	総合	Triple DES	70.2%	DES	62.9%	Blowfish	16.5%
	暗号モジュール	Triple DES	76.6%	DES	64.9%	CAST-128	11.7%
政府系情報システム調査結果（調査C）	システム	Triple DES	98.0%	DES	18.0%	Blowfish, CAST-128	10.0%
	規格	Triple DES	85.7%	DES, その他: MULTI2	14.3%	–	–
標準規格等調査結果（調査D）	国際標準	DES	100.0%	Triple DES	75.0%	CAST-128, MISTY1	25.0%
	国際的民間規格	Triple DES	80.8%	DES	46.2%	IDEA	26.9%
	特定団体規格	DES, Triple DES	50.0%	–	–	–	–
OSS調査結果（調査E）	総合	Triple DES	100.0%	DES	87.5%	Blowfish	62.5%
	暗号モジュール	Triple DES	100.0%	DES	85.7%	IDEA	71.4%

(4) 共通鍵暗号（128 ビットブロック暗号）の結果

表 28 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）	総合	AES	95.4%	Camellia	13.7%	SEED	8.6%
	暗号モジュール	AES	98.0%	Camellia	27.3%	SEED	18.2%
政府系情報システム調査結果（調査C）	システム	AES	96.9%	SC2000	7.8%	Twofish	3.1%
	規格	AES	100.0%	Camellia	25.0%	–	–
標準規格等調査結果（調査D）	国際標準	AES	75.0%	Camellia	50.0%	CLEFIA, SEED	25.0%
	国際的民間規格	AES	94.2%	Camellia	25.0%	SEED	5.8%
	特定団体規格	AES	55.6%	ARIA	16.7%	Camellia	5.6%
OSS調査結果（調査E）	総合	AES	100.0%	Camellia	46.7%	SEED, Twofish	33.3%
	暗号モジュール	AES	100.0%	Camellia	71.4%	SEED, Twofish	42.9%

(5) 共通鍵暗号（ストリーム暗号）の結果

表 29 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）	総合	RC4	79.6%	KCipher-2	10.2%	その他: 独自	5.7%
	暗号モジュール	RC4	70.5%	MULTI-S01	13.6%	その他: 独自	9.1%
政府系情報システム調査結果（調査C）	システム	RC4	100.0%	–	–	–	–
	規格	RC4	66.7%	KCipher-2	33.3%	その他: 独自	5.3%
標準規格等調査結果（調査D）	国際標準	Enocoro-128v2, KCipher-2, MUGI, MULTI-S01	50.0%	–	–	–	–
	国際的民間規格	RC4	100.0%	–	–	–	–
	特定団体規格	–	–	–	–	–	–
OSS調査結果（調査E）	総合	RC4	100.0%	–	–	–	–
	暗号モジュール	RC4	100.0%	–	–	–	–

(6) ハッシュ関数の結果

表 30 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）	総合	SHA-1	85.1%	SHA-256	61.7%	MD5	57.1%
	暗号モジュール	SHA-1	96.1%	SHA-256	88.3%	SHA-256	74.0%
政府系情報システム調査結果（調査C）	システム	SHA-1	92.6%	MD5	27.8%	SHA-256	16.7%
	規格	SHA-1	100.0%	SHA-256	36.4%	MD5, SHA-384, SHA-512	18.2%
標準規格等調査結果（調査D）	国際標準	SHA-1, SHA-256, SHA-384, SHA-512	75.0%	–	–	–	–
	国際的民間規格	SHA-1	83.0%	SHA-256	43.4%	MD5, SHA-384	37.7%
	特定団体規格	SHA-1	57.1%	SHA-256	35.7%	MD5, SHA-384, SHA-512	7.1%
OSS調査結果（調査E）	総合	SHA-1	88.9%	MD5	83.3%	SHA-256	77.8%
	暗号モジュール	SHA-256, SHA-384, SHA-512	100.0%	–	–	–	–

(7) 暗号利用モードの結果

表 31 暗号利用モードの結果

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）	総合	CBC	82.7%	CTR	23.7%	CFB	20.5%
	暗号モジュール	CBC	93.8%	CFB	43.8%	CTR	42.2%
政府系情報システム調査結果（調査C）	システム	CBC	97.8%	その他: ECB	4.4%	CFB, CTS, OFB	2.2%
	規格	CBC	100.0%	OFB	16.7%	–	–
標準規格等調査結果（調査D）	国際標準	CBC, GCM	50.0%	CCM, CFB, CTR, OFB	25.0%	–	–
	国際的民間規格	CBC	84.0%	CTR	34.0%	GCM	32.0%
	特定団体規格	CBC	64.3%	CCM, CTR, OFB	21.4%	–	–
OSS調査結果（調査E）	総合	CBC	100.0%	CFB	52.9%	OFB	47.1%
	暗号モジュール	CBC	100.0%	CTR, OFB	57.1%	–	–

(8) メッセージ認証コードの結果

表 32 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）	総合	HMAC	82.1%	CBC-MAC	17.9%	CMAC	7.5%
	暗号モジュール	HMAC	63.0%	CBC-MAC	39.1%	CMAC	19.6%
政府系情報システム調査結果（調査C）	システム	HMAC	100.0%	–	–	–	–
	規格	HMAC, CBC-MAC	50.0%	–	–	–	–
標準規格等調査結果（調査D）	国際標準	HMAC	100.0%	CBC-MAC, CMAC, GMAC	50.0%	–	–
	国際的民間規格	HMAC	87.2%	CBC-MAC, CMAC	12.8%	–	–
	特定団体規格	HMAC	66.7%	CMAC	50.0%	–	–
OSS調査結果（調査E）	総合	HMAC	100.0%	CMAC	33.3%	CBC-MAC, GMAC	16.7%
	暗号モジュール	HMAC	100.0%	CMAC	50.0%	CBC-MAC, GMAC	25.0%

(9) エンティティ認証の結果

表 33 エンティティ認証の結果

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）	総合	その他: 不明	34.8%	ISO/IEC9798-2	24.6%	その他: IPSec	28.2%
	暗号モジュール	ISO/IEC9798-2	66.7%	その他: 不明	26.7%	その他: IPSec	6.7%
政府系情報システム調査結果（調査C）	システム	ISO/IEC9798-3	32.6%	その他: パスワード認証	18.6%	ISO/IEC9798-2	16.3%
	規格	ISO/IEC9798-3	100.0%	–	–	–	–
標準規格等調査結果（調査D）	国際標準	ISO/IEC9798-2, ISO/IEC9798-3, ISO/IEC9798-4	100.0%	–	–	–	–
	国際的民間規格	–	–	–	–	–	–
	特定団体規格	その他: 不明	66.7%	その他: ITU-T X.509 (1997E)	16.7%	その他: IETF EAP	8.3%
OSS調査結果（調査E）	総合	–		–		–	
	暗号モジュール	–		–		–	

本調査では、市販製品の暗号アルゴリズムについてアンケートを用いて利用実態を調査したため本調査結果に影響を与える可能性のある内容について報告する。

○暗号アルゴリズムの利用実態に関するアンケート調査では、守るべき情報やシステムの安全性、もしくは顧客との契約等の観点から匿名扱いのアンケート調査であっても回答できない場合が存在する。本調査では、一部の応募者から『匿名性の観点から採用された実績や推奨された規格などについて回答できない事例が相当数存在する。』との意見もあり、アンケート回答を得られなかった製品やシステムが存在する。

○本アンケート調査では、回答率の向上を考慮し、製品の販売・出荷数及びシステムの利用数については必須回答設問ではないオプション回答設問とした。製品の販売・出荷数及びシステム利用数に関する回答率は48%程度であり、この回答情報についても情報非公表であるため、製品カテゴリ等、他の情報と関連付けて集計することができない。4.2 節の（11）に示した通り、直近一年間の総出荷台数の回答内容では、検証可能な情報を製品単位で集計したが、数台程度の出荷台数の製品と数千万台の出荷台数の製品とを同率で扱うことで、集計結果と暗号アルゴリズム利用の実態との間に何らかの影響を与えている可能性があることに留意すべきである。

上記の留意点を含め、本調査の成果を活かし、安全な電子政府の検討・構築に繋がれば幸いである。

5. 参考文献

[1] 総務省，経済産業省，電子政府推奨暗号リスト，平成 15 年 2 月，
http://www.cryptrec.go.jp/images/cryptrec_01.pdf

[2] 暗号技術検討会，「暗号技術検討会 2010 年度報告書」，2011，
http://www.cryptrec.go.jp/report/c10_kentou_final.pdf

[3] CRYPTREC,「CRYPTREC Report 2010 暗号方式委員会報告書」,2011，
http://www.cryptrec.go.jp/report/c10_sch_web_v1.pdf

[4] CRYPTREC，「CRYPTREC Report 2010 暗号運用委員会報告書」,2011，
http://www.cryptrec.go.jp/report/c10_opr_web_v1.pdf

[5] CRYPTREC シンポジウム 2012,「暗号運用委員会報告」,2012，
http://www.cryptrec.go.jp/symposium/20120309_cryptrec-opr.pdf

[6] 経済産業省,「暗号モジュールの市場動向等に関する調査研究」,2010，
http://www.meti.go.jp/meti_lib/report/2010fy01/E001139.pdf

6. 付録一覧

1. **調査票（A）**
2. **調査票（B）**
3. **調査票（B）簡易版**
4. **調査票（C）政府系システム版**
5. **調査票（C）政府系システム規格版**
6. **調査票（D）**
7. **調査結果表（B）**
8. **調査結果表（C）**
9. **調査結果表（D）**
10. **調査結果表（E）**

余白