Information-technology
Promotion
Agency, Japan

暗号アルゴリズムの利用実績に関する調査報告書（概要）

2012年12月

目次

1.背景・目的

□ 背景

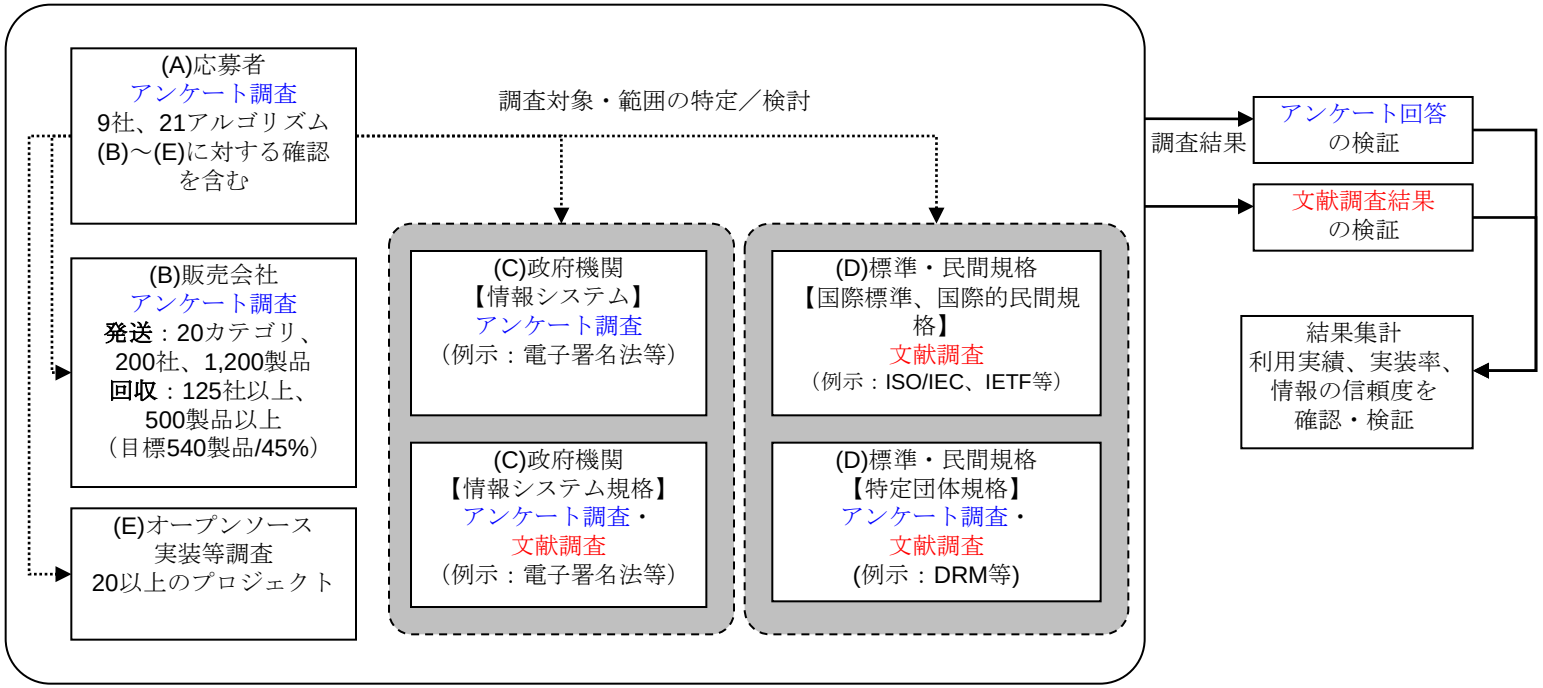
- CRYPTRECで実施している2012年度末の電子政府推奨暗号リストの改訂（以下「次期リスト」という。）では、現在の「電子政府推奨暗号リスト」の単一リスト体系から、「電子政府推奨暗号リスト」「推奨候補暗号リスト」「運用監視暗号リスト」から構成される三リスト体系に移行する。
- 次期リスト掲載の対象となる暗号アルゴリズムは、政府等による調達等を容易にすることを目的として、「安全性」及び「実装性」の観点に加え、「製品化、利用実績等」の観点も踏まえて、いずれかのリストに分類・登録される。このため、次期リスト改訂にあたって、次期リスト掲載の対象となる暗号アルゴリズムの製品化、利用実績等についても明らかにする必要がある。

□ 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。

2.実施作業内容

- 調査A:応募者調査(アンケート調査)
- 調査B:市販製品調査(アンケート調査/公開情報調査)
- 調査C:政府系情報システム・情報システム規格調査(アンケート調査/公開情報調査)
- 調査D:標準規格・民間規格・特定団体規格調査(アンケート調査/公開情報調査)
- 調査E:オープンソースプロジェクト調査(公開情報調査)



３.１.調査・集計方法（調査A）

□　調査概要・集計方法を以下に示す。

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
4	調査項目	1．電子政府推奨応募暗号アルゴリズム情報 2．暗号アルゴリズムを利用した製品・システム情報
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場合は『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

3.1.調査・集計方法（調査A）

□　アンケート調査対象企業を以下に示す。

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

3.2.調査・集計方法（調査B）

□　調査概要・集計方法を以下に示す。

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（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 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
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） ・ アンケート情報は全て匿名化処理し集計 ・ 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 ・ 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 ・ 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 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

3.2.調査・集計方法（調査B）

□　製品カテゴリを以下に示す。

※全体を「市販製品総合」、区分番号1, 2, 11, 12, 13を合わせたものを「市販暗号モジュール」とする。

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

3.2.調査・集計方法（調査B）

□　調査対象アルゴリズム等の名称を以下に示す。

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

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

公開鍵暗号
- 署名
  - DSA
  - ECDSA
  - KC-DSA
  - RSA-PSS
  - RSASSA-PKCS1-v1_5
  - SM2
- 守秘・鍵共有
  - DH
  - ECDH
  - EC-MQV
  - PSEC-KEM
  - RSAES-PKCS1-v1_5
  - 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

３.２.調査・集計方法（調査B）

□　アンケート回答内容（暗号アルゴリズム等の実装が明示的に読み取れる情報）に関する信頼度別に集計。

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

3.3.調査・集計方法（調査C）

□　調査概要・集計方法を以下に示す。

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 ・ 機構と相談のうえ決定した規格（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）
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 ・ 政府系規格における暗号アルゴリズムの採用実績 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
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）

3.3.調査・集計方法（調査C）

□　調査概要・集計方法を以下に示す。

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 ・ 機構と相談のうえ決定した規格（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）
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 ・ 政府系規格における暗号アルゴリズムの採用実績 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
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）

3.3.調査・集計方法（調査C）

□　調査対象の公開情報を以下に示す。

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
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
3	商業登記認証局	「電子証明書の方式等に関する件（告示）」
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
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
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
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

3.4.調査・集計方法（調査D）

□　調査概要・集計方法を以下に示す。

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） ・ 国際的な民間規格（例：IETF、IEEE等） ・ 特定団体規格（例：DRM、Bluetooth、ZigBee、Wi-Fi 等）
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））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（調査Bと同様） 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 ・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

3.4.調査D：国際標準規格の調査対象

□　調査対象の国際標準規格を以下に示す。

	名称
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, 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
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, -4:2005, DIS 7816-4, -4:2005/Amd 1:2008, -5:2004, -6:2004, -6:2004/Cor 1:2006, -7:1999, -8:2004, -9:2004, -10:1999, -11:2004, -12:2005, -13:2007, -13:2007/CD Cor 1, -15:2004, -15:2004/Amd 1:2007, -15:2004/Cor 1:2004, -15:2004/Amd 2:2008
10	ITU-T Y.Sec Mechanisms (NGN Security Mechanisms) Y.2704
11	ITU-T H.233/H.234 (audiovisual services)
12	ICAO Doc 9303 (Machine readable travel documents) Part 1 Volume 1 Sixth Edition 2006 Part 1 Volume 2 Sixth Edition 2006, Part 2 Third Edition 2005, Part 3 Volume 1 Third Edition 2008, Part 3 Volume 2 Third Edition 2008

3.4.調査D：国際的民間規格の調査対象

□　調査対象国際的な民間規格を以下に示す。

	名称	調査数	調査文献一覧
1	IETF TLS	20	RFC2246, RFC2712, RFC4162, RFC4492, RFC4785, RFC5246, RFC5288, RFC5289, RFC5469, RFC5487, RFC5489, RFC5932, RFC4680, RFC4681, RFC5746, RFC5878, RFC6066, RFC6176, RFC6460, RFC6367
2	IETF IPsec	34	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
3	IETF S/MIME, CMS	15	RFC2311, RFC2312, RFC3565, RFC3657, RFC3853, RFC4056, RFC5083, RFC5652, RFC5750, RFC5751, RFC5752, RFC5753, RFC5754, RFC5990, RFC3560
4	IETF PGP	3	RFC3156, RFC4880, RFC5581
5	IEEE802.11i	1	IEEE 802.11i-2004: Amendment 6: Medium Access Control (MAC) Security Enhancements
6	RSA PKCS#11	1	PKCS #11 Mechanisms v2.30: Cryptoki – Draft 7 29 July 2009 RSA Laboratories
7	EMV	2	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
8	3GPP	2	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:
9	3GPP2	3	TSG-S S.S0053-0 v2.0 Common Cryptographic Algorithms 2009/05 TSG-S S.S0054-0 v1.0 Interface Specification for Common Cryptographic Algorithms 2002/01 TSG-S S.S0055-A v4.0 Enhanced Cryptographic Algorithms 2008/01
10	OMA	1	DRM Specification V2.0 Candidate Version 2.0 – 10 December 2004
11	IETF DNSSec	10	RFC3110, RFC4033, RFC4034, RFC4035, RFC4431, RFC4470, RFC4509, RFC5074, RFC5702, RFC6014
12	IETF Kerberos	9	RFC3962, RFC4120, RFC4537, RFC5021, RFC5896, RFC6111, RFC6112, RFC6113, RFC6649
13	IEEE1619	1	IEEE Std 1619-2007 IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices
14	Trusted Computing Group	3	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
15	その他	2	RFC6272, RFC4055

3.4.調査D：特定団体規格の調査対象

□　調査対象特定団体規格を以下に示す。

・アンケート回答内容

	団体名	詳細
1	ARIB	ARIB STD-T63、ARIB STD-T64、ARIB STD-T94 、ARIB STD-T105 、ARIB STD-B25、ARIB STD-B45、ARIB STD-B48、ARIB STD-B50等
2	Marline Joint Development Association	Marlin仕様書（Marlin IPTV End-point Service System、Marlin Broadband Delivery System）
3	一般財団法人日本データ通信協会	タイムビジネス信頼・安心認定制度認定基準

・公開情報調査対象

	団体名	詳細
1	ZigBee SIG-Japan	ZigBee和訳仕様書 （ZigBee Specification Document 053474r17 January 17, 2008）
2	Bluetooth SIG, Inc	Bluetooth仕様書 （BLUETOOTH SPECIFICATION Version 4.0 [Vol 0]）
3	Wi-Fi Alliance	WiFi仕様書 （Wi-Fi Simple Configuration Technical Specification Version 2.0.2）
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
5	DCI（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
6	AACS（Advanced Access Content System）	AACS仕様書 1）Elements Book 2）Blu-ray Disc 3）HD DVD and DVD）

３.５.調査・集計方法（調査E）

□　調査概要･集計方法を以下に示す。

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	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）※詳細次頁参照
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（次ページの青色） ・ Thunderbird及びfirefox、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（次ページの黄色） ・ Qmail及びOpenSSLは、両方に実装されている場合でも1と集計（次ページの赤色） ・ 応募者からの情報があっても、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は対象外 ・ 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 ➢ 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 ・ エンティティ認証は、ISO/IEC9798等の明示がないため、対象外

3.5.調査・集計方法（調査E）

□　調査概対象のOSSを以下に示す。

	ツール名	バージョン
1	Linux	3.4.7
2	Debian	6.0.5
3	FreeBSD	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
10	Samba	3.6.6
11	Tomcat	7.0.29
12	Apache	2.4.2 (released 2012-04-17)
13	Webkit	r125966

	ツール名	バージョン
14	Thunderbird	14
15	firefox	14.0.1
16	NSS	3.13.5
17	Qmail	1.06
18	OpenSSL	1.0.1c
19	GnuPG	2.0 (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

※調査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」として扱う。

4.1.応募者情報調査結果（調査A結果）

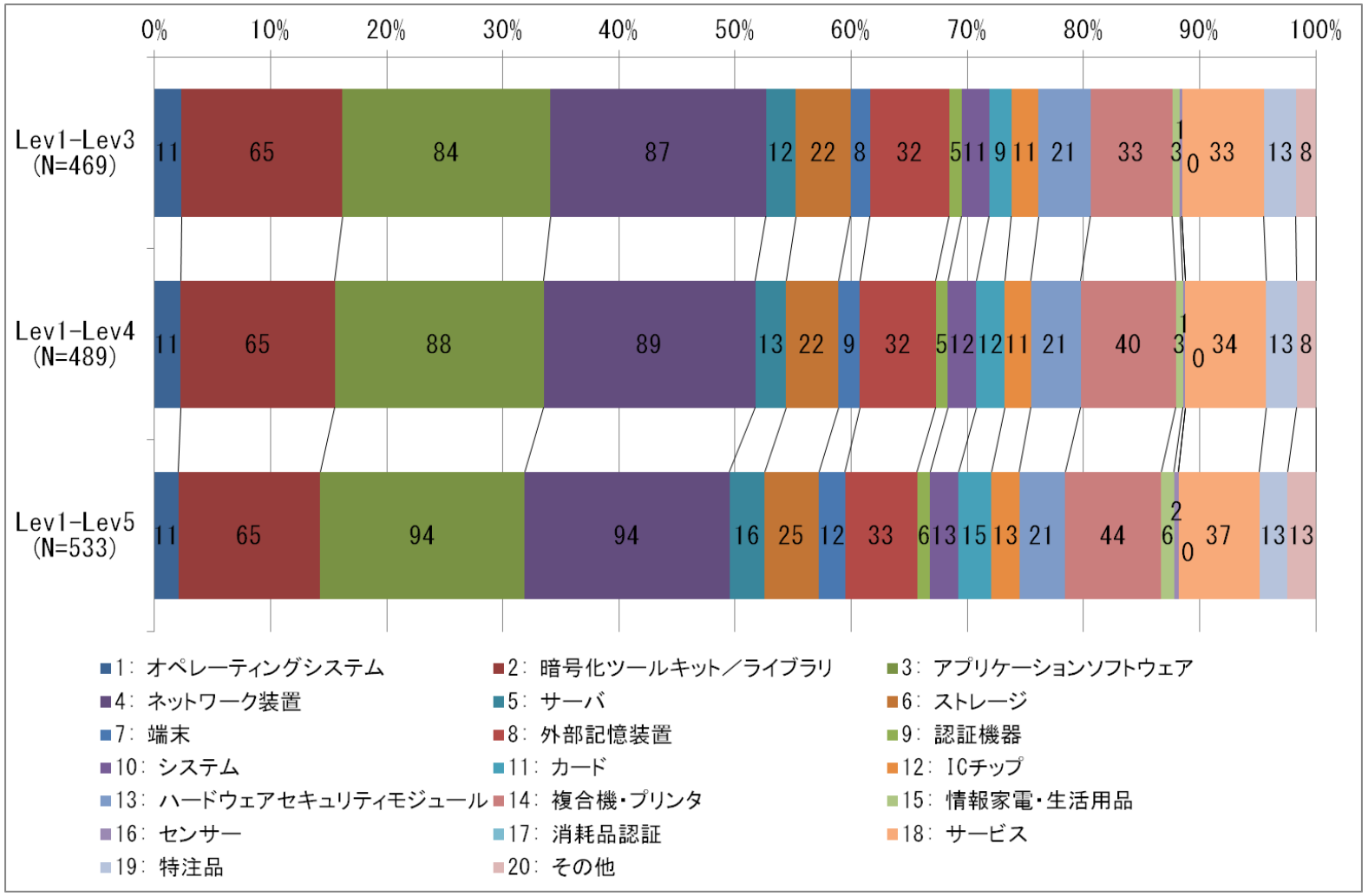
□　調査Aの結果概要を示す。

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
	8) PC-MAC-AES	○	○	0	0	0	0
富士通株式会社	9) ECDSA	○	○	0	0	0	1
	10) ECDH	○	○	0	0	0	1
	11) 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。

4.2.市販製品調査結果（調査B結果）

□　調査Bの結果概要を示す。(市販製品総合:Lev分け)



４.２.市販製品調査結果（調査B結果）

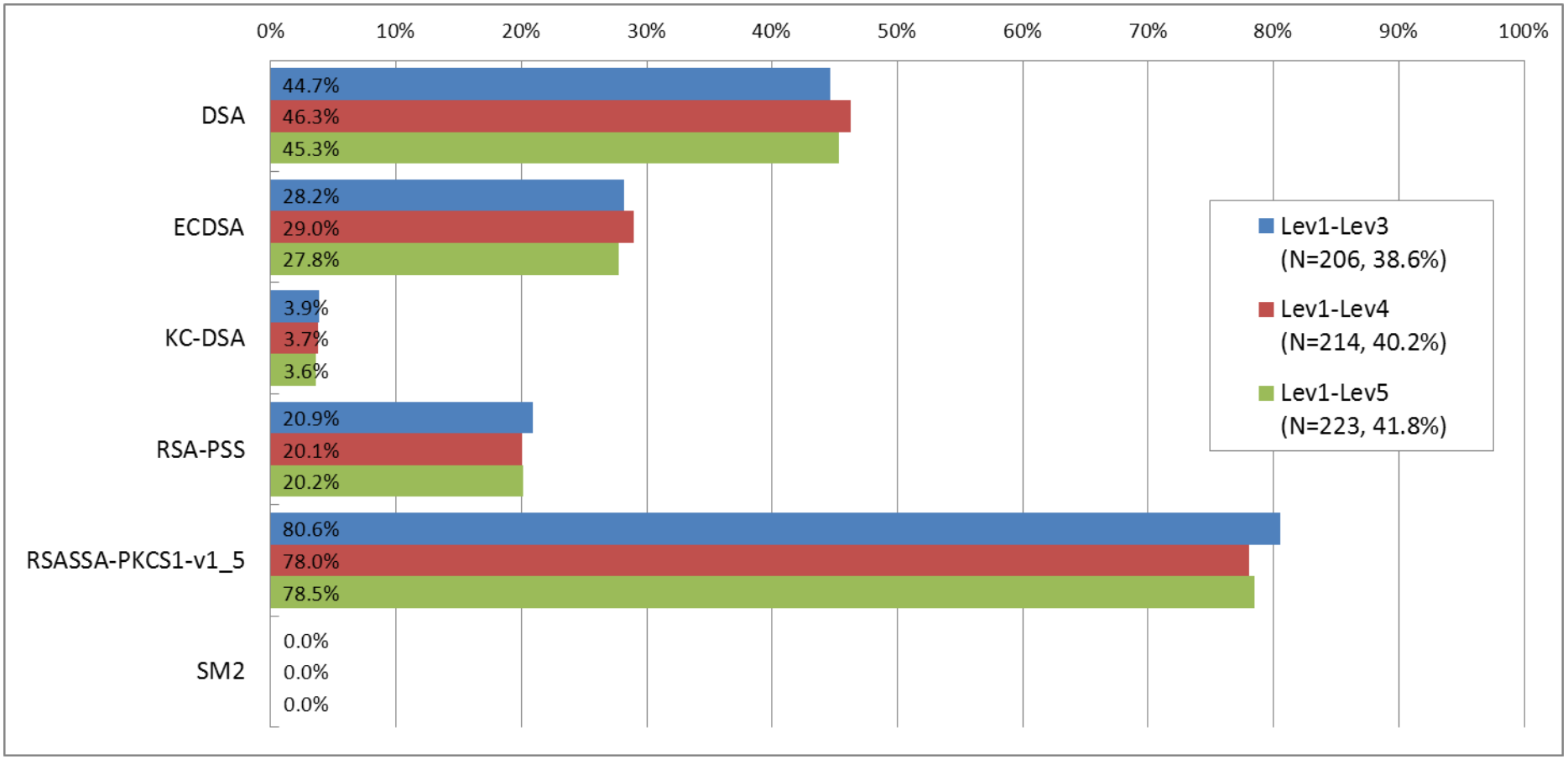
□ グラフの記法

- 凡例
  - □『公開鍵暗号（署名）』等の技術カテゴリの該当総数を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）のいづれかを選択した回答数（該当総数）：10
    - 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
    - 暗号アルゴリズムAのデータ値：50%

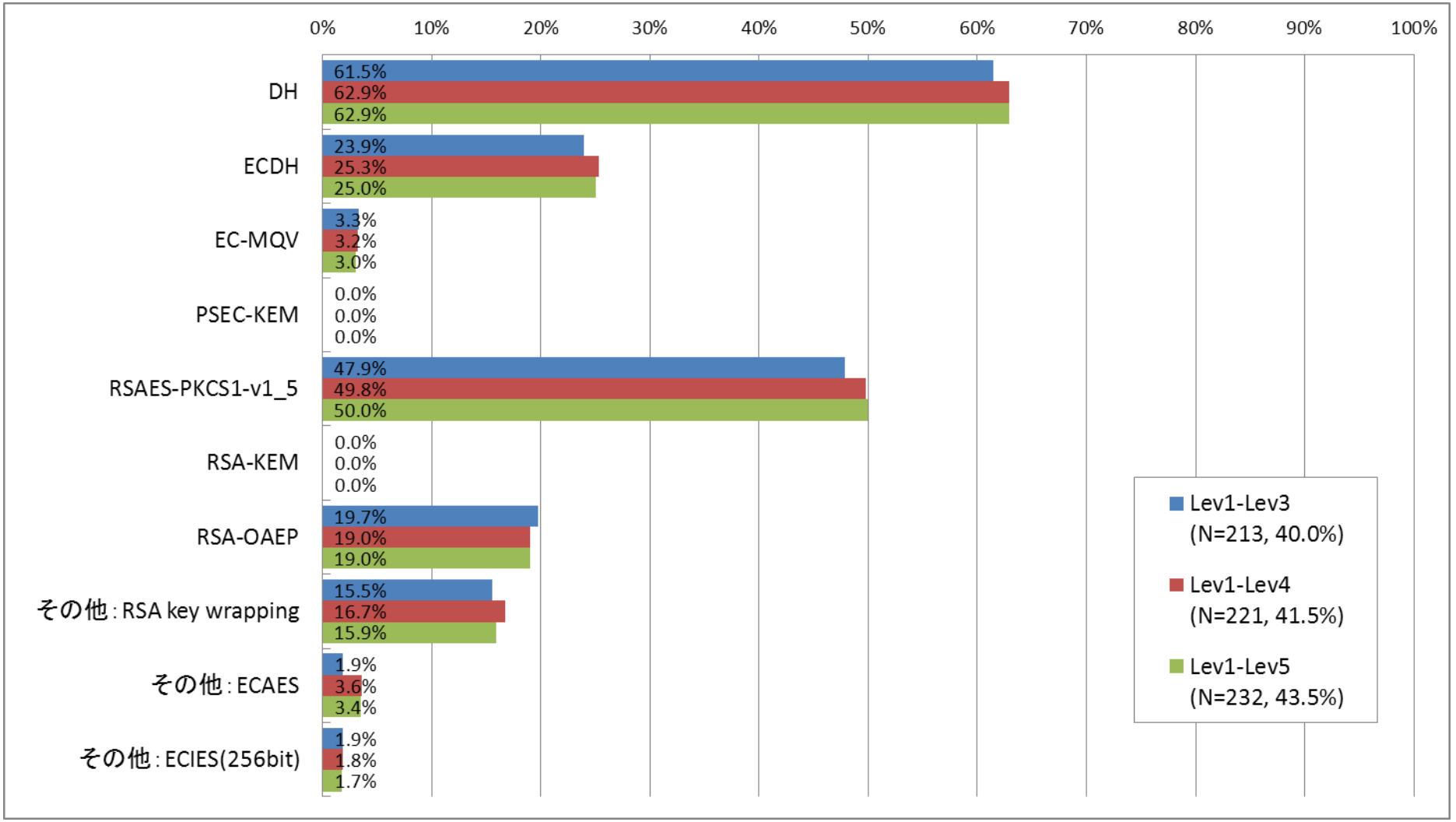
4.2.市販製品調査結果（調査B結果・総合）

1. 公開鍵暗号(署名)



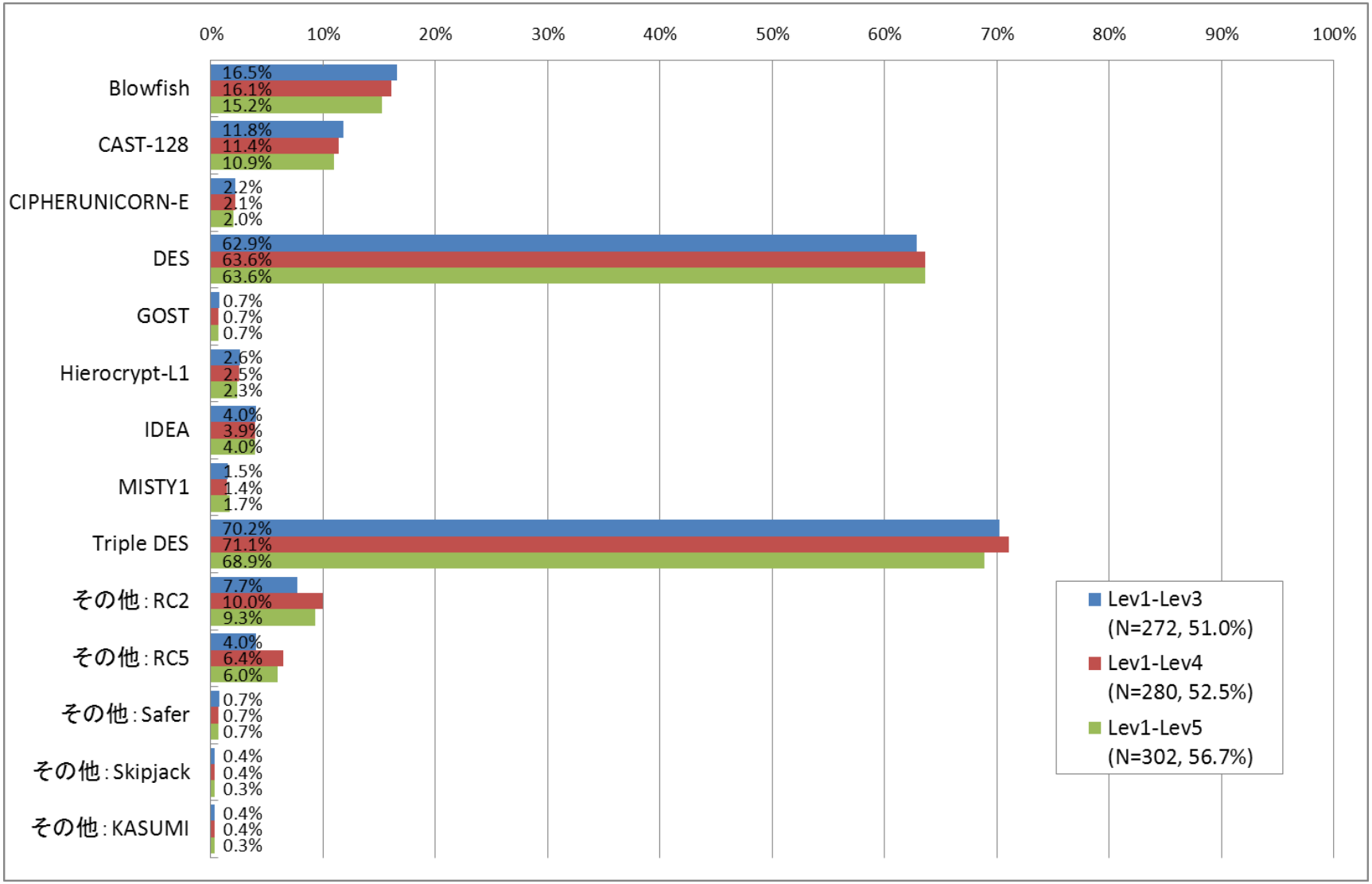
4.2.市販製品調査結果（調査B結果・総合）

2. 公開鍵暗号(守秘･鍵共有)



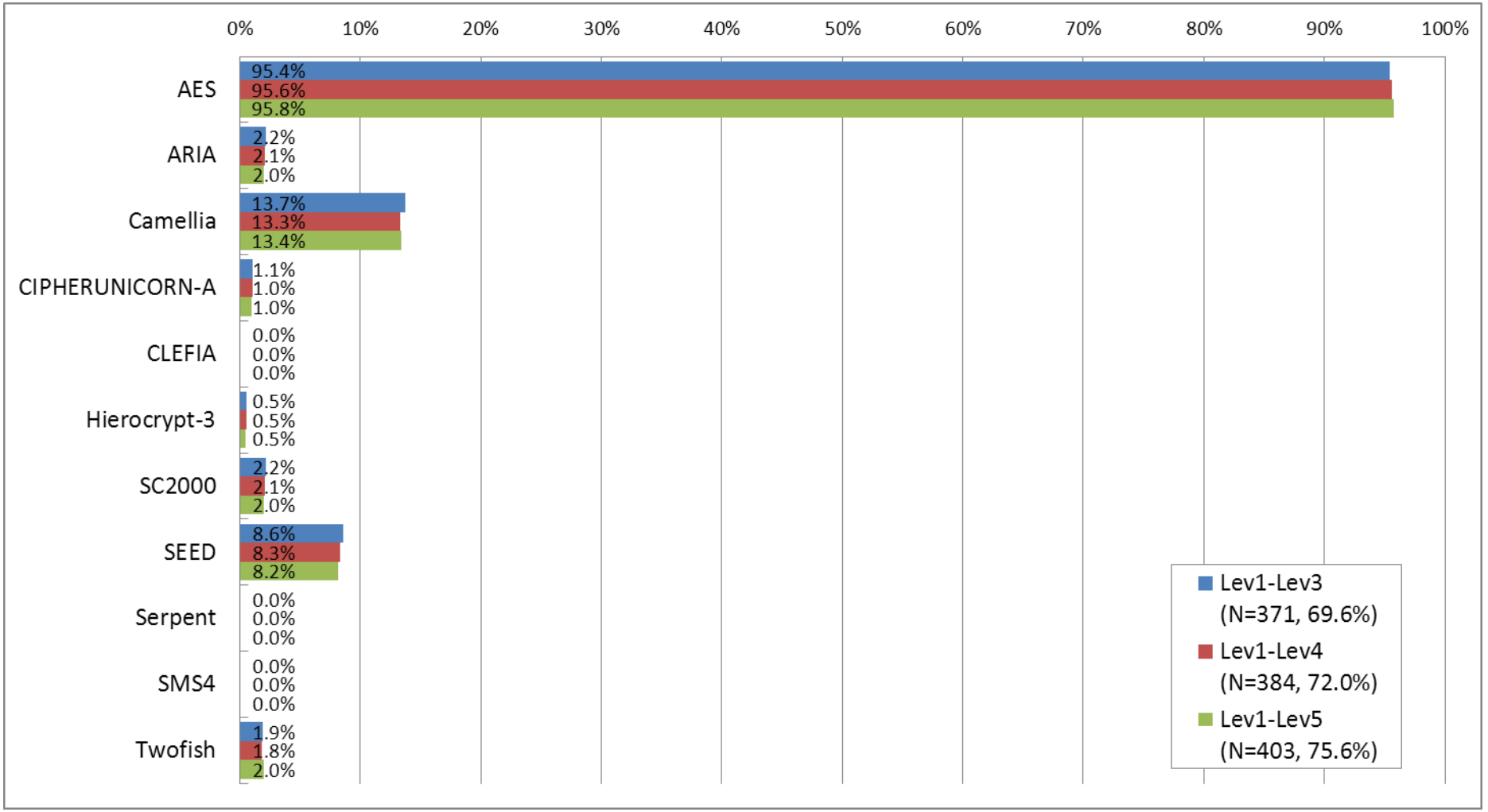
4.2.市販製品調査結果（調査B結果・総合）

3. 共通鍵暗号（64ビットブロック暗号）



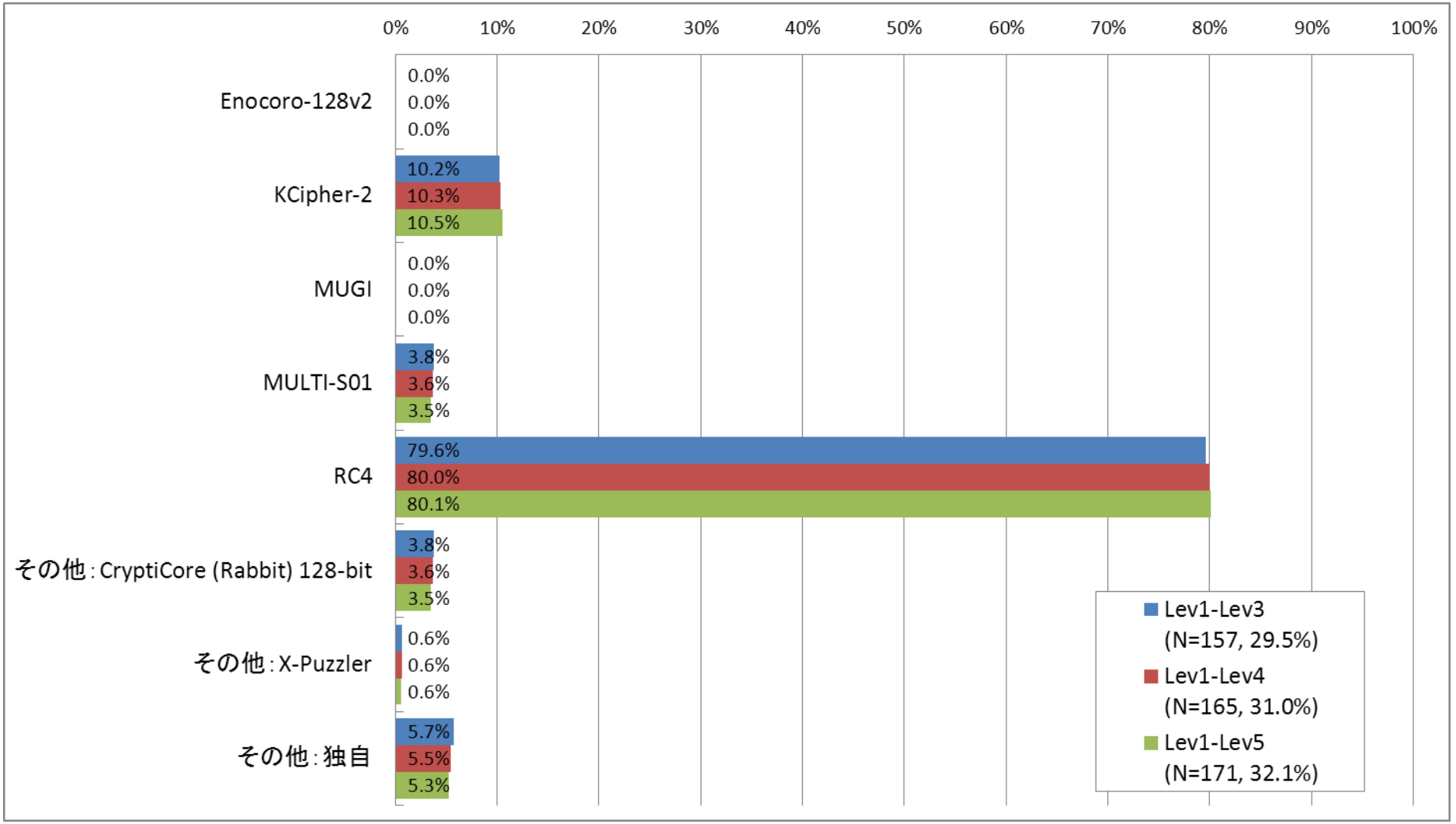
4.2.市販製品調査結果（調査B結果・総合）

4. 共通鍵暗号（128ビットブロック暗号）



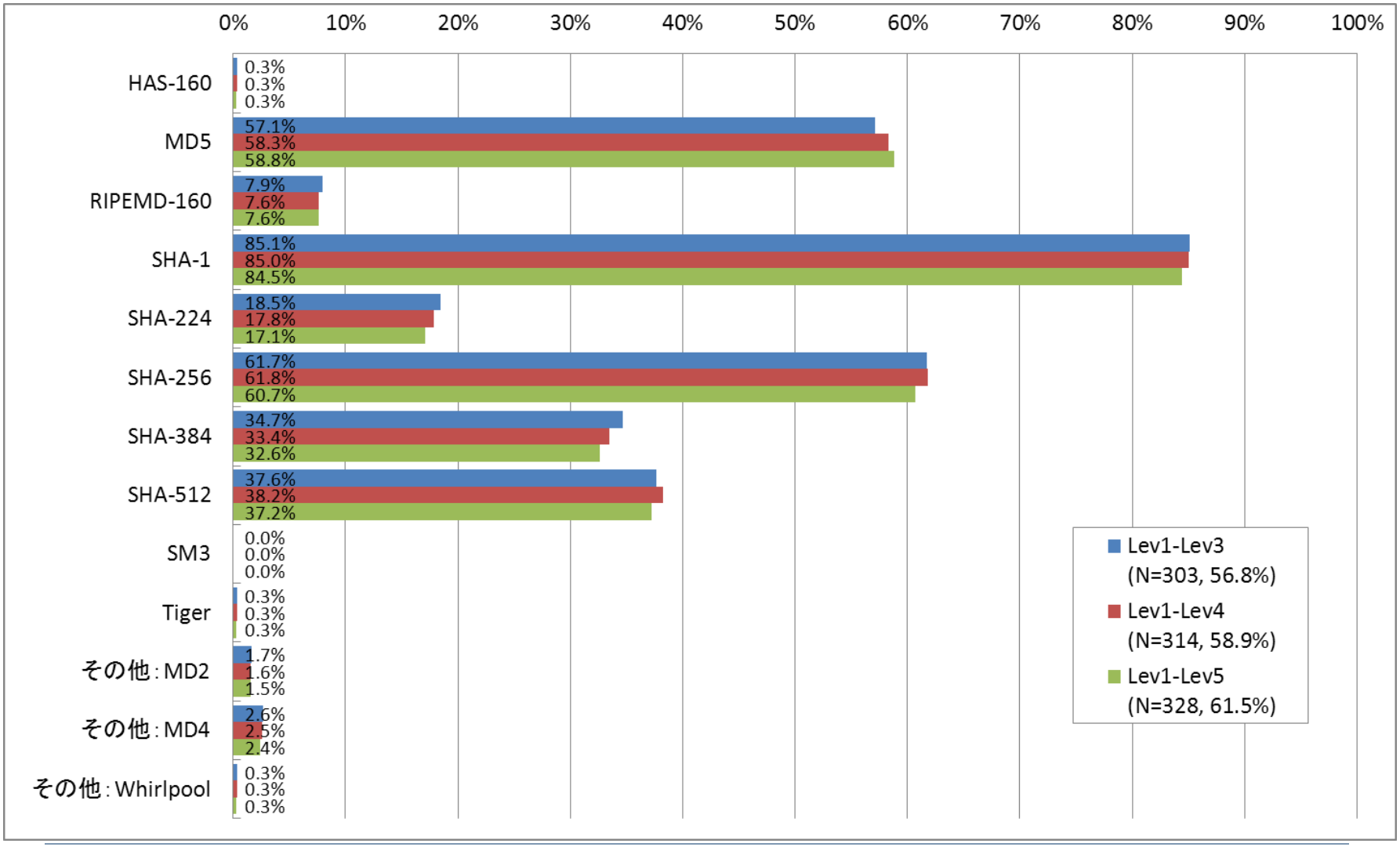
4.2.市販製品調査結果（調査B結果・総合）

5. 共通鍵暗号(ストリーム暗号)



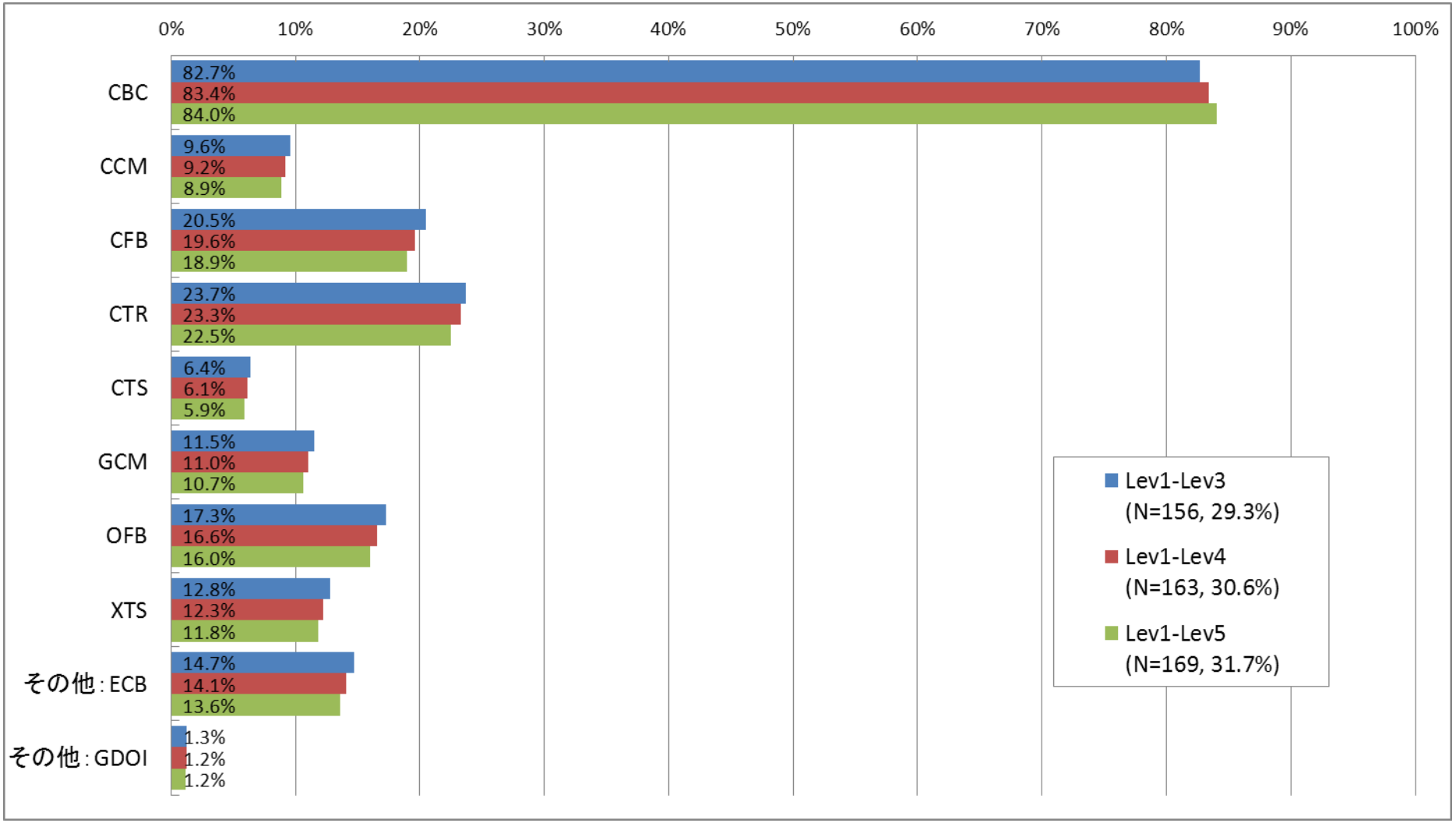
4.2.市販製品調査結果（調査B結果・総合）

6. ハッシュ関数



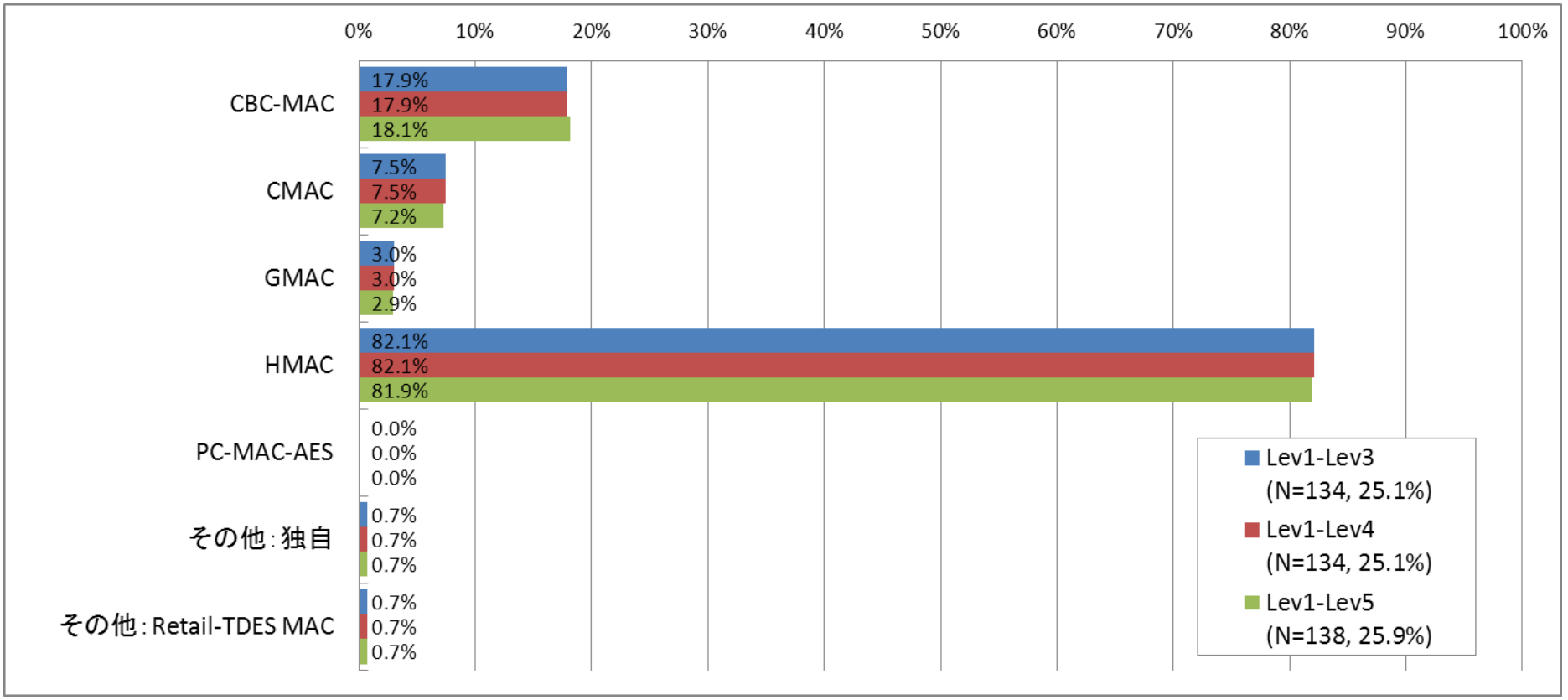
4.2.市販製品調査結果（調査B結果・総合）

7. 暗号利用モード



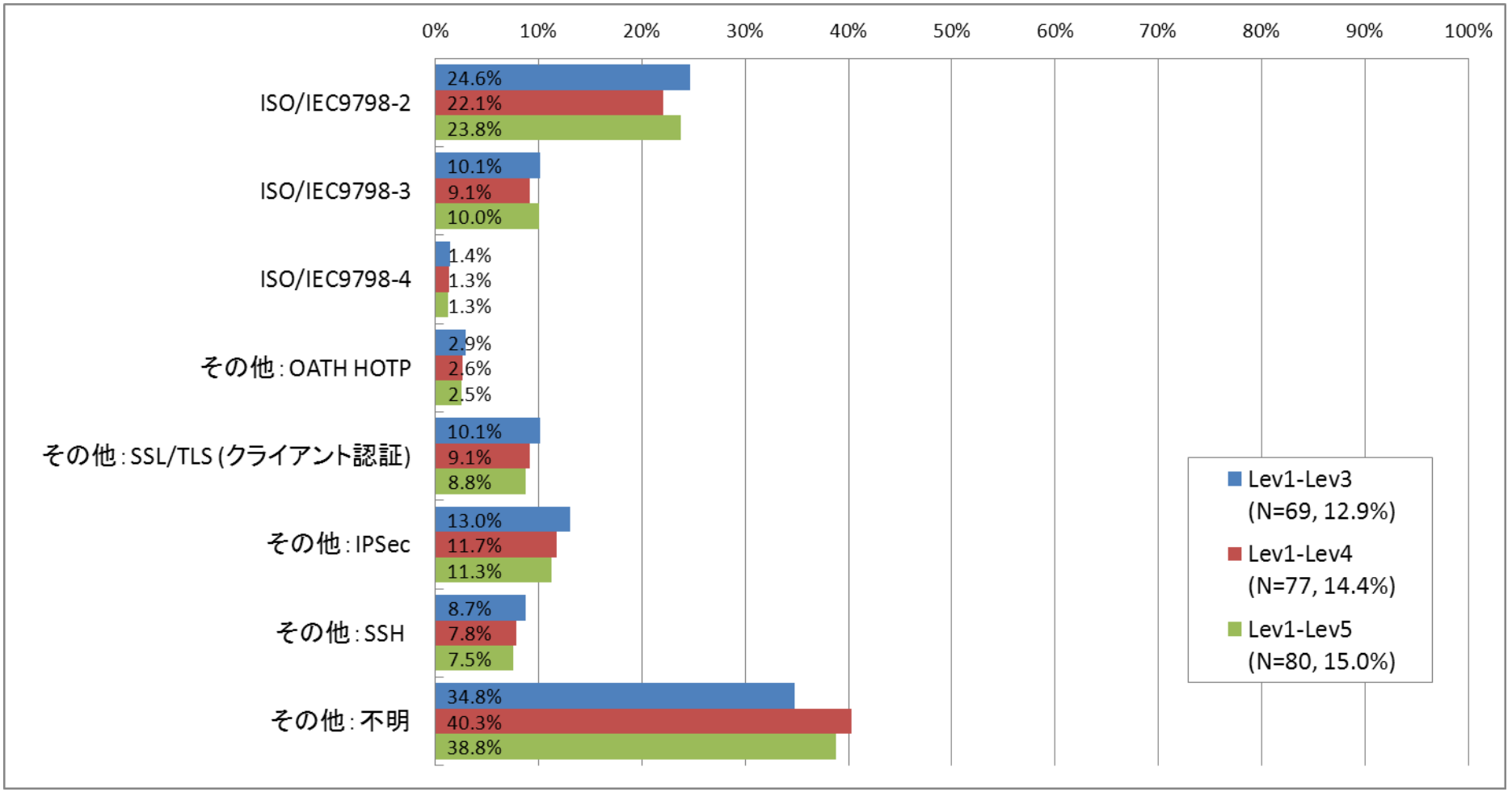
4.2.市販製品調査結果（調査B結果・総合）

8. メッセージ認証コード



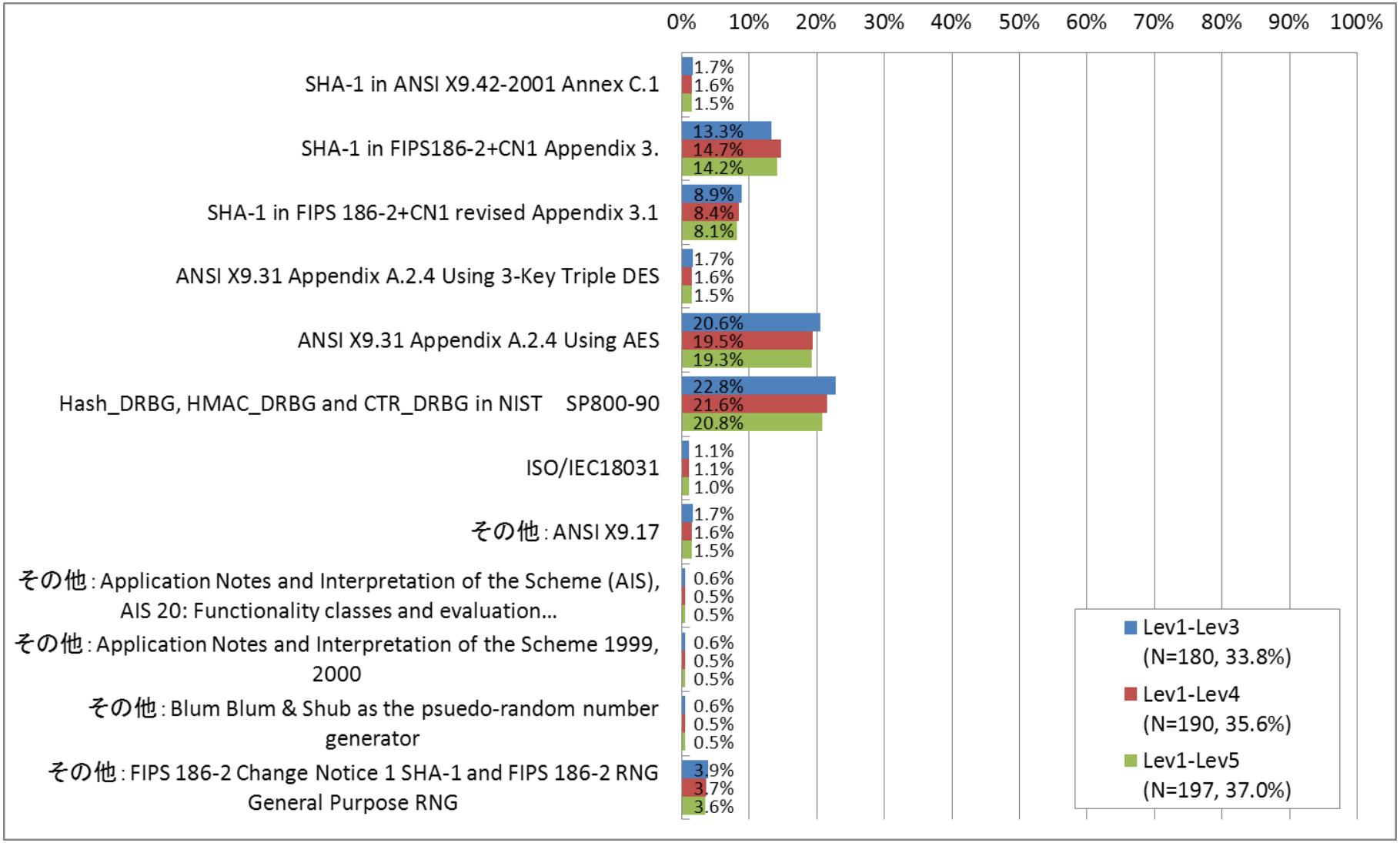
4.2.市販製品調査結果（調査B結果・総合）

9. エンティティ認証



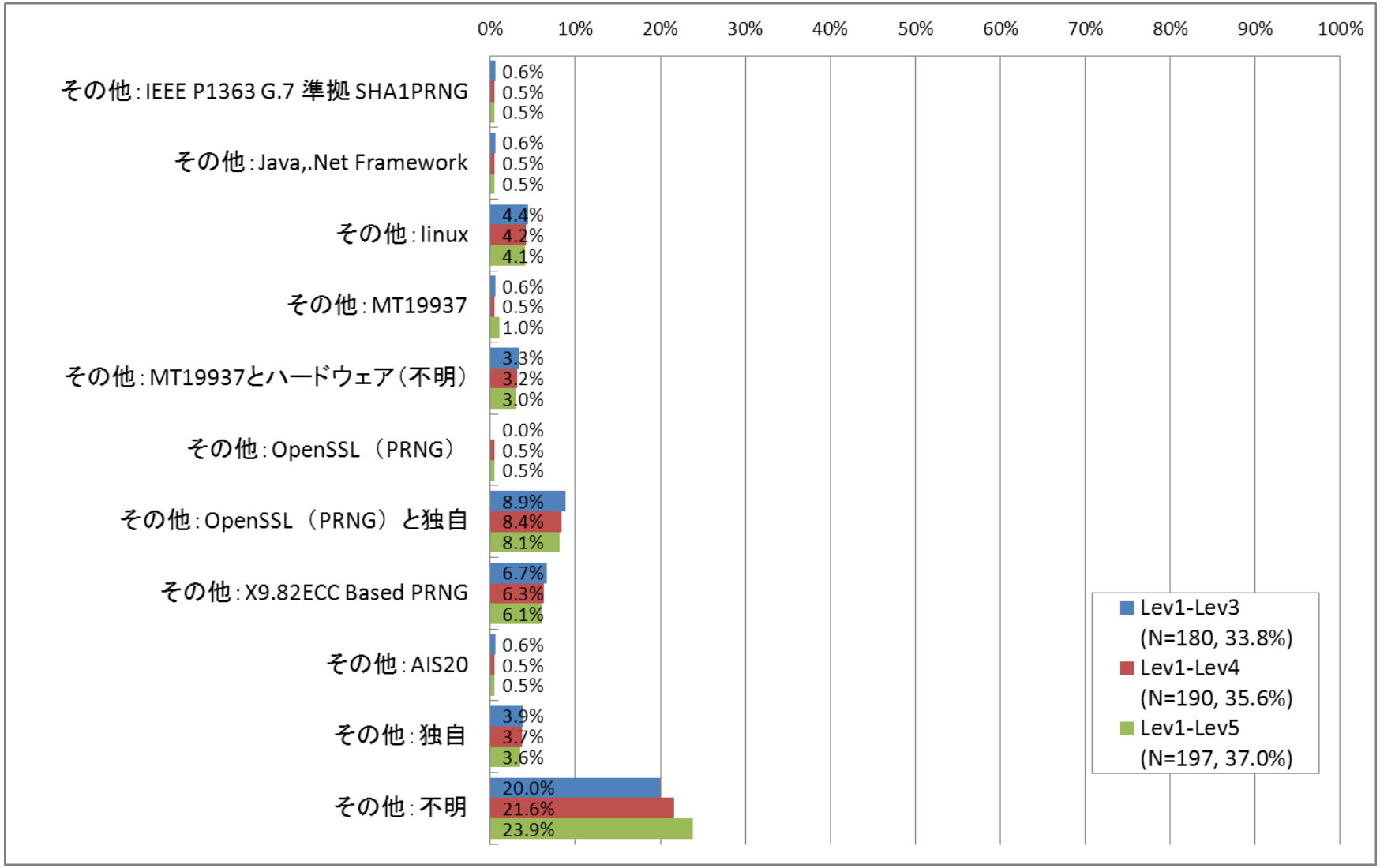
4.2.市販製品調査結果（調査B結果・総合）

10. 擬似乱数生成方式(1)



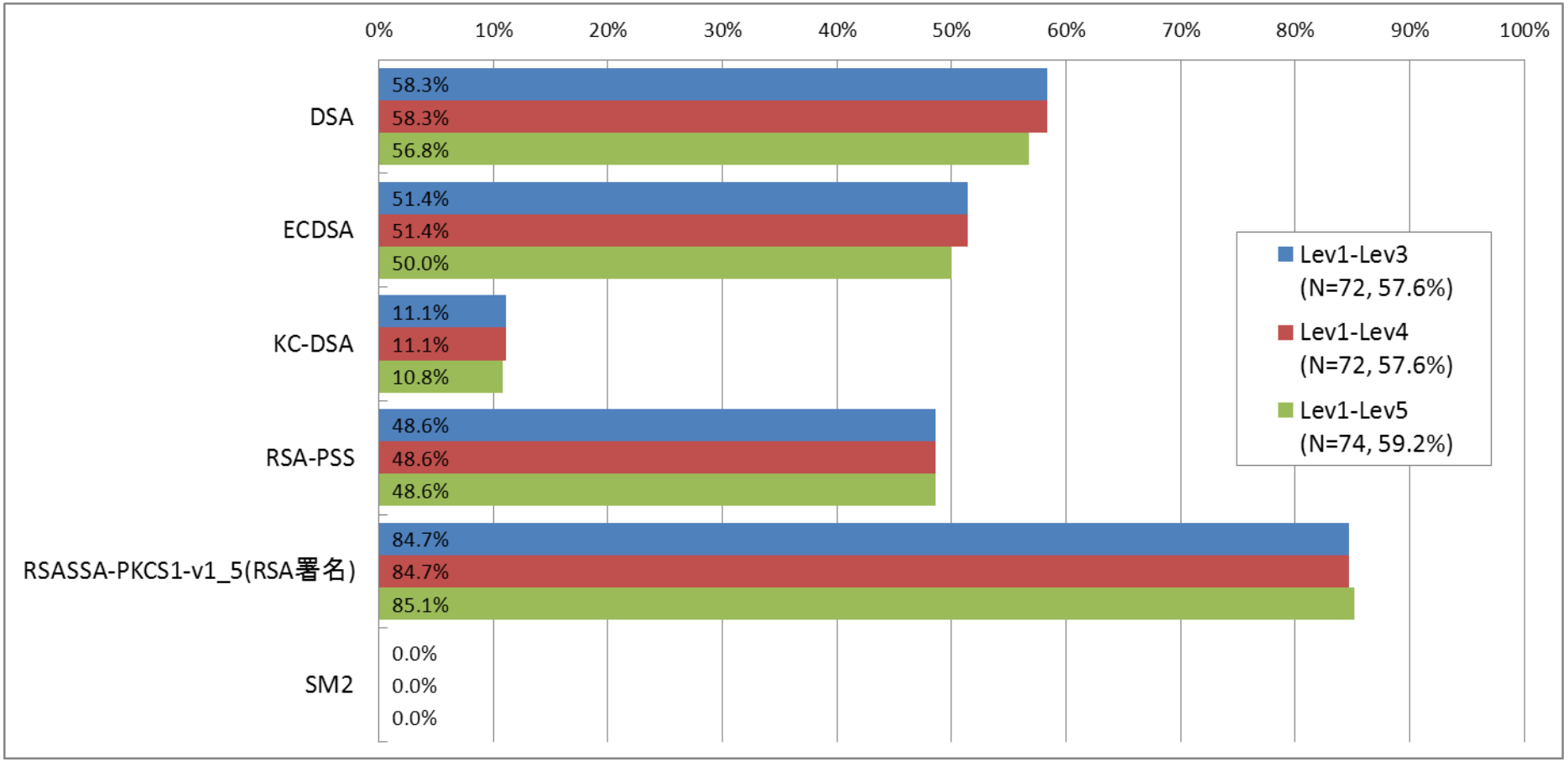
4.2.市販製品調査結果（調査B結果・総合）

10. 擬似乱数生成方式(2)



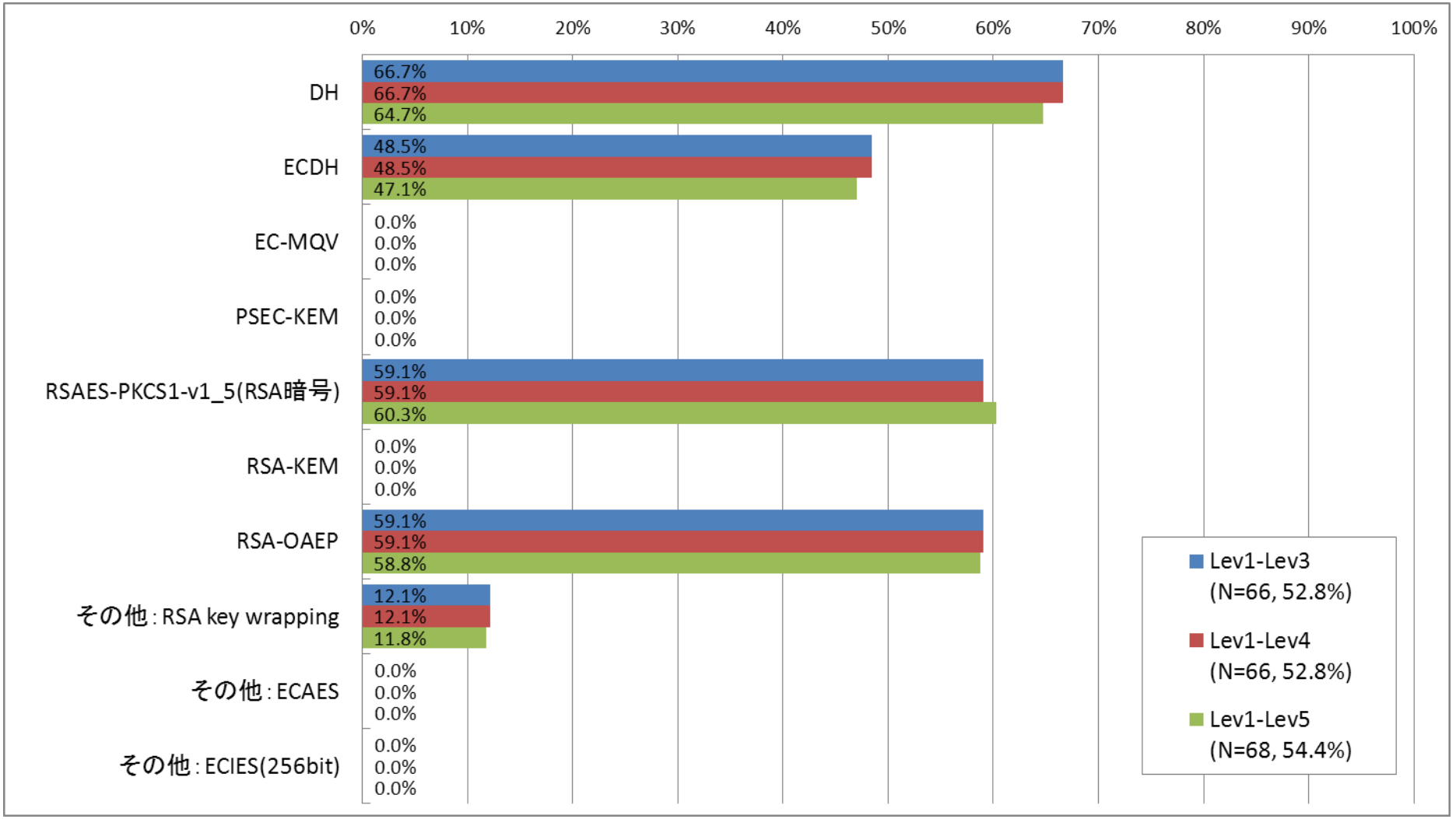
4.2.市販製品調査結果（調査B結果・暗号モジュール）

1. 公開鍵暗号(署名)



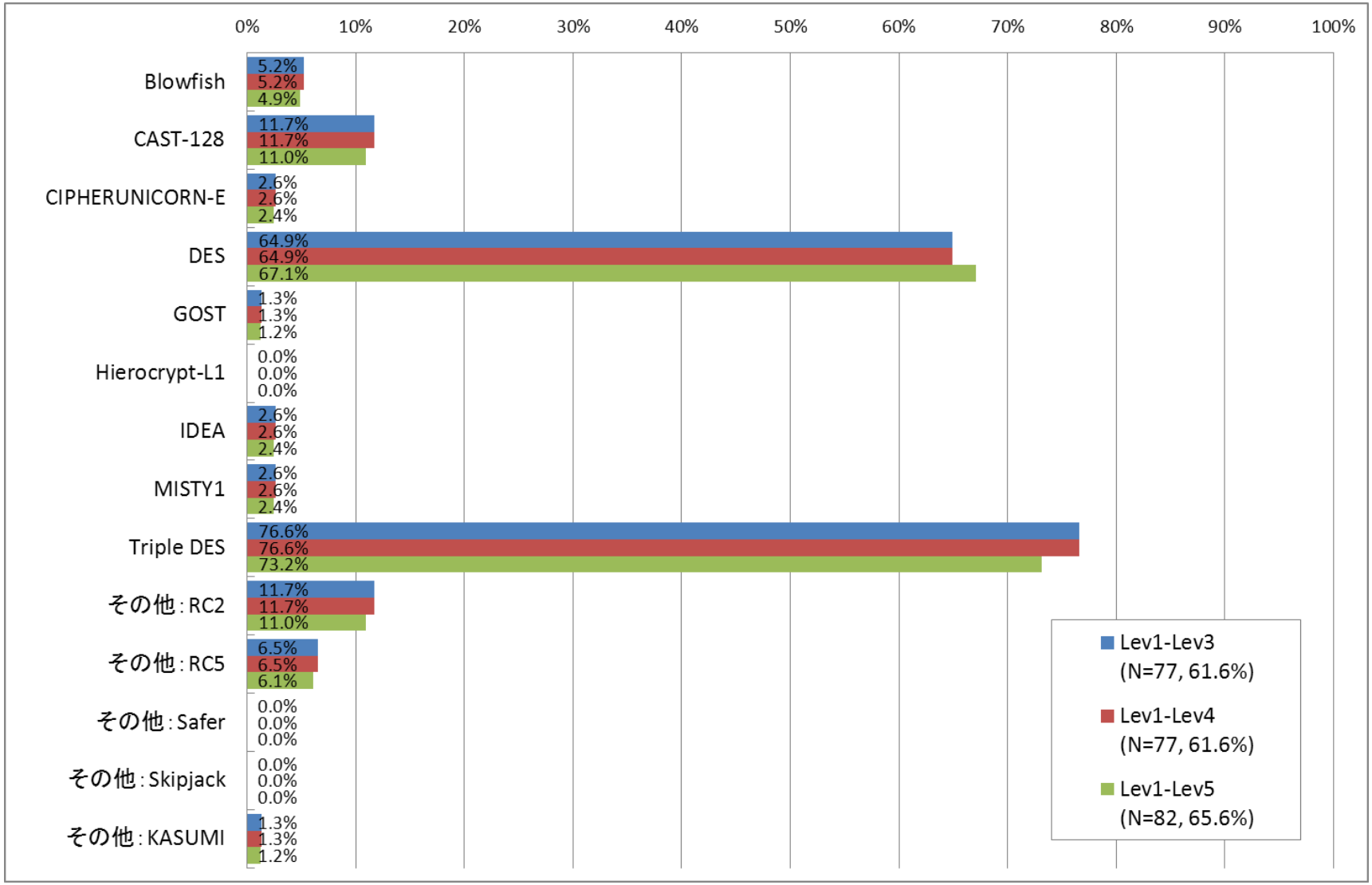
4.2.市販製品調査結果（調査B結果・暗号モジュール）

2. 公開鍵暗号(守秘･鍵共有)



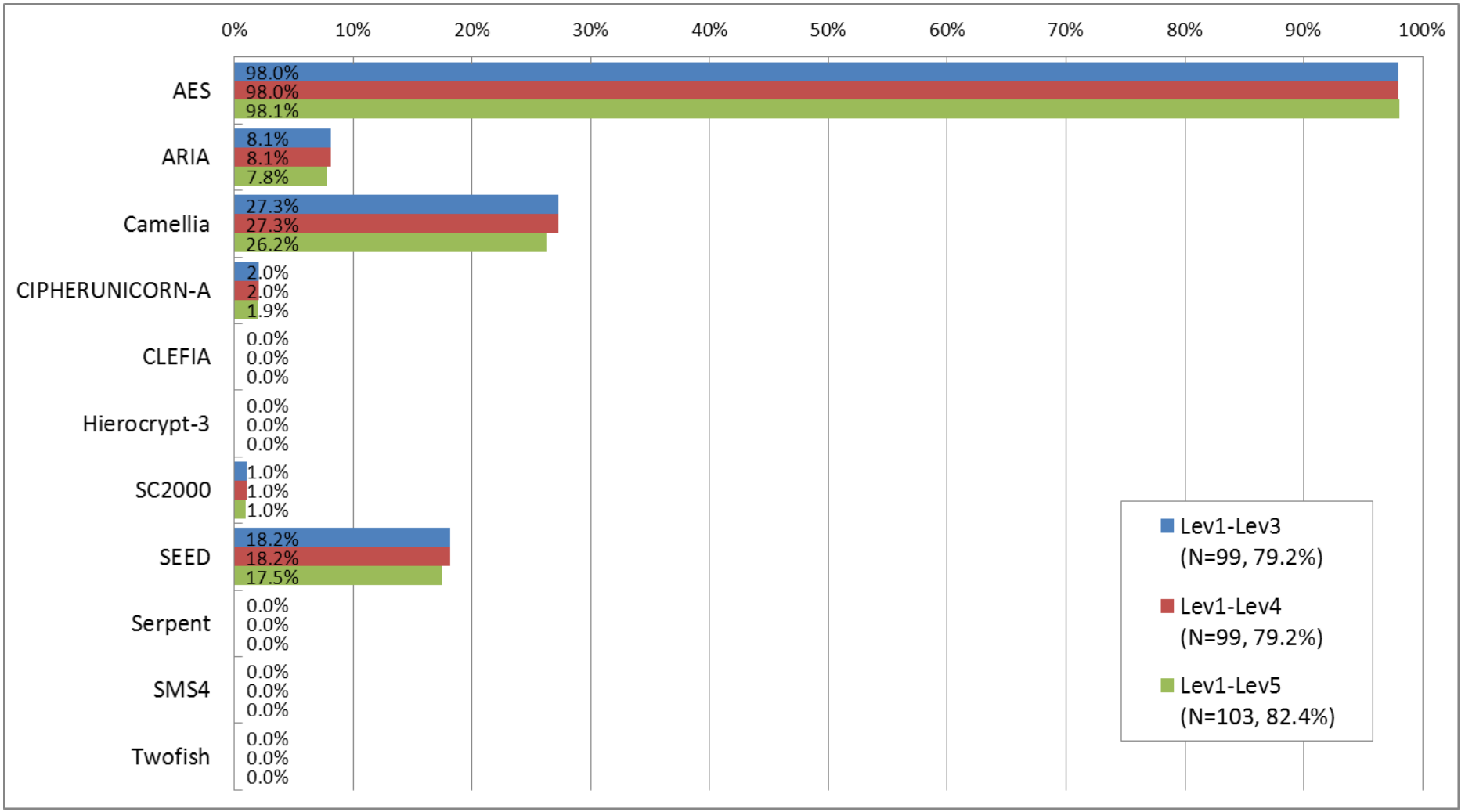
4.2.市販製品調査結果（調査B結果・暗号モジュール）

3. 共通鍵暗号（64ビットブロック暗号）



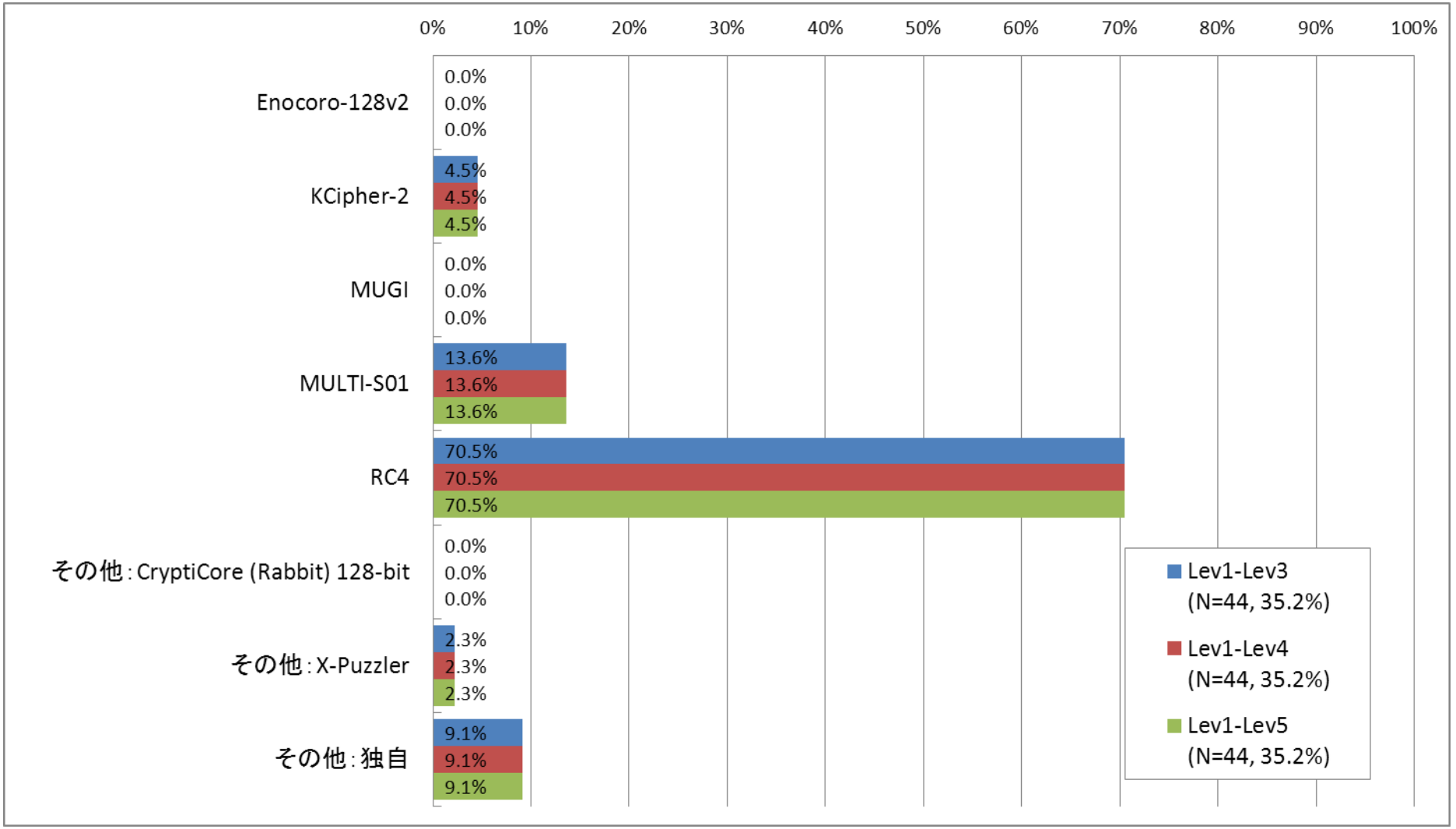
4.2.市販製品調査結果（調査B結果・暗号モジュール）

4. 共通鍵暗号（128ビットブロック暗号）



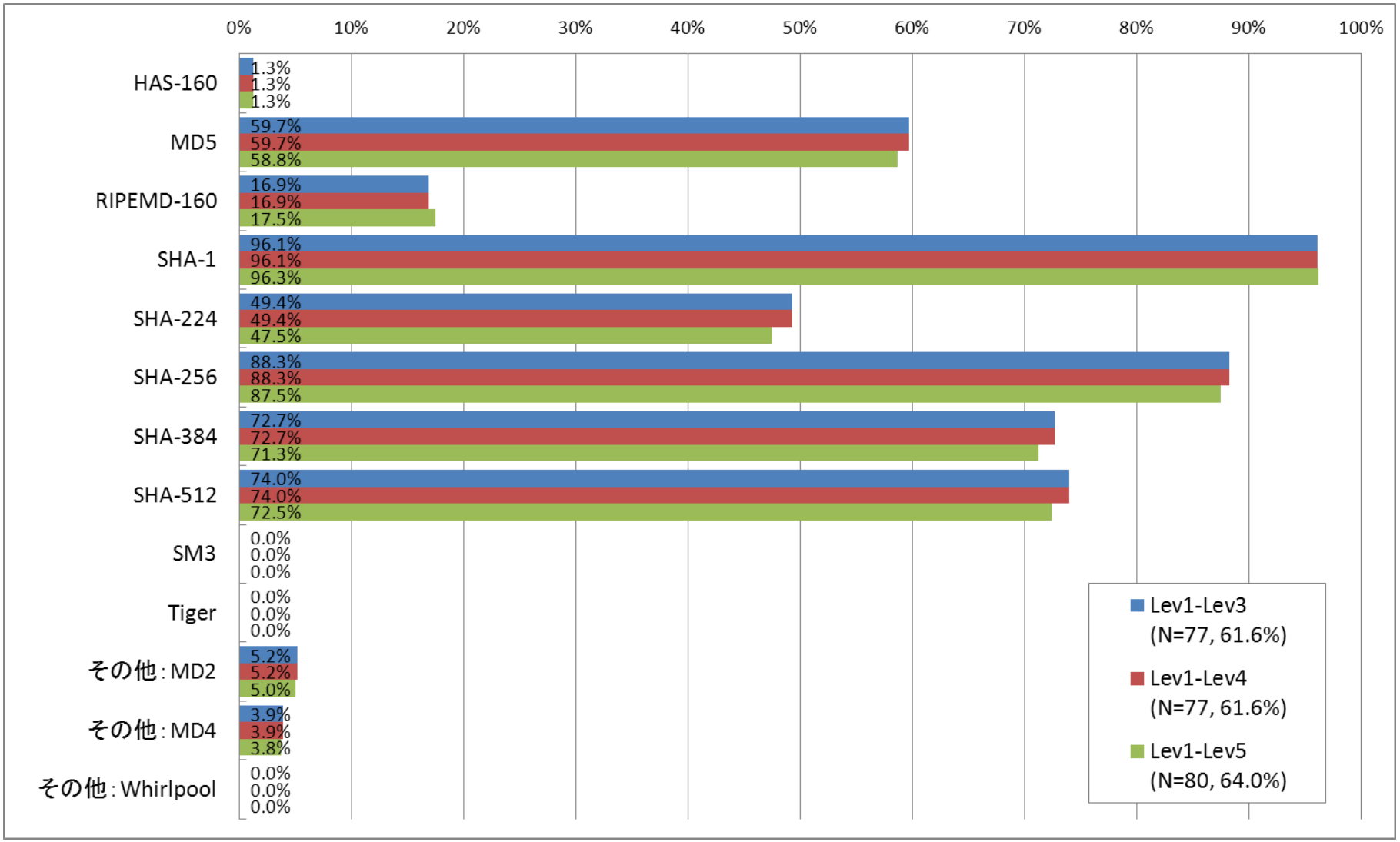
4.2.市販製品調査結果（調査B結果・暗号モジュール）

5. 共通鍵暗号(ストリーム暗号)



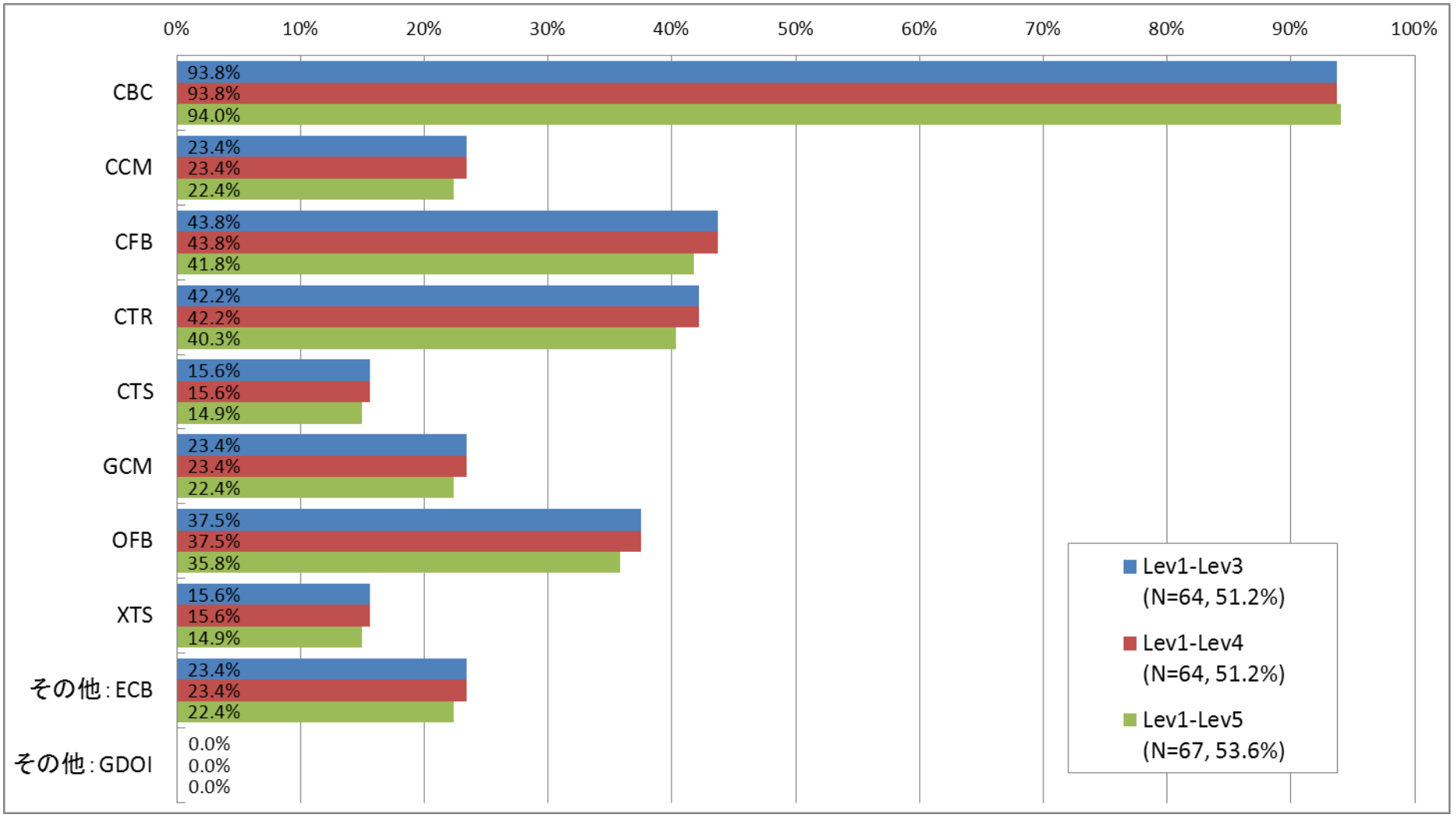
4.2.市販製品調査結果（調査B結果・暗号モジュール）

6. ハッシュ関数



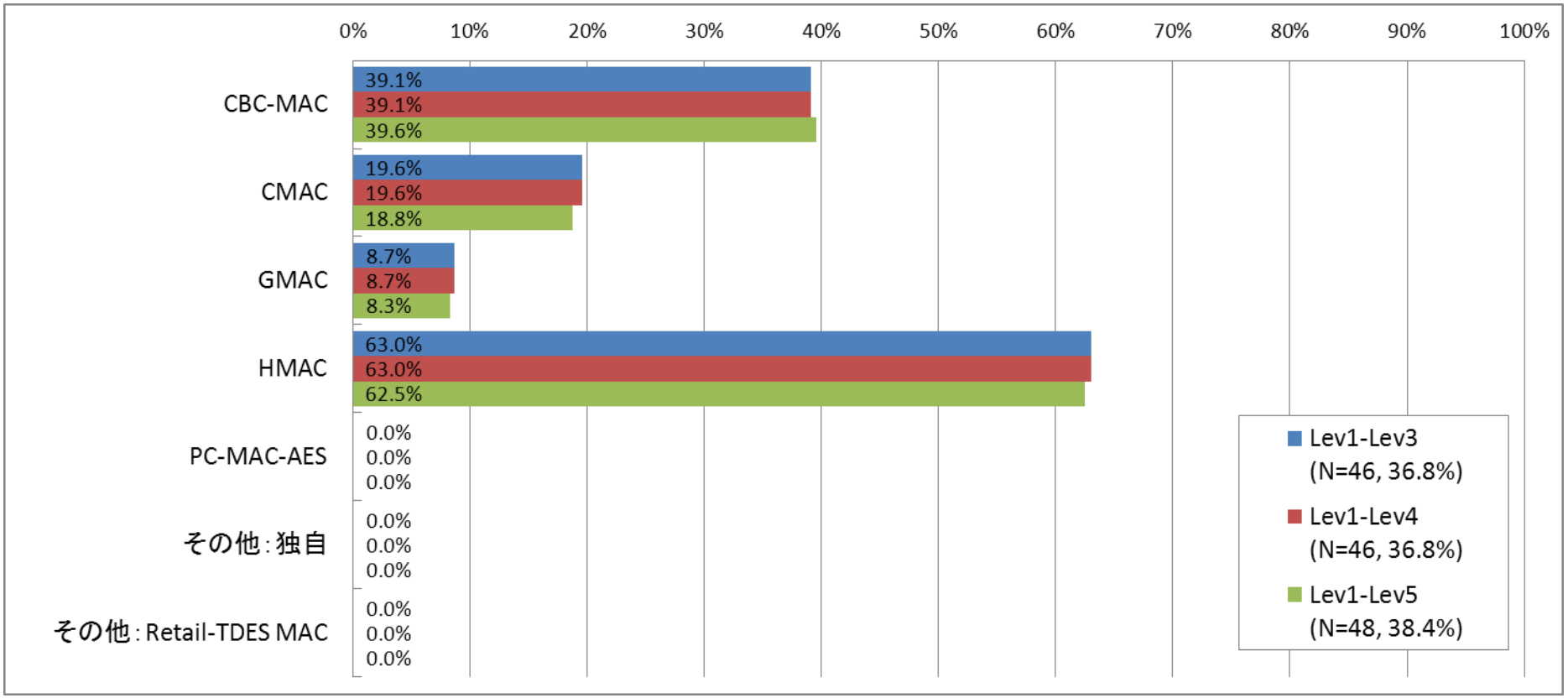
4.2.市販製品調査結果（調査B結果・暗号モジュール）

7. 暗号利用モード



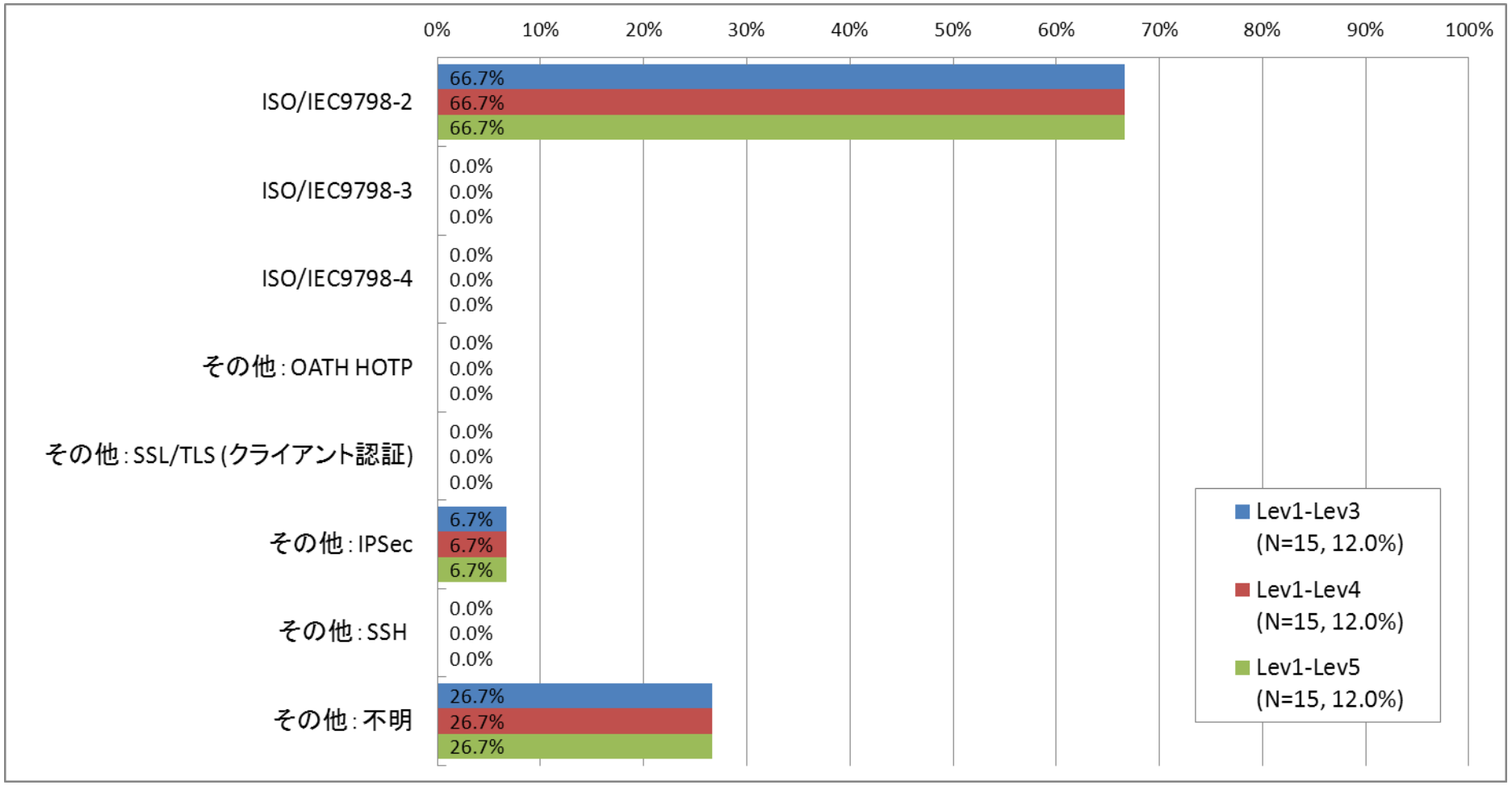
４.２.市販製品調査結果（調査B結果・暗号モジュール）

8. メッセージ認証コード



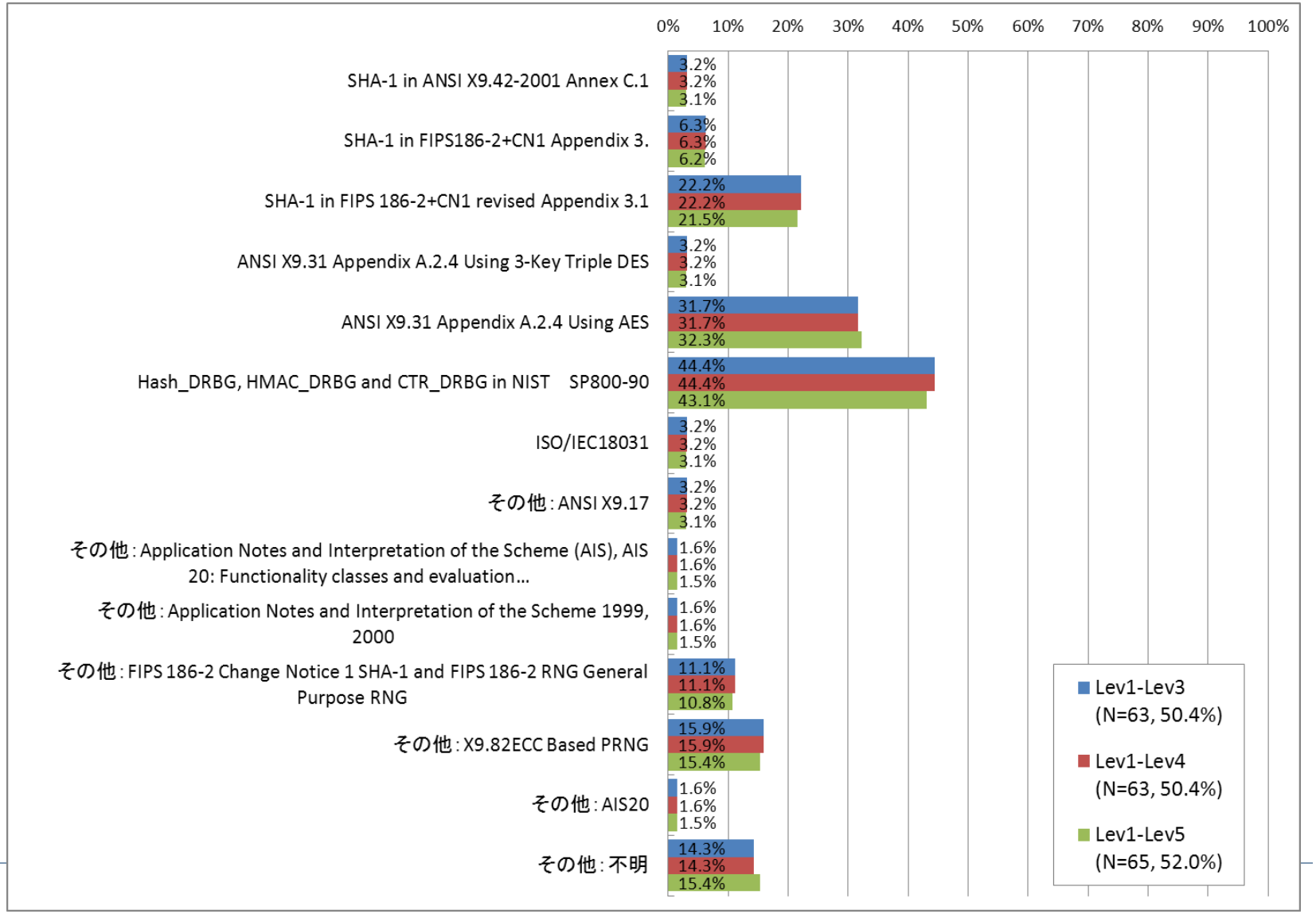
4.2.市販製品調査結果（調査B結果・暗号モジュール）

9. エンティティ認証



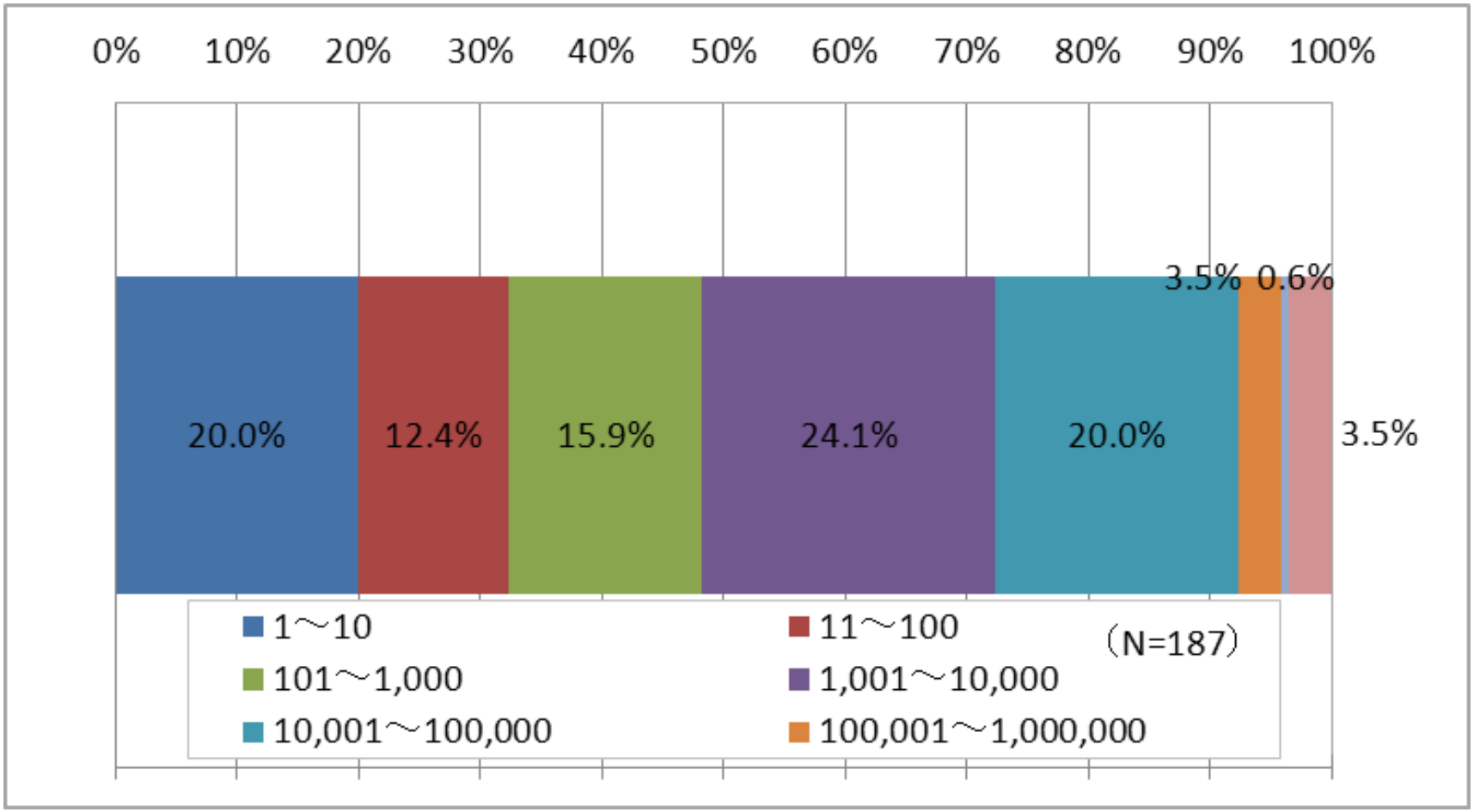
4.2.市販製品調査結果（調査B結果・暗号モジュール）

10. 擬似乱数生成方式



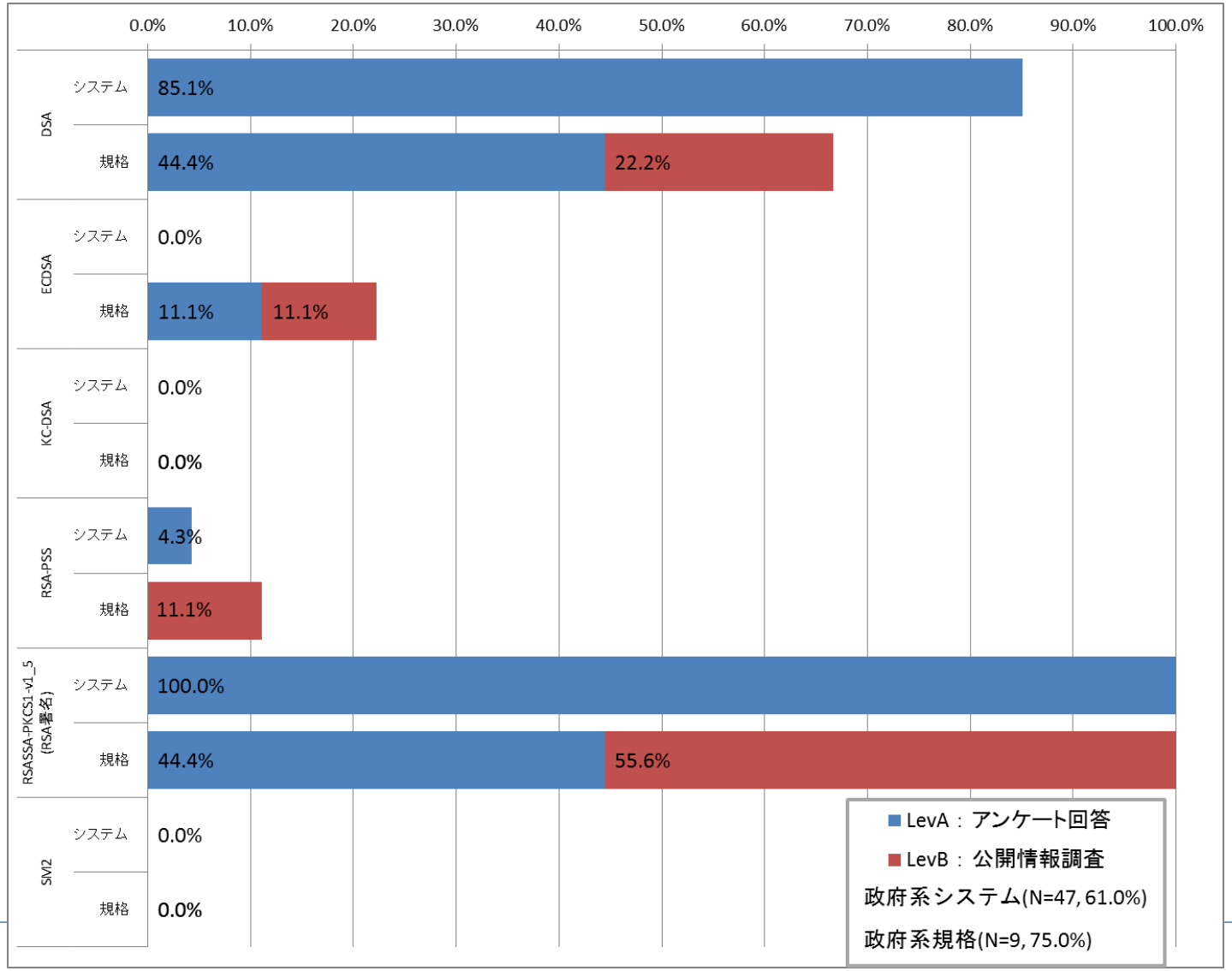
４.２.市販製品調査結果（オプション設問）

11. 直近1年間の総出荷台数（市販製品全てに対する出荷台数の比率）



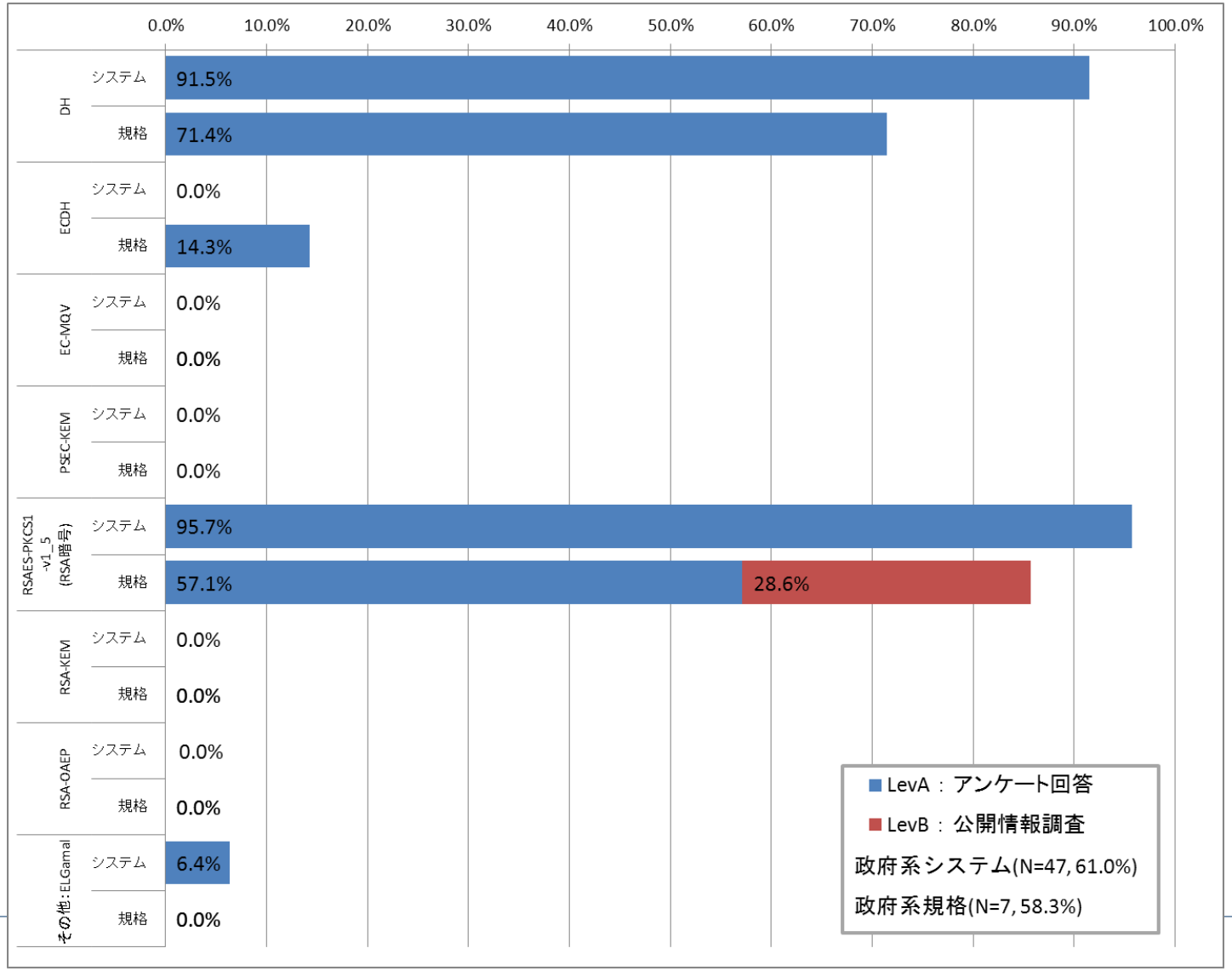
4.3.政府系情報システム調査結果（調査C結果）

1. 公開鍵暗号(署名)



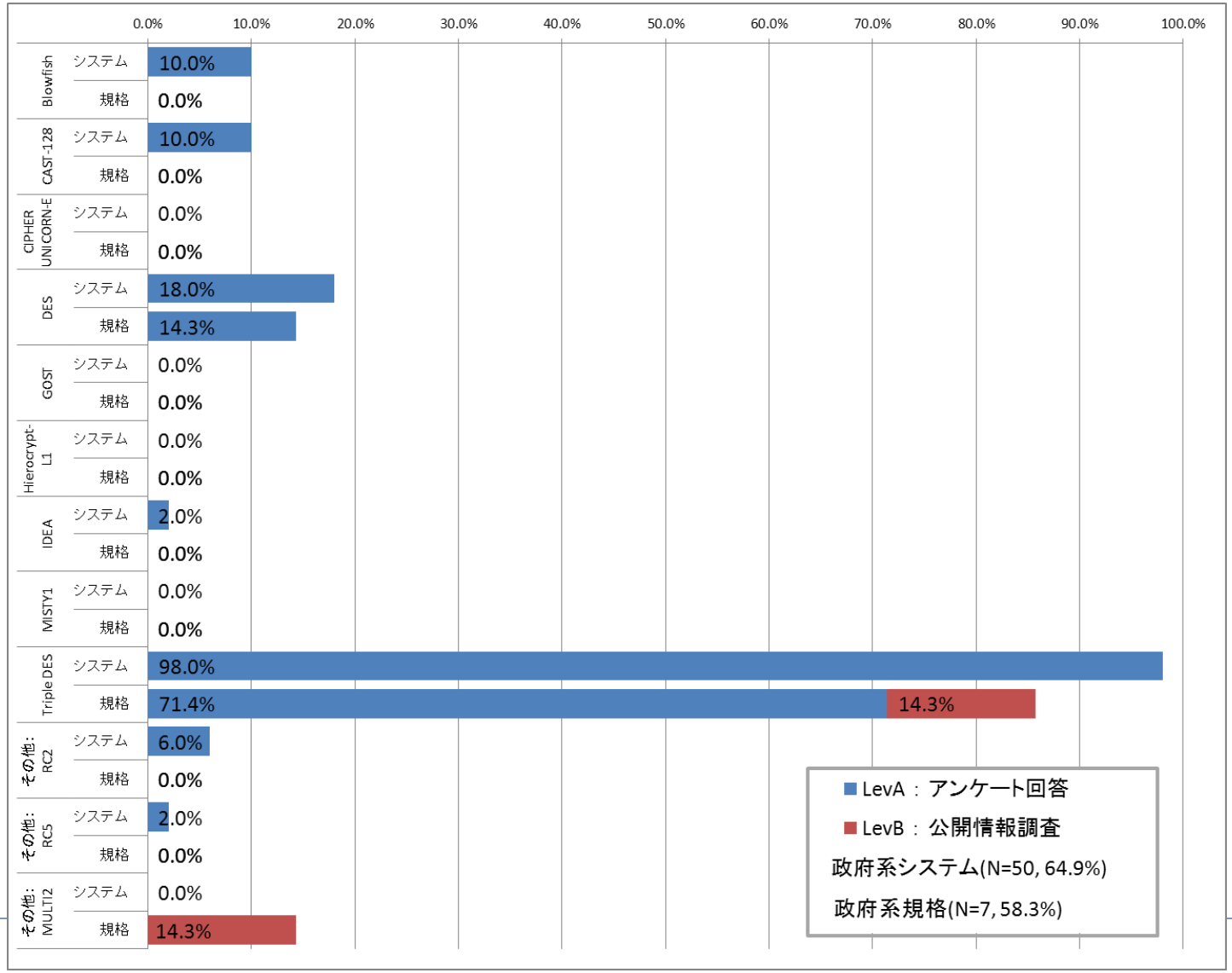
4.3.政府系情報システム調査結果（調査C結果）

2. 公開鍵暗号(守秘・鍵共有)



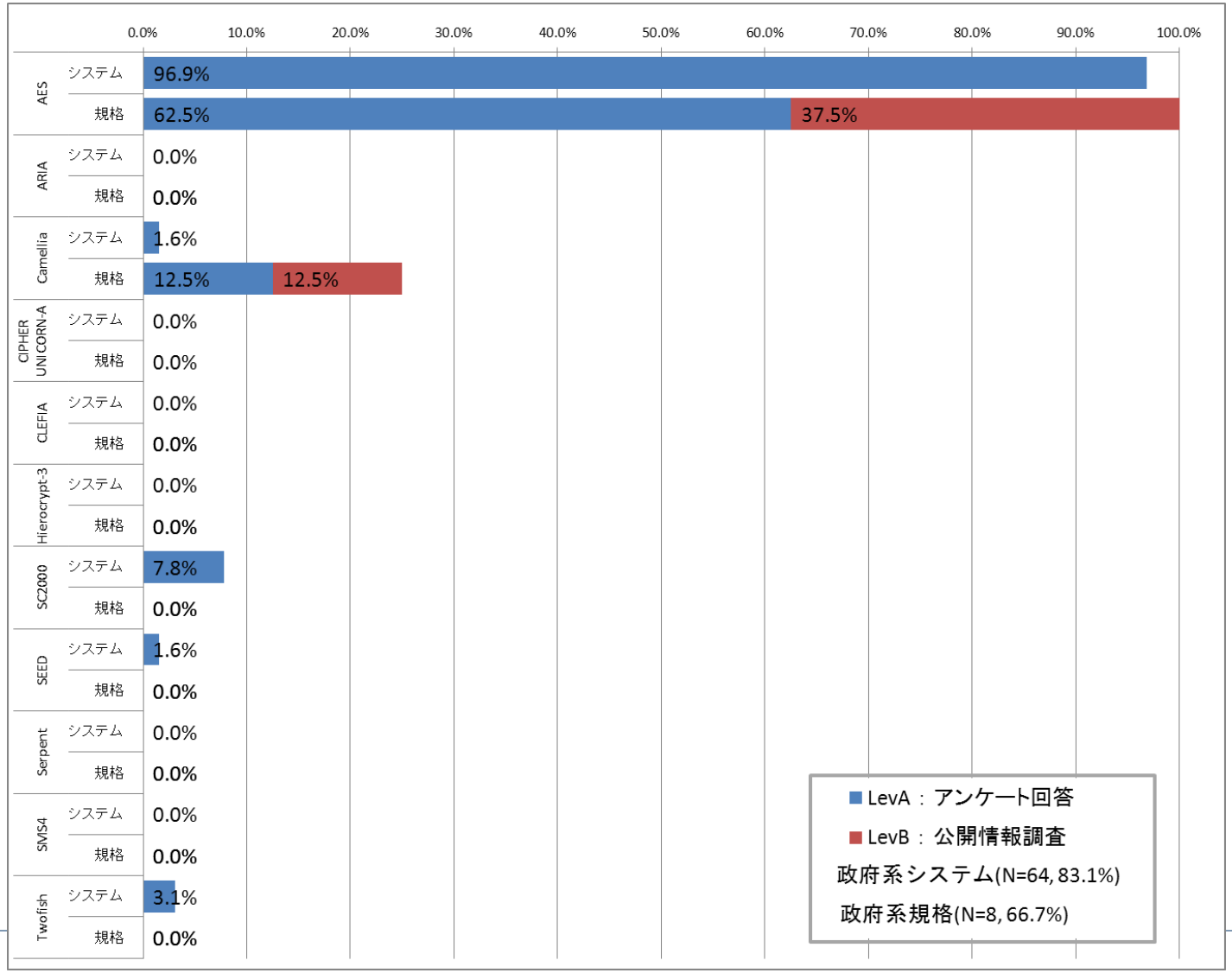
4.3.政府系情報システム調査結果（調査C結果）

3. 共通鍵暗号（64ビットブロック暗号）



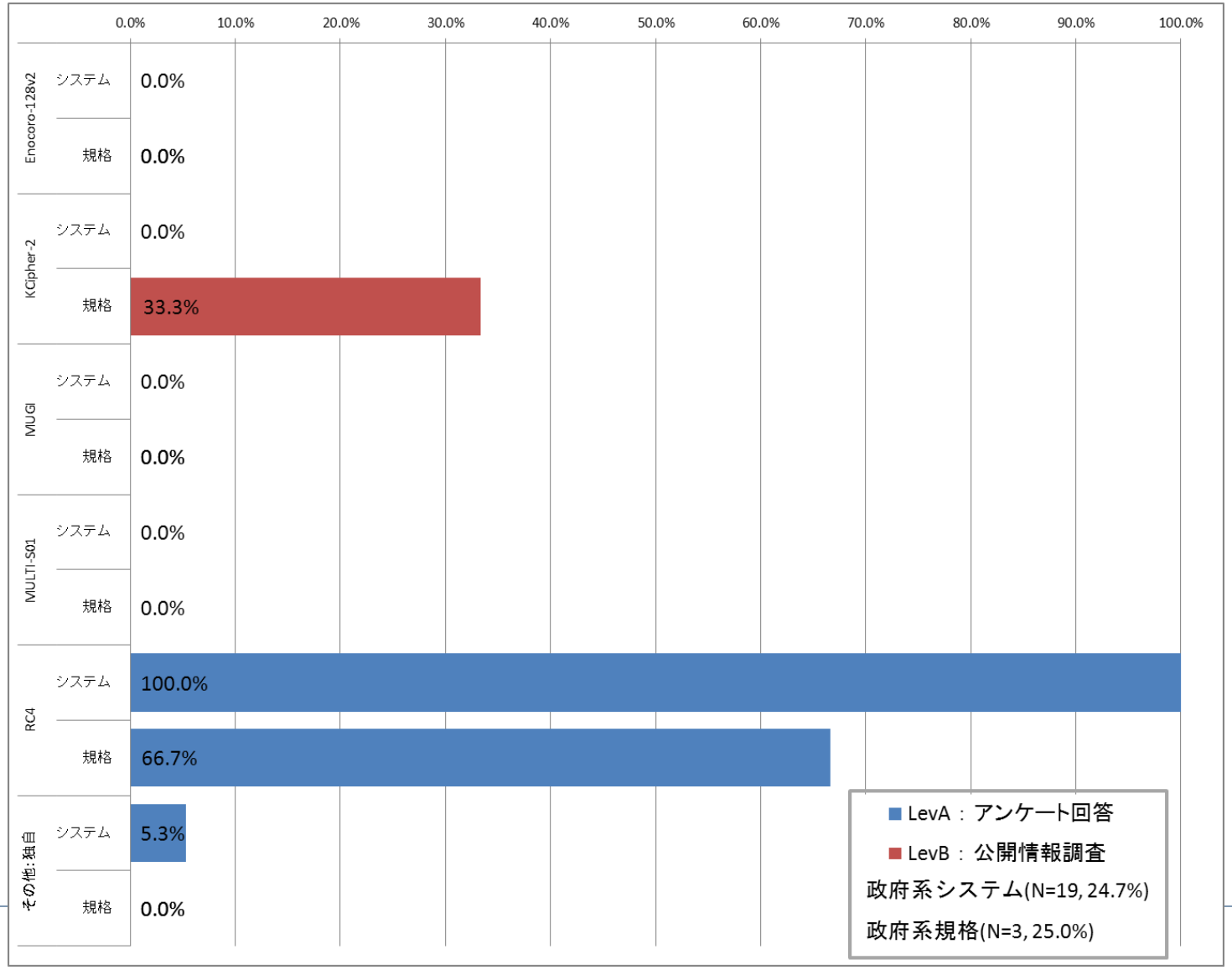
4.3.政府系情報システム調査結果（調査C結果）

4. 共通鍵暗号（128ビットブロック暗号）



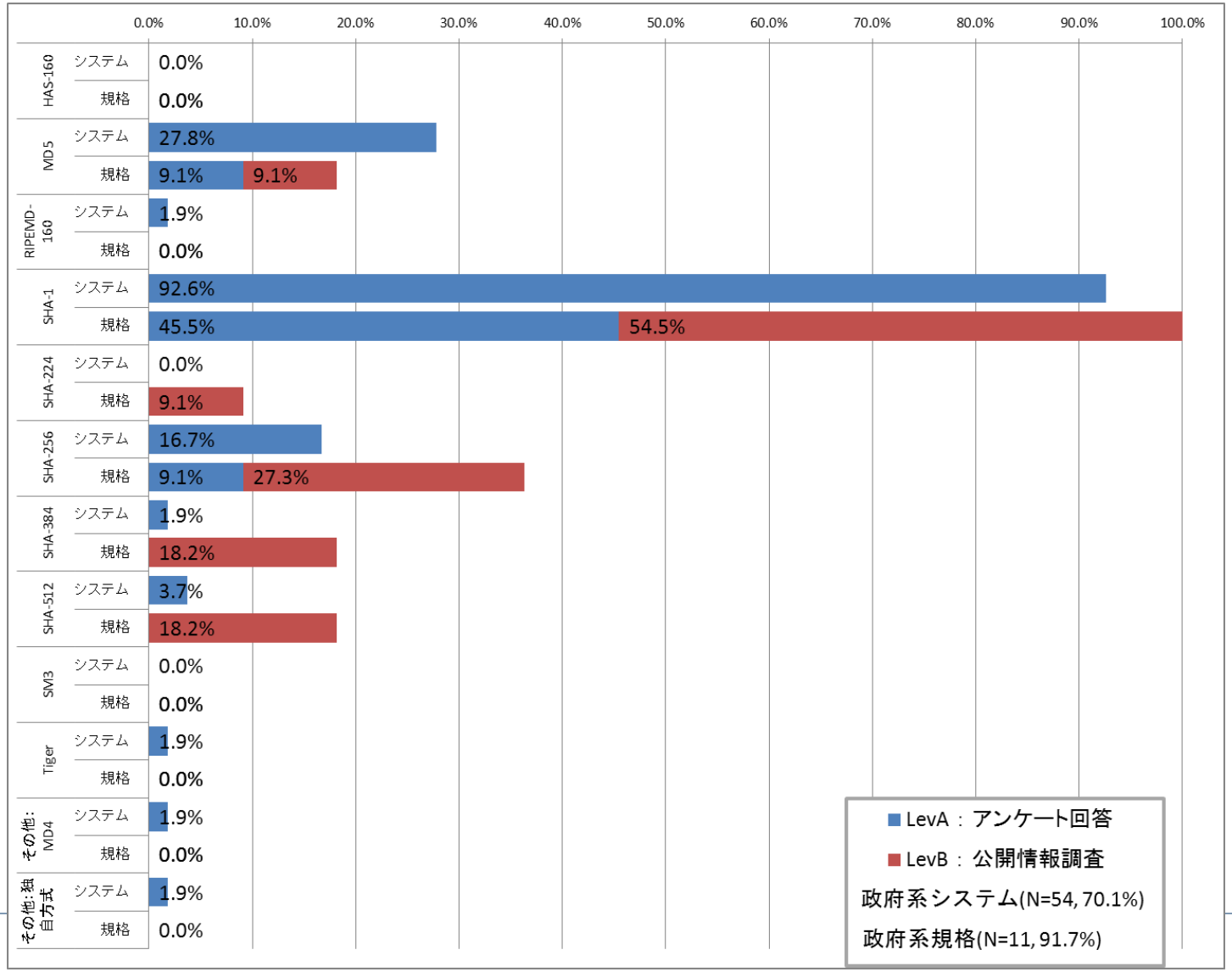
4.3.政府系情報システム調査結果（調査C結果）

5. 共通鍵暗号(ストリーム暗号)



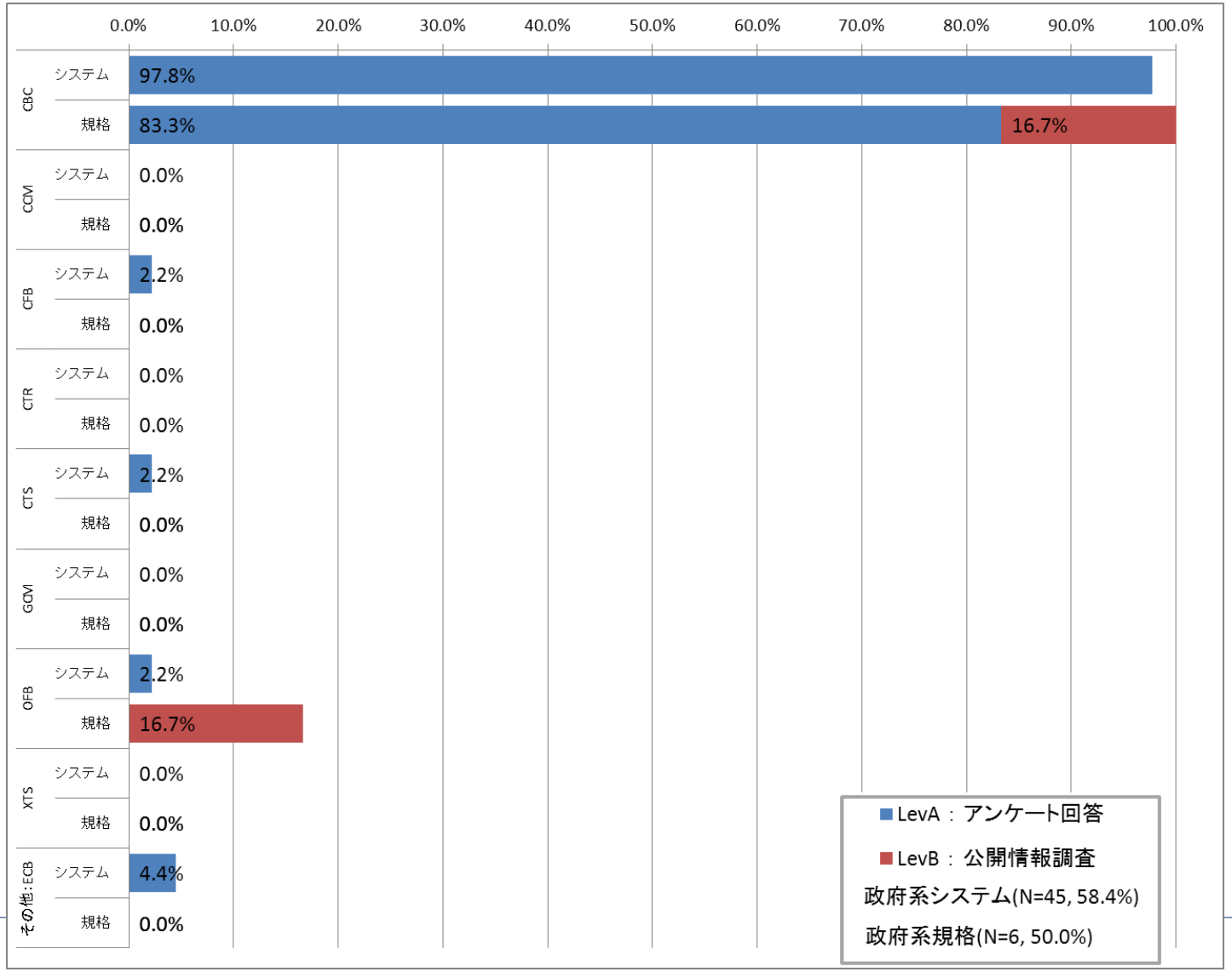
4.3.政府系情報システム調査結果（調査C結果）

6. ハッシュ関数



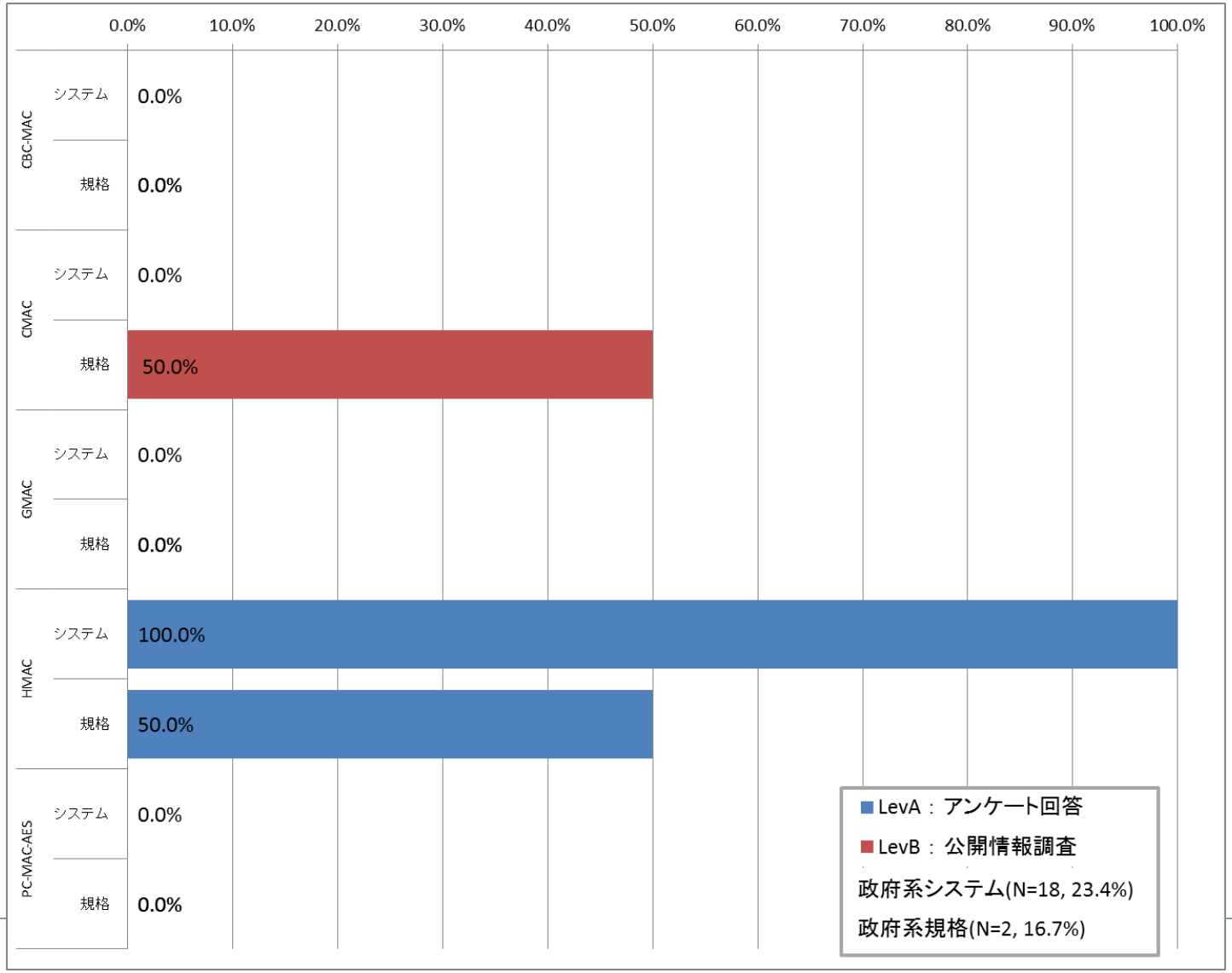
4.3.政府系情報システム調査結果（調査C結果）

7. 暗号利用モード



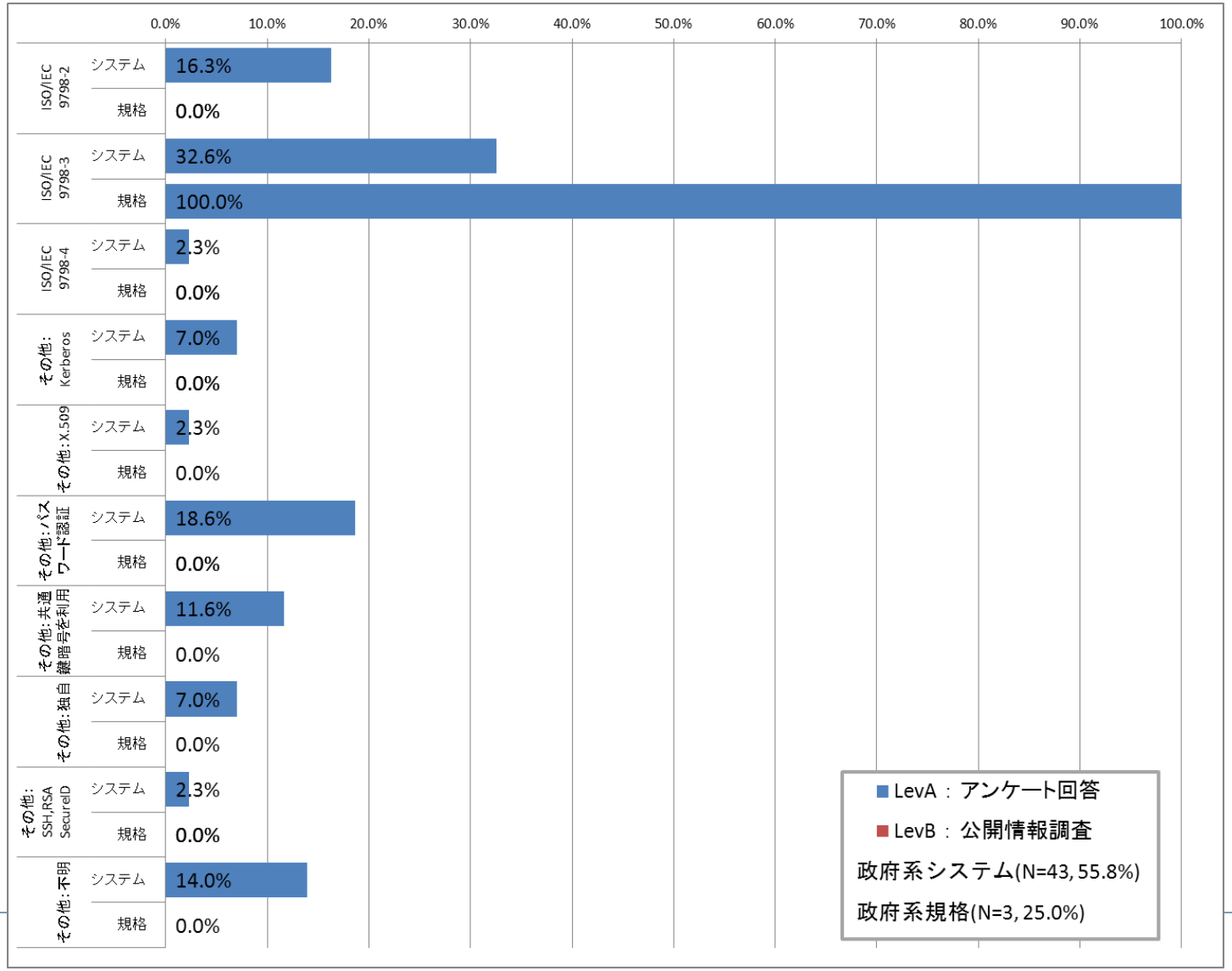
4.3.政府系情報システム調査結果（調査C結果）

8. メッセージ認証コード



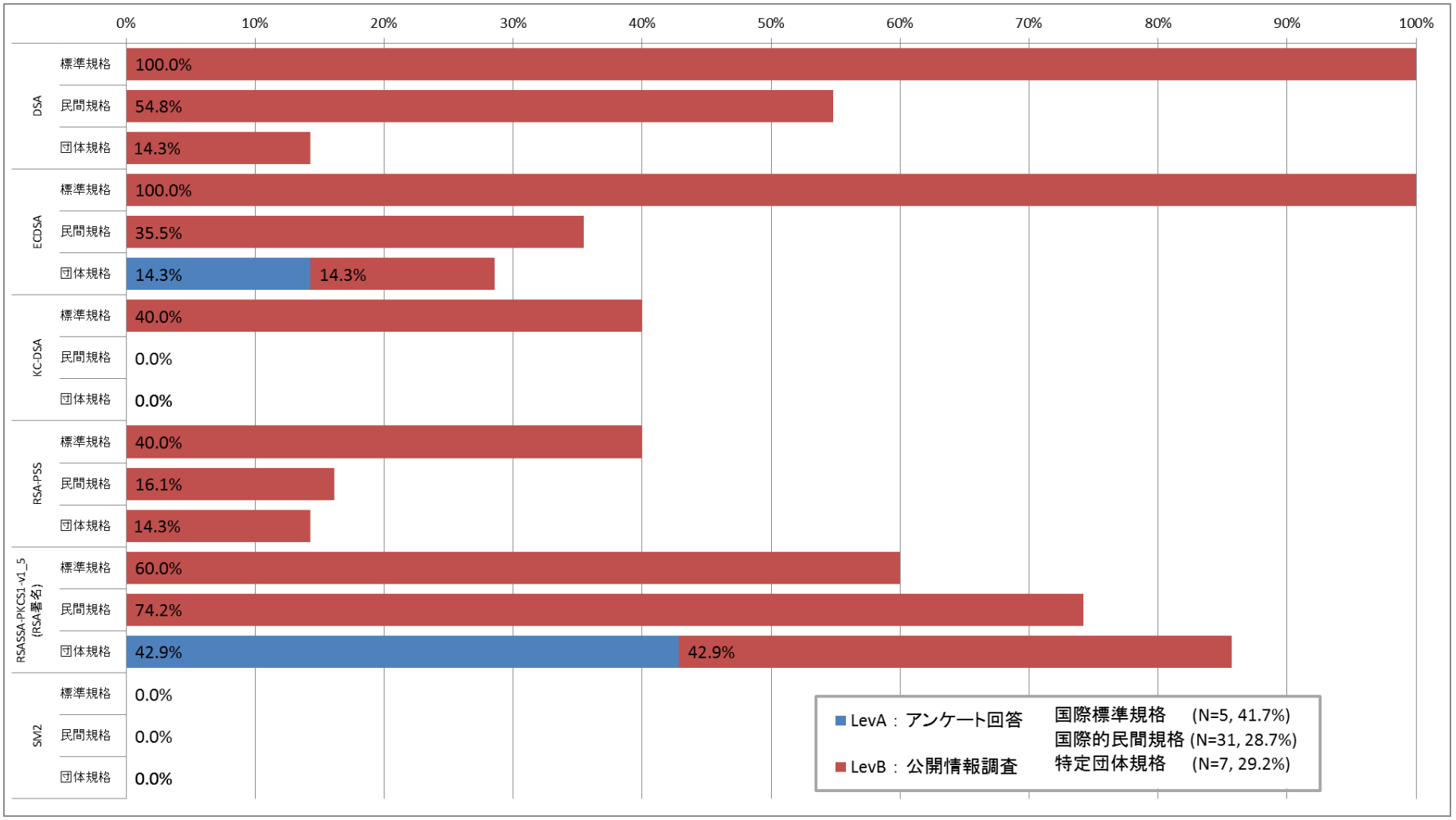
4.3.政府系情報システム調査結果（調査C結果）

9. エンティティ認証



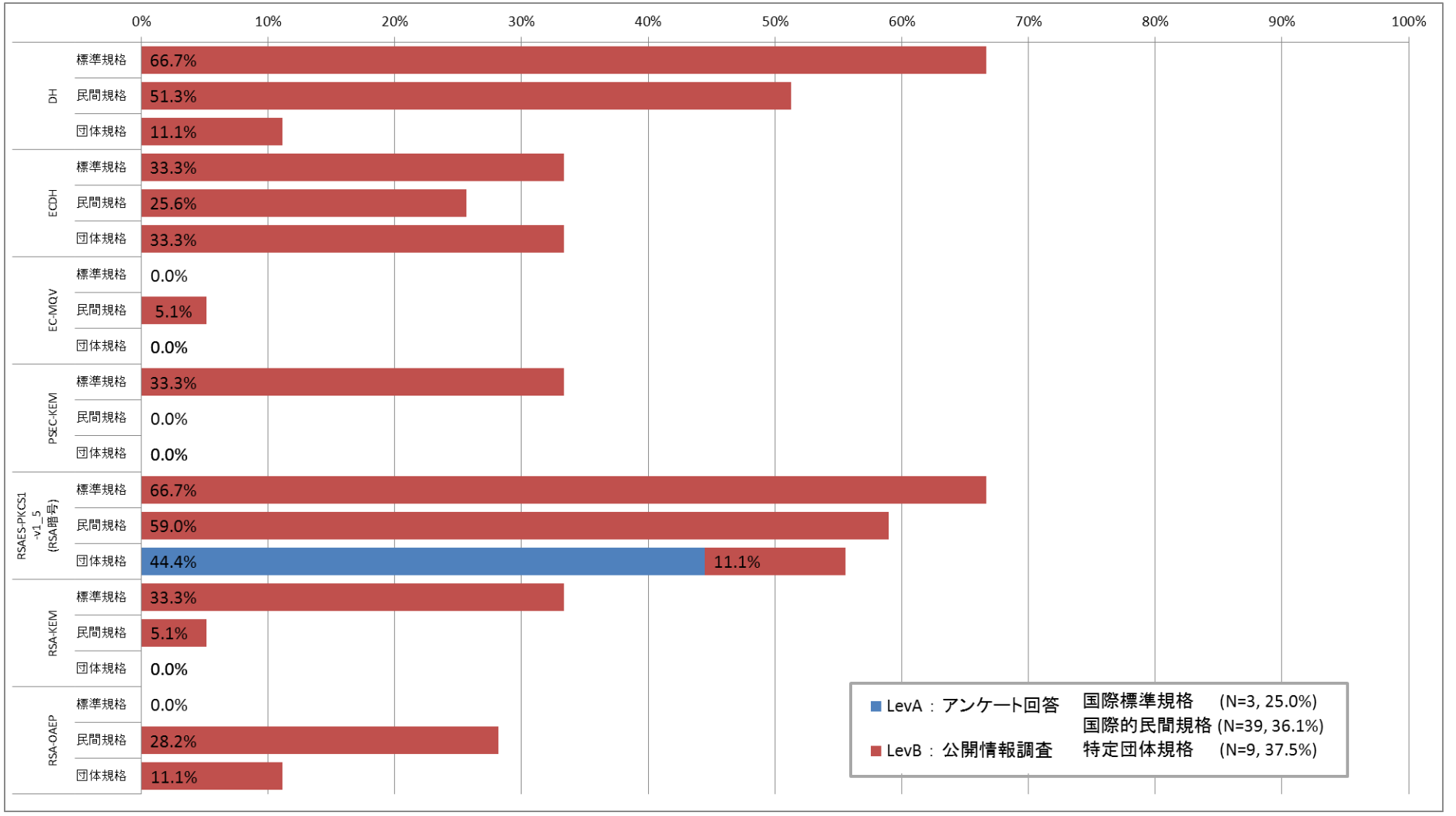
4.4.標準規格等調査結果（調査D結果）

1. 公開鍵暗号(署名)



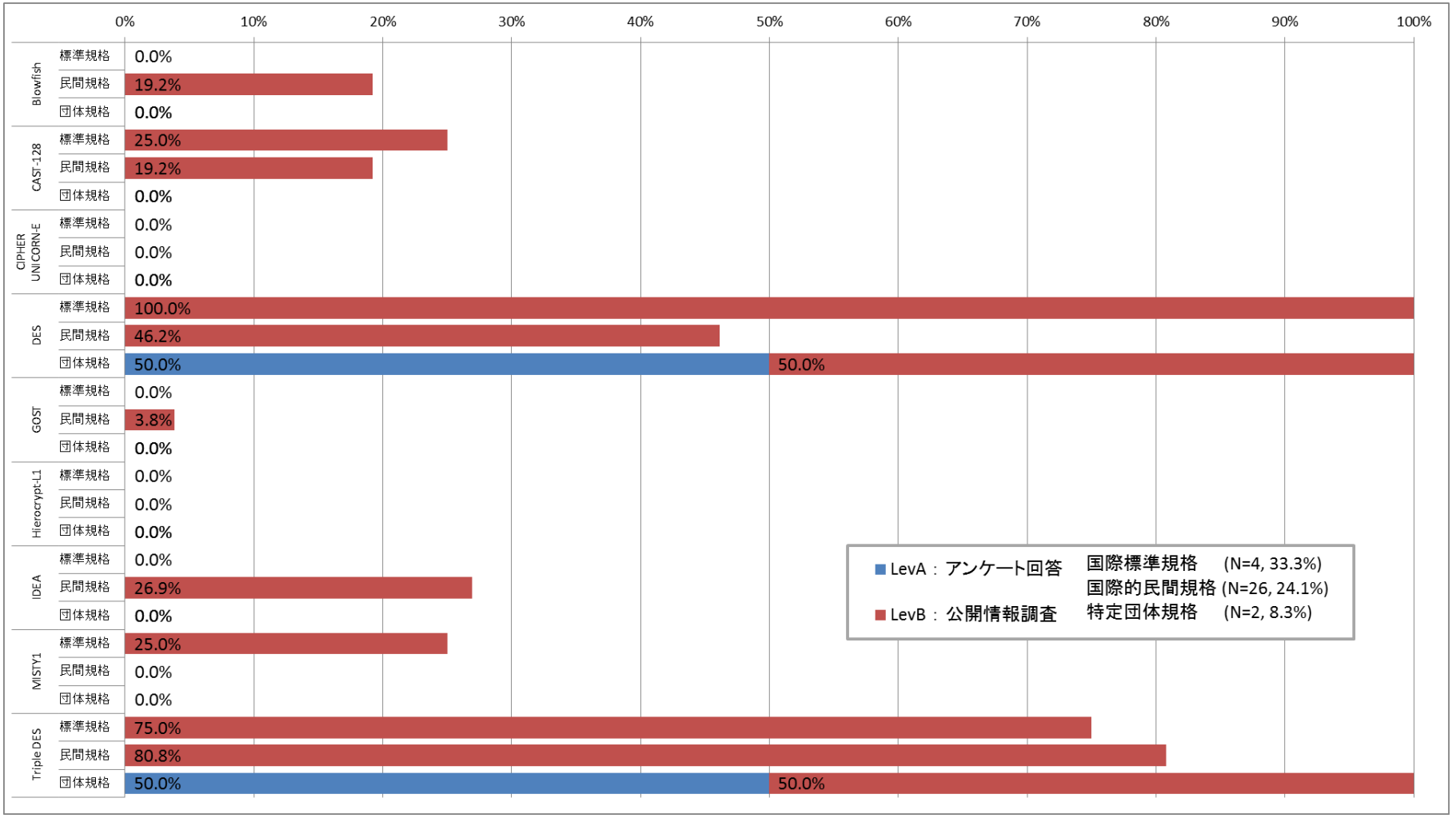
4.4.標準規格等調査結果（調査D結果）

2. 公開鍵暗号(守秘・鍵共有)



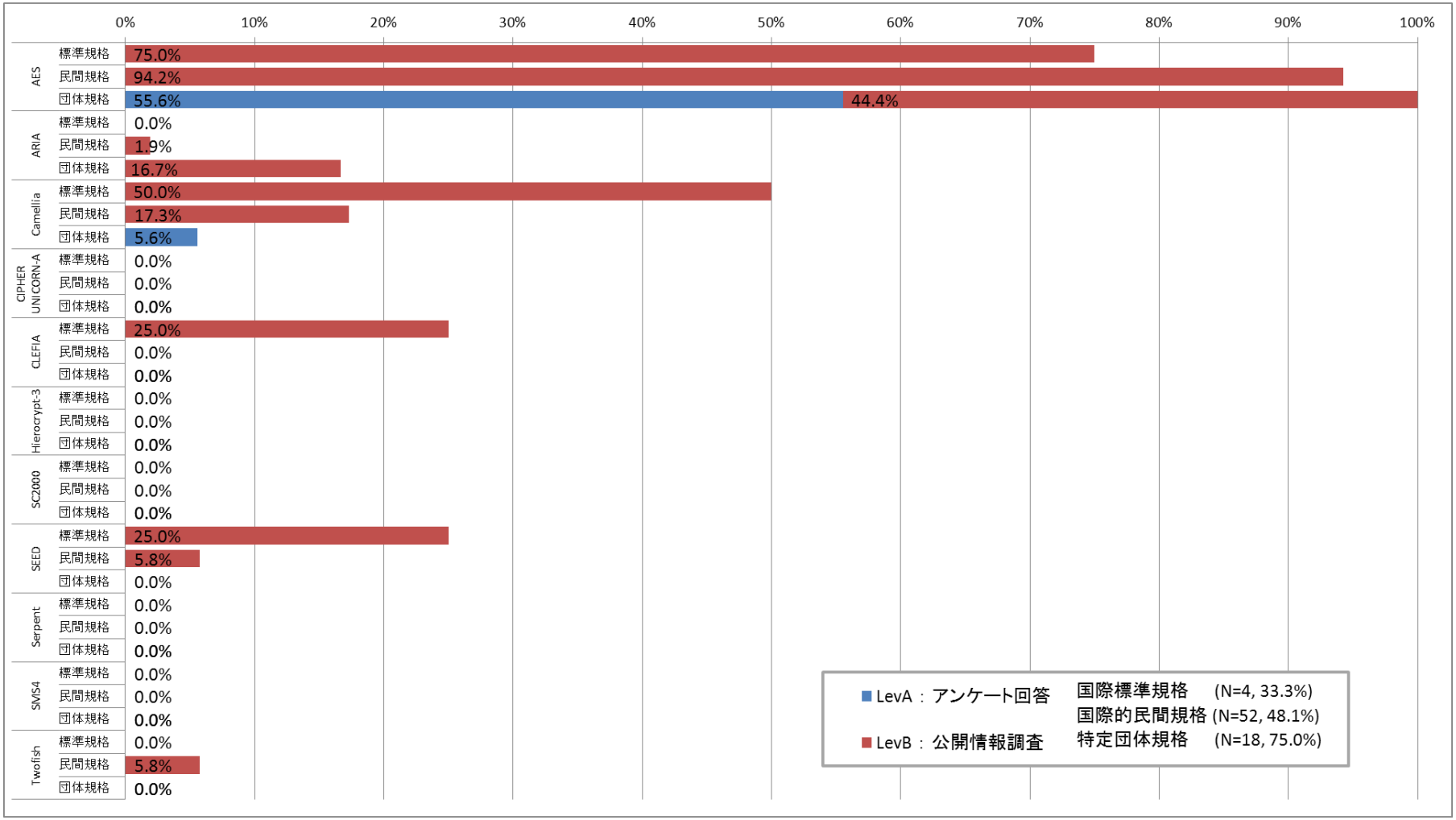
4.4.標準規格等調査結果（調査D結果）

3. 共通鍵暗号（64ビットブロック暗号）



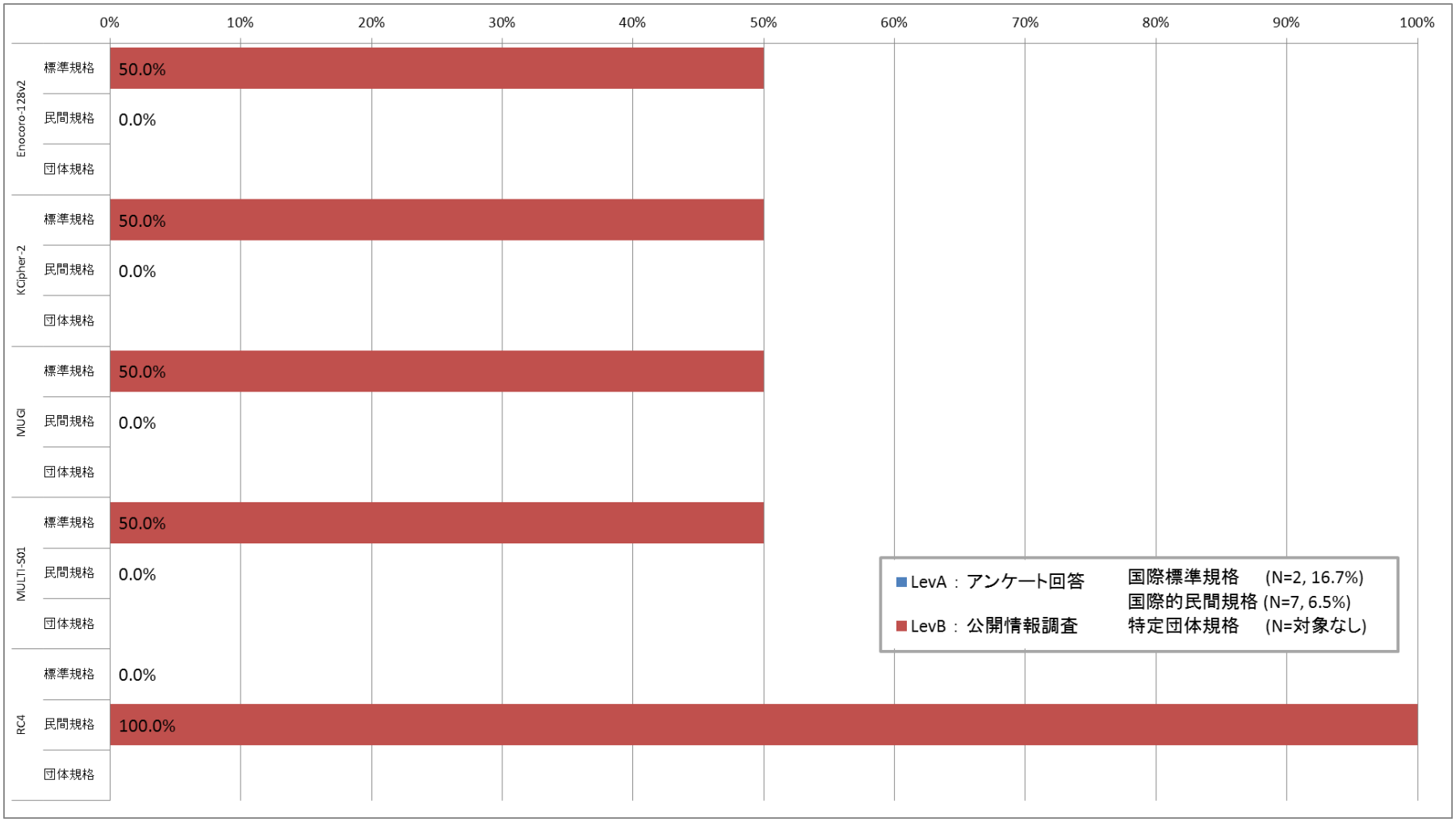
4.4.標準規格等調査結果（調査D結果）

4. 共通鍵暗号（128ビットブロック暗号）



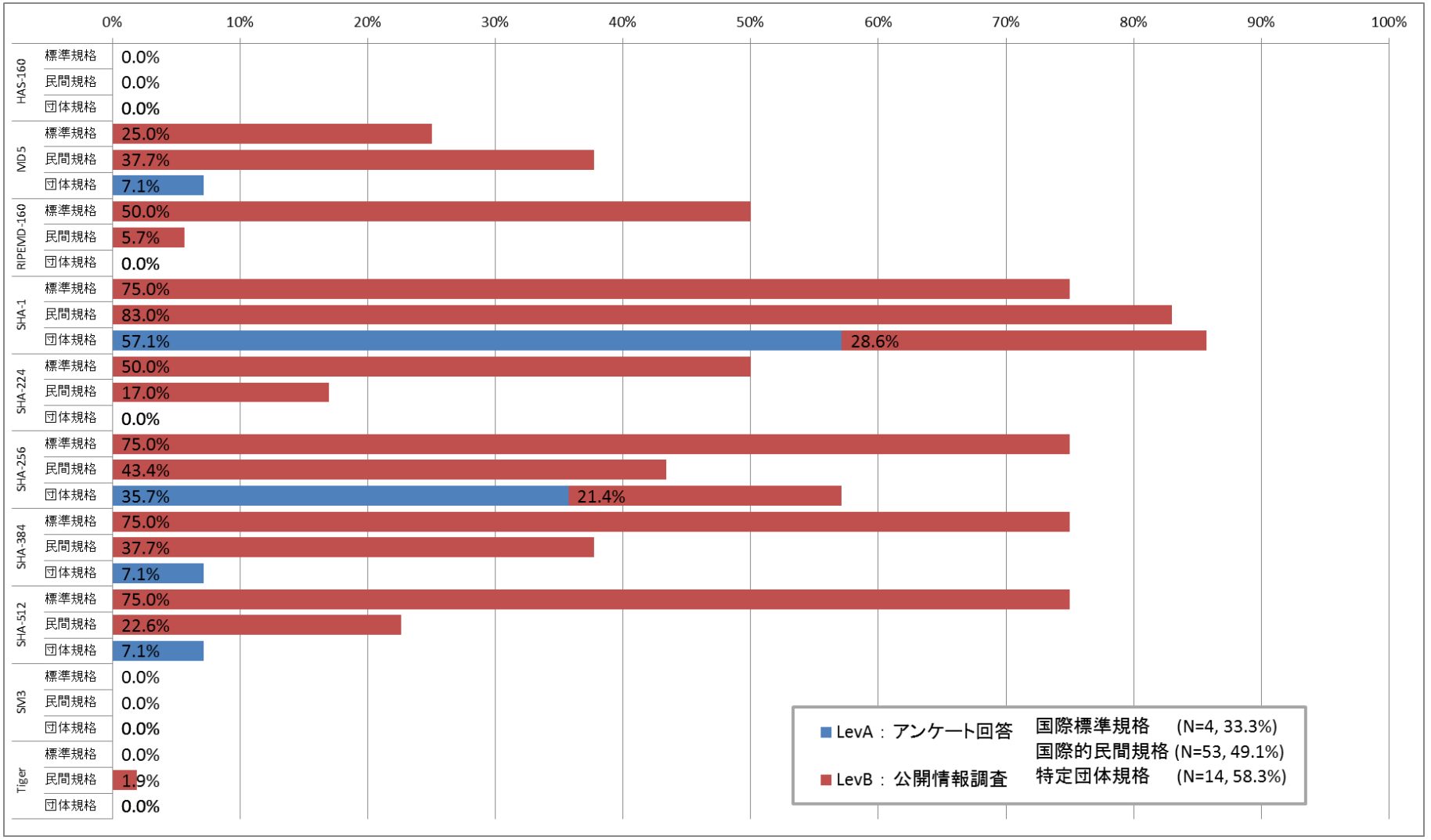
4.4.標準規格等調査結果（調査D結果）

5. 共通鍵暗号(ストリーム暗号)



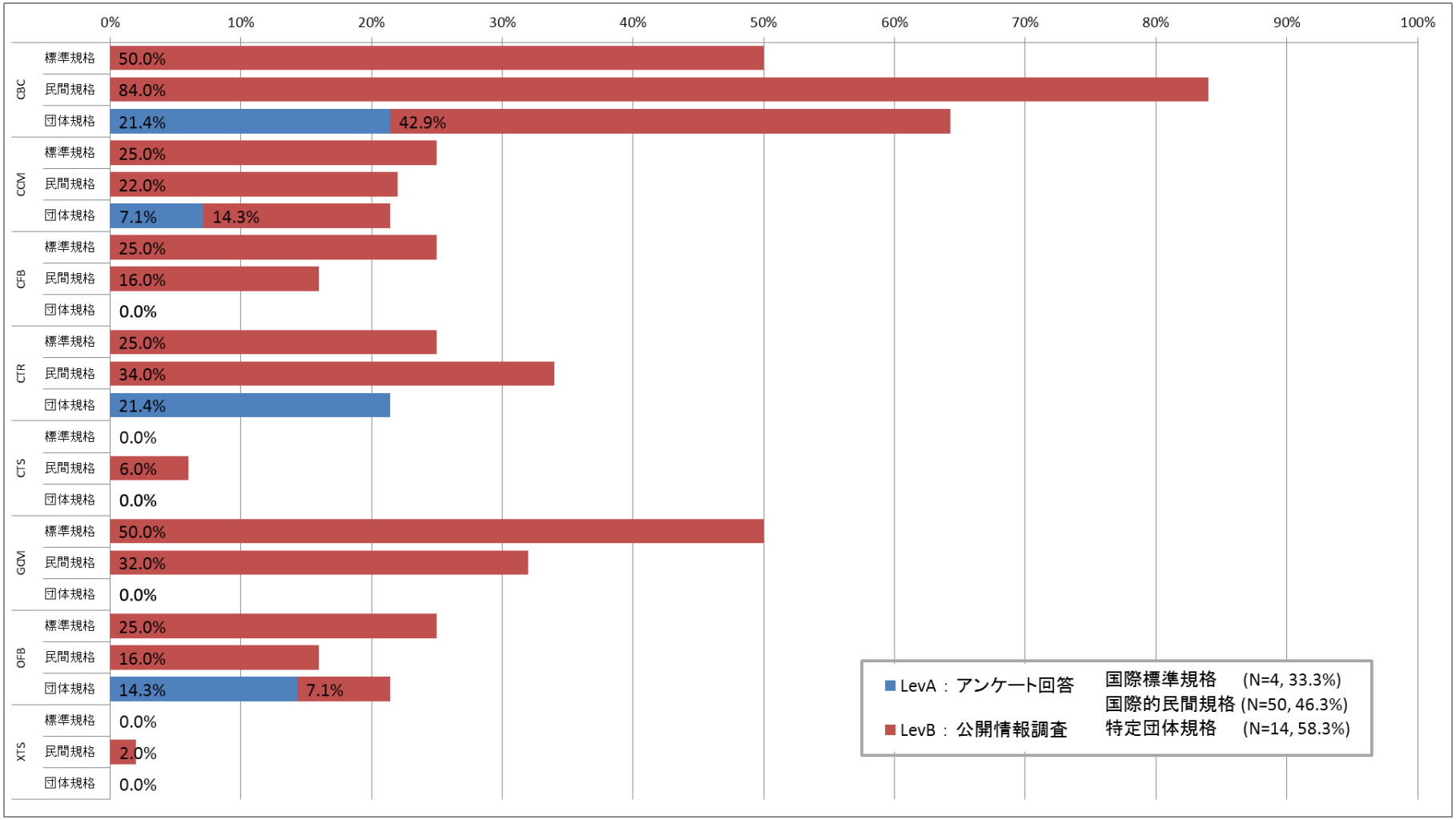
4.4.標準規格等調査結果（調査D結果）

6. ハッシュ関数



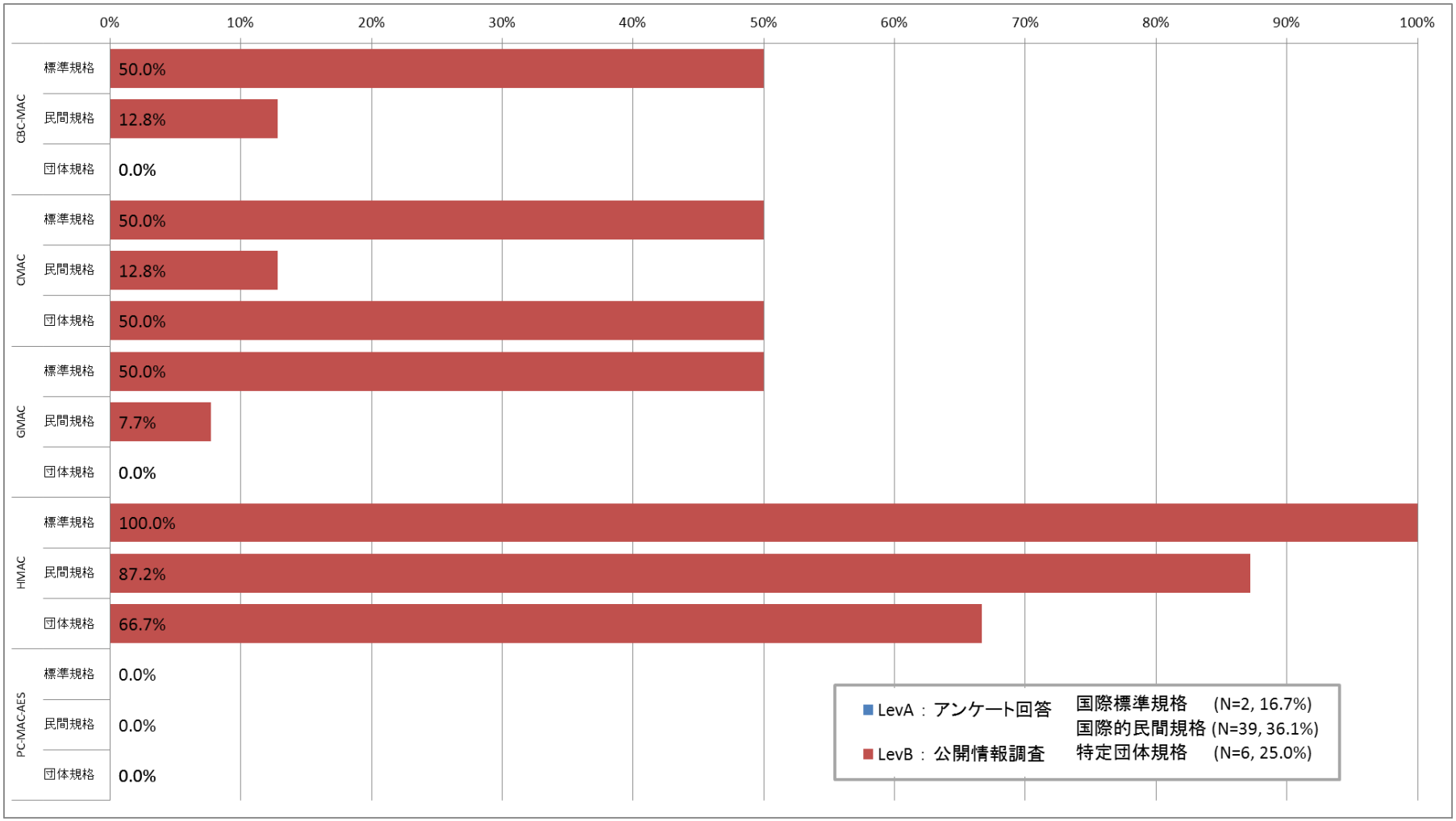
4.4.標準規格等調査結果（調査D結果）

7. 暗号利用モード



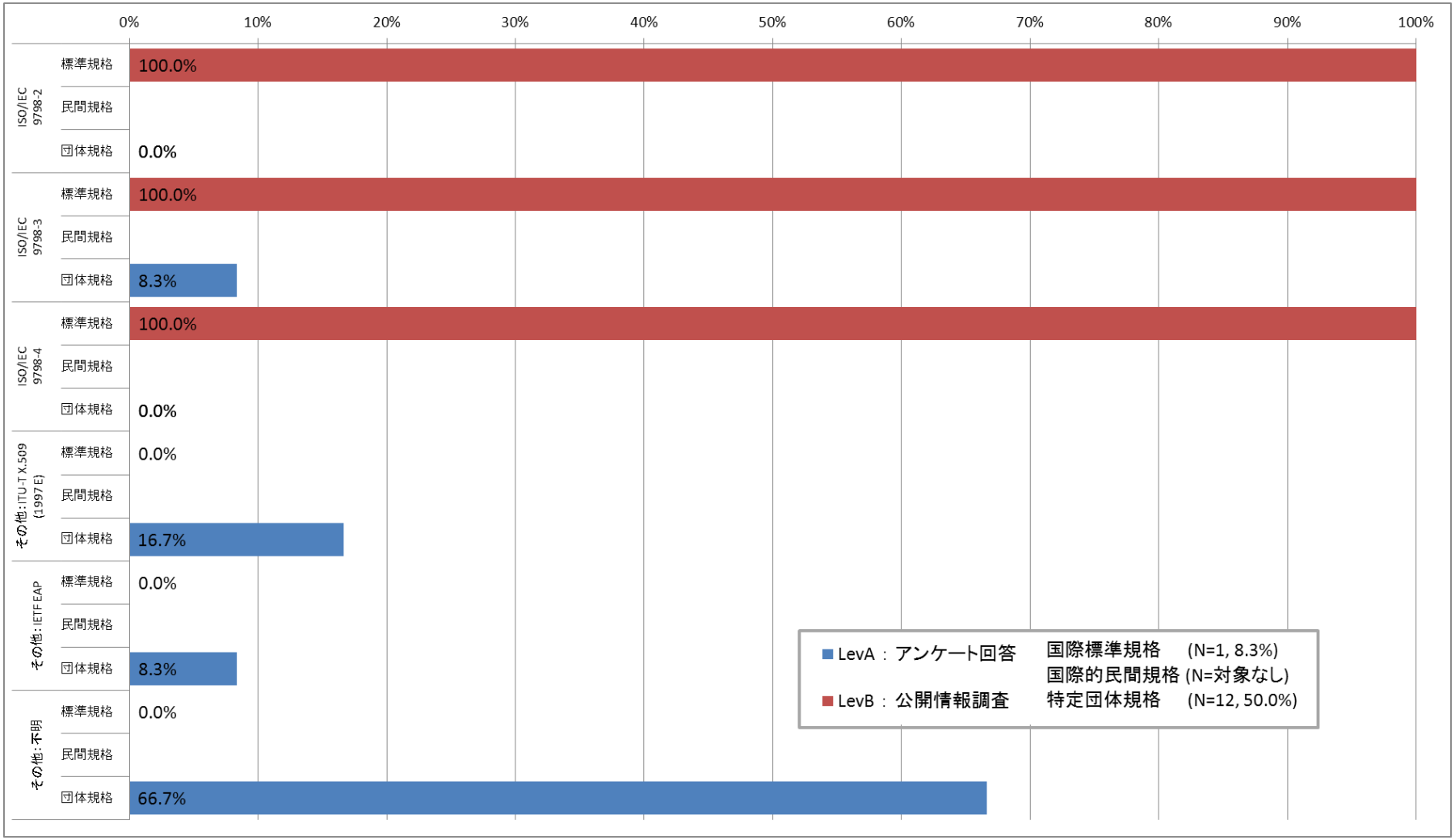
4.4.標準規格等調査結果（調査D結果）

8. メッセージ認証コード



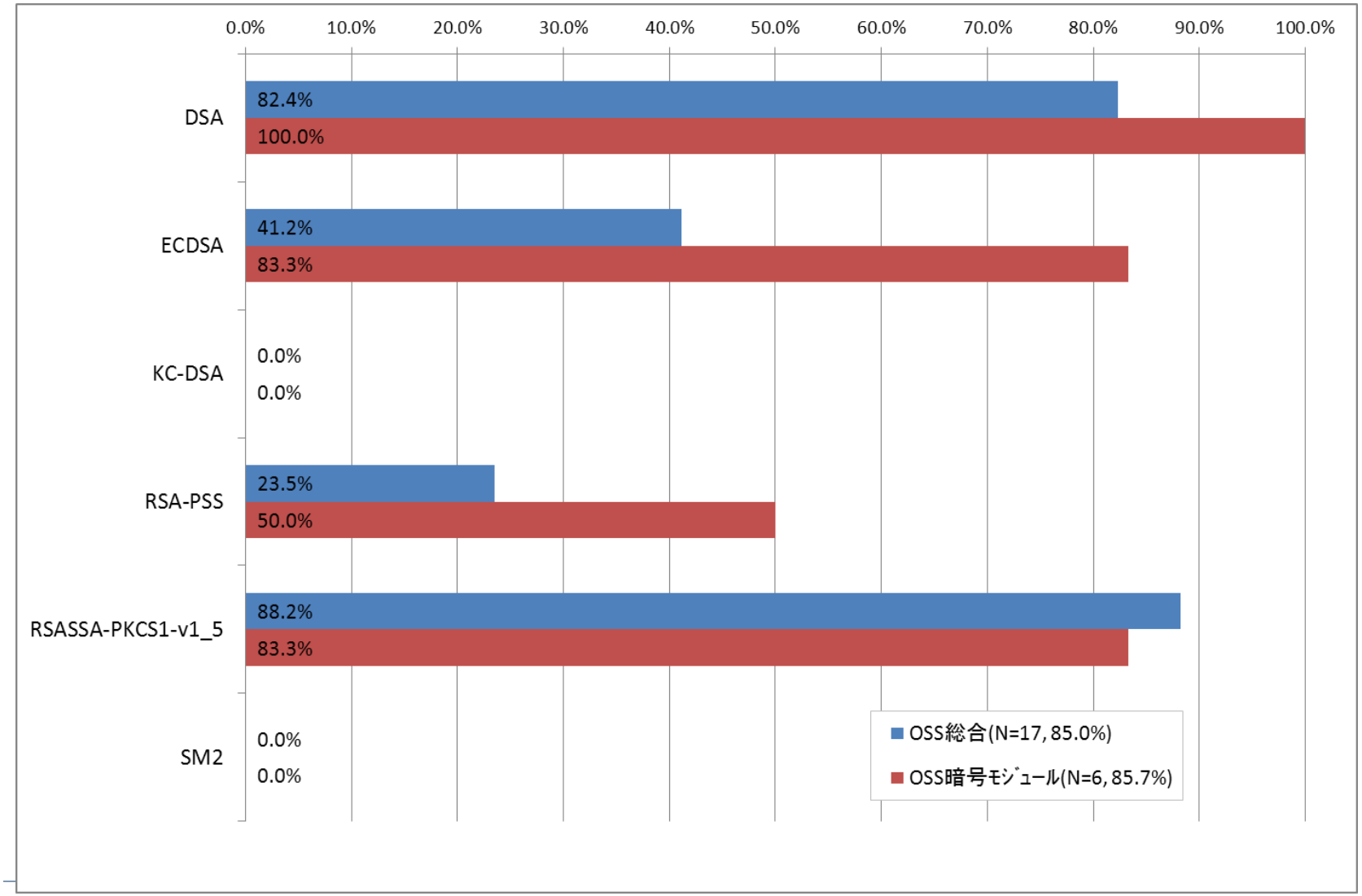
4.4.標準規格等調査結果（調査D結果）

9. エンティティ認証



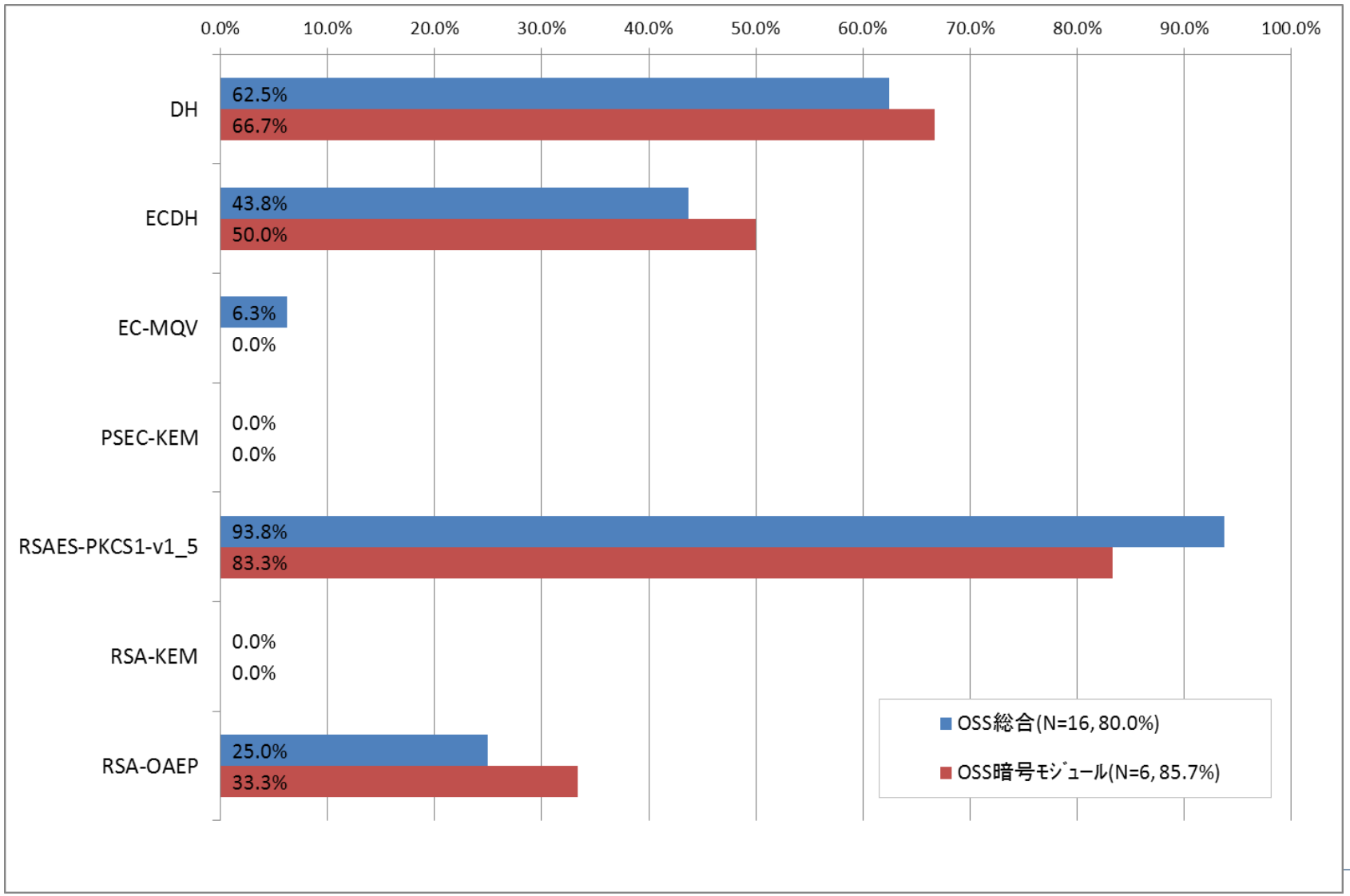
4.5.OSS調査結果（調査E結果）

1. 公開鍵暗号(署名)



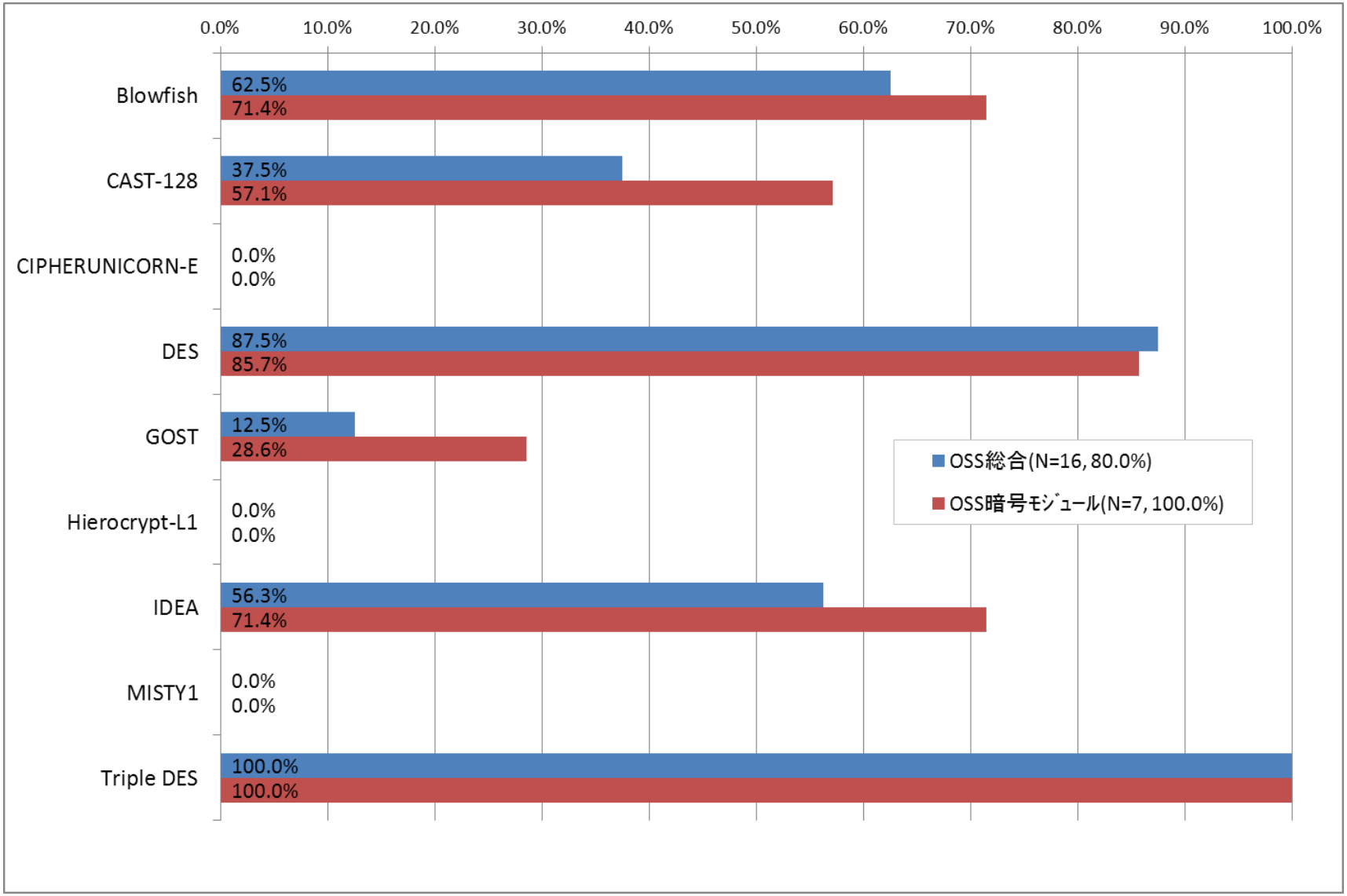
4.5.OSS調査結果（調査E結果）

2. 公開鍵暗号(守秘・鍵共有)



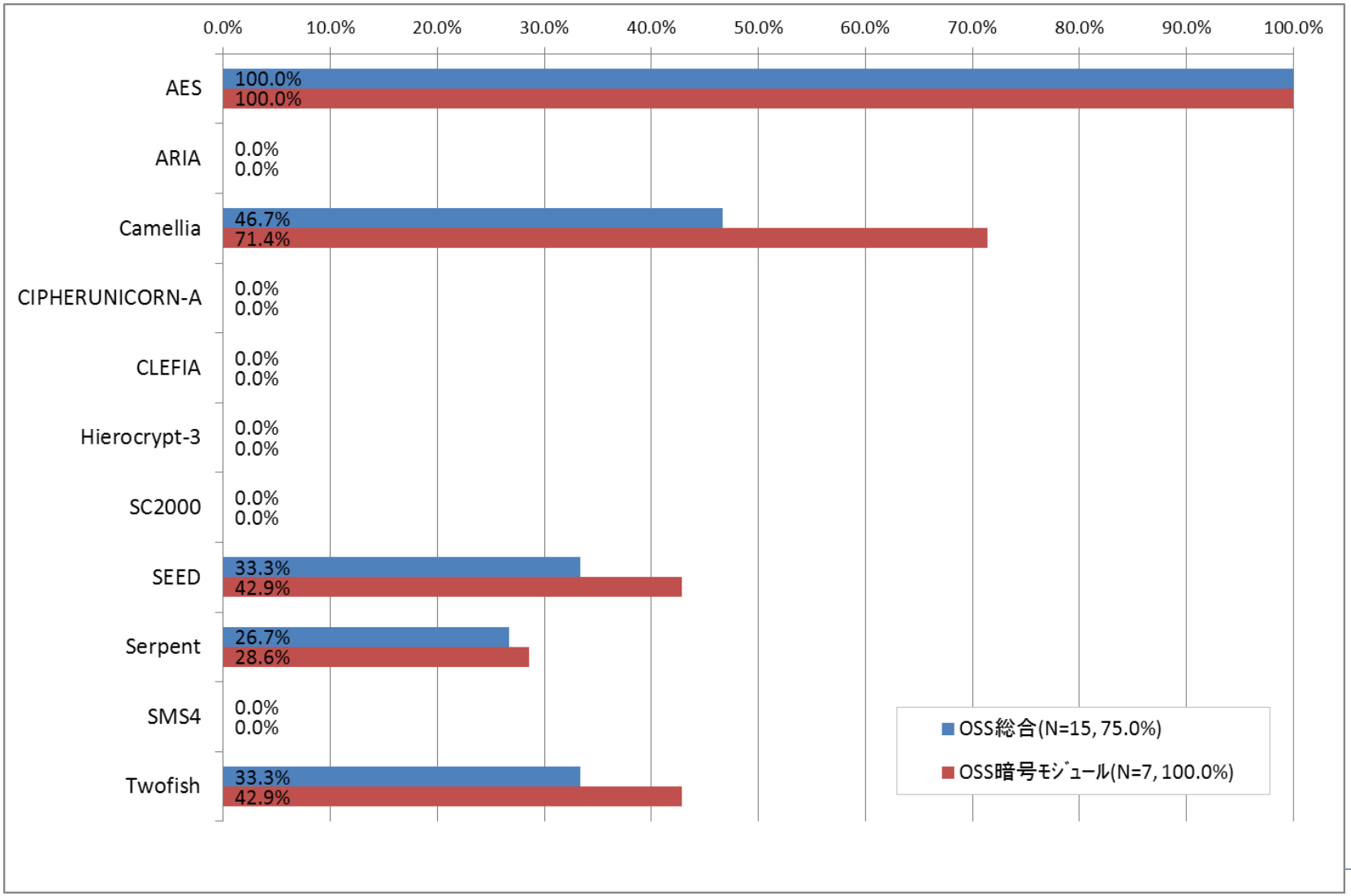
4.5.OSS調査結果（調査E結果）

3. 共通鍵暗号（64ビットブロック暗号）



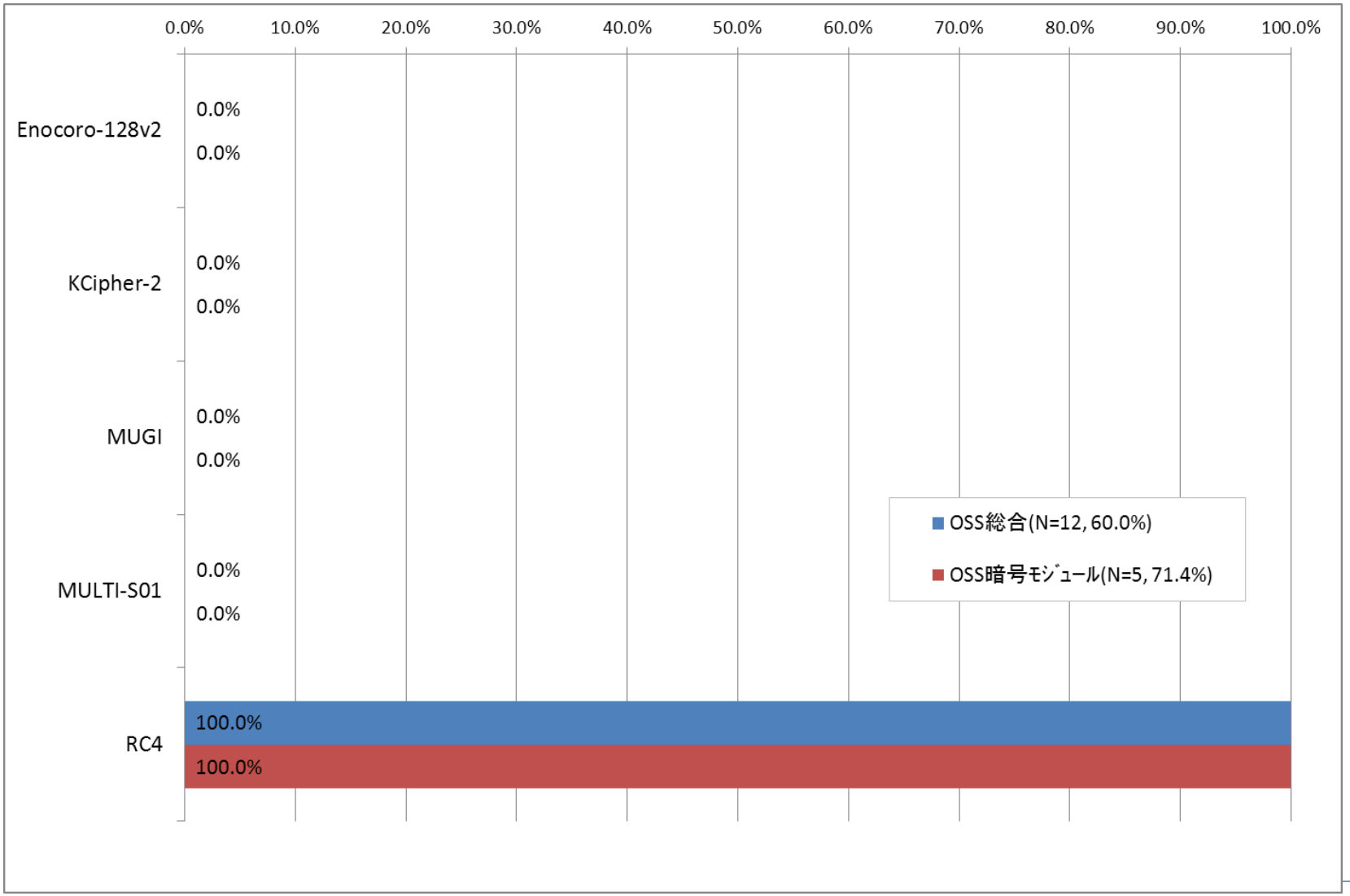
4.5.OSS調査結果（調査E結果）

4. 共通鍵暗号（128ビットブロック暗号）



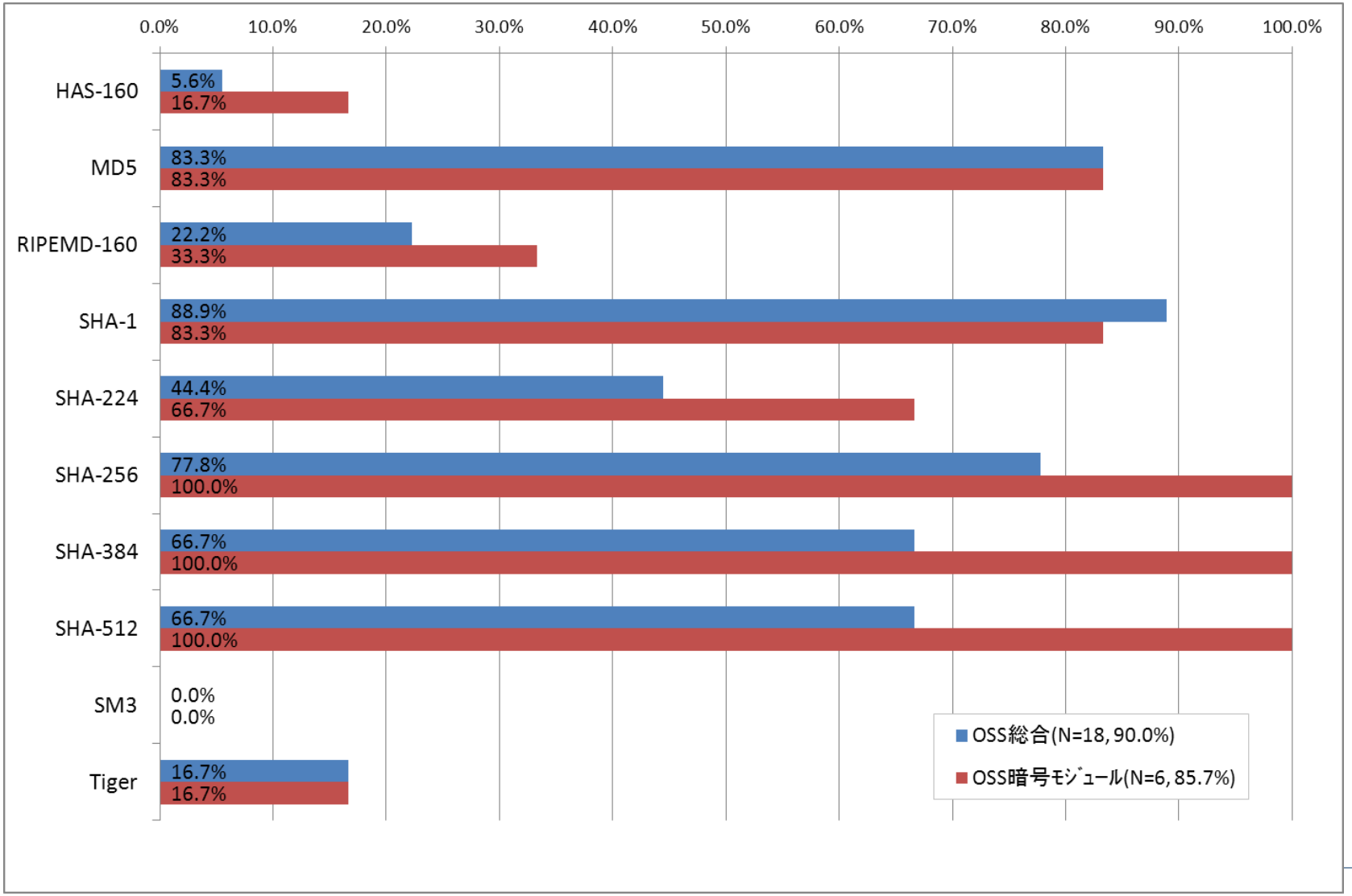
4.5.OSS調査結果（調査E結果）

5. 共通鍵暗号(ストリーム暗号)



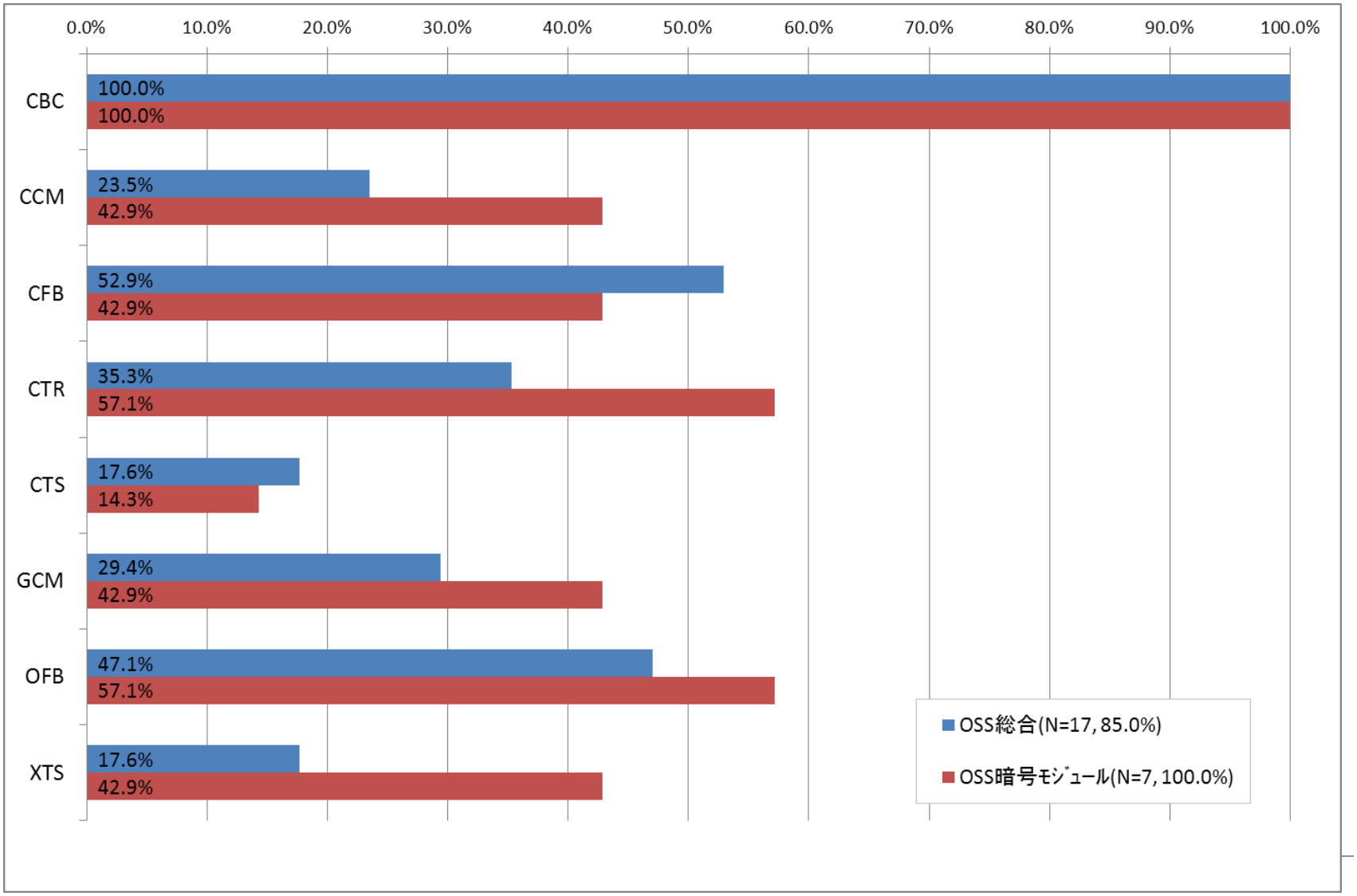
4.5.OSS調査結果（調査E結果）

6. ハッシュ関数



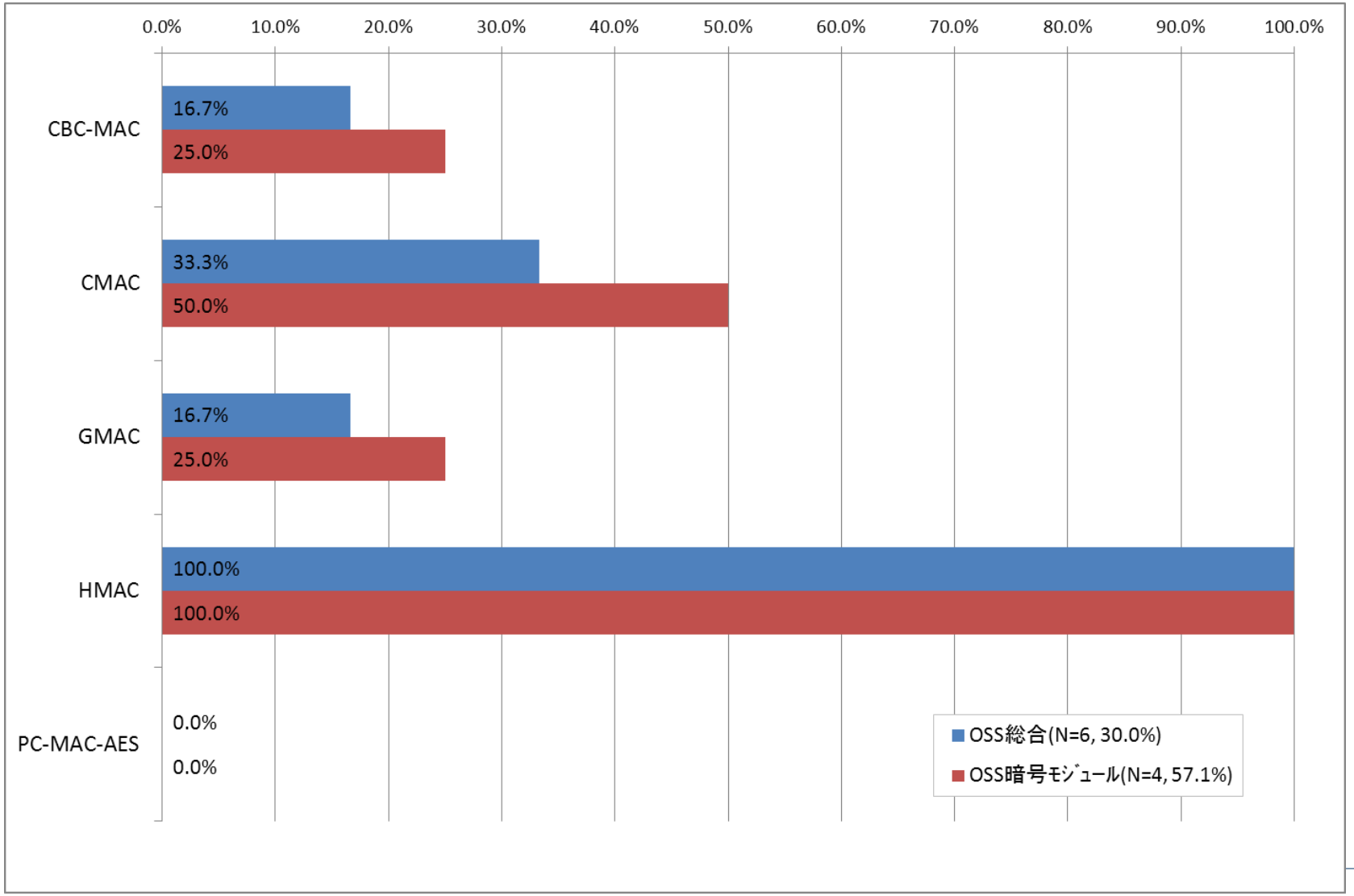
4.5.OSS調査結果（調査E結果）

7. 暗号利用モード



4.5.OSS調査結果（調査E結果）

8. メッセージ認証コード



5.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利用実績について以下の調査を行った。

調査A：参考情報として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：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：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：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：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した。

□ 次頁以降に、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。

5.まとめ

1. 公開鍵暗号(署名)

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%	―	―

5.まとめ

2. 公開鍵暗号(守秘・鍵共有)

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%	ー	ー
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%	ー	ー
	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%

5.まとめ

3. 共通鍵暗号（64ビットブロック暗号）

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%

5.まとめ

4. 共通鍵暗号（128ビットブロック暗号）

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.まとめ

5. 共通鍵暗号(ストリーム暗号)

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%	ー	ー	ー	ー
	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%	ー	ー	ー	ー
	国際的民間規格	RC4	100.0%	ー	ー	ー	ー
	特定団体規格	ー	ー	ー	ー	ー	ー
OSS調査結果 (調査E)	総合	RC4	100.0%	ー	ー	ー	ー
	暗号モジュール	RC4	100.0%	ー	ー	ー	ー

5.まとめ

6. ハッシュ関数

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%	－	－	－	－

5.まとめ

7. 暗号利用モード

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%	－	－

5.まとめ

8. メッセージ認証コード

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%

5.まとめ

9. エンティティ認証

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	－		－		－	

5.まとめ

□ 以下に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。

- また、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。