

2022年度 第 1 回 暗号技術検討会

（ 令和 5 年 2 月 27 日
～ 令和 5 年 3 月 6 日
メール開催 ）

議事次第

1. 議事

- (1) 公募提案暗号の自主取下げ要望に対する取り扱いルールの策定並びに「ECDSA、ECDH及びSC2000」の取扱いについて【承認】
- (2) CRYPTREC暗号リストの改定について【承認】
- (3) 意見募集の実施方法及びその後の対応について【承認】

配付資料一覧

資料 1	議事次第・配付資料一覧
資料 2	公募提案暗号の自主取下げ要望に対する取り扱いルールの策定並びに「ECDSA、ECDH及びSC2000」の取扱いについて（案）【承認事項】
資料 3	今次のCRYPTREC暗号リスト改定（旧“全面改定”）に至る主な経緯
資料 4－1	CRYPTREC暗号リストの改定について（案）【承認事項】
資料 4－2	CRYPTREC暗号リスト（現行版）
資料 4－3	CRYPTREC暗号リスト（改定案）
資料 5	意見募集の実施方法及びその後の対応について（案）【承認事項】
参考資料 1	電子政府推奨暗号リスト掲載への推薦候補案について
参考資料 2	暗号アルゴリズム利用実績調査報告

以上

公募提案暗号の自主取下げ要望に対する取り扱いルールの策定 並びに「ECDSA、ECDH 及び SC2000」の取扱いについて（案）

2000 年度、2001 年度及び 2009 年度の暗号技術公募への提案会社である富士通株式会社より、自社が提案した暗号アルゴリズム（以下、「公募提案暗号」という。）「ECDSA、ECDH 及び SC2000」について自主取下げの要望が寄せられた。一方、現在の CRYPTREC 暗号リストでは、ECDSA 及び ECDH は「電子政府推奨暗号リスト」に、SC2000 は「推奨候補暗号リスト」に掲載されているが、公募提案暗号の自主取下げ要望に対する扱いは規定されていない。

そのため、今回、公募提案暗号の自主取下げ要望に対する取り扱いルートを策定し、当該ルールに基づき、「ECDSA、ECDH 及び SC2000」の取扱いを決定することとしたい。

【背景】

2020 年度の暗号技術検討会で移行ルートを策定した際、「推奨候補暗号リスト」に長らく存在し続ける暗号技術については今後普及する見込みが極めて低いと推測されることから、CRYPTREC 暗号リストへの掲載から 20 年を経過したものについては「その後に実施する最初の利用実績調査の結果によって十分な利用実績が確認できなかった場合にはリストから削除」するルールを導入した。

今回、公募提案暗号の自主取下げ要望が提案会社から申請されたが、2020 年度の移行ルートを策定した際の趣旨を踏まえると、「今後の普及が見込めない公募提案暗号」とであると判断されるものについては、提案会社の意向により「推奨候補暗号リスト」からの削除を認めることができるようにすることが適切であると考えられる。

【審議事項 1】 公募提案暗号の自主取下げ要望に対する取り扱いルールの策定

提案会社からの自社の公募提案暗号の自主取下げ要望に対しては、以下の通り取り扱う。

1. 提案会社からの自社の公募提案暗号の自主取下げ要望に当たっては、別紙の「暗号技術取下げ申請書」により、CRYPTREC 事務局に申請する。
2. 申請を受けた CRYPTREC 事務局は、当該申請について、以下の判断基準を踏まえ、暗号技術活用委員会及び（暗号技術活用委員会において審議した上で）暗号技術検討会に対して付議する。
 - 取下げ申請の承認は「推奨候補暗号リスト」に掲載されている自社の公募提案暗号のうち「今後の普及が見込めない公募提案暗号」とであると判断されるものに限る
 - 「電子政府推奨暗号リスト」及び「運用監視暗号リスト」に掲載されている公募提案暗号については既に「普及している公募提案暗号」として扱い、取下げ申請は却下する
 - ただし、前 2 項の基準にかかわらず、知的財産権の無償許諾や利用状況（今後の見込みを含む）などにより、当該暗号技術の CRYPTREC 暗号リストへの掲載に伴う対応を CRYPTREC

事務局が自主的に管理すべきであると判断される場合には、取下げ申請を受けて、公募提案暗号から事務局提案暗号に位置づけを変更する

3. 2.の付議内容について、暗号技術活用委員会において審議した上で、暗号技術検討会において審議し、以下のいずれかの決定を行う。

- 「推奨候補暗号リスト」から削除する
- 公募提案暗号から事務局提案暗号へ位置づけを変更した上で、CRYPTREC 暗号リストに掲載したままとする
- CRYPTREC 暗号リストに掲載したままとする（公募提案暗号から事務局提案暗号への位置づけの変更は行わない）

【審議事項 2】 「ECDSA、ECDH 及び SC2000」の取扱いについて

上記の取り扱いルールに基づき、富士通株式会社からの「ECDSA、ECDH 及び SC2000」についての自主取下げ要望に関し、以下の通り取り扱う。

なお、当該要望については、2022 年 12 月 14 日に開催された第二回暗号技術活用委員会において、CRYPTREC での自主取下げルールの策定を前提として、暗号技術活用委員会としては当該要望に沿う方向で判断したとすることが了承されている。

- ECDSA 及び ECDH については、「電子政府推奨暗号リスト」に掲載されており、かつ各種国際標準等で規格化されていることから、CRYPTREC 暗号リストへの掲載に伴う対応を CRYPTREC 事務局が自主的に管理すべき暗号技術であると判断し、公募提案暗号から事務局提案暗号に位置づけを変更した上で、CRYPTREC 暗号リストに掲載したままとする
- SC2000 については、「推奨候補暗号リスト」に掲載されており、かつ「今後の普及が見込めない公募提案暗号」であると判断されることから削除する

以上

CRYPTREC 事務局宛

(送付先 : info@cryptrec.go.jp)

【別紙】

暗号技術取下げ申請書

申請責任者

会社名・部署名 ○○○○○○○○

役 職 ○○○○○○○○

氏 名 ○○○○○○ 印

このたび、「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」に掲載されている以下の暗号技術について、同リストからの取下げを申請いたします。

申請日： 20 年 月 日		
暗号技術名（複数列举可）：		
取下げ申請受理に関するCRYPTRECホームページでの公表 ☐ 可 ☐ 不可		
CRYPTREC暗号リストからの削除時期の希望 注1) 希望日は申請日の2ヶ月後以降としてください。 注2) CRYPTREC暗号リストからの削除有無を含め、希望通りにはならない場合もありますが、ご了承ください。申請を受けた対応内容については、決定次第、CRYPTREC事務局よりご連絡いたします。 ☐ 20 年 月 日希望 ☐ CRYPTRECのスケジュールに任せる（原則として年度末頃になります）		
取下げ申請の理由		
備考・その他の連絡事項		
連絡担当者		
担当者氏名：		所属・役職：
TEL：	FAX：	e-mail：

以 上

今次のCRYPTREC暗号リスト改定 (旧“全面改定”) に至る主な経緯

今次のCRYPTREC暗号リスト改定（旧“全面改定”）に至る主な経緯

1. リストの全面改定を実施、今後のリスト改定方針の大枠を決定（2012年度暗号技術検討会）

- ・ 2003年に策定した「電子政府推奨暗号リスト」を、「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」の3リストで構成する「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）」に再構成。
- ・ 「CRYPTREC暗号リスト」の次回の全面改定は10年後を目途に実施する等、今後のリスト改定方針の大枠を決定。

2. 2023年目途のリスト改定方針を決定（2020年度暗号技術検討会）

- ・ 2023年目途のリスト改定に当たり、3リスト構成を維持する方針、技術分類の構成を維持する方針を決定。
- ・ 上記改定に当たり、暗号技術の公募は行わない方針を決定。

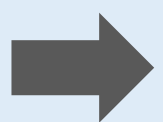
3. 2023年目途のリスト改定等に適用する新たな基準を決定（2021年度暗号技術検討会）

- ・ 「推奨候補暗号リスト」から「電子政府推奨暗号リスト」へ昇格させる暗号アルゴリズムを選定する際の、暗号アルゴリズムの利用実績による選定基準（別紙1）を決定。

※ 上記基準決定後の「CRYPTREC 暗号リスト」移行ルールは別紙2のとおり。

4. 2023年のリスト改定に係る具体的改定内容を検討（2022年度暗号技術活用委員会）

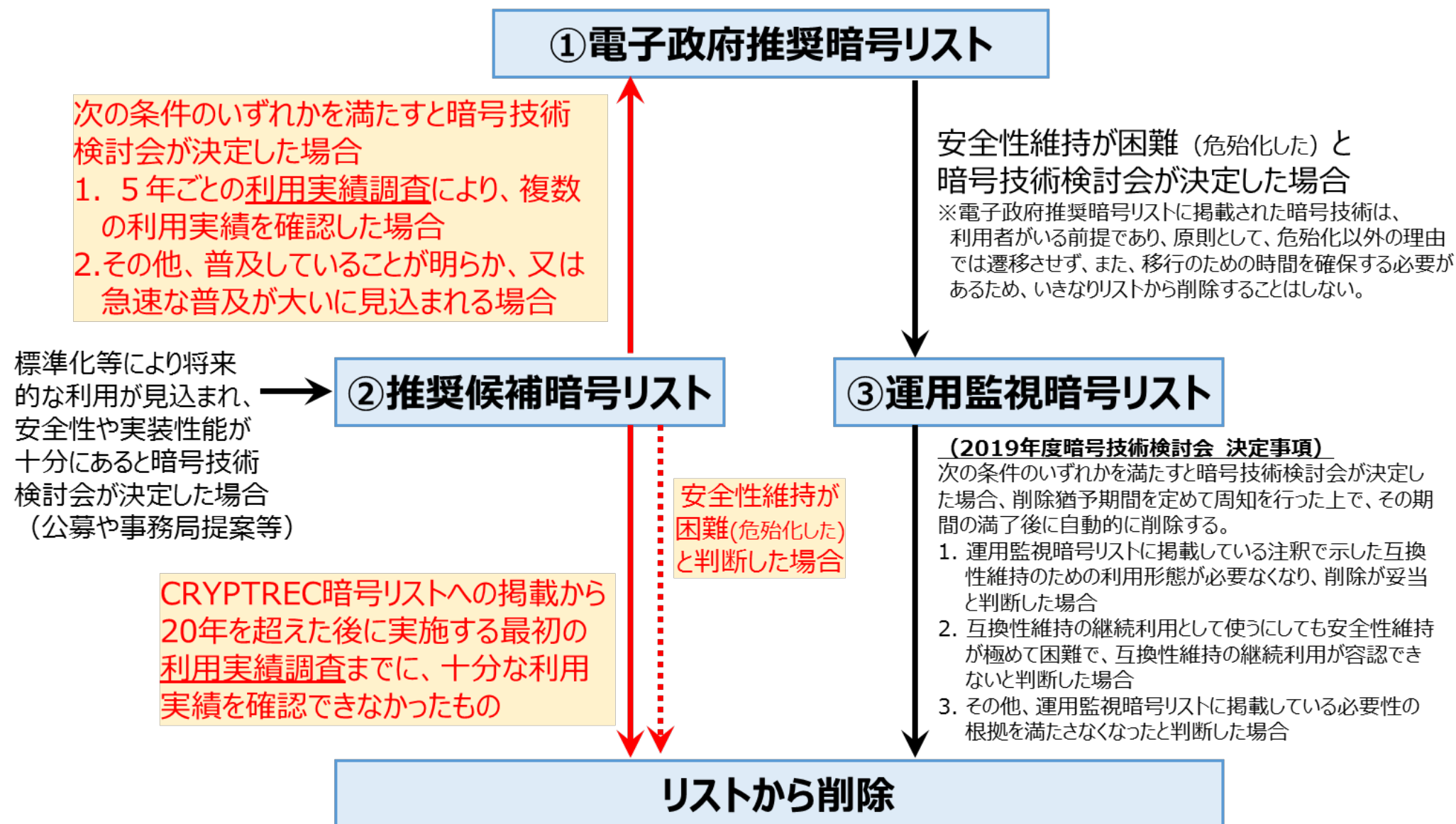
- ・ 2022年度に暗号技術活用委員会が実施した暗号アルゴリズム利用実績調査の結果を踏まえ、暗号技術活用委員会において、「推奨候補暗号リスト」から「電子政府推奨暗号リスト」への昇格候補として暗号技術検討会に推薦する暗号アルゴリズム（別紙3）を決定。



上記経緯を踏まえ、暗号技術検討会において、
「CRYPTREC暗号リスト」改定案をご審議いただきたい。

暗号アルゴリズムの利用実績による選定基準

考慮項目	選定目安
採用実績 以下のいずれかを満たす場合、昇格の検討対象に含める。なお、採用実績は、 ● 5年ごとに実施予定の大規模アンケート調査による「利用実績調査」 ● 必要に応じて、事務局が（大規模アンケート調査によらずに）情報収集する「利用実態確認」 により確認するものとする。 ① 利用実績調査の結果、電子政府推奨暗号リストに掲載されている（同一カテゴリの）暗号技術の採用実績と遜色がないことが確認された場合 ② 利用実績調査又は利用実態確認の結果、電子政府システムや重要インフラ等、日本の基幹システムにおいてすでに利用されていることが確認された場合 利用実績調査又は利用実態確認の結果、③～⑤のいずれかが確認された場合： ③ 利用者が多い主要な汎用製品群の複数に搭載されるなど、明らかに採用が進展していると判断された場合 ④ 利用者が多い主要なオープンソースソフトウェアの複数に搭載されるなど、明らかに採用が進展していると判断された場合 ⑤ 利用者が多い主要なサービスやプロトコルの複数で利用されるなど明らかに採用が進展していると判断された場合	電子政府推奨暗号リスト掲載の（同一カテゴリの）暗号技術の採用実績と同等以上の採用実績がある推奨候補暗号リスト掲載の暗号技術を昇格検討対象とする。 必要に応じて、利用実績調査に代わって、各府省庁等への照会を実施し、照会結果（クローズドな利用を含め）を基に昇格検討対象を選定する。 「複数」「利用者が多い（主要な）」というキーワードの両方を十分に満たし、明らかな採用促進が確認された場合には、必要に応じて、昇格検討対象とする。 ※「複数」の意味は、必要条件として「2個以上が必要」ということであって、「2個以上あればよい」という十分条件としての意味ではないことに留意
標準化実績 以下を満たす場合、昇格の検討対象に含める。 ⑥ 利用実績調査の結果、電子政府推奨暗号リストに掲載されている（同一カテゴリの）暗号技術の採用実績と遜色がないことが確認された場合	電子政府推奨暗号リスト掲載の（同一カテゴリの）暗号技術の採用実績と同等以上の採用実績がある推奨候補暗号リスト掲載の暗号技術は昇格検討対象とする。



暗号アルゴリズムの技術分類	推薦する暗号アルゴリズム
公開鍵暗号（署名）	EdDSA
ハッシュ関数	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE128 SHAKE256
暗号利用モード（秘匿モード）	XTS
認証暗号	ChaCha20-Poly1305
エンティティ認証	ISO/IEC 9798-4

電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）の改定について（案）

電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト、現在のリストは資料 4－2 のとおり）の改定に関して、次のとおり改定する方針とし、当該改定案（資料 4－3）に対する意見募集を実施することについて御審議いただきたい。

※ 資料 4－2 及び資料 4－3 の内容は、事前に資料 2 の内容が承認されたと仮定して作成している。

1. 認証暗号 ChaCha20-Poly1305 の電子政府推奨暗号リストへの昇格

暗号技術活用委員会において実施された認証暗号 ChaCha20-Poly1305 に対する 2022 年度の暗号アルゴリズム利用実績調査の結果(参考資料 2 参照) 及び 2021 年度に暗号技術検討会において承認された「暗号アルゴリズムの利用実績に基づく選定基準」(資料 3 別紙 2 参照) に基づく暗号技術活用委員会からの提案(参考資料 1 参照) を踏まえ、
認証暗号 ChaCha20-Poly1305 を CRYPTREC 暗号リストの「推奨候補暗号リスト」から「電子政府推奨暗号リスト」に昇格する。

2. 秘匿モード XTS の電子政府推奨暗号リストへの昇格

暗号技術活用委員会において実施された秘匿モード XTS に対する 2022 年度の暗号アルゴリズム利用実績調査の結果(参考資料 2 参照) 及び 2021 年度に暗号技術検討会において承認された「暗号アルゴリズムの利用実績に基づく選定基準」(資料 3 別紙 2 参照) に基づく暗号技術活用委員会からの提案(参考資料 1 参照) を踏まえ、
秘匿モード XTS を CRYPTREC 暗号リストの「推奨候補暗号リスト」から「電子政府推奨暗号リスト」に昇格する。

3. エンティティ認証 ISO/IEC 9798-4 の電子政府推奨暗号リストへの昇格

暗号技術活用委員会において実施されたエンティティ認証 ISO/IEC 9798-4 に対する 2022 年度の暗号アルゴリズム利用実績調査の結果(参考資料 2 参照) 及び 2021 年度に暗号技術検討会において承認された「暗号アルゴリズムの利用実績に基づく選定基準」(資料 3 別紙 2 参照) に基づく暗号技術活用委員会からの提案(参考資料 1 参照) を踏まえ、
エンティティ認証 ISO/IEC 9798-4 を CRYPTREC 暗号リストの「推奨候補暗号リスト」から「電子政府推奨暗号リスト」に昇格する。

4. ハッシュ関数 SHA-512/256, SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256 の電子政府推奨暗号リストへの昇格

暗号技術活用委員会において実施されたハッシュ関数 SHA-512/256, SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256 に対する 2022 年度の暗号アルゴリズム利用実績調査の結果(参考資料 2 参照) 及び 2021 年度に暗号技術検討会において承認された「暗号アルゴリズムの利用実績に基づく選

定基準」(資料3別紙2参照)に基づく暗号技術活用委員会からの提案(参考資料1参照)を踏まえ、ハッシュ関数 SHA-512/256, SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256 を CRYPTREC 暗号リストの「推奨候補暗号リスト」から「電子政府推奨暗号リスト」に昇格する。

5. 署名 EdDSA の電子政府推奨暗号リストへの昇格

暗号技術活用委員会において実施された署名 EdDSA に対する 2022 年度の暗号アルゴリズム利用実績調査の結果(参考資料2参照)及び2021年度に暗号技術検討会において承認された「暗号アルゴリズムの利用実績に基づく選定基準」(資料3別紙2参照)に基づく暗号技術活用委員会からの提案(参考資料1参照)を踏まえ、

署名 EdDSA を CRYPTREC 暗号リストの「推奨候補暗号リスト」から「電子政府推奨暗号リスト」に昇格する。

事前に資料2の内容が承認されたと仮定して作成

電子政府における調達のために参照すべき暗号のリスト (CRYPTREC暗号リスト)(現行版)

平成25年3月1日

デジタル庁・総務省・経済産業省

(最終更新: 令和●年●月●日)

電子政府推奨暗号リスト

暗号技術検討会¹及び関連委員会(以下、「CRYPTREC」という。)により安全性及び実装性能が確認された暗号技術²について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。なお、利用する鍵長について、「暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準」⁵の規定に合致しない鍵長を用いた場合には、電子政府推奨暗号リストの暗号技術を利用しているとは見なされないことに留意すること。

技術分類		暗号技術
公開鍵暗号	署名	DSA
		ECDSA
		RSA-PSS ^(注1)
		RSASSA-PKCS1-v1_5 ^(注1)
	守秘	RSA-OAEP ^(注1)
	鍵共有	DH
ECDH		
共通鍵暗号	64ビットブロック暗号 ^(注2)	該当なし
	128ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
暗号利用モード	秘匿モード	CBC
		CFB
		CTR
		OFB
	認証付き秘匿モード ^(注13)	CCM
		GCM ^(注4)
メッセージ認証コード		CMAC
		HMAC
認証暗号		該当なし

¹ デジタル庁統括官、総務省サイバーセキュリティ統括官及び経済産業省商務情報政策局長が有識者の参集を求め、暗号技術の普及による情報セキュリティ対策の推進を図る観点から、専門家による意見等を聴取することにより、デジタル庁、総務省及び経済産業省における施策の検討に資することを目的として開催。

² 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合、CRYPTREC暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

⁵ CRYPTREC, 暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準, <https://www.cryptrec.go.jp/list.html>

エンティティ認証	ISO/IEC 9798-2
	ISO/IEC 9798-3

- (注1) 「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」(平成20年4月情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定)を踏まえて利用すること。
https://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf
(平成25年3月1日現在)
- (注2) CRYPTREC暗号リストにおいて、64ビットブロック暗号により、同一の鍵を用いて暗号化する場合、 2^{20} ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、 2^{21} ブロックまでとする。
- (注4) 初期化ベクトル長は96ビットを推奨する。
- (注13) CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。

推奨候補暗号リスト

CRYPTRECにより安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術³のリスト。なお、本リストに記載されている暗号技術を利用する際は、「暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準」⁶の規定に合致する鍵長を用いることが求められることに留意すること。

技術分類		暗号技術
公開鍵暗号	署名	EdDSA
	守秘	該当なし
	鍵共有	PSEC-KEM ^(注5)
共通鍵暗号	64ビットブロック暗号 ^(注6)	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
	128ビットブロック暗号	CIPHERUNICORN-A
		CLEFIA
		Hierocrypt-3
	ストリーム暗号	Enocoro-128v2
		MUGI
		MULTI-S01 ^(注7)
ハッシュ関数		SHA-512/256
		SHA3-256
		SHA3-384
		SHA3-512
		SHAKE128 ^(注12)
		SHAKE256 ^(注12)
暗号利用モード	秘匿モード [△]	XTS ^(注17)
	認証付き秘匿モード ^{△(注14)}	該当なし
メッセージ認証コード		PC-MAC-AES
認証暗号		ChaCha20-Poly1305
エンティティ認証		ISO/IEC 9798-4

(注5) KEM (Key Encapsulating Mechanism) – DEM (Data Encapsulating Mechanism) 構成における利用を前提とする。

(注6) CRYPTREC暗号リストにおいて、64ビットブロック暗号により、同一の鍵を用いて暗号化する場合、2²⁰ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、2²¹ブロックまでとする。

(注7) 平文サイズは64ビットの倍数に限る。

(注12) ハッシュ長は256ビット以上とすること。

(注14) CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。

(注17) ブロック暗号には、CRYPTREC暗号リスト掲載128ビットブロック暗号を使う。利用用途はストレージデバイスの暗号化に限り、実装方法はNIST SP800-38Eに従うこと。

³ 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合、CRYPTREC暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

⁶ CRYPTREC, 暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準, <https://www.cryptrec.go.jp/list.html>

運用監視暗号リスト

実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなったとCRYPTRECにより確認された暗号技術⁴のうち、互換性維持のために継続利用を容認するもののリスト。互換性維持⁷以外の目的での利用は推奨しない。なお、本リストに記載されている暗号技術を利用する際は、「暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準」⁸の規定に合致する鍵長を用いることが求められることに留意すること。

技術分類		暗号技術
公開鍵暗号	署名	該当なし
	守秘	RSAES-PKCS1-v1_5 ^(注8) ^(注9)
	鍵共有	該当なし
共通鍵暗号	64ビットブロック暗号 ^(注15)	3-key Triple DES
	128ビットブロック暗号	該当なし
	ストリーム暗号	該当なし
ハッシュ関数		RIPEMD-160
		SHA-1 ^(注8)
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード ^(注16)	該当なし
メッセージ認証コード		CBC-MAC ^(注11)
認証暗号		該当なし
エンティティ認証		該当なし

(注8) 「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」(平成20年4月 情報セキュリティ政策会議決定、平成24年10月 情報セキュリティ対策推進会議改定)を踏まえて利用すること。
https://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf
(平成25年3月1日現在)

(注9) TLS 1.0, 1.1, 1.2で利用実績があることから当面の利用を認める。

(注11) 安全性の観点から、メッセージ長を固定して利用すべきである。

(注15) CRYPTREC暗号リストにおいて、64ビットブロック暗号により、同一の鍵を用いて暗号化する場合、2²⁰ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、2²¹ブロックまでとする。

(注16) CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。

⁴ 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合、CRYPTREC暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

⁷ 既に稼働中のシステムやアプリケーション等との間での相互運用を継続すること

⁸ CRYPTREC, 暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準, <https://www.cryptrec.go.jp/list.html>

変更履歴情報

変更日付	変更箇所	変更前の記述	変更後の記述
平成27年 3月27日	(注10)	128-bit RC4は、SSL(TLS1.0以上)に限定して利用すること。	互換性維持のために継続利用をこれまで容認してきたが、今後は極力利用すべきでない。SSL/TLSでの利用を含め、電子政府推奨暗号リストに記載された暗号技術への移行を速やかに検討すること。
平成28年 3月29日	推奨候補暗号リスト (技術分類: ハッシュ関数)	該当なし	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE256 ^(注12)
	(注12)	[新規追加]	ハッシュ長は256ビット以上とすること。
平成29年 3月30日	推奨候補暗号リスト (技術分類: ハッシュ関数)	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE256 ^(注12)	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE128 ^(注12) SHAKE256 ^(注12)
平成30年 3月29日	(注2) (注6)	より長いブロック長の暗号が利用できるのであれば、128ビットブロック暗号を選択することが望ましい。	CRYPTREC暗号リストにおいて、64ビットブロック暗号により、同一の鍵を用いて暗号化する場合、 2^{20} ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、 2^{21} ブロックまでとする。
	(注15)	[新規追加]	
	電子政府推奨暗号リスト(技術分類: 共通鍵暗号)	3-key Triple DES ^(注3)	該当なし
	(注3)	3-key Triple DESは、以下の条件を考慮し、当面の利用を認める。 1) NIST SP 800-67として規定されていること。 2) デファクトスタンダードとしての位置を保っていること。	[削除]
	運用監視暗号リスト (技術分類: 共通鍵暗号)	該当なし	3-Key Triple DES ^(注15)
	電子政府推奨暗号リスト	[技術分類の新設]	技術分類: 認証暗号 暗号技術: 該当なし
	推奨候補暗号リスト		技術分類: 認証暗号 暗号技術: ChaCha20-Poly1305
	運用監視暗号リスト		技術分類: 認証暗号 暗号技術: 該当なし

	(注13) (注14) (注16)	[新規追加]	CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。
	電子政府推奨暗号リスト(見出し)	名称	暗号技術
	推奨候補暗号リスト(見出し)		
	運用監視暗号リスト(見出し)		
令和2年 12月21日	推奨候補暗号リスト (技術分類: 暗号利用モード 秘匿モード)	該当なし	XTS ^(注17)
	(注17)	[新規追加]	ブロック暗号には、CRYPTREC暗号リスト掲載128ビットブロック暗号を使う。利用用途はストレージデバイスの暗号化に限り、実装方法はNIST SP800-38Eに従うこと。
令和3年 4月1日	運用監視暗号リスト (技術分類: 共通鍵暗号)	128-bit RC4 ^(注10)	該当なし
	(注10)	互換性維持のために継続利用をこれまで容認してきたが、今後は極力利用すべきでない。TLSでの利用を含め、電子政府推奨暗号リストに記載された暗号技術への移行を速やかに検討すること。	[削除]
令和4年 3月30日	文書クレジット	総務省・経済産業省	デジタル庁・総務省・経済産業省
	推奨候補暗号リスト (技術分類: 公開鍵暗号 署名)	該当なし	EdDSA
	電子政府推奨暗号リスト(本文)	暗号技術検討会及び関連委員会(以下、「CRYPTREC」という。)により安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。	暗号技術検討会及び関連委員会(以下、「CRYPTREC」という。)により安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。なお、利用する鍵長について、「暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準」の規定に合致しない鍵長を用いた場合には、電子政府推奨暗号リストの暗号技術を利用しているとは見なされないことに留意すること。

	電子政府推奨暗号リスト(本文)	「暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準」	「暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準」 ⁵
	電子政府推奨暗号リスト(脚注)	該当なし	⁵ CRYPTREC, 暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準, https://www.cryptrec.go.jp/list.html
	推奨候補暗号リスト(本文)	CRYPTRECにより安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術のリスト。	CRYPTRECにより安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術のリスト。なお、本リストに記載されている暗号技術を利用する際は、「暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準」の規定に合致する鍵長を用いることが求められることに留意すること。
	推奨候補暗号リスト(本文)	「暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準」	「暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準」 ⁶
	推奨候補暗号リスト(脚注)	該当なし	⁶ CRYPTREC, 暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準, https://www.cryptrec.go.jp/list.html
	運用監視暗号リスト(本文)	実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなったとCRYPTRECにより確認された暗号技術のうち、互換性維持のために継続利用を容認するもののリスト。互換性維持以外の目的での利用は推奨しない。	実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなったとCRYPTRECにより確認された暗号技術のうち、互換性維持のために継続利用を容認するもののリスト。互換性維持以外の目的での利用は推奨しない。なお、本リストに記載されている暗号技術を利用する際は、「暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準」の規定に合致する鍵長を用いることが求められることに留意すること。
	運用監視暗号リスト(本文)	互換性維持	互換性維持 ⁷
	運用監視暗号リスト(脚注)	該当なし	⁷ 既に稼働中のシステムやアプリケーション等との間での相互運用を継続すること
	運用監視暗号リスト(本文)	「暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準」	「暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準」 ⁸
	運用監視暗号リスト(脚注)	該当なし	⁸ CRYPTREC, 暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準, https://www.cryptrec.go.jp/list.html
令和●年 ●月●日	推奨候補暗号リスト (技術分類: 共通鍵暗号 128ビットブロック暗号)	SC2000	[削除]

事前に資料2の内容が承認されたと仮定して作成

電子政府における調達のために参照すべき暗号のリスト (CRYPTREC暗号リスト)(案)

令和●年●月●日
デジタル庁・総務省・経済産業省

電子政府推奨暗号リスト

暗号技術検討会¹及び関連委員会(以下、「CRYPTREC」という。)により安全性及び実装性能が確認された暗号技術²について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。なお、利用する鍵長について、「暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準」⁵の規定に合致しない鍵長を用いた場合には、電子政府推奨暗号リストの暗号技術を利用しているとは見なされないことに留意すること。

技術分類		暗号技術
公開鍵暗号	署名	DSA
		ECDSA
		EdDSA
		RSA-PSS ^(注1)
		RSASSA-PKCS1-v1_5 ^(注1)
	守秘	RSA-OAEP ^(注1)
共通鍵暗号	鍵共有	DH
		ECDH
	64ビットブロック暗号 ^(注2)	該当なし
	128ビットブロック暗号	AES
		Camellia
ハッシュ関数	ストリーム暗号	KCipher-2
		SHA-256
		SHA-384
		SHA-512
		SHA-512/256
		SHA3-256
		SHA3-384
		SHA3-512
		SHAKE128 ^(注12)
		SHAKE256 ^(注12)
暗号利用モード	秘匿モード	CBC
		CFB

¹ デジタル庁統括官、総務省サイバーセキュリティ統括官及び経済産業省商務情報政策局長が有識者の参集を求め、暗号技術の普及による情報セキュリティ対策の推進を図る観点から、専門家による意見等を聴取することにより、デジタル庁、総務省及び経済産業省における施策の検討に資することを目的として開催。

² 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合、CRYPTREC暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

⁵ CRYPTREC、暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準、<https://www.cryptrec.go.jp/list.html>

		CTR
		OFB
		XTS ^(注17)
	認証付き秘匿モード ^(注13)	CCM
		GCM ^(注4)
メッセージ認証コード		CMAC
		HMAC
認証暗号		ChaCha20-Poly1305
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3
		ISO/IEC 9798-4

- (注1) 「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」(平成20年4月情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定)を踏まえて利用すること。
https://www.nisc.go.jp/pdf/policy/general/angou_ikoushishin.pdf
(平成25年3月1日現在)
- (注2) CRYPTREC暗号リストにおいて、64ビットブロック暗号により、同一の鍵を用いて暗号化する場合、 2^{20} ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、 2^{21} ブロックまでとする。
- (注4) 初期化ベクトル長は96ビットを推奨する。
- (注12) ハッシュ長は256ビット以上とすること。
- (注13) CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。
- (注17) ブロック暗号には、CRYPTREC暗号リスト掲載128ビットブロック暗号を使う。利用用途はストレージデバイスの暗号化に限り、実装方法はNIST SP800-38Eに従うこと。

推奨候補暗号リスト

CRYPTRECにより安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術³のリスト。なお、本リストに記載されている暗号技術を利用する際は、「暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準」⁶の規定に合致する鍵長を用いることが求められることに留意すること。

技術分類		暗号技術
公開鍵暗号	署名	該当なし
	守秘	該当なし
	鍵共有	PSEC-KEM ^(注5)
共通鍵暗号	64ビットブロック暗号 ^(注6)	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
	128ビットブロック暗号	CIPHERUNICORN-A
		CLEFIA
		Hierocrypt-3
	ストリーム暗号	Enocoro-128v2
		MUGI
		MULTI-S01 ^(注7)
ハッシュ関数		該当なし
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード ^(注14)	該当なし
メッセージ認証コード		PC-MAC-AES
認証暗号		該当なし
エンティティ認証		該当なし

(注5) KEM (Key Encapsulating Mechanism) – DEM (Data Encapsulating Mechanism) 構成における利用を前提とする。

(注6) CRYPTREC暗号リストにおいて、64ビットブロック暗号により、同一の鍵を用いて暗号化する場合、 2^{20} ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、 2^{21} ブロックまでとする。

(注7) 平文サイズは64ビットの倍数に限る。

(注14) CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。

³ 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合、CRYPTREC暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

⁶ CRYPTREC, 暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準, <https://www.cryptrec.go.jp/list.html>

運用監視暗号リスト

実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなったとCRYPTRECにより確認された暗号技術⁴のうち、互換性維持のために継続利用を容認するもののリスト。互換性維持⁷以外の目的での利用は推奨しない。なお、本リストに記載されている暗号技術を利用する際は、「暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準」⁸の規定に合致する鍵長を用いることが求められることに留意すること。

技術分類		暗号技術
公開鍵暗号	署名	該当なし
	守秘	RSAES-PKCS1-v1_5 ^(注8) ^(注9)
	鍵共有	該当なし
共通鍵暗号	64ビットブロック暗号 ^(注15)	3-key Triple DES
	128ビットブロック暗号	該当なし
	ストリーム暗号	該当なし
ハッシュ関数		RIPEMD-160
		SHA-1 ^(注8)
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード ^(注16)	該当なし
メッセージ認証コード		CBC-MAC ^(注11)
認証暗号		該当なし
エンティティ認証		該当なし

(注8) 「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」(平成20年4月 情報セキュリティ政策会議決定、平成24年10月 情報セキュリティ対策推進会議改定)を踏まえて利用すること。
https://www.nisc.go.jp/pdf/policy/general/angou_ikoushishin.pdf
 (平成25年3月1日現在)

(注9) TLS 1.0, 1.1, 1.2で利用実績があることから当面の利用を認める。

(注11) 安全性の観点から、メッセージ長を固定して利用すべきである。

(注15) CRYPTREC暗号リストにおいて、64ビットブロック暗号により、同一の鍵を用いて暗号化する場合、2²⁰ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、2²¹ブロックまでとする。

(注16) CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。

⁴ 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合、CRYPTREC暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

⁷ 既に稼働中のシステムやアプリケーション等との間での相互運用を継続すること

⁸ CRYPTREC, 暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準, <https://www.cryptrec.go.jp/list.html>

意見募集の実施方法及びその後の対応について（案）

電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）の改定に係る意見募集の実施及びその後の対応を以下のとおり進めることについて、御審議いただきたい。

1. 意見募集の実施方法

【意見募集対象】

資料 4 - 3 電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）（改定案）

【意見募集期間】

令和5年3月9日（木）から同年3月23日（木）までの15日間

【意見募集方法】

電子政府の総合窓口(e-Gov)、デジタル庁、総務省及び経済産業省のHPに掲載

【意見提出方法】

e-Gov、郵送、電子メール

2. 意見募集実施後の対応

提出された意見を踏まえ、暗号技術検討会で審議の上、CRYPTREC暗号リストの改定に関して決定・公表する。

電子政府推奨暗号リスト掲載への推薦候補案について

暗号技術活用委員会では、暗号アルゴリズム利用実績調査の結果（参考資料2）及び2021年度に承認された別紙記載の利用実績に基づく選定基準（選定ルール）に基づき、現在の推奨候補暗号リストに掲載のアルゴリズムのうち、電子政府推奨暗号リスト掲載への推薦候補案を以下の通り決定したので、報告する。

(1) エンティティ認証、ハッシュ関数、署名を除いた技術分類について：

技術分類		推薦候補	推薦しない候補	理由
公開鍵暗号	鍵共有	該当なし	PSEC-KEM	●他の鍵共有と比較して優位な利用実績があるとは認められない
共通鍵暗号	64 ビットブロック暗号	該当なし	CIPHERUNICORN-E Hierocrypt-L1 MISTY1	●他の64ビットブロック暗号と比較して優位な利用実績があるとは認められない
	128 ビットブロック暗号	該当なし	CIPHERUNICORN-A CLEFIA Hierocrypt-3 SC2000	●他の128ビットブロック暗号と比較して優位な利用実績があるとは認められない
	ストリーム暗号	該当なし	Enocoro-128v2 MUGI MULTI-S01	●他のストリーム暗号と比較して優位な利用実績があるとは認められない
認証暗号		ChaCha20-Poly1305	該当なし	●考慮項目①②④について、利用実績があると認められる
暗号利用モード	秘匿モード	XTS	該当なし	●考慮項目①②④について、他の秘匿モードと比較して利用実績があると認められる
メッセージ認証コード		該当なし	PC-MAC-AES	●他のメッセージ認証コードと比較して優位な利用実績があるとは認められない

(2) エンティティ認証について：

技術分類		推薦候補	推薦しない候補	理由
エンティティ認証		ISO/IEC 9798-4	該当なし	●考慮項目①②において、他のエンティティ認証と比較して利用実績があると認められる

(3) ハッシュ関数について：

技術分類	推薦候補	推薦しない候補	理由
ハッシュ関数	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE128 SHAKE256	該当なし	● 考慮項目④において、他のハッシュ関数と比較して利用実績があると認められる

(4) EdDSA について：

技術分類	推薦候補	推薦しない候補	理由
公開鍵 署名 暗号	EdDSA	該当なし	● 考慮項目④において、他の署名と比較して利用実績があると認められる

以上

【参考】

技術分類		電子政府推奨暗号	推奨候補暗号	運用監視暗号
公開鍵暗号	署名	DSA	EdDSA	該当なし
		ECDSA		
		RSA-PSS		
		RSASSA-PKCS1-v1_5		
	守秘	RSA-OAEP	該当なし	RSAES-PKCS1-v1_5
	鍵共有	DH	PSEC-KEM	該当なし
ECDH				
共通鍵暗号	64 ビットブロック暗号	該当なし	CIPHERUNICORN-E	3-key Triple DES
			Hierocrypt-L1	
			MISTY1	
	128 ビットブロック暗号	AES	CIPHERUNICORN-A	該当なし
		Camellia	CLEFIA	
			Hierocrypt-3	
			SC2000	
	ストリーム暗号	KCipher-2	Enocoro-128v2	該当なし
			MUGI	
			MULTI-S01	
ハッシュ関数		SHA-256	SHA-512/256	RIPEMD-160
		SHA-384	SHA3-256	SHA-1
		SHA-512	SHA3-384	
			SHA3-512	
			SHAKE128	
			SHAKE256	
暗号利用モード	秘匿モード	CBC	XTS	該当なし
		CFB		
		CTR		
		OFB		
	認証付き秘匿モード	CCM	該当なし	該当なし
		GCM		
メッセージ認証コード		CMAC	PC-MAC-AES	CBC-MAC
		HMAC		
認証暗号		該当なし	ChaCha20-Poly1305	該当なし
エンティティ認証		ISO/IEC 9798-2	ISO/IEC 9798-4	該当なし
		ISO/IEC 9798-3		

＜選定基準＞

本選定基準は、暗号技術評価委員会で安全性及び実装性の評価を実施し、その評価結果により暗号技術検討会が推奨候補暗号リストに含めると決定した暗号技術に対して、電子政府推奨暗号リストへの昇格を決めるための基準である。昇格検討対象の暗号技術は、以下の考慮項目での目安に基づき、暗号技術活用委員会にて検討、選定し、暗号技術検討会に推薦する。

推薦された暗号技術について、暗号技術検討会では、その根拠となった利用実態を再度確認・審議を行い、電子政府推奨暗号リストへの昇格に問題がないと判断した場合に電子政府推奨暗号リストに選定する。

考慮項目	選定目安
採用実績	以下のいずれかを満たす場合、昇格の検討対象に含める。なお、採用実績は、 ● 5年ごとに実施予定の大規模アンケート調査による「利用実績調査」 ● 必要に応じて、事務局が（大規模アンケート調査によらずに）情報収集する「利用実態確認」により確認するものとする。
① 利用実績調査の結果、電子政府推奨暗号リストに掲載されている（同一カテゴリの）暗号技術の採用実績と遜色がないことが確認された場合	電子政府推奨暗号リスト掲載の（同一カテゴリの）暗号技術の採用実績と同等以上の採用実績がある推奨候補暗号リスト掲載の暗号技術を昇格検討対象とする。
② 利用実績調査又は利用実態確認の結果、電子政府システムや重要インフラ等、日本の基幹システムにおいてすでに利用されていることが確認された場合	必要に応じて、利用実績調査に代わって、各府省庁等への照会を実施し、照会結果（クローズドな利用を含め）を基に昇格検討対象を選定する。
利用実績調査又は利用実態確認の結果、③～⑤のいずれかが確認された場合： ③ 利用者が多い主要な汎用製品群の複数に搭載されるなど、明らかに採用が進展していると判断された場合 ④ 利用者が多い主要なオープンソースソフトウェアの複数に搭載されるなど、明らかに採用が進展していると判断された場合 ⑤ 利用者が多い主要なサービスやプロトコルの複数で利用されるなど、明らかに採用が進展していると判断された場合	「複数」「利用者が多い（主要な）」というキーワードの両方を十分に満たし、明らかな採用促進が確認された場合には、必要に応じて、昇格検討対象とする。 ※「複数」の意味は、必要条件として「2個以上が必要」ということであって、「2個以上あればよい」という十分条件としての意味ではないことに留意
標準化実績	以下を満たす場合、昇格の検討対象に含める。 ⑥ 利用実績調査の結果、電子政府推奨暗号リストに掲載されている（同一カテゴリの）暗号
	電子政府推奨暗号リスト掲載の（同一カテゴリの）暗号技術の採用実績と同等以上の

	技術の採用実績と遜色がないことが確認された場合	採用実績がある推奨候補暗号リスト掲載の暗号技術は昇格検討対象とする。
--	-------------------------	------------------------------------

暗号アルゴリズム利用実績調査報告

委託調査概要

■ 委託調査概要

- 株式会社野村総合研究所に委託して実施
- 調査対象アルゴリズムは以下の通り

分類	小分類	アルゴリズム名称等	分類	小分類	アルゴリズム名称等
共通鍵暗号	64ビットブロック暗号	1. CAST-128		暗号利用モード／メッセージ認証コード	35. GCM
		2. CIPHERUNICORN-E			36. GMAC
		3. Hierocrypt-L1			37. HMAC
		4. HIGHT			38. OFB
		5. MISTY1			39. PC-MAC-AES
		6. Triple DES			40. XTS
	128ビットブロック暗号	7. AES	公開鍵暗号	署名※	41. その他（2）
		8. ARIA			42. DSA
		9. Camellia			43. ECDSA
		10. CIPHERUNICORN-A			44. KC-DSA
		11. CLEFIA			45. RSA-PSS
		12. Hierocrypt-3			46. RSASSA-PKCS1-v1_5
		13. GOST		守秘・鍵交換	47. SM2
		14. SC2000			48. DH
		15. SEED			49. ECDH
		16. SMS4			50. PSEC-KEM
	ストリーム暗号・認証暗号	17. ChaCha20-Poly1305			51. RSAES-PKCS1-v1_5（RSA暗号）
		18. Decim v2			52. RSA-OAEP
		19. Enocoro-128v2			53. その他（3）
		20. KCipher-2		ハッシュ関数	54. RIPEMD-160
		21. MUGI			55. SHA-1
		22. MULTI-S01			56. SHA-224
		23. RC4			57. SHA-256
		24. Rabbit			58. SHA-384
		25. SNOW			59. SHA-512
	その他	26. その他（1）			60. SHA-512/256
					61. SHA3-256
暗号利用モード／メッセージ認証コード		27. CBC			62. SHA3-384
		28. CBC-MAC			63. SHA3-512
		29. CCM			64. SHAKE128
		30. CFB			65. SHAKE256
		31. CMAC			66. SM3
		32. CTR			67. その他（4）
		33. CTS			
		34. ECB			

※署名「EdDSA」は、調査(C)の規格調査、及び(D)(E)について事務局で独自に調査し、調査結果をP16-18に記載した。

委託調査概要

■ 調査内容

調査対象	中間報告時	最終実績
(A) 応募暗号アルゴリズムの応募者に対するアンケート調査	応募暗号アルゴリズムの応募者 8社(16アルゴリズム)	- 全8社から回答受領 - アルゴリズム実績提供: 11アルゴリズム → 調査(C)(D)(E)の情報として活用 - 製品実績提供: 4アルゴリズム → 調査(B)の情報として活用
(B) 暗号アルゴリズムを搭載している市販製品の販売会社への調査	合計1,500社以上 14業界団体 2,535社 - 個別コンタクト 102社 - 調査パネル 23,747名	- アンケート回収数: 211社301製品 - 業界団体: 2,535社 → 65社114製品 - 個別: 108社 → 28社37製品 (A)調査: 4社4製品 - 調査パネル: 23,747名 → 146製品 ↓ - 集計対象: 101社209製品 - アンケート有効回答: 82社128製品(利用アルゴリズム不明19製品を含む) - 公開情報調査(補充調査): 41社100製品
(C) 日本の政府機関等に対する調査	法省令・ガイドライン・政府系システム規格・重要インフラ規格 最大20件	- アンケート集計数: デジタル庁／IPA経由で提供された98システム - 規格調査数: 全30件 うち、暗号アルゴリズム記載ありは17件
(D) 国際標準規格・民間規格等に対する調査	国際標準規格・民間規格等 最大25件	規格調査数: IPAが指定した25件(※別途追加分: 146件)
(E) オープンソースソフトウェアでの利用実績調査	オープンソースソフトウェア 最大30件	OSS調査数: IPAが指定した30件(※EdDSAだけ独自追加実施)

委託調査結果(B)

■ 集計対象の選定

利用アルゴリズム不明
19製品を除外

アンケート回収数: 211社301製品

- ・ 業界団体: 2,535社 → 65社114製品
- ・ 個別: 108社 → 28社37製品
- ・ (A)調査: 4社4製品
- ・ 調査パネル: 23,747名 → 146製品

アンケート有効回答: 82社128製品

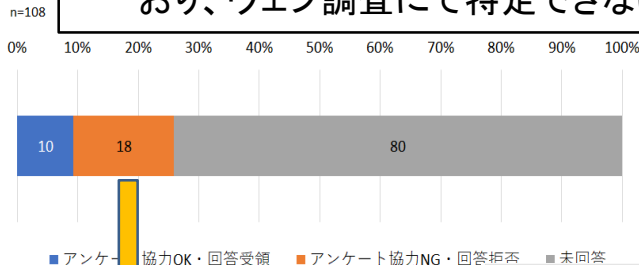
- ・ 業界団体: 65社114製品 → 65社99製品
- ・ 個別: 28社37製品 → 10社17製品
- ・ (A)調査: 4社4製品 → 3社3製品
- ・ 調査パネル: 146製品 → 9社9製品

公開情報調査: 41社100製品

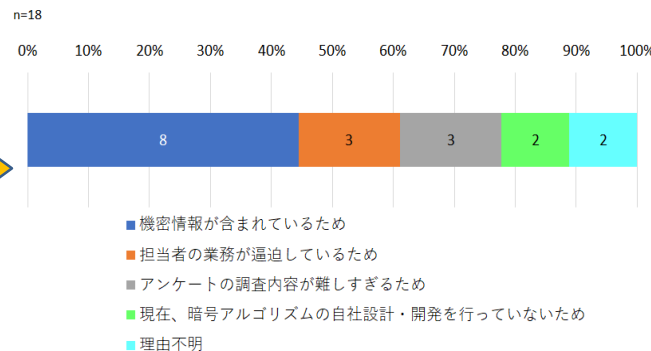
集計対象:
101社
209製品

【除外理由】

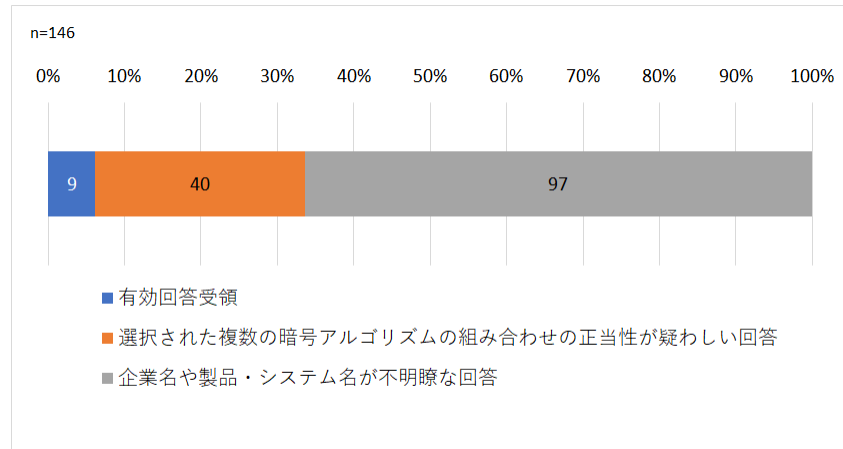
- 有効回答は1社につき5製品まで。6製品以上は、IPAと相談のうえ5製品に絞り込み
- 個別企業調査の回答には、アンケート調査への協力を辞退する旨の回答が含まれていた
- 応募者(A)調査や調査パネルの回答には、企業名や製品・システム名が不明瞭なものが多く含まれており、ウェブ調査にて特定できないものについては除外



個別企業調査の回答 (会社数ベース)

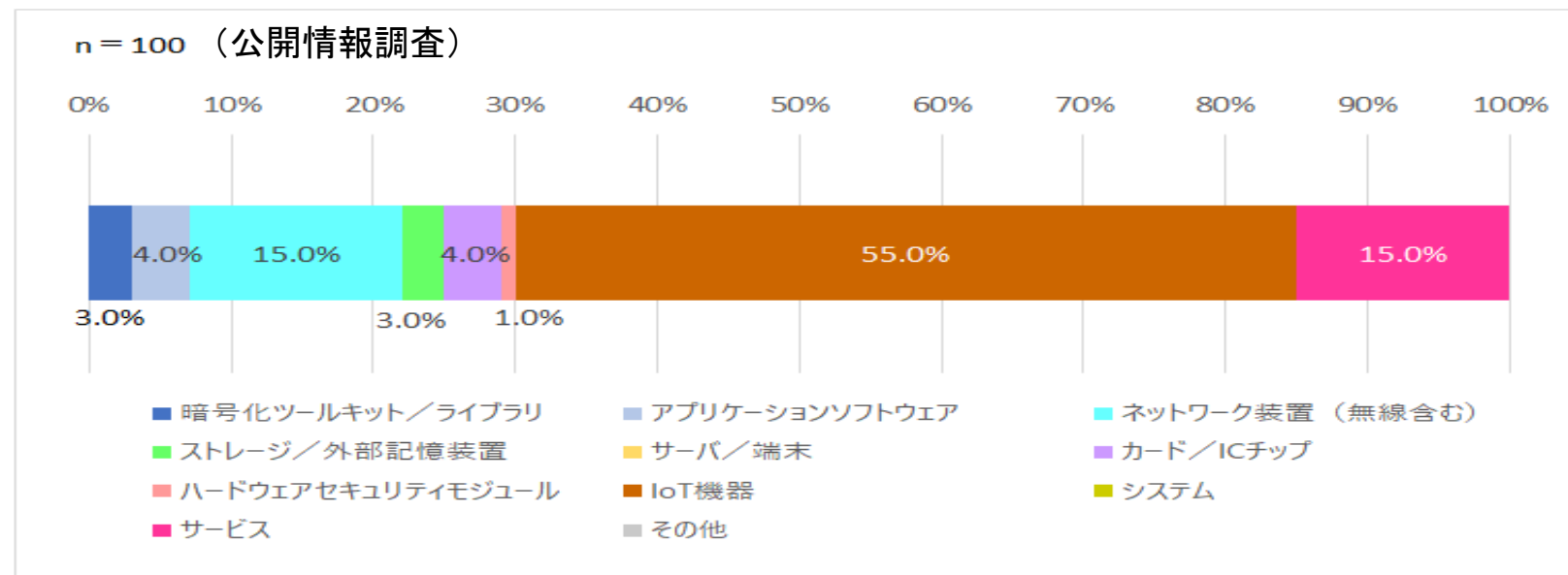
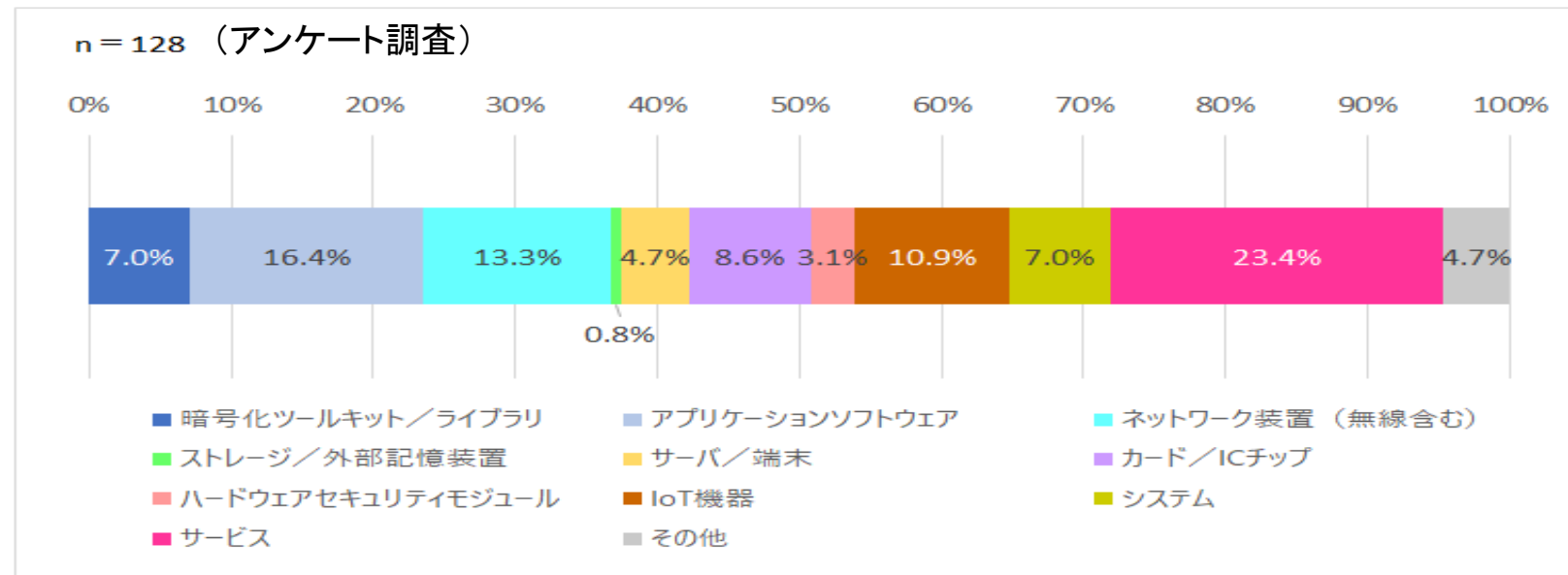


調査パネルの回答(製品数ベース)



委託調査結果(B)

■ 集計対象の製品カテゴリ分布



委託調査結果(C)

■ 規格調査対象

1	電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針 [2020年版]
2	公的個人認証サービス 利用者証明用認証局 運用規程 第2.1版(2021年9月1日)
3	商業登記認証局「電子証明書的方式等に関する件(告示)」(2019年11月29日変更)
4	政府認証基盤(GPKI) 政府認証基盤相互運用性仕様書 2021年版
5	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 [2011年1月21日]
6	標準テレビジョン放送等のうちデジタル放送に関する送信の標準方式第八条第一号及び第二号の規定に基づくスクランブルの方式 平成26年7月3日 総務省告示第235号(平成27年3月20日施行)
7	政府認証基盤(GPKI)ブリッジ認証局(BCA)との相互認証業務に関するCP/CPS(Ver. 5.0)[令和元年11月29日]
8	LGPKI組織認証局R2 CPCPS - 地方公共団体組織認証基盤(LGPKI) [2020]
9	LGPKI技術仕様書 [20190520]
10	認証業務及びこれに附帯する業務の実施に関する技術的基準 [令和三年二月十五日]
11	商業登記認証局「電子証明書的方式等に関する件(告示) [2019.11.29] 付録1 電磁的記録への記録方式(ASN.1構造とオブジェクト識別子)
12	オンライン請求ネットワーク関連システム 共通認証局運用規程 [令和2年9月]
13	総務省告示第七百六号 電子署名に係る地方公共団体の認証業務 [平成十五年十二月三日]
14	医療情報システムの安全管理に関するガイドライン 第5.2版(令和4年3月)
15	クレジットカード・セキュリティガイドライン 3.0 版(2022年3月)
16	【鉄道事業者用】情報セキュリティ対策チェックリスト(令和3年4月第2版)
17	【空港・空港ビル事業者用】情報セキュリティ対策チェックリスト(令和3年4月)

委託調査結果(D)

■ 規格調査対象

1	RFC 6043	MIKEY-TICKET Ticket-Based Modes of Key Distribution in Multimedia Internet KEYing (MIKEY)
2	RFC 6476	Using Message Authentication Code (MAC) Encryption in the Cryptographic Message Syntax (CMS)
3	RFC 6637	Elliptic Curve Cryptography (ECC) in OpenPGP
4	RFC 6781	DNSSEC Operational Practices, Version 2
5	RFC 8645	Re-keying Mechanisms for Symmetric Keys
6	RFC 8702	Use of the SHAKE One-Way Hash Functions in the Cryptographic Message Syntax (CMS)
7	RFC 8708	Use of the HSS/LMS Hash-Based Signature Algorithm in the Cryptographic Message Syntax (CMS)
8	RFC 8723	Double Encryption Procedures for the Secure Real-Time Transport Protocol (SRTP)
9	RFC 8725	JSON Web Token Best Current Practices
10	RFC 8732	Generic Security Service Application Program Interface (GSS-API) Key Exchange with SHA-2
11	RFC 8778	Use of the HSS/LMS Hash-Based Signature Algorithm with CBOR Object Signing and Encryption (COSE)
12	RFC 8812	CBOR Object Signing and Encryption (COSE) and JSON Object Signing and Encryption (JOSE) Registrations for Web Authentication (WebAuthn) Algorithms
13	RFC 8871	A Solution Framework for Private Media in Privacy-Enhanced RTP Conferencing (PERC)
14	RFC 8915	Network Time Security for the Network Time Protocol
15	RFC 9021	Use of the Walnut Digital Signature Algorithm with CBOR Object Signing and Encryption (COSE)
16	RFC 9048	Improved Extensible Authentication Protocol Method for 3GPP Mobile Network Authentication and Key Agreement (EAP-AKA')
17	RFC 9115	An Automatic Certificate Management Environment (ACME) Profile for Generating Delegated Certificates
18	RFC 9132	Distributed Denial-of-Service Open Threat Signaling (DOTS) Signal Channel Specification
19	RFC 9140	Nimble Out-of-Band Authentication for EAP (EAP-NOOB)
20	RFC 9145	Integrity Protection for the Network Service Header (NSH) and Encryption of Sensitive Context Headers
21	IEEE Std 1619-2018	IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices
22	IEEE Std 802.3-2018	IEEE Standard for Ethernet
23	IEEE Std 1609.2-2016	IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages
24	IEEE Std 1901-2020	IEEE Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications
25	IEEE Std 802.15.6-2012	IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks

【参考】委託調査結果(D)

■ 追加民間規格対象(2012調査:50, 2019調査:35, 2022独自調査:42)

	規格番号	規格名	調査年
TLS (26)	RFC2246	The TLS Protocol Version 1.0	2012
	RFC2712	Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)	2012
	RFC3268	Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)	2012
	RFC4162	Addition of SEED Cipher Suites to Transport Layer Security (TLS)	2012
	RFC4346	The Transport Layer Security (TLS) Protocol Version 1.1	2012
	RFC4785	Pre-Shared Key (PSK) Ciphersuites with NULL Encryption for Transport Layer Security (TLS)	2012
	RFC5246	The Transport Layer Security (TLS) Protocol Version 1.2	2012
	RFC5288	AES Galois Counter Mode (GCM) Cipher Suites for TLS	2012
	RFC5289	TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)	2012
	RFC5430	Suite B Profile for Transport Layer Security (TLS)	2012
	RFC5487	Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode	2012
	RFC5489	ECDHE_PSK Cipher Suites for Transport Layer Security (TLS)	2012
	RFC5932	Camellia Cipher Suites for TLS	2012
	RFC7627	Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension	2019
	RFC7905	ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS)	2019
	RFC7918	Transport Layer Security (TLS) False Start	2019
	RFC7919	Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS)	2019
	RFC7924	Transport Layer Security (TLS) Cached Information Extension	2019
	RFC7925	Transport Layer Security (TLS) / Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things	2019
	RFC8422	Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier	2019
	RFC8442	ECDHE_PSK with AES-GCM and AES-CCM Cipher Suites for TLS 1.2 and DTLS 1.2	2019
	RFC8446	The Transport Layer Security (TLS) Protocol Version 1.3	2019
	RFC6209	Addition of the ARIA Cipher Suites to Transport Layer Security (TLS)	2022
	RFC6367	Addition of the Camellia Cipher Suites to Transport Layer Security (TLS)	2022
	RFC6655	AES-CCM Cipher Suites for Transport Layer Security (TLS)	2022
	RFC7251	AES-CCM Elliptic Curve Cryptography (ECC) Cipher Suites for TLS	2022
IPsec (32)	RFC2403	The Use of HMAC-MD5-96 within ESP and AH	2012
	RFC2404	The Use of HMAC-SHA-1-96 within ESP and AH	2012
	RFC2405	The ESP DES-CBC Cipher Algorithm With Explicit IV	2012
	RFC2451	ESP CBC-Mode Cipher Algorithms	2012
	RFC2857	The Use of HMAC-RIPEMD-160-96 within ESP and AH	2012
	RFC3526	More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)	2012
	RFC3566	The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec	2012

【参考】委託調査結果(D)

	規格番号	規格名	調査年
IPsec (32)	RFC3602	The AES-CBC Cipher Algorithm and Its Use with Ipsec	2012
	RFC3686	Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)	2012
	RFC4106	The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)	2012
	RFC4196	The SEED Cipher Algorithm and Its Use with IPsec	2012
	RFC4301	Security Architecture for the Internet Protocol	2012
	RFC4305	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	2012
	RFC4308	Internet Security Association and Key Management Protocol (ISAKMP)	2012
	RFC4309	Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)	2012
	RFC4312	The Camellia Cipher Algorithm and Its Use With Ipsec	2012
	RFC4494	The AES-CMAC-96 Algorithm and Its Use with IPsec	2012
	RFC4543	The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH	2012
	RFC4615	The Advanced Encryption Standard-Cipher-based Message Authentication Code-Pseudo-Random Function-128 (AES-CMAC-PRF-128) Algorithm for the Internet Key Exchange Protocol (IKE)	2012
	RFC4868	Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with Ipsec	2012
	RFC4869	Suite B Cryptographic Suites for IPsec	2012
	RFC7296	Internet Key Exchange Protocol Version 2 (IKEv2)	2019
	RFC7427	Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)	2019
	RFC7634	ChaCha20, Poly1305, and Their Use in the Internet Key Exchange Protocol (IKE) and Ipsec	2019
	RFC8221	Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)	2019
	RFC8229	TCP Encapsulation of IKE and IPsec Packets	2019
	RFC8247	Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)	2019
	RFC8420	Using the Edwards-Curve Digital Signature Algorithm (EdDSA) in the Internet Key Exchange Protocol Version 2 (IKEv2)	2019
	RFC3830	MIKEY: Multimedia Internet KEYing	2022
	RFC4357	Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms	2022
	RFC5528	Camellia Counter Mode and Camellia Counter with CBC-MAC Mode Algorithms	2022
	RFC5748	IANA Registry Update for Support of the SEED Cipher Algorithm in Multimedia Internet KEYing (MIKEY)	2022
S/MIME (15)	RFC3565	Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS)	2012
	RFC3657	Use of the Camellia Encryption Algorithm in Cryptographic Message Syntax (CMS)	2012
	RFC3853	S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP)	2012
	RFC4056	Use of the RSASSA-PSS Signature Algorithm In Cryptographic Message Syntax (CMS)	2012
	RFC5083	Cryptographic Message Syntax (CMS) Authenticated-Enveloped-Data Content Type	2012
	RFC5652	Cryptographic Message Syntax (CMS)	2012

【参考】委託調査結果(D)

	規格番号	規格名	調査年
S/MIME (15)	RFC5753	Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)	2012
	RFC5754	Using SHA2 Algorithms with Cryptographic Message Syntax	2012
	RFC8103	Using ChaCha20-Poly1305 Authenticated Encryption in the Cryptographic Message Syntax (CMS)	2019
	RFC8418	Use of the Elliptic Curve Diffie-Hellman Key Agreement Algorithm with X25519 and X448 in the Cryptographic Message Syntax (CMS)	2019
	RFC8419	Use of Edwards-Curve Digital Signature Algorithm (EdDSA) Signatures in the Cryptographic Message Syntax (CMS)	2019
	RFC8550	Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Certificate Handling	2019
	RFC8551	Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification	2019
	RFC5990	Use of the RSA-KEM Key Transport Algorithm in the Cryptographic Message Syntax (CMS)	2022
	RFC9044	Using the AES-GMAC Algorithm with the Cryptographic Message Syntax (CMS)	2022
Open PGP (2)	RFC3156	MIME Security with OpenPGP	2012
	RFC4880	OpenPGP Message Format	2012
DNSSec (8)	RFC4034	Resource Records for the DNS Security Extensions	2012
	RFC4509	Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)	2012
	RFC5702	Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC	2012
	RFC8080	Edwards-Curve Digital Security Algorithm (EdDSA) for DNSSEC	2019
	RFC4255	Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints	2022
	RFC6594	Use of the SHA-256 Algorithm with RSA, Digital Signature Algorithm (DSA), and Elliptic Curve DSA (ECDSA) in SSHFP Resource Records	2022
	RFC6605	Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC	2022
	RFC8976	Message Digest for DNS Zones	2022
Kerberos (5)	RFC3962	Advanced Encryption Standard (AES) Encryption for Kerberos 5	2012
	RFC4120	The Kerberos Network Authentication Service (V5)	2012
	RFC8009	AES Encryption with HMAC-SHA2 for Kerberos 5	2019
	RFC8636	Public Key Cryptography for Initial Authentication in Kerberos (PKINIT) Algorithm Agility	2019
	RFC6803	Camellia Encryption for Kerberos 5	2022
SSH (3)	RFC8268	More Modular Exponentiation (MODP) Diffie-Hellman (DH) Key Exchange (KEX) Groups for Secure Shell (SSH)	2019
	RFC8332	Use of RSA Keys with SHA-256 and SHA-512 in the Secure Shell (SSH) Protocol	2019
	RFC4250	The Secure Shell (SSH) Protocol Assigned Numbers	2022
PKIX (6)	RFC6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP	2019
	RFC8410	Algorithm Identifiers for Ed25519, Ed448, X25519, and X448 for Use in the Internet X.509 Public Key Infrastructure	2019
	RFC3279	Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	2022
	RFC4055	Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	2022
	RFC5758	Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA	2022
	RFC8692	Internet X.509 Public Key Infrastructure: Additional Algorithm Identifiers for RSASSA-PSS and ECDSA Using SHAKEs	2022

【参考】委託調査結果(D)

規格番号	規格名	調査年
RFC3711	The Secure Real-time Transport Protocol (SRTP)	2022
RFC3713	A Description of the Camellia Encryption Algorithm	2022
RFC4568	Session Description Protocol (SDP) Security Descriptions for Media Streams	2022
RFC5669	The SEED Cipher Algorithm and Its Use with the Secure Real-Time Transport Protocol (SRTP)	2022
RFC5764	Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)	2022
RFC5794	A Description of the ARIA Encryption Algorithm	2022
RFC5830	GOST 28147-89: Encryption, Decryption, and Message Authentication Code (MAC) Algorithms	2022
RFC6030	Portable Symmetric Key Container (PSKC)	2022
RFC6114	The 128-Bit Blockcipher CLEFIA	2022
RFC6188	The Use of AES-192 and AES-256 in Secure RTP	2022
RFC7008	A Description of the KCipher-2 Encryption Algorithm	2022
RFC7714	AES-GCM Authenticated Encryption in the Secure Real-time Transport Protocol (SRTP)	2022
RFC7801	GOST R 34.12-2015: Block Cipher "Kuznyechik"	2022
RFC8017	PKCS #1: RSA Cryptography Specifications Version 2.2	2022
RFC8032	Edwards-Curve Digital Signature Algorithm (EdDSA)	2022
RFC8230	Using RSA Algorithms with CBOR Object Signing and Encryption (COSE) Messages	2022
RFC8269	The ARIA Algorithm and Its Use with the Secure Real-Time Transport Protocol (SRTP)	2022
RFC8439	ChaCha20 and Poly1305 for IETF Protocols	2022
RFC8452	AES-GCM-SIV: Nonce Misuse-Resistant Authenticated Encryption	2022
RFC9231	Additional XML Security Uniform Resource Identifiers (URIs)	2022
IEEE 802.11i-2004	IEEE Standard for information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements	2012
IEEE Std 802.1AE	IEEE Standard for Local and metropolitan area networks-Media Access Control (MAC) Security	2019
IEEE Std 802.1Q	IEEE Standard for Local and Metropolitan Area Network--Bridges and Bridged Networks - Redline	2019
IEEE Std 802.1Xbx	IEEE Standard for Local and metropolitan area networks -- Port-Based Network Access Control Amendment 1: MAC Security Key Agreement Protocol (MKA) Extensions	2019
IEEE Std 802.11	IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications	2019
IEEE Std 802.15.4	IEEE Standard for Low-Rate Wireless Networks	2019
IEEE Std 802.16	IEEE Standard for Air Interface for Broadband Wireless Access Systems	2019
IEEE Std 802.21	IEEE Standard for Local and metropolitan area networks--Part 21: Media Independent Services Framework	2019
FIDO [2017]	https://fidoalliance.org/specs/fido-security-requirements-v1.0-fd-20170524/fido-authenticator-allowed-cryptography-list_20170524.html	2022
TCG [2018]	https://trustedcomputinggroup.org/wp-content/uploads/TCG_-_Algorithm_Registry_Rev_1.27_FinalPublication.pdf	2022

【参考】委託調査結果(D)

■ 追加国際規格対象(2012調査:8, 2019調査:4, 2022独自調査:10)

規格番号			規格名	調査年
ISO/IEC	9797	1:2011	Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher	2012
ISO/IEC	9797	2:2021	Message authentication codes (MACs) — Part 2: Mechanisms using a dedicated hash-function	2022
ISO/IEC	9797	3:2011	Message Authentication Codes (MACs) — Part 3: Mechanisms using a universal hash-function	2022
ISO/IEC	10116	2017	Modes of operation for an n-bit block cipher	2019
ISO/IEC	10118	2:2010	Hash-functions — Part 2: Hash-functions using an n-bit block cipher	2012
ISO/IEC	10118	3:2018	Hash-functions — Part 3: Dedicated hash-functions	2019
ISO/IEC	14888	2:2008	Digital signatures with appendix — Part 2: Integer factorization based mechanisms	2012
ISO/IEC	14888	3:2018	Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms	2019
ISO/IEC	18033	2:2006	Encryption algorithms — Part 2: Asymmetric ciphers	2012
ISO/IEC	18033	3:2010	Encryption algorithms — Part 3: Block ciphers	2012
ISO/IEC	18033	AMD:2021	Encryption algorithms — Part 3: Block ciphers — AMENDMENT 1: SM4	2022
ISO/IEC	18033	4:2011	Encryption algorithms — Part 4: Stream ciphers	2012
ISO/IEC	19772	2020	Authenticated encryption	2022
ISO/IEC	29192	2:2019	Lightweight cryptography — Part 2: Block ciphers	2022
ISO/IEC	29192	3:2012	Lightweight cryptography — Part 3: Stream ciphers	2012
ITU-T	Y.2704	01/2010	Security mechanisms and procedures for NGN	2012
ITU-T	X.1197	04/2012	Guidelines on criteria for selecting cryptographic algorithms for IPTV service and content protection	2022
ITU-T	X.1197	09/2019	Guidelines on criteria for selecting cryptographic algorithms for IPTV service and content protection Amendment 1	2022
ITU-T	X.1811	04/2021	Security guidelines for applying quantum-safe algorithms in IMT-2020 systems	2022
ITU-T	X.1372	03/2020	Security guidelines for vehicle-to-everything (V2X) communication	2022
ITU-T	H235.6	01/2014	H.323 security: Encryption profile with native ITU-T H.235/H.245 key management	2019
ICAO	Doc9303-11	2021	Machine Readable Travel Documents Part 11: Security Mechanisms for MRTDs	2022

委託調査結果(E)

■ OSS調査対象

No.	OSS名	ソースコードURL(最終調査日)
1	Java	https://github.com/openjdk/ (2022年9月27日)
2	PHP	https://github.com/php/php-src (2022年9月27日)
3	Python	https://github.com/python/cpython (2022年10月13日)
4	Gitlab	https://gitlab.com/gitlab-org/gitlab (2022年9月27日)
5	Redmine	https://github.com/redmine/redmine (2022年9月27日) http://svn.redmine.org/redmine/ (2022年9月27日)
6	Eclipse	https://github.com/eclipse (2022年9月27日)
7	Apache	https://github.com/apache/httpd (2022年9月27日) https://dldn.apache.org/httpd/ (2022年9月27日)
8	Nginx	https://github.com/nginx/nginx (2022年9月27日) http://hg.nginx.org/nginx/ (2022年9月27日)
9	Samba	https://github.com/samba-team/samba (2022年9月27日) https://git.samba.org/samba.git/ (2022年9月27日)
10	MySQL	https://github.com/mysql/mysql-server (2022年9月27日) https://dev.mysql.com/downloads/mysql/ (2022年9月27日)
11	PostgreSQL	https://github.com/postgres/postgres (2022年9月27日) https://www.postgresql.org/ftp/source/ (2022年9月27日)
12	Redis	https://github.com/redis/redis (2022年9月27日) https://redis.io/download/#redis-downloads (2022年9月27日)
13	Linux	https://github.com/torvalds/linux (2022年9月27日) https://www.kernel.org/ (2022年9月27日)
14	FreeBSD	https://github.com/freebsd/freebsd-src (2022年9月27日) https://cgит.freebsd.org/src/ (2022年9月27日)
15	Debian	https://github.com/Debian (2022年10月13日) https://sources.debian.org/ (2022年10月13日)
16	Android	https://github.com/aosp-mirror (2022年9月27日) https://android.googlesource.com/ (2022年9月27日)
17	mbedOS	https://github.com/ARMmbed/mbed-os (2022年9月27日)
18	Ubuntu	https://github.com/ubuntu (2022年9月27日) https://kernel.ubuntu.com/git/ (2022年9月27日)
19	Docker	https://github.com/docker (2022年9月27日)

No.	OSS名	ソースコードURL(最終調査日)
20	Webkit	https://github.com/WebKit/WebKit (2022年9月27日)
21	Chrome	https://github.com/chromium/chromium (2022年10月13日) https://source.chromium.org/chromium (2022年10月13日)
22	OpenOffice	https://github.com/apache/openoffice (2022年9月27日) https://gitbox.apache.org/repos/asf/openoffice.git (2022年9月27日)
23	OpenSSL	https://github.com/openssl/openssl (2022年9月27日) https://git.openssl.org/ (2022年9月27日)
24	Network Security Service (NSS)	https://github.com/nss-dev/nss (2022年9月27日) https://hg.mozilla.org/projects/nspr (2022年9月27日)
25	GnuPG	https://github.com/gpg/gnupg (2022年9月27日) https://git.gnupg.org/cgi-bin/gitweb.cgi?p=gnupg.git (2022年9月27日)
26	Mcrypt	http://mcrypt.cvs.sourceforge.net/ (2022年9月27日)
27	Bouncy Castle	https://github.com/bcgit (2022年9月27日)
28	libsodium	https://github.com/jedisct1/libsodium (2022年9月27日)
29	7-zip	https://sevenzips.osdn.jp/download.html (2022年9月27日)
30	Keycloak	https://github.com/keycloak/keycloak (2022年9月27日)

委託調査結果(D)(E)

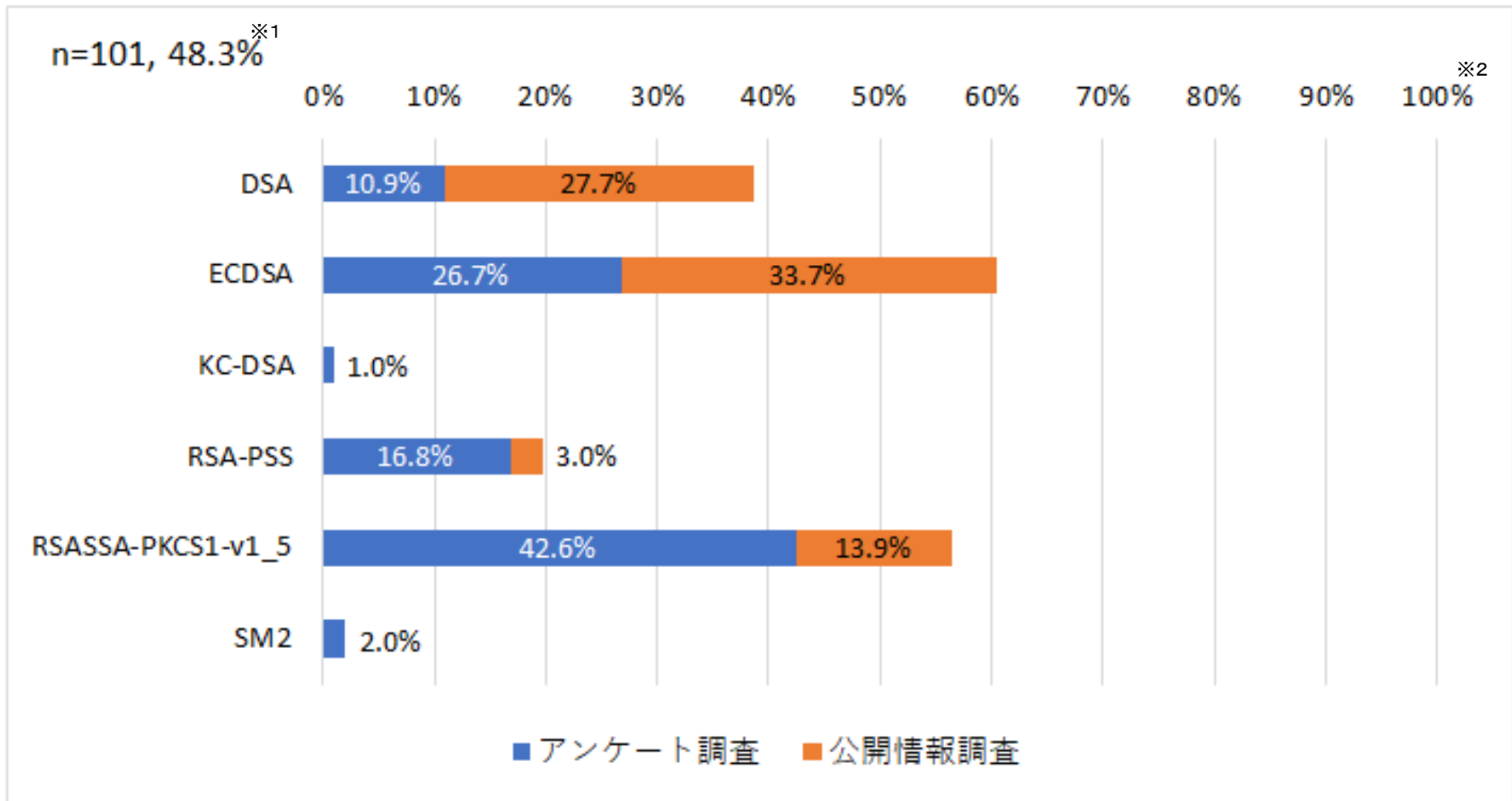
■ 調査(D)での確認方法

- 個々の規格文書ファイルに対して、検索ツールを用いて調査対象暗号アルゴリズム名で検索
- 検索にかかった暗号アルゴリズムについて、内容を確認した上でその記載が参考情報扱いでないものについて、「当該暗号アルゴリズムは実装されている」と見なす
- 検索にかからない、又は内容確認の結果、暗号アルゴリズムの記載が参考情報扱いであるものについては、「当該暗号アルゴリズムは実装されていない」と見なす

■ 調査(E)での確認方法

- ソースコードURLのサイト内検索ツールを用いて調査対象暗号アルゴリズム名で検索
※一部、ダウンロード・解凍した後にフォルダ内検索を実施したものあり
- 検索結果に表示される暗号アルゴリズムについて、ソースコードが存在する、実装されていることが明示されている、又は実装されていることが前提とした議論がある場合に「当該暗号アルゴリズムは実装されている」と見なす
- 検索結果に表示されない暗号アルゴリズム、及び検索結果に表示される暗号アルゴリズムでも情報としてのみの表示としか確認できない場合は、「当該暗号アルゴリズムは実装されていない」と見なす

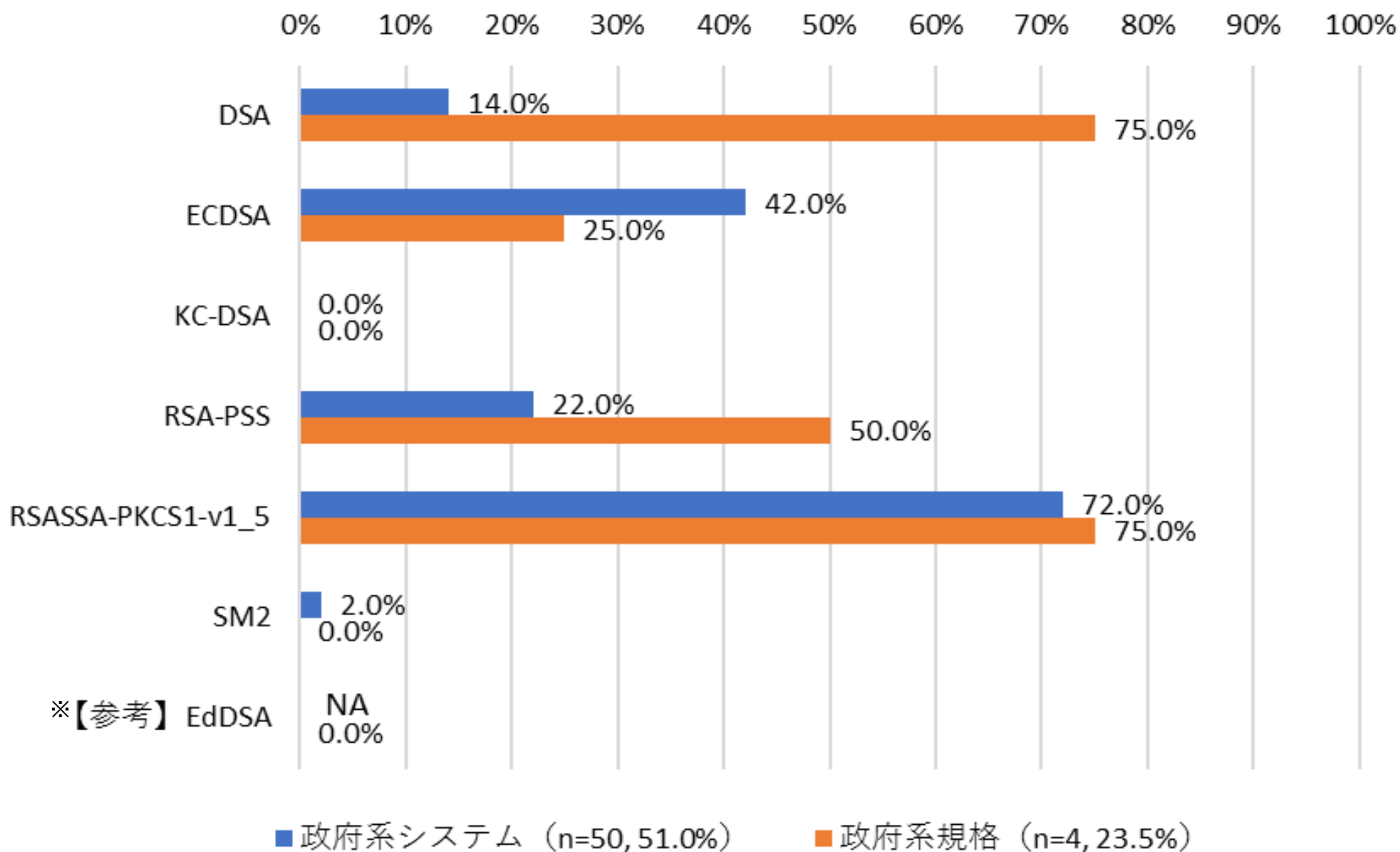
利用実績－市販製品（公開鍵暗号（署名））



※1集計対象209製品中、公開鍵暗号（署名）が101製品で実装（実装率：48.3% = 101/209）

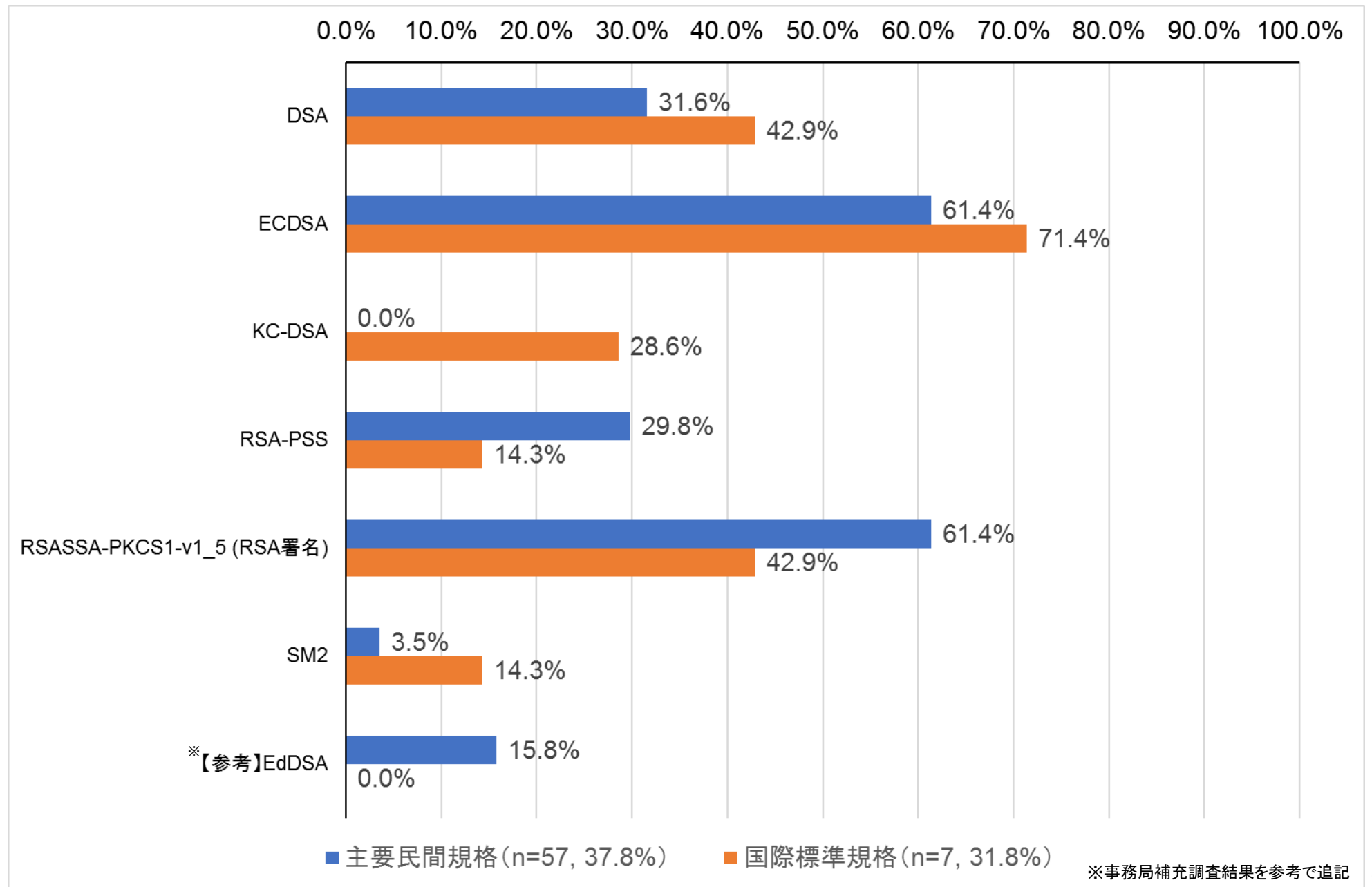
※2公開鍵暗号（署名）が実装された101製品に対する各アルゴリズムの実装率（実装率：100% = 101/101）

利用実績－政府系情報システム・規格（公開鍵暗号（署名））



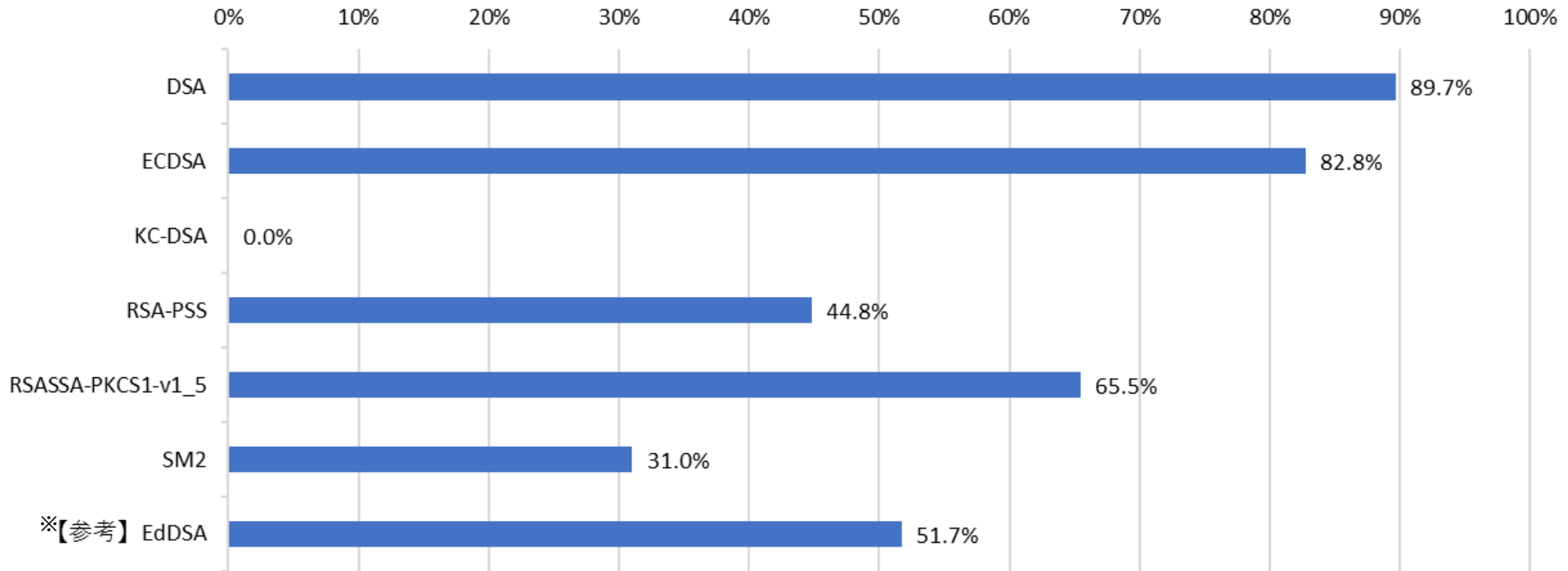
※事務局補充調査結果を参考で追記

利用実績－標準規格・民間規格(公開鍵暗号(署名))



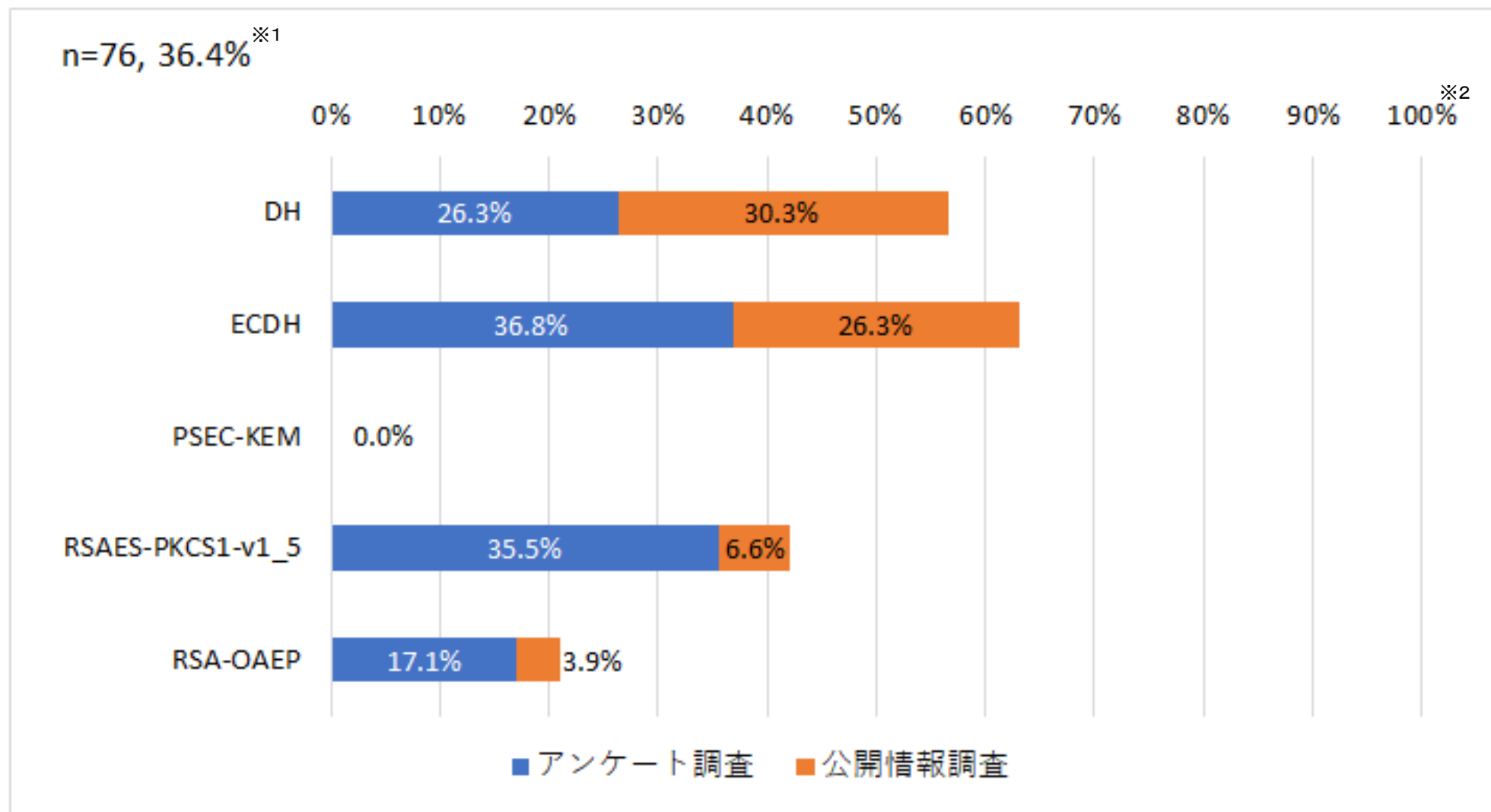
利用実績－オープンソースソフトウェア（公開鍵暗号（署名））

n = 29, 96.7%



※事務局補充調査結果を参考で追記

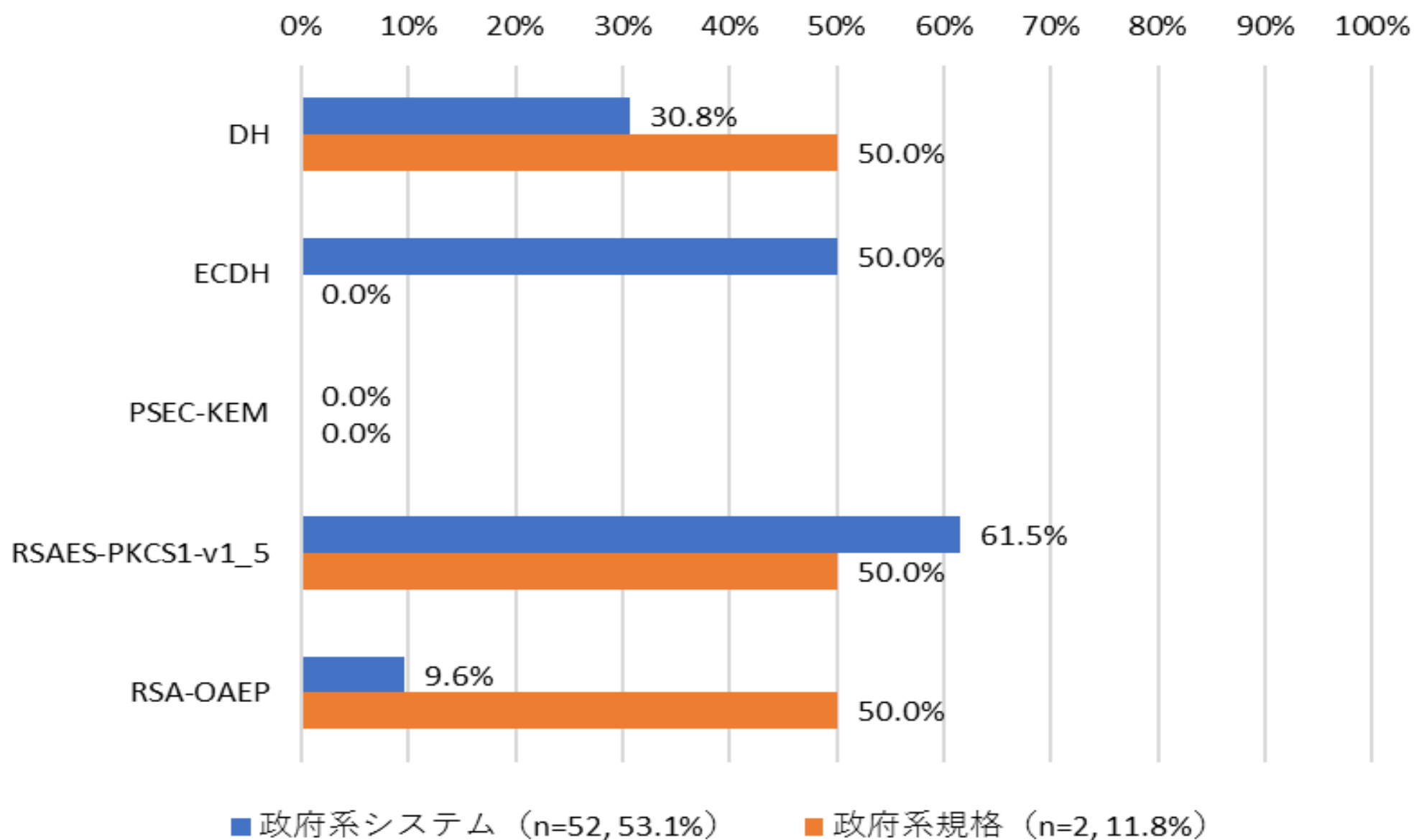
利用実績－市販製品（公開鍵暗号（守秘・鍵共有））



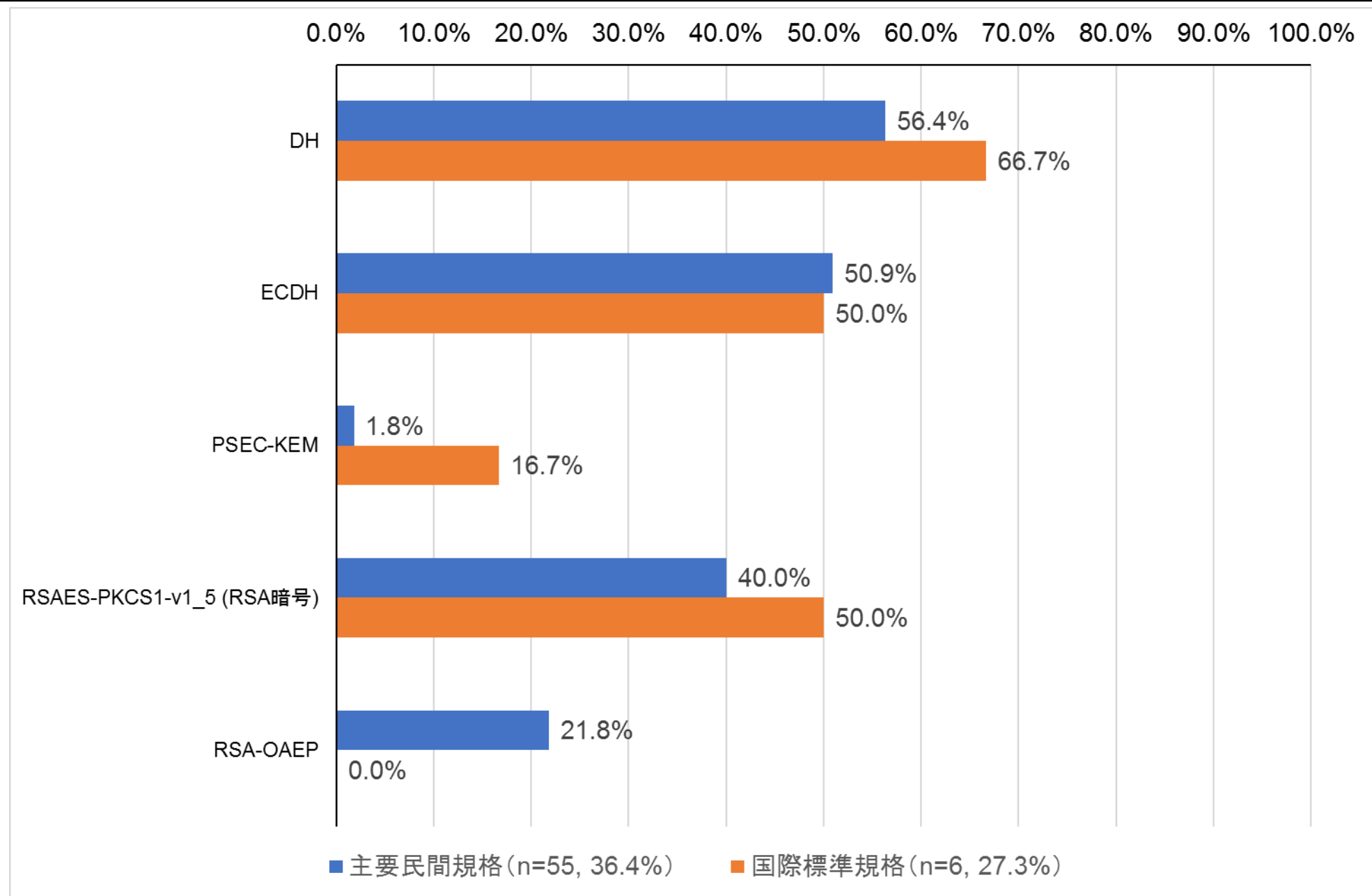
※1 集計対象209製品中、公開鍵暗号（守秘・鍵共有）が76製品で実装（実装率：36.4% = 76/209）

※2 公開鍵暗号（守秘・鍵共有）が実装された76製品に対する各アルゴリズムの実装率（実装率：100% = 76/76）

利用実績－政府系情報システム・規格(公開鍵暗号(守秘・鍵共有))

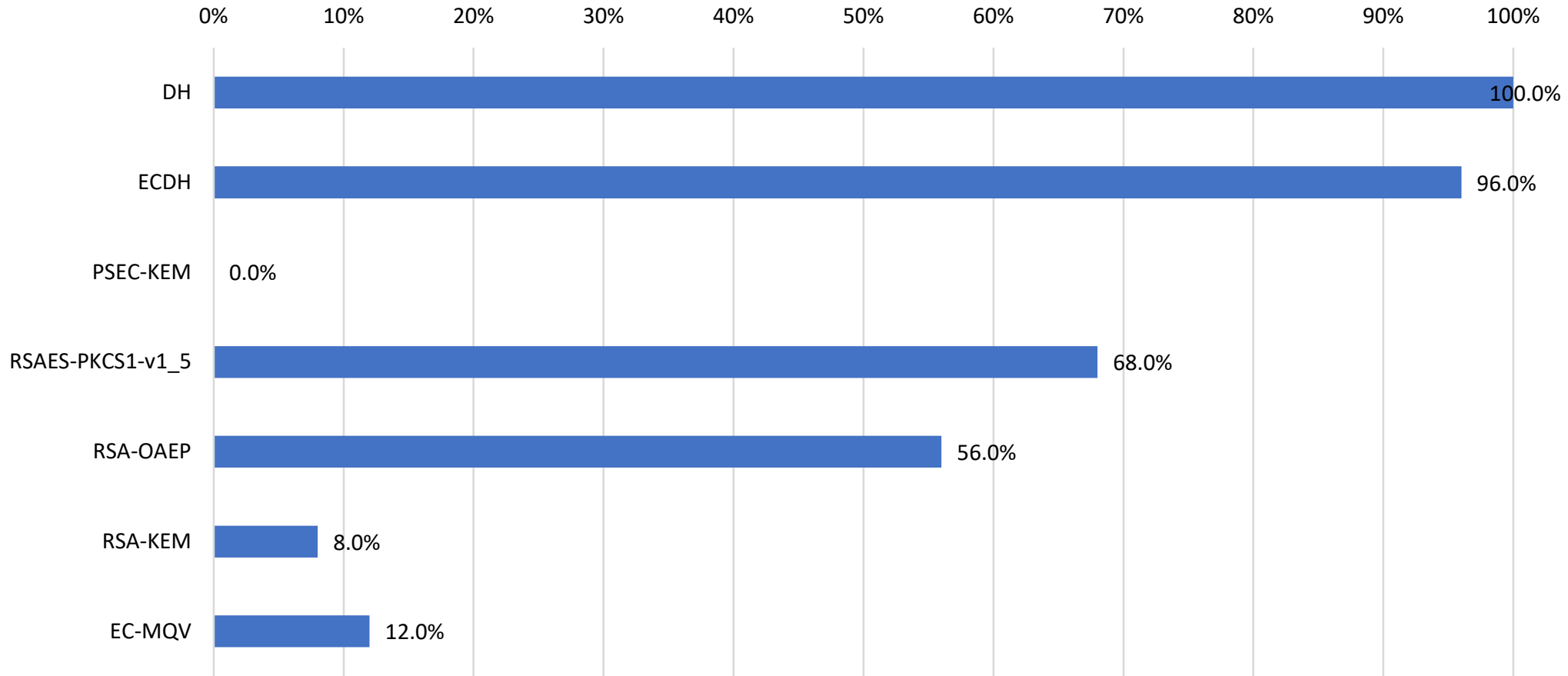


利用実績－標準規格・民間規格(公開鍵暗号(守秘・鍵共有))

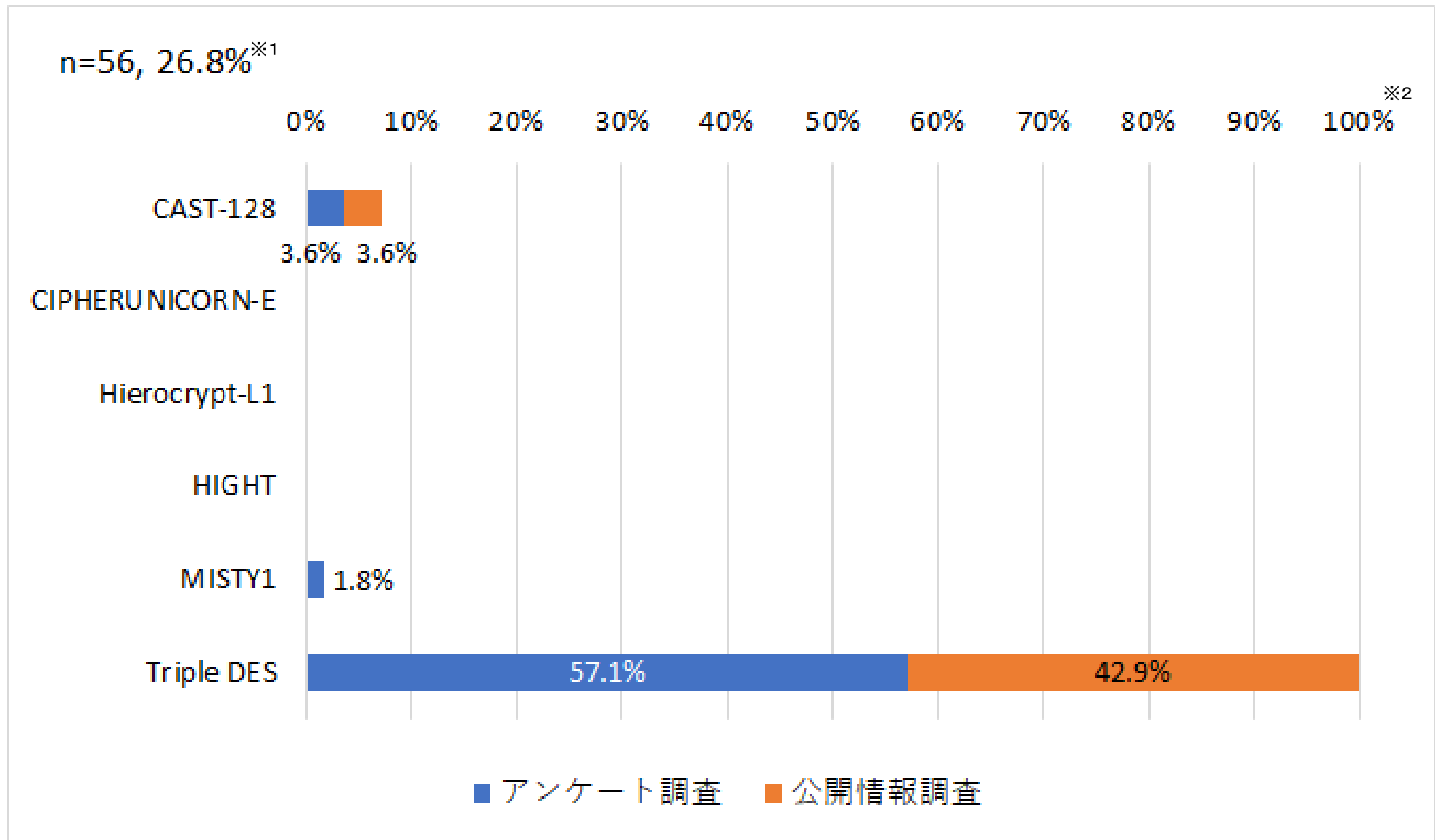


利用実績－オープンソースソフトウェア（公開鍵暗号（守秘・鍵交換））

n = 25, 83.3%



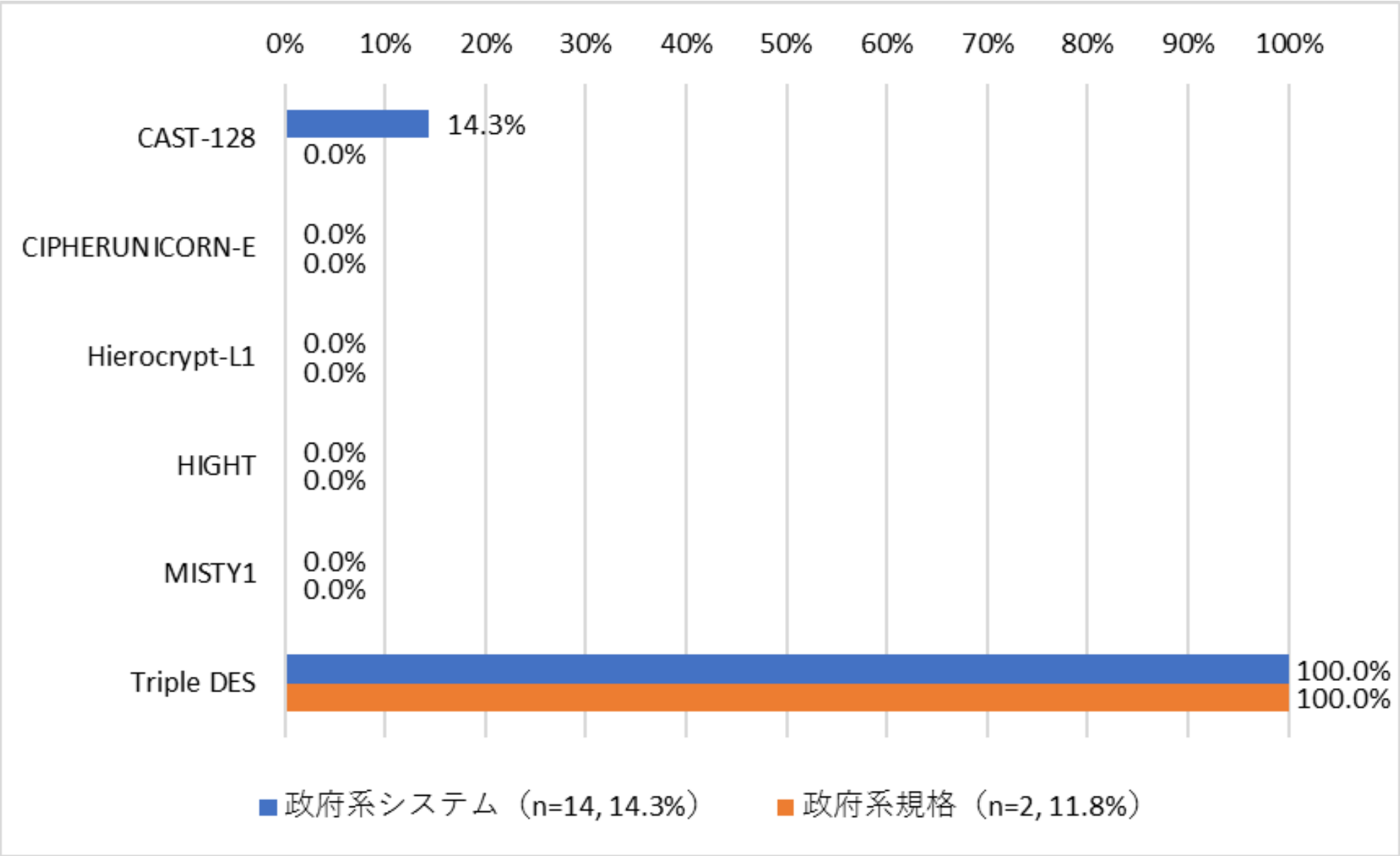
利用実績－市販製品（共通鍵暗号（64ビットブロック暗号））



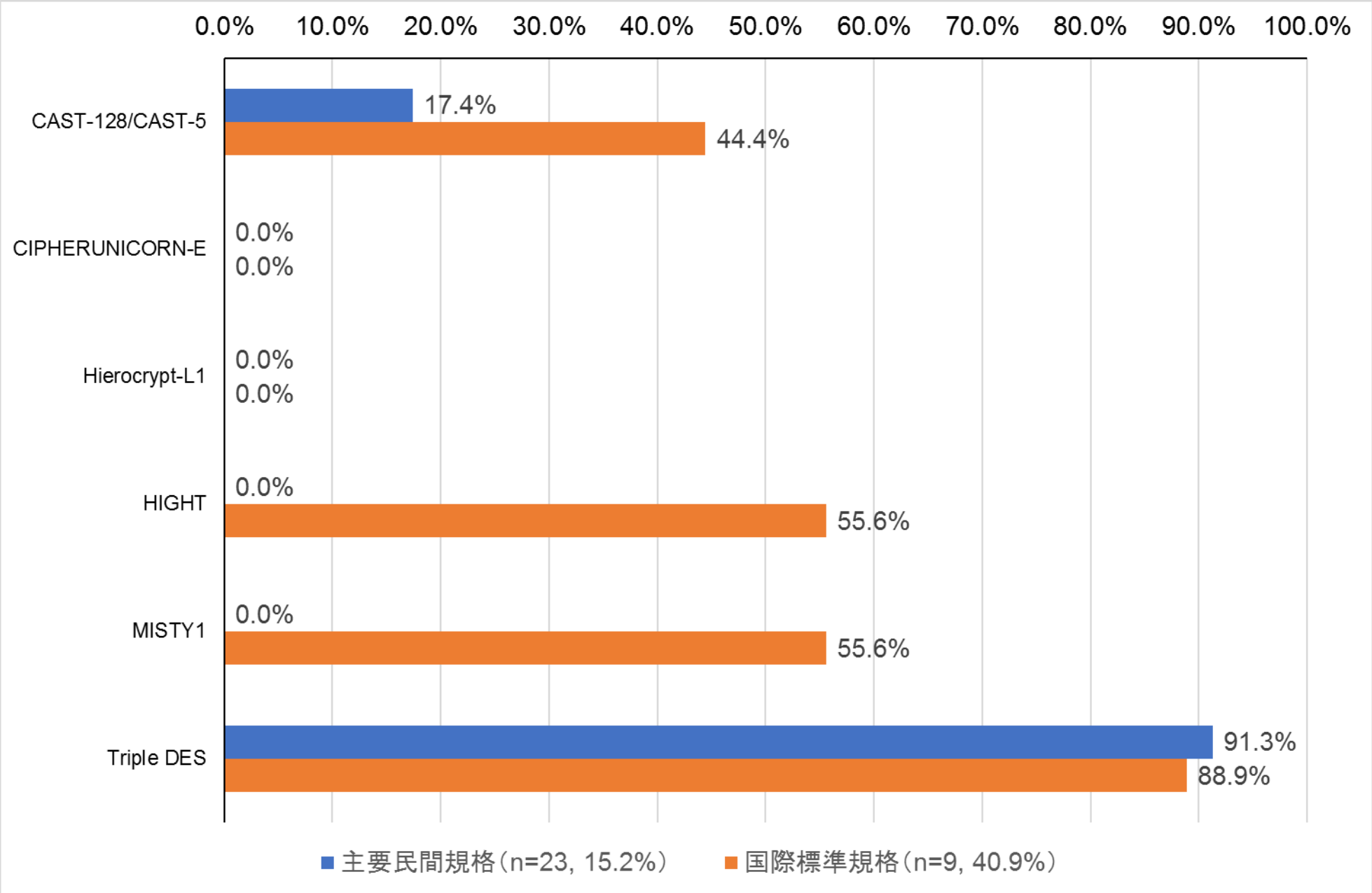
※1 集計対象209製品中、64ビットブロック暗号が56製品で実装（実装率：26.8% = 56/209）

※2 64ビットブロック暗号が実装された56製品に対する各アルゴリズムの実装率（実装率：100% = 56/56）

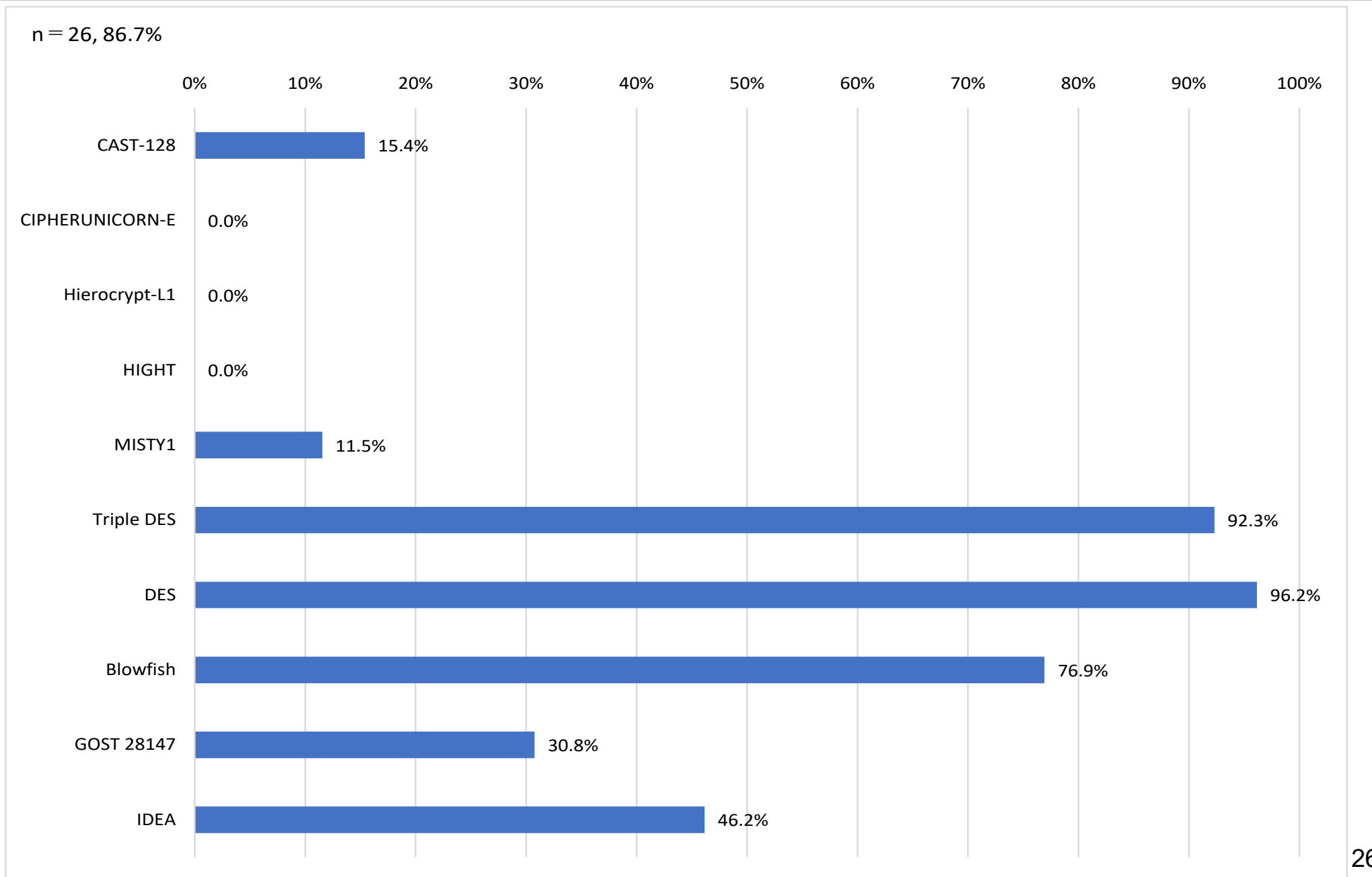
利用実績－政府系情報システム・規格（共通鍵暗号（64ビットブロック暗号））



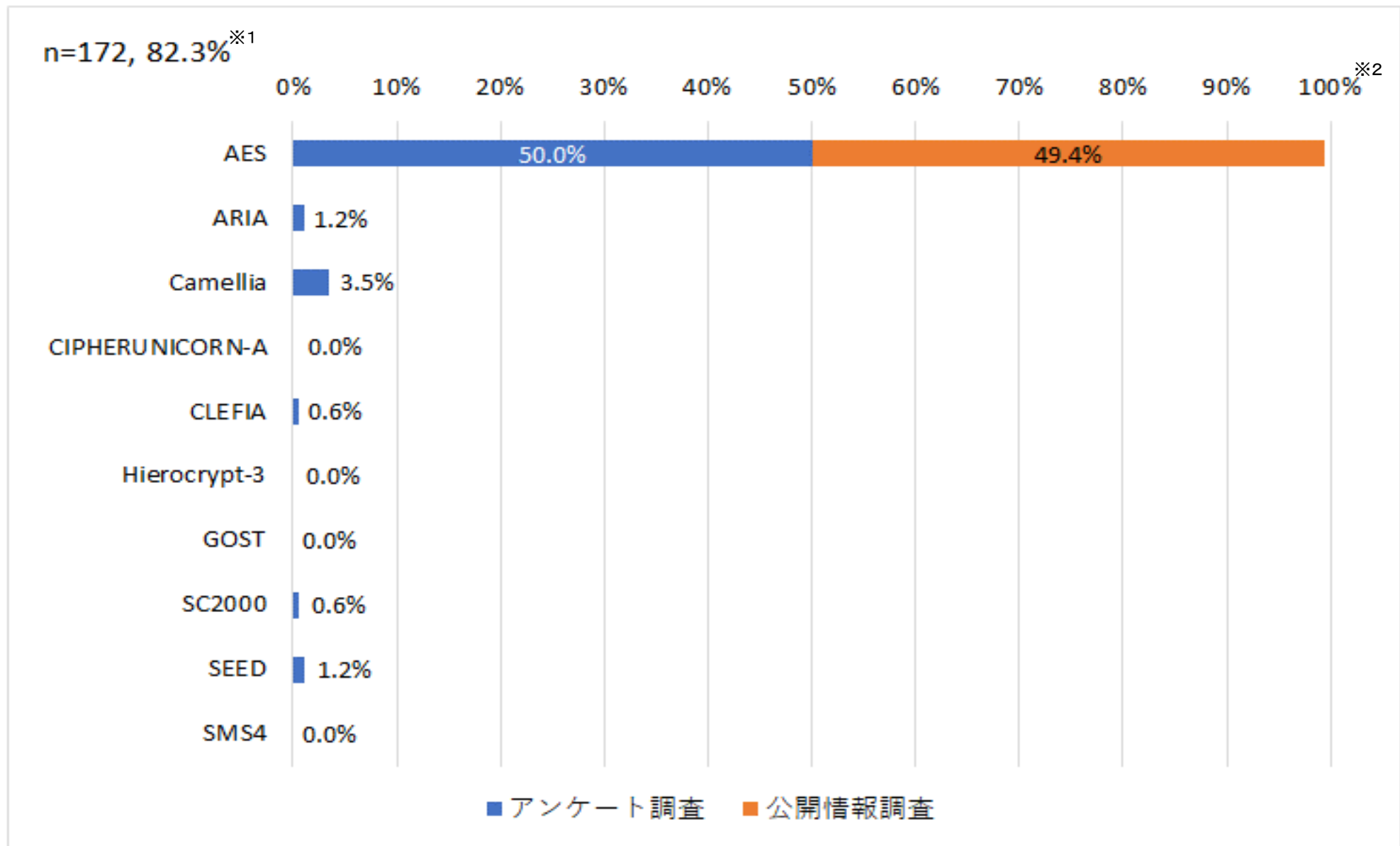
利用実績－標準規格・民間規格(共通鍵暗号(64ビットブロック暗号))



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



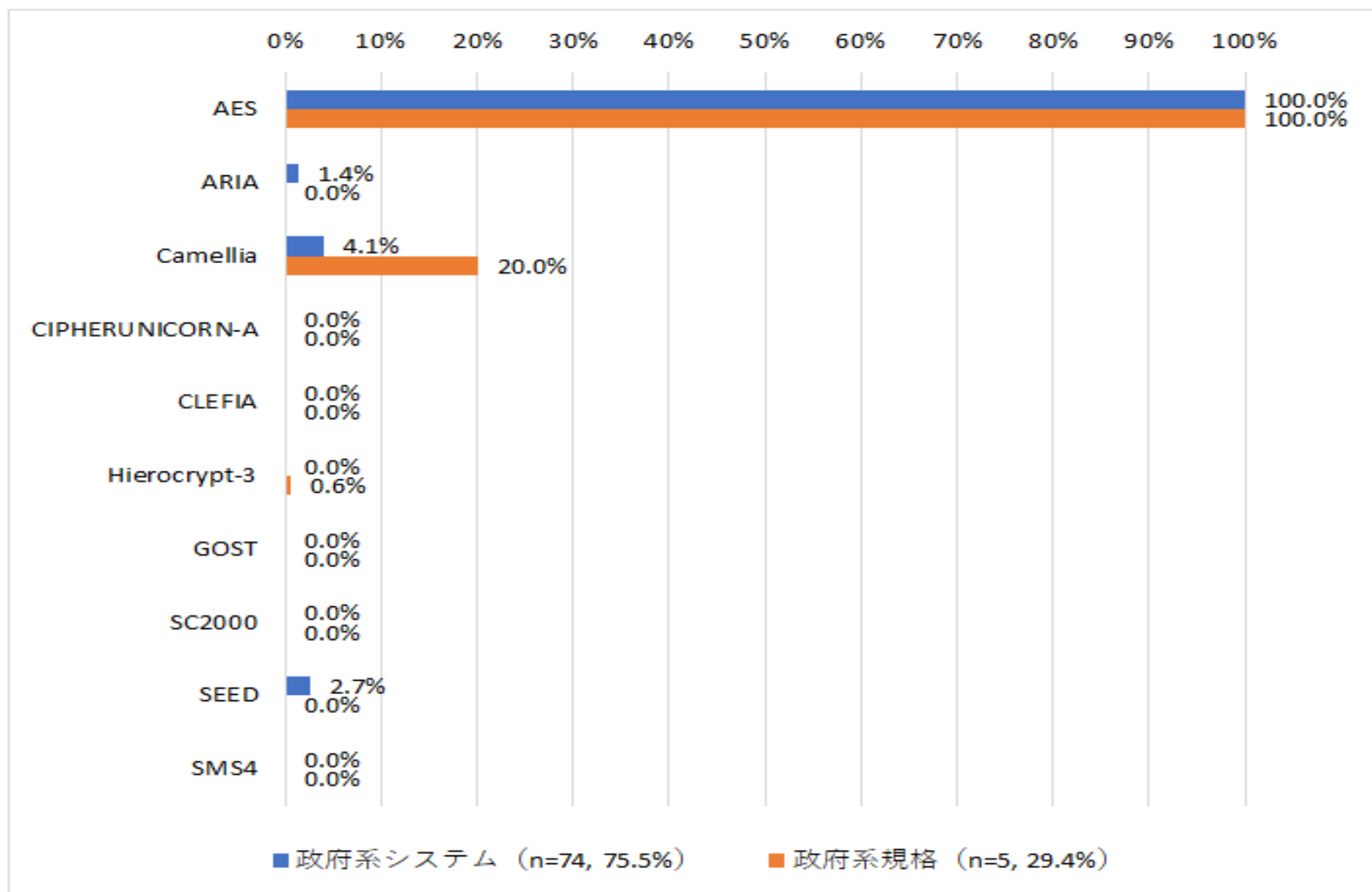
利用実績－市販製品（共通鍵暗号（128ビットブロック暗号））



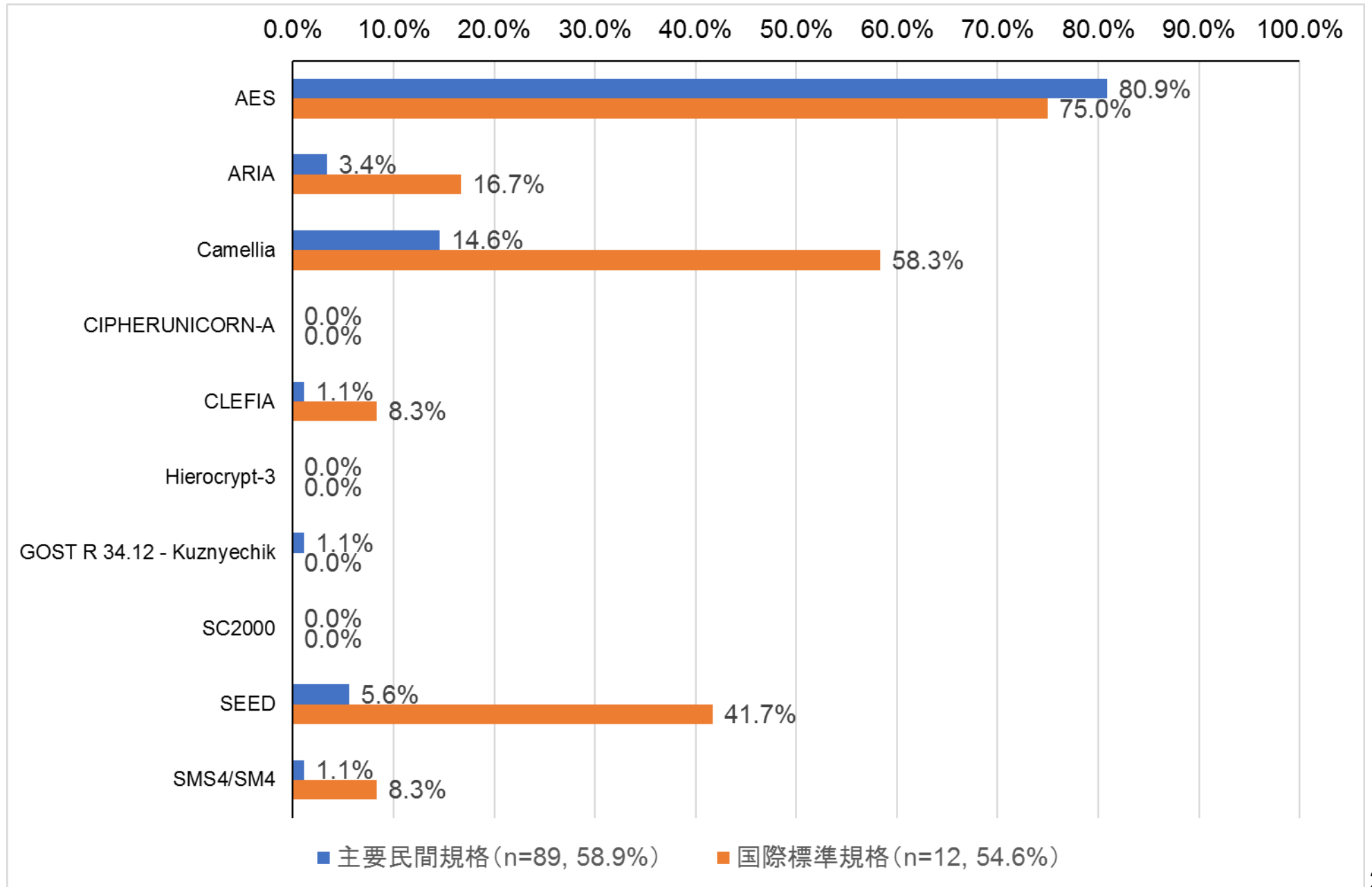
※1集計対象209製品中、128ビットブロック暗号が172製品で実装（実装率：82.3% = 172/209）

※2128ビットブロック暗号が実装された172製品に対する各アルゴリズムの実装率（実装率：100% = 172/172）

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

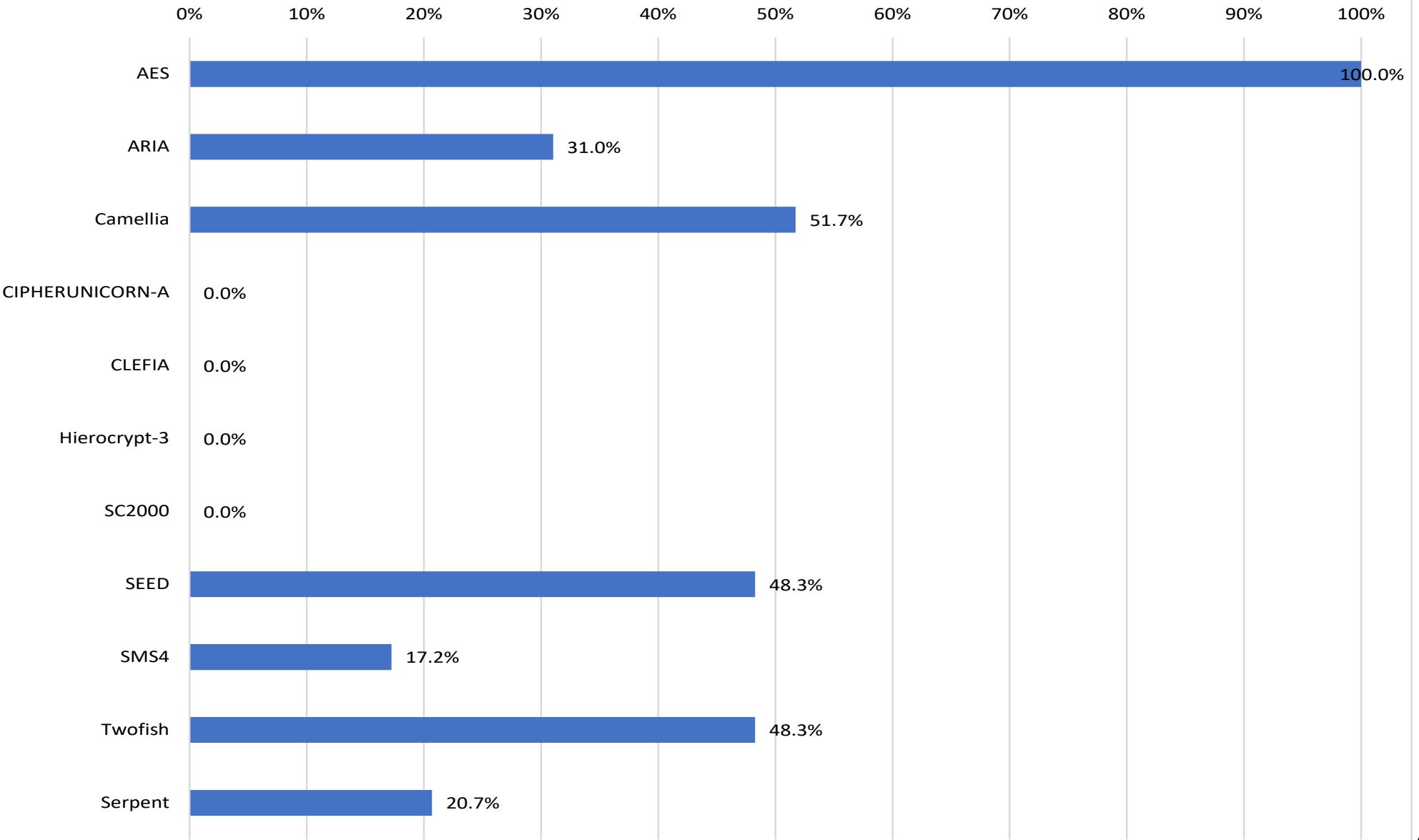


利用実績－標準規格・民間規格(共通鍵暗号(128ビットブロック暗号))

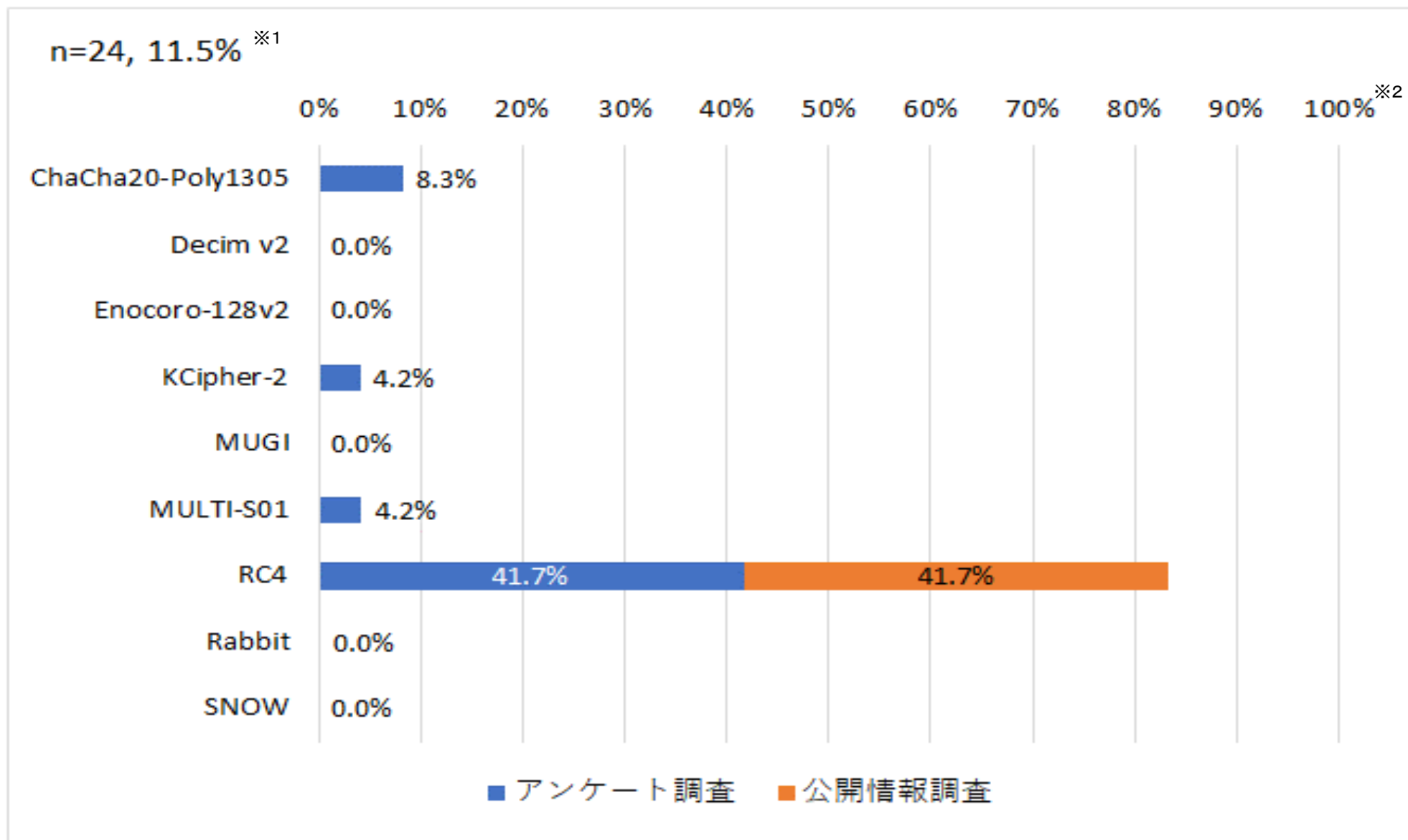


利用実績－オープンソースソフトウェア（共通鍵暗号（128ビットブロック暗号））

n = 29, 96.7%



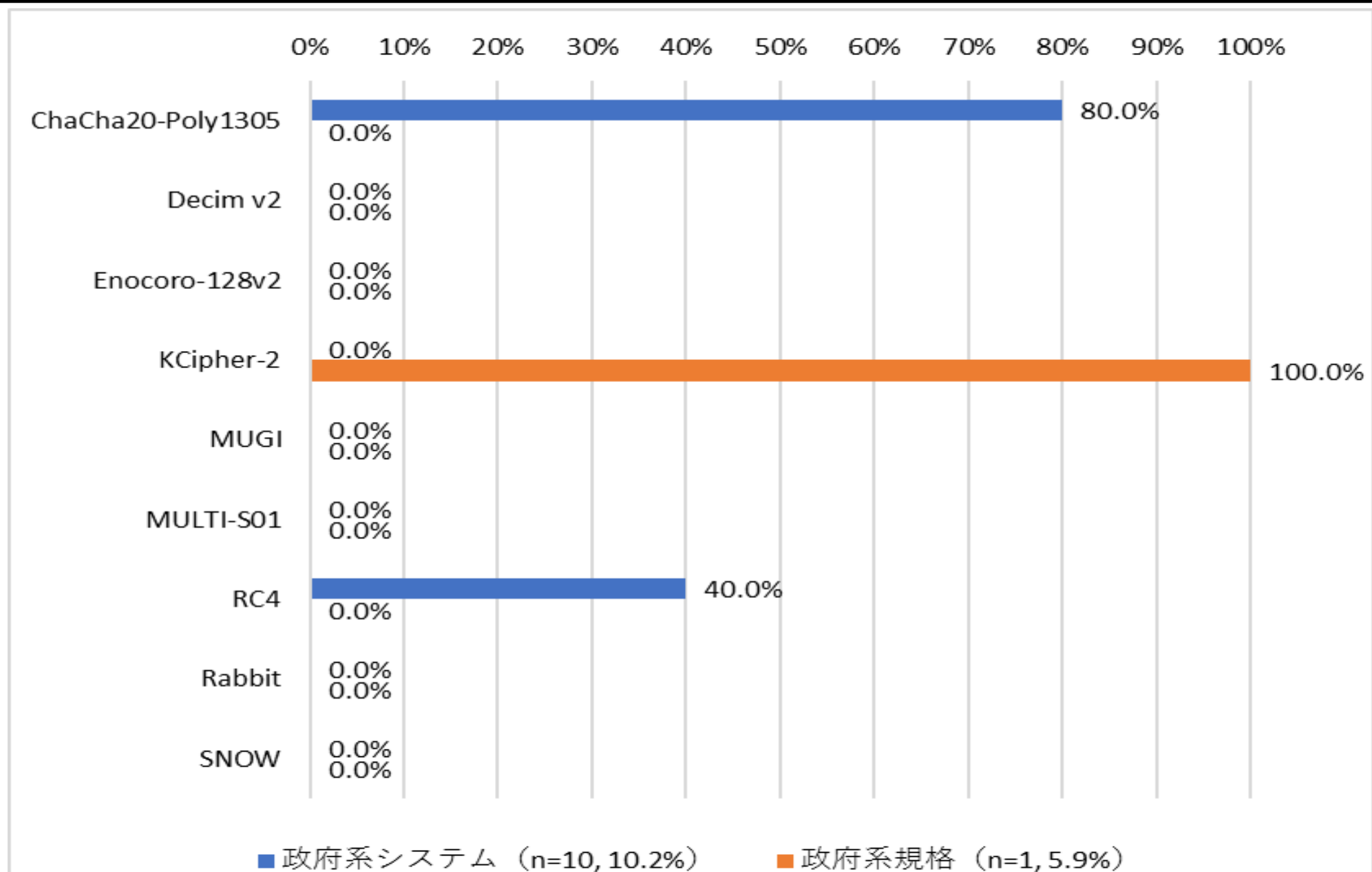
利用実績－市販製品（共通鍵暗号（ストリーム暗号・認証暗号））



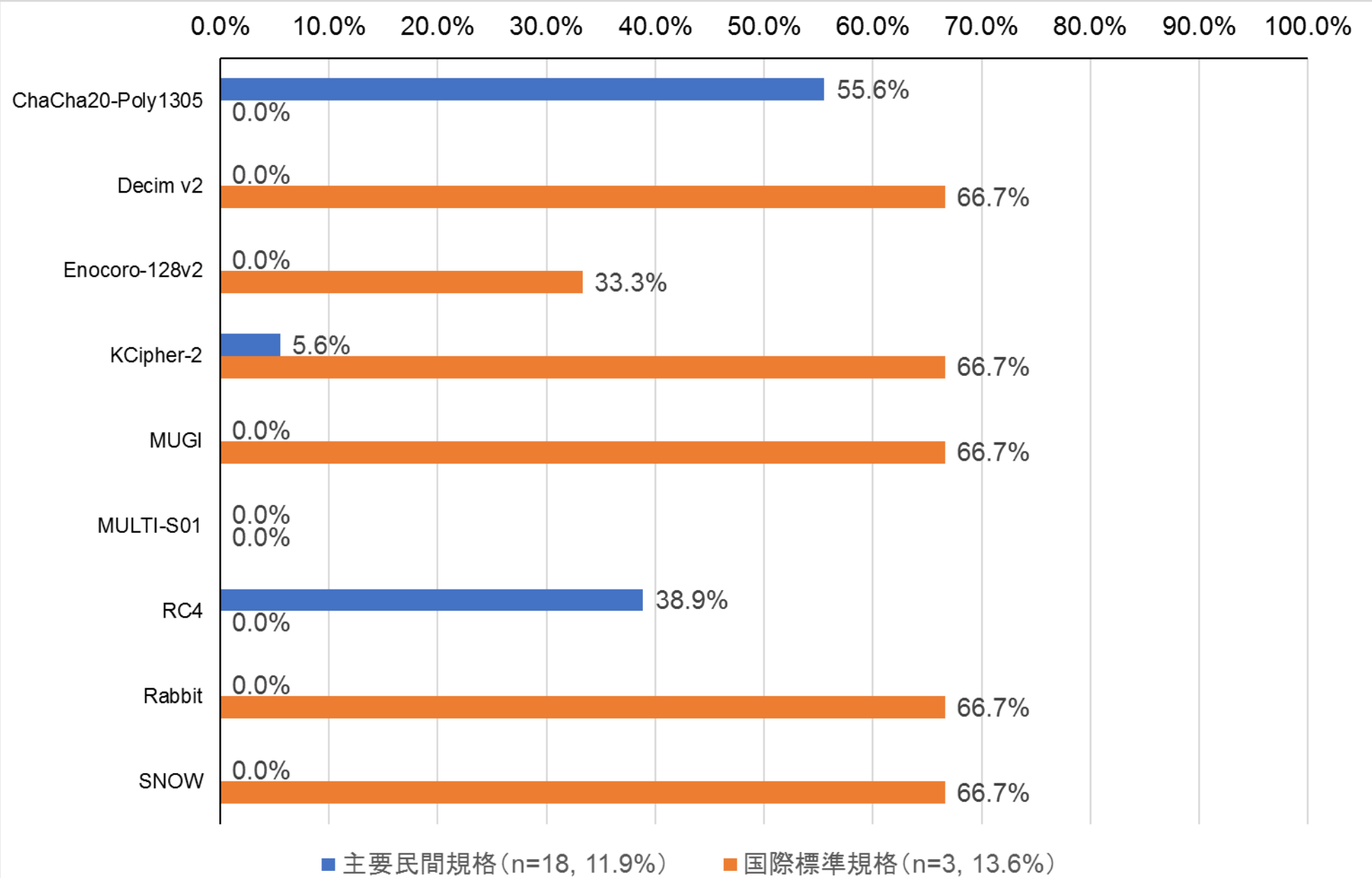
※1集計対象209製品中、ストリーム暗号・認証暗号が24製品で実装（実装率：11.5% = 24/209）

※2ストリーム暗号・認証暗号が実装された24製品に対する各アルゴリズムの実装率（実装率：100% = 24/24）

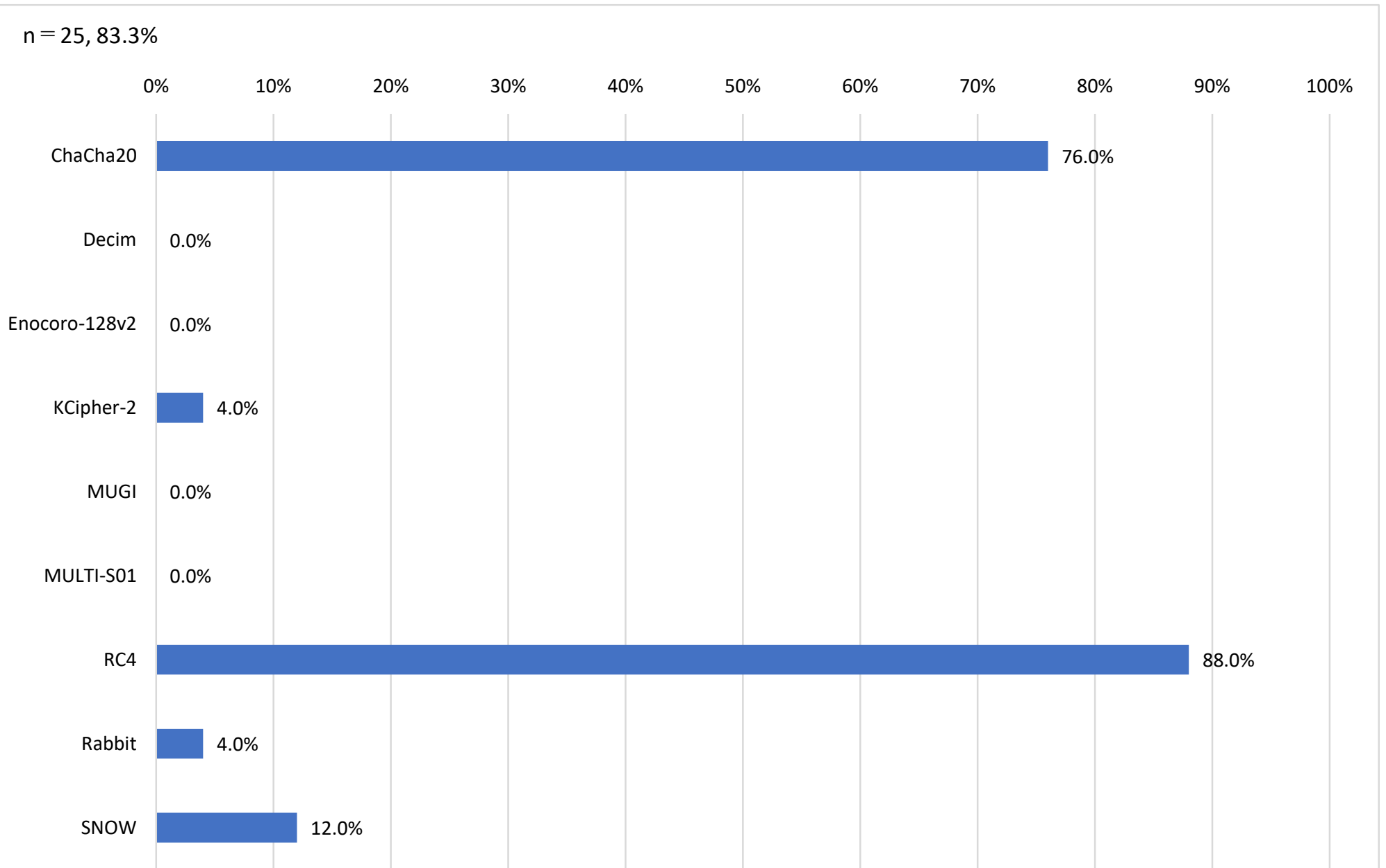
利用実績－政府系情報システム・規格（共通鍵暗号（ストリーム暗号・認証暗号））



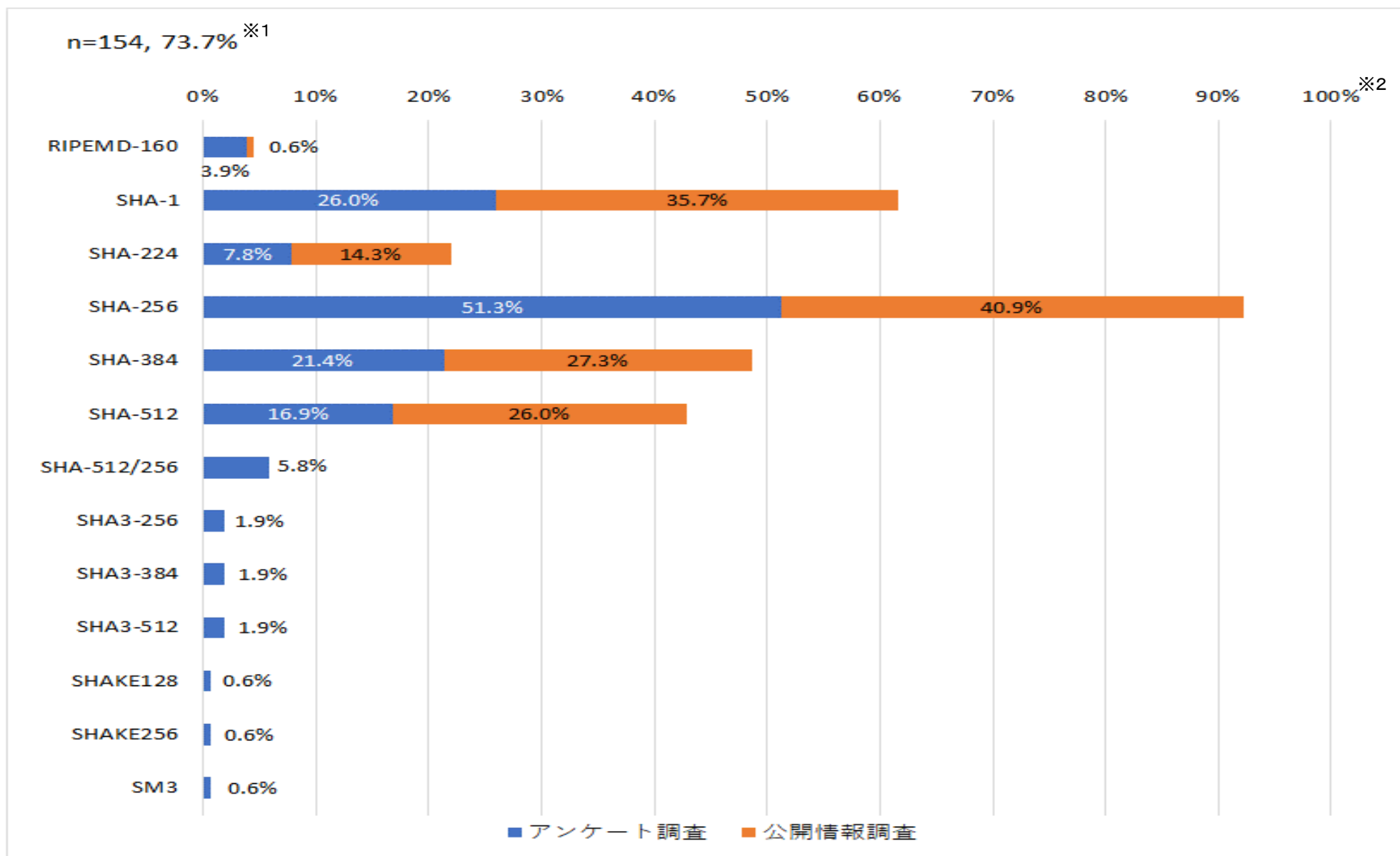
利用実績－標準規格・民間規格(共通鍵暗号(ストリーム暗号・認証暗号))



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



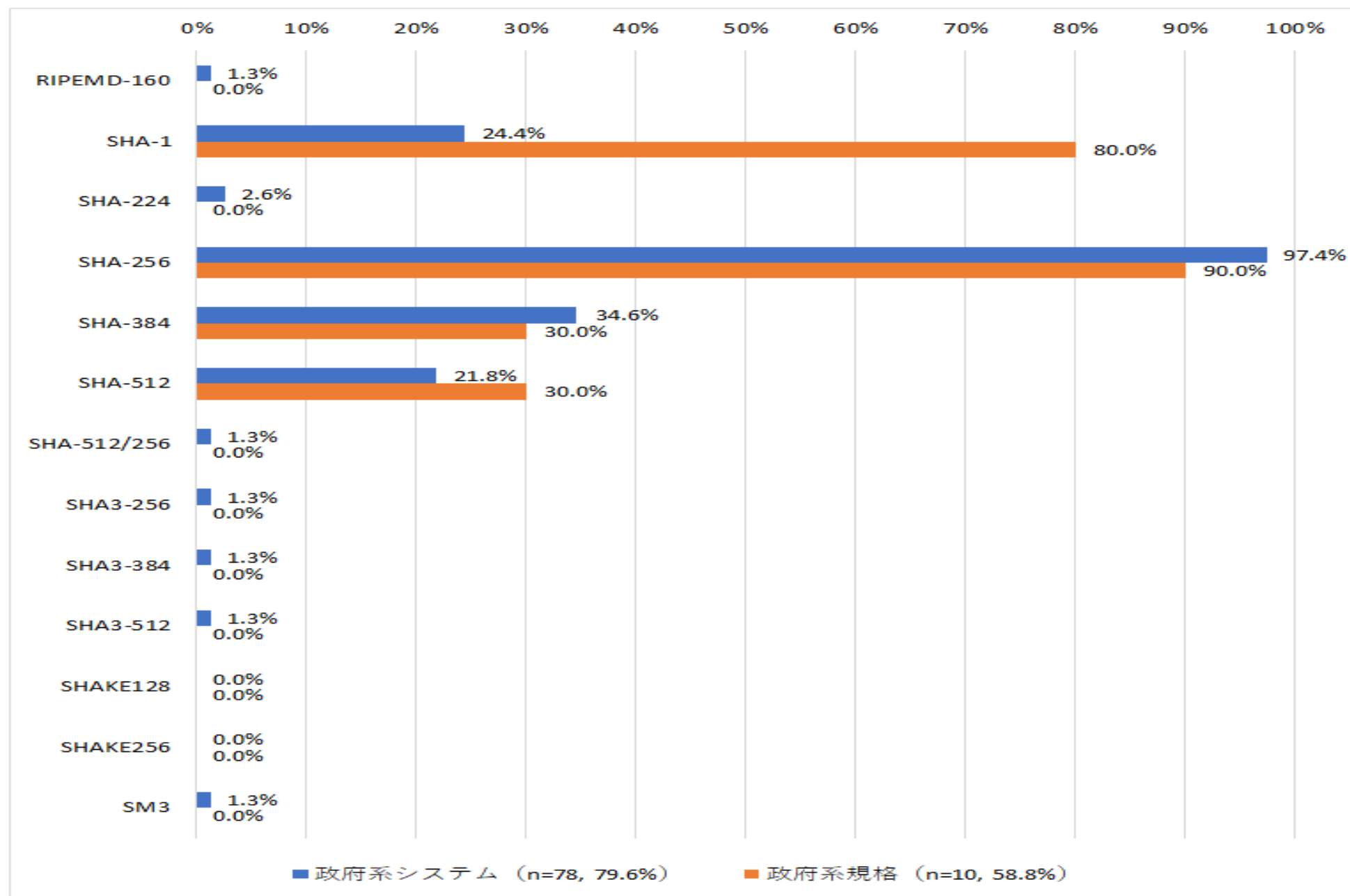
利用実績－市販製品（ハッシュ関数）



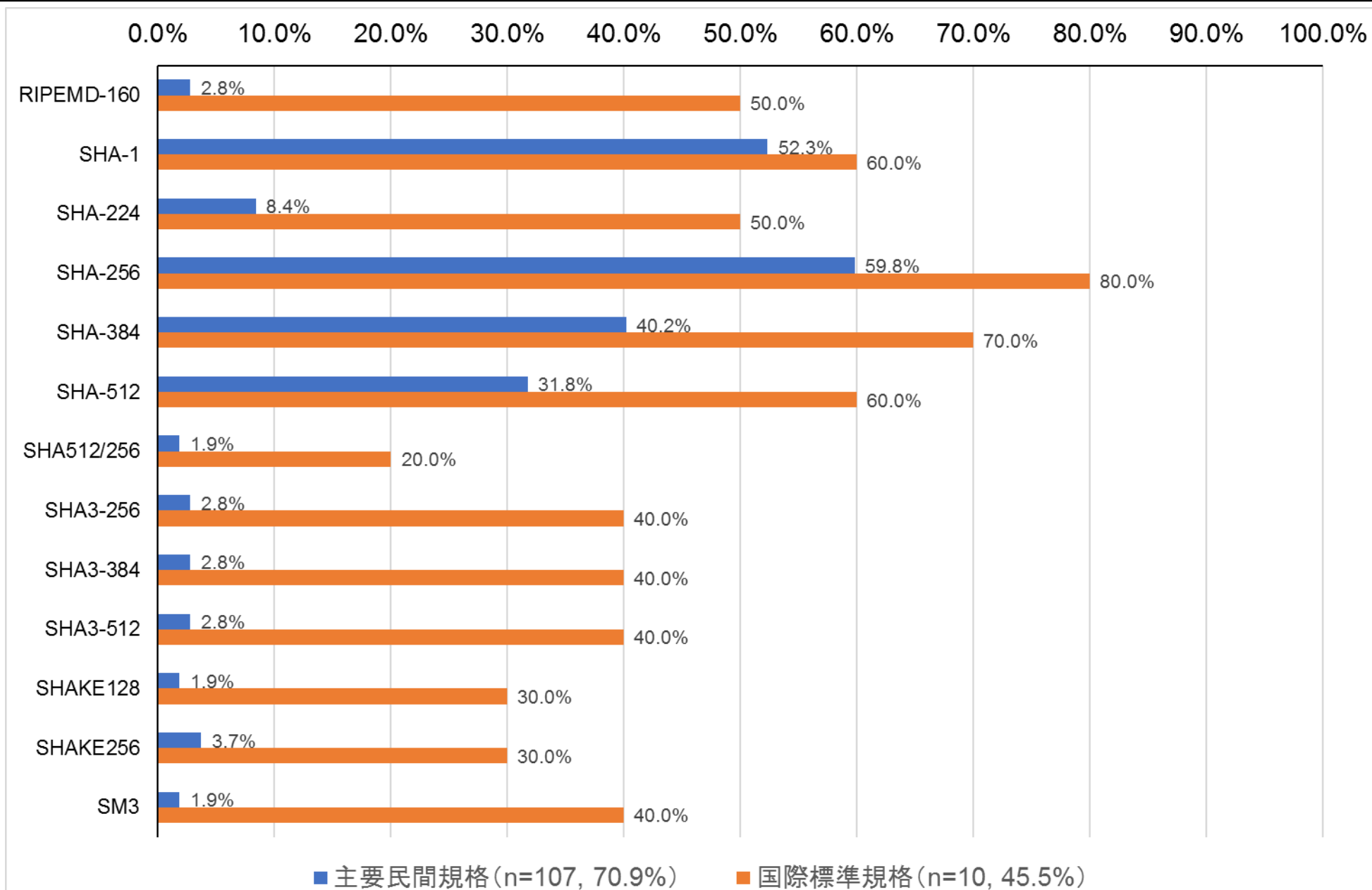
※1集計対象209製品中、ハッシュ関数が154製品で実装（実装率：73.7% = 154/209）

※2ハッシュ関数が実装された154製品に対する各アルゴリズムの実装率（実装率：100% = 154/154）

利用実績－政府系情報システム・規格(ハッシュ関数)

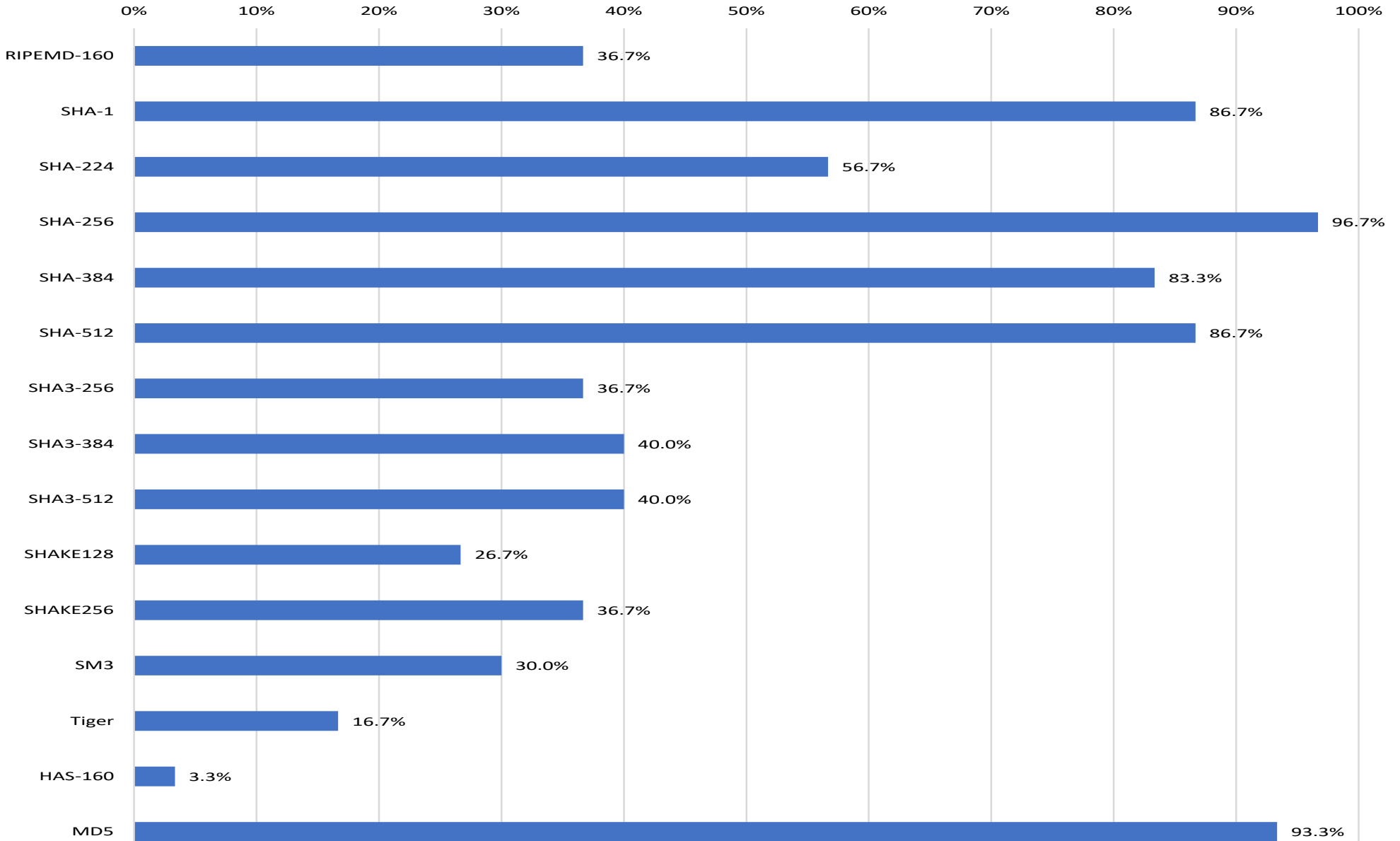


利用実績－標準規格・民間規格(ハッシュ関数)

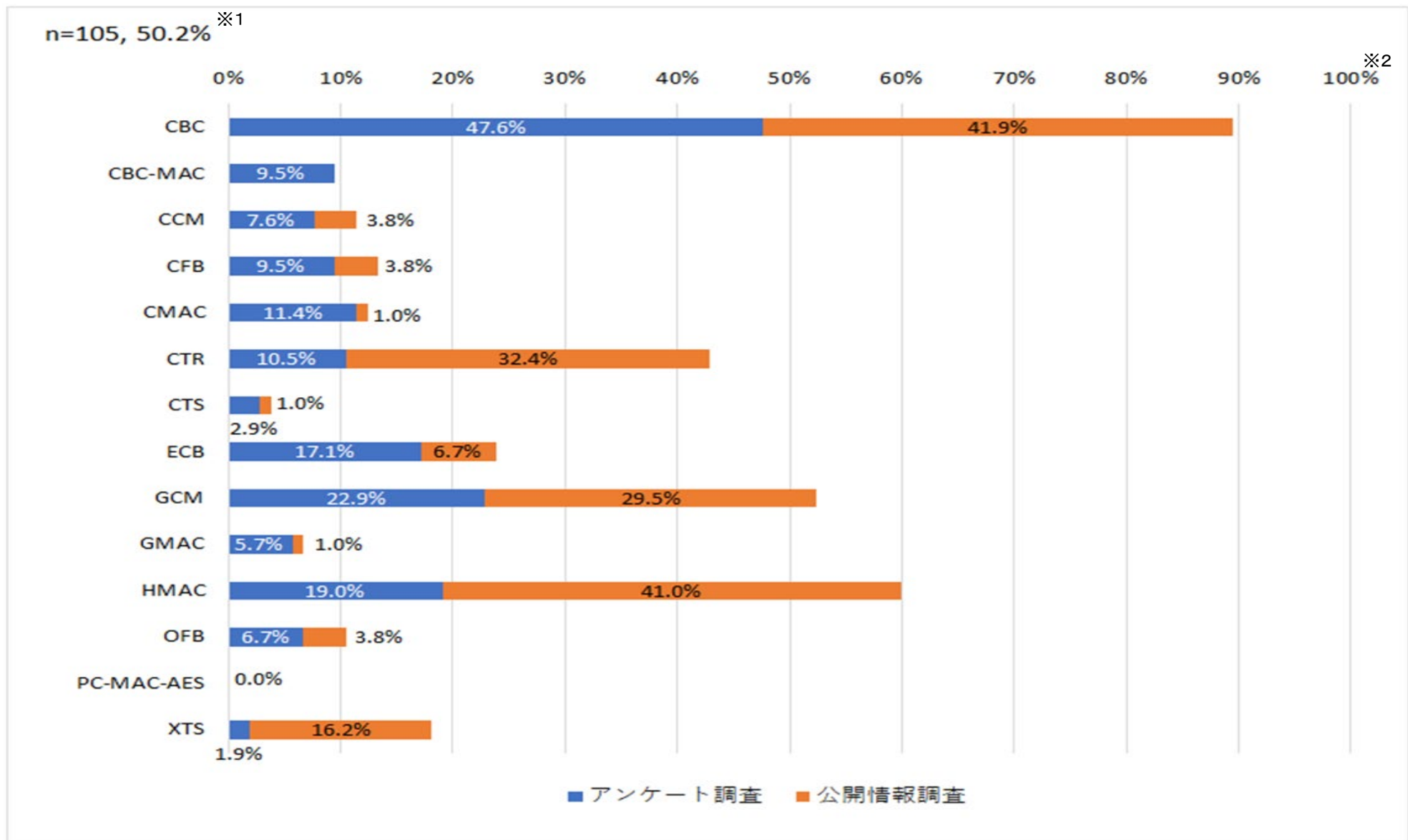


利用実績－オープンソースソフトウェア(ハッシュ関数)

n = 30, 100.0%



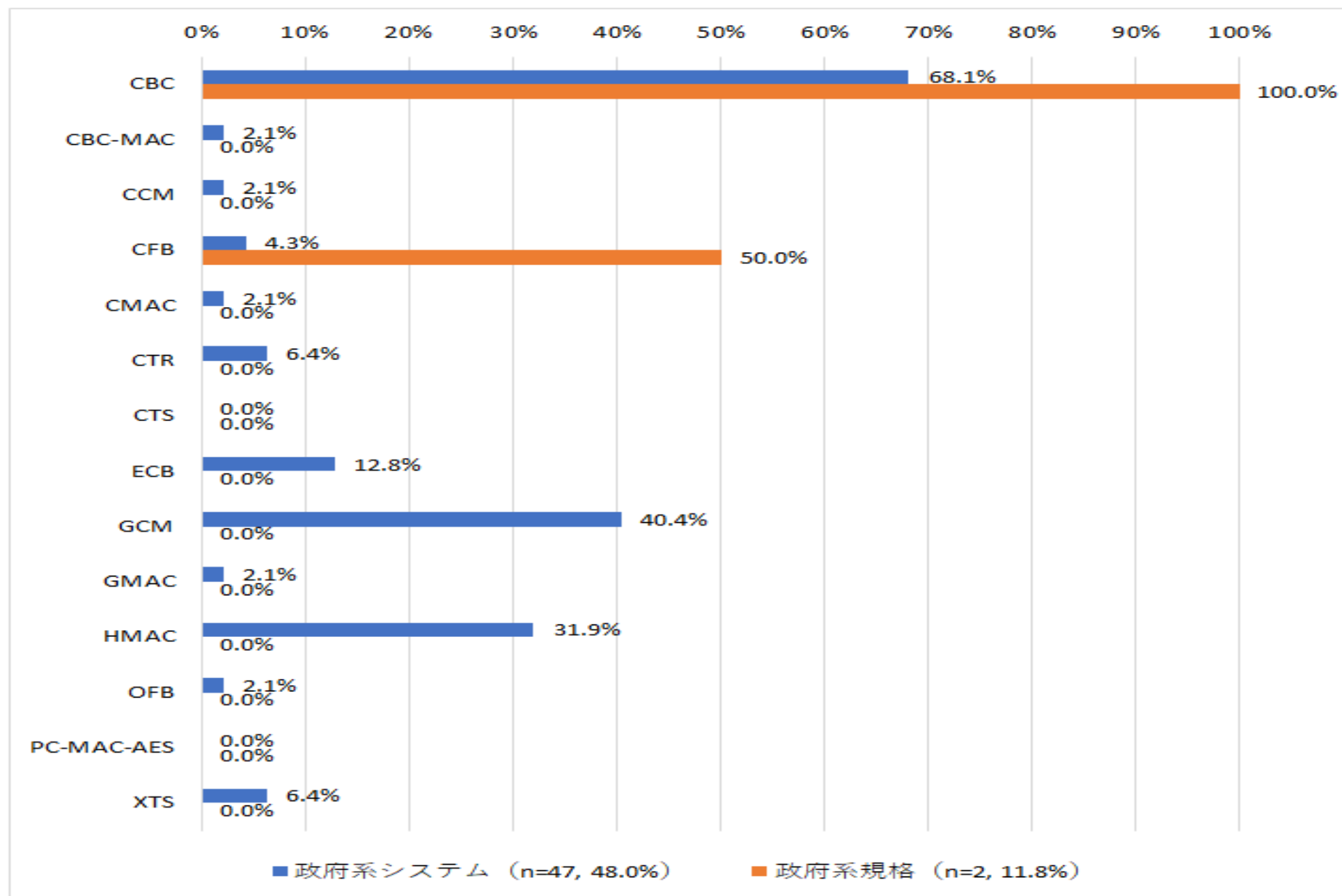
利用実績－市販製品（暗号利用モード／メッセージ認証コード）



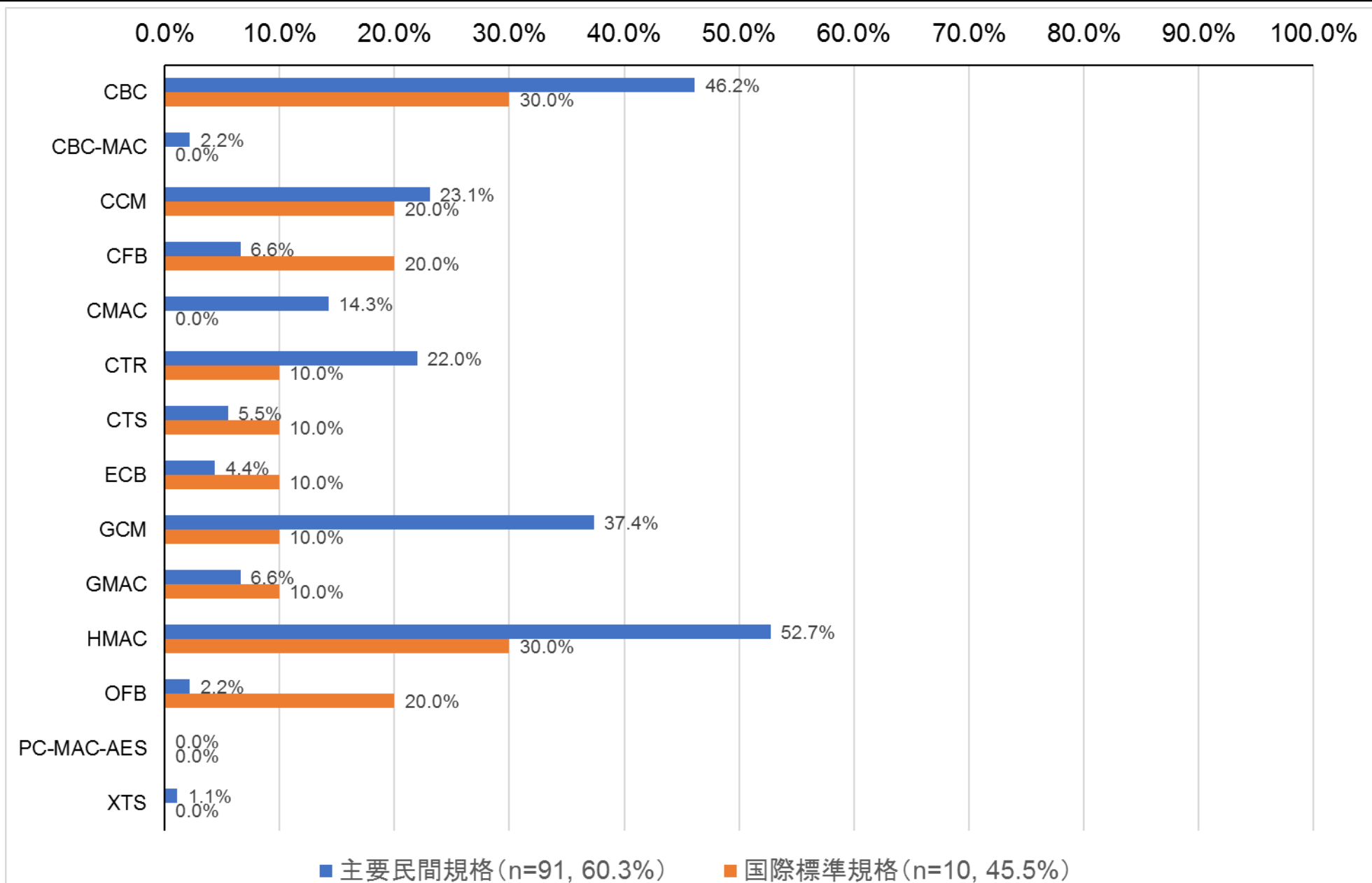
※1 集計対象209製品中、暗号利用モード／MACが105製品で実装（実装率：50.2% = 105/209）

※2 暗号利用モード／MACが実装された105製品に対する各アルゴリズムの実装率（実装率：100% = 105/105） 39

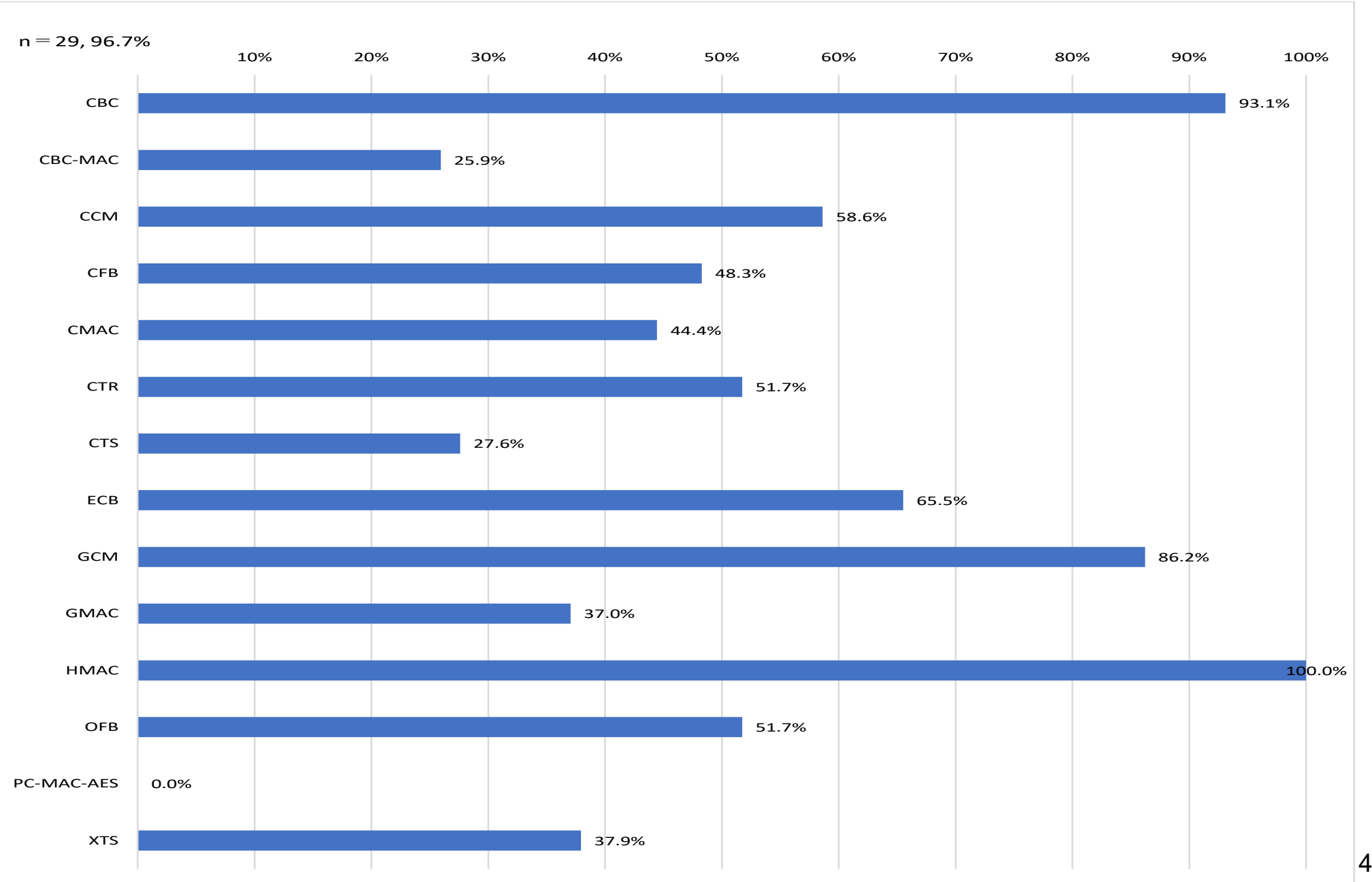
利用実績－政府系情報システム・規格（暗号利用モード／メッセージ認証コード）



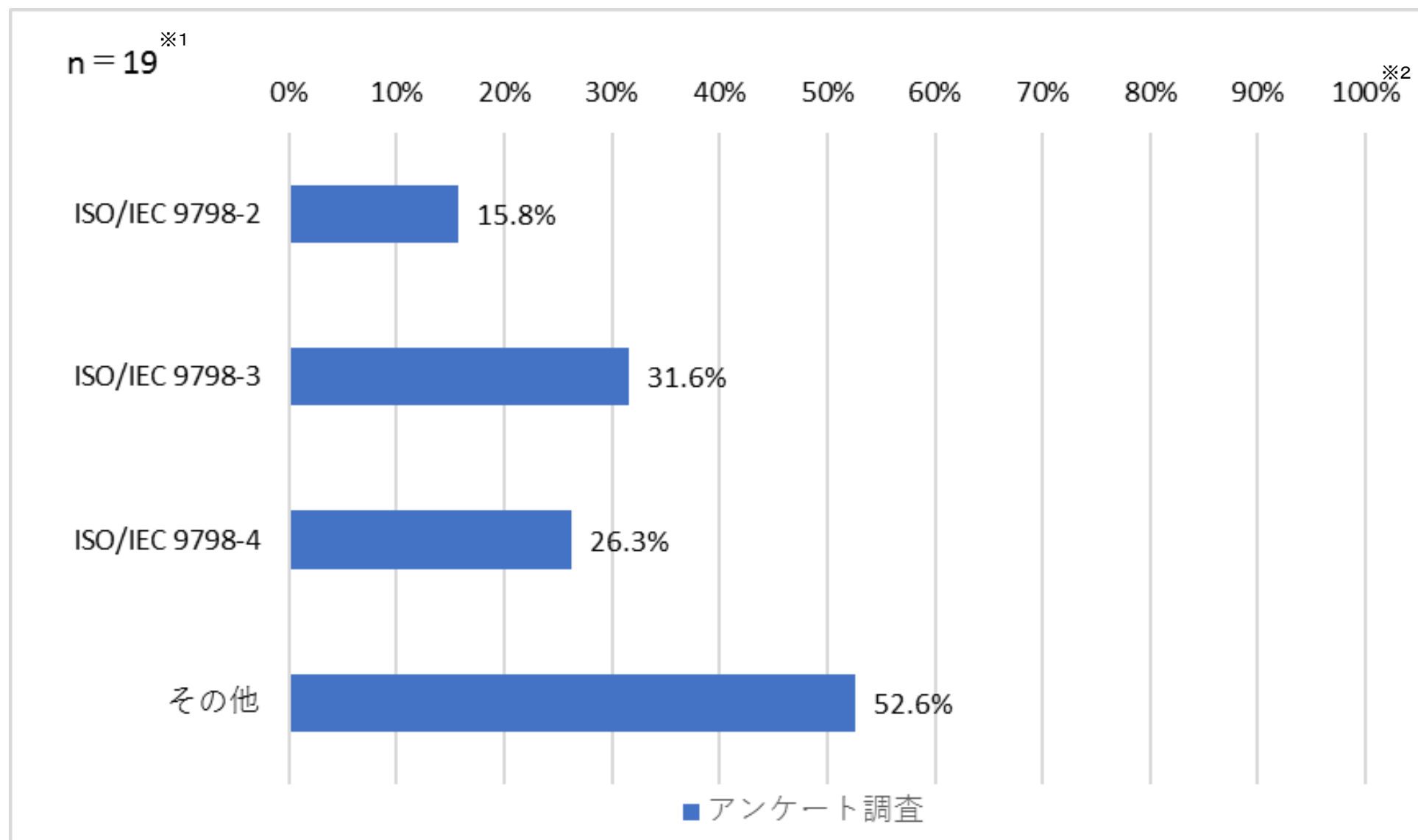
利用実績－標準規格・民間規格(暗号利用モード／メッセージ認証コード)



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



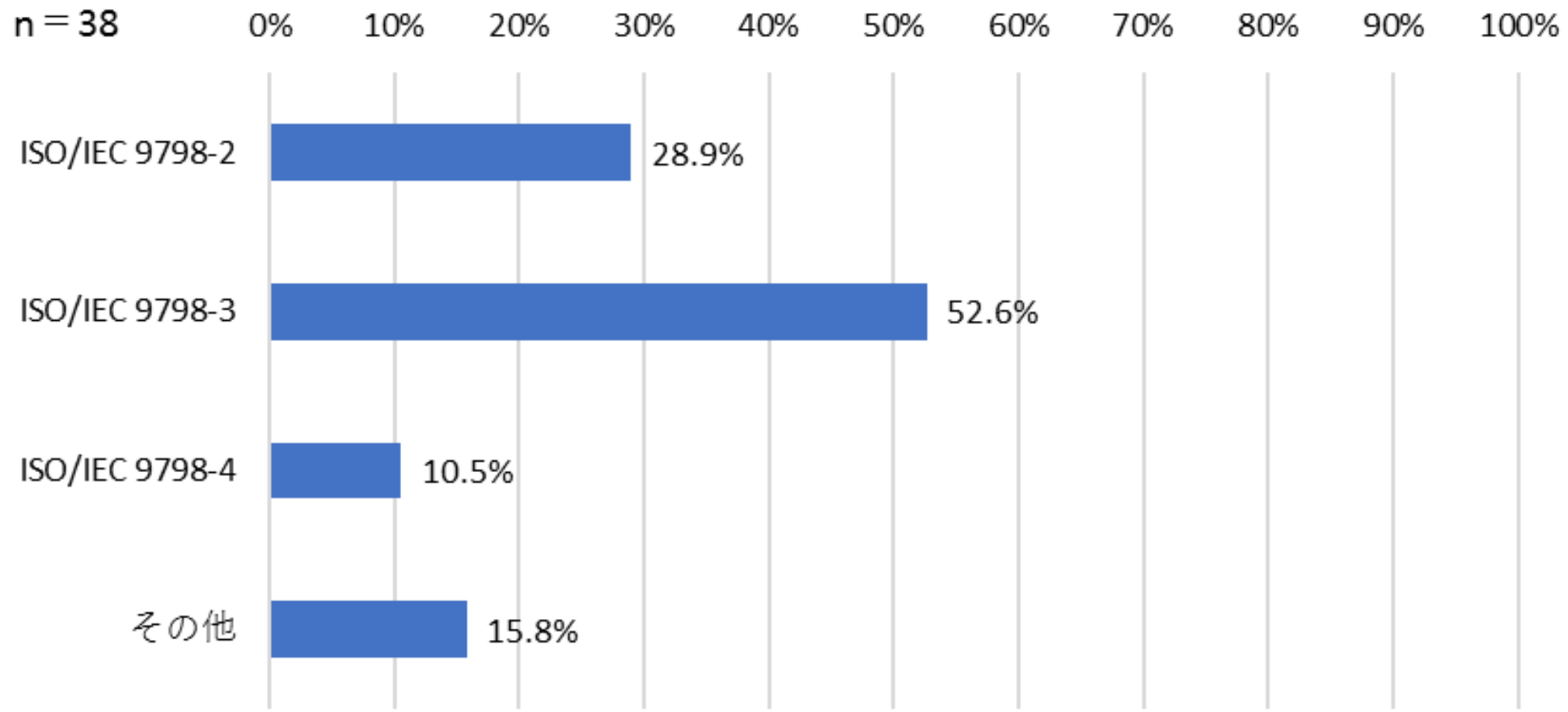
利用実績－市販製品（エンティティ認証）



※1アンケート調査の有効回答中、エンティティ認証が19製品で実装

※2エンティティ認証が実装された19製品に対する各アルゴリズムの実装率（実装率：100% = 19/19）

利用実績－政府系情報システム(エンティティ認証)



最後に

今後、同様の調査を実施する場合、以下の状況を考慮した設計が必要

■ アンケート調査の有効性

10年前に実施した同様の調査と比べて、アンケート調査への協力が得られにくいという厳しい結果。以下の2つの理由が考えられる

(1) 暗号技術に精通する技術者の減少

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

(2) 技術情報を社外に公開する障壁の高さ

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

■ 調査パネルの有効性

暗号技術全般についてのかなり深い知識を必要とする調査をインターネットアンケート調査で行うことは、信頼性の低い回答が多く含まれることが避けられない状況

(1) ポイント目当てのモニターが情報を偽って、調査対象条件に当てはまらないにもかかわらず、アンケート調査に無理に回答しようとする

(2) 正確に回答する意思があつたとしても、知識が不十分であつたり、認識に誤りがあつたりするなどの理由で適切な回答ができなかった可能性

■ 規格やOSSにおけるアルゴリズム名からの判定の難しさ(特にRSA暗号／RSA署名) 表記が統一されておらず、アルゴリズム名からだけでは厳密な判定ができないケースがある