評価A判定結果

資料構成の目次

評価Aの各評価項目における選定基準

【第1回暗号技術検討会にて承認】

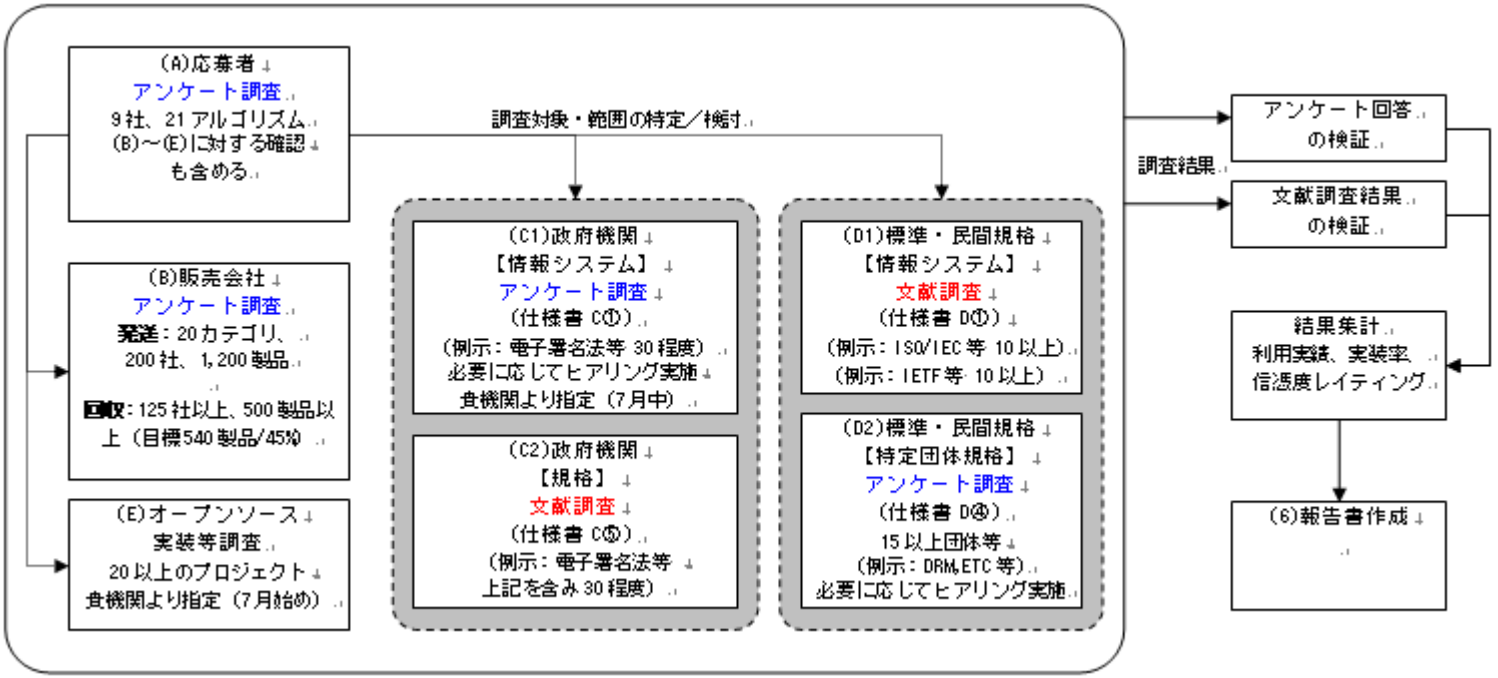
「（評価A）利用実績が十分にある」と判断するための閾値(X)
下記4項目中、**「3項目以上」**の選定基準を満たす

市販製品での採用実績	**「提案会社・グループ会社以外での採用実績」があり**、**「採用割合として50%以上」**の採用実績があること
オープンソースプロジェクトでの採用実績	**「採用割合として50%以上」**のオープンソースプロジェクトでの採用実績がある ※正式版（リリース版）に採用済みのものだけを取り上げる
政府系システム規格での採用実績	**「採用割合として50%以上」**の政府系システム規格での採用実績がある ※規格化への採用が合意された段階のものまで含める（最終承認待ち）
国際的な民間規格での採用実績	**「採用割合として50%以上」**の国際的な民間規格での採用実績がある ※規格化への採用が合意された段階のものまで含める（最終承認待ち）

⇨ IPAが実施した「暗号アルゴリズムの利用実績に関する調査」の調査結果に基づき、判定を行う

判定根拠データ ー 調査方法の俯瞰（1）

- IPAが実施した「暗号アルゴリズムの利用実績に関する調査」
  - 調査A：応募者に対するアンケート調査
  - 調査B：市販製品メーカー・販売会社等に対するアンケート調査
  - 調査C：政府系システム・規格に対する調査
  - 調査D：国際標準規格・国際的民間規格・特定団体規格に対するアンケート調査・公開情報調査
  - 調査E：オープンソースプロジェクトに関する調査



判定根拠データ ー 調査方法の俯瞰(2)

- 調査A
  - 全応募者(9社)よりアンケート回答を回収
  - 応募暗号以外の利用実績が特定できた情報は調査B～Eの有効回答にカウント、応募暗号以外の利用実績が特定できなかった情報は参考扱い
- 調査B
  - 暗号運用委員会が指定した製品カテゴリ(20個)を考慮し、調査対象を決定
  - 市販製品に関するアンケート調査(アンケート配布社数:1849; 有効回答:会社数127, 製品数443)
  - 公開情報を基にみずほ情報総研が調査(調査対象:会社数35, 製品数90)
  - それらのうち、何らかの手段で回答内容の検証が可能な担保がある信頼度(Lev1～Lev3)の情報のみを活用(総数:469)

Lev1	公開情報等により回答内容が確認できたもの	351
Lev2	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もの	66
Lev3	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もの	52
Lev4	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もの	20
Lev5	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もの	44

判定根拠データ ― 調査方法の俯瞰（3）

- 調査C
  - アンケート回答内容については当該府省庁の情報システム課が検証
  - システム利用実績：8府省庁77システム
  - 政府系規格：5規格＋公開情報を基にみずほ情報総研が調査（7規格）
- 調査D
  - 公開情報を基にみずほ情報総研が調査（調査数：国際標準規格12、国際的民間規格108（15種類））
  - 特定団体規格に対してはアンケート調査（有効回答数：16（3団体））＋公開情報を基にみずほ情報総研が調査（調査数：8（6団体））
- 調査E
  - 暗号運用委員会が指定されたオープンソースプロジェクトの最新安定版について、みずほ情報総研が調査（調査数：24）
  - 特に依存関係が強いオープンソースプロジェクト（Linux+Debian、Qmail+OpenSSL、Firefox+Thunderbird+NSS）はまとめて集計

評価Aのまとめ（1）

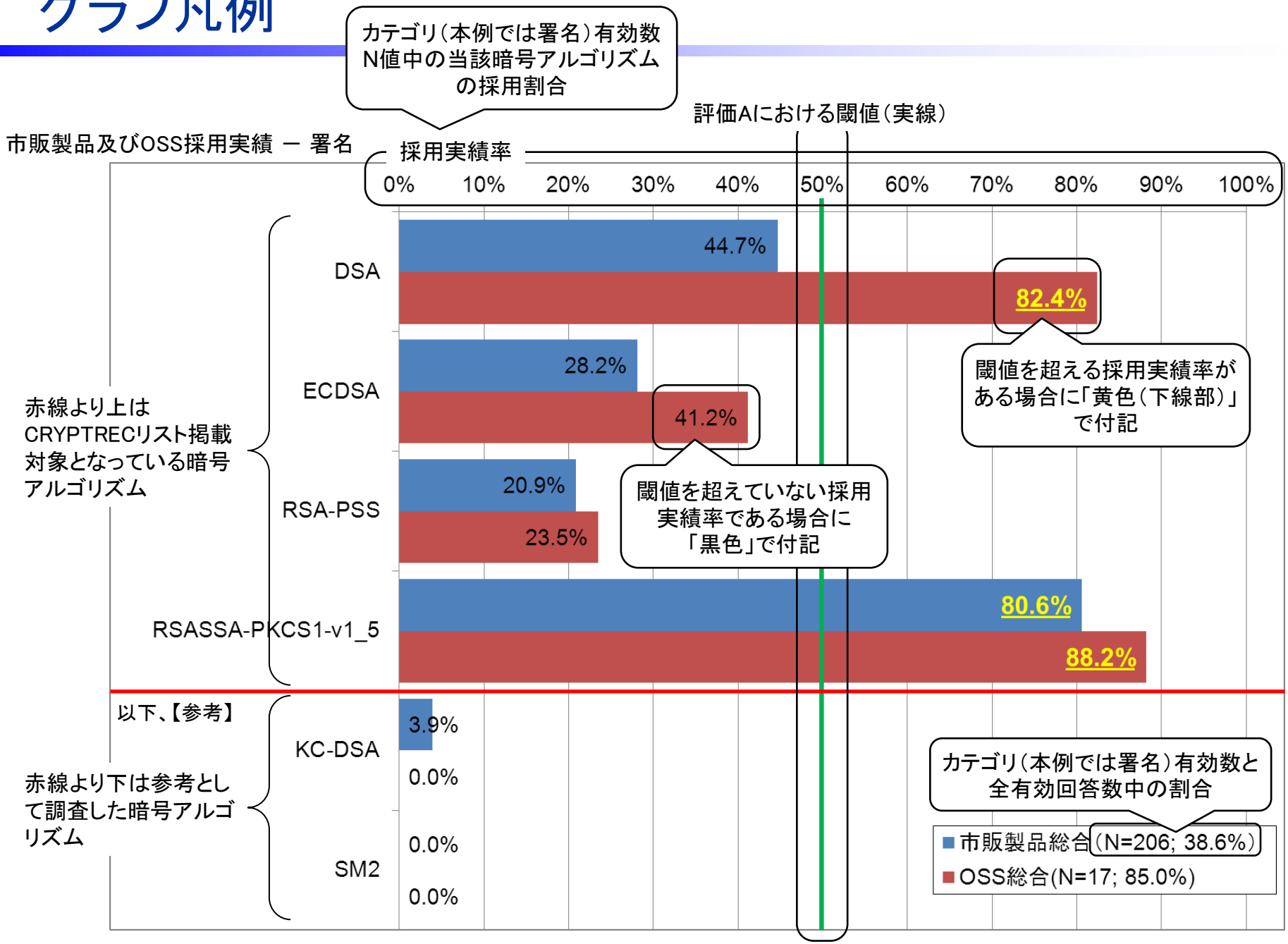
		判定結果		判定根拠データ（P.10～P.18）				判定根拠データ（P.19～P.27）			
				市販製品採用実績		オープンソースプロジェクト採用実績		政府系システム規格採用実績		国際的な民間規格採用実績	
署名	DSA	○	3/4	×	(44.7%)	○	(82.4%)	○	(66.7%)	○	(54.8%)
	ECDSA	×	0/4	×	(28.2%)	×	(41.2%)	×	(22.2%)	×	(35.5%)
	RSA-PSS	×	0/4	×	(20.9%)	×	(23.5%)	×	(11.1%)	×	(16.1%)
	RSASSA-PKCS1-v1_5	○	4/4	○	(80.6%)	○	(88.2%)	○	(100.0%)	○	(74.2%)
守秘・鍵共有	DH	○	4/4	○	(61.5%)	○	(62.5%)	○	(71.4%)	○	(51.3%)
	ECDH	×	0/4	×	(23.9%)	×	(43.8%)	×	(14.3%)	×	(25.6%)
	PSEC-KEM	×	0/4	×	(0.0%)	×	(0.0%)	×	(0.0%)	×	(0.0%)
	RSA-OAEP	×	0/4	×	(19.7%)	×	(25.0%)	×	(0.0%)	×	(28.2%)
64ビットブロック暗号	CIPHERUNICORN-E	×	0/4	×	(2.2%)	×	(0.0%)	×	(0.0%)	×	(0.0%)
	Hierocrypt-L1	×	0/4	×	(2.6%)	×	(0.0%)	×	(0.0%)	×	(0.0%)
	MISTY1	×	0/4	×	(1.5%)	×	(0.0%)	×	(0.0%)	×	(0.0%)
	Triple DES	○	4/4	○	(70.2%)	○	(100.0%)	○	(85.7%)	○	(80.8%)
128ビットブロック暗号	AES	○	4/4	○	(95.4%)	○	(100.0%)	○	(100.0%)	○	(94.2%)
	Camellia	×	0/4	×	(13.7%)	×	(46.7%)	×	(25.0%)	×	(17.3%)
	CIPHERUNICORN-A	×	0/4	×	(1.1%)	×	(0.0%)	×	(0.0%)	×	(0.0%)
	CLEFIA	×	0/4	×	(0.0%)	×	(0.0%)	×	(0.0%)	×	(0.0%)
	Hierocrypt-3	×	0/4	×	(0.5%)	×	(0.0%)	×	(0.0%)	×	(0.0%)
	SC2000	×	0/4	×	(2.2%)	×	(0.0%)	×	(0.0%)	×	(0.0%)

凡例：（判定結果）　○ 評価Aの通過条件を満たしている（総合評価に進む）　× 評価Aの通過条件を満たしていない（評価Bに進む）
（根拠データ）　○ 採用実績が選定基準を満たしている　× 採用実績が選定基準を満たしていない

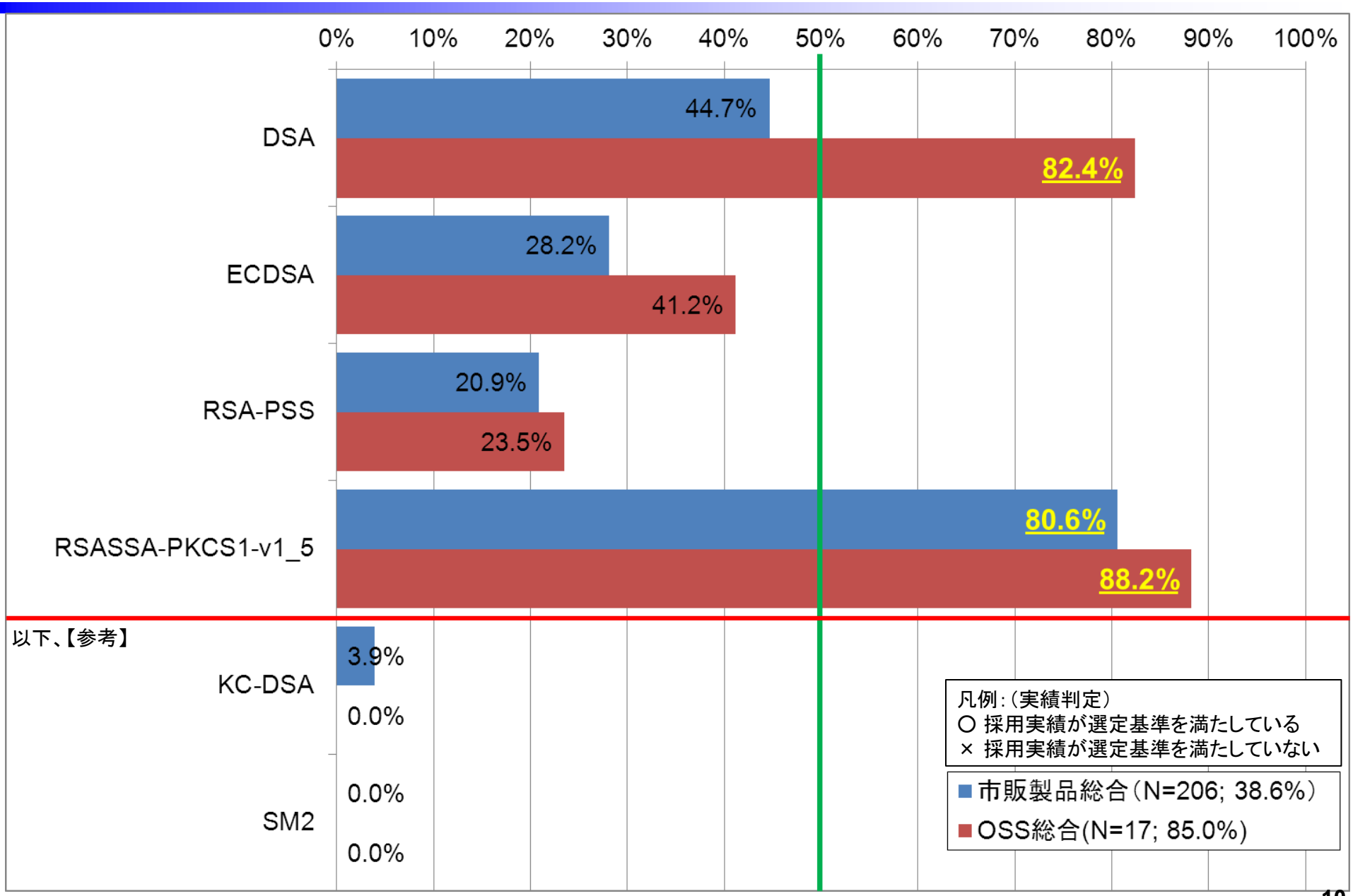
評価Aのまとめ（2）

		判定結果		判定根拠データ（P.10～P.18）				判定根拠データ（P.19～P.27）			
				市販製品採用実績		オープンソースプロジェクト採用実績		政府系システム規格採用実績		国際的な民間規格採用実績	
ストリーム暗号	Enocoro-128v2	×	0/4	×	(0.0%)	×	(0.0%)	×	(0.0%)	×	(0.0%)
	KCipher-2	×	0/4	×	(10.2%)	×	(0.0%)	×	(33.3%)	×	(0.0%)
	MUGI	×	0/4	×	(0.0%)	×	(0.0%)	×	(0.0%)	×	(0.0%)
	MULTI-S01	×	0/4	×	(3.8%)	×	(0.0%)	×	(0.0%)	×	(0.0%)
ハッシュ関数	SHA-256	×	2/4	○	(61.7%)	○	(77.8%)	×	(36.4%)	×	(43.4%)
	SHA-384	×	1/4	×	(34.7%)	○	(66.7%)	×	(18.2%)	×	(37.7%)
	SHA-512	×	1/4	×	(37.6%)	○	(66.7%)	×	(18.2%)	×	(22.6%)
暗号利用モード（秘匿）	CBC	○	4/4	○	(82.7%)	○	(100.0%)	○	(100.0%)	○	(84.0%)
	CFB	×	1/4	×	(20.5%)	○	(52.9%)	×	(0.0%)	×	(16.0%)
	CTR	×	0/4	×	(23.7%)	×	(35.3%)	×	(0.0%)	×	(34.0%)
	OFB	×	0/4	×	(17.3%)	×	(47.1%)	×	(16.7%)	×	(16.0%)
暗号利用モード（認証付秘匿）	CCM	×	0/4	×	(9.6%)	×	(23.5%)	×	(0.0%)	×	(22.0%)
	GCM	×	0/4	×	(11.5%)	×	(29.4%)	×	(0.0%)	×	(32.0%)
メッセージ認証コード	CMAC	×	1/4	×	(7.5%)	×	(33.3%)	○	(50.0%)	×	(12.8%)
	HMAC	○	4/4	○	(82.1%)	○	(100.0%)	○	(50.0%)	○	(87.2%)
	PC-MAC-AES	×	0/4	×	(0.0%)	×	(0.0%)	×	(0.0%)	×	(0.0%)
エンティティ認証	ISO/IEC9798-2	×	0/4	×	(24.6%)	ー	該当なし	×	(0.0%)	ー	該当なし
	ISO/IEC9798-3	×	1/4	×	(10.1%)	ー	該当なし	○	(100.0%)	ー	該当なし
	ISO/IEC9798-4	×	0/4	×	(1.4%)	ー	該当なし	×	(0.0%)	ー	該当なし

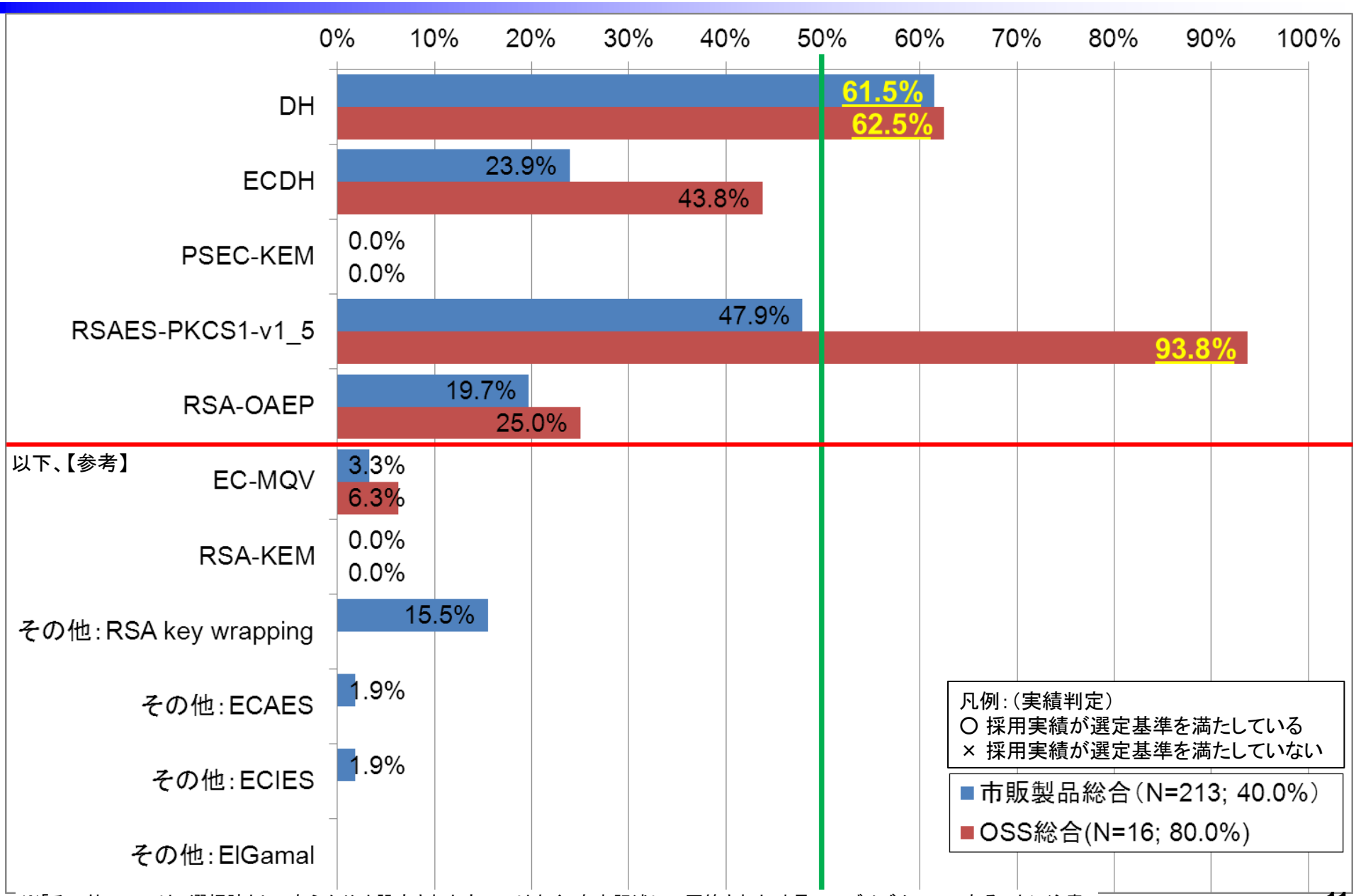
グラフ凡例


カテゴリ（本例では署名）有効数
N値中の当該暗号アルゴリズム
の採用割合
評価Aにおける閾値（実線）
市販製品及びOSS採用実績 ― 署名
採用実績率
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
DSA
44.7%
82.4%
ECDSA
28.2%
41.2%
RSA-PSS
20.9%
23.5%
RSASSA-PKCS1-v1_5
80.6%
88.2%
閾値を超える採用実績率が
ある場合に「黄色（下線部）」
で付記
閾値を超えていない採用
実績率である場合に
「黒色」で付記
赤線より上は
CRYPTRECリスト掲載
対象となっている暗号
アルゴリズム
以下、【参考】
KC-DSA
3.9%
0.0%
SM2
0.0%
0.0%
赤線より下は参考とし
て調査した暗号アルゴ
リズム
カテゴリ（本例では署名）有効数と
全有効回答数中の割合
市販製品総合（N=206; 38.6%）
OSS総合(N=17; 85.0%)

市販製品及びOSS採用実績 ― 署名

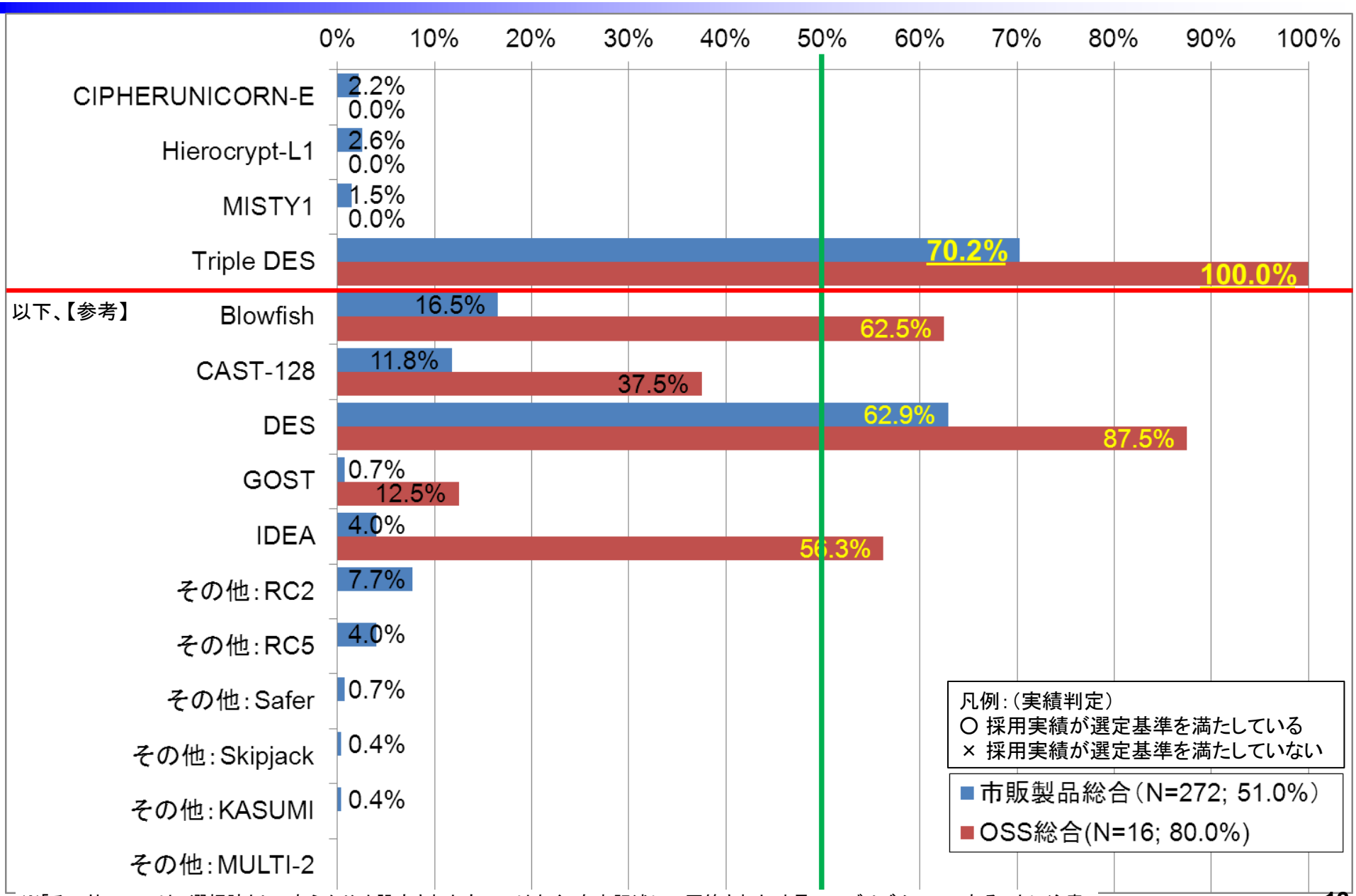


市販製品及びOSS採用実績 ― 守秘・鍵共有



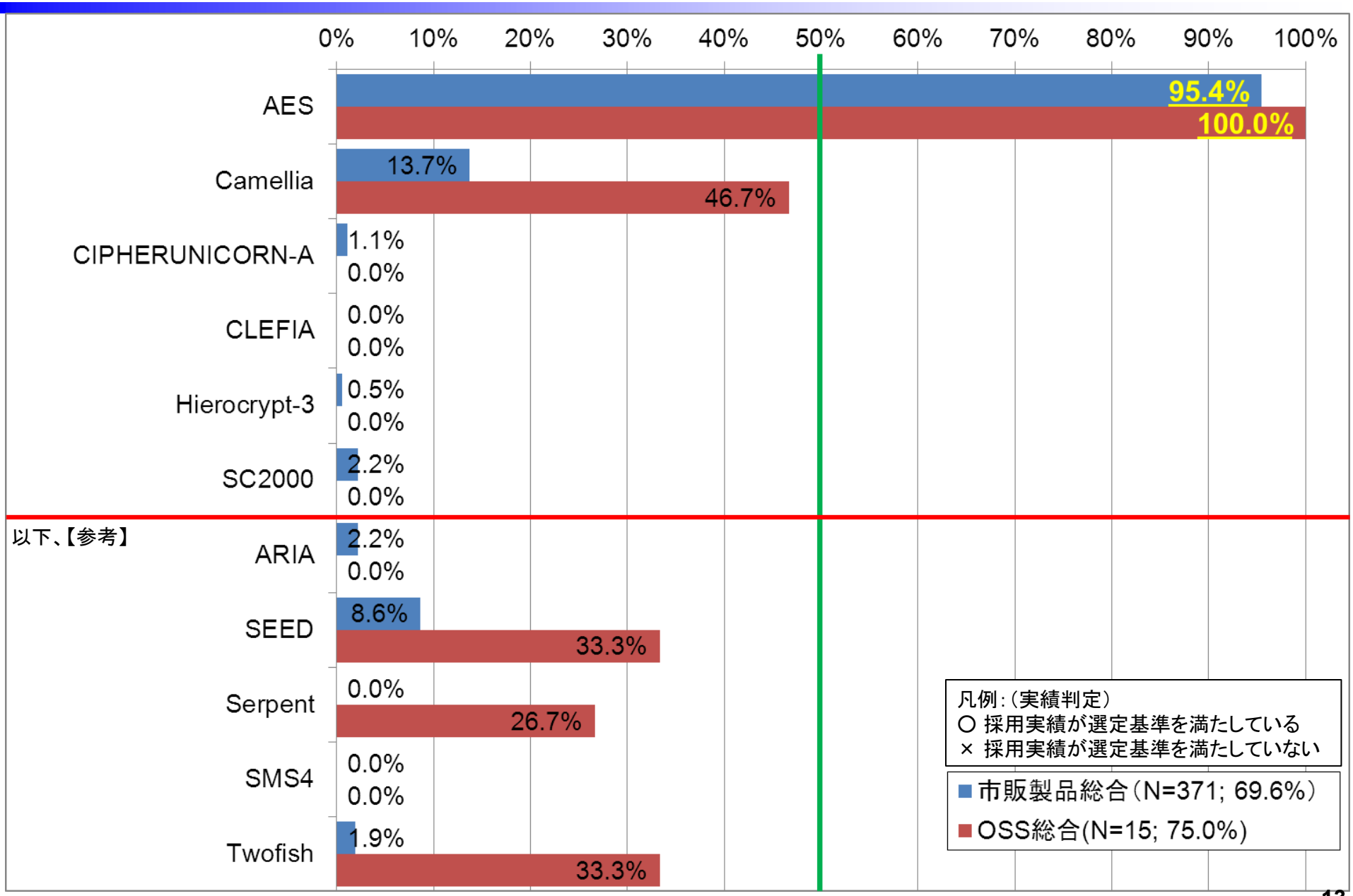
※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答された暗号アルゴリズムXXXであることに注意

市販製品及びOSS採用実績 ― 64ビットブロック暗号

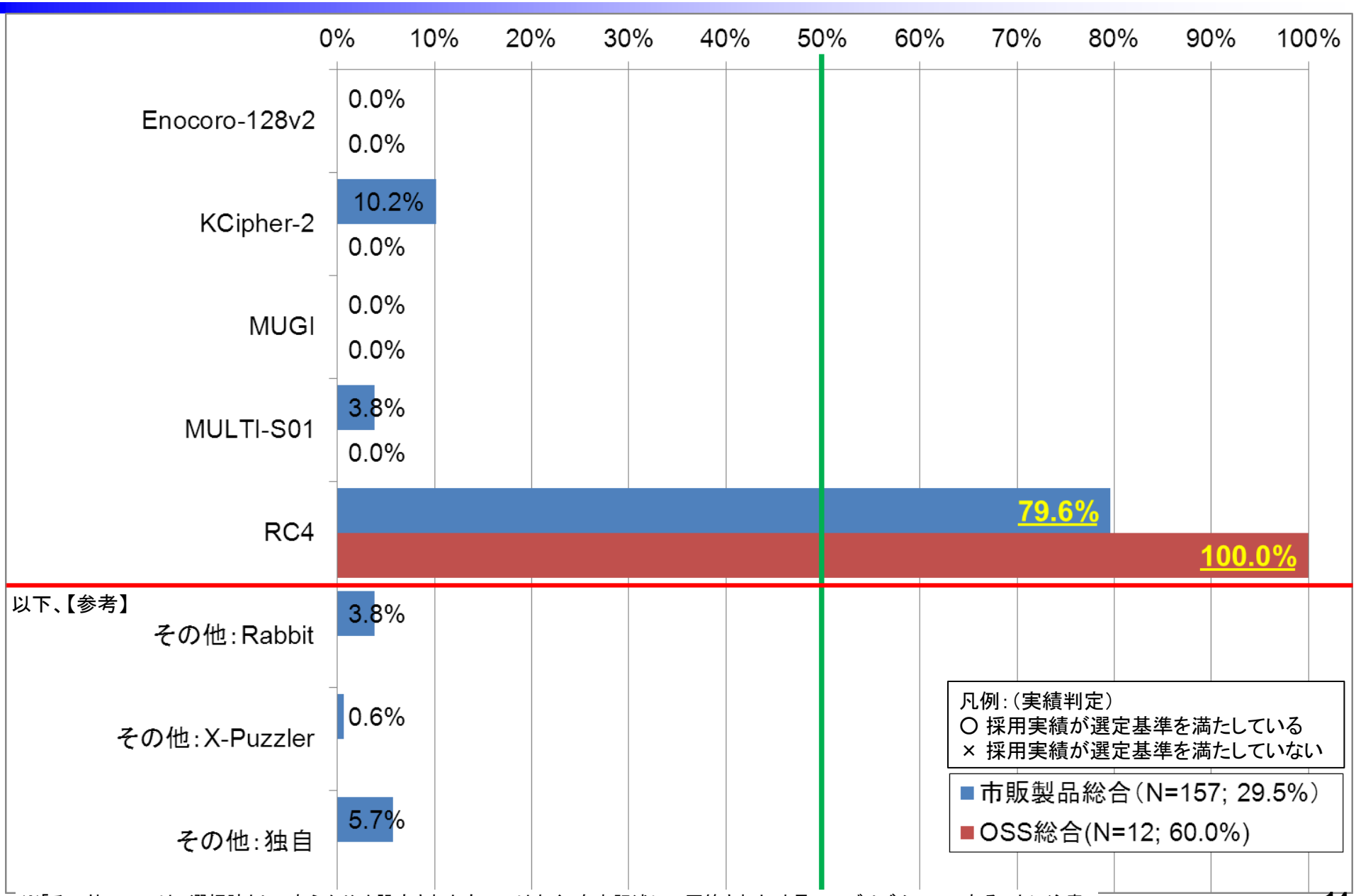


※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答された暗号アルゴリズムXXXであることに注意

市販製品及びOSS採用実績 ― 128ビットブロック暗号

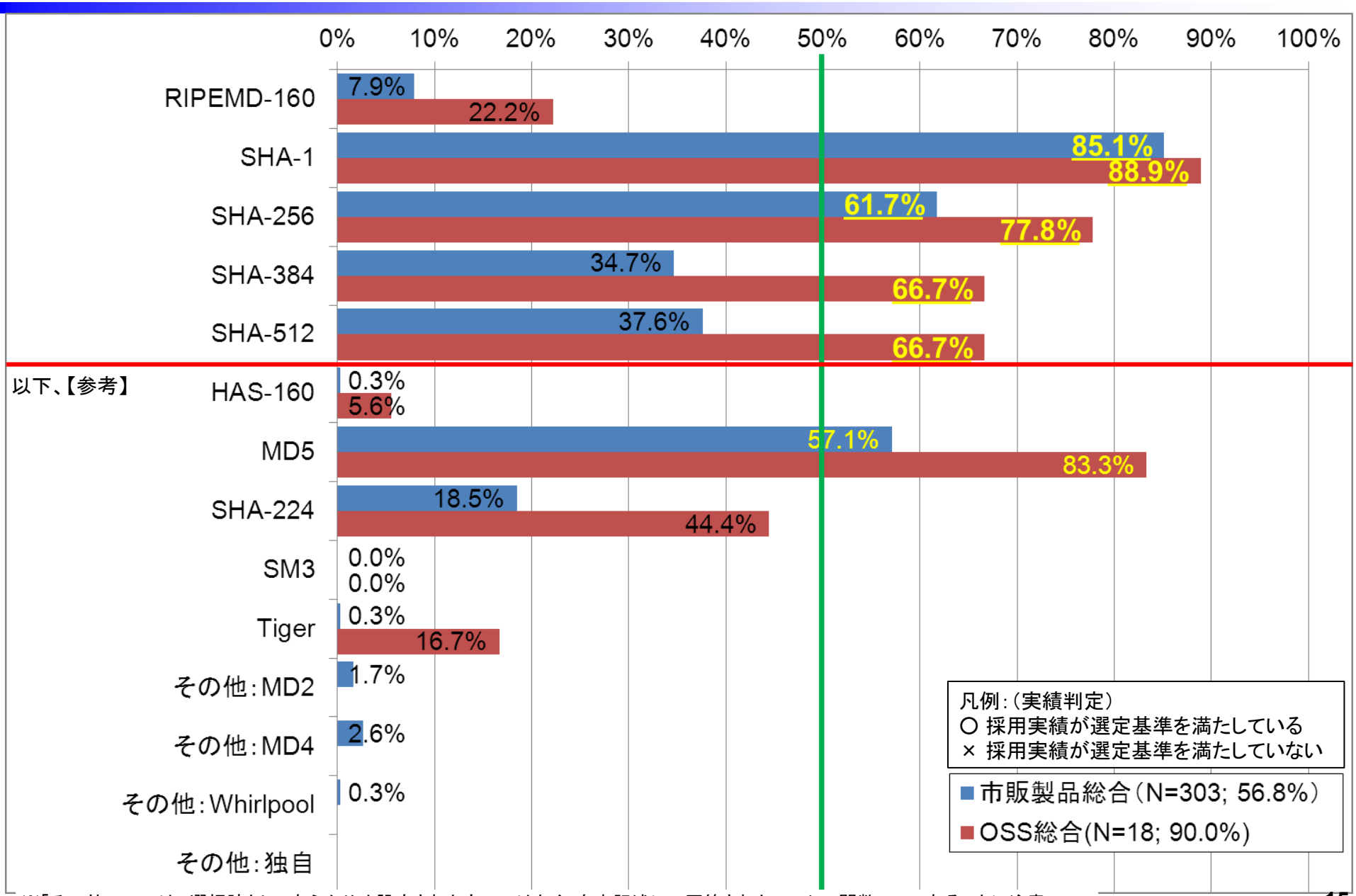


市販製品及びOSS採用実績 ― ストリーム暗号



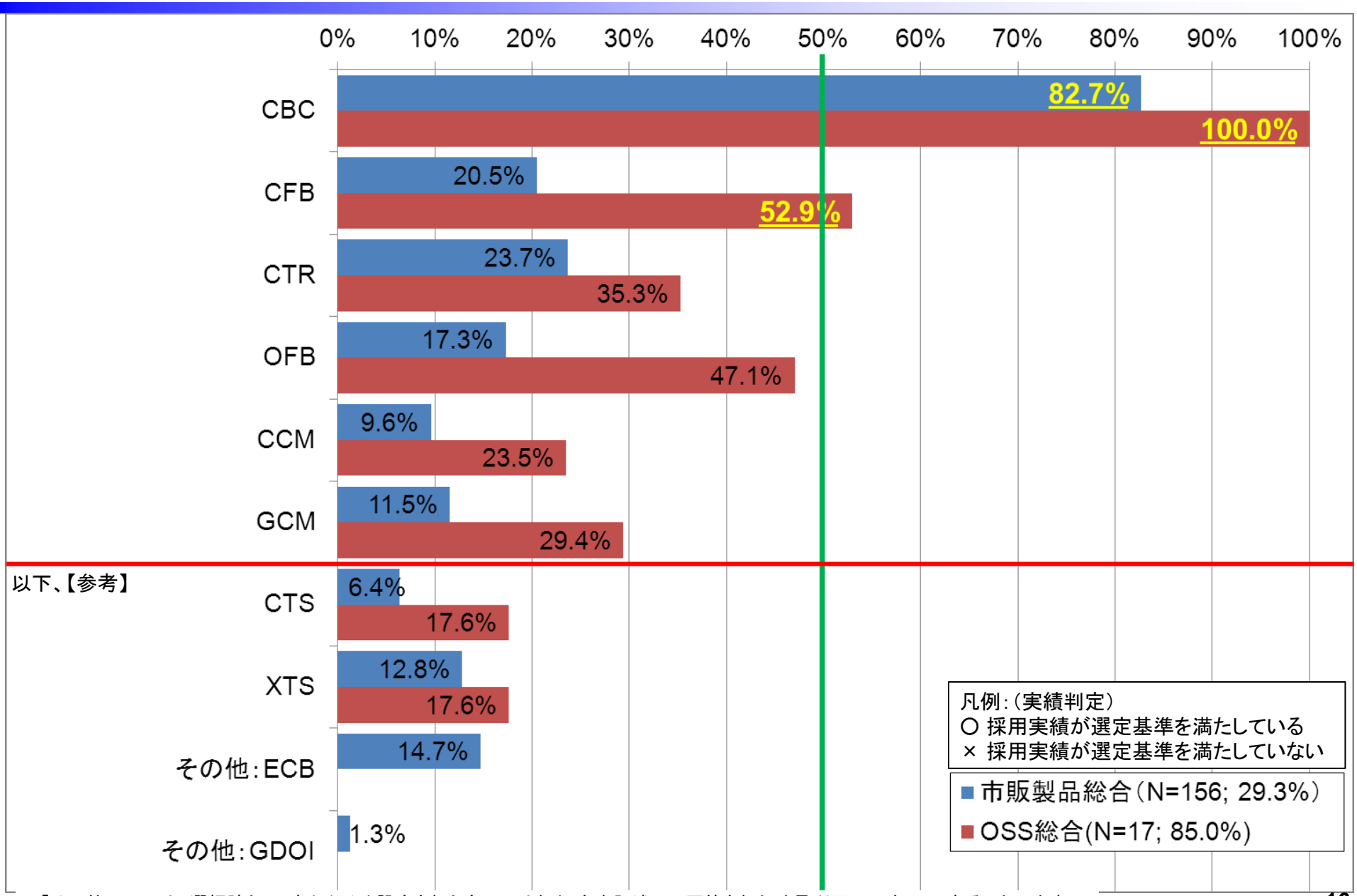
※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答された暗号アルゴリズムXXXであることに注意

市販製品及びOSS採用実績 ー ハッシュ関数



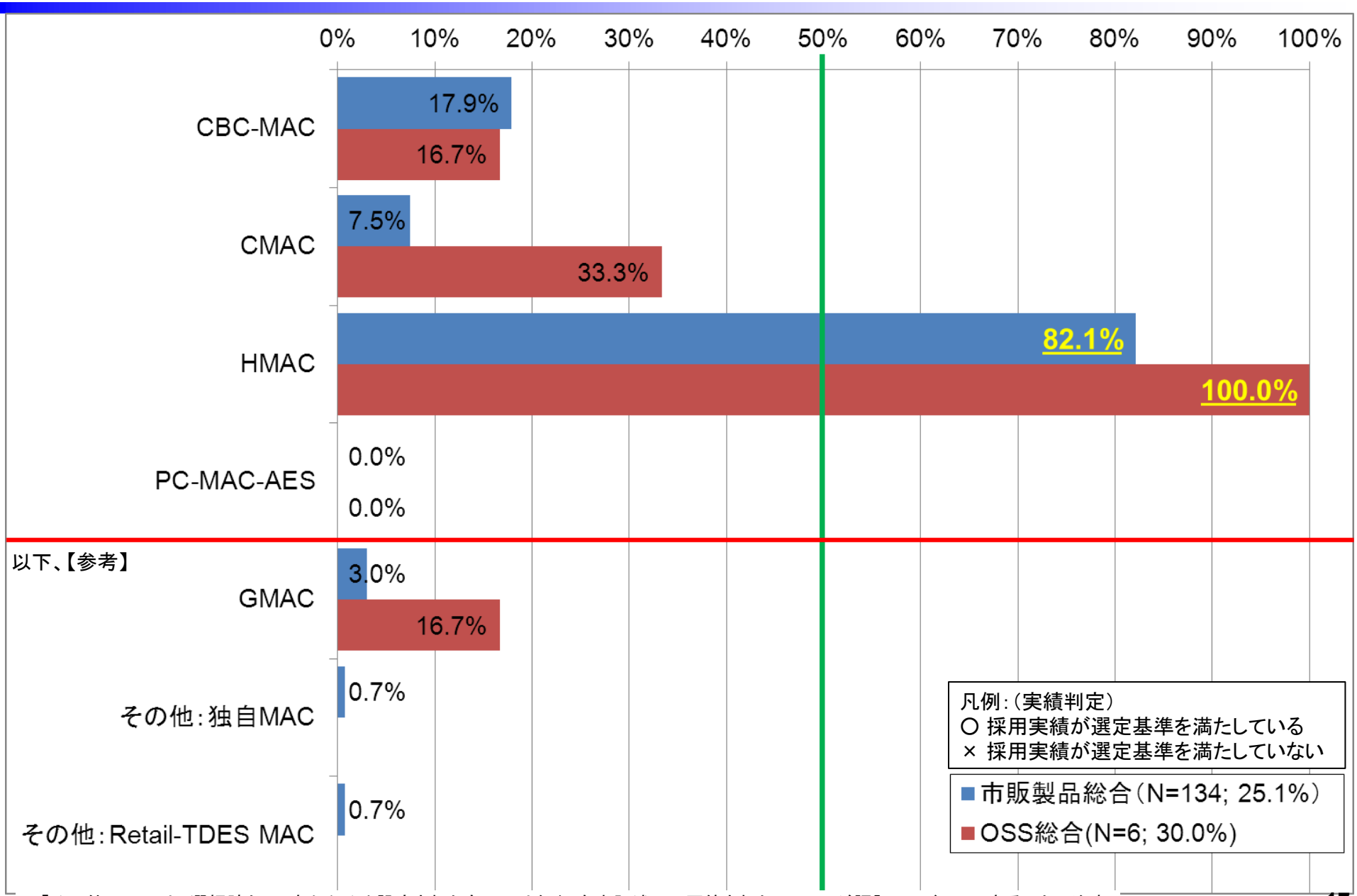
※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答されたハッシュ関数XXXであることに注意

市販製品及びOSS採用実績 ー 暗号利用モード



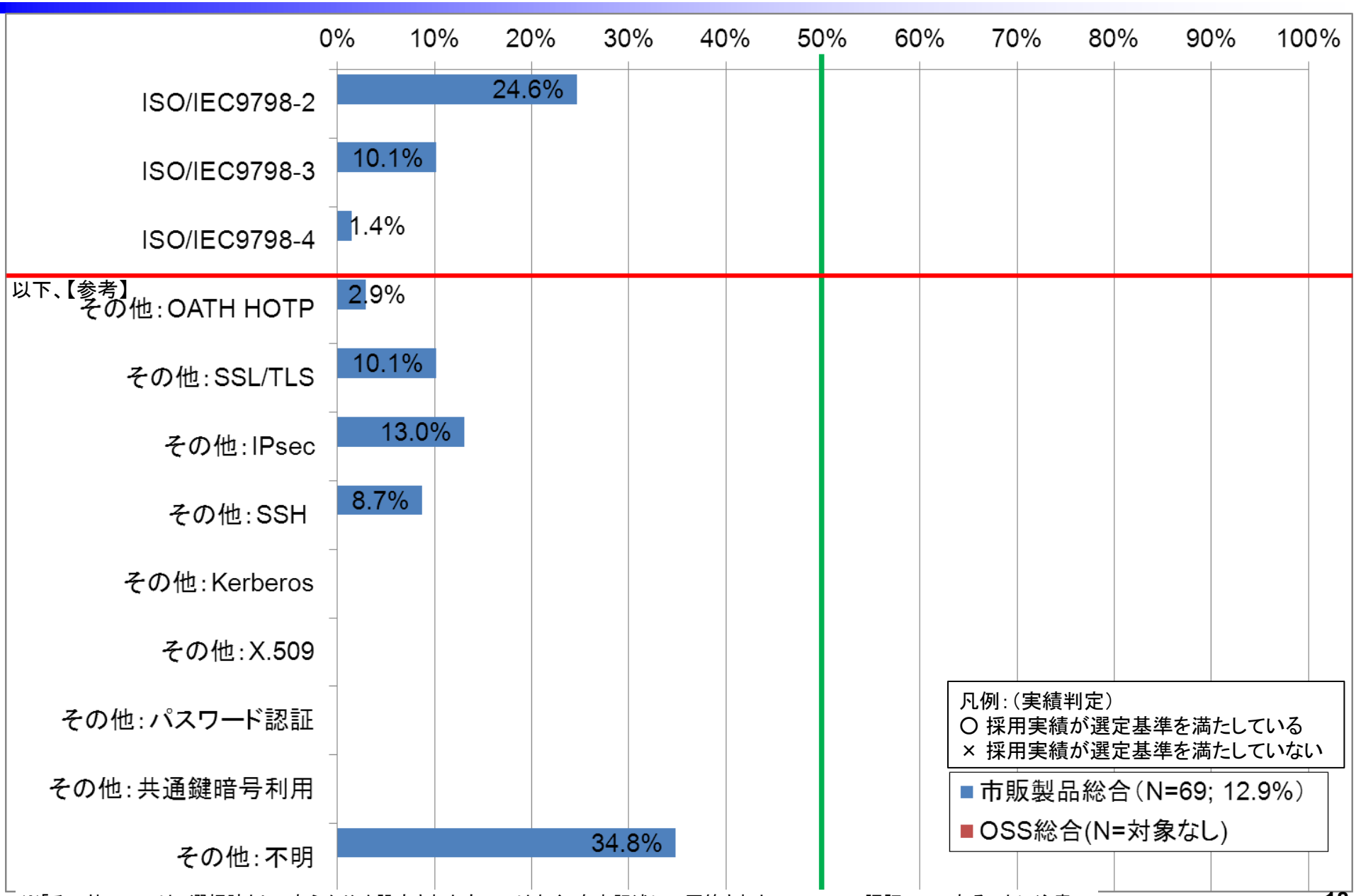
※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答された暗号利用モードXXXであることに注意

市販製品及びOSS採用実績 ― メッセージ認証コード



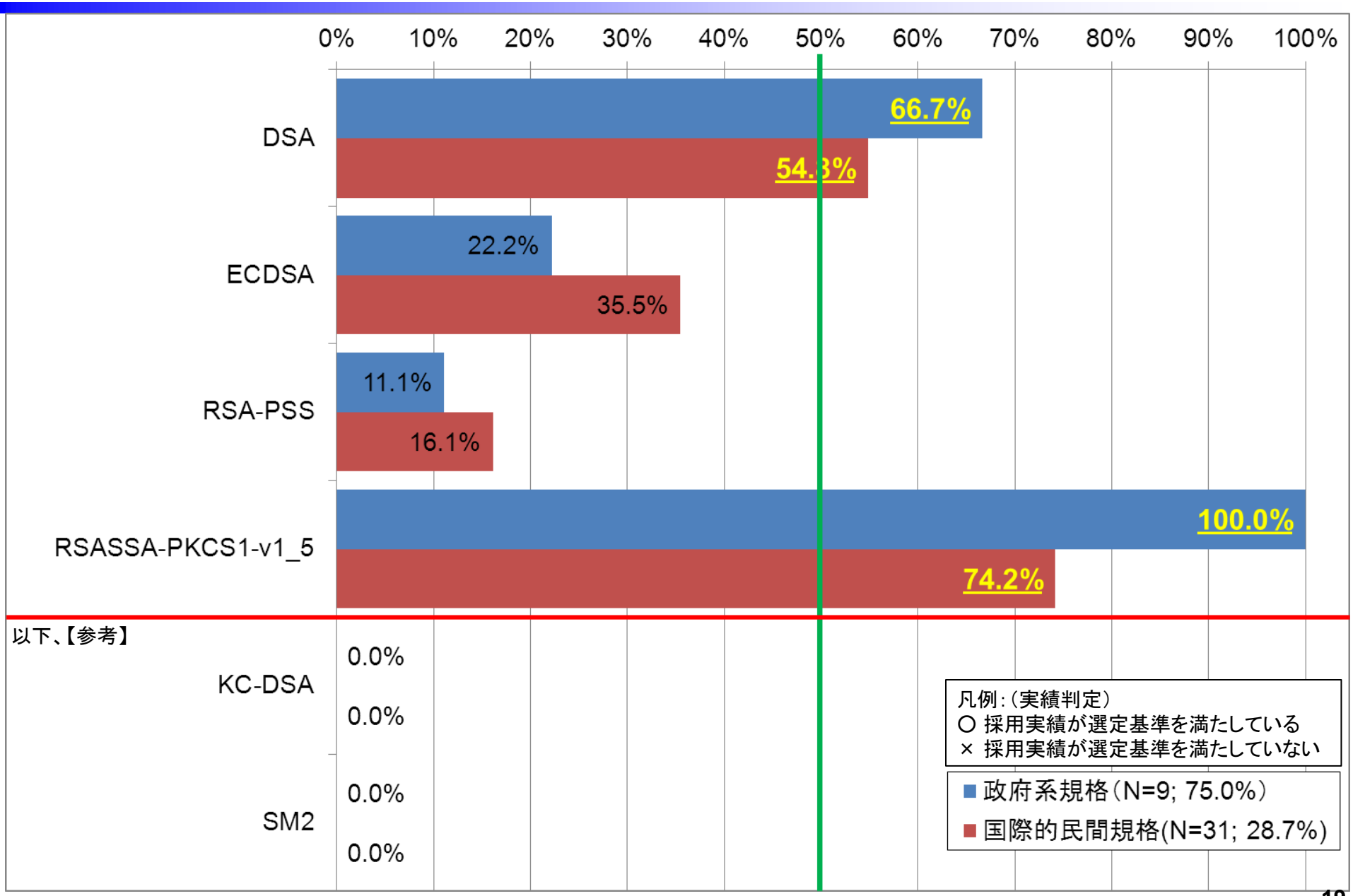
※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答されたメッセージ認証コードXXXであることに注意

市販製品及びOSS採用実績 ― エンティティ認証

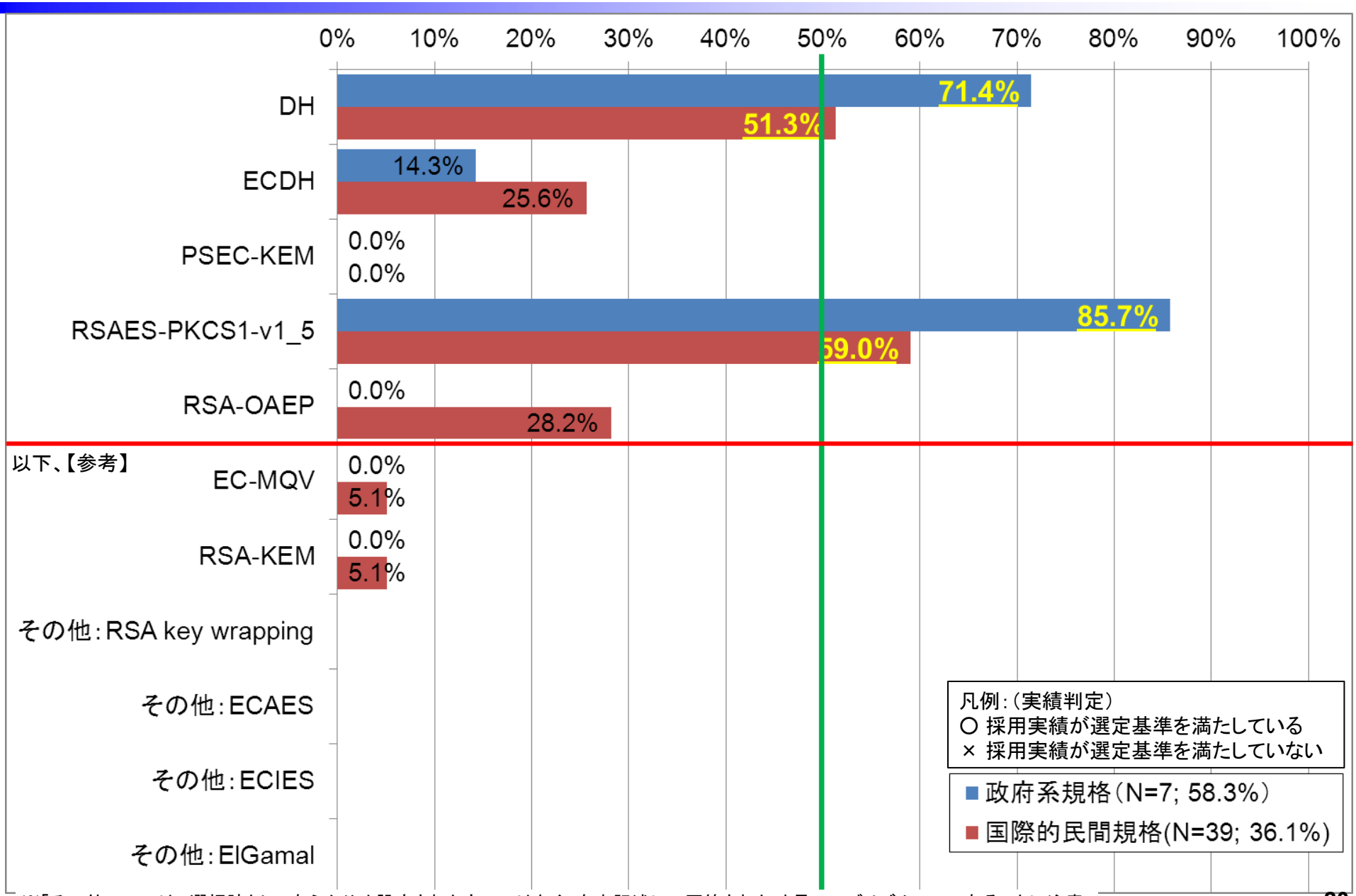


※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答されたエンティティ認証XXXであることに注意

政府及び国際的民間規格採用実績 ― 署名

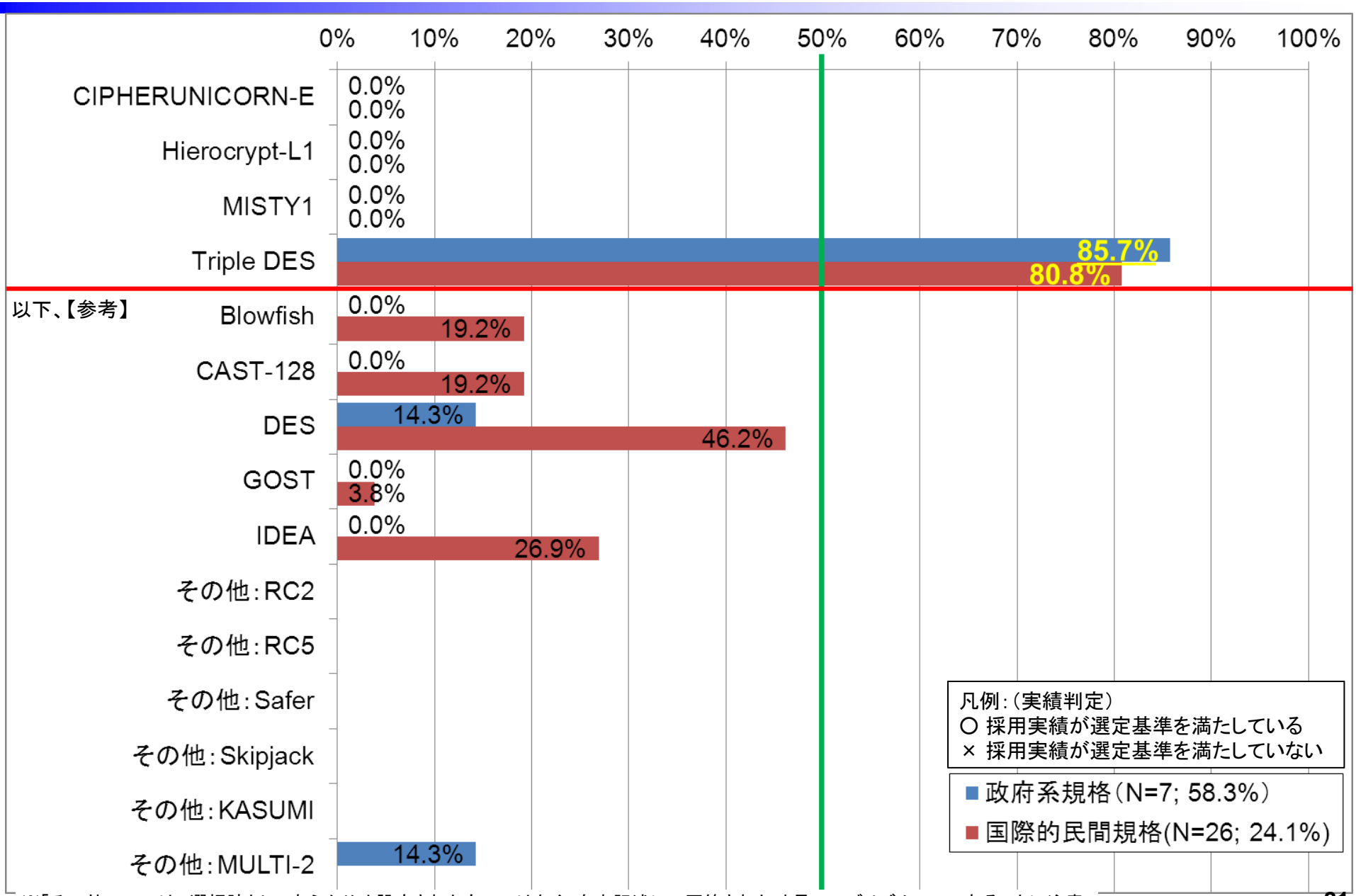


政府及び国際的民間規格採用実績 ― 守秘・鍵共有



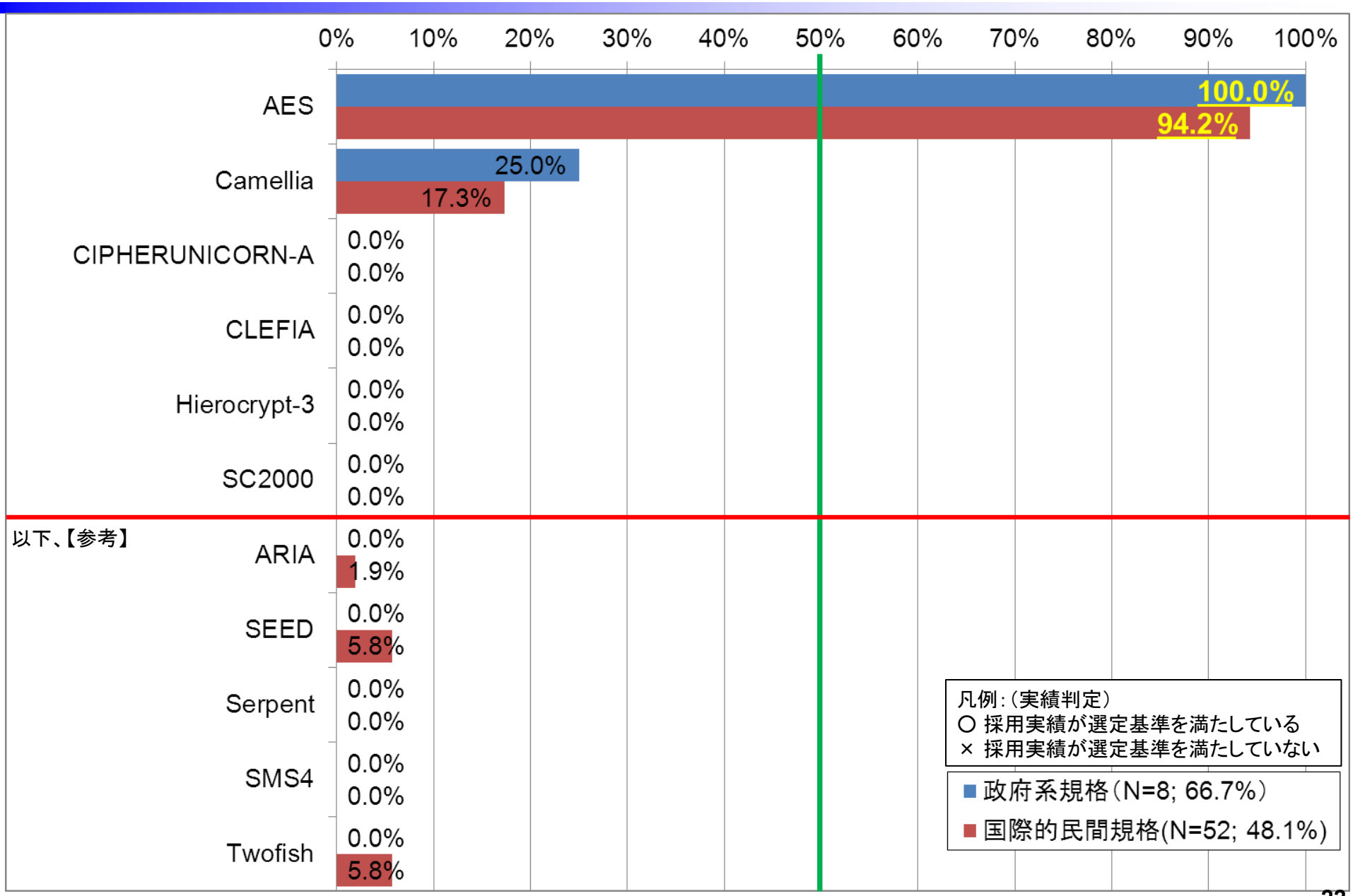
※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答された暗号アルゴリズムXXXであることに注意

政府及び国際的民間規格採用実績 ― 64ビットブロック暗号

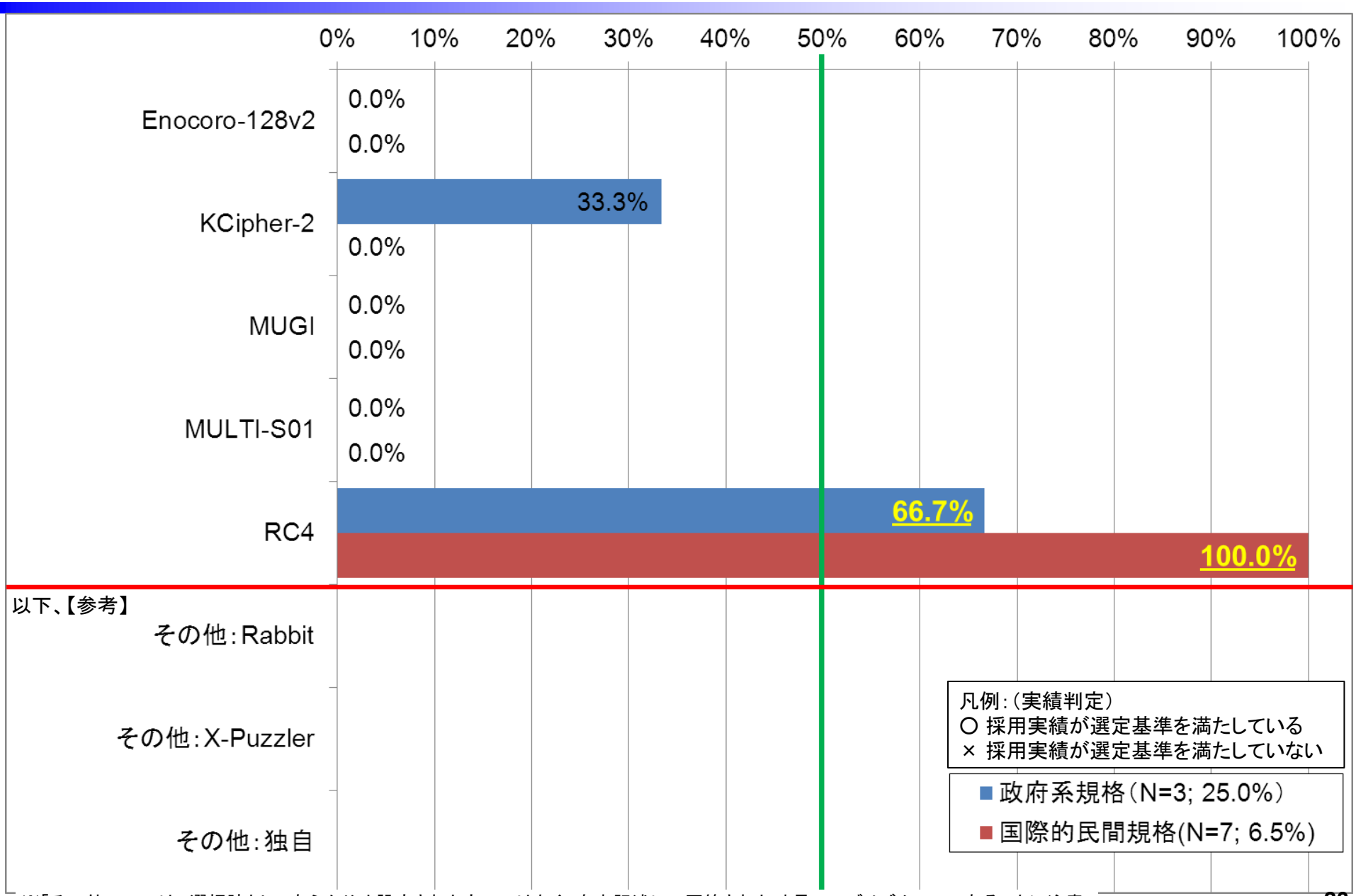


※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答された暗号アルゴリズムXXXであることに注意

政府及び国際的民間規格採用実績 ― 128ビットブロック暗号

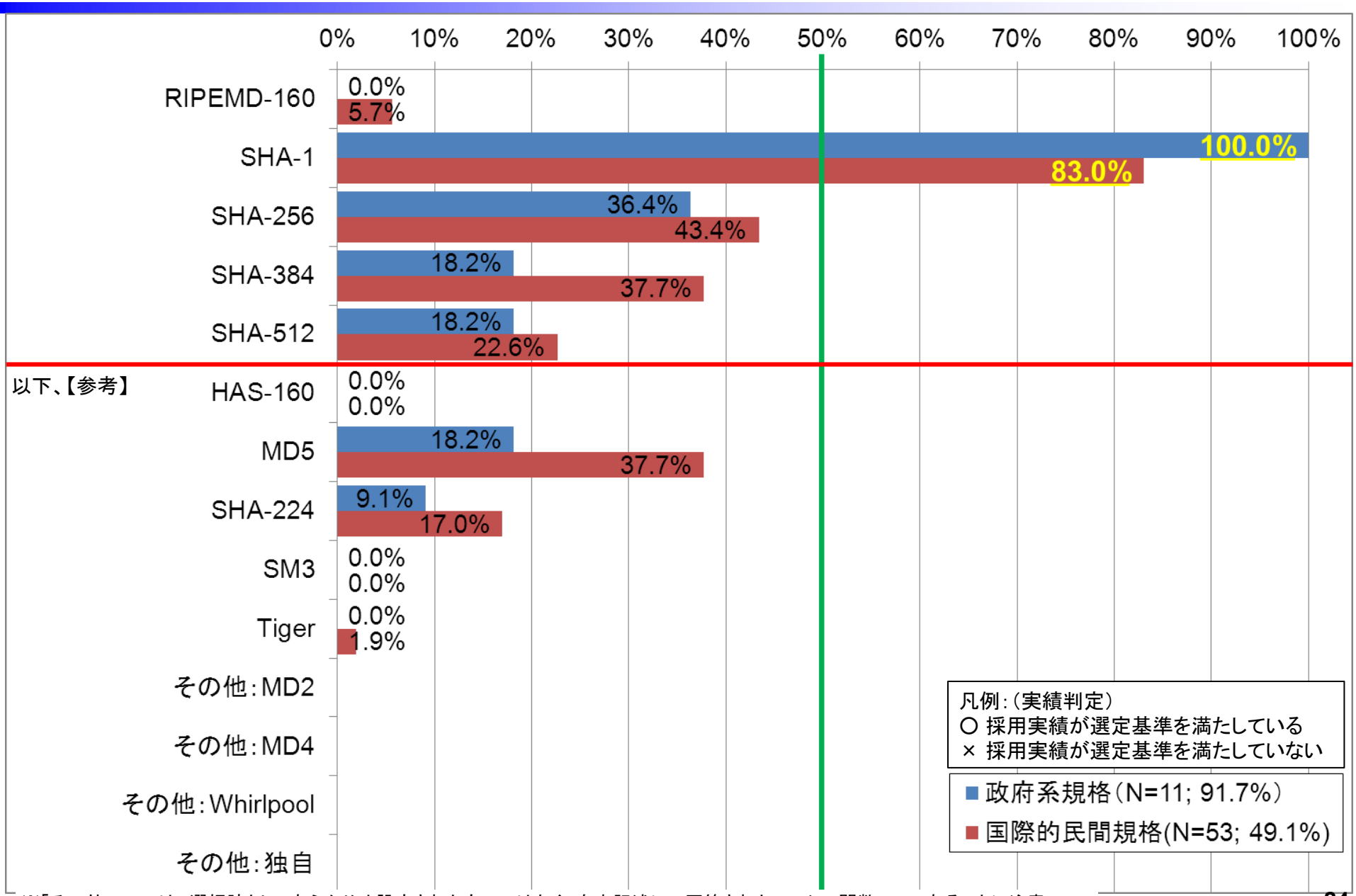


政府及び国際的民間規格採用実績 ー ストリーム暗号



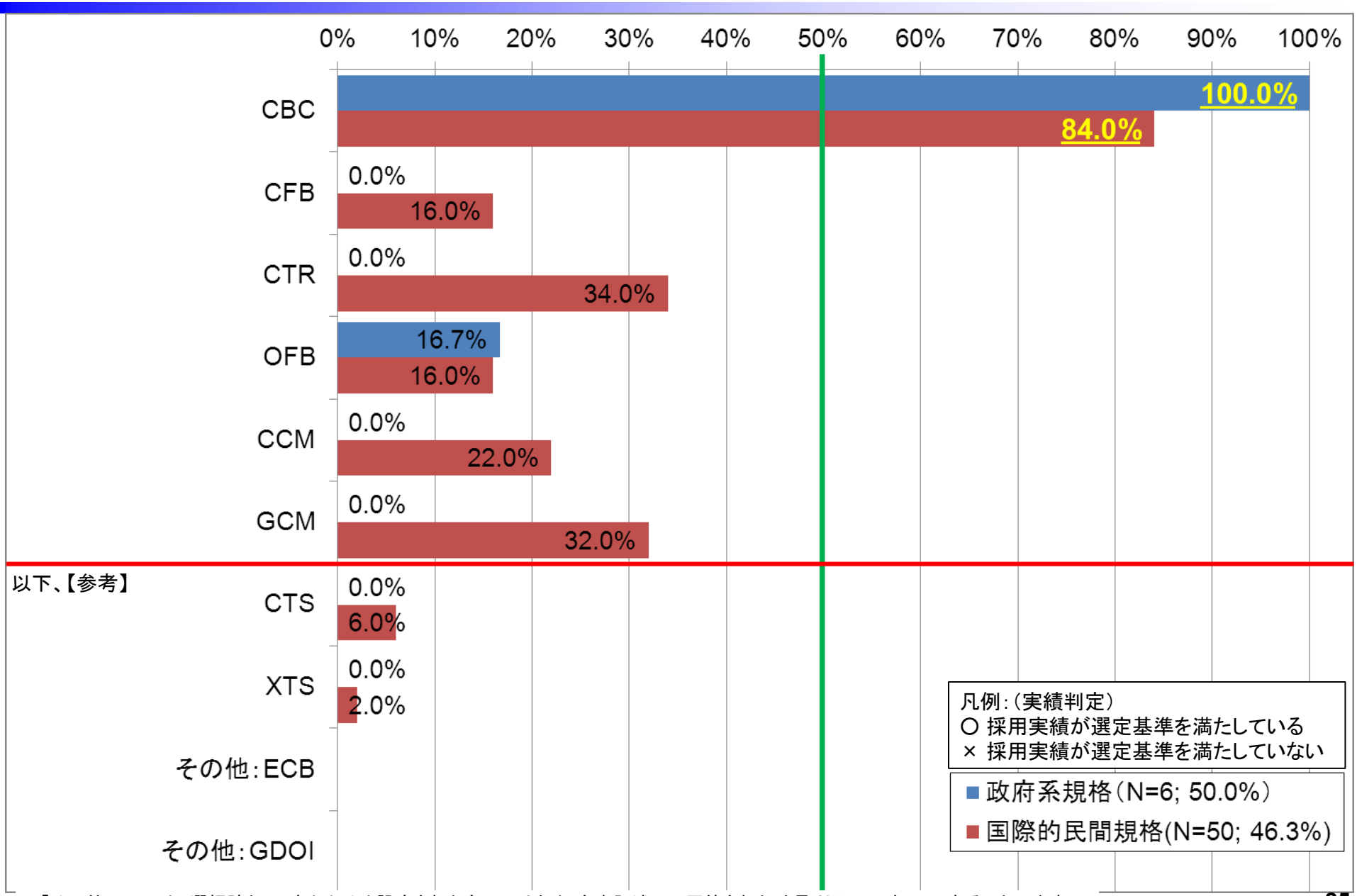
※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答された暗号アルゴリズムXXXであることに注意

政府及び国際的民間規格採用実績 ー ハッシュ関数



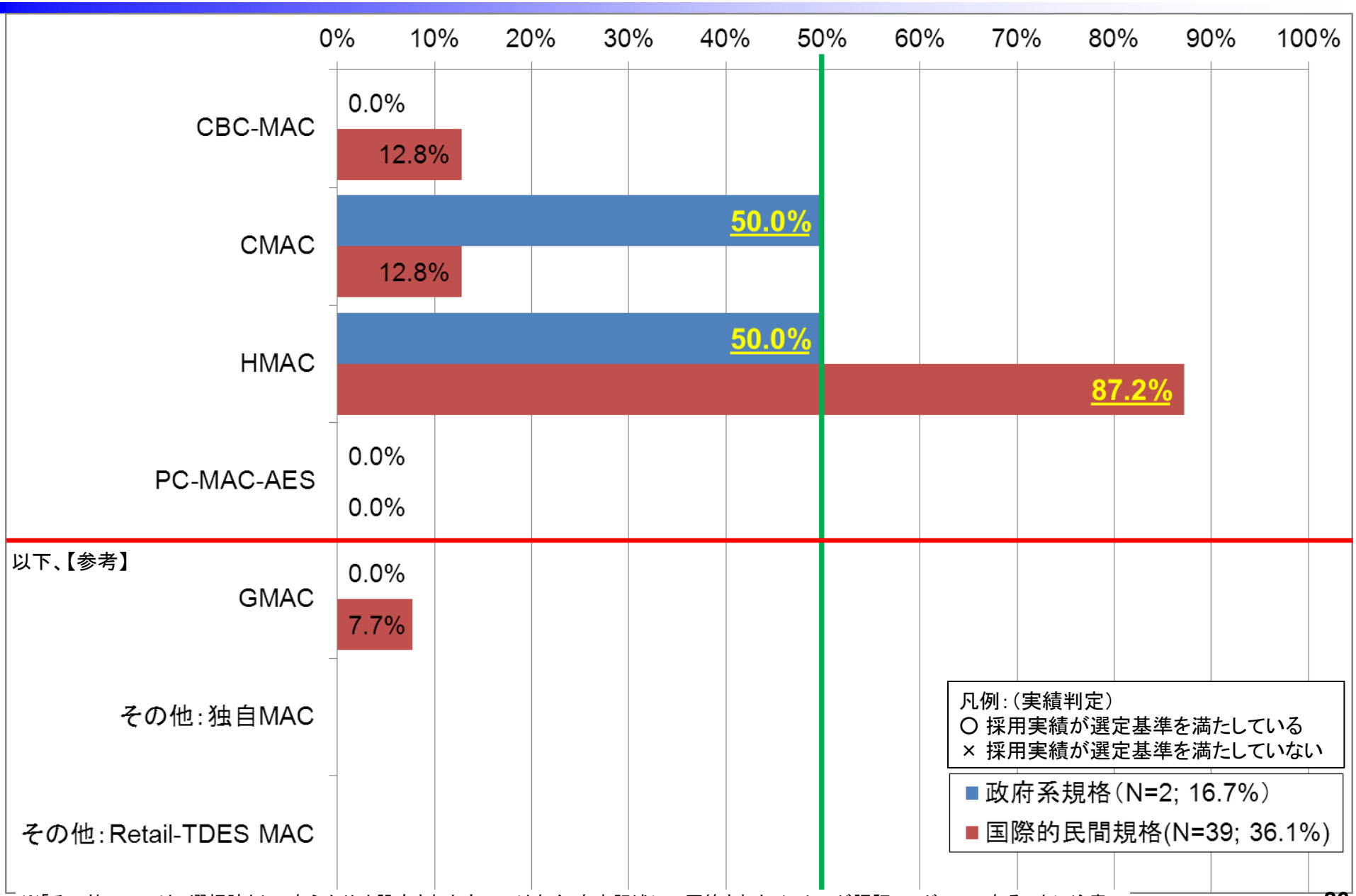
※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答されたハッシュ関数XXXであることに注意

政府及び国際的民間規格採用実績 ― 暗号利用モード



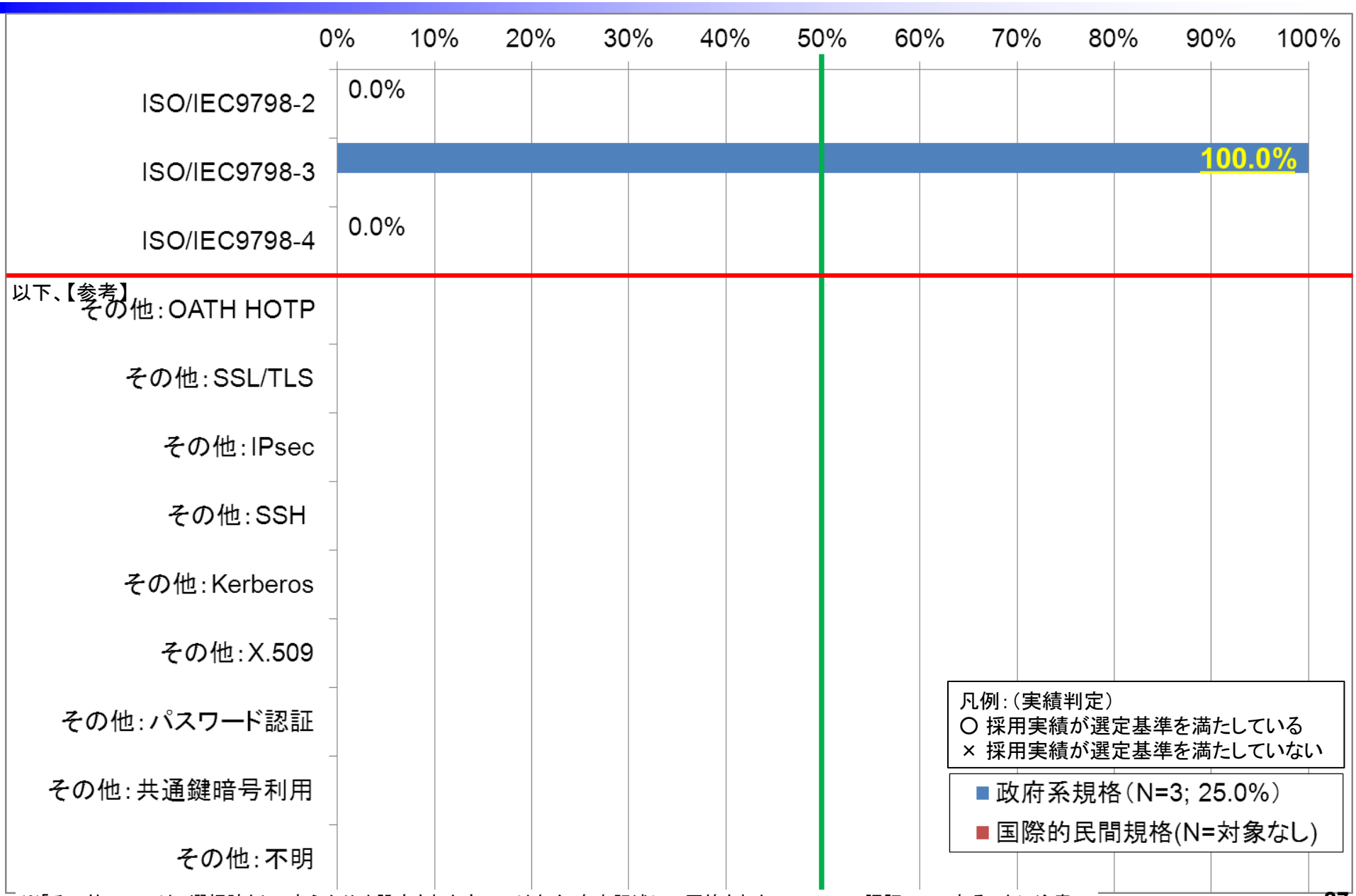
※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答された暗号利用モードXXXであることに注意

政府及び国際的民間規格採用実績 ― メッセージ認証コード



※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答されたメッセージ認証コードXXXであることに注意

政府及び国際的民間規格採用実績 ― エンティティ認証



※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答されたエンティティ認証XXXであることに注意

調査方法の概要(1)

別添

■ 調査A:応募者に対するアンケート調査

対象アルゴリズム以外の利用状況が分からない情報

対象アルゴリズム以外の利用状況も特定可能な情報

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
ソニー株式会社	CLEFIA	○	○
株式会社日立製作所	Enocoro-128v2, MUGI, MULTI-S01	○	○
KDDI 株式会社	KCipher-2	○	○
日本電気株式会社	CIPHERUNICORN-E, CIPHERUNICORN-A, PC-MAC-AES	○	○
富士通株式会社	ECDSA, ECDH, SC2000	○	○
EMC ジャパン株式会社	RSASSA-PKCS1-v1_5, RSAES-PKCS1-v1_5, RC4	×	○
	RSA-PSS, RSA-OAEP	○	○
日本電信電話株式会社	Camellia, PSEC-KEM	○	○
株式会社東芝	Hierocrypt-L1, Hierocrypt-3	○	○
三菱電機株式会社	MISTY1	○	○

調査(B)～(E)により、対象アルゴリズム以外の利用状況が特定できたか？

特定できなかった

応募者追加情報としての参考扱い(有効回答から除外)

特定できた

調査(B)～(E)の有効回答として取り扱い

調査A:応募者追加情報として集計から除外した情報

企業名	対象アルゴリズム	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	CLEFIA	0	0	1	0
株式会社日立製作所	Enocoro-128v2	0	0	0	0
	MUGI	0	0	0	0
	MULTI-S01	0	0	0	0
KDDI 株式会社	KCipher-2	2	3	0	0
日本電気株式会社	CIPHERUNICORN-E	0	0	0	0
	CIPHERUNICORN-A	0	0	0	0
	PC-MAC-AES	0	0	0	0
富士通株式会社	ECDSA	0	0	0	1
	ECDH	0	0	0	1
	SC2000	0	0	0	0
EMC ジャパン株式会社	RSASSA-PKCS1-v1_5	応募者からの回答なし			
	RSAES-PKCS1-v1_5	応募者からの回答なし			
	RC4	応募者からの回答なし			
	RSA-PSS	1	0	1	0
	RSA-OAEP	3	0	3	0
日本電信電話株式会社	Camellia	14	0	6	21
	PSEC-KEM	1	0	1	0
株式会社東芝	Hierocrypt-L1	0	0	0	0
	Hierocrypt-3	0	0	0	0
三菱電機株式会社	MISTY1	0	0	1	0

調査方法の概要(2)

- 調査B:市販製品メーカー・販売会社等に対するアンケート調査
  - 調査方法
    - 市販製品に関するアンケート調査(有効回答:会社数127、製品数443)
    - 公開情報を基にみずほ情報総研が調査(調査対象:会社数35、製品数90)
  - 集計方法
    - 2012年6月30日時点に発売中または発売予定であることをアンケートで確認
    - 製品名・システム名により重複回答を削除
    - アンケートで指定された情報により信頼度(Lev1～Lev5)を割り当て

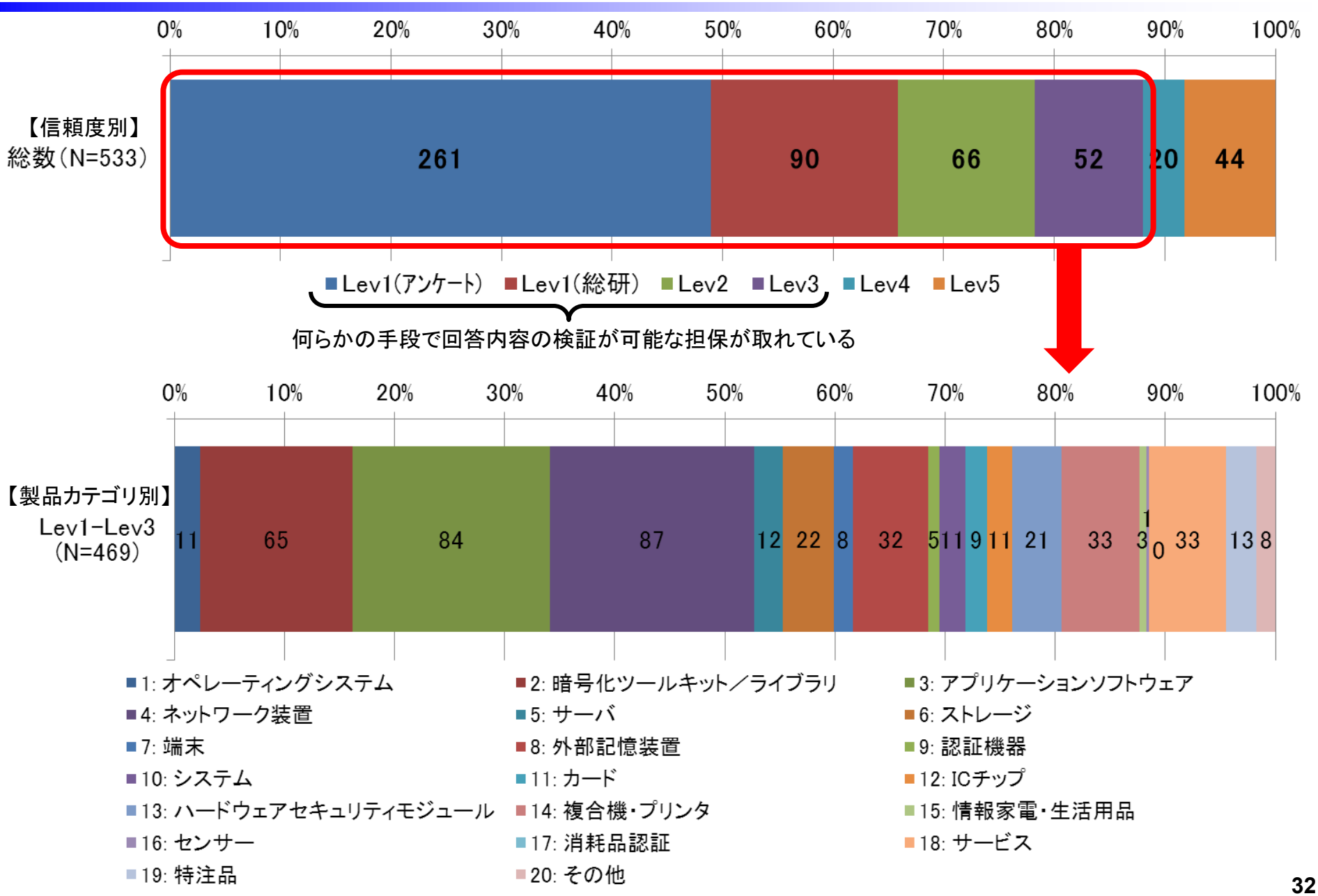
Lev1	公開情報等により回答内容が確認できたもの
Lev2	要求があれば、回答内容を検証できる情報を提供してもよいとの回答があったもの
Lev3	NDAを締結すれば、回答内容を検証できる情報を提供してもよいとの回答があったもの
Lev4	回答内容を検証できる情報はあるが、提供はできないとの回答があったもの
Lev5	回答内容を検証できる情報があるかどうか判明しなかったもの

    - Triple DESについて明示的に2-key Triple DESと判明した回答(18件)を除外
    - ブロック暗号を利用し、暗号利用モードが不明なものも有効回答とする
    - 「他社利用」の判定においては以下のルールに従う
      - 応募者と同じ社名・略称が含まれる企業はグループ会社とみなす
      - 資本関係等、応募者と関連があると広く知られている企業は関連会社とみなす
      - 応募者・グループ会社・関連会社以外の企業を他社とみなす

調査B：市販製品利用実績調査の総回収状況

製品カテゴリ	該当数	64ビットブロック暗号	128ビットブロック暗号	ストリーム暗号	モード	メッセージ認証コード	署名	守秘・鍵共有	ハッシュ関数	エンティティ認証
1: オペレーティングシステム	11	7	9	5	7	8	9	8	11	0
2: 暗号化ツールキット／ライブラリ	65	36	58	27	34	21	34	32	34	14
3: アプリケーションソフトウェア	94	35	63	26	18	13	15	18	46	12
4: ネットワーク装置	94	69	82	33	29	50	52	67	78	14
5: サーバ	16	7	9	3	2	1	7	9	9	3
6: ストレージ	25	17	22	7	7	2	13	18	20	9
7: 端末	12	3	11	2	0	3	4	3	4	0
8: 外部記憶装置	33	7	25	0	3	5	11	8	13	3
9: 認証機器	6	0	6	0	0	0	0	0	1	0
10: システム	13	4	8	5	1	0	0	1	3	4
11: カード	15	11	10	0	10	8	9	8	10	0
12: ICチップ	13	7	7	1	1	0	3	2	5	1
13: ハードウェアセキュリティモジュール	21	21	19	11	14	11	19	18	20	0
14: 複合機・プリンタ	44	42	38	32	31	5	16	18	34	11
15: 情報家電・生活用品	6	3	5	2	3	3	3	1	4	1
16: センサー	2	1	2	1	1	0	1	1	1	0
17: 消耗品認証	0	0	0	0	0	0	0	0	0	0
18: サービス	37	16	21	10	3	4	19	15	24	7
19: 特注品	13	12	4	2	0	0	1	1	3	1
20: その他	13	4	4	4	4	4	7	4	8	0
市販製品総合	533	302	403	171	168	138	223	232	328	80
市販暗号モジュール（#1,#2,#11,#12,#13）	125	82	103	44	66	48	74	68	80	15

調査B：市販製品利用実績（内訳）



調査方法の概要(3)

- 調査C:政府系システム・規格に対する調査
  - 調査方法
    - 経産省・IPAがアンケート回収。みずほ情報総研が集計
      - システム利用実績: 8府省庁77システム
      - 政府系規格:5規格
      - アンケート回答内容については当該府省庁の情報システム課が検証
    - 公開情報を基にみずほ情報総研が調査を実施(政府系規格のみ:7規格)

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
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
商業登記認証局	「電子証明書の方式等に関する件(告示)」
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
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
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
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

調査方法の概要(4)

- 調査D:国際標準・国際的民間規格・特定団体規格に対する調査
  - 調査方法
    - 国際標準規格・国際的民間規格
      - みずほ情報総研が公開情報を基に調査を実施(調査数:国際標準規格12、国際的民間規格108(15種類))
    - 特定団体規格
      - 特定団体規格に対してはアンケート調査を実施(有効回答数:16(3団体))
      - みずほ情報総研が公開情報を基に調査を実施(調査数:8(6団体))
  - 集計方法
    - 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

調査D：国際標準規格の調査対象

	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.SecMechanisms (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

調査D:国際的民間規格の調査対象

	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	16	RFC2311, RFC2312, RFC3565, RFC3657, RFC3853, RFC4056, RFC5083, RFC5652, RFC5750, RFC5751, RFC5752, RFC5753, RFC5754, RFC5990, RFC3560, RFC4056
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

調査D：特定団体規格の調査対象

	団体名	詳細	アンケート回答	総研調査
1	財団法人道路システム高度化推進機構	ORSE情報安全確保規格等	×	―
2	ZigBee SIG-Japan	ZigBee和訳仕様書	×	1
3	Bluetooth SIG, Inc	Bluetooth仕様書	×	1
4	Wi-Fi Alliance	WiFi仕様書	×	1
5	DLNA	DLNAガイドラインVer1.5	×	―
6	FISC	金融機関等コンピュータシステムの安全対策基準・解説書（第8版）	×	― 暗号の記載なし
7	ARIB	地上デジタルテレビジョン放送 ARIB TR-B14 、BS/広帯域CSデジタル放送 ARIB TR-B15、サーバー型放送 ARIB TR-B27	13	―
8	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	×	1
9	DCCJ	Digital Cinema Initiatives, LLC　DCI規格 (V1.0)	×	1
10	AACS	AACS仕様書	×	3
11	JCTEA	JCTEA標準規格（デジタル有線テレビジョン放送　限定受信方式等）	×	―
12	TTC	TTC標準／仕様書	×	―
13	Marline Joint Development Association	Marlin仕様書	2	―
14	日本鉄道サイバネティクス協議会		×	―
15	日本オンラインゲーム協会		×	―
16	一般財団法人日本データ通信協会	タイムビジネス部タイムビジネス認定センター内複数規格	1	―

調査方法の概要(5)

- 調査E:オープンソースプロジェクトに関する調査
  - 調査方法
    - 指定されたオープンソースプロジェクトの最新安定版について、みずほ情報総研が調査を実施(調査数:24)

	ツール名	バージョン
1	Linux	3.4.7
2	Debian	6.0.5
3	FreeBSD	9.0
4	Android	4.0
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)

	ツール名	バージョン
13	Webkit	r125966
14	Thunderbird	14.0
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

調査方法の概要(5)(続)

- 調査E:オープンソースプロジェクトに関する調査
  - 集計方法
    - Linux+Debian、Qmail+OpenSSL、Firefox+Thunderbird+NSSとして集計
      - OSS総合の全体個数:20
      - OSS暗号モジュールの全体個数:7 (Linux+Debian, FreeBSD, Android, NSS, OpenSSL, GnuPG, Mcrypt)
    - 応募者からの情報があっても、みずほ情報総研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
    - ダブルカウントを避けるため、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: 以下のメイン(/libcore/luni/src/main/)ではない、external直下のフォルダにCamelliaが存在します。/external/bouncycastle/, /external/ipsec-tools/, /external/openssl/crypto/evp/」

        → AndroidについてCamelliaが搭載されているとは認めない
    - 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