評価B判定結果

資料構成の目次

評価Bの各評価項目における選定基準（1）

【第1回暗号技術検討会にて承認】

「（評価B）利用促進の可能性が高い」と判断するための閾値(Y)
下記8項目中、**「3項目以上」**の選定基準を満たす

評価A基準	**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）	
追加基準	**利用促進を図る際の障壁の除去**		**特許無償ライセンスの付与（契約有無は問わない）** ● 特許なし、もしくは契約不要の特許無償ライセンス許諾 ● 非差別的無償許諾契約に基づく無償ライセンス	
	標準化・規格化の促進を図るハードルの低さ	OR条件	技術的アピールポイント	方式委員会、又は、実装委員会により**技術的アピールポイントがあると認められる**
			標準化等のアピールポイント	「政府系システム規格」「国際標準規格」「国際的な民間規格」「特定団体規格」のいずれかの規格において、**「2件以上」かつ「採用割合として10%以上」となる件数**での採用が同意されていること ※ただし、カテゴリ有効数が4件以下の時に限り、「1件」でもよいこととする
			採用実績のアピールポイント	以下のいずれかの条件を満たしている ● オープンソースプロジェクトで**「2件以上」かつ「採用割合として10%以上」となる件数**での採用があること ● 市販製品で、**「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10%以上」となる件数**の採用実績があること

評価Bの各評価項目における選定基準（2）

追加基準	**実装コスト低減を図るハードルの低さ**	OR条件	採用実績のアピールポイント	OSや暗号モジュール（ライブラリやチップなど：市販製品調査カテゴリ#1, #2, #11, #12, #13）として使える市販製品において、**「提案会社・グループ会社以外での採用実績」があり、「2件以上」かつ「採用割合として10%以上」となる件数**の採用実績があること
			オープンソースのアピールポイント	暗号モジュール（OSカーネル及び暗号化ライブラリ）として使えるオープンソースプロジェクトにおいて、**「2件以上」かつ「採用割合として10%以上」となる件数**の採用実績があること ※ただし、カテゴリ有効数が4件以下の時に限り、「1件」でもよいこととする
	調達コスト低減を図るハードルの低さ		採用実績のアピールポイント	以下のいずれかの条件を満たしている ● 市販製品で、**「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10%以上」となる件数**の採用実績があること ● 政府系システムで実際に**「2件以上」かつ「採用割合として10%以上」となる件数**での採用実績があること

⇨ 技術的アピールポイントに関わる評価項目は、暗号方式委員会及び暗号実装委員会が独自に判定を行う

⇨ 知的財産権に関わる評価項目は、2012年9月30日時点における応募会社各社の特許ライセンス宣誓を基に判定を行う
※応募会社各社に特許ライセンス宣誓の確認

⇨ 利用実績に関わる評価項目は、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

評価Bのまとめ(1)

		判定結果↓ / 判定根拠データ→		評価Aの結果と同じ				P.7	P.8	P.30	P.40
				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	利用促進を図る際の障壁除去	標準化・規格化の促進を図るハードルの低さ	実装コスト低減を図るハードルの低さ	調達コスト低減を図るハードルの低さ
署名	ECDSA	○	3/8	×	×	×	×	×	○	○	○
	RSA-PSS	○	4/8	×	×	×	×	○	○	○	○
守秘・鍵共有	ECDH	○	3/8	×	×	×	×	×	○	○	○
	PSEC-KEM	×	2/8	×	×	×	×	○	○	×	×
	RSA-OAEP	○	4/8	×	×	×	×	○	○	○	○
64ビットブロック暗号	CIPHERUNICORN-E	×	1/8	×	×	×	×	×	○	×	×
	Hierocrypt-L1	×	1/8	×	×	×	×	×	○	×	×
	MISTY1	×	2/8	×	×	×	×	○	○	×	×
128ビットブロック暗号	Camellia	○	4/8	×	×	×	×	○	○	○	○
	CIPHERUNICORN-A	×	1/8	×	×	×	×	×	○	×	×
	CLEFIA	×	1/8	×	×	×	×	×	○	×	×
	Hierocrypt-3	×	1/8	×	×	×	×	×	○	×	×
	SC2000	×	1/8	×	×	×	×	×	○	×	×

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

評価Bのまとめ(2)

		判定結果↓	判定根拠データ→	評価Aの結果と同じ				P.7	P.8	P.30	P.40
				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	利用促進を図る際の障壁除去	標準化・規格化の促進を図るハードルの低さ	実装コスト低減を図るハードルの低さ	調達コスト低減を図るハードルの低さ
ストリーム暗号	Enocoro-128v2	×	1/8	×	×	×	×	×	○	×	×
	KCipher-2	○	3/8	×	×	×	×	○	○	×	○
	MUGI	×	2/8	×	×	×	×	○	○	×	×
	MULTI-S01	×	1/8	×	×	×	×	×	○	×	×
ハッシュ関数	SHA-256	○	6/8	○	○	×	×	○	○	○	○
	SHA-384	○	5/8	×	○	×	×	○	○	○	○
	SHA-512	○	5/8	×	○	×	×	○	○	○	○
暗号利用モード（秘匿）	CFB	○	5/8	×	○	×	×	○	○	○	○
	CTR	○	4/8	×	×	×	×	○	○	○	○
	OFB	○	4/8	×	×	×	×	○	○	○	○
暗号利用モード（認証付秘匿）	CCM	○	3/8	×	×	×	×	○	○	○	×
	GCM	○	4/8	×	×	×	×	○	○	○	○
メッセージ認証コード	CMAC	○	4/8	×	×	○	×	○	○	○	×
	PC-MAC-AES	×	1/8	×	×	×	×	×	○	×	×
エンティティ認証	ISO/IEC9798-2	○	3/8	×	−	×	−	×	○	○	○
	ISO/IEC9798-3	○	3/8	×	−	○	−	×	○	×	○
	ISO/IEC9798-4	×	1/8	×	−	×	−	×	○	×	×

「利用促進を図る際の障壁の除去」の判定

凡例：○ 特許無償許諾または特許なし
× 特許有償許諾
（2012年9月30日時点）

		判定結果
署名	ECDSA	×
	RSA-PSS	○
守秘・鍵共有	ECDH	×
	PSEC-KEM	○
	RSA-OAEP	○
64ビット ブロック暗号	CIPHERUNICORN-E	×
	Hierocrypt-L1	×
	MISTY1	○
128ビット ブロック暗号	Camellia	○
	CIPHERUNICORN-A	×
	CLEFIA	×
	Hierocrypt-3	×
	SC2000	×
ストリーム暗号	Enocoro-128v2	×
	KCipher-2	○
	MUGI	○
	MULTI-S01	×

		判定結果
ハッシュ関数	SHA-256	○
	SHA-384	○
	SHA-512	○
暗号利用モード（秘匿）	CFB	○
	CTR	○
	OFB	○
暗号利用モード（認証付秘匿）	CCM	○
	GCM	○
メッセージ認証コード	CMAC	○
	PC-MAC-AES	○
エンティティ認証	ISO/IEC9798-2	×
	ISO/IEC9798-3	×
	ISO/IEC9798-4	×

「標準化・規格化の促進を図るハードルの低さ」の判定

		判定結果	P.9-11 技術的アピール	P.13-21 標準化アピール	P.22-30 採用アピール
署名	ECDSA	○	○	○	○
	RSA-PSS	○	○	○	○
守秘・鍵共有	ECDH	○	○	○	○
	PSEC-KEM	○	○	○	×
	RSA-OAEP	○	○	○	○
ブロック暗号64ビット	CIPHERUNICORN-E	○	○	×	×
	Hierocrypt-L1	○	○	×	×
	MISTY1	○	○	○	×
ブロック暗号128ビット	Camellia	○	○	○	○
	CIPHERUNICORN-A	○	○	×	×
	CLEFIA	○	○	○	×
	Hierocrypt-3	○	○	×	×
	SC2000	○	○	×	×
ストリーム暗号	Enocoro-128v2	○	○	○	×
	KCipher-2	○	○	○	○
	MUGI	○	○	○	×
	MULTI-S01	○	○	○	×

		判定結果	P.9-11 技術的アピール	P.13-21 標準化アピール	P.22-30 採用アピール
ハッシュ関数	SHA-256	○	○	○	○
	SHA-384	○	○	○	○
	SHA-512	○	○	○	○
暗号利用モード（秘匿）	CFB	○	×	○	○
	CTR	○	×	○	○
	OFB	○	×	○	○
暗号利用モード（秘匿）（認証付）	CCM	○	○	○	○
	GCM	○	○	○	○
メッセージ認証コード	CMAC	○	○	○	○
	PC-MAC-AES	○	○	×	×
エンティティ認証	ISO/IEC9798-2	○	○	○	○
	ISO/IEC9798-3	○	○	○	○
	ISO/IEC9798-4	○	○	○	×

3つのアピールポイントのOR条件で総合判定

凡例：（アピール判定）○ アピールポイントが認められる
× アピールポイントが認められない

技術的アピールポイント結果（1）

		技術的アピール判定	暗号方式委員会アピールポイント判定 （ー：判定対象外）			暗号実装委員会アピールポイント判定 （ー：判定対象外）		
			判定	比較対象		判定	比較対象	
署名	ECDSA	○	○	RSASSA-PKCS1-v1_5	Index calculus 法は楕円曲線上の離散対数問題を解くには現時点ではまだ効率的であるとは言えない	○	RSA署名	ソフトウェア実装における鍵生成時間と署名生成速度の優位性を確認した
	RSA-PSS	○	○	RSASSA-PKCS1-v1_5	証明可能安全性(適応的選択文書攻撃に対して存在的偽造不可)がランダムオラクルモデルのもとで RSA 問題の困難性に帰着される	ー	ー	ー
守秘・鍵共有	ECDH	○	○	DH	Index calculus法は楕円曲線上の離散対数問題を解くには現時点ではまだ効率的であるとは言えない	○	DH	ソフトウェア実装における鍵生成時間と鍵共有処理時間の優位性を確認した
	PSEC-KEM	○	○	DH	KEM技術に関する証明可能安全性がランダムオラクルモデルのもとで楕円曲線DH計算問題に帰着され、KEM-DEM構成が安全であることが示されている	○	DH	ソフトウェア実装における鍵生成時間と鍵共有処理時間において、ECDHと同等、DHよりも優位であることを確認した
	RSA-OAEP	○	○	RSAES-PKCS1-v1_5	証明可能安全性(適応的選択暗号文攻撃に対して強秘匿)がランダムオラクルモデルのもとでRSA 問題の困難性に帰着される	ー	ー	ー
64ビットブロック暗号	CIPHERUNICORN-E	○	○	3-key Triple DES	解析が困難な構造が採用されており、有効な攻撃法は見つかっていない	○	Triple DES	ソフトウェア実装における小型実装での優位性を確認した
	Hierocrypt-L1	○	○	3-key Triple DES	多くの攻撃手法に対する安全性評価がなされており、鍵の全数探索よりも効率の良い攻撃手法が知られていない	○	Triple DES, MISTY1	ソフトウェア実装における暗号化速度での優位性を確認した
	MISTY1	○	○	3-key Triple DES	差分攻撃および線形攻撃に対する証明可能安全性を有し、多くの攻撃手法に対する安全性評価がなされている	ー	ー	ー

2つのアピール判定のOR条件で総合判定

凡例：（アピール判定） ○ アピールポイントが認められる　× アピールポイントが認められない　ー 判断対象外

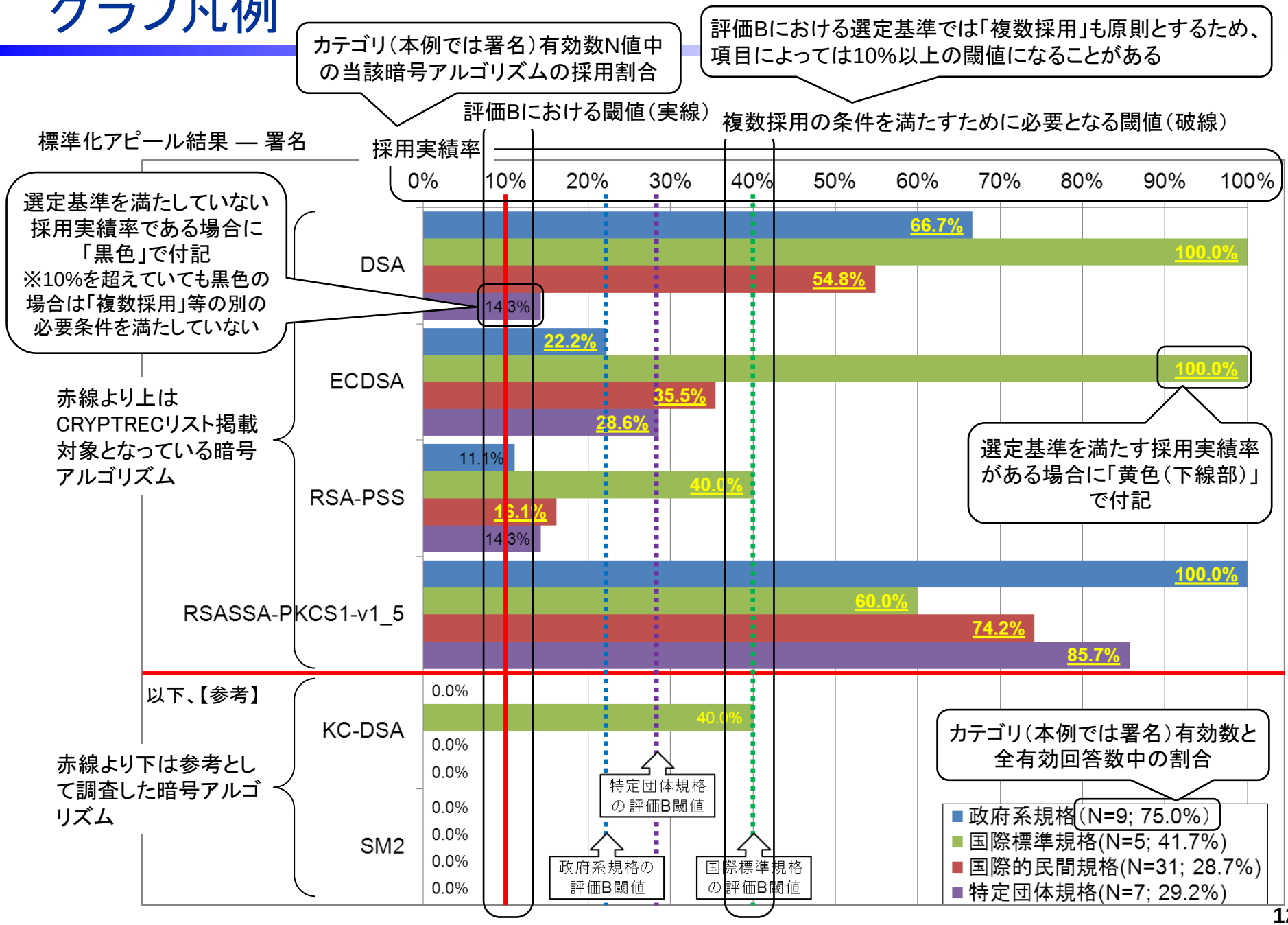
技術的アピールポイント結果（2）

		技術的アピール判定	暗号方式委員会アピールポイント判定 （－：判定対象外）			暗号実装委員会アピールポイント判定 （－：判定対象外）		
			判定	比較対象		判定	比較対象	
128ビットブロック暗号	Camellia	○	○	AES	多くの攻撃手法に対する安全性評価がなされており、特にAESに適用されているような関連鍵攻撃は見つかっていない	○	AES	ソフトウェア実装における初期化時間、実装サイズと、ハードウェア実装における実装サイズ、回路効率等の優位性を確認した
	CIPHERUNICORN-A	○	○	AES	解析が困難な構造が採用されており、関連鍵攻撃をはじめ有効な攻撃法は見つかっていない	×	AES	優位性を示す測定結果が確認できなかった
	CLEFIA	○	○	AES	多くの攻撃手法に対する安全性評価がなされており、特にAESに適用されているような関連鍵攻撃は見つかっていない	○	AES, Camellia	ハードウェア実装における回路効率での優位性を確認した
	Hierocrypt-3	○	○	AES	多くの攻撃手法に対する安全性評価がなされており、特にAESに適用されているような関連鍵攻撃は見つかっていない	○	Camellia	ソフトウェア実装における暗号化速度で優位な測定結果を確認した
	SC2000	○	○	AES	多くの攻撃手法に対する安全性評価がなされており、特にAESに適用されているような関連鍵攻撃は見つかっていない	○	AES	ソフトウェア実装における暗号化速度、実装環境への対応性、キャッシュメモリの有効活用での優位性を確認した
ストリーム暗号	Enocoro-128v2	○	○	RC4	現時点において鍵の全数探索よりも効率の良い攻撃手法が知られていない	○	MUGI	ハードウェア実装における回路規模と回路効率における優位性を確認した
	KCipher-2	○	○	RC4	現時点において鍵の全数探索よりも効率の良い攻撃手法が知られていない	○	MUGI	ソフトウェア実装における暗号化速度、初期化時間、内部状態サイズでの優位性を確認した
	MUGI	○	○	RC4	現時点において鍵の全数探索よりも効率の良い攻撃手法が知られていない	○	AES	ハードウェア実装における回路規模、暗号化速度における優位性を確認した
	MULTI-S01	○	○	RC4	現時点において鍵の全数探索よりも効率の良い攻撃手法が知られていない	×	GCM(AES), CCM(AES)	優位性を示す測定結果が確認できなかった
ハッシュ関数	SHA-256	○	○	SHA-1	Preimage attack、2nd-Preimage attack、Collision attackにおいて、generic attackよりも効率の良い攻撃は知られていない	－	－	－
	SHA-384	○	○	SHA-1	Preimage attack、2nd-Preimage attack、Collision attackにおいて、generic attackよりも効率の良い攻撃は知られていない	－	－	－
	SHA-512	○	○	SHA-1	Preimage attack、2nd-Preimage attack、Collision attackにおいて、generic attackよりも効率の良い攻撃は知られていない	－	－	－

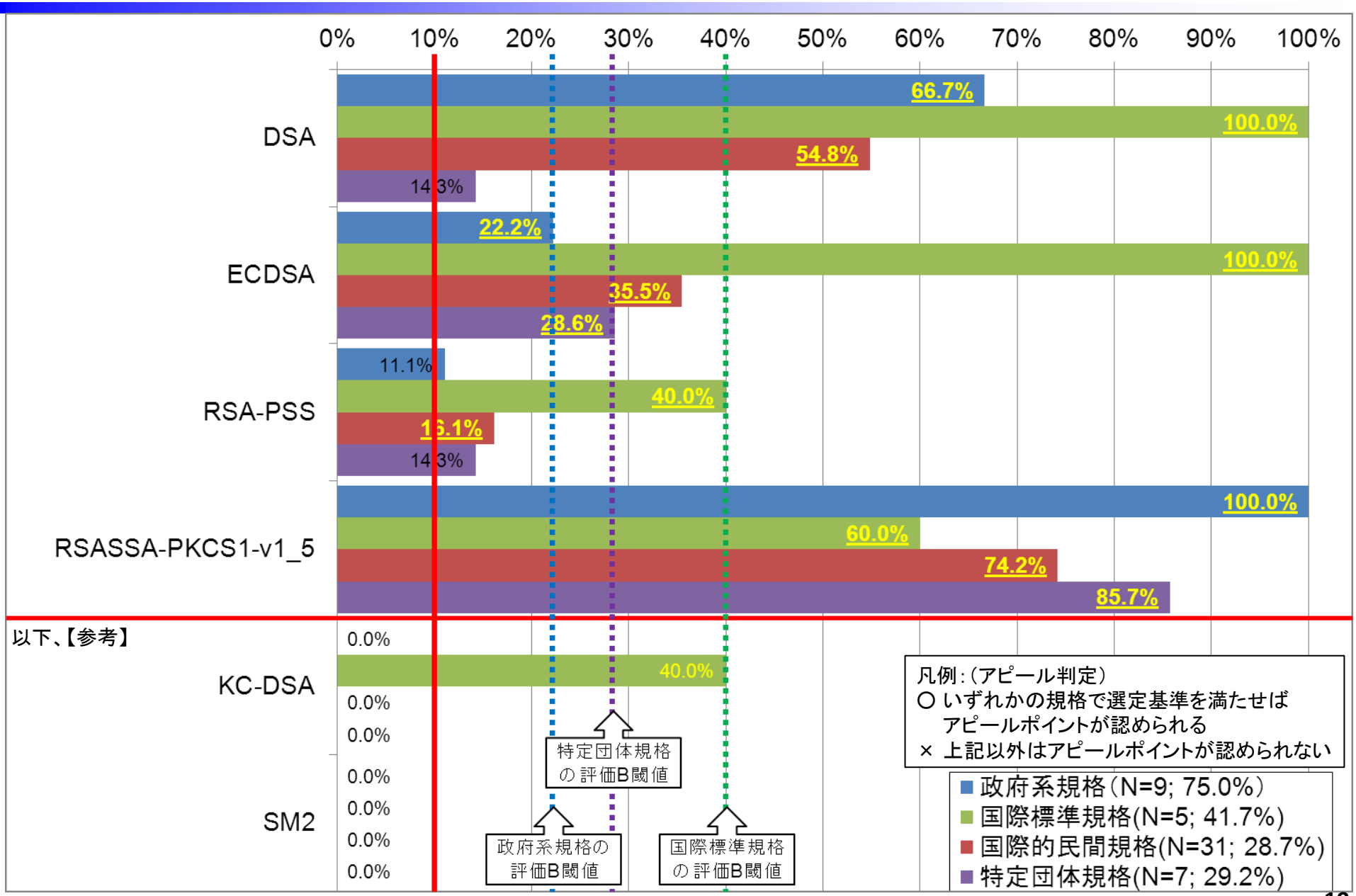
技術的アピールポイント結果（3）

		技術的アピール判定	暗号方式委員会アピールポイント判定 （ー：判定対象外）			暗号実装委員会アピールポイント判定 （ー：判定対象外）		
			判定	比較対象		判定	比較対象	
暗号利用モード（秘匿）	CFB	×	×	CBC	選択平文攻撃に対して、CBC と同程度の安全性である	ー	ー	ー
	CTR	×	×	CBC	選択平文攻撃に対して、CBC と同程度の安全性である	ー	ー	ー
	OFB	×	×	CBC	選択平文攻撃に対して、CBC と同程度の安全性である	ー	ー	ー
暗号利用モード（認証付秘匿）	CCM	○	○	CBC	仕様変更した場合(守秘用と認証用で独立な個別の鍵を用いた場合)、適応的選択暗号文攻撃に対する証明可能安全性を有する	ー	ー	ー
	GCM	○	○	CBC	適応的選択暗号文攻撃に対する証明可能安全性を有する	ー	ー	ー
メッセージ認証コード	CMAC	○	○	CBC-MAC	メッセージ空間に対して制約(prefix-free)のない安全性モデルにおいて証明可能安全性を有する	ー	ー	ー
	PC-MAC-AES	○	○	CBC-MAC	メッセージ空間に対して制約(prefix-free)のない安全性モデルにおいて証明可能安全性を有する	○	AESを使用したMAC一般	ソフトウェア実装におけるMAC生成・検証速度での優位性を確認した
エンティティ認証	ISO/IEC9798-2	○	○	特になし	ISO/IEC 29128 PAL3 レベルに沿った形式検証において安全性検証済みである。他の方式には同等のプロセスによる検証結果はない	ー	ー	ー
	ISO/IEC9798-3	○	○	特になし	ISO/IEC 29128 PAL3 レベルに沿った形式検証において安全性検証済みである。他の方式には同等のプロセスによる検証結果はない	ー	ー	ー
	ISO/IEC9798-4	○	○	特になし	ISO/IEC 29128 PAL3 レベルに沿った形式検証において安全性検証済みである。他の方式には同等のプロセスによる検証結果はない	ー	ー	ー

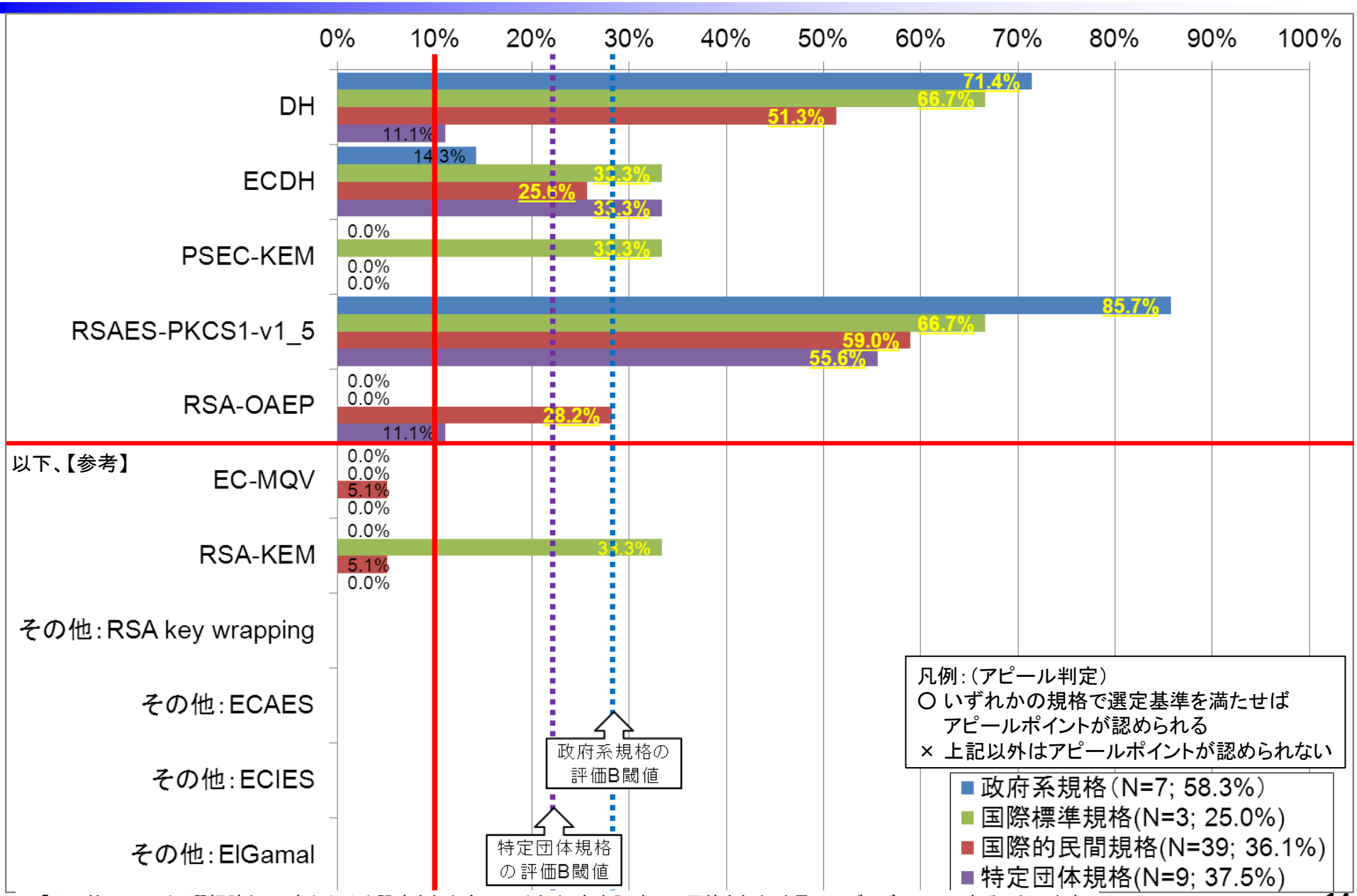
グラフ凡例


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Bにおける選定基準では「複数採用」も原則とするため、項目によっては10%以上の閾値になることがある
評価Bにおける閾値（実線）
複数採用の条件を満たすために必要となる閾値（破線）
標準化アピール結果 ― 署名
採用実績率
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
選定基準を満たしていない採用実績率である場合に「黒色」で付記
※10%を超えていても黒色の場合は「複数採用」等の別の必要条件を満たしていない
DSA
66.7%
100.0%
54.8%
14.3%
ECDSA
22.2%
100.0%
35.5%
28.6%
RSA-PSS
11.1%
40.0%
16.1%
14.3%
RSASSA-PKCS1-v1_5
100.0%
60.0%
74.2%
85.7%
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
選定基準を満たす採用実績率がある場合に「黄色（下線部）」で付記
以下、【参考】
KC-DSA
0.0%
40.0%
SM2
0.0%
0.0%
0.0%
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
特定団体規格の評価B閾値
政府系規格の評価B閾値
国際標準規格の評価B閾値
カテゴリ（本例では署名）有効数と全有効回答数中の割合
政府系規格(N=9; 75.0%)
国際標準規格(N=5; 41.7%)
国際的民間規格(N=31; 28.7%)
特定団体規格(N=7; 29.2%)

標準化アピール結果 — 署名

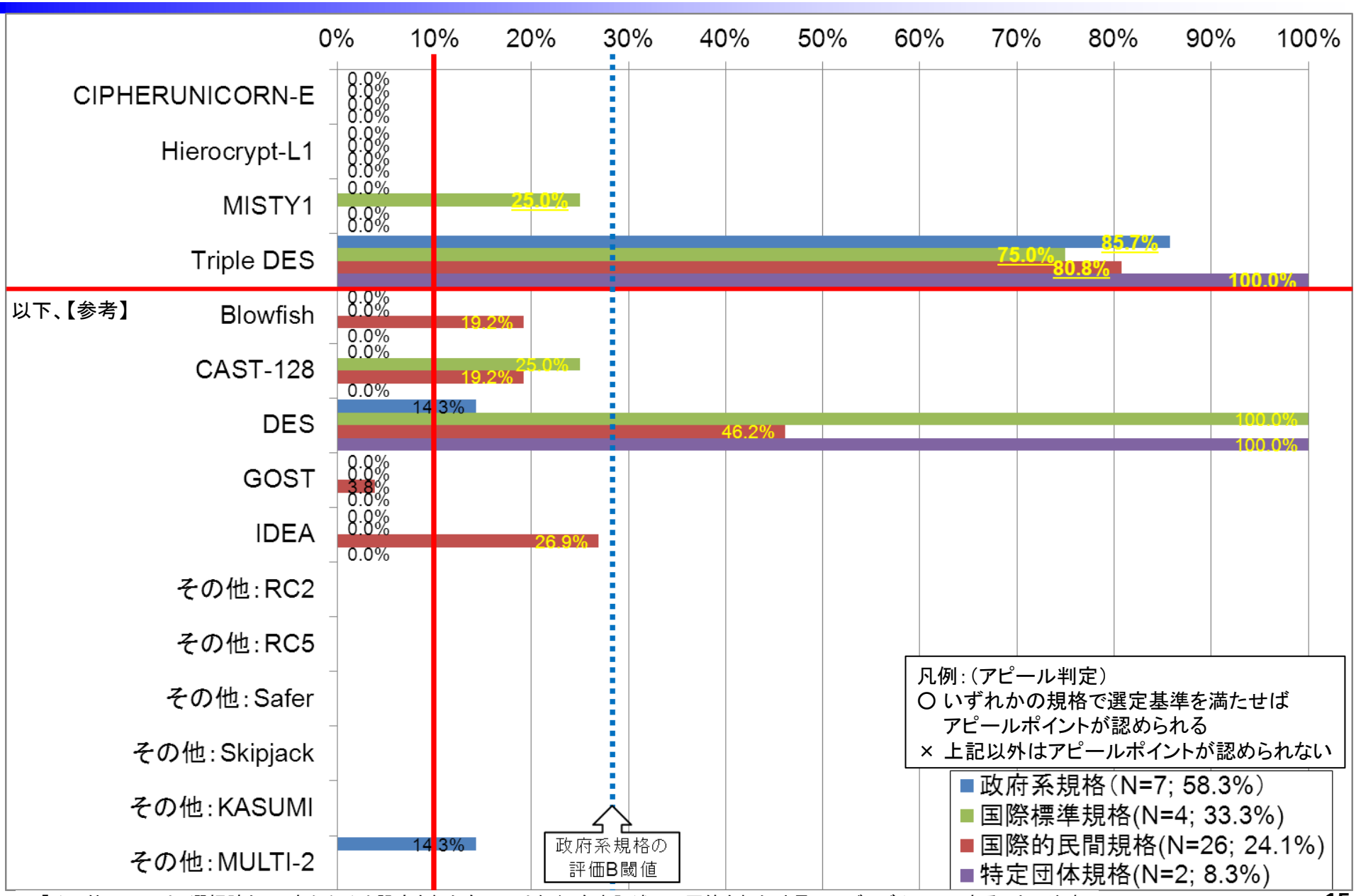


標準化アピール結果 — 守秘・鍵共有



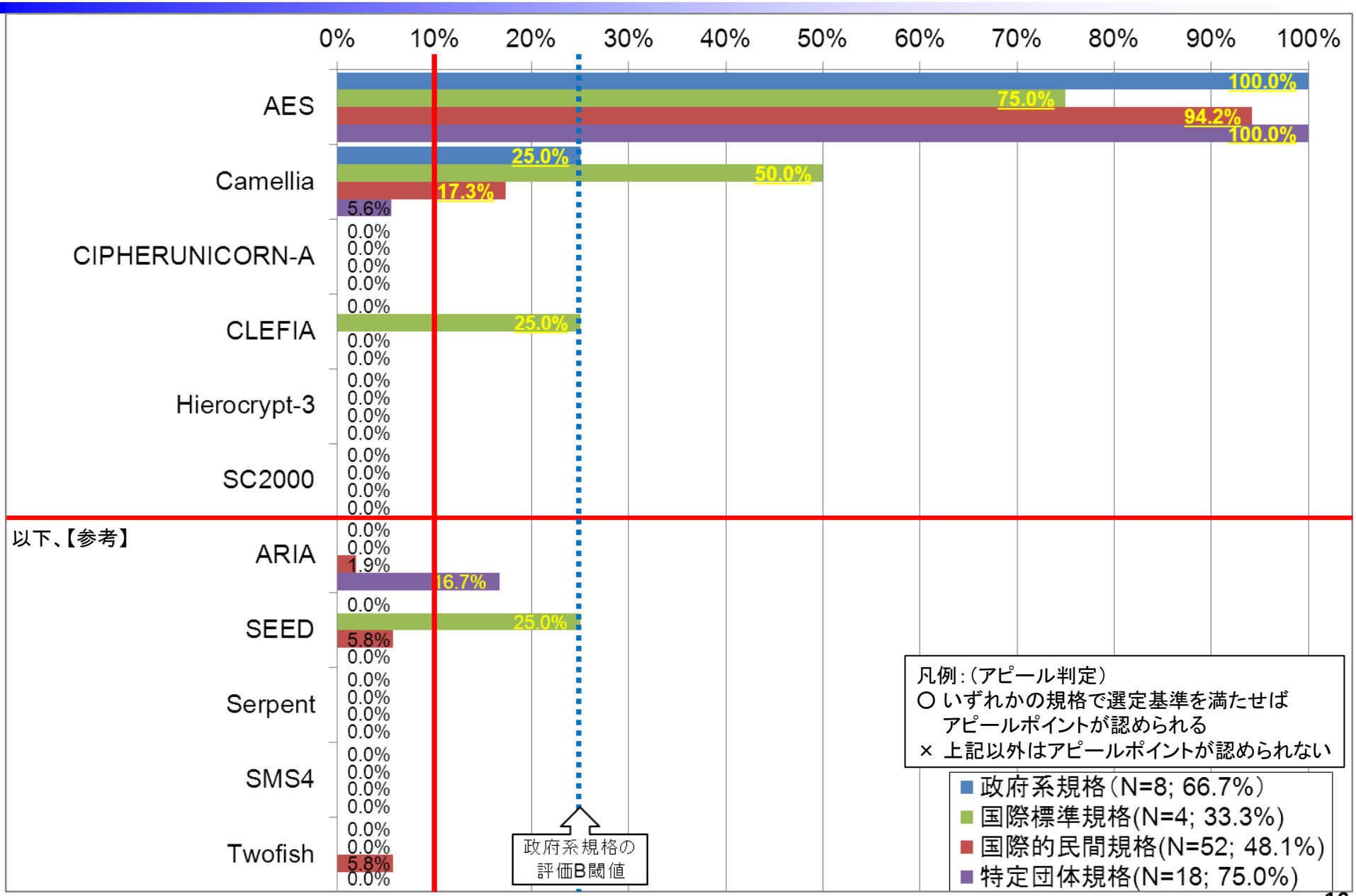
※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答された暗号アルゴリズムXXXであることに注意

標準化アピール結果 — 64ビットブロック暗号

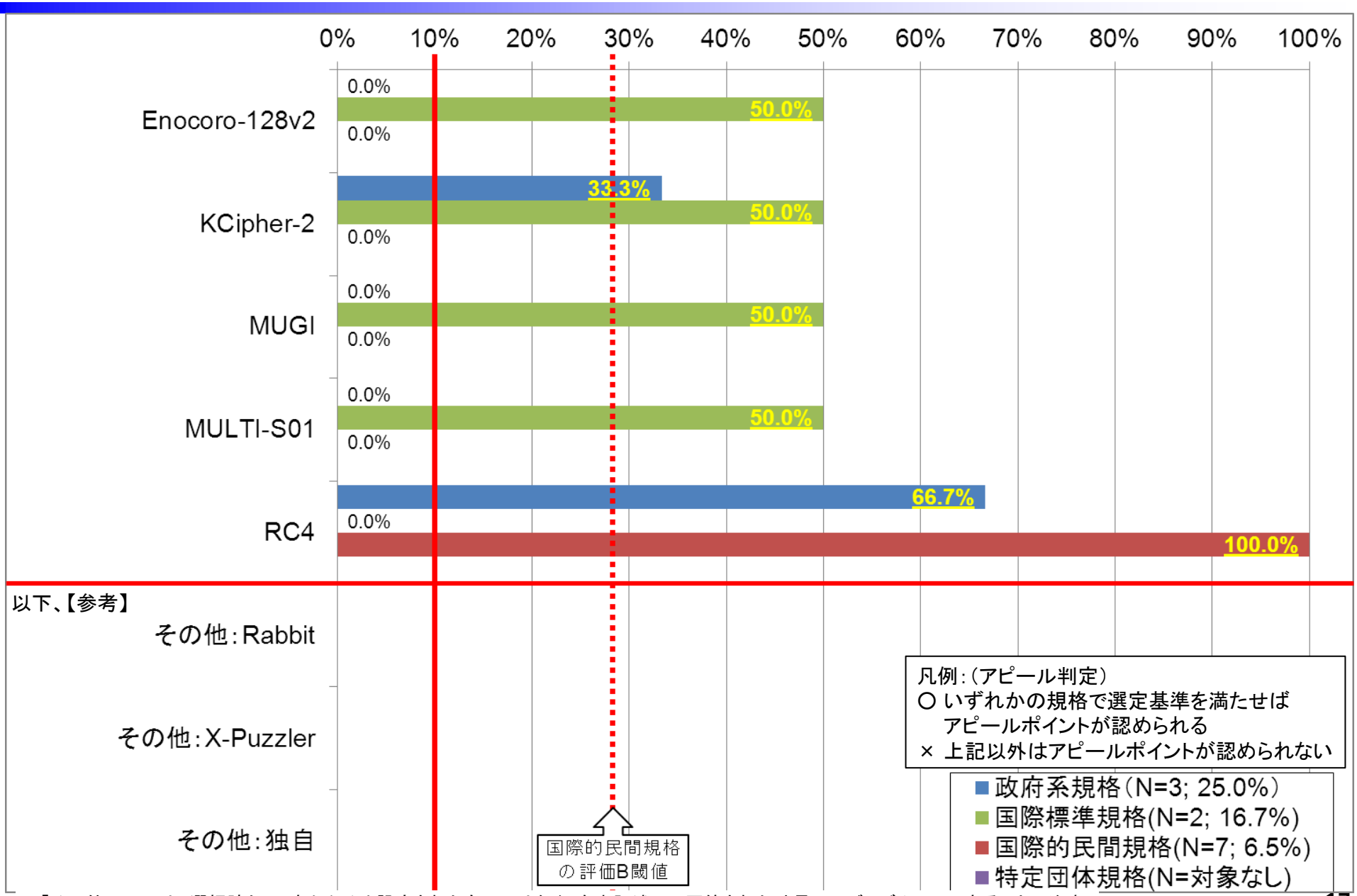


※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答された暗号アルゴリズムXXXであることに注意

標準化アピール結果 — 128ビットブロック暗号

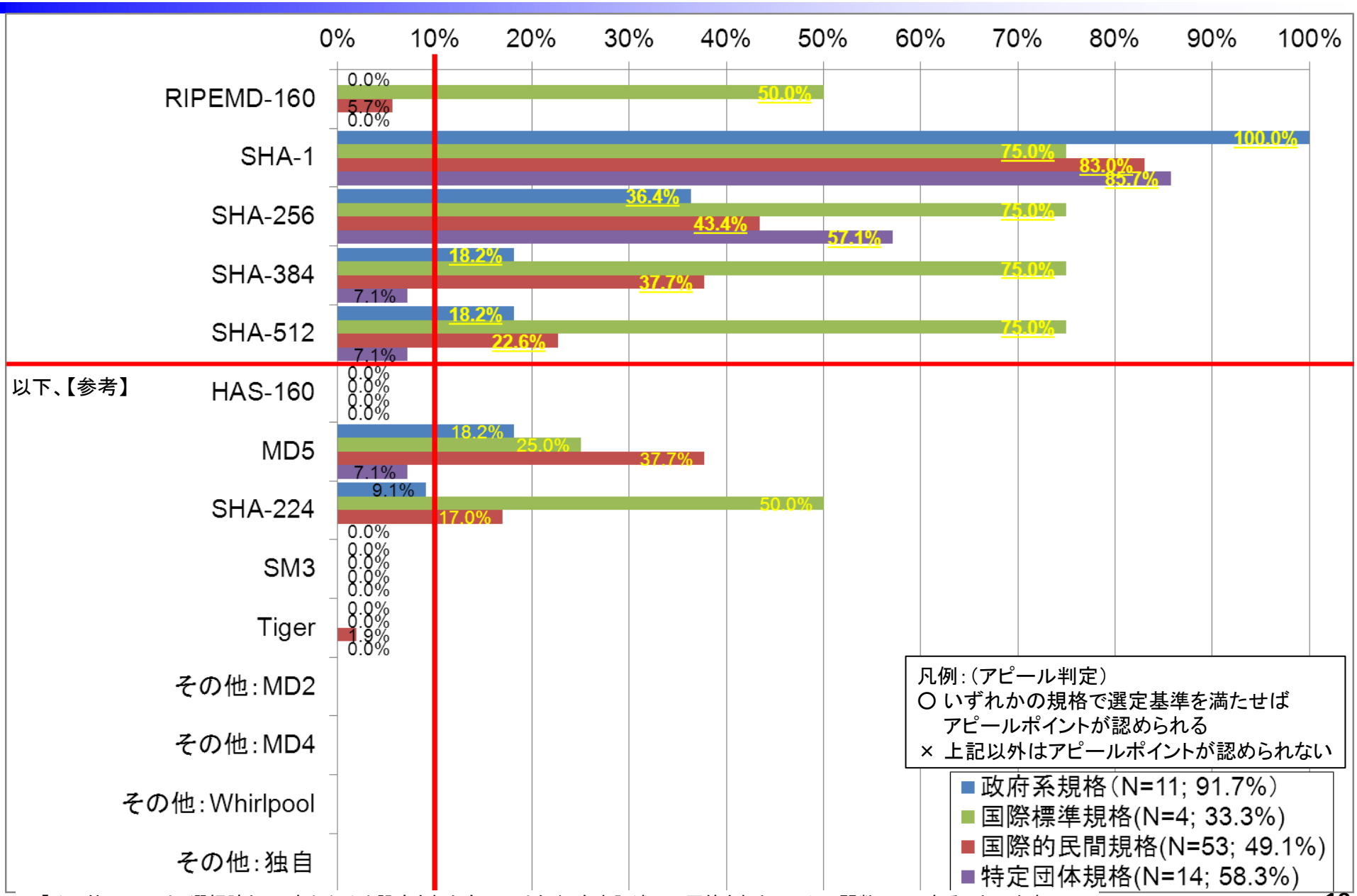


標準化アピール結果 — ストリーム暗号



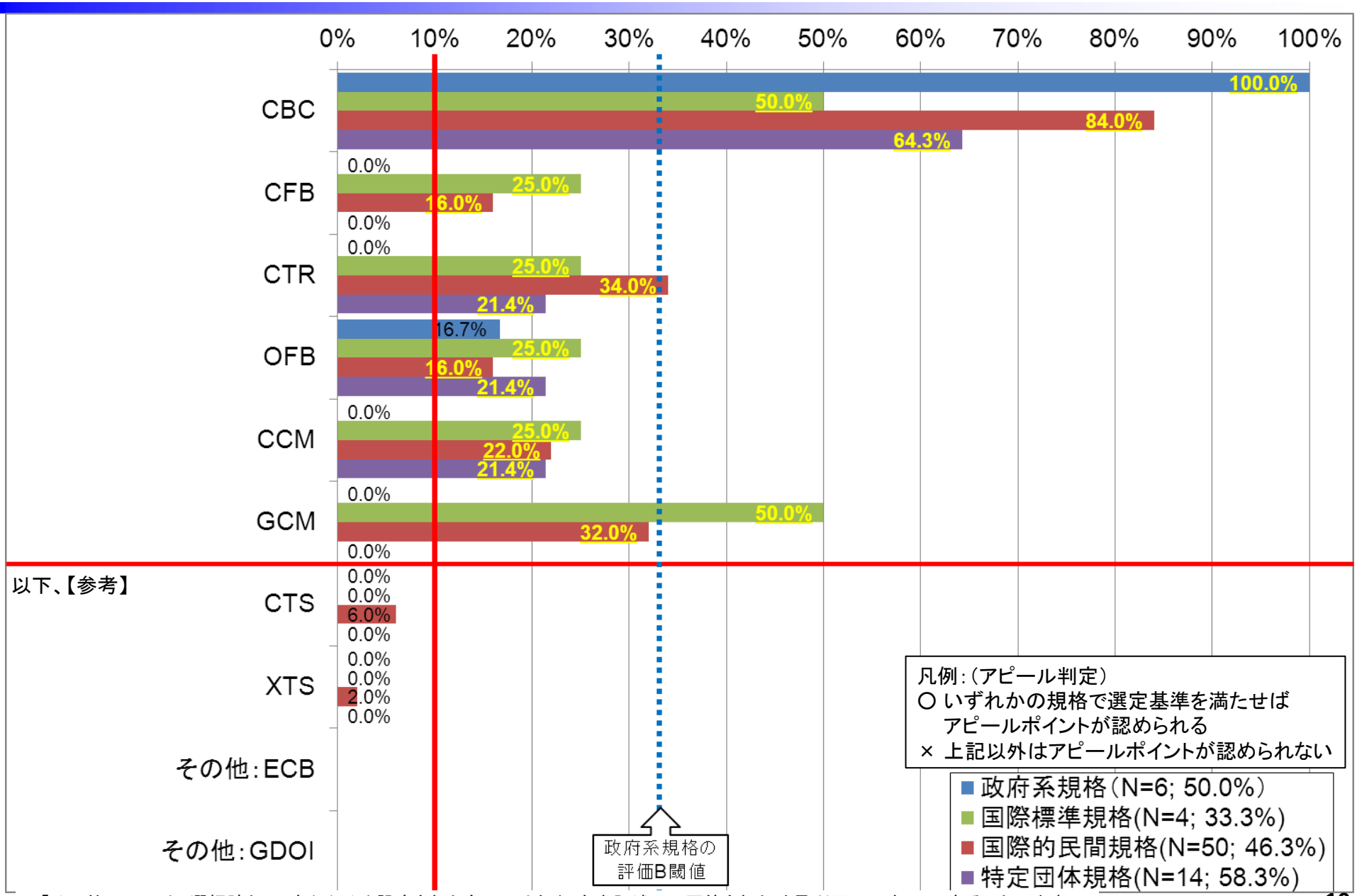
※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答された暗号アルゴリズムXXXであることに注意

標準化アピール結果 — ハッシュ関数



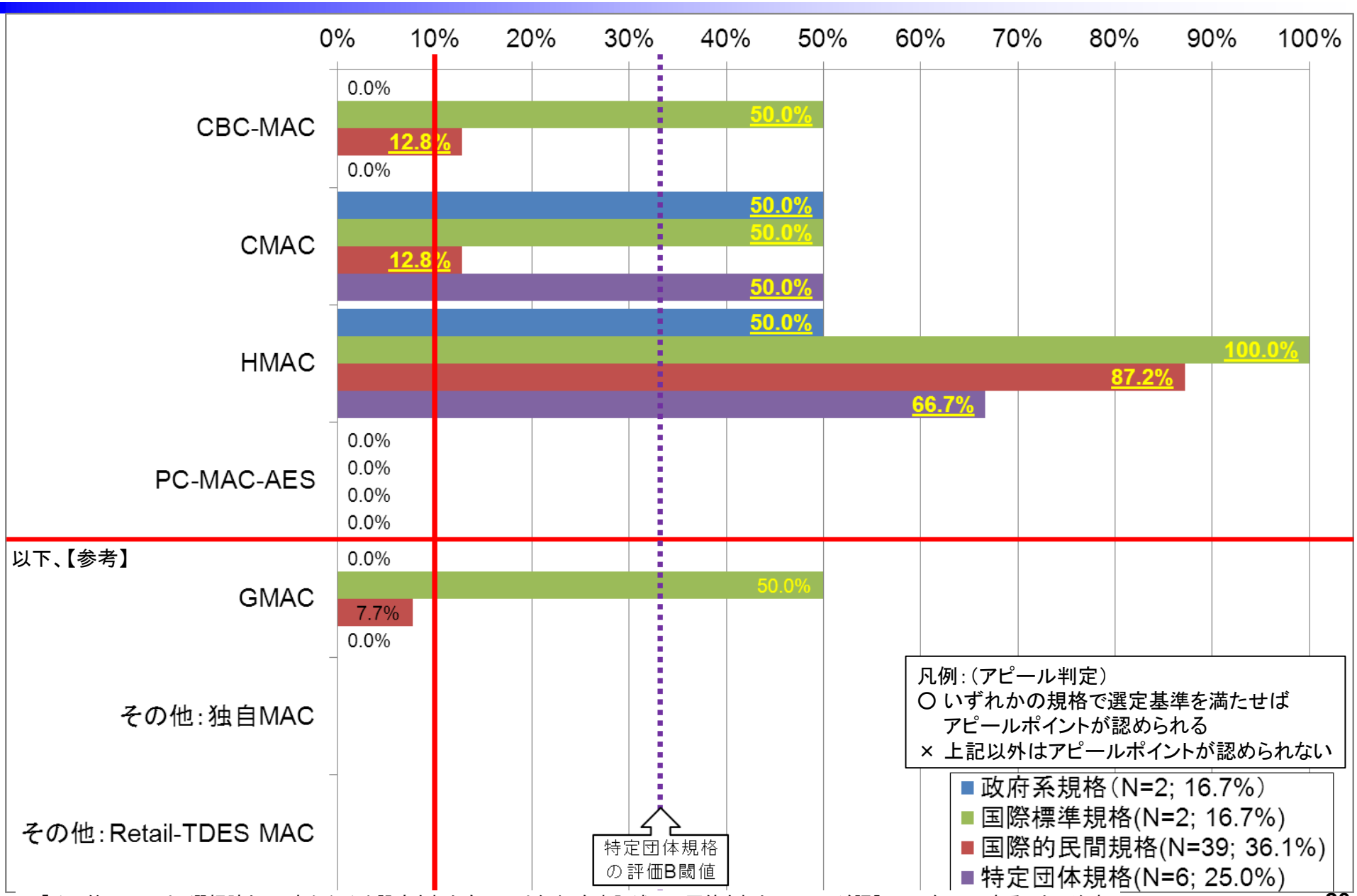
※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答されたハッシュ関数XXXであることに注意

標準化アピール結果 — 暗号利用モード



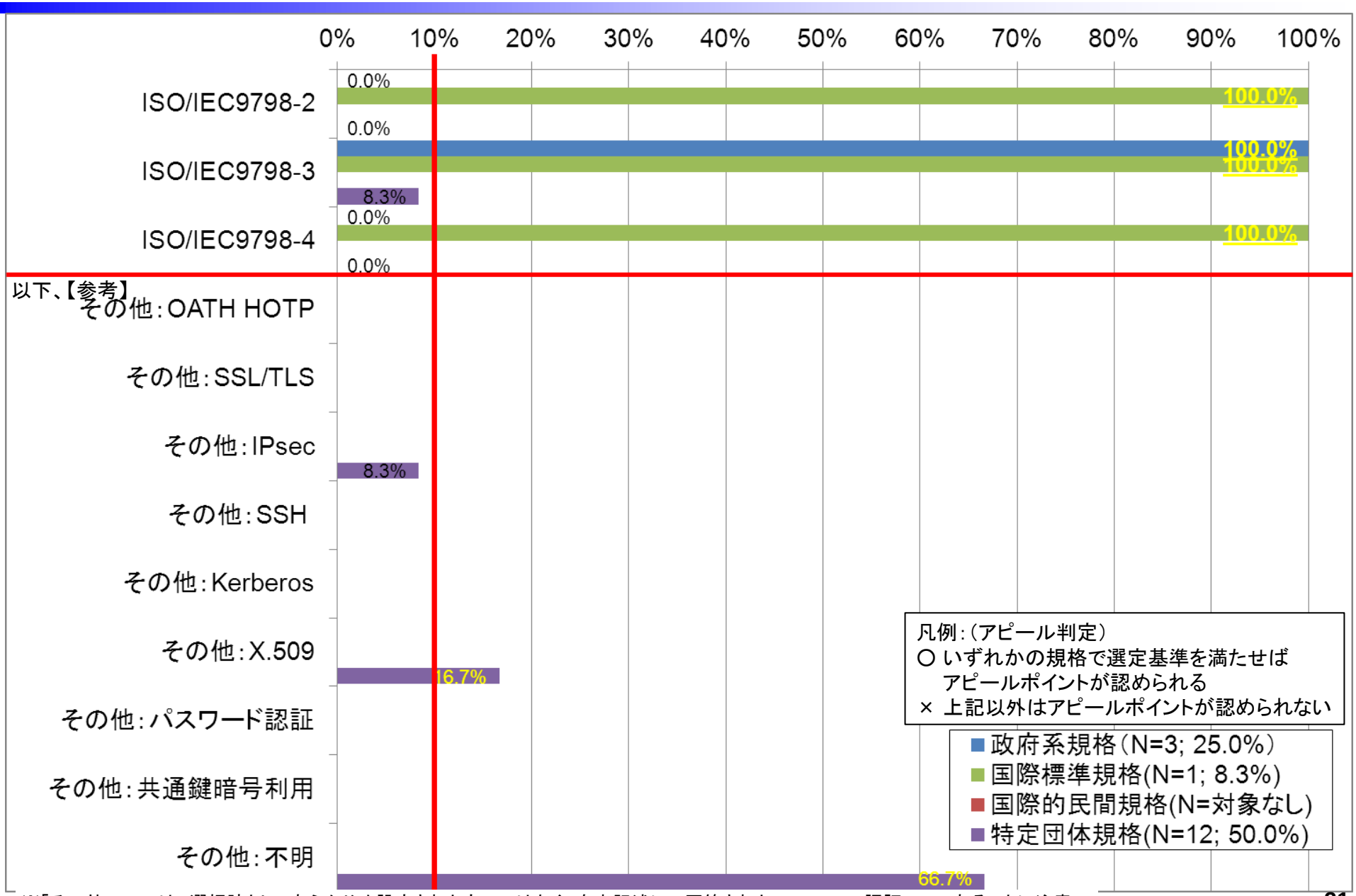
※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答された暗号利用モードXXXであることに注意

標準化アピール結果 — メッセージ認証コード



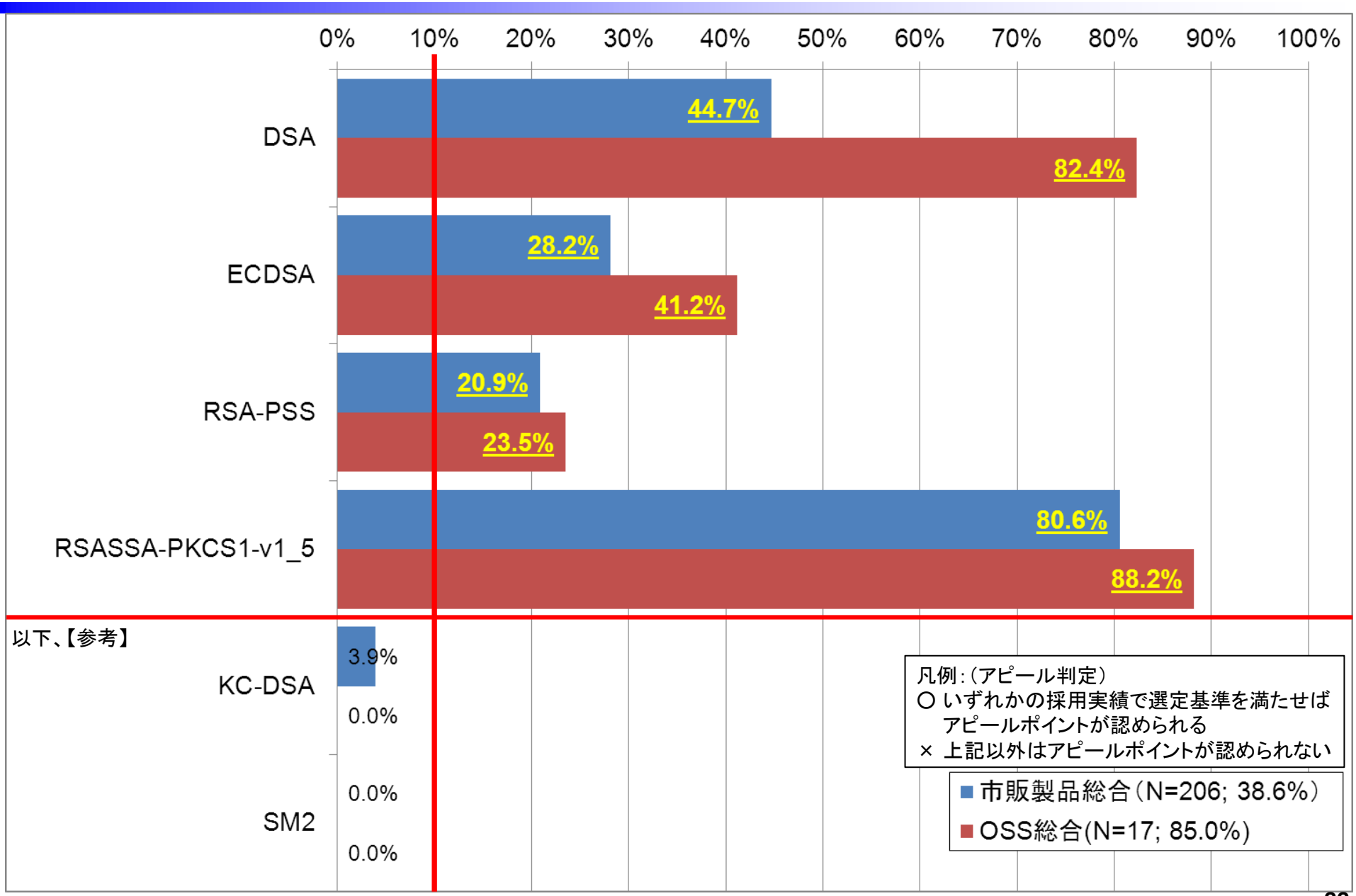
※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答されたメッセージ認証コードXXXであることに注意

標準化アピール結果 — エンティティ認証

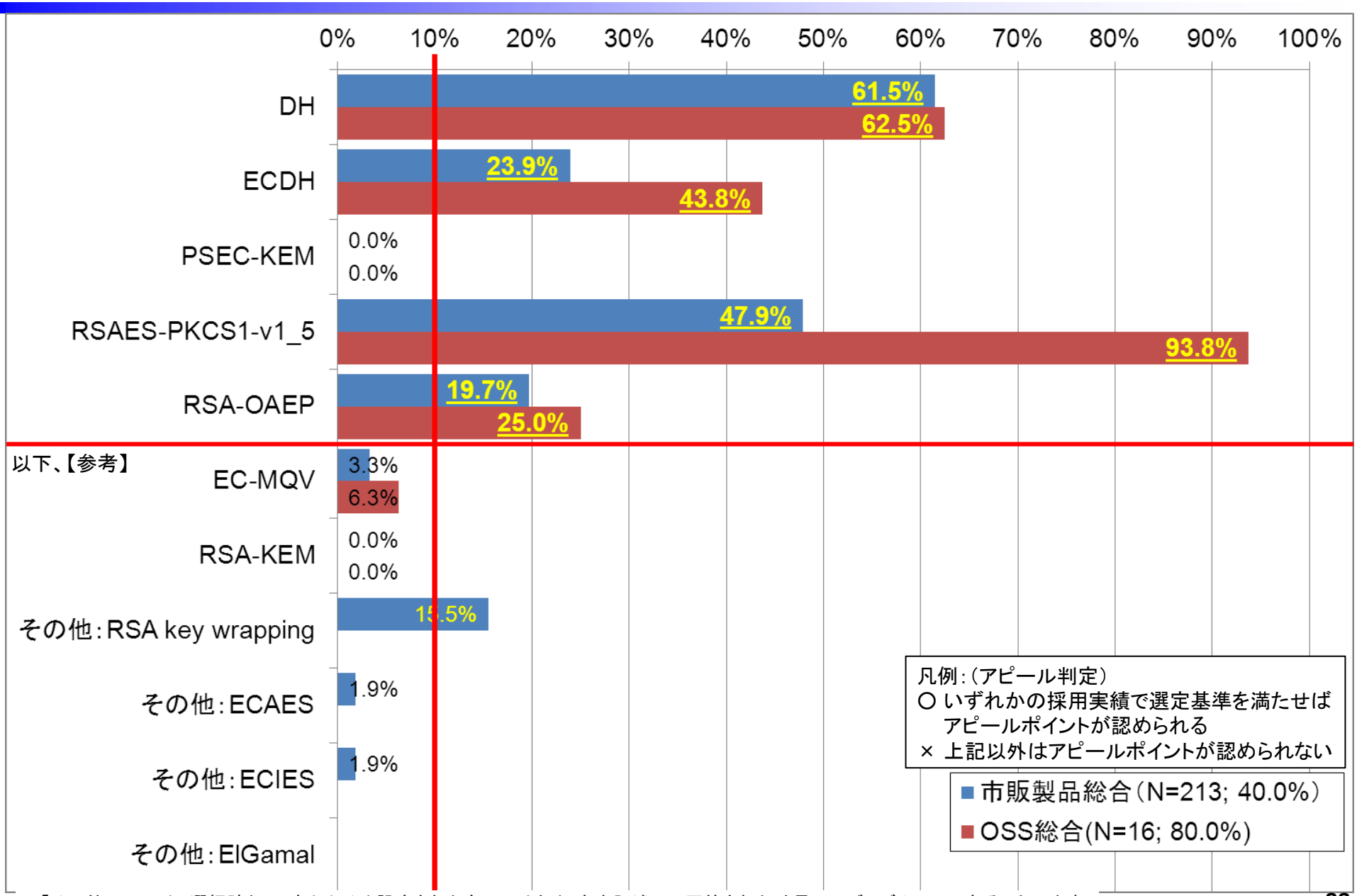


※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答されたエンティティ認証XXXであることに注意

採用アピール結果 — 署名

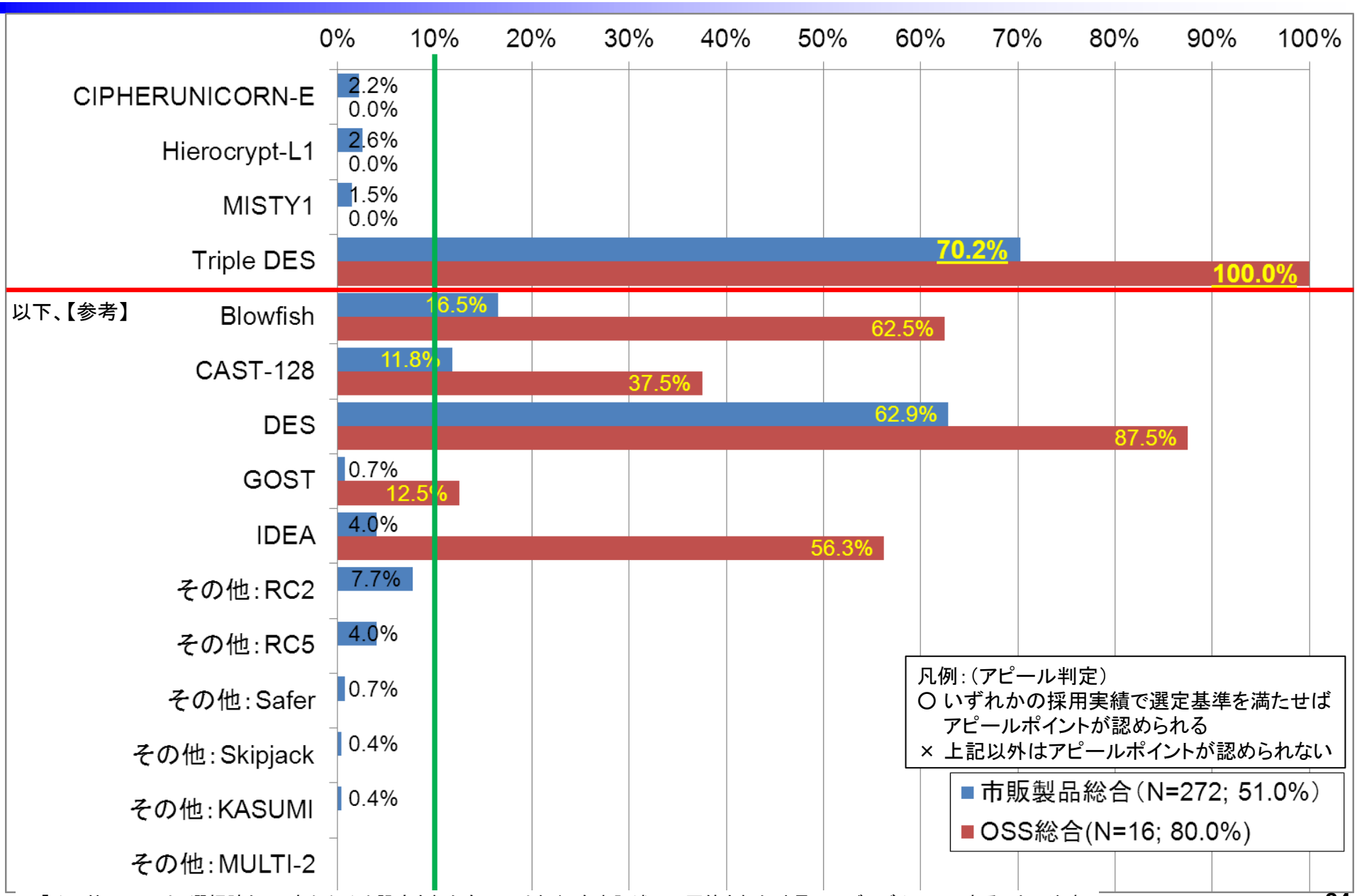

0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
DSA
44.7%
82.4%
ECDSA
28.2%
41.2%
RSA-PSS
20.9%
23.5%
RSASSA-PKCS1-v1_5
80.6%
88.2%
以下、【参考】
KC-DSA
3.9%
0.0%
SM2
0.0%
0.0%
凡例：（アピール判定）
○ いずれかの採用実績で選定基準を満たせばアピールポイントが認められる
× 上記以外はアピールポイントが認められない
市販製品総合（N=206; 38.6%）
OSS総合(N=17; 85.0%)

採用アピール結果 — 守秘・鍵共有



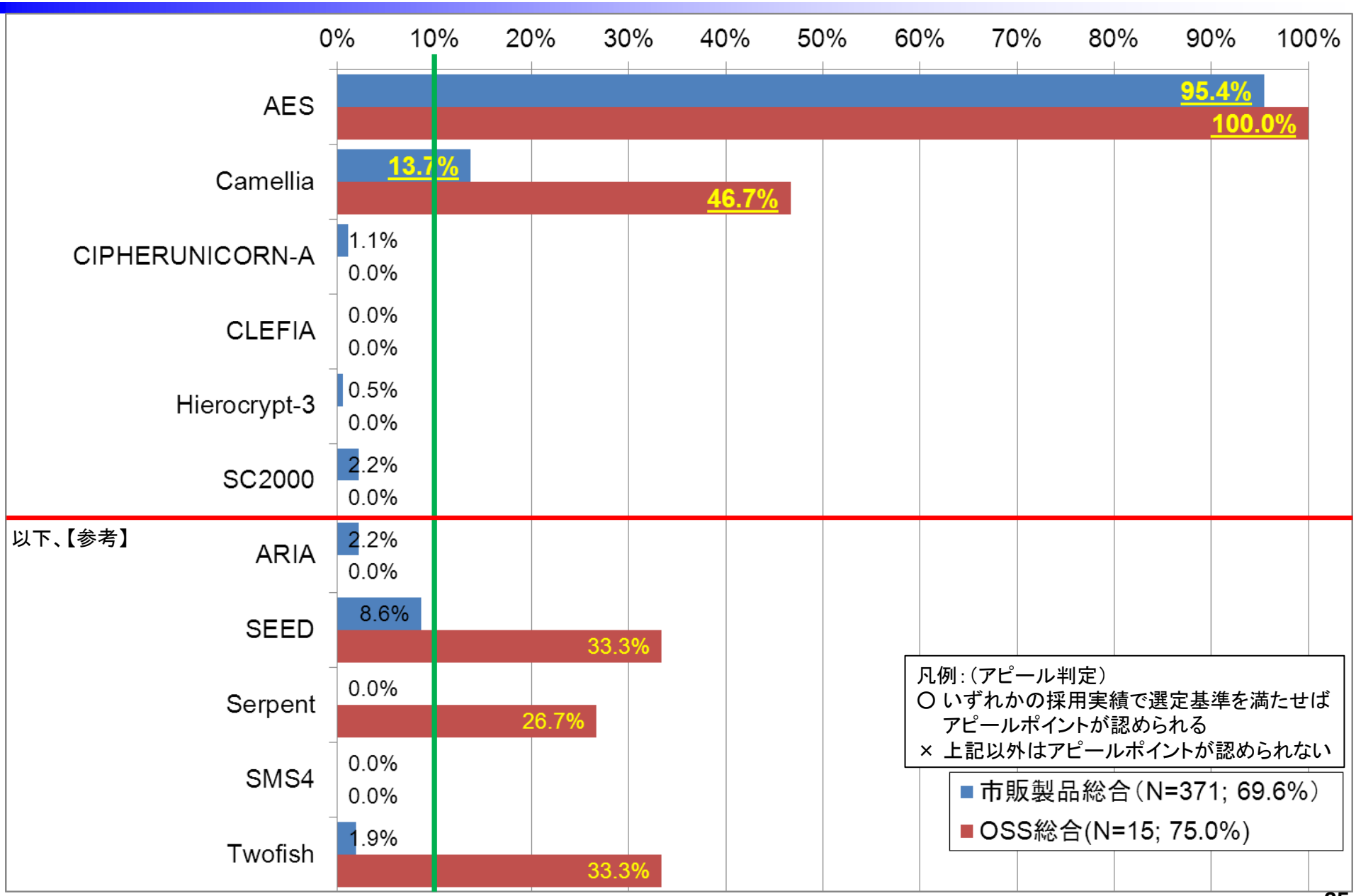
※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答された暗号アルゴリズムXXXであることに注意

採用アピール結果 — 64ビットブロック暗号

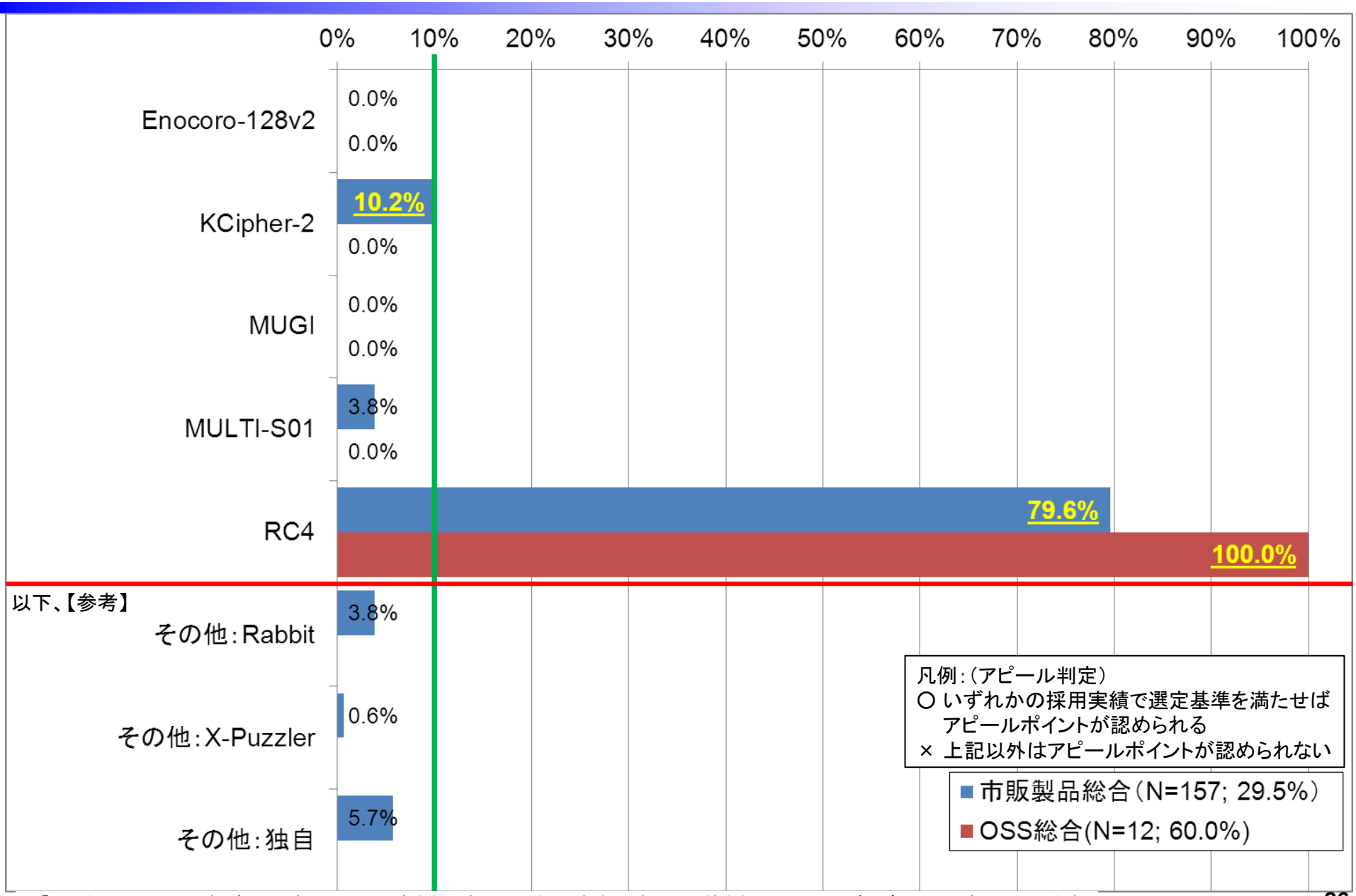


※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答された暗号アルゴリズムXXXであることに注意

採用アピール結果 — 128ビットブロック暗号

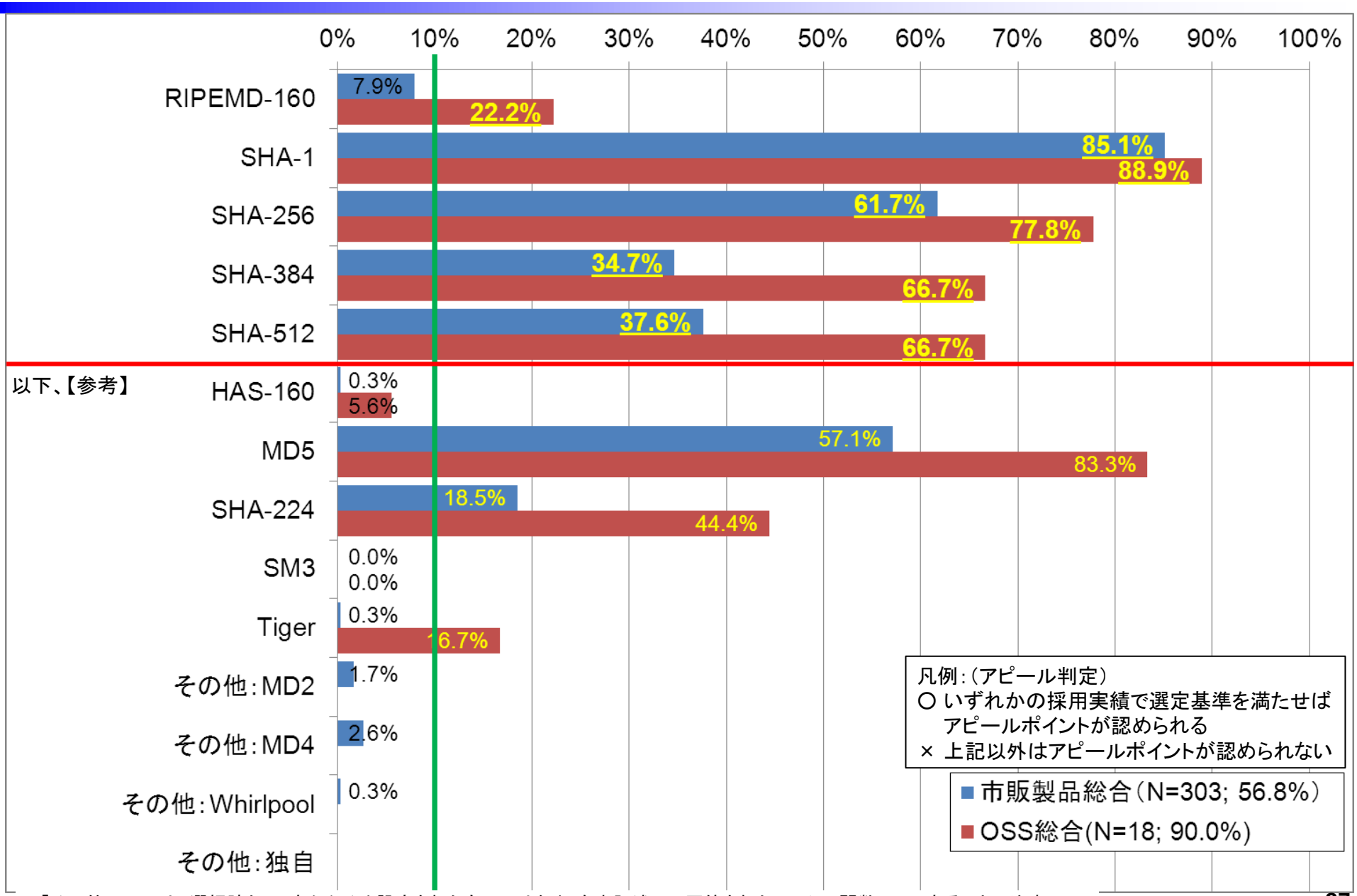


採用アピール結果 — ストリーム暗号



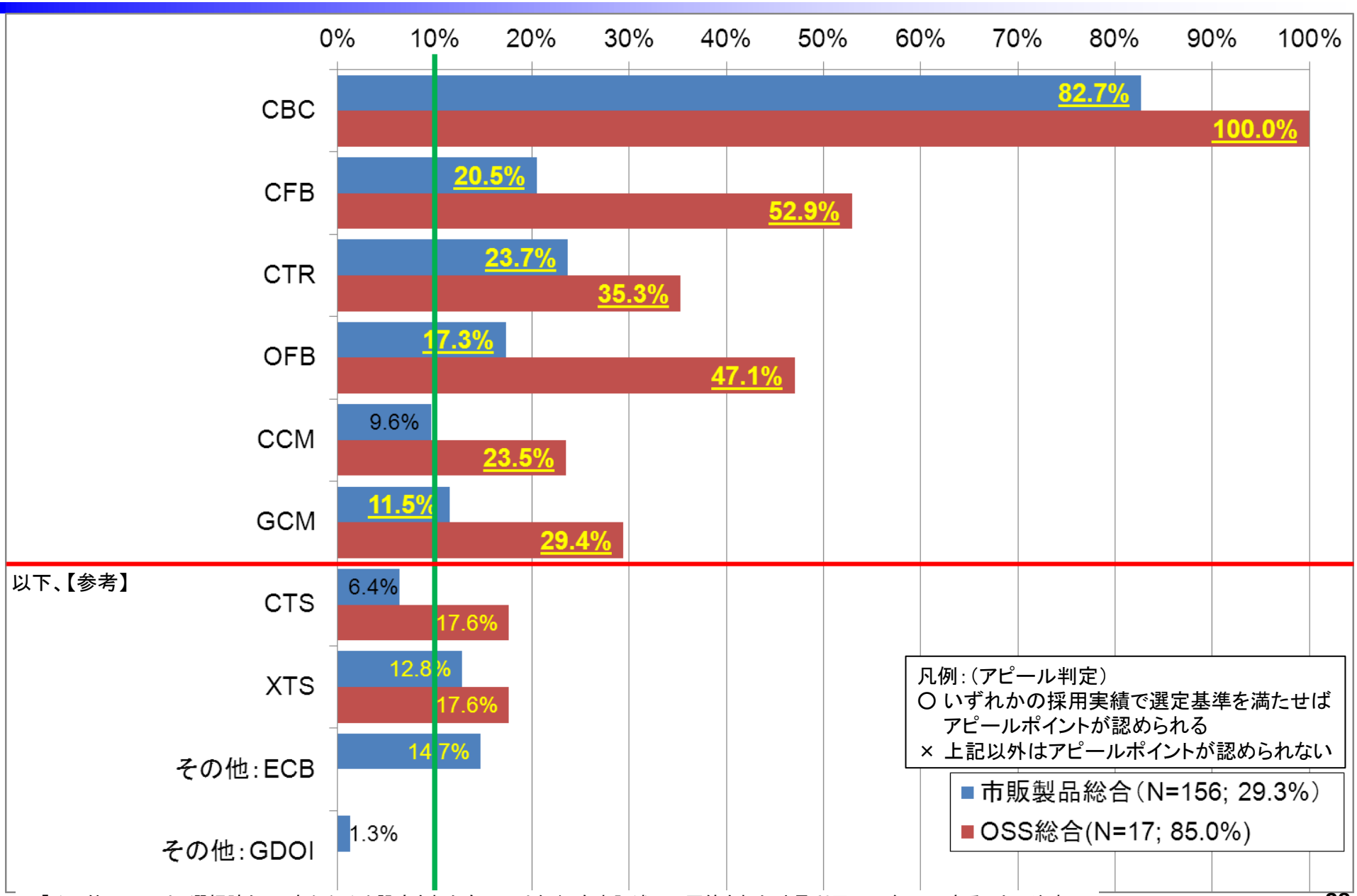
※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答された暗号アルゴリズムXXXであることに注意

採用アピール結果 — ハッシュ関数



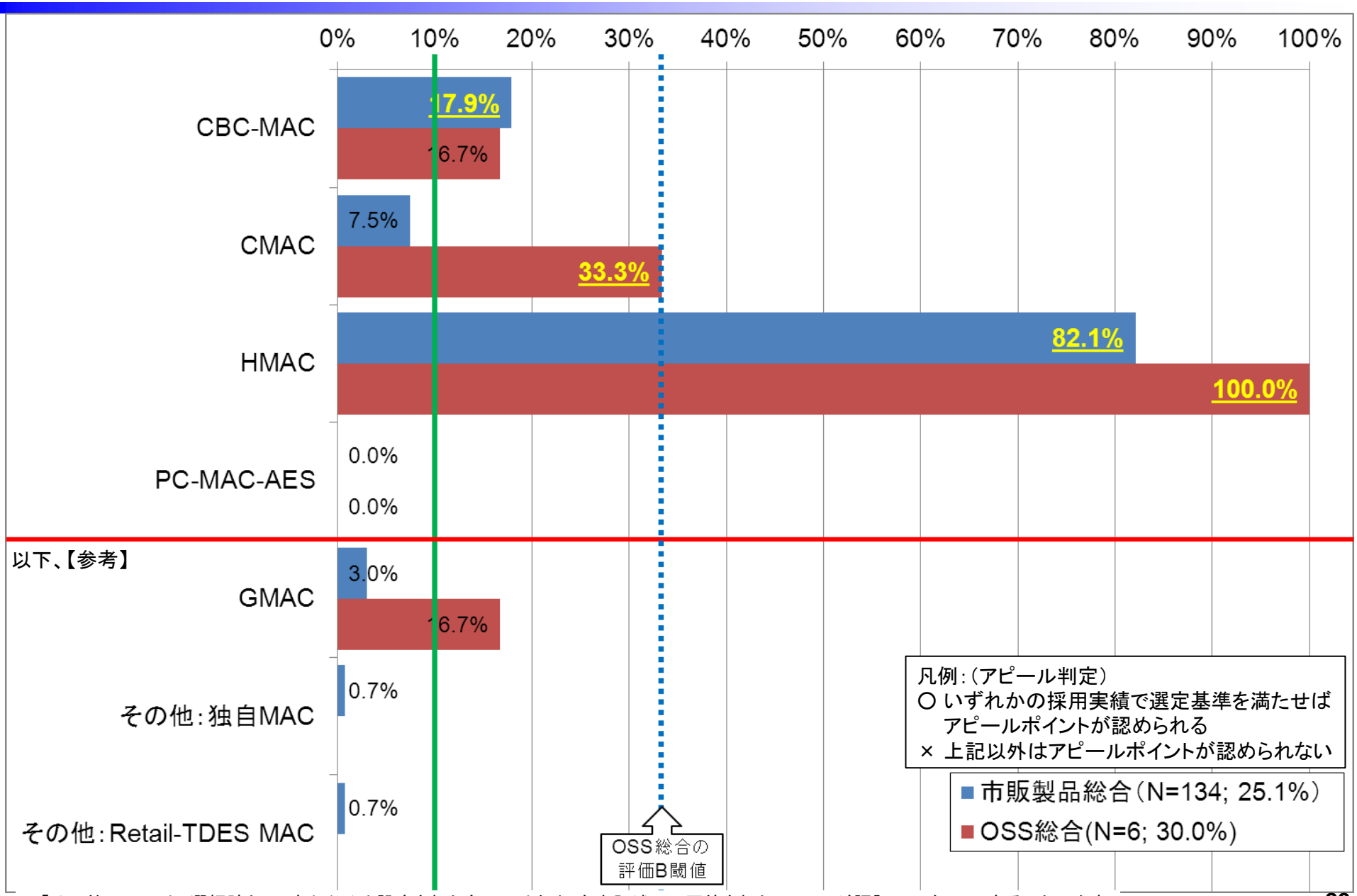
※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答されたハッシュ関数XXXであることに注意

採用アピール結果 — 暗号利用モード



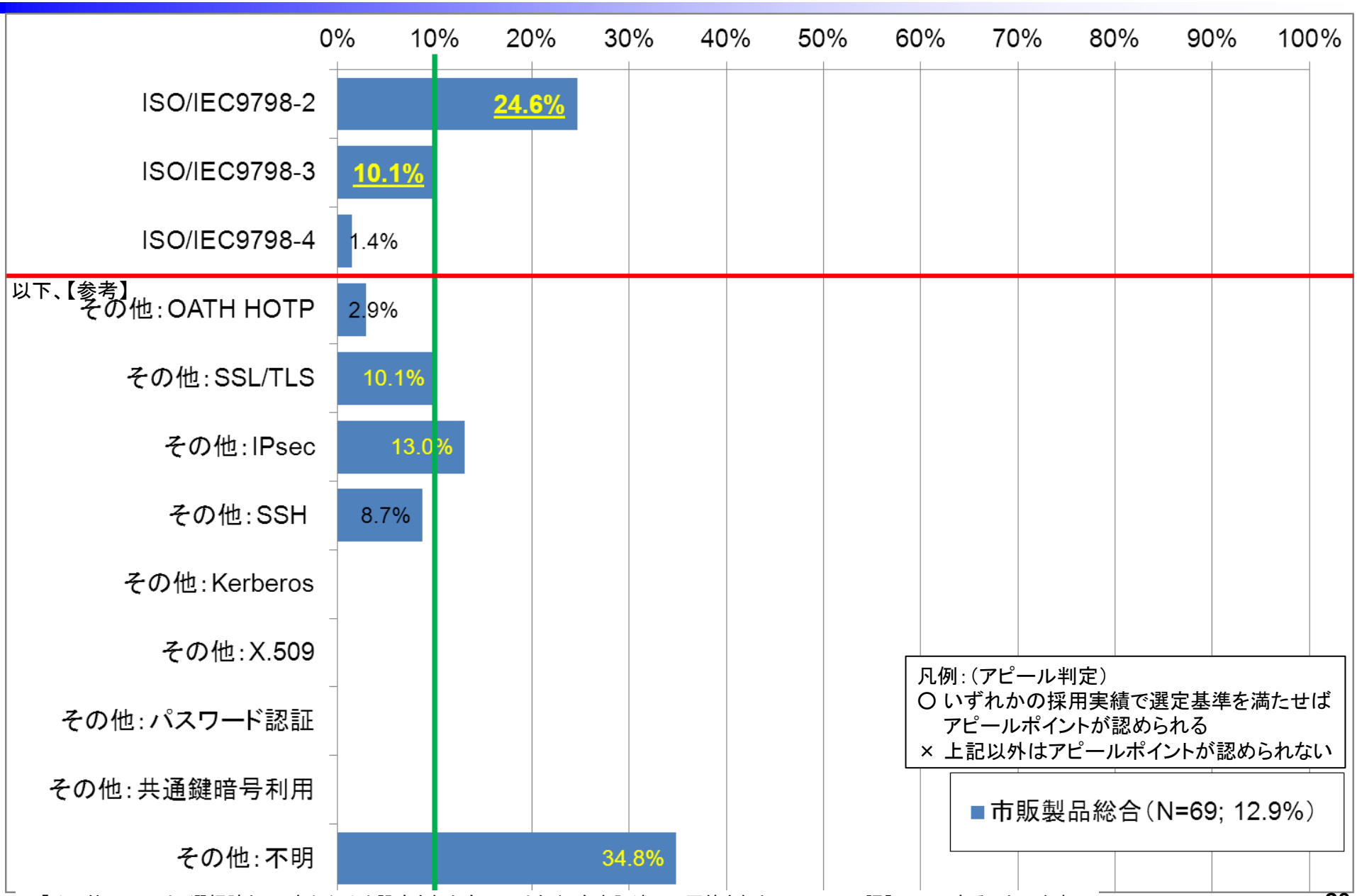
※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答された暗号利用モードXXXであることに注意

採用アピール結果 ― 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

採用アピール結果 ― 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

「実装コスト低減を図るハードルの低さ」の判定

		判定結果	P.32-40 市販暗号モジュール	P.32-40 OSS暗号モジュール
署名	ECDSA	○	○	○
	RSA-PSS	○	○	○
守秘・鍵共有	ECDH	○	○	○
	PSEC-KEM	×	×	×
	RSA-OAEP	○	○	○
64ビットブロック暗号	CIPHERUNICORN-E	×	×	×
	Hierocrypt-L1	×	×	×
	MISTY1	×	×	×
128ビットブロック暗号	Camellia	○	○	○
	CIPHERUNICORN-A	×	×	×
	CLEFIA	×	×	×
	Hierocrypt-3	×	×	×
	SC2000	×	×	×
ストリーム暗号	Enocoro-128v2	×	×	×
	KCipher-2	×	×	×
	MUGI	×	×	×
	MULTI-S01	×	×	×

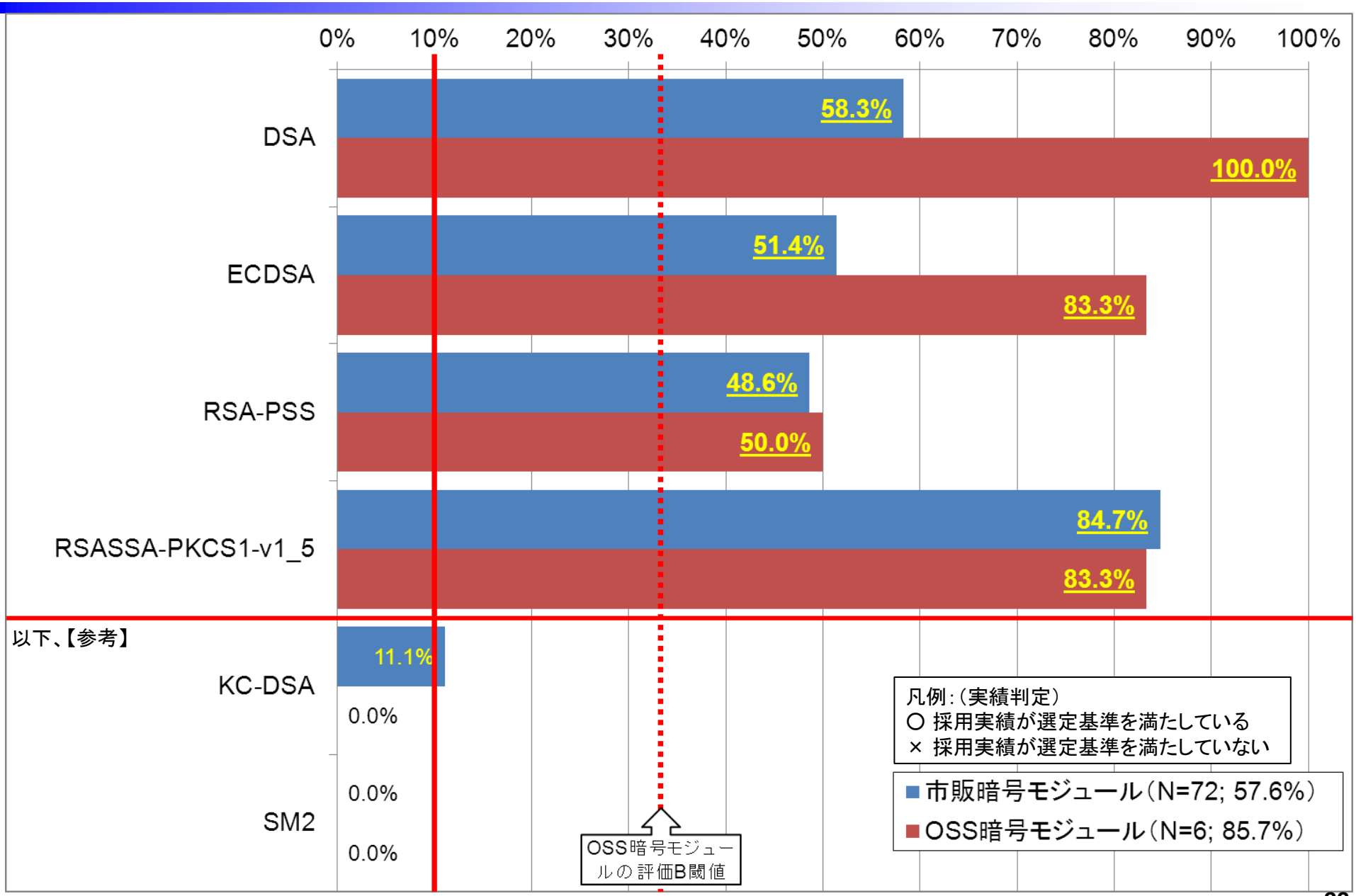
		判定結果	P.32-40 市販暗号モジュール	P.32-40 OSS暗号モジュール
ハッシュ関数	SHA-256	○	○	○
	SHA-384	○	○	○
	SHA-512	○	○	○
暗号利用モード（秘匿）	CFB	○	○	○
	OFB	○	○	○
	CTR	○	○	○
暗号利用モード（秘匿・認証付）	CCM	○	○	○
	GCM	○	○	○
メッセージ認証コード	CMAC	○	○	○
	PC-MAC-AES	×	×	×
エンティティ認証	ISO/IEC9798-2	○	○	該当なし
	ISO/IEC9798-3	×	×	該当なし
	ISO/IEC9798-4	×	×	該当なし

2つの実績判定のOR条件で総合判定

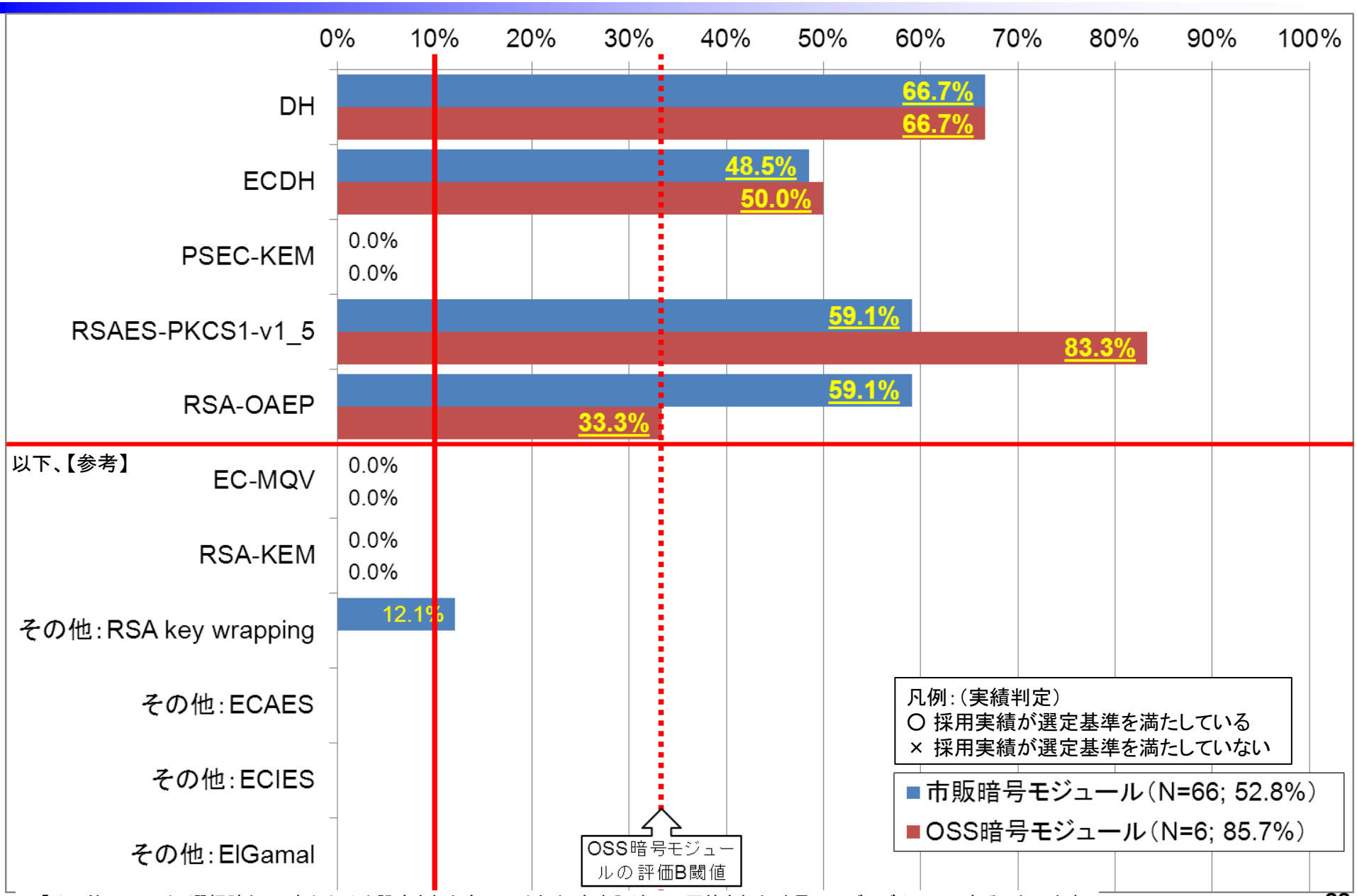
凡例：（実績判定） ○ 採用実績が選定基準を満たしている
× 採用実績が選定基準を満たしていない

閾値10%は越えているが、提案会社・グループ会社以外での採用実績が認められなかった

暗号モジュールアピール結果 — 署名

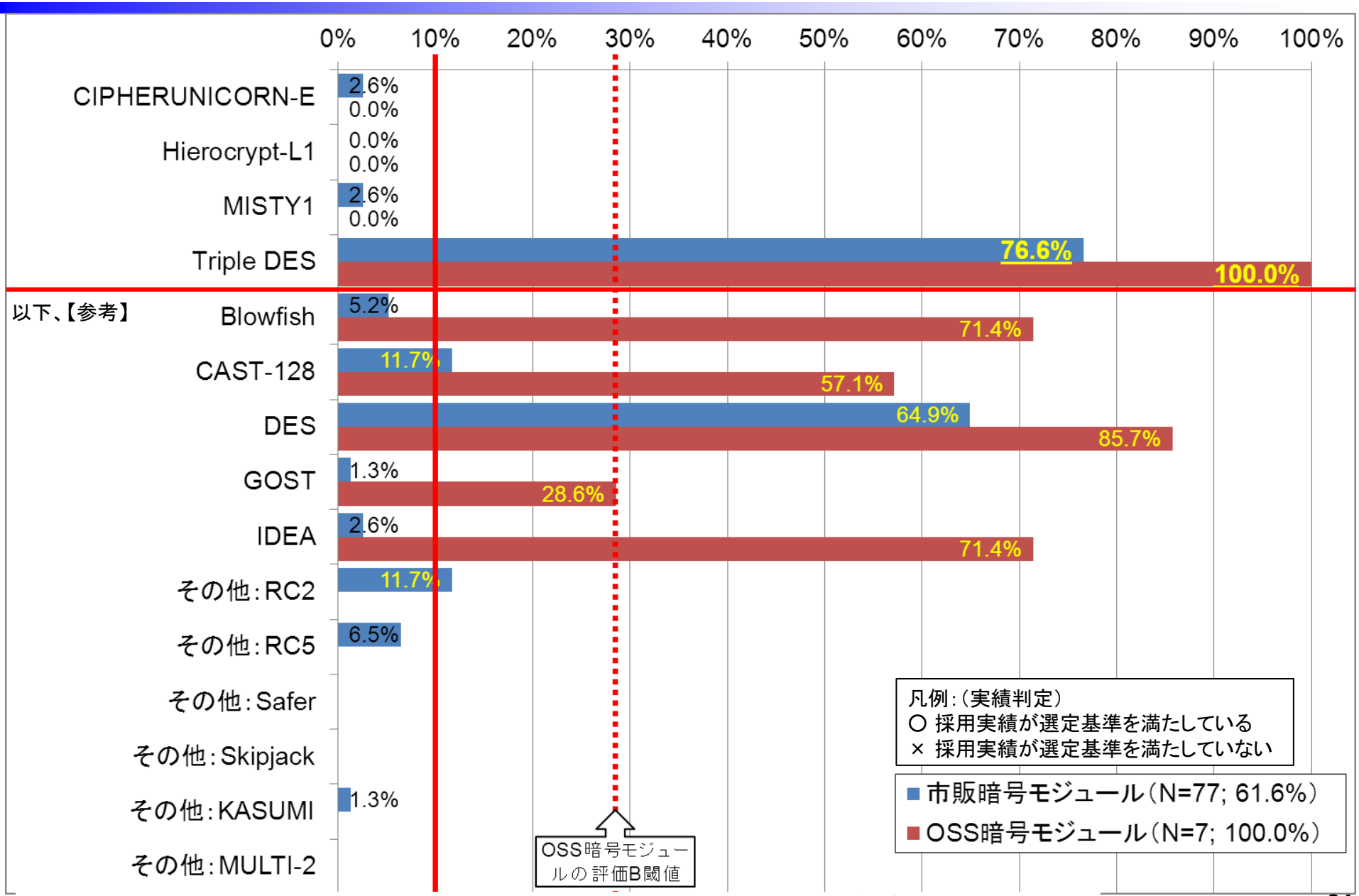


暗号モジュールアピール結果 — 守秘・鍵共有



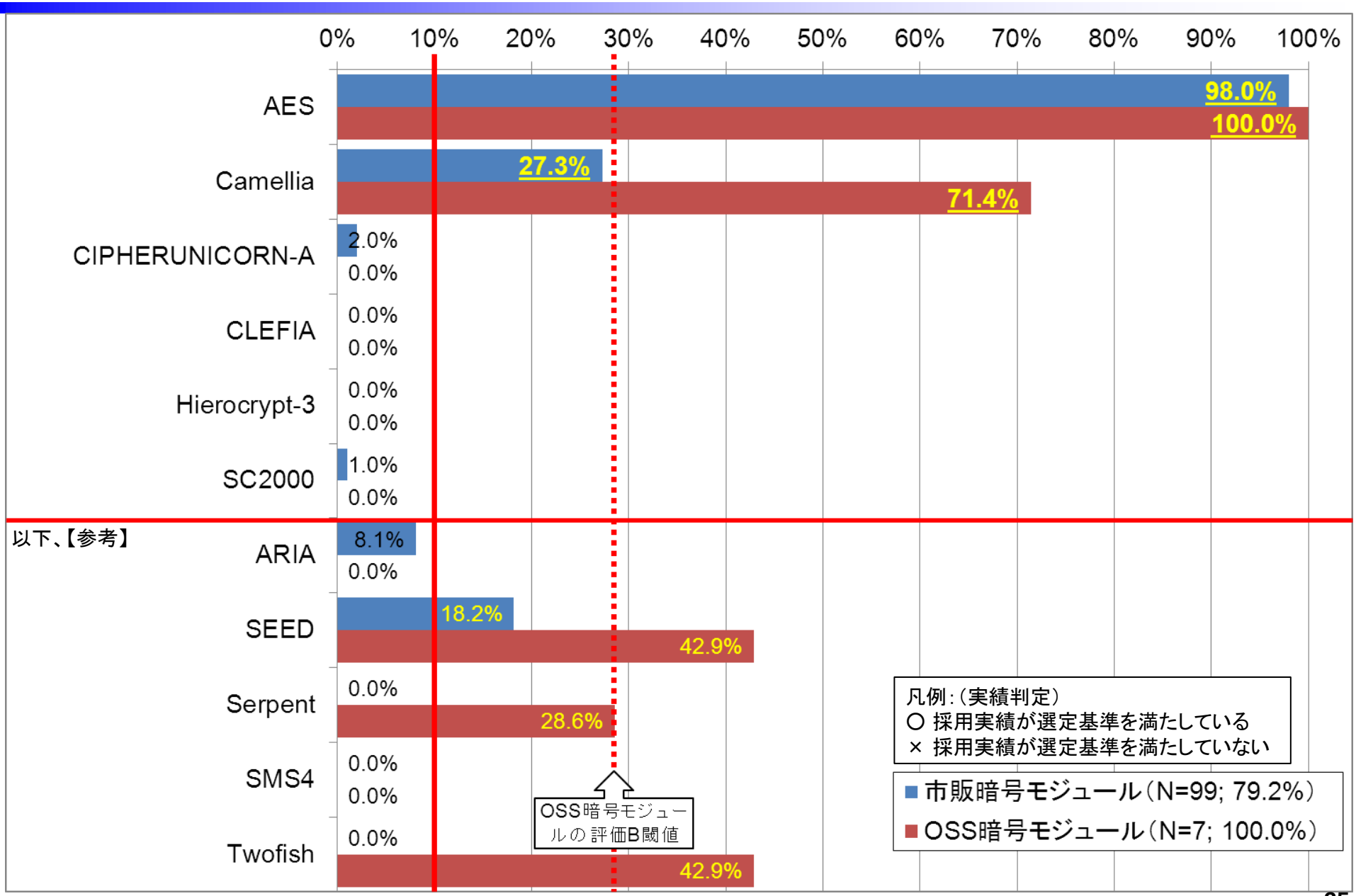
※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答された暗号アルゴリズムXXXであることに注意

暗号モジュールアピール結果 — 64ビットブロック暗号

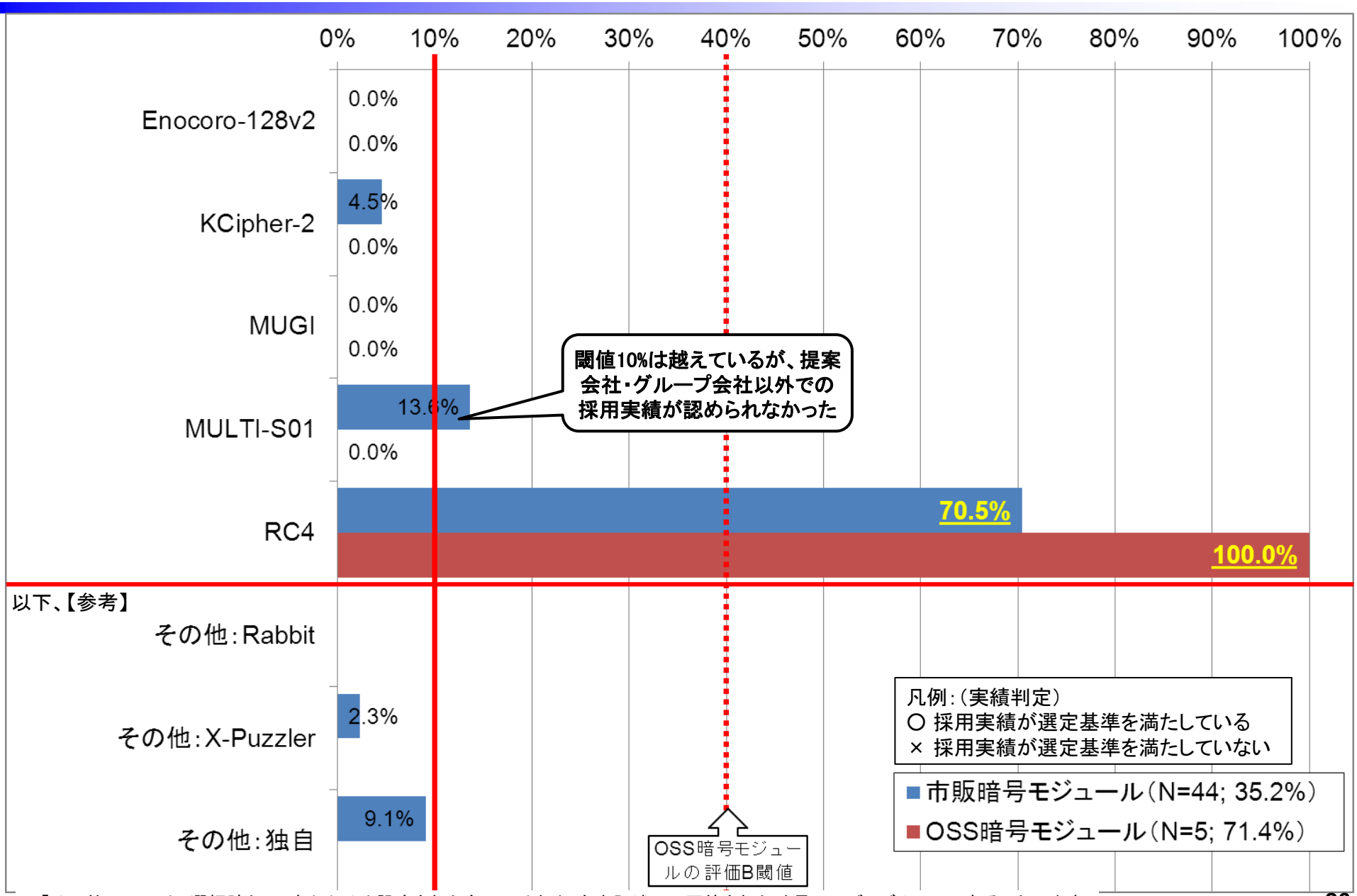


※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答された暗号アルゴリズムXXXであることに注意

暗号モジュールアピール結果 — 128ビットブロック暗号

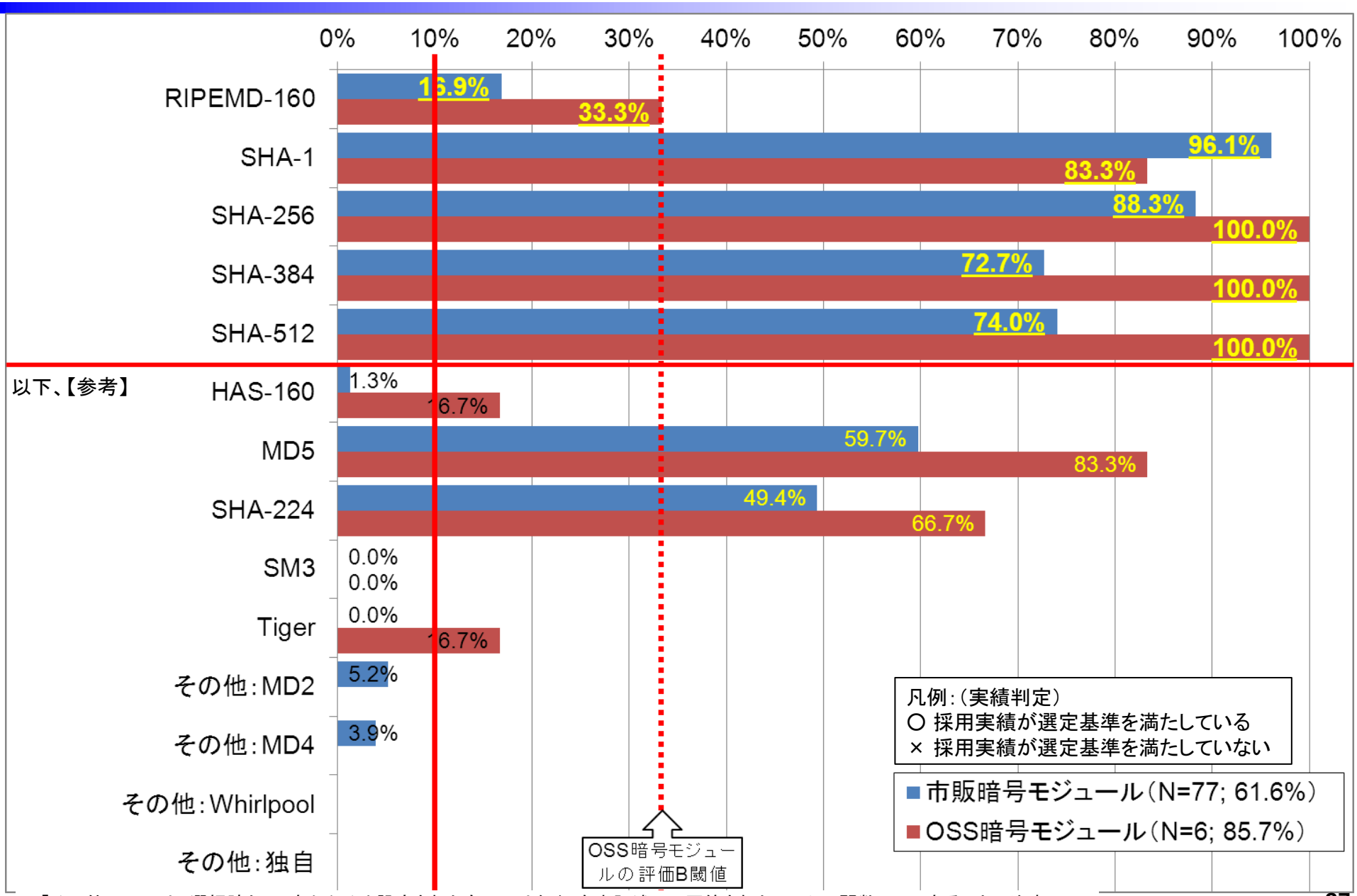


暗号モジュールアピール結果 ― ストリーム暗号



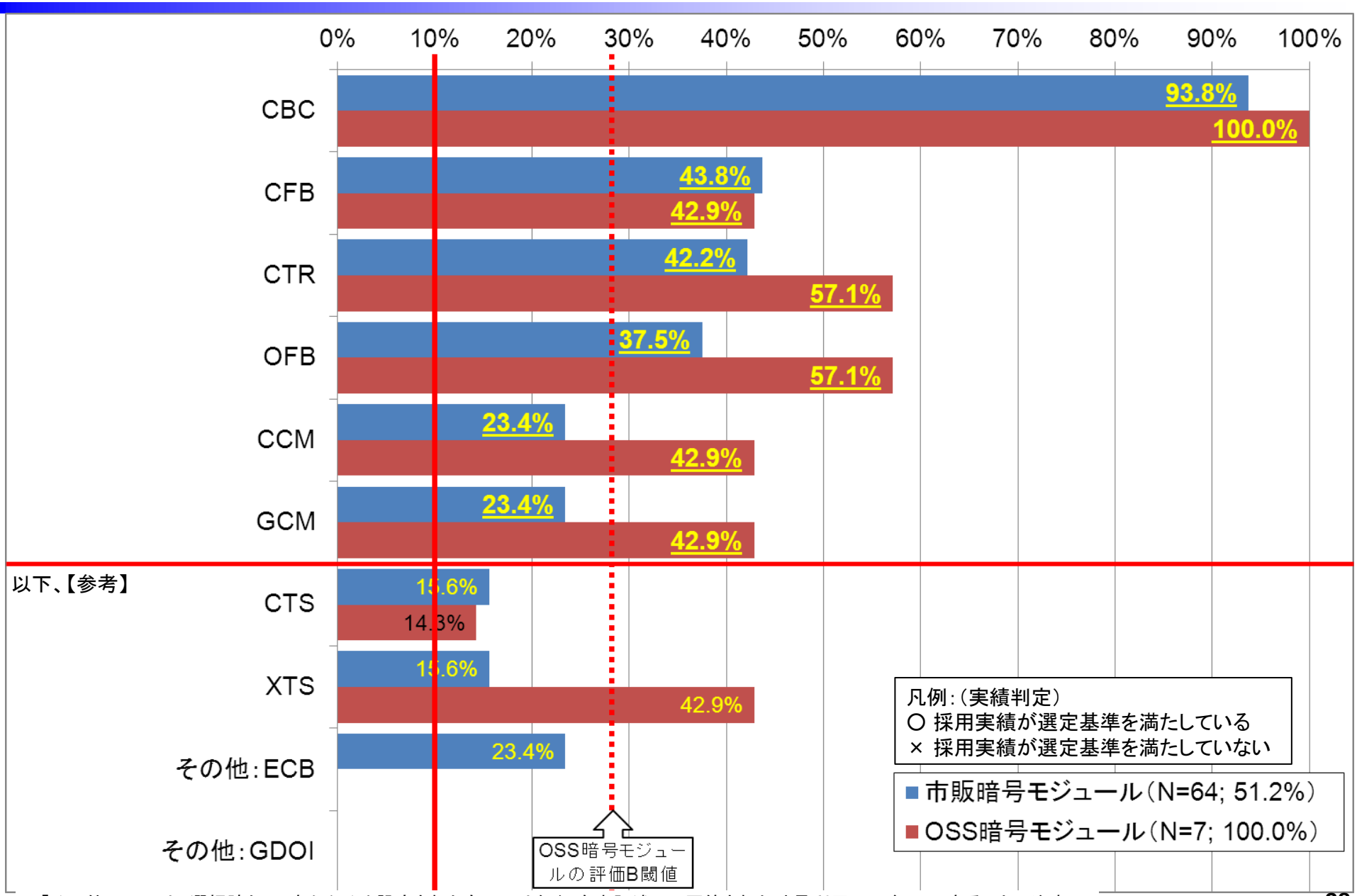
※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答された暗号アルゴリズムXXXであることに注意

暗号モジュールアピール結果 ― ハッシュ関数



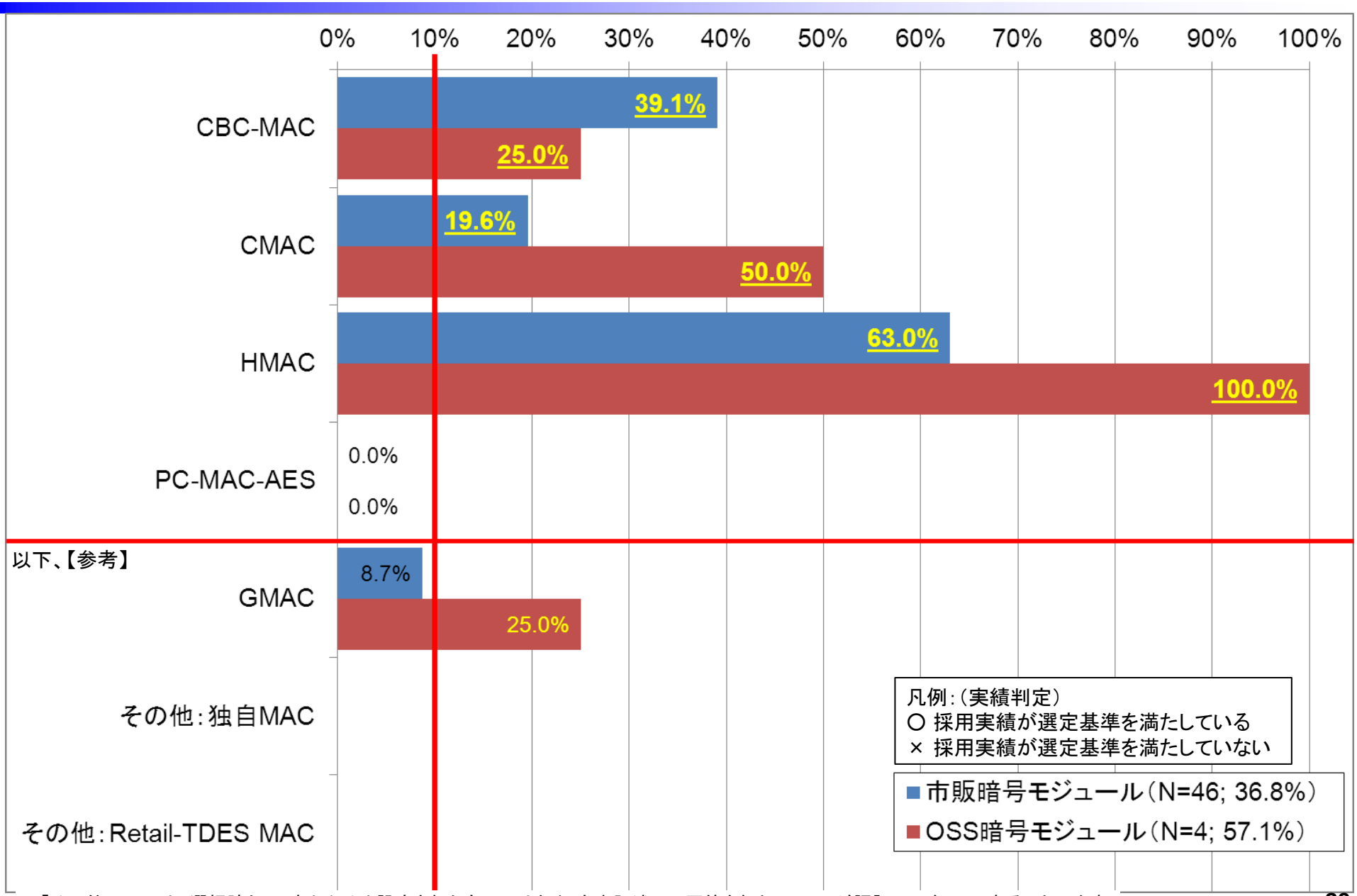
※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答されたハッシュ関数XXXであることに注意

暗号モジュールアピール結果 ― 暗号利用モード



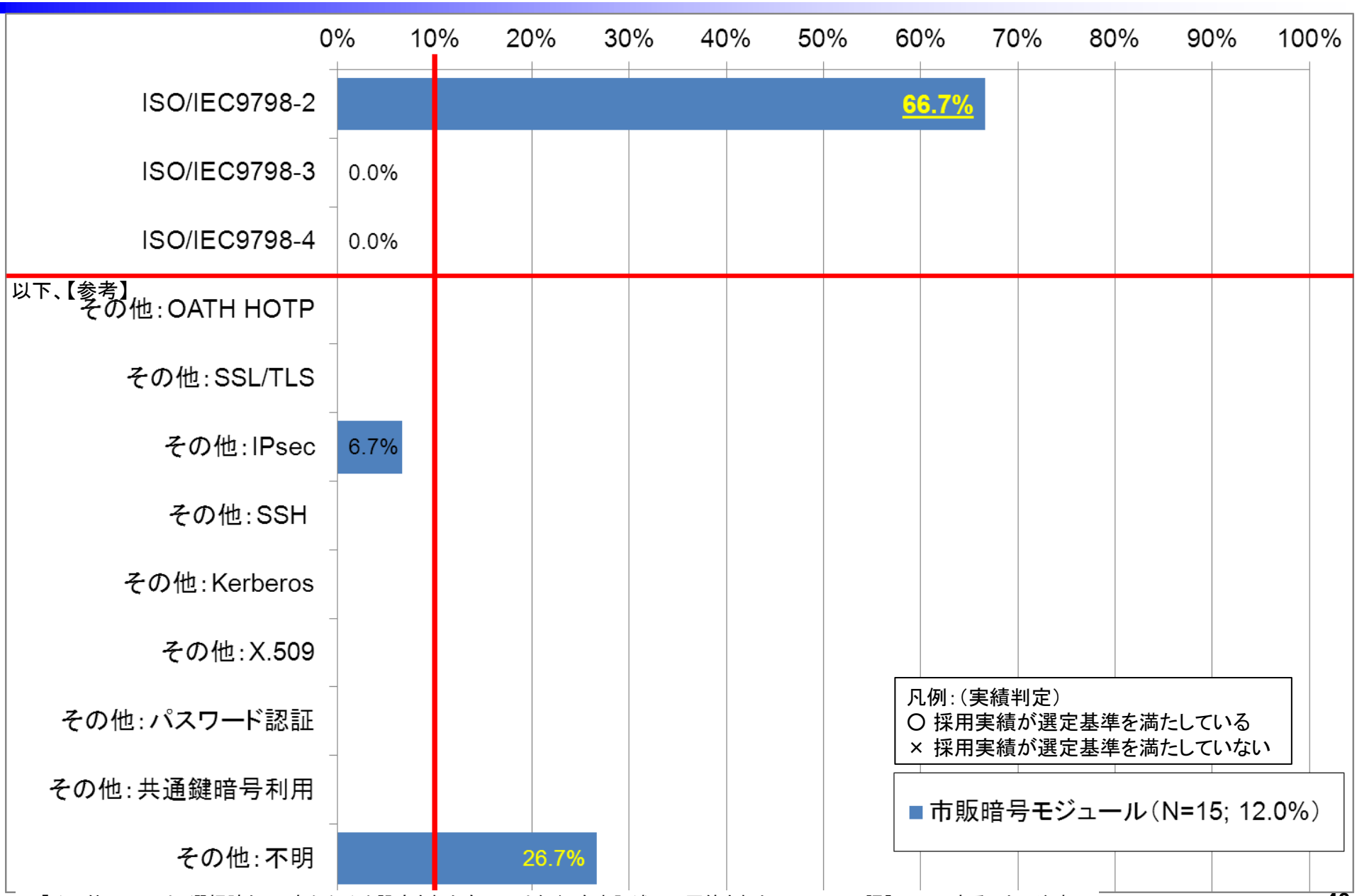
※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答された暗号利用モードXXXであることに注意

暗号モジュールアピール結果 — 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

暗号モジュールアピール結果 ― 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

「調達コスト低減を図るハードルの低さ」の判定

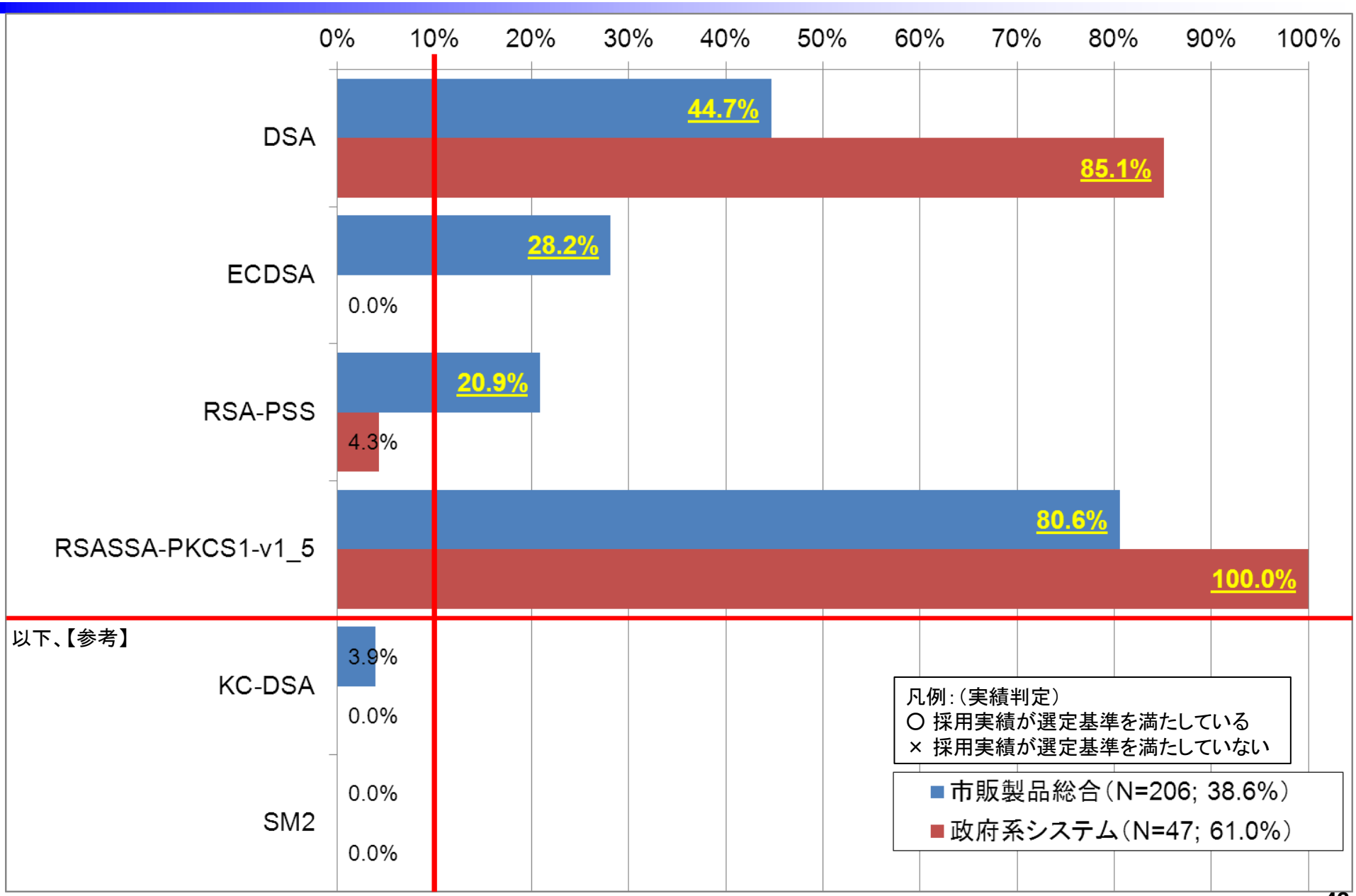
		判定結果	P.41-49 市販製品実績	P.41-49 政府系システム実績
署名	ECDSA	○	○	×
署名	RSA-PSS	○	○	×
守秘・鍵共有	ECDH	○	○	×
守秘・鍵共有	PSEC-KEM	×	×	×
守秘・鍵共有	RSA-OAEP	○	○	×
64ビットブロック暗号	CIPHERUNICORN-E	×	×	×
64ビットブロック暗号	Hierocrypt-L1	×	×	×
64ビットブロック暗号	MISTY1	×	×	×
128ビットブロック暗号	Camellia	○	○	×
128ビットブロック暗号	CIPHERUNICORN-A	×	×	×
128ビットブロック暗号	CLEFIA	×	×	×
128ビットブロック暗号	Hierocrypt-3	×	×	×
128ビットブロック暗号	SC2000	×	×	×
ストリーム暗号	Enocoro-128v2	×	×	×
ストリーム暗号	KCipher-2	○	○	×
ストリーム暗号	MUGI	×	×	×
ストリーム暗号	MULTI-S01	×	×	×

		判定結果	P.42-50 市販製品実績	P.42-50 政府系システム実績
ハッシュ関数	SHA-256	○	○	○
ハッシュ関数	SHA-384	○	○	×
ハッシュ関数	SHA-512	○	○	×
暗号利用モード（秘匿）	CFB	○	○	×
暗号利用モード（秘匿）	OFB	○	○	×
暗号利用モード（秘匿）	CTR	○	○	×
暗号利用モード（秘匿＋認証付）	CCM	×	×	×
暗号利用モード（秘匿＋認証付）	GCM	○	○	×
メッセージ認証コード	CMAC	×	×	×
メッセージ認証コード	PC-MAC-AES	×	×	×
エンティティ認証	ISO/IEC9798-2	○	○	○
エンティティ認証	ISO/IEC9798-3	○	○	○
エンティティ認証	ISO/IEC9798-4	×	×	×

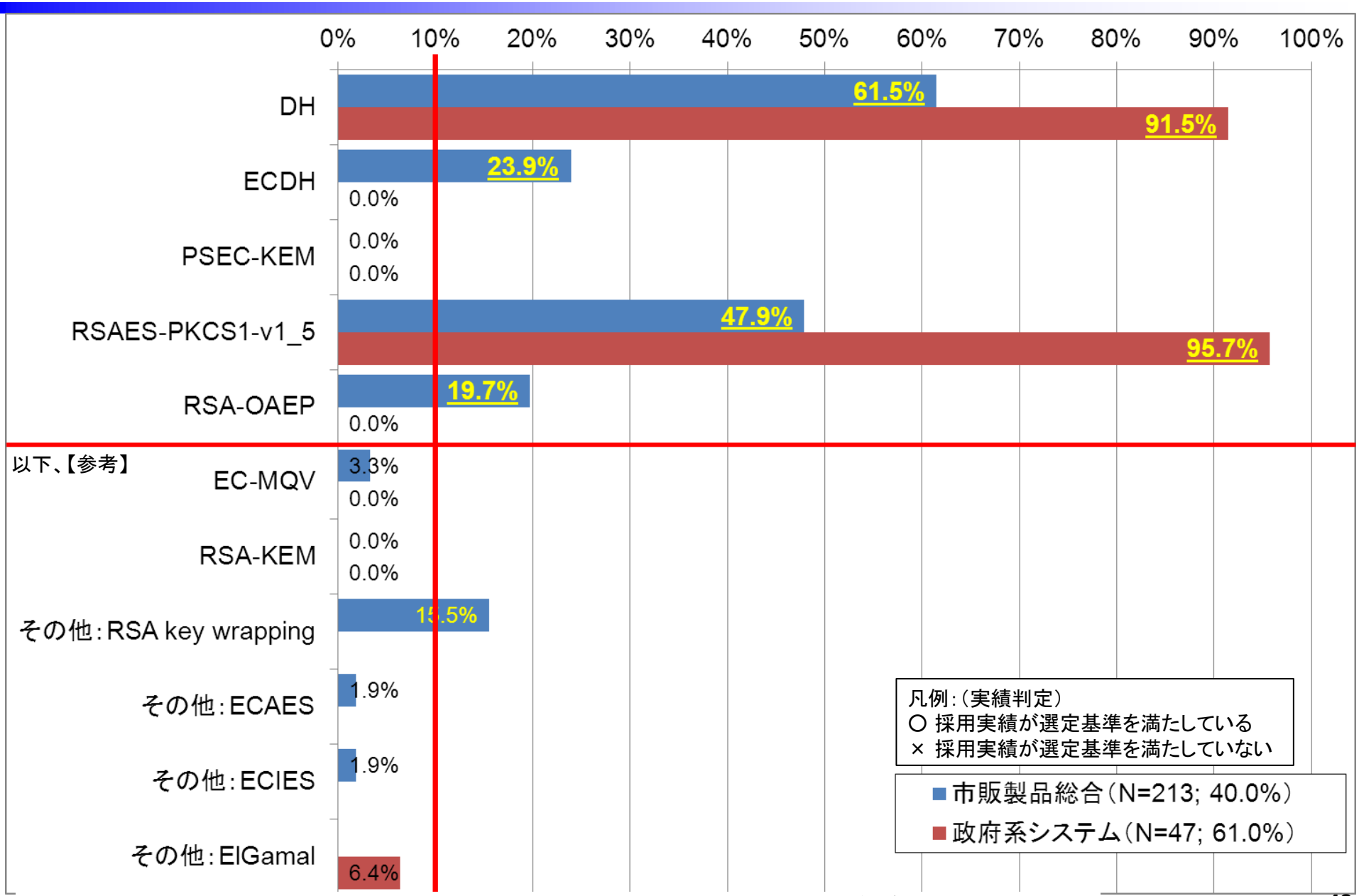
2つの実績判定のOR条件で総合判定

凡例：（実績判定） ○ 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

調達アピール結果 — 署名

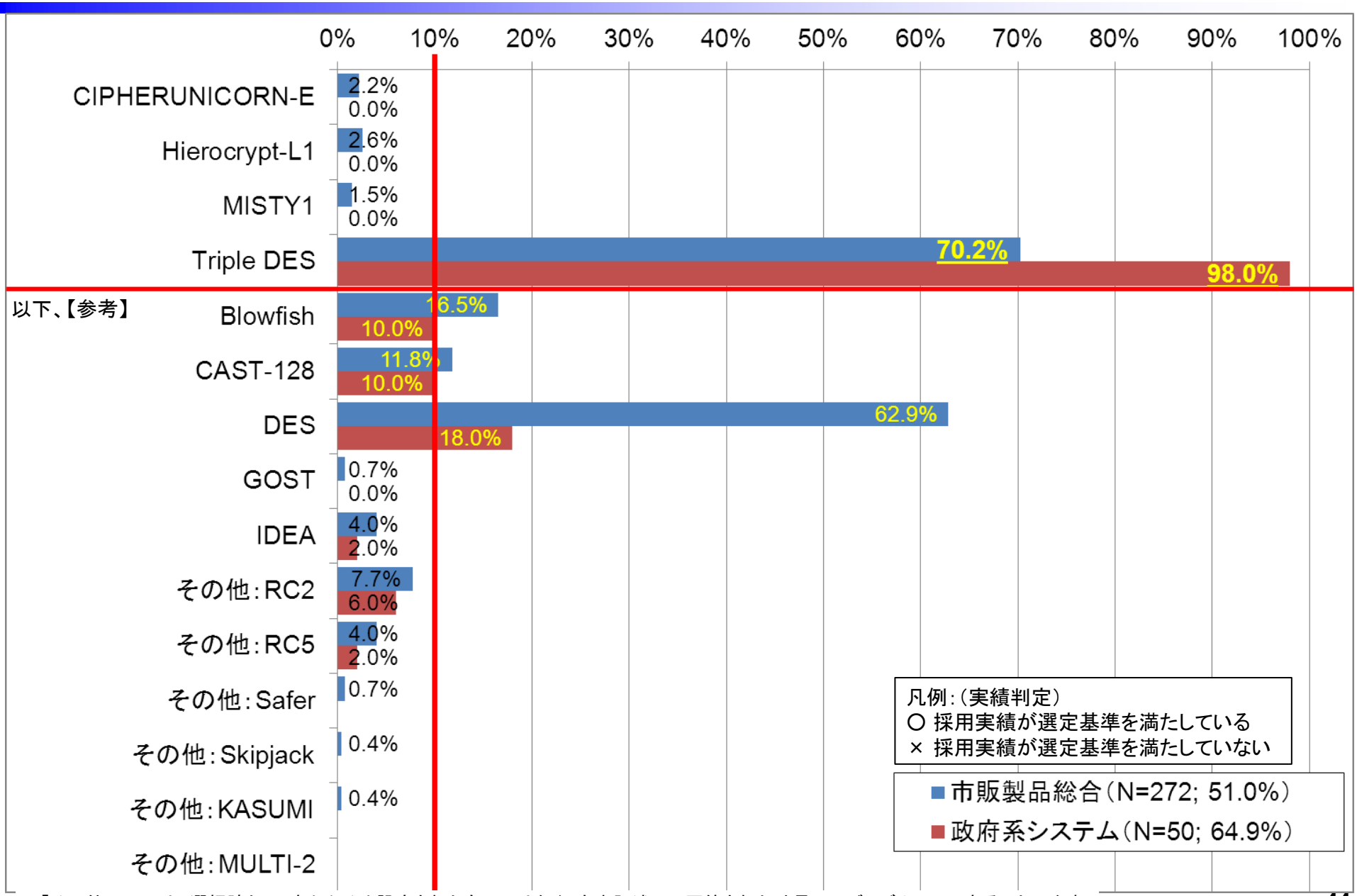

0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
DSA
44.7%
85.1%
ECDSA
28.2%
0.0%
RSA-PSS
20.9%
4.3%
RSASSA-PKCS1-v1_5
80.6%
100.0%
以下、【参考】
KC-DSA
3.9%
0.0%
SM2
0.0%
0.0%
凡例：（実績判定）
○ 採用実績が選定基準を満たしている
× 採用実績が選定基準を満たしていない
市販製品総合（N=206; 38.6%）
政府系システム（N=47; 61.0%）

調達アピール結果 ― 守秘・鍵共有



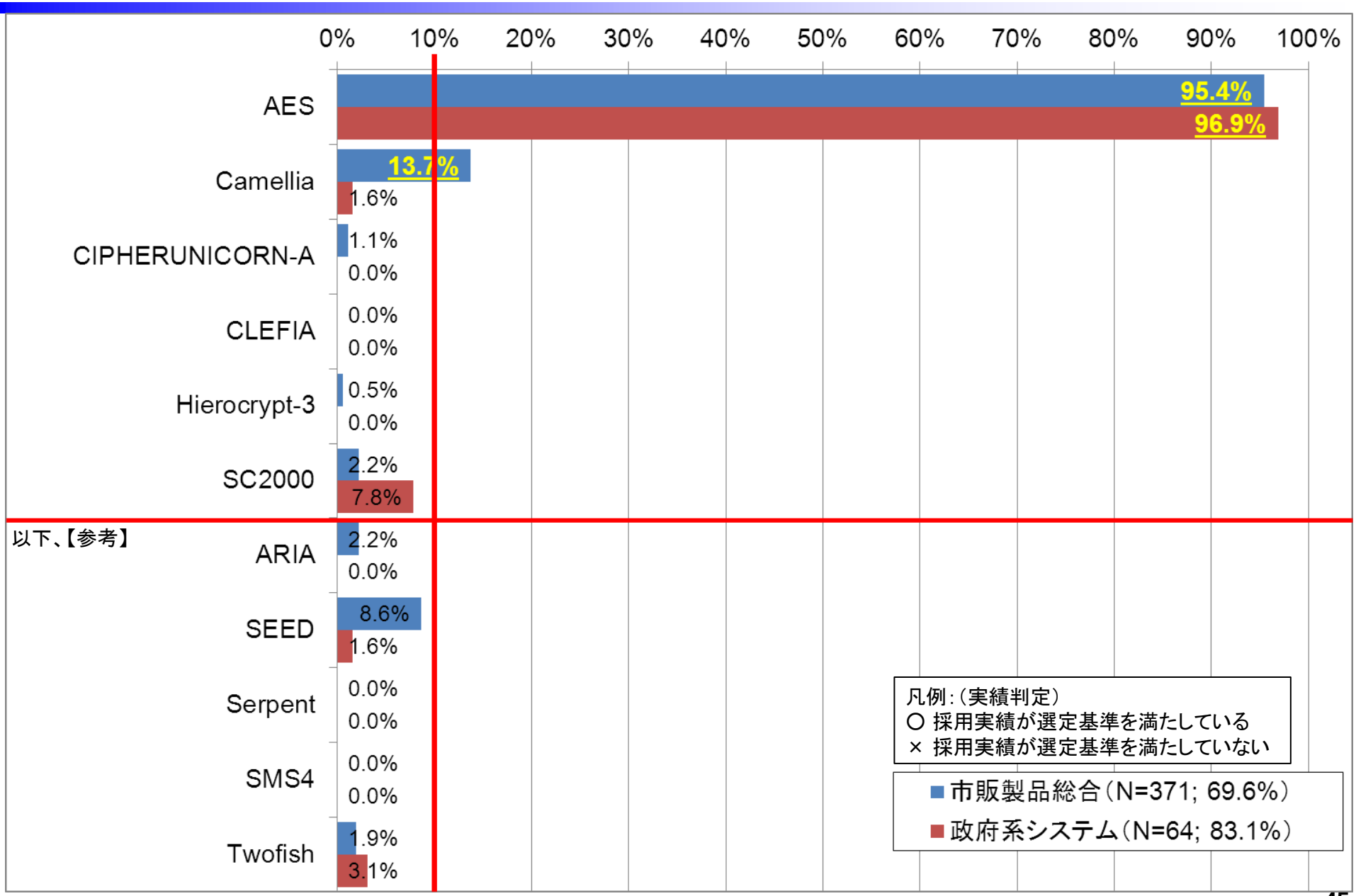
※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答された暗号アルゴリズムXXXであることに注意

調達アピール結果 — 64ビットブロック暗号

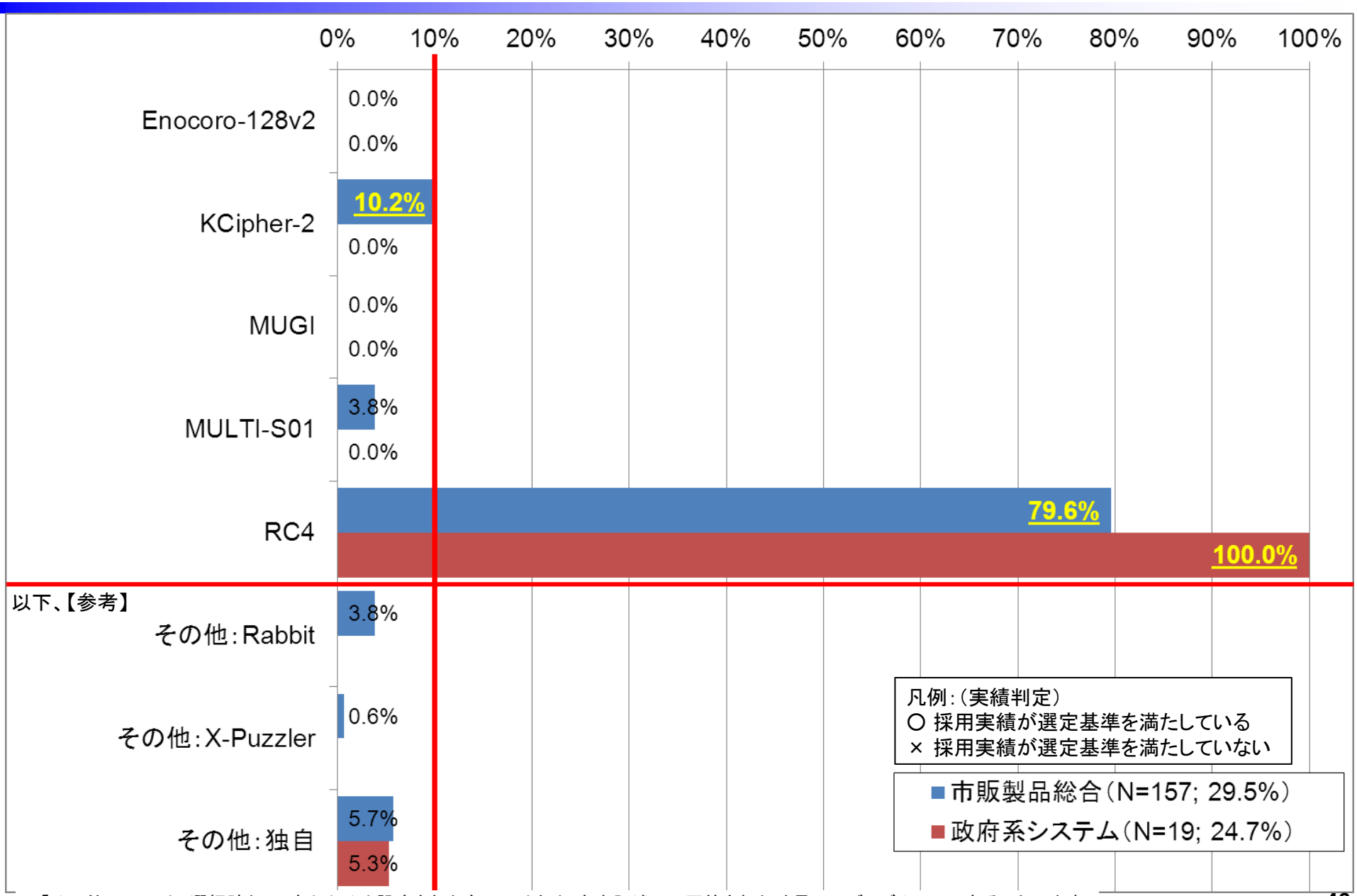


※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答された暗号アルゴリズムXXXであることに注意

調達アピール結果 — 128ビットブロック暗号

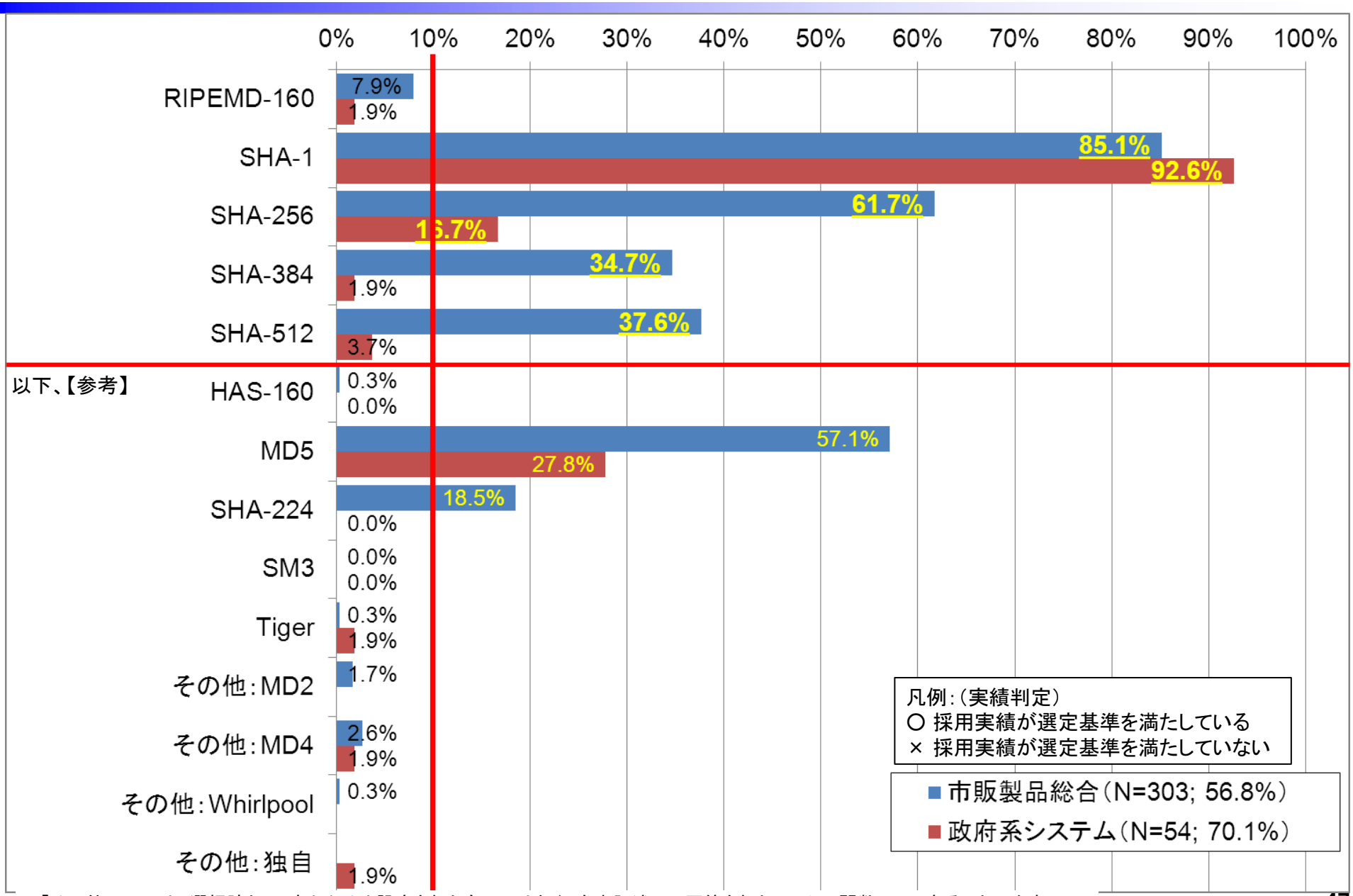


調達アピール結果 ― ストリーム暗号



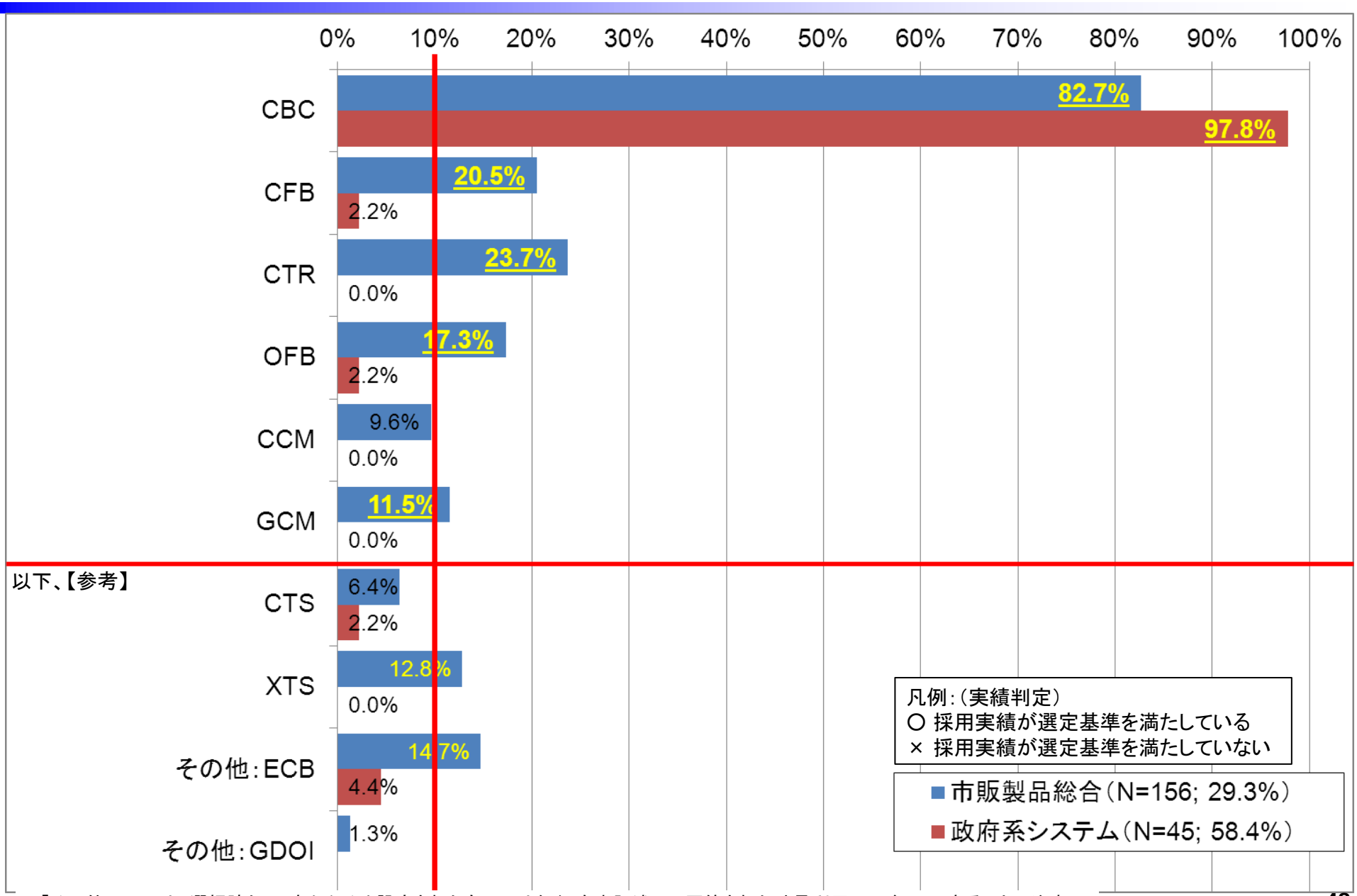
※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答された暗号アルゴリズムXXXであることに注意

調達アピール結果 ― ハッシュ関数



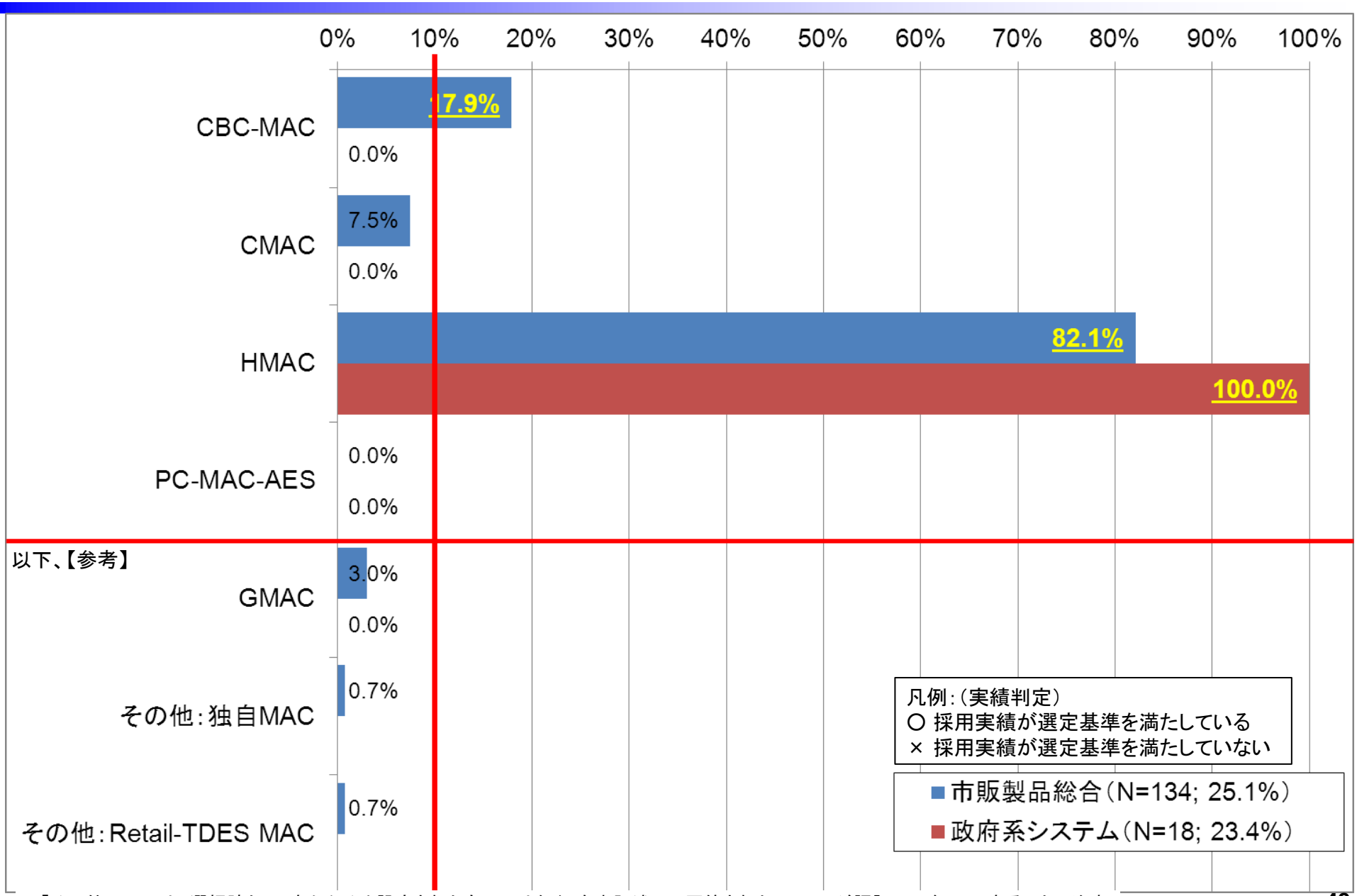
※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答されたハッシュ関数XXXであることに注意

調達アピール結果 ― 暗号利用モード



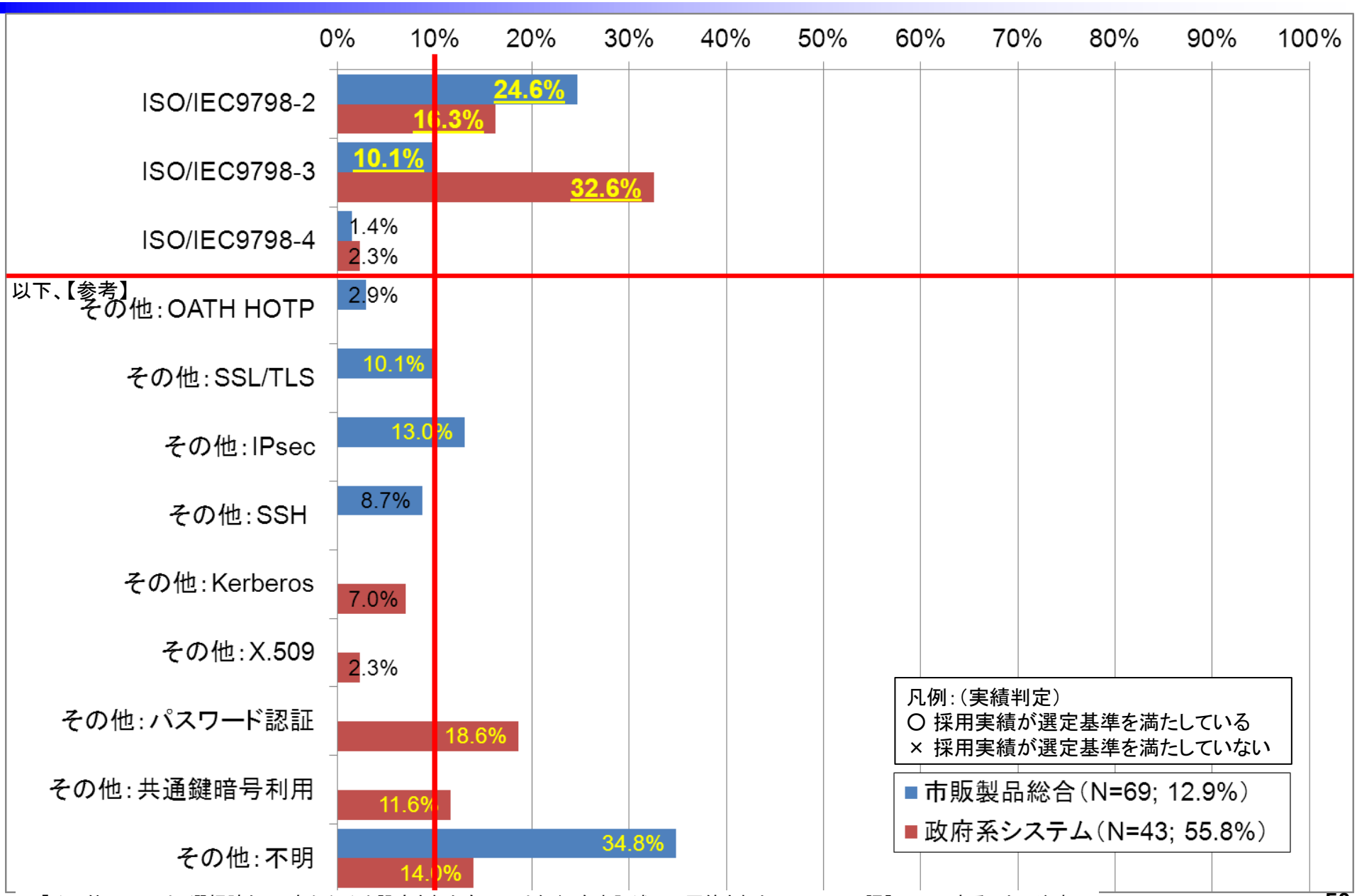
※「その他：XXX」は、選択肢としてあらかじめ設定されたものではなく、自由記述にて回答された暗号利用モードXXXであることに注意

調達アピール結果 ― 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

調達アピール結果 ― 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

参考：他社利用状況の判断

別添

	自社・グループ関連会社と判断	他社と判断
CIPHERUNICORN-E	1社	ー
Hierocrypt-L1	1社	ー
MISTY1	1社	2社
Camellia	7社	12社
CIPHERUNICORN-A	1社	ー
CLEFIA	ー	ー
Hierocrypt-3	1社	ー
SC2000	2社	1社
Enocoro-128v2	ー	ー
KCipher-2	2社	5社
MUGI	ー	ー
MULTI-S01	1社	ー
PC-MAC-AES	ー	ー
PSEC-KEM	ー	ー