暗号実装委員会報告

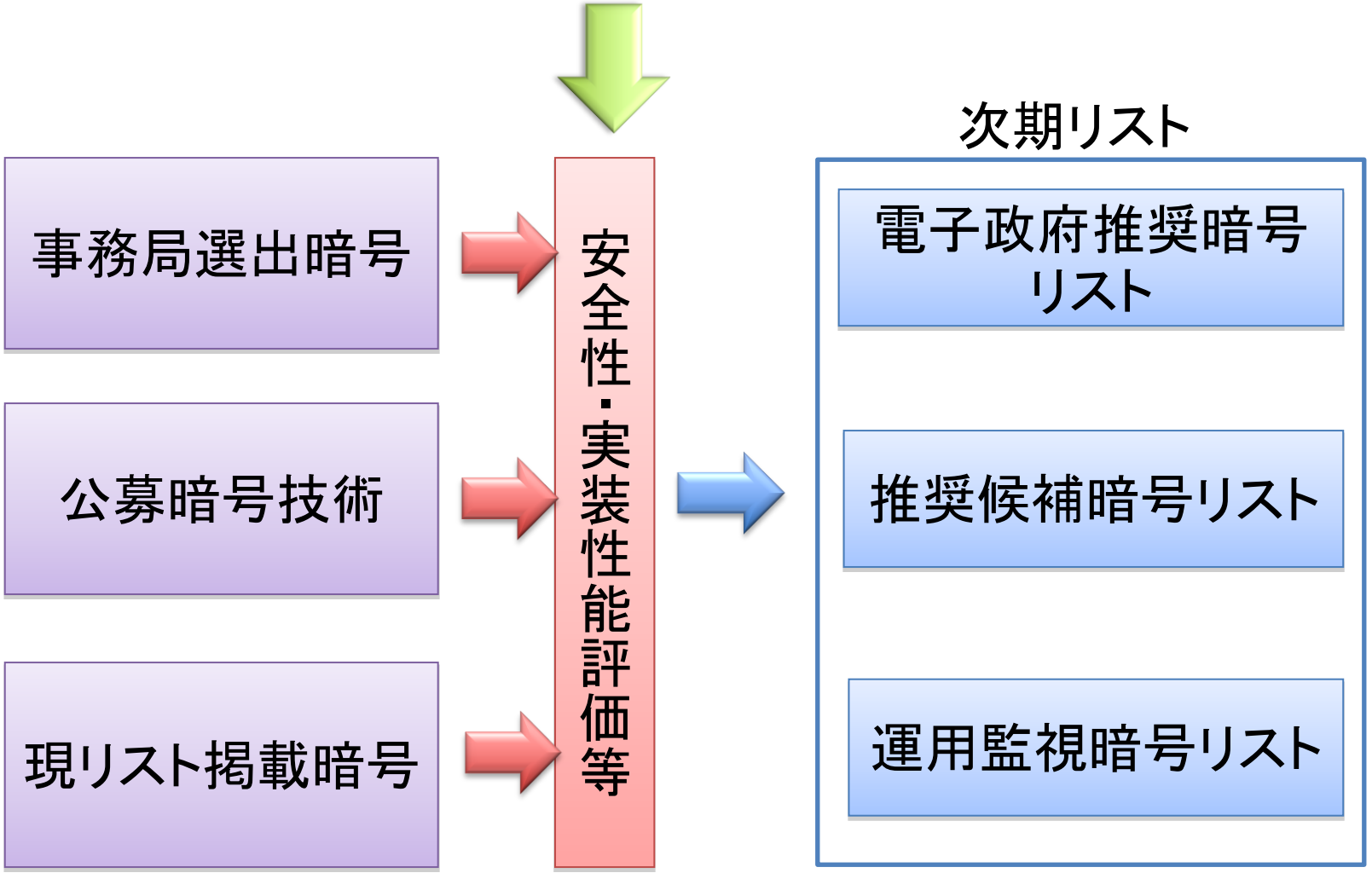
応募暗号と現リスト掲載暗号に対する実装性能評価の進行状況

CRYPTREC
Cryptography Research and Evaluation Committees

目次

1. リスト作成の基本的な流れ
2. 評価対象
3. 体制
4. スケジュール
5. 評価方針
6. 評価内容
7. 評価結果の位置づけ(精度)
8. ソフトウェア実装性能評価
9. ハードウェア実装性能評価
10. まとめ

1. リスト作成までの基本的な流れ



CRYPTREC
Cryptography Research and Evaluation Committees

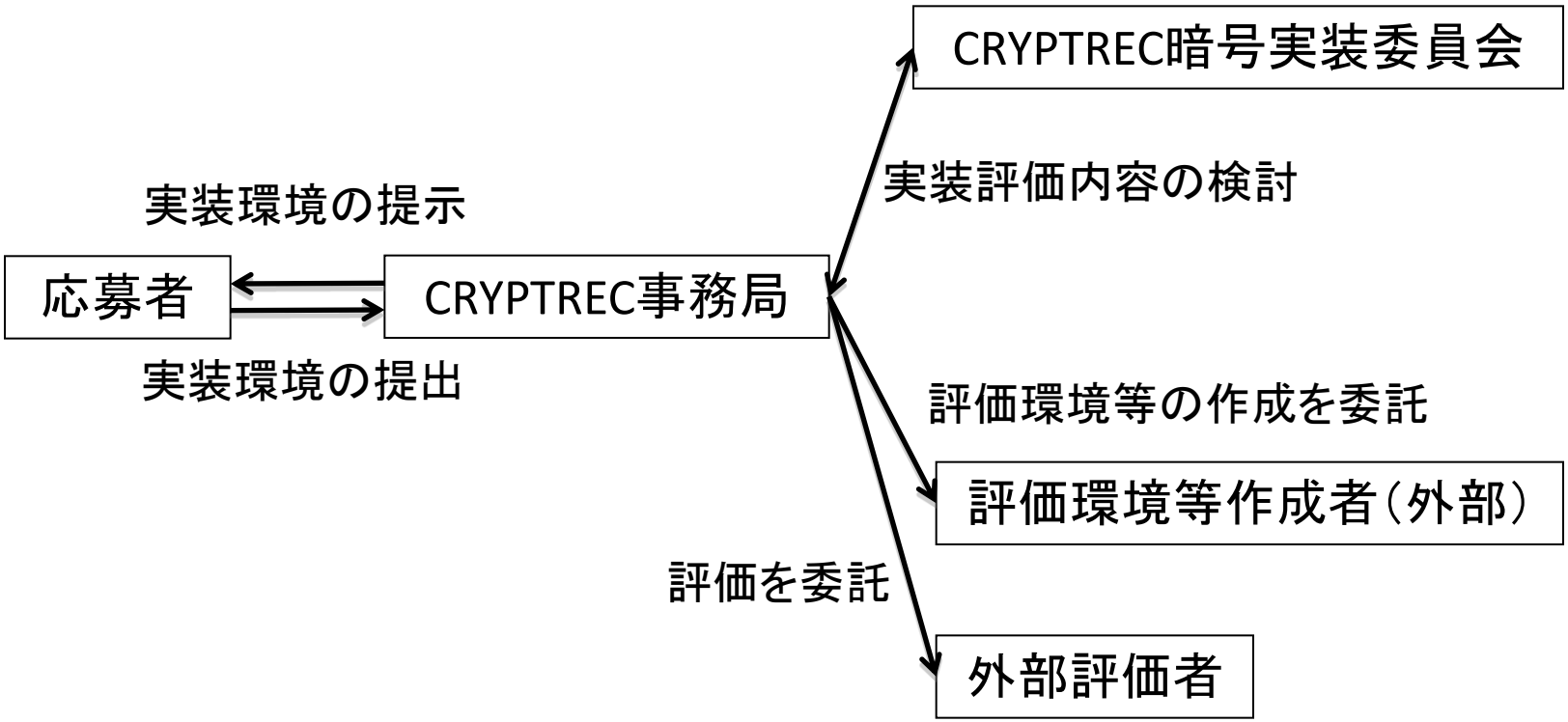
2. 評価対象

	新規応募	現リスト掲載	事務局選出
128ビットブロック暗号	CLEFIA	AES	
		Camellia	
		CIPHERUNICORN-A	
		Hierocrypt-3	
		SC2000	
ストリーム暗号	Enocoro-128v2	MUGI	
	KCipher-2	(MULTI-S01)**	
		(128-bit RC4)*	
メッセージ認証コード	PC-MAC-AES		CMAC
			(CBC-MAC)*
			(HMAC)*

• 今回の評価対象外
** ハードウェア実装のみ実施

3. 評価の体制

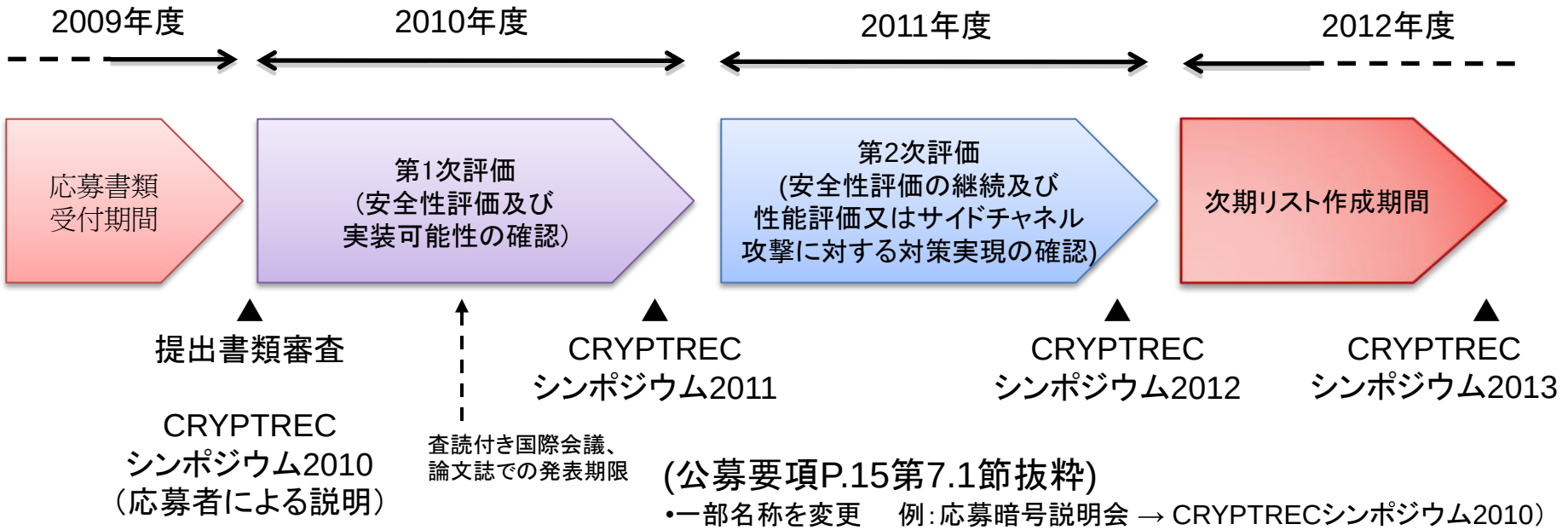
体制図



CRYPTREC
Cryptography Research and Evaluation Committees

4. スケジュール

CRYPTRECシンポジウム2010開催：	2010 年3月2-3日
第1次評価実施：	2010年4月～2011年3月
CRYPTRECシンポジウム2011開催：	2011年3月2日
第2次評価実施：	2011年4月～2012年3月
CRYPTRECシンポジウム2012開催：	2012年3月9日（本日）
CRYPTRECシンポジウム2013開催：	2013年3月頃



(公募要項P.15第7.1節抜粋)

•一部名称を変更　例：応募暗号説明会 → CRYPTRECシンポジウム2010）

CRYPTREC
Cryptography Research and Evaluation Committees

5. 評価方針

2000～2002年度の実装性能評価の教訓

「実装できない」暗号が提案された

→ 実装するための情報が不足

→ 「実現可能性の確認」 が必要

「実装できても
リソース使用量や処理性能で問題発生の可能性」

→ プラットフォーム選択のための
「性能評価」が必要

5. 評価方針　続き

今回の実装性能評価

新規応募暗号

- 「実現可能性の確認」と「性能評価」を作業項目に設定
- 応募者にこれらを提示
- 提出された実装を評価

- 「サイドチャネル攻撃対策可能性」を追加

現リスト掲載暗号

- 「実現可能性の確認」は既に完了
- 「性能確認」を実装環境の変化に対応して実施

6. 評価内容

（1）実現可能性の確認

・動作確認（参照ソースコード、参照ハードウェア設計記述）

＊テストベクトルが再現されるか確認する

（2）性能の評価

・ソフトウェア性能評価（処理速度、リソース使用量）

・ハードウェア性能評価（回路規模、クリティカルパス遅延、スループット）

＊標準的プラットフォームで実装可能であることを確認する

＊調達者にプラットフォーム選択のための参考情報を提供する

（3）サイドチャネル攻撃に対する対策実現の確認

・サイドチャネル攻撃対策の実現可能性の確認（ハードウェア）

＊攻撃対策によって攻撃が困難となることを確認する

(公募要項P.2第2.2節)

6. 評価内容

・ソフトウェア実装

評価環境

・通常のPC環境　Intel x86 CPU (Core i5) + MS-Windows 7 (32ビット)

評価項目

・処理能力:　実行速度(クロック数)、使用メモリ量

・ハードウェア実装

評価環境

・SASEBO-GII搭載のFPGA　Xilinx Virtex-5 LX50 + ISE Web Pack ver. 12.4

評価項目

・処理能力:　回路規模、クリティカルパス遅延、スループット等

・サイドチャネル攻撃対策可能性:

・2種類の実装(対策有/無)に対する攻撃の効果比較

・対策のオーバーヘッド

7. 評価結果の位置づけ（精度）

イ 第二次評価（2011 年 4 月～2012 年 3 月）

- 第二次評価の目的は、「性能評価」とし、ソフトウェア、ハードウェアの両面で評価を行う。
- 評価対象：第一次評価をパスした暗号及び現リスト掲載暗号

(i) ソフトウェア処理性能評価

- 標準的なプラットフォーム上で提案者が実装した最適化コードを用いて、処理速度、リソースの使用量等を評価する。
- 評価結果は、リスト作成に利用するとともに、調達者へプラットフォーム選定上の参考情報（処理性能の見積もり、必要なリソース量の見積もり）として提供する。

(ii)ハードウェア処理性能評価

- FPGA 上で、提案者が実装した最適化コードを用いて、処理速度、リソースの使用量等を評価する。
- 評価結果は、リスト作成に利用するとともに、調達者へプラットフォーム選定上の参考情報（処理性能の見積もり、必要なリソース量の見積もり）として提供する。

CRYPTREC Report 2008「2.1.1 実装性評価の概要」（17ページ）

7. 評価結果の位置づけ（精度）

実装評価の目的

・プラットフォームに要求される仕様（要求条件）を調達者に「参考情報」として提供すること

・具体的には、標準的なプラットフォームで使用する際の
  ・必要となるメモリー量やゲート数のおおよその見積り
  ・処理速度のおおよその見積もり

⇒　標準的な使用環境における「実現可能性の確認」と「性能評価」は十分可能

⇒　暗号選択の選定基準としては想定されていない

7. 評価結果の位置づけ(精度)

今回の実装性能評価の限界

(1) 特定のプラットフォーム上での評価
サーバ系、ICカード(SW実装)、ASIC(HW実装)など多様な環境での評価が未実施であり、評価に偏りがある

(2) 処理速度とメモリ使用量のみによる評価
実装開発、メンテナンス、高性能実装入手などの容易性も重要

(3) 新規応募暗号と現リスト掲載暗号との実装者の差
現推奨暗号は外部委託者、新規暗号は応募者が実装したため実装ノウハウに差がある

⇒ 暗号選択の選定基準としての利用には注意を要する

8. ソフトウェア実装性評価　－　概要

① 実装環境等（プラットフォーム／OS／使用言語）
- Intel x86 CPU 搭載のPC環境（HP製 Probook 6550b/CT）
- CPU: インテル Core i5 -480M (2.66 GHz)
- メモリ: DDR3 SDRAM, 4GB
- OS: MS-Windows 7 (32ビット版)
- 開発環境: Visual Studio / Visual C++ 2010 (10.0) SP1
- インライン・アセンブラやSSE/SSE2等のIntrinsic命令の使用は禁止

② 評価ツール
- 経済産業省が2009年度に実施した委託事業「クラウド環境における暗号技術評価」で作成した性能評価ツールを利用

③ 計測項目
- データ入出力時間（クロック数）
- 初期化時間（クロック数）
- データ演算時間（暗号化／復号処理のクロック数）
- 処理に利用するプロセスメモリのサイズ

8. ソフトウェア実装性能評価　－　評価環境

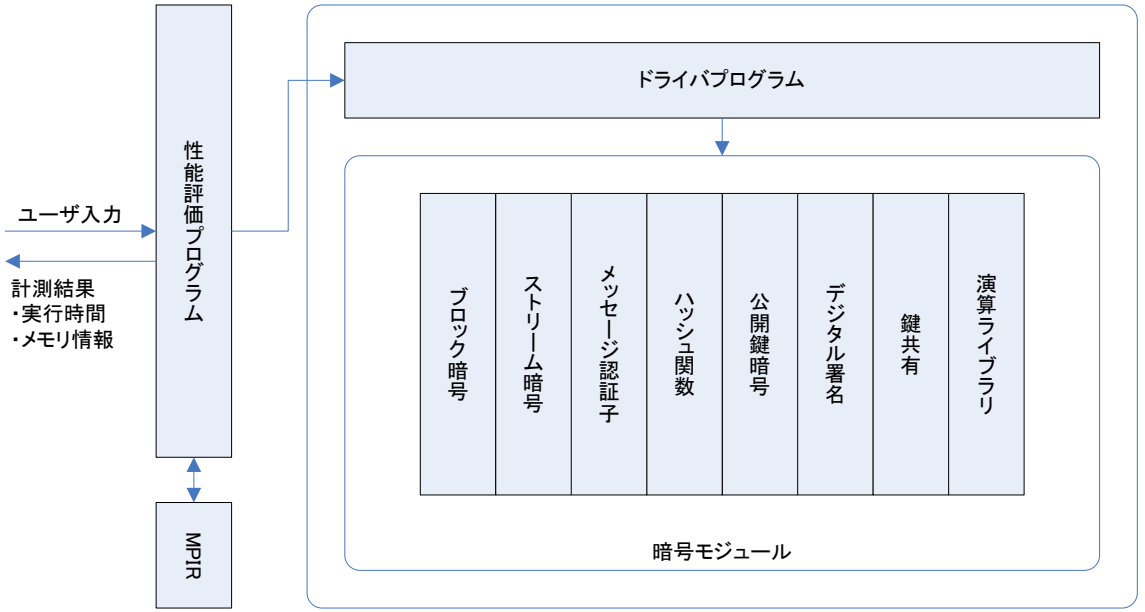
ソフトウェア性能評価ツール＊

・ドライバプログラムの機能
　・入出力ストリーム
　・計測機能

・提供される計測項目
　・実行クロック数
　・メモリサイズ

現リスト掲載暗号方式
　・暗号ライブラリとして実装済み

新規応募暗号
　・提供するサンプルコードに基づいて応募者側で実装
　・アセンブリ実装やIntel Compilerの利用は不可

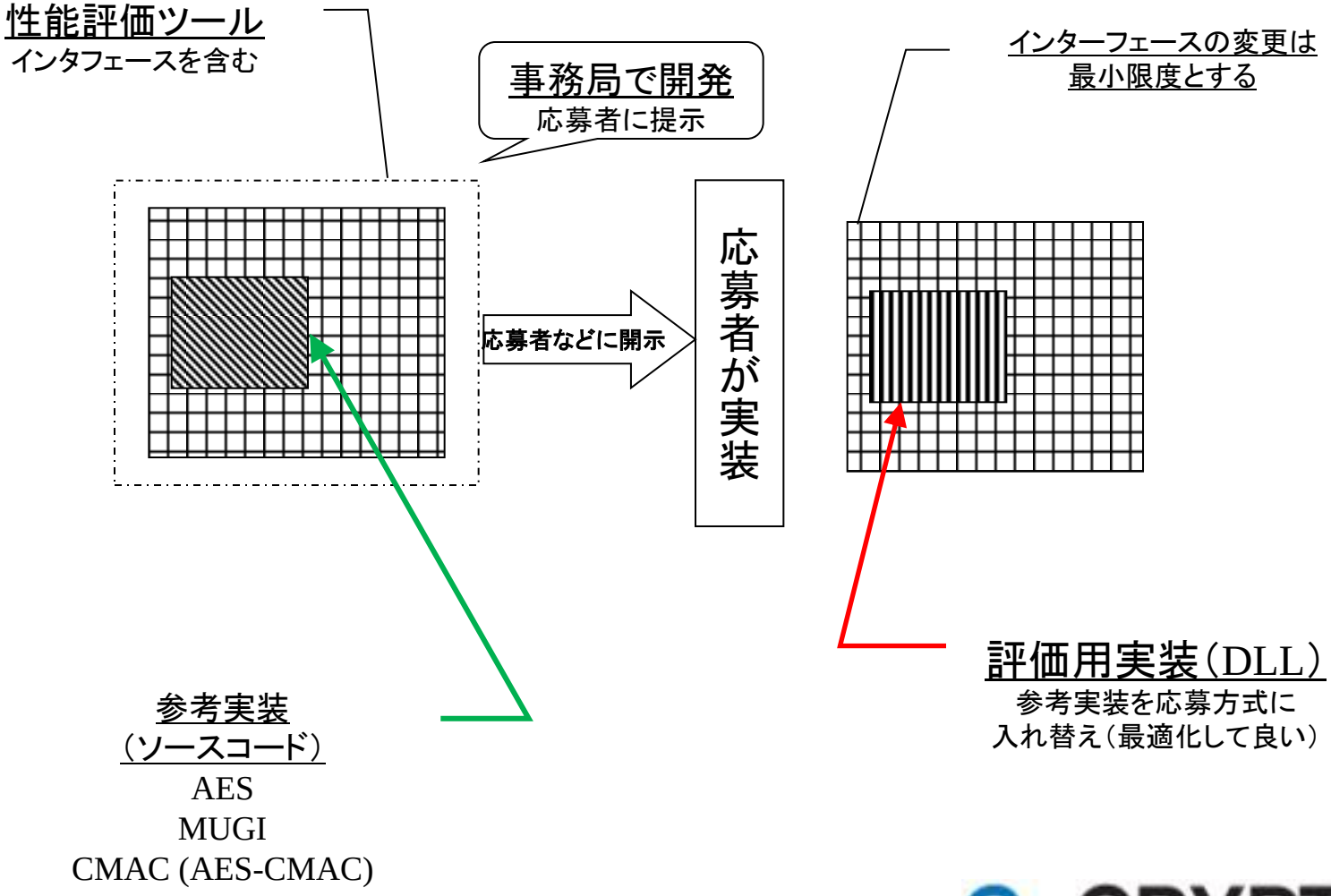


評価ツールの全体構成

＊ 2009年度に経済産業省が委託研究「クラウド環境における暗号技術評価」の一環として開発

CRYPTREC
Cryptography Research and Evaluation Committees

8. ソフトウェア実装性能評価　－　応募者の実装開発



CRYPTREC
Cryptography Research and Evaluation Committees

8. ソフトウェア実装性評価　－　評価状況

新規応募暗号

- 「実現可能性の確認」は完了
- 「性能評価」もほぼ終了

現リスト掲載暗号

- 「実現可能性の確認」は前回公募時に完了
- 「性能評価」もほぼ終了

事務局選出暗号

- 「実現可能性の確認」は完了
- 「性能評価」もほぼ終了

8. ソフトウェア実装性評価　－　評価状況　続き

評価対象の全暗号が十分な実装性能を有していることを確認

	新規応募	現リスト掲載	事務局選出
128ビットブロック暗号	CLEFIA	AES	
		Camellia	
		CIPHERUNICORN-A	
		Hierocrypt-3	
		SC2000	
ストリーム暗号	Enocoro-128v2	MUGI	
	KCipher-2	(MULTI-S01)**	
		(128-bit RC4)*	
メッセージ認証コード	PC-MAC-AES		CMAC
			(CBC-MAC)*
			(HMAC)*

数値データの公表方法は2012年度暗号実装委員会で精査する

9. ハードウェア実装性評価　ー　概要

① 実装環境等（ターゲットディバイス／開発環境）
- Xilinx Virtex-5 LX50　(SASEBO-GII搭載のFPGA)
- ISE WebPACK Version 12.4

② 評価環境
- 産業技術総合研究所（AIST）が開発した、「電子政府推奨暗号用ハードウェア評価環境」等の仕様書、説明書等

③ 計測項目　（ISE WebPACKのCADサマリ等のデータ）
- 処理速度(スライス数、クリティカルパス遅延、クロック数、動作周期)
- 状態の初期化に掛かる時間
- サイドチャネル攻撃対策可能性については次スライド

9. ハードウェア実装性評価　ー　サイドチャネル攻撃対策

・鍵長
　・評価対象：128ビット （ブロック暗号・ストリーム暗号共通）
　・他の鍵長での性能は、参考情報に留める

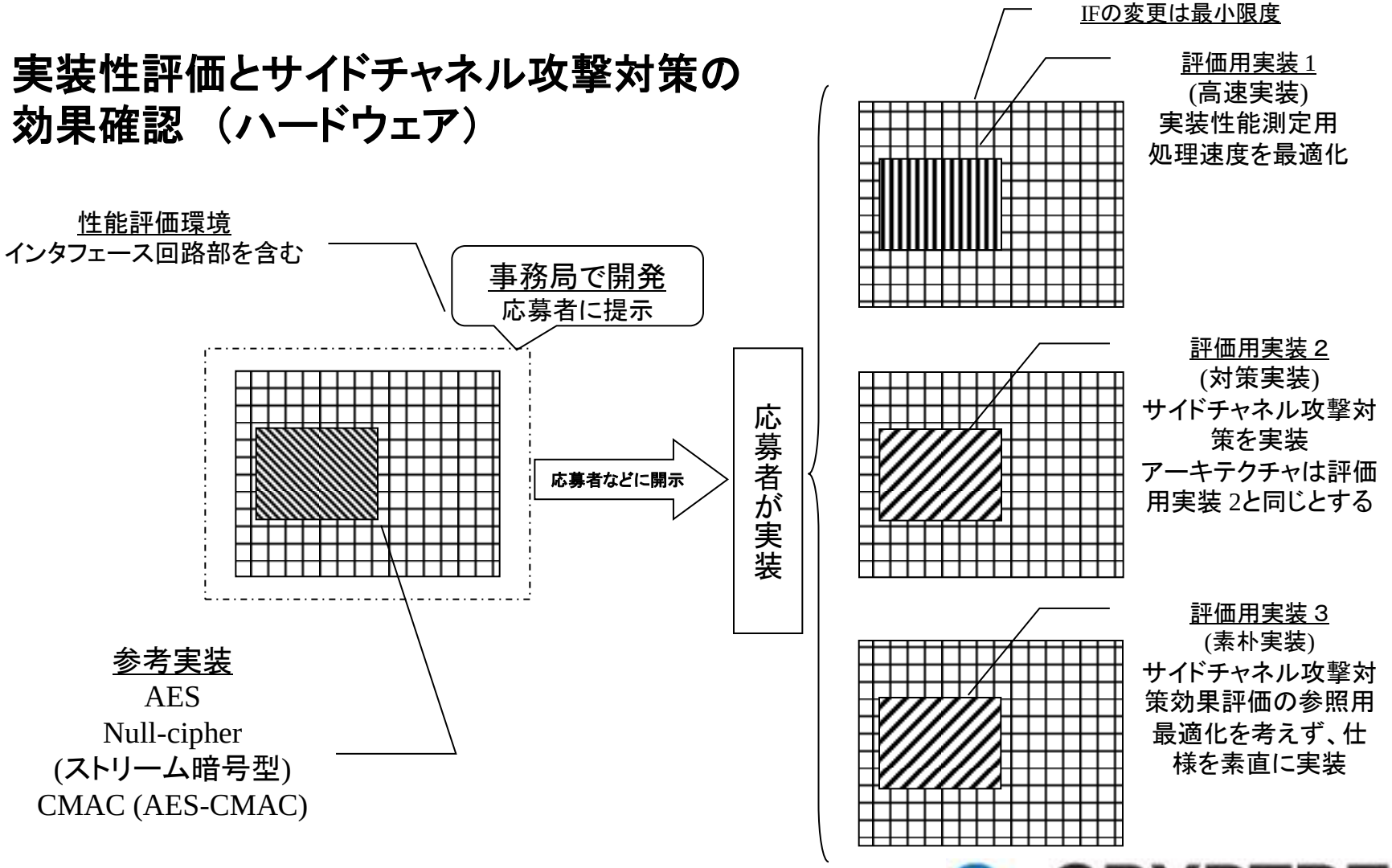
・評価対象の攻撃法
　・電力解析
　・攻撃の種類は応募者が選択（SPA, DPA, CPA, MIA …）

・選択関数
　・応募者が設定し、提案する
　・応募者は提案したものが、発見した中で最良のものであることを誓約

・有効性の確認
　・攻撃コストの上限（例: 10万波形）を設定して攻撃を適用
　・対策実装(評価用実装2)と素朴実装(評価用実装3)の攻撃耐性を比較
　・対策のオーバーヘッドを評価

9. ハードウェア実装性能評価　－　応募者による実装開発

実装性評価とサイドチャネル攻撃対策の効果確認 （ハードウェア）



CRYPTREC
Cryptography Research and Evaluation Committees

9. ハードウェア実装性評価　ー　評価状況

新規応募暗号

- 「実現可能性の確認」は完了
- 「性能評価」もほぼ終了
- 「サイドチャネル攻撃対策可能性」は評価中

現リスト掲載暗号

- 「実現可能性の確認」は前回公募時に完了
- 「性能評価」もほぼ終了

事務局選出暗号

- 「実現可能性の確認」は完了
- 「性能評価」もほぼ終了

8. ハードウェア実装性評価　－　評価状況　続き

評価対象のいずれの暗号にも実装上の問題は見つかっていない

	新規応募	現リスト掲載	事務局選出
128ビットブロック暗号	CLEFIA	AES	
		Camellia	
		CIPHERUNICORN-A	
		Hierocrypt-3	
		SC2000	
ストリーム暗号	Enocoro-128v2	MUGI	
	KCipher-2	(MULTI-S01)**	
		(128-bit RC4)*	
メッセージ認証コード	PC-MAC-AES		CMAC
			(CBC-MAC)*
			(HMAC)*

サイドチャネル攻撃対策可能性については確認中

数値データの公表方法は2012年度暗号実装委員会で精査する

10. まとめ

・評価対象カテゴリ
　ブロック暗号、ストリーム暗号、メッセージ認証コード（MAC）

・実装環境
　・SW:　Intel x86 CPU (Core i5) + MS-Windows 7 (32ビット版)
　・HW:　Xilinx Virtex-5 (SASEBO GII) + ISE WebPACK 12.4

・実装評価項目
　・実現可能性の確認（SW, HW）　第1次評価(2010年度)
　・性能評価（SW, HW）　第2次評価(2011年度)
　・サイドチャネル攻撃対策（HW）　第2次評価(2011年度)

・評価状況
　・「実装可能性の確認」は完了、「性能評価」はほぼ終了
　・「サイドチャネル攻撃対策可能性」は評価中
　・実装性能評価の精度には要注意