CRYPTRECシンポジウム2010
パネル１：暗号技術の実装について

2010年3月2 日　コクヨホール

0. イントロダクション　＜ 3分

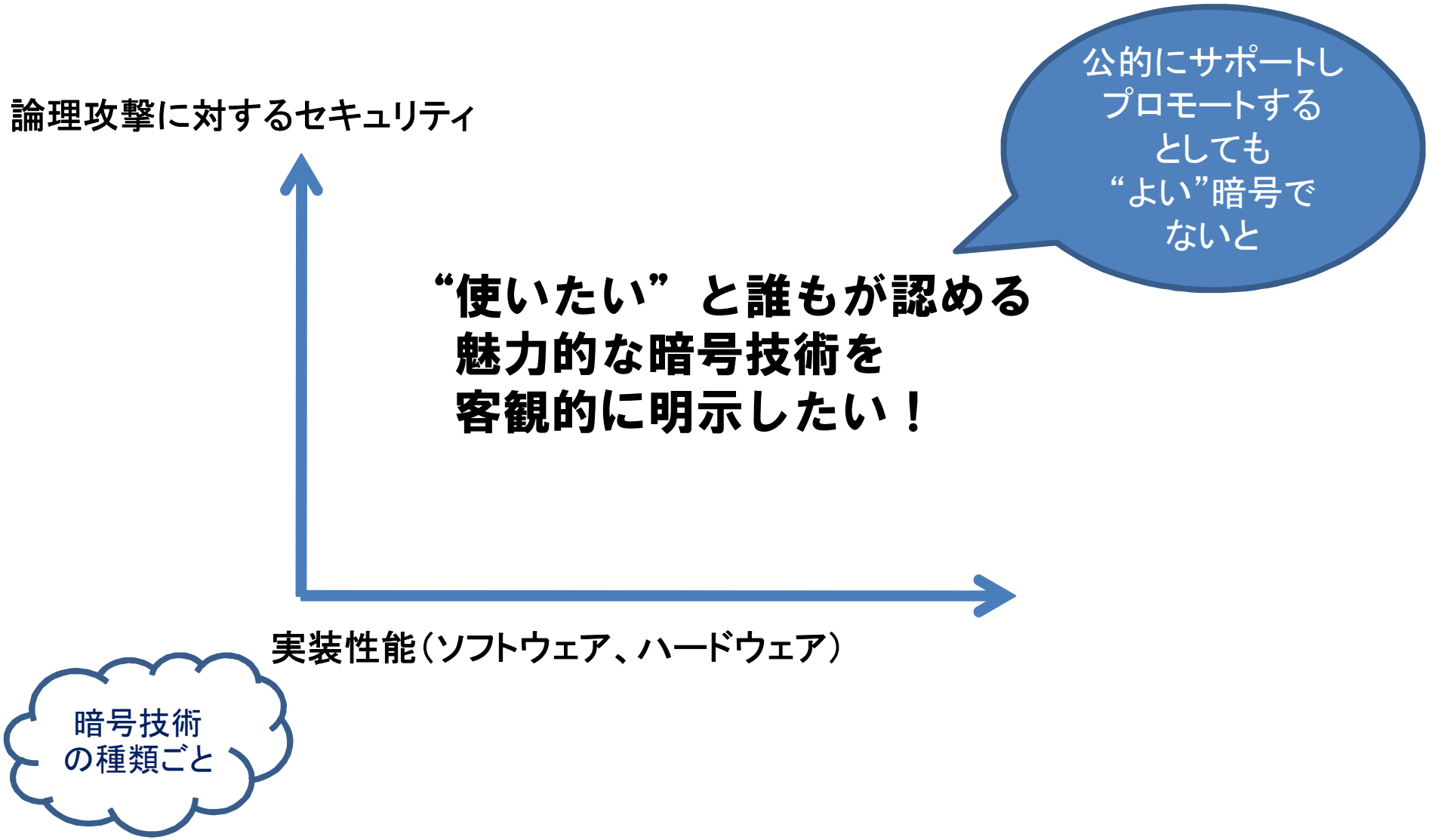
1. ソフトウェア実装評価　プレゼンテーション：10分　ディスカッション：10分
   中嶋 純子 様 （三菱電機株式会社 情報技術総合研究所）

2. 暗号モジュールのハードウェア実装について　プレゼンテーション：10分　ディスカッション：10分
   崎山 一男 先生（電気通信大学 情報通信工学科）

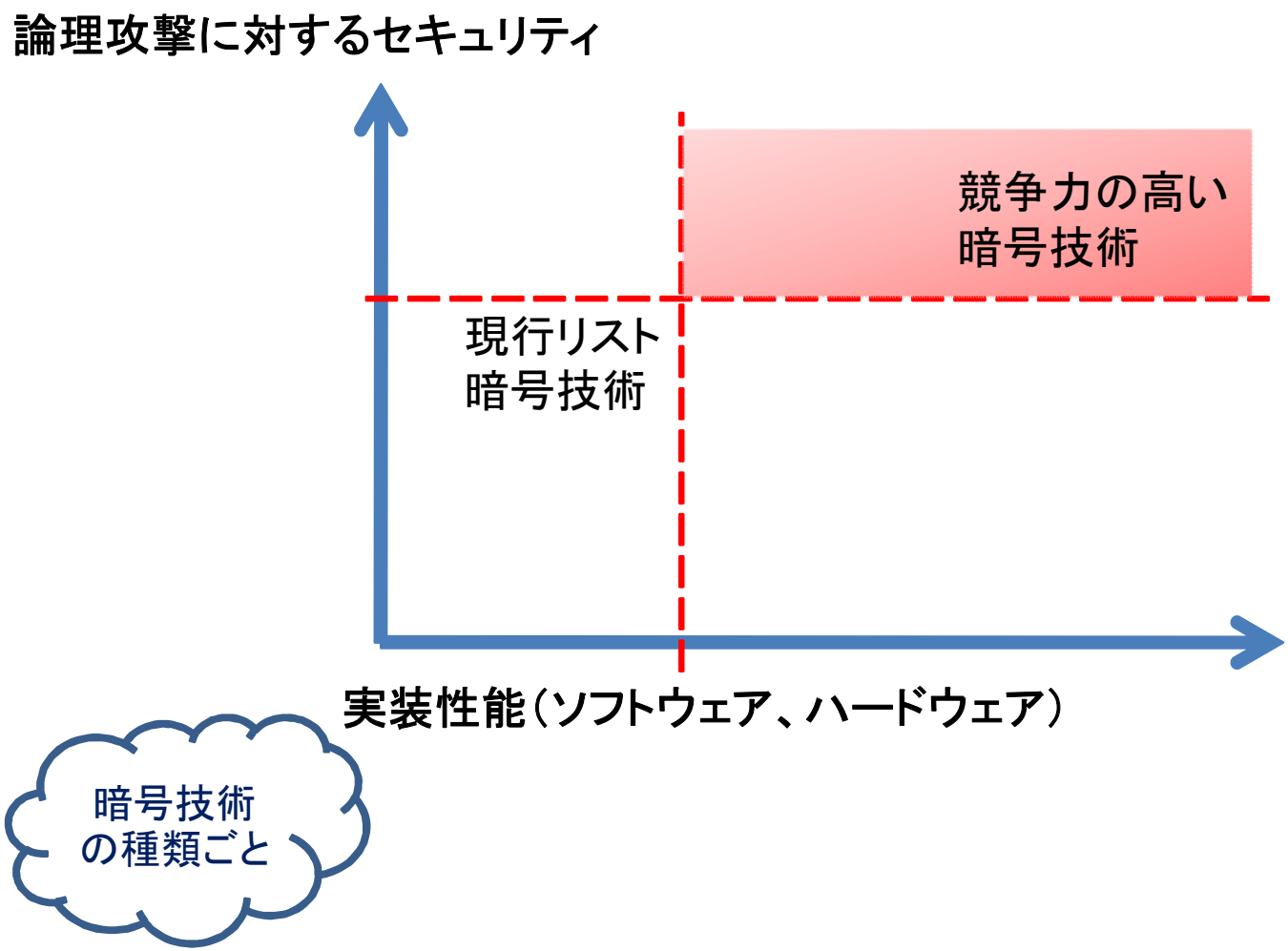
3. 暗号モジュールの実装の安全性評価　プレゼンテーション：10分　ディスカッション：10分
   佐藤　証 様 （(独)産業技術総合研究所 情報セキュリティ研究センター）

4. 総合ディスカッション　＞ 10分　[16:00までに終了]
   モデレータ
   松本　勉 （横浜国立大学大学院環境情報研究院、CRYPTREC暗号実装委員会委員長）

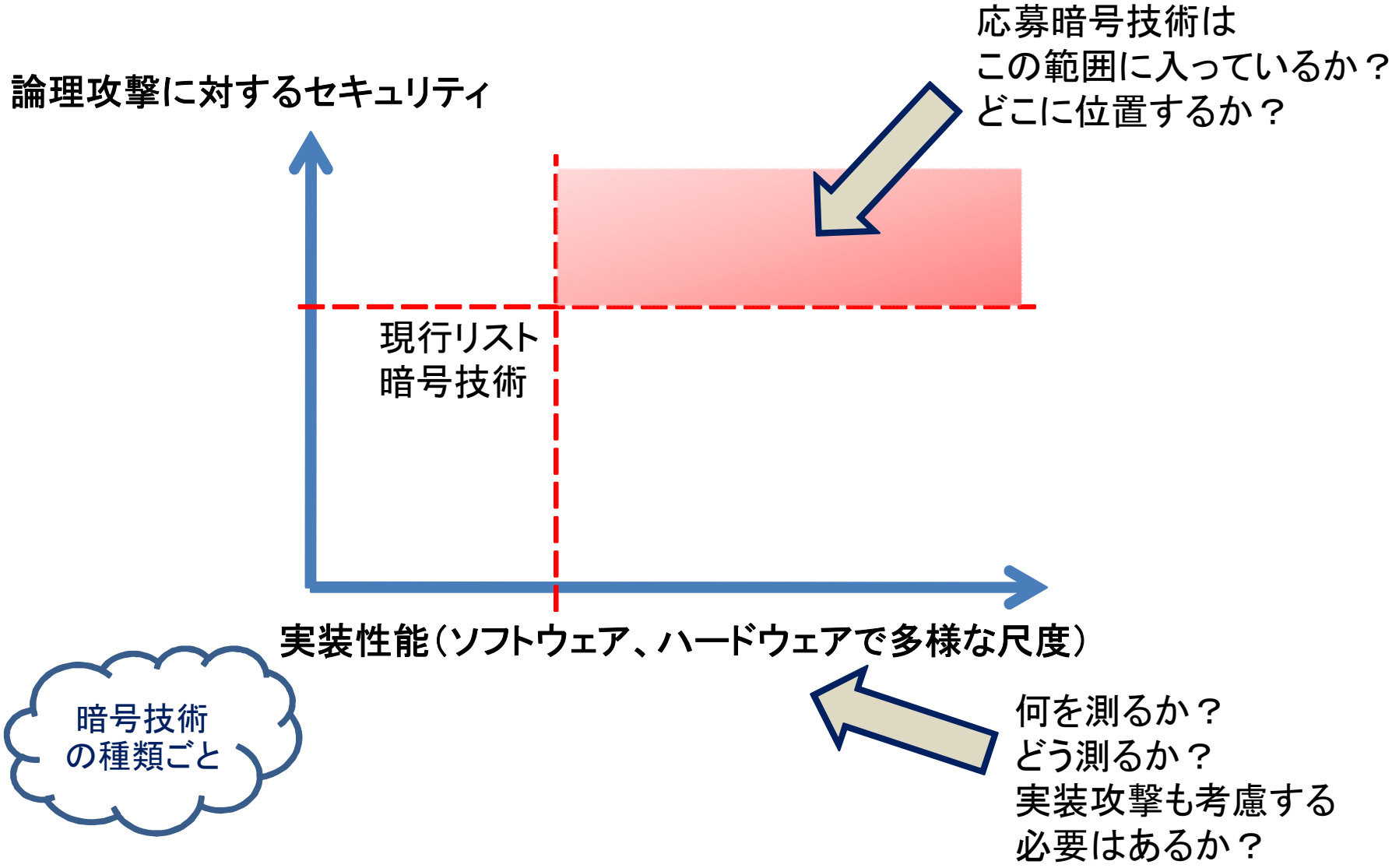
暗号技術の実装評価：何が課題か？



暗号技術の実装評価：何が課題か？

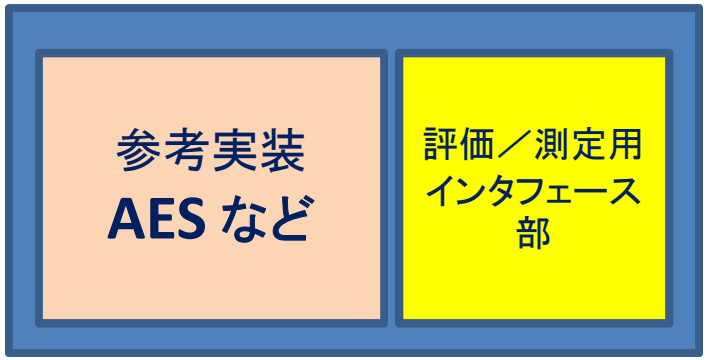


暗号技術の実装評価：何が課題か？



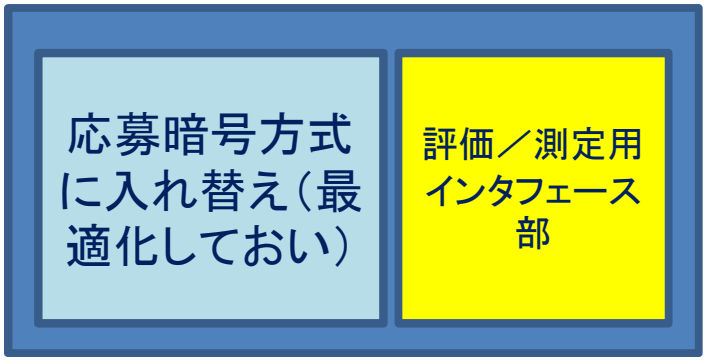
評価対象とする実装について

CRYPTREC暗号実装委員会での議論から



サンプル実装

CRYPTREC事務局で開発し
提案者に提示する。



評価用実装1

提案者が実装する。
変更は最小限度とする。

評価用実装2

提案者が実装する。
（ハードウェアの場合のみ）
サイドチャネル攻撃対策効果の
ある実装の存在確認用