CRYPTREC シンポジウム2009 ― 電子政府推奨暗号リストの改訂に向けて ―
パネル２　「日本の暗号研究と電子政府推奨暗号の今後について」

2009年2月18 日　虎の門パストラル

暗号アルゴリズム管理：目指すべきは制度的裏付けの下に専任の機関が管理し製品化されものを皆が納得して使える“標準暗号”ではないか

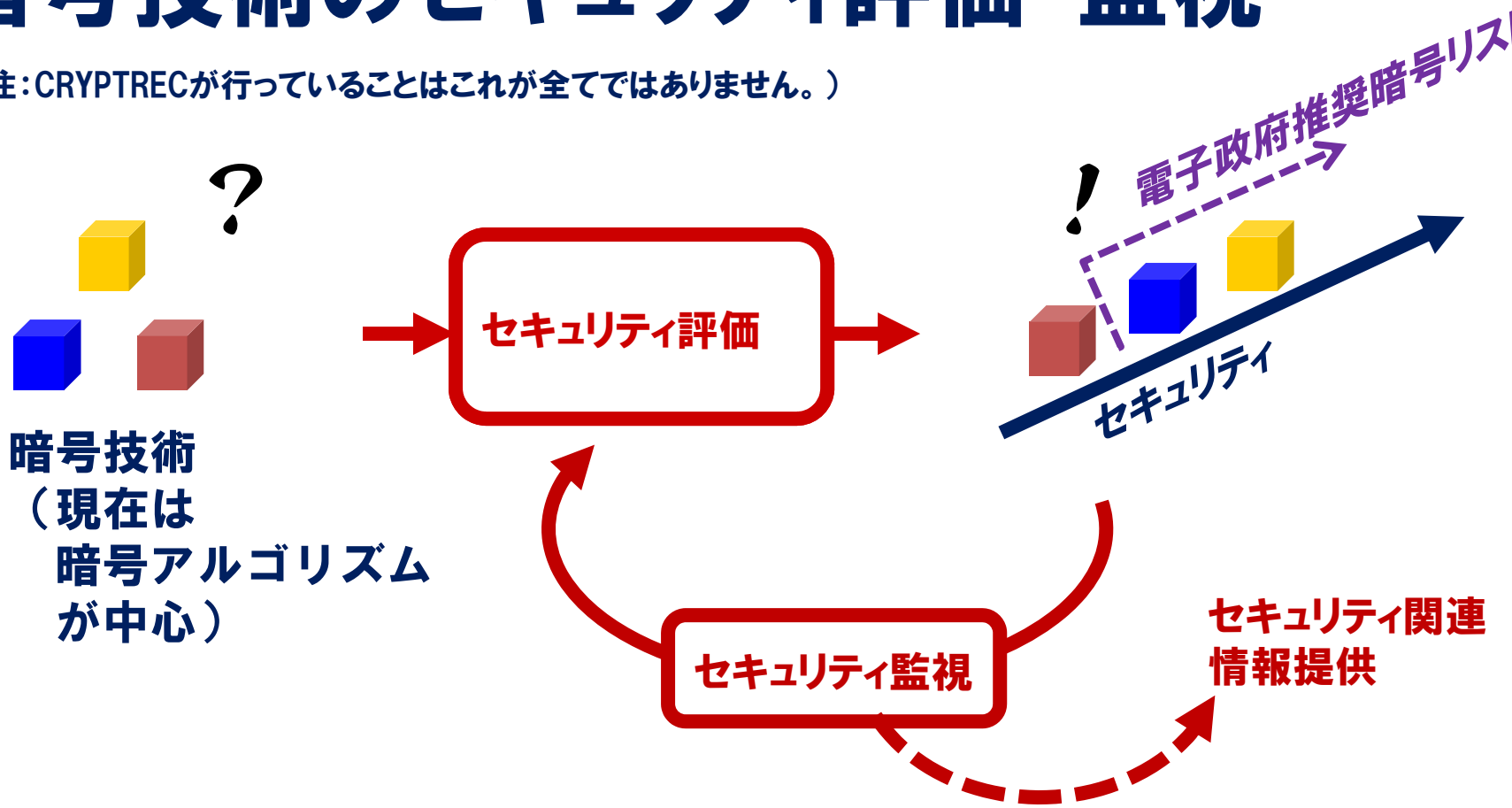
～存在意義・他標準との関係・維持コスト・製品安定供給～

松本　勉

横浜国立大学 大学院 環境情報研究院

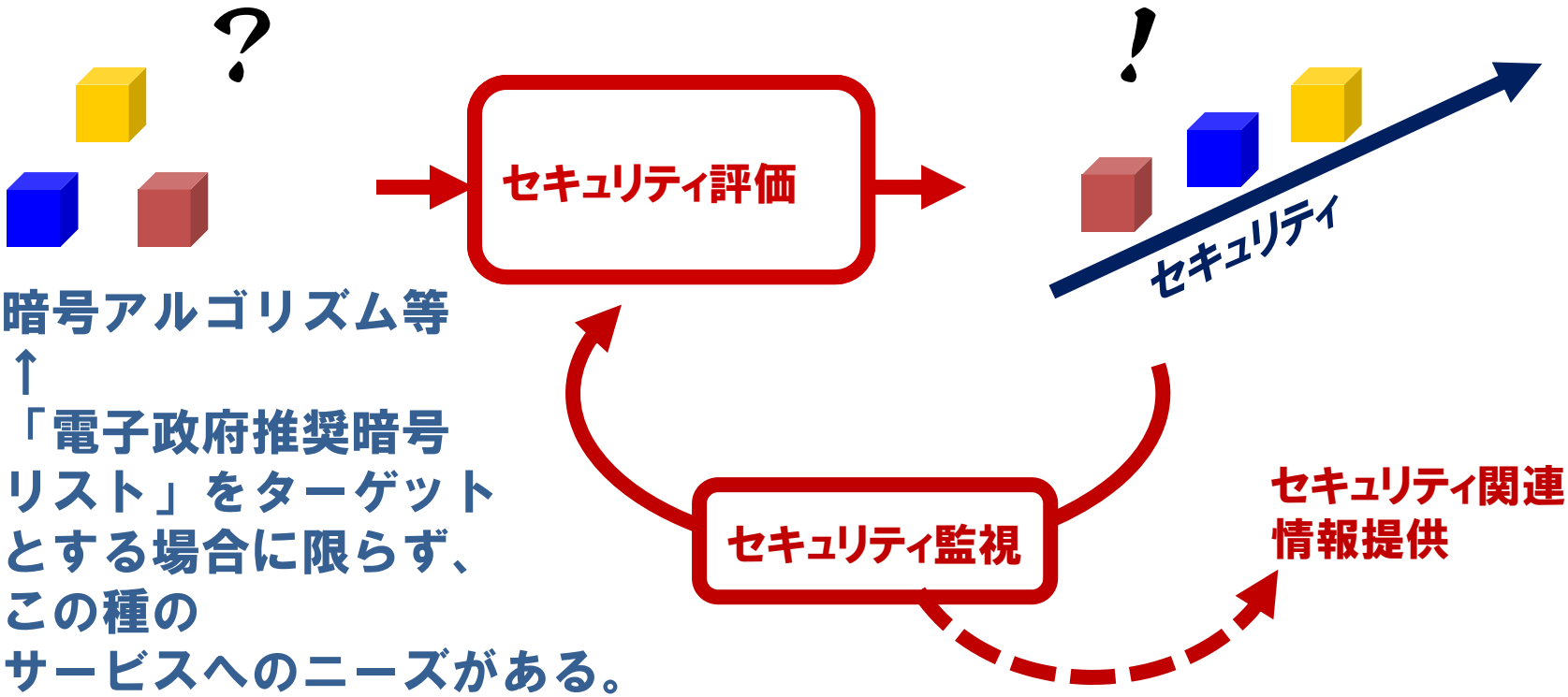
CRYPTRECが実施している暗号技術のセキュリティ評価・監視

（注：CRYPTRECが行っていることはこれが全てではありません。）



CRYPTREC = 暗号技術検討会
および　暗号技術監視委員会、暗号モジュール委員会

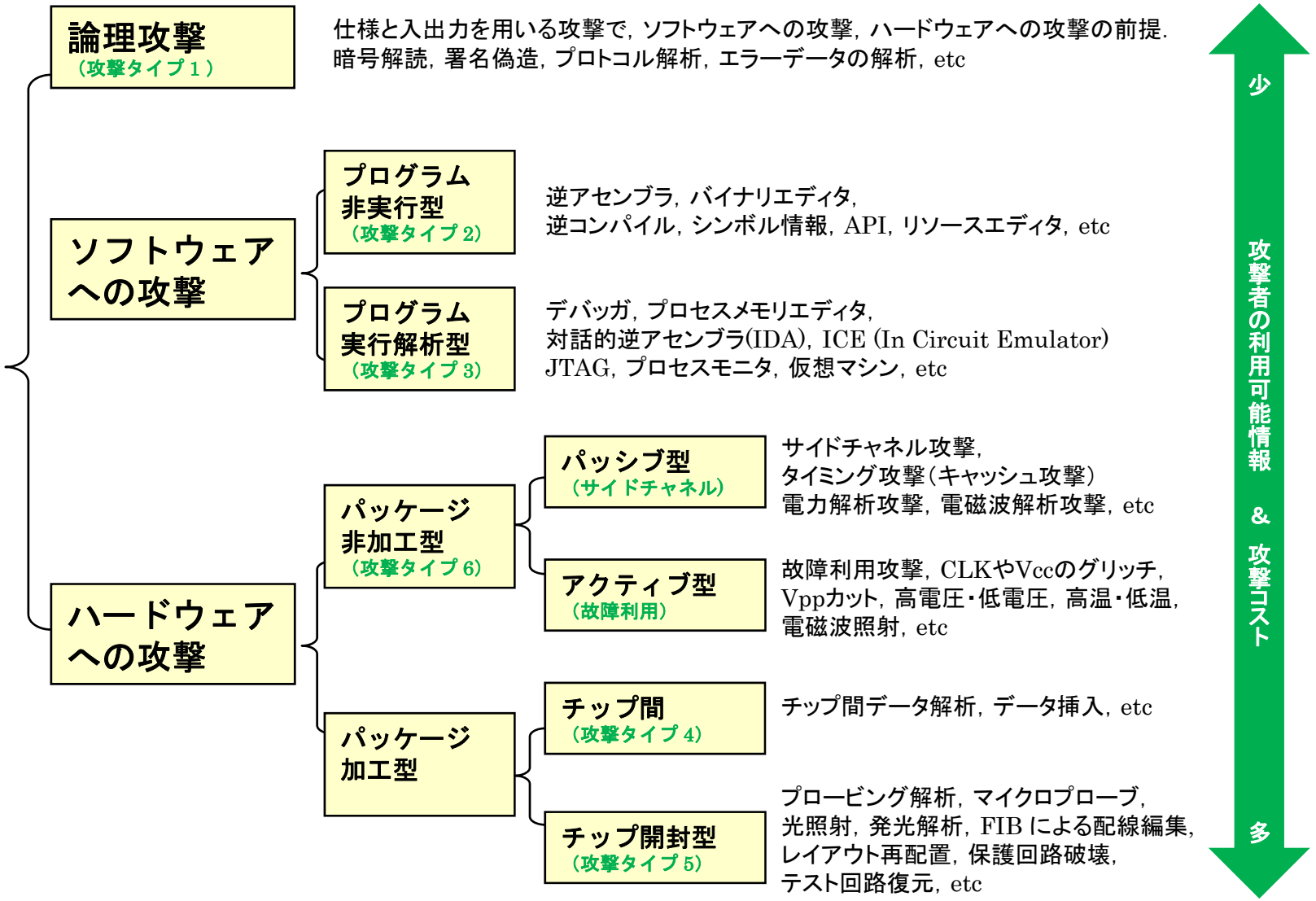
暗号アルゴリズム・プロトコル・システムのセキュリティ評価・監視サービス



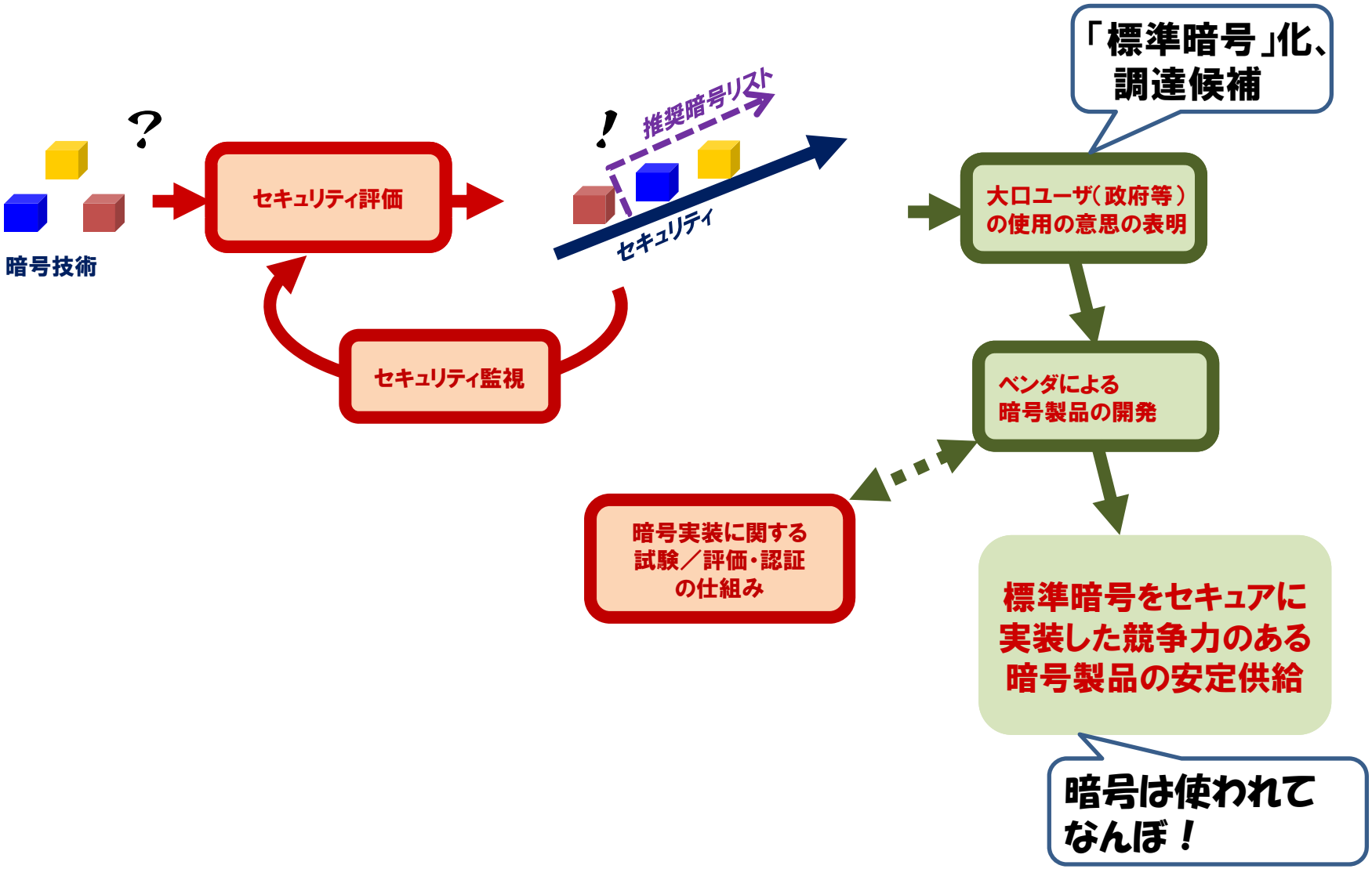
暗号アルゴリズム等
↑
「電子政府推奨暗号リスト」をターゲットとする場合に限らず、この種のサービスへのニーズがある。
↑
しかし、ハイレベルなサービスを中立的に行う能力の獲得と維持には、人材の養成・確保と日々の運用に多大な努力とコストがかかる。

システム(モジュール)に対する攻撃法の分類

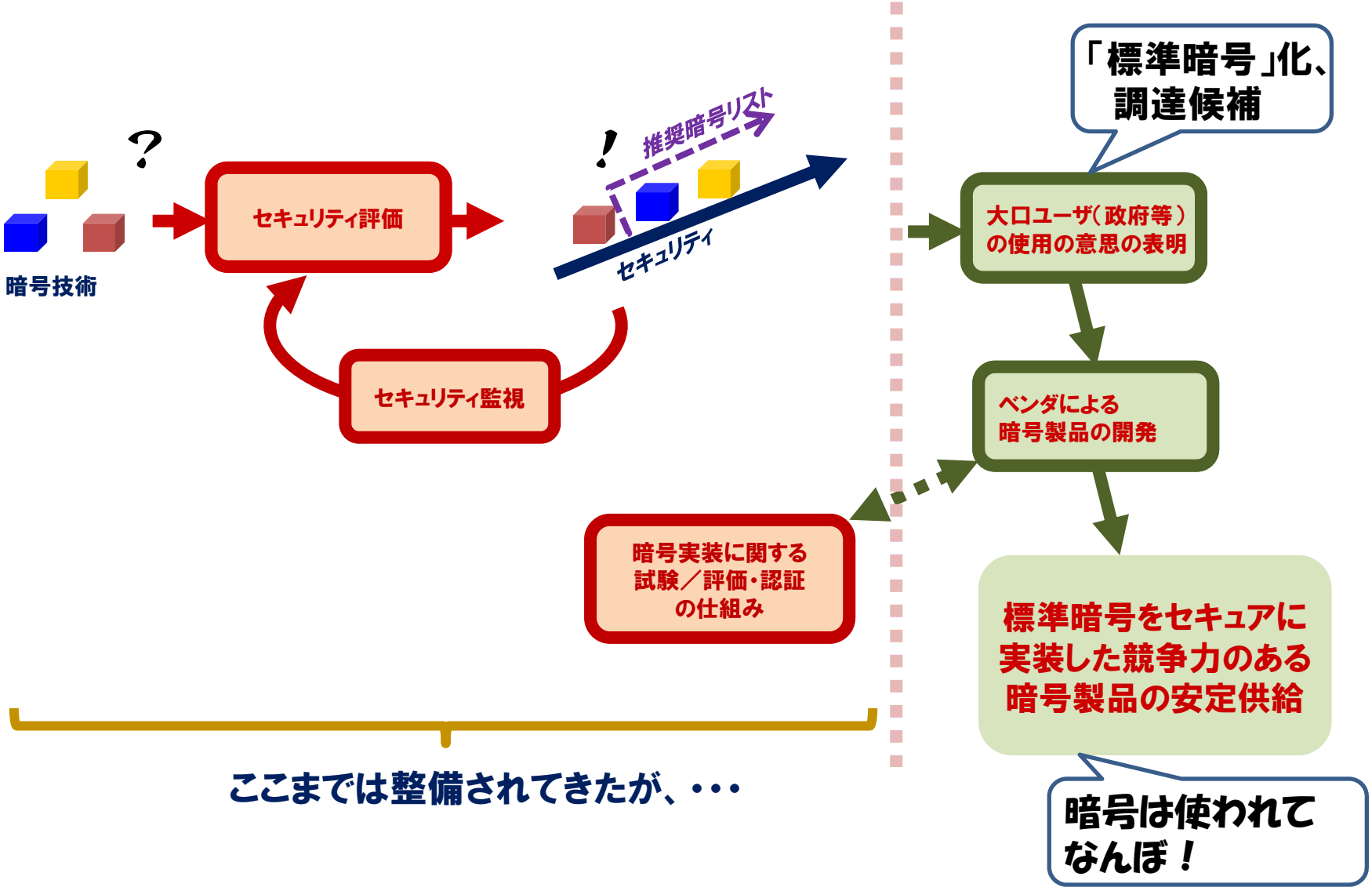
松本 勉, 大石和臣, 高橋芳夫, “実装攻撃に対抗する耐タンパー技術の動向,” 情報処理 Vol. 49, No. 7, pp. 799-809, July 2008.



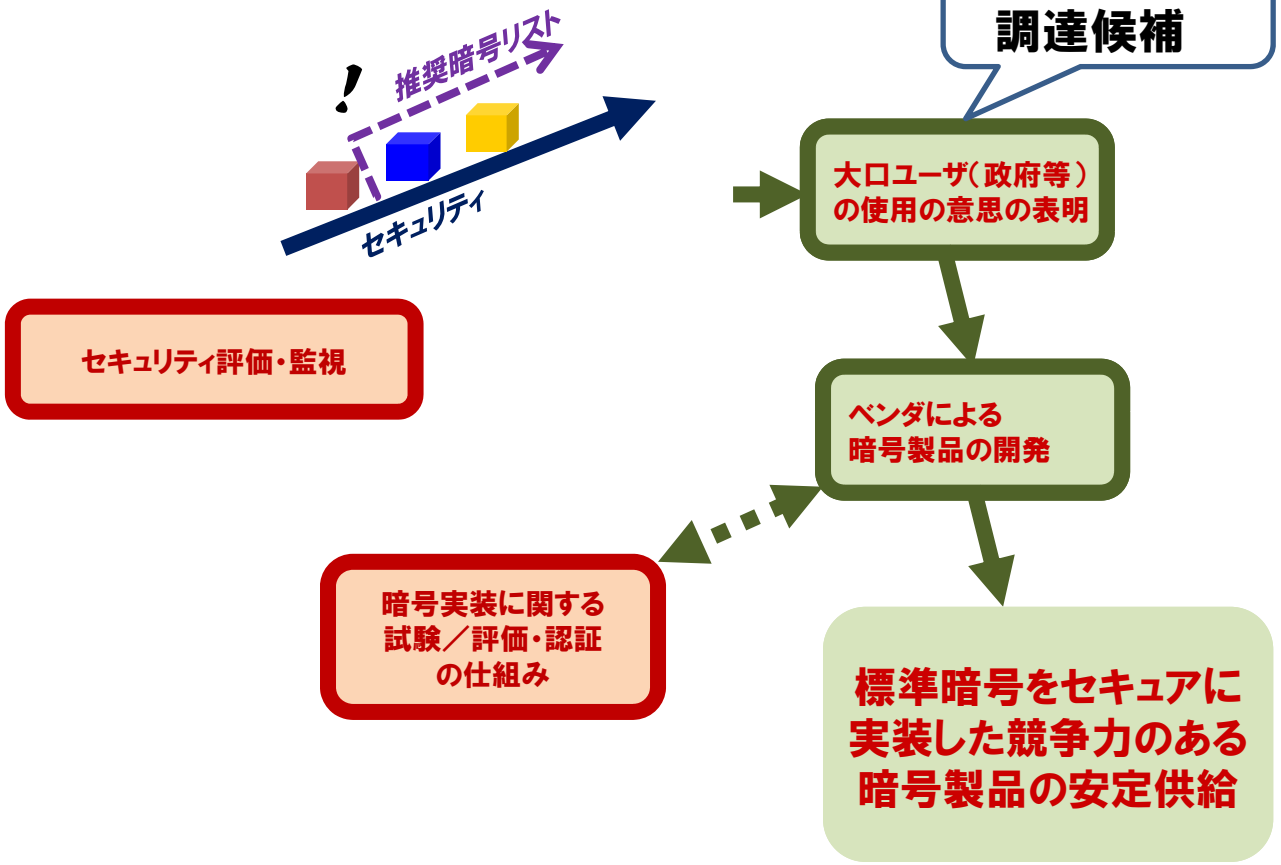
「標準暗号」化と製品安定供給が必要



「標準暗号」化と製品安定供給が必要



「標準暗号」化と製品安定供給の現実



標準化のメリット／目的
社会的コストの低減

- デファクトでない（国産の）暗号はたとえISO/IECで国際標準になっていても普及の点では壊滅状態
- ユーザ側からは製品がないので使えない、ベンダ側からは大口ユーザが見えずコアモジュールの製品化インセンティブがないという、デッドロック／宝の持ち腐れ状態
- 自律的に動く他団体が標準化した暗号を用いる場合、アルゴリズムの変更等への依存関係をどうさばくかも、大きな課題

本当に必要だと(私が考える)もの

- 評価し尽くされ(枯れた)長持ちする汎用の実用暗号アルゴリズムが必須。
  - 厳選されたもの:同じカテゴリなら高々2個。
  - 暗号アルゴリズムとして優れている(セキュアで速く軽く低消費電力)だけではだめで、少数であることが本質。暗号の競争力の点で。
- 専任の機関が(提案者のものとしてではなく)自分のものとして責任をもって維持管理していくことが必要。
  - 暗号アルゴリズムの所有も名前もベンダから独立であるべきではないか。
  - 他ベンダ管理の暗号はユーザの強い希望がなければ採用されにくい。
  - 維持管理を行う専任の機関と、その根拠となる制度・予算が必要
  - 管理コスト(監視・再評価・更新・製品試験のための要員・ツール)を保証する。
  - 開発力のある優れた暗号技術者・研究者の育成と確保。
- 大口(政府)ユーザが使用することを前提とできることが必要。
  - 使用・実装を義務づけられる対象とできるかどうかがポイント。
  - 製品開発の原動力がなければ製品が供給されず使われることはない。

電子政府推奨暗号リスト（仮称）から「仮称」をとる案

- 案1：　電子政府「暗号」リスト
- 案2：　電子政府「標準暗号」リスト

暗号アルゴリズム管理：目指すべきは制度的裏付けの下に専任の機関が管理し製品化されものを皆が納得して使える“標準暗号”ではないか

～存在意義・他標準との関係・維持コスト・製品安定供給～

松本　勉

横浜国立大学 大学院 環境情報研究院