情報システムの暗号危殆化対策とハッシュ関数への期待

松尾真一郎
株式会社　NTTデータ

2006.10.5
IPA暗号フォーラム2006

情報システムにおける暗号技術危殆化対策

情報システムにおいて、サービス仕様によって提示していた安全性を継続的に確保できるようにすること

検討項目
- 暗号モジュール、製品の置き換え
- 既に処理をしたデータの移行
- 移行に関わる運用　など

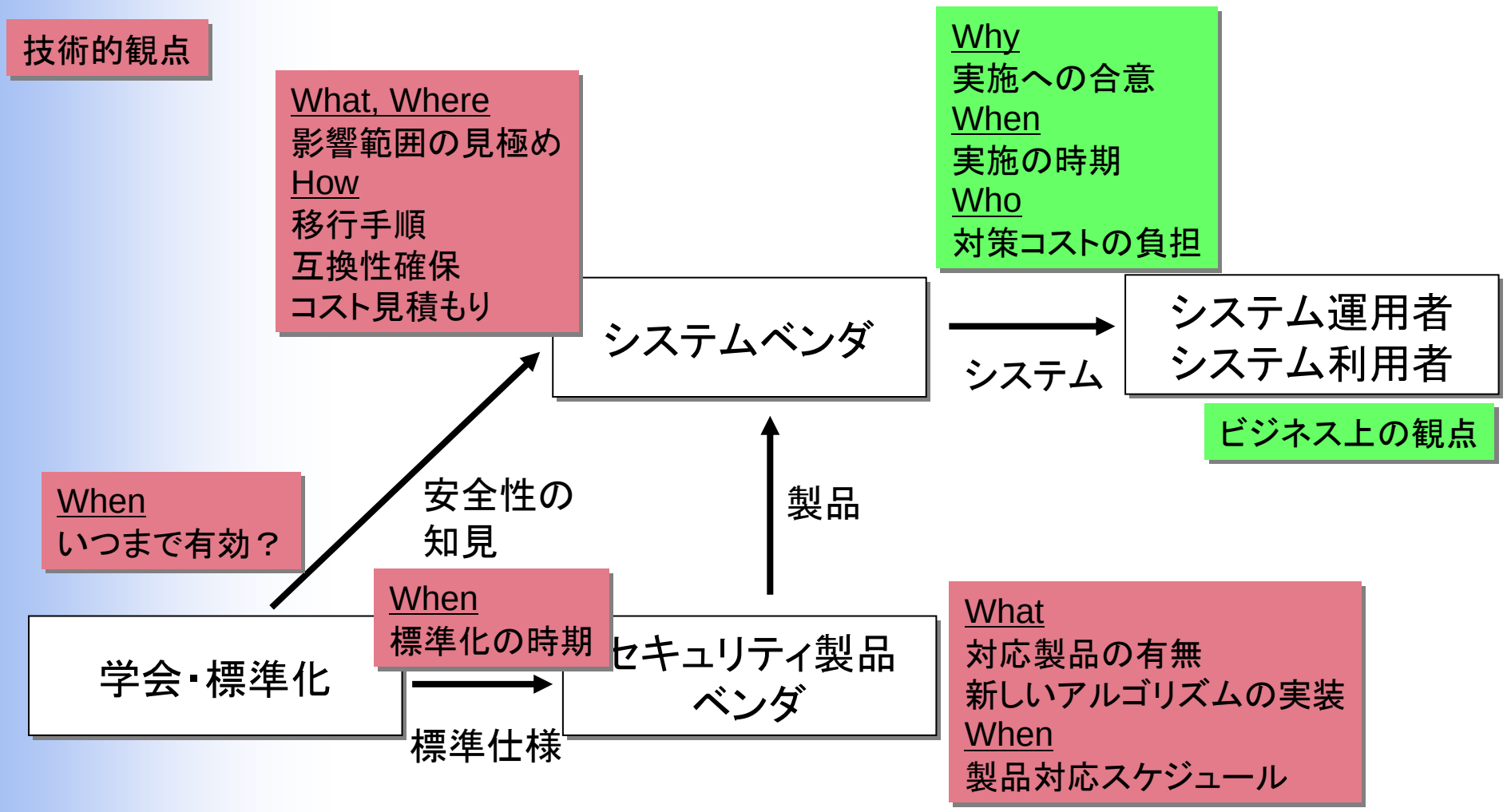
暗号に関係する処理における対策の範囲

情報システムにおける暗号利用形態	利用形態の特徴	対策の概要
通信の暗号化・認証 SSL, IPSec, Kerberos ユーザ認証 OTP, チャレンジ・レスポンス	暗号技術利用がセッション内に閉じている	暗号製品・モジュールの置き換え
ドキュメント・データの暗号化・認証 電子署名、タイムスタンプ PKI、暗号メール	•暗号データや電子署名が長期間使われる。 •広く流通する可能性がある。	•暗号製品・モジュールの置き換え •流通した暗号文、電子署名への対処（更新）

暗号処理以外にも、ハッシュの出力サイズの変更による、通信やDBのデータ構造の変更なども、必要な場合がある。

危殆化対策実施上の課題

ビジネス上の観点、技術的観点で、対策実施上の不明点が多い



システム提供者から見たハッシュ関数の安全性

システム設計者が考える安全性の考え方と、現状のハッシュ関数の
安全性の定義にはギャップが存在

現実のシステムの安全性

- サービス仕様
- リスク分析
- 法的制約
- 技術標準など

- 安全性の前提を定義
- ハッシュ値の有効期限として定義
- 証明可能安全性を求める利用法も（電子政府など）

ギャップ

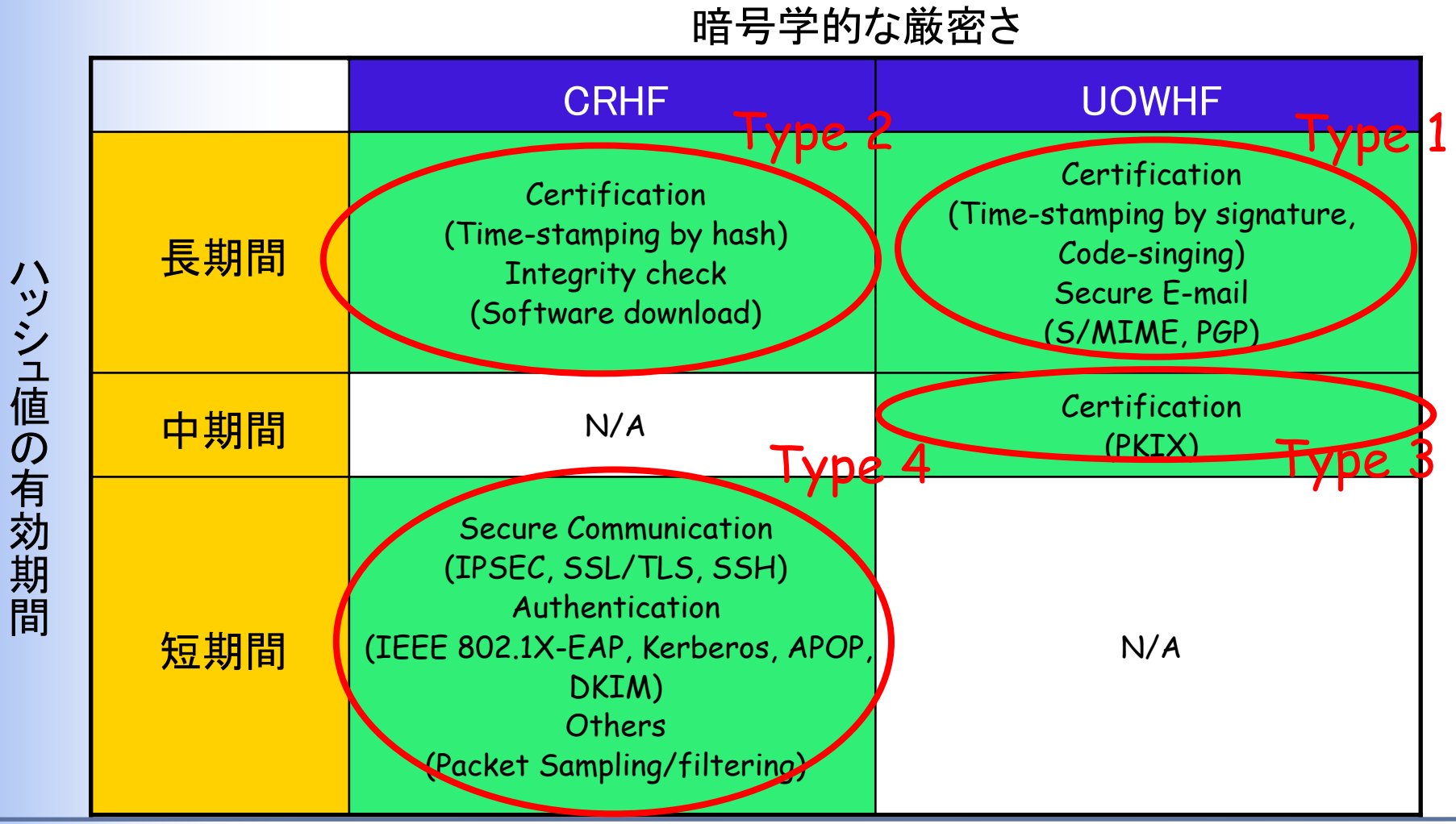
ハッシュ関数の暗号学的安全性

- 衝突困難性
- 第二現像計算困難性
- 一方向性

- 数学的に厳密な安全性の定義
- 有効期間は考慮せず
- 証明可能安全性を持つものはない

ハッシュの安全性の再定義

・必要な厳密さとハッシュ値の有効期間に応じて安全性要件を4つに分類
・4つの分類の特長を生かすようなハッシュ関数の仕様が望ましい



今後の標準ハッシュ関数への要望

- 長期有効性、短期有効性への対応
  - 長期有効性
    - 各種証明書、タイムスタンプなどに適用
    - 証明可能安全性の考慮
  - 短期有効性
    - セッション内のみで有効な利用法への適用
    - より高速な実装、ICカードで実装が容易
- 継続的なシステムの安全性確保のために
  - 互換性の確保（出力ビット長など）
  - 切り替えと継続的な安全性を考慮した、暗号技術の研究