



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



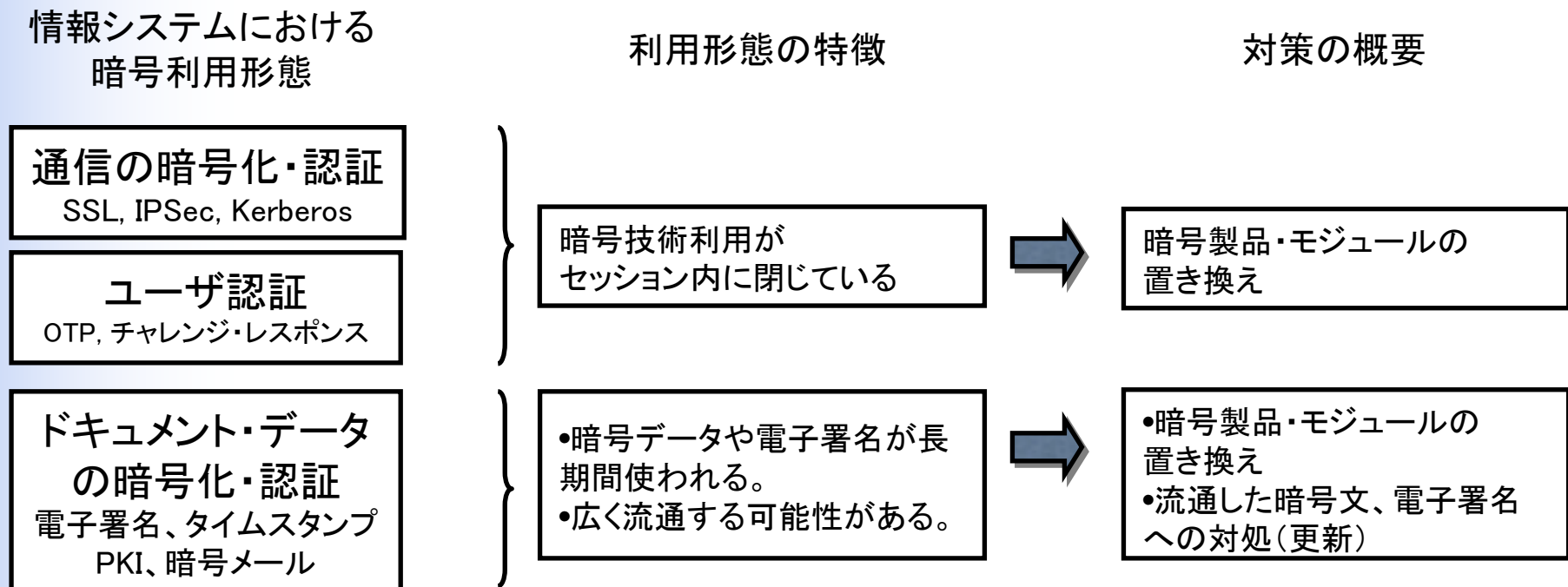
情報システムにおける暗号技術危殆化対策

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

暗号に係る処理における対策の範囲



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

技術的観点

What, Where
影響範囲の見極め
How
移行手順
互換性確保
コスト見積もり

Why
実施への合意
When
実施の時期
Who
対策コストの負担

システムベンダ

システム運用者
システム利用者

ビジネス上の観点

When
いつまで有効？

安全性の
知見

When
標準化の時期

製品

学会・標準化

セキュリティ製品
ベンダ

標準仕様

What
対応製品の有無
新しいアルゴリズムの実装
When
製品対応スケジュール

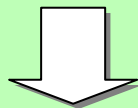


システム提供者から見たハッシュ関数の安全性

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)



ハッシュ関数の暗号的安全性

- 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

暗号学的な厳密さ

	CRHF	UOWHF
ハッシュ値の有効期間	長期間 Certification (Time-stamping by hash) Integrity check (Software download)	長期間 Certification (Time-stamping by signature, Code-signing) Secure E-mail (S/MIME, PGP)
	N/A	中期間 Certification (PKIX)
	短期間 Secure Communication (IPSEC, SSL/TLS, SSH) Authentication (IEEE 802.1X-EAP, Kerberos, APOP, DKIM) Others (Packet Sampling/filtering)	N/A

Type 2 (CRHF, Long-term)
 Type 1 (UOWHF, Long-term)
 Type 4 (CRHF, Short-term)
 Type 3 (UOWHF, Medium-term)



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