高機能暗号の社会実装に係る課題の抽出

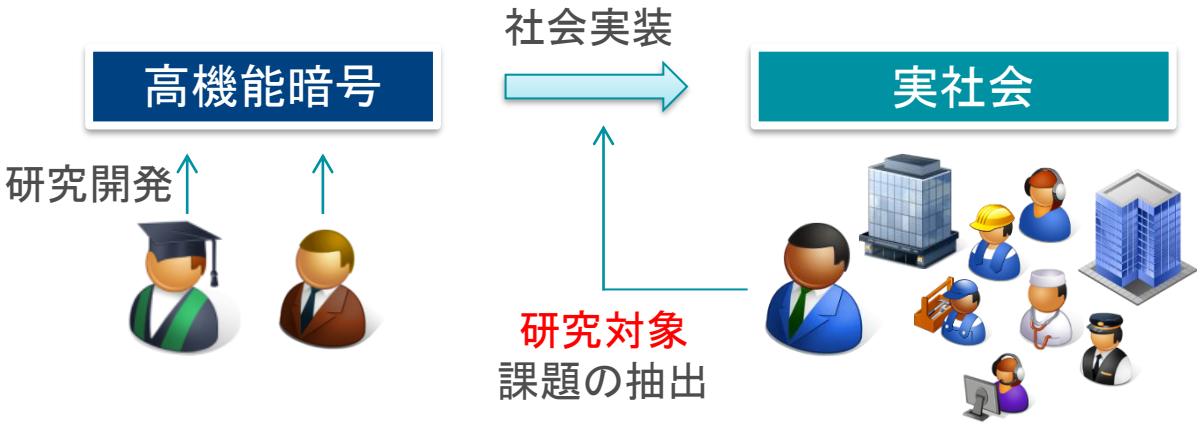
セコム株式会社 IS研究所
○国井 裕樹
伊達 浩行

研究課題

高機能暗号の研究が盛んにおこなわれる中で、

その利便性を広く社会に普及させるために必要な

条件をサービス事業者の観点から分析・考察した。



研究報告

① 高機能暗号の社会実装調査
② 高機能暗号が社会から必要とされる条件の考察
③ 高機能暗号のユースケース考察
④ 高機能暗号の技術要件考察
⑤ 個人情報保護法における暗号の最新動向

ここでの高機能暗号とは

- 共通鍵暗号・公開鍵暗号に続く、機能性に富んだ暗号技術全般の総称
  - 属性暗号
  - 検索可能暗号
  - プロキシ再暗号化
  - グループ署名
  - 集約署名
  - 不正者追跡型放送暗号
  - 時刻制御暗号
  - 等

研究報告①

- 高機能暗号の社会実装調査
  - 高機能暗号を実装したサービス
  - 高機能暗号を用いた実証実験・技術開発

[目的]
社会実装例から高機能暗号へのニーズを把握すること

高機能暗号の社会実装調査

種類	サービス等の名称	実施者	概要
サービス・製品	デジタル貸金庫	東芝	復号せずに鍵付け替え
	マイナンバーセキュア管理システム	日立ソリューションズ	秘匿検索
	パッケージプラス トランスポーター	三菱電機 ビジネスシステム	人の属性により復号権限を制御
	HPE Secure Mail	HP(Voltage)	メールアドレスを暗号化鍵として利用
	Sharemind	CYBERNETICA	秘密計算アプリ構築環境
実証実験・技術開発	化合物DBの類似検索	産総研	秘匿検索
	医療データ統計分析	NTT等	秘密計算
	TLS高速化	富士通研究所等	IDを利用した鍵交換
	Practice-Project	SAP等	クラウドのセキュリティ、完全準同型暗号、ビジネスモデル
	HEAT-Project	KU Leuven等	準同型暗号ツール

高機能暗号の社会実装調査

種類	サービス等の名称	実施者	概要
サービス・製品	デジタル貸金庫	東芝	復号せずに鍵付け替え
	マイナンバーセキュア管理システム	日立ソリューションズ	秘匿検索
	パッケー トランスポーター	ビジネスシステム	り復号権限を制御
	HPE Secure Mail	HP(Voltage)	メールアドレスを暗号化鍵として利用
	Sharemind	CYBERNETICA	秘密計算アプリ構築環境
実証実験・技術開発	化合物DBの類似検索	産総研	秘匿検索
	医療データ統計分析	NTT等	秘密計算
	TLS高		交換
	Practice Project		リティ、完全準同型暗号、ビジネスモデル
	HEAT-Project	KU Leuven等	準同型暗号ツール

ユースケースの要件の検討に利用

運用モデル、技術要件の検討に利用

研究報告②

- 高機能暗号が社会から必要とされる条件の考察
  - 代替手段の有無
  - 法規・ガイドラインによる要請
  - 専門機関による評価
  - 標準化・実装支援
  - 調達仕様
  - 特許・ライセンス
  - 利用者の認識と暗号のユーザビリティ

[目的]

高機能暗号が広く普及するための条件を多方面から考察する。

社会から必要とされる条件

- 代替手段の有無

（例）プロキシ再暗号ストレージサービス
目的：常時暗号化＆効率的アクセスコントロール

代替手段1
都度暗号化＋ID/PWアクセスコントロール

- 端末側で暗号化
  → 通信帯域・コストが高くなる
- クラウド側で暗号化
  → クラウド側での計算リソースの占有

頻度によっては、許容できる計算・通信コストとなりうる

代替手段2
信頼できる企業＋ID/PWアクセスコントロール

- 平文で保存
  → 内部犯行による覗き見などのリスク

国内の信頼できる企業であれば、おおよそ対策済みでリスクが許容できる

コストとリスクの許容によってプロキシ再暗号の利用モチベーションは低下

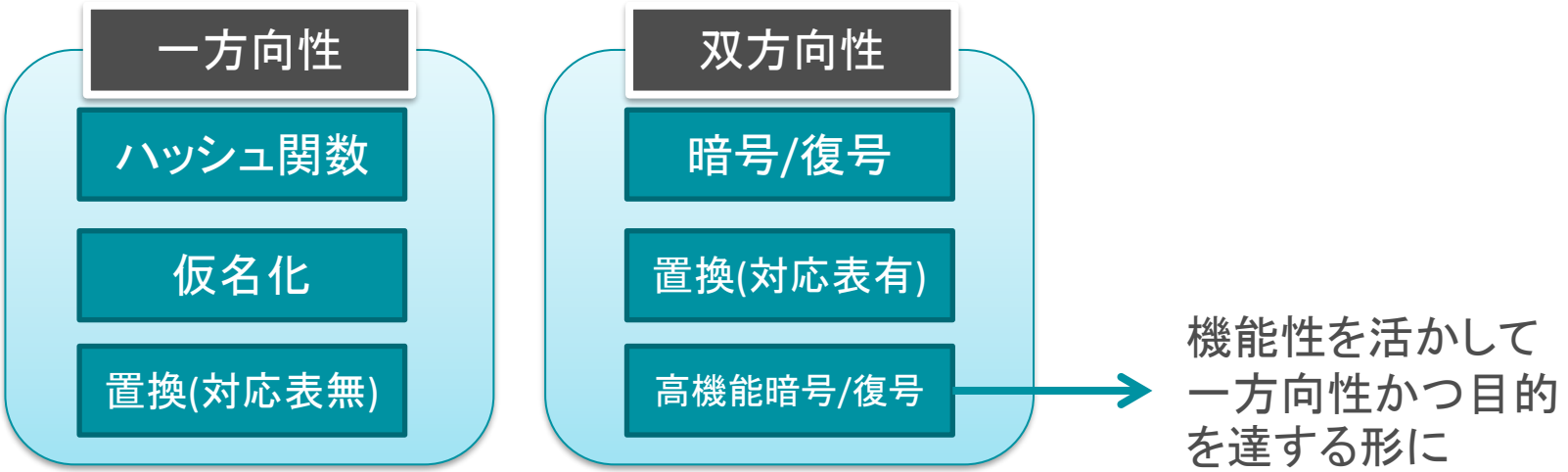
社会から必要とされる条件

- 法規ガイドラインによる要請
  - 個人情報保護法と暗号化の関係

	個人情報保護法	改正個人情報保護法
成立	2003年05月23日	2015年09月03日
施行	2005年04月01日	2016年01月01日一部施行 2017年05月30日全面施行
個人情報の定義	氏名・生年月日・その他記述等 特定個人を容易照合・識別	氏名・生年月日等・その他記述等 文書・記録・音声・動作・個人識別符号等 特定個人を容易照合・識別
暗号化の立ち位置	漏えい・滅失・棄損等防止のための安全管理措置	漏えい・滅失・棄損等防止のための安全管理措置
その他		匿名加工情報の追加

高機能暗号と改正個人情報保護法

- 暗号 → 安全管理措置
  - これを高機能暗号に置き換えることは代替手段の観点から考えて難しい
- 匿名加工に着目
  - 「復元することのできる規則性を有しない」＝「一方向性」



研究報告③

- 高機能暗号のユースケース考察
  - プライバシーの観点でのユースケース
  - 機密情報保護の観点でのユースケース

[目的]

高機能暗号へのニーズや普及のための条件をもとに利用者とサービス提供者、双方の視点でユースケースを考察

ユースケース例 一覧

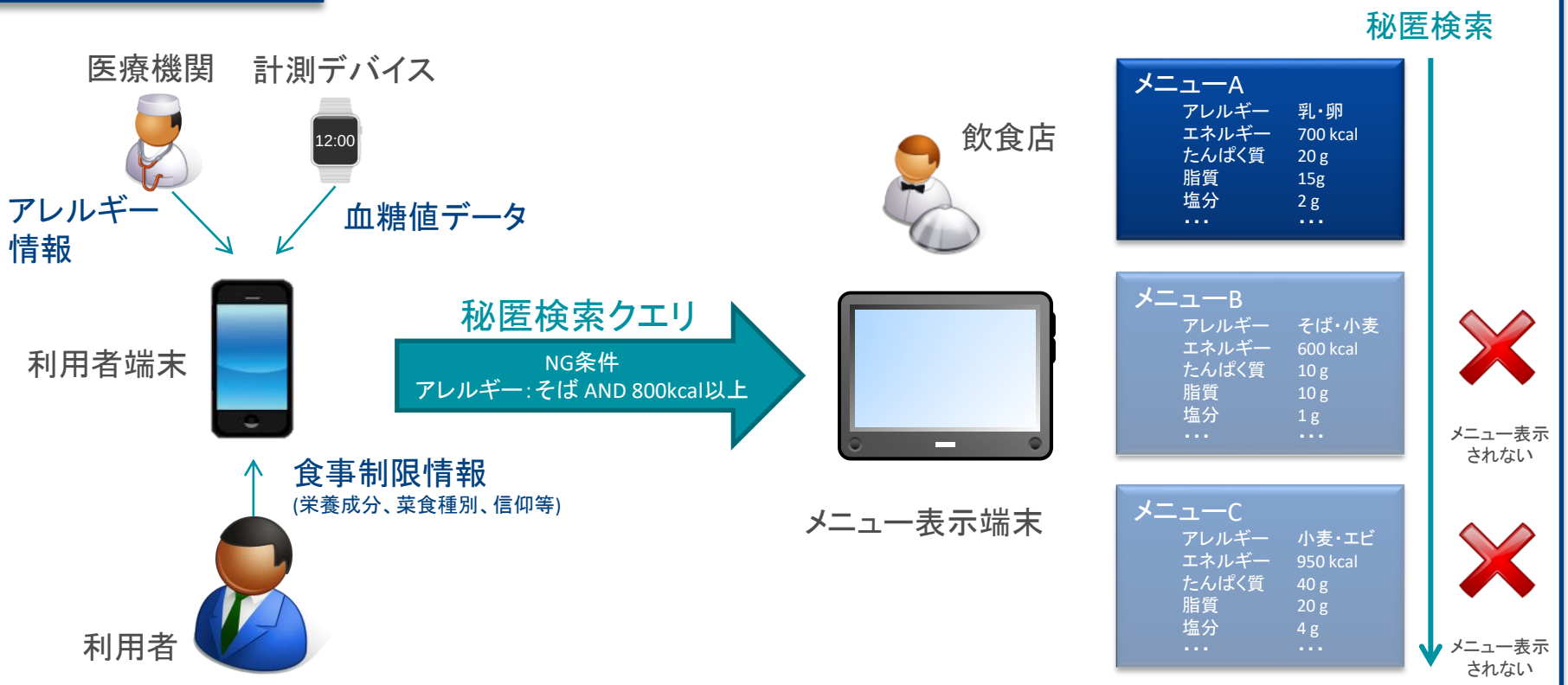
- プライバシー保護の観点
  - アレルギー等の秘匿検索
  - 秘匿保険料シミュレーション
  - 実臨床下での薬効の測定における秘匿分析
- 機密情報保護の観点
  - 多数の利用者が接続する監視カメラの映像データ秘匿
  - パケットの優先順位情報の保証

ユースケース例

アレルギー等の秘匿検索

食事のメニュー選定においてアレルギー情報や食事制限情報を
秘匿したまま条件に合ったメニューのみを表示できる

運用モデル



ユースケースの妥当性評価と課題

- 代替手段の有無
  - 条件検索でも一致検索のみであればハッシュ計算や共通鍵暗号でも可能だが、大小比較や検索条件の論理式結合も扱うのであれば検索可能暗号などの高機能暗号を使うことでしか実現しない。
  - 利用者の個人情報保護とサービス提供者のプログラム保護を両立させるための重要なパラメータ等の秘匿で、プログラムの単純な暗号化などでは代替できない。
- 法規・ガイドライン
  - PDSのデータ利用ガイドラインなどの制定
- 調達仕様・専門機関による評価
  - CRYPTREC電子政府推奨暗号リストに選定、CMVP/JCMVPでの製品評価
- 標準化・実装支援
  - ISO、IETFなどへの標準化組込み

研究報告④

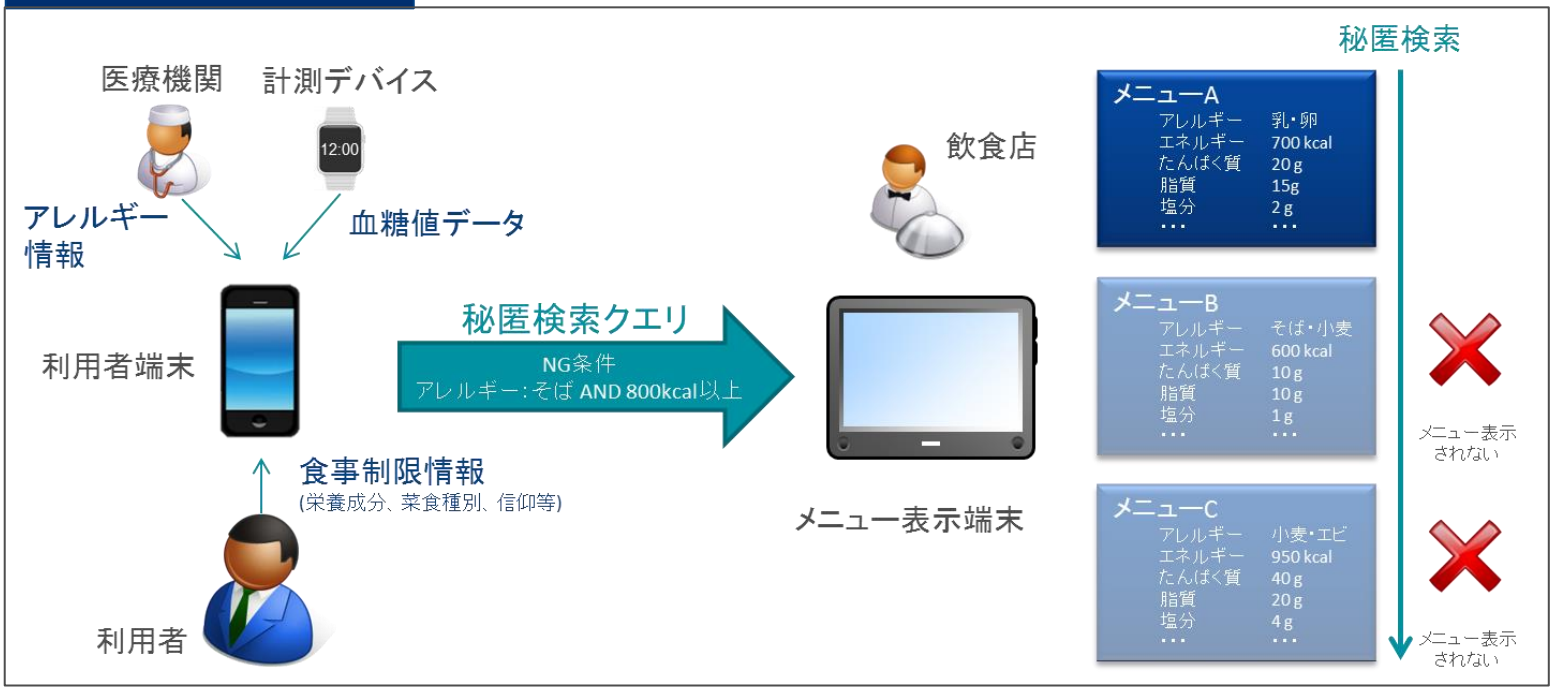
- 高機能暗号の技術要件考察
  - 高機能暗号の機能要件
  - 高機能暗号の性能要件

[目的]

ユースケースを実現するために高機能暗号に求められる技術要件を考察し、技術的課題抽出の一助とする。

運用モデルと技術要件

運用モデル



高機能暗号の機能要件

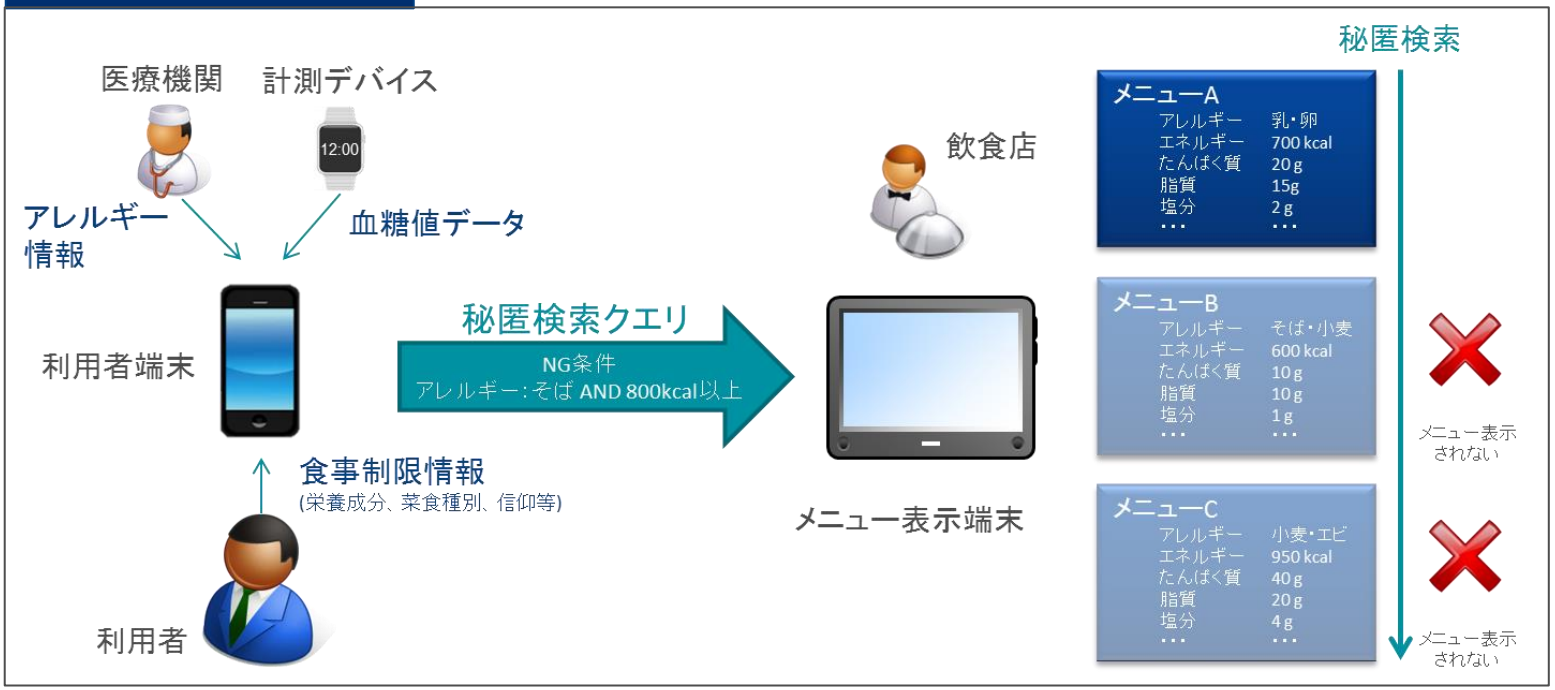
- 暗号文に対して秘匿クエリを実行し1 or 0を得る。
- 一致検索、比較検索、論理式結合に対応可能。
- 複数条件判定でどの項目で一致したかは検索者に秘匿可能

実サービスでの追加要件

- 検索処理の実行証明
- 秘匿性を強めるため検索対象外の項目も全て補完したクエリで検索を実行
- 利用者環境が多様なためサービス提供者側で検索処理の実行

運用モデルと技術要件

運用モデル

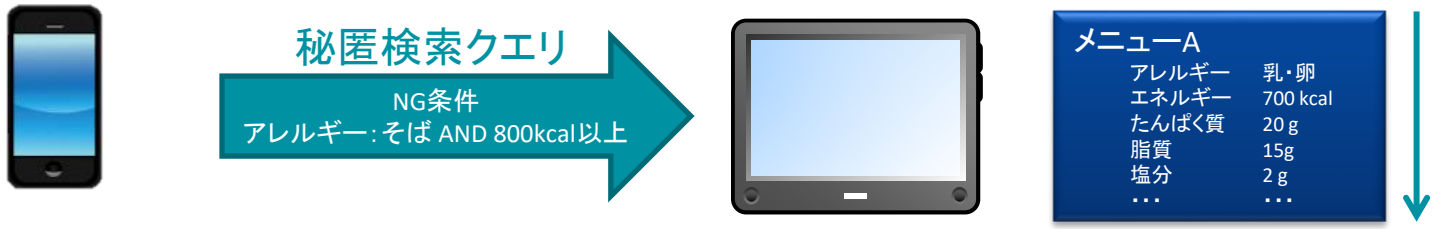


考察点

データ形式	鍵更新	端末/サービス認証	トラストアンカの配置
収益モデル	マルチベンダ対応	デバイスセキュリティ	ICカード対応

運用モデルと技術要件

- 性能要件
  - 目標
    - ユーザー操作後からメニュー表示まで10秒以内
    - 利用者：スマートフォン、サービス提供者：タブレットで実現
  - 各パラメータ
    - 検索対象項目：64項目（アレルギー品目28種＋栄養素表示6種＋他項目30 ）
    - メニュー数：100種
    - NFC通信速度：13KBps～53KBps



速度

- 鍵生成：1秒
- クエリ生成：1秒(64項目)
  ※1÷64 = 16ミリ秒/項目
- クエリ送信：4秒
- 暗号処理：2秒
- 検索処理：2秒
  ※2÷6400 = 0.3ミリ秒/項目

データ

- 鍵：2KB
- プログラム：100MB
- クエリ：128KB(64項目)
  ※2KB×64=128KB
- 検索対象：13MB(6400項目)
- プログラム：100MB

ここまでのまとめ

高機能暗号のユースケースを、これまでの社会実装の実例などを基に検討対象とした。

高機能暗号が組み込まれるサービス・システムの技術要件として、運用時の鍵管理問題やマルチステークホルダー間での証明書の配置などの技術要件について検討し、その方式に必要な性能要件を見積もった。

⑤個人情報保護法における暗号の最新動向

- PPC(個人情報保護委員会)の告示等
  - 個人データ漏えい等の事案発生時にPPCへの報告を要しないケース
    - 高度な暗号化等の秘匿化
    - 手段が適切に管理されている
    - 適切な評価機関等により評価された暗号技術
  - これまでは暗号化によって本人連絡等は不要だったが主務大臣への報告は必要だった
  - 生体認証などで用いるテンプレート保護技術にも言及
    - 高機能暗号の活用が期待される分野

研究報告

① 高機能暗号の社会実装調査
② 高機能暗号が社会から必要とされる条件の考察
③ 高機能暗号のユースケース考察
④ 高機能暗号の技術要件考察
⑤ 個人情報保護法における暗号の最新動向

おわりに

本発表で示した成果は、一部、国立研究法人新エネルギー・産業技術総合開発機構（NEDO）の委託業務「平成27年度エネルギー・環境新技術先導プログラム/高機能暗号を活用した革新的ビッグデータ処理の研究開発」の結果得られたものであり、電子商取引安全技術組合からの再委託により実施したものである。