認証運用領域報告

岡部寿男 (京都大学；幹事)
高井昌彰 (北海道大学；幹事補佐)
飯田勝吉 (東京工業大学)
垣内正年 (奈良先端科学技術大学院大学)
鈴木孝彦 (九州大学)
西村浩二 (広島大学)
湯浅富久子 (高エネルギー加速器研究機構)

活動の経緯

- 検討課題
  - 政府機関統一基準のうち認証が関連する部分の検討を行う
- 作業経過
  - 「4.1情報セキュリティについての機能」の集中検討
  - 第6部ほか関連する部分の検討
  - 証明書ポリシー(CP)、認証実施規定(CPS)に関して、先行2大学のCP/CPS案をベースに議論

サンプル規定集への対応

- 基本方針
  - 政府機関統一基準を変えないで使えるころはできるだけそのままにする
  - 教員が（少なくとも行例事務に相当する作業を行うときは）行政事務従事者としての扱いを受けるべきであるという原則を確認
- 大学の実情との整合
  - 解説は基準ではないので必ずしもそれにとらわれない

（例）政府機関統一基準4.1.1(1)(f)(イ)

- 利用者が設定した主体認証情報を他者が容易に知ることができないように保持する機能

（解説）「**不可逆の暗号化**を用いるなどにより、」

APOPなどと不整合

A2101 情報システム運用･管理規程

第四章　主体認証

第42条（主体認証機能の導入）

→政府機関統一基準の対応項番4.1.1(1)

第五章　アクセス制御

第43条（アクセス制御機能の導入）

→4.1.2(2)

第44条（利用者等による適正なアクセス制御）

→4.1.2(3)

第六章　アカウント管理

第46条（アカウント管理機能の導入）

→4.1.3(1)

第47条（アカウント管理手続の整備）

→4.1.3(2)

第八章　暗号と電子署名

第63条（暗号化機能及び電子署名の付与機能の導入）

→4.1.6(1)

第64条（暗号化及び電子署名の付与に係る管理）

→4.1.6(2)

主な検討

A2101-63（暗号化機能及び電子署名の付与機能の導入）（政府機関統一基準の対応項番4.1.6(1)）

5 部局技術責任者は、暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいて、アルゴリズムを選択するに当たっては、必要とされる安全性及び信頼性について検討を行い、電子政府推奨暗号リストに記載されたアルゴリズムが選択可能であれば、これを選択すること。ただし、新規（更新を含む。）に暗号化又は電子署名の付与のアルゴリズムを導入する場合には、電子政府推奨暗号リスト**又は、本学における検証済み暗号リストがあればそ**の中から選択すること。なお、複数のアルゴリズムを選択可能な構造となっている場合には、少なくとも一つをそれらのリストの中から選択すること。

大学においては電子政府推奨暗号リスト未記載の暗号を使いたいケースがありうる
(例) ・国外機関との共同研究契約
・当該大学で開発され安全性の確認された新暗号

CP/CPS

- UPKIイニシアティブでの共通仕様
  「キャンパスPKI CP/CPSガイドライン」
  の策定に参画
  現在、フォーラムにて公開・意見募集中
  https://upki-portal.nii.ac.jp/item/inews/news006
- **今回のサンプル規程では**
  - A**大学ではIDとパスワードによる利用者認証を対象**
  - PKI**を使用した認証のための**CP/CPS**は（当面）上記仕様へのリンクとする。**
    - A2601 **証明書ポリシー**(CP)
    - A2602 **認証実施規程**(CPS)

４．認証運用領域

幹事 岡部寿男、幹事補佐 高井昌彰

4.1 検討課題

大学における電子認証基盤の運用と利用について必要な規程について検討する。

4.2 検討経過

第１回領域分科会会合（8 月 31 日）において、「4.1 情報セキュリティについての機能」についての集中的検討ならびに第６部ほか関連する部分の検討を行った。また、証明書ポリシー（CP）、認証実施規定（CPS）に関して、東工大・阪大の CP/CPS 案をベースに議論した。

4.3 検討内容の概要

政府機関統一基準のうち認証が関連する部分の検討を行った。認証はセキュリティの根幹であることから、統一基準を変えないで使えるところはできるだけそのままにすることを原則とする。

A2101 運用・管理規程中、第四章 主体認証（政府機関統一基準 4.1.1 に対応）、第五章 アクセス制御（同 4.1.2 に対応）、第六章 アカウント管理（同 4.1.3）において、他の分科会と連携し、政府機関統一基準をほぼそのまま取り込む形で規定とする。

・ 推奨暗号リスト

また第八章「暗号と電子署名」については、電子政府推奨暗号リストにない暗号も使うことができるような修正を提案した。

・ 教員の位置付け

教員が（少なくとも行例事務に相当する作業を行うときは）行政事務従事者としての扱いを受けるべきであるという原則を確認し、他の分科会との調整を図った。

・ CP/CPS

認証に PKI を利用する際の CP/CPS については、UPKI イニシアティブのプロジェクトとしてアウトソースモデルに基づくものがフォーラム内で公開され意見募集中である。これについては公開前の段階で政府機関統一基準との整合性をチェックし問題ないことを非公式に確認した。ただし、他の部分との整合性から、今年度のサンプル規程集においては A 大学では認証に PKI を利用していないものとし、当該 CP/CPS の公開にあわせて参考情報としてその URL を記載することにした。

4.4 今後の課題

解釈上工夫が必要な箇所を解説として盛り込む作業については未完である。