資料1

# 高等教育機関の情報セキュリティ対策のためのサンプル規程集について

2012年3月19日
神戸学院大学経営学部
小川 賢

平成23年度第3回学術情報基盤オープンフォーラム

# セキュリティポリシーとクラウドサービスの導入

# 高等教育機関の情報セキュリティ対策のためのサンプル規程集

- 概要
  - 雛型となるセキュリティ関連の学内規程とその解説
  - 標準的かつ活用可能な大学向けのサンプル規程集
  - 各大学（および各種機関）でカスタマイズ
  - 政府機関統一基準とその考え方に準拠
    - 特に事務情報システム
  - 専門家集団による策定
  - 2007年10月公開 改訂を継続（2010年版は46編704p）
    - http://www.nii.ac.jp/csi/sp/ 公開中

# 統一基準におけるクラウド対応

解説の追加

- 管理基準
  - 外部委託に外部設備を利用したサービスが含まれる
  - 外部設備を利用する場合にデータの所在に留意
  - IT部門を通さずにITに相当する外部委託発注を想定
- 技術基準
  - 通信回線の用語定義に仮想ネットワークを想定
  - サーバの共用を想定

- クラウド対応として新たな規則の作成はなし

# サンプル規程集におけるクラウド対応の検証

## 検証する規則とその条項

- 情報の抹消（用語定義）
- 学外での情報処理（事務情報システム対策基準）
- 本学支給以外の情報システムによる情報処理（運用・管理規程第86条～第87条）
- 主体認証・アクセス制御・権限管理・証跡管理・保証等の標準手順（運用・管理規程第57条～第78条）
- ドメイン名の利用（運用・管理規程第89条）
- リモート保守（運用・管理規程第12条第1項）

# 学外への情報の提供

- 外部委託
  - 大学が保有する個人情報を委託先に預ける
  - 個人情報の取扱責任は大学（委託先の監督責任も）
  - 契約に基づく場合：外部委託における情報セキュリティ対策実施手順
    - 委託元としての責任者が遵守すべき手続き
  - 約款に基づく場合：約款による情報処理サービス
    - サービスを利用する上での要件が許容できるものであるか
- 第三者提供
  - 大学が保有する個人情報を大学以外の事業者が利用可能に
  - 個人の同意が前提
- その他

# 本学情報システムと約款による情報処理サービスの違い

- （サンプル規程集が対象とする）本学情報システム
  - 情報処理及び情報ネットワークに係わるシステム
    （本学情報ネットワークに接続する機器を含む）
    - 本学により、所有または管理されているもの
    - 本学との**契約**あるいは他の協定に従って提供されるもの
- 約款による情報処理サービス
  - 情報セキュリティ以外の契約内容については要求に基づいて用意される又は条件選択や修正ができる
  - 情報セキュリティに関する事項に条件選択の制限

# 大学等が外部委託の際にとるべき情報セキュリティ対策の規程（手順）

# 外部委託における情報セキュリティ対策実施手順－１

- 委託元としての責任者が遵守すべき手続き

  外部委託による業務遂行に必要な情報セキュリティ水準の確保

  - 可否の判断
    - 重要な情報を取り扱う情報処理業務は原則禁止
  - 調達：委託先の選定基準
    - 委託する情報処理業務に対する安定性を有する
    - 業務の実施に求められる情報セキュリティ対策等を遵守
    - 委託先に実施させる情報セキュリティ対策の範囲を定める
    - 委託先に実施させる情報セキュリティ対策を調達仕様として周知
    - 情報セキュリティが侵害された場合の対処手順
    - 情報セキュリティ対策の履行状況の確認

# 外部委託における情報セキュリティ対策実施手順－２

- 委託元としての責任者が遵守すべき手続き

  外部委託による業務遂行に必要な情報セキュリティ水準の確保

  - 契約
    - 委託先に実施させる情報セキュリティ対策の明示
    - 外部委託に係る確認書の提出
  - 実施中
    - 取り扱う情報の秘密保持等
    - 情報セキュリティ対策の履行状況の確認
  - 納品・検収

# 調達仕様において委託先に求める情報セキュリティ対策等（例）

| 委託する業務の分類 ／ 情報 セキュリティ対策等 | 情報システムの構築等 | 情報システムの運用 | | | | | 情報システムの 保守・点検 | 情報の加工・処理等 | 情報の保存・運搬 |
|---|---|---|---|---|---|---|---|---|---|
| | | オンサイトサービス | リモート運用サービス | データセンター | ASP サービス | ハウジングサービス | | | |
| (1) 体制の整備 | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ※ |
| (2)取扱う情報の秘密保持等 | ○ | ○ | ○ | ○ | ○ | ○ 物理的対策 | ○ | ○ | △ |
| (3)セキュリティ機能の装備 | ○ | × | × | × | × | × | × | × | × |
| (4)運用・保守・点検における情報セキュリティ対策の実施 | × | △ | △ | △ | ※ | × | △ | × | × |
| (5)脆弱性対策の実施 | ○ | △ | △ | △ | ※ | × | △ | × | × |
| (6)サービスレベル | × | △ | △ | △ | △ | △ | △ | × | × |
| (7)情報セキュリティが侵害された場合の対処 | △ | △ | △ | △ | △ | △ | △ | △ | ※ |
| ・・・ | ・ | | | | | | | | |

# 「約款による情報処理サービス」の利用に際しての注意事項

- 処理された結果生じる著作権等の権利の放棄や移管が利用条件となっている場合
- 約款上データ消去等をサービス利用者側で直接実施できない場合
- 利用したデータの削除についてサービス 提供者が個別には応じないことや、情報の置き場所が特定の場所に固定されず、海外の法執行機関等による予期せぬアクセスが行われる場合

# 無償で利用する情報処理サービスも外部委託にあたるかも

- 無償で利用を開始できる場合であっても、外部委託に該当する場合があるので関連規則を遵守することが必要
  - 無償で提供されているメールサービスの利用
  - アンケート記入及び集計に係るウェブサービスの利用
  - オンラインストレージサービスの利用
- このようなサービスの利用者が調達に従事する教職員に限られたものではないため、当該留意事項について学内に広く周知する必要がある

# 大学等が外部委託時に確認すべき情報セキュリティ対策事項

# 約款による情報処理サービスの利用における利用時の留意事項－１

| | |
|---|---|
| 1 | サービスは約款の範囲でしか提供されない。 |
| 2 | サービス時間とサポート時間が限られている場合がある。 |
| 3 | サービスのセキュリティポリシーが開示されないことが多く、ポリシー及び実施規程を満たしているか判断が困難である。 |
| 4 | サービス提供事業者から提供されるサービスレベルは可用性のみであることが多い。 |
| 5 | サービス提供事業者は利用者による監査を基本的に受け入れない。 |
| 6 | バックアップ実施や障害発生時の復旧等の実施内容やタイミングといった、情報システムの運用に関しては約款に記載されていないことが多い。 |
| 7 | バックアップするデータ形式が他の事業者のサービスに移行できない場合がある。 |
| 8 | 利用者側で情報のバックアップができない場合がある。 |
| 9 | 同一サーバ上で複数の業務（利用者）を実行しているケースがあり、その場合セキュリティ対策が十分に実行されていない業務の影響を受ける可能性がある。 |

# 約款による情報処理サービスの利用における利用時の留意事項－２

| | |
|---|---|
| 10 | 同一サーバ上で複数の利用者が情報処理を実行しているため、別の利用者情報を盗み見し、別の利用者に成りすまして処理を行う可能性がある。 |
| 11 | サーバ資源の利用者ごとの分割が不適切なことによる情報漏えいが発生する可能性がある。 |
| 12 | 情報の置き場所が特定の場所に固定されず、海外の法執行機関等による予期せぬアクセスが行われうることがある。 |
| 13 | サービスを有期契約した場合、契約終了後の情報の取り扱い（確実な消去）が不明瞭な場合がある。 |
| 14 | サービス提供事業者の経営が破たんしたり突然のサービス停止に陥った場合、預けた情報の行方は保証されず、損害賠償も支払われない場合がある。 |
| 15 | サービス提供事業者の従業員が不正を行う可能性がある。 |
| 16 | 約款の内容はサービス提供者側の都合で利用開始後一方的に変更される可能性がある。 |
| 17 | 準拠法に外国法を指定される場合がある。 |
| 18 | 管轄裁判所に海外の裁判所を指定される場合がある。 |

# 約款による情報処理サービスの利用における利用時のチェックリスト－１

- 可用性に関するチェック項目

| | |
|---|---|
| 1 | サービス時間について約款上の記載があり、その記載内容は利用上問題ありませんか？ |
| 2 | サポート時間について約款上の記載があり、その記載内容は利用上問題ありませんか？ |
| 3 | 計画停止予定通知の有無について約款上の記載があり、その記載内容は利用上問題ありませんか？ |
| 4 | サービス稼働率について約款上の記載があり、その記載内容は利用上問題ありませんか？ |
| 5 | 利用者側でデータバックアップできるかどうかについて約款上の記載があり、その記載内容は利用上問題ありませんか？ |
| 6 | 災害などによるシステム障害からの情報システム復旧の有無について約款上の記載があり、その記載内容は利用上問題ありませんか？ |
| 7 | サービス提供事業者が経営破たんした場合、情報の行方が保証されない可能性があることは利用上問題ありませんか？ |

# 約款による情報処理サービスの利用における利用時のチェックリスト－２

- 機密性及び完全性に関するチェック項目

| | |
|---|---|
| 8 | 同一サーバ上で複数の利用者が実行するサービスであることは利用上問題ありませんか？ |
| 9 | セキュリティ意識の低い他の利用者の影響（成りすましでの情報の盗み見等）を受ける可能性があることは利用上問題ありませんか？ |
| 10 | 情報が海外で保管される場合には、万一、海外の法執行機関等による予期せぬアクセスが行われた際に問題ありませんか？ |
| 11 | サービス終了後、情報がどのように消去されるかについて確認した結果は利用上問題ありませんか？ |
| 12 | サービス提供事業者の従業員が不正を行う可能性があることは利用上問題ありませんか？ |

  - サービスを利用する上でリスクを許容できるものであるかという意味を含む

# 外部委託の想定について

| サービス | 注意事項 |
| --- | --- |
| 全学・部局単位での電子メール | ・ベンダーロックイン<br>・（海外に保存される場合）国内法の適用が困難 |
| 研究室・個人単位での電子メール | ・（海外に保存される場合）国内法の適用が困難<br>・転送先を大学でコントロールできない |
| 個人単位でのSNS | ・公開範囲を大学でコントロールできない |
| 全学でのホスティング・プライベートクラウド | ・運用コストが必ずしも割安にならないことも |
| 全学でのパブリッククラウド | ・削除したデータの完全消去が困難<br>・（海外に保存される場合）国内法の適用が困難 |
| 事務システムでのSaaS利用等 | ・機密情報のデータの保護に制約<br>（暗号化したままでのデータ処理は不可能なため）<br>・削除したデータの完全消去が困難 |

# サンプル規程集でのクラウド対応

- 新たな規則制定は不要
- 現状の対策（規則体系）の検証は必要
  - 本学情報システム
  - 約款による情報処理サービス
- 外部委託の形態の一つとして対応
  - 約款による情報処理サービス（この項を追加）
- 情報の提供方法に応じた対応
  - 外部委託（契約と約款）
  - 第三者提供
  - その他

# ありがとうございました

ご意見、ご要望をお知らせください

sp-comment@nii.ac.jp