大学におけるセキュリティポリシーのクラウド対応について

情報セキュリティポリシー推進部会

作成日：2011年11月7日

クラウドサービスの導入とセキュリティポリシー

統一基準におけるクラウド対応

解説の追加

- 管理
  - 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
  - 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

大学でクラウドを導入すると

- 学外に情報システムがある状態になると・・・
  - コスト（開発、運用、保守）の削減
  - 省エネ
  - 停電（法定点検）からの解放
  - 信頼性
  - セキュリティ
- クラウドを導入する場合にセキュリティポリシーのどの規則・条文を改定すればよいのか、どの規則・条文に注意すればよいのか

クラウドサービスって？

- 雲を掴むような話ですが
  - SaaSやPaaS、IaaS

  ネットワークの向こうにあるシステムを利用するサービス
- 使い方の例
  - サーバ貸し
  - メール
  - ストレージ
  - データセンター
  - 翻訳サイト

学外に出してもよい情報だめな情報

- 情報の提供形態に応じた対応が必要
  - 外部委託、第三者提供、その中間等

  →部会として現在検討中
- 外部委託の場合でも
  - 学外に持ち出してもよい情報とその処理

    →クラウドの導入の検討対象
  - 学外に持ち出してはいけない情報とその処理

    →クラウドの導入の検討対象外
- 大学のセキュリティポリシーに基づいた取扱い

学外へ情報を出す形態

- 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）
- 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

サンプル規程集におけるクラウド対応の検証（対応するサンプル規程集）

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 http://www.nii.ac.jp/csi/sp/

- 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）

大学等が外部クラウドサービス利用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

- 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

外部委託の調達時の手続き

- 調達仕様で委託先に求める情報セキュリティ対策等
  - システム運用・保守・点検（委託業務）についてはそれぞれ対策等が必要かどうかを定める
    - オンサイト
    - リモート
    - データセンター
    - ASP
    - ハウジングの形態
  - システム構築・開発、情報の加工・処理、保存・運搬についてもそれぞれ対策等が必要かどうかを定める

外部委託における情報セキュリティ対策実施手順

- 調達システム運用・保守・点検（委託業務）についてはそれぞれ対策等が必要かどうかを定める
  - 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
- 契約
  - 情報セキュリティ対策の履行状況の確認
  - 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

策定手引書 外部委託に係る契約

- 『約款による情報処理サービス』利用時特有の留意事項

約款が用意されており、情報セキュリティに関する事項について利用者による条件選択の余地が限られている情報処理サービスを利用し、外部委託を行う場合である。

（以下略）

→いわゆるパブリック・クラウドのうち約款によって利用条件が決まっているものを「約款による情報処理サービス」と定義

策定手引書 外部委託に係る契約

- 一般に、外部事業者が提供する「約款による情報処理サービス」を利用する場合には、サービス内容の保証は提供事業者が定める利用規約等の約款の範囲に限られる。したがって、対策基準及び規定で許容されているかどうかを確認のうえ利用を検討することが必要。

「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－1

- 情報処理サービスにより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がある。（通常の情報処理サービスで生じる権利については利用者への帰属が一般的）
- 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ことがある。（賃貸借・使用貸借部分の所有権はサービス提供者等の事業者側に帰属するため、通常の情報処理サービスの利用終了時におけるデータ削除は、原状回復義務として利用者側の義務となることが想定）

「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−2

- 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ことがある。

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

- 無償で利用する場合でも外部委託に該当するサービスもあるとの認識が必要

無償で利用する例

- 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
- ストレージサービスの利用

- 学外の情報処理サービスを 利用する場合には、無償で利用を開始できる場合であっても、本手引書で解説している「外部委託における情報セキュ リティ対策実施規程」を遵守することが必要

留意事項について広く周知させること

- 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
- ストレージサービスの利用

- このような無償で利用を開始できる情報処理サービスの利用においては、そ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雛形付録に基づき 学内に広く周知する必要がある

外部委託における情報セキュリティ対策実施規程雛形付録

- 「約款による情報処理サービス」
  18項目のサービス利用時の留意事項
- 利用時チェックリスト
  - 可用性に関するチェック項目→7つ
  - 機密性および完全性に関するチェック項目→5つ
  - 約款上に記載が明記されていない場合には、サービス提供者にサービス内容を確認
  - 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もの

サンプル規程集でのクラウド対応予定

- 現状の対策（規則体系）の検証は必要
- 新たな規則制定は不要
- 外部委託における情報セキュリティ対策実施手順において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）
- 情報の提供の形態に応じた対応
  - 外部委託、第三者提供、その中間
- 部会として現在検討中

ご清聴ありがとうございました

ご意見やご質問、事例等をお寄せください。
サンプル規程集に反映させていただきます。

sp-comment@nii.ac.jp