# アンケート調査(コンテンツ分野・ICTサービス)結果の概要

- 調査対象サービス：メール, ストレージサービス，SNS, グループウェア, 各種ホスティング
- 回答機関、システム数：546機関、733システム（2013年11月29日時点）
- 回答内容等の分析
  - 各サービスで利用しているリソース（平均）：サーバ145.7台、CPU43.7コア、メモリ142.8GB、データ総量5.7TB
  - 1割強のシステムでデータのバックアップをしていない
  - ソフトウエアに、54%がベンダーの商用パッケージを利用している
  - 93%以上がBCP対策の必要性を感じているが、77%以上が着手できていない
  - 134システム（約18%）113機関（約21%）がプライベートクラウドを利用している
  - パブリッククラウドの利用については80システム（約11.6%）と少ない／今後の利用についても25%が消極的で、**個人情報を含むなどセキュリティに関する課題，メリットが不明，予算の問題が要因**となっている
  - システムの運用に平均2.2人年の稼働をかけている／68%以上のシステムが教職員のみで運用を行っている，



# コンテンツ分野から見た アカデミッククラウドの在るべき姿

- 課題
  - 既存コンテンツサービスからアカデミッククラウドサービスへの移行の方策
  - システムとデータの共有・共通化の方策，独自機能を有する場合がある
  - 他サービスと連携している場合の対策
- 要求要件
  - ユーザのアカウントが一元管理されており，教職員の所属移動等においても設定変更が容易であること，他のサービスとの統合認証であること
  - オンプレミスと同等以上のサービス品質を確保すること
    - 応答速度，セキュリティ対策，プライバシ保護
  - 各種コンテンツサービスに対応すること
  - 時間・場所に制限されることなくコンテンツサービスを利用できること
  - メールサービスでは，標準的に利用可能なIMAPサービス等が利用できること，また，安否確認等に利用できること
  - SNSサービスでは，チャットの機能があり，コミュニティ形成可能であること
  - ストレージサービスでは，データの移動が容易に行えること

# コンテンツ分野から見たロードマップ

■ １年～３年目（初期目標）
- コミュニティで共同利用できるクラウド基盤の構築（数か所、小規模）
- NII等既存のクラウドサービスの拡大と連携
- IaaSサービスの提供
- 情報共有のトライアル実施
- BCP, DR対策としてデータ保管のトライアル実施

■ 4年～7年目（中期目標）
- クラウド基盤の規模拡大
- 商用パッケージを組み込んだPaaSサービスのトライアル実施
- 商用クラウドとの相互運用のトライアルとBCP, DR対策のトライアル

■ 8年目～　（長期目標）
- SaaSサービスのトライアル
- システム集約、統合の対象拡大と商用サービス活用の推進
- データ収集対象の拡大と新たなサービスの開発・構築・トライアル



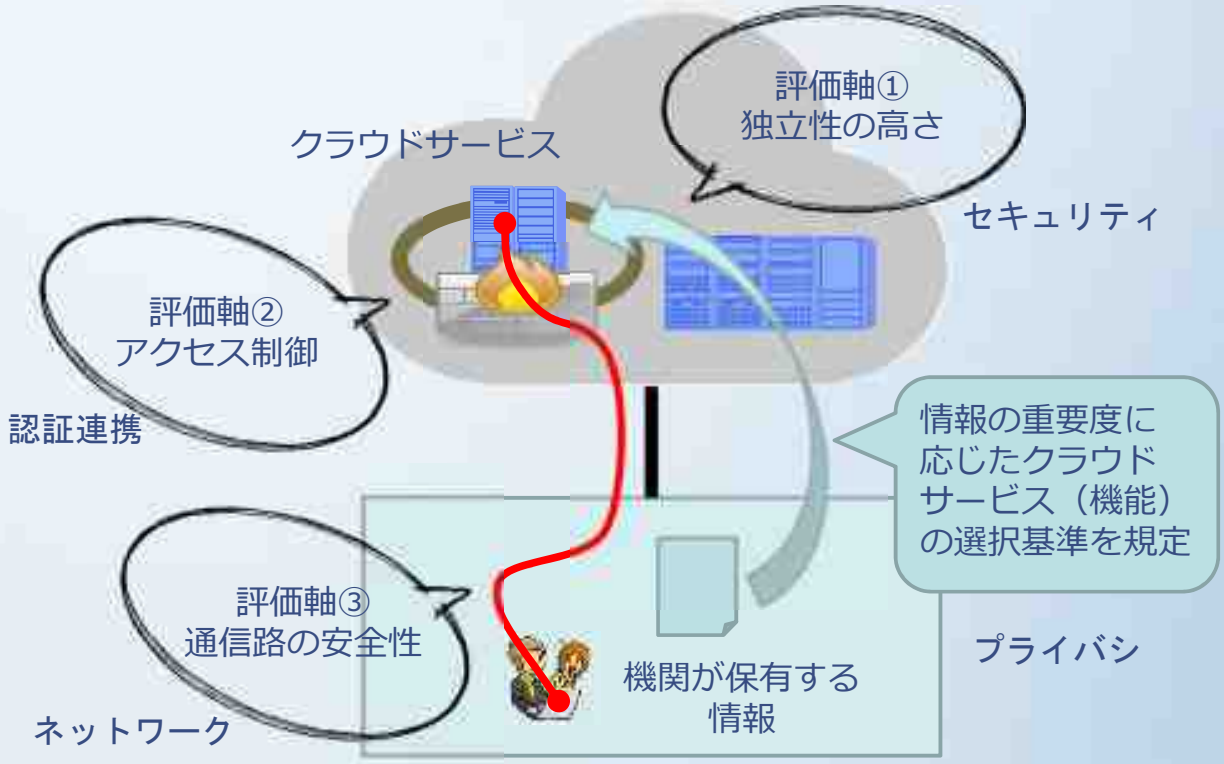
# コンテンツ分野のまとめ

- コンテンツに係るシステムでのパブリッククラウド活用は、個人情報を含むなどセキュリティの問題をはじめ，メリットが不明など様々な課題があり、あまり進んでいない状況である
- アカデミッククラウドの構築により、クラウド化やシステム集約の効果が期待できるとともに、業務アプリケーションの共同開発や共同利用の推進などの新たな効果も期待できるがメリットを理解してもらう必要がある
- BCP対策は必要性は感じているものの殆ど進んでいない状況であり、アカデミッククラウド構築によりトップダウンで対策を加速すべきである
- アカデミッククラウドによりクラウド化を推進し、加えてSLAやクラウド基盤の標準化を行うことによって、将来的にパブリッククラウドの活用につなげることができる

# サービス毎の情報格付けとガイドライン(セキュリティ，認証連携，ネットワーク，プライバシ)

Academic Cloud

## クラウドサービスの利用シーンと評価軸



# アンケート調査(セキュリティ)結果の概要

- 63.5%の機関において、情報システムの運用に関する諸規則（セキュリティポリシー等）を定めている
  - ほとんどの機関において、「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」と起を一とする諸規則を参考に規定
- 情報システムの運用に関する諸規則を定めている機関のうち、
  - 44.8%（全体の28.5%）の機関において、情報の格付けに関する事項を規定
  - 34.7%（全体の22.1%）の機関において、外部委託する場合に関する事項を規定
- 31.0%の機関において、諸規則を構成員に周知するための教育が行われている
  - 頻度は、入学・着任時と、年数回実施される講習会（eラーニングを含む）の受講
- 7.2%の機関（検討中を含む）がISMS認証取得に関心がある
- 29.1%の機関で過去1年間にセキュリティインシデントが発生している
  - 大部分が軽微なインシデントであり、68.2%は10件未満
- 48.1%の機関において、クラウドサービスを利用中、または利用を検討している
  - 利用中の機関は、1.コスト、2.利便性、3.セキュリティを重視して判断
  - 利用しない機関は、1.セキュリティ、2.コスト、3.利便性を問題視
- 48.3%の機関において、構成員のクラウドサービスの利用状況を把握している
  - 24.7%（全体の12.0%）の機関において、構成員は情報の重要度を考慮せず利用していると認識
- 62.5%の機関において、アカデミッククラウドを利用、または利用の意向がある
  - ただし、30.5%の機関は情報不足により判断できない、2.2%の機関は利用しないと回答

# 課題の洗い出しと解決策の検討

- アンケート結果から
  - 6割強の機関は情報システムの運用に関する諸規則（セキュリティポリシー等）を定めており、そのうち7割弱は「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」と起を一とする諸規則を参考にしている
  - 一方、情報の格付けや外部委託する場合に関する諸規則の整備は、3割弱の機関に留まっている
  - 3割強の機関が過去1年間にセキュリティインシデントを経験している
  - クラウドサービスの利用に対してコストの低減や利便性の向上に期待はあるが、外部委託する際のセキュリティに対して漠然とした不安を持っている

→ **情報の格付け**と**格付けに応じたクラウドサービスの選択基準**が必要

- 本事業においてセキュリティ分野が果たす役割
  - 各分野で扱われる情報の分類・格付けの基準となる考え方（重要度）を示す
  - サービスモデルおよびサービスレベルに基づいた、クラウドサービスの信頼度を定義する
  - 機関が保有する情報の重要度とクラウドの信頼度を対応づける

# 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/

- B2104 情報格付け基準
  - 機密性3段階、完全性2段階、可用性2段階



# B2104 情報格付け基準

| 格付けの区分 | 分類の基準 |
|---|---|
| 機密性３情報 | 本学で取り扱う情報のうち、秘密文書に相当する機密性を要する情報 |
| 機密性２情報 | 本学で取り扱う情報のうち、秘密情報に相当する機密性は要しないが、その漏えいにより利用者の権利が侵害され又は本学活動の遂行に支障を及ぼすおそれがある情報 |
| 機密性１情報 | 機密性２情報又は機密性３情報以外の情報 |

| 格付けの区分 | 分類の基準 |
|---|---|
| 完全性２情報 | 本学で取り扱う情報（書面を除く。）のうち、改ざん、誤びゅう又は破損により、利用者の権利が侵害され又は本学活動の適確な遂行に支障（軽微なものを除く。）を及ぼす恐れがある情報 |
| 完全性１情報 | 完全性２情報以外の情報（書面を除く。） |

| 格付けの区分 | 分類の基準 |
|---|---|
| 可用性２情報 | 本学で取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、利用者の権利が侵害され又は本学活動の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報 |
| 可用性１情報 | 可用性２情報以外の情報（書面を除く。） |

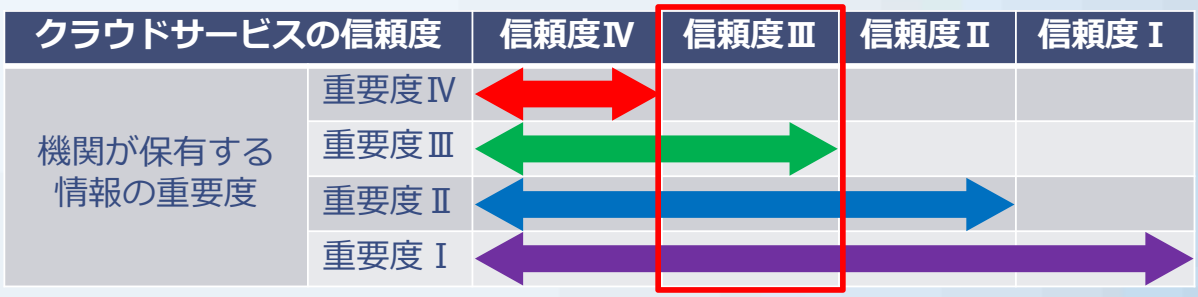
# 機関が保有する情報の重要度

| 区分 | 情報格付け基準との対応 | 区分の説明 | 情報の種類 |
|---|---|---|---|
| 重要度Ⅳ | 3-2-2<br>3-2-1 | 情報が流出（漏えい）、紛失、改ざん等した場合、機関の業務に深刻かつ重大な影響を及ぼすもの | 特定の関係者以外に対し厳重に機密を保持すべきもの |
| 重要度Ⅲ | 3-1-2<br>3-1-1<br>2-2-2<br>2-2-1 | 情報が流出（漏えい）、紛失、改ざん等した場合、機関の業務に重大な影響を及ぼすもの | 特定の職制、グループ又は部局等以外に対して機密を保持すべきもの |
| 重要度Ⅱ | 2-1-2<br>2-1-1<br>1-2-2<br>1-2-1 | 情報が流出（漏えい）、紛失、改ざん等した場合、機関の業務に軽微な影響を及ぼすもの | 公開を前提としていないもの（機関内限定） |
| 重要度Ⅰ | 1-1-2<br>1-1-1 | 情報が流出（漏えい）、紛失、改ざん等した場合、機関の業務にほとんど影響を及ぼさないもの | 積極的な公開を前提としたもの |

- 機密性、完全性、可用性の組み合わせ（例：3-2-2）を重要度4段階として再定義（現実的なレベルに簡素化）



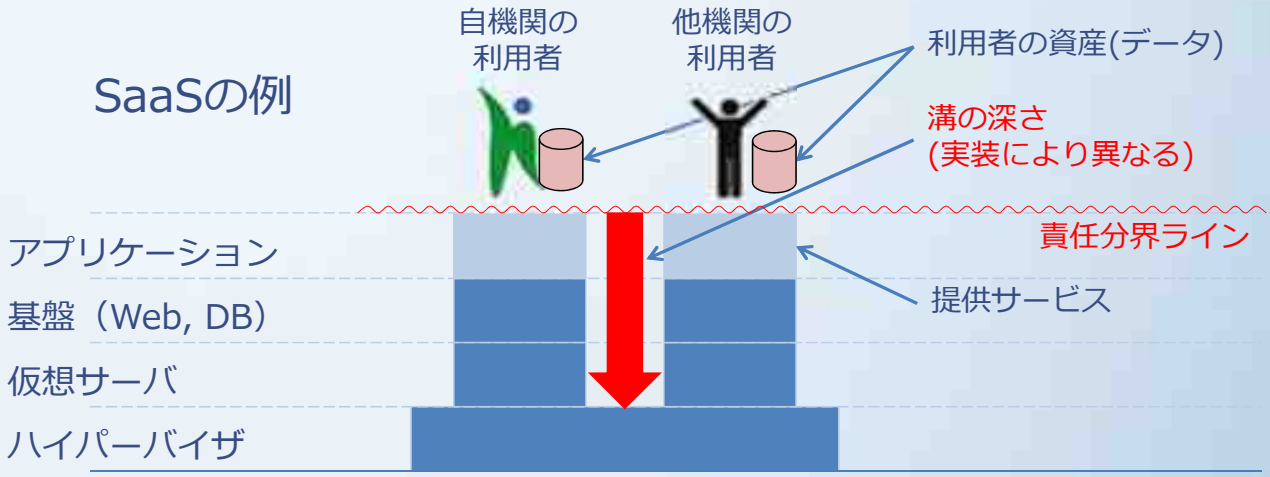
# クラウドサービスの信頼度




- 信頼度の評価軸
  - ① 独立性の高さ（他の利用者との隔離）
  - ② アクセス制御（データアクセスのための利用者認証）
  - ③ 通信路の安全性（暗号化やアクセス区域の制限）
- 機関が保有する情報の重要度との関連付け
  - 例）信頼度Ⅲのクラウドサービスには、機関が保有する重要度Ⅲ以下の情報を保存できる

# 独立性の高さ

SaaSの例

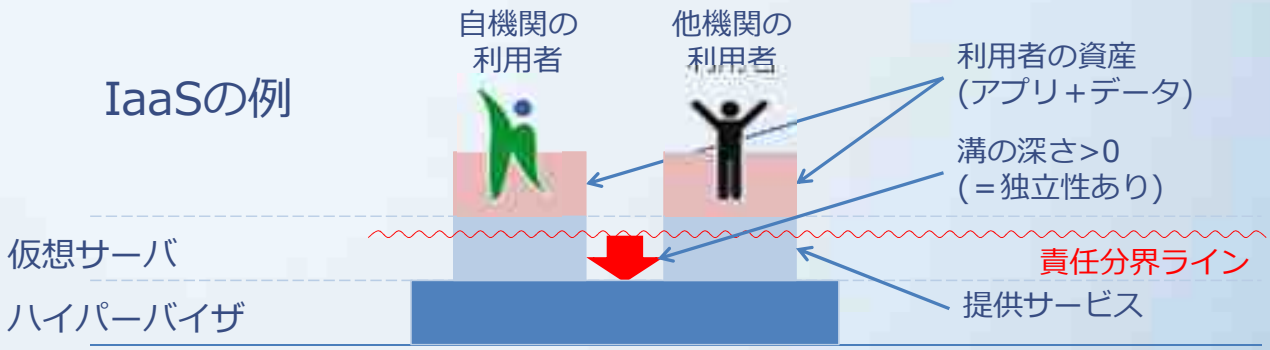



- クラウド事業者提供の情報（サービス仕様書やヒヤリング）から判断
  - サービスモデル（＝責任分界ライン）
  - 実装方法（＝溝の深さ）
- 「責任分界ラインより溝が深い」 → 独立性がある

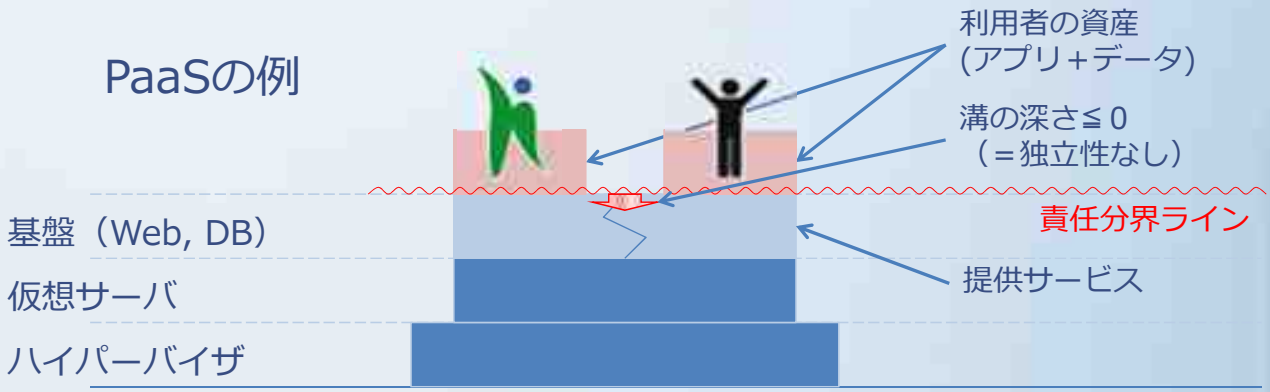


# 独立性の高さ（続き）

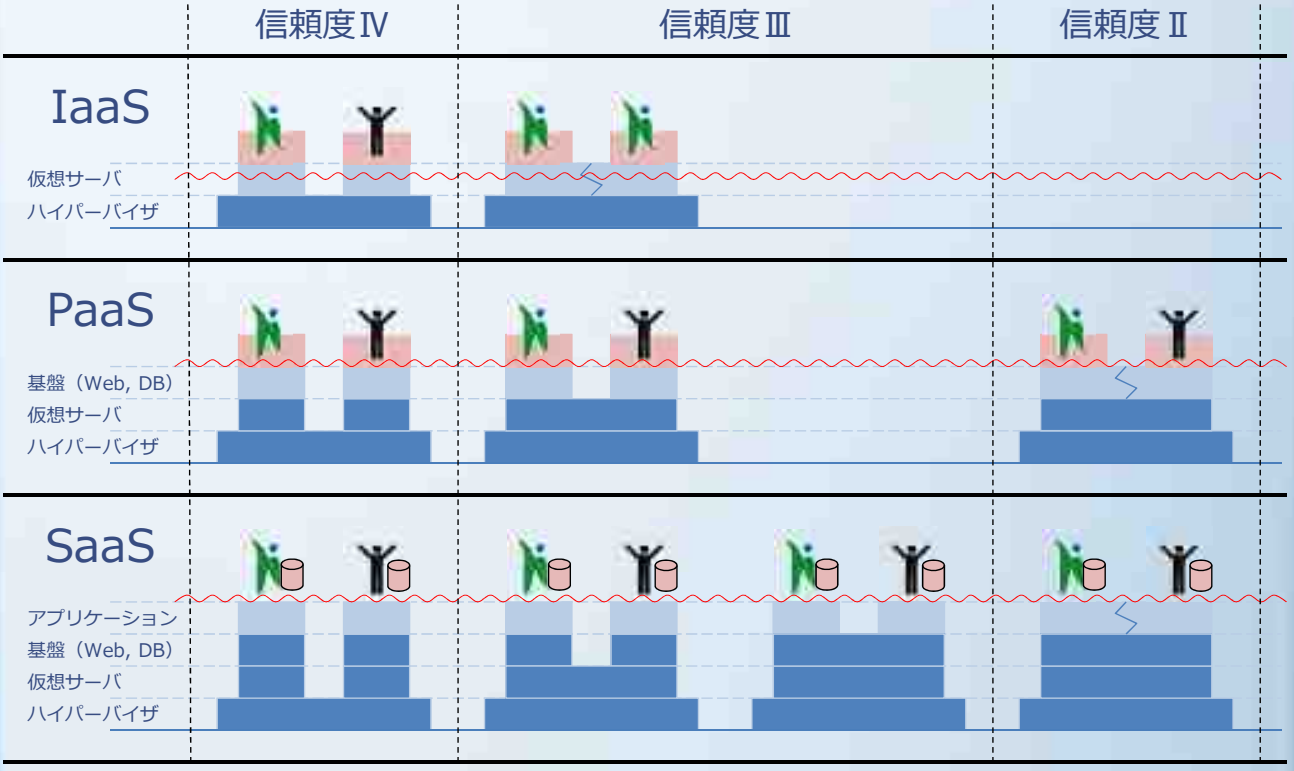
IaaSの例




PaaSの例



# サービス（実装方法）と信頼度の対応

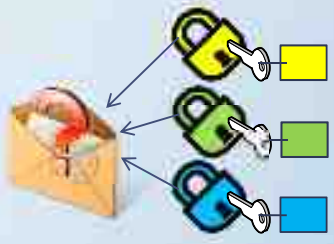





# アクセス制御と通信路の安全性

- アクセス制御
  - 重要度Ⅱ以上の情報はF/W等で保護された領域に保存
  - 重要度Ⅱ以上の情報へのアクセスには利用者認証が必要
    - 個々の情報の重要度に応じて適切な認証強度を選択

  → **認証連携分野**による格付け



- 通信路の安全性
  - 重要度Ⅱ以上の情報は保護された通信路を使用して保存
  - 重要度Ⅱ以上の情報へのアクセスには保護された通信路が必要
    - 接続先の認証強度に応じて適切なアクセス環境を選択

  → **ネットワーク分野**による格付け

# クラウドサービスの利用に関するガイドライン

- NIST: National Institute of Standards and Technology
  （米国国立標準技術研究所）
  - Cloud Computing Synopsis and Recommendations (SP-800-146)
    （クラウドコンピューティングの概要と推奨事項）
- ENISA: European Network and Information Security Agency
  （欧州ネットワーク情報セキュリティ庁）
  - Cloud Computing: Information Assurance Framework
    （クラウドコンピューティング：情報セキュリティ確保のためのフレームワーク）
  - Cloud Computing: Benefits, risks and recommendations for information security
    （クラウドコンピューティング：情報セキュリティに関わる利点・リスクおよび推奨事項）
- 経済産業省
  - クラウドサービス利用のための情報セキュリティマネジメントガイドライン
- 独立行政法人 情報処理推進機構
  - 中小企業のためのクラウドサービス安全利用の手引き
  - クラウド事業者による情報開示の参照ガイド



# 高等教育機関のための クラウドサービス利用ガイドライン・チェックリスト

- 広島大学クラウドサービス利用ガイドライン・チェックリスト
  http://www.media.hiroshima-u.ac.jp/news/cloudguide/
  - 第一版（2013年（平成25年）3月15日策定）
  - 45項目のチェックリスト
  - クラウドサービスの選択基準および契約前に確認すべき点をリストアップ
- ガイドライン・チェックリストの構成（予定）
  - 利用のための準備
    - クラウドサービス利用基準
    - 利用組織の体制（責任者、担当者）
  - 利用範囲の明確化
    - サービスの質(SLA)
    - 機能とコスト
    - サポート体制
    - 業務の継続性
  - 事業者の選定
    - 物理的セキュリティ
    - サービスの継続性
    - 情報セキュリティインシデントの管理
  - 契約条件の確認
    - データの所有権と返却・消去
    - 責任範囲の明確化
    - 準拠法と管轄裁判所

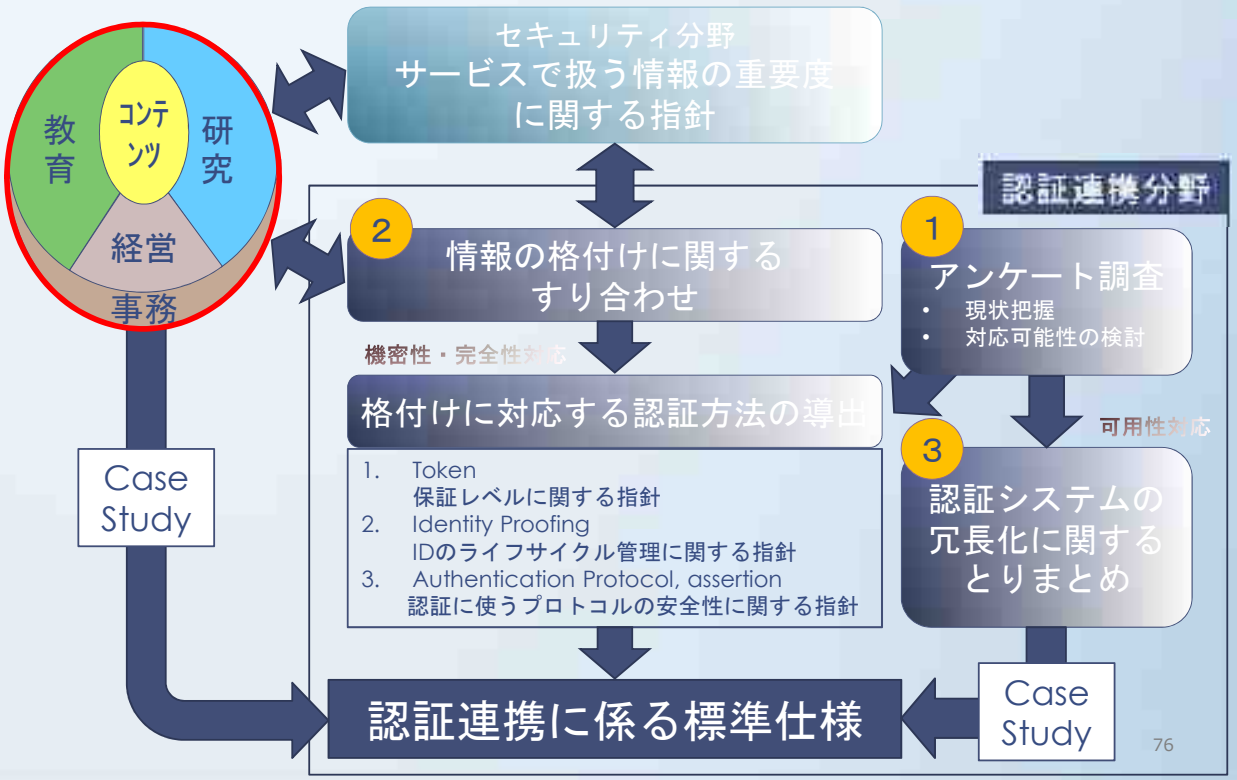
# アンケート調査（認証連携）結果の概要

- 統合認証環境の整備
  - 国立大学（80%近く）を中心（その他は50%程度）に整備が進んでいる。
- 認証連携SSO環境の整備
  - 研究機関（60%以上）と国立大学（60%以上）で整備が進んでいる。
  - 公立，私立大学，高専，短大についても多くの機関で検討が進められている。
- 認証情報の冗長化
  - 80%程度の機関で冗長化を実現済み。
  - 複数拠点における冗長化については，あまり進んでいない。
- 認証システムの冗長化
  - 40%程度の機関で冗長化を実現済み。
  - 複数拠点における冗長化については，あまり進んでいない。

**統合認証や認証連携の環境構築は比較的進んでいる**
**認証情報やシステムの冗長化についてはこれから**



# 認証連携に係る標準仕様の導出手順



# 認証保証レベル(LoA)に関する基本的概念

## 一般的なLoAの評価項目は以下の5つ

1. アイデンティティのライフサイクル管理
2. 認証トークンの採用

ACではこの2項目に対応した「認証強度レベル」を検討

3. 認証方式の採用（特にリモート）
4. 認証に用いるアサーションの性質
5. 情報システムセキュリティとしての認証システムのセキュリティ

- 1～4はNIST 800-63等の要求要件に対応
- 5は具体的なLoA認定プログラムにおいて運用の成熟度（ガバナンスの一部）の評価軸に対応



# アイデンティティのライフサイクル管理

| 認証強度レベル | 評価項目 |
|---|---|
| レベル1 | 利用資格を定めていること。 |
| レベル2 | 上記に加え、利用資格が何らかの形で保証されていること。大学で言えば、人事のDBや学務のDBと（資格喪失確認も含めて）連動して資格確認が行われること。また、それ以外の人間に対しては、適切なコントロールがなされていること。 |
| レベル≧3 | 上記に加え、その検証がなされていること。特に資格の取得時に、下の学校の卒業証明、住民票その他の記録を用いて検証可能になっていること。 |

# 認証トークンの採用

| 認証強度レベル | 評価項目 |
|---|---|
| レベル1 | パスワードで管理し、発行されたパスワードを安全な形で利用者に届けること。 |
| レベル2 | 上記に加え、パスワードポリシー等により、十分複雑なパスワードが使用されていることを保証すること。 |
| レベル3 | ワンタイムパスワードのハードトークン、または公開鍵か証明書による認証方式を採用すること。後者の場合、HD等に格納してもよいが、パスワード等を設定して二要素認証を実現すること。 |
| レベル4 | 証明書による認証方式を採用すること。ハード的に保護されたデバイスに格納すること。 |

トークンの管理方式に関する要求
- レベル1、2：利用者によるパスワード変更が可能であること
- レベル≧3　：＋CRLによる、トークンの状態の管理をすること



# 各分野における情報システム

| ICT | 教育 | 事務 | コンテンツ | 大学経営 |
|---|---|---|---|---|
| 電子メール | LMS/CMS | 人事給与 | 図書館システム | その他事務システム（具体的な対象は?） |
| ストレージサービス（ファイル共有など） | eポートフォリオ | 財務会計 | 機関リポジトリ | 大学評価情報システム |
| SNS | 履修登録(シラバス) | 学務情報 | その他リポジトリ | IRデータベース（データウェアハウス） |
| グループウエア | 遠隔講義システム | 就職支援 | OPAC | 研究者総覧データベース |
| 学生共通ポータル | CALLシステム（語学学習システム） | 出退勤 | その他検索システム | |
| 認証局＆登録局 | | 出張旅費申請システム | Webページ | |
| 認証データベース＆認証システム | | 目標管理・職員人事等評価システム | Webページ（CMS） | |
| 遠隔会議システム | | 電子職員録 | データベース | |
| 学内クラウド(IaaS) | | 施設予約 | 動画配信 | |
| 学内クラウド(PaaS) | | ペーパーレス会議システム | 教育システム | |
| ICカード発行システム | | ソフトウェアライセンス管理 | オープンコースウェア | |
| | | 電子掲示板 | セキュリティe-Learnming | |
| | | 安否確認 | | |

# ICTサービス

| サービス | 重要度 | 備考 | 認証強度 |
|---|---|---|---|
| 電子メール | Ⅱ～Ⅳ | 公開を前提としていないため，漏えい等による影響は，Ⅱ以上．どの重要度かはメールの内容による．(※機密性の高いメールはS/MIME利用などが必要) | 一般:レベル＝2 |
| ストレージサービス<br>(ファイル共有など) | Ⅱ～Ⅳ | 公開を前提としていないため，漏えい等による影響は，Ⅱ以上．どの重要度かはストレージ格納データの内容による．(※機密性1と2以上は論理的に分ける必要あり) | 一般:レベル＝2<br>管理:レベル≧2 |
| SNS | ⅠかⅡ | データが公開される場合もある．サービスの特徴から機密を保持すべきデータが置かれることはないと考えられる。公開を前提としていない利用の場合には，Ⅱに該当する。 | 一般:レベル≧1 |
| グループウエア | Ⅱ～Ⅳ | 公開を前提としていないため，漏えい等による影響は，Ⅱ以上．どの重要度かは置かれたデータの内容による。厳重に機密を保持すべき内容のデータが置かれることはないと考えられるが，ないとも言えない．<br>(※機密性2以上の情報はアクセス制限が必要な場合有) | 一般:レベル＝2<br>管理:レベル≧2 |
| 学生共通ポータル | Ⅲ～Ⅳ | 学生にとって重要なサービスを集約したサイト，入り口でしかなく機密性の高い情報は無いが，停止した場合の影響は非常に大きい． | 一般:レベル＝2 |
| 認証局＆登録局 | Ⅳ | 認証強度を高めるために，電子証明書を登録，発行，失効情報を格納しているシステム． | 管理:レベル≧3 |
| 認証データベース＆<br>認証システム | Ⅳ | 全学の認証に必要なデータを保持しているデータベースとそれらの関連システム．極めて重要． | 管理:レベル≧3 |
| 遠隔会議システム | Ⅱ～Ⅳ | Polycom等学外との多地点遠隔会議で利用するシステム．会議内容の重要度に依存する？重要な会議では使用しない等のルールが必要 | 一般:レベル＝2 |
| 学内クラウド(IaaS) | Ⅱ～Ⅳ | 部局や研究室にVMリソースを貸し出しているシステムで，その重要度はサービスに依存する．公開を前提としないデータがあるのでⅡも含まれる | 一般:レベル＝2<br>管理:レベル≧2 |
| 学内クラウド(PaaS) | Ⅰ～Ⅳ | 部局や研究室にホスティングしているサービスで，その重要度は提供者側の意識にも依存する．サービスとデータ内容に依存し様々な場合が考えられる。 | 一般:レベル＝2<br>管理:レベル≧2 |
| ICカード発行システム | Ⅲ～Ⅳ | 基本は学内限定情報，顔写真も含む。入退出に利用されるので重要度は非常に高い。 | 管理:レベル≧2 |



# 教育

| サービス | 重要度 | 備考 | 認証強度 |
|---|---|---|---|
| LMS/CMS | Ⅱ | 講義および自学自習の支援システムであり，講義内容および履修プロセスで，機密性は低い． | 学生:レベル＝2<br>教員:レベル＝2 |
| eポートフォリオ | Ⅲ | 履修プロセスを集約しているため，個人情報に準じた情報が含まれる． | 学生:レベル＝2<br>教員:レベル≧2 |
| 履修登録(シラバス) | Ⅰ，Ⅲ | 教育情報の公表にて公開を要求されているシラバスはⅠ．学務情報システムに登録する履修情報や成績情報は，学生への影響が大きい． | 学生:レベル＝2<br>教員:レベル≧2<br>管理:レベル≧3 |
| 遠隔講義システム | Ⅱ | 機密性の高い情報は扱わない．サービスの停止や中断は一過性であるが，教員と学生に迷惑をかける． | 教員:レベル＝2<br>管理:レベル≧2 |
| CALLシステム<br>(語学学習システム) | Ⅱ | 機密性の高い情報は扱わない．サービスの停止や中断は一過性であるが，教員と学生に迷惑をかける． | 学生:レベル＝2<br>教員:レベル≧2 |

# 事務

| サービス | 重要度 | 備考 | 認証強度 |
|---|---|---|---|
| 人事給与 | Ⅳ | 教職員の基本データを保有しているため，個人情報の漏えいは影響が大きいとともに，認証等の基本データとなるため改ざんの影響は非常に大きい．(※部局総務担当による入力および本部人事担当など管理者が登録・編集・削除を実施) | 管理:レベル≧3 |
| 財務会計 | Ⅳ | 個人情報として寄付，委託研究，共同研究に関わる情報を含むとともに，会計情報の改ざんは業務に深刻な影響を及ぼす(※一般教職員利用と部局・財務部の管理者が登録・編集・削除を実施) | 教員:レベル≧2<br>管理:レベル≧3 |
| 学務情報 | Ⅳ | 成績情報等の守秘性の非常に高い個人情報を保有している<br>(※正規生・非正規生など全ての学生情報を格納．部局教務担当・学務部の管理者が登録・編集・削除を実施) | 管理:レベル≧3 |
| 就職支援 | Ⅲ～Ⅳ | 企業の採用情報を掲載したものから、エントリーシート作成支援等を行うものまで、提供機能によって異なる | 検討中 |
| 出退勤 | Ⅲ | 勤務情報の改ざんは業務に影響が大きいとともに、休暇等の申請に守秘性の高い個人情報を含む | 教員:レベル＝2 |
| 出張旅費申請<br>システム | Ⅲ | 業務のIT化の一環，情報漏えいやシステムダウンは，入力した教職員に迷惑をかける． | 教員:レベル＝2<br>管理:レベル≧2 |
| 目標管理・職員人事<br>等評価システム | Ⅲ | 職員個人を対象とした人事評価に係るシステム． | 教員:レベル≧2<br>管理:レベル≧3 |
| 電子職員録 | Ⅱ | 機密性2の学内限定情報の検索システム． | 一般:レベル＝2 |
| 施設予約 | Ⅱ | 学内施設に対する予約システム | 教員:レベル＝2 |
| ペーパーレス会議<br>システム | Ⅲ | 部局長会議，教授会など重要会議での利用が定着しつつあり，重要情報も扱うため，重要度はⅢ． | 教員:レベル≧2<br>管理:レベル≧2 |
| ソフトウェア<br>ライセンス管理 | Ⅱ | ライセンスの不正利用を抑制するための，PC内ソフトウェアを自動サーチするシステム． | 教員:レベル＝2<br>管理:レベル≧2 |
| 電子掲示板 | Ⅱ | 機密性2の学内限定情報を提供するシステム | 教員:レベル＝2<br>管理:レベル＝2 |
| 安否確認 | Ⅲ | 学内構成員の携帯番号や携帯メールアドレスを登録させる場合，個人情報に相当するので漏えいした場合，重大な影響あり． | 一般:レベル＝2<br>管理:レベル≧2 |



# コンテンツ

| サービス | 重要度 | 備考 | 認証強度 |
|---|---|---|---|
| 図書館システム | Ⅰ～Ⅱ | 公開を前提としていないデータを含むが，漏えい・改ざん等による影響は大きくはない。 | 一般:レベル＝1<br>管理:レベル＝2 |
| 機関リポジトリ | Ⅰ | データは公開を前提としているため，漏えい・改ざん等による影響は小さい。 | 一般:レベル＝1<br>管理:レベル＝2 |
| その他リポジトリ | Ⅰ | データは公開を前提としているため，漏えい・改ざん等による影響は小さい。 | 一般:レベル＝1<br>レベル＝2 |
| OPAC | Ⅰ | 蔵書検索のためのシステムで，公開利用を前提としているため，漏えい・改ざん等による影響は小さい。 | 一般:レベル＝1<br>管理:レベル＝2 |
| その他検索システム | Ⅰ | 検索のためのシステムで，公開利用を前提としているため，漏えい・改ざん等による影響は小さい。 | 一般:レベル＝1<br>管理:レベル＝2 |
| Webページ | Ⅰ～Ⅱ | 公開を前提としているため，漏えい・改ざん等による影響は小さい。<br>CMS脆弱性による改ざんなど情報セキュリティインシデントの観点からはⅡ | 一般:レベル＝1<br>管理:レベル≧2 |
| Webページ(CMS) | Ⅰ～Ⅱ | 公開を前提としているため，漏えい・改ざん等による影響は小さい。<br>CMS脆弱性による改ざんなど情報セキュリティインシデントの観点からはⅡ | 一般:レベル＝1<br>管理:レベル≧2 |
| データベース | Ⅰ～Ⅱ | 公開を前提としているため，漏えい・改ざん等による影響は小さい。改ざんにより，データの信頼性が損なわれることがある。<br>CMS脆弱性による改ざんなど情報セキュリティインシデントの観点からはⅡ | 一般:レベル＝1<br>管理:レベル≧2 |
| 動画配信 | Ⅰ | 公開を前提としているため，漏えい・改ざん等による影響は小さい。 | 一般:レベル≧1<br>管理:レベル＝2 |
| 教育システム | Ⅰ | 公開を前提としているため，漏えい・改ざん等による影響は小さい。 | 一般:レベル≧1<br>管理:レベル＝2 |
| オープンコースウェア | Ⅰ | 公開を前提としているため，漏えい・改ざん等による影響は小さい。 | 一般:レベル＝1<br>管理:レベル＝2 |
| セキュリティ<br>e-Learnming | Ⅰ | 学内公開を前提としているため，漏えい・改ざん等による影響は小さい。外部コンテンツと学内専用コンテンツあり． | 一般:レベル＝2<br>管理:レベル＝2 |

# 大学経営

| サービス | 重要度 | 備考 | 認証強度 |
|---|---|---|---|
| その他事務システム | Ⅳ | 教職員の基本データを含むため，漏えい等による影響は大きい。 | 管理:レベル≧3 |
| 大学評価情報システム | Ⅳ | 教職員の業績・活動データを含むため，漏えい等の影響は大きい。 | 管理:レベル≧3 |
| IRデータベース<br>(データウェアハウス) | Ⅳ | 教職員の業績・活動データを含むため，漏えい等の影響は大きい。大学評価情報システムにIR(Institutional Research)データベースを含む場合が多い。 | 管理:レベル≧3 |
| 研究者総覧<br>データベース | Ⅰ～Ⅲ | 公開情報はⅠ，教員評価を含む場合は，機密性2－3の情報が吹き生まれるため重要度はⅡ，Ⅲ. | 教員:レベル＝2<br>管理:レベル≧2 |



# 格付けと認証強度レベルのまとめ

- 本調査における各分野と連携し、学内サービスの格付けとそれに必要な認証強度レベルを策定
- 具体的な方式や各機関におけるケーススタディを継続的に調査、情報提供していく必要あり
  - 複数の認証方法の組み合わせに関する対応マップの詳細を検討
    - IP認証とパスワード認証の組み合わせと認証強度の関係など
  - レベル2に対応する具体的なパスワード強度に関する指針の提供
  - 証明書を必要とする認証には、NIIが提供する次期証明書サービスを活用可能
  - 多要素認証に関しては、先行大学(金沢大学等)の事例を普及

AC利用における認証機能の基本的な方針を策定
今後は具体的なケーススタディの収集・展開

# データプライバシー保護のための基本的な事項

## ①事業者が行う措置の対外的明確化

プライバシーポリシー、プライバシーステートメント等の策定・公表
関係法令等の遵守、利用目的の通知・公表、開示等の個人情報の取扱手続の対外的な説明
個人情報の漏えい等の事案が発生した場合の対策（二次被害の防止、類似事案の発生回避等の観点からの事実関係等の公表）

## ②責任体制の確保

個人情報保護管理者の設置
個人情報の安全管理体制確保のための仕組みの整備
委託元と委託先のそれぞれの責任等を明確に定めることにより、再委託される場合も含めて実効的な監督体制を確保すること

## ③従業者の啓発

教育研修の実施等を通じた従業者の啓発
従業者の個人情報保護意識の徹底



# アンケート調査(プライバシ)結果の概要

- ほとんどの大学・機関において、「個人情報保護方針」が作成されており、内外に周知・公開されている。
- 「個人情報保護方針」において、利用目的の明確化や安全管理措置について言及されている機関が多いが、対象とする個人情報の定義がなかったり、問合せ窓口が明記されていないなど、実運用上に必要となる指針が不足しているケースがみられる。

- 運用のための組織・体制は多くの機関で整備されている。
- 多くの機関で、個人情報を収集するための手続き、手順が定められており、個人情報は適切に収集されていると推定される。
- 監査を実施している機関は６割程度となり、教育・訓練の実施はさらに低く、従業員への継続的な見直し体制がやや不足している。

- 多くの機関で、業務委託先への個人情報の提供を行っている。
- 第三者提供をする場合、本人の同意確認を行っているが、オプトアウト措置は用意されていないケースも少なからずみられる。
- 共同利用への手続きが定められている事例はさらに少なく、インタークラウドのような環境での利用への対応は今後の課題と考えられる。