広島大学
クラウドサービス利用ガイドライン
説 明 会

主催：広島大学情報セキュリティ推進機構
日時：2014年（平成26年）2月5日（水）
場所：広島大学情報メディア教育研究センター
本館2階セミナー室

情報メディア教育研究センター
西村　浩二

広 島 大 学

ガイドライン整備の背景

広島大学

- クラウドサービスの利用
  - クラウド事業者との間で外部委託契約
  - 事業者（メーカ、SIer）によっても定義が異なる（プライベート？パブリック？オンプレミス？オフプレミス？）
  - 現時点ではクラウド事業者および使用するサービス内容に対する基準等が定められていない
- セキュリティポリシーとの整合性
  - 広島大学情報セキュリティポリシー（平成17年4月1日）
    - http://info.office.hiroshima-u.ac.jp/policy/index.html（学内限定）
  - 平成23年度あたりから問合せが急増
    - 「Dropboxで大学の情報を扱って良いか？」
    - 「サービスの良い使い方、悪い使い方を教えて欲しい」
- 平成24年度1年をかけて検討
  - 具体的、わかりやすい、実行可能

個人向けストレージサービス

広島大学

- 個人が約款に基づいて利用するストレージサービスの例
  - Dropbox
  - iCloud
  - Microsoft SkyDrive
  - Google ドライブ、など
- 約款に同意して利用開始
  - きちんと読まずに同意する人が多い
- 改訂は事業者が考えるタイミングで
  - 改訂されたことに気が付かない
  - 利用を続けると（改訂後の）約款に同意したことになる
- コンテンツの所有権や取り扱いに関する規約にも注意が必要

Dropbox 利用規約

広島大学

- アイテムとプライバシー

  当社サービスをご利用いただくことにより、Dropbox に送信する情報、ファイルそしてフォルダを当社に提供するものとします（"アイテム"と共に）。ユーザーは自分のアイテムの完全なる所有権を保有します。当社はそれらに対していかなる権利も要求するものではありません。本規約は、下記で説明される当社のサービスを運営する上で必要とされる限定された権利を除いて、ユーザーのアイテムまたは知的財産への権利を当社に付与するものではありません。

  当社にユーザーのコンテンツの操作を委託する場合には、ユーザーの許可が必要になります。たとえば、ユーザーの指示によるファイルのホストやファイルの共有が挙げられます。これには、画像サムネイルや文書のプレビューのような可視性のある製品機能が含まれます。また、当社サービスの技術管理のために選択される設計（安全に格納するためにデータを冗長的にバックアップするなど）も含まれます。当社サービスを提供するために必要な動作に関して、貴方は当社に許可を付与する必要があります。この許可は、当社サービスを提供するために取り組んでいる信頼されるサードパーティにも適用されます。たとえば、Amazon は（当社サービスを提供するために）当社にストレージ領域を提供しています。

- *https://www.dropbox.com/terms*

  最終改訂日：2012年3月26日

Dropbox 利用規約（続き）

広島大学

- 英文はたしかに変更されていないが…

  You give us the permissions we need to do those things solely to provide the Services. This permission also extends to trusted third parties we work with to provide the Services, for example Amazon, which provides our storage space (again, only to provide the Services).

① 2012年10月4日に表示されていた内容

お客様は、本サービスを提供する目的に限り、当社がこれらを実施するために必要なアクセス権を付与するものとします。このアクセス権は、記憶領域を提供する Amazon を初めとして、当社と協力して本サービスを提供する信頼できる第三者にも適用されるものとします (同様に、本サービスを提供する目的に限り)。

② 現在の内容

当社サービスを提供するために必要な動作に関して、貴方は当社に許可を付与する必要があります。この許可は、当社サービスを提供するために取り組んでいる信頼されるサードパーティにも適用されます。たとえば、Amazon は（当社サービスを提供するために）当社にストレージ領域を提供しています。

- 訳によって受ける印象が異なる
  - ①は無条件にアクセス権を与える（デフォルト許可）印象を、
  - ②はアクセス権が制限できる（デフォルト拒否）印象を与える

iCloud 利用規約

- お客様からの使用許諾

  Appleは、当社よりお客様に使用許諾するマテリアルを除き、本サービスにおいてお客様から投入されたまたは利用可能な状態にされたマテリアルおよび/またはコンテンツについて所有権を主張しません。ただし、お客様が当該コンテンツを共有することを承認した公衆その他のユーザからアクセス可能な本サービスの領域にそのコンテンツを投入し、または掲示されますと、お客様は、お客様に対しいかなる対価または義務を負うこともなしに、そのコンテンツが投入されたまたは利用可能な状態にされた目的に限り、本サービスにおいてそのコンテンツを利用し、頒布し、再現し、修正し、翻案し、出版し、翻訳し、公演し、および公表する、世界的な使用料無料の非独占的な使用許諾をAppleに付与されたものとします。お客様は、お客様が投入しまたは掲示したコンテンツが、お客様単独の責任に帰するものであること、他者の権利を侵害しもしくはこれに抵触するものでなく、もしくは法律に違反するものでなく、侵害その他不法な行為を促進しもしくは奨励するものでなく、またはその他猥褻なもの、好ましくないものもしくは下品なものでないことに同意します。公衆その他のユーザからアクセス可能な本サービスの領域に当該コンテンツを投入しまたは掲示されますと、お客様は、お客様が当該マテリアルの所有者であることおよび/またはその頒布に必要なすべての権利、使用許諾および承認を得ていることを表明しているものとします。

- http://www.apple.com/legal/icloud/jp/terms.html

  最終改訂：2013年9月18日

Microsoft サービス規約

- 3.1. 本サービスを掲載したコンテンツは、だれが所有することになりますか。

  コンテンツには、データ、ドキュメント、写真、動画、音楽、電子メール、インスタント メッセージなど、本サービスを通じてアップロード、保存、または転送されるものすべて (以下、「コンテンツ」といいます) が含まれます。お客様が所有するコンテンツ (クリップ アートなど) に組み込むことができる、マイクロソフトがお客様にライセンス付与したマテリアルを除き、マイクロソフトは、本サービスに関連してお客様が提供したコンテンツの所有権を主張しません。お客様のコンテンツは、あくまでもお客様のものであり、お客様が責任を持ちます。また、本サービスにおいてお客様または他のユーザーが公開するコンテンツを、マイクロソフトが規制、検証、費用負担、承認することはありません。またマイクロソフトがかかるコンテンツに関する責任を負うことはありません。

- 3.3. Microsoftはコンテンツをどのように扱いますか。

  お客様がお客様のコンテンツを本サービスにアップロードした場合、お客様はお客様の保護に必要な場合、および Microsoft 製品やサービスの提供、保護、向上に必要な場合にのみ、かかるコンテンツが使用、修正、編集、保存、複製、頒布、および表示される場合があることに同意するものとします。たとえば、マイクロソフトは、スパムやマルウェアを検出してそれらから保護するため、または新機能によりサービスを改善してサービスを使いやすくするために、電子メール、チャット、または電話から情報を自動的に分離することがあります。お客様のコンテンツを処理する際、Microsoft はお客様のプライバシーを保護するための手順を実行します。

- *http://windows.microsoft.com/ja-JP/windows-live/microsoft-services-agreement*

  更新日：2012年8月27日、発効日：2012年10月19日

Google 利用規約

広島大学

- 本サービス内のユーザーのコンテンツ

  本サービスの一部では、ユーザーがコンテンツを提供することができます。ユーザーは、そのコンテンツに対して保有する知的財産権を引き続き保持します。つまり、ユーザーのものは、そのままユーザーが所有します。

  本サービスにユーザーがコンテンツをアップロードまたはその他の方法により提供すると、ユーザーは Google（および Google と協働する第三者）に対して、そのコンテンツについて、使用、ホスト、保存、複製、変更、派生物の作成（たとえば、Google が行う翻訳、変換、または、ユーザーのコンテンツが本サービスにおいてよりよく機能するような変更により生じる派生物などの作成）、（公衆）送信、出版、公演、上映、（公開）表示、および配布を行うための全世界的なライセンスを付与することになります。このライセンスでユーザーが付与する権利は、本サービスの運営、プロモーション、改善、および、新しいサービスの開発に目的が限定されます。このライセンスは、ユーザーが本サービス（たとえば、ユーザーが Google マップに追加したビジネス リスティング）の利用を停止した場合でも、有効に存続するものとします。本サービスの一部では、ユーザーがそのサービスに提供したコンテンツにアクセスし、それを削除する方法が提供されることがあります。さらに本サービスの一部には、そのサービスに提供されたコンテンツの Google による利用範囲を狭める規定または設定があります。本サービスに提供するコンテンツについて、このライセンスを Google に付与するのに必要な権利を保有していることを必ずご確認ください。

  …

- http://www.google.com/policies/terms/

  最終更新日：2013年11月11日（旧版や変更の概要を確認できる）

クラウドの定義

NISTによる クラウドコンピューティングの定義

広島大学

- 出典
  - The NIST Definition of Cloud Computing
  - NIST: National Institute of Standards and Technology（米国 国立標準技術研究所）
  - http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
  - http://www.ipa.go.jp/security/publications/nist/documents/SP800-145-J.pdf（日本語訳）

- クラウドコンピューティングは、共用の構成可能なコンピューティングリソース（ネットワーク、サーバー、ストレージ、アプリケーション、サービス）の集積に、どこからでも、簡便に、必要に応じて、ネットワーク経由でアクセスすることを可能とするモデルであり、最小限の利用手続きまたはサービスプロバイダとのやりとりで速やかに割当てられ提供されるものである。このクラウドモデルは5つの基本的な特徴と3つのサービスモデル、および4つの実装モデルによって構成される。
  - 基本的な特徴
    - On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, Measured service
  - サービスモデル
    - SaaS, PaaS, IaaS
  - 実装モデル
    - Private cloud, Community cloud, Public cloud, Hybrid cloud

- クラウドのインフラストラクチャは、クラウドコンピューティングの5つの基本的な特徴を可能にするためのハードウェアとソフトウェアの集合である。クラウドのインフラストラクチャは、物理レイヤーと抽象レイヤーの両方を含むものと考えられる。物理レイヤーは、提供されるクラウドサービスをサポートするのに必要なハードウェアリソースからなり、通常、サーバー、ストレージ、およびネットワークコンポーネントを含む。抽象レイヤーは、物理レイヤー上に配備されたソフトウェアからなり、クラウドの基本的な特徴を明白に示す部分である。概念上は、抽象レイヤーは物理レイヤーの上に位置する。

基本的な特徴

- オンデマンド・セルフサービス (On-demand self-service)
  - ユーザは、各サービスの提供者と直接やりとりすることなく、必要に応じ、自動的に、サーバーの稼働時間やネットワークストレージのようなコンピューティング能力を一方的に設定できる。
- 幅広いネットワークアクセス (Broad network access)
  - コンピューティング能力は、ネットワークを通じて利用可能で、標準的な仕組みで接続可能であり、そのことにより、様々なシンおよびシッククライアントプラットフォーム（例えばモバイルフォン、タブレット、ラップトップコンピュータ、ワークステーション）からの利用を可能とする。
- リソースの共用 (Resource pooling)
  - サービスの提供者のコンピューティングリソースは集積され、複数のユーザにマルチテナントモデルを利用して提供される。様々な物理的・仮想的リソースは、ユーザの需要に応じてダイナミックに割り当てられたり再割り当てされたりする。物理的な所在場所に制約されないという考え方で、ユーザは一般的に、提供されるリソースの正確な所在地を知ったりコントロールしたりできないが、場合によってはより抽象的なレベル（例：国、州、データセンタ）で特定可能である。リソースの例としては、ストレージ、処理能力、メモリ、およびネットワーク帯域が挙げられる。
- スピーディな拡張性 (Rapid elasticity)
  - コンピューティング能力は、伸縮自在に、場合によっては自動で割当ておよび提供が可能で、需要に応じて即座にスケールアウト／スケールインできる。ユーザにとっては、多くの場合、割当てのために利用可能な能力は無尽蔵で、いつでもどんな量でも調達可能のように見える。
- サービスが計測可能であること (Measured service)
  - クラウドシステムは、計測能力を利用して、サービスの種類（ストレージ、処理能力、帯域、実利用中のユーザアカウント数）に適した管理レベルでリソースの利用をコントロールし最適化する。リソースの利用状況はモニタされ、コントロールされ、報告される。それにより、サービスの利用結果がユーザにもサービス提供者にも明示できる。

サービスモデル

- SaaS (Software as a Service)
  - 利用者に提供される機能は、クラウドのインフラストラクチャ上で稼動しているプロバイダ由来のアプリケーションである。アプリケーションには、クライアントの様々な装置から、ウェブブラウザのようなシンクライアント型インターフェイス（例えばウェブメール）、またはプログラムインターフェイスのいずれかを通じてアクセスする。ユーザは基盤にあるインフラストラクチャを、ネットワークであれ、サーバーであれ、オペレーティングシステムであれ、ストレージであれ、各アプリケーション機能ですら、管理したりコントロールしたりすることはない。ただし、ユーザに固有のアプリケーションの構成の設定はその例外となろう。
- PaaS (Platform as a Service)
  - 利用者に提供される機能は、クラウドのインフラストラクチャ上にユーザが開発したまたは購入したアプリケーションを実装することであり、そのアプリケーションはプロバイダがサポートするプログラミング言語、ライブラリ、サービス、およびツールを用いて生み出されたものである。ユーザは基盤にあるインフラストラクチャを、ネットワークであれ、サーバーであれ、オペレーティングシステムであれ、ストレージであれ、管理したりコントロールしたりすることはない。一方ユーザは自分が実装したアプリケーションと、場合によってはそのアプリケーションをホストする環境の設定についてコントロール権を持つ。
- IaaS (Infrastructure as a Service)
  - 利用者に提供される機能は、演算機能、ストレージ、ネットワークその他の基礎的コンピューティングリソースを配置することであり、そこで、ユーザはオペレーティングシステムやアプリケーションを含む任意のソフトウェアを実装し走らせることができる。ユーザは基盤にあるインフラストラクチャを管理したりコントロールしたりすることはないが、オペレーティングシステム、ストレージ、実装されたアプリケーションに対するコントロール権を持ち、場合によっては特定のネットワークコンポーネント機器（例えばホストファイアウォール）についての限定的なコントロール権を持つ。

実装モデル

- プライベートクラウド (Private cloud)
  - クラウドのインフラストラクチャは、複数の利用者（例：事業組織）から成る単一の組織の専用使用のために提供される。その所有、管理、および運用は、その組織、第三者、もしくはそれらの組み合わせにより行われ、存在場所としてはその組織の施設内または外部となる。
- コミュニティクラウド (Community cloud)
  - クラウドのインフラストラクチャは共通の関心事（例えば任務、セキュリティの必要、ポリシー、法令順守に関わる考慮事項）を持つ、複数の組織からなる成る特定の利用者の共同体の専用使用のために提供される。その所有、管理、および運用は、共同体内の１つまたは複数の組織、第三者、もしくはそれらの組み合わせにより行われ、存在場所としてはその組織の施設内または外部となる。
- パブリッククラウド (Public cloud)
  - クラウドのインフラストラクチャは広く一般の自由な利用に向けて提供される。その所有、管理、および運用は、企業組織、学術機関、または政府機関、もしくはそれらの組み合わせにより行われ、存在場所としてはそのクラウドプロバイダの施設内となる。
- ハイブリッドクラウド (Hybrid cloud)
  - クラウドのインフラストラクチャは二つ以上の異なるクラウドインフラストラクチャ（プライベート、コミュニティまたはパブリック）の組み合わせである。各クラウドは独立の存在であるが、標準化された、あるいは固有の技術で結合され、データとアプリケーションの移動可能性を実現している（例えばクラウド間のロードバランスのためのクラウドバースト）。

マルチテナントクラウドでのセキュリティの課題

レイヤ	課題		説明
Web	コンテンツ利用制御	マッシュアップ通信制御機構	同一生成元ポリシーの順守、コンポーネント間通信を監視
		コンテンツ利用ポリシー	ポリシーを宣言して、開発者が意図しない動作を最小化
	アクセス制御の脆弱性		アクセス制御が不適切または不在、開発者側での対応
	クライアント側検証の脆弱性	エンドポイントでのリスク検出	信頼できないコード（JavaScriptなど）を安全でない形で利用
		ミドルポイントでのリスク検出	非HTMLコンテンツをサンドボックスブラウザ上で実行
アプリケーション	セキュアなデータ保存	暗号化データの操作	プロキシ再暗号化技術、準同型暗号
		データの完全性	複数サーバによるストレージの正当性の確認
		データの冗長性削除	冗長性削除技術を防ぐための暗号化
	認証と権限付与	認証フレームワーク	ロールベースアクセス制御、OpenID、x.509証明書
		クエリ制御	クエリの精査、セマンティックWeb言語
	ユーザ別のデータ隔離	プロセスの隔離	1つのコンポーネントが複数ユーザのデータを処理しない
		選択的復号技術	IDベース暗号、属性ベース暗号（ABE）
オペレーティングシステム	特権の隔離		トロイの木馬、SELinux（Disableにされることが多い）
	カーネルの脆弱性		バグ、特権ユーザによる信頼できないソフトウェア実行
ハイパーバイザー	VMM（仮想マシンモニタ）のセキュリティ	脆弱性	VM上の悪意のあるコードによるVMMの停止など
		VMベースのルートキット	ルートキット検出器による検出を回避
		透過性	リモートからのVMM存在の検出、VMMに対する攻撃
		プラットフォームの完全性	アプリケーション単位でのVM割当、vTPM、HIMA
	VM（仮想マシン）のセキュリティ	イントロスペクション	ハイパーバイザからのゲストOSのデバッグ機能
		冗長性の削除	リソースの効率的活用の追求
HW＆SWプリミティブ	プログラミングコード	マネージドランタイムセキュリティ	Java, .NETに対する信頼性の低下、JavaSnoop
		リソースの隔離	サンドボックスへのI/Oを通じたデータ混入
	ハードウェア処理	共有プロセッサリソース	ハイパースレッディング技術の脆弱性（サイドチャネル）

出典：高橋 他, “マルチテナントクラウドコンピューティング：セキュリティ上の課題とアプローチ”, 信学技報, ICSS2011-36, pp.25-32, 2011.

カントリーリスク

- 米国愛国者法(Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act in 2001)
  - テロリズム（201条）やコンピュータ関連の一定の犯罪（202条）について、通信傍受を行う権限を認める
  - 一定の場合において、裁判所の命令なしに捜査官が電子メールやボイスメールを取得できる（209条）
  - 捜査官は、令状の通知なく家宅など（データセンターを含む）を捜索できる（213条）
  - FBIは国際テロや秘密諜報活動の防止を目的とした捜査であることを明示し、金融機関や通信プロバイダの同意が得られれば、それらが有する顧客の個人情報を裁判所の関与なく得ることができる（505条）
- EUデータ保護指令(Data Protection Directive)
  - EU内での個人データの取り扱いに際するプライバシー権の保護が目的
  - EU域外の国に個人データを移転する場合、原則として、その国がEUデータ保護指令が要求する個人データ保護の水準を有していることを要求
  - 日本は、EUデータ保護指令上の個人データ保護の水準を有しているEU域外の国に含まれていない（例外規定はあるが注意が必要）
- 実例
  - 2009年4月2日、FBIの捜査官が米国愛国者法に基づいてデータセンターを捜索し、2フロア分のサーバを押収したため、約50社の顧客に対するサービスが停止した

準拠法と管轄裁判所

- amazon web service
  - AWSカスタマーアグリーメント
    - http://aws.amazon.com/jp/agreement/
  - 準拠法は「アメリカ合衆国ワシントン州法」
  - 管轄裁判所は「アメリカ合衆国ワシントン州キング郡に所在する州裁判所または連邦裁判所」
- Google Apps for Education
  - Google Apps for Education 契約
    - http://www.google.com/apps/intl/ja/terms/education_terms.html
  - 準拠法は「アメリカ合衆国カリフォルニア州の州法」
  - 管轄裁判所は「アメリカ合衆国カリフォルニア州サンタクララ郡の裁判所」
- Office 365 Education
  - マイクロソフト オンライン サブスクリプション契約
    - http://www.microsoft.com/global/en-us/office365/RenderingAssets/mosa/MOSA2011Agr(Asia)JPN(JPN)(Apr2012)(HTML).htm
  - 準拠法は「日本の法律」
  - 管轄裁判所は「東京地方裁判所」
- Windows Azure
  - Windows Azure 契約
    - http://www.windowsazure.com/ja-jp/support/legal/subscription-agreement/
  - 準拠法は「日本の法律」
  - 管轄裁判所は「東京地方裁判所」

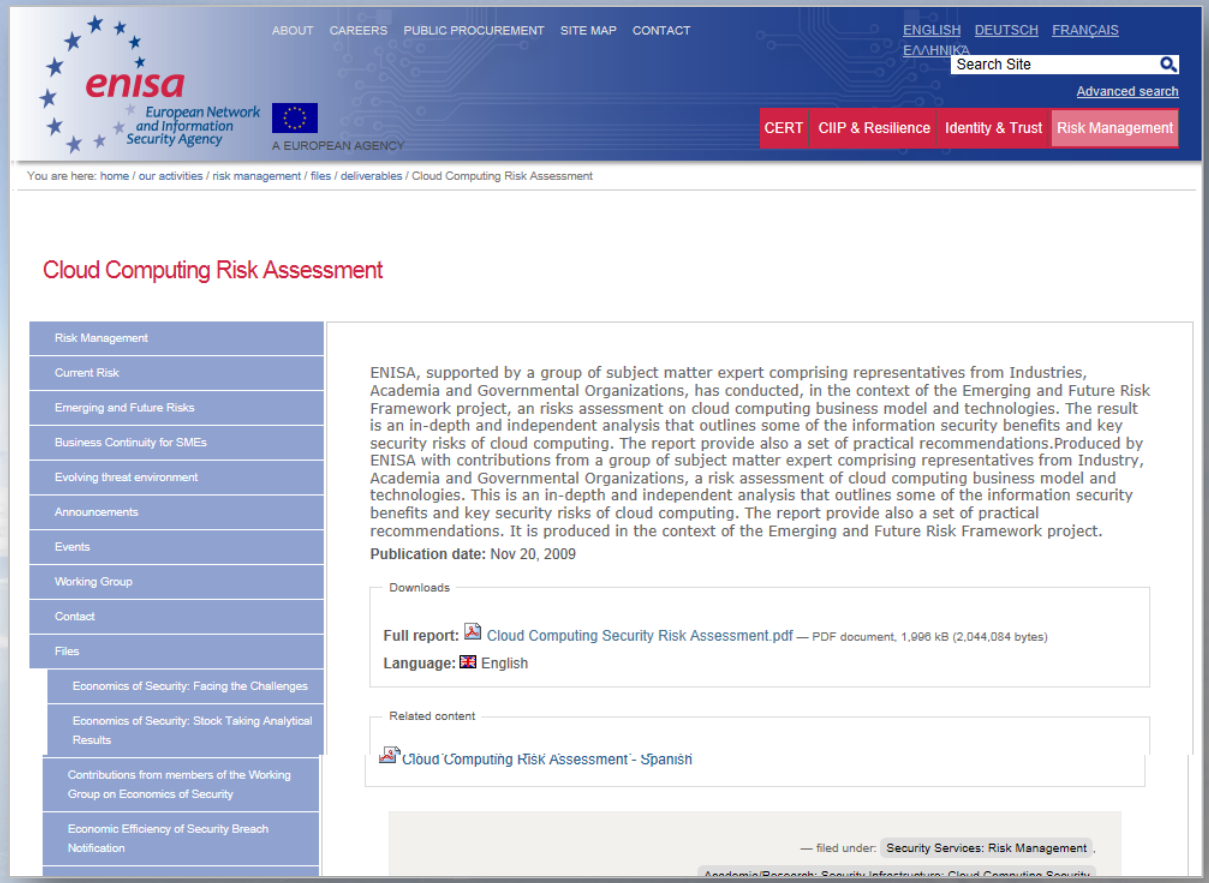
クラウド利用に関する参考文書

クラウド利用に関するガイドライン

広島大学

- NIST: National Institute of Standards and Technology
  米国国立標準技術研究所
  - Cloud Computing Synopsis and Recommendations
    クラウドコンピューティングの概要と推奨事項（SP-800-146）
    - https://www.ipa.go.jp/files/000025367.pdf（日本語訳）
- 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
    - http://www.ipa.go.jp/security/publications/enisa/documents/Cloud%20Information%20Assurance%20Framework.pdf（日本語訳）
  - 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
    - http://www.ipa.go.jp/security/publications/enisa/documents/Cloud%20Computing%20Security%20Risk%20Assessment.pdf（日本語訳）
- 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
    - http://www.meti.go.jp/press/2011/04/20110401001/20110401001.html
- 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
    - http://www.ipa.go.jp/security/cloud/tebiki_guide.html

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



- http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment
- http://www.ipa.go.jp/security/publications/enisa/documents/Cloud%20Computing%20Security%20Risk%20Assessment.pdf（日本語訳）

リスク項目（R1～R35）

広島大学

- ポリシーと組織関連のリスク

(R1) ロックイン
(R2) ガバナンスの喪失
(R3) コンプライアンスの課題
(R4) 他の共同利用者の行為による信頼の喪失
(R5) クラウドサービスの終了または障害
(R6) クラウドプロバイダの買収
(R7) サプライチェーンにおける障害

- 技術関連のリスク

(R8) リソースの枯渇（リソース割当の過不足）
(R9) 隔離の失敗
(R10) クラウドプロバイダ従事者の不正－特権の悪用
(R11) 管理用インタフェースの悪用（操作、インフラストラクチャアクセス）
(R12) データ転送途上における攻撃
(R13) データ漏えい（アップロード時、ダウンロード時、クラウド間転送）
(R14) セキュリティが確保されていない、または不完全なデータ削除
(R15) DDoS攻撃（分散サービス運用妨害攻撃）
(R16) EDoS攻撃（経済的な損失を狙ったサービス運用妨害攻撃）
(R17) 暗号鍵の喪失
(R18) 不正な探査またはスキャンの実施
(R19) サービスエンジンの侵害
(R20) 利用者側の強化手順と、クラウド環境との間に生じる矛盾

- 法的なリスク

(R21) 証拠提出命令と電子証拠開示
(R22) 司法権の違いから来るリスク
(R23) データ保護に関するリスク
(R24) ライセンスに関するリスク

- クラウドに特化していないリスク

(R25) ネットワークの途絶
(R26) ネットワークの管理（ネットワークの混雑、接続ミス、適切でない使用）
(R27) ネットワークトラフィックの改変
(R28) 特権の（勝手な）拡大
(R29) ソーシャルエンジニアリング攻撃（なりすまし）
(R30) 運用ログの喪失または改ざん
(R31) セキュリティログの喪失または改ざん（フォレンジック捜査の操作）
(R32) バックアップの喪失、盗難
(R33) 構内への無権限アクセス（装置その他の設備への物理的アクセスを含む）
(R34) コンピュータ設備の盗難
(R35) 自然災害

（出展）：ENISA「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」

リスクレベル

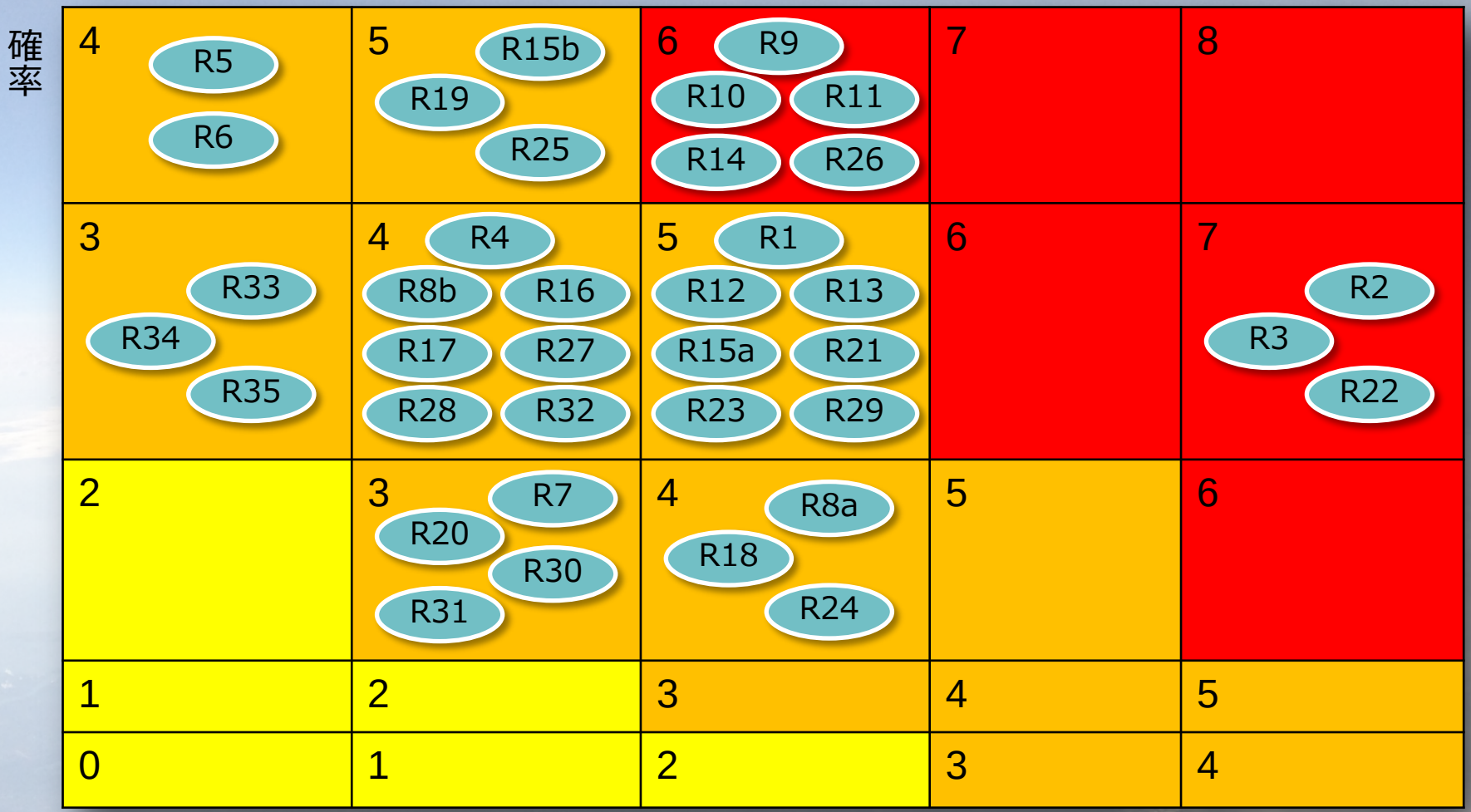
	インシデントシナリオの発生確率	きわめて低い（ほとんど発生しない）	低い（まず発生しない）	中程度（発生の可能性がある）	高い（発生の可能性が高い）	きわめて高い（頻繁に発生する）
事業影響	きわめて高い	4	5	6	7	8
	高い	3	4	5	6	7
	中程度	2	3	4	5	6
	低い	1	2	3	4	5
	きわめて低い	0	1	2	3	4

- 低リスク：0～2
- 中リスク：3～5
- 高リスク：6～8

（出展）：ENISA「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」

リスク項目の配置

広島大学



（出展）：ENISA「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」

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

広島大学

経済産業省
Ministry of Economy, Trade and Industry

›本文へ ›よくあるご質問 ›サイトマップ
文字サイズ変更 小 中 大
サイト内検索 検索 ›拡張検索

ホーム | 経済産業省について | お知らせ | 政策について | 統計 | 申請・お問合せ | English

お知らせ ▸ ニュースリリース ▸ 2011年度一覧 ▸ 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の公表～クラウドサービスの安全・安心な利用に向けて～

印刷

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の公表～クラウドサービスの安全・安心な利用に向けて～

本件の概要

経済産業省では、クラウドサービスを安全に安心して利用するために「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（以下、ガイドライン）」を策定しました。

本ガイドラインは、クラウド利用者が、クラウドサービス利用の際に、情報セキュリティ対策の観点から活用することを企図して策定しています。本ガイドラインを利用することで、より一層のクラウドサービスの利用促進を目指します。

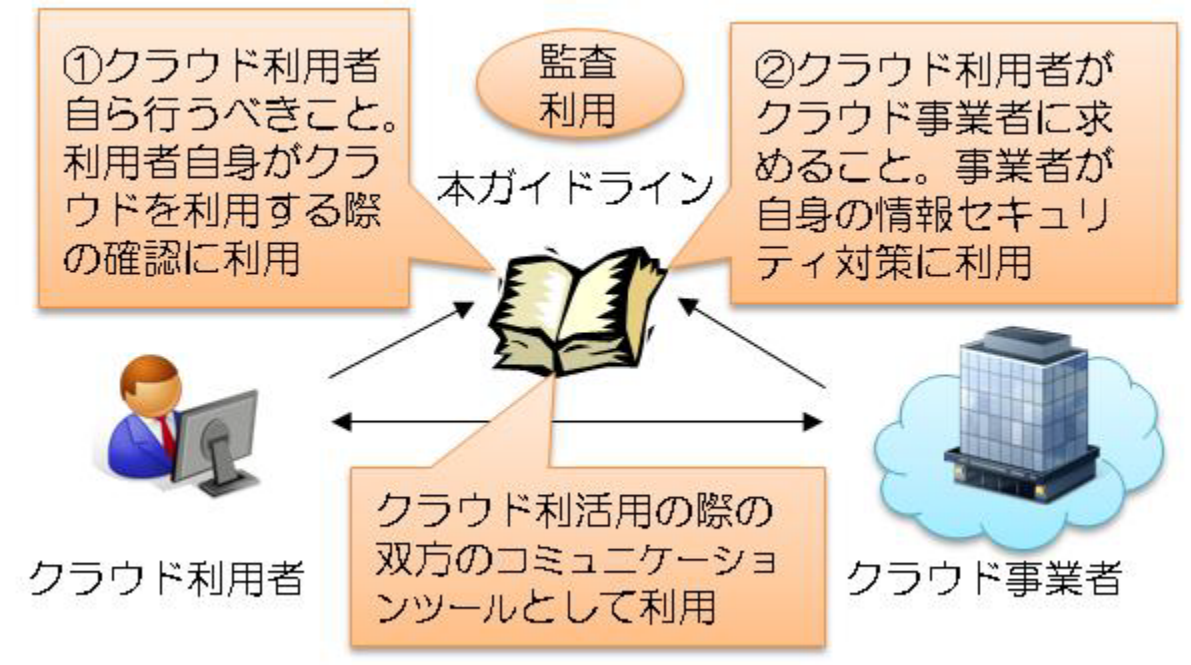
担当

商務情報政策局　情報セキュリティ政策室

お知らせ
- 会見・スピーチ・談話
- ニュースリリース
  - 2013年度一覧
  - 2012年度一覧
  - 2011年度一覧
  - 2010年度一覧
- 政府広報
- 広報誌・刊行物・パンフレット
- イベント・行事
- 意見募集
- 調達・予算執行

http://www.meti.go.jp/press/2011/04/20110401001/20110401001.html

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



ガイドラインの利用イメージ

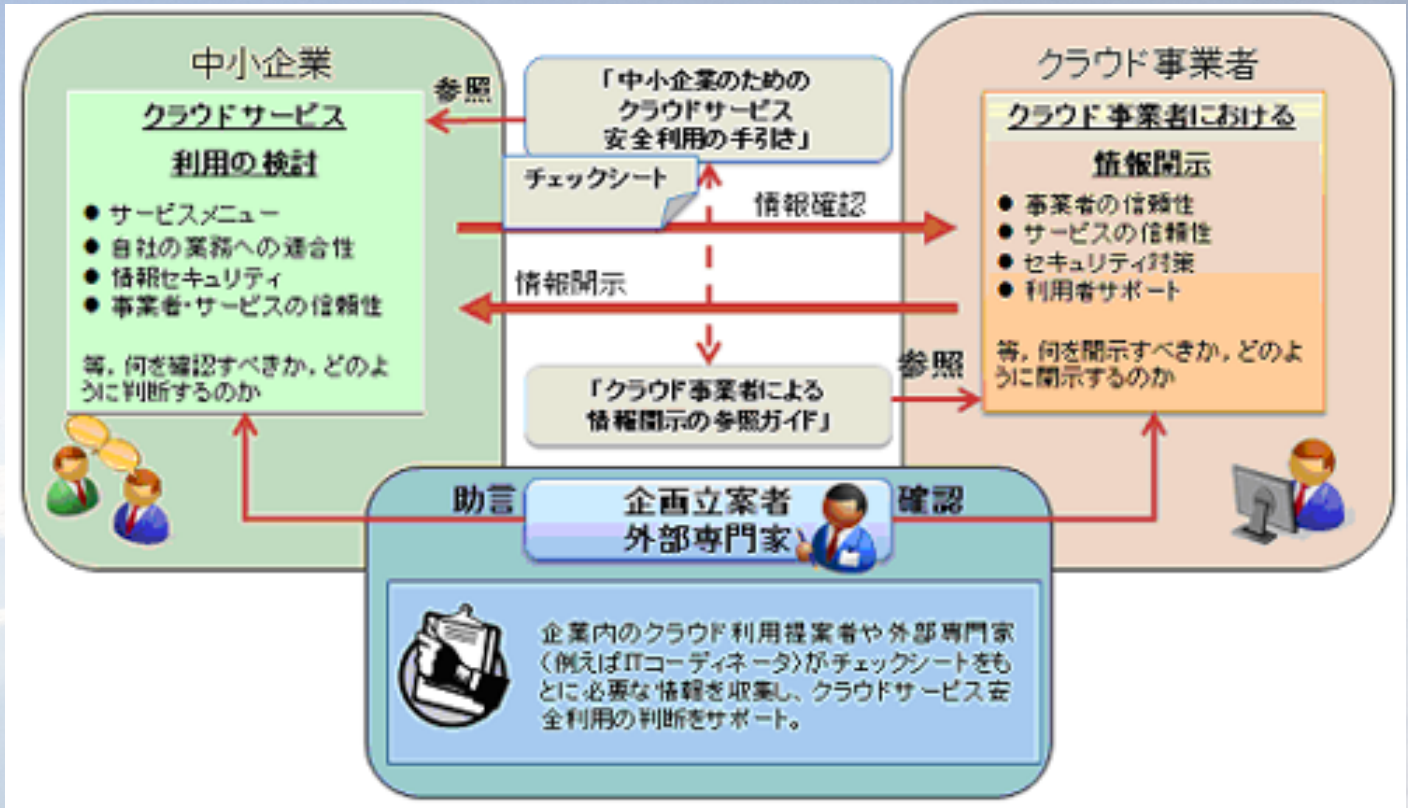
- クラウド利用者がクラウドサービスを利用する際に
  ①　クラウド利用者が自ら行うべきこと
  ②　クラウド利用者がクラウド事業者に求めること
  がまとめられている

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

広島大学

http://www.ipa.go.jp/security/cloud/tebiki_guide.html

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



- クラウド利用者がクラウドサービスの利用を検討する際に確認すべきことが、14項目のチェック項目に簡潔にまとめられている
- 「安全利用の手引き」に基づいてサービスを利用しようとしているクラウド利用者に、クラウド事業者がどのような情報をどの程度開示すべきかが示されている

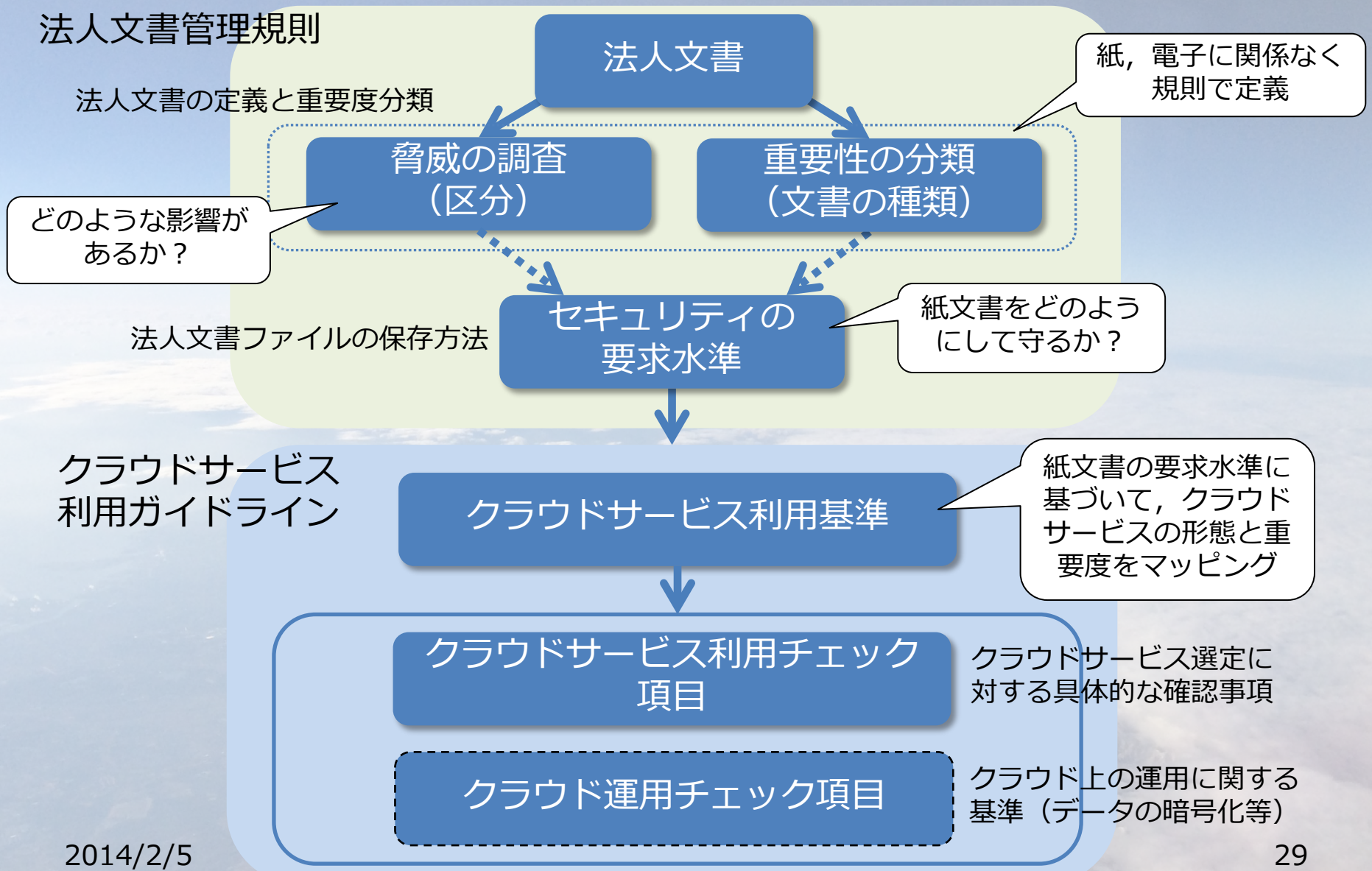
ここからが本題

クラウドサービス利用ガイドライン

ガイドライン整備の方針

- セキュリティポリシーとの整合性
  - 広島大学情報セキュリティポリシー（平成17年4月1日）
    - http://info.office.hiroshima-u.ac.jp/policy/index.html（学内限定）
  - 平成23年度あたりから問合せが急増
    - 「Dropboxで大学の情報を扱って良いか？」
    - 「サービスの良い使い方、悪い使い方を教えて欲しい」
- 平成24年度1年をかけて検討
  - 一般の構成員には具体的に何をすべきかを示す必要がある
- 本学または部局等が法人文書の保管場所としてクラウドサービスを利用する場合を想定
- 具体的には、
  - 本学における「クラウドサービスの種類」の定義
  - 法人文書の重要度に対応する「クラウドサービスの種類」の基準の設定
  - クラウドサービスを利用する際に確認すべき項目（チェックリスト）の作成
  - クラウドサービスを利用する際の諸手続きの整備

ガイドラインの位置付け



法人文書の定義と重要度分類

広島大学

区分		文書の種類	情報の類型(抜粋)
重要度Ⅳ	法人文書が流出（漏えい）、紛失、改ざん等した場合、本学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	学籍簿、成績原簿に関する情報 指導要領の情報
重要度Ⅲ	法人文書が流出（漏えい）、紛失、改ざん等した場合、本学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	学生指導に関する情報 卒業論文又は修士論文に関する情報
重要度Ⅱ	法人文書が流出（漏えい）、紛失、改ざん等した場合、本学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	住所 氏名
重要度Ⅰ	法人文書が流出（漏えい）、紛失、改ざん等した場合、本学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	公開講座等に関する情報

法人文書ファイルの保存方法

広島大学

重要度	紙文書	電子文書
重要度Ⅳ	常時人的又は機械的な入（退）室管理又は施錠がなされている部屋，又は金庫等で保存。（事務室金庫，役員室，サーバー室等）	担当者（決裁ラインにある上司を含め、業務を所掌するもの）のみ
重要度Ⅲ	無人時に機械的入（退）室管理又は施錠がなされている部屋等で，鍵のかかる鉄庫等に入れて保存。（事務室内の鍵付きキャビネット，建物内の常時施錠の書庫等）	担当グループのみ
重要度Ⅱ	時間外に機械的入（退）室管理又は施錠がなされている部屋等で保存。（事務室内のキャビネット等）	学内者のみ
重要度Ⅰ	公開用や配付用の文書以外は，重要度Ⅱと同様の保存方法が望ましい。	公開用文書以外は、「学内者のみ」のアクセス制限を設けることが望ましい

広島大学法人文書ファイル保存要領

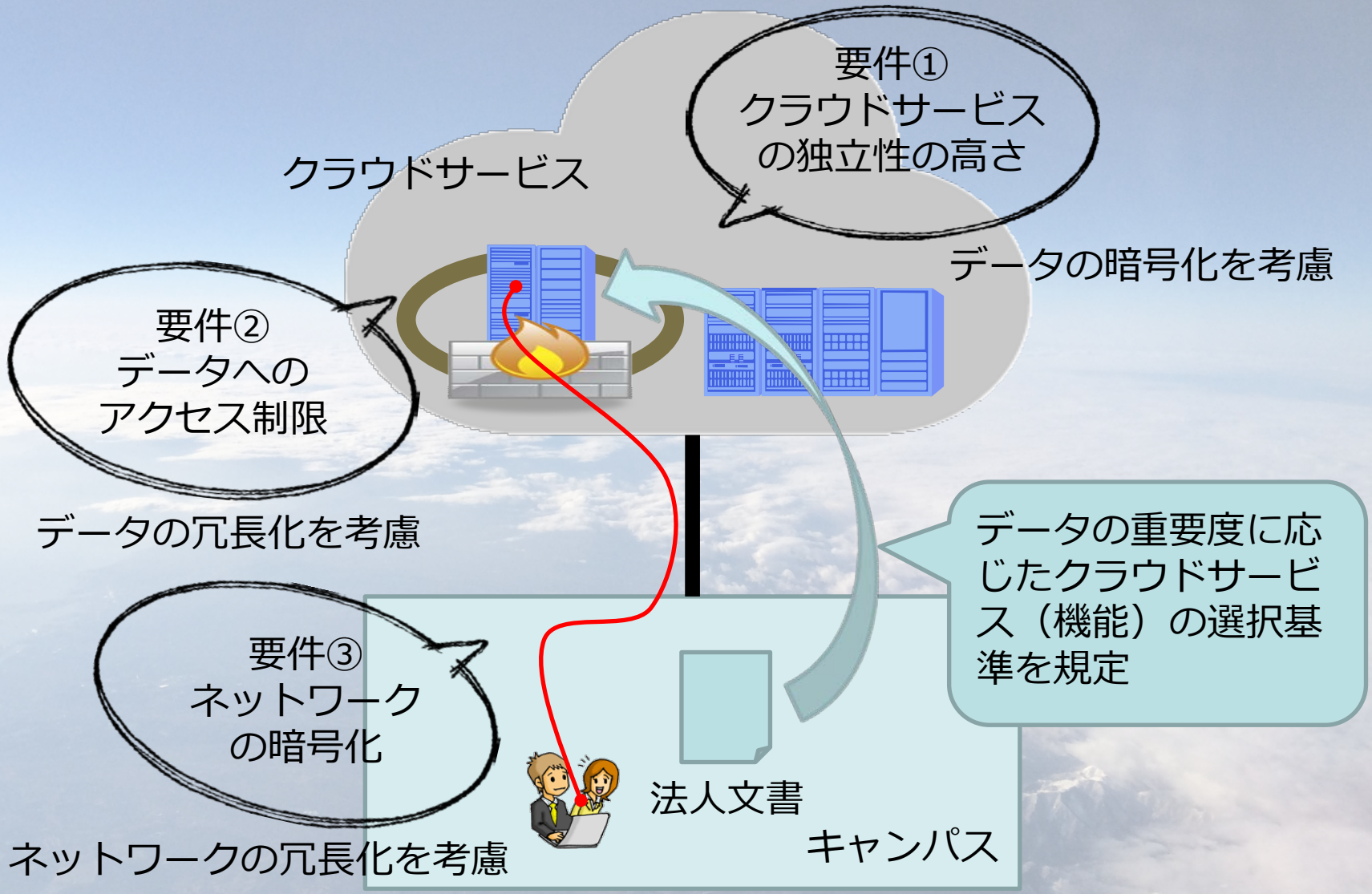
クラウドサービスの信頼度

広島大学

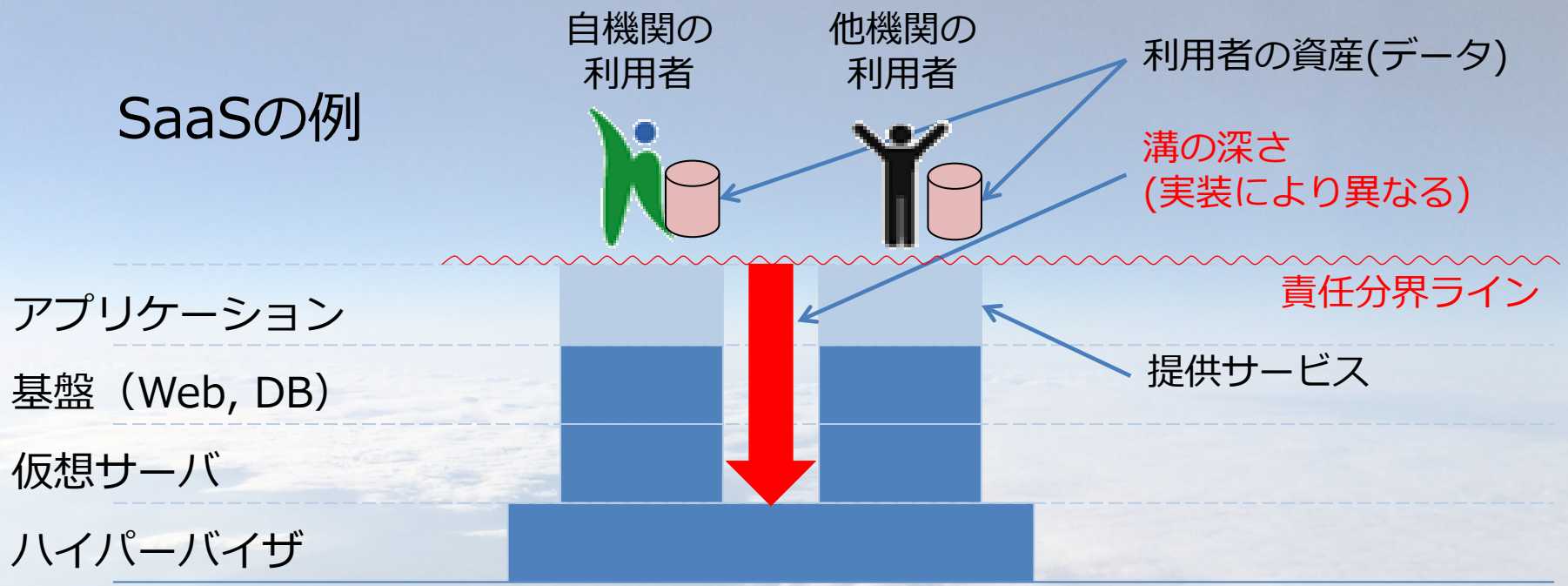
クラウドサービスの信頼度		信頼度Ⅳ	信頼度Ⅲ	信頼度Ⅱ	信頼度Ⅰ
法人文書の重要度	重要度Ⅳ	←			
	重要度Ⅲ	←	←		
	重要度Ⅱ	←	←	←	
	重要度Ⅰ	←	←	←	←

- クラウドサービスの信頼度
  - 独立性の高さ（他の利用者との隔離）
  - アクセス制御
  - 通信路の暗号化
- 本学または部局等が保有する法人文書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以下の法人文書を保存できる

クラウドサービス利用基準の要件

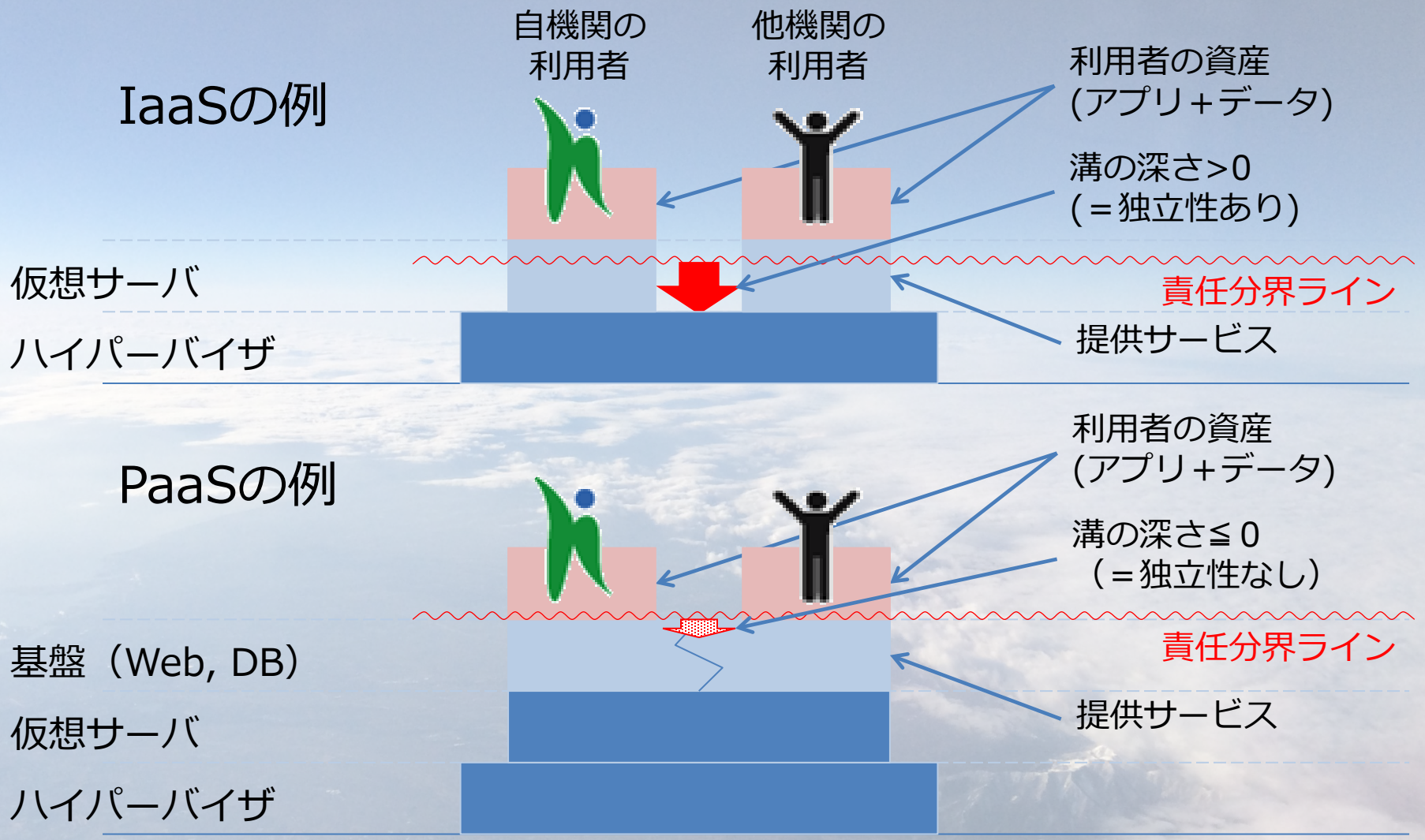


サービスの独立性の高さ



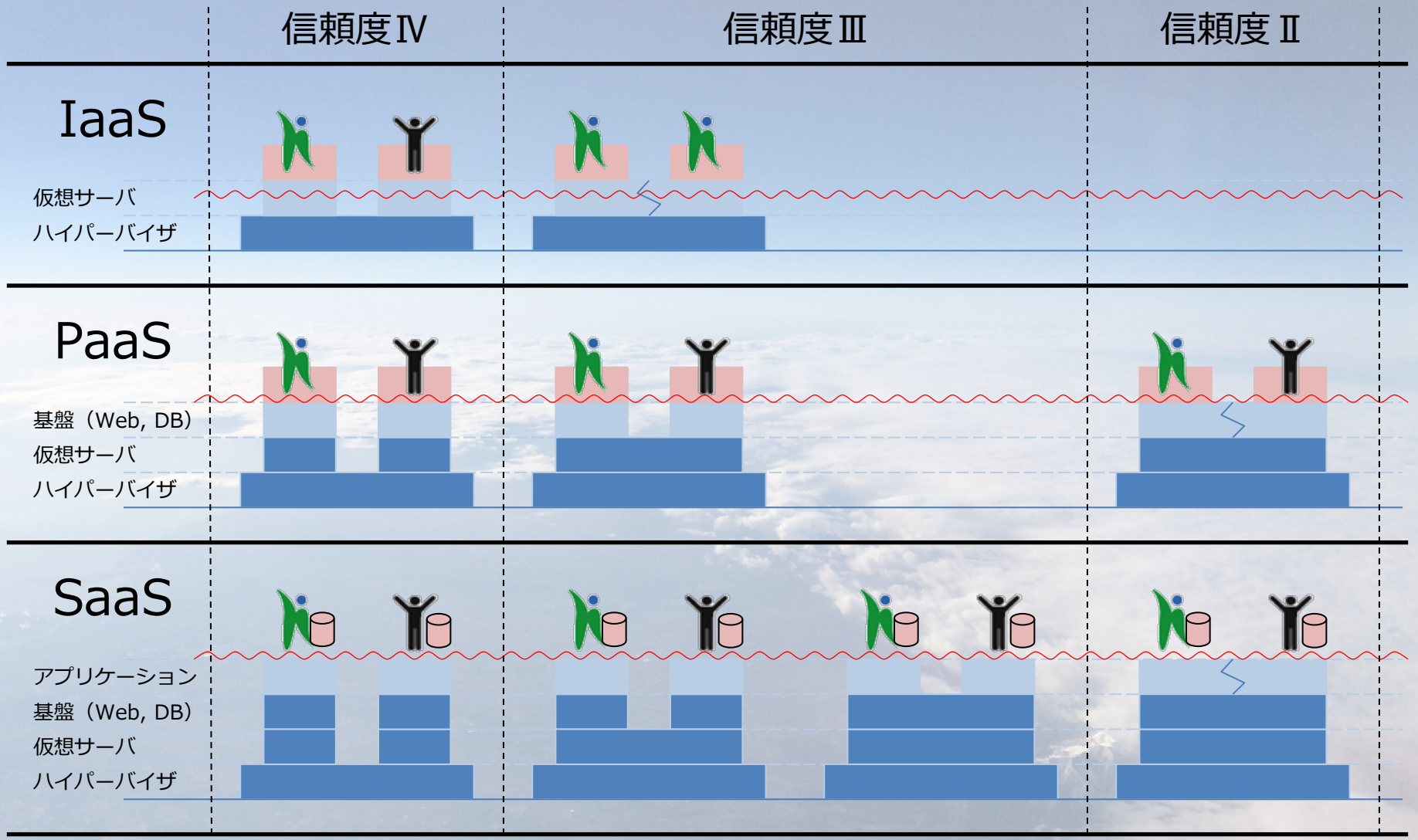
- クラウド事業者提供のサービス仕様書から以下を判断
  - サービスモデル（＝責任分界ライン）
  - 実装方法（＝溝の深さ）
- 「責任分界ラインより溝が深い」 → 独立性がある

サービスの独立性の高さ（続き）

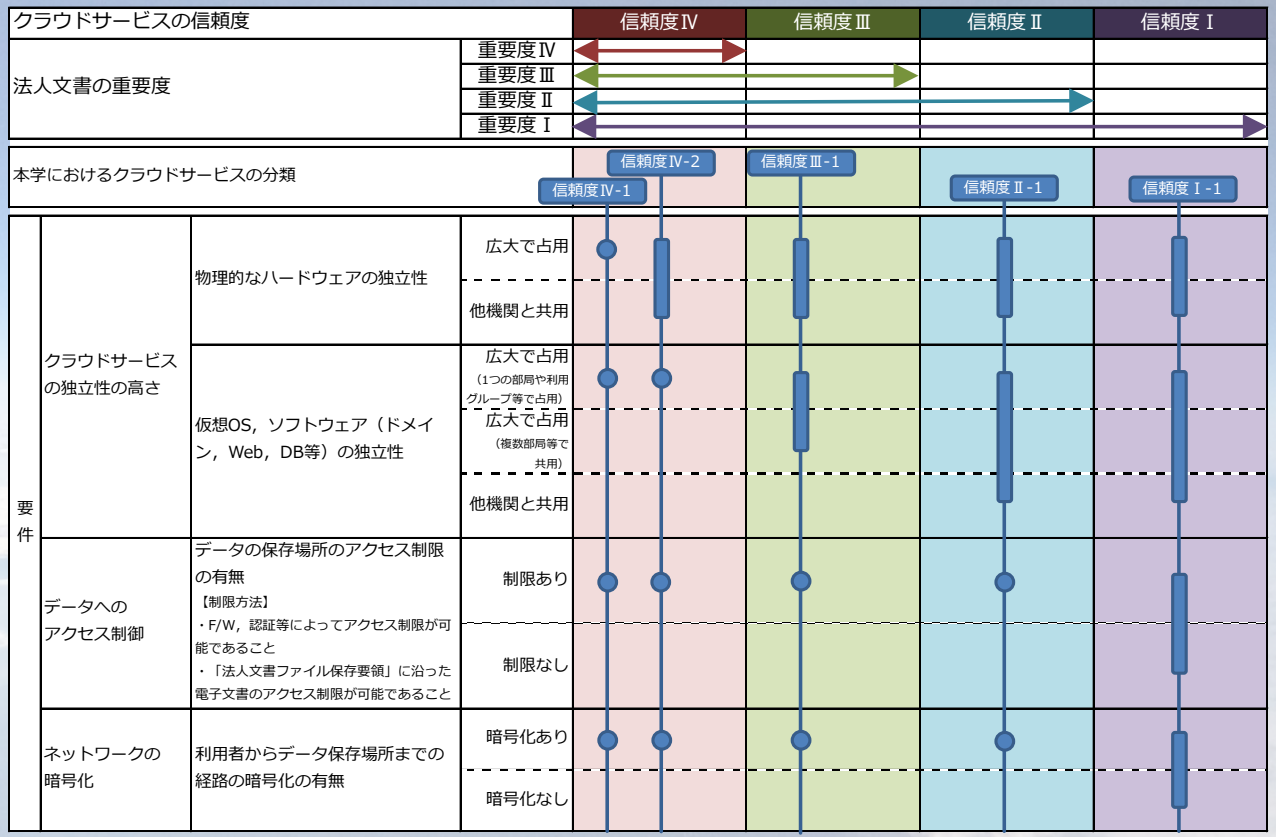


サービス(実装方法)と信頼度の対応

広島大学



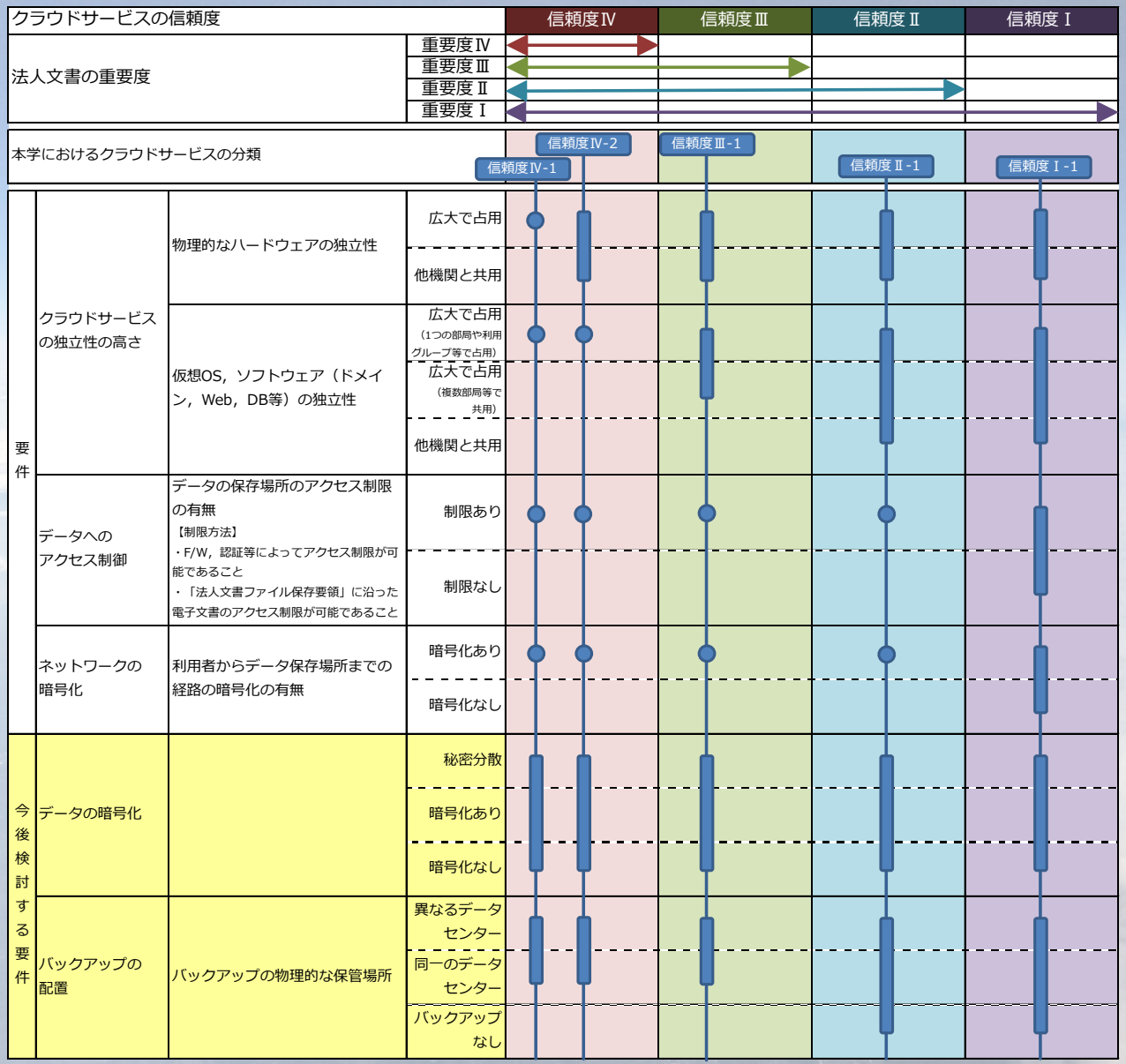
クラウドサービス利用基準



- 運用レベルの話として、以下についてもさらに検討が必要
  - データの暗号化や冗長化
  - ネットワーク（データセンター）の冗長化

クラウドサービス利用基準

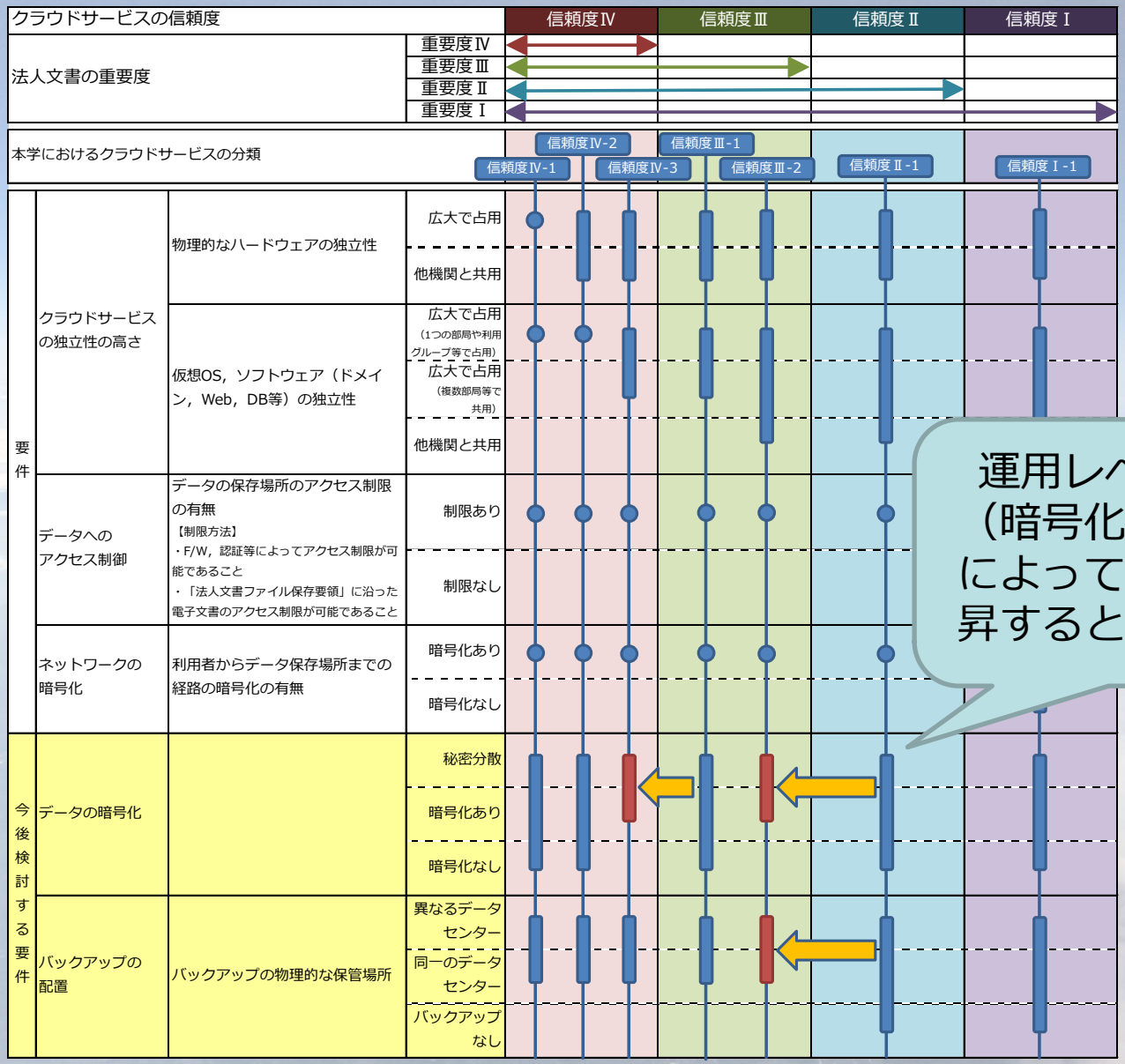
広島大学



暗号技術、秘密分散技術の利用

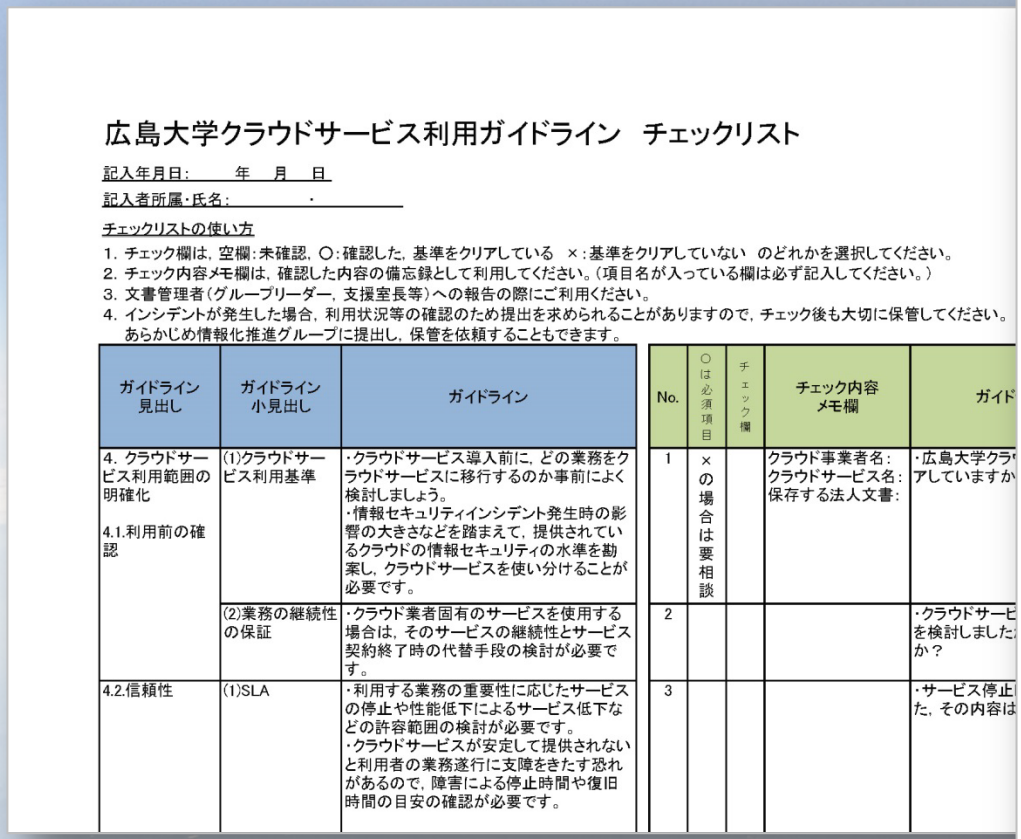
- 情報セキュリティに関する法制度
  - 会社法、個人情報保護法、著作権法、不正競争防止法、その他（銀行業法、保険業法、証券取引法など）
    → 法的責任の明確化
- 各技術の法的見解
  - 暗号技術
    - 「『個人情報』は、暗号化等によって秘匿化されているかどうかを問わない」（経済産業省個人情報保護ガイドライン）
  - 秘密分散技術
    - 「原本情報をビットレベルで分割し生成した部分集合単独では、原本情報を導き出せないため原本情報ではないと判断できる」（同上）
      → 部分集合の管理手法の確立と整備が必要
- 秘密分散に関する技術ガイドライン および 秘密分散技術利活用に関するガイドライン（平成22年3月）
  http://www.jipdec.or.jp/archives/ecom/results/h21seika/H21results-10.pdf
  - 秘密分散技術を実現するソフトウェアにおける必須・任意要件
  - 秘密分散技術を利活用するシステムで考慮すべき必須・任意要件
    - 付帯情報の追加・管理
    - 第三者機関との連携

クラウドサービス利用基準



クラウドサービス利用ガイドライン

広島大学



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

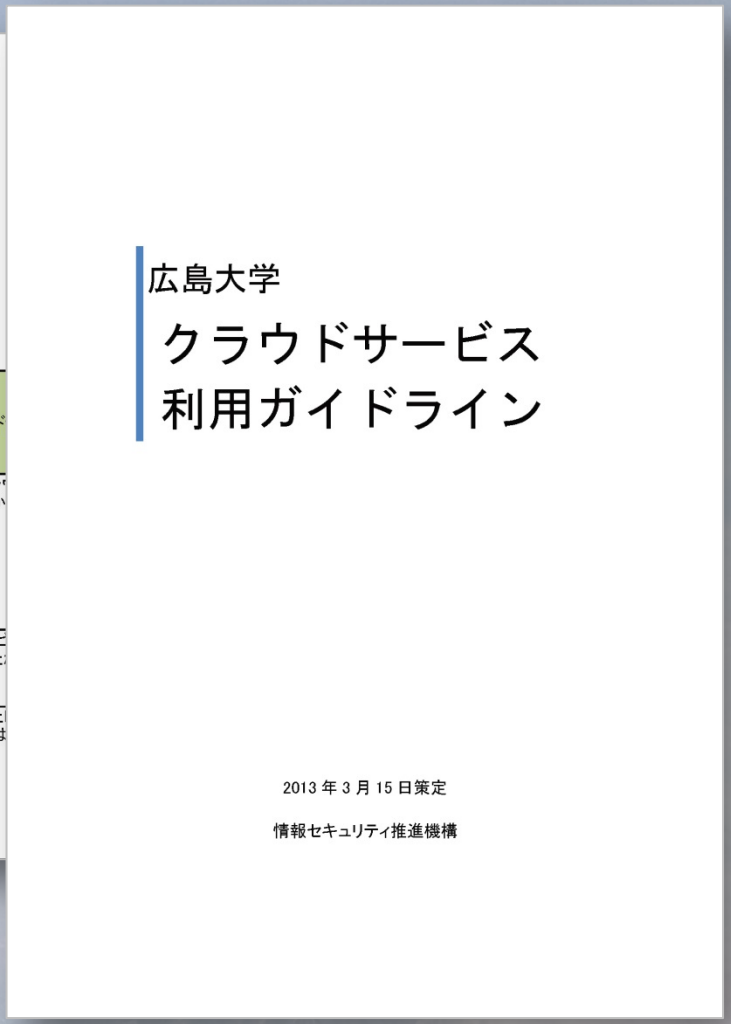
記入年月日:　　年　月　日

記入者所属・氏名:　　・

チェックリストの使い方

1. チェック欄は，空欄:未確認，○:確認した，基準をクリアしている　×:基準をクリアしていない　のどれかを選択してください。
2. チェック内容メモ欄は，確認した内容の備忘録として利用してください。(項目名が入っている欄は必ず記入してください。)
3. 文書管理者(グループリーダー，支援室長等)への報告の際にご利用ください。
4. インシデントが発生した場合，利用状況等の確認のため提出を求められることがありますので，チェック後も大切に保管してください。
   あらかじめ情報化推進グループに提出し，保管を依頼することもできます。

ガイドライン見出し	ガイドライン小見出し	ガイドライン	No.	○は必須項目	チェック欄	チェック内容メモ欄	ガイド
4. クラウドサービス利用範囲の明確化 4.1.利用前の確認	(1)クラウドサービス利用基準	・クラウドサービス導入前に，どの業務をクラウドサービスに移行するのか事前によく検討しましょう。 ・情報セキュリティインシデント発生時の影響の大きさなどを踏まえて，提供されているクラウドの情報セキュリティの水準を勘案し，クラウドサービスを使い分けることが必要です。	1	×の場合は要相談		クラウド事業者名: クラウドサービス名: 保存する法人文書:	・広島大学クラアしていますか
	(2)業務の継続性の保証	・クラウド業者固有のサービスを使用する場合は，そのサービスの継続性とサービス契約終了時の代替手段の検討が必要です。	2				・クラウドサービを検討しましたか？
4.2.信頼性	(1)SLA	・利用する業務の重要性に応じたサービスの停止や性能低下によるサービス低下などの許容範囲の検討が必要です。 ・クラウドサービスが安定して提供されないと利用者の業務遂行に支障をきたす恐れがあるので，障害による停止時間や復旧時間の目安の確認が必要です。	3				・サービス停止た，その内容は



広島大学

クラウドサービス
利用ガイドライン

2013 年 3 月 15 日策定

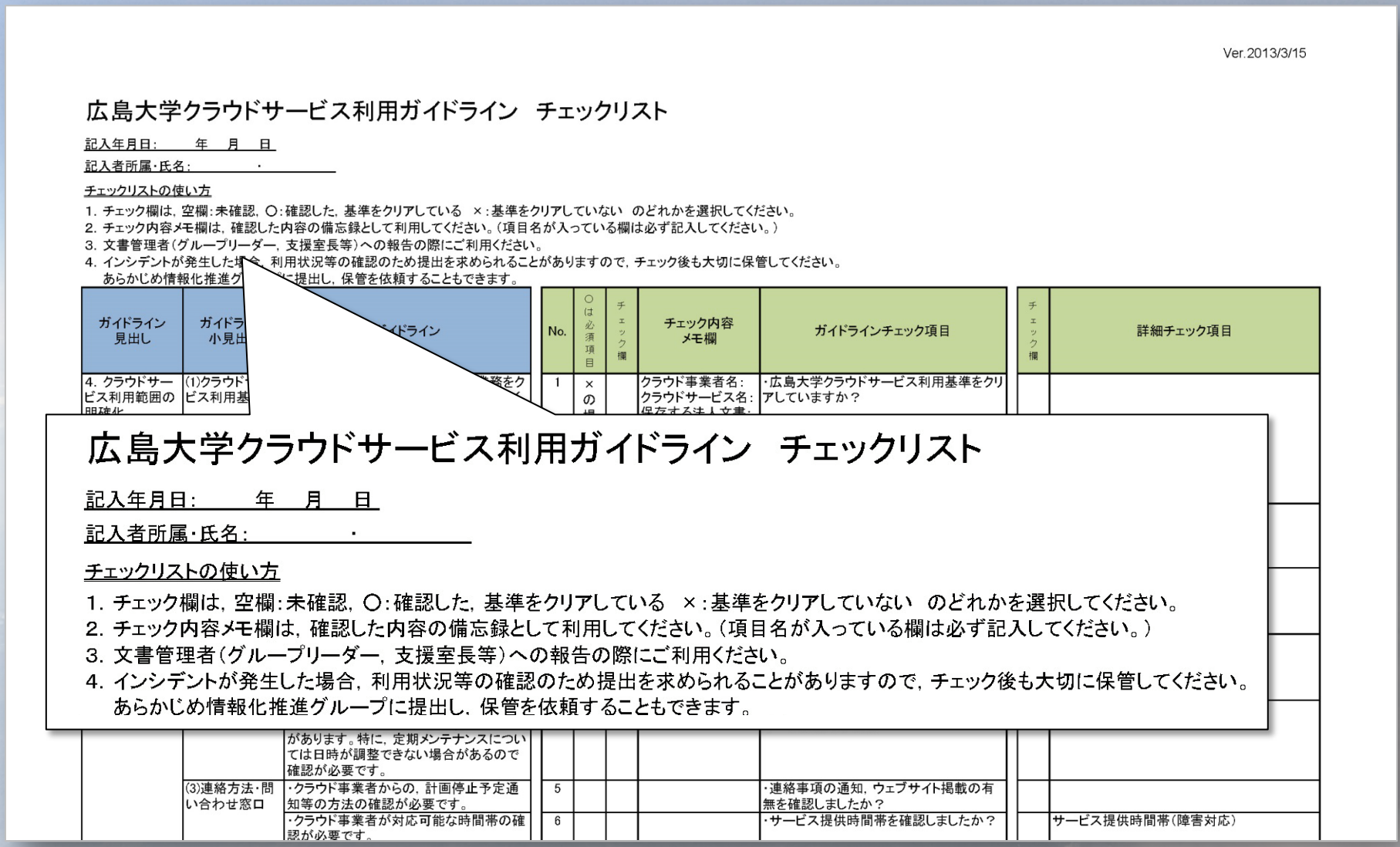
情報セキュリティ推進機構

- 第一版（2013（平成25）年3月15日策定）
- 45項目のチェックリスト
  - 利用開始前のチェックリストによる確認を推奨
  - インシデント発生時には、確認結果の提出が求められる場合がある

チェックリストの構成

- クラウドサービス利用範囲の明確化
  - 利用前の確認
    - クラウドサービス利用基準
    - 業務の継続性の保証
  - 信頼性
    - SLA
    - メンテナンス
    - 連絡方法・問合せ窓口
  - 機能
    - ネットワーク・通信
    - 管理ツール
    - ライセンス
    - スケーリング
  - コスト
    - 利用料
    - ネットワーク
    - ストレージ
  - データセンター
    - 物理的な対策
- 本学の組織・体制
  - クラウドサービス利用責任者
  - クラウドサービス利用担当者
- 本学の規則・契約
  - 本学の規則
  - 契約
- クラウド事業者の信頼性
  - クラウド事業者の選定
  - 第三者委託
- 契約条件の確認
  - 責任範囲の明確化
  - 契約条件の確認
  - クラウド事業者のペナルティ
  - 準拠法
  - 管轄裁判所
  - 所有権
  - データの確保
  - 契約終了時のデータの移行
  - 契約終了時のデータの消去
- サービスレベル
  - システムの運用に関する項目
    - セキュリティ対策
  - データ管理に関する項目
    - リソースの分離
    - アクセス制限
    - 暗号化
    - ログ
    - バックアップ
- 情報セキュリティインシデントの管理

チェックリストの使い方



Ver.2013/3/15

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

記入年月日:　　年　月　日

記入者所属・氏名:　　・

チェックリストの使い方

1. チェック欄は，空欄：未確認，〇：確認した，基準をクリアしている　×：基準をクリアしていない　のどれかを選択してください。
2. チェック内容メモ欄は，確認した内容の備忘録として利用してください。（項目名が入っている欄は必ず記入してください。）
3. 文書管理者（グループリーダー，支援室長等）への報告の際にご利用ください。
4. インシデントが発生した場合，利用状況等の確認のため提出を求められることがありますので，チェック後も大切に保管してください。
   あらかじめ情報化推進グループに提出し，保管を依頼することもできます。

ガイドライン見出し	ガイドライン小見出	ガイドライン	No.	○は必須項目	チェック欄	チェック内容メモ欄	ガイドラインチェック項目	チェック欄	詳細チェック項目
4. クラウドサービス利用範囲の明確化	(1)クラウドビス利用基	発をク	1	×		クラウド事業者名： クラウドサービス名： 保存する法人文書：	・広島大学クラウドサービス利用基準をクリアしていますか？		
		があります。特に，定期メンテナンスについては日時が調整できない場合があるので確認が必要です。							
	(3)連絡方法・問い合わせ窓口	・クラウド事業者からの，計画停止予定通知等の方法の確認が必要です。	5				・連絡事項の通知，ウェブサイト掲載の有無を確認しましたか？		
		・クラウド事業者が対応可能な時間帯の確認が必要です。	6				・サービス提供時間帯を確認しましたか？		サービス提供時間帯（障害対応）

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

記入年月日:　　年　月　日

記入者所属・氏名:　　・

チェックリストの使い方

1. チェック欄は，空欄：未確認，〇：確認した，基準をクリアしている　×：基準をクリアしていない　のどれかを選択してください。
2. チェック内容メモ欄は，確認した内容の備忘録として利用してください。（項目名が入っている欄は必ず記入してください。）
3. 文書管理者（グループリーダー，支援室長等）への報告の際にご利用ください。
4. インシデントが発生した場合，利用状況等の確認のため提出を求められることがありますので，チェック後も大切に保管してください。
   あらかじめ情報化推進グループに提出し，保管を依頼することもできます。

チェックリストの使い方（続き）

広島大学

○が付いている項目は特に重要なため、チェック結果が×の場合は文書管理者に相談する。

利用責任者や利用担当者の情報、その他チェック時に確認した事項等を記録する。

広島

記入年

記入者

チェック

1. チェ
2. チェ
3. 文書
4. インシデントが発生した場合，利用状況等の
あらかじめ情報化推進グループに提出し，保管を依

チェック後も大切に保管してください。

No.	○は必須項目	チェック欄	チェック内容メモ欄	ガイドラインチェック項目	チェック欄	詳細チェック項目
1	× の場合は要相談		クラウド事業者名: クラウドサービス名: 保存する法人文書:	・広島大学クラウドサービス利用基準をクリアしていますか？		
2				・クラウドサービス契約終了時の代替手段		
						監視体制
18	○		責任者所属: 責任者氏名:	・クラウドサービス利用について，本学の責任者が明確になっていますか？		
19	○		担当者所属: 担当者氏名:	・クラウドサービスの利用について，本学側の担当者を指名していますか？また，担当者は利用するクラウドサービスの特徴について理解していますか？		
20	○			・「法人文書管理規則」及び「個人情報の取扱いに関する規則」を確認しましたか？		
21	○			・文書管理者にクラウドサービスを利用することを報告しましたか？		

ガイドライン見出し	ガイドライン小見出し	ガイドライン
4. クラウドサービス利用範囲の明確化 4.1.利用前の確認	(1)クラウドサービス利用基準	・クラウドサービス導入前に，どの業務をクラウドサービスに移行するのか事前によく検討しましょう。 ・情報セキュリティインシデント発生時の影響の大きさなどを踏まえて，提供されているクラウドの情報セキュリティの水準を勘案し，クラウドサービスを使い分けることが必要です。
	(2)業務の継続性	・クラウド業者固有のサービスを使用する
5. 本学の組織・体制	(1)クラウドサービス利用責任者	・本学の責任者が不明だと，契約事項の確認や，インシデント発生時の対応が難しくなります。
	(2)クラウドサービス利用担当者	・クラウドサービス事業者との窓口となる担当者が必要です。 【業務内容　例】 (1) ユーザアカウントの登録や抹消の処理 (2) 利用マニュアルの整備・指導 (3) ヘルプデスク (4) クラウド事業者との連絡調整
6. 本学の規則・契約	(1)本学の規則	・法人文書は，「法人文書管理規則」及び「個人情報の取扱いに関する規則」に沿って取り扱う必要があります。
		・クラウドサービスを利用する情報は，クラウドサービス利用責任者から文書管理者（グループリーダー，支援室長等）に報告する必要があります。（平成25年4月の改

ガイドラインのこれから

広島大学

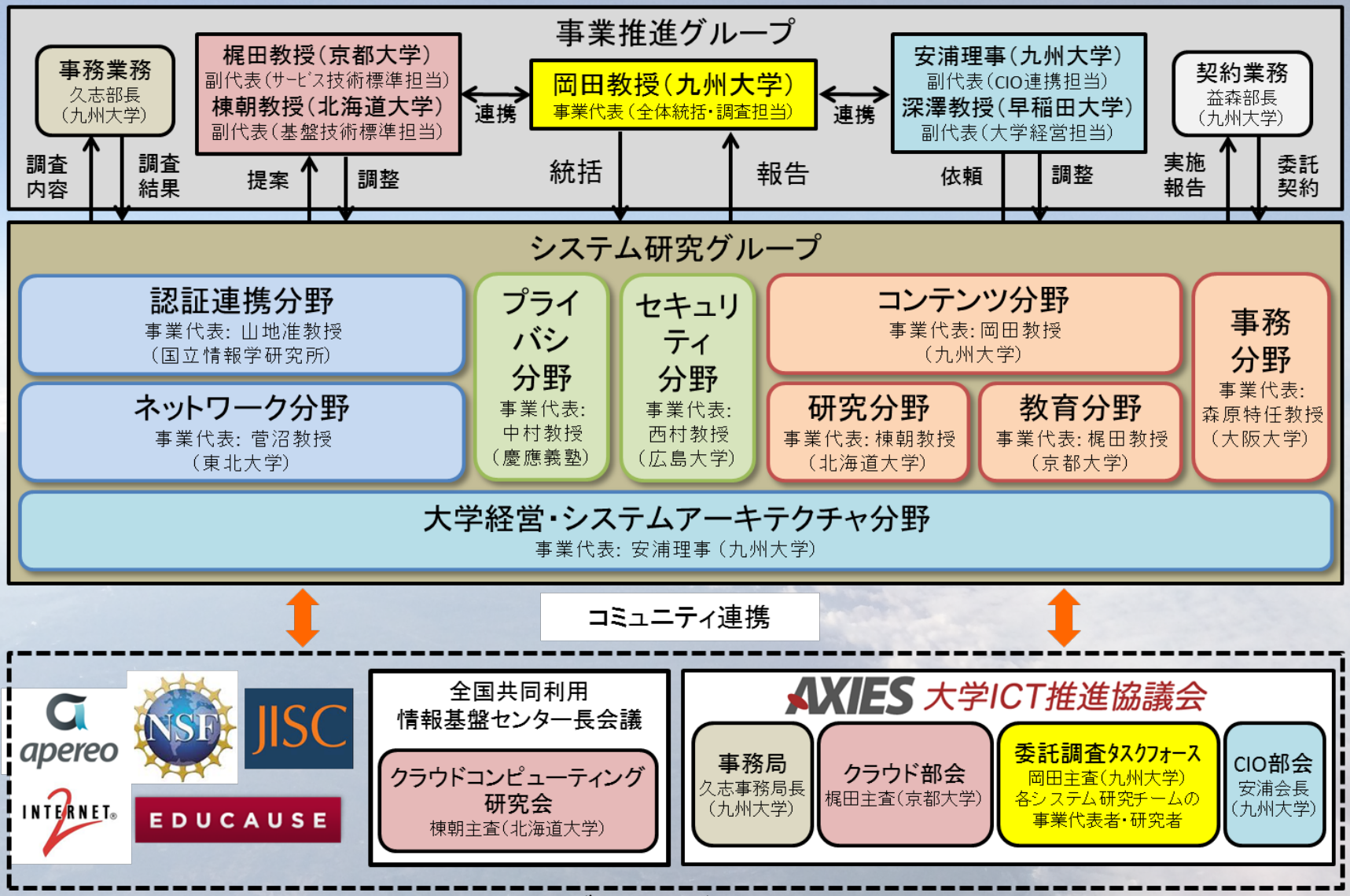
- 広島大学クラウドサービス利用ガイドライン
  - 平成25年3月15日策定
  - 定期的（1年程度）に見直し
    - チェック項目の見直し（サービスモデルにより異なるハズ）
    - 具体的なサービスでのチェック例の追加

- 以下の活動にメンバーとして参画し、フィードバックを得る
  - サイエンティフィック・システム研究会
    - 移行期にあるネットワークサービスのセキュリティWG
    - 中間まとめ「高等教育機関・研究機関のためのパブリッククラウド利用ガイド」［2013-09-27掲載］
      - http://www.ssken.gr.jp/MAINSITE/download/wg_report/net-sec/public_cloud/index.html
  - 平成25年度国家課題対応型研究開発推進事業
    「アカデミッククラウド環境構築に係るシステム研究」提案
    - 「コミュニティで紡ぐ次世代大学ICT環境としてのアカデミッククラウド」
      セキュリティ分野

    → アカデミックな組織がクラウドサービスを利用する際のガイドライン
  - 高等教育機関における情報セキュリティポリシー推進部会
    - 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

    → クラウドサービス利用に関するガイドライン

AC事業 実施体制


事業推進グループ
事務業務
久志部長
（九州大学）
梶田教授（京都大学）
副代表（サービス技術標準担当）
棟朝教授（北海道大学）
副代表（基盤技術標準担当）
連携
岡田教授（九州大学）
事業代表（全体統括・調査担当）
連携
安浦理事（九州大学）
副代表（CIO連携担当）
深澤教授（早稲田大学）
副代表（大学経営担当）
契約業務
益森部長
（九州大学）
調査内容
調査結果
提案
調整
統括
報告
依頼
調整
実施報告
委託契約
システム研究グループ
認証連携分野
事業代表：山地准教授
（国立情報学研究所）
ネットワーク分野
事業代表：菅沼教授
（東北大学）
プライバシ分野
事業代表：
中村教授
（慶應義塾）
セキュリティ分野
事業代表：
西村教授
（広島大学）
コンテンツ分野
事業代表：岡田教授
（九州大学）
研究分野
事業代表：棟朝教授
（北海道大学）
教育分野
事業代表：梶田教授
（京都大学）
事務分野
事業代表：
森原特任教授
（大阪大学）
大学経営・システムアーキテクチャ分野
事業代表：安浦理事（九州大学）
コミュニティ連携
apereo
NSF
JISC
INTERNET2
EDUCAUSE
全国共同利用
情報基盤センター長会議
クラウドコンピューティング
研究会
棟朝主査（北海道大学）
AXIES 大学ICT推進協議会
事務局
久志事務局長
（九州大学）
クラウド部会
梶田主査（京都大学）
委託調査タスクフォース
岡田主査（九州大学）
各システム研究チームの
事業代表者・研究者
CIO部会
安浦会長
（九州大学）

アンケート回答状況

広島大学

- 実施期間：平成25年10月16日（水）～平成25年11月29日（金）
- 連絡代表者登録機関数　　801機関/1230機関
  - ４年制大学　555機関(国立86(100%), 公立70(84%),私立399(66%))
  - 短大　　169機関(48%)
  - 高専　　52機関(91%)
  - 研究　　25機関(57%)
- 各アンケート回答状況
  - 教育支援分野（サービス部署向け）　593件
  - 教育支援分野（学部・研究科向け）　855件
  - 研究支援（情報サービス部署向け）　684件
  - 研究支援（個人向け）　2395件
  - 事務支援　1074件
  - 経営　496件
  - コンテンツ　496件
  - ICT　655件
  - ネットワーク　740件
  - セキュリティ　582件
  - 個人情報　594件

「セキュリティ分野」アンケート

広島大学

- 情報システムの運用に関する諸規則の整備状況
  - 整備の際に参考にした資料は何か？
- 情報の格付けに関する事項の整備状況
- 情報処理を外部委託する場合に関する事項の整備状況
- 諸規則を構成員に周知するための教育の実施状況
- 情報セキュリティマネジメントシステム(ISMS)認証の取得状況
- セキュリティインシデントの発生状況
- 機関によるクラウドサービスの利用状況
  - 利用しているクラウドサービス
  - 利用を決定する際の要件
  - 利用しない理由
- 構成員によるクラウドサービス利用状況
- アカデミッククラウドの利用予定
  - アカデミッククラウドに求める要件、期待、問題点

クラウドサービス利用の要件

広島大学

利用を決めた、あるいは利用を決める際の要件	国立大	公立大	私立大	短大	高専	研究機関	計
回答組織数	76	53	294	111	41	19	594
➢ 既存システムよりコストが安いこと	23	14	109	33	10	3	192
➢ どこでもサービスを利用できること	20	12	89	31	10	3	165
➢ 資産、保守体制を持つ必要がないこと	20	12	89	24	11	1	157
➢ 安定性、可用性が高くなること	33	9	82	26	6	1	157
➢ 初期導入コストが安価であること	21	11	88	25	5	3	153
➢ サービスの信頼性が高いこと	23	7	71	23	4	2	130
➢ 機器を選ばずに同様のサービスを利用できること	7	3	45	18	5	2	80
➢ 導入スピードが速いこと	10	2	36	12	1	1	62
➢ システムの拡張性（スケーラビリティ）が高いこと	9	3	27	14	2	0	55
➢ 情報漏洩等に対するセキュリティが高くなること	8	5	17	12	0	1	43
➢ システムの構成変更に迅速に対応できること	8	4	15	9	0	1	37
➢ ライセンス管理が楽であること	5	4	21	7	0	0	37
➢ いつでも利用停止できること	5	0	17	6	0	1	29
➢ 所属機関の諸規則を満たしていること	7	2	11	4	1	2	27
➢ サービスのラインアップが充実していること	6	1	11	5	0	2	25
➢ システムベンダーに提案されたから	2	0	9	4	1	0	16
➢ ISMS認証等を取得していること	0	1	1	0	0	1	3
➢ その他	6	1	4	2	1	1	15

クラウドサービスを利用しない理由

広島大学

パブリッククラウドサービスを利用しない、あるいは利用を妨げている理由	国立大	公立大	私立大	短大	高専	研究機関	計
回答組織数	76	53	294	111	41	19	594
➢ 情報漏洩などセキュリティに不安がある	39	25	152	47	23	6	292
➢ クラウドの導入に伴う既存システムの改修コストが大きい	14	10	59	21	8	1	113
➢ ニーズに応じたアプリケーションのカスタマイズができない	17	9	63	15	8	1	113
➢ ネットワークの安定性に対する不安がある	13	6	58	20	8	1	106
➢ 法制度や所属機関の諸規則が整っていない	24	11	48	9	6	2	100
➢ メリットが分からない、判断できない	6	8	46	21	10	4	95
➢ 通信費用がかさむ	5	4	37	5	6	1	58
➢ クラウドの導入によって所属機関の諸規則との整合性に支障をきたす	13	4	27	3	4	2	53
➢ 必要がない	3	4	23	14	3	2	49
➢ その他	12	6	21	6	2	2	49

学術機関と企業との意識の違い

広島大学

パブリッククラウドサービスを利用しない、あるいは利用を妨げている理由	学術研究機関 (n=594)	企業 (n=722)
情報漏洩などセキュリティに不安がある	49.2	34.0
クラウドの導入に伴う既存システムの改修コストが大きい	19.0	22.6
ニーズに応じたアプリケーションのカスタマイズができない	19.0	12.8
ネットワークの安定性に対する不安がある	17.8	15.2
法制度や所属機関の諸規則が整っていない	16.8	6.3
メリットが分からない、判断できない	16.0	21.5
通信費用がかさむ	9.8	10.9
クラウドの導入によって所属機関の諸規則との整合性に支障をきたす	8.9	6.2
必要がない	8.2	41.2
その他	8.2	5.8

（出展）：総務省「平成24年通信利用動向調査（企業編）」
http://www.soumu.go.jp/johotsusintokei/statistics/statistics05.html

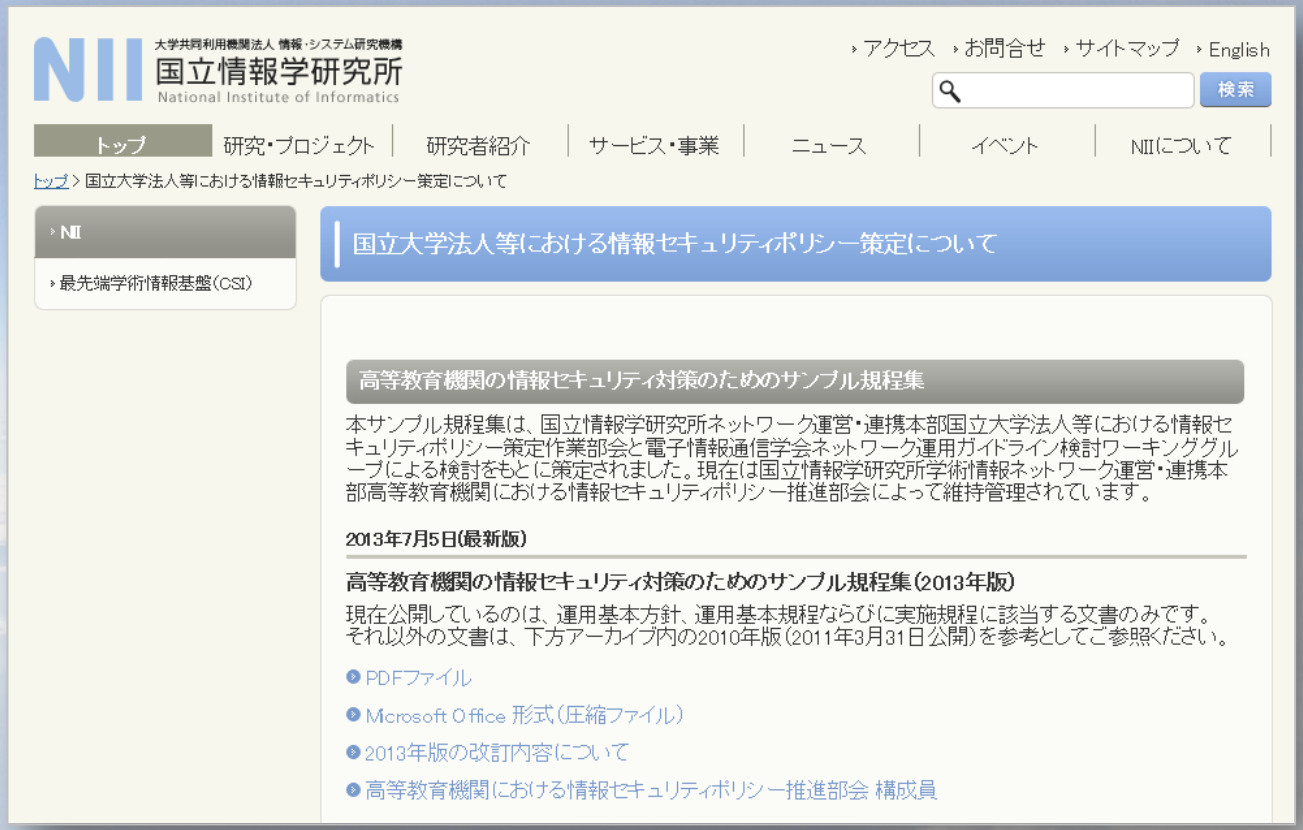
AC事業の今後は？

- 「セキュリティ分野」の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、ほとんどが「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
- アンケートの詳細や他分野の話題については「**最終報告会**」で
  - 日時：平成26年2月13日（木）10:00～16:20
  - 場所：学術総合センター2Ｆ　中会議室1～4
    （東京都千代田区一ツ橋2-1-2）
  - 参加費：無料（定員200名）
  - 対象者：大学関係機関の教職員 / 学術情報基盤を整備するITベンダー
  - 参加申込み、お問合せは
    http://www.icer.kyushu-u.ac.jp/topics_ac_20140213

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定集

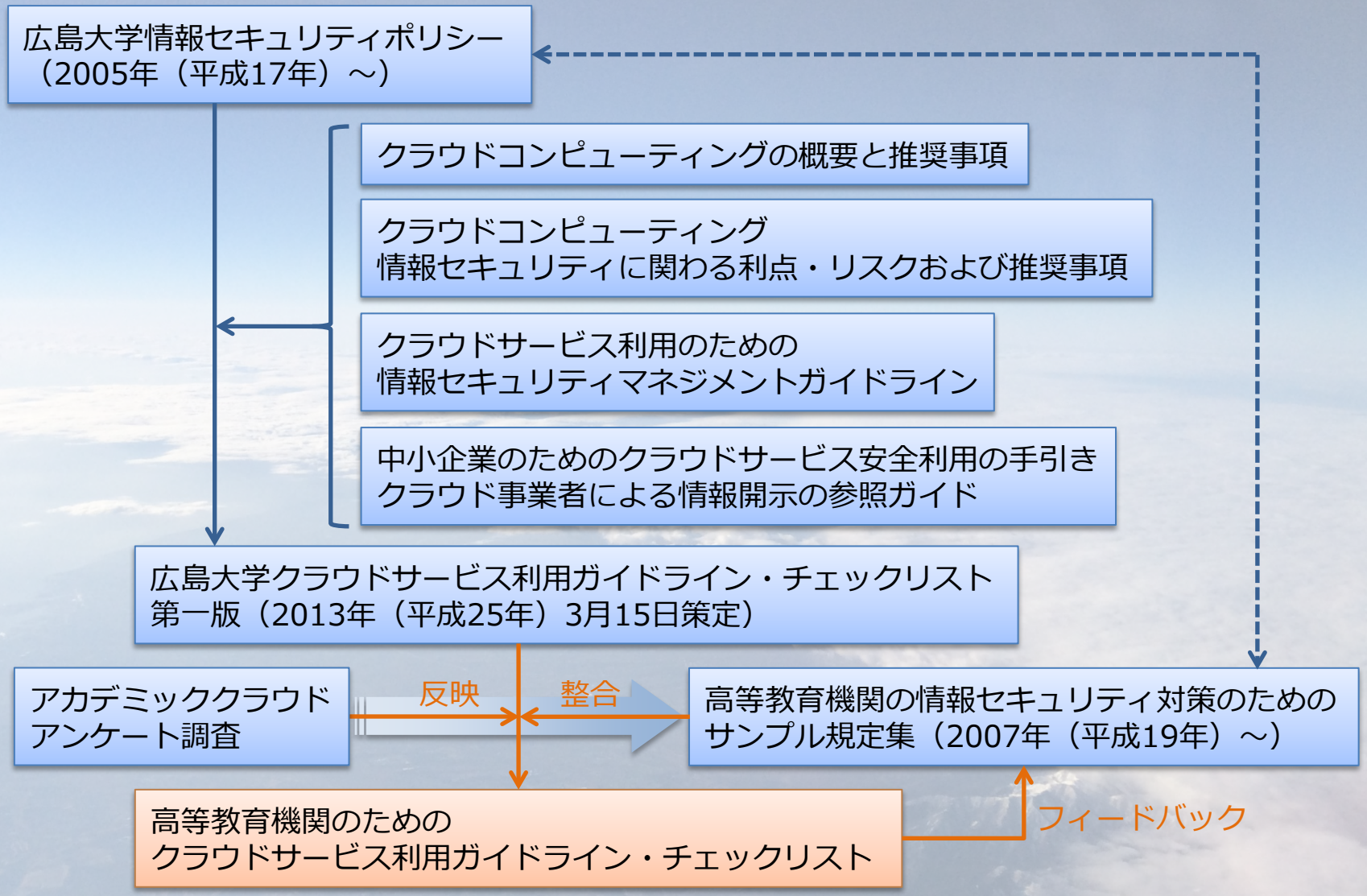
広島大学



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

- 「B2104 情報格付け基準」との対応を検討
  - 機密性3段階、完全性2段階、可用性2段階 → 重要度4段階程度に集約
- サンプル規程集に合わせた文言・表現の採用 → 関連文書化

ロードマップ


広島大学情報セキュリティポリシー
（2005年（平成17年）～）
クラウドコンピューティングの概要と推奨事項
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
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
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
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
第一版（2013年（平成25年）3月15日策定）
アカデミッククラウド
アンケート調査
反映
整合
高等教育機関の情報セキュリティ対策のための
サンプル規定集（2007年（平成19年）～）
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
フィードバック

まとめ

- 広島大学クラウドサービス利用ガイドライン
  - 整備の背景と検討の概要
  - 整備の方針（位置付け、考え方）
  - チェックリストの構成と使い方
- 今後の展開
  - 各種活動への参画→フィードバック
    - サイエンティフィック・システム研究会
      - 中間まとめ「高等教育機関・研究機関のためのパブリッククラウド利用ガイド」
    - 「コミュニティで紡ぐ次世代大学ICT環境としてのアカデミッククラウド」事業
      - 最終報告会（平成26年2月13日（水）@NII）
      - 最終報告書（平成25年度末）
    - 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
      - クラウドサービス利用に関するガイドライン
  - ロードマップ

イベント告知

広島大学

- 「コミュニティで紡ぐ次世代大学ICT環境としてのアカデミッククラウド」最終報告会
  日時：**平成26年2月13日（木）10:00～16:20**
  場所：学術総合センター2Ｆ　中会議室1～4
  （東京都千代田区一ツ橋2-1-2）
  参加費：無料（定員200名）
  対象者：大学関係機関の教職員 / 学術情報基盤を整備するITベンダー
  参加申込み、お問合せは
  http://www.icer.kyushu-u.ac.jp/topics_ac_20140213

- 大学等におけるクラウドサービス利用シンポジウム（仮）
  主催：広島大学情報メディア教育研究センター
  日時：**平成26年3月31日（月）13:30～17:00**
  場所：広島大学情報メディア教育研究センター本館2階セミナー室
  （広島県東広島市鏡山1-4-2）
  参加費：無料（事前申込みが必要）※テレビ会議・Ustreamによる参加も検討中
  参加申込み：2月下旬頃開設予定
  内容（予定）：
  アカデミッククラウド標準仕様紹介
  SINET4によるクラウド直結サービス紹介
  クラウド事業者によるサービス紹介（複数社）
  広島大学におけるクラウドサービス利用の紹介