

大学における 情報セキュリティインシデントの 現状と対策、そして今後

西村 浩二

広島大学 情報メディア教育研究センター

CAUAシンポジウム2014

2014年11月14日

広島大学の概要



- キャンパス、遠隔地区・施設、県外・海外オフィス
 - 東広島 (1) ・ 霞 (2) ・ 東千田 (3) キャンパス
 - 遠隔地区 (4) ~ (18)
 - 県外オフィス (東京、大阪、福岡)
 - 海外オフィス (中国、ロシア、ケニア、ブラジル、ベトナム、インドネシア)
- 部局等
 - 11学部、1専攻科、11研究科
 - 1附置研究所、1全国共同利用施設、1中国・四国地区国立大学共同利用施設、22学内共同教育研究施設等
 - 5図書館、4博物館等、大学病院 (診療科: 32医科、13歯科)
- 構成員数18,936名 (平成26年5月1日現在)
 - 学生15,216名, 役員8名, 教員1,695名, 職員1,621名



広島大学における 情報セキュリティに対する取り組み

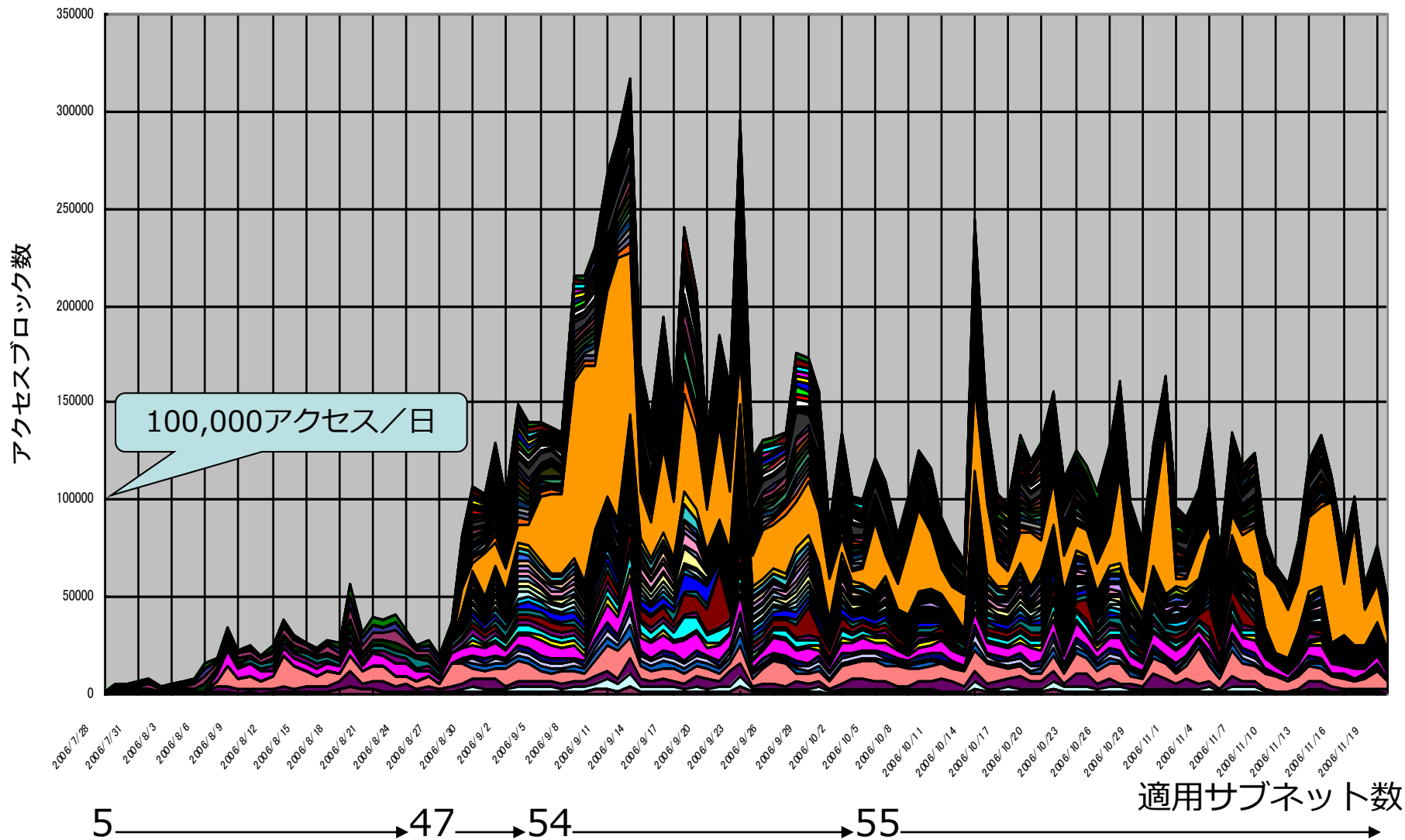
情報セキュリティに対する取り組み (1)

- 2004年度 (平成16年度)
 - ウイルス対策ソフトの全学的導入 (2005年3月～)
 - 教職員、学生が常用するパソコンへのインストールを推奨
- 2005年度 (平成17年度)
 - 情報セキュリティポリシーの制定 (4月1日)
 - 「基本方針」「対策基準」の施行
 - ホスティングサービスの提供 (5月～)
 - 部局運用サーバ (Web、メール、DNS) の移行を推奨
 - 情報セキュリティに関する組織体制の整備
 - 全学的な情報セキュリティ委員会の設置
 - 最高情報セキュリティ責任者、部局等情報セキュリティ責任者、情報セキュリティ推進機構の設置
 - 情報セキュリティ教育の実施
 - 学部1年生全員を対象にオンライン講座を提供、教職員は順次実施
 - 管理者向け研修会 (11月～)
- 2006年度 (平成18年度)
 - 「実施手順」「危機管理マニュアル」策定 (4月1日)
 - 「広島大学情報セキュリティに関する規則」制定 (4月18日)
 - 一般向けセキュリティ研修会 (4月～)
 - 全学ファイアウォール導入説明会 (6月14,16日)
- 2007年度 (平成19年度)
 - 学内基幹ネットワークHINET2007更新 (利用者認証機能、ゾーニング、ファイアウォール導入などセキュリティを大幅に強化)
 - IMCアカウント年度更新受付開始 (2008年1月～)
- 2008年度 (平成20年度)
 - IMCアカウント年度 (~5月)
 - 未更新アカウントはロック
 - HINET2007への移行 (2008年5月～2009年3月)
- 2009年度 (平成21年度)
 - 全構成員にICカード身分証を配布
 - 生協電子マネー機能付き

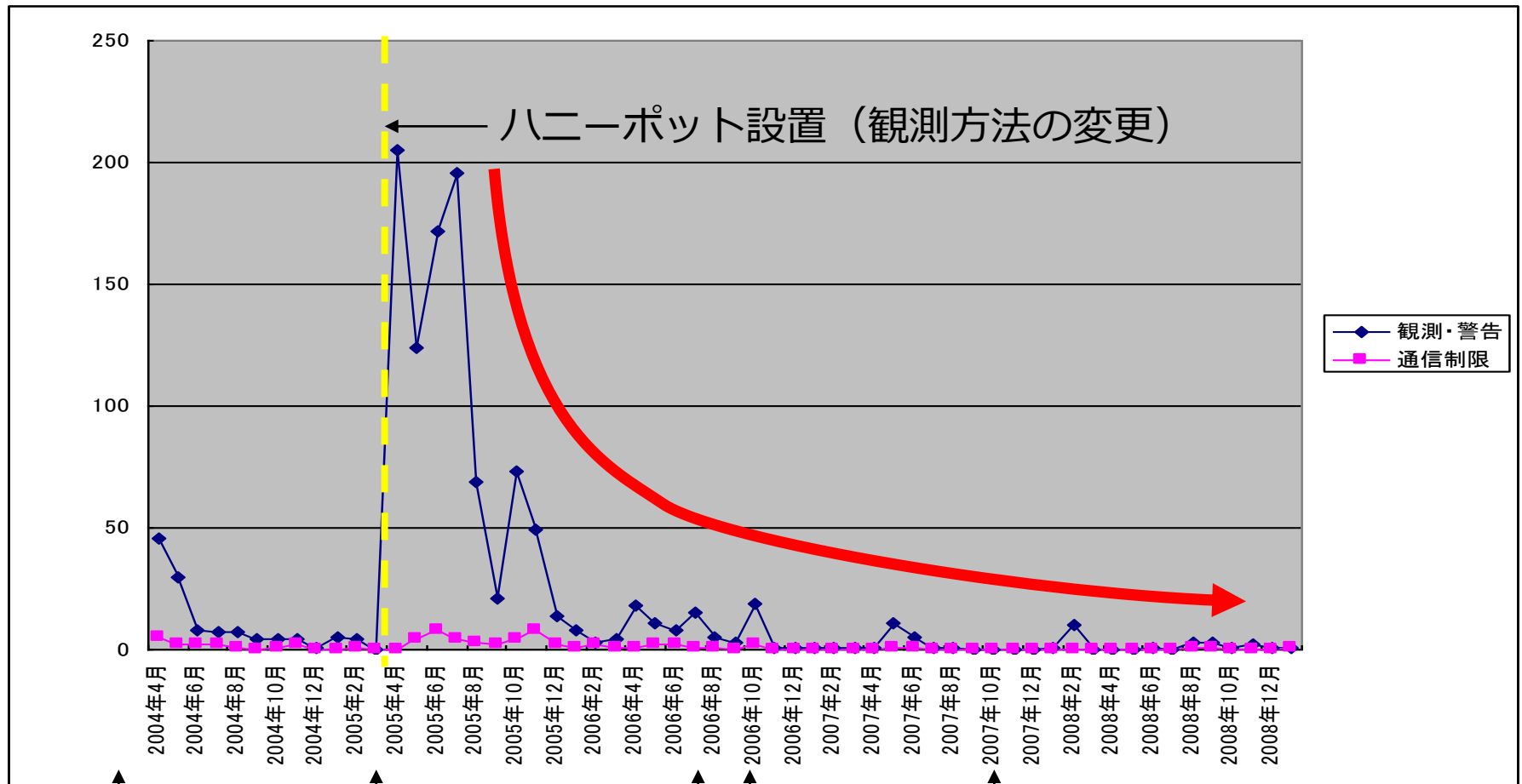
情報セキュリティに対する取り組み (2)

- 2010年度 (平成22年度)
 - マイクロソフト包括ライセンスを全構成員へ提供 (5月～)
 - セキュアUSBメモリの全常勤教員への配布 (6月～2013年10月)
 - 電子計算機システム稼働 (9月～)
 - ICカード認証 (教育用情報端末) ・ 決裁 (オンデマンドプリント)
- 2011年度 (平成23年度)
 - 情報セキュリティ・コンプライアンス (法令順守) 教育・講習の実施
 - 新入生 (学部・大学院の学生、非正規生) を対象にフレッシュマン講習 (座学+オンライン講座) を開講
 - 過年度生を対象にフォローアップ講習 (オンライン講座) を開講
 - 日本語版のほか、英語版、中国語版の資料・講習も提供
 - 終了テストで基準点以上の得点を義務付け (IMCアカウント年度更新の必要条件化)
 - セキュアUSBメモリの追加配布
- 2012年度 (平成24年度)
 - 情報セキュリティ・コンプライアンス教育 (2年目)
- 2013年度 (平成25年度)
 - 情報セキュリティ・コンプライアンス教育 (3年目)
 - フォローアップ講習の充実 (自己点検の追加 (任意))
 - 広島大学構成員におけるソーシャルメディアガイドライン策定 (9月5日)
- 2014年度 (平成26年度)
 - 情報セキュリティ・コンプライアンス教育 (4年目)
 - フォローアップ講習の充実 (自己点検の必須化)
 - 次期電子計算機システム仕様策定 (5月～)
 - HINET2014稼働 (8月～)
 - VPN機能強化

全学ファイアウォールでのブロック数 (一部)



セキュリティ対策の効果



ウイルスチェック
アクセス制限
脆弱性診断

2014年11月14日

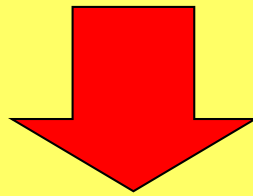
ウイルス対策ソフト

迷惑メール振分・削除
全学ファイアウォール

CAUAシンポジウム2014

大学のネットワークに求められるもの

- 高度で柔軟なキャンパスネットワーク
 - 学部、学科、研究室等の単位でサブネット構築
 - 目的に応じて比較的自由的な運用



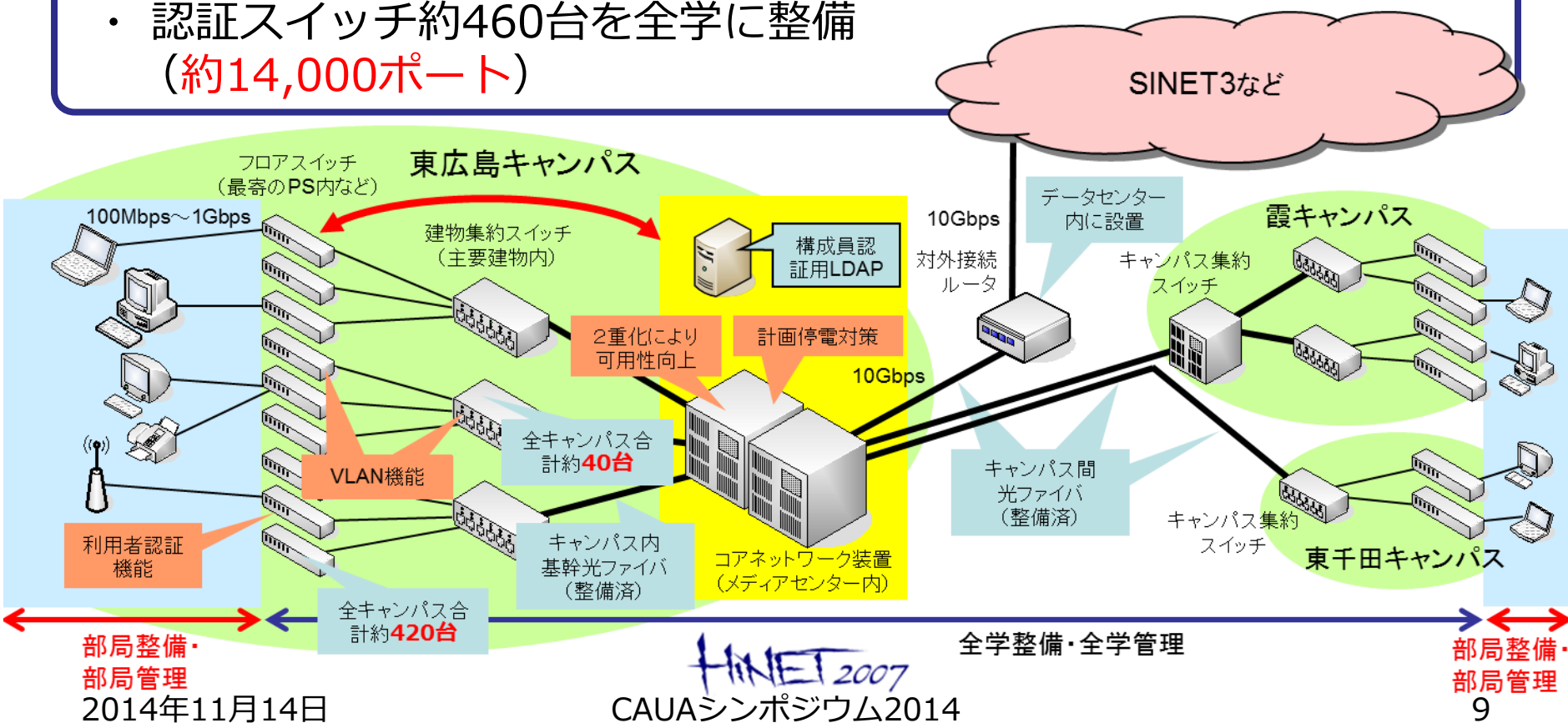
ネットワークのライフライン化
セキュリティインシデントの多発

- 管理方針の根本的な見直し
 - 研究室は独立した企業体（教員は社長）
 - しかし、外部からは同一組織とみなされる
 - さらに、経営（運用）の効率化を求められる

→ HINET2007

HINET2007の概要 (導入当時)

- 2008年5月から本格移行開始、2009年3月末完全移行
- 規模：主要3キャンパス（東広島、霞、東千田）、附属学校、小規模遠隔部局（東京，福山，尾道，竹原，呉，宮島）
- 教員約1,800人、職員約3,300人、学生15,000人
- 認証スイッチ約460台を全学に整備
(約14,000ポート)



部局整備・
部局管理
2014年11月14日

HINET2007
CAUAシンポジウム2014

全学整備・全学管理

部局整備・
部局管理
9

HINET2007の特徴

- 全学的な一元管理体制
 - ボランティアベースによるサブネット管理体制の破綻
 - 各フロアに設置するスイッチまで全学で一元管理
 - 登録システム（2008年12月～） / 申請システム（2012年9月～）
- すべての接続場所において利用者認証を要求
 - 多様な機器に対応するためWeb/MACアドレス認証を採用
 - 認証後はワイヤレートでの通信が必要
 - 利用者認証機構開発の歴史（1999年から研究（PortGuard）→製品化（FEREC）→オープンスペース・無線LANでの運用）
- 個別ファイアウォール機能の提供
 - 全学ファイアウォール（対学外）のみでは不十分
 - ブロードバンドルータ相当の機能を教員数程度（約2,000個）提供
 - キャンパスネットワークの新しいカタチの提案
- VLANによる柔軟な仮想配線の提供
 - 同一研究室（グループ）が異なる建物等に分散する場合に対応
 - 学外向けサーバの設置、JGN2plusなどの利用に対応
 - 人海戦術（5名の教員が交代で申請を受付、設定は業者に外部委託）

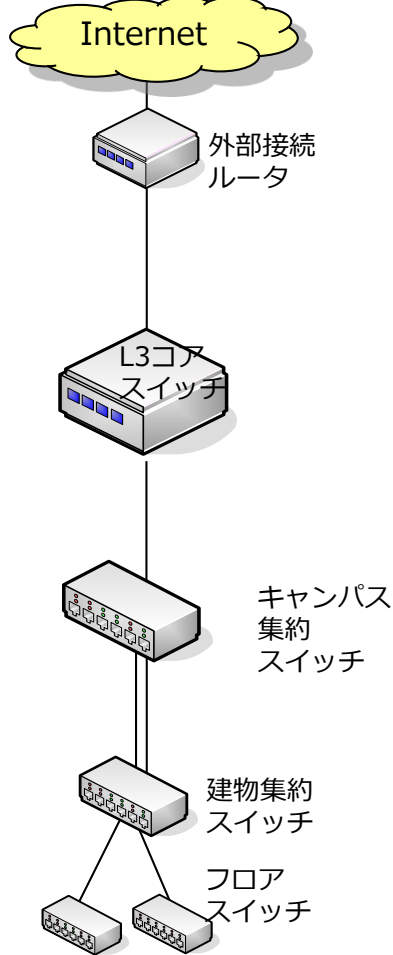
「ゾーン」の導入

ゾーン名 略称	グローバルゾーン ゾーンA	ファイアウォール ゾーン ゾーンB	ローカルゾーン ゾーンC	公衆ゾーン ゾーンD
主な用途	学外向けサーバ接続	学内共有サーバ接続	一般クライアント接続	オープンスペース
外部IPアドレス	グローバル 固定割当	グローバル 固定割当	グローバル 固定割当	グローバル DHCP割当
内部IPアドレス	外部IPアドレスと同じ	外部IPアドレスと同じ	プライベート (NAPT) DHCPまたは固定割当	外部IPアドレスと同じ
ゾーン外からの アクセス	学内外とも制限なし	学外から不可 ゾーンAを除く 学内から可	同一ローカルゾーン以外 から不可	学外から不可 ゾーンAを除く 学内から可
学外への アクセス	制限なし	制限なし	原則制限なし (NAPTによる 制限あり)	制限なし
端末認証	MACアドレス認証	MACアドレス認証	Web認証または MACアドレス認証	Web認証

これまでのサブネット構成とは異なる

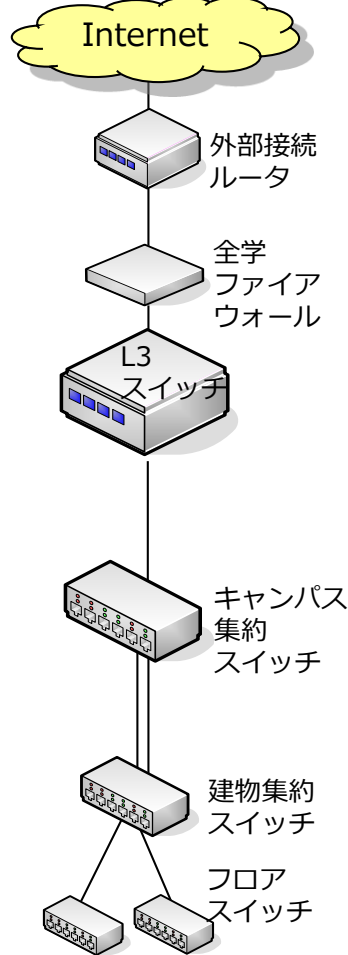
HINET2007 各ゾーンの論理構成

グローバルゾーン ゾーン A



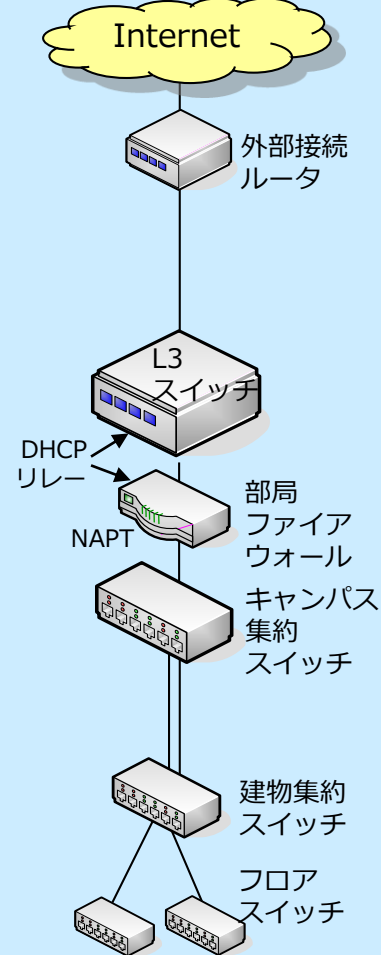
MAC認証

ファイアウォールゾーン ゾーン B



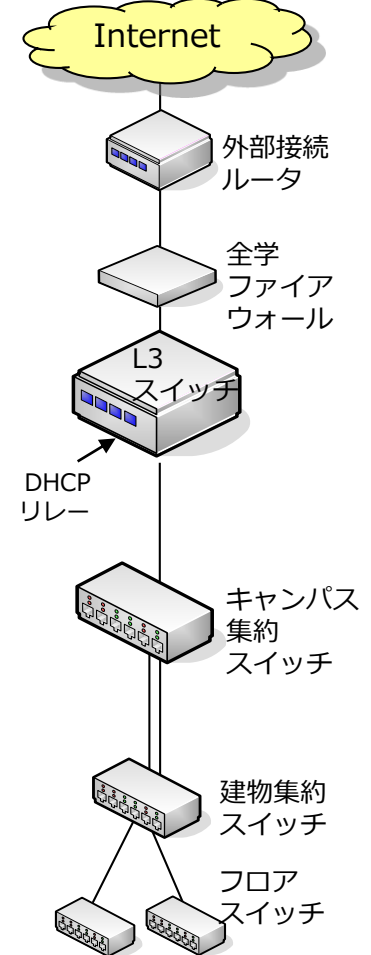
MAC認証

ローカルゾーン ゾーン C



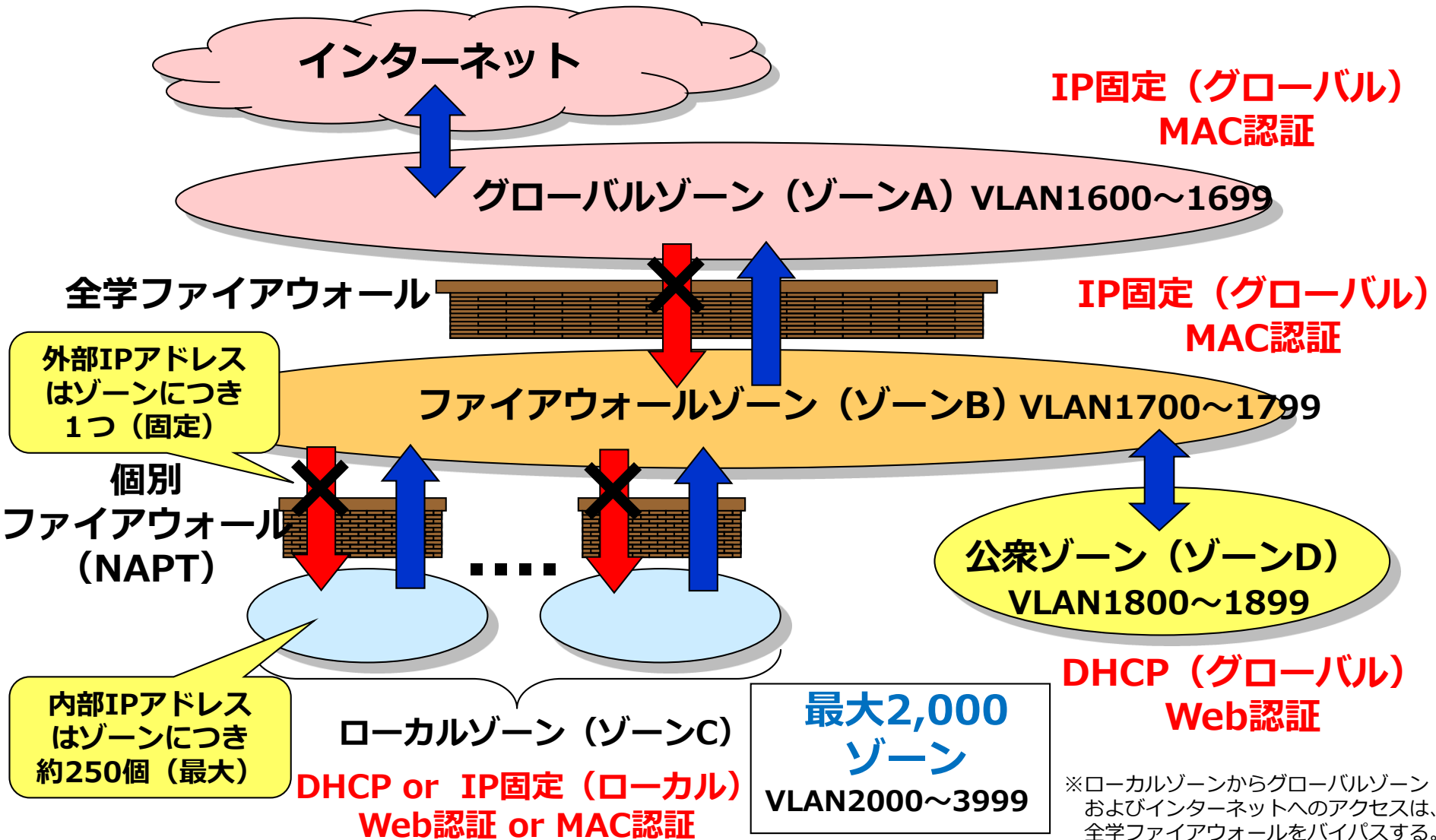
Web認証またはMAC認証

公衆ゾーン ゾーン D

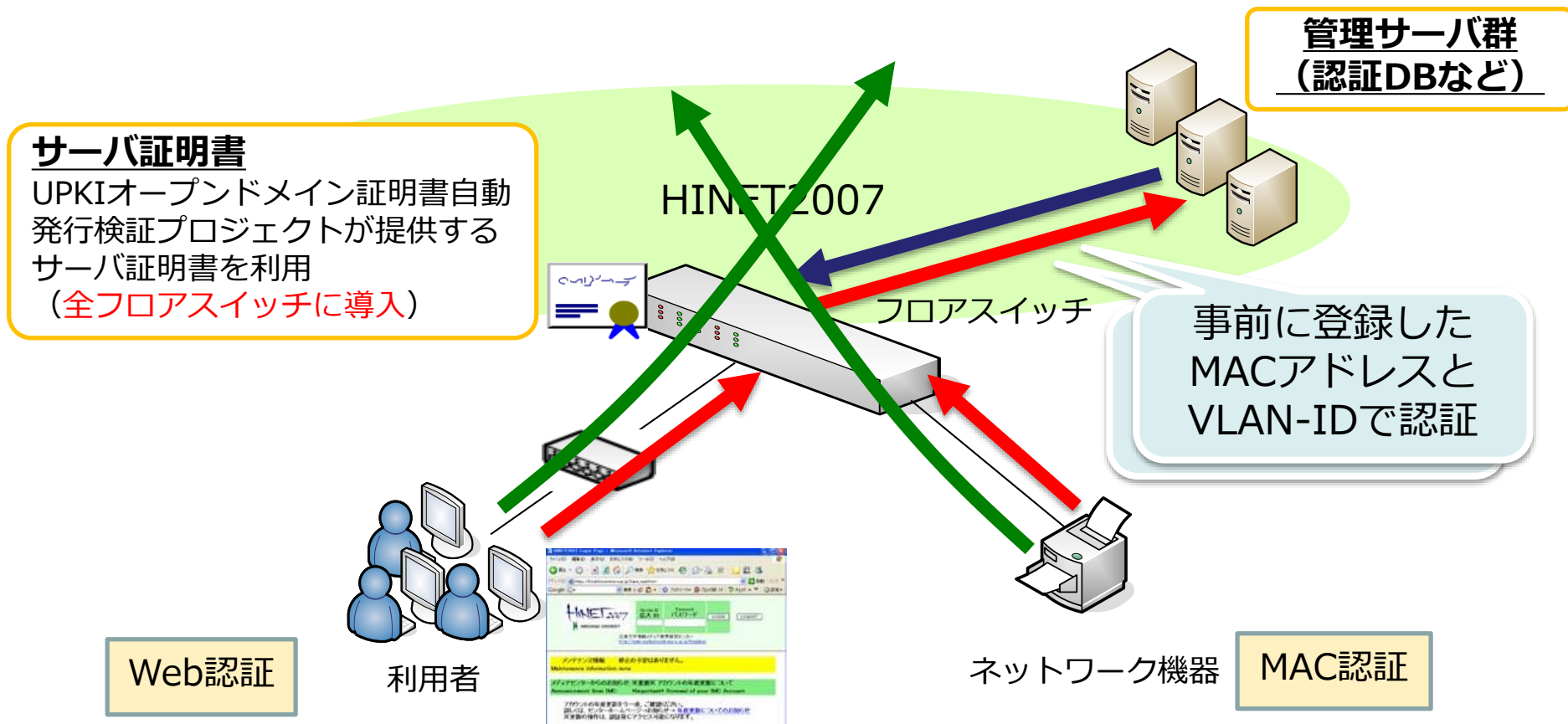


Web認証

ゾーン種別とアクセス制限



利用者認証の概要



httpsによる利用者認証
 初回接続時に認証ページをリダイレクト表示
 全学電子情報基盤で管理するIDを利用
 ARPポーリング/リンクダウンによるログアウト

MACアドレスは事前登録 (登録システムを利用)
 Web認証が困難な機器を対象 (プリンタ, NAS等)

教育用情報端末へのログイン (二要素認証)



電源 ON!



OSを選択

Linuxの場合



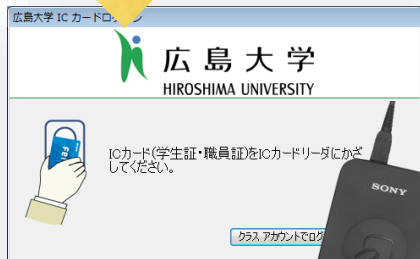
学生証をかざす
取り忘れに注意!



表示されたユーザ名を確認し、
対応するパスワードを入力



使い終わったら
シャットダウン!



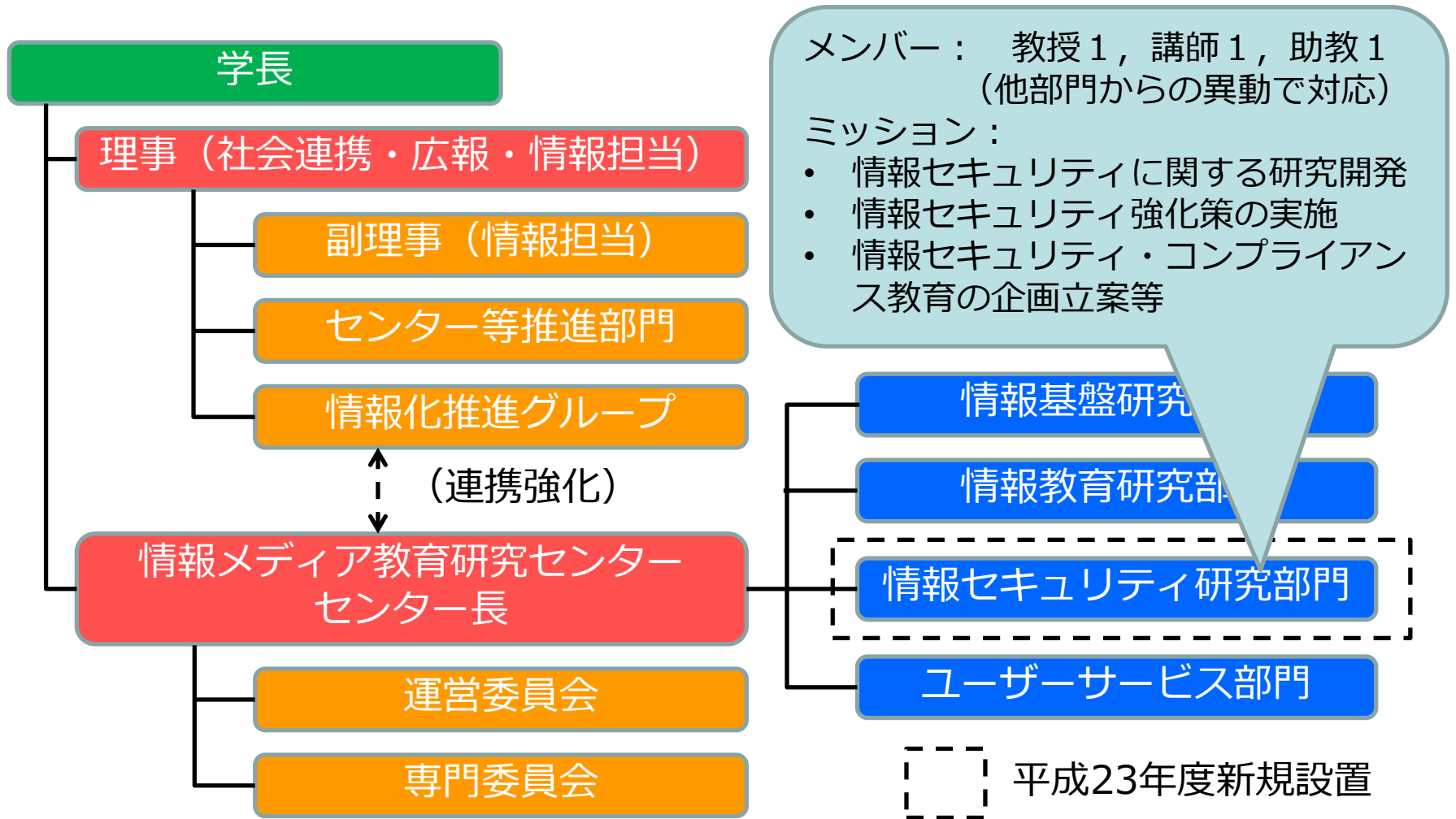
Windowsの場合



さらに新たな取り組みへ

- 情報セキュリティインシデント対応
 - 文部科学省や著作権等権利者団体等からの要請
 - 広島大学中期計画
 - 第一期（平成16～21年度）
 - 情報セキュリティポリシーの制定
 - 情報セキュリティ対策および教育の実施
 - 第二期（平成22～27年度）
 - 全構成員向け情報倫理・セキュリティ教育の充実
 - 情報セキュリティに対する取り組み
 - 情報セキュリティに関する規程等の整備
 - 情報環境の整備・充実
 - 広報等による啓発活動
- 構成員の意識や行動を根本的に変化させる必要性
- 情報セキュリティ教育の必須化

情報環境ガバナンス体制の(再)構築



情報セキュリティ・コンプライアンス教育

- 平成23年度より全学的に実施
 - 情報セキュリティの維持・違法行為の防止
 - 広島大学の学生として持つべき倫理観の醸成
- フレッシュマン講習
 - 在籍1年目の学生
 - 学部1年次生、大学院博士課程前期・後期1年次生、編入学生、研究生、科目等履修生等
 - 旧学生番号を持っている（過去に在籍記録がある）者を除く
 - 座学＋オンライン講座＋終了テスト
- フォローアップ講習
 - 在籍2年目以降の学生および全教職員（平成24年度～）
 - 自己点検（平成25年度～）＋オンライン講座＋確認テスト
 - 年度初めのアカウント年度更新に合わせて実施

情報セキュリティ・コンプライアンス教育

- 平成23年度より全学的に実施
 - 情報セキュリティの維持・違法行為の防止
 - 広島大学の学生として持つべき倫理観の醸成
- フレッシュマン講習
 - 在籍1年目の学生
 - 学部1年次生、大学院博士課程前期・後期1年次生、編入学生、研究生、科目等履修生等
 - 旧学生番号を持っている（過去に在籍記録がある）者を除く
 - 座学＋オンライン講座＋終了テスト
- フォローアップ講習
 - 在籍2年目以降の学生および全教職員（平成24年度～）
 - 自己点検（平成25年度～）＋オンライン講座＋確認テスト
 - 年度初めのアカウント年度更新に合わせて実施

フレッシュマン講習の対象者

対象者		座学 (授業)	座学 (講習)	オンライン 講座
学部1年次生	前期に開講する教養教育（情報科目）を履修する学生	情報科目	—	○
	後期に開講する教養教育（情報科目）を履修する学生	—	○	○
	教養教育（情報科目）を履修しない学生	—	○	○
	経済学部、経済学部夜間主コースの学生	教養ゼミ	—	○
大学院M1年次生	他大学から進学した学生	—	○	○
大学院D1年次生	本学から進学した学生	—	—	○
編入生		—	○	○
非正規生（研究生、科目等履修生、日本語研修コース研修生）		—	○	○
法務研修生		—	—	○

- 平成25年度対象者：

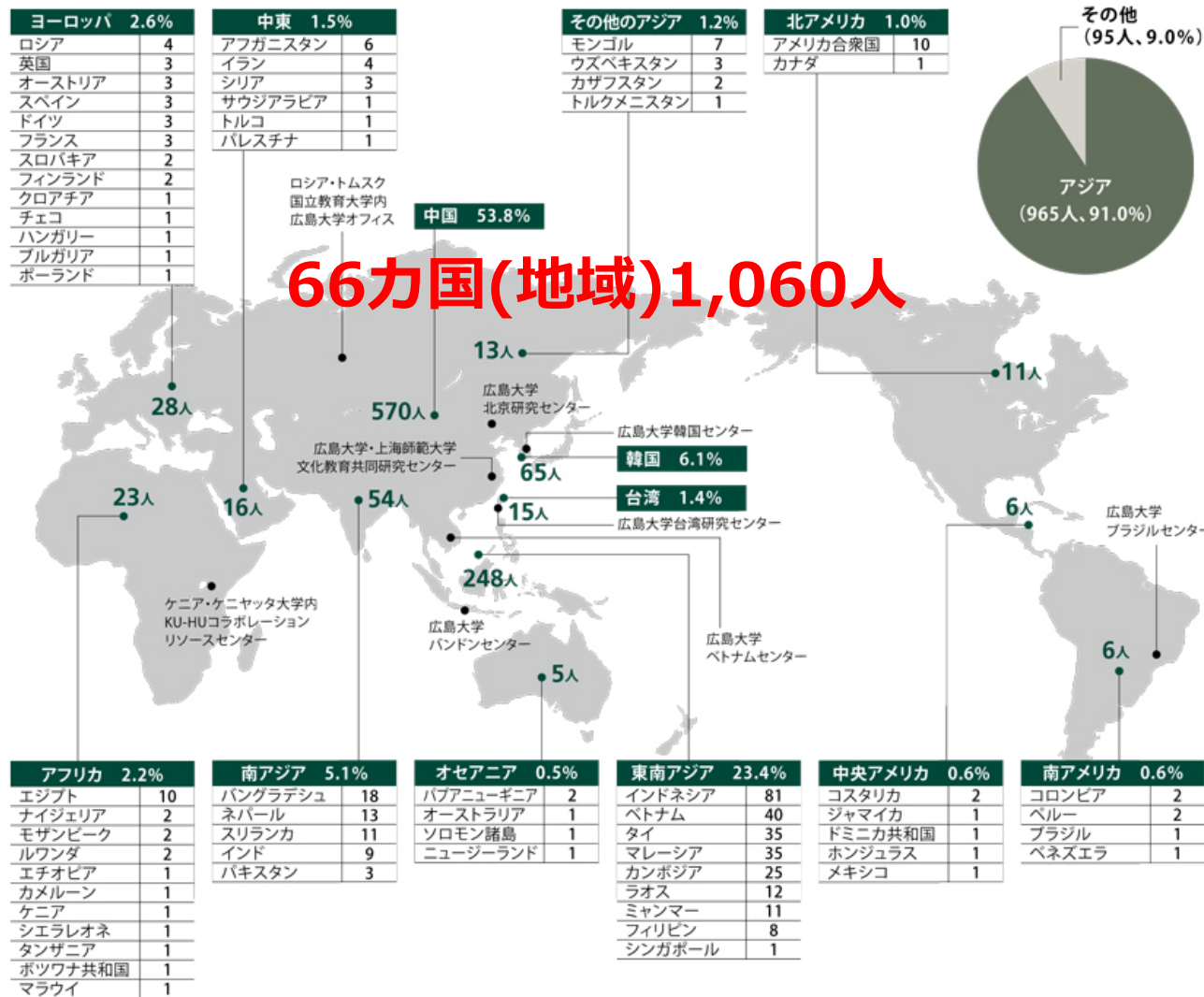
- 座学：3,350名
（前期 3,008名、後期 342名）
- オンライン講座：4,559名
（前期 4,133名、後期 426名）

- 平成26年度対象者：

- 座学：2,984名
（前期末時点）
- オンライン講座：4,141名
（前期末時点）

国(地域)別外国人留学生数(平成26年5月1日現在)

◆ 国(地域)別外国人留学生数 (66カ国(地域)1,060人)



外国人留学生の活用

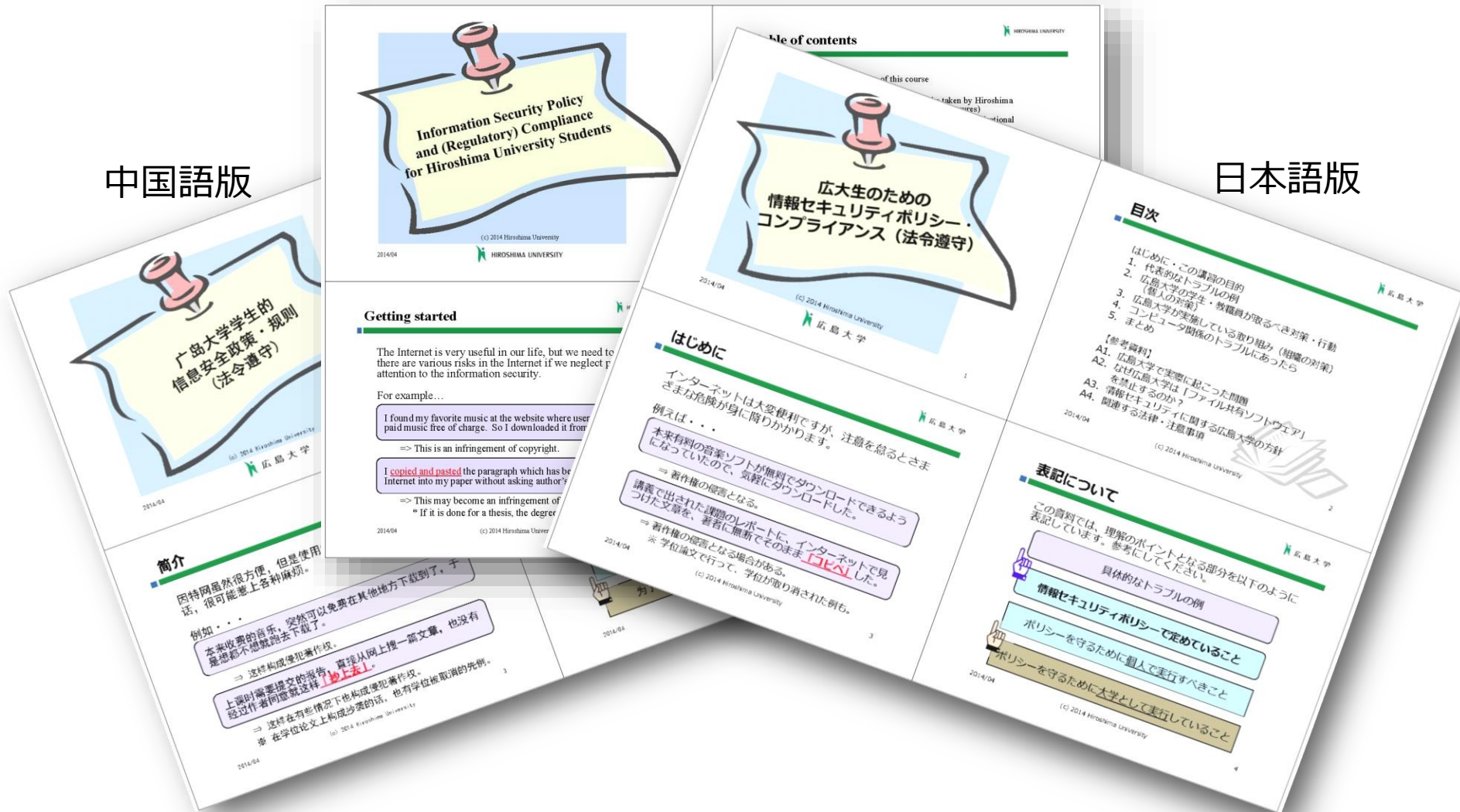
- 学生アルバイト
 - 2名1組で、半期ごとに1名を交代（最初の半期はサポート役）
 - 採用時の面接で、日本語での意思疎通と情報系の知識を確認
 - 資料（座学・オンライン講座）の翻訳と講習会での通訳を担当
- 資料（座学・オンライン講座）の翻訳
 - 日本語版をベースに英語版・中国語版を作成
 - 日本語版・英語版は担当教員が作成
 - 中国語版は学生アルバイトが翻訳
 - 講師用資料には、話す（べき）内容をノートに記述（翻訳）
 - 複数教員で担当する際の「質」を保つ
 - 教職員はダウンロード可（それぞれの部局や研究室等で使用できる）
- 講習会での通訳
 - 日本語・英語は担当教員が実施
 - 英語の回は日本語と英語の両方で解説
 - 中国語は学生アルバイトが逐次通訳
 - ノートの内容を担当教員が日本語で解説（読み上げ）した後、学生アルバイトが中国語で解説（読み上げ）

座学資料 (日本語・英語・中国語)

英語版

中国語版

日本語版



Information Security Policy and (Regulatory) Compliance for Hiroshima University Students

広大生のための情報セキュリティポリシー・コンプライアンス (法令遵守)

広島大学学生の信息安全政策・規則 (法令遵守)

Getting started

The Internet is very useful in our life, but we need to be aware of the various risks in the Internet if we neglect our attention to the information security.

For example...

I found my favorite music at the website where user paid music free of charge. So I downloaded it from there.

⇒ This is an infringement of copyright.

I copied and pasted the paragraph which has been taken from the Internet into my paper without asking author's permission.

⇒ This may become an infringement of copyright. * If it is done for a thesis, the degree will be cancelled.

はじめに

インターネットは大変便利ですが、注意を怠るとさまざまな危険が身に降りかかります。

例えば...

本来有料の音楽ソフトが無料でダウンロードできるようなウェブサイトを見つけたので、気軽にダウンロードしました。

⇒ 著作権の侵害となる。

講義で出された課題のレポートに、インターネットで見つけた文章を、著者に無断でそのまま「コピペ」しました。

⇒ 著作権の侵害となる場合があります。
* 学位論文で行って、学位が取り消された例も。

目次

はじめに・この講義の目的

- 代表的なトラブルの例 (個人大学の学生・教職員に限るべき対策・行動)
- (個人大学の学生・教職員に限るべき対策・行動)
- 広島大学が実施している取り組み (組織の対策)
- コンピュータ関係のトラブルにあつたら
- まとめ

【参考文献】

- 広島大学で実際に起こった問題
- なぜ広島大学は「ファイル共有ソフトウェア」を禁止するのかわ
- 情報セキュリティに関する広島大学の方針
- 関連する法律・注意事項

表記について

この資料では、理解のポイントとなる部分を以下のように表記しています。参考にしてください。

- 具体的なトラブルの例
- 情報セキュリティポリシーで定めていること
- ポリシーを守るために個人で実行すべきこと
- ポリシーを守るために大学として実行していること

座学資料 - 概要

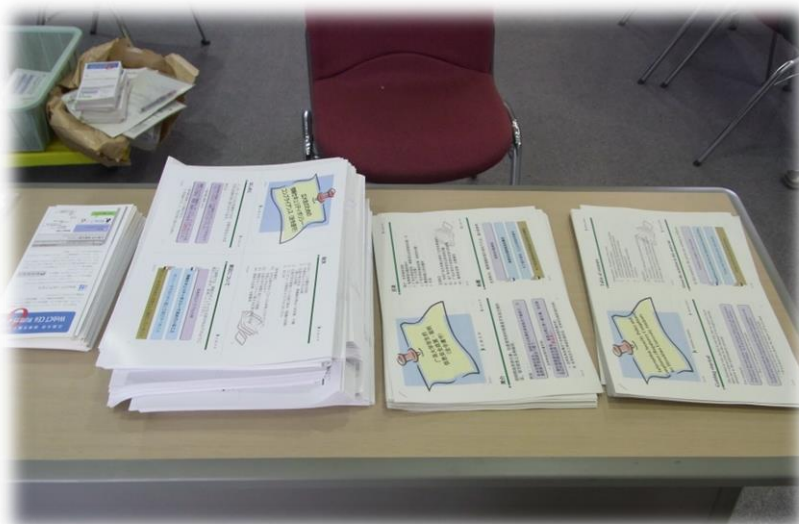
- 目的
 - 個人としてやるべきことを学び
 - 実行できるようになること
- 代表的なトラブルの例
 - 一般的なトラブル
 - 広島大学で実際に起こったトラブル
- 広島大学の学生・教職員が取るべき対策・行動（個人の対策）
 - 対策
 - ファイル共有ソフトを使用しない
 - ID、パスワードを適切に管理する
 - ウィルス対策を行う
 - ソフトウェアをアップデートする
 - 行動
 - 結果を想像して行動する
- 広島大学が実施している取り組み（組織の対策）
 - 利用者認証（ICカード、ネットワーク）
 - ネットワーク監視（P2P、IDS）
 - ウィルス対策ソフトの提供
 - マイクロソフト包括ライセンス契約
- コンピュータ関係のトラブルにあったら

ウィルス感染の様子や
情報漏洩の様子を
ビデオで紹介

なぜ広島大学は
「ファイル共有ソフトウェア」
の使用を禁止するのか？

座学（講習会）の様子

写真は2013年度の様子



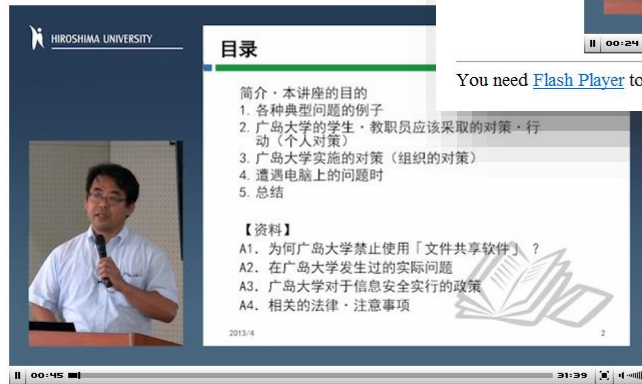
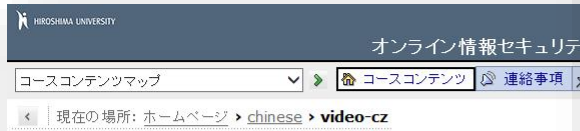
2014年11月14日

CAUAシンポジウム2014

25

講習会ビデオ(音声は日本語のみ)

画像は2013年度版



You need [Flash Player](#) to watch the video.



You need [Flash Player](#) to watch the video.



You need [Flash Player](#) to watch the video.

※ 補講終了後に公開

オンライン講座（日本語・英語・中国語）

HIROSHIMA UNIVERSITY オンライン情報セキュリティ

コースコンテンツマップ > コースコンテンツ 連絡事項

現在の場所: ホームページ > chinese

网络安全讲座

To change system language from Japanese to English, read

简介 & 前言	关于本讲座
1 网络安全的基础	2 计算机软件更新
4 电脑安全	5 认证的的安全
7 应用程序的安全对策	8 对于安全性的日常的处理
V 讲习会的录像 広島大学学的 情報セキュリティ政策・規程	

(C) 2008-2012, Information Media Center

HIROSHIMA UNIVERSITY myWebCT | アクセシビリティ | ヘルプ | ログアウト

オンライン情報セキュリティ講座 / Information Security 2013

コースコンテンツマップ > コースコンテンツ 連絡事項 ディスカッション 成績表 学習進捗 ノート

現在の場所: ホームページ > English

Information Security

To change system language from Japanese to English, read "How to use WebCT" in "Introduction".

画像は2013年度版

HIROSHIMA UNIVERSITY myWebCT | アクセシビリティ | ヘルプ | ログアウト

オンライン情報セキュリティ講座 / Information Security 2013

コースコンテンツマップ > コースコンテンツ 連絡事項 ディスカッション 成績表 学習進捗 ノート

現在の場所: ホームページ

オンライン情報セキュリティ講座

インストラクタより	この講座について	掲示板
1 セキュリティの基礎	2 ソフトウェアの更新	3 ウィルス対策
4 コンピュータセキュリティ	5 認証のセキュリティ	6 ネットワークのセキュリティ対策
7 アプリケーションのセキュリティ対策	8 セキュリティに対する日常の取り組み	e 修了試験
V ビデオ講義 広島生のための情報 セキュリティコンプライアンス	⇒ English version	⇒ 中文版

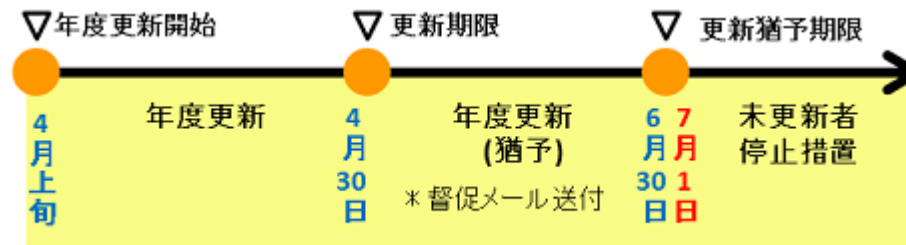
(C) 2008-2012, Information Media Center

情報セキュリティ・コンプライアンス教育

- 平成23年度より全学的に実施
 - 情報セキュリティの維持・違法行為の防止
 - 広島大学の学生として持つべき倫理観の醸成
- フレッシュマン講習
 - 在籍1年目の学生
 - 学部1年次生、大学院博士課程前期・後期1年次生、編入学生、研究生、科目等履修生等
 - 旧学生番号を持っている（過去に在籍記録がある）者を除く
 - 座学＋オンライン講座＋終了テスト
- フォローアップ講習
 - 在籍2年目以降の学生および全教職員（平成24年度～）
 - 自己点検（平成25年度～）＋オンライン講座＋確認テスト
 - 年度初めのアカウント年度更新に合わせて実施

アカウント年度更新

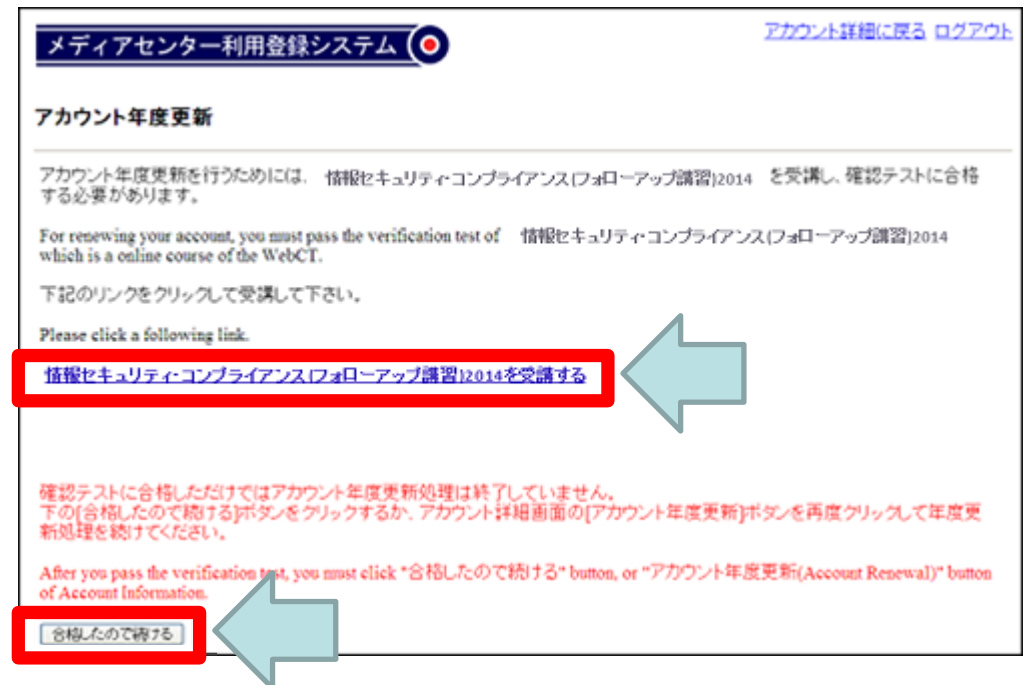
- 平成20年度～ 遊休アカウント撲滅を目的に開始
 - 3ヶ月(猶予期間含む)以内にアカウントの継続利用の意思を表示



- 意思表示のないアカウントはロック
 - 大部分のサービスが利用不可(メール、教育用端末、学外からのネットワーク接続サービス、ホームページの公開)
 - 利用登録システムへのログインのみ可能 (自主ロック解除)
- 利用者が行うこと
 - 利用規則への同意 → 機械的に同意ボタンを押す
 - 授業等への影響を考慮して確認テストの導入は見送り

アカウント年度更新 (つづき)

- 平成23年度～ フォローアップ講習開始
 - フォローアップ講習 = 自己点検
 - アカウント年度更新を完了するための前提条件に位置付け
 - 自己点検(平成25年度～)
 - 過去1年の自らの行動を振り返る
 - オンライン資料での復習(知識の更新)
 - 重要事項の(再)確認 → オンライン講習資料へのリンク
 - 最近の取組みや連絡事項の周知
 - 確認テスト
 - 80点以上獲得で合格



メディアセンター利用登録システム [アカウント詳細に戻る ログアウト](#)

アカウント年度更新

アカウント年度更新を行うためには、情報セキュリティコンプライアンス(フォローアップ講習)2014を受講し、確認テストに合格する必要があります。

For renewing your account, you must pass the verification test of 情報セキュリティコンプライアンス(フォローアップ講習)2014 which is a online course of the WebCT.

下記のリンクをクリックして受講して下さい。

Please click a following link.

[情報セキュリティコンプライアンス\(フォローアップ講習\)2014を受講する](#)

確認テストに合格しただけではアカウント年度更新処理は終了していません。下の(合格したので続ける)ボタンをクリックするか、アカウント詳細画面の[アカウント年度更新]ボタンを再度クリックして年度更新処理を終えてください。

After you pass the verification test, you must click "合格したので続ける" button, or "アカウント年度更新(Account Renewal)" button of Account Information.

[合格したので続ける](#)

フォローアップ講習実施状況

画像は2013年度版



- セキュリティポリシー実施手順に基づく自己点検
 - 実施者数：14,567名
(内訳)

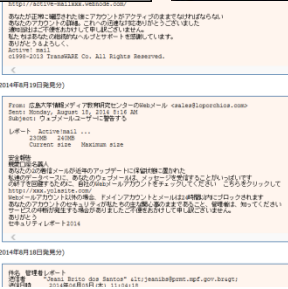
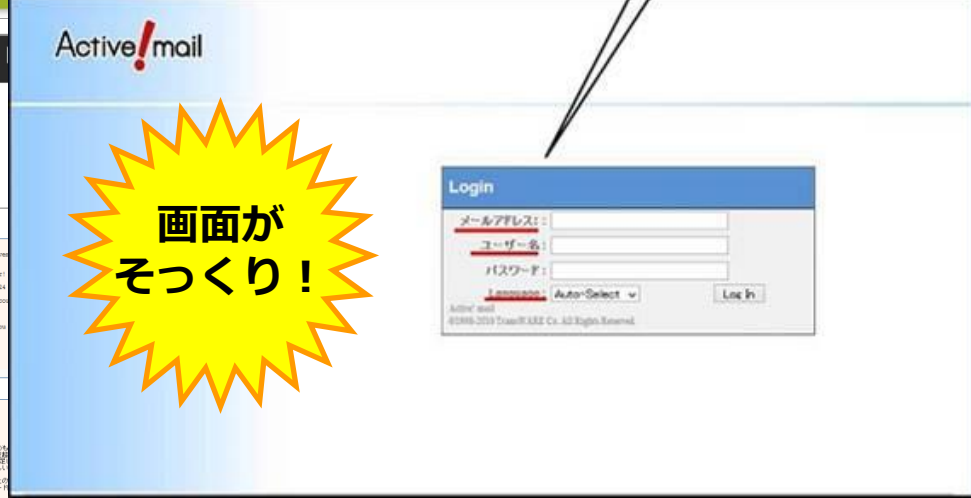
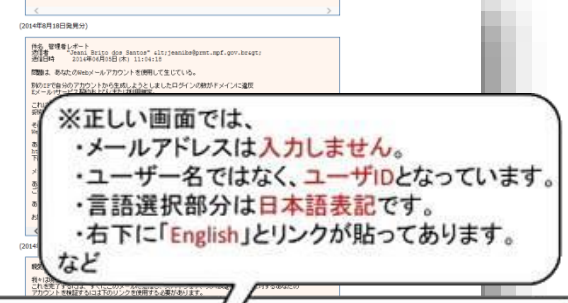
学生	9,962名
教職員	4,260名
学外者	345名
- オンライン講座＋確認テスト(年度更新)
 - 対象数：16,133アカウント
 - 実施数：14,650 (90.8%)
(内訳)

学生	10,066 (90.4%)
教職員	4,315 (92.9%)
学外者	269 (76.0%)

広島大学における 情報セキュリティインシデントの現状

会場のみ

Active!mailを利用したフィッシングメールに関する注意喚起 (標的型攻撃)



<http://www.media.hiroshima-u.ac.jp/news/2013111802>

新聞にも取り上げられました(2014/4/21)

会場のみ

注意喚起・情報提供

会場のみ

注意喚起等への対応の現状と課題

- 膨大なログから対象を検索
 - ファイアウォールログ（1日分）
 - 4,500万行、7.7GB（2013/11/9）
 - 「日本語文字入力補助ソフトによる情報漏えいの危険性」に対する調査
 - 2013/11/26～2013/12/27 →2013/12/27（通信制限）
 - 2014/1/28～2014/2/3
 - 2014/2/10～2014/2/16
 - 2014/2/17～2014/2/23
 - 「Adobe Flash Playerの脆弱性を狙った攻撃」に対する調査
 - 2014/5/4～2014/6/3
 - 2014/5/6～2014/6/5 →2014/6/9（通信制限）
- サイバーセキュリティ基本法案が成立
 - 「ログを取得し、調査できること」は組織としての責任
 - ログの肥大化
 - 組織間の連携（プライバシー問題）
 - クラウドサービスを利用している場合はどうなる？

クラウドサービス利用ガイドラインの整備

- 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

クラウドサービス利用ガイドライン

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
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	×	×	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 アしています
	(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 を検討しまし 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

広島大学

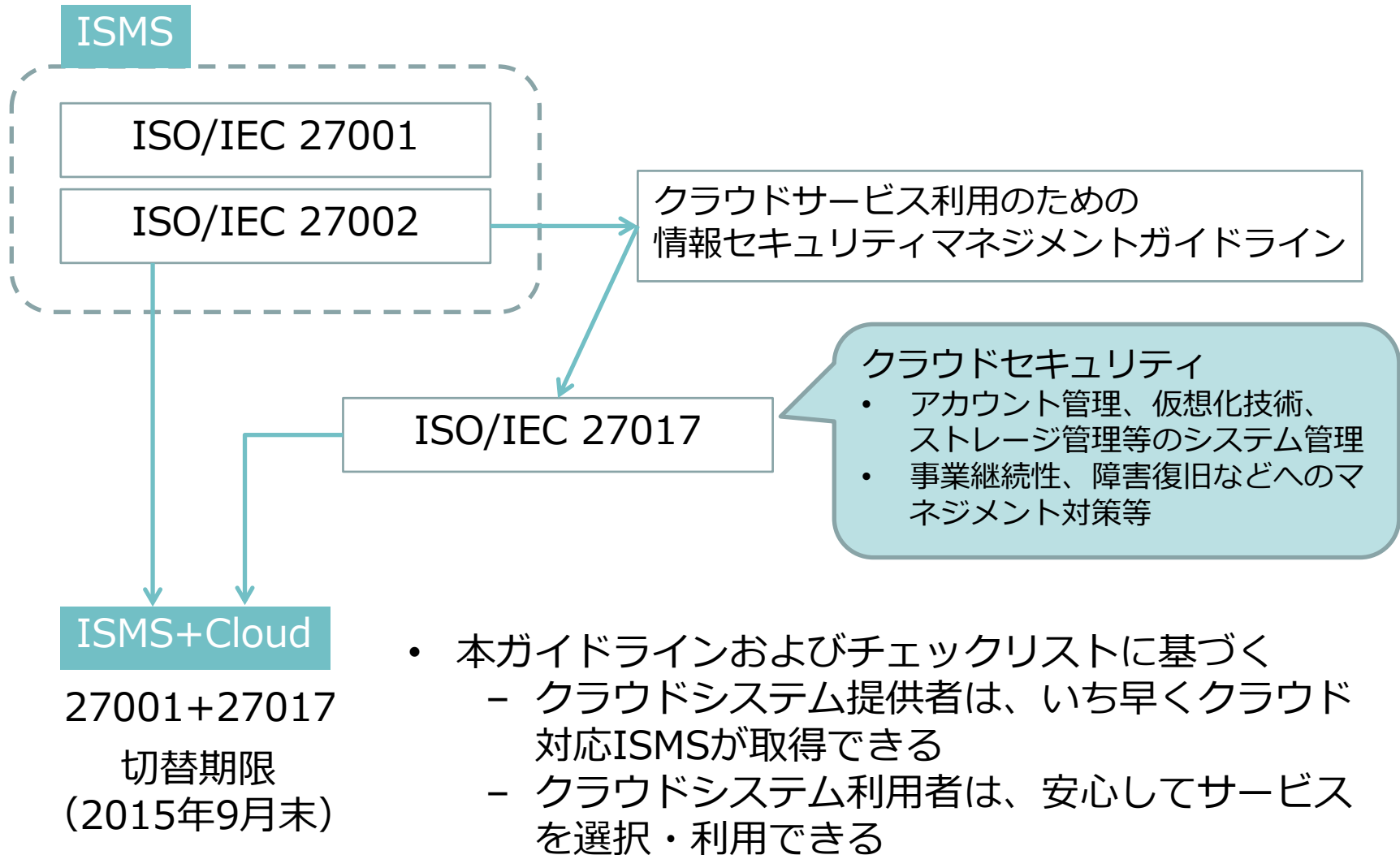
クラウドサービス 利用ガイドライン

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

ISMS規格改定への対応



クラウドサービス利用ガイドライン

[サイトマップ](#) [アクセシビリティ](#)

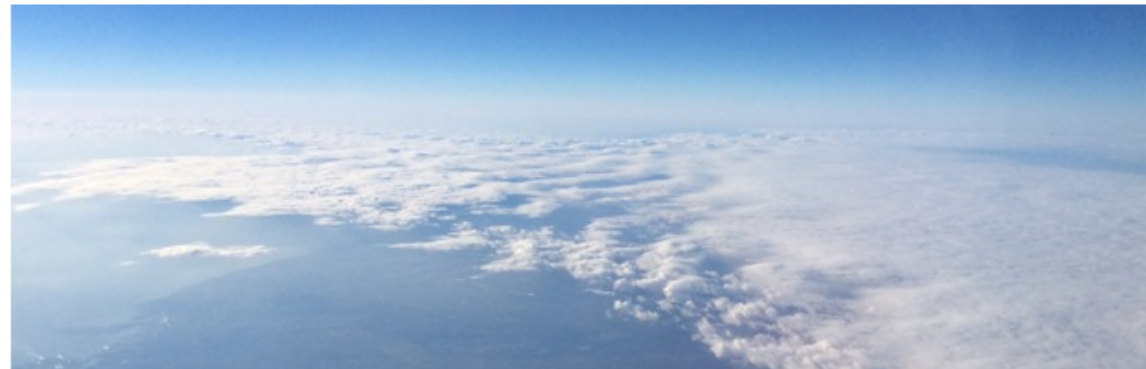
Information Media Center, Hiroshima University

広島大学 情報メディア教育研究センター

[ホーム](#)
[ニュース・お知らせ](#)
[提供サービス](#)
[センター紹介](#)
[FAQ・問い合わせ](#)

 現在位置: [ホーム](#) → [ニュース・お知らせ](#) → [クラウドサービス利用ガイドライン](#)

広島大学クラウドサービス利用ガイドライン



お知らせ

- [大学等におけるクラウドサービス利用シンポジウム2014](#)（平成26年3月31日（月）13:30～17:00）を行いました。
- [クラウドサービス利用ガイドライン説明会](#)（平成26年2月5日（水）14:30～16:00）を行いました。

クラウドサービス利用ガイドラインの整備について

<http://www.media.hiroshima-u.ac.jp/news/cloudguide>

お知らせ

[RSS](#)
[クラウドサービス利用ガイドライン](#)
[情報セキュリティ・コンプライアンス教育](#)
[セキュリティ情報](#)
[省エネ情報](#)
[カテゴリ別のお知らせ](#)
[・障害情報](#)
[・メンテナンス情報](#)
[・サービス紹介](#)
[・手続きのお願い](#)
[・端末室情報](#)
[・講習会・イベント](#)

広島大学のクラウド化手順

- クラウドサービス利用ガイドラインの整備
 - 全学の統一基準としてガイドラインを策定
 - 現時点で絶対的な基準を定めることは困難
 - 確認すべき要素の定義とチェックリストの提供
 - 運用上注意すべき項目の明確化
 - オンプレミスの場合でも同様の手順が必要
- **担当者レベルでの確認・判断が可能となった**
- 財務会計・人事システム等をクラウド化
 - アプリケーションを（原則）そのまま移行
 - **事務システムの心臓部のクラウド化が完了**

プレスリリース (財務会計システム)



Benic ベニックソリューション株式会社

[サイトマップ](#)
[お問い合わせ](#)
[ホーム](#)

[ホーム](#) > [プレスリリース](#) > 広島大学向けSAP ERPをAWS上に構築～クラウドを活用したSAP ERPビジネス展開の第一歩に～

広島大学向けSAP ERPをAWS上に構築 ～クラウドを活用したSAP ERPビジネス展開の第一歩に～

2014年2月3日
ベニックソリューション株式会社

ベニックソリューション株式会社(本社:兵庫県神戸市、取締役社長:宇野 知之)は国立大学法人 広島大学(所在:東広島市鏡山、学長:浅原 利正)にAmazon Web Services,Incの提供するクラウドサービスであるアマゾン ウェブ サービス(以下AWS)のAmazon Elastic Compute Cloud (AmazonEC2)を活用したSAP ERPの運用サービスを開始しました。国立大学法人においてAWS上でSAP ERPの運用サービスが開始されるのは、初めてのケースとなります。

広島大学は国立大学法人化に伴い、2009年にSAP R/3 Enterprise(以下SAP)を導入しました。従来、国立大学では学内にデータを置くことを基本としておりましたが、SAP ERPのバージョンアップおよびサーバの更新にあたり、データをクラウドに置くことを決断しシステム基盤としてAWSを採用することとしました。

サーバ更新にあたって検討した課題は次のとおりです。

<http://www.benic.co.jp/release/20140203.html>





プレスリリース (人事労務システム)



The screenshot shows the 'WORKS APPLICATIONS' website. The main content is a news article titled '国立大学法人で初、人事労務システムの基盤をクラウドへ ~広島大学の先進的取組みをワークスがサポート~'. The article is dated 14.2.21 and includes a PDF download link. The text describes the implementation of 'COMPANY on Cloud Managed Service' (CCMS) at Hiroshima University, a public university. The article is part of a series of news items, with a sidebar on the left containing navigation links for Home, News & Topics, Products & Services, Events, and Works Applications. A right sidebar contains contact information and a list of past news items from 2014 to 2005.

<http://www.worksap.co.jp/topics/news/2014/0221.html>

主なシステムのパブリッククラウド化予定

- 事務用メールシステム  Office 365
 - 2014年8月移行済み
- 広島大学公式Webサイト 
 - 2014年度中に順次移行
- 研究者総覧・研究力分析システム 
 - 2014年度内に新システム運用開始
- 全構成員（教職員・学生）用メールシステム  Office 365
 - 2014年度一部移行、2015年度より全面移行
- インターネット出願システム
 - 2015年度学部一般入試から導入

ガイドライン策定の功罪？！

- 確認すべきポイント（問題点）の明確化
 - － オンプレミスの安全神話化
 - PDCAサイクルの重要性を再認識
 - ISMS認証取得へ（2014年度内目標）
 - － 担当者レベルでの確認・判断
 - 安易なクラウド化を助長する、かも...
 - 定期的なチェック義務化が必要？
- システム構築手法見直しの契機
 - － ハードウェアのライフサイクルの変化
 - これまでの調達手続き（4～5年単位）とのミスマッチ
 - 大型システムの調達をどうするか？
 - － ハードウェア指向からサービス指向へ
 - 機能性能の評価方法
 - （HPC以外の）ベンチマークをどうするか？
 - ソフトウェアライセンスのクラウド上での利用
 - BYOL（Bring Your Own License）できない

大学における 情報セキュリティ対応の課題

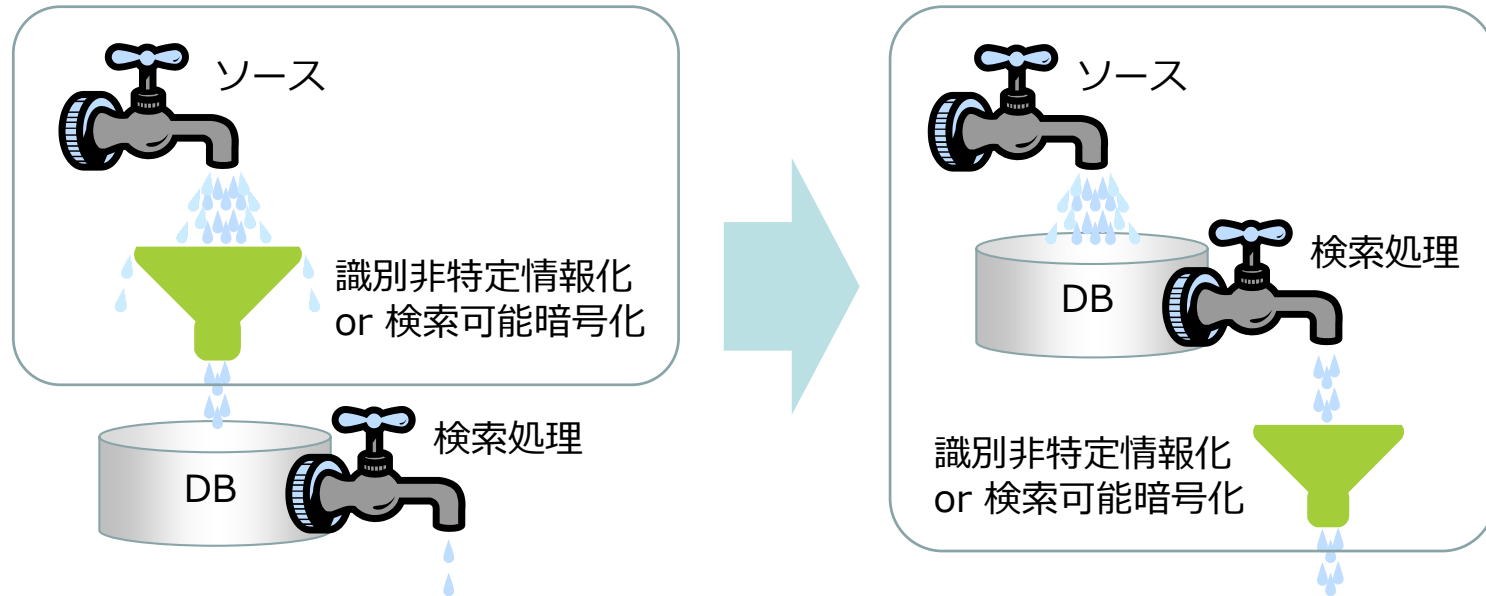
情報系センターへの期待（役割）の変化

- 計算機・ネットワークインフラの整備・運用
 - （これまで）大学が情報環境を提供
 - （これから）PC必携化、BYOD（Bring Your Own Device）
 - ガバナンス喪失の恐れ
- クラウドサービスの台頭
 - 積極的利用への圧力
 - 財政的メリット（本当？）を求める経営層からの圧力
 - 便利さ・手軽さを求める利用者層からの圧力
 - 計算リソースの調達方法の変化
 - セキュリティポリシーとの折り合いをどうつける？
 - ガバナンス喪失の恐れ
- 情報セキュリティに対する責任は増大傾向に
 - サービス等の利用の可否判断
 - 迅速かつ適切なインシデント対応
 - ガバナンスを失いつつある状況で大丈夫か？

溶け込んでいる情報（ビッグデータ）の活用

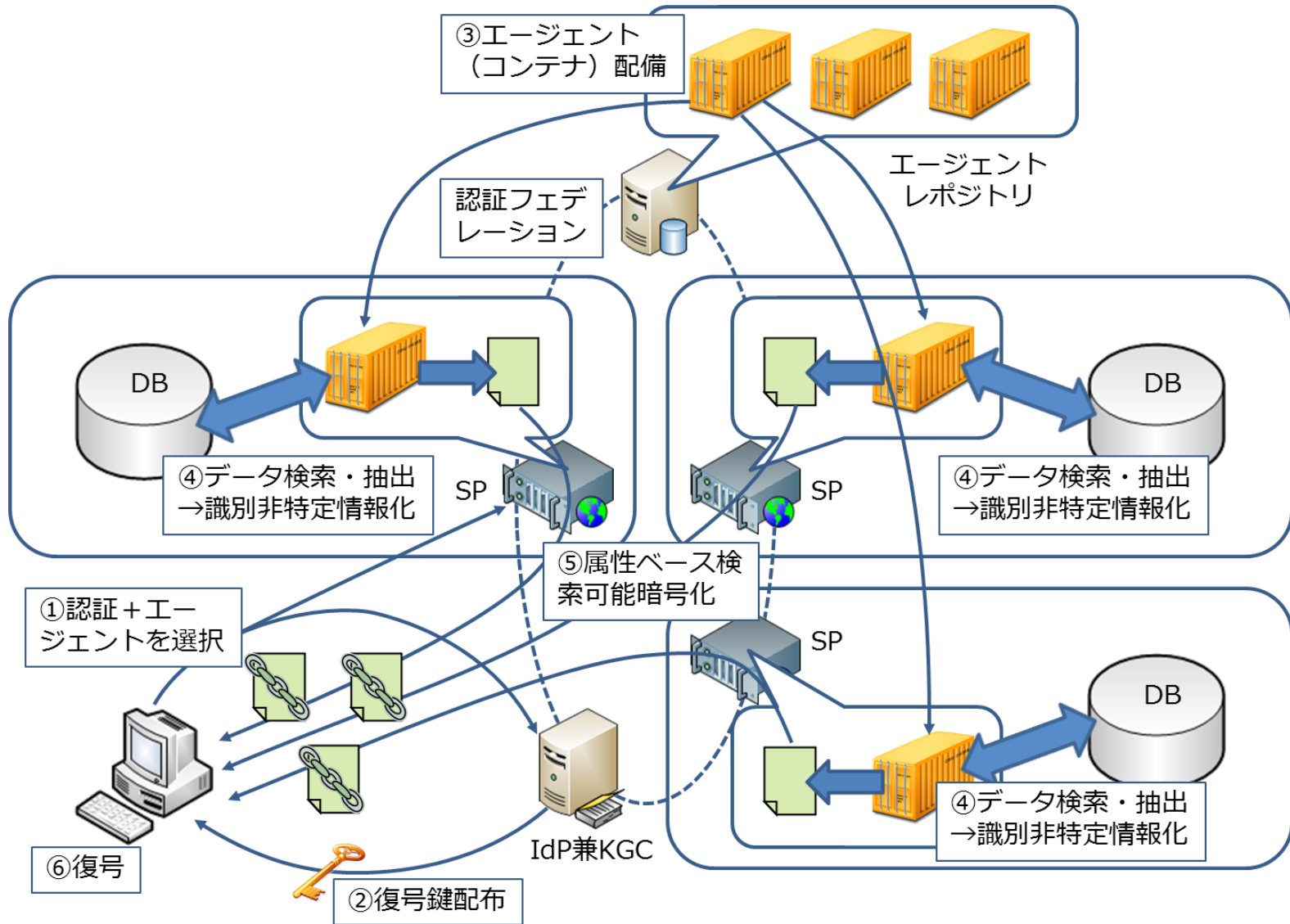
- “溶け込んでいく情報”
 - サイエнтиフィック・システム研究会
 - 合同分科会2014年度会合@神戸（2014/10/30～31）
 - Seeds orientedからNeeds orientedへ
 - 男性的思考から女性的思考へ
 - （これまで）とにかくデータを集める → 何ができる？
 - （これから）何したい？ → どんな技術が必要？
 - 「気づき」を支援する技術
 - 非日常からの「気づき」、ロングテールデータ（≡お散歩？）
 - ログの活用（通信記録、eポートフォリオ、etc.）
- クラウドサービスの料金体系から
 - アップロードは無料（データを集める）
 - 蓄積・処理は安価（データを処理する）
 - 「ダウンロードに課金（データを提供する）」がポイント
 - 発生源（蓄積場所）処理

発生源（蓄積場所）処理の必要性



- データは消費される場所で処理
 - 発生源ですべてのデータを匿名化・暗号化
 - データの取りこぼし、非効率（大部分は（結果的に）不要なデータ）
 - データは発生源（蓄積場所）で処理
 - 必要な（価値のある）データのみ匿名化・暗号化して提供
- これを組織横断的に実行できる仕組みが必要

構成案（検討中）



まとめ

- 広島大学における情報セキュリティへの取り組み
 - 規定や技術による対策
 - HINET2007からHINET2014へ
 - 利用者認証・二要素認証
 - 教育による対策
 - 情報セキュリティ・コンプライアンス教育
 - アカウント年度更新（自己点検+フォローアップ教育）
- 広島大学における情報セキュリティインシデントの現状
 - フィッシングメールへの対応
 - サイバーセキュリティ基本法への対応
 - ログの取得と検索
 - クラウドサービス利用ガイドライン
 - ガイドラインの功罪
- 大学における情報セキュリティ対策の課題
 - 溶け込んでいる情報（ビッグデータ）の活用
 - 発生源処理の必要性