広島大学における CSIRT活動の取組み

広島大学 情報メディア教育研究センター
西村 浩二

HiBiS IT勉強会

自己紹介

- 西村 浩二（にしむら こうじ）
  - 1991年 広島大学大学院工学研究科博士課程前期修了
  - 1991年 全日空システム企画（株）
    （現、ANAシステムズ（株））
  - 1994年 広島大学総合情報処理センター助手
  - 2002年 博士（工学）（広島大学大学院工学研究科）
  - 2007年 同情報メディア教育研究センター准教授
    - ユーザーサービス部門長（サービス運用責任者）
  - 2011年 同情報メディア教育研究センター教授
    - 情報セキュリティ研究部門長（セキュリティ教育・啓蒙、ガイドライン等の検討・策定）
  - 2017年 同情報メディア教育研究センター長
    - 情報セキュリティ研究部門長、ユーザーサービス部門長、財務・総務室情報部長兼務
    - 情報処理安全確保支援士（登録番号：第001322号）
  - 2018年 情報科学部教授（併任）

- 広島大学クラウドサービス利用ガイドライン
  - https://www.media.hiroshima-u.ac.jp/news/cloudguide
    → 広島大学におけるクラウドサービス利用のためのガイドライン
- 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」セキュリティ分野担当
  - http://www.icer.kyushu-u.ac.jp/ac
    → 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イポリシー推進部会
  - 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のテンプレート

本日の内容

- 概要
  - 広島大学では、2005(平成17)年度に情報セキュリティポリシーを策定し、以来、情報セキュリティ推進機構が本学におけるCSIRTに係る活動を担ってきた。近年では、文部科学省の指導により情報セキュリティ対策基本計画を策定し、それに基づいた活動を行っている。本講演では、情報セキュリティ推進機構が行っている諸活動(教育・研修、訓練、対応等)について紹介し、本勉強会の参加者との意見交換を通して、当該地域における情報セキュリティ対策強化の参考とする。
- 目次
  - 情報セキュリティに関する規則・制度
    - 情報セキュリティポリシー、ISMS/ISMSクラウドセキュリティ認証
  - 情報セキュリティ教育・研修
    - 情報セキュリティ・コンプライアンス教育、情報セキュリティ研修
  - インシデント対応
    - NII-SOCSとの連携、インシデント対応フロー
  - 訓練と成果
    - インシデント対応訓練、インシデント発生状況

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
  - ①東広島キャンパス，②霞キャンパス，③東千田キャンパス，④～⑱遠隔地区
  - 県外オフィス（東京、大阪、福岡）
  - 海外オフィス（北京，上海，ジャカルタ，バンドン，ベトナム，ブラジル，韓国，台湾，トムスク，ケニア，カイロ，ミャンマー，グアナファト，カンボジア，リトアニア）
- 部局等（平成30年4月1日現在）
  - 12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，2共同利用・共同研究拠点，1中国・四国地区国立大学共同利用施設、21学内共同教育研究施設等
  - 5図書館、3博物館等、大学病院（診療科：34医科、13歯科）
- 構成員数19,118名（平成30年5月1日現在）
  - 学部学生10,810名，大学院生4,559名，専攻科学生15名，研究生・科目等履修生308名
  - 役員10名，教員1,726名，職員1,690名

広島大学における

情報セキュリティに関する規則・制度

広島大学情報セキュリティポリシー

平成17年４月
広島大学情報セキュリティポリシー策定・施行

- 情報セキュリティポリシーとは？
  - 組織における情報セキュリティに関する方針や体制、対策を総合的・体系的かつ具体的にとりまとめたもの。

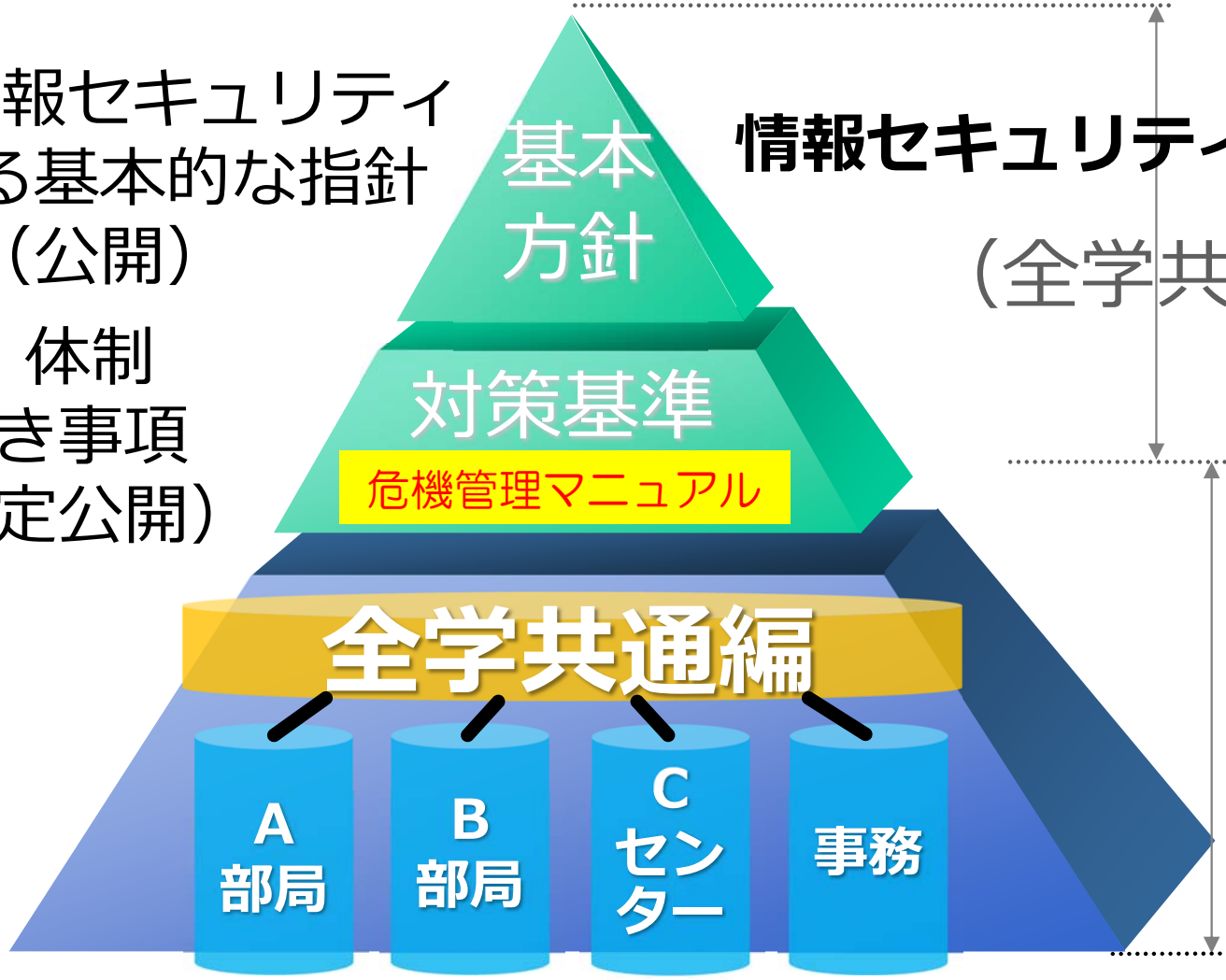
https://www.hiroshima-u.ac.jp/about/initiatives/jyoho_ka/security_policy

情報セキュリティポリシーの体系

広島大学

本学の情報セキュリティに対する基本的な指針（公開）

組織・体制
守るべき事項
（学内限定公開）

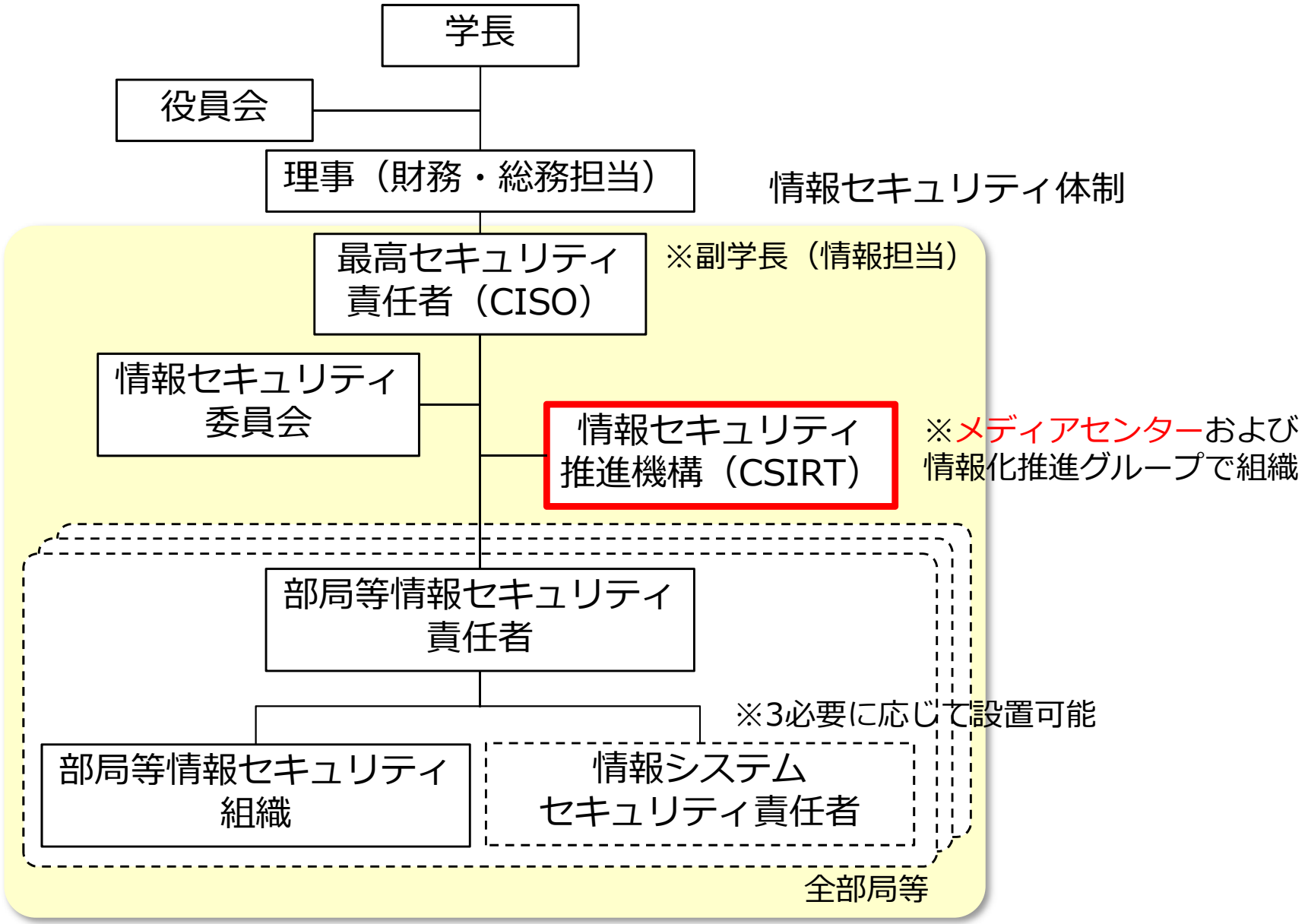


情報セキュリティポリシー
（全学共通）

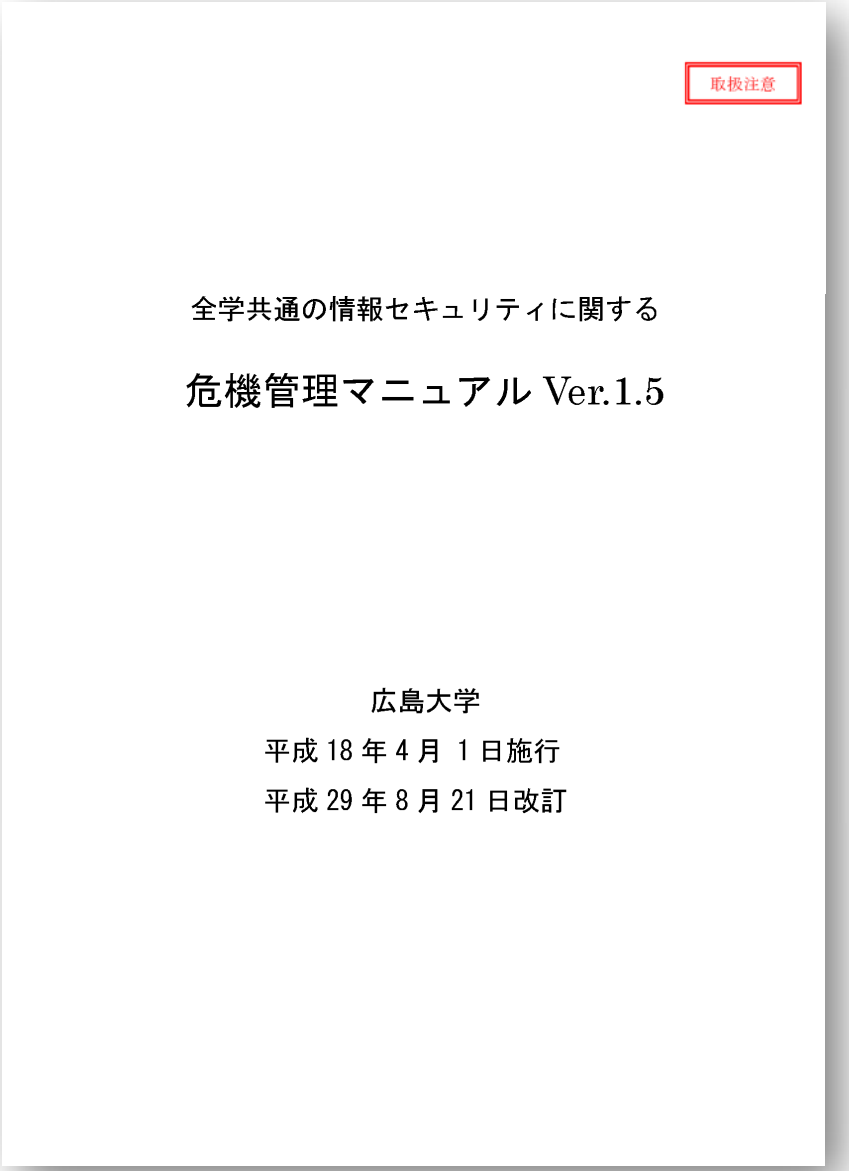
実施手順
（全学共通編＋部局編）

部局毎に守るべき事項を具体的にどういう手順で行うか（学内限定公開）

広島大学の情報セキュリティ運営体制



危機管理マニュアル


取扱注意

全学共通の情報セキュリティに関する

危機管理マニュアル Ver.1.5

広島大学

平成 18 年 4 月 1 日施行

平成 29 年 8 月 21 日改訂

情報セキュリティに関する事件や事故の具体例、及び発生時に構成員と組織が取るべき行動を全学的に定義

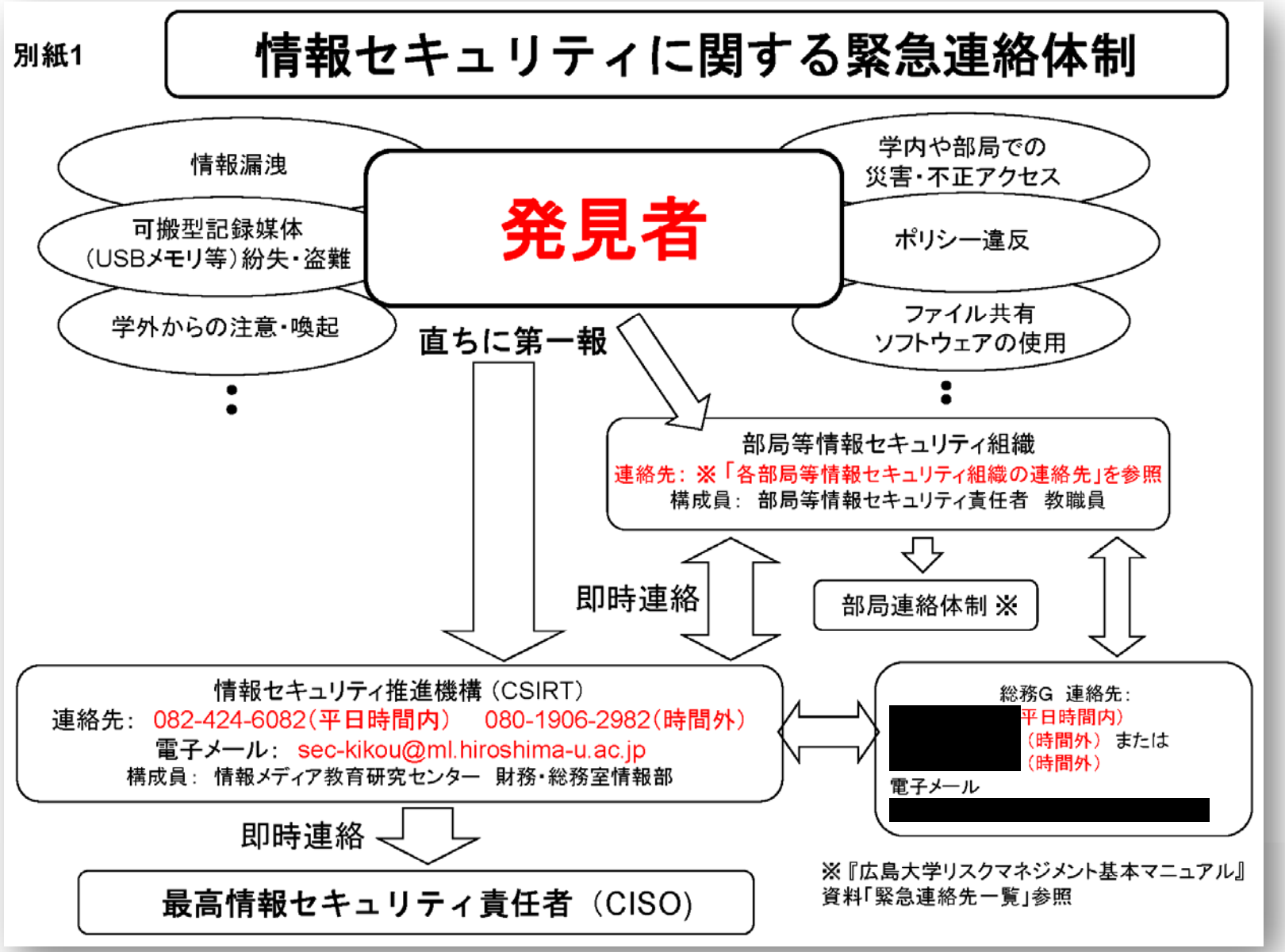
インシデント発生時の連絡先など学内ポータルで公開

平成30年度内に改訂予定

インシデント・トラブル発生時の
調査・対応手順の明確化など

情報セキュリティに関する緊急連絡体制

広島大学



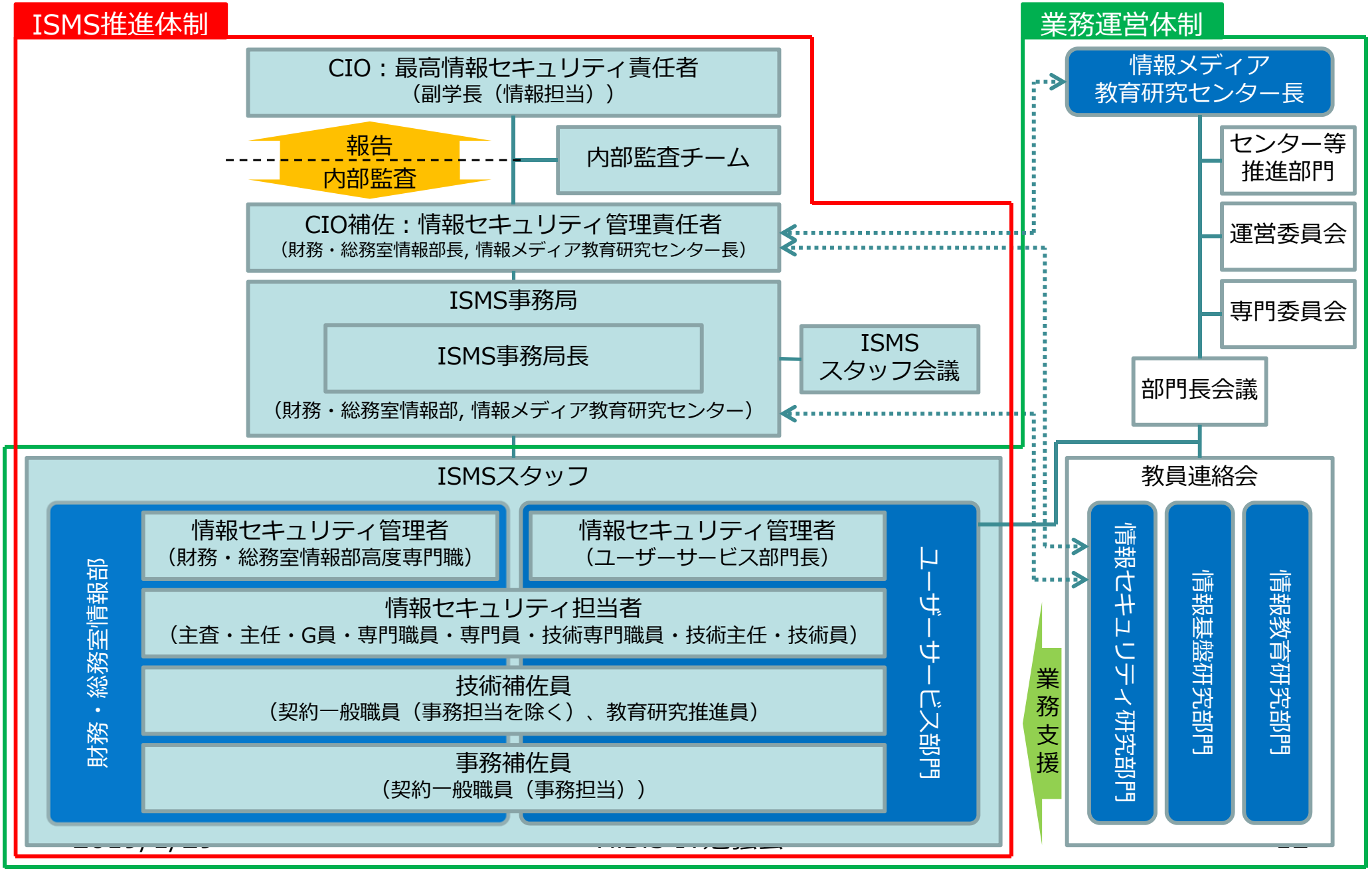
情報セキュリティクイックガイド

広島大学

緊急時の連絡先がわかるカードを配布しています。

いざという時に備えて、職員証と一緒に携帯しておきましょう！

ISMS推進体制


ISMS推進体制
CIO：最高情報セキュリティ責任者
（副学長（情報担当））
報告
内部監査
内部監査チーム
CIO補佐：情報セキュリティ管理責任者
（財務・総務室情報部長, 情報メディア教育研究センター長）
ISMS事務局
ISMS事務局長
（財務・総務室情報部, 情報メディア教育研究センター）
ISMS
スタッフ会議
ISMSスタッフ
財務・総務室情報部
情報セキュリティ管理者
（財務・総務室情報部高度専門職）
情報セキュリティ管理者
（ユーザーサービス部門長）
ユーザーサービス部門
情報セキュリティ担当者
（主査・主任・G員・専門職員・専門員・技術専門職員・技術主任・技術員）
技術補佐員
（契約一般職員（事務担当を除く）、教育研究推進員）
事務補佐員
（契約一般職員（事務担当））
業務運営体制
情報メディア
教育研究センター長
センター等
推進部門
運営委員会
専門委員会
部門長会議
教員連絡会
業務支援
情報セキュリティ研究部門
情報基盤研究部門
情報教育研究部門

ISMS/ISMS-CLS認証取得の取組み

広島大学

株式会社日本環境認証機構（JACO）様からのエンドースメント

国立大学法人広島大学（情報メディア教育センター）様では、全学への情報サービスを提供する基幹システムにおいて、クラウドサービスの積極的な活用を推進されておられます。 それに伴う情報セキュリティ強化の一環として、2015年に情報セキュリティマネジメントシステム（ISMS）認証を取得され、今回、更なる強化・改善を図るべく、学術関連では日本で初めて、ISMSクラウドセキュリティ認証も取得されました。JACOは審査の基本姿勢として、「認証の取得を、ゴールにしない」を掲げておりますが、国立大学法人広島大学様の持続可能な発展のために、今後とも審査を通じて継続的にサポートさせて頂きながら、クラウドセキュリティの更なる改善及び他の大学等への知見の展開を期待いたします。

株式会社日本環境認証機構
ISビジネスユニット長 有吉 英也 様

記念写真

JACO様から27001（左）と27017（右）の登録証を授与されました

https://www.media.hiroshima-u.ac.jp/news/isms/

ISMS/ISMS-CLS登録証

JACO
Japan Audit and Certification Organization for Environment and Quality

UKAS MANAGEMENT SYSTEMS 051

ISMS-AC ISMS ISR007

国立大学法人広島大学
情報メディア教育研究センター
広島県東広島市鏡山1-4-2

登録証

登録番号:IC14J0392

ISO/IEC 27001:2013・JIS Q 27001:2014

情報メディア教育研究センターにおける情報サービスのための
利用者/認証情報の管理・運用

適用宣言書:IMC100-002 V1

当機関は、上記組織が、当該マネジメントシステム
要求事項に適合していることを証します。

登録日　：2015年 3月27日
更新日　：2018年 3月27日
発行日　：2018年 3月23日
有効期限：2021年 3月26日

株式会社 日本環境認証機構
東京都港区赤坂 2-2-19
代表取締役社長 立上和男

本証は登録証の一部ですので、付属書と合わせてご覧ください。

JACO
Japan Audit and Certification Organization for Environment and Quality

ISMS-AC ISMS ISR007 -CLS

国立大学法人広島大学
情報メディア教育研究センター
広島県東広島市鏡山1-4-2

登録証

登録番号:SC16J0003

（基となるISMS登録番号：IC14J0392）

JIP-ISMS517-1.0

(ISO/IEC 27017:2015に基づくISMSクラウドセキュリティ認証)

次のクラウドサービスのクラウドサービスカスタマとしての利用に係る
ISMSクラウドセキュリティマネジメントシステム
・Microsoft Azure、Office 365 Education
・Hitachi Cloud: エンタープライズクラウドサービス、出前クラウドサービス、
フェデレーテッドクラウド

適用宣言書　IMC110-014 V1

当機関は、上記組織が、ISO/IEC 27017:2015 のガイドラインに沿って
JIP-ISMS517-1.0 に適合していることを証します。

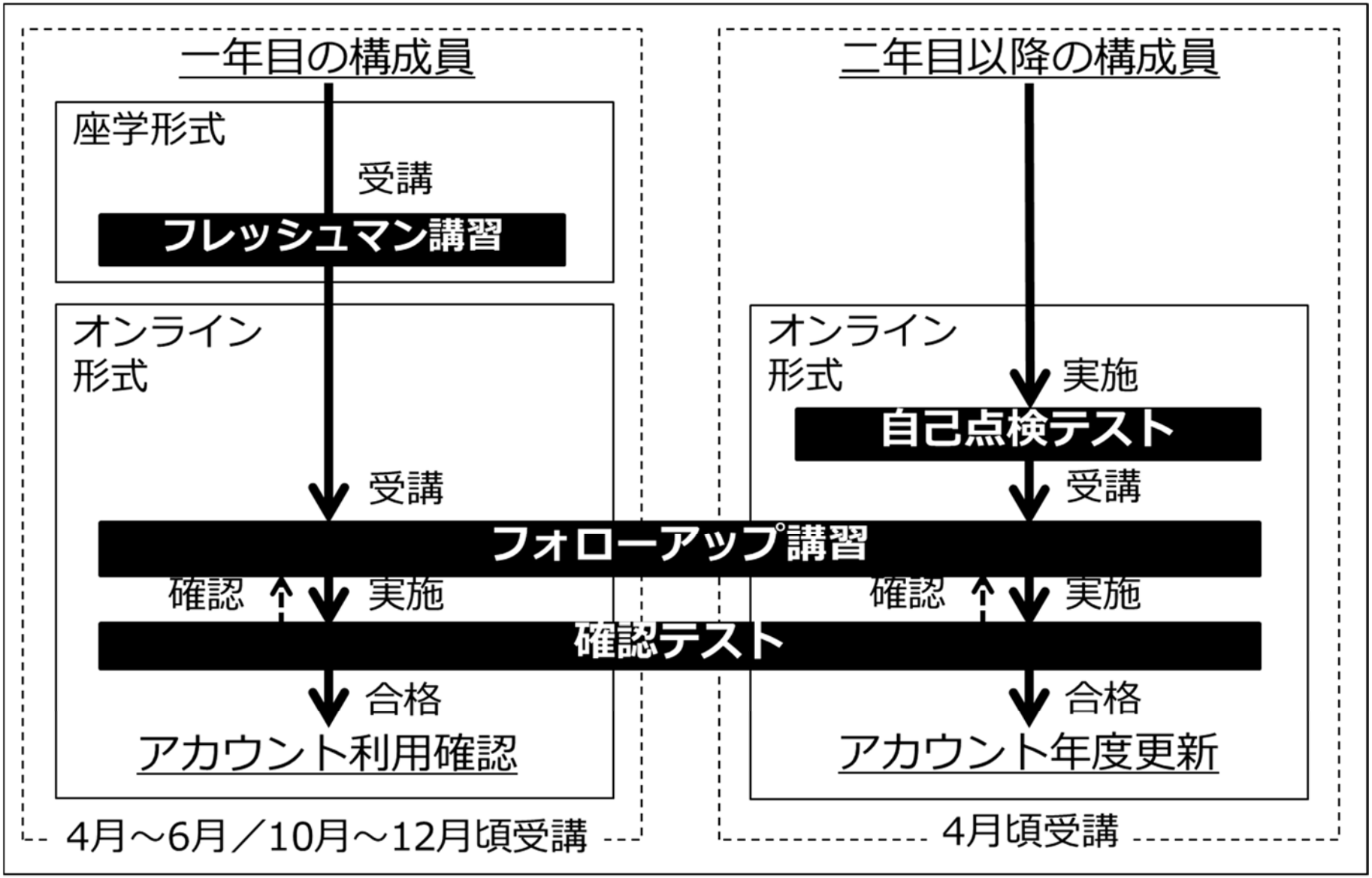
登録日　：2017年 3月23日
更新日　：2018年 3月27日
発行日　：2018年 3月23日
有効期限：2021年 3月26日

株式会社 日本環境認証機構
東京都港区赤坂 2-2-19
代表取締役社長 立上和男

広島大学における

情報セキュリティ教育・研修

情報セキュリティ・コンプライアンス教育



フレッシュマン講習の対象者

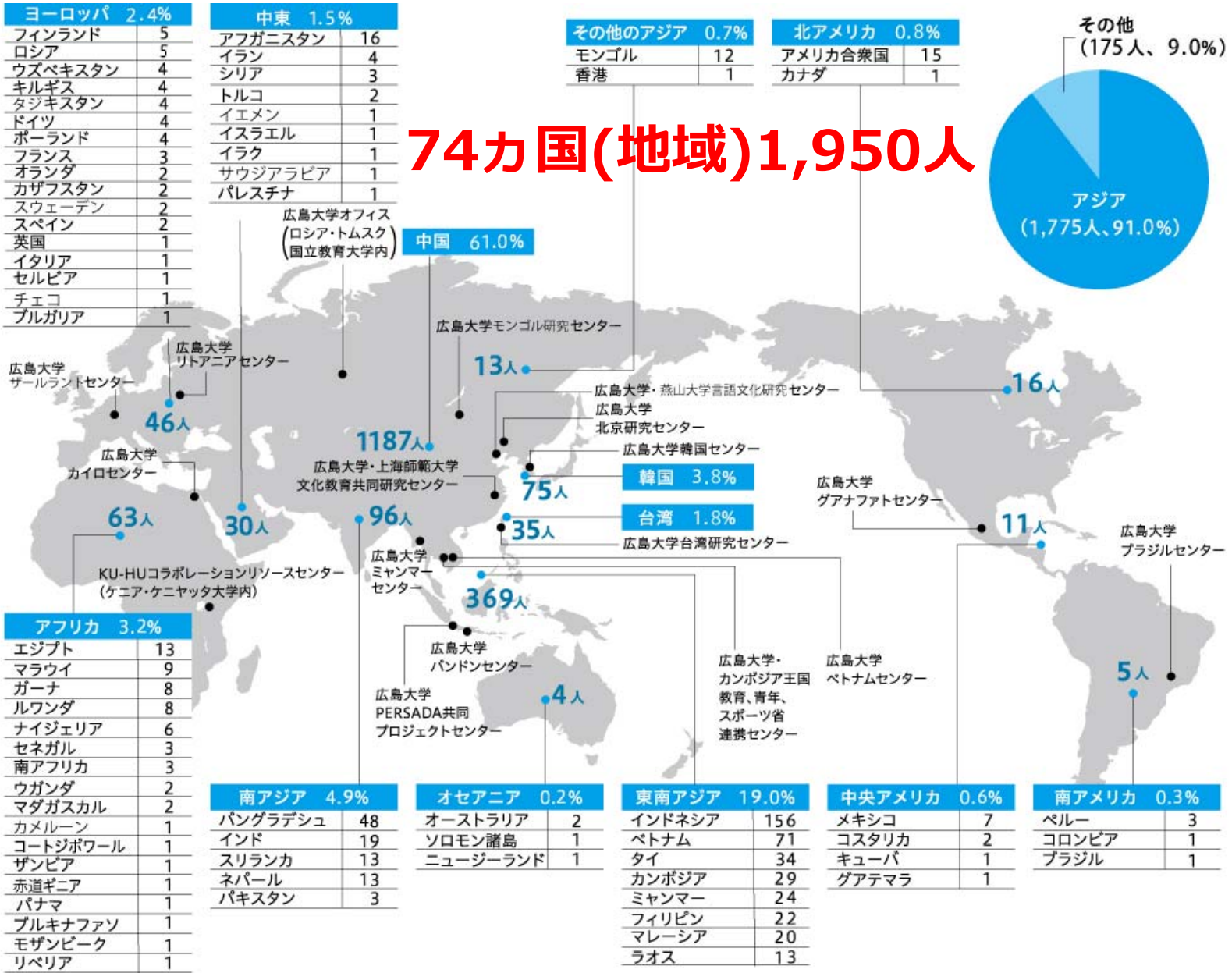
広島大学

平成30年12月20日現在

対象者		座学（授業）	座学（講習）	オンライン講習
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 大学院D1年次生	他大学から進学した学生	–	○	○
	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29年度受講者/対象者：
  - 座学：3,371/3,689名 91.4%
  - オンライン講習：4,595/4,951名 92.8%
- 平成30年度受講者/対象者：
  - 座学：3,431/3,695名 92.9%
  - オンライン講習：4,785/5,109名 93.7%

国(地域)別外国人留学生数（平成30年11月1日現在）



座学資料（日本語・英語・中国語）

広島大学

平成30年度版

大学教育入門 『第６章 情報セキュリティと情報倫理』

英語版

中国語版

日本語版

座学資料 - 概要

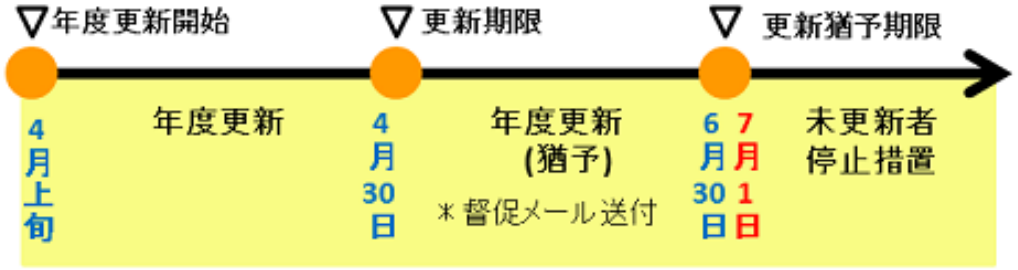
広島大学

平成30年度版

- 目的
  - 個人として行うべきことを学び、実際の学生生活の中で実行できるようになること
- 身近な情報セキュリティの脅威
  - 一般的なトラブル
  - 広島大学でのトラブル（資料へ）
- 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］ウイルス対策をする
  - ［対策］ソフトウェアを更新する
  - ［対策］ID／パスワードを適切に管理する
  - ［対策］バックアップをとる
  - 「対策］ファイル共有ソフトを使用しない
  - ［行動］フィッシングメールに注意
  - ［行動］利用規約の確認
  - ［行動］スマホの取扱いに注意
  - ［行動］公衆Wi-Fiを利用するときの注意
- 広島大学が実施している取り組み（組織の対策）
  - ［取組］利用者認証・身分証の提示
  - ［取組］パスワード強度メーター
  - ［取組］多要素認証
  - ［取組］ネットワーク監視
  - ［取組］マイクロソフト包括ライセンス
- 広島大学の構成員が備えておくべき情報倫理
  - 情報倫理とは
  - 適正な判断をするために（情報発信時）
    - ［行動］SNSでの発言での注意
    - ［行動］特定される可能性もある
    - ［行動］匿名でないことを認識する
    - ［取組］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
  - 適正な判断をするために（情報受信時）
    - ［行動］情報の内容を確認しましょう
    - ［行動］ファクトチェックをする
- 情報セキュリティトラブルが起こったら
  - ［取組］情報セキュリティクイックガイド
- まとめ
  - 重要なお知らせ
    - オンライン講習を受講してください
    - アカウントの利用確認が必要です
    - アンケートに協力してください
    - 出席確認について
- 資料
  - 情報メディア教育研究センターのサービス
  - 広島大学で実際に起こった問題
  - 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

アカウントの利用確認・年度更新

- 平成20年度～　遊休アカウント撲滅を目的に開始
  - アカウント作成または年度更新開始から90日（猶予期間含む）以内にアカウント利用の意思を表明



  - 意思表明のないアカウントをロック
    - メディアセンターサービスの利用停止（メール（Office365）、ICE端末、プリンタ出力、ネットワーク接続、ホームページ公開など）
    - 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
    - 確認テストへの合格（20問中16問以上正解する）
    - 利用規約への同意（同意ボタンを押す）

フォローアップ講習実施状況

広島大学

平成30年12月20日現在

- フォローアップ講習
  - 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：16,128名
    - 学生：10,577名、教職員：5,047名、学外者：504名
  - オンライン講習+確認テスト
    - 実施者数：16,138名
    - 学生：10,579名、教職員：5,056名、学外者：504名
- 利用確認（89.6%）
  - 確認数/対象数：5,410/6,039個
    - 学生：4,645個、教職員：670個、学外者：95個
- 年度更新（95.3%）
  - 更新数/対象数：16,168/16,968個
    - 学生：10,569個、教職員：5,086個、学外者：513個

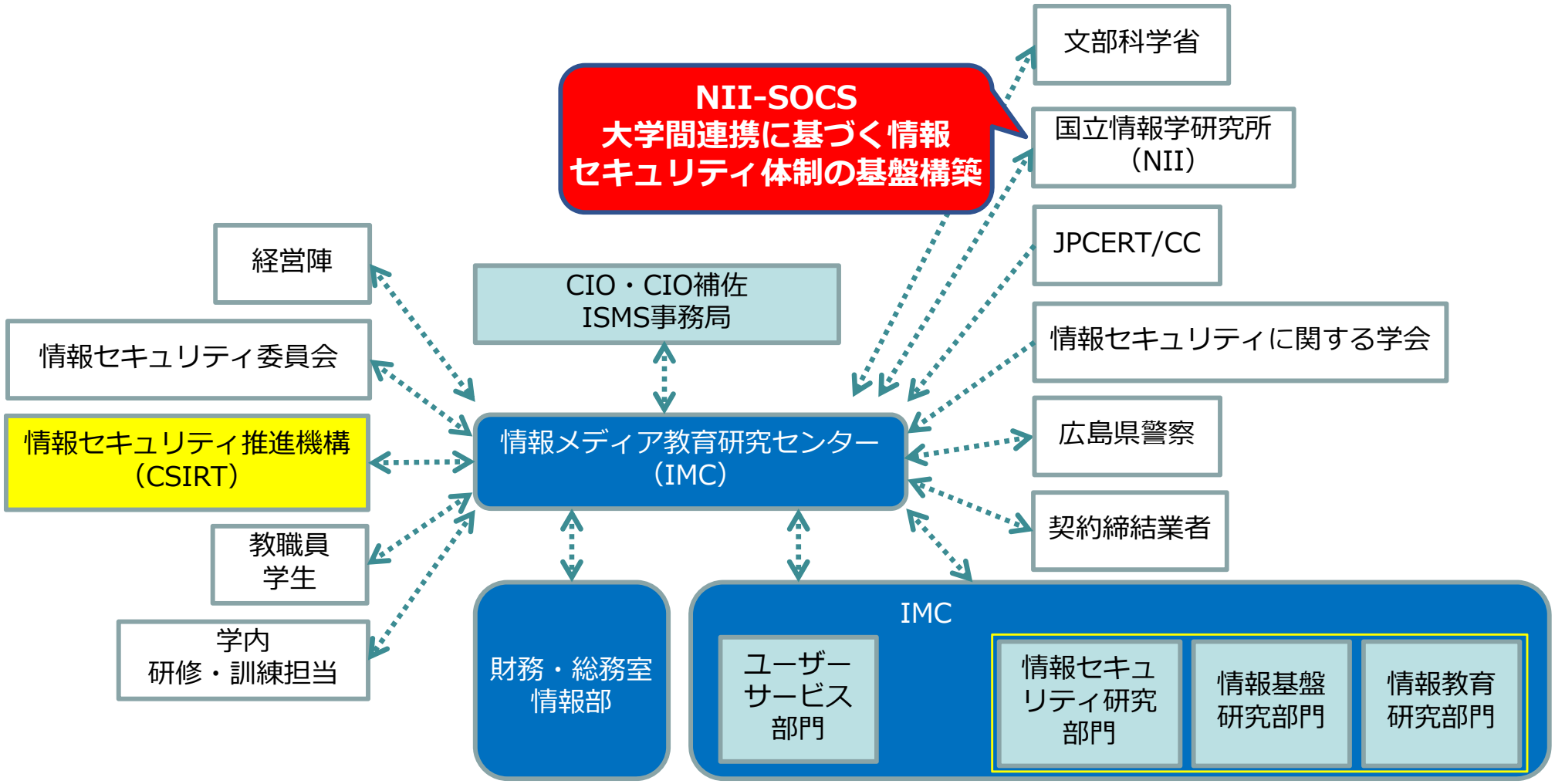
教職員向け情報セキュリティ研修

- 一般教職員向け（毎年9月頃実施）
  - Aコース：学内講師（6回・各40分～1時間）
    - 情報セキュリティに関する知識のアップデート
  - Bコース：学外講師（4回・各1.5時間）
    - スマートフォン及びタブレット端末の情報セキュリティ対策について（H24）
    - あなたは大丈夫？安全な暗号化のいろは～被害例から学ぶ～（H25）
    - 90分でわかる，危険なパスワード，安全なパスワード（H26）
    - 日常生活に潜むワナ　サイバー犯罪の手口から必要な対策を知る（H27）
    - マルウェア感染したパソコンの怪しい挙動を見つける～Windows編～（H28）
    - ランサムウェアと標的型攻撃の対策を知ろう（H29）
    - イマドキの攻撃手法とクラウドサービスの安全な利用方法（H30）
- 役員等向け（毎年9月会議内にて実施（15分程度））
  - 学内外でのインシデント発生状況
  - 電子メールやファイルの取扱い（情報漏えい対策）
  - インシデント対応訓練、など

広島大学における

インシデント対応

ISMS推進体制に見る利害関係者



NII-SOCSとは

広島大学

NII-SOCS発足の経緯

NII

- サイバーセキュリティ基本法における国立大学への要請(第32条)
  - 2018年秋国会で改正案審議(主に、オリパラ対応…)
- 中央省庁に加え、独立行政法人や府省庁と一体となり公的業務を行う特殊法人等を、内閣サイバーセキュリティセンター(NISC)の制度に基づく監視・監査の対象に追加する。
  - →独法は第2 GSOCで監視
- 国立大学法人固有の問題
  - 学生(民間人)の通信が混在
    - 学生と教職員でネットワーク論理分割が必須となるが…非現実的
  - 学問の自由との兼ね合い
  - 監視経費は各法人に請求(端末数、流量に比例)
    - 研究系独法と比べても桁違いな大学
      - 構成員数(端末数)、対外接続帯域
- 国立大学法人は自主的な対策強化へ
  - セキュリティ監視能力ではなく、インシデント対応能力の向上(5年計画)

「日本再興戦略」改訂2015
(2015年6月30日閣議決定)

大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

2

NII学術情報基盤ミーティング2018資料より

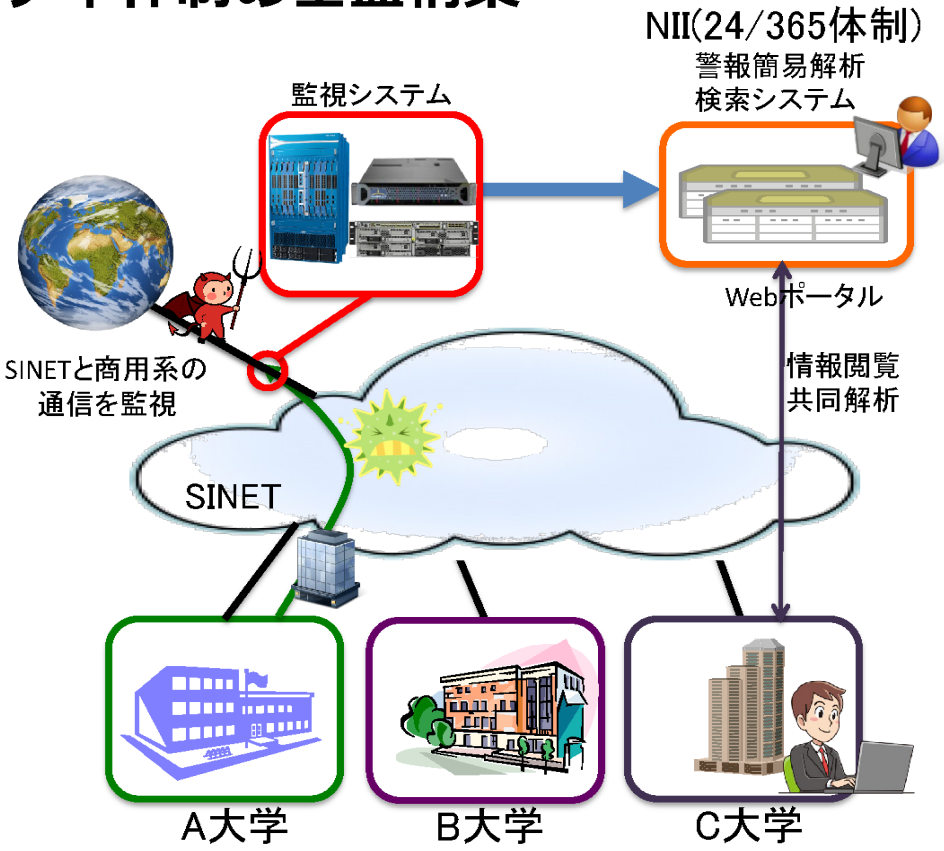
参考URL：https://www.nii.ac.jp/service/nii-socs/

NII-SOCSによる監視

NII-SOCSの監視体制

NII

- 大学間連携に基づく情報セキュリティ体制の基盤構築
  - 国立大学法人等の運営費交付金から拠出
    - 7.8億(2016)、8億(2017)、8億(2018)
      - 機能強化と予算圧縮を常に意識
  - 3種類の監視システム
    - Sandbox搭載IDS (paloalto)
    - シグネチャベースIDS (Cisco FirePower)
    - DNSトラフィック監視 (Damballa CSP)
  - 簡易解析システム＋Webポータル
    - 膨大な警報に緊急度・危険度の割付
  - 外部セキュリティ機関との情報共有
    - 国内：NDAに基づく攻撃情報の提供
      - サイバー攻撃拠点のNIIへの事前通知
      - NIIは通信の有無のみを回答
        - » セキュリティ機関：NISC経由で文科省へ
        - » NII：大学に直接通知
    - 海外：MoUに基づく技術情報の共有



大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

3

NII学術情報基盤ミーティング2018資料より
HiBiS IT勉強会
参考URL：https://www.nii.ac.jp/service/nii-socs/

NII-SOCSからの通知件数

２０１８年４月～９月末までの通知件数

NII

中項目		累計 (2018/4/1～9月末)
通知件数		3617
	分類１：マルウェア感染の可能性	2760
	分類２：アプリケーションソフトの脆弱性によるもの	225
	分類３：C&Cサーバーとの実通信の可能性	480
	分類４：ブルートフォース攻撃の可能性	0
	分類５：辞書攻撃の可能性	0
	分類６：標的型サーバー攻撃に関与している可能性	0
	分類７：man-in-the-middle 攻撃	0
	分類８：DNS Amp 攻撃への参加	0
	分類９：その他	152
誤報件数		2

大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

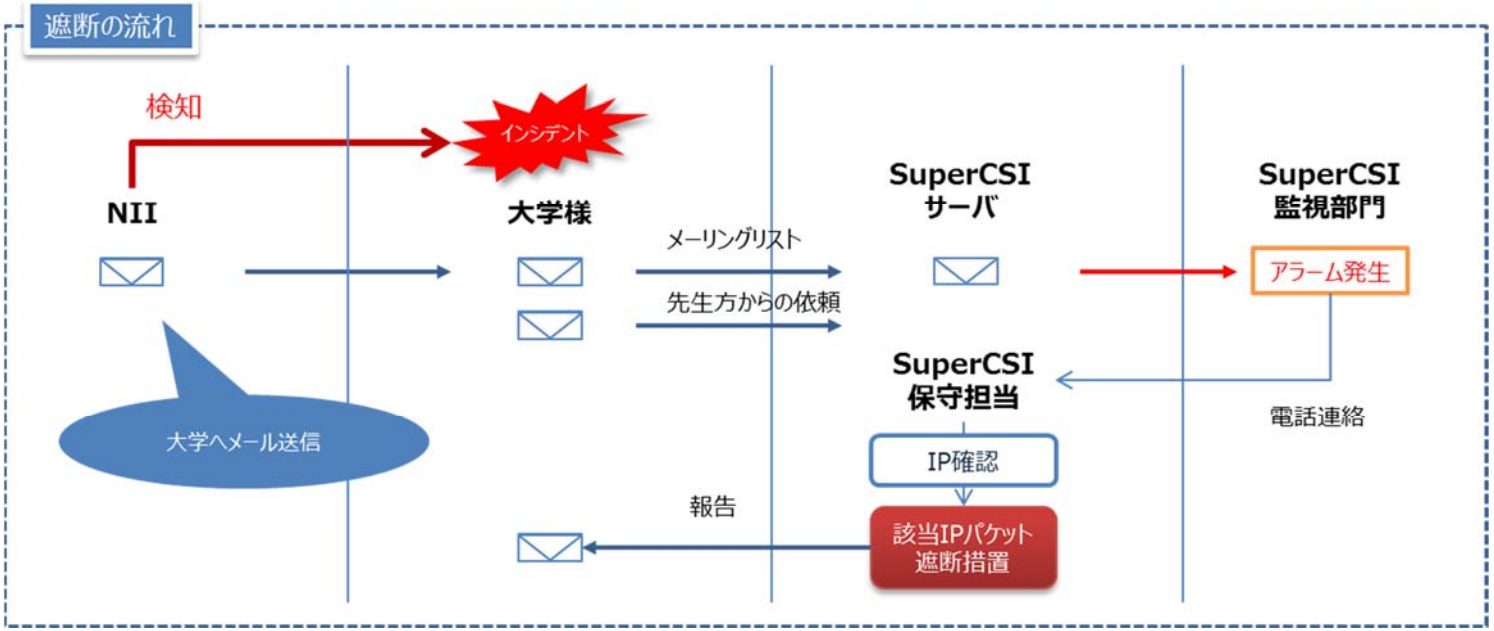
4

NII学術情報基盤ミーティング2018資料より

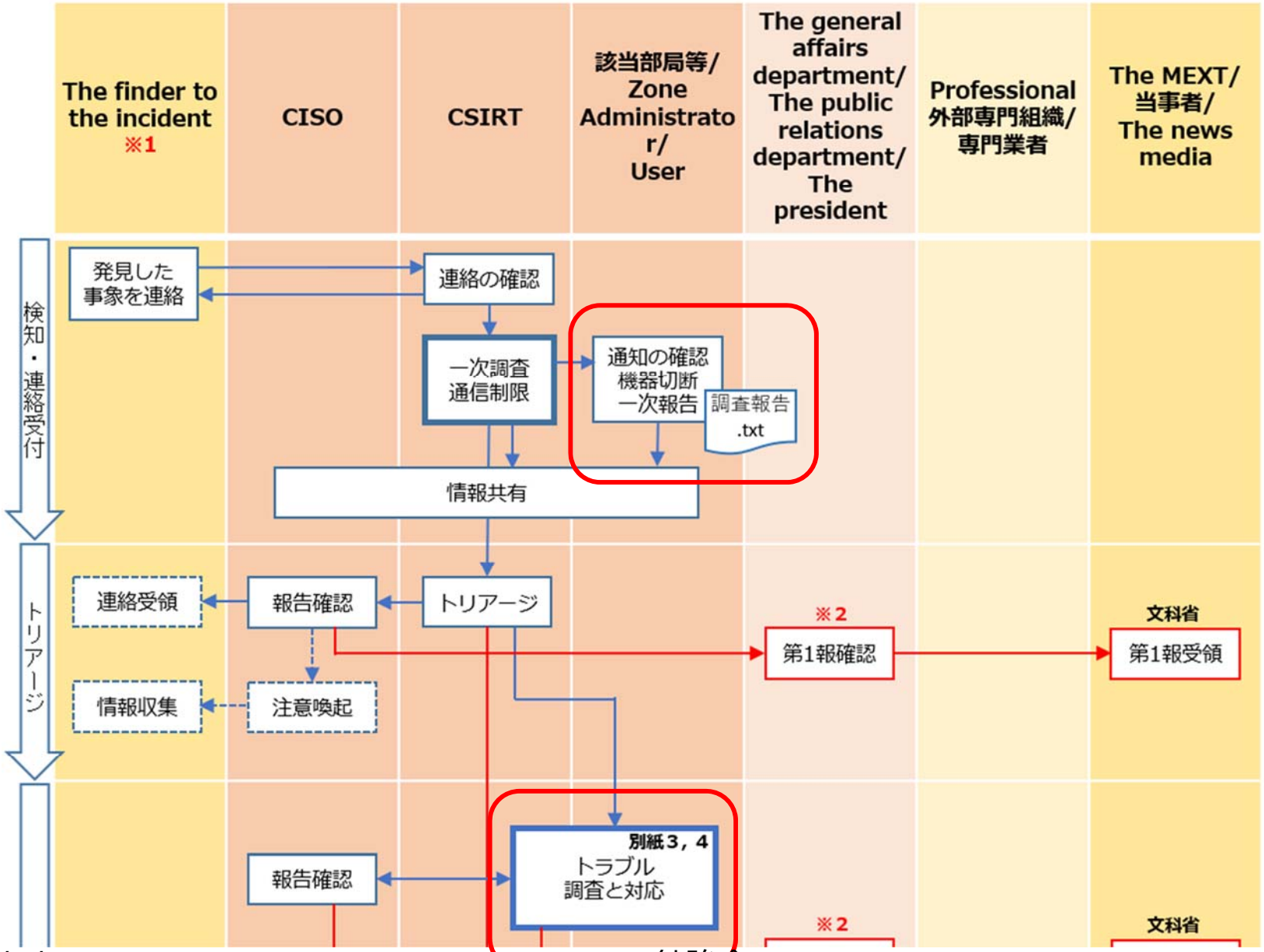
参考URL：https://www.nii.ac.jp/service/nii-socs/

インシデント一次対応体制

- 「大学間連携に基づく情報セキュリティ体制の基盤構築」事業
  - サイバー攻撃に対し、国立大学法人等と国立情報学研究所（NII）が連携し、以下の事業を実施する
    - 重大なサイバー攻撃の検知及び情報提供
    - サイバーセキュリティ人材の育成
  - 試行運用：平成29年3月～6月末、正式運用：平成29年7月～
  - 「要確認情報」の通知
    - 試行運用期間中：14件
    - 誤検知（false positive）なし → 「信頼できる情報」として通信遮断情報に利用



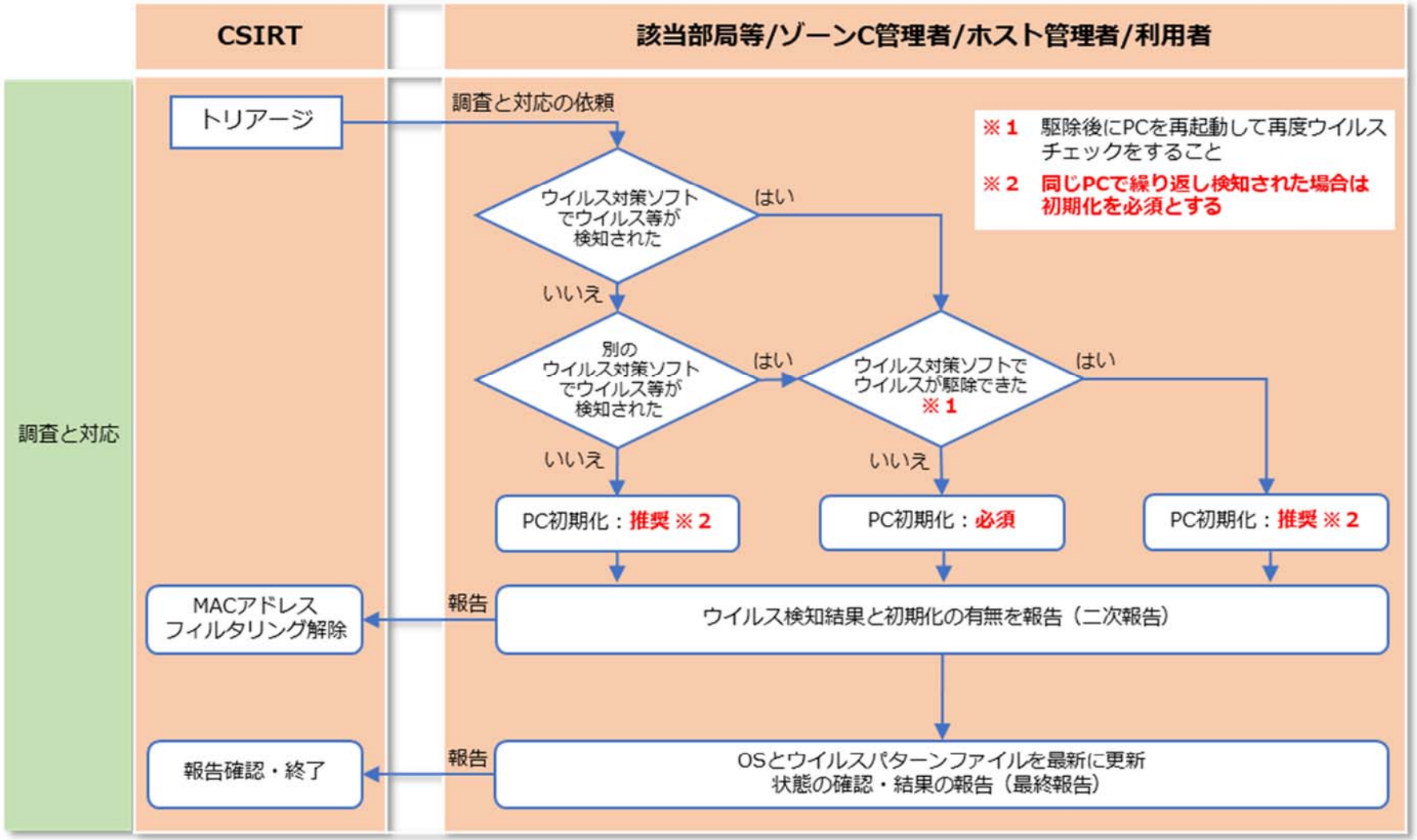
インシデント対応フロー



一次報告（調査報告.txtの内容）

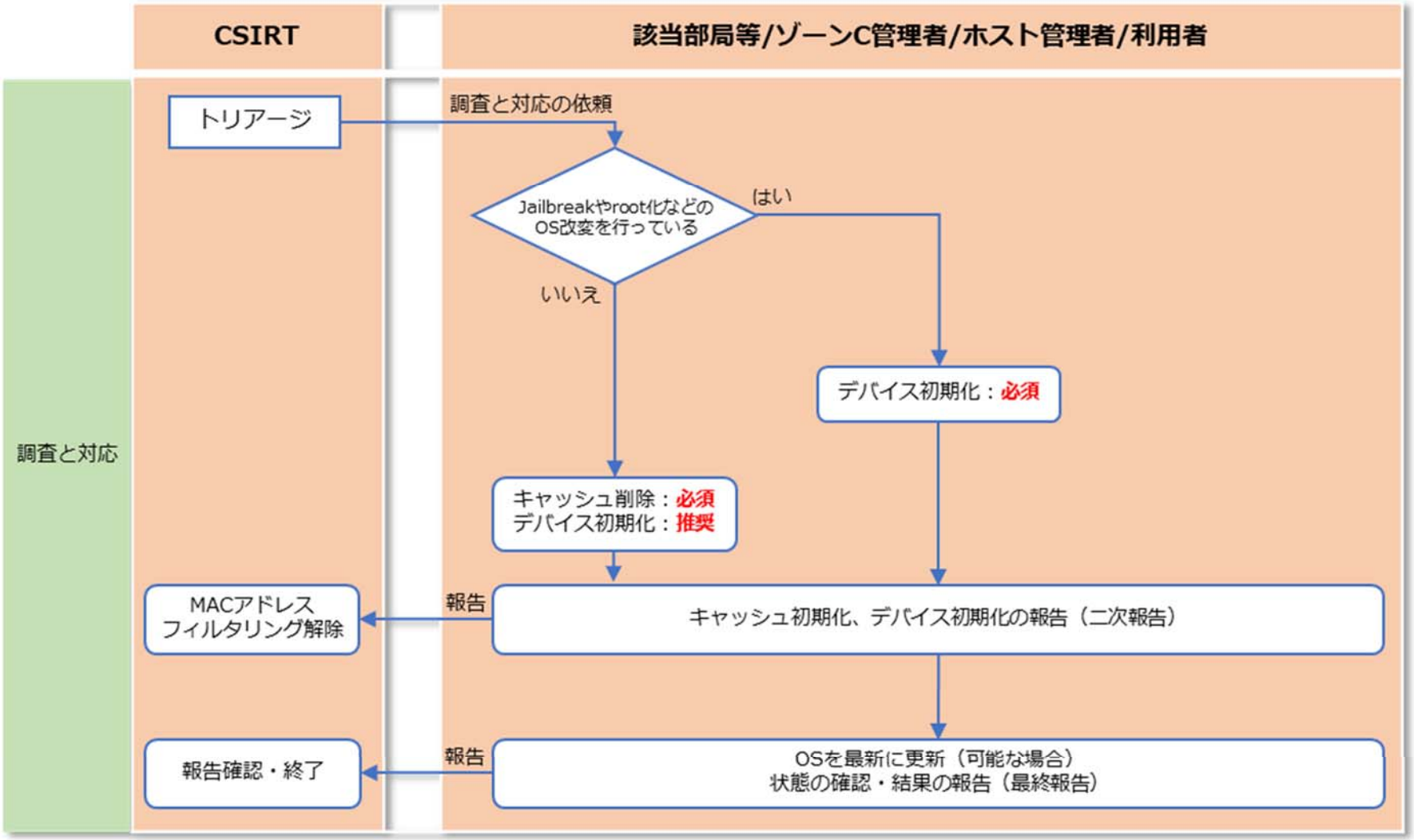
- 該当するコンピュータの利用目的
  - 共同利用や出張時使用など
- 該当するコンピュータの形状
  - コンピュータの種類、メーカ、型番など
- 該当するコンピュータの使用状況
  - OSの種類とbit数、OSの最終更新日、ウィルス対策ソフト名、パターンファイルの最終更新日、最終スキャン日など
- ウィルススキャンの結果
  - フルスキャン時の検知の有無、検知された場合のウィルス名や駆除状況など
- 暗号化されて開けないファイルの有無
- 該当するコンピュータに保存されている情報
  - 個人情報や法人文書などのデータの有無、データの内容、暗号化の有無など
- フリーソフトのインストール状況
- 指摘された原因
  - 思い当たる事象など
- 今後の対策
  - 初期化、ソフトウェア更新、フルスキャン実施など

トラブル調査と対応（PCの場合）



注意：該当機器がブロードバンドルータ（Wi-Fiアクセスポイントをルータモードで使用している場合を含む）の場合は、その配下に接続されたすべての機器（該当日時に停止していた機器は除く）について上記のフローを適用すること。

トラブル調査と対応（スマホ/タブレットの場合）



注意：該当機器がブロードバンドルータ（Wi-Fiアクセスポイントをルータモードで使用している場合を含む）の場合は、その配下に接続されたすべての機器（該当日時に停止していた機器は除く）について上記のフローを適用すること。

広島大学における

訓練と成果

再掲：一次報告（調査報告.txtの内容）

広島大学

- 該当するコンピュータの利用目的
  - 共同利用や出張時使用など
- 該当するコンピュータの形状
  - コンピュータの種類、メーカ、型番など
- 該当するコンピュータの使用状況
  - OSの種類とbit数、OSの最終更新日、ウィルス対策ソフト名、パターンファイルの最終更新日、最終スキャン日など
- ウィルススキャンの結果
  - フルスキャン時の検知の有無、検知された場合のウィルス名や駆除状況など
- 暗号化されて開けないファイルの有無
- 該当するコンピュータに保存されている情報
  - 個人情報や法人文書などのデータの有無、データの内容、暗号化の有無など
- フリーソフトのインストール状況
- 指摘された原因
  - 思い当たる事象など
- 今後の対策
  - 初期化、ソフトウェア更新、フルスキャン実施など

いつでも自分で調査できるようになっておくことが重要！！

どのような標的型攻撃訓練を行うか？

広島大学

標的型攻撃の流れ

侵入前

1. **事前調査**
   - ターゲットの組織の情報を収集する
2. **侵入**
   - 標的型メールやWebサイト等を介してマルウェアに感染させる

侵入後

3. **攻撃環境整備**
   - C&Cサーバとの通信を確立する
4. **攻撃準備**
   - 対象の情報の特定や不正プログラムを仕掛ける
5. **攻撃遂行**
   - 対象の情報を搾取する

標的型攻撃の訓練

侵入方法毎の訓練

標的型メール訓練

【目的】怪しいメールを見極める力を養う
【効果】メールを介した不正侵入確率の低減

侵入後の訓練

インシデント対応訓練

【目的】事後対応力を養う
【効果】事後対応スピードの向上

標的型攻撃訓練の実施例

- **標的型メール訓練**
  - 一ツ橋大学：2012年に約200名の事務系職員に実施
    - 伊東史人，高見澤秀幸，佐藤郁哉，標的型攻撃メールの予防対策，学術情報処理研究，No.16, pp.100-110 (2012).
  - 岡山大学：2015年から約2600名の教職員に実施
    - 村上昌己，大隅淑弘，藤原崇起，岡田学昭，川上祐介，信江輝治，早竹昭人，稗田隆，標的型メール攻撃によるセキュリティインシデントへの対応訓練，第21回学術情報処理研究集会発表論文集，pp.49-56 (2017).
  - 一般企業：2007年から8社2958名が実施
    - JPCERT/CC　IT セキュリティ予防接種報告書 (2011).
- **インシデント対応訓練**
  - 岡山大学：2016年から協力可能な教職員19名に限定で実施
    - 同上
  - 広島大学：2017年に常勤教職員3,496名を対象に実施
    - 渡邉英伸，相原玲二，西村浩二，広島大学における情報セキュリティインシデント対応訓練，大学ICT推進協議会2017年度年次大会，WF2-4, pp.1-5 (2017).

インシデント対応訓練2017

広島大学

- 訓練の流れ
  - ① 事前教育
    - 標的型攻撃の脅威やインシデント発生時の対応手順等をLMSで学習
  - ② 対応訓練
    - 普段使用しているパソコンが被害を受けた想定
    - OSやウィルス対策ソフト、アプリケーションの設定状況を調査し、LMSで報告
  - ③ 結果報告
    - 事前教育受講状況、対応訓練実施状況で評価・報告（所属部局別）

学習

被害通知

調査

報告

- 対象者
  - 常勤教職員：3,496名（平成29年10月31日現在）
- 実施期間（～平成29年11月29日（水）23:59）
  - 事前教育：平成29年10月31日（火）～
  - 対応訓練：平成29年11月15日（水）～
- 実施状況
  - 事前教育：1,986名（56.8%）
  - 対応訓練：1,919名（54.9%）

←実施率高い？低い？

結果報告

インシデント対応訓練2018

広島大学

- 訓練の流れ
  - ① 事前教育
    - 標的型攻撃の脅威やインシデント発生時の対応手順等をLMSで学習
  - ② 対応訓練
    - 普段使用しているパソコンが被害を受けた想定
    - OSやウィルス対策ソフト、アプリケーションの設定状況を調査し、アンケートシステムで報告
  - ③ 結果報告
    - 事前教育受講状況、対応訓練実施状況で評価・報告（所属部局別）

学習

被害通知

調査

報告

- 対象者
  - 常勤教職員＋学生：20,184名（平成30年11月1日現在）
- 実施期間（～平成30年11月29日（木）23:59）
  - 事前教育：平成30年11月5日（月）～
  - 対応訓練：平成30年11月15日（木）～
- 実施状況
  - 事前教育：5,508名（27.3%）
  - 対応訓練：9,967名（49.4%）

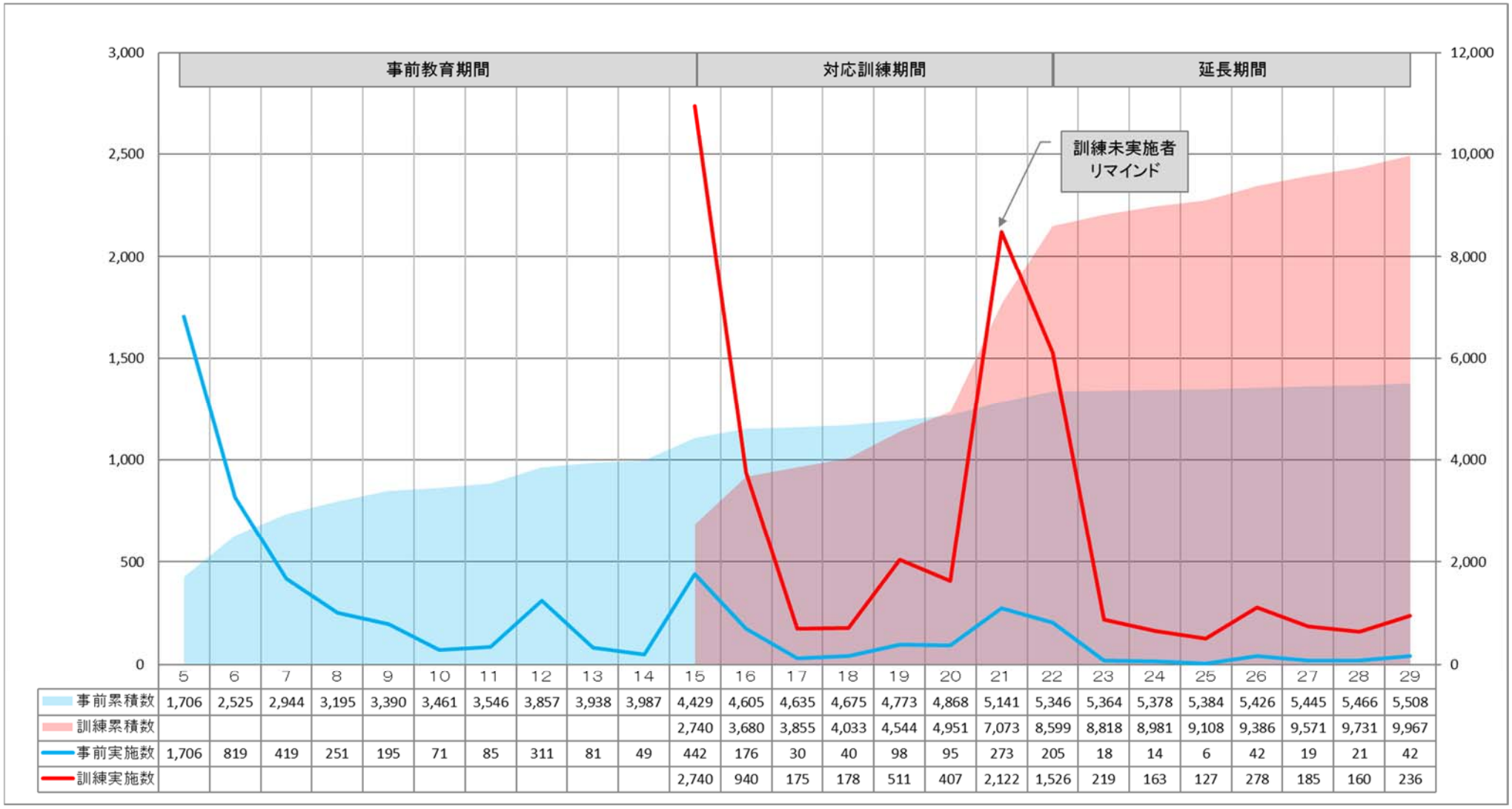
結果報告

昨年度との比較（教職員）→

年度		事前教育		対応訓練		対象者数
		実施数	実施率	実施数	実施率	
教員	2017年度	1,116	63.8%	1,153	65.9%	1,749
	2018年度	1,045	59.3%	1,568	88.9%	1,763
職員	2017年度	870	49.8%	766	43.8%	1,747
	2018年度	763	45.4%	1,087	64.6%	1,682
全体	2017年度	1,986	56.8%	1,919	54.9%	3,496
	2018年度	1,808	52.5%	2,655	77.1%	3,445

昨年度の対象者である，教員（大学教員，附属学校教員），職員（役員・一般職員，技術職員等，海事職員，看護職員，医療職員）に限って比較したもの。

事前教育・対応訓練実施数の推移



	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
事前累積数	1,706	2,525	2,944	3,195	3,390	3,461	3,546	3,857	3,938	3,987	4,429	4,605	4,635	4,675	4,773	4,868	5,141	5,346	5,364	5,378	5,384	5,426	5,445	5,466	5,508
訓練累積数											2,740	3,680	3,855	4,033	4,544	4,951	7,073	8,599	8,818	8,981	9,108	9,386	9,571	9,731	9,967
事前実施数	1,706	819	419	251	195	71	85	311	81	49	442	176	30	40	98	95	273	205	18	14	6	42	19	21	42
訓練実施数											2,740	940	175	178	511	407	2,122	1,526	219	163	127	278	185	160	236

本学で発生したインシデント等

広島大学

（年度）

2011 2012 2013 2014 2015 2016 2017 2018

インシデントは減少
トラブルは増加

不正アクセス

ワーム検知

その他

著作権侵害等

トラブル件数→
(2018/8/31現在)

パソコン・USB等紛失・盗難

まとめ

- 広島大学の規則や制度、情報セキュリティ推進機構（CSIRT）およびその関連組織で行っている活動（教育・研修、対応、訓練等)を紹介
  - 情報セキュリティポリシー、ISMS/ISMSクラウドセキュリティ認証
  - 情報セキュリティ・コンプライアンス教育、情報セキュリティ研修
  - NII-SOCSとの連携、インシデント対応フロー
  - インシデント対応訓練、インシデント発生状況
- CSIRTは自衛消防隊
  - 火消しだけでなく防火、教育・訓練も必要
  - 部署や組織単独ではなく、部署や組織を超えた連携が必要→NII-SOCS
  - 技術面の連携（ネットワークのセキュリティ強化）も必要
    - コストや人材確保・育成の課題も