シ ス テ ム 技 術 分 科 会 選 出
システム技術分科会 2015 年度第 1 回会合 より

広島大学におけるパブリッククラウド活用事例 ～クラウド化がもたらす本当の効果～

相原 玲二
(広島大学)

サイエンティフィック・システム研究会（2015 年 9 月 1 日）

広島大学におけるパブリッククラウド活用事例

～クラウド化がもたらす本当の効果～

広島大学　相原玲二

広島大学では 2014 年以来，財務会計システム，人事給与システム，公式ウェブサイト，事務用メールシステム，全構成員用メールシステムなどの基幹情報システムを順次パブリッククラウドへ移行した．さらに，2015 年 9 月より稼働する教育研究用電子計算機システムでもパブリッククラウドを積極的に利用している．

１．なぜ事務用システムから移行を開始したか

大学の情報技術を利用するシステムはその目的によりいくつかのカテゴリに分けることができる．中心的なものとしては事務基幹業務，教育支援，研究支援があり，その他に規模の大きなものとして学術情報（図書館関係），医療情報（大学病院関係）がある．

これらシステムのクラウド移行には，それぞれ微妙に質の異なる壁がある．本学では以前から事務基幹業務のためのシステム（事務用システム）は経費節減と効率的な運用を目指して，複数のアプリケーション（財務系，人事系など）を１つの部署（情報化推進グループ）が窓口となり導入していた．既に，多くのアプリケーションがオンプレミスの仮想サーバ上で稼働し，各アプリケーションの保守等は対応可能なベンダに対しそれぞれアウトソースしていた．すなわち，IaaS のパブリッククラウドを利用したとしても，契約形態にほとんど変化は無い．

本学では 2001 年より，通信事業者のデータセンターを借用し，認証システムなど一部の重要なシステムをキャンパス外に設置し運用してきた．そのため，本学の情報セキュリティポリシーには，システムの設置場所の地理的位置に関する制限は設定されてなかった．さらに，事務用システムのハードウェア仕様は導入担当部署を中心に決定していたため，クラウド移行に対する壁は低かったが，担当者は躊躇した。クラウドサービス利用ガイドラインは，担当者や責任者の決断の後押しをした．

２．なぜプライベートクラウドを採用しないか

本学は 2001 年よりデータセンターを借用し，主要キャンパスとの間に十分な芯数の光ファイバを設置し，一部のシステムをデータセンター内に設置し運用してきた．この運用経験を通してデータセンターハウジングのメリットとデメリットを理解することができた．一方，事務用システムなどはオンプレミスの仮想サーバを利用した運用も行ってきた．

これらの経験から，単にオンプレミスのシステムをデータセンターに移すだけではコスト高になること，大規模災害等を考慮して異なるデータセンター間でのバックアップを実施する場合さらなるコスト高を覚悟しなければならないことなどを実感していた．

プライベートクラウド構築により，クラウド技術の研究開発を行いその成果を社会へ還元することは

意義深いが，我々にはその余裕が無かった．ただ，2015 年 9 月より稼働する教育研究用電子計算機システムでは占有型パブリッククラウドによる提供を求めたため，本件の落札業者はクラウド構築・運用に関してスキルアップするものと期待する．

３．パブリッククラウド導入効果と課題

システム全体の経費を考えると，パブリッククラウドを導入したからと言って大幅なコスト削減効果は期待できない．本学では，財務系システムや公式ウェブサイトは IaaS を直接契約し，人事系システムはアプリケーションベンダが IaaS を契約することにより本学は SaaS として契約している．また，事務用メールシステムと全構成員用メールシステムは SaaS を利用している．それぞれの利用形態ごとにクラウドによる経済効果が出てはいるが，必要に応じてインスタンスの最適化を図り，不要なものを停止するなど，大学側の管理者が構成や課金体系を理解した上で注意を払っておく必要がある．

管理の手間については，手元に置くハードウェアが減るため軽減される．ただし，経費を最適化するため IaaS を直接管理する場合は，インスタンスの最適化や必要に応じた構成変更などが必要となり，これまでとは質の異なる管理が必要となる．それらを大学の教員や技術職員が実施する場合，改めて人材育成が必要となるが，それほどハードルは高くない．どのようなクラウドベンダを選択するかにもよるが，データセンターに設置されたシステムを利用していること，ハードウェア更新の心配が不要であること，基本的なバックアップ機能が備わっていることは，管理者の精神的負担を大幅に軽減する．

これまではシステム一式を 4〜5 年毎に更新するということが大学等においては常識だったが，パブリッククラウドの利用が進むと，大きく変わる可能性を持つ．4〜5 年に 1 度の更新は元々ハードウェアの寿命や技術進歩などが理由だと思われるが，パブリッククラウドであれば必要に応じて短期間での契約変更も行うことができる．むしろ，それをしないと無駄な投資となる．一方，アプリケーションソフト等のライフサイクルはハードウェアの寿命とは独立であり，個々のアプリケーションソフト毎に最適なライフサイクルで更新や機能追加を行う，という方向になる．また，同じクラウドベンダで動作しているのであれば，オンプレミスの時代とは異なり，他大学とのアプリケーション共同利用の可能性も各段に広がるだろう．クラウド化がもたらす本当の効果はここにある．

広島大学における パブリッククラウド活用事例

～ クラウド化がもたらす本当の効果 ～

相原玲二

広島大学　副理事（情報担当）

情報メディア教育研究センター長

2015年9月1日　サイエンティフィック・システム研究会

広島大学

概要

広島大学

- なぜ事務用システムからクラウド化したか？
  - 大学の情報システムの課題
  - クラウドサービス利用ガイドライン
- なぜプライベートクラウドを採用しないか？
  - 経費増加、管理コスト、研究成果を社会に還元
- パブリッククラウド導入効果と課題
  - 経費削減、総合的な安全性、調達の枠組み変更

なぜ事務用システムから クラウド化したか？

大学の情報システムの課題
クラウドサービス利用ガイドライン

広島大学

国立大学における情報基盤整備

広島大学

- 法人化前（　～2003年）
  - **教育研究用、事務用、学術用（図書館）**：　レンタル経費（目的別）
  - **キャンパスネットワーク**等：　一時的経費（補正予算等）
- 法人化後（2004年～　）
  - レンタル経費　→　運営費交付金（一般経費）
    - 各大学の裁量で執行可能となったが、毎年削減
  - 一時的経費　→　運営費交付金（特別経費）
    - 基盤整備の目的には配分なし
- 最近の傾向
  - **追加設備（LMS、eポートフォリオ、研究者総覧、労務管理）増加中**
  - **セキュリティ対策、事業継続計画（BCP）への対応が求められる**

国立大学における情報基盤整備

広島大学

- 法人化前（　～2003年）
  - 教育研究用、事務用、学術用（図書館）：　レンタル経費（目的別）
  - キャンパスネットワーク　　経費（補正予算等）
- 法人化後（2004年～　）
  - レンタル経費　　経費（毎年削減）
  - 一時的経費　→　運営費交付金（特別経費）
    - 基盤整備の目的には他ならない
- 最近の傾向

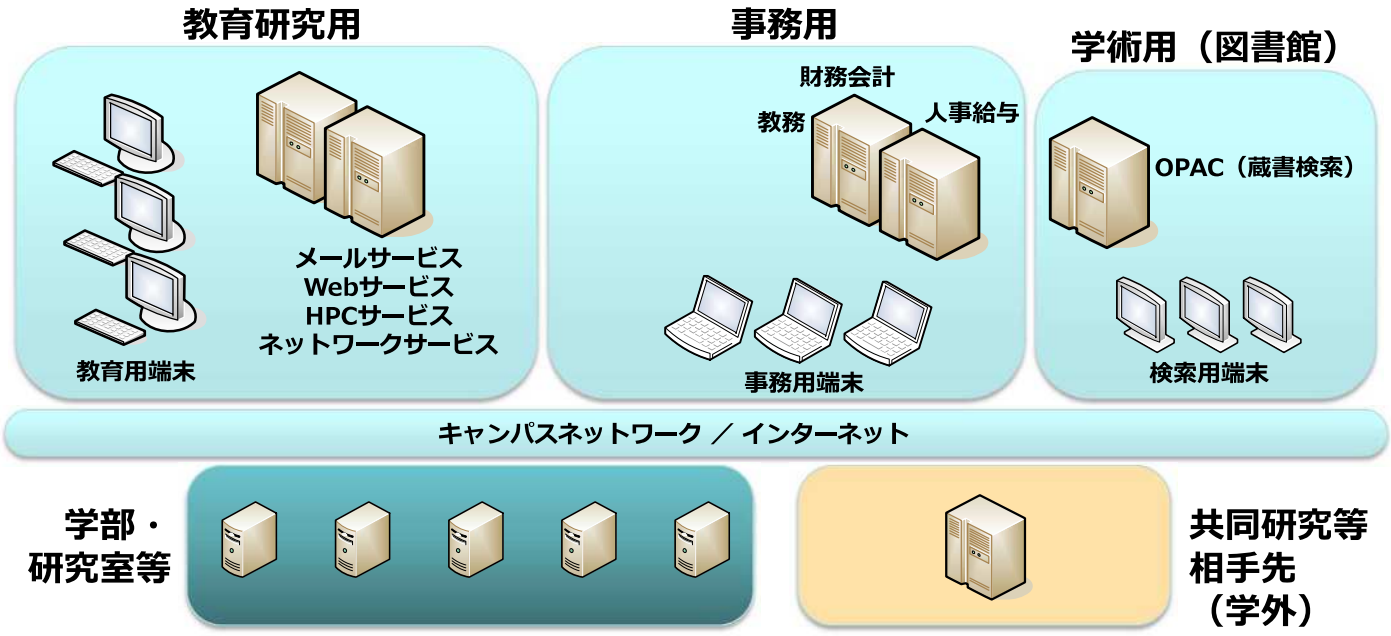
パブリッククラウドの活用

壁

  - **追加設備（LMS、eポートフォリオ、研究者総覧、労務管理）増加中**
  - **セキュリティ対策、事業継続計画（BCP）への対応が求められる**

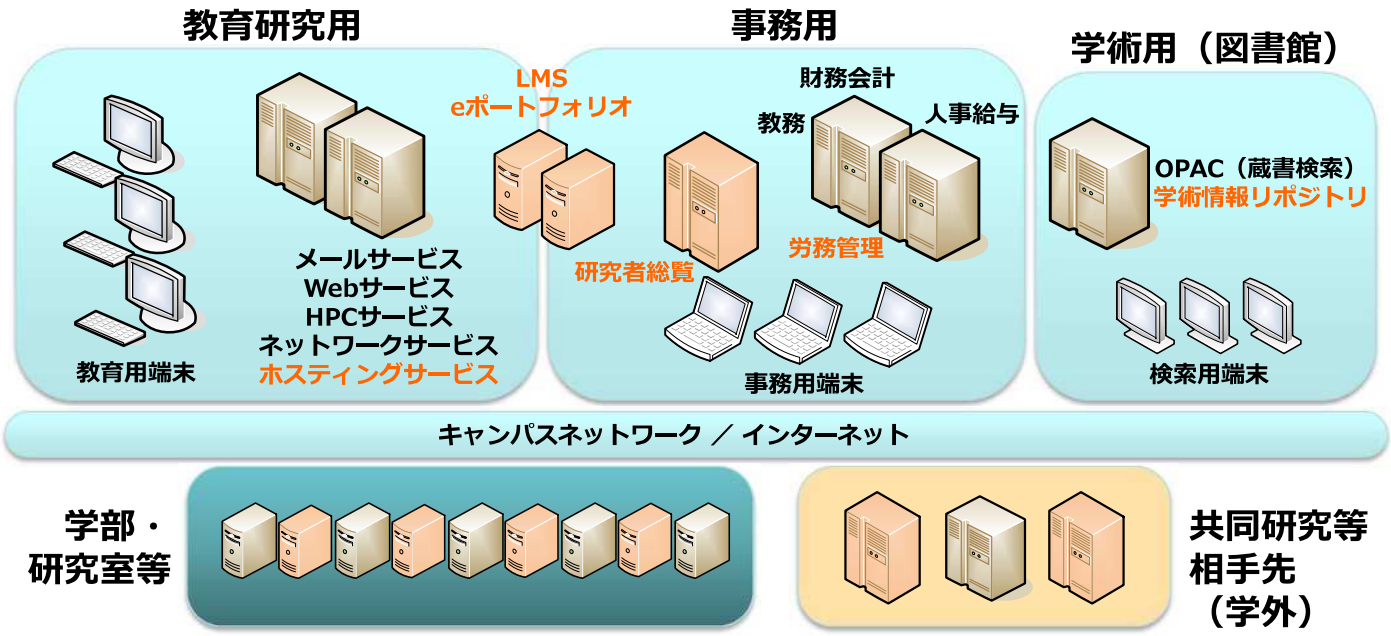
大学の情報システム（15年前）

広島大学



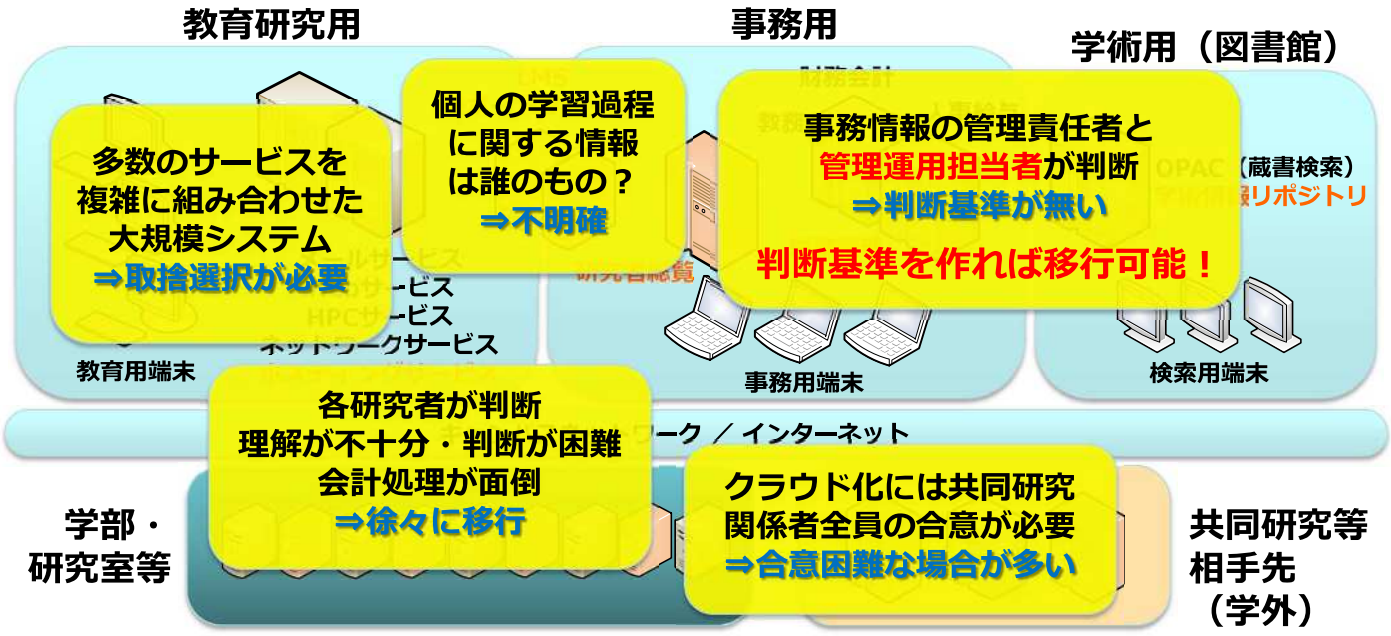
大学の情報システム（現在）

広島大学



大学の情報システム パブリッククラウド化の壁

広島大学



広島大学のクラウド化手順

広島大学

- **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
    - 運用上注意すべき部分が明確化
    - オンプレミスの場合も同様の手順は必要
  - **担当者レベルで確認・判断することが可能！**
- 財務会計システム、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！**
  - 事務用システムの心臓部がクラウド化完了

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	ガイドラインチェック項目
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：	・広島大学クラウドサービス利用基準を理解していますか？
	(2)業務の継続性の保証	・クラウド事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				・クラウドサービス契約終了時の代替手段を検討しましたか？また、それは妥当か？
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				・サービス停止時間は確認しましたか。その内容は妥当ですか？

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年（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

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
    - パブリック？　プライベート？　オンプレミス？
  - 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（2005年4月1日）
    - http://info.office.hiroshima-u.ac.jp/policy/index.html（学内限定）
  - 2011年度頃から問合せが急増
    - 「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」
- 2012年度　1年間をかけて検討
  - 具体的、わかりやすい、実行可能

ガイドラインの課題

広島大学

- 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
  - ガイドラインの定期的見直し
    - 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
  - 定期的な再チェック
    - クラウドサービスは仕様が頻繁に変更される
  - チェックリスト確認結果の提出義務化
- 2015年8月改定（予定）

なぜプライベートクラウドを採用しないか？

経費増加

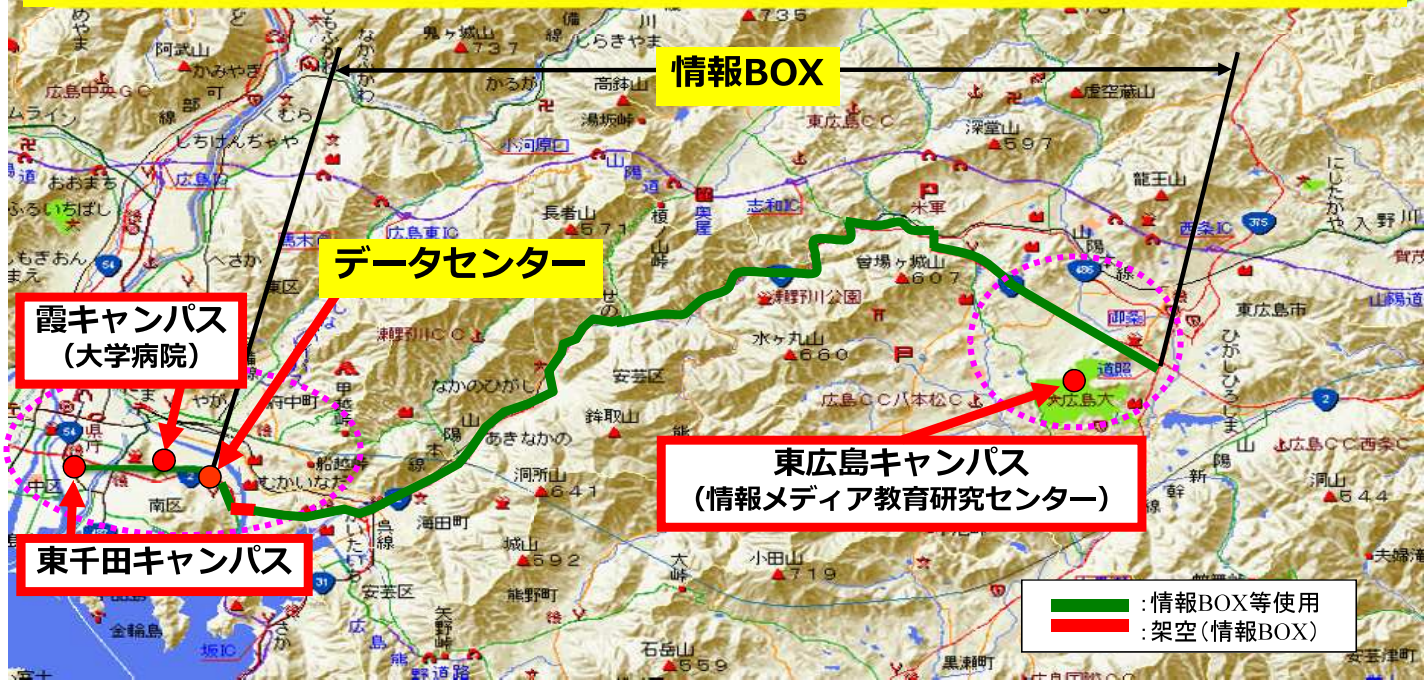
管理コスト

研究成果を社会に還元

広島大学

広島大学

広島大学自設光ファイバ【東広島市～広島市】　2001年度



データセンターの利用（１）

広島大学

- 主要キャンパスとデータセンター間の自設光ファイバ
  - 2001年度運用開始
  - SINET3接続、JGN接続等に活用
- サーバ等の設置
  - 全学認証システム等
  - キャンパスネットワーク基幹（L3 / FW / IPS等） 2014年～
  - 計算機システムの一部（ファイルサーバ等） 2015年～

- **必要性を十分精査しなければ経費は増加！**

データセンターの利用（２）

広島大学

- 利用上の注意（常識）
  - 普段の活動場所から遠い
  - 原則として事前の入室手続きが必要
  - ラック以外に物品の置き場所はない
- 設計上の注意
  - 電源と空調以外は自力で設計、保守が必要
  - データバックアップ、装置の冗長化は必要に応じて準備する
  - 大学までの通信回線の経費、冗長化について対応が必要
- **管理コストはオンプレ以上！**

研究開発の成果を社会に還元

広島大学

- パブリッククラウドにない新機能を実証可能
  - 研究成果として発表
- 経験の乏しい（地方の）技術者のスキルアップ

余裕ができたら挑戦したい

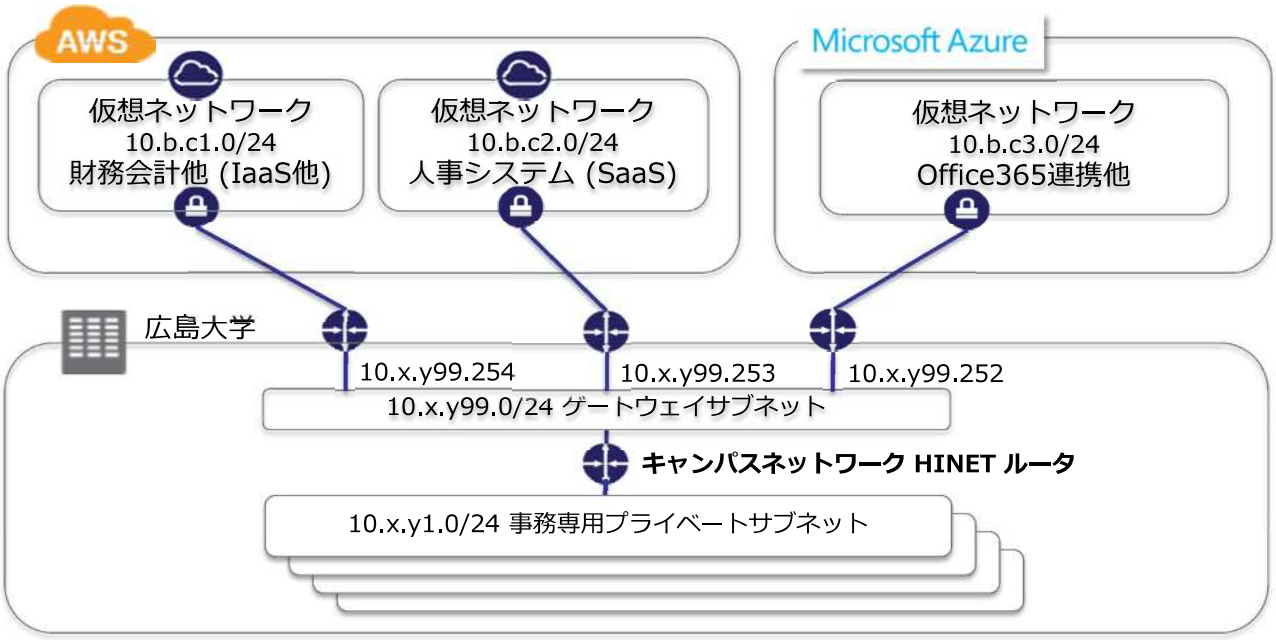
パブリッククラウド導入効果と課題

経費削減
総合的な安全性
調達の枠組み変更

広島大学

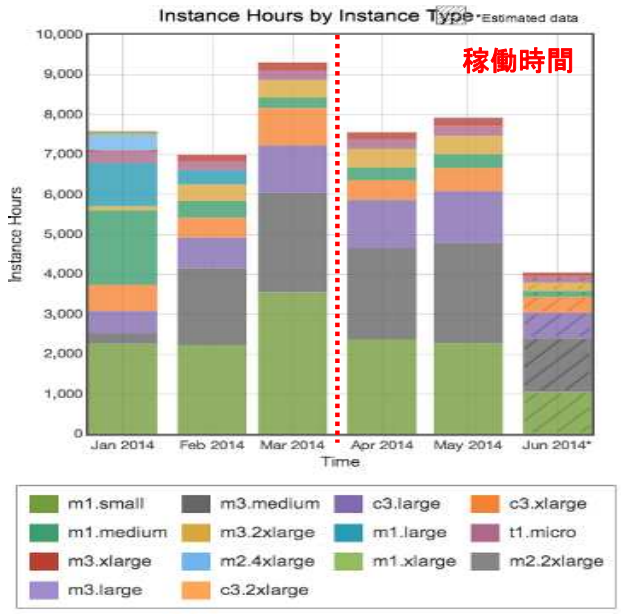
運用中のネットワーク構成（一部）

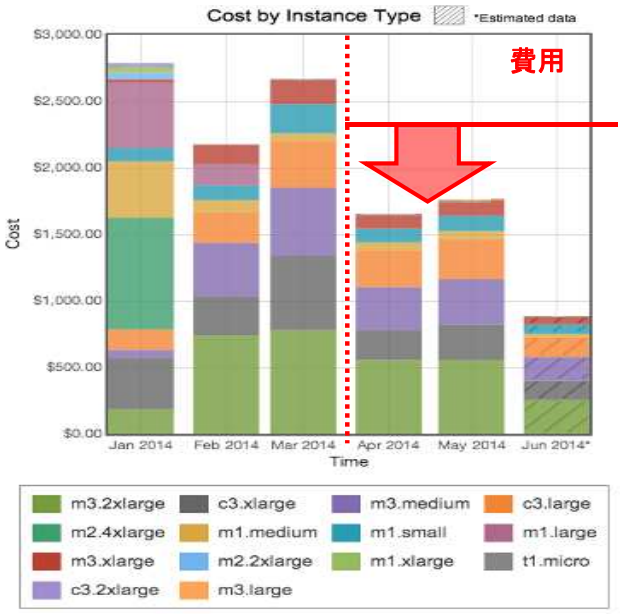
広島大学



料金改定（2014/4/1）による経費削減

広島大学

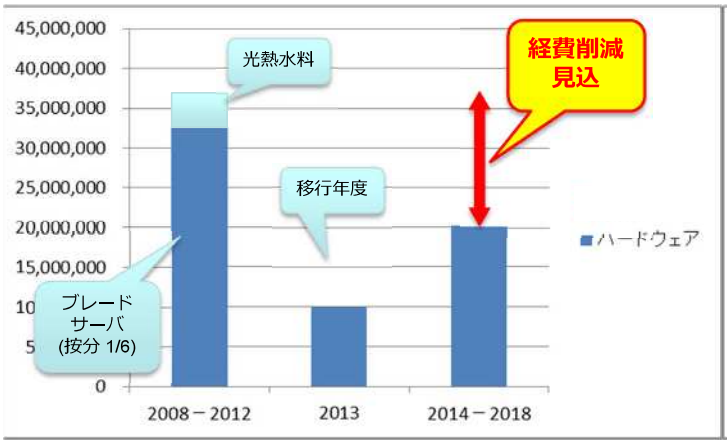


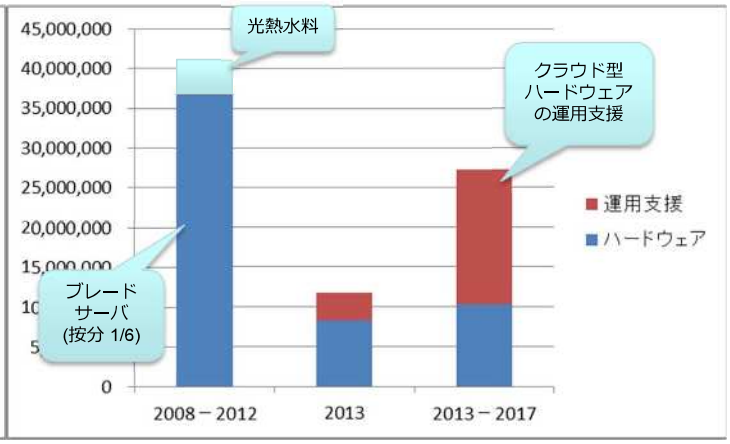


経費変化（サーバ ハードウェア）

広島大学

- 財務系（SAP／ベニック）IaaS
- 人事系（ワークス）SaaS





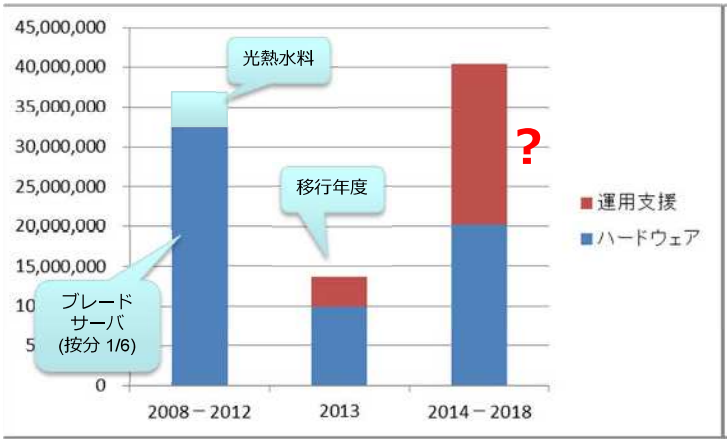
財務会計、学納金、会計支援、出張旅費

人事、給与、健康診断管理、労務管理

経費変化（サーバ ハードウェア）

広島大学

- 財務系（SAP／ベニック）IaaS→SasS
- 人事系（ワークス）SaaS



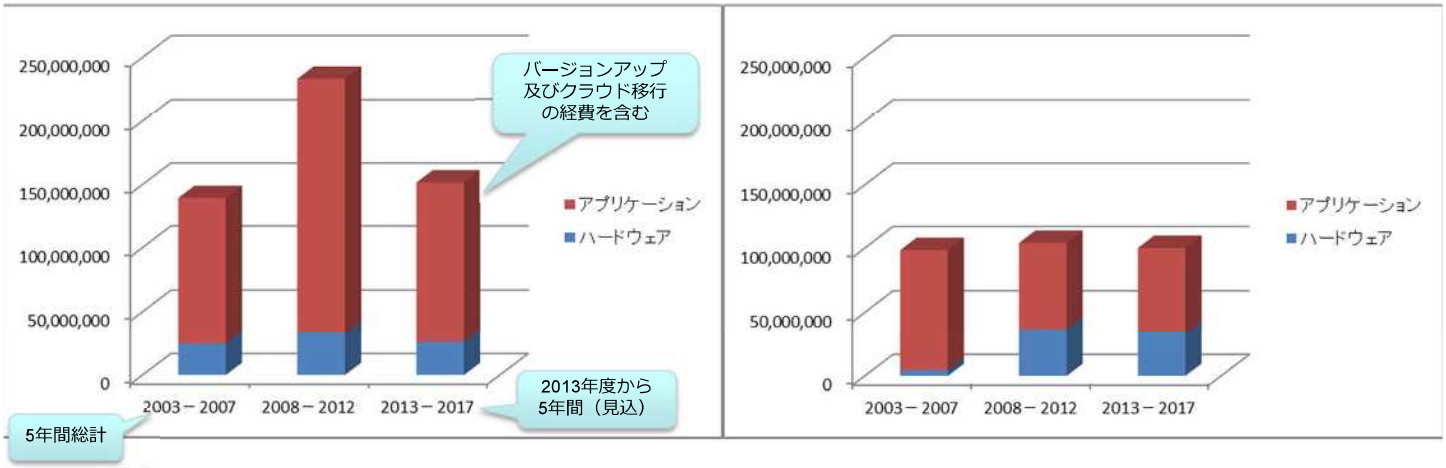
財務会計、学納金、会計支援、出張旅費

人事、給与、健康診断管理、労務管理

経費変化（サーバ 全体）

広島大学

- 財務系（SAP／ベニック）**IaaS**
- 人事系（ワークス）**SaaS**



財務会計、学納金、会計支援、出張旅費

人事、給与、健康診断管理、労務管理

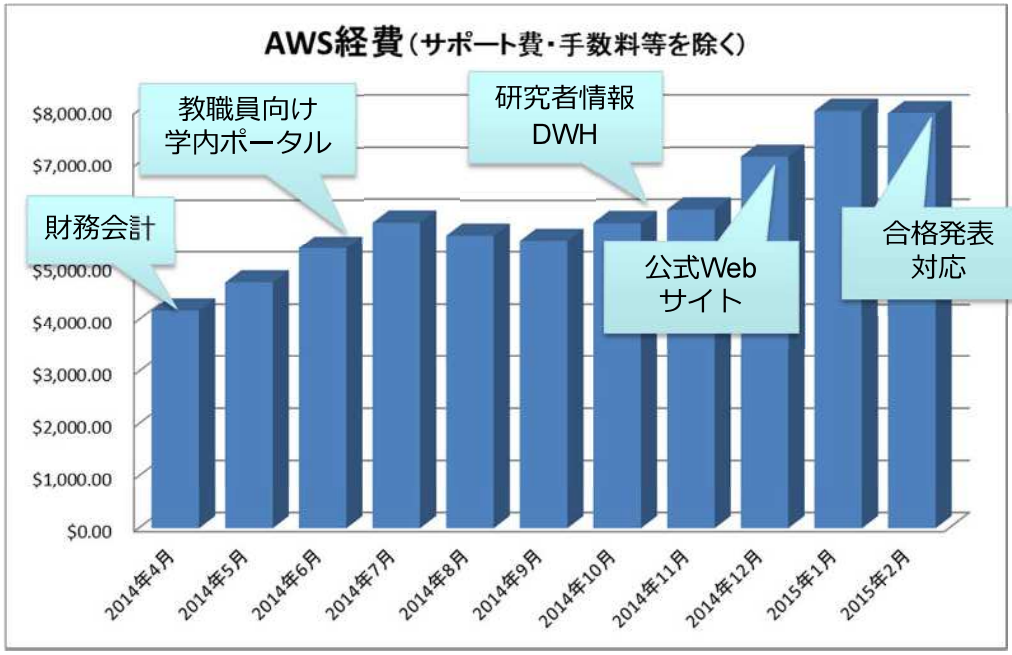
主なパブリッククラウド利用

広島大学

- AWS 広島大学公式Webサイト
  - 合格発表を含む
- Office 365 Microsoft Azure 全構成員（教職員・学生）用メールシステム
  - 2015年3月より移行開始
- AWS 研究者総覧・研究力分析システム
  - 新システム運用開始（準備中）
- SaaS インターネット出願サービス
  - 2015年度学部一般入試から導入（H27年度：約20%）

クラウド利用経費の変化

広島大学



SaaS
・人事給与
・機関リポジトリ
等を除く

パブリッククラウド導入の効果

広島大学

- 堅牢性、柔軟性、総合的な安全性
  - チェックリストからオンプレミスの問題点が浮き彫りに！
- （一般的な）パブリッククラウドなら
  - データセンターに設置されたシステムを利用
  - ハードウェア更新等の心配は不要
  - 基本的なバックアップ機能を具備

- **管理者の精神的負担を大幅に軽減！**
  - 上司（責任者）は心配で夜も眠れないかも？

パブリッククラウド導入効果と課題

広島大学

- オンプレミスやプライベートクラウド
  - ハードウェアのライフサイクル（4～5年）でシステム一式更新
- **パブリッククラウドを利用した場合**
  - ハードウェアの更新や増強時期を自由に設定可能
  - 必要な機能を必要な時に追加・変更　　**⇒実施すべき**
  - 各アプリケーションソフトのライフサイクルで更新、機能追加
  - ソフトウェア共通化による他大学等との共同利用促進

- **システム構築（IT投資）見直しの契機**

まとめ

広島大学

- なぜ事務用システムからクラウド化したか？
  - 大学の情報システムの課題
  - クラウドサービス利用ガイドライン
- なぜプライベートクラウドを採用しないか？
  - 経費増加、管理コスト、研究成果を社会に還元
- パブリッククラウド導入効果と課題
  - 経費削減、総合的な安全性、調達の枠組み変更

クラウド化がもたらす本当の効果は！？

シ	ス	テ	ム	技	術	分	科	会		選	出
システム技術分科会 2015 年度第 2 回会合 より											

東工大 CERT の立ち上げと現在の取り組み

松浦　知史
(東京工業大学)

2016年1月18日

サイエンティフィック・システム研究会
システム技術分科会　2015年度第2回会合

東工大CERTの立ち上げと現在の取り組み

東京工業大学　学術国際情報センター　准教授
松浦知史

・要旨
　組織内CSIRTの重要性が叫ばれている。攻撃手法は高度化/多様化し続けており、学内のサービス担当者が片手間でセキュリティ情報を収集し、適切な運用を行い、問題発生時には初動対応を行うといった事は到底望めない。情報セキュリティの専門チームと現場担当者が協力し安全な環境を構築して行く事が求められている一方で、実際の組織立ち上げには多くの課題が山積している。

　実行力のある組織を構築するためには、適切な権限、人材、機材、予算またそれを支えるトップ層を含む学内の理解が必要である。しかし権限一つ取っても、権限を規定するための学内規則の変更、権限の必要性に関する全学への説明が必須であり、場合に寄っては権限を定める過程で抵抗や反発も発生しかねない。新規のセキュリティに関する施策や予算獲得を行う際にも安全性、必要性、効果とコストのバランスなど幅広い観点でトップ層から現場担当者まで様々な立場の方々に説明し、説得する必要がある。

　本公演では東工大CERTの立ち上げ時期を中心に上記の様な課題に対して、どのように行動し、どのように説得してきたかを紹介する。また、インシデントレスポンスの事例や次世代型ファイヤフォールの導入など現在の活動内容も併せて紹介する。

東工大CERT
Tokyo Tech Computer Emergency Response Team
http://cert.titech.ac.jp

東京工業大学
Tokyo Institute of Technology

東工大CERTの立ち上げと現在の取り組み

東京工業大学 学術国際情報センター
松浦知史 (MATSUURA Satoshi)
matsuura@gsic.titech.ac.jp

東京工業大学
Tokyo Institute of Technology

松浦 知史 (MATSUURA Satoshi)
東京工業大学 学術国際情報センター
東工大CERT 統括責任者 (准教授)

- 東工大CERT立ち上げ前の主な活動
  - セキュリティ教育
    IT-Keys / SecCap
  - 研究活動
    geographical overlay network, large scale sensor networks, distributed Pub/Sub, DTN

東京工業大学
Tokyo Institute of Technology

本日の話題

東工大CERT
Tokyo Tech Computer Emergency Response Team

http://cert.titech.ac.jp

の設立過程、活動を例に

・なぜセキュリティ専門チームが求められているか
・どのようにしてセキュリティ専門チームを作っていったか
・どんな活動をしているか。今後の活動はどのようなものか

東京工業大学
Tokyo Institute of Technology

最近のニュース

2014年04月17日 08時00分 更新

標的型攻撃に変化、狙いは経営幹部から役員秘書に

Symantecが取りまとめた2013年の脅威動向によると、標的型攻撃では従来と異なる特徴がみられるようになった。

[ITmedia]

標的型攻撃で狙われるのは大企業や幹部――従来にみられたこうした特徴に変化が生じているという。シマンテックが4月16日に公開した最新版のインターネットセキュリティ脅威レポートで明らかになった。

同レポートは2013年のセキュリティ脅威動向を取りまとめたもの。企業に関する注目点では大規模なデータ侵害事件が多発していることや、標的型攻撃の傾向に変化がみられていることなどを挙げている。

標的型攻撃ではメールを使った攻撃の発生件数が2012年比で91%増の779件に達した。一方、1つの攻撃キャンペーンに使われるメールの数や受信者の数は減少した。キャンペーンあたりの攻撃期間は2011年平均4日から2013年は同8.3日と、2倍以上に長期化している。このことから標的を絞り込んで執ように攻撃を展開する傾向が強まっている。

標的にされた企業規模別の割合は、従業員2501人以上の大企業で50%台から39%になった一方、2500人以下の中・小規模企業が半数以上を占めるようになった。

また、標的型攻撃メールを受け取るリスクが最も高いのは、役員秘書や広報関係者であることも分かった。従来は役員などの経営層や上級管理職を狙う傾向にあったものの、その周囲の関係者を標的にする傾向が強まっているという。

* 標的型攻撃に変化、狙いは経営幹部から役員秘書に
  - <http://www.itmedia.co.jp/enterprise/articles/1404/17/news025.html>

年金機構の125万件情報流出　職員、ウイルスメール開封

2015/6/1 19:12

日本年金機構は１日、年金情報を管理するシステムに職員の端末を通じて外部から不正アクセスがあり、個人情報約125万件が外部に流出したとみられると発表した。情報には基礎年金番号や氏名が含まれ、うち約５万２千件には生年月日や住所も含まれていた。職員がウイルスの組み込まれた電子メールの添付ファイルを誤って開封し、不正アクセスされたと想定されるという。

同日記者会見した水島藤一郎理事長は「深くおわびする。誠に申し訳ない」と陳謝した。同機構を巡り、これだけ大規模な情報流出が発覚したのは初めて。

画像の拡大

個人情報が流出し、謝罪する日本年金機構の水島理事長(中)ら（１日午後、厚労省）

流出したのは年金記録を管理するのに一人一人に割り当てられている基礎年金番号と氏名の計約125万件。このうち約116万７千件には生年月日が、約５万２千件には住所と生年月日が含まれていた。

流出した約125万件のうち、約70万件にはパスワードが設定されていたが、それ以外は設定されておらず、機構の内規に違反した状態だった可能性があるという。

同機構によると、最初にウイルスへの感染を確認したのは５月８日。年金情報を管理する機構内の通信システムに不正アクセスされている記録が見つかり、１人の職員の端末の感染を確認した。機構内で職員に注意喚起したが、18日までに複数の職員の端末の感染が確認されたという。

* 年金機構の125万件情報流出　職員、ウイルスメール開封
- <http://www.nikkei.com/article/DGXLASDG01HCD_R00C15A6000000/?dg=1>

2015年12月15日 16時16分 更新

IEを最新版に切り替えて――IPAが移行を呼び掛け

2016年1月12日（米国時間）以降は、Windowsの各バージョンで使用可能な最新のInternet Explorerしかサポートされなくなる。セキュリティリスクの観点からもIPAは期日までの移行を呼び掛けた。

[ITmedia]

情報処理推進機構（IPA）は12月15日、MicrosoftのWebブラウザ「Internet Explorer」（IE）のサポートポリシーの変更に伴う対応を急ぐようユーザーに呼び掛けた。米国時間の2016年1月12日以降、IEはWindowsの各バージョンで使用可能な最新版しかサポートされなくなる。

2016年1月12日以降もサポートが継続されるIEは次の通り。

使用中のOS	サポート継続バージョン
Windows Vista SP2	IE 9
Windows 7 SP1	IE 11
Windows8	なし。Windows 8.1 UpdateやWindows 10への移行が必要
Windows 8.1 Update	IE 11
Windows 10	IE 11、Microsoft Edge
Windows Server 2008 SP2	IE 9
Windows Server 2008 R2 SP1	IE 11
Windows Server 2012	IE 10
Windows Server 2012 R2	IE 11

* IEを最新版に切り替えて---IPAが移行を呼び掛け
  - <http://www.itmedia.co.jp/enterprise/articles/1512/15/news111.html>

1．脆弱性攻撃サイトへの誘導元の8割以上が「汚染された正規サイト」

2015年第3四半期は、「汚染された正規サイト」を経由する国内向けの攻撃が多数確認されました。日本国内からのアクセスを確認した42件の脆弱性攻撃サイトのうち、86%が正規サイトの改ざんや不正広告が表示された正規サイトを経由するもので、汚染された正規サイト経由であったことが確認されました（グラフ1）。また42件の脆弱性攻撃サイトから侵入する不正プログラムの6割以上が、オンライン銀行詐欺ツールやランサムウェア（身代金要求型不正プログラム）など金銭目的の攻撃でした。

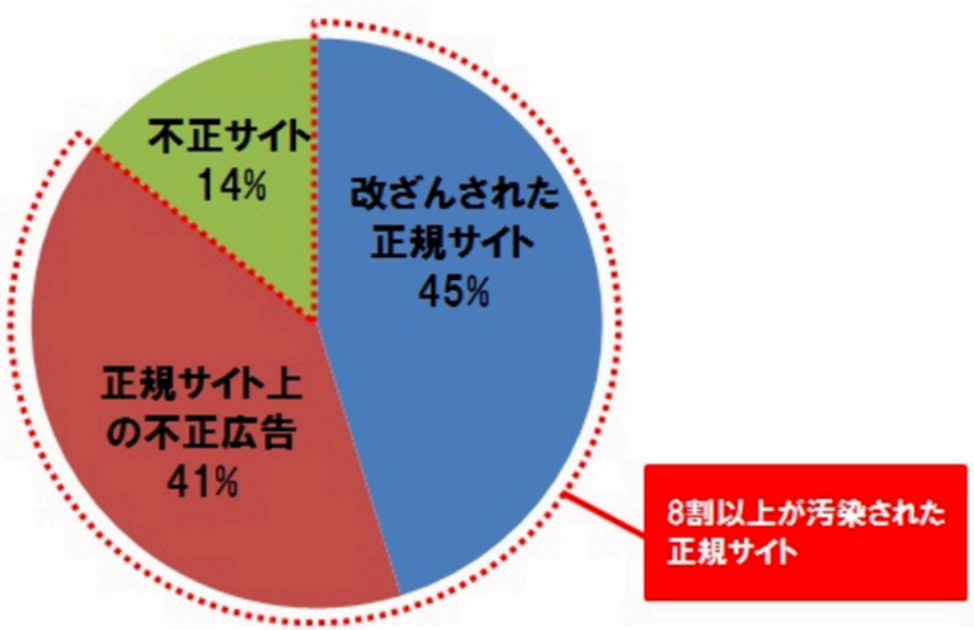
他方で2015年第3四半期は、脆弱性攻撃サイトへユーザが誘導される件数は、全世界的に増加傾向にあり、2014年第3四半期と比較して約9倍の約380万件に増加しました（グラフ2）。そのうち、日本国内からのアクセスは約170万件となり、約45%を占めています。

脆弱性攻撃サイトに設置されるエクスプロイトキット（※1）の開発は、盛んに行われています。2015年第3四半期中に確認された2件のAdobe Flash Payerの脆弱性は、メーカーが更新プログラムを公開する1～3日前にその脆弱性を狙う攻撃コードがエクスプロイトキットに追加されていました。

ユーザにとっては、普段より閲覧している正規サイトを表示しただけで攻撃にさらされる危険性があります。セキュリティ製品で不正なWebサイトへのアクセスを防止するほか、更新プログラムが公開されたら早期に適用するなど脆弱性への対策が現在最も重要な対策となっています。

※1　「エクスプロイトキット（Exploit Kit）」は、攻撃対象PCのOSやソフトウェアに存在する脆弱性を探して攻撃を行う脆弱性攻撃ツールです。

●グラフ1：日本国内からアクセスが確認された脆弱性攻撃サイトへの誘導元サイト種別割合（※2）



* 脆弱性攻撃サイトへの誘導元の8割以上が「汚染された正規サイト」
  - <http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20151117084548.html>

2015年12月15日 07時16分 更新

Joomlaに深刻な脆弱性、パッチ公開2日前から攻撃横行

セキュリティ企業によると、Joomlaの脆弱性修正パッチが公開される2日前から、この脆弱性を突くゼロデイ攻撃の発生が確認されていたという。

[鈴木聖子，ITmedia]

オープンソースのコンテンツ管理システム（CMS）「Joomla」の更新版が12月14日（米国時間）に公開され、深刻な脆弱性が修正された。セキュリティ企業のSucuriは、パッチが公開される2日前からこの脆弱性を突くゼロデイ攻撃の発生が確認されていたとして、Joomlaを使っているWebサイトでは直ちにパッチ適用やログ確認などの対応に乗り出すよう促している。

Joomlaの脆弱性はバージョン1.5.0～3.4.5に存在していて、悪用されればリモートでコードを実行される恐れがある。更新版のバージョン3.4.6でこの問題が修正された。

Joomla 3.4の特徴（Joomlaより）

Sucuriのブログによれば、この脆弱性は簡単に悪用することができるといい、12月12日の時点で既に、この問題を悪用した攻撃コードが出回っていたという。

* Joomlaに深刻な脆弱性、パッチ公開二日前から攻撃横行
  - <http://www.itmedia.co.jp/enterprise/articles/1512/15/news048.html>

東京工業大学
Tokyo Institute of Technology

レコード件数別の損失推定額範囲

レコード件数	予測（下限）	平均（下限）	推定	平均（上限）	予測（上限）
100	$1,170	$18,120	$25,450	$35,730	$555,660
1,000	$3,110	$52,260	$67,480	$87,140	$1,461,730
10,000	$8,280	$143,360	$178,960	$223,400	$3,866,400
100,000	$21,900	$366,500	$474,600	$614,600	$10,283,200
1,000,000	$57,600	$892,400	$1,258,670	$1,775,350	$27,500,090
10,000,000	$150,700	$2,125,900	$3,338,020	$5,241,300	$73,943,950
100,000,000	$392,000	$5,016,200	$8,852,540	$15,622,700	$199,895,100

情報漏洩 1,000件 : 810万円 (= $67,480 * 120円/$)

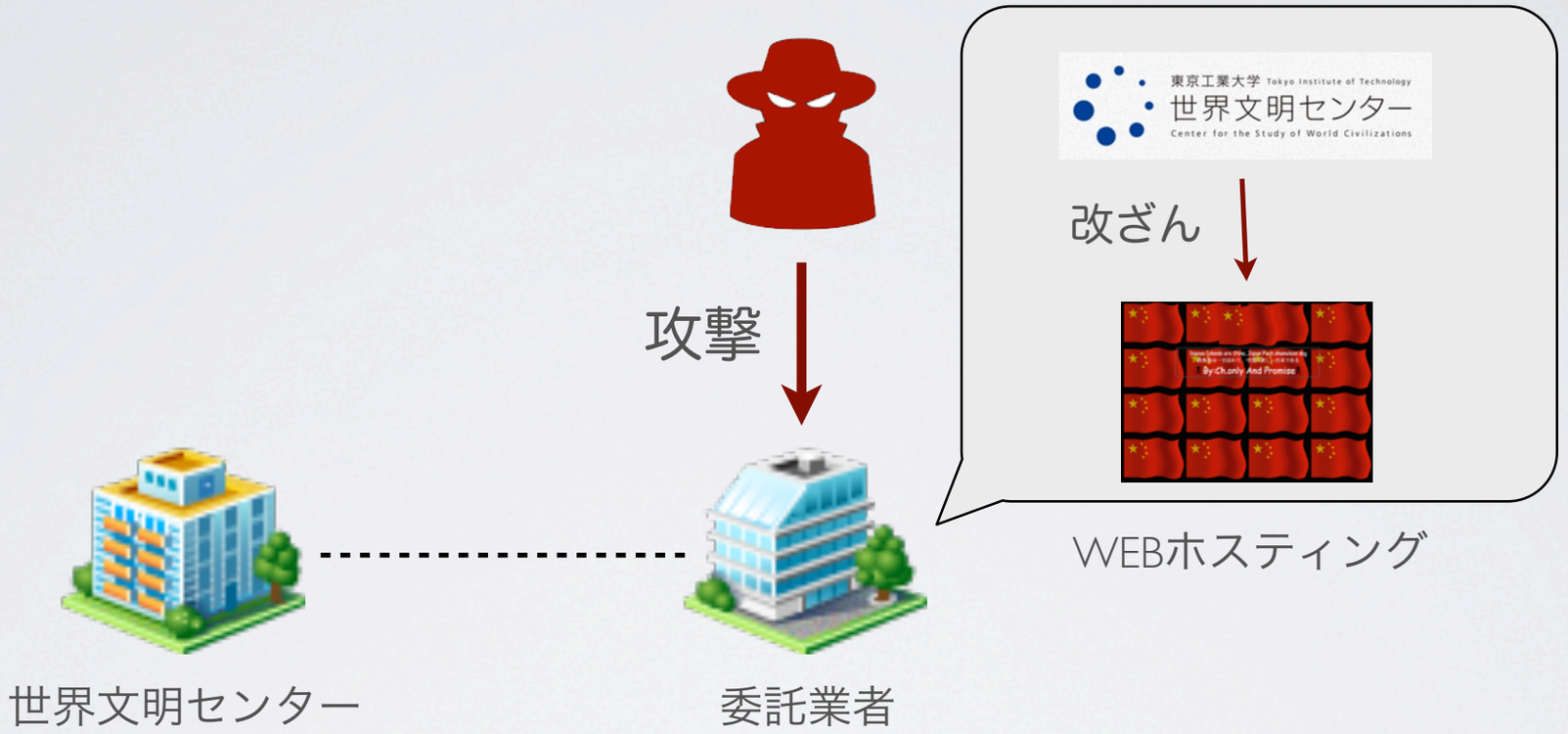
情報漏洩 10,000件 : 2148万円 (= $178,960 * 120円/$)

情報漏洩 100,000件 : 5695万円 (= $474,600 * 120円/$)

情報漏洩 1,000,000件 : 1.51億円 (= $1,258,670 * 120円/$)

* Verizon 2015年度 データ漏洩/侵害調査報告書 (p.30 図23. レコード件数別の推定損失額範囲)
  - <https://www.verizonenterprise.com/jp/DBIR/2015/>

世界文明センター@東工大に対する攻撃
(2012.09.15)



・国外からの攻撃
　→WEBページの改ざん
　→1000件の個人情報流出の恐れ

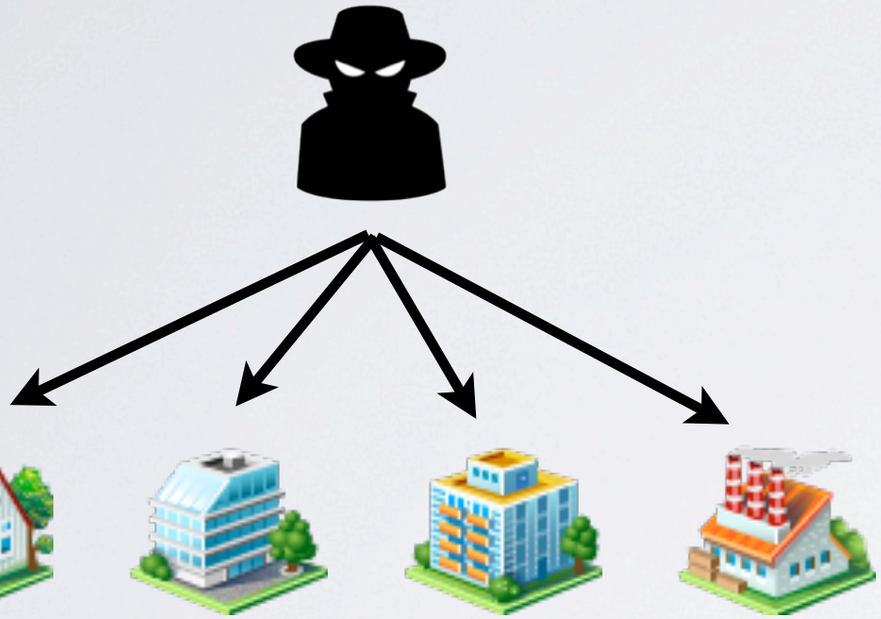
東京工業大学
Tokyo Institute of Technology

セキュリティを取り巻く複雑さ困難さ

東京工業大学
Tokyo Institute of Technology

標的型攻撃

ワーム、ボット感染



一般家庭　security企業　大学　工場

・広範囲に及ぶ攻撃
→みんなが同じ攻撃を受ける
→特定機関による攻撃の分析
→全体での対処法の共有

標的型攻撃

一般家庭　security企業　大学　工場

・個別の機関を狙った攻撃
→みんなが別の攻撃を受ける
→自分自身で気付く
→自分自身で対処する

東京工業大学
Tokyo Institute of Technology

WEBセキュリティ

Browser

Chrome, Firefox, safari, IE ...

外部からのアクセス

WEB Framework

Ruby on Rails, Apache Struts,
Django, mojolicious, Sinatra ...

Python, PHP, Perl, JAVA ...

内部からのアクセス

ActiveRecord, Doctrine, DBIx::Skinny,
SQLAlchemy ...

DB

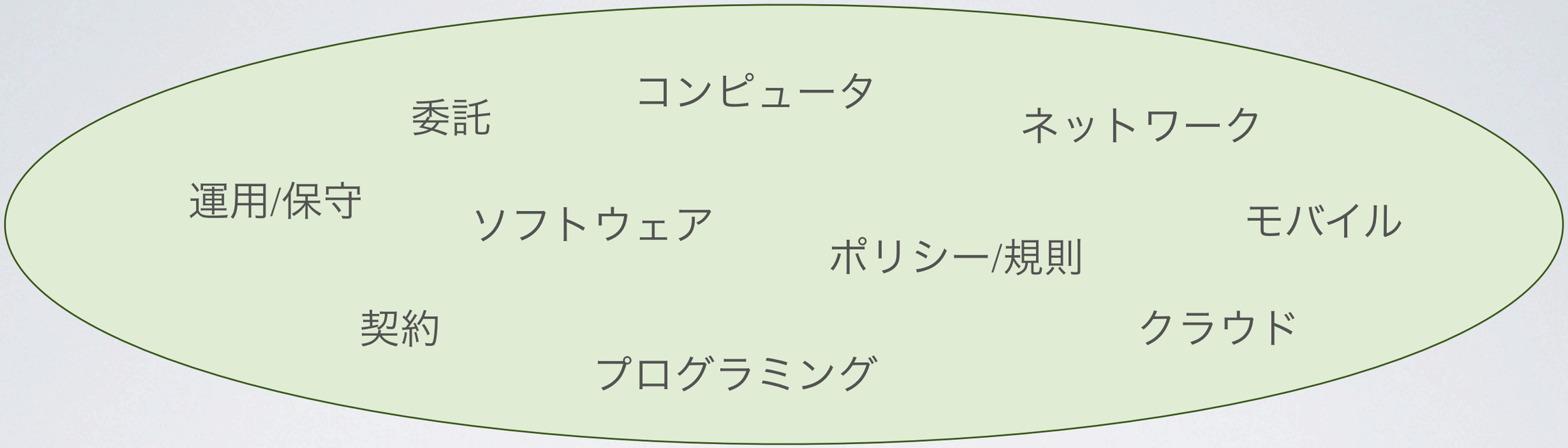
MySQL, PostgreSQL, Oracle,
MongoDB, CouchDB, Redis ...

・内部 x 外部を繋ぐそもそもの困難さ
・多くのコンポーネントx非常に種類の多いツール群

個別のケースを解決出来ても
他に応用が利かない

東京工業大学
Tokyo Institute of Technology

広範囲かつ複雑過ぎるセキュリティの現状



セキュリティ専門チームの立ち上げ

→ 事後対応から事前対策へ

東京工業大学
Tokyo Institute of Technology

東工大CERT設立を概観

東工大CERT設立までの流れ

1．NOCへの加入

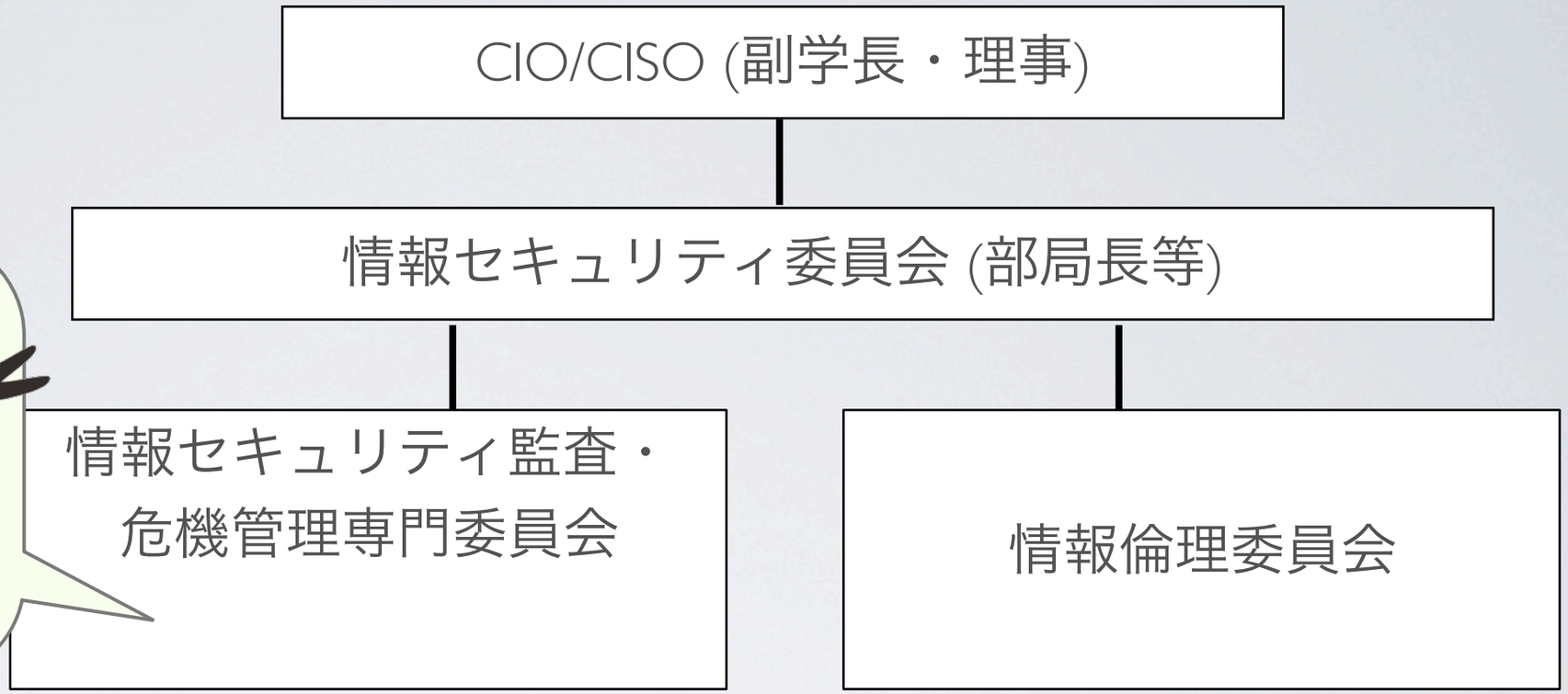
2．各委員会への参加

3．CERT規則案の作成

4．CERT規則の成立

東工大CERTの位置づけ、権限が定まった

東工大CERTの位置づけ



情報セキュリティ規則 第16条第5項

最高情報セキュリティ責任者は（中略）CERTに対して、当該事案に関する初動体制としての緊急措置を講ずる全権を委任することができる。

- 統括責任者2名、事務4名、技術職員2名 (内専任2名)
- 緊急対応に関わる権限をCISOから事前に委譲される形式
- 緊急時の初動対応 (被害の最小化を図る。最終判断は部局長等)
- セキュリティ情報の収集・分析・通知
- 学内の脆弱性調査

CERT設立・活動における困難さ

- 学内(ネットワーク)の状況把握
- 強力な権限の付与
- 部局の独立性
- セキュリティに対する意識、興味
- トップ層の理解
- 予算確保

東京工業大学
Tokyo Institute of Technology

設立・活動を間接的に推し進めた事柄

- 束縛×　安全○　(方向性の提示)
- NOCと密な関係を構築　(重要な組織連携)
- 権限/予算無しに出せる成果　(活動のアピール)
- 部局/担当者判断を尊重　(文化を大事に)
- ニュース解説の配信　(知識共有、興味喚起)

東京工業大学
Tokyo Institute of Technology

東工大CERT設立前

東京工業大学
Tokyo Institute of Technology

あらゆる機会で方向性を提示する

About

■ T2 CERT (東工大CERT) について

CERTは情報セキュリティ専門チームです。東工大における研究/教育/事務活動等を促進させるため、安全な計算機環境が構築できるようサポートする事がCERTの役割です。セキュリティ事案発生時における緊急対応を行うほか、セキュリティ情報の発信、学内の脆弱性調査など事前対応に重きを置いた情報セキュリティに関わる活動を行っています。

・　束縛×　安全○　（方向性の提示）

東京工業大学
Tokyo Institute of Technology

ミーティングを通した連携体制の構築

NOC / NAP
ネットワーク / 認証担当チーム

現場との連携

東工大CERT
Tokyo Tech Computer Emergency Response Team

情報セキュリティ
監査・危機管理専門委員会

トップ層との連携

- CERT設立前からNOCミーティングに参加
- NOC/NAPメンバーの一部がCERTミーティングに参加
- NOC/NAPメンバーの一部を含むCERTのMLでオープンに議論
- セキュリティの委員会における、トップ層との定期的な議論
- 部局長等会議におけるセキュリティ関連の報告(不定期 7回/年)

- NOCと密な関係を構築 (重要な組織連携)

東京工業大学
Tokyo Institute of Technology

Google / SHODAN検索を利用した脆弱性調査

＜ SHODAN検索 ＞

* 複合機　（情報漏洩、DDoS等の危険性）
* テレビ会議システム　（情報漏洩、DDoS等の危険性）
* ネットワーク機器　（情報漏えい、不正なサイトへの誘導）

＜ Google検索 ＞

* Movable Type　（WEBサイト改ざんの危険性等）
* WordPress　（改ざん、DDoS参加の危険性等）
* CGIスクリプトの公開　（不正アクセス等の危険性）
* ブログ/WiKiの不正利用　（悪意あるサイトへの誘導）
* ファイル一覧表示　（情報漏洩の危険性）
* Apache1.3系　（不正アクセス、情報漏洩等の危険性）

・　権限/予算無しに出せる成果（活動のアピール）

ニュース解説の配信

- CERTメンバーに向けてMLを通して
  ニュース3行解説を送信

- WEB(http://cert.titech.ac.jp)を
  通して学内にも解説記事を配信

- 各委員会の場でも毎回一つニュース
  を取り上げて、興味喚起を図る

- 現場およびトップ層に現状を把握
  してもらう。色々な先生方の意識が
  少しずつ変わっていく。

ニュース解説の配信
(知識共有、興味喚起)

セキュリティ事案発生時の対応フロー

- CERTは緊急かどうかの判断を行う
  重大/軽微の判断は部局長等が行う
- 被害の最小化を図るため、機器の
  停止/データ保全等を行う
- 意思決定のフローが進むように
  サポートする

部局/担当者判断を尊重 (文化を大事に)

* 対策本部の設置後は全学的な対応フロー(軽微な場合の対応を包含する)が発生

東京工業大学
Tokyo Institute of Technology

半年以上の丁寧な議論を経て、東工大CERTの規則・権限、またDPIに関するルールが決定

NOC / NAP
ネットワーク / 認証担当チーム

東工大CERT
Tokyo Tech Computer Emergency Response Team

情報セキュリティ
監査・危機管理専門委員会

＋顧問弁護士

部局長等会議

役員会

東京工業大学
Tokyo Institute of Technology

東工大CERT設立後

東京工業大学
Tokyo Institute of Technology

NOCとのセキュリティ機器の共同検証

- FireEye (次世代型IDS)
  - 自前の仮想環境を構築し、ウイルス検体の挙動を検証
  - 学内環境に即した通知体制を構築
    * 危険度よりも同一ホストで発生した事象を時系列に追跡し判断
    * NOCで該当する対外IPを遮断
    * ゼロデイ攻撃に関しては検証環境やvirustotalで確認後に通知
  - → 効果は高いが運用コストも高く、現状では厳しい状況にある
    * 特定の事象のみを検証してくれる外部サービスを調査済み
- Paloalto (次世代型FW)
  - 各種脅威の推移、ボットネットの活動状況を起点とした危険性の把握
  - PaloaltoおよびVirusTotalのAPIを組み合わせた脅威レポートの自動生成
  - → データ量および種類が多く、危険性の度合いを決定するのにコストがかかる
    また、レスポンスやユーザ連絡時のデータ抽出等で改善が望まれる点もある
    * ノウハウの蓄積を行い、分析/警告の過程を自動化して対応するよう検討中

その他、Cisco SourceFire, Fortinet Fortigate, Checkpoint等を検証済み

- 予算無しに出せる成果 (活動のアピール)

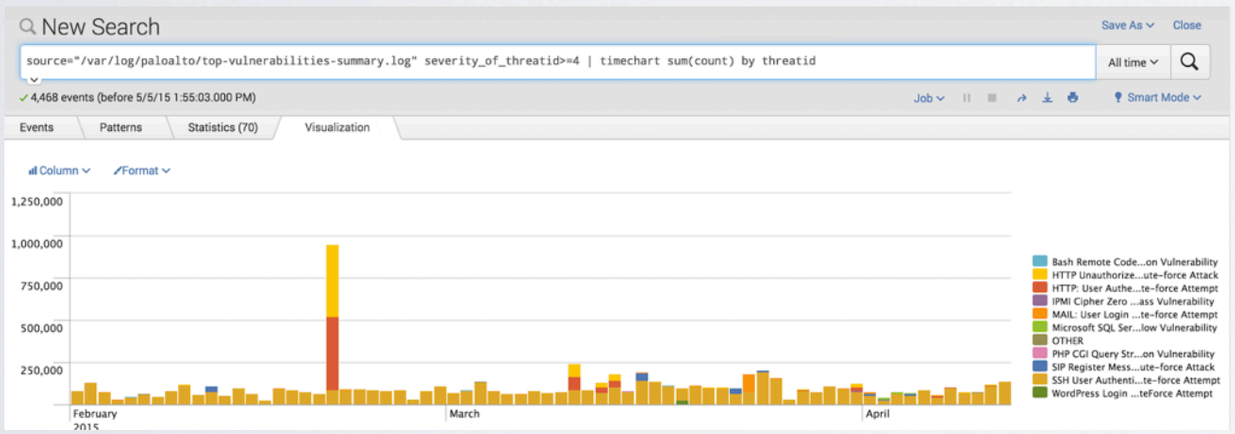
東京工業大学
Tokyo Institute of Technology

Paloaltoの運用システム例

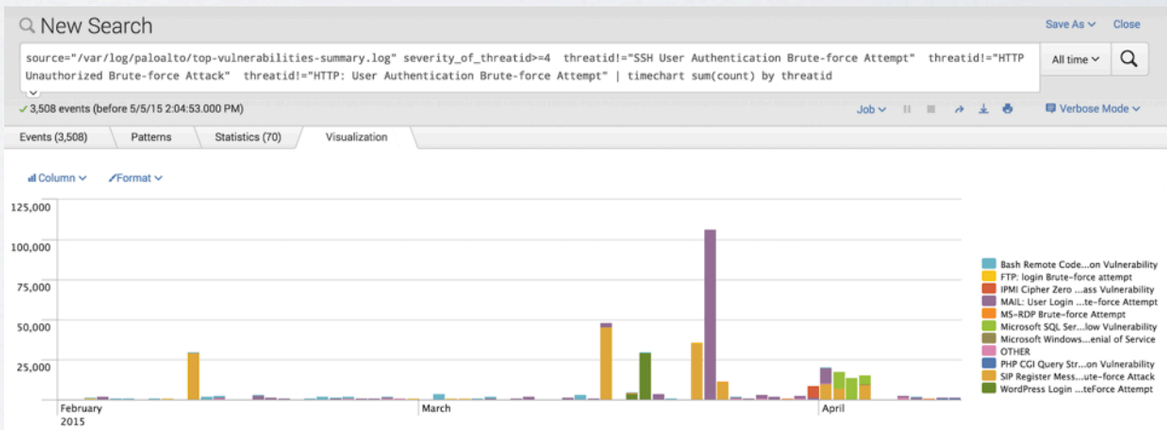
ログの保管
他のアプリとの連携

ログの分析
ログの可視化

・可視化の例：ACC (threat prevention)のグラフ化



攻撃回数を1日ごとに積算したグラフ



カウントの多い上位3つを除去したグラフ

・　予算無しに出せる成果（活動のアピール）

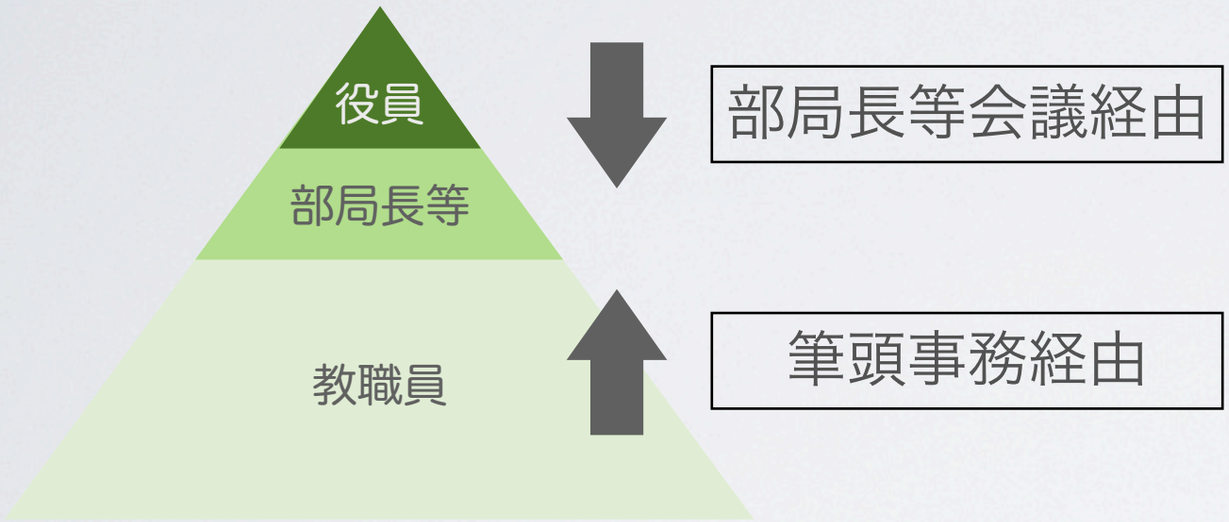
チラシの作成・配布

学内のデジタルサイネージにも同時に表示

- 少額予算で出せる成果（活動のアピール）

学内における通知、情報共有方法

緊急性の高い話題、インパクトの大きな話題などの共有手順



どちらも全学に対するアナウンス経路

・同時に別経路からアナウンスする事で、話が通じやすく行き渡りやすい
・実務的なお知らせにある種のお墨付きが付くことで実行力が増す
・WEBやチラシ、学内講演なども併用

東京工業大学
Tokyo Institute of Technology

インシデントレスポンスの例

東京工業大学
Tokyo Institute of Technology

2015年03月に発生したWEB改ざん

事件発生から2時間半程度

01. 学内研究室のWEBページが改ざんされているとの報告がNOC、CERTに届く
02. 改ざんの事実を確認し、ネットワーク遮断を行った旨該当担当者に連絡
03. 現場に赴き、機器等の状況を担当者のヒアリングを通して把握
04. CIO/CISOおよび委員会に対して状況報告

軽微な事案だと予想が付く

・権限の行使と報告

・NOCとの連携

東京工業大学
Tokyo Institute of Technology

2015年03月に発生したWEB改ざん

事件発生から数時間〜1日程度

05. 担当者を通じて調査および担当部局への注意喚起を指示
06. NOCにより通信記録から攻撃を特定。また関連した別の攻撃等が無い事も確認
#　　概ね事態は収束
07. 折り返しCERTへ機器の調査依頼が来る
08. CERTで機器のログ調査を行い、改ざん以外の被害が無い事を確認

・NOCとの連携

・組織内でのログ等の調査/分析

東京工業大学
Tokyo Institute of Technology

2015年03月に発生したWEB改ざん

事件発生から数日〜1ヶ月程度

09. CERT/委員会のミーティングで報告
10. 部局長等会議への報告を通して全学に注意喚起
#　　部局担当者が何をしたら良いか把握し切れていない
11. 該当部局内の対応フローが進まない部分をフォロー
12. 次回からは対応フロー図を添えて、担当者と連絡を取ることを決定
13. 部局長等会議で対応フローの徹底を訴える

・全学へのフィードバック

・プロセスのチェックと改善

東京工業大学
Tokyo Institute of Technology

設立前から構築していた
組織連携が役に立った。

規則・権限がある事で
スムーズに対応出来る。

東京工業大学
Tokyo Institute of Technology

予算関連の話題とまとめ

東京工業大学
Tokyo Institute of Technology

平成27年度の(予算が必要な)活動、人材、機材等

- 東工大CERTの日常業務
  - ＊ 脆弱性調査用のソフトウェア
  - ＊ ラップトップ ／ デスクトップPC
  - ＊ インシデント対応時に必要な機材（スイッチ、ケーブル等々）
  - ＊ チラシの作成（デザイン、印刷）
- 技術職員の追加（1名）
- 次世代型FWの調達
- 添付ファイルを抑制するファイル共有システム
- 標的型メール訓練
- CERT用仮想化基盤環境の構築

ほぼ予算０からのスタート

どう行動し、どう説得するか

東京工業大学
Tokyo Institute of Technology

現在/今後のCERT活動

- 平成27年度の取り組み
  - 学内の脆弱性診断（Nessus6, google, SHODAN等）
  - NOC管理機器(ネットワーク/セキュリティ)の共同利用→学内通知
  - 次世代型FWの調達
  - CERT用仮想化基盤環境の構築
  - セキュリティ秋学校（XSSやエクスプロイトに関する演習中心の合宿）
  - 学内外での情報セキュリティセミナー等の講演
  - 学内インシデント対応および情報の蓄積と分析
  - 情報セキュリティに関する情報収集と分析
  - WEBサーバの立ち上げと運用（最新情報の提供、学内通知、学内情報の整理）
- 来年度以降の取り組み
  - 平成26年度の活動を継続及び拡大
  - 学内向け契約の指針（契約テンプレートの作成）
  - 次世代型FWのNOCとの共同運用
  - セキュリティ/ネットワークログの収集および分析
  - 添付ファイルを抑制するファイル共有システムの開発/運用
  - 標的型メール訓練（セキュリティ教育）