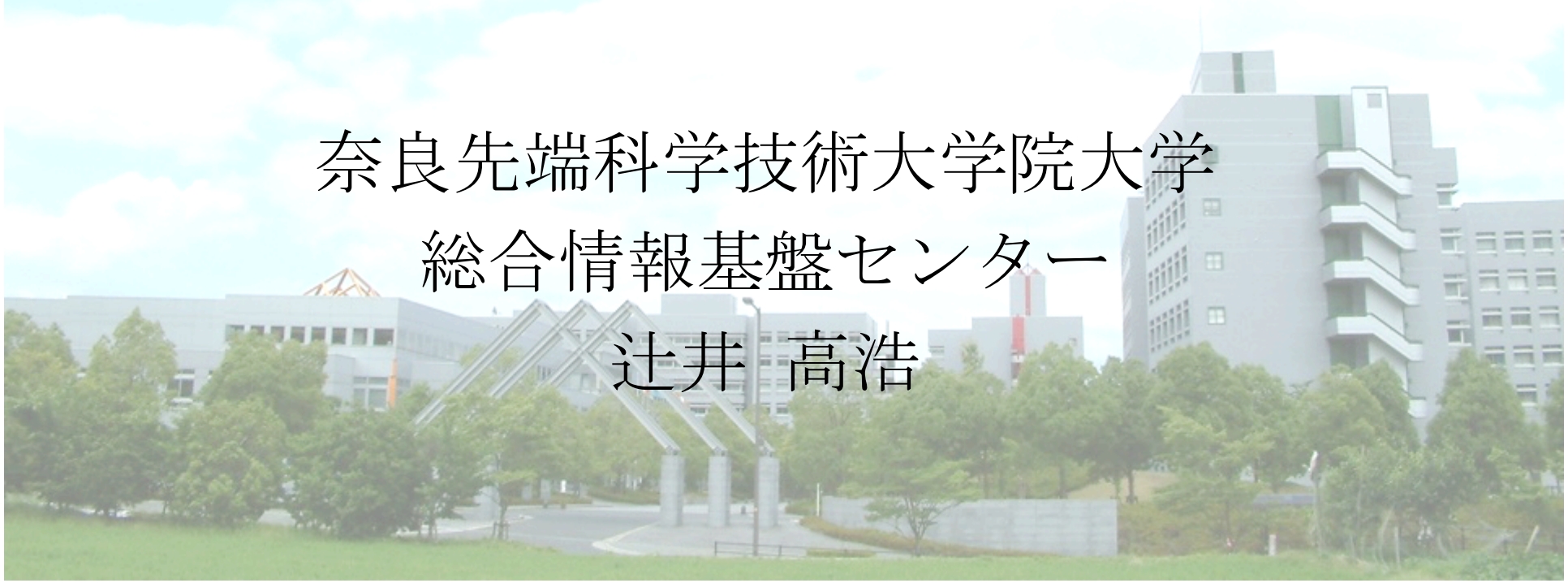
無限の可能性、ここが最先端　－Outgrow your limits－

奈良先端科学技術大学院大学における情報システムの運用とセキュリティ



奈良先端科学技術大学院大学

総合情報基盤センター

辻井　高浩

アジェンダ

- 組織紹介
  - 奈良先端科学技術大学院大学
  - 総合情報基盤センター
  - セキュリティ部署
- セキュリティ事情
- インシデント事例
- 最後に

無限の可能性、ここが最先端　－Outgrow your limits－

大学紹介

奈良先端科学技術大学院

- 独立大学院
  - 情報科学研究科
  - バイオサイエンス研究科
  - 物質創成科学研究科
- 所在
  - 奈良件生駒市高山町
- 規模
  - 教員 250、職員 150、学生 1100
  - 1991年10月創立

総合情報基盤センター

- 2010年7月設立
  - 情報科学センターと学術情報課(図書館)の統合
  - 情報科学センターは、1992年4月に設置
    - 開学当初より設置
    - 結果、一元的な運用・管理
- 組織構成
  - 次世代システム研究グループ　　4名
  - 情報基盤技術サービスグループ　　9名
  - 学術情報サービスグループ　　14名

セキュリティ部署

- CSIRTの設立
  - 2016年10月1日
  - 総合情報基盤センターの一部メンバーが兼任
- 実情
  - 文科省からの要請
    - 国の機関による複数のインシデント発生
  - 情報基盤技術サービスグループの既存業務の継続
    - 予算・人の措置はなし

無限の可能性、ここが最先端　－Outgrow your limits－

本学のセキュリティ事情

大学におけるリスク

- 情報漏洩
- Webサーバ改竄

情報漏洩

- 影響
  - 機密・機微情報が漏洩した場合は影響大
    - 組織として取り組むことが必要不可欠
- 原因
  - 技術的問題
    - いくつかの製品の組み合わせで対応
    - 設定ミス
  - 体制面
    - 既存業務との並行処理
    - 規定からの実施手順作成および手順書見直しの不徹底
    - 予算（人・製品）
- 対策
  - 技術的問題
    - 統合的な製品がほしい
    - 設定のクロスチェック
  - 体制面
    - 専任のスタッフが必要
    - 各研究室における意識改革に向けた啓発活動
    - 予算についても経営陣の理解が必要
      - 外部機関による役員向けセキュリティ講習会の実施

Webサーバ改竄

- 影響
  - 信用の失墜
    - 原因究明、対策及び復旧作業、信頼回復に向けた社会的な説明などの対応が必要
- 原因
  - 技術的問題
    - 設定ミス
    - システムの脆弱性
  - 体制面
    - 各研究室・プロジェクトでの運用・管理
      - 管理者（教員）ではなく、学生が作業を実施
    - 異動による業務引き継ぎの不徹底
- 対策
  - 技術的問題
    - 設定ミスを考慮したシステム設計を徹底
      - 規程等に記載
    - 脆弱性チェックシステムを実施
      - CMS等をチェックできてない場合もあり
  - 体制面
    - Webサーバ管理者向け講習会の実施
    - CMS等への対応製品の検討

問題点の整理

- 大学組織の構成
  - 研究室による独立運営（セキュリティも含めて）
- セキュリティに対する意識
  - 経営陣
    - マネージメントに必要な情報提供
  - システム管理者
    - スキルの向上
    - 最新情報の取得
  - 利用者
    - 最新情報の提供
- 文書類の更新・新規作成
  - 規程・実施手順書
    - CSIRTの一元管理に必要

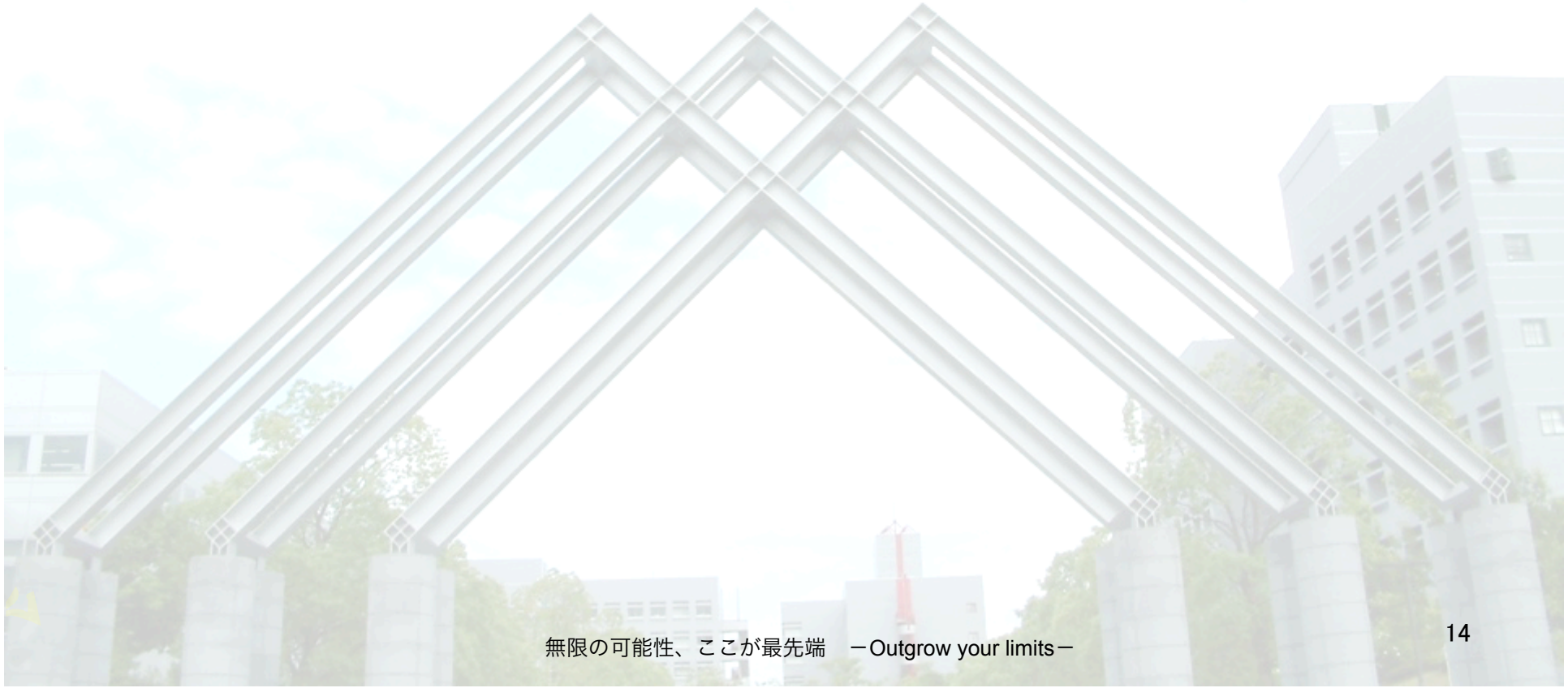
今後のアクション

- 文書の作成
  - セキュリティ基本計画
  - 対策基準(ポリシー)の更新・新規作成
    - 政府機関の情報セキュリティ対策のための統一基準
    - 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
- 自己点検の実施
  - 全構成員
- セキュリティ対策訓練の実施
  - システム管理者
  - 利用者
- 講習会の実施
  - 役員
    - 外部機関を利用
  - 利用者
    - 総合情報基盤センター/CSIRTで実施
  - システム管理者
    - 総合情報基盤センター/CSIRTで実施

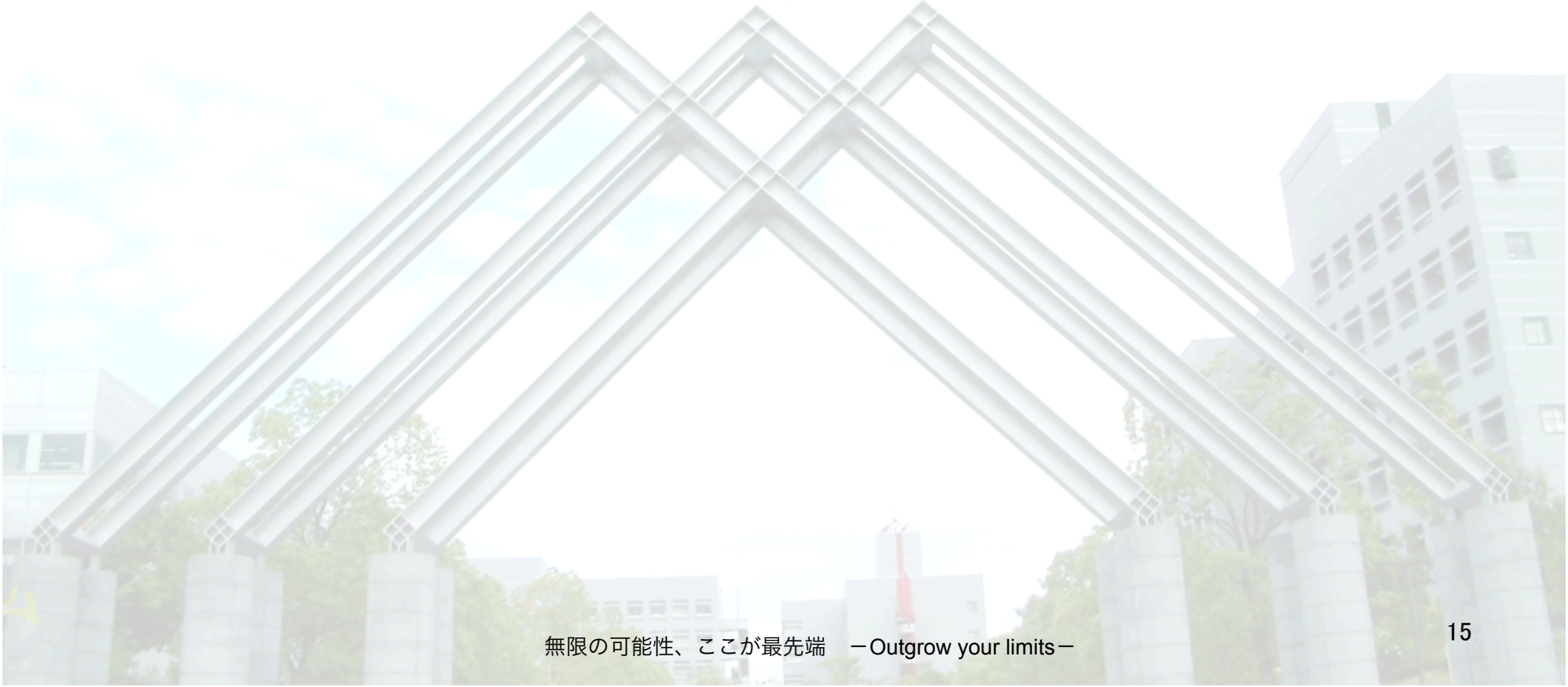
無限の可能性、ここが最先端　－Outgrow your limits－

インシデント事例

Webサーバ改竄事例(1)



外部への不正アクセス事例(2)

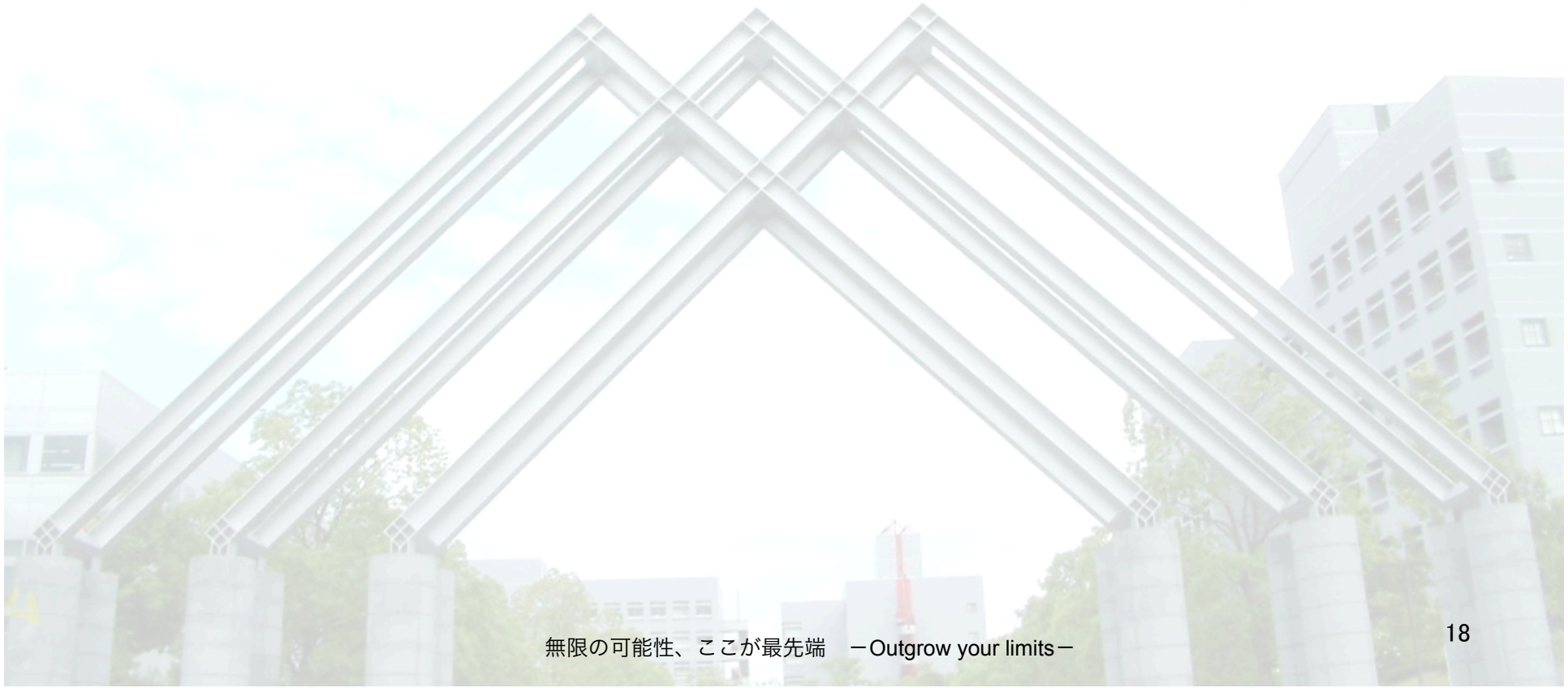


最後に

まとめ

- セキュリティ対策に完璧はない
  - インシデント発生した際の受容範囲を明確に
    - 明確にするには、情報の分類は必須
    - 周囲を落ち着かせるためにも
- システム管理者のみでの運用は避けるべき
  - 部局・研究室内全体での情報共有・対策が有用
  - クロスチェックができる体制
- 予算・人の確保
  - 計画的な予算要求
    - 本格的なチェックには人（第三者）が必要
    - 高度化するインシデントにはツール（製品）が必要

参考



無限の可能性、ここが最先端　－Outgrow your limits－

終