組織におけるサイバーセキュリティ対策
～セキュリティポリシーとCSIRT～

# 室蘭工業大学におけるセキュリティポリシー策定とその運用

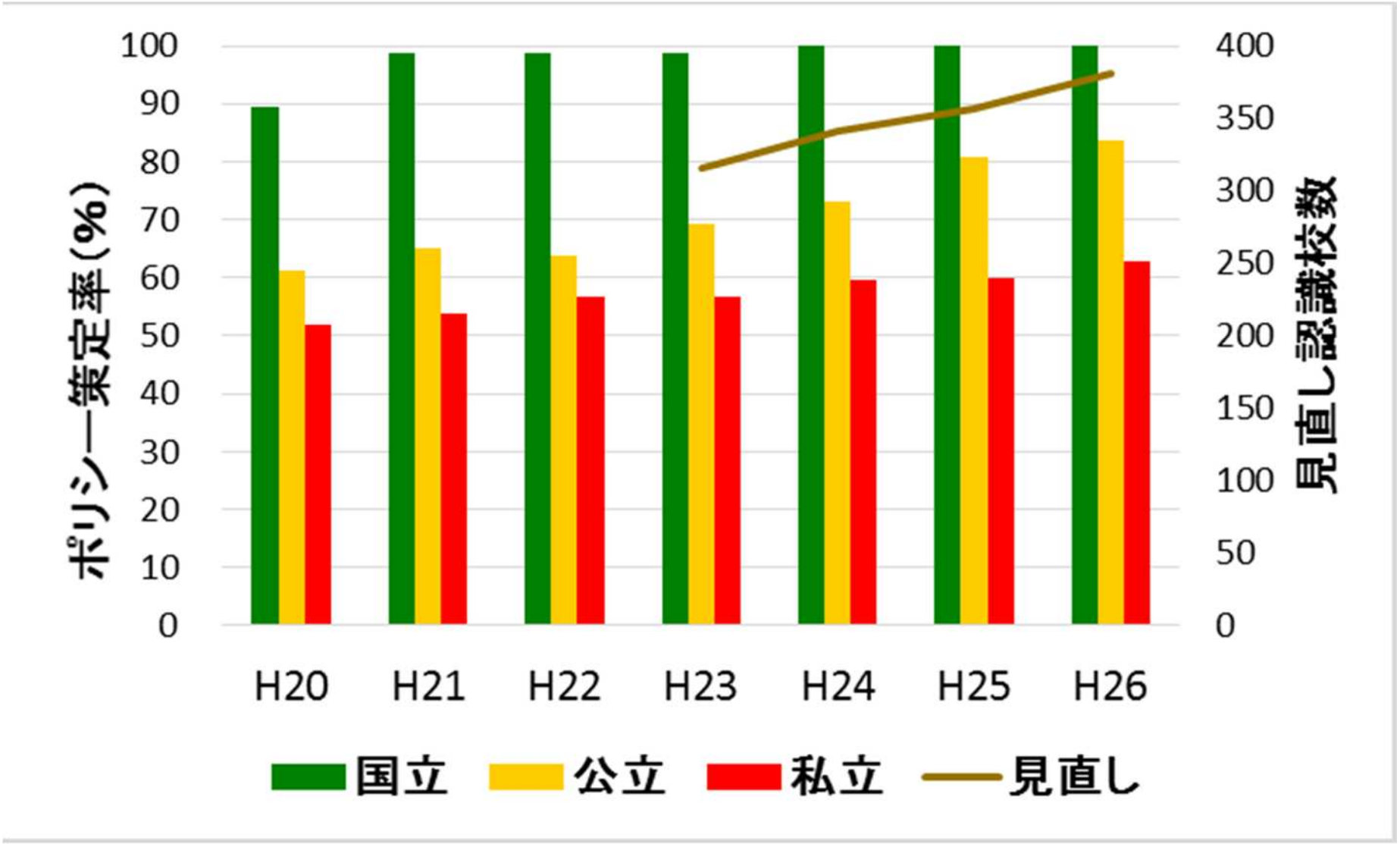
平成28年　1月　18日

室蘭工業大学
情報メディア教育センター

刀川　眞

# 1. はじめに

# 情報セキュリティポリシー策定率と見直認識




【参考】政府統計:学術情報基盤実態調査を元に作成

# 2. セキュリティポリシーの策定

# 「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」

◆国立情報学研究所（NII）
◆電子情報通信学会

合同検討、
2007月から公開

本学では2007年11月頃から、サンプル規程集を用いてセキュリティポリシー検討を開始

# ポリシー・規程集策定の基本方針

**策定における懸念**

- 膨大なサンプル規程集(解説を含むと約600ページ)をすべて施行できるか

**策定における目標**

- 実行できる規程集を作成する

**そのために**

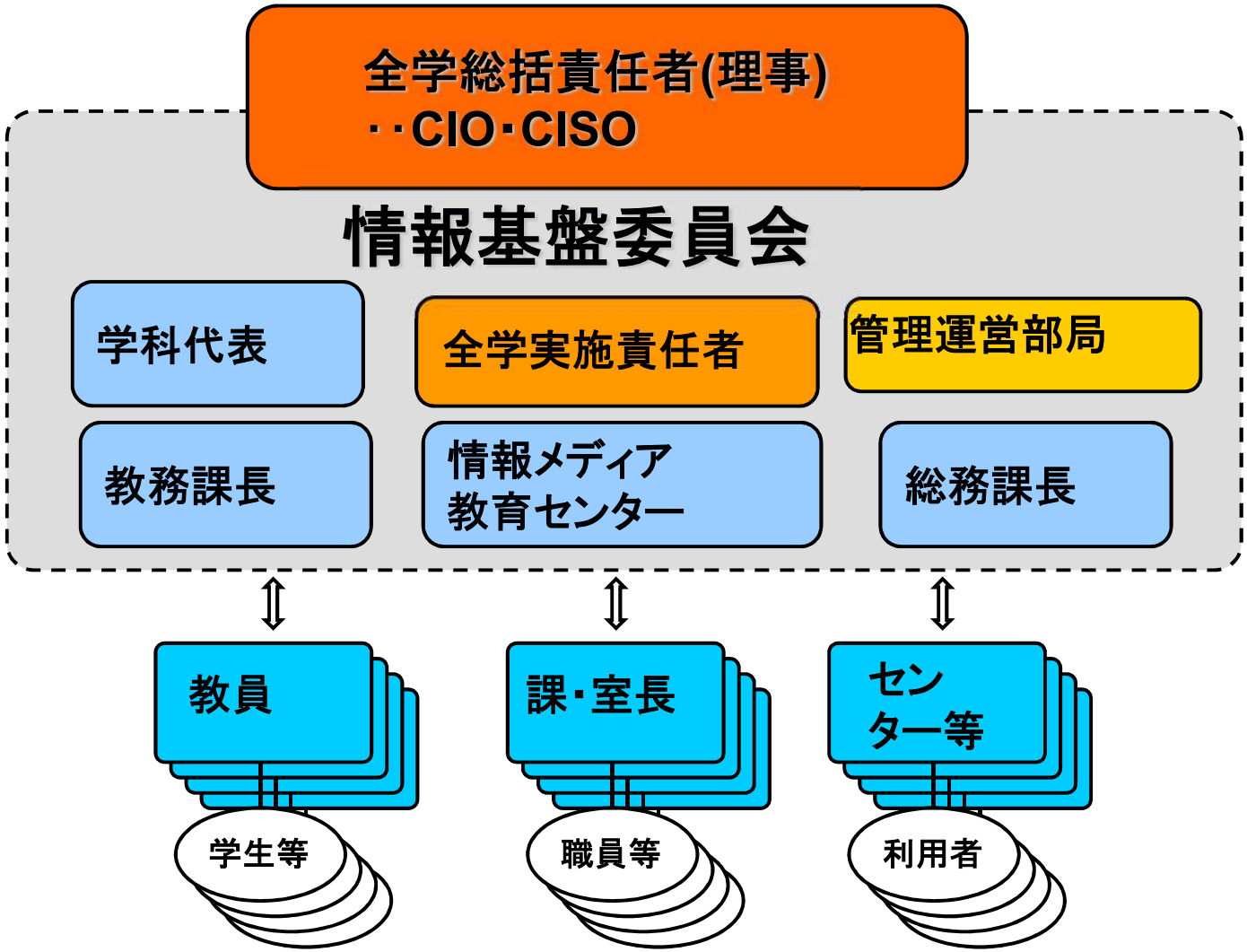
- セキュリティ管理を行う組織をコンパクト化して定義
- 事務部門との密接な協力関係

# サンプル規程集モデル大学(A大学)と本学比較

| | A大学 | 本学 |
|---|---|---|
| 学部 | 文学部、理学部（総合） | 工学部（単科） |
| 学生数 | 2,000名 | 約3,200名 |
| 単位 | 学部、事務局、情報メディアセンター、図書館等 | 教員、事務局課・室、情報メディア教育センター、図書館等 |
| 意思決定機関 | 全学情報システム運用委員会,<br>部局情報システム運用委員会 | 情報基盤委員会 |

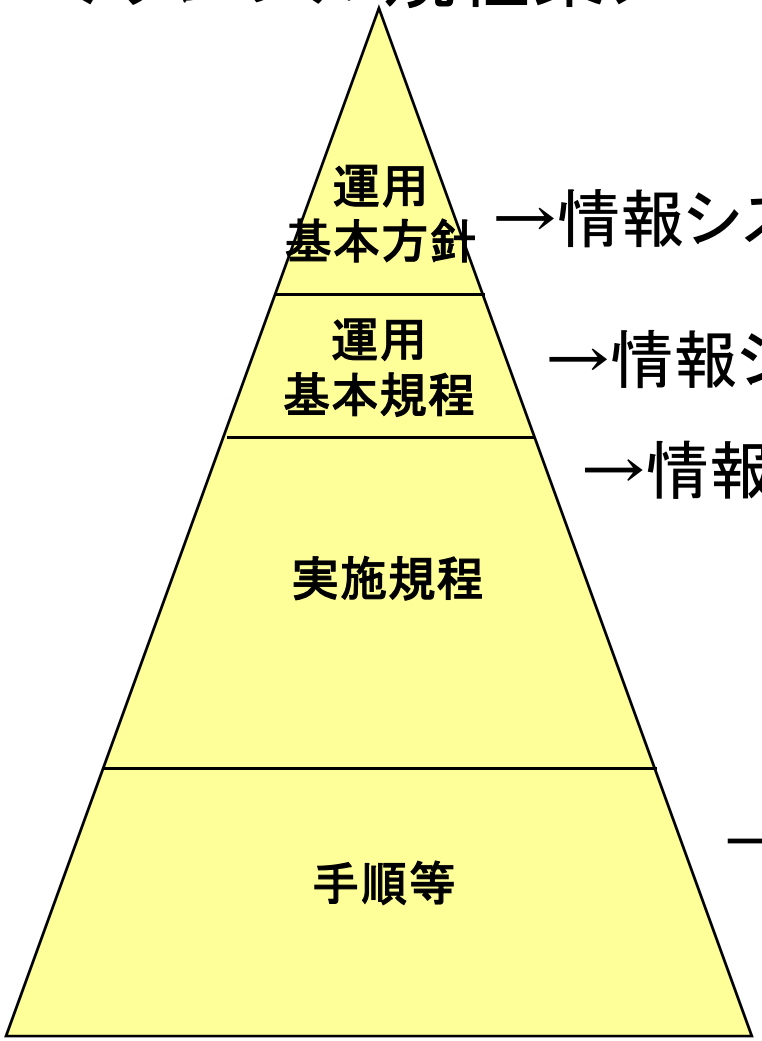
簡素化、フラット化

# 意思決定機関


全学総括責任者(理事)
・・CIO・CISO
情報基盤委員会
学科代表
全学実施責任者
管理運営部局
教務課長
情報メディア
教育センター
総務課長
教員
課・室長
センター等
学生等
職員等
利用者

# サンプル規程集と本学ポリシーの比較

＜サンプル規程集＞　＜本学ポリシー＞




→情報システム運用基本方針

→情報システム運用基本規程

→情報システム運用及び管理規程
〃　利用規定
〃　非常時行動計画に関する規定
〃　情報セキュリティ監査規程

→人事異動の際に行うべき情報セキュリティ対策実施手順

| | | |
|---|---|---|
| A1000 情報システム運用基本方針 | A3103 インシデント対応手順 | A3203 ウェブブラウザ利用ガイドライン |
| A1001 情報システム運用基本規程 | A3104 情報格付け取扱手順 | A3204 ウェブ公開ガイドライン |
| A2101 情報システム運用・管理規程 | A3105 情報システム運用リスク評価手順 | A3205 利用者パスワードガイドライン |
| A2102 情報システム運用リスク管理規程 | A3106 セキュリティホール対策計画に関する様式（策定手引書） | A3211 学外情報セキュリティ水準低下防止手順 |
| A2103 情報システム非常時行動計画に関する規程 | A3107 ウェブサーバ設定確認実施手順（策定手引書） | A3212 自己点検の考え方と実務への準備に関する解説書 |
| A2104 情報格付け基準 | A3108 電子メールサーバのセキュリティ維持手順（策定手引書） | A3300 教育テキストの策定に関する解説書 |
| A2105 情報サービス運用・管理規程 | A3109 人事異動の際に行うべき情報セキュリティ対策実施手順 | A3301 教育テキスト作成ガイドライン（一般利用者向け） |
| A2201 情報システム利用規程 | A3110 機器等の購入における情報セキュリティ対策実施手順（策定手引書） | A3302 教育テキスト作成ガイドライン（システム管理者向け） |
| A2301 年度講習計画 | A3111 外部委託における情報セキュリティ対策実施手順 | A3303 教育テキスト作成ガイドライン（CIO/役職者向け） |
| A2401 情報セキュリティ監査規程 | A3112 ソフトウェア開発における情報セキュリティ対策実施手順（策定手引書） | A3401 情報セキュリティ監査実施手順 |
| A2501 事務情報セキュリティ対策基準 | A3113 外部委託における情報セキュリティ対策に関する評価手順 | A3500 各種マニュアル類の策定に関する解説書 |
| A2601 証明書ポリシー（CP） | A3114 情報システムの構築等におけるセキュリティ要件及びセキュリティ機能の検討に関する解説書 | A3502 責任者等の役割から見た遵守事項 |
| A2602 認証実施規程（CPS） | A3115 情報システムの構築等におけるST 評価・ST 確認の実施に関する解説書 | A3600 認証手順の策定に関する解説書 |
| A3100 情報システム運用・管理手順の策定に関する解説書 | A3200 情報システム利用者向け文書の策定に関する解説書 | A3601 情報システムアカウント取得手順 |
| A3101 情報システムにおける情報セキュリティ対策実施手順（策定手引書） | A3201 情報機器取扱ガイドライン | ：本学ポリシー採用<br>：運用ルールの参考 |
| A3102 例外措置手順書 | A3202 電子メール利用ガイドライン | |

# 3. セキュリティポリシーの運用と展開

# （1）教育・講習（一覧）

| | 形態 | 時期・頻度 | 備考 |
|---|---|---|---|
| 教職員・編入生向け基礎講習 | 集合 | 新任時<br>編入時 | 独自テキスト作成（4～5回/年） |
| 学生向け基礎講習 | 集合 | 入学時<br>学科別 | 情報リテラシー授業（1回/年） |
| 留学生向け基礎講習 | 集合 | 入学時 | 英語、中国語（2回/年） |
| 教職員向け定期講習 | PC | 毎年 | IPAビデオ利用（1回/年） |
| 幹部向け講習 | 集合 | 毎年 | （1回/年） |
| サーバ管理者向け講習 | 集合 | 任命時 | （随時） |

# （1）教育・講習（テキスト）

本学の事例

ウィルスによる他パソコンへの攻撃



ウィルス感染状況

事例1 2008年9月、A学科のB教員が、パソコンを購入。すぐにデータ処理を行いたいため、ネットワークに接続し、そのまま使用し学内の他のパソコンのウィルスから感染した。

事例2 2007年12月、C学科のD院生が、英語のメールが届き、よく確認せずに「知り合い」と勘違いして添付されていたファイルを実行。ウィルスに感染した。

事例3 2008年6月、学内共用利用のE設備のパソコンはネットワーク非接続で使用していたが、F研究室の利用者がウィルスに感染したUSBメモリを持ち込んだため感染。さらにそのパソコンから別の利用者のUSBメモリにも感染を広げた。

原因と対策

ウィルスの多くは Windows の脆弱性を利用したもので、Windows Update を行っていれば、感染は防げていました。また、ウィルス対策ソフトを導入していれば、ウィルスを検出し、除去または無力化が行われていたでしょう。普段ネットワークに接続しないパソコンでも必ず Windows Update 及びウィルス対策ソフトの導入を行いましょう。

感染時の対処

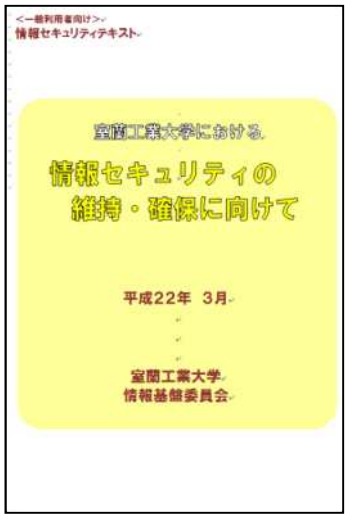
ウィルスを検出したり、ウィルスに感染していることを知らされたら、以下のように対策を行います。

1. ネットワークケーブルを抜く（ネットワーク経由での他のパソコンへの攻撃を遮断）
2. 他の安全なパソコンで修正プログラムをダウンロードする
3. 感染しているパソコンへCDやUSBメモリで修正プログラムをコピーして適用する
4. 最後にネットワークに接続して、Windows Updateの適用、ウィルス対策ソフトの導入を行う

対処に困った場合は、部局の技術担当者や情報メディア教育センターに相談するのがよいでしょう。

21

## 日本語





## 英語



## 中国語



## 留学生向け漫画教材(北大作成)

# （1）教育・講習（教職員向け定期講習）


平成27年度映像（約10分）
独立行政法人 情報処理推進機構（IPA）提供

## （2）サーバ疑似アタック

学外公開サーバを疑似アタックし、脆弱性有無を確認
改善勧告や指導を行い、最悪、ネットワークを遮断‥実際は改善実施＆使用済サーバ遮断

## （3）ウィルス対策ソフト提供とPCスキャン

学内向けにウィルス対策ソフトを無償提供

ウィルス対策ソフト導入状況、定義ファイル更新状況、OS更新状況把握のためPCをスキャン

# （4） 標的型攻撃訓練

標的型攻撃を模したメールを送信し、開封者行動（トラップ設定）を把握し注意を喚起

# （5）セキュリティ強化月間

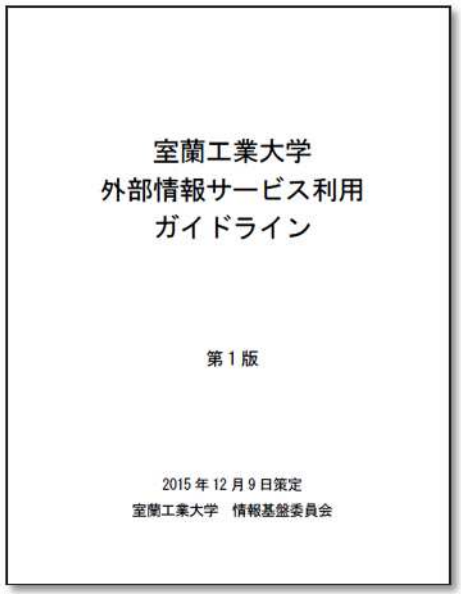
年2回、期間中にセキュリティ活動を集中させ、また啓発ポスターの学内公募などで意識高揚を図る

# （6）クラウドバックアップ

完全性・可用性向上のため、重要データを学外クラウドにバックアップ

クラウド利用の安全性確認のため「学外情報サービス利用ガイドライン」を策定

- 対象情報の重要度（4段階）
  （4：成績原簿、3：指導記録、
  2：学生名簿、1：公開情報）
  ×
- 外部サービスの信頼度（4段階）
  （独立性、アクセス制限、暗号化・・）



# （7） ISMS, BCMS国際認証取得

ISMS(Information Security Management System)

・組織が有する情報を機密性、完全性、可用性の点から維持・向上を図る体系的・総合的な仕組み

・国内の大学10番目（平成27年3月27日時点）

日本情報経済社会推進協会(JIPDEC)HPより

BCMS(Business Continuity Management System)

・ 重要業務停止の影響を最小限に抑え、長期・安定的サービスを提供する仕組み

・ 業務を整理し、リスクに対する事業インパクト分析、事業継続計画作成、実践的演習により実効性を確認

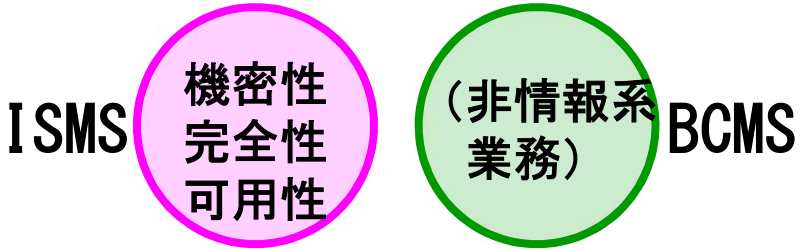
・ （世界の）大学で初（平成27年3月27時点）

# ISMSとBCMSの関係

一般組織（非情報系）の場合

- ISMS‥‥情報セキュリティの維持向上
- BCMS ‥（非情報系）業務の継続性確保

} 相互独立




情報系組織（情報センター等）の場合

- ISMS‥　情報セキュリティの維持向上
- BCMS ‥（情報系）業務の継続性確保

} 重複多


同時取得し易さ

# 4．おわりに

＜ポイント＞

・ポリシーのセキュリティ活動への具体的展開は稀
　→ 活動がぶれず一貫性を保つための「礎」
・策定部門（情報メディア教育センター）、支援部門（事務部門）、CIO/CISOとの密接連携

＜課題＞

・学内のモチベーション維持、インセンティブ確保
・利用性、実効性の常時確認 → 適用性向上

セキュリティポリシー策定はGOALでなくSTART

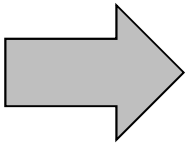
# 補足
# （活動の背景）

# 情報系センターを取巻く環境変化

＜環境＞

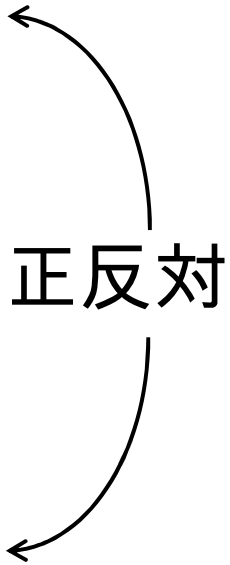
・クラウド
・アウトソーシング
：

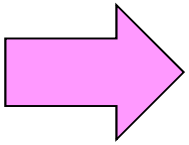
・情報セキュリティ
・情報戦略化
（IR、EM、MOOCs‥）
・事務処理効率化
：



＜情報系センター＞

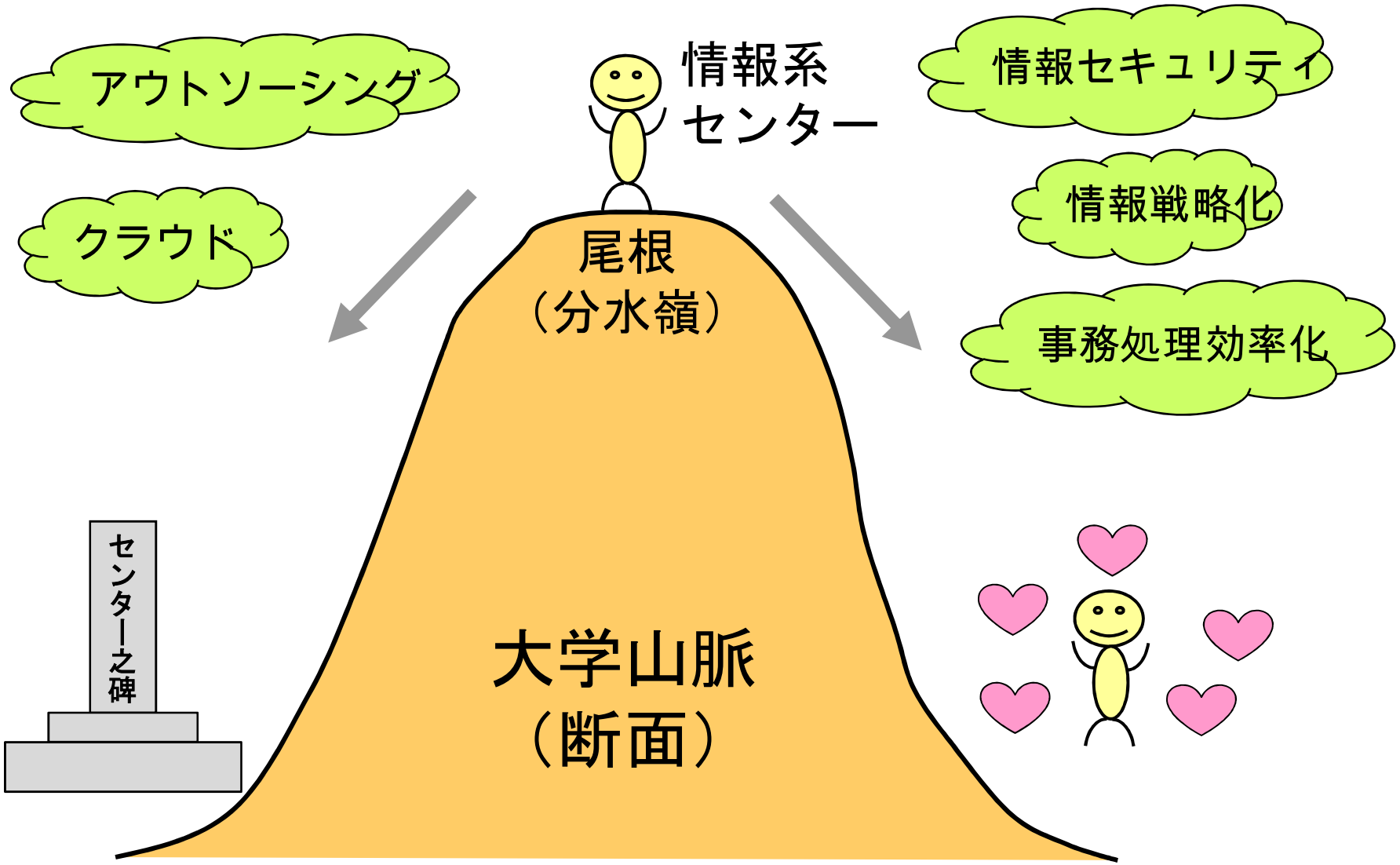
縮退、廃止



活躍増大

# 情報系センターを取巻く環境変化



# おわりに

「生き残れるのは強いものでも賢いものでもない。
常に環境に適応するものである」ダーウィン(?)

環境（学内、地域、社会‥）からの要請に応えていかなければならない。（≠自己保存）