KYUSHU UNIVERSITY 100th 2011
知の新世紀を拓く

情報統括本部における ISMSの取り組み

情報統括本部　ISMS運用事業室

2012年4月

Ver. 1.0

九州大学
KYUSHU UNIVERSITY

概　要

九州大学

1. 背景

2. ISMSとは？

3. 情報資産の洗い出しとリスクアセスメント

4. ISMS運用 – PDCAサイクル

5. 情報統括本部におけるISMSの活動

1. 背　景

九州大学

■九州大学におけるISMSの取り組み

九州大学では、第二期中期目標・計画の一環として、学内における情報セキュリティレベルの向上と、同セキュリティ文化の普及を目指し、本学の各種情報関連サービスを担う情報統括本部において、

情報セキュリティマネジメントシステム【ISMS】
（Information Security Management System）

の導入を目標に掲げた

【中期目標　33】

法令遵守の徹底に向けた取組を実施するとともに、情報セキュリティの対策に取り組む

2. ISMSとは？

九州大学

■ISMSとは

- 『Information Security Management System』の略で、「情報セキュリティを管理（マネジメント）するための仕組み（システム）」と呼ばれる国際標準（ISO）規格

- 組織が所有する様々な**情報資産**を、犯罪や災害から守り、適正に管理していくための仕組み

2. ISMSとは？

九州大学

情報資産とは？

情報資産とは、情報化に伴うビジネスに影響を与える全ての資産を意味する

例えば

ハードウェア、ソフトウェア、データ、ネットワーク、記録媒体、施設・設備、書類、人間、組織のイメージや信用など

が該当する

2. ISMSとは？

九州大学

■ISMSの狙い

「どのような**情報資産**を所有しているのかを把握し、どのようなところで**情報資産**が盗まれたり流出したりする危険があるのかを考えて、これを適正に管理する仕組みを作りましょう」

① **情報資産の保護**

② **利害関係者への安心の提供と信頼の獲得**

を実現することが最大の目的

3. 情報資産の洗い出しとリスクアセスメント

九州大学

■情報資産の洗い出し・リスクアセスメント手順

① ISMS適用範囲の決定

② ISMS適用範囲内の情報資産洗い出し

③ リスクアセスメントの実施

④ リスク低減対策内容の検討と実施

3. 情報資産の洗い出しとリスクアセスメント

九州大学

① ISMS適用範囲の決定

事業・組織・所在地・資産・技術の5つの観点から、セキュリティを守りたい範囲（ISMS適用範囲）を決定する

1. 事　業　実施しているどの事業に？
2. 組　織　どの部署に？
3. 所在地　どこの事業所に？
4. 資　産　どの情報資産に？
5. 技　術　情報資産を維持・管理するための特殊な技術は？

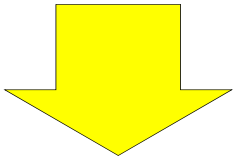
3. 情報資産の洗い出しとリスクアセスメント

九州大学

② 情報資産の洗い出し

ISMS適用範囲内における

1. 業務項目をリストアップし・・・
2. 具体的な業務プロセス（業務フロー）を明確にし・・・
3. 業務プロセスに関連する「情報資産」をリストアップする



保護すべき情報資産が確定！

3. 情報資産の洗い出しとリスクアセスメント

九州大学

③ リスクアセスメント

リスクアセスメントとは、

- 保護すべき情報資産に対する脅威と脆弱性を特定し、発生頻度などのデータに基づき、どれだけの影響があるかを評価すること

- 情報セキュリティの分野では、情報資産を**機密性**、**完全性**、**可用性**の観点からリスクを評価する

3. 情報資産の洗い出しとリスクアセスメント

- **機密性（Confidentiality）**

  アクセスを許可された者だけが情報にアクセスできるようにすること。IDとパスワードによる個人認証などが機密性を高める対策となる。

- **完全性（Integrity）**

  情報や情報の処理方法が、正確かつ完全である（改竄されていない）ことを保護すること。悪意のあるコードの侵入防止などが完全性を高める対策となる。

- **可用性（Availability）**

  許可された利用者が、必要な時に情報資産にアクセスできるようにすること。回線の二重化やバックアップシステムなどが可用性を高めるための対策となる。

3. 情報資産の洗い出しとリスクアセスメント

九州大学

④ リスク低減対策内容の検討と実施

リスクアセスメントの結果を受け、下記の4つの方針から対応を検討・選択し、これを実施する

1. リスク低減　対策を講じ脅威を遠ざける（管理策適用）
2. リスク受容　リスクを受け入れる
3. リスク回避　リスクの原因を回避する
4. リスク移転　リスクをISMS適用範囲外に移転する

4. ISMS運用 - PDCAサイクル

九州大学

■PDCAサイクルを利用した運用

ISMSでは、セキュリティルールを策定し、

PDCA

【Plan（計画）-Do（実施）-Check（点検・監査）-Act（見直し・監査）】

を繰り返し、継続的な改善を実施する

4. ISMS運用 - PDCAサイクル

九州大学

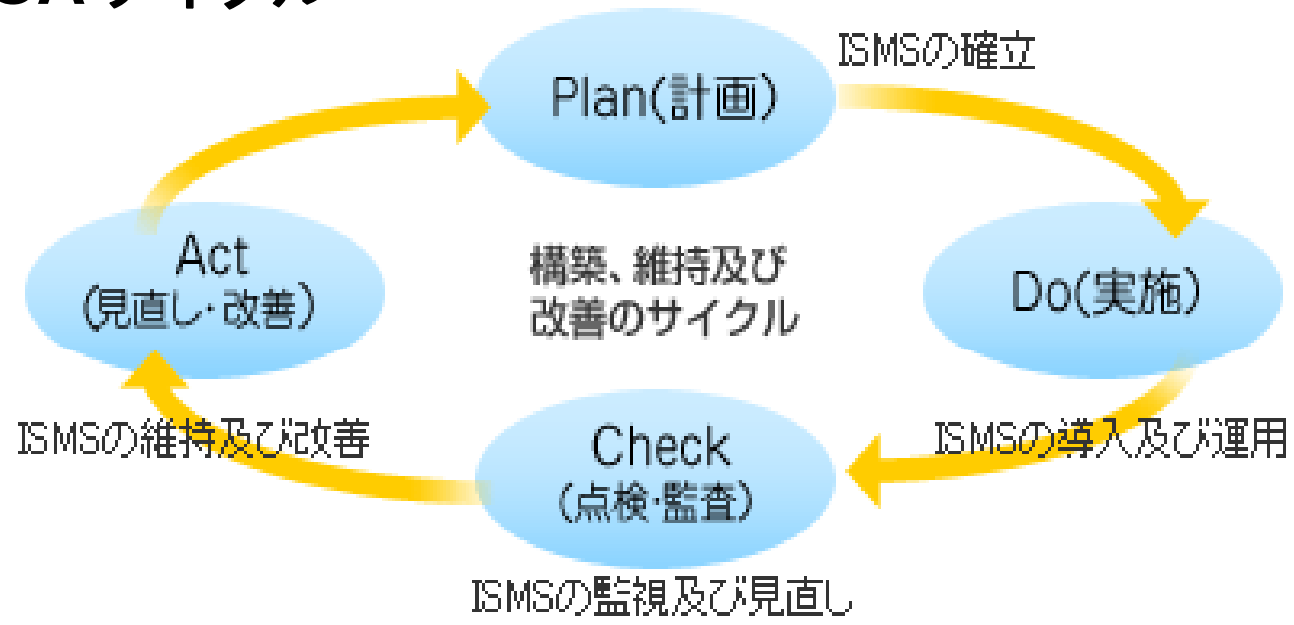
■ISMSにおけるPDCAとは

Plan 【計画】	【ISMSの確立】 ISMSに必要なルールの確立や文書等の作成、適用範囲の設定等、ISMSの形づくりを行う
Do 【実施】	【ISMSの導入及び運用】 Planフェーズで確立したISMSを実施・運用する
Check 【点検・監査】	【ISMSの監視及び見直し】 実施・運用したISMSの内容をチェックする
Act 【見直し・改善】	【ISMSの維持及び改善】 チェックの結果、発見された問題に対して改善計画を立て、これを実施する

4. ISMS運用 - PDCAサイクル

九州大学

■PDCAサイクル



POINT!

継続的改善をPDCAサイクルに従い
実施(運用)することが極めて重要

4. 情報統括本部におけるISMSの活動

九州大学

■ISMS認証取得までの経緯

【事前調査・検討及び具体的な方針の決定】

- 平成22年06月 『ISMS導入準備WG』を設置し、事前調査・検討を開始
- 平成22年12月 ISMS構築及び認証取得に向け、具体的な方針が決定

【ISMS構築及び認証取得に向け本格始動】

- 平成23年01月 『ISMS導入プロジェクト』発足
- 平成23年10月 『ISMS基本方針』制定
- 平成23年11月 『ISMS事務局』設置
- 平成24年02月 第三者認証機関によるISMS認証審査（ステージ1）受審
- 平成24年03月 同認証審査（ステージ2）受審
- 平成24年03月 ISMS認証取得
- 平成24年04月 『ISMS運用事業室』設置

4. 情報統括本部におけるISMSの活動

九州大学

■ISMS適用範囲の定義

【ISMS適用範囲（事業）】

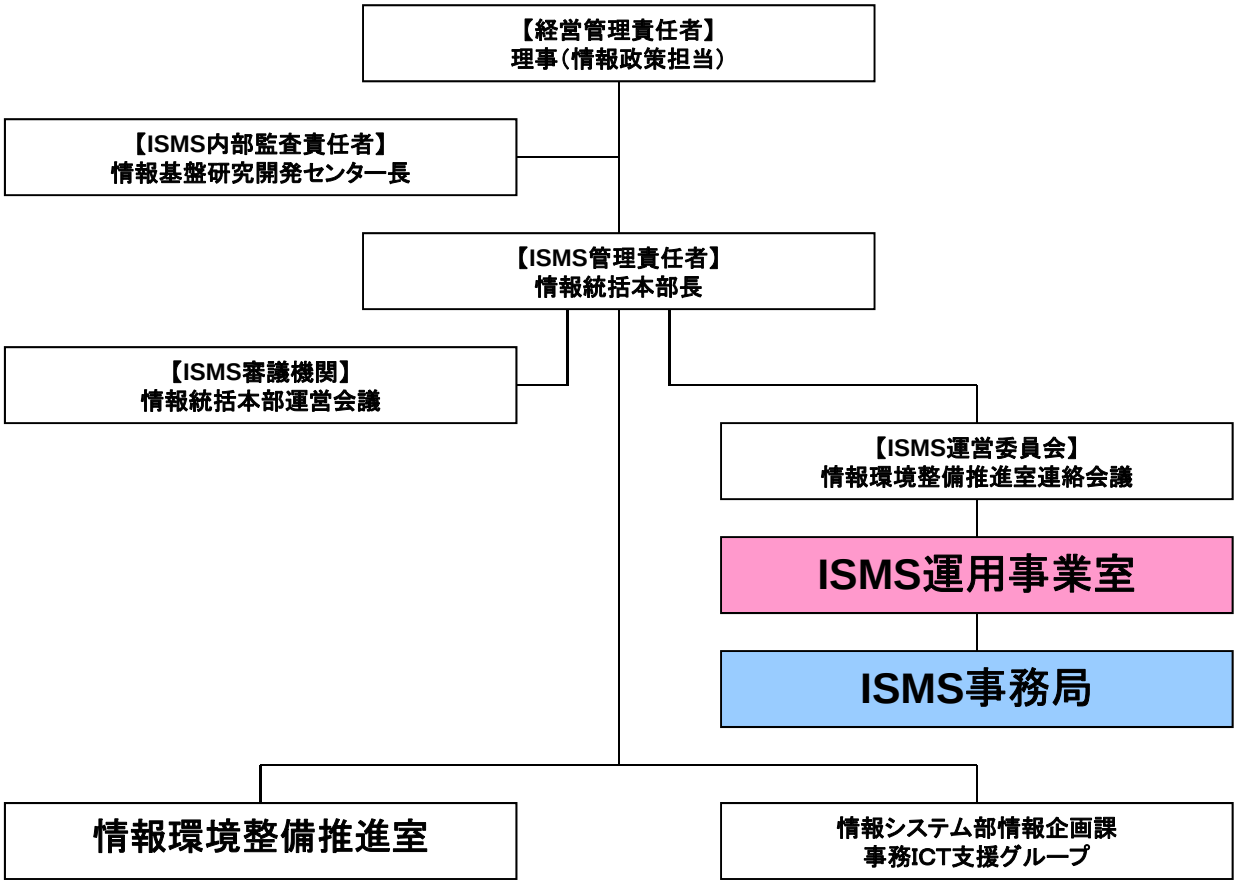
1. 情報環境整備推進室が提供する情報サービス
2. 情報システム部情報企画課事務ICT支援グループが提供する業務システムサービス

上記を事業の適用範囲とし、これに関連する組織・所在地・資産・技術の観点から、情報統括本部のISMS適用範囲を定めている（「ISMSマニュアル_§421」を参照）

4. 情報統括本部におけるISMSの活動

九州大学

■ISMS運用体制図



4. 情報統括本部におけるISMSの活動

九州大学

■運用部署

●ISMS運用事業室

- 情報統括本部におけるISMS活動の継続的な運用と、学内への普及促進を目的として設置
- スタッフは情報環境整備推進室の各事業室，情報企画課事務ICT支援グループ及びISMS事務局から各1名以上を選出
- 活動概要
  - ISMS活動の年間計画策定
  - ISMS文書類，運用方法等の見直し・改訂
  - リスクアセスメント方法の見直し・改善
  - ISMS内部監査の運用
  - マネジメントレビューの対応
  - 第三者認証機関による継続・更新審査の対応
  - 学内のISMS普及促進のための対応　など

4. 情報統括本部におけるISMSの活動

九州大学

■運用部署

●ISMS事務局

- 情報統括本部におけるISMSの管理を行うために設置
- 情報システム部の各グループ、および情報基盤課情報管理室から推薦された者　若干名で構成
- 活動概要
  - ISMS活動に係る原案作成等に関すること
  - ISMS活動に係る各種文書等の管理に関すること
  - ISMSに係る各種計画、手順等の実施管理に関すること
  - ISMSに係る各種手続きに関すること
  - その他

4. 情報統括本部におけるISMSの活動

九州大学

■ISMSの主な年間イベントスケジュール

フェーズ	実施時期	イベント項目
Plan 【計画】	4月～6月	○ISMS文書の見直し ○情報資産の洗い出し ○リスクアセスメントの実施
Do 【実施】	7月～9月	○教育・訓練の実施 ○リスク対応計画の策定 ○マネジメントレビュー（リスク対応計画） ○リスク対応計画の実施
Check 【点検・監査】	10月～12月	○内部監査実施（管理策の有効性測定含む） ○マネジメントレビュー（全体） ○リスク対応計画の更新
Act 【見直し・改善】	1月～3月	○是正処置・予防処置の実施 ○次年度のISMS作業スケジュール作成・周知 ○第三者認証機関による継続・更新審査実施

4. 情報統括本部におけるISMSの活動

九州大学

■ISMS関連文書

- **ISMSマニュアル【第1階層文書】**
  情報統括本部におけるISMSの概要及び具体的な手順

- **ISMS文書（規範類）【第2階層文書】**
  第1階層文書を補足し、情報統括本部における具体的な情報セキュリティに関連する業務の基準、規範、ルール及び手順について記述した文書

- **ISMS文書（様式類）【第3階層文書】**
  活動実績、データ収集など、記録・報告用の各種様式