KYUSHU UNIVERSITY 100th 2011
知の新世紀を拓く

九州大学情報統括本部における ISMSの構築・認証取得への取り組み

九州大学　情報統括本部　ISMS運用事業室

2013年5月

九州大学
KYUSHU UNIVERSITY

概　要

九州大学

1. 背景

2. ISMS導入に向けた取り組み

3. 導入作業において苦労した点と課題

4. 導入作業を終えて感じた反省点

5. ISMS導入の評価ポイント

6. 認証取得後の運用状況

概　要

九州大学

1. 背景

2. ISMS導入に向けた取り組み

3. 導入作業において苦労した点と課題

4. 導入作業を終えて感じた反省点

5. ISMS導入の評価ポイント

6. 認証取得後の運用状況

1. 背景

■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）

を**平成23年度内に導入**することを目標に掲げた

【中期目標　33】

3. 法令遵守に関する目標

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

1. 背景

九州大学

情報統括本部のサービス

Information Infrastructure Initiative, Kyushu University

全国共同利用サービス

- 研究用スーパーコンピュータ

教育支援サービス

- 教育情報サービス
- 附属図書館付設教材開発センター

ネットワークサービス

- ネットワーク

ISMS認証関係

- ISMS認証関係

その他の学内向けサービス

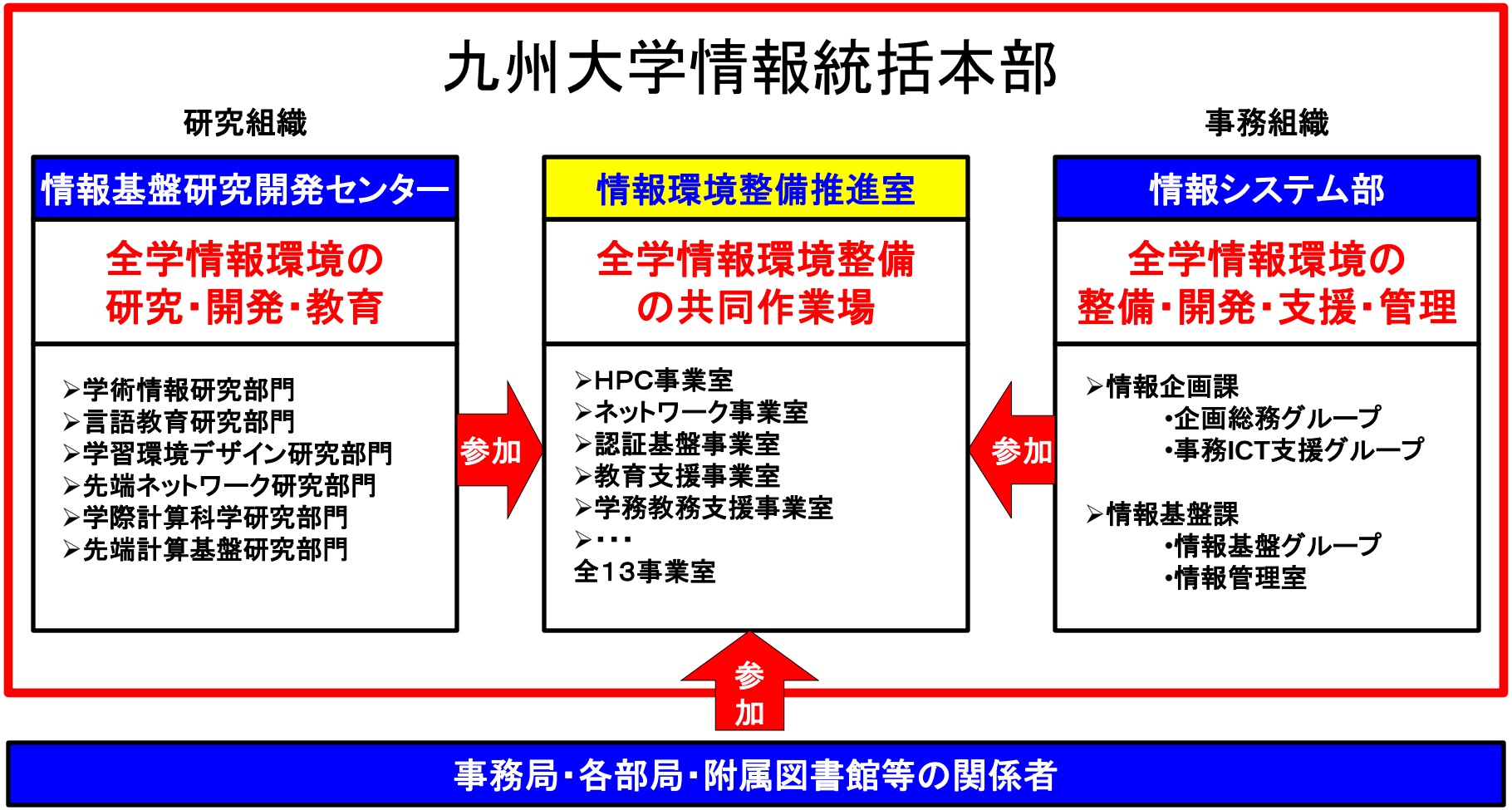
- ソフトウェア
- 全学基本メール
- 学生基本メール
- ICカード(学生証, 職員証)
- 全学共通ID(SSO-KID, 学生ID)
- 遠隔講義・会議システム
- Web会議システム
- 各種サーバのホスティング
- ファイル共有システム

電子図書館

- 図書館Webシステム
- 学術情報リポジトリQIR

1. 背景

■九州大学情報統括本部の組織構成



概　要

九州大学

1. 背景

2. ISMS導入に向けた取り組み

3. 導入作業において苦労した点と課題

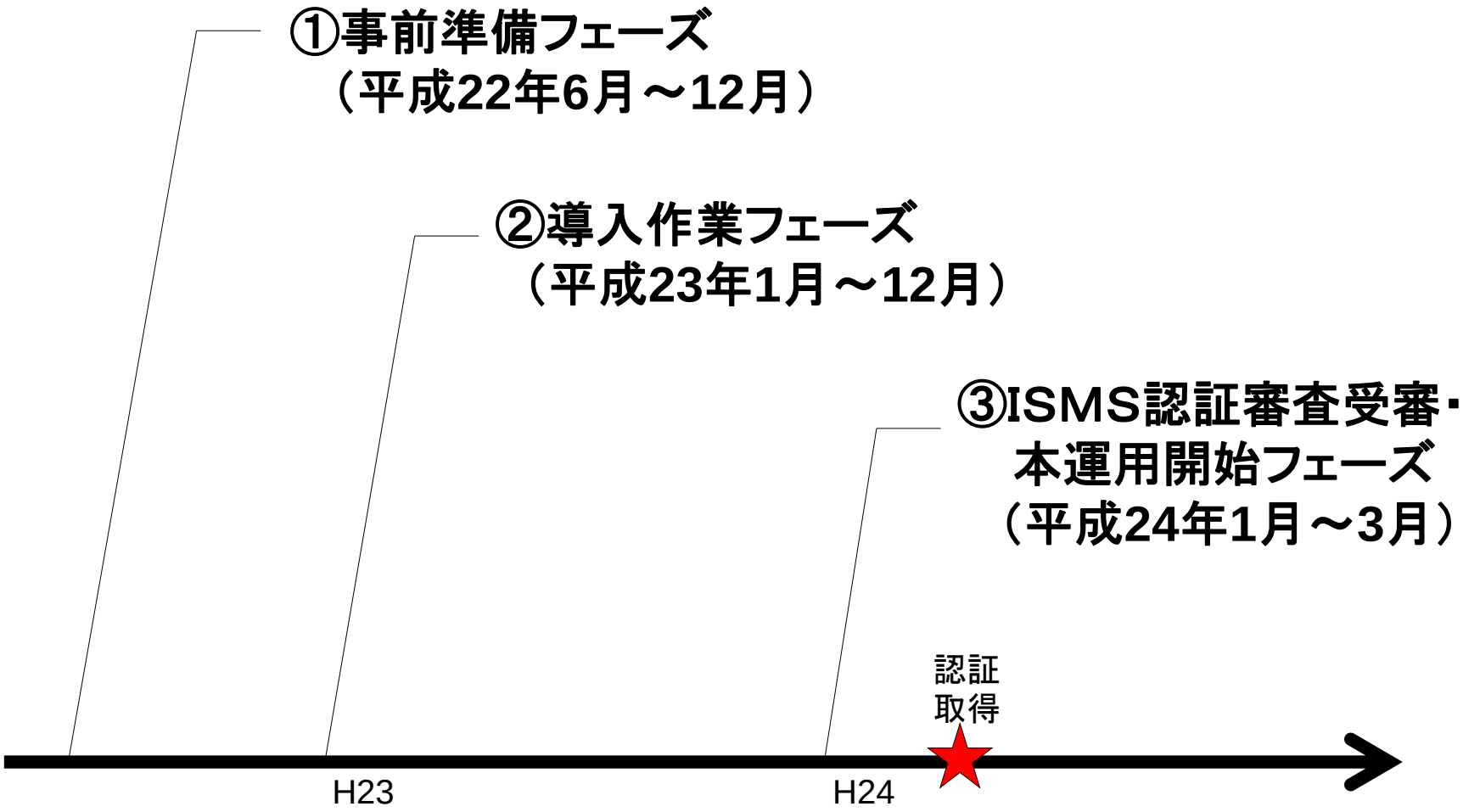
4. 導入作業を終えて感じた反省点

5. ISMS導入の評価ポイント

6. 認証取得後の運用状況

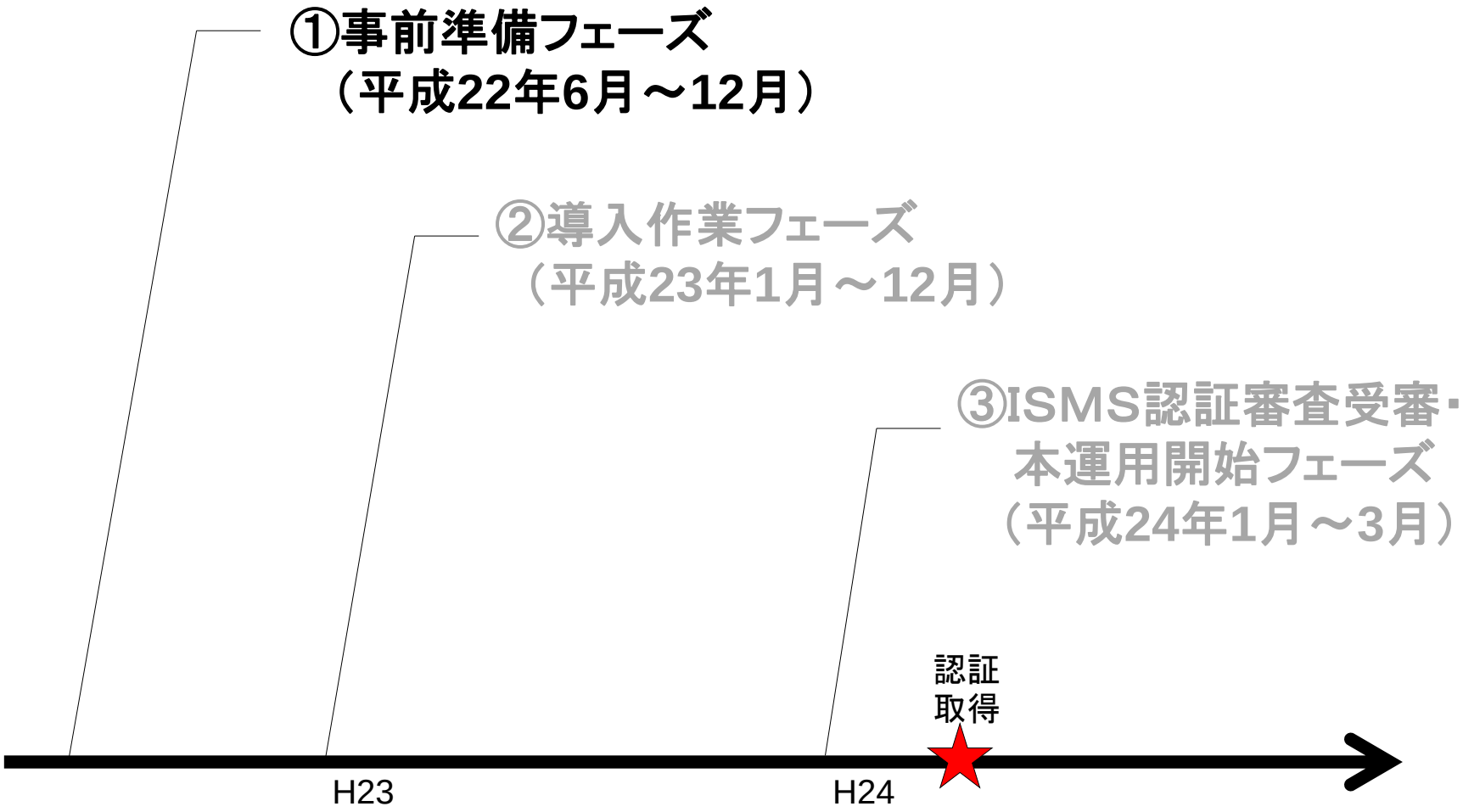
2. ISMS導入に向けた取り組み

■ISMS導入に向けた作業スケジュール概要



2. ISMS導入に向けた取り組み

■ISMS導入に向けた作業スケジュール概要



2. ISMS導入に向けた取り組み

①事前準備フェーズ詳細

■ 平成22年6月

- ISMS導入準備WGを設置
- 情報統括本部事務職員5名で構成
- 主な活動内容
  - 他大学等の事例調査・研究等の予備調査実施
  - ISMS適用範囲／方針案の作成
  - ISMS構築作業スケジュール案の作成

■ 平成22年12月

- 経営陣等に対して成果を報告

2. ISMS導入に向けた取り組み

①事前準備フェーズ詳細

■ 平成22年12月　成果報告書の内容

- ISMS認証を受けることの適切性
- 他の国立大学の状況
- 経営陣の関与の重要性
- 適用範囲の案（事業／組織／所在地／情報資産／技術）
- ISMS基本方針の案
- 認証取得までのスケジュール＆体制
- 必要経費
- コンサルタントの活用

2. ISMS導入に向けた取り組み

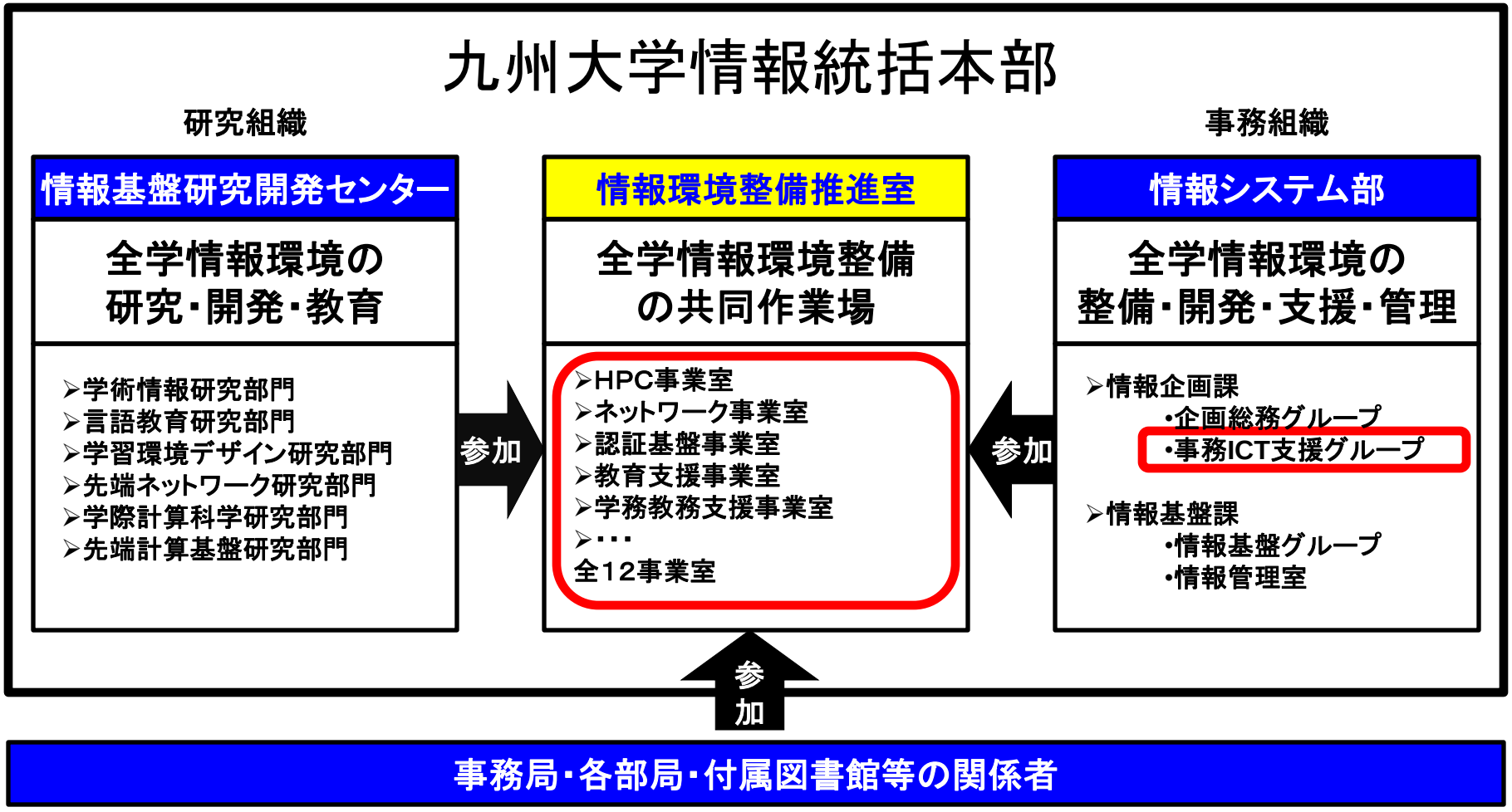
①事前準備フェーズ詳細

■ 適用範囲の2案

	A案	B案
事業	情報シスステム部情報企画課事務ICTグループが管理・運営する情報システムによって提供される事務組織向けのサービス	情報統括本部情報環境整備推進室が管理運営する情報システムによって提供される学内向けのサービス（研究関連のサービスを除く）
組織	情報システム部情報企画課事務ICT支援グループ 構成員　15名	情報統括本部情報環境整備推進室 構成員　82名
所在地	情報システム部情報企画課事務ICT支援グループ(事務局第一庁舎内)	情報基盤研究開発センター 附属図書館 情報統括本部伊都分室

2. ISMS導入に向けた取り組み

■九州大学情報統括本部の組織構成



2. ISMS導入に向けた取り組み

①事前準備フェーズ詳細

情報統括本部における**ISMS適用範囲**、および**作業体制**が決定！

■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**

■ISMS認証取得までの作業体制が決定

平成23年1月に**ISMS導入プロジェクト**を設置し、本組織を中心として、**平成24年3月のISMS認証取得を目指す**

2. ISMS導入に向けた取り組み

■ISMS導入に向けた作業スケジュール概要

①事前準備フェーズ
（平成22年6月～12月）

②導入作業フェーズ
（平成23年1月～12月）

③ISMS認証審査受審・
本運用開始フェーズ
（平成24年1月～3月）

2. ISMS導入に向けた取り組み

②導入作業フェーズ詳細

■平成23年1月

◆ISMS導入プロジェクトの設置

- 情報統括本部の教職員9名で構成
  - 教員4名　：　プロジェクトリーダー、副リーダー
情報セキュリティに強い教員
  - 事務職員5名　：　準備WGのメンバー
- 隔週ミーティング
  - 計30回以上
  - 事務職員はさらにコンサルを交えた準備ミーティング

2. ISMS導入に向けた取り組み

九州大学

②導入作業フェーズ詳細

■主な作業（平成23年1月~12月）

	ISMS導入プロジェクト	各事業室＆事務ICT支援G
資産洗い出し ~H23. 8	・特定方法の整理 •各事業室への依頼＆とりまとめ	•洗い出し作業
リスクアセスメント ~H23.9	•基準および手順の作成 •各事業室への依頼＆とりまとめ	•リスクアセスメント作業
リスク対応 H23.9~	•各事業室への依頼＆とりまとめ •適用宣言書作成	•リスク対応方法検討 •管理策の実態調査
内部監査 H23.12~	・訓練、計画、チェックシート作成 ・監査員への依頼＆とりまとめ	・被監査 ・指摘事項への対応
その他	・説明会やヒアリング実施 ・適用範囲や基本方針の検討 ・経営陣への説明 ・各文書類の素案作成　　など	・事業継続計画作成 ・是正措置、予防措置実施

2. ISMS導入に向けた取り組み

②導入作業フェーズ詳細

■文書化

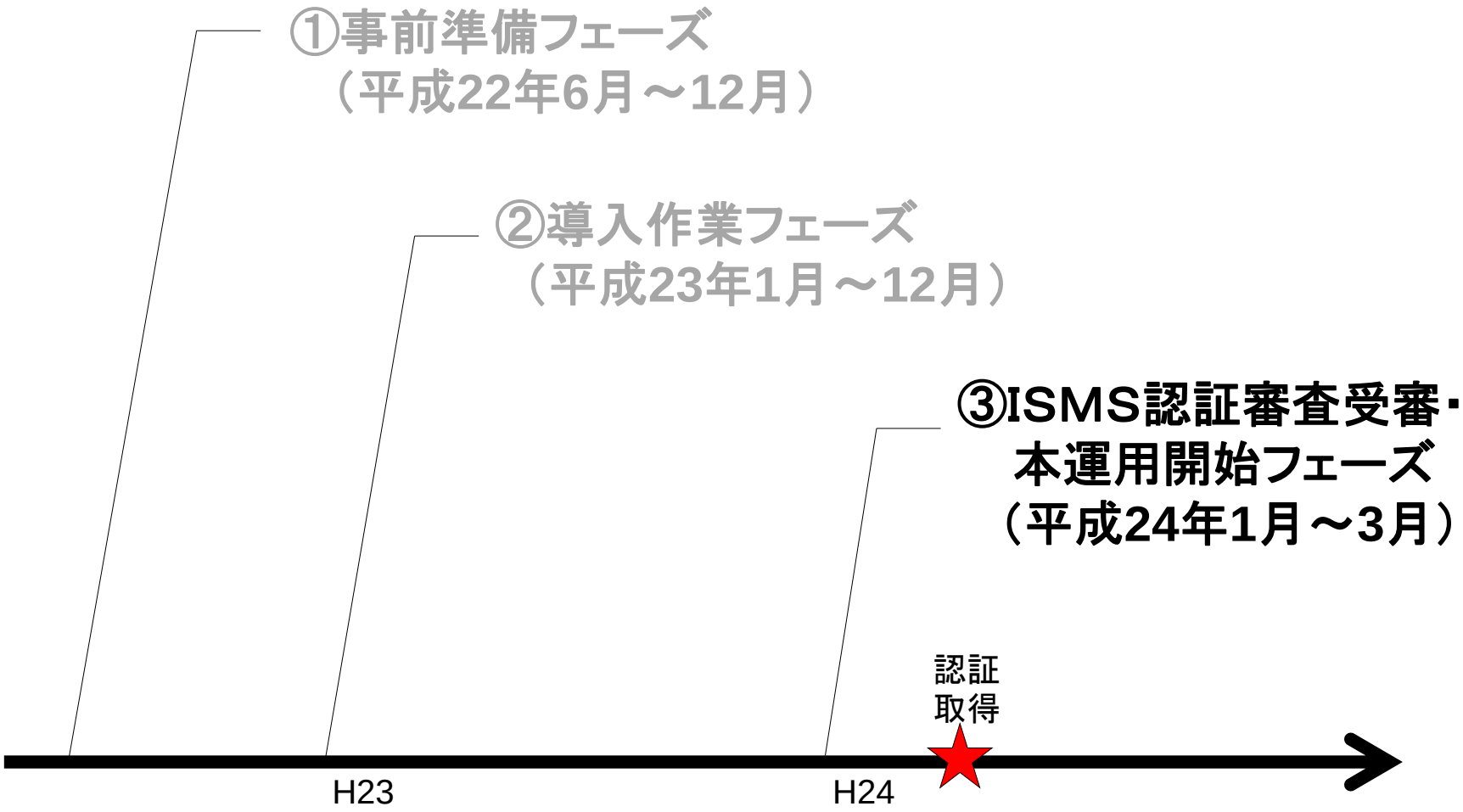
◆導入プロジェクトでセクションごとに担当決め

◆コンサルタント提供の雛型を活用して作成

- **ISMS第１階層文書【ISMSマニュアル】**
  情報統括本部におけるISMSの概要及び具体的な手順
- **ISMS第２階層文書【文書・規範類】**
  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第３階層文書【様式類】**
  活動実績、データ収集など、記録・報告用の各種様式

2. ISMS導入に向けた取り組み

■ISMS導入に向けた作業スケジュール概要



2. ISMS導入に向けた取り組み

③ISMS認証審査受審・本運用開始フェーズ

■平成24年1月

◆ISMS認証取得審査の受審準備

- ISMS関連文書（手順書・マニュアル・記録類）の整理
- ISMS認証取得審査受審対応者への事前説明会実施

■平成24年2月～3月

◆ISMS認証審査受審

- 第一次審査（書類審査）
  - 主にISMS導入プロジェクトスタッフが対応
- 第二次審査（実地審査）
  - 主にISMS導入プロジェクトスタッフ、および各事業室等の責任者／実務担当者が対応

2. ISMS導入に向けた取り組み

③ISMS認証審査受審・本運用開始フェーズ

■平成24年3月

ISMS認証を取得！


Certificate of Registration

情報セキュリティマネジメントシステム

BSI

概　要

九州大学

1. 背景

2. ISMS導入に向けた取り組み

3. 導入作業において苦労した点と課題

4. 導入作業を終えて感じた反省点

5. ISMS導入の評価ポイント

6. 認証取得後の運用状況

3. 導入作業において苦労した点と課題

■苦労した点

■ リスクアセスメント

◆リスク評価基準を作成

◆リスク評価基準をもとに、各情報資産の価値・脅威・脆弱性の視点からリスクレベルを判定し、総合的なリスク評価を行う
各担当者に作業を依頼するも、以下のような不満の声が・・・

●リスク評価基準が具体性に欠けるため、評価作業が難しい

●考えられる脅威や脆弱性について、どこまで検討すればよいのかわからない・・・

**その結果、各担当者に対して個別に説明をしながら作業を実施
結果的に本作業には約4ヶ月を費やすこととなった**

資産価値			個人情報の有無	脅　威		脆弱性			リスク値		
C(機密性)	I(完全性)	A(可用性)		区分	頻度	C(機密性)	I(完全性)	A(可用性)	C	I	A
1～4	1～4	1～4	1:無 2:有		1～4	1～4	1～4	1～4	1～64	1～64	1～64
3	4	4	2	[A]	1	1	3	3	3	12	12
3	4	4	2	[B]	1	1	2	2	3	8	8
3	4	4	2	[C]	2	1	2	2	6	16	16
3	4	4	2	[D]	3	2	2	2	18	24	24
3	4	4	2	[E]	1	2	2	2	6	8	8

資産価値			個人情報の有無	脅　威		脆弱性			リスク値		
C(機密性)	I(完全性)	A(可用性)		区分	頻度	C(機密性)	I(完全性)	A(可用性)	C	I	A
1～4	1～4	1～4	1:無 2:有		1～4	1～4	1～4	1～4	1～64	1～64	1～64
3	4	4	2	[A]	1	1	3	3	3	12	12
3	4	4	2	[B]	1	1	2	2	3	8	8
3	4	4	2	[C]	2	1	2	2	6	16	16
3	4	4	2	[D]	3	2	2	2	18	24	24
3											8

資産価値評価　機密性

1：機密性が損なわれても業務やサービスへの影響が小
2：機密性が損なわれると業務やサービスにかなり影響
3：機密性が損なわれると業務担当部署に甚大な被害
4：機密性が損なわれるとユーザーや大学へ甚大な被害

資産価値			個人情報の有無	脅　威		脆弱性			リスク値		
C(機密性)	I(完全性)	A(可用性)		区分	頻度	C(機密性)	I(完全性)	A(可用性)	C	I	A
1～4	1～4	1～4	1:無 2:有		1～4	1～4	1～4	1～4	1～64	1～64	1～64
3	4	4	2	[A]	1	1	3	3	3	12	12
3	4	4	2	[B]	1	1	2	2	3	8	8
3	4	4	2	[C]	2	1	2	2	6	16	16
3	4	4	2	[D]	3	2	2	2	18	24	24
3											8

脅威区分
A ライフ的環境脅威、B システム的環境脅威、C 物質的脅威
D 内部からの人的脅威、 E 外部からの人的脅威

脅威頻度
1: 数年に1回程度発生する　2: 年に1回程度発生する
3: 年に数回程度発生する　4: 月に1回程度発生する

資産価値			個人情報の有無	脅威		脆弱性			リスク値		
C(機密性)	I(完全性)	A(可用性)		区分	頻度	C(機密性)	I(完全性)	A(可用性)	C	I	A
1～4	1～4	1～4	1:無 2:有		1～4	1～4	1～4	1～4	1～64	1～64	1～64
3	4	4	2	[A]	1	1	3	3	3	12	12
3	4	4	2	[B]	1	1	2	2	3	8	8
3	4	4	2	[C]	2	1	2	2	6	16	16
3	4	4	2	[D]	3	2	2	2	18	24	24

脆弱性レベル

1：適切な管理策が講じられているため脅威が発生しても極めて安全である。
2：管理策が講じられているため、脅威が発生しても安全である。
3：一応管理策が講じられており、脅威が発生してもある程度防御できるが、改善の余地がある。
4：管理策が講じられておらず、脅威が発生すると防御できない。

資産価値			個人情報の有無	脅威		脆弱性			リスク値		
C(機密性)	I(完全性)	A(可用性)		区分	頻度	C(機密性)	I(完全性)	A(可用性)	C	I	A
1～4	1～4	1～4	1:無 2:有		1～4	1～4	1～4	1～4	1～64	1～64	1～64
3	4	4	2	[A]	1	1	3	3	3	12	12
3	4	4	2	[B]	1	1	2	2	3	8	8
3	4	4	2	[C]	2	1	2	2	6	16	16
3	4	4	2	[D]	3	2	2	2	18	24	24
3	4	4	2	[E]	1	2	2	2	6	8	8

情報セキュリティリスク値
= 資産価値レベル　×　脅威レベル　×　脆弱性レベル

3. 導入作業において苦労した点と課題

■課題

■ リスクアセスメント方法の見直し

リスク評価基準があいまいで具体性に欠ける・・・

【例】情報資産の価値判定基準

機密性が損なわれると**業務やサービスにかなり影響** ⇒ レベル“2”

など・・・

↓

■作業の負担感軽減の必要性を痛感
■組織として、リスク評価結果の平準化が必要

↓

より具体的なリスク評価基準を構築する必要あり！

概　要

九州大学

1. 背景

2. ISMS導入に向けた取り組み

3. 導入作業において苦労した点と課題

4. 導入作業を終えて感じた反省点

5. ISMS導入の評価ポイント

6. 認証取得後の運用状況

4. 導入作業を終えて感じた反省点

■反省点

関係者に対し、早期に理解を深めて頂くことが必要であった

- 情報資産の洗い出しやリスクアセスメント作業、ISMSマニュアル等の作成作業に追われ、関係者への詳細説明が大幅に遅れた
- その結果、関係者の理解度などにばらつきが生じ・・・
- リスクアセスメントや内部監査など、その趣旨や内容がよく理解できなかったため、「余計な仕事が増えた・・・」などの感覚が出てしまう
- 内部監査において、監査員が趣旨を理解していなかったため、被監査部署は「粗探し」を受けたと勘違いしてしまった

概　要

九州大学

1. 背景

2. ISMS導入に向けた取り組み

3. 導入作業において苦労した点と課題

4. 導入作業を終えて感じた反省点

5. ISMS導入の評価ポイント

6. 認証取得後の運用状況

5. ISMS導入の評価ポイント

■評価点

◆教職員のセキュリティに対する意識の向上

- 管理責任者だけではなく、教職員ひとりひとりの“情報保護”に対する意識が高まり、情報保護やコンプライアンスに対する責任感が強まった
- 会議や会話のなかで「ISMS的には問題ないか？」などの発言も多くなり、情報セキュリティに対する意識がより一層高まった

◆事業運営の効率化・安全性の向上

- リスクアセスメントや内部監査を通じ、“結果としての安全性”よりも、“将来の原因となり得る危険性”に着眼し、“予防”という視点で業務効率化、或いは安全性確保を目指そうとする体制が構築できた（組織力向上）
- 効果はすぐに現れ始め・・・
  サーバ室や執務室が今まで以上に整理・整頓されるなど、効果覿面！

概　要

九州大学

1. 背景

2. ISMS導入に向けた取り組み

3. 導入作業において苦労した点と課題

4. 導入作業を終えて感じた反省点

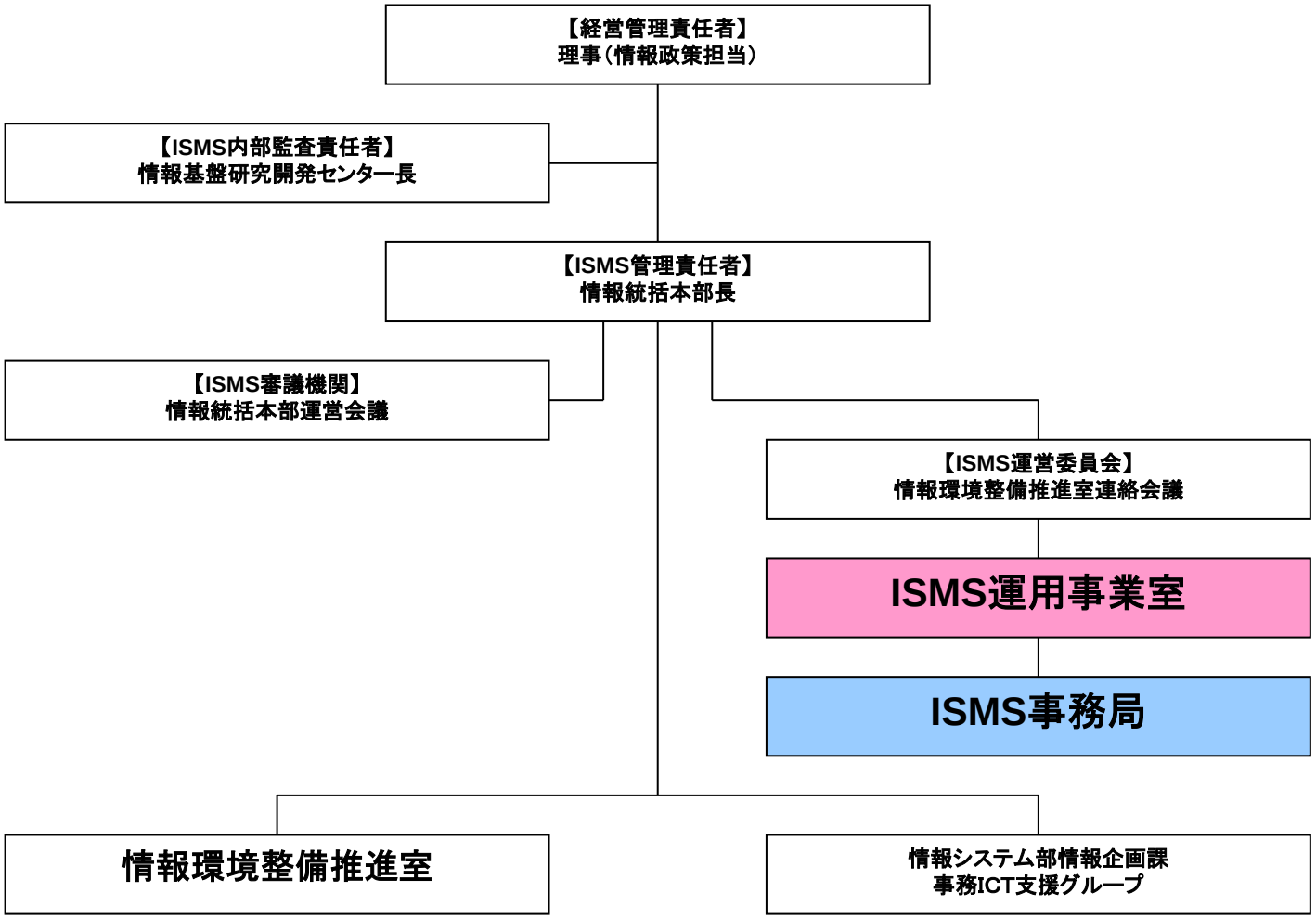
5. ISMS導入の評価ポイント

6. 認証取得後の運用状況

6. 認証取得後の運用状況

九州大学

■ISMS運用体制図



6. 認証取得後の運用状況

■運用部署

●ISMS事務局（平成23年11月～）

- 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

6. 認証取得後の運用状況

■運用部署

●ISMS運用事業室（平成24年4月～）

- 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　　合計15名
- 事業室長は事務部長
- 隔週で会議
- 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

6. 認証取得後の運用状況

九州大学

■平成24年度 ISMSの主なイベント

実施時期	イベント項目
4月	新任者説明会
5～6月	適用範囲、ISMS基本方針等確認
7月	内部監査員養成研修 ISMS標語コンクール実施 全体説明会
8～10月	リスクアセスメント実施、リスク対応計画検討 内部監査実施
11～1月	リスク対応計画を実施 内部監査による是正措置の検討・実施 事業継続計画、予防措置、管理策の有効性測定などの検討
2月	マネジメントレビュー ISMS継続審査

6. 認証取得後の運用状況

九州大学

■標語コンクール

- マネジメントレビューでのアウトプット項目
- 構成員全員のISMSに対する姿勢や意識向上

最優秀賞

護(まも)ろうよ、決めたルールで、リスク回避

優秀賞

セキュリティ　意識と実行　統括本部

備えようISMS！　日頃の努力が報われる

いつも 気にする改善点　すぐに 適用管理策　みごと 成功リスク低減　そして　安心情報セキュリティ

6. 認証取得後の運用状況

九州大学

■リスクアセスメント

- 平準化の試み
  - 事業室のグループ化で相互確認
    1. HPC事業室、ネットワーク事業室、教育支援事事業室
    2. 認証基盤事業室、学務教務支援事業室、ソフトウェア事業室
    3. 、、、、
    4. 、、、、、
- リスク受容基準を越える資産が大幅に減少

6. 認証取得後の運用状況

九州大学

■内部監査

- 実施回数を年2回から1回へ
- 内部監査員有資格者の拡大
- 合意形成の重視

時期	実施項目	実施内容詳細
6月	内部監査計画立案	○内部監査責任者は、監査方針・監査項目・監査方法等を立案
7月	内部監査員養成研修の開催	○外部専門機関による「内部監査員養成研修」の開催 ○内部監査員養成研修受講修了者を「内部監査員」有資格者として認定（部内資格）
8月	内部監査員選出	○各事業室等より「内部監査員」を1名選出 ○内部監査員2～3名を1組とした「監査チーム」を編成
9月	内部監査実施通知	○内部監査実施スケジュール作成（「監査の独立性」を確保） ○各事業室等の長に監査実施を通知
10月	内部監査の実施	○内部監査の実施
11月	報告書の作成	○内部監査報告書作成（全事業室等）
	改善指示	○発見事項報告書作成　⇒　対象事業室等に改善指示 ○対象の事業室等は改善計画を立案・実施する
12月	改善状況の確認	○フォロー監査実施　⇒　発見事項報告書に結果を記載 ○内部監査責任者に結果を報告
1月	内部監査の実施結果報告	○マネジメントレビューにて、経営陣に内部監査実施結果を報告

6. 認証取得後の運用状況

九州大学

■認証取得から1年たっての所感

- 取得してからも大変
- 情報セキュリティへの意識は確実に高まる

■今年度の展開

- リスクアセスメントの平準化をさらに進める
- 情報統括本部外での普及促進

以上で発表を終わります。
御清聴ありがとうございました。