外部評価説明資料

ISMS運用事業室

2017年5月

情報統括本部

九州大学

ISMSとは？

『**I**nformation **S**ecurity **M**anagement **S**ystem』の略で、国際標準化機構（ＩＳＯ）によって国際標準化された情報セキュリティを管理するための枠組み。

国際規格：ISO/IEC 27001 日本工業規格：JIS Q 27001

※「政府機関の情報セキュリティ対策のための統一基準」作成の基準となった規格

ISMSの目的

情報セキュリティに関する「リスクを適切に管理しているという信頼を利害関係者に与えること」

JIPDEC http://www.isms.jipdec.or.jp/isms/index.html

任せて安心

国内大学でのISMS認証取得の状況

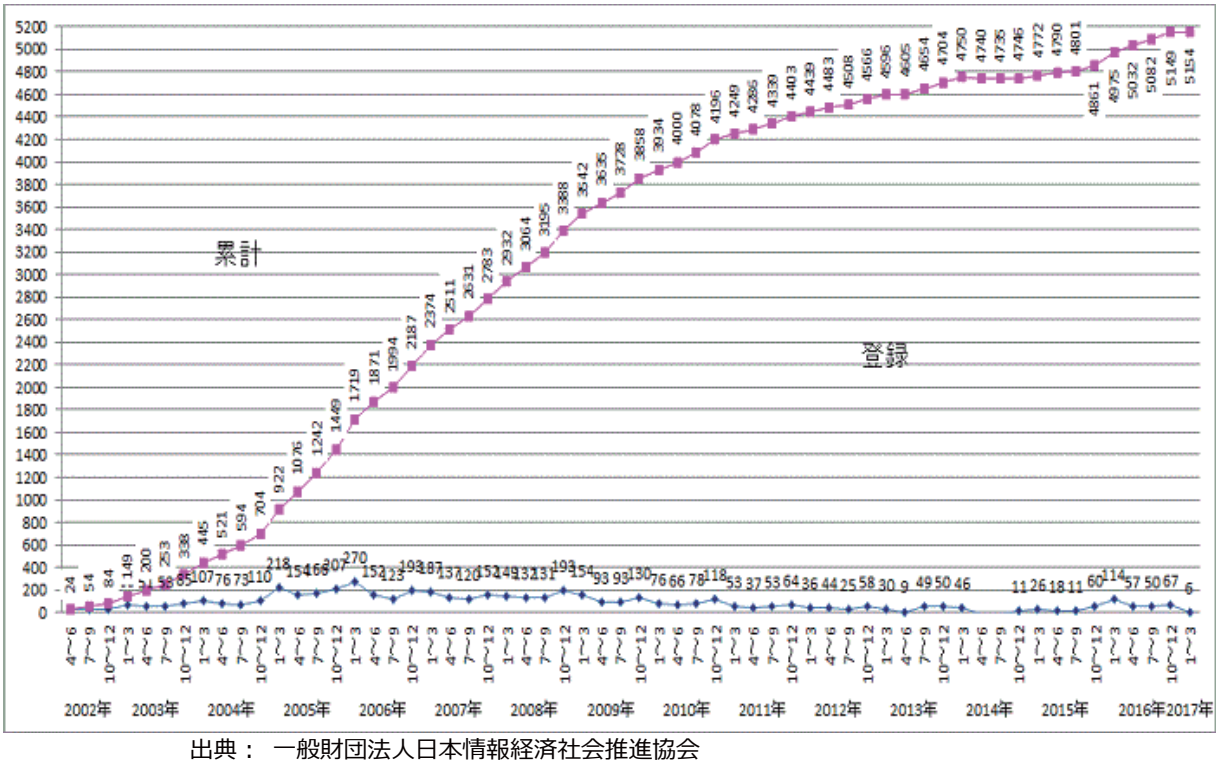
区分	組織名（登録順）	初回登録日
国立大学 12大学	静岡大学（情報基盤センター）	2003年11月25日
	宇都宮大学（総合メディア基盤センター）	2007年11月15日
	山口大学	2008年10月24日
	徳島大学（情報センター）	2012年3月9日
	九州大学　情報統括本部	2012年3月22日
	長崎大学	2013年3月4日
	鹿児島大学（学術情報基盤センター）	2013年4月23日
	岡山大学（情報統括センター）	2013年11月12日
	横浜国立大学（情報基盤センター）	2014年3月6日
	広島大学（情報メディア教育研究センター）	2015年3月27日
	室蘭工業大学（情報メディア教育センター）	2015年3月27日
	琉球大学（(総合情報処理センター)）	2015年4月13日
公立大学	会津大学（復興支援センター）	2015年12月10日
私立大学 4大学	日本福祉大学	2005年3月16日
	早稲田大学（情報企画部）	2007年1月24日
	日本大学（本部 管財部 IT管理課）	2007年12月4日
	帝京大学（本部事務部）	2016年12月22日

全17大学（2017年5月1日調査）

出典：　一般財団法人日本情報経済社会推進協会
ISMS認証取得組織検索
https://isms.jp/lst/ind/index.html

国内でのISMS認証取得状況

認証取得組織　5,152機関（2017年4月12日調査）



出典：　一般財団法人日本情報経済社会推進協会
認証取得組織数推移、認証機関別・県別認証取得組織数　https://isms.jp/lst/ind/suii.html

事業室の概要

事業室のミッション

- 情報統括本部におけるISMS活動の継続的な運用
- 九州大学内へのISMSの普及促進
- 情報セキュリティ対策基本計画の実施

事業室の体制

事業室長	副事業室長	事業室員
坂本 朝治（情報システム部長）	情報統括本部専門員 1	課長 2，課員13

事業室の業務

ISMSの規格による各種イベントの企画・実施

- ISMS関係文書（ルール）の見直し
- 説明会（ISMS構成員の知識更新，新任者への解説）
- リスクアセスメント
- 内部監査
- 内部監査員養成研修
- マネジメントレビュー
  - 担当理事への１年間の改善の状況を報告し，承認を受ける。
- ISMS認証機関による審査対応

学内の他部局へのISMS活動の紹介

情報セキュリティ対策の自己点検・監査の企画，実施

連携部局等

情報統括本部のすべての事業室と連携

保有している設備，利用している外部サービス等

保有している設備

- ISMS文書管理用サーバ，バックアップストレージ
- 共用サーバ室（免震サーバ室，ネットワーク室　等）

利用している外部サービス

- ISMS認証審査，サーバ等保守契約

活動状況等（１）

情報統括本部におけるISMSの継続的な運用

- １年間のイベントを通じたISMSによるPDCA推進
- 各事業室が利用するグループウェアの管理運用

※ISMSの適用範囲

（事　業）・情報統括本部情報環境整備推進室が提供する情報サービス
・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

（組　織）「情報統括本部」

（構成員）情報統括本部に所属する教職員（非常勤職員含む）で，上記事業に従事する者

九州大学内でのISMSの普及促進

- ISMSの導入を検討する学内組織への情報提供
- ISMSに準拠した情報セキュリティへの取組み支援
  病院における内部監査の実施　など

活動状況等（２）

情報セキュリティ対策基本計画の推進

- 情報セキュリティポリシー等の組織内浸透
  - 情報の格付け及び取扱制限の規程の作成
  - 情報の格付け等の運用ガイドライン等の原案作成
- 情報セキュリティに係る自己点検・監査の実施
  - 自己点検や監査の規程及び手順書の作成
  - 学内におけるISMSの適用範囲拡大

共用免震サーバ室の管理

- 情報統括本部で共用している免震サーバ室等の管理

実績（１）

内部監査での改善

- 内部監査で発見された課題や問題点を改善している。
- 過去５年間の改善数は，次のとおり。

年度	推奨事項（件）注１	不適合事項（件）注２	計
2012年度	8	0	8
2013年度	4	2	6
2014年度	3	0	3
2015年度	2	5	7
2016年度	7	3	１０

注１：推奨事項：改善を進めるために見直しや検討を勧めるもの
注２：不適合事項：ルールを守っていない等の事例について改善を求めるもの

実績（２）

リスクアセスメントの実施（情報資産のリスク対応）

- 情報サービスの資産についてリスクアセスメントを実施
  - 設定されたリスクを超えるものを理事に報告し，必要な対処（リスク低減，受容　など）を行う。

- 不適合・是正処置（情報サービスのインシデント対応）
  - インシデント発生及び応急処置の報告
  - 原因調査，特定
  - 再発防止のための是正措置の検討，実施，報告
  - 是正処置の有効性測定

※インシデント報告，是正処置提案，是正処置実施結果等はすべて文書で会議に報告される。是正処置の決定，有効性の測定は，会議で審議し，決定する。

実績（３）

ISMS認証機関による審査（指摘事項及びグッドポイント）

- ISMSの認証継続，更新のための認証機関による審査
  - 改善のための指摘事項や Good Point の評価
  - 指摘事項を確実に改善
  - Good Pointの評価で自信を深め，士気向上
- 主な指摘事項（すべて改善，対処済み）

年度	内　　容
2013年度	システムの重要性に応じたバックアップの方針や手順の検討を勧めます。
2014年度	廃熱用ファンが非可動状態です。意図的かどうかの確認を勧めます。
2015年度	事業継続計画の試験を実施したことが確認できない。
〃	マニュアルの改版履歴に誤りがあった。
2016年度	適用法令一覧表を最新に保つことを勧めます。

実績（４）

- 主なGood　Point

年度	区分	内　　容
2013年度	学務教務支援事業室	入試データの処理フローが可視化されている。
2014年度	事務ICT支援グループ	サーバの起動等の手順がわかりやすくまとめられている。
2015年度	ISMS事業室	内部監査での指摘事項を全事業室で再度チェックして改善している。
〃	ソフトウェア事業室	ソフトウェア管理システムを開発し運用するとともに，他大学へも提供している。
2016年度	図書館連携事業室	次期導入予定ソフトウェアの受入れ試験を早期に実施している。

2016年度ISMS年間スケジュール

時期	活動事項・内容
4月	○「リスク及び機会に対処する活動計画」案 ○「ISMS 適用範囲定義」および「ISMS 基本方針」の見直し
5～6月	○ISMS 文書見直し ○ISMS普及活動実施計画の検討・立案 ○ISMS マニュアルにおけるISO27001 規格への適合性確認
7月	○ISMS文書改版手続き
8月	○内部監査員養成研修，全体説明会（定期）の実施
9月	○ISMS普及活動計画（他部局への説明会）の実施
10月	○リスクアセスメントと発見されたリスクへの対応
11～12月	○各事業室等におけるISO27001 附属書A 管理策の適用実態確認 ○ISMS 適用宣言書の見直し（素案作成・承認） ○内部監査（監査で違反している状況を発見し，対処）
1月	○マネジメントレビュー
2月	○第三者認証機関（BSI）による維持審査，移転審査
3月	○翌年度のISMS運用スケジュールの検討・決定

成果（1）

- マネジメントレビューによる担当理事への情報提供，指示
  - 情報政策担当理事に，リスクアセスメントや内部監査で明らかになった課題や脅威を直接報告し，その対応について指示をもらう。
- 不適合・是正処置報告による課題解決，再発防止
  - 各事業室のサービスレベルを達成できないインシデントが発生した場合，不適合・是正処置報告書により会議に報告し，その対応策，改善策を検討し，実施した。改善策の効果の検証も行った。
- 内部監査による課題の抽出と改善
  - 内部監査により運用の準拠性をチェック
  - 課題を指摘し，対応策を策定，実施し，効果を検証した。
  - 2016年度は，10件の指摘があり改善された。
- リスクアセスメントによるリスクチェック
  - 情報サービスごとの資産に対する脅威とぜい弱性をチェックし，アセスメントの結果，閾値を超えたものを理事に報告した。

成果（２）

- 改善策の効果の検証
  - 発見された問題の改善策を公開の場で検討し，それを実施し，その効果を検証する。　→　改善を確実なものにする。
- 情報セキュリティを意識して考える姿勢，態度が醸成されつつある。
- 認証機関による審査でのGood Point 評価
  - 毎年の認証機関による審査において，Good Point　の評価を得ることにより，自信が持て，PDCAの改善のサイクルが好循環する。
- 情報セキュリティに関する課題や情報の共有
  - 情報セキュリティに関する課題を情報統括本部で共有
  - 課題等を共同で検討し，方針を決定する開かれた空気を醸成

今後の課題等

今後の課題

- 情報の格付け及び取扱制限の運用，浸透，定着
- 学内へのISMS適用範囲の拡大
- ISMSに係るイベント，手続き等の簡素化

今後の取組み

- 情報の格付けに応じた取扱手順の運用，見直し，浸透
- ISMSの適用範囲を事務局に拡大
  (情報セキュリティ対策基本計画の一環)
  29年度 学務情報システムへの拡大試行
  30年度 学務情報システムへの拡大
  人事・給与，財務会計システムへの拡大試行
- 情報セキュリティ対策基本計画実施のサポート
  - 情報セキュリティ対策の自己点検の実施
  - 情報セキュリティの監査の実施

情報統括本部はISMS（ISO27001）の認証を取得

2012年3月22日にISMS（ISO27001）の認証を取得し，継続中（認証範囲：情報統括本部）

認証証を掲げる安浦理事（右）と竹尾BSIジャパン社長

bsi.

By Royal Charter

Certificate of Registration

情報セキュリティマネジメントシステム

国立大学法人九州大学 情報統括本部
〒812-8581福岡県福岡市東区箱崎6-10-1

上記組織が認証登録番号IS 582429を保有し、また下記認証登録範囲の情報セキュリティマネジメントシステムについて ISO/IEC 27001:2013 / JIS Q 27001:2014 の要求事項に適合していることをここに証します。

認証登録範囲:

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
2014年10月27日付適用宣言書 第4版

上記の所在地が含まれる認証書番号: IS 582429
BSIロケーション番号: 0047430166-000

For and on behalf of BSI:

代表取締役社長 竹尾 直章

初回認証登録日: 2012/03/22
最新更新日: 2016/03/08

発効日: 2015/02/09
有効期限日: 2018/03/21

...making excellence a habit.

ISMS認証証（掲示用）