大学構成員全員を対象とした予防と事後対応手順の紹介: 遵守確認方法の取り組事例

武藏 泰雄

熊本大学総合情報統括センター

情報セキュリティ室

musashi@cc.kumamoto-u.ac.jp

http://www.cc.kumamoto-u.ac.jp/

本日の内容2

1. 準拠性・技術・フォローアップ・妥当性監査について
2. 情報セキュリティ監査支援委託仕様書
3. 監査対象の選定と監査計画書の作成
4. 部局長連絡会議での事前連絡
5. 内部監査人研修会の実施
6. 準拠性監査、技術監査、フォローアップ監査の実施
7. 監査報告書の作成と是正の指示
8. まとめ

準拠性・技術・フォローアップ・妥当性監査の概略

- 情報セキュリティ教育・啓発活動実施の効果測定が必要
- 準拠性監査、技術監査、フォローアップ監査、妥当性監査についてすべて外部支援を外部発注する
- 毎年11月中に内部監査人＋外部監査人で準拠性監査・技術監査・フォローアップ監査を実施する
- 監査対象を決定し、8月ごろから監査対象部署へ通知し、監査担当者、日程の調整を実施する。その後9月～10月までに監査準備を完了する（9月上旬に内部監査人研修を実施）
- 監査実施後、監査報告書を監査室と共同で作成し、監査室長名で、監査対象へ監査調書を送付する
- 是正事項があれば、通達し、是正報告書を求める

行動計画およびスケジュールの策定と承認

- 毎年3月～5月の期間「セキュリティ行動計画」の計画のスケジュールを策定する
- 学内の情報セキュリティ専門委員会・ICT戦略会議で承認
- 主として以下の事項が含まれる
  - ① 次期情報セキュリティ対策計画策定
  - ② 情報セキュリティ教育・啓発活動
  - ③ 情報セキュリティ監査
  - ④ 強化施策（標的型メール攻撃対策訓練・CSIRT訓練）
  - ⑤ 一般業務（管理体制整備、プライベートIP化、情報格付けの更新

行動計画およびスケジュールの策定と承認

- 情報セキュリティ監査

① 準拠性監査（毎年11月に実施、内部監査人＋外部監査人）

② 技術監査（毎年11月に実施、Nesus/Open VAS等を使用）

③ フォローアップ監査（毎年11月・対象は是正指示をした部署等）

④ 妥当性監査

⑤ 内部監査人育成研修（9月）

H31/R1年度情報セキュリティ運営費の決定

- 毎年5月ごろにセキュリティ運営費を決定
- 「セキュリティ行動計画」に基づいて運営費を見積を取り、順次契約を結び執行
- 下記の事項に予算を付ける

① 部局情報セキュリティ責任者向け説明・資料作成

② 部局システム管理者向け集合研修教材・アンケート

③ 教職員向けセキュリティ研修eラーニング教材作成・アンケート集計・自己点検の結果考察・課題分析

④ 準拠性監査・技術監査・フォローアップ監査・妥当性監査

⑤ 基本計画の見直し、作成関する助言

情報セキュリティ監査支援委託仕様書

- 毎年6月末ごろ「セキュリティ行動計画」に基づいて「情報セキュリティ監査支援委託仕様書を作成し、業者と契約
- 業者は、官公庁で過去3年間で3件以上の請負実績を有し、またISO27001/ISO9001/Pマークのどれかを取得していること
- 下記の事項について発注する

① 監査実施計画の作成

② 内部監査人研修の実施

③ 準拠性監査の実施

④ 妥当性監査の実施

⑤ フォローアップ監査の実施

⑥ 準拠性監査、妥当性監査及びフォローアップ監査結果の報告

監査対象の選定と監査計画書の作成

- 毎年7月～8月にかけて本学準拠性監査実施手順書に基づいて監査対象の選定と監査計画書の作成を依頼する

① 監査計画書の作成は毎年3月あたりから作成開始

② 準拠性監査選定対象は20部局等で、毎年対象をすべて変更

③ 技術監査対象は10サーバ（10 IPアドレス、毎年対象をすべて変更）

④ 妥当性監査は監査結果に基づく、セキュリティ関連規則・実施手順の妥当性を評価する（セキュリティフレームワーク、サンプル規定と政府統一基準群などの差分評価）

⑤ フォローアップ監査の対象は前年度の準拠性監査対象部局等で特に再監査が必要と思われる3部局等

⑥ 準拠性監査人名簿: 監査責任者1名、監査実施者14名（総括・準拠性監査）

⑦ フォローアップ監査は準拠性監査期間に同時に実施

部局長連絡会議での事前連絡

- 発信者はCISO＋CISO補佐で、部局長連絡会議（9月）、部局システム管理者向け集合研修（8月）、事務系課長・副課長向け集合研修（9月）において研修教材とともに口頭で通知する
- 監査対象者へメールで正式に通知
- 情報セキュリティeラーニング研修の受講も指示

内部監査人研修会の実施

- 毎年8月末または9月上旬ごろに、準拠性監査実施者の養成のため内部監査人研修会を実施

① グループワークで実施

② 準拠性監査の意義と監査方法の注意

③ 監査人と監査対象者に分かれて準拠性監査実施訓練

④ 監査調書の作成訓練

⑤ 是正指示書の作成訓練

準拠性監査、技術監査、フォローアップ監査の実施

- 準拠性監査に必要な書類を準備と実施

① 監査対象情報の作成（docx）：監査会場、監査対象者名、監査人名等

② 監査日程表の作成（xlsx）：監査の期日・日時。監査対象名、監査人名等

平成30年度 情報セキュリティ監査対象情報 （準拠性監査）

1	部局名等	[redacted]
	受入日時	平成３０年１１月９日（金） １５：００～１７：００
	対応者１	所属 [redacted]
		職名 [redacted]
		氏名 [redacted] 内線番号 [redacted]
		メール [redacted]
		担当業務 [redacted]
	対応者２	所属 [redacted]
		職名 [redacted]
		氏名 [redacted] 内線番号 [redacted]
		メール [redacted]
		担当業務 [redacted]
	上席者	所属 [redacted]
		職名 [redacted]
		氏名 [redacted]
	監査会場	建物名 [redacted]
		階数 [redacted]
		部屋名 [redacted]
2	部局名等	[redacted]
	受入日時	[redacted] １３：００～１５：００
		所属 [redacted]
		職名 [redacted]

平成30年度 情報セキュリティ監査日程表 （1／2）

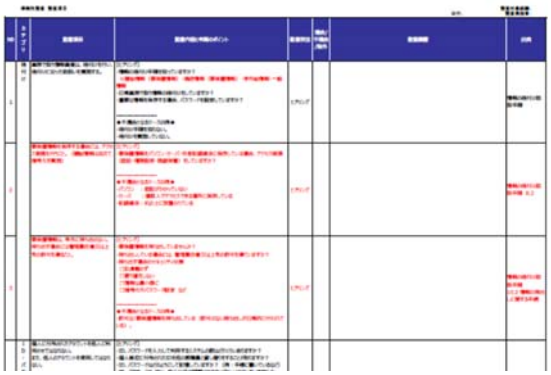
		11月5日（月）	11月6日（火）	11月7日（水）	11月8日（木）	11月9日（金）
10:00	監査対象	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	監査会場					
	集合時刻 集合場所					
	実施者	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	立会者	[redacted]			[redacted]	[redacted]
	備考		[redacted]		[redacted]	
12:00		（昼休み）	（昼休み）	（昼休み）	（昼休み）	（昼休み）

準拠性監査、技術監査、フォローアップ監査の実施

- 準拠性監査に必要な書類を準備と実施

① 準拠性監査項目の作成（xlsx）：項目、監査内容と要点、監査技法、適合の有無、監査調書、学内規則などの出典根拠

② 技術監査対象表の作成（xlsx）：監査の期日・日時、対応者、監査対象機器の完全ドメイン名（FQDN）とIPアドレス、OS、サーバ機能名など



平成30年度 情報セキュリティ監査対象情報 （技術監査）

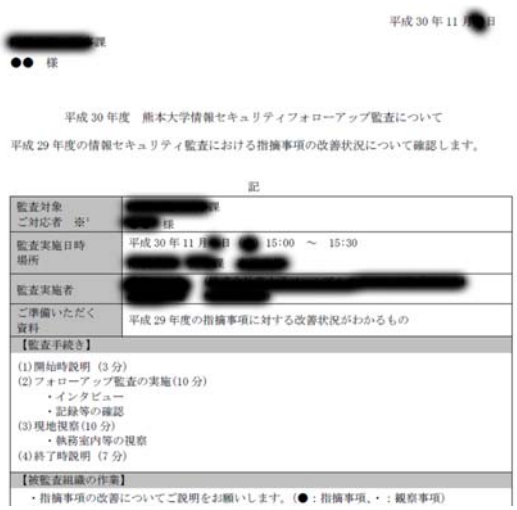
1	部局名等	[redacted]
	受入日時	平成３０年１１月５日（月） １３：３０～
	対応者	所属 [redacted]
		職名 [redacted]
		氏名 [redacted]
		内線番号 [redacted]
		メールアドレス [redacted]
	監査対象機器	機器名称 [redacted]
		セグメント [redacted]
		ＩＰアドレス 133[redacted]
		サブネットマスク 255[redacted]
		ホスト名 [redacted]
		ＯＳ [redacted]
		主要アプリ [redacted]
		その他 [redacted]
2	部局名等	[redacted]
	受入日時	平成３０年１１月５日（月） １３：３０ ～
	対応者	所属 [redacted]
		職名 [redacted]
		氏名 [redacted]
		内線番号 [redacted]

準拠性監査、技術監査、フォローアップ監査の実施

- 準拠性監査に必要な書類を準備と実施

① フォローアップ監査の対象表の作成（docx）:監査会場、監査対象者名、監査人名等

② 監査調書案（docx）:各監査実施後、速やかに監査調書案を作成



平成 30 年 11 月[redacted]日

[redacted]課

●● 様

平成 30 年度　熊本大学情報セキュリティフォローアップ監査について

平成 29 年度の情報セキュリティ監査における指摘事項の改善状況について確認します。

記

監査対象 ご対応者　※1	[redacted] [redacted]様
監査実施日時 場所	平成 30 年 11 月[redacted]日 ●● 15:00 ～ 15:30 [redacted]
監査実施者	[redacted]
ご準備いただく資料	平成 29 年度の指摘事項に対する改善状況がわかるもの

【監査手続き】

(1)開始時説明（3 分）
(2)フォローアップ監査の実施(10 分)
・インタビュー
・記録等の確認
(3)現地視察(10 分)
・執務室内等の視察
(4)終了時説明（7 分）

【被監査組織の作業】

・指摘事項の改善についてご説明をお願いします。（●：指摘事項、・：観察事項）

平成 30 年 11 月 12 日

被監査部門

様

情報セキュリティ監査実施者(総括)

[redacted]

平成30年度 熊本大学 情報セキュリティ監査調書

平成30年度 熊本大学 情報セキュリティ準拠性監査の結果の概要について、下記のとおり報告します。

記

被監査部門	[redacted]
ご対応者	[redacted]
監査実施日時・場所	平成30年11月 12 日(月)13:00～14:40[redacted]
監査実施者	[redacted]
是正報告が必要な指摘事項の有無	☑有　□無
フォローアップ監査の必要性の有無及び方法	□現地監査　☑書面　□なし

【指摘事項(重大な違反／軽微な違反)】

1. 重大な違反：　0 件

2. 軽微な違反：　1 件

[redacted]

利用した。

監査報告書の作成と是正の指示

- 監査報告書の作成（docx）:監査調書案を関係者に同意を得て確定し、総括して監査報告書を作成する

① 監査の方針と目的

② 監査実施期間

③ 監査/評価の基準及び対象範囲

1) 準拠性監査

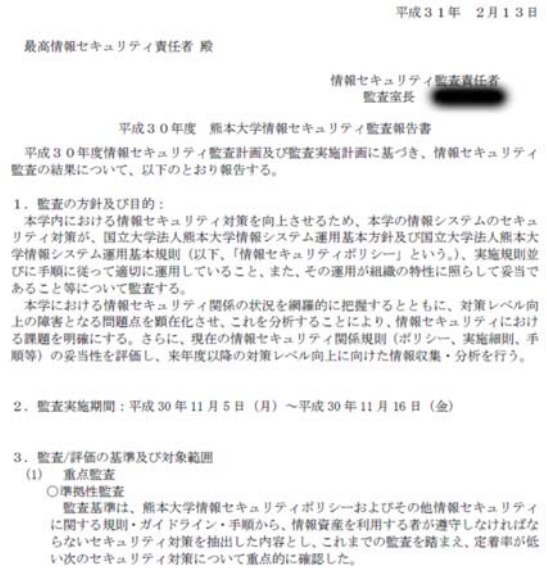
2) 技術監査

3) 妥当性監査

4) フォローアップ監査

④ 監査の実施体制

⑤ 監査結果



平成３１年　２月１３日

最高情報セキュリティ責任者 殿

情報セキュリティ監査責任者
監査室長 [redacted]

平成３０年度　熊本大学情報セキュリティ監査報告書

平成３０年度情報セキュリティ監査計画及び監査実施計画に基づき、情報セキュリティ監査の結果について、以下のとおり報告する。

1．監査の方針及び目的：
本学内における情報セキュリティ対策を向上させるため、本学の情報システムのセキュリティ対策が、国立大学法人熊本大学情報システム運用基本方針及び国立大学法人熊本大学情報システム運用基本規則（以下、「情報セキュリティポリシー」という。）、実施規則並びに手順に従って適切に運用していること、また、その運用が組織の特性に照らして妥当であること等について監査する。
本学における情報セキュリティ関係の状況を網羅的に把握するとともに、対策レベル向上の障害となる問題点を顕在化させ、これを分析することにより、情報セキュリティにおける課題を明確にする。さらに、現在の情報セキュリティ関係規則（ポリシー、実施細則、手順等）の妥当性を評価し、来年度以降の対策レベル向上に向けた情報収集・分析を行う。

2．監査実施期間：平成 30 年 11 月 5 日（月）～平成 30 年 11 月 16 日（金）

3．監査/評価の基準及び対象範囲
(1)　重点監査
○準拠性監査
監査基準は、熊本大学情報セキュリティポリシーおよびその他情報セキュリティに関する規則・ガイドライン・手順から、情報資産を利用する者が遵守しなければならないセキュリティ対策を抽出した内容とし、これまでの監査を踏まえ、定着率が低い次のセキュリティ対策について重点的に確認した。

まとめ

- 本日は以下のことについて説明した

① スライド3:準拠性・技術・フォローアップ・妥当性監（以下監査）の概略

② スライド4-5: この監査が、遵守確認方法の取り組事例であること

③ スライド6-8: 監査は、教育・啓発と同様に外注していること

④ スライド9: 監査の実施期日や教職員へ連絡方法

⑤ スライド10: 内部監査人研修を実施していること

⑥ スライド11-13: 監査の実施に必要な書類と監査調書を作成していること

⑦ スライド14: 監査報告書を作成していること

謝辞

ご清聴ありがとうございます。

- 参加者の皆様、ありがとうございます。
- 講演の機会を一度どころか二度も作っていただいた皆様方、誠にありがとうございます。
- 熊本大学情報統括センター情報セキュリティ室・情報企画課の皆様

講演者履歴職歴

- 1994年熊本大学大学院自然研究科博士課程修了(博士(学術))
- 1994年熊本大学総合情報処理センター助手
- 1997年熊本大学総合情報処理センター講師
- 2002年熊本大学総合情報基盤センター助教授
- 2005年1月-7月ドイツ・フランクフルト大学客員研究員
- 2007年4月熊本大学総合情報基盤センター准教授
- 2014年5月熊本大学総合情報統括センター准教授
- 2015年1月～現在熊本大学総合情報統括センター教授・情報セキュリティ室長