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: 教職員・学生への周知方法

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/

熊本大学の概要について

○位置　熊本県熊本市中央区

○職員数　（H28.6.1現在）

教　　員	９９３人
事務・技術職員	１，６３４人
合　　計	２，６２７人

○学生数　（R1.5.1現在）

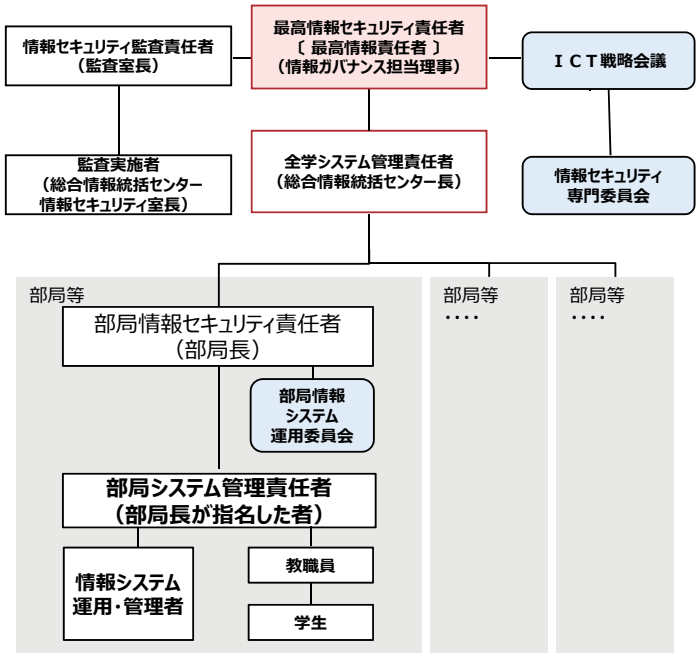
学　　部	７，７５７人
大 学 院	１，９０６人
（博士前期課程	１，２４３人）
（博士後期課程	６６３人）
その他	８２人
合　　計	９，７２７人

創造する森 挑戦する炎

本学の理念・根源的な特質を社会に広く訴えることを目的としたコミュニケーションワード

情報セキュリティ管理体制

■本学では、**トップダウンでのセキュリティを実現**するために、以下の推進体制を構成しています。ICT戦略会議で決定した事項に基づき**役割・権限を持った者が段階的に全学に展開**することになります。



本学全体の方針決定

ICT戦略会議の役割
次の事項に関して決定する
① ポリシー及び全学向け教育の実施のためのガイドラインの改廃
② 情報システムの運用リスク管理に係る規則の制定及び改廃並びにその実施状況の把握　など

情報セキュリティ専門委員会の役割
次の事項に関して審議する
① 情報セキュリティポリシー及び実施手順書に関すること
② その他情報セキュリティに関して必要な事項

運用の実現

部局情報システム運用委員会の役割
次の事項に関して推進する
① 部局等におけるポリシーの遵守状況調査及び周知徹底
② 部局におけるセキュリティ教育　など

情報セキュリティ室と熊大CSIRT

- 情報セキュリティ室構成員7名（2014年5月～）
  - 室長　総合情報統括センター教授
  - 副室長　情報企画課情報セキュリティ担当係長
  - スタッフ（主担当）　総合情報統括センター技術職員
  - スタッフ（副担当）　技術職員1＋事務職員3
- 毎週1回　定例会議を開催
  - 総合情報統括センター長、情報企画課長、副課長も参加
  - 案件の意思決定、活動の報告、情報共有等を実施
- 熊大CSIRT創設準備開始(2015年2月26日-11月30日)

情報セキュリティ室としての活動

- eラーニングによる全教職員・学生向け情報セキュリティ研修
  英語版も用意、2013年から実施、2018年では受講率98.6%
- 部局長には毎月の定例会で、部局の実務担当者・事務部各課の課長及び副課長には年1回の集合研修
- 準拠性監査と技術監査の実施、内部監査人研修の実施
- セキュリティ啓発印刷物の配布
- 標的型メール攻撃訓練
- セキュリティ啓発ビデオの配信
- セキュリティ管理体制の調査
- セキュリティポリシーや手順書・運用規定の見直し
- KU-CSIRTの設置・運用2015年11月～現在

本日の内容1

1. 情報セキュリティeラーニング研修の実施の概略
2. 行動計画およびスケジュールの策定と承認
3. H31/R1年度情報セキュリティ運営費（概算見積）
4. 情報セキュリティ教育支援委託仕様書
5. ポスター（ポスター）の制作・部局長連絡会議での事前連絡
6. 情報セキュリティeラニング研修コンテンツー式納入
7. 情報セキュリティeラーニング研修の実施と受講率の報告
8. 実施後の分析評価
9. まとめ

情報セキュリティeラーニング研修の実施の概略

- ガイドライン・規則およびサイバーセキュリティー般について全学Moodle eラーニングシステムを用いて教職員・学生に受講していただく
- 毎年10月～12月に掛けて実施する
- テキスト・自己点検・アンケートおよび英訳は外注する
- Moodleへの流し込みは情報セキュリティ室実施する
- 実施開始から受講率を調査し、受講率が低い部局・学科や部署については部局長連絡会議で報告する
- 自己点検の正答率からフィードバックを得る

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 主要施策1：次期情報セキュリティ対策計画策定
  - ② 主要施策2：情報セキュリティ教育・啓発活動
  - ③ 主要施策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

- 情報セキュリティ教育・啓発

① 部局情報セキュリティ責任者向け説明（年4回）

② 部局システム管理責任者向け集合研修（年1回8月下旬）

③ 事務系課長・副課長向け集合研修（年1回9月下旬・アンケートによる課題分析）

④ 利用者（教職員）向けeラーニング研修（年1回10月～11月・自己点検・課題分析）

⑤ 利用者（学生）向けeラーニング研修（年1回10月～12月自己点検・課題分析）

⑥ 留学生等を対象とした英語による情報セキュリティ研修会の実施（年2回4月と10月）

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）

行動計画およびスケジュールの策定と承認

- 一般業務

① 情報セキュリティ管理体制整備（毎年4月）

② グローバルIP管理の調査・再調査（通年）

③ プライベートIP化継続（クライアントPC系は、今年度、サーバ系は次年度）

④ 情報の格付け分類表の見直し（監査・教育課題分析の結果やCSIRTの対応事例に基づく）

行動計画およびスケジュールの策定と承認

- 強化施策

① 標的型メール攻撃対策訓練（年1回、今年度は7月に実施、実施後のアンケート実施・集計により訓練者に対する 理解度・認知度を把握、以降の教育・啓発活動へフィードバックする）

② 基本的なセキュリティ対策の実施

③ 情報セキュリティポリシー、関連規則及び手順等の見直し

④ CSIRT訓練（インシデント想定緊急対応訓練）

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

情報セキュリティ教育支援委託仕様書の作成

- 毎年5月末ごろ「セキュリティ行動計画」に基づいて「情報セキュリティ教育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すること
- 下記の事項について発注する

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 サイバーセキュリティ対策基本計画の見直し、作成関する助言

⑤ 啓発ポスター・情報セキュリティハンドブック

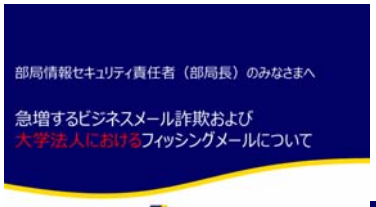
⑥ 本学に情報セキュリティ教育のまとめ

ポスター（ポスター）の制作・部局長連絡会議での事前連絡

- 毎年7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eラーニング研修」の受講促進のため、ポスター・リーフレットおよび部局長連絡会議・部局システム管理者向け・事務系課長・副課長向け集合研修で事前通知を行う。
- ポスターには研修教材の重要ポイントをまとめたものにする

ポスター（ポスター）の制作・部局長連絡会議での事前連絡

- CISO＋CISOから部局長連絡会議（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
- 全学メーリングリストおよびポータルサイトに未受講者への警告メッセージが表示されるように設定する



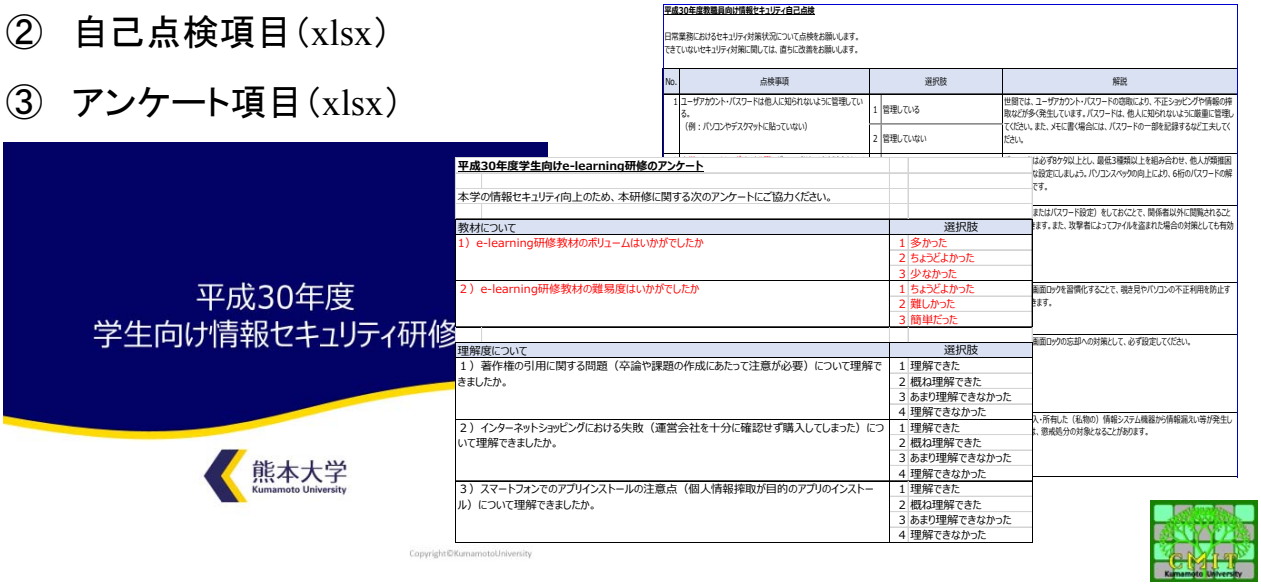
情報セキュリティeラニング研修コンテンツ一式納入

- 毎年8月末ごろ、情報セキュリティ教育支援委託業者より「情報セキュリティeラニング研修コンテンツ一式」が納入される

① 教職員向けセキュリティ研修eラーニング教材（pptx）

② 自己点検項目（xlsx）

③ アンケート項目（xlsx）



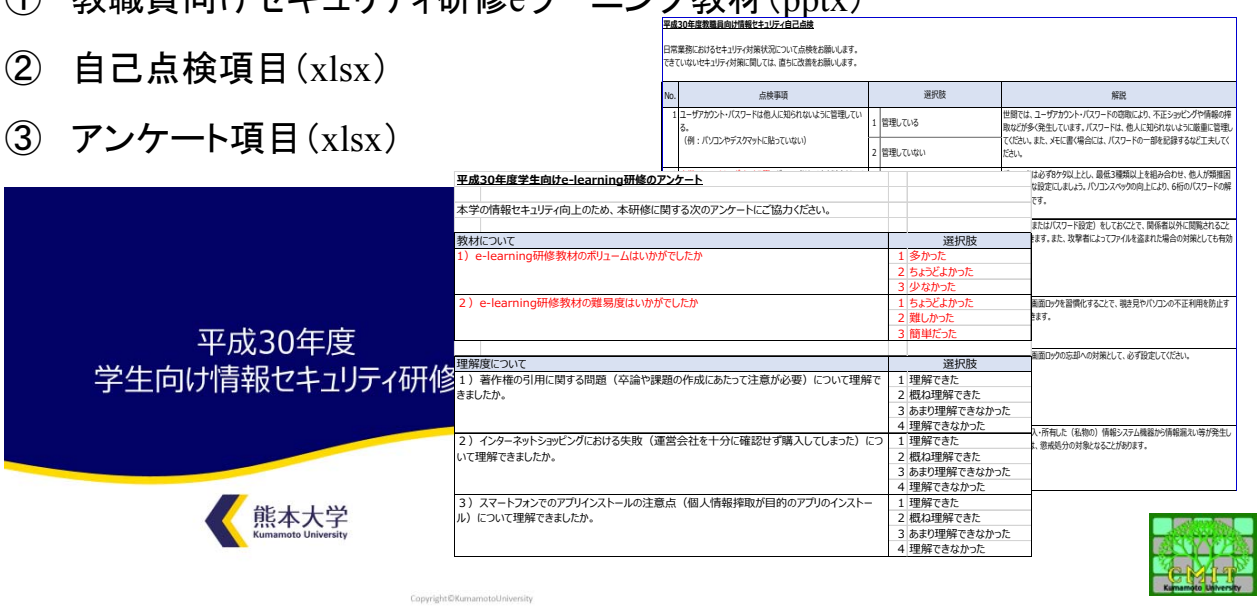
情報セキュリティeラニング研修コンテンツ一式納入・英訳

- 毎年8月末ごろ、情報セキュリティ教育支援委託業者より「情報セキュリティeラニング研修コンテンツ一式」が納入される（英訳は別の業者へ発注）

① 教職員向けセキュリティ研修eラーニング教材（pptx）

② 自己点検項目（xlsx）

③ アンケート項目（xlsx）



情報セキュリティeラーニング研修の実施と受講率の報告

- 情報セキュリティeラーニング教材をMoodleへ流し込む
  - ① 教職員向けセキュリティ研修eラーニング教材（HTML形式）
  - ② 自己点検項目（Moodleアセスメント）
  - ③ アンケート項目（Moodleアンケート）

情報セキュリティeラーニング研修の実施と受講率の報告

- 情報セキュリティeラーニング研修を実施（10月～11月上旬）
  - ① 受講率を調査（翌年1月まで）
  - ② 受講率は部局長連絡会議などで報告する（毎週調査し、各部局へ通達）
  - ③ Moodleの研修コンテンツはずっと公開している

情報セキュリティ研修（教職員用eラーニング研修）受講率一覧

10月15日 9:00現在

部局名等	受講者数	受講可能者	受講率
[redacted]	4	9	44.4%
[redacted]	4	4	100.0%
[redacted]	1	1	100.0%
[redacted]	15	21	71.4%
[redacted]	24	49	49.0%
[redacted]		1	0.0%
[redacted]	9	19	47.4%
[redacted]	7	19	36.8%
[redacted]	0	1	0.0%
[redacted]	16	21	76.2%
[redacted]	3	5	60.0%
合計	1,375	4,240	32.4%

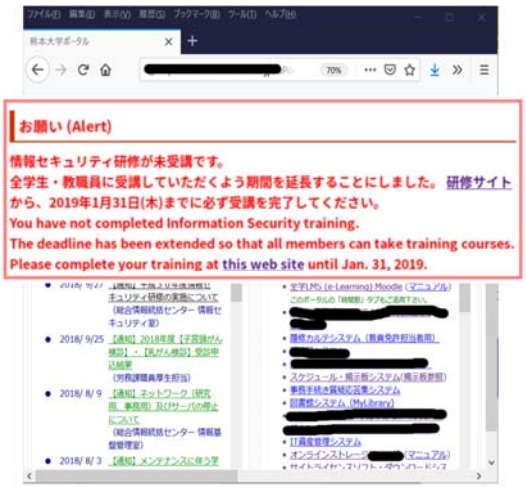
情報セキュリティ研修（教職員用eラーニング研修）受講率一覧

11月19日 8:30現在

部局名等	受講者数	受講可能者	受講率
[redacted]	9	9	100.0%
[redacted]	4	4	100.0%
[redacted]	1	1	100.0%
[redacted]	21	21	100.0%
[redacted]	45	45	100.0%
[redacted]	1	1	100.0%
[redacted]	19	19	100.0%
[redacted]	18	18	100.0%
[redacted]	1	1	100.0%
[redacted]	2	4	50.0%
[redacted]	1	2	50.0%
合計	3,607	4,054	89.0%

情報セキュリティeラーニング研修の実施と受講率の報告

- 受講率を部局長（部局情報セキュリティ責任者）へ報告
  - ① 受講率の報告とともに未受講者リストの通達も実施
  - ② ポータルサイトを全学Moodle学習支援システム（LMS）と連携させ、未受講の旨をログイン時に教職員へ連絡



実施後の分析評価

- 情報セキュリティeラーニング研修の理解度を計算
  - ① 全受講者数3957人、91の部局等（部局、学科、部署など）
  - ② 自己点検の各質問事項について、正答者の人数を数え、それを各部局等ごとに頻度分布を作成し、正答率の低い箇所について、次回の行動計画、実施手順書・学内規則の改定時に考慮する

【点検事項1】ユーザアカウント・パスワードは他人に知られないように管理している。（例：パソコンやデスクマットに貼っていない）		【点検事項2】大学のシステムにログインする際のパスワードは、8ケタ以上とし、3種類以上の文字種を混在して設定している。※文字種とは、英大文字・英小文字・数字・記号となります。		【点検事項3】入試関連情報や学生成績関連情報（極秘情報）を含むデータは、ファイルを暗号化している（またはパスワード設定している）。		【点検事項4】離席時には、パソコンの画面ロックをしている。		【点検事項5】パソコンには、パスワード付きスクリーンセーバーを設定している（推奨：5分以内）。		【点検事項6】個人が購入・所有した（私物の）情報システム機器には、職務（業務）情報を保存していない。※情報システム機器とは、パソコン・タブレット・スマートフォン・USBメモリ・デジタルカメラ（SDカードを含む）・ICレコーダーなどがあります。	
Q1正解数	（正解率）意識度	Q2正解数	（正解率）意識度	Q3正解数	（正解率）意識度	Q4正解数	（正解率）意識度	Q5正解数	（正解率）意識度	Q6正解数	（正解率）意識度
9	100%	9	100%	9	100%	7	78%	9	100%	9	100%
4	100%	4	100%	3	75%	4	100%	4	100%	4	100%
1	100%	1	100%	1	100%	1	100%	1	100%		0%
21	100%	21	100%	18	86%	19	90%	19	90%	20	95%
45	100%	45	100%	44	98%	39	87%	41	91%	45	100%
1	100%	1	100%	1	100%	1	100%	1	100%	1	100%
19	100%	19	100%	19	100%	16	84%	16	84%	19	100%
18	100%	18	100%	18	100%	17	94%	17	94%	18	100%
1	100%	1	100%	1	100%	1	100%	1	100%	1	100%
26	100%	26	100%	25	96%	25	96%	25	96%	26	100%

まとめ

- 本日は以下のことについて説明した

① スライド2-5: 本日の前提条件

② スライド7: 情セキュリティeラーニング研修（以下単に研修）実施の概略

③ スライド8-12: この研修が、情報セキュリティ教育・啓発の一環であること

④ スライド13-14: 研修の教材コンテンツは、他の教育・啓発と同様に外注していること

⑤ スライド15-16: 研修の実施期日や教職員へ連絡方法

⑥ スライド17-19: 研修コンテンツを全学Moodleシステムに導入およびテキスト、自己点検、アンケートが構成されること

⑦ スライド20-22: 研修の受講率を用いた受講促進活動にかんすること

⑧ スライド23: 実施後の正答率による分析評価を行っていること

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