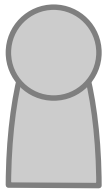
クラウドセキュリティの始め方

ISMS/ISMSクラウドセキュリティ受審報告

大学等におけるクラウドサービス利用シンポジウム2019

本日お話させていただくこじつけ

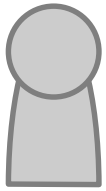


広島大学のISMSが生まれ変わりました。

ISMSはISMSクラウドセキュリティの前提です。

クラウドセキュリティを考えてみましょう。

本日お話させていただくこじつけ

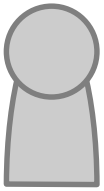


広島大学のISMSが生まれ変わりました。

ISMSはISMSクラウドセキュリティの前提です。

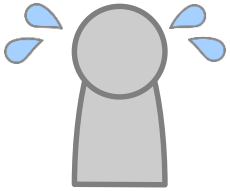
クラウドセキュリティを考えてみましょう。

本日お話させていただくこじつけ



広島大学のISMSが生まれ変わりました。

ISMSはISMSクラウドセキュリティの前提です。



クラウドセキュリティを考えてみましょう。

ISMSとは 🔰

個人情報をきちんと守っていることを内外にアピールするもの

ISMSクラウドセキュリティとは 🔰

十分なセキュリティで、クラウドサービスを利用／提供していることを内外にアピールするもの

ISMS/ISMS-CLS認証取得の表示

バックナンバー

センターからのお知らせ（学内限定）

2019年02月12日　home/hostingサーバにおけるCMS管理徹底のお願い

2019年01月24日　（至急）ホームページ検索結果の確認依頼

2018年11月26日　HINET ゾーンA ゾーンB ホストにおけるセキュリティ強化（TLS1.2以外のプロトコル無効化）のお願い

2018年06月20日　【注意喚起】Twitter等で設定しているパスワード(使いまわし)について/[Warning] Do not use Hiroshima University's passwords on Twitter and other services

2018年06月08日　メディアセンターサービスの「TLS1.0」および「TLS1.1」の無効化について/ Invalidation of "TLSv1.0" and "TLSv1.1" on IMC services

2018年03月30日　【注意喚起】マルウェアや不正アプリケーションにご注意ください

広島大学 クラウドサービス 利用ガイドライン

情報セキュリティ・コンプライアンス教育

セキュリティ情報

IMCサービス稼働情報

ICE端末利用状況

ISMS認証取得

JIS Q 27001:2014
(ISO/IEC 27001:2013)

認証登録番号：IC14J0392

JIP-ISMS517-1.0

認証登録番号：SC16J0003

言語を選択

目的からサービスを探す (Find Services)

コンピュータの利用	電子メールの利用	ネットワークへの接続	教育支援サービスの利用	ソフトウェアの利用
教育用情報端末 ICE	メールサービス POP/IMAP Mail	キャンパスネットワーク HINET	オンライン学習支援システム Bb9	マイクロソフト包括ライセンス Microsoft License
ホームページ作成 HomePage	ウェブメール Web Mail	情報コンセント（無線／有線） HINET WiFi/Guest	出欠管理システム Attendance Management	ウィルス対策ソフトウェア Anti-Virus Software
ホスティングサービス Hosting		VPN 接続サービス VPN	VNC サービス VNC	アプリケーションサービス Application Service
HPC グリッド HPC Grid		フレッツ接続サービス Flets	VODサービス VOD	キャンパスライセンス Campus Lisence

ISMS認証取得までの流れ 🔰

広島大学

○○しなければならない。○○することが望ましい。

国際規格

ISO27001

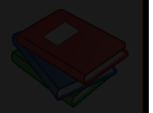
ISO27017

ISMS文書

ISMSマニュアル

ISMS基本方針

…



証跡

ログ、記録

ISMS認証取得までの流れ 🔰

広島大学

○○に対して、私たちはこうやって実施します。

国際規格

ISO27001

ISO27017

ISMS文書

ISMSマニュアル

ISMS基本方針

…

証跡

ログ、記録

ISMS認証取得までの流れ 🔰

広島大学

その証拠が△△です。認証機関さん、見てください。

国際規格	ISMS文書	証跡
ISO27001	ISMSマニュアル	ログ、記録
ISO27017	ISMS基本方針	
	… 	

よくある失敗例

セキュリティを高めるためにISMSをやっているのに、**ISMSの活動が重すぎて、本来やるべきセキュリティを守る活動ができない**

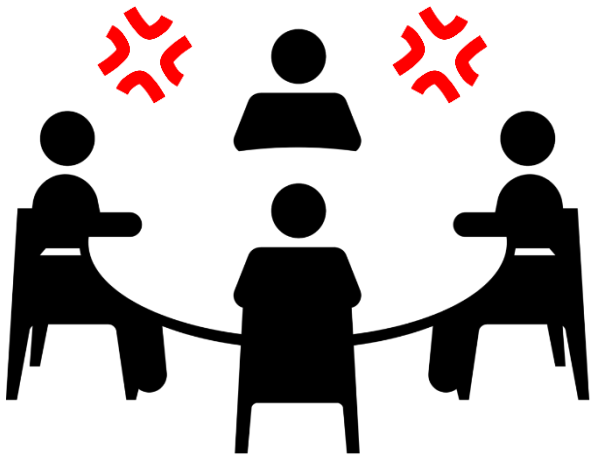
（2017年度内部監査）当時の会話

証跡がない

毎年同じ

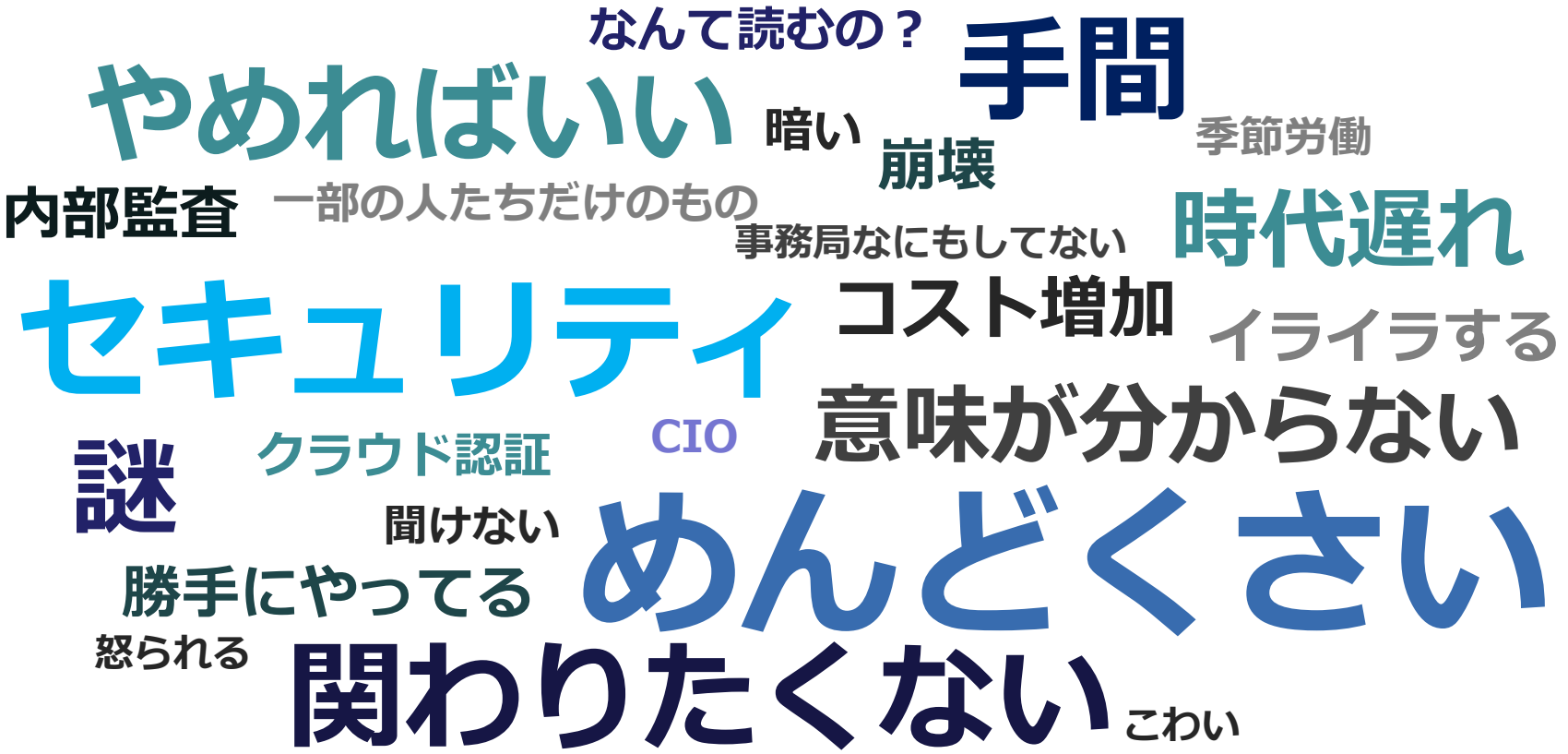
理解不足

実績が空欄



ダメ過ぎる

ISMSを取り巻く当時の状況



原因

業務の根拠＝**規則**＝**ISMS文書**

- ISMSマニュアル
- ISMS基本方針
- ISMS適用宣言書
- ISMS管理策手順書 など

ISMS文書に何が書いてあるか分からない
根拠が揺らいでいる！

ISMS文書の見直し

改善内容の一例

- ISMSマニュアル
- ISMS適用宣言書 ／ ISMS管理策手順書
- リスクアセスメント手法

ISMSマニュアル（Before）

広島大学

▪5.2 方針　⇒　関連文書:『ISMS 基本方針』

CIO/CIO 補佐は，次の事項を満たす情報セキュリティ方針を確立しなければならない。

a) 組織の目的に対して適切である。

b) 情報セキュリティ目的(6.2 参照)を含むか,又は情報セキュリティ目的の設定のための枠組みを示す。

c) 情報セキュリティに関連する適用される要求事項を満たすことへのコミットメントを含む。

d) ISMS の継続的改善へのコミットメントを含む。

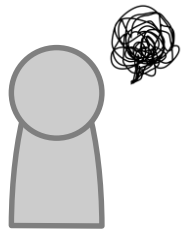
情報セキュリティ方針は，次に示す事項を満たさなければならない。

e) 文書化した情報として利用可能である。

f) 組織内に伝達する。

g) 必要に応じて，利害関係者が入手可能である。

- 規格の文言がほぼそのまま書かれただけ
- 言葉が難しく、到底理解できない



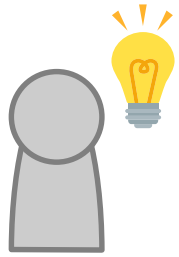
ISMSマニュアル（After）

広島大学

規格	要求事項の解釈	関連文書
5.2 方針	CIOは，次の事項を満たす情報セキュリティ方針を確立する。 a) センターサービスの可用性を確保すること。 b) 安定かつ信頼できるセンターサービスを提供すること（目的）。 c) 法令等を順守し，CIOがその責任を負うこと。 d) PDCAサイクルにより，関係者は協力してISMSを推進すること。 上記の事項は，「ISMS基本方針」として作成し，文書化した情報として利用可能とする。また，「ISMS基本方針」はホームページ等で利害関係者に広く周知する。	OneDrive > ISMS > 1_承認済み原本 > ISMS基本方針 センターホームページ > ISMS https://www.media.hiroshima-u.ac.jp/news/isms/

- 本学の解釈を追加
- 関連文書の保存場所を記載

ISMSのために何をするのかが明確になった



ISMS管理策手順書（Before）

広島大学

A.12.1.3 容量・能力の管理

管理策

要求されたシステム性能を満たすことを確実にするために，資源の利用を監視・調整しなければならず，また，将来必要とする容量・能力を予測しなければならない。

実施手順

- 全学統一 ID 管理システムについては，以下の機能で監視する。
  - Unidb，uniap の死活監視
  - 夜間バッチ，手動バッチのログのメール通知
- 全学統一 ID 管理システムの手動監視を行う場合は，「A.12.1.1 操作手順書」に定める場所に置かれた次のマニュアルを参照し，操作を行う。
  - 「共有フォルダ」→「j_情報化推進グ」→「080 情報化」→「010 システム」→「050 電子認証」→「01 ルール」→「02 マニュアル」→「02 システムマニュアル」→「01 全学統一 ID 管理システム」→「201408」→「全ドキュメント」→「全学統一 ID 管理システム AP」→「03 マニュアル」→「運用管理編」
- 以下の URL の監視システムで監視する。

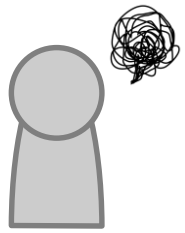
Nagios（https://mon-iij.media.hiroshima-u.ac.jp/nagi）

Federated Cloud Monitoring Service

（https://fcmsa.cs1.hitachi-cloud.com/DIRWebApplication/FedLogin.aspx）

- 利用登録システムの手動監視を行う場合は，「A.12.1.1 操作手順書」に記述した，以下のマニュアルの項目を参照し，操作を行う。
  - 「02_利用者サービス管理システム」→「02_運用管理編（スーパー管理者）」

- 何のために誰が何をすればいいのかわからない
- 項目によって文章量がバラバラ
- IMC、情報部のいずれかしか該当しないことも書かれている
- 証跡場所が書かれていたりいなかったりする
- リンクだらけ
- 多すぎて読む気にならない



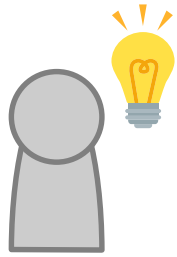
ISMS管理策手順書（After）

広島大学

規格	目的	適用/除外	管理策又は除外理由	資料等
ISO/IEC 27001:2013附属書A				
A.5 情報セキュリティのための方針群				
A.5.1 情報セキュリティのための経営陣の方向性				
A.5.1.1 情報セキュリティのための方針群	情報セキュリティの基本方針を管理層が承認し，ISMSスタッフ及び関連する外部関係者に周知するため。	○	「ISMS基本方針」において，情報セキュリティの基本方針を示し，CIOが承認・署名したものを掲示する。	・ISMS基本方針.docx OneDrive≫ISMS≫1_承認済み原本 ・IMCホームページ https://www.media.hiroshima-u.ac.jp/news/isms/
A.5.1.2 情報セキュリティのための方針群のレビュー	周辺状況の変化に伴い，管理層の情報セキュリティに対する方針を見直し，確実に反映させるため。	○	CIOが基本方針を確認するマネジメントレビューを年に1回以上実施し，その結果をISMSスタッフに周知する。	・マネジメントレビュー資料，議事要録等 OneDrive≫ISMS≫2_会議・教育等資料≫マネジメントレビュー ・ISMSスタッフへの周知メール OneDrive≫ISMS≫4_業務運用上の記録
A.6 情報セキュリティのための組織				
A.6.1 内部組織				
A.6.1.1 情報セキュリティの役割及び責任	ISMSスタッフの役割を明確にするため。	○	「ISMS推進体制と力量」において，情報セキュリティの役割と責任を定める。	・ISMS推進体制と力量.docx OneDrive≫ISMS≫1_承認済み原本
A.6.1.2 職務の分離	ISMSスタッフの役割を明確にし，個人の単独行動により情報セキュリティ事故を起こさないようにするため。	○	ISMS業務とその分担をリスト化して，相反する職務については分離する。	

- 列ごとに、目的、管理策、証跡場所を記載
- 全体の文章量を統一

62ページあった手順書が11ページになった



ISMS管理策手順書（After）

広島大学

全学共通編（ISMS適用宣言書）

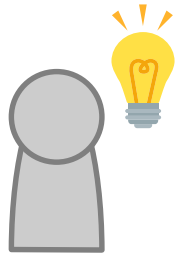
規格	管理策又は除外理由	資料等
A.5.1.1 情報セキュリティのための方針群	「ISMS基本方針」において，情報セキュリティの基本方針を示し，CIOが承認・署名したものを掲示する。	・ISMS基本方針.docx OneDrive≫ISMS≫1_承認済み原本 ・IMCホームページ https://www.media.hiroshima-u.ac.jp/news/isms/
A.5.1.2 情報セキュリティのための方針群のレビュー	CIOが基本方針を確認するマネジメントレビューを年に1回以上実施し，その結果をISMSスタッフに周知する。	・マネジメントレビュー資料，議事要録等 OneDrive≫ISMS≫2_会議・教育等資料≫マネジメントレビュー ・ISMSスタッフへの周知メール OneDrive≫ISMS≫4_業務運用上の記録

部局編（ISMS運用手順書）

運用手順	資料等
管理策A.5.1.1の記載事項を遵守する。 なお，「ISMS基本方針」の掲載場所は以下のとおりとする。 (1)電子媒体－IMCホームページ (2)紙媒体－IMC本館，西分室，北分室，霞分室	・IMCホームページ https://www.media.hiroshima-u.ac.jp/news/isms/ ・事務室掲示場所
管理策A.5.1.2の記載事項を遵守する。	

- IMC、情報部の共通部分は全学共通編として、
  独自部分は部局編として別の文書に

他部署にも展開できる文書構成となった



ISMS管理策手順書（After）

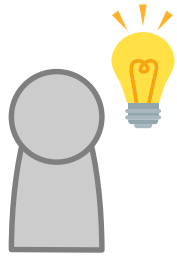
広島大学

規格	目的	管理策又は除外理由	資料等
A.7.2.3 懲戒手続	重大または悪意のある情報セキュリティ違反への対応の明確化と抑止力を備えるため。	「広島大学職員懲戒規則」に従う。	・【規】広島大学職員懲戒規則
A.7.3 雇用の終了及び変更			
A.7.3.1 雇用の終了又は変更に関する責任	雇用の終了又は変更に伴う責任の変化を明確化し，情報セキュリティ事故を防止するため。	「広島大学職員就業規則」に従う。	・【規】広島大学職員就業規則
A.8 資産の管理			
A.8.1 資産に対する責任			
A.8.1.1 資産目録	情報資産を認識・識別し，それぞれの重要度を明確にするため。	・「広島大学法人文書管理規則」に従う。 ・情報資産を特定した目録を作成し，毎月末に棚卸しを実施する。	・【規】広島大学法人文書管理規則

- 管理策手順と本学の規則との対応関係を整理

（**紫字**＝本学の規則に従う項目）

ISMSとして実施することが何か明確になった



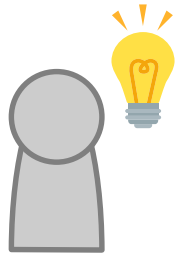
ISMS管理策手順書（After）

広島大学

規格	運用手順	資料等	（参考）ISMSスタッフ実施事項 ※定期実施確認表記載事項
A.6.2 モバイル機器			
A.6.2.1 モバイル機器の方針	管理策A.6.2.1及び以下の記載事項を遵守する。 ・業務用に支給された端末（以下「業務用パソコン」という。）以外の端末による業務は原則禁止とする。 ・業務用パソコン以外の端末で業務を行う必要がある場合は，「モバイル機器利用承認記録」により，事前に情報セキュリティ管理者の許可を得る。	・モバイル機器利用承認記録 OneDrive≫ISMS≫4_業務運用上の記録≫IMC	【A】『広島大学情報セキュリティポリシー実施手順「全学共通編」』の順守 【Y】「モバイル機器利用承認記録」の更新
A.6.2.2 テレワーキング	管理策A.6.2.2及び以下の記載事項を遵守する。 ・遠隔からの業務は原則禁止する。 ・遠隔から業務を行う必要がある場合は，「テレワーキング承認記録」により，事前に情報セキュリティ管理者の許可を得る。	・テレワーキング承認記録 OneDrive≫ISMS≫4_業務運用上の記録≫IMC	【Y】「テレワーキング承認記録」の更新 【E】業務用パソコンからのVPN接続

- ISMSスタッフが、どんなタイミングで、何をしなければならないのか、列を追加

これを見れば分かる、文書がようやくできた



ISMS管理策手順書（After）

広島大学

全学共通編（ISMS適用宣言書）

部局編（ISMS運用手順書）

- 定期的に確認する項目は確認表に実績を記載

規格	運用手順	資料等	（参考）ISMSスタッフ実施事項 ※定期実施確認表記載事項
A.6.2 モバイル機器			
A.6.2.1 モバイル機器の方針	管理策A.6.2.1及び以下の記載事項を遵守する。 ・業務用に支給された端末（以下「業務用パソコン」という。）以外の端末による業務は原則禁止とする。 ・業務用パソコン以外の端末で業務を行う必要がある場合は，「モバイル機器利用承認記録」により，事前に情報セキュリティ管理者の許可を得る。	・モバイル機器利用承認記録 OneDrive≫ISMS≫4_業務運用上の記録≫IMC	【A】『広島大学情報セキュリティポリシー実施手順「全学共通編」』の順守 【Y】「モバイル機器利用承認記録」の更新
A.6.2.2 テレワーキング	管理策A.6.2.2及び以下の記載事項を遵守する。 ・遠隔からの業務は原則禁止する。 ・遠隔から業務を行う必要がある場合は，「テレワーキング承認記録」により，事前に情報セキュリティ管理者の許可を得る。	・テレワーキング承認記録 OneDrive≫ISMS≫4_業務運用上の記録≫IMC	【Y】「テレワーキング承認記録」の更新 【E】業務用パソコンからのVPN接続

定期実施確認表

【2018年度】ISMS定期実施確認表　※行の追加や内容の変更等を行う（運用手順書…場合はISMS事

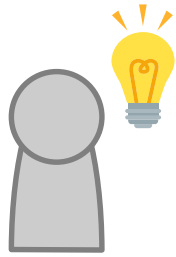
このISMS定期実施確認表は，毎月ISMS事務局会で進捗を確認する。…当初から実施しない…

各月のセルには，実施，異動，異常等の有無にかかわらず，確認日を記載する（頻度が毎日のものを除く）。確認時に異常がない場合はセルを白色

また，「確認日＋α（内容）」など，記載方法は運用に応じて分かりやすいものにする。

規格		内容	部門	実施者	実施計画	4月	5月
A.09.2.3	特権的アクセス権の管理	管理者権限一覧の更新	情報G	松尾	毎月	4/1	5/23
A.09.2.6	アクセス権の削除又は修正	「職員の採用・異動に伴う手続書」によるアクセス権の削除又は修正	情報G	松尾/落合	毎月	4/2	5/23
A.09.2.2	利用者アクセスの管理	ID管理システム利用申請書の管理	情報G	松尾/落合	毎月	4/2,3,4,9,10,11,12,16,17,25	5/2,7,23
A.09.2.5	利用者アクセス権のレビュー	ID管理システムの利用者更新	情報G	松尾/落合	毎月	4/2,3,4,9,10,11,12,16,17,25	5/2,7,23
A.09.2.6	アクセス権の削除又は修正	登録済利用者の退職等によるアクセス権の削除	情報G	松尾/落合	毎月	4/1	5/2
A.09.4.4	[illegible]	ID管理システムの特権利用ログ確認	情報G	松尾	毎月	4/1	5/2
A.09.4.5	[illegible]	プログラムソースコードへのアクセス制御	情報G	松尾	毎月	4/1	5/2
A.11.1.5	[illegible]	「仁保データセンター入室申請書」の管理	IMC/情報G	権田	毎月	4/27：1件	5/31：0件
A.11.2.4	装置の保守	HUC12懸案管理表で保守状況の確認	IMC	中川	毎月	4/18	5/24
A.12.1.4	[illegible]	HUC12メンテナンス作業概要の確認	IMC	中川	毎月	4/18	5/24
A.12.2.1	マルウェアに対する管理策	HUC12メンテナンス作業概要の確認	IMC	中川	毎月	4/18	5/24

文書の構造が確立した



リスクアセスメント手法（Before）

広島大学

IMC-ISMSリスクアセスメント結果

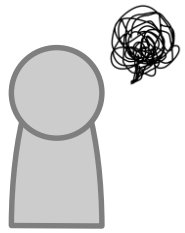
開催日 2015/2/6(金)
日時 15:00-17:00
場所 センター本館会議室

区分	きっかけとなる出来事	対象となる資産・権利等	発生する困り事（＊は様々な事態を示す）	原因となる者：学外	学内	センタ	業者	ユーザ	資産価値：機密性C	完全性I	可用性A	脅威の頻度	脆弱性	リスクI：機密性	完全性	可用性	リスクII：機密性	完全性	可用性	リスクオーナー	審議結果	対応
									2	2	2		3	32	32	24						
障害	漏水:エアコンの空調	サーバ室	サーバ破損						0	0	4	2	4	0	0	32	−	−	○	CIO		
障害	UPS異常	サーバ室	サービス停止						0	0	3	1	2	0	0	6	−	−	−	CIO		
障害	空調機器故障	サーバ室	サービス停止						0	0	3	2	2	0	0	12	−	−	−	CIO		
障害	ハード異常	サーバ室	サービス停止						0	0	3	2	2	0	0	12	−	−	−	CIO		
障害	上流の誤操作	在籍者の権利	ID消失で離籍予定メール		○				0	4	0	2	4	0	32	0	−	○	−	CIO		
管理	管理用アカウントのPWが脆弱	パスワード	クラックされる			○			4	4	4	1	2	8	8	8	−	−	−	CIO		
悪意	窓を破壊して侵入	本館事務室	＊	○					0	0	4	1	4	0	0	16	−	−	○	CIO		
悪意	事務室:不正侵入(ドア、窓)	業務データ	PC盗難	○					2	0	0	1	3	6	0	0	○	−	−	CIO		
障害	上流の誤操作でID消失	個人情報	PW強制変更業務停止		○				0	0	4	1	4	0	0	16	−	−	○	CIO		
悪意	出入り業者が個人情報販売	個人情報	個人情報漏洩				○		4	0	0	1	4	16	0	0	○	−	−	CIO		
事故	離籍した職員IDの他人への流用	個人情報保護	想定外のアカウント譲渡		○				2	0	0	1	4	8	0	0	○	−	−	CIO		
事故:台風等	飛来物で窓が破損して、浸水など	2階サーバ室	サーバ破損	○					0	0	4	1	4	0	0	16	−	−	○	CIO		
事故:台風等	飛来物で窓が破損して、浸水など	1階サーバ室	サーバ破損	○					0	0	4	1	4	0	0	16	−	−	○	CIO		
悪意	テロ:サーバ室:破壊的侵入	2階サーバ室	＊		○				0	0	4	1	4	0	0	16	−	−	○	CIO		
悪意	テロ:サーバ室:破壊的侵入	1階サーバ室	＊		○				0	0	4	1	4	0	0	16	−	−	○	CIO		
障害	鍵が故障してドア解放状態になる	サーバ室	＊						4	0	4	1	3	12	0	12	○	−	○	CIO		
障害	地震	サーバ室	サーバ倒壊						0	0	4	1	4	0	0	16	−	−	○	CIO		
障害	事務室の鍵故障:ドア開放	事務室	＊						3	0	3	1	3	9	0	9	○	−	○	CIO		
管理	作業ミス	ネットワーク	誤設定による回線断				○		0	0	4	1	4	0	0	16	−	−	○	CIO		
管理	作業ミス	ネットワーク	施設工事に伴う断線				○		0	0	4	1	4	0	0	16	−	−	○	CIO		
悪意	職員が他人のPWを勝手に変更	パスワード	アカウント(or広大ID)乗っ取り		○				2	1	2	1	4	8	4	8	○	−	○	CIO		
管理	重要書類が鍵のかからない棚にある	個人情報	盗難で個人情報漏洩						2	0	0	1	3	6	0	0	○	−	−	CIO		
管理	教員用PCの盗難	個人情報	個人情報漏洩			○			4	0	0	1	3	12	0	0	○	−	−	教員		
不注意	ユーザPCの盗難	個人情報	個人情報漏洩					○	1	0	0	3	4	12	0	0	−	−	−	ユーザ		
不注意	ユーザのパスワードが脆弱	パスワード	パスワードクラックされた					○	1	0	0	2	4	8	0	0	−	−	−	ユーザ		
不注意	ユーザがパスワードを漏洩	パスワード	SPAM発信					○	1	0	2	4	4	16	0	32	−	−	○	ユーザ		

- リスク値の計算が複雑
- 繰り返し実施できない

機密性（C）に関する受容リスク値：32 未満

資産価値	脅威 1 脆弱性 1	1 2	1 3	1 4	2 1	2 2	2 3	2 4	3 1	3 2	3 3	3 4	4 1	4 2	4 3	4 4
1	1	2	3	4	2	4	6	8	3	6	9	12	4	8	12	16
2	2	4	6	8	4	8	12	16	6	12	18	24	8	16	24	32
3	3	6	9	12	6	12	18	24	9	18	27	36	12	24	36	48
4	4	8	12	16	8	16	24	32	12	24	36	48	16	32	48	64



リスクアセスメント手法（After）

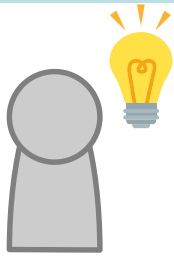
広島大学

リスクアセスメントシート（情報G）

主要な既存対策
■物理的損傷（K01,02）
■自然現象（K03）
■重要なサービスの喪失（K04,05
■放射による妨害（K06）
■情報を危うくすること（K07,K08）
■技術的な故障（K09,K10）
■認可されていない行為（K11,12）
■機能を危うくすること（K13,14）

項番	脅威の内容	脅威の要因 外部(1)	脅威の要因 内部(2)	起こり得る結果	機密性 C	完全性 I	可用性 A	対象となる情報資産	脅威により情報資産が脅かされる具体例	被害の影響度（資産の重要度） 小(1)	中(2)	大(3)	重大(4)	リスク値	対策の必要値	対策の評価結果（評価値：評価理由） 事前 抑止の確実度	事後 検知の確実度	事後 回復の確実度	リスク評価結果
1	K01~Y01 火災、水害、汚染による業務停止	●		1			A	ID管理サーバ、LDAPサーバ	サーバが火災に巻き込まれ、システムが停止し、利用者がアクセスできない			●		3	3	(3,3,3)	4 (1) サーバはクラウドサービスを利用しており、脅威の発生可能性は低い	4 (5)X21) データセンターは24時間365日監視されている	4 (20) 保守契約により、平日であれば通報後2時間以内に対処を開始する	受容
2	K02~Y01 火災、水害、汚染、機器の[illegible]塵、粉塵、腐食、凍結による業務停止		●	2			A	ID管理サーバ、LDAPサーバ	サーバが故意に破壊され、システムが停止し、利用者がアクセスできない			●		3	6	(4,3,3)	4 (1) サーバはクラウドサービスを利用しており、脅威の発生可能性は低い	4 (5)X21) データセンターは24時間365日監視されている	4 (20) 保守契約により、平日であれば通報後2時間以内に対処を開始する	受容
3	K03~Y02 高温、暴風、地震、洪水、土砂崩れによる業務停止	●		1			A	ID管理サーバ、LDAPサーバ	サーバが設置されている建物が倒壊して、システムが停止し、利用者がアクセスできない			●		3	3	(3,3,3)	4 (1) サーバはクラウドサービスを利用しており、脅威の発生可能性は低い	4 (5)X21) データセンターは24時間365日監視されている	4 (20) 保守契約により、平日であれば通報後2時間以内に対処を開始する	受容
4	K04~Y03 空調・水道システムの故障、電力供給の停止、電気通信機器の故障による業務停止	●		1			A	ID管理サーバ、LDAPサーバ	サーバが設置されている部屋の電力供給が止まり、システムが停止し、利用者がアクセスできない			●		3	3	(3,3,3)				
5	K05~Y03 電気通信機器の故障による業務停止		●	2			A	ID管理サーバ、LDAPサーバ	サーバのメンテナンス不足により故障してシステムが停止し、利用者がアクセスできない			●		3	6	(4,3,3)				
6	K06~Y04 電磁波放射、熱放射、電磁パルスによるデータ破壊又はシステム破壊	●		1		I		学生・職員・学外者情報、ID管理サーバ、LDAPサーバ、PW、各種CSV、ログファイル	サーバが電磁波放射の影響を受け、データが破壊される			●		3	3	(3,3,3)				
7	K06~Y04 電磁波放射、熱放射、電磁パルスによるデータ破壊又はシステム破壊	●		1			A	ID管理サーバ、LDAPサーバ	サーバが電磁波放射の影響を受け、システムが破壊され、利用者がアクセスできない			●		3	3	(3,3,3)				
8	K07~Y05 盗聴、機器や文書の盗難、廃棄媒体からの復元、マルウェア感染による情報漏えい	●		1	C			学生・職員・学外者情報、ID管理サーバ、LDAPサーバ、PW、各種CSV、ログファイル、利用申請書、マニュアル、その他紙媒体	サーバの廃棄時に情報が盗み出される／保管文書が盗難され個人情報が漏えいする			●		3	3	(3,3,3)				
	K07~Y06																		

- リスク値の計算を簡素化（脅威の要因×影響度＝最大8）
- 現対策を「抑止」「検知」「回復」の３つに分類し、それぞれ４段階で評価



具体的に文章化し、判断基準を明確にした

文書見直しの結果

業務の根拠＝**規則**＝**ISMS文書**

- ISMSマニュアル
- ISMS基本方針
- ISMS適用宣言書
- ISMS管理策手順書 など

ISMS文書が整備された

根拠が明確になった

文書見直しの結果

Before

道がガタガタすぎて、とても安心して話し合いできる状況じゃなかった

After

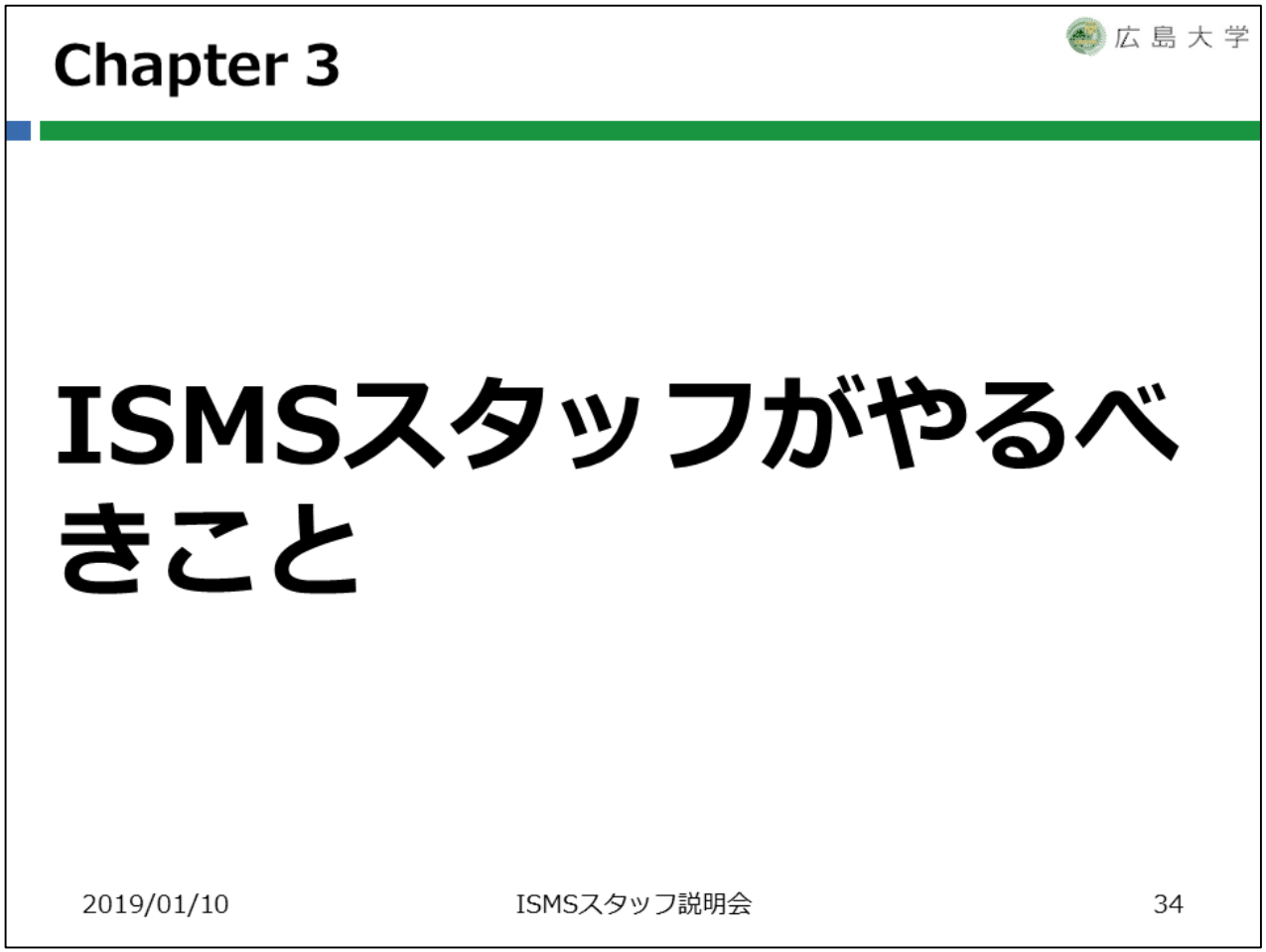
道が平らになったことで、お互いのことを考えられるようになった

ISMSを取り巻く今後の状況

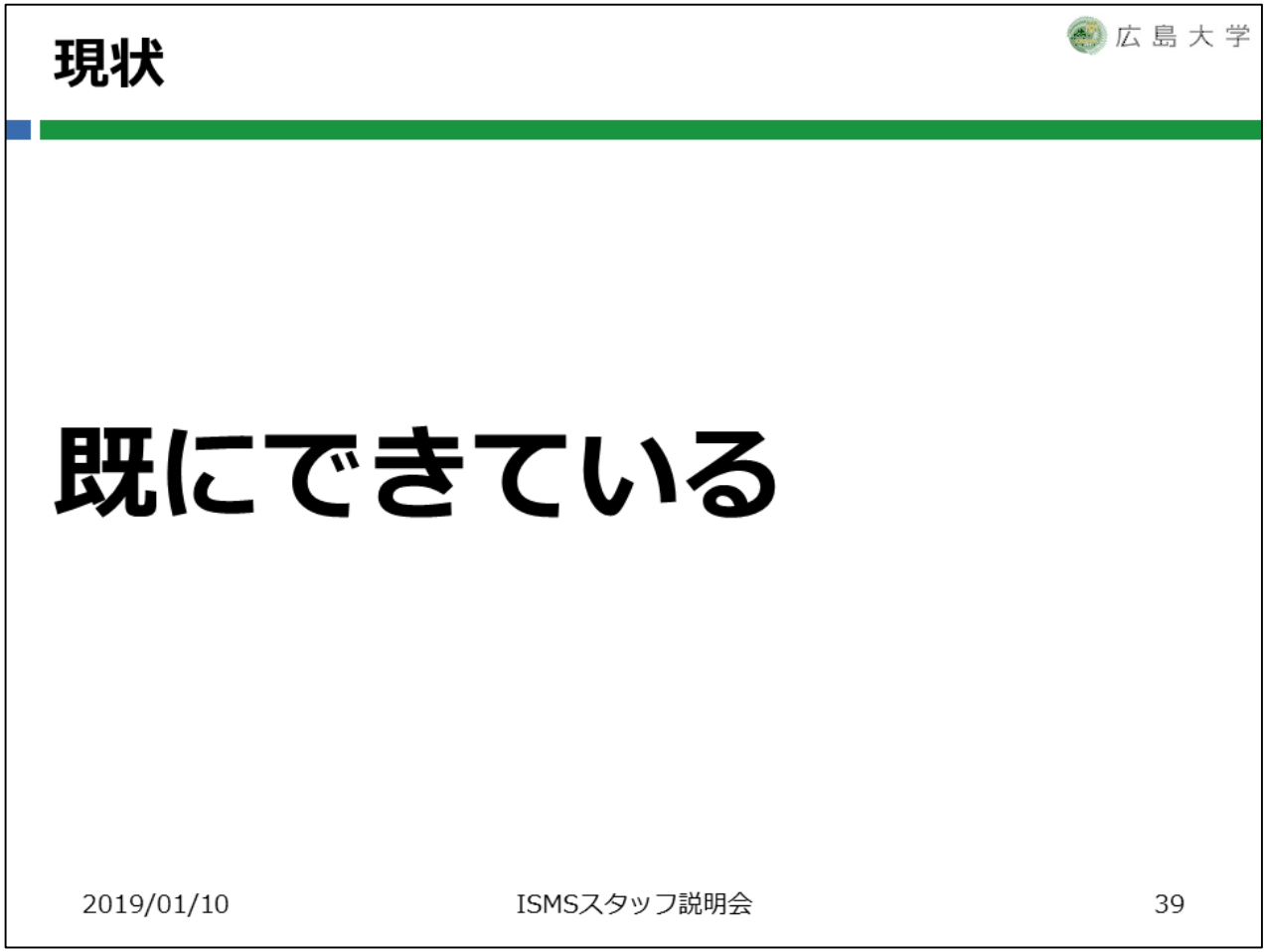
ISMSスタッフへの教育

ISMSスタッフ説明会
ISMSミニミニ通信

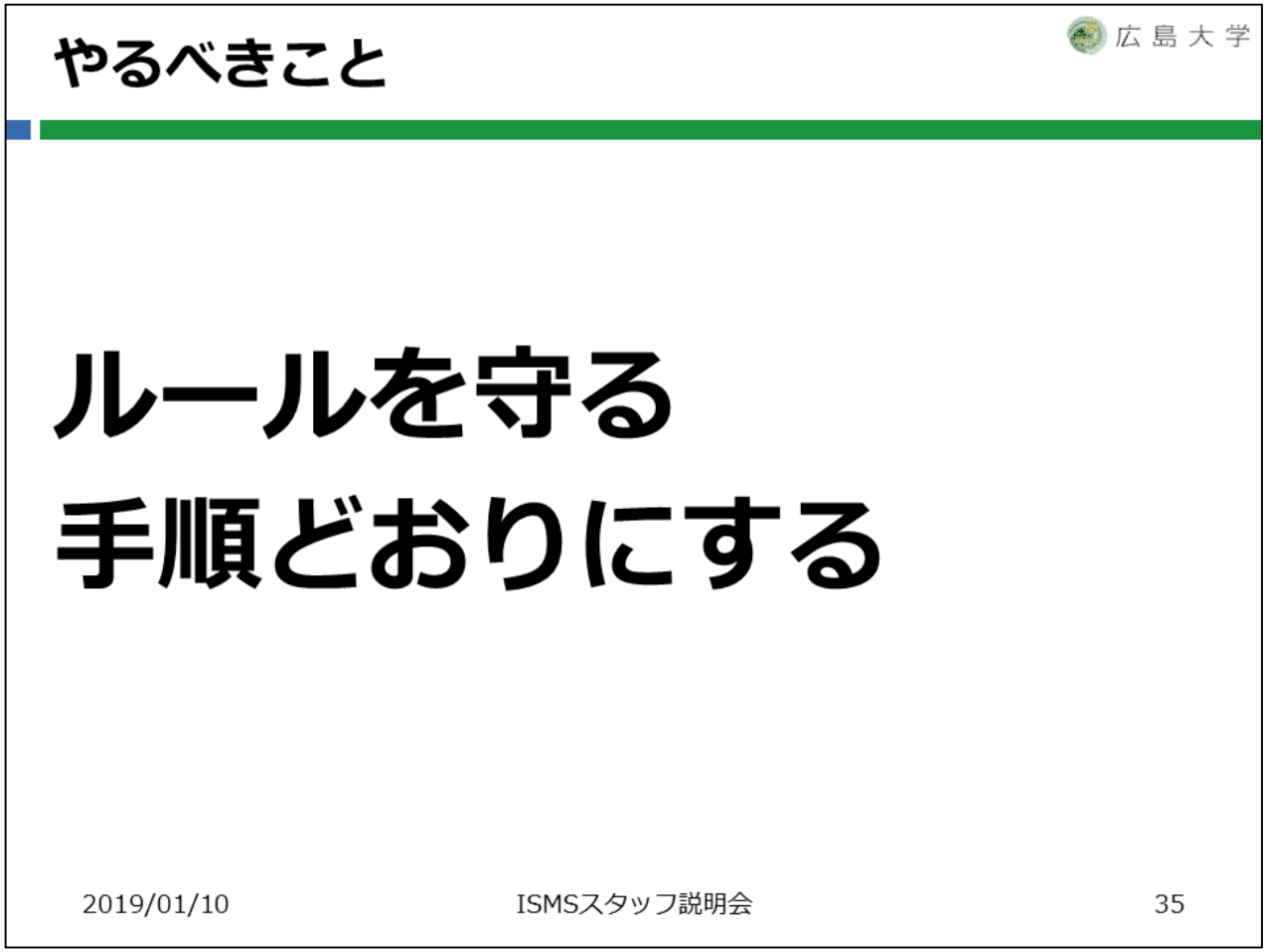
ISMSスタッフ説明会



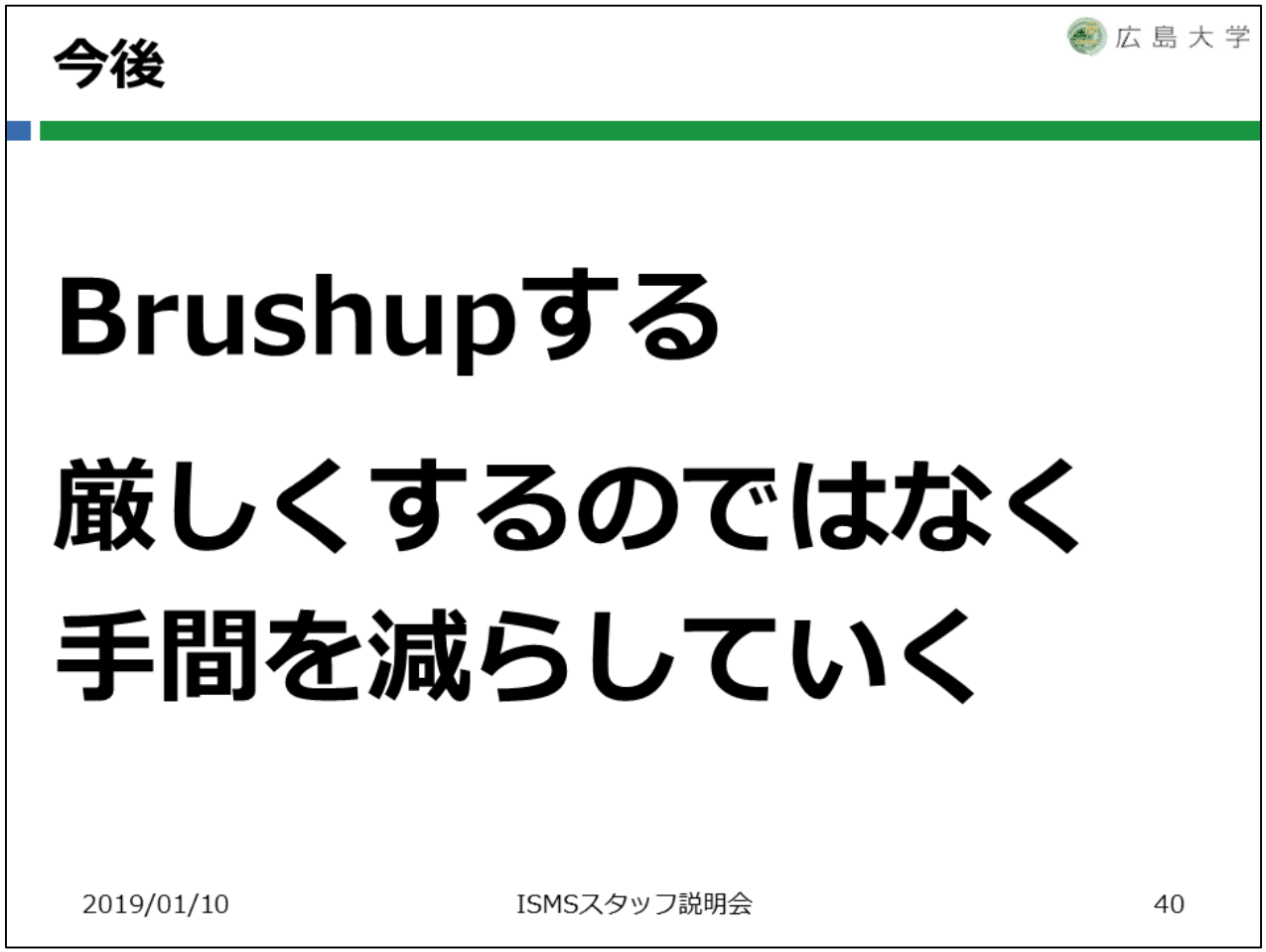
ISMSスタッフ説明会



ISMSスタッフ説明会



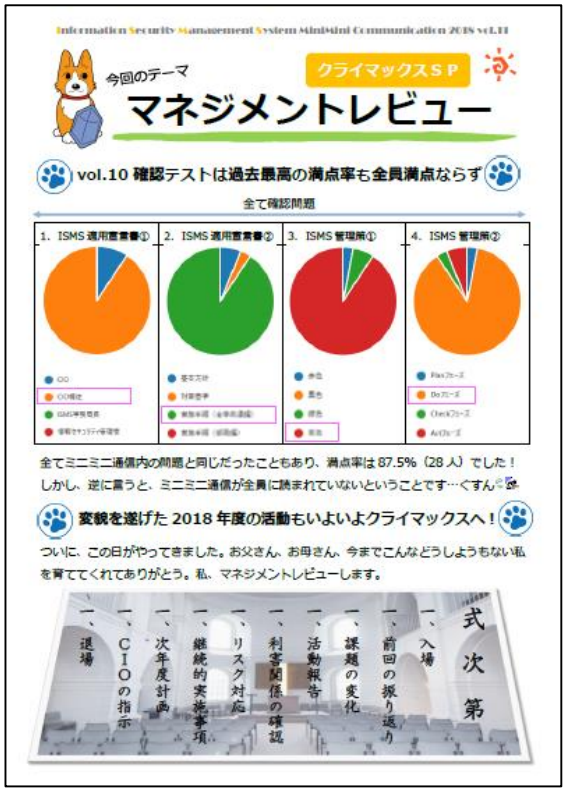
ISMSスタッフ説明会



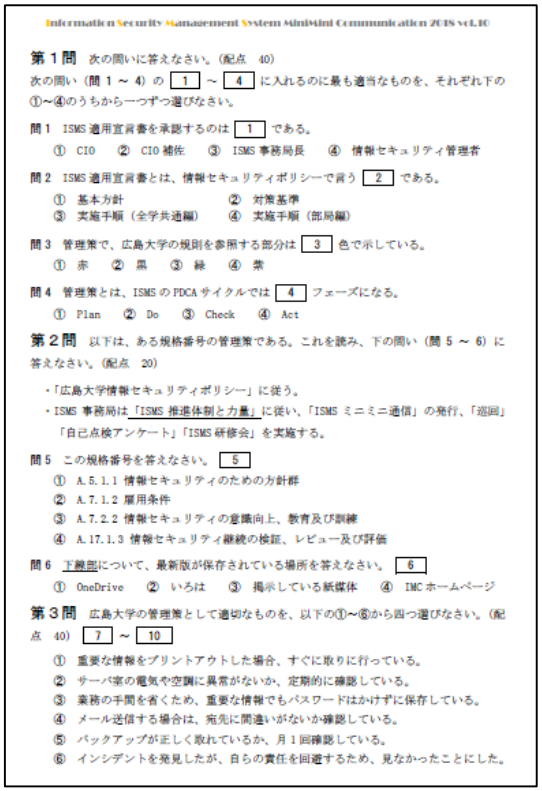
ISMSミニミニ通信

広島大学

毎月１回以上の発行（必須：確認テストの実施）



結婚式風



センター試験風

格付けチェック風

ISMSは…

広島大学のISMSが生まれ変わりました。

ISMSはISMSクラウドセキュリティの前提です。

クラウドセキュリティを考えてみましょう。

期間限定無料コンサルティング

広島大学財務・総務室情報部情報化推進グループ

主任（ISMS事務局員）谷　友博

tani17[AT]hiroshima-u.ac.jp

ありがとうございました。