日本大学総合学術情報センター
ＩＳＭＳ認証取得への道

日本大学総合学術情報センター
汗と涙の・・・

Index

日本大学総合学術情報センターの位置付け

日本大学の歴史

①創立年　明治22年（1889年），創立者　山田顕義（時の司法大臣），
　学校名　　日本法律学校，
　設立目的　日本の法治国家として整備を図る目的
②略年史　明治36年　日本大学と改称
　　明治37年　専門学校令による大学となる
　　昭和25年　短期大学（現短期大学部）設置
　　平成元年　創立100周年記念式典挙行
　　平成６年　総合学術情報センター開設
　　　情報企画課
　　　システム管理課
　　　学術情報課

日本大学の特徴

①教育機関
- 大学　14学部83学科
- 大学院　20研究科　32研究所
- 高校・中学校　11校
- 専門学校　4校
- 幼稚園
- 病院　6病院

②教員数　3,749人
- 職員数　4,011人
- 学生数　99,360人（大学，大学院 高校・中学校，幼稚園児含む）

（以上　平成21年5月1日現在）

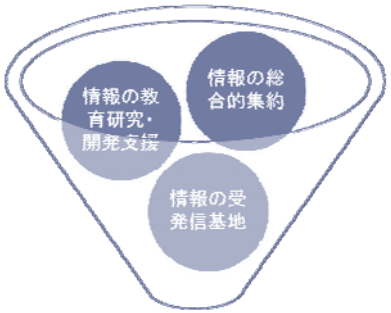
③立地条件　福島県郡山市から静岡県三島市　主に33カ所（付属高校含む）
- 校地面積　31,284,335㎡（9,463,511坪）
- 校舎面積　1,492,107㎡（451,362坪）

④その他

部科校による独立採算制

総合学術情報センターの役割

部科校からの真の信頼を得るには・・・



- 放送サービス
- ネットワークサービス
- 図書情報サービス
- データアーカイブサービス
- 研究支援サービス

ICTを活用しオール日大の総合性を発揮

ＩＳＭＳ制度について

情報セキュリティマネジメントシステム
Information Security Management System

多発する情報セキュリティ事故

個人情報のインシデントトップ10

No.	漏えい人数	業種	原因
1	99万5,023人	公務(他に分類されないもの)	管理ミス
2	76万6,356人	公務(他に分類されないもの)	管理ミス
3	65万3,424人	卸売・小売業	不正アクセス
4	34万9,827人	金融・保険業	管理ミス
5	29万1,338人	公務(他に分類されないもの)	管理ミス
6	26万9,350人	金融・保険業	管理ミス
7	26万2,781人	公務(他に分類されないもの)	管理ミス
8	25万4,677人	金融・保険業	管理ミス
9	23万2,970人	情報通信業	内部犯罪・内部不正行為
10	21万3,443人	公務(他に分類されないもの)	管理ミス

※NPO　日本ネットワークセキュリティ協会　セキュリティ被害調査ワーキンググループ
2008情報セキュリティインシデントに関する報告書V1.3より

情報セキュリティ事故の特徴

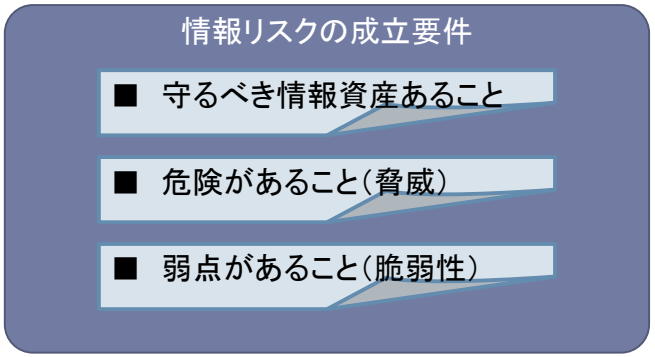
- 極秘情報がネット上に流出
  - ウイニー＋アンチニー（ウイルス）等による公的機関の機密性の高い情報の漏洩
- 大量な情報の流出
  - 電子情報は複製（コピー）が容易である弊害
- 内部者による漏洩が大半
  - 紛失/誤廃棄・・・34%
  - 意図しない漏洩・・・22%
  - 誤送信・・・13%

※最近1年間の事故：月間情報セキュリティHPより

- ネット上に流出した情報は削除不可
  - インターネット上での漏洩は全世界に情報が拡散
- 個人情報の場合は企業と個人の双方に被害
  - 企業：信用失墜，多額の賠償金
  - 個人：犯罪等への利用される恐怖，しつこい勧誘

情報セキュリティの意味

- 情報リスクからの安全性を確保することをいう

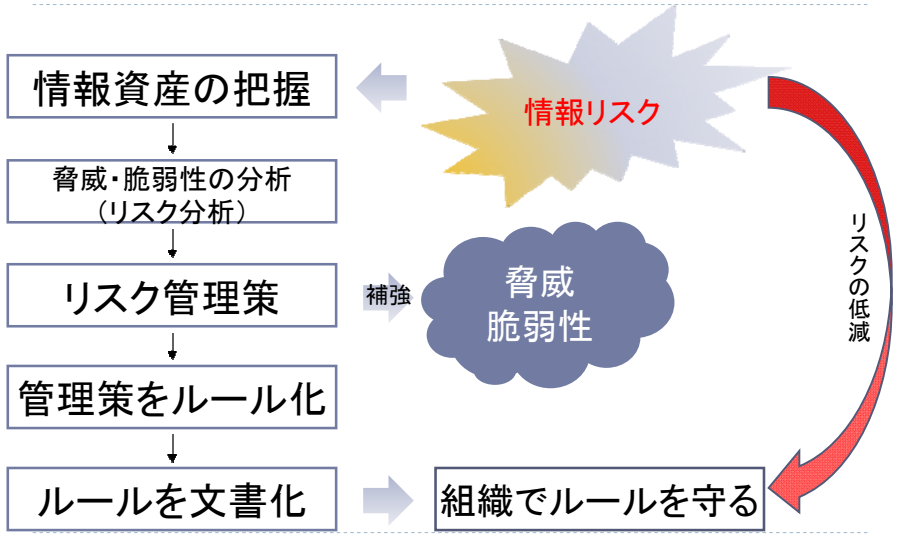


情報セキュリティ対策のポイント

- 個別に対応しても効果があがらない
  - 玄関に鍵をかけても，裏窓に鍵がかかっていなければ防犯にならないと同じこと
- 総合的な情報リスク対策を講じる
- 総合的とは
  - 組織が一体となった対策
  - 体系的な管理（マネジメントシステム）として行う

ISMS認証制度を有効に活用

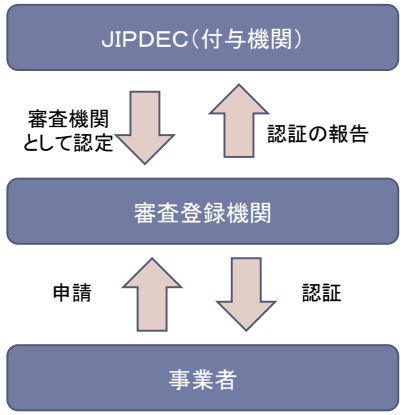
情報セキュリティ対策の考え方



ISMS認証制度とは？

- 「ISO27001(JIS Q 27001)」により，適切な情報セキュリティ管理体制を構築している事業者を(財)日本情報処理開発協会(JIPDEC)が定める審査登録機関が審査
  - http://www.isms.jipdec.jp/
- 審査がOKであれば，ISMSマークの使用が許諾。
- 正式名称は「ISMS適合性評価制度」という
- 約3200団体が認証を取得

ISMS認証制度の仕組み



ISO27001とは？

- 情報セキュリティマネジメントシステムとして，最低限必要な内容を「要求事項」として示した
- 2005年に国際規格として制定
- 日本では，ほぼ同じ内容で日本工業規格として，2006年に「JIS Q 27001」として制定
- 他のマネジメントシステム規格と同様に，PDCAサイクルを基本
  - ISO9001(品質マネジメントシステム)
  - ISO14001(環境マネジメントシステム)
  - JISQ15001(個人情報保護マネジメントシステム)
  - ISO20000(ITサービスマネジメントシステム)

ISO27001の構成

- 【0.序文】
  - 目的とISMSの確立，導入，運用，監視，見直し，維持及び改善をする手法
- 【1.適用範囲】
  - 組織等における適用範囲の宣言
- 【2.引用規格】
  - ISO17799「情報セキュリティマネジメントの実践のための規範」
- 【3.用語及び定義】
- 【4.情報セキュリティマネジメントシステム】
  - ISMSの確立及び運営管理，文書化に関する要求事項
- 【5.経営陣の責任】
- 【6.ISMSの内部監査】
  - 内部監査の実施と記録
- 【7.ISMSのマネジメントレビュー】
  - 経営陣への定期的なレビュー
- 【8.ISMSの改善】
  - 不適合な是正処置及び予防措置
- 【附属書A】:管理目的及び管理策
- 【附属書B】:OECD原則とこの規格
- 【付属書C】

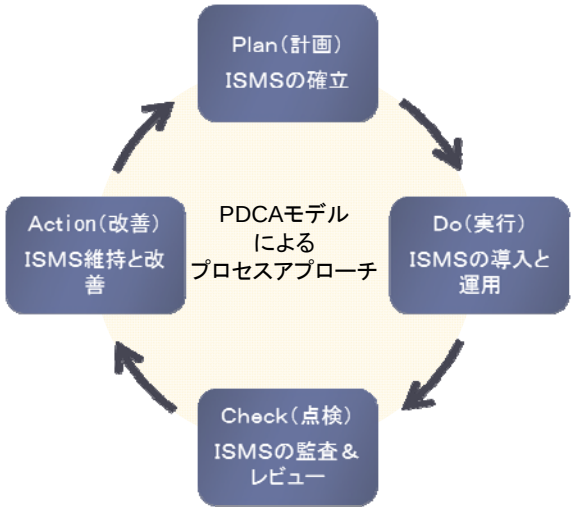
文書体系

情報セキュリティ基本方針
適用宣言書

情報セキュリティ管理手引書	情報セキュリティインシデント管理手引書
情報取扱手引書	ISMS文書管理手引書
情報機器管理手引書	教育手引書
ネットワーク運用管理手引書	ISMS内部監査手引書
アクセス制御手引書	マネジメントレビュー手引書
人的セキュリティ管理手引書	是正・予防処置手引書
情報システム開発保守手引書	外部委託管理手引書
コンピュータウイルス対策手引書	事業継続管理手引書

リスクに対する管理策はルールとして文書化される。

ISMSのアプローチ



ＩＳＭＳ認証取得に向けて

大学の情報資産には何がある？

- 情報そのもの
  - 個人情報（学生情報，校友情報，教職員情報など）
  - 教育・研究情報（論文，研究報告，教育コンテンツなど）
  - 知的財産情報（特許権，商標権，著作権など）
  - 財務情報（支出・収入，債権，負債，固定資産など）
  - 上記に伴うドキュメント類
- 情報を取り扱うシステム
  - 各種コンピュータシステム
  - ネットワーク，データベースなど
  - 上記に伴う設計書などのドキュメント類

情報資産は大学の血液だ！！

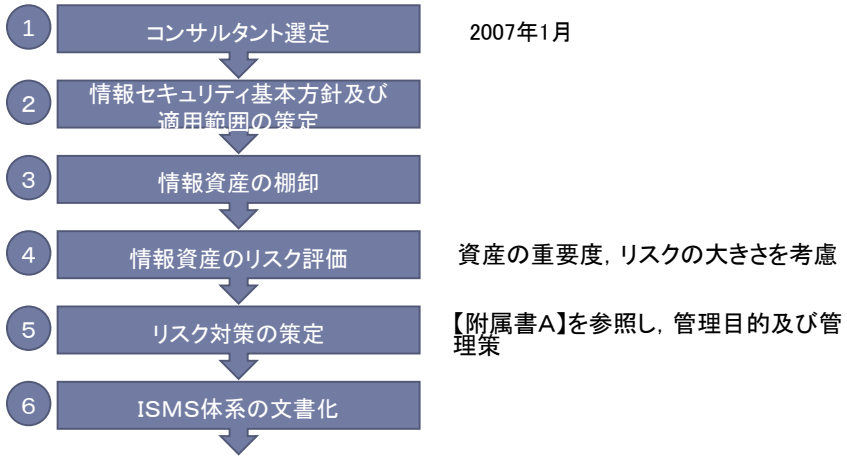
脅威には何がある？

- 不正アクセスによる脅威
  - Webサーバ改ざん，データベース侵入による情報漏えい
- パソコン等盗難による脅威
  - 事務所・車上荒らし，盗難物転売及び情報漏えい
- 災害による脅威
  - 地震，火事，水害によるシステムサービス停止
- 機器故障による脅威
  - システムダウン，通信障害によるシステムサービス停止
- 意識の低さによる脅威
  - 情報媒体のおき忘れ，紛失など人的ミス
  - 不正行為

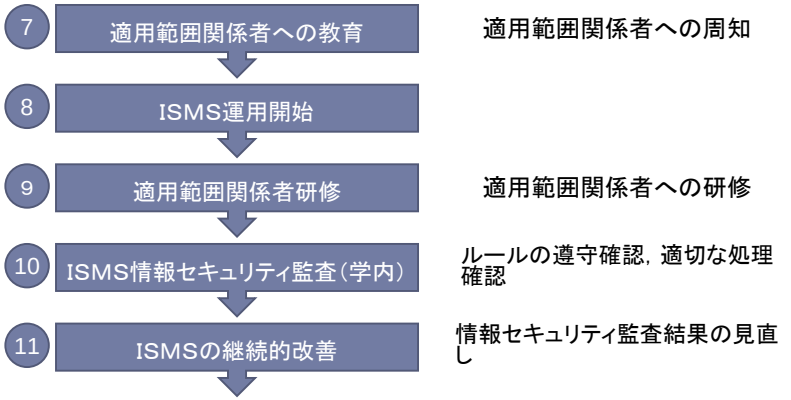
脆弱性には何がある？

- 関係外の人が自由に事務所に出入りできる
- ファイルを格納してあるキャビネットに鍵がない
- セキュリティに関する教育を教職員にしていない
- データベースにアクセス制限をしていない
- 大学のパソコンを許可なく自宅等に持ち帰っている
- 大学のネットワークに容易に接続ができる
- 秘密情報をシュレッダーでなくゴミ箱にすてている
- 外部メモリーが容易に使用できる
- 機密情報をメールに添付して送信している
- etc

ISMS取得スケジュールその１



ISMS取得スケジュールその２



ISMS取得スケジュールその３

12	第三者認証機関による審査（ステージ1）	文書審査：2日間での関係者ヒアリング
13	第三者認証機関による審査（ステージ2）	実地審査：2日間で前回の指摘事項確認及び現地での目視確認
14	ISMS認証所得	2007年12月
15	ISMS維持審査（1年後）	ヒアリング及び現地での目視確認
16	ISMS維持審査（2年後）	ヒアリング及び現地での目視確認
17	ISMS更新・移行審査（3年後）	

情報セキュリティ基本方針及び適用範囲の策定

- 情報セキュリティの定義
  - 情報資産の「機密性」，「完全性」，「可用性」を確保・維持すること
- 目的
- 適用範囲
  - 当センターサーバー室
  - 当センターにおける施設管理
  - 当センター所属の全教職員（臨時，その他従事者含む）

情報セキュリティを保つポイント

機密性

・許可された者だけがアクセス・閲覧できること。
機密性が損なわれた例：防衛庁の軍事情報の漏洩

完全性

・情報の内容や情報処理が正確であること。
完全性が損なわれた例：ホームページの改ざん

可用性

・使うべきときにその情報を使うことができること。
可用性が損なわれた例：自動改札の停止事故，座席予約システムの故障

情報資産の棚卸し

- 情報資産の目録作成
  - 情報資産（紙情報・電子情報）
  - ソフトウェア資産（各種アプリケーションソフト等）
  - ハードウェア資産（パソコン，プリンター，サーバ，ルータ等
  - 媒体（DAT，CD-ROM，USBメモリー等）
  - サービス（プロバイダー，ネットワーク回線キャリア）
  - 要員（システムオペレータ，常駐委託者）
- 情報資産グループ化

情報資産のリスクの評価

- リスクの分析
  - 情報資産価値（機密性） 影響度3段階
  - 情報資産価値（完全性） 影響度3段階
  - 情報資産価値（可用性） 影響度3段階

  ＋ 情報資産価値 =3～9
  - 脅威の評価 影響度3段階
  - 脆弱性の評価 影響度3段階

  × リスクスコア =1～9
- リスク許容値
  - 目安となる数値　情報資産価値×リスクスコア

リスク対策の策定

リスクの軽減
・適切な管理策を採用

リスクの保有
・意識的かつ客観的な受容

リスクの回避
・資産の廃棄，事業の撤退

リスクの移転
・外部委託，保険加入

附属書A 管理目的及び管理策

A.5 セキュリティ基本方針
A.6 情報セキュリティのための組織
A.7 資産の管理
A.8 人的資源のセキュリティ
A.9 物理的及び環境的セキュリティ
A.10 通信及び運用管理
A.11 アクセス制御
A.12 情報システムの取得，開発及び保守
A.13 情報セキュリティインシデントの管理
A.14 事業継続管理
A.15 順守

適用宣言書作成

運用時に行うこと―リスク対応計画―

管理策
- 既に実行している管理策
- これから実行する管理策 → 実行計画
- 実行しない管理策

有効性の測定

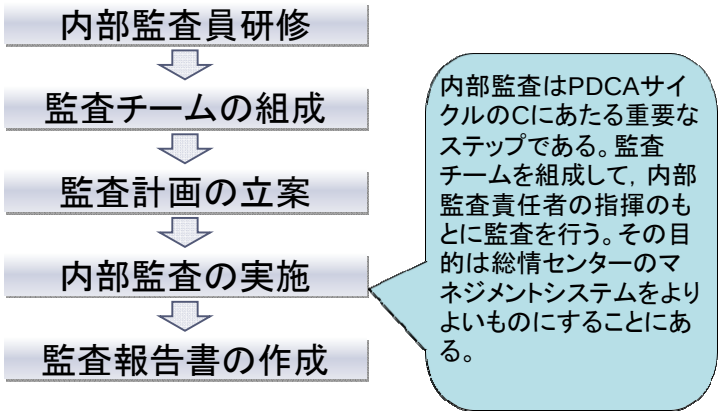
すでに実行している管理策とこれから実行する管理策の実施計画を立案して，その有効性を把握する。

運用時に行うこと―教育―

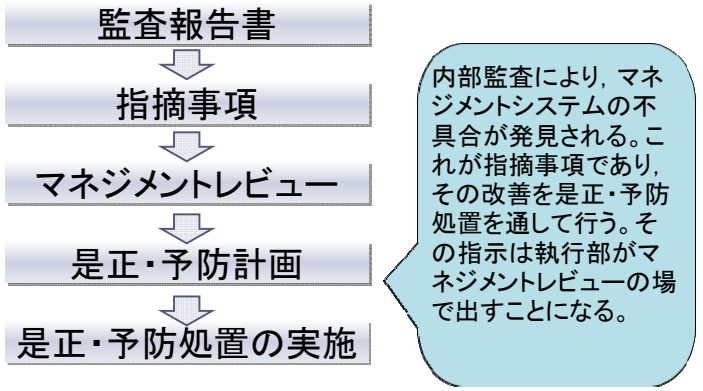
- 必要なスキルの明確化
- 教育の計画の立案
- 教育・訓練の実施 ← 教育記録
- 効果の測定 ← 理解度テスト

ISMSでは，教育を重視している。計画を立てて，実施し，その記録を残し，さらに何らかのかたちで効果（有効性）を確認する。

運用時に行うこと―内部監査－



運用時に行うこと
－マネジメントレビュと是正･予防処置－



ＩＳＭＳ認証を取得して

認証取得後の留意点

- 取得後もマネジメントシステム体制の維持が必要
  ・教職員の教育
  ・内部監査
  ・記録類の保管
  ・継続的な改善
- 毎年維持審査があり，3年後に更新審査がある
  審査ではISMSがきちんと運用されているかどうかを確認する。

最後に

- 情報資産の棚卸し＆リスク評価は重要
  - 情報資産のランク付けが，扱う教職員の意識改革
  - 情報資産のランク付けが，ICT活用
  - 守るべき情報と捨てるべき情報
- 理想の対応と現実的な対応にかい離
  - 理想的な対応を盛り込みやすい（人・物・金・情報）
  - 小さく産んで大きく育てよう
- 有事の時が大事
  - インシデント発生時の迅速な対応＝報告（責任者＆利用者）
  - インシデント対応はシステムに頼らない
  - 原因の報告と記録

ご清聴ありがとうございます。
少しでも参考になれば幸いです。

日本大学総合学術情報センター　小野
2009/11/12

※参考資料　「ISMS初期教育資料」2007　SRA柄澤明久著
【図解】よくわかるISO27001
NPO　日本ネットワークセキュリティ協会　セキュリティ被害調査ワーキンググループ