学術コンテンツ課の
ISMS推進について

2021年11月17日（水）
NIIサービス説明会

国立情報学研究所 学術情報基盤推進部
学術コンテンツ課
浅野 秀明

はじめに

国立情報学研究所　学術基盤推進部　学術コンテンツ課は、
ISMS (Information Security Management System:
情報セキュリティマネジメントシステム) に関する
国際的なセキュリティ規格 (ISO/IEC 27001:2013 /
JIS Q 27001:2014) の認証を取得しました
（2021年3月26日付け)。

適用範囲は、学術コンテンツ課における
「学術情報公開・共有に関する業務」
「利用機関向けサービスの開発・運用・保守」です。

本日は

- ISMSとは何か？
- 学術コンテンツ課が推進するねらい
- 取組の実際

をご説明することで

- ISMS自体を知って頂くとともに
- ISMS推進の考え方・重要性の概要も知って頂く

ことが目的です。

（皆様のご所属先へISMS認証取得自体を直接お願いするものではありません。）

そもそも…ISMSってなに？

ISMS：Information Security Management System

＝ 情報セキュリティマネジメントシステム

国際標準化機構の規格　ISO/IEC27001（対応する日本規格は JIS Q 27001）

による規程で、ISO上のマネジメントシステムは、目標を達成するために

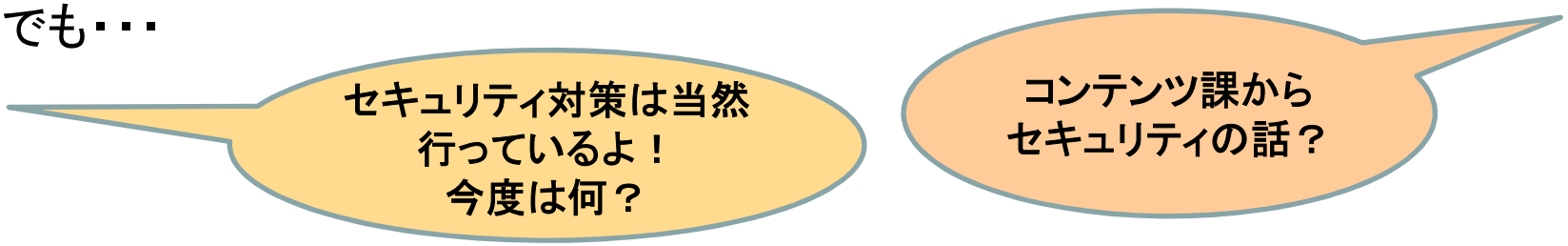
組織の構造、役割及び責任、計画及び運用を確立する仕組みを示します。

そこからISMSは、下記のように説明されます。

情報セキュリティ活動のPDCAサイクルを回し続けることで、

効果的に推進、維持、継続的に改善するもの。

でも・・・



ISMSでの「情報セキュリティ」

ISMSでの「情報セキュリティ」は、

- 組織が持つ全て（媒体は非限定）の情報＝情報資産

と捉え、それぞれの情報資産を

- 機密性：予め認められた人だけが、予め認められた範囲・方法のみ取扱可能な状態であること
- 完全性：改ざん、削除されていない、正確な状態であること
- 可用性：予め認められている人が、予め認められた方法で要求した時に、利用可能な状態であること

の観点から維持されるよう、管理、保守します。

素朴な疑問

「媒体は非限定」って
電子情報だけじゃないの？

- 対象となる「情報」は、電子情報だけではなく、紙も含め全般

言うのは簡単だけど
情報ごとに作成事情があるよね

- 「情報」ごとに「機密性・完全性・可用性」を整理

国際標準に合わせるなんて
うちじゃムリ！！

- 規定はどの組織でも利用可能なように策定されている

  （汎用性がある⇔各組織での具体的な対応は各組織で整備）

取り組む意義

ISMS推進は、負担が大きいように思うけど
取り組む意義はあるの？

- ISO/IEC27001・JIS Q 27001は、ISMSを確立し、実施し、維持し、継続的に改善するための要求事項を規定したもの
- ISMSは、組織のニーズ及び目的、セキュリティ要求事項、組織が用いるプロセス、規模、構造と、時間による変化の影響を受ける。（法令、ガイドライン・組織内規程・契約等関連する要求事項への対応も含む）

⇒組織として、上記の影響に対応した情報セキュリティ管理を実施できていることが外部認証される。

⇒組織の能力が、内外で評価可能になる。

学術コンテンツ課が取り組む意義

ISMS推進を通じて、

学術コンテンツ事業に関する日常の情報セキュリティ管理を

より組織的、継続的に行うことで,

利用者・利用機関の皆様により安心して

サービスをご利用/業務手続頂けるよう努めること

組織的な情報セキュリティ管理への取組は、

学術コンテンツ課に限らず、全ての利用機関にも

幅広くご参考頂けると思われることから、ご案内するもの

ISMS推進＝PDCAを回すこと

PDCAサイクルによる継続的改善＝認証取得がゴールではない!!

Plan:計画
対象・方針・目標の設定
リスクの特定・分析・評価の実施

- 組織方針、目標、対象範囲決定
- 情報資産の洗い出し
- リスク特定（課題・リスク源特定）
- 脅威、脆弱性の洗い出し
- 計画の詳細策定/改訂

Do:運用
計画の実施
教育・訓練の実施

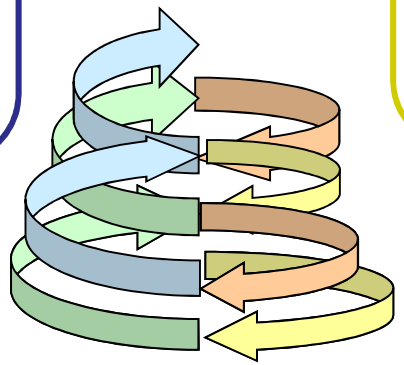
- 計画に基づく実運用を通し、適正なリスク対処
- 構成員への教育研修、訓練

Check:評価
監査・評価・レビューの実施

- 内部監査
- パフォーマンス評価
- 総括責任者によるレビュー
- 外部認証機関による審査

Action:改善
対象・方針・目標の見直し

- 方針、目標、対策の見直し

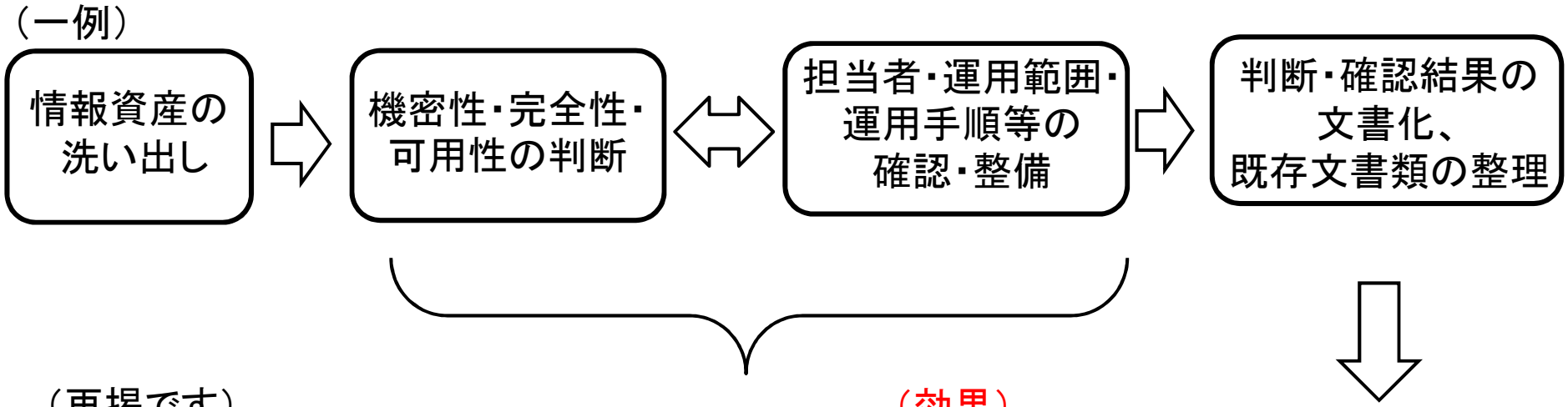


PDCAの詳細はNII内に設置したISMS-WGで検討承認

※法令、ガイドライン・組織内規程・契約等、関連する要求事項の変更には随時対応

ISMS対応の一例【文書化】

ISMS推進⇒文書化/既存文書類再整理⇒業務の整理にも繋がります



（再掲です）

機密性：予め認められた人だけが、予め認められた　範囲・方法でのみ取扱可能な状態
完全性：改ざん、削除されていない、正確な状態
可用性：予め認められている人が、予め認められた方法で要求した時に、利用可能な状態

（効果）

- 業務内の暗黙知、属人化部分の明瞭化
- 担当者、管理者間の情報共有の推進
- 関連する要求事項への対応度合の底上げ、組織内対応方法の共通化

⇒PDCAサイクルへ載せ継続的な向上を図る

最後に…苦労しやすい点

- 外部認証を取る＝文書化した内容は、認証評価担当者が分かる形にする
- 組織としての情報確認・整理＝担当外職員でも理解可能な形にする

各担当者の専門性がベースにある業務・運用情報には

各担当者が【常識的な知識・取扱】と捉える部分が入りにくい印象

⇒ 積極的な調整と、未知情報の習得意識が必要

- 関連する要求事項では、規定・契約書的観点から情報取扱は厳密化の傾向

コンテンツ業務の「オープン化」と相反性がある

⇒ISMS推進への煩雑感、負担感の軽減に努める必要

⇒要求事項とコンテンツ業務、双方の観点を意識する必要

学術コンテンツ課のISMS推進はスタートしたばかりなので、

PDCAサイクルを継続し、向上を図って参ります。