パネルディスカッション

討議テーマ

テーマ1：「気候変動に関わるマネジメントシステム規格の追補版への対応について」

テーマ2：「 NIST OSCALが切り開く、ISMSと情報セキュリティの未来」

2024.12.6
JNSA 標準化部会
日本ISMSユーザグループ

パネリストのご紹介

パネリスト			パネリストの立場
ISMS-AC	**保木野 昌稔 氏**	一般社団法人情報マネジメントシステム認定センター(ISMS-AC)	**ISMSのその信頼性の向上と維持に向けて活動している認定機関としてのアドバイス**
SC27/WG1	**山下　真 氏**	ISO/IEC JTC1/SC27 WG1小委員会、WG4小委員会（国立研究開発法人 情報通信研究機構）	**標準化の観点でのアドバイス**
	土屋 直子 氏	ISO/IEC JTC1/SC27 WG1小委員会（NTTテクノクロス株式会社）	
ISMS-UG	**羽田 卓郎 氏**	日本ISMSユーザグループインプリメンテーション研究会｜ISO/IEC JTC1/SC27 WG1小委員会リエゾン（リコージャパン株式会社）	**規格を具体的に実装する上でのアドバイス**
	井崎 友博 氏	標準化部会 日本ISMSユーザグループ　インプリメンテーション研究会 ISO/IEC SC 27/WG 1小委員会　井崎　友博 （SecureNavi株式会社 代表取締役CEO）	

モデレータ：魚脇 雅晴
（標準化部会 日本ISMSユーザグループ WGリーダー
（エヌ・ティ・ティ・コミュニケーションズ株式会社）

パネルディスカッション（テーマ1）

パネルディスカッション概要

テーマ1：「気候変動に関わるマネジメントシステム規格の追補版への対応について」

「気候変動に関わるマネジメントシステム規格の追補版への対応について」標準化の観点での要求事項についての解説とそれをどのように現行のISMSの中に取り入れていけば良いかについて標準化のメンバーとISMS-UGのメンバーでディスカッションして方向性を模索する。

主な論点

- 気候変動を課題（issue）とするか否かの判断プロセス＆考慮ポイント
- 気候変動を課題（issue）とする場合のその内容と対応レベルの考え方
- 具体的なISMSへの実装方法について
- 課題としない選択肢はあるのか？　など

認定機関の観点

マネジメントシステム認証、認定、相互承認

相互承認

認定機関(ISMS-AC) ⇔ **認定機関**

ISO/IEC 17011

認定

ISO/IEC 17021-1、
ISO/IEC 27006-1

認証機関（審査機関）

認証

ISO/IEC 27001

被認証組織（企業等）

IAF（国際認定フォーラム）

**TC（技術委員会）において、
追補版の適用に伴う被認証組織、認証機関及び認定機関の対応内容を決定**

１．被認証組織に求められる対応

■既存のマネジメントシステム規格に対する気候変動への配慮の追補版に関するIAF及びISO共同コミュニケ

- Joint ISO-IAF Communique re Climate Change Amds to ISO MSS

■追補版の適用に伴う、認証された適合組織、認証機関及び認定機関の対応に関するIAF TCの決定

- https://iaf.nu/en/news/iaf-and-iso-publish-joint-communique/

■上記を参照し、自組織のマネジメントシステムの開発、維持、有効性において、気候変動の側面とリスクを考慮し、該当する場合、組織の目標や活動に組み込まれていることを確認してください。

2．マネジメントシステム認証機関に求められる対応

■被認証組織への対応

➢追補版の発行及び組織として必要な対応について、認証した組織に周知してください。

■認証審査における対応

➢認証審査で、気候変動を含め、関連性があると判断されたすべての外部及び内部の課題が考慮されていることを被認証組織が証明できない場合には、その内容に応じて、適切な所見としてください。

➢参考：

- 被認証組織が**気候変動について考慮して**おり、そのマネジメントシステムに関連する**課題である**と判断している場合には、必要に応じて被認証組織による目標や活動に組み込まれていることを確認してください。
- 被認証組織が、そのマネジメントシステムにとって**気象変動は関連性のある課題ではない**とみなしている場合、その決定を下し、関連する措置を実行するための被認証組織のプロセスの有効性を確認してください。

標準化の視点

気候変動への二つの取り組み：　一般　(1/2)

講演資料より

1. 気候変動を人類の課題と認識し、国、社会、組織、人々がこれに取り組む。
   a. 気候変動を抑制するために、原因に働きかける。
      ・・・ COP21：温室効果ガス排出の管理　等
   b. 気候変動の結果に国、社会、組織、人々が適応する。
      気温上昇、海面上昇、激甚災害増加等に対処する。
      ・・・ SDGs 目標13「気候変動に具体的な対策を」 等

2. 気候変動の結果が組織にもたらす影響に組織が対処する。

注　組織にもたらす影響を低減するために、組織が気候変動の原因に働きかける（温室効果ガス排出を削減する）ことは、現実にはない。「2. a.」

気候変動への二つの取り組み： ISMS

講演資料より

	1. a. 人類の課題と認識し、原因に働きかける。	2. 結果が組織にもたらす影響に対処する。
ISOにおける活動	ロンドン宣言、マネジメントシステム規格の追補	---
ISMSにおける活動	気候変動を抑制するために原因に働きかける。	気候変動の結果がもたらす情報セキュリティリスクを特定し、対処する。
リスクマネジメントのプロセス（ISO 31000:2018）	特に、 「組織及びその状況の理解」	主にリスクアセスメント／リスク対応
ISO/IEC 27001:2022で関係する事項	特に、 4.1 組織及びその状況の理解、 **同 追補（2024）**	主に　6.1.2 情報セキュリティリスクアセスメント 6.1.3 情報セキュリティリスク対応 8.2 情報セキュリティリスクアセスメント 8.3 情報セキュリティリスク対応
ISMSにおける施策の例	温室効果ガス排出の少ない手段を選ぶ。	気候変動の結果に応じて、情報及び施設・設備・装置・機器の可用性を確保する管理策を実施する。
追補との関係	追補で「課題（前提や与件）とするか否かの決定」を求めている活動	ISOのロンドン宣言を背景とする追補とは別の、組織自身のための活動

まとめ (1/2)

講演資料より

1. ISO/IEC 27001:2022 追補の発行

　2024年2月に、ISO/IEC 27001:2022 追補が発行された。背景に、国連における気候変動対応の活動と、これに沿うISOの『ロンドン宣言』がある。

2. 追補で加えた要求事項

　気候変動に関する事項が、箇条4に本文と注記として追加された。気候変動がISMSにおける組織の課題であるか否かを決定することが、追加の要求事項である。

まとめ (2/2)

講演資料より

3. 気候変動の原因に働きかける活動　「1. a.」

国連における気候変動対応、ISOのロンドン宣言を背景とする活動。

例えば、ISMSの活動における製品やサービスの調達に際して、環境負荷を考慮する。この考慮は、多くの場合、組織全体の気候変動への取組みの一部に位置づけられるのではないか。

4. 気候変動の結果への対応　「2.」

気候変動の結果が組織自身にもたらす影響への対応は、ISO/IEC 27001箇条6及び箇条8に規定する情報セキュリティリスクアセスメント及び情報セキュリティリスク対応の要求事項に基づき決定し、実施する。

対応の内容は、「情報及び施設・設備・装置・機器の可用性の確保」である。

ISMSへの実装の観点

パネルディスカッション：気候変動

1. ISO/IEC 27001:2022 気候変動に関する追補対応の考慮点

　気候変動が箇条4.1の「ISMSの意図した成果を達成する組織の能力に影響を与える課題」となるかについては、組織の判断であるが地球上で活動する組織であれば、気候変動に全く影響を受けないという事は考えられない。

　1組織のISMS活動が地球規模の気候変動にどれだけ寄与出来るかも評価しにくいが、ISOのマネジメントシステムを導入する全ての組織が、気候変動を自組織の課題とすることは、長期的に気候変動に対する好ましい影響を与えるものであると信じたい。

パネルディスカッション：気候変動

2.　気候変動に関する組織の対応

- 気候変動による環境変化（気温上昇、災害の発生など）に対する組織の適応

  ⇒既に事業継続や災害対応などで考慮し対応している（必要があれば組織の外部状況の課題にしているはず）。

- 気候変動への貢献（緩和）対応

  ⇒緩和的対策に関しては、組織のISMS適用範囲における情報の保護という観点では、これまで課題とはみなしてこなかった

  ⇒CO2削減を組織の義務でもあると解釈すれば、ISMSの活動を行う上で少しでもCO2削減につながるよう検討することが望ましい。

  ⇒考えられる対策は、「ICT設備の冗長化対策における消費電力の削減」「クラウド事業者など供給者の選定において気候変動への取り組みを考慮する」「情報システムの開発及び更新に際し、セキュリティに配慮した開発のライフサイクルに電力消費削減の考慮を組み込む」などが考えられるが、あくまでも組織のビジネス活動の中で可能な範囲で行えばよいと考える。

パネルディスカッション（テーマ２）

パネルディスカッション概要

テーマ2：「 NIST OSCALが切り開く、ISMSと情報セキュリティの未来」
（自動化/省力化に向けての取り組み、マネジメントシステムとの連携など）

ISMSの運用について自動化/省力化に向けての取り組みとしてNISTが開発したOSCALを利用して効率化を模索出来ないかについて未来を語ります。システム化によって効率化する観点とマネジメントシステムとしての特性を考慮した連携方法などバランスの取り方などディスカッションを行う。

主な論点

- **ISMSの自動化、省力化は可能か？**
- **なぜOSCALが求められているか？ニーズは？**
- **マネジメントシステムとのギャップと協調点（バランス）**
- **OSCALにマッチした適用領域として考えられるものは？**

認定機関の観点

標準化の視点

テーマ２ NIST OSCALが切り開く、ISMSと情報セキュリティの未来

＜標準化の視点から＞

１．OSCALの対象範囲

情報システムにおける技術的管理策だけでなく、組織的管理策、人的管理策、物理的管理策も
評価できるか？

２．異なるフレームワーク間の対応づけ

ISO/IEC 27001、ISO/IEC 27002 の管理策と 他の例えばNIST SP800-53 の管理策の
対応づけは、どの程度までOSCALでできるのか、また、対応付けの手掛りと手法は？

３．人との役割分担

ISMS活動の中で、OSCALの支援を活用できることと、人の思考や活動として残ることの
切り分けや役割分担はどのようになるのか。人に求められる能力、知識は、どのように変わるか？

４．未来の標準文書

OSCALがより効果的であるために、今後の標準文書（規格）はどのようにできているとよいのか？

ISMSへの実装の観点

テーマ２ OSCALのISMSにおける活用方法

1. **ISMSの未来**

   NIST OSCAL のみならず、AI等の技術を活用した業務の自動化・効率化が、様々な産業において発生している。認定機関観点・標準化観点・実装観点のそれぞれの立場から、ISMSの自動化・効率化についてどのような考えや意見があり、ISMSの未来はどうなると考えているか？

パネルディスカッション：OSCAL

●全般：

OSCALがマネジメントシステムの効率化と省力化に貢献して欲しいという期待は大きいが、現時点では使い勝手の面で課題も大きいと思われる。一般の組織に普及するために、使いやすさ、変更のしやすさ、他の要求事項との組み合わせ対応、評価の自動化などについて、OSCAL自体とベンダーの取り組みに期待したい。

パネリスト　羽田　卓郎

パネルディスカッション：OSCAL（期待したいこと）

	利用者の期待する事	現状	今後実現してほしいこと
使いやすさ	27001等の規格改訂や他の要求事項（NIST、FISC、自工会部工会ガイドライン等）の組み合わせに対応	△	マージ機能があるが、自動的にはできない。何をマージするかは組織が行う。また、他の要求事項やガイドラインの組み合わせ機能はないが、その発行団体からカタログモデルが提供され、ベンダーがマージ機能を提供してくれることに期待
	プロファイルから規定書としてWordやPDFで出力したい	×	ベンダーがプリント機能を提供してくれることに期待
実装面	OSCALに登録した情報でICT機器やアプリケーションのセキュリティ制御	△	OSCALファイル同士で参照を貼ることは可能だがフリーフォーマットのコントロールリストを参照はできない。セキュリティ設定の自動化機能をベンダーが提供に期待
	OSCAL以外のアプリのコントロールリストを取り込んだり出力するなどの連携	×	OSCALフォーマットを読み書きするソフトウェアがサードパーティーから提供されることを期待
	プロファイルの実施記録の入力やCSV 形式の読み込み	×	ベンダーからの使いやすいツールの提供に期待
評価機能	実装した内容をもとに、SYSログや実行記録などを自動的に取り込んで評価	△	ログや記録を取り込む「評価結果モデル」があり、取り込むためのフォーマットは用意されている。但し、評価自体は組織が行う事になる（自動評価はできない）。