日本 ISMS ユーザグループ／日本ネットワークセキュリティ協会 主催

情報セキュリティマネジメント・セミナー2023

ISO/IEC 27000 ファミリー規格の動向 及び ISO/IEC 27002 管理策について

2023年12月18日
NTTテクノクロス株式会社
土屋 直子
ISO/IEC JTC1 SC27 WG1国内委員会委員

目次

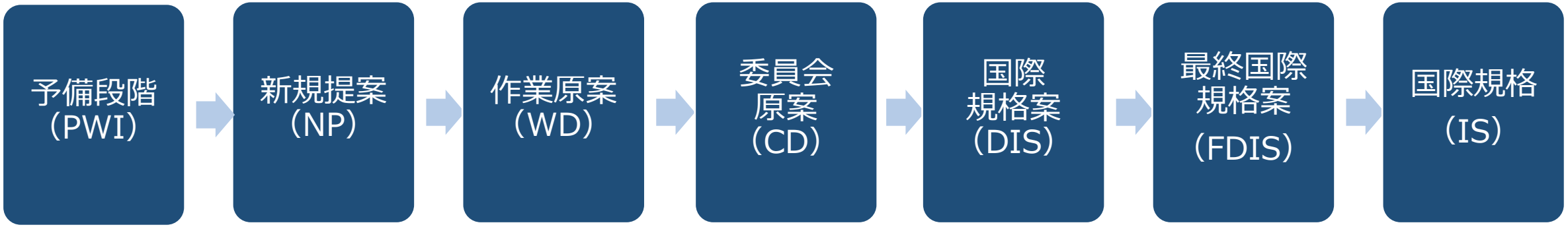
1. ISO/IEC 27000 ファミリー規格の動向

2. ISO/IEC 27002:2022 管理策

3. 属性（Attribute）- 管理策の理解のために

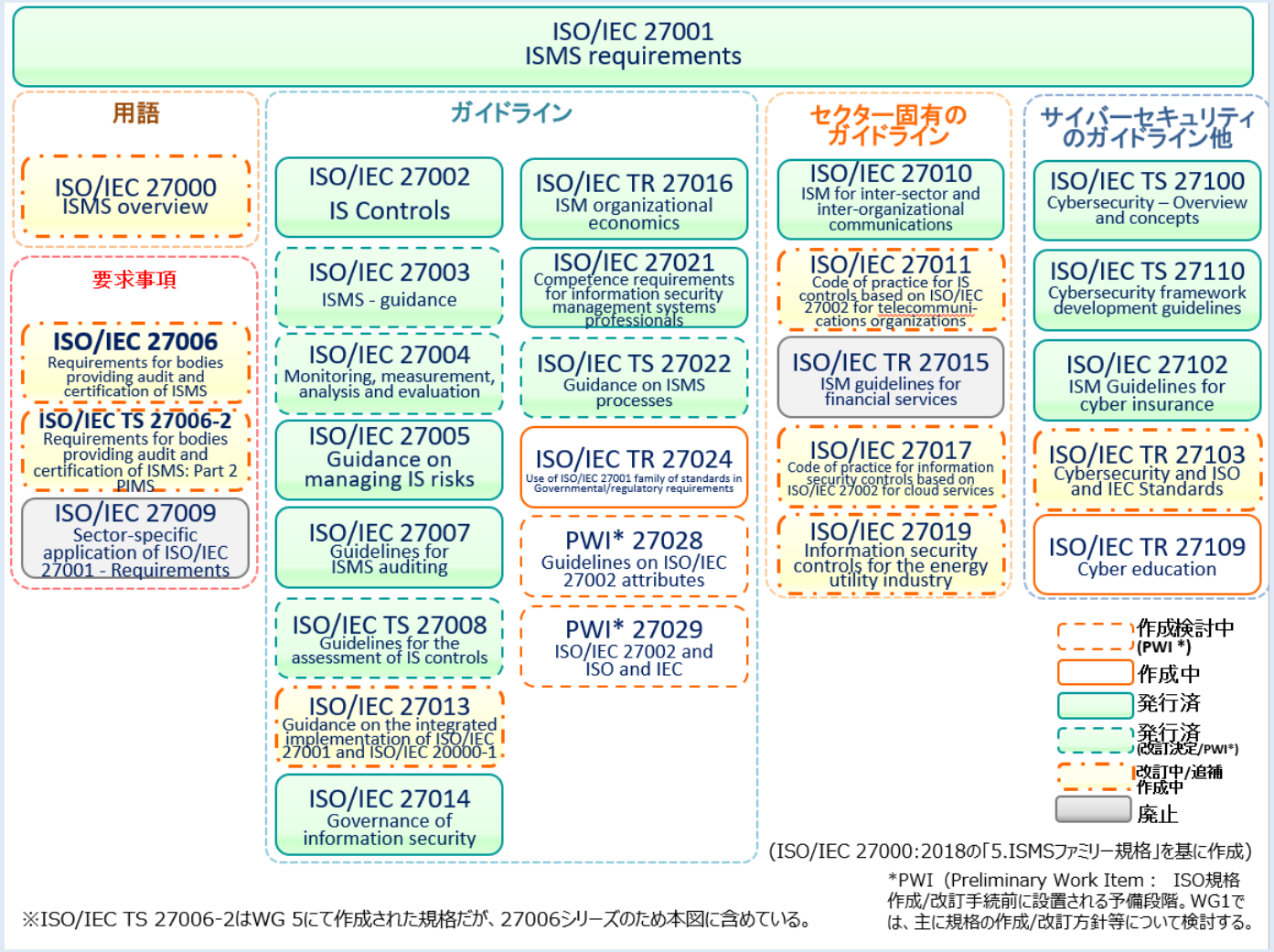
ISO規格が発行されるまで

国際標準化組織
JTC 1: 情報技術
SC 27: 情報セキュリティ、サイバーセキュリティ及びプライバシー保護
WG 1: 情報セキュリティマネジメントシステム



「ISO/IEC 27000 ファミリー規格の動向 及び ISO/IEC 27002 管理策について」 NTTテクノクロス 土屋直子

ISO/IEC 27000 ファミリー規格とは



出典：JIPDEC「ISO/IEC 27000 ファミリー規格について」（2022年11月1日）をもとに作成
https://www.jipdec.or.jp/project/smpo/u71kba000000jjgv-att/27000family_20221101.pdf

「ISO/IEC 27000 ファミリー規格の動向 及び ISO/IEC 27002 管理策について」 NTTテクノクロス 土屋直子

ISO/IEC 27000 ファミリー規格の改訂

ISO/IEC 27002:2022改訂を受けて、その他のISO/IEC 27000ファミリー規格が順次、改訂中

ISO/IEC 27002:2022（情報セキュリティ管理策）
ISO/IEC 27001:2022（ISMS-要求事項）
ISO/IEC 27005:2022（情報セキュリティリスクマネジメント指針）

ISO/IEC 27006-1（ISMSの審査及び認証を行う機関向け要求事項）**【FDIS】**
ISO/IEC 27011（通信事業者向け情報セキュリティ管理策）**【FDIS】**
ISO/IEC 27017（クラウドサービス向け情報セキュリティ管理策）**【CD】**

ISO/IEC 27019（エネルギー業界向け情報セキュリティ管理策）**【DIS】**
ISO/IEC 27103（サイバーセキュリティとISO/IEC規格）**【CD】**
ISO/IEC 27000（ISMS-概要及び用語）**【WD】**
ISO/IEC 27008（情報セキュリティ管理策の評価ガイドライン）**【PWI】**
・・・

「ISO/IEC 27000 ファミリー規格の動向 及び ISO/IEC 27002 管理策について」 NTTテクノクロス 土屋直子

ISO/IEC 27000 ファミリー 改訂状況

規格番号	発行年	規格内容	改訂段階
27000	2018年	ISMS-概要及び用語	WD
27001	2022年	ISMS-要求事項	
27002	2022年	情報セキュリティ管理策	
27003	2017年	ISMS-指針	PWI
27004	2016年	情報セキュリティマネジメント - 監視、測定、分析及び評価	
27005	2022年	情報セキュリティリスクマネジメント指針	
27006-1	2015年	ISMSの審査及び認証を行う機関向け要求事項	FDIS
27006-2 （WG5）	2021年	ISMSの審査及び認証を行う機関向け要求事項 - 第2部 プライバシー情報マネジメントシステム （ISO/IEC 27701認証対応）	
27007	2020年	ISMS監査ガイドライン	
TS 27008	2019年	情報セキュリティ管理策の評価ガイドライン	PWI
27009	2020年	ISO/IEC 27001の分野固有の適用の要求事項	廃止
27010	2015年	セクター間及び組織間のコミュニケーションのための 情報セキュリティマネジメント	

「ISO/IEC 27000 ファミリー規格の動向 及び ISO/IEC 27002 管理策について」 NTTテクノクロス 土屋直子

ISO/IEC 27000 ファミリー 改訂状況

規格番号	発行年	規格内容	改訂段階
27011	2016年	通信事業者向け情報セキュリティ管理策	FDIS
27013	2021年	ISO/IEC 27001とISO/IEC 20000-1の統合実装のための指針	DIS
27014	2020年	情報セキュリティガバナンス	
TR 27016	2014年	情報セキュリティマネジメントの組織活動の経済性	
27017	2015年	クラウドサービス向け情報セキュリティ管理策	CD
27018 （WG5）	2019年	PIIプロセッサとして作動するパブリッククラウドにおける 個人識別可能情報(PII)の保護のための実践の規範	CD
27019	2017年	エネルギー業界向け情報セキュリティ管理策	DIS
27021	2017年	ISMS専門家のための力量の要求事項	
TS 27022	2021年	ISMSプロセスの指針	
TR 27024	（開発中）	政府／規制上の要求事項におけるISO/IEC 27001ファミリー規格の利用	WD
27028	（開発中）	ISO/IEC 27002の属性の指針	WD
27029	（開発中）	ISO/IEC 27002とISO/IEC規格	DTR
27701 （WG5）	2019年	プライバシー情報マネジメントのためのISO/IEC 27001及びISO/IEC 27002への拡張―要求事項及びガイドライン	

「ISO/IEC 27000 ファミリー規格の動向 及び ISO/IEC 27002 管理策について」 NTTテクノクロス 土屋直子

ISO/IEC 27000 ファミリー 改訂状況

規格番号	発行年	規格内容	改訂段階
TS 27100	2020年	サイバーセキュリティー概要及び概念	
27102	2019年	情報セキュリティマネジメントーサイバー保険のためのガイドライン	
TR 27103	2018年	サイバーセキュリティとISO/IEC規格	CD
TR 27109	(開発中)	サイバーセキュリティの教育・訓練	AWI
TS 27110	2021年	サイバーセキュリティフレームワーク開発のためのガイドライン	

「ISO/IEC 27000 ファミリー規格の動向 及び ISO/IEC 27002 管理策について」 NTTテクノクロス 土屋直子

まとめ（1. ISO/IEC 27000 ファミリー規格の動向）

- ISO/IEC 27002:2022の改訂を受けて、
  ISO/IEC 27000 ファミリー規格が順次、改訂されている
- ISO/IEC 27017（クラウドセキュリティ）改訂は現在CD
- ISO/IEC 27028（ISO/IEC 27002の属性のガイドライン）
  などいくつかの規格が新規に開発中

1. ISO/IEC 27000 ファミリー規格の動向

2. ISO/IEC 27002:2022 管理策

3. 属性（Attribute）- 管理策の理解のために

新規管理策

No.	ISO/IEC 27002:2022 新規管理策	
1	5.7 Threat intelligence	脅威インテリジェンス
2	5.23 Information security for use of cloud services	クラウドサービスの利用における情報セキュリティ
3	5.30 ICT readiness for business continuity	事業継続のためのICTの備え
4	7.4 Physical security monitoring	物理的セキュリティの監視
5	8.9 Configuration management	構成管理
6	8.10 Information deletion	情報の削除
7	8.11 Data masking	データマスキング
8	8.12 Data leakage prevention	データ漏えい防止
9	8.16 Monitoring activities	監視活動
10	8.23 Web filtering	ウェブフィルタリング
11	8.28 Secure coding	セキュリティに配慮したコーディング

※ISO/IEC 27002:2022の新規管理策、統合された管理策についての参考資料

土屋直子「ISO/IEC 27002 改定の解説」（情報セキュリティマネジメント・セミナー2022）
https://www.jnsa.org/seminar/2022/isms2022/index.html
土屋直子「改定版ISO/IEC 27002の概要及びISO/IEC 27001最新動向」（情報セキュリティマネジメント・セミナー2021）
https://www.jnsa.org/seminar/2021/isms2021/index.html

「ISO/IEC 27000 ファミリー規格の動向 及び ISO/IEC 27002 管理策について」 NTTテクノクロス 土屋直子

対象が広がった管理策 概要

- 新しい脅威や技術動向に合わせて、
  管理策の内容が更新された。
  （１）表現が修正されているが、対象はほぼ同じ管理策
  （２）対象が広がった管理策
    １）管理策レベルでの対象の拡大
    ２）手引のレベルでの対象の拡大

「ISO/IEC 27000 ファミリー規格の動向 及び ISO/IEC 27002 管理策について」 NTTテクノクロス 土屋直子

5.19 供給者関係における情報セキュリティ

15.1.1 供給者関係のための情報セキュリティの方針

管理策　組織の資産に対する供給者のアクセスに関するリスク管理

実施の手引　組織の資産に供給者がアクセスする際のセキュリティ対策

5.19 供給者関係における情報セキュリティ

管理策　供給者の**製品又はサービスの利用に関連する**情報セキュリティリスク管理

手引　**組織の情報の機密性、完全性及び可用性に影響を与える供給者を利用**する際のセキュリティ対策

ICT基盤の提供なども含め、組織の資産にアクセスするか、しないかに関わらず、組織の情報の機密性、完全性、可用性に影響を与える供給者のセキュリティ対策に対象を広げた

「ISO/IEC 27000 ファミリー規格の動向 及び ISO/IEC 27002 管理策について」 NTTテクノクロス 土屋直子

5.16 識別情報の管理

9.2.1 利用者登録及び登録削除

管理策　利用者の登録及び登録削除の正式なプロセス

実施の手引　利用者IDの登録、無効化、削除

5.16 識別情報の管理

管理策　識別情報の**ライフサイクル全体**の管理

手引　利用者IDの登録、**変更**、無効化、削除

機器・システム等の識別情報の管理

利用者IDの変更も含めた、ライフサイクル全体の識別情報の管理、
機器・システム等の識別情報の管理も対象とした手引の拡充

「ISO/IEC 27000 ファミリー規格の動向 及び ISO/IEC 27002 管理策について」 NTTテクノクロス 土屋直子

8.3 情報へのアクセス制限

9.4.1 情報へのアクセス制限

管理策　情報及びアプリケーションシステム機能へのアクセス制限

実施の手引　アプリケーションシステム機能へのアクセス制御

8.3 情報へのアクセス制限

管理策　情報及び**その他の関連資産**へのアクセス制限

手引　情報及び**その他の関連資産**への
物理的・論理的アクセス制御、**動的アクセス管理**

アプリケーション機能だけでなく、情報及びその他の関連資産の全般的なアクセス制限に対象を広げた

「ISO/IEC 27000 ファミリー規格の動向 及び ISO/IEC 27002 管理策について」 NTTテクノクロス 土屋直子

8.1 利用者エンドポイント機器

6.2.1 モバイル機器の方針
モバイル機器のセキュリティ対策

ノートPC、スマホ、
タブレットなど

11.2.8 無人状態にある利用者装置
無人状態にある装置の適切な保護対策

無人状態のPC、
サーバ、ATMなど

8.1 利用者エンドポイント機器
利用者エンドポイント機器のセキュリティ対策

**デスクトップPC、ノートPC、
スマートフォン、タブレット、
シンクライアントなど**

6.2.1、11.2.8に加え、
有人状態のデスクトップPCなども対象とした

「ISO/IEC 27000 ファミリー規格の動向 及び ISO/IEC 27002 管理策について」 NTTテクノクロス 土屋直子

6.7 リモートワーク

6.2.2 テレワーキング

在宅勤務中心の手引

管理策　テレワーキングのセキュリティ対策

実施の手引　在宅などから職場のネットワークや情報システムに接続する場合のセキュリティ対策

6.7 リモートワーク

管理策　組織の構外で、要員が遠隔で作業する場合のセキュリティ対策

手引　**組織の構外の作業全般**
接続は必ずしも前提としない

在宅勤務以外の、組織の構外全般の作業も対象とした手引の拡充

「ISO/IEC 27000 ファミリー規格の動向 及び ISO/IEC 27002 管理策について」 NTTテクノクロス 土屋直子

7.9 構外にある資産のセキュリティ

11.2.6 構外にある装置及び資産のセキュリティ

管理策　構外にある資産に対するセキュリティの適用

実施の手引　構外に持ち出した装置及び媒体の保護

7.9 構外にある資産のセキュリティ

管理策　構外にある資産の保護

手引　構外に持ち出した機器、装置、BYODの保護

構外に設置した装置（アンテナ、ATMなど）の保護

モバイル機器などの情報を格納する機器の構外への持ち出しに加え、情報は格納しなくても、組織の情報のCIAに影響を及ぼす、構外に設置したアンテナなどの装置などにも対象を広げた

「ISO/IEC 27000 ファミリー規格の動向 及び ISO/IEC 27002 管理策について」 NTTテクノクロス 土屋直子

まとめ（2. ISO/IEC 27002:2022 管理策）

- セキュリティ脅威や技術動向を反映した手引の充実化
- 対象範囲が広がった管理策
- 管理策の一般化による全体的な網羅性の確保

「ISO/IEC 27000 ファミリー規格の動向 及び ISO/IEC 27002 管理策について」 NTTテクノクロス 土屋直子

1. ISO/IEC 27000 ファミリー規格の動向

2. ISO/IEC 27002:2022 管理策

3. 属性（Attribute）- 管理策の理解のために

ISO/IEC 27002:2022に含まれている属性（Attribute）

情報セキュリティ管理策を様々な観点から見るための属性を設定

属性(属性値)

管理策タイプ	情報セキュリティ特性	サイバーセキュリティ概念	運用機能	セキュリティドメイン
#予防 #検知 #是正	#機密性 #完全性 #可用性	#識別 #防御 #検知 #対応 #復旧	#ガバナンス #資産管理 #情報保護 #人的資源のセキュリティ #物理的セキュリティ #システム及びネットワークのセキュリティ #アプリケーションセキュリティ #セキュリティを保った構成 #識別情報及びアクセスの管理 #脅威及びぜい弱性の管理 #継続 #供給者関係のセキュリティ #法令及び順守 #情報セキュリティ事象管理 #情報セキュリティ保証	#ガバナンス及びエコシステム #保護 #防御 #レジリエンス

「ISO/IEC 27000 ファミリー規格の動向 及び ISO/IEC 27002 管理策について」 NTTテクノクロス 土屋直子

属性の用途

- 管理策の分類
  （組織・人・物理・技術による分類以外の分類）
- リスク対応プロセスにおける管理策の決定の補完
  （例：予防・検知・是正のための管理策がバランスよく採用されているか、等）
- 他のフレームワークとの互換性
  （例：サイバーセキュリティフレームワークとの互換性）
- 組織独自の属性の導入
  （ISO/IEC 27002:2022に記載されている５つの属性以外の属性を作って
  活用することもできる）
- **管理策の理解を深めるツールとして**

「ISO/IEC 27000 ファミリー規格の動向 及び ISO/IEC 27002 管理策について」 NTTテクノクロス 土屋直子

属性 管理策タイプ

属性名 **管理策タイプ**

用途例 予防の管理策、検知の管理策、是正の管理策のバランスをチェックするなど

観点 情報セキュリティインシデントとの発生との関係において、
該当管理策が、いつ、そしてどのようにリスクを修正するか

属性値と管理策例

属性値	該当する管理策例
予防	・アクセス制御 ・暗号の利用 ・セキュリティに配慮したコーディング ・専門組織との連絡
検知	・ログ取得 ・監視活動
是正	・監視活動 ・情報セキュリティインシデントへの対応 ・情報のバックアップ ・専門組織との連絡

【管理策をより理解するために】

- 「専門組織との連絡」はインシデントの予防の管理策でもあり、かつ是正の管理策ともなりえる
- 「情報のバックアップ」はインシデントを予防することはできない。是正する管理策である
- ISO/IEC 27002:2022では、検知・是正の管理策を強化した

「ISO/IEC 27000 ファミリー規格の動向 及び ISO/IEC 27002 管理策について」 NTTテクノクロス 土屋直子

属性 管理策タイプ 参考

予防の管理策
（情報セキュリティインシデントの発生を防ぐ）

検知の管理策
（情報セキュリティインシデントの発生を検知する）

是正の管理策
（情報セキュリティインシデントの結果を制限する）

検知の管理策
予防の管理策が失敗した場合にリスクを低減する

是正の管理策
検知の管理策が失敗した場合にリスクを低減する

予防の管理策と検知の管理策は、**情報セキュリティインシデントの発生頻度を下げる**

是正の管理策は、情報セキュリティインシデントの発生頻度を下げることはできないが、**情報セキュリティインシデントの重大度を下げる**ことができる

「ISO/IEC 27000 ファミリー規格の動向 及び ISO/IEC 27002 管理策について」 NTTテクノクロス 土屋直子

属性 情報セキュリティ特性

属性名 **情報セキュリティ特性**

用途例 各管理策の性質を理解するためなど

観点 該当管理策が、情報のどの性質を維持するために貢献するか

属性値と管理策例

属性値	該当する管理策例
機密性	・秘密保持契約又は守秘義務契約 ・クリアデスク・クリアスクリーン ・装置のセキュリティを保った処分又は再利用 ・情報の削除 ・データマスキング ・データ漏えい防止 ・ケーブル配線のセキュリティ
完全性	・クロックの同期 ・情報のバックアップ
可用性	・情報処理施設・設備の冗長性 ・事業継続のためのICTの備え ・情報のバックアップ ・ケーブル配線のセキュリティ

【管理策をより理解するために】

- 機密性・完全性・可用性の中の一部の性質を維持するために貢献する管理策がある
- 多くの管理策は、機密性・完全性・可用性の全ての性質を維持するために貢献する

「ISO/IEC 27000 ファミリー規格の動向 及び ISO/IEC 27002 管理策について」 NTTテクノクロス 土屋直子

属性 サイバーセキュリティ概念

属性名 **サイバーセキュリティ概念**

用途例 組織がISMSとサイバーセキュリティフレームワークの両方を構築していて、
ISMS管理策とISO/IEC 27110 (NIST CSF）の５つのコンセプトとの関連性を知りたい場合など

観点 ISO/IEC 27110（NIST CSF)のサイバーセキュリティフレームワークとの関連性

属性値と管理策例

属性値	該当する管理策例
識別	・情報セキュリティのための方針群 ・情報及びその他の関連資産の目録
防御	・アクセス制御 ・暗号の利用
検知	・ログ取得 ・監視活動
対応	・監視活動 ・情報セキュリティインシデント管理の計画策定及び準備
復旧	・情報セキュリティインシデント管理の計画策定及び準備 ・情報のバックアップ

【管理策をより理解するために】

- ISO/IEC 27002:2022の全ての管理策が、サイバーセキュリティ概念の５つの属性値とマッピングされている
- 管理策タイプとの整合も取れている

「ISO/IEC 27000 ファミリー規格の動向 及び ISO/IEC 27002 管理策について」 NTTテクノクロス 土屋直子

（参考）新規管理策の属性例（サイバーセキュリティ概念）

No.	ISO/IEC 27002 新規管理策	章	サイバーセキュリティ概念（属性）
1	脅威インテリジェンス	組織	Identify（識別）, Detect（検知）, Respond（対応）
2	クラウドサービスの利用における情報セキュリティ		Protect（防御）
3	事業継続のためのICTの備え		Respond
4	物理的セキュリティの監視	物理	Protect, Detect
5	構成管理	技術	Protect
6	情報の削除		Protect
7	データマスキング		Protect
8	データ漏えい防止		Protect, Detect
9	監視活動		Detect, Respond
10	ウェブフィルタリング		Protect
11	セキュリティに配慮したコーディング		Protect

「ISO/IEC 27000 ファミリー規格の動向 及び ISO/IEC 27002 管理策について」 NTTテクノクロス 土屋直子

まとめ（3. 属性（Attribute）- 管理策の理解のために）

属性を活用することによって

- 管理策の理解を深めることができる
- リスク対応プロセスにおいて管理策を決定する際の補完情報を得ることができる

「ISO/IEC 27000 ファミリー規格の動向 及び ISO/IEC 27002 管理策について」 NTTテクノクロス 土屋直子

全体 まとめ

1. ISO/IEC 27000 ファミリー規格の動向

2. ISO/IEC 27002:2022 管理策

3. 属性（Attribute）- 管理策の理解のために

ご清聴ありがとうございました。