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2022

ISO/IEC 27002 改定の解説

2022年12月16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 27002 改定概要

2. 新規管理策

3. 統合された管理策

4. 更新された管理策

5. その他

1. ISO/IEC 27002 改定概要

2. 新規管理策

3. 統合された管理策

4. 更新された管理策

5 . その他

ISO/IEC 27002 規格タイトル

2022年版

ISO/IEC 27002
Information security, cybersecurity and privacy protection – Information security controls
（情報セキュリティ管理策）

2013年版

ISO/IEC 27002
Information technology - Security techniques – Code of practice for information security controls
（情報セキュリティ管理策の実践のための規範）

ISO/IEC 27002:2022 のスコープ

1. **ISO/IEC 27001に基づくISMS**において使用

2. ISMSとは**独立した情報セキュリティ管理策の情報源**として使用

   - 国際的なベストプラクティスとして、組織にて情報セキュリティ管理策を実施するため
   - 組織独自の情報セキュリティ管理ガイドラインの策定のため

ISO/IEC 27002 改定概要

- 基本的には、ISO/IEC 27002:2013を踏襲
- 章構成の見直し
- 新しい脅威や技術動向に合わせて、
  11個の新規管理策を追加
- 各管理策を様々な観点からの見方で見ることができるようにするための属性（Attribute）を設定

ISO/IEC 27002:2022 管理策構成

ISO/IEC 27002:2013

5	情報セキュリティのための方針群
6	情報セキュリティのための組織
7	人的資源のセキュリティ
8	資産の管理
9	アクセス制御
10	暗号
11	物理的及び環境的セキュリティ
12	運用のセキュリティ
13	通信のセキュリティ
14	システムの取得、開発及び保守
15	供給者関係
16	情報セキュリティインシデント管理
17	事業継続マネジメントにおける 情報セキュリティの側面
18	順守

ISO/IEC 27002:2022

5 組織的管理策 （Organizational controls）
6 人的管理策 （People controls）
7 物理的管理策 （Physical controls）
8 技術的管理策 （Technological controls）

NTTテクノクロス

ISO/IEC 27002:2022 目次構成

- まえがき
- 序文
- 1. 適用範囲
- 2. 引用規格
- 3. 用語、定義及び略語
- 4. この文書の構成
- 5. 組織的管理策
- 6. 人的管理策
- 7. 物理的管理策
- 8. 技術的管理策
- 附属書 A (参考) 属性の使用
- 附属書 B (参考) ISO/IEC 27002:2022（この文書）とISO/IEC 27002:2013との対応
- 参考文献

管理策配下の構成

5．組織的管理策　5.1 情報セキュリティのための方針群

属性

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	#機密性 #完全性 #可用性	#識別	#ガバナンス	#ガバナンス及びエコシステム #レジリエンス

管理策（Control）

情報セキュリティ方針及びトピック固有の方針は、これを定義し……

目的（Purpose）

管理層の方向性の継続的な適合性……するため。

手引（Guidance）

……

その他の情報（Other information）

……

管理策概要

2013年版 **114個** ▶▶▶▶▶ 2022年版 **93個**

新規: **11個**
統合: **24個**
更新: **58個**
削除: **0個**

管理策の種類	管理策数
5 組織的管理策	37個
6 人的管理策	8個
7 物理的管理策	14個
8 技術的管理策	34個
合計	**93個**

1. ISO/IEC 27002 改定概要

2. 新規管理策

3. 統合された管理策

4. 更新された管理策

5. その他

新規管理策 概要

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

新規管理策

5.7　脅威インテリジェンス (Threat intelligence)

脅威インテリジェンス（脅威の防止や検知に利用できる情報）の収集・分析

サイバー攻撃などの
脅威に対応するため

- 情報セキュリティの脅威に関する情報の収集・分析
- 組織の情報セキュリティリスク管理プロセスに組み込む

5.23 クラウドサービスの利用における情報セキュリティ (Information security for use of cloud services)

クラウドサービスを利用するプロセスを確立する

クラウドサービスの
普及に対応するため

- 組織がクラウドサービスを利用する時のセキュリティ対策
- クラウドサービスの提供は対象外。ISO/IEC 27017とも整合

NTTテクノクロス

新規管理策

5.30 事業継続のためのICTの備え (ICT readiness for business continuity)

ICTの継続について、計画・実施・維持・試験を実施する

災害やサイバー攻撃などの有事の際にも事業継続を可能にするため

- 災害等が発生しても情報の可用性を確実にする
- ビジネス継続のためのICTの備え

7.4　物理的セキュリティの監視 (Physical security monitoring)

組織の敷地を物理的に監視する

物理的な監視を強化するため

- 守衛
- 侵入探知機、監視カメラ　等

新規管理策

8.9　構成管理 (Configuration management)

ハードウェア、ソフトウェア、サービス（クラウド含む）、ネットワーク等の構成管理

構成管理を確実にするため

- 標準テンプレートの使用
- 構成の管理、監視

8.10 情報の削除 (Information deletion)

情報は不要になった際に削除する

機器・装置の廃棄段階における情報漏えいを防止するため

- 削除手法の選択、削除記録
- 情報削除サービスを利用する際は、削除証明書の取得

新規管理策

8.11 データマスキング (Data masking)

アクセス制御方針や法的要求事項を考慮し、
データマスキングを利用する

個人情報の保護と
利用活用のため

- データマスキング
- 匿名化・仮名化

8.12 データ漏えい防止 (Data leakage prevention)

情報漏えいを検知し防止する

情報漏えいの技術的な
監視を強化するため

- 利用者のデータ利用の監視
- データ漏えいの検知
  （情報が信頼できない外部サービスにアップロードされた時、等）

新規管理策

8.16 監視活動 (Monitoring activities)

ネットワーク、システム、アプリケーションを監視する

技術的な監視を
強化するため

- 利用者のシステムへのアクセスの監視
- 利用者の異常なシステム上の行動を監視

8.23 ウェブフィルタリング (Web filtering)

外部Webサイトへのアクセス制御

不正なWebサイトへの
アクセスを防止するため

- 不法な情報、マルウェアを含むウェブサイト、
フィッシングサイトへのアクセスを防ぐ
- IPアドレスやドメインをブロック（技術的な対策）

新規管理策

8.28 セキュリティに配慮したコーディング (Secure coding)

セキュリティに配慮したコーディング原則をソフトウェア開発に適用する

開発段階からのセキュリティを強化するため

- コーディング前の計画、コーディングの際の考慮事項
- レビュー及び維持

1. ISO/IEC 27002 改定概要

2. 新規管理策

3. 統合された管理策

4. 更新された管理策

5 . その他

統合された管理策 概要

- 管理策と目的が1対1に対応する形になったことにより、同じ目的を持つ複数の管理策が統合、整理された。

（１）ライフサイクルに沿った管理策の統合

（２）統合による管理策の一般化

（1）ライフサイクルに沿った管理策の統合

例）

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ための方針群の定義

5.1.2 情報セキュリティのための方針群のレビュー
情報セキュリティのための方針群のレビュー

5.1 情報セキュリティのための方針群
情報セキュリティ方針及びトピック固有の方針を定義し**(and)**、レビューする。

方針群の定義から承認、発行、伝達、認識、レビューまでの一連の流れを一つの管理策としてまとめた

（1）ライフサイクルに沿った管理策の統合

例）

9.2.2 利用者アクセスの提供(provisioning)
利用者アクセス提供の正式なプロセスの実施

9.2.5 利用者アクセス権のレビュー
利用者のアクセス権の定期的なレビュー

9.2.6 アクセス権の削除又は修正
従業員の雇用、契約の終了時のアクセス権の削除・修正

5.18 アクセス権
アクセス権は提供し、レビューし、変更し **(and)**、削除する。

アクセス権の提供から、レビュー、変更、削除までの一連の流れを一つの管理策としてまとめた

（2）統合による管理策の一般化

例）

18.1.1 適用法令及び契約上の要求事項の特定
関連する法令、規制及び契約上の要求事項の特定

18.1.5 暗号化機能に対する規制
暗号化機能に関する法令及び規制の順守

5.31 法令、規制及び契約上の要求事項
関連する法令、規制及び契約上の要求事項の特定

法規制、契約上の要求事項の特定についての一般的な内容とし、
18.1.5の個別具体的な管理策を吸収した

（2）統合による管理策の一般化

例）

12.4.1 イベントログ取得
イベントログの取得、保持、定期的なレビュー

12.4.2 ログ情報の保護
ログ情報の保護

12.4.3 実務管理者及び運用担当者の作業ログ
実務管理者等の作業ログの記録、保護、定期的なレビュー

8.15 ログ取得
ログの取得、保存、保護、分析

12.4.1と12.4.2を合わせ、ログの取得、保存、保護、分析についての一般的な内容とし、12.4.3の個別具体的な管理策を吸収した

（２）統合による管理策の一般化

例）

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

対象範囲の拡大

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

1. ISO/IEC 27002 改定概要

2. 新規管理策

3. 統合された管理策

4. 更新された管理策

5. その他

更新された管理策 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

対象が広がった管理策

例）

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

対象が広がった管理策

例）

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

対象が広がった管理策

例）

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ための資源の利用の監視、調整

【実施の手引】システムの容量・能力

8.6 容量・能力の管理

【管理策】資源の利用の監視、調整

【手引】**情報処理施設、人的資源、オフィス**などの容量・能力。

システムの容量・能力だけでなく情報処理施設、人的資源、オフィスの容量・能力も含めた手引の拡充

1. ISO/IEC 27002 改定概要

2. 新規管理策

3. 統合された管理策

4. 更新された管理策

5. その他

サイバーセキュリティへの対応

- サイバーセキュリティに対応するための
  管理策の充実化
  例）5.7 脅威インテリジェンス
  　　5.30 事業継続のためのICT の備え
  　　8.16 監視活動、など

- サイバーセキュリティフレームワークとの互換性
  属性：サイバーセキュリティ概念の導入
  （識別、防御、検知、対応、復旧）

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

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）

ISO/IEC 27002:2022 改定のまとめ

- 監視や検知などの管理策の充実化
- 管理策の一般化による全体的な網羅性の確保
  （個別具体的な管理策を吸収した管理策の一般化、
  管理策の対象を広げた一般化）
- 手引の充実化
- サイバーセキュリティへの対応

ご清聴ありがとうございました。