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2021

改定版ISO/IEC 27002の概要及び ISO/IEC 27001最新動向

2021年12月17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. 属性（Attribute）

4. ISO/IEC 27001 改定

ISO/IEC 27002 規格タイトル

改定版

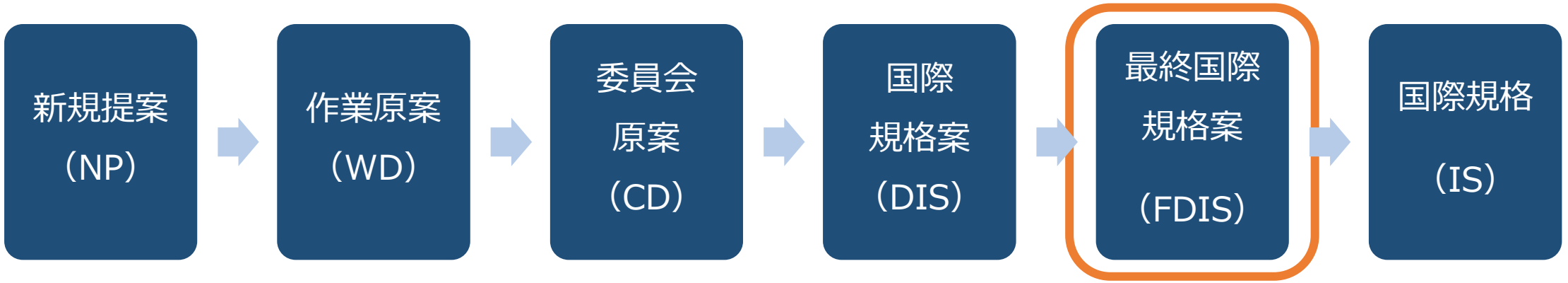
ISO/IEC 27002
Information security, cybersecurity and privacy protection – Information security controls
（情報セキュリティ管理策）

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規範）

ISO/IEC 27002 改定状況

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



ISO/IEC 27002 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/IEC27002改定 章構成

ISO/IEC27002:2013（既存）
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

改定版ISO/IEC 27002

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）

ISO/IEC27002改定 目次構成

- Foreword
- Introduction
- 1. Scope
- 2. Normative references
- 3. Terms, definitions and abbreviated terms
- 4. Structure of this document
- 5. Organizational controls
- 6. People controls
- 7. Physical controls
- 8. Technological controls
- Annex A (informative) Using attributes
- Annex B (informative) Correspondence with ISO/IEC 27002:2013
- Bibliography

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	情報セキュリティプロパティ	サイバーセキュリティコンセプト	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）

情報セキュリティのための方針群は、これを定義し……

目的（Purpose）

情報セキュリティのための経営陣の方向性及び支持を……するため。

実施の手引き（Guidance）

……

関連情報（Other information）

……

管理策概要

2013年版 → 次期改定版

114個 ▶▶▶▶▶ 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. 属性（Attribute）

4. ISO/IEC 27001 改定

新規管理策

No.	ISO/IEC 27002 新規管理策案	
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	クラウドサービス利用のための情報セキュリティ
3	5.30 ICT readiness for business continuity	ビジネス継続のためのICTの備え
4	7.4 Physical security monitoring	物理的セキュリティ監視
5	8.9 Configuration management	設定管理
6	8.10 Information deletion	情報削除
7	8.11 Data masking	データマスキング
8	8.12 Data leakage prevention	データ漏洩の防止
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	セキュアコーディング

5.7 Threat intelligence（脅威インテリジェンス）

脅威インテリジェンスとは

脅威の防止や検知に利用できる情報の総称

- 情報セキュリティの脅威に関する情報の収集
- 情報セキュリティの脅威に関する情報の分析
- 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

ISO/IEC27002:2013の関連する管理策例
■6.1.4 専門組織との連絡

5.23 Information security for use of cloud services
（クラウドサービス利用のための情報セキュリティ）

クラウドサービスを利用するプロセスを確立する

- 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

ISO/IEC27002:2013の関連する管理策例
■ 15 供給者関係

5.30 ICT readiness for business continuity
（ビジネス継続のためのICTの備え）

ICTの継続について、計画・実行・維持・試験を実施する

- 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
- ICT継続計画の定期的な評価、試験、承認

ISO/IEC27002:2013の関連する管理策例
■ 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

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

組織の敷地を物理的に監視する

- 守衛
- 侵入探知機
- 監視カメラ　等

ISO/IEC27002:2013の関連する管理策例

- 11.1.3 オフィス、部屋及び施設のセキュリティ
- 11.2.1 装置の設置及び保護

8.9 Configuration management（設定管理）

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

- 新しくシステムを導入した時のセキュリティ設定
- ベンダ推奨設定
- デフォルトパスワードの変更
- 定期的な設定の見直し
- 設定変更の承認プロセス

ISO/IEC27002:2013の関連する管理策例
■ 14.2.2 システムの変更管理手順

8.10 Information deletion（情報削除）

情報は不要になった際に削除する

- 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

ISO/IEC27002:2013の関連する管理策例
■ 8.1.4 資産の返却 ■ 8.2.3 資産の取扱い ■ 8.3.2 媒体の処分 ■ 11.2.7 装置のセキュリティを保った処分又は再利用

8.11 Data masking（データマスキング）

**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**

- データマスキング
- 匿名化・仮名化
- 利用目的に応じた強度
- 利用の際の合意事項又は制限事項

ISO/IEC27002:2013の関連する管理策例
■ 8.2.3 資産の取扱い ■ 18.1.4 プライバシー及び個人を特定できる情報（PII）の保護

8.12 Data leakage prevention（データ漏洩の防止）

情報漏洩を防止し検知する

- データ漏洩防止ツールの利用
- 利用者のデータ利用の監視
- データ漏洩の検知（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）

ISO/IEC27002:2013の関連する管理策例
■ 9.1.2 ネットワーク及びネットワークサービスへのアクセス ■ 12.4.1 イベントログ取得 ■ 12.4.2 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

8.16 Monitoring activities（監視活動）

ネットワーク、システム、アプリケーションを監視する

- アウトバウンド／インバウンドのネットワークトラフィックの監視
- 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

ISO/IEC27002:2013の関連する管理策例

- 12.4.1 イベントログ取得
- 12.4.2 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
- 16.1.2 情報セキュリティ事象の報告

8.23 Web filtering（ウェブフィルタリング）

外部Webサイトへのアクセス制御

- 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）
- 制限されているウェブサイトへの例外的な使用の承認プロセス

ISO/IEC27002:2013の関連する管理策例
■ 9.1.2 ネットワーク及びネットワークサービスへのアクセス

8.28 Secure coding（セキュアコーディング）

セキュアコーディング原則をソフトウェア開発に適用する

- 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

ISO/IEC27002:2013の関連する管理策例
■ 14.2.5 セキュリティに配慮したシステム構築の原則
■ 14.2.6 セキュリティに配慮した開発環境

1. ISO/IEC 27002 改定概要

2. 新規管理策

3. 属性（Attribute）

4. ISO/IEC 27001 改定

属性（Attribute）

情報セキュリティ管理策を様々な視点から見るための属性を設定

属性(属性値)

管理策タイプ	情報セキュリティプロパティ	サイバーセキュリティコンセプト	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セキュリティ ・アプリケーションセキュリティ ・セキュア設定 ・アイデンティティ及びアクセス管理 ・脅威及び脆弱性管理 ・継続 ・供給者関係セキュリティ ・法的順守 ・情報セキュリティ事象管理 ・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

（参考）新規管理策の属性例

No.	ISO/IEC 27002新規管理策案	章	サイバーセキュリティコンセプト（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	クラウドサービス利用のための情報セキュリティ		Protect（防御）
3	ビジネス継続のためのICTの備え		Respond
4	物理的セキュリティ監視	物理	Protect Detect
5	設定管理	技術	Protect
6	情報削除		Protect
7	データマスキング		Protect
8	データ漏洩の防止		Protect Detect
9	監視活動		Detect Respond
10	ウェブフィルタリング		Protect
11	セキュアコーディング		Protect

1. ISO/IEC 27002 改定概要

2. 新規管理策

3. 属性（Attribute）

4. ISO/IEC 27001 改定

ISO/IEC 27001 改定

ISO/IEC 27001の当面の動向

- ISO/IEC 27002改定を受けて、ISO/IEC 27001の主に附属書Aのみを改定版ISO/IEC 27002の内容に反映させる改定を行う。
- 今回の改定では、主にISO/IEC 27002の附属書Aのみの改定を行い、基本的には本文の改定は行わない。
- 可能な限り、早期の改定を行い、ISO/IEC 27002改定版の発行（2022年Q1）から大幅に遅延しない改定版の発行を目指す。

ISO/IEC 27001の本格改定

- 上記と並行して、ISO/IEC 27001の本格的な改定プロジェクトを立ち上げる。

ご清聴ありがとうございました。