

JT-X1051

情報技術 — セキュリティ技術 — ISO/IEC 27002 に基づく電気通信事業者のための情報セキュリティ管理策の実践のための規範

I.<概要>

本標準は、電気通信事業者において情報セキュリティ管理策を実施するにあたってのガイドラインを規定している。

II.<参考>

1. 国際勧告等の関連

2016年4月に発行されたITU-T勧告X.1051に準拠している。

2. 参照文書

- ・ISO/IEC 27000, 情報技術 - セキュリティ技術 - 情報セキュリティマネジメントシステム - 概要及び用語
- ・ISO/IEC 27002:2013, 情報技術-セキュリティ技術-情報セキュリティ管理策のための実践の規範

3. 改版の履歴

版数	制定日	改版内容
1	2018年2月15日	新規制定

4. 標準策定部門

第1版:セキュリティ専門委員会 (WG2100)

III.<目次>

<参考>

1	適用範囲
2	引用規格
3	定義及び略語
3.1	定義
3.2	略語
4	概要
4.1	本標準の構成
4.2	電気通信事業者における情報セキュリティマネジメントシステム
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
6.1	内部組織
6.2	モバイル機器及びテレワーキング
7	人的資源のセキュリティ
7.1	雇用前
7.2	雇用期間中
7.3	雇用の終了及び変更
8	資産の管理
8.1	資産に対する責任

- 8.2 情報分類
- 8.3 媒体の取扱い
- 9 アクセス制御
 - 9.1 アクセス制御に対する業務上の要求事項
 - 9.2 利用者アクセスの管理
 - 9.3 利用者の責任
 - 9.4 システム及びアプリケーションのアクセス制御
- 10 暗号
- 11 物理的及び環境的セキュリティ
 - 11.1 セキュリティを保つべき領域
 - 11.2 装置
- 12 運用のセキュリティ
 - 12.1 運用の手順及び責任
 - 12.2 マルウェアからの保護
 - 12.3 バックアップ
 - 12.4 ログ取得および監視
 - 12.5 運用ソフトウェアの管理
 - 12.6 技術的ぜい弱性管理
 - 12.7 情報システム監査に対する考慮事項
- 13 通信セキュリティ
 - 13.1 ネットワークセキュリティ管理
 - 13.2 情報の転送
- 14 システム取得、開発及び保守
 - 14.1 情報システムのセキュリティ要求事項
 - 14.2 開発及びサポートプロセスにおけるセキュリティ
 - 14.3 試験データ
- 15 供給者関係
 - 15.1 供給者関係における情報セキュリティ
 - 15.2 供給者のサービス提供の管理
- 16 情報セキュリティインシデント管理
 - 16.1 情報セキュリティインシデントの管理及びその改善
- 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
 - 17.1 情報セキュリティ継続
 - 17.2 冗長性
- 18 順守

附属書 A 電気通信事業者のための拡張管理策集

- TEL. 9 アクセス制御
 - TEL. 9.5 ネットワークのアクセス制御
- TEL. 11 物理的及び環境的セキュリティ
 - TEL. 11.1 セキュリティを保つべき領域
 - TEL. 11.3 他組織の管理下におけるセキュリティ
- TEL. 13 通信のセキュリティ

- TEL. 13.1 ネットワークセキュリティ管理
- TEL. 18 順守
- TEL. 18.1 法的及び契約上の要求事項の順守

- 附属書 B ネットワークセキュリティのための補足的な手引き
- B.1 ネットワーク攻撃に対抗するためのセキュリティ対策
- B.2 ネットワーク輻輳に対するネットワーク対策

参考文献

JT-X1051

Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations

I.<Overview>

This standard provides guidelines for implementing information security controls in telecommunications organizations.

II.<References>

1. Relation with international standards and national standards

This standard is based on ITU-T Recommendation X.1051 (04/2016).

2. References

- ISO/IEC 27000, Information technology – Security techniques
 - Information security management systems – Overview and vocabulary.
- ISO/IEC 27002:2013, Information technology – Security techniques
 - Code of practice for information security controls.

3. Change history

Version	Date	Outline
1	Feb. 15, 2018	Published

4. Working Group that developed this standard

Version 1: TTC Security Working Group (WG2100)

III.<Table of contents>

1 Scope

2 References

3 Definitions and abbreviations

3.1 Definitions

3.2 Abbreviations

4 Overview

4.1 Structure of this Standard

4.2 Information security management systems in telecommunications organizations

5 Information security policies

6 Organization of information security

6.1 Internal organization

6.2 Mobile devices and teleworking

7 Human resource security

7.1 Prior to employment

7.2 During employment

7.3 Termination or change of employment

8 Asset management

- 8.1 Responsibility for assets
- 8.2 Information classification
- 8.3 Media handling
- 9 Access control
 - 9.1 Business requirement for access control
 - 9.2 User access management
 - 9.3 User responsibilities
 - 9.4 System and application access control
- 10 Cryptography
- 11 Physical and environmental security
 - 11.1 Secure areas
 - 11.2 Equipment
- 12 Operations security
 - 12.1 Operational procedures and responsibilities
 - 12.2 Protection from malware
 - 12.3 Backup
 - 12.4 Logging and monitoring
 - 12.5 Control of operational software
 - 12.6 Technical vulnerability management
 - 12.7 Information systems audit considerations
- 13 Communications security
 - 13.1 Network security management
 - 13.2 Information transfer
- 14 System acquisition, development and maintenance
 - 14.1 Security requirements of information systems
 - 14.2 Security in development and support processes
 - 14.3 Test data
- 15 Supplier relationships
 - 15.1 Information security in supplier relationships
 - 15.2 Supplier service delivery management
- 16 Information security incident management
 - 16.1 Management of information security incidents and improvements
- 17 Information security aspects of business continuity management
 - 17.1 Information security continuity
 - 17.2 Redundancies
- 18 Compliance

Annex A – Telecommunications extended control set

- TEL.9 Access control
 - TEL.9.5 Network access control
- TEL.11 Physical and environmental security
 - TEL.11.3 Security under the control of other party
- TEL.13 Communications security

TEL.13.1 Network security management

TEL.18 Compliance

TEL.18.1 Compliance with legal and contractual requirements

Annex B – Additional guidance for network security

B.1 Security measures against network attacks

B.2 Network security measures for network congestion

Bibliography