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＞

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＞

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