

# 2017年度3Q標準案説明資料

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

一般社団法人情報通信技術委員会 (TTC)

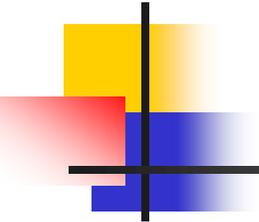
セキュリティ専門委員会

2017年12月6日

# 標準化対象と作成委員会

## セキュリティ専門委員会(WG2100)

新規対象のTTC標準	対応する国際標準
JT-X1051	ITU-T X.1051   ISO/IEC 27011 Information technology – Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations



# 本資料の内容

---

- ITU-T X.1051策定の背景
- 標準化理由
- JT-X1051の内容

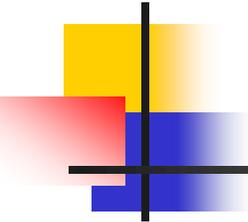
# ITU-T X.1051 | ISO/IEC 27011 策定の背景

## ■ ITU-T X.1051 | ISO/IEC 27011

(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規範)

本規格は、電気通信事業を行う組織が ISO/IEC 27002 に基づいた情報セキュリティ管理策の実装を支援するためのガイダンス文書である。

- 2008年にITUとISO/IEC JTC1の共同文書として策定、発行された。
- ISO/IEC 27002(情報セキュリティマネジメントの実践のための規範。ISMSを導入し運用する組織が、必要な管理策を実装するためのガイダンス)をベースとし、通信事業者特有の環境や事業形態を考慮し、セキュリティ管理策および実装のガイダンスを新たに規定。
- 2013年にISO/IEC ISO/IEC 27002 が全面改訂されたことに伴い、本勧告についての改訂プロジェクトがスタート。(ITU-T SG17及びISO/IEC JTC1/SC27/WG1)
- 2016年に改訂文書が発行された。



# 標準化の理由

---

- ISO/IEC 27001に基づく情報セキュリティマネジメントシステム (ISMS) は国内外において広く普及した認証スキームであり、その国内版であるJIS Q 27001とともに情報セキュリティを維持・推進する多くの企業が認証を取得している。
- またISMSを導入・実装する企業にとってガイダンスとなるISO/IEC 27002およびJIS Q 27002も、27001とともに多くの企業によりされている規格である。
- ISO/IEC 27002をベースとして、通信事業者向けの追加管理策を含むITU-T X.1051 | ISO/IEC 27011については同等の国内標準規格がなく、TTC標準化によりISMSを導入・実装する国内通信事業者にとって有益なガイダンスとなることが期待される。
- 上記を理由として、セキュリティ専門委員会では、JT-X1051の標準化を実施したい。なおJT-X1051は、ITU-T X.1051 | ISO/IEC 27011 の日本語版であり、内容の差分は無い。

# JT-X1051の内容

## ■電気通信事業者特有の管理策と実施の手引き

- JT-X1051では、ISO/IEC 27002 (JIS Q 27002) で定義されている114の管理策 (Control) のうちの、29の管理策に対して電気通信事業者特有の実施の手引きを定めている。また、JT-X1051独自の管理策として、14の電気通信事業者特有の管理策も定めている。

表1. JT-X1051 (X.1051 | ISO/IEC 27011) で独自に追加された管理策と実施の手引き

規格	管理策	電気通信特有の実施の手引き
ISO/IEC 27002	114	—
ITU-T X.1051   ISO/IEC 27011	128 (電気通信特有の <b>14</b> の管理策を含む)	<b>29</b>

- また、附属書B(非必須)には、参考情報としてサイバー攻撃に対するネットワーク対策の例や、輻輳対策などが記載されている。

# JT-X1051の例

## ■電気通信事業者特有の実施の手引きの例（抜粋）

### • 12.5.1 運用システムに関わるソフトウェアの導入

電気通信事業者は、運用システムへの深刻な損害のリスクを最小化するため、重要なシステムのアプリケーションやOSの変更は、十分に検証することが望ましい。アップグレードのような作業では、ロールバックの手順を含むことが望ましい。

### • 15.1.1 供給者関係のための情報セキュリティの方針

機微情報（個人情報や通話記録）へのアクセス権を供給者に与える場合は、供給者が適切に情報を保護できることを確実にすることが望ましい。

## ■電気通信事業者特有の管理策の例（抜粋）

### • TEL. 11.1.7 通信センターのセキュリティ

電気通信事業を提供するための交換設備のような電気通信設備が收容される通信センターの物理的セキュリティを設計し、開発し、適用することが望ましい。

### • TEL. 13.1.5 スпамへの対応

電気通信事業者はスパムへの対応方針を規定し、電子メール通信に適した良好かつ望ましい環境を確立するために適切な管理策を導入することが望ましい。