情報セキュリティの国際標準の動向

－ ISO/IEC 27002と外部委託関連の標準を中心に －

富士通株式会社 IT戦略本部
山下　真
ISO/IEC JTC 1/SC 27 WG 1 国内幹事、WG 4 国内委員

2013年1月25日

本日取り上げる標準

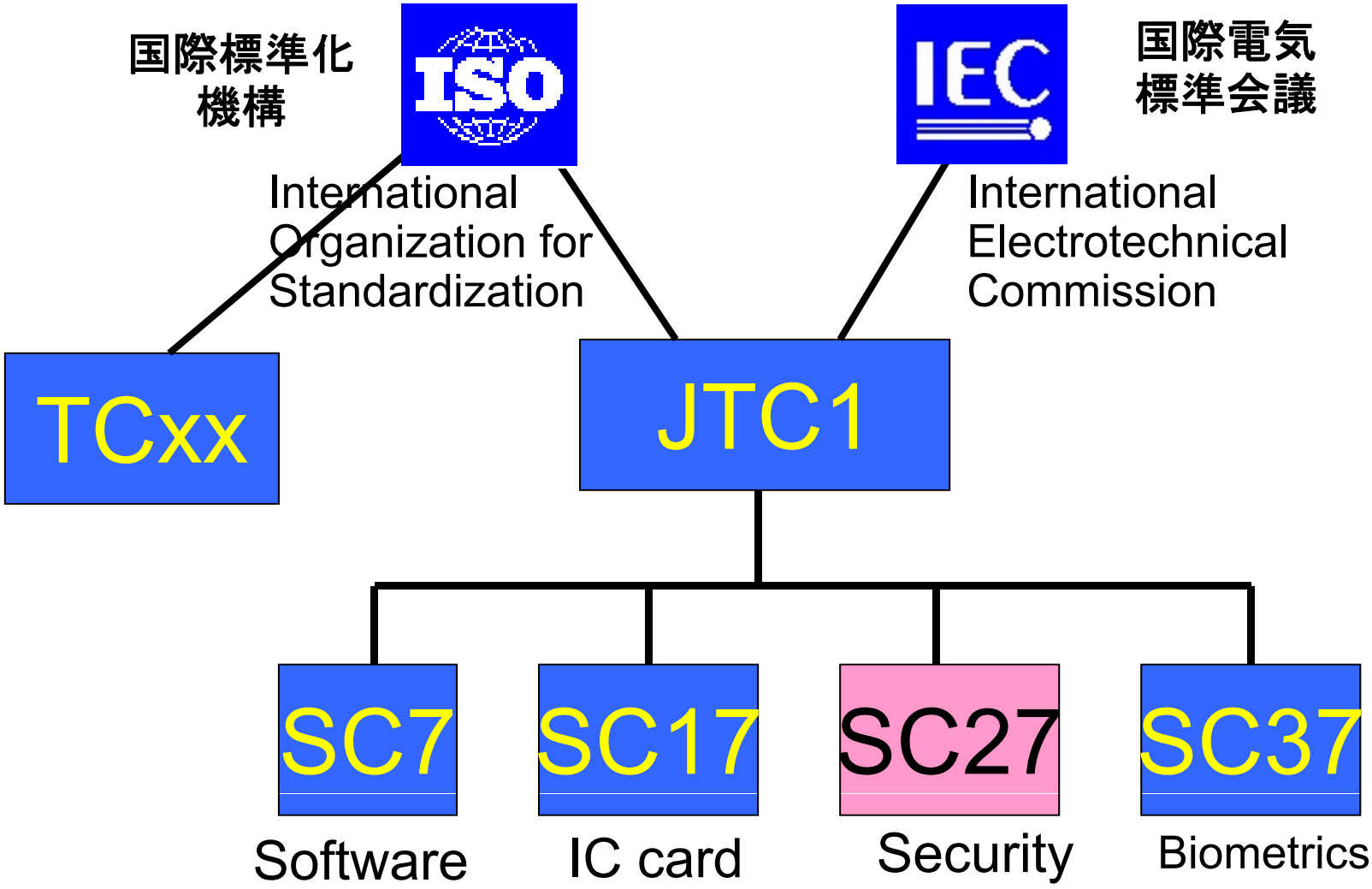
- SC 27/WG 1
  - ISO/IEC 27002 Information technology – Security techniques – Code of practice for information security controls
  - ISO/IEC 27017 Information technology – Security techniques - Guidelines on Information security controls for the use of cloud computing services based on ISO/IEC 27002
- SC 27/WG 4
  - ISO/IEC 27036 Information technology – Security techniques - Information security for supplier relationships

目次

1. 国際標準開発の体制
2. ISO/IEC 27000 ファミリーの体系
3. ISO/IEC 27002 の開発状況
4. クラウドコンピューティング関連標準の開発状況
   (1) ISO/IEC 27017
   (2) ISO/IEC 27036

国際標準開発の組織

- ISO/IEC JTC 1/SC 27 セキュリティ技術



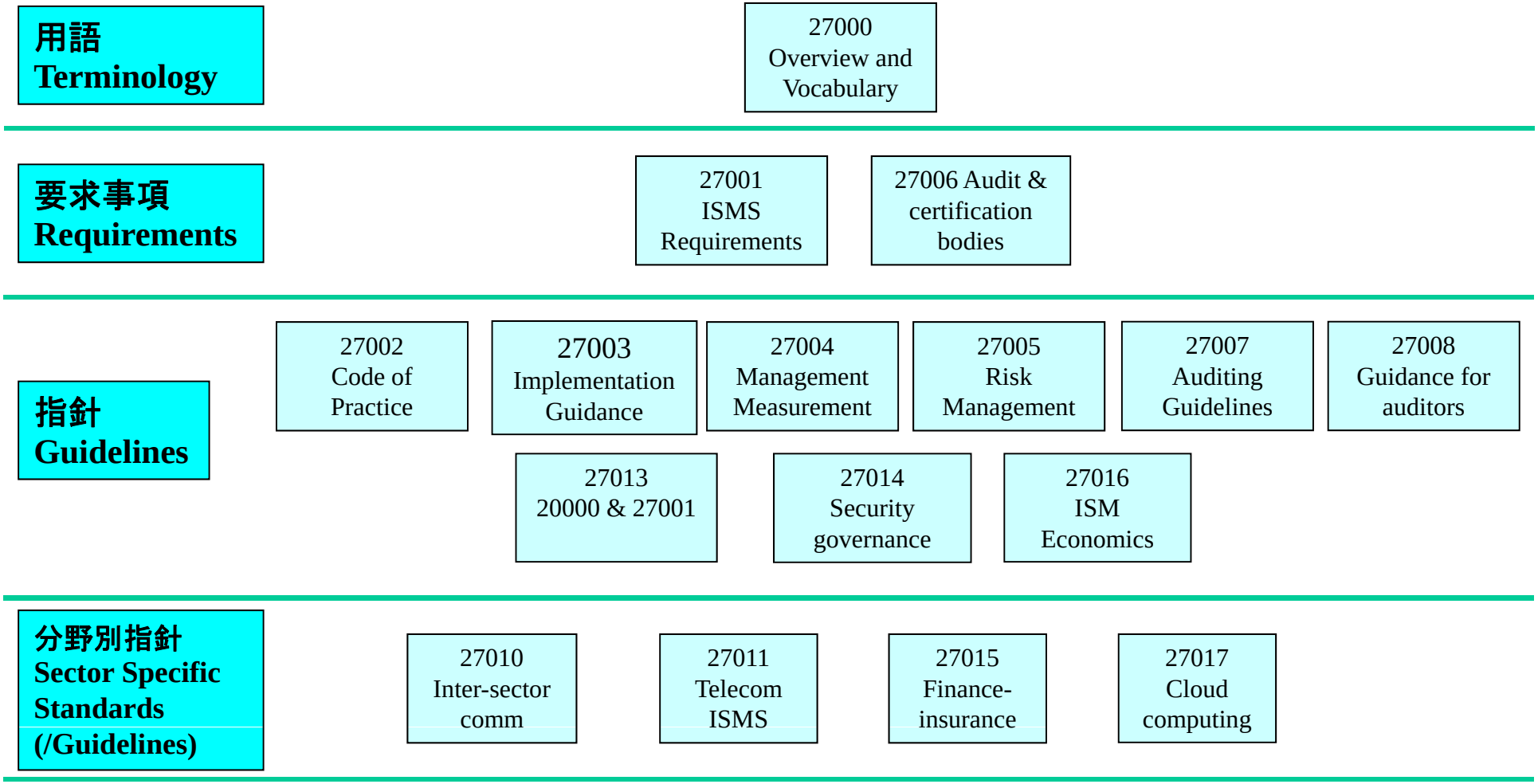
SC 27の構成

- ISO/IEC JTC 1/SC 27 セキュリティ技術
  - **WG 1: 情報セキュリティマネジメントシステム**
  - WG 2: 暗号とセキュリティメカニズム
  - WG 3: セキュリティ評価技術
  - **WG 4: セキュリティコントロールとサービス**
  - WG 5: アイデンティティ管理とプライバシー技術

ISO: International Organization for Standardization
IEC: International Electrotechnical Committee
JTC: Joint Technical Committee
SC: Sub Committee　　WG: Working group

目次

ISO/IEC 27000 ファミリーの体系



目次

ISO/IEC 27002 とは

1. 情報セキュリティの管理策（controls, 対策）集

   例：

   「すべての資産を明確に識別し、また、重要な資産すべての目録を作成し、維持することが望ましい」（2005年版、7.1.1）

   「システムの実務管理者及び運用担当者の作業は、記録することが望ましい。」（2005年版、10.10.4）

2. 幅広い管理策を収録した基本文献、
   2005年版では133件

3. 管理策ごとに、その実装方法の指針である「実施の手引（implementation guidance）」を提示

ISO/IEC 27002 改訂内容の概観

1. 2005年版を継承している。
   - 多くの管理策は、2005年版の管理策を継承している。標題と管理策が同一か、ほぼ同一。
2. 他方で、2005年以後の新しい動向や概念を取り入れている。
   - 14.2 開発・サポートプロセスにおけるセキュリティ
   - 15 供給者関係（supplier relationships）

ISO/IEC 27002 改訂内容の概観

3. 情報セキュリティマネジメントの指針を提供し、技術的な指針は他の標準に譲ることにした。
   - 2005年版 「11.4 Network access control」のいくつかの管理策は、27002から削除し、ISO/IEC 27033 に委ねる。
4. 陳腐化した記事を書き換え、又は削除している。
   - 2005年版「10.9 電子商取引」を書き換えた。
   - 2005年版「12.5.4 情報漏洩」を削除した。
5. 各所で記述を改善している。

ISO/IEC 27002 改訂の特徴　位置づけ

- 2005年版における本標準の位置づけを維持し、改訂版でこれを明文化している。「1 Scope」 第2段落より:

> この規格は、以下を意図する組織で使われるように作られている。
>
> a) 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を導入するプロセスにおいて管理策を選択する。
>
> b) 広く受け入れられている情報セキュリティの管理策を実施する。
>
> c) 組織が自身の情報セキュリティマネジメントの指針を開発する。

ISO/IEC 27002 箇条構成　改定版

改訂版
5 Security policies
6 Organization of information security
7 Human resource security
8 Asset management
9 Access control
10 Cryptography
11 Physical and environmental security
12 Operations security
13 Communications security
14 System acquisition, development and maintenance
15 Supplier relationships
16 Information security incident management
17 Information security aspects of business continuity management
18 Compliance

ISO/IEC 27002 改訂内容

- 2005年版
  「4. リスクアセスメント及びリスク対応」

  – 改訂版では、2005年版の本箇条を削除している。
  – ISO/IEC 27002の位置づけを、リスクアセスメントとリスク対応で選択の対象とする管理策一覧を提示するものとした。

  – リスクマネジメントの記事は、改訂版では、序文に、「管理策の選択」が残る。
  – ISMSにおいて、リスクマネジメントの要求事項と指針は、ISO/IEC 27001 及び ISO/IEC 27005 を参照する。

ISO/IEC 27002 改訂内容

- 2005年版
  「5.1.1 情報セキュリティ基本方針文書」
- 改訂版
  「5.1.1 情報セキュリティ方針」

  – 改訂版のこの管理策で、情報セキュリティ基本方針文書に加えて、場面ごとの方針文書も対象に含めた。

    例示:

    - 許可されるIT使用の方針
    - モバイルコンピューティングの方針
    - ネットワークセキュリティの方針
    - 外部委託の方針　等

ISO/IEC 27002 改訂内容

- 2005年版
  「10.9 電子商取引サービス」
  「10.9.1 電子商取引」「10.9.2 オンライン取引」「10.9.3 公開情報」
- 改訂版
  「14.1.2 公共ネットワーク上の業務処理サービスのセキュリティ」
  「14.1.3 業務処理サービスのトランザクションの保護」

  – 2005年版における「電子商取引」という用語・概念を、改訂版では一般化している。

ISO/IEC 27002 改訂内容

- 2005年版
  「11.2.3 利用者パスワードの管理 」
- 改定版
  「9.2.3 利用者の秘密認証情報の管理」

  – 改訂版では、秘密鍵などパスワード以外の手段も対象として一般化している。

ISO/IEC 27002 改訂内容

- 2005年版
  「6.2.3 供給者との契約におけるセキュリティの考慮」
  「10.2 第三者が提供するサービスの管理」
- 改訂版
  「15 供給者関係」

  – 外部委託、サプライチェーン等、外部の製品及びサービスの調達・利用に関する管理策を、改訂版では箇条15にまとめている。
  – 調達者の情報を供給者がアクセス又は管理すること等に伴う情報セキュリティリスクへの対応である。
  – 他の箇条が、組織が自ら管理する情報についての管理策であることと区別される。

ISO/IEC 27002 改訂内容

- 改訂版
  「17.2.1 情報処理施設の可用性」

  – 新規管理策である。

  – 「管理策
    情報処理施設は、可用性の要求に対応するために十分な冗長性を実装することが望ましい。」

  – 2005年版では、情報或いは情報を保有する資産の可用性に関係する管理策が体系的には見えにくかった。改訂版では、この管理策で可用性確保の対応を包括的に示している。

  – 情報処理施設の可用性確保は、事業継続管理の一部でもあるため、本管理策が箇条17に置かれている。

ISO/IEC 27002 改訂想定スケジュール

- 2012年11月　Draft International Standard (DIS)
- 2013年5月　Final Draft International Standard (FDIS)
- 2013年秋　International Standard 出版
- その後半年から1年程度でJIS規格を出版

上記スケジュールは、ISO/IEC 27001と同じ

目次

1. 国際標準開発の体制
2. ISO/IEC 27000 ファミリーの体系
3. ISO/IEC 27002 の開発状況
4. クラウドコンピューティング関連標準の開発状況

(1) ISO/IEC 27017

(2) ISO/IEC 27036

ISO/IEC 27017 開発の契機

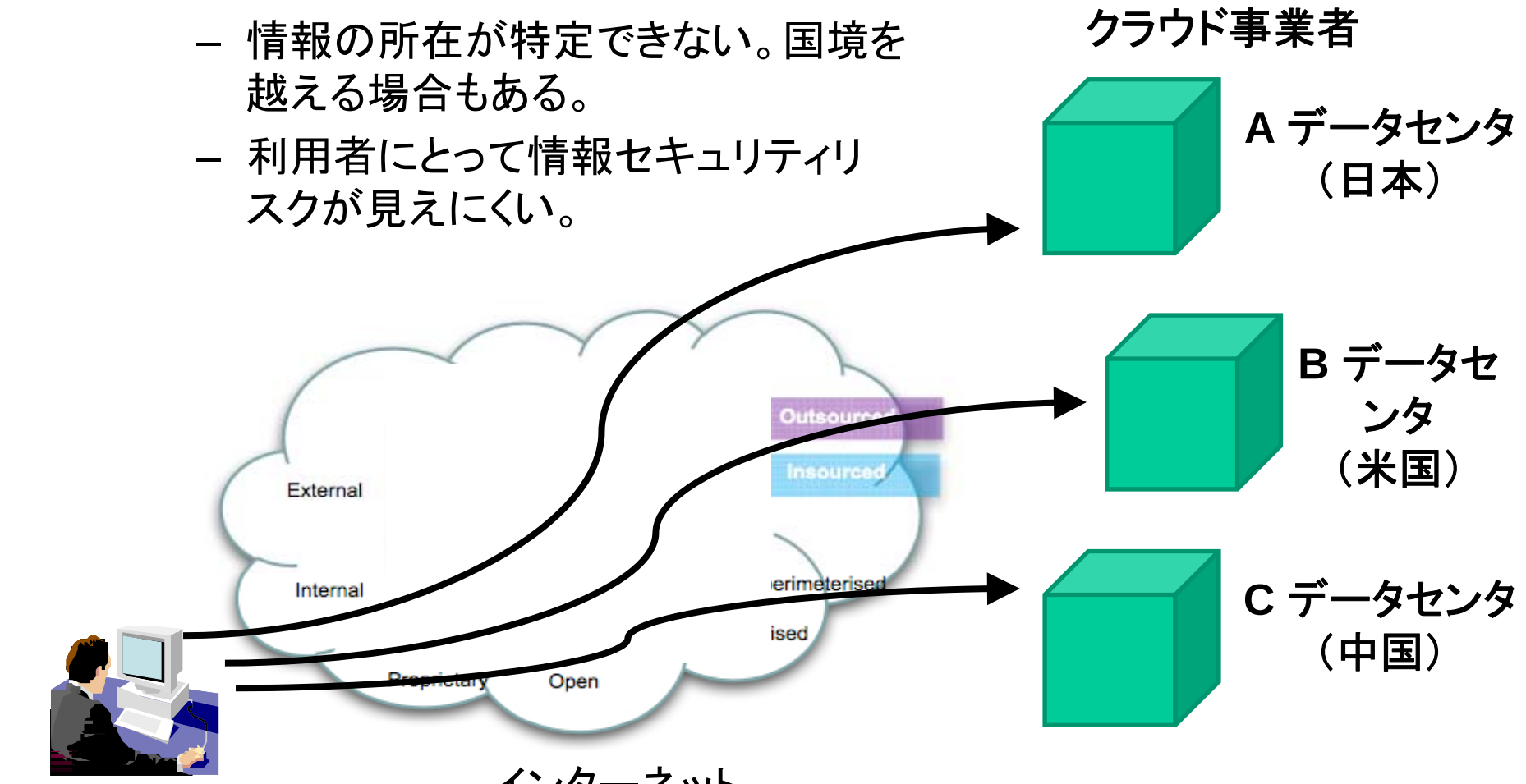
- 経済産業省において国内向け指針を開発
  - 「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」 2011年4月1日
    http://www.meti.go.jp/press/2011/04/20110401001/20110401001.html

- 経済産業省指針を基礎に、日本から国際SC 27/WG 1へクラウドコンピューティングにおける情報セキュリティの国際標準化を提案： 2010年10月

- 1st WD: 2011年5月、2nd WD : 2011年12月、3rd WD: 2012年6月

クラウドコンピューティングの環境と課題

- 課題
  - 利用者の情報がその組織の管理を離れる
  - 情報の所在が特定できない。国境を越える場合もある。
  - 利用者にとって情報セキュリティリスクが見えにくい。



G

ISO/IEC 27017 の構造

- ISO/IEC 27002 Code of practice for information security controls が前提

- ISO/IEC 27017 は、ISO/IEC 27002 に対して、クラウドコンピューティングに固有の事項を追加
  - 方法1: 固有の Control, Implementation guidance, Other information の組を追加
  - 方法2: 27002 の Control の下に、固有の Implementation guidance を追加
    - » 利用者向け
    - » 提供者向け

ISO/IEC 27017 の内容

- クラウド利用者向けImplementation guidance の例

  – “Monitoring and review of supplier services”

    [27002のImplementation guidanceに加えて]
    Cloud consumer should regularly monitor and review the services, reports and records provided by the cloud provider.

    クラウド利用者は、クラウド事業者から提供されるサービス、レポート及び記録を定常的に監視及びレビューすることが望ましい。

ISO/IEC 27017 の内容

- クラウド利用者向けImplementation guidance の例

  – “Security requirements analysis and specification”

    [27002のImplementation guidanceに加えて]
    Cloud consumer should specify the security requirements for the cloud service.

    クラウド利用者は、クラウドサービスに対するセキュリティ要求事項を定めることが望ましい。

ISO/IEC 27017 の内容

- クラウド利用者向けImplementation guidance の例

  – “Reporting information security events”

    [27002のImplementation guidanceに加えて]
    Cloud consumer should request cloud provider to report information security events which could affect cloud consumer’s environment to respond those events.

    クラウド利用者は、情報セキュリティ事象に対応するために、クラウド事業者に対してクラウド利用者の環境に影響を与えうる情報セキュリティ事象を報告することを求めることが望ましい。

ISO/IEC 27017 の内容

- クラウド事業者向け Implementation guidance の例

  – “Addressing security within supplier agreements”

    [27002のImplementation guidanceに加えて]
    Service delivery of the cloud provider should match the policy requirements of the cloud consumer and the legal requirements of the contract between the provider and the consumer of the cloud consumer’s physical jurisdiction.

    クラウド事業者は、サービスの提供において、クラウド利用者の方針に基づく要求事項と、事業者と利用者の契約における利用者の法域での法的要求事項に対応することが望ましい。

ISO/IEC 27017 の内容

- クラウド事業者向け Implementation guidance の例
  - “17.1.2 Implementing information security continuity”

[27002のImplementation guidanceに加えて]
Cloud provider should provide the following information to the cloud consumer to develop and implement business continuity plan covering cloud service:

a) disaster recovery plan;

b) availability ensuring measure such as system duplication.

クラウド事業者は、クラウド利用者に対して、クラウドサービスを対象とする事業継続計画を策定し実施するために、次の情報を提供することが望ましい。

a) 災害復旧計画;

b) システムの多重化のような対策を確実にする可用性

目次

1. 国際標準開発の体制
2. ISO/IEC 27000 ファミリーの体系
3. ISO/IEC 27002 の開発状況
4. クラウドコンピューティング関連標準の開発状況
   (1) ISO/IEC 27017
   (2) ISO/IEC 27036

ISO/IEC 27036　供給者関係

- 標題
  - Information technology – Security techniques – Information security for supplier relationships
- 内容
  - 組織が製品やサービスを外部から調達する際の情報セキュリティリスクのマネジメントに関する指針
- ISO/IEC 27002 との関係
  - “15 Supplier relationships” を受けて詳細化
- 対象
  - 調達者 (acquirer) と 供給者 (supplier)
- 構成
  - マルチパート標準：　Part 1, Part 2, Part 3, Part 4

ISO/IEC 27036 の位置づけ (1/2)

- 組織における情報セキュリティとは、情報の機密性、完全性、可用性の維持
  - 情報を組織が自ら管理していることを一般に想定

- 調達に伴う情報セキュリティリスク
  - 供給者が組織の情報にアクセスする。
    - 例： 情報システムの運用を委託
  - 供給者の環境に組織の情報を預ける。
    - 例： クラウドコンピューティングの利用
  - 調達した製品が組織において情報セキュリティ事故の原因になりうる。
    - 例： 製品の脆弱性（情報セキュリティ上の弱点）

ISO/IEC 27036 の位置づけ (2/2)

- 供給者関係における情報セキュリティ対策
  1. 調達者による供給者の管理： 案件ごと
     - 供給者や製品・サービスの選定
     - 契約
     - 契約の履行
     - 契約履行の管理
     - 契約履行の保証
  2. 供給者が製品・サービスの提供において組織として実施する対策： 供給者の事業の基礎として

- ISO/IEC 27036 は、これらの管理についての指針を提供する。

ISO/IEC 27036 Part 1

- 標題：Overview and concepts
- 内容：
  - ISO/IEC 27036 の各パートの共通用語定義
  - Supplier relationship の概要
- 開発スケジュール
  - 現在、1st CD を終えて DIS を準備中
  - 2013年秋に出版される見込み

ISO/IEC 27036 Part 2

- 標題：Common requirements
- 内容：
  - Supplier relationship の共通の指針
  - 組織共通のプロセスと個別案件ごとのプロセス
  - システムのライフサイクルに関する標準 ISO/IEC 15288 の概念と章・節構成に準拠
- 開発スケジュール
  - 現在、1st CD を終えて DIS を準備中
  - 2013年秋に出版される見込み

ISO/IEC 27036 Part 3 (1/2)

- 標題：Guidelines for ICT supply chain security
- 内容：
  - ICTサプライチェーンにおける情報セキュリティの指針
  - Part 1 と Part 2 が前提
  - 個別案件ごとのプロセスと、組織共通のプロセス
  - システムのライフサイクルに関する標準 ISO/IEC 15288 の概念と章・節構成に準拠
- 開発スケジュール
  - 現在、1st CD を終えて DIS を準備中
  - 2013年秋に出版される見込み

ISO/IEC 27036 Part 3 (2/2)

- 課題と対応
  - ICTサプライチェーンの情報セキュリティリスク：多段の取引関係のため、調達する製品・サービスに関する情報セキュリティの実態把握と対策徹底が困難
    → 多段の調達・供給関係における上流供給者の管理についての指針を提示。
  - 情報セキュリティに閉じない渾然一体の安全確保を取り上げることになる側面
    → 上流での品質問題、事業継続の不備、信頼性不足、模倣品等の不正等も下流において情報セキュリティの脅威となる。

ISO/IEC 27036 Part 4

- 標題：Guidelines for security of cloud services
- 内容：
  - クラウドサービスにおける情報セキュリティの指針
  - Part 1 と Part 2 が前提
  - ISO/IEC 27017 が ISO/IEC 27002 同様マネジメントの視点での標準であるのに対し、ISO/IEC 27036 Part 4 は技術内容を盛り込む予定
- 2012年10月の会議（ローマ）での話題
  - クラウドコンピューティングの利用例（use cases）に基づく検討と記述
  - 個別案件ごとのライフサイクル採用 (Part 2の形式)
  - Cloud supply chain におけるリスク目標の導入　等

ISO/IEC 27036 Part 4

- 開発スケジュール
  - 現在、Preliminary Draft を終えて WD (Working Draft) を準備中
- 関係組織との協力
  - クラウドコンピューティング及びその情報セキュリティの標準化に関わる組織の協力を得て開発を進める。
    - ISO/IEC JTC 1/SC 38
    - ITU-T
    - CSA

まとめ

- ISO/IEC JTC 1/SC 27 において情報セキュリティ分野の国際標準を開発
- ISO/IEC 27002 の改定が進展し、2013年秋に出版される見込み、ISO/IEC 27001改定と同時
- クラウドコンピューティング関連でも、情報セキュリティの指針を示す国際標準を開発
  - ISO/IEC 27017： ISO/IEC 27002 を基礎とする指針
  - ISO/IEC 27036： 供給者関係における情報セキュリティ、特にPart 4でクラウドコンピューティング関連の指針を提示

ご静聴ありがとうございました。

富士通株式会社　IT戦略本部
山下　真

ISO/IEC JTC 1/SC 27 WG 1 国内幹事、WG 4 国内委員