Japan Information Security
Management Systems User Group

2019年度

JNSA　日本ISMS-UG

インプリメンテーション研究会

クラウドセキュリティ議論のスタートライン

<抜粋版>　現在公開可能な情報

小梁　康志（リコージャパン㈱）
日本ISMSユーザグループ

2019年12月4日

2. クラウドコンピューティングとは:ISO規格

- ISO規格でのクラウドコンピューティングの解説
  - セルフサービスのプロビジョニング及びオンデマンド管理を使いスケーラブルで弾力性のある共用可能な物理的又は仮想的なリソースへのネットワークアクセスを行うパラダイムである。 JIS X 9401:2016「6.1はじめに」より
  - クラウドコンピューティングは、進化しているパラダイムである。＜中略＞特徴を取り上げ解説するが＜中略＞特定の手法を規定する又は制限する意図はない。 JIS X 9401:2016「6.2主な特徴」 より

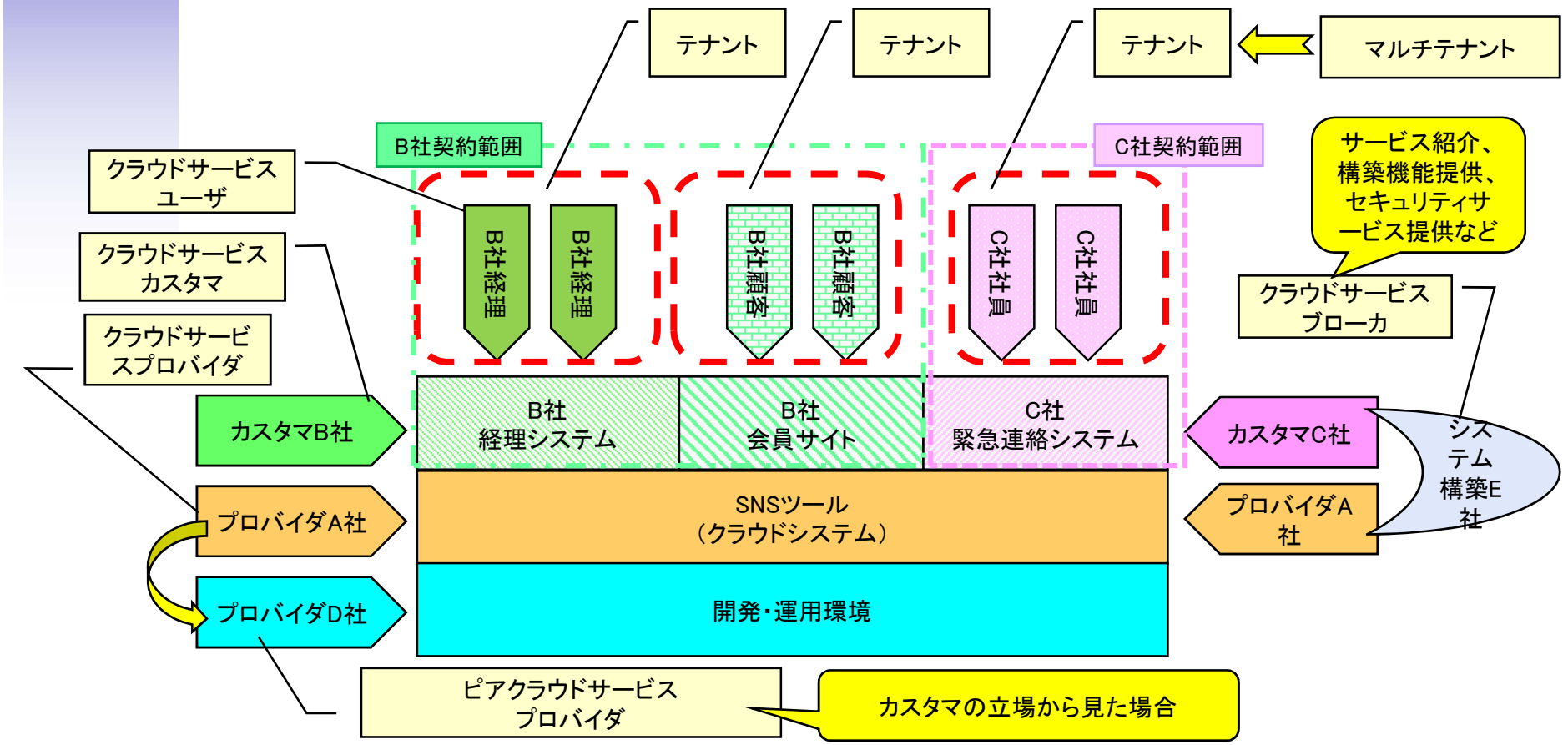
「クラウドコンピューティング」は進化しつつある概念である

人それぞれ、持っている認識が異なる可能性がある

JIS X 9401:2016 ＝情報技術　－クラウドコンピューティング－概要及び用語（ISO/IEC 17788:2014を翻訳して日本産業規格化したもの）

6．最小限の用語説明図

- クラウドサービスに係る立場



JIS X 9401:2016 での定義

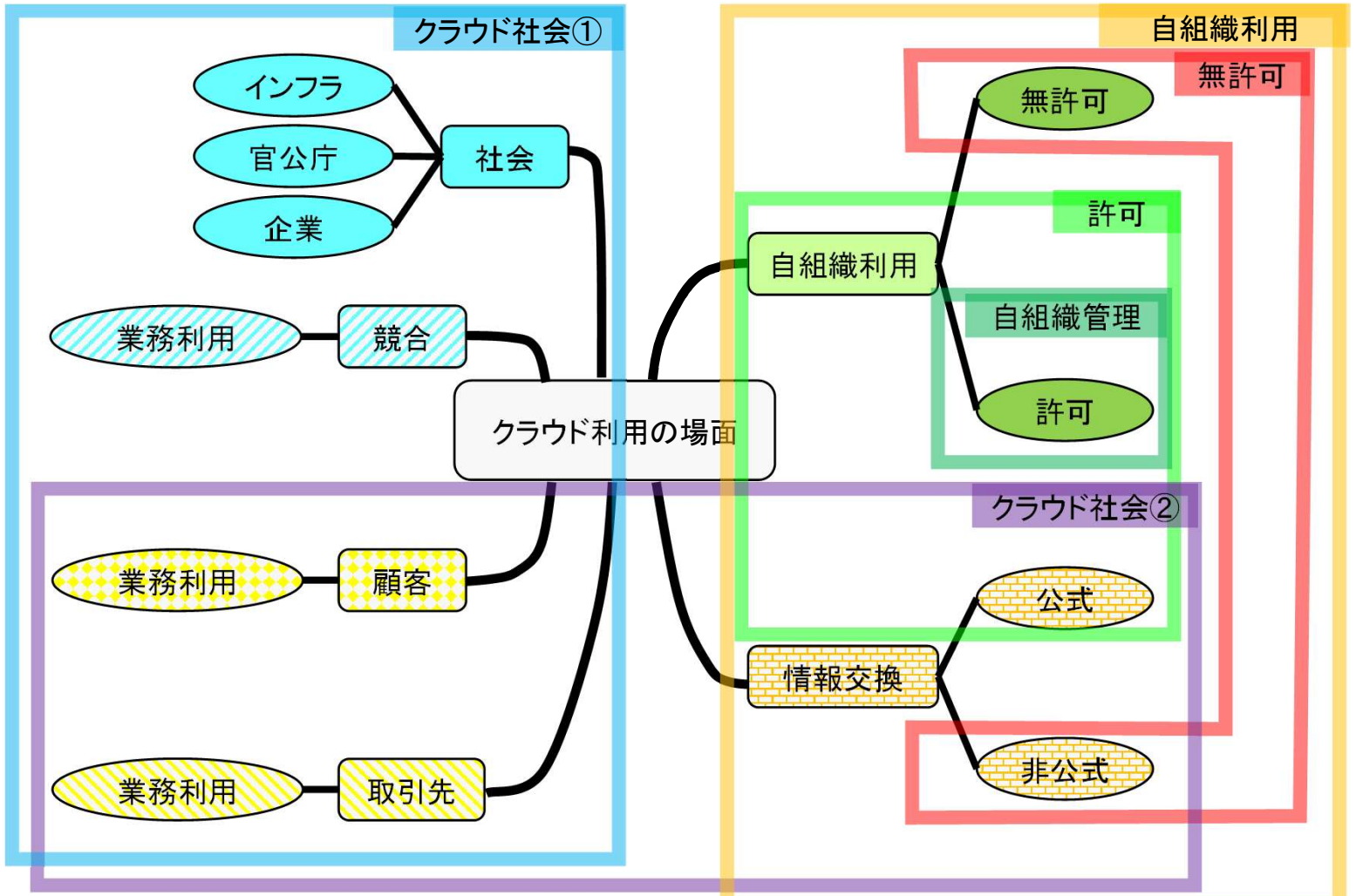
7.最小限の用語説明

- クラウドサービスカスタマ：クラウドサービスを使うために契約する組織。
- クラウドサービスプロバイダ：クラウドサービスを提供する組織。
- クラウドサービスユーザ：カスタマに関係してクラウドサービスを利用する者。カスタマの組織内の者の場合もあれば、会員であったり、顧客であったりする。
- クラウドサービスブローカ：カスタマとプロバイダの間を仲介する組織。
- テナント：特定のクラウドサービスを使うユーザーの集まり。
- マルチテナント：同じハードウエア環境を複数のテナントが共用している状態。共用はしていても、論理的に隔離されていることになっている。
- SaaS:Software as a Service　　アプリケーション機能提供サービス
- PaaS:Platform as a Service　　開発・運用環境提供サービス
- IaaS:Infrastructure as a Service　ハードウエア提供サービス
- パブリッククラウド　誰でもカスタマとして契約できるクラウドサービス。
- プライベートクラウド　特定の組織向けのクラウドサービス。

※赤文字部分は「クラウドサービス」を省略しています。

分かりやすい表現に変えています。正確な定義は規格書を確認してください。

2. リスク検討のための領域分割



3.クラウドリスクの領域

- 事業環境
  - クラウドを使うように誘導する圧力
  - クラウド利用が社会に広がっている状況
- クラウド利用
  - 取引先要求などで「使わざるを得ない」利用でのリスク
  - 自社で管理して利用する上でのリスク
  - 自社の情報資産が「管理できない状況でクラウド上にある」リスク

3つの領域で
リスク検討

クラウドがある社会のリスク

自組織管理上のリスク

無許可利用のリスク

領域によって、「考慮すべきリスク」「考慮の前提」が異なる

1. クラウドリスクの検討

●ENISA (European Network and Information Security Agency)2009年発表

「情報セキュリティに関わる利点、リスクおよび推奨事項」

◆35の「リスク」、53の「ぜい弱性」、23の「影響を受ける資産」を記述

https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

◆IPAによる翻訳版

https://www.ipa.go.jp/security/publications/enisa/documents/Cloud%20Computing%20Security%20Risk%20Assessment.pdf

●JASA(Japan Information Security Audit Association)

ENISAの発表を受けて「クラウド管理基準」との関連付けを行って「クラウドサービスにおけるリスクと管理策に関する有識者による検討結果　2011年度版」として公表

http://jcispa.jasa.jp/downloadf/pdf2012/2012_cloud_doc04.pdf

2.ENISA35リスク＋JASA追加2リスク

No.	ポリシーと組織関連のリスク
R.1	ロックイン
R.2	ガバナンスの喪失
R.3	コンプライアンスの課題
R.4	他の共同利用者の行為による信頼の喪失
R.5	クラウドサービスの終了または障害
R.6	クラウドプロバイダの買収
R.7	サプライチェーンにおける障害

No.	技術関連のリスク
R.8	リソースの枯渇（リソース割当の過不足）
R.9	隔離の失敗
R.10	クラウドプロバイダ従事者の不正－特権の悪用
R.11	管理用インタフェースの悪用（操作、インフラストラクチャアクセス）
R.12	データ転送途上における攻撃
R.13	データ漏えい（アップロード時、ダウンロード時、クラウド間転送）
R.14	セキュリティが確保されていない、または不完全なデータ削除
R.15	DDoS攻撃（分散サービス運用妨害攻撃）
R.16	EDoS攻撃（経済的な損失を狙ったサービス運用妨害攻撃）
R.17	暗号鍵の喪失
R.18	不正な探査またはスキャンの実施
R.19	サービスエンジンの侵害
R.20	利用者側の強化手順と、クラウド環境との間に生じる矛盾

No.	法的なリスク
R.21	証拠提出命令と電子的証拠開示
R.22	司法権の違いから来るリスク
R.23	データ保護に関するリスク
R.24	ライセンスに関するリスク

No.	クラウドに特化していないリスク
R.25	ネットワークの途絶
R.26	ネットワークの管理（ネットワークの混雑、接続ミス、最適でない使用）
R.27	ネットワークトラフィックの改変
R.28	特権の（勝手な）拡大
R.29	ソーシャルエンジニアリング攻撃（なりすまし）
R.30	運用ログの喪失または改ざん
R.31	セキュリティログの喪失または改ざん（フォレンジック捜査の操作）
R.32	バックアップの喪失、盗難
R.33	構内への無権限アクセス（装置その他の設備への物理的アクセスを含む）
R.34	コンピュータ設備の盗難
R.35	自然災害

JASA追加リスク
H01:リソース・インフラの高集約によるインシデントの影響の拡大
H02:仮想／物理の設計・運用の不整合

ENISA「情報セキュリティに関わる利点、リスクおよび推奨事項(2009年版IPA翻訳)」および
「クラウドサービスにおけるリスクと管理策に関する有識者による検討結果」から抜出し

1.情報セキュリティ管理の規格

●一般的な情報セキュリティ

- JIS Q 27001(ISO/IEC27001)
  - ■ISMS認証の認証基準
- JIS Q 27002(ISO/IEC27002)
  - ■27001を実装する際の手引書

●クラウドセキュリティ

- JIS Q 27017(ISO/IEC27017)
  - ■27002にクラウドセキュリティの観点を加えたもの
  - ■管理策が7つ追加され、44項目の手引きが追加されている

JIS

情報技術-セキュリティ技術-JIS Q 27002に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範

JIS Q 27017:2016

日本では、2016年から「ISMSクラウドセキュリティ認証」の仕組みが動いている。

2.クラウドセキュリティのガイドライン類

それぞれ最新版を探すよう
お願いいたします

- 政府
  - 総務省　クラウドサービスを利用する際の情報セキュリティ対策
    http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/admin/15.html
  - 総務省　クラウドサービス提供における　情報セキュリティ対策ガイドライン(第2版)
    http://www.soumu.go.jp/main_content/000566969.pdf
  - 総務省　クラウドサービスの安全・信頼性に係る情報開示指針
    http://www.soumu.go.jp/menu_news/s-news/01ryutsu02_02000167.html
    http://www.soumu.go.jp/menu_news/s-news/01ryutsu02_02000216.html
- NPO
  - IPA クラウドサービス安全利用のすすめ
    https://www.ipa.go.jp/security/cloud/cloud_tebiki_handbook_V1.pdf

2.無許可利用のリスク

- 近年「野良クラウド」と呼ばれ話題になっている
  - 組織によって考え方は、まちまち

	情報システム部門承認	使用部門承認	承認なし
目的内利用	正規	野良？	野良
目的外利用	野良？	野良？	野良

ところで、取引先の担当者からから「無料のクラウドを使ってデータ交換しましょう」と言われたらどうしますか？

クラウドサービスの在り方が多様であるように野良クラウドも多様

- 「野良クラウド」のリスクと対策
  - この後の講演でご確認ください

ご清聴ありがとうございました