



ISO/IEC 27017:2015に基づく クラウドセキュリティの 構築のポイント

一般財団法人日本情報経済社会推進協会
ISMS適合性評価制度技術専門部会
主査 駒瀬 彰彦

2016年4月26日
<http://www.isms.jipdec.or.jp/>

クラウドセキュリティの構築のポイント

- 要求事項とは
 - 順守すべく規格、参照すべく規格
- 適用範囲の考え方
- リスクアセスメント・リスク対応の考え方
 - 適用宣言書の記載
- 内部監査の考え方
- その他の情報

要求事項について

- ▶ ISMSクラウドセキュリティ認証取得にあたり順守しなければならない要求事項とは？
- ▶ ISO/IEC27017:2015に基づくISMSクラウドセキュリティ認証に関する要求事項（文書番号:JIP-ISMS517-1.0）に記載されている4章の基本的要件のこと

要求文章の構成

本文

序文

1. 概要
2. 引用規格
3. 用語及び定義
4. 基本的要件

参考A

- A.1 考慮事項
- A.2 クラウドセキュリティにおける適用範囲
の考え方
- A.3 クラウドセキュリティにおける
リスクアセスメント・リスク対応
- A.4 適用宣言書 (SoA)



基本的要件について

▶ 構成

- 本要求事項の項番
- タイトル
- JIS Q 27001の項番（箇条）のどこに相当する追加要求なのかの記載
- 詳細

基本的要件の詳細

- ▶ 大別すると以下の3つが要求事項である
 - 適用範囲
 - ISO/IEC 27017の規格に沿ったクラウド情報セキュリティ対策の実施
 - 情報セキュリティリスクアセスメント
 - 情報セキュリティリスク対応
 - 内部監査



適用範囲について（1/2）

4.1 クラウドサービスを含む情報セキュリティマネジメントシステムの適用範囲の決定【JIS Q 27001の4.3】

組織は、クラウドサービスを含めたISMSの適用範囲を定めるために、その境界及び適用可能性を決定しなければならない。

クラウドサービスを含めたISMSの適用範囲は、クラウドサービス名を含む文書化した情報として利用可能な状態にしておかなければならない。

適用範囲を定める際、クラウドサービスプロバイダが自らのサービスを提供するに当たり、別のクラウドサービスを利用している場合は、クラウドサービスプロバイダ及びクラウドサービスカスタマの両方を適用範囲としなければならない。

注記：ISO/IEC27017の箇条4では、クラウドサービスプロバイダの情報セキュリティ管理の対象は、クラウドサービスカスタマの情報セキュリティ対策のための情報提供や機能提供を含むものと規定されている。これに従い、クラウドサービスプロバイダは、リスクアセスメントの範囲にクラウドサービスカスタマとの関係を含めたリスク対応を検討することが必要である。

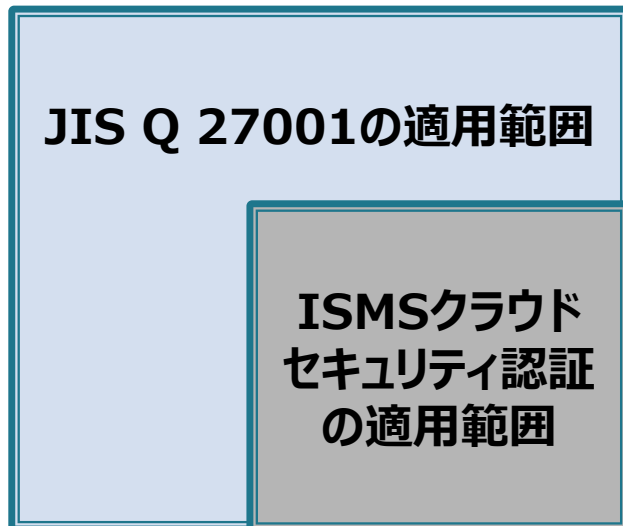
関連する参考項目： A.2 クラウドセキュリティにおける適用範囲の考え方



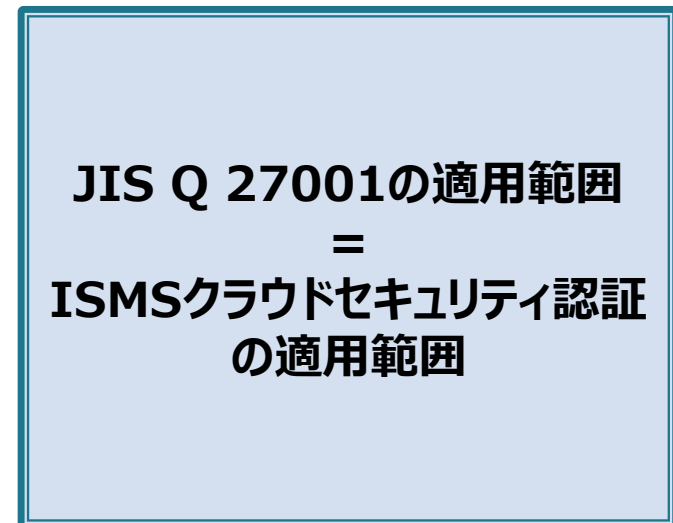
適用範囲について(2/2)

ISMSクラウドセキュリティ認証は、JIS Q 27001認証を前提としており、適用範囲は、次の2つの範囲のどちらかとなる。

① JIS Q 27001の範囲の一部



② JIS Q 27001の範囲と同じ



ISO/IEC 27017の規格に沿ったクラウド 情報セキュリティ対策の実施について

4.2 ISO/IEC 27017の規格に沿ったクラウド情報セキュリティ対策の実施

・4.2.1 情報セキュリティリスクアセスメント【JIS Q 27001の6.1.2c）】

組織は、次の事項を行う情報セキュリティリスクアセスメントのプロセスを定め、適用しなければならない。

c) 次によって情報セキュリティリスクを特定する。

1) ISMSの適用範囲内におけるクラウドサービスに関する情報の機密性、完全性及び可用性の喪失に伴うリスクを特定するために、情報セキュリティリスクアセスメントのプロセスを適用する。

2) これらのリスク所有者を特定する。

関連する参考項目： A.3.1) ISO/IEC 27017の管理策を参照した、
リスクアセスメント・リスク対応



ISO/IEC 27017の規格に沿ったクラウド 情報セキュリティ対策の実施について

- ▶ A.3.1)を参考にしても、クラウド固有のリスクってなんだかわからない
- ▶ ISO/IEC 27017に記載があるの？
 - はい。 でも。。。。



ISO/IEC 27017について (4.1)

▶ ISO/IEC 27017

4.1 概要

この規格は、更に、**クラウドサービスの技術的及び運用上の特徴に伴うリスク（附属書B参照）**を低減するための、クラウドサービス固有の管理策、実施の手引き及び関連情報を提供する。

クラウドサービスカスタマ及びクラウドサービスプロバイダは、ISO/IEC 27002及びこの規格を、管理策及び実施の手引きを選択するために参照し、必要であればその他の管理策を追加することもできる。
このプロセスは、クラウドサービスが利用又は提供される組織及び事業の状況における、**情報セキュリティリスクアセスメント及びリスク対応の実施によって行うことができる。**

ISO/IEC 27017:2015 附属書B

▶ 【参照】

ISO/IEC 27017は情報セキュリティリスクアセスメント及び対応の取り組みに焦点を当てたものではない。

→ 附属書Bにクラウドサービスの適用及び利用におけるリスク源及びリスクの説明を含む参考文献のリストを記載する

※留意点

リスク源及びリスクはサービスの種類及び性質並びにクラウドコンピューティングの新技术に依じて変化することに留意

附属書B の活用 例1： ITU-TX.1601 (2014)

目次

ITU-T 勧告 X.1601 に基づく、クラウドコンピューティングの脅威について	1
1. はじめに	1
2. 勧告 X.1601 が想定するクラウドコンピューティングの参加者（エコシステム）	1
3. クラウドコンピューティングに対する直接的脅威	2
3.1 クラウド利用者（CSC）に対するセキュリティ上の脅威	2
3.1.1 データの棄損と漏えい	2
3.1.2 セキュリティが欠落している（Insecure）サービスアクセス	3
3.1.3 インサイダーの脅威	3
3.2 クラウド事業者(CSP)に対するセキュリティ上の脅威	3
3.2.1 認可されない管理上のアクセス	3
3.2.2 インサイダーの脅威	4

- ▶ ITU-T 勧告 X.1601 に基づく クラウドコンピューティングの脅威の解説 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使い方ガイド【抜粋版】平成 27 年 1 月 特定非営利活動法人 ASP・SaaS・クラウド コンソーシアム より（目次を抜粋）

附属書B の活用 例1： ITU-TX.1601 (2014)

4.	クラウドコンピューティングに対する間接的脅威	4
4.1	クラウド利用者の観点からみた間接的脅威（チャレンジ）（CSC）	4
4.1.1	責任の曖昧さ	4
4.1.2	信頼の欠如	5
4.1.3	ガバナンスの欠如	5
4.1.4	プライバシーの欠如	5
4.1.5	サービス利用不可	5
4.1.6	プロバイダーへのロックイン	6
4.1.7	知的所有権の不適切な流用	6
4.1.8	ソフトウェアの完全性の欠如	6
4.2	クラウド事業者の観点からみた間接的脅威（チャレンジ）（CSP）	6
4.2.1	責任の曖昧さ	6
4.2.2	共有環境	7
4.2.3	防御メカニズムの一貫性の欠如と相反（conflict）	7
4.2.4	法令適用上の相反（conflict）	7
4.2.5	システム進歩上のリスク	7
4.2.6	適切でないマイグレーションとインテグレーション	8
4.2.7	事業の継続停止	8
4.2.8	クラウドサービスパートナーへのロックイン	8
4.2.9	サプライチェーンのぜい弱性	8
4.2.10	ソフトウェアの依存性	9
4.3	クラウドサービスパートナーのセキュリティ上の間接的脅威（チャレンジ）（CSN）	9
4.3.1	責任の曖昧さ	9
4.3.2	知的所有権の誤った流用	9
4.3.3	ソフトウェアの完全性の欠如	9

附属書B の活用 例2：

Cloud Computing Security Risk Assessment:2009 ENISA

▶ ENISAとは

- European Network and Information Security Agency
 - 欧州ネットワーク情報セキュリティ機関
 - 2004年3月の欧州議会(460/2004)で承認され、2005年9月よりクレタ島で運用を開始
 - ENISA came into being following the adoption of Regulation (EC) No 460 /2004 of the European Parliament and of the Council on 10 March 2004. Operations started in Crete in September 2005.
 - **Cloud Computing Security Risk Assessment–Novemberを2009年9月に発刊**
- 目的
 - EU内に高レベルのネットワーク及び必要な情報セキュリティを確実にする
 - ENISA's role is to ensure the high level of network and information security necessary in the EU.



ENISAのリスク評価基準

Cloud Computing Security risk Assessment November 2009, ENISA より引用

- ▶ インシデントの発生頻度とビジネスへの影響を考慮して、クラウドについて分析
- ▶ **ISO/IEC 27005:2008**のリスク値マトリクスを利用

※
クラウド固有リスク
の紹介であって、
RA手法を紹介
しているものではない

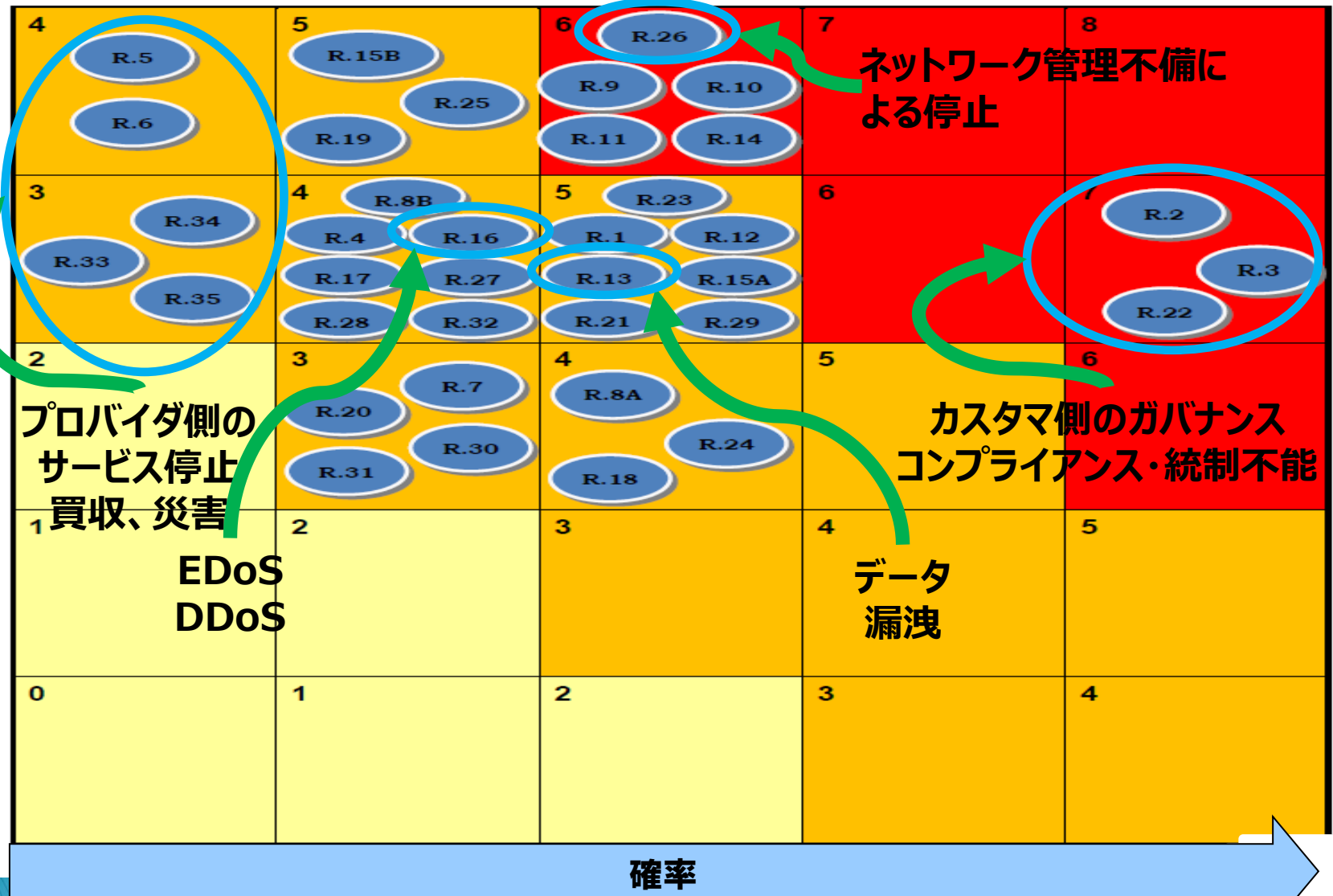
Likelihood of incident scenario		Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

We have based the estimation of risk levels on ISO/IEC 27005:2008 (10).

※ ISO/IEC 27005:2008を参照したリスク値のマトリクスを利用しているため、リスクアセスメント手法という意味では、
「ISMSユーザーズガイド--リスクマネジメント編-」を参照されたい

リスク評価分布

Cloud Computing Security risk Assessment November 2009, ENISA より引用





組織関連リスク

Cloud Computing Security risk Assessment November 2009, ENISA より引用
仮訳：株式会社アズジェント

方針群と組織関連のリスク

- ▶ **R1 LOCK-IN** ロックイン （閉鎖的なサービス（各クラウドプロバイダにおけるデータフォーマットの互換性が乏しいことから、単一プロバイダしか利用できない））
- ▶ **R2 LOSS OF GOVERNANCE** ガバナンスの喪失 （IaaS : VH, SaaS:L）
- ▶ **R3 COMPLIANCE CHALLENGES** コンプライアンスの課題
- ▶ **R4 LOSS OF BUSINESS REPUTATION DUE TO CO-TENANT ACTIVITIES**
他の共同利用者の行為による信頼の喪失
- ▶ **R5 CLOUD SERVICE TERMINATION OR FAILURE** クラウド・サービスのサービス終了または障害
- ▶ **R6 CLOUD PROVIDER ACQUISITION** クラウドプロバイダの買収
- ▶ **R7 SUPPLY CHAIN FAILURE** サプライ・チェーンにおける障害



技術関連リスク

Cloud Computing Security risk Assessment November 2009, ENISA より引用

仮訳：株式会社アズジェント

技術関連のリスク

- ▶ **R8** RESOURCE EXHAUSTION (UNDER OR OVER PROVISIONING) リソースの枯渇（不足/過剰）
- ▶ **R9** ISOLATION FAILURE 隔離の失敗（独立性（サービスの共有による）の問題）
- ▶ **R10** CLOUD PROVIDER MALICIOUS INSIDER - ABUSE OF HIGH PRIVILEGE ROLES
クラウドプロバイダ従事者の不正 - 特権の悪用 濫用
- ▶ **R11** MANAGEMENT INTERFACE COMPROMISE (MANIPULATION, AVAILABILITY OF INFRASTRUCTURE) 管理用インターフェースの悪用（操作、インフラストラクチャアクセス）
- ▶ **R12** INTERCEPTING DATA IN TRANSIT データ転送途上における攻撃
- ▶ **R13** DATA LEAKAGE ON UP/DOWNLOAD, INTRA-CLOUD データ漏洩（アップロード時、ダウンロード時、クラウド間転送）
- ▶ **R14** INSECURE OR INEFFECTIVE DELETION OF DATA 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
- ▶ **R15** DISTRIBUTED DENIAL OF SERVICE (DDOS) DDoS攻撃(分散サービス運用妨害)
- ▶ **R16** ECONOMIC DENIAL OF SERVICE (EDOS) EDOS攻撃(経済的損失を狙うサービス運用妨害)
- ▶ **R17** LOSS OF ENCRYPTION KEYS 暗号かぎの喪失
- ▶ **R18** UNDERTAKING MALICIOUS PROBES OR SCANS 不正な探査またはスキャンの実施
- ▶ **R19** COMPROMISE SERVICE ENGINE サービスエンジンの侵害
- ▶ **R20** CONFLICTS BETWEEN CUSTOMER HARDENING PROCEDURES AND CLOUD ENVIRONMENT カスタマー側の強化手順と、クラウド環境との間に生じる矛盾



法的リスク

Cloud Computing Security risk Assessment November 2009, ENISA より引用
仮訳：株式会社アズジェント

法的リスク

- ▶ **R21** SUBPOENA AND E-DISCOVERY 証拠提出命令と電子的証拠開示
- ▶ **R22** RISK FROM CHANGES OF JURISDICTION 司法権の違いから来るリスク
- ▶ **R23** DATA PROTECTION RISKS データ保護に関するリスク
- ▶ **R24** LICENSING RISKS ライセンスに関するリスク



共通的なリスク

Cloud Computing Security risk Assessment November 2009, ENISA より引用

仮訳：株式会社アズジェント

クラウドに限定していないリスク

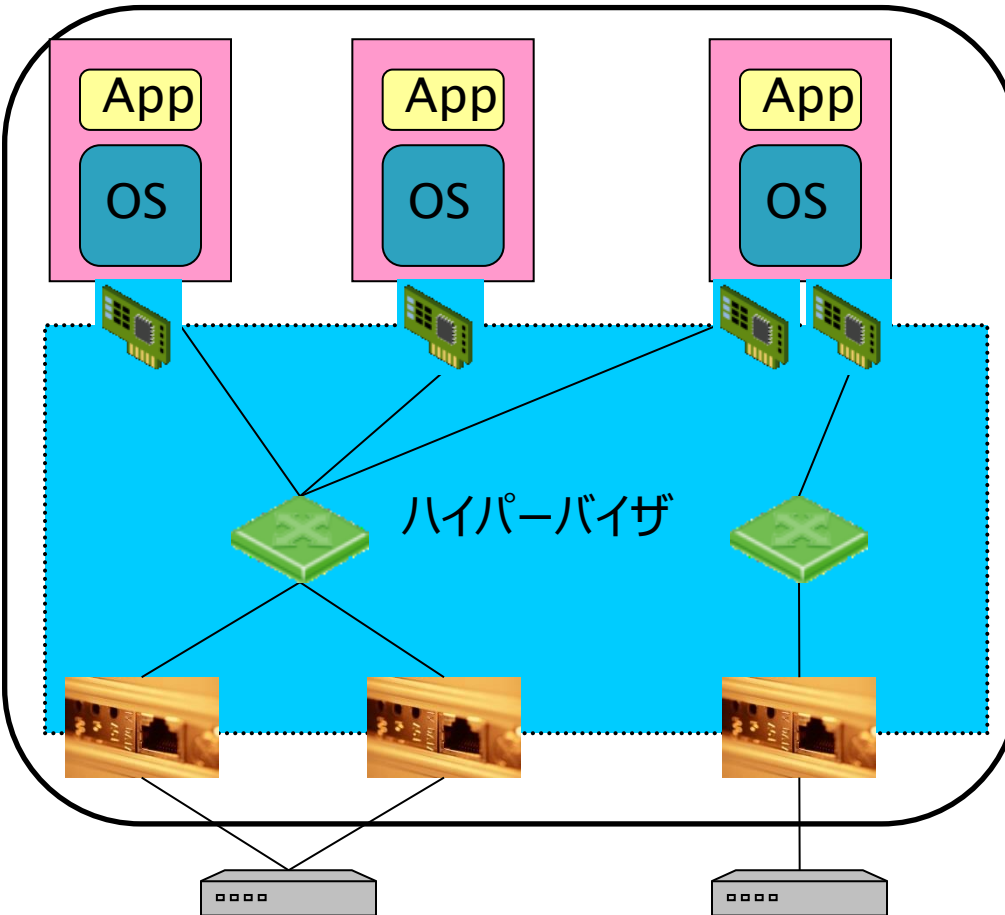
- ▶ **R25** NETWORK BREAKS ネットワークの途絶
- ▶ **R26** NETWORK MANAGEMENT (IE, NETWORK CONGESTION / MIS-CONNECTION / NON-OPTIMAL USE) ネットワークの管理(例、輻輳/誤接続/不適切な利用)
- ▶ **R27** MODIFYING NETWORK TRAFFIC ネットワークトラフィックの改変
- ▶ **R28** PRIVILEGE ESCALATION 権限奪取 (特権の勝手な拡大)
- ▶ **R29** SOCIAL ENGINEERING ATTACKS (IE, IMPERSONATION)
ソーシャルエンジニアリング攻撃
- ▶ **R30** LOSS OR COMPROMISE OF OPERATIONAL LOGS ログの滅失又は漏洩
- ▶ **R31** LOSS OR COMPROMISE OF SECURITY LOGS (MANIPULATION OF FORENSIC INVESTIGATION) セキュリティ・ログの滅失又は改ざん
- ▶ **R32** BACKUPS LOST, STOLEN バックアップの毀損、盗難
- ▶ **R33** UNAUTHORIZED ACCESS TO PREMISES (INCLUDING PHYSICAL ACCESS TO MACHINES AND OTHER FACILITIES) 構内への無権限アクセス(装置やその他の施設への物理的アクセスを含む)
- ▶ **R34** THEFT OF COMPUTER EQUIPMENT コンピュータ施設の盗難
- ▶ **R35** NATURAL DISASTERS 自然災害

技術関連リスク： 仮想化環境におけるリスク ～既存ISMS認証 & クラウド認証～

仮想化環境

サーバ・ハードウェア

仮想サーバ内にLAN が構成される



仮想マシン(VM)

物理環境でのサーバにあたる部分。OSをインストールしてアプリケーションを実行する

仮想NIC

仮想マシンとハイパーバイザ（仮想化カーネル）との間のイーサネット・フレームの送受信を担う

仮想スイッチ

物理環境でのレイヤー2スイッチにあたる部分。ハイパーバイザに内包されている。仮想化環境でのネットワークを柔軟にするための様々な機能を提供する

物理NIC

NIC Teamsなどによって冗長化できる。仮想化環境では物理NICが多数必要になりやすい

物理スイッチ

仮想化環境でも基本的には物理環境と同様の役割（フレーム処理やVLAN）を担う

※ NIC: network Interface card

※ APP:アプリケーション

仮想化環境におけるリスク

職務分掌の欠如

独立した管理者の下、アクセス管理を実施しなければ、様々な権限をもつ管理者が仮想化環境全体を制御可能となる。これにより、情報漏洩や各種妨害により企業に多大な損害を与える危険が生じる。

仮想化のセキュリティリスク

- ・仮想化環境での最大のリスクは、管理を行っている特権パーティションからすべてのVMへアクセスした際、多数のクリティカルなサービスが制御可能となるため、脆弱性の単一障害点となりうる。ハイパーバイザ型の場合、サービスコンソールに侵入されてしまうと管理対象下のあらゆる仮想化セッションがリスクにさらされることになる。
- ・仮想化環境では、各専用VMイメージによるサービスの分離により、同じサーバ上で実行されるVMが、相手側の攻撃には影響されないと思われがちであるが、ネットワーク帯域、ディスク領域、CPUリソースなどは共有されるため、ウィルス、不正アクセスなどにより、これらのリソースを大量消費すれば、他のサービスへ与える影響は大きい。

不十分な監査

企業は、特権ユーザを含めた各ユーザが、特権パーティションおよび各VM上で行った操作を追跡する必要がある。しかし、OSが装備する標準監査機能では不十分である。また、仮想化環境下では、特権パーティションや各VMをそれぞれに監視し監査するだけでなく、企業の規制要件遵守のもと、仮想化環境下全体の整合性を保つ必要がある。

仮想化サーバ構築の誤った考え方

仮想化サーバ

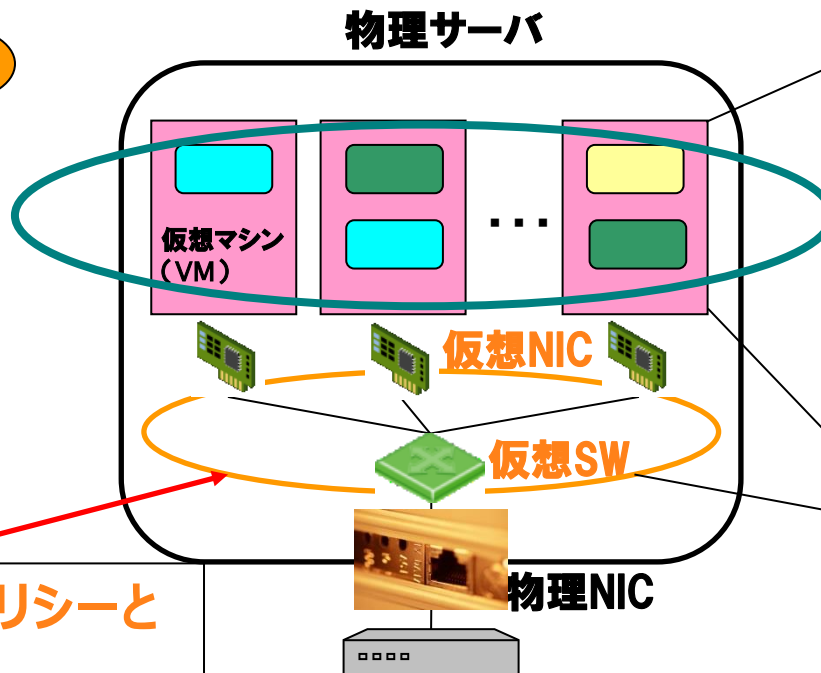
仮想化環境にうっかり適用すると
運用を誤ることがある

- ▶ 仮想化サーバはサーバなんだから、サーバ管理者が管理するんだよね
 - サーバ管理者
 - ・ サーバ管理者の責任範囲は、物理NIC－ 仮想NIC,OS,アプリケーションであり、その間のネットワークを含む
 - ネットワーク管理者
 - ・ ネットワーク管理者の責任範囲は、サーバーマシンの物理NICまでのネットワーク
- ▶ 問題点
 - 従来型のサーバ管理者は、通常ネットワーク（レイヤー2）に精通していない
 - ・ 冗長性や、VLANなどを意識して、設計することを得意としていない
 - サーバ管理者は、通常全てのアプリケーションに精通していない
 - ネットワーク管理者は、サーバー内に内在するネットワークの管理に至らない

仮想化サーバ構築の留意事項

- ▶ 1つの仮想システムコンポーネントに複数のアプリケーションやサービスが混在するモデルは、人的ミス、職務分掌の欠如に繋がる
- ▶ サーバ内部のネットワークが外部から見えないためトラブルを招きやすい

仮想化サーバー



APP1 VM

APP2 VM

APP3 VM



ネットワーク運用ポリシーとズレが生じやすい

理由：ネットワークに疎いサーバ管理者が、仮想サーバ内のネットワークを実装するため

複数のサービスなどを混在させると人的ミスが増加する。
また、権限が偏ることがある

13.1.3 ネットワークの分離

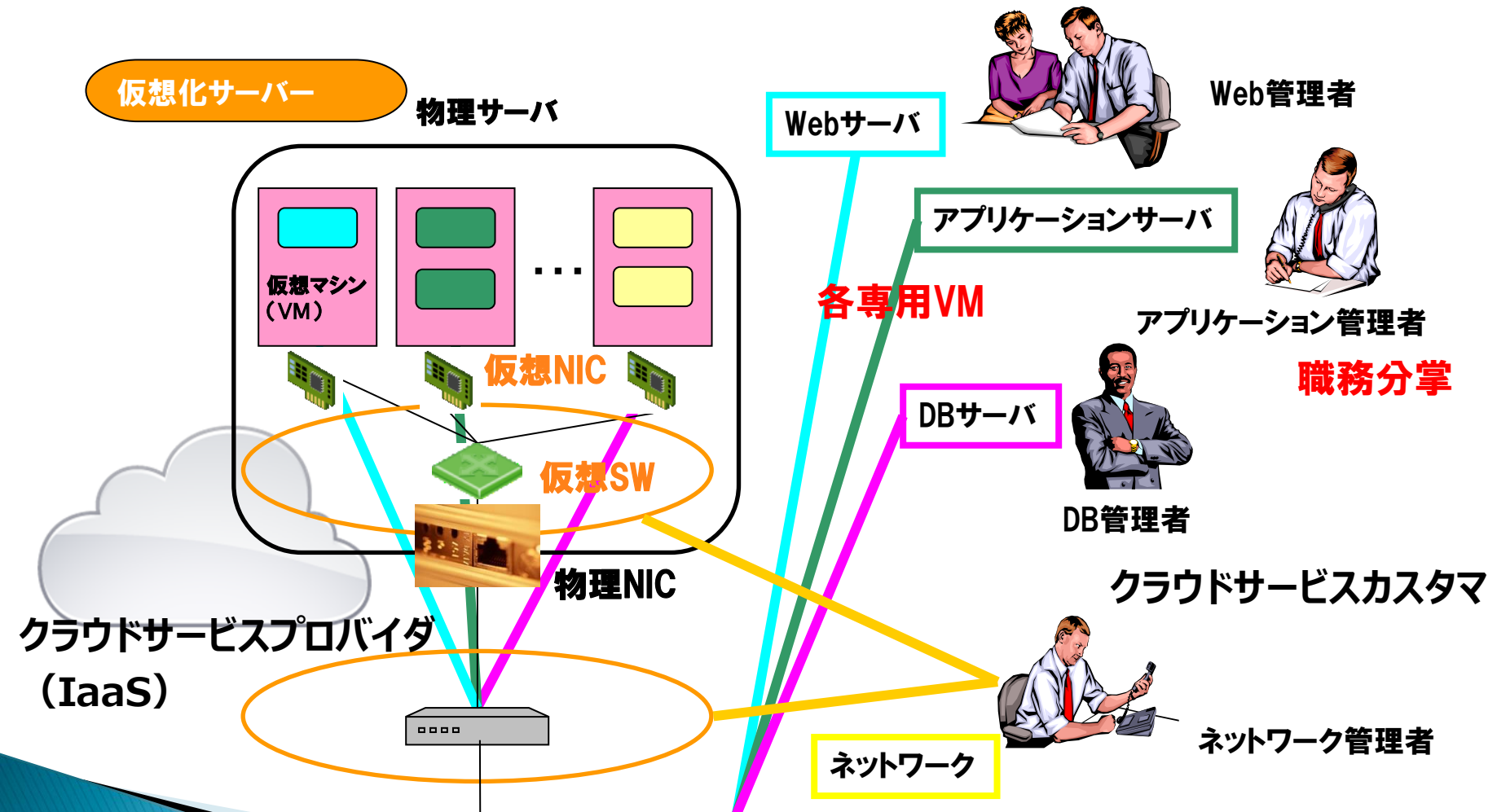
▶ JIS Q 27002 13.1.3 関連情報

ビジネスパートナーの関係が、情報処理施設及びネットワーク設備の相互接続又は共有を必要するものになりつつあることから、ネットワークが組織の境界を越えて拡張することも少なくない。

▶ ISO/IEC 27017 13.1.3

クラウドサービスカスタマ	クラウドサービスプロバイダ
クラウドサービスカスタマは、クラウドサービス共有環境において、テナントの分離を実現するためのネットワークの分離に関する要求事項を定義し、クラウドサービスプロバイダがその要求事項を満たしていることを検証することが望ましい。	クラウドサービスプロバイダは、次の場合においてネットワークアクセスの分離を確実にすることが望ましい。 – マルチテナンド環境におけるテナント間の分離 – クラウドサービスプロバイダ内部の管理環境とクラウドサービスカスタマのクラウドコンピューティング環境との分離 必要な場合には、クラウドサービスプロバイダは、クラウドサービスプロバイダが実施している分離を、クラウドサービスカスタマが検証することを助けることが望ましい。

13.1.3 ネットワークの分離



参考：PCI DSS V3.1

職務分掌：

(仮想環境)

各アプリケーション毎に仮想システムコンポーネントを分離し、管理者を設置する。ハイパーバイザ内のネットワーク管理は、従来のネットワーク管理者を設置する、または、協力を得ること。

各専用VMイメージによるサービスの分離：

PCI DSS V 3.1要件	テスト手順
2.2.1 同じサーバに異なったセキュリティレベルを必要とする機能が共存しないように、1つのサーバには、主要機能を 1つだけ実装する。（たとえば、Webサーバ、データベースサーバ、DNS は別々のサーバに実装する必要がある。） 注：仮想化テクノロジーを使用している場合は、1つの仮想システムコンポーネントに主要機能を 1つだけ実装する。	2.2.1a システムコンポーネントのサンプルを選択し、システム構成を調べて 1つのサーバに主要機能が 1つだけ実装されていることを確認する。 2.2.1.b 仮想テクノロジーが使用されている場合は、システム構成を調べて、1つの仮想システムコンポーネントまたはデバイスに主要機能が 1つだけ実装されていることを確認する。

Payment Card Industry (PCI)データセキュリティ基準
要件とセキュリティ評価手順 バージョン3.1 翻訳版（3.0を利用）

管理策：組織が自ら提供するか外部委託しているかを問わず、全てのネットワークサービスについて、セキュリティ機能、サービスレベル及び管理上の要求事項を特定しなければならない、また、ネットワークサービス合意書にも、これらを盛り込まなければならない JIS Q 27001:2014

The diagram illustrates a virtualized network architecture with the following components and connections:

- Physical Layer (Top):** Consists of four server types: Webサーバ (Web Server), 物理サーバ (Physical Server), アプリケーションサーバ (Application Server), and DBサーバ (Database Server).
- Virtual Layer (Middle):** Contains virtual machines (仮想マシン (VM)) and virtual network components:
 - 仮想NIC (Virtual Network Interface Card):** Connects each VM to its respective virtual switch.
 - 仮想SW (Virtual Switch):** Includes Internet v-switch, Intranet v-switch, Web v-switch, App v-switch, and DB v-switch.
- Physical Network (Bottom):** Includes a LAN cloud, an Internet cloud, and physical network interface cards (物理NIC) connecting the virtual switches to the physical network.
- Security and Management:**
 - セキュリティ機能 (Security Function):** Represented by a brick wall icon, indicating firewalls and other security measures.
 - ネットワーク (Network):** A central hub for network management.
 - ネットワーク管理者 (Network Administrator):** Shown as a person managing the network.
- Connections:** Red arrows indicate the flow of traffic and security policies from the physical servers through the virtual layer to the physical network and Internet.

ISO/IEC 27017の規格に沿ったクラウド 情報セキュリティ対策の実施について

4.2.2 情報セキュリティリスク対応【JIS Q 27001の6.1.3】

組織は、次の事項を行うために、情報セキュリティリスク対応のプロセスを定め、適用しなければならない。

- a) ISMSの適用範囲内におけるクラウドサービスのリスクアセスメントの結果を考慮して、適切な情報セキュリティリスク対応の選択肢を選定する。
- b) 選定した情報セキュリティリスク対応の選択肢の実施に必要な全ての管理策を決定する。
- c) 4.2.2b)で決定した管理策をJIS Q 27001の附属書A及びISO/IEC 27017に示す管理策と比較し、必要な管理策が見落とされていないことを検証する。
- d) 次を含む**適用宣言書**を作成する。
 - － 必要な管理策[4.2.2のb)及びc)参照]
 - － それらの管理策を含めた理由
 - － それらの必要な管理策を実施しているか否か
 - － JIS Q 27001の附属書A及びISO/IEC 27017に示す管理策を除外した理由

注記1：ISO/IEC 27017に示す管理策には、ISO/IEC 27017の本文に実施の手引が示されている管理策、及びISO/IEC 27017の附属書Aの管理策が含まれる。

注記2：クラウドセキュリティに基づくリスク分析の結果に基づいて、ISO/IEC 27017に記載されている実施の手引を参照し、クラウドサービス固有のリスクに対する管理策として、必要な事項を選択し、実施する。

注記3：ISO/IEC 27017に示す管理策は、クラウドサービスプロバイダ及びクラウドサービスカスタマに対する固有の管理策であるため、原則は全ての管理策の評価を実施することとなる。

但し、サービスの種類によって、管理策が存在しない場合には、適用除外することができる。

関連する参考項目： A.3.1) ISO/IEC 27017の管理策を参照した、
リスクアセスメント・リスク対応、A.3.2) 「**適用宣言書 (SoA)**」における
27017適用の記載方法 及び **A.4 適用宣言書**



適用宣言書について

- ▶ A.4 適用宣言書の例示を参考に、作成してください
- ▶ クラウドカスタマ/プロバイダのいずれかまたは両方を明記
- ▶ 上記を考慮し、ISO/IEC27017の実施の手引き及び附属書Aの管理策に対して実施
- ▶ 除外の理由などを明記

内部監査について

4.3内部監査【JIS Q 27001の9.2】

組織は、ISMS内のクラウドサービスが次の状況にあるか否かに関する情報を提供するために、あらかじめ定めた間隔で内部監査を実施しなければならない。

a) 次の事項に適合している。

- 1) ISMS に関して、組織自体が規定した要求事項
- 2) この規格の要求事項

b) 有効に実施され、維持されている。

注記1： 内部監査の一部として、第三者による独立したレビュー（外部監査など）の結果を利用することができる。

注記2： クラウドサービスプロバイダのコミットメント（クラウドサービスの提供にかかる情報セキュリティガバナンス及びマネジメントに関するコミットメント）が適正に実施されていることを確認することが望ましい。

関連する参考項目： A.1 考慮事項

ISO/IEC 27017 18.2.1 実施の手引き

内部監査について

- ▶ クラウドサービスに対する利用者の懸念
(他者にシステムの主要な部分を委ねているのに、)
 - システムの状態をリアルタイムに把握しにくい
 - 障害の原因が分からない
 - 説明責任が果たせない
- ▶ クラウドサービスに関わるセキュリティ情報伝達の課題
 - 利用者には、セキュリティ対策を理解するための基礎知識が必要となる
 - クラウド事業者が、多数の利用者に個別に説明することが難しい
- ▶ 必要な「利用者代表の目で確認して、結果を知らせてくれる」立場の人の必要性
 - 専門的な知識が分かる人に任せたい
 - 公正で的確な評価ができる人に任せたい



監査が必要



クラウドサービス



オンプレミス

特定非営利活動法人 日本セキュリティ監査協会
JASA-クラウドセキュリティ推進協議会 説明会資料参照より 2016年2月15日

どのような監査が求められるか

ISMSの一般的の内部監査

目的： 自身の対策の有効性の確認

水準： 経営者が求める水準

基準： 情報セキュリティ一般

監査人の力量： 経営者の期待に応える
評価能力



クラウドに必要な監査

目的： **提供する環境**での対策の有効性
確認

水準： **利用者**が求める水準
・公正さ
・クラウドの知識

基準： **クラウドに特化した**情報セキュリティ
基準
・事業者責任部分のセキュリティ対策
・利用者への支援
(情報・機能の提供)

監査人の力量： 客観的に評価された能力

クラウドセキュリティ監査制度
SOC 2、SOC3など

特定非営利活動法人 日本セキュリティ監査協会
JASA-クラウドセキュリティ推進協議会 説明会資料参照より 2016年2月15日



ISO/IEC 27017 18.2.1について

- ▶ 18.2.1 情報セキュリティの独立したレビュー
- ▶ クラウドサービスプロバイダは、クラウドサービスプロバイダが主張する情報セキュリティ管理策の実施を立証するために、クラウドサービスカスタマーに文書化した証拠を提供することが望ましい

その他の情報

JIPDEC発刊の参考情報

- ▶ ITSMSハンドブック
運用管理のお手本ISO/IEC 20000～事例から学ぼう～
「クラウドの時代の ITSMS編」
 - 制度は異なるものの、クラウドサービスの活用を中心に、どのように適用範囲を決定するかについて参考になる
- ▶ ISMSユーザーズガイド27001:2014(ISO/IEC 27001:2013)
対応--リスクマネジメント編--
 - リスクアセスメント手法を理解する際に役立つ
- ▶ 外部委託におけるISMS適合性評価制度の活用方法
－ JIS Q 27001:2014 対応 －
 - クラウドプロバイダを選択する際に役立つ



ISO/IEC27017の参考情報

ISO/IEC17789:2014 Information technology — Cloud computing
— Reference architecture

3 definition

- ▶ 3.2.5 cloud computing: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand. NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.
- ▶ 3.2.11 cloud service customer: Party (3.1.6) which is in a business relationship for the purpose of using cloud services (3.2.8). NOTE – A business relationship does not necessarily imply financial agreements.
- ▶ 3.2.15 cloud service provider: Party (3.1.6) which makes cloud services (3.2.8) available.



ご清聴ありがとうございました。

アンケートに‘ガイド’に対する要望も記載してください

【問い合わせ先】

一般財団法人 日本情報経済社会推進協会
情報マネジメントシステム認定センター

TEL: 03-5860-7570

FAX: 03-5573-0564

Web: <http://www.isms.jipdec.or.jp/>