経済産業省　平成２６年度サイバーセキュリティ経済基盤構築事業

クラウドセキュリティ監査制度の見直し

平成２７年２月

特定非営利活動法人

日本セキュリティ監査協会

目次

Ⅰ. はじめに

経済産業省は、クラウドサービス利用に係る情報セキュリティに関して、クラウド利用者及びクラウド事業者が適切に管理すべき事項について、「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」に基づき２０１１年にクラウド情報セキュリティ管理基準を策定した。これに基づき、クラウドサービスに係る情報セキュリティ監査を実施するための制度の開発に取り組んでいる。

２０１１年のクラウド情報セキュリティ管理基準策定以降、その基本となる「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２０１３年度版」ならびに「ISO/IEC 27001及び27002（2013年版）」が改訂された。また、「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」に基づいて日本が提案した国際規格が、ISO/IEC 27017として策定中である。

更に、ISO/IEC27017が策定された段階で、そこに定義されている管理策のうち技術的な内容についてどのような監査を行うかの指針が求められている。現在、クラウド情報セキュリティ監査の実現に向けて民間において、監査の方法を検討中であるため、これを生かし国際標準とすることが望ましい。

本事業では、クラウド情報セキュリティ管理基準について、改訂された基準文書等の内容を反映するとともに、ISO/IEC 27017の動向を適切に踏まえた改訂のための検討資料を作成した。また、クラウド情報セキュリティ管理基準の前提となる情報セキュリティ管理基準（経済産業省告示）についても、同様の改訂をするための検討資料を作成した。更に、民間の検討内容を踏まえたISO提案文書の作成支援を行った。

Ⅱ. クラウド情報セキュリティ管理基準並びに情報セキュリティ管理基準の改訂

1. 検討の方法

本事業において、以下を行い、検討方針に反映した。

- 10人程度の有識者からなるワーキンググループを3回程度開催し、意見を反映させる
- ワーキンググループメンバに、過去に情報セキュリティ管理基準又はクラウド情報セキュリティ管理基準の作成に携わった者を含み、その意見を参考にし、専門的な立場から品質を確保する
- ISO/IEC 27017について、わが国の代表として、ISO/IEC策定の国際会議に参加しているクラウドセキュリティコントロール標準化委員会（情報処理学会　情報規格調査会）の委員の意見を聴取し、2014年10月にメキシコで開催されたCD2の結果を含めた最新の動向を把握し、改訂のための検討資料に反映すること

2. 検討資料内容の報告

2.1情報セキュリティ管理基準の改訂に関する検討

2.1.1　改訂方針

JIS Q 27001及び27002（2014年版）は、同規格2006年版より、構成等が大幅改訂されているため、「情報セキュリティ管理基準」も、全面改訂すべきである。

また、「情報セキュリティ管理基準」（平成20年版）の構成・内容等も考慮し、「情報セキュリティ管理基準」の改訂では、以下を反映するべきである。

No	反映箇所	改訂方針
1	全体	JIS Q 27001及び27002（2014年版)の章構成に可能な限り合わせ、全体の編・章構成・章番号を変更すべきである。 ただし、「Ⅳ.マネジメント基準」については、No4も考慮した章構成とすべきである。
2	Ⅰ主旨、Ⅱ本基準の位置づけ	・No1に対応するため、「Ⅰ主旨」を「Ⅰ主旨」「Ⅱ本基準の位置づけ」に変更するべきである ・本改訂の概要を追記すべきである
3	Ⅲ構成	・No1、No4により、変更された章構成を反映すべきである。
4	Ⅳマネジメント基準	以下を考慮して、章構成を全面的に変更すべきである。 ・JIS Q 27001(2014年版)の改訂による章構成の変更 ・情報セキュリティ管理基準平成20年度版のマネジメントプロセスを考慮した章構成
5	Ⅳマネジメント基準	以下により、管理策及びその説明の記載方法を変更すべきである。 ・管理策に相当する内容については、JIS Q 27001（2014年版)の改訂を反映する ・情報セキュリティ管理基準平成20年度版において、JIS Q 27001の管理策の他に、独自記載した部分（以下「独自記載部分」とする）を、インデント（補足/適用指針）を付与し、管理策部分と識別できるように記載する
6	Ⅳマネジメント基準	独自記載部分については、以下を反映するべきである。 ・情報セキュリティ管理基準平成20年度版に基づく記載 ・ISO 31000に基づく、リスクアセスメントに関する独自記載の追加
7	Ⅴ管理策基準	JIS Q 27002（2014年版）改訂に伴い、章番号、管理策内容、目的等を全面的に改訂すべきである。

2.1.2 JASA内意見募集に基づく改訂

情報セキュリティ管理基準の改訂について、JASA（日本セキュリティ監査協会）内で提示された意見募集で寄せられたコメントについて、以下の対応を行うべきである。

・コメント期間：2015/1/5(月)～2015/1/19(月)[1]

	コメント種別	
	反映すべき	反映すべきではない
コメント数	36	6

2.1.3 ISO/IEC規格からの表現修正

ISO/IEC 27001及び27002(2013年版)から、以下については、修正すべきである。

[1] 対象：JASA会員、ならびに情報セキュリティ監査人資格保有者（約1,000人）
方法：会員専用ホームページに掲示し、メールによる募集広告を実施

(1)正誤表に基づく修正

規格協会から発行された正誤表に基づき、表現を修正すべきである。

(2)より明確な表現が必要とされる箇所の修正

JIS Q 27001:2014には、”Resource”については、「資源」と「経営資源」の訳がある。このうち、「経営資源」と訳されている部分に関しては、コンピュータリソースが含まれると解釈される方が望ましいことから、単なる「資源」とすべきである。

2.1.4 検討資料（サンプル）

情報セキュリティ管理基準の改訂の検討資料(サンプル)

Ⅴ.管理策基準

5 章タイトル

5.1 大項目

目的

5.1.1 中項目

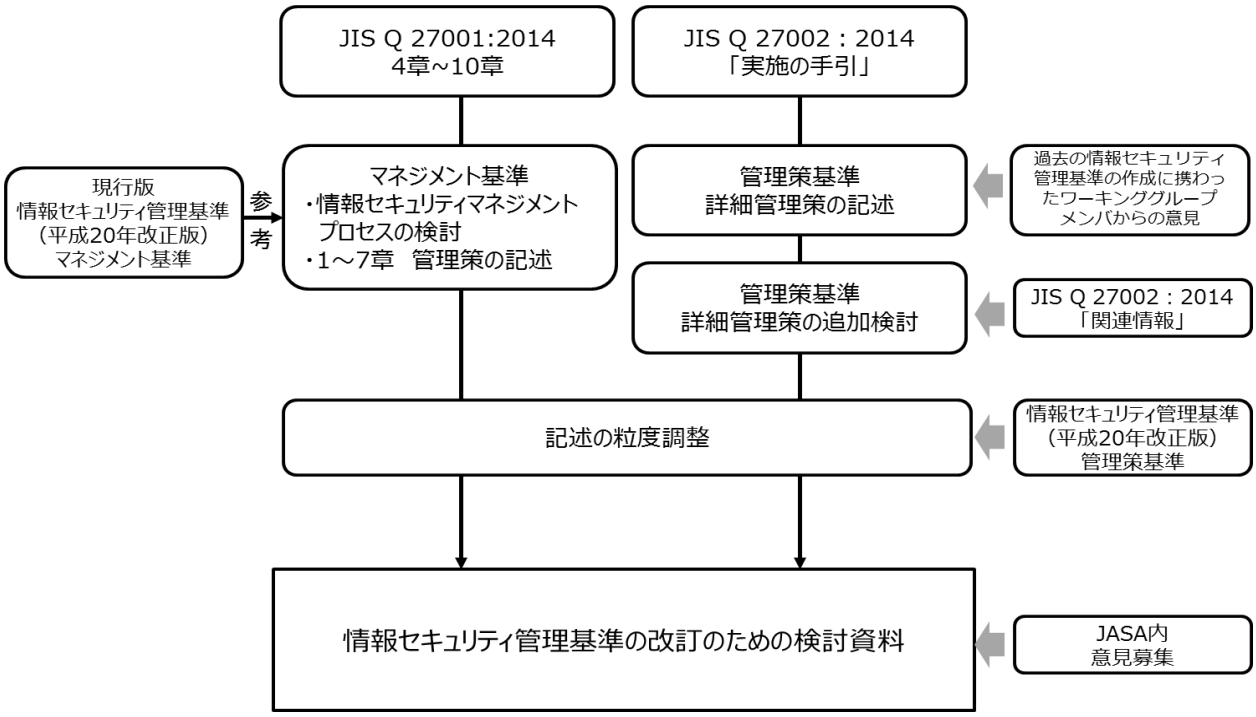
5.1.1.1 小項目

5.1.1.2 小項目

：

・JIS Q 27002(2014年版)を参考に、管理策及び実施例相当の内容を記載
・管理策が行われていることを監査するための基準となるようにする
・一つの項目が一つの管理策、実施事例を示すよう記載
・JIS Q 27002(2014年版)の文意がわかりやすくなるよう、必要に応じて、表現修正

2.1.5 検討のための調査フロー



3. クラウド情報セキュリティ管理基準の改訂に関する検討

3.1 改訂方針

以下に伴い、クラウド情報セキュリティ管理基準は、全面改訂すべきである。

・JIS Q 27001及び27002（2014年版）の大幅な改訂及び「情報セキュリティ管理基準」の全面改訂

・ISO/IEC 27017の策定動向を反映

主に反映すべき事項を以下に示す。

No	反映箇所	改訂方針
1	全体	JIS Q 27001及び27002（2014年版）及び「情報セキュリティ管理基準」の構成変更に伴い、全体の編・章構成・章番号を変更すべきである。
2	全体	ISO27000シリーズの体系に準じ、汎用的な内容は情報セキュリティ管理基準を参照し、クラウド固有の管理策についてのみ、記載する形式とすべきである。
3	Ⅰ主旨	本改訂の概要を追記すべきである。
4	Ⅱ構成と用語の定義	No1、6、7により、変更された章構成を反映すべきである。
5	Ⅲガバナンス基準	変更なしとすべきである。
6	Ⅳマネジメント基準	・情報セキュリティ管理基準改訂に伴い、章構成を変更すべきである ・No2を反映し、クラウド固有の「リスクコミュニケーション」のみ記載するべきである
7	Ⅴ管理策基準	・ISO/IEC 27017策定動向（2014年10月メキシコ会議の結果）の情報に基づき、管理策内容、目的などを改訂すべきである ・No2の反映し、クラウド固有のクラウド事業者向け管理策のみを記載するべきである。
8	Ⅵ基本言明要件	リスクに対応する基本言明要件[2]と、クラウド固有の管理策（CLD)を再掲すべきである。 ・JIS Q 27001（2014年版）改訂に伴い、リスクに対応する管理策番号を変更するべきである ・ISO/IEC 27017策定動向（2014年10月メキシコ会議の結果）の情報に基づき、クラウド固有の管理策を基本言明要件として記載するべきである
9	Ⅶ 付録 クラウド利用者向け管理策基準	参考として、クラウド利用者向け管理策を記載するべきである。

[2] JASA-クラウドセキュリティ推進協議会「基本言明要件に関わる基本リスク」(2013年)に対応する基本言明要件

3.2 JASA-クラウドセキュリティ協議会内意見募集に基づく改訂

クラウド情報セキュリティ管理基準の改訂について、JASA-クラウドセキュリティ推進協議会内で提示された意見募集に寄せられたコメントについて、以下の対応を行うべきである。

・コメント期間：2015/1/16(金)～2015/1/26(月)[3]

	コメント種別	
	反映すべき	反映すべきではない
コメント数	9	0

3.3 検討資料（サンプル）

クラウド情報セキュリティ管理基準の改訂の検討資料（サンプル）

Ⅴ.管理策基準

5 章タイトル

5.1 大項目

目的

5.1.1 中項目

5.1.1.1 / 5.1.1.2 / 5.1.1.3 / 5.1.1.4 / …5.1.1.23は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

5.1.1.24.P 小項目（クラウド事業者向け）

5.1.1.25.P 小項目（クラウド事業者向け）

：

・ISO/IEC 27002(2013年版)及びISO/IEC 27017策定動向の情報を参考に、管理策及び実施例相当の内容を記載

・汎用的な管理策の実装例については、「情報セキュリティ管理基準」を参照する

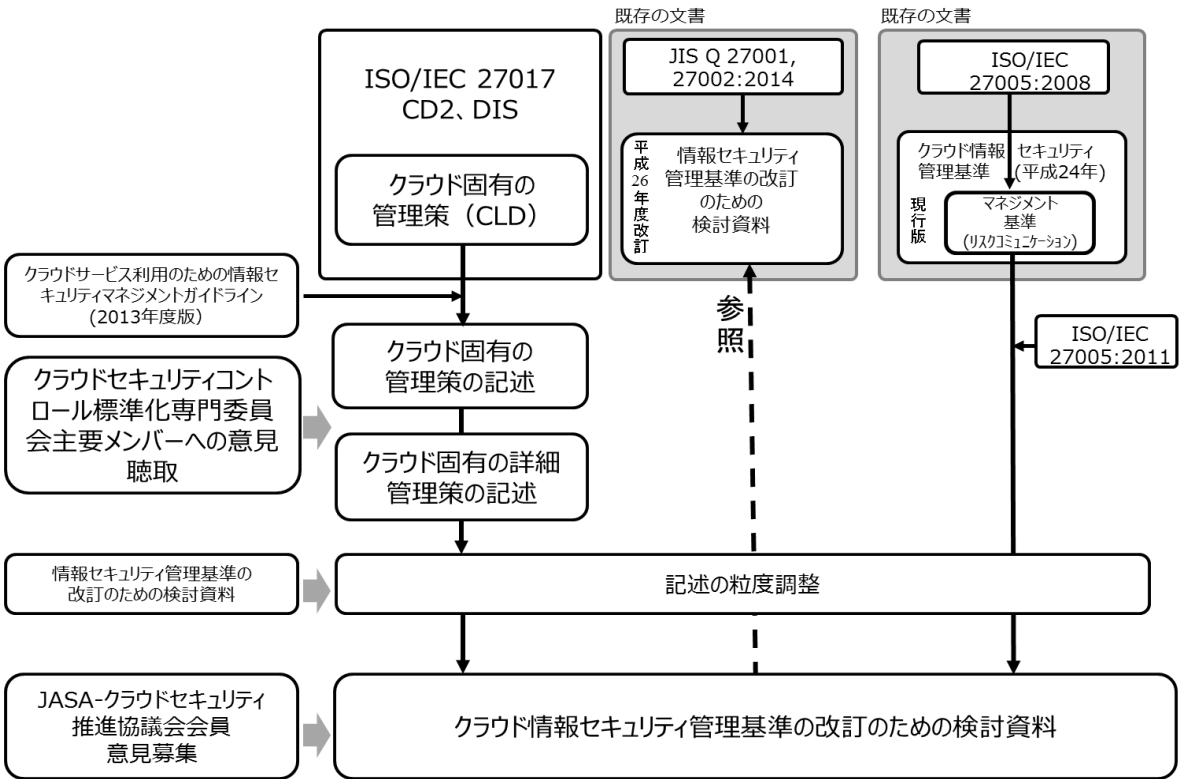
・クラウド固有の実装例（クラウド事業者向けの実装例）を記載する

・一つの項目が一つの管理策、実施事例を示すよう記載

・文意がわかりやすくなるよう、必要に応じて、表現修正

[3] 対象：JASA-クラウドセキュリティ推進協議会会員40社
方法：会員専用ホームページに掲示し、メールによる募集広告を実施

3.4　検討のための調査フロー



Ⅲ．クラウド情報セキュリティの監査及びアセスメントに関するガイドの作成支援

1.支援の経緯及び内容

クラウド情報セキュリティ管理基準に対応した監査については、技術的な内容についてどのように監査するかが問われる。管理基準は多様な技術に対応できる表現になっているが、監査においては実装された技術に応じて、何をどのように監査することが必要かを問われる。このため、管理基準に対応した技術的なガイドが必要となる。

そこで、ISO/IEC27017に対応した監査のための評価ガイドを日本セキュリティ監査協会で作成している。今回、この内容をベースにISOに監査及びアセスメントガイドの標準を提案することとなった。

2014年10月にメキシコシティのISO/IEC JTC1 SC27委員会のWG4おいて、Cloud Security AuditのStudy Period（SP）の検討会が開催されるので、この場に提案する文書について作成を行った。今回提案した内容は、ISO/IEC27008のAnnex Aと同水準の内容である。

会合での主要な意見は以下のとおりである。

【否定的意見】

- 詳細すぎる点が問題
- ISO/IEC27017のみに焦点を当てることは、対象が狭すぎる
- アーキテクチャ（主体および役割）が不明確

【肯定的意見】

- 早めに監査の基準が必要

【他のISO規格との関係】

・ISO/IEC27007、27008及び27018等との関係の整理が必要

SPでは、後述する通りクラウド監査のための国際標準の必要性は認められたが、内容については合意が得られなかった。会合での検討を踏まえて、別途改訂が行われているISO/IEC27008の次のバージョンのAnnex　として提案することが適切との判断を行った。

そこで、メキシコでの提案資料に内容を付け加え、様式もISO/IEC27008のAnnexにあわせたものに直して、次の会合に提案する資料とした。

2.提案文書の内容

2.1　Mexico会合

Mexico会合の提案文書は、全く新しい規格の提案として行った。このため、文書はISO規格の標準書式に従った。以下に示すのが、全体構成である。

内容

2.2 Kuching会合への提案

2.2.1 全体構成

提案文書の構成は下記のとおりである。

本来付属書には目次を必要としないが、これ自体が独立した文書であるため、付属書の冒頭に目次を付けた。

全体のうち1～4章の部分で文書の位置づけならびに、基本的な考え方を述べている。この中では、クラウドのアーキテクチャに基づいて、サービス管理、サーバ仮想化、ネットワーク仮想化、ストレージ仮想化の４つで構成されるクラウドモデルの形式をベースとして叙述であることを示した。5章以降はこれらの構成に共通する事項と構成要素ごとに分かれる事項を、章立てして記述している。

付属書 C内容目次

2.2.2　提案内容

提案文書に基づいて規格化が決定した場合に、編集会議における議論に基づき内容は大きく変更されることが予想される。このため、提案内容そのものを詳述することはあまり意味がない。本節では、政府支援の内容を明示することを目的としているため、上述のC.1.～C.4.までの全文とC.5.以降の例として、C.8.の一部を掲載する。

C.1.　本付属書の位置づけおよび目的

本付属書は、ISO/IEC 27017:201xが規定するクラウドサービスに対する情報セキュリティ管理策に関し、ISO/IEC 2008:2011で規定された情報セキュリティ管理策の監査ガイドラインに準じた監査を行うための技術的な手引きである。

本書では、クラウドサービスのうち、コンピュータ資源の提供を主とするIaaSもしくはPaaSを想定し、監査に必要な技術的な着目点、監査方法を解説する。監査方法を解説する上では、IaaSの提供環境について一定のモデルが必要となる。このため、本書ではIaaSの抽象モデルを設定し、同モデルに基づいた説明を行う。

本書はISO/IEC 27017:201xを中心とし、クラウドサービスに特有な情報セキュリティ管理策についてのみ解説を行う。一般の情報システムと共通する情報セキュリティ管理策については本書では触れない。

本書により、監査人はクラウドサービスに特有の監査ポイントを理解することが可能である。また、監査を受ける側の技術者にとっては、監査人に対しどのような挙証を行い、証跡を示すべきかのヒントを与える。

クラウドサービスを提供するシステムは、IaaSにおいても千差万別であり、技術的進歩が著しいことから日々変化する。本書は特定のシステムを想定するものではなく、監査の方法、留意点、監査対象などについて、実践指針となるものである。

本付属書は、クラウドサービスを提供するコンピュータシステムに関する、技術的な監査方法について、モデルと例により解説するものである。

クラウド事業者は、採用したセキュリティ管理策のうち、ITシステムで実装可能な事項を自己のクラウドシステムに組み込む。本付属書は、セキュリティ管理策が正しくクラウドシステムに実装されているかを監査することを中心に解説をする。

セキュリティ管理策の実施においては、以下の検証も必要だが、これらは本付属書の対象外とする。

- 設計の妥当性の検証
- セキュリティ管理策に関する運用が文章化されていることの検証
- セキュリティ管理策に関する運用が実施されていることの検証

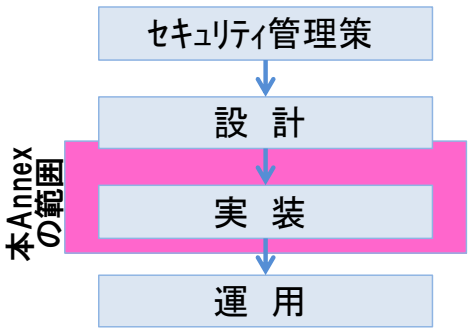


図 1 本付属書の対象範囲

C.2. 他の国際標準との関係

(1) ISO/IEC 27017:201x

本付属書は、ISO/IEC 27017:201xが規定する、クラウドサービスに対する情報セキュリティ管理策の実践のための規範の監査方法について、技術面から監査の具体的方式を提示するものである。

本付属書では、ISO/IEC 27017:201xにおいて、クラウド事業者が行うべき情報セキュリティ管理策に対する監査手段を規定している。

(2) ISO/IEC 27018:2014

ISO/IEC 27018:2014では、クラウドサービスにおける個人識別情報Personally Identifiable Information (PII)について規定している。本付属書はIaaSを対象としている。IaaSではクラウド利用者が利用する仮装マシンの中に格納される情報については、クラウド利用者自身が情報セキュリティを講じる責任がある。

すなわち、仮装マシン中のPIIについてはクラウド事業者が管掌できないことから、本規格の対象外とする。

クラウド事業者が保持すべきPIIとしては、クラウド利用者に関する情報がある。これらは後に述べるクラウドサービス環境モデルの「サービス管理」において、管理・格納される。サービス管理におけるPIIの扱いは、ISO/IEC 27018:2014に準拠する必要がある。

(3) ISO/IEC 17788, Information technology - Cloud computing — Overview and vocabulary

本付属書では、ISO/IEC 17788に規定するクラウドコンピューティングに関する概観および用語を準用する。

(4) ISO/IEC DIS 17789, Information technology - Cloud Computing - Reference Architecture

クラウドサービスを構成するコンポーネントの基本的な考え方については、ISO/IEC 17789を踏襲する。ただし、ISO/IEC 17789では、役割と活動の観点から、クラウドコンピューティングのアーキテクチャを規定している。これに対し、監査においては、仮想化機構の設定の確認など、クラウドシステムの実装を意識した観点が必要となる。このため、本付属書では、クラウドシステムの実装をモデル化した実装モデルを提示し、ISO/IEC 17789の規定による機能コンポーネントと監査項目との対応づけを図っている。

C.3. 本付属書の構成

本書では、まずIaaS/PaaSを想定したクラウドサービスの提供環境のモデルを提示する。このモデルでは、リソースの種別と仮想化との関係、クラウド利用者とテナントの概念を規定する。本モデルでは、リソースの種別として、サーバ、ネットワーク、ストレージの３つを規定した。

次に、リソース種別ごとに、次の順で、本モデルにおける管理策とその監査方法を示す。

(1) 一般的/代表的な技術の解説

当該仮想化の実装に関する技術的要素とその指針。複数の実装方式がある場合には、代表的な幾つかの方式を列挙する。

(2) ISO/IEC 2017:201xで規定されている管理策

当該仮想化に密接に関連する、ISO/IEC 2017:201xの管理策。

(3) (2)の管理策に対する監査方法

(2)の管理策に対する監査方法の指針。(1)で複数の実装が考えられる場合には、その１つを示す。

C.4. クラウドサービス環境モデル（IaaS）

本付属書が想定するIaaSにおいて、クラウドを提供する環境は、利用者が直接使用する仮想化されたリソースと、それを具現化する仮想化機構、および、仮想化機構を制御しサービスとして提供するためのサービス管理とから成る。

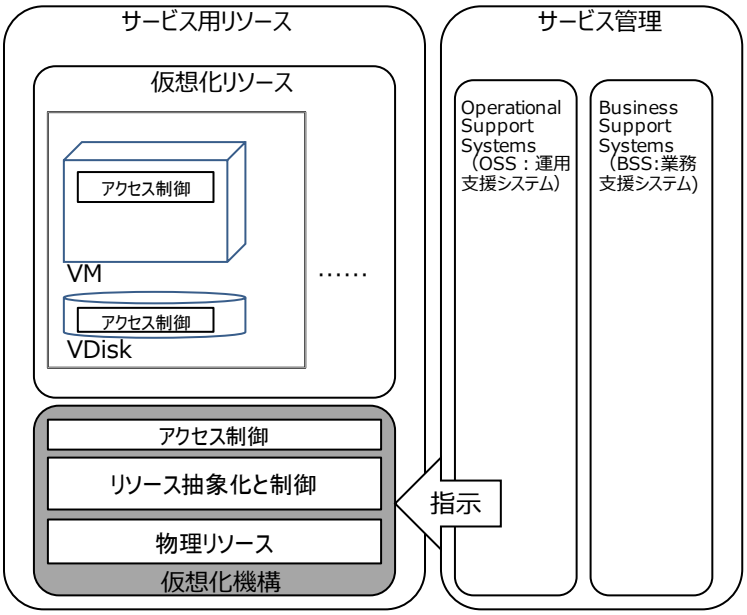


図 2 実装モデルの基本構造

仮想化機構では、物理リソースがリソース抽象化・制御コンポーネントにより、テナントごとにアクセス権などが分離され、仮想化されたリソースとして提供される。これらの処理は、サービス管理により、仮想化機構に指示(Direct)される。

ISO/IEC 17789で規定される機能コンポーネントは、実際にはこの仕組みの中で、対象となるリソースの種別、階層により、それぞれを実現する実装上の要素によって実現される。

アクセス制御を例にした場合、以下のようになる。

- 物理ディスクのアクセス管理　・・・・ディスク装置
- テナントごとのアクセス権管理　・・・　仮想化機構
- 仮想ディスクのアクセス管理　・・・　仮想化機構
- 各VMの中のアクセス管理　・・・・　VMのOS

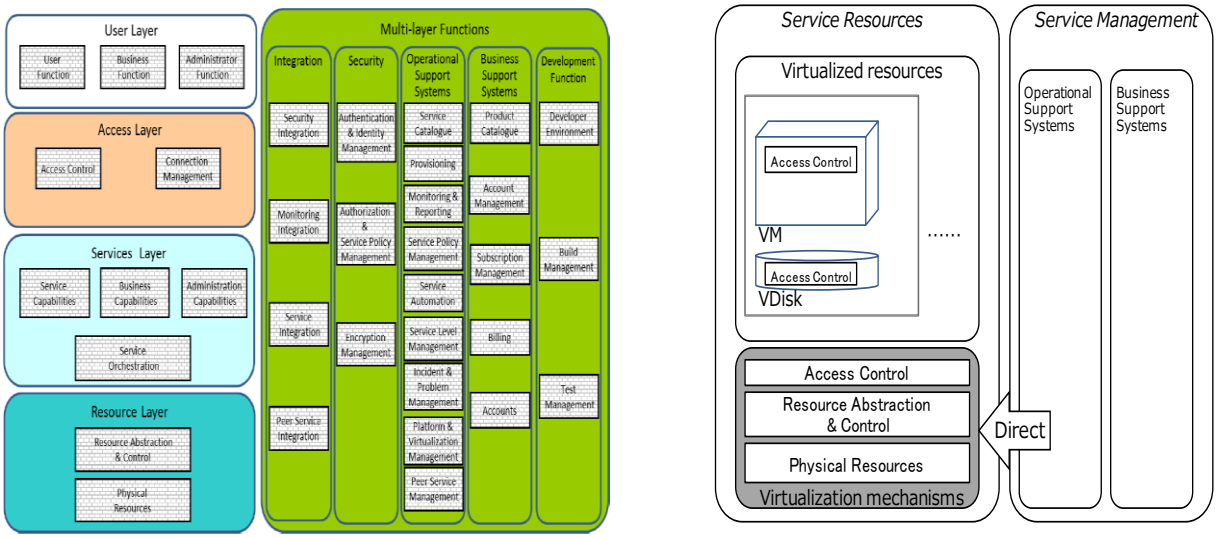


図 3 実装モデルにおけるアクセス権実装の例（ISO/IEC17789に加筆）

ISO/IEC 17789で、多層機能Multi-layer Functions)として規定される機能、コンポーネントの内、サービスに提供に関わるものは、本規格の実装モデルではサービス管理に含まれる。業務支援機能(Business Support Systems)や運用支援機能(operational Support Systems)がこれに当たる。

多層機能のなかで、インテグレーション(Integration)とセキュリティ(Security)に関するものは、前述のアクセス権と同様に、対象となる機構において実装される。

仮想化リソースと仮想化機構は、ネットワーク、サーバ、ストレージで異なることから、これらリソース種別ごとの区分が必要となる。

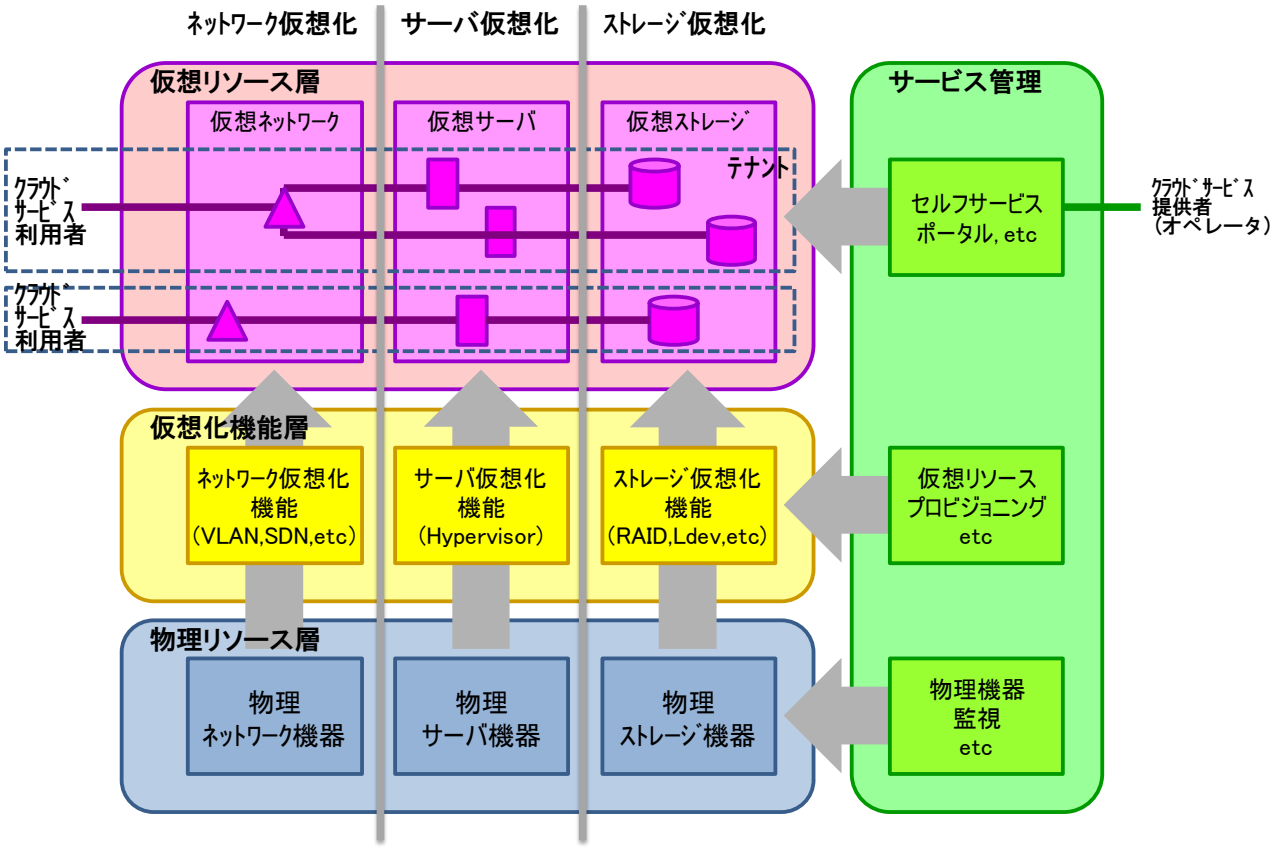


図 4評価対象として想定するクラウド環境

本モデルでは、４つの要素がある。このうちの３つである、物理リソース、仮想化機能、仮想化リソースは、ネットワーク、サーバ、ストレージの３種に分類される。

（注記１）クラウドサービスに用いられる技術は多岐にわたることから、これらを詳細に取り上げることは個別・具体的すぎる。また、クラウドサービスに用いられるコンピューティング技術は、新しい分野であり、技術的に発展途上にある。これらのことから、個別・具体的な技術に基づく評価の方法を定めることは、標準化になじまない。これにより、管理策の意図するところを具体的な技術としてイメージすることができるため、評価に際しての具体的な方法を示唆することができる。実際に評価を行う際に、このモデルを念頭に置き、管理策のために実装されている実際の技術が、管理策の意図に沿ったものであるか、また、それらの評価のための証拠の収集はどのよう

にするかを、評価者（または監査人）が想起できる。

（注記２）本指針に従うことで、監査人は的確な監査を実施することが可能となる。また、クラウド事業者においても、自サービスをISO/IEC 27017：201Xに準拠させるための具体的な管理策を策定することが可能となる。

(1) 物理リソース

クラウドサービスを提供するために必要となる、物理的機器の層である。サーバ機器、ネットワーク機器、ストレージ機器などが構成要素となる。物理ネットワーク機器としては、サーバとネットワークを接続する物理NIC などが挙げられる。物理ストレージ機器としては、サーバとストレージを接続するHBA 、ファイバスイッチなどが挙げられる。

(2) 仮想化機能

物理リソースを仮想化し、クラウドサービスで提供される仮想リソースを作製する機能を実装する層である。サーバの仮想化の場合、ハイパバイザがこれにあたる。ネットワークの仮想化では、VLAN やSDNなどにあたる。ストレージにおいては、多くの場合、ストレージ装置がこの仮想化機能を有している。

(3) 仮想リソース

仮想化機能によって作り出され、クラウドサービスにおいてクラウド利用者に提供される仮想的なリソースの層である。仮想化機能は、仮想リソースを実現するための機能に対し、仮想リソースは作製された仮想リソースの集合を指す概念である。

（注記）前述のとおり、仮想化される対象から、各層はネットワーク、サーバ、ストレージに分類したが、仮想リソースは必ずしも該当する種別の仮想化機能により作られるものではない、仮想ネットワークを構成する仮想化スイッチはサーバ仮想化を行うハイパバイザにより作製されるなどの場合がある。

(4) サービス管理

サービス管理は、主としてクラウド事業者がクラウド環境の管理・運用のために利用するシステムである。前述の仮想化機能を利用し、クラウドサービスに必要な仮想リソースのプロビジョニングなどを行う。また、物理リソースの監視、管理などを行い、クラウド提供環境全体が健全に動作するための制御を司っている。

また、プロビジョニングやVMの起動/停止など、クラウド利用者が許された範囲の操作を行うためのポータル機能や、ユーティリティ、APIなどもこのサービス管理に含まれる。

これらの層や系に加え、重要な概念は「テナント」である。テナントはクラウド利用者ごとに割り当てられた仮想リソースを集約する領域であり、他のクラウド利用者とアクセスを分離する境界である。

C.8.　ネットワーク仮想化（内容例示）

C.8.1.　ネットワーク仮想化の概略

従来のネットワーク仮想化は、1つの物理ネットワーク上で、複数の独立した通信を可能とする手段である。一方、サーバ仮想化におけるネットワークの仮想化は、1つの物理サーバ内にある複数の仮想マシンをつなぐ手段となる。仮想マシンは物理サーバの故障や物理資源の高使用率を契機に別の物理サーバに移動することがある。このとき仮想マシンのVLAN IDやIPアドレスは変わらない点に特徴がある。仮想マシンとそれをつなぐネットワークの概略構成は次のとおりである。

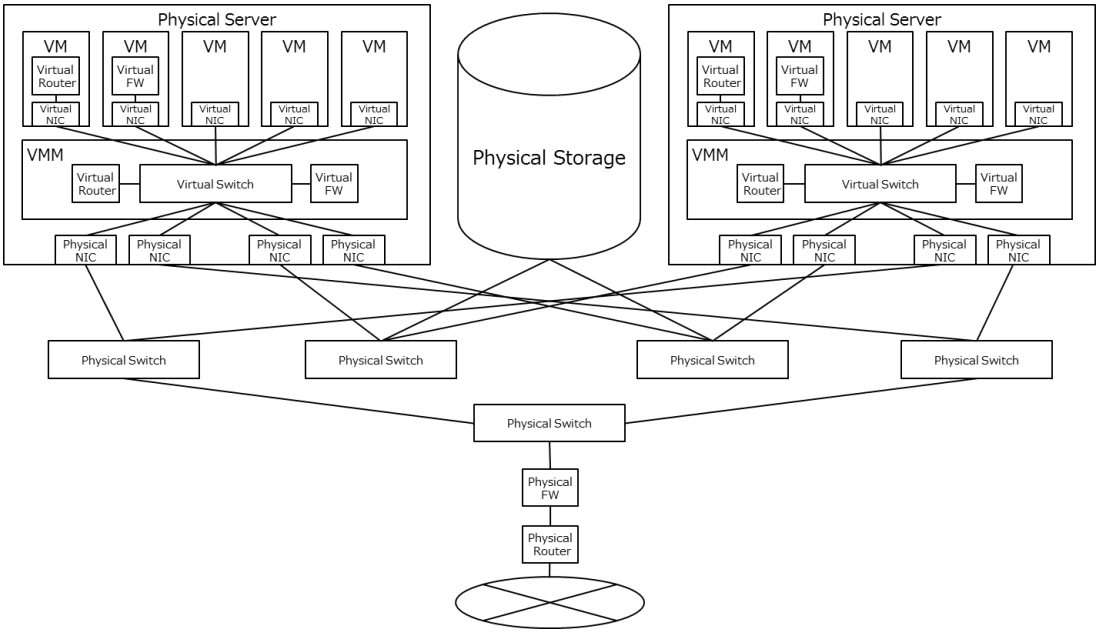


図 7　仮想マシンをつなぐネットワークの概略構成

(1)　仮想スイッチ

仮想マシンモニタによって提供される論理的なL2スイッチの機能。物理NICと仮想マシンの間に介在し、フレームの受け渡しを行う。物理NICは透過的にフレームを中継するため、仮想スイッチは物理NICをはさんで物理スイッチとスイッチ間接続される。

(2)　仮想 NIC

仮想マシンを仮想スイッチに接続するために、仮想マシンモニタによって提供される論理的なネットワークインタフェースカードの機能。

(3)　仮想ルータ

仮想マシンにインストールされたソフトウェアによって提供される論理的なルータの機能、又はルータとして機能する仮想マシンそのものを指す。仮想スイッチがルータ機能を併せ持つこともある。

(4)　仮想ファイアウォール

仮想マシンにインストールされたソフトウェアによって提供される論理的なファイアウォールの機能、又はファイアウォールとして機能する仮想マシンそのものを指す。

C.8.2.　クラウドサービスにおけるネットワーク仮想化の適用と着目点

(1)　ネットワーク仮想化におけるテナント分離

テナントが利用する仮想マシンは固有の仮想MACアドレス、IPアドレスをもち、1つ又は2つ以上の仮想マシンをつなぐ論理ネットワークがテナント毎に独立して設定されることにより、各テナントは物理ネットワーク上でも物理サーバ上でも分離される。

(2)　ネットワーク仮想化における可用性の確保

I物理サーバの故障の場合、その上の仮想マシンと仮想ネットワークは、他の物理マシンに移動することで可用性が維持される。物理サーバに実装された物理NICの故障の場合には、物理NICが冗長化されていれば、他の物理NICに仮想ネットワークが迂回して可用性が維持され、仮想マシンそのものが移動することはない。

(3)　ネットワーク仮想化における帯域及びアドレス空間の管理

一般にクラウドサービスでは、限られた物理資源の上に多くの仮想資源を集約して高密度に設定するために、仮想ネットワークの論理帯域の総和が物理ネットワークの物理帯域をはるかに上回ることがある。また、多数の仮想マシンがVLAN IDやIPアドレスを保持したまま、ある物理サーバから他の物理サーバへと移動することがあるため、物理スイッチに設定が必要なVLAN ID数や学習が必要なMACアドレス数が多くなる傾向がある。

C.8.3.　ネットワーク仮想化に関する監査

C.8.3.3通信のセキュリティ〈13〉

管理策		ISO/IEC 27017:201x　13.1.3 Segregation in networks
技術情報補足		クラウドサービスにおけるネットワークの分離は、物理資源が独立した物理ネットワークによる物理的分離と物理資源を共有した論理ネットワークによる論理的分離がある。論理ネットワークは、物理ネットワークだけでなく、物理サーバ上にも展開される。
1	セキュリティ実装基準（詳細管理策）	個別の物理資源（物理サーバ、物理ストレージ等）をクラウドサービス利用者がそれぞれ使用する場合、各クラウドサービス利用者毎に独立した通信機器と通信ケーブルで構成される物理ネットワークを各クラウドサービス利用者用の個別のネットワークとして使用する。 同一の物理資源（物理サーバ、物理ストレージ等）を複数のクラウドサービス利用者がテナントとして共同して使用する場合、テナント毎又は仮想マシン毎に論理的に独立したVLANを使用する。 クラウドサービス利用者の使用する物理資源（物理サーバ、物理ストレージ等）を管理するクラウドサービス提供者は、クラウドサービス利用者とは別の物理ポートに接続し、物理的に独立した通信機器と通信ケーブルで構成される物理ネットワークを管理用ネットワークとして使用する。 クラウドサービス利用者の使用する物理資源（物理サーバ、物理ストレージ等）

		を管理するクラウドサービス提供者は、クラウドサービス利用者とは別の論理ポートに接続され、論理的に独立したVLANを管理用ネットワークとして使用する。	
	セキュリティ実装基準の技術的解説	ネットワークが物理的に分離している場合、同一物理資源における複数の物理ポートには異なるIDが割り当てられる。ネットワークが論理的に分離している場合、同一物理ネットワーク上における複数の論理ネットワークには異なるVLAN ID、VSAN ID又はサブネットマスク等が割り当てられる。	
	1.1	監査実施ガイド	テナント毎に独立したテナント用ネットワークが設定されているか確認し、その他にバックドアがないことを確認する。
		想定される証拠	テナントに割り当てられたネットワークのID及びそのネットワークの経路設定（スイッチングテーブル、ルーティングテーブル等）
		監査技法	観察，閲覧
	1.2	監査実施ガイド	設定されたテナント用ネットワークにアクセスできるのは許可された者のみであることを確認する。
		想定される証拠	テナントに割り当てられたネットワークに対するアクセス権設定（アクセス制御を実行するサーバ、ネットワーク機器のアクセス権管理テーブル等）
		監査技法	観察，閲覧
	1.3	監査実施ガイド	クラウドサービス提供者が利用する管理用ネットワークがその他のネットワークと独立して設定されているか確認し、設定された管理用ネットワークにアクセスできるのはクラウドサービス提供者のうち許可された者のみであることを確認する。
		想定される証拠	クラウド事業者が利用する管理用ネットワークのID、経路設定及びアクセス権設定
		監査技法	観察，閲覧

付録

付録1　第1回ワーキンググループにおける改訂方針

No	対象文書	項目	改訂方針
1	情報セキュリティ管理基準	項番の整理について	・基準の項番は重複を避けることが望ましい ・項番は、ISO/IEC規格との整合について照合しつつ、読みやすさを重視した方向とすべき
2	情報セキュリティ管理基準	重複項目とされる内容	経営が責任をとる話と実際に現場で行われていることは、監査対象として別であり、現場での実施を監視すべき。
3	情報セキュリティ管理基準	マネジメントレビューのインプット	平成20年度版 3.4.1リスクアセスメント、4.3予防措置は概念として残すべき。
4	情報セキュリティ管理基準	記録管理の取り扱い	記録については、8.2.2文書化した情報の管理の「適用指針」として明記すべき。
5	情報セキュリティ管理基準	独自記載の意義1	・平成20年度版ではISMSの理解不足を補う意図があったが、改訂版では本部分は不要とすべき ・ISO/IEC規格の改訂で記載の抽象度が高くなったものは、補足すべき
6	情報セキュリティ管理基準	独自記載の意義2	ISO/IEC規格の改訂で粒度が粗くなったものについて、監査ができるレベルで具体化すべき。
7	情報セキュリティ管理基準	独自記載の意義3	リスクアセスメントの記載がISO31000を参照することとなり、分かりにくくなったため補足すべき。
8	情報セキュリティ管理基準	独自記載の取扱い	インデントをつけるなど、ISO/IEC規格本文と区別できる記載方法とすべき

付録2　第2回ワーキンググループにおける改訂方針

No	対象文書	項目	改訂方針
1	情報セキュリティ管理基準	項番の整理について	ISO/IEC27001、27002規格の章構成並びに情報セキュリティ管理基準平成20年度版のマネジメントプロセスを重視した章構成を考慮して、項番を付与すべき
2		独自記載の取扱い	独自記載部分にインデントをつけ、ISO/IEC規格を元にした記載と、区別できる記載方法とすべき。
3	クラウド情報セキュリティ管理基準	項番の整理について	・「情報セキュリティ管理基準」の改訂における構成変更に基づき、クラウド情報セキュリティ管理基準の構成も変更すべき ・ISO27000シリーズの体系に準じ、汎用的な内容は情報セキュリティ管理基準を参照し、クラウド固有の管理策についてのみ、記載すべき
5		Ⅰ主旨	本改訂の概要を追記すべき。
6		Ⅱ構成と用語の定義	変更された章構成を反映すべき。

7		Ⅲガバナンス基準	変更なし。
8		Ⅳマネジメント基準	・情報セキュリティ管理基準改訂に伴い、章構成を変更すべき ・クラウド固有の「リスクコミュニケーション」のみ記載すべき
9		Ⅴ管理策基準	・汎用的な管理策は、情報セキュリティ管理基準を参照し、クラウド固有のクラウド事業者向け管理策のみを記載すべき ・クラウド利用者向け管理策は、付録として記載するべき
10		Ⅵ基本言明要件	リスクコミットで、対応する基本言明要件を記載するべき。

付録3　第3回ワーキンググループにおける改訂方針

No	対象文書	項目	改訂方針
1	情報セキュリティ管理基準、 クラウド情報セキュリティ管理基準	Ⅱ構成 Ⅱ構成と用語の定義	以下を追記すべきである。 ・「マネジメント基準」の章構成は、プロセスを考慮し、ISO/IEC 27001規格の章構成を変更すべき ・「マネジメント基準」は、原則全て実施すべき ・「管理策基準」は、管理策は実施すべき事項であり、詳細管理策は、実施方法等により任意に選択する事項である

付録4　ISOメキシコ会合の概要とクラウド情報セキュリティ管理基準のあり方

1.　概要

ISO/IEC JTC1 SC27は、情報セキュリティの国際規格の制定を行う組織である。2014年10月19日（月）から24日（金）において、SC27委員会がメキシコシティのイベロサンタフェ大学（Universidad Iberoamericana） で行われた。

会議は、5つのWGに分かれて行われた。このうち、クラウド情報セキュリティに関わる議論は、情報セキュリティマネジメントに関わる規格を検討するWG1と情報セキュリティ技術に関わる規格を検討するWG4において行われた。

各々に関わる議論は下記のとおりである。

WG1：　ISO/IEC27017 CD2
　　SP CSRMF (Cloud adopted Risk Management Framework)
WG4:　ISO/IEC27036-4
　　SP Cloud audit and assessment

上記のうち、ISO/IEC27017は、日本が「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」に基づき提案し、規格化が始まったものである。

2.　検討の結果

1）ISO/IEC27017 CD2

- ISO/IEC 27017 は各国の賛同を得て、DIS 投票へと進むことになった。
- 議論した結果、ISO/IEC 17789 を Normative Reference となった。こちらについては ISO/IEC 17788 と同様に無料で配布されているが、現在のところ JIS 化は未定。
- DoC および Revised Texts のエディタ提出締め切りが 11 月 14 日、発行後 5 ヶ月投票となる（BCM Resolution 1 of SC27N14700）。
- 内容はほぼ確定し、今後は編集上の問題を修正することとなる。
- 2015 年 5 月のマレーシア会合で FDIS の投票に持ち込まれる見通。なお、ITU-T は同年 9 月の会合で FDIS の承認を行う予定。この結果、2015 年秋には ISO 化される見通し。

2）SP　CSRMF

- クラウドの規格化（27017）にあまり関与しなかったメンバーの議論であり、本規格の必要性について、議論された。
- CRMF(Cloud Risk Management Framework)に内容を変更し継続検討することとなった。

3）ISO/IEC27036-4

- 全体の構造を整理する大幅な提案を日本が行ったが、概ね了承された。

・　CD 投票に諮られることとなった。

4）SP Cloud audit and assessment

・　このような規格が必要であることが認識され、継続的に議論することとなった。
・　日本から詳細な提案を行ったが、以下の点で議論が分かれた。結論としては採択されなかった。

【否定的意見】

・　詳細すぎる点が問題
・　ISO/IEC27017のみに焦点を当てることは、対象が狭すぎる
・　アーキテクチャ（主体および役割）が不明確

【肯定的意見】

・　早めに監査の基準が必要
・　ISO/IEC27007、27008及び27018等との関係の整理が必要

3.　クラウド情報セキュリティ管理基準のあり方

ISO/IEC27017の全体構造が確定し、内容も９５%以上確定している。この内容は、2013年度版の「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」の内容も反映されている。

2015年秋のISO化に合わせて、各社が監査に早急に取り組めるように、内容について理解しつつ、可能な限り早急な管理基準の作成が望ましい。

付録5　ワーキンググループ委員

委員長	大木 榮二郎	（工学院大学教授）
副委員長	高原 清	（株式会社日立製作所）
副委員長	間形 文彦	（日本電信電話株式会社）
委員	内田 仁史	（セールスフォース・ドットコム）
	加藤 雅彦	（株式会社インターネットイニシアティブ）
	岸 泰弘	（あらた監査法人）
	久保田 朋秀	（日本マイクロソフト株式会社）
	佐藤 元彦	（伊藤忠テクノソリューションズ株式会社）
	長尾 慎一郎	（新日本有限責任監査法人）
	山田 英史	（株式会社ディアイティ）
	和貝 享介	（有限責任監査法人トーマツ）

（敬称略、順不同）

事務局	永宮　直史	（特定非営利活動法人日本セキュリティ監査協会）
	中田　美佐	（エヌ・ティ・ティ・ソフトウェア株式会社）
	牧野　建	（エヌ・ティ・ティ・ソフトウェア株式会社）
	土屋　直子	（エヌ・ティ・ティ・ソフトウェア株式会社）

（敬称略、順不同）