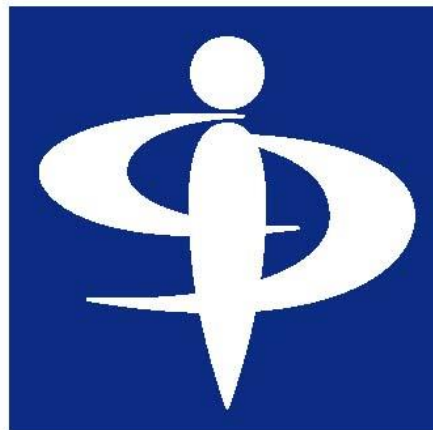


外部委託におけるISMS適合性評価制度の  
活用方法

*-JIS Q 27001:2014 対応-*

ISMS : Information Security Management System  
情報セキュリティマネジメントシステム



2015年11月30日

**JIPDEC**

一般財団法人 日本情報経済社会推進協会

JIPDECの許可なく転載することを禁じます

## 目次

1	はじめに.....	1
1.1	本書の目的.....	1
1.2	本書の対象者.....	1
2	ISMS 適合性評価制度.....	1
2.1	ISMS 制度の概要.....	1
2.1.1	ISMS 制度の目的.....	1
2.1.2	ISMS 制度の認証基準.....	1
2.1.3	ISMS 認証.....	2
2.1.4	ISMS 制度の運用体制.....	2
2.1.5	ISMS 制度に関する情報公開.....	2
2.1.6	ISMS 制度に関する問い合わせ先.....	3
2.2	ISMS 制度の活用.....	3
3	ISMS 認証の活用方法.....	3
3.1	登録証.....	4
3.2	適用範囲定義書.....	6
3.3	適用宣言書.....	6
付録 1.	登録証（例）.....	8
付録 2.	適用範囲定義書（例）.....	9
付録 3.	適用宣言書（例）.....	11
付録 4.	JIS Q 27001 附属書 A 管理目的.....	14

## 1 はじめに

### 1.1 本書の目的

本書は、組織又は企業において情報処理業務の一部又は全てを外部委託する場合に、情報セキュリティ責任者及び担当者が委託先の選定に情報セキュリティマネジメントシステム（ISMS）適合性評価制度（以下、ISMS 制度という。）を活用するためのガイドである。また、委託先候補における情報セキュリティ対策の履行状況を確認する手段として ISMS 制度を利用する場合のガイドとして活用することを目的としたものである。

また、本書では、JIPDEC(一般財団法人日本情報経済社会推進協会)が認定した認証機関より発行される登録証（詳細は本書「3.1 登録書」を参照）を活用するためのガイドであり、その他の認証機関から発行される登録書については対象としていない。

この度、JIS Q 27001:2006 から JIS Q 27001:2014 への移行に伴い、2006 年に発行した「外部委託における ISMS 適合性評価制度の活用方法」を JIS Q 27001:2014 対応として改訂した。

注記 JIS Q 27001:2014 では、「ISMS は、リスクマネジメントプロセスを適用することによって情報の機密性、完全性及び可用性を維持し、かつ、リスクを適切に管理しているという信頼を利害関係者に与える。」としている。

### 1.2 本書の対象者

本書は、各組織又は企業で情報処理業務の外部委託に係る手続を行う情報システムの情報セキュリティ責任者及び担当者を対象としている。

## 2 ISMS 適合性評価制度

### 2.1 ISMS 制度の概要

#### 2.1.1 ISMS 制度の目的

ISMS 制度は、国際的に整合性のとれた情報セキュリティマネジメントに対する第三者適合性評価制度である。ISMS 制度は、わが国の情報セキュリティ全体の向上に貢献するとともに、諸外国からも信頼を得られる情報セキュリティを達成し、維持することを目的としている。

#### 2.1.2 ISMS 制度の認証基準

認証基準とは、第三者である認証機関が ISMS 制度の認証を希望する事業者の適合性を評価するための基準である。ISMS 制度では、JIS Q 27001:2014（ISO/IEC 27001:2013）を認証基準と

して用いている。なお、JIS Q 27001:2014と ISO/IEC 27001:2013 は同一（identical）であり言語が日本語か英語かの違いのみである。

### 2.1.3 ISMS 認証

ISMS 認証とは、ISMS の要求事項を定めた JIS Q 27001（ISO/IEC 27001）に基づいた認証のことである。

### 2.1.4 ISMS 制度の運用体制

ISMS 制度は、組織が構築した ISMS が JIS Q 27001:2014（ISO/IEC 27001:2013）に適合しているかを審査し登録する「認証機関」、審査員の資格を付与する「要員認証機関」、及びこれらの各機関がその業務を行う能力を備えているのかをみる「認定機関（JIPDEC：一般財団法人日本情報経済社会推進協会）」からなる、総合的な仕組みである。なお、審査員になるために必要な研修を実施する「審査員研修機関」は要員認証機関が承認する。

なお、運用体制については、次の「図 制度のスキーム」を参照されたい。

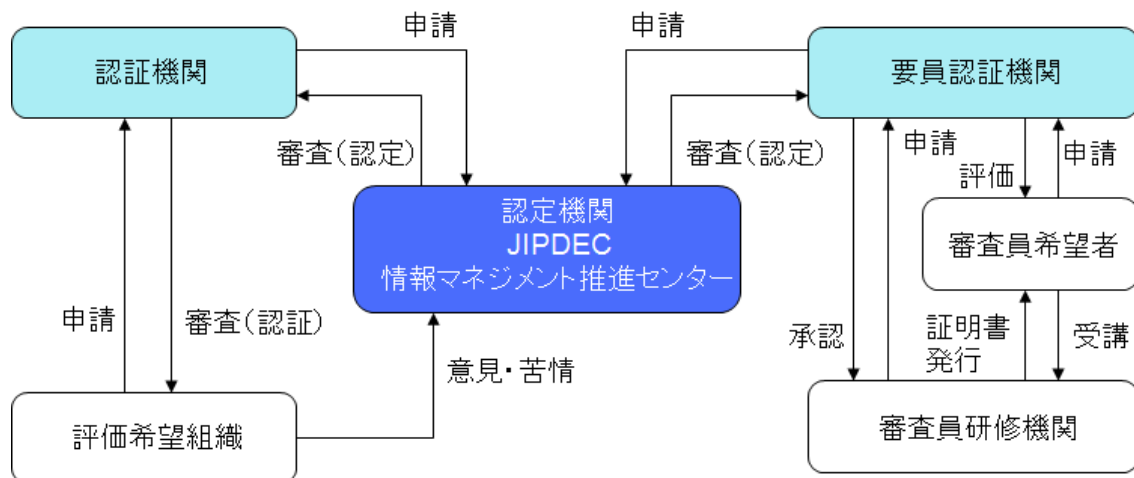


図 制度のスキーム（2015年11月現在）

### 2.1.5 ISMS 制度に関する情報公開

ISMS 制度の概要や認定された ISMS 認証機関及び要員認証機関等については、下記の URL を参照されたい。

- ・ ISMS 適合性評価制度のホームページ <http://www.isms.jipdec.or.jp/>
- ・ ISMS 認証機関一覧 <http://www.isms.jipdec.or.jp/lst/isr/index.html>
- ・ 要員認証機関 <http://www.isms.jipdec.or.jp/youin/lst/isr/index.html>

- ・ 認証取得事業者一覧 <http://www.isms.jipdec.or.jp/lst/ind/index.html>

### 2.1.6 ISMS 制度に関する問い合わせ先

ISMS 制度に関するお問い合わせは、下記 URL を参照されたい。

URL : <http://www.isms.jipdec.or.jp/toiawase.html>

また、入札条件等で ISMS の認証取得を条件にしているケースなどの例や、ISMS 制度の概要と特徴、ISMS 制度と他の情報セキュリティ制度との関連等については、下記 URL の FAQ – よくある質問とその回答集 – を参照されたい。

URL : <http://www.isms.jipdec.or.jp/faq/>

## 2.2 ISMS 制度の活用

各組織又は企業では、委託先の選定に当たり、委託先における事業の安定性に加え、委託する業務の種類に応じて必要とされる情報セキュリティ対策の遂行能力が要求する水準に到達していることを確認することが望ましい。

一般的に ISMS 認証を取得している企業であれば、情報セキュリティマネジメントに関して一定の水準に到達していることを容易に確認でき、これを第三者の認証機関が客観的に評価・認証していることから、委託先の候補者が ISMS 認証を取得しているか否かを委託先の選定における評価に利用することは、極めて効果的かつ信頼性が高いといえる。

具体的には、ISMS 認証は情報セキュリティを確保するための体制の整備、取り扱う組織又は企業の情報の秘密保持等、及び情報セキュリティが侵害された場合の対処といった情報セキュリティ対策を客観的に評価する指標として参考にできる。

技術的なセキュリティ対策の詳細については、認証を取得している事実のみからすべて充足しているとする根拠とはならないことに留意する必要がある。これについては、委託先が、委託先の ISMS を対象として過去に内部監査又は情報セキュリティ監査を行っていた場合に、必要に応じてその結果報告書の提出を求め、確認することもできる。

## 3 ISMS 認証の活用方法

委託先の選定に ISMS 認証を活用する際には、次の文書を確認することが有効である。

### ①登録証

- ・ 認証を取得したことを証する登録証

### ②適用範囲を定義した文書（以下、「適用範囲定義書」と呼ぶ）

- ・ どのような範囲（組織、部門、業務、プロセス、サービス等）で認証を取得したのかを定義

した文書。「適用範囲定義書」と呼ばれることが多い。

### ③適用宣言書等

- ・どのような管理策を実施しているのかを宣言している文書

注記 ②と③の開示には、委託先候補からの同意が必要であり、さらに機密保持に関する契約（NDA）が必要な場合がある。

以下で登録証、適用範囲定義書及び適用宣言書の見方について解説する。

## 3.1 登録証

登録証は、ISMS 認証を取得していることを証した文書であり、JIPDEC が認定した認証機関より発行される。登録証を確認する際のポイントは次の通りである。なお、登録証の例については、付録 1 を参照されたい。

### ①名称及び所在地

- ・適用範囲を示す法人名及び部門名の記載から、委託業務に適しているかどうかについて、ある程度の確認ができる。
- ・例えば、営業部のみが記載されている場合において、開発業務を委託したいという要求に対してすべて充足している根拠とはならない。

### ②登録範囲

- ・登録範囲内の活動（業務プロセスやサービス）の記述から、委託業務に適しているかどうかについて、ある程度の確認ができる。
- ・例えば、システムの開発を委託する予定であるが、システムの運用が登録範囲である場合は、委託内容に対してすべて充足している根拠とはならない。

### ③有効期限

- ・現在も有効な登録であるかどうかについて、有効期限により確認ができる。ただし、有効期限内であっても登録を一時停止されたり抹消されている可能性もあるため、直近の審査報告書の提出を求めることもあり得る。

### ④適用宣言書のバージョン

- ・登録証に記載されている適用宣言書のバージョンと提出された適用宣言書のバージョンが異なっている場合は、変更されている箇所についての説明を求める。

## ⑤ 認証機関

- ・記載されている認証機関の名称、ロゴマーク及び認定シンボルにより、認定されている認証機関であることを確認する。



図 認証機関マークと認定シンボル

■ 認証機関マークと認定シンボルによる認証取得の確認

・認証機関マークの意味合い

認証機関マークは上図「認証機関マークと認定シンボル」の左側部分を指す。

これは、その組織に対して JIS Q 27001:2014 の審査を行い、認証した機関を示している。

・認定シンボルの意味合い

認定シンボルは上図「認証機関マークと認定シンボル」の右側部分を指す。上図の認定シンボルは、JIPDEC の認定を受けた認証機関であることを示す。

JIPDEC の認定は、その認証機関が、適切な ISMS 認証審査を実施することができる体制、及び力量のある ISMS 審査員などを確保すること等について、JIS Q 27006 (ISO/IEC 27006) という ISMS の認証機関に対する要求事項に適合していることを示している。

そのため、認定を受けた認証機関は、適切な ISMS 認証審査を実施することのできる信頼のある ISMS 認証機関であることを意味する。

JIPDEC 認定の ISMS 認証機関は、以下のウェブページで確認することができる。

<http://www.isms.jipdec.or.jp/lst/isr/index.html>

・認証取得の確認

JIPDEC 認定の認証機関による認証を組織が取得すると、上図「認証機関マークと認定

シンボル」の左下部分にある認証登録番号が組織ごとに与えられる。組織が認証を受けているかを確認するためには、認証登録番号や組織名を使って JIPDEC のウェブページで確認することができる。

<http://www.isms.jipdec.or.jp/lst/ind/index.html>

ただし、認証取得について非公開の組織については上記ページ上で確認できない場合もある。その場合には、組織から登録証を提示してもらうか、もしくは登録証のコピーを入手して内容を確認するのが確実である。

※なお、登録証には、認定シンボルが記載されていないものもあるが、そのようなケースは、本書では考慮していない。

### 3.2 適用範囲定義書

ISMS 認証を取得した事業者は、登録証の他に、適用範囲定義書を作成している。適用範囲定義書は、認証を取得している業務やサービス内容を記載しているほか、それを運用している組織やシステム等について組織図やネットワーク構成図を用いて説明している文書である。

この文書では、外部・内部の状況を把握して課題を分析し、例えば「事業、組織、その所在地、資産及び技術」の各特徴の観点から対象とした組織を説明している場合が多く見られる。その内容は、業務を委託する場合の課題を把握するためにも有益であり、委託したい業務プロセスが、それらの中に含まれていることを確認できる。

例えば、委託したい業務と合致していることについて、適用範囲定義書の該当部分を明記し説明することを委託先候補に要求して確認する必要がある。

適用範囲定義書の記載例、及び適用範囲の妥当性の確認の仕方については、付録 2. を参照されたい。なお、組織によっては必ずしも適用範囲定義書という名称を用いているわけではないことに留意すること。

適用範囲を確認する際のポイントは次の通りである。

#### ■ 委託業務との合致

委託を予定している業務が概ね適用範囲と合致していること。

### 3.3 適用宣言書

ISMS 認証を取得した事業者は、適用宣言書を作成している。適用宣言書では、必要な管理策と JIS Q 27001 附属書 A から除外した管理策とそれらの理由、及び必要な管理策を実施しているか否かについて説明している。委託する業務に応じて要求すべき管理策が適切に採用されているかどうかを、最新の適用宣言書において確認する。仮に、一部又は全部の管理策が実施されていない場合









は、その理由が合理的であることを確認する必要がある。例えば、代替的なセキュリティ対策がとられている、もしくはリスクが存在していなかった場合などは、合理的な理由であると判断し得る。

なお、適用宣言書の記載例については、付録 3. を参照されたい。

また、業務を委託するにあたり、その業務における必要な管理策（管理目的）に○印を付けるなどにより管理策（管理目的）の採用を確認することが望ましい。

なお、組織が JIS Q 27001 附属書 A に示す以外にも、追加の管理策を採用している場合には、適用宣言書にはその追加の管理策が記載されている。

付録 1. 登録証 (例)

<p>登録証 (例)</p> <p>株式会社 * * * * * ××部 ①</p> <p>〒***-****</p> <p>東京都千代田区××××</p> <p>上記組織が登録範囲に詳述された活動について JIS Q 27001:2014(ISO/IEC 27001:2013)の要求事項に適合した ISMS を実施していることをここに証します。</p> <p>登録範囲 ②</p> <p>データセンタ事業、運用監視事業、運用委託事業にかかわる情報セキュリティマネジメントシステム</p> <p>登録番号 : ×××××</p> <p>初回登録日 : 2015 年 6 月 1 日</p> <p>有効期限 : 2018 年 5 月 31 日 ③</p> <p>適用宣言書 第 1 版 (2015 年 6 月 1 日付) ④</p> <p>株式会社○○○○審査機構 (ISR○○○) ⑤</p>					
	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th style="width: 50%; padding: 5px;">(認証機関のマーク)</th> <th style="width: 50%; padding: 5px;">(認定マーク)</th> </tr> <tr> <td style="text-align: center; padding: 10px;">  </td> <td style="text-align: center; padding: 10px;">  </td> </tr> </table>	(認証機関のマーク)	(認定マーク)		
(認証機関のマーク)	(認定マーク)				
					

補足 : ①～⑤は、「3.1 登録証」の①～⑤に対応している。

付録 2. 適用範囲定義書 (例)

適用範囲定義書 (例)

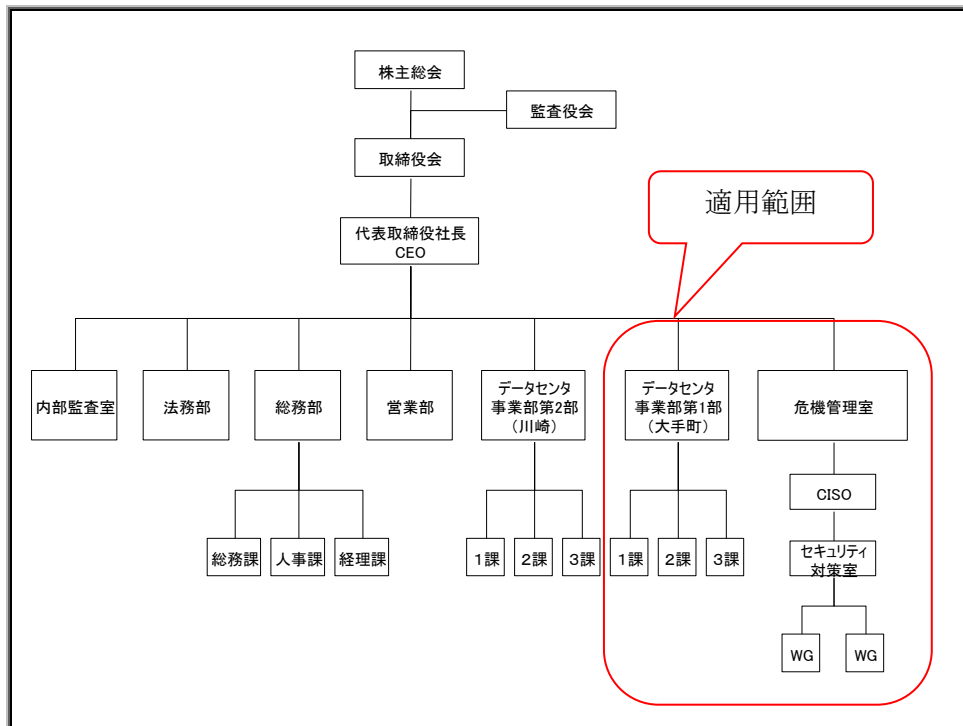
【適用範囲内の主な業務】

データセンタ事業、運用監視事業、運用委託事業

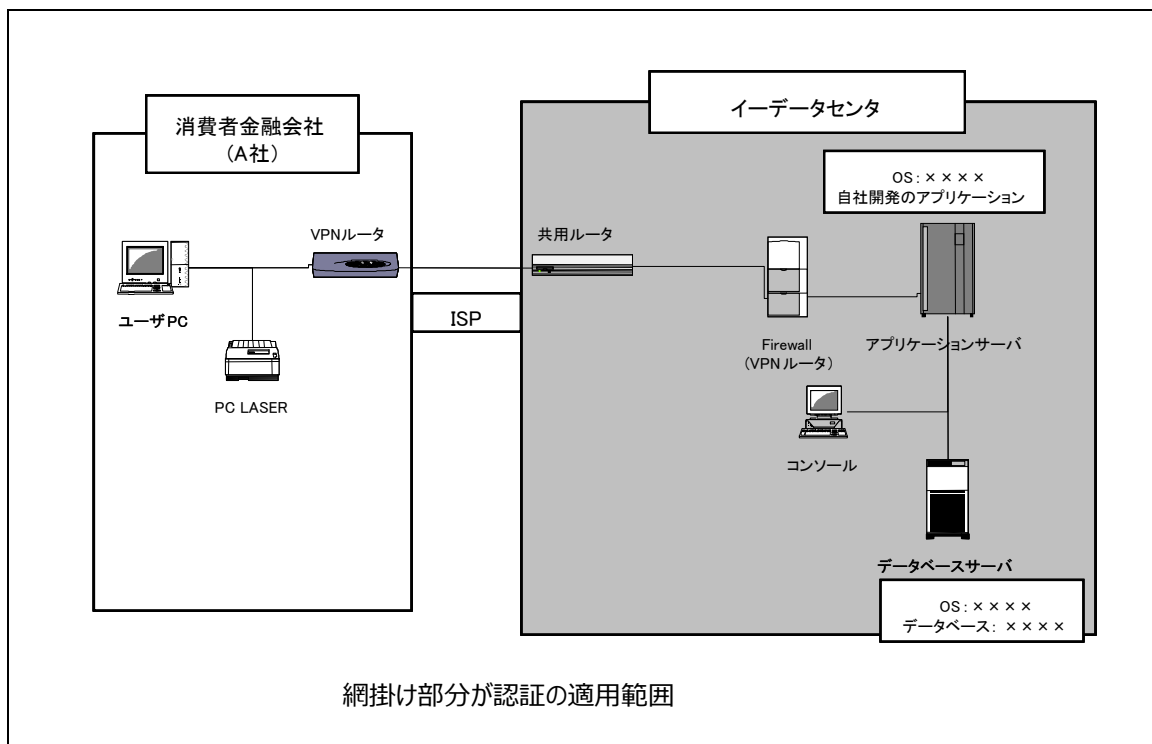
【適用範囲内の要員数】

	従業員 (アルバイトを含む)	派遣社員
大手町事業所	35 名	7 名
全社	150 名	50 名

【組織図】



【適用範囲内のシステム構成】



#### ■ 適用範囲の妥当性確認（例）

##### ① 妥当性を確認できる例

- ・メルマガサービスの委託を予定している。
- ・委託先候補 A に確認したところ、大手町データセンタでメルマガサービスを提供している。
- ・大手町データセンタのすべての業務において認証を取得している。

##### ② 妥当性を確認できない例 1

- ・委託先候補では当該業務を川崎データセンタで行う予定である。
- ・大手町データセンタは認証を取得しているが、川崎データセンタは認証を取得していない。

##### ③ 妥当性を確認できない例 2

- ・大手町データセンタで認証を取得している。
- ・適用範囲に含まれない川崎データセンタの設備を用いたメルマガサービスを用いた提案。

## 付録3. 適用宣言書 (例)

## ■適用宣言書 (例)

適用宣言書 (例)		
附属書 A 管理策		
項番 ①	採否 ②	採否の理由、及び実施の有無 (実施がない場合の理由) ③
A.6.1.1 情報セキュリティの役割及び責任 全ての情報セキュリティの責任を定め、割り当てなければならない。	○	情報セキュリティにおける責任は、職務定義書に記載し実施している。
中略		
A.6.2.2 テレワーキング テレワーキングの場所でアクセス、処理及び保存される情報を保護するために、方針及びその方針を支援するセキュリティ対策を実施しなければならない。	×	在宅勤務をしておらず、遠隔作業を行うこともしていないため。
中略		
A.18.1.5 暗号化機能に対する規制 暗号化機能は、関連する全ての協定、法令及び規制を順守して用いなければならない。	○	「外国為替および外国貿易法」(外為法)を順守するため採用し、暗号化機能への規制への対応手順は整備済み。 実施無：業務が発生していない状況であるため。
以下略		

■ 委託する業務と管理目的との表

次の表は、業務を委託するにあたり、想定されるリスク及び期待される対策などを識別するために、委託業務内容から必要な管理策を判断する際に利用することが出来るような様式である。なお、この表は便宜的に管理目的のみをのせているが、一般的な適用宣言書の様式とは管理策が記載されていない点で異なる。

委託する業務の特徴 情報セキュリティ対策 JIS Q 27001:2014 附属書 A 管理目的	委託業務内容： <input type="checkbox"/> 常駐 <input type="checkbox"/> 非常駐 主なリスクの特定： 期待される対策：	
	必要な対策	備考欄
<b>A.5 情報セキュリティのための方針群</b>		
A.5.1 情報セキュリティのための経営陣の方向性		
<b>A.6 情報セキュリティのための組織</b>		
A.6.1 内部組織		
A.6.2 モバイル機器及びテレワーキング		
<b>A.7 人的資源のセキュリティ</b>		
A.7.1 雇用前		
A.7.2 雇用期間中		
A.7.3 雇用の終了及び変更		
<b>A.8 資産の管理</b>		
A.8.1 資産に対する責任		
A.8.2 情報分類		
A.8.3 媒体の取扱い		
<b>A.9 アクセス制御</b>		
A.9.1 アクセス制御に対する業務上の要求事項		
A.9.2 利用者アクセスの管理		
A.9.3 利用者の責任		
A.9.4 システム及びアプリケーションのアクセス制御		
<b>A.10 暗号</b>		
A.10.1 暗号による管理策		
<b>A.11 物理的及び環境的セキュリティ</b>		
A.11.1 セキュリティを保つべき領域		
A.11.2 装置		

<b>A.12 運用のセキュリティ</b>		
A.12.1	運用の手順及び責任	
A.12.2	マルウェアからの保護	
A.12.3	バックアップ	
A.12.4	ログ取得及び監視	
A.12.5	運用ソフトウェアの管理	
A.12.6	技術的せい弱性管理	
A.12.7	情報システムの監査に対する考慮事項	
<b>A.13 通信のセキュリティ</b>		
A.13.1	ネットワークセキュリティ管理	
A.13.2	情報の転送	
<b>A.14 システムの取得, 開発及び保守</b>		
A.14.1	情報システムのセキュリティ要求事項	
A.14.2	開発及びサポートプロセスにおけるセキュリティ	
A.14.3	試験データ	
<b>A.15 供給者関係</b>		
A.15.1	供給者関係における情報セキュリティ	
A.15.2	供給者のサービス提供の管理	
<b>A.16 情報セキュリティインシデント管理</b>		
A.16.1	情報セキュリティインシデントの管理及びその改善	
<b>A.17 事業継続マネジメントにおける情報セキュリティの側面</b>		
A.17.1	情報セキュリティ継続	
A.17.2	冗長性	
<b>A.18 順守</b>		
A.18.1	法的及び契約上の要求事項の順守	
A.18.2	情報セキュリティのレビュー	

## 付録4. JIS Q 27001 附属書 A 管理目的

<b>JIS Q 27001:2014</b>	
<b>項番</b>	<b>条文</b>
<b>A.5</b>	<b>情報セキュリティのための方針群</b>
A.5.1	<b>情報セキュリティのための経営陣の方向性</b> 目的： 情報セキュリティのための経営陣の方向性及び支持を，事業上の要求事項並びに関連する法令及び規制に従って提示するため。
<b>A.6</b>	<b>情報セキュリティのための組織</b>
A.6.1	<b>内部組織</b> 目的： 組織内で情報セキュリティの実施及び運用に着手し，これを統制するための管理上の枠組みを確立するため。
A.6.2	<b>モバイル機器及びテレワーキング</b> 目的： モバイル機器の利用及びテレワーキングに関するセキュリティを確実にするため。
<b>A.7</b>	<b>人的資源のセキュリティ</b>
A.7.1	<b>雇用前</b> 目的： 従業員及び契約相手がその責任を理解し，求められている役割にふさわしいことを確実にするため。
A.7.2	<b>雇用期間中</b> 目的： 従業員及び契約相手が，情報セキュリティの責任を認識し，かつ，その責任を遂行することを確実にするため。
A.7.3	<b>雇用の終了及び変更</b> 目的： 雇用の終了又は変更のプロセスの一部として，組織の利益を保護するため。
<b>A.8</b>	<b>資産の管理</b>
A.8.1	<b>資産に対する責任</b> 目的： 組織の資産を特定し，適切な保護の責任を定めるため。
A.8.2	<b>情報分類</b> 目的： 組織に対する情報の重要性に応じて，情報の適切なレベルでの保護を確実にするため。
A.8.3	<b>媒体の取扱い</b> 目的： 媒体に保存された情報の認可されていない開示，変更，除去又は破壊を防止するため。
<b>A.9</b>	<b>アクセス制御</b>



A.9.1	<b>アクセス制御に対する業務上の要求事項</b> 目的： 情報及び情報処理施設へのアクセスを制限するため。
A.9.2	<b>利用者アクセスの管理</b> 目的： システム及びサービスへの、認可された利用者のアクセスを確実にし、認可されていないアクセスを防止するため。
A.9.3	<b>利用者の責任</b> 目的： 利用者に対して、自らの秘密認証情報を保護する責任をもたせるため。
A.9.4	<b>システム及びアプリケーションのアクセス制御</b> 目的： システム及びアプリケーションへの、認可されていないアクセスを防止するため。
<b>A.10</b>	<b>暗号</b>
A.10.1	<b>暗号による管理策</b> 目的： 情報の機密性、真正性及び／又は完全性を保護するために、暗号の適切かつ有効な利用を確実にするため。
<b>A.11</b>	<b>物理的及び環境的セキュリティ</b>
A.11.1	<b>セキュリティを保つべき領域</b> 目的： 組織の情報及び情報処理施設に対する認可されていない物理的アクセス、損傷及び妨害を防止するため。
A.11.2	<b>装置</b> 目的： 資産の損失、損傷、盗難又は劣化、及び組織の業務に対する妨害を防止するため。
<b>A.12</b>	<b>運用のセキュリティ</b>
A.12.1	<b>運用の手順及び責任</b> 目的： 情報処理設備の正確かつセキュリティを保った運用を確実にするため。
A.12.2	<b>マルウェアからの保護</b> 目的： 情報及び情報処理施設がマルウェアから保護されることを確実にするため。
A.12.3	<b>バックアップ</b> 目的： データの消失から保護するため。
A.12.4	<b>ログ取得及び監視</b> 目的： イベントを記録し、証拠を作成するため。
A.12.5	<b>運用ソフトウェアの管理</b> 目的： 運用システムの完全性を確実にするため。

A.12.6	<b>技術的ぜい弱性管理</b> 目的： 技術的ぜい弱性の悪用を防止するため。
A.12.7	<b>情報システムの監査に対する考慮事項</b> 目的： 運用システムに対する監査活動の影響を最小限にするため。
<b>A.13</b>	<b>通信のセキュリティ</b>
A.13.1	<b>ネットワークセキュリティ管理</b> 目的： ネットワークにおける情報の保護，及びネットワークを支える情報処理施設の保護を確実にするため。
A.13.2	<b>情報の転送</b> 目的： 組織の内部及び外部に転送した情報のセキュリティを維持するため。
<b>A.14</b>	<b>システムの取得，開発及び保守</b>
A.14.1	<b>情報システムのセキュリティ要求事項</b> 目的： ライフサイクル全体にわたって，情報セキュリティが情報システムに欠くことのできない部分であることを確実にするため。これには，公衆ネットワークを介してサービスを提供する情報システムのための要求事項も含む。
A.14.2	<b>開発及びサポートプロセスにおけるセキュリティ</b> 目的： 情報システムの開発サイクルの中で情報セキュリティを設計し，実施することを確実にするため。
A.14.3	<b>試験データ</b> 目的： 試験に用いるデータの保護を確実にするため。
<b>A.15</b>	<b>供給者関係</b>
A.15.1	<b>供給者関係における情報セキュリティ</b> 目的： 供給者がアクセスできる組織の資産の保護を確実にするため。
A.15.2	<b>供給者のサービス提供の管理</b> 目的： 供給者との合意に沿って，情報セキュリティ及びサービス提供について合意したレベルを維持するため。
<b>A.16</b>	<b>情報セキュリティインシデント管理</b>
A.16.1	<b>情報セキュリティインシデントの管理及びその改善</b> 目的： セキュリティ事象及びセキュリティ弱点に関する伝達を含む，情報セキュリティインシデントの管理のための，一貫性のある効果的な取り組みを確実にするため。
<b>A.17</b>	<b>事業継続マネジメントにおける情報セキュリティの側面</b>
A.17.1	<b>情報セキュリティ継続</b> 目的： 情報セキュリティ継続を組織の事業継続マネジメントシステムに組み込まなければ

	ばならない。
A.17.2	<b>冗長性</b> 目的： 情報処理施設の可用性を確実にするため。
<b>A.18</b>	<b>順守</b>
A.18.1	<b>法的及び契約上の要求事項の順守</b> 目的： 情報セキュリティに関連する法的、規制又は契約上の義務に対する違反、及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。
A.18.2	<b>情報セキュリティのレビュー</b> 目的： 組織の方針及び手順に従って情報セキュリティが実施され、運用されることを確実にするため。

## おわりに

本ガイドは、委託先候補における情報セキュリティ対策の履行状況を確認する手段として ISMS 適合性評価制度を利用する場合の解説書として活用することを目的としており、本制度が委託先を選定するための有効な方法の一つであることをご理解いただければ幸いです。なお、本ガイドでご紹介している方法は、あくまでも一例であり委託先を選定する際の組織又は企業における全ての要件を満たしているものではないことにご留意願いたい。

ISMS 技術専門部会

(順不同・敬称略)

氏名	会社・機関名
駒瀬 彰彦	株式会社アズジェント【主査】
丸山 満彦	デロイト トーマツ リスクサービス株式会社【副主査】
相羽 律子	株式会社日立製作所 情報・通信システム社
小寺 くれは	KPMG コンサルティング株式会社
佐藤 慶浩	株式会社 日本 HP
竹下 和孝	株式会社筑波総合研究所
中村 良和	日本マネジメントシステム認証機関協議会 (BSI グループジャパン株式会社)
平野 芳行	独立行政法人 情報処理推進機構
松尾 正浩	株式会社三菱総合研究所
事務局	
一般財団法人 日本情報経済社会推進協会 情報マネジメント推進センター	

(2015年11月30日現在)