NCWGクラウドセキュリティセミナー

第二回「実践クラウドセキュリティ」研修会

クラウドを安心して使うための セキュリティのポイント解説

2015年2月2日

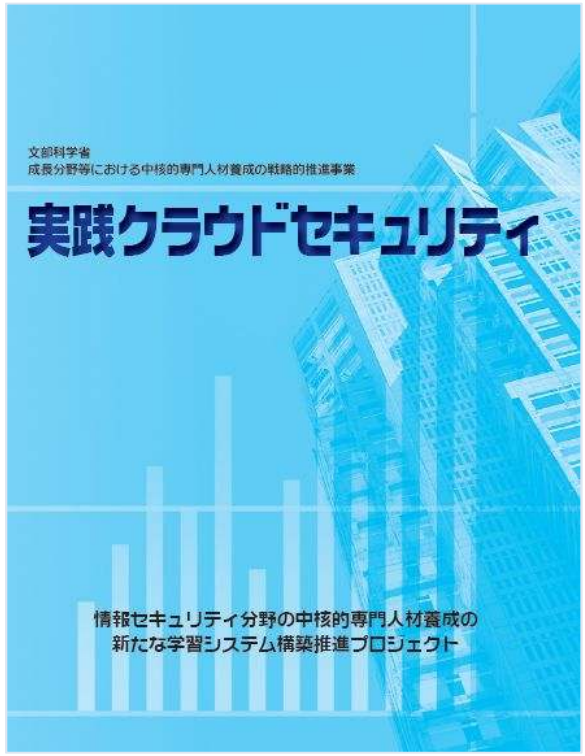
株式会社ディアイティ　山田 英史

目次

1. クラウドサービスにおける情報セキュリティ
2. クラウドサービスのセキュリティの要件
3. クラウドサービスのSLA、規約の解釈

はじめに

- 本資料は、平成25年度 文部科学省「成長分野等における中核的専門人材養成の戦略的推進事業」の一環で作成した教科書『実践クラウドセキュリティ』の3章～6章の代表的な項目を取り上げ、解説したものである。
  - 平成25年度 事業成果　http://25monka-itaku.net/security/

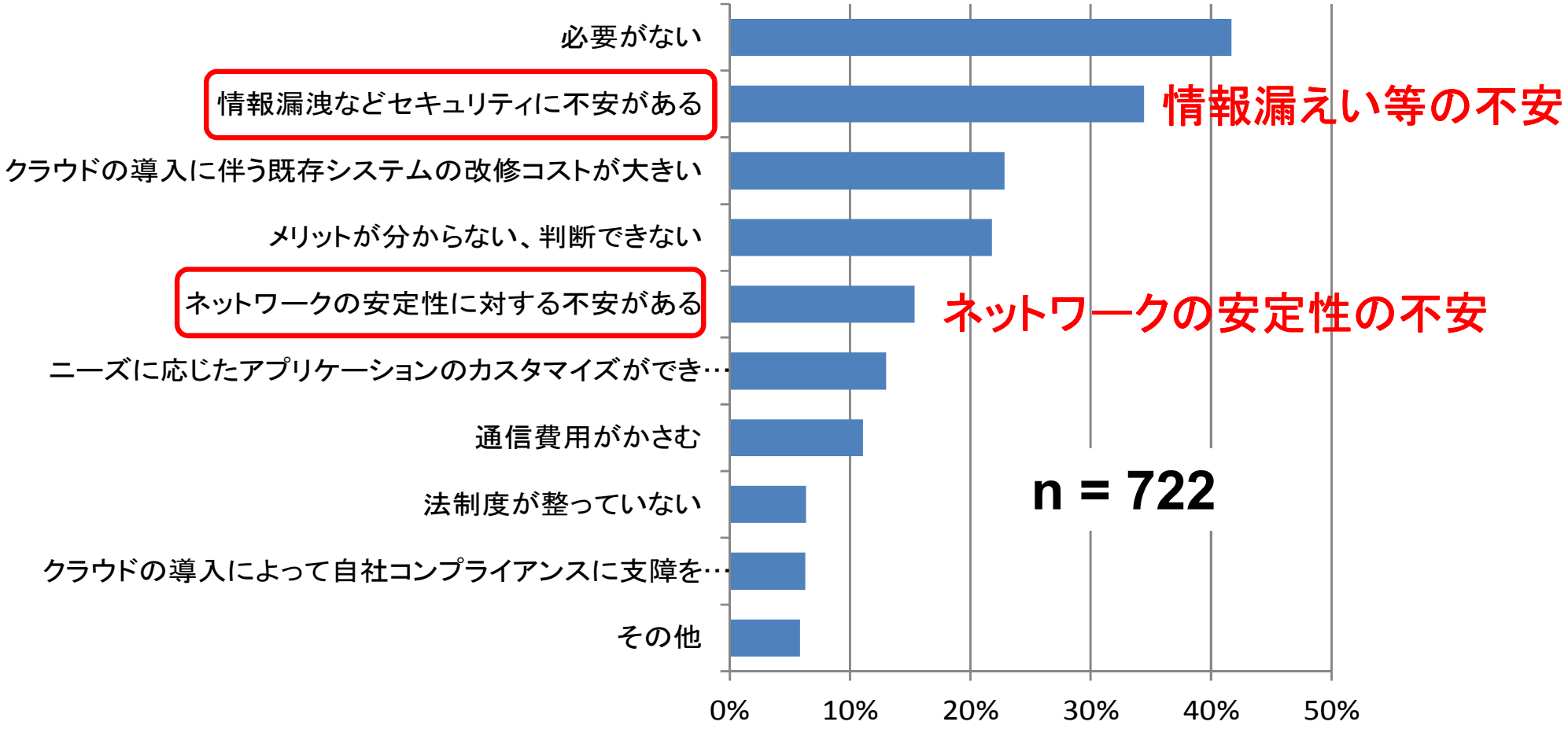


1. クラウドサービスにおける情報セキュリティ

教科書 76ページ

クラウドサービスに対する不安と期待(1/2)

クラウドサービスを導入しない理由

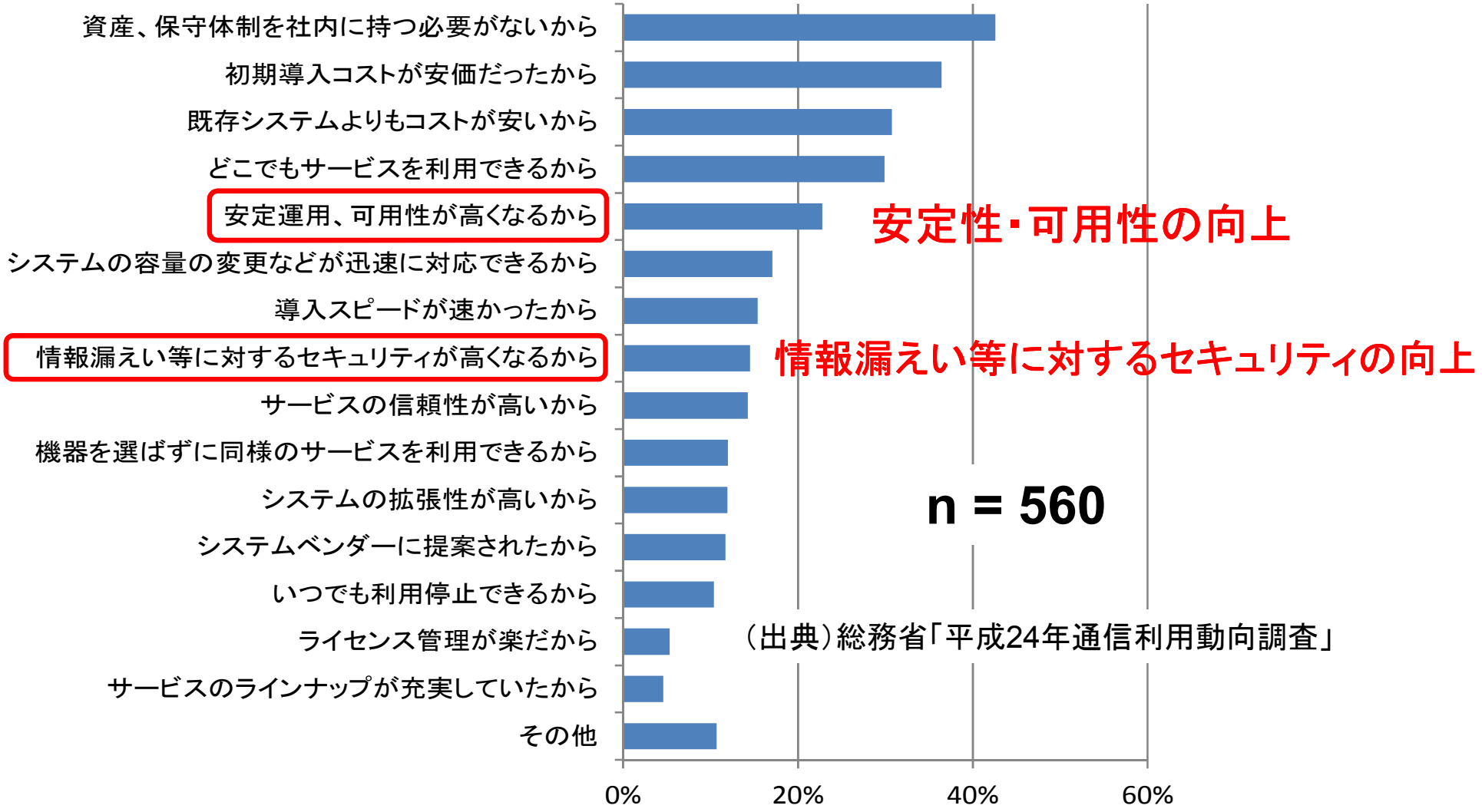


(出典)総務省「平成24年通信利用動向調査」

教科書 77ページ

クラウドサービスに対する不安と期待(2/2)

クラウドサービスの導入理由



クラウドを安心して使うために

クラウドを安心して使うために

↓

安全なクラウドを選定する

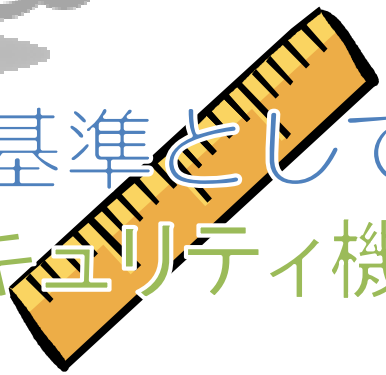
↓

安全なクラウドとは？

教科書 77ページ

システム要件定義の必要性

クラウドに対する漠然とした不安



選定基準としてのシステム要件の定義

セキュリティ機能・性能を明確に定義

クラウドの評価

不安の払拭

クラウド選定

教科書 78ページ

セキュリティ要件定義の方法

セキュリティ要件定義の考え方

階層	概要
機　能	システムやサービスに機能として実装するセキュリティ機能要件。 機能と併せ、処理能力、応答性、容量等の性能も要件に含む。
維持・運用管理	実装した機能を維持するための要件、及び機能として実装できなかったセキュリティ対策の代替策としての運用によるセキュリティ要件。
利　用	システムの利用（入力、処理、出力、保存、移送）におけるセキュリティ要件。
開発・変更工程	システムの開発・変更の工程におけるセキュリティ確保のための要件。

教科書 79ページ

クラウドサービス特有のシステム構成・運用環境

直接管理できないリスク

- 直接コントロールできなくなる
- 直接モニタリングできなくなる

新たな機能に関連する新たなリスク

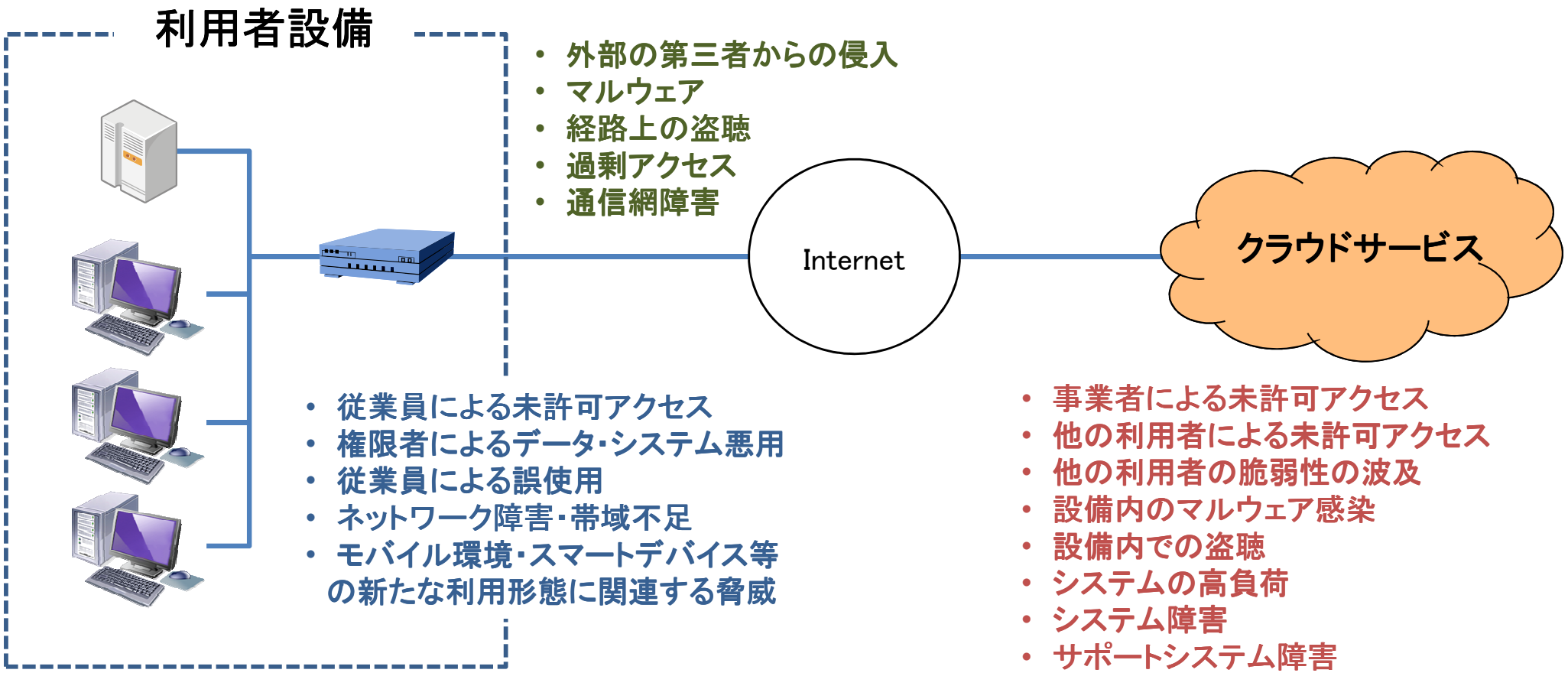
- 仮想化技術の脆弱性
- ネットワークへの依存

利用方法の拡大による新たなリスク

- モバイル環境の導入
- スマートデバイスの利用

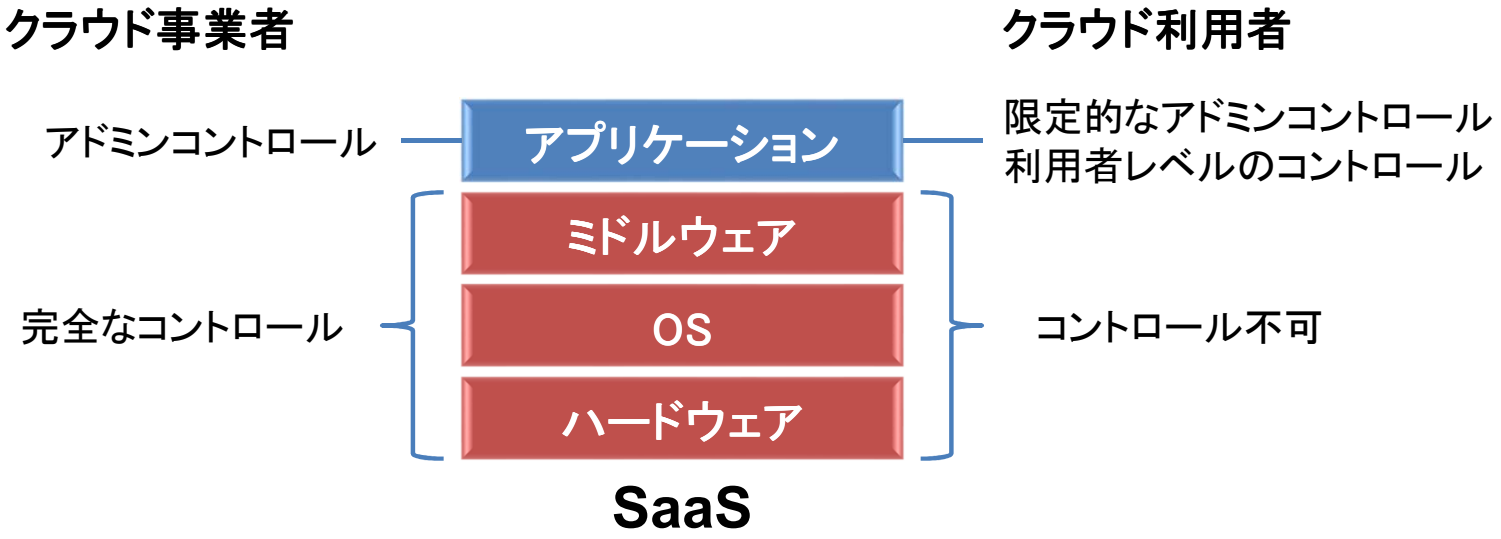
教科書 86ページ

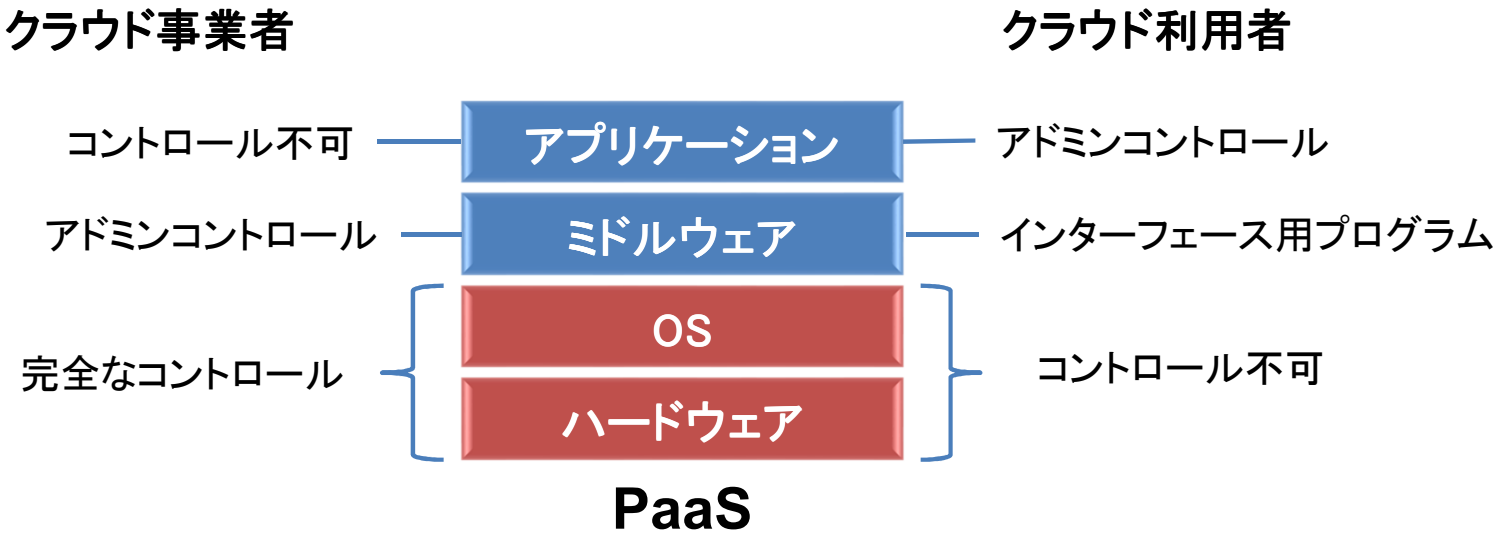
クラウドサービス利用における脅威の洗い出し



教科書 87ページ

クラウド提供者と利用者の管理範囲(1/2)

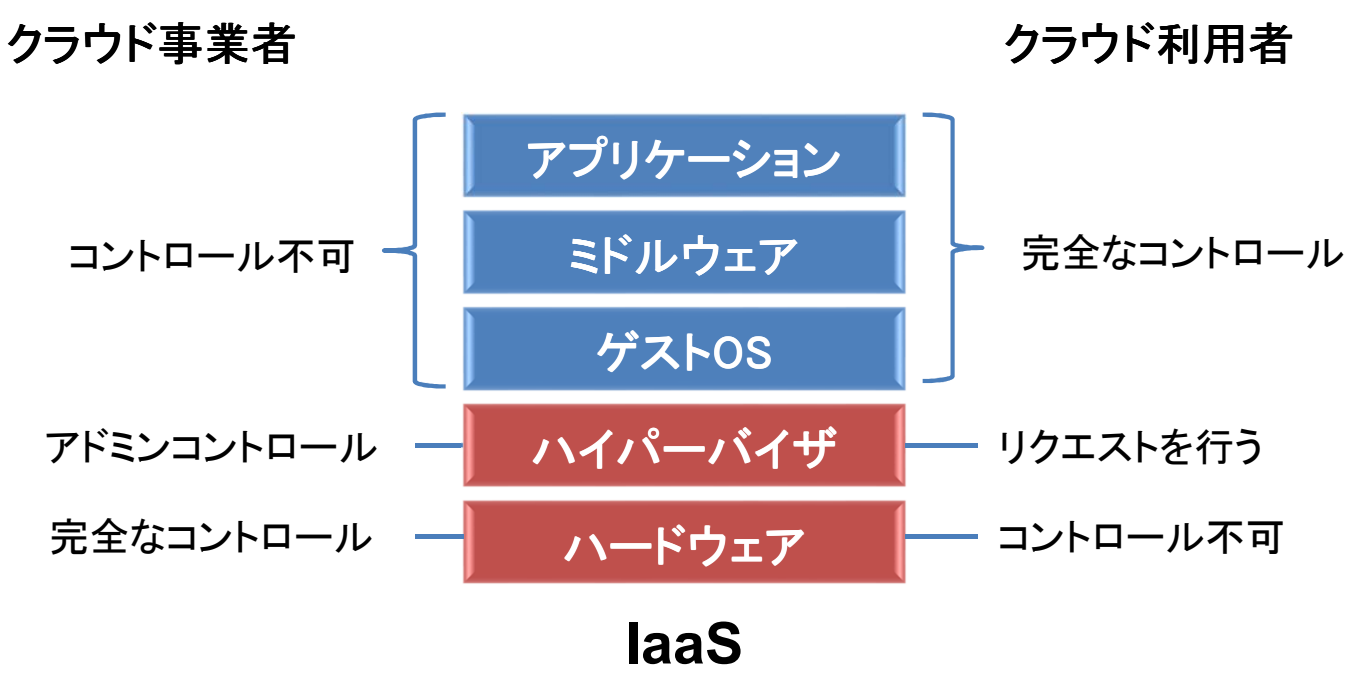




参考：NIST SP800-146『クラウドコンピューティングの 概要と推奨事項』IPA翻訳版

教科書 87ページ

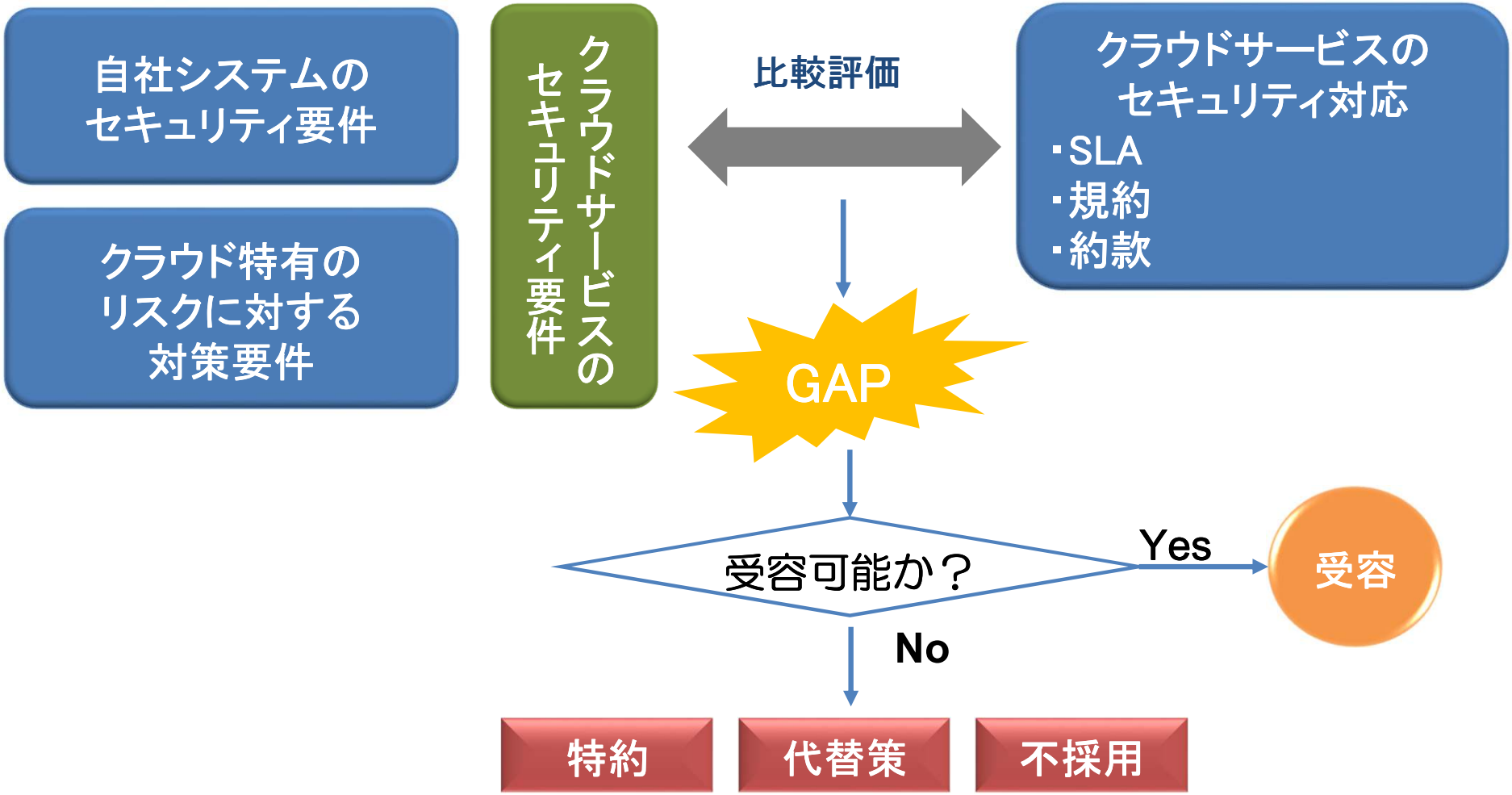
クラウド事業者と利用者の管理範囲(2/2)



参考：NIST SP800-146『クラウドコンピューティングの 概要と推奨事項』IPA翻訳版

教科書 94ページ

クラウドサービスの選定



2. クラウドセキュリティの要件

教科書 102ページ

クラウドセキュリティの検討のためのガイドラインの利用(1/2)

■ 経済産業省『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』の概要

•本ガイドラインの箇条5～15は，クラウド利用者がJIS Q 27002(実践のための規範)の箇条5～15の管理策を実施するための補足として活用できる。
•参考として附属書Aは，クラウドサービス利用に係るリスクを例示し，附属書Bは，クラウドサービス利用におけるリスクアセスメントの実施例の一つを示す。

序文
0.1 一般
0.2 クラウドサービス及び情報セキュリティ
0.3 このガイドラインの位置づけ及び構成

1 適用範囲
2 引用規格
3 用語及び定義
4 クラウドサービス利用における情報セキュリティガバナンス及び情報セキュリティマネジメント
4.1 クラウドサービス利用における情報セキュリティガバナンス
4.2 クラウドサービス利用における情報セキュリティマネジメント

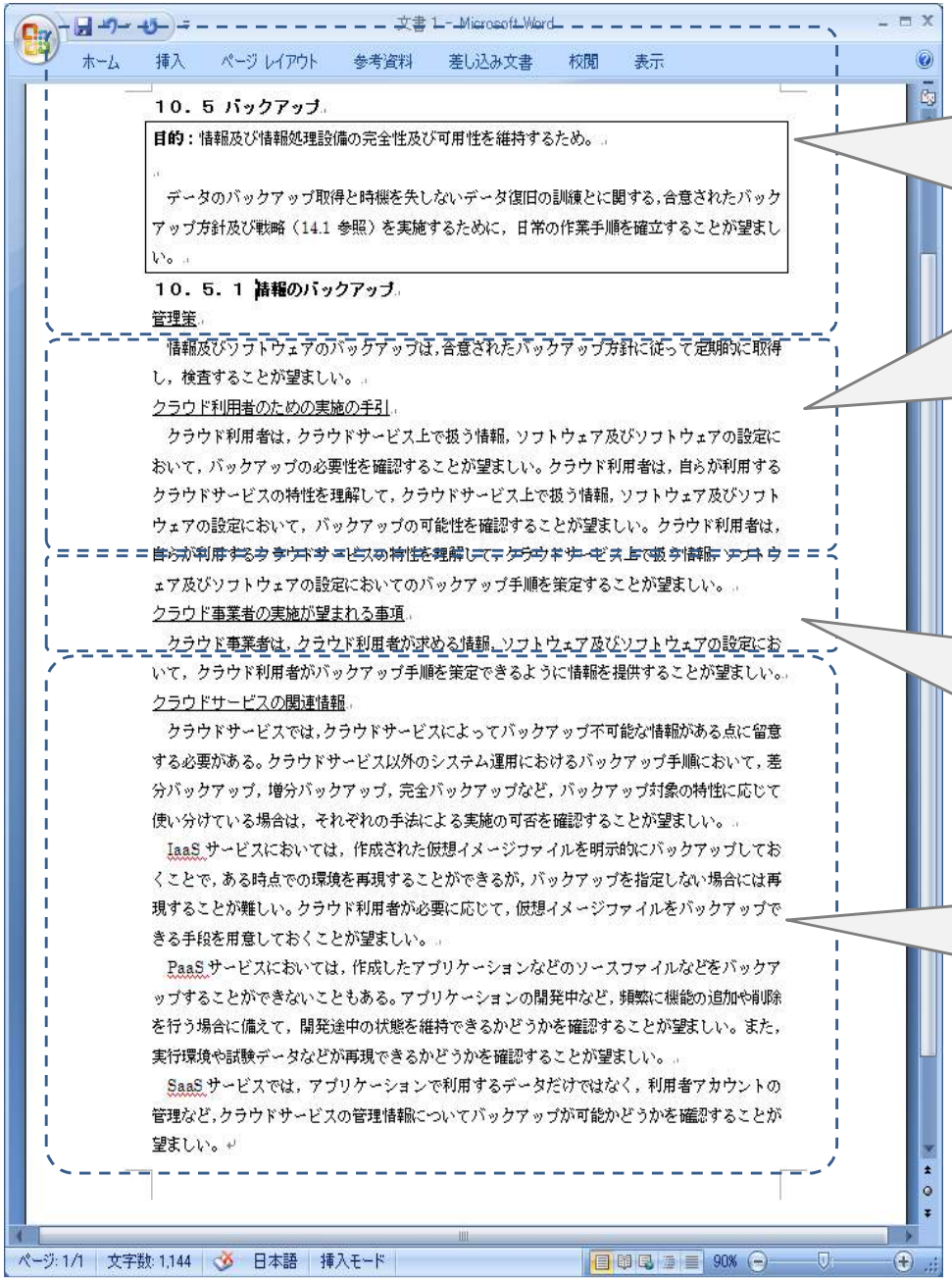
5 セキュリティ基本方針
6 情報セキュリティのための組織
7 資産の管理
8 人的資源のセキュリティ
9 物理的及び環境的セキュリティ
10 通信及び運用管理
11 アクセス制御
12 情報システムの取得，開発及び保守
13 情報セキュリティインシデントの管理
14 事業継続管理
15 順守

附属書 A(参考) クラウドサービス利用に係るリスク
附属書 B (参考)クラウド利用におけるリスクアセスメントの実施例

引用: 経済産業省資料

教科書 103ページ

クラウドセキュリティの検討のためのガイドラインの利用(2/2)



目的と管理策

目的と管理策は，情報セキュリティ管理における目的が変更されないように，JIS Q 27002(実践のための規範)をそのまま引用している。それぞれの実施項目の必要性や背景などを理解するため，また，情報セキュリティ監査に利用する場合にも目的を明確にするために利用出来る。

クラウド利用者のための実施の手引

クラウドサービス利用において，クラウド利用者が実施する管理策を支持し，管理目的を満たすための情報を提供する。この手引にはすべての場合に適していないものもあるため，他の方法でその管理策を実施する方がより適切な場合もある。

クラウド事業者の実施が望まれる事項

クラウドサービス利用において，クラウド事業者の協力が必要となる管理策については，クラウド利用者が実施する管理策を支持し，管理目的を満たすために，クラウド事業者の実施が望まれる事項に係る情報を提供する。

クラウドサービスの関連情報

クラウドサービス利用において考慮が必要と思われる関連情報(関連するクラウドサービスの種類，利用環境又は利用技術に関する情報など)を提供する。

注)クラウド固有の事項がない場合は，それぞれの項目は記載していない

引用：経済産業省資料

教科書 103ページ

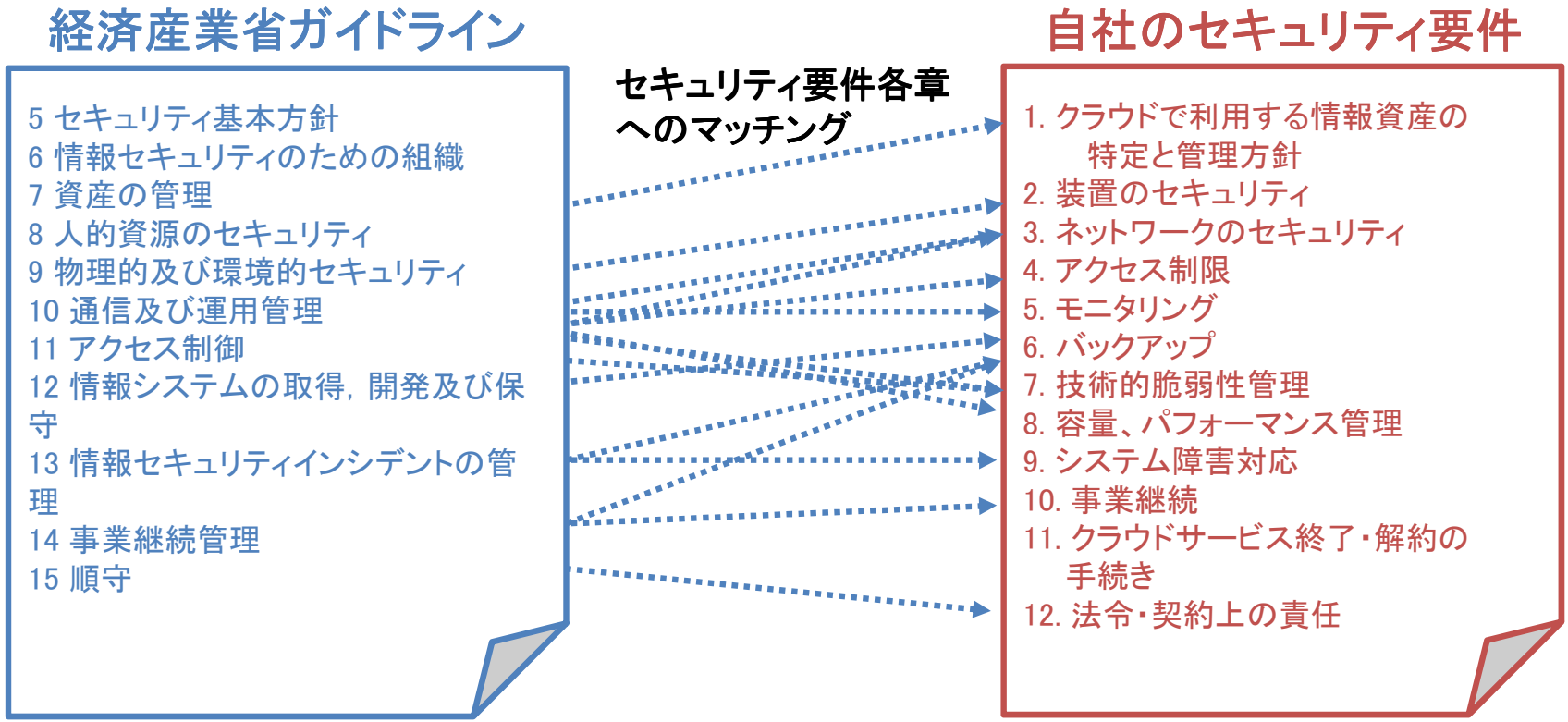
クラウドセキュリティ要件の編集方法

- 以下のシステム機能と運用に関連する事項のセキュリティ要件の洗い出しについて解説する。
  1. クラウドで利用する情報資産の特定と管理方針
  2. 装置のセキュリティ
  3. ネットワークのセキュリティ
  4. アクセス制限
  5. モニタリング
  6. バックアップ
  7. 技術的脆弱性管理
  8. 容量、パフォーマンス管理
  9. システム障害対応
  10. 事業継続
  11. クラウドサービス終了・解約の手続き
  12. 法令・契約上の責任
- ガバナンス、マネジメントおよびシステム開発・変更に関わるセキュリティ要件は対象外とした。

教科書 104ページ

セキュリティ対策（管理策）の選定（1/2）

- 前ページに挙げた管理項目を実施するために経済産業省ガイドラインのどの管理策を適用すべきか検討する。



教科書 104ページ

セキュリティ対策（管理策）の選定（2/2）

ガイドラインと管理項目の対応表（例）

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			クラウドで利用する情報資産の特定と管理方針	装置のセキュリティ	ネットワークのセキュリティ	アクセス制限	モニタリング	バックアップ	技術的脆弱性管理	容量、パフォーマンス管理	システム障害対応	事業継続	クラウドサービス終了・解約の手続き	法令・契約上の責任
11 アクセス制御	11.1 アクセス制御に対する業務上の要求事項	11.1.1 アクセス制御方針				●								
	11.2 利用者アクセスの管理	11.2.1 利用者登録				●								
		11.2.2 特権管理				●								
		11.2.3 利用者パスワードの管理				●								
		11.2.4 利用者アクセス権のレビュー				●								
	11.3 利用者の責任	11.3.1 パスワードの利用				●								
		11.3.2 無人状態にある利用者装置												
		11.3.3 クリアデスク，クリアスクリーン方針												
	11.4 ネットワークのアクセス制御	11.4.1 ネットワークサービスの利用についての方針			●									
		11.4.2 外部から接続する利用者の認証			●	●								
		11.4.3 ネットワークにおける装置の識別			●									
		11.4.4 遠隔診断用及び環境設定用ポートの保護			●									
		11.4.5 ネットワークの領域分割			●									
		11.4.6 ネットワークの接続制御			●									
		11.4.7 ネットワークルーティング制御			●									
	11.5 オペレーティングシステムのアクセス制御	11.5.1 セキュリティに配慮したログオン手順				●								
		11.5.2 利用者の識別及び認証				●								
		11.5.3 パスワード管理システム				●								
		11.5.4 システムユーティリティの使用							●					
		11.5.5 セッションのタイムアウト				●								
		1.5.6 接続時間の制限				●								
	11.6 業務用ソフトウェア及び情報のアクセス制御	11.6.1 情報へのアクセス制限				●								
		11.6.2 取扱いに慎重を要するシステムの隔離				●								
	11.7 モバイルコンピューティング及びテレワーキング	11.7.1 モバイルのコンピューティング及び通信			●									
		11.7.2 テレワーキング			●									

クラウドセキュリティ要件の解説について

- 各要件の解説は、「目的」「クラウド利用者が要件定義で検討すること」「クラウド事業者に確認する事項」で構成する。
- 目的
  - 対象となるセキュリティ要件をなぜ定める必要があるのか、どのようなリスクを想定した要件なのか等を記述。
- クラウド利用者が要件定義で検討すること
  - セキュリティ要件定義を策定するために検討し決定すべき事項を記述。ここではクラウドサービス特有の要件に限らず、システム仕様を決める際に必要な一般的な事項を取り上げる。
- クラウド事業者に確認する事項
  - 上で記述した要件をクラウドサービスに適用する場合に、その実現性について事業者に確認する事項を記述。

教科書 117ページ

4. アクセス制限(1/2)

目的	提供されるクラウドサービスへのアクセス制御及びクラウドサービス上の利用者の情報への未許可アクセス及び誤用、悪用から保護するための、本人認証をベースにしたアクセス制御を行います。
クラウド利用者が要件定義で検討する事項	a. アクセス制御方針の決定。 b. アクセス制御を実装する階層の決定。 c. アクセス制限技術の適用。 d. アクセス権管理の原則の定義。 e. 本人確認に基づく認証 f. 権限の分割。 g. ID/パスワードの登録・発行・変更・停止・削除機能の実装。 h. パスワード保護。 i. 正式なログオン機能の定義。 j. アクセス権の維持・管理。

教科書 119ページ

4. アクセス制限(2/2)

クラウド事業者に確認する事項	a. アクセス制御可能な階層。 b. 利用できるアクセス制限技術。 c. アクセス権管理機能。 d. 仮想環境の隔離の方法。 e. 利用者ID/パスワード管理の機能と設定項目。 f. パスワード保護方法。 g. ログオン手順。 h. 既存の認証システム等との連動性。 i. 選択可能な暗号機能。

教科書 121ページ

5. モニタリング

目的	システム障害や不正行為の検知、記録、原因究明のためにイベントログの取得と分析、及び運用の正当性や不正行為の裏付けとしての管理者／ユーザの作業記録の取得・分析といったモニタリングを行います。
クラウド利用者が要件定義で検討する事項	a. モニタリングの目的の明確化。 b. 目的に応じた記録の決定。 c. 記録の保存期間の決定。 d. 記録保護方法の決定。 e. 記録の評価手順の策定。 f. 監視の適用。 g. 法的証拠の保全。 h. 時間の同期。
クラウド事業者に確認する事項	a. 利用者がコントロール可能なログの範囲。 b. 利用者によるログ管理の機能。 c. 事業者からの記録の開示及び通知。 d. ログ保存に利用できるストレージ容量。 e. ログ等記録の保護方法。 f. 利用可能な監視機能。 g. 時間同期方法。 h. ログ統合管理ツールとの連携。

教科書 122ページ

6. バックアップ

目的	システム障害やインシデントによりクラウドサービスが利用できなくなる、あるいはデータが消失したといった状況が発生することを想定し、事業の継続及び速やかな復旧のためのバックアップを実施します。
クラウド利用者が要件定義で検討する事項	a. バックアップの目的の明確化。 b. 目的に応じたバックアップ項目の決定。 c. バックアップ方法の決定 d. バックアップの保存期間の決定。 e. バックアップの保護方法の決定。 f. バックアップの検証。
クラウド事業者に確認する事項	a. バックアップ管理の責任範囲。 b. 利用者によるバックアップ管理の機能。 c. 事業者によるバックアップの範囲と方法。 d. バックアップ保存に利用できるストレージ容量。 e. バックアップの保護方法 f. バックアップからの復旧方法。

9. システム障害対応

目的	クラウド設備、インターネット、利用者内システムが複合的に連携したクラウドコンピューティング環境では、システム障害の原因の切り分けが難しく、また、責任分界や障害対応の役割が曖昧であると速やかな対応が取れません。障害の検知、原因究明、復旧のための関係者の協力体制、対応手順を整備します。
クラウド利用者が要件定義で検討する事項	a. システム保守契約の締結。 b. 記録の活用。 c. システム障害対応の手順の策定。 d. システム障害対応の手順の検証。 e. SLAの維持または違反の証跡の入手。
クラウド事業者に確認する事項	a. システム障害対応における利用者と事業者の責任範囲。 b. 事業者の対応窓口。 c. システム障害の協力体制。 d. 障害情報の入手方法。 e. SLAの維持または違反証跡の入手方法。

教科書 130ページ

11. クラウドサービス終了・解約の手続き

目的	クラウドサービス終了の条件、解約の手続き及びデータ移行、残留データの消去といった確認事項を明らかにします。
クラウド利用者が要件定義で検討する事項	a. クラウドサービスの終了時の情報資産の回収と消去。 b. クラウドサービスの移譲に伴う情報資産への影響の評価。
クラウド事業者に確認する事項	a. クラウドサービスの終了・解約の条件と手続き。 b. クラウドサービスの終了・解約の情報資産の回収と消去の手続き。 c. クラウドサービス移譲の影響の確認。

教科書 131ページ

12. 法令・契約上の責任

目的	クラウドサービスのデータセンターが海外にある場合は、その所在地の国のデータ保護法法令、個人情報保護法令等の影響を受けます。法令による影響を知り、クラウドサービス選定時に留意すべき事項を明らかにします。
クラウド利用者が要件定義で検討する事項	a. 情報資産の物理的な所在地による法規制の影響の評価。 b. 業界ガイドラインの影響の評価。 c. 情報資産の所有権の明確化。
クラウド事業者に確認する事項	a. クラウド上の利用者情報資産の物理的な所在地。 b. 考慮すべき法的リスク。 c. 捜査機関への協力に関するリスク。 d. ライセンスの所有権。

教科書 132ページ

クラウドサービス選定のためのチェックリストの例(1/2)

管理項目	No.	セキュリティ要件	評価	コメント
アクセス制御	1	クラウドサービスへのログインを、ID／パスワード認証により制限できること。		
	2	ユーゼの権限により表示するメニューが制限できること。		
	3	処理機能毎にユーザの権限に応じて、登録・参照・変更・削除の設定が行えること。		
	4	各ユーザに一意のIDの付与できること。		
	5	共有IDを利用する場合は、以下のいずれかの条件が満たせること。 ・業務上の利点がある例外的状況においてのみ、システム管理者の承認を得た上で使用する。 ・ID利用者の行動について追跡性を維持するための管理策を導入する。(共有IDのパスワードを一度に一人の要員だけに発行し、その使用事例のログを取る等) ・そのIDによって利用可能な機能又は行動を追跡する必要がない場合。(読出し専用アクセス等)		
	6	パスワードは、10文字以上が設定でき、英小文字／英大文字／数字／記号の内3種類以上で構成できること。		
	7	ID／パスワード管理が、既存のアカウント管理サーバと連携できること。		

教科書 132ページ

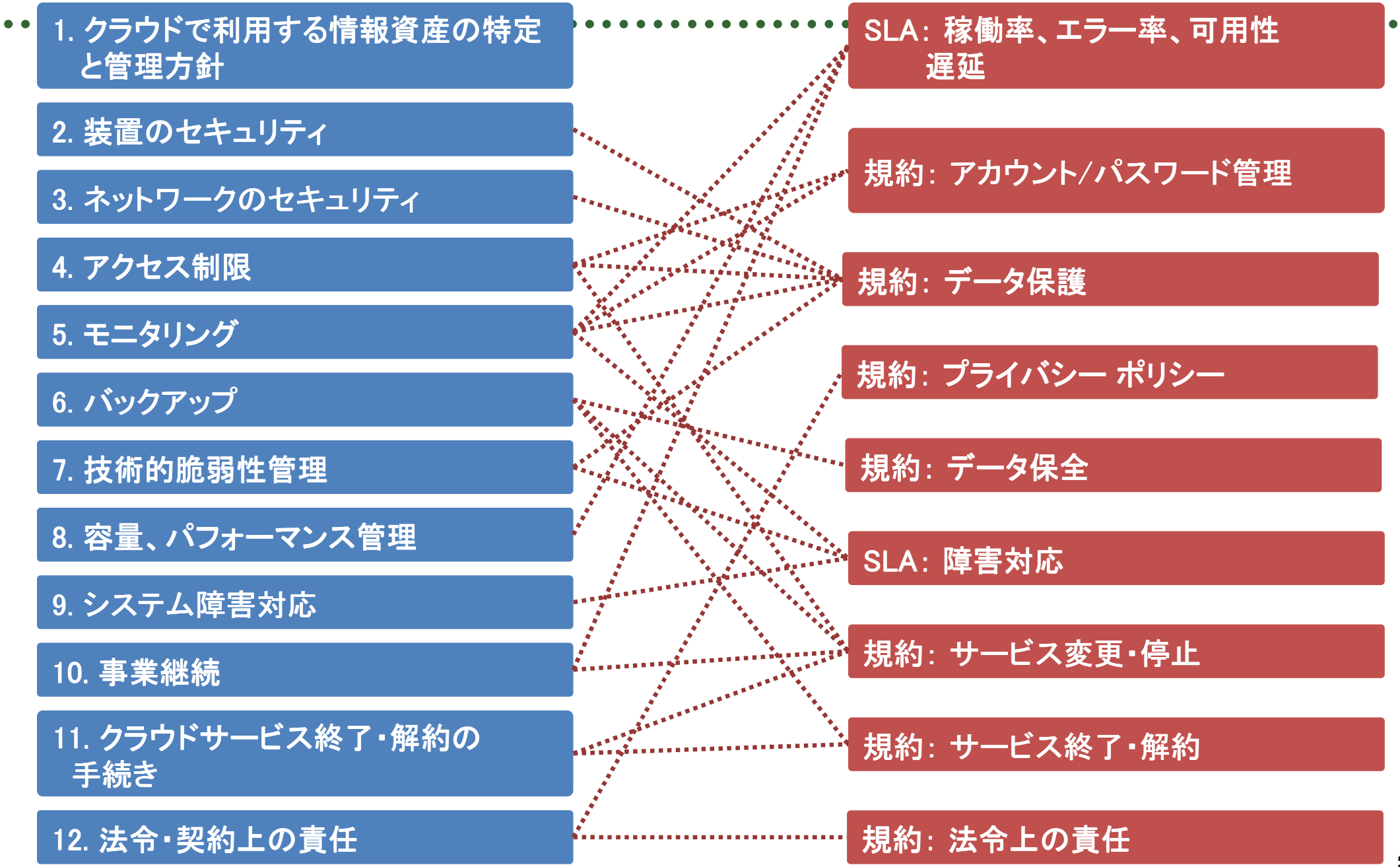
クラウドサービス選定のためのチェックリストの例(2/2)

管理項目	No.	セキュリティ要件	評価	コメント
アクセス制御	8	以下の条件で権限が分割できること。 ・データ利用権限を持つ者にアクセス権管理権限を与えると、未許可で自己の権限を昇格させることができる。 ・システム設定権限を持つ者にログ管理権限を与えると、未許可で設定変更した記録を削除又は改ざんできる。		
	9	ID/パスワードの登録・発行・変更・停止・削除が利用者側で操作できること。		
	10	クラウドに保存するパスワードはハッシュ化等で秘匿されていること。		
	11	仮想マシン環境において他利用者から自社仮想環境へのアクセス制限がされていること。		
	12	事業者内の権限者から自社仮想環境へのアクセス制限がされていること。		
	13	データ保護に暗号機能が利用できる場合以下の条件を満たすこと。 ・AESその他第三者機関で安全性が評価された暗号アルゴリズムを選択できること。 ・暗号鍵は128bit以上が選択できること。		

3. クラウドサービスのSLA、規約の解釈

教科書 140ページ

情報セキュリティ要件と規約条項の対比



SLAの解釈(1/3)

SLAのサンプル

a. サービスレベル

- ご契約いただいた仮想サーバを動作させるハイパーバイザの月間稼働率が、99.99%以上であることを保証します。
- 以下を以って、ハイパーバイザの稼働とみなします。

  ●●が●●●●●の状態にあること。

b. 月間稼働率

$$\text{稼働率(\%)} = \left(1 - \frac{\text{月間累計非稼働時間(分)}}{\text{月間稼働時間(分)}}\right) \times 100$$

c. 非稼働時間

- 1回あたりの非稼働時間について、1分未満は切り捨てます。

教科書 145ページ

SLAの解釈(2/3)

SLAのサンプル

a. 請求方法

- インシデントの発生から5営業日以内に、提供者が定めた手順に従ってカスタマーサポートにインシデントを報告。
- インシデントの詳細な説明、インシデントの発生期間、ネットワークのトレースルート、影響を受けたURL、ならびに利用者がインシデント解決のために講じた措置などを含む（ただし、これらに限定されない）、請求に関する合理的な詳細をすべて提供。
- 請求の対象インシデントが発生した請求月の翌請求月末までに、その請求の内容を裏付ける十分な証拠を添えて、請求を提出。

b. 請求できる金額

月間稼働率	サービスクレジット
＜ 99.99%	10%
＜ 99%	25%

- 1 請求月に付与されるサービス クレジットは、事情の如何を問わず、顧客の月間のサービス使用料金を超えない

SLAの解釈(3/3)

SLAのサンプル

a. SLAが適用されない条件

- 事業者が合理的な方法で制御不能な要因によるもの。
- 利用者または第三者のハードウェアまたはソフトウェアに起因するもの。
- 利用者または第三者の作為または不作為に起因するもの。
- 事業者がサービスの使用上の改善を利用者に助言した後に、利用者が助言されたとおりの改善を実施せずにサービスを使用したことに起因するもの。
- ベータ版または試用版のサービス(事業者の定めるところによる)中に発生したもの。
- 利用者または利用者の従業員、代理人、下請業者、ベンダーもしくは利用者のパスワードまたは機器を利用して事業者のサービスにアクセスできる者の行為または不作為に起因するもの。

教科書 153ページ

データ保全に関する規約の解釈

【データ保全の規約のサンプル】

a. バックアップの目的
   - サーバ故障・停止時の復旧便宜に備えて
   - 情報の喪失、改変、破壊に備えて

b. バックアップの内容
   - お客様がサーバ上において利用、作成、保管記録等するファイル、データ、プログラム及び電子メールデータ等全て。

c. バックアップの期間
   - お客様によって指定された保持期間。

d. 事業者の責任範囲
   - お客様によって指定された保持期間を超えてのバックアップの保存義務はないものとする。
   - バックアップデータは、当社がお客様からのバックアップデータの提供要求に応じる場合であっても、当社は、当該データの完全性等を含め何らかの保証をするものではない。
   - お客様が契約上の責任を果たさず保有データをバックアップしなかったことによって被った損害について、当社は損害賠償責任を含め何らかの責任を負わないものとする。

法令上の責任に関する規約の解釈

【法令上の責任の規約のサンプル】

a. 関連法規
   - 個人情報保護関連法
   - 知的財産権
   - 輸出入規制法

b. 法令等による開示
   - 政府機関が、当社クラウドサービス上に存在するお客様データの開示請求をした場合、最初に利用者に請求するように政府機関に依頼する。
   - それにもかかわらず、情報を開示するように要請された場合は当社（事業者）は、開示することが法的に要求される場合のみ、利用者の情報を提供する。

【補足】クラウドのセキュリティの標準化動向

教科書 166ページ

クラウドセキュリティの標準化(1/2)

- 経済産業省　クラウド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
  - JIS Q 27002 管理策群を活用しクラウドで考慮すべき点を、JIS Q 27002の構造を変えずガイドライン化
  - クラウド利用者のための実施の手引、クラウド事業者のための実施の手引、クラウドサービス関連情報で構成
- IPA 中小企業等によるクラウド利用検討WG
  - クラウド利用前のチェックリストとして、ITコーディネータや銀行のシステム開発子会社、コンサルタント等が利用できる形で提供

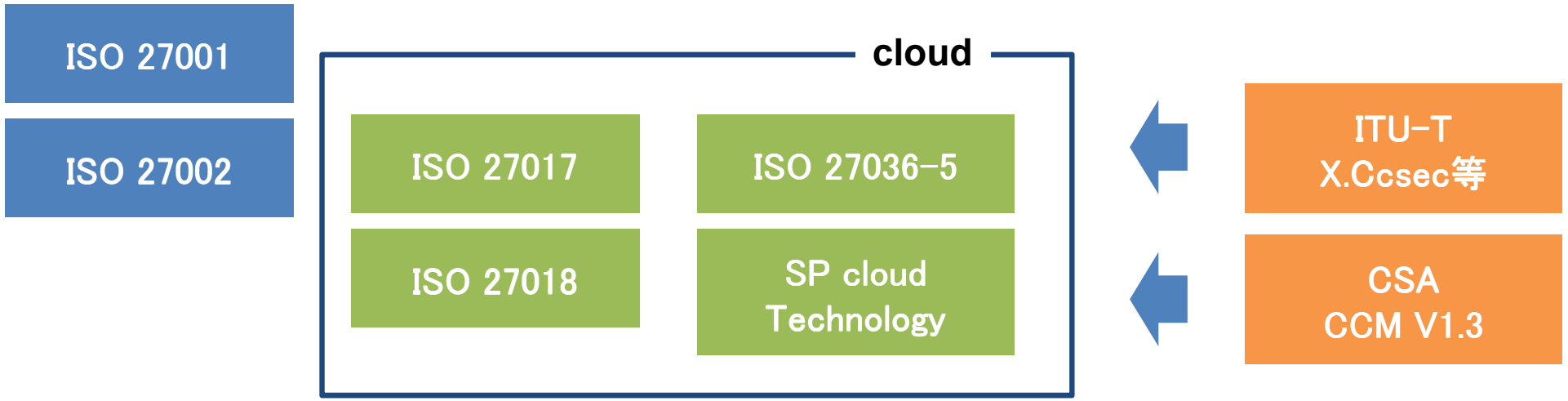
教科書 168ページ

クラウドセキュリティの標準化(2/2)

- Cloud Security Alliance (CSA)
  - 世界で最も大きなクラウドセキュリティ団体
  - 国際標準化に際し、CSAのセキュリティマトリクスなどを参考にしている
- ENISA: Cloud computer risk assessment
  - EUにおける法律やレギュレーションの共有化の一部であるデータ保護法制の中のクラウドコンピューティングのリスクアセスメントレポート
- JASA クラウドセキュリティ監査制度
  - 経済産業省受託事業としてクラウドセキュリティ監査の実証実験を実施

教科書 169ページ

クラウドセキュリティの国際標準化



ISO 27001　組織のISMSを認証するための要求事項

ISO 27002　ISMS実践のための規範

ISO 27017　クラウドコンピューティング・セキュリティの実践規範

ISO 27018　クラウド・データ保護の実践規範

ISO 27036　クラウド・サプライヤー・セキュリティ 指針