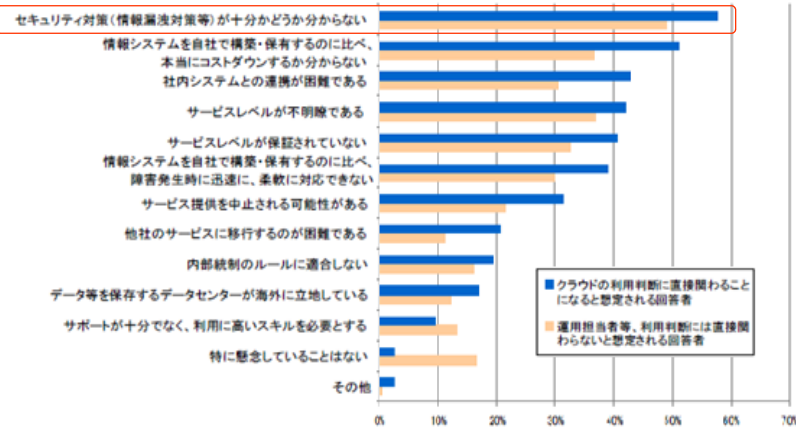


クラウドサービス利用のための 情報セキュリティマネジメントガイドラインについて

経済産業省 商務情報政策局
情報セキュリティ政策室

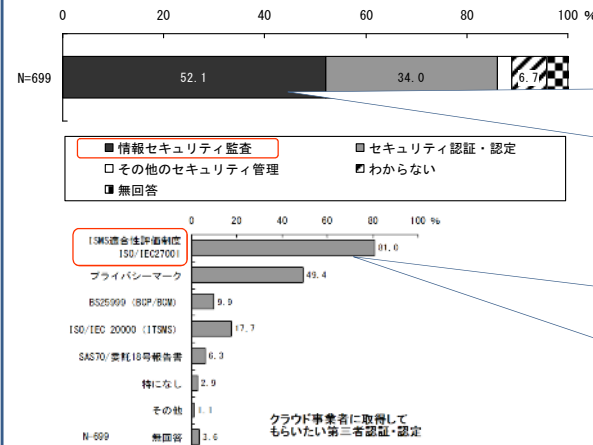
クラウド利用者の不安



*「高度情報化社会における情報システム・ソフトウェアの信頼性及びセキュリティに関する研究会」(経済産業省2009年3月)

クラウド利用においてセキュリティ上の不安が払拭できていない

クラウド事業者への要求



半数の利用者が、クラウド事業者には情報セキュリティ監査による、具体的な報告を望んでいる

利用者が事業者へJIS Q 27001ベースのセキュリティ管理を望むのは、利用者組織と同様のセキュリティ体制を望んでいるため

*「クラウドサービスの情報セキュリティ監査に関するアンケート調査報告書」(経済産業省2010年1月)

クラウド利用者はクラウド事業者へ、情報セキュリティ監査及びJIS Q 27001ベースのセキュリティ管理を望んでいる。

「情報セキュリティ」および「事業者におけるシステム運用」が見えないことに関する不安を「見える化」する

クラウド利用者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策定

利用者視点による
セキュリティリスクの
共通認識の形成

事業者選択における
基準として利用できる
対策標準

情報セキュリティ監査による
利用者との事業者との
信頼関係の構築

本ガイドラインの策定体制（委員一覧）

本ガイドラインの策定にあたっては、「クラウドセキュリティ管理基準策定TF」を設置し、平成22年7月～10月にかけて議論・取りまとめ。

座長

大木 栄二郎 工学院大学 情報学部 情報デザイン学科 教授

委員

河野 省二 独立行政法人情報処理推進機構 セキュリティセンター

佐藤 元彦 伊藤忠テクノソリューションズ株式会社
ITサービスコンサルティング部 セキュリティアシュアランス課 課長

首藤 一幸 国立大学法人東京工業大学 大学院 情報理工学研究科
数理・計算学専攻 准教授

菅谷 光啓 NRIセキュアテクノロジーズ株式会社
コンサルティング事業本部長

米澤 一樹 ベライゾンビジネス グローバルサービス本部
シニアコンサルタント

オブザーバ

加藤 雅彦 JPCERTコーディネーションセンター
株式会社インターネットイニシアティブ
サービス本部 セキュリティ情報統括室 シニアエンジニア

事務局

経済産業省 商務情報政策局 情報セキュリティ政策室

（五十音順，敬称略，所属は委員就任時）

目的

◆本ガイドラインを情報セキュリティ管理、及び情報セキュリティ監査に活用することにより、クラウド利用者とクラウド事業者における信頼関係の強化に役立てることを目的とする。

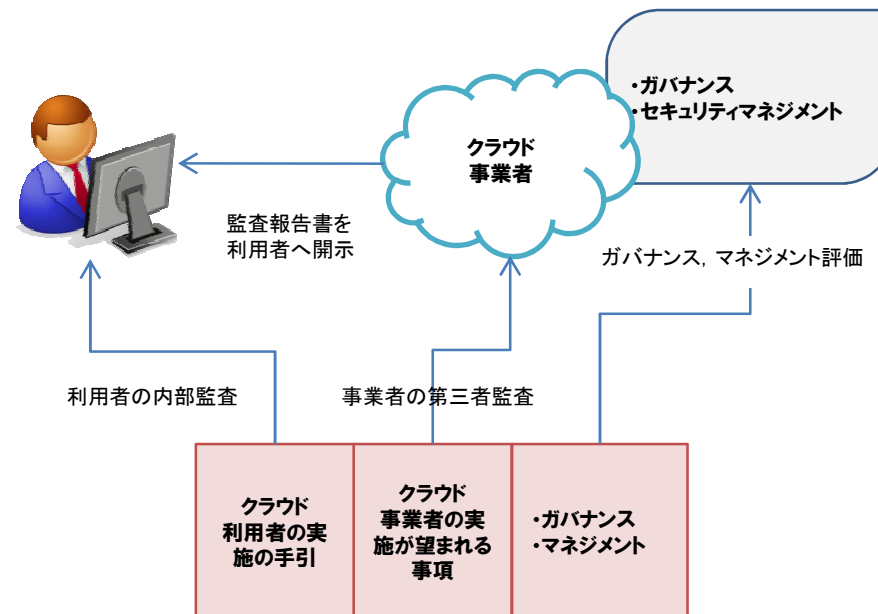
適用範囲

◆本ガイドラインは、組織事業の基礎を成す情報資産の多くを、外部組織であるクラウド事業者が提供するクラウドサービスに委ねようとする組織が、JIS Q 27002（実践のための規範）に規定された管理目的を達成するための管理策を実施しようとする場合を想定している。

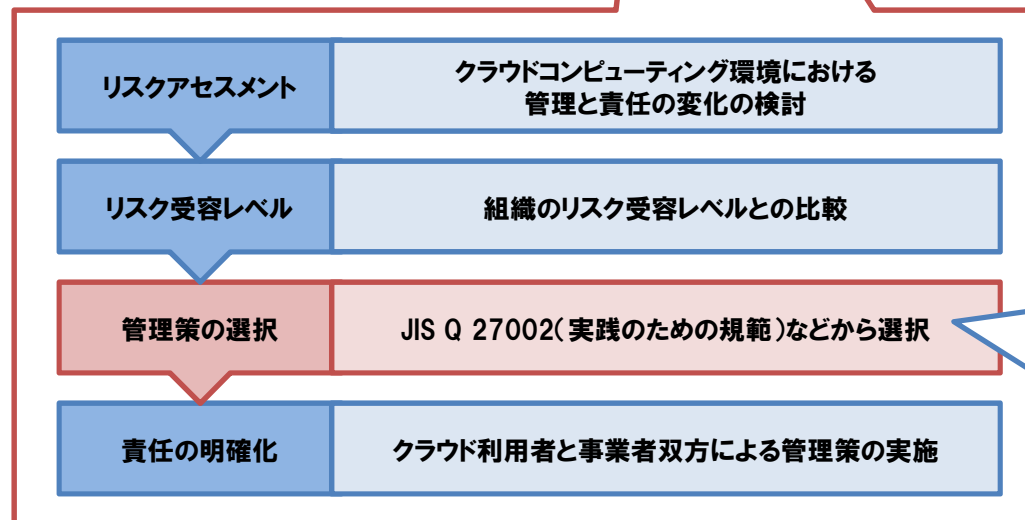
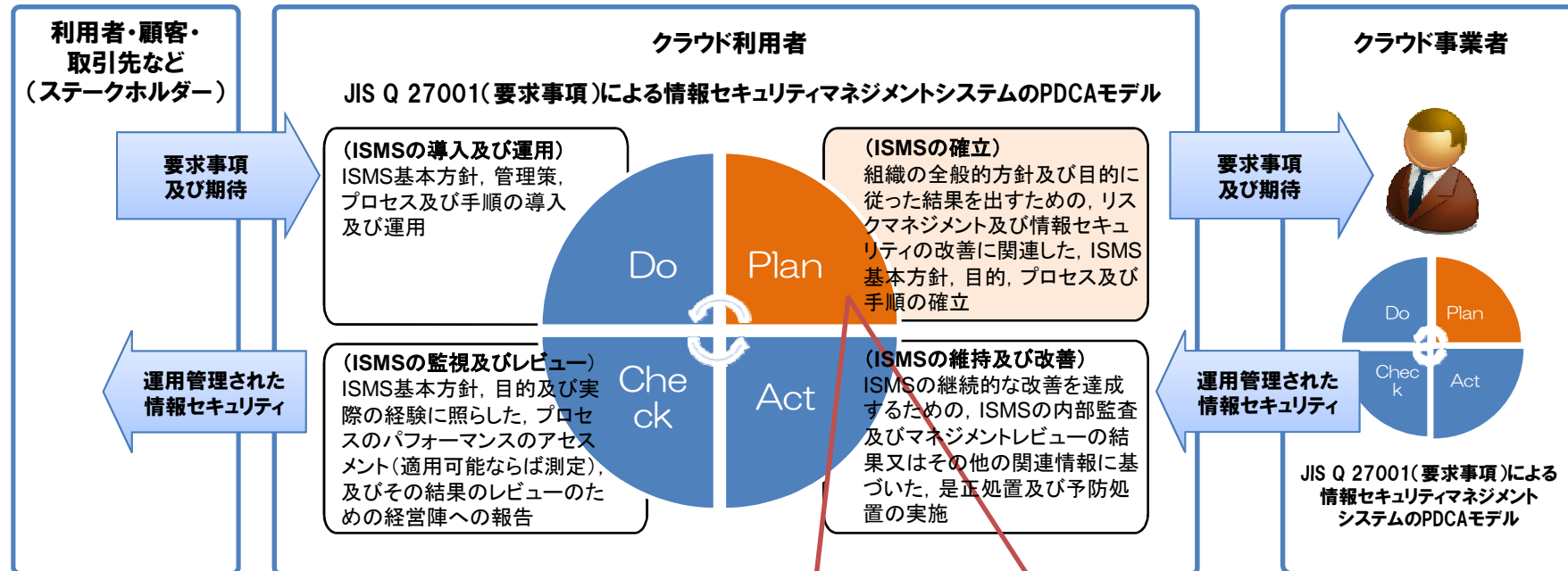
特徴

◆全面的にクラウドサービスを利用する際のJIS Q 27002（実践のための規範）の管理目的達成という究極的な状況を想定することにより、クラウドサービスの利用において変化するシステム環境、責任の所在、事故や事象の判断基準を明確にする。

◆クラウドサービスを全面的に利用することにより生ずるリスクの変化に対応するため、JIS Q 27002（実践のための規範）の管理策に、「クラウド利用者のための実施の手引」と、「クラウド事業者の実施が望まれる事項」を追加している。

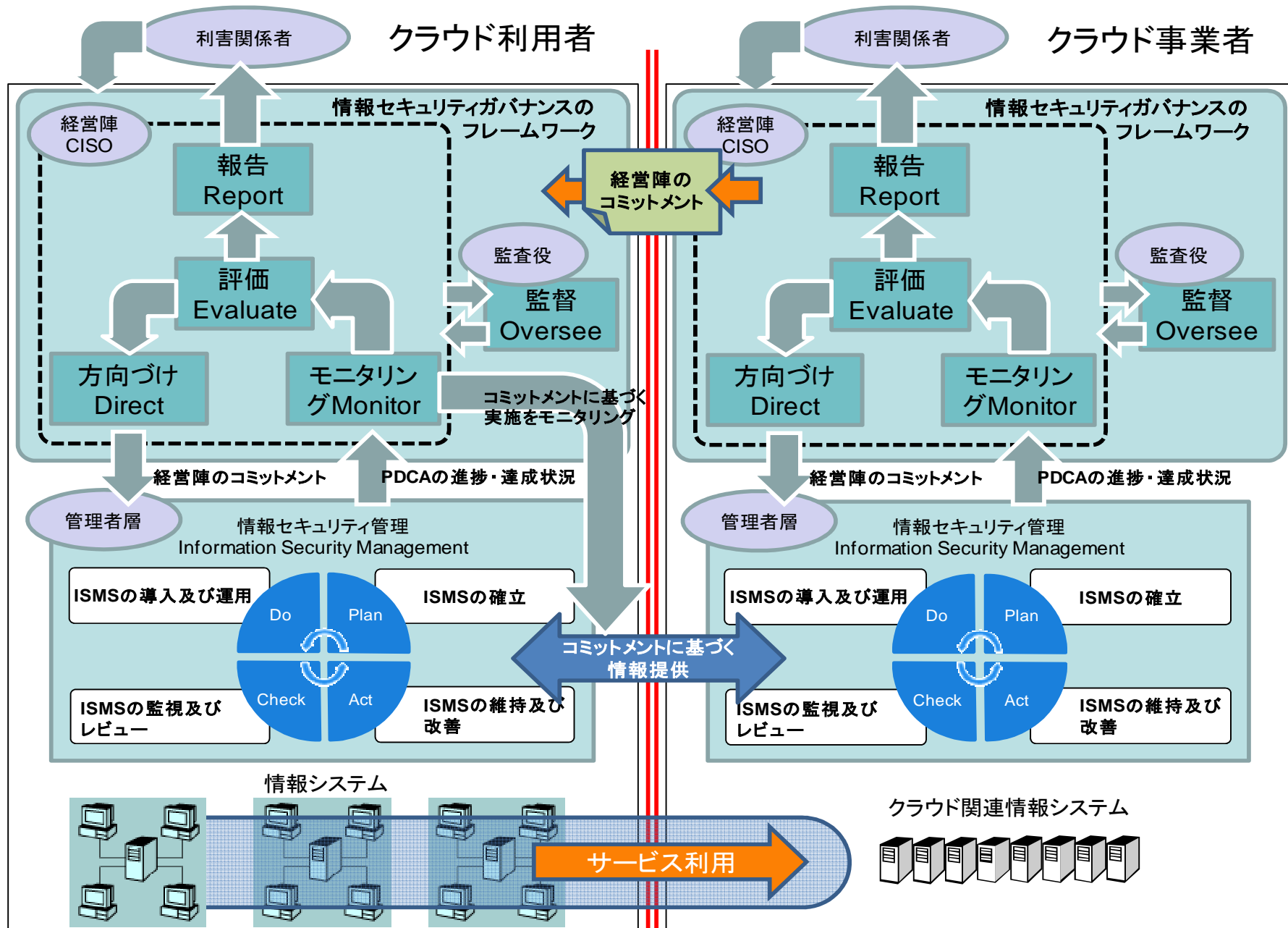


クラウドサービス利用に係る管理策の選択

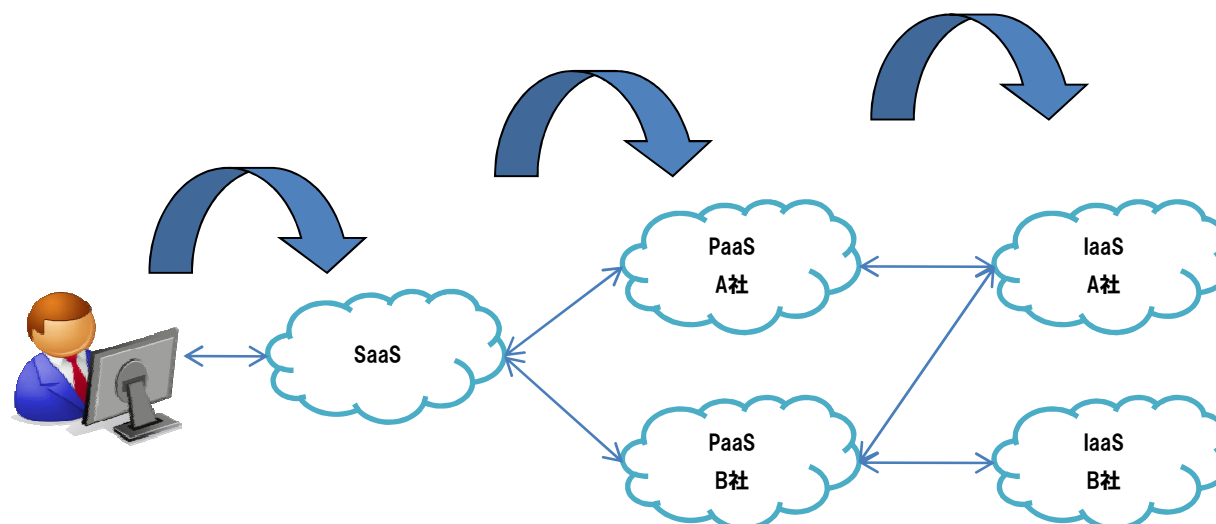


クラウドサービス利用のための管理策の実施の手引があれば、マネジメントシステムを維持しながら、クラウドサービスを利用した適切な情報セキュリティ管理が容易に行える

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



- クラウドサービスにおいては、IaaS、PaaS及びSaaSそれぞれが関連しあってサプライチェーンを形成し、クラウドサービス全体を提供することがある。
- 本ガイドラインにおいては、クラウドサービスを供給する側が利用する側に回ることで、サービスの供給と利用の連鎖が形成される。
- 「クラウド利用者のための実施の手引」を自らの組織に活用できるだけでなく、「クラウド事業者の実施が望まれる事項」を自らが利用するクラウドサービスの供給者に対して要請し、サプライチェーンを形成するクラウド事業者の情報セキュリティマネジメントに活用することもできる。



- 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

10.5 バックアップ

目的：情報及び情報処理設備の完全性及び可用性を維持するため。

データのバックアップ取得と時機を失さないデータ復旧の訓練とに關する、合意されたバックアップ方針及び戦略(14.1 参照)を実施するために、日常の作業手順を確立することが望ましい。

10.5.1 情報のバックアップ

管理策

情報及びソフトウェアのバックアップは、合意されたバックアップ方針に従って定期的に取得し、検査することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は、クラウドサービス上で扱う情報、ソフトウェア及びソフトウェアの設定において、バックアップの必要性を確認することが望ましい。クラウド利用者は、自らが利用するクラウドサービスの特性を理解して、クラウドサービス上で扱う情報、ソフトウェア及びソフトウェアの設定において、バックアップの可能性を確認することが望ましい。クラウド利用者は、自らが利用するクラウドサービスの特性を理解して、クラウドサービス上で扱う情報、ソフトウェア及びソフトウェアの設定においてのバックアップ手順を策定することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は、クラウド利用者が求める情報、ソフトウェア及びソフトウェアの設定において、クラウド利用者がバックアップ手順を策定できるように情報を提供することが望ましい。

クラウドサービスの関連情報

クラウドサービスでは、クラウドサービスによってバックアップ不可能な情報がある点に留意する必要がある。クラウドサービス以外のシステム運用におけるバックアップ手順において、差分バックアップ、増分バックアップ、完全バックアップなど、バックアップ対象の特性に応じて使い分けられている場合は、それぞれの手法による実施の可否を確認することが望ましい。

IaaSサービスにおいては、作成された仮想イメージファイルを明示的にバックアップしておくことで、ある時点での環境を再現することができるが、バックアップを指定しない場合には再現することが難しい。クラウド利用者が必要に応じて、仮想イメージファイルをバックアップできる手段を用意しておくことが望ましい。

PaaSサービスにおいては、作成したアプリケーションなどのソースファイルなどをバックアップすることができないこともある。アプリケーションの開発中など、頻繁に機能の追加や削除を行う場合に備えて、開発途中の状態を維持できるかどうかを確認することが望ましい。また、実行環境や試験データなどが再現できるかどうかを確認することが望ましい。

SaaSサービスでは、アプリケーションで利用するデータだけでなく、利用者アカウントの管理など、クラウドサービスの管理情報についてバックアップが可能かどうかを確認することが望ましい。

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用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

管理策

すべての情報セキュリティ責任を、明確に定めることが望ましい。

実施の手引 (JIS Q 27002)

情報セキュリティ責任の割当ては、情報セキュリティ基本方針に従って行うことが望ましい(箇条4参照)。個々の資産の保護に対する責任及び特定のセキュリティプロセスの実施に対する責任を、明確に定めることが望ましい。必要な場合には、この責任に、個別のサイト及び情報処理施設に関する、より詳細な手引を追加してもよい。資産の保護及び事業継続計画のような特定のセキュリティプロセスの実行に限定される責任を明確に定めることが望ましい。

セキュリティ責任を割り当てられた個人は、セキュリティに関する職務を他者に委任してもよい。しかしながら、責任は残ったままであり、いずれの委任した職務も正しく実行されていたと判断することが望ましい。

個人が責任をもつ領域を明確に規定することが望ましい。特に、次を実施することが望ましい。

- a) 個々の特定のシステムに関連した資産及びセキュリティのプロセスの識別、並びに明確な規定
- b) 各資産又はセキュリティのプロセスに対する責任主体(例えば、個人、職位)の指名、及びその責任の詳細の文書化(7.1.2参照)
- c) 承認の権限の明確な規定及び文書化

組織が自らのシステムを所有することを想定して作成されたJIS Q 27002では、利用という形態をとるクラウドサービスに対して、管理策を実施するための手引をそのまま適用できない！

管理策

すべての情報セキュリティ責任を、明確に定めることが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は、クラウドサービス利用における責任において、クラウド事業者が果たす内容について明確にすることが望ましい。クラウド利用者は、情報セキュリティ責任について、クラウド利用者だけでは対応できない内容について一覧を作成することが望ましい。クラウド利用者は、クラウド事業者が負う責任についてクラウド事業者を確認することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は、クラウドサービスに関する情報セキュリティ責任者を専任することが望ましい。クラウド事業者は、クラウドサービスの情報セキュリティに関する窓口を明確にし、開示することが望ましい。

クラウドサービスの関連情報

クラウドサービスにおいては、情報セキュリティに関する一部の業務がクラウド事業者に委任される。しかしながら、情報セキュリティに関する責任はクラウド利用者に残ったままであるため、クラウド事業者が情報セキュリティに関する業務を正しく実行していることを、クラウド利用者が判断することが望ましい。また、個人が情報セキュリティに責任を持つ領域がクラウドサービスによって変化をする場合(例えば、ID管理が一元化できずにパスワードの変更を個人が配慮して行わなければならないなど)には、クラウド利用者はその責任範囲を明確にし、クラウドサービスの利用者に伝えなければならない。

管理策

情報及びソフトウェアのバックアップは、合意されたバックアップ方針に従って定期的を取得し、検査することが望ましい。

実施の手引 (JIS Q 27002)

災害又は媒体故障の発生の後に、すべての重要な情報及びソフトウェアの回復を確実にするために、適切なバックアップ設備を備えることが望ましい。情報のバックアップについて、次を考慮することが望ましい。

- a) 情報のバックアップの必要なレベルを明確化する。
- b) バックアップ情報の正確で完全な記録及び文書化したデータ復旧手順を作成する。
- c) バックアップの範囲、及びバックアップの頻度は、組織の業務上の要求事項、関連する情報のセキュリティ要求事項、及びその情報の組織の事業継続に対する重要度を考慮して決定する。
- d) バックアップ情報は、主事業所の災害による被害から免れるために、十分離れた場所に保管する。
- e) バックアップ情報に対して、主事業所で媒体に適用している管理策は、バックアップ情報の保管場所にも適用する。
- f) バックアップに用いる媒体は、必要になった場合の緊急利用について信頼できることを確実にするために、定めにしたがって試験する。
- g) 復旧手順は、有効であること、及び回復のための運用手順で定められた時間内に完了できることを確実にするために、定めに従って点検し試験する。
- h) 機密性が重要な場合には、暗号化によってバックアップ情報を保護する。

管理策

情報及びソフトウェアのバックアップは、合意されたバックアップ方針に従って定期的を取得し、検査することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は、クラウドサービス上で扱う情報、ソフトウェア及びソフトウェアの設定において、バックアップの必要性を確認することが望ましい。クラウド利用者は、自らが利用するクラウドサービスの特性を理解して、クラウドサービス上で扱う情報、ソフトウェア及びソフトウェアの設定において、バックアップの可能性を確認することが望ましい。クラウド利用者は、自らが利用するクラウドサービスの特性を理解して、クラウドサービス上で扱う情報、ソフトウェア及びソフトウェアの設定におけるバックアップ手順を策定することが望ましい。

クラウド事業者の実施が望まれる事項

クラウド事業者は、クラウド利用者が求める情報、ソフトウェア及びソフトウェアの設定において、クラウド利用者がバックアップ手順を策定できるように情報を提供することが望ましい。

クラウドサービスの関連情報

IaaSサービスにおいては、作成された仮想イメージファイルを明示的にバックアップしておくことで、ある時点での環境を再現することができるが、バックアップを指定しない場合には再現することが難しい。・・・PaaSサービスにおいては、作成したアプリケーションなどのソースファイルなどをバックアップすることができないこともある。・・・SaaSサービスでは、アプリケーションで利用するデータだけではなく、利用者アカウントの管理など、クラウドサービスの管理情報についてバックアップが可能かどうかを確認することが望ましい。

管理策

情報の漏えいの可能性を抑止することが望ましい。

実施の手引 (JIS Q 27002)

例えば、隠れチャンネルの使用、展開によって発生するような、情報の漏えいのリスクを制限するために、次の事項を考慮することが望ましい。

- a) 外向けに公開された媒体及びコミュニケーションを、隠された情報がないか詳しく調べる。
- b) 情報を導き出すことができる第三者の可能性を低減させるためのシステム及び通信の振舞いを隠して調節する。
- c) 例えば、評価された製品(JIS X5070参照)を使用して、高い完全性を考慮されているシステム及びソフトウェアを利用する。
- d) 既存の法規定の下で許されている場合には、要員及びシステムのアクティビティを常に監視する。
- e) コンピュータシステムにおけるリソースの使い方を関する。

管理策

情報の漏えいの可能性を抑止することが望ましい。

クラウド利用者のための実施の手引

クラウド利用者は、情報漏えいが起きないように、クラウドサービスの利用手順を策定することが望ましい。クラウド利用者は、情報漏えいの可能性を考慮して、クラウドサービスの利用者にリスクと対策を周知することが望ましい。

クラウド事業者の実施が望まれる事項

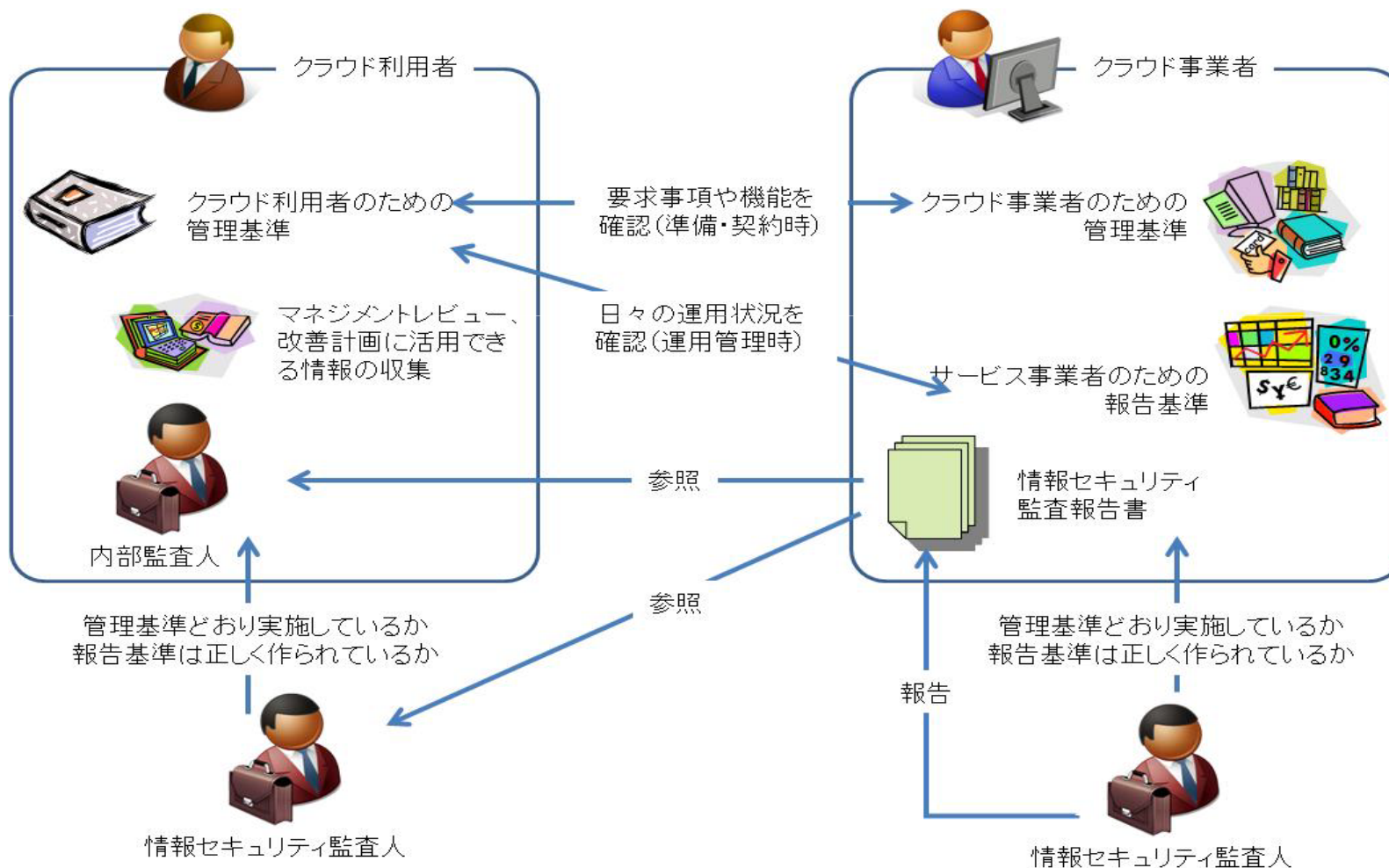
クラウド事業者は、クラウドサービスにおける情報漏えいに関する対策を行い、円滑なシステムの運用に支障のない範囲でクラウド利用者にその対策内容を開示することが望ましい。

クラウドサービスの関連情報

クラウドサービスではデータをひとつのサーバ上に保存するのではなく、複数のサーバ上に分散して配置され、さらに冗長性を高めるために、分割されたデータが複製されて複数のサーバ上に配置されることも多い。そのため、データの移動や削除などにともなってすべてのデータが完全に消去をされず、残存オブジェクトとしてデータの一部分が残ってしまう可能性がある。そのため、資産分類において完全消去を前提としているデータについては取り扱いに慎重を要することが望ましい。

本ガイドラインの情報セキュリティ監査への活用例

本ガイドラインの実施項目を、情報セキュリティ監査の枠組みで利用することにより、クラウド利用者及びクラウド事業者間の信頼関係を構築。



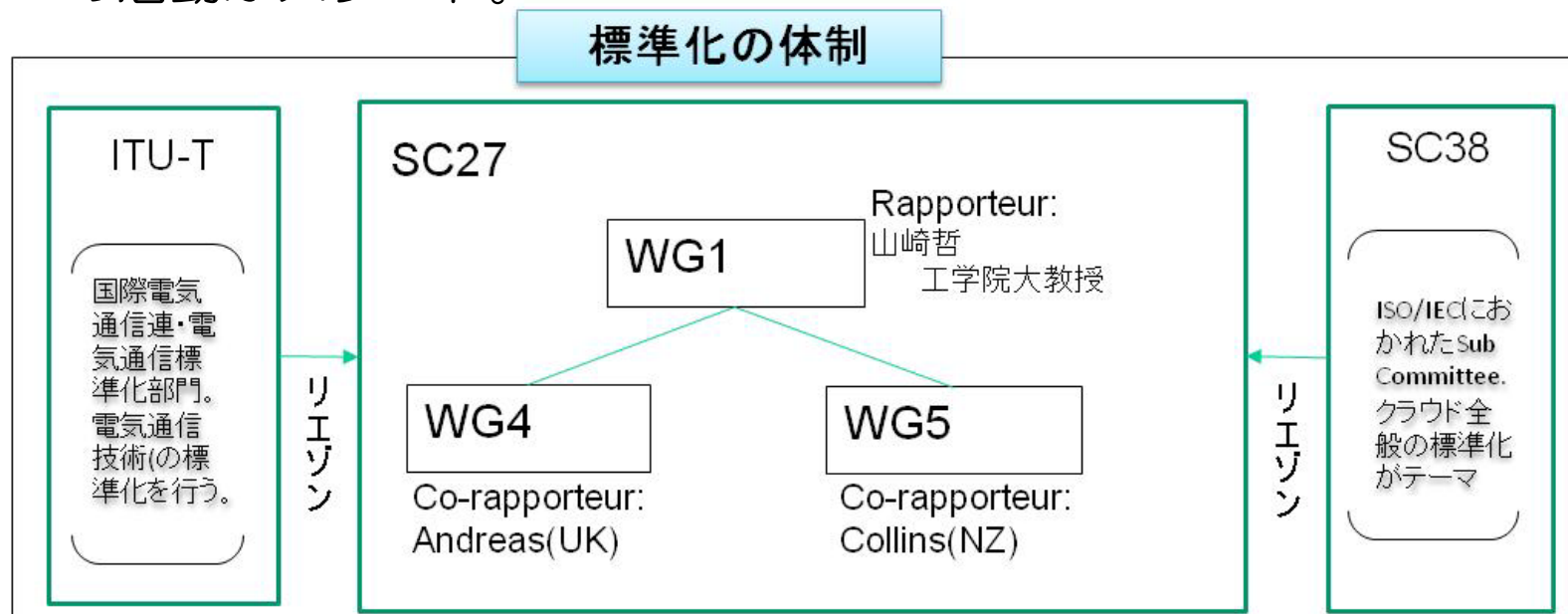
過去のクラウド障害事例と本ガイドラインの主な対応

	セキュリティリスク			その他のリスク (BCP,制度等)
	ネットワーク セキュリティ	プロセス セキュリティ	データ セキュリティ	
2000年		「技術的ぜい弱性管理」	「事業継続管理手続きへの情報セキュリティの取組み」	<ul style="list-style-type: none"> 10月、Digital Railroadが、突然オンラインストレージサービスの終了。
2006年	<ul style="list-style-type: none"> 12月、セールスフォースのDNSサービスプロバイダーがDDoS攻撃によりアクセス障害。 <p>「情報セキュリティインシデントの管理及びその改善」</p>	<ul style="list-style-type: none"> 4月、Vaserv.com内のウェブサイトのデータの消失。 <p>「技術的ぜい弱性管理」「情報セキュリティインシデントの管理」</p>	<ul style="list-style-type: none"> 3月、Google Docsの、意図しない相手へのドキュメント共有。 10月、T-Mobileの多機能携帯電話「Sidekick」用のサービスからユーザーデータが消失。 <p>「情報のバックアップ」</p>	<ul style="list-style-type: none"> 4月、FBIによるサーバ等押収。
2010年			「外部及び環境の脅威からの保護」	<ul style="list-style-type: none"> 2月、Google App Engineの停止。

◆クラウド利用における情報セキュリティ監査に必要な文書の整理・策定

◆ISO/IEC SC27[※]における国際標準化の推進

- 2010年10月、独ベルリンにて開催された上記会合にて、我が国より国際標準化の推進を提案し、仕様文書案を提出。これを受けて、日本案をベースに同会合において国際標準化を進めるための活動がスタート。



※ISO(国際標準化機構)とIEC(国際電気標準会議)の間に合同で設置されたセキュリティ技術に関する標準を検討する委員会(Sub Committee)15