クラウドサービス利用者の保護と
コンプライアンス確保のためのガイド

～経営層による的確なリスクマネジメントのために～

第 1.0 版

平成 23 年 7 月

特定非営利活動法人

ASP・SaaS・クラウド コンソーシアム

目次

本ガイドは、総務省と ASPIC が合同で設立した「ASP・SaaS・クラウド普及促進協議会」において、2010 年度に設置した「クラウドサービス利用者の権利保護のあり方検討委員会」の検討結果に基づき、ASPIC が意見募集を経て策定しました。

第1章　クラウドサービスを安心して利用していただくために

1. 本ガイドの読み方

（1） 本ガイドの目的

現在、クラウドサービスの利用は世界的に見ても着実に拡大しています。また、国境を越えたグローバルサービスを提供するクラウドサービス事業者も多くあります。多様化する事業者とサービスの中で、企業に明らかなメリットを提供するサービスが増える一方で、企業のリスクマネジメントポリシーにそぐわない事業者やサービスを選んでしまう危惧も存在し、企業は賢く選択する「目」を求められるようになっています。

本ガイドでは、企業がパブリッククラウド（技術用語の解説については参考資料１を参照）を利用するにあたり、自社のリスクマネジメントポリシーに合致するクラウドサービス事業者とサービスを選択し、的確なリスクマネジメントを実践して安全にサービスを利用できるようにするための管理プロセスと重点チェックポイントについて解説しています。パブリッククラウドを選んだ理由は、クラウドサービスの利点と特徴を最も典型的に引き出す形態だからですが、プライベートクラウド（参考資料１参照）を利用する場合においても、本ガイドの記述は幅広く参考になります。

（2） 本ガイドを読んでいただきたい方

本ガイドでは、パブリッククラウドの利用を検討している/または既に利用している企業のリスクマネジメント担当の経営層の方に読んでいただきたいことを記述しています。

- ■ 大会社（取締役会設置会社）、上場企業の経営層の方：
  取締役の善管注意義務を果たし、経営層が率先してクラウドサービス利用にあたって的確なリスクマネジメントを実践できる体制・プロセスを構築するために役立ちます
- ■ 中小企業の経営者の方：
  クラウドサービス利用の不安感を払拭し、ITの専門能力（運用・管理等）と人材をクラウドサービス事業者に委ねつつ、安心して廉価にサービスを利用するために役立ちます
- ■ グローバル企業の経営層の方：
  海外から/海外で提供されるクラウドサービスの利用にあたり、企業の権利を保護し、コンプライアンスを確保するためのチェックポイントを解説しています。

（3） 本ガイドの読み方

本ガイドは、３つの章と３つの参考資料から構成されています。

第１章はこのガイドの読み方、クラウドサービス利用の利点とリスクマネジメントの必要性、利用者の権利保護やコンプライアンス確保において対象とした法体系と今後の拡大予定について記しています。第２章は、クラウドサービスの利用サイクルの各フェーズにおいて実施すべきリスクマネジメントプロセスについ

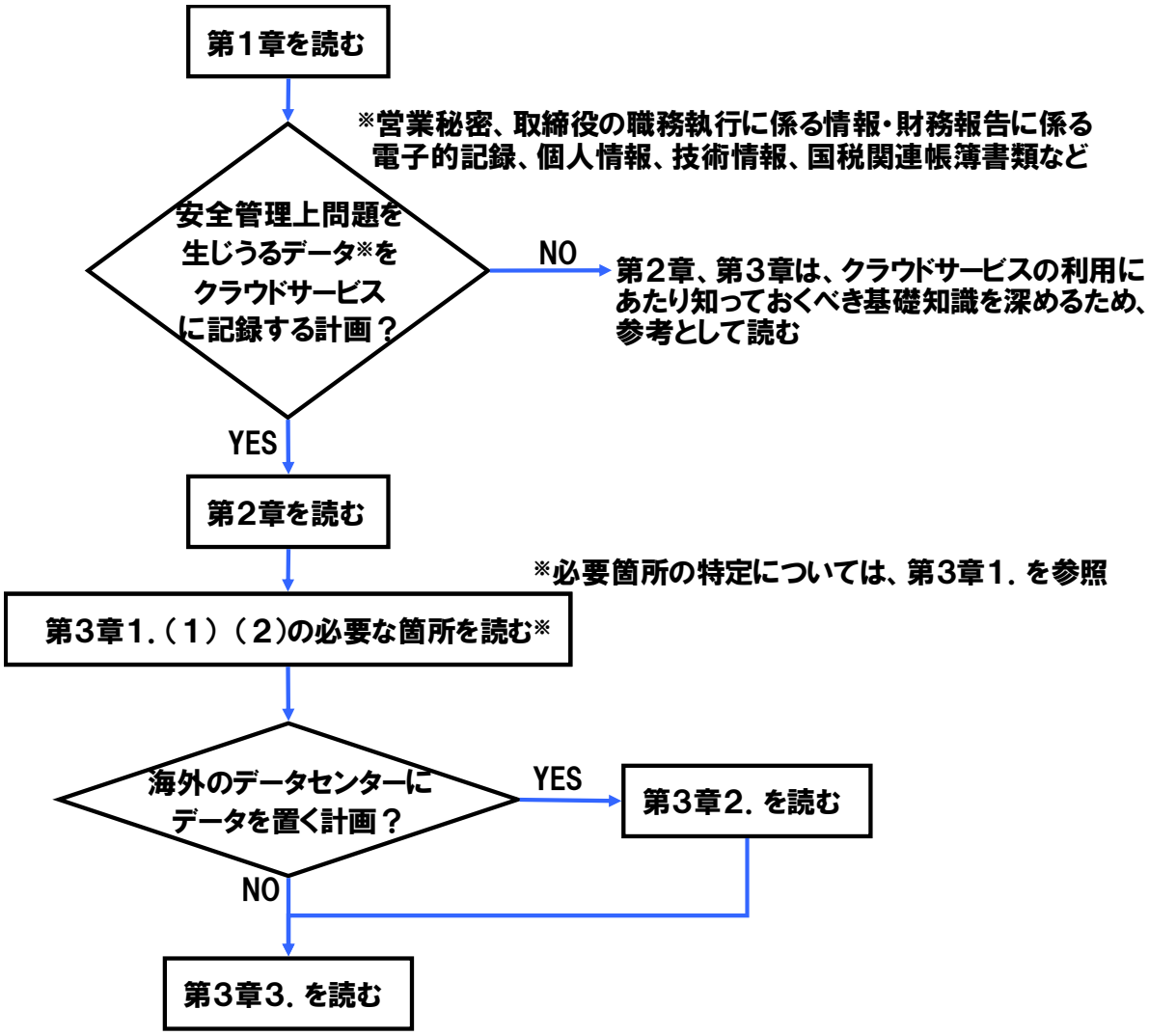
て解説しています。この解説においては、経営層が担当者に指示すべきこととその結果に基づき判断・意志決定すべきことを明示しました。第３章は、クラウドサービスを比較選定するにあたり、特に重点的に確認すべき留意事項を、３つの観点から示しています。利用者の権利保護及びコンプライアンス確保についてチェックする際に参照するガイドライン等については、参考資料３に列挙されています。

第１章は、本ガイドを読む方全員が読んでいただきたいと思います。

クラウドサービスのリスクマネジメントをこれから導入する企業の経営層の方はさらに第２章と第３章の両方を読んで下さい。

既にクラウドサービスのリスクマネジメントを実践している企業の経営層の方は、第３章の必要箇所を選んで読むことにより、リスクマネジメント対策のピンポイントの強化に役立てることができます。

クラウドサービスに記録する予定の情報種別や、海外のデータセンターに情報を記録するかどうか等によって、本ガイドの重点を置いて読むべき箇所は異なります。次ページに示した図表を参考にして下さい。



（4） 本ガイドの位置付けと関連するガイドライン（参考資料２参照）

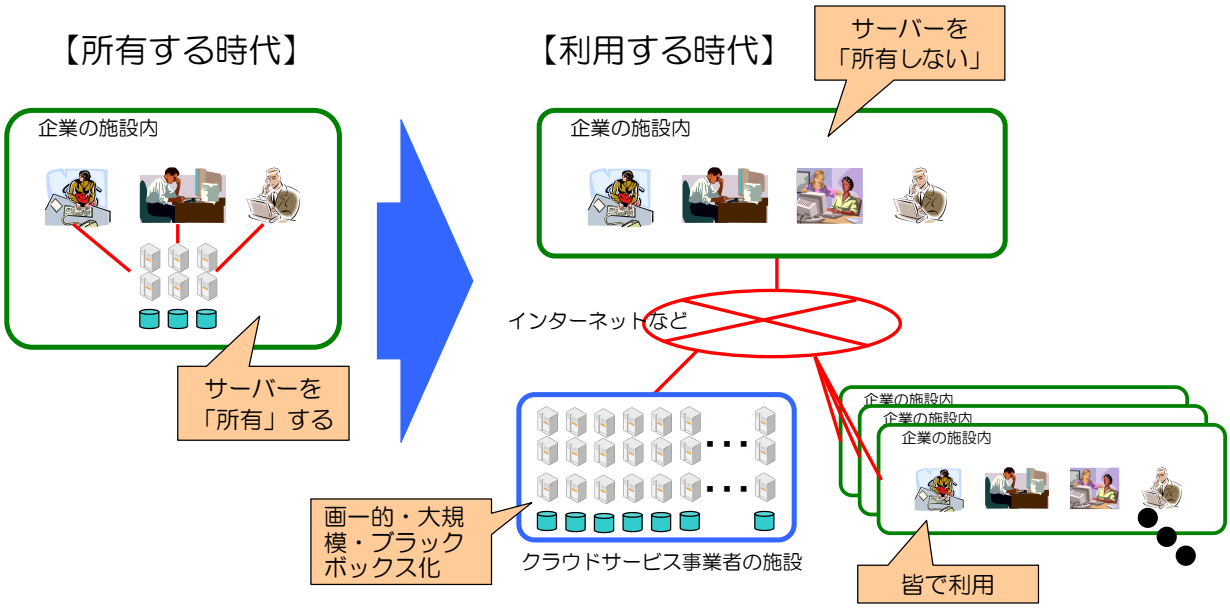
本ガイドは、クラウドサービスの利用サイクルの各フェーズにおいて、リスクマネジメントを適用するためのプロセスと重点留意事項を、経営層のために解説したものです。特に、利用者が持つ法的に守られている権利の保護や、利用者のコンプライアンス確保に重点を置いて記述していることが特徴となっています。

クラウドサービスの利用者向けに書かれたガイドライン、手引きとしては、この他に、「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」（経済産業省、2011 年 4 月）と「中小企業のためのクラウドサービス安全利用の手引き」（独立行政法人情報処理推進機構、2011 年 4 月）があります。

2. さまざまな利点があるクラウドサービス

（1） コンピューティングリソースを「所有する時代」から「利用する時代」へ

我が国におけるブロードバンドネットワークの急速な普及を背景として、情報システムを自分で「所有」せず、外部委託事業者の情報システムを「利用」する企業が着実に拡大しています。近年、クラウドサービス事業者がブラックボックス化された大量なコンピューティングリソースを備えるようになり、利用者は物理的な構成を意識することなくカタログベースでリソースを注文してすぐに利用できる環境が整ってきました。



（2） パブリッククラウドの利用により実現性が高まる利点

クラウドサービスには様々な利点があります。以下に代表的な利点を紹介します。これらの利点はパブリッククラウドに限定したものではありませんが、パブリッククラウドを用いると特に優位性が出やすいものを中心に示しています。

企業の高速経営を助ける有力なツール

企業が新規ビジネスに参入したり、ベンチャーを立ち上げたりする際に一般に ICT 投資が必要になります。クラウドサービスを利用すれば、必要な ICT リソースを短期間で安く「利用」できるため、企業はスピーディな攻めの経営をしやすくなります。

企業の競争力と差別化に重点投資するためのツール

企業の競争力は他社との差別化によって生み出されます。総務・経理・管理等の企業の差別化に関わらない業務においてクラウドサービスを活用することにより、ICT コストと人材を戦略差別化分野に振り向けることができます。

また、システムバージョンアップコストからも解放されます。
一方、中小企業においては、クラウドサービスを利用することにより、大企業と同じ機能を利用できるようになるため、支援業務の質の向上にも役立ちます。

企業の地球環境負荷低減への貢献のためのツール

エネルギー効率を高めたデータセンターで運用されるクラウドサービスを利用することにより、CO_2の排出量削減をより一層効果的に実現できます。

企業の防災力を高めるためのツール

東日本大震災のような広域大災害はいつ発生するか分かりません。クラウドサービスは、大災害に直面しても企業のサービスを継続させるための有力な BCP（Business Continuity Plan）ツールとなります。

ICTの調達に関わる負担からの解放または負担の軽減

中小企業においては、クラウドサービスを利用することにより ICT 調達の敷居が下がり、ICT を導入しやすくなります。

ICTの運用・保守の負荷からの解放または負荷の軽減

ICT 専門人材が不足する中小企業では、ICT の運用・保守の負荷を軽減することは大きな利点となります。

セキュリティ対策の負担と負荷からの解放または負担軽減

情報セキュリティ人材が不足する中小企業では、自社システムの情報セキュリティ対策は不安にさらされていることが多いものです。専門人材と高度な安全管理を実現するデータセンターで運用されるクラウドサービスを利用することにより、自社システムを運用していた時よりも、情報セキュリティ管理レベルが高まることが期待できます。

3. リスクマネジメントがなぜ必要か

パブリッククラウドでは様々な利点を生み出す半面、物理的なコンピューティングリソースがブラックボックス化され、その運用がクラウドサービス事業者に任されているため、リスクコントロールが効きにくくなります。これが様々な派生リスクを生み出す可能性があります（参考資料１参照）。例えば、利用者の営業秘密が不十分な秘密管理のために法的保護の対象と認められない、クラウドサービス事業者からの個人情報漏洩により利用者が社会的信頼を失墜した、海外で輸出規制の対象となる技術情報がクラウドサービス事業者から流出した、クラウドサービス事業者の不完全なデ

ータ消去が原因で情報漏えいが発生した等の事故が実際に起こりえます。
　また、取締役会を持つ大企業や上場企業においては、取締役がリスクマネジメント体制の構築義務を負うとされています。
　以上のことを勘案し、経営層はクラウドサービスの利用サイクルの全般に渡りリスクマネジメントを適用する仕組みを、企業内に率先して構築することが望ましいと解釈されています。

4. 利用者の権利保護とコンプライアンス確保のカバー範囲について

　すでに述べたように、本ガイドでは利用者の権利保護とコンプライアンス確保に重点を置いた解説をしています。第１版では以下の法体系をカバーしました。第２版以降では、重点テーマを持って、さらにこのカバレージを拡大していく予定です。

【本ガイドの第１版がカバーした法体系】
1．利用者の権利保護の側面
- ■ 不正競争防止法（営業秘密管理）

2．利用者のコンプライアンス確保の側面
- ■ 会社法、金融商品取引法（いわゆるJ-SOX法）
- ■ 個人情報保護法
  「健康保険・福祉分野」「放送・郵便分野」「経済産業分野」「雇用管理分野」「法務分野」「企業年金分野」「外務分野」「財務分野」「農林水産分野」「国土交通分野」「環境分野」
- ■ 外国為替及び外国貿易法（外為法）：技術情報の海外流出防止
- ■ 電子計算機を使用して作成する国税関係帳簿書類の保存方法の特例に関する法律（電子帳簿保存法）、法人税法等：帳簿等の電子保存

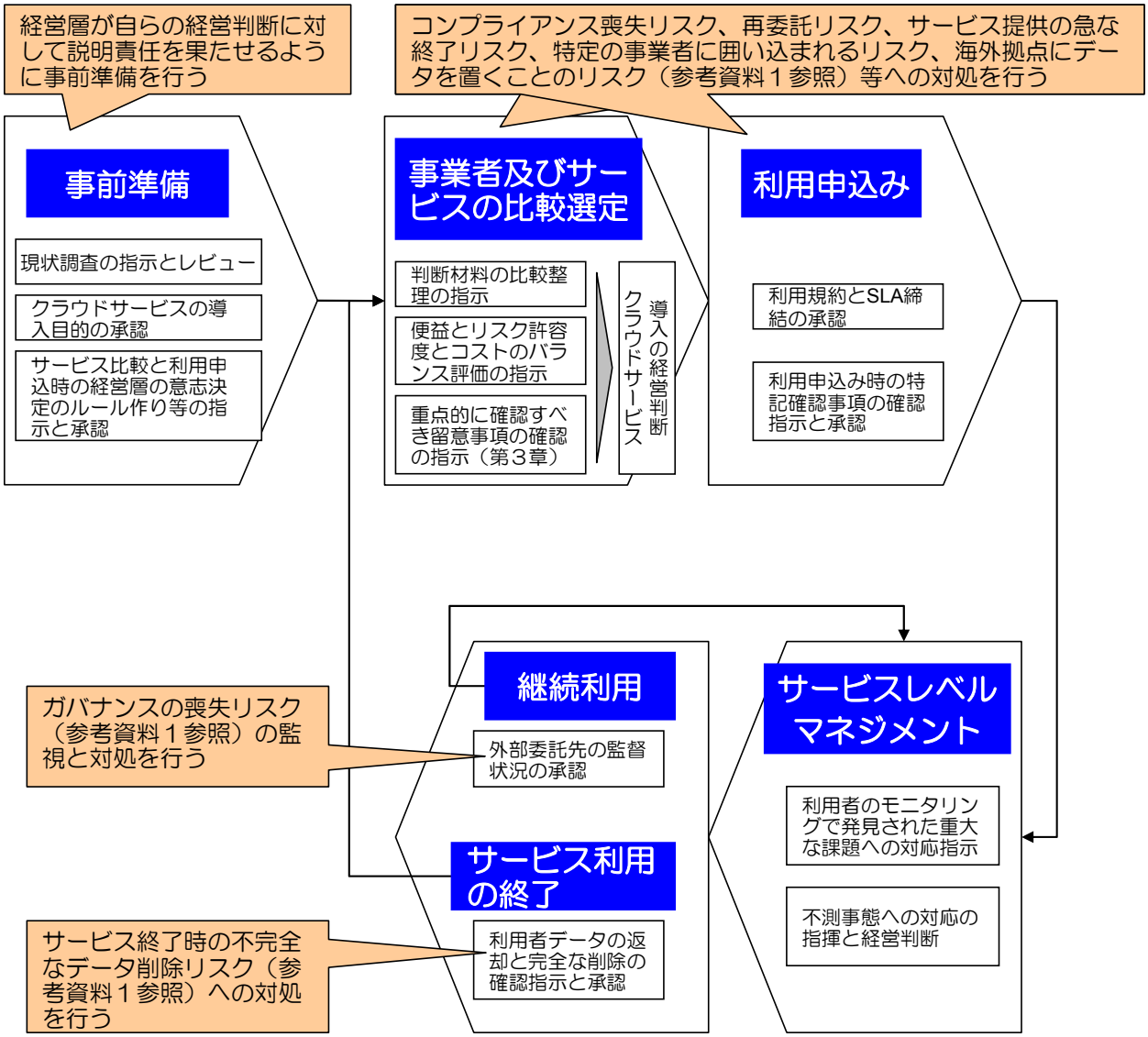
【本ガイドの第２版以降でカバーする予定の法体系】
1．利用者の権利保護の側面
- ■ 知的財産権（産業財産権、著作権等）に係る法体系

2．利用者のコンプライアンス確保の側面
- ■ 個人情報保護法
  「医療・介護分野」「金融・信用分野」「医療・遺伝等の研究やその情報を用いた事業分野」「労働関連分野」「教育分野」「警察・防衛分野」
- ■ e-文書法に関連する帳簿・台帳・図面等の電子保存を認めている法体系
- ■ 建設業法等の業法

第2章　サービスの利用サイクルとリスクマネジメント

クラウドサービスの利用サイクルは、事前準備→サービスの比較選定→利用申込み→サービスレベルマネジメント（利用中）→継続利用→・・・・→サービス利用の終了というフェーズから構成されます。

以下では、クラウドサービス利用の各フェーズにおいて、サービスを安心して利用できるように経営層が行うべきリスクマネジメントについて解説していきます。



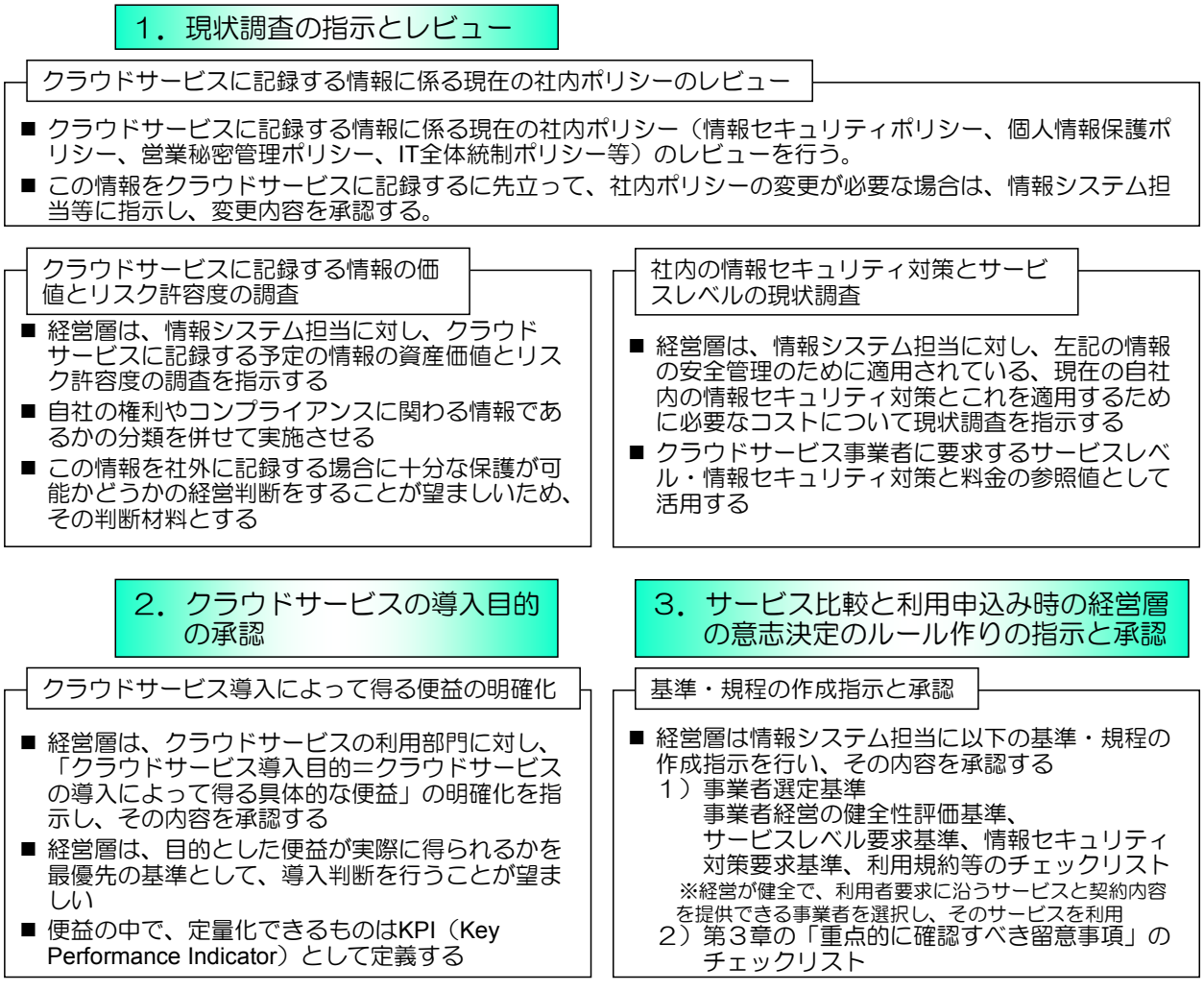
1. 事前準備

事前準備の目的は、現状調査と契約時の経営層の意志決定に向けての準備です。

現状調査は、経営層が率先して、クラウドサービスに預けようとしている情報の価値とリスク許容度を理解し、その上で、この情報に対して現在社内でどのくらいのコストをかけてどのくらいのサービスレベルと情報セキュリティ対策を実現しているかを把握しようとするものです。クラウドサービス事業者への要求を決めるにあたっての基礎資料として活用します。経営層は、現状調査を情報システム担当に指示し、その報告内容をレビューします。

経営層は、クラウドの利用部門に対し、クラウドサービスの導入によって得られる具体的な便益の明確化を指示し、その内容を承認します。サービス導入にあたって最優先されるべき判断基準は便益であり、この便益が確保されることを前提に、他の導入条件を比較評価します。

経営層は、情報システム担当に対し、事業者選定基準と第３章の「重点的に確認すべき留意事項」のチェックリストの作成を指示し、その内容を承認しておきます。これにより、透明性の高い事業者選定を行うことができるようになります。



2. 事業者及びサービスの比較選定

サービスの比較選定段階では、まず、実務担当者がクラウド事業者から情報収集し、判断材料の整理を行います。その報告に基づき、経営層は便益を第１として、リスク許容度やコストとのバランスを勘案し、クラウドサービスを導入するかどうかを経営判断します。次に、業者選定基準に従って、クラウドサービス事業者を選定し、経営層が選定結果を承認します。

但し、クラウドサービス事業者の選定にあたり、①第３章に示された重点的に確認すべき留意事項に対応することが可能であり、②自社のポリシーとニーズに合致した利用規約を提示できる事業者が選定されていることを確認しておく必要があります。

１．判断材料の比較整理の指示

- 経営層は、情報システム担当に、「事前準備」のプロセスで策定した「業者選定基準」と第３章の「重点的に確認すべき留意事項」のチェックリストに従って、必要な情報をクラウドサービス事業者から収集し、比較整理して報告することを指示する。

２．便益とリスク許容度とコストのバランス評価の指示

便益とリスク許容度とコストの比較

- 最優先事項として、便益を確保し、クラウドサービス導入の正当な目的を達成する。
  （例：導入目的が、中小企業の情報セキュリティ体制強化である場合は、導入目的に合致した良いサービスの選択が比較的容易）
- 便益の確保と利用者の社内ポリシー遵守を前提として、必要な情報セキュリティ対策・サービスレベルを実現できるコストと、記録する情報のリスク許容度のバランスを比較評価する。また、社内にそのまま置くことと、クラウドサービス事業者に情報を預けることと、どちらがリスクが高くなるかも比較検討する。
- 経営層は、情報システム担当に、この比較評価の報告作成を指示し、その内容をレビューする。

３．重点的に確認すべき留意事項の確認の指示

特記確認事項の確認の指示

- 経営層は、情報システム担当に、第３章の「重点的に確認すべき留意事項」の確認を指示する
- クラウドサービス事業者に預ける情報が自社の権利やコンプライアンス確保に関係するものである場合は、第３章１．のチェックを行うために必要な情報を個別に事業者から確認するよう指示する
- 海外のデータセンターに情報を記録する計画である場合は、第３章２．のチェックを行うために必要な情報を個別に事業者から確認するよう指示する
- 第３章３．の「利用者とクラウドサービス事業者の意識のずれが生じやすい項目」についてチェックを行うために必要な情報を個別に事業者から確認するよう指示する

４．クラウドサービス導入の経営判断

- 便益とリスク許容度とコストの比較評価結果に基づき、クラウドサービスの導入可否の経営判断を行う
- 予め経営層が承認しているクラウドサービス事業者の選定基準に則り、判断材料の比較整理結果に基づいて事業者及びサービスの選定を実施し、選定結果を経営層が承認する。
- 事業者及びサービスの選定の承認にあたっては、重点的に確認すべき特記確認事項に対応できる事業者とサービスが選択されているかを確認の上、意志決定を行う
- 自社の情報セキュリティポリシーが求めている場合は、クラウドサービス事業者が自社の内部監査に必要な協力をしてくれるかを情報システム担当に確認させ、その報告を確認する

3. 利用申込み

利用申込みにあたっては、利用規約の内容を予め用意したチェックリストに従って細かくチェックし、その結果を経営層が見て承認を行います。SLA については、サービスの比較選定のフェーズで行った事業者選定の経営判断に従い、その内容を再確認して締結します。

SLA の締結にあたっては、第３章３．に「利用者とクラウドサービス事業者の意識が潜在的にずれやすい注意点」を示しています。経営層は、情報システム担当に対し、事業者選定の段階で行った比較評価の結果を参考にしつつ、これらの注意点の最終確認を行うように情報システム担当に指示し、その報告を承認します。

１．利用規約とSLA締結の承認

利用規約とSLA締結の承認

- 経営層は、情報システム担当に対し、事前準備で策定した「利用規約等のチェック内容」文書に基づいて、利用規約を慎重にチェックするように指示する。特に問題がなければ、経営層が承認を行う。
- SLAについては、サービスの比較選定のフェーズで、事業者選定基準に基づいて、自社が求めるサービスレベルを妥当なコストで提供できるクラウドサービス事業者を経営層が承認済みであるため、ここでは、情報システム担当は、クラウドサービス事業者が提示するSLAメニューと自社の社内ポリシーを詳しく照らし合わせ、細かい詰めの確認作業を行う。
- その結果定められたSLAの内容につき、経営層が承認の上、SLAを締結する。

２．利用申込み時の特記確認事項の確認指示と承認

利用申込み時の特記確認事項の確認指示と承認

- 利用者とクラウドサービス事業者の意識が潜在的にずれやすい注意点があり、利用申込み時の特記確認事項となっている（第３章３．参照）。
- 経営層は、本ガイド第３章３．の記述に基づき、情報システム担当に対して、これらの特記確認事項の確認を指示し、その報告を承認する。実際には、サービスの比較選定の段階で、意識のずれが生じないように下調べをしてあるため、ここでは再確認の意味合いが強くなる。

4. サービスレベルマネジメント

サービスレベルマネジメントのフェーズにおける経営層の役割は、主として不測事態等への対応となります。

（１） 利用者のモニタリングで発見された重大な課題への対応指示

自社の日常の運用モニタリングにおいて、クラウドサービス事業者の管理監督やサービスレベル確保に係る重大な課題が発見された場合は、経営層は情報システム担当に原因の究明と対応策の作成を指示し、その報告をレビューして承認します。

（２） 不測事態への対応の指揮と経営判断

広域災害や個人情報の大規模漏洩など、不測事態に直面した場合には、経営層は対応を指揮し、企業としての説明責任を果たし、必要な経営判断を行います。

5. 継続利用またはサービス利用の終了

このフェーズでは、クラウドサービスの契約を更新するかどうかを判断します。

継続利用の場合、経営者は、自社が過去１年間外部委託先を適切に監督できたかの報告を情報システム担当から受け、その内容をレビューします。自社が外部委託先を適切に監督できたことを証明するために、クラウドサービス事業者から第三者証明の提出を求めることもできます。

サービスの利用を終了し、他のサービスに変更する際には、利用者データの返却と、クラウドサービス事業者のストレージからの完全な消去が不可欠です。特にパブリッククラウドを利用している場合には、十分に注意して作業の完遂を確認することが必要です。経営層は、情報システム担当に注意深い確認を指示し、その完了報告を承認します。

１．継続利用

外部委託先の監督状況の承認

- 適用法が、「システム業務の外部委託」先の適切な監督を求めていることは多い。
- 経営層は、情報システム担当者に指示して年間の外部委託先の監督状況について報告させ、承認する。
- 経営層としては、外部委託先を適切に監督していることを証明するために、クラウドサービス事業者に対し、第三者証明の提出を求めることもできる。
- この場合には、クラウドサービス事業者に対し、日本公認会計士協会IT委員会研究報告第39号（平成22年5月）が定める「情報セキュリティ検証業務」による情報セキュリティ検証報告書の提出を求めることも一案である。

※会計報告に係る内部統制確保の観点からは、クラウドサービス事業者がSAS70を取得しているかどうかが「外部委託先のコントロールの証明」にあたり重要になる。会計報告に限定されない場合は、SAS70は厳密には「第三者証明」にはならない。しかし、当該クラウドサービス事業者の経営姿勢を示すものとして、広く参考にされている実状がある。

２．サービス利用の終了

利用者データの返却と完全な削除の確認指示と承認

- クラウドサービス利用の終了時に、利用者のデータを利用者が取扱い可能なフォーマットで受け取ることは非常に重要である。経営層は、情報システム担当に対し、予めデータ受領のルール（必要な時間、方法、データ書式等）を定めておき、このルールに従ってデータの返却を確実に受けるように指示する。また、データ返却の完了報告を受け、これを承認する。

- パブリッククラウドを利用している場合は、データ消去証明書を受領するか、それが困難な場合には代替する方法により、利用者データが完全に消去されたことを確認する必要がある。経営層は、情報システム担当に確認を指示し、その完了報告を承認する。データ消去証明書に代替する手法を用いる場合は、その手法の妥当性を情報システム担当に十分に確認させること。

第3章　重点的に確認すべき留意事項について

本章では、クラウドサービス利用者を保護するとともに、利用者がコンプライアンスを確保できるようにするため、重点的に確認すべき留意事項を３つの観点から解説します。

1. 利用者の権利保護とコンプライアンス確保のチェックについて

ここでは、クラウドサービスを利用するにあたり、利用者の権利を国内法に基づいて守り、利用者が国内法に基づいてコンプライアンスを確保するためのチェック方法について解説します。利用者がクラウドサービスに記録することを計画している情報の種別に合わせて、関係する箇所を読んで下さい。

クラウドサービスに記録する計画の情報種別		読者が読むべき記載箇所
利用者の権利保護	営業秘密	（１）
利用者のコンプライアンス確保	取締役の職務執行に係る情報・財務報告に係る電子的記録（内部統制関連）	（２）ア.
	個人情報	（２）イ.
	技術情報	（２）ウ.
	国税関連帳簿書類	（２）エ.

（１） 利用者の権利保護の側面

国内法によって保護されるクラウドサービス利用者自身の権利として代表的なものは、利用者の営業秘密、利用者の持つ知的財産権などです。

営業秘密については、法的保護を受けるための必要３要件（①秘密として管理されていること、②有用な情報であること、③公然と知られていないこと）を確保することが重要です。クラウドサービスを利用する際には、「①秘密管理性」の成立要件が確保できなくなるリスクがあるため、経営層は注意が必要です。クラウドサービスの利用によって、自社の営業秘密管理ポリシーや運用ルールとの齟齬が生じ、この齟齬が「①秘密管理性」要件の成立を妨げないかを、経済産業省が策定した「営業秘密管理指針」（参考資料３参照）に基づいて確認して下さい。

【「営業秘密管理指針」に基づくチェックにおける重点確認ポイント】

１．秘密管理方法に係る契約内容等
- 技術管理における「アクセス及びその管理者の特定・限定」、「外部からの侵入に対する防御」「データの消去、廃棄」
- 法的証拠能力確保等に関する管理

２．秘密管理を適切に機能させるための組織的管理に係る契約内容等
- 内部監査への協力

この確認にあたっては、担当者に調査させ、経営層が調査内容をレビューして下さい。このレビュー結果に基づいて、「営業秘密をクラウドサービスに記録する」「クラウドサービスに記録する情報は営業秘密として管理しない」「営業秘密をクラウドサービスには預けない」等の経営判断を行います。

※この他にも、知的財産権（産業財産権・著作権等）などがあり、本ガイドの今後の更新において、権利保護について記述を増補していく予定です。

（2） 利用者のコンプライアンス確保の側面

利用者のコンプライアンス確保については、主として次のような法令が関係してきます。

【利用者のコンプライアンス確保に関係する法令】
ア. 会社法、金融商品取引法（いわゆる J-SOX 法）：上場企業や大会社における内部統制
イ. 個人情報保護法
ウ. 外国為替及び外国貿易法（外為法）：技術情報の海外流出防止
エ. 電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関する法律（電子帳簿保存法）、法人税法等：帳簿等の電子保存
オ. 利用者が日常遵守している業法：監督官庁による規制　等

個々の法令によって、クラウドサービスの利用に際し利用者のコンプライアンスが確保されるかのチェック方法は異なっています。以下では、業法以外についてこのチェック方法を解説します。なお、チェックにあたっては、担当者に調査させ、経営層が調査内容をレビューして下さい。このレビュー結果に基づいて、クラウドサービス導入可否の経営判断を行います。

※利用者が日常遵守している監督官庁制定の業法等については、本ガイドの今後の更新において、コンプライアンス確保について記述を増補していく予定です。

ア. 内部統制に係るチェック

取締役会を設置する大会社においては、クラウドサービスを利用することにより、会社法施行規則第百条の一が求める「業務の適正を確保するための体制」の確立が阻害されないかをチェックします。リスクマネジメントの方針策定、体制構築、モニタリング方法の整備などが求められるほか、これらが実態的に機能していることを後から検証できる仕組み作りが必要とされています。

同じように、上場企業においては、J-SOX 法に基づき、クラウドサービスを利用するにあたって、財務報告に関して同様のリスクマネジメント確立が求められており、これが実態的に機能しているかを後から検証できる仕組み作りも要求されています。

本ガイドではこれらについては詳しく解説しません。COSO フレームワークの解説等を参照して下さい。

イ．個人情報保護に係るチェック

個人情報保護に係るコンプライアンス確保については、各省庁が定めている個人情報保護に関するガイドライン（参考資料３参照）が、「個人データの委託先の監督」についての指針を定めています。クラウドサービスを利用する際にコンプライアンスを確保できるかのチェックもこれらの指針に従って行って下さい。

指針の内容は策定した省庁によりかなりの違いがあるため、自社の事業分野に即したガイドライン（参考資料３参照）を選択してチェックを行って下さい。

【個人情報保護に関するガイドラインを見る際の注意点（ガイドライン間で異なる部分）】

1．委託先の選定基準策定を求めているか
2．委託契約に含めるべき事項の要求内容（詳細さ、再委託の扱い、契約終了時の扱い等）
3．委託先に対する定期・非定期の監査を求めているか
4．個人データ漏洩等の事故時における委託元への報告義務を要求しているか。また、事故時の委託先の責任の明確化を求めているか。
5．契約内容の定期的な見直しを求めているか
6．委託にあたっての個人データの匿名化について言及しているか

※本ガイドでは、「健康保険・福祉分野」「放送・郵便分野」「経済産業分野」「雇用管理分野」「法務分野」「企業年金分野」「外務分野」「財務分野」「農林水産分野」「国土交通分野」「環境分野」をカバーしています。この他にも、「医療・介護分野」「金融・信用分野」「医療・遺伝等の研究やその情報を用いた事業分野」「労働関連分野」「教育分野」「警察・防衛分野」などで個人情報保護関連のガイドラインが策定されており、本ガイドの今後の更新において、コンプライアンス確保について記述を増補していく予定です。

ウ．技術情報の流出防止に係るチェック

海外のデータセンターを用いたクラウドサービスを利用する際には、輸出貿易管理令の別表に掲載されている「海外に流出させてはならない技術情報」の流出リスクを考慮する必要があります。

経済産業省が策定した技術流出防止指針（参考資料３参照）では、「重要なノウハウを安易に文書に表示しないように配慮するとともに、図面や書面上ノウハウが記載されている場合には営業秘密等として厳格に管理することが必要」としています。従って、自社の営業秘密管理ポリシーに基づいて、営業秘密を海外のデータセンターに保存できるかを意志決定することにより、海外のデータセンターを用いたクラウドサービスに技術情報を記録することができるかを経営判断することができます。

エ．国税に関する帳簿書類の電子保存に係るチェック

電子帳簿保存法施行規則によると、国税に関する帳簿書類の電子保存に関し、次のような要件を課しています[1]（参考資料３参照）。

【電子帳簿保存法施行規則における帳簿書類の電子保存要件】
1．　真実性の確保（データの訂正削除の履歴確保）
2．　相互関連性（帳簿の記録事項と関連する記録事項の関連性が確認できる）の確保
3．　関連書類（電磁的記録の備え付け及び保存に関する事務手続を明らかにした書類）の備え付け
4．　見読性の確保（ディスプレイ、プリンタに整然と出力可）
5．　検索性の確保（取引年月日、勘定科目、取引金額等での検索機能）
6．　電子署名とタイムスタンプの付与

真実性の確保及びこれに係る法的証拠能力、見読性確保の方式、法が求める長期間保存を確保するためのサービス継続性、電子署名・タイムスタンプの運用上の問題点の有無等を検討し、クラウドサービスの利用可否を経営判断します。

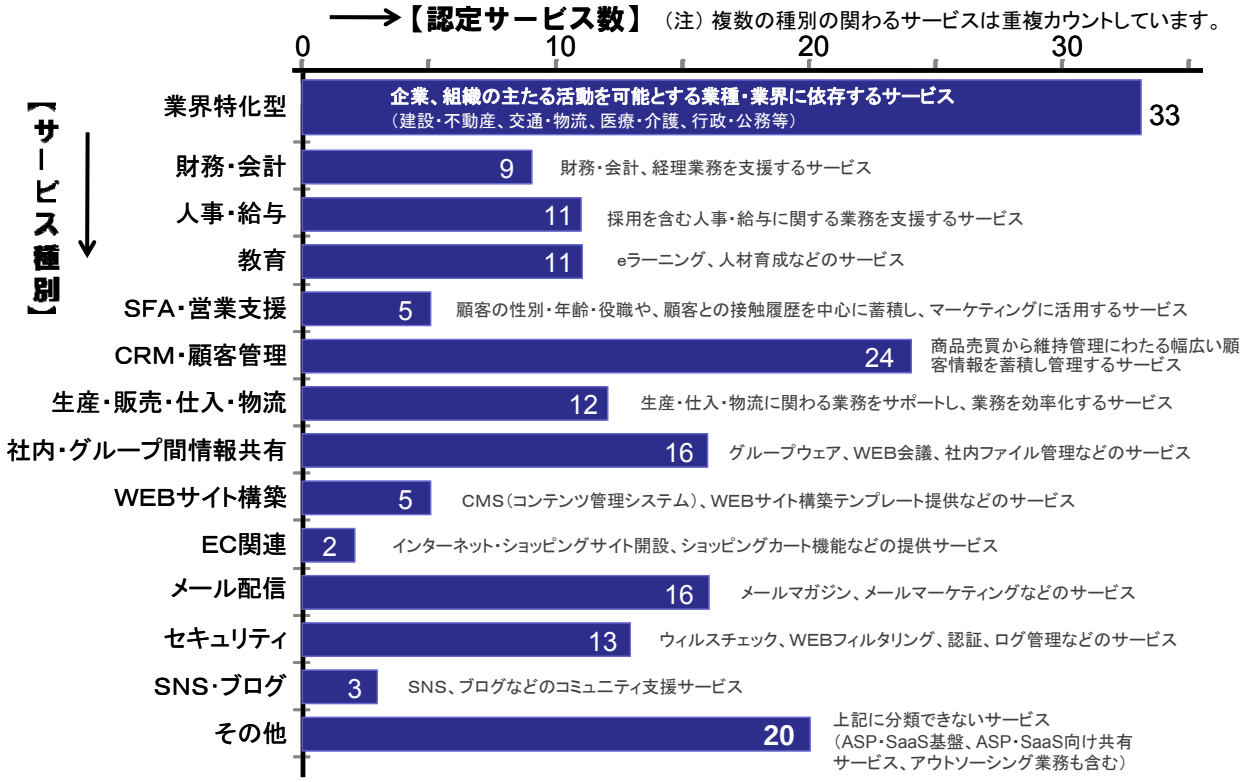
※電子保存に関しては、e-文書法に関係して、他省庁においても、帳簿・台帳・図面等の電子保存を認めていることから、本ガイドの今後の更新において、コンプライアンス確保について記述を増補していく予定です。

（３）　ASP・SaaS 安全・信頼性に係る情報開示認定制度の活用

経営判断のための情報収集において、クラウドサービス事業者の情報開示の実態と取組姿勢が重要となります。現時点では、財団法人マルチメディア振興センターが運用する「ASP・SaaS の安全・信頼性に係る情報開示認定[2]」を取得した優良なクラウドサービス事業者を率先して選択することが望ましいと言えます。この認定を取得したクラウドサービス事業者は、提供しているサービスの安全・信頼性に係る情報開示を徹底して行っています。

現在、「クラウドサービスの安全・信頼性に係る情報開示指針」及びその認定制度について検討が進められており、今後はこの新しい指針と認定制度が重要な役割を果たすものと期待されています。

[1] 電算処理を外部委託し、処理プログラムとして自社開発ではないものを用いている場合。クラウドサービスの利用は一般にこの条件に合致します。
[2] http://www.fmmc.or.jp/asp-nintei/



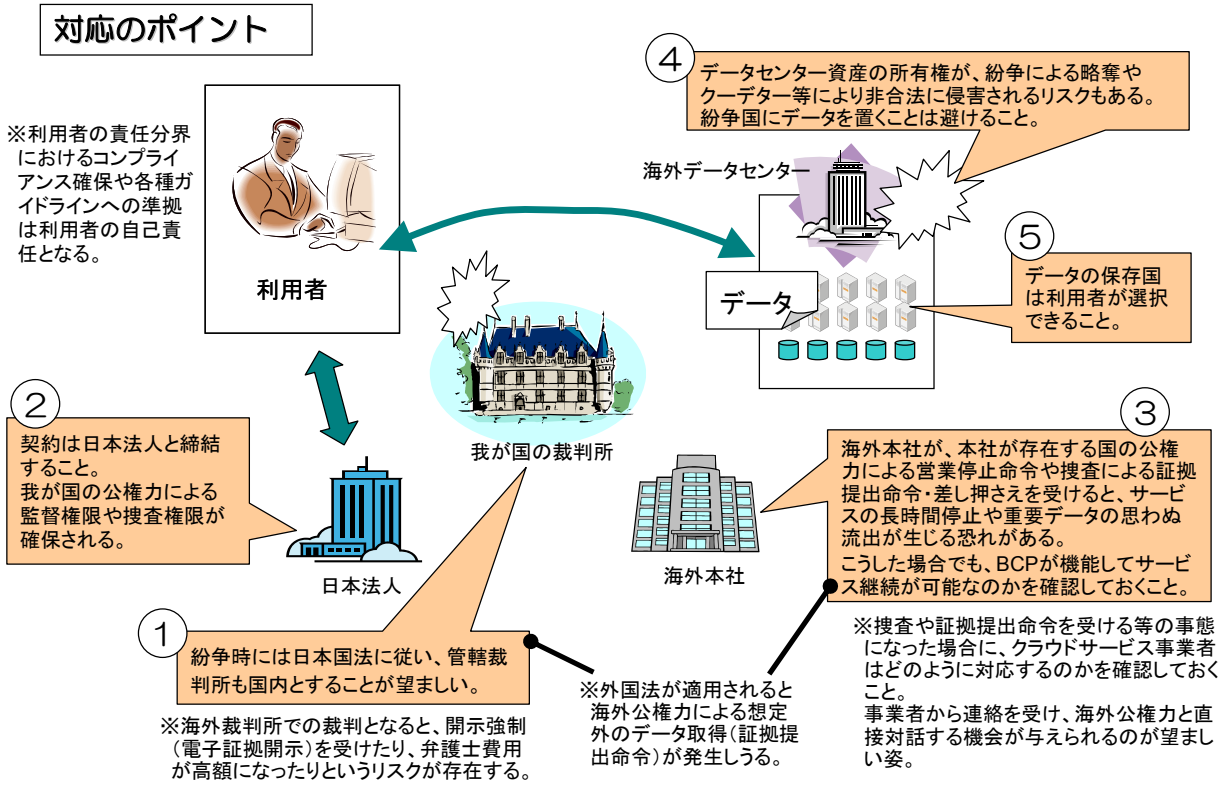
「ASP・SaaS安全信頼性に係る情報開示認定制度」における
サービス種別ごとの認定サービス数

※ASP・SaaS安全信頼性に係る情報開示認定制度のWebサイト（ http://www.fmmc.or.jp/asp-nintei/ ）情報をもとに作成

2. 海外にデータを置く場合等について

海外のデータセンターにデータを置く場合、または海外に本社がある外資系企業のサービスを利用する場合には、国内法と海外法の適用関係をきちんと整理しておく必要があります。

契約時の注意点（適用法と管轄裁判所の場所、日本法人との契約）、海外の公権力の捜査等が及んだ場合の連絡対応とサービス継続能力、紛争国にデータを置くことを避けることなどが主たる注意点となります。



※データの保存国を利用者が選択しても、紛争時の適用法が当該国の法になるという保証はありません。⑤だけでは不十分であり、契約により①も確保することが望ましい対応です。

3. 利用者とクラウドサービス事業者の意識のずれを防止するために

クラウドサービスの契約時に、利用者とクラウドサービス事業者の意識が潜在的にずれやすい注意点があります。これらは、サービス選定時の特記確認事項となりますので、経営層は情報システム担当に十分な注意を払うように指示して下さい。

（1） クラウドサービスにおける利用者と事業者の責任分界

利用者とクラウドサービス事業者の間で、責任分界の意識が食い違うことが良くあります。経営層から情報システム担当に対し、以下の項目に関する責任分界の意識の食い違いを予防するための方針を定めるように指示して下さい。

1． 利用者とクラウドサービス事業者と通信プロバイダの間のネットワークの運用管理
2． OS やコンピューティングリソースの管理運用
3． アプリケーションレベルの運用管理
4． クラウドサービス事業者が自社内に設置する機器・設備等の運用管理

（2） 利用者とクラウドサービス事業者の意識がずれやすい注意点

クラウドサービスを利用する上で、利用者とクラウドサービス事業者の間で、「コンプライアンス違反リスク」「ガバナンスの喪失リスク」「サービス提供の急な終了リスク」「サービス終了時の不完全なデータ削除リスク」等に関して、基本方針レベルで責任に対する意識が潜在的にずれている場合があります。このずれはこれらのリスクが顕著に発現する重要なきっかけとなりえます。具体的な対応としては、クラウドサービス事業者の考え方を十分に聴取して意識のずれをなくした上で比較検討を行い、利用者のポリシーやニーズを満足する事業者とサービスを選択するようにします。主要な７つのチェックポイントは以下の通りです。

1．コンプライアンス義務に対する認識の違いがないか
＜解説＞個人情報保護、営業秘密の秘匿、内部統制の構築・運用等に関するコンプライアンス確保の考え方が、利用者とクラウドサービス事業者の間で経営方針レベルで食い違っていると、クラウドサービスの利用によって利用者が求めるコンプライアンス義務を遵守できなくなる恐れがあります。自社が重視するコンプライアンス確保について、クラウドサービス事業者がどのような考えで取り組んでいるかを詳しく確認して下さい。

2．個人情報や営業秘密が漏れる等の「重要インシデント」が発生した場合の説明責任の果たし方に対する認識の違いがないか
＜解説＞重要インシデントがクラウドサービス事業者側で発生した場合でも、利用者企業側が主体となって説明責任を果たす必要がある場合が多くあります。例えば、利用者企業が顧客から預かった個人情報が、クラウドサービス事業者側で漏洩した場合がこれにあたります。この場合、利用者企業がきちんと説明責任を果たせるように、クラウドサービス事業者と一体となって活動するためには、両者の責任に対する認識を合せる必要があります。契約前に情報提供の内容と方法等、具体的アクションを確認して下さい。

３．損害賠償と稼動保証違反
＜解説＞クラウドサービス事業者の責任により利用者が損害を受けた場合の損害賠償の範囲について意識にずれが生じることがあります。例えば、クラウドサービス事業者が稼働率を保証をしているといっても、それは時間的なものに過ぎず、損害賠償もその時間に対する代金の減額が約定されているにすぎないのが一般です。履行されないことによる事業の損失や、データの損失による損害が賠償されるわけではないことに留意する必要があります。

４．クラウドサービス事業者側からの要請でサービス内容を変更する場合の手続き
＜解説＞アプリケーションサービスでは、サービス機能の更新はクラウドサービス事業者に任されており、利用者はシステムバージョンアップコストを払わなくても済みます。一方で、利用者の意図に沿わない改修が事業者によって行われることもありえます。サービス機能の更新にあたり、クラウドサービス事業者がどのような手続きプロセスを踏むのかを詳しく確認して下さい。

５．クラウドサービス事業者側の都合でサービス終了する場合の手続
＜解説＞クラウドサービスが突然終了すると、利用者側に唐突に深刻な影響を及ぼすことがあり得ます。企業経営が健全なクラウドサービス事業者を選択するとともに、事前告知期間の確認を契約前にしておく必要があります。

６．データのオーナーシップと取扱いの確認
＜解説＞クラウドサービスの利用にあたり、クラウドサービス事業者のストレージに蓄積されるデータ（アプリケーションデータ、文書データ、図面データ、ログデータ等）のオーナーシップについて、利用者とクラウドサービス事業者の間で意識のずれが生じることがあります。この潜在的な意識のずれは、これらのデータの２次的利用（統計処理、データマイニング等）の可否に対する見解の相違という形で顕在化しやすいのが実状です。利用者がオーナーシップを持つデータの範囲について、クラウドサービス事業者の考え方を詳しく確認し、自社の考え方と合致する事業者を選択するようにして下さい。
※オーナーシップ：データを作成・改変・消去する権利のこと

７．利用者データの完全な消去
＜解説＞「利用者データの完全な消去」に対する利用者とクラウドサービス事業者の考え方にずれが生じる可能性があります。特に、データの消去方法について意識の違いがないかを良く調査し、利用者が許容できる方法をクラウドサービス事業者が提供できるかを契約前に詳しく確かめて下さい。

参考資料１　技術用語の解説

本文書で用いられている技術用語の解説を以下に示します。

【クラウドサービスの提供形態】

■ IaaS（Infrastructure as a Service）：
利用者にサーバーやストレージをサービスとして提供します。利用者は、これらのハードウェアを自ら保有しなくても、自由に利用できるようになります。

■ PaaS（Platform as a Service）：
利用者がアプリケーションを開発したり、開発したアプリケーションを利用したりする（または外部にサービスを提供する）ためのハードウェア/ソフトウェア基盤を提供するサービスです。利用者は少ない投資で新しいアプリケーションを構築できるようになります。

■ アプリケーションサービス：　　※ASP・SaaS と呼ぶことも多い
アプリケーションの利用をサービスとして提供します。利用者は、高機能アプリケーションを、自ら開発したり更新したりすることもなく、利用することができます。

【クラウドサービスの実現形態】

■ プライベートクラウド：
クラウドサービスを、企業の情報セキュリティ管理区域内に閉じたシステム構成で提供します。自社開発システムとあまり異ならない運用管理方法で利用することができます。利用者の要求に即した運用管理やカスタマイズが可能です。

■ パブリッククラウド：
クラウドサービスを、企業の情報セキュリティ管理区域外に構築されたシステムにより提供します。最もクラウドらしい特徴（リソースの割り勘効果、蛇口をひねると欲しいだけの水がすぐに出る水道サービスのようなリアルタイムオンデマンド性等）を備えたサービスです。しかしながら、レディメイドの色合いが強く、安全管理に係る利用者の細かい要求に応じにくいため、利用者が賢く選択することが求められます。

■ ハイブリッドクラウド：
プライベートクラウドとパブリッククラウドの両者を組み合わせたクラウドサービスです。両者の利点を使い分けることができるようになります。

【その他の用語】

■ SLA（サービスレベルアグリーメント）：
利用者とクラウドサービス事業者が運用管理におけるサービスレベルについて合意した内容を書面で作成したものです。サービスの信頼性や性能、安全管理の品質、サポートの品質等について、サービスレベルの合意を行います。SLA の締結は追加費用を伴うため、必要十分な合意のみを行い、記録するようにします。

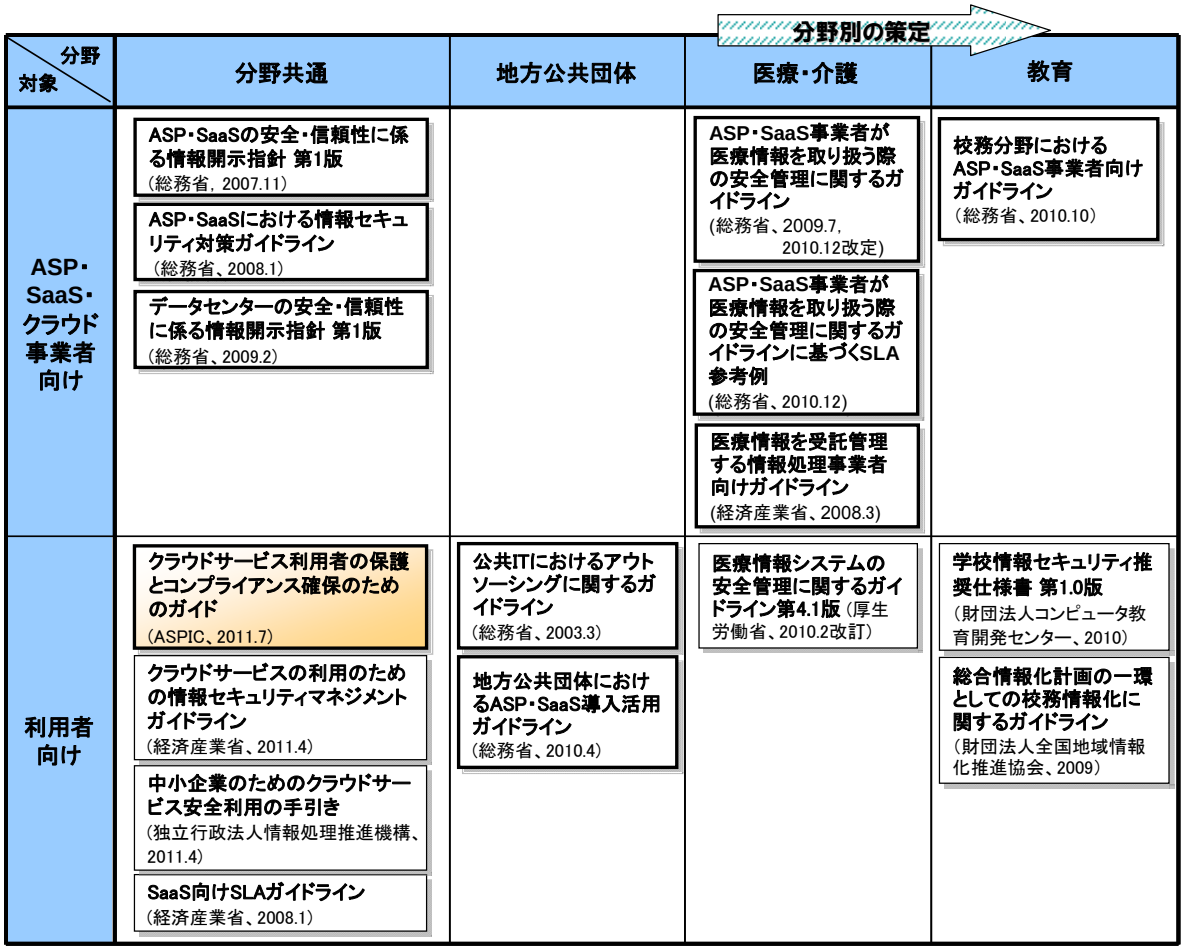
【クラウドサービスに関するリスクの解説】

クラウドサービスは、「システム業務の外部委託」を行うサービスの技術的な進化形であると言えます。パブリッククラウドでは、物理的なハードウェアやデータセンターが利用者から「ブラックボックス化」されたため、もともと意識されてきた以下のようなリスクがさらに重視されるようになってきました。特に、ガバナンス喪失リスク、コンプライアンス違反リスク、サービス終了時の不完全なデータ削除リスク、海外拠点にデータを置くことのリスクは重視されています。

用語	リスクの発現状態
ガバナンスの喪失リスク	細かいリスクコントロールが効かない、システム運用のブラックボックス化、証拠保全が困難になる、SLA の設定が難しい、重大インシデント発生時の事業者の情報開示が不十分になる　等
コンプライアンス違反リスク	ガバナンスの喪失により、法制度遵守に必要かつ適切なクラウドサービス事業者の監督が困難。事業者が情報開示しないと、第三者監査ができず、正当性の確認ができない。
再委託によるリスク	クラウドサービス事業者がサービス提供に係る再委託先をきちんと監督していない
サービス提供の急な終了リスク	クラウドサービス事業者の倒産や買収等に伴い、サービス提供が突然終了してしまう
特定の事業者に囲い込まれるリスク	データ移行が難しく特定のクラウドサービス事業者に囲い込まれる
サービス終了時の不完全なデータ削除リスク	サービス利用の終了にあたり、クラウドサービス事業者が利用者データを完全に消去できない
海外拠点にデータを置くことのリスク	どの国の法律により紛争解決されるのかが複雑になる。海外公権力による想定外のデータ取得（証拠提出命令）・開示強制（電子証拠開示）や紛争・クーデターによる非合法略奪を受ける。技術情報の海外持ち出しが外為法に抵触する。

参考資料２　クラウドサービス関連のガイドライン・指針

＜全体像（網掛けが本文書）＞



【ASP・SaaS の利用者に関するもの】

■地方公共団体における ASP･SaaS 導入活用ガイドライン[総務省]：平成 22 年４月

地方公共団体が ASP･SaaS の利用にあたって留意すべきことを整理したもの

■SaaS 向け SLA ガイドライン[経済産業省]：平成 20 年 1 月

企業の経営者および情報システム担当者が SaaS を利用するにあたって適切な取引関係を確保し、より効果的に利用することを目的に、情報セキュリティ確保の観点に重点を置き SaaS の特徴について解説し、利用するサービスおよびサービス事業者選定の際に参考となるような利用者への対策向上のガイドラインを提供したもの

【クラウドサービスの利用者に関するもの】

■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[経済産業省]：平成 23 年 4 月

組織がクラウドコンピューティングを全面的に利用する極限状態を想定し，①自ら行うべきこと，②クラウド事業者に対して求める必要のあること，③クラウドコンピューティング環境における情報セキュリティマネジメントの仕組みについて記載したもの。
JIS Q 27002（実践のための規範）の各管理策を再考し、クラウド・コンピューティングを利用する組織においてこの規格に基づいた情報セキュリティ対策が円滑に行われることを目的としている。

■中小企業のためのクラウドサービス安全利用の手引き[独立行政法人情報処理推進機構]：平成 23 年 4 月

中小企業によるクラウドの利用についての判断やその条件の確認、注意点の点検等が比較的容易にできるように、解説やチェック項目を整理したもの。

参考資料３　利用者の権利とコンプライアンスに係る資料

ここでは、本ガイドが参照した利用者の権利とコンプライアンスに係る各省庁等の指針について示しています。

（注）本参考資料は各省庁が策定したガイドラインを網羅したものではありません。御社が遵守している法規・ガイドラインが他にもありましたら、それを補ってご活用下さい。

【利用者の権利に関するもの】

■経済産業省　不正競争防止法による営業秘密の保護

名称	公表・見直し（最新のみ）	監督官庁または発行主体
営業秘密管理指針 第２章　１．営業秘密の定義 第３章　２．営業秘密の管理のために実施することが望ましい秘密管理方法　３．営業秘密の管理を適切に機能させるために実施することが望ましい組織的管理の在り方	平成 22 年４月	経済産業省

※システム業務の外部委託に関して明示した記述はない。クラウドサービスを利用する場合は、事業者側に保存される営業秘密が、営業秘密の定義が示す要件を満足するかどうかが論点となる。

【利用者のコンプライアンス確保に関するもの】

■法務省・金融庁　大会社（取締役会設置会社や上場企業）の内部統制

名称	公表・見直し（最新のみ）	監督官庁または発行主体
会社法施行規則 （業務の適正を確保するための体制）　第百条の一	平成 21 年３月	法務省
財務報告に係る内部統制の評価及び監査に関する基準 Ⅰ．２．（６）IT への対応	平成 19 年２月	金融庁
財務報告に係る統制の評価及び監査に関する実施基準 Ⅱ．３．（３）⑤ IT を利用した内部統制の評価　（４）③ IT に係る内部統制の有効性の判断	平成 19 年２月	金融庁

※IT 統制の詳細や外部委託への対応については、COSO フレームワーク等が参考になる。

■各省庁　個人情報保護関連のガイドライン[3]：外部委託要件を明記

[1] 健康保険、福祉分野

名称	公表・見直し（最新のみ）	監督官庁または発行主体
健康保険組合等における個人情報の適切な取扱いのためのガイドライン（局長通達）　Ⅲ ４．（３）業務を委託する場合の取扱い	平成 16 年 12 月	厚生労働省
国民健康保険組合における個人情報の適切な取扱いのためのガイドライン（局長通達）　Ⅲ ４．（３）業務を委託する場合の取扱い	平成 16 年 12 月	厚生労働省
国民健康保険団体連合会等における個人情報の適切な取扱いのためのガイドライン（局長通達）　Ⅲ ４．（３）業務を委託する場合の取扱い	平成 17 年９月	厚生労働省
福祉関係事業者における個人 情報の適正な取扱いのためのガイドライン（局長通達）　Ⅲ ４．（３）業務を委託する場合の取扱い	平成 16 年 11 月	厚生労働省

[2]放送・郵便分野

名称	公表・見直し（最新のみ）	監督官庁または発行主体
放送受信者等の個人情報の保護に関する指針（告示） （委託先の監督）第十六条、第十七条	平成 21 年９月	総務省
郵便事業分野における個人情報保護に関するガイドライン（告示） （委託先の監督）第十一条	平成 20 年３月	総務省
信書便事業分野における個人情報保護に関するガイドライン（告示） （委託先の監督）第十一条	平成 20 年３月	総務省

[3] 消費者庁： http://www.caa.go.jp/seikatsu/kojin/gaidorainkentou.html

[3] 経済産業分野

名称	公表・見直し（最新のみ）	監督官庁または発行主体
個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（告示）　2-2-3-4.委託先の監督（法第２２条関連）	平成 21 年 10 月	経済産業省

[4] 雇用管理分野

名称	公表・見直し（最新のみ）	監督官庁または発行主体
雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針（告示） 第三 四 法第二十二条に規定する委託先の監督に関する事項	平成 16 年７月	厚生労働省

[5] 法務分野

名称	公表・見直し（最新のみ）	監督官庁または発行主体
法務省所管事業分野における個人情報保護に関するガイドライン（告示） 第6 個人データの管理に関する義務 4 委託先の監督【法第 22 条関係】	平成 21 年９月	法務省
債権管理回収業分野における個人情報保護に関するガイドライン 第７個人データの管理に関する義務 4 委託先の監督（法第 22 条関係）	平成 22 年３月	法務省

[6] 企業年金

名称	公表・見直し（最新のみ）	監督官庁または発行主体
企業年金等に関する個人情報の取扱いについて（局長通達） 第五　委託先の監督に関する事項	平成 16 年 10 月	厚生労働省

[7] 外務分野

名称	公表・見直し（最新のみ）	監督官庁または発行主体
外務省が所管する事業を行う事業者等が取り扱う個人情報の保護に関するガイドライン（告示） （個人データの委託に伴う措置） 第十一条	平成 17 年３月	外務省

[8] 財務分野

名称	公表・見直し（最新のみ）	監督官庁または発行主体
財務省所管分野における個人情報保護に関するガイドライン（告示） （委託先の監督） 第 13 条	平成 22 年３月	財務省

［9］農林水産分野

名称	公表・見直し（最新のみ）	監督官庁または発行主体
農林水産分野における個人情報保護に関するガイドライン（告示） 第6 5 委託先の監督（法第 22 条関係）	平成 21 年７月	厚生労働省

［10］国土交通分野

名称	公表・見直し（最新のみ）	監督官庁または発行主体
国土交通省所管分野における個人情報保護に関するガイドライン（告示） （委託先の監督） 第十一条	平成 16 年 12 月	国土交通省

［11］環境分野

名称	公表・見直し（最新のみ）	監督官庁または発行主体
環境省所管事業分野における個人情報保護に関するガイドライン(告示) 第六 4 委託先の監督（法第 22 条関係）	平成 21 年 12 月	環境省

■経済産業省　技術情報の流出防止

名称	公表・見直し（最新のみ）	監督官庁または発行主体
技術流出防止指針 Ⅰ．2.（2） 「意図せざる技術流出」 Ⅱ．5. 製造に必要な図面やノウハウの流出を通じた技術流出 Ⅲ．4．6．製造に必要な図面やノウハウの流出を通じた技術流出を防止するための留意事項（22 ページ）	平成 15 年３月	経済産業省

※流出させてはならない技術の対象は、輸出貿易管理令の別表[4]を参考に判断する。

[4] http://www.kyushu.meti.go.jp/seisaku/boueki/bouekikanri/yushutsurei.html

■財務省　国税に関する帳簿書類の電子保存

名称	公表・見直し（最新のみ）	監督官庁または発行主体
法人税法施行規則　　＜保存場所限定＞ （連結法人の帳簿書類の整理保存）　第八条の三の十 （帳簿書類の整理保存）　第五十九条 （帳簿書類の整理保存等）　第六十七条 ※（参考）帳簿の電子化については、電子帳簿保存法および電子帳簿保存法施行規則（財務省）で定められている[5]。	平成 22 年 10 月	財務省
平成 17 年 1 月 31 日財務省令第 1 号　電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関する法律施行規則の一部を改正する省令　　＜保存要件等の提示＞	平成 17 年 1 月	財務省

[5] http://www.nta.go.jp/taxanswer/hojin/5930.htm