ASP・SaaS における
情報セキュリティ対策ガイドライン

ASP・SaaS の情報セキュリティ対策に関する研究会

平成２０年　１月３０日

目次

Ⅰ　序編

Ⅱ　組織・運用編

Ⅲ　物理的・技術的対策編

Ⅳ　参考資料

Annex 1　ASP・SaaS サービスの典型的な構成要素と情報資産

Annex 2　組織・運用編　対策項目一覧表

Annex 3　物理的・技術的対策編　対策項目一覧表

Ⅰ　序編

Ⅰ．１　はじめに

ブロードバンド化の進展により、国民生活や社会経済活動における ICT への依存度が高まる中、ネットワークを通じてオンデマンドにアプリケーションを機能として提供する ASP や SaaS と呼ばれる新たな ICT サービスの利用が進展してきている。企業等における ASP・SaaS の利用は、自前で開発するよりも短期間で情報システムの構築・運用が可能となるほか、当該情報システムの保守・運用・管理にかかる負担が軽減される等のメリットがある一方で、ASP・SaaS 事業者及びその関係組織に利用者である企業等の膨大な機密情報・顧客情報等の情報資産が集積されることとなるため、ASP・SaaS サービスが健全に発展していくためには、ASP・SaaS 事業者における適切な情報セキュリティ対策の実施が重要である。

本ガイドラインは、ASP・SaaS サービスの利用が企業等の生産性向上の健全な基盤となるよう、ASP・SaaS 事業者における情報セキュリティ対策の促進に資するため、ASP・SaaS 事業者が実施すべき情報セキュリティ対策を取りまとめたものである。

Ⅰ．２　ASP・SaaS とは

ASP（Application Service Provider）及び SaaS（Software as a Service）は、ともにネットワークを通じてアプリケーション・サービスを提供するものであり、基本的なビジネスモデルに大きな差はないものと考えられる。

したがって、本ガイドラインでは、ASP インダストリ・コンソーシアム・ジャパン[1]の発行した 2004 年版『ASP 白書』による ASP の定義「ネットワークを通じて、アプリケーション・ソフトウェア及びそれに付随するサービスを利用させること、あるいはそうしたサービスを提供するビジネスモデルを指す」を採用するとともに、ASP と SaaS を特に区別せず、「ASP・SaaS」と連ねて呼称することとする。また、ASP・SaaS といった形態で提供されるサービスを「ASP・SaaS サービス」と呼び、ASP・SaaS サービスを提供する主体を「ASP・SaaS 事業者」と呼ぶこととする[2]。

Ⅰ．３　ガイドラインの対象範囲

---

1 平成 11 年に任意団体として誕生。その後、平成 14 年 2 月に特定非営利活動法人（NPO）の認証を取得。ASP を活用した情報サービスにより、社会生活の改善及び企業の活性化の更なる促進を図ることを目的に、市場活性化支援等の活動を推進している。会員数は 140 社（平成 20 年 1 月末現在）。

2 本ガイドラインでは、一 ASP・SaaS 事業者が一 ASP・SaaS サービスを提供する場合を基本としているが、一 ASP・SaaS 事業者において複数の ASP・SaaS サービスを提供する場合、各 ASP・SaaS サービスを提供するそれぞれの担当部署等の主体が ASP・SaaS 事業者としての「主体」であるとみなすこととする。

本ガイドラインは、ASP・SaaS 事業者が ASP・SaaS サービスを提供する際に実施すべき情報セキュリティ対策を対象としている。また、利用者が ASP・SaaS 事業者との契約の範囲外で独自に利用するハードウェア及びソフトウェア（他の ASP・SaaS サービスを含む）、並びに利用者が契約する通信回線及びインターネット・サービスにおける情報セキュリティ対策は、本ガイドラインの対象外としている。

なお、本ガイドラインが、利用者が ASP・SaaS サービスを選定する際に、ASP・SaaS 事業者が実施している情報セキュリティ対策の状況を確認するための指標として活用されることも期待している。

Ⅰ．４　ガイドラインの位置付け

本ガイドラインは、ASP・SaaS 事業者が、提供するサービス内容に即した適切な情報セキュリティ対策を実施するための指針として、可能な限り分かりやすくかつ具体的な対策項目を提示することを目指して策定されている。また、ASP・SaaS 事業者は、本ガイドラインをそのまま利用することで、比較的簡単に自ら提供する ASP・SaaS サービスに即した情報セキュリティ対策が実施できるよう構成されている。しかしながら、利用者との契約において、より厳しい対策を設定し実施する等、各 ASP・SaaS 事業者の実情に合わせて活用することも可能である。なお、本ガイドラインは、ASP・SaaS 事業者が ASP・SaaS サービスを提供するにあたり実施すべき対策に絞り構成されているため、本ガイドラインに示されている対策を全て実施したことにより、企業におけるあらゆる情報セキュリティ脅威に対応できるものではない点に留意する必要がある。

また、本ガイドラインは JIS Q 27001（ISO/IEC 27001）に示される情報セキュリティマネジメントシステム[3]の考え方を参考としている。本ガイドラインを足がかりとして、ASP・SaaS 事業者における情報セキュリティマネジメントシステムの確立、導入、運用、監視、見直しが実施され、継続的に情報セキュリティ対策が改善されていくことを期待している。

Ⅰ．５　ガイドライン活用の効果

情報セキュリティマネジメントに関する既存の基準・規範（JIS Q 27001（ISO/IEC 27001）、JISQ27002（ISO/IEC 27002）等）は、ASP・SaaS サービス等の個別のサービスの内容や形態を念頭に置いて作成されたものではないため、ASP・SaaS 事業者がこれらの基準・規範をそのまま利活用する場合、ASP・SaaS 事業者の実態に即した情報セキュリ

[3] 例えば、「電気通信事業における情報セキュリティマネジメント指針 pp.8-11」、「情報セキュリティマネジメントシステム適合性評価制度の概要 pp3-4」を参照されたい。

ティマネジメントが導入・運用しにくいといった問題がある。

そこで、本ガイドラインは、ASP・SaaS サービスの特性に基づいたリスクアセスメントを実施し、ASP・SaaS 事業者が実施すべき情報セキュリティ対策を取りまとめることにより、どの ASP・SaaS 事業者にも実践的で取り組みやすい対策集となっている。本ガイドラインを活用することで、以下の効果が見込まれる。

- 大企業と比較して、情報セキュリティ対策に人的・金銭的な資源を割くことが困難な中小の ASP・SaaS 事業者に対して、独自の脅威分析の負担を軽減し、優先的に取り組むべき対策の指針を与える。
- 他の ASP・SaaS サービスと連携[4]する際、連携 ASP・SaaS 事業者に対する情報セキュリティ対策の要求事項として、本ガイドラインが一定の指針となる。
- これまで、ASP・SaaS の情報セキュリティ対策に関する明確な指針が存在しなかったため、利用者が ASP・SaaS サービスを選択するにあたり、その ASP・SaaS 事業者が実施している情報セキュリティ対策の妥当性を判断し得なかった。本ガイドラインは、利用者が ASP・SaaS サービスを選択する際の、一定の指針となる。

Ⅰ．６　ガイドラインの全体構成

本ガイドラインは、「序編」「組織・運用編」「物理的・技術的対策編」の 3 編から構成される。

Ⅰ．６．１　序編

本ガイドラインの目的、対象とする範囲、利用方法、注意事項、用語の定義等を取りまとめた、「組織・運用編」「物理的・技術的対策編」をより良く活用するための導入編。

Ⅰ．６．２　組織・運用編

情報セキュリティを確保するために求められる運用管理体制、外部組織との契約における留意事項、利用者に対する責任等の、組織・運用に係る対策を取りまとめた対策集。主に、経営者等の組織管理者によって参照されることを想定している。

Ⅰ．６．３　物理的・技術的対策編

ASP・SaaS の典型的なシステム構成を基に、各構成要素[5]における情報資産[6]に対する情

---

4 他の ASP・SaaS サービスを自らの ASP・SaaS サービスに組み込むことにより、異なるアプリケーション間の連携が可能となる。

5 「Ⅰ．９ 用語の定義」参照。

6 「Ⅰ．９ 用語の定義」参照。「構成要素における情報資産」とは、サーバ等の構成要素及びサーバ上のデータ、ログ等の情報そのものを指すこととなる。

報セキュリティ対策を取りまとめた対策集。構成要素は「アプリケーション、プラットフォーム、サーバ・ストレージ」「ネットワーク」「建物、電源（空調等）」の 3 つに大きく分類し、どの構成要素にも属さない情報資産を「その他」としている。また、次項「Ⅰ．7」に示す 6 つのパターンで、具体的な対策をパッケージ化している。主に、実際に ASP・SaaS サービスを運用している現場の技術者等によって参照されることを想定している。

Ⅰ．7　ASP・SaaS サービス種別のパターン化

ASP・SaaS 事業者が提供するサービスは、基幹系業務システムからグループウェアに至るまで多岐に渡っており、その取り扱う情報の違いから、各 ASP・SaaS サービスに要求される「機密性」「完全性」「可用性」のレベルも必然的に異なってくる。

そこで、本ガイドラインでは、ASP・SaaS のサービス種別を「機密性」「完全性」「可用性」の観点から、その特性ごとに 6 パターンに分類している。また、この分類を基に「物理的・技術的対策編」の対策項目をパターン化している。

Ⅰ．7．1　パターン化の考え方

「機密性」「完全性」「可用性」に基づく、パターン分類の考え方は以下のとおりである（簡略化し整理したものを図表 1 に示す）。

【パターン 1】
機密性・完全性・可用性の全てへの要求が「高」いサービス
【パターン 2】
機密性・完全性への要求は「高」いが、可用性への要求は「中」程度のサービス
【パターン 3】
機密性・完全性への要求は「高」いが、可用性への要求は「低」[7]いサービス
【パターン 4】
機密性への要求は「低」いが、完全性・可用性への要求が「高」いサービス
【パターン 5】
機密性への要求は「低」いが、完全性への要求は「高」く、可用性への要求は「中」程度のサービス
【パターン 6】
完全性への要求は「高」いが、機密性・可用性への要求は「低」いサービス

[7] 本ガイドラインでは、一定の条件に合致するかどうかを示す相対的な見出しとして「低」という表現を用いているが、これは情報セキュリティ要求レベルが絶対的に低いことを示すものではない。

パターン	機密性への要求	完全性への要求	可用性への要求
1	高	高	高
2	高	高	中
3	高	高	低
4	低	高	高
5	低	高	中
6	低	高	低

図表１　各パターンの位置付け

ここでの「機密性」「完全性」「可用性」への要求の高低に関する考え方は次のとおりである。

【機密性への要求】

以下の情報を扱う場合には、その件数に関わりなく、機密性への要求は「高」いものとする。

⑴個人情報

利用者及び利用者の顧客に関する、特定の個人を識別することができる情報。

⑵営業秘密情報

秘密として管理されている生産方法、販売方法、その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないもの。

【完全性への要求】

ASP・SaaS 事業者が利用者のデータを管理するという特性上、そのデータに改ざん・削除等のインシデントが発生した場合、顧客の事業継続に多大な影響を与えるものと考えられる。また、ASP・SaaS 事業者が提供する情報においても、その情報に改ざん等のインシデントが発生した場合、その情報に依存している顧客にとって大きな損害が発生することが想定される。したがって、ASP・SaaS 事業者においては、そのサービス種別に関わらず、完全性への要求は「高」いものと考えられる。

【可用性への要求】

⑴可用性への要求が「高」いサービス

a 運用時間中は原則として必ず稼働させておくことが求められるサービス

b サービスが停止することで、利用者に多大な経済的損失や人命危害が生じる恐れのあるサービス

⑵可用性への要求が「中」程度のサービス

a サービスが停止することで、利用者に部分的な経済的損失が生じる恐れのあるサービス

b サービスが停止することで、利用者の基幹業務に明確な影響を及ぼすサービス

(3)可用性への要求が「低」いサービス

(1)(2)以外のサービス

Ⅰ．７．２　典型的サービスのパターン分類

上記「Ⅰ．７．１」に基づき、典型的な ASP・SaaS サービスについて、その特性を考慮してパターンごとに分類した結果が、図表 2 である。本ガイドラインに基づいて「物理的・技術的対策編」の対策を実施する場合は、提供するサービスがどのパターンに分類されているかによって、具体的な対策が異なってくるので、注意が必要である。

パターン	サービス種別
1	受発注、人事給与・勤怠管理・経理、ERP（財務会計等）、EC サポート（電子商取引のアウトソーシング）、ネットショッピング支援（仮想店舗貸しサービス）、コールセンター支援、金融業特化型サービス（地銀・信金共同アウトソーシング）、医療・介護・福祉業特化型サービス、電子入札、公共住民情報、決済サービス、不正アクセス監視
2	販売管理・売掛金管理、公共窓口業務、在庫管理、建設業特化型サービス、卸売・小売・飲食業特化型サービス、保険業特化型サービス（生命保険見積）、宿泊業特化型サービス、公共電子申請、公共個別部門業務、グループウェア、アドレス帳サービス、位置時間証明サービス
3	購買支援、CRM（顧客管理）・営業支援、販売支援、契約、採用管理、資産管理、ネットショッピング（自らの売買支援）、金融業特化型サービス（信用情報提供）、保険業特化型サービス（自賠責保険見積）、アフィリエイト、メール配信
4	ネットワーク監視
5	EC サポート（産地直送等、物流・決済を一括で提供）
6	広告、IT 資産管理、ニュースリリース業務、運輸業特化型サービス、電話会議・TV 会議・Web 会議、乗り換え、不動産物件検索、検索サービス（一般向け）
※	e ラーニング・LMS、文書管理、オンラインストレージ、ワークフロー、Web サイトのホスティング、ブログ・コミュニティコーディネート、コンテンツデリバリー・ストリーミングサービス、GIS（地図情報システム）/GIS 応用、映像監視、メディア・言語変換サービス、検索サービス（個別用途）、認証サービス、セキュリティサービス

※一律にパターンを設定することが困難なサービス

図表 2　パターンごとのサービス種別

なお、上記の図表は全ての ASP・SaaS サービスの特性を網羅しているものではない。したがって、自らが提供する ASP・SaaS サービスが、図表 2 で分類されているパターンにそぐわない場合、図表中に存在しない場合、「一律にパターンを設定することが困難なサービス」に該当する場合等は、上記Ⅰ．７．１に示した考え方に基づき、該当するパターンを独自に判定することを推奨する。

Ⅰ．８　ガイドラインの利用方法

本ガイドラインは、上記「Ⅰ．７」に示すASP・SaaS事業者が提供するサービス種別に即して分類したパターンごとに、適切な情報セキュリティ対策が実施できるようにすることを基本としている。下記「Ⅰ．８．１」から「Ⅰ．８．５」に示す「組織・運用編」「物理的・技術的対策編」の各項目の意味をよく理解し、また、「Ⅰ．８．６」に示す「利用手順」に従って、自らが行うべき情報セキュリティ対策を判定し、実施されたい。

Ⅰ．８．１　対策項目

ASP・SaaS事業者が実施すべき情報セキュリティ対策事項。認証基準等で用いられるような実施必須事項を示すものではなく、情報セキュリティ対策を実施する上での指標となることを期待している。

Ⅰ．８．２　基本・推奨

対策を「基本」と「推奨」に分類することで、対策実施の優先度を示している。

・基本：ASP・SaaSサービスを提供するにあたり、優先的に実施すべき情報セキュリティ対策
・推奨：ASP・SaaSサービスを提供するにあたり、実施することが望まれる情報セキュリティ対策

Ⅰ．８．３　ベストプラクティス

対策を実施するにあたっての、具体的な実施手法や注意すべき点をまとめた参考事例。

Ⅰ．８．４　評価項目

対策項目を実施する際に、その実施レベルを定量的あるいは具体的に評価するための指標。SLA[8]の合意事項として活用されることも想定される。

Ⅰ．８．５　対策参照値

対策項目の実施レベルの目安となる評価項目の値で、パターンごとに設定されている。特に達成することが必要であると考えられる値については「*」を付している。また、評価項目によっては、対策参照値が「-」となっているパターンが存在するが、これについては、ASP・SaaS事業者が任意に対策参照値を設定することで、対策項目の実施レベルを評価されたい。

---

8 Service Level Agreement。ASP・SaaS事業者が利用者と締結するサービス品質保証契約。

Ⅰ．８．６　利用手順

本ガイドラインを基に具体的な情報セキュリティ対策を実施する場合は、以下の手順に従って利用されたい。その際、利用手順を示す図表 3 を併せて参照すると良い。

また、本ガイドラインには参考資料として Annex 1「ASP・SaaS サービスの典型的な構成要素と情報資産」、Annex 2「組織・運用編　対策項目一覧表」、Annex 3「物理的・技術的対策編　対策項目一覧表」を付属している。Annex 1 は、ASP・SaaS サービスの典型的な構成要素を図式化し、対策の対象となる情報資産を例示したものである。Annex 2・3 は、『Ⅱ.組織・運用編』及び『Ⅲ.物理的・技術的対策編』それぞれの対策を一覧表にしたものであり、対策を実施する際の実施計画や実績管理等に使用できるようになっている。これらの資料についても、適宜参照されたい。

・経営者等の組織管理者

i.　『Ⅰ.序編』を読み、本ガイドラインの位置付け、利用方法、用語の定義等を確認する。

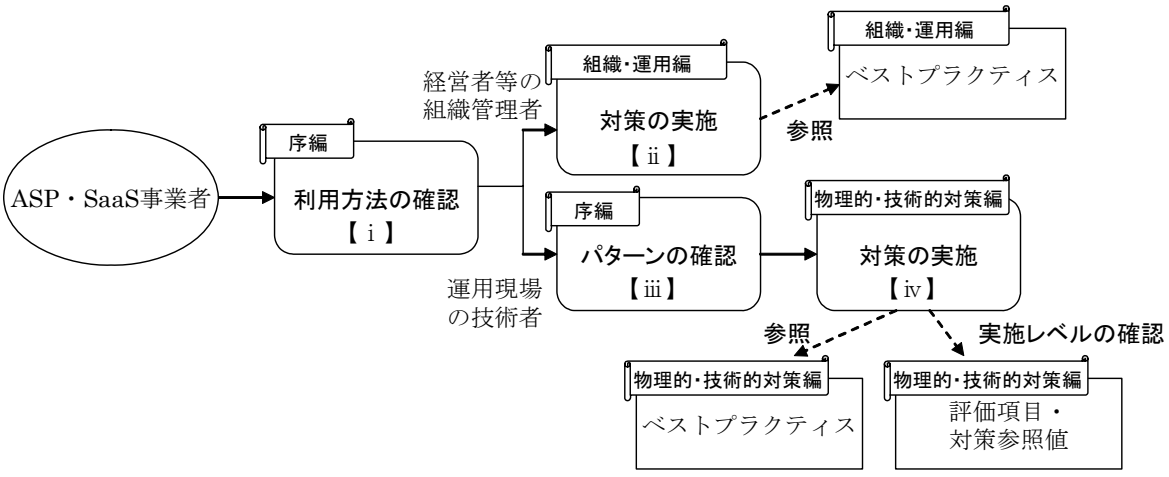
ii.　『Ⅱ.組織・運用編』の対策を実施する。対策を実施する際には、ベストプラクティスを参照すると良い。

・運用現場における技術者等

i.　『Ⅰ.序編』を読み、本ガイドラインの位置付け、利用方法、用語の定義等を確認する。

iii.　『Ⅰ.序編』「Ⅰ・７」に基づき、自らが提供する ASP・SaaS サービスがどのパターンに該当するかを確認する。

iv.　『Ⅲ.物理的・技術的対策編』を見て、自分のパターンに該当する対策を実施する。「基本」の対策から優先的に実施し、さらに「推奨」の対策を実施することが望ましい。対策を実施する際には、ベストプラクティスを参照すると良い。また、評価項目を使用し、対策参照値を目安に対策の実施レベルを判断することができる。



図表 3　利用手順

Ⅰ．９　用語の定義

Ⅰ．９．１　JIS Q 27001 の定義を踏襲している用語

i.　機密性

認可されていない個人、エンティティ又はプロセスに対して、情報を使用不可又は非公開にする特性。

ii.　完全性

資産の正確さ及び完全さを保護する特性。

iii.　可用性

認可されたエンティティが要求したときに、アクセス及び使用が可能である特性。

iv.　情報セキュリティ

情報の機密性、完全性及び可用性を維持すること。さらに、真正性、責任追跡性、否認防止及び信頼性のような特性を維持することを含めてもよい。

v.　情報セキュリティ事象

システム、サービス又はネットワークにおける特定の状態の発生。特定の状態とは、情報セキュリティ基本方針への違反若しくは管理策の不具合の可能性、又はセキュリティに関連するかもしれない未知の状況を示していることをいう。

vi.　情報セキュリティインシデント

望ましくない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。

vii.　リスク

事象の発生確率と事象の結果との組合せ。

viii.　リスク分析

リスク因子を特定するための、及びリスクを算定するための情報の系統的使用。

ix.　リスクアセスメント

リスク分析からリスク評価までのすべてのプロセス。

Ⅰ．９．２　本ガイドライン独自に定義する用語

i.　構成要素

ASP・SaaS サービスの提供に用いるハードウェア、ソフトウェア、通信機器・回線、建物等の固定資産。

ii.　情報資産

構成要素及び構成要素を介する情報。

iii.　情報セキュリティポリシー

情報セキュリティに関する組織的取組についての基本的な方針及び情報セキュ

リティ対策における具体的な実施基準や手順等の総称。

iv. 利用者

ASP・SaaS サービスを利用する法人又は個人。

v. 従業員

ASP・SaaS 事業者に所属し、当該 ASP・SaaS 事業者の提供する ASP・SaaS サービスの提供に携わる者で経営陣を除く者。派遣社員、アルバイト等を含む。

vi. 管理責任者

ASP・SaaS サービスの提供に使用する設備の運用管理を担当する現場責任者。

vii. 連携 ASP・SaaS 事業者

自らの ASP･SaaS サービスに他の ASP･SaaS サービスを組み込むことにより、アプリケーション間の統合・連携を実施する際に、他の ASP・SaaS サービスを提供する ASP・SaaS 事業者。

viii. 外部組織

連携 ASP・SaaS 事業者や ASP・SaaS 事業者からサービスの一部を委託された企業等、ASP・SaaS サービスの提供にあたり契約関係のある組織の総称。

ix. 業務プロセス

ASP・SaaS サービスを提供するために行われる一連の活動。

x. ユーザサポート

ASP・SaaS サービスに関する問い合わせ窓口（ヘルプデスク）と ASP・SaaS サービスの品質や継続性を維持するための組織の総称。

xi. 情報処理施設

ASP・SaaS 事業者がサービスを提供するための設備が設置された建物。

xii. 物理的セキュリティ境界

情報処理施設の特定の領域を保護するために設置される壁、カード制御による出入口等の物理的な仕切り。

xiii. サーバ・ストレージ

ASP・SaaS サービスを提供する際に利用するアプリケーション等を搭載する機器及びアプリケーション上の情報を蓄積・保存するための装置の総称。なお、付随する OS 等の基盤ソフトウェア、蓄積されているデータ・ログ等の情報を含む。

xiv. プラットフォーム

認証、決済等の付加的機能を提供する、ASP・SaaS サービスで提供されるアプリケーションの基盤。

xv. 通信機器

ルータ、スイッチ等、通信を制御するための装置。

xvi. 情報セキュリティ対策機器

ファイアウォール、IDS 等、コンピュータウイルスや不正アクセス等の情報セキ

ュリティ事象から、ASP・SaaS 事業者の設備を防護するための機器。

xvii. 外部ネットワーク

情報処理施設とその外部とを結ぶネットワークの総称で、ASP・SaaS 事業者と ISP 間、ASP・SaaS 事業者と連携 ASP・SaaS 事業者間、ASP・SaaS 事業者の保守管理用回線等を指す。本ガイドラインの対象外である、利用者が契約する通信回線及びインターネット・サービスは除く。

Ⅰ．１０　参考文書

- JIS Q 27001:2006 (ISO/IEC 27001:2005)
- JIS Q 27002:2006 (ISO/IEC 17799:2005)
- JIS Q 13335-1:2006（MICTS-1）
- MICTS-2[9]
- 総務省「公共 IT におけるアウトソーシングに関するガイドライン」
- 財団法人 金融情報システムセンター「金融機関等コンピュータシステムの安全対策基準・解説書 第 7 版」

[9] ISO/IEC 27005 として規格化される予定。

Ⅱ　組織・運用編

【凡例】

対策項目

ASP・SaaS 事業者が実施すべき情報セキュリティ対策事項。認証基準等で用いられるような実施必須事項を示すものではなく、情報セキュリティ対策を実施する上での指標となることを期待している。

基本・推奨

対策を「基本」と「推奨」に分類することで、対策実施の優先度を示している。

・基本：ASP・SaaS サービスを提供するにあたり、優先的に実施すべき情報セキュリティ対策

・推奨：ASP・SaaS サービスを提供するにあたり、実施することが望まれる情報セキュリティ対策

ベストプラクティス

対策を実施するにあたっての、具体的な実施手法や注意すべき点をまとめた参考事例。

Ⅱ．１　情報セキュリティへの組織的取組の基本方針

Ⅱ．１．１　組織の基本的な方針を定めた文書

Ⅱ．１．１．１　**【基本】**

経営陣は、情報セキュリティに関する組織的取組についての基本的な方針を定めた文書を作成すること。また、当該文書には、経営陣が承認の署名等を行い、情報セキュリティに関する経営陣の責任を明確にすること。

【ベストプラクティス】

i.　情報セキュリティに関する組織的取組とは、経営陣主導で組織全体が自ら定めた指針、ルール、具体的手続・手順等に従って、情報セキュリティ向上の実現に取組むことを言う。

ii.　作成した情報セキュリティに関する組織的取組についての基本的な方針（以下、「情報セキュリティに関する基本的な方針」と言う。）を定めた文書について、全ての従業員及び利用者並びに外部組織に対して公表し、通知することが望ましい。その際、事業所内の多くの場所に見やすく掲示する等、利用、理解しやすい形で、適切に知らせることが望ましい。

iii. 情報セキュリティに関する基本方針を定めた文書には，次の事項に関する記述を含めることが望ましい。

a）情報セキュリティの定義、目的及び適用範囲

b）事業戦略や事業目的に照らし合わせて、経営陣が情報セキュリティの重要性をどう考えているのか

c）経営陣が情報セキュリティへの組織的取組の目標と原則を支持していること

d）体制の構築と情報資産保護への取組の宣言

e）組織における遵守事項の宣言

1）法令、規制等の遵守

2）教育・訓練の実施

3）事件・事故の予防と対応への取組

4）管理責任者や従業員の義務

f）見直し及び改善への取組の宣言　等

Ⅱ．１．１．２　**【基本】**

情報セキュリティに関する基本的な方針を定めた文書は、定期的又はASP・SaaSサービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。この見直しの結果、変更の必要性が生じた場合には、経営陣の承認の下で改定等を実施すること。

Ⅱ．２　情報セキュリティのための組織

Ⅱ．２．１　内部組織

Ⅱ．２．１．１　【基本】

経営陣は、情報セキュリティに関する取組についての責任と関与を明示し、人員・資産・予算の面での積極的な支援・支持を行うこと。

【ベストプラクティス】

i. 情報セキュリティに関する取組にあたっては、必要となる調整（各種判断や連絡・指示、協力等）が適切に行われるよう、関連する役割及び職務機能を持つ代表者（CIO[10]、CISO[11]等）を定めることが望ましい。

ii. 組織の規模によっては、取締役会などが CIO、CISO 等の役割を担ってもよい。

iii. 経営陣は、情報セキュリティに関する専門的な助言が必要と判断した場合には、CISO や内部の情報セキュリティ専門技術者から助言を受け、その結果をレビューした上で組織内で調整することが望ましい。

Ⅱ．２．１．２　【基本】

従業員に対する秘密保持又は守秘義務についての要求を明確にし、文書化すること。当該文書は、定期的又は ASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。

Ⅱ．２．１．３　【基本】

情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又は ASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。

---

10 Chief Information Officer（最高情報責任者）

11 Chief Information Security Officer（最高情報セキュリティ責任者）

Ⅱ．２．２　外部組織（データセンタを含む）

Ⅱ．２．２．１　【基本】

外部組織が関わる業務プロセスにおける、情報資産に対するリスクを識別し、適切な対策を実施すること。

【ベストプラクティス】

i. 情報資産に対するリスクとしては、不正アクセス、情報資産の盗難・不正変更、情報処理設備の悪用・破壊等がある。

ii. これらのリスクを軽減するために、外部組織（特に、データセンタ、電気通信事業者、情報セキュリティサービス提供事業者等）による情報資産へのアクセスを、各ASP・SaaS 事業者の実環境に合わせて管理・制限することが望ましい。以下に、情報資産にアクセス可能な外部組織を例示する。

a) 情報処理施設に定期・不定期に出入りする外部組織（配送業者、設備点検等）

b) 情報処理施設に常駐する外部組織（SE、警備会社等）

c) ネットワークを通じサービスを提供する外部組織（連携 ASP・SaaS 事業者、ネットワーク監視サービス等）

iii. 情報資産へアクセスする手段を区別し、それぞれに対してアクセスを管理・制限する方針と方法を定めることが望ましい。

Ⅱ．２．２．２　【基本】

情報資産へのアクセスが可能となる外部組織との契約においては、想定される全てのアクセスについて、その範囲を規定すること。

【ベストプラクティス】

i. 外部組織によるアクセス手法としては、以下のようなものが想定される。

a）物理的セキュリティ境界からの入退室

b）情報システムの管理用端末の利用

c）外部ネットワークからの接続

d）データを格納した媒体の交換

ii. ASP・SaaS サービスの提供にあたっては、連携 ASP・SaaS 事業者等外部組織が多岐に渡ることが多いため、契約の締結を慎重に行うことが望ましい。

Ⅱ．３　連携 ASP・SaaS 事業者に関する管理

Ⅱ．３．１　連携 ASP・SaaS 事業者から組み込む ASP・SaaS サービスの管理

Ⅱ．３．１．１　【基本】

連携 ASP・SaaS 事業者が提供する ASP・SaaS サービスについて、事業者間で合意された情報セキュリティ対策及びサービスレベルが、連携 ASP・SaaS 事業者によって確実に実施されることを担保すること。

【ベストプラクティス】

i. 連携 ASP・SaaS 事業者から ASP・SaaS サービスの提供を受ける場合には、情報セキュリティに係る取決めを連携 ASP・SaaS 事業者が確実に実施するように、契約や SLA を締結することが望ましい。

ii. 連携 ASP・SaaS 事業者の提供するサービス内容が、同意なしに変更されたり、サービスレベルが要求を満たさないことが無いように、契約や SLA を締結することが望ましい。

Ⅱ．３．１．２　【基本】

連携 ASP・SaaS 事業者が提供する ASP・SaaS サービスの運用に関する報告及び記録を常に確認し、レビューすること。また、定期的に監査を実施すること。

【ベストプラクティス】

i. 連携 ASP・SaaS 事業者が提供する ASP・SaaS サービスの確認及びレビューの実施例としては、連携 ASP・SaaS 事業者との契約等において、SLA 項目の計測方法及び計測結果を定期報告するように義務付けると共に、定期的に実施結果を確認するという方法が考えられる。

ii. 連携 ASP・SaaS 事業者に起因する情報セキュリティインシデント及び問題点について、自らのログ記録により監査できるようにすることが望ましい。

Ⅱ．４　情報資産の管理

Ⅱ．４．１　情報資産に対する責任

Ⅱ．４．１．１　**【基本】**

取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。

【ベストプラクティス】

i. 情報資産の目録を作成し、情報セキュリティインシデントから復旧するために必要な全ての情報を記載することが望ましい。
   例：　種類、形式、所在、バックアップ情報、ライセンス情報、業務上の価値　等
ii. 情報資産の目録における記載内容は、他の目録における記載内容と整合がとれていることが望ましい。また、不必要に重複しないことが望ましい。
iii. 情報資産の分類方法と各情報資産の管理責任者を定め、組織内での合意の下に文書化することが望ましい。
iv. 情報資産の重要度を業務上の価値に基づいて定め、組織内での合意の下に文書化することが望ましい。
v. 情報資産の保護のレベル（例：機密性・完全性・可用性に対する要求レベル）を各情報資産が直面するリスクの大きさに基づいて定め､組織内での合意の下に文書化することが望ましい。
vi. 全ての従業員及び外部組織に対して、情報資産の利用の許容範囲に関する規則に従うよう、義務付けることが望ましい。

Ⅱ．４．２　情報の分類

Ⅱ．４．２．１　【基本】

組織における情報資産の価値や、法的要求（個人情報の保護等）等に基づき、取扱いの慎重さの度合いや重要性の観点から情報資産を分類すること。

【ベストプラクティス】

i. 情報資産の分類結果は、ラベル付け等により、従業員に対して明示することが望ましい。

ii. 情報資産の分類及び保護管理策の選定においては、情報資産の共有又は利用制限に係る業務上の必要性とこれにより生じる影響を考慮することが望ましい。

iii. 情報資産の分類は複雑すぎないことが望ましい（管理コストの増加をきたすため)。

iv. 外部組織からの文書に付いている分類ラベルは、定義が異なることがあるので、名称が同じか又は類似していたとしても、その解釈には注意する必要がある。

v. 情報資産の各分類レベルごとに、安全な取扱い手順（処理・保存・伝達・秘密解除・破棄等）を定めることが望ましい。

vi. 取扱いに慎重を要する又は重要と分類される情報を含むシステム出力には、適切な分類ラベルを付与することが望ましい。システム出力の例としては､印刷された文書、スクリーン表示、記録媒体（例えば、テープ、ディスク、CD)、電子的なメッセージ及び転送ファイル等がある。

Ⅱ．４．３　情報セキュリティポリシーの遵守、点検及び監査

Ⅱ．４．３．１　【基本】

各情報資産の管理責任者は、自らの責任範囲における全ての情報セキュリティ対策が、情報セキュリティポリシーに則り正しく確実に実施されるよう、定期的にレビュー及び見直しを行うこと。

【ベストプラクティス】

i. 管理責任者は、レビュー及び見直しの方法を予め定めておくことが望ましい。

ii. 管理責任者が実施したレビュー及び見直しの結果を記録し、その記録を保管管理することが望ましい。

Ⅱ．４．３．２　【基本】

ASP・SaaS サービスの提供に用いる情報システムが、情報セキュリティポリシー上の要求を遵守していることを確認するため、定期的に点検・監査すること。

【ベストプラクティス】

i. 点検・監査は、十分な技術的能力及び経験を持つ者（例：情報セキュリティアドミニストレータ資格を持ち､情報セキュリティに係る技術的対策の実務を一定年数以上経験している者）の監督の下で行うことが望ましい。

ii. 情報システムの点検・監査にあたっては、ASP・SaaS サービスの提供中断によるリスクを最小限に抑えるよう、考慮することが望ましい。

Ⅱ．５　従業員に係る情報セキュリティ

Ⅱ．５．１　雇用前

Ⅱ．５．１．１　**【基本】**

雇用予定の従業員に対して、機密性・完全性・可用性に係る情報セキュリティ上の要求及び責任の分界点を提示・説明するとともに、この要求等に対する明確な同意をもって雇用契約を締結すること。

【ベストプラクティス】

i.　雇用条件には、情報セキュリティに関する基本的な方針を反映させることが望ましい。

ii.　雇用条件では、次の事項を明確に記述することが望ましい。

a)　取扱注意情報へのアクセス権を与えられる全ての従業員に対して、アクセスが認められる前に、秘密保持契約書又は守秘義務契約書に署名を求める

b)　従業員の法的な責任と権利

c)　従業員が担うべき情報資産に対する責任

d)　雇用契約を締結する過程で取得した個人情報の扱いに関する組織の責任

iii. 雇用終了後も、一定期間は雇用期間における責任が継続するよう、雇用条件を規定することが望ましい。

Ⅱ．５．２　雇用期間中

Ⅱ．５．２．１　【基本】

全ての従業員に対して、情報セキュリティポリシーに関する意識向上のための適切な教育・訓練を実施すること。

Ⅱ．５．２．２　【基本】

従業員が、情報セキュリティポリシーもしくはASP・SaaSサービス提供上の契約に違反した場合の対応手続を備えること。

【ベストプラクティス】

i. 雇用条件において、従業員が情報セキュリティポリシー等に従わない場合の対応手続等を明確にすることが望ましい。

Ⅱ．５．３　雇用の終了又は変更

Ⅱ．５．３．１　【基本】

従業員の雇用が終了又は変更となった場合のアクセス権や情報資産等の扱いについて、実施すべき事項や手続き、確認項目等を明確にすること。

【ベストプラクティス】

i. 雇用終了時には、支給したソフトウェア、電子ファイル等の電子媒体、会社の書類、手引書等の紙媒体、モバイルコンピューティング装置、アクセスカード等の設備等、全ての返却を求めることが望ましい。

ii. 雇用終了後には、情報資産に対する個人のアクセス権を速やかに削除することが望ましい。

iii. 雇用の変更を行う場合には、新規の業務に対して承認されていない全てのアクセス権を削除することが望ましい。

iv. アクセス権の削除に当たっては、情報システムへの物理的なアクセスキー（情報処理施設の鍵、身分証明書等）及び電子的なアクセスキー（パスワード等）等を返却・消去することが望ましい。

v. 雇用終了後には、組織の現行の一員であることを認定する書類から削除することが望ましい。

vi. 雇用が終了又は変更となる従業員が、稼働中の情報システム等の情報資産にアクセスするために必要なアクセスキーを知っている場合には、雇用の終了又は変更時に当該情報資産へのアクセスキーを変更することが望ましい。