資料５－３

ASP・SaaS における
情報セキュリティ対策ガイドライン
（最終案）

ASP・SaaS の情報セキュリティ対策に関する研究会

平成　　年　月　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。

削除：32

削除：19

削除：0

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）。

削除：表

【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

削除：表

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。

(1)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。

(2)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】

(1)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

(2)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。

削除：表

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

削除：ASP

削除：ASP

削除：（電子カルテ、レセプト）

削除：ASP

削除：ASP

削除：ASP

削除：ASP

削除：医療・介護・福祉特化型 ASP（診療予約、介護業務支援）、

削除：ASP

削除：ASP

削除：ASP

削除：医療・介護・福祉業特化型 ASP（処方箋サービス）、

削除：表

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。

削除：表

削除：表

削除：表

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。

削除：表３

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。

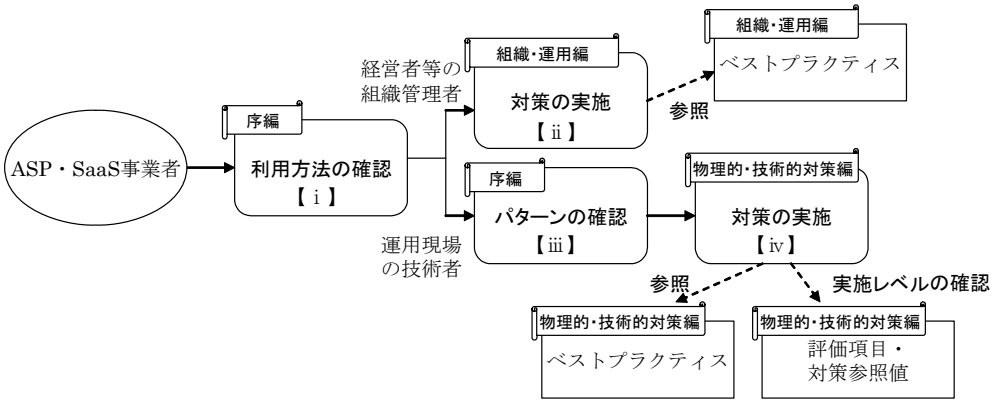
ii.　『Ⅱ.組織・運用編』の対策を実施する。対策を実施する際には、ベストプラクティスを参照すると良い。

・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

削除：表

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[10]
- 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」

削除：ISO/IEC 27005 [9]（

削除：）

[10] 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[11]、CISO[12]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。

11 Chief Information Officer（最高情報責任者）

12 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。

削除：<#>ASP・SaaS サービスの提供にあたり、海外にデータセンタがある場合等、海外法が適用される場合があるので注意する必要がある。

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。

Ⅱ．６　情報セキュリティインシデントの管理

Ⅱ．６．１　情報セキュリティインシデント及びぜい弱性の報告

Ⅱ．６．１．１　**【基本】**

全ての従業員に対し、業務において発見あるいは疑いをもった情報システムのぜい弱性や情報セキュリティインシデント（サービス停止、情報の漏えい・改ざん・破壊・紛失、ウイルス感染等）について、どのようなものでも記録し、できるだけ速やかに管理責任者に報告できるよう手続きを定め、実施を要求すること。

報告を受けた後に、迅速に整然と効果的な対応ができるよう、責任体制及び手順を確立すること。

【ベストプラクティス】

i. 情報セキュリティインシデントの正式な報告手順を、報告を受けた後のインシデント対応及び段階的取扱い（例：原因切り分け、部分復旧、完全復旧のフェーズに分けた取扱い）の手順と共に確立することが望ましい。また、情報セキュリティインシデントの報告手順は全ての従業員に周知徹底することが望ましい。

ii. 情報セキュリティインシデント報告のための連絡先を明確にすることが望ましい。さらに、この連絡先を全ての従業員が認識し、いつでも利用できるようにすることで、適切で時機を逸しない対応を確実に実施できることが望ましい。

iii. 全ての従業員に対し、情報システムのぜい弱性や情報セキュリティインシデントの予兆等の情報資産に対する危険を発見した場合には、いかなる場合であってもできる限り速やかに管理責任者に報告する義務があることを認識させておくことが望ましい。

iv. 収集した情報セキュリティインシデント情報を分析し、必要に応じて対策の見直しに資することが望ましい。

Ⅱ．７　コンプライアンス

Ⅱ．７．１　法令と規則の遵守

Ⅱ．７．１．１　【基本】

個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。

【ベストプラクティス】

i. 関連する法規としては、個人情報保護法、不正競争防止法、著作権法、e-文書法、電子帳簿保存法等が考えられる。

ii. 上記の法令を遵守するにあたり、下記に示すようなガイドライン等を参照することが望ましい。

a) 個人情報保護法関係のガイドライン
22 分野に 35 のガイドラインがある。
（参考）内閣府国民生活局「個人情報の保護に関するガイドラインについて」

b) 不正競争防止法関係のガイドライン
日本弁理士会「不正競争防止法ガイドライン」　等

c) 著作権法関係のガイドライン
文化庁「平成 19 年度著作権テキスト」、社団法人テレコムサービス協会「著作権関係ガイドライン」　等

d) e-文書法関係のガイドライン
経済産業省『文書の電磁的保存等に関する検討委員会』の報告書、タイムビジネス推進協議会「e-文書法におけるタイムスタンプ適用ガイドライン　Ver1.1」　等

e) 電子帳簿保存法関係のガイドライン
国税庁　「電子帳簿保存法取扱通達」　等

iii. ASP・SaaS サービスの提供にあたり、海外にデータセンタがある場合等、海外法が適用される場合があるので注意する必要がある。

Ⅱ．７．１．２　【基本】

ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。

【ベストプラクティス】

i. 記録類は、記録の種類（例：会計記録、データベース記録、ログ記録、運用手順等）によって大分類し、さらにそれぞれの種類において保存期間と記録媒体の種別（例：紙、光媒体、磁気媒体等）によって細分類することが望ましい。

ii. 記録の保存は媒体の製造業者の推奨仕様に従って行うことが望ましい。

iii. 媒体が劣化する可能性を考慮し、長期保存のためには紙又はマイクロフィルムを利用することが望ましい。

iv. 国又は地域の法令又は規制によって保存期間が定められている記録を確実に特定することが望ましい。

Ⅱ．７．１．３　**【基本】**

利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと。

【ベストプラクティス】

i. 情報システム又は情報処理施設を利用しようとする者に対して、利用しようとしている情報システム又は情報処理施設が ASP・SaaS 事業者の所有であること、認可されていない目的のためアクセスは許可されないこと等について、警告文を画面表示する等によって警告することが望ましい。

ii. 利用を継続するためには、警告に同意を求めることが望ましい。但し、利用者については、サービスの利便性を考慮し、ASP・SaaS サービスの利用開始時にのみ同意を求めることで対応することも可能である。

Ⅱ．８　ユーザサポートの責任

Ⅱ．８．１　利用者への責任

Ⅱ．８．１．１　**【基本】**

ASP・SaaS サービスの提供に支障が生じた場合には、その原因が連携 ASP・SaaS 事業者に起因するものであったとしても、利用者と直接契約を結ぶ ASP・SaaS 事業者が、その責任において一元的にユーザサポートを実施すること。

【ベストプラクティス】

i. 連携 ASP・SaaS 事業者が提供している ASP・SaaS サービス部分に係るユーザサポートについては、利用者便益を最優先した方法によって実施することが望ましい。このため、ASP・SaaS 事業者は、連携 ASP・SaaS 事業者との間で利用者からの故障対応要求や業務問合せ、作業依頼等に対する取扱手続を定め、合意を得た手段で実施することが望ましい。

例：ASP・SaaS 事業者が、連携 ASP・SaaS 事業者のサービス部分に係る問合せについても一括して受け付ける等

Ⅲ.　物理的・技術的対策編

【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。

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 の合意事項として活用されることも想定される。

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。

Ⅲ．１　アプリケーション、プラットフォーム、サーバ・ストレージ、ネットワークに共通する情報セキュリティ対策

Ⅲ．１．１　運用管理に関する共通対策

Ⅲ．１．１．１　【基本】

ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の稼働監視（応答確認等）を行うこと。
稼働停止を検知した場合は、利用者に速報を通知すること。

【ベストプラクティス】

i. 監視対象機器の死活監視を行うための方法（ping[13]コマンドなど）、監視インターバル、監視時間帯、監視体制等の実施基準・手順等を明確にすることが望ましい。

ii. 実施基準・手順等に従い監視を行い、監視結果について評価・見直しを行うことが望ましい。

iii. 稼働停止を検知した場合は、短文の電子メール等で利用者に速やかに速報を通知することが望ましい。ここで、通知先には、利用者側の管理連絡窓口だけでなく、ASP・SaaS サービスを利用する全ての者を含むことが望ましい。

削除：P

削除：コマンド

【評価項目】

a. 死活監視インターバル（応答確認）

パターン	対策参照値
1	1 回以上／5 分*
2	1 回以上／10 分*
3	1 回以上／20 分*
4	1 回以上／5 分*
5	1 回以上／10 分*
6	1 回以上／20 分*

[13] Packet INternet Groper。TCP/IP ネットワークの状態を診断するためのツール。監視対象機器に ping コマンドを送信すると受信した機器から応答が返ってくる。その応答状況から、対象機器の動作状態や通信に要する時間等を確認することができる。

削除：の略号

b. 通知時間（稼働停止検知後、利用者に通知するまでの時間）

パターン	対策参照値
1	20 分以内*
2	60 分以内*
3	5 時間以内*
4	20 分以内*
5	60 分以内*
6	5 時間以内*

Ⅲ．１．１．２ **【基本】**

ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の障害監視（サービスが正常に動作していることの確認）を行うこと。 障害を検知した場合は、利用者に速報を通知すること。

【ベストプラクティス】

i. サービス稼働状態を監視するための方法、監視インターバル、監視時間帯、監視体制等の実施基準・手順等を明確にすることが望ましい。

ii. 実施基準・手順等に従い監視を行い、監視結果について評価・見直しを行うことが望ましい。

iii. 障害を検知した場合は、短文の電子メール等で利用者に速報を通知することが望ましい。ここで、通知先は利用者側の管理連絡窓口のみとすることが望ましい。

【評価項目】

a. 障害監視インターバル

パターン	対策参照値
1	1 回／10 分
2	1 回／30 分
3	1 回／60 分
4	1 回／10 分
5	1 回／30 分
6	1 回／60 分

b. 通知時間（障害検知後、利用者に通知するまでの時間）

パターン	対策参照値
1	20 分
2	60 分
3	5 時間
4	20 分
5	60 分
6	5 時間

Ⅲ．１．１．３ **【推奨】**

ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ、ストレージ、ネットワークに対し一定間隔でパフォーマンス監視（サービスのレスポンス時間の監視）を行うこと。 また、利用者との取決めに基づいて、監視結果を利用者に通知すること。

【ベストプラクティス】

i. 監視の実施にあたり、監視方法（コマンドの入力手順、監視ツールの操作手順等）、監視インターバル、監視時間帯、監視体制等の実施基準・手順等を明確にすることが望ましい。

ii. 監視の結果、ASP・SaaS サービスのレスポンス時間が大きく増加した場合には、SLA 等の利用者との取決めに基づいて、利用者に速報を通知することが望ましい。ここで、通知先は利用者側の管理連絡窓口のみとすることが望ましい。

iii. 管理責任者は、監視結果をレビューし、必要ならば実施基準・手順等の評価・見直しを行うことが望ましい。

【評価項目】

a. パフォーマンス監視インターバル

パターン	対策参照値
1	1 回／10 分
2	1 回／30 分
3	1 回／60 分
4	1 回／10 分
5	1 回／30 分
6	1 回／60 分

b.　通知時間（異常検知後、利用者に通知するまでの時間）

パターン	対策参照値
1	20 分
2	60 分
3	5 時間
4	20 分
5	60 分
6	5 時間

Ⅲ．１．１．４**【推奨】**

ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等の稼働監視、障害監視、パフォーマンス監視の結果を評価・総括して、管理責任者に報告すること。

【ベストプラクティス】

i. 監視結果の報告内容、報告時期、報告先等の実施基準・手順等を明確にすることが望ましい。

ii. 管理責任者への報告は電子メール、紙文書等で直接伝えることが望ましいが、管理用 Web ページに掲載して伝えることでも良い。

Ⅲ．１．１．５**【基本】**

ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）の時刻同期の方法を規定し、実施すること。

【ベストプラクティス】

i. タイムビジネス信頼・安心認定制度における時刻提供精度要求等を参考にして、日本標準時との同期を取ることが望ましい。

ii. ASP・SaaS サービスでは、責任分界の観点から、ログによる証拠保全が重要であるため、サーバ・ストレージ間でも時刻同期を取ることが望ましい。

iii. 全ての機器の時刻同期を行う方法、及び時刻に誤差が生じた場合の修正方法について明確にすることが望ましい。（例：NTP[14]サーバの利用）

[14] Network Time Protocol。ネットワークを介してコンピュータの内部時計を同期する通信規約。

iv. 定期的に時刻同期の状況を確認することが望ましい。

Ⅲ．１．１．６**【基本】**

ASP・SaaS サービスの提供に用いるプラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器についての技術的ぜい弱性に関する情報（OS、その他ソフトウェアのパッチ発行情報等）を定期的に収集し、随時パッチによる更新を行うこと。

【ベストプラクティス】

i. 情報セキュリティに関する情報を提供している機関（@police、JPCERT/CC、IPA セキュリティセンター等）や、ハードウェアベンダ、ソフトウェアベンダ、オープンソフトウェア・フリーソフトウェア等のセキュリティ情報を提供している Web サイト等からぜい弱性に関する情報を入手することができる。

ii. ぜい弱性が発見された場合は、提供されたパッチを適用することによる情報システムへの影響を確認した上で、パッチ適用を実施することが望ましい。

【評価項目】

a. OS、その他ソフトウェアに対するパッチ更新作業の着手までの時間

パターン	対策参照値
1	ベンダリリースから 24 時間以内*
2	ベンダリリースから 24 時間以内*
3	ベンダリリースから 24 時間以内*
4	ベンダリリースから 3 日以内*
5	ベンダリリースから 3 日以内*
6	ベンダリリースから 3 日以内*

Ⅲ．１．１．７**【推奨】**

ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）の監視結果（障害監視、死活監視、パフォーマンス監視）について、定期報告書を作成して利用者等に報告すること。

【ベストプラクティス】

i. 定期報告書には、稼働率、SLA の実施結果、パフォーマンス監視結果等を含めることが望ましい。

ii. 定期報告内容は、月単位で集計することが望ましい。

【評価項目】

a. 定期報告の間隔（Web 等による報告も含む）

パターン	対策参照値
1	1 ヶ月
2	3 ヶ月
3	6 ヶ月
4	1 ヶ月
5	3 ヶ月
6	6 ヶ月

Ⅲ．１．１．８**【基本】**

ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）に係る稼働停止、障害、パフォーマンス低下等について、速報をフォローアップする追加報告を利用者に対して行うこと。

【ベストプラクティス】

i. 稼働停止、障害、パフォーマンス低下、その他の情報セキュリティ事象について、第一報(速報)に続いて、より詳しい分析報告を利用者に対して行うことが望ましい。ここで、報告先は利用者側の管理連絡窓口のみとすることが望ましい。

ii. 追加報告については、電子メールや FAX 同報等で実施することが望ましい。

iii. 原因の分析結果や復旧の予測を含んだ報告を行うことが望ましい。

【評価項目】

a. 第一報（速報）に続く追加報告のタイミング

パターン	対策参照値
1	発見後 1 時間
2	発見後 1 時間
3	発見後 12 時間
4	発見後 1 時間
5	発見後 12 時間
6	発見後 12 時間

Ⅲ．１．１．９**【基本】**

情報セキュリティ監視（稼働監視、障害監視、パフォーマンス監視等）の実施基準・手順等を定めること。 また、ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ、ストレージ、ネットワークの運用・管理に関する手順書を作成すること。

【ベストプラクティス】

i. 運用・管理対象、運用・管理方法（コンピュータの起動・停止の手順、バックアップ、媒体の取扱い、情報セキュリティインシデントへの対応・報告、ログの記録と管理、パフォーマンス監視・評価、システム監査ツールの不正使用の防止等）、運用・管理体制等を明確にすることが望ましい。

ii. 管理責任者は、運用・管理報告についてレビューを実施し、必要ならば実施基準・手順等の評価・見直しを行うことが望ましい。

Ⅲ．２　アプリケーション、プラットフォーム、サーバ・ストレージ

Ⅲ．２．１　アプリケーション、プラットフォーム、サーバ・ストレージの運用・管理

Ⅲ．２．１．１【基本】

ASP・SaaS サービスを利用者に提供する時間帯を定め、この時間帯における ASP・SaaS サービスの稼働率を規定すること。 また、アプリケーション、プラットフォーム、サーバ・ストレージの定期保守時間を規定すること。

【ベストプラクティス】

i. ASP・SaaS サービスを利用者に提供する時間帯（サービス時間帯）とは、契約サービス時間から定期保守時間を差し引いたものである。ここで、契約サービス時間とは、契約時に利用者に提示した ASP・SaaS サービスの提供時間（例：365 日/24 時間、休日・日祭日を除く 8:00-20:00 等）のことであり、定期保守時間とは、事前通知された定期保守による ASP・SaaS サービス停止総時間（例：5 時間/1 年）のことである。

ii. 稼働率とは、サービス時間帯に締める実稼働時間の割合のことである。ここで、実稼働時間とは、サービス時間帯において実際に ASP・SaaS サービスの提供が実施された時間のことである。

【評価項目】

a. ASP・SaaS サービスの稼働率

パターン	対策参照値
1	99.5%以上*
2	99%以上*
3	95%以上*
4	99.5%以上*
5	99%以上*
6	95%以上*

Ⅲ．２．１．２【基本】

ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージに対し、利用者の利用状況の予測に基づいて設計した容量・能力等の要求事項を記録した文書を作成し、保存すること。

【ベストプラクティス】

i. 要求されたサービス性能を満たすことを確実にするために、アプリケーション、プラットフォーム、サーバ・ストレージの利用を監視・調整し、また、将来必要とする容量・能力を予測することが望ましい。

ii. 定期的にアプリケーション、プラットフォーム、サーバ・ストレージの利用状況を監視することが望ましい。

【評価項目】

a. 容量・能力等の要求事項を記録した文書の保存期間

パターン	対策参照値
1	サービス提供期間＋1 年間
2	サービス提供期間＋6 ヶ月
3	サービス提供期間＋3 ヶ月
4	サービス提供期間＋1 年間
5	サービス提供期間＋6 ヶ月
6	サービス提供期間＋3 ヶ月

Ⅲ．２．１．３**【基本】**

利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。

【ベストプラクティス】

i. 利用者の利用状況、例外処理及び情報セキュリティ事象の記録として何を取得するか、取得した記録の保管期間、取得した記録の保管方法、取得した記録のチェック（監査等）方法等を明確にすることが望ましい。取得することが望ましい情報の例は以下の通り。

a) 利用者 ID

b) 主要な事象の日時及び内容（例：ログオン、ログオフ、下記 d)e)g)h）の事象発生）

c) 可能な場合には，端末装置の ID 又は所在地

d) 情報システムへのアクセスの、成功及び失敗した試みの記録

e) データ及び他の情報資産へのアクセスの、成功及び失敗した試みの記録

f) 情報システム構成の変更

g) 特権の利用

h) 情報システムユーティリティ及びアプリケーションの利用

i) アクセスされたファイル及びアクセスの種類
j) ネットワークアドレス及びプロトコル
k) アクセス制御システムが発した警報
l) 保護システム（例えば，ウイルス対策システム，侵入検知システム）の作動及び停止　等

ii. システム障害などによるログの欠損をできる限りを少なくするために、スタンバイ機等を用いてログサーバの運転を迅速に再開できる状態にしておくことが望ましい。

【評価項目】

a. 利用者の利用状況の記録（ログ等）の保存期間

パターン	対策参照値
1	3 ヶ月
2	1 ヶ月
3	1 週間
4	3 ヶ月
5	1 ヶ月
6	1 週間

b. 例外処理及び情報セキュリティ事象の記録（ログ等）の保存期間

パターン	対策参照値
1	5 年
2	1 年
3	6 ヶ月
4	5 年
5	1 年
6	6 ヶ月

c.　スタンバイ機による運転再開

パターン	対策参照値
1	可能（ホットスタンバイ[15]）
2	可能（コールドスタンバイ[16]）
3	-
4	可能（ホットスタンバイ）
5	可能（コールドスタンバイ）
6	-

15 使用する情報システムと同じものを別に用意し、同じ動作を行いながら待機状態にしておくことで、情報システムに障害が発生した際に即座に切り替えができるようにしておく冗長化手法。

16 使用する情報システムと同じものを別に用意するが、ホットスタンバイと異なり同じ動作を行うことはせず、情報システムに障害が発生した際に作動させ切り替える冗長化手法。

Ⅲ．２．１．４**【推奨】**

ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージについて定期的にぜい弱性診断を行い、その結果に基づいて対策を行うこと。

【ベストプラクティス】

i. ぜい弱性の診断対象（アプリケーション等）、診断方法（ポートスキャンツールやぜい弱性診断ツールの使用等）、診断時期等の計画を明確にすることが望ましい。

ii. 診断によりぜい弱性に対する対策を実施した場合は、対策の実施についての記録を残すことが望ましい。

iii. ASP・SaaS サービスの提供に用いるアプリケーションについては、開発段階からぜい弱性診断を行うこと等により、導入前にあらかじめぜい弱性対策を実施しておくことが望ましい。

【評価項目】

a. ぜい弱性診断の実施間隔（サーバ等への外部からの侵入に関する簡易自動診断（ポートスキャン等））

パターン	対策参照値
1	1 回／1 ヶ月
2	1 回／1 ヶ月
3	1 回／1 ヶ月
4	1 回／1 ヶ月
5	1 回／1 ヶ月
6	1 回／1 ヶ月

b. ぜい弱性診断の実施間隔（サーバ等への外部からの侵入に関する詳細診断（ネットワーク関係、外部委託を含む））

パターン	対策参照値
1	1 回／6 ヶ月
2	1 回／1 年
3	1 回／1 年
4	1 回／6 ヶ月
5	1 回／1 年
6	1 回／1 年

c. ぜい弱性診断の実施間隔（アプリケーションの脆弱性の詳細診断（外部委託を含む））

パターン	対策参照値
1	1回／1年
2	1回／1年
3	1回／1年
4	1回／1年
5	1回／1年
6	1回／1年

Ⅲ．２．２　アプリケーション、プラットフォーム、サーバ・ストレージの情報セキュリティ対策

Ⅲ．２．２．１**【基本】**

ASP・SaaS サービスの提供に用いるプラットフォーム、サーバ・ストレージ（データ・プログラム、電子メール、データベース等）についてウイルス等に対する対策を講じること。

【ベストプラクティス】

i. 利用者によるサーバ・ストレージ上のデータへのアクセスに対して、ウイルス対策ソフトによるリアルタイムスキャン、情報システムの完全スキャン等による情報セキュリティ対策を行うことが望ましい。

ii. ウイルス対策ソフトについては、常に最新のパターンファイルを適用することが望ましい。

iii. ソフトウェアに対する情報セキュリティ対策として、ソフトウェアの構成管理（ソフトウェアのバージョンが正しいこと、意図しないソフトウェアが存在しないことの確認等）を行うことが望ましい。

iv. 提供する ASP・SaaS サービスの一環として、利用者によるダウンロードを許可するファイルについては、ウイルス等の不正なコードが含まれていないことを十分に確認してから提供することが望ましい。

【評価項目】

a. パターンファイルの更新間隔

パターン	対策参照値
1	ベンダリリースから 24 時間以内*
2	ベンダリリースから 24 時間以内*
3	ベンダリリースから 3 日以内*
4	ベンダリリースから 24 時間以内*
5	ベンダリリースから 3 日以内*
6	ベンダリリースから 3 日以内*

Ⅲ．２．２．２**【推奨】**

データベースに格納されたデータの暗号化を行うこと

【ベストプラクティス】

i. 特に、個人情報、機密情報等のデータについては、暗号化を行うことが望ましい。

削除：特に

ii. 暗号化・復号に使用する鍵については、改変、破壊、紛失から保護するために厳密に管理することが望ましい。
iii. 使用する暗号アルゴリズムは、電子政府推奨暗号リストに掲載されているアルゴリズムのように、その強度について評価、監視されているものが望ましい。

Ⅲ．２．３　サービスデータの保護

Ⅲ．２．３．１【基本】

利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。

【ベストプラクティス】

i. 業務要件、セキュリティ要件等を考慮して、バックアップ方法（フルバックアップ、差分バックアップ等）、バックアップ対象（利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報等）、バックアップの世代管理方法、バックアップの実施インターバル、バックアップのリストア方法等を明確にすることが望ましい。

【評価項目】

a. バックアップ実施インターバル

パターン	対策参照値
1	1回／1日
2	1回／1週間
3	1回／1ヶ月
4	1回／1日
5	1回／1週間
6	1回／1ヶ月

b. 世代バックアップ

パターン	対策参照値
1	5世代
2	2世代
3	1世代
4	5世代
5	2世代
6	1世代

Ⅲ．２．３．２【推奨】

バックアップされた情報が正常に記録され、正しく読み出すことができるかどうかについて定期的に確認すること。

【ベストプラクティス】

i. 日常の定期確認においては、ファイルをリストアし、ファイルサイズを確認することが多い。より確実な方法としては復旧試験の実施がある。

ii. 定期的に復旧訓練を計画・実施し、結果のレビューを行い、必要に応じて方法の見直しを行うことが望ましい。

【評価項目】

a. バックアップ確認の実施インターバル（ディスクに戻してファイルサイズを確認する等）

パターン	対策参照値
1	バックアップ実施の都度
2	バックアップ実施の都度
3	バックアップ実施の都度
4	バックアップ実施の都度
5	バックアップ実施の都度
6	バックアップ実施の都度

Ⅲ．３　ネットワーク

Ⅲ．３．１　外部ネットワークからの不正アクセス防止

Ⅲ．３．１．１【基本】

ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。 また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。 また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。

【ベストプラクティス】

i. 利用者、情報システム等の管理者、連携 ASP・SaaS 事業者等アクセスの主体ごとに、アクセス制御に適合する業務上の要求を明確に規定することが望ましい。

ii. i.で示した要求に基づいてアクセス制御方針を確立し、文書化し、レビューすることが望ましい。

iii. アクセス制御には、論理的な方法と物理的な方法があり、この両面を併せて考慮することが望ましい。

Ⅲ．３．１．２【基本】

情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限すること。

【ベストプラクティス】

i. アクセス制御方針に則り、情報システム管理者及びネットワーク管理者に情報システム又はネットワークへのアクセス権を与える場合は、正式な認可プロセスによってそのアクセス権の割当を管理することが望ましい。

ii. 特に、情報システム管理者及びネットワーク管理者に情報システム又はネットワークへのアクセス特権を与える必要がある場合は、必要最小限の者に限定し、かつ厳格にその割当を管理することが望ましい。

iii. 管理者権限の割当一覧を作成して管理することが望ましい。

iv. 管理者権限の割当又は使用制限を行うための実施マニュアルを整備することが望ましい。

Ⅲ．３．１．３**【基本】**

利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。

また、運用管理規定を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。

【ベストプラクティス】

i. 情報システム管理者、ネットワーク管理者、連携 ASP・SaaS 事業者等が運用・管理・保守等の目的で遠隔から情報システム又はネットワークにアクセスする必要がある場合は、情報セキュリティポリシーに従って、適切な認証方法を利用し、なりすまし対策を行うことが望ましい。

ii. ID・パスワード等の認証情報は、文字列ではなくハッシュ値[17]を保存することが望ましい。

【評価項目】

a. 利用者のアクセス認証方法

パターン	対策参照値
1	生体認証 又は IC カード
2	IC カード 又は ID・パスワード
3	ID・パスワード
4	ID・パスワード
5	ID・パスワード
6	ID・パスワード

17 ハッシュ関数（入力データから固定長の疑似乱数を生成する関数）で演算することにより得られるデータ。ハッシュ値からは元のデータを復元できない。

b.　情報システム管理者、ネットワーク管理者等のアクセス認証方法

パターン	対策参照値
1	デジタル証明書による認証、 生体認証 又は IC カード
2	生体認証 又は IC カード
3	IC カード 又は ID・パスワード
4	生体認証 又は IC カード
5	IC カード 又は ID・パスワード
6	IC カード 又は ID・パスワード

Ⅲ．３．１．４【基本】

外部及び内部からの不正アクセスを防止する措置（ファイアウォール、リバースプロキシ[18]の導入等）を講じること。

【ベストプラクティス】

i. 外部からの不正アクセスを防止するためには、ファイアウォールを導入することが望ましい。
ii. ファイアウォールを導入する際には、情報セキュリティポリシーに基づいたソフトウェアやハードウェアを選定し、構築することが望ましい。
iii. ファイアウォールは、情報セキュリティポリシーに従って運用されることが望ましい。

Ⅲ．３．１．５【推奨】

不正な通過パケットを自動的に発見、もしくは遮断する措置（IDS[19]/IPS[20]の導入等）を講じること。

【ベストプラクティス】

i. 外部からの不正アクセスを検出するには、IDS/IPS 等を導入することが望ましい。
ii. IDS/IPS 等を導入する際には、業務要件や業務環境に適合したソフトウェアやハードウェアを選定し、構築することが望ましい。
iii. IDS/IPS 等は、業務要件や業務環境に合わせた設定により運用されることが望ましい。

削除：[21]

18 外部ネットワークと ASP・SaaS サービスに用いられるアプリケーションの搭載されたサーバとの間に設置されるプロキシサーバ。利用者は必ずリバースプロキシを経由してサーバにアクセスすることとなるため、外部からサーバへの直接的な不正侵入や攻撃等を防止することができる。
19 Intruder Detection System。予め保持している不正パケットのパターン（シグネチャ）と通過パケットを照合することで、リアルタイムで不正パケットを検知するシステム。
20 Intrusion Prevention System。IDS の機能を拡張し、不正な通過パケットを検知するだけでなく、不正パケットを遮断することで、内部システムへの侵入を防止するシステム。

削除：クライアントからのサーバへの要求を中継するプロキシサーバ。クライアントからのアクセスは、リバースプロキシを経由するため、クライアントはサーバに直接アクセスできない。

【評価項目】

a.　シグニチャ（パターンファイル）の更新間隔

パターン	対策参照値
1	1 回／1 日
2	1 回／3 週間
3	1 回／3 週間
4	1 回／1 日
5	1 回／3 週間
6	1 回／3 週間

Ⅲ．３．２　外部ネットワークにおける情報セキュリティ対策

Ⅲ．３．２．１【基本】

外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、情報交換の実施基準・手順等を備えること。

【ベストプラクティス】

i. 情報交換の手順については、以下の項目を考慮した手順書を作成することが望ましい。
   a) 電子メールの送受信における悪意のあるコードの検知及びそのコードからの保護手順
   b) 添付ファイルとして送受信される電子データの保護手順
   c) 特別なリスクが伴うことを考慮した、無線通信の利用手順
   d) 暗号技術の利用手順　等
ii. 管理者と連携 ASP･SaaS 事業者間の情報交換に外部ネットワークを利用する場合は、情報交換の実施基準・手順等を契約等において明確にすることが望ましい。
iii. 管理者間又は管理者と連携 ASP･SaaS 事業者間の情報交換に外部ネットワークを利用する場合は、交換手段（電子メール、インスタントメッセンジャ、電話、ファクシミリ、ビデオ等）ごとに、交換される情報を適切に保護するための対策（誤送信防止、盗聴防止、改ざん防止等）を講じることが望ましい。

Ⅲ．３．２．２【推奨】

外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、通信の暗号化を行うこと。

【ベストプラクティス】

i. 使用する暗号アルゴリズム･プロトコル及び実装については十分に新しく安全なものを使用すると共に、これらについてのぜい弱性に関する最新の情報を確認し、必要に応じて設定変更や機能変更等の対応をすることが望ましい。
ii. 使用する暗号アルゴリズムは、電子政府推奨暗号リストに掲載されているアルゴリズムのように、その強度について評価、監視されているものが望ましい。

【評価項目】

a. 通信の暗号化

パターン	対策参照値
1	IP 暗号通信（VPN(IPsec)[20]等） 又は HTTP 暗号通信（SSL (TLS)[21]等）
2	IP 暗号通信（VPN(IPsec)等） 又は HTTP 暗号通信（SSL(TLS)等）
3	IP 暗号通信（VPN(IPsec)等） 又は HTTP 暗号通信（SSL(TLS)等）
4	HTTP 暗号通信（SSL(TLS)等）
5	HTTP 暗号通信（SSL(TLS)等）
6	HTTP 暗号通信（SSL(TLS)等）

削除：22

削除：23

削除：24

Ⅲ．３．２．３【基本】

第三者が当該事業者のサーバになりすますこと（フィッシング等）を防止するため、サーバ証明書の取得等の必要な対策を実施すること。

【ベストプラクティス】

i. なりすまし対策のために、正規のサーバ証明書を取得することが望ましい。

ii. 正規のサーバ証明書の取得に加え、紛らわしくないドメイン名を使うこと等により、利用者によるサーバ正当性の確認を容易にすることが望ましい。

Ⅲ．３．２．４【基本】

利用する全ての外部ネットワーク接続について、情報セキュリティ特性、サービスレベル（特に、通信容量とトラヒック変動が重要）及び管理上の要求事項を特定すること。

【ベストプラクティス】

[20] Virtual Private Network。インターネットや多数の利用者が帯域を共有するような公衆回線を、専用線のように利用することができる仮想ネットワーク。IPSec は VPN における通信経路の暗号化方式の１つ。

[21] Secure Socket Layer。公開鍵暗号方式等を組み合わせ、送受信するデータを暗号化するプロトコル。TLS は SSL3.0 を基に作成された暗号化プロトコル

i. ASP・SaaS 事業者と ISP 間、ASP・SaaS 事業者の保守管理用、ASP・SaaS 事業者と連携 ASP・SaaS 事業者間ごとに、情報セキュリティ特性、サービスレベル及び管理上の要求事項を特定することが望ましい。

ii. 提供する ASP・SaaS サービスに利用者の契約する通信回線が含まれていない場合には、利用者に対して当該通信回線については責任を負わない旨を明示することが望ましい。

Ⅲ．３．２．５**【推奨】**

外部ネットワークの障害を監視し、障害を検知した場合は管理責任者に通報すること。

【ベストプラクティス】

i. ASP・SaaS 事業者と ISP 間、ASP・SaaS 事業者の保守管理用、ASP・SaaS 事業者と連携 ASP・SaaS 事業者間等、全ての外部ネットワークに対して監視を実施することが望ましい。

ii. ASP・SaaS 事業者と ISP 間、ASP・SaaS 事業者の保守管理用、ASP・SaaS 事業者と連携 ASP・SaaS 事業者間等、それぞれの外部ネットワークごとに管理責任者を設置し、障害を検知した場合には、それぞれの外部ネットワークの管理責任者に対して通報することが望ましい。

【評価項目】

a. 通報時間（障害が発生してから通報するまでの時間）

パターン	対策参照値
1	検知後 60 分以内
2	-
3	-
4	検知後 60 分以内
5	-
6	-

Ⅲ．４　建物、電源(空調等)

Ⅲ．４．１　建物の災害対策

Ⅲ．４．１．１【推奨】

ASP・SaaS サービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムが設置されている建物（情報処理施設）については、地震・水害に対する対策が行われていること。

【ベストプラクティス】

i. 情報処理施設は、地震や水害が発生しやすい地域の立地を避けることが望ましい。

ii. 情報処理施設には、激しい地震の振動にも耐えられるように、免震構造（建物の振動を緩和する仕組）又は耐震構造（強い振動にも耐えうる頑強な構造）を採用した建物を利用することが望ましい。

iii. サーバルームは建物の 2 階以上に設置することが望ましい。また、屋上からの漏水の危険がある最上階や､水使用設備が隣室または直上階にある場所は避けることが望ましい。

Ⅲ．４．２　電源・空調の維持と災害対策

Ⅲ．４．２．１**【基本】**

ASP・SaaS サービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムを設置する場所には、停電や電力障害が生じた場合に電源を確保するための対策を講じること。

【ベストプラクティス】

i. 非常用無停電電源（UPS 等）は、非常用発電機から電力の供給を受けられることが望ましい。

ii. 複数給電には、本線と予備線を需要家ごとに用意する方式、複数の需要家によってループ経路を形成する方式等がある。

iii. 非常用無停電電源と非常用発電機が非常時に正しく機能するよう、定期的に点検することが望ましい。

【評価項目】

a. 非常用無停電電源（UPS 等）による電力供給時間

パターン	対策参照値
1	10 分
2	10 分
3	10 分
4	10 分
5	10 分
6	10 分

b. 複数給電の実施

パターン	対策参照値
1	実施
2	実施
3	-
4	実施
5	実施
6	-

c. 非常用発電機の設置

パターン	対策参照値
1	実施
2	-
3	-
4	実施
5	-
6	-

Ⅲ．４．２．２**【推奨】**

ASP・SaaS サービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムを設置する場所では、設置されている機器等による発熱を抑えるのに十分な容量の空調を提供すること。

【ベストプラクティス】

i. サーバルームには、サーバルーム専用の空調設備を設置することが望ましい。

ii. 空調能力の設計にあたっては、情報処理施設の構造、サーバルームの規模と発熱量、設置された機器の使用目的と使用条件等を考慮した検討を行うことが望ましい。

Ⅲ．４．３　火災、逃雷、静電気から情報システムを防護するための対策

Ⅲ．４．３．１**【推奨】**

サーバルームに設置されている ASP・SaaS サービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムについて、放水等の消火設備の使用に伴う汚損に対する対策を講じること。

【ベストプラクティス】

i. 代表的な汚損防止対策としては、ガス系消火設備の設置がある。

ii. ガス系消火設備としてよく利用されるのは二酸化炭素消火器である。二酸化炭素消火器は、液化二酸化炭素を圧力により放射して消火を行う消火器である。

【評価項目】

a. 汚損対策の実施

パターン	対策参照値
1	汚損対策消火設備（ガス系消火設備等）の使用
2	汚損対策消火設備（ガス系消火設備等）の使用
3	-
4	汚損対策消火設備（ガス系消火設備等）の使用
5	汚損対策消火設備（ガス系消火設備等）の使用
6	-

Ⅲ．４．３．２**【基本】**

ASP・SaaS サービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムを設置するサーバルームには、火災検知・通報システム及び消火設備を備えること。

【ベストプラクティス】

i. 火災感知器は、熱感知器、煙感知器、炎感知器に大別される。設備メーカーと協議の上、これらの最適な組合せを検討することが望ましい。

ii. 火災感知器の取付場所、取付個数等は感知器の種類により決めることが望ましい。

iii. 火災の原因になりやすい通信・電力ケーブル類が多量にあるフリーアクセス床下にも火災検知器を設置することが望ましい。

Ⅲ．４．３．３**【基本】**

情報処理施設に雷が直撃した場合を想定した対策を講じること。

【ベストプラクティス】

i. 情報処理施設には避雷針を設置することが望ましい。

Ⅲ．４．３．４**【推奨】**

情報処理施設付近に誘導雷が発生した場合を想定した対策を講じること。

【ベストプラクティス】

i. 雷サージ（落雷により誘起された大きな誘導電圧）対策として、電源設備の電源引込口にできるだけ近い場所に、避雷器、電源保護用保安器、CVCF[22]等を設置することが望ましい。

ii. 情報処理施設は等電位化（全ての接地の一本化）を行うことが望ましい。

Ⅲ．４．３．５**【推奨】**

ASP・SaaS サービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムについて、作業に伴う静電気対策を講じること。

【ベストプラクティス】

i. 静電気の発生を防止するため、サーバルームの床材には静電気を除去する帯電防止フリーアクセスフロア、アースシート等を使用することがのぞましい。導電材を添加した塩化ビニルタイル、高圧ラミネート、帯電防止用カーペット等を使用することもできる。

ii. サーバルームの湿度を 40～60%程度に保つことが望ましい。

[22] Constant-Voltage Constant-Frequency。一定の電圧、周波数に維持された電力を供給する装置。

削除：の略号

Ⅲ．４．４　建物の情報セキュリティ対策

Ⅲ．４．４．１【基本】

重要な物理的セキュリティ境界（カード制御による出入口、有人の受付等）に対し、個人認証システムを用いて、従業員及び出入りを許可された外部組織等に対する入退室記録を作成し、適切な期間保存すること。

【ベストプラクティス】

i. 入退室を確実に記録するため、常時利用する出入口は１ヶ所とすることが望ましい。
ii. 個人の資格確認による入退室管理を行うことが望ましい。
iii. 個人認証システムとしては、磁気カード照合、IC カード照合、パスワード入力照合、生体認証による照合等のシステムがある。
iv. 個人認証システムは、入退室者の氏名及び入退室時刻を記録することが望ましい。

【評価項目】

a. 入退室記録の保存

パターン	対策参照値
1	2 年以上*
2	2 年以上*
3	2 年以上*
4	2 年以上*
5	2 年以上*
6	2 年以上*

Ⅲ．４．４．２【推奨】

重要な物理的セキュリティ境界に対して監視カメラを設置し、その稼働時間と監視範囲を定めて監視を行うこと。また、監視カメラの映像を予め定められた期間保存すること。

【ベストプラクティス】

i. 監視性を高めるため、死角を作らないことが望ましい。
ii. 監視カメラは、カラー撮影であり、デジタル記録が可能であることが望ましい。
iii. 監視カメラは用途に応じて十分な解像度を持つことが望ましい。
iv. 監視カメラは、撮影日時が画像内に時分秒まで記録可能であることが望ましい。
v. 非常時に防犯機関等への通報ができる非常通報装置を併設することが望ましい。
vi. 重要な物理的セキュリティ境界においては、個人認証システムと併設することが望

ましい。

【評価項目】

a. 監視カメラの稼働時間

パターン	対策参照値
1	365 日 24 時間
2	365 日 24 時間
3	365 日 24 時間
4	-
5	-
6	-

b. 監視映像保存期間

パターン	対策参照値
1	6 ヶ月
2	1 ヶ月
3	1 週間
4	-
5	-
6	-

Ⅲ．４．４．３**【基本】**

重要な物理的セキュリティ境界からの入退室等を管理するための手順書を作成すること。

Ⅲ．４．４．４**【推奨】**

重要な物理的セキュリティ境界の出入口に破壊対策ドアを設置すること。

【ベストプラクティス】

i. 出入口の扉は十分な強度を有する破壊対策・防火扉を使用し、不法侵入、危険物の投込み、延焼を防止することが望ましい。

Ⅲ．４．４．５**【推奨】**

重要な物理的セキュリティ境界に警備員を常駐させること。

【ベストプラクティス】

i. 警備員の常駐時間を定めることが望ましい。

【評価項目】

a. 警備員の常駐時間

パターン	対策参照値
1	365 日 24 時間
2	365 日 24 時間
3	-
4	365 日 24 時間
5	365 日 24 時間
6	-

Ⅲ．４．４．６**【基本】**

サーバルームやラックの鍵管理を行うこと。

【ベストプラクティス】

i. ラックやサーバルームの出入口の鍵は定められた場所に保管し、管理は特定者が行うことが望ましい。

ii. ラックやサーバルームの出入口の鍵については、受渡し時刻と氏名を記録することが望ましい。

Ⅲ．５　その他

Ⅲ．５．１　機密性・完全性を保持するための対策

Ⅲ．５．１．１【推奨】

電子データの原本性確保を行うこと。

【ベストプラクティス】

i. 電子データの原本性（真正性）確保の手段としては、時刻認証[25]による方法、署名（ハッシュ値によるもの等）による方法、印刷データ電子化・管理による方法等が考えられる。

削除：（タイムスタンプ）

削除：[26]

削除：も含む

【評価項目】

a. 原本性（真正性）確認レベル

パターン	対策参照値
1	時刻認証、署名 及び 印刷データ電子化・管理
2	署名 及び 印刷データ電子化・管理
3	印刷データ電子化・管理
4	時刻認証、署名 及び 印刷データ電子化・管理
5	署名 及び 印刷データ電子化・管理
6	印刷データ電子化・管理

削除：　※時刻認証（タイムスタンプ）、署名（ハッシュ値によるもの等

挿入：値によるもの等

削除：も含む

削除：）、印刷データ電子化・管理等

Ⅲ．５．１．２【基本】

個人情報は関連する法令に基づいて適切に取り扱うこと。

【ベストプラクティス】

i. 個人情報を収集する際には、利用目的を明示し、各個人の同意を得た上で収集することが必要である。また、個人情報の漏洩、滅失、棄損を防止するための措置（例：従業員や協力会社要員に対する必要かつ適切な監督等）を講じる必要がある。

ii. 事前の本人同意無しに個人情報を第三者に提供してはならない。

iii. 本人から利用目的の通知、データ開示、データ訂正・追加・削除、データの利用停止等の求めがあった場合は、これに応じなければならない。また、本人から苦情があ

25 タイムスタンプ（特定の電子情報と時刻情報を結合したもの）を付与することにより、その時刻以前に電子データが存在していたこと（存在性）及び変更・改ざんされていないこと（非改ざん性）を電子的に証明する手法。

った場合には、迅速かつ適切に対応しなければならない。

iv. 法令の適用に際し、関連するガイドラインを参考にすることが望ましい。代表的なガイドラインとしては以下がある。

a)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（経済産業省）

b)電気通信事業における個人情報保護に関するガイドライン（総務省）

c)金融分野における個人情報保護に関するガイドライン（金融庁）

d)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について（厚生労働省）

Ⅲ．５．２　ASP・SaaS 事業者の運用管理端末における情報セキュリティ対策

Ⅲ．５．２．１【基本】

運用管理端末に、許可されていないプログラム等のインストールを行わせないこと。 従業員等が用いる運用管理端末の全てのファイルのウイルスチェックを行うこと。 技術的ぜい弱性に関する情報（OS、その他ソフトウェアのパッチ発行情報等）を定期的に収集し、随時パッチによる更新を行うこと。

【ベストプラクティス】

i. 運用管理端末の管理者権限の付与を厳しく制限することが望ましい。

ii. 運用管理端末において、従業員等が行うログイン・ログアウト、特定プログラムの実行、データベース接続などの重要操作等について、操作ログを取得し、保存することが望ましい。

iii. 許可されていないプログラム等を運用管理端末にインストールすることを禁止し、従業員に周知徹底し、違反した場合には罰則を課すことが望ましい。

iv. 運用管理端末は、ウイルス対策ソフトによるリアルタイムスキャン、システムの完全スキャン等による情報セキュリティ対策を行うことが望ましい。

v. ウイルス対策ソフトについては、常に最新のパターンファイルを適用することが望ましい。

vi. 情報セキュリティに関する情報を提供している機関（@police、JPCERT/CC、IPA セキュリティセンター等）や、ハードウェアベンダ、ソフトウェアベンダ、オープンソフトウェア・フリーソフトウェア等のセキュリティ情報を提供している Web サイト等からぜい弱性に関する情報を入手することができる。

vii. パッチは、運用管理機能への影響が無いと確認した上で適用することが望ましい。

【評価項目】

a. パターンファイルの更新間隔

パターン	対策参照値
1	ベンダリリースから 24 時間以内*
2	ベンダリリースから 24 時間以内*
3	ベンダリリースから 3 日以内*
4	ベンダリリースから 24 時間以内*
5	ベンダリリースから 3 日以内*
6	ベンダリリースから 3 日以内*

b.　OS、その他ソフトウェアに対するパッチ更新作業の着手までの時間

パターン	対策参照値
1	ベンダリリースから 24 時間以内*
2	ベンダリリースから 24 時間以内*
3	ベンダリリースから 24 時間以内*
4	ベンダリリースから 3 日以内*
5	ベンダリリースから 3 日以内*
6	ベンダリリースから 3 日以内*

Ⅲ．５．３　媒体の保管と廃棄

Ⅲ．５．３．１【基本】

紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。

【ベストプラクティス】

i. 個人情報、機密情報等を含む紙、これらのデータを格納した磁気テープ、光メディア等の媒体を保管する際には、鍵付きキャビネット（耐火金庫等）や施錠可能な保管室等を利用することが望ましい。また、保管中の媒体の閲覧記録の作成、コピー制限の設定等の対策を行うことが望ましい。

ii. 紙、磁気テープ、光メディア等の媒体の保管管理手順書を作成することが望ましい。

iii. 保管管理手順書に基づいて、媒体の管理記録を作成するとともに、保管期間を明確にすることが望ましい。

Ⅲ．５．３．２【基本】

機器及び媒体を正式な手順に基づいて廃棄すること。

【ベストプラクティス】

i. 機器の廃棄作業に着手する前に、当該情報システムの運用が完全に終結していることを確認することが望ましい。

ii. 機器の廃棄にあたっては、当該機器の重要度を考慮し、機密保護、プライバシー保護及び不正防止のための対策を講じることが望ましい。内部の重要なデータの読み出しを不可能とすることが必要である。

iii. 機器の廃棄方法及び廃棄時期を明確にし、廃棄作業完了後には廃棄記録について管理責任者の承認を得ることが望ましい。

iv. 廃棄対象にソフトウェアが含まれる場合は、機器からのソフトウェアの削除に加えて、記録媒体とドキュメントを破壊・焼却・裁断等することが望ましい。

v. 紙媒体の廃棄については、機密性が求められるものは裁断または焼却することが望ましい。

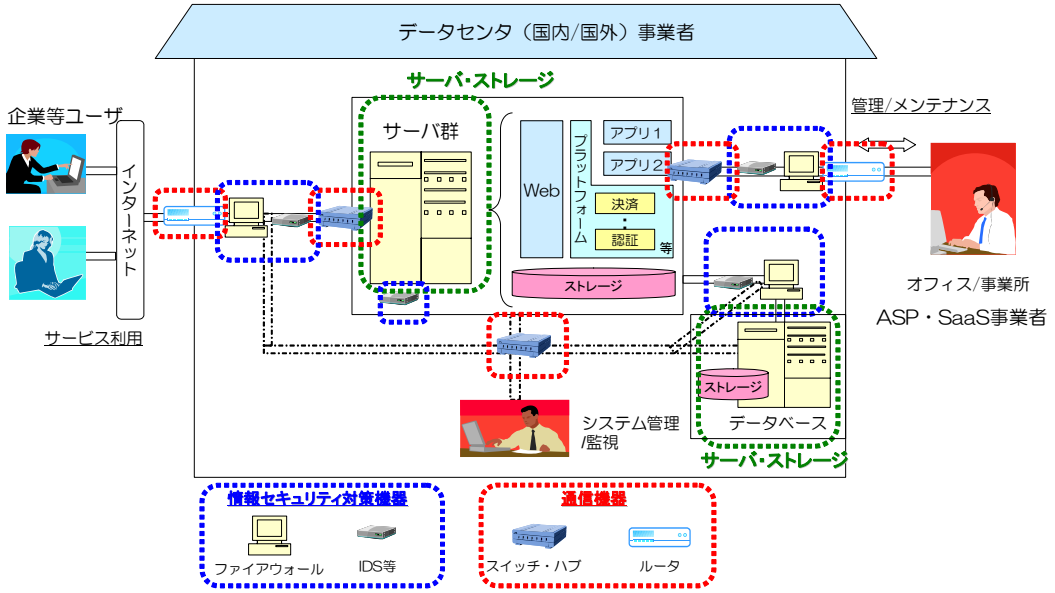
vi. 第３者に廃棄を委託する場合には、秘密保持契約を締結することが望ましい。

Ⅳ.　参考資料

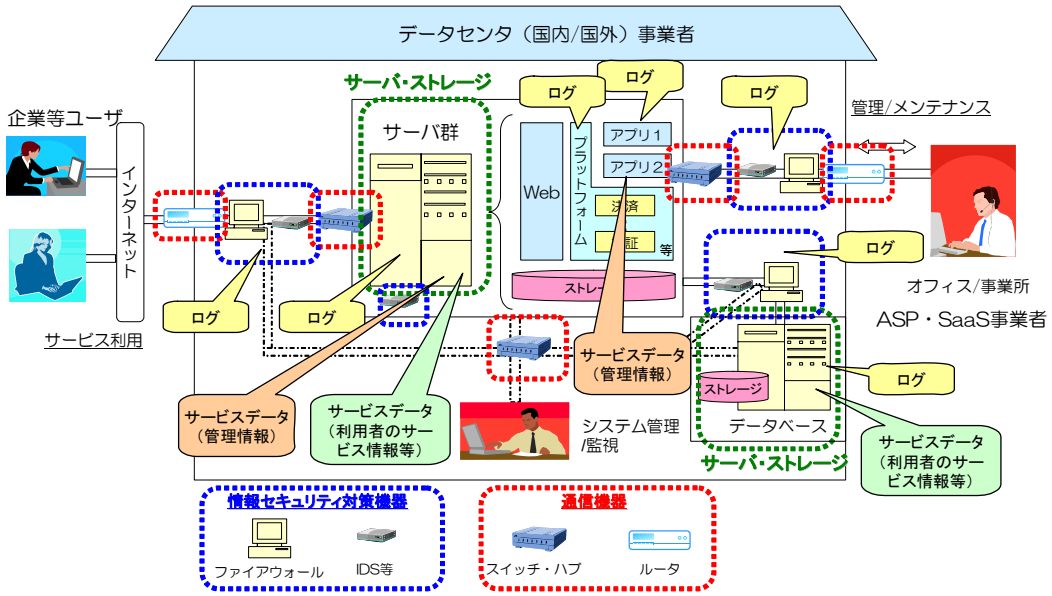
Annex 1

ASP・SaaS サービスの典型的な構成要素と情報資産

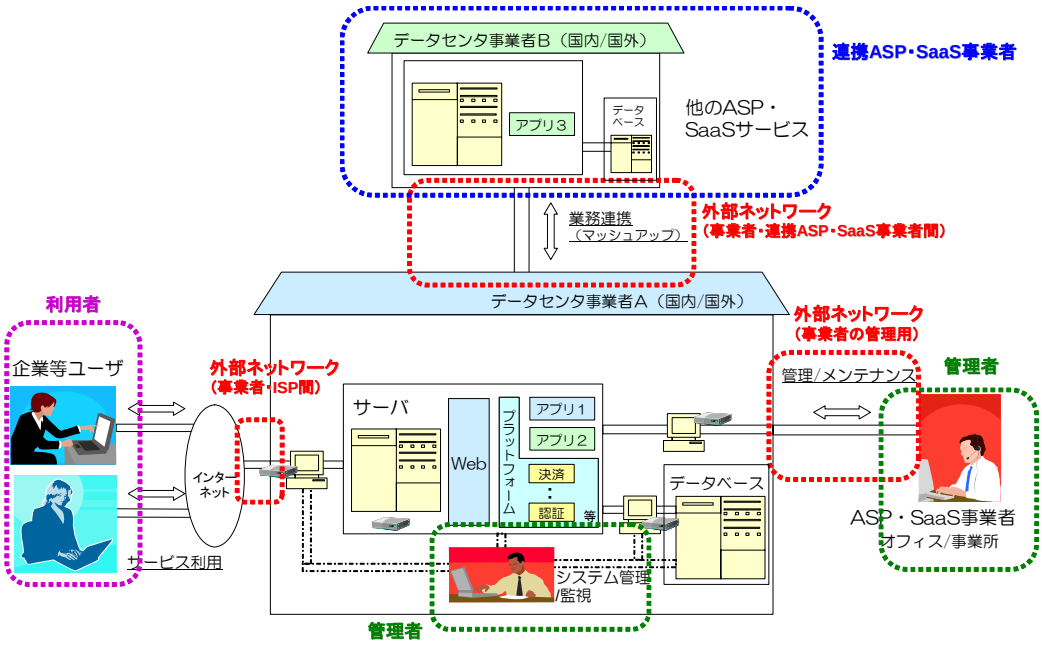
Ⅲ．１　アプリケーション、プラットフォーム、サーバ・ストレージ、ネットワークに共通する情報セキュリティ対策



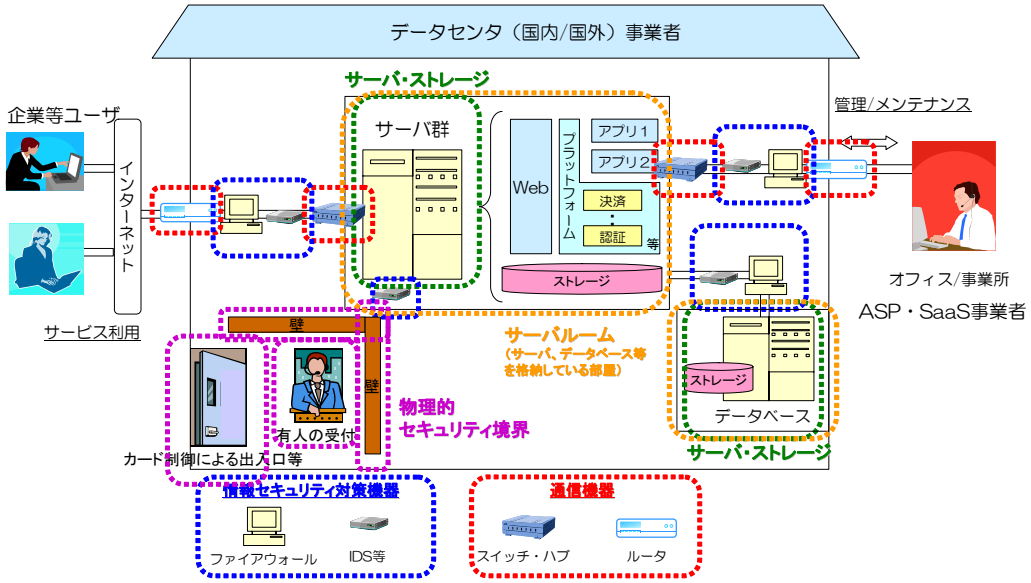
Ⅲ．２　アプリケーション、プラットフォーム、サーバ・ストレージ



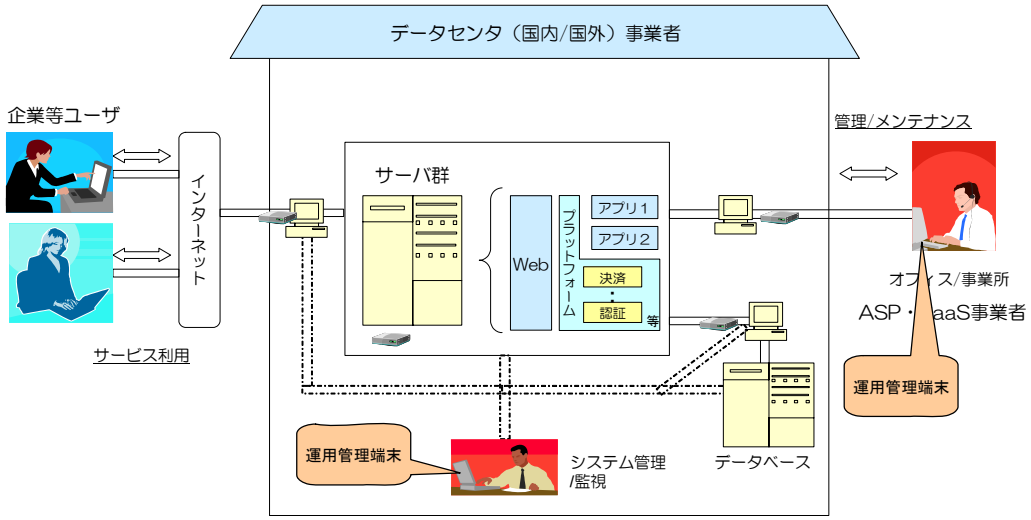
Ⅲ．３　ネットワーク


データセンタ事業者B（国内/国外）
連携ASP・SaaS事業者
アプリ３
データベース
他のASP・SaaSサービス
業務連携
（マッシュアップ）
外部ネットワーク
（事業者・連携ASP・SaaS事業者間）
利用者
データセンタ事業者A（国内/国外）
外部ネットワーク
（事業者の管理用）
企業等ユーザ
外部ネットワーク
（事業者・ISP間）
管理/メンテナンス
管理者
サーバ
Web
フラットフォーム
アプリ１
アプリ２
決済
認証
等
インターネット
データベース
ASP・SaaS事業者
オフィス/事業所
サービス利用
システム管理/監視
管理者

Ⅲ．４　建物、電源（空調等）


データセンタ（国内/国外）事業者
サーバ・ストレージ
企業等ユーザ
インターネット
サービス利用
サーバ群
Web
プラットフォーム
アプリ１
アプリ２
決済
認証
等
ストレージ
管理/メンテナンス
オフィス/事業所
ASP・SaaS事業者
壁
壁
有人の受付
カード制御による出入口等
物理的
セキュリティ境界
サーバルーム
（サーバ、データベース等
を格納している部屋）
ストレージ
データベース
サーバ・ストレージ
情報セキュリティ対策機器
ファイアウォール
IDS等
通信機器
スイッチ・ハブ
ルータ

Ⅲ．５　その他


データセンタ（国内/国外）事業者
企業等ユーザ
インターネット
サービス利用
サーバ群
Web
プラットフォーム
アプリ１
アプリ２
決済
認証
等
管理/メンテナンス
オフィス/事業所
ASP・SaaS事業者
運用管理端末
運用管理端末
システム管理
/監視
データベース

Annex 2

組織・運用編　対策項目一覧表

Annex2　組織・運用編 対策項目一覧表

項番.	対策項目	区分	実施チェック
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	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。	基本	
Ⅱ．1．1．2	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。	基本	
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	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。	基本	
Ⅱ．2．1．2	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。	基本	
Ⅱ．2．1．3	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。	基本	
Ⅱ．2．2　外部組織（データセンタを含む）			
Ⅱ．2．2．1	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。	基本	
Ⅱ．2．2．2	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。	基本	
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	連連携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。	基本	
Ⅱ．3．1．2	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。	基本	
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	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。	基本	
Ⅱ．4．2　情報の分類			
Ⅱ．4．2．1	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。	基本	

項番.	対策項目	区分	実施チェック
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	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。	基本	
Ⅱ．4．3．2	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。	基本	
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	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。	基本	
Ⅱ．5．2　雇用期間中			
Ⅱ．5．2．1	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。	基本	
Ⅱ．5．2．2	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。	基本	
Ⅱ．5．3　雇用の終了又は変更			
Ⅱ．5．3．1	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。	基本	
Ⅱ．6　情報セキュリティインシデントの管理			
Ⅱ．6．1　情報セキュリティインシデント及びぜい弱性の報告			
Ⅱ．6．1．1	全ての従業員に対し、業務において発見あるいは疑いをもった情報システムのぜい弱性や情報セキュリティインシデント（サービス停止、情報の漏えい・改ざん・破壊・紛失、ウイルス感染等）について、どのようなものでも記録し、できるだけ速やかに管理責任者に報告できるよう手続きを定め、実施を要求すること。 報告を受けた後に、迅速に整然と効果的な対応ができるよう、責任体制及び手順を確立すること。	基本	
Ⅱ．7　コンプライアンス			
Ⅱ・7．1　法令と規則の遵守			
Ⅱ．7．1．1.	個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。	基本	
Ⅱ．7．1．2	ASP・SaaSサービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。	基本	
Ⅱ．7．1．3	利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと。	基本	
Ⅱ．8　ユーザサポートの責任			
Ⅱ．8．1　利用者への責任			
Ⅱ．8．1．1	ASP・SaaSサービスの提供に支障が生じた場合には、その原因が連携ASP・SaaS事業者に起因するものであったとしても、利用者と直接契約を結ぶASP・SaaS事業者が、その責任において一元的にユーザサポートを実施すること。	基本	

Annex 3

物理的・技術的対策編　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

				機密性	高			低			
				可用性	高	中	低	高	中	低	
					パターン1	パターン2	パターン3	パターン4	パターン5	パターン6	
対策項目番号	評価項目番号	対策項目	区分	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	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。						実施チェック
Ⅲ．1　アプリケーション、プラットフォーム、サーバ・ストレージ、ネットワークに共通する情報セキュリティ対策											
Ⅲ．1．1　運用・管理に関する共通対策											
Ⅲ．1．1．1	a	ASP・SaaSサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の稼働監視（応答確認等）を行うこと。 稼働停止を検知した場合は、利用者に速報を通知すること。	基本	死活監視インターバル （応答確認）	1回以上／5分*	1回以上／10分*	1回以上／20分*	1回以上／5分*	1回以上／10分*	1回以上／20分*	
	b			通知時間 （稼動停止検知後、利用者に通知するまでの時間）	20分以内*	60分以内*	5時間以内*	20分以内*	60分以内*	5時間以内*	
Ⅲ．1．1．2	a	ASP・SaaSサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の障害監視（サービスが正常に動作していることの確認）を行うこと。 障害を検知した場合は、利用者に速報を通知すること。	基本	障害監視インターバル	1回/10分	1回/30分	1回/60分	1回/10分	1回/30分	1回/60分	
	b			通知時間 （障害検知後、利用者に通知するまでの時間）	20分	60分	5時間	20分	60分	5時間	
Ⅲ．1．1．3	a	ASP・SaaSサービスの提供に用いるアプリケーション、プラットフォーム、サーバ、ストレージ、ネットワークに対し一定間隔でパフォーマンス監視（サービスのレスポンス時間の監視）を行うこと。 また、利用者との取決めに基づいて、監視結果を利用者に通知すること。	推奨	パフォーマンス監視インターバル	1回/10分	1回/30分	1回/60分	1回/10分	1回/30分	1回/60分	
	b			通知時間 （異常検知後、利用者に通知するまでの時間）	20分	60分	5時間	20分	60分	5時間	
Ⅲ．1．1．4	-	ASP・SaaSサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等の稼働監視、障害監視、パフォーマンス監視の結果を評価・総括して、管理責任者に報告すること。	推奨								
Ⅲ．1．1．5	-	ASP・SaaSサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）の時刻同期の方法を規定し、実施すること。	基本								
Ⅲ．1．1．6	-	ASP・SaaSサービスの提供に用いるプラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器についての技術的ぜい弱性に関する情報（OS、その他ソフトウェアのパッチ発行情報等）を定期的に収集し、随時パッチによる更新を行うこと。	基本	OS、その他ソフトウェアに対するパッチ更新作業の着手までの時間	ベンダーリリースから24時間以内*	ベンダーリリースから24時間以内*	ベンダーリリースから24時間以内*	ベンダーリリースから3日以内*	ベンダーリリースから3日以内*	ベンダーリリースから3日以内*	
Ⅲ．1．1．7	-	ASP・SaaSサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）の監視結果（障害監視、死活監視、パフォーマンス監視）について、定期報告書を作成して利用者等に報告すること。	推奨	定期報告の間隔 （Web等による報告も含む）	1ヶ月	3ヶ月	6ヶ月	1ヶ月	3ヶ月	6ヶ月	
Ⅲ．1．1．8	-	ASP・SaaSサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）に係る稼働停止、障害、パフォーマンス低下等について、速報をフォローアップする追加報告を利用者に対して行うこと。	基本	第一報（速報）に続く追加報告のタイミング	発見後1時間	発見後1時間	発見後12時間	発見後1時間	発見後12時間	発見後12時間	

対策項目番号	評価項目番号	対策項目	区分	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	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。						実施チェック
Ⅲ．1．1．9	-	情報セキュリティ監視（稼働監視、障害監視、パフォーマンス監視等）の実施基準・手順等を定めること。 また、ASP・SaaSサービスの提供に用いるアプリケーション、プラットフォーム、サーバ、ストレージ、ネットワークの運用・管理に関する手順書を作成すること。	基本								
Ⅲ．2 アプリケーション、プラットフォーム、サーバ・ストレージ											
Ⅲ．2．1 アプリケーション、プラットフォーム、サーバ・ストレージの運用・管理											
Ⅲ．2．1．1	-	ASP・SaaSサービスを利用者に提供する時間帯を定め、この時間帯におけるASP・SaaSサービスの稼働率を規定すること。 また、アプリケーション、プラットフォーム、サーバ・ストレージの定期保守時間を規定すること。	基本	ASP・SaaSサービスの稼働率	99.5%以上*	99%以上*	95%以上*	99.5%以上*	99%以上*	95%以上*	
Ⅲ．2．1．2	-	ASP・SaaSサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージに対し、利用者の利用状況の予測に基づいて設計した容量・能力等の要求事項を記録した文書を作成し、保存すること。	基本	容量・能力等の要求事項を記録した文書の保存期間	サービス提供期間＋1年間	サービス提供期間＋6ヶ月	サービス提供期間＋3ヶ月	サービス提供期間＋1年間	サービス提供期間＋6ヶ月	サービス提供期間＋3ヶ月	
Ⅲ．2．1．3	a	利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。	基本	利用者の利用状況の記録（ログ等）の保存期間	3ヶ月	1ヶ月	1週間	3ヶ月	1ヶ月	1週間	
	b			例外処理及び情報セキュリティ事象の記録（ログ等）の保存期間	5年	1年	6ヶ月	5年	1年	6ヶ月	
	c			スタンバイ機による運転再開	可能 （ホットスタンバイ）	可能 （コールドスタンバイ）	-	可能 （ホットスタンバイ）	可能 （コールドスタンバイ）	-	
Ⅲ．2．1．4	a	ASP・SaaSサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージについて定期的にぜい弱性診断を行い、その結果に基づいて対策を行うこと。	推奨	ぜい弱性診断の実施間隔（サーバ等への外部からの侵入に関する簡易自動診断（ポートスキャン等））	1回/1ヶ月	1回/1ヶ月	1回/1ヶ月	1回/1ヶ月	1回/1ヶ月	1回/1ヶ月	
	b			ぜい弱性診断の実施間隔（サーバ等への外部からの侵入に関する詳細診断（ネットワーク関係、外部委託を含む））	1回/6ヶ月	1回/1年	1回/1年	1回/6ヶ月	1回/1年	1回/1年	
	c			ぜい弱性診断の実施間隔（アプリケーションの脆弱性の詳細診断（外部委託を含む））	1回/1年	1回/1年	1回/1年	1回/1年	1回/1年	1回/1年	
Ⅲ．2．2 アプリケーション、プラットフォーム、サーバ・ストレージの情報セキュリティ対策											
Ⅲ．2．2．1	-	ASP・SaaSサービスの提供に用いるプラットフォーム、サーバ・ストレージ（データ・プログラム、電子メール、データベース等）についてウイルス等に対する対策を講じること。	基本	パターンファイルの更新間隔	ベンダーリリースから24時間以内*	ベンダーリリースから24時間以内*	ベンダーリリースから3日以内*	ベンダーリリースから24時間以内*	ベンダーリリースから3日以内*	ベンダーリリースから3日以内*	
Ⅲ．2．2．2	-	データベースに格納されたデータの暗号化を行うこと	推奨								
Ⅲ．2．3 サービスデータの保護											
Ⅲ．2．3．1	a	利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。	基本	バックアップ実施インターバル	1回/1日	1回/1週間	1回/1ヶ月	1回/1日	1回/1週間	1回/1ヶ月	
	b			世代バックアップ	5世代	2世代	1世代	5世代	2世代	1世代	

対策項目番号	評価項目番号	対策項目	区分	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	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。						実施チェック
Ⅲ．2．3．2	−	バックアップされた情報が正常に記録され、正しく読み出すことができるかどうかについて定期的に確認すること。	推奨	バックアップ確認の実施インターバル （ディスクに戻してファイルサイズを確認する等）	バックアップ実施の都度	バックアップ実施の都度	バックアップ実施の都度	バックアップ実施の都度	バックアップ実施の都度	バックアップ実施の都度	
Ⅲ．3 ネットワーク											
Ⅲ．3．1 外部ネットワークからの不正アクセス防止											
Ⅲ．3．1．1	−	ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。 また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。 また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。	基本								
Ⅲ．3．1．2	−	情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限すること。	基本								
Ⅲ．3．1．3	a	利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。 また、運用管理規定を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。	基本	利用者のアクセス認証方法	生体認証 又は ICカード	ICカード 又は ID・パスワード	ID・パスワード	ID・パスワード	ID・パスワード	ID・パスワード	
	b			情報システム管理者、ネットワーク管理者等のアクセス認証方法	デジタル証明書による認証、生体認証 又は ICカード	生体認証 又は ICカード	ICカード 又は ID・パスワード	生体認証 又は ICカード	ICカード 又は ID・パスワード	ICカード 又は ID・パスワード	
Ⅲ．3．1．4	−	外部及び内部からの不正アクセスを防止する措置（ファイアウォール、リバースプロキシの導入等）を講じること。	基本								
Ⅲ．3．1．5	−	不正な通過パケットを自動的に発見、もしくは遮断する措置（IDS /IPS の導入等）を講じること。	推奨	シグニチャ（パターンファイル）の更新間隔	1回/1日	1回/3週間	1回/3週間	1回/1日	1回/3週間	1回/3週間	
Ⅲ．3．2 外部ネットワークにおける情報セキュリティ対策											
Ⅲ．3．2．1	−	外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、情報交換の実施基準・手順等を備えること。	基本								
Ⅲ．3．2．2	−	外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、通信の暗号化を行うこと。	推奨	通信の暗号化	IP暗号通信 （VPN(IPsec)等） 又は HTTP暗号通信 （SSL(TLS)等）	IP暗号通信 （VPN(IPsec)等） 又は HTTP暗号通信 （SSL(TLS)等）	IP暗号通信 （VPN(IPsec)等） 又は HTTP暗号通信 （SSL(TLS)等）	HTTP暗号通信 （SSL(TLS)等）	HTTP暗号通信 （SSL(TLS)等）	HTTP暗号通信 （SSL(TLS)等）	
Ⅲ．3．2．3	−	第三者が当該事業者のサーバになりすますこと（フィッシング等）を防止するため、サーバ証明書の取得等の必要な対策を実施すること。	基本								
Ⅲ．3．2．4	−	利用する全ての外部ネットワーク接続について、情報セキュリティ特性、サービスレベル（特に、通信容量とトラヒック変動が重要）及び管理上の要求事項を特定すること。	基本								
Ⅲ．3．2．5	−	外部ネットワークの障害を監視し、障害を検知した場合は管理責任者に通報すること。	推奨	通報時間 （障害が発生してから通報するまでの時間）	検知後60分	−	−	検知後60分	−	−	

対策項目番号	評価項目番号	対策項目	区分	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	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。						実施チェック
Ⅲ．4　建物、電源（空調等）											
Ⅲ．4．1　建物の災害対策											
Ⅲ．4．1．1	−	ASP・SaaSサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムが設置されている建物（情報処理施設）については、地震・水害に対する対策が行われていること。	推奨								
Ⅲ．4．2　電源・空調の維持と災害対策											
Ⅲ．4．2．1	a	ASP・SaaSサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムを設置する場所には、停電や電力障害が生じた場合に電源を確保するための対策を講じること。	基本	非常用無停電電源（UPS等）による電力供給時間	10分	10分	10分	10分	10分	10分	
	b			複数給電の実施	実施	実施	−	実施	実施	−	
	c			非常用発電機の設置	実施	−	−	実施	−	−	
Ⅲ．4．2．2	−	ASP・SaaSサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムを設置する場所では、設置されている機器等による発熱を抑えるのに十分な容量の空調を提供すること。	推奨								
Ⅲ．4．3　火災、逃雷、静電気から情報システムを防護するための対策											
Ⅲ．4．3．1	−	サーバルームに設置されているASP・SaaSサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムについて、放水等の消火設備の使用に伴う汚損に対する対策を講じること。	推奨	汚損対策の実施	汚損対策消火設備（ガス系消火設備等）の使用	汚損対策消火設備（ガス系消火設備等）の使用	−	汚損対策消火設備（ガス系消火設備等）の使用	汚損対策消火設備（ガス系消火設備等）の使用	−	
Ⅲ．4．3．2	−	ASP・SaaSサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムを設置するサーバルームには、火災検知・通報システム及び消火設備を備えること。	基本								
Ⅲ．4．3．3	−	情報処理施設に雷が直撃した場合を想定した対策を講じること。	基本								
Ⅲ．4．3．4	−	情報処理施設付近に誘導雷が発生した場合を想定した対策を講じること。	推奨								
Ⅲ．4．3．5	−	ASP・SaaSサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムについて、作業に伴う静電気対策を講じること。	推奨								
Ⅲ．4．4　建物の情報セキュリティ対策											
Ⅲ．4．4．1	−	重要な物理的セキュリティ境界（カード制御による出入口、有人の受付等）に対し、個人認証システムを用いて、従業員及び出入りを許可された外部組織等に対する入退室記録を作成し、適切な期間保存すること。	基本	入退室記録の保存	2年以上*	2年以上*	2年以上*	2年以上*	2年以上*	2年以上*	
Ⅲ．4．4．2	a	重要な物理的セキュリティ境界に対して監視カメラを設置し、その稼働時間と監視範囲を定めて監視を行うこと。また、監視カメラの映像を予め定められた期間保存すること。	推奨	監視カメラの稼働時間	365日24時間	365日24時間	365日24時間	−	−	−	
	b			監視映像保存期間	6ヶ月	1ヶ月	1週間	−	−	−	
Ⅲ．4．4．3	−	重要な物理的セキュリティ境界からの入退室等を管理するための手順書を作成すること。	基本								

対策項目番号	評価項目番号	対策項目	区分	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	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。						実施チェック
Ⅲ．4．4．4	−	重要な物理的セキュリティ境界の出入口に破壊対策ドアを設置すること。	推奨								
Ⅲ．4．4．5	−	重要な物理的セキュリティ境界に警備員を常駐させること。	推奨	警備員の常駐時間	365日24時間	365日24時間	−	365日24時間	365日24時間	−	
Ⅲ．4．4．6	−	サーバルームやラックの鍵管理を行うこと。	基本								
Ⅲ．5 その他											
Ⅲ．5．1 機密性・完全性を保持するための対策											
Ⅲ．5．1．1	−	電子データの原本性確保を行うこと。	推奨	原本性（真正性）確認レベル	時刻認証、署名 及び 印刷データ電子化・管理	署名 及び 印刷データ電子化・管理	印刷データ電子化・管理	時刻認証、署名 及び 印刷データ電子化・管理	署名 及び 印刷データ電子化・管理	印刷データ電子化・管理	
Ⅲ．5．1．2	−	個人情報は関連する法令に基づいて適切に取り扱うこと。	基本								
Ⅲ．5．2 ASP・SaaS事業者の運用管理端末における情報セキュリティ対策											
Ⅲ．5．2．1	a	運用管理端末に、許可されていないプログラム等のインストールを行わせないこと。 従業員等が用いる運用管理端末の全てのファイルのウイルスチェックを行うこと。 技術的ぜい弱性に関する情報（OS、その他ソフトウェアのパッチ発行情報等）を定期的に収集し、随時パッチによる更新を行うこと。	基本	パターンファイルの更新間隔	ベンダーリリースから24時間以内*	ベンダーリリースから24時間以内*	ベンダーリリースから3日以内*	ベンダーリリースか24時間以内*	ベンダーリリースから3日以内*	ベンダーリリースから3日以内*	
	b			OS、その他ソフトウェアに対するパッチ更新作業の着手までの時間	ベンダーリリースか24時間以内*	ベンダーリリースか24時間以内*	ベンダーリリースか24時間以内*	ベンダーリリースから3日以内*	ベンダーリリースから3日以内*	ベンダーリリースから3日以内*	
Ⅲ．5．3 媒体の保管と廃棄											
Ⅲ．5．3．1	−	紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。	基本								
Ⅲ．5．3．2	−	機器及び媒体を正式な手順に基づいて廃棄すること。	基本								