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。

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