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[12]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。

【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*

[12] 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。

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[13]サーバの利用）

[13] 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. システム障害等によるログの欠損をできる限り少なくするために、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[14]）
2	可能（コールドスタンバイ[15]）
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	-

14 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。

15 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。

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[16]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

16 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[17]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[18]/IPS[19]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。

17 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。

18 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。

19 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。

【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）

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】

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。

---

[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

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。