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

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[20]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。

【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

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

20　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。

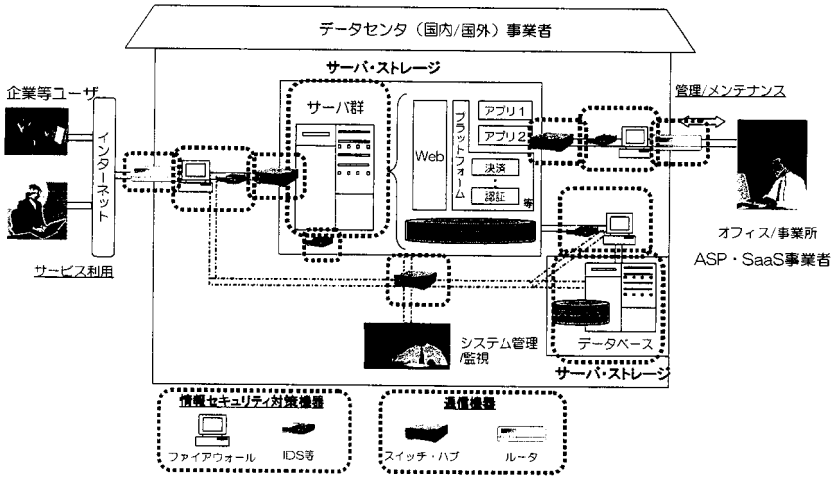
Ⅲ．５．３．２**【基本】**

機器及び媒体を正式な手順に基づいて廃棄すること。

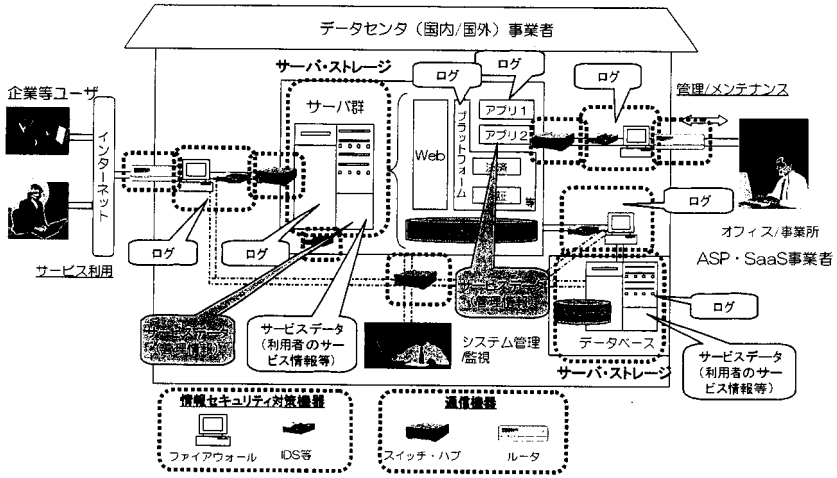
【ベストプラクティス】

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。

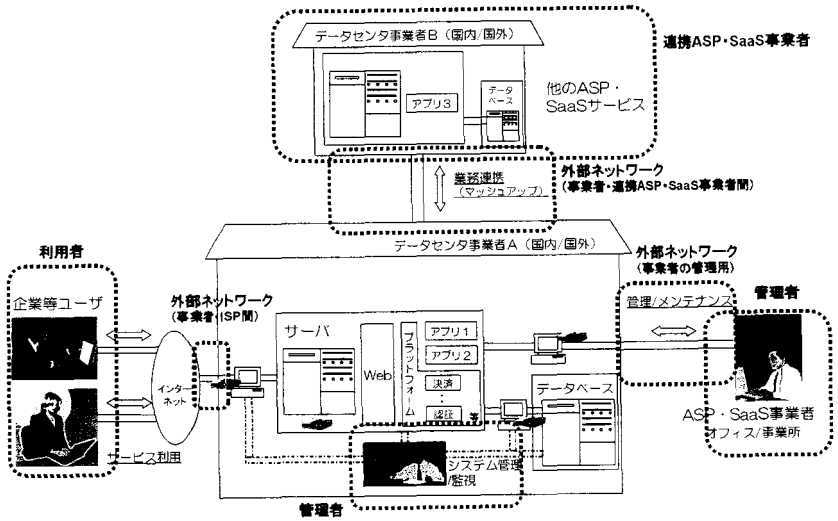
Ⅲ. 1　アプリケーション、プラットフォーム、サーバ・ストレージ、ネットワークに共通する情報セキュリティ対策



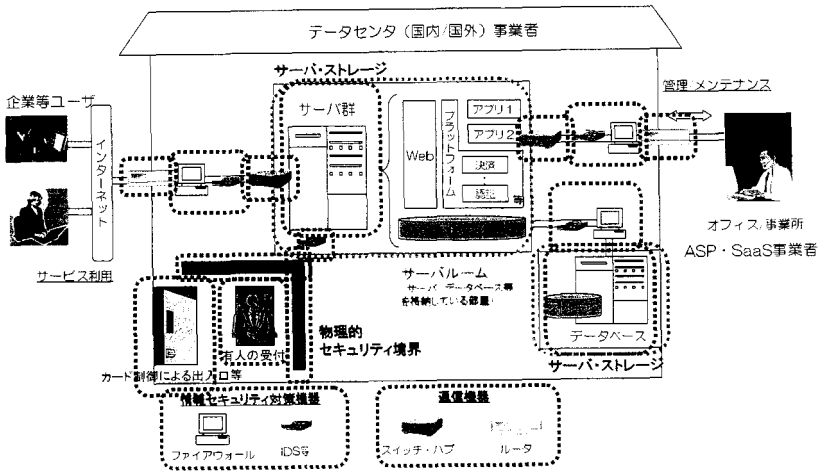
Ⅲ. 2　アプリケーション、プラットフォーム、サーバ・ストレージ



Ⅲ．３　ネットワーク



Ⅲ．４　建物、電源（空調等）



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事業者から提供される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状況の点検及び監査			
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弱い弱性の報告			
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

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
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	
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、通雷、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。	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								