

情報セキュリティ対策要件書

項番	対策項目	区分	備考
Ⅱ 組織・運用編			
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（データセンターを含む）			
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	
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	

情報セキュリティ対策要件書

項番	対策項目	区分	備考
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きを備えること。	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脆弱性の報告			
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脆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 ユーザーサポートの責任			
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ーサポートを実施すること。	基本	
Ⅲ 物理的・技術的対策編			
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10分に1回以上行うこと。	基本	
	b 稼働停止を検知した場合は、速報を利用者に60分以内に通知すること。	基本	
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等）を30分に1回以上行うこと。	基本	
	b 障害を検知した場合は、速報を利用者に60分以内に通知すること。	基本	
Ⅲ. 1. 1. 3	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30分に1回以上は行うこと。また、異常検知時は、監視結果を利用者に60分以内に通知すること。	推奨	
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、社内規定に基づき管理責任者に報告すること。	推奨	

情報セキュリティ対策要件書

項番	対策項目	区分	備考
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脆弱性に関する情報（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ベンダーリリースから24時間以内に行うこと。	基本	
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3ヶ月に1回以上作成し、利用者等に報告すること。	推奨	
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発見後1時間以内に行うこと。	基本	
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99%以上と規定すること。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	
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、サービス提供期間後6ヶ月間は保存すること。	基本	
Ⅲ. 2. 1. 3	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）の保存期間について次のとおり明示すること。		
	a 利用者の利用状況の記録（ログ等）の保存期間を1ヶ月以上とすること。また、例外処理及び情報セキュリティ事象の記録（ログ等）の保存期間を1年以上とすること。	基本	
	b スタンバイ機による運転再開をコールドスタンバイで可能にすること。	基本	
Ⅲ. 2. 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・ストレージについて、次のとおり定期的に脆弱性診断を行い、その結果に基づいて対策を行うこと。		
	a 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）を1ヶ月に1回以上実施すること。	推奨	
	b 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）を1年に1回以上実施すること。	推奨	
	c アプリケーションの脆弱性の詳細診断（外部委託を含む）を1年に1回以上実施すること。	推奨	
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ベンダーリリースから24時間以内に講じること。	基本	
Ⅲ. 2. 2. 2	データベースに格納されたデータの暗号化を社内規定に基づき行うこと。	推奨	
Ⅲ. 2. 3 サービスデータの保護			
Ⅲ. 2. 3. 1	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次により実施すること。		
	a バックアップを1週間に1回以上実施すること。世代バックアップは2世代以上実施すること。	基本	
	b バックアップを1日に1回以上実施すること。世代バックアップは7世代以上実施すること。	推奨	

情報セキュリティ対策要件書

項番	対策項目	区分	備考
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、バックアップ実施の都度確認すること。	推奨	
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	利用方法及び管理者（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次により行うこと。また、運用管理規定を作成し、ID・パスワードを用いる場合は、その運用管理方法及びパスワードの有効期限を規定に含めること。		
	a 利用者のアクセス認証方法は、ICカード又はID・パスワードとする。	基本	
	b 前項に記載した方法及び生体認証等による多様化認証を行っている。	推奨	
	c 情報システム管理者及びネットワーク管理者等のアクセス認証方法は、デジタル証明書による認証、生体認証又はICカードとする。	基本	
	d 前項に記載した方法等により多様化認証を行っている。	推奨	
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又は遮断する措置（IDS／IPSの導入等）を講じ、シグニチャ（パターンファイル）の更新間隔を3週間に1回以上とすること。	推奨	
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IP暗号通信（VPN（IPsec）等）又はHTTP暗号通信（SSL（TLS）等）とすること。	推奨	
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、通信容量とトラフィック変動が重要）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、社内規定に基づき管理責任者に通報すること。	推奨	
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	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次により講じること。		
	a 非常用無停電電源（UPS等）による電力供給時間を10分とすること。	基本	
	b 複数給電を実施すること。		
	c 非常用発電機を設置すること。		
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	

情報セキュリティ対策要件書

項番	対策項目	区分	備考
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	サーバー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として、汚損対策消火設備（ガス系消火設備等）を備えること。	推奨	
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ールームには、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マニュアルを作成し対策を講じること。	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マニュアルを作成し対策を講じること。	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、2年以上保存すること。	基本	
Ⅲ. 4. 4. 2	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次により監視を行うこと。また、監視カメラの映像を次により保存すること。		
	a 監視カメラの稼働時間を365日24時間とすること。	推奨	
	b 監視映像保存期間を1ヶ月以上とすること。	推奨	
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	
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365日24時間常駐させること。	推奨	
Ⅲ. 4. 4. 6	サーバー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（真正性）確保を行うため、原本性確認レベルを署名及び印刷データ電子化・管理とすること。	推奨	
Ⅲ. 5. 1. 2	個人情報に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	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。技術的脆弱性に関する情報（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、次によりパッチによる更新を行うこと。		
	a パターンファイルの更新間隔をベンダーリリースから24時間以内とすること。	基本	
	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をベンダーリリースから24時間以内とすること。	基本	
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	