Annex2　組織・運用編 対策項目一覧表

※『実施チェック欄』をクリックすると、自動的 にチェックが記入されます。
(Adobe Acrobat(R)、 Adobe Reader(R)等を使用する場合)

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	