Annex 3　物理的・技術的対策編　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)

				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	
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　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、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。 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	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								