ASP・SaaSにおける情報セキュリティ対策ガイドライン　物理的・技術的対策編(たたき台)

資料3-6-2

[物理的・技術的対策編の読み方]

物理的・技術的対策編においては、手順1から3に従って、各事業者が適用する具体的対策を決定する。

1.用語の定義

【パターン】
ASP・SaaS事業者のサービス種別において取り扱われている情報資産について、機密性（confidentiality）及び完全性（integrity）に基づいて適用すべきセキュリティ対策の設定を12種類作成（現段階の数で、今後集約される予定）したものであり、機密性・完全性・可用性の要求レベルの組み合わせによってどれか1つを適用する。

【基本】
物理的・技術的対策編においてASP・SaaS事業者が実施すべき基本的なセキュリティ対策

【推奨】
物理的・技術的対策編においてASP・SaaS事業者がユーザ要求等によって、より高いセキュリティレベルを要求される際、追加的に適用されるセキュリティ対策

2.具体的対策（物理的・技術的対策）選定の手順

2-1セキュリティ対策のパターン判定

【手順1】 自社が提供するASP・SaaSサービスについて機密性、完全性及び可用性に関する要求レベルを「サービス種別の分類結果とセキュリティ対策パターン対応表（別添1）」にあてはめ、セキュリティ対策のパターンを特定する。

2-2セキュリティ対策、基準値の決定

【手順2】 「ASP・SaaSにおける情報セキュリティ対策ガイドラインの物理的・技術的対策編」の「適用するセキュリティ対策のパターン」欄から該当する（手順1によって適用した）パターン（1～12）を1つ選択適用する。

3.対策の実施

【手順3】 「ASP・SaaSにおける情報セキュリティ対策ガイドラインの物理的・技術的対策編」の「基本・推奨区分」欄の「基本」に該当するセキュリティ対策及び基準値は全て適用する。また、「推奨」に該当するセキュリティ対策及び基準値は、ユーザ要求に基づき、各事業者の判断で適宜追加適用する。

ASP・SaaSにおける情報セキュリティ対策ガイドライン　物理的・技術的対策編（たたき台）

資料3-6-2

新項番号	項目名	セキュリティ対策	区分	機密性（C）	完全性（I）	可用性（A）	評価項目	基準値（パターン欄にある数字は、基準値の種類） 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	パターン7	パターン8	パターン9	パターン10	パターン11	パターン12
第1章 アプリケーション、基盤、ストレージ																			
1.1.1	ソフトウエアの提供	ソフトウエアの稼動監視を行うこと	基本			○	監視インターバル 監視時間 通知時間	1	2	3	1	2	3	1	2	3	1	2	3
1.1.2	ソフトウエアの提供	ソフトウエアの障害監視を行うこと	基本			○	死活監視	1	2	3	1	2	3	1	2	3	1	2	3
1.1.3	ソフトウエアの提供	ソフトウエアのサービス時間を規定すること	基本			○	インフラ保守時間 稼働率	1	2	3	1	2	3	1	2	3	1	2	3
1.1.4	ソフトウエアの提供	システムの時刻同期の方法を規定すること	基本		○	○													
1.1.5	ソフトウエアの提供	新しいシステムを導入する際には試験を実施すること	基本		○	○													
1.1.6	ソフトウエアの提供	ウイルス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	1	2	3	4	5	6	7	8	9	10	11	12
1.1.7	ソフトウエアの提供	ネットワークを適切に管理し、制御すること	基本	○		○													
1.1.8	ソフトウエアの提供	利用者の活動、例外処理及びセキュリティ事象の記録をとること	基本		○	○													
1.1.9	ソフトウエアの提供	IDやパスワードの運用管理方法を規定すること	基本	○															
1.1.10	ソフトウエアの提供	技術的ぜい弱性に関する情報を定期的に収集すること	基本	○	○	○													
1.1.11	ソフトウエアの提供	情報セキュリティに関する事故や障害発生時の体制を整備すること	基本			○	事故や障害の公表のタイミング	1	2	3	1	2	3	1	2	3	1	2	3
1.1.12	ソフトウエアの提供	個人情報は関連する法令に基づいて取り扱うこと	基本	○	○		個人情報を収集する際の利用目的の明示	1	1	1	2	2	2	3	3	3	4	4	4
1.1.x	ソフトウエアの提供	ソフトウエアに対し一定間隔でパフォーマンス監視を行うこと	推奨			○	・監視インターバル ・監視時間 ・通知時間	1	2	3	1	2	3	1	2	3	1	2	3
1.2.1	バックアップ／リストア	情報やシステム構成の定期的なバックアップを実施すること	基本		○	○	・実施インターバル ・世代バックアップ	1	2	3	4	5	6	1	2	3	4	5	6
1.2.2	バックアップ／リストア	バックアップが正常に行われているか定期的に確認すること	基本		○	○	・実施インターバル	1	2	3	4	5	6	1	2	3	4	5	6
1.3.1	機器の提供	機器の稼動監視を行うこと	基本			○	監視インターバル 監視時間 通知時間	1	2	3	1	2	3	1	2	3	1	2	3
1.3.2	機器の提供	機器の障害監視を行うこと	基本			○	死活監視	1	2	3	1	2	3	1	2	3	1	2	3
1.3.3	機器の提供	機器のサービス時間を規定すること	基本			○	インフラ保守時間 稼働率	1	2	3	1	2	3	1	2	3	1	2	3
1.3.4	機器の提供	システムの時刻同期の方法を規定すること	基本		○														
1.3.5	機器の提供	新しいシステムを導入する際には試験を実施すること	基本		○	○													
1.3.6	機器の提供	情報セキュリティに関する事故や障害発生時の体制を整備すること	基本			○	事故や障害の公表のタイミング	1	2	3	1	2	3	1	2	3	1	2	3

【凡例】
○:選択

ASP・SaaSにおける情報セキュリティ対策ガイドライン　物理的・技術的対策編（たたき台）

新項番号	項目名	セキュリティ対策	区分	機密性（C）	完全性（I）	可用性（A）	評価項目	基準値（パターン欄にある数字は、基準値の種類） 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	パターン7	パターン8	パターン9	パターン10	パターン11	パターン12
1.3.x	機器の提供	パフォーマンス要件、稼動要件に合致する、システム機器を選択し、構成すること	推奨			○													
1.3.x	機器の提供	サービス対象機器に対し一定間隔でパフォーマンス監視を行うこと	推奨			○	・監視インターバル ・監視時間 ・通知時間	1	2	3	1	2	3	1	2	3	1	2	3
1.4.1	オペレーションサービス	サービス対象機器の稼動監視を行うこと	基本			○													
1.4.2	オペレーションサービス	運用監視手順を策定すること	基本			○													
1.4.3	オペレーションサービス	契約終了時の資産返却等の責任を明確に定めること	基本	○															
1.5.1	バックアップ／リストア	対象機器のストレージエリアの定期的なバックアップを実施すること	基本		○	○													
1.5.2	バックアップ／リストア	バックアップが正常に行われているか定期的に確認すること	基本		○	○													
1.6.1	サーバセキュリティ	OS、ミドルウェアのセキュリティパッチの管理を行うこと	基本	○			パッチの更新間隔	1	1	1	1	1	1	2	2	2	2	2	2
1.6.2	サーバセキュリティ	サーバ上のデータ管理を実施すること	基本	○	○														
1.6.3	サーバセキュリティ	サーバのログを収集し、管理すること	基本	○	○		保存期間	1	1	1	2	2	2	3	3	3	4	4	4
1.6.4	サーバセキュリティ	タイムスタンプ機能を備えること	基本		○														
1.7.x	運用管理	稼働状況の監視やパフォーマンス監視の結果を評価すること	推奨			○	報告タイミング	1	2	3	1	2	3	1	2	3	1	2	3
第2章 ネットワーク																			
2.1.1	アクセス制御	アクセス制御方針を策定すること	基本	○															
2.1.x	アクセス制御	特権の割当及び使用を制限すること	推奨	○															
2.2.1	ネットワークセキュリティ	ファイアウォールにより通過パケットを確認すること	基本	○															
2.2.2	ネットワークセキュリティ	不正侵入検知システムにより通過パケットのパターンを解析し、不正とみなしたパケットの報告を行うこと	基本	○			シグニチャー(パターンファイル)の更新間隔	1	1	1	1	1	1	2	2	2	2	2	2
2.2.3	ネットワークセキュリティ	リバースプロキシーを用いて外部からの攻撃に対して情報資産を防御すること	基本	○															
2.2.4	ネットワークセキュリティ	ネットワークセキュリティ機器の障害監視を行うこと	基本			○	死活監視	1	2	3	1	2	3	1	2	3	1	2	3
2.3.1	メールセキュリティ	メールの添付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	1	2	3	4	5	6	7	8	9	10	11	12
2.3.x	メールセキュリティ	電子メールの利用に関する対策を講じること	基本	○	○	○													
2.4.1	Webセキュリティ	ダウンロードされる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	1	2	3	4	5	6	7	8	9	10	11	12

【凡例】
○:選択

ASP・SaaSにおける情報セキュリティ対策ガイドライン　物理的・技術的対策編（たたき台）

新項番号	項目名	セキュリティ対策	区分	機密性（C）	完全性（I）	可用性（A）	評価項目	基準値（パターン欄にある数字は、基準値の種類） 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	パターン7	パターン8	パターン9	パターン10	パターン11	パターン12
2.4.2	Webセキュリティ	認証基盤を通じた厳密な個人認証を行うこと	基本	○			認証方法	1	1	1	1	1	1	2	2	2	2	2	2
2.4.3	Webセキュリティ	非権限者による不正なサーバへの侵入に対する検知を実施すること	基本	○			シグニチャー(パターンファイル)の更新間隔	1	1	1	1	1	1	2	2	2	2	2	2
2.4.4	Webセキュリティ	データの暗号化を行うこと	基本	○	○														
2.5.1	サーバセキュリティ	ファイルアクセス時に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	1	2	3	4	5	6	7	8	9	10	11	12
2.5.2	サーバセキュリティ	本人が接続していることの認証を行うこと	基本	○			認証方法	1	1	1	1	1	1	2	2	2	2	2	2
2.5.3	サーバセキュリティ	非権限者による不正なサーバへの侵入に対する検知を実施すること	基本	○			シグニチャー(パターンファイル)の更新間隔	1	1	1	1	1	1	2	2	2	2	2	2
2.5.4	サーバセキュリティ	データの暗号化を行うこと	推奨	○	○														
2.6.1	ディレクトリサービス	データの暗号化を行うこと	推奨	○	○														
2.7.1	運用管理	不正侵入、ウイルス侵入など問題が起こった場合の連絡方法を定めること	基本			○	報告	1	2	3	1	2	3	1	2	3	1	2	3
2.7.2	ネットワーク接続	ネットワークサービスの一部を外部委託している場合には、そのセキュリティ管理策、サービスの定義、及び提供されるサービスレベルを明確にすること	基本			○													
2.7.x	ネットワーク接続	ネットワーク回線の保証帯域を明確にすること	推奨			○	帯域保証	1	2	3	1	2	3	1	2	3	1	2	3
2.7.3	ネットワーク接続	ネットワークを監視し、障害を通報すること	基本			○	通報時間	1	2	3	1	2	3	1	2	3	1	2	3
2.7.x	ネットワーク接続	保守用のポートの使用を制限すること	推奨	○															
2.7.x	ネットワーク接続	ネットワークの領域分割を行うこと	推奨	○															
第3章 建物、電源（空調等）																			
3.1.1	建築物	地震・水害に対する対策が行われていること	基本			○	免震構造 制震構造	1	2	3	1	2	3	1	2	3	1	2	3
3.1.2	建築物		基本			○	排水対策の完備等	1	2	3	1	2	3	1	2	3	1	2	3
3.1.3	建築物	ストレージ等の設置を考慮した荷重に耐え得る構造とすること	基本			○	最大床荷重	1	2	3	1	2	3	1	2	3	1	2	3
3.2.1	IT機器設置スペース	IT機器を設置するスペースには、塵や埃に対する対策が行われていること	基本			○	ウィスカ対策	1	2	3	1	2	3	1	2	3	1	2	3
3.2.2	IT機器設置スペース	法令に基づき避難経路を確保すること	基本			○		1	2	3	1	2	3	1	2	3	1	2	3
3.3.1	電源管理	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			○	電力供給時間	1	2	3	1	2	3	1	2	3	1	2	3

【凡例】
○：選択

ASP・SaaSにおける情報セキュリティ対策ガイドライン　物理的・技術的対策編（たたき台）

新項番号	項目名	セキュリティ対策	区分	機密性（C）	完全性（I）	可用性（A）	評価項目	基準値（パターン欄にある数字は、基準値の種類） 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	パターン7	パターン8	パターン9	パターン10	パターン11	パターン12
3.3.2	電源管理					○	受電方法	1	2	3	1	2	3	1	2	3	1	2	3
3.3.3	電源管理					○	別の給電ルート	1	2	3	1	2	3	1	2	3	1	2	3
3.3.4	電源管理					○	受電容量	1	2	3	1	2	3	1	2	3	1	2	3
3.3.5	電源管理					○	連続稼働時間	1	2	3	1	2	3	1	2	3	1	2	3
3.4.1	空調管理	設置されているIT機器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	基本			○	空調容量	1	2	3	1	2	3	1	2	3	1	2	3
3.4.2	空調管理					○	稼働時間	1	2	3	1	2	3	1	2	3	1	2	3
3.4.3	空調管理					○	ラック下吹き出し、上吸い込み型の空調	1	2	3	1	2	3	1	2	3	1	2	3
3.4.4	空調管理					○	予備空調	1	2	3	1	2	3	1	2	3	1	2	3
3.4.5	空調管理	空調機からIT機器設置スペースへの水漏れを防止するための措置を講じること	基本			○	漏水検知システム	1	2	3	1	2	3	1	2	3	1	2	3
3.5.1	消火設備	放水等の消火設備の使用に伴うサーバルームに設置されているIT機器の汚損に対する対策を講じていること	基本			○	消火設備	1	2	3	1	2	3	1	2	3	1	2	3
3.5.2	消火設備					○	消火設備	1	2	3	1	2	3	1	2	3	1	2	3
3.5.3	消火設備	火災検知・通報システムを備えること	基本			○	火災検知システム	1	2	3	1	2	3	1	2	3	1	2	3
3.6.1	避雷・静電気対策設備	建築物に雷が直撃した場合を想定した対策を講じること	基本			○	直撃雷対策	1	2	3	1	2	3	1	2	3	1	2	3
3.6.2	避雷・静電気対策設備	建築物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	基本			○	最大対応電圧	1	2	3	1	2	3	1	2	3	1	2	3
3.6.3	避雷・静電気対策設備	設置されているIT機器について作業に伴う静電気対策を講じること	基本			○													
3.7.1	建築物のセキュリティ	IT機器や情報処理施設を保護するための物理的セキュリティ境界を定めること	基本	○															
3.7.2	建築物のセキュリティ	重要なセキュリティ境界に対する入退室管理を実施すること	基本	○			入退室記録	1	1	1	1	1	1	2	2	2	2	2	2

【凡例】
○:選択

新項番号	項目名	セキュリティ対策	区分	機密性（C）	完全性（I）	可用性（A）	評価項目	基準値（パターン欄にある数字は、基準値の種類） 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	パターン7	パターン8	パターン9	パターン10	パターン11	パターン12
3.7.3	建築物のセキュリティ			○			監視カメラ	1	1	1	1	1	1	2	2	2	2	2	2
3.7.4	建築物のセキュリティ			○			個人認証システム	1	1	1	1	1	1	2	2	2	2	2	2
3.7.5	建築物のセキュリティ			○			委託事業者の氏名管理	1	1	1	1	1	1	2	2	2	2	2	2
3.7.6	建築物のセキュリティ			○			サーバールーム入退館・入退室管理手順書	1	1	1	1	1	1	2	2	2	2	2	2
3.7.7	建築物のセキュリティ					○	入館可能時間	1	2	3	1	2	3	1	2	3	1	2	3
3.7.8	建築物のセキュリティ			○			監視カメラ稼働時間	1	1	1	1	1	1	2	2	2	2	2	2
3.7.9	建築物のセキュリティ			○			監視映像保存期間	1	1	1	1	1	1	2	2	2	2	2	2
3.7.10	建築物のセキュリティ			○			監視範囲	1	1	1	1	1	1	2	2	2	2	2	2
3.7.11	建築物のセキュリティ			○			破壊対策ドア	1	1	1	1	1	1	2	2	2	2	2	2
3.7.12	建築物のセキュリティ						常駐時間												
3.7.13	建築物のセキュリティ					○	仮眠・休憩室	1	2	3	1	2	3	1	2	3	1	2	3
3.7.14	建築物のセキュリティ					○	前室	1	2	3	1	2	3	1	2	3	1	2	3
3.7.x	建築物のセキュリティ	オフィス、部屋及び施設の物理的セキュリティを設計すること	推奨	○															
3.7.x	建築物のセキュリティ	通信ケーブルの傍受対策を講じること	推奨	○															
3.7.15	建築物のセキュリティ	監視記録は適切な期間保存すること	基本	○			入退室記録	1	1	1	1	1	1	2	2	2	2	2	2
3.7.16	建築物のセキュリティ	サーバルームやラックの鍵管理を行うこと	基本	○															
3.8.1	媒体のセキュリティ	磁気テープや光メディア等の媒体の保管管理を行うこと	基本	○	○	○	空調設備 ガス消火設備	1	2	3	4	5	6	7	8	9	10	11	12
3.8.2	媒体のセキュリティ			○			個人認証システム	1	1	1	1	1	1	2	2	2	2	2	2
3.8.3	媒体のセキュリティ			○	○	○	耐火金庫	1	2	3	4	5	6	7	8	9	10	11	12

【凡例】
○:選択

ASP・SaaSにおける情報セキュリティ対策ガイドライン　物理的・技術的対策編（たたき台）

新項番号	項目名	セキュリティ対策	区分	機密性（C）	完全性（I）	可用性（A）	評価項目	基準値（パターン欄にある数字は、基準値の種類） 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	パターン7	パターン8	パターン9	パターン10	パターン11	パターン12
3.8.4	媒体のセキュリティ			○	○		管理手順	1	1	1	2	2	2	3	3	3	4	4	4
3.8.x	媒体のセキュリティ	媒体は正式な手順に基づいて廃棄すること	基本	○	○														
第4章 サービスサポート																			
4.1.1	故障対応、業務問い合わせ、作業依頼	サービス対応の手段を明確にすること	基本			○													
4.1.2	故障対応、業務問い合わせ、作業依頼	サービス対応時間を明確にすること	基本			○	稼働率	1	2	3	1	2	3	1	2	3	1	2	3
4.1.3	故障対応、業務問い合わせ、作業依頼					○	放棄率	1	2	3	1	2	3	1	2	3	1	2	3
4.1.4	故障対応、業務問い合わせ、作業依頼					○	バックログ率	1	2	3	1	2	3	1	2	3	1	2	3
4.1.5	故障対応、業務問い合わせ、作業依頼					○	再コール比率	1	2	3	1	2	3	1	2	3	1	2	3
4.1.6	故障対応、業務問い合わせ、作業依頼					○	応答時間遵守率	1	2	3	1	2	3	1	2	3	1	2	3
4.1.7	故障対応、業務問い合わせ、作業依頼					○	基準時間完了率	1	2	3	1	2	3	1	2	3	1	2	3
4.1.8	故障対応、業務問い合わせ、作業依頼	サービスのサポート範囲を明確にすること	基本			○	障害復旧・保守応答時間	1	2	3	1	2	3	1	2	3	1	2	3
						○		1	2	3	1	2	3	1	2	3	1	2	3
4.2.1	運用管理	定期的に、セキュリティサービス運用状況についての報告を行うこと	基本			○	報告	1	2	3	1	2	3	1	2	3	1	2	3
第5章 その他																			
5.1.1	サーバセキュリティ	出力した紙書類の原本性確保を行うこと	基本		○														
5.2.1	端末セキュリティ	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	1	2	3	4	5	6	7	8	9	10	11	12
5.2.x	端末セキュリティ	モバイルコードに対する対策を行うこと	基本	○	○	○		1	2	3	4	5	6	7	8	9	10	11	12
5.2.2	端末セキュリティ	本人が接続していることの認証を行うこと	基本	○			認証方法	1	1	1	1	1	1	2	2	2	2	2	2
5.2.3	端末セキュリティ	データの暗号化を行うこと	基本	○	○														
5.2.x	端末セキュリティ	OSにログオンする際には、IDとパスワード用いてログインを行うこと	基本	○															

【凡例】
○：選択

ASP・SaaSにおける情報セキュリティ対策ガイドライン　物理的・技術的対策編（たたき台）

新項番号	項目名	セキュリティ対策	区分	機密性（C）	完全性（I）	可用性（A）	評価項目	基準値（パターン欄にある数字は、基準値の種類）											
								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	パターン7	パターン8	パターン9	パターン10	パターン11	パターン12
5.3.1	運用管理	運用管理方法を明確にすること	基本			○													
5.3.2	運用管理	運用管理方法を定期的に見直しをすること	基本			○	見直し期間	1	2	3	1	2	3	1	2	3	1	2	3
5.3.3	運用管理	新規にシステムを導入する場合や既存の情報システムを改善する場合には要求事項を仕様化すること	基本		○	○													
5.3.4	運用管理	情報システムの構成管理及び変更管理を行うこと	基本			○													
5.3.x	運用管理	OSやパッケージソフトウェアの変更管理を行うこと	推奨			○													
5.3.5	運用管理	業務用情報システムにおいて相互連携を行う場合には、個別方針と手順を策定すること	基本	○	○	○													
5.3.x	運用管理	リモート保守やテレワーキングによる作業については、正式な手順に基づくこと	基本	○															
5.3.x	運用管理	相互牽制の観点から職務や施設の分離を行うこと	推奨	○															
5.3.x	運用管理	システム試験データ（本番データ）は保護し、管理すること	推奨	○	○														
5.3.x	運用管理	プログラムソースコードへのアクセスを制限すること	推奨	○	○														
5.3.x	運用管理	外部委託したソフトウェア開発を監視し、監督すること	推奨	○															
5.3.x	運用管理	公開システムの認可されていない変更や改ざんを防止し、保護すること	推奨		○														
5.3.x	運用管理	入力データの妥当性確認のしくみを実装すること	推奨		○														
5.4.1	監査	発注者が実施する監査に対しては、SLAの遵守状況を提出すること	基本			○													
5.4.2	監査	システム監査ツールの不正使用を防止すること	基本	○	○														
5.5.x	事業継続計画	重要な業務プロセスの最大停止許容時間（MTO）を明確にし、事業継続計画を策定すること	推奨			○													
5.5.x	事業継続計画	策定した事業継続計画は、組織の全部門にわたって整合性をとること	推奨			○													
5.5.x	事業継続計画	策定した事業継続計画を定期的に試験すること	推奨			○													

【凡例】
○：選択

ASP・SaaSにおける情報セキュリティ対策ガイドライン　物理的・技術的対策編（たたき台）

新項番号	項目名	セキュリティ対策	区分	機密性（C）	完全性（I）	可用性（A）	評価項目	基準値（パターン欄にある数字は、基準値の種類）											
								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	パターン7	パターン8	パターン9	パターン10	パターン11	パターン12
5.6.x	コンプライアンス	法的な措置に備えて関連する法域で定めている措置に従って証拠（ログ等）を収集すること	基本	○	○														
5.6.x	コンプライアンス	ログ機能やログ情報は改ざんや認可されていないアクセスから保護すること	推奨	○	○														
5.6.x	コンプライアンス	個人情報保護法および関連する法令・ガイドラインを遵守すること。	基本	○	○														
5.6.x	コンプライアンス	情報セキュリティに関連する（個人情報保護法以外の）法令、業界規制を特定し、順守すること	基本	○															

【凡例】
○:選択