資料3-6-1

ASP・SaaSにおける情報セキュリティ対策ガイドライン　組織・運用編
（たたき台）

ASP・SaaSにおける情報セキュリティ対策ガイドライン（組織・運用編）の現バージョンの位置づけについて

　組織・運用編は、まだISO/IEC 27001：2005及びISO/IEC 20000-1：2005を参照してASP・SaaSにおける情報セキュリティ対策ガイドラインに必要な項目を選定した段階である。

　引き続き、ASP・SaaSサービス内容等を踏まえた具体的な対策の例示、用語の修正等を行うこととしている。

資料3-6-1

章	内容	ISO/IEC 27001：2005の該当部分	ISO/IEC 20000-1：2005の該当部分
0.1	情報セキュリティガイドラインの目的 このガイドラインは、ASP・SaaS事業者においてASP・SaaS向け情報セキュリティガイドライン（以下、ガイドラインという。）に関する体制を確立、導入、運用、監視、見直し、維持及び改善するためのモデルを提供することを目的として作成されたものである。	0.序文 0.1 一般	序文
0.2	ガイドラインで導入するプロセスアプローチ このガイドラインでは、組織において情報セキュリティを確立、導入、運用、監視、見直し、維持及び改善する際に、プロセスアプローチを採用している。 組織は、有効に機能するために、多くの活動を明確にし、運営管理する必要がある。 このガイドラインに示す情報セキュリティマネジメントのためのプロセスアプローチによって、その利用者は次の事項の重要性を明確に認識できるようになる。 a) 組織の情報セキュリティ要求事項を理解し、情報セキュリティ基本方針及び目的を確立する必要性を理解すること。 b) 組織における全般的な事業上のリスクを考慮に入れて、情報セキュリティのリスクマネジメントを実施するために、対策を導入し、運用すること。 c) ガイドラインの運用状況を監視し、見直すこと。 d) 継続的に改善すること。 このガイドラインでは、「Plan-Do-Check-Act（計画-実施-点検-処置）」（PDCA）モデルが採用されており、このモデルは、あらゆるガイドラインの運用プロセスの構築に適用される。 図1-ガイドラインの運用プロセスに適用されるPDCAモデル 図表する Plan-計画（ガイドライン運用体制導入）　組織の全般的な基本方針及び目的に沿った結果を出すための、リスクマネジメント及び情報セキュリティの改善に関連する情報セキュリティ基本方針、目的、プロセス及び手順を確立する。 Do-実施（ガイドライン運用体制導入及び運用）　そのガイドラインの運用に関する基本方針、対策、プロセス及び手順を導入して運用する。 Check-点検（ガイドライン運用体制に関する監視及び見直し）ガイドラインの運用に関する基本方針、目的及び実際の経験に照らしてプロセスの実施状況を評価し、その結果を見直しのために経営陣に報告する。 Action-処置（ガイドライン運用体制の維持及び改善）ガイドラインの運用に関して継続的な改善を達成するために、ガイドラインの運用に関する内部監査及びマネジメントレビューの結果や、その他関連情報に基づいて是正処置及び予防処置を講ずる。	0.序文 0.2 プロセスアプローチ	序文
1.1	一般 このガイドラインは、ASP・SaaS事業者を対象としたものである。このガイドラインは、組織の事業上のリスク全般に対して、文書化されたガイドライン運用体制確立、導入、運用、監視、見直し、維持及び改善に関する対策法を提供するものである。またこのガイドラインは、個々の組織又は組織の一部が、その必要性に応じて情報セキュリティ対策を適切に実施できるように基本セキュリティ対策・評価項目・基準値と推奨セキュリティ対策を提供している。	1.適用範囲 1.1 一般	1.適用範囲

章	内容	ISO/IEC 27001：2005の該当部分	ISO/IEC 20000-1：2005の該当部分
第2章（1）	このガイドラインで用いる主な用語及び定義は、以下による。 2．1 資産(asset) 組織にとって価値をもつもの。 2．2 可用性(availability) 認可されたエンティティ（団体等）が要求したときに、アクセス及び使用が可能である特性。 2．3 機密性(confidentiality) 認可されていない個人、エンティティ（団体等）又はプロセスに対して、情報を使用不可又は非公開にする特性。 2．4 情報セキュリティ(information security) 情報の機密性、完全性及び可用性を維持すること。さらに、真正性、責任追跡性、否認防止及び信頼性のような特性を維持することを含めてもよい。 2．5 情報セキュリティ事象(information security event) システム、サービス又はネットワークにおける特定の状態の発生。特定の状態とは、情報セキュリティ基本方針への違反若しくは対策の不具合の可能性、又はセキュリティに関連するかもしれない未知の状況を示していることをいう。 2．6 情報セキュリティインシデント(information security incident) 望まない又は予期しない単独又は一連の情報セキュリティ事象であって、事業運営を危うくする確立、及び情報セキュリティを脅かす確立が高いもの。 2．7 情報セキュリティマネジメントシステム(information security management system) マネジメントシステム全体の中で、事業リスクに対する取り組み方に基づいて、情報セキュリティの確立、導入、運用、監視、見直し、維持及び改善を担う部分。 参考　マネジメントシステムには、組織の構造、方針、計画作成活動、責任、実践、手順、プロセス及び経営資源が含まれる。 2．8 完全性(integrity) 資産の正確さ及び完全さを保護する特性。 2．9 リスクアセスメント(risk assessment) リスク分析からリスク評価までのすべてのプロセス。 2．10 リスクマネジメント(risk management) リスクに関して組織を指揮し管理するために調整された活動。 2．11 リスク対応(risk treatment) リスクを変更させるための方策を、選択及び実施するプロセス。	3.用語及び定義	2.用語及び定義
第2章（2）	2．12 サービスデスク 全体のサポート業務の内、多くの割合を実施する、顧客と直接接するサポートグループ 2．13 サービスレベルアグリーメント（SLA） サービス及び合意されたサービスレベルを文書化した、サービスプロバイダと顧客間の書面による合意。物理的・技術的対策編では、SLAに関する評価項目と基準値をレベル別に設定している。 2．14 サービスマネジメント 事業上の要求事項を満たすための、サービスのマネジメント。 2．15 サービスプロバイダ 本ガイドラインを適用し、顧客との間でSLAを締結する事業者。		

章	内容	ISO/IEC 27001：2005の 該当部分	ISO/IEC 20000-1：2005の 該当部分
3.1	文書・記録に関する基本原則 文書には、経営陣の決定に関する記録を含めること。 ガイドラインの運用に関する文書には、次の事項を含めること。 a) 情報セキュリティ及びサービスマネジメント基本方針及び目的の表明。 b) ガイドラインの適用範囲。 c) ガイドラインの運用を支える手順及びセキュリティ対策、評価項目、基準値。 d) リスク対応計画。 e) その他、組織において必要と判断したもの。 ＜文書の例＞ ① 基本方針：情報セキュリティ基本方針、サービスマネジメント基本方針 ② 適用範囲宣言書 ③ 規程書：情報セキュリティ規程、サービスマネジメント規程 （上記文書には、本ガイドラインより選択したセキュリティ対策、評価項目、基準値の一覧が含まれる。） ④ 手順書：情報セキュリティ実施手順、サービスマネジメント実施手順 ⑤ 各種計画書：リスク対応計画、サービス提供計画、監査計画、教育計画 ⑥　その他：教育・訓練用テキスト、各種申請フォーマット、各種報告書	4.情報セキュリティマネジメントシステム 4.3 文書化に関する要求事項 4.3.1 一般	3.マネジメントシステム要求事項 3.2文書化に関する要求事項
3.2	文書管理 ガイドラインの運用において必要とされる文書は、管理し、必要に応じて共有すること （共有しない方が適切な場合もありうる）。	4.3.2 文書管理	同上
3.3	記録の管理 記録は、ガイドラインの運用が適切に行われている証拠を示すために、作成され、維持すること。	4.3.3 記録の管理	同上
4.1	情報セキュリティ運用計画の策定（Plan） 当該適用範囲からの除外の詳細及びその理由も含め、事業、組織、その所在地、情報資産及び技術の各特徴の観点から、ガイドラインの適用範囲及び境界を定義する。 事業、組織、その所在地、情報資産及び技術の各特徴の観点から、次の事項を満たすガイドラインの運用に関する情報セキュリティ基本方針を策定する。 a) 情報セキュリティに関する全般的な方向性及び行動指針を確立する。 b) 事業上の要求事項及び法的又は規制要求事項、並びに契約上のセキュリティ義務を考慮する。 c) ガイドライン運用体制確立及び維持が行われるように、組織の戦略的なリスクマネジメントの観点から整合をとる。 d) 経営陣による承認を得る。 提供しているASP・SaaS事業で取り扱っているサービス種別を特定し、どの対策パターン・基準値のレベルに属するか特定する。 各パターン・基準に対応したセキュリティ対策及び関連する基準値をガイドラインの物理的・技術的対策編から選択する。 選択したセキュリティ対策・基準値は、経営陣の許可を得てから適用する。	4.2.1 ISMSの確立	－

章	内容	ISO/IEC 27001：2005の該当部分	ISO/IEC 20000-1：2005の該当部分
4.2	サービスマネジメント計画の策定（Plan） サービスマネジメントを計画すること。この計画では、少なくとも次を定義すること。 a) サービスプロバイダの、サービスマネジメントの適用範囲。 b) サービスマネジメントによって達成すべき目標及び要求事項 c) 実行すべきプロセス d) 上級責任オーナ、プロセスオーナ及びサプライヤの管理を含む、管理の役割及び責任についての枠組み。 e) サービスマネジメントプロセス間のインターフェースと活動を調整する方法。 f) 定義した目標の達成に対する課題及びリスクを特定し、アセスメントを実施し、管理するために採用すべきアプローチ。 g) サービスを生み出し又は修正するプロジェクトに対するインターフェースをとるためのアプローチ。 h) 定義した目標を達成するために必要なリソース、設備及び予算。 i) サービス品質を管理、監査及び改善する方法。 計画のレビュー、認可、伝達、実施及び維持について、経営陣の明確な方向付け責任を定めること。	－	4.サービスマネジメントの計画及び導入 4.1サービスマネジメントの計画（Plan）
4.3	情報セキュリティ運用体制の導入及び運用（Do） 組織は次の事項を実施すること。 a) 情報セキュリティについてのリスクを管理するための、経営陣の適切な活動、資源、責任及び優先順位が明確にされたリスク対応計画を策定する。 b) 識別された管理目的を達成するためにリスク対応計画を実施する。これには、必要な資金の拠出を考慮し、役割及び責任を割り当てることを含む。 c) 適用対象となったガイドラインのセキュリティ対策（組織・運用編及び物理的・技術的対策編）を実施する。 d) 教育・訓練及び認識させるためのプログラムを実施する。 e)ガイドラインの運用を管理する。 f) ガイドラインの運用に関する経営資源を管理する。 g) セキュリティ事象を迅速に検出し、セキュリティインシデントに対して迅速な対応を行うことのできる手順及びその他の対策を実施する。	4.2.2 ISMSの導入及び運用	－
4.4	サービスマネジメントの導入及びサービスの提供（Do） 組織は、次のことを実施すること。 サービスプロバイダは、サービスを管理して提供するために、次の事項を含むサービスマネジメントの計画を実施すること。 a) 資金及び予算の割当て b) 役割及び責任の割当て c) 各プロセス又は一連のプロセスのための方針、計画、手順及び定義の文書化及び維持。 d) サービスに対するリスクの特定及び管理 e) チームの管理(例えば、適切なスタッフの採用及び育成、並びにスタッフの継続性の管理)。 f) 設備及び予算の管理 g) サービスデスク及び運用を含む、チームの管理。	－	4.2サービスマネジメントの導入及びサービスの提供（Do）

章	内容	ISO/IEC 27001：2005の該当部分	ISO/IEC 20000-1：2005の該当部分
4.5	情報セキュリティ運用体制及びサービスマネジメントの監視及び見直し（Check） 組織は、次のことを実施すること。 a) 次の事項を行うため、監視及び見直しのための手順及び他の対策を実施する。 1) 処理結果から誤りを速やかに検出する。 2) セキュリティ上の違反行為及びインシデントは未遂であっても、迅速に識別する。 3) 人又は情報技術によって導入されたセキュリティ活動が意図した通りに実施されているかどうかを、経営陣や管理者が判断できるようにする。 4) 指標を利用することにより、セキュリティ事象の検出を容易にし、その結果セキュリティインシデントを防止する。 b) あらかじめ定められた間隔で、ガイドラインの運用に関する内部監査を実施する。 c) 適用範囲が引き続き適切であり、ガイドラインの運用プロセスにおける改善策が明確にされていることを確実にするために、定期的にガイドラインの運用に関するマネジメントレビューを実施する。 d) 監視及び見直しの活動で検出された事項を踏まえて、セキュリティ計画を更新する。 e) ガイドラインの運用に影響を与える可能性のある活動及び事象を記録する。	ISMSの監視及び見直し	4.3監視、測定及びレビュー（Check）
4.6	情報セキュリティ運用体制及びサービスマネジメントの継続的改善（Act） 組織は、定期的に次の事項を実施すること。 a) 識別されたガイドラインの運用に関する改善策を実施すること。 b) 適切な是正処置及び予防処置を実施する。 c) 利害関係者全てに対し、状況に応じた詳細さで講じた処置及び改善を伝達し、該当する場合は、今後の進め方について合意を得る。 d) 改善が、その意図した目的を確実に達成するようにする。	ISMSの維持及び改善	4.4継続的改善
5.1	経営陣のコミットメント 経営陣は、ガイドライン運用体制の確立、導入、運用、監視、見直し、維持及び改善に対するコミットメントの証拠を、次の事項によって示すこと。 a) ガイドラインの運用に関する基本方針を確立する。 b) ガイドラインの運用の目的が設定され、計画が策定されることを確実にする。 c) 情報セキュリティに対する役割及び責任を定める。 d) 情報セキュリティ目的を達成することの重要性及び情報セキュリティ基本方針に適合することの重要性、当該組織の法的責任、並びに継続的改善の必要性を組織内に周知する。 e) ガイドライン運用体制の確立、導入、運用、監視、見直し、維持、及び改善に十分な経営資源を提供する。 f) ガイドラインの運用に関する内部監査が実施されることを確実にする。 g) ガイドラインの運用に関するマネジメントレビューを実施する。	5.経営陣の責任 5.1経営陣のコミットメント	3.マネジメントシステム要求事項 3.1経営陣の責任
5.2	経営資源の提供 組織は、次の事項を実施するために必要な経営資源を決定し、提供すること。 a) ガイドライン運用体制を確立、導入、運用、監視、見直し、維持及び改善する。 b) 情報セキュリティの手順が事業上の要求事項を満たすものであることを確実にする。 c) 法的及び規制要求事項と契約上の情報セキュリティに関する義務を識別し、適切に対処する。 d) 実施される全ての対策を的確に適用することにより、十分な情報セキュリティを維持する。 e) 必要な場合には見直しを行い、その結果に対して適切に対応する。	5.2経営資源の運用管理 5.2.1経営資源の提供	同上

章	内容	ISO/IEC 27001：2005の該当部分	ISO/IEC 20000-1：2005の該当部分
6.1	教育・訓練、意識向上及び力量 組織は、ガイドラインの運用において、明確にされた責任を割り当てられた要員全てが要求される業務を実施する力量をもつことを、次の事項を実施することによって確実にすること。 a) ガイドラインの運用に影響がある業務に従事する要員を採用する際は、必ず秘密保持契約を締結するとともに、ガイドラインを含め要因が遵守すべき事項について教育する。 b) セキュリティ違反を犯した要員に対する正式な懲戒手続きを備え、十分に要員に対して趣旨・内容を説明すること。 c) 要員の雇用（契約期間の場合もある）を終了する場合、組織から貸与された資産を全て返却させること。 d) 要員の雇用（契約期間の場合もある）を終了する場合、ガイドラインの運用に関連する情報処理設備に対するアクセス権をなるべく早い段階で削除もしくは変更すること。	5.2.2教育・訓練・認識及び力量	3.3力量、認識及び教育・訓練
7.1	内部監査・自主点検 　組織は、当該ガイドラインの運用におけるプロセス、手順が次の事項を満たしているか否かを明確にするために、予め定められた間隔でガイドラインの運用に関する内部監査もしくは自主点検を実施すること。 a) ガイドラインの組織・運用編に適合していること。 b) 関連する法令又は規制に適合していること。 c) 適用されたガイドラインの物理的・技術的対策編のセキュリティ対策が適切に実施されていること。	6.ISMSの内部監査	4.3監視、測定及びレビュー（Check）
8.1	一般 経営陣は、ガイドラインの運用が、引き続き適切で、妥当で、かつ、有効であることを確実にするために、予め定められた間隔の運用をレビューすること。	7.ISMSのマネジメントレビュー 7.1一般	同上
8.2	マネジメントレビューへのインプット マネジメントレビューへのインプットには次の事項を含めること。 a) ガイドラインの運用に関する監査及びレビューの結果。 b) 予防処置及び是正処置の状況。 c) 過去のマネジメントレビューの結果に対するフォローアップ d) 改善のための提案	7.2 マネジメントレビューへのインプット	同上
8.3	マネジメントレビューからのアウトプット マネジメントレビューからのアウトプットには、次の事項に関する決定及び処置を含めること。 a) リスク対応計画の更新。 b) ガイドラインの運用に影響を与える可能性のある内部又は外部の事象に対応するために必要に応じて加えられる、情報セキュリティを実現する手順及び対策の修正。それらの事象には、次の事項に対する変更が含まれる。 　1) 事業上の要求。 　2) 情報セキュリティ要求。 　3) 規制又は、法的要求。 　4) 契約上の義務。 c) 必要となる経営資源。	7.3マネジメントレビューからのアウトプット	同上

章	内容	ISO/IEC 27001：2005の該当部分	ISO/IEC 20000-1：2005の該当部分
9.1	一般 組織は、ガイドラインの基本方針及び目的、監査結果、監視した事象の分析、是正及び予防の処置、並びにマネジメントレビューを利用して、ガイドラインの有効性を継続的に改善しなければならない。	8.ISMSの改善 8.1継続的改善	4.4継続的改善（continual improvement）（Act）
9.2	是正処置 組織は、ガイドラインの運用における不適合の再発防止のため、必要に応じて処置（是正処置）を講ずること。	8.2是正処置	4.4.2改善のマネジメント
9.3	予防処置 組織は、ガイドラインの運用において不適合となる原因を除去する処置（予防処置）を決めること。	8.3予防処置	同上
10.1	新規サービス又はサービス変更の計画及び導入 新規サービス又はサービスの変更の提案は、サービスデリバリ及びサービスマネジメントから生じる可能性のある、コスト上、組織上、技術上、及び営業上のインパクトを考慮したものであること。 サービスのクローズを含む、新規サービス又はサービス変更の導入について計画し、正式な変更管理を通じて、これを認可すること。 この計画及び導入には、サービスデリバリ及びサービスマネジメントに必要な変更を行うための、適切な資金調達及びリソースを含めること。 この計画には、次を含めること。 a) 顧客及びサプライヤの行う活動を含む、新規サービス又はサービス変更の導入、運用及び維持についての役割及び責任。 b) 現行のサービスマネジメントの枠組み及びサービスに対する変更。 c) 該当関係者へのコミュニケーション d) 事業上のニーズの変化と整合した、新たな契約及び合意、又は契約及び合意の変更。 e) 人的資源及び人員採用の要求事項。 f) 技能及びトレーニングに関する要求事項（例えば、ユーザ及び技術サポート）。 g) 新規サービス又はサービス変更に関連して使用する、プロセス、指標（measures）、手法及びツール（例えば、キャパシティ管理、財務管理）。 h) 予算及び期間。 i) サービス受け入れ基準。 j) 測定可能なかたちで示された、新規サービス運用からの、期待される効果。 新規サービス又はサービス変更については、稼働環境に導入する前に、サービスプロバイダの承諾を得ること。 サービスプロバイダは、導入後に新規サービス又はサービス変更が、計画された結果をどの程度達成したかについて、報告すること。計画された結果と実際の結果を比較する、導入後のレビューについては、変更管理プロセスを通して行うこと。	－	5.新規サービス又はサービス変更の計画及び導入
11.1	サービスレベル管理 対応するサービスレベル目標値及び作業負荷の特性とあわせて提供されるサービスの全範囲について、関係者と合意し、記録すること。 提供されるサービスを1つ又は複数のサービスレベルアグリーメント（SLA）のなかで定義し、合意し、文書化すること。 SLAについては、支援的なサービスに関する合意、サプライヤとの契約及び対応する手順を合せて、すべての当該関係者と合意し、記録すること。 SLAを、変更管理プロセスのコントロール下におくこと。 SLAが常に最新の状態であり、有効であることを確実にするために、関係者による定期的なレビューによってSLAを維持すること。 最新情報及びトレンド情報を示すため、サービスレベルを目標値に照らして監視し、報告すること。不適合の理由については、報告し、レビューすること。また、このプロセスにおいて識別された、改善のための処置を、記録すること。この処置は、サービス改善のための計画へのインプットを提供するものであること。	－	6.サービスデリバリプロセス 6.1サービスレベル管理

章	内容	ISO/IEC 27001：2005の該当部分	ISO/IEC 20000-1：2005の該当部分
11.2	サービスの報告 各サービスレポートは、文書識別、目的、報告相手及びデータの出典の詳細を含む、明確な説明を記載していること。 特定された必要性及び顧客要求事項を満たすために、サービスレポートを作成すること。サービスの報告には、次を含めること。 a) サービスレベル目標値に対するパフォーマンス。 b) 不遵守及び課題（例えば、SLAに対するもの、セキュリティ違反など） c) 作業負荷の特性（例えば、使用量、リソースの稼働率など）。 d) 重大なイベント（例えば、重大なインシデント、変更）後の、パフォーマンスの報告。 e) トレンド情報。 f) 満足度の分析 管理上の決定及び是正処置では、サービスレポートの所見を考慮すること。また、この決定及び是正処置を、該当関係者に伝達すること。	－	6.2サービスの報告
11.3	サービス継続性及び可用性管理 可用性及びサービス継続性の要求事項を、事業計画、SLA及びリスクアセスメントに基づき特定すること。要求事項には、アクセス権、応答時間、システムコンポーネントの終端間の可用性を含めること。 通常の状態からのサービスの重大な中止にいたるまで、あらゆる状況において、合意されたとおりに要求事項を確実に満たすようにするために、可用性及びサービス継続性計画を策定し、少なくとも年1回レビューすること。こうした計画に、事業の要求する合意された変更を、確実に反映するようにするために、これらの計画を維持すること。 事業上の環境に対して重大な変更を行った場合は、必ず可用性及びサービス継続性計画を再テストすること。 変更管理プロセスでは、可用性及びサービス継続性の計画に対して行った、あらゆる変更のインパクトを評価すること。 可用性を測定し、記録すること。計画外の非可用性については調査し、適切な処置を講じること。 参考　可能な場合、起こり得る課題を予測し、予防処置を講じることが望ましい。 通常のオフィスの利用が妨げられた場合、サービス継続性計画、連絡先一覧、構成管理データベースが使用可能であること。サービス継続性計画には、業務の平常復帰についても含めること。 事業上のニーズに沿って、サービス継続性計画をテストすること。 すべての継続性テストを記録すること。また、テストの失敗については、処置計画を策定すること。	－	6.3サービスの継続性及び可用性管理
12.1	一般 関係プロセスでは、サプライヤ管理と事業関係管理という、2つの関連する側面を説明する。	－	7.関係プロセス

章	内容	ISO/IEC 27001：2005の該当部分	ISO/IEC 20000-1：2005の該当部分
12.2	事業関係管理 サービスプロバイダは、サービスの利害関係者と顧客を識別し、文書化すること。 サービスプロバイダ及び顧客は、サービスの適用範囲、SLA、（契約があれば）契約、又は事業上のニーズに対する変更すべてについて討議するために、少なくとも年1回、サービスレビューに参加すること。また、パフォーマンス、達成度、課題、処置計画について討議するため、合意された間隔で中間会議を開催すること。これらの会議内容は、文書化すること。 サービスにおける他の利害関係者を、この会議に招請してもよい。 契約があれば、その契約に対する変更、及びSLAに対する変更を、必要に応じて、この会議を受けて実施すること。この変更は、変更管理プロセスに従うこと。 サービスプロバイダは、事業上へのニーズへ対応に備えるために、こうしたニーズ及び重大な変更について認識していること。 また、苦情処理プロセスを備えていること。正式なサービスの苦情の定義について、顧客と合意すること。サービスプロバイダは、すべての正式なサービス苦情を記録し、調査し、これに対する処置を講じ、報告して、正式にクローズすること。通常の経路では苦情が解決しなかった場合、顧客がエスカレーションを使用できるようになっていること。 サービスプロバイダは、顧客満足及びすべての事業関係プロセス管理についての責任を持つ、一人又は複数の個人を指名しておくこと。顧客満足度の定期的な測定からのフィードバックを得て、このフィードバックに対して処置を講じるためのプロセスを定めていること。このプロセスにおいて識別された、改善のための処置については、記録し、サービス改善のための計画にインプットすること。	－	7.1事業関係管理
12.3	サプライヤ管理 参考1　この規格の適用範囲には、サプライヤの手配は含まない。 参考2　サービスプロバイダは、サプライヤを利用して、サービスの一部を提供してもよい。サプライヤ管理プロセスへの適合を実証する必要があるのは、サービスプロバイダである。一例として、下図に示すように、複雑な関係が存在する場合もある。 図3　図表する 図3 － サービスプロバイダ及びサプライヤ間の関係の例 サービスプロバイダは、サプライヤ管理プロセスを文書化しておくこと。また、サプライヤごとに担当の契約マネージャを一人指名すること。 サプライヤが提供する、要求事項、適用範囲、サービスのレベル及びコミュニケーションプロセスについては、SLA又は他の文書のなかで文書化し、全関係者の合意を得ること。 サプライヤとのSLAは、事業とのSLAと整合のとれたものであること。 各関係者の利用するプロセス間におインターフェースについては、文書化し、合意を得ること。 統括サプライヤと再契約先サプライヤとの間の、すべての役割及び関係を、明確に文書化すること。 統括サプライヤは、再契約先サプライヤが、契約上の要求事項を満たしていることを確実にするためのプロセスを実証できること。 事業上のニーズ及び契約上の義務が依然として満たされていることを確実にするために、契約又は正式な合意についての大規模なレビューを行うためのプロセスを少なくとも年1回実施すること。 契約があれば、その契約に対する変更、及びSLAに対する変更をこのレビューを受けて、必要に応じて実施するか、又はその他必要な場合に実施すること。変更はすべて、変更管理プロセスに従うこと。 また、契約上の紛争を処理するプロセスを、定めていること。 サービスの終了予定、サービスの早期終了、又は他の関係者へのサービスの再委託を扱うプロセスを、備えていること。 サービスレベル目標値に対するパフォーマンスを監視し、レビューすること。このプロセスにおいて識別された改善のための処置については、記録し、サービス改善のための計画にインプットすること。	－	7.3サプライヤ管理