資料3-5

ASP・SaaSにおける
情報セキュリティ対策ガイドライン
基本的考え方等

ASP・SaaSの情報セキュリティ対策に関する研究会
事務局

2007年10月17日

目次

ASP・SaaSにおける情報セキュリティ対策ガイドライン検討の背景

人口減少社会下の我が国経済を新たな成長のトレンドに乗せるためには、ICTを活用した生産性の向上が不可欠であり、経済財政諮問会議等においてASP・SaaS等の普及促進の必要性が指摘されたところである。しかしながら、ASP・SaaSが安全に利用できる環境が整備されないと、その普及促進が阻害される恐れがある。

成長力加速プログラム
（平成19年4月25日：経済財政諮問会議）

- 人口減少社会に直面
- 活力に満ちた経済を築くこと
  →我が国の喫緊の課題
- 戦後の経済システムからの脱却
  →社会変化に対応した新たなレジーム
  →生産性の向上、高い潜在力の発揮

1. 成長力底上げ戦略
2. ITによる生産性向上
   「・・・ASPやSaaSなど中小企業にとって使いやすい新たなサービスの普及促進のための共通基盤の整備等環境整備を促進する。」
3. 成長可能性拡大戦略

克服すべき課題等

- ASP・SaaS事業者及びその関係企業において、企業等の膨大な機密情報・顧客情報が集積されることになる。
- 一方、ASP・SaaSを安全に利用できる環境が整備されないと、利用者は情報漏えい、改竄等の危惧にさらされ、企業存続にさえ影響を及ぼしかねない。
- ASP・SaaSの普及促進にも影響し、ITによる生産性向上にも波及する恐れ

「ASP・SaaSの情報セキュリティ対策の底上げが不可欠である」との強い社会的要請

ASP・SaaSが安全に利用できる環境の整備

ASP・SaaSの情報セキュリティ対策の課題を認識し、「 ASP・SaaSにおける情報セキュリティ対策ガイドライン」の策定を推進する必要がある。

■ ASP・SaaSの情報セキュリティ対策の課題とは？

- 事業規模も多様である中、十分な対策が施されてきたか
- 或いはどの程度の対策を講じるべきか、不明瞭であったのではないか
- 利用者に対して必ずしも十分な説明、情報開示がなされていなかったのではないか

■ ASP・SaaSサービスの十分な安全・信頼性を確保するための情報セキュリティ対策の明確化が不可欠

■ 利用者が安心して選択できる判断基準を与えるための仕組みとしての利用も考慮。

ASP・SaaSにおける情報セキュリティ対策ガイドラインの必要性

現在、国際標準はASP・SaaSに特化したものではないことから、中小企業にとってハードルが高すぎる実状がある。また、総務省「公共ITにおけるアウトソーシングに関するガイドライン」は電子自治体の共同アウトソーシングに係る自治体側の要求事項を示したものであり、民間向けASP・SaaS事業者にそのまま適用できるものではないことから、ASP・SaaS事業者が自らの情報セキュリティ対策を適切に実施するための新しいガイドラインの策定が必要である。

国際標準 （事業者側の認証）

ISO/IEC 27001（ISMS認証基準）

・ASP・SaaSに特化していない
・中小企業にとってハードルが高すぎる

①ASP・SaaS事業者は中小企業が多く、既存標準の規格体系は「規模」が大きすぎる
②リスクアセスメント等の作業負担が大きく、またそれに要するコンサルティングフィーも高額
③①②が理由となって、中小事業者としては新しく情報セキュリティ対策に取り組む際のハードルが高いのが実状

★ASP・SaaSに即した優先度分けをし、分かり易く記述

ASP・SaaSにおけるガイドライン
（電子自治体に係る自治体側の要求事項）

総務省公共ITにおけるアウトソーシングに関するガイドライン

地方公共団体が共同アウトソーシングをする場合に特化している

★民間向けに展開可能な形にカスタマイズ

ユーザ目線の追加

相乗効果

ASP・SaaSにおける情報セキュリティ対策ガイドラインが必要

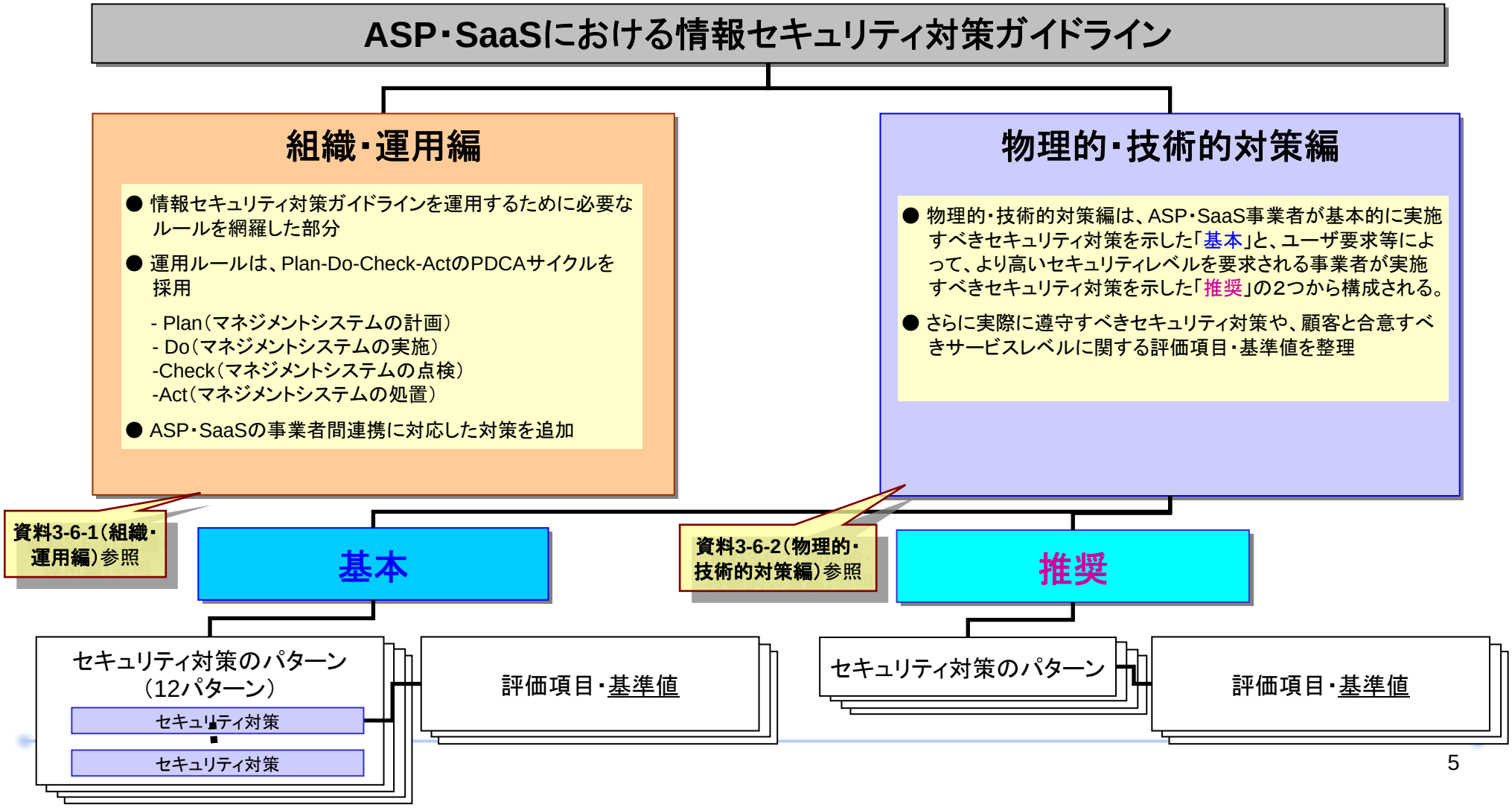
①電子自治体の要求事項に特化している
②民間向けASP・SaaS事業者が守るべきものとしてのガイドラインではない

※利用者（自治体）側の要求事項をまとめたもの

情報セキュリティ対策ガイドラインの構成

ガイドライン全体

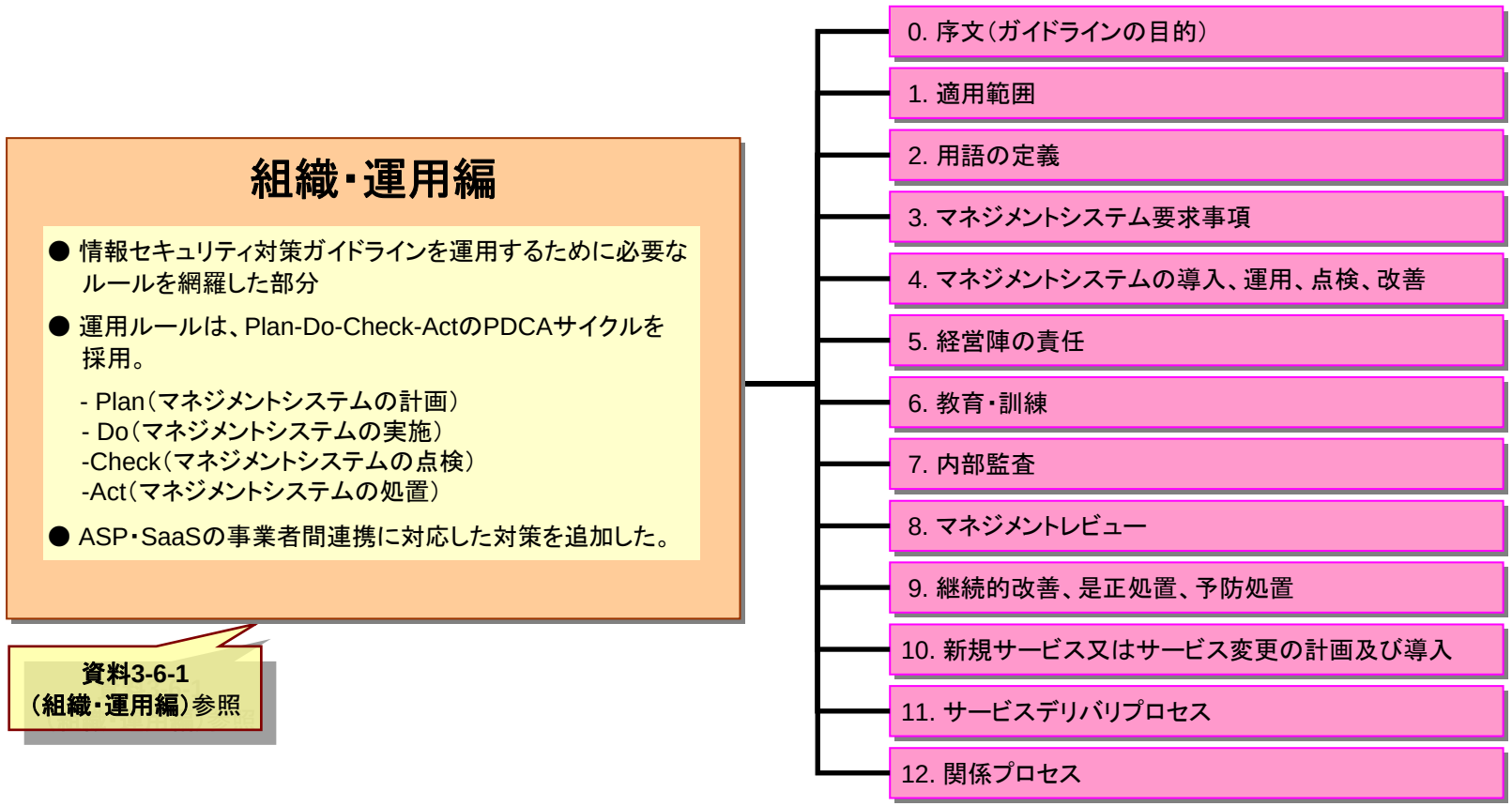
情報セキュリティ対策ガイドラインは、マネジメントシステムの運用ルールをまとめた「組織・運用編」と、実際に現場で適用するセキュリティ対策を列挙した「物理的・技術的対策編」の2つから構成される。



組織・運用編の構成

組織・運用編の内容は、以下のとおり。ISO/IEC27001をベースとして作成し、10章から12章については、SLA及びASP・SaaS事業者間連携等に対応するために必要なルールをISO/IEC20000-1から選別・追加している。また、それぞれの規格を参考にしつつ、ASP・SaaS事業者に特化して広く利用可能となるよう、運用に必要なプロセス数や要求項目を選別している。

※今後、本格的に情報セキュリティに取り組むASP・SaaS事業者も本ガイドラインが活用できるよう、わかりやすい用語を用いることとする。



【参考】組織・運用編の内容

資料3-6-1
（組織・運用編）参照

情報セキュリティ対策ガイドライン 組織・運用編	
0. 序文（ガイドラインの目的）	・・・本ガイドラインの目的、基本的な考え方、構成等について説明した章
1. 適用範囲	・・・本ガイドラインを適用するにあたっての留意事項をまとめた章
2. 用語の定義	・・・本ガイドラインを理解するために必要な用語とその用語の定義を列挙した章
3. マネジメントシステム要求事項	・・・マネジメントシステムに関する文書、記録に関するルールをまとめた章
4. マネジメントシステムの計画及び導入	・・・マネジメントシステムの運用（PDCAサイクル）の基本的なルールをまとめた章
5. 経営陣の責任	・・・マネジメントシステムに対する経営陣の役割・責任に関するルールをまとめた章
6. 教育・訓練	・・・情報セキュリティ、SLA実行に関する社員等への教育・訓練に関するルールをまとめた章
7. 内部監査	・・・マネジメントシステムの実施状況のCheck（内部監査）に関するルールをまとめた章
8. マネジメントレビュー	・・・マネジメントレビュー（経営陣による見直し）に関するルール（インプット・アウトプット）をまとめた章
9. 継続的改善、是正処置、予防処置	・・・マネジメントシステムの改善に関する一般原則と、是正処置・予防処置に関するルールをまとめた章
10. 新規サービス又はサービス変更の計画及び導入	・・・SLAの計画・変更・導入に関するルールをまとめた章
11. サービスデリバリプロセス	・・・SLAの管理、サービスの報告等、SLAの維持に必要なルールをまとめた章
12. 関係プロセス	・・・ユーザ（顧客）、アグリゲータ及びサプライヤの関係に関するルールをまとめた章

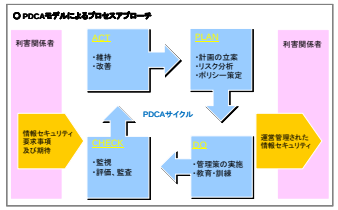
組織・運用編の作成方針

組織・運用編は、ASP・SaaS事業者にも広く活用してもらうため、ISMSで要求されている情報セキュリティの維持に必要な枠組み（PDCAサイクル）は残しつつ、マネジメントシステムの構築・運用に必要なプロセスをASP・SaaSの実態に合せて選別するとともに、例示を増やし、理解しやすい用語を用いることとしている。

【基本構成】

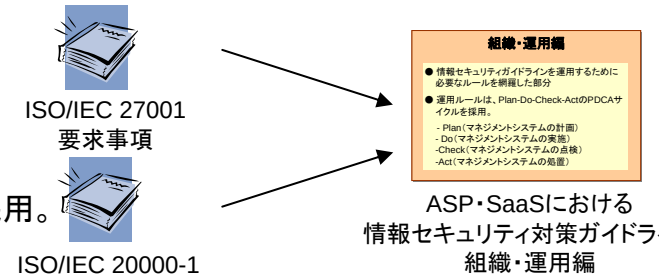
1. 組織・運用編の運用ルールの基本原則として、ISO/IEC27001のPlan-Do-Check-ActのPDCAサイクルを採用。

   - Plan（マネジメントシステムの計画）
   - Do（マネジメントシステムの実施）
   - Check（マネジメントシステムの点検）
   - Act（マネジメントシステムの処置）



2. 組織・運用編の構成要素として、

   - 情報セキュリティ対策に関する組織的・人的対策の中心となる情報セキュリティマネジメントシステム（ISO/IEC 27001/ISMS）と、
   - 顧客とのSLA締結及びASP・SaaSサービス提供に関連の深い、ITサービスマネジメントシステム（ISO/IEC20000-1/ITSMS）の一部を採用。



【特徴】

1. PDCAサイクルに必要な作業プロセス数を大幅に削減し、ASP・SaaS事業者に本当に必要なプロセスのみに絞込み。

   - リスクアセスメントのプロセス数を **11→4** に削減。（詳細については、リスクアセスメントp.16を参照）
   - 文書化に関する要求事項を削除。
   - 内部監査に関する要求事項を削除。
   - 継続的改善、是正処置、予防処置に関する要求事項を大幅に削減（**12 → 3**）。（詳細については、次ページ参照）

2. 情報セキュリティマネジメントシステムとITサービスマネジメントサービスのPDCAサイクルを一本化（p.6の3章から9章）。

3. SLA及びASP・SaaS事業者間連携等に対応した章を設定（p.6の10章から12章）

継続的改善、是正処置、予防処置における違い

ISMSにおける継続的改善、是正処置、予防処置に関する要求事項 （12項目）

8.1 継続的改善 ・・・・1項目

8.2 是正処置 ・・・・ 6項目

8.3 予防処置 ・・・・ 5項目

【参考】8.2で削除した項目
- a) 不適合の識別。
- b) 不適合の原因の特定。
- c) 不適合の再発防止を確実にするための処置の必要性の評価。
- d) 必要な是正処置の決定及び実施。
- e) 実施した処置の結果の記録。
- f) 実施した是正処置のレビュー。

【参考】8.3で削除した項目
- a) 起こり得る不適合及び原因の識別。
- b) 不適合の発生を予防するための処置の必要性の評価。
- c) 必要な予防処置の決定及び実施。
- d) 実施した処置の結果の記録。
- e) 実施した予防処置のレビュー。

本ガイドラインにおける継続的改善、是正処置、予防処置に関する対策項目 （3項目）

ASP・SaaSの場合は、事業者が自主的に実施することを考慮して、必要な対策項目のみ残した。

8.1 継続的改善 ・・・・ 1項目

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。

8.2 是正処置 ・・・・ 1項目

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。

8.3 予防処置 ・・・・ 1項目

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。

物理的・技術的対策編の構成

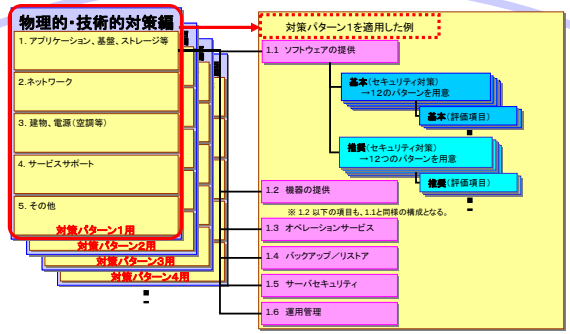
物理的・技術的対策編の章構成及び各章の内容は、以下のとおりとしている。

物理的・技術的対策編

- 物理的・技術的対策編は、ASP・SaaS事業者が基本的に実施すべきセキュリティ対策を示した「基本」と、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事業者が実施すべきセキュリティ対策を示した「推奨」の2つから構成される。
- さらに実際に遵守すべきセキュリティ対策や、顧客と合意すべきサービスレベルに関する評価項目・基準値を整理

12のパターンを用意

資料3-6-2
（物理的・技術的対策編）参照



各パターンごとに対策を設定

- 1. アプリケーション、基盤、ストレージ等
  - 1.1 ソフトウェアの提供
  - 1.2 機器の提供
  - 1.3 オペレーションサービス
  - 1.4 バックアップ／リストア
  - 1.5 サーバセキュリティ
  - 1.6 運用管理
- 2.ネットワーク
  - 2.1 アクセス制御
  - 2.2 ネットワークセキュリティ
  - 2.3 メールセキュリティ
  - 2.4 Webセキュリティ
  - 2.5 サーバセキュリティ
  - 2.6 ディレクトリサービス
  - 2.7 運用管理
  - 2.8 ネットワーク接続
- 3. 建物、電源（空調等）
  - 3.1 施設建築物
  - 3.2 IT機器設置スペース
  - 3.3 電源設備（受電方法、非常用電源）
  - 3.4 消化設備
  - 3.5 避雷・静電気対策設備
  - 3.6 空調設備
  - 3.7 入退室管理等
  - 3.8 バックアップ対策・管理
- 4. サービスサポート
  - 4.1 サービス窓口・サービス通知
  - 4.2 運用管理
- 5. その他
  - 5.1 サーバセキュリティ
  - 5.2 端末セキュリティ
  - 5.3 運用管理
  - 5.4 監査
  - 5.5 事業継続管理
  - 5.6 コンプライアンス

物理的・技術的対策編の構成（詳細）

本ガイドラインの「物理的・技術的対策編」では、ASP・SaaSに特化した対策を設定するため、公共ITにおけるアウトソーシングに関するガイドライン等を参考に、セキュリティ対策を5つに章立てしている。

物理的・技術的対策編

1. アプリケーション、基盤、ストレージ等
2. ネットワーク
3. 建物、電源（空調等）
4. サービスサポート
5. その他

対策パターン1用
対策パターン2用
対策パターン3用
対策パターン4用

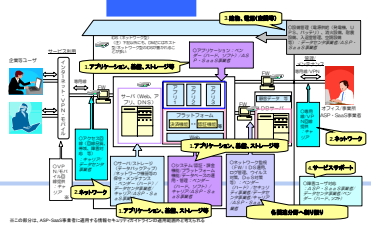
対策パターン1を適用した例

- 1.1 ソフトウェアの提供
  - **基本**（セキュリティ対策）→12のパターンを用意
    - **基本**（評価項目）
  - **推奨**（セキュリティ対策）→12つのパターンを用意
    - **推奨**（評価項目）
- 1.2 機器の提供

※ 1.2 以下の項目も、1.1と同様の構成となる。

- 1.3 オペレーションサービス
- 1.4 バックアップ／リストア
- 1.5 サーバセキュリティ
- 1.6 運用管理

● セキュリティ対策の項目により評価項目が設定されない場合がある。
● セキュリティ対策の項目により評価項目が2個以上設定される場合がある。



ASP・SaaSの構成要素

「公共ITにおけるアウトソーシングに関するガイドライン」等を参考にし、ASP・SaaSの構成要素を5つ（1章から5章）に層別化

【参考】物理的・技術的対策編における各章の詳しい意味

物理的・技術的対策編の各章は、以下の対策項目から構成される。これらの対策項目別にセキュリティ対策、SLAを適用することにより、漏れのない対策を実施することが可能となる。

物理的・技術的対策編の章構成	各章を構成する要素とその定義・具体例
1. アプリケーション、基盤、ストレージ 等	アプリケーション部分 【定　義】ユーザが直接アクセスするソフトウェア及びアプリケーションプラットフォーム 【具体例】グループウェア、財務会計ソフト、文書管理ソフト、検索ソフト、アプリケーション開発・実行基盤 基盤部分（プラットフォーム） 【定　義】ASP・SaaS事業者が利用するプラットフォーム 【具体例】決裁基盤、文書管理基盤、メディア・言語変換基盤、位置時間照明基盤、検索基盤 サーバ、ストレージ等のハード部分 【定　義】Webサーバ、アプリケーションサーバ、DBサーバ、ストレージ、Windows、UNIX、Linux、Solaris等 【具体例】決裁基盤、文書管理基盤、メディア・言語変換基盤、位置時間照明基盤、検索基盤
2. ネットワーク	【定　義】建物内のネットワーク、建物を起点した対ユーザ向けアクセス回線、メンテナンス用アクセス回線 【具体例】LAN、専用線、VPN　等
3. 建物、電源（空調等）	【定　義】サーバ、ネットワーク、監視設備、監視・メンテナンス要員等を収容している建物、部屋及びインフラ 【具体例】スペース、電源、空調、ラック、災害対策（地震、水害、火災、雷）
4. サービスサポート	【定　義】ASP・SaaSユーザからの問合窓口、緊急時対応等の顧客支援のための体制・サービス 【具体例】緊急問合せ窓口、ヘルプデスク、技術サポートセンター
5. その他	【定　義】上記1. から4. に分類不可能な対策項目 【具体例】紙媒体に関する対策、端末に関する対策

ASP・SaaSの情報セキュリティ対策のポイント

物理的・技術的対策編

ASP・SaaS事業特有の管理策

A.①・②のシーンで検討すべき管理策

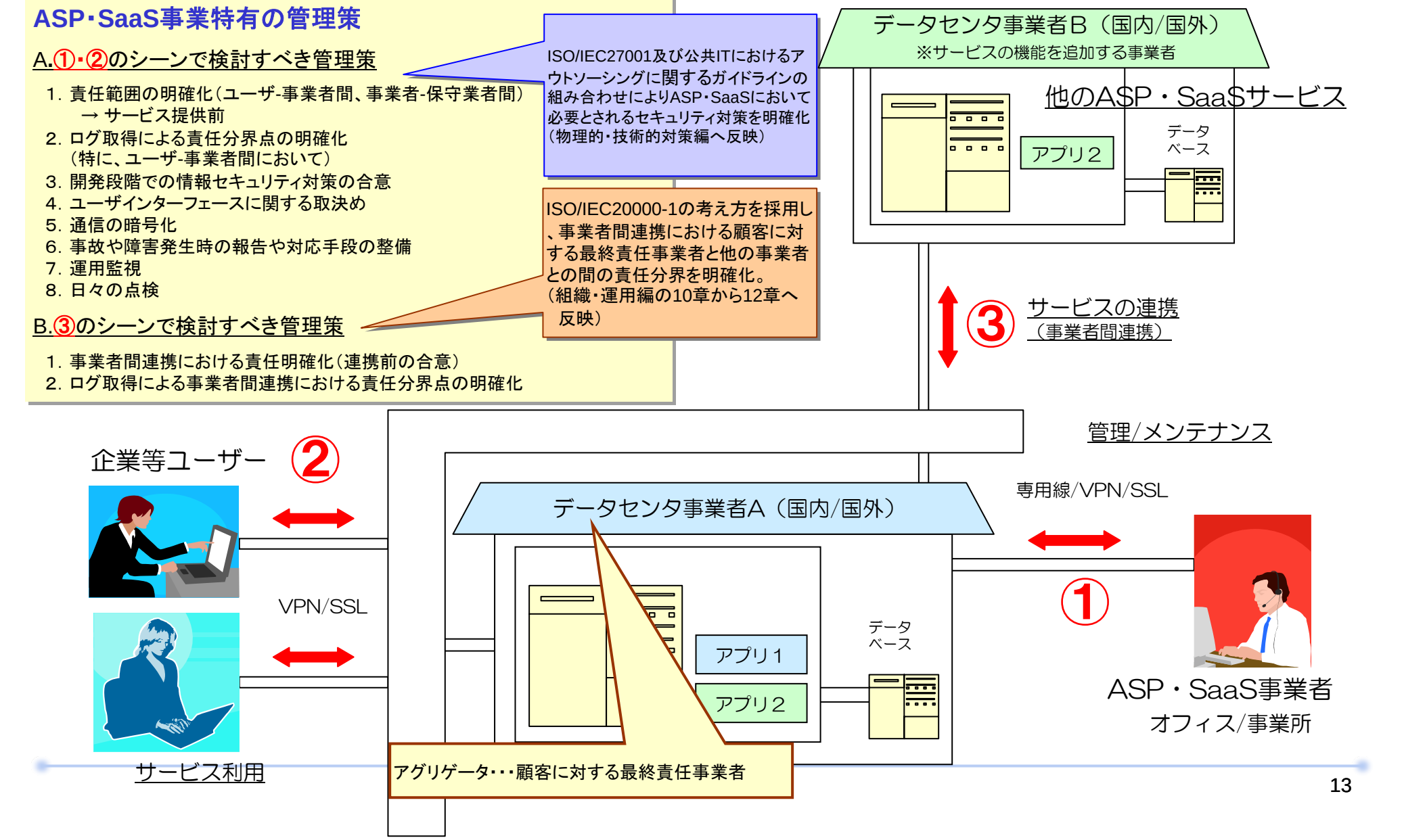
1. 責任範囲の明確化（ユーザ-事業者間、事業者-保守業者間）
   → サービス提供前
2. ログ取得による責任分界点の明確化
   （特に、ユーザ-事業者間において）
3. 開発段階での情報セキュリティ対策の合意
4. ユーザインターフェースに関する取決め
5. 通信の暗号化
6. 事故や障害発生時の報告や対応手段の整備
7. 運用監視
8. 日々の点検

B.③のシーンで検討すべき管理策

1. 事業者間連携における責任明確化（連携前の合意）
2. ログ取得による事業者間連携における責任分界点の明確化

ISO/IEC27001及び公共ITにおけるアウトソーシングに関するガイドラインの組み合わせによりASP・SaaSにおいて必要とされるセキュリティ対策を明確化（物理的・技術的対策編へ反映）

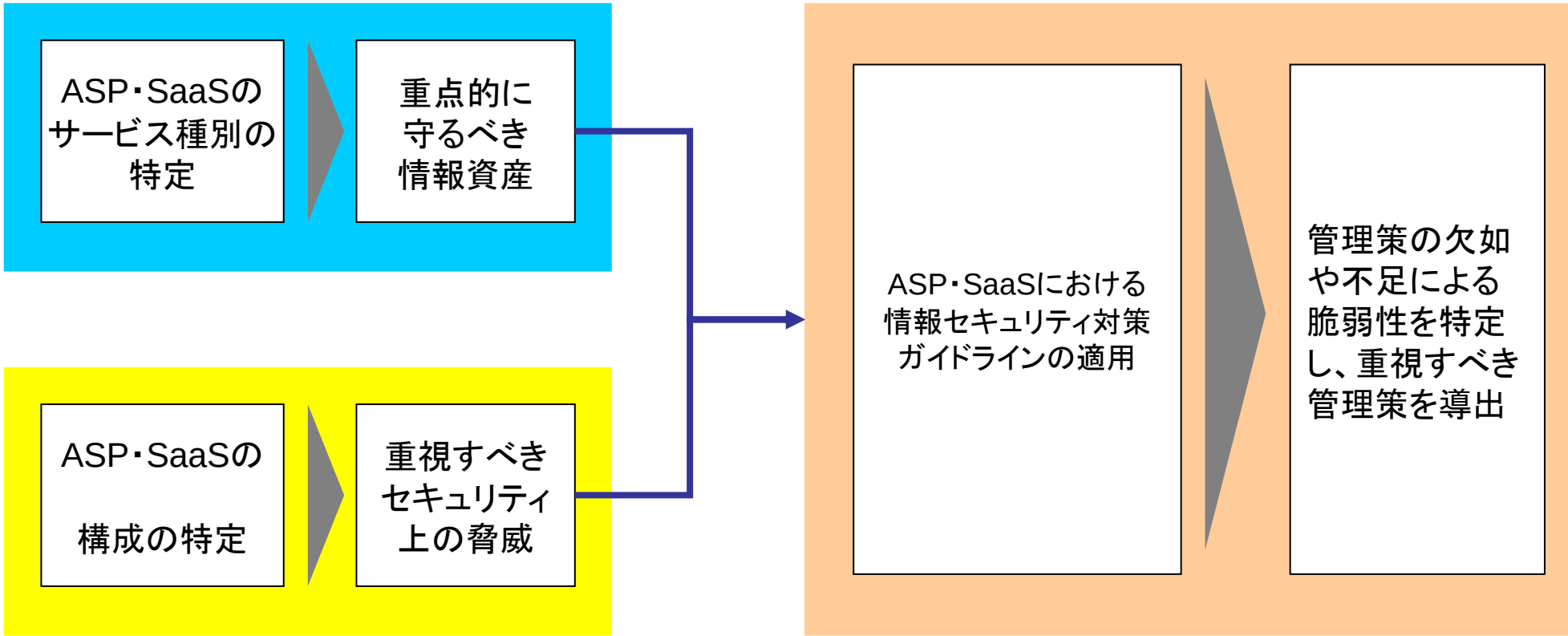
ISO/IEC20000-1の考え方を採用し、事業者間連携における顧客に対する最終責任事業者と他の事業者との間の責任分界を明確化。（組織・運用編の10章から12章へ反映）



重視すべき管理策を導出する流れ

リスクアセスメント

ASP・SaaSのサービスを分類することにより重点的に守るべき情報資産を分類し、また、ASP・SaaSを提供する構成を分類することにより重視すべきセキュリティ上の脅威をガイドライン作成段階で抽出する。その結果、各々のASP・SaaSが重点的に取り組むべき管理策が明確になり、その情報セキュリティ向上に資することができる。



リスクアセスメントで使用する用語の定義

ISMS適合性評価制度を運用しているJIPDEC（日本情報処理開発協会は、「ISMSユーザーズガイド（平成18年12月1日）」の中で、ISMSで用いられる用語について以下のように定義している。今回策定するガイドラインもこの定義に準拠するものとする。

情報セキュリティの定義：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。（JIS Q 27001：2006 3 用語及び定義　より引用）

機密性の定義：認可されていない個人、エンティティ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。
（JIS Q 13335-1：2006 2 用語及び定義　より引用）

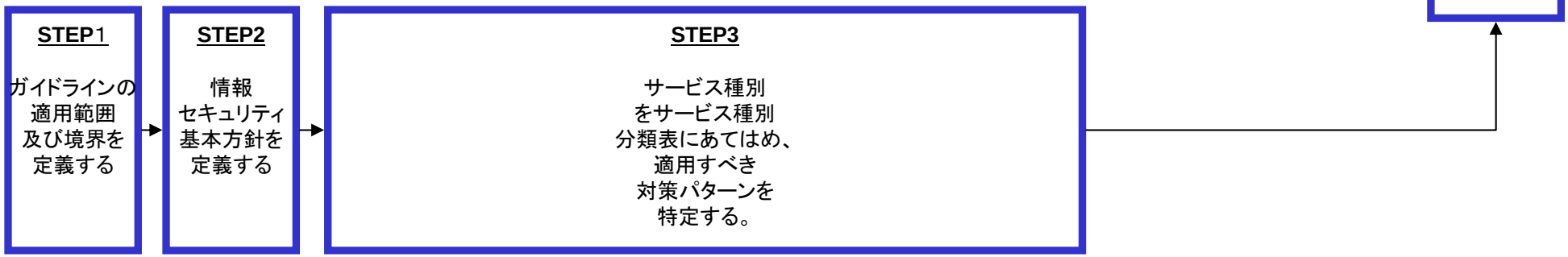
完全性の定義：資産の正確さ及び完全さを保護する特性。
（JIS Q 13335-1：2006 2 用語及び定義　より引用）

可用性の定義：認可されたエンティティが要求したときに、アクセス及び使用が可能である特性。
（JIS Q 13335-1：2006 2 用語及び定義　より引用）

リスクアセスメントの流れ

ISMS確立フェーズにおけるリスクアセスメントの流れ

本ガイドラインにおけるリスクアセスメントの流れ



リスクの捉え方

本ガイドラインでは、ISMSのリスクアセスメントで広く用いられている以下の手法に基づいてリスクを特定することとする。

情報資産の価値 × 脆弱性 × 脅威 ＝ リスク

ISMSガイドでは「情報資産の価値」を算出する際の情報資産の要素として「機密性」、「完全性」、「可用性」を用いて算出している。本ガイドラインのリスクアセスメントにおいても、情報資産の価値を把握する（=発生しうるリスクの範囲を把握する）際は、この三要素を中心に検討する。

情報資産の価値 ＝ 機密性（C） × 完全性（I） × 可用性（A）

この機密性（C）、完全性（I）、可用性（A）の各要素は、情報資産の価値を決定する時だけ利用されるのではなく、その情報資産が機密性（C）、完全性（I）、可用性（A）の観点からみてどの要素を重視しているかを判断するために利用することもできる。

本ガイドラインでは、ASP・SaaSのサービス種別ごとに、機密性（C）、完全性（I）、可用性（A）に対し、どのようなレベルを維持する必要があるのか分析した。

リスクアセスメントの基本的な考え方

ISMSにおけるリスクの捉え方

情報資産の価値 × 脆弱性 × 脅威 ＝ リスク

●情報資産については、ASP・SaaSのサービス種別に要求される機密性（C）、完全性（I）、可用性（A）のレベルを定義する。

●ぜい弱性については、組織、資産、運用方法によってその範囲にバラつきが生じるため、今回のリスクアセスメントにおいては、ぜい弱性を「既存の対策が実施されていない」としています。

●今回、ガイドライン策定時に実施するリスクアセスメントでは、ASP・SaaSの構成要素に存在しうる「脅威」をGMITSの手法を用いて洗い出しています。（p.22-24参照）

●ASP・SaaSの構成要素に存在しうる「脅威」をGMITSの手法を用いて洗すことで、情報資産に対し、機密性（C）、完全性（I）、可用性（A）のどこに影響を与えるのか特定しました。

サービス種別
の分類結果とセキュリティ対策
パターン・基準値レベル対応表
（別添1）

サービス種別ごとに要求される機密性（C）、完全性（I）、可用性（A)を維持するために必要なセキュリティ対策のセットを選択する。

本ガイドラインにおける対応

資料3-6-1
組織・運用編
のセキュリティ対策

資料3-6-2
物理的・技術的対策編の
セキュリティ対策
（12個のパターン）

①情報資産の機密性（C）
維持及びASP・SaaSに特化した
セキュリティ対策の選定

②情報資産の完全性（I）
維持及びASP・SaaSに特化した
セキュリティ対策の選定

③情報資産の可用性（A）
維持及びASP・SaaSに特化した
セキュリティ対策の選定

パターン判定表

物理的・技術的対策編におけるセキュリティ対策のパターンのCIAにおける特徴と件数は、以下のとおり整理できる。

【セキュリティ対策パターン判定表】

対策パターン	件数	機密性		完全性		可用性		
		高	低	高	低	高	中	低
1	5	○		○		○		
2	4	○		○			○	
3	3	○		○				○
4	4	○			○	○		
5	9	○			○		○	
6	15	○			○			○
7	0		○	○		○		
8	0		○	○			○	
9	1		○	○				○
10	3		○		○	○		
11	15		○		○		○	
12	14		○		○			○
全体	73							

パターン判定の流れ（全体）

物理的・技術的対策編におけるセキュリティ対策のパターン選択・基準値のレベル決定の流れは以下の通り。

手順1

「サービス種別の分類結果と基準値の関係」で、自社サービスの属するサービス種別を特定する。

手順2

特定したサービス種別に付随した機密性（C）、完全性（I）、可用性（A）及びその他の要素で該当する対策のパターン（1～12）を確認する。

手順3

「物理的・技術的対策編」に手順1と2で決定した基準値のレベルとセキュリティ対策のパターンを自社のサービスに適用する。

※「推奨」は、各事業者の判断で選択する。

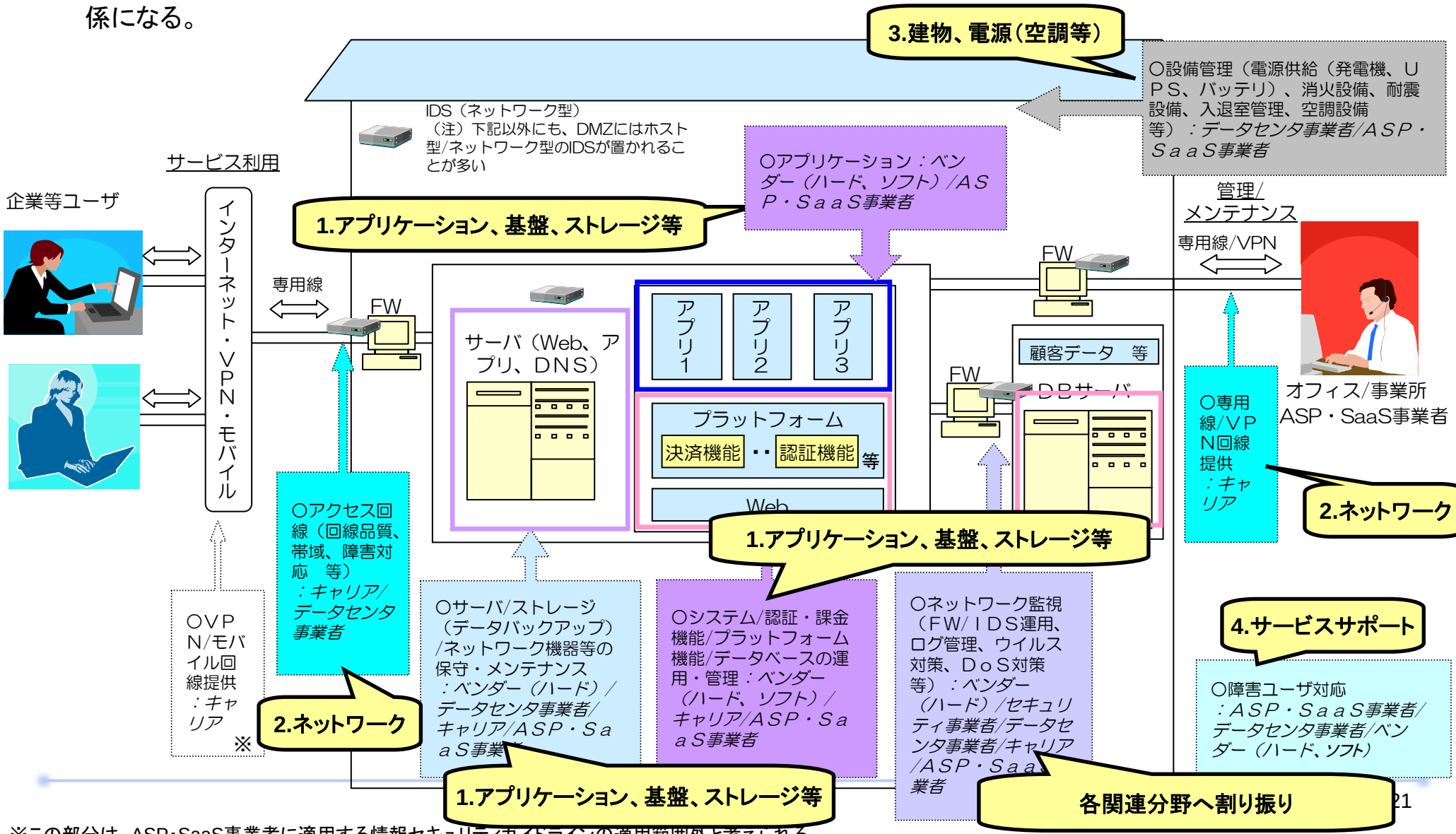
【サービス種別の分類結果とセキュリティ対策パターン・基準値レベル対応表（別添1）】

【物理的・技術的対策編】

ASP・SaaSの構成の特定

リスクアセスメント

ASP・SaaSの構成要素は下図のように整理される。各構成要素を情報セキュリティ標準の項目案で分類すると以下の関係になる。



※この部分は、ASP・SaaS事業者に適用する情報セキュリティガイドラインの適用範囲外と考えられる

GMITS(MICTS)における脅威の分類 ①

リスクアセスメント

ASP・SaaSの構成要素に対して、GMITSで定義されているような一般的な情報セキュリティに関するすべての脅威を想定する。

脅威が対象とするもの	脅威の分類	脅威の詳細分類
外部の第三者もしくは内部の人間の悪意に起因する脅威を対象とするもの	情報資産の機密性の損失	セキュリティ違反、ウイルス感染 不正プログラム実行、情報資産の盗難 情報資産の持ち出し、不正アクセス 許可されていない区域への侵入 情報処理施設や設備の悪用、盗聴
	情報資産の完全性の損失	従業員によるセキュリティ違反、ウイルス感染 不正プログラム実行、情報資産の盗難 情報資産の不正変更 情報処理施設や設備の破壊
	情報資産の可用性の損失	従業員によるセキュリティ違反、ウイルス感染 不正プログラム実行、情報資産の盗難 情報処理施設や設備の破壊 情報処理施設や設備の悪用、システムリソースの浪費 サービス不能攻撃、スタッフ不在、障害復旧の妨害

参考資料： GMITS (ISO/IEC TR 13335-3) 付属書C 考えうる脅威のタイプのリストより抜粋
電子自治体アウトソーシング実践の手引き p44 (6) 情報セキュリティと安全性

GMITS(MICTS)における脅威の分類 ②

リスクアセスメント

脅威が対象とするもの	脅威の分類	脅威の詳細分類
内部の人間の過失に起因する脅威を対象とするもの	情報資産の機密性の損失	セキュリティ違反（理解不足に起因）、ウイルス感染 不正プログラムによる被害 情報資産の持ち出し 従業員の操作エラー システムの誤動作
	情報資産の完全性の損失	セキュリティ違反（理解不足に起因） ウイルス感染、不正プログラムによる被害 情報資産の持ち出し 情報資産の変更 事故による情報処理施設や設備の破壊
	情報資産の可用性の損失	セキュリティ違反（理解不足に起因）、ウイルス感染 不正プログラムによる被害、情報資産の持ち出し 事故による情報処理施設や設備の破壊 システムの誤動作、システムリソースの浪費 スタッフ不在、障害復旧の遅れ

参考資料： GMITS (ISO/IEC TR 13335-3) 付属書C 考えうる脅威のタイプのリスト
電子自治体アウトソーシング実践の手引き p44 (6) 情報セキュリティと安全性

GMITS(MICTS)における脅威の分類 ③

リスクアセスメント

脅威が対象とするもの	脅威の分類	脅威の詳細分類
自然災害等、人的でない要因に起因する脅威を対象とするもの	災害	地震、振動 洪水 台風 落雷 火災 煙
	インフラストラクチャーの障害	通信回線の不安定 電話回線の不安定 電力の不安定
	一般的な環境障害	極端な温度及び湿気 ほこり 電磁波放射
	情報資産の劣化	ハードウエアの劣化 ネットワーク機器の劣化 媒体の劣化 ドキュメントの劣化

参考資料： GMITS (ISO/IEC TR 13335-3) 付属書C 考えうる脅威のタイプのリスト
電子自治体アウトソーシング実践の手引き p44 (6) 情報セキュリティと安全性