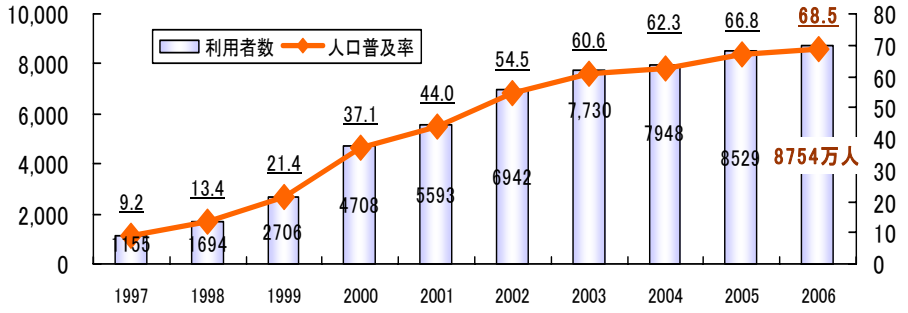
参考資料

ASP・SaaSの情報セキュリティ対策に関する研究会
報告書 要旨

研究会開催の背景

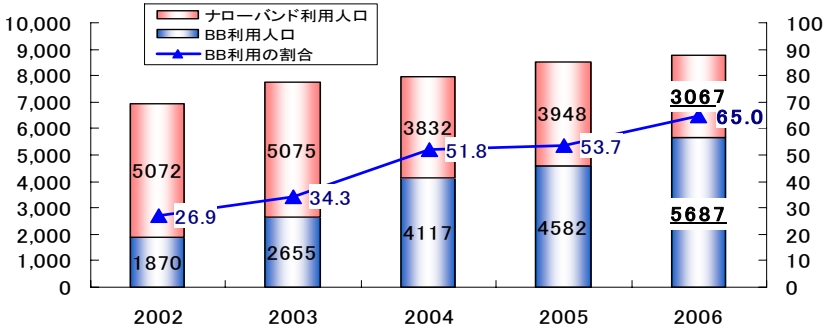
- ブロードバンド環境の進展により、インターネットは国民生活・社会経済活動を支える重要なインフラとして必要不可欠な存在。
- 国際競争力強化・生産性向上への切り札として、ASP・SaaSの普及促進に向けた取組を実施。

国内のインターネット利用者数



・国民の7割近くがインターネットを利用

ブロードバンド回線の利用者数



・インターネット利用者の65.0%がブロードバンド回線を使用

○「ICT改革促進プログラム」(平成19年4月20日)

・生産性向上のためのICT共通基盤の整備

「・・・ASPやSaaS等の新たなネットワーク・サービスの普及促進のための環境整備などICT共通基盤の整備に取り組む。」

○「ICT国際競争力懇談会 最終取りまとめ」(平成19年4月23日)

・経済成長、生産性向上の基本戦略

>> ASP・SaaSの普及促進

○「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)

・サービス革新戦略 >> ITによる生産性向上

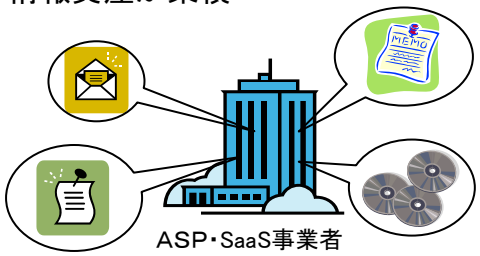
「・・・ASPやSaaSなど中小企業にとって使いやすい新たなサービスの普及促進のための共通基盤の整備等環境整備を促進する。」

研究会開催の目的

● 適切な情報セキュリティ対策が施されたASP・SaaSサービスの提供が促進され、企業等の生産性向上の健全な基盤となるよう、ASP・SaaS事業者が講じるべき情報セキュリティ対策を検討。

ASP・SaaSサービスの現状

○ ASP・SaaS事業者及びその関係組織には、利用者の膨大な機密情報・顧客情報等の情報資産が集積



○ ASP・SaaSサービスが健全に発展していくためには、ASP・SaaS事業者における適切な情報セキュリティ対策が必要不可欠

ASP・SaaSの情報セキュリティ対策に関する問題意識

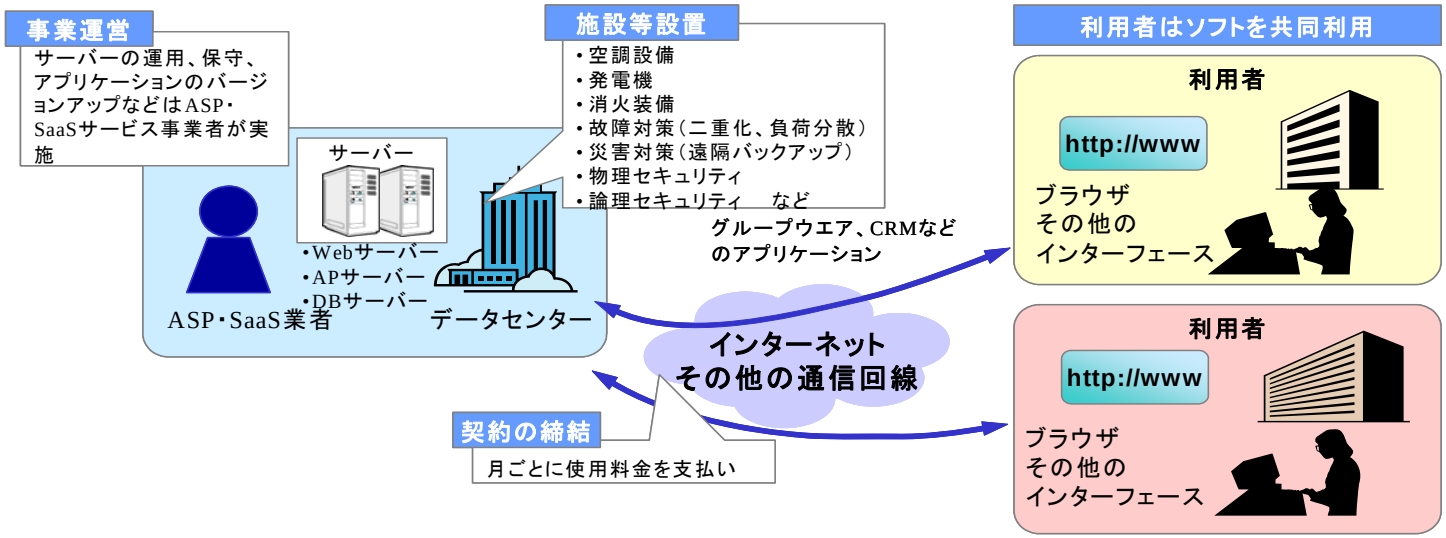
○ 多数を占める中小のASP・SaaS事業者においても適切な情報セキュリティ対策が施されているのか。
○ 講じるべき情報セキュリティ対策の基準が不明瞭ではないか。
○ 利用者に対して、必ずしも十分な説明や情報開示がなされていないのではないか。

ASP・SaaS事業者が講じるべき、適切な情報セキュリティ対策の検討が必要

ASP・SaaSに関する諸動向 ①　～ ASP・SaaSとは

- ASPは、「ネットワークを通じて、アプリケーション・ソフトウェア及びそれに付随するサービスを利用させること、あるいはそうしたサービスを提供するビジネスモデルを指す。」と定義※。
- 本研究会でも当該定義を採用するとともに、ASP及びSaaSを特に区別せず、「ASP・SaaS」と呼称。

ASP・SaaSサービスの提供・利用形態



ASP・SaaSサービスの特徴

- ○ アプリケーション機能をネットワーク経由で提供
- ○ 複数の利用者による共同利用
- ○ 使用時間等に応じて定期的に料金を支払
- ○ ASP・SaaS事業者が運用・保守を実施

利用者のメリット

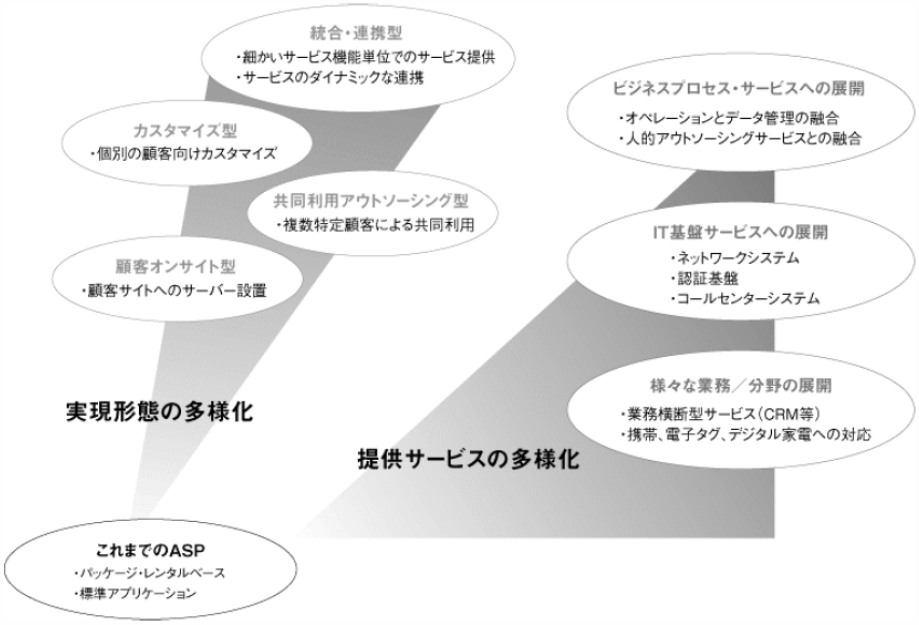
- ○ システム導入時の初期投資や運用・保守コストの軽減
- ○ 迅速かつ柔軟なシステム利用
- ○ 専門事業者による高レベルのノウハウでの運用・保守

※　2004年版「ASP白書」におけるASPの定義

ASP・SaaSに関する諸動向 ②　～ ASP・SaaSサービスの多様化と市場規模の拡大

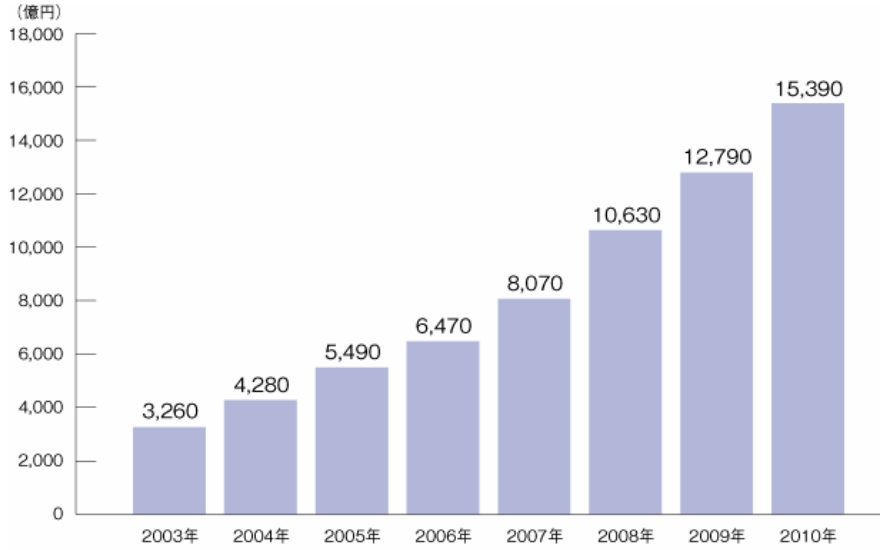
- 実現形態・提供サービス内容という二つの側面から、ASP・SaaSサービスの多様化が急激に進展。
- ASP・SaaSサービスの多様化に呼応して、利用者層も広範な業種に拡大。
- ASP・SaaS関連市場の規模は、2003年時点の3，260億円から年1．3倍前後のペースで拡大を続け、2010年には、2003年の5倍弱となる15，390億円に達すると予測。

ASP・SaaSの実現形態・提供サービスの多様化



出典：2005年ASP白書 ASPIC Japan／マルチメディア振興センター

ASP・SaaS関連市場の規模の推移と予測（国内）



注：ASP関連市場には、セキュリティ・ホスティング等のデータセンターを含む。
情報通信白書2002のASP市場予測、データセンター市場規模予測、eラーニング白書のeラーニング市場のうちシステム事業に分類される事業のベンダー売上げとASP化が見込まれる領域の売上げ、e-Japan関連予算のうち、「行政の情報化及び公共分野における情報通信技術の活用」に対する予算額、ASP関連市場に投下される予算額について、それぞれパラメータを設定して推計した。

出典：2005年ASP白書 ASPIC Japan／マルチメディア振興センター

ASP・SaaSにおける情報セキュリティ対策の現状と課題

- ASP・SaaSの現状（中小規模の事業者が大半を占める、提供サービスが多岐にわたる等）を踏まえると、適切な対策の優先度付けや提供サービスの特徴に応じた対策が十分に実施できていない等の課題。
- ASP・SaaS事業者の実態やASP・SaaSサービスの特性に即した基準・ガイドライン等が存在しない。

ASP・SaaSの現状を踏まえた情報セキュリティ対策の課題

○ ASP・SaaS業界は、中小規模の事業者が大半を占める	○ 人的・金銭的資源に限りがある事業者は、優先すべき情報セキュリティ対策に対し、重点的に資源配分することが求められるが、適切なリスクアセスメントを通じた**情報セキュリティ対策の優先度付けができていない**
○ ASP・SaaS事業者が提供するサービスは多岐にわたる	○ 扱う情報の違いから、「何を」「どの程度」実施すればよいかサービスごとに異なるにもかかわらず、**サービスの特徴に基づく適切な情報セキュリティ対策が実施できていない**

情報セキュリティ対策に関する既存の基準・ガイドライン等

○ ASP・SaaSサービスの特性を念頭に置いて作成されたものではない	○ ASP・SaaS事業者がこれらの基準・ガイドライン等をそのまま利活用する場合、**ASP・SaaS事業者の実態に即した情報セキュリティ対策を導入・実施しにくい**

ASP・SaaS事業者の実態に即した、新たな情報セキュリティ対策ガイドラインの作成が必要

（参考）情報セキュリティに関する既存の法令・基準・ガイドライン等

1．情報セキュリティに関する分野

- JIS Q 27001 ：2006
- MICTS（情報及び通信技術セキュリティの管理）
- NIST（米商務省標準技術局）
- プロバイダ責任制限法（平成13年法律第137号）
- 不正アクセス禁止法（平成11年法律第128号）
- JIS Q 27002 ：2006
- FISC（金融情報システムセンター）
- 電気通信事業法（昭和59年法律第86号）
- 不正競争防止法（平成5年法律第47号）

2．個人情報保護に関する分野

- JIS Q 15001 ：2006
- 個人情報保護法（平成15年法律第57号）
- 電気通信事業における個人情報保護に関するガイドライン（平成16年8月31日総務省告示第695号）

3．内部統制に関する分野

- COBIT（IT Governance Institute）
- SysTrust（米国公認会計士協会 ）
- WebTrust（米国公認会計士協会 ）
- SAS70（米国公認会計士協会 ）
- 金融商品取引法（昭和23年法律第25号）
- 財務報告に係る内部統制の評価及び監査の基準（金融庁）

4．SLAに関する分野

- 電子自治体 基幹系SLA設定例（ASPIC Japan）
- 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（総務省）
- 民間向けITシステムのSLAガイドライン（第3版）（日本情報技術産業協会（JEITA））
- 情報システムに係る政府調達へのSLA導入ガイドライン（経済産業省）

5．ITサービスに関する分野

- ISO/IEC 20000-1 ：2005
- PD0005 PD0015
- ISO/IEC 20000-2 ：2005
- ITIL

6．事業継続に関する分野

- BS 25999（英国規格協会）
- 事業継続ガイドライン（第1版）（内閣府防災担当）
- 事業継続計画策定ガイドライン（経済産業省）
- 中小企業BCP策定運用方針（中小企業庁）
- 金融機関等におけるコンティンジェンシープラン策定のための手引書（FISC）

7．信頼性に関する分野

- 情報通信ネットワーク安全・信頼性基準（昭和62年郵政省告示第73号）

凡例：法令（法律、告示、省令を含む）／ガイドライン

情報セキュリティ対策ガイドラインに関する基本的な考え方

● 『ASP・SaaS事業者が、提供するサービスの特徴に基づいた適切な情報セキュリティ対策の実施を検討する際の具体的な指針』と位置づけ、ASP・SaaS事業者の実態や提供サービスの特性を反映した、新たな情報セキュリティ対策ガイドラインを策定。

ASP・SaaSの情報セキュリティ対策の現状と課題

○ ASP・SaaS事業者及びサービスの特性を反映し、「どこに」「何を」「どの程度」実施すべきかを示した情報セキュリティ対策の指針がない

- 情報セキュリティ対策の優先付けがされていない
- 提供するASP・SaaSサービスの特徴に基づいた、適切な情報セキュリティ対策の実施がされていない

情報セキュリティ対策ガイドラインへの期待

- 利用者がASP・SaaSサービスを適切に選別できるような判断基準としての役割
- 様々な規模のASP・SaaS事業者への対応
- 新規に参入するASP・SaaS事業者にとっての指南書としての役割

ガイドライン策定にあたっての重点ポイント

○ ASP・SaaS事業者及びサービスの特性を反映し、優先的に取り組むべき情報セキュリティ対策を絞り込む

○ ガイドラインをそのまま利用することで、比較的簡単に自ら提供するサービスに即した情報セキュリティ対策を実施可能にする

○ ASP・SaaS事業者が理解および実施しやすい具体的な情報セキュリティ対策を示す

○ 利用者にとっての理解しやすさも考慮する

本ガイドラインを足がかりとして、ASP・SaaS事業者における情報セキュリティマネジメントシステムの確立、導入、運用、監視、見直しが実施され、継続的に情報セキュリティ対策が改善されていくことを期待

情報セキュリティ対策ガイドライン策定へのアプローチ

● 「基本的な考え方」において整理したガイドラインの基本的位置づけ、策定にあたっての重点ポイントを踏まえて、ガイドライン策定に向けた具体的なアプローチを検討。

ガイドライン策定にあたっての重点ポイント

○ ASP・SaaS事業者及びサービスの特性を反映し、優先的に取り組むべき情報セキュリティ対策を絞り込む

○ ガイドラインをそのまま利用することで、比較的簡単に自ら提供するサービスに即した情報セキュリティ対策を実施可能にする

○ ASP・SaaS事業者が理解および実施しやすい具体的な情報セキュリティ対策を示す

ガイドライン策定に向けた具体的アプローチ

✓ASP・SaaSの**典型的なシステム構成に基づく情報セキュリティ対策の導出**、個々に対策導出する負担を軽減

✓**優先的に取り組むべき対策**と、実施することが望まれる対策に分類

✓**分かりやすい記述**、定量的あるいは具体的な**対策実施レベルの目安**を提示

✓特に**達成が必要と考えられる対策レベル**については区別して明示

✓技術的な対策だけではなく、**組織・運用に係る情報セキュリティ対策**も用意

✓多様なASP・SaaSサービスに対する網羅性と適合性を確保するために、**サービスをセキュリティ要件に基づいてパターンに分類**する基準を導入

✓ガイドライン利用の際は、**パターンごとに定められた情報セキュリティ対策の実施レベルを参照**することで、ASP・SaaS事業者自らが適切な対策実施レベルを容易に選択可能

ガイドライン策定に向けた検討 ①　～ 検討の進め方

- 「ガイドライン策定へのアプローチ」を受け、必要な情報セキュリティ対策を検討してガイドライン化。
- ASP・SaaS事業者内の運用管理体制の整備等に関する組織・運用面の対策、並びにASP・SaaSを構成するハードウェア及びソフトウェア等に施す物理的・技術的対策を導出。

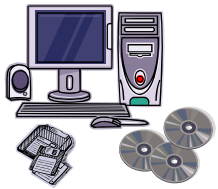
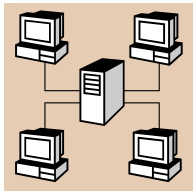
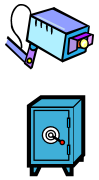
組織・運用面の対策

○ ASP・SaaS事業者内の運用管理体制の整備
（情報資産管理、従業員管理等）
○ 外部関係組織との取り決め事項
○ ユーザーサポート責任　等

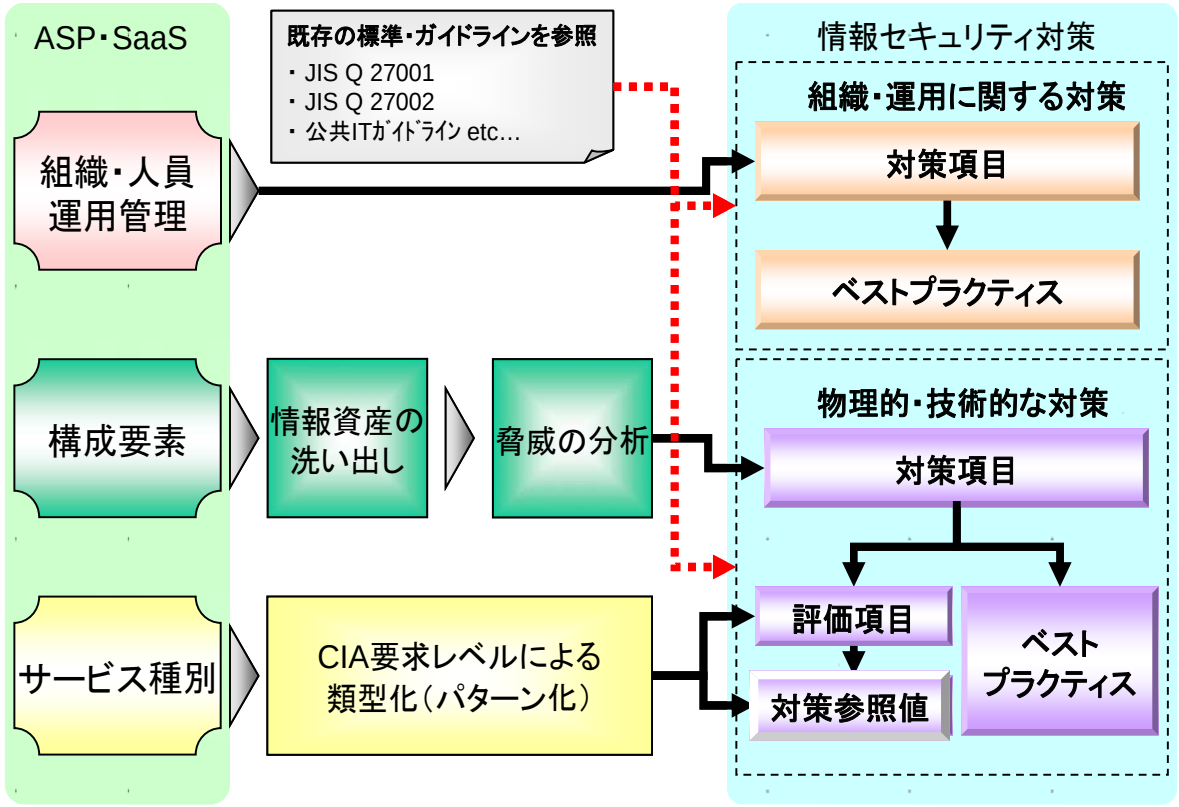


物理的・技術的対策

○ ASP・SaaSを構成するハードウェア及びソフトウェアの稼動監視・障害監視、ウィルス対策
○ 不正アクセス防止、データのバックアップ
○ 管理者権限割当ての制限、入退室管理　等


情報セキュリティ対策の導出の流れ



ガイドライン策定に向けた検討 ②　～「組織・運用」に関する対策の導出

● 情報セキュリティ対策の継続的な改善を図るため、ASP・SaaS事業者内の運用管理体制の整備及びリソースの確保、外部関係組織に対する要求事項等を定めた「組織・運用」に関する対策を導出。

① 情報セキュリティマネジメントにおけるステークホルダの確認

○ ASP・SaaSサービスの提供において、重点的に考慮すべきステークホルダ（内部・外部）の洗い出しを実施

→

○ 多岐にわたるステークホルダをリストアップ
- ASP・SaaS事業者（経営陣、管理責任者、それ以外の従業員）
- 連携事業者、サービス利用者、その他の外部組織

② 対策項目の導出

○ 各ステークホルダに対し、どのような組織・運用面での対策が必要になるかを検討し、対策項目として導出

→

○ 組織・運用面の情報セキュリティ管理策として網羅性の非常に高いJIS Q 27001附属書Aを参照

○ ASP・SaaS事業者の実情を考慮し、中小事業者にとっても優先的に取り組むべき対策に重点を置いた検討を実施

○ 類似した対策項目を集約したり、ASP・SaaSの実態に即して表現を書き換える等、分かりやすさに留意した編集を実施

③ ベストプラクティスの作成

○ 対策項目に関する理解促進のため、具体的な実施方法や注意すべき点をまとめた事例集（ベストプラクティス）を対策項目ごとに作成

→

○ 関連分野の専門家（ASP・SaaS事業者、情報機器メーカ、ISP及びデータセンタ事業者等）の知見を積極的に取り入れ、ASP・SaaSの実態に即した内容及び表現となるよう留意

○ JIS Q 27002におけるベストプラクティスを参照

（参考）「組織・運用」に関する対策の概略

1. 情報セキュリティへの組織的取組の基本方針

○ ASP・SaaS事業者が、組織として情報セキュリティに取組むにあたっての基本方針の作成、経営陣の役割等の要求事項

2. 情報セキュリティのための組織

○ ASP・SaaS事業者の内部組織及び外部組織に対して行うべき規程、マニュアル、契約等に関する基本的な要求事項

3. 連携ASP・SaaS事業者に関する管理

○ ASP・SaaSのステークホルダとして特徴的な、連携ASP・SaaS事業者に対する要求事項

4. 情報資産の管理

○ ASP・SaaS事業者の内部組織及び外部組織に対する、情報資産の管理に特化して適用すべき要求事項

5. 従業員に係る情報セキュリティ

○ ASP・SaaS事業者の従業員との契約等に特化して適用すべき要求事項

6. 情報セキュリティインシデントの管理

○ ASP・SaaS事業者の従業員の情報セキュリティインシデント対応に特化して適用すべき要求事項

7. コンプライアンス

○ ASP・SaaS事業者の従業員等に対する、法令・規則の遵守に関する要求事項

8. ユーザサポートの責任

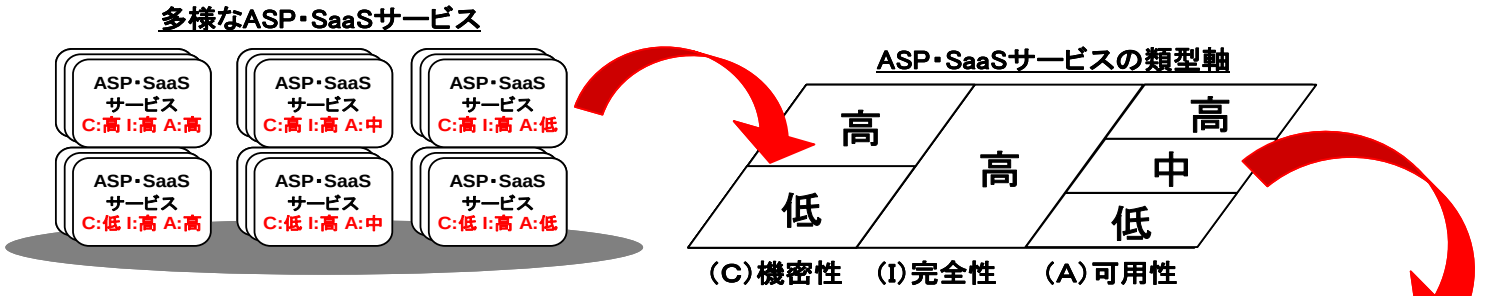
○ 事業連携等において、ASP・SaaS事業者のユーザーサポート組織が果たすべき役割に関する要求事項

ガイドライン策定に向けた検討 ③　～「物理的・技術的」対策の導出 ①

- ASP・SaaSの典型的なシステム構成から構成要素（ハードウェア、ソフトウェア、ハウジング等）を特定し、情報資産を洗い出した上で、それらを保護するための「物理的・技術的」対策を導出。
- 多種多様なASP・SaaSサービスごとに異なる情報資産のCIA※要求レベルを、導出した情報セキュリティ対策に適切に反映させるため、ASP・SaaSサービスをCIA要求レベルに基づき類型化（パターン化）。

① ASP・SaaSサービスの類型化（パターン化）

○ 取り扱う情報の内容や求められる品質等に着目し、ASP・SaaSサービスをCIA要求レベルに応じてパターン化



ASP・SaaSサービスの類型結果

パターン	パターンの定義	機密性への要求	完全性への要求	可用性への要求
1	機密性・完全性・可用性の全てへの要求が高いサービス	高い	高い	高い
2	機密性・完全性への要求は高いが、可用性への要求はそれほど高くないサービス	高い	高い	中程度
3	機密性・完全性への要求は高いが、可用性への要求は低いサービス	高い	高い	低い
4	機密性への要求は低いが、完全性・可用性への要求が高いサービス	低い	高い	高い
5	機密性への要求は低いが、完全性への要求は高く、可用性への要求はそれほど高くないサービス	低い	高い	中程度
6	完全性への要求は高いが、機密性・可用性への要求は低いサービス	低い	高い	低い

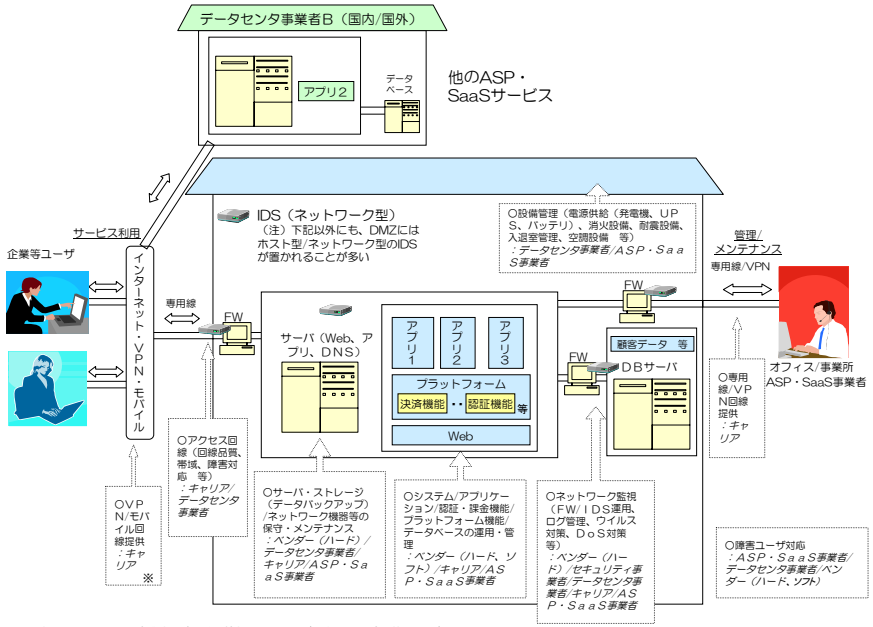
※CIA：「機密性（C：Confidentiality）」・「完全性（I：Integrity）」・「可用性（A：Availability）」

ガイドライン策定に向けた検討 ④　～「物理的・技術的」対策の導出 ②

② ASP・SaaSの構成要素の特定

- ASP・SaaSのサービス形態に大きく依存する以下の事項を踏まえつつ、典型的なシステム構成を想定
  - データセンタ等の外部事業者活用の有無
  - 他のASP・SaaS事業者との業務連携の有無
- 典型的なシステム構成から、ASP・SaaSの構成要素を特定

ASP・SaaSの典型的な構成要素



※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

③ 構成要素に基づく情報資産の洗い出し

- 情報セキュリティ対策の対象となる情報資産を、「構成要素そのもの及び各構成要素を介する情報」とみなし、新たに各構成要素を介する情報をリストアップ
- リストアップした情報に基づき、情報資産をとりまとめ

ASP・SaaSの構成要素における情報資産

分類	情報資産（構成要素＋情報）
1.アプリケーション、プラットフォーム、ストレージ等	【アプリケーション部分】 ・ASP・SaaS アプリケーション＆アプリケーションログ（利用、管理） ・サービスデータ（利用者情報） ・サービスデータ（管理者情報）
	【プラットフォーム】 ・ASP・SaaS 事業者が利用するプラットフォーム＆ログ（利用、管理） （例）決済、認証、検索、位置時間証明等
	【サーバ・ストレージ等のハード部分】 ・サーバ群（付随する OS 等の基盤ソフトを含む）＆サーバログ（利用、管理） ・データベース（付随する OS 等の基盤ソフトを含む）＆データベースログ（利用、管理） ・ストレージ＆管理ログ ・通信機器＆管理ログ ・情報セキュリティ対策機器＆管理ログ
2.ネットワーク	・外部ネットワーク
3.建物、電源(空調等)	・建物 ・サーバルーム（サーバ群、データベース等を格納している部屋） ・物理的セキュリティ境界 ・電源 ・空調
4.その他	・運用管理端末 ・保管媒体（紙、磁気メディア、光メディア等）

ガイドライン策定に向けた検討 ⑤　～「物理的・技術的」対策の導出 ③

④ 情報資産に対する脅威分析

○ 各情報資産のCIAに被害を与える可能性のある脅威を抽出

○ 情報資産に対応する脅威を網羅的に分析するため、情報セキュリティ分野の一般的な脅威がリスト化されているMICTS（Part1：JIS Q 13335-1、Part 2）を参照

○ 情報資産のCIAに直接作用する脅威のみを抽出することにより、情報資産を保護するために必要最小限の対策を効率的に導出可能となる

情報資産に対する脅威の事例

（情報資産：「利用者情報」に対する脅威）

種別	分類	脅威の詳細分類
外部もしくは内部の人間の悪意に起因する脅威	機密性損失	情報セキュリティ違反、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、盗聴
	完全性損失	従業員による情報セキュリティ違反、不正プログラム実行、情報資産の不正変更
	可用性損失	従業員による情報セキュリティ違反、不正プログラム実行
内部の人間の過失に起因する脅威	機密性損失	情報セキュリティ違反(理解不足に起因)、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
	完全性損失	情報セキュリティ違反(理解不足に起因)、不正プログラムによる被害、情報資産の変更
	可用性損失	情報セキュリティ違反(理解不足に起因)、不正プログラムによる被害
自然災害等、人的でない要因に起因する脅威	災害	－
	インフラ障害	－
	一般的な環境障害	－
	情報資産の劣化	－

⑤ 対策項目の導出

○ 脅威分析の結果に基づき、各情報資産を保護するために必要な物理的・技術的対策を検討し、対策項目として導出

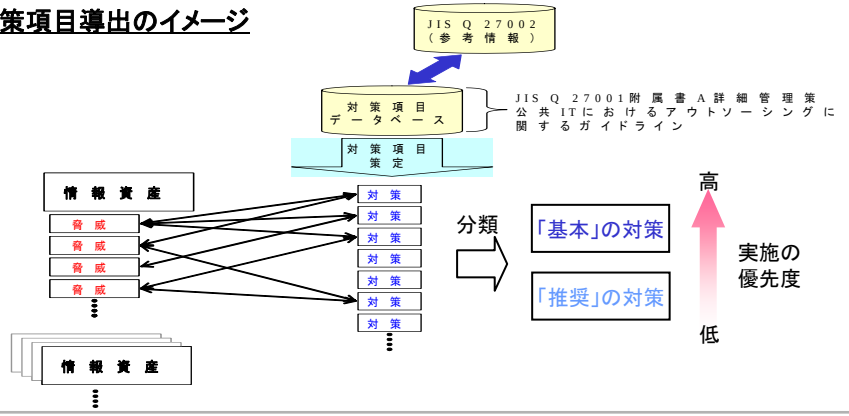
○ 物理的・技術的な情報セキュリティ管理策として網羅性の非常に高いJIS Q 27001附属書Aを参照

○ 公共分野におけるASP・SaaSのSLA設定のためのガイドラインとして実績のある「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」を参照

○ ASP・SaaS事業者の実態を考慮するため、関連分野の専門家の知見を積極的に取り入れつつ、実施の優先度の観点から対策を「基本」と「推奨」に分類

○ 類似した対策項目を集約したり、ASP・SaaSの実態に即して表現を書き換える等、分かりやすさに留意した編集を実施

対策項目導出のイメージ



ガイドライン策定に向けた検討 ⑥　～「物理的・技術的」対策の導出 ④

⑥ ベストプラクティスの作成

○ 対策項目に関する理解促進のため、具体的な実施方法や注意すべき点をまとめた事例集（ベストプラクティス）を対策項目ごとに作成

○ 関連分野の専門家の知見を積極的に取り入れ、ASP・SaaSの実態に即した内容及び表現となるよう留意

○ JIS Q 27002及び「金融機関等コンピュータシステムの安全対策基準・解説書」におけるベストプラクティスを参照

ベストプラクティスの事例

（対策項目：「定期バックアップ」に対するベストプラクティス）

Ⅲ．２．３　サービスデータの保護

Ⅲ．２．３．１【基本】

ユーザのサービス情報、アプリケーション・サーバ等の管理情報や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。

【ベストプラクティス】

i.　業務要件、セキュリティ要件等を考慮して、バックアップ方法（フルバックアップ、差分バックアップ等）、バックアップ対象（ユーザデータ、システム情報等）、バックアップの世代管理方法、バックアップの実施インターバル、バックアップのリストア方法等を明確にすることが望ましい。

⑦ パターンに応じた対策レベルの設定

○ 導出した対策項目に対し、ASP・SaaSサービスのパターン間で異なるCIA要求レベルを対応付けするため、各対策項目に対策の実施レベルを設定

○ 対策項目を実施する際、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となる「評価項目」を設定

○ 各評価項目に対し、対策項目の実施レベルの目安となる「対策参照値※」を設定

○ その際、CIAとの関連性に応じて最大で6パターンのレベル差を持った値を設定し、ASP・SaaSサービスのパターンと対応付け

○ 「対策参照値」の設定にあたり、「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」を参照

○ ASP・SaaS事業者の実態を反映するため、関連分野の専門家の知見を積極的に取り入れつつ検討を実施

ASP・SaaSサービスのパターンと対策実施レベルの対応（イメージ）

パターン判定するASP・SaaSサービス　C:低 I:高 A:高（パターン4）

対応するパターンの値を採用することで対応付け

	機密性	高			低		
	可用性	高	中	低	高	中	低
	パターン分類	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
対策項目	評価項目1	99.5%以上＊	99%以上＊	95%以上＊	99.5%以上＊	99%以上＊	95%以上＊
	評価項目2	【5時間/1年】	【24時間/1年間等】	【24時間/1年間等】	【5時間/1年】	【24時間/1年間等】	【24時間/1年間等】

・・・（以下対策項目が繰り返す）

※CIA関連性に応じて対策参照値にレベル差

※実施レベルの目安であるが、情報セキュリティ対策を確保する上で特に達成することが必要と考えられる値については、「＊印」を付して表示

（参考）「物理的・技術的」対策の概略

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

- 稼動監視（応答確認）
- 障害監視（正常動作の確認）
- 時刻同期の方法の規定・実施
- 異常検知時の利用者への通知
- ぜい弱性情報の収集、パッチ更新
- 運用・管理に関する手順書の策定

2. アプリケーション、プラットフォーム、サーバ・ストレージに対する情報セキュリティ対策

- サービス稼働率・定期保守時間の規定
- 利用状況等のログ取得・保存
- ウィルス対策の実施
- 定期的なバックアップの実施

3. ネットワークに対する情報セキュリティ対策

- アクセス制御方針の策定
- アクセス制御の許可・無効化手順の策定
- 適切な認証方法によるなりすまし対策の実施
- 不正アクセス防止措置の実施
- サーバ証明書によるフィッシング等の防止

4. 建物、電源（空調等）に対する情報セキュリティ対策

- 停電・電力障害発生時の電源確保
- 火災検知・通報システム及び消火設備の具備
- 落雷（直撃・誘導雷）対策の実施
- 個人認証による入退室記録の作成・保存
- 入退室の管理手順書の作成
- サーバルームやラックの鍵管理

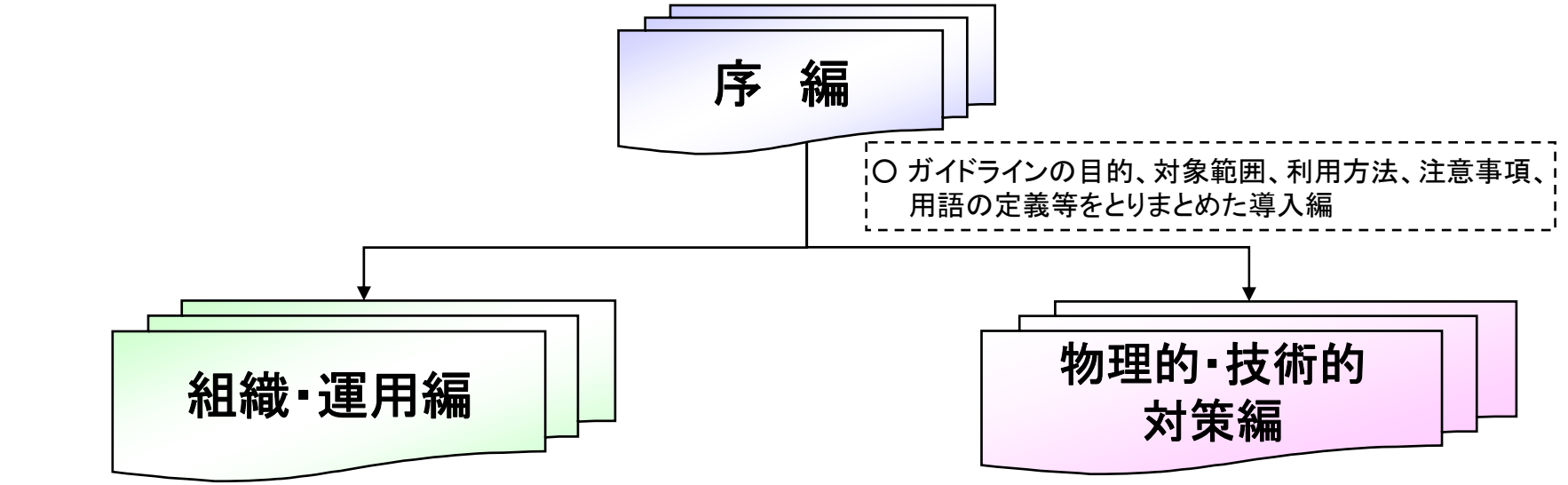
5. その他の情報セキュリティ対策

- 個人情報の取扱に関する法令遵守
- 運用管理端末におけるウィルス対策等の実施
- 記録媒体の適切な保管・管理の実施

情報セキュリティ対策ガイドラインの特長

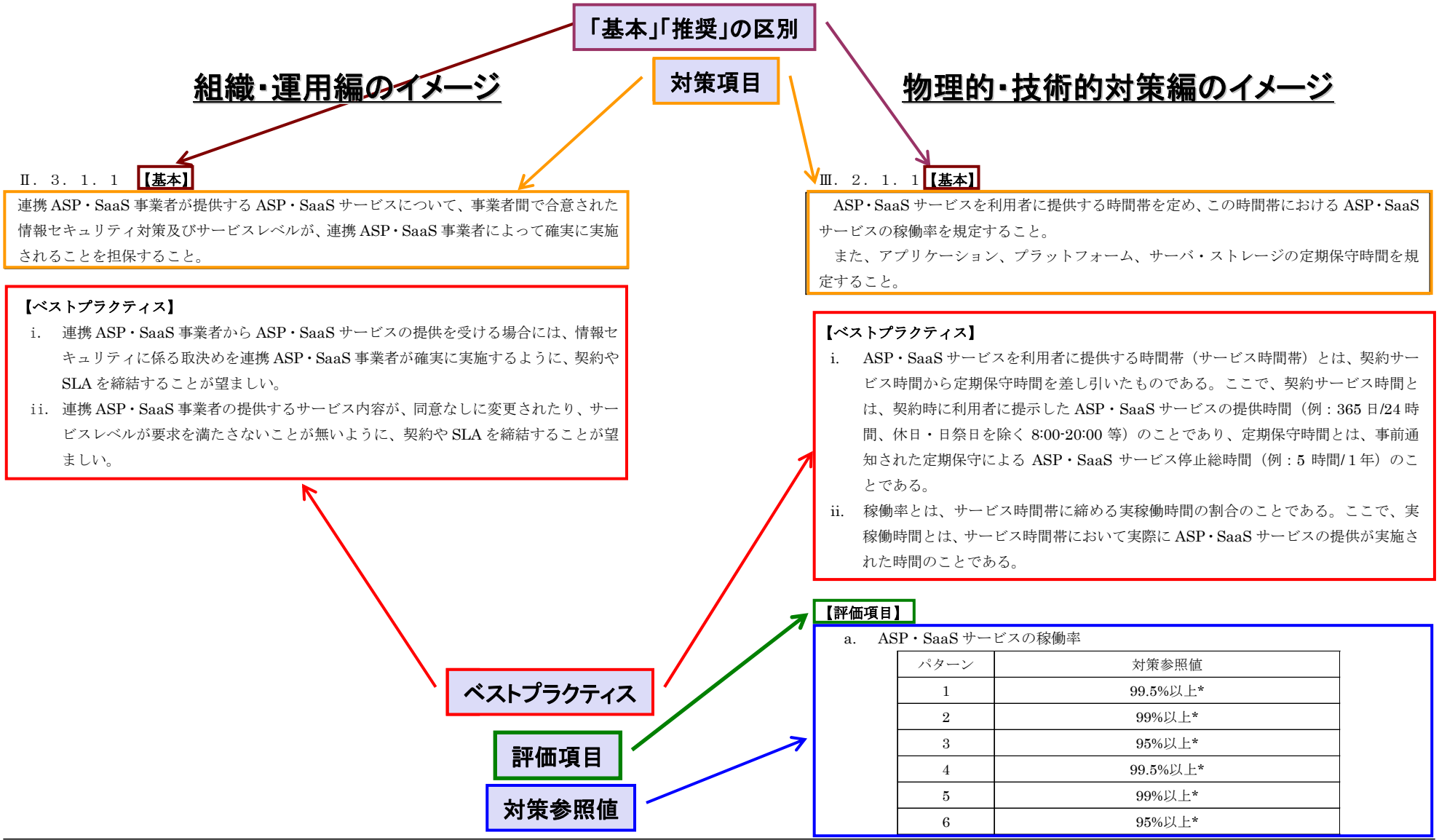
- ASP・SaaS事業者がASP・SaaSサービスを提供する際、実施すべき情報セキュリティ対策全般を対象※。
- 積極的かつ幅広い利用を促すため、可能な限り分かりやすく、かつ使いやすいものになるように留意して作成しており、「序編」、「組織・運用編」及び「物理的・技術的対策編」の3編から構成。

「ASP・SaaSにおける情報セキュリティ対策ガイドライン」の構成



※ 利用者がASP・SaaS事業者との契約の範囲外で独自に利用するハードウェア及びソフトウェア、並びに利用者が契約する通信回線及びインターネット・サービスにおける情報セキュリティ対策を除く

（参考）情報セキュリティ対策ガイドラインの記載内容（イメージ）



情報セキュリティ対策ガイドラインの利活用効果と今後の課題

● ガイドラインの利活用により、ASP・SaaS業界の活性化と健全な発展が期待できる。
● そのためには、ガイドラインの幅広い普及とASP・SaaSの利用環境の変化に応じた見直し・改善が必要。

ガイドラインの利活用により期待される効果

○ ASP・SaaS事業者による適切な情報セキュリティ対策実施の促進（中小・新規参入事業者の取組の促進）
○ 連携ASP・SaaS事業者に対する情報セキュリティ要求事項の指針として活用
○ 利用者に対する情報セキュリティ対策実施状況の提示内容の指針として活用
○ ASP・SaaS事業者の情報セキュリティ対策実施状況の妥当性を、利用者が評価する際の指針として活用

○ ASP・SaaS業界全体の情報セキュリティレベルの底上げ、利用者も含めた情報セキュリティに対する意識向上

ASP・SaaS業界の活性化と健全な発展が期待できる

今後の課題

○ ガイドラインの幅広い普及の促進

ASP・SaaS事業者の対策実施のガイドラインとしてのみでなく、利用者との契約におけるSLAの設定基準、あるいは利用者への実施状況の公表など、業界における積極的な活用及びそれによるガイドラインの認知拡大を期待

○ ASP・SaaSの利用環境の変化に対応した見直し・改善

技術の進歩などASP・SaaSサービスを取り巻く環境の変化に伴って、ガイドラインの内容が陳腐化し、実態にそぐわなくなるおそれ
→ 継続的に見直し・改善を行う体制の構築を期待

ASP・SaaS業界による普及促進及び継続的見直し・改善を期待

（参考）「ASP・SaaSの情報セキュリティ対策に関する研究会」報告書 目次