資料2-5

ASP・SaaSの情報セキュリティガイドライン検討に向けての論点整理

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8月8日

目次

ページ

●論点1：ASP・SaaSの定義 …… 2

●論点2：2005年以降のASP・SaaSの進化と情報セキュリティ要求の変化 …… 3

●論点3：ASP・SaaSの構成の類型化 …… 4

●論点4：ASP・SaaSの典型的な構成要素 …… 9

●論点5：ASP・SaaSのサービス分類について …… 10

●論点6：ASP・SaaSのリスク分析の流れ …… 12

●論点7：既存の基準・ガイドラインと認証制度の課題 …… 13

●論点8：ASP・SaaSの情報セキュリティガイドラインの役割と期待 …… 15

論点1：ASP・SaaSの定義

【ASPの定義】

「ASPとは、アプリケーション・サービス・プロバイダの略で、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。」

出典：2004年版ASP白書（ASPIC Japan刊）

※SaaSは「ユーザーがネットワーク経由でWebベースのソフトウェア機能にアクセスできるようにしたソフトウェア形態」として解釈されているが、明確な定義が存在するわけではない。

本研究会では、ASPとSaaSを特に区別せず「ASP・SaaS」と連ねて呼称し、その定義については上記に基づくこととする。

論点2：2005年以降のASP・SaaSの進化と情報セキュリティ要求の変化

2005年を境にASP・SaaSは急速に多様化してきており、これに伴ってASP・SaaSに求められる情報セキュリティ要求も変化している。

	2005年以前	2005年以降	情報セキュリティ要求の変化
実現形態の多様化	シングルアプリケーション	マルチベンダーマルチアプリケーション（マッシュアップ）	提示内容や項目の標準化等により、ベンダー間で情報セキュリティに対する共通理解を熟成することが求められる
提供サービスの多様化	グループウェア等の共通アプリケーション	★基幹系サービスの広がりビジネスプロセスサービス、IT基盤サービス、業務別・分野別アプリケーション	情報セキュリティ要求が高く求められる基幹系サービスの割合が高まり、要求レベルの広がりと対策の多様化が進んでいる

論点3：ASP・SaaSの構成の類型化

ASP・SaaSの構成は以下の4ケースに類型化することができる。この類型化に基づいて、情報セキュリティ上の脅威想定を検討することができる。

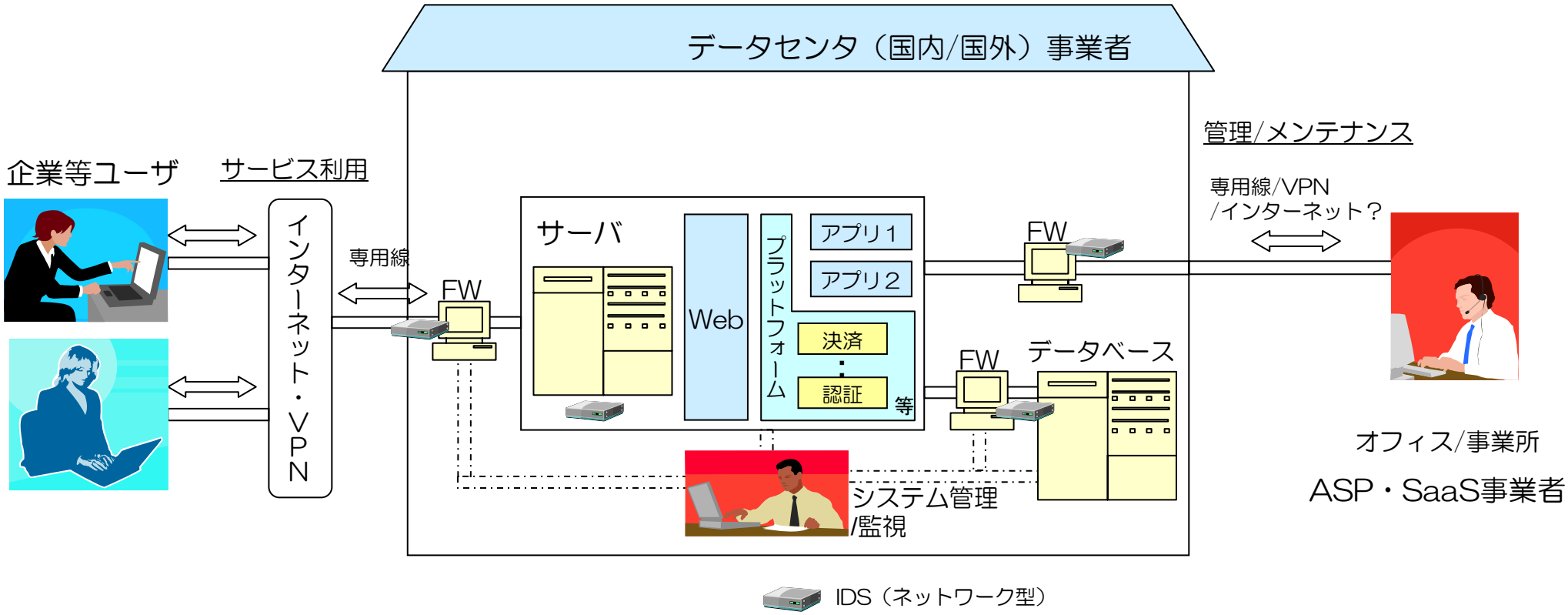
1. ASP・SaaS事業者がデータセンター事業者を活用する場合 （5ページ）

2. ASP・SaaS事業者自らが設備等を管理する場合 （6ページ）

3. 一般ユーザ等が画面表示のみを統合化する場合 （7ページ）

4. ASP・SaaS事業者が業務提携する場合＜事業者間でサーバ連携あり＞ （8ページ）

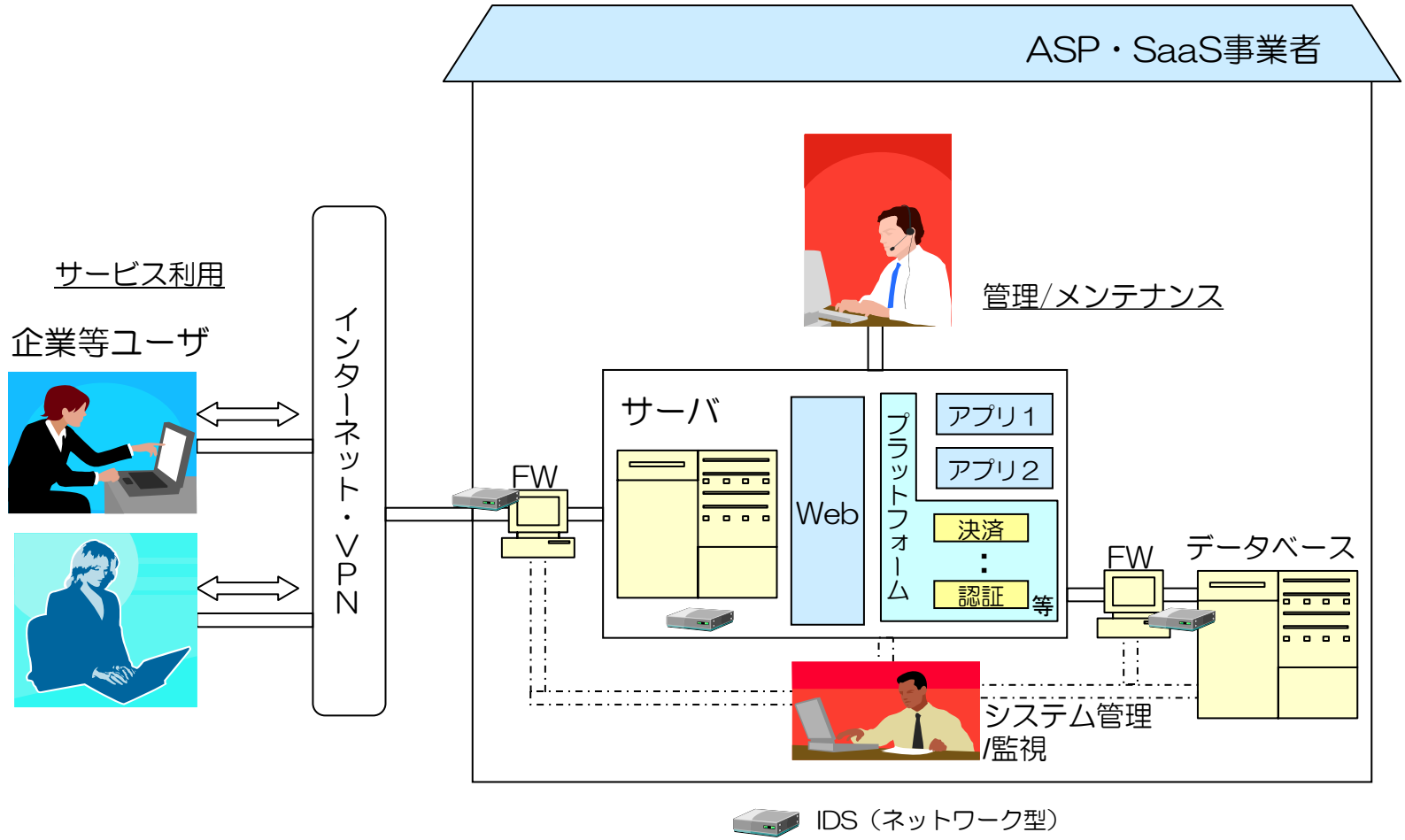
ASP・SaaSの構成の類型化　～ケース1：ASP・SaaS事業者がデータセンタ事業者等を活用～



☆ FW、IDS、ログ監視等のセキュリティ対策をASP・SaaS事業者が自ら構築・維持管理しているか、それともデータセンタ事業者等にアウトソーシングしているかに注意が必要

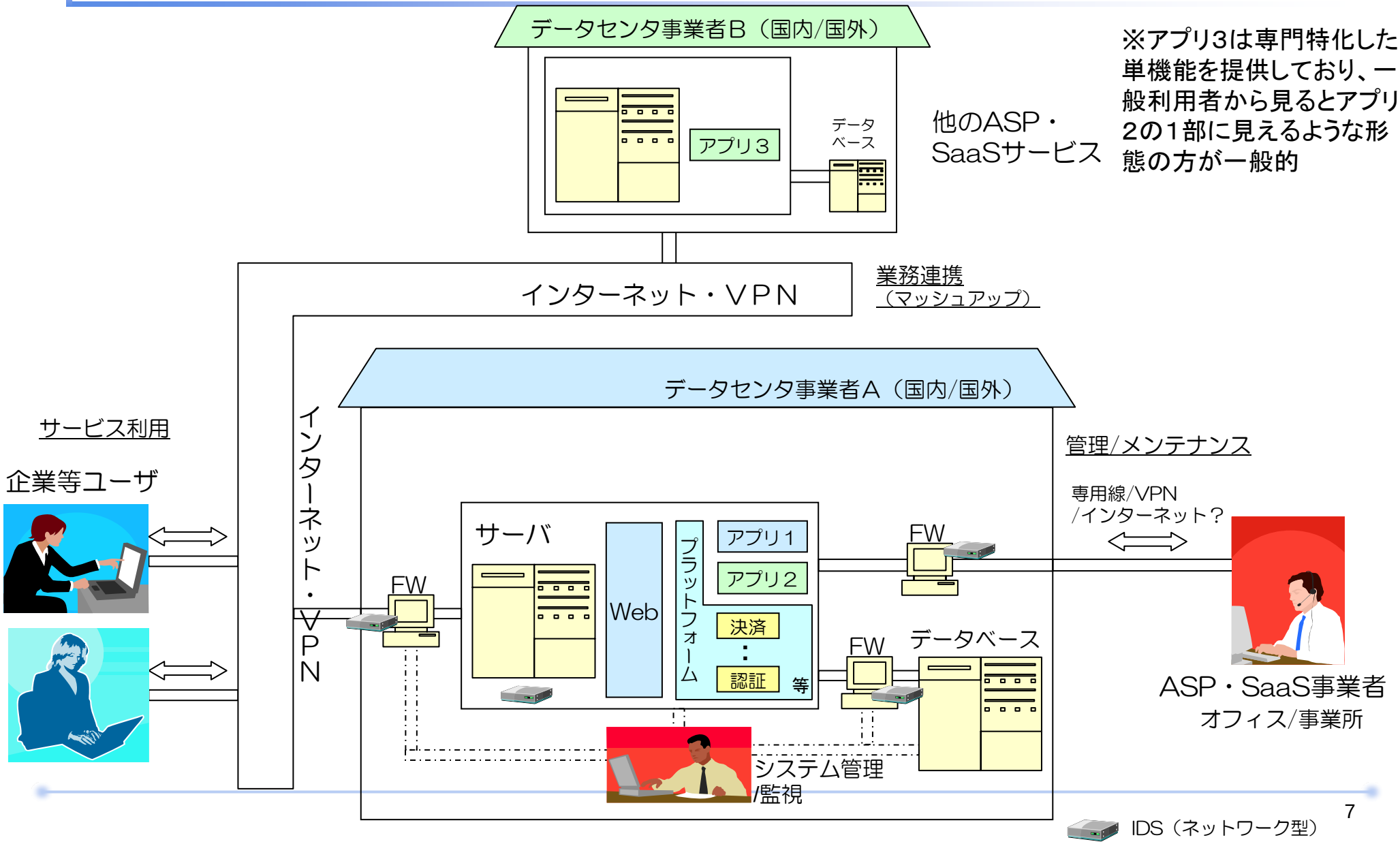
☆ サーバ、FW等のOSレベル維持管理のみをデータセンター事業者等にアウトソーシングしている事例も見られる

ASP・SaaSの構成の類型化　～ケース2：ASP・SaaS事業者自らが設備等を管理～

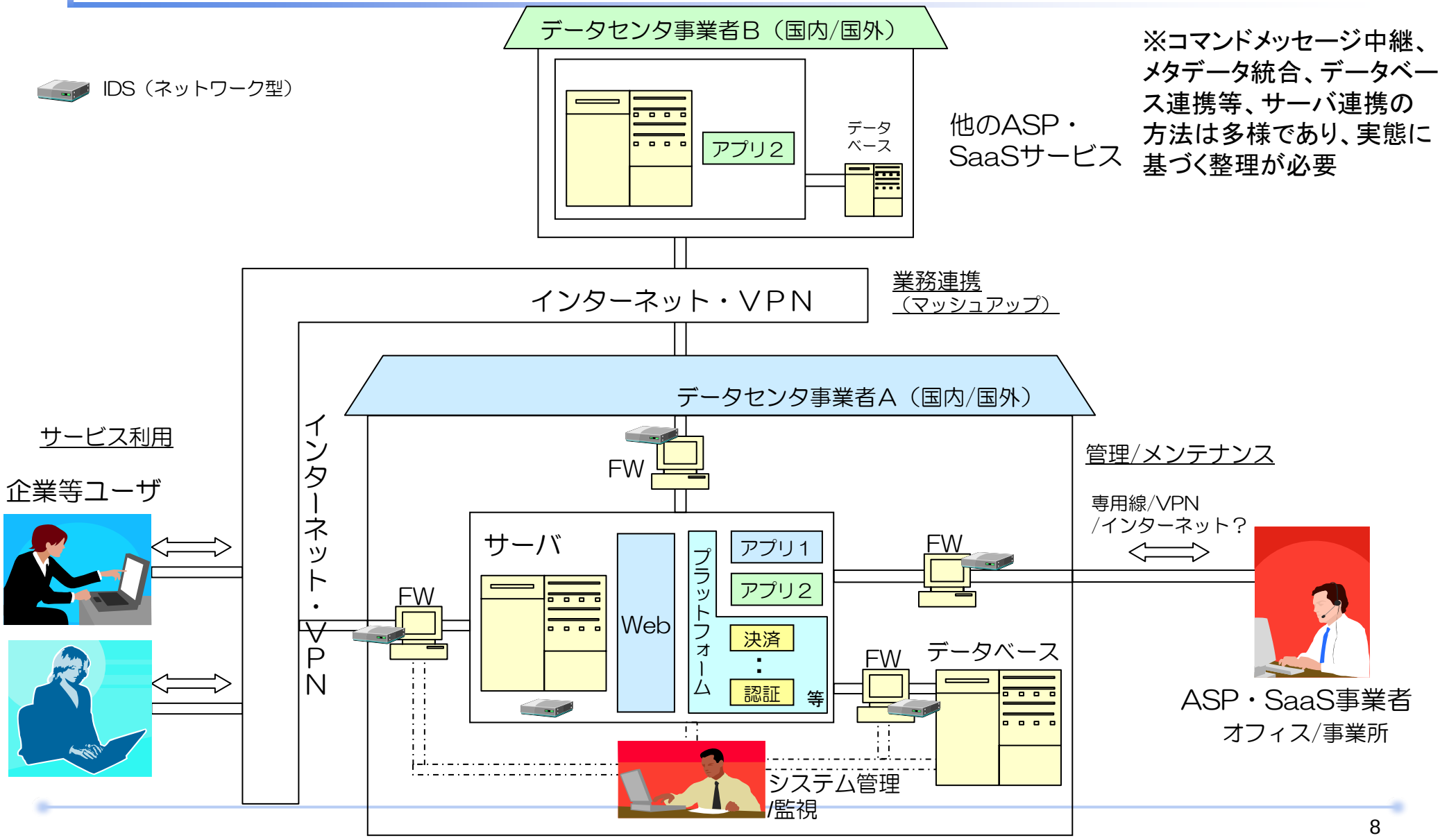


☆ ウィルスやサーバー負荷分散等の対策として、ISPの提供するアプライアンスサービス等を利用する可能性が想定される

ASP・SaaSの構成の類型化　～ケース3：一般ユーザ等が画面表示のみを統合化する場合～

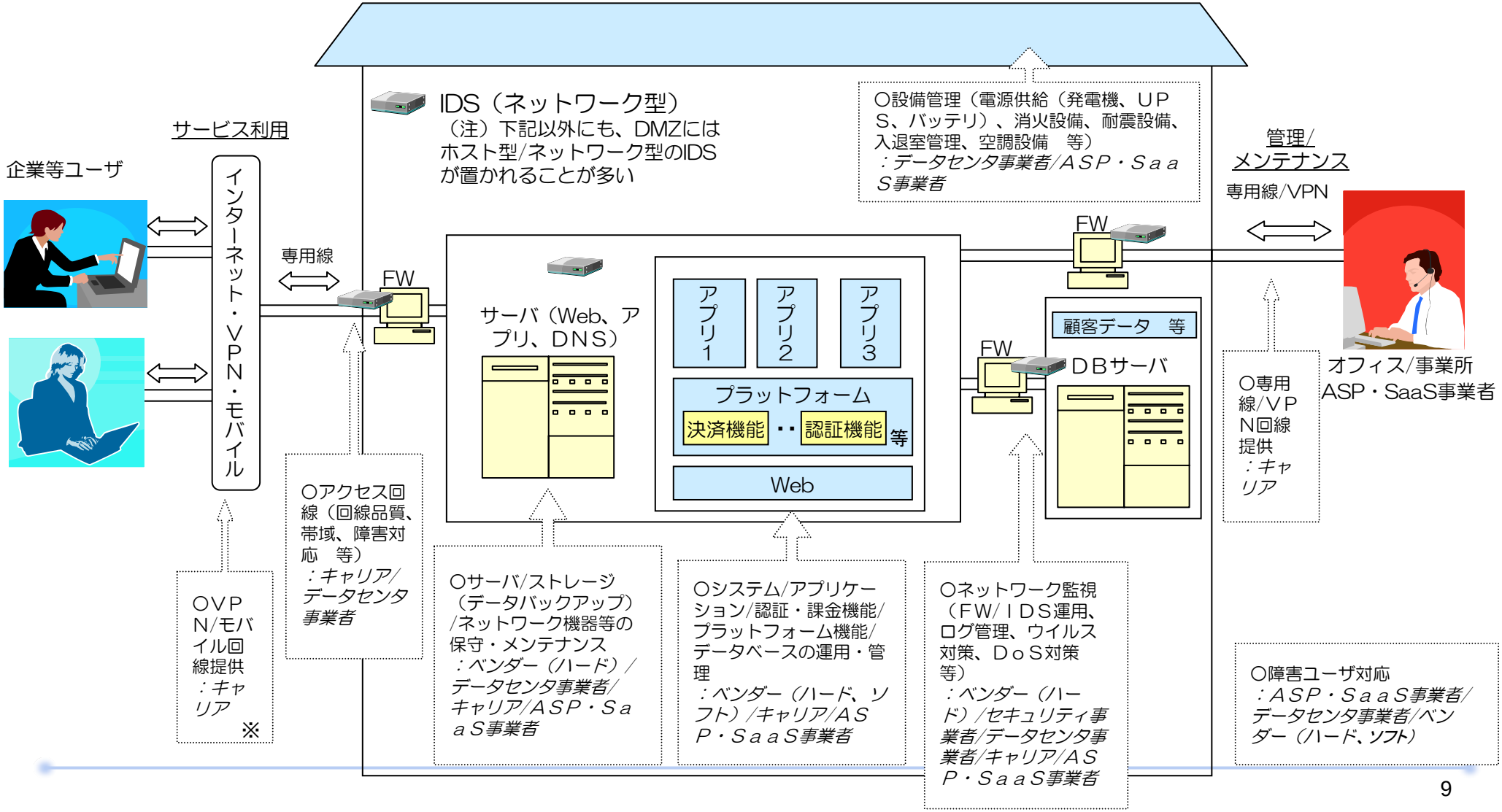


ASP・SaaSの構成の類型化 ～ケース4：ASP・SaaS事業者が業務連携 ＜事業者間でサーバ連携あり＞～



論点4：ASP・SaaSの典型的な構成要素

ASP・SaaSの4つの類型に基づくと、その典型的な構成要素は下図のように整理される。構成要素の洗い出しにより、ASP・SaaSの情報セキュリティリスク分析における情報資産の特定に資することができる。



※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

論点5：ASP・SaaSのサービス分類について

ASP・SaaSにおいて重点的に守るべき情報資産は、一般利用者の業態（業種）やサービス種別（会計、CRM、SFA、グループウェア、メール配信・・・）により異なるものと考えられる。

ASP・SaaSのリスク分析に資するように、本研究会では業種やサービス種別毎に重点化すべき情報資産が何であるのかを研究する必要がある。

【重点化すべき情報資産の検討イメージ】

大分類	分析軸		情報資産洗い出しの視点等
公共向けASP・SaaS	電子政府・自治体関連サービス		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」に基づく検討
民間向けASP・SaaS	利用者業種とサービス種別の2つの軸で分類を設定	利用者業種による分類	業種に特化した重要な情報資産とは？ 業種共通の重要な情報資産とは？
		サービス種別による分類	サービス特有の重要な情報資産とは？ サービスに拠らない重要な情報資産とは？

ベース資料

参照・活用

（参考） 公共ITアウトソーシングに関するガイドラインについて

「e-Japan重点計画－2002」では、「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の促進」が重点政策5分野の1つとして位置付けられ、電子自治体の構築が推進されたが、人材確保、期間確保、財源確保等が課題であった。そこで、公共ITを民間にアウトソーシングし、住民サービスの向上、IT投資コスト削減、調達適正化、地方公共団体への技術的支援、地域経済活性化、地方公共団体における業務改革の推進等の効果を得る方針が打ち出された。

しかしながら、地方公共団体のIT共同アウトソーシングには、自治体側の経験不足、標準的な契約書式が無い、サービス選択が難しい等の問題点が指摘された。そこで、総務省では平成15年度に「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」を策定した。

【「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」が対象としているサービス】

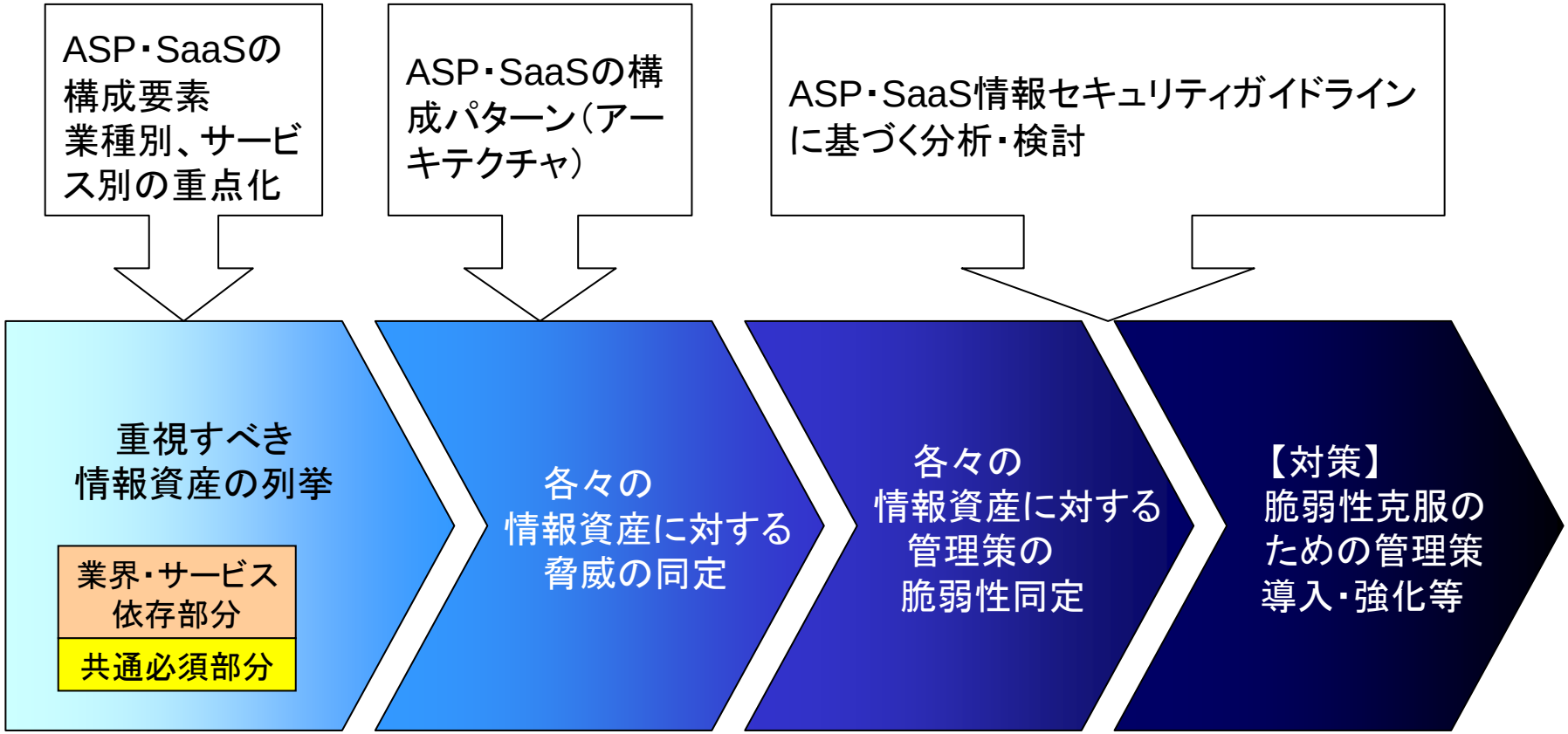
1. サービスサポート
2. セキュリティ
3. アプリケーション
4. ホスティング
5. ネットワーク
6. ハウジング

このガイドライン事例は、今回のASP・SaaSの情報セキュリティガイドライン作成の骨格を構成する素材として活用することができる。

論点6：ASP・SaaSのリスク分析の流れ

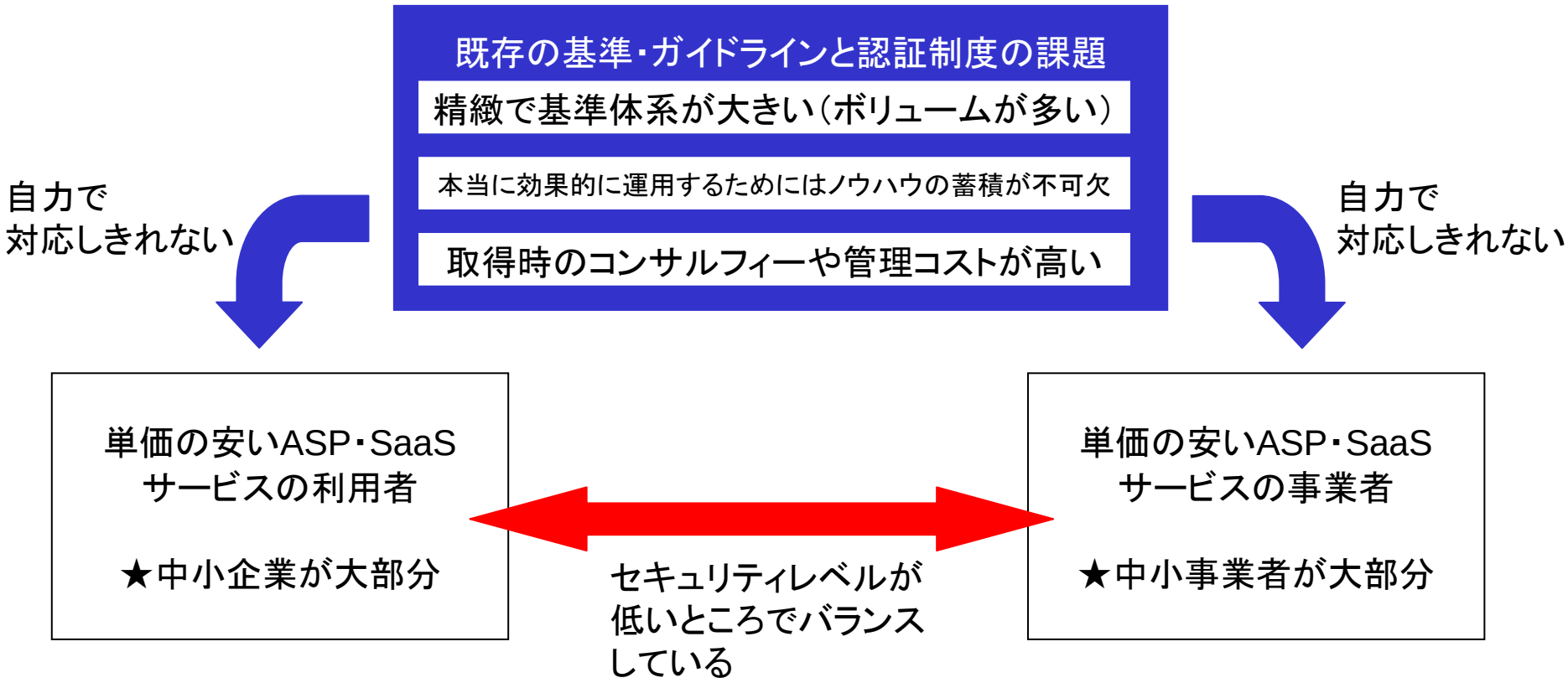
ASP・SaaSの情報セキュリティガイドラインは、下記のような情報セキュリティリスク分析の流れを支援することが期待される。

また、このガイドラインは、業種やサービスに依存しない共通必須部分(コア部分)と、業種やサービス別に選択的に適用されるオプション部分から構成されるべきである。



論点7：既存の基準・ガイドラインと認証制度の課題

現在、既存の基準・ガイドラインと認証制度（例：ISO 27001とISMS認証制度）は社会的認知と普及が進み、社会全体の情報セキュリティ向上に貢献している。しかしながら、精緻で基準体系が大きい（ボリュームが多い）こと、本当に効果的に運用するためにはノウハウの蓄積が不可欠であること、管理コストが高いことなどが災いして、ASP・SaaSに関しては下記の課題が生じている。



（参考）ノウハウ不足によって既存の認証制度等がうまく回らない例

ノウハウ不足により、既存の認証制度等がうまく機能しなかったり、コスト過剰になったりする例について以下に示す。

（例）

既存の基準・ガイドラインで陥りやすい問題
・どこまで対策すべきかの判断ができないため過剰な対策になる傾向がある
・リスクアセスメントの方法を誤ると、本来守るべき情報資産が対象にならない場合がある
・コンサルタントに大きく依存すると、不在時に運用が回らなくなる
・形式的に運用を行っているだけでも認証を継続できる場合がある （PDCA運用の形骸化）

論点8：ASP・SaaSの情報セキュリティガイドラインの役割と期待

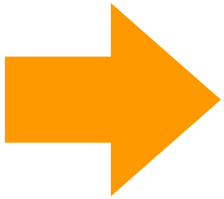
ISMS等の既存の基準・ガイドラインを本当に効果的に運用していくためには、ある程度のノウハウが必要である。既存の基準・ガイドラインに頼らなくても容易に適用可能な業界標準としてのガイドラインを活用することで、ASP・SaaSの情報セキュリティを向上させることが可能になる。

ASP・SaaSの情報セキュリティガイドラインに対しては、既存の基準・ガイドラインが持つ課題、特にそのノウハウとコストに関する課題を解決することが期待されている。

（例）

既存の基準・ガイドラインで陥りやすい問題

- ・どこまで対策すべきかの判断ができないため過剰な対策になる傾向がある
- ・リスクアセスメントの方法を誤ると、本来守るべき情報資産が対象にならない場合がある
- ・コンサルタントに大きく依存すると、不在時に運用が回らなくなる
- ・形式的に運用を行っているだけでも認証を継続できる場合がある （PDCA運用の形骸化）



解決策

業界標準としてのガイドラインを適用する

- ・ASP・SaaS業界標準として最低限の対策を網羅したガイドラインという位置づけであるため、どこまで対策を講じるべきかの判断が明確になる
- ・ ASP・SaaS業界の類型毎にリスクアセスメントされた結果がガイドラインに反映されているため、組織が独自に行うべきリスクアセスメント作業を軽減し、適切なセキュリティ対策を構築することができる
- ・ ASP・SaaS業界のために策定されたガイドラインであるため、大きなカスタマイズを必要としない。
  従って、コンサルタントに頼らずにセキュリティを構築し、運用していくことが可能となる

ガイドラインの適用結果を公表する

- ・ガイドラインの適用状況を対外的に公表することで、その説明責任により運用における自己点検機能の向上が期待される

ASP・SaaSの情報セキュリティガイドラインが中小企業に対して及ぼす効果の期待

ASP・SaaSの情報セキュリティガイドラインは、中小企業ユーザと中小事業者の両者を活性化する役割を担うことを期待されている。両者のマッチアップ及び事業者間のマッシュアップの民ー民ベースでの活性化、投資資金の調達促進等の効果が期待される。