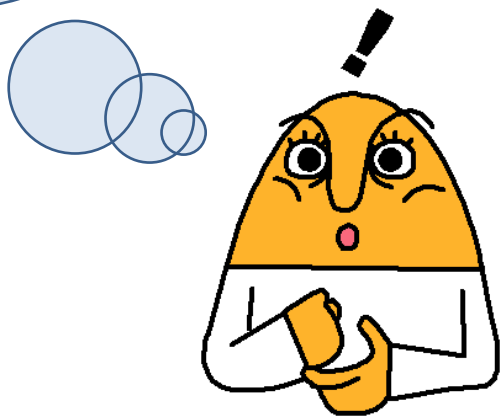
クラウド時代の
セキュリティガバナンスの考え方と実践

株式会社ディアイティ セキュリティサービス事業部
河野省二, CISSP <shoji@dit.co.jp>

クラウドコンピューティングとは

コンピュータリソースを
ネットワーク上に配置し、
サービスとして利用する環境



本日のアジェンダ

- クラウドコンピューティングとクラウドサービス
  - 情報セキュリティのフレームワークを利用して、クラウドのセキュリティを正しく考える
  - ITセキュリティの最重要課題とはなにかを考える
- セキュリティガバナンスとクラウドサービス
  - ポリシーマネジメントの限界
  - 情報セキュリティマネジメントに足りない基準？
- クラウドサービスとセキュリティマネジメント
  - ISMSとクラウドサービス
  - プライバシーマークとクラウドサービス

本資料はドラフト版です。当日の資料は(ISC)2のホームページからダウンロード可能です。

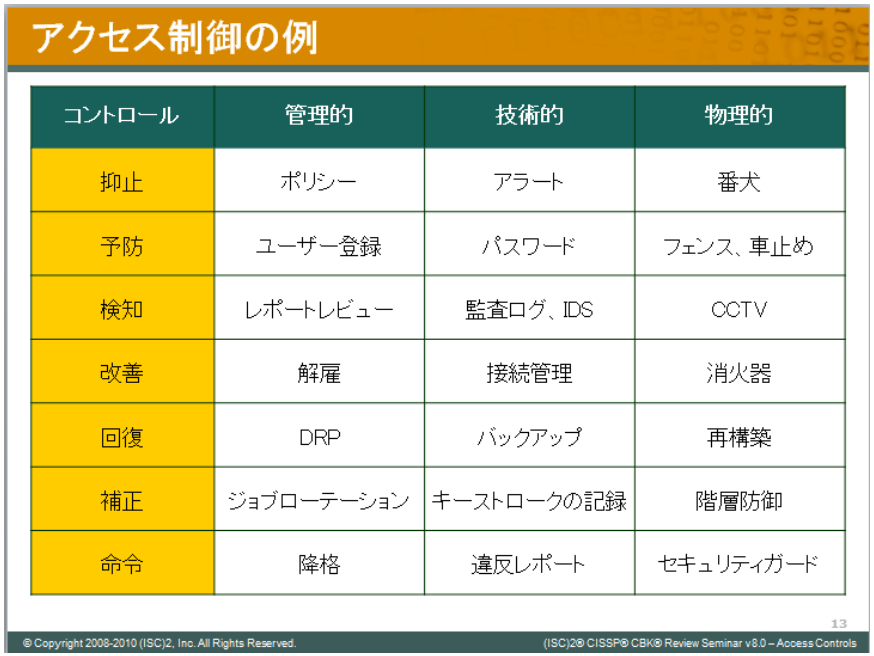
クラウドコンピューティングとクラウドサービスの違いをよく理解して、
リスクアセスメントに活かす

クラウドコンピューティングとクラウドサービス

クラウドはサービスである。

- クラウドコンピューティング
  - クラウドを構成するシステム環境
  - 仮想化や分散処理をはじめとした技術によって構成されたシステム環境であり、ネットワークを通じたコンピュータリソースの提供を実現する
- クラウドサービス
  - ネットワークを通じてリソースを提供するサービスおよび付帯サービス
  - 提供されるリソースに応じて、クラウドサービスプロバイダ（CSP）が、利便性の高い付帯サービスを提供することで、IT環境を構築するのに役立てることができる

CISSPのテキストでは・・・



アクセス制御の例

コントロール	管理的	技術的	物理的
抑止	ポリシー	アラート	番犬
予防	ユーザー登録	パスワード	フェンス、車止め
検知	レポートレビュー	監査ログ、IDS	CCTV
改善	解雇	接続管理	消火器
回復	DRP	バックアップ	再構築
補正	ジョブローテーション	キーストロークの記録	階層防御
命令	降格	違反レポート	セキュリティガード

セキュリティ対策のマトリクスを作成する

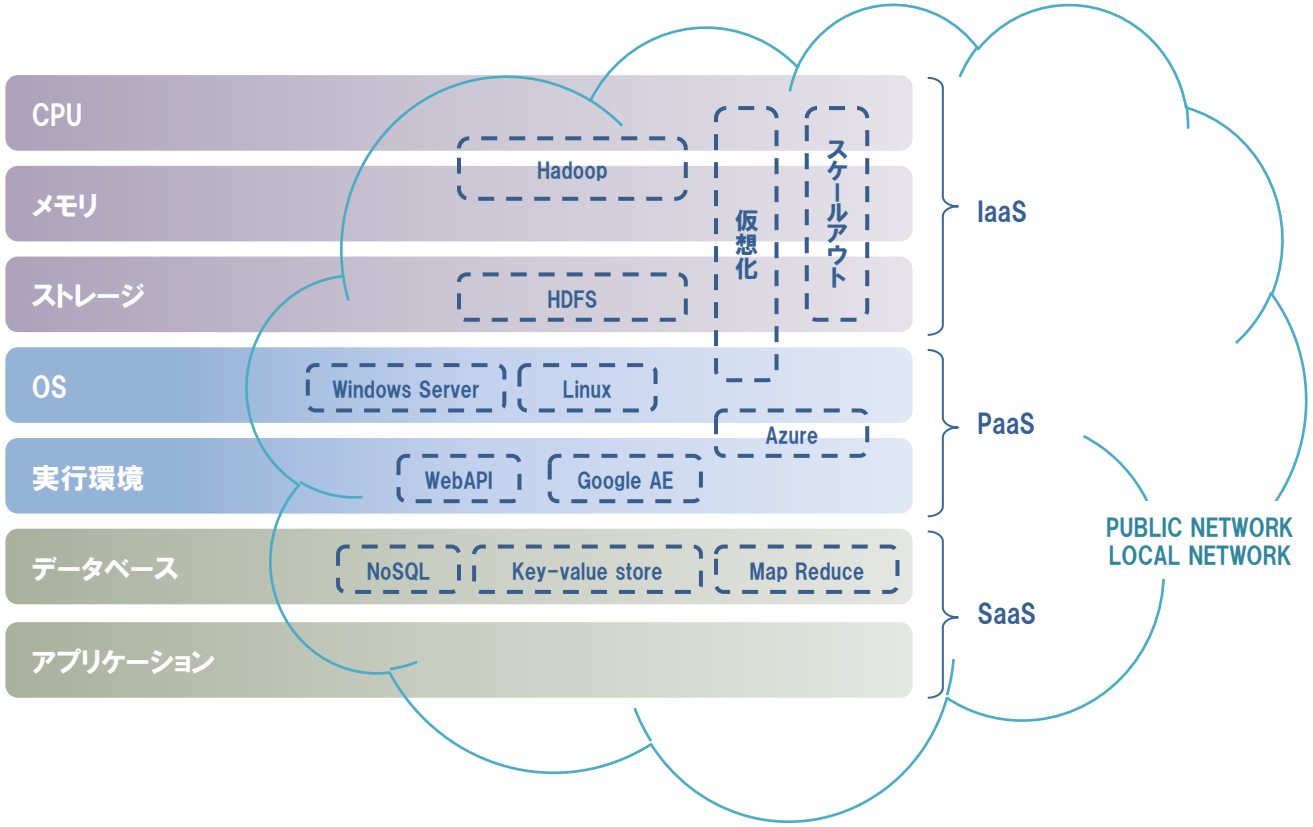
管理的、技術的、物理的の3つの観点から、全体最適化されたセキュリティ対策を実現する

CISSPオフィシャルセミナーテキスト
「アクセスコントロール」からの引用

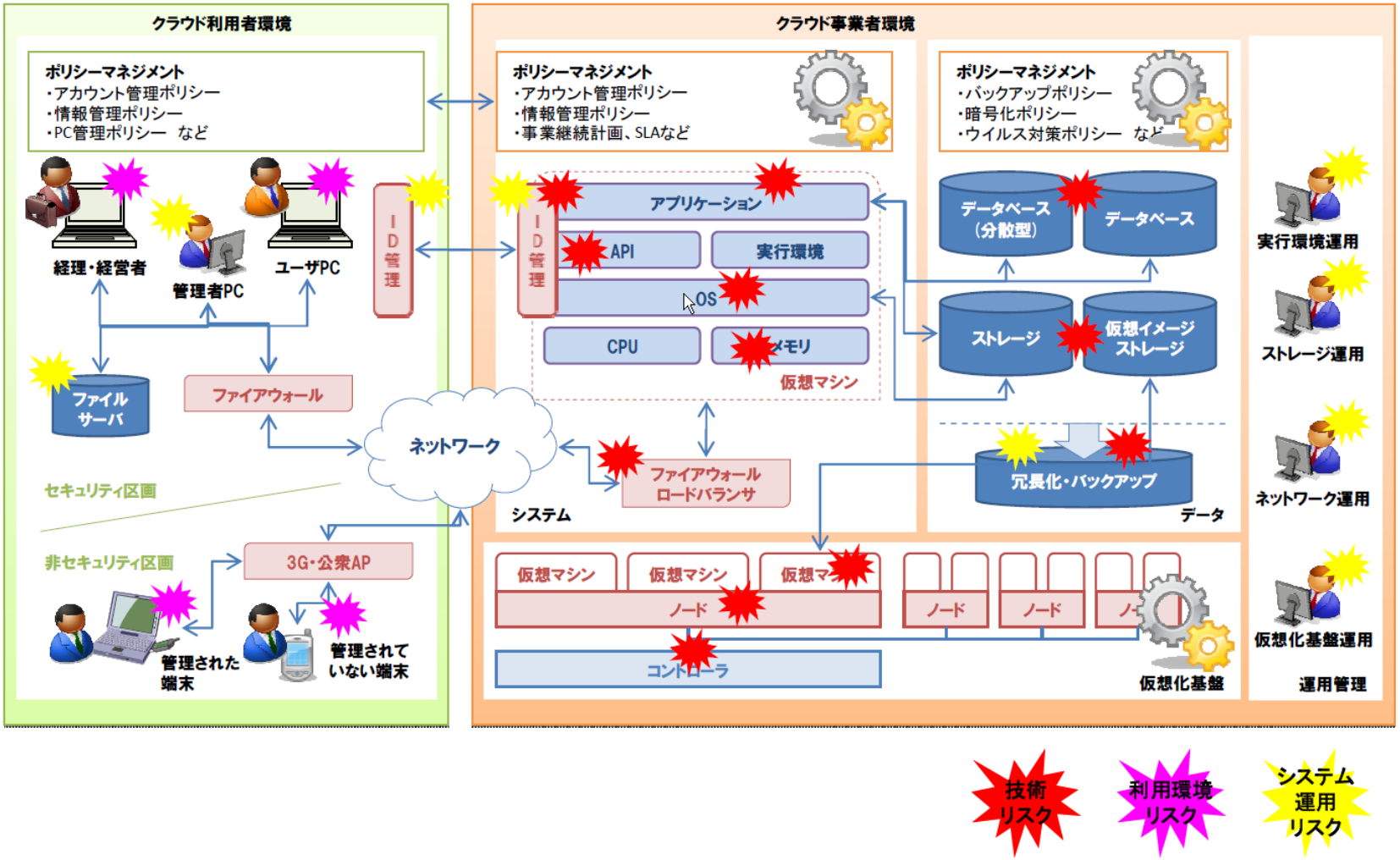
- セキュリティ対策の網羅性を確保する
  - クラウドコンピューティングにおけるセキュリティ対策は主に技術的セキュリティ対策によって実施できる
  - クラウドサービスにおけるセキュリティ対策については主に管理的セキュリティ対策によって実施できる
  - データセンターセキュリティは物理的セキュリティによって対策できる
- 本マトリクスにはリスクが記載されていない
  - リスクは表の裏に隠れている

クラウドによって提供されるリソース

クラウドとは、従来手元にあったコンピュータ環境をネットワーク上に配置し、必要に応じて利用すること



クラウドの環境とセキュリティのポイント



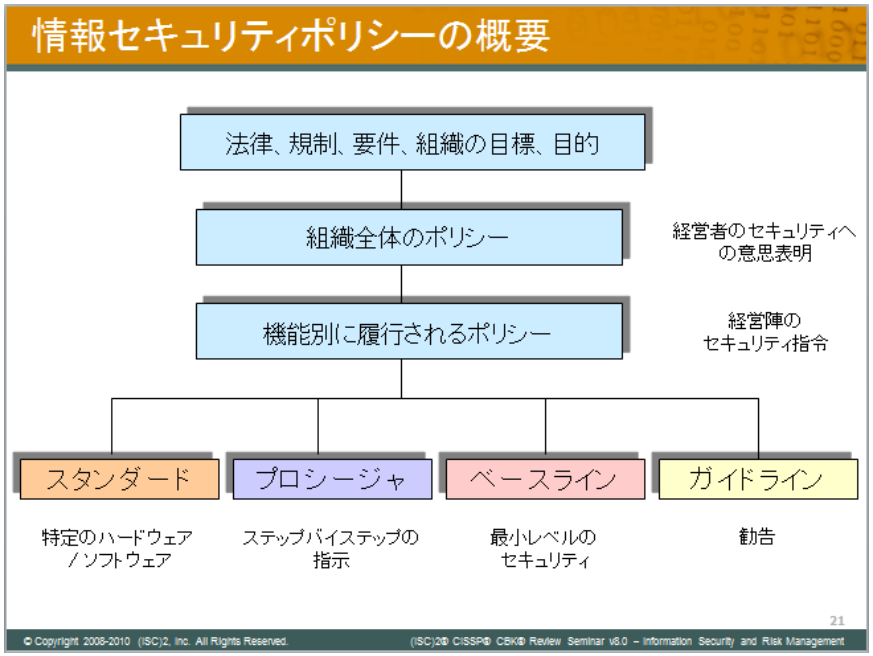
現場ではセキュリティ対策が正しく実施されているか
セキュリティ対策を改善するための情報を入手できているか

セキュリティガバナンスとクラウドサービス

クラウドにおけるセキュリティガバナンス

- セキュリティガバナンス
  - コーポレート・ガバナンスと、それを支えるメカニズムである内部統制の仕組みを、情報セキュリティの観点から企業内に構築・運用すること（経済産業省の定義）
- 情報セキュリティガバナンスに必要な情報は手に入れることができるのか
  - たとえばインシデントレスポンスやIDマネジメントのために必要な「ログ」を手に入れることができるのかなどを考える
  - 手に入れることができるとしたら、どのくらいの時間で手に入れることができるのかを考える
  - システムが正しく動いているかどうかを判断することができるか

CISSPのテキストでは・・・



情報セキュリティポリシーの概要

クラウドを利用出来るかどうかについては、スタンダードで規定する。システムの概要について、スタンダードに記載するとともに、最小レベルのセキュリティをベースラインに記載する。

CISSPオフィシャルセミナーテキスト
「アクセスコントロール」からの引用

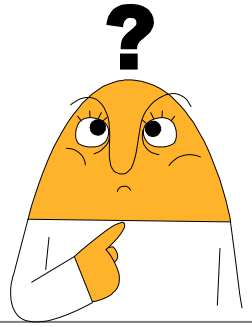
- クラウドサービスを利用出来るかどうかの判断
  - スタンダードでは、ハードウェアやソフトウェア、サービスの利用における標準を規定している
  - クラウドサービス利用時になにをすべきかを、プロシージャやベースラインに記載する
- 規定前の内容はガイドラインに
  - 決定したわけではないが、提案をしたい場合などはガイドラインに記載する

セキュリティガバナンスとクラウドサービス

- セキュリティガバナンス
  - セキュリティを確保できているかどうかを現場レベルで把握する
  - 現場の見える化の実現
- ポリシーマネジメント
  - 環境が異なれば、情報セキュリティ対策も異なるという前提が必要
  - 「PC持ち出し禁止」は中国ではさらにリスクを高めている
- スタンダードとベースライン
  - ベースラインとガイドライン、スタンダードを正しく設定する

ISMSにおけるポリシーマネジメントではベースラインが欠如しているように見える。

CISSPで学ぶ「ベースライン」はISMSではなににあたるのかをかんがえてみよう。



セキュリティマネジメントの基本はリスクマトリクスの作成から

クラウドサービスとセキュリティマネジメント

セキュリティポリシーを他の国で使う

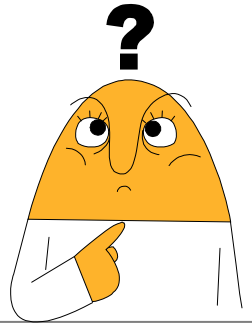
- それぞれの国によってリスクが異なるため、セキュリティポリシーをそのまま持って行っても使えない
  - PCの持ち帰り禁止　→　会社のほうが安全（日本）
  - PCの持ち帰り推奨　→　会社に置いておくほうが危険（中国）
- ポリシーをそのまま運用するのではなく、リスク対応を共通化する
  - 情報資産ごとにポリシーを決めるのではなく、リスクごとに対策を決め、それを個別のポリシーとして策定する
  - 他の国や取引先ではどのようなリスクがあるのかを確認し、リスク受容レベルに応じたセキュリティ対策を実施する
- グローバル展開するクラウドにおけるポリシーマネジメントも同様に考える

クラウドサービスと情報セキュリティマネジメント

- 情報管理はどうなるか
  - パブリッククラウドによって、変化する情報管理リスクにはなにがあるか
- IDマネジメントはどうなるか
  - パブリッククラウドによって、ID管理、アクセスコントロールはどのように変化するか
  - 認証の強度やトレーサビリティについて考える
- 個人情報はどうなるか
  - クラウドで個人情報は使えるのか

そもそもクラウドを利用する目的はなにか？

CISSPなら、「目的」に対して「効果」を検討することで、クラウドに適したITサービスを理解することが出来る



CISSPのテキストでは・・・

リスク受容と費用対効果

セキュリティ対策選択時には、リスクアセスメントの結果を踏まえて、費用対効果を十分に吟味することが重要

CISSPオフィシャルセミナーテキスト
「アクセスコントロール」からの引用

- リスク受容をどのように考えるのか
  - ITマネジメントやセキュリティマネジメントは経営の課題であることを考えて、費用対効果についていつも考えることが重要
- そもそもリスク受容基準があるか
  - 明確なリスク受容基準がなければ、リスク受容レベルを決めることができない

クラウドサービス利用者の不安

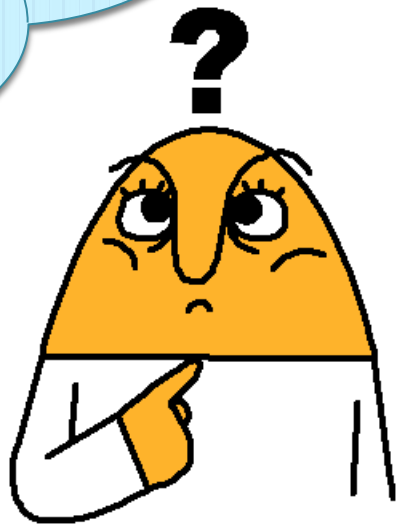
中小企業を主としたアンケートでは、以下の2点が不安要素として挙げられた

■ セキュリティに関する不安

- 自組織の情報がネットワーク上のどこにあるか分からない
- 情報管理をどこまでプロバイダに任せられるかわからない

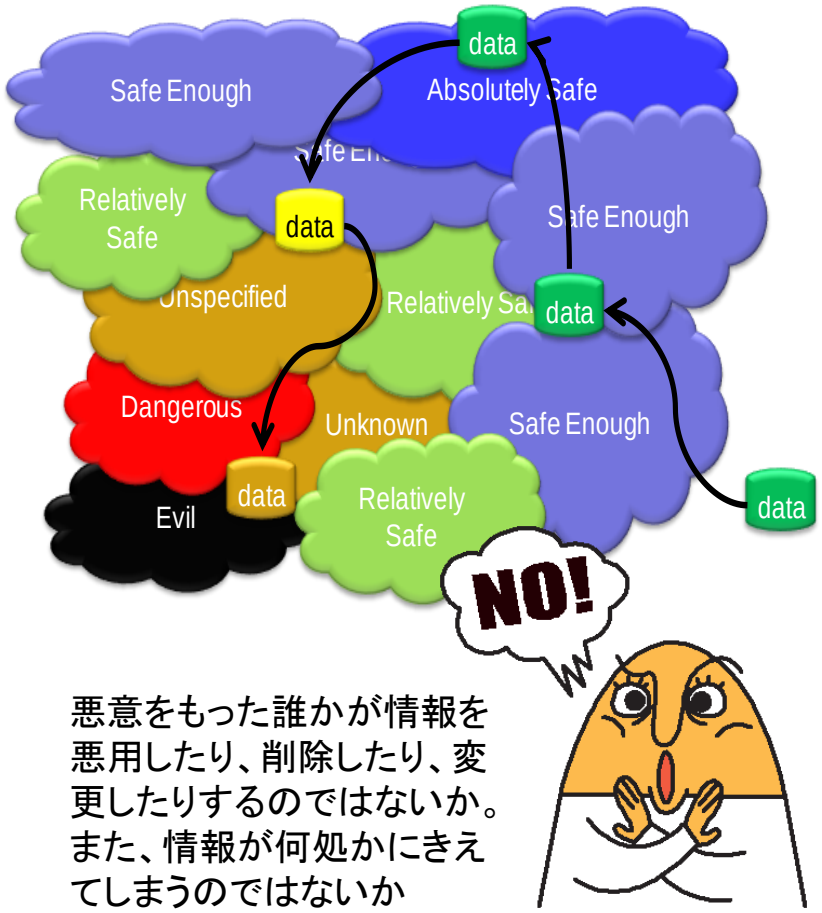
■ コストに関する不安

- サービスコストは低価格に見えるが、付帯する運用コストを考慮すると、価格が見えない
- 移行に関してどのくらいのコストがかかるか見えない



クラウドサービス利用の判断基準となる情報が少ない！
クラウドサービスの見える化が急務！

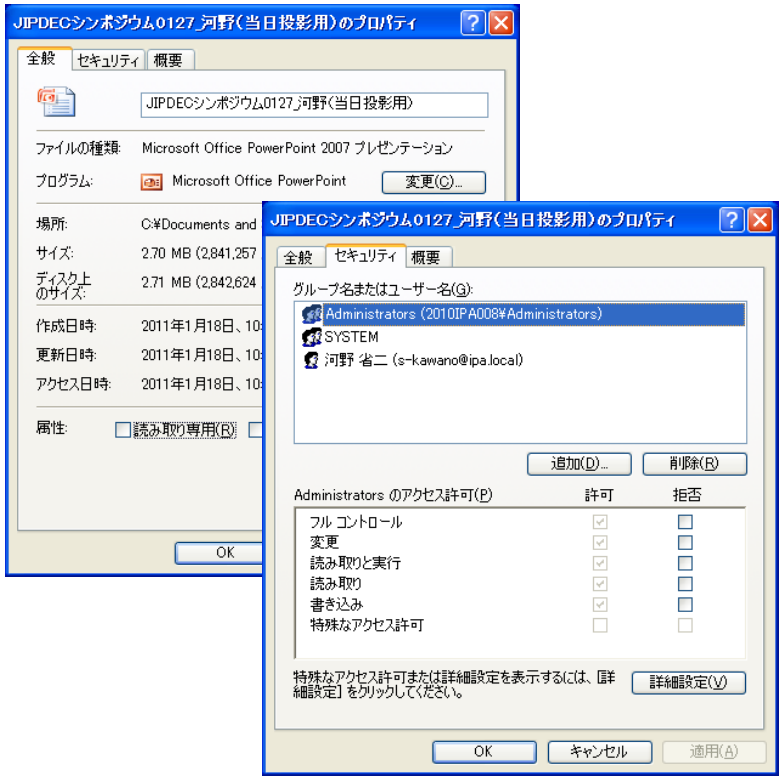
クラウドサービスと情報分類



悪意をもった誰かが情報を悪用したり、削除したり、変更したりするのではないか。また、情報が何処かにきえてしまうのではないか

- クラウドサービスを利用する前に情報分類を行うことが重要
  - クラウドサービスでは、どこに情報が置かれているかわからないという不安がある
- 基本的には、データがどこにあるかという問題は、だれにも明確ではない
  - システムがリアルタイムに理解しているのであり、誰かがそれを特定するのは難しい
  - アクセス権を明確にし、データ管理を行うことが重要

ファイルのプロパティ（メタデータ）

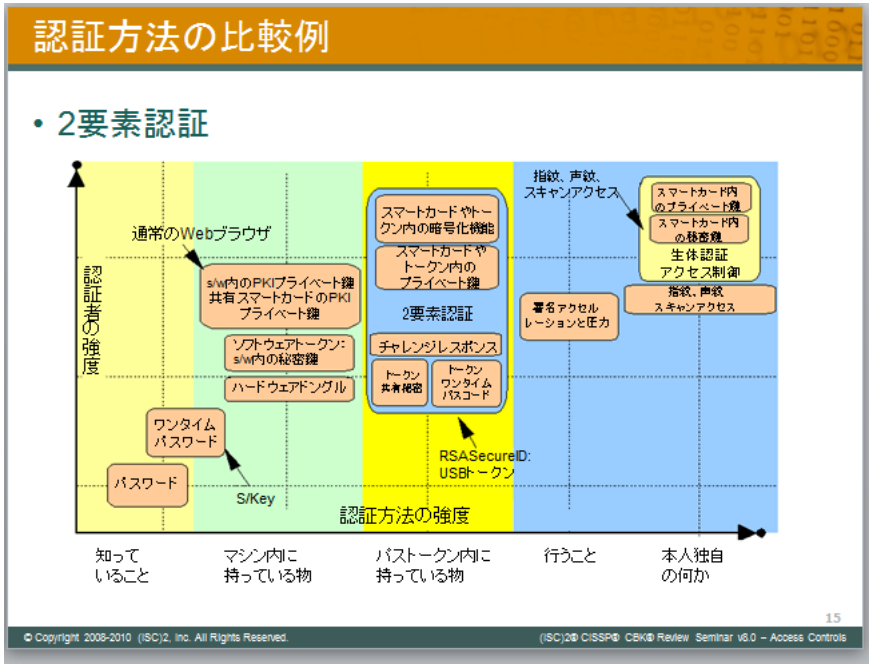


- 管理用のデータがファイルには付属している
  - どのようなファイルにも、OSが管理するためのデータがついている
  - これらの属性をそのまま移行するためのコストを計画しておく必要がある
- クラウドサービスでは新たな管理情報が付与されることもある
  - クラウドサービスを変更する際には理解が必要

リアルタイムコラボレーション

- メールでのファイル添付をしない
  - クラウドサービスを利用してファイル管理を行うことによって、個別の端末にデータを持たなくなる
  - ファイルへのアクセスはアクセス権を設定するだけで、ひとつのファイルに対してそれぞれがデータの更新をする
- 必要なときだけアクセス権の設定をする
  - 情報を収集する際は書き込みをOKにして、情報を共有する際は読み取り専用にするといった対応でセキュリティを確保する
  - 相手の手元にデータが残らない
- 情報管理コストが低減される
  - 持っている情報が極めて少なくなるために、管理コストや監査コストが低減される
  - しかし、ツールなどが提供されていないと一覧などを作ることが難しい

CISSPのテキストでは・・・



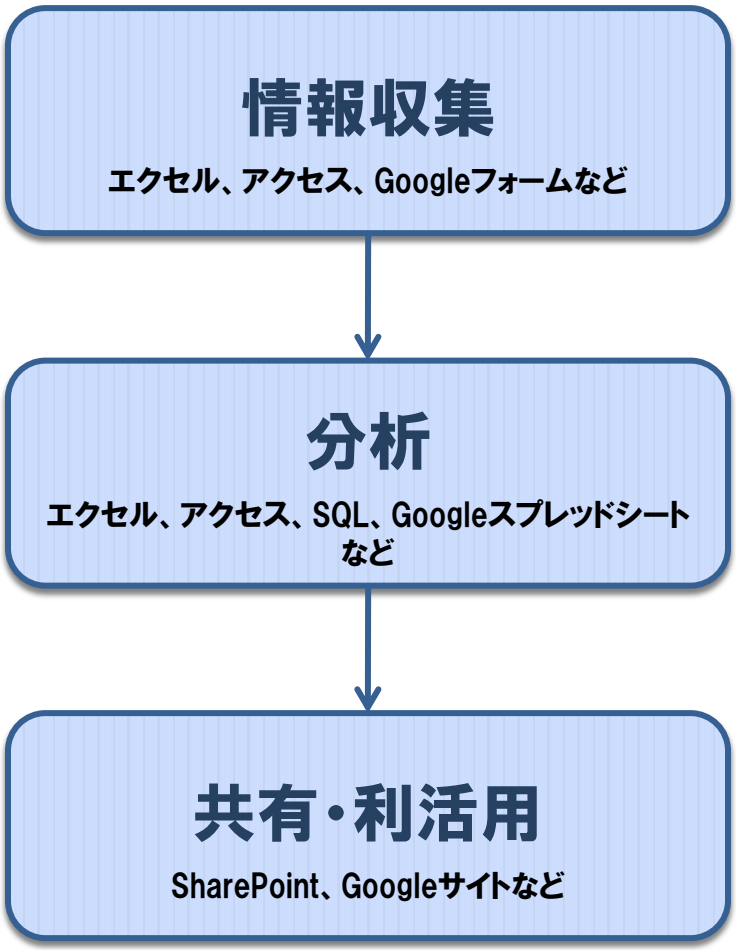
認証方法の比較例

クラウドサービスにおいては、ファイルの所在よりも認証の強度について検討を擦る必要があります。認証のフレームワークを明確にし、より良い認証を論理的に選択できるようなスキルを身につけます。

CISSPオフィシャルセミナーテキスト
「アクセスコントロール」からの引用

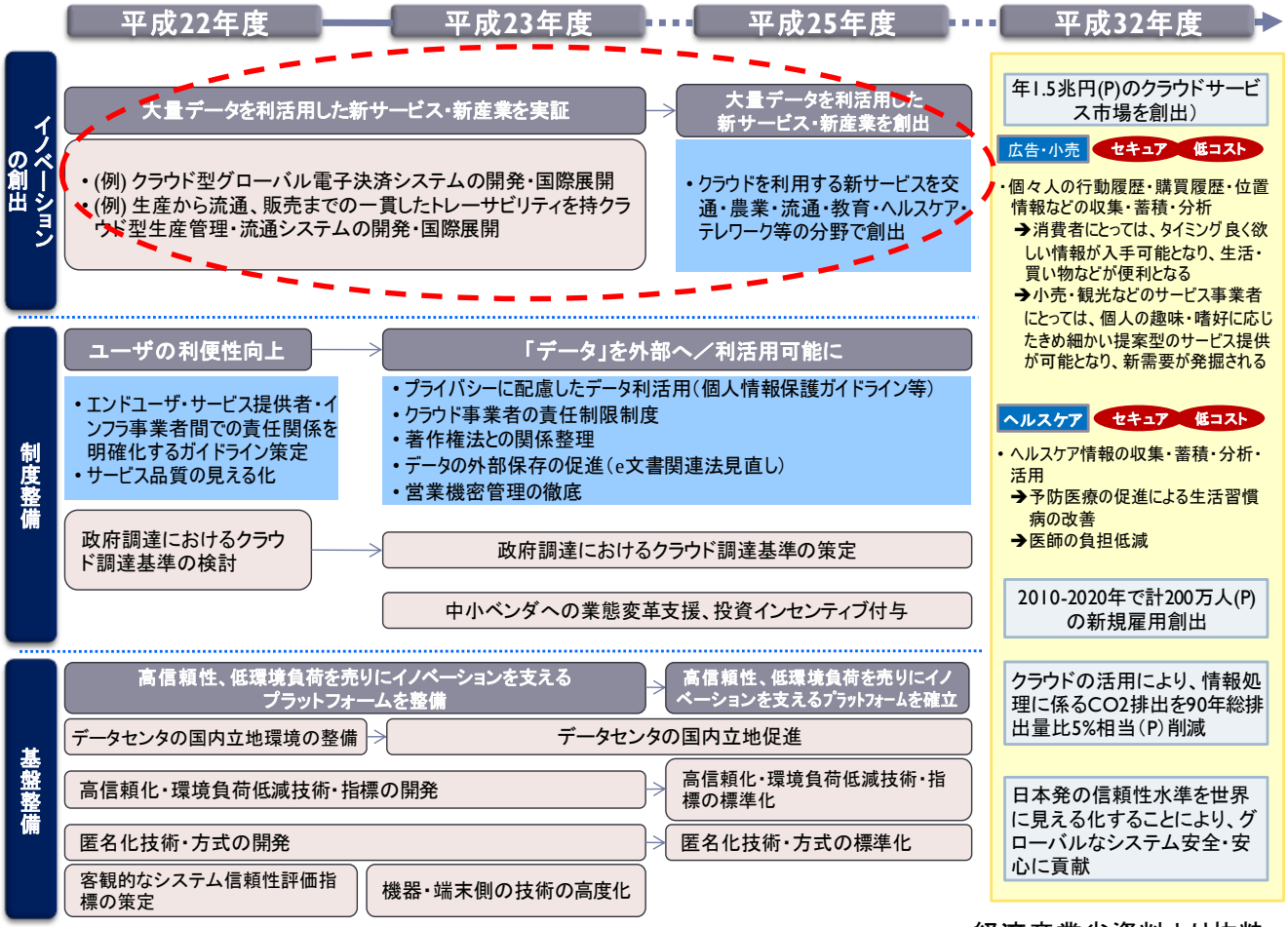
- 認証のフレームワーク
  - 識別
  - 認証
  - 認可
  - 説明責任
- 認証の一元化
  - ローカルの認証システムとクラウドサービス上の認証システムをどのように整合すべきかを考慮する
  - 認証を一元化するサービスやシステムが提供されている

クラウドサービスの基本をもう一度



- クラウドコンピューティングに向いている業務とは何かをお客様と共有
  - 情報収集
    - 〉大量のデータを収集するための基盤の提供
  - 分析
    - 〉柔軟に利用出来るCPUパワー利用による高速な情報分析
  - 共有・利活用
    - 〉分析したデータをどのように共有すべきかの検討

クラウド普及のための政策

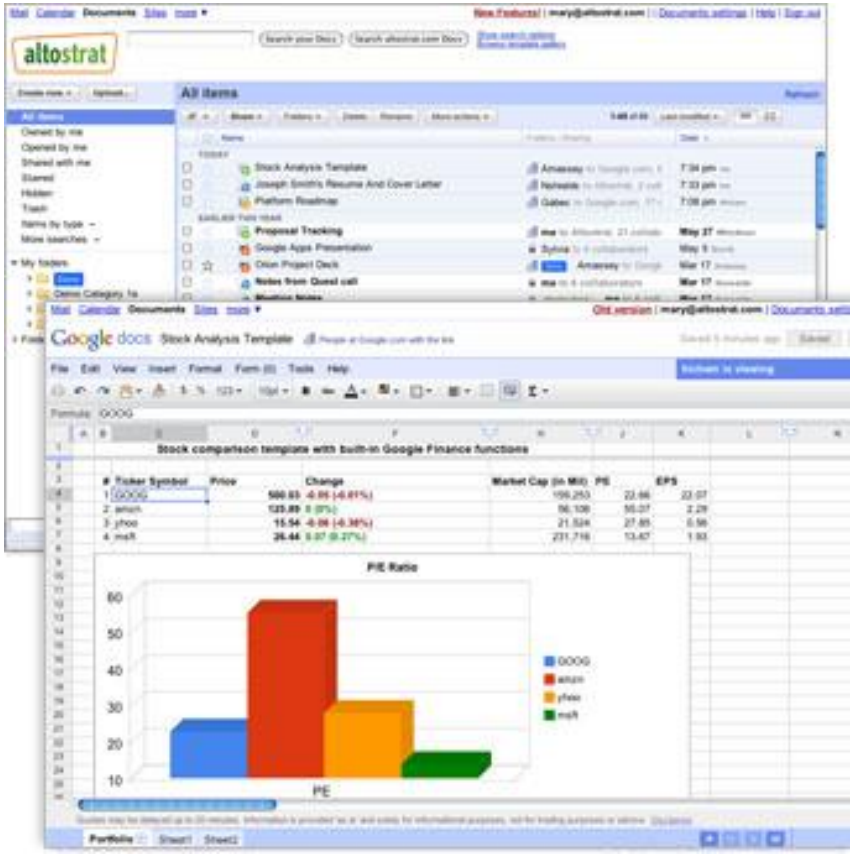


経済産業省資料より抜粋

Google Apps

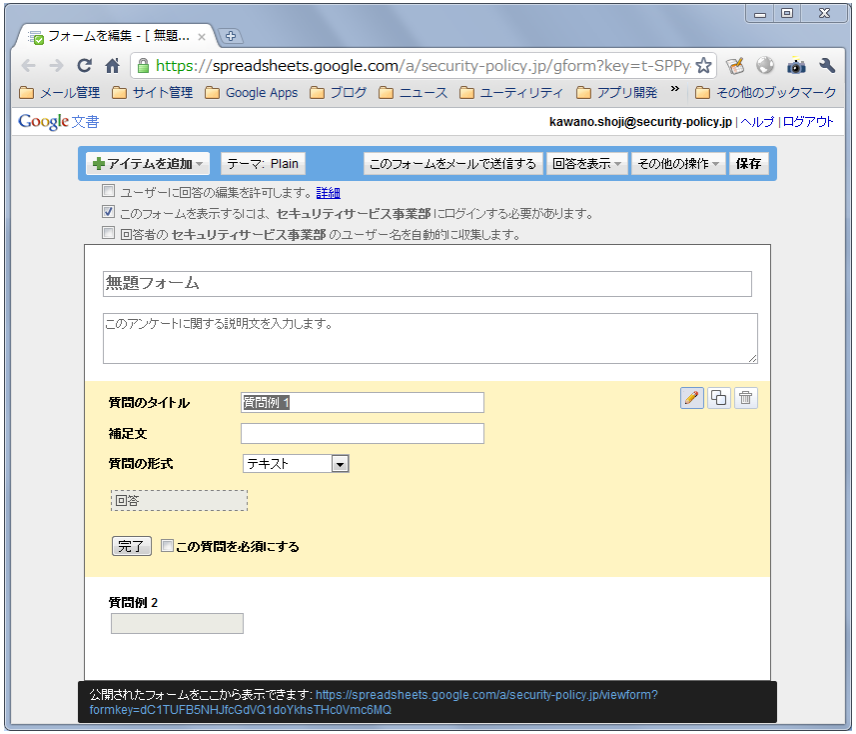
- オフィスアプリケーションを提供するSaaS
  - コミュニケーションツール
    - 〉 Gmail
    - 〉 Google サイト
    - 〉 Googleグループ
  - コラボレーションツール
    - 〉 Googleカレンダー
    - 〉 Google ドキュメント
    - 〉 Googleビデオ　など

Googleドキュメントを利用した業務改革



- コラボレーションワーク
  - メールの添付書類による文書管理はセキュリティ上の問題が影響する
  - １枚の書類を共有して作業することで、管理コストを削減することが可能
- リアルタイムコラボレーションを実現
  - １枚の書類に同時にアクセスすることで、協調作業がより効果的に実施できる

Googleフォームを利用した社内情報収集



Googleフォーム

Googleスプレッドシートの補助ツール
ワープロ感覚でウェブ上で共有できるフォームを作ることができる。ただし、モバイル環境には対応していない・・・
ユーザのログイン管理と連携して誰が記入したかを同時に取得できる

- Googleフォームなら、ユーザ管理を行いながら、情報収集が簡単にできる
  - ワープロ感覚で情報収集
  - スプレッドシートを活用した情報管理
  - 自動で作られる「概要」
  - APIを活用した情報分析ツール（マクロの簡単なものだと考えればよい）
  - リアルタイムに集計可能

Googleサイトを利用した情報共有

- 共有しないのなら情報は管理する必要がない
  - 情報管理の基本は「だれに」「どんな情報」を共有するかであり、共有しない情報は捨てたほうが良い
- 比較ができることが重要
  - 自社内のデータだとしても、なにかと必ず比較することでしかその有用性を評価できない

Googleサイト

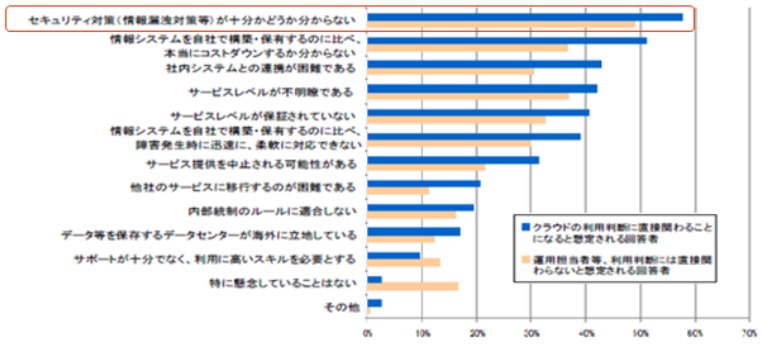
Googleのホムページ作成ツール
主に社内での情報共有や自らの情報収集を一元的に管理するために利用出来る
対応する「ガジェット」を作成することで、ページ上に自由に配置ができる
ページにはコメント機能やファイル添付機能もあり、コミュニケーションにも利用出来る

経済産業省やIPAの取り組み

情報セキュリティに関する政策

クラウドセキュリティガイドラインの策定

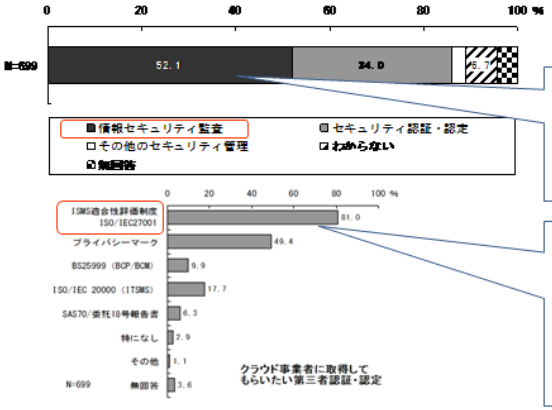
クラウド利用者の不安



＊「高度情報化社会における情報システム・ソフトウェアの信頼性及びセキュリティに関する研究会」（経済産業省2009年3月）

クラウド利用においてセキュリティ上の不安が払拭できていない

クラウド事業者への要求



半数の利用者が、クラウド事業者には情報セキュリティ監査による、具体的名報告を望んでいる

利用者が事業者にJIS Q 27000ベースのセキュリティ管理を望むのは、利用者組織と同様のセキュリティ体制を望んでいるため

＊「クラウドサービスの情報セキュリティ監査に関するアンケート調査報告書」（経済産業省2010年1月）

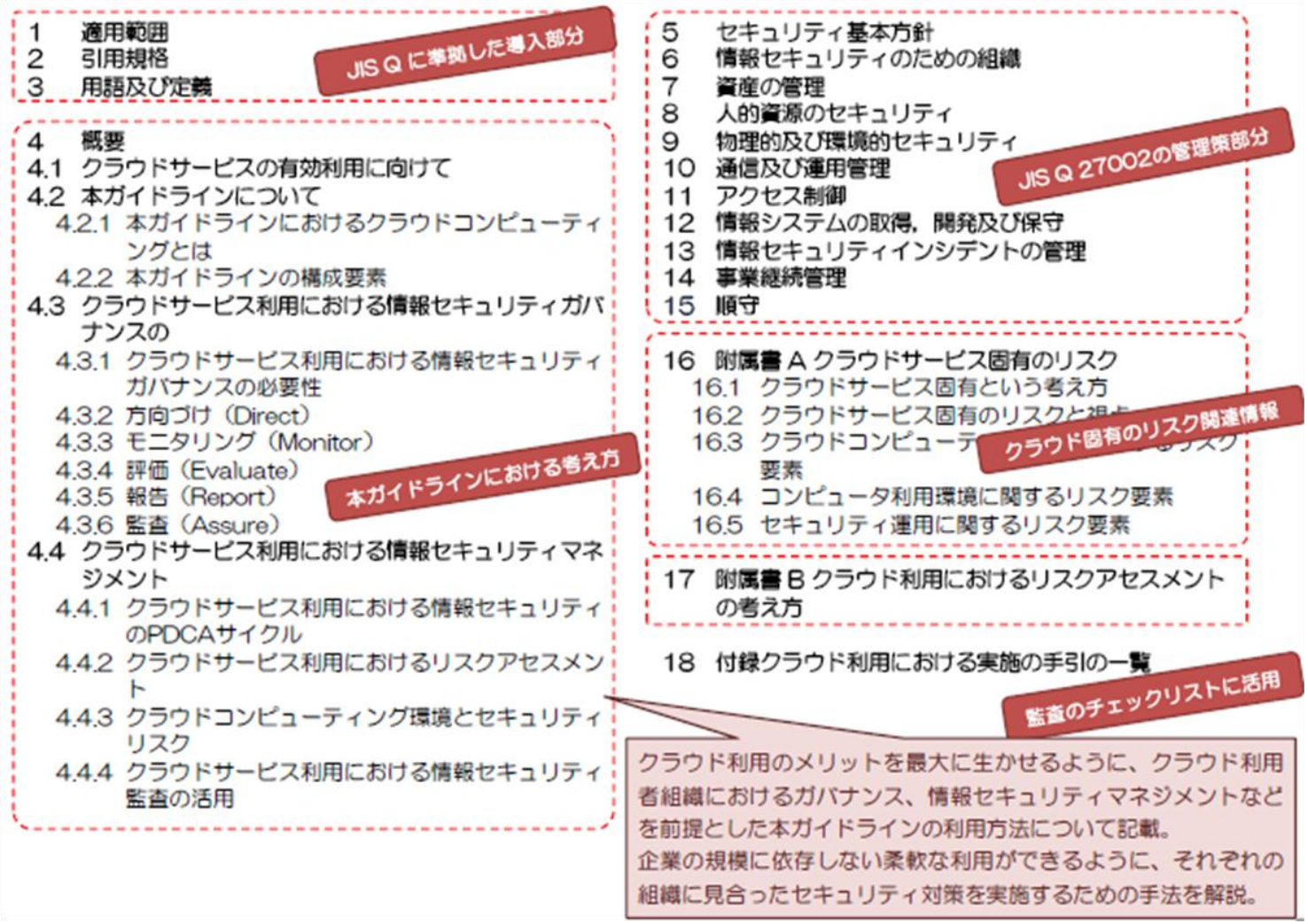
クラウド利用者はクラウド事業者に、情報セキュリティ監査およびJIS Q 27000ベースのセキュリティ管理を望んでいる。

「情報セキュリティ」および「事業者におけるシステム運用」が見えないことに関する不安を「見える化」する

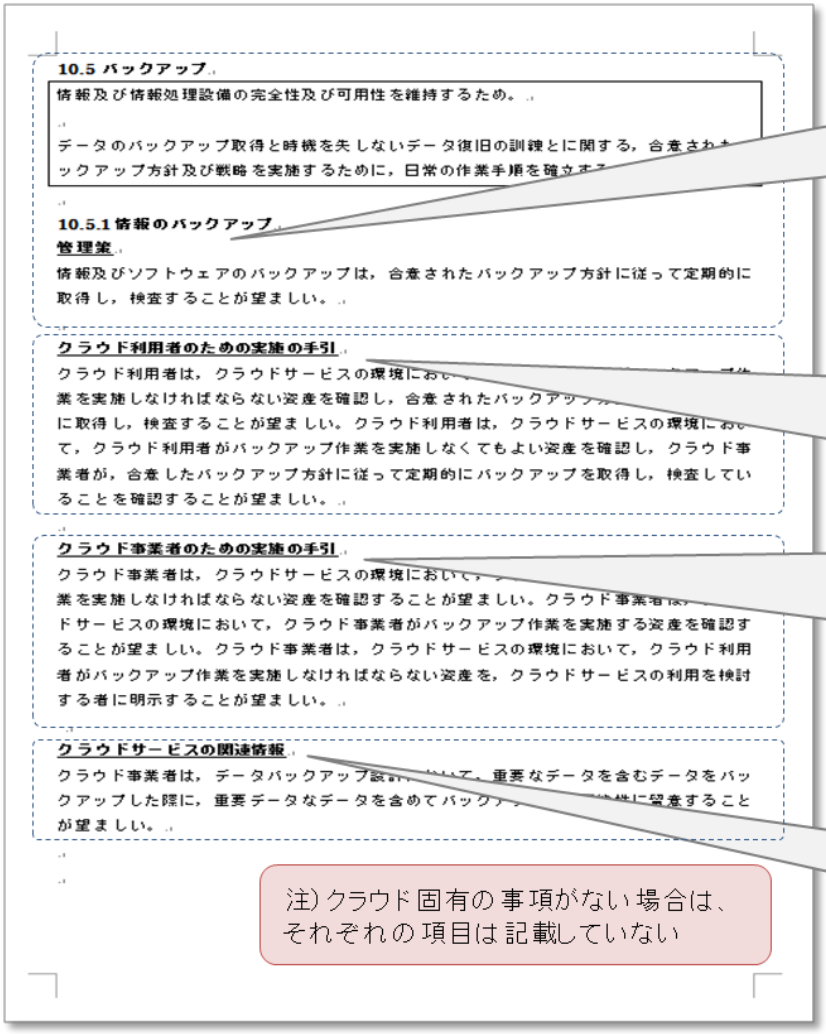
クラウドサービスの利用のための情報セキュリティマネジメントガイドライン

- 利用者における セキュリティリスクの 共通認識の形成
- 事業者選択における 基準として利用できる 対策標準
- 情報セキュリティ監査による 利用者と事業者の 信頼関係の構築

マネジメントシステムを活用する



ガイドラインのサンプル



管理策の目的と管理策

- 管理策の目的と管理策は、JIS Q 27002:2006をそのまま引用。
- 情報セキュリティ監査に利用する場合にも、目的を明確にするために利用が可能。

クラウド利用者のための実施の手引

- 管理策を順守するための、クラウド利用者組織における実施事項を記載。
- 実施事項には、クラウドサービス利用組織における、情報システム等の変化に伴うリスクの軽減のためのセキュリティ対策や考え方を記載。

クラウド事業者のための実施の手引

- クラウド利用者組織が管理策を順守するために自ら実施するのではなく、クラウド事業者に実施してもらう必要があるセキュリティ対策事項について記載。
- クラウド事業者を選定する際の選定基準や、情報セキュリティ監査における管理基準として活用が可能。

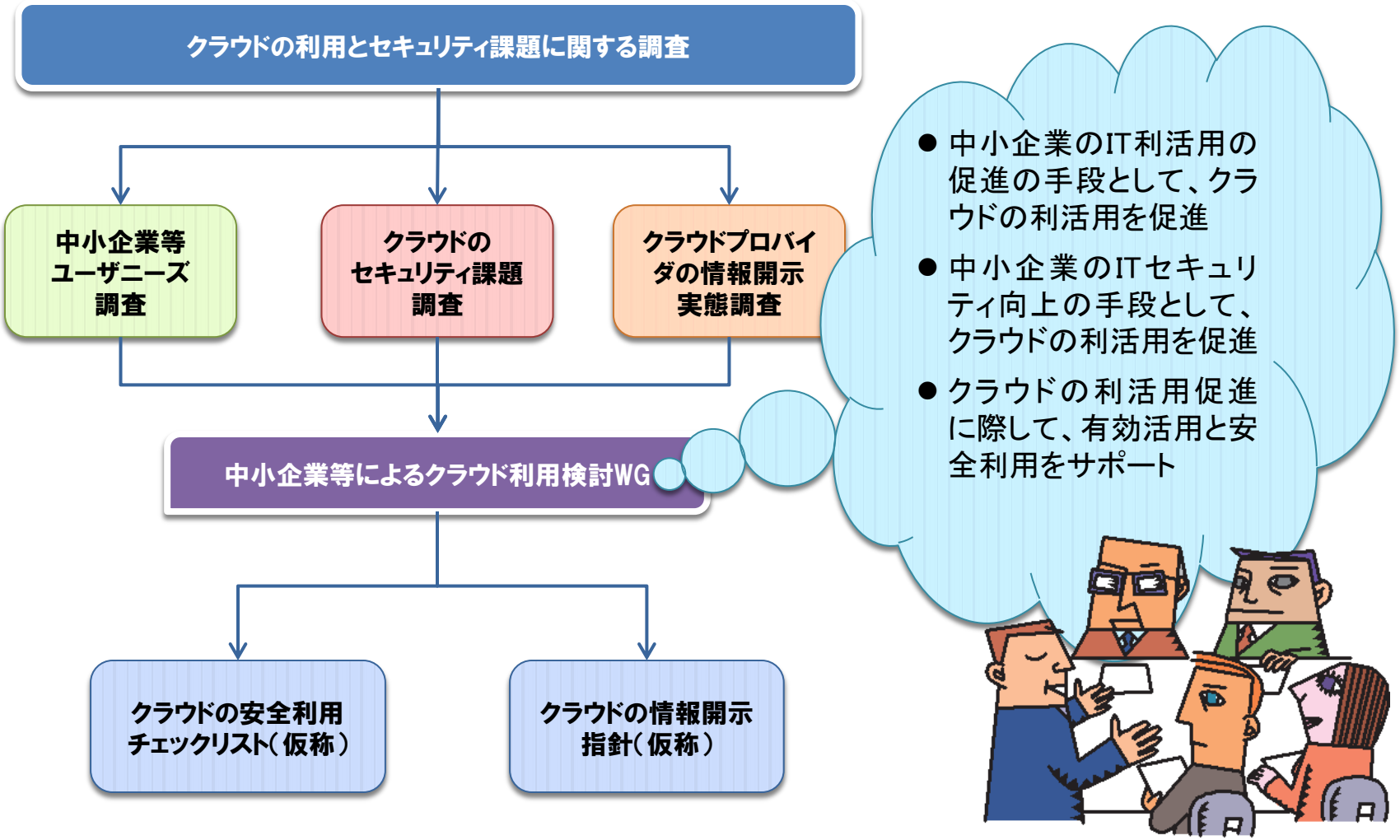
クラウドサービスの関連情報

- 当該項目では、クラウドサービスの形態や環境に特有の、個別の実施事項について記載。

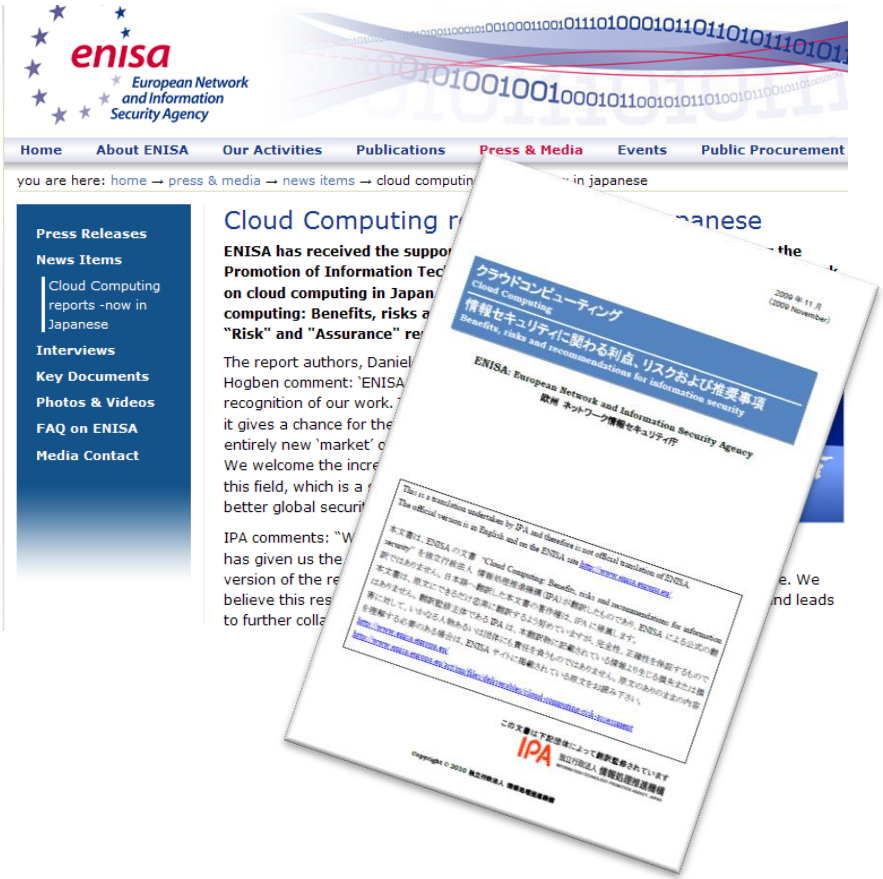
ガイドラインの国際化に向けて

- IS Technical Specification
  - ISOに向けて技術文書として策定中
  - 日本発の取り組みとして、国際化のリードを行う
- スケジュール
  - 2010/10 Study Period start
  - 2011/04 NP vote propose
  - 2011/10 WD start
  - 2012/10 PDTR
  - 2013/xx published

中小企業等によるクラウド利用検討WG

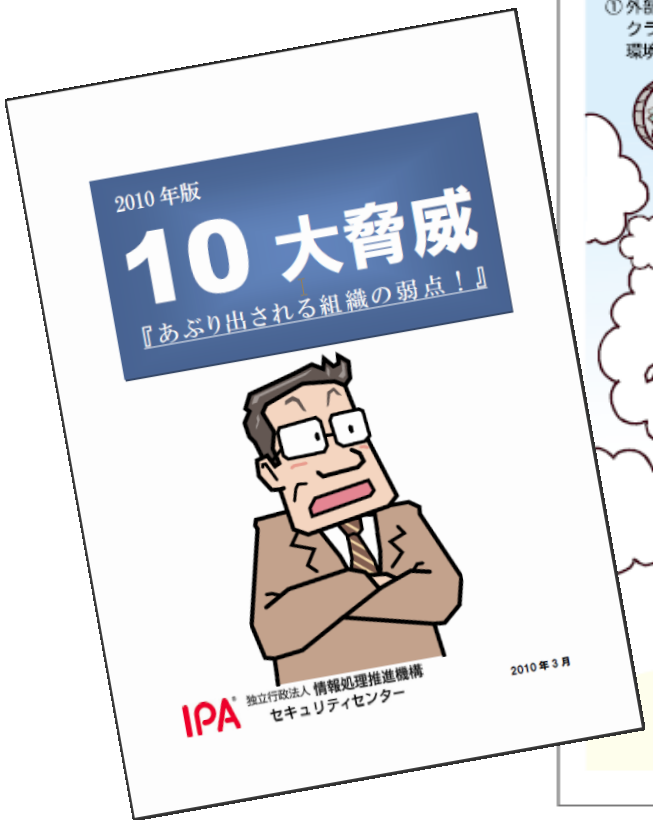


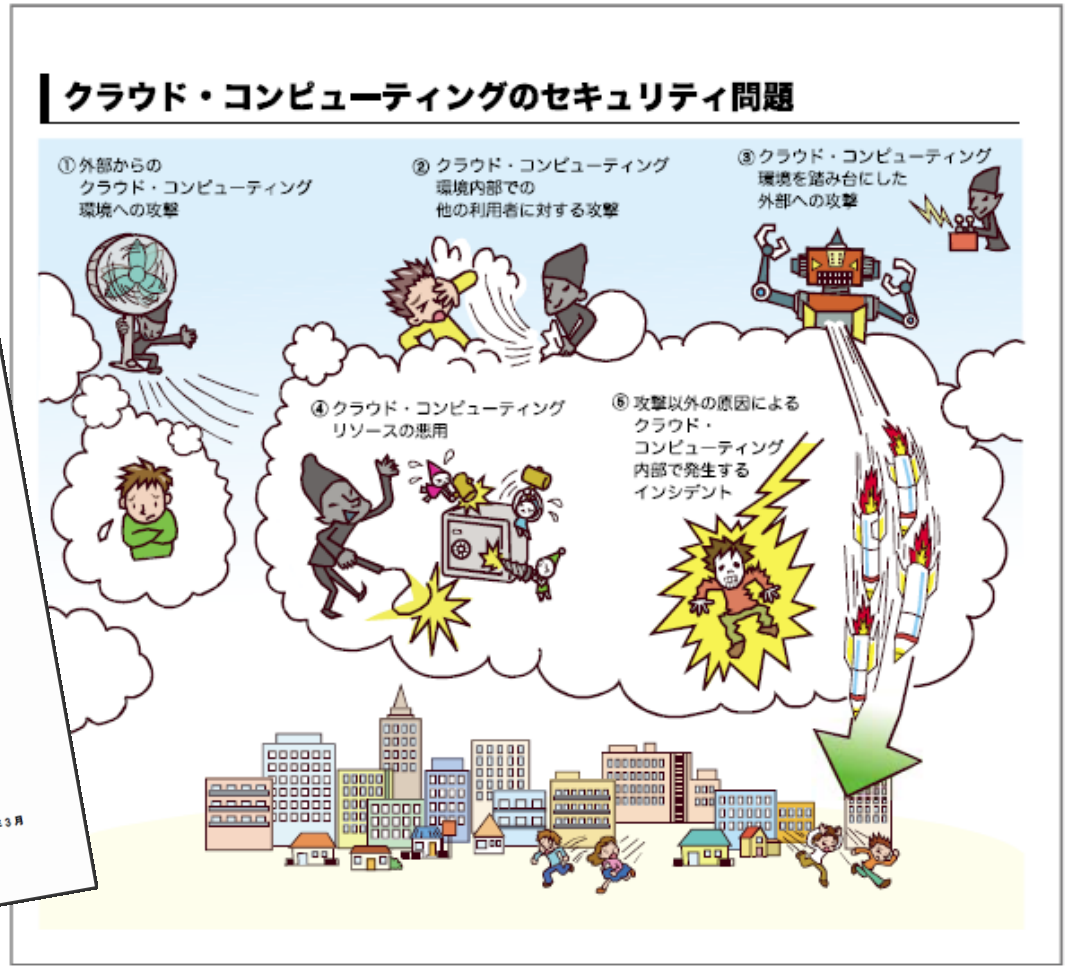
enisaのレポートを翻訳



- 2つのレポートを翻訳
  - クラウドコンピューティング：情報セキュリティ確保のためのフレームワーク
    - 〉企業（特に、中小企業）がクラウドサービスを利用する際に、情報セキュリティ確保のために、クラウドプロバイダに対して質問すべき項目をしまとめている
    - 〉利用者側・プロバイダ側の法的責任の範囲や責務の範囲をまとめ、利用者の責任を明確にしている
  - クラウドコンピューティング：情報セキュリティに関わる利点、リスクおよび推奨事項
    - 〉クラウドコンピューティングを利用する際のセキュリティ上のリスクと利点の評価を可能にするために、クラウドコンピューティングの既存および潜在ユーザーに対して、セキュリティ上のガイダンスを提供する文書

2010年版 10大脅威を発表





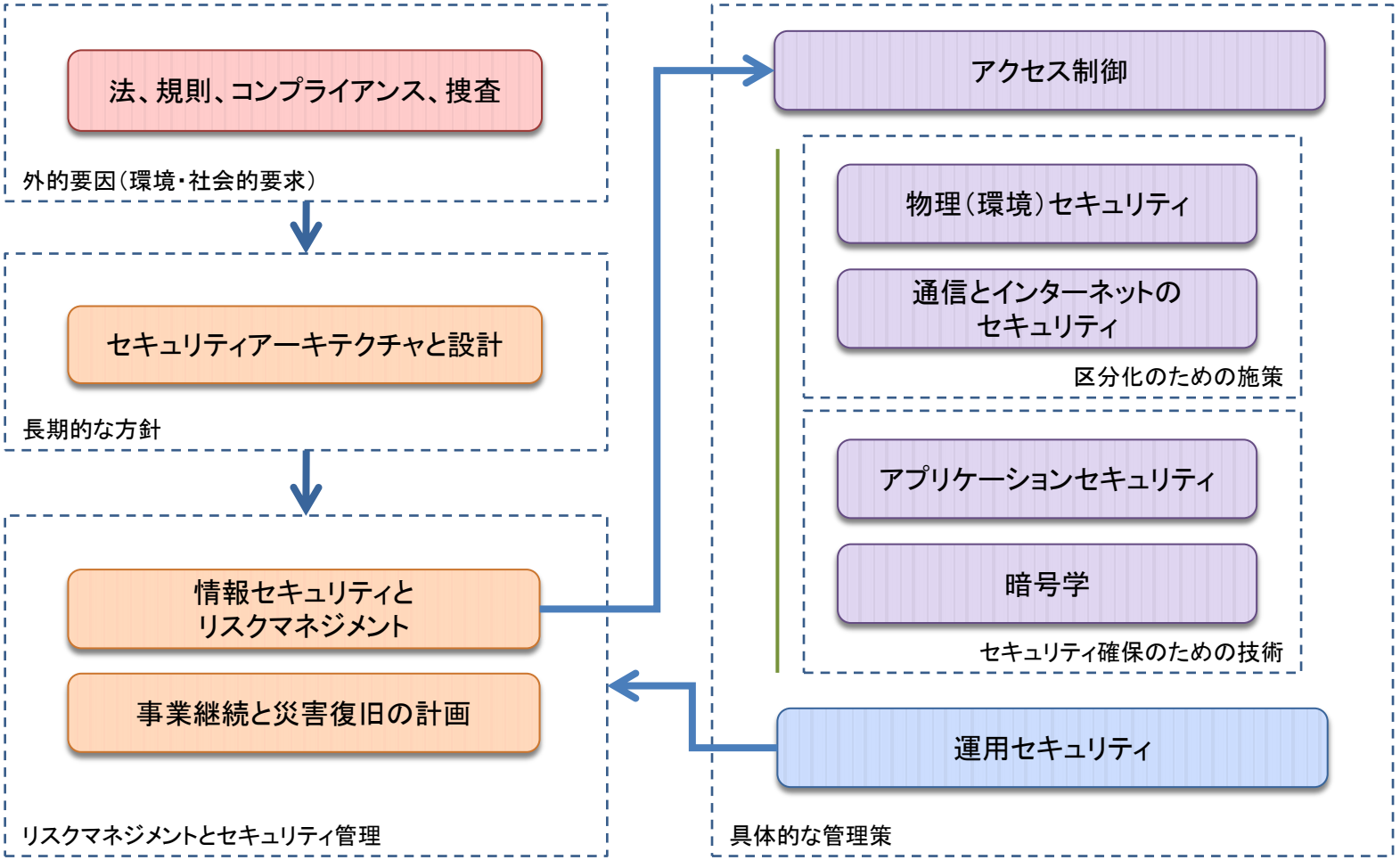
http://www.ipa.go.jp/security/vuln/documents/10threats2010.pdf

社内向けクラウド構築のために活用できるソフトウェアカタログ

クラウド構築を行うために用いられるソフトウェアの中から30種のOSS、18種の商用ソフトウェアを9つの機能分野に分類してカタログとしてまとめました。 OSSについては以下のような5項目について評価し、結果を記載してあります。

評価項目	評価内容
基本情報	日本語コミュニティの有無、機能概要、類似ソフトウェア、ライセンス等
サポート	ドキュメント整備状況、コミュニティサポート書籍、サポート企業の有無等
開発体制	開発主体組織、参加企業、参加形態、開発者数、開発ロードマップ、標準化活動等
成熟度	バグ数、フィックスまでの期間、フィックス率、脆弱性公開数と対応数等
機能	評価製品ごとに調査項目を設定

CISSPの10ドメイン



CISSPの考え方を身につけましょう

- CISSPセミナーで体系的な知識とスキルを身につけましょう
  - 情報セキュリティのフレームワークを学ぶことで、環境が変化しても対応できる知識とスキルを身につけることが可能です
- CISSPのコミュニティにも
  - 定期的にコミュニティを開催しています。ぜひ、ご参加ください。