クラウド利用でなにが変わるのか

～クラウド利用のメリットとセキュリティの確保について～

日本マイクロソフト株式会社
チーフセキュリティアドバイザー
高橋　正和

Microsoft

アジェンダ

- クラウドの歴史を振り返る
- セキュリティを考える前にクラウドの特徴を確認する
- 何のためのセキュリティか
- クラウドの形態と責任分界点と利用のメリット
- 取り扱うデータと必要とされるセキュリティ レベル
- クラウドサービス利用における主要な懸念点
- セキュリティとセキュリティに関連する事項
- Windows Azureにおけるセキュリティの実装

クラウドの歴史を振り返る

クラウドの歴史-1

- インターネットとWEBの普及（1990年代）
  - 3-Tier Model (クライアント、Webサーバー、DB)
  - 成功事例：Amazon(1997),eBay(1998),楽天(2000)
- アクセスの増大への対応（WEBサービスがScaleしない）
  - ある規模を超えるとDBがボトルネックとなる
  - 複数データの突合せ（Amazonのリコメンデーション等）が要求するスケール
  - ユーザーからの情報発信の急増＝データとアクセスの急増
    - YouTube, Flickr, Facebook, Twitter (Web 2.0)

- クラウドの始まり：Googleの大規模分散システム(2004)
  - 安価なマシンをネットワーク上で協調動作をさせることで、Scale-outを実現
    - GFS: Google File SystemによるStorageのScale-out
  - システムの故障を前提としたモニタリング、エラー検出、自動回復
    - ハードではなく、ソフトによるアプローチ
  - MapReduce - GFSで実現した巨大なデータを突き合わせる技術
  - BigTable Key/Value型デザイン - 超大容量の高速データベース
  - エネルギーコストへの注目と削減

クラウドの歴史-2

- 商用クラウドの登場： Amazon EC2/S3（2006）
  - Googleが一般消費者をユーザーとしていたのに対し、エンタープライズを対象とするクラウド・サービスの提供を開始
  - Amazonは、自社サイトの運用経験から、リソースを合理的に管理する手法を編み出す
  - Webでは、開発者はプログラムのサイズに関わらず、仕事の70%を保守作業やビジネス上の差別化に結びつかない仕事に費やしていると分析
  - ネットワーク上に分散しているディスクや、物理的なサーバーを、仮想化して論理的に管理し、稼働していないものはリソースプールに登録し、変動する要求に動的に対応
- クラウド概念の成立（2006年ころ）
  - Scale-outアーキテクチャ、Availabilityの確保、Key/Valueデータ・ストア、BASE トランザクション
- エンタープライズ・クラウドの新段階　Microsoft Azure(2008)
  - エンドユーザーではなく、サービス提供者にクラウドを提供
  - Google App Engineの開始
  - Microsoft Azure
    - クラウド上のリソース管理を、クラウドOSとしてユーザーに公開
    - データストレージ：Key/Value データ」・ストア、Queue、Blob
    - サービスモデルによる、ファブリックコントローラー
    - 既存のシステムを、クラウド上への移植を容易にする
    - クラウドと、ON Premiseの柔軟性、動的な、Scale-out, Scale-in、データの整合性に対するアプローチ：Eventually Consistency

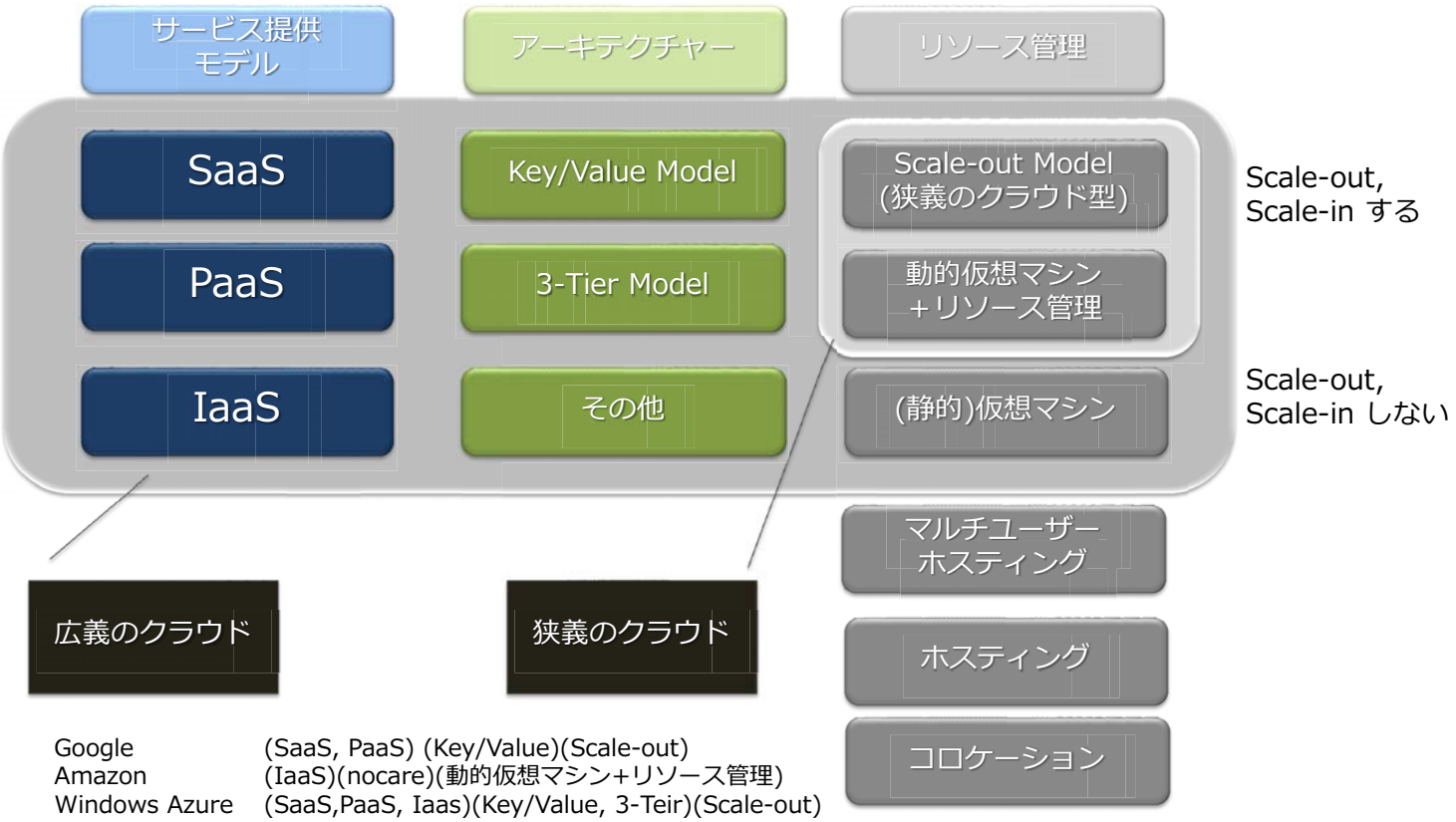
Trend of Information Security

	2000	2005	2010	Challenges
Malware / Cyber Attacks	Worm / Virus	Bot / Botnet	APT (Advanced Persistence Attack)	
	• Propagation • System Down	• Silent intrusion • Economical harm	• Breaking-in to Unexpected Target • Critical Info. leakage	• Enhance endpoint security • Ensure right configuration
	CodeRed, Nimda, Blaster, Slammer	Agobot, Waledac, Zeuse	Operation Aurora (Google) Stuxnet, intrusion onto DOD	
	• Curiosity and Vandal	• Infrastructure of Underground economy • Economic/Business Risk	• Critical limitation of Perimeter protection • National Security	• Windows 7 • Domain management
Network Architecture	Intranet + Internet + DMZ (RAS)	Intranet + Internet + DMZ + Satellite (VPN)	Cloud	• Data(Information) protection on borderless network • Ensure following compliances with Cloud • Data Jurisdiction
	• Good guys in / Bad guys out (out=Internet)	• Part of good guys out	• No border between Intranet and Internet	
Information Assurance / Compliance	ISMS	Private Information Protection Law	SOX/J-SOX	New Challenges
	Information Leakage Cases			

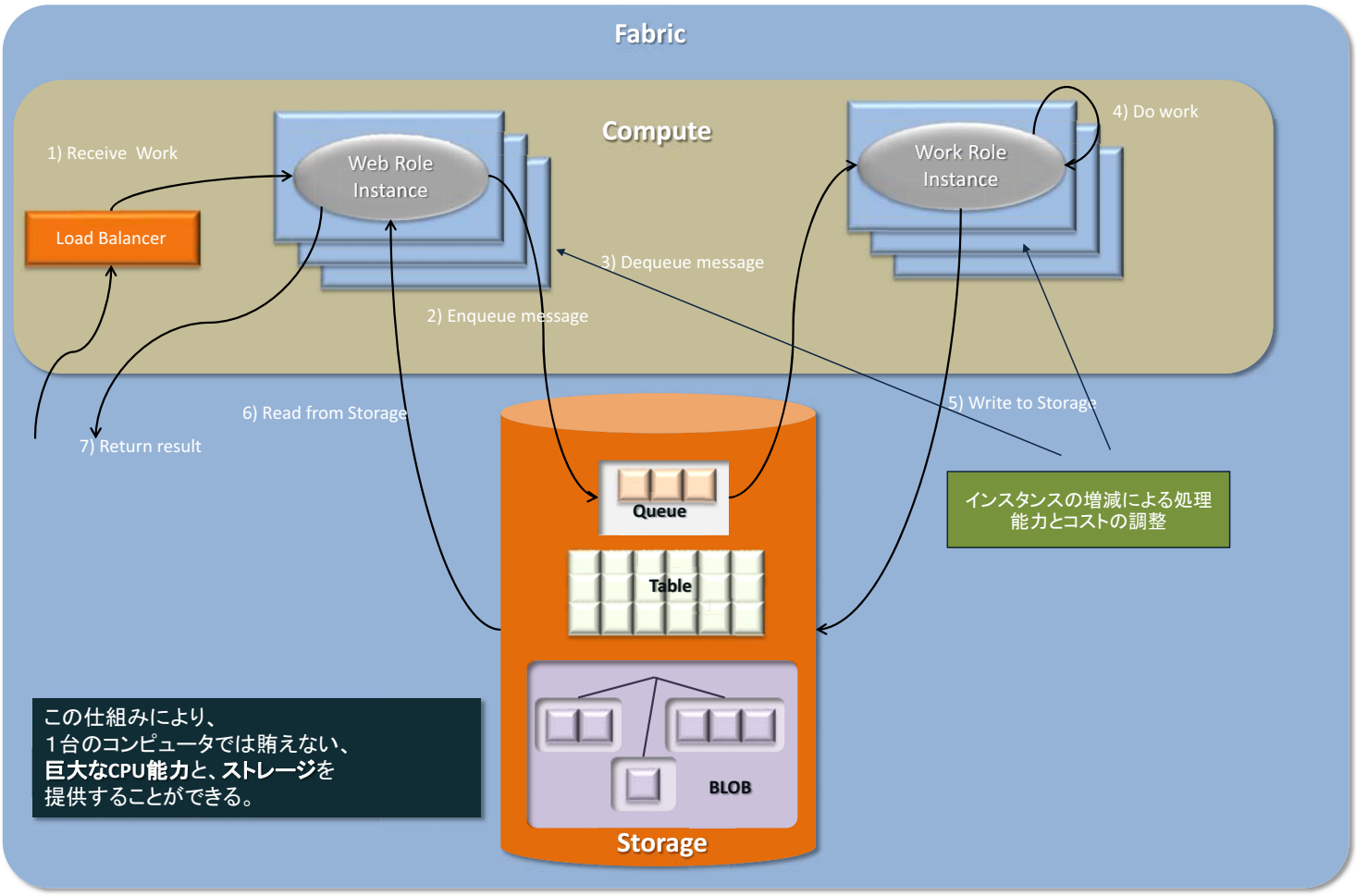
セキュリティを考える前に
クラウドの特徴を確認する

クラウドとは何か

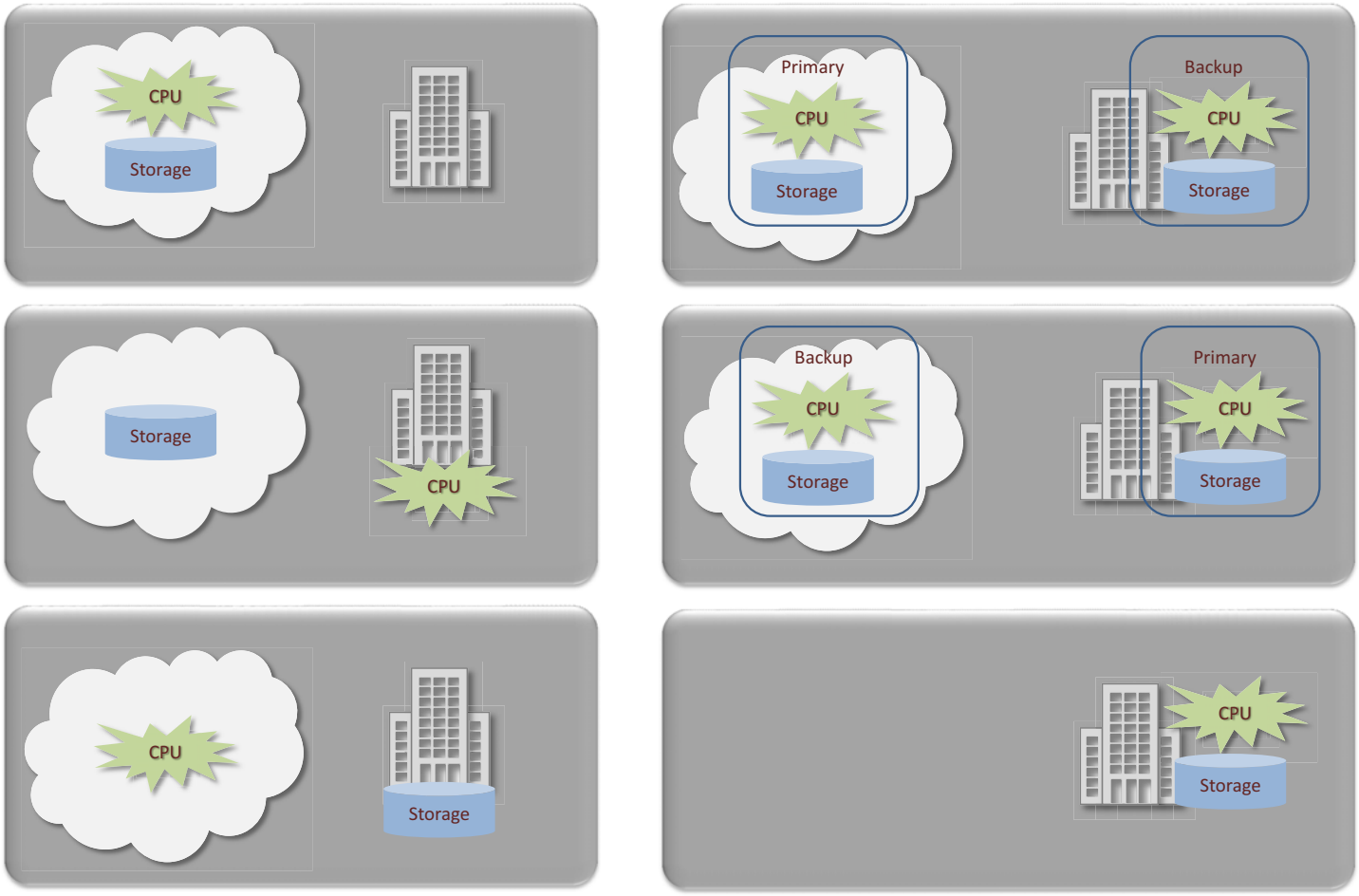
ひとつの見方＝Scale-out/Scale-inすること



Scale-out/inを実現する仕組み(Azureの例)

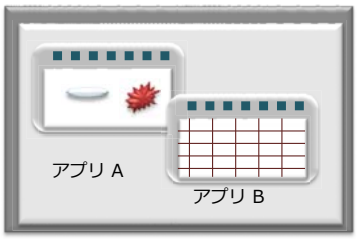


クラウド利用の形態は複数ある

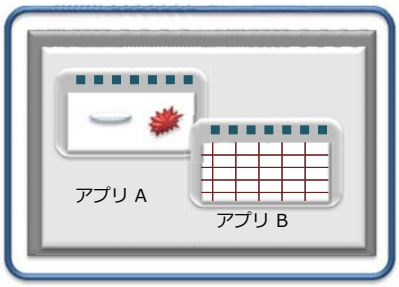


ローカルとリモートの構成

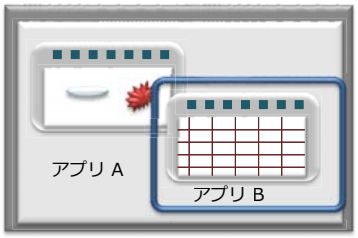
～すべてをリモートで行う必要はない～



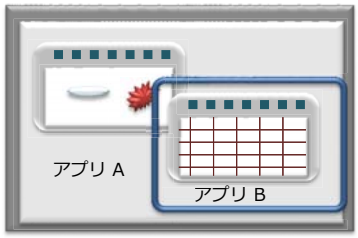
すべてがPC上で稼働するモデル



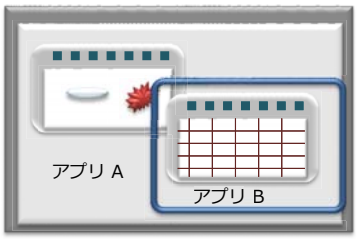
PCのディスクトップをリモート上の
サーバーに構成するモデル
(リモートデスクトップ)



デスクトップはPC上で、アプリBだけを、
リモートサーバー上で動作させる
アプリAは、PC上で稼働している
(Application Virtualization)



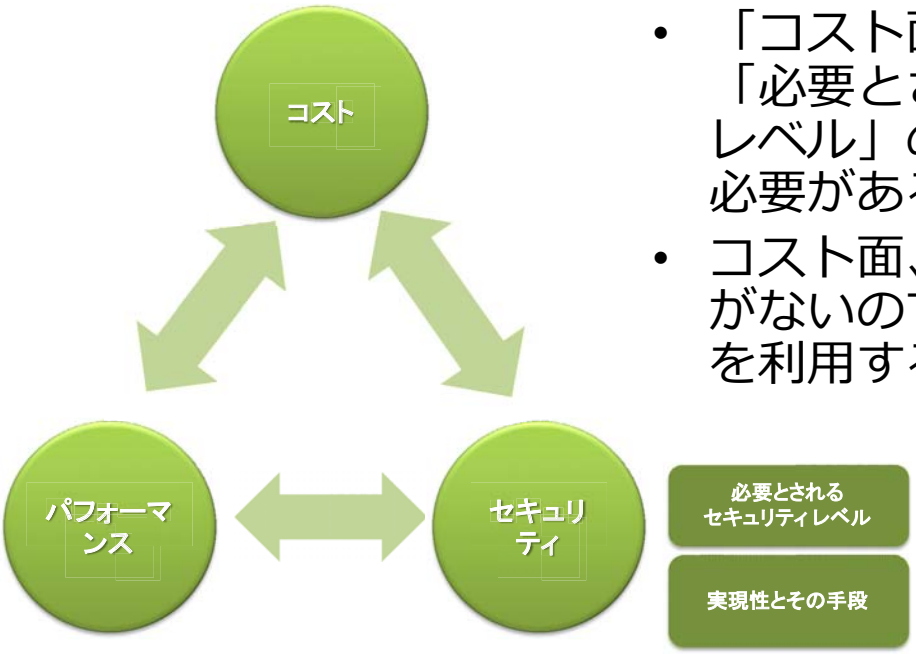
デスクトップはPC上で、アプリBがブ
ラウザなどを使って、リモートサーバ
上で動作する。
いわゆるWebアプリケーション



デスクトップはPC上で、アプリBがス
テージとして、クラウドを利用する

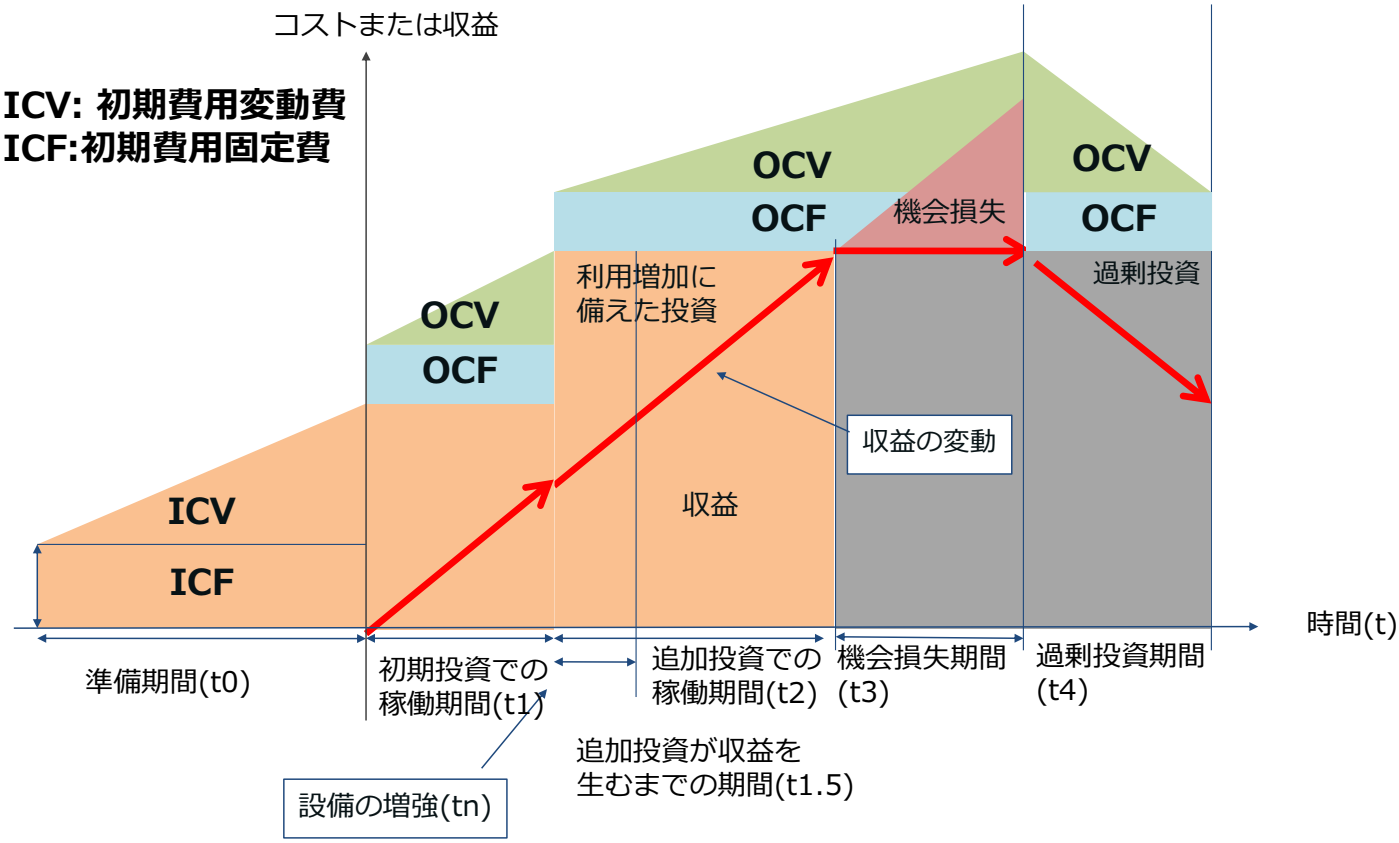
何のためのセキュリティか?

クラウドのセキュリティ



- セキュリティだけを考えても、あまり意味はない
- 「コスト面」、「性能面」と「必要とされるセキュリティレベル」のバランスで考える必要がある
- コスト面、性能面でメリットがないのであれば、クラウドを利用する必要はない

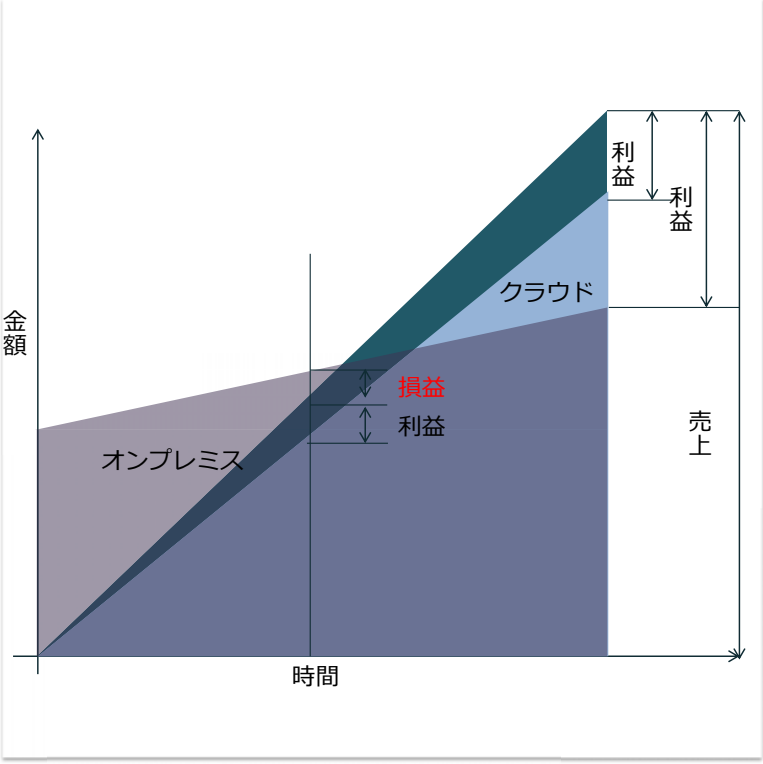
クラウドのコストメリットの一面



ROIを考えた場合、クラウドは以下の狙いがある

1. イニシャルコスト(ICF,ICV)を下げる(固定費を変動費へ)
2. 運用コスト(OCF, OCV)を下げる(固定費を変動費へ)
3. 投資期間(t0, t1.5)を短くすることで、投資の回収期間を短くする
4. 投資期間(t1.5)を短くすることで機会損失を最小化する
5. 需要が減少しに対応し、OCF, OCVを減少させ回収率を改善する

ビジネスステージにみる傾向



一般的に、クラウドのようなサービスは、初期費用が安価で、変動費の割合が高い
オンプレミスは、初期費用がかかるが、変動費の割合が低い

このためビジネスが軌道に乗り、規模が大きくなった場合に、クラウドでは、オンプレミスと比較して、利益が出せない構造になる場合がある

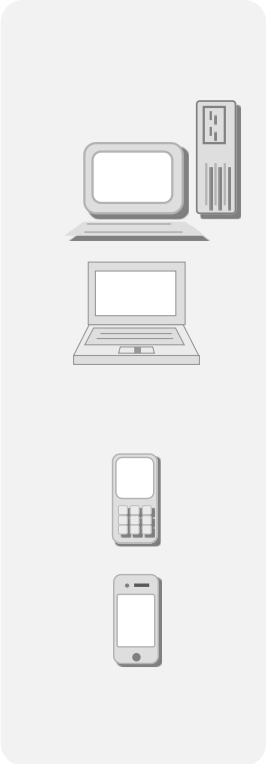
このようなケースが考えられる場合、クラウドとオンプレミスの移行性、互換性を考慮する必要がある。

ITインフラのサービス化

クラウドの形態と責任分界点と利用のメリット

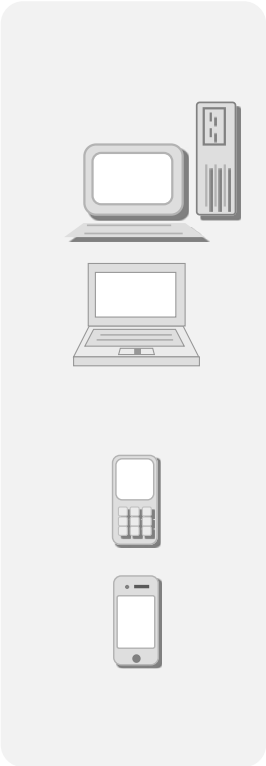
クラウドの利用における ＩＴシステムのセキュリティ

基本的なITインフラの階層



クラウドの利用における
ＩＴシステムのセキュリティ

IaaS型のクラウド
ホストレベルのサービス化



IaaSのメリットとセキュリティ

- システム調達の迅速化し増強も容易。
- 従来のIT資産の移行もしやすい
- サーバーなどの資産が、利用状況に応じて費用化される

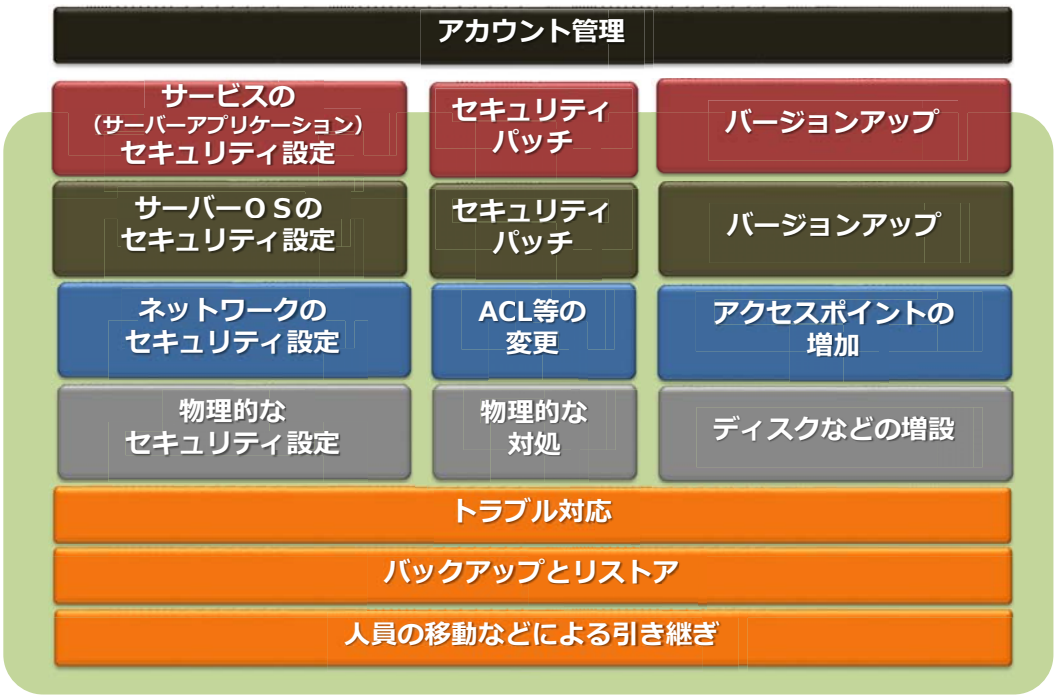
- オンプレミスと同様に、物理的なセキュリティを除いた、すべてのセキュリティ設計と、セキュリティ更新が必要

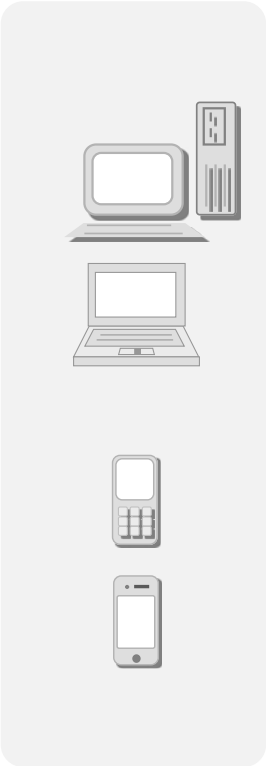
イメージ：自家所有の配送車をリースで利用

	メリット	セキュリティ
アカウント管理	任意の管理方法が選択可能	
サービス（サーバーアプリケーション）		利用者がすべて対応する必要がある
サーバーＯＳ		設計・構築・パッチの適用などを含めて、利用者がすべて対応する必要がある
ネットワーク	利用者が構築 幅広い実装の選択ができる	
サーバー等のデバイス	即時に利用が可能で、増強も容易 費用化が可能	一般的に物理的なセキュリティは信頼できる
データ		すべてのデータに対して、利用者が対応する必要がある
トラブル対応	OSより下位については、クラウドプロバイダが対応	

クラウドの利用における
ＩＴシステムのセキュリティ

PaaS型のクラウド
プラットフォームのサービス化





PaaSのメリットとセキュリティ

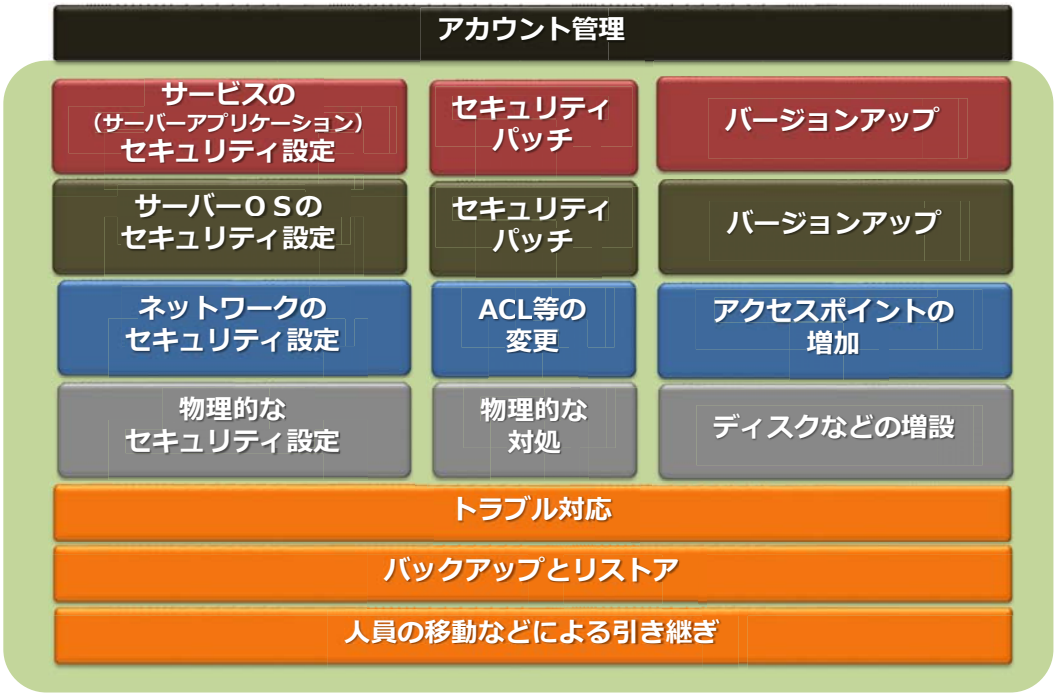
- システム調達の迅速化し増強も容易。
- 利用状況に応じて費用化され、柔軟なリソースの増強が可能
- オンプレミスとの併用など、多様な形態が選択可能
- アプリケーションより下位については、一定のセキュリティレベルが確保されている
- プラットフォームのセキュリティ更新を自動的に行うことができる
- バックアップやミラーリングの仕組みが用意されている（自動化されている場合も多い）

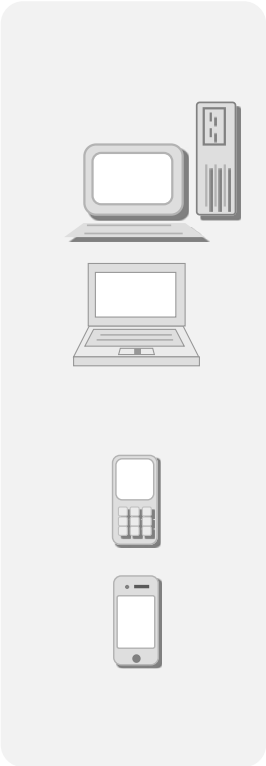
イメージ：拠点間の配送に配送業者を利用し、自社配送にはレンタカーを利用

	メリット	セキュリティ
アカウント管理	制限がある場合が多い	フェデレーションなどの仕組みが用意されている場合が多い
サービス（サーバーアプリケーション）		利用者が対応する必要がある
サーバーＯＳ		クラウドプロバイダが対応
ネットワーク	クラウドプロバイダの環境	サービス用の通信を除き、クラウドプロバイダが対応
サーバー等のデバイス	即時に利用が可能で、柔軟な増強も容易費用化が可能	一般的に物理的なセキュリティは信頼できる
データ		バックアップやミラーリングの仕組みが用意されている場合が多い。
トラブル対応	プラットフォームより下位については、クラウドプロバイダが対応	

クラウドの利用における
ＩＴシステムのセキュリティ

SaaS型のクラウド
ITインフラのサービス化





SaaSのメリットとセキュリティ

- ITインフラをサービス化することができる
- サービス（メール、CRM、その他）を迅速に利用することができる
- サービス構築やIT基盤に関する知識を必要としない
- ITサービスについて、一定のセキュリティレベルが確保されており、セキュリティ更新も、プロバイダが行う
- バックアップについては、SLAに応じて、利用者が対応する必要がある

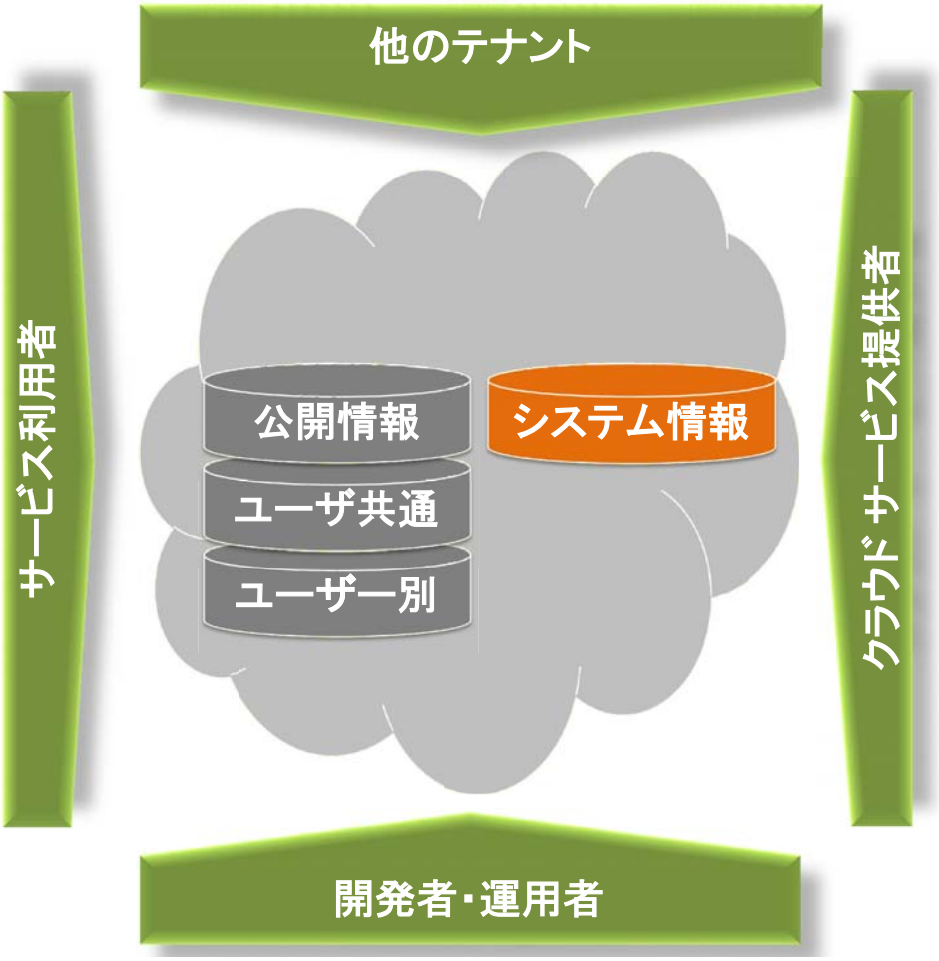
イメージ：自家配送をやめて宅配便を利用

	メリット	セキュリティ
アカウント管理	制限がある場合が多い	フェデレーションなどの仕組みが用意されている
サービス（サーバーアプリケーション）	即時利用することができる	クラウドプロバイダが対応
サーバーＯＳ	意識しない	クラウドプロバイダが対応
ネットワーク	クラウドプロバイダの環境	クラウドプロバイダが対応
サーバー等のデバイス	意識しない	一般的に物理的なセキュリティは信頼できる
データ		
トラブル対応	基本的にクラウドプロバイダが対応	

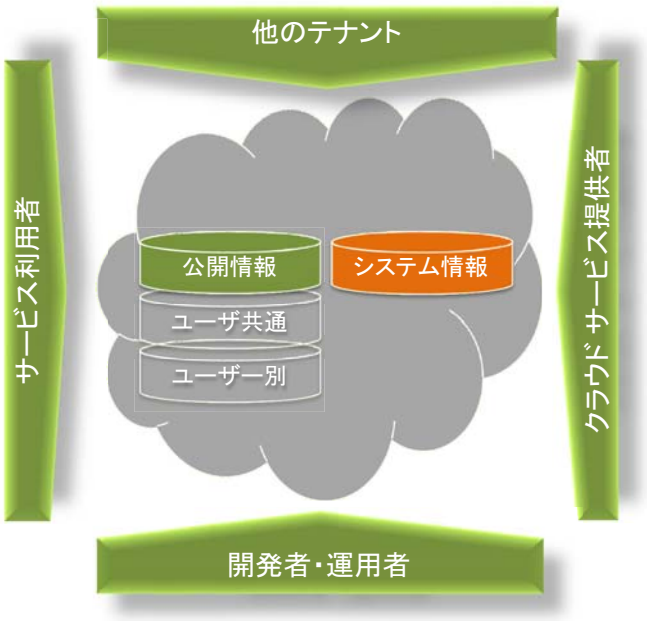
主にPaaSを想定

取り扱うデータと
必要とされるセキュリティ レベル

クラウド利用時の情報と関係者

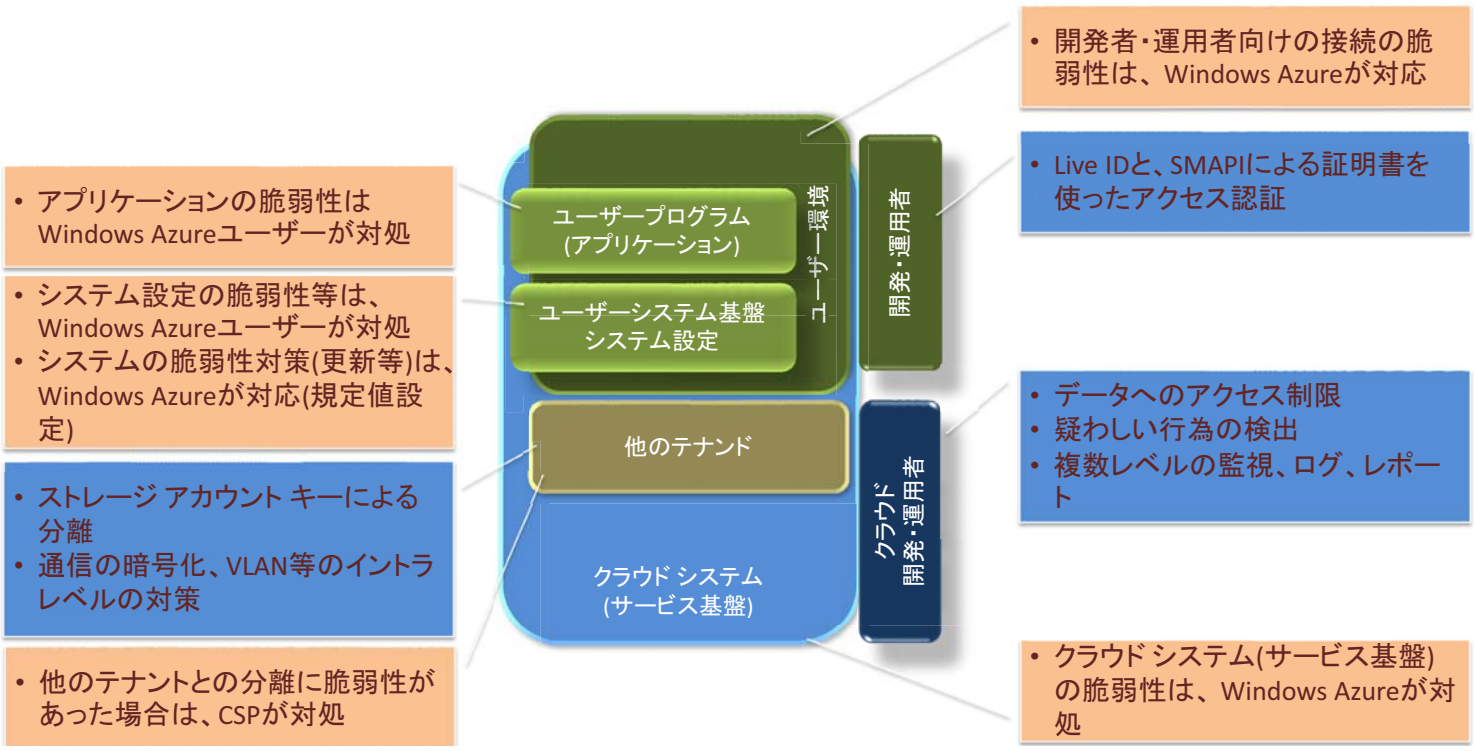


ユーザー管理なし≒公開情報のみ

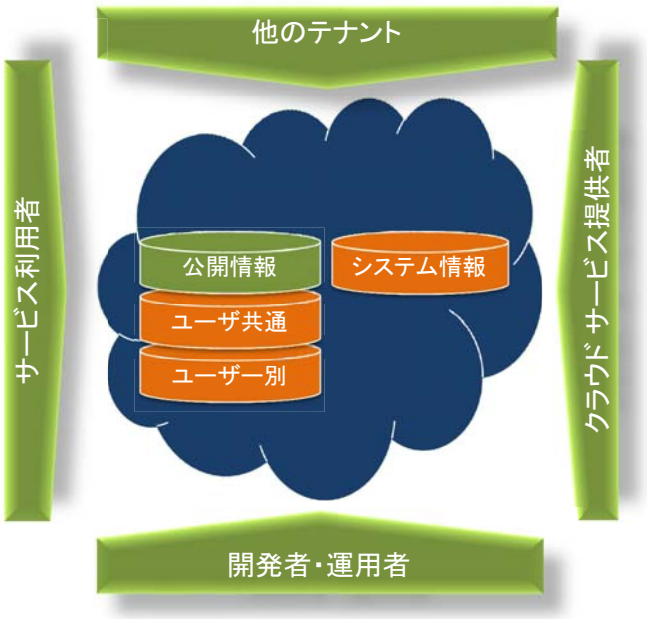


- 要求されるセキュリティ レベルは、それほど高くない
  - ユーザー管理：なし
  - 改ざんの防止
    - 運用管理者アカウント
    - マルチ テナントの他の利用者
    - 不正アクセス
  - DoS/DDoS
    - 一般的には、クラウドが有利

不正利用からの保護と脆弱性の対処 公開情報だけを扱う場合



ユーザー管理あり≒保護すべきデータあり



- 要求されるセキュリティ レベルが上がる
  - ユーザー管理
    - アカウント情報
  - 改ざんと漏えいの防止
    - 運用管理者アカウント
    - マルチ テナントの他の利用者
    - 不正アクセス
    - 他のユーザー アカウント
  - DoS/DDoS
    - 一般的には、クラウドが有利

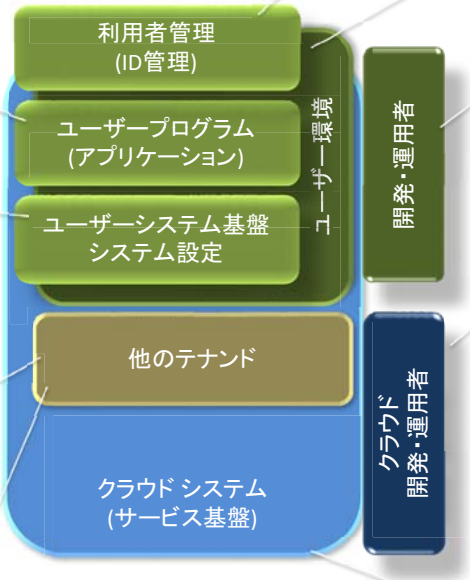
不正利用からの保護と脆弱性の対処 イントラネットを展開する場合

- ID間の分離はアプリに依存
- 認証基盤(フェデレーションが可能)
- Windows Identity Foundation(WIF), Windows Live ID, Open ID

- ID管理の問題は利用者が対処
- クラウドの認証基盤の問題は、Windows Azureが対処

- 開発者・運用者向けの接続の脆弱性は、Windows Azureが対応

- Live IDと、SMAPIによる証明書を使ったアクセス認証



- アプリケーションの脆弱性はWindows Azureユーザーが対処

- システム設定の脆弱性等は、Windows Azureユーザーが対処
- システムの脆弱性対策(更新等)は、Windows Azureが対応(規定値設定)

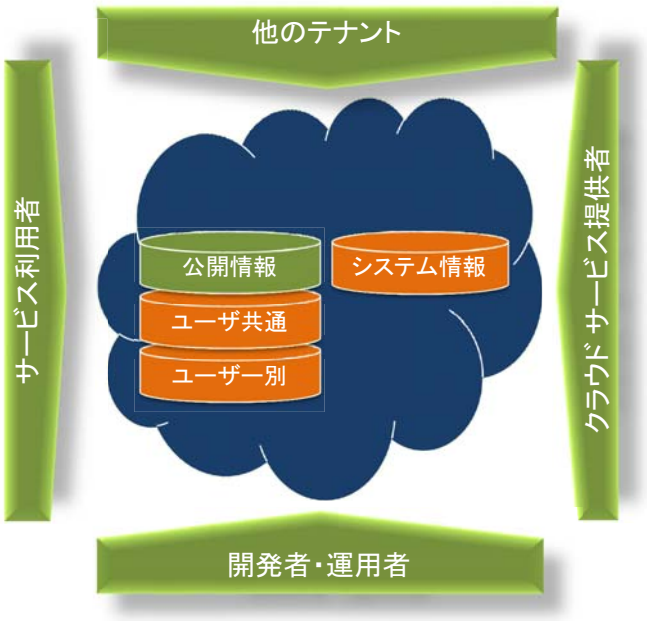
- ストレージ アカウント キーによる分離
- 通信の暗号化、VLAN等のイントラレベルの対策

- 他のテナントとの分離に脆弱性があった場合は、CSPが対処

- データへのアクセス制限
- 疑わしい行為の検出
- 複数レベルの監視、ログ、レポート

- クラウド システム(サービス基盤)の脆弱性は、Windows Azureが対処

イントラネット≒センシティブなデータあり



- 要求されるセキュリティ レベルが上がる
  - ユーザー管理
    - アカウント情報
  - 改ざんと漏えいの防止
    - 運用管理者アカウント
    - マルチ テナントの他の利用者
    - 不正アクセス
    - 他のユーザー アカウント
  - アクセス元管理
    - 原則イントラネット内からアクセス
  - DoS/DDoS
    - 一般的には、クラウドが有利

不正利用からの保護と脆弱性の対処 イントラネットを展開する場合

- ID間の分離はアプリに依存
- 認証基盤(フェデレーションが可能)
- Windows Identity Foundation(WIF), Windows Live ID, Open ID

- SQL Azure：アクセス元制限が可能
- Windows Azureでは、Webロールでアクセス元制限を行うことが可能

- アプリケーションの脆弱性はWindows Azureユーザーが対処

- システム設定の脆弱性等は、Windows Azureユーザーが対処
- システムの脆弱性対策(更新等)は、Windows Azureが対応(規定値設定)

- ストレージ アカウント キーによる分離
- 通信の暗号化、VLAN等のイントラレベルの対策

- 他のテナントとの分離に脆弱性があった場合は、CSPが対処

- ID管理の問題は利用者が対処
- クラウドの認証基盤の問題は、Windows Azureが対処

- 開発者・運用者向けの接続の脆弱性は、Windows Azureが対応

- Live IDと、SMAPIによる証明書を使ったアクセス認証

- データへのアクセス制限
- 疑わしい行為の検出
- 複数レベルの監視、ログ、レポート

- クラウド システム(サービス基盤)の脆弱性は、Windows Azureが対処

クラウドサービス利用における主要な懸念点

サービス利用上の懸念点

- クラウドプラットフォームは安全なのか
- サービスがダウンしたらなにもできないのか
- データが漏れたらどうするのか
- 運用者は信用できるのか
- SLAは信用できるのか

Azureのセキュリティ対策

レイヤ	対策
データ	▪ ストレージ アクセス制御のための秘密キー ▪ パーティ間のデータ転送における SSL サポート
アプリケーション	▪ 部分信頼のもとでの .NET コード 実行 ▪ 最低限の権限しか持たない Windows アカウント
ホスト	▪ 余分な装備を取り除いた Windows Server 2008 R2 OS イメージ ▪ 外部のハイパーバイザーによるホスト境界の強化
ネットワーク	▪ VM へのトラフィックを制限するファイアウォール設置 ▪ VLAN、ルーターにおけるパケットフィルタリング

サービスがダウンしたらなにもできないのか?

Office 365 SLA: Service Level Agreement

- 99.9%の稼働率(月間)
  - 年間10時間以内の計画停止は含まない

Office 365 Disaster Recovery and Data Retention

- Office 365のデータは、定期的にデータ―センター内のディスクにバックアップされる
- 加えて、セカンダリーのデータセンターへも定期的にバックアップされる
- データセンターに致命的な問題が発生した際には、セカンダリーのデータセンターにフェイルオーバーする
  - Recovery Time Objective (RTO):サービス復旧までの時間
  - Recovery Point Objective (RPO): データを失う可能性のある時間

サービス	データ保有期間	RTO	RPO
Exchange Online	削除アイテムのリカバリー= 14 日 削除したメールボックスのリカバリー = 30 日	4 時間	2時間
Microsoft SharePoint® Online	削除アイテムのリカバリー = 30 日	24 時間	12時間
Microsoft Lync™ Online	N/A	72時間	24時間

サービスがダウンしたらなにもできないのか?

Exchange Online

- PC上のOutlook のキャッシュファイルを使った作業が可能
  - サービス停止時に、送受信はできないが、過去のメールの閲覧、検索、メールの作成はできる
- OWAのアクセスはできなくなる

SharePoint Online

- PCに保存したデータについては操作可能
  - ただし、SharePoint Onlineからのダウンロード、アップロードはできない

データが漏れたらどうするのか?

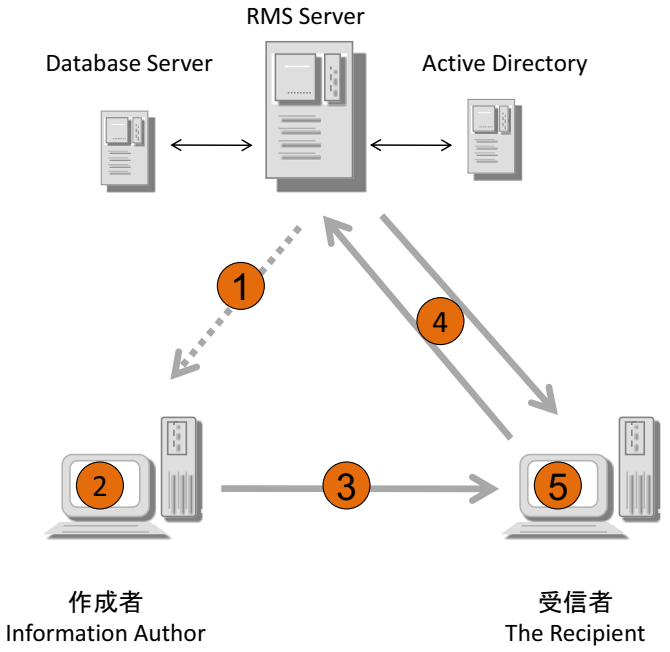
Exchange Online

- RMS（Rights Management System)を利用したメールと添付ファイルの保護

SharePoint Online

- RMS（Rights Management System)を利用したメールと添付ファイルの保護

データレベルの暗号化（RMS）の基本的な動作と利点



RMSの基本的な動作

①作成者は、RMSの設定に際して、RMSサーバからクライアントライセンス証明書を受け取る。
②作成者は、一連の権利とルールを定義する。アプリケーションは、RMSクライアントソフトを使って“発行ライセンス”を作成し、ファイルを暗号化する
③作成者は、必要に応じて任意の方法でファイルを配信する。
④受信者が、ファイルを開くと、RMSサーバを呼び出す。RMSサーバはユーザーの検証を行い、使用ライセンスを発行する。
⑤アプリケーションは、ファイルを複合化し、使用ライセンスにおいて定義された権利を適用する。

RMSの利点

- ファイルが移動しても、暗号や付与した権利が維持される。
- 万一、社外にファイルが流出しても、情報が漏れる可能性は極めて少ない。
- ファイルを開く際に、必ずRMSサーバにアクセスが行われるので、ファイルアクセスの追跡ができる。
- 特定のドキュメントへのアクセスを、後から禁止することもできる。

運用者は信用できるのか?

Certifications

Services
(Office 365 and Microsoft Forefront® Online Protection for Exchange)

- ISO 27001 (Office 365 and BPOS-Dedicated)
- SAS 70 Type I (Office 365)
- SAS 70 Type II (BPOS-Dedicated)

Data Centers

- ISO 27001
- SAS 70 Type II

Microsoft

- U.S.-E.U. Safe Harbor
- More certifications planned

SLAについて確認する(Windows Azureの例)

コンピューティング コネクティビティ	インスタンス監視 & 再起動	ストレージ Availability	データベース Availability	サービスバス & アクセス コントロール Availability
● Web を通して接続されているサービス ● インターネットに接続されているロールとの外部接続性	● すべての起動中のロールは継続的にモニター ● もしロールに不具合があれば Microsoft が検知し正常な状態に起動	● ストレージ サービスの利用可能（接続可能）性 ● ストレージ リクエストのプロセスが成功したかどうか	● インターネット ゲートウェイに接続されるデータベース ● すべてのデータベースは継続的にモニター	● サービスバスとアクセスポイントのエンドポイントは外部接続性を持つ ● メッセージ操作リクエストが正常にプロセス完了したかどうか
>99.95%	>99.9%	>99.9%	>99.9%	>99.9%

SLAを考える上でのポイント -1

- SLAの契約(agreement)：努力目標にしない
  - 本来、SLAの契約には、サービスレベルが守られない場合のペナルティを明記するが、日本では明記しないケースが少なくない。
  - この場合、SLAと呼ぶよりは、SLO(Service Level Objective: サービスレベル目標)と呼んだ方が適切と思われる
- データ保障、バックアップ
  - あってはならないことだが、クラウド上のデータが何らかの理由で無くなった場合、CSPによる復旧は困難
  - クラウドのファイルシステムは、一般的なファイルシステムと違うため、バックアップとリストアが、これまでよりも困難で、制限される可能性がある
  - ミラーリングとバックアップを区別して考える必要がある

SLAを考える上でのポイント -2

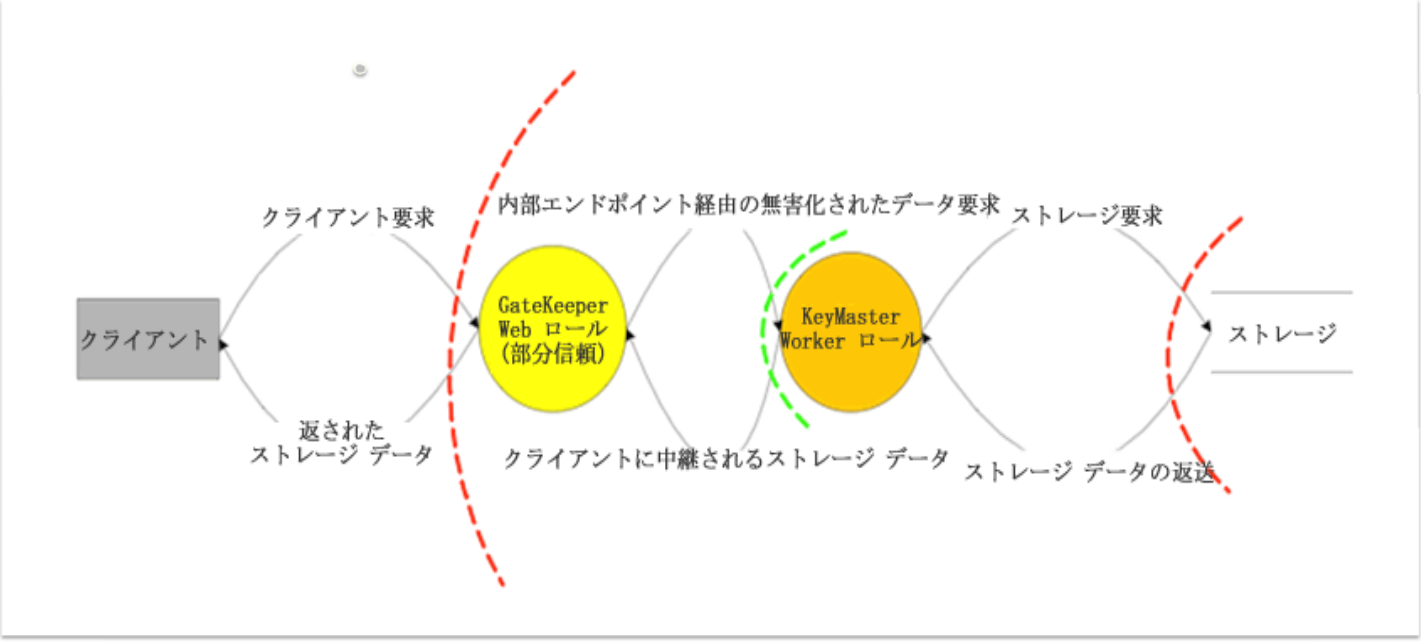
- 稼働率について
  - 工学的な意味での稼働率(信頼性)は、MTBFとMTTRの組み合わせだが、SLAではMTBF/MTTRの記載がないのが一般的
  - 稼働率が、年間なのか、月間なのか、週間なのかに注意する
    - 99.9%の稼働率の場合、それぞれ最長の非稼働時間は、年:8.8時間、月:0.7時間、週:0.2時間　となる
  - 例外措置にも注意する
    - 10分未満の停止は、停止とは扱わないなど
  - サービス停止に伴う損失を補償しないことが一般的
  - 通常のシステム運用を自社で行った場合、99.9%の稼働率を維持することは、かなり大変な作業になる。
    - 月間で考えた場合、42分しか停止できない

WINDOWS AZUREにおける セキュリティの実装

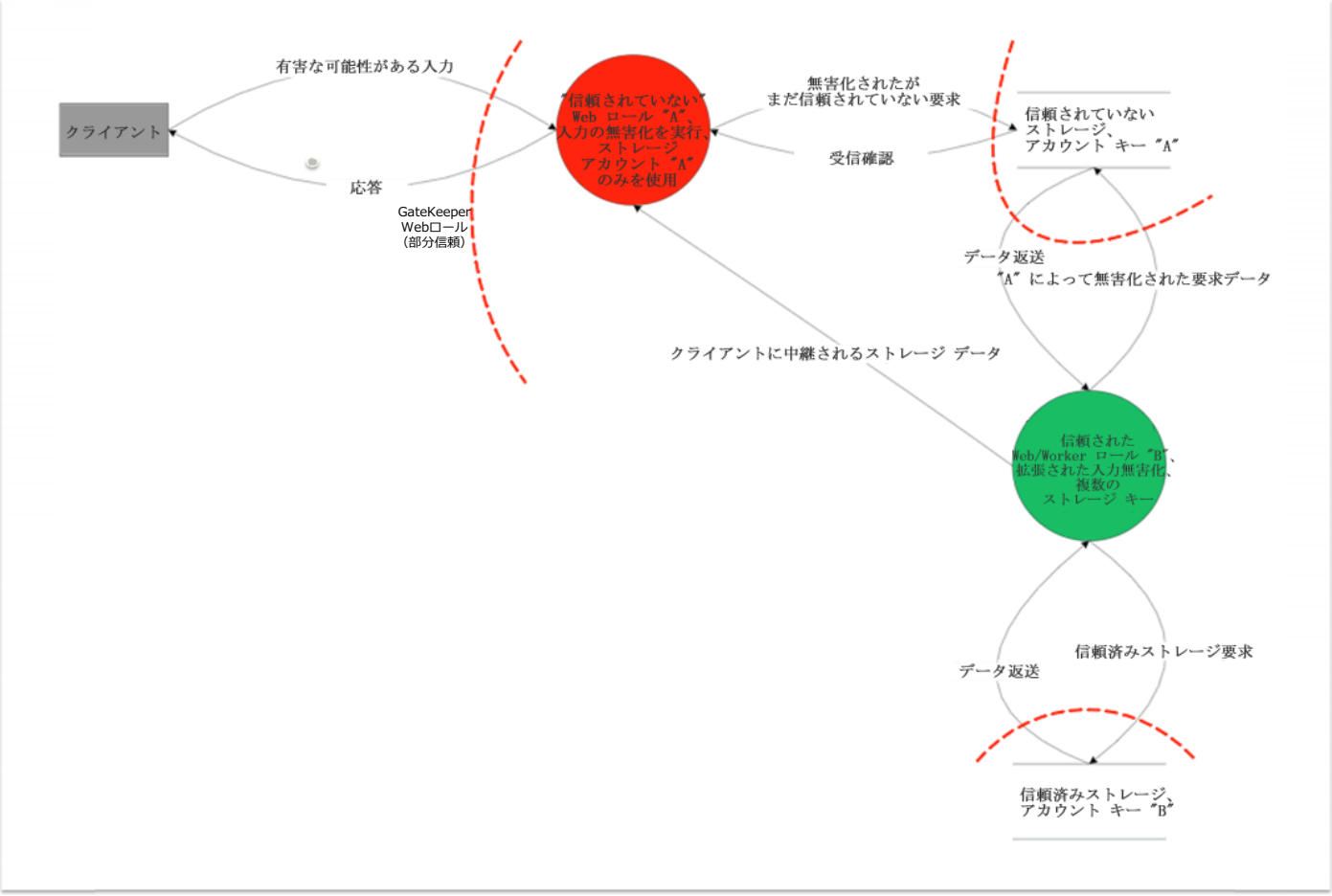
事故前提の対策：データアクセスの制限

- 実行権限の制限：ASP.NET partial trust(部分信頼)での実行(設定が必要)
  - アプリケーションへの侵入が成功した場合でも、システムリソースなどへのアクセスを防止するため、 ASP.NET partial trust(部分信頼)で実行する。
- ストレージアクセスの設計
  - Webロールから直接ストレージにアクセスせずに、Workerロールを通じてストレージにアクセスをする(Gate Keeper Design)
  - 重要度に応じてストレージを分離し、信頼度の低いロールには、重要度の低いストレージのみのアクセスを許す(Multi key design)

アプリの対策：GateKeeperモデル



アプリの対策：マルチキーモデル



事故前提の対策：データの保護

- データの暗号化
  - データが流失・漏えいした場合でも、機密が守られるように、暗号化サービス プロバイダー (CSP) を利用してデータの暗号化を行う
- バックアップ
  - ストレージのバックアップを行う
    - オンプレミスまたは、別の国で運営されている Windows Azureへバックアップを行う

監査証跡

- 監査ログ
  - 任意のログを取得し、ストレージ等に保存が可能
    - コードから生成される Windows Azure のログ
    - IIS のログ
    - Windows 診断インフラストラクチャのログ
    - Windows イベント ログ
    - パフォーマンス カウンター
    - クラッシュ ダンプ
    - カスタム エラー ログ
  - アカウントについては、IDストアのログで管理する

法的な対処への考察

- データが保存される国の法律が適用される問題
- データの傍受、差し押さえなどの問題
  - データの傍受
    - 暗号化による対策
  - データの差し押さえ(システム停止)
    - バックアップによる対処(データのインスタンスを、別の国に展開するなど)

むすび

今、おきているクラウドセキュリティ

- アカウントハックが多発
  - テストケースとしてアカウントを作成し、簡単なパスワードを設定してそのまま利用しているケース
  - クラウド管理用のアカウントは、専用のアカウントを利用し、他の目的には使わない。
  - 複雑なパスワードを徹底する。

むすび

- クラウドは単なる選択肢のひとつである
  - ただし、ITの運用や、ITが基盤となっている企業運営・経営に大きな影響を与えることができる、魅力的な選択肢である
  - もしかすると、システム部門の新しいあり方が問われているのかもしれない
- クラウドのセキュリティも理性的に考える
  - セキュリティ上の要件を分解して考えると、多くのセキュリティ上の懸念点は、対処できるものが多い

忘れてならないのは…

エンドポイント(PCなど)
セキュリティ

参考資料

他の考慮すべき事項(CSA, Security Guidanceから)

項目	内容
ガバナンスとリスクマネージメント	クラウドコンピューティングに対する組織のガバナンスとリスクに対応する能力
法的な問題	クラウドコンピューティングの利用に伴う法的なリスク
コンプライアンスと監査	クラウドコンピューターを利用する際のコンプライアンスの維持と証明
情報のライフサイクルマネージメントガバナンスとリスクマネージメント	クラウド上のデータの管理
ポータビリティと互換性	他のプロバイダーへの移行または、インハウスへの移行

項目	内容
伝統的なセキュリティ、事業継続、ディザスタリカバリー	現在行われているオペレーションプロセスと手順に対するセキュリティと事業継続に対してクラウドコンピューティングが与える影響
データセンター　オペレーション	データセンターのアーキテクチャと運用に対する評価方法
インシデント対応、周知、改善	適切で十分な、インシデントの発見、対応、通知、改善
アプリケーションセキュリティ	クラウドで稼働している、または、開発中のアプリケーションのセキュリティを確保する
暗号と鍵管理	適切な暗号の利用と、スケーラブルな鍵管理
ID管理とアクセス管理	アクセス管理を提供するために、IDを管理し、ディレクトリサービスを提供する
仮想化	クラウドコンピューティングにおける、仮想化の利用

出典：Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1

ENISA: ポリシーや組織に関するリスク

ポリシーや組織に関するリスク	
R.1	データやサービスを他のクラウド提供者に移行困難である。（ロックイン）
R.2	クラウド提供者の情報システムに対するクラウド利用機関による統制が十分取れない。
R.3	アプリケーション特有の要件や規制への適合性をクラウド利用機関が確認できない。
R.4	特定のクラウド利用機関等による不正行為によって、他のクラウド利用機関のアプリケーションが風評の被害を受ける。
R.5	クラウド提供者が営業を停止し、クラウド利用機関のアプリケーションの提供が困難になる。
R.6	クラウド提供者が買収され、同サービスの内容等が変更されてしまう。
R.7	クラウド提供者の業務委託先において問題が発生し、クラウドのサービス提供が困難になる。

ENISA：技術的リスク

技術的リスク	
R.8	計算資源の配分方法等が不適切であり、必要な計算資源がタイムリーに供給されない。
R.9	複数のクラウド利用機関が使用する場合に、クラウド利用機関間における計算資源の分離が不適切であり、情報漏洩等が発生する。
R.10	クラウド提供者の従業員が不正を行い、クラウド利用機関のアプリケーションにおいてセキュリティ上の問題が発生する。
R.11	クラウドのサービスを管理するためのインタフェースに脆弱性が存在し、問題が発生する。
R.12	クラウドの情報システム内における通信データが傍受され、機密データが漏洩する。
R.13	クラウド提供者とクラウド利用機関との間の通信データが傍受され、機密データが漏洩する。
R.14	サービスの利用終了時に、クラウドにおいて管理されるデータを完全に消去困難である。
R.15	分散型サービス拒否攻撃（Distributed Denial of Service）が実行される。
R.16	クラウド利用機関のアカウントを乗っ取る等の手段によって、クラウド利用機関に経済的な損害を与える攻撃（Economic Denial of Service）が行われる。
R.17	暗号鍵やパスワードの紛失・漏洩が発生する。
R.18	攻撃者がクラウドのサービスを利用し、当該クラウドの脆弱性等に関する情報を収集する
R.19	仮想マシン等、クラウドの管理機構（service engine）に対して攻撃が行われる。
R.20	クラウド利用機関とクラウド提供者の責任範囲が不明瞭であり、問題発生時にクラウド利用機関が想定外の損害を被る可能性がある。

ENISA：法的リスク

法的リスク	
R.21	法執行機関によるハードウエア没収や電子証拠開示（e-discovery）により、想定外の情報漏洩が発生する。
R.22	データ・センターの場所によって司法管轄が変更され、想定外の法的措置等が取られる可能性がある。
R.23	クラウドにおいて処理されるデータの保護形態が関連法令に適合しているか否かの確認が困難である。
R.24	クラウドにおけるソフトウエアの利用形態がその使用規約に違反している可能性がある。

ENISA：クラウド特有ではないリスク

クラウド特有ではないリスク	
R.25	クラウドにおいて使用されるネットワークに障害が発生する。
R.26	クラウドにおいて使用されるネットワークの管理が不適切である（輻輳、接続ミス等）。
R.27	ネットワーク上のデータが改ざんされる。
R.28	クラウドの管理やサービス利用における権限が乗っ取られる。
R.29	クラウドにおける運用上の問題から無権限者によるなりすましが可能となってしまう。
R.30	操作ログの紛失・改ざんが発生する。
R.31	セキュリティ・ログの紛失・改ざんが発生する。
R.32	バックアップされたデータの紛失・盗難が発生する
R.33	計算資源への不正アクセスが発生する。
R.34	計算機等のハードウエアの盗難が発生する。
R.35	自然災害が発生し、クラウド利用機関のアプリケーションが停止する等の影響が及ぶ。

リファレンス：クラウド全般

マイクロソフトのクラウドコンピューティング
http://www.microsoft.com/japan/cloud/

Windows Azure Platform 製品情報
http://www.microsoft.com/japan/windowsazure/

Windows Azure Platform 開発者情報
http://msdn.microsoft.com/ja-jp/windowsazure/

クラウド開発
http://msdn.microsoft.com/ja-jp/windowsazure/

Windows Azure の法的情報
http://www.windowsazure.com/ja-jp/support/legal/

リファレンス：クラウドのセキュリティ

Windows Azure セキュリティ概要
http://download.microsoft.com/download/E/9/1/E91ADDD8-6E37-4E7B-84B8-77AFE27E5DB2/WindowsAzureSecurityOverview_20100922.pdf

Windows Azure アプリケーション開発におけるセキュリティのベストプラクティス
http://download.microsoft.com/download/2/E/7/2E7D98A8-2B3E-4936-B09C-7BF3956177F5/SecurityBestPracticesWindowsAzureApps_20100624.pdf

Introducing Windows Azure Diagnostics
http://blogs.msdn.com/b/sumitm/archive/2009/11/18/introducing-windows-azure-diagnostics.aspx

Windows Azure における暗号化サービスとデータ セキュリティ
http://msdn.microsoft.com/ja-jp/magazine/ee291586.aspx

Windows Azure でログ記録とトレースを制御する
http://msdn.microsoft.com/ja-jp/magazine/ff714589.aspx

参考資料

Windows Azure: ホワイトペーパー
http://www.windowsazure.com/ja-jp/community/whitepapers/

Windows Azure™ のセキュリテけと コンプラ□かンスについてのFAQ
http://download.microsoft.com/download/5/1/2/512208B9-AA0F-4188-A016-FCEAC2D1906E/AzureSecurityFAQ_Japan.pdf

Windows Azure Trust Center
http://www.windowsazure.com/en-us/support/trust-center/

Office 365 セキュリティセンター
http://www.microsoft.com/ja-jp/office365/trust-center.aspx

Office 365クラウドに対するアクセスの2要素認証によるセキュリティ保護
http://community.office365.com/ja-jp/forums/358/t/63471.aspx

Microsoft