WHITE PAPER:

White Paper

5 分でわかるクラウドセキュリティの 5 つのポイント

クラウド導入を検討している企業担当者様向け

Symantec

Norton SECURED powered by Symantec

CONTENTS

はじめに

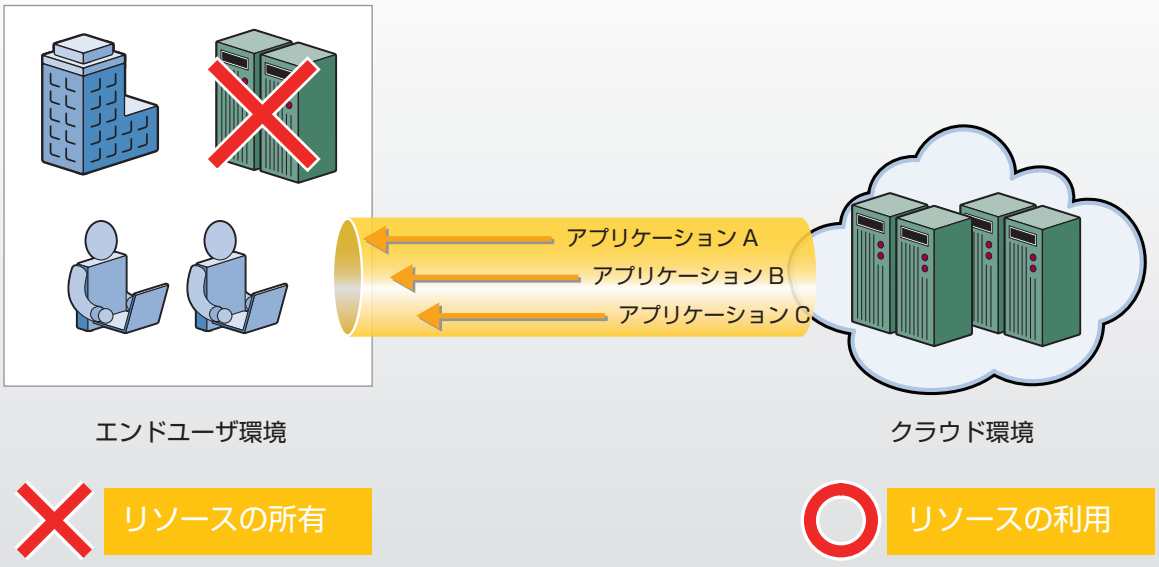
「クラウド」というキーワードは、IT に関わっている企業担当者だけではなく、テレビや新聞雑誌などを通じて一般消費者でも認知されるようになっています。「クラウド」をシンプルに表現すると、アプリケーションやサーバリソースなどを【所有する】のではなく、【利用する】形態のことです。今までアプリケーションをダウンロードしてパソコンにインストールして利用していたものが、インターネット経由でブラウザ等を通じて必要なときに必要なだけ利用することになるため、エンドユーザは安価にアプリケーションやサービスが利用できるようになります。また、サービスを提供する企業や公共団体は、短期間で安価にサービスの提供開始ができるようになります（「クラウド」の定義に関しては、文末のコラムで掲載）。

一方、重要なデータがデータセンターで管理され、インターネットを通じて利用することになるため、セキュリティに関する懸念が増えます。つまり、インターネットを前提とするため、常に第三者による不正アクセスや盗聴などの攻撃により、情報漏えいやデータ改ざんのリスクが今まで以上に顕在化します。特に、自社の情報セキュリティポリシー策定や運用が十分でない場合、どこから対策を行ってよいのか、わからないケースが多いと思います。

本ホワイトペーパーでは、クラウド導入を検討している企業担当者様向けに、クラウドセキュリティに関する 5 つのポイントを掲示することで、より安全にクラウドでサービス提供ができるように解説してきます。この 5 つのポイントをおさえることで、情報セキュリティポリシー策定や運用に不安がある場合でも、どのように対策を行っていけばよいのかわかります。また、先進的な事例をご紹介することで、具体的な対策について解説します。

1. クラウド導入前に検討すべき内容
2. クラウドセキュリティの 5 つのポイント
3. 導入事例

クラウドの定義

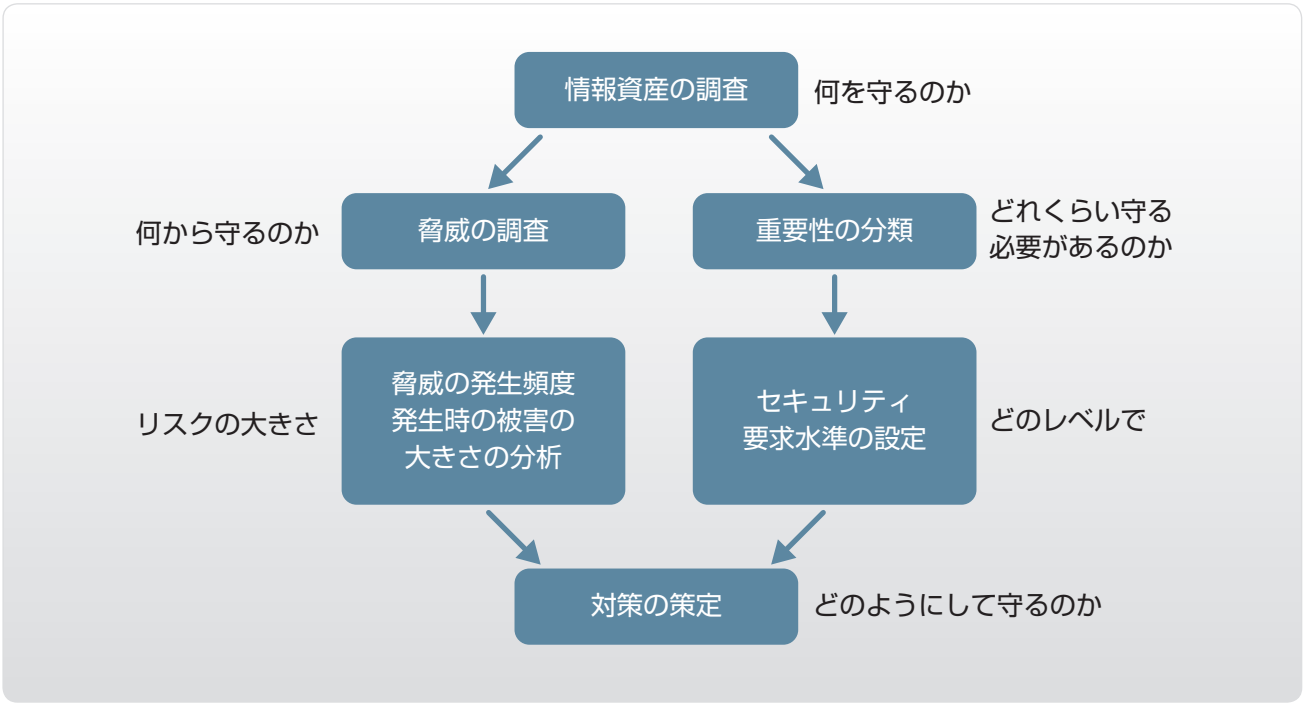


クラウド環境ではリソースを【所有する】から【利用する】形態へ

1. クラウド導入前に検討すべき内容

クラウド導入にあたって、今までにない特別な目新しいセキュリティ対策というのは基本的には存在しません。クラウド、ホスティング、ASP、社内サーバ(オンプレミス環境)に共通して言えることは、セキュリティの基本要素をおさえることが重要であるということです。つまり、その企業の情報セキュリティ戦略や情報セキュリティポリシーに従い、情報資産や対象データの重要度を分類し、その重要度に応じたアクセス制御や運用設計、危機管理体制を構築することが必要です。

各種調査結果によると、クラウド導入においてセキュリティに不安があるため採用をためらうという意見が多数あります。今までは、社内のサーバに保管していたデータに対して社内 LAN/WAN 経由でアクセスしていましたが、クラウドではクラウド事業者のデータセンターに保管されるデータに対してインターネットを経由してアクセスするようになります。このため、第三者による不正アクセスや盗聴による情報漏えいやデータ改ざんなどの不安が存在するのです。企業にとって重要なデータとは何かを分類し、重要度に応じた管理体制や運用設備を使い分けることが必要です。



情報資産の重要度に応じた対策手順

データ種類	データ価値		リスク評価		対策例
	重要度	公開レベル	金銭・機会損失	信用・ブランド損失	
製品カタログ、価格表	中	公開	小	中	パブリッククラウドにコンテンツを公開。コンテンツのアップロード権限の厳格な管理、データの改ざん対策を実施。
勤怠管理	中	社外秘	中	小	信頼性の高いパブリッククラウドにアプリケーションを構築。SSL による通信の暗号化や ID/ パスワードでのアクセス制御を実施。また、定期的なバックアップやアクセスログ管理を実施。
顧客リスト	大	極秘	大	大	重要度の高いデータのため、堅牢で厳格なプライベートクラウドやオンプレミス環境にデータを管理。SSL による通信の暗号化やワンタイムパスワードでのアクセス制御を実施。また、定期的なバックアップやアクセスログ管理、監査証跡を取得。さらに、DLP※1 による情報漏えい対策を実施。

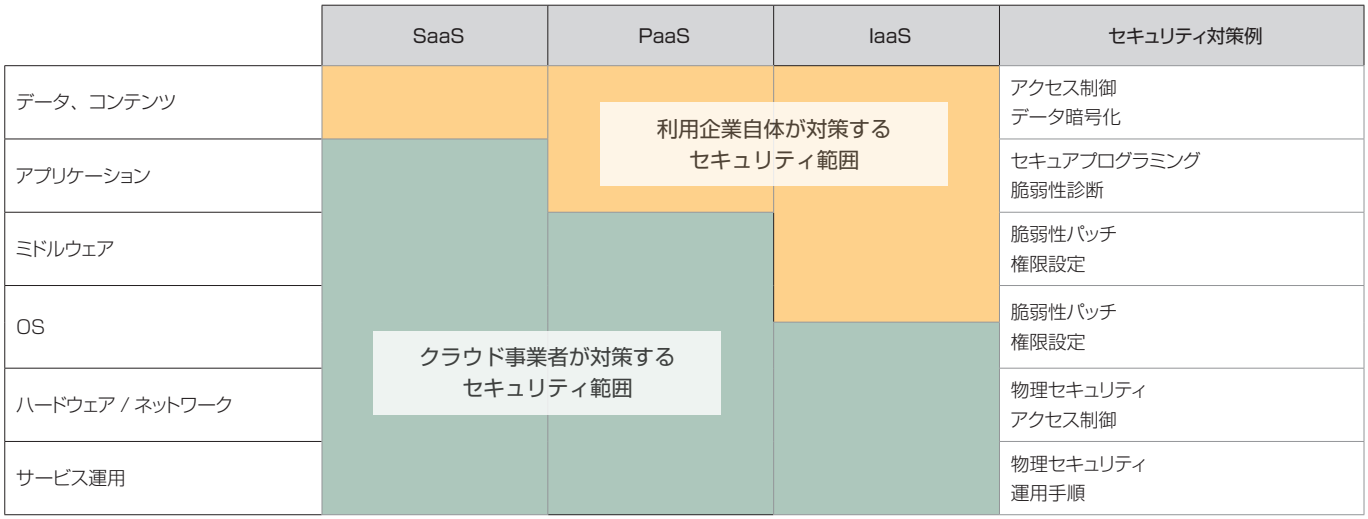
情報資産評価の例

このようにクラウドを導入するためには、自社の情報セキュリティポリシーを再度確認し、クラウドで利用する予定のデータの重要度やサービス、アプリケーションの特性を鑑みた対策を取ることが必要です。クラウドを導入検討している企業の社内では、本当にクラウド事業者に情報を預けても問題ないのか、という意見が出てクラウドの採用が進まないというケースがあるようです。このような場合でも、あらためて上記のような情報資産の整理を行い、リスク評価とそれに対する対策を明確にすることで、クラウドの導入障壁が下がります。なお、リスク評価手法については、既に確立されたものがあり、ISMS や ISO/IEC27001 などで定義された手法が参考になます。

※ 1：data loss prevention、data leak prevention の略。保存場所や使用場所に左右されずに機密データを検出、監視、保護する包括的な情報漏えい対策のこと。

2. クラウドセキュリティの 5 つのポイント

クラウドのサービスには、その提供形態によって、SaaS / PaaS / IaaS に分かれます。SaaS / PaaS / IaaS 毎に責任分界点が異なり、「クラウド利用企業自体が対策するセキュリティ」と「クラウド事業者が対策するセキュリティ」に分かれます。



[SaaS]

SaaS 利用企業は、データやコンテンツに関してのみ自社でセキュリティ対策が必要になります。例えば、Salesforce.com の場合、ログイン ID/ パスワードのポリシー設定、コンテンツやデータに対するアクセス権限設定は自社のセキュリティポリシーを遵守した設計が必要になります。一方で、アプリケーションからサービス運用までの領域はクラウド事業者がセキュリティ対策を実施します。

[PaaS]

PaaS 利用企業は、データからアプリケーションまでの領域のセキュリティ対策が必要です。特にアプリケーションに関しては、近年の SQL インジェクション攻撃やクロスサイトスクリプト攻撃などを想定したセキュアなアプリケーションを構築する必要があります。また、定期的な脆弱性診断やマルウェアスキャンを実施することで、最新のセキュリティ脅威に対する対策も重要です。具体的な PaaS のサービスとしては、Microsoft の Windows Azure が挙げられます。

[IaaS]

IaaS 利用企業は、データからミドルウェアまでの領域のセキュリティ対策が必要です。Amazon の AWS では、仮想マシン上で稼動する OS が併せて準備されています。利用企業は、この OS に対して、ミドルウェアをインストールして利用します。ミドルウェアに対するパッチ適用や脆弱性対応などの対策が必要です。

次の表は、クラウドの導入を検討している企業が特に気をつけていただきたいポイントをまとめたものです。

5 つのポイント

① SSLサーバ証明書やSSHにより、通信データを暗号化すること

クラウドでは、データがクラウド事業者のデータセンターに保管されるため、通常はインターネットを経由してサービスを利用することになります。インターネットを経由することは、通信経路上で盗聴や改ざんなどのリスクが発生します。公開情報でない限り、必ず通信データを SSL によって暗号化する必要があります。また、プライベートクラウドのようなイントラネット環境でも、SSL サーバ証明書や SSH を用いることで、組織内部の盗聴によるリスクを回避できます。

具体的対策例	SSL サーバ証明書、SSH、FTP over SSL、POP/SMTP over SSL、S/MIME
ここをチェック	□ https（SSL）による公開サイト領域があること □ 視覚的に本物のウェブサイトであることがわかり、通信データを暗号化できる EV SSL 証明書を利用すること □ 管理コンソール（コントロールパネル）へのアクセスには、http（SSL）によるアクセスが可能であること □ FTP の利用時には、ID/ パスワードを暗号化できる FTP over SSL を利用すること

② ワンタイムパスワードや強固なユーザ認証により、厳格なアクセス制御を実施すること

クラウドでは、インターネットの利用が前提となるため、不正アクセスやなりすましによるデータの閲覧や改ざん、情報漏えいのリスクが発生します。まず、データの重要度を定義し、アクセスするユーザがどのデータに対してどのような操作（閲覧、変更、削除など）を行えるかという権限設定を行うことが重要になります。強固なユーザ認証として、ワンタイムパスワードや SSL クライアント認証が有効です。ID やパスワードを利用する場合でも、類推されやすいパスワードは禁止し、定期的に変更させるような設定にすることが重要です。

具体的対策例	SSL クライアント認証、ワンタイムパスワード、IP アドレス認証、アクセスコントロールソフト
ここをチェック	□ ユーザ認証の強化のため、ワンタイムパスワードや SSL クライアント認証などの二要素認証を利用すること □ データの重要度に応じたアクセス権限やアクセス制御ポリシーを策定し、システムに適用すること

③ セキュアなアプリケーション/OSを構築すること

インターネットを経由したアプリケーションや OS の脆弱性を狙った攻撃により、情報漏えいや改ざんが発生するリスクがあります。最近では、SQL インジェクション攻撃、クロスサイトスクリプト攻撃やアプリケーション /OS の脆弱性を狙った攻撃が主流になっています。攻撃を受けた場合でも影響を軽減させるために、定期的な外部からの診断テスト、開発したプログラムのコードレビューを行うことが重要です。また、攻撃を検知したり、被害の発生をすぐに検知したりするために、リバースプロキシ型の Web Application Firewall の導入、マルウェアスキャン、改ざん検知などが効果的な対策となります。

具体的対策例	脆弱性診断、脆弱性スキャン、マルウェアスキャン、アンチウィルスソフト、セキュアプログラミング、 ソースコード検査、クラウド型 WAF、IDS/IDP、改ざん検知
ここをチェック	□ リリースするアプリケーションに対してコードレビューや脆弱性診断を実施すること □ 定期的な脆弱性スキャン、マルウェアスキャンを実施すること
参考情報	IPA セキュアプログラミング講座 http://www.ipa.go.jp/security/awareness/vendor/programming/index.html

④ データの保管場所を明確にし、暗号化やバックアップの対策を行うこと

海外のデータセンターを利用する場合、政府機関によりデータに対して検閲が入る可能性があります。例えば、米国の場合、米国愛国者法（USA PATRIOT ACT）により、米国内に存在するサーバであればあらゆるデータに対して、米連邦捜査局（FBI）または政府が調査権限を持っています。実際、FBI がデータセンターからサーバを押収したという事例が発生しています。可能である場合、データ自体に暗号化を行う、秘密分散などの技術を採用するなどの対策が必要です。また、可用性の観点から、データのバックアップを定期的に取得することが推奨されます。

具体的対策例	データの暗号化、DB 暗号化、ハードウェアセキュリティモジュール（HSM）による鍵管理、秘密分散処理、データバックアップ
ここをチェック	□ クラウド事業者のデータセンター設置場所を確認すること □ 保管するデータの暗号化を実装すること、強固な暗号アルゴリズムが利用できること

⑤ 適切なクラウド事業者を選定すること

クラウドを導入することは、自社で行う業務の一部をアウトソーシングという意味になります。アウトソーシング先の企業を選定することは、発注者側の責任であり、非常に重要なことです。昨今のクラウドサービスの進化や多様化を鑑みると、この適切なクラウド事業者を選定することとは、非常に困難で時間のかかる業務であるといえます。また、クラウド事業者の経営次第によっては、途中でサービスポリシーが変更になったり、サービス自体を終了したりする可能性もあります。自社のセキュリティポリシーに合致しているかどうかを、サービス仕様書や契約書、及びクラウド事業者へのヒアリングなどを通じて確認することが必要です。

具体的対策例

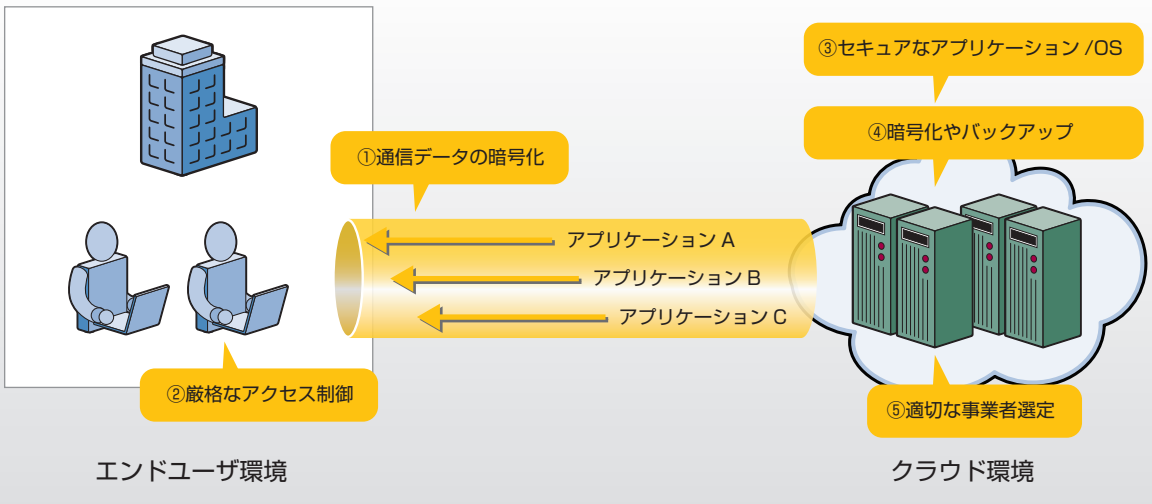
クラウド事業者のサービス仕様書・契約書を確認する、クラウド事業者に対してヒアリングを実施する、コンサルティング会社に事業者選定を依頼する

ここをチェック

- ☐ ハイパーバイザレベルでのセキュリティコントロール有無
- ☐ 仮想マシンイメージやメモリーの完全性検証の仕組みの有無
- ☐ 事業者の脆弱性管理、パッチ管理、構成変更管理、SLA の基準、可能性の管理体制
- ☐ データセンターの物理セキュリティ対策
- ☐ 事業者の障害発生時のサポート窓口や復旧体制、インシデントレスポンス体制、事業継続や障害復旧体制
- ☐ 事業者の ISMS、ISO/IEC27001、プライバシーマーク、SAS70 などの取得有無
- ☐ 事業者の経営状態、事業継続性、過去の導入実績、過去のセキュリティインシデント

参考情報

経済産業省　SaaS 向け SLA ガイドライン
http://www.meti.go.jp/press/20080121004/20080121004.html

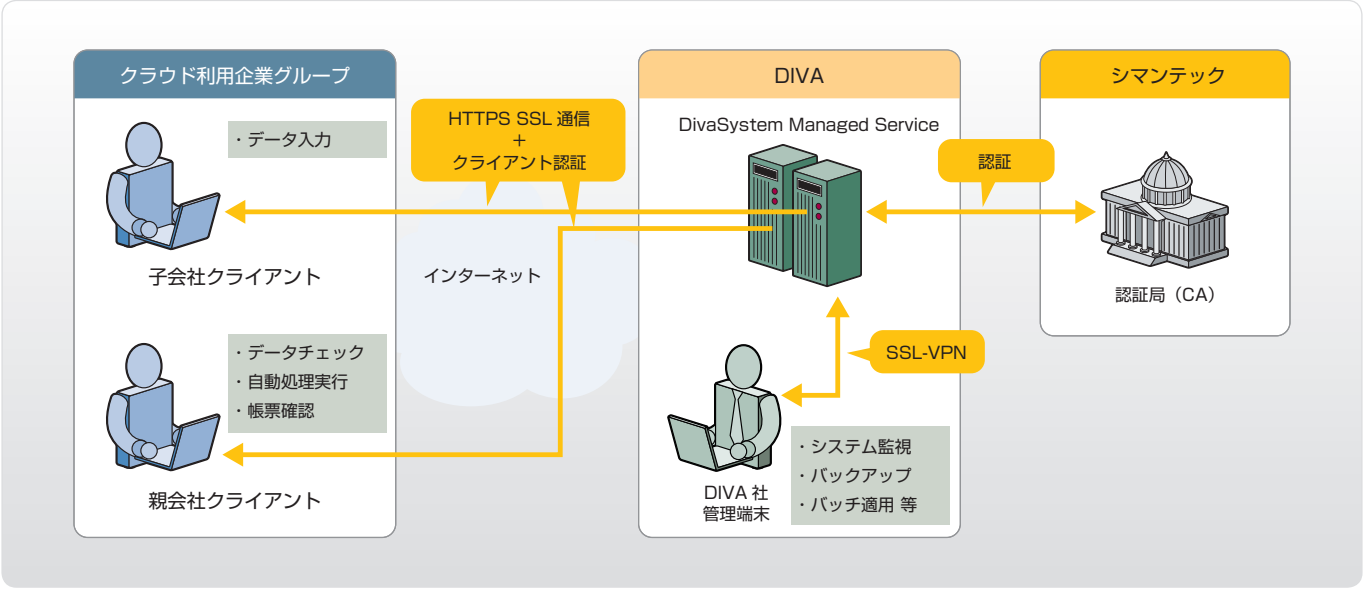


5 つのポイント　（エンドユーザ環境から、通信経路、クラウド環境まで包括的な対策が必要）

3. 導入事例

上場企業の連結会計システム導入の事例

課題	連結決算システムを検討するにあたり、スピーディーに導入が可能で、海外拠点からも利用しやすいクラウド型サービスを検討しているが、機密データの盗聴や不正アクセスに不安を感じていた。
要件	· 開示前の決算情報は、インサイダー情報であり、企業秘密情報のため、アクセス制御や暗号化を強固に行う。 · 海外子会社でも利用できるインターネットを前提とする。 · コストを抑えたい。
ソリューション	株式会社ディーバのクラウド型連結会計システム「DivaSystem Managed Service」を導入。更に、強固なアクセスコントロールや情報漏えい対策を採用。
採用した製品	· Symantec Managed PKI Service · シマンテック SSL サーバ証明書



最後に

情報セキュリティには 100% 安全というものは存在しません。常に、新しい脅威が発生し、対策が必要になります。最も重要なことは、データの重要度を評価し、その重要度に応じた対策を実施することです。非常に重要なデータに関しては、複数の対策を網羅的に実施することにより、セキュリティリスクを限りなく最小化することが可能です。

本ホワイトペーパーでは、可能な限りわかりやすくシンプルにクラウド導入に対する対策を列挙させていただきました。ここで挙げた対策はあくまでもシマンテックとしてピックアップした対策例にはなりますが、クラウドの導入を検討している担当者様にとって少しでもお役に立てることができれば幸いです。

コラム:クラウドの定義

「クラウド（クラウドコンピューティング）」の言葉が示す意味は、説明される状況や説明する者の立場によって様々な定義がさますが、世界的には米国の NIST（国立標準技術研究所）が 2009 年 10 月に定義した文書が活用されることが多いです。このコラムでは、NIST のクラウドの定義について解説します。
（本内容は、NIST の定義に対する翻訳版です。読者の方が読みやすいよう、独自の解釈を含めて翻訳しております。）

参考 URL　http://csrc.nist.gov/groups/SNS/cloud-computing/

NIST が定義するクラウドの必須特性

オンデマンドセルフサービス（On-demand Characteristics）
人手を介在せずに、利用者がサーバやネットワーク、ストレージなどの資源をプロビジョニングできること。

広範なネットワーク経由でのアクセス（Broad network access）
各種端末（携帯電話やノートパソコン、PDA など）から、ネットワークを経由して、標準的な通信方式でアクセスができること

リソースプーリング（Resource pooling）
複数の利用者に対してクラウド資源がマルチテナントモデルで提供されること。一般的に、そこで供給されるリソースの正確な位置を、利用者が制御したり、把握したりすることはない。

迅速な伸縮性（Rapid elasticity）
迅速にスケールアウト / スケールインすることが可能であること。利用者にとって、このリソースが無限に利用できるように見え、必要なときに必要なだけ購入できること。

計測可能なサービス（Measured Service）
自動的にリソース利用を制御し、最適化すること。このリソース利用量の計測結果については、プロバイダーと利用者の双方に透明性があるように、監視、制御、報告されること。

合同会社シマンテック・ウェブサイトセキュリティ
https://www.jp.websecurity.symantec.com/
〒104-0028　東京都港区赤坂1-11-44赤坂インターシティ
Tel : 0120-707-637
E-mail : websales_jp@symantec.com

WPCloudSec2010_1308