NCWGクラウドセキュリティセミナー

第二回「実践クラウドセキュリティ」研修会

ケーススタディを通して学ぶ『実践クラウドセキュリティ』SaaS編

2015年2月2日

株式会社ディアイティ　山田 英史

はじめに

- 本資料では、クラウドサービスを導入する際に検討すべきセキュリティ要件の定義方法を、クラウドサービス選定のケーススタディにより学ぶ一例をしまします。

クラウドを利用したシステム構築の流れ

- セキュリティ要件を主眼に置いたシステム構築の流れ

STEP1	クラウドの導入目的を明確にする
STEP2	情報の流れを明確にする
STEP3	セキュリティ要件を決定する
STEP4	クラウドサービスを選定する
STEP5	利用環境を構築する
STEP6	サービスを社内にリリースする

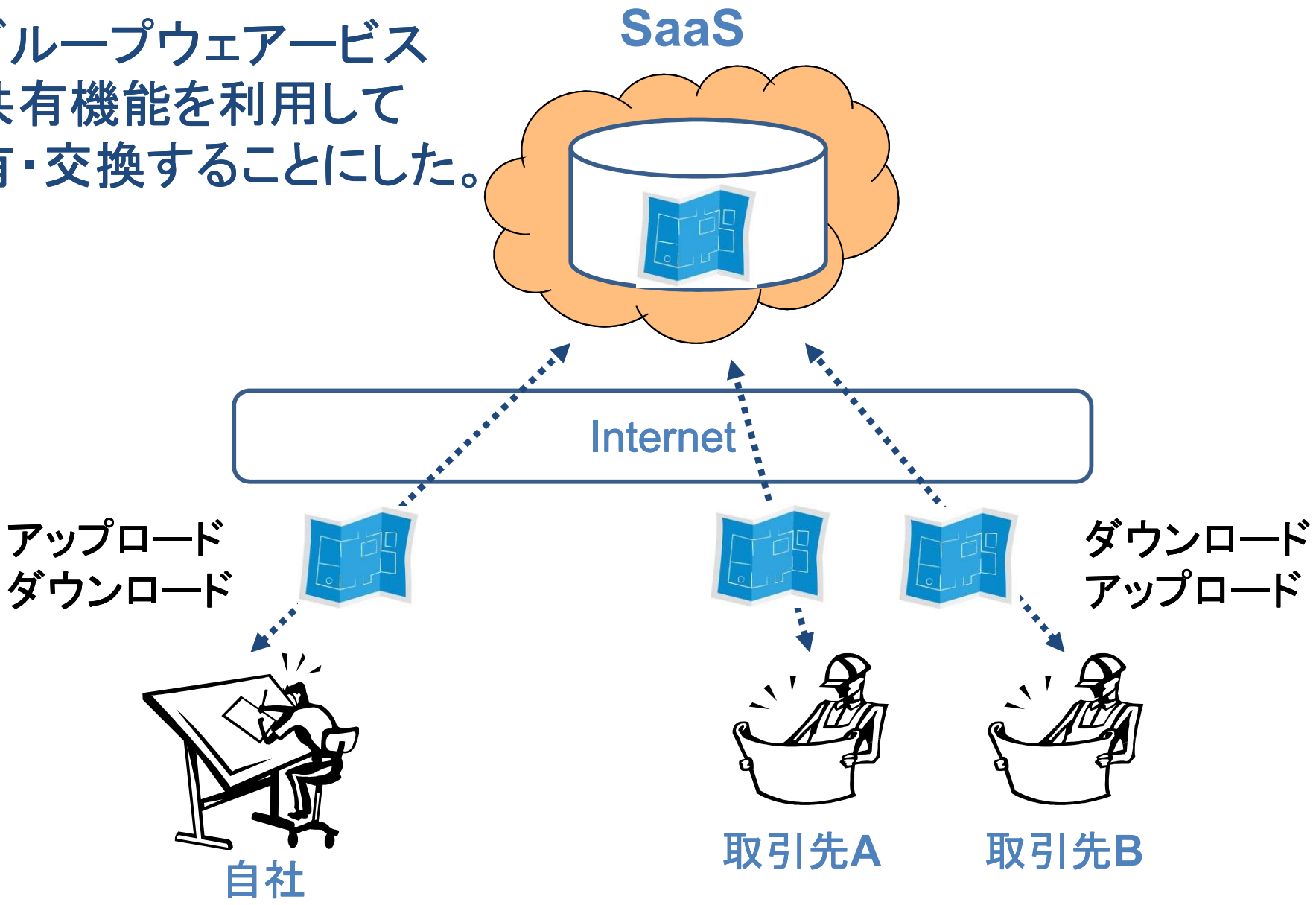
STEP1　クラウドの導入目的を明確にする

■クラウドサービス導入の背景

- 当社は大手自動車メーカである。
- 現在、取引先の部品メーカと図面等製造データの交換をメールに添付して行っているが、次のような問題がある。
  1. 取引先によっては大きな容量のデータがメールで受信できない。
  2. メールは誤送信等のリスクがある。
  3. 製造データがメール添付ファイルとして、複数の受信者の端末に残留する。
- これらの問題を解決するため、ファイル共有が可能なSaaSサービス導入を検討することとなった。

STEP2　情報の流れを明確にする

クラウド型グループウェアービス
のファイル共有機能を利用して
ファイル共有・交換することにした。



STEP3　セキュリティ要件を決定する（1）

セキュリティ条件の検討

- アクセス権限管理は当社が行う。
- 取引先別にフォルダを設定し、フォルダ毎にアクセス制限する。
- Webベースで操作でき、通信経路上のデータが保護できること。
- クラウド上のデータは、インターネットからの不正アクセスから保護されていること。
- クラウド上のデータは、他のクラウド利用者の不正アクセスから保護されていること。
- クラウド上のデータは、クラウド事業者の不正アクセスから保護されていること。

STEP3　セキュリティ要件を決定する（2）

■管理項目毎のセキュリティ要件の定義（つづき）

- アクセス制御
  - 自社及び委託先は、以下の原則でアクセス権を管理する。
    - 本人認証ベースのアクセス制限を行う
    - 各ユーザに一意のIDの付与
    - 役割に応じた最小限の権限の付与
    - 最少人数への権限付与
  - アクセス制御はSaaSの基本機能で行う。
  - クラウド事業者への確認事項
    - アクセス権管理機能
    - 仮想環境の隔離の方法
    - 利用者ID/パスワード管理の機能と設定項目
    - 選択可能な暗号機能

STEP3　セキュリティ要件を決定する（3）

- 管理項目毎のセキュリティ要件の定義（つづき）
  - モニタリング
    - SaaS上の図面データのアクセス記録を定期的に確認する。
    - クラウド事業者への確認事項
      - 利用者がコントロール可能なログの範囲
      - 利用者によるログ管理の機能
      - 利用可能な監視機能
  - 技術的脆弱性管理
    - 自社及び委託先は、各社の責任でマルウェア対策を講じる。
    - クラウド事業者への確認事項
      - アップロード/ダウンロード時のマルウェア対策の機能

STEP4　クラウドサービスを選定する

セキュリティ要件に基づきクラウドサービスを評価する。

- ネットワークのセキュリティ
  - インターネットからの侵入への防御策
  - 経路上の情報保護策
- アクセス制御
  - アクセス権管理機能
  - 仮想環境の隔離の方法
  - 利用者ID/パスワード管理の機能と設定項目
  - 選択可能な暗号機能
- モニタリング
  - 利用者がコントロール可能なログの範囲
  - 利用者によるログ管理の機能
  - 利用可能な監視機能
- 技術的脆弱性管理
  - アップロード/ダウンロード時のマルウェア対策の機能

公開情報で確認
・SLA、規約、約款、WP

チェックリストによる事業者への確認

STEP5　利用環境を構築する

セキュリティ要件を反映したシステム設計を行う

↓

システム設計に基づいた実装と設定を行う
クラウドサービスを契約し設定する

↓

評価計画に基づいた機能試験、動作試験を行う

STEP6　サービスをリリースする

利用マニュアル、管理マニュアルを作成する

利用者を教育・訓練する

関係者にリリース案内する