

# 企業情報システムにおけるWEB APIの利用

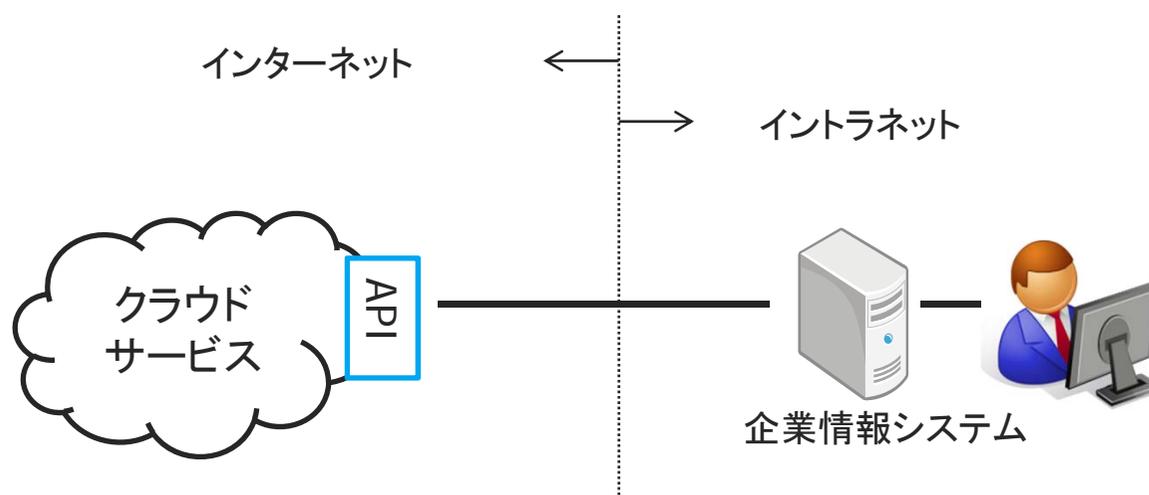
株式会社オージス総研  
齋藤 伸也



- 齋藤伸也(さいとう しんや)
- 株式会社オージス総研 技術部クラウドインテグレーションセンター所属
- 以下の業務に従事する
  - 技術開発
  - 案件支援
  - 提案支援



- 企業情報システムにおけるWeb API利用の実践を通して得られた課題を考察する。
  - Web API：インターネットを介して提供されるアプリケーションやプログラムのためのインタフェース



- Web APIを利用することで、企業情報システムにクラウドサービスを容易に組み込むことができる。
- 従来の企業情報システムの構築とWeb APIの利用は以下の点が異なる。
  - インターネットを介してAPIを呼出す。
  - Web APIを自分たちの都合で変更することができない。

## 利用の課題

1. Web APIのプロトコル/スタイル
2. ID・アクセス情報管理
3. Web APIの認証・認可
4. Web API変更への対応
5. 利用制限への対応

- Web APIのプロトコル/スタイルは様々な種類がある。大きく分けるとSOAP/RESTに分類される。
  - **課題**
    - Web APIごとに異なっている点が多い
    - プロトコル/スタイルに関する情報が十分ではないこともある。
- Web APIごとに利用方法を学ばないといけない。

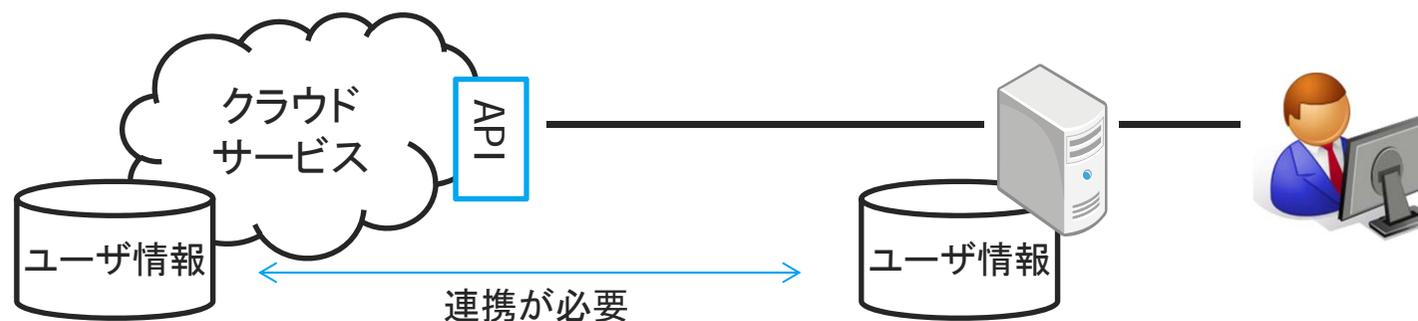
	仕様	メッセージ形式	定義言語
SOAP	W3C	XML	WSDL
REST	なし	XML	WADL
		JSON	なし(サンプルコール)

- SOAP
  - Web APIによっては提供されていないものがある。
    - 新しいWeb APIの大部分がREST APIとなっている。
    - AmazonやGoogleなどのクラウドベンダーはSOAPによるAPIの提供を止めている。
- REST
  - 仕様不在による実装のばらつき。
    - HTTP Methodの使用方法
    - HTTP Responseコード、特に例外/エラー処理
    - URIのスキーム
    - データフォーマット、XML or JSON

## □ 課題の解決のために

- Web API提供側に期待すること
  - 統一したプロトコル/スタイルの提供。
    - 現実的にはかなり難しい。
- Web API利用側のアプローチ
  - 利用者はWeb APIを受け入れるしかない。利用しやすいプロトコル/スタイルのWeb APIを選択する。
  - Web APIを選択する際、以下の観点でチェックする。
    - 利用するプログラミング言語用のライブラリが提供されているか。
    - Web APIのドキュメントが十分に提供されているか。
    - Web APIに関するQAが行えるコミュニティが存在しているか。
    - サポート窓口が存在しているか。

- IDプロビジョニング
  - ユーザ情報の登録, 更新, 削除
- ユーザ情報の変化(入社, 退職, 部署・役職の変化)が一時期に集中して大量に発生する
- 課題
  - プロビジョニングAPIを提供しているサービスが少ない。
  - サービスごとに異なるプロビジョニングAPI。
  - 良い機能を提供していても利用しづらい。Web API ごとにプロビジョニング処理に頭を悩ませる。

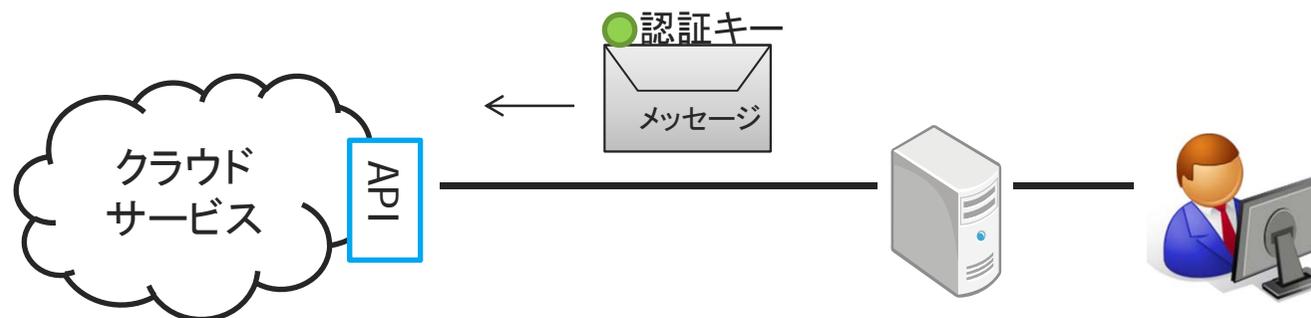


## □ 課題の解決のために

- Web API 提供側に期待すること
  - 標準化されたプロビジョニングAPIを提供するクラウドサービスが増える
    - SCIM (Simple Cloud Identity Management) の策定と普及に期待。
- Web API利用側のアプローチ
  - クラウドサービスのID・アクセス情報管理を統合したソフトウェアを利用する。

- Web APIの認証・認可はWeb 画面による認証と異なり、認証キーやセキュリティトークンを含めてWeb APIを呼出す方式が一般的である。
- 課題 APIごとに異なる認証の仕組み
  - トークンの種類、数
    - 認証キー/セキュリティトークン/アクセスキー etc
  - トークンの取得方法
    - 事前通知/Web画面/トークン取得用API etc
  - トークンを含める場所
    - URL/HTTP header/HTTP body etc

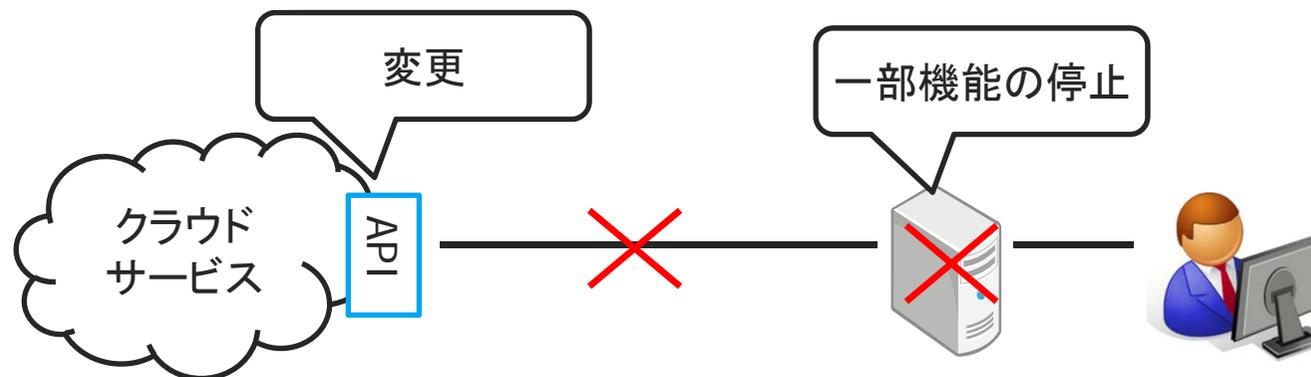
→ Web APIごとに認証の仕組みに頭を悩ませる。仕組みが異なるため、どの程度安全なのかよくわからない。



## □ 課題の解決のために

- Web API 提供側に期待すること
  - 標準化された認証・認可の仕組みを提供するクラウドサービスが増える
    - OAuth 2.0 の策定と普及に期待。
- Web API利用側のアプローチ
  - Web APIの認証、セキュリティに関する正しい知識を身につけ、安全なWeb APIを選択する。

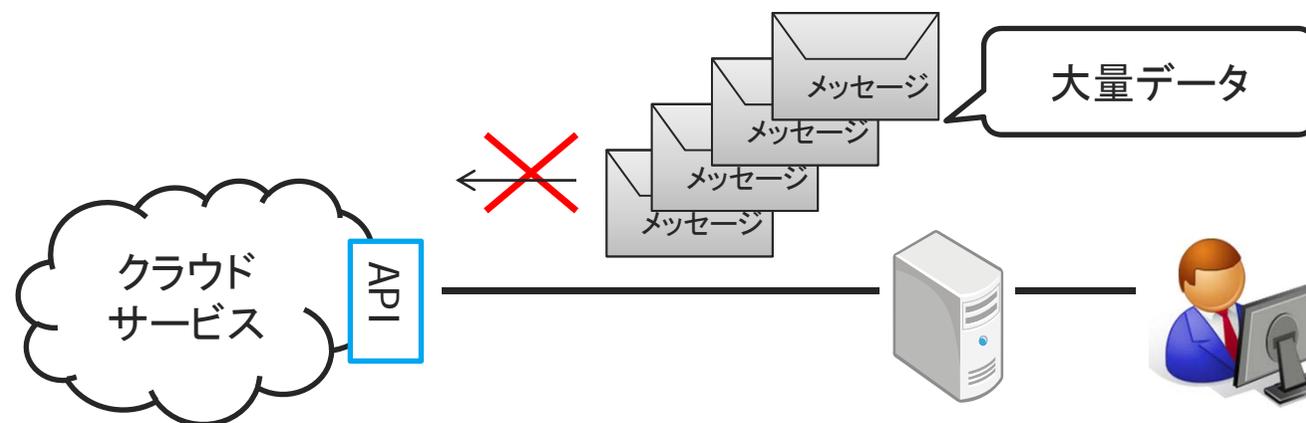
- Web APIのバージョンアップやAPI提供の停止など変更が発生するとAPIを利用して  
いるシステムに大きな影響が発生する。
- 課題 Web API変更への対応
  - Web APIを利用して  
いるシステムが停止する。
  - 変更に対応するためのコストが発生する。



## □ 課題の解決のために

- Web API 提供側に期待すること
  - 互換性のあるWeb APIの提供
  - Web APIのバージョンング情報の提供
- Web API利用側のアプローチ
  - 変更情報のキャッチアップ
  - 変更による影響範囲の局所化
    - システム全体が停止しないように縮退運転を可能にする
    - 腐敗防止層(Anticorruption Layer)[7]パターンの利用
  - 代替Web APIの検討
    - Web API提供の停止のような大きな変更にも備える

- クラウドサービスは負荷を抑えるためWeb APIの利用に制限を加えているものも存在する。利用制限の例は以下の通りである。
  - 単位時間あたりのAPI呼び出し回数
  - リクエスト/レスポンスのデータサイズ
  - コンピュータリソース(CPU、メモリ、ストレージ、ネットワーク帯域)  
クラウドサービスの価格にも関連
  - データの利用範囲
- **課題 API利用制限の範囲内でシステムを実現する必要がある。**



## □ 課題の解決のために

- Web API 提供側に期待すること
  - 利用制限の緩和や廃止。
    - コストの関係で現実的には難しい。
- Web API利用側のアプローチ
  - 利用制限の範囲に収まるような工夫を行う。
    - データサイズ制限：バッチ処理のような大量データを送受信する場合、分割して行う。
    - APIコール制限：呼出頻度を抑えるため、まとめて処理を行う。
    - コンピュータリソース：リソースを多く使う処理は別の方法で実現する。

- 外部のサービスをWeb API経由で利用してシステムを構築する「サービス指向」の時代が来ている。
- 優れたサービスをシステムに組み込んで利用することができるWeb APIは非常に有効であるが、「作るから利用する」の大きなパラダイムの変化により従来のシステム開発・運用にはなかった新たな課題が生まれている。