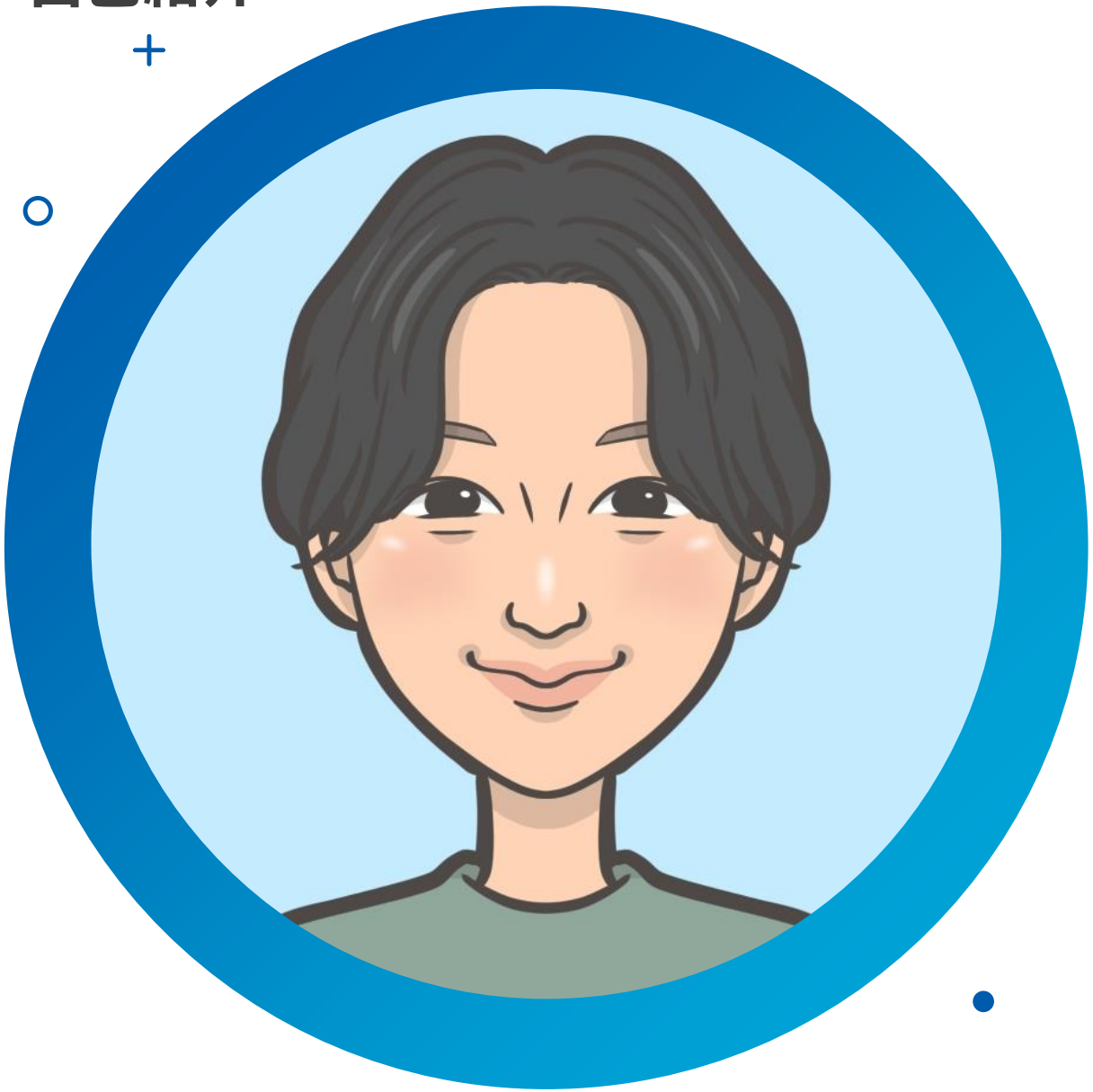
API 通信の管理とセキュリティ対策
NGINX Plus API Gateway で実践

東京エレクトロン デバイス株式会社

アジェンダ

- API とは？
- API 市場について
- API の課題
- API Gateway の役割
- NGINX Plus API Gateway
- デモ
- QA

自己紹介



名前：西川　常（ニシカワ　ジョウ）

経歴：

ネットワークエンジニアとして設計・検証・構築

現在はプリセールスエンジニアとして、F5製品を担当

趣味：

サッカー見てます（J🐬とプレミア）

会社紹介

- メーカー日本法人ができる前からの一次代理店　1999年～
- F5国内販売額9年連続No.1の一次代理店
- 各ブランドに関するPoC、ハンズオントレーニング、構築支援サービス、日本語ヘルプデスクの提供
  - F5 BIG-IP
  - F5 NGINX
  - F5 Distributed Cloud Services
- 保守契約ユーザーに対する手厚い付加価値サービス
  - 会員制Webサポートサイトの提供(製品FAQ、各種ドキュメント等)
  - F5製品の重要情報をPush型でメール配信

    (脆弱性、既知の重大不具合及び改修情報、リリース情報等)

API とは？

API とは？

Application　アプリケーション

Programing　プログラミング

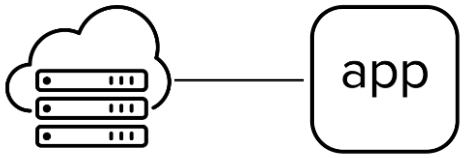
Interface　インターフェース

アプリケーションやサービス同士を連携させるための窓口のこと

API とは？

ひとつのアプリで全てを対応

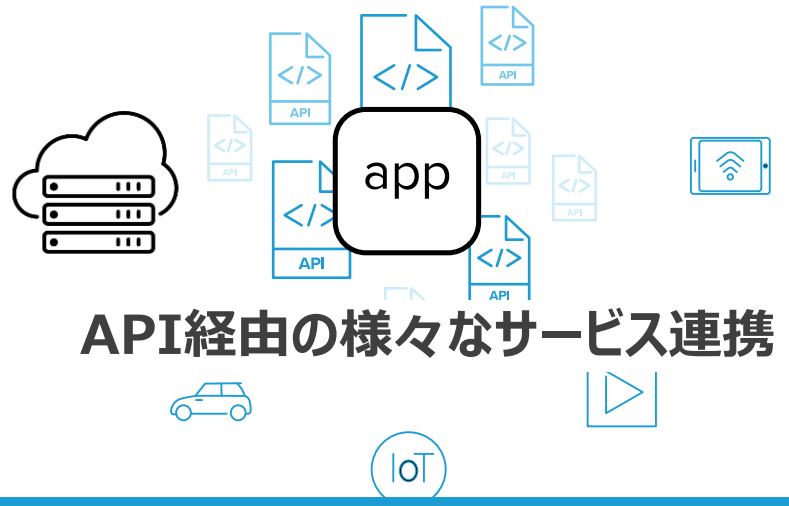
従来のアプリケーション



バックエンドサーバー連携

機能ごとにアプリを分割

今後のアプリケーション

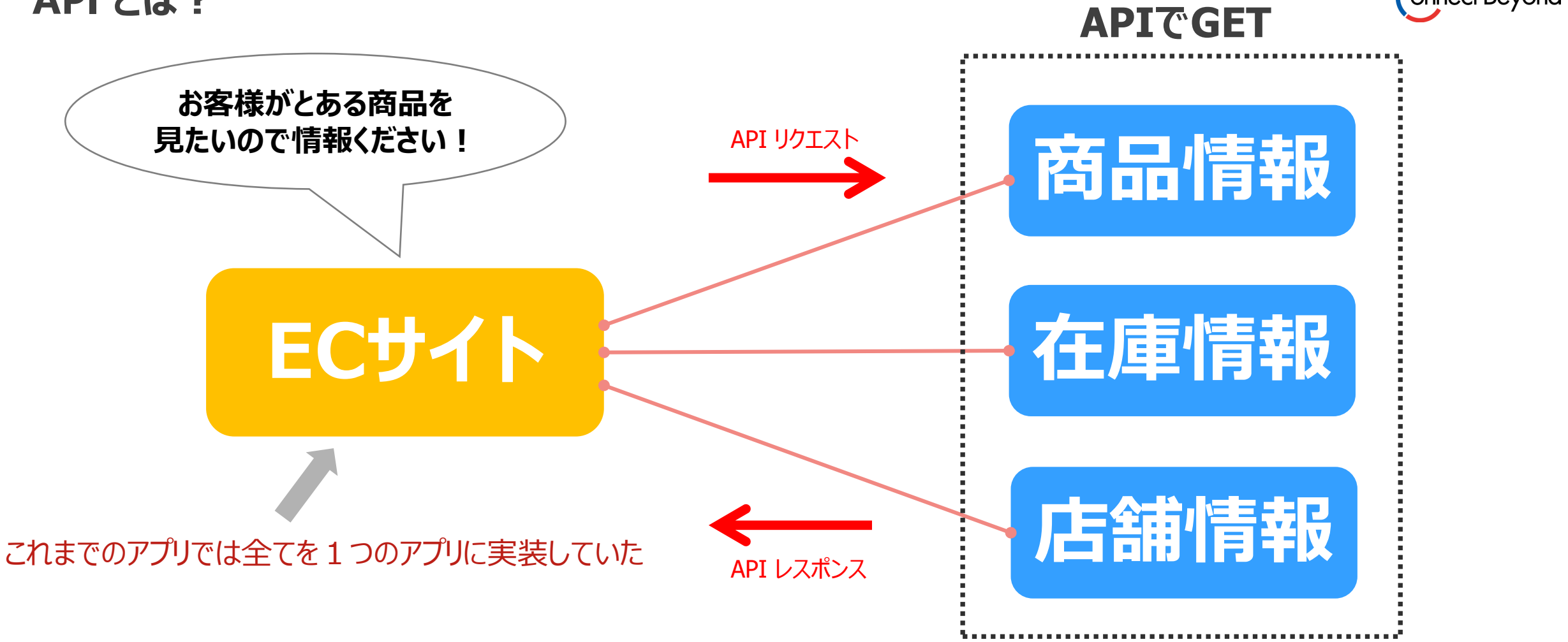


API経由の様々なサービス連携

市場投入までの時間を短縮	マルチデバイス・マルチプラットフォーム
新たなビジネスモデルの開拓	外部企業とのシステム連携

APIアーキテクチャを主流とした、分散アプリケーションへ

API とは？



機能拡張が容易になり開発コストの削減が可能！

API 市場について

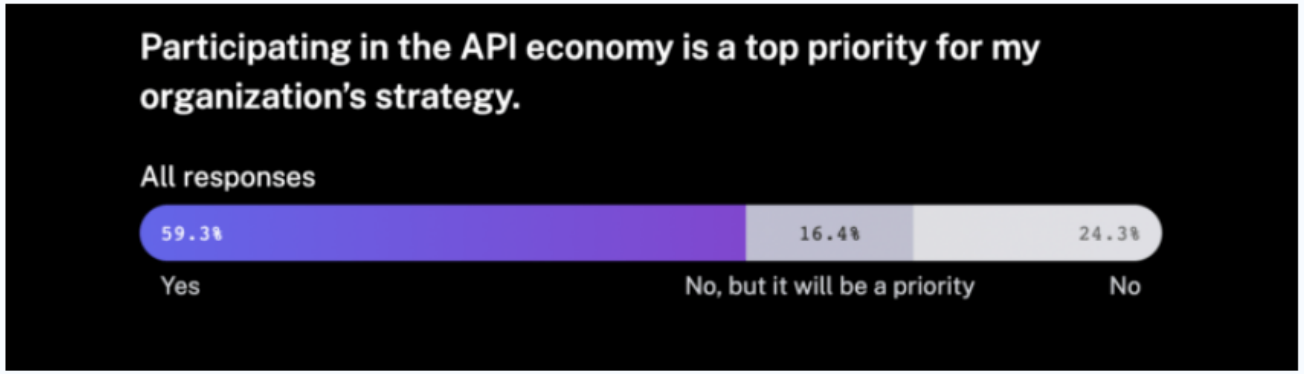
API 市場について

API の需要は高まっており、増加傾向にある

開発者の70%がAPI利用を増やすと回答しており、63%は2022年と比べAPIを活用したと回答している

Demand for APIs is strong—and growing

Everyone, it seems, is jumping on the API bandwagon. Some 70% of developers indicate they will increase API usage this year, while 63% note that they utilized APIs more in 2022 than they did the previous year. As a whole, more than 75% of developers are prioritizing participating in the API economy, or plan to prioritize it soon.



引用:https://rapidapi.com/blog/state-of-apis-growth-and-more-growth-on-tap-for-2023/

API の課題

API ってすごく便利そう・・・
API 使ってみようかなぁ

API の課題

セキュリティ

- 認証/認可の欠陥
- データ漏洩
- 流量制限
- 攻撃者からの攻撃

etc …

管理

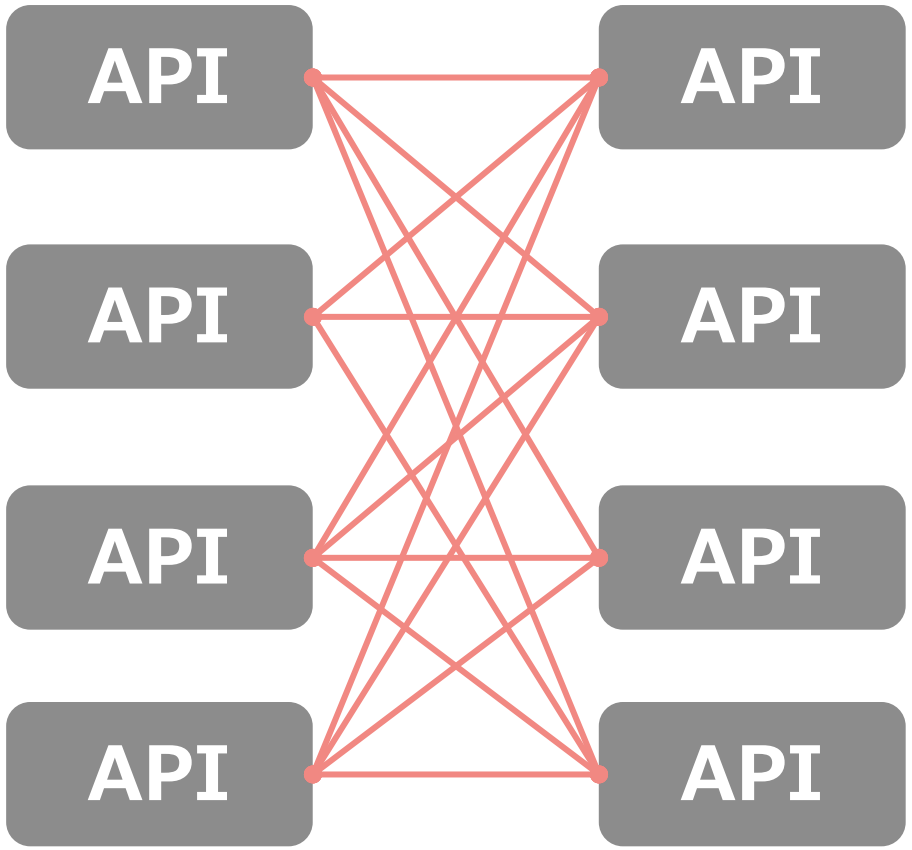
- シャドー API
- APIガバナンスの欠如
- APIドキュメンテーション
- 可視性の欠如

etc …

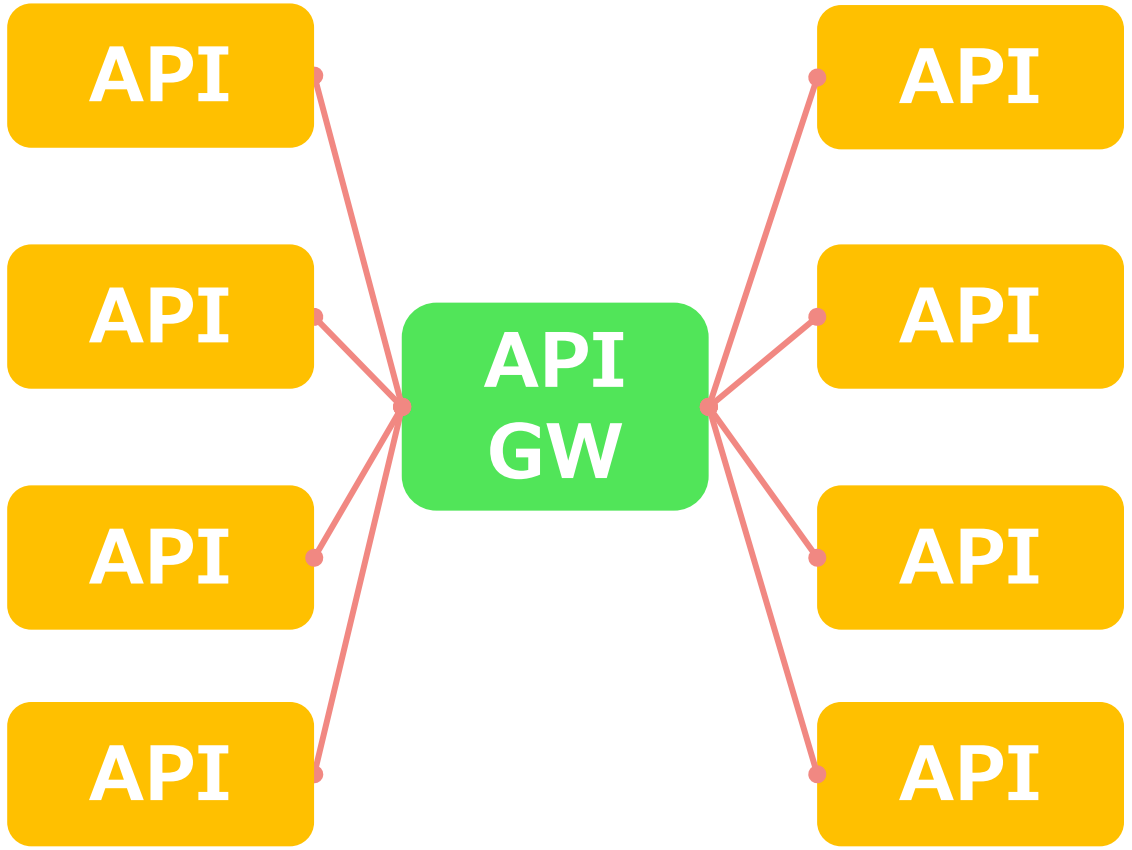
API Gateway の役割

API Gateway の役割

API Gateway がない場合
API 同士が管理されず接続



API Gateway を導入！
API 接続を集中管理



API Gateway の役割

API 通信のセキュリティや管理の向上

認証認可、ルーティング、流量制限、監視、分析、ポリシー、アラート、セキュリティなど

全ての API 要求を受け取り、適切に処理を実施

onnect Beyond

NGINX Plus API Gateway

F5 NGINX の歴史

2002：イゴール・シソエフ (CTO of NGINX, Inc.)
NGINXの開発を開始

NGINX
(オープンソース)

2004：NGINX
最初のリリース

2014：NGINXが世界中上位10,000サイト中
最も利用されているWebServerとなる

2020：シェアTOP(約36%)、
4.5億サイトでWebトラフィックを処理

2011：
Nginx, Inc. 設立

2013：
Nginx Plusリリース

2017：Announced;
- NGINX Controller
- NGINX Unit 等

2019
+
NGINX
買収

APACHE HTTP SERVER PROJECT

Apache httpdでは、1つのサーバーでの同時アクセス数の上限に問題（C10K問題）を感じていた。
Apache httpdより同時アクセス数の多いサーバーソフトもあったが、機能が限定されていた。「そこで、C10K問題に対応しつつ、静的ファイルだけでなくほかのサーバーとの連携機能を持ったWebサーバーとしてNGINXを開発することを決めた」

イゴール・シソエフ

F5 NGINX Plus

リバース
プロキシ

ロード
バランサー

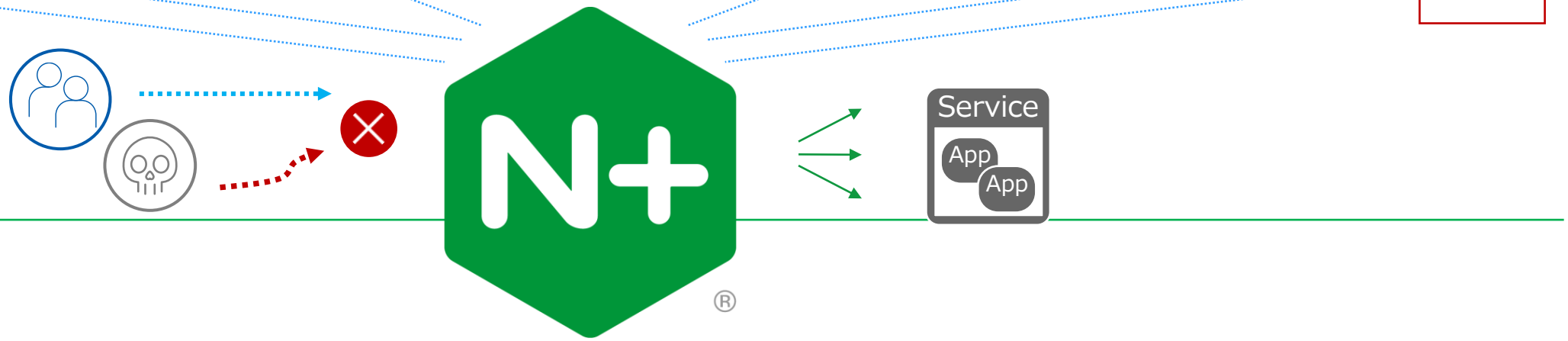
API GW
認証 GW

WEB
サーバ

キャッシュ
サーバ

WAF/
L7DoS

Add On



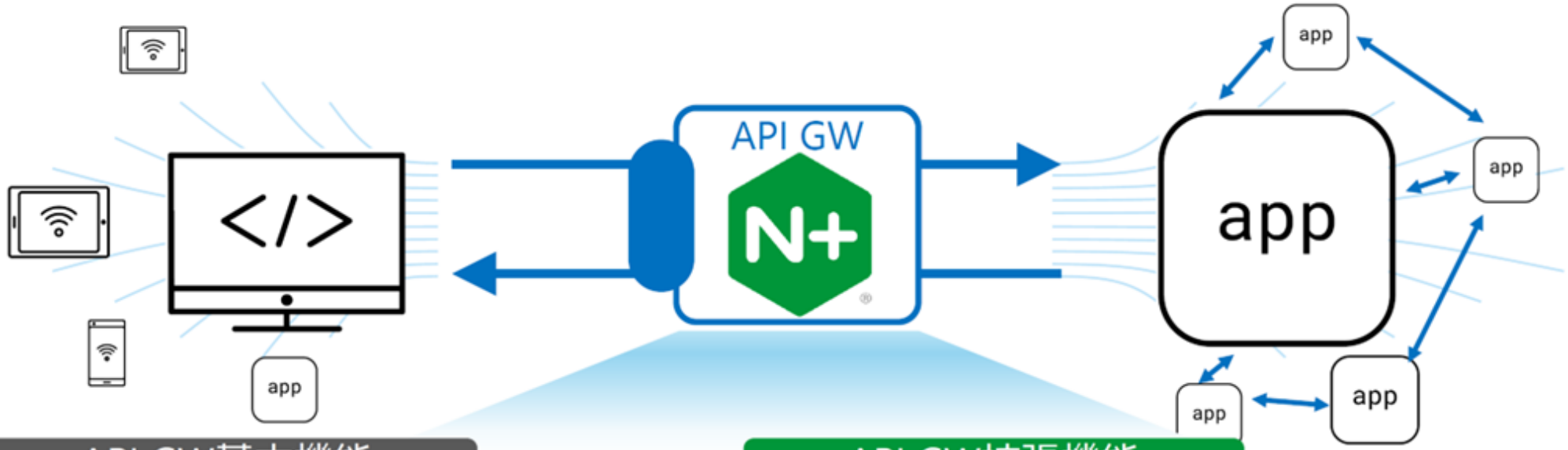
プライベートクラウド

パブリッククラウド

コンテナ

東京エレクトロン デバイス

NGINX Plus API Gateway



API GW基本機能

- APIルーティング
- Service Discovery
- Rate Limit
- TLS / mTLS

API GW拡張機能

- API認証・認可 (JWT/OAuth/OIDC/SAML)
- 細かなアクセス制御・HTTP操作
- WAF/L7DoS対策
- NJS / LUAによる機能拡張

NGINX Plus API Gateway

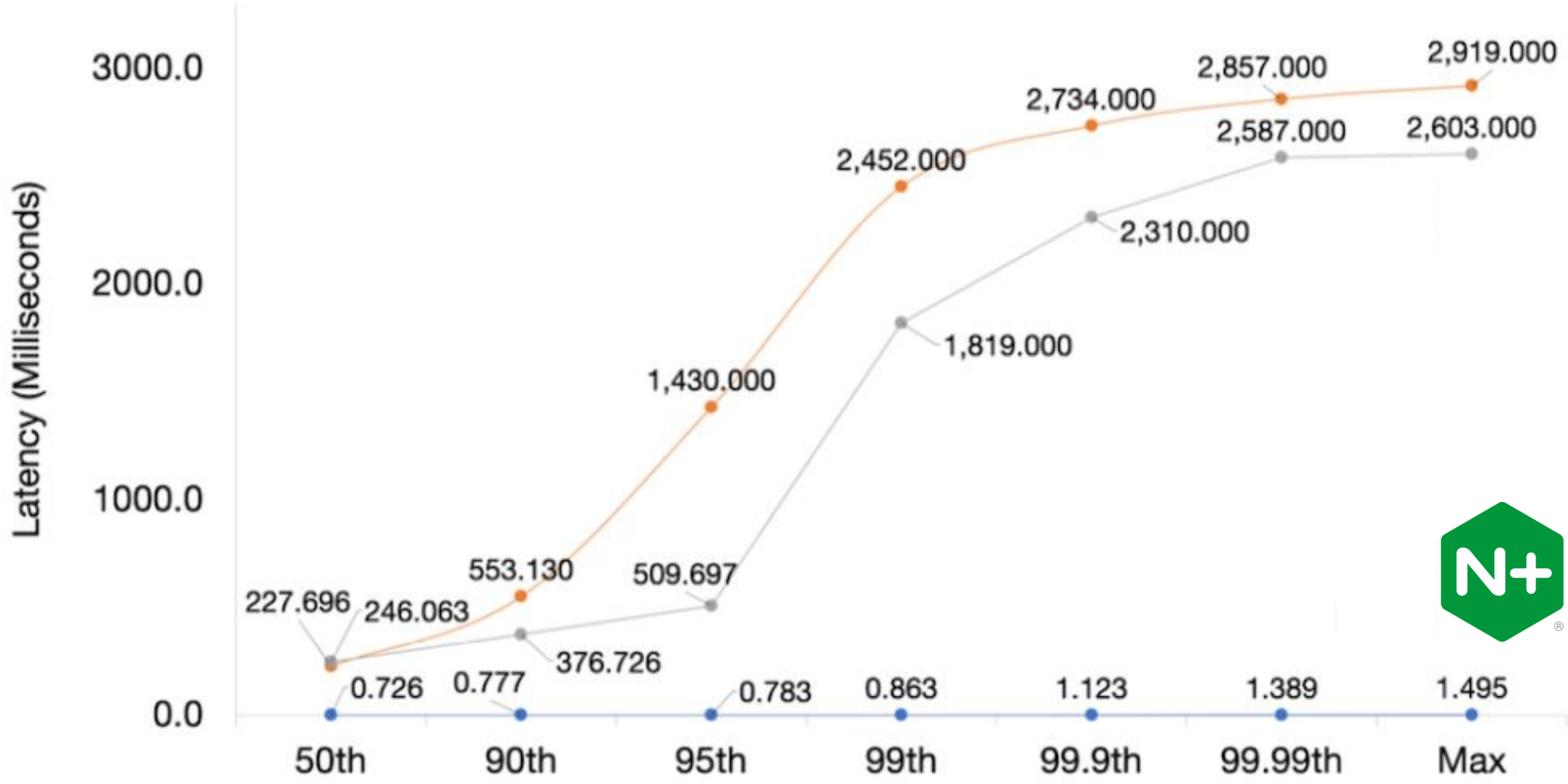
NGINX Plus は

高速軽量で

オンプレやクラウドを問わず動作が**可能！**

API Gateway としても**高性能**

NGINX Plus API Gateway



onnect Beyond デモ

API の課題

セキュリティ

- 認証/認可の欠陥
- データ漏洩
- 流量制限
- 攻撃者からの攻撃

etc ...

管理

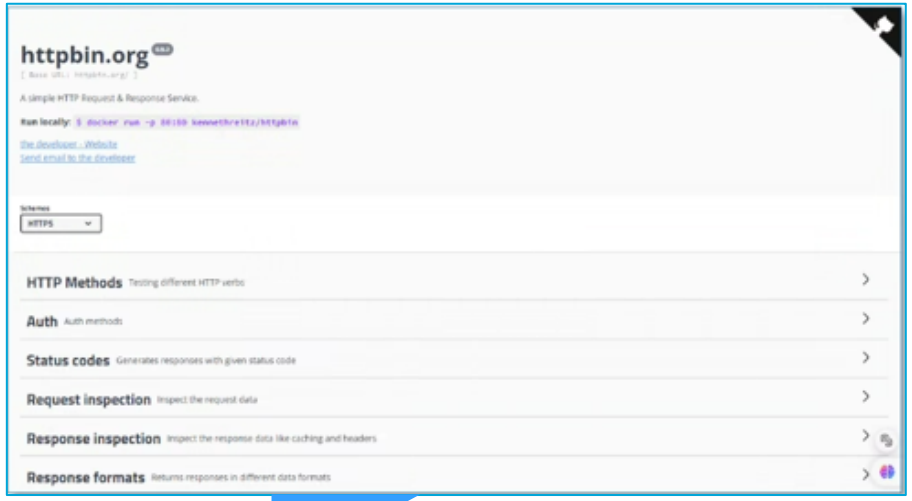
- シャドー API
- APIガバナンスの欠如
- APIドキュメンテーション
- 可視性の欠如

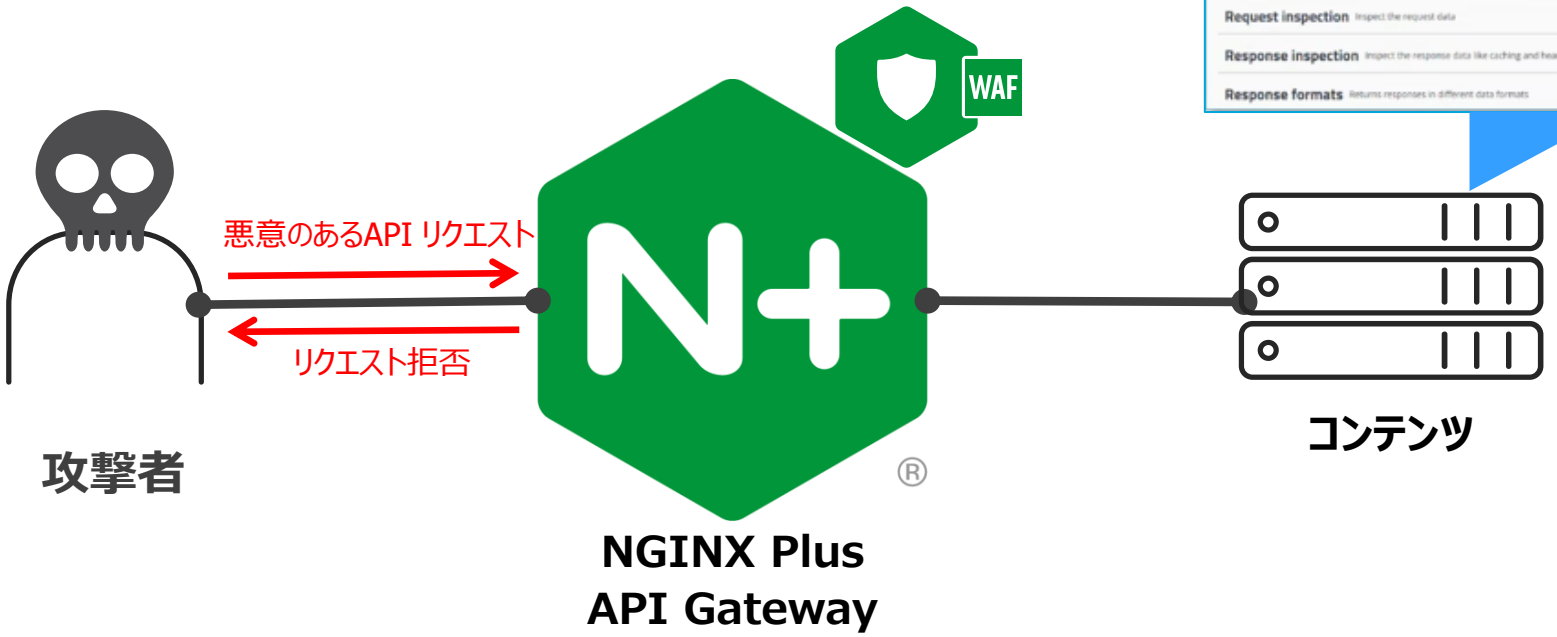
etc ...

デモシナリオ

httpbin.orgはHTTPやAPIの送受信テストをが可能なサイト

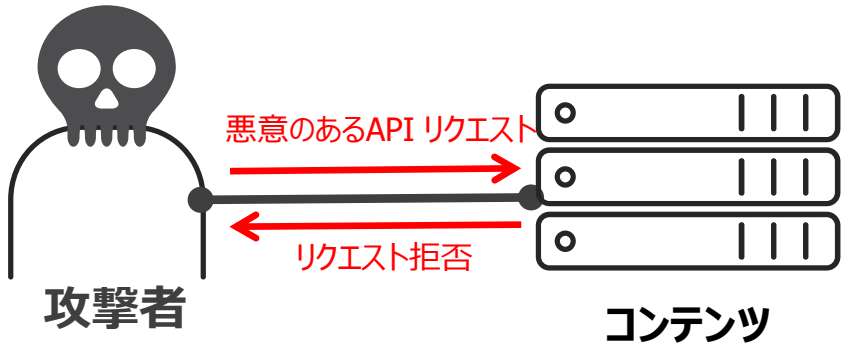
- 流量制限でコンテンツへの過度なアクセスの制限
  - 1分間に3回までのアクセスを許可
- WAFでコンテンツへの攻撃をブロック
  - XSS 攻撃を<script>という文字列で検知してブロック



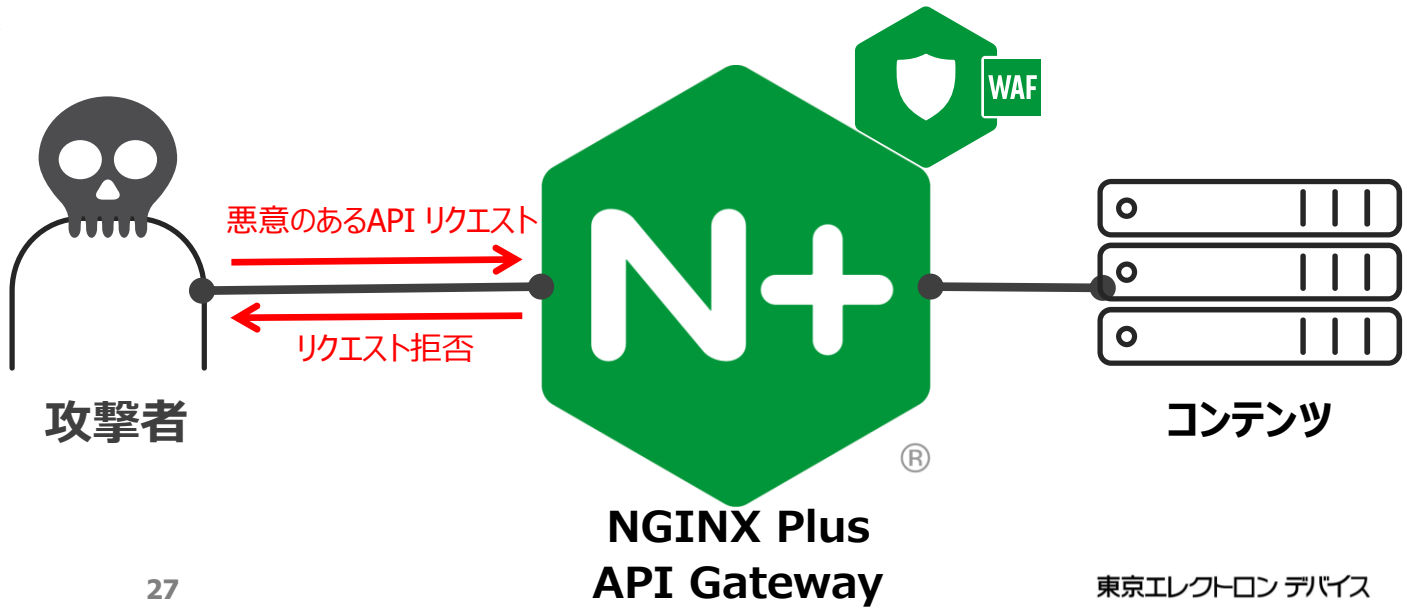


デモシナリオ

- **NGINX Plus API Gateway** を経由せずに **httpbin.org** へ **API リクエスト**を実施
  - 1分間に何回もアクセス
  - XSS 攻撃を実施



- **NGINX Plus API Gateway** を経由して **httpbin.org** へ **API リクエスト**を実施
  - 1分間あたりのアクセスを制御できているか
  - XSS 攻撃を検知してブロックできるか



デモシナリオ：NGINX Plus の設定

```
user  nginx;
worker_processes  auto;

# NGINX App Protect WAF
load_module modules/ngx_http_app_protect_module.so;

error_log  /var/log/nginx/error.log notice;
pid        /var/run/nginx.pid;

events {
    worker_connections  1024;
}

http {
    # レート制限のための共有メモリを定義
    limit_req_zone $binary_remote_addr zone=mylimit:10m rate=3r/m;
```

流量制限の設定

WAFを有効化する設定

```
# NGINX App Protect WAF
app_protect_enforcer_address 127.0.0.1:50000;
app_protect_enable on;

server {
    listen 80;

    location / {
        # レート制限の設定を適用
        limit_req zone=mylimit burst=5 nodelay;
        proxy_pass http://httpbin.org;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
    }
}
```

まとめ

- 昨今 急速に API が普及してきており便利な世の中になっている
- 便利な一方で API は攻撃者から狙われることがある
- API Gateway は API 通信のセキュリティ対策をしたり通信の制御をすることができる
- NGINX Plus API Gateway を利用することでセキュリティ対策などができる