F5 update

F5ネットワークジャパン合同会社

2025/10/7

F5営業組織図 FY25

カントリーマネージャー
木村 正範

サービスプロバイダ営業本部
本部長 恩田 本部長

エンタープライズ営業本部

公共・社会インフラ営業本部
部長 円谷 浩次

パートナー営業本部
部長 岡本 裕司

SE本部
本部長 Joe Tejome Poehls

サービスプロバイダ営業部
部長 野口 六根雄

メジャーアカウント営業部

- BFSI
- Manufacturing
- Transportation

- Central Government
- Local Government
- Education (Higher Ed)
- Utility

サービスプロバイダSE部
部長 堂脇 隆浩

エンタープライズSE部
部長　折原　直美

MSP営業部

- Web
- Ecommerce
- Gaming

テリトリー営業部
部長 本田 育子

- All Enterprise verticals

公共・社会インフラSE部
部長 石井 裕之

パートナーSE部
部長 石井 裕之

公共・社会インフラ営業本部 / SE部

営業部長
円谷 浩次

- **須藤 雅寛**
  中央省庁・外郭団体　担当
- **野本 浩幸**
  中央省庁・外郭団体　担当
- **今西 智之**
  西日本 自治体・大学　担当
- **屋代 哲**
  東日本 自治体・大学　担当
- **山村 拓朗**
  電力・ガス会社グループ　担当

SE部長
石井 裕之

- **田邊 淳一**
  中央省庁・外郭団体　担当
  東日本 自治体・大学　担当
- **小野寺 裕希**
  中央省庁・外郭団体　担当
  東日本 電力・ガス会社グループ担当
- **間所 雅人**
  西日本 自治体・大学　担当
  西日本 電力・ガス会社グループ担当

FY25 組織図 パートナー営業本部

木村 正憲
代表執行役員社長

- SP営業本部
- 公共・社会 インフラ営業本部
- パートナー営業本部
  - 
  - Partner Team 部長/岡本 裕治
    - TBH
    - 外岡 豪
    - 犬童　硬士
- エンタープライズ営業本部
  - ラージエンタープライズ 営業本部
  - テリトリービジネス 営業本部
- SE本部
  - 本部長/執行役員 テホメ ジョーペルス
    - 
    - ハイタッチ SE 兼 パートナー SE Team 部長/石井 裕之
      - 辻　哲也
      - 松中　栄貴
      - TBH
- マーケティング本部
- Global Service 本部
- Support & Engineering サービス本部

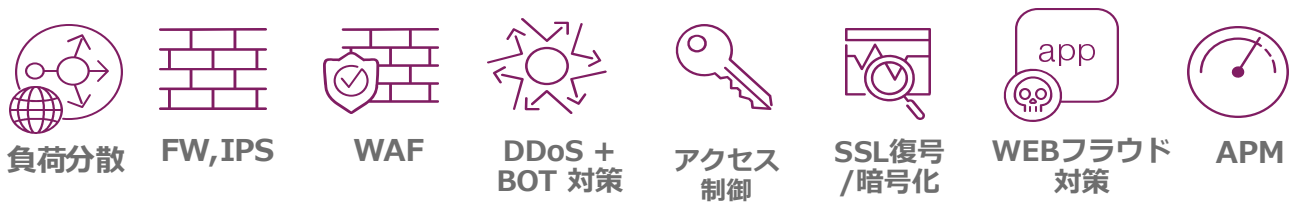
営業本部・SE本部

マーケティング本部、サポート本部他

F5 のトランスフォーメーション

全ての人々が快適安全にアプリケーションを使える世界を目指す

世界LB市場	導入実績	従業員数	年間売上高
No.1	25,000社以上	7,100名	約3,510億円
ロードバランサー市場 ※日本でもシェアNo.1[1]	175ヵ国以上の導入実績	#F5 Japan: 140名 43ヵ国に85のオフィスを展開	約27億USドル $1=130円



負荷分散 / FW,IPS / WAF / DDoS + BOT 対策 / アクセス制御 / SSL復号/暗号化 / WEBフラウド対策 / APM

アプリケーション基盤のための幅広い機能を提供

F5 BIG-IP

Distributed Cloud Services
（F5のテクノロジーを統合したSaaS）

SHAPE（不正アクセス対策）
NGINX（モダンアプリケーション）
Volterra（Edge Cloud / MCN）
LiLAC（CDN）
Heyhack（App Security）
wib.（API Security）

- 1996 BIG-IPリリース
- 1997 F5設立
- 1999 NASDAQ上場
- 2000 F5日本オフィス設立
- 2004 WAF大手 MagniFire WebSystem買収
- 2010
- 2015
- 2019 NGINX
- 2020 SHAPE
- 2021 Volterra
- 2022 Distributed Cloud Services
- 2023 LiLAC
- 2024 Heyhack / wib.

1 IDC Quarterly Ethernet Switch Tracker, ADC Segment, 2019Q4 Historical Release.
2 For a complete reconciliation of GAAP to non-GAAP measures, please see F5's most recent quarterly earnings press release.
3 ADN : Application Defined Network

製品・サービス

F5 BIG-IP

安全かつ快適な基盤を提供するハードウェアおよび仮想アプライアンス

- ADC
- Remote Access
- FW
- SSL可視化
- WAF
- DNS

F5 rSeries

F5 Distributed Cloud Services (XC)

F5のテクノロジーを統合し、包括的にF5の価値を提供するSaaS型クラウドサービス

- WAF
- DDoS対策
- API Security
- 悪性Bot対策
- DNS
- MCN / NaaS
- EDGE/ADN
- コンテナ基盤
- Penetration Test/DAST

F5 NGINX

Webアプリケーションのモダナイゼーションを下支えするクラウドネイティブソフトウェア

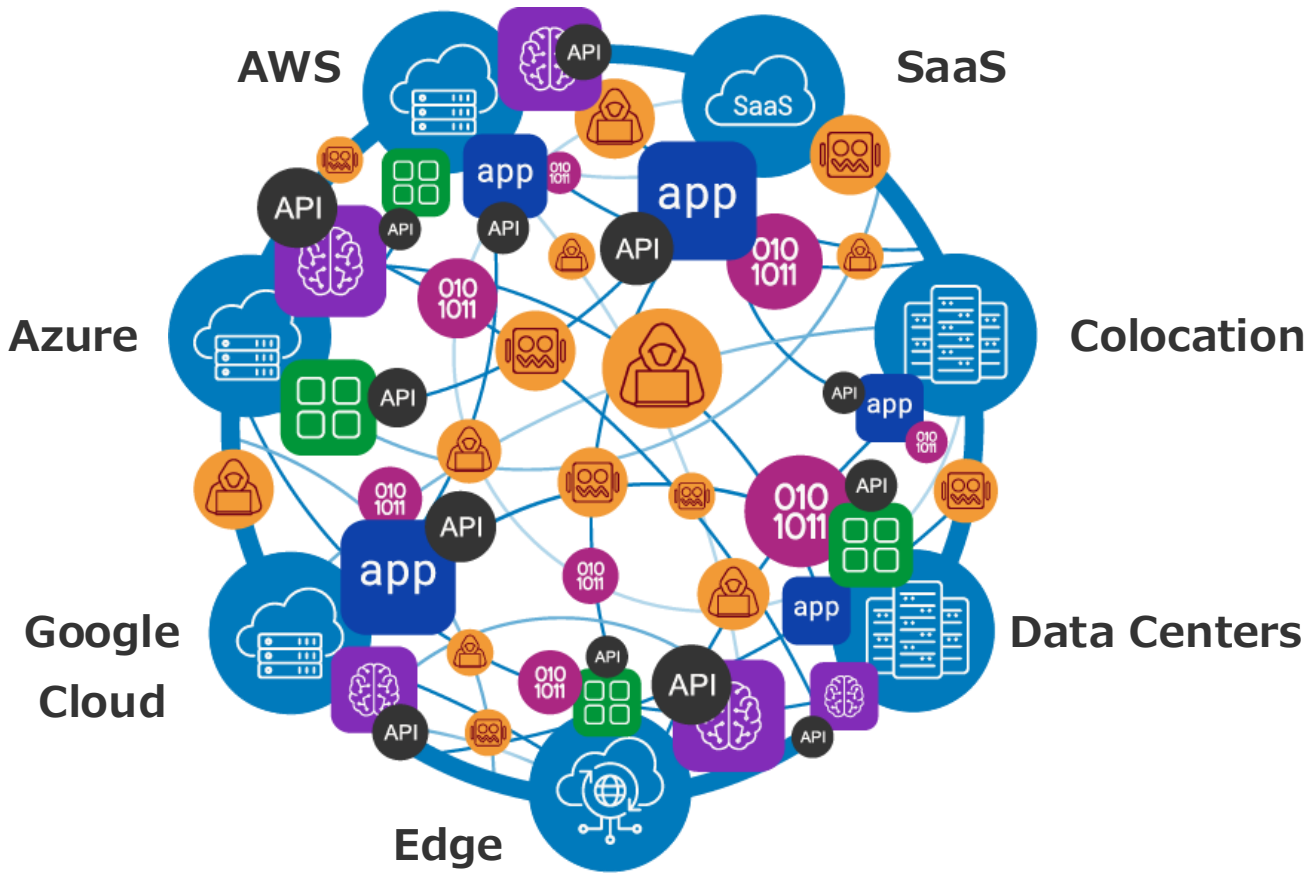
- Microservice
- Ingress Controller
- API GW
- ADC
- WAF
- DoS攻撃対策
- Web Server

ソリューション マトリックス

	アプリケーション セキュリティ	アプリケーション デリバリー	アプリケーション 基盤	AI
ハードウェア	**F5 BIG-IP** WAF / SSL可視化 FW / アクセス管理 Remote Access	**F5 BIG-IP** 負荷分散 / DNS Proxy / CGNAT	**F5 BIG-IP** Container Ingress Service	
ソフトウェア	**F5 BIG-IP** WAF / SSL可視化 FW / アクセス管理 Remote Access / DoS攻撃対策 WAF **F5 NGINX**	**F5 BIG-IP** 負荷分散 / DNS Proxy / Cashe Server 負荷分散 / Proxy **F5 NGINX**	**F5 NGINX** Microservice / Ingress Controller API GW Web Server	**F5 BIG-IP** GPUインフラ 負荷分散 **F5 NGINX** AI GW
SaaS	**F5 XC** WAF / DDoS対策 API Security / 悪性Bot対策 Penetration Test / DAST	**F5 XC** マルチサイト・マルチクラウド ネットワーク接続, NaaS DNS / CDN 外形監視	**F5 XC** コンテナ基盤 EDGE/ADN	**F5 XC** AI実行基盤 API Security / DDoS対策 AIデータ連携

F5 の領域を拡大

複雑なアプリ環境が AI の登場によりさらに複雑に



ポイントソリューションが多すぎる

複数の管理コンソール

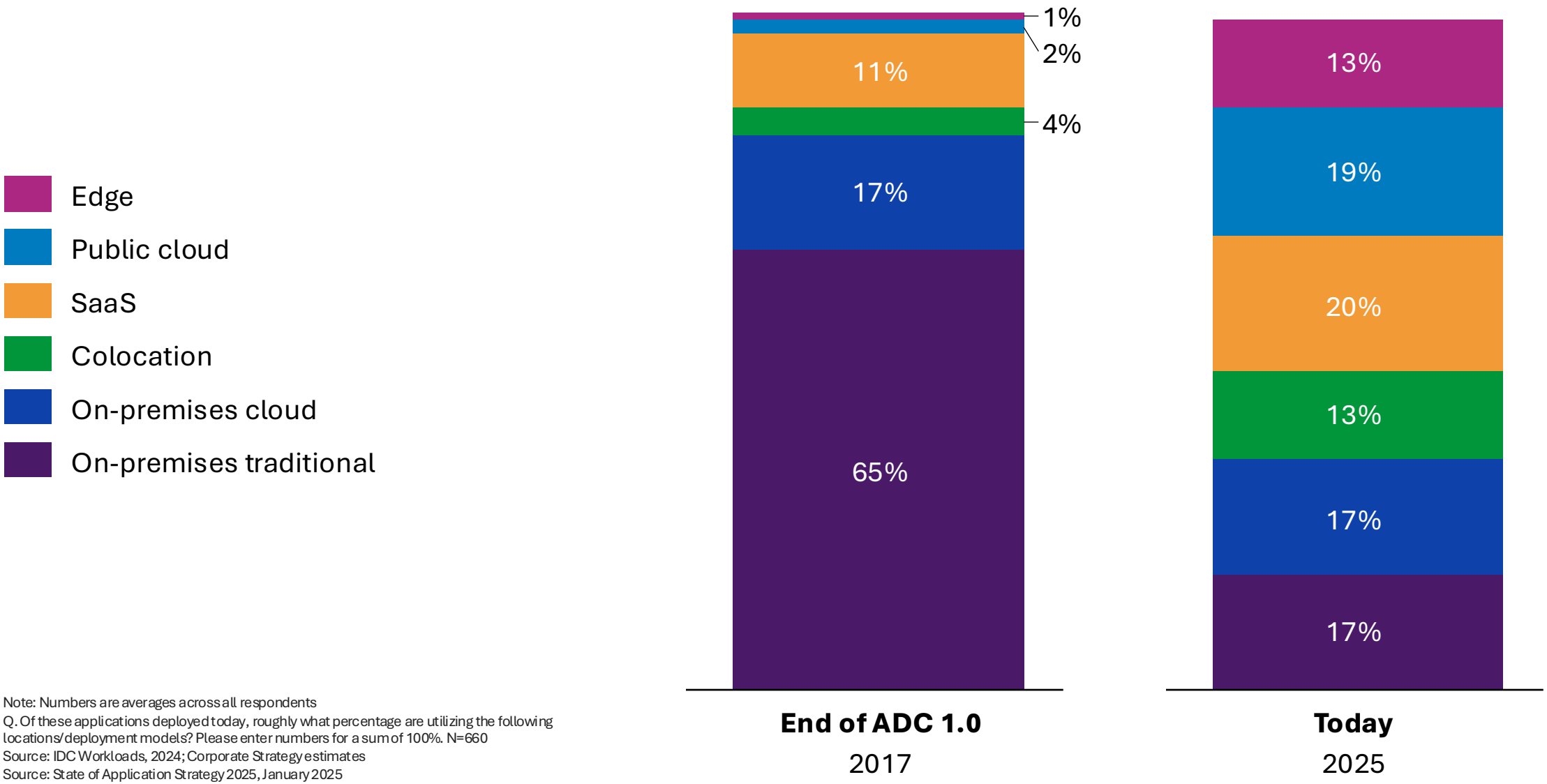
ポリシー矛盾の悪夢

マニュアルの複雑さ

非効率なアプリケーションルーティング

分散するアプリ環境

Apps deployed across locations & deployment models

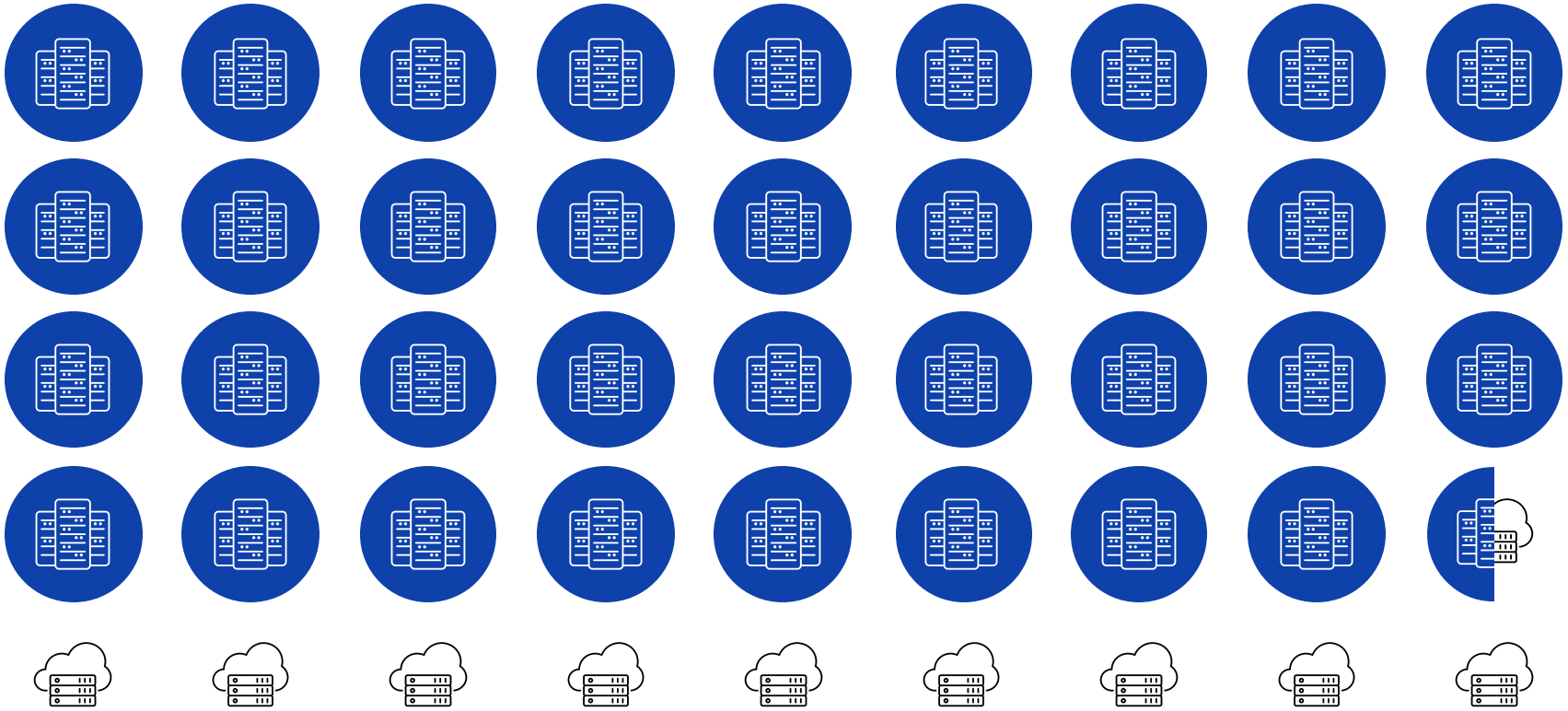


Note: Numbers are averages across all respondents
Q. Of these applications deployed today, roughly what percentage are utilizing the following locations/deployment models? Please enter numbers for a sum of 100%. N=660
Source: IDC Workloads, 2024; Corporate Strategy estimates
Source: State of Application Strategy 2025, January 2025

オンプレ回帰

過去12ヶ月間に、パブリッククラウドからオンプレミス、またはコロケーションデータセンターにアプリケーションを戻しましたか？あるいは今後１年間で戻す予定はありますか？

13%
2021

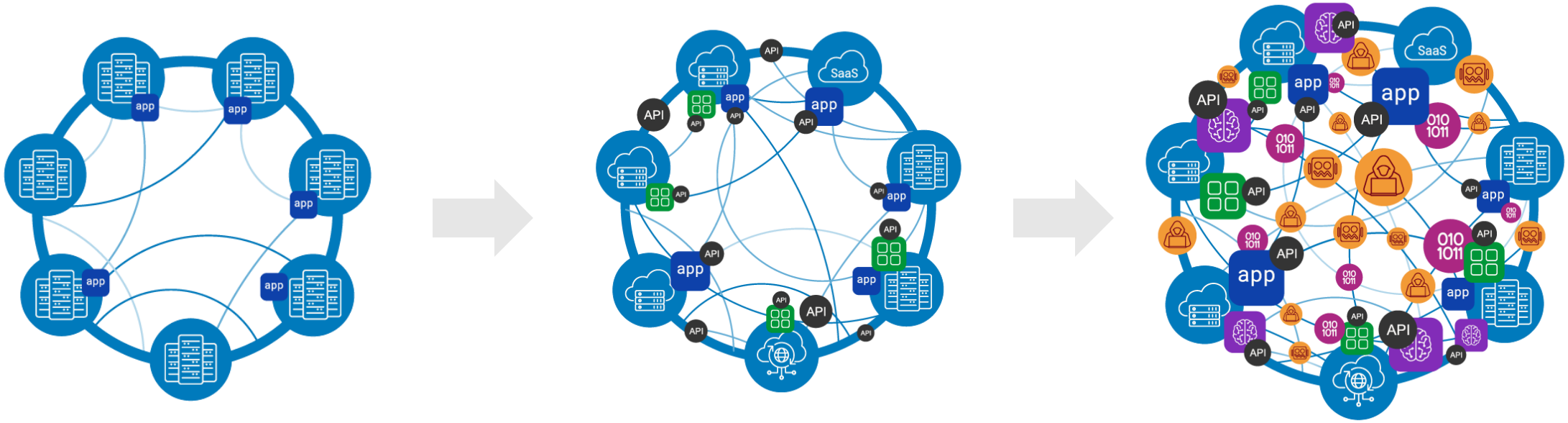


79%
2025

Q. Have you repatriated applications from the public cloud back to your on-premises or colocation data center in the past 12 months, or are you planning to do so in the coming year? N=660
Source: State of Application Strategy 2025, January 2025

ADC 時代からの進化

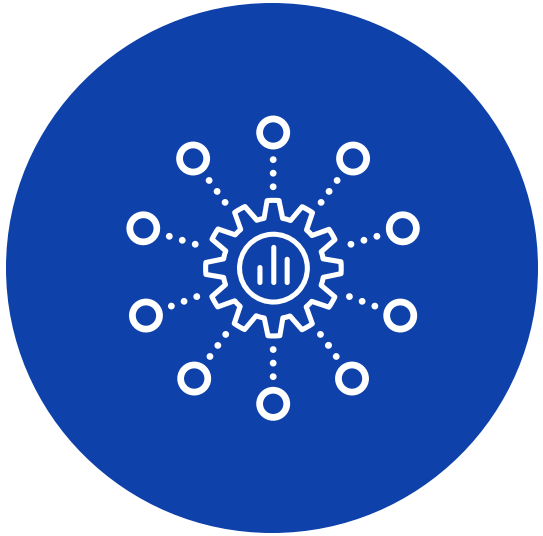
オンプレ環境で始まったADCは、クラウドとコンテナ化によって非現実的なアプローチに



複雑さにより増大する
コスト、運用の断片化、サイバーセキュリティリスク

コスト増

クラウド支出と
複数の運用サイロが原因



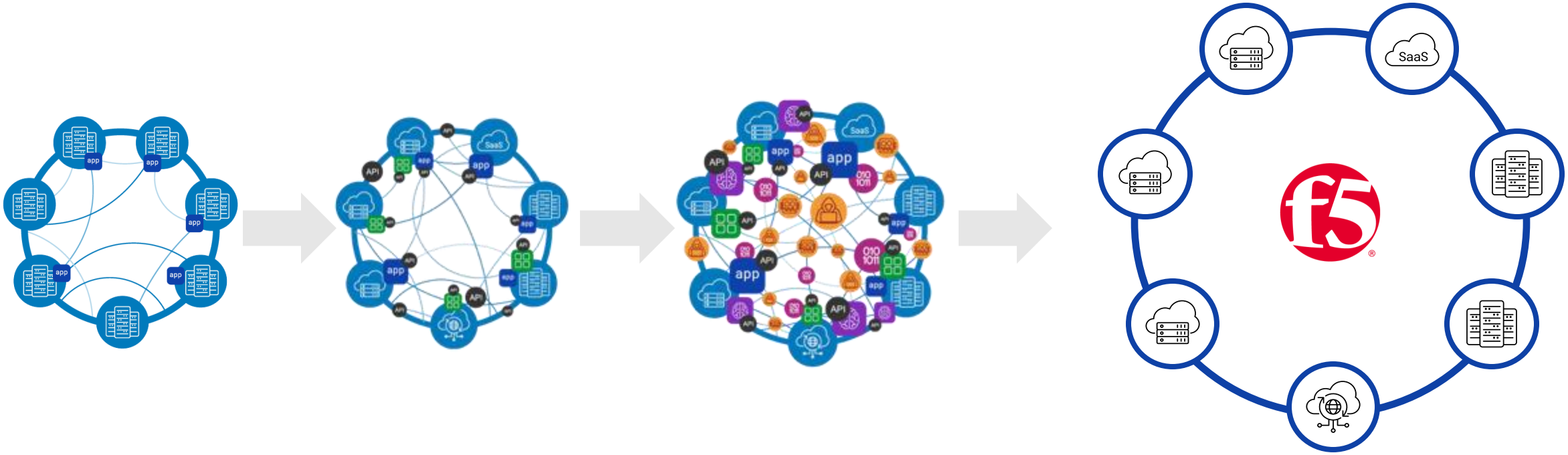
運用の複雑化

ポイントソリューションの拡大による、
チーム、ポリシー、コンソール間での
断片化された制御

管理不能なサイバーリスク

アプリとAPIの分散と
リソース不足による脅威の拡大

再びシンプルな世界へ



Application Delivery & Security 統合プラットフォームである F5 ADSP

1
完全なアプリケーション配信とセキュリティ

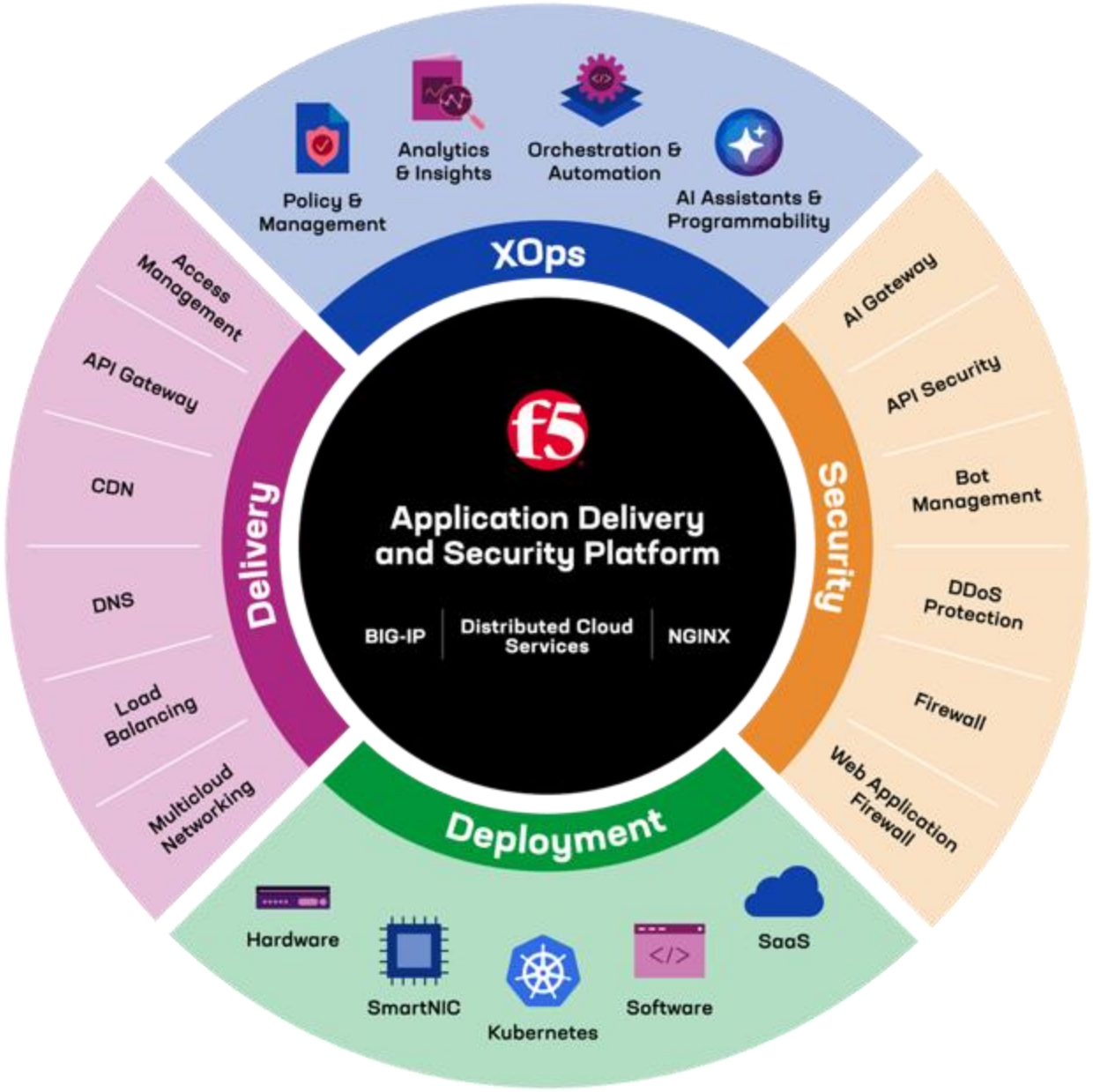
2
あらゆる場所にあらゆる形態で展開可能

3
統一ポリシーによるシンプルな運用管理

4
高度な分析とインサイト

5
プログラム制御可能なデータプレーン

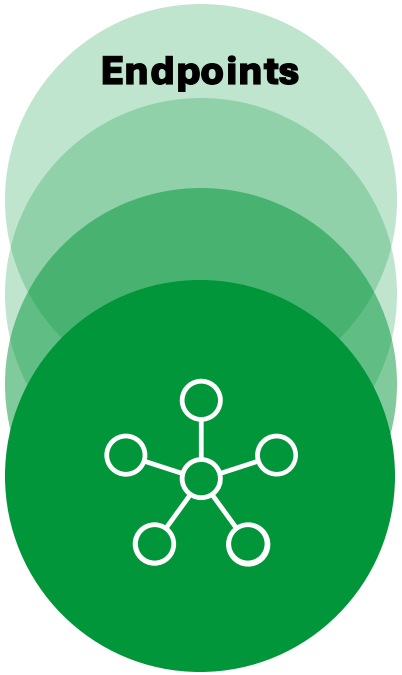
6
ライフサイクル全体の自動化



過去、膨大な数のポイントソリューションが提供されていた

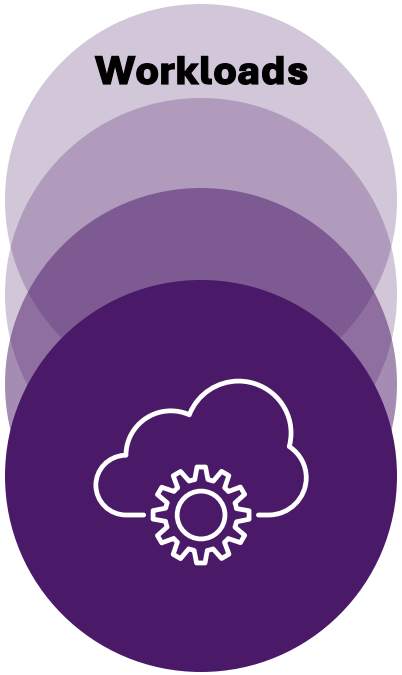
Endpoints	Networks	Workloads
Anti-virus	Secure web gateway	Cloud workload protection
Anti-spyware	Cloud access security broker	Cloud posture management
Behavioral analysis	Firewall-as-a-service	Cloud infra entitlement
Host firewall	Zero trust network access	Infra scanning
Device control	Browser isolation	Cloud svc network security
Host data loss protection	Data protection	Encryption
File encryption	Software-defined WAN	Data protection
File integrity	WAN optimization	Identity & access management
Threat intelligence	Network-as-a-service	Threat detection
…	…	…

プラットフォームへの統合



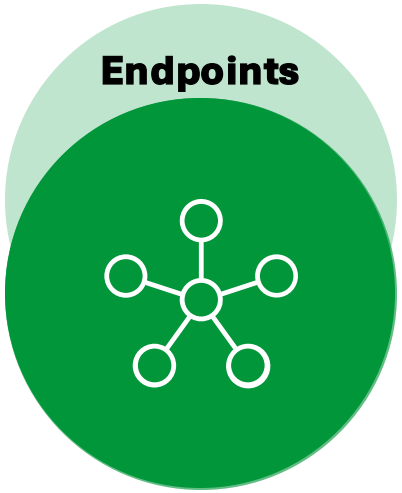
Endpoint Protection Platform
(EPP)

Secure Access Service Edge
(SASE)



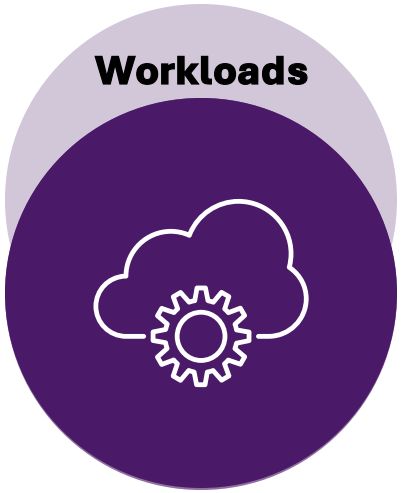
Cloud Native Application Protection Platform
(CNAPP)

世界を代表するセキュリティ企業 = プラットフォーマー



Endpoint Protection Platform
(EPP)

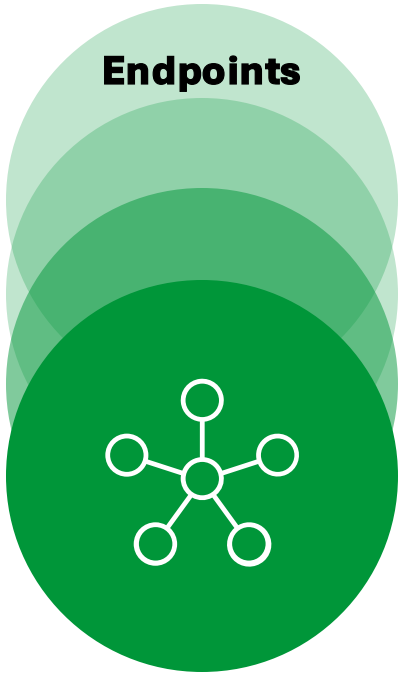
Secure Access Service Edge
(SASE)



Cloud Native Application Protection Platform
(CNAPP)

Microsoft CROWDSTRIKE zscaler™ paloalto NETWORKS WIZ

進化するF5ポートフォリオのその先に・・



Endpoint Protection Platform
(EPP)

Secure Access Service Edge
(SASE)

Load balancing

Web app & API protection

Access security

Domain name service

API gateway

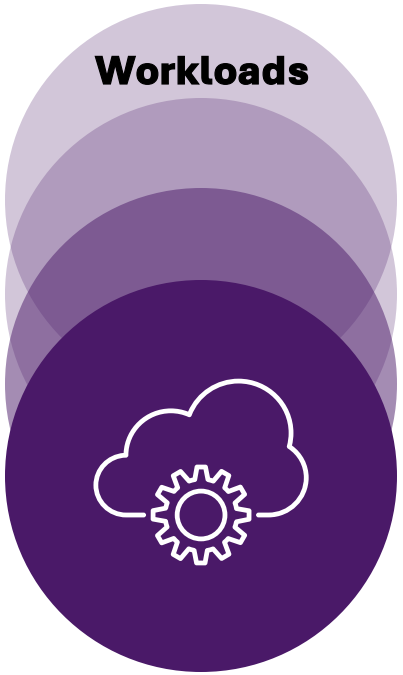
Network firewall

Zero trust network access

AI gateway

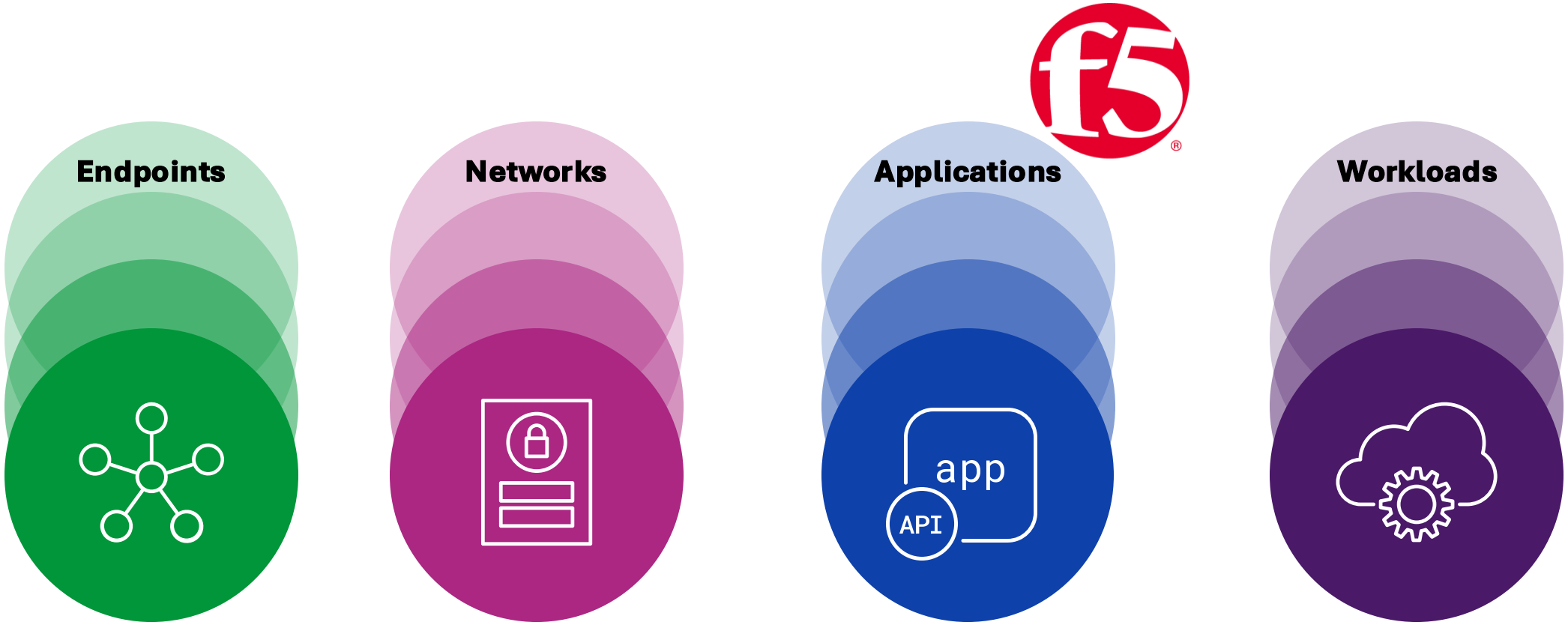
Multicloud networking

...



Cloud Native Application Protection Platform
(CNAPP)

F5が創る新しいプラットフォーム ADSP



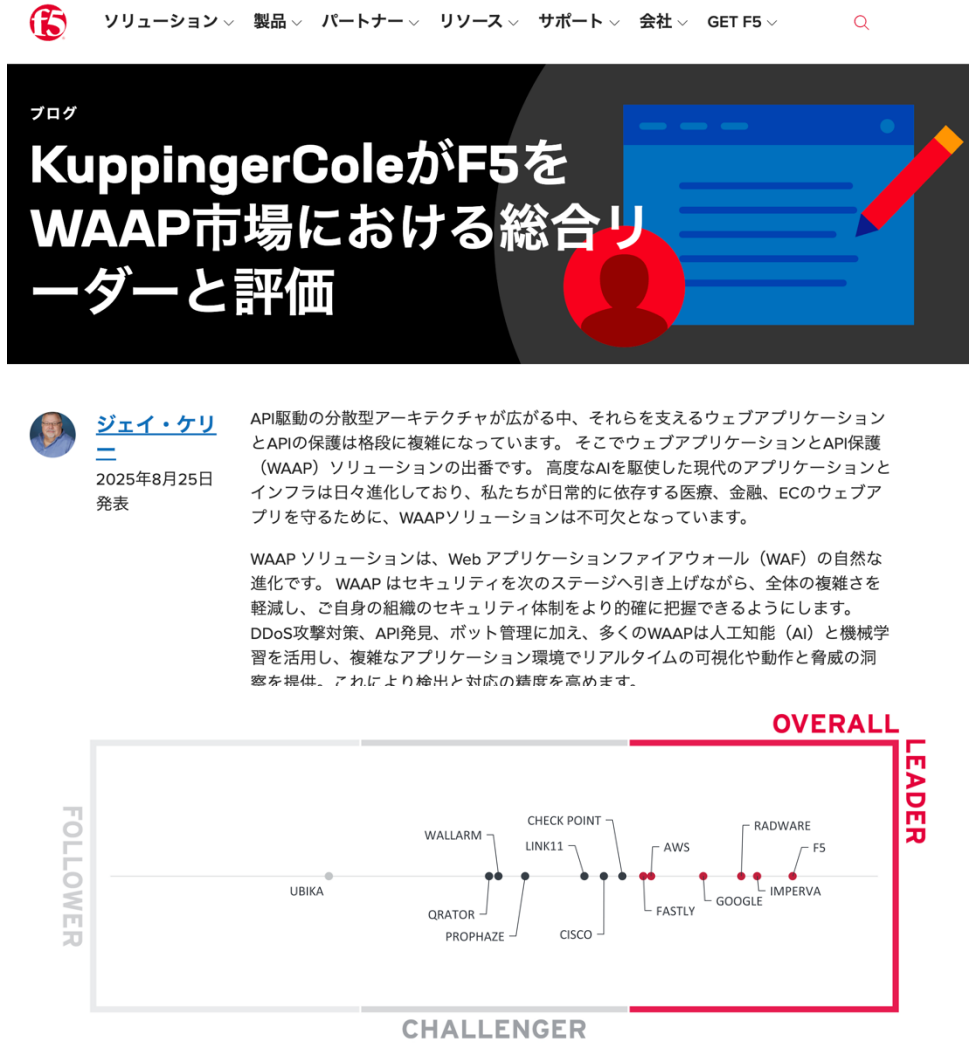
Endpoint Protection Platform
(EPP)

Secure Access Service Edge
(SASE)

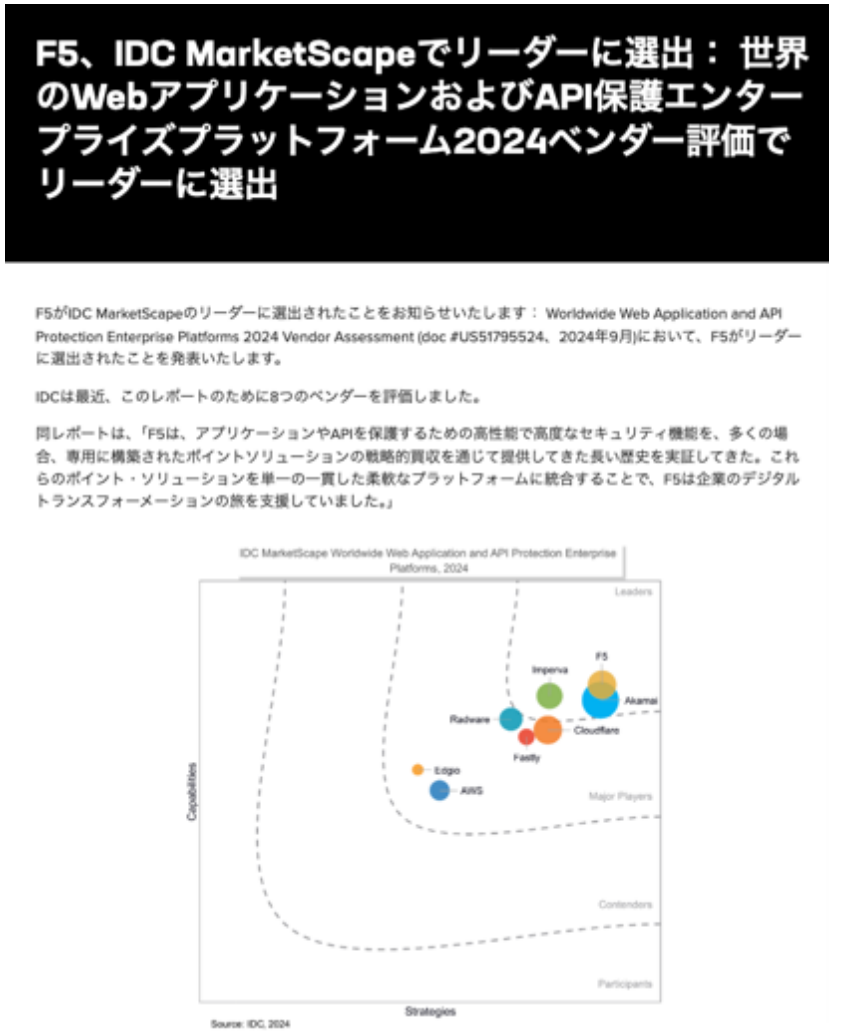
App Delivery & Security Platform
(ADSP)

Cloud Native Application Protection Platform
(CNAPP)

外部からの高い評価



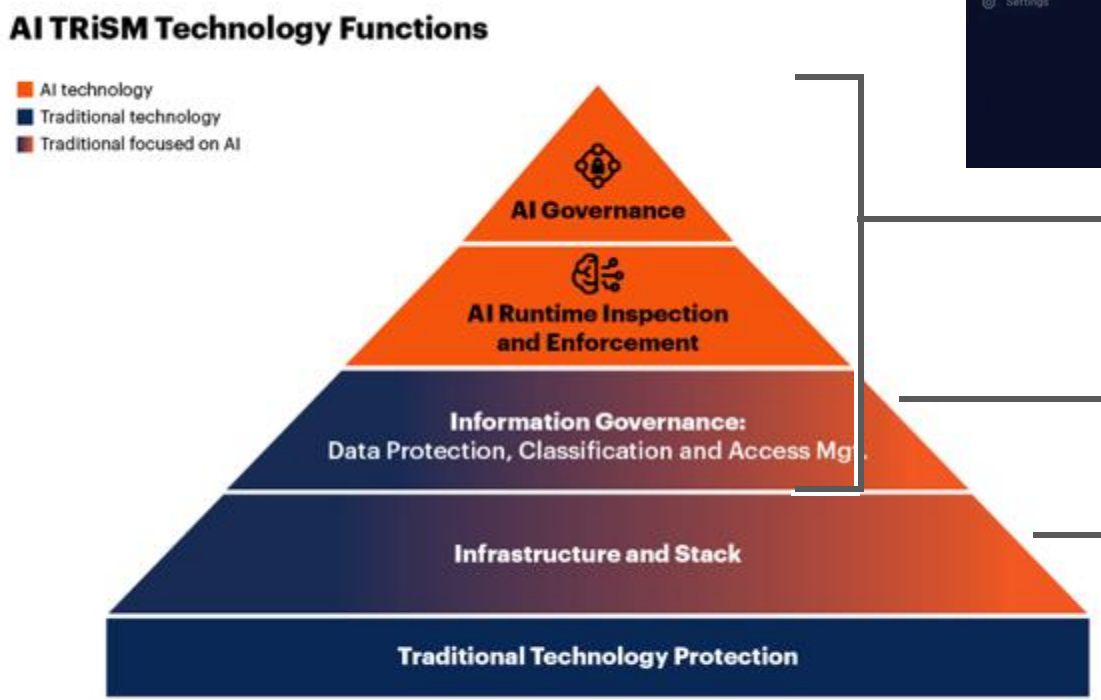
https://www.f5.com/ja_jp/company/blog/kuppingercole-recognizes-f5-as-overall-market-leader-in-waap



https://www.f5.com/ja_jp/go/report/f5-named-a-leader-in-the-idc-marketscape-worldwide-web-application-and-api-protection-enterprise-platforms-2024-vendor-assessment

2025/9 AI Security solutionを買収

適応型AI推論セキュリティソリューション



CalypsoAI

SSLO + LeakSignal (Shadow AI)
BIG-IP APM (Access Management)

WAAP (API Security)
MCN (Secure Data for RAG)
BNK (BIG-IP Cloud Native Edition for Nvidia DPU)

BIG-IP (AWAF, DDoS, etc.)
WAAP (WAF, Bot, DDoS)

F5大学様向けソリューションの概要

大学様向けF5ソリューションの概要

提案製品： F5 BIG-IP、 F5 XC、 NGINX

① キャンパスネットワーク DX（クラウド向けトラフィック制御、認証、リモートアクセスなど）

F5 BIG-IP LTM, APM, SSLO

② DDoS攻撃対策と脆弱性を突いた攻撃への対策

F5 XC WAAP, BIG-IP, NGINX

③ DNS 運用負荷削減・セキュリティ対策

F5 XC DNS

①キャンパスネットワーク DX

クラウド向けトラフィック制御、認証、リモートアクセスなど

キャンパスネットワークにおけるBIG-IPのユースケース

プラットフォームであるBIG-IPに追加モジュールを組み合わせ、拡張性の高い利用が可能です。

1. クラウド利用を安定化させるためのクラウドプロキシ、トラフィック制御

F5 Local Traffic Manager（LTM）, SSL Orchestrator(SSLO)

2. リモートアクセス、ポリシーによるアクセス制御、多要素認証、SSO対応

F5 Access Policy Manager（APM）

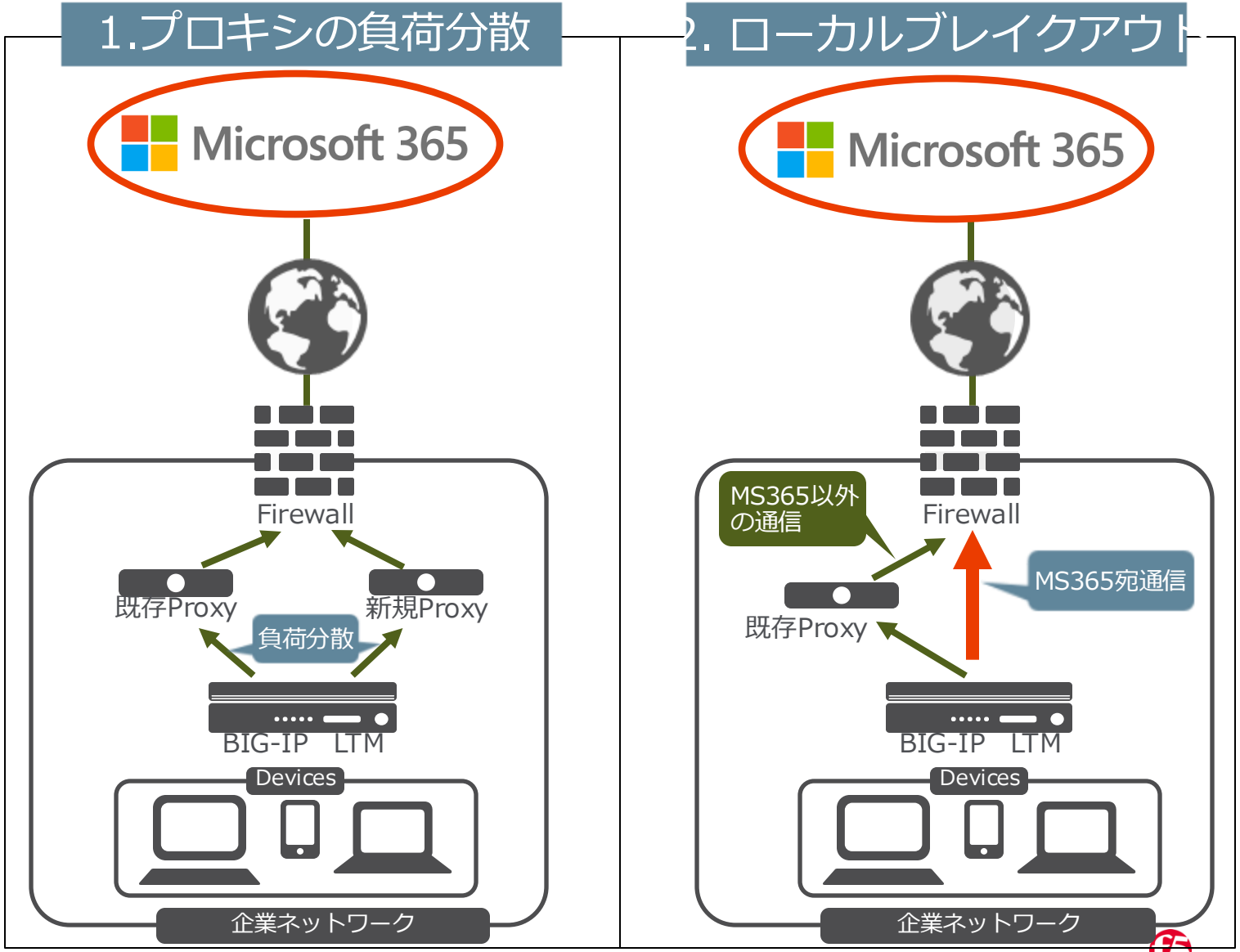
ユースケース1. プロキシ向け負荷分散 & ローカルブレイクアウト

F5のソリューション
プロキシ負荷分散、ローカルブレイクアウト

MS365を利用する場合、各端末が大量のセッションを利用します。膨大な通信トラフィックやコネクションに対応するため、プロキシの増強が必要になります。

BIG-IP LTMを利用することで、**プロキシの新旧の負荷分散が可能です。**

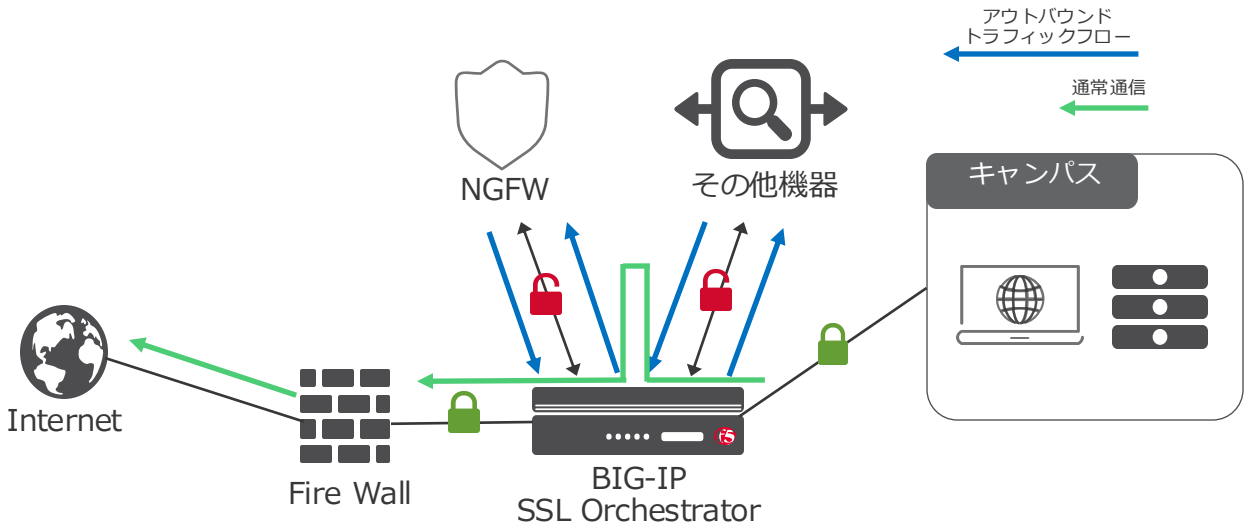
また、MS365を利用する通信のみBIG-IPをプロキシとして動作させ、既存のプロキシをバイパスさせることで、投資を抑えることも可能です。



BIG-IPにてアウトバウンド通信を可視化

Palo Altoの可視化を行うことでセキュリティデバイス導入メリットを最大限に活用

Industry	CSP	BFSI	ENT	PUB
Function	BIG-IP	XC	NGINX	



■導入製品

- F5-BIG-LTM x 2, F5-ADD-BIG-SSLO-3 x 2

■課題と要件

- ハイエンドのNGFW製品を導入したが、暗号化通信が急増
  → 暗号通信にもセキュリティを確保したい
- セキュリティデバイスでSSL処理を行うとパフォーマンスが低下
  → 暗号復号を一元的に実施できる機能がほしい
- SSL処理を専用に行う製品でもパフォーマンスが低下
  → 実際に暗号復号を動かしても想定通りのパフォーマンスで動作して欲しい

■F5導入のメリット

- サイトアクセス時のセキュリティ強化とパフォーマンス向上の両面でトラフィックを最適化できた
- Transparent構成にて導入することで、セキュリティ強化をしつつ、既存の設定の変更を少なくすることができた
- 他社製品としてパフォーマンスが優れていた

F5導入決定のポイント

1 Transparent構成

既存設定の変更を極小化

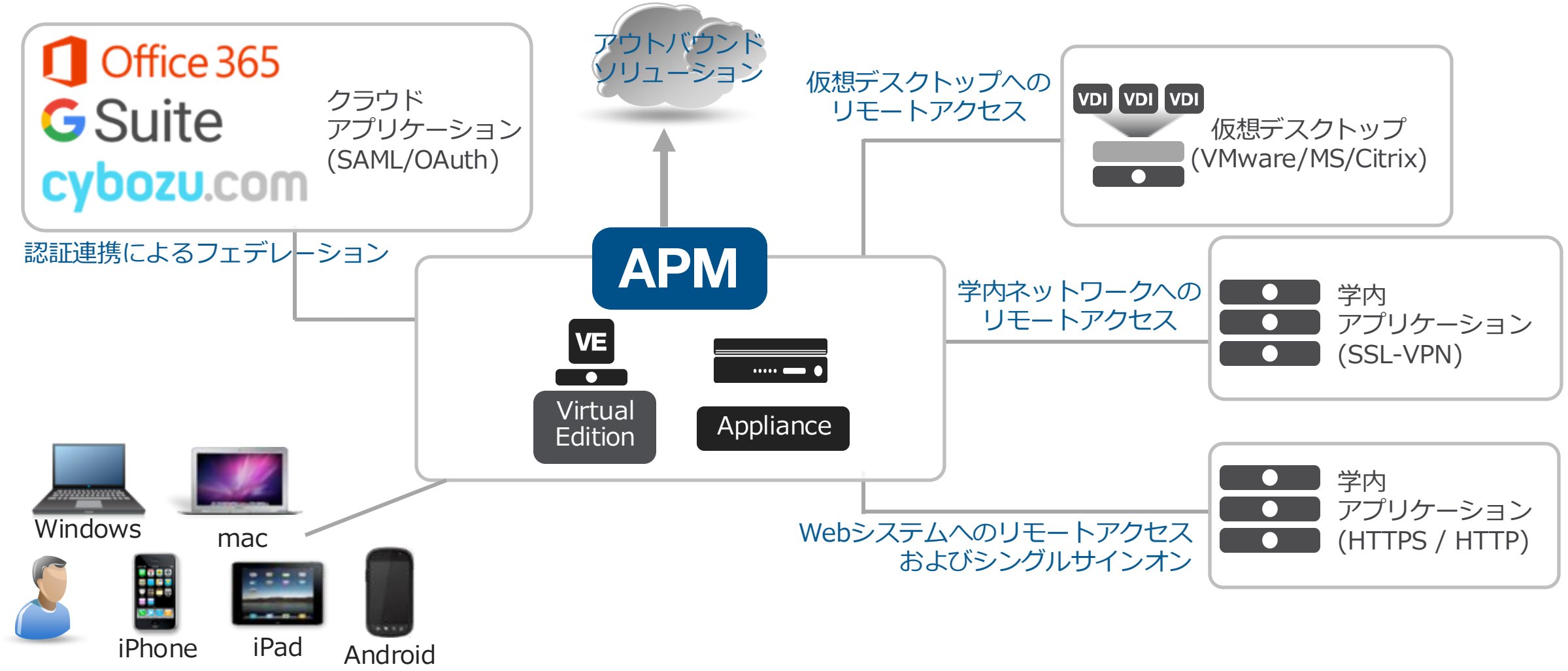
2 サービスチェーン構成

物理ポートの制約を受けない構成が実現可能

3 高パフォーマンス

他社製品に比べ圧倒的なスループット性能を実現

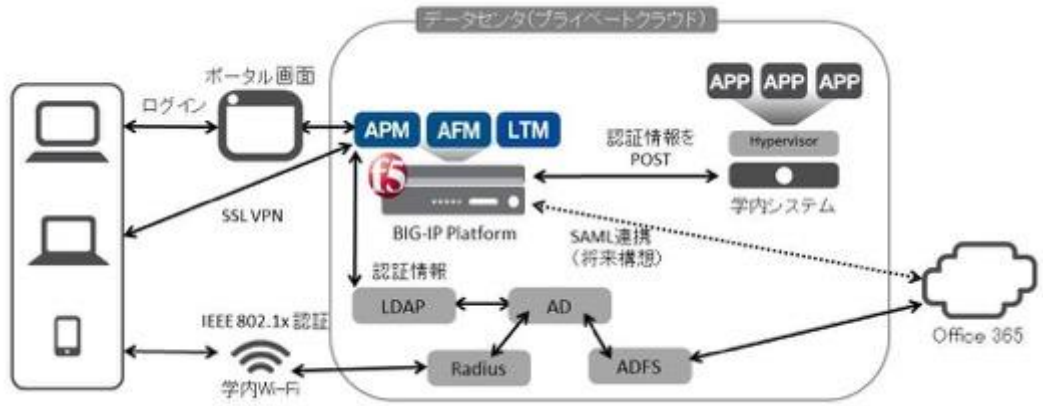
ユースケース2. 学外からのリモートアクセス、認証およびSSO



アプリケーションへの認証、認可、シングルサインオンを提供し、
あらゆるアプリケーションへの接続を安全、快適にします

同志社女子大学様
～機能集約によりコストを抑え、シンプルなキャンパスネットワークを実現～

同志社の創設者・新島襄、妻・八重、アメリカ人宣教師A.J.スタークウェザーらによって1876年に設立された女子総合大学。「キリスト教主義」「国際主義」「リベラル・アーツ」の伝統と柔軟な変革の歴史を持ち、現在は京田辺、今出川の両キャンパスの6学部11学科1専攻科4研究科で、約6,500名の学生が学んでいる。



「BIG-IPなら機器集約が可能な上、多様なシステムをカバーしたSSOも実現でき、WAF等のセキュリティ機能も実装可能。これらを徹底的に使い倒すことが、このプロジェクトの要だと考えています」

同志社女子大学　経理部 ネットワークインフラ課　課長
長南 敏彦 氏

- ネットワーク機器をプライベートクラウドに移行するために、利用できるラックスペースが限られていた。
- メールシステムをOffice 365へと移行する上で、認証連携が求められた。
- 学内認証やSSL VPNのシステムリプレースも迫っており、認証基盤システムの見直しも必要だった。

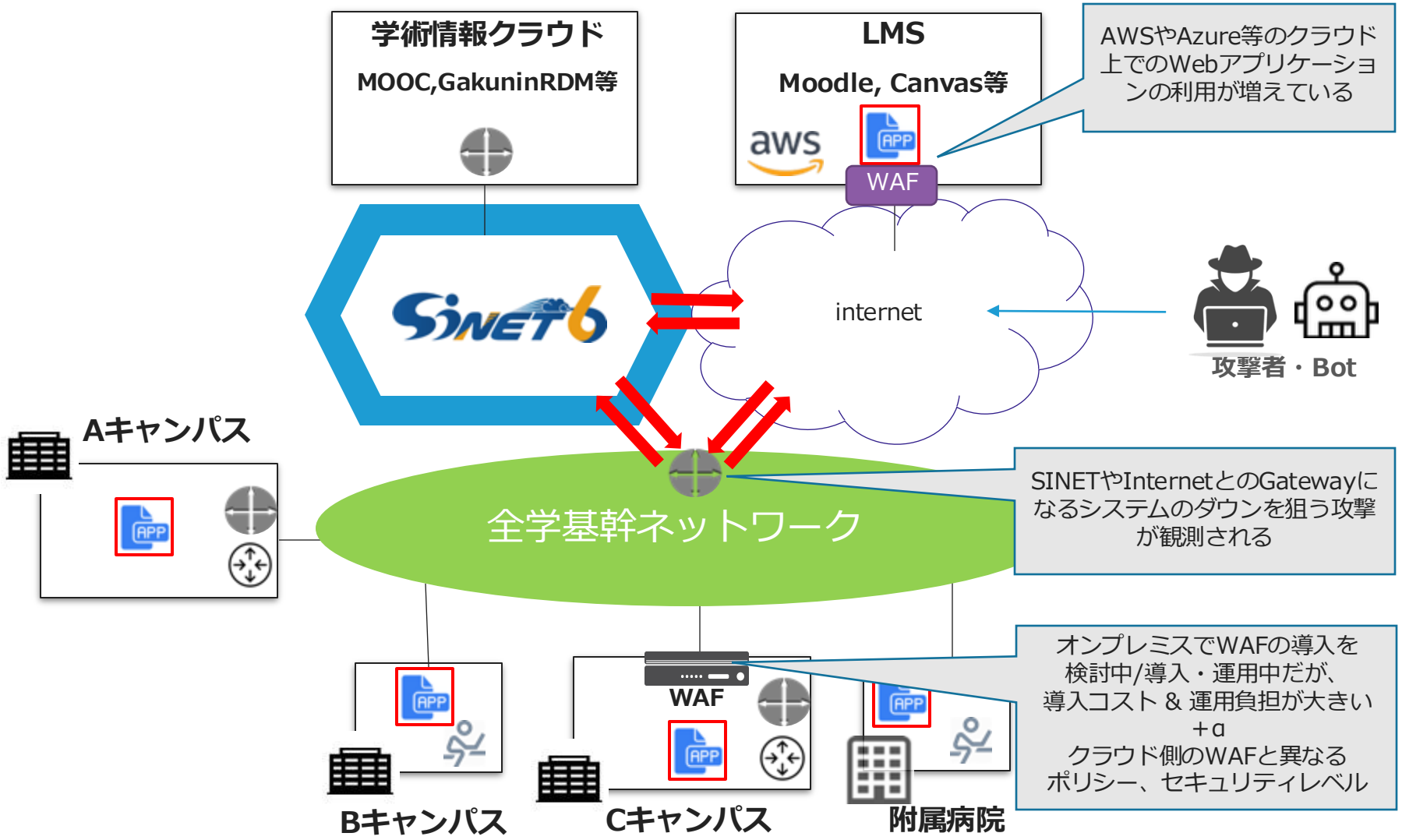
APM Access Policy Manager　**AFM** Advanced Firewall Manager

LTM Local Traffic Manager

- ✓ 複数のネットワーク機器をBIG-IPに集約することで、設置スペースを削減できた。
- ✓ 幅広いシステムをカバーしたSSO基盤が整備できた。
- ✓ セキュリティを強化する各種機能も利用可能になった。

② DDoS攻撃対策と脆弱性を突いた攻撃への対策

近年増加傾向にある大学へのサイバー攻撃の種類と課題



学術関係者・大学に対する高度なサイバー攻撃は増えている一方、導入・運用コストがネック

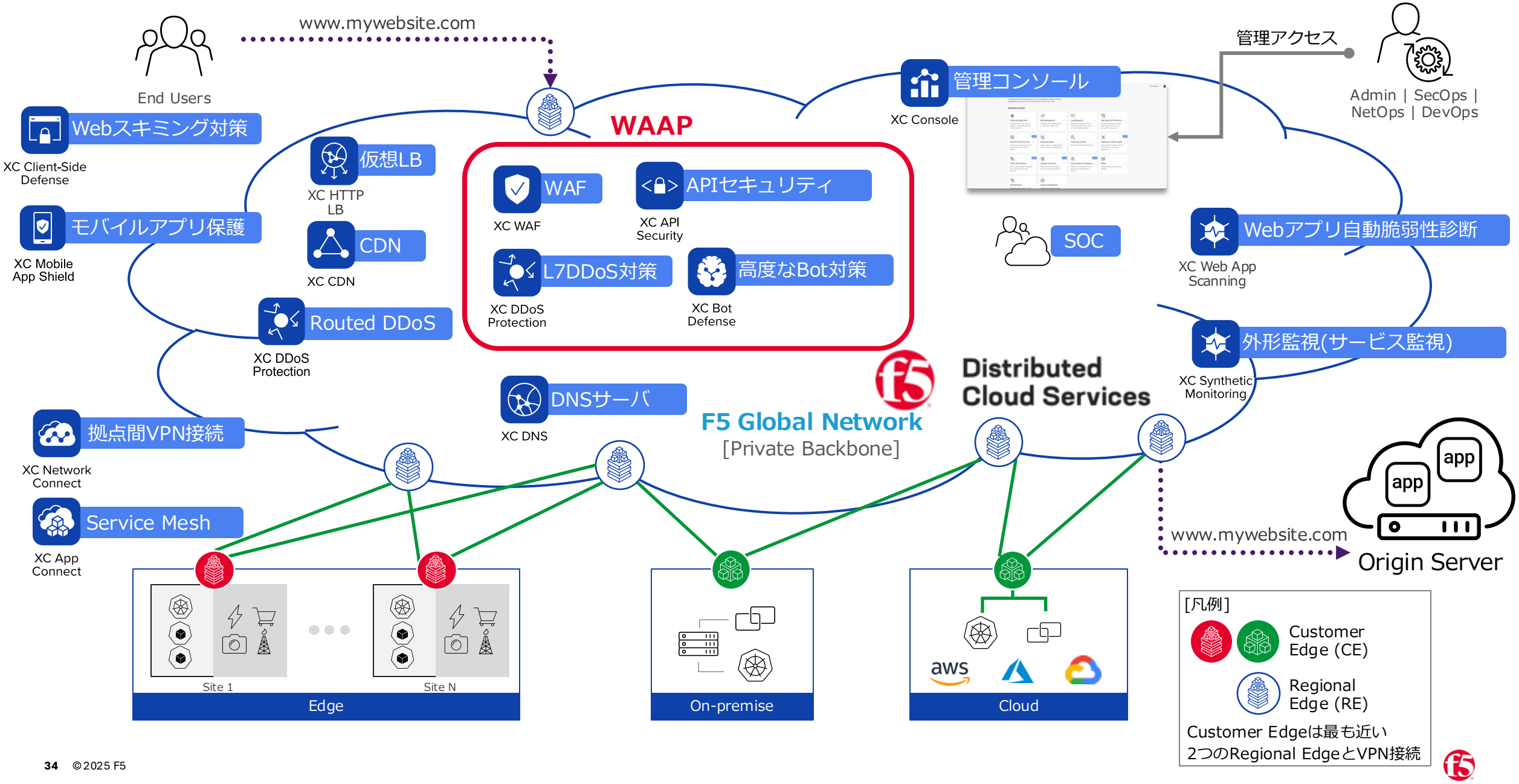
F5クラウド型セキュリティサービスのメリット

OWASP Top10 の対応
高度な脆弱性への攻撃をクラウドで検知

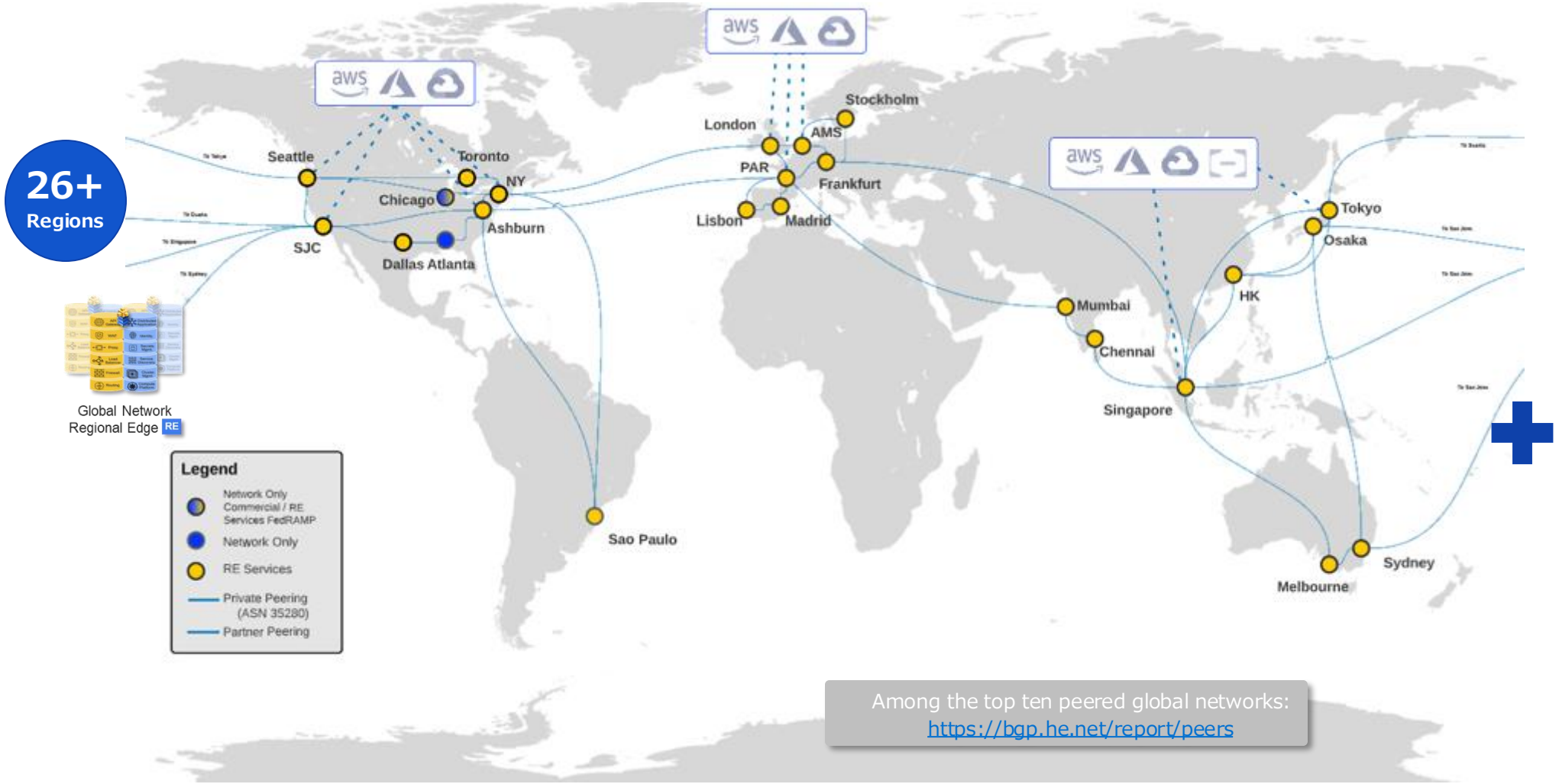
大規模なDDoS攻撃を分散防御
さらにSOCによる解析

クラウド/オンプレを一元管理し
セキュリティレベルを統一

F5 XC の全体像



F5 XC のPrivate Global Network



Customer Edge

お客様のオンプレや
利用クラウドVPC内に
配置し、XCサービスを
稼働させることが可能

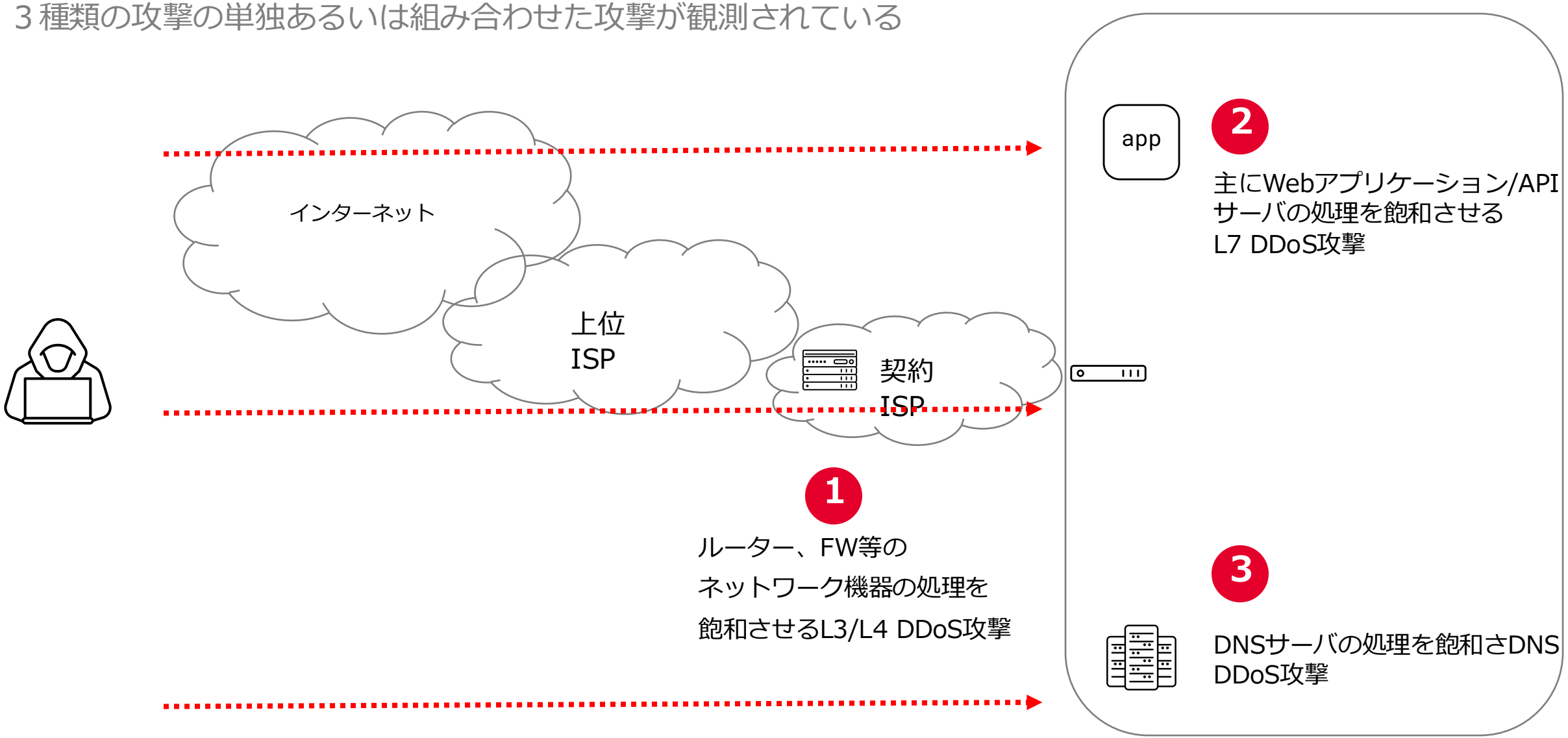
17+ Tbps capacity
(Tier-1 Carriers: NTT, Telia, Level3)

Multi-Tbps private backbone
(Zayo, Telia, CenturyLink)

Dedicated connectivity
(Cloud providers, SaaS providers)

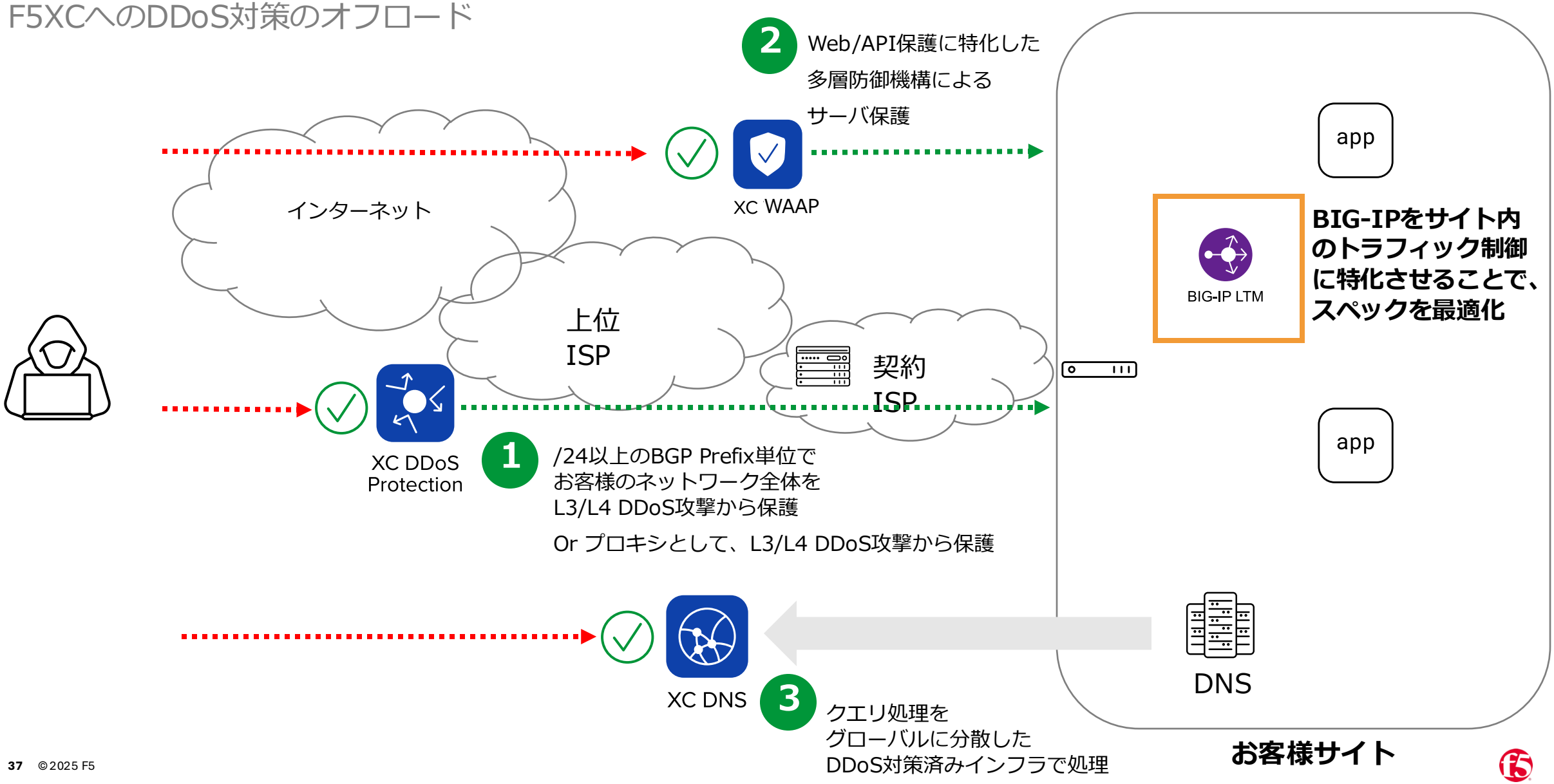
DDoS攻撃の種類

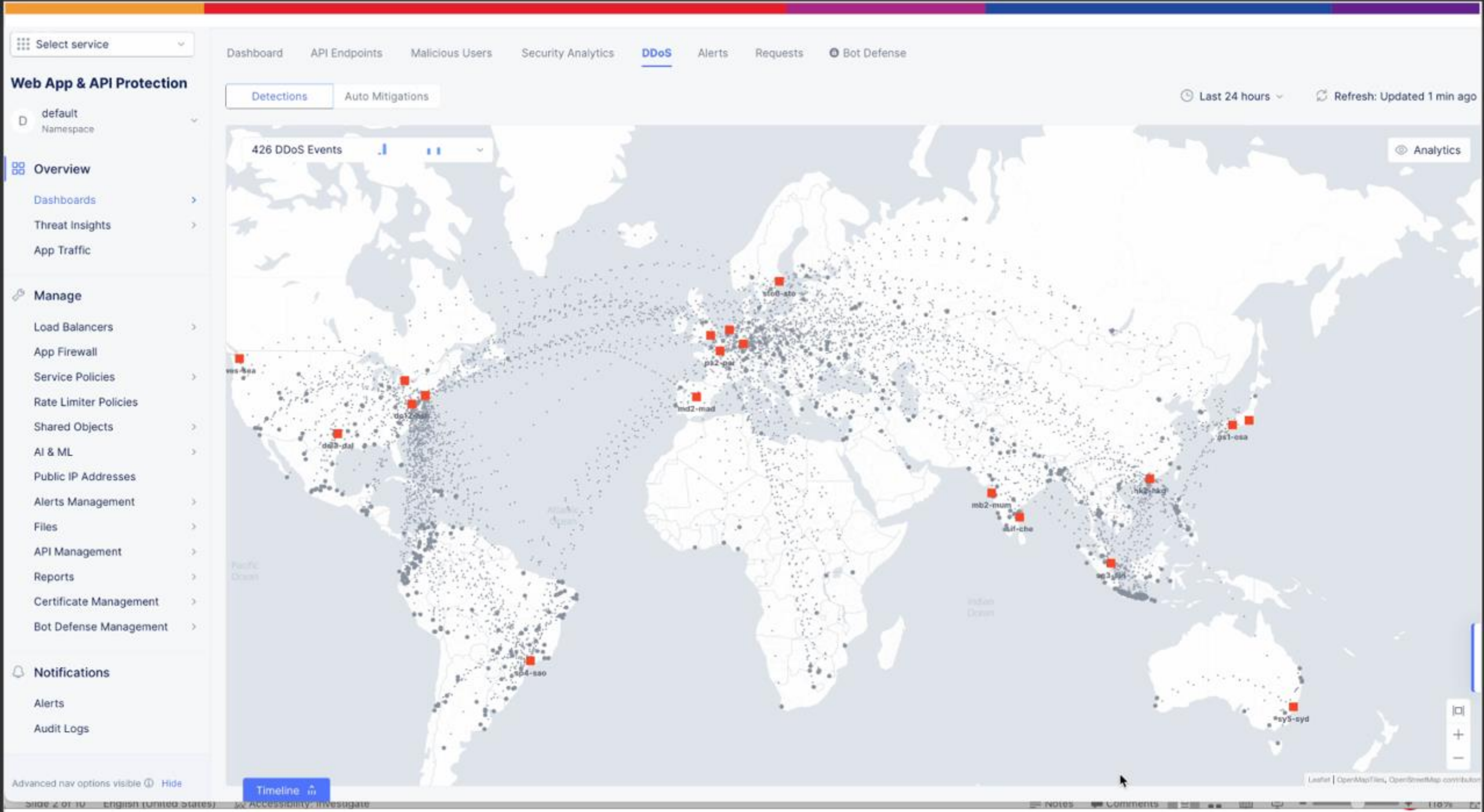
3種類の攻撃の単独あるいは組み合わせた攻撃が観測されている



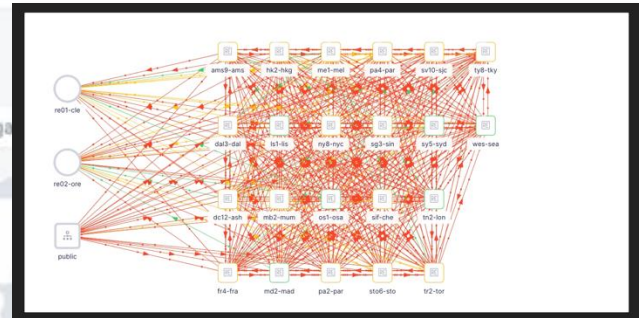
F5XCのDDoS対策ソリューションとの組み合わせ

F5XCへのDDoS対策のオフロード




Select service
Web App & API Protection
default
Namespace
Overview
Dashboards
Threat Insights
App Traffic
Manage
Load Balancers
App Firewall
Service Policies
Rate Limiter Policies
Shared Objects
AI & ML
Public IP Addresses
Alerts Management
Files
API Management
Reports
Certificate Management
Bot Defense Management
Notifications
Alerts
Audit Logs
Advanced nav options visible
Hide
Dashboard
API Endpoints
Malicious Users
Security Analytics
DDoS
Alerts
Requests
Bot Defense
Detections
Auto Mitigations
Last 24 hours
Refresh: Updated 1 min ago
426 DDoS Events
Analytics
sto-sto
ps2-par
md2-mad
ves-iad
dc12-iad
dc13-dal
ps1-osa
hk2-hkg
mb2-mum
blr-che
sg3-sin
sp4-sao
syS-syd
Timeline

世界の各地域からターゲットサイトへの攻撃



1,250,000 Requests/Sec

Bot Defense

Last 24 hours

Refresh: Updated 1 min ago

Analytics

App Traffic

Manage

Load Balancers

App Firewall

Service Policies

Rate Limiter Policies

Shared Objects

AI & ML

DoS

DoS

DoS

app

Eight Minutes and Two Peaks

After the start of the attack, traffic rose rapidly over the next two minutes to the first peak at approximately 400 Gbps. It then fell off to 125 Gbps, until about 3:07 AM UTC, when it ramped up again, sharply, to a second peak of 840 Gbps by 3:10 AM UTC. A minute and a half later, it returned to normal levels (Figure 1).

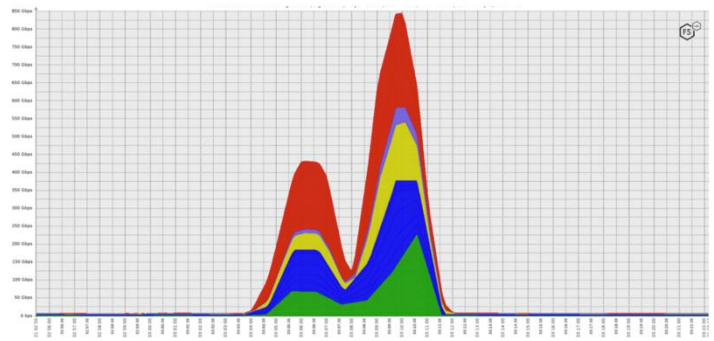


Figure 1. DDoS traffic observed. The colors indicate different Silverline datacenters.

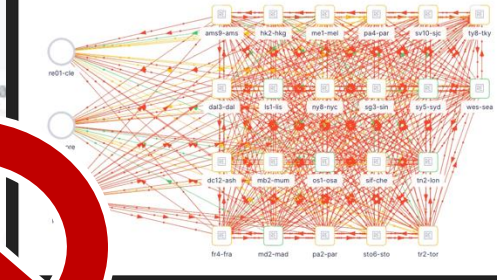
もしDMZがアプリ拠点にしかなかったら・・
世界中からの大量の攻撃を防ぎ切れますか？

Advanced nav options visible ⓘ Hide

Timeline

世界の各地域からターゲットサイトへの攻撃

120,000
Requests/Sec



1,250,000 Requests/Sec

Bot Defense

Last 24 hours

Refresh: Updated 1 min ago

Analytics

App Traffic

Manage

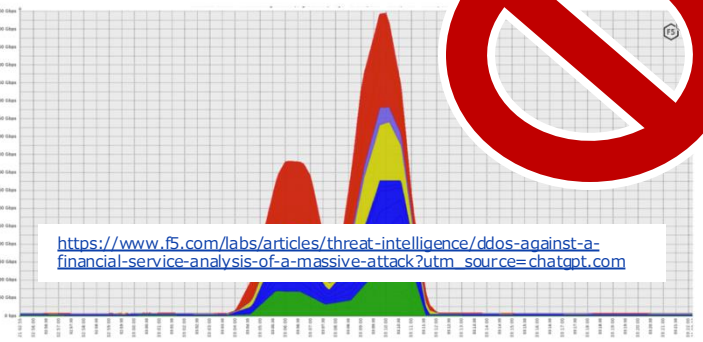
- Load Balancers
- App Firewall
- Service Policies
- Rate Limiter Policies
- Shared Objects
- AI & ML

DoS

app

Eight Minutes and Two Peaks

After the start of the attack, traffic rose rapidly over the next two minutes to the first peak at approximately 400 Gbps. It then fell off to 125 Gbps, until about 3:07 AM UTC, when it ramped up to the second peak of 840 Gbps by 3:10 AM UTC. A minute and a half later, it retu



https://www.f5.com/labs/articles/threat-intelligence/ddos-against-a-financial-service-analysis-of-a-massive-attack?utm_source=chatgpt.com

Figure 1. DDoS traffic observed. The colors indicate different Silverline datacenters.

Global Service Tier (= External DMZ) で
大量のDoS攻撃から防御可能です

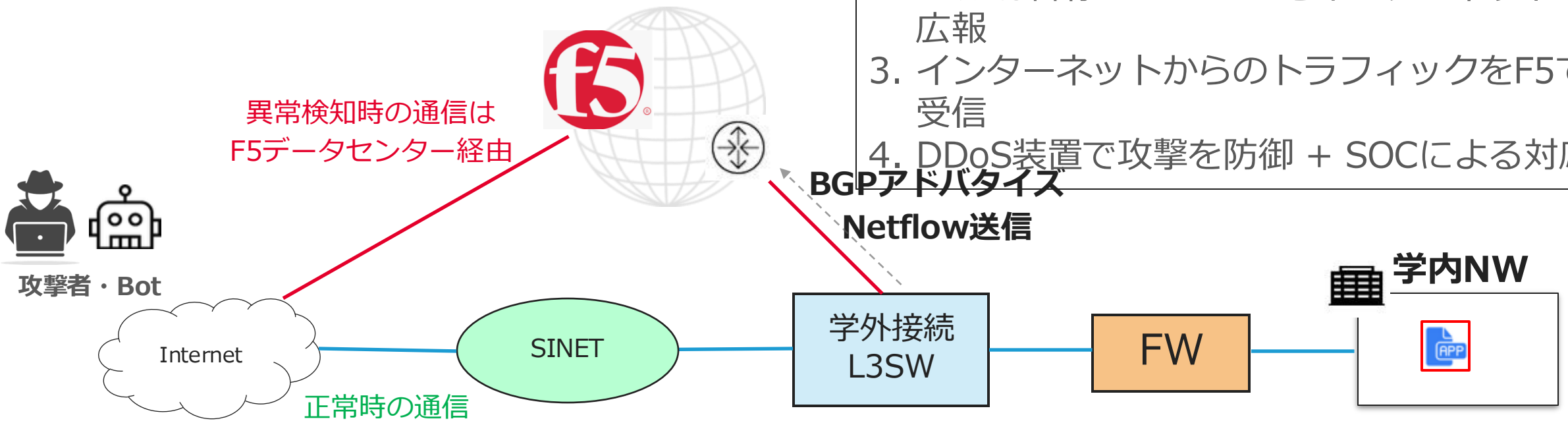
Advanced nav options visible Hide

Timeline

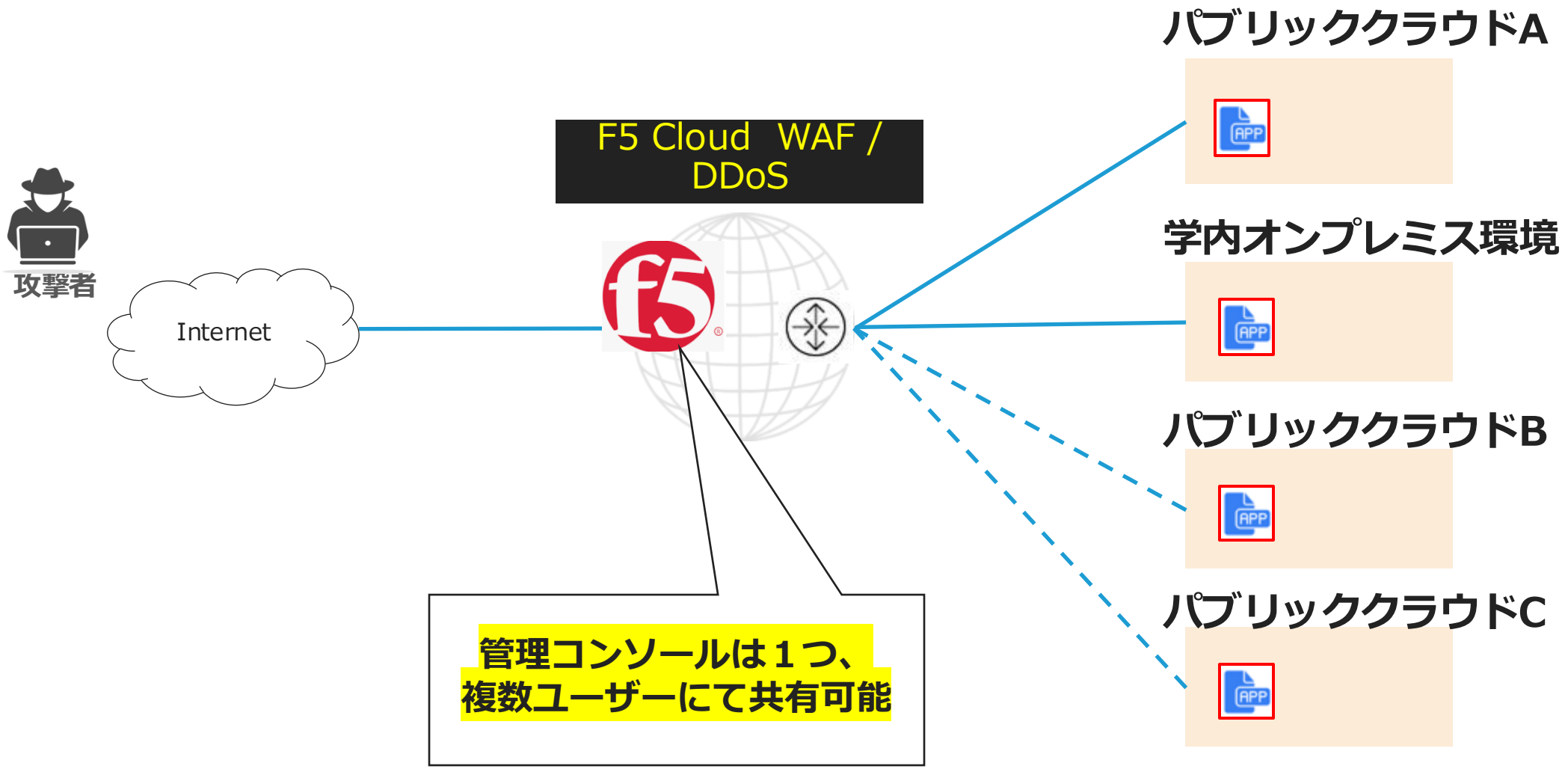
ポイント① 低コストで豊富な機能

BGPを活用したDDoS通信の迂回型の対策も可能

1. Netflow情報などで攻撃を検知
2. F5がお客様のIP Prefixをインターネットへ広報
3. インターネットからのトラフィックをF5で受信
4. DDoS装置で攻撃を防御 + SOCによる対応



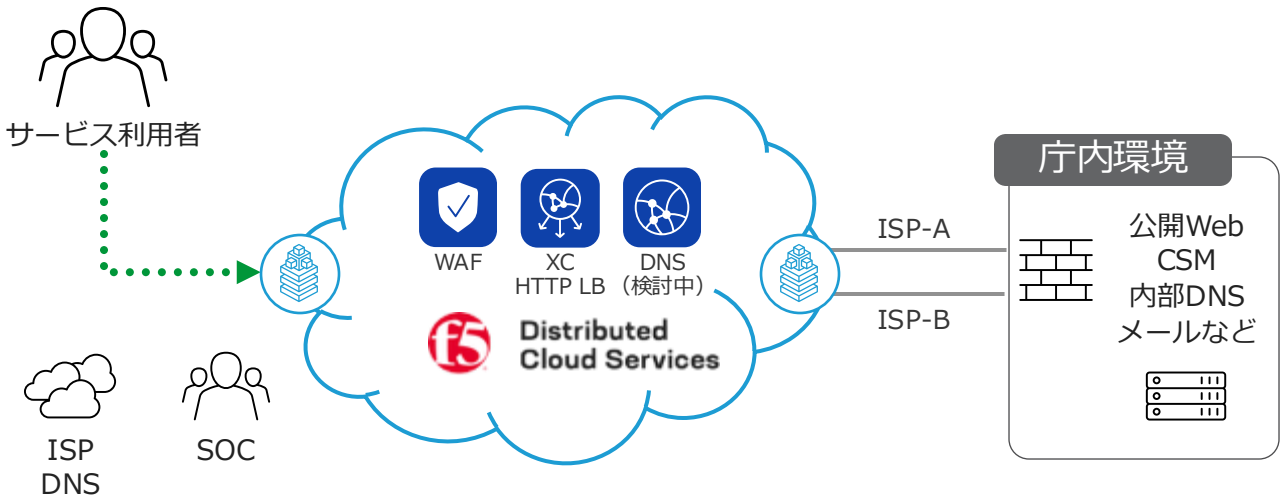
ポイント② マルチクラウド環境でも、一つの GUI から 運用・管理



教育委員会向け
F5 Distributed Cloud Services WAAP 導入

Industry: CSP | BFSI | ENT | **PUB**

Function: BIG-IP | **XC** | NGINX



■製品名・ソリューション名

- F5 XC WAAP (DNS 検討中)

■セキュリティ課題と要件

- オンプレミスのBIG-IP AWAFのリプレース
  →F5 XCとBIG-IP AWAFの比較検討（価格・機能・性能・管理などの観点で総合評価）
- 公開ウェブサーバのクラウド化
  →公開ウェブサーバをパブリッククラウドへ移行する場合の技術制約や作業工数を考慮

■F5導入のメリット

- マルチクラウドに対応
- ライフサイクル管理
- BIG-IP AWAFエンジンの継承
- SOCサービス

F5導入決定のポイント

1 マルチクラウドに対応

セキュリティ機能をF5 XCにオフロードすることで、公開Webサーバのクラウド移行にも柔軟に対応可能。

2 簡単なライフサイクル管理

F5 XCはライフサイクル管理もサービス化されているため、オンプレミスと比較してバージョンアップやパッチ管理の工数を大幅に削減可能。

3 BIG-IP AWAFエンジンの継承

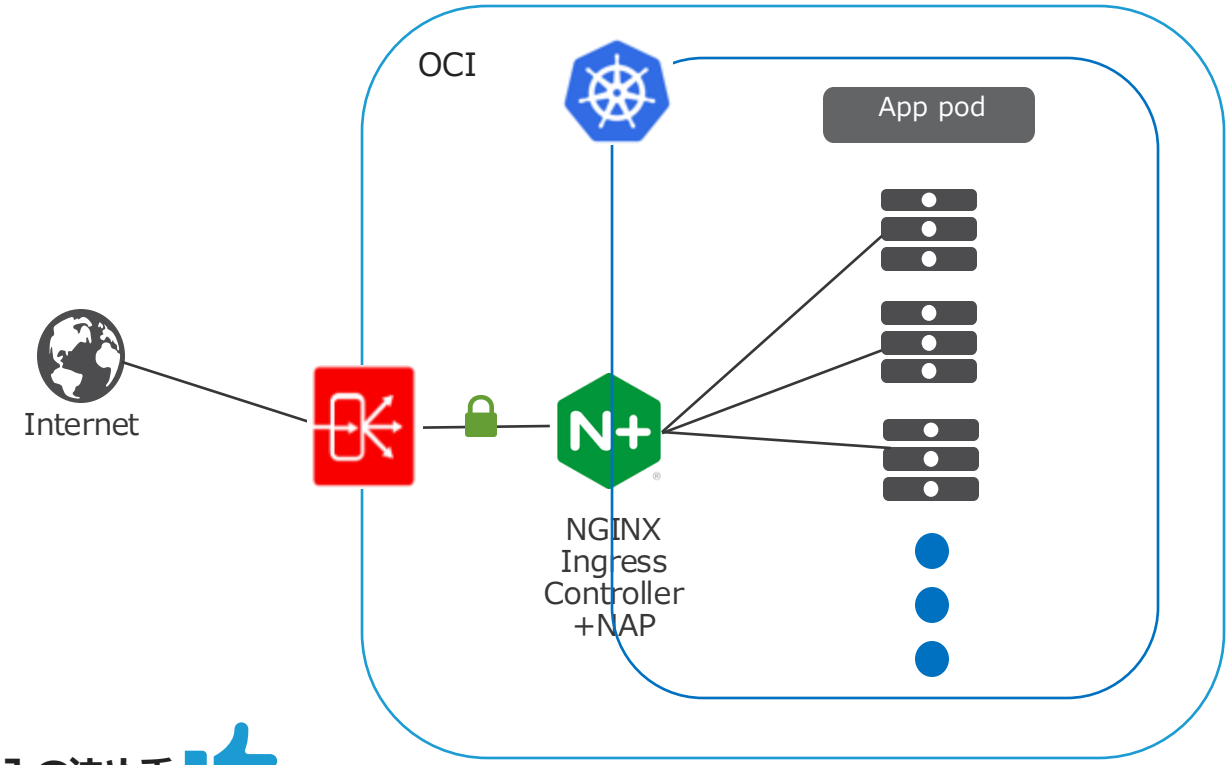
F5 XCのWAFはオンプレミスのBIG-IP AWAFと同じエンジンを採用しているため、セキュリティレベルや運用を維持しながら移行可能。

4 SOCサービス

パートナーにてF5 XCのSOCサービスを新設。構築から運用までをトータルサポート。

学術機関リポジトリ環境提供サービス用WAF

Industry	CSP	BFSI	ENT	PUB
Function	BIG-IP	XC	NGINX	



■セキュリティ課題と要件

- 外部アクセスが多いレポジトリサービスのため、WAFの導入が必須だが
  クラウドWAFだとトラフィック課金のためコストが高くなってしまう
  → コストを抑えつつ、セキュリティ機能を担保したい
- クラウド側の設計上、SSLの復号化を行う場合は
  証明書ごとに設定が個別に必要となり、運用工数が煩雑となる
  → 一元的に証明書を管理出来る仕組みがほしい
- 700を超えるBackend Podに対して証明書の管理/SSL復号化が必要
  → 暗号化通信の復号化を行ってもパフォーマンスを出してほしい

■導入のメリット

- クラウドWAFと比較して安価、かつ実績が豊富な
  F5 WAFによる高機能なセキュリティ機能を提供
- ポリシーファイル1つをメンテナンスすることで、証明書を簡単に管理可能に
- replica setを増やすことで容易に拡張/耐障害性をもたせることが出来た
- SSL復号化とWAF機能によるブロッキングを行いつつ
  低レイテンシ/高スループットによる通信を実現

F5導入の決め手

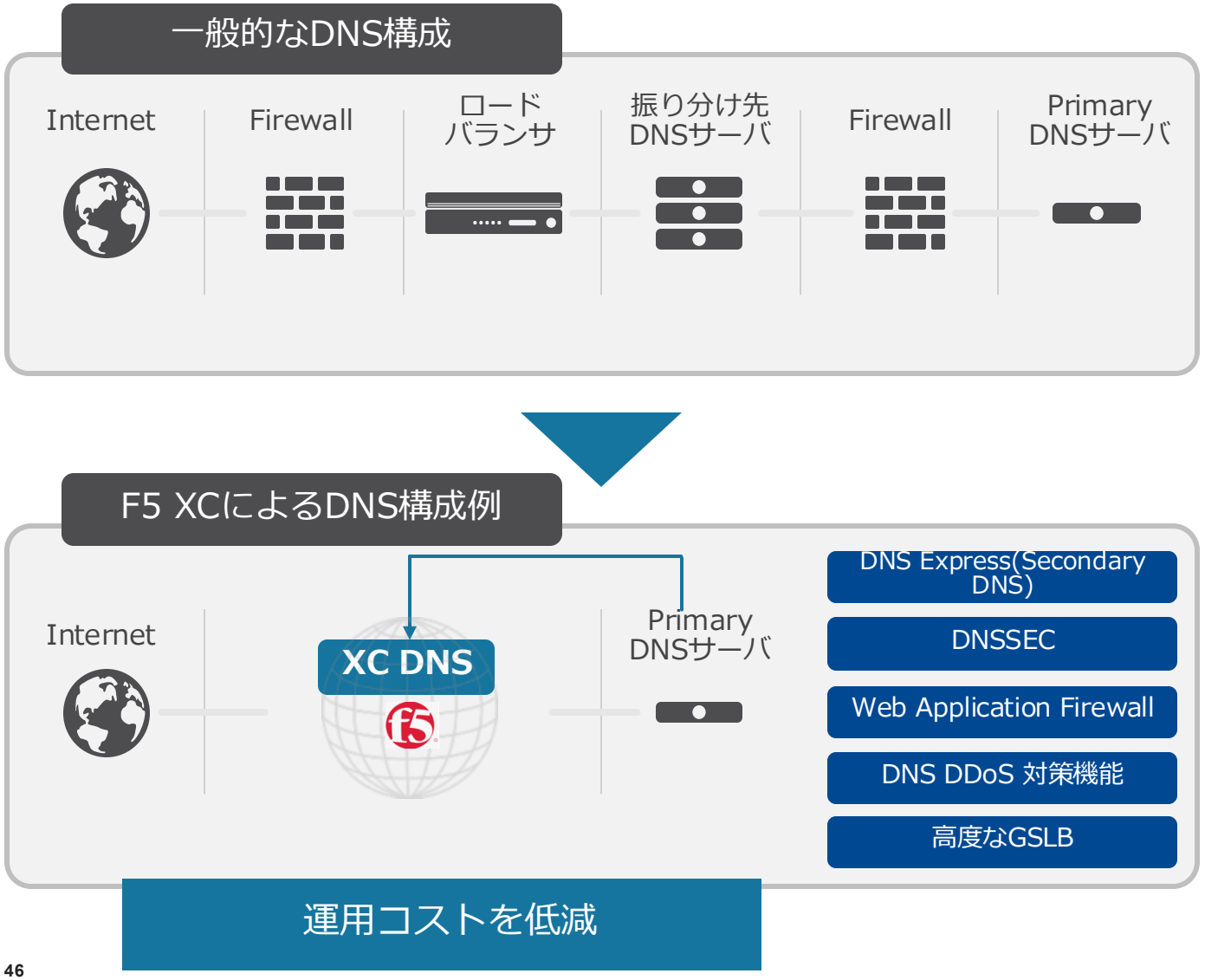
1 k8s環境で動作するWAF
k8sのデファクトスタンダードである
NGINX Ingress ControllerでWAF機能を提供

2 構成変更が不要
K8s環境外部にWAFを必要としないため
サーバ/アプライアンスを追加せず導入可能

3 高いパフォーマンス
証明書管理とWAF機能を提供しつつ
低レイテンシ/高スループットを実現

③DNS 運用負荷削減・セキュリティ対策

DNSサービスが抱える課題 ： XCの導入で解決



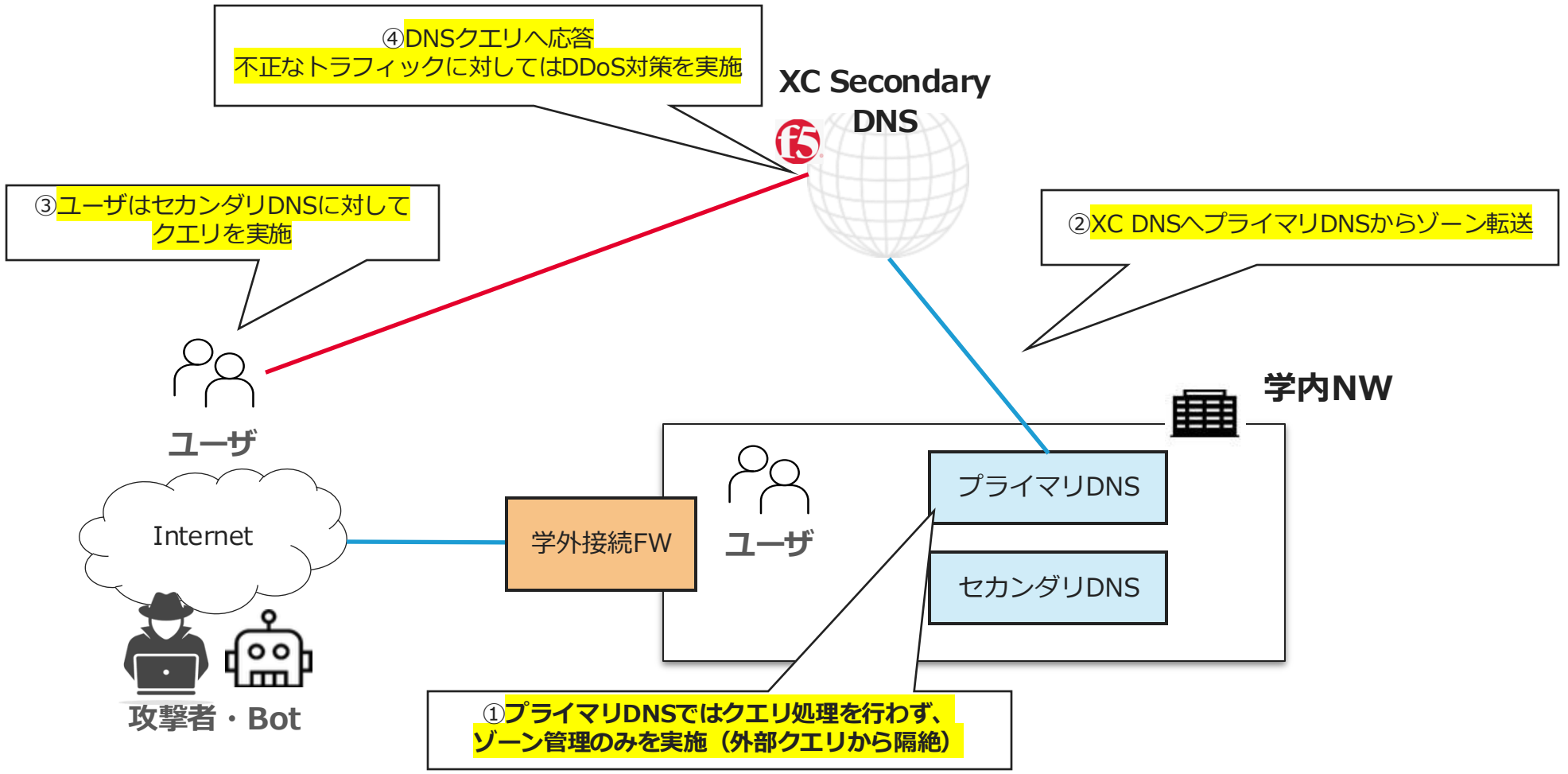
課題

- 複数DNSサーバでパフォーマンスを提供
- ロードバランサで複数DNSサーバへ振り分け
- BINDの脆弱性やログの不足
- DDoS対策は別途対応

XC DNSによる構成

- ハイパフォーマンスな クラウドDNS
  (BIND独自の脆弱性対策)
- 学内オンプレミス環境のPrimary DNSを
  そのまま利用しながら、セキュリティ対策が可能
- DNS向けのDDoS対策機能も装備

ユースケース ： セカンダリDNSとしての利用(Hidden Primary構成)



F5 Distributed Cloud DNSの特徴

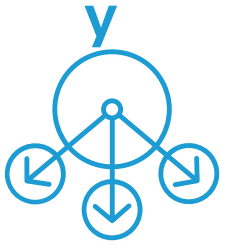
Speed and Simplicity

数クリックで、設定が完了

設定完了後、
数分でクエリに応答開始

DNSクエリ量に応じて、自動的にスケールし応答を継続

Flexibility



直感的なGUIの操作、
また宣言型APIでの自動化も可能

グローバルに分散されたインフラで構成されており、高可用性、
高性能なDNSを提供

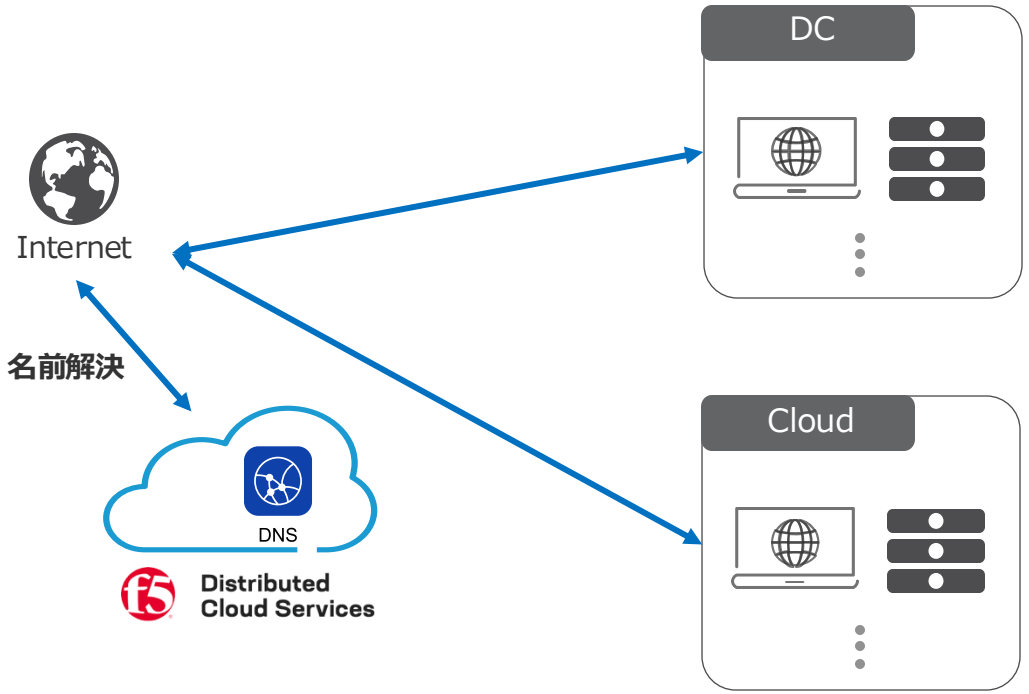
Security

セキュリティ機能の提供

- DDoSプロテクション構成済
- TSIG（Transaction Signature）認証機能サポート
- DNSSEC対応

Industry	CSP	BFSI	ENT	PUB
Function	BIG-IP	XC	NGINX	

XCでハイブリッド環境のDNS管理



■導入製品

- XC DNS (Base package)

■課題と要件

- DCとパブクラのハイブリッド環境でアプリケーションを展開
- DCで運用している既存BIG-IP LTM/DNS/ASMの更改を検討
- BIG-IP DNSで当該アプリケーション群のFQDNの権威サーバを担当
  → **課題: DC回線がダウンしてしまうと名前解決ができなくなる**

■F5導入のメリット

- クラウド化によるDNSの可用性向上
- DDoSなどのセキュリティ対策
- Base Packageによる将来的なクラウドベースのWAF導入も可能

F5 導入決定のポイント

1 良好な提案タイミング

既存BIG-IP（LTM/DNS/ASM）の更改検討において、DNS課題を起点にクロスセルに成功

2 既存環境との互換性

PoCにて既存環境のレコードをXCで利用できることを確認し、不安を解消

3 DNSの高い可用性とセキュリティ

DC回線障害時のリスクを解消しつつ、セキュリティ向上

4 DNS以外の機能活用

Base Package を購入済みのため、クラウドアプリ向けに既存BIG-IP AWAFと同等のセキュリティレベルであるWAAPを実装予定

大学ICT推進協議会2025年度 年次大会

AXIES 大学ICT推進協議会

日時：2025年12月1日(月)～3日(水)

施設：札幌コンベンションセンター