

The logo for A10, consisting of the letters 'A10' in a bold, white, sans-serif font.

Always Secure. Always Available.

自治体向けソリューション紹介

A10ネットワークス株式会社

ソーシャルインフラ・WEBサービス営業部

岩倉 弘明

A10ネットワークスについて

A10ネットワークス株式会社

設立：2009年4月

(物産ネットワークスより独立)

日本代表：川口 亨

所在地：東京本社・大阪支店

A10 Networks Inc.

設立：2004年9月

CEO：Dhrupad Trivedi

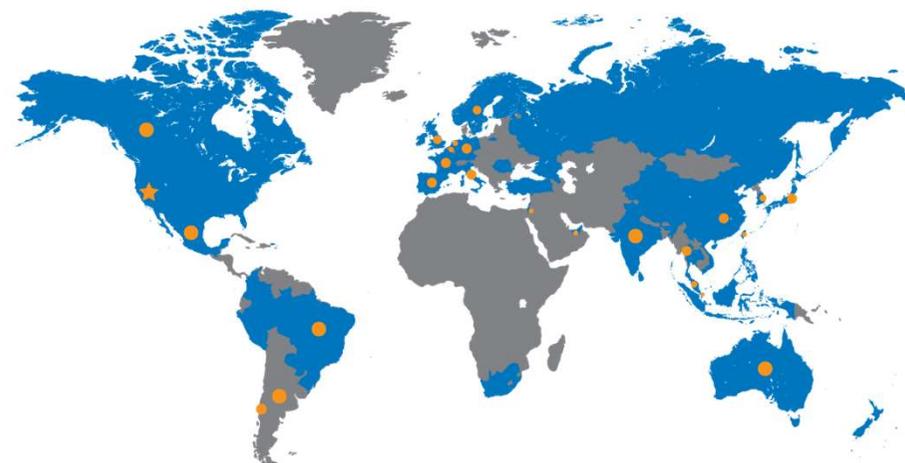
本社：San Jose, California USA

従業員数：約800名

顧客数：約8,000社

株式上場：ニューヨーク証券取引所(2014年3月)

拠点数：27ヶ国



自己紹介

名前：

岩倉 弘明

経歴：

2009年7月～2015年9月

大手通信会社公共営業部にて中央省庁を担当

2015年10月～

A10ネットワークス入社

資格：

情報セキュリティマネジメント(IPA)

趣味：

モータースポーツ(元日本チャンピオン)・釣り・ダイビング

酒場放浪(日本酒・クラフトビール)

豊富な導入実績

通信キャリア



データセンター



官公庁/自治体



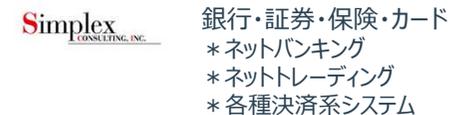
ポータルサイト



Game



金融



サービスプロバイダー/メディア



EC/SNSサービス



製造業



文教



サービス



製品機能について

豊富なネットワーク及びセキュリティ機能を搭載したソリューション

サーバー負荷分散

回線負荷分散

IPv4 <-> IPv6変換

SSL可視化

クラウドアクセスプロキシ

無害化・マルチスキャン

DDoS攻撃対策

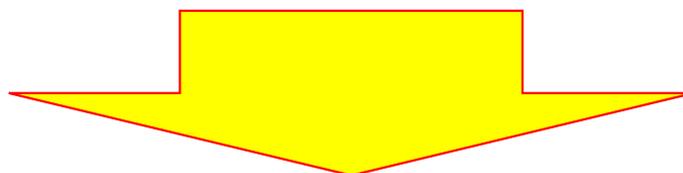
WAF

Stateful Firewall

IPLレピュテーション

URLクラシフィケーション

SSLアクセラレーション



全てのソリューションをワンボックスに統合

ソリューション紹介

クラウドサービス導入で生じるネットワークの問題

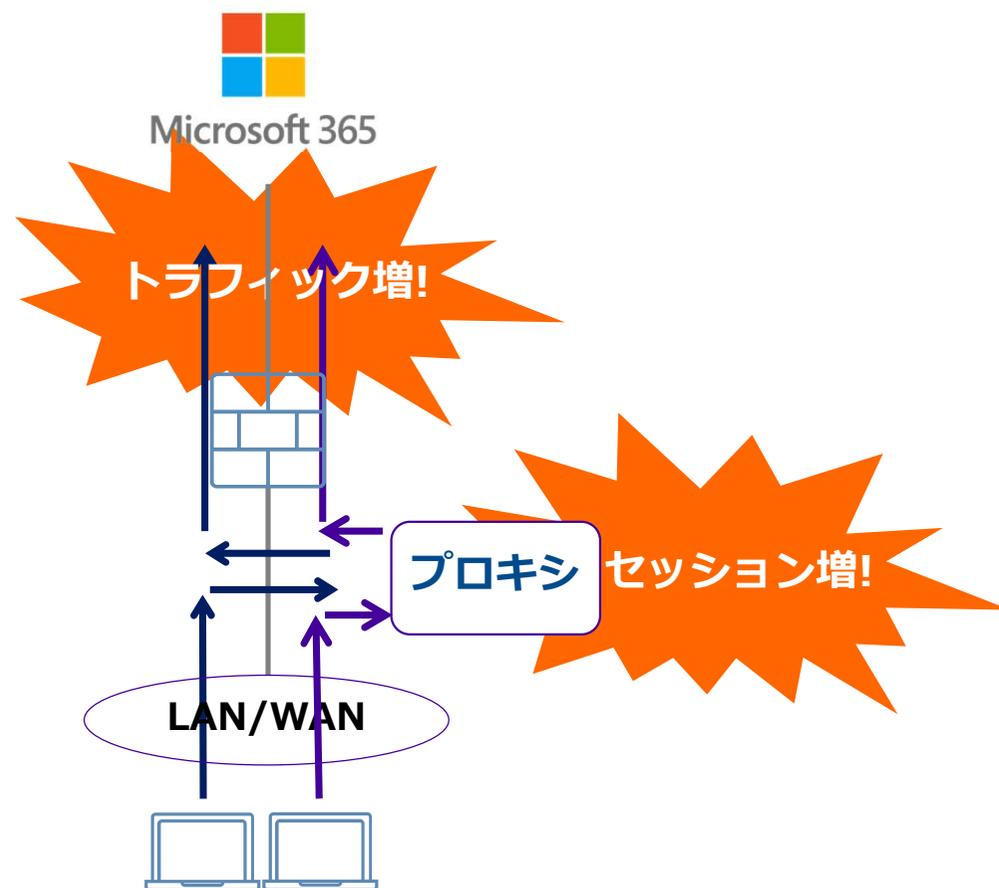
クラウドサービス導入によって、インターネット宛のトラフィックが増加し、以下の問題が発生

1. セッション増による プロキシやFWの処理限界

クラウドサービス利用によってユーザーあたり多数の同時セッションが発生します。

2. トラフィック増による インターネット回線/WAN回線の逼迫

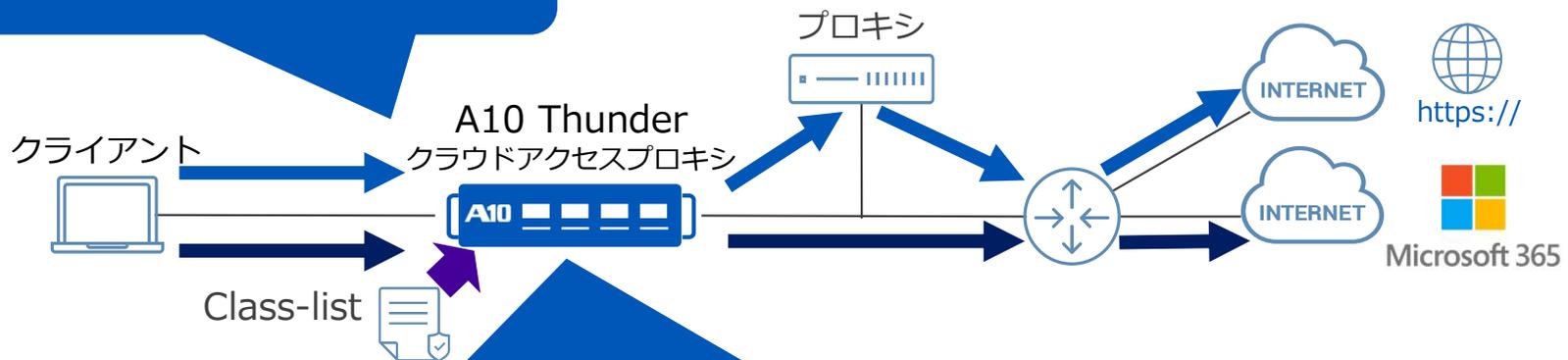
これまで社内で閉じていたトラフィックがインターネットへ向かうようになります。



A10のソリューション: クラウドアクセスプロキシ

クライアントのプロキシ接続先をA10 Thunderに変更するだけで、宛先ドメイン名に応じて通信を振り分け、プロキシをオフロード

プロキシ接続時、
宛先ドメイン名で振り分け (宛先IPも可)

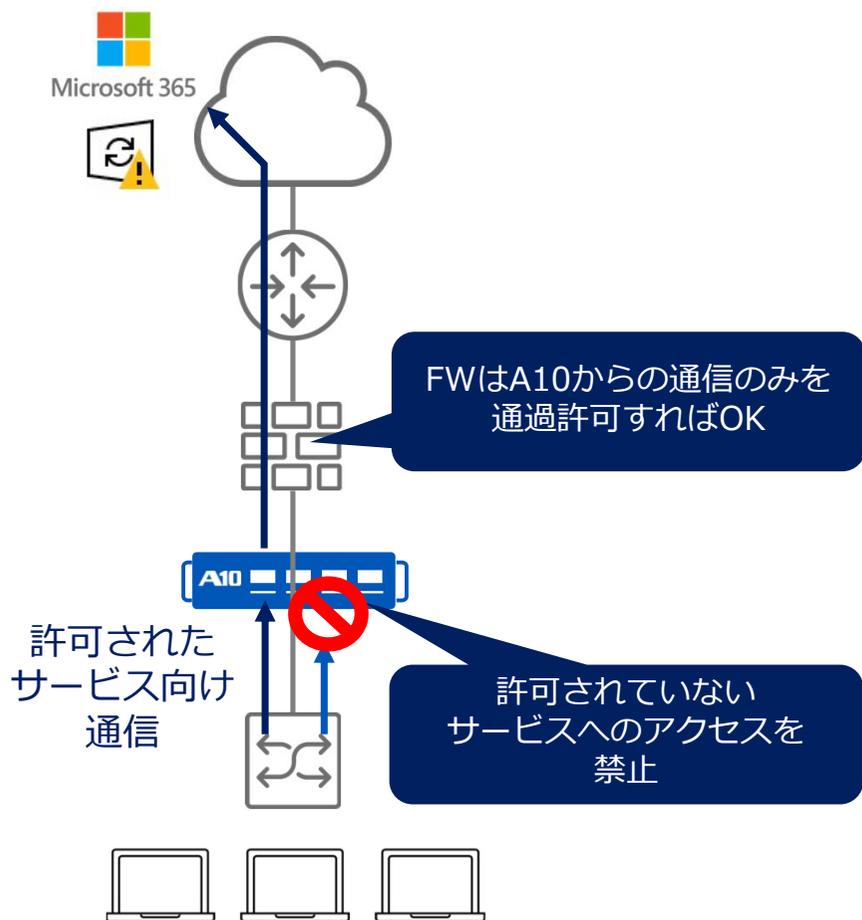


- Class-listとURL・Hostヘッダーなどをマッチング
 - サービスのドメイン以外 → プロキシサーバへ振り分け
 - サービスのドメイン → インターネット回線へ振り分け

あらゆるサービスに
ドメイン名ベースで
柔軟な振り分け設定が可能

* ドメインリスト (Class-list) の自動更新や通過するトラフィックのアクセスログ取得が可能

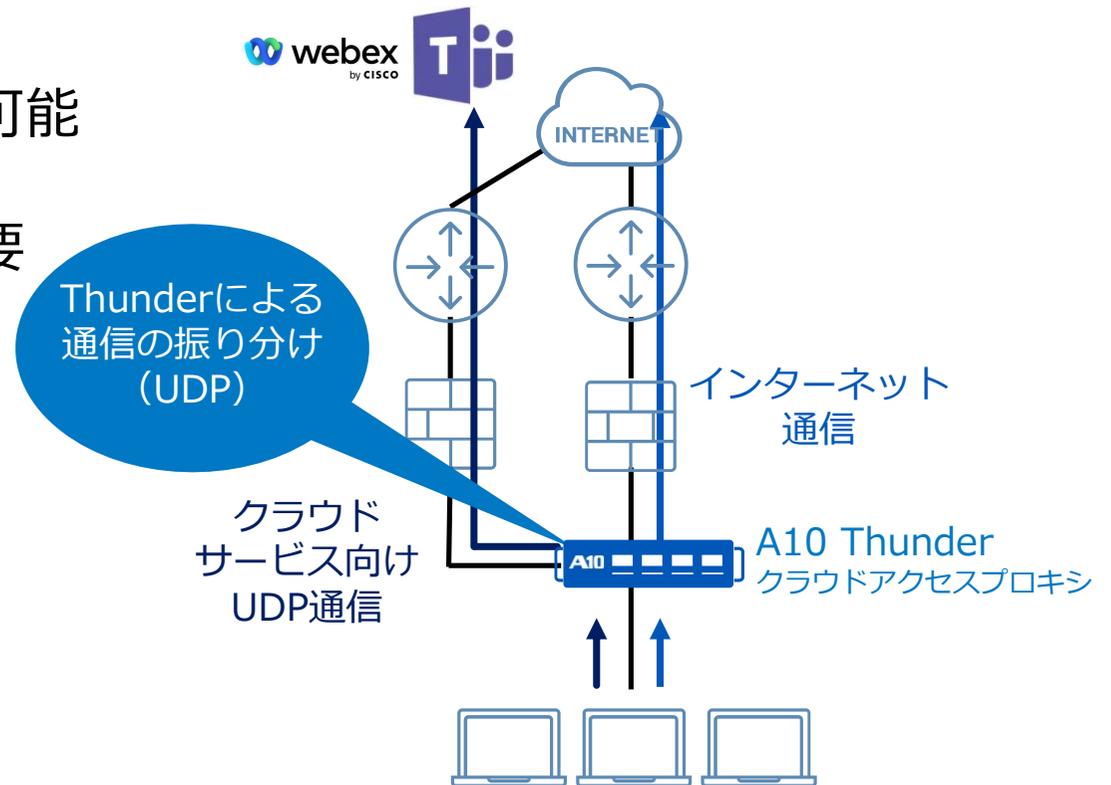
特定サイト以外へのアクセスのブロック



- Thunderを外部アクセス時のプロキシとして利用
- 特定サイト以外へのアクセスをブロック可能
 - 宛先サイト (URL、ホスト、IPアドレス)
 - ・ 送信元のリストに基づくアクセス制限が可能 (例：閉域網のクライアントからMicrosoft 365とWindows Updateのみに接続を許可)
 - リクエストのログ保管
- 認証サーバーとも連携可能
- 厳格な運用を必要とするFWとの並存が容易

ビデオ会議などの品質確保

- 通話、ビデオ会議などで発生するUDPトラフィックをThunderでステアリング
 - 専用回線への振り分けが可能
(安定した通信の実現)
 - 社内ルータの経路設定不要
 - 運用負担を軽減



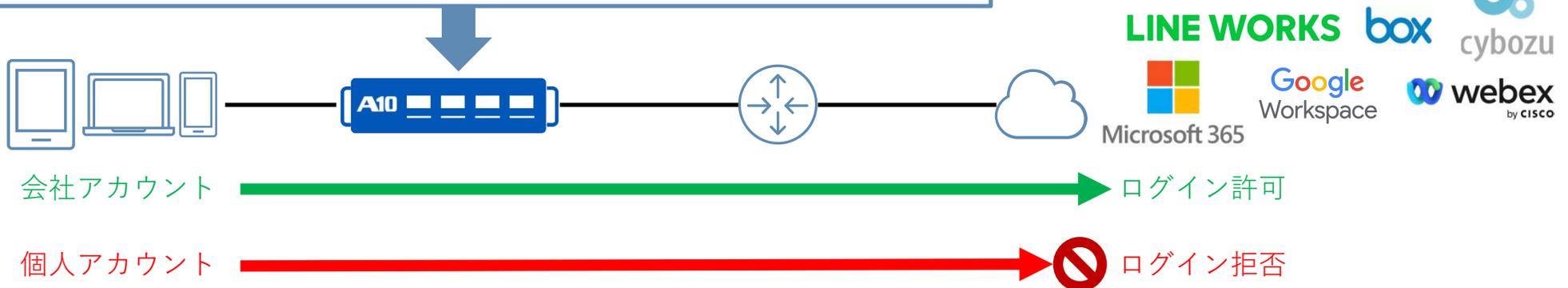
SSL/TLS復号機能の活用： クラウドサービスの利用アカウント制御

指定した法人アカウントのみクラウドサービスへのログインを許可し、
個人アカウントや他の法人アカウントでのログインを制限可能

ゼロトラスト/IDベースセキュリティ実現のための重要な要素

(ID管理基盤で制御可能なアカウントのみにログインを絞るための機能)

SSL通信を復号しテナント識別用のHTTPヘッダーを挿入、その後再暗号化後
Azure ADにてログインプロセスを検査



Microsoft 365の利用アカウント制御の動作例

許可されている法人アカウントでログインした場合



Microsoft 365に問題なくログインできる



許可されていないアカウントでログインした場合



Microsoft 365へのログインが拒否される

Google Workspaceの利用アカウント制御の動作

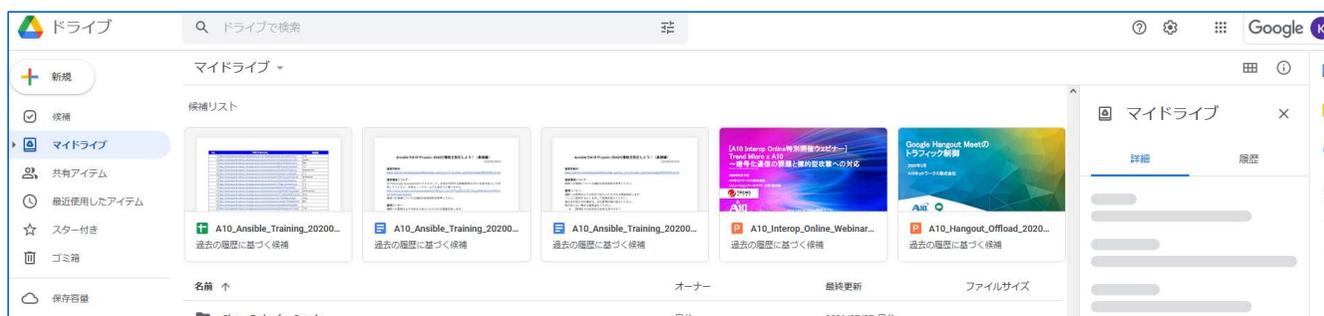
許可されている法人アカウントでログインした場合



The screenshot shows the Google login interface for a permitted corporate account. At the top, it says "Google" and "Kentaro Ishizuka". Below that, there is a dropdown menu showing the email address "k...@a10kkttest.net". A password input field is present with a "パスワードを表示する" (Show password) checkbox. A "次へ" (Next) button is at the bottom right.



Google Workspaceに問題なくログインできる



許可されていないアカウントでログインした場合



The screenshot shows the Google login interface for a non-permitted account. It says "Google" and "ログイン" (Login). Below that, it says "Google ドライブに移動する" (Move to Google Drive). There is a dropdown menu showing the email address "k...@gmail.com". A "次へ" (Next) button is at the bottom right.



Google Workspaceへの
ログインが拒否される

ルータ/UTM/FWなどのIPアドレスベースでのトラフィック制御ではダメなのか？

- 同じIPアドレスで動作する複数のサービスの区別がつかない
- クラウドサービスが利用しているCDNへの対応が十分できない
- 宛先更新にタイムラグが生じる場合がある
- 後段にプロキシがある場合、うまくトラフィック制御ができない

脅威スコアの異なるドメインが同じIPアドレスを持っている

(Microsoft 365で利用されていないrooptekno.comがoffice.comと同じIPアドレスを持つ)

```
コマンドプロンプト
Microsoft Windows [Version 10.0.19042.830]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\kishizuka>nslookup www.rooptekno.com
サーバー: Unknown
Address: 10.200.0.193

*** Unknown が www.rooptekno.com を見つけられません: Non-existent domain

C:\Users\kishizuka>nslookup rooptekno.com
サーバー: Unknown
Address: 10.200.0.193
制限のない回答:
名前: rooptekno.com
Address: 13.107.6.156

C:\Users\kishizuka>nslookup office.com
サーバー: Unknown
Address: 10.200.0.193
制限のない回答:
名前: office.com
Addresses: 2620:1ec:a92::156
13.107.6.156

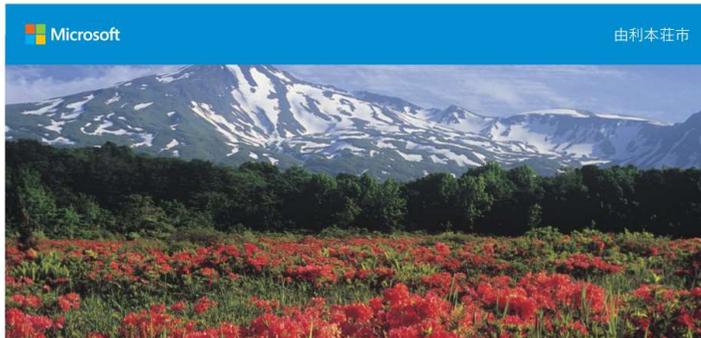
C:\Users\kishizuka>
```

ADC（プロキシベース）でのトラフィック制御の利点

- 同じIPアドレスを利用する異なるサービスがあってもドメイン名で適切に振り分け可能
- 自身で名前解決をするため、CDNが利用されていても柔軟に対応できる（CDNでIPアドレスが共有されていてもドメイン名で識別）
- テナント制御・ユーザ認証・アクセスログの取得などのセキュリティ強化も可能
- データセンターにプロキシがあっても適切にトラフィック制御可能

自治体導入事例

由利本荘市様の導入事例（日本マイクロソフト様）



お客様プロフィール
由利本荘市
<https://www.city.yuribetsu.lg.jp/>

製品とサービス
Office 365 E1
Microsoft Enterprise Mobility + Security(EMS) E3
Microsoft Defender for Office 365
Surface Go 2

業界
行政

組織の規模
大規模（従業員数 1,000 ~ 9,999 人）

国
Japan

LGWAN から直接 Office 365 を利用可能に。 三層分離の課題を解決し、 「2040 問題」に備える“由利本荘市モデル”

「セキュリティと利便性の両立」は常につきまとう課題ですが、最も苦慮している組織のひとつが行政です。高いセキュリティを保持するための「三層分離」が施されたシステムの中で、いかんして現代的なコミュニケーションへと脱皮するのか。日本中の担当者が頭を悩ませています。

由利本荘市は、Microsoft Office 365 の導入によって職員のコミュニケーション基盤を刷新しながら、「ゼロトラストセキュリティ」を段階的に進めている、先駆的な自治体です。他の市町村だけでなく、官公庁や県からも注目されている同市は、どのように ICT 化を進めているのでしょうか。

根本的なコミュニケーションの変革が必要だった

由利本荘市は秋田県で最も広大な自治体です。鳥海山を源流とする子吉川が市域を流れ、日本海まで続く、変化に富んだ自然が揃っています。同市において特に精密機械工業が発展しているのも、その清純な空気と水が、不純物の混入を防ぎ、洗い落とすことができるためです。

平成の大合併によって誕生した由利本荘市は、2013 年より「由利本荘市情報通信技術利活用推進本部（ICT 推進本部）」を立ち上げ、電子申請やコンビニ交付、AI-OCR、RPA の導入など、各種デジタルイニシアティブを展開しています。2014 年には、市レベルでは珍しい「CIO 補佐官」を外部から任用するなど、先進的な取り組みを進めてきました。

その背景について、秋田県由利本荘市 総務部 行政改革推進課の今野氏は次のように振り返ります。

「実は、ICT 推進本部の発足当初、コンサルタントを雇おうとしたのですが、コストの大きさに二の足を踏んでいたのです。そんな時、「CIO 補佐官」という制度を知り、これを軸にどうすれば市内に CIO 体制を築けるのか、卒びながら進めていきました。現在は、各部門の長が情報化を協議する本部会議を年 3 回開催するなど、全庁的な動きになっています」（今野氏）



同市において、個々の ICT 施策は比較的進んでいるものの、それが「DX（デジタルトランスフォーメーション）」として有機的に機能していないことが課題だったと、今野氏は言葉を続けます。



秋田県 由利本荘市
総務部 行政改革推進課
デジタル推進室
主任 今野 篤氏

「道具」はある程度揃ってきていて、ここ数年は「市内デジタル研修」にも力を入れてきたのですが、どうも盛り上がり欠けるなど感じていました。部分の集合が全体にならず、DX という大きなうねりが生まれていなかったのです。その根本にコミュニケーションの課題があるのではと思い、次の施策を 2、3 年前から検討していました」（今野氏）

新たな「職員コミュニケーション基盤」の在り方が検討される中、訪れたのが、新型コロナウイルス感染症（COVID-19）の世界的な流行でした。テレワークの必要性が急速に理解されたこともあり、議論は加速します。そして、由利本荘市に本格的なワークスタイル変革をもたらすソリューションとして選ばれたのは、マイクロソフトの“Office 365”と、セキュリティサービスである“Microsoft Enterprise Mobility + Security (EMS)”、“Microsoft Defender for Office 365”でした。

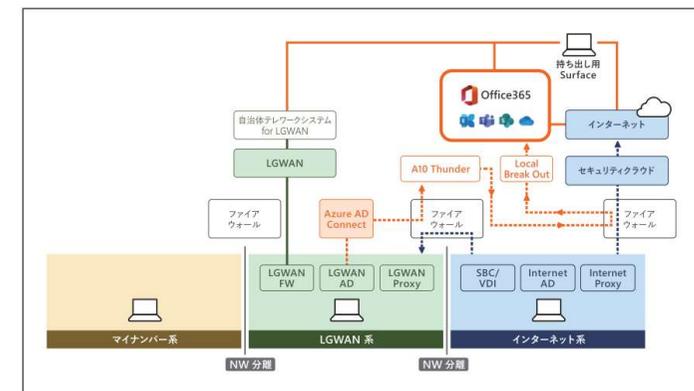
行政のセキュリティ水準を満たす アーキテクチャを設計

今野氏は、マイクロソフトのソリューションを選んだ理由について、「場当たり的なテレワーク対応にしないため」という視点を強調します。

「ビジネス チャットやオンライン会議ツールの個別導入や、現状のシステム構成に VPN 接続を加える場合など、他の方法も検討しましたが、それでは場当たり的だと考えたのです。たとえば、VPN によって遠隔地から既存システムへのアクセスを可能にしても、連絡が電話のままだと、革新的な効果など見込めるはずもないでしょう。本来目指すべきは、コミュニケーションの進化による「働き方改革」であり、テレワークの実現はその結果、あるいは過程に過ぎないはず。その視点で考えた場合、最も費用対効果が高いソリューションが、ビジネスチャットや Web 会議、グループウェアにファイル共有など、コミュニケーションのすべてが包括されている“Office 365”だったのです」（今野氏）

地方自治体のコミュニケーション基盤として、Office 365 をどのように導入していくのか、由利本荘市の試行錯誤が始まりました。重要度の高い個人情報扱う行政のシステムには、高いセキュリティ水準が求められます。インターネット接続ができる領域と、主要業務システムを扱う領域（LGWAN 系）や個人番号・個人情報扱う領域（マイナンバー系）が別れた、「三層分離」の仕組み（α モデル）が前提となっているのです。

とはいえ、インターネットの活用は DX には欠かせません。国は政府情報システムの整備において、クラウドサービスを第一候補として検討する「ク



LGWAN 系の中に業務システムを置いたまま、クラウドサービスである Office 365 の利用を可能にした“由利本荘市モデル”

由利本荘市導入事例

A10

Case Study

LGWANから直接Microsoft Office 365へ、快適かつ安全な利用を実現 A10 Thunder CFWにより「三層分離」の課題を克服した 円滑なコミュニケーション基盤を構築

顧客名：
由利本荘市
業種：
地方自治体

A10のソリューション：

A10 Thunder CFWによるMicrosoft Office 365トラフィックのオフロードと、SSL/TLS可視化機能（SSLインサイト）によるテナント制御

課題：

- 働き方改革に資するコミュニケーション基盤の構築
- LGWAN環境におけるMicrosoft Office 365の運用の最適化
- テナント制御およびドメイン更新に自動追従できる環境の構築

導入効果：

- A10 Thunder CFWのローカルブレイクアウト機能により、LGWAN環境からMicrosoft Office 365への快適な直接接続を実現
- テナント制御によるセキュアな環境構築
- Microsoft Office 365のドメイン変更を自動追従し、運用負荷を軽減



由利本荘市
総務部 行政改革推進課
デジタル化推進班
主査 今野 篤氏



由利本荘市

「A10 Thunder CFWは、コミュニケーション活性化の点で働き方改革にも大きく貢献しています。年額1億5000万円ほどの人件費の削減を見込むことができたのも、優秀なコンシェルジュであるA10 Thunder CFWのおかげです。」

由利本荘市
総務部 行政改革推進課 デジタル化推進班 主査 今野 篤氏



由利本荘市では、デジタルトランスフォーメーション（DX）による抜本的な業務効率化や働き方改革の実現を目指し、コミュニケーションの活性化に貢献するMicrosoft Office 365を導入。しかし、「三層分離」の原則を守りながら、いかにコミュニケーション基盤を活用した働き方改革を推進するか課題としていた同市は、A10 ネットワークス（以下、A10）のセキュリティプラットフォーム「A10 Thunder® CFW」を採用し、LGWAN環境におけるMicrosoft 365の運用の最適化を可能にしました。

課題：場当たりのテレワーク対応ではなく、根本的な働き方改革を実現できる基盤の構築
秋田県西部に位置し、2005年に本荘市と由利町の7つの町が合併して誕生した由利本荘市。秋田県のおよそ10%を占める広大な面積を誇り、南に秀麗な山容を誇る鳥海山、東に出羽丘陵を望み、日本海にまで貫流する一級河川の子吉川が流れる、美しい自然に恵まれています。

そんな同市は、2013年に情報通信技術利活用推進本部を設置してCIO体制を確立、翌年にはCIO補佐官を外部から招へいし、IT 関連政策や電子申請の基盤整備などのIT 戦略を推進してきました。そんななか、コミュニケーションの効率化が課題として顕在化しているのは、総務部 行政改革推進課 デジタル化推進班 主査 今野 篤氏です。「広大な面積を誇る由利本荘市では、合併の影響もあって7つの総合支所が市内のあちこちに在り、移動に車で片道1時間ほどかかることもあり。たとえば各支所長が集まる会議を実施する際には、移動時間を含めて多くの人件費がかかっていた。」

上記の課題だけではなく、コロナ禍によってテレワークの重要性が高まったことから、チャットやオンライン会議に対応する環境を検討し始めました。ただし同市が目指したのは、場当たりのテレワークの実現ではなく、根本的な働き方改革です。「テレワークは目的ではなく、あくまでデジタル化による働き方改革の結果の1つに過ぎません。物理的に離れた現場でも部署横断的な、風通しの良いコミュニケーションが実現でき、効率的な会議運営で意思決定が迅速化できることを目指しました」と今野氏は力説します。コミュニケーション基盤として選択されたのが、多くの企業や自治体で活用されているMicrosoft Office 365でした。

検証：ドメイン変更への自動追従による効率化やテナント制御によるセキュリティ強化を高く評価
オンライン会議システムの利活用にあたって、閉じられたLGWAN（統合行政ネットワーク）接続系で運用すると、テレワーク時にVPNで市内にアクセスした上でオンライン会議に接続するといった複雑な操作が求められ、使い手の面で働き方改革が阻害されることを危惧していた今野氏。そこで、業務システムの一部をインターネット環境に移すいわゆるβモデルでの自治体情報セキュリティ対策ではなく、LGWAN接続系に閉じるというαモデルの原則を踏襲しながらクラウドサービスを活用できる環境構築を検討しました。そこで注目ののが特定通信をオフロードできるA10 Thunder CFWでした。「LGWAN-ASPからパブリッククラウドの認証を可能にするサービスもありますが柔軟性が乏しく、手元でオフロードできる環境を構築しました」と今野氏は言います。

なかでも必須要件の1つとして挙げられたのが、頻繁に更新されるMicrosoft Office 365のドメインに自動追従できる仕組みでした。「Microsoft Office 365のトライアル時には、頻繁に変更されるURLに手作業にて対応していたため運用負荷が生じていましたが、A10 Thunder CFWであればこの負荷を軽減できると考えました」と今野氏は評価します。

また、Microsoft Office 365はパブリッククラウドサービスであるがゆえに、個人アカウントでのログインができてしまいます。A10 Thunder CFWであればSSL/TLS可視化機能（SSLインサイト）によるテナント制御によって、ログインするアカウントを制限し、セキュアな環境が維持できる点を評価しました。さらに、「A10はMicrosoft Office 365利用のためのオフロード実績が豊富にあるとマイクロソフトから直接聞いたため安心して利用できました」と検証初期の段階にマイクロソフトから紹介されたことも大きかったと語ります。

実際には入札要件に想定製品としてA10 Thunder シリーズを提示し、地元のインテグレータがA10 Thunder CFWを踏まえた提案にて応札。その結果、働き方改革の中核基盤であるMicrosoft Office 365の利活用を支えるソリューションとして、A10 Thunder CFWが採用されました。

ソリューション：自治体のクラウドサービスによる変革を支えるセキュリティプラットフォーム

A10 Thunder CFWは、サービス・クラウド事業者だけではなく企業や自治体まで、さまざまな組織の可用性とセキュリティを確保するための機能を統合したセキュリティプラットフォームです。

クラウドアプリケーションの通信を振り分けてLGWAN接続系からのクラウドサービスの利用やトラフィックの負荷軽減を実現するクラウドアクセスプロキシ機能、暗号化通信を悪用する攻撃の対策やテナント制御を実現するSSL/TLS可視化機能、サーバー負荷分散による可用性の確保やサイト間 IPsec VPN など、自治体のクラウドサービスの利活用を支える多様な機能をオールインワンで備えています。

これらの機能は、独自OSであるACOS(Advanced Core Operating System)に組み込まれ、ソフトウェアハードウェアによって高い性能を提供されます。

導入効果：Microsoft Office 365の柔軟なオフロードによって1億5000万円もの人件費削減に貢献

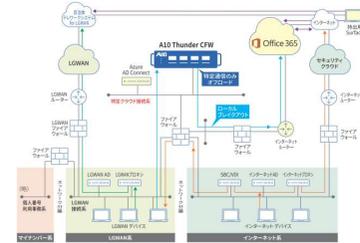
現在、在籍する約1,500人の職員全員がMicrosoft Office 365を活用しており、市内で利用されているLGWAN接続系の端末からMicrosoft Office 365にアクセスする際のオフロード処理をA10 Thunder CFWが担っています。自治体情報セキュリティクラウドを経由せず、直接インターネット接続可能な形でローカルブレイクアウトできる環境が整備されました。

また、SSL/TLS可視化機能によるテナント制御にて、個人や無料アカウントなどでのログインをブロックしています。また市外からのテレワークの実施においては、IPAが開発元となっている「自治体テレワークシステム for LGWAN」を利用し、持ち出し専用の端末からアクセスしています。なお、Microsoft Office 365についてはクラウドセッションプラットフォームとしてのMicrosoft Teamsを優先的に立ち上げ、SharePointやExchangeなどはこれから活用していく予定です。

A10 Thunder CFWのオフロード機能によって、インターネット分離によるVDIや画面転送などの環境を経由せずともMicrosoft Office 365に円滑にアクセスできるようになり、移動せずとも会議開催が可能になるなど、年間で1億5000万円ほどの人件費削減が見込まれています。「セキュリティを維持したままコミュニケーションが活性化されるなど、働き方改革にも大きく貢献します。人件費の削減でもMicrosoft Office 365のライセンス費用をすくんに還元できたのは、ローカルブレイクアウトができたからこそです」と今野氏は高く評価します。

現場で撮影された写真の共有などもOneDriveにて手軽に実施できるようになり、働き方改革という視点で試算した削減額に含まれない効果も期待できると今野氏は

システム構成図



力説します。頻繁に行われるMicrosoft Office 365のドメイン更新にも自動的に対応でき、運用面の負担軽減にも大きく寄与しています。

また運用に関しては、GUIで簡単に設定できるため、A10のソリューションを扱ったことのない地元のパートナー企業からも好評で、手厚いサポートも評価されています。「Microsoft Office 365に限らず、ホワイトリスト方式にて特定通信のオフロードが可能という面でも、A10 Thunder CFWがクラウドサービス利活用における要となっていました。適切なネットワーク経路を案内してくれるA10 Thunder CFWは、優秀なコンシェルジュと感じています」

今後の展開：クラウド活用における要として重要性が高まるA10 Thunder CFW

今後は、特定の省庁が設置している環境やその他のクラウドサービスなどの特定通信に対しても、A10 Thunder CFWによるオフロードを適用するが検討中です。「相手先が信頼できるクラウドサービスであるかどうかを適切に評価しううえで、特定通信を追加していきたい」と今野氏。LTにおけるオフロード処理の中期を扱う環境として、A10 Thunderの活用範囲はさらには拡大していく予定です。

政府の方針として「クラウドバイデフォルト」が掲げられるなか、パブリッククラウド利用に大きく舵を切り、業務の効率化を加速させることが求められています。もちろんβモデルを中心としたゼロトラスト環境を構築することも想定されていますが、完全な移行には高額の予算が必要となるため、αモデルから特定通信をオフロードする体制が現時点では費用対効果も高いと今野氏。「パブリッククラウドを柔軟に活用するには必要不可欠です。LT処理も含めてさまざまな用途で活用しながら、A10 Thunder CFWのパフォーマンスを引き出していきたい」と今野氏について語っていただきました。

A10 Networks / A10 ネットワークス株式会社について

A10 Networks (NYSE:ATEN)は、サービス事業者やクラウド事業者および企業で利用される5Gネットワークやマルチクラウドアプリケーションのセキュリティを確保します。高度な分析や機械学習、インテリジェントな自動化機能により、ミッションクリティカルなアプリケーションを保護し、信頼性と可用性を確保します。A10 Networksは2004年に設立されました。米国カリフォルニア州サンノゼに本拠地を置き、世界117か国のお客様にサービスを提供しています。

A10 ネットワークス株式会社はA10 Networksの日本子会社であり、お客様の意見や要望を積極的に取り入れ、革新的なアプリケーションネットワークソリューションをご提供することを使命としています。

www.a10networks.com/jp/

Facebook: <https://www.facebook.com/A10networksjapan>

記載された内容は2021年5月時点の情報がです。

LEARN MORE
ABOUT A10 NETWORKS

お問い合わせ：
a10networks.co.jp/contact

A10ネットワークス株式会社
www.a10networks.com/jp/

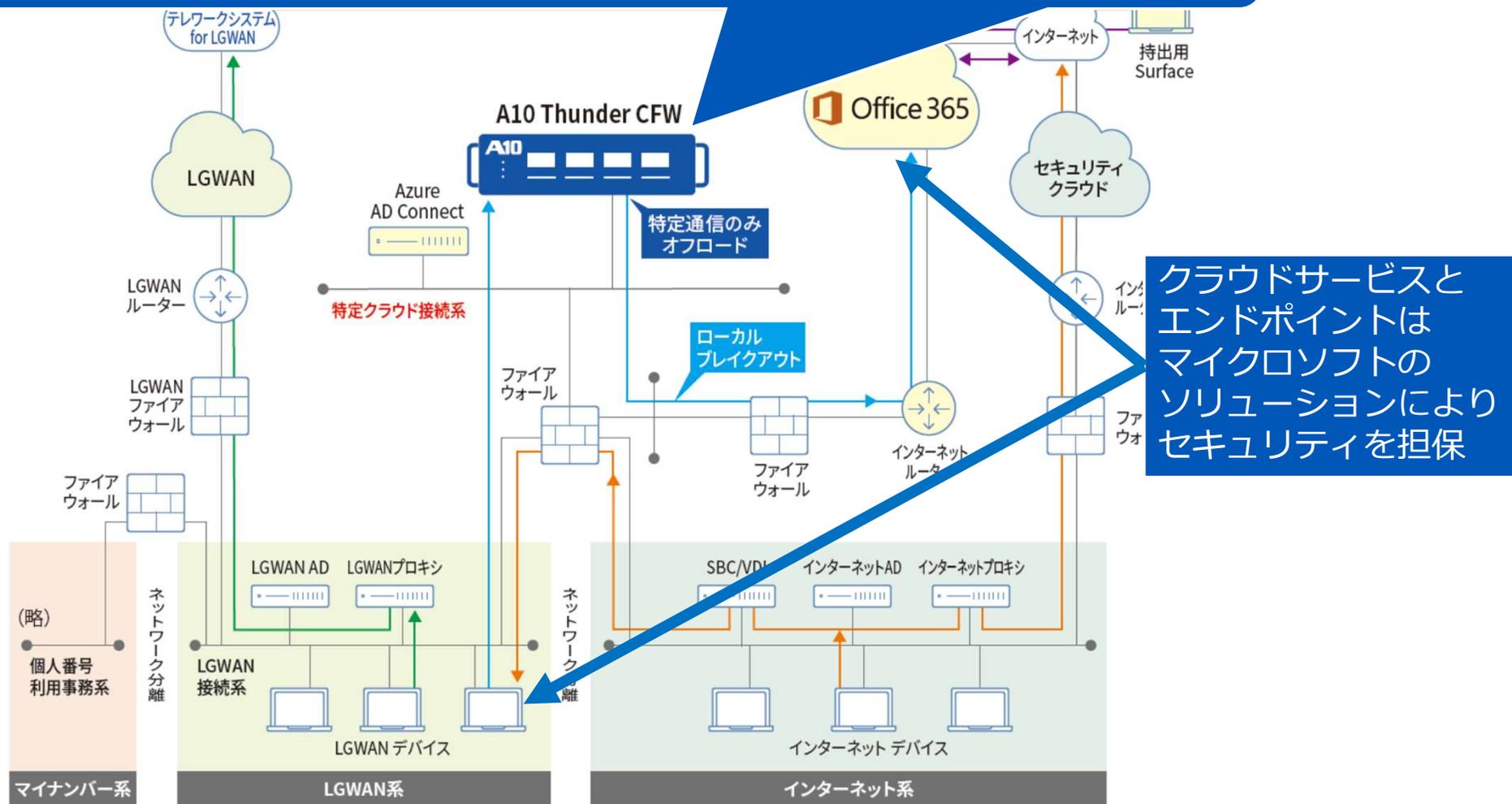
©2023 A10 Networks, Inc. All rights reserved. A10 日本: A10 Networks株式会社 2023年5月現在 | A10 Networks, Inc. 日本法人は日本法人です。本社は2004年に設立され、米国カリフォルニア州サンノゼに本拠地を置き、世界117か国のお客様にサービスを提供しています。A10 Networksは2004年に設立されました。米国カリフォルニア州サンノゼに本拠地を置き、世界117か国のお客様にサービスを提供しています。

©2023 A10 Networks, Inc. All rights reserved. A10 日本: A10 Networks株式会社 2023年5月現在 | A10 Networks, Inc. 日本法人は日本法人です。本社は2004年に設立され、米国カリフォルニア州サンノゼに本拠地を置き、世界117か国のお客様にサービスを提供しています。A10 Networksは2004年に設立されました。米国カリフォルニア州サンノゼに本拠地を置き、世界117か国のお客様にサービスを提供しています。

©2023 A10 Networks, Inc. All rights reserved. A10 日本: A10 Networks株式会社 2023年5月現在 | A10 Networks, Inc. 日本法人は日本法人です。本社は2004年に設立され、米国カリフォルニア州サンノゼに本拠地を置き、世界117か国のお客様にサービスを提供しています。A10 Networksは2004年に設立されました。米国カリフォルニア州サンノゼに本拠地を置き、世界117か国のお客様にサービスを提供しています。

由利

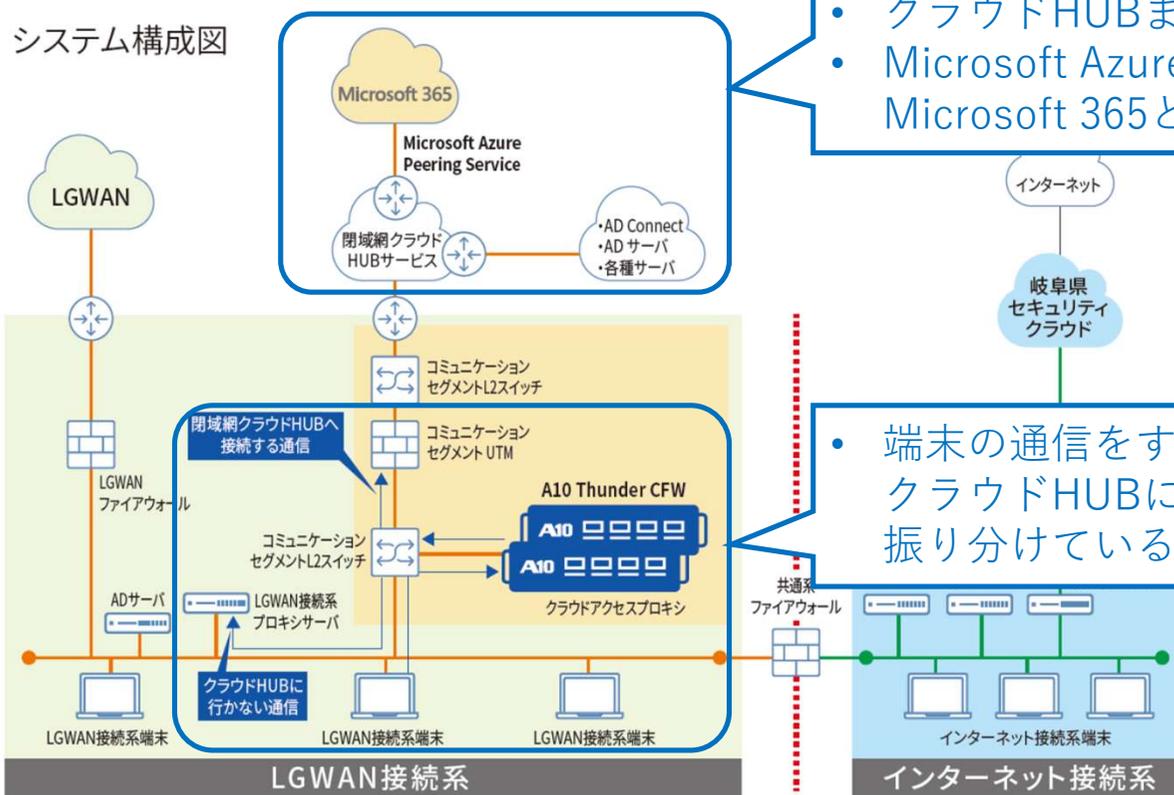
- 宛先ドメインによりOffice 365向け通信のみ許可
- テナント制御により許可されたアカウントのみOffice 365にログインを許可
- アクセスログを収集



クラウドサービスとエンドポイントはマイクロソフトのソリューションによりセキュリティを担保

岐阜市：Microsoft Azure Peering Serviceとの接続

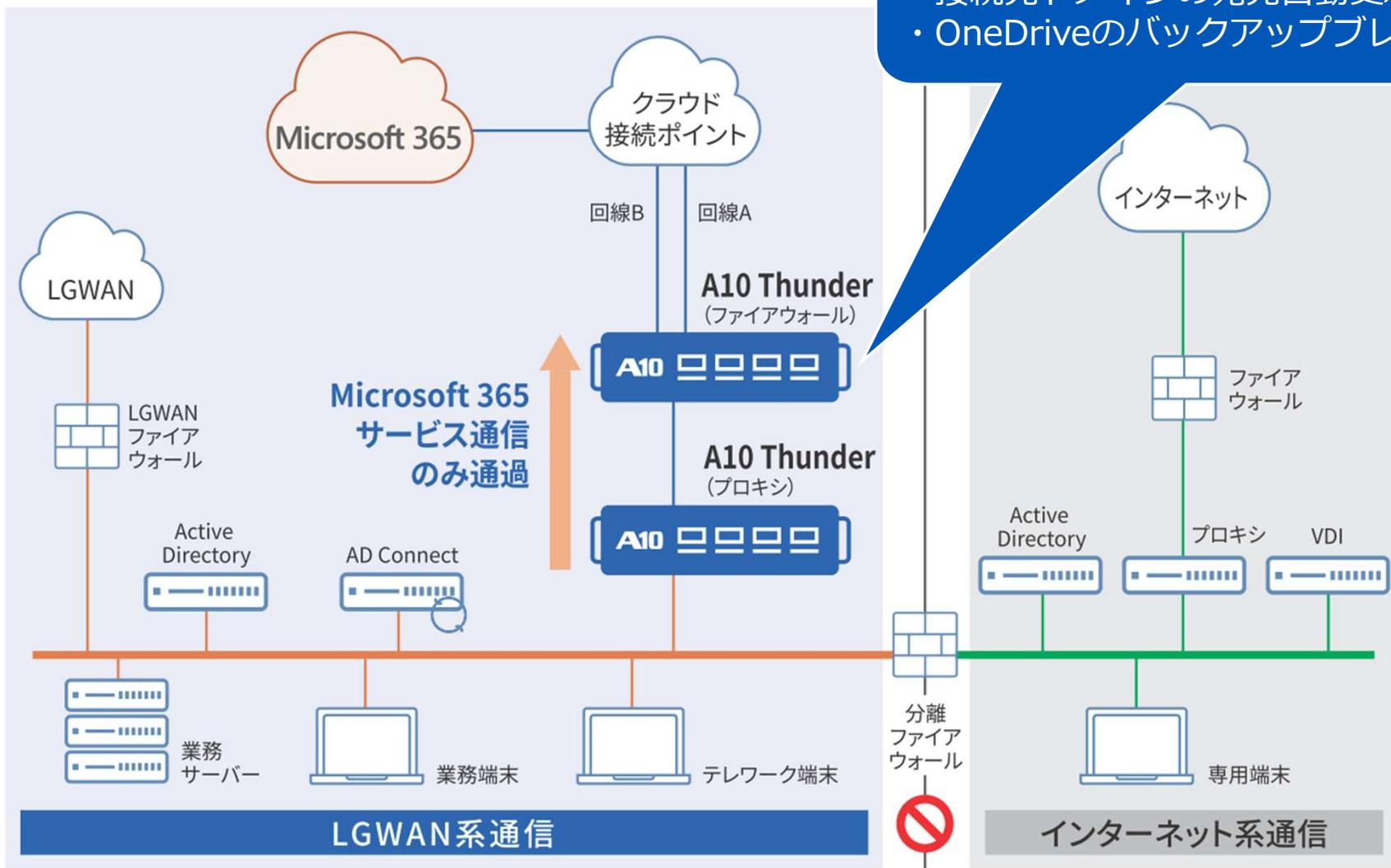
システム構成図



- クラウドHUB（通信事業者の各種クラウド接続サービス）を利用
- クラウドHUBまでは閉域網で接続
- Microsoft Azure Peering Serviceによる1ホップでのMicrosoft 365との接続

- 端末の通信をすべてクラウドアクセスプロキシに集約し、クラウドHUBに行く通信とLGWAN系プロキシに行く通信を振り分けている

名古屋市市導入事例



- ・ LGWAN系からMS365ライセンス認証通信のブレイクアウト
- ・ 接続先ドメインの宛先自動更新
- ・ OneDriveのバックアップブレイクアウト

総務省情報セキュリティ ポリシーガイドライン

情報セキュリティポリシーガイドライン

地方公共団体における
情報セキュリティポリシーに関する
ガイドライン(令和4年3月版)

平成13年 3月30日 策 定
令和 4年 3月25日 改 定

総 務 省

第1章 本ガイドラインの目的等

1. 本ガイドラインの目的

情報セキュリティポリシーとは、組織内の情報セキュリティを確保するための方針、体制、対策等を包括的に定めた文書をいう。

地方公共団体における情報セキュリティは、各地方公共団体が保有する情報資産を守るにあたって自ら責任を持って確保すべきものであり、情報セキュリティポリシーも各地方公共団体が組織の実態に応じて自主的に策定するものである。

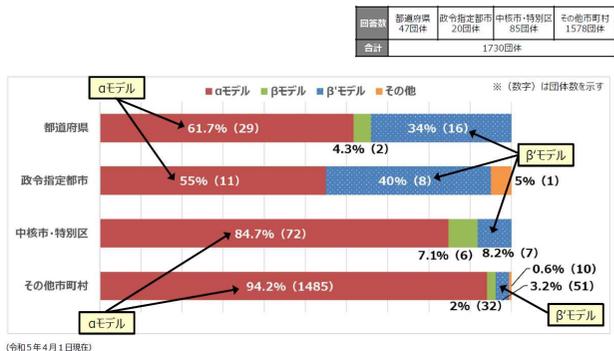
本ガイドラインは、各地方公共団体が情報セキュリティポリシーの策定や見直しを行う際の参考として、情報セキュリティポリシーの考え方及び内容について解説したものである。したがって、本ガイドラインで記述した構成や例文は、参考として示したものであり、各地方公共団体が独自の構成、表現により、情報セキュリティポリシーを定めることを妨げるものではない。

情報セキュリティポリシーガイドラインの改定

- 1 β'モデル 移行のための支援方策の検討/
- 2 LGWAN接続系のローカルブレイクアウト (α'モデル) の検討

「三層の対策」の状況 (自治体分類別)

- ✓ 回答のあった1,730団体のうち、都道府県は約3割、政令指定都市は約4割がβ'モデル団体である。
- ✓ 一方、中核市・特別区は8割以上、その他市町村は9割以上が従来型のαモデル団体であった。



今後の方向性

- ✓ 団体のネットワーク環境に応じた支援を検討することとしてはいかがか。
- ✓ αモデル採用団体のうち、β'移行を希望している団体は一定数存在しているものの断念している場合が多い。
- ✓ β'に移行した団体から、β'移行にあたっての工夫点が共有されている。

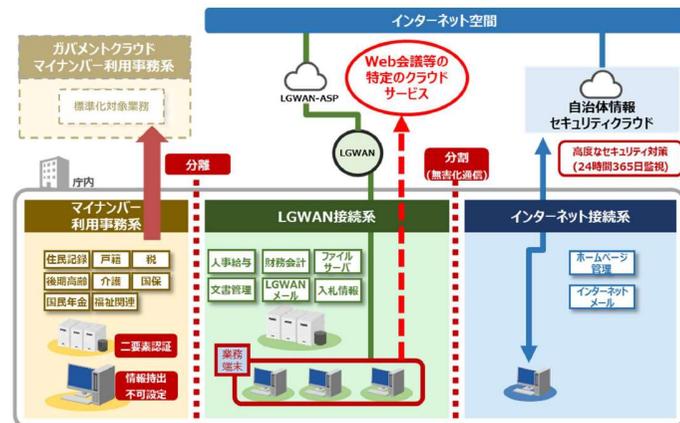
β'移行の事例や移行にあたっての工夫を横展開することで、β'モデルへの移行を推進してはいかがか。

- ✓ 他方、政令指定都市以外の市町村の大多数が、業務環境がインターネットから分割されたαモデルの状態、インターネットに接続しクラウドサービスを利用する必要があると考えられる。

セキュリティ対策を徹底の上、LGWAN接続系からWeb会議等の特定のクラウドサービスに対して直接接続を行うモデル (α'モデル) を検討してはいかがか。

α'モデルについて ~LGWAN接続系からローカルブレイクアウト~

- ✓ LGWAN接続系から外部のクラウドサービスに接続 (ローカルブレイクアウト) するための、必要なセキュリティ対策をガイドライン上で規定する必要がある。
- ✓ α'モデルのリスク評価を行い、評価結果を踏まえてガイドラインに必要なセキュリティ対策を規定する。



令和5年10月10日
地方公共団体における情報セキュリティポリシーに関するガイドラインの改定等に係る検討会 (第9回)
https://www.soumu.go.jp/main_sosiki/kenkyu/chiho_security/02gyosei/02_05001010.html

導入実績

公共ユーザ様導入実績(一部抜粋)

名称	規模	ソリューション	備考
独立行政法人	TH3040S×2台 TH1030S×2台	クラウドアクセスプロキシ SSL可視化(テナント制限)	
政府系金融機関	TH3040S×4台	クラウドアクセスプロキシ SSL可視化(テナント制限)	
中央省庁	TH4440×6台	クラウドアクセスプロキシ	
由利本荘市	TH1040S×2台	クラウドアクセスプロキシ+ SSL可視化(テナント制限)	導入事例化
中央省庁	TH3040S×12台	ADC・クラウドアクセスプロキシ SSL可視化(テナント制限)	
中央省庁	TH5840S×4台 TH940×8台	クラウドアクセスプロキシ SSL可視化(テナント制限)	
自治体セキュリティクラウド	TH1040S×12台	ADC クラウドアクセスプロキシ	
岐阜市	TH1040S×2台	クラウドアクセスプロキシ+ SSL可視化(テナント制限)	導入事例化
北本市	TH940×2台	クラウドアクセスプロキシ+ SSL可視化(テナント制限)	導入事例化
山口県	TH3040S×2台	クラウドアクセスプロキシ+ SSL可視化(テナント制限)	導入事例化
名古屋市	TH3350E×1台	クラウドアクセスプロキシ+ SSL可視化(テナント制限)	導入事例化
足利市	TH1040S×2台	クラウドアクセスプロキシ+ SSL可視化(テナント制限)	導入事例化予定

參考資料

参考資料：パートナー体制

《Platinum Partner》



Empowered by Innovation

NEC

CTC
Challenging Tomorrow's Changes



MKI

FUJITSU
富士通ネットワークソリューションズ

〈Distributor〉

SCSK

《Gold Partner》



NTT DATA
NTTデータ先端技術株式会社

HITACHI
Inspire the Next
株式会社 日立システムズ



《Bronze Partner/Authorized Reseller》



- NEC ネットエスアイ株式会社
- ジェイズ・コミュニケーション株式会社
- 日商エレクトロニクス株式会社
- 日鉄ソリューションズ株式会社

- 株式会社日立ソリューションズ
- 株式会社富士通ソーシアルサイエンスラボラトリ



- 株式会社インターネットイニシアティブ
- エイチ・シー・ネットワークス株式会社
- 株式会社エーピーコミュニケーションズ
- キヤノンITソリューションズ株式会社
- スターネット株式会社
- SB C&S株式会社
- ソフトバンクテクノロジー株式会社

- 株式会社宝情報
- デジタルテクノロジー株式会社
- 日本ビジネスシステムズ株式会社
- 株式会社ネットケアサービス
- 株式会社ネットワールド
- 株式会社富士通エフサス

参考資料：SCSK社宛先自動更新サービス

SCSK Classlist自動更新サービス (Office365ドメイン/IP 自動更新サービス/ソリューション)

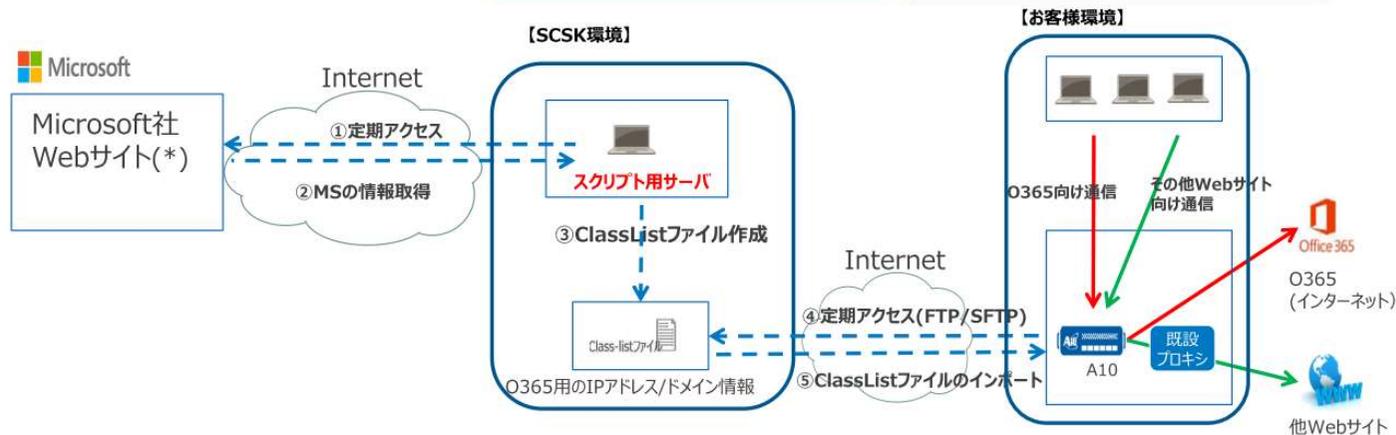
○サービス内容：A10機器へのClassListファイル自動更新サービス

お客様環境のA10機器から当社環境に定期的にアクセスし、最新のClassListファイル（O365で利用されているIPアドレス/URL）をインポートすることで、従来のO365のIPアドレス/URLの変更に伴う管理者の手動変更作業の手間を軽減するサービス

(1)MicrosoftのWebサイトを定期参照し、最新情報をJson形式で取得

(2)当社環境にて、取得した情報からOffice365のIPアドレス、URLを抽出し、A10にインポートする為のClassListファイルを作成

(3)お客様環境のA10機器からSCSK環境に定期アクセスし、最新のClassListファイルをA10機器にインポートし、機器に自動反映。



(*) <https://endpoints.office.com/endpoints/worldwide>

参考資料：他社製品比較

	A10	他社FW/UTM	他社ADC	SD-WAN
ブレイクアウト	○	○	△ (追加ライセンス要)	×
パフォーマンス	○	△	○	×
トラフィック制御	○ (URL/ドメイン/IPベース)	△ (IPアドレスベース)	○ (URL/ドメイン/IPベース)	△ (アプリケーション識別やIPベース、トラフィック制御の精度が必ずしもよくない)
FW機能	○ (L4/L7 FW)	○	△ (追加ライセンス要)	×
テナント制限	○ (標準機能)	△ (パフォーマンスに懸念あり)	△ (追加ライセンス要)	×
宛先更新	○	△ (DB更新にタイムラグあり) (DB精度にやや難あり)	△ (別途サービス契約が必要)	○
導入実績	○	△	△	△

参考資料： セキュリティ担保に必要と想定される技術的対策

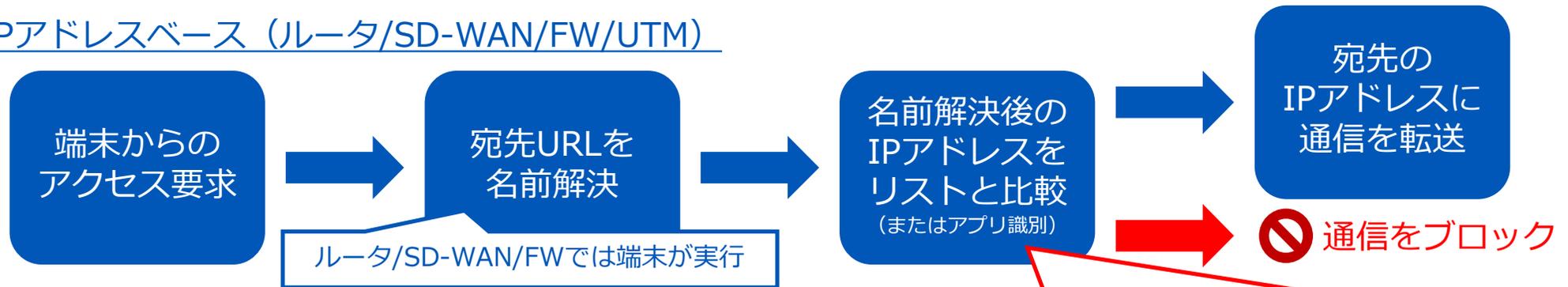
技術的対策	対策の適用場所			
	ネットワーク	業務端末	業務サーバー	クラウドサービス
接続先クラウドサービスの制限	○			
クラウドサービスを利用可能なテナントの制御	○			
通信の暗号化	○			
DDoS対策	○			
冗長化	○			
侵入検知/侵入防止	○		○	
権限管理とアクセス制御	○	○	○	○
EDR		○	○	
パッチ適用	○	○	○	
ファイルの無害化	○			○
マルウェア対策		○	○	○
ファイルダウンロードの制限				○

A10 Thunderで提供可能な機能範囲
ネットワークセキュリティの提供範囲
エンドポイントセキュリティの提供範囲
クラウドサービスの提供範囲
OPSWAT等のソリューションで提供可能な範囲

参考資料：

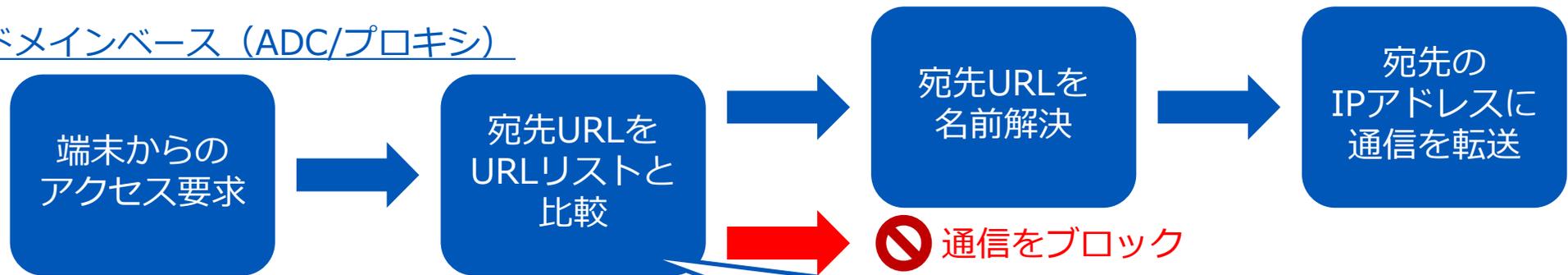
IPアドレスベースとドメインベースの処理の違い

IPアドレスベース (ルータ/SD-WAN/FW/UTM)



IPアドレスだけでは真にサービスで利用されているかどうかの保証はない
IPアドレスのリストが正確に更新されていなければサービス利用の障害となる

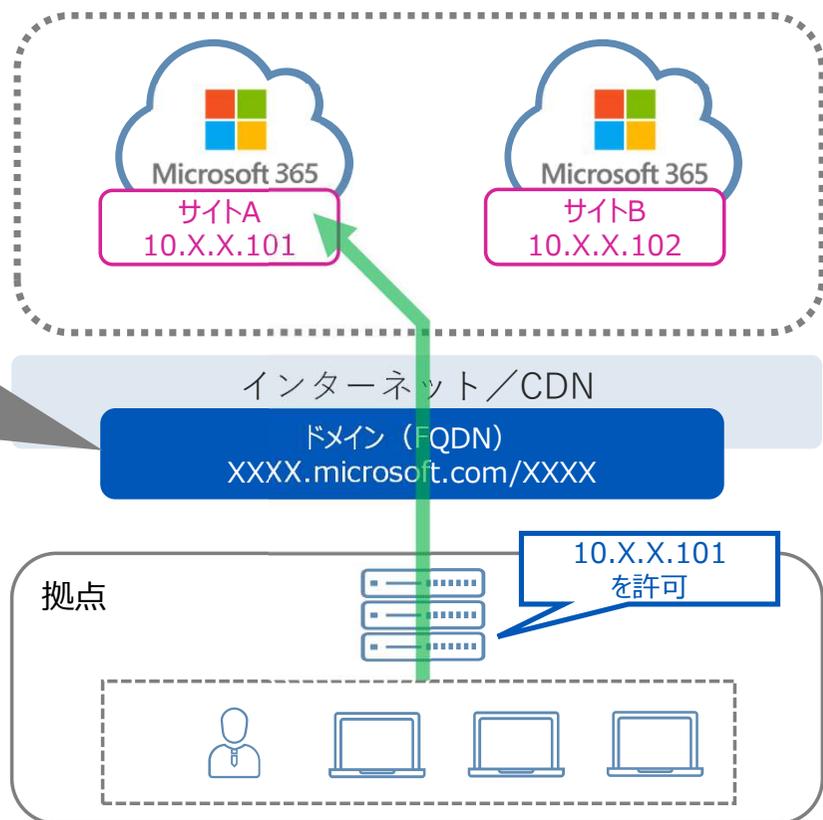
ドメインベース (ADC/プロキシ)



真にサービスで利用されるドメインかどうかを判定し制御できる
ドメインリストの更新はIPアドレスの変更に対して頻度は低い

参考資料：

IPアドレスではサービス接続が上手く動作しないパターン



パブリッククラウドサービスの多くがドメインで宛先を定義

障害等なんらかの理由でサイト (IPアドレス) が変わったときに接続できなくなる恐れ

IPアドレスとドメインのデータベースの更新が遅れた場合に接続できなくなる恐れ

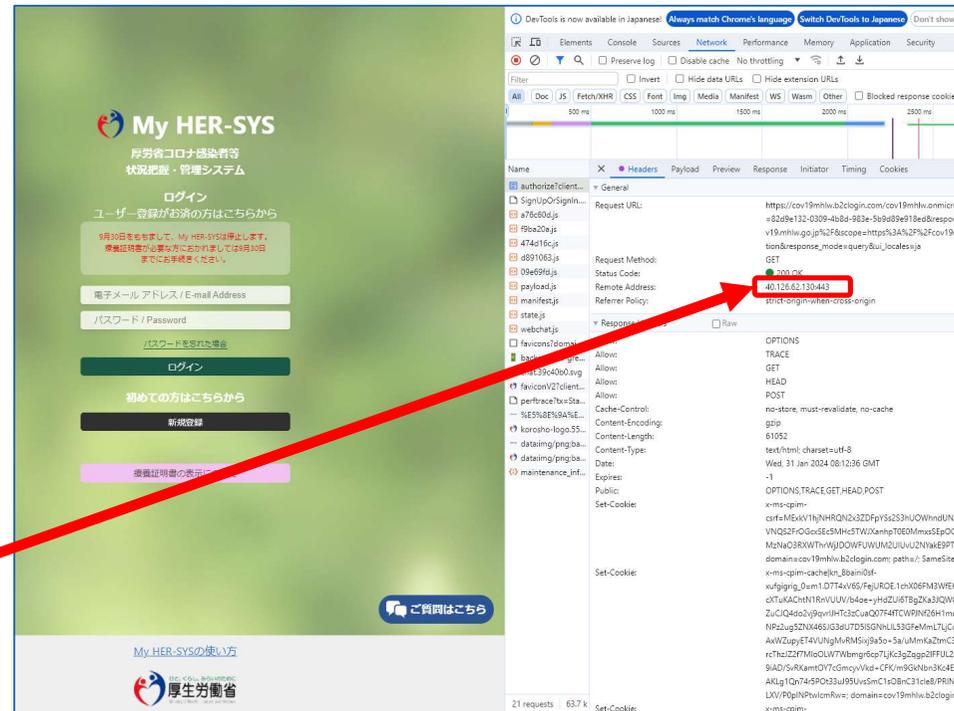
参考資料：

IPアドレスだけではサービスの区別がつかないパターン

- 例えば厚生労働省が提供していたHER-SYSの認証サイトは login.microsoft.com と利用するIPアドレスが同じ

```
C:\>nslookup login.microsoft.com
...
名前:      www.tm.a.prd.aadg.trafficmanager.net
Addresses: 2603:1037:1:128::9
...
          20.190.190.196
          40.126.62.130
          40.126.62.131
...
Aliases:   login.microsoft.com
           a.privatelink.msidentity.com
           prda.aadg.msidentity.com

C:\>nslookup cov19mhlw.b2clogin.com
...
名前:      www.tm.a.prd.aadg.trafficmanager.net
Addresses: 2603:1036:3000:f8::3
...
          20.190.190.196
          40.126.62.132
          40.126.62.130
...
Aliases:   cov19mhlw.b2clogin.com
           prda.aadg.msidentity.com
```



40.126.62.130をlogin.microsoft.comへのアクセスのために通信許可すれば、HER-SYSの認証ページにも通信できてしまう

A10

Always Secure. Always Available.

[A10networks.com](https://www.a10networks.com)

お問い合わせ先：

岩倉 弘明

TEL : 03-4520-5700

携帯 : 080-4006-1247

Mail : hiwakura@a10networks.com

