SDP利用シナリオ集

ソフトウェア・ディファインド・ペリメタ

(Software Defined Perimeter : SDP) の活用

CSA ジャパン　SDP ワーキンググループ

バージョン 1.0

本書の提供について

本書「**SDP利用シナリオ集**」は、CSAジャパン SDPワーキンググループの以下のメンバーが作成し公開したものです（順不同、敬称略）。

生田隆由　ベライゾンジャパン合同会社　（SDP-WG リーダー）
太田拓也　テクマトリックス株式会社
斉藤晃一　株式会社日立ソリューションズ
坂本晋一　ベライゾンジャパン合同会社
塩田英二　CSA ジャパン　会員
矢部沖比古　ベライゾンジャパン合同会社
諸角昌宏　CSA ジャパン　業務執行理事

また、本書は予告なく変更される場合があります。以下の変更履歴（日付、バージョン、変更内容）をご確認ください。

変更履歴

日付	バージョン	変更内容
2019 年 4 月 25 日	1.0	新規リリース

日本クラウドセキュリティアライアンスに関する情報は、以下の URL より参照可能です。
https://cloudsecurityalliance.jp

2019 年 4 月 25 日

コンテンツ

はじめに

ソフトウェア・ディファインド・ペリメタ (Software Defined Perimeter ：SDP) は、ネットワークを経由した様々な脅威からアプリケーションインフラや利用者の情報を守るための技術です。

従来、企業の外部と内部の間に境界 (Perimeter) としてファイアウォール等の物理的な装置を設置し、内部へのアクセスまたは外部へのアクセスを制御してきました。これらの機能は、外部からの脅威をブロックして内部を守る単純な機能としては有効でした。しかし、昨今、BYOD、内部に入り込んでのフィッシング攻撃、また、外部にある各種クラウド利用の増加に対して、従来の防御方法では対応が困難になってきました。

「ゼロトラスト ネットワークの考え方」に基づいた SDP の思想

「あらゆるデータ侵害は『信頼する』としたネットワークモデルのほころびから生じている。データ侵害をなくすには『ゼロトラスト』が必要である。（John Kindervag（2010）「Zero Trust Network Architecture、『Forrester Research』）」。

「ゼロトラスト」、つまり「信頼しない」ことを前提としたセキュリティが叫ばれています。クラウドに代表されるように、機密データ等が、企業の境界の中（いわゆるオンプレ）だけでなくあらゆる場所に保存されるようになり、今までのようにネットワークの境界をファイアウォールなどのネットワーク・ベースのセキュリティ対策で守ることが難しくなってきています。このような状況では、以下に述べるセキュリティの原則に基づいて、ゼロトラスト環境下にあるデータをいかに守っていくかを考える必要があります。

ゼロトラスト下での 3 原則

- 場所に関係なく、全てのリソースに安全にアクセスできることを保証する
- すべてのトラヒックのログを調査する
- 最小権限の原理を維持・強化する

このためには、従来のネットワーク型のセキュリティをアイデンティティ型のセキュリティに変える必要があり、その対策として以下の 3 点が重要になります。

- アクセスが許可される前は、全ての内部・外部の接続要求を信用しない
- 誰がアクセスしてきたかがわかるまでは、ネットワークを閉じておく
- 認証されるまでは IP アドレス、デバイスなどのアクセスを許可しない

SDP は、その名前に由来するように「境界線（Perimeter）をソフトウェア上で構築、集中的に制御し、アクセス制御に関わる設定を柔軟に動的に変更して安全にデータを転送する」技術です。SDP は、常に動的に相手先のアドレスなどを決定するため、その通信経路を外部侵入者から発見されず、従って、攻撃やデータ漏洩・侵害を防ぐ仕組みを提供することができます。

また、SDP が実際に「ゼロトラスト」環境において安全であることを実証するために、定期的に「SDP ハッカソン」を実施しています。「SDP ハッカソン」では、SDP 環境を攻撃できる情報（SDP を構成する要素の IP アドレスやクレデンシャルなど）を公開し、世界中から実際に攻撃を仕掛けていただき、その攻撃に対して SDP が安全に対応できるかどうかを検証しています。今まで 2014 年から 2016 年の間に 4 度開催された SDP ハッカソンの内容を以下に記載します。4 回のすべてのハッカソンにおける攻撃において、SDP は一度も破られたことはなく、世界中の参加者にその堅牢な仕組みを経験いただいております。

CSA 本部におけるハッカソンの実績

第 1 回：2014 年 2 月

目的：内部脅威
概要：攻撃者に SDP の全てのコンポ―ネットの情報を提供。正規のユーザーのターゲットサーバーへのアクセスのフルキャプチャを提供。SDP のアーキテクチャモデルの理論を証明。

第 2 回：2014 年 10 月

目的：DDoS 攻撃
概要：攻撃者に SDP Gateway の IP アドレスを提供。SDP コントローラー側の強度を実証。

第 3 回：2015 年 4 月

目的：クレデンシャル詐取（Credential Theft）
概要：攻撃者に SDP クライアントのクレデンシャルとアプリケーションサーバーの情報を提供。クレデンシャルを詐取されても接続を防御できることを証明。

第 4 回：2016 年 3 月

目的：パブリッククラウドを使用した高可用性
概要：攻撃者に SDP の全てのコンポ―ネットの情報を提供。正規のユーザーのターゲットサーバーへのアクセスのフルキャプチャを提供。第 1 回の実証を複数のクラウド事業者と共同で実証。クラウド内のデータが安全に守られることを実証。

これまでは SDP の技術精度の向上と標準化を進めてまいりました。本 SDP 利用シナリオ集は、日本市場において SDP の有効性を理解していただくことを目的としており、海外での利用事例、CSA の SDP-WG メンバーによる想定シナリオをご紹介します。戦略的な SDP の活用方法を昨今のサイバーセキュリティ対策の参考にしていただけると幸いです。

1. SDP 利用概要

1-1 技術的な利用

認証手順

SDP を利用しない従来のクライアントからのアプリケーションサーバーへの接続では、接続後に、ID とパスワードでシステムにログインし、最後に多要素認証を行う流れとなります。

つまり、クライアントの信用性が確認される前にアプリケーションサーバーに接続されてしまうため、ネットワーク上のすべてのデバイスが外向きに公開されます。従って、最初の接続で、攻撃者はネットワークに入り込み、ネットワークをスキャンし、サーバーまたはそのいずれかのアプリケーションに脆弱性があるかを調べることができます。また、ログイン情報もモニタリングできるため、クレデンシャルを詐取することもできます。結果、攻撃者は、信頼性が確立される前に必要な情報を入手し、悪意をもった仕掛けを作ることができます。そこにセキュリティの脅威が発生する可能性があります。

SDP を利用した場合、アプリケーションサーバーとは別のところで、最初の多要素認証を行い、デバイスの信頼性を検証し、最後に信頼されたデバイス上の更に信頼できるユーザーのみが承認済みサーバーに接続できるようになります。そのため、この方法を使用することで、サーバーの悪用、クレデンシャル詐取、接続ハイジャックを防ぐことができるようになります。

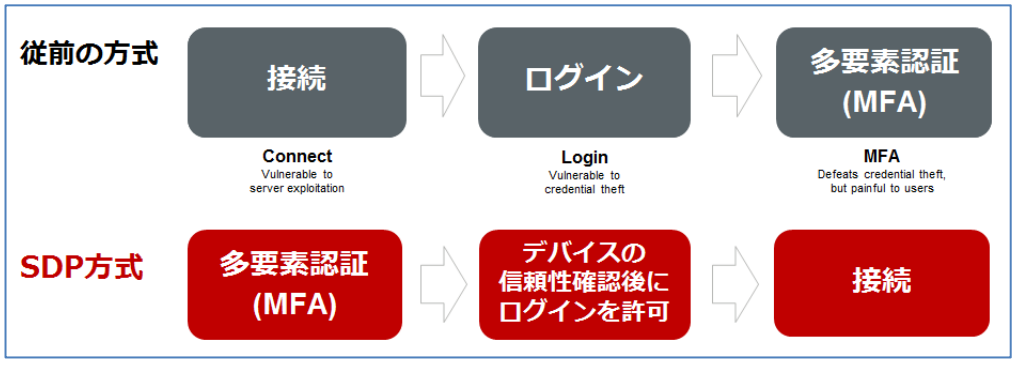

図 1: 認証手順の違い

接続手順

SDP では、クライアントが正当であることを事前認証するために SDP コントローラーを設置します。クライアントとコントローラーとの間で、事前に双方向 TLS の確立、デバイスの物理認証、ID とパスワードによるユーザー認証を組み合わせた多要素認証を行います。また、アプリケーションサーバー側に SDP ゲートウェイを置いて外部から見えなくします。これは Deny-All のファイアウォールと同じ考え方です。

その結果、信頼性が確認できた場合のみ、接続先のアプリケーションサーバーに接続依頼を伝達し、接続許可が得られた場合のみ、接続先の情報が SDP コントローラー経由でクライアントに伝えられ、SDP ゲートウェイとクライアントの間にダイナミックコネクションが確立されます。

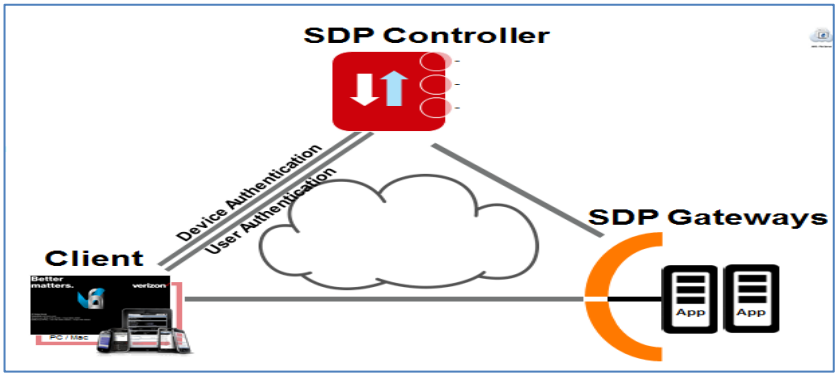

図 2: SDP の接続方式

これは、アプリケーションサーバー側のみを守るだけでなく、仮にアプリケーションサーバー側が何らの攻撃を受けていたり、脆弱性がある状態に陥り、クライアントからのアクセスを制限したい場合、SDP コントローラー側に情報を設定することで、対象となるアプリケーションサーバーへのアクセスを制限することができます。

情報・インフラの見えない化の実現技術（SPA とは）

SDP ではクライアントが認証・認可されるまで、いかなる接続も行われないように構成されており、インターネットとの境界線では、サービスが“Deny-All”で設計されています。また、SDP コントローラー側では SPA（Single Packet Authorization）を採用し、SPA パケット以外は攻撃とみなしてドロップさせます。SPA は RFC4226 ベースで規定されたコントローラー等への安全な接続方式です。

SPA のベースとなる考え方は Port-Knocking 方式です。これは、通常時はファイアウォールによって閉じられているポートを外部から密かに開く方法であり、予め決めておいた順番で閉じているポートを叩き、正しい順番のポートの“ノック”（接続試行）を受け取った時に、はじめてファイアウォールは特定のポートを開いて接続を許可するものです。

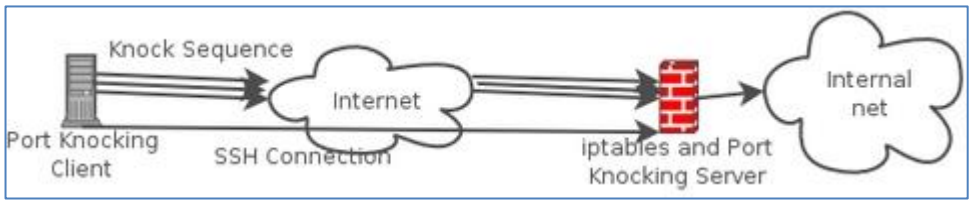

図 3: 従来の Port-Knocking 方式

しかしながら、従来の Port-Knocking は、リプレイ攻撃に弱い、悪意のある第三者によるノック・シーケンスの破壊に弱い、ノック・シーケンスは一連のパケットの流れになるので探索が可能である、との課題がありました。そこで、SPA では、これらの課題に取り組み、①パケット内に 16 バイトのランダム・データを挿入し同じパケットが来たらドロップする、②シングル・パケットにすることでスプーフィングだけでは攻撃できないようにする、③シングル・パケットにすることで解析を不可にする、ことを行いました。

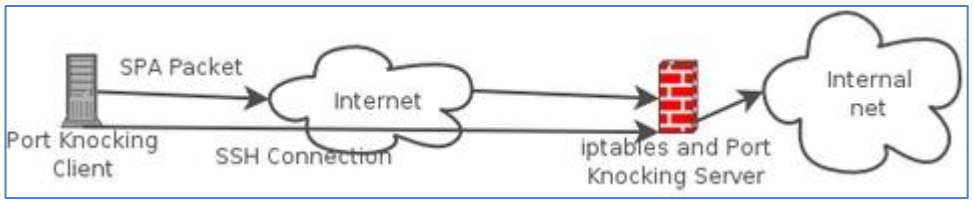

図 4: SPA 方式

これによって、SDP コントローラーを外部から安全に守ることができ、ポートスキャンを行っても空きポートを見つけることができず、DDoS 攻撃も最小化できることになります。

引用：https://www.linuxjournal.com/article/9565

実装可能端末

本技術の開発においては、複数の大手クラウド事業者、グローバルなネットワーク事業者、および利用者となるグローバル企業が関わりました。そのため、これらの機能が特別な装置を購入するのではなく、既に利用可能なクラウド、サーバー、PC、タブレット、スマートフォンおよび IoT 機器に実装できることに大きなメリットがあります。ただし、OT のエッジのデバイスによっては SDP のソフトウェアすらインプリできない可能性があります。特に工場内には様々な機器があり、構成も様々であることが考えられるため、SDP の適用前に現地調査の工程を踏むことが推奨されます。

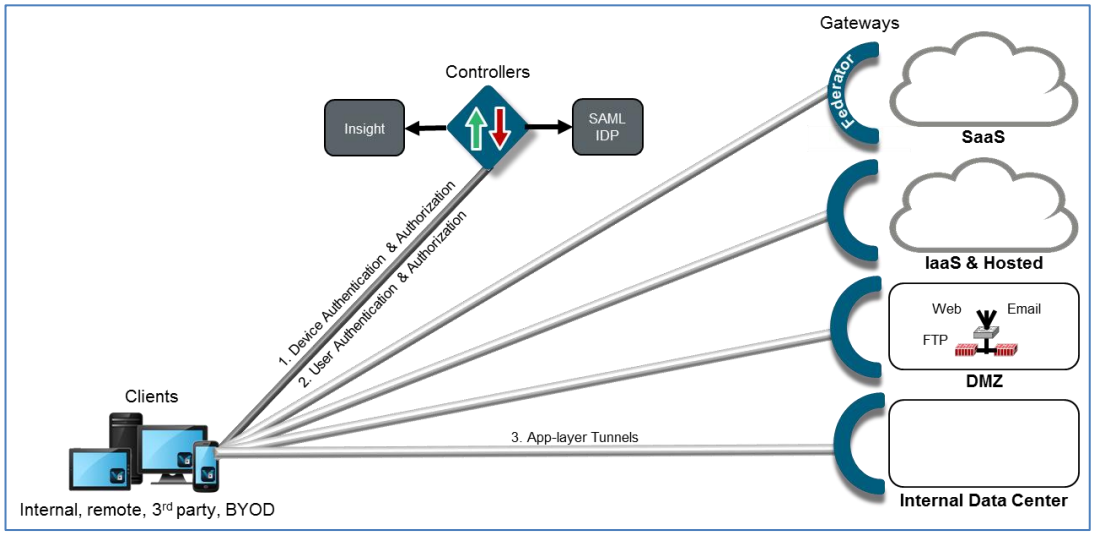

図 5: 様々な接続環境

＜ポイント＞

- インターネットからの隔離（境界線の確立）
- 独立した認証機能の確立
- 許可されたユーザーのみの接続
- 端末認証の実施
- ユーザーの認証後の接続許可の実施
- 動的な接続の提供

1-2 ビジネス的な利用

アプリケーションの共同利用

企業の業務システムは、自社のデータセンターに構築される時代からクラウドを有効活用する時代へ移行しています。そのため、ビジネスシーンとして、これらのクラウドへのアクセスを有効に利用したいという要望があります。また、社内メンバーの利用だけでなく、関係会社や委託会社のメンバーも同じアプリケーションを利用し、同じデータへアクセスするビジネスシーンが増加しています。これにより、クラウド内にある業務用アプリケーションやデータへ許可されたクライアントのみが、必要な時にアクセスをできることが期待されます。図 6：アクセス制御の例では、エグゼクティブ（Executive）だけがアクセスできるアプリケーションがありますが、一方で業務委託先（Third-Party）には 1 つのアプリケーションしか接続を許可しない状況を作り出しています。

このように、SDP を利用することで、自社内のユーザーだけでなく、グループ会社、関係会社、委託会社のユーザーが共同でサービスや情報を利用できる環境を、簡単に安全に構築できます。

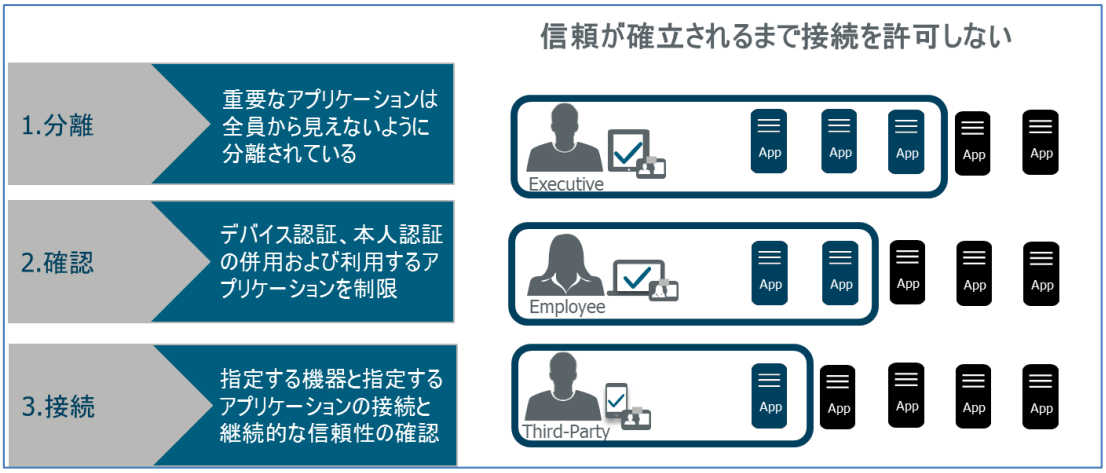

図 6: アクセス制御の例

リモートワーク

最近では、リモートワークを導入している企業の割合が増えてきており、大企業だけでなく中小企業やベンチャー企業でも、リモートワークを導入する傾向にあります。

リモートワークを実現するには、データセンターなどに認証用のリモートアクセスサーバーを準備し、様々なネットワーク機器やセキュリティ機器を経由したうえで、インターネット越しにあるクラウド上のアプリケーションサーバー等に接続する仕組みが必要となります。

現在のリモートアクセス用 VPN の課題

- 設定は IP アドレスでありユーザーではないのでセキュリティレベルが低い。
- ユーザーのトラフィックが必ず企業のネットワークを経由すると、クラウド上のアプリケーションやデータアクセスまでに複雑な構成となり遅延値も大きくなる。
- リモートアクセス用の VPN 機器障害など単一障害点となりやすい。
- 設定追加やセキュリティの維持のための定期的な設定変更に手間がかかる。
- ユーザーのデバイスからクラウドアクセス、企業ネットワークとの整合性などを考えると構成が複雑になる。

これらの課題からわかる通り、大企業ではその仕組みを安全に導入するために常に設備投資を行う必要があり、中小企業やベンチャー企業ではその投資ができないためにリモートワークを諦めてしまうところも少なくありません。

SDP は、これらのリモートワークを簡単な仕組みで安価に導入できるとして期待されています。また、SDP 技術を活用した場合、クラウドに直接、セキュアにアクセスすることが可能となるため、接続遅延を解消し、簡単な構成で、かつ安全な接続が可能となります。更に、必要な投資を低減しつつ安全にクラウドにアクセスができるようになり、また、全ての接続制御を簡単に変更することができるようになります。

＜ポイント＞

- 大企業：設備投資の軽減、拡張性の確保、運用の軽減、ネットワークの可視化
- 中小企業：設備投資の軽減、セキュリティ対策の実施

2. SDP 利用方法

2-1 クラウド接続における利用方法

基幹システムをクラウドに移行していく中で、どの企業においても、クラウドアクセスに対するセキュリティをどのように確保するか、が最も大きな懸念となります。従来は、レイヤ 3VPN、IPS/IDS、WAF といった、いわゆるトラディショナルなセキュリティアプライアンスによるソリューションで対応していました。しかし、この方法では、なりすましや中間者攻撃のリスクを排除することができません。また、運用面におけるコスト（ハード）、および管理面における人的コスト（ソフト）が大きな課題です。

SDP では、デバイスおよびユーザーの認証・認可のプロセスをまず行うことで、他者からの不正なクラウドアクセスを防ぎます。さらに、SDP において一元的に RBAC（Role Based Access Control）を実現できるため、ユーザーごとにアクセスポリシーに基づくクラウドアクセス制御が可能となります。また、これによりセキュリティアプライアンスの配置を見直しコストを削減できます。

2-2 IoT における利用方法

IoT デバイスがネットワークに接続する場合、これらのデバイスから情報を管理し、安全で信頼性の高い接続を提供する必要がありますが、現在のセキュリティアーキテクチャでは、様々なネットワーク攻撃にさらされる危険性があります。特に OT 環境においては、セキュリティ対策が十分に実施できないことを理由に、ネットワーク接続が切り離され独立していることも多くあります。しかしながら、より生産性を向上させるためには、AI や IT を利用した新技術の導入が必須となっており、結果、ネットワークに接続しないわけにはいかなくなってきています。

SDP の技術はソフトウェアベースであり、IoT や OT デバイスへの実装も容易となります。そのため、現在のセキュリティの課題を解決し、今後の IoT における幅広いビジネスシーンをサポートする技術として期待されています。ただし、OT のエッジのデバイスによっては SDP のソフトウェアすらインプリできない可能性があります。特に工場内には様々な機器があり、構成も様々であることが考えられます。そのため、SDP の適用前に現地調査の工程を踏むことが推奨されます。

＜適用領域事例＞

- プラント稼働状況のデータアップロード
- 都市の防災情報のデータアップロード
- テレマティクス（自動車）における新しい安全なサービスの実現
- 産業機器の稼働状況のデータアップロードおよび産業機器の制御

3. SDP を選択する理由

3-1 SDP を選択する理由

SDP には、強力なユーザー認証と RBAC（Role Based Access Control）に基づく認可のプロセスがあるため、内部外部問わず悪意ある者あるいはミスオペレーションによる資産へのアクセスを制御できます。また、認可された者のみが SDP ゲートウェイの IP アドレスを通知されるため、なりすましの脅威を排除します。更に、通信は双方向 TLS（Mutual TLS）によりセキュリティを確保し中間者攻撃などの不正を防ぎます。このような安全性の確保に加え、これまでは人手を介していたアクセス制御などのマニュアル作業を自動化できるため、運用稼働を下げることが可能となります。

これまでの事例より、SDP サービスを選択する主な理由は以下の通りとなります。

- **統合された多要素認証**：ユーザー認証およびデバイス認証を施すことでクレデンシャル詐取による不正アクセスを防ぎます。
- **サーバーの隔離**：SDP ゲートウェイにおいて認可されたユーザー以外のアクセスはすべて Deny にすることができるため、サーバーへのエクスプロイト攻撃を防ぎます。
- **堅牢なトンネル**：クライアントと SDP コントローラー間、およびクライアントと SDP ゲートウェイ間は Mutual TLS により安全な接続が確立されるため、中間者攻撃を防ぐことができます。
- **個別構築**：SDP コントローラーはユーザーごとに専用の VPC が構築されるため、データやアクセスの混在は発生しません。
- **サービスとしての利用**：SDP の各コンポーネント（SDP コントローラー、SDP ゲートウェイ、および SDP クライアント）はサービスとして提供されるため、ユーザーはハードウェアを購入する必要はなく、また構築のためのプロフェッショナルを整える必要はありません。
- **操作性の向上**：ユーザー端末が起動すると同時に SDP クライアントが自動起動するため、ユーザーエクスペリエンスを阻害しません。
- **可視化の実現**：専用の SDP ダッシュボードにより、ユーザー、利用端末、アプリケーションの挙動をリアルタイムに確認できます。

3-2 SDP への期待

SDP は AWS や Azure などのホスティングサービス上にコントローラーおよびゲートウェイを構築できるため、非常に短期間で実装できます。また、クライアントの配布はツールやアプリにより行われるため、ユーザーの負担を極小化することができます。そのため、昨今のビジネスサイクルの短縮に IT が対応することができ、ビジネス部門へ大きな貢献を果たすことができます。

4. SDP 活用事例

以下に SDP の活用事例を示します。これには想定される活用シナリオを含みます。

4-1 政府・行政

① シナリオ

政府機関の扱う機微情報は、個人のプライバシー情報から国家機密まで多岐に渡ります。そのため、外部からのアクセスだけでなく、内部からのアクセスにおいても、厳格に定められたセキュリティポリシーに基づき、適正な権限を付与された者だけが必要な情報にアクセスできるようにコントロールされなければなりません。しかしながら、多数の省庁が利用する政府機関のネットワークは複雑化し、それに伴いセキュリティ機器が増大し、NAC（Network Access Control）を随時適切に遂行することが困難になってきています。

② SDP 利用例

SDP では、SDP コントローラーにより一元的に RBAC（Role Based Access Control）を実現できます。そのため、各省庁や各組織単位、さらに各役職（Role）単位に細かく定められたセキュリティポリシーであっても、容易に運用可能です。それにより、機密レベルに応じた適切なアクセスコントロールを行うことがでます。さらに、SDP の導入によりセキュリティ機器を削減でき、複雑化したネットワークを整理することにより、運用管理コストの削減および潜在的な脆弱性を最小化できます。

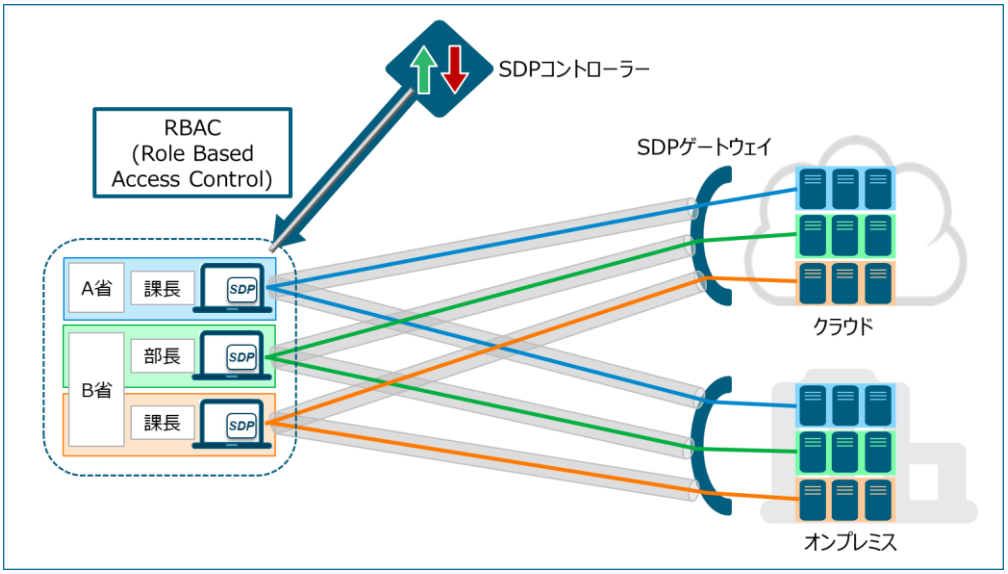

図 7: SDP 活用事例（政府・行政）

4-2 製造業

① シナリオ

A 社は海外に生産拠点を多くもつ製造業です。これまで自社運用のデータセンターにおいてオンプレミスでデータを管理し、設計データなどの機密情報を海外拠点に共有する際には、キャリアの専用線を利用して情報の転送を行ってきました。しかしながら、近年、設計データが大容量化し、既存の専用線帯域では転送が難しくなっています。コスト削減圧力が強まっている現状では回線帯域の増強は難しいため、インターネット経由でクラウドによるデータ共有を検討しています。ただ、機密情報をインターネットおよびクラウドにのせることにはセキュリティ面で懸念を抱いています。

② SDP 利用例

SDP では、まず多要素認証方式によりユーザー認証が行われ、適切なユーザーにクラウド上のデータへのアクセスが認可されます。ユーザーは認可されるまでは SDP ゲートウェイの IP アドレスにアクセスできないため、認可されていない者はクラウド上のデータへアクセスする術がありません。更に、通信経路のセキュリティは Mutual TLS により確保されます。

A 社は、SDP を利用することで、インターネット通信を利用して回線コストを抑制しつつ、大容量データをクラウドにて安全に共有することができました。

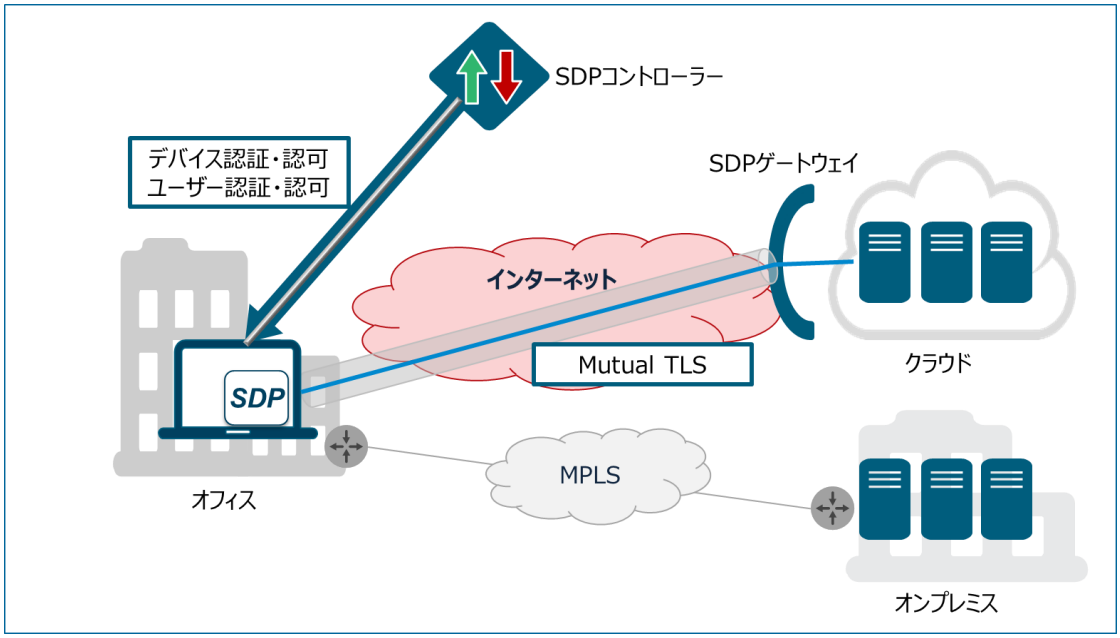

図 8: SDP 活用事例（製造業）

4-3 金融業

① シナリオ

2014 年の NISA 開始以降、2016 年にジュニア NISA が、2018 年にはつみたて NISA が開始となり、若い世代に対しても金融投資のハードルが低くなってきています。業界中堅の B 証券は、これまで中高年顧客向けの窓口サービスに注力してきましたが、若者にもターゲットを広げるため、スマートフォンを含むオンラインサービスを拡充するつもりです。しかし、セキュアなオンライン取引を実現するための設備投資やその運用コストが膨らむうえ、計画から実装までのリードタイムが長く、その間に先行するネット証券や大手証券に潜在顧客を奪われる懸念があります。

② SDP 利用例

SDP に必要なコンポーネントは、SDP コントローラー、SDP ゲートウェイ、SDP クライアントの 3 点です。このうち、コントローラーとゲートウェイは AWS や Azure といったホスティングサービス上に構築されます。また、クライアントはソフトウェア配布ツールにより自動配布されるほか、スマートフォンへはアプリのインストールにより配布されます。

B 証券は、SDP を利用することで、必要な様々な設備を整え運用管理を行う従来のセキュリティ環境を構築する場合に比較し、非常に低コストかつ迅速にセキュアなオンライン環境を構築でき、他社に先行して新規顧客、特に若い世代を獲得することができました。

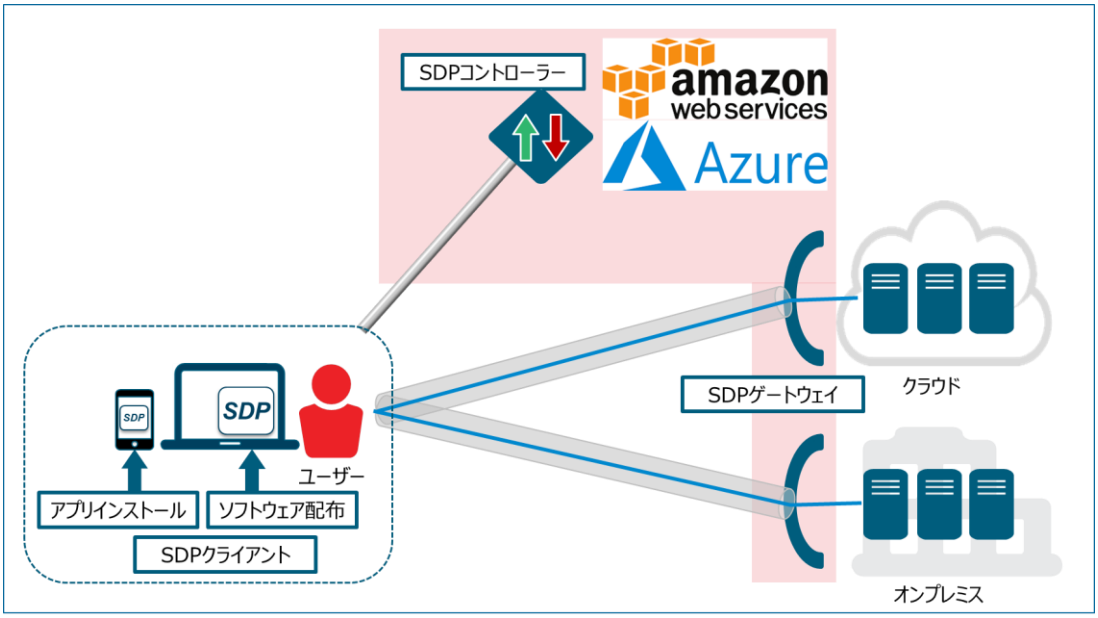

図 9: SDP 活用事例（金融業）

4-4 流通業

① シナリオ

アパレル業の C カンパニーでは、バイヤーが海外の各地に赴き素材の買い付けを行っています。商談に必要なデータにアクセスするには各地のブランチオフィスから本社へ接続していますが、商談のたびに遠方の外出先からブランチオフィスへ戻らなければいけないことに不満が出ています。一方国内では、幅広い世代のデザイナーやパタンナーが働いていますが、昨今の働き方改革の流れから、家事や育児、介護との両立を望む声が高まっています。C カンパニーでは、海外および国内において、時間や場所を問わず働ける環境の構築が急務となっています。

② SDP 利用例

SDP は最新のセキュアリモートアクセスサービスです。ユーザーは多要素認証による認可を得て初めて SDP ゲートウェイの IP を知らされます。万一クレデンシャルを詐取されたとしても多要素認証により認可を受けることができません。そのため、リモートアクセスにおいて、認証・認可から実際の接続までがすべてセキュアに行われます。また、ユーザーは自身の端末（PC、タブレット、スマートフォン）に SDP クライアントをインストールするか自動でインストールされることで、すぐに SDP を利用することができるため、ユーザーエクスペリエンスが損なわれることはありません。

C カンパニーは、SDP を利用することで、海外のバイヤーの生産性を高め、また国内従業員の満足度を高めることができました。

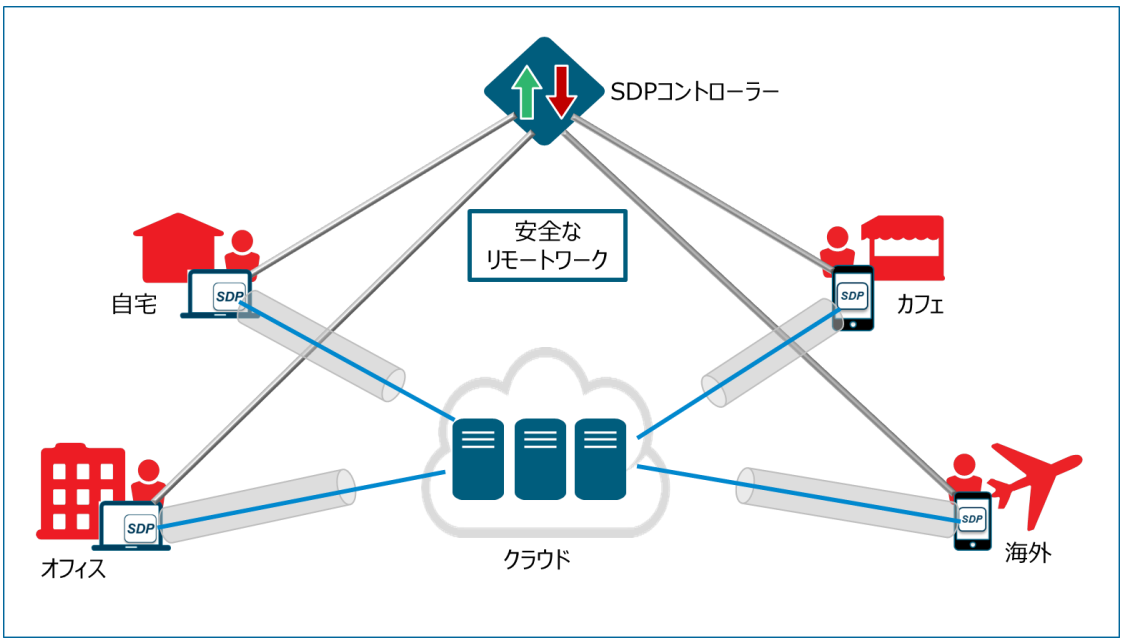

図 10: SDP 活用事例（流通業）

4-5 商社

① シナリオ

D 商社は国内海外あわせ 100 社以上の関係会社およびパートナー会社を抱えています。各社は D 商社の様々なアプリケーションサーバーやデータベースにアクセスしますが、各社が必要なリソースにのみアクセスできる（不必要なリソースにはアクセスできない）セキュアな環境を整備し、不正なデータ流出を防がなければなりません。現状の NAC（Network Access Control）の環境ではその整備が追い付いていない状況となっています。

② SDP 利用例

SDP では、保護対象の資産がインターネット上であれイントラネット上であれ、コントローラーによる認証・認可によって RBAC（Role Based Access Control）を行い、完全にセキュアなセグメンテーション化を実現できます。また、ポータルサイトによりユーザー、デバイスおよび通信がすべて可視化されるため、接続状況をリアルタイムに把握することができます。

D 商社は、SDP を利用することで、多数の関係会社およびパートナーの自社資産へのアクセスを容易にかつ安全に管理することができました。

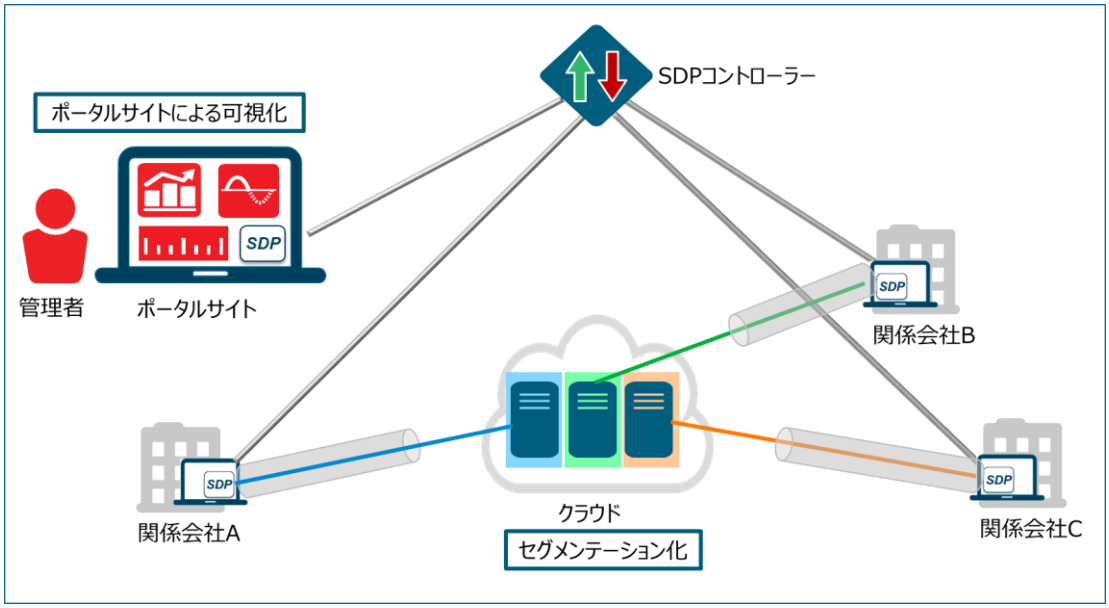

図 11: SDP 活用事例（商社）

4-6 電気・ガス事業

① シナリオ

E ガス会社はヨーロッパでガス事業を展開しており、安全で革新的なサービスを提供していると評判な会社です。しかし、様々な新サービスを提供するにあたり、マルチセグメンテーションを実施するには多大な CAPEX 投資が必要でした。また、クラウドを利用した検針用のシステム構築では、オンプレとクラウドの両方を利用したハイブリッド環境の導入を検討していますが、予算を十分に確保できない状況でした。

② SDP 利用例

E ガス会社では、SDP の導入によって、様々な端末から安全なアクセスを実施できるようになり、各家庭や企業からのガス設備情報を安全にオンプレとクラウドの両方に転送することを、想定予算の範囲内での設備構築により実現できました。

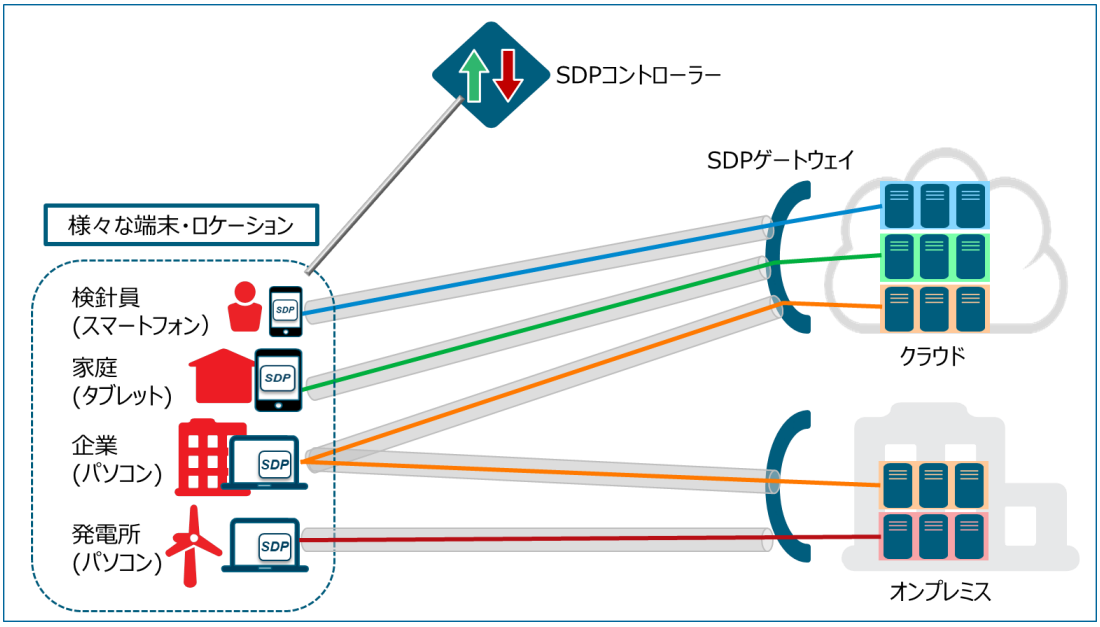

図 12: SDP 活用事例（電気・ガス事業）

4-7 不動産業

① シナリオ

F 不動産会社は米国にて不動産業を展開していますが、事業においては、不動産事業の販売に関わる情報が、ビジネス上最も重要な情報として扱われています。その情報に、オフィス、リモート（現場）、パートナー不動産会社、契約社員からアクセスが行われており、そのセキュリティ対策が急務となっています。また、企業ブランドの確保も重要であり、お客様情報の漏洩などが発生した場合にはビジネスに重大な影響を与える懸念があります。

② SDP 利用例

F 不動産会社は、静的なセキュリティソリューション（Firewall、NAC 等）は、コストが高く、扱いにくく、また最新のマルウェアからリスクの高いアプリケーションを守るのには十分ではない、と判断しています。

SDP の技術をオンプレ、IaaS、SaaS に適用し、進化したサイバー脅威（最新のマルウェア、クレデンシャル詐取等）からの保護に向けた対策を実施しました。

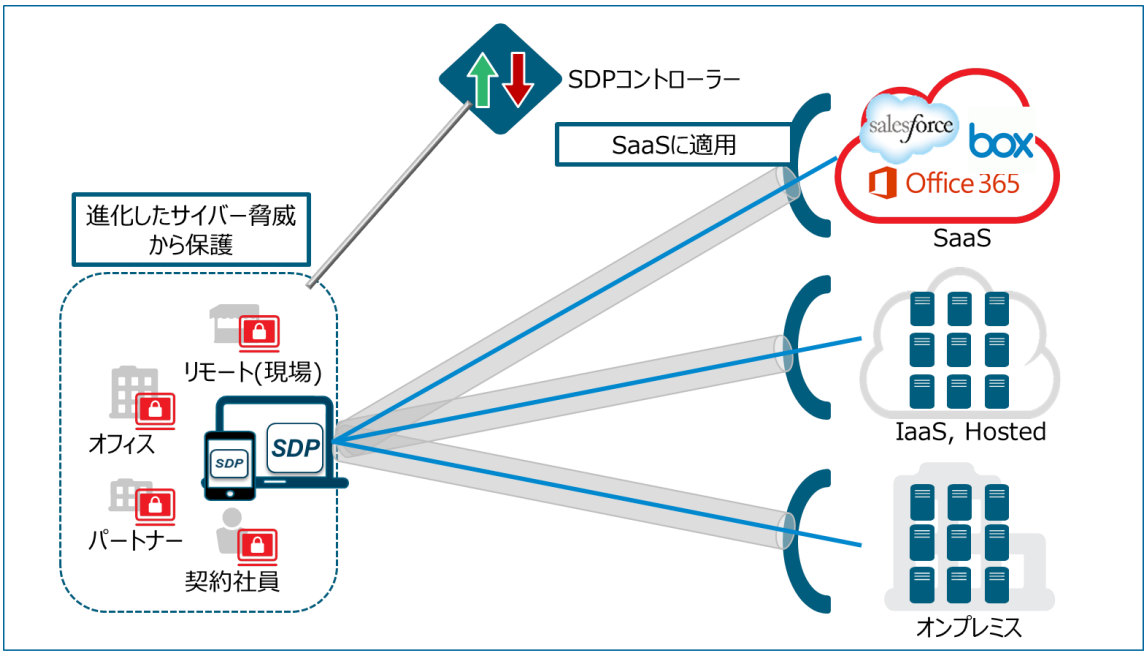

図 13: SDP 活用事例（不動産業）

4-8 医療事業

① シナリオ

G 社は多国籍ヘルスケア複合企業であり、複数のビジネス部門を持っています。ビジネスにおいては、その複数のビジネス部門が連携した業務が多く、情報の取り扱いには細心の注意が必要な状況です。また、人事異動、組織変更にも素早く対応しなければなりません。グローバルでの悪意あるマルウェアの脅威を防ぐために、セキュリティチームは膨大な数のファイアウォールの導入、マルチ VLAN の構築を実施しましたが、依然として発生する多くの攻撃に重大な懸念を抱いています。

② SDP 利用例

G 社では、SDP を利用したゼロ・トラスト・ゾーンの構築による論理セグメント分割を実施しました。ユーザーとアプリケーション間の接続においては、承認された機器からのみアクセス可能な制限を付ける方法としました。これにより外部からのアプリケーション攻撃を排除することができました。

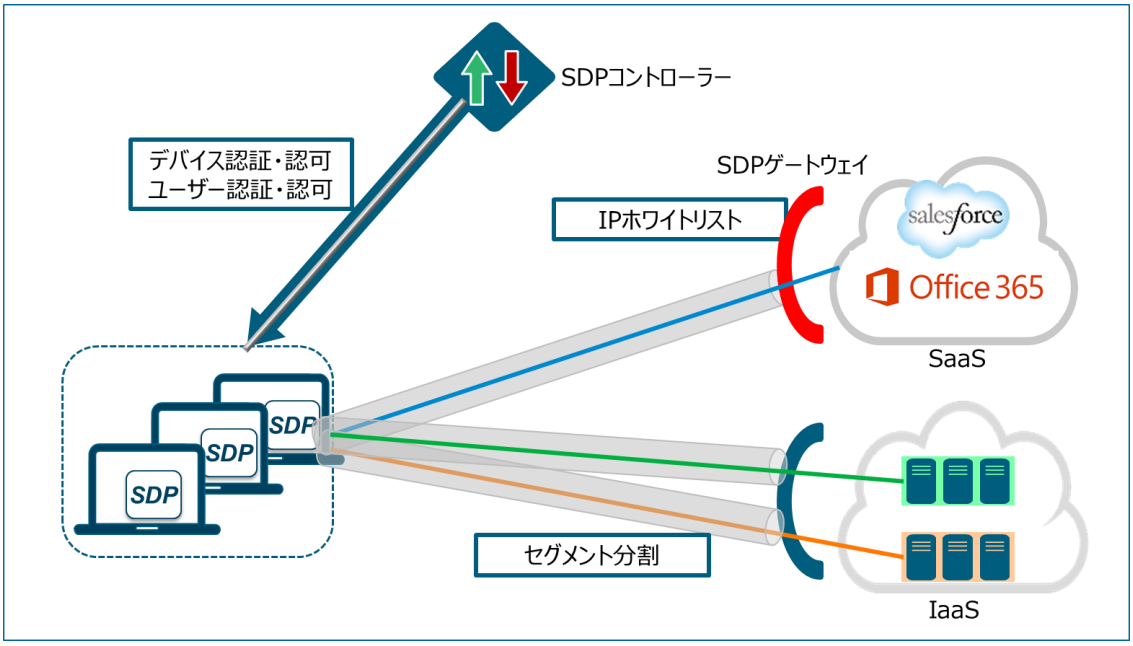

図 14: SDP 活用事例（医療事業）

4-9 学術公共

① シナリオ

K 大学は複数キャンパスを有する大学であり、各キャンパスには多数の学生のみならず複数の業務関連システムが存在しています。セキュリティを守る必要性はもちろんありますが、大学という性格上、一方では自由な学術的研究を促進するため、ある程度自由で融通の利く通信インフラが求められています。また、過去の経緯から学内(内部)で利用しているアドレスとして Global IP が付与されております。これにより、境界セキュリティとしてファイアウォールが導入されていたとしても、潜在的には学外(外部)から学内(内部)への到達が懸念される状態でもあります。また、一般企業のように Windows ドメイン統合による管理が難しい状態です。

② SDP 利用例

K 大学においては、学内(内部)ネットワークのセキュリティを高めるため、NAC やインターナル FW 導入を検討しましたが、自由度が大幅に下がること、また、単一メーカー単一システムへの囲い込みによりシステムリプレースの自由度が下がる懸念から、断念していました。そこで、ゼロトラストの概念を持つ SDP を導入し、学内/学内を問わず、全てを信頼しない事を原則とし、守るべきリソースを明確に定義し境界防御する構成としました。これにより、保護されたリソースへアクセスする場合には、学内/学外を問わず適切な権限を有した認可ユーザーのみに制限した上で、自由で融通の利く構成が維持できました。そして、それらが SDP の有する一元的なログ監視/保存により、証跡監査が可能となりました。また、スイッチやファイアウォールなどのメーカーに依存しない状況となり、リプレースの自由度も向上しました。

SDP が備える多要素認証（MFA）、例えばワンタイムパスワード（OTP）を用いる事で、Windows ドメインなどディレクトリとの連動を伴わずにユーザーアカウントのセキュリティを高めることが可能になり、クレデンシャル詐取への対処も同時に実現出来ました。

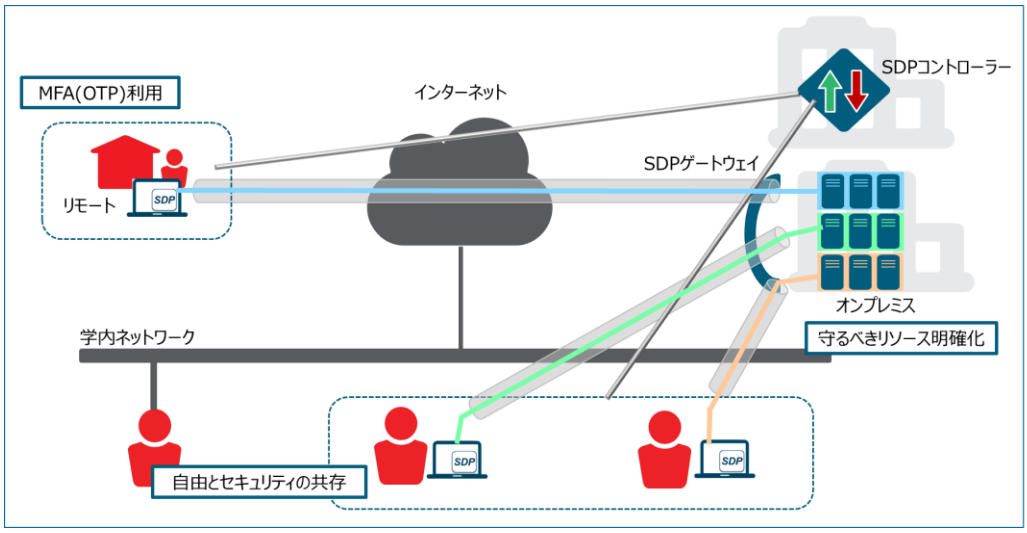

図 15: SDP 活用事例（学術公共）

4-10 マルチクラウド

① シナリオ

T 株式会社は、国内に複数の拠点を持つ企業です。これまでは本社およびデータセンターに各種サーバーを設置し、各拠点を閉域網で接続することで、いわば安全な社内 LAN に設置してある社内向けサービスを提供してきました。しかしながら、昨今のクラウドシフトにより、各機能を Public クラウド,Public SaaS や、クラウドに借り受けた Private クラウドにシステムを設置するなどのシフトが進んできています。回線についても今までは通信キャリアによるキャリア VPN を使用してきましたが、コスト削減を追求し、VPN 装置による暗号化通信にシフトしています。これにより、リソースが分散したことにより複数の VPN 装置を導入する事となり、また、通信制御を複数装置で実施する必要性や、通信設計の確認を広範囲に実施する手間があります。複数メーカーの VPN 装置の対応、ハードウェアアプライアンス、仮想アプライアンスと形態の異なる装置の保守運用、また、特に通信の一貫性を保つ事、何がどこで発生しているのかの証跡監査が困難な状態となっています。そして、Public SaaS はインターネットに存在し社内 LAN と同様の制御が難しくなりました。

② SDP 利用例

SDP はソフトウェア製品であり、ゲートウェイを各種クラウドに配置することで単一製品による一貫した通信制御が可能となりました。Private クラウドのみならず、Public クラウド、Public SaaS にも対応するため、会社からの接続のみならず、働き方改革に伴う会社外からの制御にも一貫した対応が可能となりました。また、SDP コントローラーが設定を保持しており、SDP ゲートウェイはコントローラーと接続する方法についての最小限設定しか持たない SDP の性質を活かし、クラウドベンダが変更になったケースや、アドレスが変更になった場合でも容易にも追従できる状態となりました。LAN 間 VPN 時ではネットワーク単位で許可していたルーティング制御から、ユーザーとリソースごとのセグメントオブワンの制御による、ルーティングレベルでの 1 対 1 接続構成となり、セキュリティの向上も図る事ができました。

また、通信状況を一元的に保管する事が可能となり、容易な証跡保管/監査を実施できました。ISMS やプライバシーマークの監査対応も容易となりました。

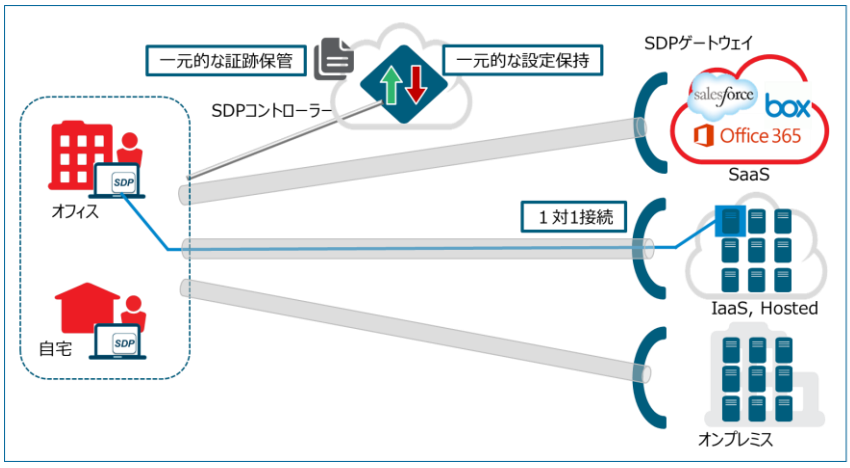

図 16: SDP 活用事例（マルチクラウド）

おわりに

本 SDP 利用シナリオ集では、SDP の技術的な検証について述べるのではなく、その有効性について、シナリオ、利用事例を用いて説明してまいりました。

SDP の利用の仕方、導入方法については、各企業によって千差万別です。多くの事例を知ることで、SDP の活用について理解を深めていただき、今後のサイバーセキュリティ対策の参考にしていただければ幸いです。