ソフトバンク株式会社

「業務」を軸にアクセスを制御
複数PCの使い分けを解消し社内LAN運用を変革

セキュリティ要件から業務ごとに PC を使い分けていたソフトバンクの社内 LAN。複数 PC の運用負荷や持ち歩きの負担を軽減するため、同社は Cisco ISE を導入し、Cisco TrustSec を実装しました。IP アドレスではなく「業務」に基づくアクセス制御へと転換し、既存基盤を活かしながら利便性と運用効率を高めています。

ソフトバンク株式会社

本社所在地
東京都港区海岸一丁目 7 番 1 号

設立
1986 年（昭和 61 年）12 月 9 日

従業員数
単体：18,895 人（2025 年 3 月 31 日現在）
連結：55,070 人（2025 年 3 月 31 日現在）

モバイル通信事業を中心に、固定通信やインターネットサービスを展開する総合通信事業者のソフトバンク。近年は、これらの通信基盤を生かし、クラウド、セキュリティ、IoT（Internet of Things）、AI などの先端分野でも企業向け ICT ソリューションを提供し、企業や社会のデジタル変革を支えています。

課題

- セキュリティ要件により、業務内容ごとに PC を使い分ける必要があった
- PC の使い分けは台数の増加にもつながり OS などのライセンスコストが増大していた
- ACL によるアクセス制御では更新作業が多く、運用面での負担が大きかった

ソリューション

- Cisco ISE を導入し Cisco TrustSec を実装。ACL ではなく業務を軸にしたアクセス制御へ移行
- 既存のネットワーク機器を活かし、最小限の投資で課題を解決
- 技術的な課題をシスコと協力して解決し、VDI にも Cisco TrustSec を適用

結果

- PC の使い分けが不要となり、複数 PC を持ち歩く負担が大幅に軽減
- ライセンスや VPN 設定など端末運用に関わるコストが削減
- シンプルな運用が実現し、アクセス制御の管理工数を大幅に縮減

今後

- ゼロトラストセキュリティの実現に向けて、SASE との連携などを検討
- オンプレミス機器のクラウド化によってさらなる運用管理負荷を軽減

長年の課題だった複数PC運用の煩雑さと負担を解消できました

前田 高尚（たか より） 氏

ソフトバンク株式会社
テクノロジーユニット統括 共通プラットフォーム開発本部
IT&AI クラウド開発統括部 ネットワーク開発部
部長

課題

社内 LAN の課題だった PC 使い分けの手間

ソフトバンクの IT&AI クラウド開発統括部 ネットワーク開発部は、AI の能力を最大限に活かすために設計した AI インフラ向けネットワーク、プライベートクラウドを支えるデータセンターネットワークなど、同社の事業を支える重要なネットワークの構築と運用を担っています。例えば、ソフトバンクの AI インフラは、国際スーパーコンピューティング会議 SC25 で発表された TOP500 ランキングに入っており、現地でも高い関心を集めました。

社内 LAN も同部門が構築し、運用しているネットワークの 1 つです。約 2 万人の従業員が日々利用する業務基盤として、性能、安定性、運用性を考慮した設計となっています。セキュリティの観点では、ファイアウォールの適切な設置などに加え、情報の機密性に応じてネットワークを物理的に 3 つに区分。IP アドレスに基づく ACL（Access Control List）制御で許可されたデバイスのみが各ネットワークにアクセスできるようにしています。「区分間の通信も原則として許可しない方針です」とソフトバンクの前田 高尚氏は言います。

しかし、この構成はセキュリティの強化にはつながりますが、利便性の面では課題がありました。業務上、複数のネットワークにアクセスする必要がある従業員は、PC を複数台持ち歩き、VDI（Virtual Desktop Infrastructure）を含めて使い分けなければならないからです。

「業務ごとに利用するネットワークやシステムが異なるため、一部の従業員は 2 台以上の PC を使い分ける必要がありました。その使い分けの手間や複数の PC を持ち歩く負担が大きいという声が上がっていました」と同社の澁谷 広軌氏は話します。

また、複数 PC の運用は OS やアプリケーション、セキュリティソフトのライセンスコストの増大、PC ごとの VPN 設定といった運用管理負荷の増大にもつながるため、コストや運用面でも課題となっていました。

既存ネットワークを活かして課題を解決できる

ソリューション

業務内容に応じてネットワークアクセスを制御

利用者だけでなく管理側の負担も小さくありませんでした。2 万人規模の環境での ACL の運用は、人事異動やレイアウト変更の度に大量のリストを更新しなければならないからです。そこで、同社は PC を使い分けずとも、従業員が必要なネットワークにだけアクセスできる仕組みの実現を目指しました。

まず模索したのが SASE（Secure Access Service Edge）による解決策です。インターネットアクセスやリモートアクセスを制御する SASE と連動させ、社内 LAN のアクセスも制御できないかと考えたのです。「実現が不可能というわけではありませんでしたが、SASE 側で社内 LAN へのアクセス制御まで一元化しようとすると、VPN やプロキシサーバーといった既存のネットワーク要素や、セキュリティアーキテクチャ全体の再設計が必要になります。導入コストも相応に大きくなるため、複数 PC の使い分けを解消するという今回の目的とはスコープが異なると判断しました」と同社の西村 優氏は話します。

こうした検討を経て、ソフトバンクが着目したのがデバイスではなく「業務」に基づいてアクセス制御を行う方法です。業務内容や役割を識別子として扱い、従業員が業務を切り替えた際、その情報がネットワーク側の属性として自動的に切り替わるようにすれば、1 台の PC で複数の業務ネットワークにアクセスでき、PC を使い分ける必要がなくなるからです。

それを実現する仕組みとして選んだのがシスコの Cisco TrustSec です。

Cisco TrustSec は、デバイス証明書や IP アドレスではなく、SGT（Security Group Tag）というタグでアクセス制御を

行う仕組みです。ソフトバンクの場合なら、従業員の業務内容や役割などを属性としてタグに設定すれば、同社が構想する「業務」によるアクセス制御を実現できます。「既存のネットワークを活かしながら導入できる点も大きな利点でした。すでに当社は、ネットワークスイッチにCatalyst 9000シリーズ、ファイアウォールのCisco Secure Firewallを利用しており、認証基盤としてCisco ISE（Cisco Identity Services Engine）を追加すればCisco TrustSecを実装できました。最小限の初期投資で、長年の課題であった複数PCの使い分けを解消できたのです」と西村氏は言います。

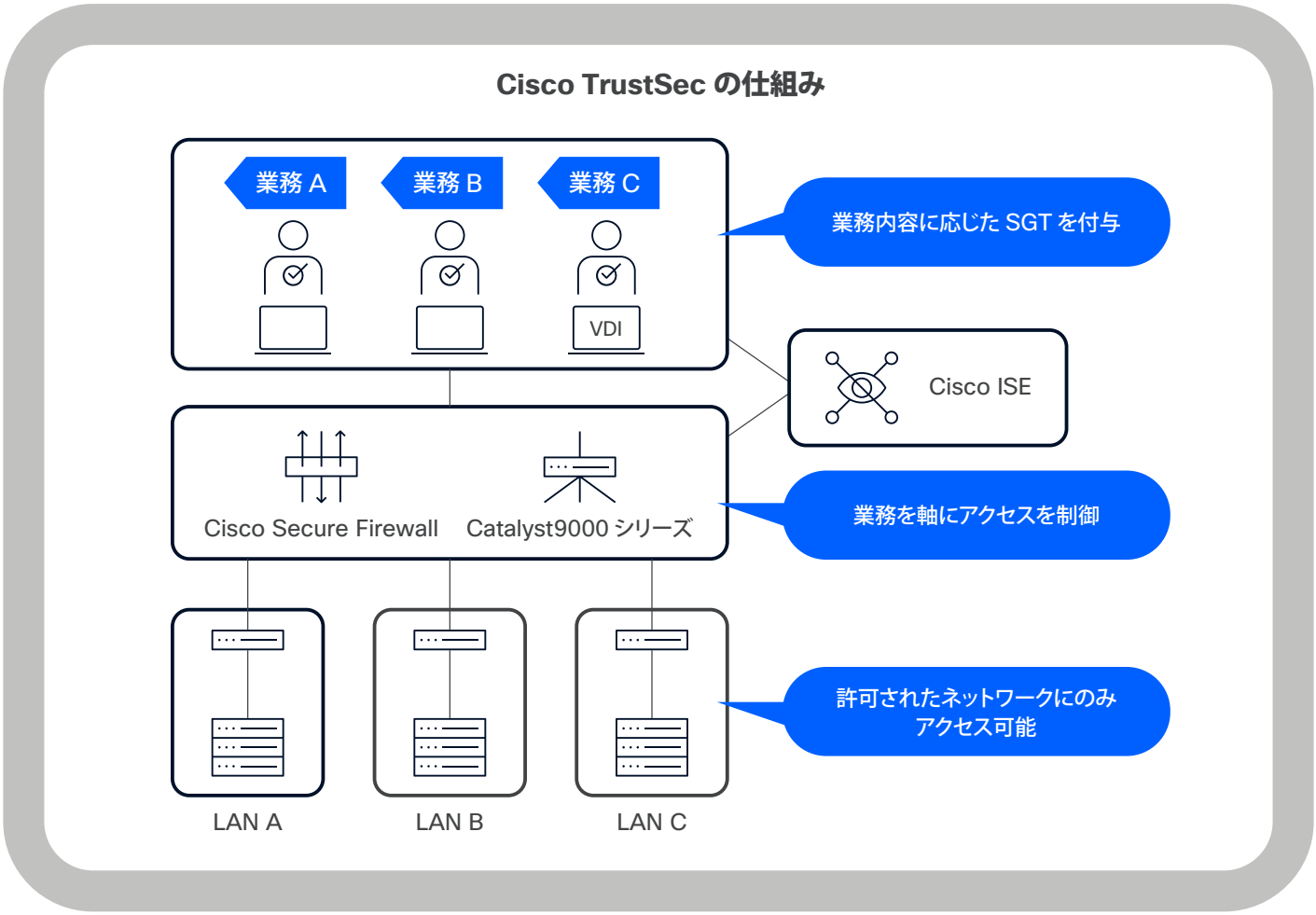
結果～今後

PC使い分けの手間、コスト、運用管理負荷を軽減

アクセス制御はネットワーク部門だけでなく、デバイス部門、セキュリティ部門などにも関係する領域となります。そのため同社のCisco TrustSecの導入は部門横断のプロジェクトとして進められました。

「一斉導入ではなく段階的に導入を進めていますが、導入を終えた従業員は業務に応じてPCを使い分ける手間から解放されています。ネットワーク区分によってはVDIを使うポリシーとなっていますが、他の業務で利用しているPCからVDIにログインし、最初の画面で行う業務を選択する仕組みにしています。オフィスに出社していなければ行えない業務の場合は、入館記録とも連携して認証を行います。この仕組みによって、従来のように複数PCを持ち歩く必要はなくなり、業務もシンプルになったと好評です」と前田氏は話します。

PCの使い分けが不要になり、PC台数が削減されれば、当然OSやアプリケーション、セキュリティソフトのライセ



ンスコストや運用管理負荷の削減にもつながります。「デバイスごとの VPN 設定といった作業も減ります。導入範囲が広がるにつれて、このようなメリットは大きくなるはずです」と澁谷氏は言います。

SGT の運用は想像していた以上にシンプルだと西村氏は言います。「Active Directory と連携させて業務グループにタグを割り当てるだけで、IP アドレスを管理したり、大量のルールを記述したりする必要はありません。従業員の異動や組織再編があっても、個人の業務が変わらなければタグを更新する必要もなく、長い目で見ると、かなりの運用工数を削減できると考えています」。

導入時には、いくつかの技術的な課題に直面しましたが、シスコおよびシスコのパートナーと協力しながら克服しました。例えば、一部の部門は独自に構築したネットワークを運用しており、そこへのアクセスも同じ PC からアクセスしたいというニーズが浮上しました。「そのような独自ネットワークはアドレス体系までは考慮されておらず、社内 LAN とアドレスが重複しているものもありましたが、タグベースのルーティングで対応できました」（西村氏）。

また、VDI への Cisco TrustSec の適用は、ほとんど事例がなかったことから、同社もシスコも慎重に臨みました。「途中、特定の条件下でゲートウェイへの ARP（Address Resolution Protocol）要求が発生せず、802.1X 認証後の通信が開始できない事象が発生しましたが、スイッチ側の認証関連設定の調整で解決しました。物理 PC だけでなく VDI にも Cisco TrustSec を適用することは今回のプロジェクトの前提条件ですから、VDI でも安定して動作することが確認でき、ほっと胸をなで下ろしました」と西村氏は続けます。

次の大きなテーマはゼロトラストへの移行

PC 使い分けの課題を解消したソフトバンクの社内 LAN において、次の検討テーマとなるのがゼロトラストセキュリティへの移行です。前述のとおり、ゼロトラストは今回のプロジェクトではスコープ外でしたが、ネットワークやセキュリティの将来像を考える上で避けて通れないテーマだと同社は捉えています。

ソフトバンク株式会社
テクノロジーユニット統括 共通プラットフォーム開発本部
IT&AI クラウド開発統括部 ネットワーク開発部
部長
前田 高尚 氏

ソフトバンク株式会社
テクノロジーユニット統括 共通プラットフォーム開発本部
IT&AI クラウド開発統括部 ネットワーク開発部
エンタープライズネットワーク課
課長
澁谷 広軌 氏

ソフトバンク株式会社
テクノロジーユニット統括 共通プラットフォーム開発本部
IT&AI クラウド開発統括部 ネットワーク開発部
エンタープライズネットワーク課
担当課長
西村 優 氏

インターネットアクセスを制御するSASEは、ゼロトラストを実現するための重要な技術です。複数の選択肢がありますが、シスコのSASEソリューションであるCisco Secure Accessも有力な選択肢となります。Cisco Secure Accessを利用すれば、Cisco TrustSecで設定したSGTを社外からのアクセスやクラウドサービスの利用、インターネットアクセスの制御にも応用できるからです。さらにユーザーやデバイスのセキュリティ状況に応じて割り当てるSGTを変更することで、アイデンティティセキュリティの観点でも効果的な施策となる可能性があります。「Cisco TrustSecとCisco Secure Accessの組み合わせであれば、SGTのメリットを最大限に引き出すことができると考えています」と西村氏は話します。

認証やアクセス制御の仕組みをクラウド側に集約できれば、従来運用してきたVPN、プロキシ、認証サーバーといったオンプレミス機器を段階的に削減することも可能。運用管理負荷の軽減に加え、EoS（End of Sales）対応から解放される点も大きなメリットです。「社内LANをどのように進化させるかは常に重要なテーマです。具体的な検討はこれからですが、シスコからのよい提案を期待しています」と前田氏は続けます。

Cisco TrustSecによる業務を軸にしたアクセス制御の実現によって利用者の利便性と運用効率化を両立した同社は、さらに長期的な視点で社内LAN全体の最適化を進めていく考えです。

SoftBank

移動通信サービスを中心に、固定通信、インターネット、クラウド、IoTなど多様なICTサービスを提供する通信事業者。AIをはじめとする先端技術を活用した新たなサービスの創出や企業のデジタル化支援にも注力している。
URL https://www.softbank.jp/

製品 & サービス

- Cisco TrustSec
- Cisco ISE
- Catalyst 9000シリーズ
- Cisco Secure Firewall

2601-1-AS