ICT 特集

ゼロトラストのはじめ方

ネットワーク＆セキュリティの新潮流「ゼロトラスト」にどう取り組むべきか
経営者やIT担当者が抱える課題や悩みを解決するための道筋を描く

Contents　会報Family VOL.407

会報編集部では、読者の皆様からのご意見をいただきたくアンケート調査を実施いたします。
ご協力お願いします。

1 第1部 Commentary ｜ エキスパートが解説する「ゼロトラスト」最新事情

「ゼロトラスト」とは何か、どこからアプローチするか

テレワークの普及やクラウド化の進展、サイバー攻撃の増加など、企業を取り巻くネットワーク環境が大きく変化する中、外部と内部を切り分ける「境界防御型」のセキュリティから、すべての信頼性をゼロベースで検証する「ゼロトラスト」への転換が求められています。今回の特集では、ゼロトラストについて検討したい、理解を深めたいという経営者やIT担当者に向けて、富士通と技術パートナーであるパロアルトネットワークス様、両社の担当者による対談をお届けします。

1-1 なぜ今、「ゼロトラスト」が求められるのか

林　近年、企業内のネットワークやセキュリティを検討する上で、「ゼロトラスト」が重要なキーワードとなっています。特に国内では、この3年間のコロナ禍でテレワークが拡大したことが大きなきっかけになったと感じています。セキュリティ対策を施された社内環境だけでなく、自宅などテレワーク環境から社内システムにアクセスする機会が増える中で、いかに安全性を維持するかが緊急課題となったことで、多くの企業が一斉に「ゼロトラスト」を検討し始めました。

染谷　短期的に見れば、コロナ禍が大きな要因であることは間違いありませんが、もう少し長期的に見れば、その背景には2つの潮流があると思います。1つは、企業におけるITインフラの変化。これまでは社内で完結していたネットワークが、グローバル化によって海外のグループ企業、さらにはサプライチェーン各社とも接続されるようになりました。加えて、IoTの浸透によってネットワークにつながる端末数が急増。さらにオンプレミスからクラウドへの変化やSaaS利用の拡大、そこにテレワークの普及が加わったことで、社内／社外という明確な境目がなくなり、ありとあらゆるものがネットワークにつながる社会が到来しました。

林　従来のように「安全な社内」と「危険な社外」を区分けし、その境界で防御するという考え方が通用しなくなり、ネットワークにつながるあらゆる端末、あらゆるトラフィックを対象に、その信頼性をゼロベースで検証する「ゼロトラスト」という考え方が生まれたわけですが、この数年で国内企業での認識も広まってきました（図1）。

染谷　もう1つの潮流が、その結果としてのリスクの増大です。以前はメールやWeb経由でのサイバー攻撃が主流でしたが、ネットワークの接続先が拡大したことで外部からの侵入経路も拡大。例えば、海外のグループ会社がサイバー攻撃を受けた結果、専用線を介して本社のシステムまで侵入されたり、業務委託先やサプライチェーンが侵害された結果としてビジネスが影響を受けるなど、リスクが多様化しています。

林　ネットワーク上の脅威が多様化したことで、より根本的かつ包括的な対策が必要になり、企業が本腰を入れ始めたことも、ゼロトラストが注目された理由の1つですね。実際、ネットワークに関するリスクが企業経営に及ぼす深刻度も増してきており、実際に被害にあったお客様からの相談が増えてきたように感じます。

染谷　かつてはユーザーの個人情報が流出するといったケースが一般的でしたが、近年ではビジネスへの影響がさらに深刻化しています。例えば、システムを停止させるなどして“身代金”を要求する「ランサムウェア」によって機密情報を公開される被害は、当社が把握しているだけでも2021年には年間で2千5百件以上に及びます。同時に被害額も拡大しており、かつては数万円程度だった身代金が、今では平均1億3千万円にまで達しています。こうした金銭的被害を特別損失に計上する以外にも、店舗運営や輸送業務が停止に追い込まれるなど、ステークホルダーへの影響が大きくなっているのが近年の特徴です。

林　それだけ被害が大きくなると、企業側でも深刻にならざるを得ませんが、実際に多くの企業と接していると、業界ごとに温度差を感じるのも事実です。

染谷　実際に同業他社で深刻な被害が生じているかどうかで、経営層の意識に違いが出ているように感じます。例えば自動車業界では、業界を代表する大手企業において、サプライチェーンへのサイバー攻撃によって生産ライン全体がストップしたことから、各社が一斉に対策を打ち始めています。ネットワーク上のリスクが、事業そのものの存続を揺るがしかねないことを認識すべきでしょう。

Takeaways

「ゼロトラスト」が注目される背景

1 環境変化によるネットワーク接続先の多様化
2 上記によるネットワークリスクの拡大・深刻化
3 コロナ禍によるテレワーク拡大により、1 2への対応が喫緊の課題に

1-2「ゼロトラスト」の本質を捉える

林　コロナ禍で「ゼロトラスト」が注目されたことで、多くのベンダーが一挙に参入した結果、言葉は悪いですが、ユーザーが振り回された感もあります。

パロアルトネットワークス株式会社
チーフサイバーセキュリティ
ストラテジスト
染谷 征良 氏

富士通株式会社
ゼロトラストサービス事業部
サービス企画開発部 部長
林 和重

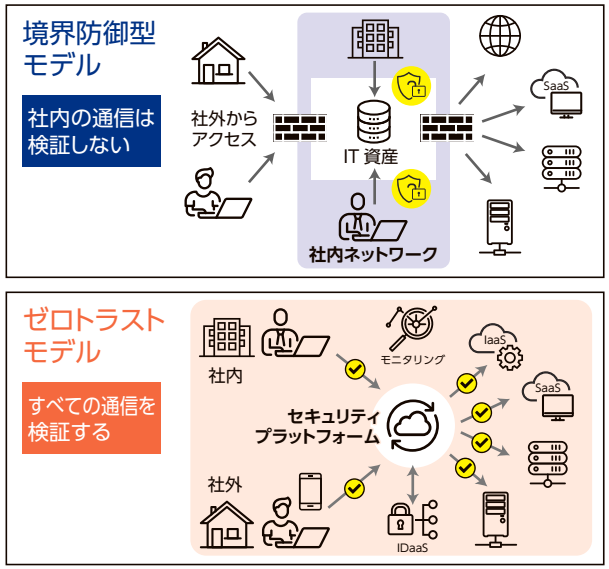


図1）境界防御型とゼロトラストの違い

染谷　確かに、中には多数のベンダーから異なる提案を受けて「ゼロトラスト疲れ」を訴える担当者さんも見られます。一方で、より深刻なのが、ゼロトラストについて誤解したまま検討されているケースが多いこと。当社の調査によると、ゼロトラストを正しく理解できていない意思決定者や決裁権者、担当者が全体の7割近くに達しています。

林　実際に、お客様と会話する中で、十分にご理解いただけていないと感じることがあります。

染谷　例えば、よく言われるのが「ゼロトラストをやろうとするとお金がかかる」。これはネットワーク基盤から設備まで、すべて刷新しないとゼロトラストは実現できないという誤解から来ています。一方で「ゼロトラストはテレワーク対策」とか「認証システムを導入すればゼロトラスト」とか、限定的な範囲でしか捉えられていない担当者も少なくありません。

林　「ゼロトラスト＝何も信頼しない」という前提に立って、回線から端末、トラフィック、ユーザーまで、ネットワークの全要素を検証し、リスクを排除しつつ、誰もが効率的に活用できるネットワークを構築するという、本来の意義に立ち返る必要がありますね。

染谷　ゼロトラストは事業継続を支えるセキュリティの「手段」の1つであって、それ自体が「目的」ではありません。ゼロトラスト採用を検討する一方で、テレワークなどの部分的な課題解決や単なるツールの導入に終始していたり、組織としての課題やゼロトラストが必要な理由を全体的に整理できず、「何から始めればよいのか？」というお客様も少なくありません。

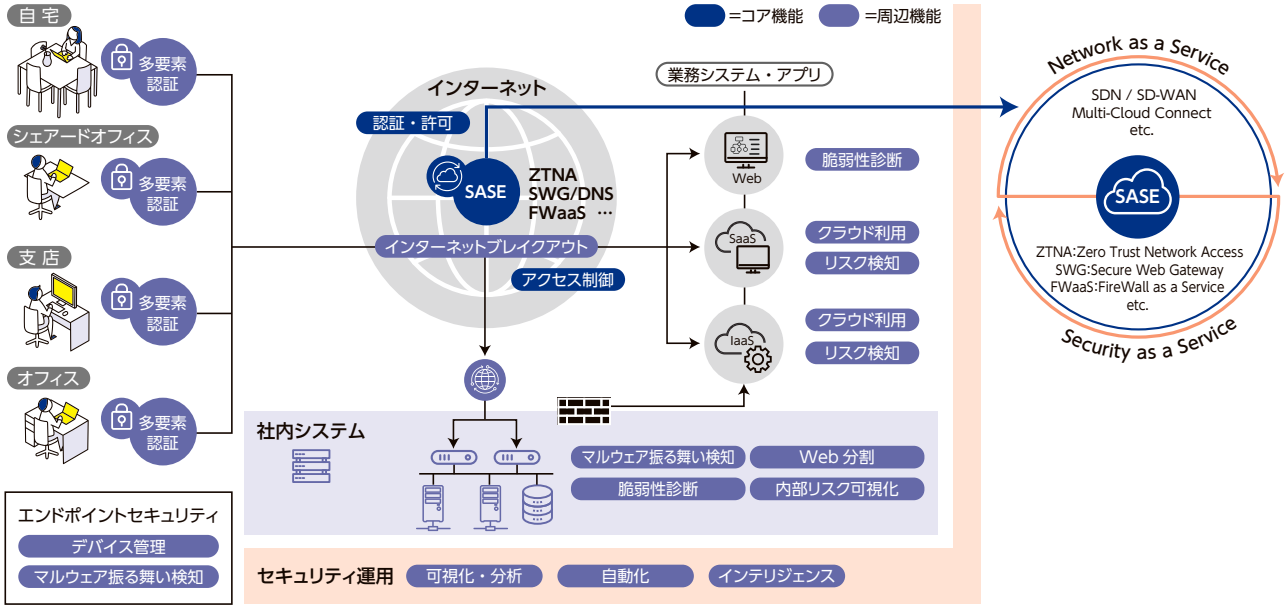


図2）ゼロトラストネットワークの全体像

林　富士通では、そうしたお客様向けに、ネットワークの全体像を整理し、課題を棚卸しして解決への道筋を可視化する「ロードマップ策定支援サービス」を提供していますので、ぜひご活用いただきたいですね。

Takeaways

- 「何も信頼しない」という前提からネットワークの全要素を検証し、「場所に関係なく一貫したセキュリティレベルを実現する」のが「ゼロトラスト」の本質
- 「ゼロトラスト」は目的を実現するための“手段”であって、それ自体が“目的”ではない

1-3 ゼロトラストネットワーク構築の要「SASE」

林　ゼロトラストネットワークの実現に欠かせない要素として「SASE（Secure Access Service Edge：サシー）」が注目を集めていますが、国内で提供されたのはパロアルトネットワークスさんが初めてでしたね。

染谷　SASEとは、そもそも世界的なアナリストファームが2019年8月に定義したもので「ネットワークやセキュリティに関する多様な機能を、クラウド上で統合したサービスとして提供するプラットフォーム」を意味しています。当社が「Prisma® Access」として発表したのが翌年1月という、まさにコロナ禍直前というタイミングもあって、ゼロトラストとともに認知度を高めてきましたが、必ずしも「ゼロトラスト＝SASE」ではありません。

林　確かに、SASEはゼロトラストの実現に重要なツールですが、私たちがより注目しているのが「一貫性」と

いうキーワード。海外など場所を問わず、どこでも同じレベルのセキュリティを実現できるというのは、画期的な仕組みだと感じています。

染谷　SASEの登場は、「マルチベンダー」から、「ベンダー統合」へのトレンド変化を象徴しています。以前はベンダーごとに得意／不得意があり、セキュアウェブゲートウェイはA社、ファイアウォールはB社、リモートアクセスはC社と、異なるベンダーの製品を導入する「個別最適」が一般的でした。その結果、導入や運用に関わるコストや作業負荷が膨れ上がるとともに、それぞれ規格や仕様が異なるためデータ連携が困難といった事態が生じていました。各社バラバラに提供していたツールを、網羅性の高い1つのプラットフォームとして提供することで、セキュリティ面で一貫性があるだけでなく、よりシンプルで使い勝手の良いネットワークを実現できるのです。

林　富士通も複数のベンダーのツールを扱っていますが、SASEのようにプラットフォームとして提供することで、構築・運用の負荷が下がることを実感しています。ネットワークの接続先が多様化してリスクも増加し、個々のツール頼みでは対応しきれなくなっている現在、求められるのは、すべてのツールを統合管理し、専門家やAIの分析によって網羅的にリスクを管理する仕組み。そのためのポイントがベンダー統一です。

Takeaways

- SASEとは、ネットワークやセキュリティに必要な様々な機能を統合したクラウドプラットフォーム
- SASEは従来の「マルチベンダー」から「ベンダー統合」へのトレンド変化を象徴する概念

1-4 ゼロトラストネットワーク構築に何が必要か

染谷　ゼロトラストを検討される企業に共通する悩みの1つに、自社内にネットワークやセキュリティの専門家が少ないという「人の問題」があります。人材不足やスキル不足は短期的に解決できるものではありませんが、だからといって「人がいないからできない」では、高まるリスクに対応できません。

林　大規模な社内ネットワーク全体を再構築するのは、IT担当者にとって一大事で、人材も含め、いかに実現し運用するかを考える必要があります。そこで富士通では、導入から構築、運用支援までトータルなサービスをワンストップで提供し、現場の負荷を下げながら、最適なネットワーク構築をお手伝いしています。

染谷　ユーザー企業がやるべきは、自社のビジネスにおいて何が致命的な脅威なのか、将来的な事業戦略を踏まえて検討し、優先順位を付けること。そして、その検討結果をもとに、富士通さんのような外部パートナーと対話すること。そうしたサイクルを回していくことが、ビジネス要件に合ったITインフラの構築はもちろん、社内におけるIT人材の成長にもつながるでしょう。

林　経営層には、私たち外部パートナーとの対話に加えて、IT部門とも継続的な対話を心掛け、ネットワーク上のリスクに対する危機感を浸透させてもらいたいですね。実際に構築を担う担当者から「明日にでも対策が必要」という切実さを感じる場合もあれば、検討を指示されたものの、何から着手すべきか迷っている場合もあります。そうした危機感の差が、ネットワークの品質を左右しかねません。

染谷　ネットワーク上のトラブルの多くは、経営層やビジネス現場のニーズと、セキュリティ要件との乖離によって生じています。例えば、ある企業で工場内のデータ収集・活用を検討したところ、IT部門がセキュリティ上の懸念から難色を示したため、製造部門が独自に回線を引いてデータ収集を開始。その結果、セキュリティに不備があって問題になりました。こうした事態を避けるため、ビジネス部門とIT部門、双方の意見をすり合わせるのが経営層の役割と言えます。

林　本日は具体例を交えた貴重なご意見をいただき、大変参考になりました。今後もお客様に最適なネットワークを提供できるよう、連携していきましょう。

Takeaways

- 社内にIT人材が不足する場合、企業はまず「事業戦略を踏まえたリスク検討」により優先順位を付ける
- ICT部門との継続的な対話によって、危機感の共有やビジネスニーズとのすり合わせを行うのが経営層の役割

Check it

パロアルトネットワークス様では、ネットワークセキュリティ業界最大規模のカンファレンス「IGNITE」を2022年10月から12月にかけてオンライン開催します。視聴を希望される方は、以下のURLにアクセスし、招待コードを記入の上、お申し込みください。

●申し込みURL
https://seminar.jp/ignite22japan/index.html
招待コード：3026

2 Fujitsu Presents　課題・目的別オファリングモデル

ゼロトラストネットワークの構築は、対処療法によって“部分最適”を積み重ねてきた結果、運用上のコストや業務負荷、リスクが増大した既存ネットワークに根本療法を施し、“全体最適”を目指す絶好の機会と言えます。とはいえ、その実現は容易ではなく、既存ネットワークの構成要素や課題を詳細に把握し、最適なソリューションを選択する高度で広範、専門的なノウハウが求められます。富士通は、ネットワークやセキュリティに関する幅広い知見や技術を駆使し、トータルサポートを提供することで、多様なネットワーク構築実績を積み重ねてきました。ここでは、3つのケースを取り上げて、ネットワークとセキュリティの課題解決策をご提案します。

- Case 1　テレワーク拡大に伴うセキュリティリスクと通信量の増加に対処したい
- Case 2　グループ規模の拡大に対応し、安全性を維持しながらネットワークを拡張したい
- Case 3　逼迫回避とセキュリティ対策を、ユーザーへの影響を最小限にして実現したい

サポートフロー

1 ヒアリング
詳細なヒアリングを通じてネットワークを構成する全要素を洗い出し、課題を整理・分析します。

2 設計・提案
中長期の事業戦略や組織体制を踏まえて、あるべき理想のネットワーク像を可視化します。

3 構築支援
経験豊富なエンジニアによるスピーディーかつ高品質な構築により、業務への影響を最小化します。

4 運用支援
専門知識を要する煩雑な運用業務を代行し、IT部門の負荷と運用上のリスクを軽減します。

5 アフターフォロー
運用時のデータを構想段階における「目標値」と照らし合わせ、全体最適に向けた改善を繰り返します。

ソリューションメニュー

SASE (Secure Access Service Edge)

ネットワークやセキュリティに関する各種の機能をクラウド上で統合しサービスとして提供する、新たなセキュリティフレームワークの考え方。（詳細は4ページを参照）

XDR (eXtended Detection & Response)

エンドポイントを監視するEDR※1や、ネットワークを監視するNDR※2に、AI解析やログ管理などを組み合わせ、外部からの脅威による不審な挙動を検知するソリューション。

※1 EDR：Endpoint Detection & Response
※2 NDR：Network Detection & Response

WEBプロキシ

社内や社外などの場所を問わずに安全なインターネットアクセスが可能となるCloudProtectで提供するクラウド型プロキシサービス。全端末からのインターネットアクセスを集約し、共通のセキュリティポリシーを適用することで、高度なセキュリティ統制を実現。

DNS (Domain Name System) セキュリティ

ドメイン名（インターネット上の住所）を管理するDNSサーバに問い合わせて、閲覧するサイトの運営者を確認（名前解決）し、危険なサイトへのアクセスを防止する仕組み。

ローカルブレイクアウト※3

輻輳※4による通信品質低下を避けるため、安全性が確認されたサイトやシステムについては、データセンターなどを経由させず、PCなどから直接アクセスする仕組み。

※3「インターネットブレイクアウト」とも言う
※4 通信が集中し混雑した状態

Case 1 テレワーク拡大に伴うセキュリティリスクと通信量の増加に対処したい

課題 1 社外からのインターネット利用によるセキュリティリスクが増大

対策 1 SASEとXDR導入によるセキュリティ強化

A社では、テレワークの増加に伴い、社外からのインターネット接続が急増したため、社外でマルウェア感染した端末が社内に持ち込まれたり、リモートで社内システムにアクセスするなどのセキュリティリスクの増大が懸念されました。そこで、SASEを導入してすべての接続を集約し、アクセス・セキュリティを一括制御する仕組みを構築。また、SASEも含めてXDR基盤に情報集約可能なEDRを導入し、横断的な分析など将来のセキュリティ強化・拡張が可能な構成でご提供しました。

課題 2 SaaS利用の増加に伴い、DC集約型のインターネットゲートウェイが逼迫

対策 2 分散アーキテクチャのSASE導入とローカルブレイクアウトにより逼迫を解消

業務効率化を目的にSaaS活用を推進したところ、アクセスの集中により回線が逼迫し、通信品質が低下する事態が頻発。今回、新たに導入したSASEは複数のアクセスポイントを利用者のアクセス元に応じて使い分ける、あるいは通信量に応じて利用帯域を拡張するなど、輻輳しづらいアーキテクチャを採用しているため、通信負荷の軽減が期待できました。加えて、安全性が確認された一部の通信については、SASEを介さず端末から直接アクセスするローカルブレイクアウトを併用することで、必要とするSASE基盤の帯域を適正に維持する構成を実現しました。

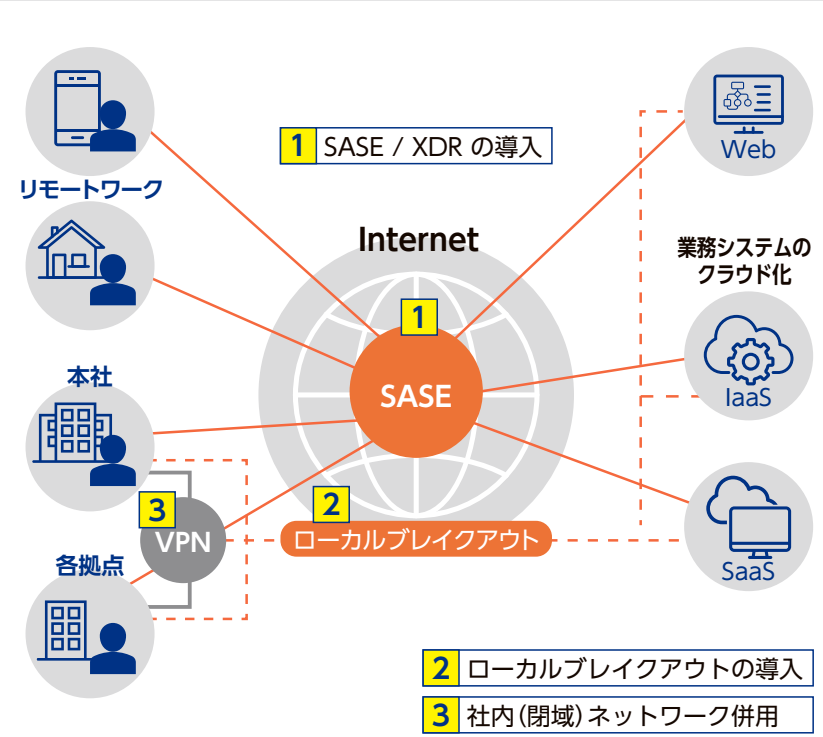
課題 3 インターネット利用時のミッションクリティカル業務へのリスク懸念

対策 3 セキュリティの高い閉域網を構築し、対象業務の通信を順次移行

A社の事業には社会的影響が大きい“ミッションクリティカル”な業務が含まれており、ベストエフォート回線※が主体となる社外からのインターネット利用では、通信品質やセキュリティの強化が業務に影響を与えることが懸念されました。そこで、正常に業務が行えることを確認しながら、徐々に適用範囲を拡大していく段階移行を検討し、ミッションクリティカルな業務向けに閉域ネットワークを維持したまま、SASEの導入を並行して推進、業務に影響しない移行計画を策定しました。スモールスタートが可能なSASEのメリットを活かし、通信品質を見定めながら業務ごとに段階的な移行を進めています。

※「最大限の努力」を意味し、条件が揃わない場合の通信品質は保証されない回線

ネットワーク構成



ソリューションメニュー

SASE	CloudProtect Zero Trust Network powered by Prisma Access from Palo Alto Networks
XDR	CloudProtect XDR for Endpoint powered by Cortex XDR from Palo Alto Networks
閉域網構築	FENICS ビジネスVPNプラス

Case 2 グループ規模の拡大に対応し、安全性を維持しながらネットワークを拡張したい

課題1 グローバルでクラウド接続が増加し、既存ネットワークが逼迫

対策1 オートスケール可能なWEBプロキシを導入し、回線逼迫を回避し拡張性を確保

B社では、ホールディングス体制のもとグローバルでグループを拡大しているため、社内データセンター（DC）内のWANにグループ企業からアクセスが集中。今後もさらなる拡大を計画しており、回線逼迫による通信品質の低下が危惧されていました。そこで、インターネットへのアクセス経路として、オートスケール可能なWEBプロキシを導入し、逼迫を回避するとともに将来的な拡張性を確保しました。

課題2 グループ各社が個別に運用する複雑なネットワーク構成の見直し

対策2 WEBプロキシとクラウド接続、2系統のシンプルなネットワーク構成に再編

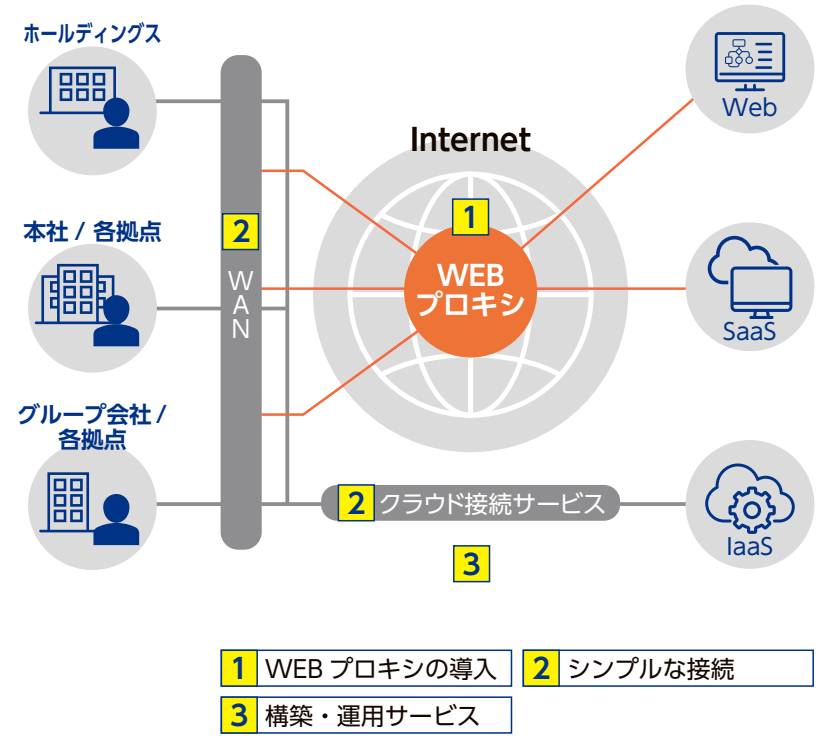
B社グループ内には、WAN以外にも各拠点が個別に運用するネットワークがあり、ネットワーク構成が複雑化し、運用の難易度が高まっていました。そこで、富士通のネットワークサービスを活用した再構築を提案。各拠点のWANネットワークをFENICSビジネスマルチレイヤーコネクトに統合してシンプルな構成とし、外部クラウド（IaaS）の利用はオプションのクラウド接続サービスを経由させることで、セキュリティを確保しながら運用負荷を軽減しました。

課題3 ネットワーク規模の拡大に伴う運用負荷やリスクの増大

対策3 ゼロトラストセキュリティ構築・運用サービスによる構築・運用支援

全世界で5,000名規模の組織を支えるネットワークは、再構築に関わる作業負担が大きいため、社内スタッフだけでは対応が難しく、稼働後の運用リスクも懸念されました。そこで、「ゼロトラストセキュリティ構築・運用サービス」を採用いただき、富士通のSE/CEがトータルなサポートを提供。短期間での導入を実現するとともに、稼働後も安定した運用品質を確保しています。

ネットワーク構成



ソリューションメニュー

WEBプロキシ	CloudProtect WEBプロキシ
ネットワーク	FENICS ビジネスマルチレイヤーコネクト
構築・運用支援	ゼロトラストセキュリティ構築・運用サービス

Case 3 逼迫回避とセキュリティ対策を、ユーザーへの影響を最小限にして実現したい

課題1 DCへのトラフィック集中を軽減しつつ、従来と同様のセキュリティを担保

対策1 ローカルブレイクアウトによる逼迫回避とともに、DNSセキュリティを導入

C社では従来、社内DC内にファイアウォールなどを備えたセキュリティシステムを構築し、各拠点からのアクセスを一元管理していました。しかし近年、Web会議やSaaS利用の増加に伴いDC内のトラフィックが急増し、回線が逼迫。通信品質の低下を招いていました。そこで、セキュリティを確保しながら通信負荷を軽減するため、ローカルブレイクアウトによるトラフィック分離と併せて、DNSセキュリティを導入しました。

課題2 導入作業はユーザーへの影響を最小限に、かつ短時間で実施

対策2 ソフト不要のDNS導入により、ルータ設定の一括変更のみで対応

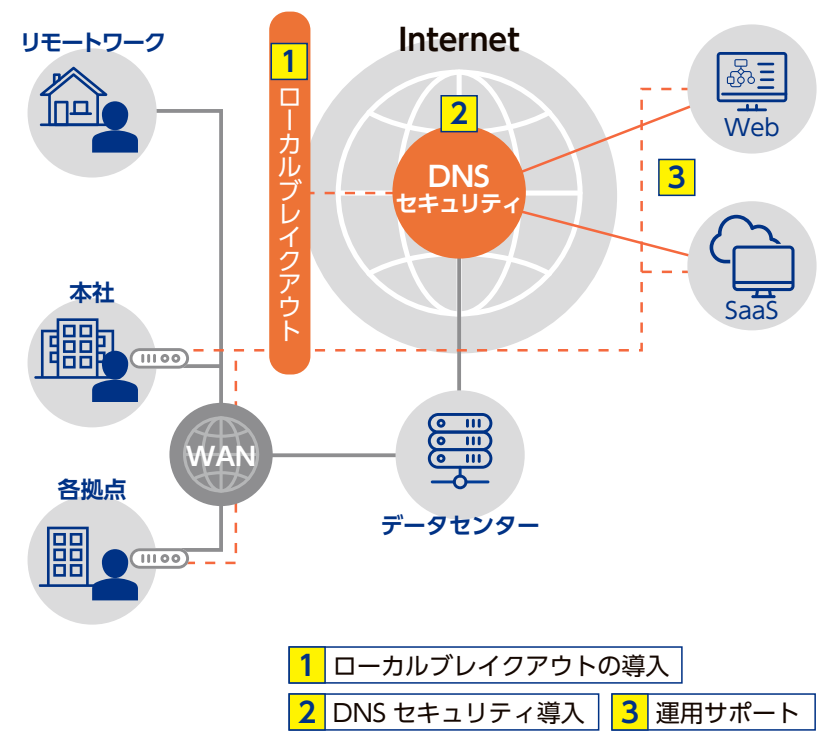
DNSセキュリティの導入に際しては、通常は端末にソフトウェアをインストール・再設定する必要があり、各拠点での作業負荷に加えて、ユーザーの業務に対する影響が長期化することが懸念されました。そこで、ソフト不要な構成のDNSを提案。各拠点のルータの設定を、本社から一括制御で変更するだけで導入できるため、拠点側の手間は最小限で済み、短時間でのスムーズな導入を実現しました。

課題3 DNSの過剰検知に対応するための業務負荷が増大

対策3 対応業務を富士通が引き受け、業務負荷を軽減しつつ迅速な対応を実現

DNSセキュリティの「名前解決（P6参照）」は、一般の企業サイトなどもブロックされる「過剰検知」が生じる場合があり、その都度、運用担当者が当該サイトの安全性を確認し、除外設定する必要があります。また、セキュリティの専門家ではない担当者の判断には限界があり、作業負荷の増大が予想されました。そこで、過剰検知への対応をアウトソーシングすべく運用サポートを導入。運用負荷を軽減するだけでなく、専門家のスピーディーな対応により運用品質が向上しました。

ネットワーク構成



ソリューションメニュー

DNSセキュリティ	CloudProtect DNSセキュリティ powered by Cisco Umbrella
構築・運用支援	ゼロトラストセキュリティ構築・運用サービス