net one

IT インフラの全体最適化と表裏一体

組織の DX 推進を支えるために必要なセキュリティアーキテクチャとは

IT 部門は、広がる IT インフラ基盤を確実に把握し、新たな境界におけるセキュリティ面での制御や管理を徹底しなければならない。多様化する組織 IT のセキュリティ保護に向け、ネットワンはアーキテクチャによるアプローチを重視する。

デジタルトランスフォーメーション（DX）推進に向け、企業は機動的かつ柔軟に IT を展開したい。一方で、IT ガバナンスとセキュリティの確保は至上命令だ。機動性や柔軟性と管理やセキュリティという相反する課題に直面する IT 部門に対し、ネットワンシステムズ（以下、ネットワン）は複数の角度から支援策を打ち出している。

1 つ目が「netone Elastic インフラストラクチャー」だ。このアーキテクチャは、企業や組織のデータセンターやパブリッククラウドなどの IT インフラとそこにアクセスするユーザーも対象にネットワークおよびセキュリティを統合的に管理、運用できるようにする。

2 つ目が「オペレーショナブルセキュリティ」（OPSec）だ。このアプローチは、IT インフラ運用の自動化と自律化を進めつつ、組織が迅速に適切な対策を打てるようにすることを目指す。ツールや運用、組織上のサイロを排除した上でセキュリティ状態の健全性と運用状況を継続的にモニタリングし、改善することでセキュリティ対策の全体最適化を実現する。

3 つ目が本稿で説明する「セキュリティアーキテクチャ」だ。netone Elastic インフラストラクチャーや OPSec と連動し、機動的な IT と確かなセキュリティを両立させるための枠組みとして機能する。

サイバーセキュリティでは「アーキテクチャ」が重要になる

これまで組織は、本社や事業拠点とその中で働く人を「内」、それ以外を「外」としてデータセンターを中心とした境界型セキュリティの確保に取り組んできた。しかし境界は大きく変化している。パブリッククラウドをイノベーション基盤として積極的に活用するために社内データセンターとのハイブリッド構成は当たり前になった。複数クラウドの併用も始まっている。

その結果、さまざまな部署が IT 部門の許可を得ず、組織のセキュリティポリシーに準じない状態でサービス追加を繰り返した。また、それぞれの保護対象領域に導入されたポイントソリューションも IT 部門の悩みの種だ。このようなパッチワーク的なアーキテクチャでは可視性のギャップを生み出し、運用担当者も異なることも相まって統合的なアクションができないままの状態が続く。

サイバー攻撃の高度化やクラウド利用が進んだことで境界は曖昧になり、境界型セキュリティ対策だけでは IT 資産を守り切れなくなったという事実もある。IT 部門は、広がる IT インフラ基盤や端末、従業員、サードパーティーが多様化するデジタルアイデンティティーを確実に把握し、クラウド前提の新たなセキュリティ制御や管理を徹底しなければならない。

したがって個別に導入してきたセキュリティ製品やサービスを効果的に組み合わせ、インフラの変化に合わせて効率的に使いこなす必要がある。新しい考え方や技術を導入するためのハードルを下げることも重要だ。

多様化する組織 IT のセキュリティ保護に向け、ネットワンはアーキテクチャによるアプローチを重視する。取り組みの一つとしてアーキテクチャをモジュール化してユースケースとのひも付けを行い、「Validated Design」（検証済み構成）によって実証されたアーキテクチャを提供する。

ネットワンが提唱する
セキュリティアーキテクチャの構成要素とは

その根底には、クラウド活用を前提としたネットワークセキュリティの進化とともにインフラに融合されたセキュリティという要素がある。

およそ十数年の間にネットワークのアーキテクチャは大きく変わった。物理層を中心としたアンダーレイから抽象化・仮想化、そしてクラウドへと進化した。それに伴いセキュリティやアプリケーションの考え方も変化した。

アンダーレイ型ネットワークでは、内と外の間に配置された境界型セキュリティにより安全を確保していた。抽象化・仮想化が進むとトラフィックの流れも East-West（末端間通信）が多くなり、信頼する領域をより細かい単位で制御するマイクロセグメンテーションの必要性が高くなった。

そして現在、クラウド化が進んだことで場所を問わず、ユーザーや端末に必要なサービスを迅速に提供するためにクラウドベースのセキュリティモデル「SASE」（Secure Access Service Edge）やゼロトラストセキュリティの考え方が注目されていることは周知の事実だ。

ネットワンは高度なネットワーク技術やノウハウ、経験をコアにして、ネットワークの変化に合わせて企業ネットワークの全てのエンティティーを安全に接続し、高速かつ信頼性が高いネットワークセキュリティを実現する。

また、企業ネットワークにあるエンティティー間のアクセス品質などのトラフィック要素やセキュリティ状況を監視して、ユーザーアクティビティとパフォーマンスを包括的に可視化して分析することで組織のセキュリティポリシーに基づいたインフラを制御することを目指す。

その上で「ゼロトラスト」を推進する。SASE によるネットワークレベルの保護とともに、ゼロトラストによるアクセスポリシーでアクセス元／アクセス先の双方でアプリケーションやサービスへの接続を最小限の権限で許容するポリシーの徹底を例外なく包括的かつ機動的に行えるようにする。

具体的には、以下の技術要素を活用してセキュリティアーキテクチャの裏付けを行う。

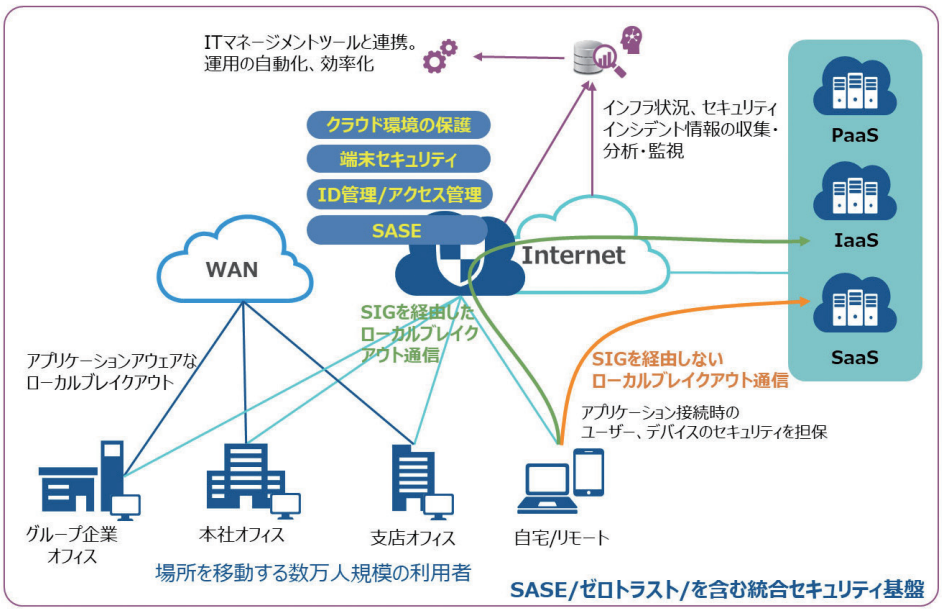
SASE を構成する技術群で IT リソースへのアクセスを可視化するとともに制御することで、アクセス元の場所にかかわらず一貫したセキュリティポリシーの提供が可能になる。

クラウドアプリケーションや社内へのアクセスにはクラウド型 VPN や SDP（Software Defined Perimeter）の機能を適用する。SASE をネットワークの中心としてエッジや SaaS、インターネット全般へのアクセスを可視化し、制御する。

クラウドの活用を前提としたネットワークセキュリティシステム

管理・実装が容易なクラウドサービス基盤を活用した、統合セキュリティシステム

- セキュリティを考慮したリモートワーク環境、場所にとらわれないセキュリティの確保
- 持ち出しPC、モバイルデバイスなどの利用ユーザー、デバイスのセキュリティを担保
- アプリケーションアウェアなローカルブレイクアウト
- セキュリティを考慮したクラウド環境の利用
- インフラ、セキュリティインシデント情報の蓄積、分析
- 運用の自動化、効率化



利便性向上や統合化を実現、ポイントは ～監視・分析～

クラウド活用を前提としたネットワークセキュリティシステム（出典：ネットワンシステムズ説明資料）

アクセス元の端末管理も引き続き重要となる。EDR（Endpoint Detection and Response）やNGAV（次世代アンチウイルス）、EMM（Enterprise Mobility Management）などの適用が考えられる。人だけでなくマシンや場所など多様化する全てのアイデンティティーを検出して管理し、制御する。

NDR（Network Detection and Response）は、攻撃対象領域が広がる複雑なインフラ環境全体を可視化し、異常検知が可能だ。エンドポイント対策を導入しにくいOT環境などでの適用も考えられる。

サイロ化しやすいパブリッククラウドのセキュリティはオンプレミスと同等のセキュリティレベルを維持し、セキュリティポリシーも統一的な運用による一元管理が必要となる。クラウドが備えるネイティブセキュリティ機能を活用しながらサードパーティーのセキュリティソリューションをインテグレーションすることでオンプレミス環境との運用の親和性を確保しつつ、統一的な監視と対応を図る。

基本的には自社データセンターやパブリッククラウド、サーバ、端末などに導入したネットワークおよびセキュリティ製品をセンサーとして利用しながら情報を収集し、SIEM（Security information and event management）やSOAR（Security Orchestration, Automation and Response）を活用した統合的な管理と収集した情報の分析、それに基づいた対応を進める。これによってセキュリティインシデントを迅速に把握し、効果的なアクションができる。

セキュリティ機能の実装は、ソフトウェアおよびクラウドサービスを活用することで機動性、柔軟性、拡張性を向上できる。セキュリティインシデントへの対応は、自動化および機械学習を始めとするAI技術を最大限に活用する。

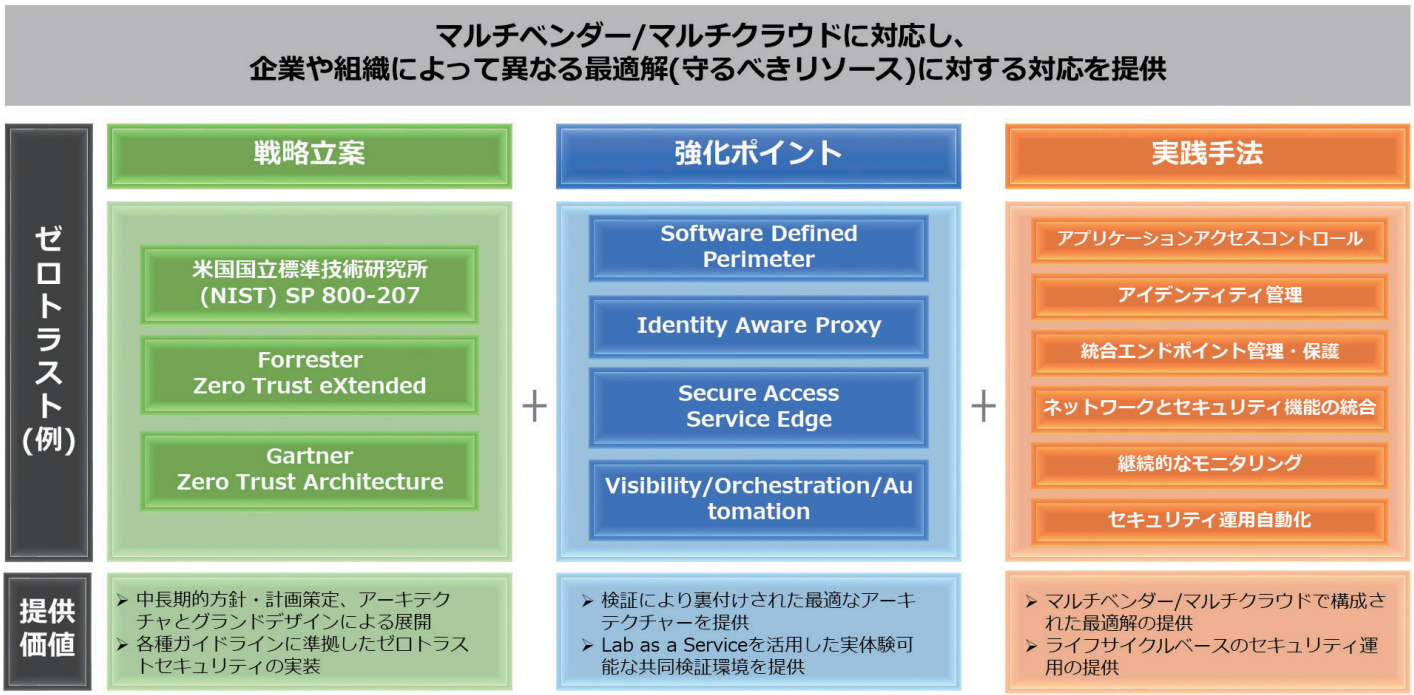
活用可能な技術や製品ジャンルの例を示したが、やみくもに製品を導入すればいいというわけでもない。組織のIT展開の状況に合わせて「守るべき情報資産の特定」「攻撃対象領域の把握」「事業部門におけるIT活用の拡張や展開をどう促進し、追随するか」「そのために最適なセキュリティはどのようなものか」といった戦略的観点に基づいて判断し、投資対効果を高める必要がある。

納得して導入を進められる「Validated Design」と「LaaS」

セキュリティアーキテクチャを形にしていくのは単純な作業ではない。ネットワンは、顧客が優先順位に応じて段階的にセキュリティを強化していけるようにさまざまなサポートを提供する。

その一つがValidated Designだ。ネットワンが製品やシステムを顧客に先駆けて検証し、検証済みのシステム構成を

netone ゼロトラストセキュリティ



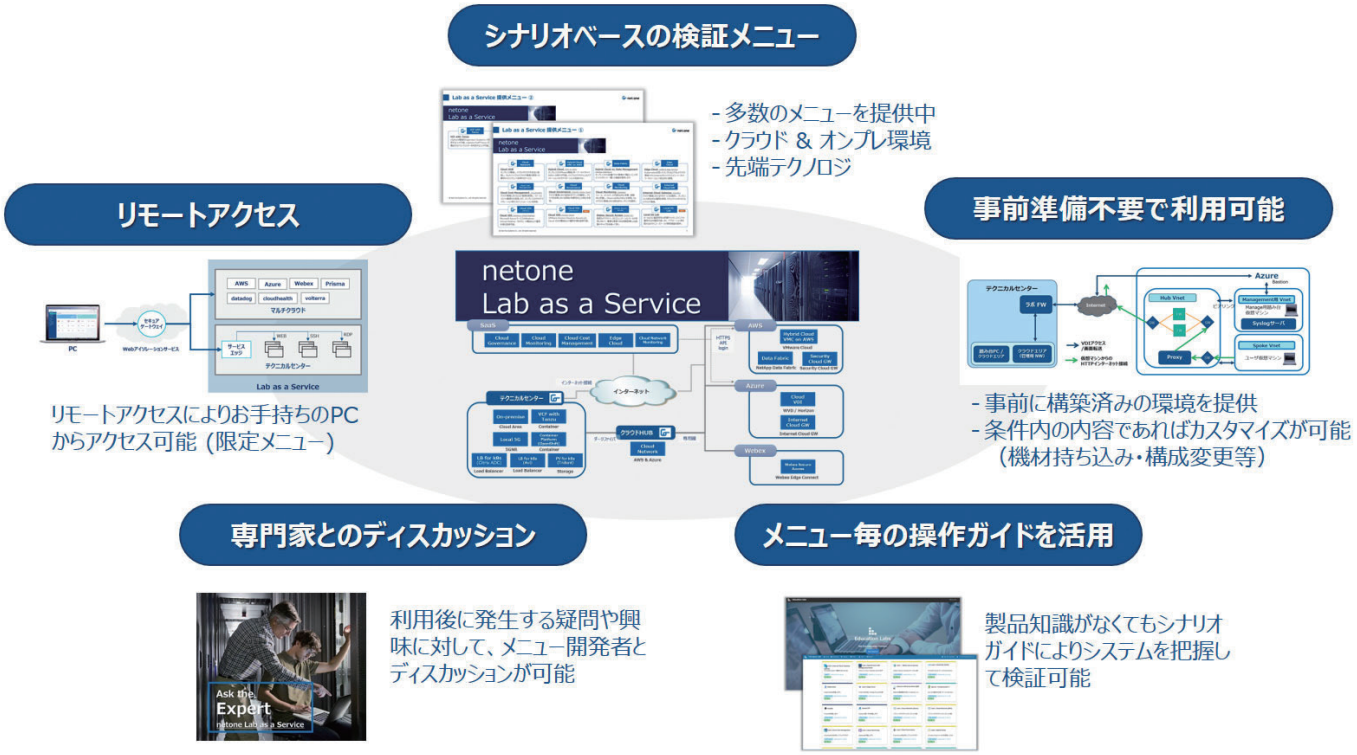
netone ゼロトラストセキュリティ（出典：ネットワンシステムズ説明資料）

提示する活動だ。顧客にとって導入したことがないシステムや技術でも、検証済みのシステム構成をベースとすれば安心感をもって検討できる。

また顧客自ら技術の利用シナリオを試せるサービス「Lab as a Service」（LaaS）もある。ネットワンの技術ラボ施設は、さまざまなシナリオに基づく環境を自動的に構築できる。シナリオ例にはクラウドアクセスセキュリティやクラウドSIEMなどが挙げられる。これを活用して顧客は特定技術を導入する前に自らテスト環境を準備することなく検証し、運用を体験することができる。

ネットワンが提唱するセキュリティアーキテクチャは、インフラアーキテクチャの全体最適化と密接に連携している。顧客は部分最適から始め、全体最適の実現を目指せる。今後もITインフラはダイナミックに変化するだろう。ネットワンは顧客に寄り添い、継続的なモニタリングを通じてセキュリティ確保のための改善と提案を続けていく。

Lab as a Service の特徴



Lab as a Service の特徴（出典：ネットワンシステムズ説明資料）

●お問い合わせ
ネットワンシステムズ株式会社／マーケティングチーム セキュリティ担当
Sec-pm-Gr@netone.co.jp

※この冊子は、ITmedia エンタープライズ（https://www.itmedia.co.jp/enterprise/）に 2022 年 3 月に掲載されたコンテンツを再構成したものです。
https://www.itmedia.co.jp/enterprise/articles/2203/18/news007.html