net one

netone
推奨ソリューションパッケージ
総合カタログ

netone 推奨ソリューションパッケージとは

事業環境や働き方がデジタル化に向けて急速に変化する中、あらゆる企業や組織は、ネットワークをいかに変革するかが重要な課題となっています。

商談やミーティングのオンライン化とテレワークが加速、場所を問わないハイブリッドな働き方が求められる一方、SaaS や Web 会議などクラウドサービス利用による通信量増大、セキュリティ要件の高度化・複雑化など、もはや従来型の構造では、迅速・安全な事業運営は困難になってきています。

それらの課題を解消するべく、ネットワンでは、レガシーな IT 基盤をモダナイズしてビジネスの継続性を高めると共に、クラウドを活用して DX を着実に推進できるビジネスインフラへと変革するための「推奨ソリューションパッケージ」を提供しています。

netone 推奨ソリューションパッケージの特長と活用メリット

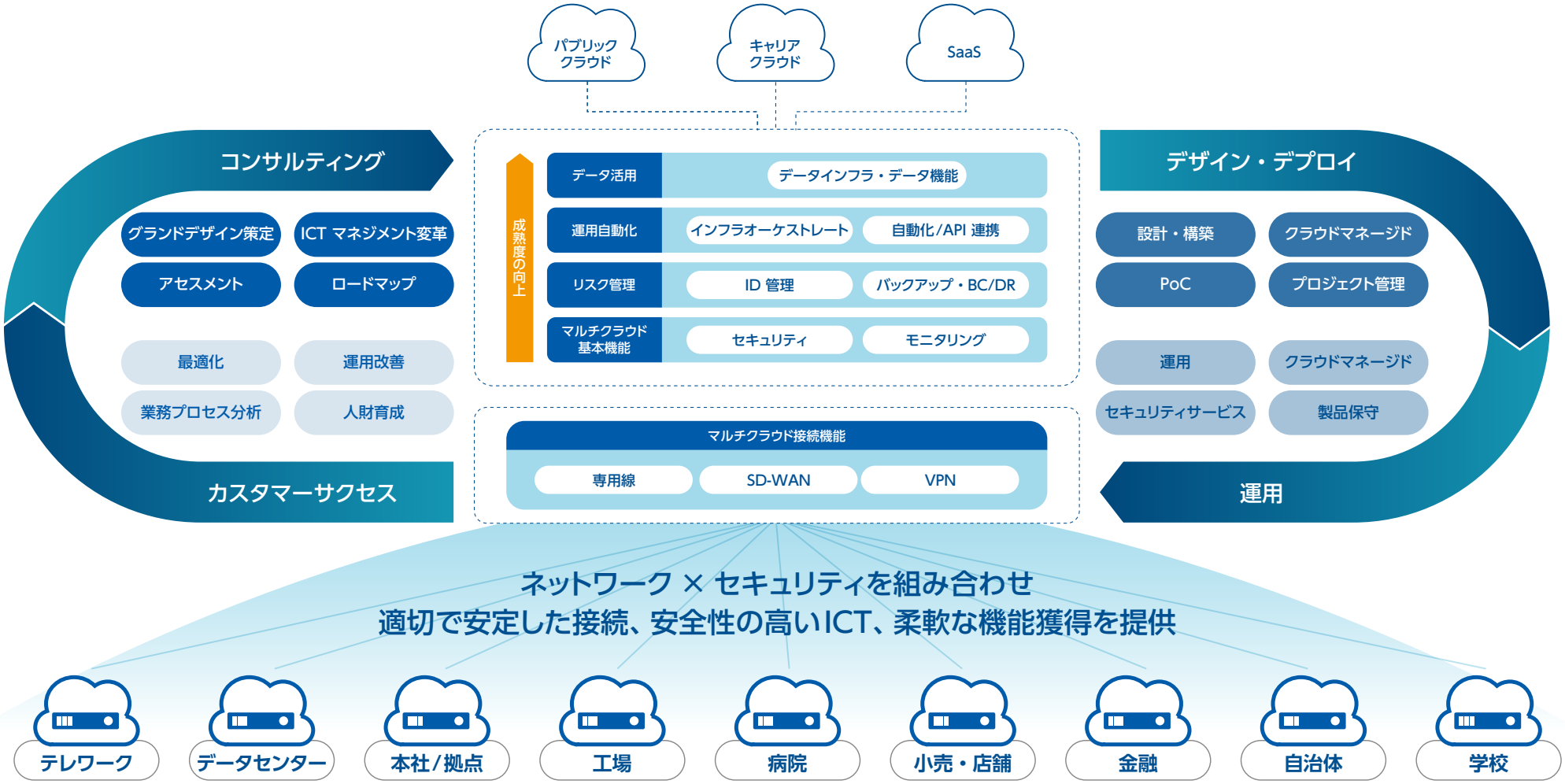
推奨ソリューションパッケージの活用により、さまざまな製品やサービスの検討が不要に。
お客様はスピーディかつ高品質な、導入が可能となります。

- お客様ニーズごとに用意された、推奨製品・サービスの組み合わせパターンです。
- 各テクノロジー分野で機能面、非機能面でも他と比べ高い優位性を持つラインナップが選抜されています。
- ネットワンが事前に検証を実施済、かつ豊富な導入実績を持つため、安心して導入いただけます。
- ソリューションの導入企画フェーズ、設計・構築フェーズ、運用・保守フェーズとライフサイクルに沿った、サービスをご提供します。

ぜひ活用いただき、ネットワンと共に、BCP（事業継続性）と DX（デジタルトランスフォーメーション）の両立による、ビジネスレジリエンスを実現しましょう。

ネットワンが提供するサービスの全体像

ネットワンは、高度化・複雑化するお客様 ICT 環境のライフサイクルに沿った、多様なサービスを幅広く展開しています。
これまで培ってきた技術・知見を余すことなく活かし、あらゆるものを“ネットワーク”でつなぎ、支え、お客様価値の最大化を支援します。



LAN/WAN ▶P9～13
Security ▶P6～8,19,20,24
Platform ▶P15～17
DC Network ▶P14,21,22
Cloud ▶P18,23

ソリューションパッケージインデックス(1)

	お客様のインフラにおけるニーズ・課題		netone 推奨ソリューションパッケージ	
Security	テレワーク、クラウドサービス利用増により、 ネットワークセキュリティに課題がある	▶	SASE アーキテクチャによるセキュリティ強化 (Palo Alto Networks / Cisco)	P6,7
Security	ランサムウェア被害に遭うと、情報漏洩や業務停止の他 企業の社会的信用を失墜するリスクがある	▶	ランサムウェア対策ソリューション (Palo Alto Networks Cortex XDR)	P8
LAN/WAN	インターネットも活用する最適な WAN ネットワークに マイグレーションしたい	▶	SD-WAN による WAN 最適化 (Cisco SD-WAN / FortiGate SD-WAN)	P9,10
LAN/WAN	安定した稼働実績のあるキャンパスネットワークを 導入したい	▶	キャンパス LAN (Cisco Catalyst 9000)	P11
LAN/WAN	IT インフラの重要性が増しシステムが複雑化する中、 キャンパスネットワーク運用に課題がある	▶	統合キャンパスネットワーク管理 (Cisco Catalyst Center / HPE Juniper Mist)	P12,13
DC Network	IT インフラの重要性が増しシステムが複雑化する中、 DC ネットワーク運用に課題がある	▶	SDN による DC ネットワーク最適化 (Cisco ACI / Palo Alto Networks PA シリーズ / F5 / Red Hat Ansible)	P14
Platform	セキュアかつユーザ利便性が向上するリモートでの 働き方を実現したい	▶	オンプレミス VDI による Hybrid Work 実現 (Omnissa Horizon)	P15
Platform	オンプレミス環境での ICT 共通基盤として 柔軟な環境がほしい	▶	3Tier 仮想基盤によるリソース最適化 (Cisco / Dell / NetApp / Pure Storage / Veeam / Veritas)	P16
Platform	仮想基盤のアップグレード対応に時間がかかる、 障害時対応が煩雑になる等、運用負荷がかかっている	▶	HCI による仮想基盤の運用効率化 (Dell Technologies / Nutanix)	P17

ソリューションパッケージインデックス(2)

お客様のインフラにおけるニーズ・課題		netone 推奨ソリューションパッケージ	
Cloud	出社しないと電話対応ができない 会社だけではなく、自宅や外出先でも代表番号の利用が必要	クラウド電話ソリューション (Cisco Webex Calling)	P18
製造業界 Security	工場ネットワークにおいてネットワーク構成の把握や セキュリティ対策の懸念がある	OT ネットワークセキュリティ強化 (Forescout / Palo Alto Networks)	P19
ヘルスケア Security	安心・安全な医療提供体制を構築したいが セキュリティ対策に懸念がある	HC ランサムウェア対策ソリューション (Cisco SNA)	P20
放送業界 DC Network	4K、8K 放送の大容量通信に対応できる 放送 IP ネットワークを実現したい	放送 DX を実現するネットワーク基盤 (Cisco IP Fabric for Media)	P21
自治体 DC Network	ガバメントクラウド対応を進める中、 接続・運用の設計・体制整備に不安がある	ガバメントクラウド接続サービス	P22
自治体 Cloud	基幹業務のクラウド移行に伴い、 安全・効率的なファイル連携基盤の構築が必要	ガバメントクラウドファイル連携	P23
教育 Security	校務 DX 推進に向け、端末統合と 情報漏洩リスクの低減を両立したい	端末論理分離ソリューション (Security Platform)	P24

SASE アーキテクチャによるセキュリティ強化 (Palo Alto Networks SASE Architecture)

テレワーク、クラウドサービス利用増に最適化されたネットワークセキュリティ

課題

- インターネット、クラウド上の脅威が拡大 場所やデバイスを問わず、安全かつ統合的なネットワークセキュリティの 提供が求められる
- テレワーク、クラウドサービス利用増により、DC 側のVPN装置・ゲートウェイにトラフィックが集中 社員の生産性が低下している
- セキュリティ人財が不足し、高度・複雑化する脅威の対応および、継続的な運用オペレーション対応が困難
- クラウドサービスと既存のオンプレシステムが混在し、システムごとの 管理が分離・複雑化 障害の検知、トラブルシューティングが困難

netone 匠エンジニアの推奨ポイント

- 従来のPAシリーズと同等のFW機能を有する FWaaS 型の SASE (Secure Access Service Edge) により、ネットワークとセキュリティを一元的に提供
- ユーザー&アクセス制御+通信検査・脅威防御をワンストップで提供
- VMware SD-WAN のローカルブレイクアウトによって DC 経由のボトルネックを解消
- クラウド連携や機械学習によりゼロデイマルウェアを含む未知の脅威をリアルタイムで阻止
- ユーザーやデバイスの真正性、健全性を確認することでゼロトラストセキュリティを提供

コンポーネント

- Palo Alto Networks Prisma Access
- VMware SD-WAN

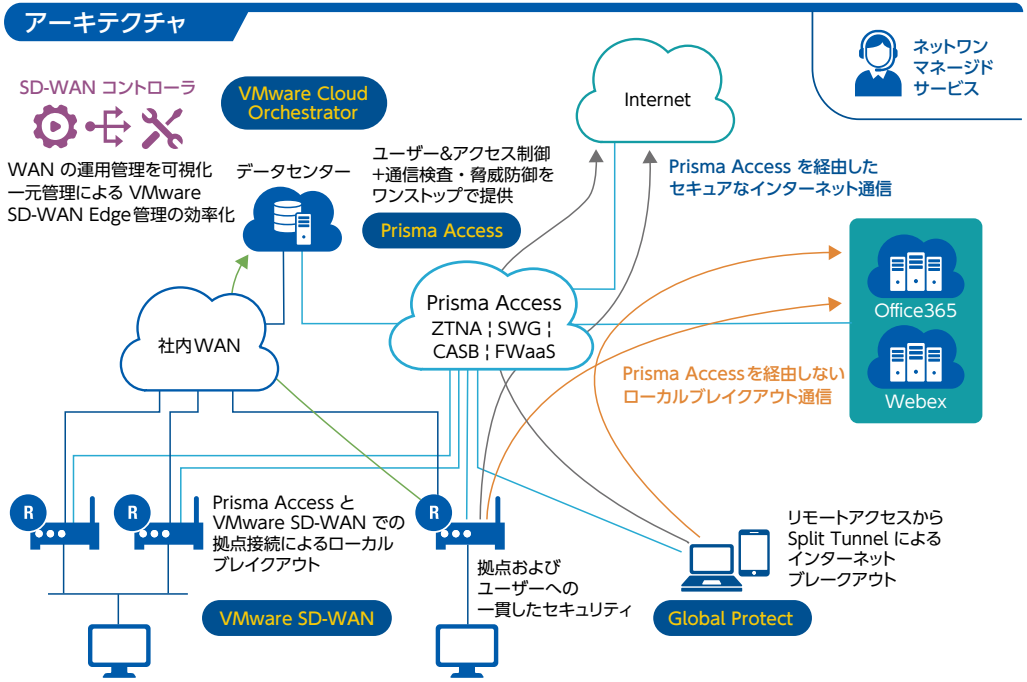
関連するネットワンのマネージドサービス

- netone Managed SASE powered by Prisma® Access (ネットワンマネージドサービス)

解決

- 本社、拠点、外出先などの働く場所に捉われず、一貫したネットワークとセキュリティを提供
- 「働き方改革」を支援
- ゼロトラストの考えの元、クラウドベースの高度なセキュリティ対策を提供 アクセス元のネットワークを問わずサイバー攻撃や不正アクセスから顧客を保護
- クラウドベースのリモートアクセス、インターネットへの出口を提供し DC 中心の負荷を軽減 ローカルブレークアウトにより、Microsoft 365、ビデオ会議などのトラフィックによる 通信帯域圧迫を解消し、品質の高いネットワークを提供
- 一元化されたセキュリティ機能とネットワーク管理機能で、ユーザのロケーションに関係なく、継続的かつシンプルな運用を実現

アーキテクチャ



SASE アーキテクチャによるセキュリティ強化 (Cisco SASE Architecture)

テレワーク、クラウドサービス利用増に最適化されたネットワークセキュリティ

課題

- インターネット、クラウド上の脅威が拡大 場所やデバイスを問わず、安全かつ統合的なネットワークセキュリティ の提供が求められる
- テレワーク、クラウドサービス利用増により、DC 側の VPN 装置・ゲートウェイにトラフィックが集中 社員の生産性が低下している
- セキュリティ人財が不足し、高度・複雑化する脅威の対応および、継続的な運用オペレーション対応が困難
- クラウドサービスと既存のオンプレシステムが混在し、システムごとの管理が 分離・複雑化 障害の検知、トラブルシューティングが困難

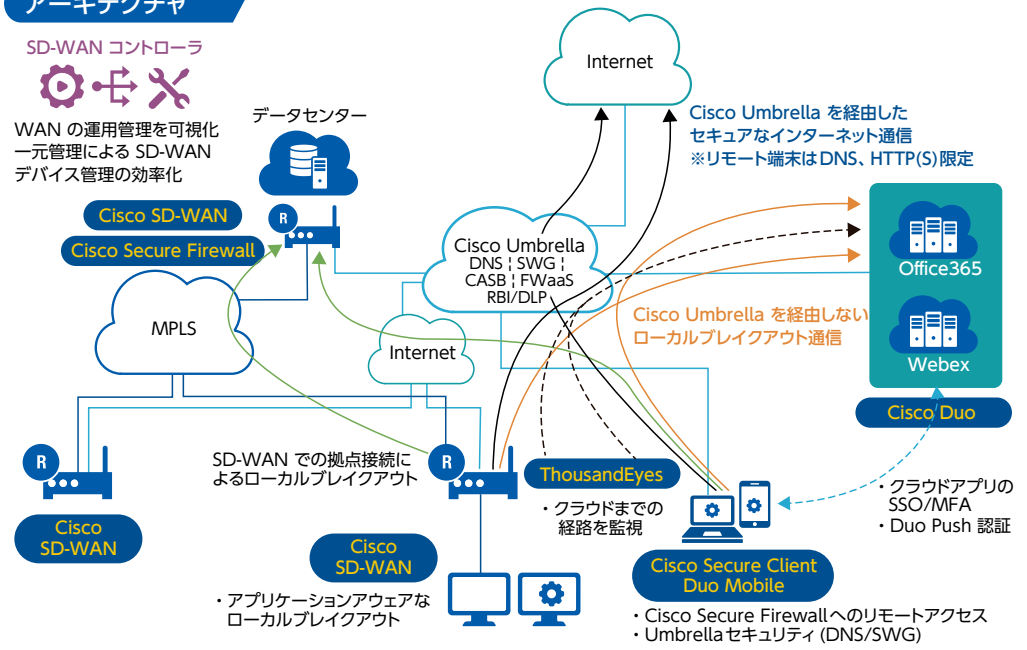
解決

- 本社、拠点、外出先などの働く場所に捉われず、一貫したネットワークとセキュリティを提供
- 「働き方改革」を支援
- ゼロトラストの考えの元、クラウドベースの高度なセキュリティ対策を提供
  アクセス元のネットワークを問わずサイバー攻撃や不正アクセスから顧客を保護
- クラウドベースでインターネットの出口を提供し DC 中心の負荷を軽減
  ローカルブレークアウトにより、Microsoft 365、ビデオ会議などのトラフィックによる通信帯域圧迫を解消し、品質の高いネットワークを提供
- 一元化されたセキュリティ機能とネットワーク管理機能で、
  ユーザのロケーションに関係なく、継続的かつシンプルな運用を実現

netone 匠エンジニアの推奨ポイント

- SASE (Secure Access Service Edge) により、ネットワークとセキュリティを一元的に提供
- ユーザー&アクセス制御+通信検査・脅威防御をワンストップで提供
- SD-WAN のローカルブレイクアウトにより、DC 経由のボトルネックを解消
- DNS セキュリティ、SWG (Secure Web Gateway)、ファイアウォールをクラウドベースで提供
- ユーザーやデバイスの真正性、健全性を確認することでゼロトラストセキュリティを提供
- ユーザ目線でのクラウドまでの経路を監視し通信状況を把握

アーキテクチャ



コンポーネント

- Cisco Umbrella
- Cisco Secure Access by Duo
- Cisco Secure Client
- Cisco Secure Firewall
- Cisco SD-WAN
- Cisco Thousand Eyes

ランサムウェア対策ソリューション (Palo Alto Networks Cortex XDR)

NDR を取り入れた高度な保護機能でランサムウェアを阻止

課題

- システムがランサムウェアに感染してしまうと、ファイル暗号化、情報漏洩、業務停止、金銭的被害など、企業の社会的信用の失墜を招くリスクを伴う
- 医療機関であれば人命に関わる可能性もある
- 従来のエンドポイント側の対応では限界があり、ネットワーク全体での検知や MTTR 短縮の必要性がでてきている
- ランサムウェアの実行前に環境内が探索され、機密情報が既に窃取されるなど、気が付いた時には甚大な被害が出ている可能性がある

netone 匠エンジニアの推奨ポイント

- PA / VM シリーズの豊富な導入実績から得たノウハウにより スムーズなサービス提供の実現
- 製品単体では対応しきれないエージェント非対応デバイスについても 考慮した網羅性のある設計
- MDR サービスにより、運用フェーズでの技術的な支援を実施し、 ランサムウェア被害発生時も安心の対応

コンポーネント

- Palo Alto Networks Cortex XDR Pro per Endpoint
- Palo Alto Networks Cortex XDR Pro per GB
- Palo Alto Networks Advanced URL Filtering
- Palo Alto Networks PA / VM シリーズ (Prisma Access)

関連するネットワンのマネージドサービス

- ネットワン SOC マネージド・ディテクション&レスポンス サービス

解決

- NDR により、ネットワーク上の異常な活動を検出し、潜在的な攻撃や 侵入を早期に特定することが可能
- EDR により、エンドポイントで発生したインシデントを検知し対応できる
- NGAV により、エンドポイントに近い位置で防御
- IoT/OT デバイスの不正通信は FW で遮断

おとりファイル
ランサムウェアが実行されても業務ファイル暗号化前に活動停止

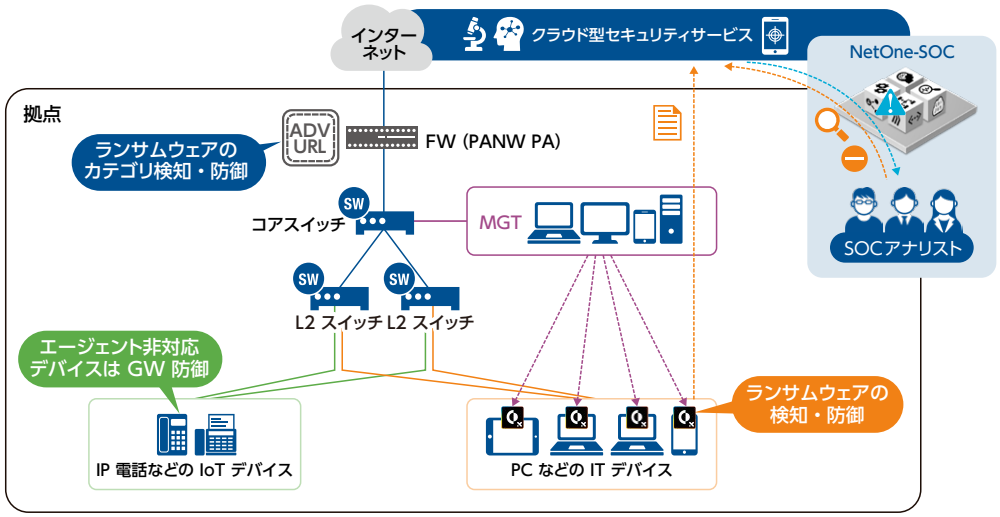
ファイル暗号化
ランサムウェアによる暗号化を即時に発見

ネットワークで阻止
ネットワークを介した暗号化活動を阻止して、攻撃元の IP アドレスを自動阻止

ふるまい検知
ランサムウェアが行う特定の行動を阻止

MBR 保護
Petya などの MBR 破壊型のランサムウェアによる破壊活動を阻止

アーキテクチャ



※Prisma Access も対応可能

SD-WAN による WAN 最適化 (Cisco SD-WAN)

インターネットも活用する WAN ネットワークへのマイグレーション

課題

- テレワーク、クラウドサービス利用増によりインターネット接続機会が増加
  従来のデータセンター集約ネットワークアーキテクチャの限界に直面
- アプリケーション毎のネットワークの最適化の必要性に対して、
  アプリケーションや回線品質状況の把握と最適な通信経路の実現が難しい
- ネットワーク設計の複雑化、運用管理の高度化要求に対し、高度なスキルを持つ
  ネットワーク管理者の維持が難しく、人のスキルに依存しない運用を実現したい
- 企業買収、グループ会社統合、拠点統廃合、新たなアプリケーションのリリースなど、
  企業の意思決定の迅速化に対して、追従できるネットワークになっていない

netone 匠エンジニアの推奨ポイント

- ローカルブレークアウトにより各拠点からのクラウドアプリケーションの
  通信を同拠点のインターネット回線を利用
- インターネット閲覧をダイレクトインターネットアクセスとし、
  セキュアウェブゲートウェイと連携する事でセキュリティの強化も可能
- IPアドレスやポート番号ではなく、DPI エンジンやシグネチャによる
  高度なアプリケーション識別
- ネットワーク上の遅延やパケットロス率を監視、その情報を活用した
  動的通信経路の切り替え
- GUIをベースとしたインテントネットワーキングの実現、ルータ個々ではなく、
  作りたいネットワークの全体ポリシー設計
- 仮想ルータ、回線論理分割機能によるセキュアな統合ネットワークの実現

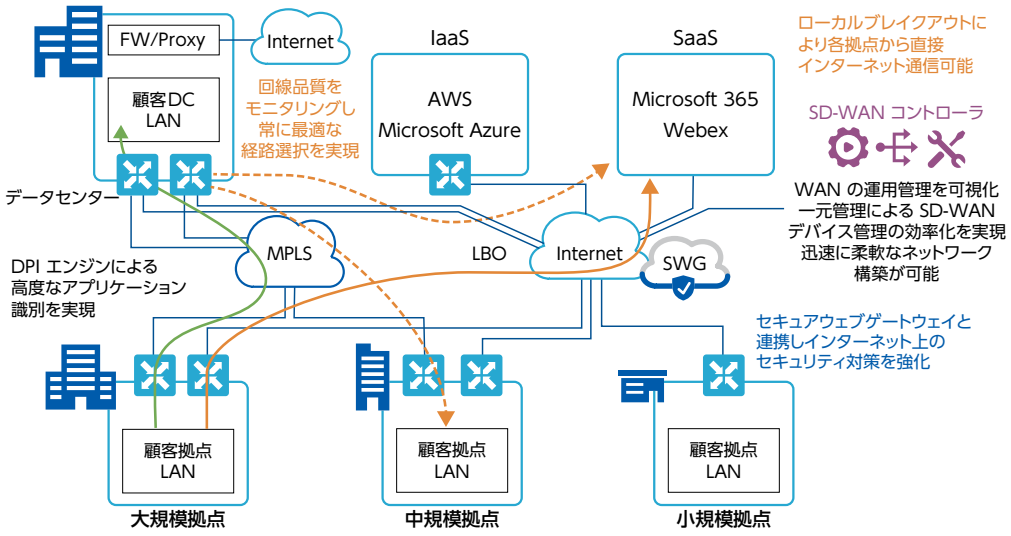
コンポーネント

- Cisco ISR 1100シリーズ
- Cisco Catalyst 8000 シリーズ
- Cisco SD-WAN
  (vManage、vBond、vSmart)

解決

- クラウドサービス利用拠点にはインターネット回線を導入、
  各ロケーションからアプリケーション毎に最適な通信経路を実現 Microsoft 365や
  ビデオ会議などによるデータセンターにおけるインターネット回線の
  ボトルネック解消と、閉域網の必要帯域増を抑止
- インターネット回線と閉域網を Active/Active で無駄なく効率的に利用
  管理者が設定したポリシーに従い、動的に最適な通信経路への切り替えを実現、
  各アプリケーションにおけるユーザエクスペリエンスを向上
- コントローラによる GUI での設定管理の一元化、ポリシーベースでの一括設定、
  ログの集中管理、クラウドへの回線品質や アプリケーション・通信フローの
  可視化機能など、専門知識がなくてもネットワークの日々の運用を可能に
- 仮想化技術にてセキュアかつ迅速なネットワーク統合へ対応 テンプレートや
  簡単なプロビジョニングによって迅速な拠点展開や機器故障時における交換対応を実現

アーキテクチャ



AWS:Amazon Web Services / Azure:Microsoft Azure

SD-WAN による WAN 最適化 (FortiGate SD-WAN)

インターネットも活用する WAN ネットワークへのマイグレーション

課題

- テレワーク、クラウドサービス利用増によりインターネット接続機会が増加
  従来のデータセンター集約ネットワークアーキテクチャの限界に直面
- インターネットへのアクセス増加により、ファイアウォールやプロキシなどの
  セキュリティ機器の負荷が増加している
- クラウドや社内システムが多様化するなかで、どのような通信が流れているか
  把握できていない
- 企業買収、グループ会社統合、拠点統廃合、
  新たなアプリケーションのリリースなど、企業の意思決定の迅速化に対して、
  追従できるネットワークになっていない

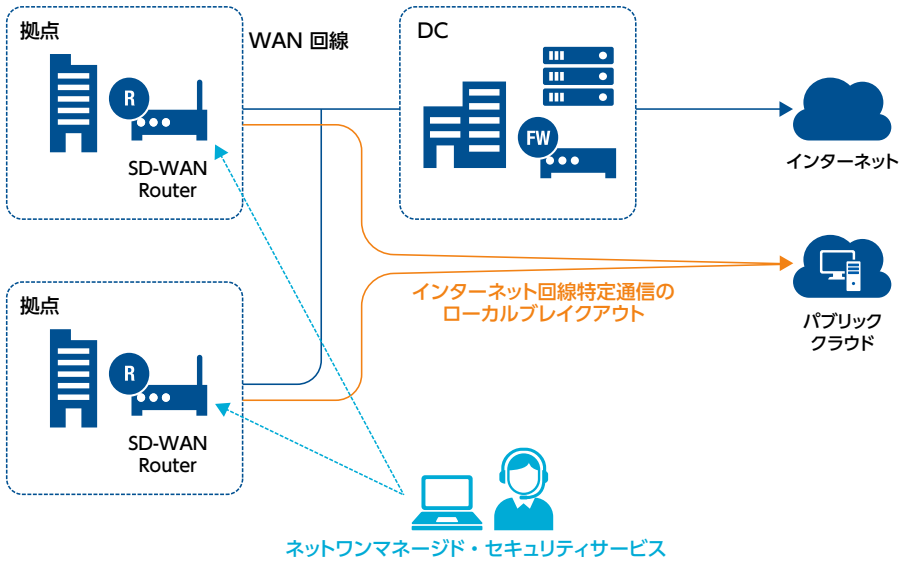
解決

- 拠点へのローカルブレイクアウトの導入
- 利用拠点にはインターネット回線を導入
  Microsoft 365 やビデオ会議などによるデータセンターにおけるインターネット
  回線のボトルネック解消と、閉域網の必要帯域増を抑止
- 拠点単位での導入といったスモールスタートができるため、
  拠点の増減に合わせた柔軟な対応が可能
- SD-WAN ルータにファイアウォールの機能をアドオンすることで、
  1台でセキュリティまでカバーすることができるため、
  管理工数、運用工数の削減が可能

netone 匠エンジニアの推奨ポイント

- トラフィックを常に分析し、悪意あるアクティビティを検知する
- SD-WAN ルータにファイアウォールの機能をアドオンすることで、
  1台でセキュリティまでカバーすることができる
- 複数の拠点に SD-WAN ルータを導入した場合でも、マネジメント機器を
  導入することで一元的な管理が可能となり、運用負荷を軽減することができる

アーキテクチャ



コンポーネント

- FortiGate 40-80シリーズ
- FortiGate 100-400シリーズ
- FortiGate 600シリーズ

関連するネットワンのマネージドサービス

- ネットワンマネージド・セキュリティサービス
  (FortiGate 100、200、400シリーズのみ対応)

AWS:Amazon Web Services / Azure:Microsoft Azure

キャンパス LAN (Cisco Catalyst 9000)

安定した稼働実績のあるキャンパスネットワークを導入したい

課題

- 安定したキャンパス LAN ネットワークを導入したい
- 運用負荷を軽減したい
- 端末やフロア増加による煩雑な継ぎ接ぎネットワークを改善したい
- 機器の故障時も業務が停止しないネットワークを導入したい

解決

- 実績のある構成とネットワーク機器にて構成された標準デザインを採用
- Cisco 社の Catalyst9000 シリーズで統一された構成であるため、均一のオペレーションで運用が可能
- 端末数やフロア数に応じた標準デザインであり拡張性が高いネットワーク
- Stack や LACP といった冗長機能により機器の故障時もネットワークが全体停止しない設計

netone 匠エンジニアの推奨ポイント

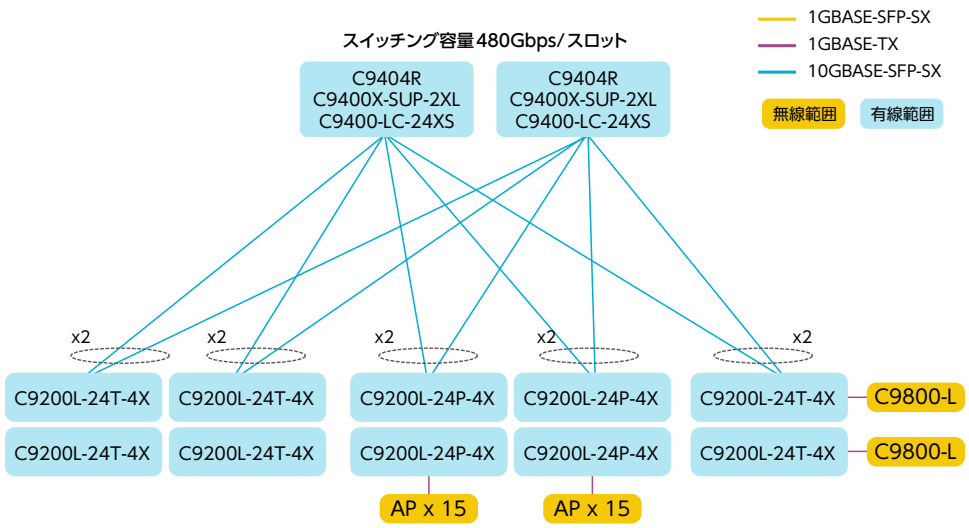
- 稼働実績のある設計を採用しているため、安定したネットワーク環境を導入できる
- Stackwise や Stackwise Virtual といった Catalyst9000 の筐体冗長機能による高い耐障害性
- カスタム機能をアドオンしやすいスタンダードなテクノロジーを使用した設計
- シンプルであり運用がしやすいネットワーク構成

コンポーネント

- Cisco Catalyst 9600 シリーズ
- Cisco Catalyst 9400 シリーズ
- Cisco Catalyst 9300 シリーズ
- Cisco Catalyst 9200 シリーズ

アーキテクチャ

1フロア想定規模	500～1000ユーザ	想定VLAN(SVI)数	100
最大フロア拡張	5フロア	冗長技術	筐 体：STACK リンク：LACP
コア最大スイッチ容量	480Gbps		



統合キャンパスネットワーク管理 (Cisco Catalyst Center)

IT インフラの重要性が増しシステムが複雑化する中、キャンパスネットワーク運用を最適化

課題

- クラウド利用やセキュリティの考慮などシステムが複雑化・ITの重要性が増しているが、それに適合したネットワーク運用の変革が進んでいない
- ナレッジベースや手順書による対応の限界、複雑な問題に対処できるエンジニアの要員確保が難しい
- ハイブリッドワークにおけるリモートからのトラブルシューティング方法が確立できていない
- ネットワークに問題がないことの証明も含め、依然として生産性のない障害対応に工数とコストを費やしている
- 誤った設定や変更、メンテナンス作業中のミスなどの人為的ミスが減らないネットワークが意図したポリシーで稼働しているか判断がつかない

netone 匠エンジニアの推奨ポイント

- ネットワークデバイスからストリーミングテレメトリでデータを受信、アプリケーションパフォーマンスやユーザー接続に関する状態をリアルタイムでモニタリング可能
- AIやMLなどの先進的なテクノロジーを活用、パストレースの可視性とガイド付き障害切り分けにより、問題の原因を迅速かつ正確に特定することが可能、また発生した問題によっては、自動対処も可能
- インテリジェントキャプチャーにて自動でパケットキャプチャを取得、ネットワーク接続に関わる問題を自動で分析
- デバイスの自動認識、構成バックアップおよび復元、ゼロタッチプロビジョニングおよび ソフトウェアイメージ管理機能にて、ネットワーク全体のセキュリティとコンプライアンスを維持

コンポーネント

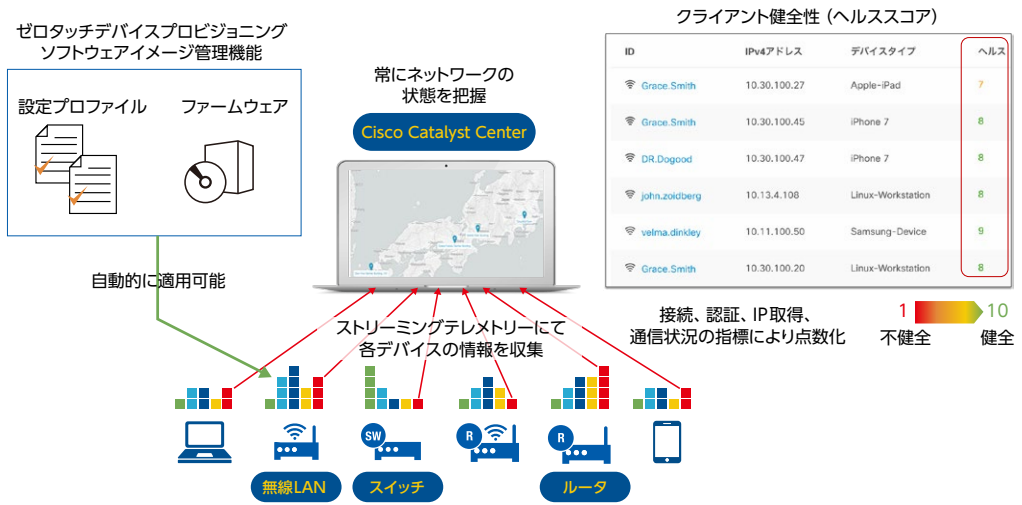
- Cisco Catalyst Center

※統合ネットワーク管理を実現するには、Cisco Catalyst Center 対応デバイス（スイッチ、ルータ、無線LAN）かつ Catalyst Center ソフトウェアライセンスサブスクリプションが必要です。

解決

- Cisco Catalyst Center を導入、ネットワークの可視化と自動化を行い、抜本的な運用プロセスの改善を行う
- 障害発覚後から人が情報収集するのではなく、常に Catalyst Center がクライアントの状態を含めてネットワーク状態を把握、リモートからのトラブルシュートを大幅にサポートし、対応にかかる時間を大幅に削減
- Catalyst Center がネットワークの健全性を可視化、健全性に影響を与える「原因・インパクト・対応策」を確認しての 対応が可能、また障害が発生する前の予防措置を講じる事も可能
- Catalyst Center が現在稼働している機器の構成管理（構成図、バージョン、コンフィグ、シリアル、ライセンスなど）を実施不完全な管理ドキュメントの維持からの脱却
- 機器増設、多くのデバイスの設定変更、バージョンアップ作業を人為ミスなく、夜間などでの計画的な実施が可能

アーキテクチャ



統合キャンパスネットワーク管理 (HPE Juniper Mist)

IT インフラの重要性が増しシステムが複雑化する中、キャンパスネットワーク運用を最適化

課題

- クラウド利用やセキュリティの考慮などシステムが複雑化・ITの重要性が増しているが、それに適合したネットワーク運用の変革が進んでいない
- ナレッジベースや手順書による対応の限界、複雑な問題に対処できるエンジニアの要員確保が難しい
- ハイブリッドワークにおけるリモートからのトラブルシューティング方法が確立できていない
- ネットワークに問題がないことの証明も含め、依然として生産性のない障害対応に工数とコストを費やしている
- 誤った設定や変更、メンテナンス作業中のミスなどの人為的ミスが減らないネットワークが意図したポリシーで稼働しているか判断がつかない

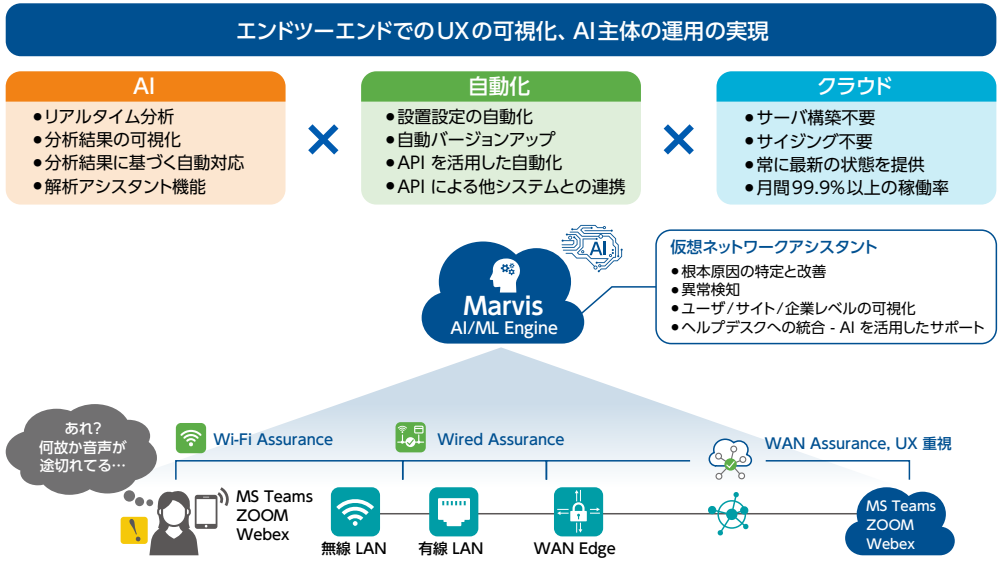
解決

- Juniper Mist AI を導入し、ネットワークの可視化と AI によるトラブルシューティングにより抜本的な運用プロセスの改善を行う
- 障害発覚後から人が情報収集するのではなく、常に Juniper Mist AI がクライアントの状態を含めてネットワーク状態を把握、リモートからのトラブルシュートを大幅にサポートし、対応にかかる時間を大幅に削減
- Juniper Mist AI がネットワークの健全性を可視化、健全性に影響を与えている『原因・インパクト・対応策』を確認して対応が可能、また障害が発生する前の予防措置を講じる事も可能
- 機器増設、多くのデバイスの設定変更、バージョンアップ作業を人為ミス無く、夜間など計画的に実施可能

netone 匠エンジニアの推奨ポイント

- ネットワークデバイスからストリーミングテレメトリでデータを受信、アプリケーションパフォーマンスやユーザー接続に関する 状態をリアルタイムでモニタリング可能
- AIやMLなどの先進的なテクノロジーを活用、パストレースの可視性とガイド付き障害切り分けにより、問題の原因を迅速かつ正確に特定可能、また発生した問題によっては、自動対処も可能
- 端末の障害発生時などに自動でパケットキャプチャを取得、AI を活用しネットワーク接続に関わる問題を自動で分析
- デバイスの自動認識、構成バックアップおよび復元、ゼロタッチプロビジョニングおよび ソフトウェアイメージ管理機能にて、ネットワーク全体のセキュリティとコンプライアンスを維持

アーキテクチャ



コンポーネント

- Juniper Mist AI

※統合ネットワーク管理を実現するには、
Juniper Mist AI 対応デバイス（スイッチ、ルータ、無線 LANアクセスポイント）かつ
ソフトウェアライセンスサブスクリプションが必要です。

SDN による DC ネットワーク最適化 (Cisco ACI/Palo Alto Networks PAシリーズ/F5/Red Hat Ansible)

IT インフラの重要性が増しシステムが複雑化する中、DC ネットワーク運用を最適化

課題

- ネットワーク内で管理が必要な機器が多く、日々の運用負荷が高い
- ネットワークの高度化、複雑化が進み、管理者が迅速にネットワークを構築できない
- ファイアウォールやロードバランサーなどの機器を柔軟に利用したいが、既存のネットワーク構成を変更することが難しい
- 各機器ログ取得、設定変更などの定常業務や構成変更で対象が多く時間がかかり、作業ミスも発生しやすい

解決

- 全機器に対する設定変更、監視、可視化を APIC から一元的に提供することで個別管理から脱却、管理者の負荷を軽減
- 各機器を相互接続するポリシーを定義することで、ネットワークの知識有無にかかわらず迅速なネットワーク構築が可能
- 必要に応じてファイアウォールやロードバランサーにトラフィックをリダイレクトすることで提供サービスの切り替えが可能
- 構成管理ツールによる繰り返し実施する定常業務の自動化で工数を削減、ヒューマンエラーも軽減

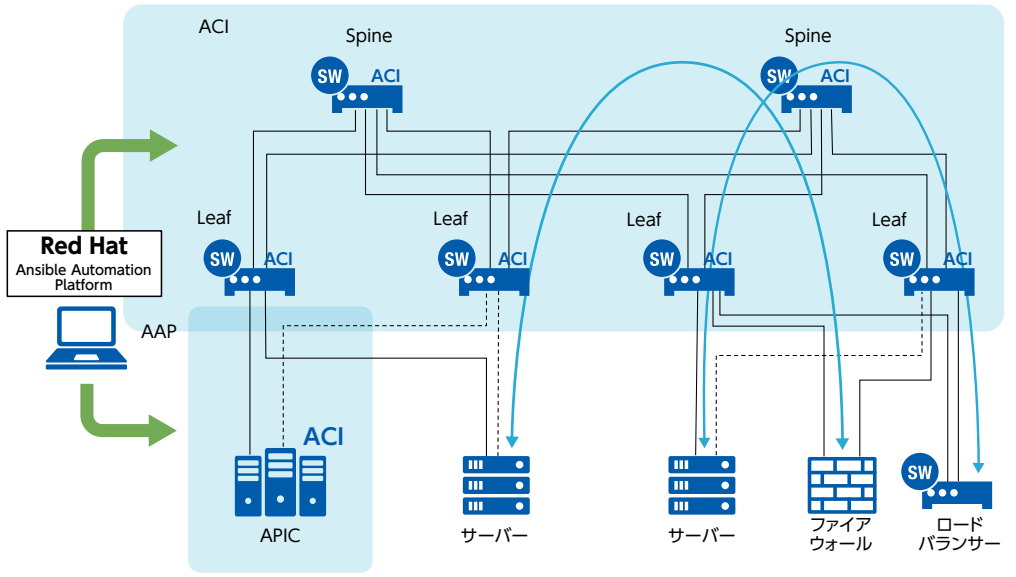
netone 匠エンジニアの推奨ポイント

- SDN コントローラー (APIC)による機器の一元管理
- 管理者のインテントに近い形で各種設定をポリシーとして定義可能
- 定義したポリシーの再利用が可能で管理者の運用負荷を軽減
- L4-L7 連携機能でネットワーク構成に影響を与えずトラフィックをリダイレクト
- 構成管理ツールである Ansible を利用した定常業務や構成変更の自動化

コンポーネント

- Cisco APIC
- Cisco Nexus 9000シリーズ
- Palo Alto Networks PAシリーズ
- F5 BIG-IPシリーズ
- Red Hat Ansible Automation Platform (AAP)

アーキテクチャ



オンプレミス VDI による Hybrid Work 実現 (Omnissa Horizon)

セキュアかつユーザ利便性が向上するリモートでの働き方を実現

課題

- 自然災害やパンデミックなど、出社が困難な状況にも事業継続可能な働き方の仕組みが必要
- セキュアかつユーザーの利便性が向上するリモートでの働き方を実現したい
- スモールスタートで導入費用を削減しつつ、将来的には適用範囲を広げたい
- デジタルワークスペースの状態監視、権限管理、新規作成/削除などの運用負荷を軽減したい
- FAT PC のセキュリティパッチやアプリケーションなどのバージョンアップの統制がコントロールしにくい

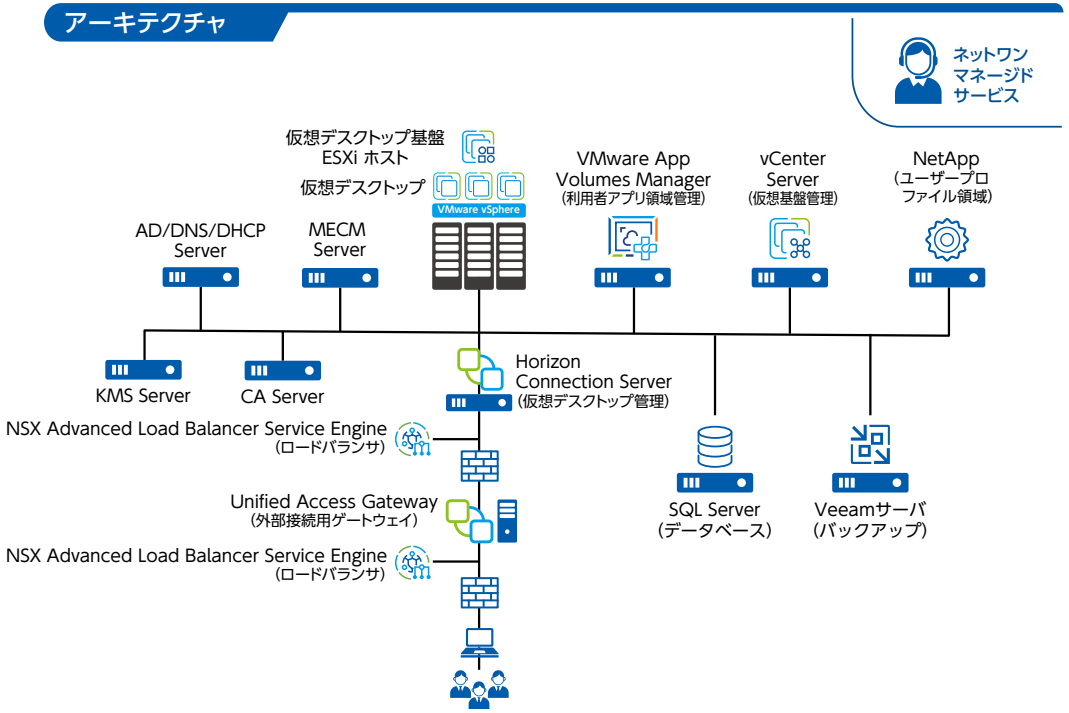
解決

- 仮想デスクトップを導入することで、場所や環境に影響を受けず、どこでも業務可能
- 管理者側でアプリケーションの提供や制限でき、利便性とガバナンスの両立が実現
- スモールスタートでき、ユーザーの増減にも柔軟な対応が可能
- 管理ツールにより新規払い出しや削除、権限変更など 日々の運用管理とメンテナンスの一元管理が可能

netone 匠エンジニアの推奨ポイント

- ユーザプロファイル方式に FSLogix を利用、マウント処理によるログイン / ログオフ処理の高速化
- デスクトップ展開方式インスタントクローンを採用、ストレージ容量削減と高速プロビジョニングを提供
- アプリケーション配信・保持方式を VMware App Volumes にすることで管理者にてアプリケーションを一元管理 マスターイメージ数も最小限に抑え、リフレッシュ時にもアプリケーションを保持可能
- リモートアクセス環境も Omnissa Horizon にて展開可能 RADIUS/SAML などで認証サービス連携も実現

アーキテクチャ



コンポーネント

- サーバー Cisco UCS Series など
- ストレージ Pure Storage FlashArray など
- ファイルサーバ NetApp FAS など
- バックアップストレージ Dell Technologies PowerProtect DD など
- Omnissa Horizon
- VMware vSphere
- VMware App Volumes
- FSLogix

関連するネットワンのマネージドサービス

- WSI 運用 (VDI 運用) サービス (ネットワン運用サービス)

3Tier 仮想基盤によるリソース最適化 (Cisco/Dell Technologies/NetApp/Pure Storage/Veeam/Veritas)

オンプレミス環境での柔軟な ICT 共通基盤の実現

課題

- 仮想基盤を導入しつつ、各リソースを個別拡張、運用管理したい
- 共通基盤としてリソースが共有可能な、柔軟な環境がほしい
- ベアメタルサーバーのリソースを、仮想化によって有効活用したい
- 既存のネットワークの空きポートを使って仮想基盤の増強のコストを抑えたい
- 低コスト化を図るために複数のメーカーから選択したい

netone 匠エンジニアの推奨ポイント

- サーバー、ストレージ、バックアップストレージ、バックアップサーバーを
  スケールや用途に合わせた仮想基盤として構成可能
- ストレージはファイル、ブロックと用途に合わせて最適なモデルを選択できる
- バックアップは下記構成のどちらか一方を選択可能、障害復旧対策を提供
  ① バックアップソリューション（例：Veeam+DataDomain）
  ② ストレージレプリケーション（例：2台構成によるレプリケーション）

コンポーネント

- サーバー　Cisco UCS、Dell Technologies PowerEdge
- ストレージ　NetApp FAS、Pure Storage FlashArray、Dell Technologies PowerStore
- バックアップストレージ　Dell Technologies PowerProtect DD
- バックアップサーバー　Veeam、Veritas
- データネットワーク　Cisco Nexus など
- 管理ネットワーク　Cisco Catalyst など

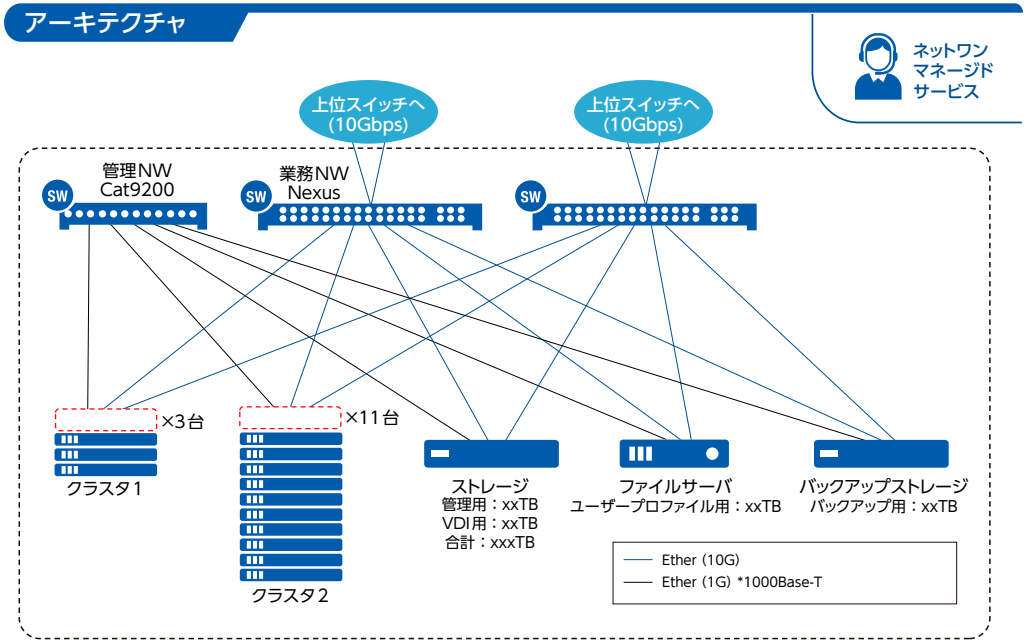
関連するネットワンのマネージドサービス

- 仮想化基盤運用サービス（ネットワン運用サービス）

解決

- サーバー、ストレージ、バックアップのリソースを個別に管理でき、
  利用状況に応じた拡張が可能
- リソースを論理分割でき、システムごとに仮想基盤を分けつつも、
  物理環境は共有できる
- ベアメタルサーバから仮想化基盤へ移行することで CPU・メモリリソースを
  有効利用、余剰リソース低減が可能に
- 既存ネットワーク構成に合わせて機器選定でき、仮想基盤拡張時の機器導入を
  最小限に抑えられる
- 特定メーカの機器に制限されることなく、自由な選択が可能

アーキテクチャ



HCI* による運用効率化 (Dell Technologies / Nutanix) *HCI：ハイパーコンバージドインフラストラクチャ

仮想基盤のアップグレード対応および運用負荷を軽減

課題

- バージョンアップや導入時、HW/SW/FW/ドライバーの組み合わせを都度確認する必要があり、仮想基盤の準備やアップグレードに時間とコストがかかる
- 仮想基盤の新規展開時の作業手順が多く、常時待機している必要がある
- 仮想基盤のハードウェアの設置スペースに制限がある
- 各機器のサポートサービスがメーカーごとに分かれており、障害時対応が煩雑

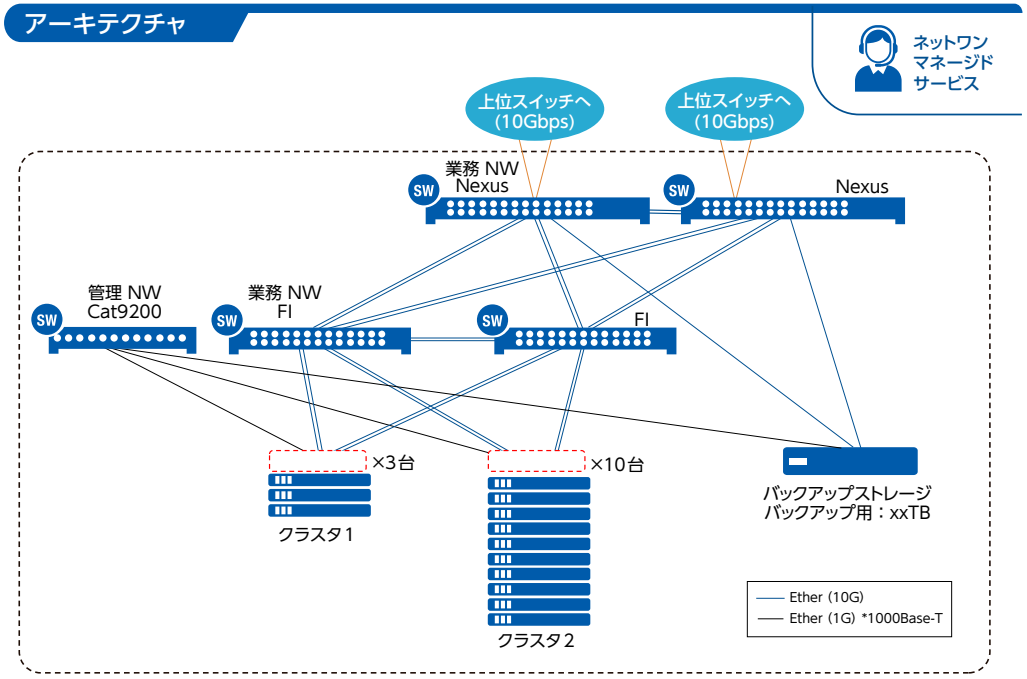
解決

- HCIは関連コンポーネントが動作確認済みのパッケージで提供されるため、導入時やアップグレード時に掛かる調査確認時間を大幅に削減可能
- パッケージ化されたコンポーネントのため新規展開が簡単で作業手順が簡素化
- 物理的な機器数が削減でき、物理スペース縮小、消費電力の削減、資産管理コストも低減
- サポート窓口の統合により、問題解決のスピードが向上

netone 匠エンジニアの推奨ポイント

- 初期構築は専用ウィザードから簡単に実施でき、統合仮想基盤がすぐに利用可能
- バージョンごとに HW/SW/FW/ドライバーなど関連するコンポーネントが検証済みパッケージで提供
- アップグレード、ノード追加などの運用は管理インターフェースから簡単実行
- 2RU ～ 4RU 程度の大きさに統合仮想基盤が集約できる
- 障害時にはサーバとストレージの切り分けが不要になり、HCI としての動作確認に集約できる

アーキテクチャ



コンポーネント

- Dell Technologies VxRail
- Nutanix
- バックアップストレージ
  Dell Technologies PowerProtect DD
- データネットワーク
  Cisco Nexus、Cisco Fabric Interconnect など
- 管理ネットワーク　Cisco Catalyst など

関連するネットワンのマネージドサービス

- 仮想化基盤運用サービス（ネットワン運用サービス）

クラウド電話ソリューション (Cisco Webex Calling)

新しい働き方、コミュニケーションを実現する電話ソリューション

課題

- ハイブリッドワークの導入により、電話の在り方が変化した
- 会社だけではなく、自宅や外出先でも代表番号の利用が必要
- BYOD 端末利用によって電話利用料の負担が上がってしまう
- 出社しないと電話の対応ができない
- オンプレミス PBX による金額負担 (バージョンアップコスト)

解決

- 固定電話から脱却し、スマートフォン、PC などで
  自宅や外出先からでも会社の電話番号を利用できる
- BYOD 端末からでも会社の電話番号は会社負担になる ※データ通信は負担が必要
- サードパーティの電話帳により、BYOD 端末からでも番号の把握が可能
- チャット、Web会議と連動により1アプリで働き方を柔軟にする

netone 匠エンジニアの推奨ポイント

- Cisco ZTN ソリューションとの連携
- Webex クライアントサポートによって運用面も安心

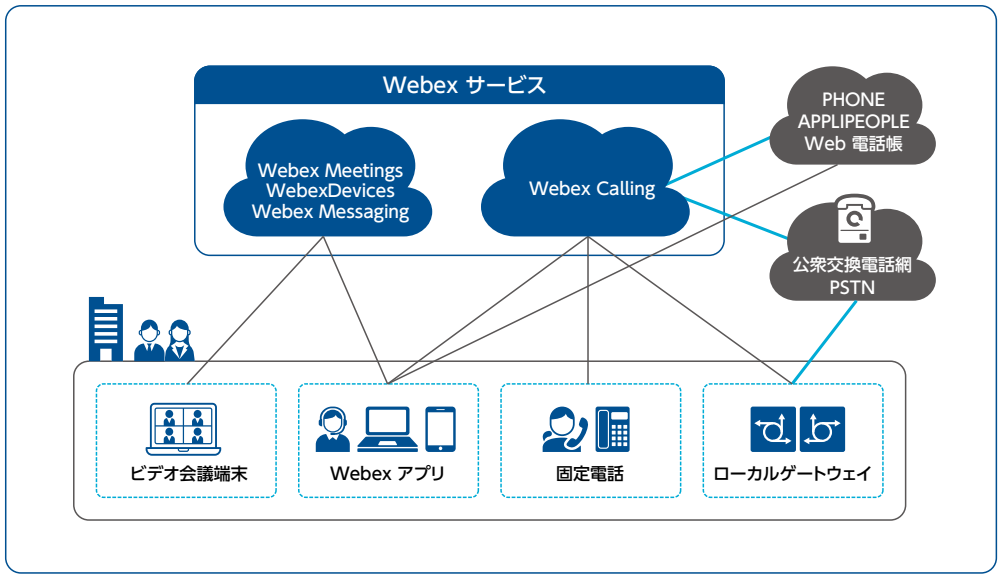
コンポーネント

- Cisco Webex Calling
- Phone Appli社 Phone Appli People

関連するネットワンのマネージドサービス

- ネットワン Webex クライアントサポート

アーキテクチャ



OT ネットワークセキュリティ強化 (Forescout/Palo Alto Networks)

工場ネットワークにおけるネットワーク構成の把握・セキュリティ対策強化

課題

- 工場・プラントでネットワーク構成変更や更新に応じた資料が更新されておらず、現在のネットワーク構成を把握できていない
- 構築当時の担当者が異動などの事情で不在、不可解な構成があっても理由が不明
- 可用性が最重視されるため、セキュリティ強化対策であってもシステムへの影響発生が許されず、安易に実行できない
- IT/OT ネットワークに接続されている資産が把握できておらず、不正デバイスが接続されても異常検知できない

netone 匠エンジニアの推奨ポイント

- IT/IoT ネットワーク領域では、Intelligence スイッチや NGFW などと連携した デバイスの制御が可能
- 収集したデータからセキュリティリスクを診断
  組織のセキュリティポリシーを定義することで、ポリシー外のデバイスをリアルタイムで異常検知
- インシデントの調査に時間を費やすことが無くなるので、初期対応を迅速に行える
- OT 環境のネットワーク構成図の作成、脆弱性検知、トラフィック可視化による change ログの確認など、より詳細な可視化機能も提供可能

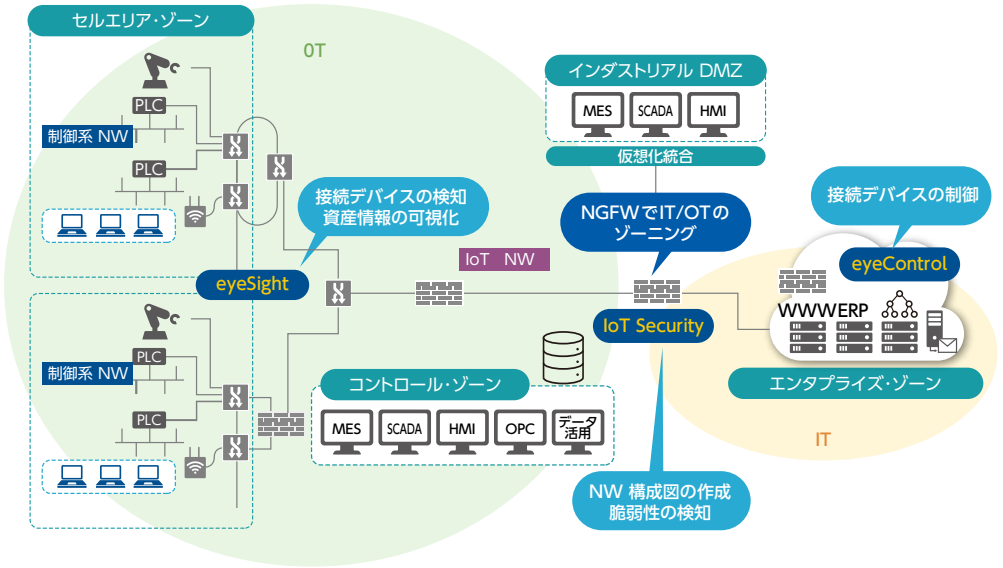
コンポーネント

- Forescout eyeSight シリーズ Forescout eyeControl シリーズ
- Palo Alto Networks IoT Security Subscription

解決

- 組織内の IT/OT ネットワークに対して現在接続されている資産情報を可視化、どんなデバイスがどこに接続されているかを把握することが可能に
- 過去の経緯にとらわれずに、今現在のリアルタイムの接続情報を継続的にモニタリングすることが可能
- スイッチのミラーポートを利用して、システム内の通信をキャプチャするなど Passive な手法を活用することで、システムの可用性に影響を与えることなく、調査できる
- 接続されている機器の IP アドレス、MAC アドレス、OS、バージョン、アプリケーション一覧などを洗い出し、組織のセキュリティポリシー外のデバイスを検知、通知することが可能

アーキテクチャ



HC（ヘルスケア）ランサムウェア対策ソリューション（Cisco SNA）

院内の通信を常時監視するセキュリティ対策で安心・安全な医療を提供

課題

- 安心・安全な医療提供体制を構築したい
- セキュリティ対策をしたいが、ノウハウが無い。昨今のサイバー攻撃に対応できる対策を打ちたい
- きりのないセキュリティ対策の中で、最も投資効果の高い網羅的な対策を選択したい
- セキュリティ運用のできる人財不足に悩んでいる

netone 匠エンジニアの推奨ポイント

- トラフィックを常に分析し、悪意あるアクティビティを検知する
- 機械学習や行動分析によって未知の攻撃に対しても効果を発揮する。万が一侵害されてしまった後の調査にも活用できる
- NW機器単位でミラーポートを設定する必要がなく、Netflow 対応機器であれば不審な挙動を検出するためのデータ収集が可能。そのため、さまざまなエリアを比較的容易に検知対象にすることもでき、柔軟に対策を展開できる
- SNA はグループとポリシーを組み合わせて定義できるため部門間で異なるポリシー設計が可能、これによって検出精度を高めて過検知/誤検知を抑制できる

コンポーネント

- Cisco Secure Network Analytics

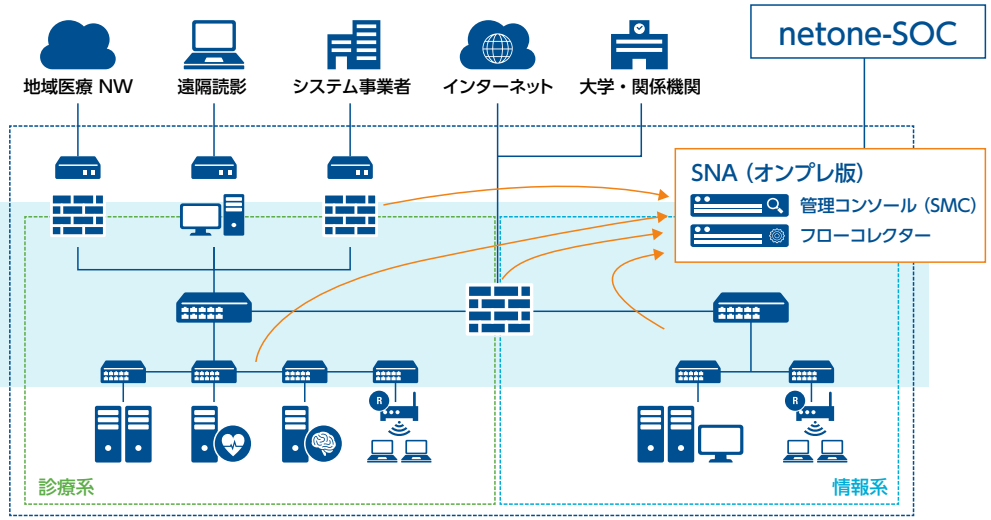
関連するネットワンのマネージドサービス

- ネットワン SOC マネージド・ディテクション&レスポンスサービス（SNA）

解決

- NW内の通信の“振る舞い”を監視することで、通常とは異なる不審な通信があった際に検出。また、その後の分析も可能なため、異常の原因を把握することができれば、被害拡大の抑止や再発防止に繋げられる
- EDR 製品とは異なり、各端末に専用ソフトウェアを導入する必要がないため（エージェントレス）、医療システムや端末のパフォーマンスに影響を与えずに院内のセキュリティ強化を実現可能
- ネットワン SOC サービスによって24 時間 365 日プロのアナリストが監視することで不審なふるまいを検出。また、ケースに応じて緊急隔離も可能なため、被害を最小限に抑えられる。人材不足に悩むお客様の運用負荷も軽減できる

アーキテクチャ



放送 DX を実現するネットワーク基盤 (Cisco IP Fabric for Media)

4K、8K 放送の大容量通信に対応できる放送 IP ネットワークを実現

課題

- 4K、8K 放送で大容量通信が求められるが、既存の SDI の物理構成では伝送速度、距離、ケーブル重量、帯域幅密度などで限界が目前
- 既存 SDI では物理的な制限に依存度が高く、構成変更や拡張にも制限が多い
- SDI で構成された放送システムは独自システムとして動作しており、他の IT システムとの連携が乏しい
- 放送局内でそれぞれのスタジオでシステムが独立しており、利用していない期間に他システムで活用することができていない、リモートからの操作なども制限されていたりする

netone 匠エンジニアの推奨ポイント

- NBM (Non-Blocking Multicast) によってオーバーサブスクリプションを考慮したフロー制御
- 放送業界プロファイル PTP 対応による高精度な時刻同期を提供
- 管理ソフトウェア(Cisco Nexus Dashboard Fabric Controller) による可視性、運用性向上
- IP ネットワーク化による他システムとの連携性、スモールスタート可能な高い拡張性、論理分割によるリソースシェアの実現

  Ethernet テクノロジー導入による、広帯域化、物理的な軽量化、高密度化の実現

コンポーネント

- Cisco Nexus 9000 シリーズ

解決

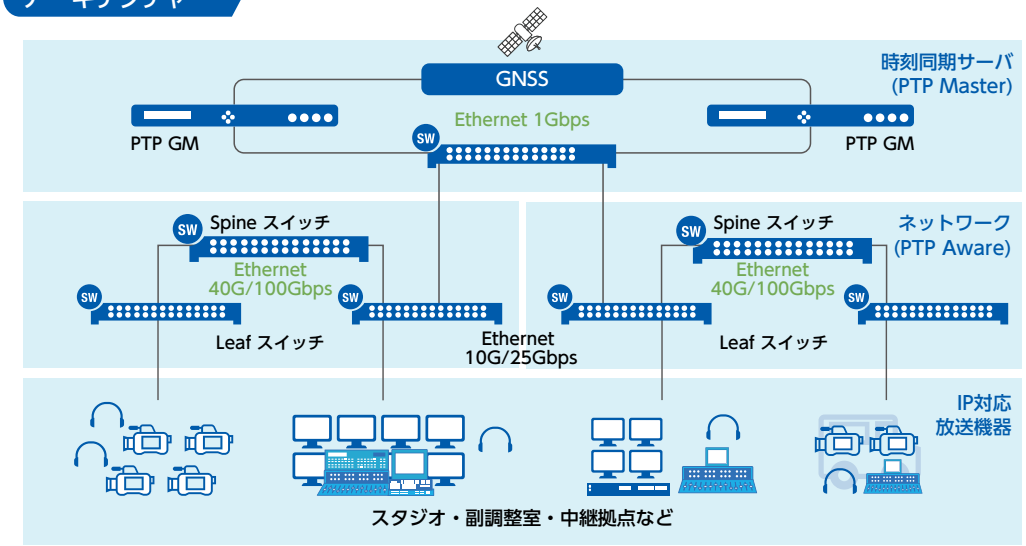
- 同じ転送量に対する機器の大きさも1/7ほどに物理的なサイズを縮小

  IP は1 インターフェースで現在 400 Gbpsまで伝送可能（12G SDIとの比較で33 倍以上高速）SDI は最長 100m まで、IPでは最大 80 kmまで伝送可能、重量も1/3 程度
- スモールスタートで始め、必要に応じて投資をすることにより柔軟な投資計画が実現
- ネットワーク機器やその管理ソフトウェアは他システムと連携するための仕組みを保有

  インターネットやクラウド、スマートフォンなど同時再配信サービスのシームレスな提供が可能に
- IP ネットワークのルーティング/スイッチング動作による論理分割で 1 つのサブで複数スタジオを管理可能

  リモートプロダクションの実現により、遠隔の制作環境を IP を通じて局内設備のように扱うことができ、VE などのエンジニアは常に現場に出向く必要がなく、柔軟な働き方が可能に

アーキテクチャ



ガバメントクラウド接続サービス（Amazon Web Services）

自治体のガバクラ接続と運用を支える、柔軟・高品質なマルチクラウド接続サービス

課題

- 基幹業務システムのガバメントクラウド接続の準備や対応が遅れている
- 接続方式（単独接続・共同接続）や閉域回線・クラウド接続サービス（LGWAN 統合・専用線）など選択肢が多く、判断が難しい
  ガバメントクラウド移行に伴い、ネットワーク運用業務が複雑化し、既存システムベンダーでは対応が困難なケースがある
- マルチクラウド（Amazon Web Services など）にまたがる接続が必要となり、運用設計や管理体制整備が追いつかない
- セキュリティ・パフォーマンス・コストのバランスを取りながらの運用体制構築が難しい

netone 匠エンジニアの推奨ポイント

- 複数クラウド（マルチクラウド）への柔軟な接続と運用に対応した「ガバメントクラウド接続運用サービス」を提供
- 冗長性、帯域幅、品質（SLA）など、要件に応じた最適設計が可能
  運用管理補助者の設置を前提とし、ネットワーク運用業務を包括的に支援
- BGP ルーティング、Transit Gateway 内部のルーティング、基幹業務システムの名前解決などの高度な接続技術にも対応
- LGWAN 統合・個人番号系など、既存の自治体ネットワークとの親和性を確保

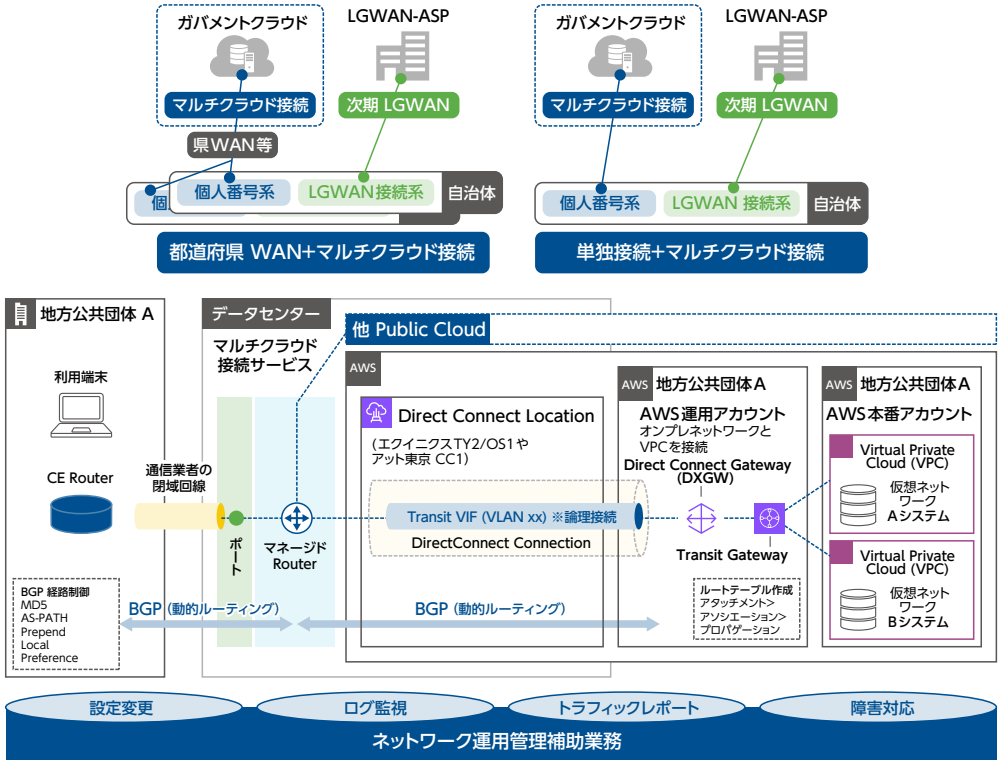
コンポーネント

- AWS Direct Connect
- AWS Transit Gateway
- Amazon Virtual Private Cloud
- Amazon Route 53

解決

- ガバメントクラウドへの確実な接続を実現し、標準化対応を期限内に完了可能
- マルチクラウド環境でも安全かつ効率的なネットワーク運用を実現
- システムベンダーでは対応できないネットワーク領域を補完し、業務の空白を解消
- ネットワーク管理の負担を軽減し、運用コストやトラブル対応リスクを最小化
- 自治体全体での DX 推進や窓口業務のクラウド活用をネットワーク面から支援

アーキテクチャ



ガバメントクラウドファイル連携（Amazon Web Services）

自治体の基幹業務クラウド移行に伴う高信頼・高可用なファイル連携基盤を提供

課題

- 現行の庁内データ連携機能は基幹業務システムのクラウド移行後も必要だが、新たな環境に最適化されていない
- 基幹業務システム移行後、自治体～ CSP 間のネットワーク帯域が枯渇する恐れがある
- 移行スケジュールと連携基盤の提供スケジュールの整合性がとれていないケースがある
- AWS 外デバイスへの管理ツール導入や認証・鍵管理の負担が発生しやすい
- 新たな IdP 基盤運用が追加され、運用コストや管理負担が増加する可能性がある

解決

- CSP 内ファイル連携基盤の導入により、自治体～ CSP 間の帯域問題を解消
- AWS S3 の活用により、従来比で耐久性と可用性が大幅向上
- 認証に IAM や SSH 鍵を利用することで認証運用負荷を軽減
- ファイル連携通信や格納データは暗号化を行い、安全かつ効率的なファイル連携を実現

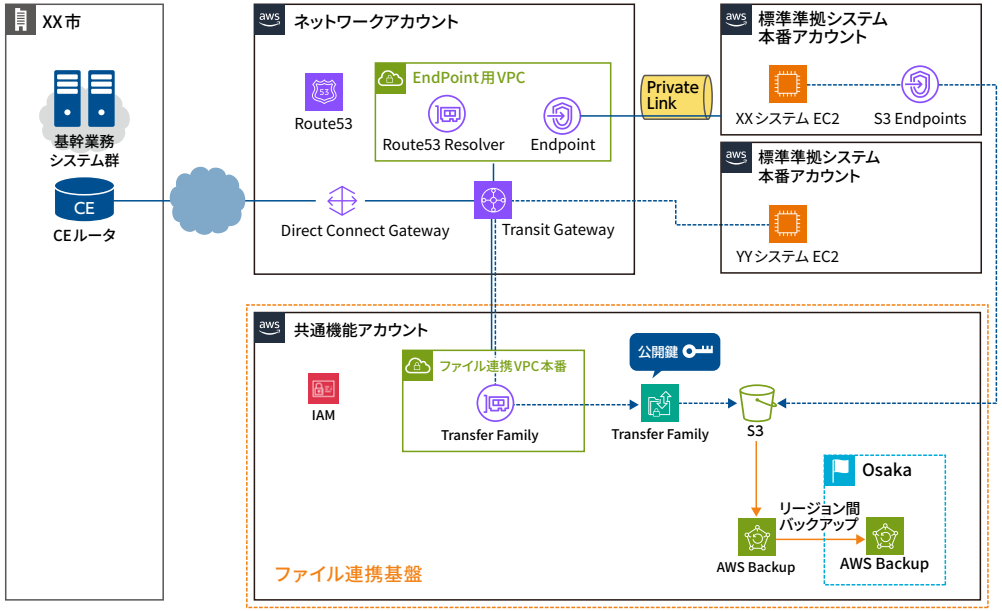
netone 匠エンジニアの推奨ポイント

- 基幹業務が稼働する CSP 内にファイル連携基盤を構築することで CSP 内に閉じた形で庁内データ連携機能を提供
- AWS のS3 をファイル置き場として活用し、高い耐久性・可用性・拡張性を確保
- 基幹業務システムの接続方式ごとに柔軟なファイル連携方式（クロスアカウント S3 アクセス、Transfer Family アクセス）を提案

コンポーネント

- Amazon Virtual Private Cloud
- AWS Transfer Family
- Amazon Simple Storage Service
- AWS Identity and Access Management
- AWS Backup
- AWS Key Management Service
- Amazon CloudWatch

アーキテクチャ



端末論理分離ソリューション（Security Platform）

1台の端末で安全に業務を使い分けられる、教育向けセキュアな端末利用

課題

- 端末利用におけるファイルの情報漏洩リスクを十分に制御できていない
- 校務用・学習（指導者）用といった複数端末を用途別に管理しており、コスト・管理負荷が大きい
- ファイルの持ち出しや共有に関して統制の取れた運用ができておらず、内部統制上の懸念がある
- インシデント（ファイルの漏洩）発生時、調査に多大な時間を要する

解決

- 情報漏洩リスクを抑えつつ、必要なデータを安全に共有できる仕組みを構築
- 1台のWindows端末で、校務・学習（指導者）など複数業務に安全に対応でき、端末数を削減、コストを削減
- セキュアなファイル運用と暗号化機能により、強固なセキュリティ対策を実現
- インシデント発生時、容易な運用で迅速なインシデント調査が可能

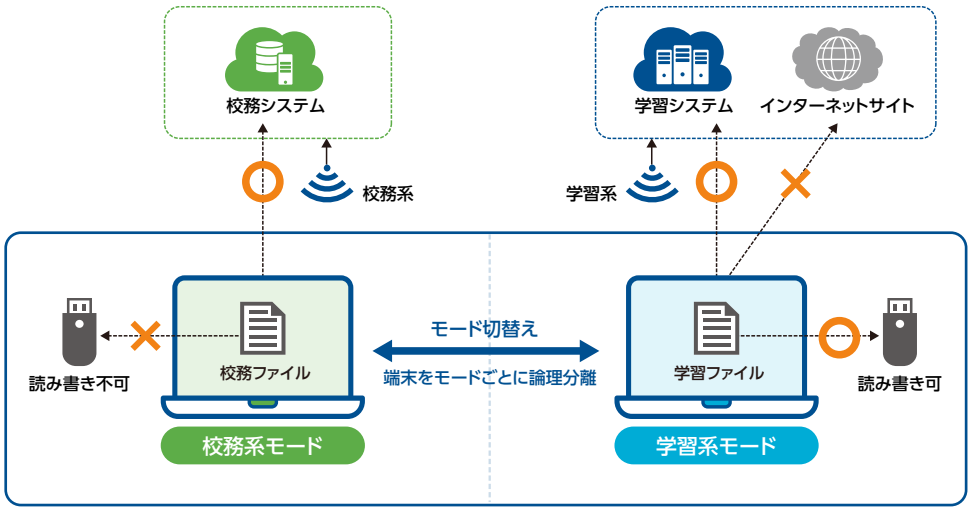
netone 匠エンジニアの推奨ポイント

- 端末起点でファイル持ち出しにおける情報漏洩対策が可能
- 端末に複数モードを定義、モードごとに業務に合わせたセキュリティ対策が可能
- 利用中のモードを壁紙で視覚的にわかるようにし、利用者が迷わない運用が可能
- 校内領域／校外領域を明確に区分し、ファイル持ち出し時には自動で暗号化を適用
- 校外へファイル持ち出しが必要な場合、承認制フォルダを活用し安全に運用
- 端末の操作履歴を 5W1H 形式でわかりやすく管理し迅速なインシデント調査が可能

コンポーネント

- ハミングヘッズ Security Platform（セキュリティプラットフォーム、略称 SeP）
- Security Platform オプション
  セパレートオプション、ストレージエンクリプションオプション、エンクリプションオプション、トレーサオプション、イントラネットオプション

アーキテクチャ



校務系モード設定		学習系モード設定
校務系のみ通信可	通信先	学習系/インターネットへ通信可
書き込み/読み込み”不可”	外部記憶媒体	書き込み/読み込み”可”
校務システムのみ	ファイルアップロード	許可サイト（学習システムなど）のみ
制限なし	アプリ起動制限	指定アプリのみ起動可

net one

ネットワンシステムズ株式会社

〒100-7024 東京都千代田区丸の内 2-7-2 JPタワー
https://www.netone.co.jp/