net one

Net One Security Solution & Service Guide

いま、求められる新たなセキュリティ要件

今日のビジネス環境の変化と新技術の採用で組織のインフラやセキュリティ環境は急速に変化しています。
組織では持続的な成長のためにデジタル戦略を実行し、事業活動のニーズに即応するための多種多様なクラウド技術やサービス活用の促進と同時に、
確実なセキュリティ対策を講じながらビジネスに貢献可能なITインフラを実現しようとしています。

DX（デジタルトランスフォーメーション）への対応

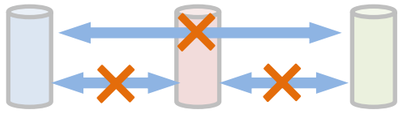
- クラウドシフトの加速
- サービタイゼーションの広がり
- 自動化/効率化

人やリソースが企業内インフラの枠外に分散
=攻撃面が拡大、複雑化しセキュリティリスクが増大

- アクセス元の場所に係わらず一貫したセキュリティポリシーの整備
- マイクロサービス、コンテナなどクラウドネイティブなセキュリティへの対応
- ツール間の連携や自動化による迅速かつ確実なセキュリティ対策

×

急速に変化するITインフラに伴うセキュリティ上の課題



各対策領域のツールやソリューション、運用体制のサイロ化により効率的なオペレーションの実現を阻害

各ツールで収集したデータに対して包括的な分析・対応によるシステム全体の脅威の可視性とリスクコントロールが困難

パブリッククラウドやコンテナなど先進技術利用による新たなテクノロジが持つ脆弱性からの不正侵入や情報漏洩等のリスクが表面化

ネットワンはこれらの課題に対して
「オペレーショナブルなセキュリティ」（OPSec）のアプローチで
セキュリティ対策の全体最適化を実現

- 効率的なオペレーションモデルを阻害するツール・運用・組織上のサイロを排除
- 継続的な「アセット、脅威・脆弱性、セキュリティ状態の健全性・運用状況等」のモニタリング・評価・改善により全体最適化されたライフサイクルでのセキュリティ対策を提供
- 組織内の情報資産、システム状態などの把握と利用状況を可視化、システム上に潜む脆弱性の危険性を最小化し、セキュリティ侵害に発展しづらい環境を確立

セキュリティ ソリューション・サービス ラインナップ

DX推進に求められる新たなセキュリティ要件に対応するセキュリティソリューション

- ネットワークセキュリティ
- クラウドセキュリティ
- エンドポイントセキュリティ
- アイデンティティ&アクセス管理
- 監視及びセキュリティ運用

高度・複雑化するセキュリティ要件に対して、お客様ICTのライフサイクルに応じた幅広いセキュリティ サービスを提供

幅広いお客様の課題を解決するセキュリティプロダクト

cisco Partner Gold Certified / paloalto NETWORKS / vmware / f5 / FORESCOUT / Infoblox NEXT LEVEL NETWORKING / Soliton / splunk> / TANIUM / tenable / TREND MICRO / LogRhythm / okta

セキュリティ サービス ラインナップ

次世代脅威分析基盤

高度・複雑化するセキュリティ要件に対して、ネットワンはお客様ICTの
ライフサイクルに応じた幅広いセキュリティ サービスを提供。
必要に応じて組み合わせでのご利用が可能です。

マネージド・セキュリティ・サービス（MSS）

IDS/IPSのログをリアルタイムに分析し、重要度の高いインシデントは速やかに通知
インシデントに係わる特定通信の遮断などをオプションで提供

マネージド・ディテクション＆レスポンス(MDR)サービス

NDR製品、EDR製品をリアルタイム監視し、感染を検知した際には速やかに通知
被害の拡大を防止するため被疑端末を隔離、詳細調査を実施し恒久対応を支援

マネージドSIEMサービス

各種ログをお客様環境に設置したSIEMによって分析し、インシデント対応の支援を実施
MSS/MDRの提供対象外のログも含め、環境に合わせたカスタマイズが可能

クラウドセキュリティ運用支援サービス

パブリッククラウド上のリソースに対して、セキュリティリスクにつながる構成ミスや
ポリシー違反及び脅威の検知と通知、設定修復の実施、脆弱性可視化を実施

脆弱性管理支援サービス

お客様環境の情報システムに対し、継続的に脆弱性や構成状況を評価
リスクと資産の重要度を加味した評価により、対策や投資に係る的確な判断材料を提供

WAF運用サービス

WAF製品による過検知を調査し、適切なセキュリティレベルを維持した対応策を提案
メーカー提供のシグネチャが対応していない脆弱性に対して、カスタムシグネチャを作成

OTセキュリティサービス

様々なデバイスタイプとプロトコルが存在するOT環境において、正確な資産把握が可能
通信のモニタリングとデバイスへのスキャンにより、資産が抱える脆弱性情報を提供

セキュリティ診断サービス

お客様環境の情報システムを診断し、脆弱性を評価
確認された脆弱性に対するリスク緩和のため、対策を含めた結果を提示

セキュリティアセスメントサービス

可視化された通信ログやクラウド環境の情報からリスクにつながる要因を評価
計画段階での設計への反映や導入後の効果測定と改善に利用することが可能

セキュリティ ソリューション

ネットワークセキュリティ

課題

どこからでも安心・安全に働けるハイブリッドなワークスタイル（テレワークとオフィス勤務の組み合わせによる働き方）環境の実現

- ✓ 社内と同じように外からでも社内と同一のセキュリティ対策を行いたい
- ✓ テレワークの導入、クラウドサービスの利用によりデータセンター側のVPN装置やゲートウェイへトラフィックが集中、社員の生産性が低下
- ✓ 働き方の多様化や社内リソースのクラウドシフトにより、社内外の境界が曖昧になり従来の境界型セキュリティでは未知や高度化された脅威への対策が不十分

効果

サイバー攻撃や情報漏洩から企業のネットワークを守り、クラウドへの安全なアクセスや安定したネットワーク環境を実現

- クラウド型のリモートアクセスVPNの導入によりテレワーク環境からでも安全にインターネット、クラウド利用が可能となり、場所にとらわれない働き方を実現
- 各拠点から直接インターネットへアクセスするローカルブレイクアウトの採用とともに、クラウド型ファイアウォール/Proxyを導入することで一貫したセキュリティ対策を実現。データセンタートラフィックの遅延・輻輳が解消され、従業員の生産性を維持
- 一貫したセキュリティとアクセスをクラウド上で提供し、ネットワーク構成の簡素化やセキュリティ管理の一元化による運用管理負荷の軽減とネットワーク保護の最大化を実現

- **不正アクセス、トラフィック対策**
  次世代ファイアウォール、UTM、Web/Mailセキュリティ、セキュアインターネットゲートウェイ、DDoS対策
- **Web改ざん,不正アクセス対策**
  Webアプリケーションファイアウォール(WAF)
- **内部ネットワーク対策**
  アセット管理、ネットワークの脅威検知とインシデント対応(NDR)
- **脆弱性管理**
  脆弱性診断、コンプライアンスチェック

クラウドセキュリティ

課題

IaaS/PaaS、SaaSなど多岐にわたるクラウド環境におけるセキュリティ対策の強化

- ✓ 組織の管理外のクラウドサービスを把握したい
- ✓ クラウドに対応した組織の「セキュリティ基準/利用ガイドライン」を策定したい
- ✓ BYODによる複数クラウドサービス利用時にユーザーの利便性を損なうことなくセキュリティを確保したい
- ✓ アプリケーションがクラウド環境の仮想サーバ、コンテナ、サーバレス等多様なワークロードに分散しており、一貫した保護が困難

効果

クラウド（IaaS/PaaS/SaaS）環境や組織における各種クラウドサービスの利用状況を可視化し、クラウド利用時のガバナンス向上を図る

- 利用されているクラウドサービスを可視化、リスク評価することで組織のポリシーへ準拠したクラウド利用を実現
- パブリッククラウド環境におけるセキュリティ対策状況の可視化と評価を行うことでセキュリティ対策の標準化を図り、クラウドからの情報漏洩リスクを低減。
- 複数のクラウド環境の仮想サーバやコンテナ、サーバレス等のワークロードを一元管理でき脅威検知の自動化によりクラウド環境の管理負荷を軽減し、利便性とセキュリティ向上を実現

- **クラウド利用の可視化・コントロール**
  Shadow IT対策、クラウド利用状況の可視化(CASB)
- **パブリッククラウドの利用統制・監査**
  クラウド環境におけるセキュリティリスクの可視化と対策の実行(CSPM)
- **クラウドワークロードの保護**
  仮想サーバ、コンテナ環境などの保護(CWPP)
- **ID管理・アクセス制御**
  多要素認証、シングルサインオン

エンドポイントセキュリティ

課題

クラウド利用の促進とテレワークに対応したエンドポイントセキュリティ対策の強化

- ✓ 導入済アンチウィルス対策では検知、防御できない高度な標的型攻撃やゼロデイ攻撃への対策
- ✓ 標的型攻撃などによる情報漏洩やインシデント発生時、端末感染状況の調査・対応、報告に時間がかかる
- ✓ ワークスタイル変革の一環として支給されたモバイルデバイスによるクラウドや社内リソースへの効率的かつ安全なアクセスとデバイスの一元管理を実現し、運用に関わる負荷を低減したい

効果

ファットクライアント/シンクライアント/モバイル環境など多岐にわたるエンドポイントの管理、マルウェアなどの脅威に対応

- 未知のマルウェアやファイルレス攻撃などの高度な攻撃の検知・防御が可能となり、情報漏洩などセキュリティインシデントの被害を最小化
- 感染PCや影響範囲の特定、感染端末のリモートからのネットワーク隔離が可能となり運用の負荷を軽減。クライアント状況の可視化が可能となり、定期的な社内への報告が可能となる
- PC、モバイル端末の垣根を越えて業務アプリケーションの利用が可能となり、移動中の従業員が空き時間にメールの確認、承認処理などの業務が可能となり、業務効率の向上を実現

- **マルウェア対策**
  シグネチャレスの次世代エンドポイント保護(EPP)、サイバー攻撃に対する検知・調査・対応(EDR)
- **PC、モバイルデバイス管理**
  統合エンドポイント管理（UEM)

アイデンティティ＆アクセス管理

課題

リモートワークの普及に伴い、社内リソースのクラウド環境への保管やオフィス外にあるデバイスを利用するシーンが増加

- ✓ 機密情報の漏洩、社外から社内リソースへアクセス可能なユーザー/デバイスを制限するといった対策が必要
- ✓ なりすましや不正アクセス防止のために常にユーザーの本人確認を行う仕組みが必要
- ✓ リモートワークの浸透とクラウドシフトに伴い、複数のクラウド環境やオンプレミスのシステムにドメインやActive Directoryに依存しない「ゼロトラスト」の実装が必要

効果

強固な認証技術、柔軟なポリシーによるコンディショナルアクセス制御、統合エンドポイント管理によるポリシー準拠チェックにより、場所を問わずに認可されたリソースへのアクセスを実現

- 乱立するID管理システムを統合し、企業のセキュリティポリシーに基づいた一元的な管理が可能で、オンプレミスとクラウド環境が混在するハイブリッド環境への対応が可能
- シングルサインオン(SSO)、多要素認証(MFA)やデバイスコンプライアンスチェックにより、アプリケーション毎のアクセス制御を実現
- 認証によって組織のネットワークやシステムを利用するユーザまたは端末が正規のものであると確認し、正規のユーザ/端末以外のアクセスを制御

- **ID管理・アクセス制御**
  クラウド型ID管理・統合認証サービス (IDaaS)
- **PC、モバイルデバイス管理**
  統合エンドポイント管理 (UEM)

監視及びセキュリティ運用

課題

複数のセキュリティ製品から取得したデータに包括的にアプローチできず、高度化された脅威への検知と迅速な対応が困難

- ✓ 複数のセキュリティ製品から収集・検知したデータに対して、包括的な分析や相関付けができずツールがサイロ化している
- ✓ インシデントアラートへの対応に長い時間を要し、脅威の発見が長引くことによりセキュリティ被害が拡大するおそれがある
- ✓ 従来の境界型セキュリティ対策をすり抜ける正規のサービスやステルス性の高い攻撃手法の増加により、未知の攻撃に対する内部ネットワークの可視化が必要

効果

各種ログ、脆弱性、NWトラフィック情報をベースに脅威検知や様々なデバイス・システムの状態を可視化し、各セキュリティ製品と連携することでシステム全体のセキュリティ強化を図る

- ログ、NWトラフィック解析をベースに非管理デバイス含むあらゆるITデバイスを可視化しネットワーク内部に潜む脅威を迅速に検知することが可能
- 機械学習を活用してインシデント対応プロセスを自動化することによりランサムウェアや情報漏洩のようなインシデントが検知された場合に自動的に迅速な対処が可能
- 様々なセキュリティ製品からのデータを収集・統合し、相関分析により可視性を向上。検知できない侵害の検知および、過検知を低減し生産性を向上

- **内部ネットワーク対策**
  アセット管理、ネットワークの脅威検知とインシデント対応(NDR)
- **脆弱性管理**
  脆弱性診断、コンプライアンスチェック
- **セキュリティ運用の自動化と効率化**
  セキュリティインシデントの分析から対応までの自動化と効率化(SOAR)、セキュリティ情報とイベント管理 (SIEM)

セキュリティ サービス

セキュリティサービス

課題

サイバー攻撃の複雑化・高度化へ対応するため、様々なセキュリティ対策を行っているが、対応の優先度の検討、増え続ける検知アラートへの対応により運用の負荷が増大

- ✓ 組織が保持する機微情報などのセキュリティ対策は、会社としての最重要課題
- ✓ 24×365でサイバー攻撃へ対応する自社設備を保持することの運用・コスト面の懸念、セキュリティ人材の不足
- ✓ 日々進化する攻撃手法の調査・分析への対応や継続的なセキュリティ対策の見直しが必要

効果

自動化×脅威インテリジェンスを組み込んだ高度な分析基盤×サイバーセキュリティスペシャリストによる先進のセキュリティ運用監視・サービスを提供。
ICT基盤全体の企画・設計から運用までの全ライフサイクルにわたるセキュリティ提供により、最新の脅威へ対応提供

- SOCサービスを導入することで脅威の早期検知が可能となり、情報漏洩やマルウェアの感染リスクが低減
- 最新の攻撃手法や脅威情報の収集、調査作業、教育などから解放され、対応・運用コスト、人材リソースを削減
- 定期的なアセスメントやコンサルテーションを通じたシステムの評価、改善提案により、継続的なセキュリティ対応計画の見直しが可能となる

- **セキュリティ サービス**
  MSS、MDRサービス、マネージドSIEMサービス、クラウドセキュリティ運用支援サービス、脆弱性管理支援サービス、WAF運用サービス、OTセキュリティサービス、セキュリティ診断サービス、セキュリティアセスメントサービス

お客様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様々なサポートを提供いたします

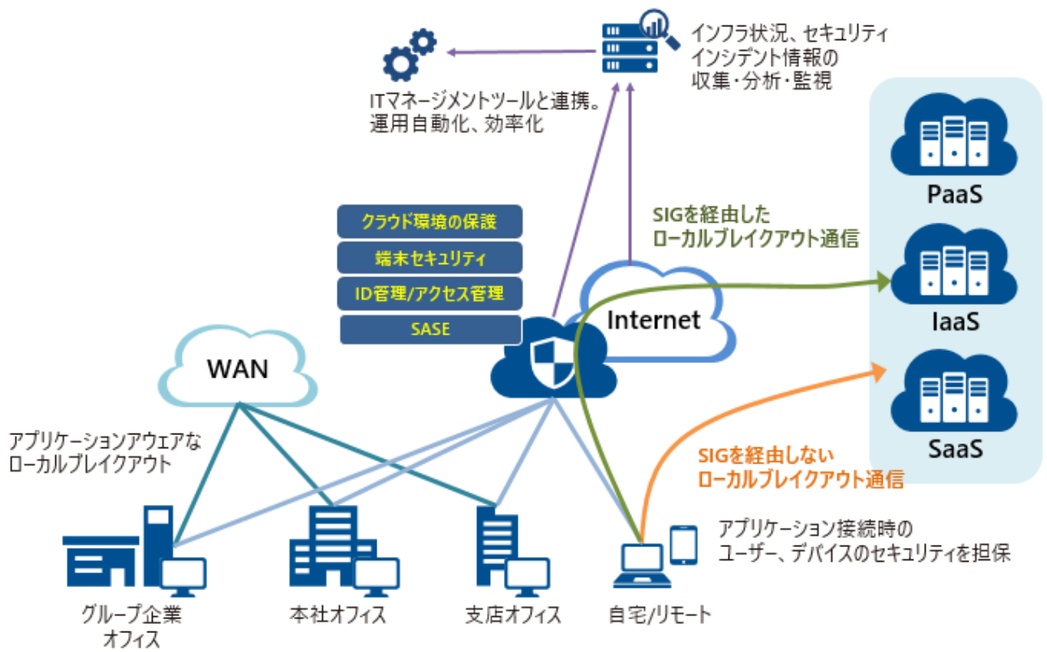
サイバーセキュリティにおける「アーキテクチャ」の重要性

これまで、オフィスとその中で働く人を「内」、リモート環境などそれ以外を「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対策が主流でした。しかし、クラウド環境活用の増加やサイバー攻撃の高度化によって境界は曖昧になり、従来の境界型でのセキュリティ確保は困難を極めます。

そのため、ITインフラの変化に合わせてセキュリティ製品やサービスを単体ではなく効果的に組み合わせた「セキュリティ・アーキテクチャ」の実装が重要となってきます。しかしながら、セキュリティ アーキテクチャを実装していくのは単純ではありません。

ネットワンでは、アーキテクチャをモジュール化してユースケースとの紐付けを行い、検証済みのシステム構成（Validated Design）によって実証されたアーキテクチャをお客様に提供します。

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 アーキテクチャ



ネットワン共同検証環境「Lab as a Service」

デジタルトランスフォーメーション（DX）実現の重要性が高まる中、ITシステムは多様化・複雑化し、既存のITインフラを用いた「セキュアな環境準備」「新たな技術スキルの習得」「クラウドソリューションの運用」の準備には時間を要する傾向にあります。
ネットワンでは、お客様が優先順位に応じて段階的にセキュリティ強化および、業務の効率性・利便性を向上させるための様々なサポートを提供します。

その一つとして、ネットワンの技術ラボ施設「Lab as a Service」（LaaS）があります。
LaaSはお客様とネットワンの共同検証環境として、様々なシナリオに基づいて事前に構築された環境にリモートでアクセスすることで、お客様はテスト環境を保有することなく複数ベンダーによるシステム連携や先端技術を比較しながら検証することが可能です。

シナリオ例として、アプリケーション実行環境構築の自動化や、情報漏洩対策とインターネットアクセスの利便性を両立した検証環境があります。

ネットワンはLaaSを活用して、セキュリティ領域のみにかかわらず、具体的な解決策・価値をお客様と一緒に創出しDX推進に向けた全体構想の立案と最先端技術の実証を支援します。

DXを推進するお客様に、すぐに利用可能なマルチクラウド／ハイブリッドクラウド検証環境を提供

事前準備不要

事前に構築済みの環境を提供
条件内の内容であれば機材持ち込み、構成変更などのカスタマイズが可能

リモートアクセス

お客様のお手元のPCからリモートアクセスでテスト実施が可能

シナリオベースの機能確認

多数のシナリオベースの検証メニューを提供

専門家とのディスカッション

ネットワンの専門家から技術アドバイスを提供

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/

記載情報は2022年 7月現在のものであり、
予告なく変更される場合があります。

最新の仕様および価格については、弊社営業までご確認下さい。