Nippon Techno Lab Inc.

世界の40%を占めるサイバー攻撃発生源から生まれた
安心と信頼のサイバーセキュリティソリューション

CYBER SECURITY SOLUTION

アンチDDoS / Webアプリケーション脆弱性対策 / スレットインテリジェンス

www.ntl.co.jp

セキュリティのリスクゼロを目指し
信頼性、運用効率を強化し様々な脅威から資産を守ります

今やあらゆるビジネスの現場において、ITの利用は企業の収益向上に不可欠なものとなっている一方で、企業が保有する顧客の個人情報や重要な技術情報等を狙うサイバー攻撃は増加傾向にあり、その手口は巧妙化しています。被害を受けた企業は信用を失い、取り返しのつかない情報漏えい等による経営危機を招くリスクは、ますます高まっております。

2016年に入り、メール経由での不正プログラム（マルウェア、ランサムウェア等）拡散は約5倍になり、DDoS攻撃は約40%の増加がうかがえます。

最も多くの攻撃を受けている国は、中国、米国となりますが、これは日本への攻撃が少ないことを示しているわけではなく、日本も脅威に晒され、常に狙われています。

攻撃は高度化、巧妙化が著しく、従来のAnti VirusソフトウェアやOSへのパッチ適用では防ぎきれないものが多く見つかっております。

マルウェア、ランサムウェアの特徴は、攻撃されたこと、感染していることに気づきにくいという点です。一度侵入されてしまうと、気づかないうちに複数のサーバーやPCを通して内部に感染し、外部に情報が漏えい、または重要ファイルを使用不可能にし身代金を要求するといった手口で企業の信頼を失墜させます。

マルウェアに感染している場合、企業のPCやIoTデバイスが他社のサイトに対して知らぬ間にDDoS攻撃を行っている場合もあります。

また、企業のホームページを改ざんしたり、クレジットカード番号を盗み取るサイトへ誘導するなどの被害も増加しています。

昨今増加している標的型サイバー攻撃は、高度化かつ巧妙化していることもあり、従来の侵入、感染を未然に防ぐという入口対策だけでは攻撃を防ぐことは難しく、多層防御を行うことが一般的です。しかしながら、サイバー攻撃を完全に防ぐことは難しく、インシデントが発生することを前提に取り組むことが必要です。

この多層防御を行うには、マルチベンダー機器が導入されることが多く、インシデント発生の際には攻撃による影響範囲や原因究明の特定に高度なセキュリティ知識と高い技術力が必要となります。

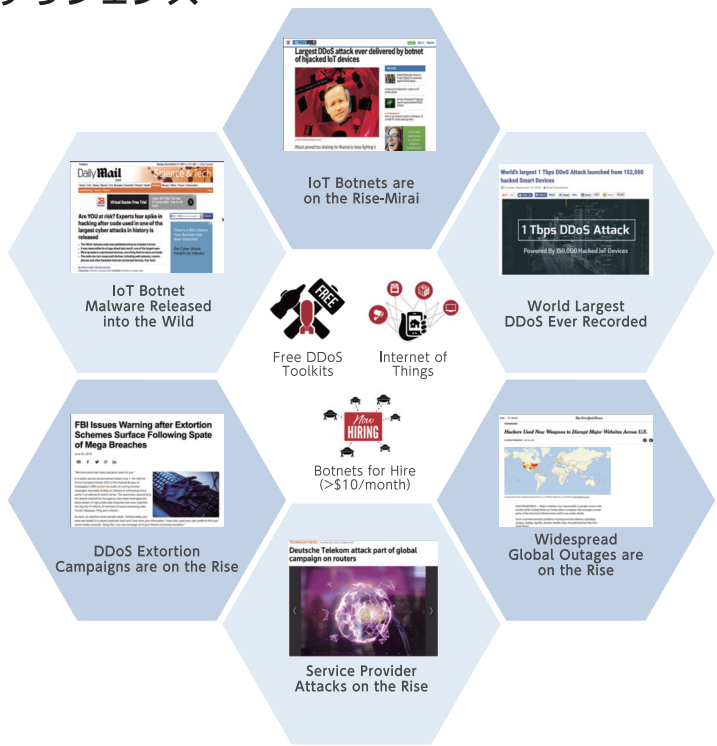
このような課題解決のために、セキュリティ専門家による高度標的型攻撃等の対策としてサイバーセキュリティソリューションをご提供します。

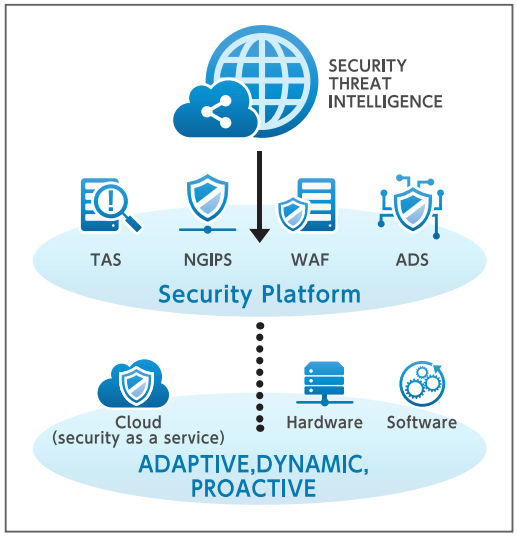
NSFOCUS
GLOBAL THREAT INTELLIGENCE

NSFOCUS グローバル・スレットインテリジェンス

世界の40%を占める サイバー攻撃発生源である 中国での研究技術をベースとした セキュリティ脅威インテリジェンス

近年のサイバー攻撃は、今までになく巧妙であり、攻撃力も大規模になっています。攻撃者の動向は、趣味を目的とした個人によるものから、サイバーテロ、サイバー犯罪といった組織を狙った脅威へと変化しています。知らないうちに、従業員、顧客、または一般市民のインターネット接続デバイスが危険にさらされる恐れがあります。同時に、プロトコル、オペレーティングシステム、ネットワークデバイスおよびアプリケーション内で新たな脆弱性が日々発見されており、新たな脆弱性を悪用する攻撃に追いつくことは非常に困難なことです。結果として、ネットワークやアプリケーションのセキュリティに莫大な投資をしたにも関わらず、企業はオンラインシステムや大きな犠牲を伴う情報漏えいといった混乱に悩まされ続けることになります。





包括的なセキュリティを提供するためには、単純に新たな脅威アクター、ベクトル、動機などについての研究、理解、解析、報告をすればいいわけではありません。価値を持たせるためには、有効かつセキュリティポリシーに直接組み込むことのできる情報が提供され、ただちに侵入をブロックできなければなりません。

NSFOCUSグローバル・スレットインテリジェンスは、IPレピュテーション、悪意のあるWeb/URL、コマンド、マルウェアデータフィードへの情報を提供するサービスです。フィードは、NSFOCUS社のオンプレミスの全ソリューション、およびクラウドDDoS防御ソリューション(DPS) と統合されています。

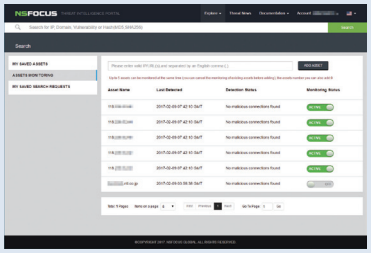
Search IOCs: IP, File MD5 Hash, Domain, CVE, Payloads

IP・ドメインレピュテーション

IPアドレスまたはドメイン名で検索を行うことで、デバイス、ミドルウェア、脅威の分析レポートを確認することができます。

Monitoring IP addresses - automatic notification

グローバルIPアドレスが割り当てられたデバイスや、URLを登録することで資産監視を行い、内部デバイスに感染の予兆があれば通知をします。



マルウェアの検索

疑いのあるファイルのMD5ハッシュ値を検索すると、そのファイルがマルウェアかどうかを判断することができます。

最新の脆弱性情報

新たに発表されたCVEナンバーから、脆弱性の影響範囲を特定する事ができます。

DDoS ATTACK COUNTERMEASURE

DDoS攻撃対策

1台で最大40Gbpsを誇る高性能のDDoSミティゲーション能力

近年では、今までになく容易に、利益や顧客の損失、サービス可用性の低下、会社の信頼の損失、機密データの窃取などの被害をもたらすような、複雑で破壊的な大規模のDDoS攻撃を仕掛けることができるようになっています。

ボットネットの増加や高度な攻撃増幅技術の発達により、かつては数百Mbps程度だったDDoS攻撃が、今では数Tbpsへと進化しています。近年のDDoS攻撃に対応でき、かつ、将来あらわれる可能性のあるパフォーマンス面への要求に応えることのできる拡張可能なDDoSミティゲーションソリューションの導入が今まで以上に重要視されています。当社のDDoSセキュリティ対策（Anti-DDoS）ソリューションは、大企業、ホスティング会社、クラウドおよびサービスプロバイダーにおける現在そして未来のニーズに合った最適なパフォーマンスを可能にするスケーラブルテクノロジーを採用しています。

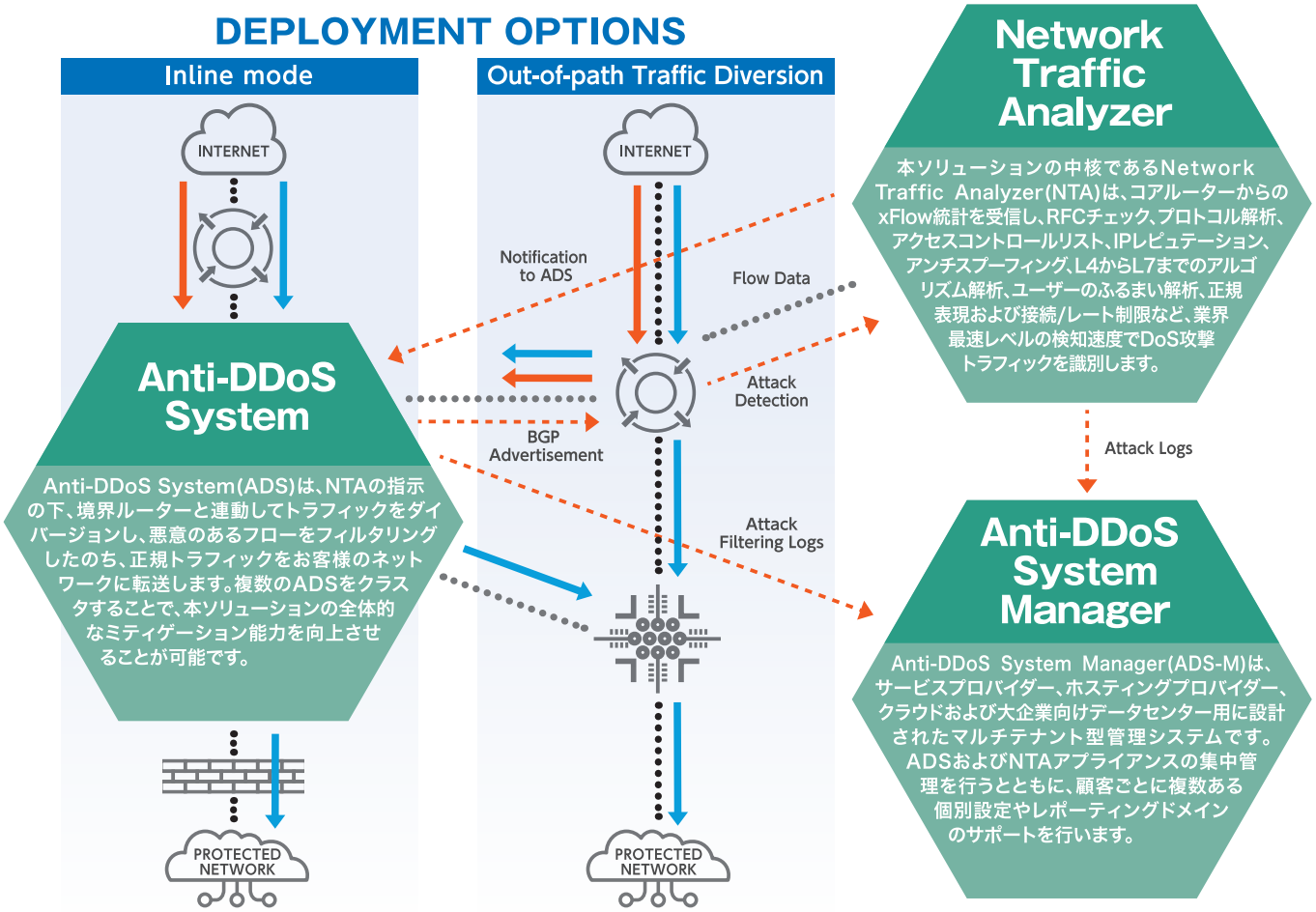
DDoS攻撃とは?

（分散型サービス妨害攻撃）

DDoS（攻撃）とはネットワークを通じたサイバー攻撃の一種で、標的となるコンピューターに対して、複数のコンピューターから一斉に大量の処理負荷を与えることで、サービスを機能停止状態へ追い込む手法のことをいいます。

大規模DDoS攻撃対策を可能とする3つの構成要素

本ソリューションは、数Gbpsを超えるDDoSミティゲーション能力を必要とするネットワーク環境向けに開発されています。分散型のアーキテクチャーを採用することで、DDoSミティゲーション、脅威の検知および集中管理を分離して実行し、それぞれの役割ごとに調整を行います。クラスタおよびアウトオブパスモードでの構成により、数百Gbpsおよびそれ以上のミティゲーション能力を発揮することができます。



SECURITY CLOUD DAS

Cloud DDoS Analysis Service

クラウドDDoS攻撃分析サービス

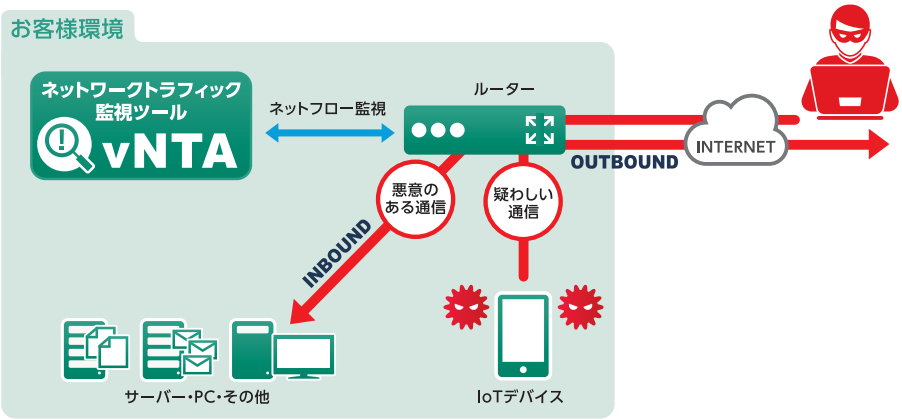
SECURITY vNTA

外部からの悪意のある通信を検出
内部の通信を監視して
疑わしいデバイスを検知することができます

ネットワークトラフィックの可視化

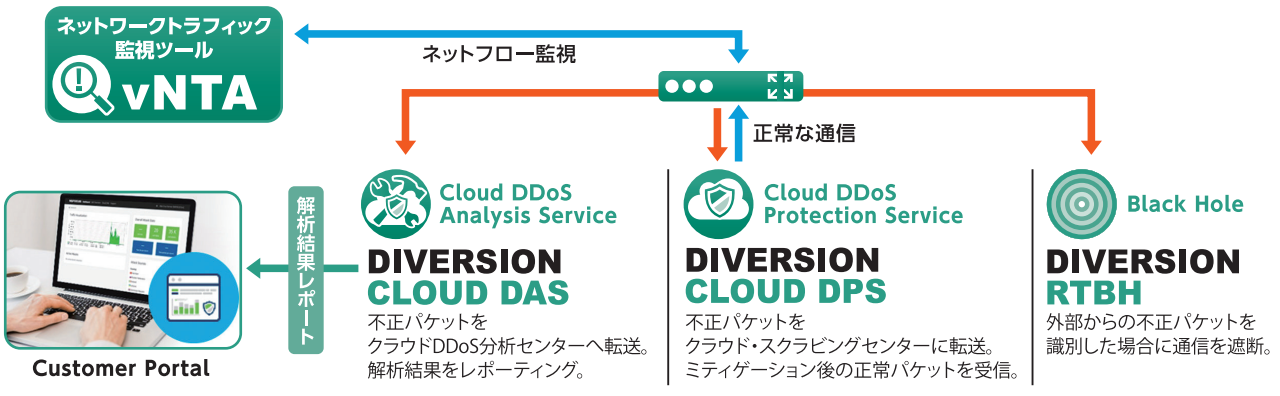
「vNTA」は、NetFlow/sFlow/IPFIX/Flexible Netflowなどのフローデータを受信し、リアルタイムで分析します。外部からのDoS攻撃トラフィックを識別した場合、ダイバージョン（ルート変更）を実施し、致命的な障害から企業ネットワークを守ります。また、内部におけるデバイスから疑わしい通信が識別された場合には、即座に警告を出します。

これらの機能により、ネットワーク状況を可視化することで、ネットワークの障害解析や必要なセキュリティ対策の実施を容易にすることができます。



SECURITY vNTA-DIVERSION

ネットワークダイバージョン（ルート変更）



機能 vNTA

フロー監視	ADSトラフィックダイバージョン	DDoS攻撃検知	管理インターフェースおよびレポート
sFlow-v4/v5, Netflow-v5/v9, NetStream-v5, Flexible Netflow, IPFIX	トラフィック量に応じてルーターにダイバージョン通知を送信	SYN/ACK/UDP/ICMP/IGMP/HTTP/HTTPS/DNS/Land/SIP floods、TCP flag misuse、flag null、プライベートIP、異常なトラフィック、アラート閾値の自己学習、IPグループインバウンド/アウトバウンド攻撃トラフィック、ビジネスドメインおよびリージョンインバウンド/アウトバウンド攻撃トラフィック	SNMP GET/Trap、syslog、Email、フローデータ転送 フォレンジックおよびコンプライアンスイニシアチブのためのWebサービスAPI

WEB APPLICATION VULNERABILITY COUNTERMEASURE

Webアプリケーション脆弱性対策

大規模環境に利用しやすい マルチテナントアーキテクチャー採用

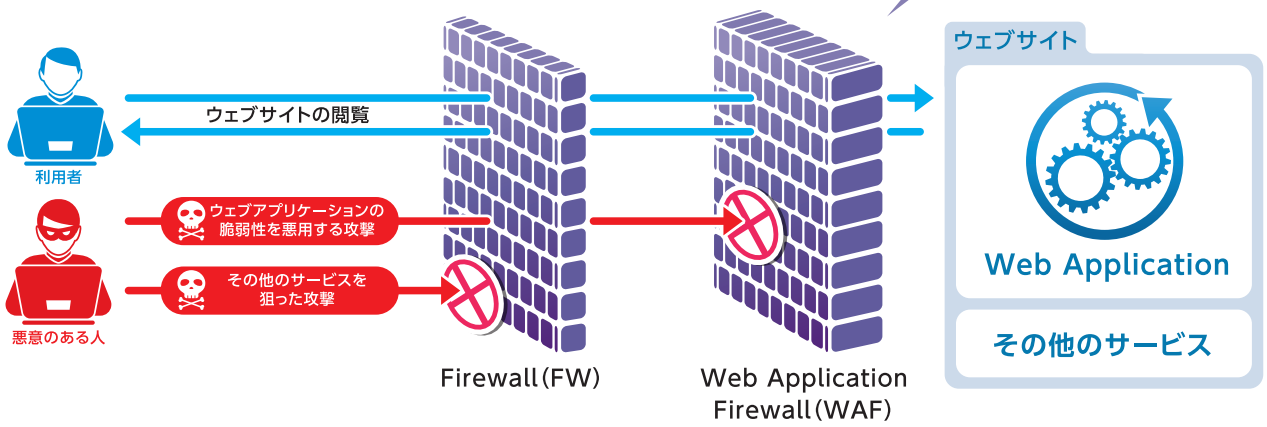
ECサイト、ネットバンク等、インターネットを利用した様々な顧客向けサービスを提供するために、現代ではWebアプリケーションが必須となりました。その一方、Webアプリケーションの脆弱性を悪用したサイバー攻撃によって、Webサービスの提供妨害や個人情報の漏えい事件は後を絶ちません。

インターネットに公開されたWebサイトは、個人、中小、大企業といった規模を問わず、すべてのWebサイトが攻撃にさらされる危険性があります。

Webアプリケーションファイアウォール(WAF)は、包括的なアプリケーションレイヤーセキュリティを提供することで、これらの問題に悩まされることのないよう、重要なサーバーやWebアプリケーションのセキュリティ防御を行います。Open Web Application Security Project (OWASP) Top 10に対応しており、アプリケーション、サーバー、プラグイン、プロトコル、ネットワーク接続性などのインフラを保護するよう特別に構成されています。

Webアプリケーションファイアウォール(WAF)とは?

保護対象となるWebサイトの前面に配置して、Webサイト利用者からアクセスされる全ての通信を検疫し、Webアプリケーションの脆弱性に対する不正アクセスを防止する機能や、アクセス制御ポリシー機能によって、不正なファイルダウンロード検知、Webシェル防止、クレジットカード番号やマイナンバー等の機密情報のフィルタリングを可能とし、サイバー攻撃による情報漏えいを防止します。



導入のメリット

■データ漏えいリスク削減

Webベースのインタラクティブ・アプリケーションは、データベースにアクセスしますが、攻撃者は、SQLインジェクションやその他の方法を使用してデータベースに侵入し、データ漏洩の原因となることがよくあります。

WAFは、これらの攻撃を防御し、データ漏洩のリスクを低減します。

■Webアプリケーションの可用性のサポート

WAFは、さまざまな動的保護アルゴリズムを持った専門的なDDoS防御機能を備えており、DDoS攻撃をオンラインでフィルタリングすることができます。

WAFは、DDoS防御とSQLインジェクション防御を組み合わせることで、ネットワークレイヤーからアプリケーションレイヤーまでの攻撃を防御し、Webサービスの可用性を確保します。

■悪意のあるアクセスの制御

自動攻撃ツールによる大規模な悪意のある攻撃によって、Webアプリケーションは安定性を大きく損なう可能性があります。

WAFは、さまざまな顧客のニーズを満たす複数のWebアクセス制御機能を提供します。(HTTPアクセスコントロール、自動攻撃ツール識別、不正ファイルアップロード、クロウラー防止など)

■Webクライアントの保護

Webユーザーは罠にはまって、攻撃者に利用されたり、情報を奪取される可能性があります。

WAFは、クロスサイトリクエストフォージェリ(CSRF)、クロサイトスクリプティング(XSS)、セッションハイジャックなどから、Webクライアントを保護します。

MULTI-LAYER SECURITY

マルチレイヤーセキュリティ

WAFシリーズは、高度な検査およびWebアプリケーションレイヤーのセキュリティに特化したセキュリティを提供しており、多層防御アーキテクチャー全体における要となっています。

最大1GbpsのDDoS防御機能を搭載することで、TCP floodや、HTTP/S GET/POST floodを含む大容量のアプリケーションレイヤー攻撃からお客様を防御します。

より高い能力を誇るNSFOCUS ADSシリーズのAnti-DDoSアプライアンスと連動して配置することで、WAFはリアルタイムでフローをADSに転送し、いかなる過酷な状態でもサーバーを正常に稼働させることができます。

データ漏洩リスクの削減

- ■SQLインジェクション保護
- ■HTTP保護
- ■Web脆弱性攻撃の保護
- ■ステータスコードのフィルタリングと変装による情報漏洩防止
- ■Webコンテンツセキュリティ保護
- ■ブルートフォース保護

Webアプリケーションの可用性のサポート

- ■HTTPフラッド防止
- ■TCPフラッド防止
- ■低速および低速の攻撃からの保護

悪意のあるアクセスの制御

- ■URLアクセス制御
- ■違法ファイルのアップロードとダウンロードの防止
- ■Anti-leech
- ■Anti-crawler

Webクライアントの保護

- ■CSRFの保護
- ■XSS保護
- ■暗号化と署名によるCookieのセキュリティ保護

ご提供形態

WAF Appliance（アプライアンス）

ゲートウェイ型WAF（ネットワーク型WAF）を貴社ネットワーク内に設置します。現在ご利用のWebサーバーには特別なソフトウェアのインストールや変更などを行う必要がなく、アプライアンスとして手軽に設置いただけます。（レンタルプランもご用意しております）

アプライアンスモデル性能

モデル	2000	1600	1000
性能	6Gbps / 110,000TPS	3Gbps / 55,000TPS	1Gbps / 30,000TPS
インターフェース	4スロット (4×10/100/1000 BaseT, 4×GE SX または 4×GE LX Fiber)	4スロット (4×10/100/1000 BaseT, 4×GE SX または 4×GE LX Fiber)	6×10/100/1000 BaseT (copper) オプションで 1つのスロット

vWAF Software（ソフトウェア）

WAFソフトウェアを貴社のサーバーにインストールします。アプライアンス製品モデルとは異なり、処理能力には制限がございます。（詳しくはお問い合わせください）

動作環境

vWAF は仮想イメージでのご提供となります。動作環境は以下の通りです。

- ・VMware Player 5.0 以上
- ・VMware Workstation 9.0 以上
- ・VMware vSphere ESXi 5.0 以上

VULNERABILITY DIAGNOSIS SERVICE

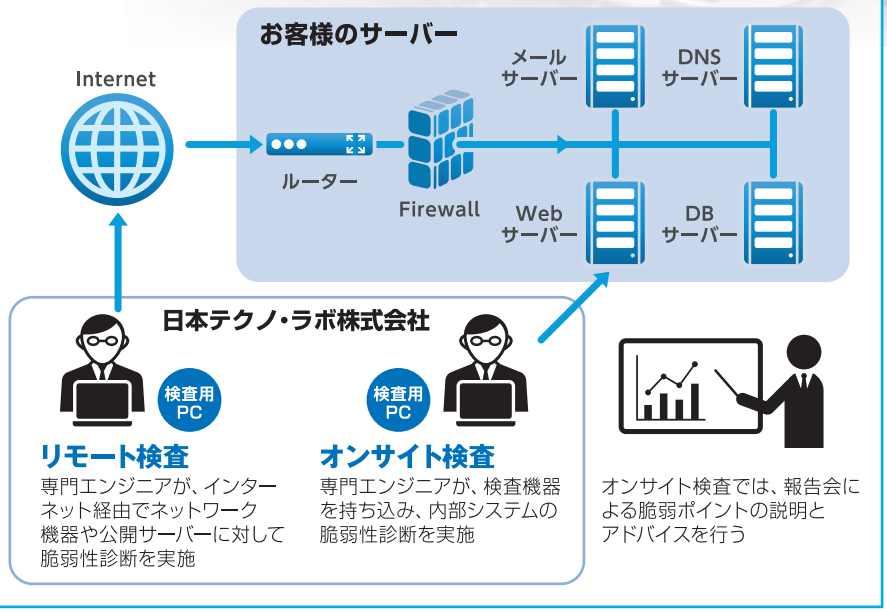
脆弱性診断サービス

情報セキュリティ対策といっても、脅威の性質はさまざまで、対策方法も多岐にわたります。

ただし、サイバー攻撃などの脅威は、日常的に使っているOSやデータベースなどのミドルウェア、あるいはそのほかの基盤技術に対する脆弱性をついてきます。そのため、対策を打つ前に内部システムのリスクを可視化することが重要となります。

当社のシステム脆弱性診断サービスをご利用いただくことでネットワークトラフィックの状態、IoTデバイスなどに潜む脅威の予兆の発見、インバウンド、アウトバウンドの通信の傾向、Webサーバーの脆弱性の発見など、さまざまなセキュリティ脅威の発見にお役立ていただくことが可能です。

システム脆弱性診断のサービスイメージ



NSFOCUS

- HQ カリフォルニア州サンタクララ & 中国北京に本社拠点
- インテリジェント・ハイブリッド セキュリティソリューションプロバイダ
- 16年以上のセキュリティ専門集団
- 2,000人以上のグローバル社員
- グローバルセキュリティコミュニティの アクティブメンバー

#2 WAF APAC — Frost & Sullivan

Microsoft Bug Bounty Program — MSRC 4 Years

8,000+ Customers

817 Million Subscribers — 中国移动 China Mobile

$3.32 Trillion in Assets — ICBC

■ お問い合わせ先

NTL Nippon Techno Lab Inc.

日本テクノ・ラボ株式会社

〒102-0093
東京都千代田区平河町1-2-10 平河町第一生命ビル5F
問い合わせ：営業部 03-5276-2810（代表）
ＦＡＸ 03-5276-2820
URL: http://www.ntl.co.jp　E-mail: sales@ntl.co.jp

ISO 27001:2005 UKAS MANAGEMENT SYSTEMS 127