機能のご紹介

NISGは、アプリケーションベースの次世代ファイアウォール、IPS、VPN 、セキュリティ管理機能を提供します。

ファイアウォール
ユーザとアプリケーションに基づき制御を行う次世代ファイアウォールのアーキテクチャは、従来のファイアウォール機能である領域保護、アクセス制御、スタティックルーティング、ポリシーベースルーティング、DNSプロキシ、DHCPサービスなど機能の上にアプリケーション層の制御、アカウント制御機能が搭載され、より安全なネットワークアクセスを保障します。

IPS
国際特許技術のIPSエンジンは一般的なオペレーティングシステム、データベース、Webサーバ、メールサーバやアプリケーションソフトなどに対する数千種類の攻撃を検知・識別し、効果的にブロック・警告を行い、不正侵入からネットワークを保護します。

Dos/DDos
SYNフラッド攻撃、UDPフラッド攻撃、ICMPフラッド攻撃、IPオプション攻撃、ポートスキャンなど54種類のDoS/DDoSネットワーク攻撃に対する防御を行います。

アンチウイルス
ヒューリスティックウイルススキャン技術を持ち、社内メールシステムでウイルスの拡散を防いで、HTTP/FTPプロトコルでファイルダウンロードまたはアプリケーションに対してスキャンとフィルタリングできます。効果的にウイルスや不正ソフトを防御できます。

アンチスパム
スパムフィルタエンジンはメールの送受信者、件名またはメール本文に対するフィルタリングができます。知能的な解析アルゴリズムは正確にスパムメールを判別できる上、スパムメーカーの情報を常時管理することによって、効果的にスパムメールをブロックできます。

URLフィルタリングとコンテンツフィルタリング
URLフィルタリングとWebコンテンツフィルタリング機能は効果的にウェブサイトのアドレスと内容をフィルタリングし、暴力や性的な内容を含むサイトへのアクセスをブロックすることができます。

アプリケーション制御
日本国内や世界中によく使われる2200種類以上のネットワークアプリケーションを識別・制御できます。更に企業でよく使用されるソフトウェアを管理し、企業のネットワークリスクを軽減します。

DNS 防護
DNSドメインのブラックリスト解析機能とDNSキャッシュポイズニング保護を提供し、効果的にフィッシングサイトやオンライン詐欺から企業イントラネットを守ります。

プロトコル検出
一般的なネットワークトランスポートプロトコルを解析し、標準的なプロトコル検知を行い、潜在的な不正パケットによる攻撃をブロックし、効果的にイントラネットやサーバを保護します。

サーバー情報保護
メールサーバとWebサーバに対して重要な情報を保護し、メールサーバとWebサーバから情報漏洩を防ぎます。企業内部のサーバソフトウェアへの攻撃を効果的にブロックし、対策実施までの空白期間を補います。

IPSec VPN
ほとんどのゲートウェイとIPSec VPNを構築することができ、企業間、本社-支社間のデータに対する暗号化し、盗聴されずに安全なデータ転送ができます。暗号化されたデータに対するアクセス制御ができ、ポリシーベースルーティングとポリシーベースVPNを提供します。

アクセスVPN
外部からリモートVPNを介して企業イントラネットへ接続することができます。暗号化と認証を行うことにより、データが盗聴/改ざんされないようにになります。また、社員ごとにアクセス制御を行うことにより、一層効果的に企業データを保護できます。

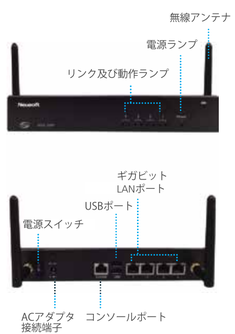
ログとモニタリング
管理ログ、トラフィックログ、IPSログ、アンチウイルスログ、アンチスパムログ、アプリケーション識別ログを提供し、オフィスへの脅威を迅速的に把握できます。リアルタイム監視機能により、ネットワークの状況を常時把握できる上、よく利用されているアプリケーションやトラフィック、URLなどの情報を表示することができます。

IPv6
国際的な認証であるIPv6 Readyを取得しており、日本国内のIPv6ネットワークへの接続を完璧にサポートします。

ワイヤレス
別途で無線デバイスを用意せず、NISGに付いている無線モジュールは企業に無線接続ソリューションを提供できます。
無線アクセスポイントとクライアントとして同時に動作でき、802.11a/b/g/nプロトコルに準拠し、電波周波数帯は2.4GHzと5GHzを提供するため、すべての無線接続と拡張機能におけるニーズを満たせます。また、暗号化において、AESとTKIPアルゴリズムに準拠し、WEP/WPA2-PSK/WPA2-RADIUSなどのモードが満載でございます。

性　能	NISG 3000-N3	NISG 3000-N5	NISG 3000-N7
ファイアウォール スループット	2.7 Gbps	2.7 Gbps	2.7 Gbps
VPN スループット	110 Mbps	110 Mbps	110 Mbps
IPS スループット	200 Mbps	200 Mbps	200 Mbps
AV スループット	205 Mbps	205 Mbps	205 Mbps
最大同時接続数	200,000	200,000	200,000
新規接続数/秒	12,000	12,000	12,000
登録可能ユーザ数	15	30	100

ハードウェア仕様	NISG 3000-N3 / N5 / N7
インターフェース	有線WAN GBEthernet Port × 1 有線LAN GBEthernet Port × 3 無線LAN 802.11 a/b/g/n USB 3.0 × 2 Rs-232C × 1
拡張インターフェース	Mini-PCIe × 1
サイズと重量	208(W) × 180(D) × 38(H)　1.8 kg
消費電力と電源	AC電源 最大40W 1.3A 対応周波数 50-60Hz
動作環境	温度 0℃~45 ℃
認証とコンプライアンス	CE emission, FCC Class A, RoHS, UL



Neusoft®
Neusoft Corporation
〒135-0063
東京都江東区有明3-6-11
東京ファッションタウンビル東館7階
TEL: 03-3570-9322
E-mail: securityinfo@neusoft.com
URL: https://neteye.neusoft.com/jp/

NISG 3000
N3 / N5 / N7

UTM
統合脅威管理アプライアンス

Neusoft®

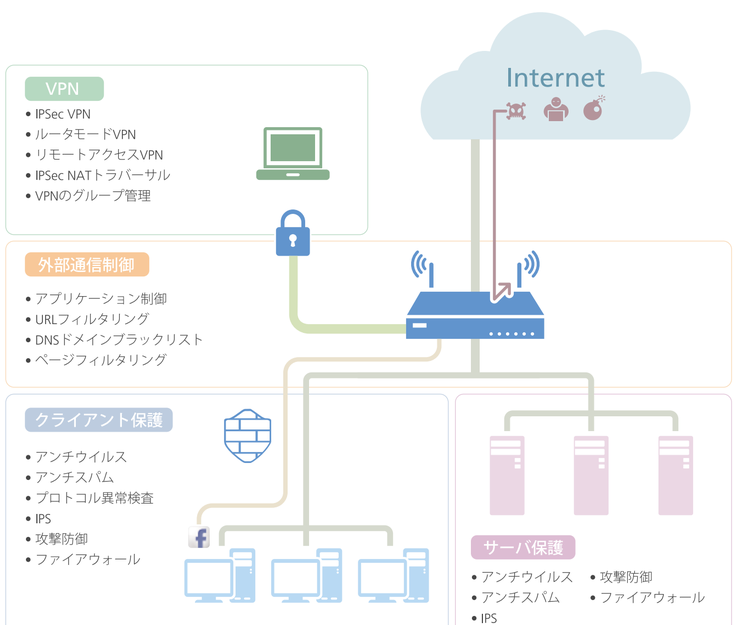
NISG3000 概要

全ての機能を統合したオールインワンのセキュリティソリューション

NISG 3000 シリーズ（ Neusoft Integrated Security Gateway）は、全てのセキュリティ機能を 1 つに統合した統合脅威管理アプライアンス（UTM）です。

サーバ、クライアントを保護するだけでなく、統合的な管理機能を提供します。

優れたセキュリティ対策をコンパクトなボディに搭載
インターネットの脅威から企業のオフィスを守ります



Q-オフィスのアプリケーションやWebアクセスを管理したい…

アプリケーションの利用や
Web サイトアクセスの規制などを一元管理
できるソリューションが必要です。

Q-情報漏洩はこわい、でもどうしたらいいの…？

多発する情報漏えい事件で安心できる
ネットワークセキュリティ対策が必要です。

Q-さまざまなネットワーク脅威からオフィスを守りたい…

ウイルス、迷惑メール、なりすまし、
盗聴など、オフィスは常に危険にさらされており、
信頼できる保護が必要です。

Q-Wi-Fiはセキュリティ問題が心配…

Wi-Fiを利用したいがセキュリティ問題が心配…
便利且つ安全な無線LAN が必要です。

Q-簡単にオフィスのセキュリティ管理をする方法はないか…？

セキュリティはとても大事だが、会社に専門的
な人がいないため管理が難しい、そんな悩みを
解消したい…

日本国内向けにカスタマイズ
使い易い高性能なUTM

簡　単 —— 世界で最も管理し易いUTM

簡単な設定ウィザード

PCは勿論、スマートフォンからも素早く
リアルタイム管理や監視を実現できます。
直観的な設定ウィザードを使用してセキュリティの
設定を技術者不要で行えます。

国内仕様 —— 日本市場を意識した専用設計

アプリケーション識別
国内仕様ゲートウェイのVPN構築

日本でのみ使われるアプリケーションも精細に識別して
管理できます。
国内仕様ゲートウェイに応じて、VPNウィザードが搭載
されることでVPNトンネルの構築がより簡単にできます。

高性能 —— 業界最高性能

最高のアプリケーション識別性能
最速の新規接続スピード

2.7Gbpsのスループットは同レベル のセキュリティ製品よりも
はるかに高速です。
優れた性能により、多くのユーザはネットワークアクセスにおい
てもストレスを感じません。