認証

- VMware Ready
- Citrix Ready
- IPv6 Ready
- CVE Compatibility
- Microsoft MaPP
- Membership
- Patented IPS
- ...

パブリッククラウドのグローバルサービスシステムに基づき、
すべてのサービスをリアルタイムで提供することができます。

Firewall　Cloud Management Center　Regional Database

Anti-virus rule base update　Application list update　Anti-span rule base update　URL Filtering rule base update　Attack Signature rule base update

V-Guard

株式会社ビジョン
〒160-0022
東京都新宿区新宿六丁目27番30号
新宿イーストサイドスクエア８階
TEL：0120-187-019
https://www.vision-net.co.jp/

V-Guard 3000

統合的なセキュリティ機能 ◆ 簡単設定＆管理 ◆ クラウド監視プラットフォーム

NGFW機能を統合した

中小企業様向けの新しいUTM

V-Guard

中小企業向けの多機能UTMセキュリティゲートウェイ

V-Guard3000は中小企業向けに最適な次世代UTMです。
さまざまなセキュリティ機能を１台に統合し、簡単導入、リアルタイム管理などを有するオールインワンセキュリティソリューションを提供します。

外部からの脅威を防御

ネットワーク攻撃

外部からのDos、DDos、フラッディング攻撃、ボットネット攻撃などは攻撃防御機能を使うことでブロックすることができます。

ウイルス侵入

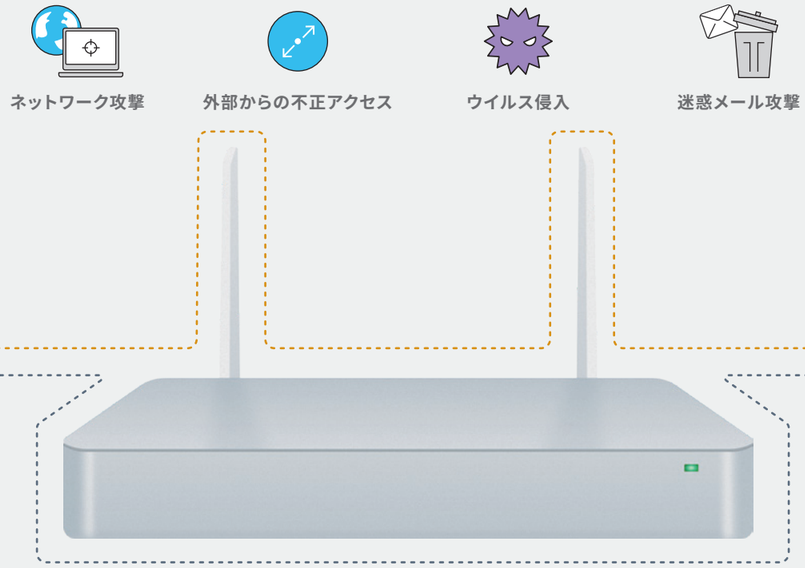
ファイルダウンロード時及びメール受信時にアンチウイルス機能にてウイルススキャンを行い、マルウェア、ランサムウェアなどのセキュリティ脅威から利用者を守ります。

迷惑メール攻撃

フィッシングメールやSPAMメール、詐欺メールなどをアンチスパム機能でブロックできます。

外部からの不正アクセス

IPS機能にて外部からの攻撃動作を素早く識別。攻撃者によるシステムバグを利用した企業サーバーへの攻撃、ユーザー情報の盗聴、マイニング、ボットネット構築、トロイの木馬の感染などの侵入をブロックできます。



不正なWebアクセス

Webフィルタリング機能にて、キーワード検知で特定のWebサイトへのアクセスを禁止することができます。

不当アクセスの制御

URLフィルタリング機能にて、利用者が暴力系、ギャンブル関係、アダルトサイト、犯罪行為など、明らかに業務に関係ないWebサイトへのアクセスを制御できます。

ウイルス拡散

アンチウイルス機能にて、利用者が送信したメール、ファイルを検知し、ウイルス拡散を防止します。

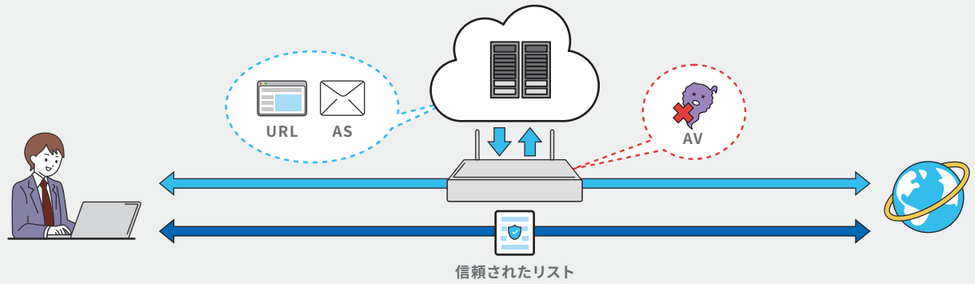
ユーザー認証と管理

利用者をユーザーアカウントで管理し、ネットワークアクセスやアプリケーションを監視することができます。

内部からの脅威を防御

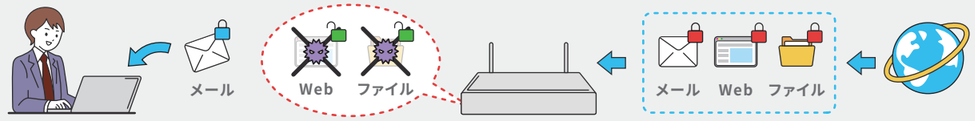
Q V-Guard3000はローカル検出だけではなくオンライン検査にも対応していますか？

A はい、クラウドサーバを通じてアンチスパムやURLフィルタリングのウイルス情報を更新しています。
ローカル検出のリアルタイム検知とクラウドの定期更新により複雑なネットワーク脅威に対し、多面的なセキュリティを提供することができます。



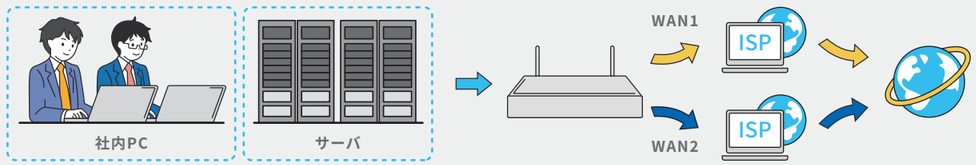
Q 暗号化された通信を利用しているネットワークの場合、マルウェアや脅威のある通信を防御するにはどうすればいいですか？

A V-GuardシリーズはSSLで暗号化された通信をウイルススキャンすることができます。



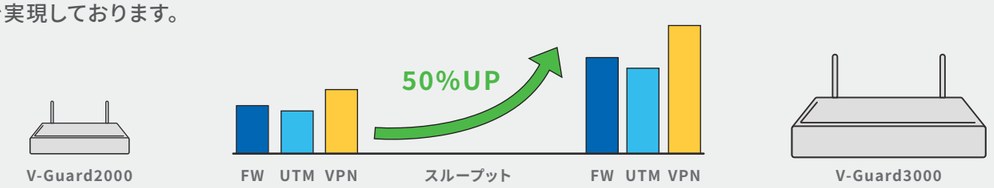
Q ネットワーク接続に問題が発生した場合、すぐにISP(プロバイダ)を切り替えることはできますか？

A V-Guard3000はダブルWANポートに対応しているため、同時に異なるISP(プロバイダ)へのアクセスに対応し、緊急時のネットワークの正常化と業務の停滞を防ぐことができます。

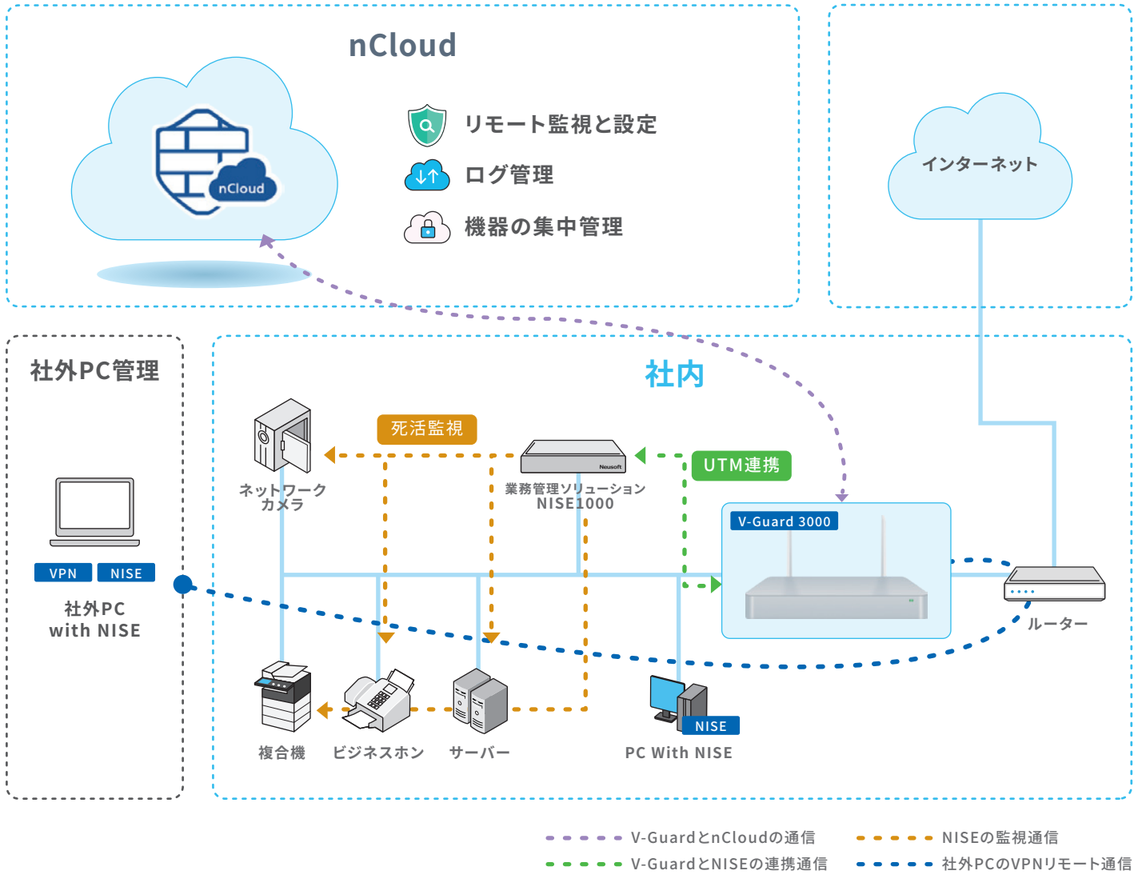


Q 複雑化した企業の業務通信を、V-Guard3000のセキュリティは安全で効率的にサポートできますか？

A V-Guard3000のパフォーマンスは、以前の製品と比べて、ネットワーク性能やさまざまな機能の大幅な性能向上を実現しております。



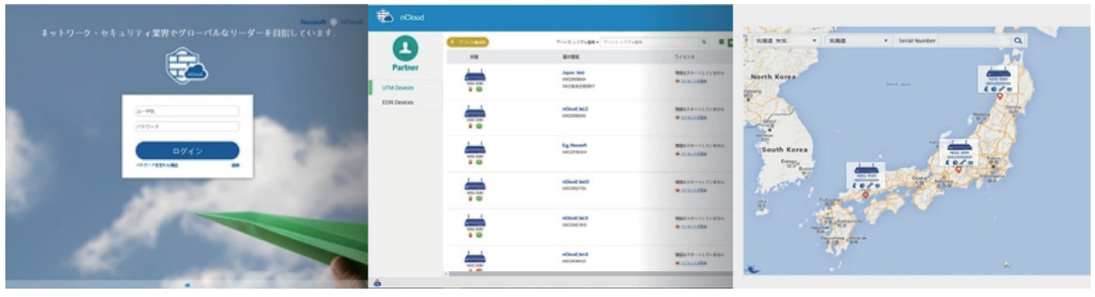
中小企業向けのUTMセキュリティソリューション



1 nCloudでリモート管理保守と機器の状態監視を実現

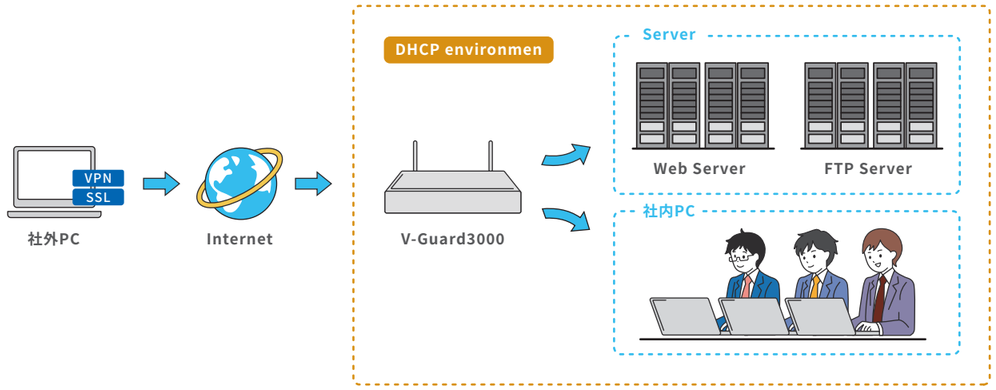
nCloudはのサービス品質を向上させるクラウド管理プラットフォームです。
クラウドでセキュリティを監視することにより、迅速に対応が可能となるため運用コストを削減できます。

リモート管理 | リアルタイム監視 | デフォルト/カスタマイズレポート | ログの保存



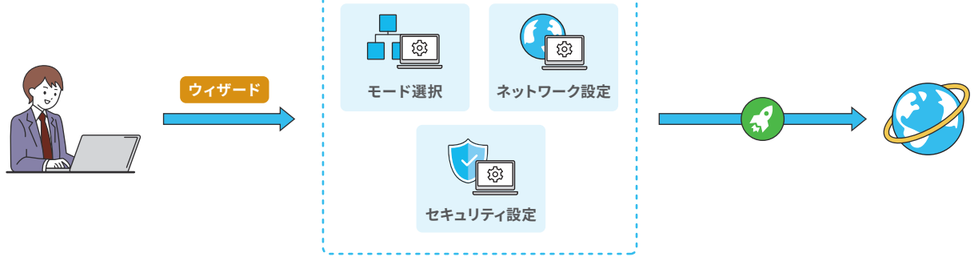
2 UTMのVPNで安心なリモートアクセス

社内ネットワークの中に専用の仮想ネットワークを構築し、リモートアクセスを利用したユーザーと社内のネットーワーク間の通信を確立できます。



3 迅速で簡単な導入で保守難易度を軽減

機器の設定と導入はウィザードを利用することで簡単にでき、長時間作業する必要がなく、作業負担を軽減できます。



4 業務管理ソリューションとの連携で更なるセキュリティ防御機能の向上と社内の端末を可視化

機能の紹介

V-Guard3000に搭載された次世代ファイアウォールやセキュリティ、便利な機能などをご紹介いたします。

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環境を提供します。

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セキュリティを保護します。IPSポリシー設定をサポートし、攻撃署名をカスタマイズすることができます。

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60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ができます。効果的にウイルスや不正ソフトを防御します。

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。

nCloud管理プラットフォーム
V-GuardのnCloud管理プラットフォームにより、管理者はいつでもどこでも簡単にV-Guard3000デバイスの管理と設定を行うことができます。

レポート
V-Guard3000にて検知したデータを書き出し、レポートとしてカスタマイズしてメールなどで配信できます。 配信頻度や時間を設定することも可能なのでお客様の環境に適した提供が可能です。

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
V-Guard3000で複数のゲートウェイにIPSec VPNを構築することができます。さらに企業間、本社-支社間のデータを暗号化することでアクセス制御したポリシーベースルーティングとポリシーベースVPNが提供できますのでより安全にデータ転送ができます。

アクセスVPN
社外にいるユーザがVPNで社内ネットワークにリモート接続することができます。暗号化と認証機能により、通信データの盗聴や改ざんを防止することも可能です。現在IKEv1とIKEv2のプロトコルスタックをサポートしておりますので、よりネットワークセキュリティの信頼性と高性能なマルチプラットフォーム環境の提供でオフィスを安全な環境にします。

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。

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、サイトのアドレスとコンテンツをフィルタリングする機能です。暴力表現やポルノ、業務に関係ないジャンルの事柄などを分類してサイトのアクセス制御します。

アプリケーション制御
日本国内や世界中でよく使われる3000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ていますのでフィッシングサイトやオンライン詐欺から企業のネットワークを守ります。

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、アプリケーション制御ログを提供し、オフィスへの脅威を迅速に把握できます。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もできます。

ワイヤレス
V-Guard3000の無線モジュールで無線環境を提供できます。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可能です。802.11a/b/g/n/acプロトコルに準拠し、電波の周波帯は2.4GHzと5GHzに対応しております。また、暗号化においてはAESとTKIPアルゴリズムに準拠しており、WEP/WPA2-PSK/WPA2-RADIUSなどのモードを選択可能です。

SSLインスペクション
V-Guard3000は大部分のSSL暗号化されたトラフィックに対して、チェックすることができます。アンチウイルス、アンチスパム、URLフィルタリング、IPSおよびアプリケーション制御などを含めます。データリークのリスクを最低限まで下げて、企業へ統合セキュリティを提供することが可能です。対応可能なSSLプロトコルにQUIC、HTTPS、IMAPS、POP3SおよびSMTPSが含まれます。

スペック

ハードウェアスペック

ハードウェア仕様	V-Guard3000
ハードウェア	Denverton
CPU	Intel Atom® Processor C3558
メモリー	8 G
ストレージ	64 G
インターフェース	WAN/LAN GB Ethernet Port x6 Dual Band Wireless-PCI-E,2.4G/5G IEEE 802.11 a/b/g/n/ac USB ×2 Console x 1
質量	1.25kg
サイズ	277{W} x 174.5{D} x 38{H}(mm)
消費電力と電源	ADS-65HI-12N-1,AC Max 48W
動作環境	0~40° C（Work) -40~70° C（Storage）
認証とコンプライアンス	CE emission, FCC Class A, RoHS, UL, VCCI

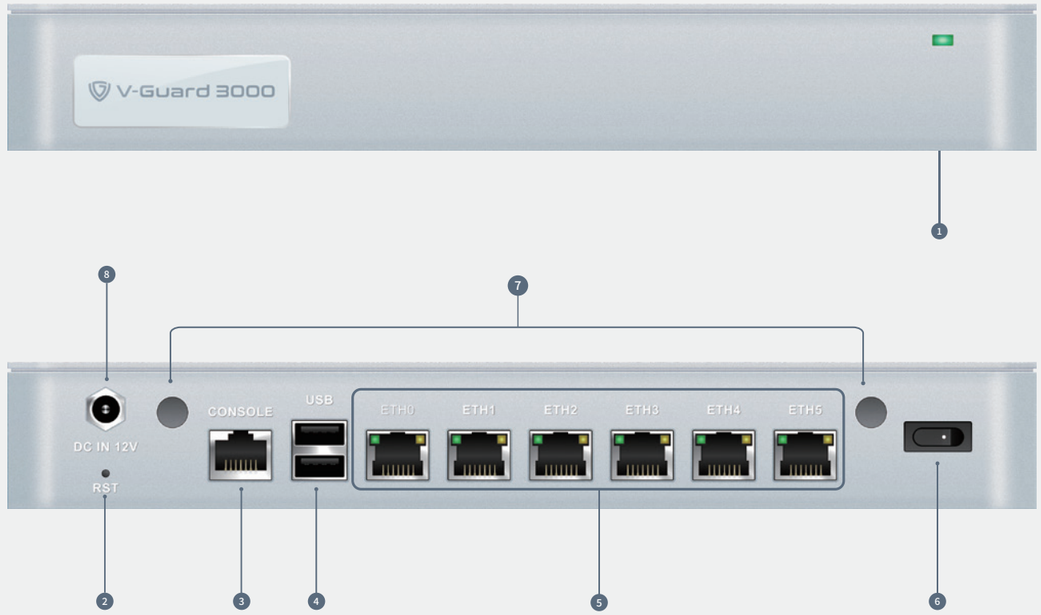
性能スペック

パフォーマンス	V-Guard3000
ファイアウォールスループット	6,000 Mbps
VPNスループット	1,900 Mbps
IPSスループット	800 Mbps
AVスループット	850 Mbps
最大同時接続数	500,000
新規接続数/秒	57,000

機器モデル

モデル	登録ユーザー数
V-Guard3000 S	15
V-Guard3000 M	30
V-Guard3000 L	100

ハードウェア仕様



1 設備ステータスランプ　2 リセットボタン　3 コンソールポート　4 USB ポート

5 WAN /LANポート　6 電源スイッチ　7 Wifi用アンテナ　8 電源コネクタ

サイバー保険

V-Guard3000には、サイバーセキュリティ事故や情報漏えいによる各種損害を補償する「サイバー保険」が付帯されています。

リスクの発見・確認 → リスクの分析・評価 → リスクの処理方法検討 → **リスクコントロールリスクファイナンシング実施**

『サイバー保険』で貴社の費用負担をカバーすることができます。

貴社が業務遂行するにあたって発生した、次の①または②に掲げる事由に起因する損害に対して保険金をお支払いします。

①ネットワークの所有、使用もしくは管理または情報メディア（※）の提供にあたり生じた偶然な事由
②情報の漏えいまたはそのおそれ

（※）電子データ、データベース、ソフトウェアおよびプログラムを指します。

SOMPO
損保ジャパン

【補償概要】
・賠償責任に関する補償
・事故対応に関する費用
事故につき合わせて100万円

損害賠償責任への対応費用	事故発生時の各種対応費用
●お詫び状送付費用 ●被害者への見舞金・見舞品 ●賠償金支払い ●情報漏えいのモニタリング など	●事故原因調査・影響範囲調査 ●会見・マスコミ対応・コールセンター設置 ●データ復旧・情報機器復旧 ●再発防止コンサルティング ●専門コンサルタントへの相談費用 ●文書作成や報告に要する費用 ●証拠収集費用・翻訳費用 など
他人に対する損害	事故対応に要する諸費用
	

保守・サポートサービスについて

「V-Guard3000」をご利用のお客様を対象としたサービスです。動作不良時のハードウェアの無償交換及びお困り事など何でもご相談いただけるオンラインサポートのセット保守となります。

ハードウェア保守
対象機器に動作不良などが生じた場合に、ハードウェアの交換対応をいたします。

オンラインサポート
お電話または電子メールにて技術サポートを受けることが可能です。「リモート管理ツール（nCloud）」を利用し、遠隔にてサポートいたします。

ご利用料金 FREE 無料

お問い合わせ・お申込みはこちら
0120-187-019
[受付時間] 月～金 / 9:00～18:00

エンドポイントセキュリティのご案内

Neusoft NISE1000

NISE1000は、業務分析機能により従業員の業務を可視化し、生産性の向上策を支援しながらPC端末をウィルスの脅威から全面的に保護する総合資産管理ソリューション製品です。

製品特徴

社内外PCの統合管理

従業員のWebサイト閲覧、アプリケーションの使用時間や使用人数、PCの利用時間、およびインターネット通信時間などを分析し、視覚的にわかりやすいグラフカルな表示を通じて、社内外のPC利用状況を統合的に管理するとともに作業の効率化と業務改善の支援ができます。

IT資産管理とセキュリティ

NISE 1000をIT資産管理ツールとして活用することができます。ネットワーク上のPCの機器情報やアップデート状況、ソフトウェアのインストール状況に加え、EDRとEPP機能を持つセキュリティも備えており、それらをNISEの管理プラットフォームから一括で確認することができるため、管理者にとっても利用しやすいツールとなっています。

UTM連携とクラウド管理

NISE1000は、ビジョンのUTM製品V-Guardと連携可能です。この連携により、エンドポイント情報がUTMに転送され、脅威と判断された端末の通信を自動的に遮断することができます。またNeusoftが提供するクラウド型管理プラットフォームnCloudを介して、V-GuardとNISE1000を集中的に管理できるため、利用者の管理負担を軽減できます。

ユーティリティ

【周辺機器の死活監視】社内サーバや複合機、Webカメラなど重要な機器に対して、Pingなどを使用してネットワーク診断を行うことにより、機器の障害による影響を最小限に抑え、問題を早期に解決することができます。
【USBメモリのウイルス対策】NISE 1000のUSBポートを使用して、USBメモリ内のファイルのウイルスチェックが可能です。

機能一覧

業務分析
インターネット使用時間統計
アプリ使用時間統計
PC使用時間統計

nCloud管理
NISE 1000のリモート管理
NISEのリモート管理

PC管理
PC情報収集
脅威検出
ソフトウェア管理
アカウント管理
リモートデスクトップ
UTM管理
脆弱性管理
社外PC管理
セキュリティポリシー
レポート

ユーティリティ
死活監視
USBメモリウィルス対策

セキュリティHUBのご案内

saxa セキュリティスイッチ
LG1000

マルウェア感染の拡大を防御。
安心・安全な社内ネットワークへ。

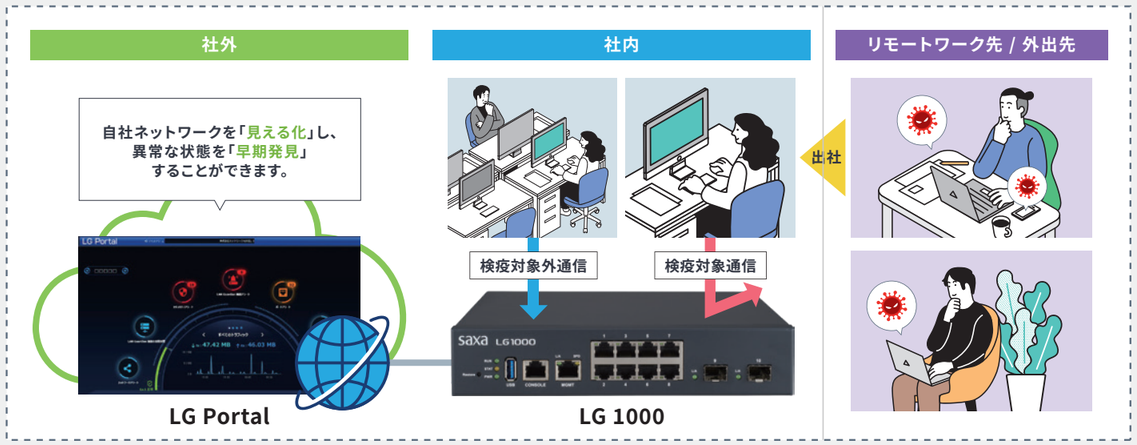
✔不正通信遮断機能
大量アクセス攻撃、不正侵入、盗聴＆なりすましなどの不正通信を遮断します。

✔LG Portal機能
遠隔操作で設定変更や状態確認が出来たり、検知した攻撃をレポート型式で閲覧ができます。

✔アラート機能
検知した情報を管理者にリアルタイムでお知らせし、驚異の早期発見ができます。

✔ウイルス感染PCブロック(サクサUTM連携)
社内ネットワークで異常な通信をしているPCを検知し、該当PCのネットワークを遮断することが可能です。

✔スケジュール機能
ポートの通信制限のスケジュール設定ができます。業務時間外の利用を禁止することが可能です。



セキュリティアクセスポイントのご案内

saxa セキュリティAP
LG1000AP

無線でもマルウェア感染の拡大を防ぎ、安心・安全な社内ネットワーク環境へ。

✔不正通信遮断機能
LG1000APに接続している端末からのさまざまな攻撃の通信やランサムウェアなどの拡散の通信をLG1000APで検知します。攻撃が発生している端末、かつ該当の攻撃通信のみLG1000APで遮断します。

✔LG Portal機能
遠隔操作で設定変更や状態確認が出来たり、検知した攻撃をレポート型式で閲覧ができます。

✔LG Portalネットワーク構成
遠隔管理と可視化
自動設定とアップデート
迅速なネットワーク構築と拡張
ランサムウェアなどの有害トラフィックの拡散を遮断

サーバーのご案内

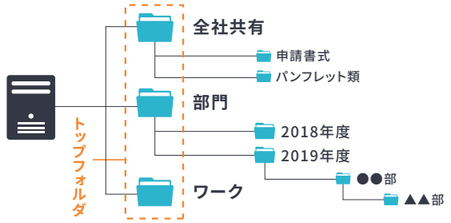
saxa 働き方改革サーバー
GF1000Ⅱ

これからのオフィスに、柔軟で新しい働き方を。

5年間ハードウェア無償保証＆駆けつけ保証

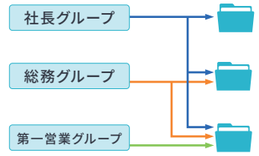
設置時から5年間分の機器保証(交換パーツ代不要)付き。
サポートセンターによる切り分け診断と、技術者による駆けつけ修理を行いますので、安心してお使いいただけます。

らくらくフォルダ管理 その1



アクセス権限はトップフォルダだけのシンプル管理!
ITスキルがなくても運用できます。余計な管理工数がかからず、専任の管理者でなくとも取扱い可能です。

らくらくフォルダ管理 その2



グループによるシンプルな権限設定が可能です。所属しているグループ単位でアクセス制御ができますので実際の社内体制に合わせて運用いただけます。

らくらくフォルダ管理 その3

アカウントを作成するだけで、個人専用の「マイボックス」が自動で作成されます。自分しかアクセスできない専用フォルダなので作成中のファイルや他の社員と共有したくないファイルの管理に便利です。

保守サービス / 機能 Maintenance

1 5年間ハードウェア無償保証＆駆けつけ保証

設置時から5年間分の無償機器保障(交換パーツ不要)がついています。
サポートセンターによる切り分け診断と、技術者による駆けつけ修理を行いますので、安心してお使いいただけます。

※自然災害またはお客様過失による場合は、有償修理となります。
※駆けつけ修理対応は翌営業日以降で調整となります。

2 リモート設定変更

お客様からのお電話で、ユーザーアカウントの追加や設定変更をリモートで対応いたします。

※サポートセンター運営時間に限ります。導入時に顧客登録されている必要があります。
※アカウントの削除や装置のIP変更など、運用に影響が出る可能性のある設定は対象外です。(サクサHPの製品紹介ページのリモート保守規約に詳細が記載)

3 停電監視機能

UPSの専用ソフトがなくても、停電時の自動シャットダウンに対応!

4 データ復旧サービス

HDDが2台同時故障した場合、ファイルを復元するサービスを無償提供します。

※本サービスはデータの100%復旧を保証するものではありません。
※本サービスはGF1000 II Proが対象となります。(GF1000 II Stdは対象外)
※データ復旧作業期間は10営業日が目安となります。なお故障の状態や容量によって作業期間が前後する可能性があります。
※詳細はサクサHPの製品紹介にある復旧サービス規定を参照してください。