NISE 1000

Neusoft Integrated Security EDR 1000

次世代トータルエンドポイントセキュリティ製品

EPP + EDR + 端末管理型

Neusoft

製品概要

NISE 1000は、ウイルス対策と端末セキュリティ管理を一体化した軽量な次世代端末セキュリティ製品です。脅威からPC端末を全面的に保護するとともに、従業員の業務分析機能により、業務の可視化と生産性の向上対策を支援します。また、UTMと連動し、nCloudを介した遠隔管理により社内外PCを一元管理でき、付加機能として周辺機器の死活監視とUSBメモリのウイルス対策機能を提供します。

導入メリット

- リアルタイム保護（PC常駐）とクラウド脅威情報を用いた検知で、新種のウイルスや未知の脅威も見逃しません。
- PCの脆弱性診断と自動修復の実施で万全なセキュリティ強化対策を実施します。
- UTMと情報連携することで、ネットワークの出入口の防御だけではなく、社内LANを含む全体の多重化セキュリティ対策を実現します。
- リモート接続によって、感染リスクのあるPCの調査、手動隔離、メンテナンス保守が簡単に実施できます。
- 感染後の自動対処、自動隔離、アラート通知とレポート分析によって、運用負担を軽減します。
- 管理画面で社内資産を一覧化し、セキュリティレベルやカテゴリー分類によって効率の良いセキュリティ運用が可能となります。
- 従業員のインターネットアクセス分析機能により、生産性の向上対策や業務改善対策を支援します。

NISE 1000製品››› 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、インターネット通信時間を分析し、グラフィカルに表示することで、社内外PCの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をサポートします。

UTMと連携

NISE　1000は、NeusoftのUTM製品NISGと連携が可能です。UTMへエンドポイント情報を転送し、脅威と判断した端末の通信を、自動的に遮断することができます。また、NISEエージェントをインストールしていない管理外PCが社内ネットワークに接続された場合も、自動的に通信を遮断することができます。

nCloud統合管理

クラウド管理プラットフォームnCloudを通して、NISGとNISE　1000を集中的に管理することができ、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。チェック結果をWEBベースの管理画面で確認でき、USBメモリによる内部ネットワークや端末へのウイルス感染を防ぐことができます。

軽量なハードウェア設備

NISE　1000は、コンパクトなデスクトップ型製品であり、企業のネットワークに簡単に導入できます。

NISE 1000製品 ››› 機能一覧

業務分析

インターネットとアプリ使用時間統計

PC使用時間統計

nCloudリモート管理

NISE 1000のリモート管理

NISGのリモート管理

ユーティリティ

死活監視

USBメモリウイルス対策

PC管理

PC情報収集

ソフトウェア管理

リモートデスクトップ

脆弱性管理

セキュリティポリシー

脅威検出

アカウント管理

UTM連携

社外PC管理

レポート

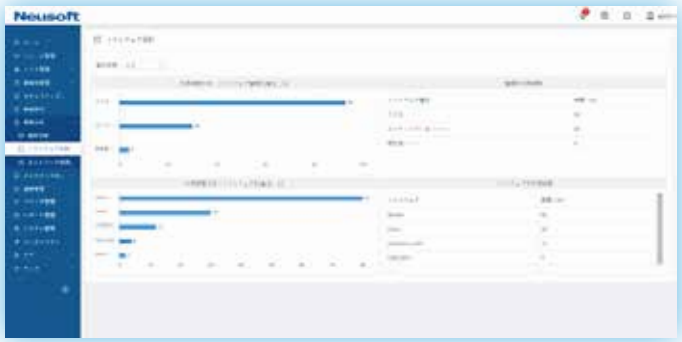
PC業務の分析と可視化

業務統計の概要

- サイト閲覧やソフトウェアの利用時間について、該当する操作人数が集計可能
- 各種操作（同一のサイト閲覧やソルトウェア利用）の社員ごとの実行時間が集計可能
- グラフ表示により、リソース投入の多い業務や業務時間の可視化が可能
- 統計結果により、業務調整と業務方針の見直しが容易に可能

社員の業務統計

- 社員毎のPC稼動時間、インターネット閲覧やアプリ利用にかかる時間に統計を行います
- 統計により、社員の業務が把握可能となり、業務の効率化に利用できます

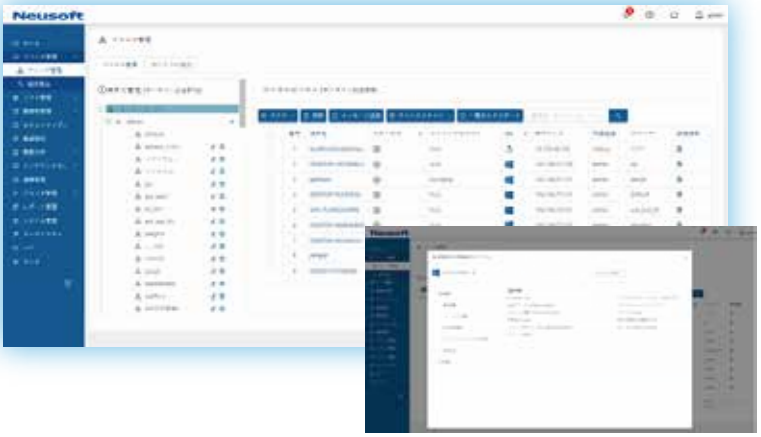


IT資産管理の手間を軽減

NISEエージェントをインストールしたPCの把握とインストールされているソフトウェアの状況を確認できます。
また、Windowsホストであれば、リモートで脆弱性を容易に確認できます。

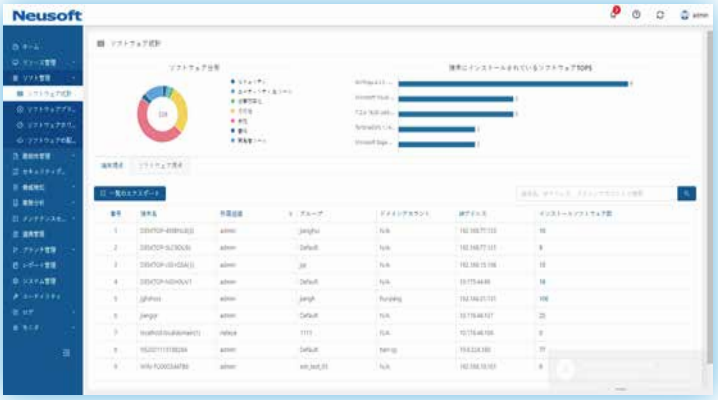
社内PCの利用状況確認

NISEエージェントをインストールした管理対象のPCの利用状況を把握することができます。
PCのハードウェアのリソース情報や、Windows OSの更新管理など、IT資産を適切に管理することができます。また、不正なソフトウェアによる異常な高負荷状態やネットワーク接続も確認することができます。
異常を確認した場合には、速やかに端末のシャットダウンや再起動を実施することができ、脅威の拡散を防止することができます。



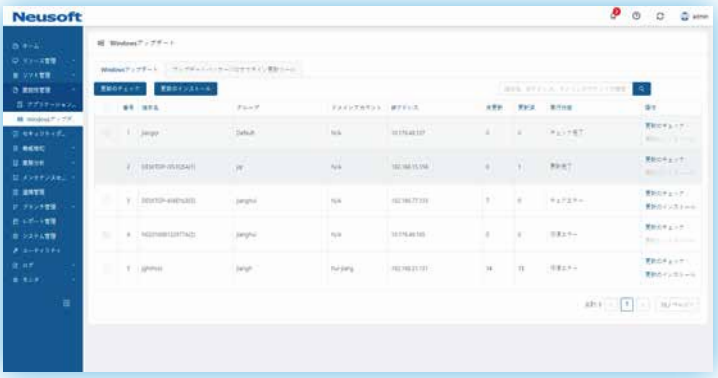
社内PCの利用ソフトウェアの確認

NISEエージェントをインストールした管理対象のPCにインストールされているソフトウェアを抽出し把握することができます。
許可されていないソフトウェアの無断インストールや、不正なソフトウェアのインストールを速やかに確認し対処することができます。
また、ソフトウェアをブラックリスト登録やホワイトリスト登録することで、業務に必要なソフトウェアのインストール制御と管理ができます。



Windowsの脆弱性管理

Windows OSの脆弱性情報を抽出・管理することができ、更新状況を確認することができます。
必要に応じて、リモートで脆弱性の更新を実行することができます。



リモートオペレーションによる運用の手間を軽減

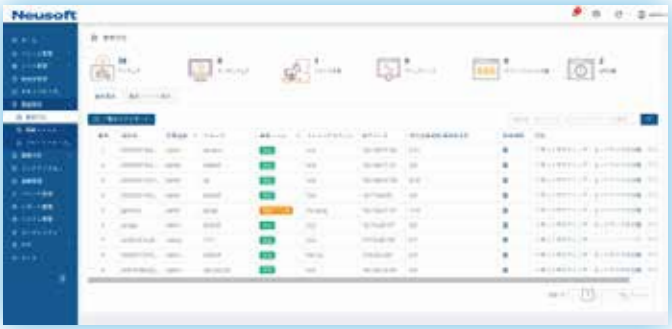
NISE 1000の管理プラットフォームを経由して、リモートで様々なオペレーションが可能です。ファイルスキャン、ネットワークアクセスのブロック、隔離ファイルの復旧などが可能であり、リモートデスクトップにより詳細に調査を実行することも可能です。

リモートからオペレーション実行

NISE 1000の管理プラットフォームを使用して、遠隔で様々なタスクを実行できます。
端末の再起動やシャットダウン、ウイルススキャン、リモートデスクトップなど、日々の保守において、現場に向かうことなく管理作業を実施できます。

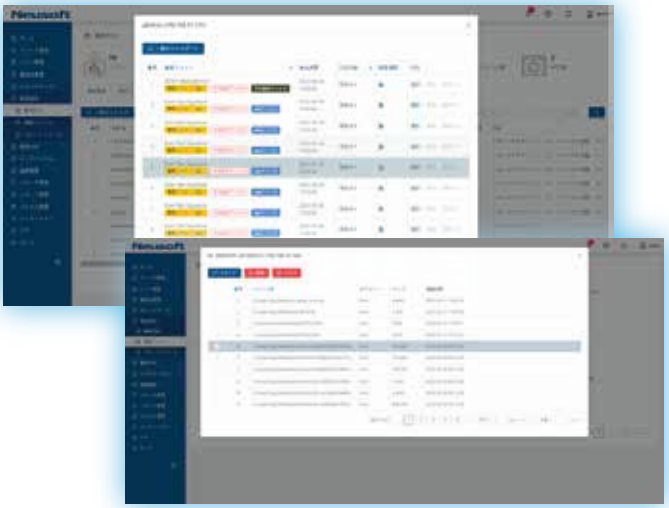
リモートからネットワークアクセスをブロック

端末が脅威を検出した場合、リモートで速やかに社内ネットワークから切り離すことができ、
不正アクセスの拡散を防止できます。
切り離した状態でも、統合管理プラットフォーム経由でリモートデスクトップにアクセスでき、調査が可能です。



万一の誤検知でもリモートで隔離ファイルを復旧

万一、正常なファイルを誤って隔離してしまっても、リモートから隔離の解除やホワイトリスト化することができます。

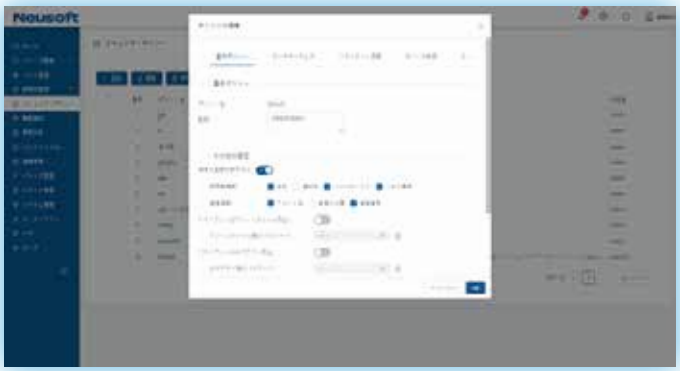


高機能な検知エンジンによる多様な脅威を防御

軽量化したシグネチャーベースの検知エンジンに加え、ふるまい検知エンジン、ブルートフォース攻撃検知エンジンなど、複数の検知エンジンを使用し、様々な脅威をより素早く、正確に検知します。
検知ポリシーは複数設定することができますので、業務内容に合わせた様々なセキュリティ対策パターンによる運用が可能です。

資産管理ポリシーの設定

社内の資産情報管理に関するポリシーを設定できます。
利用者でも資産情報の登録や変更を設定し、管理プラットフォームに転送することができますので、管理者の負担が軽減できます。
また、利用者によるNISEエージェントの強制終了やアンインストールの防止設定が可能です。
誤操作などでセキュリティエンジンが停止することを防ぎ、社外利用の多いPCでも、常に安全な状態を維持します。



セキュリティポリシーの設定

ご利用の環境に合わせて、マルウェアやブルートフォース攻撃の検知ポリシーを設定できます。
アンチマルウェアエンジンによるリアルタイム防御だけでなく、スキャンスケジュールを設定することにより、時間のかかるスキャンタスクを自動で実行し、利用者の作業の手間を軽減します。
ブルートフォース攻撃防御のリアルタイム防御設定により、検知時に自動でネットワーク通信を一定時間遮断することで攻撃による脅威の拡散が防止されます。

外部デバイスの接続制御設定

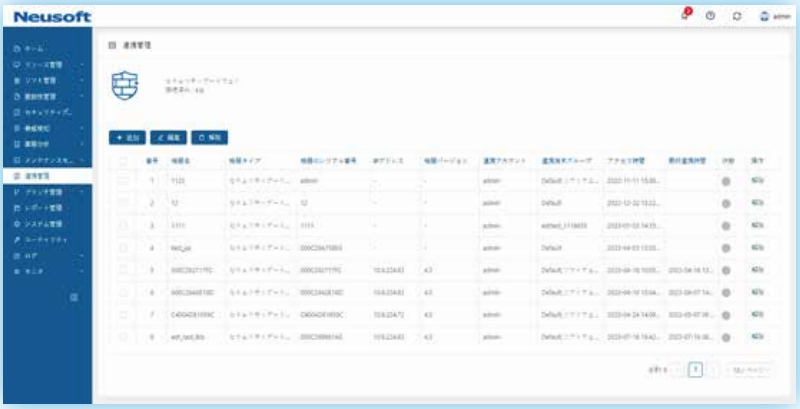
USBメモリやプリンタなど、端末に接続する様々なデバイスからの脅威の侵入防止や機密情報の漏洩防止のためにデバイスの接続制御を行うことができます。
ユーザーの業務内容に合わせた運用が可能です。

UTM連携によるPCアクセスを自動制御

NISE 1000をUTMのNISGと連携することで、防御をより高度にすることが可能となりました。UTMとの連携設定は、NISE 1000の管理プラットフォームとUTMの管理画面で簡単に設定可能です。連携により管理外PCのネットワークへのアクセスを自動的にブロックできるようになります。また、ユーザーごとのセキュリティポリシーに合わせたアクセス制御設定が可能です。

NISE 1000管理プラットフォームの設定

管理プラットフォームに、連携する機器の情報と連携に必要なキー情報を登録するだけで、連携が可能です。

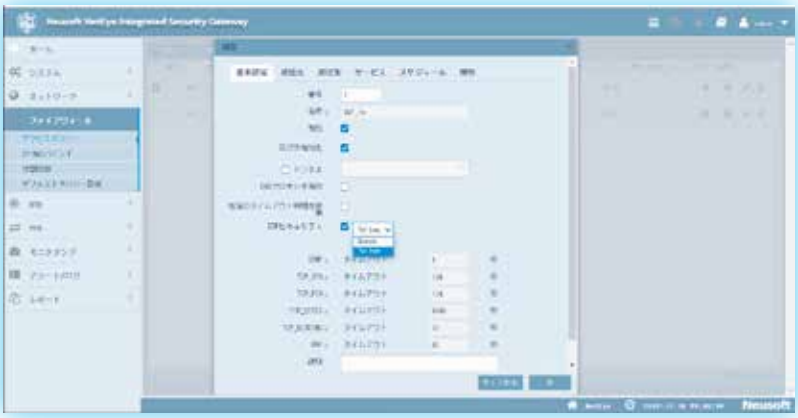


UTM側の設定

NISGに、連携する管理プラットフォームの情報と連携に必要なキー情報を登録するだけで、連携が可能です。

セキュリティポリシーに合わせたアクセス制御設定

NISGの設定で、ポリシーに合わせたアクセス制御レベルの設定が可能です。



ユーティリティ：周辺機器の死活監視

社内業務に必要なサーバや複合機、Webカメラなど重要な機器が、予期せぬネットワークトラブルが原因でダウンタイムが発生し、業務への影響が問題なる場合があります。ダウンタイムの発生を早期に検出するために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。

- 社内ネットワークに接続されているNAS、複合機、監視カメラなどのオンライン状態ををPingなどを使用し監視
- 監視中に反応がない機器があれば、アラート表示（PCなど、頻繁に外す機器はホワイトリスト登録可能）
- 機器状態の可視化により稼働状態を確認

ユーティリティ：USBメモリのウイルス対策

USBメモリ使用時の端末保護をNISE 1000を使用して保護することが可能です。
USBメモリをNISE 1000に挿入し、USBメモリ内のファイルのチェック結果をWEBベースの管理画面で確認できます。
USBメモリをNISE 1000を介してチェックすることにより、内部ネットワークや端末へのウイルス感染を防ぐことができます。

- USBメモリ挿入時、自動的にウイルススキャンを実行
- USBメモリ情報（シリアル番号、メーカ）を記録
- USBメモリチェック結果を記録
  NISE 1000のWEB画面にUSBメモリ情報とチェック結果を表示

nCloudによる統合機器管理

nCloudは、効率的で使いやすいクラウド管理プラットフォームです。Neusoft社のUTMとNISE 1000機器をリモートで集中管理でき、パートナーの管理負担と運用コストを軽減できます。

EDR機器のリモート集中管理

画面ですべてのEDR機器情報を確認できます。

- 基本情報：シリアル番号、運行情報、IPアドレス
- ライセンス情報：端末数、アクティベートされた端末数、有効期限
- 関連するUTM

下記操作を対応可能：

- ライセンス期限追加
- リモート管理NISE 1000

ハードウエア仕様&スペック

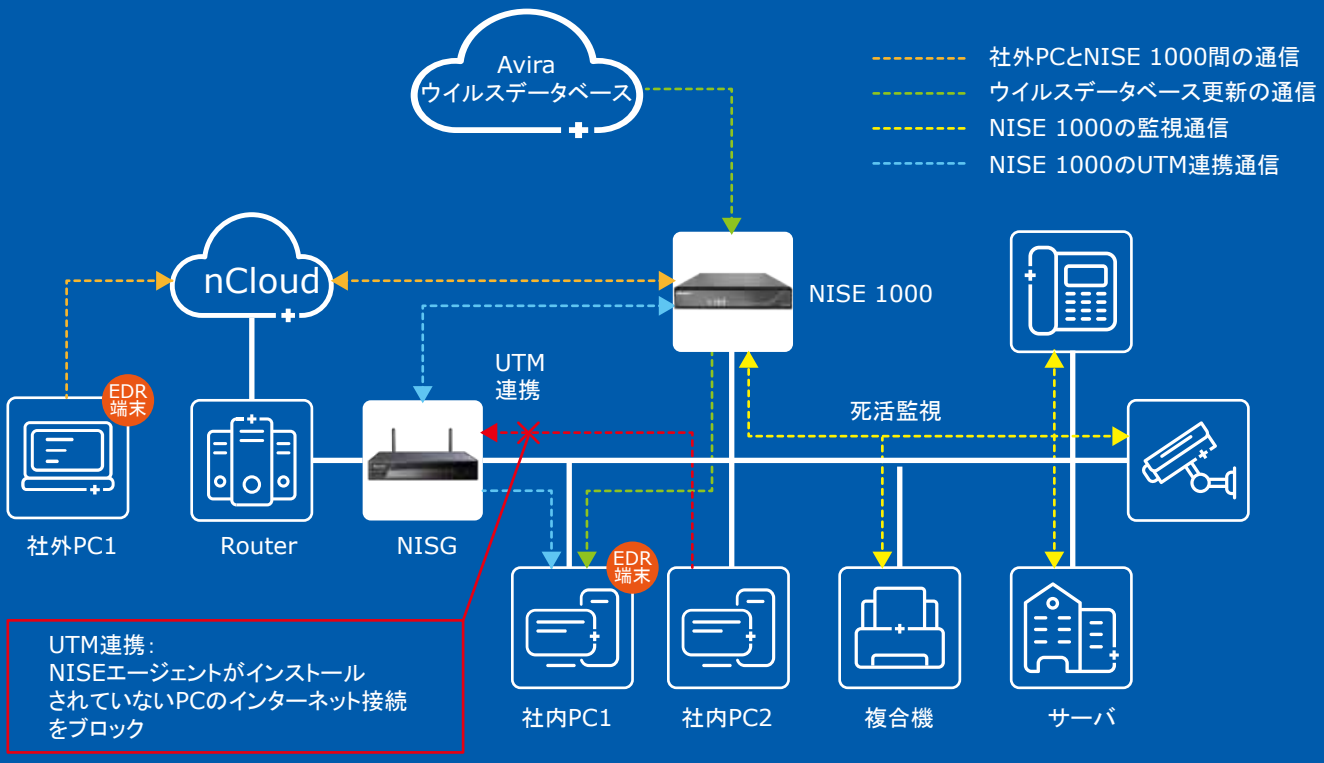
正面の筐体外観

NISE 1000

裏面の筐体外観

項目	仕様
接続端末数	50
インターフェース	4 x GB Ethernet RJ45 2 x Bypass (Optional), 1 x mini-PCIe
USB	2 x USB 2.0, 1 x Console, 1 x VGA
本体寸法	ミニ・デスクトップ型 173（L）*198（W）*37（H）（mm）
質量	1.04 kg
電源	DPS-60PBA. 60W. DC：12V-5A AC：100-240V, 50-60HZ
環境温度	-20℃~60℃
相対湿度	0~95%

NISE 1000製品 ››› 運用イメージ



エンドポイント保護	マルウェア対策、ランサムウェア対策、不正侵入防止、RDP不正アクセス対策 不正ソフトウェア自動隔離、不正ソフトウェア削除、Windows脆弱性更新 USB/Bluetooth装置利用可否制御
端末管理	端末ハードウェア情報取得、導入済みアプリケーション情報取得、 端末リソース(CPU、メモリ、ストレージ)利用率取得 パフォーマンス情報取得、導入サービス情報取得、ネットワーク利用プロセス情報取得 スタートアップ・タスクスケジューラの情報取得 組織別のソフトウェア導入管理(ホワイトリスト/ブラックリスト)
端末操作	再起動、シャットダウン、ネットワーク通信遮断、リモートデスクトップ接続 ウイルススキャン、ソフトウェアの隔離、ソフトウェアのアンインストール
対応OS・リソース	NISEエージェント Microsoft Windows 11 / 10 / 8.1 / 8 / 7 Windows Server 2019 / 2016 / 2012 / 2008 メモリ容量:4GB以上 ディスク容量:128GB以上

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: 0120-655-350
E-mail: securitybz.jp@neusoft.co.jp
http://neteye.neusoft.com/jp/