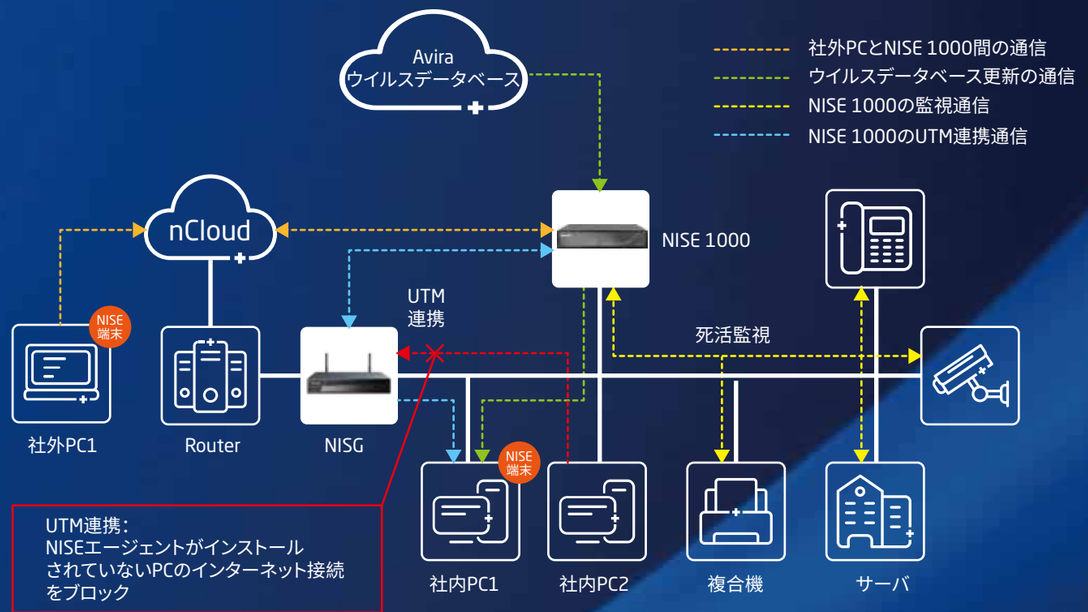
## NISE 1000製品 ››› 運用イメージ




| | |
|---|---|
| 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<br>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<br>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、<br>端末リソース（CPU、メモリ、ストレージ）利用率取得<br>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<br>スタートアップ・タスクスケジューラの情報取得<br>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<br>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<br>Microsoft Windows 11 / 10 / 8.1 / 8 / 7<br>Windows Server 2019 / 2016 / 2012 / 2008<br>メモリ容量：4GB以上<br>ディスク容量：128GB以上 |

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: neteye.neusoft.com/jp/

# NISE 1000

## Neusoft Integrated Security Endpoint 1000


SMB向け資産管理ソリューション製品

端末管理　＋　死活監視　＋　EPP

Neusoft

## 製品概要

NISE 1000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端末をウイ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。

## 導入メリット

- インターネットアクセス分析機能により、生産性向上や業務改善の支援が可能です。
- 死活監視機能とUSBメモリのウイルス対策により、周辺機器や持ち込まれたUSBメモリに関連する問題を検出し、対処できます。
- 企業が使用を許可していないソフトを従業員が勝手にインストールするなど、コンプライアンス違反の監視に役立ちます。
- 脆弱性診断や修復の実施、リアルタイム保護とクラウド脅威情報を用いた未知のウイルス検知などセキュリティ対策も万全です。
- リモート接続やUTMの連携による感染後の自動対処により、メンテナンス保守を容易に実行できるため、運用コストを軽減できます。

## NISE 1000 ››› 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ィ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、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

NISE 1000は、NeusoftのUTM製品NISG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、NISGとNISE 1000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。

## NISE 1000 ››› 機能一覧

# PC業務の分析と可視化

「業務分析」とは、企業や組織内の業務を可視化することで、業務の実態を把握し、改善するプロセスのことを指します。
統計結果に基づいて、業務の調整や業務方針の見直しが容易になります。

### 業務統計

- PCを操作した際、サイトの閲覧やソフトウェアの利用時間について、該当する端末の集計が可能
- サイトの閲覧やソフトウェアの利用時間を端末ごとに集計
- グラフで可視化されているのでリソースの多い業務が一目瞭然


### 社員ごとの業務統計

端末ベースでPCの稼働時間、インターネット閲覧、アプリの利用時間の統計を可視化し、社員ごとの管理が可能です。統計結果により社員の業務状態が把握可能となりますので効率化するためのデータとして活用できます。

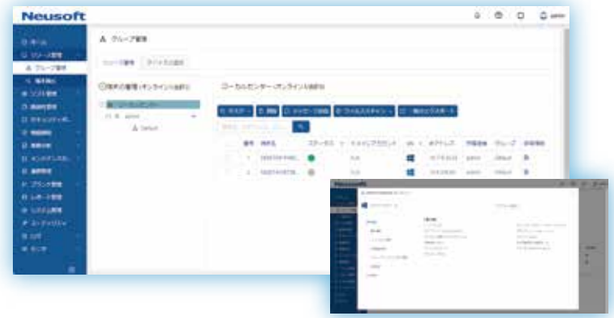


# IT資産管理の手間を軽減

「IT資産管理」とは、企業や組織内のハードウェアやソフトウェアなど、ITに関連する資産の状況を把握し、管理することを指します。
NISE 1000を管理のツールとして利用することで、セキュリティ対策やコンプライアンス対応、コスト削減が可能です。

### 社内PCの利用状況確認

NISE 1000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リース情報や、Windows OSの更新なども可能です。
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、速やかに端末のシャットダウンや再起動を実施、脅威の拡散を防ぎます。

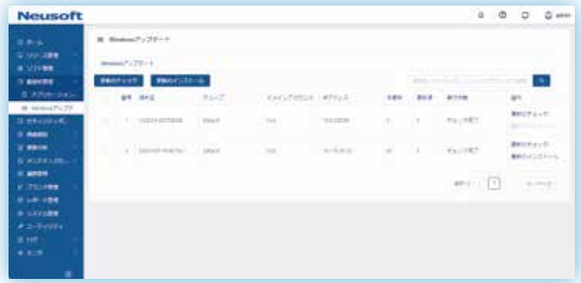



### 社内PCの利用ソフトウェアの確認

NISE 1000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確認することができます。
許可されていないソフトウェアのインストールや、不正なソフトウェアのインストールを速やかに発見、対処が可能です。
また、事前に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、インストール状況の管理も可能です。


### 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。
（Windowsのみ対応）



## リモートオペレーションによる運用の手間を軽減

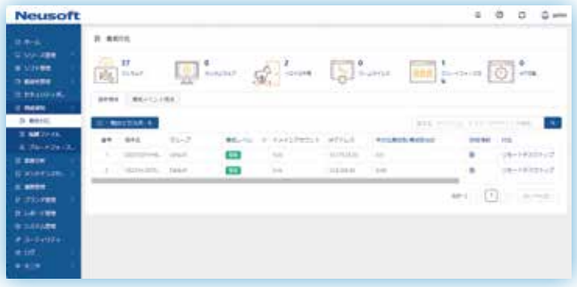
NISE 1000の管理プラットフォームを経由して、リモートで様々なオペレーションが可能です。ファイルスキャン、ネットワークアクセスのブロック、隔離ファイルの復旧などが可能であり、リモートデスクトップにより詳細に調査を実行することも可能です。

### 豊富なオペレーション内容

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。

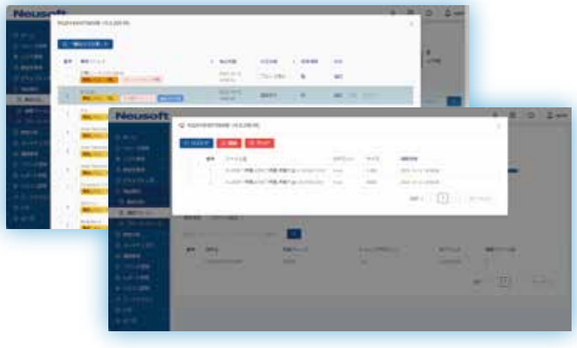

### ネットワークアクセスをブロック

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。




### 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、リモートで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出来ますので、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。
管理者による資産管理の負担を減らすため、利用者が登録・変更した資産情報を自動的に収集することが可能です。
また、利用者によるNISE 1000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はなく、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

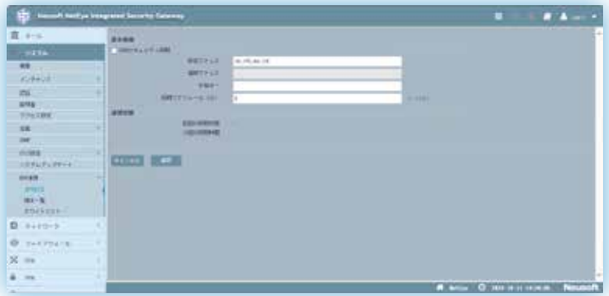
NISE 1000をNeusoftのUTM NISGと連携することにより、防御をより強固にすることができます。
連携設定により管理外の端末のネットワークアクセスを自動的にブロックできるようになります。

### 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を決めて登録するだけで、簡単に連携ができます。


### UTM側の設定

NISE 1000の管理プラットフォームに設定したものと同じキーを登録するだけで連携できます。



### セキュリティポリシーに合わせたアクセス制御設定

連携するとNISG内に設定追加できるようになるため、ポリシーに合わせたアクセス制御が可能になります。

## ネットワーク機器の死活監視

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、業務に問題が起こらないよう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るNASやサーバ、複合機、監視カメラなどのオンライン状態をPingを使って監視します。
- 監視中に反応がない機器があれば、アラート表示されます。PCなどの頻繁に外す機器があれば、ホワイトリスト登録も可能です。


## USBメモリのウイルス対策

USBメモリをNISE 1000のUSBポートに接続してウイルスチェックを行うことで、内部ネットワークへのウイルスの感染を防ぐことができます。

- USBメモリを挿入し、ウイルススキャンを実行
- USBメモリの情報（シリアル番号、メーカ）を記録
- USBメモリのチェック結果を記録
  NISE 1000のWEB画面にUSBメモリの情報とチェック結果を表示します。

# nCloudによる統合機器管理

クラウド型管理プラットフォーム「nCloud」でNISE 1000を連携させることで遠隔の管理が可能となり、技術者派遣などの運用コストを削減できます。

NISE機器のリモート集中管理

専用ページですべてのNISE 1000の機器情報を確認することができます。

- 基本情報：
  シリアル番号、IPアドレス、運用情報など
- ライセンス情報：
  端末数、アクティベート端末数、有効期限
- 連携したUTM機器の情報
- クラウド上で操作可能な設定：
  ライセンスの期限追加、リモート管理


# ハードウエア仕様&スペック


筐体外観：正面

NISE 1000


筐体外観：裏面

| 項目 | 仕様 |
|---|---|
| 最大接続端末数 | 60 |
| インターフェース | 4 x GB Ethernet RJ45 |
| USB | 2 x USB 2.0, 1 x Console |
| 本体寸法 | 173 (L) *200 (W) *38 (H) (mm) |
| 質量 | 1.10 kg |
| 電源 | DPS-65VB, 65W<br>DC:12V-5.417A<br>AC:100-240V, 50-60HZ, 2.0A |
| 作業環境温度 | -10°C~60°C |
| 相対湿度 | 5~95% |