NISE

Neusoft Intelligence Security EDR

次世代トータルエンドポイントセキュリティ製品

EDR＋EPP＋端末管理型

Neusoft

製品概要

NISEは、すべてのセキュリティ脅威からPC端末を保護し、企業の事業継続性の確保をサポートする、総合セキュリティ製品です。
統合的なクラウド管理プラットフォームと軽量化されたエンドポイントセキュリティで、企業のセキュリティを強化します。

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。
- クラウド管理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よいセキュリティ運用が可能となります。

NISE製品 ››› 製品特徴

EDR+EPP+端末管理型のトータルエンドポイントセキュリティ

EDR と EPPを備えたセキュリティ強化に加え、IT資産も総合的に管理できます。
デバイス名、IPアドレス、MACアドレス、組織情報、資産情報等を一覧表示することで、効率よく社内ネットワークの管理ができます。

多機能で軽量化したマルウェア検知エンジン

従来のシグネチャーベーススキャンは、膨大なシグネチャーデータベースを使用するため、メモリリソースを多く使用しパソコンに高負荷がかかります。
NISEは、軽量化したシグネチャー、AIクラウドエンジン、ふるまい検知など、複数のエンジンで端末の負荷を軽減し、より素早く正確にマルウェアを検知できます。

リモートデスクトップ管理

NISEは、クラウド上の統合管理プラットフォームを使用して、脅威を検知した端末にリモート接続し、ウイルスのブロックや削除、脅威調査を行うことができます。
また、リモート接続時にファイルのコピー操作も禁止されますので、感染していない端末に対しても脅威の拡散を防ぐことができます。

IT資産管理と脆弱性診断

NISEは、企業にあるPC及びインストールされたソフトウェアの一覧情報を取得し、セキュリティ脆弱性の有無をリアルタイムで診断することができます。
脆弱性を検出した場合、アラートでの警告および管理者による強制アップデートの実施も可能です。
また、社内のIT資産を可視化することによって、効率よく統合的に管理することができます。

UTM連携

NISE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、脅威と判断した場合、自動的に通信を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。

NISE製品 ››› 機能一覧

【 主要機能 】

NISE

- リアルタイム保護
- 資産管理
- マルウェア検知
- セキュリティー括設定
- フィッシング対策
- 周辺機器の調査
- ランサムウェア対策
- ネットワーク保護・UTM連動
- リモートVPN接続
- アラート・ログ解析・レポート

【セキュリティ防御方法】 NISE

セキュリティ強化
- 脆弱性診断
- ファイアウォール
- 脆弱性自動修復

予防
- シグネチャースキャン
- クラウド脅威情報
- デバイス制御

検知と対処
- プロセス監視
- アンチマルウェア
- ウイルス隔離＆駆除
- リモート手動対処 通信ブロック

レポートと通知
- ダッシュボード&レポート
- 通知メッセージ

UTM連携によるPCアクセスを自動制御

NISE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

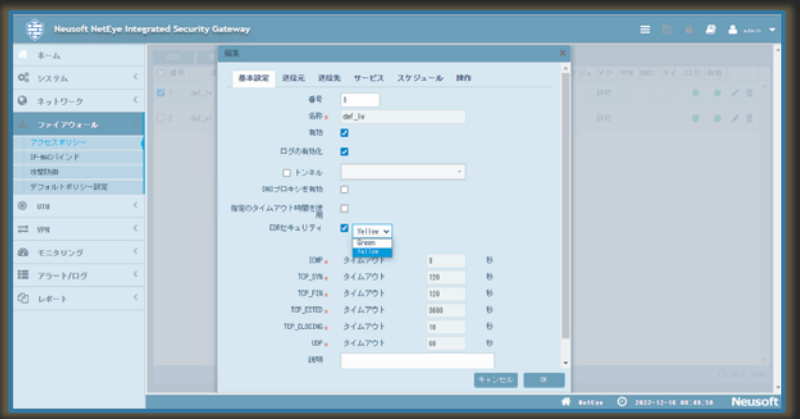
管理プラットフォームに、連携する機器の情報と連携に必要なキー情報を登録するだけで、連携が可能です。

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

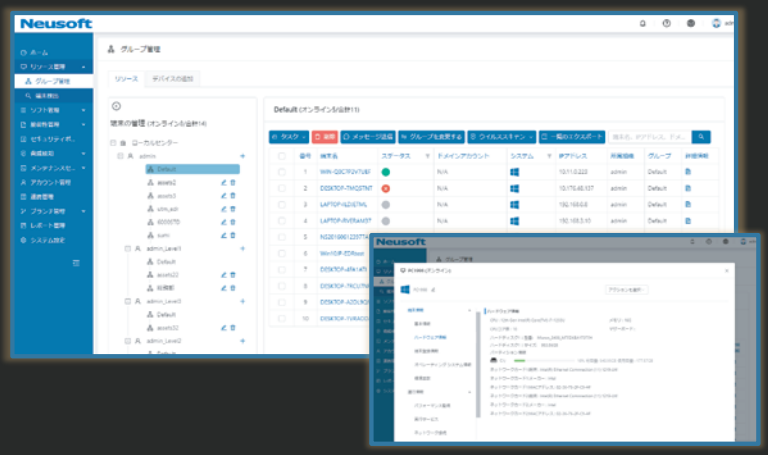


IT資産管理の手間を軽減

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、WindowsOS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。

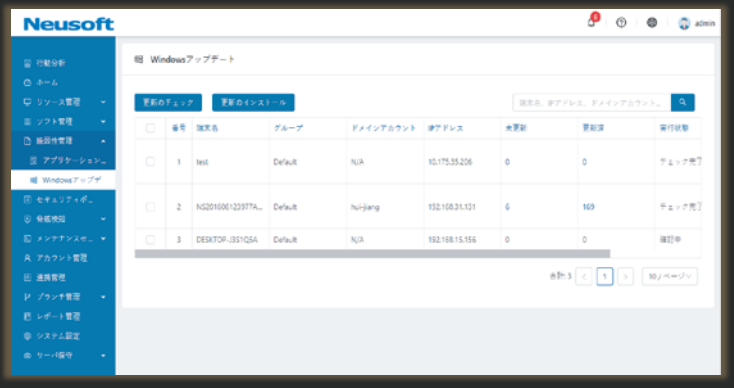


社内PCの利用ソフトウェアの確認

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

WindowsOS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。

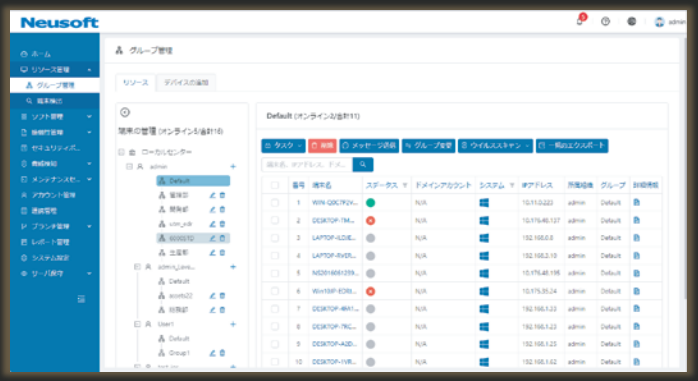


リモートオペレーションによる運用の手間を軽減

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。

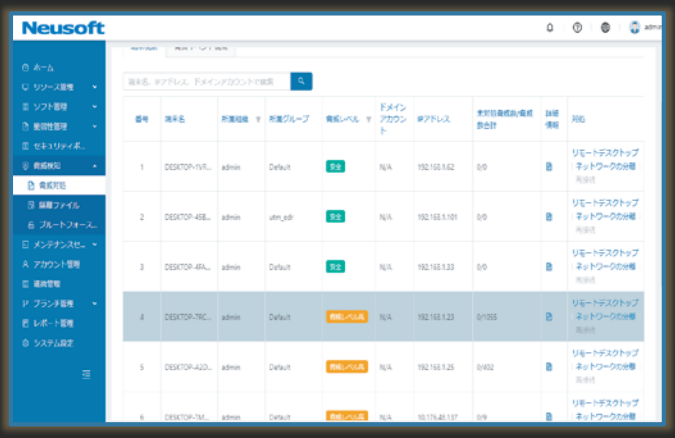
リモートからオペレーション実行

クラウド上の統合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。



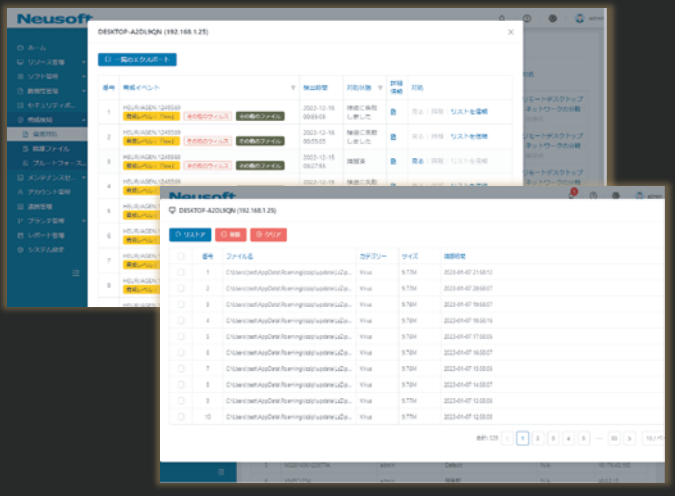
リモートからネットワークアクセスをブロック

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。



NISE 製品 ››› 運用イメージ

統合管理プラットフォーム

多様な環境に存在する
端末を一元的に統合管理

社内PC

パブリッククラウド

プライベートクラウド

ミックスクラウド

社内サーバ

物理PC、サーバ、IPC

クラウドデスクトップ

統合管理プラットフォームを利用することで、
オフィスネットワーク及びデータセンターのリソースを守ります。

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