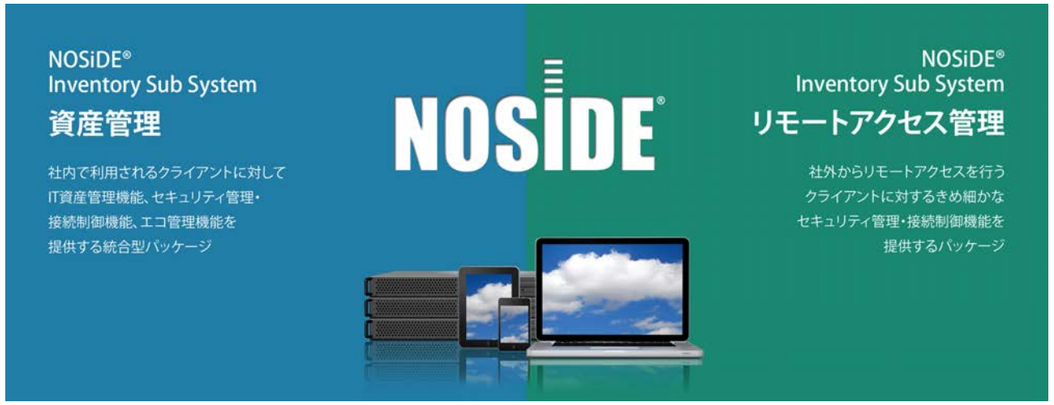
■NOSiDE® Inventory Sub System について

NOSiDE® Inventory Sub System は、社内で利用されるクライアントデバイスの各種管理機能・セキュリティ対策機能を提供するパッケージソリューションです。
利用目的・適用箇所に応じて2種類の製品を提供しています。



NTTデータ先端技術株式会社
ソリューション事業部　パッケージソリューションビジネスユニット
〒104-0052　東京都中央区月島 1-15-7　パシフィックマークス月島
URL http://noside.intellilink.co.jp/　E-mail：noside-info@intellilink.co.jp

NTT DATA
Global IT Innovator

NOSiDE®

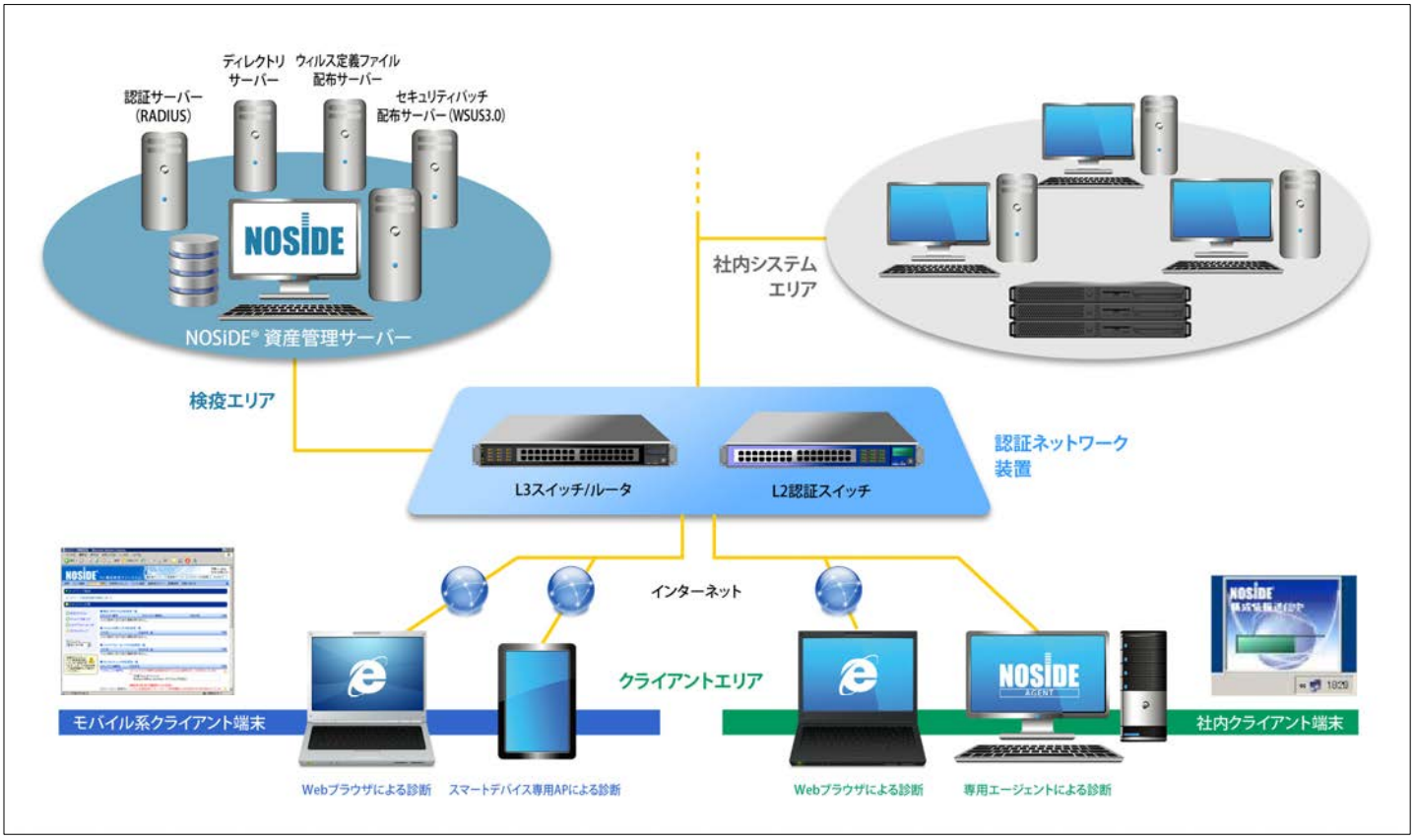
NOSiDE Inventory Sub System
資産管理

セキュリティ・IT統制・PCエコ管理
対応型統合ソリューション

NTTデータ先端技術株式会社

NOSiDE®
資産管理

「NOSiDE® Inventory Sub System 資産管理」は、社内の多種多様な端末資産から取得する情報をもとに、端末のセキュリティ診断や接続制御、さらには IT 資産管理や PC 消費電力管理を可能とします。
エンドポイントセキュリティ管理、IT 資産管理、エコ管理の統合機能により、IT 化の進展や端末デバイスの高性能化・ネットワーク化に伴い多様化・複雑化している企業情報システムにおけるクライアント端末の安全な利用に貢献するとともに、業務端末における適性なライセンス使用状況の確認や省エネ貢献も可能とする統合型エンドポイント管理パッケージです。



セキュリティ管理

社内 LAN 接続時に、端末から情報収集を行い、サーバのポリシー情報との照合により、クライアントのセキュリティ対策状況を検査・判定し、その結果に応じ最新のパッチを即時に適用したり、アクセスコントロール（接続制御）を行うことが可能です。さらに、各クライアントの接続認証ログやセキュリティ対策状況の一元管理を可能にします。

●端末セキュリティ診断機能

社内 LAN に接続された端末に対して、オンデマンド、あるいは定期的にセキュリティ診断を行うことが可能です。多様なネットワーク装置との連携により、さまざまな導入環境・防御ニーズへの対応が可能です。
診断可能な項目は以下のとおりです。

- ●OS パッチ適用状況診断
- ●ウィルス対策ソフト状態診断
- ●ファイアウォールソフト状態診断
- ●カスタムチェック
  - ・ソフトウェア診断
  - ・ファイル診断
  - ・レジストリ診断
  - ・プロセス・サービス診断
- ●端末/ユーザ単位の接続可否判定（MAC アドレス等）

●端末診断後のアクション

端末診断の判定結果に応じて、以下のアクションを実行することが可能です。

合格（〇）	検査条件を満たす状態（すべての検査項目が合格または警告となった場合、社内ネットワークへの接続を許可）
不可（×）	検査条件を満たしていない状態（検査項目が一つでも不合格となった場合、社内ネットワークへの接続を拒否）
警告（△）	検査条件は満たしていないが、設定期限内のため、合格と同等の扱い（社内ネットワークへの接続を許可するが、期限内に対策をとるよう、警告を表示）

●端末セキュリティ診断結果に応じたアクセスコントロール

社内 LAN 接続時の端末診断結果に応じて、以下の方法で端末の接続制御を行うことが可能です。

認証スイッチ連携	認証機能を持つ NW スイッチによる制御
ARP 偽装アプライアンス連携	ARP 情報を制御する専用デバイスによる制御
SSO 認証基盤連携	シングルサインオン認証基盤によるサービスの利用制御

●認証スイッチ連携

多様なネットワーク装置との連携により、さまざまな導入環境・防御ニーズへの対応が可能です。

■連携可能なネットワーク装置

Web 認証スイッチ	Apresia 2024 / 2124 / 4348 / 4248（日立金属）［※1］
	NetScreen 5GT/25/50/204/208/500（Juniper Networks）［※2］
	SSG シリーズ（Juniper Networks）
	OmniSwitch シリーズ（Alcate-Lucent）［※3］
	Mobility Controller シリーズ（ARUBA Networks）［※4］
	Secure Controller（Top Layer Networks）［※5］
	AX1230S / 2430S（アラクサラネットワークス）
802.1X認証スイッチ	DGS3426 / DGS-3200-10（D-Link）
	Apresia2124（日立金属）［※1］
	AX1230S / 2430S（アラクサラネットワークス）
	DGS3426 / DGS-3200-10（D-Link）
	Catalyst2940 / 2950 / 2960（Cisco Systems）
	H3C S5100（H3C Technologies）
	Summit X450, Summit 200（Extreme Networks）
	Enterasys Matrix N シリーズ（Enterasys Networks）

※1 Apresia®の Access Defender もしくは NA オプションが必要です。
※2 NetScreen®5GT を利用する場合、Extended オプションが必要です。
※3 OmniSwitch の IP アドレス再取得 Applet 使用時には、資産管理エージェントは使用できません。
※4 Aruba Policy Enforcement Firewall オプションライセンスが必要です。
※5 TLNS 認証サーバの設定が必要です。

●ARP 偽装アプライアンス連携（オプション）

ARP 偽装アプライアンスとの連携によるネットワーク接続制御に対応することも可能です。

※連携可能な ARP 偽装アプライアンスについてはお問い合わせください。

●SSO 認証基盤連携（オプション）

シングルサインオン認証基盤製品との連携により、端末診断に合格した端末のみ、特定の Web アプリケーションのみへの接続を許可することが可能です。

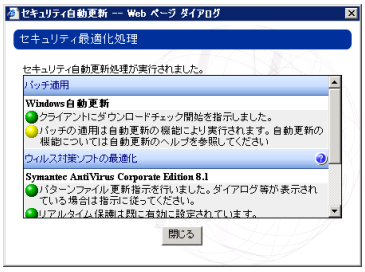
※連携可能なシングルサインオン認証基盤についてはお問い合わせください。

●その他の制御機能

未登録 PC の制御	社内接続を許可するマシンの固有情報（MAC アドレス/マシンシリアル/IP アドレス等）の登録有無による不正接続の防止が可能です。
非推奨ソフトウェア診断機能	Winny、Share 等の非推奨ソフトの利用状況を検査し、検査履歴の記録や発見時のソフト強制削除、管理者への通知等が可能です。

●クライアント治療機能

Web ブラウザによる端末チェック時に、未適用パッチがあったり、ウィルス定義ファイルが古かった場合、設定を最新状態に更新することが可能です。
また、WSUS（Windows Server Update Services）連携により、セキュリティチェックに不合格となったクライアントに対して、Microsoft Update サイトへの接続等を行うことなく、即座にパッチのダウンロード・インストールを行うことが可能です。



■セキュリティ最適化処理画面

検査不合格クライアントの治療（最適化）機能	クライアント検査の結果、対策に不備があるために不合格と診断された場合、パッチの適用やウィルス定義ファイルの更新等の治療指示が可能です。 WSUS 連携による診断後のパッチ即時適用や、利用者の指示による手動実行にも対応可能です。

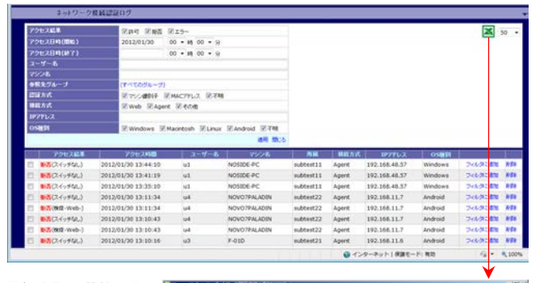
●検疫後拡張機能

セキュリティチェックに合格したクライアントには、以下のサービスを提供することが可能です。

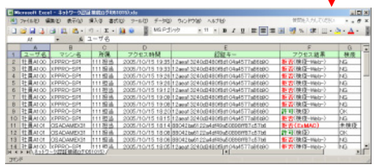
リモートデスクトップ接続の実行（検査に合格した Windows / Mac OS X クライアント）	社内接続が許可されたクライアントのリモートデスクトップ接続が可能です。これにより、社内接続時の情報漏洩リスクの低減が可能となります。
RemoteApp アプリケーションの公開（検査に合格した Windows クライアント）	RemoteApp 機能を利用して、社内接続を許可されたクライアントに対してアプリケーション単位でのシンクライアント型サービスを提供することが可能です。また、クライアントが利用できるアプリケーションをユーザ・グループごとに制限することも可能です。
プログラム実行（Windows / Mac OS X / Linux クライアント）	検査に合格/不合格となったクライアントそれぞれについて、コマンド実行により、クライアントにあるプログラム（スクリプト等）の自動実行を行うことが可能です。

●ネットワーク接続認証ログ管理

ネットワーク接続時の検疫ログが一覧でき、ユーザ/マシン単位、あるいは OS 種類別に、認証方法（検疫/許可/拒否）を指定することも可能。また、ログから対象端末の MAC アドレス等をフィルタに追加することが可能です。



■ネットワーク接続認証ログ画面（認証ログの外部出力も可能）



●検疫辞書管理機能

クライアントのセキュリティ診断を行うためにサーバに保持する辞書データのうち、Windows パッチ情報、ウィルス対策ソフト定義ファイル情報については、自動メンテナンスが可能です。

●セキュリティ対策状況の一元管理

管理者に対して、組織内 PC のセキュリティ対策状況を一元管理するための I/F を提供すると同時に、未対策 PC への警告・遠隔操作等の対策手段を提供します。

■セキュリティ対策状況一覧画面と未対策 PC への対応

是正項目を記載した警告メールの送信

リモートデスクトップ接続による遠隔操作

エコ管理

一般オフィスにおける PC の消費電力を概算する機能により、オフィスの省エネルギー対策をサポートします。

●エコ管理機能の動作イメージ

IT 機器の利用に伴う電力消費状況を「見える化」するとともに、省電力施策のシミュレーション機能や、省電力ポリシーの配布機能により機器の省電力対策の実施に貢献します。

●「ゼクノタップ」の併用で総合的に省力化

電力計と無線機能を内蔵したインテリジェント電源タップ「ゼクノタップ（XECHNO® TAP）」と NOSiDE®の連携により、消費電力をタップ単位できめ細かく管理したり、終業後の電源 OFF を自動制御することなどが可能になります。

■ゼクノタップ コントローラ（左）とコンセント（下）

IT 資産管理

コンピュータを構成するインベントリ情報（クライアントハードウェア・ソフトウェア情報）を収集し、管理サーバに DB 登録を行うことで、IT 資産管理業務の効率化に寄与します。

●インベントリ情報収集機能

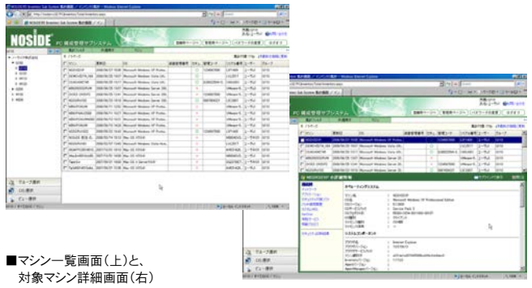
下記のソフトウェア/ハードウェア各情報を収集します。検疫実行時にも、バックグラウンドでインベントリ情報を自動収集することが可能です。

ソフトウェア情報	OS 情報、Webブラウザ情報、アプリケーション情報、ウィルス対策ソフト情報、ファイアウォール情報、パッチ情報、その他
ハードウェア情報	マシン情報、BIOS 情報、CPU / メモリ / HDD 情報、ネットワーク情報、その他

※管理者の追加定義により、取得項目を追加することも可能です。
※カテゴリ単位で収集項目の絞り込み・収集頻度の変更を行うことも可能です。

●PC 集計機能

マシン別、ユーザ別、セキュリティ対策状況別、ソフトウェア別、未使用ライセンス、サブネット別といった切り口でのマシン集計が可能です。

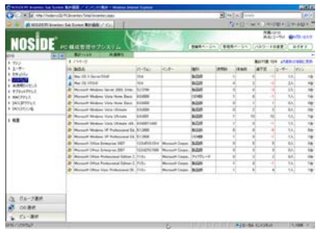


■マシン一覧画面（上）と、対象マシン詳細画面（右）

●ソフトウェアライセンス管理機能

ソフトウェアライセンス管理の重要性は日増しに高まっていますが、実現は容易ではありません。当システムの導入により、効率的なソフトウェアライセンス管理を実現します。

■ライセンス一覧画面
全体、部署別、OS 別、アプリケーション別など、様々な切り口でソフトウェアライセンスの過不足を集計することが可能です。
ライセンスが余っている組織から、不足している組織へ移動する処理が簡単に行えるため、ライセンスの有効活用が図れます。



●集計帳票出力機能

集計データを簡易な操作でワークシートに帳票出力することができます。

●カスタムビュー機能

PC から収集したインベントリ情報の集計時に、ユーザ定義による帳票を作成し、帳票出力することも可能です。

●契約資産管理機能

会計・購買系システムから契約資産情報（固定資産、リース・レンタル、購入物品、保守）を CSV ファイルでインポートし、インベントリ情報と連携管理することが可能です。

●ライセンス管理ワークフロー機能

ソフトウェアライセンスの棚卸業務（ライセンス購入数・使用実態の調査・調整）を実施するためのライセンス管理ワークフロー機能を搭載しています。

●その他の特徴

ソフトウェアライセンス管理用の種別設定機能、ソフトウェア追加検出機能、ライセンス集約機能を搭載しています。

対応プラットフォーム

「NOSiDE® Inventory Sub System 資産管理」は、以下の OS を搭載したサーバー/クライアントを管理することができる、マルチプラットフォーム対応です。

サーバー	Windows Server 2008 / 2008R2 / 2012 / 2012R2（x86 / x64） SQL Server 2008 / 2008R2 / 2012 IIS / NPS / WSU	
クライアント	Windows（※1）	Windows 8 / 8.1（x86 / x64） Windows 7（x86 / x64） Windows Vista（x86 / x64） Windows XP SP2（x86 / x64）, SP3（x86） Windows Server 2003 / 2008 / 2008 R2 / 2012 / 2012R2（x86 / x64） Internet Explorer
	Mac OS X（※2）	Mac OS X 10.4～10.9 Safari
	Android OS 搭載スマートデバイス（※2）	Android OS 2.3、3.2、4.0～4.3 （専用アプリの搭載が必要）
	Linux	RPM 系、Ubuntu Firefox

※1 RemoteApp 連携機能を利用する場合、クライアントに.NET Framework が必要となります。
※2 リモートデスクトップ接続を行う場合、別途リモートデスクトップクライアントアプリが必要となります。