

AX シリーズ 検疫ソリューションガイド (NOSiDE[®]編)



(第2版)





はじめに

本ガイドは、NTT データ先端技術株式会社製の NOSiDE Inventory Sub System 2009 と AX シリーズ (AX1200S / AX2400S / AX3600S) でサポートしている認証機能を用いた検疫ネットワークシス テム構築のための技術情報をシステムエンジニアの方へ提供し、安全・安心な検疫システムの構築と 安定稼動を目的として書かれています。

関連資料

AX シリーズ

- AX シリーズ製品マニュアル
- AX シリーズ認証ソリューションガイド

NOSiDE

- NOSiDE Inventory Sub System (インストール編)v1.19 対応版
- NOSiDE Inventory Sub System (管理画面) v1.19 対応版
- NOSiDE Inventory Sub System (操作画面) v1.19 対応版
- NOSiDE Inventory Sub System (エージェント運用編) v1.19 対応版
- NOSiDE Inventory Sub System 検疫環境構築手順書 v1.19 対応版

本資料使用上の注意事項

本資料に記載の内容は、弊社が特定の環境において基本動作を確認したものであり、機能・性能・ 信頼性についてあらゆる環境条件すべてにおいて保証するものではありません。弊社製品を用いたシ ステム構築の一助としていただくためのものとご理解いただけますようお願いいたします。 本資料作成時の OS ソフトウェアバージョンは特記の無い限り以下となっております。

AX1230S / AX1240S Ver1.4.D / Ver2.1 AX2430S / AX3630S Ver11.1A 本資料の内容は、改良のため予告なく変更する場合があります。

輸出時の注意

本資料を輸出される場合には、外国為替および外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上、必要な手続きをお取りください。

商標一覧

- NOSiDE は、株式会社 NTT データの登録商標です。
- Ethernet は、米国 Xerox Corp.の商品名称です。
- イーサネットは、富士ゼロックス(株)の商品名称です。
- Microsoft は、米国およびその他の国における米国 Microsoft Corp.の登録商標です。
- Windows は、米国およびその他の国における米国 Microsoft Corp. の登録商標です。
- そのほかの記載の会社名、製品名は、それぞれの会社の商標もしくは登録商標です。

使用機器一覧

- AX1240S (Ver2.1)
- AX3630S (Ver11.1A)
- AX2430S (Ver11.1A)
- Windows XP Professional SP2
- Windows Vista Ultinate SP1
- Windows Server 2003 SP2

使用ソフトウェア一覧

- NOSiDE Inventory Sub System 2009 (V1.19)
- Microsoft SQL Server 2005

使用ブラウザ

- Internet Explorer (Version6)
- Internet Explorer (Version7)

改定履歴

| 版数 | rev. | 日付 | 変更内容 | 変更箇所 |
|-----|------|-----------|---|--|
| 初版 | - | 2008.1.23 | 初版発行 | - |
| 第2版 | _ | 2009.6.29 | 初版発行時からの AX シリーズのバージョンアップに伴い以下の 機能を本ガイドに取り入れる ・URL リダイレクト機能 ・Web 認証画面入れ替え機能 ・Web 認証専用 IP アドレス | 本ガイド 全般 |
| | | | AX と NOSiDE の連携に「1.2.2 特徴」を追加 「1.2.4 エージェント方式との連携」を追加 「1.2.5 IEEE802.1X 認証と連携した NOSiDE 検疫システム概要」 を追加 「2章 サポート状況と収容条件」にて連携可能な認証方式一覧表 を追加、最大認証端末の表を認証モードごとにまとめた1つの表 に変更 | 1.2.2 1.2.3 1.2.4 1.2.5 2章 |
| | | | 初版「3 章 検疫ネットワークの構築」を URL リダイレクト機能を用いた構成に変更し章のタイトルも 「3 章 システム構築例1(固定 VLAN モード)」に変更 「4 章 システム構築例2(動的 VLAN モード)」を追加 初版「4 章 注意事項と構築上のノウハウ」を | 3章 4章 |
| | | | 追加機能による見直しと変更を行い「7 章 注意事項」に変更 「付録」のコンフィグレーションファイルの更新と Web 認証画面入れ替え用ファイル(login.html)の追加 | 7 章 付録 |

目次

| 1.1 NOSiDE検疫について |
|--|
| 1.1.5 NOSiDE検疫対応クライアント. 8 1.1.6 NOSiDE検疫サーバに必要な役割とコンポーネント 9 1.2 AXとNOSiDEの連携. 10 1.2.1 検疫概要. 10 1.2.2 特徴 11 1.2.3 Web認証と連携した検疫シーケンス(エージェントレス方式) 12 1.2.4 Web認証と連携した検疫シーケンス(エージェント方式) 13 1.2.5 IEEEE802 1X認証と連携した検疫シーケンス(エージェント方式) 14 |
| 1.2.3 IEEE802.1 X認証と連張したNOSIDE検疫ノスクム報要 |
| 2.1 サポート状況 15 2.1.1 連携可能な認証方式一覧 15 2.2 収容条件 15 2.2.1 最大認証端末数 15 |
| 3. システム構築例1(固定VLANモード)16 |
| 3.1 検疫システムの構成 16 3.1.1 固定VLANモード導入シナリオ 16 3.1.2 検疫システム基本構成 17 3.1.3 ネットワーク構成図(詳細) 18 3.1.4 各VLANの定義 19 3.1.5 クライアント端末の検疫結果に応じた各サーバへの通信可否 19 2.4.6 割まえくいてのポート様式 10 |
| 3.1.6 認証スイッチのホート構成19 3.2 AXシリーズの設定 |
| 3.2.1 構築ポイント 20 3.2.2 AX2430Sのコンフィグレーション 21 3.2.3 AX1240Sのコンフィグレーション 23 3.2.4 Web認証画面入れ替え 25 3.3 検疫サーバの設定 26 2.24 専業準備 22 |

| 3.3.2 IASの設定 | 27 |
|---|----|
| 3.3.3 DNSサーバの設定 | 28 |
| 3.3.4 DHCPサーバの設定 | |
| 3.3.5 ネットワーク接続認証設定 | 29 |
| 3.3.6 検疫除外端末の設定 | 32 |
| 4. システム構築例2(ダイナミックVLANモード) | |
| 4.1 検疫システムの構成 | |
| 4.1.1 ダイナミックVLANモード導入シナリオ | |
| 4.1.2 検疫システム基本構成 | |
| 4.1.3 ネットワーク構成図(詳細) | |
| 4.1.4 各VLANの定義 | |
| 4.1.5 クライアント端末の検疫結果に応じた通信可否 | |
| 4.1.6 認証スイッチのポート構成 | |
| 4.2 AXシリーズの設定 | 40 |
| 4.2.1 構築ポイント | 40 |
| 4.2.2 AX2430Sのコンフィグレーション | 41 |
| 4.2.3 AX1240Sのコンフィグレーション | 43 |
| 4.2.4 Web認証画面入れ替え | 45 |
| 4.3 検疫サーバの設定 | 45 |
| 4.3.1 事前準備 | 45 |
| 4.3.2 IASの設定 | 45 |
| 4.3.3 DNSサーバの設定 | 45 |
| 4.3.4 DHCPサーバの設定 | 45 |
| 4.3.5 ネットワーク接続認証設定 | 46 |
| 4.3.6 検疫除外端末の設定 | 52 |
| 5. クライアント端末の設定 | |
| 5.1 エージェントレス方式の設定 | |
| 5.2 エージェント方式の設定 | |
| 6. 動作確認方法 | 57 |
| | |
| 6.1 AXシリーズにおける確認方法 | 57 |
| 6.1.1 show web-authentication login | 57 |
| 6.1.2 show web-authentication logging | 57 |
| 6.1.3 clear web-authentication auth-state | 57 |
| 6.2 NOSiDE検疫サーバでの確認 | |
| 6.2.1 ネットワーク接続認証ログ | |
| 7. 注意事項 | |

| 7.1 Web | 認証連携時の注意事項 | 59 |
|---------|----------------------|----|
| 7.1.1 | 翌証スイッチ種別について | 59 |
| 7.1.2 N | as-Ip-Addressの設定に関して | 59 |
| 付録 | Ε | 30 |

1. NOSiDE 検疫概要

1.1 NOSiDE 検疫について

1.1.1 NOSiDE 検疫システムの概要

NOSiDE の検疫システムは、業務サーバへ接続する前に、ユーザ認証及びセキュリティ対策チェック、端末認証を行い、検疫通過した端末のみ業務サーバへ接続を許可します。セキュリティ基準を満たしていない場合は、ユーザのセキュリティ対策作業を支援します。



図 1.1-1 NOSiDE 検疫概要

1.1.2 NOSiDE でチェック可能な検疫項目

NOSiDE でチェックすることが出来る主な検疫項目を以下に示します。

| 項番 | チェックポイント | 詳細 |
|----|-------------------|-----------------------------|
| 1 | OS パッチ適用チェック | 期間を指定して警告、および切断 |
| 2 | ウイルス対策 | ソフトの導入状況、リアルタイム保護の有無、ウイル |
| | | ス定義ファイルの更新 |
| 3 | 禁止ソフトウェアチェック | Winny 等の禁止ソフトのチェック任意のソフトを検疫 |
| | | 対象に登録可能 |
| 4 | 必須ソフトの導入チェック | 任意のソフト導入チェックを登録可能 |
| 5 | レジストリ診断 | 例)スクリーンセーバーのパスワードロックチェック |
| | | など |
| 6 | ファイル/フォルダ暗号化診断 | 例)マイドキュメントが暗号化(EFS)されていなけ |
| | | れば接続されない。 |
| 7 | 登録済み MAC アドレスチェック | 登録されていない MAC アドレスの場合接続拒否 |

表 1.1-1 NOSiDE の主な検疫項目一覧

注)上記検疫項目に関しては、Windows 系 OS の検疫項目です。詳細は NOSiDE マニュアルを参照 下さい。

1.1.3 NOSiDE の検疫システムの種類について

NOSiDE 検疫システムは、以下の2つのネットワーク検疫をサポートしています。

(1) 検疫 LAN

社内 LAN 内で使用されるコンピュータや、持ち込み端末に対する検疫 LAN 機能、セキュリティ管理機能ならびに IT 資産管理機能が実現出来ます。

(2) 検疫 VPN

社外からのリモート VPN 接続するコンピュータに対する検疫 VPN を構築する事が出来ます。

本ガイドでは、NOSiDE と AX シリーズの認証機能を用いた検疫 LAN システムの構築と運用上の 注意事項を解説します。

1.1.4 NOSiDE 検疫ネットワークへの端末接続方法

NOSiDE 検疫ネットワークへの端末接続方法を以下に示します。

(1) エージェント方式

あらかじめクライアント端末側に検疫 LAN システムの専用エージェントを導入し、自動的に検 疫及びネットワーク接続する方式。

(2) エージェントレス方式

AX シリーズを用いた検疫ネットワーク構築に関しては、どちらの方式でも違いはありません。

1.1.5 NOSiDE 検疫対応クライアント

NOSiDE 検疫に対応しているクライアントを以下に示します。

| 項番 | プラットフォーム |
|----|--|
| 1 | ・Windows Vista, ・Windows XP, ・Winows 2000 SP4 以降 |
| | Windows Server 2003(SP1, R2) |
| | ・Windows Server 2008、x64 対応 |
| 2 | Linux(カーネル 2.4.x~2.6.x,x86 互換 CPU 対応,RPM 対応) |
| 3 | Mac OS X Ver10. 3. 9/10. 4. 4~11/10. 5. 2~ |

表 1.1-2 NOSiDE 検疫対応クライアント

エージェント方式のサポートや、検疫チェック可能な項目は各 OS ごとにサポート範囲が異なりま すので、NOSiDE の製品情報を参照ください。

各ユーザが手動で NOSiDE 検疫サーバヘ Web ブラウザを用いてログインし、検疫及びネット ワーク接続する方式。

1.1.6 NOSiDE 検疫サーバに必要な役割とコンポーネント

NOSiDE 検疫ネットワークを構築するためには、以下の役割が必要になります。

- ●検疫サーバ・・・・・クライアント端末の検疫、資産情報の登録。
- •RADIUS ・・・・・認証リクエストの処理。
- ●ディレクトリサーバ・・認証時に参照するユーザデータベース。

各役割を実現するためにインストールする必要があるコンポーネントを以下の表に示します。

| 項番 | 役割 | プラットフォーム | コンポーネント種別 | コンポーネント |
|----|---------------|--|---|--|
| 1 | | | NOSiDE | NOSiDE Inventory Sub System (管理画面) |
| 2 | 検疫サーバ | Windows Server 2003 Windows Server 2008 | コンポーネント | NOSiDE Inventory Sub System (操作画面) |
| 3 | | | Windows Server 2003 Windows Server 2008 コンポーネント | IIS |
| 4 | データベー | Windows Server 2003 Windows Server 2008 | NOSiDE コンポーネント | NOSiDE Inventory Sub System (データベース) |
| 5 | スサーバ | | Microsoft SQL Server | Microsoft SQL Server 2005 及び Microsoft SQL Server 2008 |
| 6 | RADIUS サ | Windows Server 2003 | NOSiDE コンポーネント | NOSiDE Inventory Sub System RADIUS(拡張モジュール) |
| 7 | - <i>i</i> ĭ | Windows Server 2008 | Windows Server 2003 Windows Server 2008 コンポーネント | IAS(Windows Server 2003) NPS(Windows Server 2008) |
| 8 | ディレクト リサーバ | Windows Server 2003 Windows Server 2008 | Windows Server 2003 Windows Server 2008 コンポーネント | ActiveDirectory |

表 1.1-3 NOSiDE 検疫サーバに必要な役割とコンポーネント

※本ガイドでは**表 1.1-3** に示すコンポーネントを1台の Windows Server 2003 にインストールし、 Microsoft SQL Server には Microsoft SQL Server 2005 を使用した構築例を紹介しています。

また、ネットワーク環境により上記以外の役割(DHCPサーバ、DNSサーバ)を設置する必要があります。詳細は3章システム構築例1(固定VLANモード)を参照して下さい。

※表 1.1-3 以外にも NOSiDE コンポーネントは存在しますが、本ガイドでは記載していません。 詳細につきましては NOSiDE のマニュアルを参照して下さい。

1.2 AXとNOSiDEの連携

1.2.1 検疫概要

NOSiDE を用いた検疫ネットワークでは、決められたセキュリティポリシーに応じてクライアント 端末に対し、ネットワーク制御を実施します。例えばセキュリティポリシーに違反した端末は業務サ ーバに接続させない、ポリシー違反を修復した端末については業務サーバへのアクセス権を与える等 のネットワーク制御を行います。

NOSiDE 検疫ネットワークでは、AX シリーズのサポートするネットワーク認証機能と NOSiDE 検疫サーバの連携により、このようなネットワーク制御を実現しています。

クライアント用 VLAN に接続された端末は、当初接続先を検疫用 VLAN に限定されます。接続制限を解除し、業務サーバに接続する為に NOSiDE 検疫サーバに接続し検疫のチェックを行います。

接続許可を受けたセキュリティ対策済みの端末のみ、自動的にAXシリーズのネットワーク認証を 行い社内業務サーバへアクセス可能となります。



図 1.2-1 NOSiDE と AX を用いた検疫ネットワーク概要

1.2.2 特徴

AX シリーズのサポートする認証方式には Web 認証、IEEE802.1X 認証、MAC 認証があり、その 中で Web 認証と IEEE802.1X 認証で NOSiDE 検疫システムと連携することが可能です。本ガイドで は推奨する認証方式として Web 認証方式を中心に記述しています。

以下に NOSiDE 検疫システムと AX シリーズの認証スイッチが連携した場合の特徴を示します。

(1) 導入環境に応じた認証モードの選択

AX シリーズがサポートする認証方式では端末が認証後に所属する VLAN に応じて以下 2 種類の認 証モードが存在します。それぞれの認証モードにて NOSiDE 検疫システムと連携が可能なため、導 入環境に応じた柔軟な検疫システムの構築が可能です。

本ガイドでは Web 認証方式にてそれぞれの認証モードを使用した構築例を示しています。

- 固定 VLAN モード
 ポート単位に VLAN が固定に設定されたモードです。
 本モードの構築例は3システム構築例1(固定VLANモード)を参照してください。
- ダイナミック VLAN モード
 ユーザー単位に所属する VLAN が動的に変化するモードです。
 本モードの構築例は4システム構築例2(ダイナミックVLANモード)を参照してください。

(2) ブラウザ起動後すぐに NOSiDE 検疫サーバの検疫画面を表示

Web 認証と連携した場合、検疫前のクライアント端末はブラウザを起動すると自動的に NOSiDE サーバの検疫画面にリダイレクトされるため、管理者は検疫サーバのアドレスをユーザーに周知させ る必要がなく、またユーザー側でも検疫サーバのアドレスを指定する必要がないためシステム全体の 利便性が向上します。

なお1.2.3Web認証と連携した検疫にて本特徴をシーケンス図にて解説しています。

(3) MAC 認証を使用して検疫除外端末を認証する。

NOSiDE 検疫システムでは、クライアント端末の検疫チェックが実施されない限り通信を制限して います。検疫を行わない端末(以下検疫除外端末とする)を接続する方法としては NOSiDE の検疫 サーバで認証許可ユーザーの設定と AX シリーズがサポートする MAC 認証の連携により本システム 内で検疫除外端末を認証することが可能です。

これにより検疫チェックやブラウザによる Web 認証をサポートしていないプリンタ等の端末に関 してもネットワーク認証を行うことが可能です。

なお本システムでの検疫除外端末の設定方法は<mark>3.3.6検疫除外端末の設定</mark>を参照してください。

また別の方法として AX シリーズがサポートする「認証方式毎の RADIUS サーバ指定機能」を使用して MAC 認証専用の RADIUS サーバを別で用意することにより、NOSiDE 検疫サーバの設定は一切行わず検疫除外端末の MAC 認証による接続が可能となります。

1.2.3 Web 認証と連携した検疫シーケンス(エージェントレス方式)

Web 認証を用いた NOSiDE 検疫システムの検疫シーケンスを以下に示します。AX シリーズの Web 認証と NOSiDE 検疫システムを連携した場合、AX シリーズの URL リダイレクト機能と Web 認証画 面入れ替え機能を使用して認証前のクライアント端末からの Web アクセスを NOSiDE の検疫画面に リダイレクトすることが出来ます。

クライアント端末は接続方法にエージェントレス方式を使用しています、クライアント端末ではブ ラウザを起動すると自動的に NOSiDE 検疫サーバにリダイレクトされ認証と検疫を実行します。



※1...検疫ソフトのダウンロードは初回のみで次回より省略可能

※2...ダイナミック VLAN モード使用時はクライアント端末の IP アドレス再取得が実施されます。

図 1.2-2 検疫シーケンス

1.2.4 Web 認証と連携した検疫シーケンス(エージェント方式)

クライアント端末に NOSiDE 検疫エージェントをインストールした場合、端末の認証と検疫はエ ージェントにより自動的に実行されます。ユーザーはエージェントの初期設定と検疫失敗時の修復操 作以外には通常運用時の操作が全く無いため、検疫システムを意識することがありません。



図 1.2-3 エージェント使用時の検疫シーケンス

本ガイドにて<u>5.2</u>にてクライアント端末のエージェント初期設定例を示しています。

1.2.5 IEEE802.1X 認証と連携した NOSiDE 検疫システム概要

本ガイドでは構築例を示していませんが、認証方式として IEEE802.1X(ダイナミック VLAN)との連携も可能です。AX シリーズの IEEE802.1X 認証(ダイナミック VLAN モード)と NOSiDE 検疫システムの連係動作の概要を以下に示します。

本検疫システムでは、クライアント端末は認証と検疫の状態に応じて動的に所属 VLAN が変化し ます。その様子を以下順番に解説します。

①認証前

クライアント端末は認証スイッチに接続した時点で認証前 VLAN に所属しています。認証前 VLAN に所属しているクライアント端末は IEEE802.1X 認証に成功すると検疫 VLAN に移動しま す。(通常 IEEE8021.X 認証をシングルサインオンで構成した場合はクライアント端末起動時に 自動的に完了するため、ユーザーは認証前 VLAN に所属している事を意識しません。)

②検疫前

検疫 VLAN に所属したクライアント端末は NOSiDE 検疫サーバに接続し検疫チェックを行いま す。セキュリティポリシーに準拠しない端末は修復サーバに接続してセキュリティ状態の修復を 行います。なお認証前 VLAN と検疫 VLAN に所属するクライアント端末からの業務サーバ宛通 信は認証スイッチのアクセスリストにより制限されています。

検疫チェックに成功したクライアント端末は NOSiDE 検疫サーバの指示により再度 IEEE802.1X 認証を実行します。この時 NOSiDE 検疫サーバと RADIUS サーバの連携により検 疫チェックに成功したクライアント端末のみ通常 VLAN への所属を許可します。

③認証と検疫に成功

通常 VLAN に所属したクライアント端末は業務サーバとの通信が可能となります。また定期的 に検疫チェックを行うことでセキュリティポリシーに違反したクライアント端末は自動的に検 疫 VLAN に隔離されます。



図 1.2-4 IEEE802.1X 認証方式の連携動作概要

 なお IEEE802.1X 認証方式にて構築する場合、AX シリーズの設定に関しては、「AX シリーズ認 証ソリューションガイド」の「3.3 動的 VLAN モード」を参照して下さい。また NOSiDE 検疫サ ーバの設定に関しては、「NOSiDE Inventory Sub System 検疫環境構築手順書 v1.19 対応版」を 参照してください。

2.1 サポート状況

2.1.1 連携可能な認証方式一覧

NOSiDEの検疫システムと連携可能なAXシリーズの認証方式と認証モードの一覧を以下の表に示します。

| 認証方式 | 認証モード | AX1230S | AX1240S | AX2400S AX3600S |
|------------|---------|---------|---------|--------------------|
| IEEE802.1X | 固定 VLAN | - | - | - |
| 認証 | 動的 VLAN | 0 | 0 | 0 |
| Web 認証 | 固定 VLAN | 0 | 0 | 0 |
| | 動的 VLAN | 0 | 0 | 0 |
| MAC 認証 | 固定 VLAN | _ | - | - |
| | 動的 VLAN | _ | | _ |

表 2.1-1 連携可能な認証方式一覧

(凡例) 一:連携不可、〇:連携可能

2.2 収容条件

AX シリーズにて NOSiDE 検疫サーバと連携する際に関連する収容条件を以下に示します。

2.2.1 最大認証端末数

AX シリーズのサポートする各認証モードごとの最大認証端末数を以下に示します。

| 認証モード | 認証方式 | AX1200S | | AX2400S AX3600S | |
|----------------|-------------------|---------|---------|--------------------|-----------------|
| 固定 VLAN | IEEE802.1X 認 | 64/ポート | | 64/ポート | |
| モード | 証 | 256/装置 | 合計 | 256/VLAN | 合計 |
| | MAC 認証 | 1024/装置 | 1024/装置 | 1024/装置 | 1024/装置 |
| | Web 認証 | 1024/装置 | | 1024/装置 | |
| 動的 VLAN モード | IEEE802.1X 認 証 | 256/装置 | 合計 | 256/装置(*1) | 合計 |
| | MAC 認証 | 256/装置 | 256/装置 | 256/装置(*1) | _200/装直 (*1) |
| | Web 認証 | 256/装置 | | 256/装置(*1) | () |

表 2.2-1 認証モードごとの最大認証端末数

(凡例) -: 未サポート

(*1) AX3640S では 1024/装置となります

3. システム構築例1(固定 VLAN モード)

3.1 検疫システムの構成

本章では、AX シリーズの Web 認証(固定 VLAN)方式を用いた NOSiDE 検疫システムの構築例を示します。

3.1.1 固定 VLAN モード導入シナリオ

本システムは、キャンパスネットワークへの導入を想定しています。

図 3.1-1 に示すキャンパスネットワークでは、教室毎に固定の VLAN を割り当て、教室単位にサー バアクセス制御を行います。

このようなネットワークに NOSiDE 検疫システムを導入する場合、AX の固定 VLAN モードを導入 するのが最適です。各フロアに設置された AX の認証スイッチは、学部の教室ごとに対応するポート に対し、固定で VLAN を割り当てることができます。このため、クライアント端末を接続するポー トごとに決められた VLAN に所属させることができます。

図3.1-1に示す構成では2つの学部の学生がそれぞれの教室からクライアント端末をネットワークに接続し、NOSiDE検疫サーバによる検疫とAXの認証スイッチによるネットワーク認証を行った後、 各学部の専用サーバにアクセスすることができるようになります。



図 3.1-1 固定 VLAN モードシナリオ

3.1.2 検疫システム基本構成

以下に本章にて構築する検疫システムの基本的なネットワーク構成図と構成機器一覧表を示しま す。



コアスイッチには AX3630S を配置し、VRRP を用いて装置を冗長化します。また、装置間はリン クアグリゲーションを用いて回線を冗長化します。検疫サーバおよび検疫により隔離された端末を治 療する修復サーバは、コアスイッチ配下に接続します。コアスイッチ同士の経路交換には、OSPF 等 のルーティングプロトコルを使用します。

エッジスイッチには認証スイッチとして動作する AX2430S と AX1240S を配置し、スパニングツ リーを用いて冗長化します。

検疫を行う端末は、エッジスイッチに直接またはハブを介して接続します。IP アドレスに関しては コアスイッチ配下にある DHCP サーバより配布されます。なお本ガイドの構成では修復サーバに疎 通確認用の PC を使用していますが、実環境では WSUS やセキュリティパッチ配布サーバなどを設 置することを想定しています。

本ガイドで使用するサーバとクライアント端末を以下に示します。

| | 36 |
|---------------------------------|---------------|
| 検疫サーバ | クライアント端末 |
| Windows Server 2003 | Windows XP |
| •ActiveDirectory ドメインサービス | Windows Vista |
| •DNS サーバ | |
| •DHCP サーバ | |
| •Web サーバ(IIS) | |
| •RADIUS サーバ(IAS) | |
| データベースサーバ(Microsoft SQL Server) | |
| NOSiDE 検疫サーバ | |

表 3.1-1 サーバとクライアント一覧

3.1.3 ネットワーク構成図(詳細)

AX シリーズの Web 認証(固定 VLAN モード)と NOSiDE を連携した検疫ネットワークの詳細 な構成図を以下に示します。



図 3.1-3 ネットワーク構成図(詳細)

3.1.4 各 VLAN の定義

本構築例にて使用する VLAN の定義情報を以下の表に示します。

| VLAN 名 | VLANID | ネットワーク IP アドレス | 用途 | 設置サーバ |
|--------------------|--------|-------------------|---|----------|
| | 5 | 10.5.0.0/24 | | |
| OSPF 用 VI AN | 15 | 10.15.0.0/24 | OSPF ネットワーク。 | — |
| | 25 | 10.25.0.0/24 | | |
| 検疫サーバ用 | 50 | 10.50.0.0/24 | 検疫前、及び検疫失敗した端末が通信可能 | 検疫サーバ |
| VLAN | 51 | 10.51.0.0/24 | なサーバが所属する VLAN。 | 修復サーバ |
| 学部 1 用 サーバ VLAN | 52 | 10.52.0.0/24 | 学部1に所属する端末が検疫に成功した 際に通信可能なサーバが所属する VLAN。 | 学部 1 サーバ |
| 学部 2 用 サーバ VLAN | 53 | 10.53.0.0/24 | 学部2に所属する端末が検疫に成功した 際に通信可能なサーバが所属する VLAN。 | 学部2サーバ |
| 学部 1 VLAN | 30 | 192.168.30.0/24 | 学部1の端末が所属する VLAN。 | — |
| 学部 2 VLAN | 100 | 192.168.100.0/24 | 学部2の端末が所属する VLAN。 | _ |
| 管理用 VLAN | 1000 | 172.16.0.0/24 | 各装置を管理するための VLAN。 | _ |

表 3.1-2 各 VLAN の定義

3.1.5 クライアント端末の検疫結果に応じた各サーバへの通信可否

クライアント端末の通信制御には AX シリーズの認証前アクセスリストを使用します、クライアン ト端末の検疫結果に応じた各サーバへの通信可否を以下の表に示します。

| 端末→各サーバ | 学部1サーバ | 学部2サーバ | 検疫サーバ | 修復サーバ | DHCP、DNS サーバ |
|------------------------|------------|--------|-------|------------|-----------------|
| 検疫実施前及び、 検疫失敗端末(※1) | × | × | 0 | 0 | Δ |
| 学部1の検疫成功端末 | 0 | × | 0 | 0 | 0 |
| 学部2の検疫成功端末 | × | 0 | 0 | 0 | 0 |
| (∇例) 〇·通信 | T能 x · 诵信7 | | | CP DNS) のみ | 通信可能 |

表 3.1-3 クライアント端末の認証状態に応じた通信可否

(凡例) 〇:通信可能、×:通信不可、△:一部プロトコル(DHCP、DNS)のみ通信可能
 (※1):学部 1,2 共通

3.1.6 認証スイッチのポート構成

ここで、認証スイッチのポートを以下のように設定します。本構築例ではプリンタなど検疫ができない機器を検疫除外端末として設定しています。検疫除外端末の設定に関しては3.3.6検疫除外端末の設定を参照して下さい。

| 認証スイッチ | 用途 | ポート種別 | VLAN | ポート番号 | 認証方式 |
|---------|----------|---------|-------------|-------|----------|
| | 物計用 | マクセフポート | 30 | 1~10 | \//ob 認証 |
| AX2430S | 心証用 | | 100 | 11~20 | |
| | アップリンク接続 | トランクポート | 30,100,1000 | 47,48 | _ |
| | 物計用 | マクセフポート | 30 | 1~10 | |
| AX1240S | 心証用 | | 100 | 11~20 | Web認証 |
| | アップリンク接続 | トランクポート | 30,100,1000 | 25,26 | _ |

表 3.1-4 認証スイッチのポート構成

3.2 AX シリーズの設定

3.2.1 構築ポイント

本検疫システムにて認証スイッチの設定に関する構築ポイントを以下に示します。

(1) Web 認証用画面を入れ替える。

AX シリーズの Web 認証画面入れ替え機能を用いて「login.html」ファイルを入れ替え、直接クライアント端末からスイッチへの Web 認証操作をできないようにします。

認証スイッチへのWeb認証はNOSiDEの検疫チェック後に自動的に実行されるためユーザは意識 する必要がありません。Web認証画面入れ替え手順に関しては3.2.4Web認証画面入れ替えを参照 して下さい。

(2) URL リダイレクト機能のリダイレクトモードを変更する。

(1) で示す画面入れ替えと URL リダイレクト機能を併用する事で検疫前のクライアントが任意の http アクセスを実行した場合自動的に NOSiDE の検疫画面へジャンプするようにします。デフォルトの https モードでは証明書エラーが出ますので、リダイレクトモードを http に変更します。

(3) 認証前アクセスリストの作成

クライアント端末の検疫前及び検疫失敗時に以下の通信を許可するため、認証スイッチに認証前 アクセスリストを定義します。

- 本ガイドではクライアント端末の IP アドレスを DHCP サーバより配布しています。その ためクライアント端末からの DHCP パケットを許可します。
- ② 検疫前のクライアント端末から名前解決を可能にします。クライアント端末から DNS サ ーバ宛、DNS クエリパケットを許可します。
- クライアント端末から NOSiDE の検疫サーバへの IP 通信を許可します。
- ④ クライアント端末から修復サーバへの IP 通信を許可します。

(4) Web 認証専用 IP アドレスを設定する

Web 認証用の IP アドレスを設定します。この IP アドレスは全認証スイッチに共通して設定することが出来ます。この例では、「10.10.10.10」としています。

また、認証用 VLAN のインタフェースにも IP アドレス設定が必要です。

(5) Web 認証の最大接続時間を調整する

セキュリティ上、Web 認証は一度認証成功するとデフォルトで1時間後に自動的にログアウト します。運用方針に従って、適宜最大接続時間を調整して下さい。この例では、一日一回は必ずロ グアウトさせることを目的として1400分に設定しています。

(6) RADIUS サーバの設定をする

本ガイドでは RADIUS サーバと NOSiDE 検疫サーバは 1 台のマシンで構成していますが、別々 にサーバを設置する場合は、NOSiDE の RADIUS プロキシサーバを RADIUS サーバとして設定し て下さい。

(7) 検疫除外端末の設定

プリンタなどの検疫が出来ない端末を接続する場合、接続するポートにMAC認証を設定します。 この場合、NOSiDE側に該当端末のMACアドレスを登録しておく必要があります。(3.3.6検疫除外 端末の設定を参照)

3.2.2 AX2430S のコンフィグレーション

本構成における、認証スイッチのコンフィグレーションの解説を下記に示します。なおコアスイッチに関しては付録を参照して下さい。

AX2430S のコンフィグレーション

| edge#1 (AX2430S)の設定 | |
|--|---|
| 事前設定 | |
| (config)# hostname "edge#1" (config)# clock timezone "JST" +9 0 | ホスト名の設定をします。 タイムゾーンの設定をします。 |
| VLAN の定義 | |
| (config)# vlan 1 | VLAN1は使用しないため、無効にします。 |
| (config-vlan)# state suspend (config)# vlan 30, 100, 1000 (config-vlan)# state active | 認証用VLANとしてVLAN30, 100を、管理用VLANとして VLAN1000を作成します。 |
| スパニングツリーの設定 | |
| <pre>(config)# spanning-tree mode mst (config)# spanning-tree mst configuration (config-mst)# name NOSiDE (config-mst)# revision 1 (config-mst)# instance 1 vlans 1000 (config-mst)# instance 2 vlans 30,100</pre> | マルチプルスパニングツリーを有効にし、リージョン、イ ンスタンスを設定します。 リージョン名:NOSiDE リビジョン番号:1 MSTインスタンス1:VLAN1000 MSTインスタンス2:VLAN30,100 |
| (config)# interface range gigabitethernet 0/1-20 (config-if-range)# spanning-tree portfast | 認証用ポート0/1~0/20に対して、スパニングツリーの PortFast機能を適用し、スパニングツリー対象外とします。 |
| インターフェイスの設定 | |
| 物理ポートの設定 | |
| (config)# interface range gigabitethernet 0/1-4 (config-if-range)#media-type rj45 | ポート0/1-4のメディアタイプをUTPに変更します。 ※本設定は該当ポートがSFP/UTP選択型ポートのときに必 要です。 |
| Web認証用 (config)# interface range gigabitethernet 0/1-10 (config-if-range)# switchport access vlan 30 (config-if-range)# web-authentication port (config-if-range)# authentication ip access-group "Auth" (config-if-range)# authentication arp-relay | 認証ポートの設定 ポート0/1~0/10をアクセスポートのVLAN30に設定します。 Web認証対象ポートの設定をします。 認証前アクセスリスト "WebAuth"を設定します。 認証前の端末から送信される他宛てARPパケットを認証対 象外のポートへ出力させます。 |
| <pre>(config)# interface range gigabitethernet 0/11-20 (config-if-range)# switchport access vlan 100 (config-if-range)# web-authentication port (config-if-range)# authentication ip access-group "Auth" (config-if-range)# authentication arp-relay</pre> | ポート0/11~0/20をアクセスポートのVLAN100に設定しま す。 Web認証対象ポートの設定をします。 認証前アクセスリスト"WebAuth"を設定します。 認証前の端末から送信される他宛てARPパケットを認証対 象外のポートへ出力させます。 |
| MAC認証用 (config)# interface gigabitethernet 0/1 (config-if-range)# mac-authentication port | <mark>検疫除外端末の設定</mark> ポート0/1に検疫除外端末用にMAC認証設定をします。 |
| アップリンク用 (config)# interface range gigabitethernet 0/47-48 (config-if-range)# switchport mode trunk (config-if-range)# switchport trunk allowed vlan 30, 100, 1000 | アップリンクポートの設定 ポート0/47~0/48をトランクポートに設定し、VLAN30、100、 1000を設定します。 |

| VLAN インターフェイスの設定 | |
|---|---|
| <pre>(config)# interface vlan 30 (config-if)# ip address 192.168.30.11 255.255.255.0 (config-if)# ip access-group Faculty1 in</pre> | 認証用VLAN30にインタフェースIPアドレスを設定します。 アクセスリスト「Faculty1」を適応します。 |
| (config)# interface vlan 100 (config-if)# ip address 192.168.100.11 255.255.255.0 (config-if)# ip access-group Faculty2 in | 認証用VLAN100にインタフェースIPアドレスを設定します。 アクセスリスト「Faculty2」を適応します。 |
| (config)# interface vlan 1000 (config-if)# ip address 172.16.0.11 255.255.255.0 | 管理用VLAN1000にインタフェースIPアドレスを設定しま す。 |
| デフォルトルートの設定 | |
| (config)# ip default-gateway 172.16.0.254 | RADIUSサーバと通信を行うため、デフォルトルートを設定 します。 |
| アクセスリストの作成 | |
| <pre>(config)# ip access-list extended "Auth" (config-ext-nacl)# 10 permit udp any any eq bootps (config-ext-nacl)# 20 permit udp any any eq domain (config-ext-nacl)# 30 permit ip 192.168.30.0 0.0.0.255 host 10.50.0.1 (config-ext-nacl)# 40 permit ip 192.168.100.0 0.0.0.255 host 10.50.0.1 (config-ext-nacl)# 50 permit ip 192.168.30.0 0.0.0.255 host 10.51.0.1 (config-ext-nacl)# 60 permit ip 192.168.100.0 0.0.0.255 host</pre> | 認証前アクセスリストとして定義する "Auth"を作成します。 DHCPパケットの許可を設定します DNSパケットの許可を設定します 検疫サーバ宛IP通信を許可します 修復サーバ宛IP通信を許可します ●設定ポイント(3) 「認証前アクセスリストの設定」 |
| 10.51.0.1 (config)# ip access-list extended "Faculty1" (config-ext-nacl)# 10 deny ip 192.168.30.0 0.0.0.255 10.53.0.0 0.0.0.255 (config-ext-nacl)# 20 permit ip any any | 学部1用に他の学部のサーバに通信できないようにするア クセスリスト「Faculty1」を作成する。 |
| (config)# ip access-list extended "Faculty2" (config-ext-nacl)# 10 deny ip 192.168.100.0 0.0.0.255 10.52.0.0 0.0.0.255 (config-ext-nacl)# 20 permit ip any any | 学部2用に他の学部のサーバに通信できないようにするア クセスリスト「Faculty2」を作成する。 |
| Web 認証の設定 | |
| (config)# web-authentication system-auth-control (config)# web-authentication ip address 10.10.10.10 | Web認証を有効にします。 Web認証専用IPアドレスを設定します。本ガイドでは 「10. 10. 10」としています。●設定ポイント(4) 「Web認証専用IPアドレスを設定する」 |
| (config)# web-authentication redirect-mode http | URLリダイレクトのリダイレクトモードをHTTPに設定しま す。 <mark>●設定ポイント(2)</mark> 「URLリダイレクト機能のリダイレクトモードを変更する」 |
| (config)# web-authentication max-timer 1400 | ●設定ポイント(5) 「Web認証の最大接続時間を調整する」 |
| (config)# aaa authentication web-authentication default group radius | Web認証機能でのRADIUSサーバの使用有無を設定します。 |
| MAC 認証の設定 | |
| <pre>(config)# mac-authentication system-auth-control (config)# mac-authentication password macpass</pre> | MAC認証を有効にします。 MAC認証で, RADIUSサーバに認証要求を出すときの端末ユー ザで使用するパスワードを設定します。 |
| (config)# aaa authentication web-authentication default group radius | MAC認証機能でのRADIUSサーバの使用有無を設定します。 ● <mark>設定ポイント(7)「検疫除外端末の設定」</mark> |
| RADIUS サーバの設定 | |
| (config)# radius-server host 10.50.0.1 key "alaxala" | RADIUSサーバのIPアドレス、シークレットキーを設定します。●設定ポイント(6)「RADIUSサーバの設定をする」 |

3.2.3 AX1240S のコンフィグレーション

| edge#2 (AX1240S)の設定 | |
|---|--|
| 事前設定 | |
| (config)# system function filter extended-authentication | フィルタ機能と拡張認証機能を使用するため、システムフ ァンクションリソース配分を変更します。 ※設定後は、装置の再起動が必要です。 |
| (config)# hostname "edge#2" (config)# clock timezone "JST" +9 0 | ホスト名の設定をします。 タイムゾーンの設定をします。 |
| VLAN の定義 | |
| (config)# vlan 1 | VLAN1は使用しないため、無効にします。 |
| (config-vlan)# state suspend (config)# vlan 30,100,1000 (config-vlan)# state active | 認証VLANとしてVLAN30,100を、管理用VLANとしてVLAN1000 を作成します。 |
| スパニングツリーの設定 | |
| <pre>(config)# spanning-tree mode mst (config)# spanning-tree mst configuration (config-mst)# name NOSiDE (config-mst)# revision 1 (config-mst)# instance 1 vlans 1000 (config-mst)# instance 2 vlans 30,100</pre> | マルチプルスパニングツリーを有効にし、リージョン、イ ンスタンスを設定します。 リージョン名:NOSiDE リビジョン番号:1 MSTインスタンス1:VLAN1000 MSTインスタンス2:VLAN30,100 |
| (config)# interface range fastethernet 0/1-20 (config-if-range)# spanning-tree portfast | 認証用ポート0/1~0/20に対して、スパニングツリーの PortFast機能を適用し、スパニングツリー対象外とします。 |
| インターフェイスの設定 | |
| 物理ポートの設定 | |
| 認証用 (config)# interface range fastethernet 0/1-10 (config-if-range)# switchport access vlan 30 (config-if-range)# web-authentication port (config-if-range)# authentication ip access-group "Auth" (config-if-range)# authentication arp-relay | 認証ポートの設定 ポート0/1~0/10をアクセスポートのVLAN30に設定します。 Web認証対象ポートの設定をします。 認証前アクセスリスト "Auth"を設定します。 認証前の端末から送信される他宛てARPパケットを認証対 象外のポートへ出力させます。 |
| <pre>(config)# interface range fastethernet 0/11-20 (config-if-range)# switchport access vlan 100 (config-if-range)# web-authentication port (config-if-range)# authentication ip access-group "Auth" (config-if-range)# authentication arp-relay</pre> | ポート0/11~0/20をアクセスポートのVLAN100に設定しま す。 Web認証対象ポートの設定をします。 認証前アクセスリスト "Auth"を設定します。 認証前の端末から送信される他宛てARPパケットを認証対 象外のポートへ出力させます。 |
| MAC認証用 (config)# interface fastethernet 0/1 (config-if-range)# mac-authentication port | <mark>検疫除外端末の設定</mark> ポート0/1に検疫除外端末用にMAC認証設定をします。 |
| アップリンク用 (config)# interface range gigabitethernet 0/25-26 (config-if-range)# switchport mode trunk (config-if-range)# switchport trunk allowed vlan 30,100,1000 | <mark>アップリンクポートの設定</mark> ポート0/25~0/26をトランクポートに設定し、VLAN30、100、 1000を設定します。) |
| VLAN インターフェイスの設定 | |
| (config)# interface vlan 30 (config-if)# ip address 192.168.30.12 255.255.255.0 (config-if)# ip access-group Faculty1 in | 認証用VLAN30にインタフェースIPアドレスを設定します。 アクセスリスト「Faculty1」を適応します。 |
| (config)# interface vlan 100 (config-if)# ip address 192.168.100.12 255.255.255.0 (config-if)# ip access-group Faculty2 in | 認証用VLAN100にインタフェースIPアドレスを設定します。 アクセスリスト「Faculty2」を適応します。 |
| (config)# interface vlan 1000 (config-if)# ip address 172.16.0.12 255.255.255.0 | 管理用VLAN1000にインタフェースIPアドレスを設定します。 |

| デフォルトルートの設定 | |
|---|--|
| (config)# ip route 0.0.0.0 0.0.0.0 172.16.0.254 | RADIUSサーバと通信を行うため、デフォルトルートを設定 します。 |
| アクセスリストの作成 | |
| <pre>(config)# ip access-list extended "Auth" (config-ext-nacl)# 10 permit udp any any eq bootps (config-ext-nacl)# 20 permit udp any any eq domain (config-ext-nacl)# 30 permit ip 192. 168. 30. 0 0. 0. 0. 255 host 10. 50. 0. 1 (config-ext-nacl)# 40 permit ip 192. 168. 100. 0 0. 0. 0. 255 host 10. 50. 0. 1 (config-ext-nacl)# 50 permit ip 192. 168. 30. 0 0. 0. 0. 255 host 10. 51. 0. 1 (config-ext-nacl)# 60 permit ip 192. 168. 100. 0 0. 0. 0. 255 host 10. 51. 0. 1</pre> | 認証前アクセスリストとして定義する"Auth"を作成しま す。 DHCPパケットの許可を設定します DNSパケットの許可を設定します 検疫サーバ宛IP通信を許可します ●設定ポイント(3) 「認証前アクセスリストの設定」 |
| (config)# ip access-list extended "Faculty1" (config-ext-nacl)# 10 deny ip 192.168.30.0 0.0.0.255 10.53.0.0 0.0.0.255 (config-ext-nacl)# 20 permit ip any any | 学部1用に他の学部のサーバに通信できないようにするア クセスリスト「Faculty1」を作成する。 |
| (config)# ip access-list extended "Faculty2" (config-ext-nacl)# 10 deny ip 192.168.100.0 0.0.0.255 10.52.0.0 0.0.0.255 (config-ext-nacl)# 20 permit ip any any | 学部2用に他の学部のサーバに通信できないようにするア クセスリスト「Faculty2」を作成する。 |
| Web 認証の設定 | |
| (config)# web-authentication system-auth-control (config)# web-authentication ip address 10.10.10.10 | Web認証を有効にします。 Web認証専用IPアドレスを設定します。本ガイドでは 「10.10.10」としています。●設定ポイント(4) 「Web認証専用IPアドレスを設定する」 |
| (config)# web-authentication redirect-mode http | URLリダイレクトのリダイレクトモードをHTTPに設定しま す。●設定ポイント(2) 「URLリダイレクト機能のリダイレクトモードを変更する」 |
| (config)# aaa authentication web-authentication default group | ●設定ポイント(5) 「Web認証の最大接続時間を調整する」 RADIUSサーバでユーザ認証を行うことを設定します。 |
| | |
| MAC 認証の設定 | |
| <pre>(config)# mac-authentication system-auth-control (config)# mac-authentication id-format 1</pre> | MAC認証を有効にします。 RADIUSサーバへ認証要求する際のMACアドレス形式をフォ ーマット1に設定します。 |
| (config)# mac-authentication password macpass | MAC認証で、RADIUSサーバに認証要求を出すときの端末ユー ザで使用するパスワードを設定します。 |
| (config)# aaa authentication web-authentication default group radius | MAC認証機能でのRADIUSサーバの使用有無を設定します。 ●設定ポイント(7) 「検疫除外端末の設定」 |
| RADIUS サーバの設定 | |
| (config)# radius-server host 10.50.0.1 key "alaxala" | RADIUSサーバのIPアドレス、シークレットキーを設定しま す。●設定ポイント(6) 「RADIUSサーバの設定をする」 |

3.2.4 Web 認証画面入れ替え

NOSiDE 検疫サーバの検疫画面へリダイレクトするように設定した HTML ファイルをスイッチの login.html ファイルと入替えます。 以下に Web 認証画面入れ替え手順を示します。

- ①本ガイド付録に添付されている「login.html」ファイルを編集します。「login.html」ファイルを メモ帳等のエディタで開き以下2行のXXX.XXX.XXX 部分を検疫サーバのアドレスに修正 します。
 - ※ 本ガイドの環境に合わせる場合 XXX.XXX.XXX.XXX を 10.50.0.1 に修正してください。
- ②編集した「login.html」ファイルを MC または FTP で認証スイッチへコピーし以下のコマンドを 実行してください。

set web-authentication html-files <directory> -f

ただし、本コマンドはディレクトリ指定のため下記コマンドでディレクトリ作成してファイル移 動後に set コマンドを実行してください。

AX2400S、AX3600S mkdir <directory name>

AX1200S mkdir ramdisk <directory name>

※ 本ガイド付録の「login.html」ファイルを使用しない場合は、AXシリーズ製品マニュアル「コ ンフィグレーションガイド」の「Web認証画面作成手引き」を参照し作成してください。

3.3 検疫サーバの設定

NOSiDE 検疫サーバは、Windows Server 2003 に RADIUS サーバや Microsoft SQL Server を含め、 複数のサーバコンポーネント及び NOSiDE コンポーネントをインストールします。各コンポーネン トについては、それぞれ別のサーバマシンで構成して連携させる事で NOSiDE 検疫ネットワークシ ステムを構築する事も可能です。

本ガイドでは、1 台の Windows Server 2003 に必要なコンポーネントを全て構成したうえで、 NOSiDE 構成管理サブシステムにて AX シリーズと連携するネットワーク認証関連設定のみを示しま す。各サーバコンポーネント、NOSiDE コンポーネントは既にインストール及び初期設定済みである ことが前提です。OS ならびに Microsoft SQL Server、サーバコンポーネントに関してのインストー ル及び設定手順等は Microsoft のホームページを、NOSiDE コンポーネントのインストール及び設定 手順は NOSiDE のマニュアルを参照して下さい。

以下に NOSiDE 検疫サーバの構成ステップを記載します。

- (1) **事前準備**…本ガイドで記載しているネットワーク接続認証関連の設定以前に検疫サーバに 必要な設定や作業について示します。
- (2) IASの設定…本ガイドのネットワーク構成に合わせたIASの設定手順を示します。
- (3) DNSサーバの設定…本システムにて動作するDNSサーバの設定を行います。
- (4) DHCPサーバの設定…本システムにて動作するDHCPサーバの設定を行います。
- (5) ネットワーク接続認証設定…NOSiDE検疫サーバの設定手順を示します。
- (6) 検疫除外端末の設定…NOSiDE検疫が出来ないプリンタなどを、AXシリーズのサポートす るMAC認証により接続許可させる設定手順を示します。

3.3.1 事前準備

(1) 検疫サーバにインストールするコンポーネント

Windows Server の各コンポーネントや NOSiDE のコンポーネントのインストール順やパラメータ 等については「NOSiDE Inventory Sub System 検疫環境構築手順書 v1.19 対応版」、「NOSiDE INVENTORY SUB SYSTEM V1.19 インストール編マニュアル」を参照して下さい。

本構成でインストールするNOSiDEコンポーネント

- NOSiDE 構成管理サブシステム(データベース)
- NOSiDE 構成管理サブシステム(管理画面)
- NOSiDE 構成管理サブシステム(操作画面)
- NOSiDE 構成管理サブシステム(RADIUS 拡張モジュール)
- (2) NOSiDE 検疫サーバの初期設定

全てのコンポーネントのインストール完了後、以下の検疫サーバの初期設定を行います。

- ・設定時は必ず「NOSiDE Inventory Sub System 検疫環境構築手順書 v1.19 対応版」、「NOSiDE INVENTORY SUB SYSTEM V1.19 管理画面マニュアル」を参照して下さい。
 - システム環境設定
 - サービスを提供する企業の追加
 - ユーザ情報の設定(学部 1,2 のグループ及びグループに所属するユーザーの作成)
 - 動作確認

3.3.2 IAS の設定

ここでは本システム内で動作する IAS の設定方法を示します。

本項目の設定やシステムを利用するユーザやグループの登録については、NOSiDE構成管理サブシ ステム(管理)によって作成されているものとします。本項では以下3項目の設定を行います。

なお本設定は「NOSiDE Inventory Sub System 検疫環境構築手順書 v1.19 対応版」の参照が不可欠です必ずご用意してください。

- (1) RADIUS クライアントの設定
- (2) リモートアクセスポリシーの設定
- (3) 接続要求ポリシーの設定
- (1) RADIUS クライアントの設定

RADIUS クライアントの設定方法を以下に示します。

①「スタート」→「管理ツール」→「インターネット認証サービス」を開き、左画面の「RADIUS クライアント」を選択して該当フレンドリ名のプロパティを開く。(フレンドリ名が存在しない場 合は新規作成する)

②プロパティ画面にて下記2項目を確認する。

- アドレス : 認証スイッチの IP アドレス。
 本ガイドでは(172.16.0.11 と 172.16.0.12)と設定しています。
- ・共有シークレット:認証スイッチのコンフィグレーションで設定したキー。
 本ガイドでは "alaxala"と設定しています。

| ♪インターネット認証サービス | | |
|--|---|---------------|
| ファイル(E) 操作(A) 表示(V) ヘルブ(H) | | |
| | | |
| ◆ インターネット認証サービス (ローカル) ● AADIUS クライアント ● リモート アクセスのログ ● ダ リモート アクセス ポリシー ● ● 1945年世の知識 | フレンドリ名 アドレス プロトコル 3 A/2430S 172.160.11 RADIUS 3 A/2430S 172.160.12 RADIUS 3 A/2430S 172.160.12 RADIUS | 21 |
| □ 接続要求の処理 | AX2430507(1)/574 設定 フレンドリ名(E): AX243058 アドレス (IP または DNS)(D): [172160.11 確認(型) クライアント ベンダの層性に基づくリモート アクセス ポリシーを使用している場合、 RADIUS クライアントのベンダを指定してください。 クライアント製造元(E): RADIUS Standard 要求はメッセージ認証層性を含んでいる必要がある(B) 共有シークレット(S): ******* 共有シークレットの確認入力(Q): | × × |
| | OK キャンセル 道用 |](<u>A</u>) |

図 3.3-1 RADIUS クライアント設定

(2) リモートアクセスポリシーの設定

 IAS のリモートアクセスポリシーの設定をする必要があります。詳細は「NOSiDE Inventory Sub System 検疫環境構築手順書 v1.19 対応版」の「10.3.1. インターネット認証サービスの設定の⑥ ~⑨ 」を実施してください。

(3) 接続要求ポリシーの設定

 IAS の接続要求ポリシーにてプロファイルの編集を行う必要があります。詳細は「NOSiDE Inventory Sub System 検疫環境構築手順書 v1.19 対応版」の「10.3.1. インターネット認証サー ビスの設定の①~⑤」を実施してください。

3.3.3 DNS サーバの設定

本構築例では AX シリーズの Web 認証で URL リダイレクト機能を使用しています。クライアント 端末からの任意の Web アクセスに対し検疫画面を表示させるため、認証前に名前解決が可能な環境 となっています。

DNS サーバには特別な設定が必要ないため本ガイドでは設定方法の記載を省いています。構築時 はクライアント端末から名前解決が成功することを確認してください。

3.3.4 DHCP サーバの設定

本構築例では DHCP を使用してクライアント端末に IP アドレスを配布しています。そのため各学 部用 VLAN (VLAN30,100) に対して DHCP サーバでプールを作成して下さい。 本ガイドでは以下の様に設定しています。

| 学部名 | プール名 | ネットワーク | リース期間 | デフォルトルータ | DNS サーバ |
|------|---------|------------------|-------|-----------------|-----------|
| 学部 1 | VLAN30 | 192.168.30.0/24 | 8日 | 192.168.30.254 | 10.50.0.1 |
| 学部 2 | VLAN100 | 192.168.100.0/24 | 8日 | 192.168.100.254 | 10.50.0.1 |

表 3.3-1 DHCP サーバの設定

3.3.5 ネットワーク接続認証設定

本ガイドで構築する検疫ネットワーク構成図について、NOSiDE構成管理サブシステム(管理)の 設定方法を示します。

- 以下に示す設定項目以外は「NOSiDE Inventory Sub System 検疫環境構築手順書 v1.19 対応版」 にて設定済みであるものとします。
 - 認証スイッチ設定
 - サブネット別認証スイッチ設定

①ログオン

NOSiDE 構成管理サブシステムにシステム管理者としてログオンする。 (インストール時に設定した管理者のログオン ID でログオンしてください。)

| 🗿 NOSiDE PC構成管理サブシステム(管理画面)~ログオン - Microsoft Internet Explorer |
|---|
| ファイル(主) 編集(主) 表示(公) お気に入り(4) ツール(エ) ヘルプ(日) 10 11 11 11 11 11 11 11 11 11 11 11 11 |
| ③ 戻る ▼ ⑤ - 🖹 2 6 / 2 検索 ☆お気に入り 6 2 でドレス 2 をかけた //105001/PCInve 2 2 移動 |
| リンク 🥑 駅探 🧃 日情動意 🧃 リシテア(ログイン画面) 🧃 リモート デスクトップ 🥑 @IT 🍠 OSEWeb 🥑 Google 🍯 Excite エキサイト 💙 |
| NOSIDE [®] PC 構成管理サブシステム |
| 9℃ 認証情報を入力してください |
| ログオンID: |
| パスワード: |
| ■システム管理者でログオン |
| <u>ログオン</u> |
| Copyright(c) 2002–2007, NTT DATA Corp., NTT DATA INTELLILINK Corp. |
| ◎ ページが表示されました |

図 3.3-2 NOSiDE 設定画面 1

②認証スイッチ設定

管理画面にログオン後、「管理企業の選択」画面にて作成した対象の企業を選択する。 「ネットワーク接続認証管理」→「認証スイッチ設定」→「認証スイッチ追加」をクリックし、 下記 6 項目を設定する。

- ・IP アドレス:認証スイッチにて「Web 認証専用 IP アドレス」として定義した IP アドレス。(本ガイドでは 10.10.10 を設定しています。)
- ・プロトコル:「HTTP」を選択。
- ポート:80を入力。
- 認証スイッチ種別:「AlaxalA (AX2430S)」を選択。
- ・リクエストタイムアウト:60秒(目安値です。環境に応じて変更して下さい)

• 説明:任意

| 認証スイッチ設定 | 2 | | | | | | |
|------------------------|--------------|-------------|------------------|-------------------|---------------|-----|-----------|
| | | | | | | | |
| 認识イッチ設定 | 認正スイッチグループ設定 | サプネット別認証スー | イッチ設定 | | | | |
| フィルタ: AlaxalA(AX2430S) | | | | | | | 表示件数 10 토 |
| IPアドレス 🔺 | プロトコル | オート | 認証スイッチ種別 | リク タイ <i>1</i> | ፲፲ አት ፊፖሳት | 〕此明 | |
| 10 . 10 . 10 . 10 | C http | 80 | AlaxaIA(AX2430S) | • 6 | 50 秒 | | 更新 キャンセル |
| 全選択 全解除 | 認証スイッチ削除 | 認証スイッチョ自加 | | | | | 1件 |
| | | | | | | | 1 |
| ■インポート | 参照 米差分レコー | ドのみ更新・追加します | t | | | | |
| ■エクスポート □ フォーマット(| ወው | | | | | | |
| | | | | | | | |

図 3.3-3 NOSiDE 設定画面 2

※認証スイッチ種別に関してはAX1200Sシリーズを使用する場合でも「AlaxalA(AX2430S)」を 選択してください。詳細は7.1.1認証スイッチ種別についてを参照して下さい。

③認証スイッチ設定確認

「更新」ボタンをクリックし、認証スイッチが登録された事を確認する。

| 認証スイッチ設定 | | | | | | |
|------------------------|-----------------|------------------|------------------|-----------------|------|----|
| 語Iスイッチ設定 | 語正スイッチグループ設定 | サブネット別語正スイッチ設定 | | | | |
| フィルタ: AlaxalA(AX2430S) | | | | | 表示件翻 | 10 |
| IPアドレス 🔺 | אבאסל | ポ−ト | 認証スイッチ種別 | ሀクエスト タイムアウト | 說明 | |
| 10.10.10 | http | 80 | AlaxaIA(AX2430S) | 60 秒 | | 編集 |
| 全選択 全解除 | 認識正スイッチ削り除 | 認証スイッチ追加 | | | | |
| 全選択 全解除 | 記録正スイッチ肖明余 | 認識正スイッチ注意力の | | | | |
| ∄ インポート | 参照 米差分レコードのる | ゆ更新・追加します | | | | |
| 🖹 エクスポート 🗆 フォーマッ | ትወ ው | | | | | |

図 3.3-4 NOSiDE 設定画面 3

④サブネット別認証スイッチ設定

「サブネット別認証スイッチ設定」タブを選択して「手動追加」をクリックし、下記6項目を 設定する。

・サブネットアドレス: クライアント用 VLAN のネットワークアドレス。

- ・サブネットマスク:クライアント用 VLAN のサブネットマスク。
- 認証スイッチの選択:②にて登録した認証スイッチにチェックする。

・ログオン時の認証処理:「実行する」を選択。拡張処理は「なにもしない」を選択。

・ログアウト時の認証処理:「実行しない」を選択。拡張処理は「なにもしない」を選択。

• 説明:任意

| ₹₩≦ []] | ネット別型証スイッチ設定 - の名のので、 サブネットアドレス: 192 | - Microsoft ネット別認言 | Internet Explorer 正スイッチ設定/約 | 新規作成 | | |
|------------|---|-----------------------|--|------|------------------|-----------|
| ſ | サブネットマスク: <mark>255 .</mark> 1992 1 | 255 | 255 0 📑 | 8明: | | |
| l | 802.1x認証を行う すべてのWEB認証スイッラ | チヘリクエストを | 行う | | | |
| | 認証スイッチ | 認証スイ | ッチグループ | | | |
| | フィルタ: AlaxaIA(AX243 | 30S) | • | | đ | 長示件数 10 💌 |
| | IPアドレス・ | ^ | プロトコル | ポート | 認証スイッチ種別 | 説明 |
| | ☑ 10.10.10.10 | | http | 80 | AlaxalA(AX2430S) | |
| | 全選択 全解除 | | | | | 1件 |
| | | | | | | 1 |
| 3 3 | 記証 りカ 鉄続ポリシーOK (ログオン) 実 鉄続ポリシーNG (ログアウト) 実 | 認証処理 【行する | <u> 並張処理</u> ↓ なにもしない ・ なにもしない ・ 更新 | | ンセル | |

図 3.3-5 NOSiDE 設定画面 4

⑤サブネット別認証スイッチ設定の確認

「更新」ボタンをクリックし、サブネット別認証スイッチが登録された事を確認する。 クライアント用 VLAN 毎に④の追加設定を行う。

| 諸正スイッチ設定 | 2 12 | Eスイッチグル | レープ設定 | マト別 | 読まれ | いチ設定 | 1 | | | | | | |
|---------------|---------------|------------|------------------|--------|-----------------------------|-------------------|-------------------|--------------|----|-----|--------------|----------------------|--------------|
| | | | | | | | | | | | | | 表示件数 |
| サブネットアドレス | サブネットマスク | ⊇録√シン 敷 | WEB | 2証入1 | (9 5 | | WEB認証スイッチグル ープ | 802.1x翌 ≣ | 説明 | リクオ | ログオン拡張動 作 | לי <i>ידע</i> ם א | ログアウト拡 動作 |
| 192.168.100.0 | 255.255.255.0 | 1 | 10.10.10.10 | http 8 | 0 (A) | NaxalA X2430S) | | | | 0 | | | |
| 全選択 全解除 | サブネット設定削 | 手動追加 | 登録マシン情報から追 tm | | | | | | | | | | |

図 3.3-6 NOSiDE 設定画面 5

3.3.6 検疫除外端末の設定

NOSiDE 検疫システムでは、クライアント端末は検疫チェックを実施しない限り通信を制限されて います。そのため、検疫チェックやブラウザによる Web 認証をサポートしていないプリンタ等の端 末を接続する場合は、事前に許可設定を行う必要があります。

ここでは、NOSiDE 検疫システムにて検疫除外端末であるプリンタを、AX シリーズのサポートする MAC 認証を用いて接続を許可する設定方法を示します。

(1) AX の設定

プリンタを接続するポートに対して MAC 認証の設定を行います。 コンフィグレーションに関しては**3.2.1構築ポイントの(7)**を参照して下さい。

(2) NOSiDE 検疫サーバの設定

NOSiDE 構成管理サブシステム(管理)にて、プリンタの MAC アドレスをログオン ID としてユ ーザ登録を行い、そのユーザのみ検疫チェックを実施しなくても接続制限が解除されるように設定し ます。

①プリンタのユーザ登録

NOSiDE 構成管理サブシステムにシステム管理者としてログオンし、「管理企業の選択」画面にて作成した対象の企業を選択する。

「ユーザー情報管理」→「ユーザー情報の設定」をクリックし、「表示切替」のドロップダ ウンメニューから「取得元リソース情報(リソース元により編集可)」を選択する。 「検索」ボタンをクリックし、一覧表示されている下の「追加」リンクボタンをクリックし て下記3項目を設定する。

- ・ユーザー名:接続が許可されるユーザ。(この例では「プリンタ」)
- ・ログオン ID: 接続するプリンタの MAC アドレス。
- パスワード:認証スイッチのコンフィグレーションで設定した専用パスワード。
 (本例では "macpass" と設定しています。)



図 3.3-7 検疫除外端末の設定1

②ユーザ登録の確認

「更新(戻る)」ボタンをクリックし、ユーザー情報の設定画面にて作成したユーザ(プリンタ)が登録されている事を確認する。

| | | | serrvanie=occonowrype=r | 1 487 01.12 | |
|-------------|---------------------------------|---------------|------------------------------------|------------------|--------------------------|
| | PC 構成管理サノン. | | | 米町月 | |
| | | ユーリー信報管理 中版 | ウノトリェア情報管理 ハー 管理 エージェント情報管理 | ・トリェア情報管理 果訂情報 | 管理 ゼキュリティ情報 製造設定 お問いき |
| フーザー | 情報の設定 | | | | |
| - , | IN TROPIECAL | | | | |
| 表示切替 | 取得テロリース情報(い) | ノーフ(こと)の編集(T) | | | |
| 303745 B | [4x107672 - 741848(7) | | | | |
| | | 基本情報 | 1 | | - |
| 表題 | | | | | 更新 |
| _ | | フーザーのオ | 全 金 | | |
| グループ名 | 全て | - | e de | | |
| ユーザー名 | | | | | 検索 |
| | | | | | |
| | | | | | 件数: 10 👤 |
| | ユーザー名 🔺 | 所属 | 役職 | メールアドレス | |
| 🗆 user100 | | Students | | | 編集 |
| 🗖 user101 | | Gakubu1 | | | 編集 |
| 🗆 user102 | | Gakubu2 | | | 編集 |
| 🗖 teacher01 | | Teachers | 講師 | | 編集 |
| ロザリンタ | | | | | 編集 |
| 全選択 全解除 追加 | 0 削除 | | | | 5件 |

図 3.3-8 検疫除外端末の設定 2

③グループへの所属

ユーザ情報の設定画面にて、登録したユーザ(プリンタ)をチェックし、画面右の「編集」 リンクボタンをクリックする。ユーザーの編集画面にて、所属するグループをチェックし「選 択項目所属設定」リンクボタンをクリックする。最後に「更新」ボタンをクリックする。

| ーザーの編集 - Microsoft Intern | et Explorer | یلے | | | | |
|------------------------------------|---|--|--|--|--|--|
| (ル(E) 編集(E) 表示(⊻) お気() | (入り(品) ツール(① ヘルブ(出) | | | | | |
| る ▼ ② → 🖹 🗿 🏠 🔎 検索 🏂 お気に入り 🔗 😥 😓 ▼ | | | | | | |
| パロ) 🕘 http://localhost/PCInven | toryManage/EditUser.aspx?GroupID=NOSiDESearch1&UserName=&IDorPath=LDAP%3a%2f%2fexan | nple.co.jp%2fCN%3d0019b97d4b 🗾 💽 移動 リン | | | | |
| | ユーザー情報管理 市販ソフトウェア情報管理 ハードウェア | 情報管理 集計情報管理 セキュリティ情報管理 | | | | |
| | 資産管理 エージェント情報管理 ネット | ・ワーク接続認証管理 環境設定 お問い合わ | | | | |
| ユーザーの編集 | | A | | | | |
| | ユーザー情報 | | | | | |
| ログオンID | 0019b97d4bfa | | | | | |
| ユーザー名 | プリンタ | | | | | |
| ユーザー名(カナ) | プリンタ | | | | | |
| 役職 | | | | | | |
| 電話番号 | | | | | | |
| メールアドレス | メールアドレス | | | | | |
| | パスワードの変更 | | | | | |
| | | · | | | | |
| | | 件数: 10 💌 | | | | |
| グループ名 ▲ | 所属 | 説明 | | | | |
| 🗖 Gakubu1 | 所属 | | | | | |
| 🗖 Gakubu2 | | | | | | |
| Students | | 生徒G | | | | |
| Teachers | | 講師G | | | | |
| | 選択項目所属設定 選択項目所属設定解除 | 4件 | | | | |
| | | 1 | | | | |
| | 更新リセット | | | | | |
| | | | | | | |
| ◀ ユーザー情報の設定 へ | | | | | | |
| | | | | | | |
| | Copyright(c) 2002–2009, NTT [| DATA Corp., NTT DATA INTELLILINK Corp | | | | |
| | | | | | | |

図 3.3-9 検疫除外端末の設定 3

④グループへの所属確認

ユーザー情報の設定画面にて、登録したユーザ(プリンタ)が指定したグループに所属して いる事を確認する。

| ユーザー名 🔺 | 所属 | 役嚍 | メールアドレス | |
|---------------|----------|----|---------|----|
| 🗆 user100 | Students | | | 編集 |
| 🗆 user101 | Gakubu1 | | | 編集 |
| 🗆 user102 | Gakubu2 | | | 編集 |
| 🗖 teacher01 | Teachers | 講師 | | 編集 |
| ロプリンタ | Gakubu1 | | | 編集 |
| 全選択 全解除 追加 削除 | | | | 5件 |
| | | | | 1 |

図 3.3-10 検疫除外端末の設定 4

※ユーザの登録後は「SQL Server Management Studio」にて日時バッチを実行して下さい。 詳細は NOSiDE のマニュアルを参照して下さい。

⑤許可ユーザの登録

メインメニューより「ネットワーク接続認証管理」→「認証の許可・拒否」をクリックし、 「ユーザー追加」リンクボタンをクリックする。

認証の許可・拒否/ユーザの追加画面にて、下記5項目を入力し「追加」ボタンをクリック する。

検索方法:「組織階層表示」を選択。

• 組織階層 [1]:作成したユーザ(プリンタ)の所属するグループを選択。 (本ガイドでは検疫除外端末Gと設定しています。)

- •**ユーザー名**:作成したユーザ(プリンタ)をチェック。
- ・認証:「許可」を選択。
- •**備考**:任意



図 3.3-11 検疫除外端末の設定5

⑥許可ユーザ登録の確認

戻る」ボタンをクリックし、認証の許可・拒否画面にてユーザ(プリンタ)が認証許可指定され ている事を確認する。

| 認証の許 | F可·拒否 | | | | | |
|-------------|------------------------------|--------|---------|----|--------|----------|
| ユーザー制御設定 | ₽インポート: ₽エリスポート:■フォーマットのみ | 参照 | | | 表示 | 件數 200 💌 |
| | ユーザー名 🔺 | 電話番号 | グループ名 | 認証 | 備考 | |
| 拡張フィルタ設定 | □ プリンタ | | Gakubu1 | 許可 | 検疫除外端末 | 編集 |
| ■ フィルタ基本設定 | 全選択 全解除 | ユーザー削除 | ユーザー追加 | | | 1件 |
| □ フィルタリスト設定 | | | | | | 1 |
| | | | | | | |
| マシンを設定してくだき | | | | | | |

図 3.3-12 検疫除外端末の設定6

⑦以上で検疫除外端末の設定は終了です。

4. システム構築例2(ダイナミック VLAN モード)

4.1 検疫システムの構成

本章では、AXシリーズのWeb認証(ダイナミックVLAN)方式を用いたNOSiDE検疫システムの構築 例を示します。なお本構成の構築方法は3章システム構築例1(固定VLANモード)を基本に必要な 設定を追加、変更していく手順となっています。

4.1.1 ダイナミック VLAN モード導入シナリオ

本システムは、キャンパスネットワークへの導入を想定しています。

図 4.1-1 に示すキャンパスネットワークでは、講師と学生が混在し、認証スイッチの同一ポートを 共用して使用する運用ですが、講師と学生のサーバへのアクセス制御を、別々とします。

このようなネットワークに NOSiDE 検疫システムを導入する場合、AX シリーズのダイナミック VLAN モードを導入するのが最適です。各フロアに設置された AX シリーズの認証スイッチは、認証 ポートに接続するクライアント端末ごとに所属する VLAN を動的に変更することが可能です。

図 4.1-1 に示す構成では、同じ教室内の同じスイッチングハブに講師と学生がそれぞれクライアン ト端末を接続して NOSiDE 検疫サーバによる検疫と AX シリーズの認証スイッチによるネットワー ク認証を行います。同じ場所で認証と検疫に成功しても学生は学生用 VLAN に所属し、学生用のサ ーバのみ通信可能です。講師の場合は講師用 VLAN に所属し学生用サーバと講師用サーバの両方に 通信可能となります。



図 4.1-1 ダイナミック VLAN モードシナリオ

4.1.2 検疫システム基本構成

以下に本章にて構築する検疫システムの基本的なネットワーク構成図と構成機器一覧表を示しま す。



コアスイッチには AX3630S を配置し、VRRP を用いて装置を冗長化します。また、装置間はリン クアグリゲーションを用いて回線を冗長化します。検疫サーバおよび検疫により隔離された端末を治 療する修復サーバは、コアスイッチ配下に接続します。コアスイッチ同士の経路交換には、OSPF 等 のルーティングプロトコルを使用します。

エッジスイッチには認証スイッチとして動作する AX2430S と AX1240S を配置し、スパニングツ リーを用いて冗長化します。

検疫を行う端末は、エッジスイッチに直接またはハブを介して接続します。IP アドレスに関しては コアスイッチ配下にある DHCP サーバより配布されます。なお本ガイドの構成では修復サーバに疎 通確認用の PC を使用していますが、実環境では WSUS やセキュリティパッチ配布サーバなどを設 置することを想定しています。

本ガイドで使用するサーバとクライアント端末を以下に示します。

| | 56 |
|---------------------------------|---------------|
| 検疫サーバ | クライアント端末 |
| Windows Server 2003 | Windows XP |
| •ActiveDirectory ドメインサービス | Windows Vista |
| •DNS サーバ | |
| •DHCP サーバ | |
| •Web サーバ(IIS) | |
| •RADIUS サーバ(IAS) | |
| データベースサーバ(Microsoft SQL Server) | |
| NOSiDE 検疫サーバ | |

表 4.1-1 サーバとクライアント一覧

4.1.3 ネットワーク構成図(詳細)

AX シリーズの Web 認証(ダイナミック VLAN モード)と NOSiDE を連携した検疫ネットワークの詳細な構成図を以下に示します。



図 4.1-3 ネットワーク構成図(詳細)

4.1.4 各 VLAN の定義

本構築例にて使用する VLAN の定義情報を以下の表に示します。

| VLAN 名 | VLANID | ネットワーク IP アドレス | 用途 | 設置サーバ |
|-----------------|--------|-------------------|---|-------|
| | 5 | 10.5.0.0/24 | | |
| OSPF 用 VI AN | 15 | 10.15.0.0/24 | OSPF ネットワーク。 | _ |
| | 25 | 10.25.0.0/24 | | |
| 検疫サーバ用 | 50 | 10.50.0.0/24 | 検疫前、及び検疫失敗した端末が通信可能 | 検疫サーバ |
| VLAN | 51 | 10.51.0.0/24 | なサーバが設置される VLAN。 | 修復サーバ |
| 講師用サーバ | 52 | 10.52.0.0/24 | 検疫に成功した端末が通信可能なサーバ | 講師用 |
| VLAN | | | が設置される VLAN。(講師のみ通信可) | サーバ |
| 学生用サーバ | 53 | 10 53 0 0/24 | 検疫に成功した端末が通信可能なサーバ | 学生用 |
| VLAN | 00 | 10.00.0.0/24 | が設置される VLAN。(講師、学生が通信可) | サーバ |
| 認証前 VLAN | 10 | 192.168.10.0/24 | 認証、検疫前にクライアント端末が所属す る VLAN。 | _ |
| 学生用 VLAN | 30 | 192.168.30.0/24 | 学生がログオンし認証と検疫に成功した クライアント端末が所属する VLAN。 | _ |
| 講師用 VLAN | 100 | 192.168.100.0/24 | 講師がログオンし認証と検疫に成功した クライアント端末が所属する VLAN。 | _ |
| 管理用 VLAN | 1000 | 172.16.0.0/24 | 各装置を管理するための VLAN。 | — |

表 4.1-2 各 VLAN の定義

4.1.5 クライアント端末の検疫結果に応じた通信可否

クライアント端末の検疫結果に応じた各サーバへの通信可否を以下の表に示します。

| 端末→各サーバ | DHCP、DNS サーバ | 検疫サーバ | 修復サーバ | 学生用サーバ | 講師用サーバ |
|--------------|-----------------|-------|-------|--------|--------|
| 認証前 VLAN の端末 | Δ | 0 | 0 | × | × |
| 学生用 VLAN の端末 | 0 | 0 | 0 | 0 | × |
| 講師用 VLAN の端末 | 0 | 0 | 0 | 0 | 0 |

表 4.1-3 クライアント端末の認証状態に応じた通信可否

(凡例) 〇:通信可能、×:通信不可、△:一部プロトコル(DHCP、DNS)のみ通信可能

4.1.6 認証スイッチのポート構成

ここで、認証スイッチのポートを以下のように設定します。本構築例ではプリンタなど検疫ができない機器を検疫除外端末として設定しています。検疫除外端末の設定に関しては4.2.1構築ポイントの(7)を参照して下さい。

| 認証スイッチ | 用途 | ポート種別 | VLAN | ポート番号 | 認証方式 |
|---------|----------|-------------|----------------|-----------|-------|
| AX2430S | 認証用 | MACVLAN ポート | 10,30,100 | 0~10 | Web認証 |
| AA24303 | アップリンク接続 | トランクポート | 10,30,100,1000 | 0/47~0/48 | |
| AV1240S | 認証用 | MACVLAN ポート | 10,30,100 | 0~10 | Web認証 |
| AX12403 | アップリンク接続 | トランクポート | 10,30,100,1000 | 0/25~0/26 | _ |

表 4.1-4 認証スイッチのポート構成

4.2 AX シリーズの設定

4.2.1 構築ポイント

本検疫システムにて認証スイッチの設定に関する構築ポイントを以下に示します。

(1) Web 認証用画面を入れ替える。

AX シリーズの Web 認証画面入れ替え機能を用いて「login.html」ファイルを入れ替え、直接ク ライアント端末からスイッチへの Web 認証操作をできないようにします。

認証スイッチへのWeb認証はNOSiDEの検疫チェック後に自動的に実行されるためユーザは意識 する必要がありません。Web認証画面入れ替え手順に関しては3.2.4Web認証画面入れ替えを参照 して下さい。

(2) URL リダイレクト機能のリダイレクトモードを変更する。

(1) で示す画面入れ替えと URL リダイレクト機能を併用する事で検疫前のクライアントが任意の http アクセスを実行した場合自動的に NOSiDE の検疫画面へジャンプするようにします。デフォルトの https モードでは証明書エラーが出ますので、リダイレクトモードを http に変更します。

(3) 認証前アクセスリストの作成

クライアント端末の検疫前及び検疫失敗時に以下の通信を許可するため、認証スイッチに認証前 アクセスリストを定義します。

- 本ガイドではクライアント端末の IP アドレスを DHCP サーバより配布しています。その ためクライアント端末からの DHCP パケットを許可します。
- ② 検疫前のクライアント端末から名前解決を可能にします。クライアント端末から DNS サ ーバ宛、DNS クエリパケットを許可します。
- ③ クライアント端末から NOSiDE の検疫サーバへの IP 通信を許可します。
- ④ クライアント端末から修復サーバへの IP 通信を許可します。

(4) Web 認証専用 IP アドレスを設定する

Web 認証用の IP アドレスを設定します。この IP アドレスは全認証スイッチに共通して設定することが出来ます。この例では、「10.10.10.10」としています。

また、認証用 VLAN のインタフェースにも IP アドレス設定が必要です。

(5) Web 認証の最大接続時間を調整する

セキュリティ上、Web 認証は一度認証成功するとデフォルトで1時間後に自動的にログアウト します。運用方針に従って、適宜最大接続時間を調整して下さい。この例では、一日一回は必ずロ グアウトさせることを目的として1400分に設定しています。

(6) RADIUS サーバの設定をする

本ガイドでは RADIUS サーバと NOSiDE 検疫サーバは 1 台のマシンで構成していますが、別々 にサーバを設置する場合は、NOSiDE の RADIUS プロキシサーバを RADIUS サーバとして設定し て下さい。

(7) 検疫除外端末の設定

プリンタなどの検疫が出来ない端末を接続する場合、接続するポートにMAC認証を設定します。 この場合、NOSiDE側に該当端末のMACアドレスを登録しておく必要があります。(3.3.6検疫除外 端末の設定を参照)

(8) スパニングツリーのモードを変更する

AX シリーズではダイナミック VLAN モードでは認証ポートに MAC VLAN を使用します。MAC VLAN を使用する場合デフォルトの PVST+が使用できません。そのため本ガイドではマルチプルス パニングッリーを使用しています。

4.2.2 AX2430S のコンフィグレーション

本構成における、認証スイッチのコンフィグレーションの解説を下記に示します。なおコアスイッチに関しては付録を参照して下さい。

AX2430S のコンフィグレーション

| edge#1 (AX2430S)の設定 | |
|---|--|
| 事前設定 | |
| (config)# hostname "edge#1" (config)# clock timezone "JST" +9 0 | ホスト名の設定をします。 タイムゾーンの設定をします。 |
| VLAN の定義 | |
| (config)# vlan 1 (config-vlan)# state suspend (config)# vlan 10,1000 (config-vlan)# state active | VLAN1は使用しないため、無効にします。 認証前VLANとしてVLAN10を、管理用VLANとしてVLAN1000を 作成します。 |
| (config)# vlan 30,100 mac-based (config-vlan)# state active | 学生用VLANとしてVLAN30を、講師用VLANとしてVLAN100を作 成します。 |
| スパニングツリーの設定 | |
| <pre>(config)# spanning-tree mode mst (config)# spanning-tree mst configuration (config-mst)# name NOSiDE (config-mst)# revision 1 (config-mst)# instance 1 vlans 100, 1000 (config-mst)# instance 2 vlans 30 (config-mst)# instance 3 vlans 10 (config)# interface range gigabitethernet 0/1-10</pre> | マルチプルスパニングツリーを有効にし、リージョン、イ ンスタンスを設定します。 リージョン名:NOSiDE リビジョン番号:1 MSTインスタンス1:VLAN100,1000 MSTインスタンス2:VLAN30 MSTインスタンス3:VLAN10 |
| (contig-it-range)# spanning-tree portfast | 「スパニングツリーのモードを変更する」 認証用ポート0/1~0/10に対して、スパニングツリーの PortFast機能を適用し、スパニングツリー対象外とします。 |
| インターフェイスの設定 | |
| 物理ポートの設定 | |
| Web認証用 (config)# interface range gigabitethernet 0/1-10 (config-if-range)# switchport mode mac-vlan (config-if-range)# switchport mac vlan 30,100 (config-if-range)# switchport mac native vlan 10 (config-if-range)# web-authentication port (config-if-range)# authentication ip access-group "Auth" (config-if-range)# authentication arp-relay | 認証ポートの設定 ポート0/1~0/10を認証ポートに設定します。 MACVLANポートに設定します。 MACVLAN30,100を設定します。 ネイティブVLAN10を設定します。 Web認証対象ポートの設定をします。 認証前アクセスリスト "WebAuth"を設定します。 認証前の端末から送信される他宛てARP パケットを認証対 象外のポートへ出力させます。 |
| MAC認証用 (config)# interface gigabitethernet 0/1 (config-if-range)# mac-authentication port | <mark>検疫除外端末の設定</mark> ポート0/1に検疫除外端末用にMAC認証設定をします。 |
| アップリンク用 (config)# interface range gigabitethernet 0/47-48 (config-if-range)# switchport mode trunk (config-if-range)# switchport trunk allowed vlan 10,30,100,1000 | アップリンクポートの設定 アップリンクポートの設定 ポート0/47~0/48をトランクポートに設定し、VLAN10、30、 100、1000を設定します。 |

| VLAN インターフェイスの設定 | |
|---|--|
| (config)# interface vlan 10 (config-if)# ip address 192.168.10.11 255.255.255.0 | 認証前VLAN10にインタフェースIPアドレスを設定します。 |
| (config)# interface vlan 30 (config-if)# ip address 192.168.30.11 255.255.255.0 (config-if)# ip access-group Students in | 学生用VLAN30にインタフェースIPアドレスを設定します。 アクセスリスト「Students」を適応します。 |
| (config)# interface vlan 100 (config-if)# ip address 192.168.100.11 255.255.255.0 | 講師用VLAN100にインタフェースIPアドレスを設定します。 |
| (config)# interface vlan 1000 (config-if)# ip address 172.16.0.11 255.255.255.0 | 管理用VLAN1000にインタフェースIPアドレスを設定しま す。 |
| デフォルトルートの設定 | |
| (config)# ip default-gateway 172.16.0.254 | RADIUSサーバと通信を行うため、デフォルトルートを設定 します。 |
| アクセスリストの作成 | |
| <pre>(config)# ip access-list extended "Auth" (config-ext-nacl)# 10 permit udp any any eq bootps (config-ext-nacl)# 20 permit udp any any eq domain (config-ext-nacl)# 30 permit ip 192.168.10.0 0.0.0.255 host 10.50.0.1 (config-ext-nacl)# 40 permit ip 192.168.10.0 0.0.0.255 host 10.51.0.1</pre> | 認証前アクセスリストとして定義する"Auth"を作成しま す。 DHCPパケットの許可を設定します DMSパケットの許可を設定します 検疫サーバ宛IP通信を許可します 修復サーパ宛IP通信を許可します ●設定ポイント(3) 「認証前アクセスリストの設定」 |
| (config)# ip access-list extended "Students" (config-ext-nacl)# 10 deny ip 192.168.30.0 0.0.0.255 10.52.0.0 0.0.0.255 (config-ext-nacl)# 20 permit ip any any | 学生用VLANに講師用サーバに通信できないようにするアク セスリスト「Students」を作成する。 |
| Web 認証の設定 | |
| <pre>(config) # web-authentication system-auth-control (config) # web-authentication ip address 10.10.10.10 (config) # web-authentication redirect-mode http</pre> | Web認証を有効にします。 Web認証専用IPアドレスを設定します。本ガイドでは 「10.10.10.10」としています。●設定ポイント(4) 「Web認証専用IPアドレスを設定する」 URLリダイレクトのリダイレクトモードをHTTPに設定しま す。●設定ポイント(2) 「URLリダイレクト機能のリダイレクトモードを変更する」 |
| (config)# web-authentication max-timer 1400 | ● <mark>設定ポイント(5)</mark> 「Web認証の最大接続時間を調整する」 |
| (config)# aaa authentication web-authentication default group radius | RADIUSサーバでユーザ認証を行うことを設定します。 |
| MAC 認証の設定 | |
| <pre>(config)# mac-authentication system-auth-control (config)# mac-authentication password macpass</pre> | MAC認証を有効にします。 MAC認証で, RADIUSサーバに認証要求を出すときの端末ユー ザで使用するパスワードを設定します。 |
| (config)# aaa authentication web-authentication default group radius | MAC認証機能でのRADIUSサーバの使用有無を設定します。 ●設定ポイント(7) 「検疫除外端末の設定」 |
| RADIUS サーバの設定 | |
| (config)# radius-server host 10.50.0.1 key "alaxala" | RADIUSサーバのIPアドレス、シークレットキーを設定しま す。●設定ポイント(6) 「RADIUSサーバの設定をする」 |

4.2.3 AX1240S のコンフィグレーション

| edge#2 (AX1240S)の設定 | |
|--|--|
| 事前設定 | |
| (config)# system function filter extended-authentication | フィルタ機能と拡張認証機能を使用するため、システムフ ァンクションリソース配分を変更します。 ※設定後は、装置の再起動が必要です。 |
| (config)# hostname "edge#2" (config)# clock timezone "JST" +9 0 | ホスト名の設定をします。 タイムゾーンの設定をします。 |
| VLAN の定義 | |
| (config)# vlan 1 (config-vlan)# state suspend | VLAN1は使用しないため、無効にします。 |
| (config)# vlan 10,1000 (config-vlan)# state active | 認証前VLANとしてVLANIOを、皆理用VLANとしてVLANIOUOを 作成します。 |
| (config)# vlan 30,100 mac-based (config-vlan)# state active | 学生用VLANとしてVLAN30を、講師用VLANとしてVLAN100を作 成します。 |
| スパニングツリーの設定 | |
| <pre>(config)# spanning-tree mode mst (config)# spanning-tree mst configuration (config-mst)# name NOSiDE (config-mst)# revision 1 (config-mst)# instance 1 vlans 100,1000 (config-mst)# instance 2 vlans 30 (config-mst)# instance 3 vlans 10</pre> | マルチプルスパニングツリーを有効にし、リージョン、イ ンスタンスを設定します。 リージョン名:NOSiDE リビジョン番号:1 MSTインスタンス1:VLAN100,1000 MSTインスタンス2:VLAN30 MSTインスタンス3:VLAN10 ●設定ポイント(8) 「スパニングツリーのモードを変更する」 |
| (config)# interface range fastethernet 0/1-10 (config-if-range)# spanning-tree portfast | 認証用ポート0/1~0/10に対して、スパニングツリーの PortFast機能を適用し、スパニングツリー対象外とします。 |
| インターフェイスの設定 | |
| 物理ポートの設定 | |
| Web認証用 (config)# interface range fastethernet 0/1-10 (config-if-range)# switchport mode mac-vlan (config-if-range)# switchport mac vlan 30,100 (config-if-range)# switchport mac native vlan 10 (config-if-range)# web-authentication port (config-if-range)# authentication ip access-group "Auth" (config-if-range)# authentication arp-relay | 認証ポートの設定 ポート0/1~0/10を認証ポートに設定します。 MACVLANポートに設定します。 MACVLAN30,100を設定します。 ネイティブVLAN10を設定します。 Web認証対象ポートの設定をします。 認証前アクセスリスト "WebAuth"を設定します。 認証前の端末から送信される他宛てARP パケットを認証対 象外のポートへ出力させます。 |
| MAC認証用 (config)# interface fastethernet 0/1 (config-if-range)# mac-authentication port | <mark>検疫除外端末の設定</mark> ポート0/1に検疫除外端末用にMAC認証設定をします。 |
| アップリンク用 (config)# interface range gigabitethernet 0/25-26 (config-if-range)# switchport mode trunk (config-if-range)# switchport trunk allowed vlan 10, 30, 100, 1000 | アップリンクポートの設定 ポート0/25~0/26をトランクポートに設定し、VLAN10、30、 100、1000を設定します。 |

| VLAN インターフェイスの設定 | |
|---|--|
| (config)# interface vlan 10 (config-if)# ip address 192.168.10.12 255.255.255.0 | 認証前VLAN10にインタフェースIPアドレスを設定します。 |
| (config)# interface vlan 30 (config-if)# ip address 192.168.30.12 255.255.255.0 (config-if)# ip access-group Students in | 学生用VLAN30にインタフェースIPアドレスを設定します。 アクセスリスト「Students」を適応します。 |
| (config)# interface vlan 100 (config-if)# ip address 192.168.100.12 255.255.255.0 | 講師用VLAN100にインタフェースIPアドレスを設定します。 |
| (config)# interface vlan 1000 (config-if)# ip address 172.16.0.12 255.255.255.0 | 管理用VLAN1000にインタフェースIPアドレスを設定しま す。 |
| デフォルトルートの設定 | |
| (config)# ip route 0.0.0.0 0.0.0.0 172.16.0.254 | RADIUSサーバと通信を行うため、デフォルトルートを設定 します。 |
| アクセスリストの作成 | |
| <pre>(config)# ip access-list extended "Auth" (config-ext-nacl)# 10 permit udp any any eq bootps (config-ext-nacl)# 20 permit udp any any eq domain (config-ext-nacl)# 30 permit ip 192.168.10.0 0.0.0.255 host 10.50.0.1 (config-ext-nacl)# 40 permit ip 192.168.10.0 0.0.0.255 host 10.51.0.1</pre> | 認証前アクセスリストとして定義する"Auth"を作成しま す。 DHCPパケットの許可を設定します DNSパケットの許可を設定します 検疫サーバ宛IP通信を許可します 修復サーバ宛IP通信を許可します ●設定ポイント(3) 「認証前アクセスリストの設定」 |
| (config)# ip access-list extended "Students" (config-ext-nacl)# 10 deny ip 192.168.30.0 0.0.0.255 10.52.0.0 0.0.0.255 (config-ext-nacl)# 20 permit ip any any | 学生用VLANに講師用サーバに通信できないようにするアク セスリスト「Students」を作成する。 |
| Web 認証の設定 | |
| <pre>(config)# web-authentication system-auth-control (config)# web-authentication ip address 10.10.10.10</pre> | Web認証を有効にします。 Web認証専用IPアドレスを設定します。本ガイドでは 「10.10.10.10」としています。●設定ポイント(4) 「Web認証専用IPアドレスを設定する」 |
| (config)# web-authentication redirect-mode http | URLリダイレクトのリダイレクトモードをHTTPに設定しま す。●設定ポイント(2) 「URLリダイレクト機能のリダイレクトモードを変更する」 |
| (config)# web-authentication max-timer 1400 | ● <mark>設定ポイント(5)</mark> 「Web認証の最大接続時間を調整する」 |
| (config)# aaa authentication web-authentication default group radius | RADIUSサーバでユーザ認証を行うことを設定します。 |
| MAC認証の設定 | |
| <pre>(config)# mac-authentication system-auth-control (config)# mac-authentication id-format 1</pre> | MAC認証を有効にします。 RADIUSサーバへ認証要求する際のMACアドレス形式をフォ ーマット1に設定します。 |
| (config)# mac-authentication password macpass | MAC認証で, RADIUSサーバに認証要求を出すときの端末ユー ザで使用するパスワードを設定します。 |
| (config)# aaa authentication web-authentication default group radius | MAC認証機能でのRADIUSサーバの使用有無を設定します。 ●設定ポイント(7) 「検疫除外端末の設定」 |
| RADIUS サーバの設定 | |
| (config)# radius-server host 10.50.0.1 key "alaxala" | RADIUSサーバのIPアドレス、シークレットキーを設定しま す。●設定ポイント(6) 「RADIUSサーバの設定をする」 |

4.2.4 Web 認証画面入れ替え

Web認証画面入れ替え方法は3.2.4Web認証画面入れ替えを参照して下さい。

4.3 検疫サーバの設定

検疫サーバの設定方法は3章システム構築例1(固定VLANモード)から一部変更、追加する手順 となっています。3.3検疫サーバの設定を参照してください。

4.3.1 事前準備

(1) 検疫サーバにインストールするコンポーネント

必要なコンポーネントに関しては3.3.1事前準備を参照して下さい。

(2) NOSiDE 検疫サーバの初期設定

- 全てのコンポーネントのインストール完了後、以下の検疫サーバの初期設定を行います。設定時は 必ず「NOSiDE Inventory Sub System 検疫環境構築手順書 v1.19 対応版」、「NOSiDE INVENTORY SUB SYSTEM V1.19 管理画面マニュアル」を参照して下さい。
 - システム環境設定
 - サービスを提供する企業の追加
 - ユーザ情報の設定(講師、学生グループ及び各グループに所属するユーザーの作成)
 - 動作確認

4.3.2 IAS の設定

IASの設定方法は3.3.2IASの設定を参照してください。

4.3.3 DNS サーバの設定

本構築例では AX シリーズの Web 認証で URL リダイレクト機能を使用しています。クライアント 端末からの任意の Web アクセスに対し検疫画面を表示させるため、認証前に名前解決が可能な環境 となっています。

DNS サーバには特別な設定が必要ないため本ガイドでは設定方法の記載を省いています。構築時 はクライアント端末から名前解決が成功することを確認してください。

4.3.4 DHCP サーバの設定

本構築例では DHCP を使用してクライアント端末に IP アドレスを配布しています。そのためクラ イアントが所属する各 VLAN (VLAN10,30,100) に対して DHCP サーバでプールを作成して下さい。 本ガイドでは以下の様に設定しています。

| VLAN | プール名 | ネットワーク | リース期間 | デフォルトルータ | DNS サーバ |
|----------|---------|------------------|-------|-----------------|-----------|
| 認証前 VLAN | VLAN10 | 192.168.10.0/24 | 8日 | 192.168.10.254 | 10.50.0.1 |
| 学生用 VLAN | VLAN30 | 192.168.30.0/24 | 8日 | 192.168.30.254 | 10.50.0.1 |
| 講師用 VLAN | VLAN100 | 192.168.100.0/24 | 8日 | 192.168.100.254 | 10.50.0.1 |

表 4.3-1 DHCP サーバの設定

4.3.5 ネットワーク接続認証設定

本ガイドで構築する検疫ネットワーク構成図について、NOSiDE構成管理サブシステム(管理)の 設定方法を示します。

- ・以下に示す設定項目以外は「NOSiDE Inventory Sub System 検疫環境構築手順書 v1.19 対応版」 にて設定済みであるものとします。
 - VLAN 割り当て機能の有効化
 - 認証スイッチ設定
 - サブネット別認証スイッチ設定
 - VLAN 割り当て

①ログオン

NOSiDE 構成管理サブシステムにシステム管理者としてログオンする。 (インストール時に設定した管理者のログオン ID でログオンしてください。)



図 4.3-1 NOSiDE 設定画面 1

②VLAN 割り当て機能の有効化

ログオン後「企業情報管理」→「ネットワーク接続認証管理」→「RADIUS サーバー設定」を開き VLAN 割り当て機能を有効にして下さい。

| NOSĪDI | [®] PC 構成管 | 理サブシステ <i>」</i> | | | 所属: 氏名:インス | と体管理 に、トール時に作成されたシフ 集計用ページへ ロ | トレビス (F) |
|------------------------------------|------------------------------------|---------------------------|------------------------------|-----------------------------|-----------------------|-------------------------------------|--|
| | 管理企業の設定 | システム管理者の | 設定 共通セキュリティ | 青報の設定 エージェン | ト情報管理 ネットワーク | 安統認証管理 システム | ム環境設定 |
| RADIU | Sサーバー設定 | | | | | | A |
| VLAN割り当て機構 ※ネットワーク接続 RADIUSt | 巻: ◎有効 ◎無効 器証機能を有効にして ナーバー ▲ |) いる企業が複数ある: サービス状態 | 場合は、VLAN割り当て機能 セキュリティチェック | 乾有効にできません。 PolicyTimeout | DefaultVLANType | 表示件数 <mark>10</mark> DefaultVLAN | |
| 全選択 全解除 | 削除 追加 | サービス再起動 | 有効 💌 一括設定 | | | | |
| | 売認証管理メインへ メインへ へ | | | Convright(c) 2002- | 2000 NTT DATA Corp. 1 | NTT DATA INTELLI | |

図 4.3-2 NOSiDE 設定画面 2

③認証スイッチ設定

管理画面にログオン後、「管理企業の選択」画面にて作成した対象の企業を選択する。 「ネットワーク接続認証管理」→「認証スイッチ設定」→「認証スイッチ追加」をクリックし、 下記6項目を設定する。

- ・IPアドレス:認証スイッチにて「Web認証専用IPアドレス」として定義した IPアドレス。(本ガイドでは 10.10.10 を設定しています。)
- ・プロトコル:「HTTP」を選択。
- ポート:80を入力。
- ・認証スイッチ種別:「AlaxalA (AX2430S)」を選択。
- ・リクエストタイムアウト:60秒(目安値です。環境に応じて変更して下さい)

・説明:任意

| 🚰 認証スイッチ設定 - Microsoft Internet Explorer | | | | |
|--|------------------|---|---|---------------------------------|
| ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H) | | | | A. |
| 🔾 戻る 🔹 🗇 💌 😰 🏠 🔎 検索 🧙 お気に入り 🤣 🍰 🍉 🔹 | | | | |
| アドレス(D) 🗃 http://localhost/PCInventoryManage/NASWConfig.aspx | | | | 💌 🔁 移動 リンク 🌺 |
| NOSIDE [®] PC 構成管理サブシステム | | | 所属:システム管理 氏名:インストール時 (集計用イ | 者 に作成されたシステム管理者 ページへ ログオフ |
| | ユーザー情報管 | 理 市販ソフトウェア情報管 資産管理 エージェント | 理 ハードウェア情報管理 集計情報管 - 情報管理 ネットワーク接続認証管理 | 理 セキュリティ情報管理 環境設定 お問い合わせ |
| 認証スイッチ設定 | | | | ^ |
| 調に バッチが 調にスイッチグループを使 サブネット別の語 | Eスイッチ設定 | | | |
| フィルタ: AlaxalA(AX2430S) 💽 | | | | 表示件数 10 💌 |
| IPアドレス ▲ プロトコル ポート | 認証スイッチ種別 | ሀሳ፲スト タイムアウト | 説明 | |
| 10.10.10.10.00 Phttp 80 | AlaxalA(AX2430S) | 60秒 | | 更新 キャンセル |
| 全選択 全解除 認証スイッチ削除 認証スイッチ追加 | | | | 1件 |
| | | | | 1 |
| ■ 「「「」」 ● 「「」、 ● 「」、 ※ 差 公 しコードの み 更 新・ 流加し | . # # | | | |
| | | | | |
| IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII | | | | |
| | | | | |
| ◀ ネットワーク接続認証管理メインへ | | | | |
| 1974-94 | | Copyright(c) 2 | 002-2009, NTT DATA Corp., NTT DA | TA INTELLILINK Corp. |
| | | | | |
| | | | | |
| B | | | | |

図 4.3-3 NOSiDE 設定画面 3

④認証スイッチ設定確認

「更新」ボタンをクリックし、認証スイッチが登録された事を確認する。

| 語記スイッチ設定 | 語正スイッチグループ設定 | サブネット別語正スイッチ設定 | | | | |
|------------------------|--------------|----------------|------------------|-------------------------|-----|----|
| フィルタ: AlaxalA(AX2430S) | | | | | 表示件 | 10 |
| IP7ドレス 🔺 | עבאסל | ポート | 認証スイッチ種別 | ሀ クエスト タイムアウト | 說明 | |
| 10.10.10.10 | http | 80 | AlaxaIA(AX2430S) | 60 秒 | | 編集 |
| 全選択 全解除 | 認証スイッチ削除 | 認証スイッチ追加 | | | | 1 |
| | | | | | | |

図 4.3-4 NOSiDE 設定画面 4

⑤サブネット別認証スイッチ設定

「サブネット別認証スイッチ設定」タブを選択して「手動追加」をクリックし、下記の項目を設定 する。

なお本構成では3つのサブネット別認証スイッチ設定を行います。

1. 認証前 VLAN

・サブネットアドレス:認証前 VLAN のネットワークアドレス。(本ガイドでは 192.168.10.0/24)

- ・サブネットマスク:認証前 VLAN のサブネットマスク。(本ガイドでは 255.255.255.0)
- ・認証スイッチの選択:③にて登録した認証スイッチにチェックする。
- ・ログオン時の認証処理:「実行する」を選択。拡張処理に「IP 再取得」を選択。
- ・ログアウト時の認証処理:「実行しない」を選択。拡張処理は「なにもしない」を選択。
- · 説明:任意

| 🚳 サブネット別認証スイッチ設定 | - Microsoft | Internet Explorer | | | | |
|---|--------------|---------------------------|---------------------|------------------|-----------|----------|
| NOS DE 1972 | ネット別認調 | 証スイッチ設定/ | 192.168.10. | 0 | | <u> </u> |
| サブネットアドレス: 192 サブネットマスク: <mark>255</mark> | 168 255 | 10 0 255 0 B | 如: <mark>認証前</mark> | | | |
| ■ 802.1x認証を行う ■ すべてのWEB認証スイ ッ : | チヘリクエストを | fī þ | | | | |
| 認証スイッチ | 認証スイ | ッチグループ | | | | |
| フィルタ: 全ての認証スイ | (ッチ | • | | | 表示件数 10 💽 | |
| IPアドレス | • | プロトコル | ボート | 認証スイッチ種別 | 説明 | |
| ☑ 10.10.10.10 | | http | 80 | AlaxalA(AX2430S) | | |
| 全選択 全解除 | | | | | 1件 | |
| | | | | | 1 | |
| 2011年1月1日 | 認証処理 そ行する | · 拉張処理 · IP再取得 · | 1 | | | |
| 接続ポリシーNG(ログアウト) | 見行しない 🔤 | • なにもしない • | I | | | |
| | | 更新 | キャ | ンセル | | |
| | | | | | | |
| | | | | | | |
| é | | | | | | |

図 4.3-5 NOSiDE 設定画面 5

⑥その他のサブネット認証スイッチ設定

残りの2つのサブネット別認証スイッチ設定を同じ手順で行ってください。

2. 学生用 VLAN

- ・サブネットアドレス:学生用 VLAN のネットワークアドレス。
- ・サブネットマスク:学生用 VLAN のサブネットマスク。
- 認証スイッチの選択:③にて登録した認証スイッチにチェックする。
- ログオン時の認証処理:「実行しない」を選択。拡張処理に「何もしない」を選択。
- ・ログアウト時の認証処理:「実行する」を選択。拡張処理は「IP 再取得」を選択。
- **説明**:任意

3. 講師用 VLAN

- ・サブネットアドレス:講師用 VLAN のネットワークアドレス。
- ・サブネットマスク:講師用 VLAN のサブネットマスク。
- ・認証スイッチの選択:③にて登録した認証スイッチにチェックする。
- ・ログオン時の認証処理:「実行しない」を選択。拡張処理に「何もしない」を選択。
- ・ログアウト時の認証処理:「実行する」を選択。拡張処理は「IP 再取得」を選択。
- 説明:任意

⑦サブネット別認証スイッチ設定の確認

「更新」ボタンをクリックし、サブネット別認証スイッチが登録された事を確認する。

| 語正スイッチ設 | 定 1 | 福正スイッチ | ビグループ設定 | 艺 | 尽 | ット別語語アスイット | 冠定 | | | | | | | |
|---------------|---------------|------------|-------------|------|----|----------------------|-------------------|--------------|-----------|----------|--------------|-----------|---------------|---|
| | | | | | | | | | | | | 3 | 長示件数 10 | |
| サブネットアドレス | サブネットマスク | 登録マシ ン数 | WEB | 2.4 | አተ | °£ | WEB認証スイッチ グループ | 802.1x認 証 | 説明 | ログオ ン | ログオン拡 張動作 | עקם קר | ログアウト拡 張動作 | |
| 192.168.10.0 | 255.255.255.0 | 1 | 10.10.10.10 | http | 80 | AlaxalA (AX2430S) | | | 認証 前 | 0 | IP再取得 | - | - | |
| 192.168.100.0 | 255.255.255.0 | 0 | 10.10.10.10 | http | 80 | AlaxalA (AX2430S) | | | グルー プ1 | - | - | 0 | IP再取得 | |
| 192.168.30.0 | 255.255.255.0 | 0 | 10.10.10.10 | http | 80 | AlaxalA (AX2430S) | | | グルー プ2 | - | - | 0 | IP再取得 | |
| | サブネット設定削 | 手编highn | 登録マシン情報から | | | | | | | | | | | 2 |

図 4.3-6 NOSiDE 設定画面 6

⑧VLAN 設定

ここでは検疫を行うユーザーごとに所属する VLAN の VLAN-ID を設定します。 「ネットワーク接続認証管理画面」に戻り「VLAN 設定」をクリック「VLAN 設定画面」の左側「ク ライアント別設定」をクリックして設定画面を開きます。

(ここではデフォルト VLAN 設定の VLANID を "0"に設定しています。)

| 叠 VLAN設定 - Microsoft Internet Explorer | |
|---|---|
| ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルブ(H) | A. |
| ③ 戻る ▼ ④ ▼ 📓 🐔 🔎 検索 ☆ お気に入り 🤣 🍰 ♥ | |
| アドレス(D) 💩 http://localhost/PCInventoryManage/VLan.aspx | _ ▶ 移動 リンク ≫ |
| NOSIDE [®] PC 構成管理サブシステム | 所属:システム管理者 氏名:インストール時に作成されたシステム管理者 集計用ページへ ログオフ |
| | 報管理 集計情報管理 セキュリティ情報管理 アーク接続認証管理 環境設定 お問い合わせ |
| VLAN設定 | A |
| | |
| VLAN試力当て ● 基本設定 ● グライアント別職定 ● カスタム設定 ■ スイッチ別設定 ■ 液素 記証入イッチ 設定 ● スイッチー覧 VLAN割り当ての基本ルー JARATEPT 2000 (Late 4) ● Machine 1000 (Late 4) <td< th=""><td></td></td<> | |
| ← トラフスージス Copyright(c) 2002-2009, NTT DA | TA Corp., NTT DATA INTELLILINK Corp. |
| | |

図 4.3-7 NOSiDE 設定画面 7

⑨VLAN-ID の設定

クライアントの所属するグループごとにそれぞれ「認証前」と「認証後」の VLAN-ID を設定して ください。該当のグループにチェックして右の「編集」ボタンをクリックする。 (本ガイドでは以下の様に設定しています。)

| | クルーフ名 | 認証前の VLAN-ID | 総証後の VLAN-ID |
|----------|----------|--------------|--------------|
| 字生用 VLAN | Students | 0 | 30 |
| 講師用 VLAN | Teachers | 0 | 100 |

表 4.3-2 VLAN 設定

| ルート | | | | |
|-------------------|------|-----|-----|----------|
| 対象 | 情報 | 認証前 | 認証後 | |
| 💁 Students | | 0 | 30 | 更新 キャンセル |
| 💁 Teachers | | 0 | 100 | |
| 一括設定: ● 認証前 ● 認証後 | Pro- | 夷行 | | |

図 4.3-8 NOSiDE 設定画面 8

※Web 認証(ダイナミック VLAN モード)の NOSiDE 検疫システムの連携では認証前の VLAN-ID は使用しません。そのため本ガイドでは VLAN-ID に"0"を設定しています。

⑩スイッチー覧設定

次に VLAN 割り当てを適応する認証スイッチの定義を行います。

VLAN 設定画面左側の「スイッチー覧」をクリックして開き、画面真ん中の「追加」をクリックします。「NAS IP」には認証スイッチの「NAS IP アドレス」を入力して右の「更新」ボタンで登録してください。(本ガイドでは以下の様に設定しています。)

- AX2430S シリーズ: 172.16.0.11
- AX1240S シリーズ: 192.168.10.12

※なおAXシリーズごとにNAS IPアドレスに使用する値が違います。本設定時は 7.1.2Nas-Ip-Addressの設定に関してを必ず参照してください。

| 🖉 VLAN設定 - Microsoft Internet | Explorer | | | - D × |
|--|------------------------|---------------------------|---|--|
| | に入り(A) ツール(T) ヘルプ(H) | | | |
| 🔇 戻る 🔹 🕥 🖌 👔 🚷 🔎 t | 🏚 🧙 お気に入り 🥝 🍰 💂 | - | | |
| アドレス(D) 🙋 http://localhost/PCInve | entoryManage/VLan.aspx | | | 予移動 リンク ※ |
| NOSĪDE® PO | 構成管理サブシステム | 市販ソフトウェア情報管理 ハードウ | 所属:システム管理者 氏名:インストール時に作取 集計用ページ ウェア情報管理 集計情報管理 t | ばなれたシステム管理者 ログオフ ア マ ログオフ マ オ コリティ情報管理 |
| | | 資産管理 エージェント情報管理 | ネットワーク接続認証管理 環境 | 設定お問い合わせ |
| VLAN設定 | | | | ^ |
| ን በ ለህምሥ ሥፖ | ∎.chattask | 参照 () 法) () 果) | <u>à</u> | |
| VENNED E | | | | |
| ■ 基本設定 | 1974-L D3-48-00 | » | 18.36 | 表示件数 200 🔽 |
| ⇒ カスタム設定 | NAS II | P Devezal | 调 伤 | 再新 キャンセット |
| □ スイッチ別設定 | 1 1021601012 | AV19405 | , | |
| ●検索 | 1 192.100.10.12 | HA12400 | | |
| 認証スイッチ設定 | | | | |
| スイッチー覧 | | | | |
| ネットワークに配置された VLAN制御対象の認証機 器を定義します。ここで定 業されたNAS-IPを持つ機器からの RADIUS認証に対し、VLAN層性 値を返却します。 | | | | |
| ◀◀ ネットワーク接続認証管 ◀◀ トップページへ | 理 メインへ | Copyright(c) 2002–2009, N | TT DATA Corp., NTT DATA I | NTELLILINK Corp. |
| E | | | | イントラネット // |

図 4.3-9 NOSiDE 設定画面 9

①設定確認

最後にすべての認証スイッチが登録できたことを確認します。設定は以上です。

| 🖉 VLAN設定 - Microsoft Internet | Explorer | | - 🗆 × |
|--------------------------------------|--|---|---|
| ファイル(<u>E</u>) 編集(E) 表示(⊻) お気(2 | こ入り(A) ツール(T) ヘルプ(H) | | |
| 🔇 戻る 🔹 🕥 🔺 📓 🐔 🔎 検討 | 索 👷 お気に入り 🕢 🍰 🍡 🔄 | • | |
| アドレス(D) (参) http://localhost/PCInven | toryManage/VLan.aspx | ء 🔁 🖈 | 多動 リンク >> |
| NOSIDE" PC 7 | 構成管理サブシステム | 所属:システム管理者 氏名:インストール特に作成されたシス: 集計用ページへ ロー | テム管理者 グオフ 44 40 66 78 |
| | | コ版ソフトウェア情報管理 ハートウェア情報管理 集計情報管理 2キュウテ・ 8産管理 エージェント情報管理 ネットワーク接続認証管理 環境設定 お得 | 明報管理 |
| VLAN設定 | | | |
| | | | |
| VLAN割り当て | ■∰インポート | 参照 ♀追加 ● 置換 | |
| ■ 基本設定 | ₴ <mark>₮</mark> ₽₽₮₭₽₣ ₮ ₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽ | 表示件数 | 200 - |
| ■ クライアント別設定 | NAS IP 🔺 | 備考 | |
| ⇒ カ人タム設定 ■ スイッチ別設定 | □ 172.16.0.11 | AX2430S | 編集 |
| | □ 192.168.10.12 | AX1240S | 編集 |
| 認証スイッチ設定 | 全選択 全解除 | 追加 削除 | |
| ローフィッチー教 | | | |
| | | | |
| (i) ネットワークに配置された VLAN制御対象の認証機 | | | |
| 器を定義します。ここで定 義されたNAS-IPを持つ機器からの | | | |
| RADIUS認証に対し、VLAN属性 値を返却します。 | | | |
| | | | |
| | 242A | | |
| | | Copyright(c) 2002–2009, NTT DATA Corp., NTT DATA INTELLILI | NK Corp. |
| é | | | 7ħ //. |

図 4.3-10 NOSiDE 設定画面 10

4.3.6 検疫除外端末の設定

検疫除外端末の設定は3.3.6検疫除外端末の設定を参照してください。



エージェント方式(Web ブラウザのみで検疫を実行します) エージェントレス方式(専用ソフトをインストールすることにより検疫の自動化ができます)

5.1 エージェントレス方式の設定

エージェントレス方式の場合、事前に行う設定はありません。直接検疫サーバに接続してブラウザ から ActiveX をインストールすることで検疫と認証を実行できます。以下に検疫と認証の実行手順を 示します。

①検疫画面の表示

認証スイッチ配下にクライアント端末を接続する。ブラウザを起動して任意のアドレスにHTTPア クセスする。(ここでは<u>http://www.alaxala.com</u>にアクセスしています。)

| 🏉 空白のページ - Windows Internet Explorer | |
|--------------------------------------|---------------------------------------|
| http://www.alaxala.com | X Live Search |
| ファイル(F) 編 | |
| 🔆 🎄 👰 空白のページ | · · · · · · · · · · · · · · · · · · · |
| | |
| | |
| | |

図 5.1-1 エージェントレス設定1

※通常ブラウザのホームページが登録されていればそのアドレスにアクセスします。

②ログオン

DNS の名前解決が完了すれば HTTP アクセスはリダイレクトされ以下の検疫画面が自動的に表示 されます。ログオン ID とパスワードを入力して「ログオン」ボタンをクリックしてください。

| | x |
|---|------|
| کې ک | • |
| ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(I) ヘルプ(H) | |
| 👷 🎄 🌈 NOSIDE(R) PC構成管理サブシステム~ログオン 🍡 🖓 🔻 🔝 🔹 🎂 ページ(P) 🔻 🍈 ツール(Q) 🤨 | • » |
| NOSIDE [®] PC 構成管理サブシステム | ^ |
| | |
| ジョン 認証情報を入力してください | н |
| ログオンID: パスワード: | |
| ログオン | |
| | - |
| ページが表示されました ● インターネット 保護モード: 無効 🔍 100% ・ | • ,4 |

図 5.1-2 エージェントレス設定 2

③ActiveX のダウンロード

ログオンに成功したら以下のような PC 構成管理サブシステムにログオンします。画面上段の赤枠 をクリックして ActiveX のインストールを開始してください。赤枠が表示されない場合はブラウザに て ActiveX コントロールの許可設定を行ってください。

| 🖉 http://noside.example.co.jp/PCInventory/main.aspx - Windows Internet Explorer | | | | | | |
|---|--|---|--|--|--|--|
| 💽 🕞 🗢 🛃 http://noside.example.co.jp/PCInventory/main.aspx 🔹 47 🗙 Live Search | | | | | | |
| ファイル(E) 編集(E) 表示(V) お気に | ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(I) ヘルプ(出) | | | | | |
| 😭 🎄 🌈 http://noside.example.co | .jp/PCInventory/m | | 島 ▼ 📴 ページ(E) ▼ 🍈 ツール(<u>0</u>) ▼ " | | | |
| 🦁 このサイトには、'NTT DATA INTELLI | LINK CORP.' からのソフ | 7トウェアが必要な可能性があります。インストールするにに | t、ここをクリックしてください × | | | |
| | 成管理サブシステ | - <u>人</u> (集計用ページ 調: 2018/22.11-51-51: 8h/CE19は、1:5 F (7):0:544 | 所属:Students 氏名:user100 へ パスワードの変更 ログオフ | | | |
| いたい日 マンノ豆取 ホットワージ付加元 木口 | (用フリビノス ノアリル豆) | ■ 玉田が何のインノ 動川FBR圧 10101/101/12 | ^ | | | |
| | | | | | | |
| | 説明 | システムに関する説明わよび設定方法 | | | | |
| | マシン登録 | ActiveXを利用しPCの構成情報を取得し登録を行います。 | | | | |
| | ネットワーク接続 | 構成情報をキーにネットワーク接続の為の認証を行います。 | | | | |
| | 未使用ライセンス | 未使用ライセンスの登録を行います。 | | | | |
| | ファイル登録 | エージェントから出力したPC構成情報ファイルで登録を行います。 | | | | |
| | 登録済みマシン | 登録済みマシンの参照と編集・削除・移動を行います。 | | | | |
| | 動作設定 | クライアントマシンの動作設定を行います。 | | | | |
| | お問い合わせ | ご意見・ご要望をご記入ください。 | | | | |
| | | | | | | |
| ۲ | | 😝 インターネット 保護モー | ド:無効 🔍 100% 👻 | | | |

図 5.1-3 エージェントレス設定3

④ActiveX のインストール

「はい」をクリックして NOSiDE 関連の ActiveX をインストールしてください。



図 5.1-4 エージェントレス設定 4



図 5.1-5 エージェントレス設定 5

※なお ActiveX のダウンロードは初回のみで次回以降ダウンロードの必要はありません。

⑤検疫の実施

PC構成管理サブシステムのメインメニューに戻り、「ネットワーク接続」をクリックします。するとクライアント端末の検疫が開始されます。

| NOSĪDE [®] pol | 構成管理サブシステ | 集計用ページへ)パスワー | ////al:stu 氏名:use ードの変更 ログオ: |
|-------------------------|----------------|---------------------------------|------------------------------------|
| 月 マシン登録 ネットワーク接続 | 未使用ライセンス ファイル登 | 録 登録済みマシン 動作設定 お問い合わせ | |
| ~ | | | |
| (| | | |
| | 説明 | システムに関する説明および設定方法 | |
| | マシン登録 | ActiveXを利用しPCの構成情報を取得し登録を行います。 | |
| | ネットワーク接続 | 構成情報をキーにネットワーク接続の為の認証を行います。 | |
| | 未使用ライセンス | 未使用ライセンスの登録を行います。 | |
| | ファイル登録 | エージェントから出力したPC構成情報ファイルで登録を行います。 | |
| | 登録済みマシン | 登録済みマシンの参照と編集・削除・移動を行います。 | |
| | 動作設定 | クライアントマシンの動作設定を行います。 | |
| | お問い合わせ | ご意見・ご要望をご記入ください。 | |
| | | | |
| | | | |

図 5.1-6 エージェントレス設定6

※初回接続時は通常「マシン登録」を行ってから「ネットワーク接続」を実施してください。マシン登録の手順に関しては「NOSiDE Inventory Sub System (操作画面) v1.19 対応版」を参照してください。

⑥Web 認証の完了

検疫に成功したクライアント端末では自動的に Web が開始されます。Web 認証に成功した場合以下の画面赤枠のメッセージが表示され認証スイッチによる通信制御が解除されます。

| Attp://noside.example.co. | jp/PCInventory/main.aspx - Windo | ws Internet Explorer | A COLOR | |
|----------------------------|--|----------------------|------------------------|------------------------------------|
| 🕒 🗸 🖉 http://nosid | le.example.co.jp/PCInventory/mair | n.aspx | + + X Live Search | ۍ م |
| ファイル(E) 編集(E) 表示 | (⊻) お気に入り(<u>A</u>) ツール(I) ^ | ∨レプ <u>(</u> 且) | | |
| 😭 🍄 🌈 http://noside. | example.co.jp/PCInventory/m | | 🟠 🔹 🗟 🔹 🖶 🗮 🖓 ページ(E) 🔹 | • ② ツール(<u>0</u>) ▼ [≫] |
| NOSIDE | 。 PC 構成管理サブシステ <i>1</i> | | (集計用ページへ)(パスワードの変更 | 所属:Students 氏名:user100 |
| 説明 マシン登録 ネットワーク | 接続 未使用ライセンス ファイル登録 | 登録済みマシン 動作部 | 定 お問い合わせ | |
| - ネットワーク接続 | | | | |
| ネットワーク接続制限を解 | 除しました。 | | | |
| シセキュリティ対策 | | | | |
| 〇修正プログラム | ● 修正プログラム対応状況一覧 セキュリティ番号 | セキュリティ情報名 | 対応状況 | 判定 |
| 〇ウィルス対策ソフト | フィルタ条件に当てはまる情報はありませ/ | Vo | - ALIAN | |
| ○ファイアウォールソフト | ● ウィルス対策ソフト対応状況一覧 | | | |
| O חגפעדיס | ソフト名 | 対応状況 🥑 | | 判定 |
| 表示フィルタ: 警告と未対策 + | フィルタ条件に当てはまる情報版はありません ファイアウォールソフト対応状況一 | Uo 覧 | | |
| ▶自動車新ポパンーの復元 | ソフト名 | 対応状況 🕘 | | 判定 |
| - CIEDOC #1010 5 - 00180 E | ノイルクネイトにヨしはよる1首和見よめりません | Vo | | 1111 |
| 定義されたセキュリテ (1) | ● カスタムチェック対応状況一覧 セキュリティ情報名 | | 対応状況 | 判定 |
| I need workship | | | 😜 インターネット 保護モード: 無効 | a 100% 👻 |

図 5.1-7 エージェントレス設定7

⑦操作手順は以上です。

5.2 エージェント方式の設定

ここではクライアント端末にインストールしたエージェントに本環境用の初期設定を行う手順を 示しています。クライアント端末をエージェントレスで運用する場合は本設定は必要ありません。

① 初期設定

NOSiDEマニュアル <u>NOSiDE® Inventory Sub System (エージェント運用編)</u> を参照してインスト ールおよび接続サーバのURLやユーザID, パスワードなど検疫サーバへの接続に必要な設定を実施し てください。

② PC 起動時に自動検疫するための設定

PC 起動時に自動的に検疫を実施して接続可能とするため以下を設定することを推奨します。 エージェントを起動して「PC 構成管理サブシステムのプロパティ」の左メニューの「スケジュー ル」をクリックし「タスクのスケジュール」の項目を「ログオン時」に変更します。検疫と認証の実 施タイミングをログオン時に設定します。(本設定は環境に合わせて適切なスケジュールを選択して ください。)設定後「OK」ボタンで「PC 構成管理サブシステムのプロパティ」を閉じ、エージェン トマネージャーの画面も右上の「×」をクリックして閉じて下さい。

| MRNOSIDE(R) PC構成管理サブシ NOSIDE [®] Inventory Sub Syste | ステムのプロパティ |
|---|---|
| WINVISTA | ② エージェントを動作させるスケジュールを設定してください。 タスク名(N): NSPCInv ▼ |
| び 基本設定 認証情報 | ユーザーログオン時 タスクのスケジュール(<u>S</u>): ログオン時 |
| マイルタ ● フィルタ ● 動作設定 ● 自動更新情報 ● ○ ○ ○ ○ | |
| | _リトライ設定 回数(C): 3 三 間隔(D: 60 三 秒おき |
| | 実行する7かり/名(U): WINVISTA¥tatsuta パペスワートの設定(P) |
| | <u>OK</u> <u>キャンセル</u> 道用(<u>A)</u> |

図 5.2-1 エージェント設定 4

自動検疫のための設定を行なうと PC ログオン時に自動的に認証と検疫が開始されます。

6. 動作確認方法

6.1 AX シリーズにおける確認方法

6.1.1 show web-authentication login

認証スイッチの Web 認証の認証状態表示コマンド

検疫クライアントが AX 認証スイッチの Web 認証に成功しているか確認出来ます。

edge#2# show web-authentication login

Date 2009/04/24 16:08:56 UTC Dynamic VLAN mode total login counts(Login/Max): 1 / 256 Port roaming : Disable No F User Name Port VLAN Login time Limit 1 user100@7, k0, 1 0/3 30 2009/04/24 16:00:02 23:11:05

※上記は AX1240S の表示例となっています。

6.1.2 show web-authentication logging

認証スイッチの Web 認証の動作ログ表示コマンド(固定 VLAN モード)

検疫クライアントがいつ再認証を行ったか等を確認することが出来ます。また、認証失敗時の原因 についても確認することが出来ます。

edge#2# show web-authentication logging

Date 2009/04/24 16:09:06 UTC AUT 04/24 16:00:02 WEB No=1:NORMAL:LOGIN: MAC=0019.b97d.4bfa USER=user100@7,k0,1 IP=192.168.10.50 PORT=0/3 VLAN=30 Login succeeded. AUT 04/24 16:00:01 WEB No=264:NORMAL:SYSTEM: USER=user100@7,k0,1 IP=192.168.10.50 Received login request.

※上記は AX1240S の表示例となっています。

6.1.3 clear web-authentication auth-state

認証スイッチの Web 認証ユーザーを強制的にログアウトさせるコマンドです。 検疫クライアントを強制的にログアウトさせる場合に使用します。

ユーザ指定 clear web-authentication auth-state user <ユーザ名> 全ユーザ clear web-authentication auth-state user -all MAC アドレス指定 clear web-authentication auth-state mac-address <mac アドレス>

6.2 NOSiDE 検疫サーバでの確認

6.2.1 ネットワーク接続認証ログ

NOSiDE 検疫サーバによる認証、検疫のログを表示します。

表示方法:

NOSiDE PC 構成管理サブシステムに管理者としてログオン→「該当企業 ID を選択」→「ネット ワーク接続認証管理」をクリック→「ネットワーク接続認証ログ」をクリックする。

詳細につきましては、「NOSiDE Inventory Sub System (管理画面)v1.19 対応版」のネットワーク接続認証ログを参照して下さい。

| 🥘 X | ■ ネットワーク接続記録ログ - Microsoft Internet Explorer | | | | | | | |
|----------------------|--|-----------------------|----------------|------------------------------|---|---|----------|--------------|
| ファ | ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(D) ヘルプ(E) 🥂 | | | | | | | |
| (] I | ② 戻る • ② • ▶ 2 🖄 🔑 検索 📩 お気に入り @ 🗇 + 😓 🚍 • | | | | | | | |
| דאק | /Z@) 🧧 | http://localhost | /PCInventoryMa | mage/NAAccessLog.aspx | | | | 🔽 🄁 移動 リンク 🎽 |
| NOSIDE PC 構成管理サブシステム | | | | 所属:シス . 氏名:1ンフ | た」管理者 、トール時に作成されたシステム管理者 集計用ページへ ログオフ | | | |
| | ユーザー情報管理 市販ソフトウェア情報管理 ハードウェア情報管理 単計情報管理 セキュリティ情報管理 変変等時 コージント 情報管理 ユージント 情報管理 コーソーン に 情報管理 コーク に いたローク な の の の の の の の の | | | | | | | |
| | | ネットワー | り接続認証ロ | 1グ | | | | |
| | _ | | | | | | | |
| | アクセフ | 、結果 | ▶ 評可 ▶ : | 酒酒 🔽 エラー | | | | 🔀 表示件数 50 👤 |
| | 7クセス日時 開始 年 月 日 00 ・時 00 ・ | | 分 | | | | | |
| | 終了 年 月 日 00 • 時 00 • | | 分 | | | | | |
| | ユーザ | -名 | | | | | | |
| | マシンネ | 3 | | | | | | |
| | 参照先グループ (すべてのグループ) | | | | | | | |
| | 認証方式 | đ, | ☑ マシン識別 | 子 🗹 МАСアドレス | | | | |
| | | | | | 適用 閉じる | | | |
| | | アクセ | ス結果 | アクセス時間 👻 | ユーザージ | ፚ | マシン名 | 所属 |
| | 削除 | 許可(ユーザ) | | □ 2009/04/15 18:11:30 | プリンタ | | | Sales |
| | 削除 | <mark>拒否</mark> (その他) | | □ 2009/04/15 18:07:49 | | | | |
| | 削除 | 許可(検疫) | | □ 2009/04/15 18:04:23 | user100 | | WINVISTA | NTS |
| | 削除 | 許可(検疫) | | 2009/04/15 17:39:27 | user100 | | WINVISTA | NTS |
| | 削除 | 許可(ユーザ) | | □ 2009/04/15 17:36:06 | プリンタ | | | Sales |
| | 削除 | <mark>拒否</mark> (その他) | | 009/04/15 17:35:51 | | | | |
| | 削除 | <mark>拒否</mark> (その他) | | D 2009/04/15 17:28:59 | | | | |
| | 削除 | 許可(ユーザ) | | □ 2009/04/15 16:23:03 | プリンタ | | | Sales 🚽 |
| ^ (چ) | 2) ページが表示されました | | | | | | | |

図 6.2-1 ネットワーク接続認証ログ

7. 注意事項

本章ではAX シリーズとNOSiDE 検疫システムが連携する際の注意事項を示します。

7.1 Web 認証連携時の注意事項

7.1.1 認証スイッチ種別について

AX シリーズの各認証スイッチでは Web 認証に使用する認証ページのアドレスが現在は統一されています。NOSiDE 検疫サーバの設定では認証スイッチ種別に「AlaxalA(AX2430S)」を使用してください。

7.1.2 Nas-Ip-Address の設定に関して

ダイナミックVLANモードを使用する場合、NOSiDE検疫サーバにて認証スイッチの定義にNAS-IP (認証スイッチのIPアドレス)を設定します。設定箇所は4.3.5ネットワーク接続認証設定のVLAN 設定を参照して下さい。

AX シリーズごとに RADIUS-Request に使用する NAS-IP の値を決定する条件が異るため、本設定を行う場合注意が必要です。

条件

AX2400S: RADIUS サーバと通信するインタフェースの IP アドレスを使用します。 AX1200S: IP アドレスが登録されている VLAN インタフェースのうち、最も小さい VLAN ID の IP アドレスを使用します。

付録

(1) AX シリーズのコンフィグレーションファイル

本ガイドにて紹介した構成のコンフィグレーション例です。

「3章 システム構築例1(固定 VLAN モード)」と「4章 システム構築例2(動的 VLAN モード)」 のネットワーク構成における各装置のコンフィグレーションをテキスト形式のファイルとして本ガ イドに添付しております。(添付ファイルを抽出するには、Adobe Acrobat 5.0 以降もしくは Adobe Reader 6.0 以降が必要です。)

各コンフィグレーションについては、以下に示すファイル名と同じ名前の添付ファイルを参照下さい。

| 構築例 | 対象機器 | 装置名 | 対象ファイル |
|-------|---------|-----------------|--------------------|
| | 認証スイッチ | edge#1(AX2430S) | edge#1s_config.txt |
| | 認証スイッチ | edge#2(AX1240S) | edge#2s_config.txt |
| 構築例1 | L3 スイッチ | core#1(AX3630S) | core#1s_config.txt |
| | L3 スイッチ | core#2(AX3630S) | core#2s_config.txt |
| | L3 スイッチ | core#3(AX3630S) | core#3s_config.txt |
| | 認証スイッチ | edge#1(AX2430S) | edge#1d_config.txt |
| | 認証スイッチ | edge#2(AX1240S) | edge#2d_config.txt |
| 構築例 2 | L3 スイッチ | core#1(AX3630S) | core#1d_config.txt |
| | L3 スイッチ | core#2(AX3630S) | core#2d_config.txt |
| | L3 スイッチ | core#3(AX3630S) | core#3d_config.txt |

(2) Web 認証画面入れ替え用 HTML ファイル

本ガイド**3.2.4Web認証画面入れ替え**にて示した「login.html」を付録として添付しています。(添付ファイルを抽出するには、Adobe Acrobat 5.0 以降もしくはAdobe Reader 6.0 以降が必要です。)

| 構築例 | 対象機器 | 装置名 | 対象ファイル |
|---------------|----------|------------------------------------|------------|
| 構築例 1,2 共通 | 認証スイッチ共通 | edge#1(AX2430S) edge#2(AX1240S) | Login.html |



2009年6月29日 第2版

アラクサラネットワークス株式会社 ネットワークテクニカルサポート

〒212-0058 川崎市幸区鹿島田 890 番地 新川崎三井ビル西棟 http://www.alaxala.com/