NETAPHOR SOFTWARE, INC.

SiteAudit™
デプロイメントガイド

ユーザー用

2007 年 11 月

Pioneering Printer Asset Management

目次

製品概要

プリンタ資産の使用状況、サービス、コストを計測し、レポートするための資産管理ツール **SiteAudit** は以下の機能を提供します。

- ネットワークプリンタとローカルプリンタのインベントリ作成
- プリンタの使用状況のモニタ
- プリンタの問題検知

SiteAudit のプリンタ・データ収集、分析、レポート機能を使用することで、組織に必要なプリンタ台数などが予測できます。SiteAudit はプリンタ資産のパフォーマンスを「コスト」と「生産性」の二つの面から計測します。

> **本ガイドについて**
>
> 本ガイドは、Netaphor SiteAudit をエンタープライズ・ネットワークにデプロイ（インストール・設定）する方法を記述したものです。
>
> インストール・設定に必要なタスクの一覧は 33 ページの「チェックリスト」を参照してください。

デバイス検索

SiteAudit はネットワークをスキャンし、ネットワーク上のデバイスを検索します。検索にはデフォルトの検索条件またはユーザー指定の条件が指定できます。サブネットワークやデバイスの IP アドレスを手動で入力することも可能です。

デフォルト検索条件を用いた自動デバイス検索を行う場合、以下の動作を実行します。

- ローカルネットワークにブロードキャスト送信を行い、応答したデバイスをすべて検出します。
- SNMP および RIP に応答したルーターと各ルーターに接続されているネットワークを検出し、各ネットワークに接続されているデバイスを検索します。この手順は再帰的に実行されます。
- 既知のネットワーク上にある全 IP アドレスを個別にチェックします。これはブロードキャストに応答しないデバイスも存在するからです。この場合、各ネットワーク上で、ネットワーク番号とサブネットマスクから IP アドレスを算出します。

データ収集・分析

SiteAudit では収集したデータを Microsoft SQL Server データベースに格納します。データ分析には SQL Server 上に格納された手続きと関数を使用します。

SiteAudit のコンポーネント

SiteAudit は以下の 3 つのコンポーネントから構成されています。

- **SiteAudit Viewer**：プリンタ使用状況などのデータを表示するユーザーインターフェース
- **SiteAudit Monitor**：プリンタ検索、（プリンタ使用状況などの）データ収集、データベースへのデータ格納を実行する Microsoft Windows サービス
- **Scheduled Reports:** プリンタやコピー機のメーターの読み出し作業を自動化するユーティリティ（メーター値を定期的にメール送信し、インボイス処理を簡易化）

インストールの前に

SiteAudit をインストール・設定する前に、以下の点を決定してください。

- SiteAudit コンポーネントの配置場所
- SiteAudit を実行するハードウェア、OS、データベースサーバープラットフォーム
- SiteAudit のビューやレポート作成時における組織構造の表示方法

コンポーネントの配置場所

SiteAudit Viewer

SiteAudit Viewer は収集データ、データ分析結果を表示したいユーザーのコンピュータにインストールします。（例：資産管理、購買、プリンタを扱う IT 担当者のコンピュータ）

SiteAudit Monitor

SiteAudit Monitor サービスがインストールされているコンピュータには SiteAudit Viewer も必ずインストールされています。SiteAudit Viewer を用いて SiteAudit Monitor サービスの開始/停止、検索やデバイスの設定を行います。

動作環境（ハードウェア、Windows、SQL Server）

SiteAudit は Windows XP、Windows Server 2003、SQL 2005（SQL Server Express を含む全バージョン）に対応しています。

Netaphor では SiteAudit を利用するために必要な CPU の速度やメモリサイズを特に定めていませんが、ユーザビリティを考慮した場合、以下の値が推奨されます。ハードウエア環境は、SiteAudit でモニタするプリンタの台数に基づいて決定する必要があります。

250 台以上のプリンタが接続されているネットワーク上で SiteAudit Viewer と SiteAudit Monitor を実行する場合に推奨される CPU の速度とメモリサイズは以下の通りです。

OS	ハードウェア	SQL Server
Windows 2003 Server	• Pentium 4 3.2 GHz 以上 • RAM　4GB • HDD の空き容量　200 MB	SQL Server 2005 以降

250 台以下のプリンタが接続されているネットワーク上で SiteAudit Viewer と SiteAudit Monitor を実行する場合に推奨される CPU の速度とメモリサイズは以下の通りです。

Operating System	Hardware	SQL Server
Windows XP with SP2	• Celeron 2.8 GHz 以上 • RAM 4GB • HDD の空き容量　200 MB	SQL Server Express 2005

インストール条件

SiteAudit をインストールする前に以下の点を確認してください。

全般

旧バージョンの SiteAudit

SiteAudit がすでにインストールされている場合、データベースのバックアップを行います。旧バージョンの SiteAudit がインストールされている場合はアンインストールします。

データベースサーバー

対応するバージョンの SQL Server がネットワーク上にインストールされている場合、1)SQL Server にアクセスでき、2)　sa パスワードを持っていることを確認します。（SQL Server がインストールされていない場合は後述のインストール手順を参照してください。）

Windows サービス

直接接続されているプリンタ（USB または LPT）をリモート検索する場合、特定のサービスが無効にできないように設定する必要があります。スタートアップの種類を以下の通り設定してください。

1. Start ⇒　ファイル名を指定して実行
2. services.msc と入力し、Enter を押します。
3. スタートアップの種類を設定する各サービスについて、以下の変更を行います。
    - サービス名をダブルクリック
    - **全般**タブの**スタートアップの種類**で**自動**または**手動**を設定します。以下の表を参照してください。

サービス名	サービスが必要なコンポーネント	スタートアップの種類
COM+ Event System	SiteAudit Monitor スキャン対象の PC	サーバー：自動 ワークステーション：手動
Remote Access Auto Connection Manager	SiteAudit Monitor SiteAudit Viewer	手動
Remote Access Connection Manager	SiteAudit Monitor SiteAudit Viewer	手動

サービス名	サービスが必要なコンポーネント	スタートアップの種類
Remote Procedure Call (RPC)	SiteAudit Monitor または SiteAudit Viewer	手動
Remote Procedure Call (RPC) Locator	SiteAudit Monitor または SiteAudit Viewer	手動
Remote Registry	SiteAudit Monitor	自動
Server	SiteAudit Monitor または SiteAudit Viewer	自動
Windows Management Instrumentation	SiteAudit Monitor スキャン対象 PC	自動
Windows Management Instrumentation Driver Extensions	SiteAudit Monitor	手動
Workstation	SiteAudit Monitor または SiteAudit Viewer	自動

ホストクレデンシャル（資格情報）

直接接続されているプリンタとそのキューのホストをスキャンするためには、特定の Windows クレデンシャル（「ローカル」管理者グループのメンバであるユーザーのクレデンシャル）が必要です。Windows ドメインの一部であるホストの場合、通常ドメイン管理者グループはローカル管理者グループのメンバでもあります。その場合、ドメイン管理者グループのメンバであるユーザークレデンシャルがあれば十分です。

全ホストで同じユーザー名/パスワードが使用できる場合は SiteAudit に***\username** とパスワードをクレデンシャルとして登録するだけで、あとは SiteAudit が必要に応じて各ホスト名を置換します。これはワークグループ環境の場合に良くあるケースです。

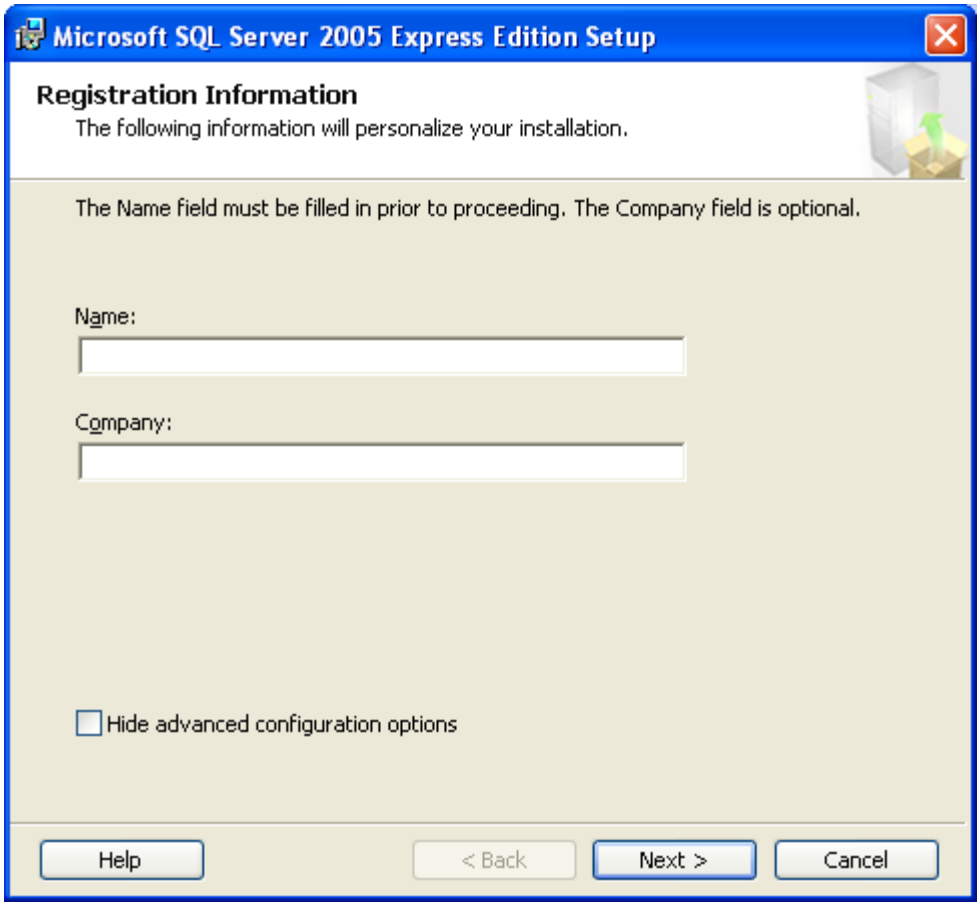
SQL Server のインストール・設定

SQL Server または SQL Server Express データベースのインストールには sa パスワードが必要です。統合セキュリティを使用する場合はデータベースに管理者レベルのアクセス権限を持つユーザーのログインクレデンシャルが必要です。

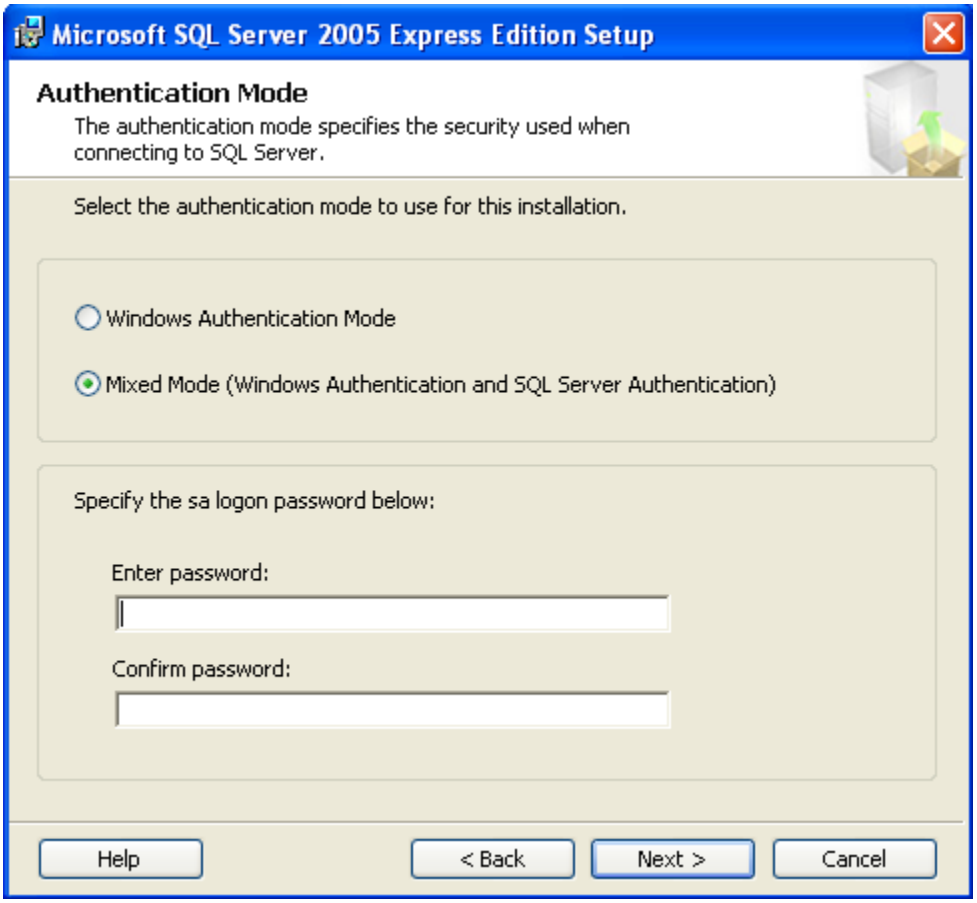
SQL Server 2005 Express

SQL Server Express のインストール手順に関しては SQL Server Express のインストール手順書を参照してください。SiteAudit を使用するためには、SQL Server Express のインストール時に以下の設定を行う必要があります。

- [登録情報]ビューで[詳細構成オプションを非表示にする]チェックボックスを非選択状態にします。



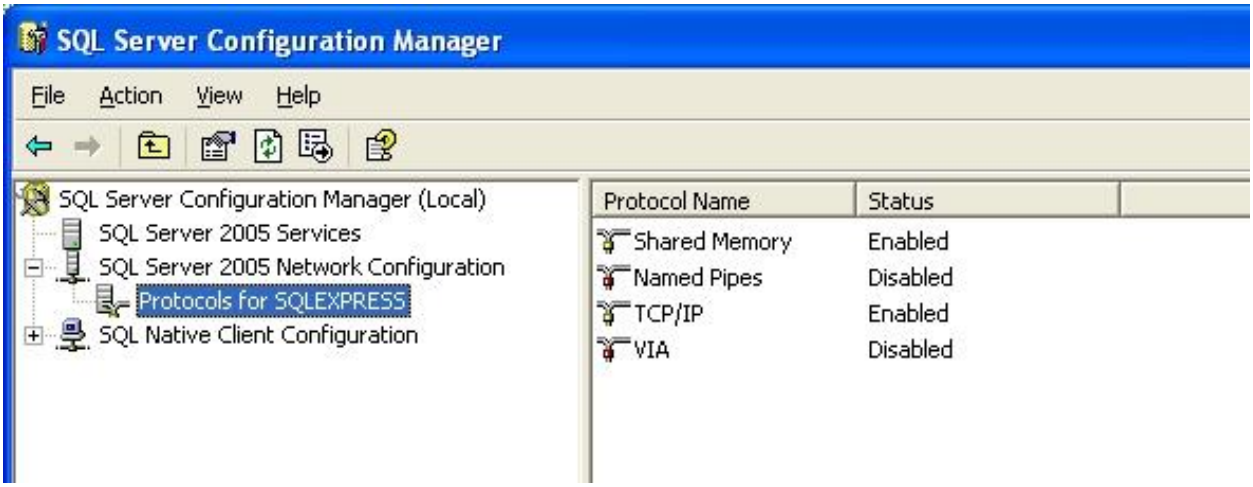
- [認証モード]ビューで[混合モード（Windows 認証と SQL Server 認証）]を選択し、sa パスワードを入力します。



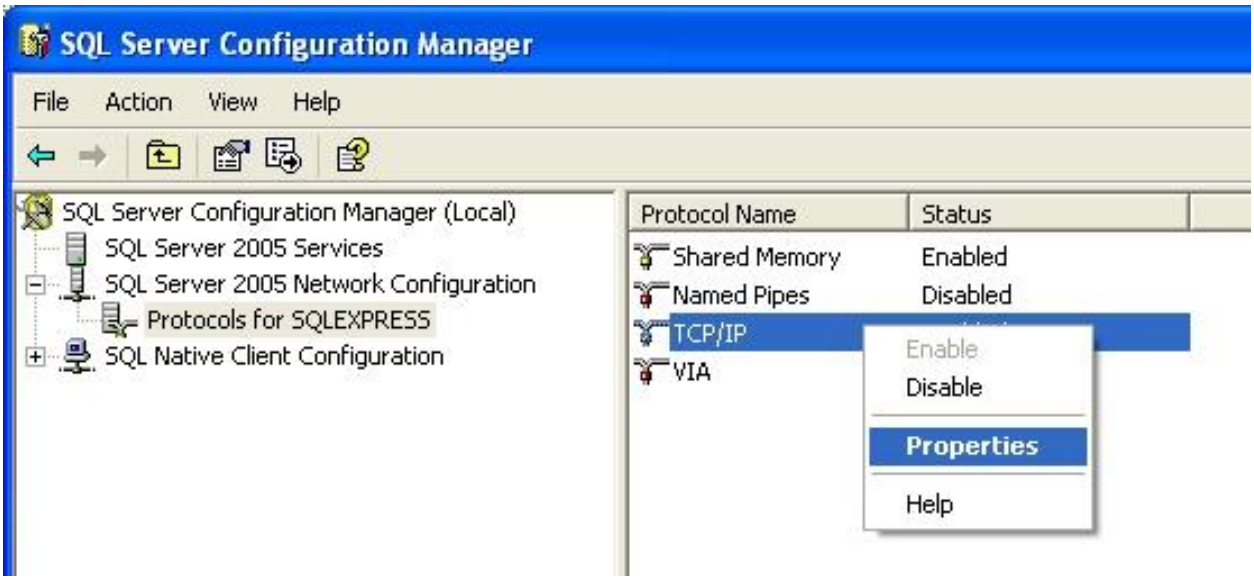
SQL Server Express は sa パスワードと TCP/IP ネットワーク接続を有効にして設定します。TCP/IP の有効化は SQL Server Express のインストール後に行います。

1. **Start ⇒ すべてのプログラム ⇒ Microsoft SQL Server 2005 ⇒ セキュリティ構成ツール ⇒ SQL Server 構成マネージャ**

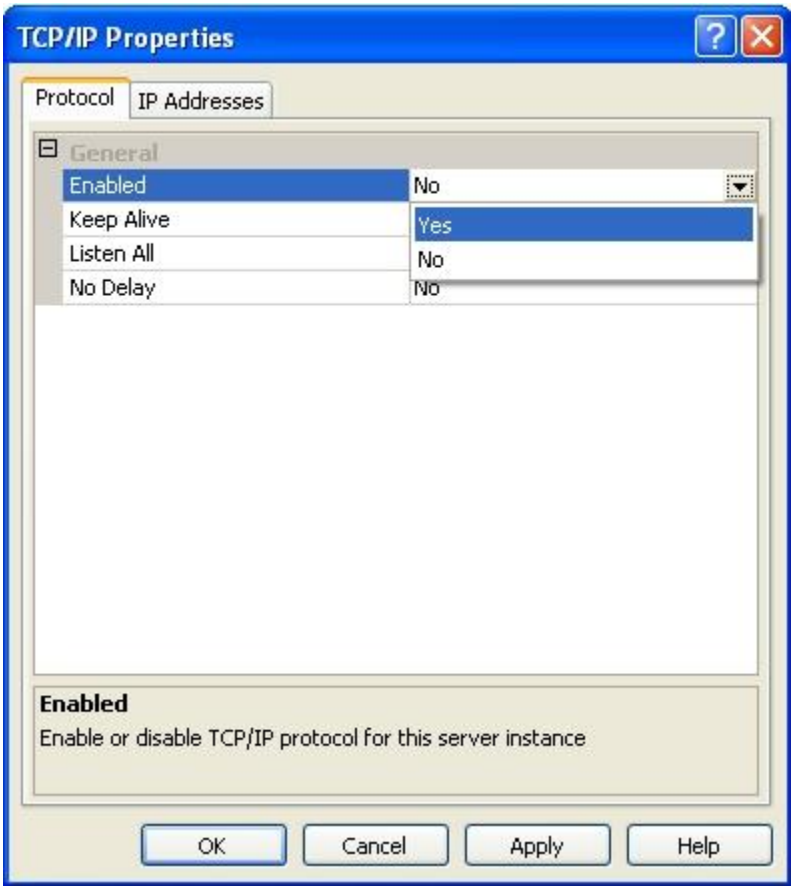
2. 左側のペインで **SQLEXPRESS のプロトコル**を選択します。



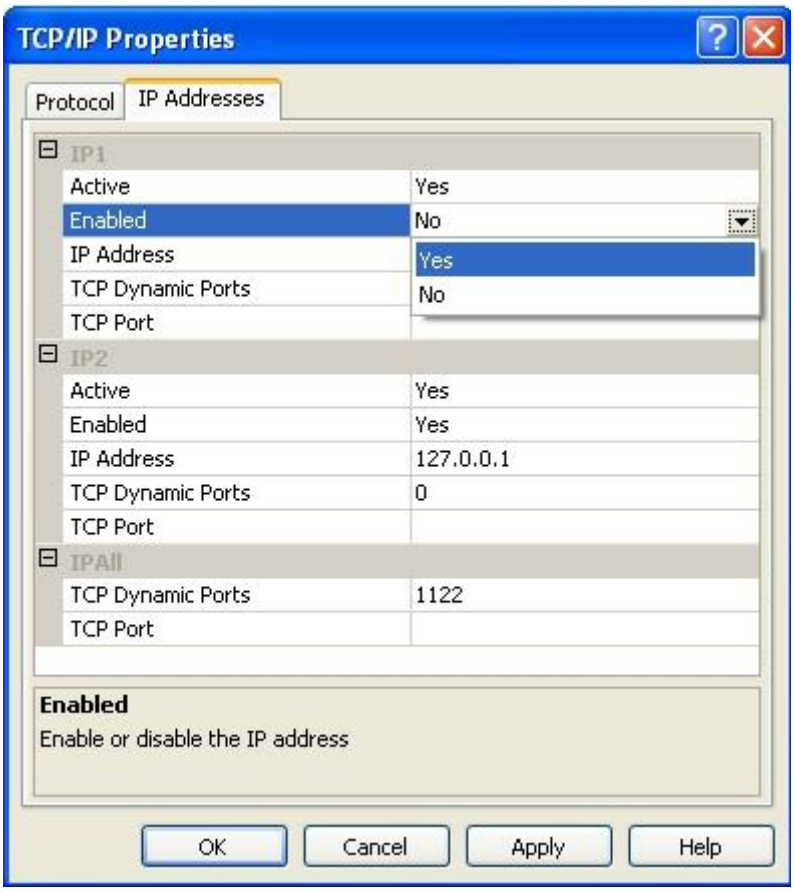
3. 右側のペインで **TCP/IP** を選択し、**プロパティ**をクリックします。



4. **[プロトコル]**タブで**有効**の欄を**はい**に設定します。



5. **[IP アドレス]**タブで、全 IP アドレスに対して**有効**の欄を**はい**に設定します。



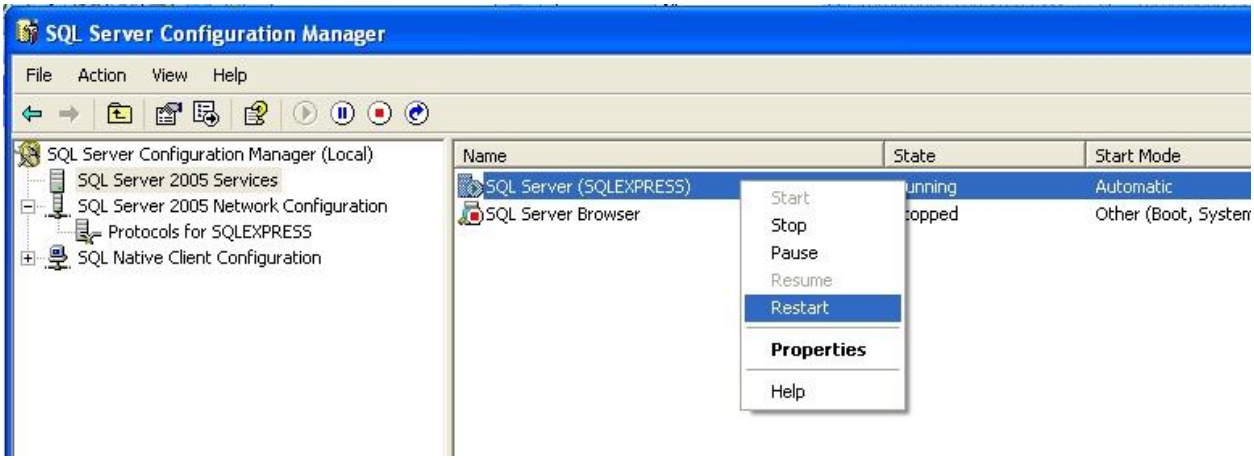
6. **適用**をクリックします。

   以下の警告が表示されます。

7. **OK** をクリックします。

8. 左側のペインで **SQL Server 2005 のサービス**をクリックします。

9. 右側のペインで **SQL Server (SQLEXPRESS)**を選択し、右クリックで**再起動**を選択します。



再起動後、SiteAudit からデータベースに接続する設定を行います。詳細は 28 ページの「データベース」の章を参照してください。

データベースのサイズ指定について

SiteAudit では SQL Server のインストールをほかのアプリケーションと共有できるため、専用のデータベースサーバーが不要です。ハードウェアおよびデータベースサーバー条件は、データベースの動作、データ収集量、使用するデータベースの数などによって異なります。このような条件は通常データベース管理者が決定します。

データ収集量は、以下のような条件によって異なります。

- モニタするプリンタ台数
- プリント量
- インシデント、通知数

必要なメモリサイズの概算には以下を目安にしてください。

アクティブ状態のプリンタ 2000 台をモニタしている場合で、4 ヶ月間のインシデント数が 22 万件にのぼる場合、1GB のメモリを使用します。1 年間ではそれが 3GB から 5GB になります。

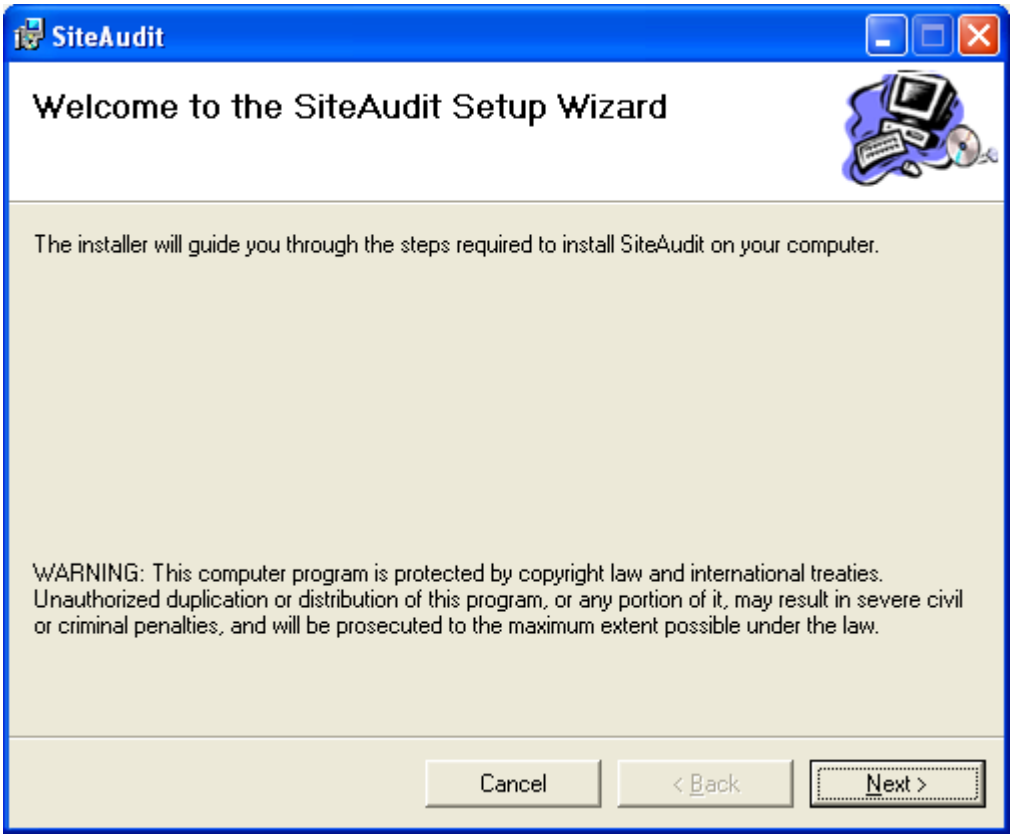
SiteAudit のインストール

SiteAudit をサーバーまたはワークステーションにインストールする場合、サービスとして動作しているローカルアカウントが必要です。

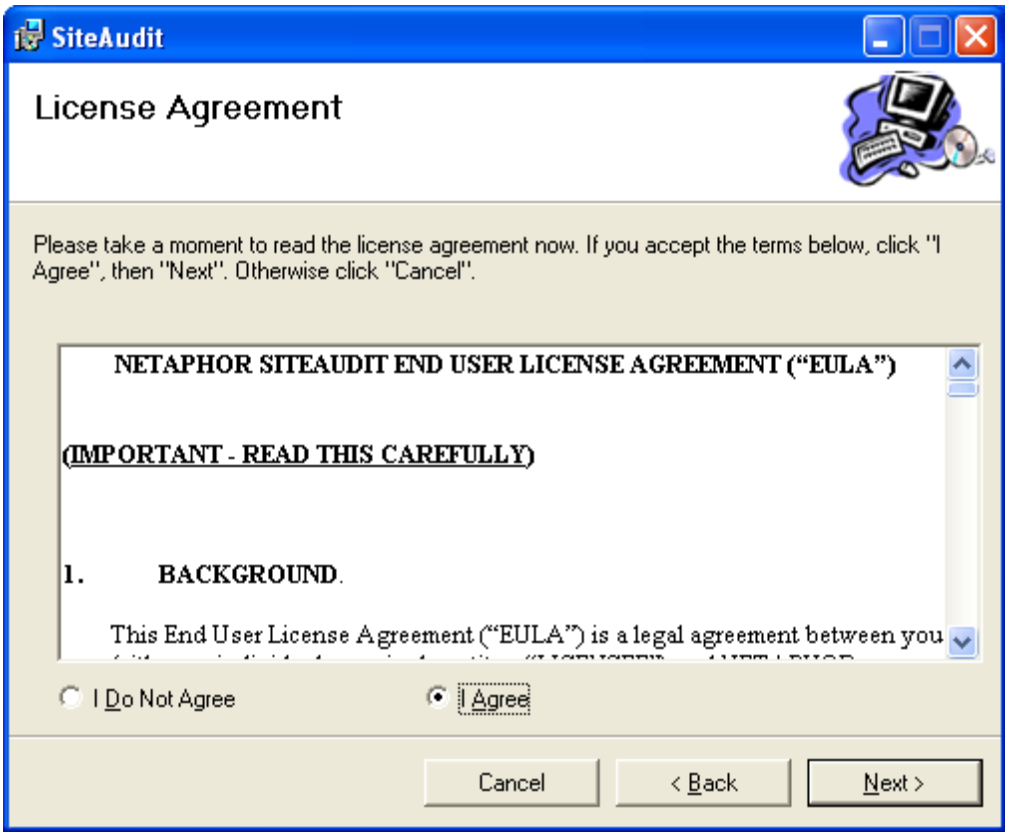
その他の Microsoft コンポーネントについて

以下の説明は、Microsoft　.NET Framework 3.5 がインストール済であることを前提としています。まだの場合は、SiteAudit のインストールを開始する前にインストールする必要があります。インストールの前に使用許諾書に同意してください。

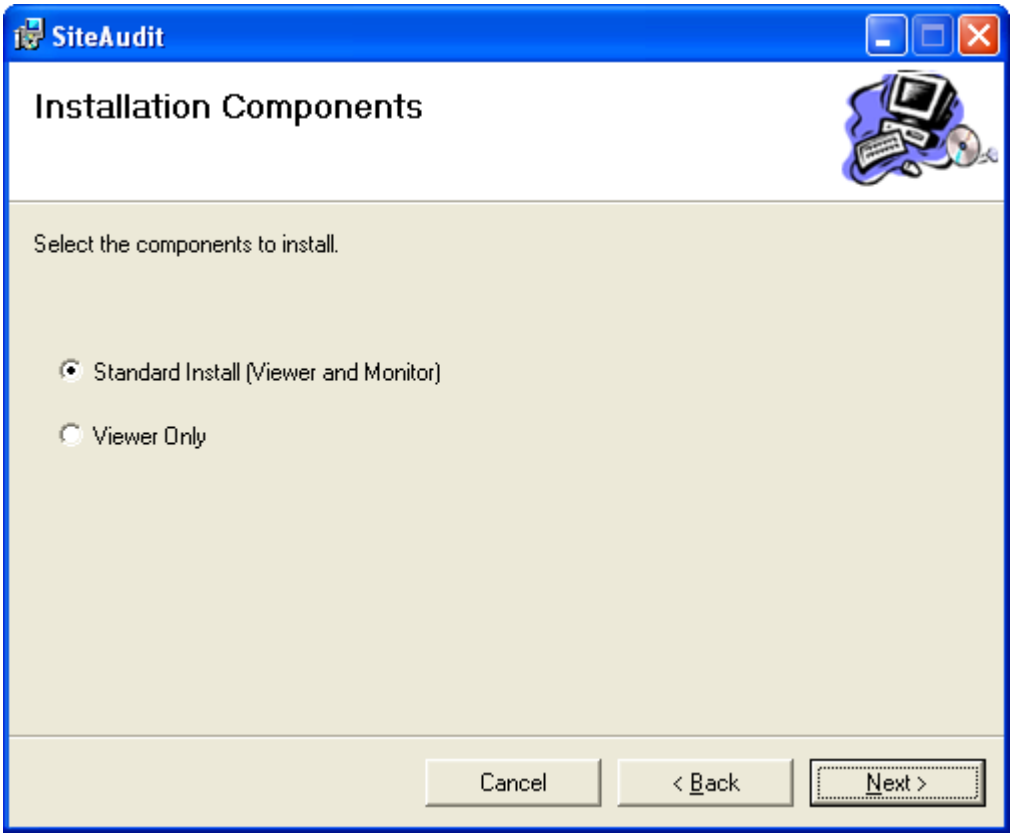
1. インストール CD から setup.exe を実行します。



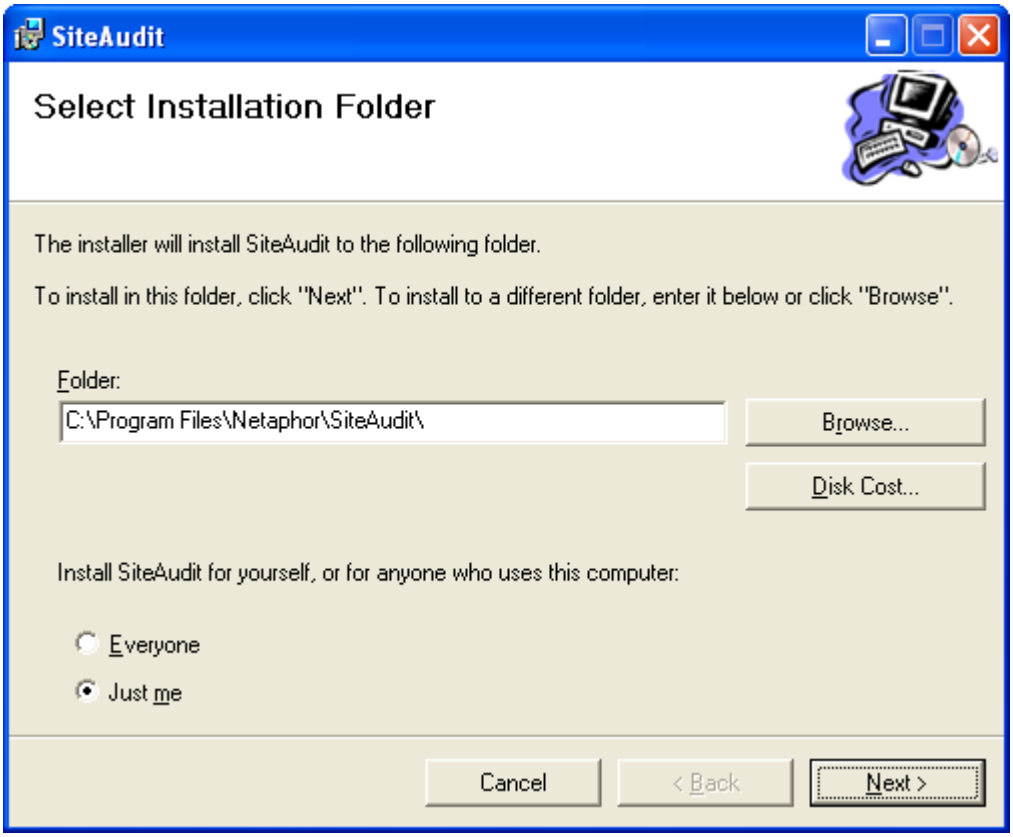
2. **次へ**をクリックします。



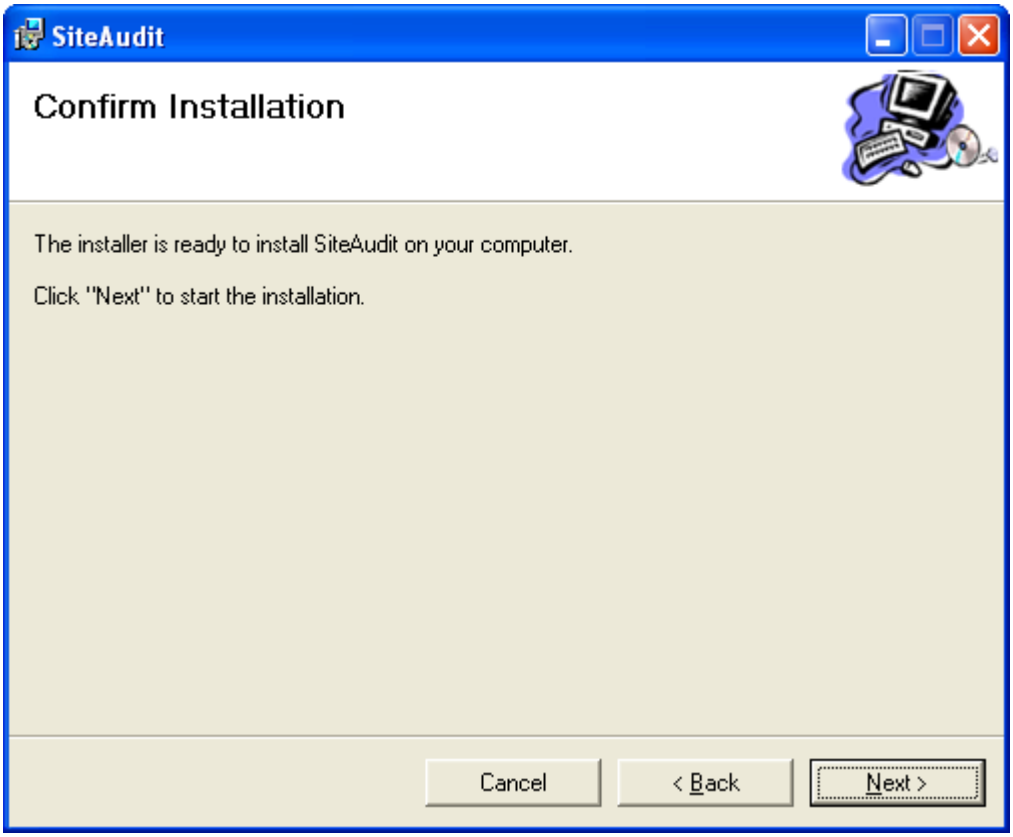
3. 使用許諾書に同意し、**次へ**をクリックします。



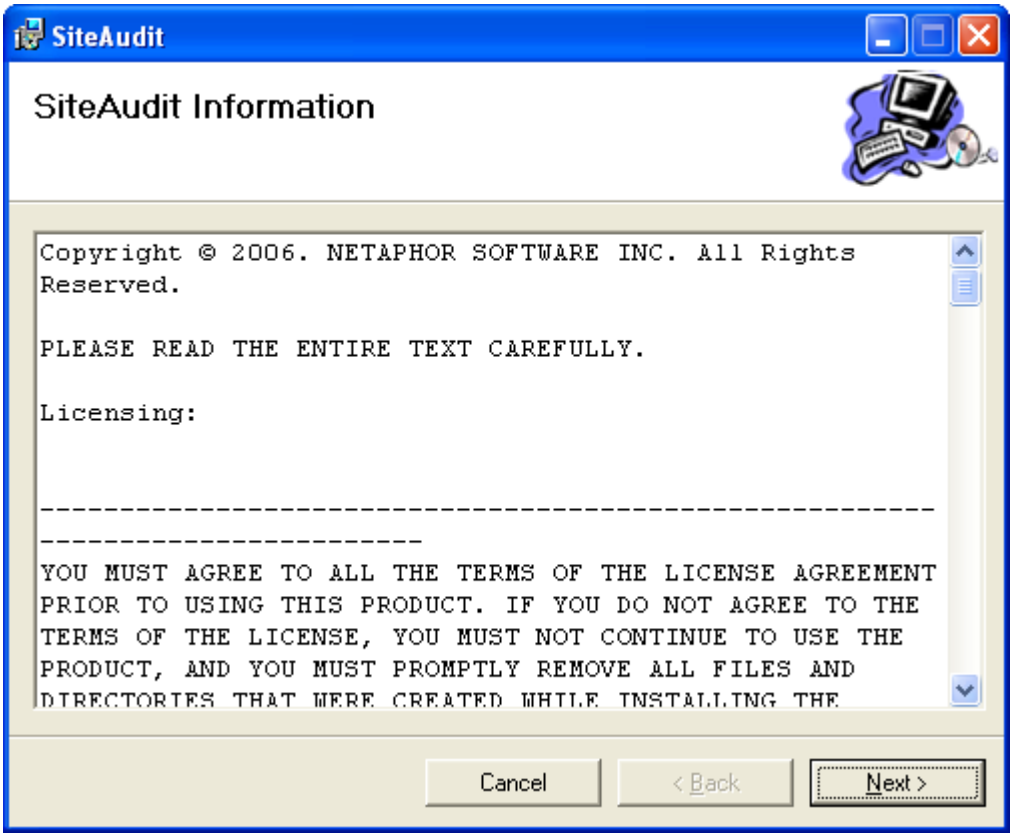
4. **標準インストール（Viewer と Monitor）**を選択し、**次へ**をクリックします。



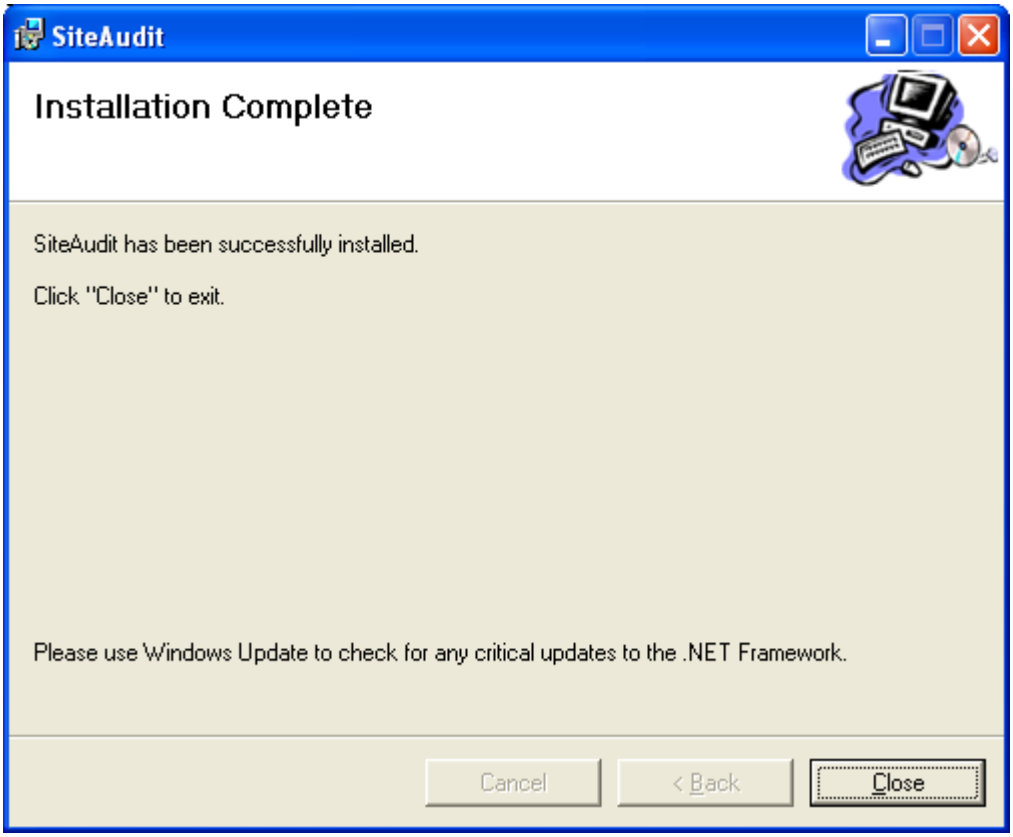
5. インストール先のフォルダと SiteAudit にアクセスするユーザーを指定し、**次へ**をクリックします。



6. **次へ**をクリックします。



7. 追加情報を読み、 **次へ**をクリックします。.



8. **閉じる**をクリックします。

SiteAudit の設定

SiteAudit のインストール終了後、**設定**メニューで以下の設定を行います。設定作業は通常一度しか行う必要がありません。

デバイス検索

SiteAudit のデバイス検索機能を設定するには **設定**メニューから**検索**を選択します。

SiteAudit ではネットワークプリンタも直接 USB または LPT ポートに接続されているプリンタ（ローカルプリンタ）も検索できます。ネットワークプリンタは一意の IP アドレスによって識別します。ローカルプリンタはホスト IP アドレスと各ホスト上で一意のデバイス ID の組み合わせで識別します。

プリンタの種類（ネットワークまたはローカル）はインベントリビュー（**ビュー⇒インベントリ**）内の**接続**コラム、または詳細情報細ビュー（**ビュー⇒詳細情報**）で確認できます。

設定⇒検索を選択すると**検索設定**ダイアログボックスが表示されます。**検索設定**ダイアログボックスは以下の 4 つのタブから構成されています。

- **ネットワーク**：SiteAudit がデバイスを検索できるネットワークの一覧を表示します。「**ネットワークを自動的に検索**」（小さいネットワークの場合に推奨）チェックボックスをチェックすると、SiteAudit が自動的にネットワークを検索します。**追加**ボタンを押してネットワークを手動で追加することも可能です。SiteAudit は一覧表示された各ネットワークに検索パケットをブロードキャスト送信します。ブロードキャスト送信先から特定のデバイスを除外するには、**デバイス**タブにネットワークのブロードキャストアドレスを追加し、デバイスの横のチェックボックスを非選択状態にします。ネットワーク上のデバイス検索を無効にするには、ネットワークの横のチェックボックスを非選択状態にします。

- **デバイス**：SiteAudit がモニタするデバイスの一覧を表示します。「**デバイスを自動的に検索・モニタ**」（推奨）チェックボックスをチェックすると、SiteAudit が自動的にデバイスを検索します。**追加**ボタンを押してデバイスを手動で追加することも可能です。デバイスの横のチェックボックスを非選択状態にすることで、デバイスのモニタリングを無効にできます。

- **ホストクレデンシャル（資格情報）**：ローカルプリンタの接続されているホストごとに、そのホストの管理者のユーザー名とパスワード情報が必要です。組織によっては、ドメイン管理者のホスト・クレデンシャルが、ネットワーク上の全ホストワークステーションの管理者クレデンシャルと同じである場合があります。その場合、ドメイン管理者のクレデンシャルのみが必要になります。SiteAudit ではホスト権限情報を暗号化して保存します。「**ローカルデバイスを検索・モニタ**」チェックボックスを非選択状態にすることで、ローカルデバイスの検索を無効にできます。

- **SNMP パラメータ**：SNMP を使用してデバイスにリモートアクセスを行う際に使用するコミュニティストリングの一覧を表示します。

次ページの表は、デバイス検索時に行うタスクの要点をまとめたものです。デバイス検索の詳細は、その後の項を参照してください。

検索に必要なタスク	手順
デフォルト設定でデバイスを検索	なし。デフォルトで自動検索が有効になっています。
ブロードキャスト送信がローカルネットワークに到達しないように設定	**検索設定**ダイアログボックスの**ネットワーク**タブで「**ネットワークを自動的に検索**」チェックボックスを非選択状態にした後、**デバイス**タブで「**デバイスを自動的に検索・モニタ**」チェックボックスを非選択状態にします。
検索対象から特定のネットワークを除外	**検索設定**ダイアログボックスの**ネットワーク**タブで、検索対象から除外したいネットワークの横のチェックボックスを非選択状態にします。「**ネットワークを自動的に検索**」オプションが選択されていない場合は、ネットワークを手動で入力し、チェックボックスを非選択状態にします。
特定のネットワークのみ検索	**検索設定**ダイアログボックスの**ネットワーク**タブで、「**ネットワークを自動的に検索**」チェックボックスを非選択状態にします。その後、**追加**ボタンを押し、ネットワークアドレスとネットワークマスクを入力します。SiteAudit は新しく追加した全ネットワークにブロードキャスト送信し、入力したネットワークアドレスとサブネットマスクを使用して全アドレスを個別にチェックします。
特定のデバイスのみ検索	**検索設定**ダイアログボックスの**デバイス**タブで、「**デバイスを自動的に検索・モニタ**」チェックボックスを非選択状態にします。その後、**追加**ボタンを押し、デバイス検索したいアドレス領域またはデバイスの IP アドレスを入力します。特定の IP アドレスを入力する場合は「**開始 IP アドレス**」ボックスに入力します。アドレス領域を入力する場合は「**領域を指定**」チェックボックスをチェックし、**開始 IP アドレス**と**終了 IP アドレス**を入力します。
検索対象から特定のデバイスを除外	**検索設定**ダイアログボックスの**デバイス**タブで**追加**ボタンを押し、検索対象から除外したいデバイスの IP アドレス、またはアドレス領域を入力して **OK** を押します。**スキャン**列で、検索対象から除外したいアドレスまたはアドレス領域の横のチェックボックスを非選択状態にします。
ホスト接続されているデバイスを検索する場合ホストクレデンシャルを使用するよう指定	**検索設定**ダイアログボックスの**ホストクレデンシャル**タブで**追加**ボタンを押し、ホストユーザー名とパスワードを入力します。
検索対象からローカルプリンタを除外	**検索設定**ダイアログボックスの**ホストクレデンシャル**タブで「**ローカルデバイスを検索・モニタ**」チェックボックスを非選択状態にします。
使用する SNMP コミュニティストリングを入力	**検索設定**ダイアログボックスの **SNMP パラメータ**タブで**追加**ボタンを押し、コミュニティストリングを追加します。
使用する SNMP コミュニティストリングを並び替える	**検索設定**ダイアログボックスの **SNMP パラメータ**タブでコミュニティストリングを選択した状態で上向きまたは下向き矢印を使用してストリングを並び替えます。

ネットワークプリンタ

SiteAudit では自動的にネットワークをスキャンしてデバイスを検索することも、ユーザーが指定したネットワークまたはデバイスを検索することもできます。ブロードキャスト送信には RIP、SNMP、ICMP の 3 種類のパケットを使用します。

自動検索（デフォルト）では以下の動作を実行します。

- ローカルネットワークにブロードキャスト送信を行い、ブロードキャストに応答したネットワーク上の全デバイスを検索。
- SNMP および RIP に応答したルーターと各ルーターに接続されているネットワークを検出し、各ネットワークに接続されているデバイスを検索します。この手順は再帰的に実行されるため、ネットワーク内の全ネットワークとそのネットワーク上の全デバイスを検索します。
- 既知のネットワーク上にある全 IP アドレスを個別にチェックします。これはブロードキャストに応答しないデバイスも存在するからです。この場合、各ネットワーク上で、ネットワーク番号とサブネットマスクから IP アドレスを算出します。

ネットワークと**デバイス**タブで SiteAudit が自動検索を実行するかどうか、また、実行する場合、検索対象となる IP アドレス領域が選択できます。その他、指定領域内でモニタするデバイスを追加または除外できます。すなわち、デバイスの検索・モニタを行いたい IP アドレス領域をユーザーが指定できます。ネットワーク、IP アドレス領域、IP アドレスを追加あるいは除外するにはネットワークマスクを指定します。

デバイス検索の際には以下の 2 点に注意してください。

- 特定の IP アドレス領域内のデバイスを検索する場合は、「**ネットワークを自動的に検索**」を無効にし、IP 領域を手動で追加してください。
- 特定のネットワークを検索対象から除外する場合は、SiteAudit がそのネットワークを検出するか、手動でそのネットワークを追加するように設定した後で、検索を開始する前にそのネットワーク上での検索を無効（ネットワークの横のチェックボックスを非選択状態にする）にしてください。

> **ネットワークトラフィックについて**
>
> 自動検索の最初の数分間にトラフィックがネットワーク帯域の 3%から 5%を占めます。*これが SiteAudit 使用時の最大トラフィック量となります。*プリンタ・インベントリ作成後は、6 日間に 1 度デバイス検索を実行しますが、ネットワークトラフィックへの影響はほとんどありません。
>
> サブネット、ルーティングなどを含むネットワーク・デザインもネットワークトラフィックに影響を及ぼす可能性があります。

ローカルプリンタ

SiteAudit では直接 USB または LPT ポートに接続されているプリンタ（ローカルプリンタ）も検索できます。検索できるのは SiteAudit がアクセスできるネットワークエレメント上のホストに直接接続されているプリンタあるいは**検索設定**ダイアログボックスの**ネットワーク**または**デバイス**タブで指定したセグメント内のプリンタに限られています。

デバイスの IP アドレスを手動で入力して検索することも可能です。

検索データのインポート

検索データを XML ファイルにインポートするには**ツール⇒インポート**を選択してください。

ファイル内で以下の点を指定できます。

- 検索対象に含むネットワーク、ネットワーク領域、デバイス
- 検索対象から除外するネットワーク、ネットワーク領域、デバイス
- 使用する SNMP コミュニティストリング

デバイス固有の情報も指定できます。

- 設置場所
- プリンタ名
- シリアル番号
- 資産タグ
- 購入日
- インストール日
- MAC アドレス
- IP アドレス

ファイルのシンタックスは以下の通りです。

```
<root>

 <Import>

  <Discovery>

   <Networks>
    <Include>
                        検索対象に含むIPアドレス、アドレス領域
    </Include>
    <Exclude>
                        検索対象から除外するIPアドレス、アドレス領域
    </Exclude>
   </Networks>

   <Ranges>
    <Include>
                        検索対象に含むIPアドレス領域
    </Include>
```

```
    <Exclude>
                        検索対象から除外するIPアドレス、アドレス領域
    </Exclude>
   </Ranges>

   <Devices>
    <Include>
                        検索対象に含むデバイスIPアドレス
    </Include>
    <Exclude>
                        検索対象から除外するデバイスIPアドレス
    </Exclude>
   </Devices>

   <CommunityStrings>
                        使用するコミュニティストリング
   </CommunityStrings>
  </Discovery>

  <Provisioning>
                        デバイス固有の情報（シンタックスは以下のサンプルファイルを参照のこと）
  </Provisioning>

 </Import>

</root>
```

必須のタグは<root>タグと<Import>タグだけです。<Provision>タグと<Printer>タグはいくつあってもかまいません。

サンプルファイル：

```
<?xml version="1.0" encoding="utf-8"?>
<root>
  <Import>

   <Discovery>
    <Networks>
     <Include>
      10.0.0.0 - 255.255.255.0, 192.168.0.0 - 255.255.255.0
     </Include>
     <Exclude>
      192.168.10.0-255.255.255.0
     </Exclude>
    </Networks>
    <Ranges>
     <Include>
      192.168.0.0 - 192.168.1.255
     </Include>
    </Ranges>
    <Devices>
     <Exclude>
      10.25.25.192,10.25.25.193
     </Exclude>
    </Devices>
    <CommunityStrings>
```

```
    public,private
   </CommunityStrings>
  </Discovery>

  <Provisioning>
   <Provision TYPE="MACAddress">
    <Printer>
     <MacAddress>
      AA-BB-CC-DD-EE-FF-00
     </MacAddress>
     <SerialNumber>
      <![CDATA[061901628T]]>
     </SerialNumber>
     <Name>
      <![CDATA[SalesPrinter-01]]>
     </Name>
     <Location>
      <![CDATA[Irvine]]>
     </Location>
     <AssetTag>
      <![CDATA[QYYE234]]>
     </AssetTag>
     <AcquiredOn>
      <![CDATA[10/1/97]]>
     </AcquiredOn>
     <InstalledOn>
      <![CDATA[10/12/97]]>
     </InstalledOn>
    </Printer>
   </Provision>
   <Provision TYPE="SerialNumber">
    <Printer>
     <SerialNumber>
      <![CDATA[061901628T]]>
     </SerialNumber>
     <Name>
      <![CDATA[SalesPrinter-01]]>
     </Name>
    </Printer>
   </Provision>
   <Provision TYPE="IPAddress">
    <Printer>
     <IPAddress>
      10.0.0.17
     </IPAddress>
     <SerialNumber>
      <![CDATA[061901628T]]>
     </SerialNumber>
     <Name>
      <![CDATA[SalesPrinter-01]]>
     </Name>
    </Printer>
   </Provision>
  </Provisioning>

 </Import>
</root>
```

ホストクレデンシャル

Windows ホストに接続する場合、SiteAudit は**ホストクレデンシャル**タブに入力されているユーザー名/パスワードの組み合わせを試みます。これはホストへのアクセスが成功するか、リスト内のすべての組み合わせを試し終わるまで繰り返されます。最も頻繁に使用するユーザー名/パスワードの組み合わせが上にくるようにリストを並び替える必要があります。また、クレデンシャルの入力に何度か失敗した後でもロックされないように設定しておく必要があります。

SiteAudit の「非認証ホスト」レポートにはアクセスを許可しなかったホストの詳細情報が記載されています。それを参考にローカルプリンタを完全に検索できるようにクレデンシャルを追加します。その場合、すべてのホストまたはホストのグループに使えるクレデンシャルを追加すると良いでしょう。

ドメイン管理者のクレデンシャルではネットワーク内のホストワークステーションに管理者アクセスが行えない場合は、各ホストのクレデンシャルを 1 つずつ入力できます。あるいは**ホスト名\ユーザー名**と同等である***\ユーザー名**を使用することも可能です。その場合、検出した各ホストに合った名前を SiteAudit が置換します。

データベース

SiteAudit をデータベースに接続するためには**設定⇒データベース**を選択して設定を行います。

SiteAudit のデータベースを設定する際、サーバー名には以下の形式を使用します。

HOSTNAME\INSTANCE_NAME

その場合、HOSTNAME は SQL Server Express がインストールされているホスト名で、INSTANCE_NAME は SQL Server Express のインスタンス名になります。

バージョン 1.6.1 では、オーナー権限をもつユーザーのみがデータベースの設定/更新、バックアップ、リストアを実行できるようになっています。

データベースの設定に関してはナレッジベースの以下の記事を参照してください。
http://www.netaphor.com/products/Support/Documentation/KB/DeploymentGuide.pdf.

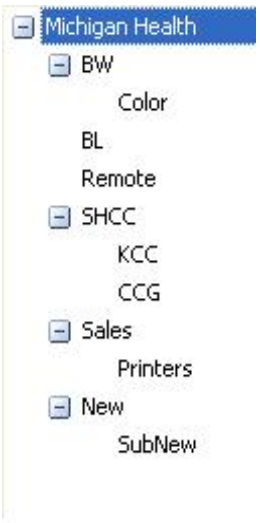
組織情報

組織の階層構造を設定するためには**設定⇒組織情報**を選択します。

SiteAudit では、ニーズに合った単位でプリンタを配置できます。例えば、部門別にコストをトラッキングする場合は、プリンタを部門別に配置します。収集したデータに基づいてプリンタの購入、課金、設置台数の検討が可能になります。

場所（フロア、建物、キャンパスなど）単位でプリンタを配置することも可能です。その場合のビューやレポートは、部門別ではなく、場所単位で作成されます。

以下の例を参照してください。



プリンタの割当

組織構造を設定した後、プリンタを部門や場所などに割り当てます。

セキュリティ上の問題点

ネットワーク検索

ネットワーク検索を行う際、SiteAudit はまずデバイスを検出し、そのデバイスがプリンタであるかどうか確認します。その一連の動作にセキュリティソフトが反応する場合があります。

セキュリティソフトの誤判定を防ぐためには、**SiteAudit Monitor が動作している IP アドレスからの要求を無視するようにセキュリティソフトを設定する必要があります。**

SiteAudit が行うネットワーク検索の手順は以下の通りです。

1. ブロードキャスト送信を行い、デバイスとルータを検出します。
2. Ping スイープを実行し、ネットワークデバイスを検出します。
3. 以下のポートをスキャンし、プリンタを検出します。

   161　SNMP ポート。　SNMP はデータ収集に使用します。

   80　HTTP ポート。組み込み web サーバーが存在するか確認します。HTTP はデータ収集に使用します。

   9100　プリンタ用プリントプロトコル。データ収集に使用します。

   1650　同上

   631　IPP プリントプロトコル。データ収集に使用します。

   135　RPC（リモートプロシージャコール）。ローカルプリンタの Windows ホスト検出に使用します。

ローカルプリンタ検索

SiteAudit では直接 Windows ホストに USB またはパラレル接続されているプリンタ（ローカルプリンタ）も検索できます。ホストにアクセスするためには、そのホストの管理者のユーザークレデンシャルを必要とします。

ローカルプリンタの検索が成功するためには、以下の点を確認する必要があります。

- 全ホスト上で使用できるクレデンシャルが入力されている。
- クレデンシャルの入力に何度か失敗した後でもロックされないよう設定されている。
- 「非認証ホスト」レポートに記載されているアクセスが許可されなかったホストに対してクレデンシャルが追加されている。

SNMP アクセス

SNMP プロトコルでは「コミュニティストリング」を用いたアクセス制御も行います。SiteAudit ではデバイスにアクセスする際に必要なコミュニティストリングの一覧が管理されています。

SiteAudit ではデフォルトのコミュニティストリングの一覧を提供しています。コミュニティストリングは、デフォルトの順序で一覧表示されており、SiteAudit は上から順番に試します。これはデバイスへのアクセスが成功するか、すべてのコミュニティストリングを試し終わるまで繰り返されます。

デバイス内の SNMP エージェントの中には、そのデバイスに対して有効でないコミュニティストリングを受信した場合に認証の失敗を示すトラップを生成するように設定されているものがあります。認証失敗トラップが生成されないようにするためには、以下の手順を実行してください。

- コミュニティストリングの一覧に必要なコミュニティストリングのみ入っていることを確認する。
- 認証失敗トラップが要求のソース（無効なコミュニティストリングのメッセージの送信元アプリ）を SiteAudit と示している場合、トラップを無視する。
- デバイスの認証失敗トラップ機能を無効にする。

クレデンシャル

SiteAudit では以下のケースでクレデンシャルの入力が必要になります。

- サーバーまたはワークステーションに対する SiteAudit のインストール：サービスとして動作しているローカルアカウントが必要。
- SQL Server または SQL Server Express のインストール：sa パスワード、統合セキュリティを使用する場合はデータベースに管理者レベルのアクセス権限を持つユーザーのログインクレデンシャルが必要。
- ローカルプリンタの検索：プリンタの接続されている Windows ホストの Windows 管理者クレデンシャルが必要。
- WMI を使用したローカルプリンタ検索：ルートネームスペースのフルアクセス許可をもつアカウントが必要。

Windows ファイアウォール

Windows XP 上で Windows ファイアウォールが有効になっている場合は、SiteAudit が RIP、ICMP、SNMP、SQL Server およびローカルプリンタのリモートホストにアクセスできるよう設定する必要があります。SiteAudit がアクセスするリモートホストに関しては Windows ファイアウォール上で、外部から内部に向かうパケットも内部から外部に向かうレスポンスも許可する必要があります。「リモートモニタリング」を有効にすることで、SiteAudit がリモートホスト上で必要なファイアウォール・アクセスが可能になります。

Windows XP Professional 上ではリモートログオンの際に、ユーザーが GUEST アカウントの使用を強制されないようにする必要があります（これはドメインに参加していないコンピュータのデフォルト設定です）。**管理ツール⇒ローカルセキュリティポリシー⇒セキュリティオプションのネットワークアクセス：ローカルアカウントの共有とセキュリティモデル**を「クラシック」に設定します。

Windows XP SP2 Professional 版と Home 版では、リモート管理が許可されていることを確認してください。SiteAudit Monitor のホストと全 Windows ターゲットコンピュータ上で TCP135 番ポートへのアクセスが許可されている必要があります。

チェックリスト

SiteAudit のインストール・設定の開始前と終了後に以下の点を確認してください。

1. プラットフォーム

   ☐ 5 ページに説明されているプラットフォーム条件が満たされている。

2. インストール・設定の前に

   ☐ SiteAudit がすでにインストールされている場合はデータベースをバックアップする。

   ☐ 旧バージョンの SiteAudit がインストールされている場合はアンインストールする。

3. データベース

   ☐ ネットワーク上に SQL Server がインストールされている場合は、それが使用可能でデータ収集用のデータベースがあることを確認する。

   ☐ SQL Server を選択した場合に SQL セキュリティを使用する場合は、sa パスワードを持っていることを確認する。統合セキュリティを使用する場合は、SiteAudit Monitor が動作しているホストアカウントが SQL Server データベースに対してデータベース管理者クレデンシャルをもっていることを確認する。

4. Windows サービス

   ☐ 7 ページに説明されている Windows サービスが開始しているか開始できる状態であることを確認する。

   ☐ スキャン対象の全クライアントコンピュータ上および SiteAudit Monitor が動作しているホスト上で WMI（Windows Management Instrumentation）へのアクセスが有効になっていることを確認する。

5. ネットワーク検索

   ☐ **検索設定**ダイアログボックスの**ネットワーク**タブで、デバイス検索を行う全ネットワークが表示されており、チェックボックスが選択状態になっていることを確認する。

   ☐ **検索設定**ダイアログボックスの**ネットワーク**タブで、デバイス検索の検索対象から除外する全ネットワークが表示されており、チェックボックスが非選択状態になっていることを確認する。

   ☐ 自動的に検索されないものの、検索対象に含めたい、あるいは検索対象から除外したい領域を追加し、チェックボックスが選択状態（検索対象に含める場合）、あるいは非選択状態（除外する場合）になっていることを確認する。

   ☐ **デバイス**タブで追加したい、あるいは除外したいデバイスを追加する。除外するべきデバイスには UPS デバイスや DNS サーバーのほか、アクセスしてはならないデバイスなどがある。

   ☐ ブロードキャスト送信を使用するかどうか決定する。

6. SNMP

   ☐ 必要な全コミュニティストリングがリストに追加されていることを確認する。

   ☐ 使用頻度が最も高いコミュニティストリングを最初に試すようにコミュニティストリングの順序を並び替える。

   ☐ 使用しないコミュニティストリングを削除する。

7. Windows ホスト

   ☐ 必要な全クレデンシャルが**検索設定**ダイアログボックスの**ホストクレデンシャル**タブに追加されていることを確認する。

   ☐ ファイアウォール設定が正しいことを確認する。

8. セキュリティ

   ☐30 ページに説明されているようにセキュリティソフトを設定する必要があるかどうか確認する。

トラブルシューティング

問題：デバッグに役立つデータがほしいのですが・・・。

RegEdit でレジストリキーHKLM\Software\Netaphor\PALM に Debugging という名前のキーを追加します。Debugging に EnableEventLog という名前の DWORD 値を追加し、それを 0 以外の値に設定します。こうすることで SiteAudit から Windows イベントログが生成できます。

問題：WAN リンク経由でデータベースサーバーをアクセスしようとしているのですが、タイムアウトしてしまいます。

RegEdit でレジストリキーHKLM\Software\Netaphor\PALM\Database に CommandTimeout という名前の DWORD 値を追加し、それを 2000（10 進）に設定します。

問題：データベースへのアクセスにかなり時間がかかるのですが・・・。

データベース管理者にデータベースを圧縮する必要がないか問い合わせてください。

お問い合わせ

お問い合わせ全般

15510 Rockfield Blvd., Suite C-100
Irvine, CA 92618 USA

Phone: +(949) 470 7955
Fax: +(949) 470 4966

Toll free: 1-877-638-2479 – 米国内のみ

SiteAudit テクニカルサポート

SiteAudit のテクニカルサポート

メールアドレス: support@netaphor.com

メールにはテクニカルサポートを希望する人の名前、SiteAudit のバージョン番号（例：1.3）、問題の名前とその説明を必ず記載してください。

営業担当

電話番号: +(949) 232 9170

メールアドレス: sales@netaphor.com