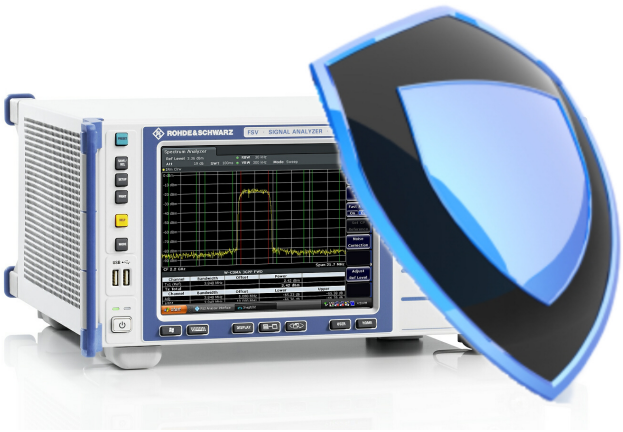
悪意のあるソフトウェアからの保護
ホワイト・ペーパー



ローデ・シュワルツは、Windows®ベースのテスト機器をローカル・エリア・ネットワーク（LAN）経由で他のコンピュータに接続したり、リムーバブル・ストレージ・デバイスを使用したりした場合のコンピュータ・ウィルス感染の潜在的リスクを認識しています。
このホワイト・ペーパーではマルウェアによる脅威を最小限に抑える手段を紹介し、機器の性能を損なうことなくリスクを軽減するための方法についてご紹介いたします。
ここでは、アンチウィルス・ソフトウェアの使用とその推奨構成設定について述べるとともに、OS パッチの定期的なインストールを通じて Windows® XP オペレーティング・システムを正しくアップデートし、これを常に最新の状態に維持する方法の概要を示します。

Jochen Wolle
06.2012-1EF73_0J

ROHDE&SCHWARZ

目次

1 Windows®ベースの機器

1.1 概要

ローデ・シュワルツは、そのすべての製品をウィルスの心配がない状態（ウィルスフリー）で出荷できるよう、最大限の努力を払っています。Windows オペレーティング・システムで動作する機器は、他の PC と同様にマルウェアから保護する必要があります。ユーザには、アンチウィルス・ソフトウェアを使用したり、定期的に OS パッチをインストールして更新を行ったりするなどして、その使用機器を保護するための手段を講じることが強く推奨されます。また、自社のネットワークに機器を接続するときは、IT 部門やシステム管理者と密接に協力し合い、自社のポリシーに従って接続を行うことを強くお勧めします。

1.2 コンピュータ・ウィルス管理プログラム

ローデ・シュワルツは、ローカル・エリア・ネットワークに接続される Windows ベース機器に関するコンピュータ・ウィルス感染の潜在的リスクを認識しています。
ローデ・シュワルツは、機器からお客様のコンピュータやネットワークにウィルスが拡散するのを防ぐために、適切なあらゆる予防措置を講じるためのプロセスを自社内で確立しています：

- ローデ・シュワルツで使用され、お客様への出荷が予定されている機器に接続する可能性のあるすべてのコンピュータには、集中管理されたファイアウォールとアンチウィルス・ソフトウェアがインストールされており、ウィルス定義も最新の状態に維持されています。また、コンピュータとリムーバブル・ストレージ・デバイスは、コンピュータ・ウィルスの拡散を防ぐために定期的にスキャンされています。
- 製造、サービス、サポート、営業、販売、およびデモなどの環境においては、厳密なウィルス管理プロトコルが確立されています。これには機器の構成に応じ、隔離された LAN の使用、装置やリムーバブル・ストレージ・デバイスのスキャン、ハード・ドライブの再イメージングなどが含まれます。
- アンチウィルス・セキュリティ・プロトコルを強化するために、お客様の機器に接触するすべてのローデ・シュワルツ従業員が従うべき手順が確立されています。これは、製造、サービス、サポート、営業、販売などに携わる従業員が対象となります。

1.3 予防的メンテナンスに関する検討

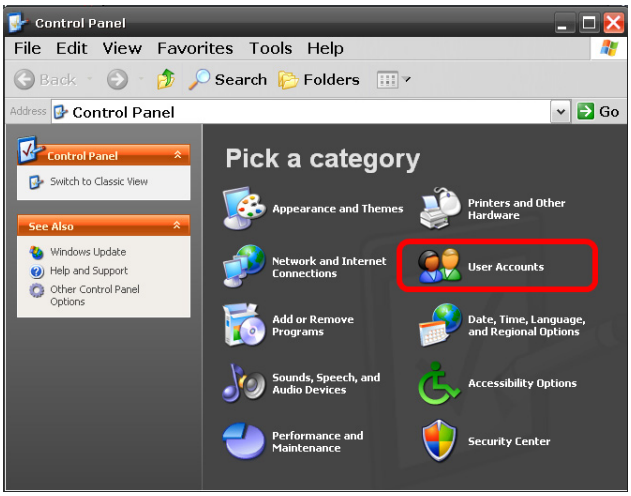
以上に述べたステップは、ローデ・シュワルツがお客様へ機器を納入する際に、それらすべての機器がウィルスフリーの状態であることを保証する一助となっています。このような点からすると、機器のセキュリティはユーザの努力によって維持されていく必要があります。
機器を自社のネットワークに接続する前に IT 部門またはシステム管理者に相談して、具体的にどのようなポリシーを適用するのかを決定してください。機器は、ネットワークからは標準的なコンピュータに見えます。コンピュータのセキュリティとウィルスからの保護は、自社のポリシーに従って行ってください。
また、ウィルス定義とオペレーティング・システムを定期的に更新することも重要です。ローデ・シュワルツは、機器をスキャンしてマルウェアの有無を確認することに加え、ウィルス定義とオペレーティング・システム両方の更新を少なくとも週に 1 回はチェックすることを推奨します。IT 部門やシステム管理者から OS とアンチウィルス定義を更新するようアドバイスがあった場合は、常にこれに従って更新を行うようにしてください。機器のオペレーティング・システムの保護は、以下の手順に従って行ってください：

- 機器上のインターネット・ファイアウォールを使用します。

- 機器とともに使用するすべてのリムーバブル・ストレージ・デバイス（例えば USB メモリ・スティックなど）を定期的にスキャンし、悪意あるコードが意図せずに実行されてしまうのを防ぐために、自動実行機能（Autorun）と自動再生機能（Autoplay）を無効にします。
- 最新の Windows®パッチをインストールして機器の更新を行います。
- アンチウィルス・ソフトウェアを使って機器を定期的にスキャンし、ウィルス定義ファイルを常に最新の状態に保ちます。アンチウィルス・ソフトウェアをバックグラウンド（「オンアクセス」モード）で実行することは推奨できません。これは機器の性能に大きく影響します。

1.4 ユーザ／管理者アカウント

Windows のユーザは、ログイン・ウィンドウにユーザ名とパスワードを入力して認証を行う必要があります。一般に、ローデ・シュワルツの機器には、あらかじめ自動ログイン機能がインストールされています。つまり、機器を起動すると自動的にログインが行われます。この自動ログイン機能の工場デフォルトは管理者権限で、アクセス権限に制限はありません。したがって、プリンタをインストールしたりネットワークの構成設定を行ったりすることができます。
多くの機器では、2 種類のユーザ・アカウントを設定できます。機器の OS に制限なしでアクセスできる管理者アカウントと、限定的なアクセス権限の標準ユーザ・アカウントです。アカウントの管理は、**Windows Start（スタート）⇨ Control Panel（コントロールパネル）⇨ User Accounts（ユーザーアカウント）**で行うことができます。ユーザの変更または新しいユーザの追加の方法、および自動ログインを無効にする方法の詳細については、機器のユーザ・マニュアルを参照してください。



注：ファイアウォールの設定変更、アンチウィルス・ソフトウェアのインストールと設定、および Windows のアップデートには、無制限の管理者権限が必要です。

2 ファイアウォールの設定

Windows XP SP2 以降のバージョンでは、ファイアウォールを使用することにより、ネットワークからの攻撃に対してコンピュータや機器を保護することができます。ローデ・シュワルツの機器は、Windows ファイアウォールを有効にしてあらかじめ設定を完了させた状態で出荷されます。機器上でファイアウォールを有効にすることは、自社の保護されたネットワーク内で機器を使用する場合であっても役に立ちます。数多くのワームやウィルス、その他のマルウェアが出回っている今日のインターネット上では、何らかのマルウェアが企業のファイアウォールを潜り抜けてしまうことは避けられません。機器のファイアウォールはペリメータ内の脅威に対する保護の助けとなるだけではなく、数多くのウィルスやワームの拡散を防ぐ役割も果たします。
セキュリティや保護について追加的な要求がある場合は、自社の IT 部門またはシステム管理者に連絡して、そのセキュリティ・ポリシーに従うようにしてください。

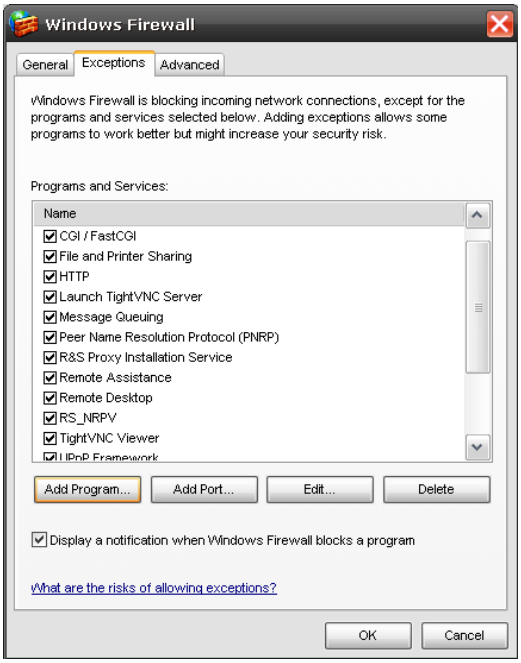
2.1 ファイアウォール ― ポート設定

ローデ・シュワルツの機器は、リモート・コントロール用のすべてのポートと接続が有効状態になるように事前設定されています。詳細については以下の表を参照してください：

ポート	*サービス*	*内容*
21 tcp	FTP	機器ウェブ・サーバ ― FTP ポート
80 tcp（HTTP）	ウェブ・サーバ	機器ウェブ・サーバ（LXI）
111 tcp、111 udp	ポートマッパ	VXI-11/LXI 用ポートマッパ・サービス
161 udp 162 udp 705 tcp（AgentX）	SNMP	SNMP エージェント用標準ポート
319 tcp udp 320 tcp udp	1588 PTP	LXI クラス B/A – IEEE1588 PTP（Precision Time Protocol）
2525 tcp	RSIB	R&S SCPI ソケット接続
4880 tcp	HiSLIP	高速 LAN インタフェース・プロトコル
5025（データ） 5125（アボート）	TCP ソケット	「未加工 SCPI」ソケット接続
5044 tcp udp	LXI クラス B	LXI LAN メッセージとイベント マルチキャスト・アドレス udp: 224.0.23.159
5800 tcp 5900 tcp	VNC	ウェブ・サーバ経由の機器ソフト・フロント・パネル（ブラウザ・インタフェース）
13217 tcp udp	RS インストーラ	R&S ソフトウェア・ディストリビュータ・サービス
14142 - 16383 tcp udp （ダイナミック割り当て）	ONC-RPC	Sun ONC-RPC プロトコル – VXI-11

2.2 ファイアウォール設定の変更

機器上ではファイアウォールを有効にすることを強くお勧めします。
ファイアウォール設定を変更するには、管理者権限が必要です。ファイアウォール設定の操作は、**Windows Start（スタート）⇨ Control Panel（コントロールパネル）⇨ Windows Firewall（Windows ファイアウォール）**で行うことができます：



デフォルトのファイアウォール設定に伴う問題は、次の 2 点が考えられます。

- クライアント・プログラムが機器からデータを受け取ることができない。
- その機器上で実行されているサーバ・プログラムが、クライアントの要求に対応できない。

プログラムがブロックされる場合は、次のような Windows ファイアウォールのセキュリティに関する警告が表示されます：

プログラムがブロックされないようにするには、**Security Alert（セキュリティの重要な警告）**ダイアログ・ボックスの**Unblock（ブロックを解除する）**をクリックします。ファイアウォールの設定と構成の詳細については、次のサイトで参照できます：

http://support.microsoft.com/kb/875357/en-us

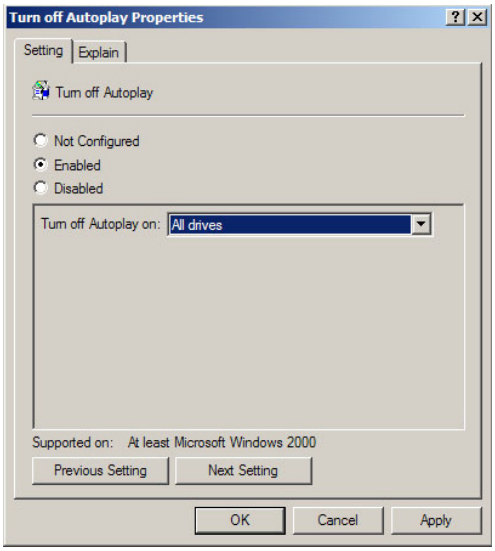
3 USB デバイス

今日では、USB メモリ・スティックやリムーバブル・ハード・ドライブは大きな保存容量を持ち、これを使用すれば機器の設定、測定結果、ハードコピーなどを非常に便利な形で保存することができるので、職場ではごく一般的な存在となっています。しかし、これらのメディアは新たな問題も引き起こしています。数多くのウィルス、トロイの木馬、その他のマルウェアが、USB ストレージ・デバイスを介して感染します。感染した USB デバイスを機器に接続すると、その中のマルウェアがネットワーク全体に拡散する恐れがあります。

3.1 USB自動実行機能を無効にする

一般に、USB ドライブを介して増殖するウィルスは Windows の自動実行機能を使用します。この機能はユーザの確認を必要とせず、バックグラウンドで密かに実行されるためです。ローデ・シュワルツの機器では、事前に自動実行／自動再生機能が無効に設定されています。これにより、マルウェアが USB から自動的に実行されてしまうのを防ぐことができます。
グループ・ポリシー・エディタを使用すれば、この設定を制御または変更することができます。機器を社内ネットワーク上で使用する場合で、その機器がネットワーク・ドメインのメンバーの 1 つである場合は、IT 部門またはシステム管理者がグループ・ポリシー設定を一括して構成することができます。

- **Windows Start（スタート）⇨ Run（ファイル名を指定して実行）** をクリックし、**gpedit.msc** と入力してグループ・ポリシー設定を開きます。
- **Computer Configuration（コンピュータの構成）⇨Adminstrative Templates（管理用テンプレート）⇨System（システム）**を選択し、画面を下にスクロールさせて **Turn off Autoplay（自動再生機能をオフにする）**をダブルクリックし、設定ダイアログを開きます：



- **Enabled（有効）**ラジオボタンをクリックして「**Turn off Autoplay on（自動再生機能をオフにする）**」ドロップダウン・リストから **All drives（すべてのドライブ）**を選択して、どの USB ドライブやリムーバブル・メディアからもプログラムが自動的に実行されないようにします。

- **注**：**System（システム）**がリストされない場合は、設定テンプレートを追加する必要があります。**Administrative Templates（管理用テンプレート）**を右クリックして**Add/Remove Templates…（テンプレートの追加と削除...）**を選択してください。表示されたダイアログで **Add（追加）**をクリックして、「system.adm」を選択します。メイン・ウィンドウに戻るには **Open（ｏↄķfi）**をクリックしてから **Close（◒ↄ☼）**をクリックします。

自動実行機能に関する詳細が必要な場合は、次のサイトで参照できます：
http://support.microsoft.com/kb/967715/en-us

3.2 USBデバイスのスキャン

USB メモリ・スティックとリムーバブル・ハード・ドライブへのマルウェアの感染を防ぐには、アンチウィルス・ソフトウェアを使って定期的にこれらのメディアをスキャンすることをお勧めします。
USB ストレージ・デバイスは、ローデ・シュワルツの機器に挿入する前に、ご使用のコンピュータとアンチウィルス・ソフトウェアを使ってスキャンしてください。

4 アンチウィルス・ソフトウェア

パーソナル・コンピュータや業務用コンピュータと同様に、ユーザは、適切なステップを踏んで使用機器をウィルス感染から保護する必要があります。ローデ・シュワルツ機器に強力なファイアウォール設定を使用することや、リムーバブル・ストレージ・デバイスを定期的にスキャンすることに加えて、アンチウィルス・ソフトウェアをインストールすることもお勧めします。Windows ベースの機器上でアンチウィルス・ソフトウェアをバックグラウンド（「オンアクセス」モード）で実行すると機器の性能を低下させる恐れがあるので、これは推奨**できません**。アンチウィルス・ソフトウェアは、機器にかかる負荷が小さい時間帯を選んで、少なくとも週に 1 回実行することをお勧めします。
現在のアンチウィルス・ソフトウェアは、大量のシステム・リソースを必要とします（ハード・ドライブ・スペースの消費とメモリ消費の両面において）。したがって、一部の機器ではリソースに限りがあるため、アンチウィルス・ソフトウェアをインストールしたり実行したりすることができません。このような場合に取り得る選択肢は、USB メモリ・スティックからソフトウェアを実行してこれらの機器をスキャンするか、これらの機器をネットワーク上のドライブとして取り付け、アンチウィルス・ソフトウェアをインストールした別のコンピュータからそれらの機器をスキャンすることです。これらの選択肢については、後で詳しく説明します。

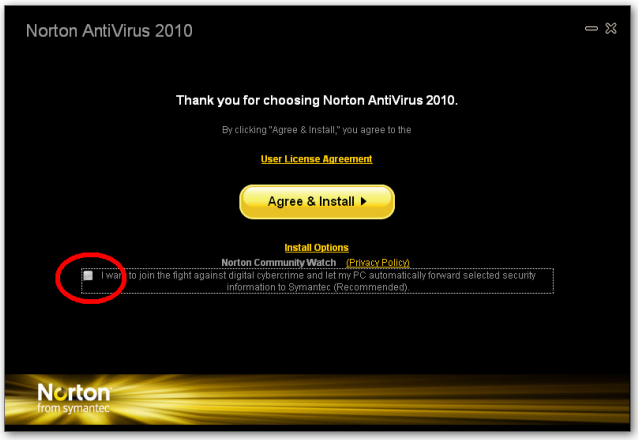
注：以下の項ではアンチウィルス・ソフトウェアに関する推奨事項に焦点を当て、一般的に使用されるいくつかのプログラムを例に挙げて説明します。他にも同様の機能を持つプログラムは存在しますが、以下の項で使用するものは一般的な例として挙げたもので、その原理は、ユーザの IT 部門やシステム管理者が使用する他のプログラムにもあてはまります。
アンチウィルス・ソフトウェアのインストール、構成設定、および使用には管理者権限が必要です。

4.1 Norton™ AntiVirus 2010

この項では、アンチウィルス・ソフトウェア Norton AntiVirus 2010 をローデ・シュワルツの機器へインストールし、構成設定をして使用する方法を説明します。

4.1.1 インストール

Norton の説明書に従って、ローデ・シュワルツの機器に Norton AntiVirus 2010 ソフトウェアをインストールします。インストール開始画面上にある **I want to join the fight...（サイバー犯罪対策のための...）**という制御チェックボックスを無効にし、**Agree & Install（同意してインストール）**をクリックしてインストールを開始します：



インストールが完了すると、Norton AntiVirus 2010 は Symantec のサーバに接続し、最新のウィルス・シグネチャを入手してプログラムを更新します（ライブアップデートと呼ばれるプロセス）。

4.1.2 要件

Norton AntiVirus 2010 のシステム要件は次の通りです：

- 機器のハード・ドライブの空きスペース　200MB
- 256MB のメモリ
- Windows XP SP2 以降

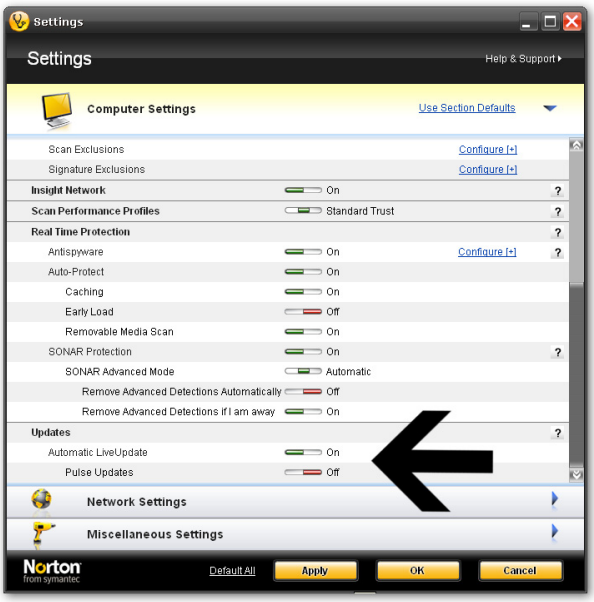
ご使用のローデ・シュワルツ機器にも Windows XP SP2 以降がインストールされていることを確認してください。機器の OS バージョン確認方法については、機器のユーザ・マニュアルを参照してください。これ以前のバージョンがインストールされている場合は、ローデ・シュワルツの最寄りの営業所または代理店へご連絡の上、更新方法をご確認ください。ローデ・シュワルツ製機器の多くには最新の OS バージョンを使用したリカバリ DVD が付属しており、機器のハード・ドライブの再イメージングを行うことができます。
ライブアップデートやウィルス・スキャン中、機器上では 2 つのプロセス（両方とも **ccSvcHst.exe**）が実行され、**最大 270MB** のメモリが占有されます。
したがって、ライブアップデートやウィルス・スキャンを開始する時は、事前にファームウェアを停止することをお勧めします。機器のファームウェアの実行を停止する方法については、各機器のマニュアルを参照してください。

4.1.3　自動アップデートとウィルス・スキャンを無効にする

Symantec のライブアップデートを実行するには、インターネット接続と管理者権限が必要です。アップデートは、Symantec のサーバか、ユーザの社内プロキシ・サーバからダウンロードされます。自社のポリシーについては、IT 部門またはシステム管理者にご確認ください。
機器性能が低下するのを防ぐために、「LiveUpdate(ライブアップデート)」と「Scans to be executed on demand（オンデマンドでスキャンを実行）」の設定を行います。システム・トレイにある Norton AntiVirus のアイコンをダブルクリックして、メイン・ダイアログを開きます：

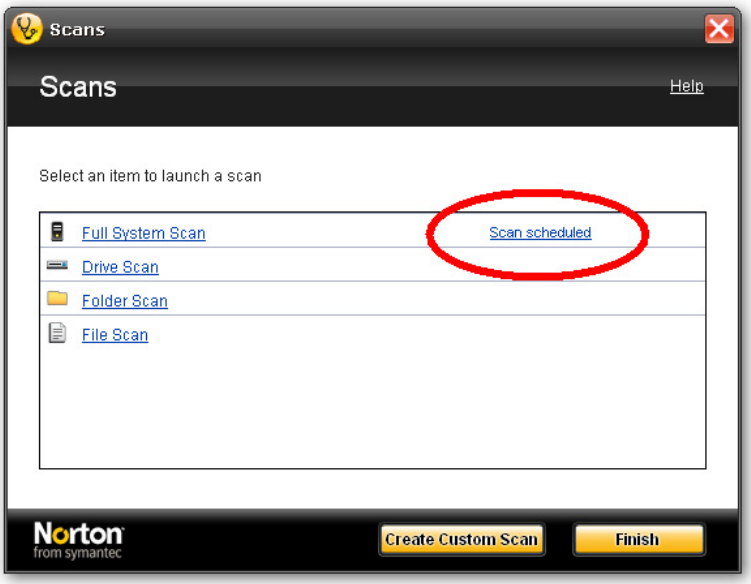
Settings（設定）をクリックして、ライブアップデートとスキャンの設定を行います：

Computer Settings(コンピュータの設定)ダイアログの **Automatic LiveUpdate(自動ライブアップデート)**と **Pulse Updates(パルスアップデート)**を両方とも無効にします：

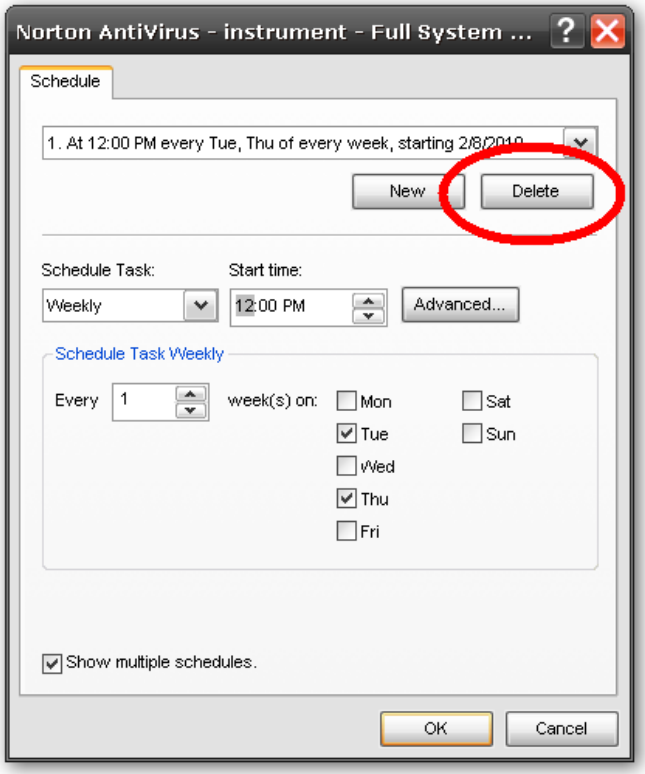


OK をクリックして設定を保存します。

設定の最終ステップは、自動ウィルス・スキャンを無効にすることです。上に述べた手順に従ってメイン・ダイアログを開き、**Run Custom Scan（カスタム・スキャンを実行）**を選択します。
Scan scheduled（スケジュールされたスキャン）を選択して、スケジュールされたウィルス・スキャンのリストを変更します：



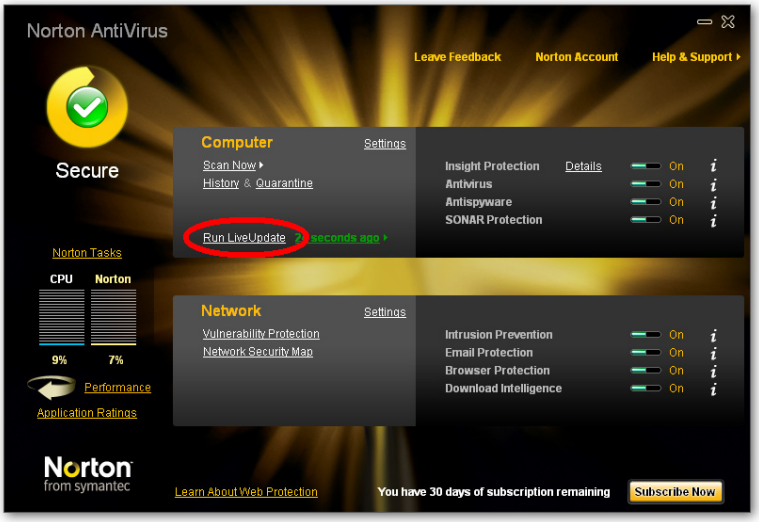
ドロップダウン・ボックスが空になるまで、スケジュール・ダイアログ内のエントリを削除します。これによって、すべての自動ウィルス・スキャンが無効になります：



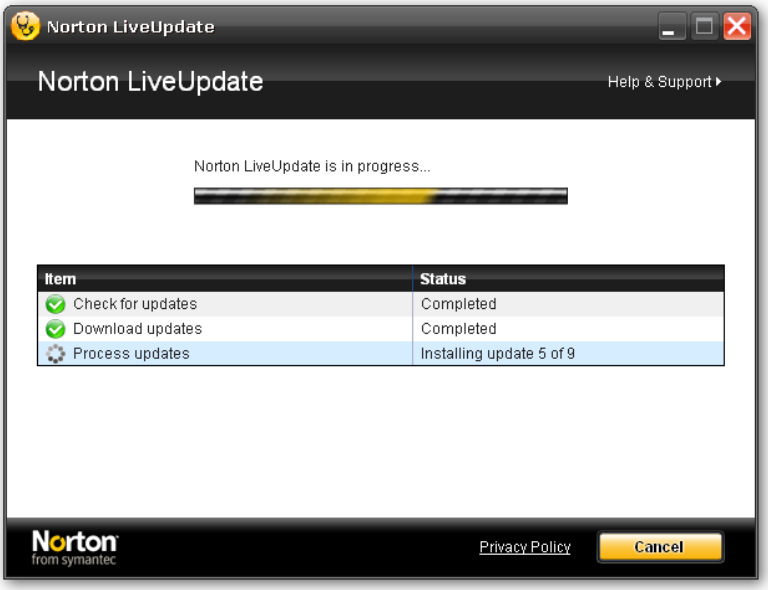
4.1.4 ウィルス・シグネチャを更新してオンデマンドでウィルスをスキャン

機器上のウィルス・シグネチャ・データベースとアンチウィルス・ソフトウェアのライブアップデートを開始するには、インターネット接続が必要です。システム・トレイにある Norton AntiVirus のアイコンをダブルクリックして、メイン・ダイアログを開きます：

Run LiveUpdate（ライブアップデートを実行）をクリックして、アップデート・プロセスを開始します：



ライブアップデートが完了したら、**OK** ボタンをクリックします。



ウィルス・シグネチャ・データベースのアップデートが完了したら、ウィルス・スキャン・プロセスを開始することができます。

ウィルス・スキャン・プロセスを開始するには、メイン・ダイアログの **Scan Now（スキャンを開始）**をクリックします。

下に示すダイアログでは、3 種類のスキャン・オプションを選ぶことができます。

選択できるオプションは、感染しやすい領域をスキャン（**Quick Scan（クイック・スキャン）**）、機器全体をスキャン（**Full System Scan（フル・システム・スキャン）**）、またはドライブ、フォルダ、およびファイルを指定してのカスタム・スキャン（**Custom Scan（カスタム・スキャン）**）のいずれかです。

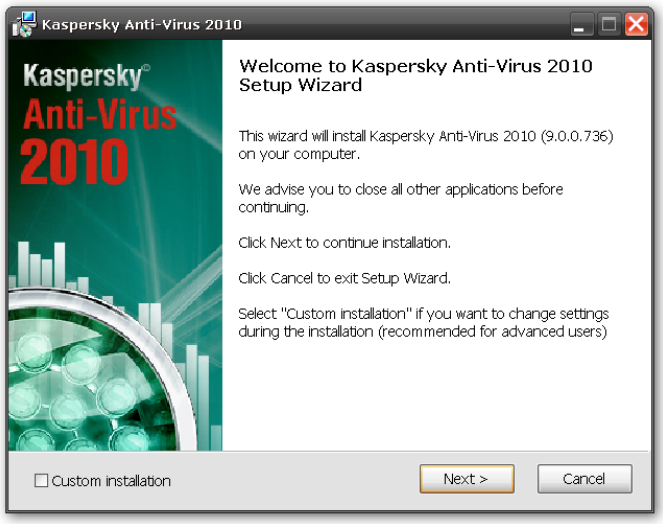
スキャン・プロセスが終了したら、**Finish（終了）**をクリックしてダイアログ・ボックスを閉じます。

4.2 Kaspersky® Anti-Virus 2010

この項では、アンチウィルス・ソフトウェア Kaspersky Anti-Virus 2010 をローデ・シュワルツの機器へインストールし、構成設定をして使用する方法を説明します。

4.2.1 インストール

Kaspersky の説明書に従って、ローデ・シュワルツの機器に Kaspersky Anti-Virus 2010 ソフトウェアをインストールします。



インストールが完了したら、Kaspersky Anti-Virus 2010 を起動して Kaspersky のサーバに接続し、最新のウィルス・シグネチャとプログラム・アップデートを入手する必要があります。

4.2.2 要件

Kaspersky Anti-Virus 2010 のシステム要件は次の通りです：

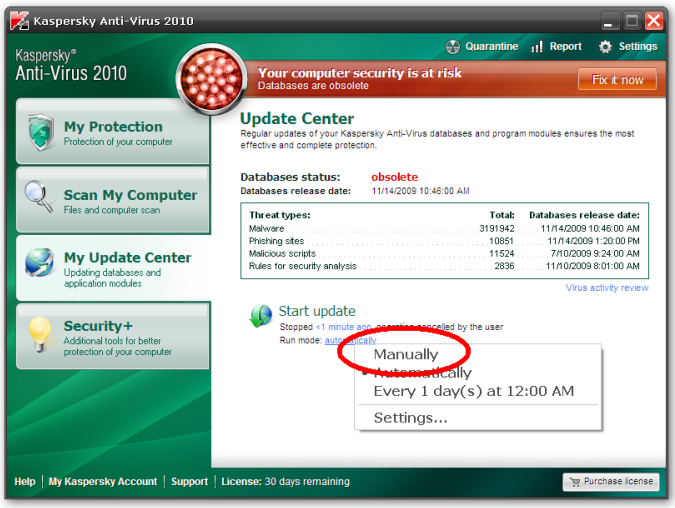
- 機器のハード・ドライブの空きスペース　300MB
- 256MB のメモリ
- Windows XP SP2 以降

ご使用のローデ・シュワルツ機器にも Windows XP SP2 以降がインストールされていることを確認してください。機器の OS バージョン確認方法については、機器のマニュアルを参照してください。これ以前のバージョンがインストールされている場合は、ローデ・シュワルツの最寄りの営業所または代理店へご連絡の上、更新方法をご確認ください。ローデ・シュワルツ製機器の多くには最新の OS バージョンを使用したリカバリ DVD が付属しており、機器のハード・ドライブの再イメージングを行うことができます。
ウィルス・シグネチャ／プログラムのアップデートやウィルス・スキャン中、機器上では 2 つのプロセス（両方とも **avp.exe**）が実行され、**最大 320MB** のメモリが占有されます。
したがって、アップデートやウィルス・スキャンを開始する時は、事前にファームウェアを停止することをお勧めします。機器のファームウェアの実行を停止する方法については、各機器のマニュアルを参照してください。

4.2.3 自動アップデートとウィルス・スキャンを無効にする

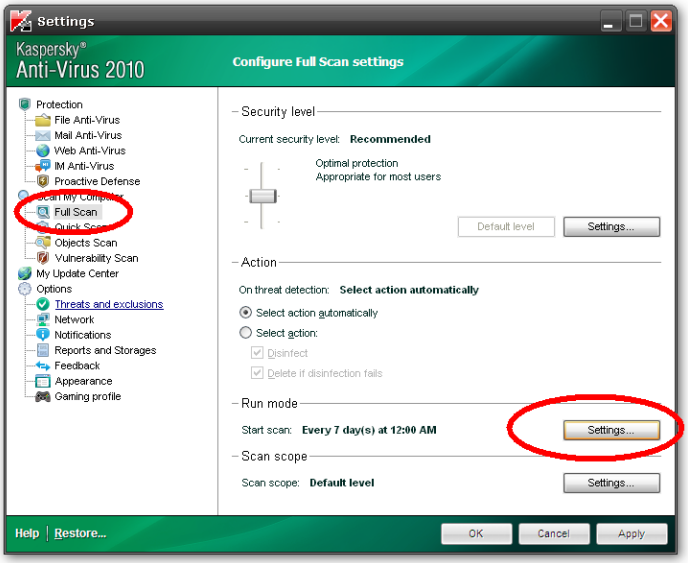
Kaspersky Anti-Virus 2010 を実行するには、インターネット接続と管理者権限が必要です。アップデートは、Kaspersky のサーバかユーザの社内プロキシ・サーバからダウンロードされます。自社のポリシーについては、IT 部門またはシステム管理者にご確認ください。
機器性能が低下するのを防ぐために、ウィルス定義アップデートの設定と、オンデマンドで実行するウィルス・スキャンの設定を行います。システム・トレイにある Kaspersky Anti-Virus のアイコンをダブルクリックして、メイン・ダイアログを開きます：

My Update Center（アップデート）をクリックします。自動ウィルス／プログラム・アップデートを無効にするには、**Start update（アップデートの開始）** ⇨ **Run mode（実行モード）**の下にある **Manually（手動）**を選択します：

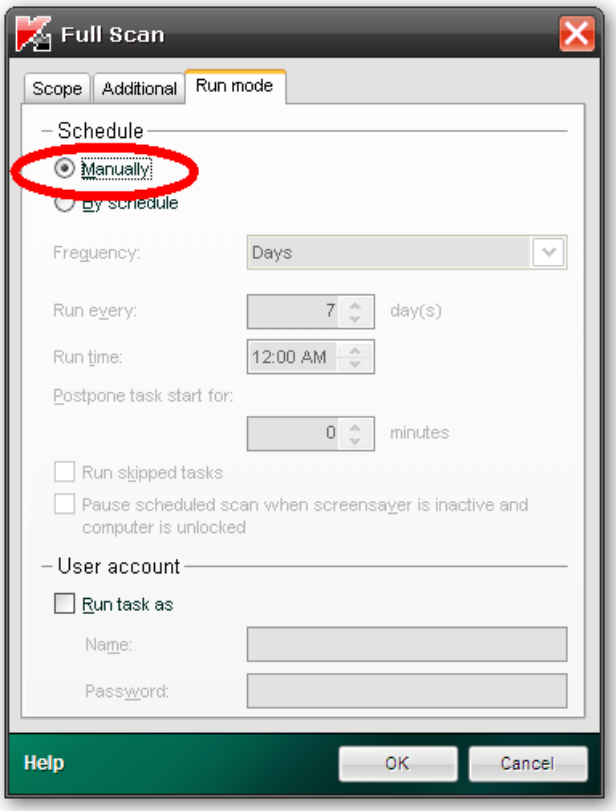


自動ウィルス・スキャンの設定を行うには、メイン・ダイアログの右上にある **Settings（設定）**を選択します：

左側のナビゲーション・ペーンにある **Full Scan（完全スキャン）**を選択してから **Settings（設定）**を選択して、実行モードの設定を行います：



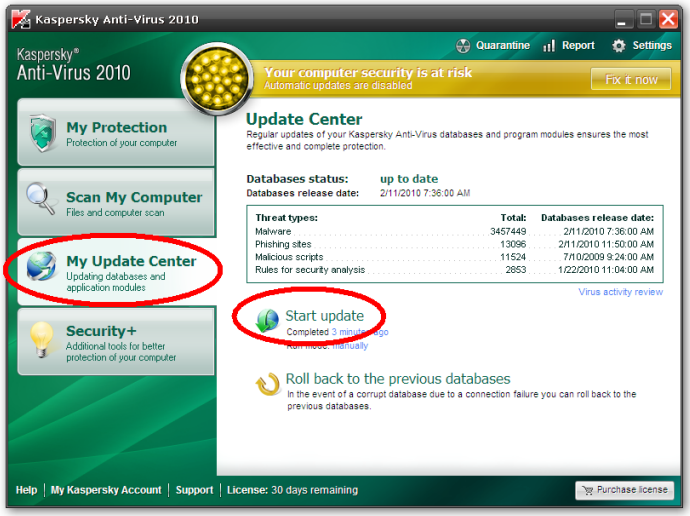
Schedule（スケジュール）の下にある **Manually（手動）**を選択し、**OK** で選択を確定して自動ウィルス・スキャンを無効にします：



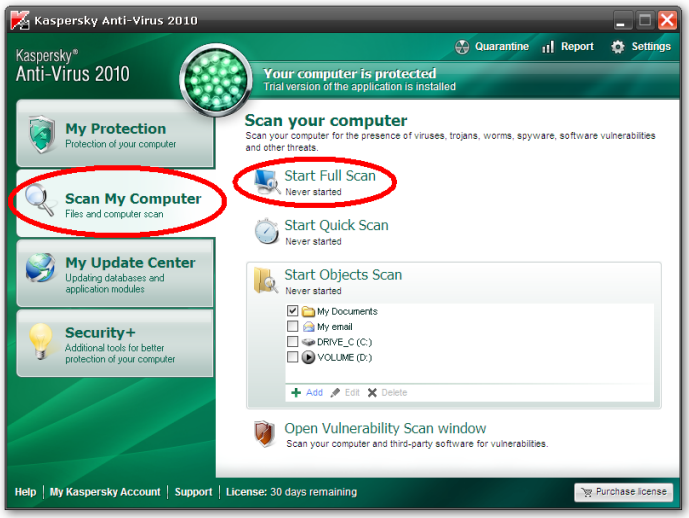
4.2.4 ウィルス・シグネチャを更新してオンデマンドでウィルスをスキャン

機器上のウィルス・シグネチャ・データベースとアンチウィルス・ソフトウェアのアップデートを開始するには、インターネット接続が必要です。システム・トレイにある Kaspersky Anti-Virus のアイコンをダブルクリックして、メイン・ダイアログを開きます：

アップデート・プロセスを開始するには、メイン・ダイアログの左側にある **My Update Center（アップデート）**タブを選択してから **Start Update（アップデートの開始）**を選択します：



ウィルス・スキャンを開始するには、メイン・ダイアログの左側にある **Scan My Computer（スキャン）**タブを選択してから **Start Full Scan（完全スキャンの開始）**を選択します：



ウィルス・スキャンの他のオプションは **Quick Scan（簡易スキャン）**と **Objects Scan（オブジェクト・スキャン）**です。

4.3 Microsoft® Security Essentials

この項では、アンチウィルス・ソフトウェア Microsoft Security Essentials をローデ・シュワルツの機器へインストールし、構成設定をして使用する方法を説明します。

4.3.1 インストール

Microsoft の説明書に従って、ローデ・シュワルツの機器に Microsoft Security Essentials アンチウィルス・ソフトウェアをインストールします。このソフトウェアはインターネット接続なしでもインストールできます。

インストールが完了すると、Microsoft Security Essentials は、Microsoft のサーバに接続して最新のウィルス・シグネチャとプログラムのアップデートを入手しようとします。これを防ぐために、**Scan my computer for potential threats（最新の更新プログラムを入手した後、このコンピューターをスキャンして潜在的な脅威を検出します）**というコントロール・ボックスをオフにし、**Finish（完了）**をクリックしてインストールを完了します。

4.3.2 要件

Microsoft Security Essentials のシステム要件は以下の通りです：

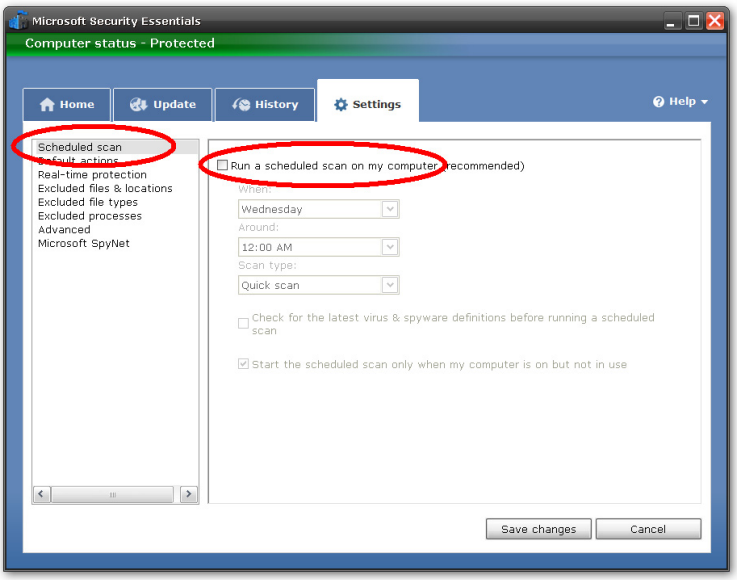
- 機器のハード・ドライブの空きスペース　300MB
- 256MB のメモリ
- Windows XP SP2 以降

ご使用のローデ・シュワルツ機器に Windows XP SP2 以降がインストールされていることを確認してください。機器の OS バージョン確認方法については、機器のマニュアルを参照してください。これ以前のバージョンがインストールされている場合は、ローデ・シュワルツの最寄りの営業所または代理店へご連絡の上、更新方法をご確認ください。ローデ・シュワルツ製機器の多くには最新の OS バージョンを使用したリカバリ DVD が付属しており、機器のハード・ドライブの再イメージングを行うことができます。
ウィルス・シグネチャ／プログラムのアップデートやウィルス・スキャン中、機器上では 2 つのプロセス（**MsMpEng.exe** と **msseces.exe**）が実行され、**最大 110MB** のメモリが占有されます。
したがって、ウィルス・スキャンを開始する時は、事前にファームウェアを停止することをお勧めします。機器のファームウェア実行を停止する方法については、各機器のマニュアルを参照してください。

4.3.3 自動ウィルス・スキャンを無効にする

Microsoft Security Essentials を実行するには、インターネット接続と管理者権限が必要です。
注：*最後にウィルス・シグネチャ・データベースのアップデートを行ってから 24 時間以上経過している場合は、Microsoft のサーバから自動的にウィルス・シグネチャのアップデートがダウンロードされます。このアップデートを無効に設定することはできません。また、ユーザのプロキシ・サーバを使用するように Microsoft Security Essentials を設定することもできません。*
機器性能が低下するのを防ぐために、ウィルス・スキャンはオンデマンドで実行するように設定します。システム・トレイにある Microsoft Security Essentials のアイコンをダブルクリックして、メイン・ダイアログを開きます：

Settings（設定）タブを選択して、左側のナビゲーション・ペーンにある **Scheduled scan（スキャンスケジュール）**を選択します。**Run a scheduled scan...（このコンピュータで...）**というチェックボックスをオフにして、自動ウィルス・スキャンを無効にします。

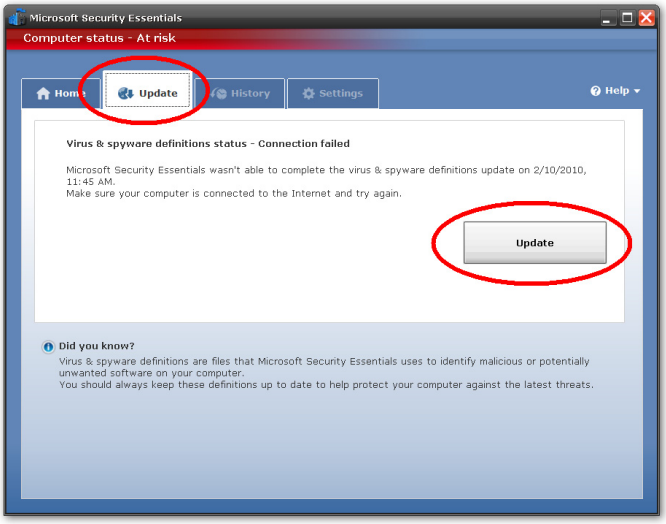


Save changes（変更の保存）をクリックして、設定を保存します。

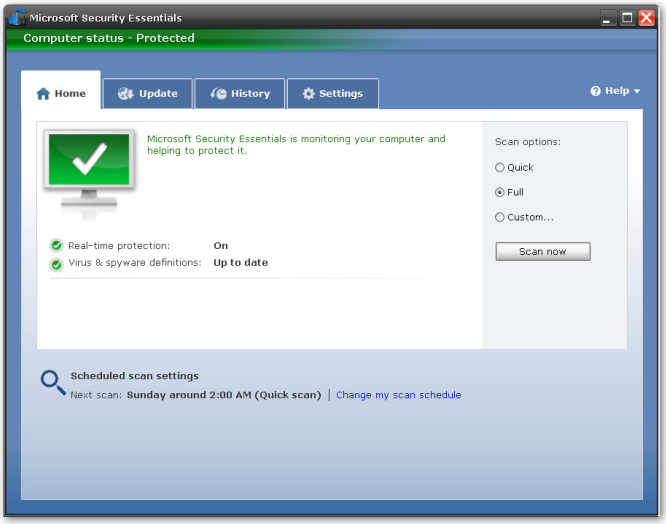
4.3.4 ウィルス・シグネチャを更新してオンデマンドでウィルスをスキャン

機器上のウィルス・シグネチャ・データベースとアンチウィルス・ソフトウェアのアップデートを開始するには、インターネット接続が必要です。システム・トレイにある Microsoft Security Essentials のアイコンをダブルクリックして、メイン・ダイアログを開きます：

メイン・ダイアログで **Update（更新）**タブを選択し、さらに **Update（更新）**をクリックして更新プロセスを開始します。



ウィルス・スキャンを開始するには、メイン・ダイアログで **Full Scan（フルスキャン）**を選択してから **Scan now（今すぐスキャン）**をクリックします：



ウィルス・スキャンの他のオプションは **Quick Scan（クイック・スキャン）**と **Custom Scan（カスタム・スキャン）**です。

4.4 USBメモリ・スティックからスキャン

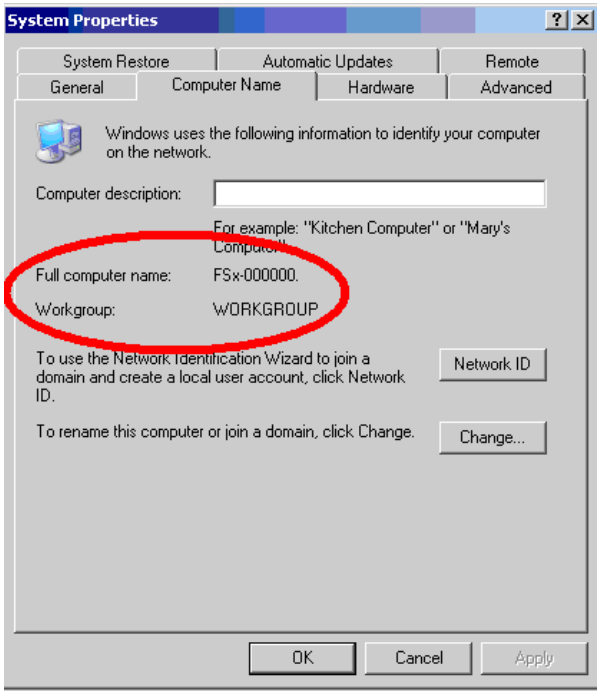
機器の中には、アンチウィルス・ソフトウェアをインストールするリソースを持たないものもあります。これらの機器については、USB メモリ・スティックからスキャンを行うことができます。

4.5 別のPCから機器をスキャン

別のコンピュータからアンチウィルス・ソフトウェアを使ってスキャンを行う場合は、事前に、機器をネットワーク上のドライブとしてマウントする必要があります。
注：機器のハード・ドライブをリモートでスキャンする場合は次に示すようにいくつかの制約があるので、この方法の使用は、他の選択肢を選べない場合だけに限るようにしてください。まず、スキャンできるのは表示されているファイルに限られます。メモリとプロセスはスキャンされません。また、ルートキットを検出することはできません。

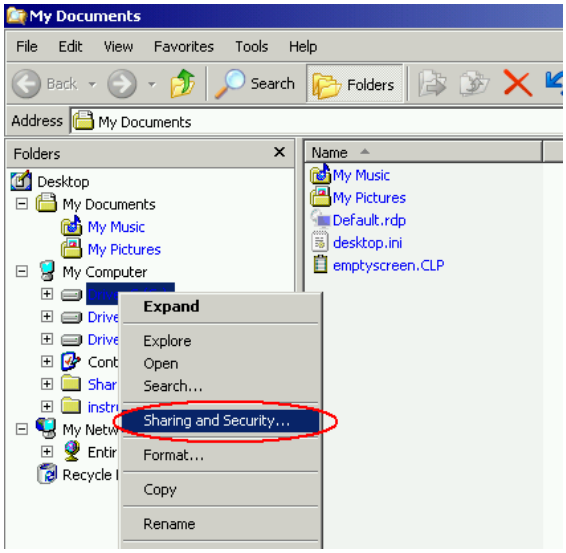
4.5.1 機器のドライブの共有

機器をネットワークに接続します。その機器のコンピュータ名とワークグループを確認します（この情報は、後でその機器をコンピュータからスキャンする時に必要になります）。これらの設定を表示するには、**Windows Start（スタート）⇨ Control Panel（コントロールパネル）⇨ System（システム）**を選択して、表示されたダイアログ内の **Computer Name（コンピュータ名）**タブをクリックします。

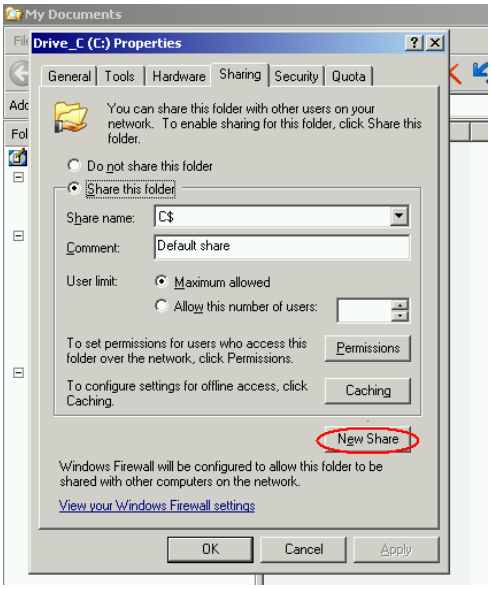


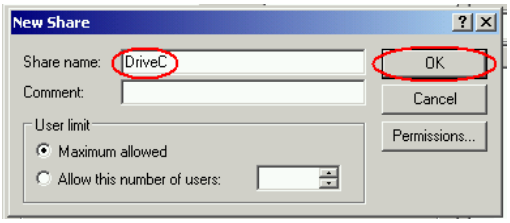
この場合の機器のコンピュータ名は FSx-000000 で、WORKGROUP というワークグループの一部です。

機器上で Windows Explorer を起動して **My Computer（マイコンピュータ）**フォルダを開き、すべてのドライブを表示します。ドライブ C:を右クリックしてコンテキスト・メニューを開き、**Sharing and Security（共有とセキュリティ）**を選択します：



表示されたダイアログ上で **New Share（新しい共有）**を選択して「DriveC」などの名前を入力し、OK をクリックして確定します。



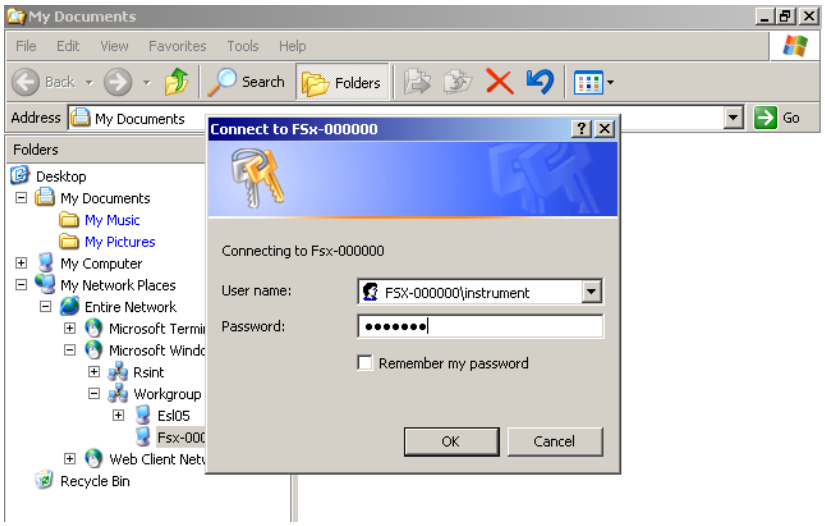


以上で、ドライブ C:の表示が共有ドライブの表示に変更されます：

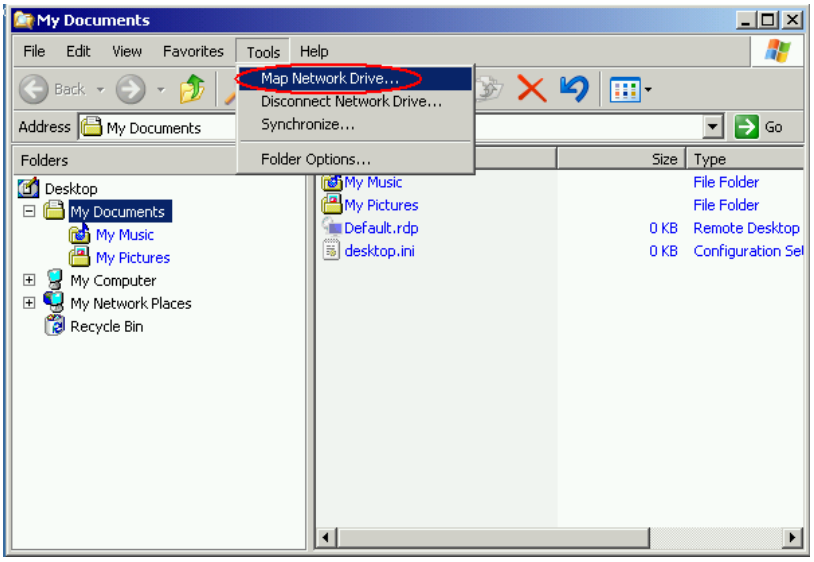
他のドライブについても同じ操作を繰り返します（例えば使用機器のドライブ D:やドライブ E:）。これにより、リモート・ウィルス・スキャンがその機器のすべてのドライブにアクセスできるようになります。

4.5.2　ドライブの割り当てとウィルスのスキャン

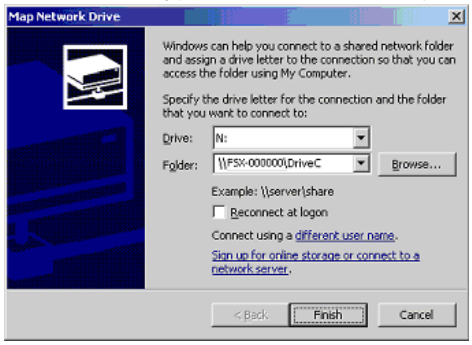
使用している PC 上で Windows Explorer を開き、 **My Network Places（マイネットワーク）⇨ Entire Network（ネットワーク全体）⇨ Microsoft Windows Network ⇨ Workgroup** フォルダを開きます。
ワークグループ設定時にユーザが別の名前を使った場合、**Workgroup** は別の名前で表示されます。
スキャンしたい機器のコンピュータ名をクリックします（たとえば、この例では Fsx-000000）。ユーザ名とパスワードの入力を求めるダイアログが表示されます。**User Name（ユーザ名）**と**Password（パスワード）**を入力します。これらの設定については、機器のマニュアルを参照してください。



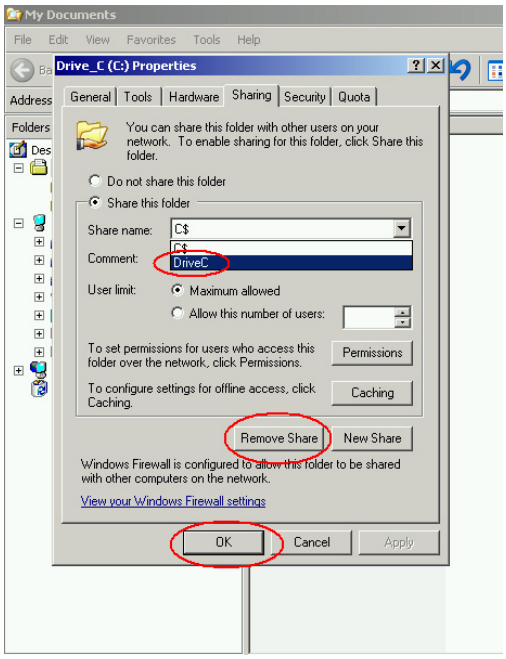
機器のフォルダが右側のウィンドウに表示されます。メニューバーの **Tools（ツール）**を選択して、**Map Network Drive...（ネットワークドライブの割り当て...）**を選択します。



Map Network Drive（ネットワークドライブの割り当て）ダイアログで、最初の共有ドライブ（たとえば機器の「DriveC」）をネットワーク・ドライブ（たとえば、制御 PC の「N:」）として割り当てます。**Browse（参照）**を使用し、ネットワーク・ツリー上で共有ドライブの完全なネットワーク名（たとえば、「\\FSX-000000\DriveC」）を参照することもできます。**Finish（完了）**をクリックして、ネットワーク・ドライブの割り当てを終了します。この例では、これで機器のドライブ C:が制御 PC のドライブ N:に割り当てられました。



他の機器のハード・ドライブについても同じ手順を繰り返して、それらのドライブを制御 PC の空きドライブに割り当てます。
機器のハード・ドライブをスキャンするには、制御 PC 上でアンチウィルス・ソフトウェアを起動します。割り当てた機器のドライブを 1 つ選択して、ウィルス・スキャンを実行してください。ネットワーク・ドライブのスキャン方法については、アンチウィルス・ソフトウェアのユーザ・マニュアルを参照してください。
機器をオリジナル状態に戻すには、その機器に関するドライブ共有を削除する必要があります。Windows Explorer を起動して **My Computer（マイコンピュータ）**フォルダを展開し、すべてのドライブを表示してください。ドライブ C:を右クリックして、コンテキスト・メニューを開きます。プロパティ・ダイアログで **Sharing（共有）**を選択します。



Share name（共有名）リストを展開して「DriveC」を選択し、**Remove Share（共有を削除）**か、**Do not share this folder（このフォルダを共有しない）**ラジオボタンをクリックします。最後に **OK** をクリックして、ドライブの共有を削除します。必要に応じ、他の共有ドライブにもこれらの手順を繰り返します。

5 Windows のパッチとアップデート

Microsoft では、Windows ベースのオペレーティング・システムを保護するために、定期的にセキュリティ・アップデートやその他のパッチを作成しています。これらは Microsoft Update というウェブサイトと、それに対応するアップデート・サーバを通じてリリースされます。Windows を使用する機器、特にネットワークに接続された機器は、定期的にアップデートを行う必要があります。

Windows Update は Windows ベースの製品のみを対象としていますが、Microsoft Update はその他の製品も対象になっています。

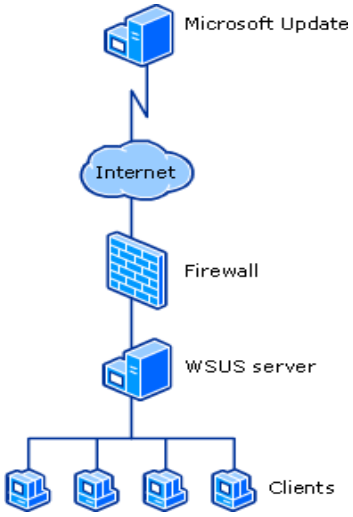
以下の項では、Windows Update Agent のインストールと設定について説明します。これは、機器が最新の Windows パッチとアップデートをダウンロードしてインストールすることを可能にします。

ご使用のローデ・シュワルツ機器にも Windows XP SP2 以降がインストールされていることを確認してください。機器の OS バージョン確認方法については、機器のマニュアルを参照してください。これ以前のバージョンがインストールされている場合は、ローデ・シュワルツの最寄りの営業所または代理店へご連絡の上、更新方法をご確認ください。ローデ・シュワルツ製機器の多くには最新の OS バージョンを使用したリカバリ DVD が付属しており、機器のハード・ドライブの再イメージングを行うことができます。

注：Microsoft Update サービスを使用したり、スタンドアロンの実行型サービス・パックを手動インストールしたりすることによって、機器を SP2 から SP3 にアップグレードすることは推奨**できません**。ほとんどの機器では、OS の再イメージングが必要です。

一般に、Microsoft Update サービスを使用する機器には 2 つのシナリオがあります。

- 機器がインターネットへのアクセスを許可されていて、アップデートを Microsoft Update サーバから直接ダウンロードする。
- 機器が、ユーザの社内アップデート・サーバからアップデートをダウンロードする。



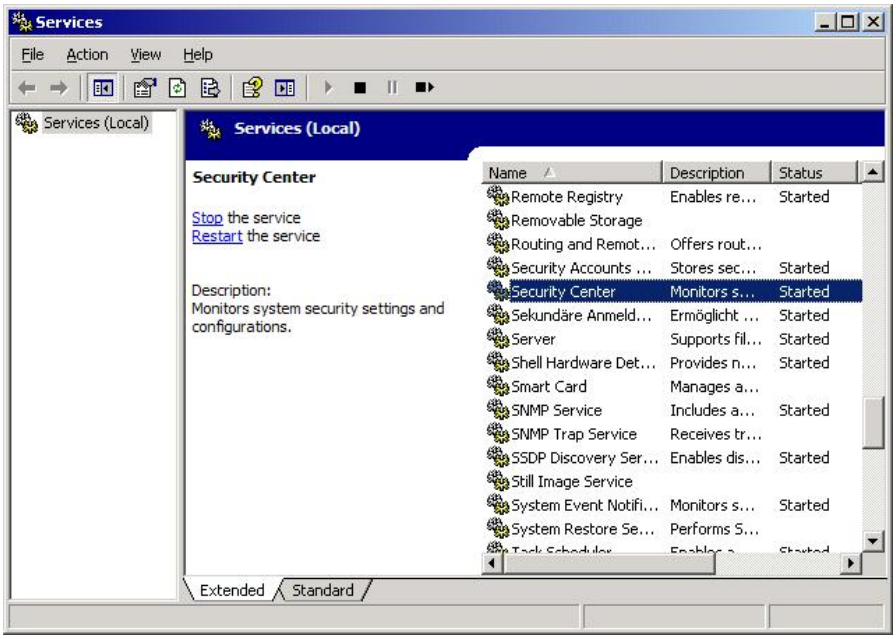
2 つめのシナリオでは、システム管理者が、社内用ファイアウォールの内側に Windows Server Update Services（WSUS）を実行するサーバをセットアップします。このサーバが Microsoft Update の内容と直接同期して、クライアント・コンピュータと機器にアップデートを配布します。

5.1 Windows Update Agentのインストールと設定

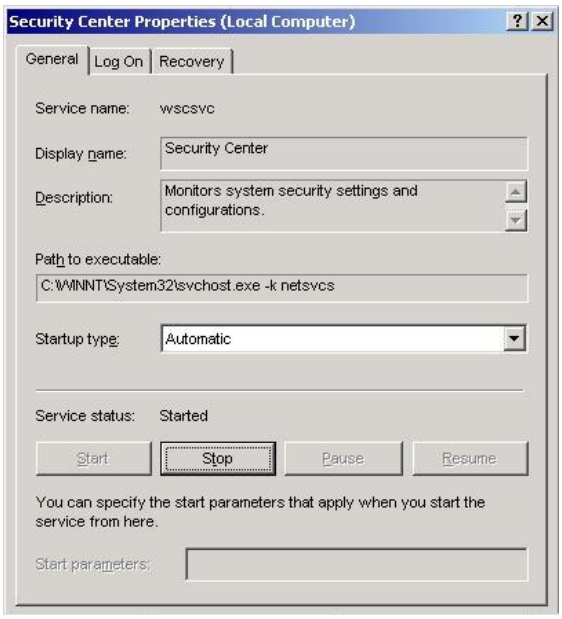
ほとんどのローデ・シュワルツ製機器は、Windows XP Professional の組込機器を対象としたバージョンである Windows XP Embedded をベースとしています。OS に対しては、それぞれの機器の要件に合わせてスケーリングと最適化が行われます。したがって、多くの場合は、Windows アップデート・サービスを個別に機器にインストールする必要があります。
Windows Update Agentのインストーラ**WindowsUpdateAgent30-x86.exe**をMicrosoftのウェブサイトhttp://go.microsoft.com/fwlink/?LinkID=100334からダウンロードして、それをUSBメモリ・スティックにコピーします。インストールは容易で、重要なインストール・オプションもありません。
Windows Update Agent のインストール手順を以下に示します：

- CTRL + ESC キーを押すか **Start（スタート）**をクリックして **Windows Start（スタート）**メニューを開き、Windows Explorer を起動します。
- Windows Update Agent のインストーラが保存されている USB メモリ・スティック上のディレクトリを選択します。
- EXE ファイルをダブルクリックしてインストールを開始します。
- 使用許諾契約を読み、合意する場合は Next（次へ）ボタンを押します。
- インストール・ウィザードの指示に従ってインストールを完了させます。

Windows Update Agent の設定を行うには、**Windows Start（スタート）⇨ Control Panel（コントロールパネル）**を選択してから **Administrative Tools（管理ツール）⇨ Services（サービス）**を選択し、**Security Center（セキュリティセンター）**をダブルクリックして設定ダイアログを開きます：



Startup Type（スタートアップの種類）を **Automatic（自動）**にし、**Start（開始）**をクリックしてサービスを開始します：



設定を終了するには **OK** をクリックします。

5.2 自動アップデートの設定

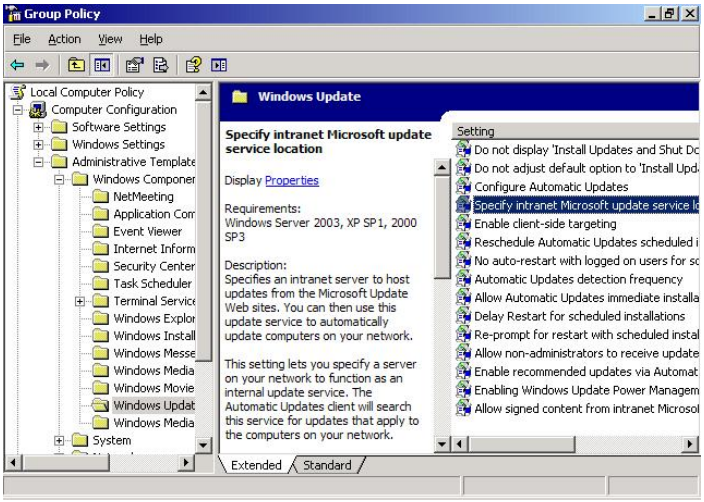
Windows は、自動アップデートを有効にすることにより、重要なアップデートが使用できるようになった時点でそれらをインストールするように設定することができます。オプションのアップデートのダウンロードとインストールは自動では行われません。

自動アップデートを開始するには、**Windows Start（スタート）⇨ Control Panel（コントロールパネル）⇨ Security Center（セキュリティセンター）**を開きます。ダイアログを開いて **Turn on Automatic Updates（自動更新を有効にする）**を選択します。

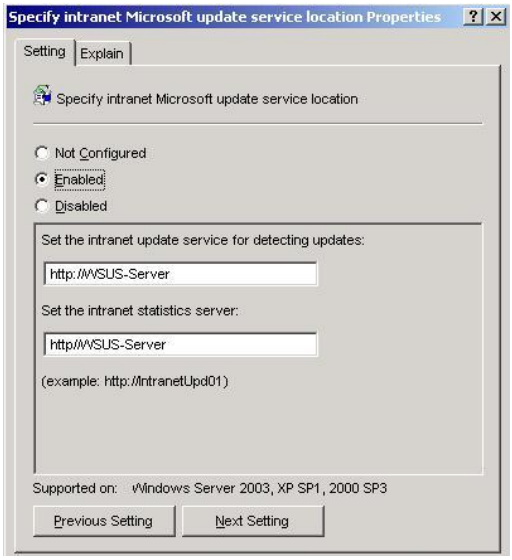
これで、機器の自動更新が有効になります。

5.3 Windows Updateサーバに接続された機器

多くの企業が、そのネットワーク上で Windows Update（WSUS）サーバを実行しています。機器がネットワークに接続されている場合は、WSUS サーバを使用して Windows のアップデートを行うように、その機器を設定することができます。自社のポリシーに従って機器のアップデート構成を設定する方法については、IT 部門またはシステム管理者にお問い合わせください。機器の WSUS クライアントの設定は、**Windows Start（スタート）⇨ Run（ファイル名を指定して実行）**を選択し、**gpedit.msc** と入力してグループ・ポリシー設定を行うことにより、制御または変更することができます。表示されたペーン上で **Computer Configuration（コンピュータの構成）⇨ Administrative Templates（管理用テンプレート）⇨ Windows Components（Windows コンポーネント）⇨ Windows Updates** を選択します。次に、表示をスクロールさせて **Specify intranet Microsoft update service location（イントラネットの Microsoft 更新サービスの場所を指定する）**をクリックし、設定ダイアログを開きます：



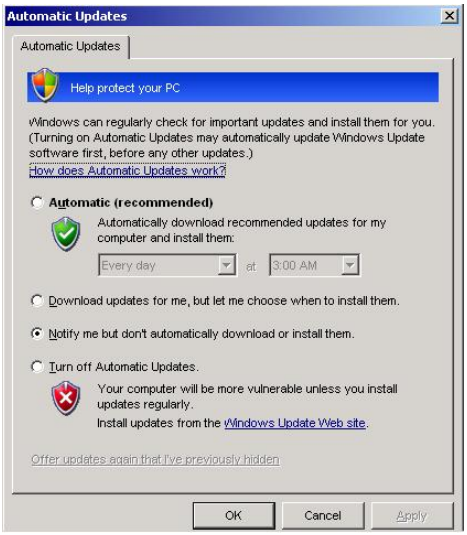
最初に **Enabled（有効）**をクリックしてオンにし、更新を検出するために使用する自社内ネットワーク上のサーバ名を指定します。



注：5.1項に示すように、自動更新が有効になっていることを確認してください。

5.4 自動アップデートの設定

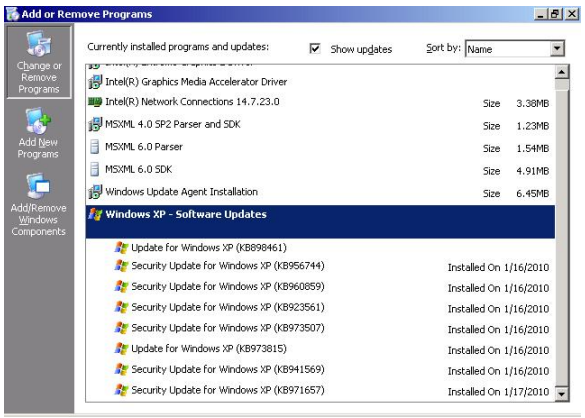
自動アップデートの構成は、非常に柔軟な設定が可能です。たとえば、特定の日付と時刻でアップデートをスケジュールしたり、ユーザへの通知を有効にしたりすることができます。自動アップデートの設定は、**Windows Start（スタート）⇨ Control Panel（コントロールパネル）⇨ Automatic Updates（自動更新）**で管理することができます：



ローデ・シュワルツ製機器については、「Notify me...（更新をダウンロードやインストールする前に通知）」を有効にして、ダウンロードとインストールを実行する前にユーザの確認が必要な設定とすることを強く推奨します。アップデートのダウンロードとインストールを行うとその時点での機器の性能が低下し、リブートが必要になることがあります。したがって、ユーザは、機器の使用中に更新が実行されることがないように、更新プロセスの実行タイミングを管理する必要があります。

5.5 インストールされたアップデートの表示

インストールされたアップデートは、**Windows Start（スタート）⇨ Control Panel（コントロールパネル）⇨ Add or Remove Programs（プログラムの追加と削除）**で表示することができます：



ダイアログ・ボックスにある **Show updates（更新プログラムの表示）**というプロパティが選択されていることを確認してください。

6 関連ドキュメントとリンク

- NSA セキュリティ関連文書
  http://www.nsa.gov/ia/guidance/security_configuration_guides/
- セキュリティ上の脅威に関するニュース
  http://www.securityfocus.com/
- Microsoft Windows Update Agent － ダウンロード・リンク
  http://go.microsoft.com/fwlink/?LinkID=100334
- Microsoftサポート：Windowsの自動実行機能を無効にする方法
  http://support.microsoft.com/kb/967715/en-us
- Microsoft Support：Windows XP サービス・パック 2 における Windows ファイアウォール設定の上級ユーザ向けトラブルシューティング
  http://support.microsoft.com/kb/875357/en-us

ローデ・シュワルツについて
ローデ・シュワルツ・グループ（本社：ドイツ・ミュンヘン）は、エレクトロニクス分野に特化し、電子計測、放送、無線通信の監視・探知および高品質な通信システムなどで世界をリードしています。
75 年以上前に創業し、世界 70 カ国以上で販売と保守・修理を展開している会社です。

ローデ・シュワルツ・ジャパン株式会社
本社／東京オフィス
〒160-0023 東京都新宿区西新宿 7-20-1
住友不動産西新宿ビル 27 階
TEL:03-5925-1288/1287 FAX:03-5925-1290/1285

神奈川オフィス
〒222-0033 神奈川県横浜市港北区新横浜 2-8-12
Attend on Tower 16 階
TEL : 045-477-3570 (代) FAX : 045-471-7678

大阪オフィス
〒564-0063 大阪府吹田市江坂町 1-23-20
TEK 第 2 ビル 8 階
TEL:06-6310-9651 (代) FAX:06-6330-9651

サービスセンター
〒330-0075 埼玉県さいたま市浦和区針ヶ谷 4-2-20
浦和テクノシティビル 3 階
TEL:048-829-8061 FAX:048-822-3156

E-mail: info.rsjp@rohde-schwarz.com
http://www.rohde-schwarz.co.jp/

Certified Quality System
ISO 9001
DQS REG. NO 1954 QM

Certified Environmental System
ISO 14001
DQS REG. NO 1954 UM

ローデ・シュワルツ・ジャパン株式会社
〒160-0023 東京都新宿区西新宿 7-20-1 住友不動産西新宿ビル 27 階
TEL:03-5925-1288/1287 FAX:03-5925-1290/1285

www.rohde-schwarz.co.jp