SOPHOS

そこにある危機、ここにある安心

家庭のセキュリティも アンチウイルスからUTMの時代へ

～無償版「Sophos UTM Home Edition」活用のススメ～

Part 1　IoT 時代のデジタル・セキュリティと UTM

Part 2　Sophos UTM Home Editionを使ってみよう

ソフォス株式会社

IoT 時代のデジタル・セキュリティと UTM

さまざまなデバイスがインターネットに接続され、以前には考えられなかったような新たな利便性を提供する、IoT（Internet of Things）の時代は既に現実になりつつあります。さまざまな情報が瞬時に得られ、高度な情報処理が可能になる一方、従来は問題とならなかった部分にも新たなリスクが生じ始めています。そこでソフォスは、IoT時代に向けた新たなセキュリティ・ソリューションを提案します。

オープンソースがもたらすリスク

IoTと言うと、各種のセンサーなどによって実現されるもので、一部の大企業が活用するもの、というイメージがあるかも知れません。実際にIoTを実現する上で大きな力となったのが、各種のセンサーなどの小型化／高機能化やネットワークに接続するための通信デバイスの低価格化などです。しかし、“全てのモノをネットワークに繋ぐ”という動きは家電製品を含め、あらゆる分野に波及しつつあります。たとえば、ゲーム機やデジタルカメラ、家庭用のテレビなどにインターネット接続機能が組み込まれ、豊富なデータをやりとりするようになってきています。IoTとは特殊なセンサーデバイスに限った話ではなく、既に多くの人が日常生活で利用する電子機器の多くがインターネットに接続されるようになってきているということでもあるのです。

IoTの実現には、ソフトウェアの開発モデルの変化も大きな役割を果たしています。特に目立つのが、オープンソース・モデルで開発されたOSであるLinuxの成熟／発展です。UNIX系OSであるLinuxは当初はインターネットサーバなどで活用されましたが、その後各種アプライアンス製品やデジタル家電などにもLinuxをベースにカスタマイズしたOSが利用されるようになりました。たとえば、スマートフォン用OSとして大きなシェアを占めるAndroidもLinuxをベースに開発されたOSです。

オープンソース・ソフトウェアであるLinuxの利用拡大は、機器のコストを下げ、開発期間を短縮するなどのさまざまなメリットをもたらしていますが、一方でセキュリティ・リスクも存在しています。というのも、さまざまな機器がLinuxベースで制御されている状況では、悪意ある攻撃者にとってはLinuxの脆弱性の研究に集中することでさまざまな機器への浸入や外部からの制御が可能になるわけで、高度な攻撃ソフトウェアの開発に成功すればその成果は大きなものになることが期待できるためです。

従来型セキュリティ対策の限界

家庭におけるPCやデジタルデバイスの活用スタイルも大きく変化してきました。かつては、“一家に一台”のPCを1日数分～数時間程度電話回線経由でインターネットに接続する、という使い方が一般的だった時代もありましたが、いまではブロードバンド接続が普及し、常時インターネット接続が当たり前、接続されるデバイスも複数のPCに加えて無線LAN経由でスマートフォンやプリンター、デジタルカメラやゲーム機、各種AV機器などがインターネットに接続されているという状況が珍しくなくなってきました。1台しかないPCを保護するなら、そのPCにセキュリティ・ソフトウェアをインストールするのが有効な対策となり得ますが、さまざまな機器が家庭内LANに接続されている状況では、その全てにセキュリティ・ソフトウェアをインストールするというのは到底現実的ではありません。そもそも、セキュリティ・ソフトウェアが提供されていない機器も多数存在しています。

そこで、機器単位でのセキュリティ対策の他に、ネットワーク全体を保護するための対

策を導入する、というのがソフォスの提案となります。具体的には、UTM（Unified Threat Management：統合脅威管理）と呼ばれるセキュリティ・アプライアンスを導入するという形になります。ネットワークの入り口に一種の関所を設けることでインターネット側からの悪意ある攻撃を防御し、家庭内ネットワークに接続されている全ての機器を一括して保護する、というのが基本的な考え方です。ネットワークの入り口に置かれる機器として一般的に利用されているブロードバンドルータにもファイアウォール機能が実装されていますが、UTMでは“統合”と言う言葉が示す通り、複数のセキュリティ保護機能をまとめて実装しており、より高度な保護を実現できる点が優位点となります。

ネットワーク保護の現状

ここで改めて、セキュリティ保護の重要性について振り返ってみましょう。初期のウィルスやワームは、いわば悪質な悪戯といったもので、最悪の被害は使用しているPCが正常に動作しなくなることでした。しかし、現在では“サイバー犯罪”という言葉が使われるようになっていることからも分かる通り、悪戯では済まされない深刻な被害をもたらすようになっています。よく知られているところでは、情報の盗み出しからオンラインバンキングなどでの預金の不正引き出しやクレジットカードの悪用など、直接的な金銭被害の報告が増えています。また、ニュース等でも盛んに報道されたのでご記憶の方も多いと思いますが、“パソコン遠隔操作事件”として知られる事件では、マルウェアに感染したPCから本人が知らぬ間に送出された犯罪予告メッセージなどの責任を問われる形で本来は被害者であるはずのPC所有者が犯人と間違われて誤認逮捕されるという事態も起こりました。自宅のネットワークに侵入され、そこに接続された機器を悪用されるような状況になった場合、金銭的被害や社会的信用の失墜など、さまざまな被害を被る可能性が否定できません。

自宅やオフィスのネットワークへの侵入を許してしまうと多大な被害が生じる可能性があるわけですが、一方で特に家庭内LANに関してはネットワーク自体を保護するという発想はまだまだ浸透しているとは言いがたい状況です。UTMは以前から存在してはいましたが、主なユーザーとして企業や学校といった大規模な組織を想定して製品化されており、個人レベルで導入するにはコストやサポート契約の問題など、さまざまな障壁が存在していたのです。UTMの開発当初は家庭内LANがこれほどまでに普及していたわけではなく、LANと言えば基本的には企業などで利用されるもの、という前提があったことも間違いないでしょう。家庭内LANがこれほどまでに急速に一般化し、PC以外のさまざまなデバイスが無線LAN経由でインターネットにアクセスできるようになったのは、UTM提供企業にとっても想定外のスピードだったと言えるでしょう。

オープンソースに基づくネットワーク保護

オープンソース・ソフトウェアの進化がさまざまなデジタルデバイスの進化を促し、急速な高機能化を実現する一方、ソフトウェア・プラットフォームの共通化が進んだことで攻撃者にとってもターゲットを絞りやすくなってきたという現状がある一方で、オープンソースというアイデアはさまざまなメリットをもたらしています。その一つが、高度な機能を実装したソフトウェアを無償もしくはごく低価格で利用可能としたことです。UTMも例外ではなく、従来は企業や法人などが対象だったUTMにも、オープンソースを活用した製品が出てきています。ソフォスでは、2011年7月にAstaro社の買収を行ないました。Astaro社では、“Astaro Security Gateway（Astaro Security Linux）”というオープンソース・プロジェクトを通じてオープンソース・コミュニティの協力の元でUTMの開発を進めていました。この開発成果は現在ソフォスが提供するUTMのソフトウェアとして活用されているわけですが、ソフォスはオープンソースの考え方を尊重し、個人や非営利での利用に関しては無償の“Sophos UTM Home Edition”を提供しています。これは、オープンソース・コミュニティへの開発成果の還元であると同時に、従来コスト的な問題から対象外となっていた家庭内LANに適切な保護手段を提供することでセキュリティを高めて頂きたいという願いを込めた取り組みでもあります。

製品版のUTMは専用ハードウェアに組み込まれてアプライアンスという形で提供されるものが中心で、接続して電源を入れればすぐに使い始められる簡便さも大きな魅力となっていますが、オープンソース・ソフトウェア版では別途適切なハードウェアを準備して自分でソフトウェアをインストールする手間がかかります。とはいえ、個人利用であれば無償で提供されるので、多少の手間と技術的な知識は必要となりますが、家庭内LANのセキュリティを大幅に強化することが可能となります。

そこにある危機、ここにある安心

ソフォスでは、一般家庭にまで迫る危機に対して、UTMによるネットワークの保護とデバイスごとにインストールされるエンドポイント・セキュリティ・ソフトウェアの組み合わせにより、ユーザーが安心してデジタルデバイスを活用し、インターネットにアクセス出来る環境を実現することに取り組んでいます。ソフォスのWebサイトには「無償ツール」のダウンロードが可能になっており、Sophos Anti-Virus for Mac Home Edition をはじめ、さまざまなセキュリティ・ソフトウェアの無償提供を行なっておりますので、こちらも是非ご活用頂きたいと考えています。

Sophos UTM Home Editionを使ってみよう

Sophos UTM Home Editionは、自宅利用者向けに無償で提供されるSophos UTMファイアウォールのソフトウェア版です。VPNやネットワークセキュリティ、メールセキュリティ、Webアプリケーションセキュリティなど、商用製品版と同等の機能を制限なしで実装しており、最大で50IPアドレスまでを保護できます。ソフトウェアのみなので、ユーザーが自分で適切なハードウェアを準備し、インストールを行なう必要がありますが、商用版と同じ高度なネットワーク保護機能を無償で利用できます。ここでは、ソフトウェアの入手からインストールまでの手順を簡単に紹介します。

ハードウェアの要件

Sophos UTM Home Editionは、UTM製品のソフトウェアだけを抜き出した形になっていますので、実際の利用に当たっては適切なハードウェアが必要です。PCやサーバなどで一般的なIntel Architectureのハードウェアで良いので、使わなくなった旧モデルのPCなどを流用することも可能です。Sophosが目安としているハードウェア要件は、

- 1.5GHz以上のプロセッサ
- 最低1GBのRAM（2GB以上を推奨）
- 40GBのHDD等のストレージ容量
- 起動可能なCD-ROMドライブ（インストール時に使用）
- 2つ以上のNIC（ネットワークインターフェイス）

となっています。プロセッサやRAM／HDDの容量に関しては現在の標準的なPCの構成から見ればごく控えめなスペックと言えますので条件を満たすPCを見つけるのは容易ですが、注意すべき点はNICが最低2ポート必要な点です。これは、UTMの動作の仕方に理由があります。UTMはネットワークの途中に挟み込むように設置され、通過するパケット全てをチェックすることでセキュリティを確保します。1つのNICをインターネット側、もう1つをLAN側とし、インターネット側NICから届いたパケットを検査した上でLAN側NICに出力する、というのが基本的な動作となります。自宅に設置する場合は、インターネット側NICをブロードバンドルータのLAN側ポート、もしくはUTM自体をブロードバンドルータと置き換えて回線終端装置などに接続し、LAN側NICをスイッチングハブに接続することになるでしょう。

現在では、PCにNIC（Ethernetポート）が標準搭載されるのはごく当たり前の仕様ですが、複数のNICを標準で備えるPCはまず見かけません。さらに、ノートPCなどでは最近のWi-Fiの普及を受けてEthernetポートを省略し、無線接続のみとしている機種も増えています。拡張スロットを多数備えたタワー型筐体のPCなどであれば対応は簡単ですが、ノートPCを使うにはいろいろ工夫が必要となる点には注意して下さい。

インストールの種別

Sophos UTM Home Editionでは、ハードウェアに直接インストールするほか、仮想アプライアンスとして実行することも出来るようになっています。直接インストールする場合にはSophos UTM Home Editionだけを実行する専用のハードウェアを用意する必要がありますが、仮想アプライアンスとしての実行であればVMwareやWindows Hyper-V、Linux KVMな

どの仮想化プラットフォーム上で動作するので、他の用途で利用しているハードウェアに共存させることが出来ます。リソース要件は専用ハードウェアの場合と同様で、Sophos UTM Home Editionを実行する仮想マシンには1GB以上（2GB推奨）のRAMと40GB以上のディスクスペース、2つ以上のNICを割り当てます。

仮想アプライアンスとして実行する場合は専用のハードウェアを準備する必要がないため、仮想化プラットフォームを既に運用中のユーザーであればほんのわずかな手間でSophos UTM Home Editionを試してみることが可能です。ただし、試用や検証といった用途であればともかく、自宅のネットワークを保護するために運用する場合には、専用のハードウェアを準備して直接インストールする方が望ましいと思われます。理由としては、仮想化プラットフォーム自体や同じ仮想化プラットフォーム上で稼働している他の仮想マシンを仮想アプライアンスのSophos UTM Home Editionで保護するのは簡単ではないことや、システム構成が複雑になってしまうことなどが挙げられます。そこで、ここでは直接インストールする場合に限って説明を行ないます。

ベアボーンPCの利用

UTMのようなネットワークセキュリティ機器は基本的には24時間365日常時稼働し続けることが前提になります。さらに、家庭内で利用することを考え合わせると、ハードウェアに求められる要件もさらに増えることになります。スペースの問題を考えれば、大きなタワー型筐体をむやみに増やすのは難しいでしょうし、騒音や発熱、消費電力の問題からも、大きな冷却ファンを備えたPC用の筐体はできれば避けたいところです。そこで、省スペースの静音PCとして、“ベアボーンキット”などの名称で販売されているハードウェアが魅力的な選択肢となり得ます。フットプリントの小さなマザーボードにCPUとRAMを載せ、ストレージとしてSSDを接続しただけ、といったシンプルなハードウェアですが、中身はインテルアーキテクチャのPCそのものですから、Sophos UTM Home Editionの動作には問題ありません。手のひらに載せられるほどのサイズで動作音もほとんど聞こえませんから、常時動かしっぱなしのUTMとしては理想的です。ただし、一般的なベアボーンキットは省スペースPCというよりは、むしろデジタルサイネージのためのコントローラとしての用途を想定しているため、ディスプレイ出力が充実している一方、複数のNICを備える機種はそう多くはありません。とはいえ、市場にはそうした製品も存在しているので、探してみる価値はあるでしょう。

今回は、日本Shuttle株式会社が販売する“DS6100”というモデルを利用しました。幅165mm×奥行き190mm×高さ43mmというコンパクトな筐体で、選定のポイントは標準でギガビットEthernetを2ポート備えている点です。ソフォスが公式に推奨するということではありませんが、サイズやスペックの面でSophos UTM Home Editionを実行するには都合のよいハードウェアであることは間違いないでしょう。

http://www.shuttle-direct.jp/shopdetail/012004000005/012/X/page1/price/

ソフトウェアの入手

では、まずはSophos UTM Home Editionのソフトウェアを入手するところから始めましょう。Sophosの日本語サイト（http://www.sophos.com/ja-jp.aspx）にアクセスし、ページ最上部の「製品」リンクをクリックします。するとネットワーク保護製品の紹介ページに移動しますが、ここで画面上部の青いバーの左端にある「無償ツール」というリンクをクリッ

クすると、Sophosが無償で提供しているさまざまなソフトウェアを集めたページに移動します。ここには、Androidスマートフォン向けのセキュリティソフトウェアやPC向けのウィルス除去ツールなどもありますので、必要に応じてこれらのツールもご活用下さい。このページの下の方に、Sophos UTM Home Editionのダウンロードボタンも用意されています。「ダウンロード」ボタンをクリックすると、Sophos UTM Home Editionの紹介ページに移動しますが、ここでページの右上に緑色の「ダウンロード」ボタンが用意されていますので、これをクリックするとユーザー登録ページに移動します。最低限、氏名とメールアドレス、郵便番号と企業名（個人の方は"個人"と記入）を入力する必要があります。入力を終えて「送信」ボタンをクリックすると入力したメールアドレス宛てに説明のメールが届きますので、このメールの指示に従ってソフトウェアを入手し、インストールの準備をします。

現時点では送られてくるメールは英文なのですが、重要なポイントは2点だけです。1つは、"How do I Install Sophos UTM?"という見出しのすぐ下に書かれているダウンロードサイトのURLで、もう1つは"Your Personal MyUTM Account"という見出しの下に書かれているMyUTMサイトのURLとユーザー名（メールアドレス）とパスワードです。MyUTMサイトにはSophos UTM Home Editionのライセンス管理などを行なうためにアクセスする必要があるので、この情報は控えておいてください。

使っているメーラーにもよりますが、通常はメール画面上でダウンロードサイトのリンクをクリックすれば直接ダウンロードサイトに移動できるはずです。ダウンロードサイトも英語のみの表記となるのですが、最初の見出しである"Sophos UTM"の下に青い文字で3行のリンクが置かれています。"-UTM ISO for hardware appliances""-UTM ISO for software and virtual appliances""-Sophos UTM Smart Installer"の3つです。Sophosの商用製品であるハードウェアアプライアンスに対応するのが最初の"hardware appliances"で、ソフトウェア版が2番目の"software and virtual appliances"ですので、こちらを選びます。いずれもISOイメージとなっていますので、CD-Rを準備してインストールCDを作成するか、あるいはISOイメージを直接マウントしてインストールを開始することになります。

なお、このリンクをクリックすると画面が切り替わり、"download.astaro.com"というドメイン名のサイトに移動します。これは、Sophos UTM Home Editionが元々はAstaro社のオープンソース・プロジェクトだった名残りですので、心配はいりません。ここで、拡張子が.isoとなっているファイルのリンクをクリックすれば、ダウンロードが開始されます。ダウンロードされるファイルのサイズはCD-ROM 1枚分で、およそ660MBとなります。

ソフトウェアのインストール

ソフトウェアのISOイメージが無事に入手でき、インストール用のディスクの作成が済んだら、インストール作業を始めましょう。具体的なインストール手順はハードウェアによっても異なってきますが、ここでは前述のDS6100にインストールするという前提で紹介していきます。

まず、システムをインストールディスクから起動できるようにする必要があります。DS6100にはCD-ROMドライブはありませんから、別途USB接続のCD-ROMドライブなどを用意する必要があります。USBメモリブートをサポートしているハードウェアであれば、CD-ROMドライブの代わりにUSBメモリを利用できます。DS6100でもUSBメモリブートがサポートされていますが、ここでは直感的に分かりやすいUSB接続のCD-ROMドライブを利用してインストールを行ないます。とはいえ、インストールの作業自体はごく単純で、

特筆するような部分もありません。ダウンロードしたISOイメージを書き込んだインストールディスクを使ってシステムを起動すれば、自動的にインストールが開始されます。

最初に表示される画面には赤字で“WARNIG”とありますが、これはインストールによってHDDのデータが全て消されますという注意喚起です。ここで“boot: ”プロンプトに対して単にリターンキーを打てば、インストールが開始されます。インストールプロセスの途中で何度か確認を求められたり、いったん作業が停止したりしますが、基本的にはそのままリターンキーを打つだけで順次作業が進んでいくので心配はいりません。“Select Keyboard”の画面ではキーボードのキー配列を指定するのですが、日本語配列は選択候補に含まれていません。そこでここでは“English (USA)”を選択しておきます。続いて、“Select Timezone”画面では、システムを運用する場所のタイムゾーンを指定します。日本の場合、“Asia”から“Tokyo”を選べば大丈夫です。続いて、日付けと時刻の設定を行ないます。少々分かりにくいのですが、デフォルトでは“Host clock is UTC”という項目にチェックが入った状態になっています。このチェックをオフにすると、PCのハードウェアクロックの時刻を現在時刻として表示するので、その上で正しい日時が表示されていることを確認しておけば良いでしょう。

“Select Admin Interface”では、NICのリストが表示され、運用管理のためのWebAdminを使う際のインターフェイスを選択します。基本的に、インターネット側から運用管理を行なうことは避けるべきですので、ここではLAN側インターフェイスとして利用する予定のNICを管理インターフェイスとして選択しておきます。次の“Network Configuration”では、先に選択した運用管理インターフェイスのネットワーク設定として、IPアドレスとネットマスク、デフォルトゲートウェイアドレスを入力します。新規にLANを構築する場合はデフォルトのままでも問題ありませんが、既存のLANに追加する場合は、運用中のLANの設定に合わせて適切な設定を行なう必要があります。ちなみに、デフォルトではIPアドレスが“192.168.2.100”となっています。

次の、“64 bit Kernel Support”は、プロセッサが64bit対応の場合に表示されます。現在では、64bitプロセッサが標準と言えますが、デフォルトでは“No”が選択されており、32bitカーネルを選ぶようになっています。ここは“Yes”を選択して64bitカーネルを選択しておくことをお勧めします。“Enterprise Toolkit”の選択は、端的に言えば「オープンソース・ソフトウェア以外のソフトウェアもインストールして良いか？」という質問です。全ての機能を利用するにはオープンソース以外のソフトウェアのインストールが必要なので、ここでは“Yes”を選択します。最後に、ディスクの内容を消去するという確認が改めて表示されるので、リターンキーを打てばHDDのパーティショニングとフォーマットが行なわれ、インストールが開始されます。これにはしばらく時間がかかります。

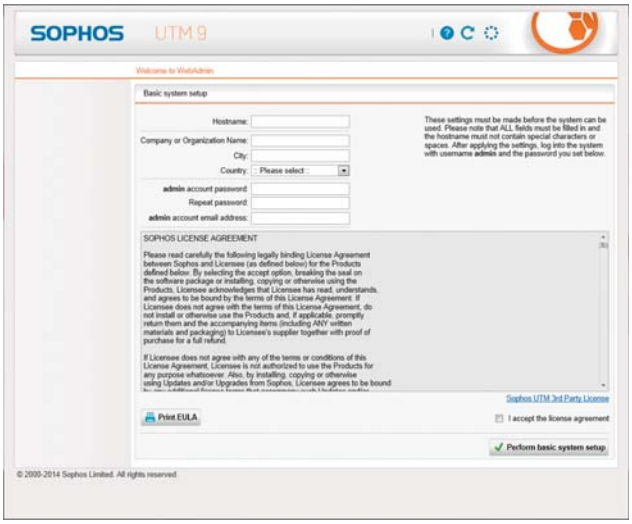
インストール作業が終了すると、“Install Finished”という画面が表示されます。ここで、CD-ROMドライブからインストールディスクを取り出すか、あるいはもう使いませんのでCD-ROMドライブ自体を外してしまいます。また、重要な情報として、以後の運用管理作業はリモートから行なうので、そのためのアクセス情報が中央付近に記載されています。デフォルトのIPアドレスを使っている場合は、“https://192.168.2.100:4444/”というURLにアクセスすることになります。この情報を確認したら、“Reboot”ボタンが選択された状態でリターンキーを打てば作業完了です。システムがリブートすると、最終的にはログインプロンプトが出た状態で止まることになりますが、これについてはもう気にしないで大丈夫です。以後の運用管理等はすべてリモートから行ないますので、本体にはキーボードやマウス、ディスプレイを接続しておく必要すらなくなります。

WebAdmin（管理者用コンソール）へのアクセス

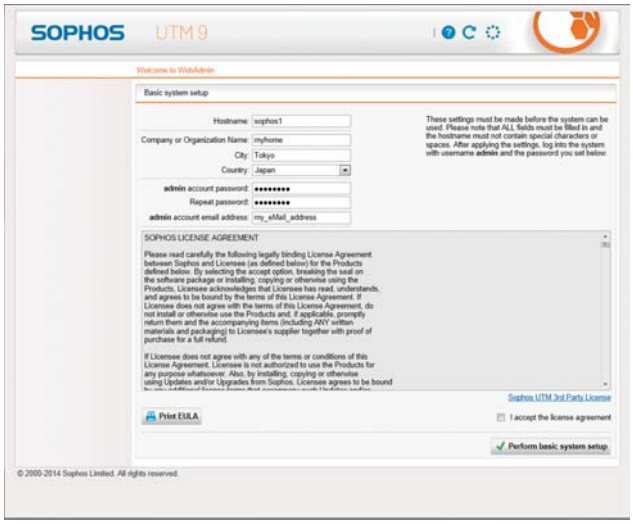
インストールが終わったら、コンソールから直接操作することは以後もう基本的にはありません。以後の設定や運用管理はすべてリモートからWebブラウザ経由でアクセスして実行することになります。このために用意されているのが、Webを利用して運用管理を行なうためのツールである“WebAdmin”です。インストールの最終段階で表示された通り、WebAdminにはLAN側のネットワークに接続されたPCからWebブラウザでUTMの4444番ポートに接続します。

インストール直後にWebAdminに接続すると、インストール作業の続き、といった形でウィザード形式による初期設定作業が自動的に開始されます。この手順を見ておきましょう。おおよそ10ステップの設定画面が順次表示されます。

1. Basic system setup



（初期画面）

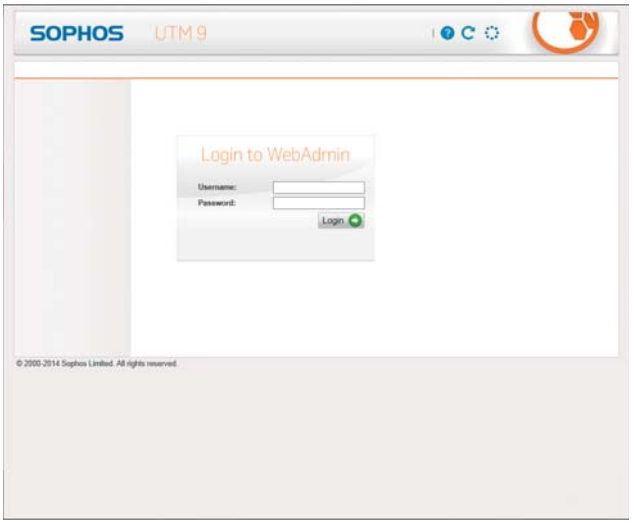


（入力例）

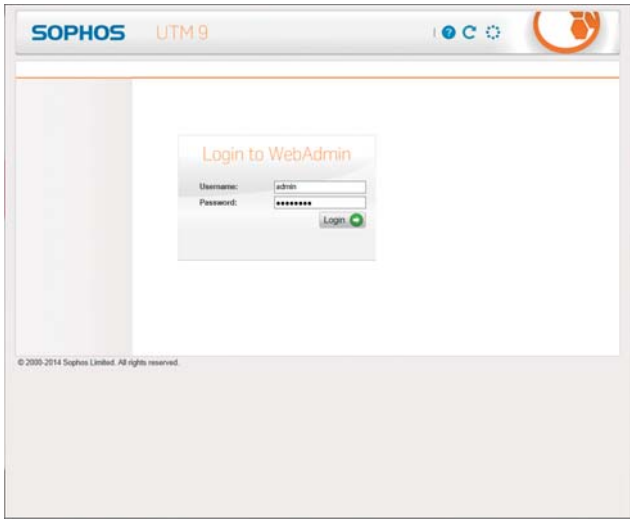
まず、UTMのホスト名や管理者のパスワード登録などを行ないます。なお、画面右側に英文で記載されていますが、管理者のログインIDは“admin”となり、ここで設定したパスワードを使ってログインします。次の画面で早速ログインすることになりますから、このパスワードは控えておきます。

また、この画面ではもう1つの重要な作業として、ライセンスの確認を行ないます。画面の下側に表示されているのがSophos UTM Home Editionのエンドユーザー・ライセンスです。画面右下の“I accept the license agreement”にチェックを入れないと次の画面に進むことはできません。

2. ログイン



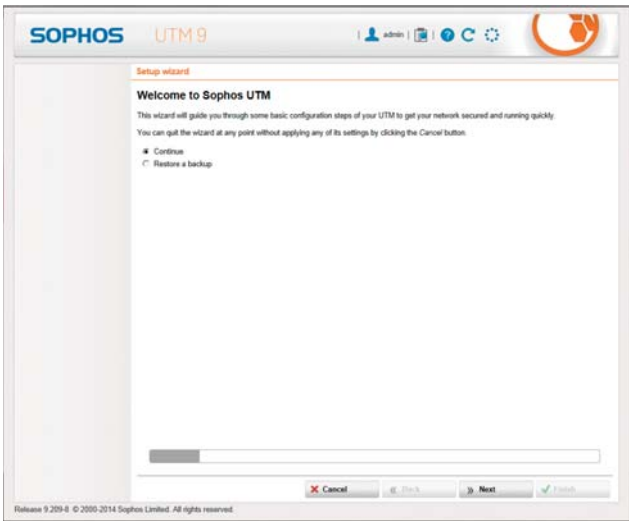
（初期画面）



（入力例）

ログイン画面では、“Username:”の欄に“admin”と入力し、“Password:”の欄に先に設定したパスワードを入力して“Login”ボタンをクリックします。

3. Setup wizard

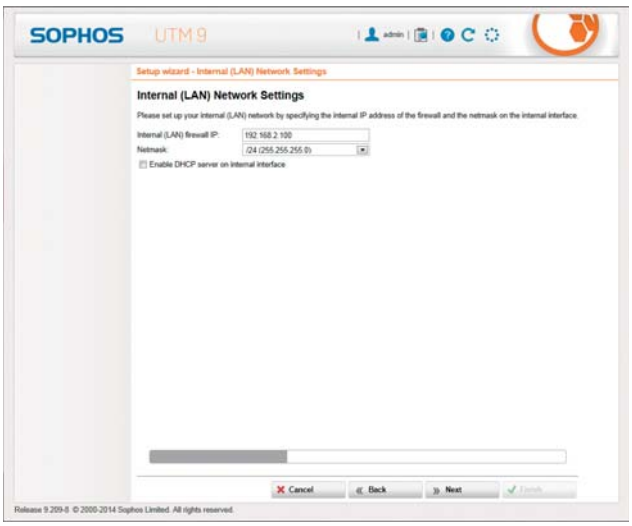


ログイン直後に表示される画面では、ウィザードによる初期設定はいつでも中断可能であることなど、簡単な注意事項が表示されます。ここは“Continue”にチェックが入った状態で次に進みます。

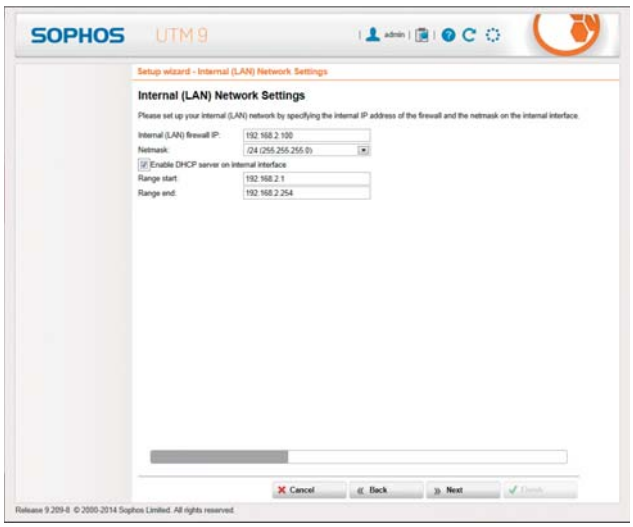
4. Setup wizard - License Installation

“License Installation”では、ライセンスファイルをUTMにアップロードすることができます。Sophos UTM Home Editionは実際に運用する際にはユーザー登録を行ない、有効なライセンスの発行を受ける必要があります。ライセンスファイルは、ダウンロードの際に登録したユーザーのメールアドレスに届いたメールに記載されていた“MyUTM”サイトで入手できるのですが、とりあえずはライセンスファイルなしでも30日間のトライアルライセンスで運用を開始できますので、ここではライセンスファイルの入手は後回しにして、先に進みましょう。後ほど改めてライセンスファイルの登録を行ないます。

5. Setup wizard - Internal (LAN) Network Settings



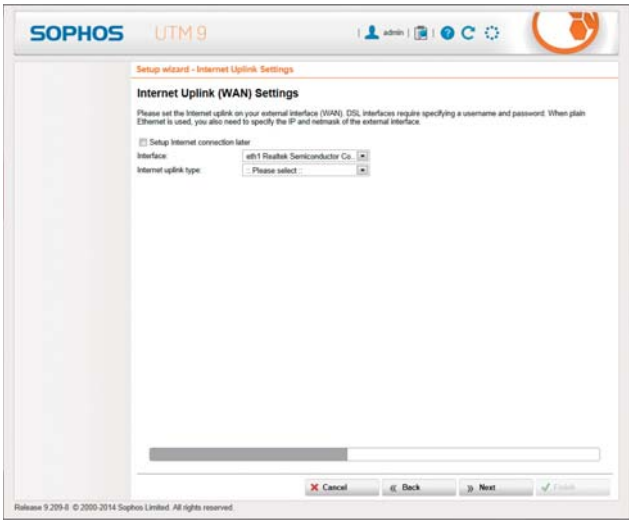
（初期画面）



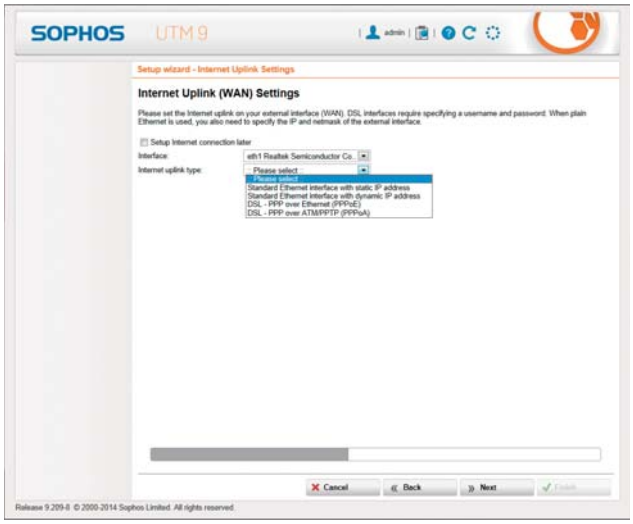
（入力例＋DHCP設定）

“Internal (LAN) Network Settings”から、具体的な初期設定作業に入ってきます。まずはUTMのLAN側NICのIP設定です。インストール時に設定したUTMのLAN側IPアドレスが表示されています。ここでIPアドレスを変更してしまうと設定に利用しているクライアントPCからWebAdminへのアクセスも一度切断されることになりますので、できればインストールの際に正しいIPアドレスを設定しておき、以後変更しないのが望ましいでしょう。なお、LAN側ネットワークに接続されるPC等のデバイスに対しては、UTMがDHCPサーバとなってIPアドレスの自動配布を行なうことも出来ます。通常はDHCPサーバ機能をオンにしておく方が便利です。“Enable DHCP server on internal interface”にチェックを入れておけばDHCPサーバ機能が有効になります。

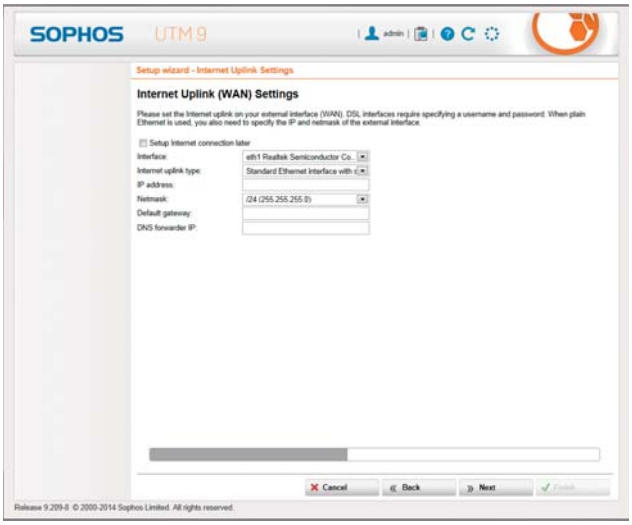
6. Setup wizard - Internet Uplink Settings



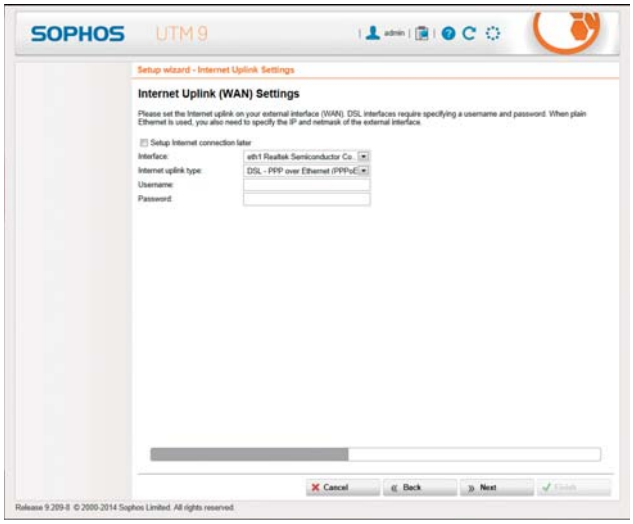
（初期画面）



（メニュー一覧）



（Ethernet設定例）



（PPPoE設定例）

続いて、WAN側（インターネット側）のインターフェイス設定を行ないます。ここで例として使用しているDS6100では、NICが2ポートありますので、LAN側として使用しているNICではない方のNICが自動的にWAN側インターフェイスとして選択され、変更できない状態になっています。そのため、“Interface”の欄はそのままにしておいて大丈夫です。次の“Internet uplink type:”は、接続状況に合わせて4種類の選択肢から適切なものを選び、必要に応じてさらに追加の設定を行なう必要があります。

まずは、UTMの上流側（インターネット側）にブロードバンドルータが存在するかどうかがポイントとなります。Sophos UTM Home Editionは標準的なブロードバンドルータの機能を全て含んでいますから、ブロードバンドルータは不要で、Sophos UTM Home Editionをブロードバンドルータの代替として利用することが可能です。ただし、最近のブロードバンドルータでは無線LANアクセスポイントの機能が標準的に搭載されていますが、これに関してはハードウェアに依存する機能なので利用できるとは限りません。今回サンプルとして使用しているDS6100には無線LANの機能はないので、無線LANを家庭内

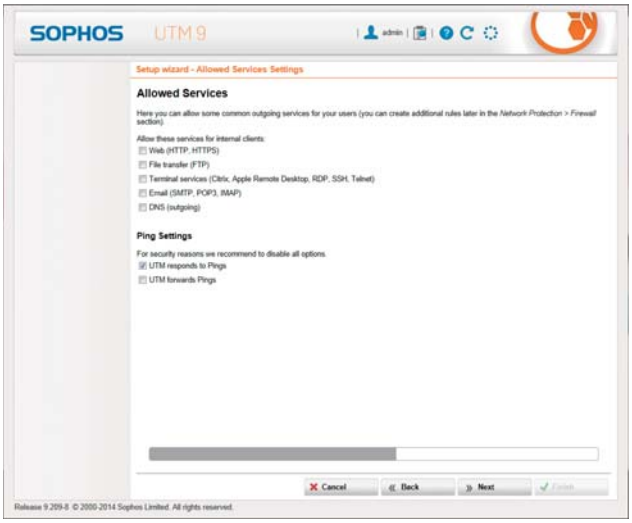
で利用している場合はブロードバンドルータを残しておきたくなるでしょう。ただし、この場合ブロードバンドルータの内蔵ハブに接続されたPCや無線LANで接続されるデバイスに関してはUTMの保護が適用されなくなるという問題も生じますので、充分な検討が必要です。セキュリティの観点からは、UTMのLAN側に既存のブロードバンドルーターを無線LANのアクセスポイントモードとして設置する方が望ましいと言えます（FIG1）。

FIG1.TIF –– UTMの上流側（インターネット側）にブロードバンドルータを残したままにした場合、UTMが保護するのはUTMの下流側（LAN側）に接続された機器（水色の範囲）だけとなる点に注意が必要です。ブロードバンドルータのWi-Fi機能を利用して接続されるデバイスや、ブロードバンドルータの内蔵ハブに接続されたPCなどはUTMによる保護を受けられず、ブロードバンドルータの簡易ファイアウォール機能だけを頼ることになります。

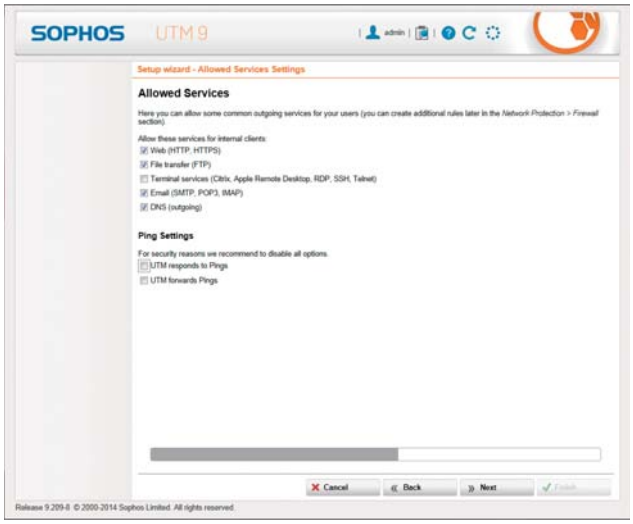
では、具体的な選択について見ていきましょう。UTMのWAN側にブロードバンドルータが存在している場合、UTMは通常のハブに接続される形になりますから、“Standard Ethernet interface”のどちらかを選ぶことになります。UTMのWAN側インターフェイスのIPアドレスをブロードバンドルータのDHCP機能で自動設定する場合は“Standard Ethernet interface with dynamic IP address”を選択し、固定的なIPアドレスを割り当てる場合は“Standard Ethernet interface with static IP address”を選択します。static IP addressを選んだ場合は、追加でIPアドレスを指定するための入力欄が表示されるので、そこで設定します。

一方、ブロードバンドルータを撤去してUTMをブロードバンドルータの代わりに接続する場合は、“DSL”のどちらかを選択します。一般的なブロードバンド接続の場合は“DSL - PPP over Ethernet (PPPoE) ”を選びます。この場合は、ISPと接続するためのIDやパスワードなどの詳細を入力する必要があります。

7. Setup wizard - Allowed Services Settings



（初期画面）

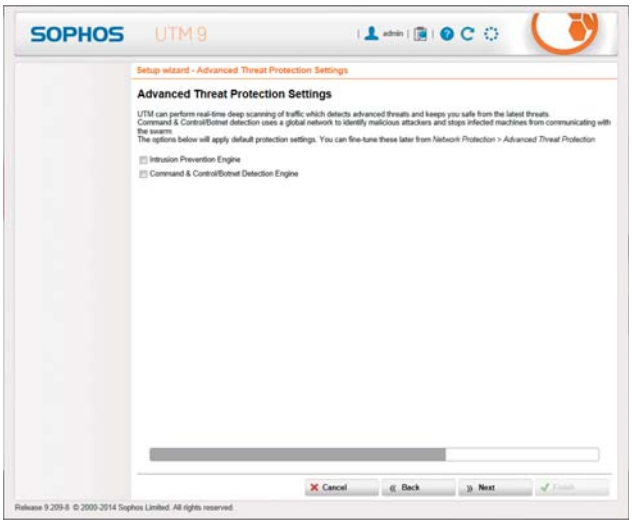


（入力例）

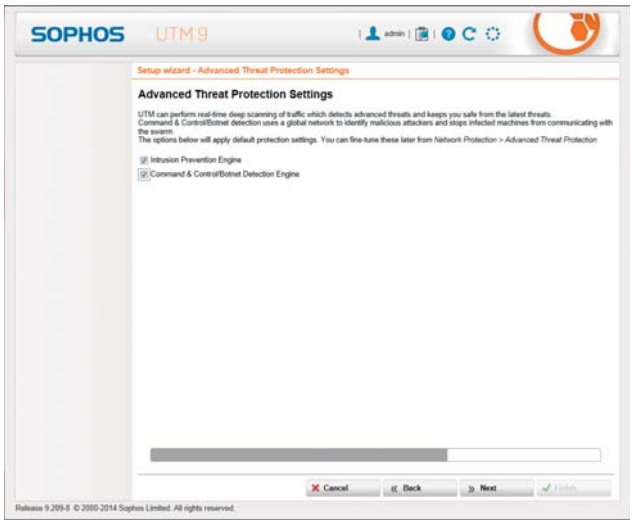
“Allowed Services”では、UTMのLAN側からインターネットにアクセスする際にUTMを通過できるアプリケーションプロトコルを選択します。デフォルトでは何も選択され

ていない状態ですが、Web（HTTP，HTTPS）とEmail（SMTP，POP3，IMAP）を利用する場合は通過を許可する設定が必要です。なお、“Ping　Settings”ではデフォルトで“UTM responds to Pings”にチェックが入った状態になっていますが、特に必要がない場合、このチェックも外してしまって全てオフにしておくことを推奨します。

8. Setup wizard - Advanced Threat Protection Settings



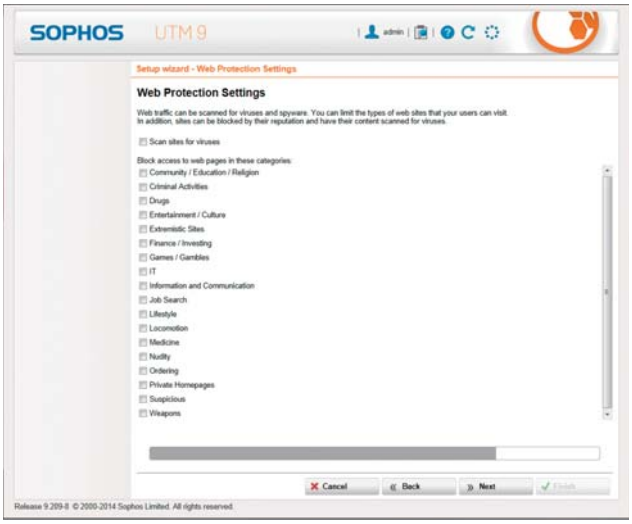
（初期画面）



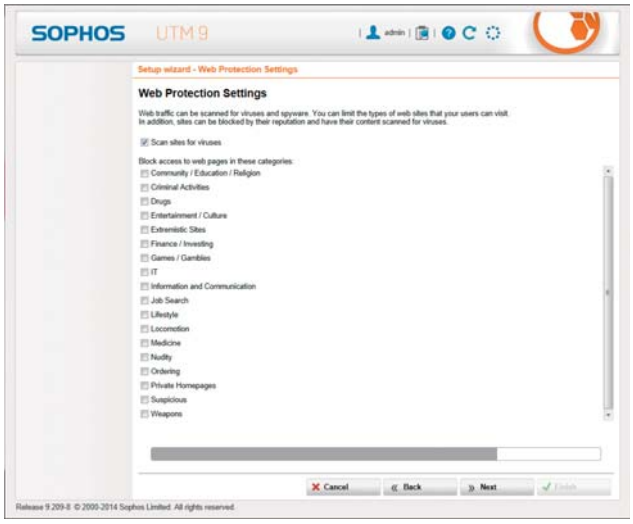
（入力例）

“Advanced Threat Protection Settings”では、IPS機能やボットネット対策を有効にするかどうかの選択を行ないます。デフォルトでは両方ともオフになっていますが、セキュリティを高める上では両方ともオンにしておく方がよいでしょう。ハードウェアの処理能力によっては、全てをオンにしてしまうと処理が重くなってしまう懸念もありますが、DS6100のスペックであれば問題ないでしょう。この辺りは、運用しながら適宜調整していくというやり方でも構いません。

9. Setup wizard - Web Protection Settings



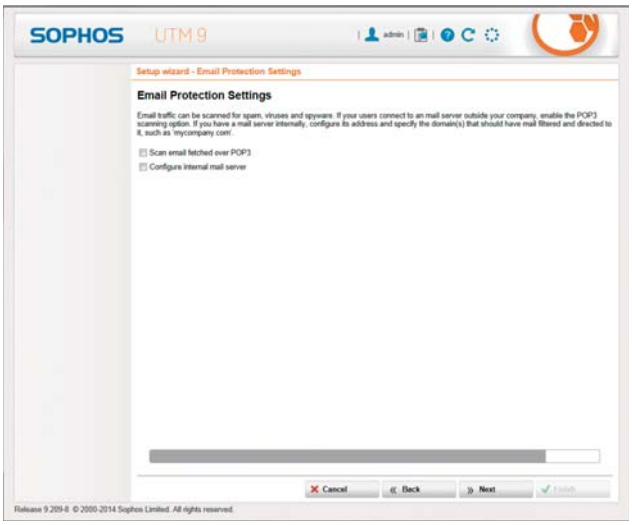
（初期画面）



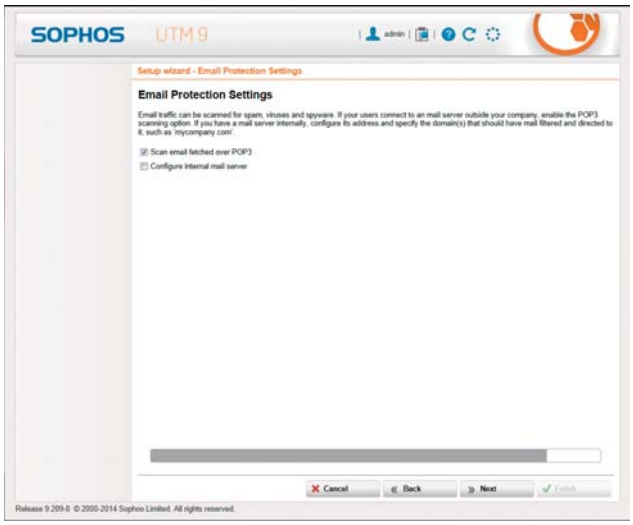
（入力例）

“Web Protection Settings”は、Webサイトに対するウィルスチェックやコンテンツフィルタリング機能の設定となります。先頭にある“Scan sites for viruses”は、Webサイトがウィルスに感染していないかどうかをチェックするための設定で、以後の“Block access to web pages in these categories”は、ブロックするWebページの内容のリストです。犯罪行為やドラッグ、ヌード、兵器といったカテゴリは、小さな子供がいる家庭ではブロックすることもできます。この設定も、運用を開始した後で任意に調整が可能ですから、必ずしもこのタイミングで全てを確定させる必要はありません。

10. Setup wizard - Email Protection Settings



（初期画面）

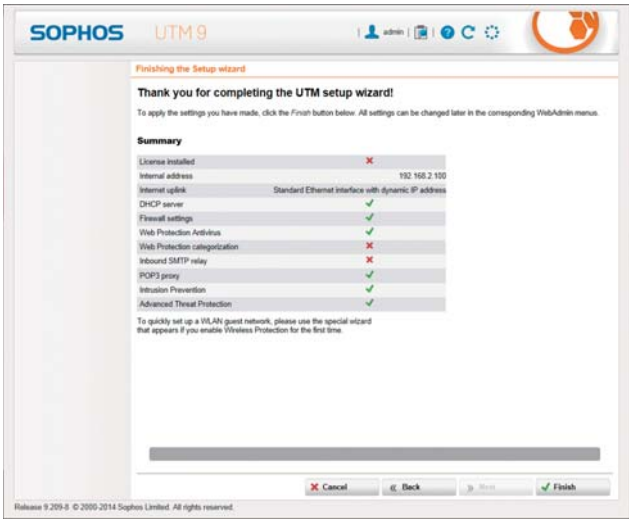


（入力例）

“Email Protection Settings”では、電子メールの保護に関する設定を行ないます。ここでは、チェック対象となるプロトコルの指定を行ないます。外部のメールサーバのメールをPOP3で読み込むのか、LAN側にメールサーバがあってSMTPでメール転送を行なっている

のかの違いです。通常は“Scan email fetched over POP3”にチェックを入れておけば良いのですが、LAN内でメールサーバを運用している場合は別途必要な設定を行なう必要があります。

11. Finishing the Setup wizard



（初期画面）

以上で、ウィザードによる初期設定は完了です。どのような保護を設定したか、概略が表示されますので、確認のうえ、右下の“Finish”ボタンをクリックすればウィザードは終了し、本来のWeb Adminの初期画面が表示されます（図1）。これはいわゆるダッシュボード画面で、UTMの動作状況を一覧し、必要な設定を行なうための基本画面となります。

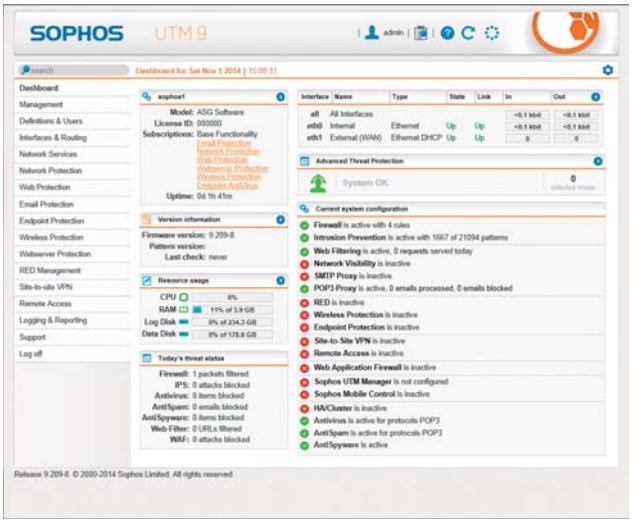


図1

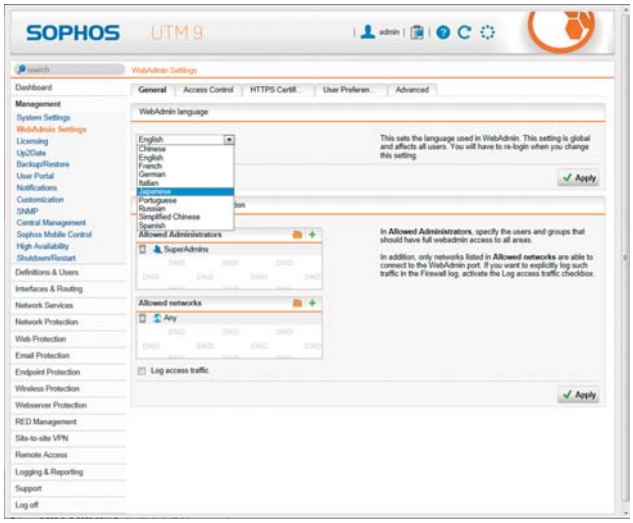


図2

まず、インターフェイスを日本語化します。ここまでのインストール作業は全て英語で行なってきましたが、日常的な運用監視に利用するWeb Adminの画面は国際化されており、任意の言語に切り替えることが可能です。設定は、左側のメニューの“Management”から“WebAdmin Settings”を選び、“General”タブの“WebAdmin language”の欄のドロッ

プダウンリストから任意の言語を選びます。デフォルトは英語ですが、それ以外にも中国語やフランス語、ドイツ語、イタリア語、ポルトガル語、ロシア語、簡体中国語、スペイン語、そして日本語が選択できます(前頁図2)。言語を切り替えると一度ログアウトし、改めてログインし直すことになりますが、このときのログイン画面が既に日本語化されています(図3)。ただし、当然ながら入力するログインIDとパスワードは従来通りに英数字での入力となります。ログインしてみると、表示が全て日本語に切り替わっています(図4)。

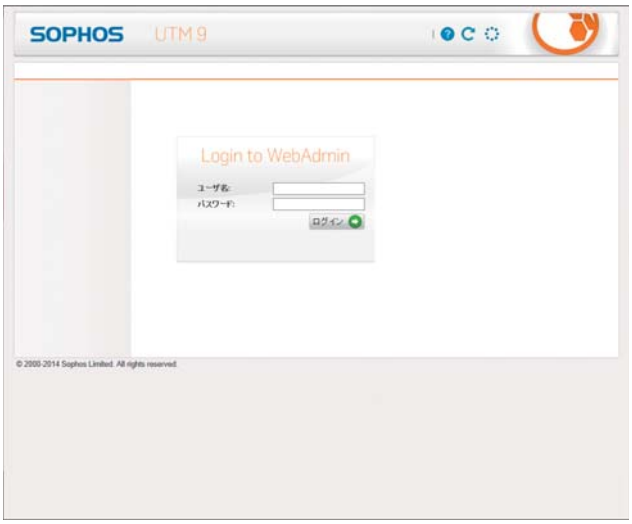


図3

図4

では最後に、ライセンスファイルのインストールを行なっておきましょう。ライセンスファイルは、ダウンロードサイトのURLが記載されたメールの中に書かれていたMyUTMサイトにアクセスして入手します。メールの中にログインID（登録したメールアドレス）とパスワード（Sophos側で設定したもの）が記載されていましたので、この情報を使ってMyUTMサイトにログインします（図5）。メールアドレスとパスワードを入力して“Access MyUTM”ボタンをクリックすると、“MyUTM Licensing Portal”に移動します（図6）。ここで、画面の下の方にある“Shortcuts”のリストの中の“View licenses”アイコンをクリックすると、“License Management”画面に移動します（図7）。画面下部の“Home Use License”欄を見るとライセンスが既に発行済みとなっていることが確認できますので、ここで“License ID”の数字をクリックしてみると、ライセンスの詳細を確認できます（図8）。この画面の下の方にある“Actions”欄の“Download License File”をクリックすれば、ライセンスファイルをダウンロードできます。なお、このライセンスファイルは、登録時に送付される”Sophos UTM Home Use Firewall”のメールにも添付されております。ライセンスファイルはテキストファイルで、いったんアクセスに使用したPCに保存されますので、このファイルを改めてUTMに転送します。

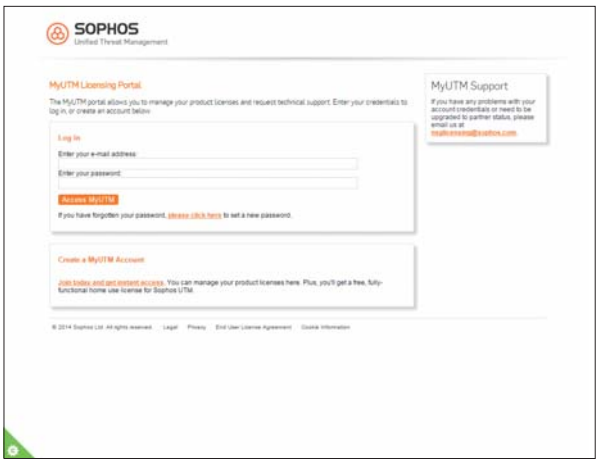


図5

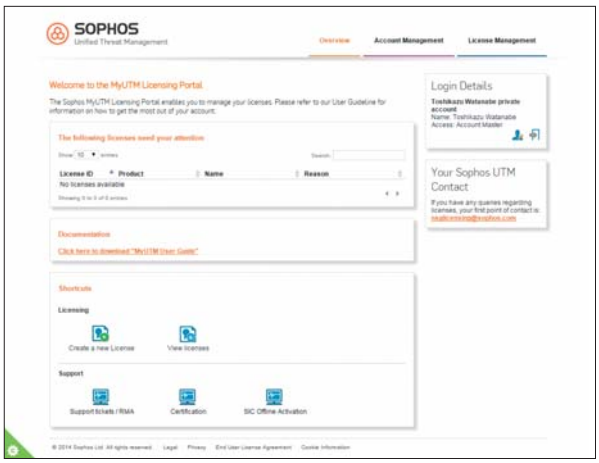


図6

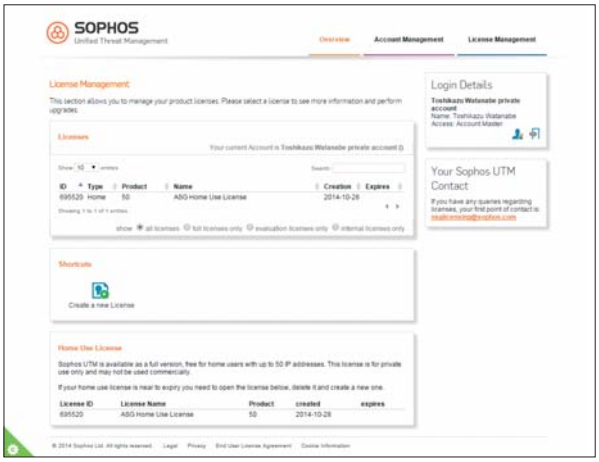


図7

図8

Web Admin画面の左側のメニューから「マネジメント」の「ライセンス」を選び、「インストール」タブを開くと、ライセンスファイルを指定するためのインターフェイスが用意されています（図9）。ここでさきほどダウンロードしたライセンスファイルを指定して「アップロード開始」ボタンをクリックすれば、ライセンスファイルをUTMにインストールすることができます。ライセンスファイルをインストールしなければ30日間の試用版ライセンスで運用されますが、ライセンスファイルのインストール後は3年間の有効期限でUTMを使い続けることができます。ライセンスの発行には費用は掛かりませんので、ライセンスファイルをダウンロードしてインストールすることをおすすめします。

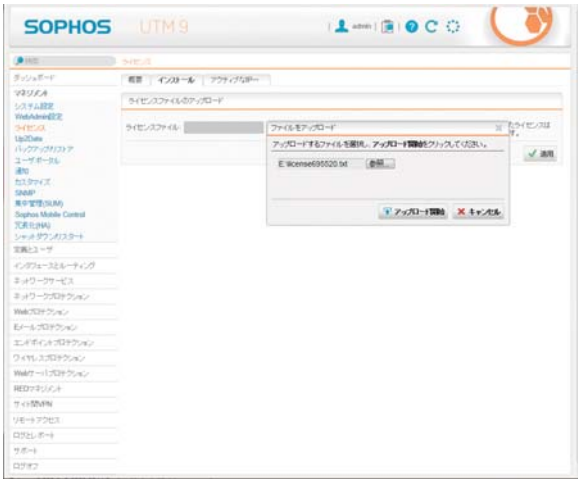


図9

以上の作業が完了すると、UTMを自宅で使い始めることができます。Sophos UTM Home Editionには多彩なセキュリティ機能が実装されています。Web Admin画面の左側のメニューを開けばさまざまな設定画面が表示されますので、実際に確認し、必要に応じて設定を変更することでさまざまなセキュリティ機能を実際に試してみて下さい。

Sophos UTM Certification

Sophos UTM Home Edition
(個人利用に限り無償)
http://www.sophos.com/ja-jp/products/free-tools/sophos-utm-home-edition.aspx

ソフォス株式会社営業部
Tel:03-3568-7550
Email: sales@sophos.co.jp

SOPHOS

2017.08.14DD.dsjp.simple