個人における常時接続時代のセキュアな環境

(株) バガボンド 発行
「無料セキュリティツールで構築するセキュアな環境」から転載
http://vagabond.co.jp/vv/p-fss01.htm
著者：office
E-mail: office@ukky.net　http://www.office.ac/

無料ツールで作るセキュアな環境（1）

～Zone Alarm のインストール～

要望の多い Windows で動作する個人用ファイヤーウォールについて解説する。

個人用ファイヤーウォールは最近急速な広がりをみせるフレッツ ISDN、xDSL、CATV といった個人ユーザのための常時接続環境には必要度が高い。特に JCOM@NetHOME や ZAQ インターネットの安価なサービスにおいてはルータの使用やサーバの構築が禁止されている[1][2]ために個人用ファイヤーウォールは必須である。

無料で使える個人用ファイヤーウォールには Zone labs[3] の Zone Alarm の他に cygate[4] の cygate personal firewall がある。両ソフトとも個人で非商用の場合に無料で使える。日本では Zone Alarm のユーザが多いようで多くの使用報告が web に見られ、人気があるようだ。そこで今回は Zone Alarm のインストール方法をまず解説する。

Zone Alarm の入手とインストール

Zone Alarm のフリー版は zdnet からダウンロードできる[5]。現在の最新版は version 2.1.44（1,745KB）で、動作環境は Windows 95/98/Me/NT/2000 となっている。Windows 95 の場合には winsock2 以上が推奨されている。

ダウンロードした zonalarm.exe を起動すると、「Welcome!」と書かれたウィンドウ出る。ここで書かれている説明はインストール時には他のプログラムを止めて行うようにとの要請と、プログラムが著作権で保護されているという説明である。Next ボタンを押して次に進む。

次に現れる「Important Information!」のウィンドウには注意書きが書かれている。インストールには最小 3MB のディスクスペースが、動作するには 8M 以上のメモリのある環境が必要とされている。また windows95A で winsock1.1 を用いている場合、16bit コードのプログラムによる通信は High security mode においては全てブロックされること、windowsNT においては 16bit コードのプログラムは NTVDM.EXE として一つのグループとして取り扱われることなどが説明されている。Next ボタンを押して次に進む。

User Information のウィンドウでユーザ情報を登録する。最上段の欄にはユーザの名前、次の欄には所属組織名、三段目にはメールアドレスを記入する。所属組織名を空欄のままにすることはできないようだ。最初のチェックボックスは Zone Alarm を Update できるよう登録する場合に、2 つ目のチェックボックスは重要な Update やニュースがある場合に連絡を希望する場合にボックスをクリックしてチェックの印を入れる。チェックボックスに印を入れた場合には、メールアドレス欄には実際に使っているメールアドレスを間違いなく記入しているかどうか注意して欲しい。記入が済んだら Next ボタンで次に進む。

次は「License Agreement」、つまりライセンス許諾条件への同意だ。主な内容は：

個人でかつ非商用の場合にプログラムの使用とバックアップ用としてのコピーが可能であること。（政府の活動や教育目的の場合、60 日を超えて使用できない。）リバースエンジニアリング、改変、再配布が禁止されていること。Update バージョンが出た場合には 1 年以内に Update することができること。

などだ。自分自身でよく確認した後にその内容に納得できれば Accept ボタンを押して次に進む。

Select Destination Directory ではインストールするディレクトリを選択する。何も指定しなければ c:¥Program Files¥Zone Labs¥ZoneAlarm にインストールされる。別の場所にインストールしたい場合は Browse ボタンを押して指定する。

Next ボタンを押すと「Ready to Install!」が出る。インストールしてよいのならまた Next ボタンで進む。

最後に User survey ウィンドウでネット環境について入力する。最初の欄は「モデムを用いた普通のダイヤルアップによる接続」「xDSL」「IDSN」「ケーブルテレビ」「LAN 接続」の選択だ。次は「個人使用」か「ビジネス使用」かの選択である。ライセンスからすると「個人使用」しかないように思われるが「ビジネス使用」にチェックしてもインストールは一応正常に行われるようだ。次の欄は同じローカル LAN 内に何台コンピュータがあるかという数字を入れる。最後の欄は二段目の欄で business use を選んだ場合にだけ社員の数を記入する欄なので普通は記入せずそのままでよい。

Next ボタンを押して Installation Completed! が出たら無事インストールが済んだということなのでプログラムを開始するために Start ボタンを押す。ここですぐプログラムを起

動したくないのなら Don't Start を選べばよい。これでインストールはひととおり終わりである。

起動して出てくる ZoneAlarm tips というウィンドウは起動の度に毎回でてきて邪魔なので、左下の Don't show this message again にチェックを要れて OK ボタンを押そう。

スタートアップフォルダにショートカットを入れておけば Zone Alarm をマシン起動時から自動的に常駐させることができる。スタートアップフォルダからショートカットを消せば好きなときに起動させることができる。

以上でインストールの解説は終わり、次に Zone Alarm の設定方法について解説する。

[1] http://titus-users.monyo.com/service/ALLNET/
[2] http://www.zaq-net.com/faq/faq03.html#q14
[3] http://www.zonelabs.com/
[4] http://www.sygate.com/
[5] http://www.zdnet.com/downloads/partners/zonealarm/download.html

無料ツールで作るセキュアな環境 (2)

～ ZoneAlarm の基本設定～

前の記事では無料で使える個人用ファイヤーウォールである ZoneAlarm [1] のインストール方法について解説した。今回はその続きとして ZoneAlarm の基本的な設定方法について解説する。

ウィンドウ画面

起動して現れるウィンドウには 5 グループの表示画像がある。左からトラフィック表示用バー、ネット接続 / 接続停止表示用の鍵アイコン、ネット接続停止用ボタン、アクティブなネット用アプリケーションアイコン、Help ボタン（Zone Alarm ロゴ）である。

ウィンドウの右上端の×を押せば、タスクトレイ表示になる。タスクトレイ内のアイコンをダブルクリックするとウィンドウが再び表示される。ZoneAlarm の終了はウィンドウ上端か、タスクトレイアイコンを右クリックして "Shutdown ZoneAlarm" を選択して行う。

ウィンドウ下側には 5 つのボタンが並び、左から [ALERTS] [LOCK] [SECURITY] [PROGRAMS] [CONFIGURE] と表示されている。これらボタンを押して現れる画面で詳細設定をする。

アプリケーションの登録

ZoneAlarm は特に設定しなくても、起動しただけで Firewall としての動作を始めている。しかし、インターネットに接続して用いるアプリケーションを使うには ZoneAlarm に個別に登録、設定しなければならない。

ネット用アプリケーション（例:Outlook Express）を起動し、ネットへの接続要求が発生する操作をする（例:メールの受信ボタンを押す）と、クリーム色のバルーンが現れる。その表示は「Outlook Express のインターネット接続を許可しますか?」と言う意味であり、接続を許可するなら Yes ボタンを押す。予期していないアプリケーション（例:スパイウェア、トロイの木馬）がインターネット接続をしようとした場合にも必ずこのバルーンは現れるので、接続を許可しないなら No のボタンを押せばよい。今後このソフトについてこの Yes や No ボタンを一々押したくない場合は、バルーンの左の方にあるチェックボックスをクリックしてチェックを入れ、その後に Yes, No の指定をする。

ここで [PROGRAMS] ボタンを押すと、先ほどのアプリケーション（Outlook Express）が Program 欄に登録されていることがわかる。このように ZoneAlarm 設定後、ネット用アプリケーションを新たに使う度にそのアプリケーションを ZoneAlarm に登録することになる。

この登録画面の Allow connect 欄はアプリケーションの外部への接続を許可するかの設定欄である。左端にチェックが入っている場合には常時許可、真中に×が入っている場合には常時不許可、右端に？マークの場合には接続の度にバルーン表示して許可不許可を決定、という設定となる。この選択設定を Local と Internet について個々に決定する。Local というのは予め登録した同組織内などの比較的信用できるマシン群のことで、Internet は Local 以外のマシン群である。

Allow server は該当アプリケーションのサーバ機能に対して外部のマシンから接続要求があったときにそれを許可するかどうかの設定だ。チェックボックスにチェックを入れた場合には接続許可、つまりサーバを公開したことになる。

右端の Pass Lock のチェック欄は、ウィンドウ上方真中の STOP ボタンなどによってネット接続を停止した場合にも Allow connect、Allow server の設定を優先させたい場合に印を入れる。

セキュリティレベルの設定

[SECURITY] ボタンを押して、セキュリティレベルを Local と Internet それぞれについて設定する。デフォルトでは Local が Medium、Internet が High になっており、特別な理由がなければこの設定のままでよい。

セキュリティレベルを Low にすると [PROGRMS] で設定したこと以外、何も保護されない。Medium の場合、ファイ

ルやプリンターの共有サービスがブロックされる。しかしサーバを立てていたりしてポートが開いていてもブロックはされない。Highにした場合には、[PROGRMS]で設定したものが使用している場合以外、Portは全て閉じられる。Block Internet serversにチェックするとサーバ機能は全て閉じられる。

“*.VBS e-mail attachment protection”はe-mailに添付されてきた.vbsファイルによってVisual Basic Scriptが実行されないようにする設定である。デフォルトでチェックボタンはオンになっている。この設定によってメールソフトとの競合などが起こるなどしない限り変更の必要はない。

デフォルトではLocalとして登録されているマシンはない。Localに登録したいマシンがある場合にはAdvancedボタンを押してそれらを選択、決定する。Adapter Subnetsの欄にはネットワークカードに対して設定された同一セグメントのアドレスが最初から記載されている。左側のチェックボタンに印を入れればこれらがLocalとして決定される。これら以外にLocalとして信用するマシンがあればAddボタンを押して、ホスト名やIPで登録することが可能である。

警告

不審アクセスの履歴のチェックや、logファイルの設定などは[ALERTS]ボタンを押して行う。

Today"s summary欄にはZoneAlarmを起動してからのトラフィック量が示され、左側は送信バイト数、右側は受信バイト数である。

Current alerts欄ではZoneAlarmを起動してからのその時までの外部からの不審なアクセスのlogが見れる。不審アクセスの内容について詳しく知りたければMore infoボタンを押すとZone Labs,Inc.のWebサーバに接続され、ブラウザにその詳細な説明が表示される。ClearAlertsボタンを押すと、Current alerts欄の内容が消去される。

Alert settings欄の上段ではLogをtextファイルとして記録するかどうか、下段では警告をPopupウィンドウで表示させるかどうかが選択できる。右側のDelete Log Fileボタンはlogファイルの中身を消去するためのものだ。

[1] http://www.zonelabs.com/

無料ツールで作るセキュアな環境 (3)

～ZoneAlarmの詳細～

前の記事までに無料で使える個人用ファイヤーウォールであるZoneAlarm[1]のインストールと基本設定について解説した。今回はその続きとしてZoneAlarmのその他設定方法などZoneAlarmに関する詳細を解説する。

インターネット接続の停止

ZoneAlarmのウィンドウの真中にあるSTOPボタンを押すと、[PROGRAMS]で予め設定した通信以外は全てブロックされるようになる。この時STOPボタンの左隣の鍵アイコンは鍵のかかった状態に変化し、下に赤地でLockedと表示され、またタスクトレイ内のアイコンも鍵に×印がついたものになる。

再びSTOPボタンを押せば通常の通信設定に戻る。STOPボタンの隣の鍵は開いたものに変化し、その下に緑地でUnlockedと表示さる。タスクトレイ内のアイコンはトラフィック表示に変化する。

また[LOCK]ボタンを押して表示されるウィンドウで自動ロックを設定することができる。自動ロックとはマシン操作や通信が一定期間ない場合に通信ロックする機能だ。設定はAutomatic LockのEnableのラジオボタンをクリックして印を入れて行う。Disableに印が入っているときには自動ロックはされない。

“Engage Internet lock after”の左のラジオボタンに印を入れ、数字（分）を指定入力すれば、通信が途切れたまま指定した時間が経つと自動的にロックされるようになる。ロックがかかるまでの残り時間は鍵アイコンの下に表示される。

“Engage Internet Lock when screen save activates”の左に印を入れた場合にはスクリーンセーバーが起動している間はロックされている。

“Lock mode to use while the automatic lock is engaged:”の欄の二つのラジオボタンは、[PROGRAMS]で予め設定した通信以外を自動ロックしたい場合には上段を、全ての通信を自動ロックしたい場合には下段を選択するとよい。

その他の設定

Configuration欄の左のチェック欄に印を入れるとインターネットへのアクセスがある毎にZoneAlarmのウィンドウが最前面に来るようになる。右のチェック欄に印を入れるとスタートアップフォルダに登録しなくてもマシンの起動時にZoneAlarmが自動起動される。

Update欄はZoneAlarmのUpdate情報に関するものだ。

個人における常時接続時代のセキュアな環境

チェックボックスに印を入れておけば自動的にZone LabsへUpdateがあるかどうか起動時に確かめてくれる。Check for Updateボタンは手動で確かめるためのものだ。Updateがあった場合Get updateボタンで新しいZoneAlarmをダウンロードできるようだ。

登録情報を変更したい時にはChange Registrationボタンを押す。但しフォントの問題によって日本語で入力された情報は文字化けして読めなくなっていることがある。

ZoneAlarmの特徴

ZoneAlarmは使用するアプリケーションを明示的に指定し、それ以外のマシン内部からネットワークへの接続要求を禁止している。このため、トロイの木馬によるバックドアなど予期せぬプログラムによって使用者に気付かれないうちに外部へ接続されてしまう危険性が大幅に低減されている。これはWindowsマシンにとっては、踏み台にされる危険性が下がっていることを意味する。このことはマシンで高額なデータを扱っているわけではない個人ユーザにとっては最も優先されるべき安全性が確保されていると評価できる。

一方、[PROGRAMS]のAllow Serverの設定で許可されたサーバへの接続要求があった場合、その通信内容までは解析していないようである。従ってサーバを立てている場合、バッファオーバーフローなどのサーバプログラム固有の脆弱性を防ぐことはできないようだ。

Security Levelを一括して設定できるのはネットワークに詳しくない一般ユーザにもわかりやすく便利である。しかし特定のプログラムとZoneAlarmの間で競合が起こり望むネットワーク機能が使えなくなった場合には、Portごとの細かい設定ができないためSecurity Levelを変更してマシン全体の堅牢性を低下させて対応するしかない。

ZoneAlarm情報

ZoneAlarmを無料で使っている場合にはZone Labs社からサポートはなされない。日本語でZoneAlarmの設定方法などが掲示板などで情報交換されている個人サイトとして以下の2サイトがある。

・Firewallと森遊びの部屋
http://members.tripod.co.jp/eazyfox/

・セキュリティUP! - ZoneAlarm
http://gto.freehosting.net/

「Firewallと森遊びの部屋」ではZoneAlarmのみならず数多くの個人用ファイヤーウォールについて解説、議論されている。また「セキュリティUP! - ZoneAlarm」ではZoneAlarmと競合するアプリケーションの情報が多く流されており、例えば桜時計がうまく作動しないとの報告が何件かなされている。

ダウンロードサイト

現在のZoneAlarmの最新版は2.6.362
http://download.cnet.com/downloads/
0-10105-108-57636.html

関連プログラム

ZoneAlarmを使いやすくする無料のプログラムには次のようなものがある。動作保証されているわけではないので、使用にあたっては自己責任であることに注意していただきたい。

・日本語化パッチ:
http://gto.freehosting.net/

ダイヤログ等の一部表示を日本語化する。
http://www.ryulife.com/net/zonealarm.html
http://etcd.virtualave.net/zaj.html

・ZA Log Lookup:
http://www.tznet.com/ghost/

ZoneAlarmのlogに記されたIPアドレスをドメインに変換して表示する。

・ZoneLogAnalyzer:
http://zonelog.co.uk/

ZoneAlarmのlogを様々な方法で見やすく整理して表示できる。

[1] http://www.zonelabs.com/