ISSN 0915-6372

NATIONAL INSTITUTE FOR FUSION SCIENCE

所内向けウイルス定義ファイルサーバの開発
Development of the Intramural Server for Disributing the Virus-definition-file.

山本孝志
T. Yamamoto

(Received - Feb. 1, 2007)

NIFS-MEMO-52 Feb. 2007

RESEARCH REPORT
NIFS-MEMO Series

TOKI, JAPAN

所内向けウイルス定義ファイルサーバの開発

山本 孝志
核融合科学研究所 計算機・情報ネットワークセンター

Development of the Intramural Server for Distributing the Virus-definition-file.

Takashi YAMAMOTO
Computer and Information Network Center, National Institute for Fusion Science

Abstract

Computer and Information Network Center has the site license of the vaccine, Symantec AntiVirus for Corporate Edition (SAV CE), and is distributing to our staff in "National Institute for Fusion Science" for protecting the virus. It is important to use the latest virus definition file for protecting ones PC from the current virus which is born day by day.

There are two methods to obtain the fresh virus definitions for SAV CE, LiveUpdate and Intelligent Updater. LiveUpdate can minimize the traffic to send only the difference between server's definition and client's one. Intelligent Updater is convenient for off-line update because it comes from a single file. Although the clients can directory connect to the server of Symantec Corp. to update the virus definitions, we prepare the in-house servers for LiveUpdate and Intelligent Updater to reduce the traffic to the Internet and stable distribution for our staff.

In this report, we describe these update systems, especially how to keep automatically the newest virus definitions on our server. This system is a part of automation of the system administration. The technique using "Services for UNIX" written in this report would be useful for various tasks, particularly the cooperation between UNIX system and Windows system.

keywords: PC security, automation, network administration, virus definition, Services for UNIX

概要

核融合科学研究所では所員の PC 端末に対するウイルス対策としてシマンテック社 Symantec AntiVirus Corporate Edition (SAV CE) のサイトライセンスを取得し配布している．時々刻々と新しい種類が発生するウイルスに対応するためには，常に最新のウイルス定義ファイルを使用することが重要である．SAV CE のウイルス定義ファイルを更新する方法は，定義ファイルの差分のみダウンロードが可能なる LiveUpdate と，1 つの定義ファイルで配布する Intelligent Updater パッケージの 2 つの方法がある．利用者はシマンテック社が用意したサーバに接続してウイルス定義ファイルを更新することが可能だが，所外へのトラフィックを減少させるため，また，安定した配布を行うため，ウイルス定義ファイルを所内から両者の方法で配布できるシステムを開発した．

開発したシステムは，OS の異なるサーバを協調させるためマイクロソフト社 Windows XP に Services for UNIX というモジュールを利用した．各種業務の自動化において，本報告に述べる手法が活用される機会があれば幸いである．（1999 年 6 月にワクチン配布を開始，2004 年 4 月に自動更新システムの稼動開始.）

1　ワクチンの導入

1.1　深刻化するウイルス

セキュリティ修正プログラムの適応を行っていない OS をインストールした直後のパソコン（PC）をインターネットに接続すると 10 分以内にウイルスなど不正なプログラムが侵入するという [1, 2]．ウイルス（ワーム）とは自己増殖機能を持つプログラムのことで，感染すると PC のファイルを改ざんする他，ネットワークに接続している他の PC へアプリケーションファイル（Word, Excel ファイル），電子メール，ファイル共有などを利用して自分自身を送りこむ感染活動を行う．すなわち，ウイルスに感染するという被害をうけた PC は，他の PC からみればウイルスを送ってくる加害者の側面を同時に持つ．さらに，最近のウイルスは定期的に感染した PC の内部情報を特定のサーバへ送信し，自己更新，別種のウイルスのダウンロード，他のサイトへの攻撃等外部からの指令を待つ独自のネットワーク（ボットネット） を構築するものある．

1.2　ワクチンによる防御

大多数のウイルスの侵入経路の電子メールであり，何らかの方法で受信者に添付ファイルを開かせ，ウイルスを実行させる．過去には，OS のセキュリティホールを利用し，添付ファイルを実行しなくてもメッセージを見るだけで感染行為を行うものもあった．また，感染したウイルスは同じネットワークに接続された他の PC にファイル共有などを通じても増殖活動を行う．ワクチンは常時 PC 内に起動され，これらファイルの変更を監視し，これらの感染を未然に防ぐものである．

ワクチンを配布する以前は，大規模な感染事故こそは発生しなかったが，ウィルスに感染したマイクロソフト Word 文章を研究所から他の研究機関へ送り，先方より注意を受ける事象が徐々に増加していた．この様な状況を考慮し，計算機センター[*1]では，ウイルス対策として 1999 年 6 月より，シマンテック社 Symantec

[*1] 現，計算機・情報ネットワークセンター.

AntiVirus Corporate Edition (SAV CE) [*2]のサイトライセンスを取得し所員へ配布している[*3]．以下，本報告では，Windows 用 SAV CE の管理を中心に述べる．

1.3 ウイルス定義ファイルとは

ワクチンは一度インストールするだけでは完全ではない．一般にワクチンはウイルスの特徴（指紋のようなもの）をデータベース化して対象となるファイルと比較することによりウイルスを検知する．そのため最新のデータベースを用いないと日々刻々と出現している新種，変種，亜種のウイルスには対応することができない． ワクチンを販売している会社の研究機関は 24 時間体制でこれら新種ウイルスを調査し，その結果をウイルス定義ファイルとして利用者に提供している．シマンテック社の場合，Windows 用ワクチンのウイルス 定義ファイルは毎日更新されており，新種の発生による大規模感染などの緊急時には，一日に数回の更新が行われている．

1.4 ウイルス定義ファイルの更新方法

シマンテック社によるウイルス定義ファイルを更新する代表的な方法として，LiveUpdate と Intelligent Updater がある [3].

LiveUpdate は PC 上のワクチンがシマンテック社の用意する LiveUpdate サーバに接続し，必要なファイルのみダウンロードを行い更新する．ウイルス定義ファイル以外にもワクチンの機能を改善するモジュールが配布されることもある．SAV CE には自動 LiveUpdate 機能があり定期的に LiveUpdate サーバに接続しウイルス定義ファイルを更新することができる．緊急時を除きシマンテック社による LiveUpdate の更新頻度は，SAV CE 10.0 以降は毎日，それより古いバージョンは毎週である．なお，LiveUpdate の場合，ネットワークに接続する必要があるため，ウイルスの感染の疑いがある PC には利用できない．

一方，Intelligent Updater はウイルス定義ファイルを更新するに当たり必要となるファイルを 1 つにまとめた状態で配布される．そのためウイルス感染の疑いがある PC に対してもネットワークを外した状態でも USB メモリ等で転送し，更新することができる．また，何らかの原因で LiveUpdate 機能が働かない場合も Intelligent Updater により更新することができる場合が多い．シマンテック社による更新頻度も毎日と比較的データベースの鮮度が高い．欠点としては，LiveUpdate よりもファイルのサイズが大きくなること（15MB 以上），提供される機能はウイルス定義ファイルのみでありワクチンのモジュールについての更新は行われないことである．

1.5 所内向けウイルス定義ファイルサーバ

ウイルス定義ファイルの更新のためには，いずれの方法でも PC はシマンテック社のサーバにアクセスを行う必要がある．現在ではネットワーク環境も改善され，ウイルス定義ファイルのダウンロードに待つことはなくなったが，導入当時は対外回線が細く[*4]，特に急いで更新を行う必要がある緊急時には所内からのアクセスが集中し，タイムアウトとなり，結果として更新が不能となることが予想された．

[*2] http://www.symantec.com/Products/enterprise?c=prodinfo&refId=805&ln=ja_JP

[*3] 2006 年度では Windows 1300 台, Macintosh250 台のライセンスを提供している．

[*4] ワクチンを導入した当時（1999 年）は海外回線が最大 256kbps であり，常に飽和状態であった．2007 年 1 月現在の対外接続回線は 1Gbps まで増強された．

そこで，ワクチンを導入した当初より計算機センターの Web サーバ（UNIX; Sun Solaris）を所内向けウイルス定義ファイルサーバ（LiveUpdate, Intelligent Updater の両方法に対応）として利用できるよう整備し，利用者へウイルス設定ファイルの配布・公開を行った．

開始からしばらくの間は手動でシマンテック社のファイルをダウンロードし，所内向けサーバへ転送していたが，作業のために管理者の時間が取られる，また，管理者不在時には更新が滞るなど問題点が露になった．これらの問題を解消するために，2004 年 4 月に所内向けウイルス定義ファイルサーバの自動更新化を行った．なお，ネットワーク環境が改善された現在でも，トラフィクを減少させることはインターネットを使う上での依然重要である．

2 所内ウイルス定義ファイルサーバの自動更新化

すでに述べた様に所内向けウイルス定義ファイルサーバは，LiveUpdate サーバと Intelligent Updater サーバの 2 つの機能がある，本節では，それぞれに必要となる定義ファイル更新方法を述べる．

2.1 LiveUpdate

組織内向け LiveUpdate サーバ向けにウイルス定義ファイルを更新するプログラムは，シマンテック社より「管理 LiveUpdate ユーティリティ」として提供されている．このプログラムは Windows の GUI アプリケーションであり通常は管理者が手動で実行することを想定されている．コマンドラインからはウイルス定義ファイルの更新のみ行うことができる．しかし，当然ながら UNIX サーバである所内ウイルス定義ファイルサーバ上では直接実行できず，別途，管理 LiveUpdate ユーティリティを稼動させる作業用 Windows PC（以下，作業用 PC）を用意した．この作業用 PC に保存されたウイルス定義ファイルを，直接，所内に公開することも検討したが，セキュリティ面を考慮し，UNIX サーバへ転送することにした．

なお，将来，Web サーバと所内ウイルス定義ファイルサーバが分離する場合に備え，ホスト名は Web サービスとは異なるネットワーク上の名前をつけている．

2.1.1 Services for UNIX

Windows 上で UNIX 環境を実現できるソフトウェアとして，Cygwin[*5]が有名だが，マイクロソフト社からも無償で提供している Services for UNIX (SFU) がある [4]．SFU は，POSIX 準拠の UNIX 環境を実現しており，Windows と UNIX 間での認証情報の統合や NFS によるファイル共有を行うことができる．また，これに含まれないコマンド（`ssh`, `rsync`, `bash`, `zsh` 等）も追加モジュールとして，Interop Systems Inc. より提供されている [5]．今回は，安定性を重視し SFU を採用した．

2.1.2 システム概要

スクリプトは SFU 上のシェルスクリプト（`bash`）で作成した．リストを付録 B.1 に示す．コマンドのパス名の指定方法が特殊の他は，普通の UNIX シェルスクリプトと変りがない．これは `cron` により 1 時間毎に起動され，スクリプト内より管理 LiveUpdate ユーティリティを起動される．もし，ウイルス定義ファイルに更新があればこれらを `rsync` を用いて所内ウイルス定義ファイルサーバへ転送し，管理者へ更新内容をメールで報告する．また，一日に一度，その日の更新状況を管理者へメールで通知することにより，何らかの障害が

[*5] http://cygwin.com/

発生した場合でも速やかに対応が取れるようにしている．

所内ウイルス定義ファイルサーバが管理するファイル数は総計約 280 だが，頻繁に更新されるのはその内 50 ファイル前後である．rsync は PC 間のファイルやディレクトリの同期に用いられるコマンドであり差分情報のみ転送するため，通常の rcp（scp）に比べ，効率良く短時間でファイルを送ることができる．なお，rsync でファイル転送する際には ssh（Secure SHell）を利用している．予め作業用 PC の SFU 上の ssh でパスワード無しの公開鍵を作成し，ファイルの転送先である所内ウイルス定義ファイルサーバーに転送，および，設定することによりパスワードなしで ssh の利用を可能としている．

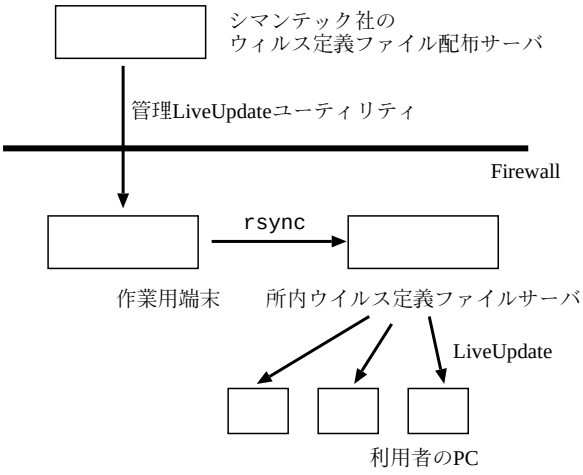

図 1. LiveUpdate 更新システム

古くなったウイルス定義ファイルは自動的に削除されないため，時間の経過とともに作業用 PC，ならびに所内 LiveUpdate サーバのディスクに蓄積さえる．管理 LiveUpdate ユーティリティでは不要になったファイルの削除を行う機能は GUI により提供されているため，管理者が頃合いを見計って削除作業を行う必要がある．そのタイミングをスクリプトから知らせるために，一日に一度，ディレクトリ内のファイル数をチェックし，規定数を越えていた場合は，管理者にメールを送る．なお，そのメールの内容については，スクリプトとは分離し，別ファイルにて保存している．

2.2 Intelligent Updater

Intelligent Updater ファイルは，ウイルス定義ファイルの更新に必要なファイルが 1 つにまとめられており，シマンテック社より入手可能であり[*6]，これを自動更新する perl スクリプトを作成した．このスクリプトは所内ウイルス定義ファイルサーバ上で稼動し，利用者に Web ブラウザを通じて公開するために，ウイルス定義ファイルへのリンクを自動生成する機能を持たせた．リストを付録 B.2 に示す．

Intelligent Updater ファイルの入手には wget コマンドを用い, その時点でシマンテック社において公開されているファイルを一括してダウンロードしている．その際，すでにダウンロードしていたファイルがある場合はスキップするよう指定している（wget の -N オプション）．

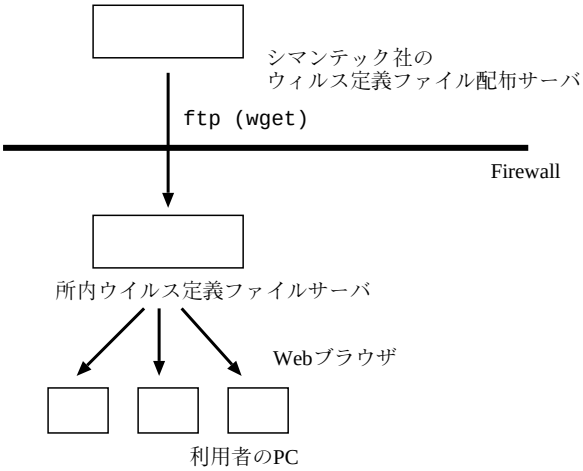

図 2. Intelligent Updater 更新システム

[*6] http://www.symantec.com/region/jp/sarcj/download.html

Intelligent Updater ファイルのファイル名は，公開日とウイルス定義ファイルのバージョン，ならびに対応するクライアントの OS 情報を示しているので，これを利用して公開日とバージョン情報を明記した HTML ファイル（`windows-list.html`）を生成している．

利用者が Web ブラウザでアクセスするページでは，Web サーバの Server Side Include (SSI) 機能で，このファイルを動的に取りこんでいる．

なお，LiveUpdate と同じく，運用を続けていくと古くなった Intelligent Updater ファイルが蓄積していく．これを防ぐために最新の 3 バージョンを保存対象とし，それ以前のファイルは随時削除している．

3 運用状況とまとめ

2004 年 4 月より本システムによるウイルス定義ファイルの自動更新を開始し，今日まで安定に運用を続けている．途中，LiveUpdate ファイルの更新が 2 度停止した．1 度目は作業用 PC が温度異常でダウンしたこと，2 度目は作業用 PC に蓄積されるファイルが増加し，所内ウイルス定義ファイルサーバのハードディスクが溢れたことである．後者はすでに述べたように，規定のファイル数を越えると管理者へメールを出すようにスクリプトを修正した．

本システムによるウイルス定義ファイルの自動更新がどれだけ研究所内で利用されているかを 2006 年 12 月の 1 ヶ月間について調べた．その結果，所内 LiveUpdate サーバの使用台数は約 300 台，Intelligent Updater ファイルの使用台数は約 80 台であった[*7]．実際に所内で使用されているライセンス数と比較すると，全体の 3 割以上の PC がこの更新システムを利用している．使用比率としては若干少なく感じるが，これはノート PC の普及で直接シマンテック社の LiveUpdate サーバへアクセスする機会が増えたためと推測される．一方，デスクトップ PC については所内ウイルス定義ファイルサーバが活用されていると考えられる．また，所内のセキュリティ対策の一環として，2005 年 3 月より毎月各部局宛にワクチン一式（ワクチンのインストールファイルと配布時点における最新の Intelligent Updater ファイル）を USB メモリで配布している事情がある．

本システムを構築することにより管理者が手動でファイルをダウンロードし，公開サーバへ転送し，必要に応じて Web のリンク情報を変更するという手間を省くことができた．同時に，24 時間，常にウイルス定義ファイルの更新状態を監視しているため，所内 LiveUpdate サーバや Intelligent Updater ファイルの提供に遅れが生ずることもなくなり，所内におけるセキュリティ体制の強化に大きく寄与したと言える．また，この開発を通じて，Windows 専用のアプリケーションもコマンドラインから起動できるならば，マイクロソフト社の Services for UNIX を用いることにより，UNIX 機と連携を取ることが十分実用的であることが実証された．

[*7] アクセスログに残されたクライアントのユニークな IP アドレスの数を集計．いずれも固定 IP アドレスからの利用が 8 割以上を占める．

参考

[1] “Time to Live on the Network”, http://www.avantgarde.com/xxxxttln.pdf, セキュリティ修正プログラムが適用していない Windows XP SP1 の PC をインターネットへ直接接続すると 4 分余りで侵入されたという報告．Windows XP SP2（Windows Firewall を有効）, Mac OS X 10.3.5 では攻略されなかった．

[2] “Survival Time”, http://isc.sans.org/survivaltime.html , インターネットに PC を接続してから，何らかの攻撃が来るまでの予想時間の調査活動．2006 年では 3〜5 分であった．

[3] “SAVCE のウイルス定義ファイルを更新する方法”, http://service1.symantec.com/SUPPORT/INTER/entsecurityjapanesekb.nsf/jp_docid/20021226094520949, 本報告で説明した LiveUpdate，Intelligent Updater の他に，“ウイルス定義転送方式 （VDTM）”, “.xdb ファイルのコピー” についての解説がある．

[4] http://www.microsoft.com/japan/windows/sfu/. Windows 2000/XP/2003 Server 向け SFU が無償で入手可能．Windows Server 2003 R3 以降，ならびに Windows Vista Enterprise, 同 Ultimate は，Subsystem for UNIX-based Applications (SUA) として同様な機能が実装されている．この場合も UNIX コマンド等を利用する場合は，別途配布されているユーティリティ・開発キットのダウンロードが必要となる．

[5] `http://www.interopsystems.com/`. 予めコンパイルされたパッケージが入手可能．ダウンロードには無料の会員登録が必要．最初にパッケージを管理する pkg モジュール（`pkg-curent-bin.sh`）をインストールした後．追加すべきコマンド（例 `rsync`）のパッケージをダウンロードし，

```
% pkg_add rsync-current-bin.tgz
```

で追加する．詳しいインストール方法は，Google で “SFU インストール” 等をキーワードとして検索するとよい．

付録 A　LiveUpdate サーバの指定方法と解除方法

LiveUpdate の際に使用される LiveUpdate サーバを任意のサーバに変更する方法を以下に述べる．

1. 管理者が LiveUpdate 管理ユーティリティを開き，この左側のメニューにある「ホストファイルエディター」にて必要事項を記入して，「LiveUpdate ホストファイル」を作成する．
2. このファイルを利用者に配布し，LiveUpdate のフォルダ（`C:\Program Files\Symantec\LiveUpdate\`）にコピーするよう指示する．

この LiveUpdate サーバの解除方法は，以下のフォルダにある `Settings.LiveUpdate` を削除すればよい．

Windows 9x/Me	`C:\WINDOWS\Application Data\Symantec\LiveUpdate`
あるいは，	`C:\WINDOWS\All Users\Application Data\Symantec\LiveUpdate`
あるいは，	`C:\WINDOWS\Profiles\All Users\Application Data\Symantec\LiveUpdate`
Windows NT	`C:\WINNT\Profiles\All Users\Application Data\Symantec\LiveUpdate`
Windows 2000/XP	`C:\Documents and Settings\All Users\Application Data\Symantec\LiveUpdate`

付録 B　ソースコード

B.1　管理 LiveUpdate ユーティリティ自動更新スクリプト

リスト 1. 管理 LiveUpdate ユーティリティ自動更新スクリプト（liveupdate.sh）

```
#!/usr/local/bin/bash
#
# Automatic Update for Symantes Administrative LiveUpdate.
#
# 2004 Apr 20 Takashi YAMAMOTO <yama@nifs.ac.jp>
# 2006 Mar 06 Takashi YAMAMOTO, Add file number check

PATH=/usr/local/bin:$PATH
export PATH

LOG=/var/tmp/liveupdate.log
LLOG=$LOG.lv
TLOG=$LOG.tmp
LUD=/dev/fs/C/LiveUpdate
LU_OPTION=""

MAX_NUMBER=2000
EXCEED_MAIL=/pbin/exceed.mail

DAILY=0; # if DAILY=1, force delete old files.
UPDATE=0

if [[ 10#`date +%H` -eq 7 ]]; then DAILY=1; fi

touch /pbin/liveupdate.touch $LOG $LLOG $TLOG
cp /dev/null $LLOG
date >> $TLOG

/dev/fs/C/Program\ Files/LiveUpdate\ Administration/SilntLuA.exe >> $LLOG

if [[ `cat $LLOG | wc -l` -ne 2 ]]; then UPDATE=1; fi
cat $LLOG >> $TLOG
echo >> $TLOG

chmod a+r $LUD/* >> $TLOG
chmod o-w $LUD/* >> $TLOG
if [[ $DAILY -eq 1 ]]; then
  LU_OPTION="--delete"
fi
rsync -av $LU_OPTION $LUD/ ccweb.nifs.ac.jp:/data/ftp/pub/symantec >> $TLOG

if [[ $UPDATE -eq 1 ]]; then
  SUBJECT="LiveUpdate, Update Notification"
  mailx -s "$SUBJECT" yama@nifs.ac.jp < $TLOG
fi
```

```
46
47  echo "------------------------" >> $TLOG
48  cat $LOG >> $TLOG
49  mv -f $TLOG $LOG
50
51
52  if [[ $DAILY -eq 1 ]]; then
53    SUBJECT="LiveUpdate, Daily Report"
54    mailx -s "$SUBJECT" yama@nifs.ac.jp < $LOG
55    rm $LOG
56
57    if [[ `ls $LUD | wc -l` -gt $MAX_NUMBER ]]; then
58      SUBJECT="Exceed file number limit (> $MAX_NUMBER)"
59      mailx -s "$SUBJECT" yama@nifs.ac.jp < $EXCEED_MAIL
60    fi
61  fi
```

リスト 2. 管理 LiveUpdate ユーティリティ自動更新スクリプトのメール本文 （exceed.mail）

```
1  The number of files in LiveUpdate pattern directory is exceed.
2  The exceed would cause the disk full on ftp server.
3
4  To remove unused files, do the manual operation as follows;
5    LuAdmin.exe --> "tool" Tab --> "Clean up of Download file" Button -->
6  "Delete the unused files" Button.
7
8
9   from LiveUpdate Script
```

B.2 Intelligent Updater 自動更新スクリプト

リスト 3. Intelligent Updater 自動更新スクリプト （symantec-update）

```
1  #!/usr/local/bin/perl
2  #
3  # 2004 Apr 27 <yama@nifs.ac.jp> initial. [ccpuck]-->[ccweb]
4  # 2006 Sep 14 <yama@nifs.ac.jp> script is moved to ccweb, itself.
5  #
6
7  $web_dir     = "/web/htdocs/nifsnet/vaccine";
8  $pattern_dir = "$web_dir/data";
9  $link_file   = "$web_dir/windows-list.html";
10
11 $script_dir  = "/home/yama/symantec";
12 $wget_log    = "$script_dir/symantec-wget.log";
13 $wget        = "/usr/sfw/bin/wget";
14
```

```
15  $pattern     = '200*-x86.exe';
16  $symantec_ftp = "ftp://ftp.symantec.com/AVDEFS/norton_antivirus/$pattern";
17
18  chdir "$pattern_dir";
19
20  # Get virus pattern files from Symantec.
21  system "$wget -nv -N -a $wget_log $symantec_ftp";
22
23  # Keep 3 old files for backup
24  @pattern_files = sort glob $pattern;
25
26  $new_file = pop @pattern_files;
27  for ($i = 0; $i < 3; $i++) {
28    pop @pattern_files;
29  }
30  unlink @pattern_files;
31
32  # Make hyperlink file
33  ($day, $version) = split /-/, $new_file;
34  $y = substr($day, 0, 4);
35  $m = substr($day, 4, 2);
36  $d = substr($day, 6, 2);
37  open LIST, "> $link_file" or die "can't open $link_list";
38    print LIST "<a href=\"data/$new_file\">$y 年$m 月$d 日版 ($version)</a> \n";
39  close LIST;
40
41  exit 0;
```

リスト 4. Intelligent Updater 自動更新スクリプトで生成される HTML ファイル例（windows-list.html）

```
<a href="data/20070124-024-x86.exe">2007 年 01 月 24 日版 (024)</a>
```

リスト 5. 利用者に公開するファイル （該当部分を抜粋）

```
                              :
<TABLE BORDER=0 cellspacing=0 cellpadding=5>
  <TR><TH COLSPAN=3 ALIGN=CENTER bgcolor="#ffdddd"><A NAME="news">最新の</A>
    <A HREF="install.html#def-renewal">ウィルス定義ファイル</A>
  <TR><TD>Windows 用 (5MB)</TD>
  <TD><!--#include file="windows-list.html" --></TD></TR>
                              :
```