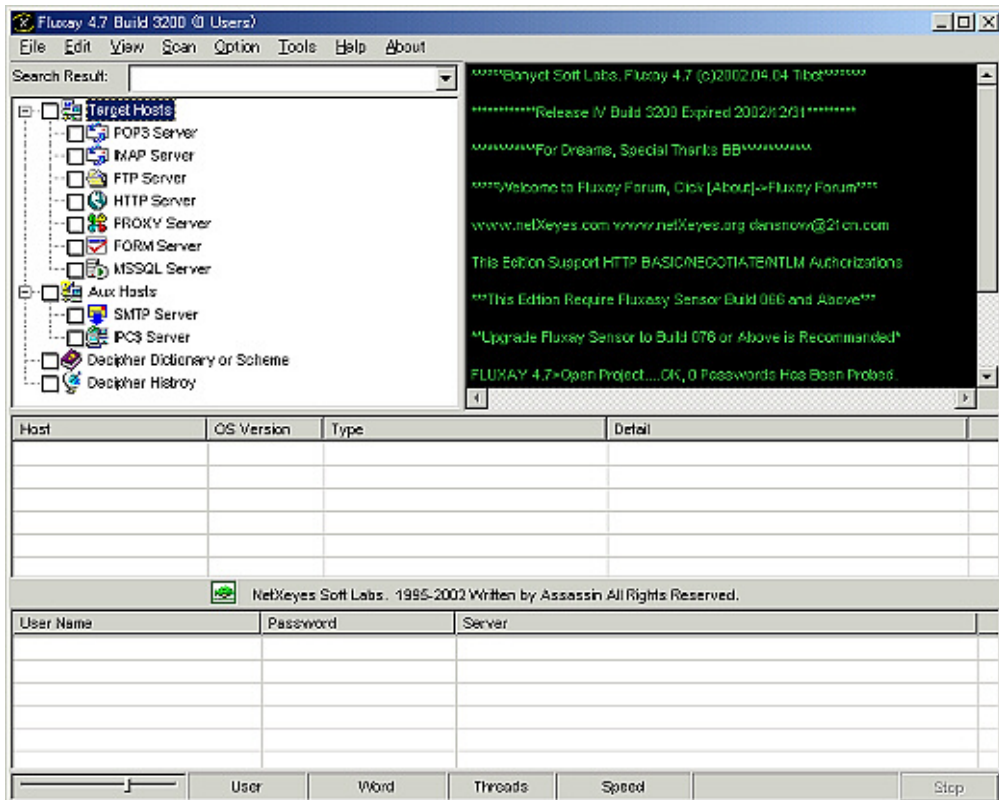


ウイルス解析報告書

ウイルス名	Fluxay 4.7 (GUI Build 3200 Sensor Build 091) Chinese/English Edition For Windows NT/2000/XP
プログラム名及び容量 (添付ファイル名)	Program Files¥NetXeye¥*. * 216ファイル 7,582,703バイト
種別	アプリケーション(バックドア、クラッキングツール)
プログラム言語:	C言語およびアセンブラ
発症環境	Windows9x/Me/NT/2000/XP(コントローラ) Windows NT/2000(センサー)
発見日時	2002年4月4日
発見場所(発信地)	中国
危険性	少ない(潜在的危険性は中程度)
発症条件	条件なし
ウイルスの活動、影響	<p>このプログラムはウイルスではなく、アプリケーションである。</p> <p>このアプリケーションは主にサーバーとして稼働しているWindows NT/2000またはUnix(Linux, SunOS)をターゲットに作成されており、使用可能ポートのスキャン、既知のセキュリティホールが存在チェック等、サーバーのセキュリティ検査が可能である。</p> <p>このことはセキュリティチェックツールとしての利用と、攻撃可能なポートやセキュリティホールを探すためのクラッキングツールとしての利用の両面が考えられる。</p> <p>また、センサーと呼ばれる常駐型サーバープログラムを検査対象にインストールし、Telnetを用いてコマンドを実行させることが可能である。</p> <p>これもリモートコンピュータのメンテナンスという用途と同時に、遠隔操作で対象コンピュータのファイル削除や動作妨害、内容破壊の用途があるということになる。</p> <p>すなわち利用者の意図によってセキュリティツールとして有効に使うことも可能であるし、凶悪なクラッキングツールとして使うことも可能である。</p>
被害の規模	日本国内では非常に希と思われる。(ヘルプ、説明書がすべて中国語)
亜種、変種の有無	2002年6月13日時点のバージョンは4.7。
	<p>このプログラムがウイルス等と最も異なる部分は、特定の「目的」を内部に持たないことである。すなわち、人間が悪意を持って操作して初めてクラッキングツールとなりうる。</p> <p>したがって、ここでは「クラッキングツールとしてFluxay4.7を利用した場合」というシチュエーションで概要説明を行う。</p> <p>まずFluxay4.7をインストールし、起動すると次のような画面が表示される。</p>



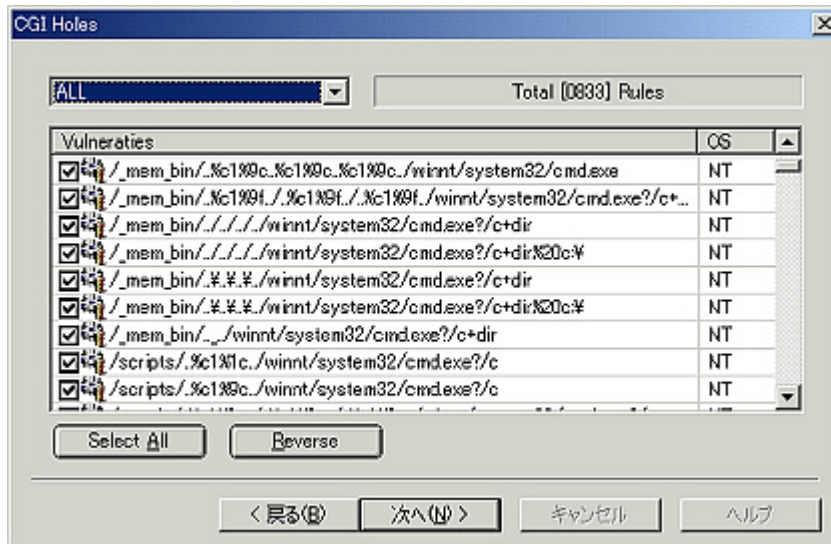
以後このプログラムをコントロールプログラム、またはコントローラと呼称する。

ポートスキャン

最初にポートスキャンである。ポートスキャンを行うためには、対象のコンピュータがアクセス可能なネットワーク上にあり、かつIPアドレスの存在する範囲が既にわかっている必要がある。メニューのFileからAdvanced Scan Wizardを選択すると、Scan Setupダイアログが表示され、スキャンの開始アドレスと終了アドレスの入力、ターゲットとするOS、対象とするサービス名を求めてくる。



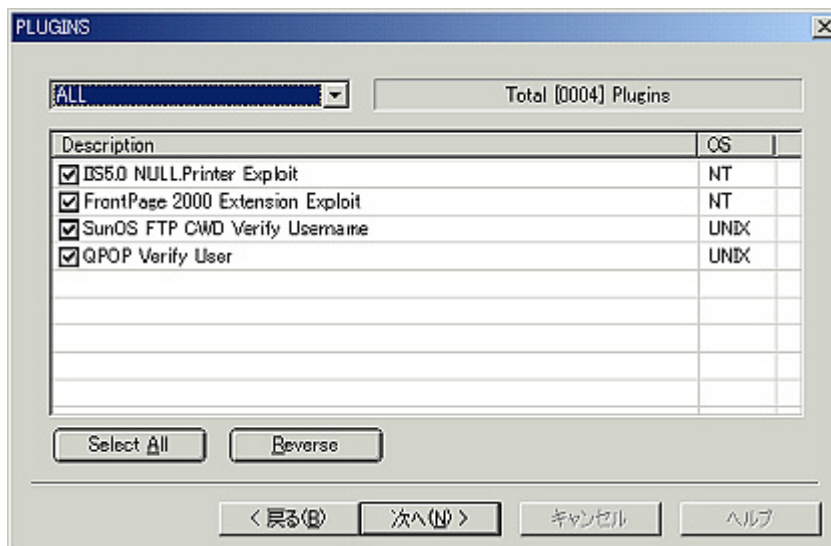
スキャンするポート番号が標準的なものか範囲指定するかを選び、各ダイアログでPOP3、FTP、SMTP、IMAP、Telnet、HTTP、のスキャンオプションを入力すると、次にWebのCGIが持ちうる、標準的なセキュリティホール(833種類)の検査を選択するダイアログ画面が表示される。標準ではすべて検査するように設定されている。



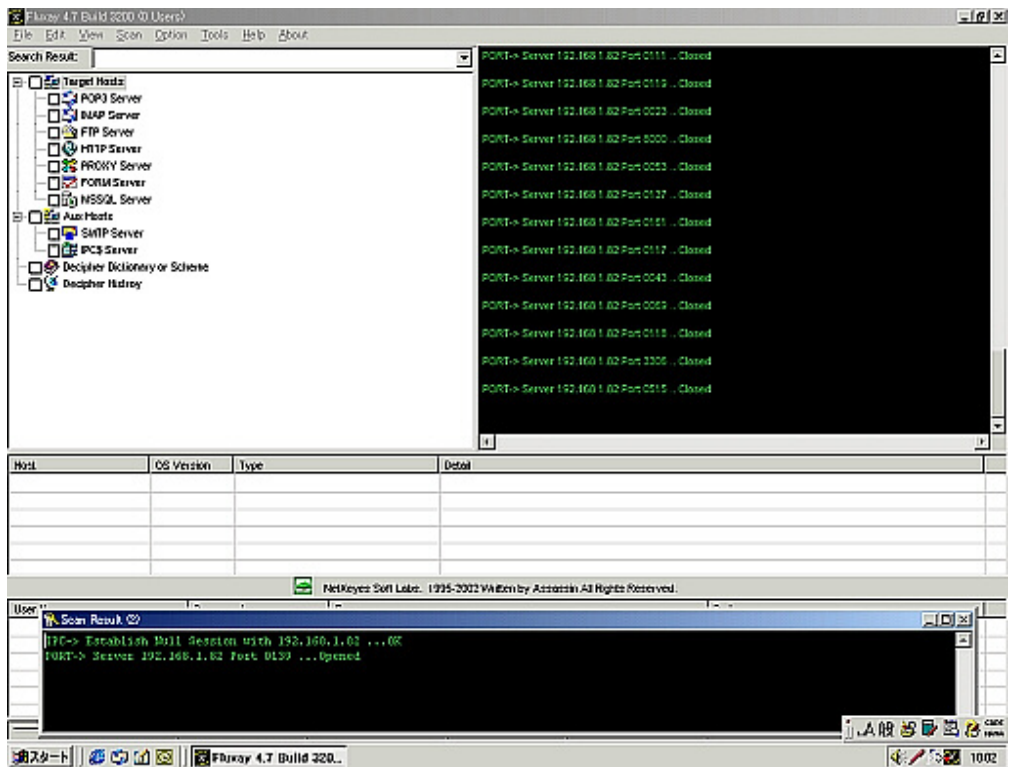
その次には、IISを通じてSA Passwordを調査するか、ユーザーリストを調査するか、FrontPageのバグ、PCAnywhereのパスワードファイルを調査するか、などの質問ダイアログが続き、最終的にプラグイン拡張の確認ダイアログが表示される。

なお、パスワードの調査は数字や一般的な辞書にあるような単語を次々に検査するブルートフォースアタックである。

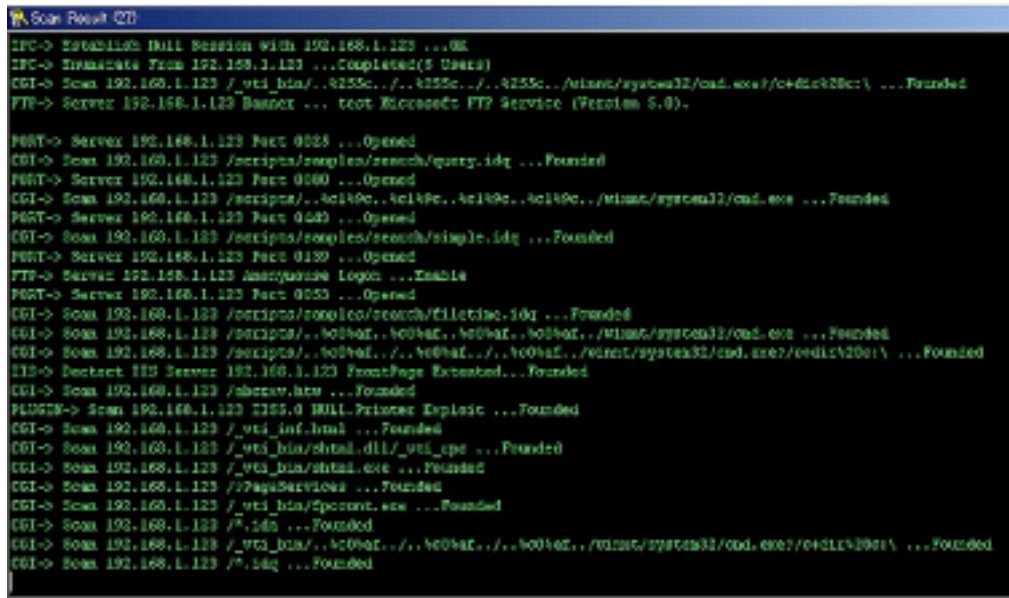
ウイルス動作概要



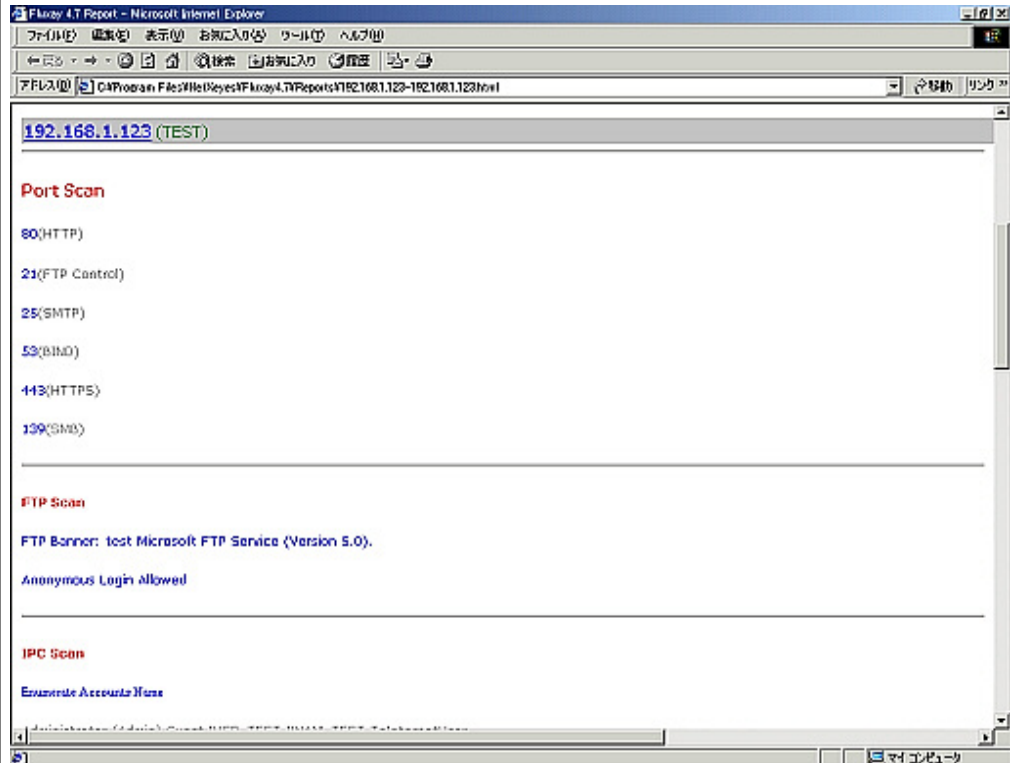
これによって新しいセキュリティホールのチェックが可能となる。検査が終了すると、次のような画面となる。



右側の黒い画面は調査中項目名がスクロールし、下の黒いウィンドウにはサービスが検出されたポート番号が表示される。拡大すると次のようになっている。表示されている項目はすべてWindows2000Serverをインストールした直後のセキュリティホールである。



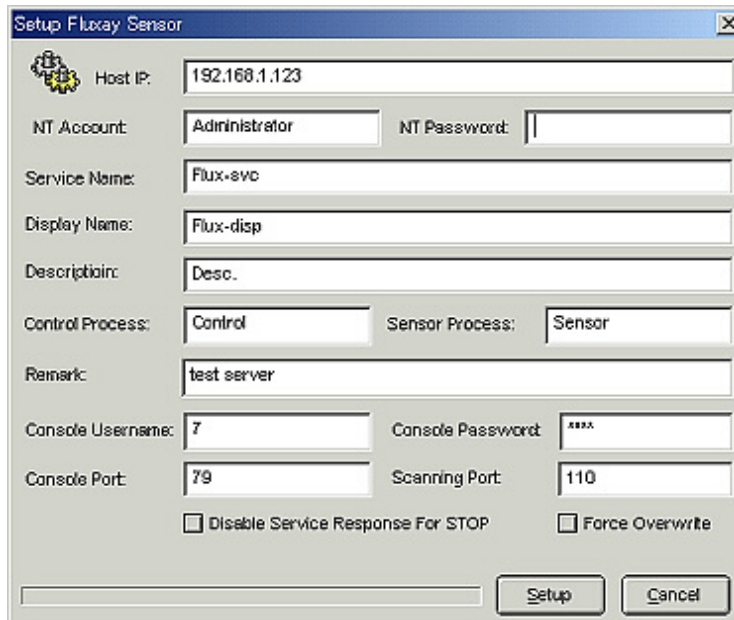
最終的にステータスがHTMLファイルとして保存され閲覧可能となる。



センサーによるリモート操作
メニューのToolsからFluxay Sensor Toolsを選択すると次のようなダイアログが表示される。

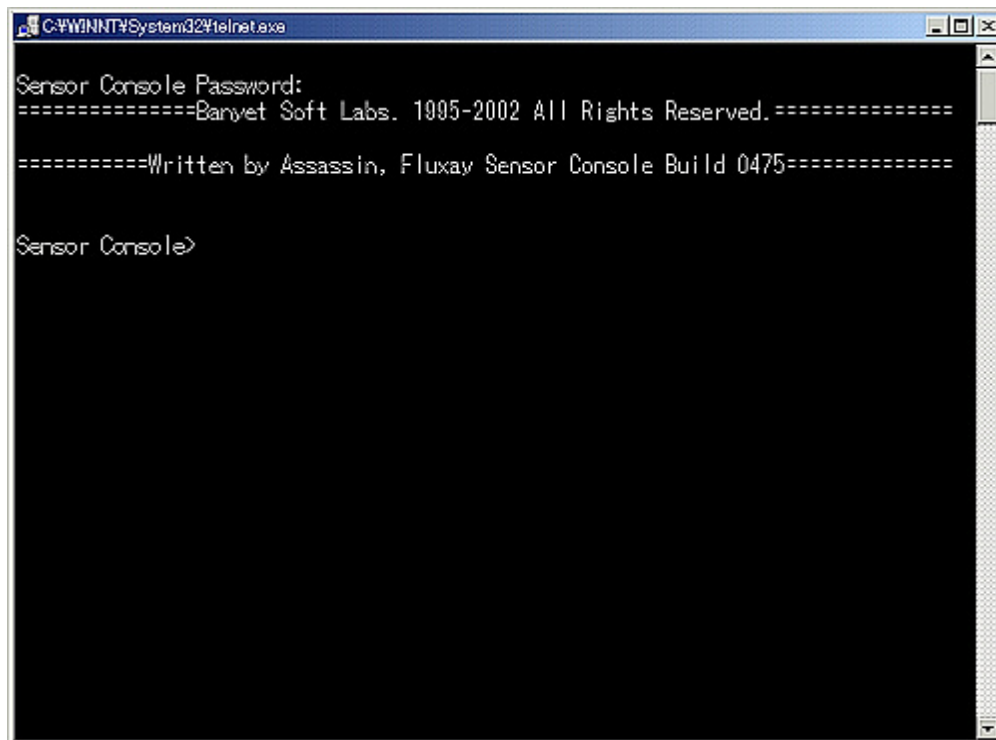


Install Fluxay Sensorを選択すると次のダイアログが表示される。



ここで重要なことは、センサーをターゲットコンピュータにインストールするためには、IPアドレスとアカウント名、パスワードがわからなければならないということである。したがって、ブルートフォースアタックでパスワードが調査できなかった場合、またはパスワードの設定されていないアカウントなどが無かった場合、Fluxayに装備されている機能以外の方法でこれを調査する必要がある。

センサーのインストールが成功すると、Telnetで指定ポートにつないだときに次のような画面が表示される。

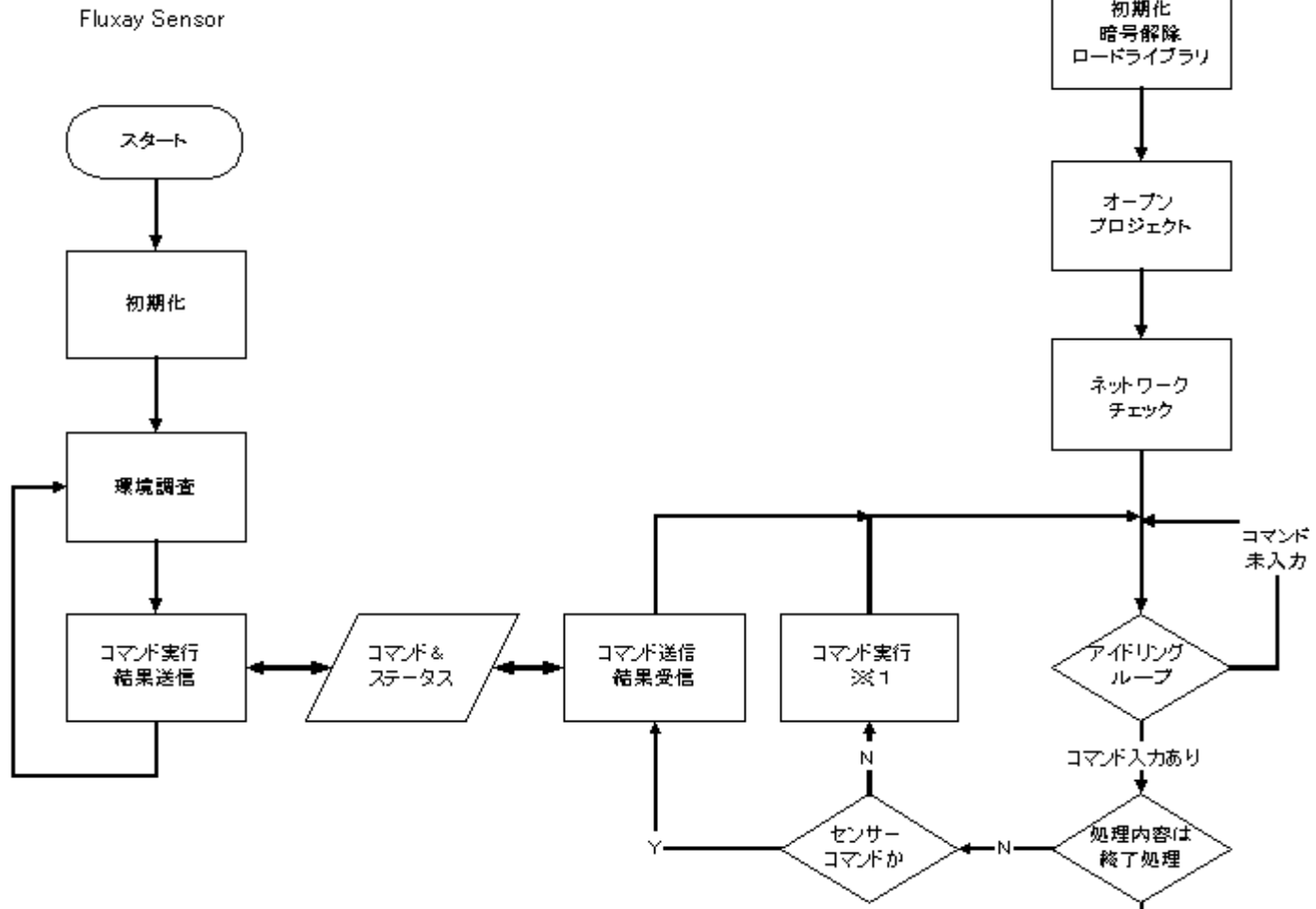


センサーのインストール時に指定したパスワード(NTアカウントとは別の)を打ち込むと、コマンド待機状態となり、次の画面のようにセンサーを通じてコマンドを実行することができる。つまり、ファイルの閲覧や削除ができるということになる。

	 <pre> C:\WINNT\System32\Telnet.exe 1999/12/18 21:00 832,592 winssnap.dll 1999/12/18 21:00 37,136 winsta.dll 1999/12/18 21:00 19,728 winstrm.dll 1999/12/18 21:00 166,160 wintrust.dll 19 個のファイル 2,523,184 バイト 0 個のディレクトリ 39,884,771,328 バイトの空き領域 Sensor Console> ドライブ C のボリューム ラベルがありません。 ボリューム シリアル番号は 981A-18EE です C:\WINNT\system32 のディレクトリ 1999/12/18 21:00 66,832 winchat.exe 1999/12/18 21:00 8,978 winhlp32.exe 1999/12/18 21:00 177,424 winlogon.exe 1999/12/18 21:00 98,528 winmine.exe 1999/12/18 21:00 11,536 winmsd.exe 1999/12/18 21:00 151,312 wins.exe 1999/12/18 21:00 2,112 winspool.exe 1999/12/18 21:00 4,368 winver.exe 8 個のファイル 519,088 バイト 0 個のディレクトリ 39,884,771,328 バイトの空き領域 Sensor Console> </pre>
感染・発症防止方法	<ul style="list-style-type: none"> ・物理的鍵やパスワードを利用し、コンピュータを必要な人間以外に利用させない。 ・ネットワークから切断・隔離する。 ・ルーターを導入し、外部ネットワークからのアクセスをしにくくする。 ・ファイアウォールソフトを使い、ポートの監視や接続制限を行う。
ウイルスの駆除方法	<p>< 確認 ></p> <ul style="list-style-type: none"> ・タスクマネージャを利用して不審なプログラムやプロセスが動作していないかどうか確認する。(標準ではセンサーはSensor.exeというファイル名である) ・ネットワークモニタプログラムを用い、意図しない接続の存在やポート利用がなされていないか確認する。 <p>< 駆除 ></p> <ul style="list-style-type: none"> ・発見された不審なプログラムを終了させる。必要に応じて当該ファイルを削除する。 ・ネットワークモニタプログラム等で不審な接続を切断する。
その他	報告書作成: 2002年7月31日現在

Fluxay4.7 ゼネラルフローチャート

Fluxay Control



※1コマンド実行の詳細

【調査】

- 【ポートスキャン】
指定された開始アドレスと終了アドレス、ターゲットOS、サービス名、ポート番号に従い、スキャンを行う。
- 【CGIセキュリティホール調査】
WebのCGIが持ちうる、標準的なセキュリティホール(833種類)を検査する。
- 【ブルートフォースアタック】
IISを通じてパスワードを調査する。
PCAnywhereのパスワードファイルを調査する。
- 【ユーザー調査】
ユーザーリストを調査する。
- 【FrontPageバグ調査】
FrontPageのバグを調査する。

【結果の保存】
調査結果をHTMLファイルとして保存する。