

avast! 4 Server Edition
Windows 2000/2003 用アンチウイルス



平成 20 年 11 月 18 日

ジュピターテクノロジー株式会社

1 AVAST! VERSION 4 へようこそ	7
2 技術サポート	8
3 サイレント・インストレーション	9
4 基本機能ユーザ・インターフェース	10
4.1 概要:	10
4.2 基本機能ユーザ・インターフェース・ウィンドウ.....	10
4.3 基本機能ユーザ・インターフェース による 検査.....	12
4.4 検査結果.....	14
4.5 常駐保護.....	15
4.6 基本機能ユーザ・インターフェース メニュー	15
4.7 基本機能ユーザ・インターフェース の スキンの変更.....	17
4.8 スキンのない基本機能ユーザ・インターフェース.....	17
5 高機能ユーザ・インターフェース	19
5.1 概要	19
5.2 基本用語.....	19
5.3 高機能ユーザ・インターフェース メイン メニュー	19
6 タスク	24
6.1 タスクの取扱い.....	24
6.2 供給されるタスク.....	24
6.3 スクリーン・セーバー	25
6.4 タスクの環境設定	26
TASK	26
SENSITIVITY.....	27
AREAS	27
TPYE	28
RESULTS	29
EXCLUSIONS	30
VIRUS.....	30
PACKER.....	31
REPORT	33
ALERTS	33
SCHEDULE	34
7 常駐保護	35
7.1 概要	35

7.2 常駐保護の設定.....	36
7.3 常駐保護プロバイダ.....	36
7.4 標準シールド - プロバイダの設定.....	37
常駐保護:標準シールド - <i>Scanner (Basic)</i>	37
常駐保護:標準シールド - <i>Scanner (Advanced)</i>	38
常駐保護:標準シールド - <i>Blocker</i>	38
常駐保護:標準シールド - <i>Advanced</i>	39
常駐保護:標準シールド - <i>Packers</i>	40
常駐保護:標準シールド - <i>Virus</i>	41
7.5 OUTLOOK/EXCHANGE" - プロバイダの設定.....	42
常駐保護 : <i>Outlook/Exchange - Scanner</i>	42
常駐保護 : <i>Outlook/Exchange - Inbound Mail</i>	42
常駐保護 : <i>Outlook/Exchange - Outbound Mail</i>	43
常駐保護 : <i>Outlook/Exchange - Signature</i>	43
常駐保護 : <i>Outlook/Exchange - Virus Storing</i>	44
常駐保護 : <i>Outlook/Exchange - Advanced</i>	45
常駐保護 : <i>Outlook/Exchange - Heuristic</i>	45
常駐保護 : <i>Outlook/Exchange - Heuristic Advanced</i>	46
常駐保護 : <i>Outlook/Exchange - Packers</i>	47
7.6 インターネット・メール - プロバイダの設定.....	48
常駐保護 : インターネット・メール - <i>POP</i>	49
常駐保護 : インターネット・メール - <i>SMTP</i>	49
常駐保護 : インターネット・メール - <i>IMAP</i>	49
常駐保護 : インターネット・メール - <i>NNTP</i>	49
常駐保護 : インターネット・メール - <i>Redirect</i>	50
常駐保護 : インターネット・メール - <i>Advanced</i>	51
常駐保護 : インターネット・メール - <i>Heuristics</i>	51
常駐保護 : インターネット・メール - <i>Heuristic Advanced</i>	53
常駐保護 : インターネット・メール - <i>Packers</i>	54
常駐保護 : インターネット・メール - <i>Virus</i>	54
7.7 スクリプト・ブロック - プロバイダの設定.....	55
常駐保護: スクリプト・ブロック - <i>Protected Programs</i>	56
常駐保護: スクリプト・ブロック - <i>Advanced</i>	56
常駐保護: スクリプト・ブロック - <i>Virus</i>	56
7.8 インスタント・メッセージ - プロバイダの設定.....	58
常駐保護 : インスタントメッセージング - <i>Program</i>	58
常駐保護 : インスタントメッセージング - <i>Archives</i>	59
常駐保護 : インスタントメッセージング - <i>Virus</i>	59
7.9 P2P シールド - プロバイダの設定.....	61

常駐保護 : P2P シールド - Program	62
常駐保護 : P2P シールド - Archives	62
常駐保護 : P2P シールド - Virus.....	63
7.10 ネットワーク・シールド - プロバイダの設定.....	64
常駐保護: ネットワーク・シールド - Settings.....	64
常駐保護: ネットワーク・シールド - Last attacks.....	64
7.11 WEB シールド - プロバイダの設定	64
常駐保護 : Web シールド - Basic	66
常駐保護 : Web シールド - Web Scanning	66
常駐保護 : Web シールド - Exceptions	67
常駐保護 : Web シールド - URL Blocking	67
常駐保護 : Web シールド - Advanced.....	68
常駐保護 : Web シールド - Packers	68
8 メール保護のセットアップ.....	69
8.1 概要	69
8.2 基本設定.....	70
8.3 MS OUTLOOK / EXCHANGE	70
8.4 サービスの一時停止.....	70
8.5 E-MAIL アカウントの選択	70
8.6 サービスの設定	71
8.7 タスクの設定.....	71
8.8 サービスの開始.....	72
8.9 メール保護のマニュアル設定	72
ステップ 1 : AVAST4.INI ファイルの変更.....	72
ステップ 2 : メール プログラム の アカウント プロパティ を 編集.....	72
メールの送信と受信	73
INI ファイル.....	74
他のソフトウェアとの連携.....	76
コマンドライン パラメータ.....	77
既知の問題.....	77
8.10 挿入される記録の書式	77
クリーン・メッセージに対する HTML 形式の記録の変更.....	78
感染メッセージに対する HTML 形式の記録の変更.....	78
感染していないメッセージに対する 純粋なテキスト形式の記録の変更.....	79
感染メッセージに対する純粋なテキスト形式の記録の変更.....	80
9 ウィルス・チェスト.....	80
9.1 概要.....	80
9.2 チェスト・ファイル の 取扱い.....	80

9.3	チェストの使用	81
9.4	チェストのファイル・カテゴリ	82
9.5	使用方法	82
	ファイルを追加	82
	ファイルを削除	82
	ファイルを復帰させる	83
	ファイルを抽出	83
	ファイル・プロパティを表示	83
	ファイル検査	84
	内容をリフレッシュ	84
10	拡張エクスプローラ - ASHQUICK プログラム	85
10.1	概要	85
10.2	拡張エクスプローラのセットアップ	85
11	ASHCMD プログラム	85
11.1	概要	85
11.2	ASHCMD	85
11.3	ASHCMD のパラメータとスイッチ	86
11.4	リターン・コード	88
12	AVAST! の設定	88
12.1	COMMON(一般)	88
12.2	APPEARANCE(外観)	89
12.3	ENHANCED INTERFACE(拡張インターフェイス)	89
12.4	CHEST(チェスト)	90
12.5	CONFIRMATION(確認)	90
12.6	LANGUAGE(言語)	90
12.7	SOUNDS(サウンド)	90
12.8	LOGGING(記録)	90
12.9	EXCLUSION(例外)	90
12.10	UPDATE-BASIC(更新 - 基本)	91
12.11	UPDATE-CONNECTIONS(更新 - 接続)	93
12.12	ALERTS(警告)	93
12.13	SMTP	94
12.14	TROUBLE SHOOTING(トラブルシューティング)	95
13	ログ・ビューア	95
12.1	概要	95
12.2	ログ・ビューアの取扱い	96

12.3 イベントのカテゴリ.....	97
13 復旧	97
13.1 AVAST! ウィルス・クリーナーで復旧	97
VRDB	99
13.2 スプラッシュ・スクリーン	101
13.3 よくある質問	101
13.4 ウィルスについての情報	106
<i>ウィルスの特徴の意味.....</i>	<i>106</i>
13.5 AVAST! iNEWS	107
13.6 登録.....	108

1 avast! version 4 へようこそ

お客様各位

avast! アンチウイルスパッケージを導入下さり、誠にありがとうございます。本製品はアンチウイルス製品において、最も優れたプログラムの一つです。

このプログラムが快適に動作し、本製品にご満足頂けるよう願います。

アプリケーション・パッケージ avast! が目的とするのは、ウイルスの感染からお客様のコンピュータを保護することです。正確に、定期的に、そしてデータ バックアップ ユーティリティなど、他プログラムと一緒にお使いいただくことにより、お使いのコンピュータがウイルスに感染するリスクを劇的に減少させ、お客様の個人データの損失を回避することを保証します。

このマニュアルは長年に渡って本製品に親しんで頂けるよう作成しました。また、全体的だけでなく個々の特性や機能についてもご理解頂きたいと願います。少々難解と思われる部分を除いて、Windows オペレーティング システムの環境に関する基本的項目の十分な知識と一般的なスキルがあることを想定しています。フォルダ、ファイル、ウィンドウのような項目についてほとんど御存知ない場合やウィンドウをアクティブにしたりボタンを押したりする方法がわからないときは、相当するユーザーズ マニュアルかオペレーティング システムのヘルプをお調べ頂くことをお勧めします。

avast! は 専用のアンチウイルス プログラムに期待するすべての特徴を備えています。初心者や不慣れたユーザーに適した 基本機能ユーザ・インターフェース、任意の設定や avast! の 全ての制御にアクセス可能な高機能インターフェースも備えています。avast! には常駐保護があります。コンピュータの日常作業中いかなる危険な操作も監視します。例えば起動中のアプリケーションや、効果的なウイルスの感染の回避です。avast! は 今日のほとんどの e-mail クライアントによって処理される 受信/送信 双方の e-mail メッセージをチェックすることができます。また avast! には コマンドライン・インターフェイス も用意されています。

2 技術サポート

インストール、登録、使用や設定について何か問題がある時、Tech Support にお問い合わせ下さい。問題解決のお手伝いをさせていただきます。

E-mail: tech-support1@jtc-i.co.jp

e-mail に次の情報を記載してください。

- ・ avast! アプリケーションのバージョン(build) (例 .4.7.211) "avast! について..." ウィンドウでご利用のプログラムのバージョンを見つけることができます。

- ・ ご使用中 (または問題のある) オペレーティング・システムのバージョン 例: Windows 2000 サーバー

- ・ 基本的なハードウェア環境 (CPU, RAM)

- ・ インターネット接続(オンライン更新や電子メールに関する問題がある場合のみ) 重要なデータは接続のタイプ (ダイヤルアップ, ケーブル・モデム, LAN) とネットワーク・デバイス (プロキシ・サーバー, ファイアウォール, ...)

- ・ e-mail クライアントの名前とバージョン (e-mail の動作に関する問題がある場合のみ)

- ・ エラーメッセージのテキストまたはスクリーン・ショット

- ・ エラー発生の詳細(少なくとも エラーが発生した様子 - その時何をしたか 等)

.

電話:042-358-1251 FAX:042-360-6112

営業時間(平日): 9:00 - 17:00

3 サイレント・インストール

この章はネットワーク管理者様向けです。ユーザーからのインターフェースを全く用いず、複数のコンピュータに avast! をインストールすることが可能に（そして容易に）なります。インストールには事前に定義されたプログラムとタスクの設定が必要になります。

サイレント・インストールの作成

- 1 1 台のコンピュータに avast! をインストール
2. avast! の設定変更。他コンピュータに対してそれぞれ適切な設定をして下さい。
3. タスクのパラメータの設定（必要に応じて）
4. 必要に応じて常駐保護の設定（または終了）、とパスワードの設定
5. 高機能ユーザ・インターフェース で File → Create Silent Installation を選択
6. サイレント・インストールのパラメータの設定

- o Silent mode - 対象コンピュータにインストールする間、エラーメッセージのみ表示
- o Very Silent mode - 対象のコンピュータにインストールする間、メッセージは一切表示されません。
- o Installation path - avast! をインストールするフォルダを入力（デフォルトでは、%PRGFILES%\¥Alwil Software¥Avast4）。
- o No reboot - avast! インストール後、コンピュータに再起動を要求します。このオプションを選択すると再起動を要求しません。
- o Ask for reboot - インストール終了時にユーザーに再起動を質問します。

"No reboot" または "Ask for reboot" どちらも選択されていない場合、インストール終了時にシステムは自動的に再起動されます。

7. Create ボタンをクリック
8. サイレント・インストールに必要なファイルを保存するフォルダを選択してください。
9. 2 つのファイル admin.ini および tasks.xml が選択したフォルダに書き出されます。admin.ini ファイルは avast! プログラムの設定を含みます。tasks.xml ファイルは固有タスクの設定を含みます。常駐保護の設定のためのパスワードが設定されていれば、目標のフォルダにもう一つのファイル aswResp.dat が存在します。常駐保護の設定と終了をするための暗号化されたパスワードが含まれています。
10. これら 2 つまたは 3 つのファイルを共有フォルダに置いてください。
11. avast! インストーラー を 同じ フォルダに入れてください。
12. このフォルダから対象のコンピュータへの avast! インストールを起動してください。

4 基本機能ユーザ・インターフェース

4.1 概要：

基本機能ユーザ・インターフェースではプログラムを細かく設定せず、プログラムをそのまま使用するユーザー様を想定しています。基本機能ユーザ・インターフェースで全ての必要な機能に容易にアクセスすることができます：ウィルス検査、ウィルス・チェストへのアクセス、ウィルス・データベースの更新、常駐保護のレベル設定などです。

avast! はプログラムの外観を替えるためのスキンがございます。その為、ここで説明する一部の管理項目は実際にご覧になる管理項目とは異なる事もございます。ですが、プログラム使用の基本は常に同じです。

4.2 基本機能ユーザー・インターフェース・ウィンドウ

avast! はスキンと呼ばれる、複数の外観がございます。その為、これから説明するいくつかの管理項目はご使用中のものとは違う事もございます。ですが、基本的な原理は常に同じです。

表示される情報

avast! を起動すると、基本機能ユーザ・インターフェースは様々な管理項目の情報を表示します。

- ・ **Virus Database version** - フォーマットのバージョン番号、バージョン公開日
- ・ **Resident protection** - 常駐保護のレベルの表示
- ・ **Date of last scan** - 最後にローカル・ハードディスクを完全検査した日付
- ・ **Virus Recovery Database (VRDB)** - ウィルス修復データベースの最終更新日。感染したファイルを修復に使用します。
- ・ **Automatic updates** - 自動更新の設定を表示。

管理項目

- ・ **Chest** - ウィルス・チェスト・ウィンドウを開きます。
- ・ **Resident protection** - 常駐保護のレベルを管理するスライド式のバーを表示します。 次の 3 つのレベルがあります。 左端 - 常駐保護は無効。 標準 - デフォルト。 右端 - 高 レベルの常駐保護が設定。 作成済みまたは編集された全ファイルを検査。
- ・ **iAVS** - ウィルス・データベース のインターネット経由の更新を開始。
- ・ **Local hard disks** - ウィルス検査のためにすべてのローカル・ハードディスクを選択。 検査レベルの設定ができます。
- ・ **Drives selection** - ドライブを選択(フロッピーディスク, CD-ROM, DVD-ROM 等) ウィルスの存在を検査します。 検査レベルを設定することも可能です。
- ・ **Area selection** - 検査する フォルダ(ディレクトリ) を選択。 同時に検査レベルも選択可能
- ・ **START ボタン** - 選択した領域の検査を開始します。
- ・ **PAUSE ボタン** - 検査を一時停止します。(開始ボタンが検査中はこのボタンに変わります。)
- ・ **STOP ボタン** - 検査を停止します。
- ・ **Menu** - メニューがポップアップします。 ここでユーザ・インターフェースの外観(スキンの選択)、高機能ユーザ・インターフェースへの切替え 等 ができます。

4.3 基本機能ユーザ・インターフェース による 検査

領域の指定

最初に、ウィルスの検査をする領域を選択します。以下3つのボタンで設定できます。

- ・ **Removable media** - このボタンで、検査するリムーバブル・メディアを選択します。CD-ROM, DVD-ROM またはディスクドライブ（または それらの可能なものを一緒に） 対応する項目をチェックして選びます。
- ・ **Folders** - 個々のフォルダ(ディレクトリ)を直接選択。 ツリーを表示して、検査したいフォルダを1 つ以上選択します。フォルダをタイプする事で、ウィンドウの下の部分に直接パスを付けが可能です。この方法でタイプしたパスは引用符" "で囲み、またいくつもあればセミコロン;で区切ります。例えば、 "C:\Windows"; "C:\Program Files"
- ・ **Local disks** - このボタンでスキャン対象コンピュータの全ハードディスクを選択します。

感度の設定

検査する領域を選択するとスライド式のバーが現れます。 スライダーを動かして検査感度を指定してください。3つのレベルがあります。

- ・ **Quick scan** - 拡張子に従って、危険だと思われるファイルのみ検査します。つまり拡張子が EXE, SCR, COM, DOC 等 のファイルを検査します。そのファイル内で、avast! は 対応するファイルのタイプに感染するウイルスだけを探します。つまり EXE ファイル等のマクロウイルスは検索しません。
- ・ **Standard scan** その内容により危険だと思われるファイルだけを検査します。ファイルの拡張子は無視されます。ここでも、個々のファイル・タイプに対応するウイルスだけが検索されます。
- ・ **Through scan** すべてのウイルスに対して、すべてのファイルを検査します。

アーカイブの検査

検査する圧縮ファイル(ZIP, RAR 等) を指定。

検査の 開始, 一時停止 および 停止

領域と検査感度を選択した後"START" ボタンを押して検査を開始します。検査中、このボタンは検査を一時停止する "PAUSE" ボタンに変わります。"STOP" ボタン により、検査を完全に中断します。

検査している間は 基本機能ユーザ・インターフェース のウィンドウで確認できるのは ウィルス・データベース・バージョン, 選択した検査感度, 検査ファイルの数 等です。

4.4 検査結果

avast! が検査によりウイルスを全く発見せず、また検査ファイルにエラーが全く生じなかったとします。基本機能ユーザ・インターフェースのメイン・ウィンドウは今回の検査について 検査したフォルダとファイルの数、検査に要した時間 等 の 基本情報を表示します。しかし検査中にひとつでもウイルス本体が発見された場合、またファイル検査に問題があった場合、検査終了時に結果を表示する特別なウィンドウが開きます。

結果ウィンドウで検査についての詳細な情報;その結果に対する処理が表示されます。

以下、3つの列(コロン)が表示されます。

- ・ **Name of file** - 感染ファイル(または検査中に問題のあったファイル) のパスとファイル名

- ・ **Result** - ファイルに発見されたウイルスの名前 (または "検査不能:ZIP 圧縮ファイル は壊れています。" といった問題の簡単な説明)

- ・ **Operation** - 該当ファイルに対する処理を表示。 例)削除、チェストに移動、 等

結果でリストアップされたファイルを処理できます。ファイルを選択して "Action" ボタンをクリックしてください。ウイルス発見と同じアクションを選択できます。 例) 削除、修復、移動、チェストへ移動、 検査

4.5 常駐保護

常駐スキャナ ボタンで avast! 常駐保護の感度を設定することができます。保護には 3 つの基本レベルがあります。

- ・ **Disabled** 常駐保護を停止します。お勧めしません。
- ・ **Standard** 一般的、デフォルト設定です。起動時にすべての実行型ファイルは検査されます。また、オープン時にすべてのドキュメントと スクリプトは検査されます。MS Outlook では未読メッセージのみ検査されます。
- ・ **High** パラノイド・モードと呼ばれます。標準モードと同様に動作しますが、コピーされたファイルでさえ検査されます。更に、MS Outlook を開くと、すべてのメッセージが検査されます。

4.6 基本機能ユーザ・インターフェース メニュー

以下の項目は 基本機能ユーザ・インターフェース メニュー にございます。

- ・ **Settings** プログラム設定の変更を行います。詳細については "プログラムの設定" の章をご覧ください。
- ・ **Select skin** ここでは お好きなスキンを選択できます。弊社 WEB ページで他のスキンも御利用いただけます。
- ・ **Status Information** avast! ウィンドウで以下の情報が表示されます。ウイルス・データベースのバージョン、常駐保護のレベル、最終検査日時、VRDB の状態 および 自動更新の設定
- ・ **Last scan Results** 最後に検査した結果を表示します。
- ・ **View Scan Reports** 検査レポートを表示(レポート作成を許可した場合)。Notepad にテキストフォーマットのレポートが表示されます。XML フォーマットのレポートはお使いの WEB ブラウザ (Internet Explorer, Opera, Mozilla, Netscape その他...) で表示されます。
- ・ **avast! iNews.** お知らせ (News) を表示します。詳細は "avast! News" の章をご覧ください。
- ・ **Virus database** データベース内のウイルスの基本情報を表示します。広範囲に広がったウイルスについては、極めて包括的な情報を得るには、avast! から Alwil 社 WEB ウィルス・データ

ベースへ接続します。avast! 詳細は "ウイルス情報" の章をご覧ください。

・ **Schedule boot time scan** オペレーティング・システムが起動する前にウイルス検査の予定を入れます。この検査の設定を行うダイアログが表示されます。

・ **Virus Chest** ウィルス・チェスト ウィンドウを表示します。

・ **Log viewer** 動作中に avast! 実行中、複数の記録(ログ)ファイルを作成されます。このオプションを選択することで ログ・ビューア を実行できます。

・ **Updating** 更新作業を開始します。

○ **iAVS update** ウィルス・データベース を更新します。

○ **Program update** ウィルス・データベース を含む全プログラムを更新します。

・ **Switch to Enhanced user interface** このスイッチで avast! インターフェースを 基本機能 から高機能に切替えます。これにより、すべての設定をおこなないプログラムの完全な制御が出来るようになります。高機能ユーザ・インターフェースが向いているのは、経験豊かなユーザーや使い勝手を良くするためより多くの設定をしたい方です

・ **Introductory help** 基本機能ユーザ・インターフェース 起動時にいつも表示されるクイック・ガイド を表示します。avast! 基本機能ユーザ・インターフェース の使用についていくつかの基本事項が含まれています。

・ **Help** このヘルプ・マニュアルを開きます。

・ **About avast!** プログラム、ライセンスその他の基本情報を表示します。また ライセンスキーの入力も行います。

・ **Exit** プログラムを終了します。

4.7 基本機能ユーザ・インターフェース の スキンの変更

基本機能ユーザ・インターフェース の外観は変更できます。 avast! には、いくつかのスキンがございますので、すぐにご利用できます。 追加のスキンは弊社 WEB ページからダウンロードできます。

スキンを変更するには（基本機能ユーザ・インターフェース で）Menu → Skin を選択 を選択してください。 利用可能なスキンのリストが表示されます。 スキンの名前をマウスでクリックすると avast! は直ちにその外観を変更します。 新しいスキンが気に入ったらそれを選択したまま OK を押してください。 そうでなければ、Cancel をクリックして下さい。 スキンは更新されません。

追加のスキンは我々の WEB ページからダウンロードすることができます。 "Get more skins from our www server now" のテキストの上でクリックするだけで、お好きなスキンを選択してダウンロードできます。 スキンのダウンロードが完了すると、スキンリストに表示されます。

"Choose random skin on application startup" オプションにチェックを入れた場合、基本機能ユーザ・インターフェースを起動する度に（インストールされているものの中から）新しいスキンが選択されます。

4.8 スキンのない基本機能ユーザ・インターフェース

もし、何かの理由で、基本機能ユーザ・インターフェースのスキンを使用したくない場合、簡単にスキンをオフにする事ができます。 スキンをオフにすると、avast! 基本機能ユーザ・インターフェース の外観と操作性は普通の Windows アプリケーションと同じになります。

スキンをオフにするには次のようにしてください。

1. avast! 基本機能ユーザ・インターフェース を起動する。
2. 基本機能ユーザ・インターフェースの上でマウスの右ボタンをクリックし、ポップアップメニューから Settings... を 選択する。
3. 左のカラムで、Common をクリックする。
4. 右側のカラムで、"Enable skins for Simple User Interface" のチェックを外す。

ここで avast! 基本機能ユーザ・インターフェース を再起動します - 一度閉じて再起動してください。 基本機能ユーザ・インターフェースがスキン無しで表示されます。

このプログラムのインターフェースはスキン有りものとても良く似ています。 検査すべき領域を

選び、検査パラメータ（例えば、圧縮ファイルの内容を展開すべきかどうか）を選択します。最後に Start scan ボタンにより検査を開始します。これらの一連の操作についての説明は基本機能ユーザ・インターフェースに関するヘルプにございます。

5 高機能ユーザ・インターフェース

5.1 概要

avast! の 高機能ユーザ・インターフェースは経験豊かなユーザーに適しています。 avast! の機能とオプションを全てご利用いただけます。 経験の少ないユーザーには 基本機能ユーザ・インターフェース のご使用をお勧めします。

詳細については 高機能ユーザ・インターフェース・メイン・メニュー をご覧ください。

5.2 基本用語

高機能ユーザ・インターフェース を起動する場合、タスク、セッション および 結果 という 3 つの主要な項目を理解する必要があります。

・ **Task:** avast! が検査すべき対象と方法を指示するための情報を含みます。 例えば、avast! が検査すべきフォルダ、ファイルのタイプ、ウィルス発見時にとるべき行動、圧縮ファイルを 検査すべきかどうか、などです。 タスクは新規作成、編集、削除、 コピーができます。

・ **Session:** タスクを実行する工程です。 つまりタスクを開始すると セッションは進行していきます。 セッションを一時停止、停止、削除することができます、その結果を表示することができます。

・ **Results:** 過去のセッションについての情報です。 セッションの結果かは、例えば感染したファイルの数、検査したファイルの数などです。

5.3 高機能ユーザ・インターフェース メイン メニュー

FILE

・ **iAVSupdate:** ウィルス・データベース のダウンロードと更新します。 この作業にはインターネット接続が必要です。

・ **Program Update:** ウィルス・データベース と一緒にプログラムを更新します。 この作業にはインターネット接続が必要です。

・ **Settings:** プログラムの設定を変更します。 詳細はプログラム設定の章をご覧ください。

・ **Start avast! Virus Cleaner:** お使いのコンピュータから最も一般的なウィルスを完全に削除する特別なツールを起動。

- ・ **Create Silent Installation:** サイレント・インストール を作成 (現行の avast! 設定による)
- ・ **Go to Background:** このオプションにより avast! のプライオリティが下がります。他のアプリケーションよりも少ないリソースが avast! に提供されます。avast! が バック・グラウンドで動いているときは他のアプリケーションの速度を落としません。
- ・ **Shutdown Computer When Scan Has Completed:** 動作中のすべてのタスクが終了すると、コンピュータが自動的にシャットダウンします。
- ・ **Close:** avast! プログラムを閉じる。

VIEW

- ・ **Simple User Interface:** 基本機能ユーザ・インターフェースに切り替え。
- ・ **Show Log Files:** ログ・ビューア を起動。
- ・ **Tool bars selection:** 高機能ユーザ・インターフェース に 表示されているツールバーを選択します。

TASKS

- ・ **Create New:** 新しいタスクを作成します。
- ・ **Edit:** 選択したタスクを編集します。
- ・ **Delete:** 選択したタスクを削除します。
- ・ **Create copy** 選択したタスクと同じ設定の新しいタスクを作成します。この新しいタスクはタスク・リストに表示され、その名前は、例えば "検査:ローカル・ディスク の コピー" のように、単語 "コピー" が付きます。このオプションは (元のタスクの変更ができない) 予め定義されているタスク の 設定を変更したいときに役立ちます。
- ・ **Start:** 選択したタスクを起動します。
- ・ **Stop:** 動作中の 常駐タスクを停止します。

・ **Mark as Default**: 常駐タスクをデフォルトに 設定します(即ち、システム起動時に開始されるようになります)。

・ **Unmark (as Default)**: そのタスクはもはや "デフォルト" ではなくなります (即ち、システム起動時に自動的に開始されなくなります)。常駐保護の自動起動をこの方法でやめることができます。

SESSIONS

・ **Pause**: 動作中のセッションを一時停止します。

・ **Continue**: 一時停止したセッションを再開します。

・ **Stop**: 動作中のセッションを停止します。

・ **Delete**: 選択したセッションを削除します。

・ **Show results**: 終了したセッションの情報を表示します (例えば、発見したウイルス)。

・ **Properties**: 対応するタスクの設定を表示します。

・ **Show Report**: 現在のレポート・ファイルを表示します。

結果

・ **Delete File**: コンピュータから選択したファイルを削除します。

・ **Repair File**: 感染したファイルを修復します。修復 の章をご覧ください。

・ **Move / Rename File**: 選択したファイルを移動 および/または 削除します。

・ **Move to Chest**: ウィルス・チェストにファイルを移動します。

・ **Scan File**: 選択したファイルについてウイルスの存在を検査します。

・ **Print**: 結果をプリンタで印刷します。

・ **Select All**: 結果リストのすべての項目を選択します。

- ・ **Invert Selection**: 選択を反転します。
- ・ **Refresh**: 結果のページをリフレッシュします。

チェスト

- ・ **Refresh all files**: チェスト 内のファイルでページをリフレッシュします。
- ・ **Add**: チェストにファイルを追加します（ファイルはコピーされ、移動しません！）。このオプションは システム・ファイル・カテゴリ が表示されている時だけ有効です。
- ・ **Delete**: 選択したファイルを チェスト から削除します。
- ・ **Restore**: 選択したファイルを チェスト から元の場所に戻します。
- ・ **Extract**: 選択したファイルを チェスト から選んだ場所にコピーします。
- ・ **Scan**: 選択したファイルについてウィルスの存在を検査します。
- ・ **Properties**: 選択したファイルのプロパティを表示します。
 - **Original file name**:
 - **Original folder**: チェスト に移動される前にファイルがあったフォルダ。
 - **Size of file**: ファイルのバイト数。
 - **Last modification time**: ファイルが更新された日付と時刻。
 - **Time of transfer to Chest**: ファイルが チェスト に移動された日付と時刻。
 - **Category**: ファイルが位置する チェスト 内の区分の名前。
 - **Virus description**: avast! ウィルス・データベース 内にある全ウィルス名。
 - **File ID**: ファイル識別番号 avast! の内部目的で付与されます。

スケジューラ

- ・ **Create Event**: 新規イベント（タスクの起動）の予定を入れるウィンドウを表示します。
- ・ **Edit Event**: 選択したイベントを編集します。
- ・ **Delete Event**: 選択したイベントを削除します。
- ・ **Schedule Boot-Time Scan**: オペレーティング システム起動前のウイルス検査の予定を入れるダイアログを表示します。ほとんどすべてのウイルスはオペレーティング システムと共に起動しますので、このようにウイルスが活動し始める前に削除することができます。この検査の間、avast! は aswboot.txt という名前の レポート・ファイル を C:\Program Files \ALWIL Software\Avast4\Data\Report に作成します。この機能は Windows NT, 2000 および XP においてのみ有効です。
 - **Scan archive files**: 圧縮ファイルも検査します。このスキャナは圧縮形式として ZIP, ARJ, 自己解凍式 EXE, NTFS stream, TNEF stream, MIME および DBX を サポートしていません。
 - **Scan all local disks**: すべてのローカル・ディスクについてウイルスの存在を検査します。
 - **Select path to scan**: 再起動後に検査するフォルダのパスを直接入力することができ、また、"..." ボタンを使ってフォルダを見る事ができます。
 - **Advanced options**: タスク スケジュールを詳しく設定します。
 - Ask for action**: ウィルス発見時に avast! は検査を停止し、感染したファイルをどうするかを選択します。
 - Delete infected file**: 感染したすべてのファイルを削除します。
 - Move infected file**: 感染したすべてのファイルを C:\Program Files \ALWIL Software \Avast4 \Data \Moved に 移動します。
 - Ignore infected file**: 感染したファイルについて何も行いません。
- システム・ファイルが感染すると、そのようなファイルの移動や削除はシステムの安定性に重大な結果をもたらします。この理由から、avast! は システム・ファイルを処理するときには 削除または 移動のほかに追加オプションを用意しています。
- Ask for confirmation**: システム・ファイルの削除や移動を追認するのか拒否するのか尋ねま

す。

□**Allow delete or move:** avast! は確認をせずにシステム・ファイルでさえ 削除 または 移動します。このオプションは きわめて危険でありオペレーティング システムを機能不全に陥らせるかもしれません。

□**Ignore delete or move for system files:** 感染したシステム・ファイルが発見されたときに、avast! はいかなる変更もせずに元の場所に放置します。

警告！ キーボードを USB ポートを介して PC に接続していると、ブート検査中にはドライバを全く読まないのでは動作しません。

6 タスク

6.1 タスクの取扱い

・ **タスクの作成:** メイン・メニューから、Tasks → Create を選択する、または、タスク・リストの上でマウスの右ボタンをクリックして Create new を選択するか、ツールバーの Create new ボタンをクリックしてください。タスク・パラメータを定義するに新しいウィンドウが現れます。

・ **タスクの編集:** 編集したいタスクを選択して Tasks → Edit をメイン・メニュー から 選ぶか、タスクの上でマウスの右ボタンをクリックして Properties を選択する、または、タスクを選択してツールバーの Edit ボタンをクリックしてください。

・ **タスクの削除:** 削除したいタスクを選択して Tasks → Delete をメイン・メニュー から選ぶか、タスクの上で右ボタンをクリックして Delete を 選択、または、タスクを選択してツールバーの Delete を選んでください。

・ **タスクの開始:** 開始したいタスクを選択して Tasks → Start をメイン・メニュー から選ぶか、タスクの上でマウスの右ボタンをクリックして Run を選択か、タスクを選択してタスク・ツールバーの Start ボタンをクリック、タスクを選択して ENTER を押すか、タスクをダブル・クリックして下さい。

6.2 供給されるタスク

avast! プログラムのインストールの一部は、既に作成されます。インストール後すぐにユーザーが利用することができます。

供給されるタスクのリスト

・ Scan: local disks

このタスクは、問題のあるコンピュータの全ハードディスクのすべての実行可能なファイルと OLE 文書を検査します。avast! がウイルスを発見した場合には、警告メッセージ と(コンピュータにサウンド カードがインストールされていれば)アラーム音で通知します。このタスクで各ウイルスの発見を知らせます。圧縮ファイルやコンピュータのオペレーティング メモリも検査します。同様に各ディスクのシステム領域も検査します。ウイルスが全く見つからなければ、ウイルスを検出することなくタスクが終了したことを知らせる ダイアログが表示されます。

・ Scan: interactive selection

このタスクではウイルスの存在に対して前のタスクと同じ検査を実行します。検査の前に、ユーザーは検査する範囲を選択することができます。勿論同時にいくつかの範囲を選択することができます。

・ Scan: diskette A:

このタスクは前の 2 つのタスクと同じ動作をしますが、ドライブ A の フロッピー ディスク に対して行います。感染した可能性のあるすべての フロッピー ディスク についてこのタスクの実行をお勧めします。特に、他のコンピュータや他の人が使ったフロッピー ディスクに関係します。更にフロッピー ディスクの システム エリア(即ちブート セクタ)も検査します。

・ Resident protection

このタスクは(設定により)すべての起動したアプリケーション や 開いている文書を検査します。また、PC での作業のバックグラウンドでコンピュータを保護します。このタスクは、例えばファイル システムや e-mail といったコンピュータの主要な部分の保護に役立つ いくつかのプロバイダ(特別のモジュール)を含んでいます。プロバイダは別々に設定することができます。常駐保護はシステム起動時に自動的に開始されます。avast! の有効性をより高いレベルに設定して保護を実行し続けることをお勧めします。詳細については 常駐保護 の章をご覧ください。

・ Special tasks

これらは avast! プログラムにおいて特別な意味があります。そのタスクとは、スクリーン セーバー と 拡張エクスプローラです。

6.3 スクリーン・セーバー

avast! はお使いのコンピュータが動いておらずにスクリーン・セーバーが実行されている時でさえファイル検査を行うことができます。お気に入りのスクリーン・セーバーの中に小さなウィンドウを表示して検査中であることをお知らせします。例えば、検査したファイル数など。avast! が検査中にウイルスを見つけたときには検査を中断し、既知の警告ウィンドウを表示します。

スクリーン・セーバー・タスク をお使いになりたいときは、お使いの コントロール・パネル(画面)
- スクリーン・セーバーの設定に "avast! antivirus" を選択しなければなりません。

スクリーン・セーバー・タスク の設定は他のすべてのタスクの場合と同じで、スクリーン・セーバー
のページだけが追加されます。

・ **Screen saver** インストールされた スクリーン・セーバーのリストから実行するものを1つ選択し
てください。

・ **Settings.** avast! の 設定ではなく選択した スクリーン・セーバーに対応する通常の
Windows スクリーン・セーバーの設定です。 問題が生じたときは Windows OS のヘルプを調
べて下さい。

・ **Scan for viruses** このオプションは スクリーン・セーバーの中のウィルスを検査します。 チェッ
クをしなければ avast! スクリーン・セーバーは通常のものと同様の動作をします。

・ **Loop scanning** スクリーン・セーバーが定義されたすべての領域を検査したあと、最初からもう
一度開始します。

・ **Windows movement speed** 検査の進捗を示すウィンドウのスクリーン上の位置をどのくらい頻
繁で変えるかを指定します。

6.4 タスクの環境設定

タスクの作成または編集時に、タスクのパラメータの変更ができるたくさんのページのあるウィンド
ウが表示されます。 ここにはパラメータの意味やデフォルトの値といった説明があります。 すべ
てのページにアクセスするために、"追加環境設定" (ウィンドウの左下の部分) オプションにチ
ェックを入れてください。

Task

・ **Task name** タスク名。 デフォルトの名前は "Unnamed" 。

・ **Task comment** タスクの説明。 実行中のタスクの解説について概要を入力してください。 (例)
"C:\Windows フォルダのウィルス検索"

・ **Task job** タスクを常駐にするか標準(オンデマンド)にするかを選択してください。

○ **Scan files for viruses** タスクが標準化します。 ディスク および/または その他メディアの フ

ファイルに存在するウイルスを検査します。

o **Resident** タスクは常駐化します。つまりバックグラウンドで実行されコンピュータの活動を継続的に調べます。

Sensitivity

・ **Test whole files** ファイル全域についてウイルスの存在を検査するか、それともウイルスによりもっとも強く影響を受ける部分だけを検査するか、指示して下さい。ほとんどのウイルスがファイルの開始部分を上書きするか、ファイルの終わりにウイルスを付足します。この選択により avast! にファイル全域を検査させます。当然ですが、検査が少し遅くなります。

・ **Ignore virus targeting** このオプションをチェックすると avast! にデータベース中のすべてのウイルスに対してファイルを検査させます。このオプションがないと与えられたファイルのタイプに影響するウイルスに対してだけファイルを検査します。つまり avast! は COM 拡張子を持つファイルにだけ EXE ファイルに感染するウイルスを探すことになります。

Areas

ここでは検査する領域を選ぶことができます。デフォルトの値は "ローカル・ハードディスク" です。同時にいくつもの領域を選択することができ、それらはフォルダ および/または ファイルの全域であることが可能です。

領域の選択

・ **"Browse" ボタン** Explorer 風のウィンドウが開きます。ここでは個々のフォルダやファイルをチェックして検査する領域を選択できます。

・ **"Add" ボタン** このボタンを押すと予め設定された、いくつかの領域がポップアップメニューで現れます。領域は以下のとおりです。

- o ローカル・ハードディスク
- o フロッピーディスク A:
- o ディスク C:
- o すべてのフロッピーディスク

- CD-ROM および DVD
- すべてのメディア
- メモリ
- オートスタート・プログラム
- オートスタート・プログラム (全ユーザー)
- その他
- 対話による選択

一番下の選択肢はタスクを実行するたびに検査する領域を選択できるようにします。その他 を選ぶとウィンドウに テキスト"<領域をタイプ>" を入力することになります。このテキストを正しいパス(例えば、"C:/Windows/System/file.exe")で置き換えてください。

・ **マウスの右ボタン** "Add" ボタン と同じ意味です。

Remove ボタンはそのリストから選択された領域を削除します。

Typye

このページでは avast! により検査するファイルのタイプを定義します。

ファイル・タイプを認識

・ **content** ファイルの拡張子を無視してファイル・タイプをそのコード (内容) により決定します。この選択は、それぞれのファイルを開いてそのタイプを解析しなければならないので、ファイルの拡張子によってタイプを 認識するよりも遅くなります。

・ **name extension** ファイルのタイプをその拡張子により決定します。この選択はウィルス検査の処理を スピード・アップします。

内容 によるファイル・タイプの決定を選択すると、ひとつの追加オプション Scan all files だけになります。つまりテキストファイルやイメージファイルのように通常ウィルスを含んでいないファイルでさえ検査します。

拡張子 によるファイル・タイプの決定を選択すると検査するための拡張子(タイプ)のリストが表示

されます。

- ・ **Add** このボタンを押すと検査するタイプのリストに拡張子を追加することができます。拡張子が判っている場合にはその種類が表示されます。(例えば、EXE を入力すれば種類 ("アプリケーション") が自動的に現れます。)

- ・ **Browse** 既知の拡張子のアルファベット順のリストを表示します。ひとつ以上の対応するファイル・タイプを選択することができます。(いくつも選択するには CTRL キーと SHIFT キーを使います)

- ・ **Remove** 選択した拡張子を検査するためのタイプのリストから削除します。

"Scan default extensions" の選択は すべての "危険な" 拡張子を上記のリストに追加します。

Results

チェックボックスを使用して、表示する結果と後で使用する為に保存する結果を選択できます。

- ・ **Infected files** ウィルス・コードを含んでいるファイルについての情報

- ・ **Files with hard errors** ファイルの検査中に重大な、予期しないエラー (例えば、検査するファイルの入っているフロッピーディスクが 読めない) が生じるとファイル名を表示します。

- ・ **Files with soft errors** 検査することができないファイルを表示します。大抵は共有違反(一部のシステムファイル)かファイルへのアクセスが拒否された(例えば、現在のユーザーが その権限内にあるフォルダにアクセスしない)などです。

- ・ **Files not testes by the scanner** (例えばその大きさのために)スキップしたファイルを表示します。(ファイルが小さすぎてどんなウィルス・コードも入りようがなければスキップします)

- ・ **Files not tested due to exclusions settings** 現行の 例外 設定によりスキップしたファイルを表示します。

- ・ **OK files** 今検査した(および感染していないことが判った)ファイルのすべてを表示します。

Store results in internal database for later を選択するとその結果を avast! の内部データベースに保存します。後でその結果を使って処理することができます。 選択しない場合には 次回 avast! が起動された時にその結果は失われます。

Exclusions

avast! は 検査から一部の領域を、たとえそれが1つのファイルであっても、除外することができます。つまり avast! はそこではウィルスを検索しません。それは様々な場合に利用されます。

・ **Avoiding false alarms** avast! がファイル内のウィルスの感染を報告しそれが誤報であることが確かであれば、そのファイルを検査から除外してそれ以上の誤報を回避することができます。しかしながら、我々がこの問題を解決できるよう、該当するファイルを送信して頂けると嬉しく思います。

・ **Speeding up the processing** 例えばイメージだけを含んでいるようなディレクトリがハードディスク上にあるのなら、それを例外リストに追加することで検査から除外することができます。その結果ファイルの検査に要する時間が短縮されます。

設定

・ **Add** リストに空のアイテムを追加します。そこに除外するフォルダやファイルを書くことができます。すべてのサブフォルダを含むフォルダを選択したければ、"C:¥Windows¥*" のように "¥*" を付け足して下さい。

・ **Remove** 除外リストから選択したフォルダやファイルを削除します。

・ **Browse Explorer** 風のウィンドウが開きます。ここでは全てのパスをタイプしなくても、希望するフォルダやファイルを選択できます。

Virus

このページではタスクがウィルスを発見した時、どのような行動を取るか指示できます。デフォルトの設定は **choose action** です。演算命令 "...and..." と "...if failed, then..." を使用して、ひとつだけでなく、様々な行動を定義できます。

・ **演算命令 "...and..."** 選択したすべての動作を指示した順番(左から右へ)に行います。

・ **演算命令 "...if failed, then..."** avast! は指示された最初の動作を試みます。成功すれば他のものはすべて無視します。しかしその動作に失敗すると avast! はそれに続く動作を処理しようとしています。

ウィルスについての動作 ;

・ **Choose action** ウィルスが見つかりとタスクは一時的に停止します。ウィンドウが開いて採用する動作を選べます。対話 ボタンを押して、このウィンドウ内に提示される可能な動作を選択して下さい。

・ **Repair** avast! は感染したファイルの修復を試みます。選択するとファイルを修復する方針を記述したウィンドウを表示されます。このウィンドウですべてのマクロを Word 6 文書から削除するか、選択できます。ウィルスが正確に鑑定されないときは、全てのマクロが Word 6 文書から自動的に削除されます。Word97, Excel95 および Excel97 文書については、この選択で全てのマクロが削除されます。実行型ファイルのウィルス の場合、avast! は ウィルス修復データベース に保存されている情報を基づき、削除を試みます。ウィルス修復データベース に全く記録がないファイルは修復することができません！ ブート・ウィルス の場合、avast! は フロッピーディスク の ブートセクタに上書きしてウィルスを除去します。

・ **Move / Rename** 感染したファイルを移動するか名前を書き換えます。ファイルを移動するフォルダを指示することができます。

・ **Move to Chest** 感染したファイルを ウィルス・チェスト に移動します。

・ **Delete** 感染したファイルを削除します。削除の追加オプションを設定することができます。デフォルトの設定は delete file(s) permanently で、ファイルはお使いのコンピュータ（ハードディスク、フロッピーディスク、...）から完全に削除されます。再起動が組込まれていれば OS を再起動したときにファイルを削除するよう、この選択で指示できます。実行中はウィルスのファイルをすぐに削除することができませんのでとても 便利な設定です。avast! はどれが対象ファイルか"覚えています"、次のオペレーション・システム起動時(即ち、ウィルスが再び活動する前に)できるだけ早くファイルを削除します。delete file(s) to recycle bin オプションは ファイルを物理的に削除するのではなく、「ごみ箱」に移動します。

・ **Stop** 最初のウィルス本体が見つかったときにタスクを停止します。ウィルスに対して何も動作しません。

Packer

このページでは タスクの処理中に avast! が検査する圧縮ファイルを設定します。デフォルトの設定は 自己解凍式実行ファイル のみです。もちろん検査は遅くなりますが、追加圧縮ファイルを設定して処理することができます。All packers オプションをチェックすると avast! は 処理することができるすべての圧縮ファイルを検査します。

avast! は 次の圧縮ファイルを処理することができます。

- ・ 自己解凍式 DOS 実行ファイル
- ・ 自己解凍式 Win32 実行ファイル (UPX, AsPack, PESHield, ...)
- ・ 7ZIP 圧縮ファイル
- ・ ACE 圧縮ファイル
- ・ ARC 圧縮ファイル
- ・ ARJ 圧縮ファイル
- ・ BZIP2 圧縮ファイル
- ・ CAB 圧縮ファイル
- ・ CHM 圧縮ファイル
- ・ CPIO 圧縮ファイル
- ・ DBX 圧縮ファイル (Outlook Express)
- ・ GZIP 圧縮ファイル
- ・ インストーラー 圧縮ファイル (Wise, ...)
- ・ ISO 圧縮ファイル
- ・ LHA 圧縮ファイル
- ・ MAPI ファイル (*.pst)
- ・ MIME
- ・ NTFS ストリーム
- ・ OLE 圧縮ファイル (DOC, XLS, MSI, ...)

- ・ RAR 圧縮ファイル
- ・ RPM 圧縮ファイル
- ・ SIS 圧縮ファイル
- ・ TAR 圧縮ファイル
- ・ TNEF ストリーム
- ・ ZIP 圧縮ファイル
- ・ ZOO 圧縮ファイル

Report

avast! は 過去のセッションについての情報を含むレポートを作成し保存できます。基本的に、結果セッションと同じ情報を含みます。

- ・ **Create report file** このオプションをチェックして、レポート・ファイルの作成。
- ・ **Report File Folder** レポート・ファイルのパスや名前を、例えば C:\¥Reports¥task_name.rpt と入力します。 Browse ボタンを押すことで、フォルダの選択を実行します。デフォルトのレポート・ファイル名は対応するタスクの名前です。
- ・ **Log Record For** レポートに記載すべきアイテムをチェックします。 **Task start** は タスクを起動した日時をレポートに記載します。同様に **task stop** は タスクを停止した日時を記載します。残りの **hard errors, soft errors, skipped files, infected files** および **OK files** の説明は結果の ページにあります。
- ・ **Type of file** レポート・ファイルの書式を選択します。単純な テキストファイル か、または新しい XML フォーマットを選ぶことができます

注意: デフォルトのレポート・ファイル名は task_name.rpt です。*.rpt ファイルは実際には単純なテキストファイルですので、例えば Notepad で閲覧 / 編集することができます。

Alerts

avast! は ウィルスの発生について警告メッセージを送ることができます。この機能がネットワーク管理者にとって役立つのは、管理下にあるコンピュータにウィルスが存在するとネットワーク管理者に通知されるからです。その結果、素早く対応することができます。

警報を次のような方法で送ることができます。

- ・ **SMTP** SMTP プロトコルを使って e-mail で警報を送ります。SMTP サーバーを定義して下さい。例)メッセージが通過するメールサーバ (例えば smtp.company.com または 192.168.1.1) 更に使用する ポート を指定して下さい(標準値は 25 です)。最後に送信者アドレス("From", つまりユーザー・アドレス)を入力して下さい。
- ・ **MAPI** MAPI プロトコルを使って e-mail として 警報を送ります。MAPI プロファイル名を対応する利用パスワードと一緒に入力してください。
- ・ **WinPopup** net send コマンドを使って警報を送ります。警報送信先コンピュータの IP アドレスまたはネットワークアドレスを入力してください。
- ・ **ICQ** 警報を ICQ メッセージで送信します。警報送信先の ICQ クライアントの UIN を入力してください。
- ・ **Windows Messenger** Windows Messenger プログラムのメッセージとして警報を送信します。警報を受信者の e-mail アドレスを入力してください。Windows Messenger サービスにログイン用に使用します。
- ・ **Add** ボタンを押した後、使用するプロトコル(SMTP/MAPI/ICQ...) を選択します。更に、対応する設定(上記参照)を入力できます。
- ・ **Remove** 選択したアドレスを削除します。
- ・ **Edit** 選択したアドレスを編集します。
- ・ **Test** テスト・メッセージを選択したアドレスに送ります。
- ・ **Test all** テスト・メッセージをリスト上のすべてのアドレスに送ります。

Schedule

avast! は 指定した日時にタスクの自動起動をスケジュール化できます。

- ・ **Add** 新規の予定イベントを加えます。つまりタスクの起動をスケジュール化します。

・ **Modify** 選択した予定イベントを変更します。

・ **Delete** 選択されたイベントを削除します。

指定した日時にタスクを起動させたいときは **追加** を 選択してください。新しいウィンドウが現れて、新しいイベントを定義するパラメータを入力します。

・ **Name** イベントの名前、例) "週末検査"

・ **Comment** イベントの概要を入力。例) "毎週日曜日の夜、すべてのハードディスクを検査"

・ **Disabled** このオプションは予定したタスクの実行を取りやめます。タスクの実行を停止しなければならないが、そのタスクを完全に削除することを望まず、後で再びそれを記入しなければならないときに使用します。

・ **Do not start the task if running on batteries** 特にノートブック・パソコンの所有者にとって有用です。コンピュータがバッテリーで動いているときには、そのイベントを開始しません。

・ **Terminate the task if battery mode begins** もし、予定されたイベントの実行中に、コンピュータが電源を切ってバッテリーに切り替わると、タスクを終了します。これも特にノートブック・パソコンの所有者にとって有用です。

・ **Scheduled task** 既存タスクを選択してスケジュール化

・ **Scheduling type** ここではタスクを実行する時間を指定します。可能なオプションは **once**, **daily**, **weekly** および **monthly** です。 **once** を選択した場合、実行日時を入力します。 **daily** を選択した場合、時間のみ入力します。タスクは毎日、指定時間に起動します。最後に、 **weekly(monthly)** を選択すると、タスクの起動時間だけでなく、曜日(月)も選択して下さい。

7 常駐保護

7.1 概要

常駐保護は特別なタイプのタスクです。全ての実行プログラムと開示される文書全てを(その設定に従って)監視します。これによりウィルスの感染をリアルタイムに効果的に回避します。タスクには多数のプロバイダと呼ばれるモジュールが存在します。プロバイダは特別なモジュールで、ファイル・システム や e-mail 等、コンピュータの様々な部分を保護します。これらの各モジュールは個別に設定できます。

常駐保護には "デフォルト" と呼ばれる、特別なタスク・プロパティが与えられています。デフォルトに指定されたタスクはオペレーティング・システムが起動するたびに自動的に起動します。それを停止することはお勧めしません。システムトレイの 文字"a" のアイコンで表示されます。

7.2 常駐保護の設定

常駐保護の設定へ到達するには、基本機能ユーザ・インターフェース、高機能ユーザ・インターフェース、またはシステムトレイの常駐保護アイコンをクリックします。

- ・ **Simple User Interface** 一般的な設定に限り 基本機能ユーザ・インターフェース から選択することができます。選択には 3 つのレベルがあります。詳細については、基本機能ユーザ・インターフェース の 常駐保護 を ご覧ください。
- ・ **Enhanced User Interface** 高機能ユーザ・インターフェース で、常駐保護でご利用頂ける全設定に繋がります。常駐保護 タスクを直接編集ができます。(マウスの右ボタンで "Resident protection" タスクをクリックして Edit を選択してください)
- ・ **System tray icon** マウスの右ボタンでシステムトレイにある常駐保護アイコン (文字 "a") をクリックして、On-Acess Protection Control を選択してください。高機能ユーザ・インターフェース の場合と同じ機能を持った環境設定になります。

7.3 常駐保護プロバイダ

avast! 常駐保護には常駐プロバイダと呼ばれる、特別なモジュールを基礎にしています。ファイル・システムや e-mail 等、コンピュータの様々な部分を保護します。

- ・ **Standard Shield** 実行中のアプリケーションと開封された文書を検査します。感染したアプリケーションの起動や、感染したドキュメントを開きません。ウィルスの活動 / 拡散 から保護します。
- ・ **Outlook/Exchange** MS Outlook クライアントや MS Exchange が処理する、e-mail メッセージの送受信を検査します。(MS outlook は MS Office パッケージの一部です。より簡単な Outlook Express と同じではありません！)
- ・ **Internet Mail** MS Outlook や Exchange 以外のクライアントで処理される e-mail メッセージの送受信を検査します。例) Outlook Express, Eudora 等。ここでもウィルスのコードを含んだメッセージの送受信を拒否します。

- ・ **Script blocking** 閲覧になる WEB ページに含まれるスクリプトを検査します。ご利用される WEB ブラウザの潜在的なバグによる感染を回避します。
- ・ **Instant Messaging** ICQ や MSN Messenge 等、一般的な コミュニケーション プログラム により ダウンロードされたファイルを検査します。
- ・ **P2P Shield** Kazaa、その他の一般的な P2P (ファイル共有) プログラム により ダウンロードされたファイルを検査します。
- ・ **Network Shield** インターネット ワーム (例えば Blaster, Sasser 等) の 攻撃 から コンピュータを保護します。
- ・ **Web Shield** (閲覧、ファイルのダウンロード 等 の) インターネットによる一般的な作業中において、コンピュータ を ウィルスから保護します。また、特定の Web ページへのアクセスもブロックできます。

7.4 標準シールド - プロバイダの設定

標準シールドは起動したプログラムとアクセスしたファイルを検査します。 感染したプログラムの起動は許可しませんので、ウィルスのコードは活動することができません。

- ・ **Normal**

デフォルトの設定。

- ・ **High**

デフォルトの設定に加えて、作成および変更されたファイルの検査もします。

常駐保護：標準シールド - Scanner (Basic)

Scan diskette boot sector

フロッピー・ディスクを読み込み前に、avast! がブート・セクタのウィルスを検査します。

Scan OLE documents on open

開示前、全ての OLE 文書を検査します。(例えば、MS Word 文書のウィルス検査)

Scan executed programs

全てのプログラムについて起動前にウィルス検査をします。

32/64 ビット Windows(Win32/Win64)実行型ファイル

32/64-bit アプリケーションを起動時に検査します。

16-bit Windows 実行型ファイル

16-bit アプリケーションを起動時に検査します。

MS-DOS プログラム

MS-DOS プログラムを起動時に検査します。

Scan dynamic libraries on load

アプリケーションがダイナミックリンクライブラリ (DLL ファイル) をロードするとすぐに DLL ファイルが検査されます。アプリケーションが起動するのが少し遅くなるかもしれませんが、さらなるセキュリティを保証します。

常駐保護：標準シールド - Scanner (Advanced)

Scan files on open

スキャナ (基本) ページにおいて設定したファイル・タイプに加えて、ファイル拡張子により認識される、他のファイル・タイプを指定することができます。ファイルは開始/開封時に検査されます。拡張子はカンマで区切って下さい。ワイルドカード "?" を使用できます (例えば、全ての .htm と .html の開いたファイルを検査する場合、"htm,html" またはワイルドカードを使って "ht?" を入力します。後者の場合、"htt" のように "ht" で始まる拡張子を持つ全てのファイルが検査されます)。

Always scan WSH-script files

このオプションにより確実に全てのスクリプト・ファイル (Windows Scripting Host) が検査されます。

Do not scan system libraries

開始時に信用するシステムライブラリを検査せずに、認証を有効にするための迅速な検査のみを行います。このオプションを選択すると、システムの開始が少し早くなるかもしれません。

Scan created / modified files

開いたファイルを検査するだけでなく、新規作成または修正されたファイルも含まれます。

All files

上記の設定が全てのファイルに適用されます。

Only files with selected extension

一定の拡張子(下記参照)のある、作成/修正されたファイルを検査します。

Default extension set

作成または修正されたファイルが "危険な" 拡張子を備えているときだけ検査します。

Additional extensions

作成または修正時に検査すべきファイルの拡張子を追加することができます。

常駐保護：標準シールド - Blocker

Default extension set

下で選択する処理は "危険な" 拡張子を有するすべてのファイルについてブロックされます。

Additional extension

標準拡張子セットのほかに、処理をブロックするための追加拡張子を指定することができます。ここでそれらの拡張子を入力します。複数の拡張子はコンマで区切って下さい。ここでも、ワイルドカード "?" を使うことができます。

Blocked operations

ブロックする処理をチェックします。

Opening file for writing

ファイルを読み取り専用として開くことができます。いかなる変更も保存することはできません。

Renaming file

ファイル名の変更が出来なくなります

Deleting file

ファイルの削除が出来なくなります。

Formatting

フロッピーディスクやハードディスクを初期化出来なくなります。この場合、処理がファイルに無関係なので選択された拡張子は無視されます。

Allow the operation

ブロックした処理を実行しようとする企てが検出されると、その処理を許可するのか拒否するのかを尋ねます。avast! が質問しないときは、その処理は許可されます。

Deny the operation

ブロックした処理を実行しようとする企てが検出されると、その処理を許可するのか拒否するのかを尋ねます。avast! が質問しないときは、その処理は拒否されます。

常駐保護：標準シールド - Advanced

Show detailed info on performed action

このオプションを設定すると、常駐保護は現在検査しているファイルについて情報提供します。情報はスクリーンの右下の角、システムトレイの真上に表示されます。

"Silent" モード

サーバー・オペレーティング・システムで主に用います。このオプションにより確実に常駐保護はユーザーとの対話要求を行わず、全てのウィンドウを表示しなくなります。上記の理由より、サイレント・モードのウィルス のページで "動作を選択する" 設定はお勧めしません。対話型アクションの選択はユーザーとの対話を要求するからです。ファイルの削除やチェストへの移動等、特定のアクションを予め設定する事をお勧めします。

With answer Yes (OK) と答える

普通的环境下でスクリーンに表示される avast! のすべての質問に対して「Yes」と返信します。選択したアクションが"choose action"である場合は、結局 OK ボタン を 押したのと同じこととなります。

With answer No (Cancel) と答える

普通的环境下でスクリーンに表示される avast! のすべての質問に対して「No」と返信しま

す。 選択したアクションが 結局 choose action である場合は、Delete ボタンを 押したのと同じこととなります (即ち、感染したファイルは削除されます。)。

List of excluded areas

ここに掲載された領域は検索や検査をされません。 そのリストに予め調整した領域を置いておくことをお勧めします。 "Add と Remove" ボタンを使用してリストを編集できます。

常駐保護：標準シールド - Packers

このページでは タスクの処理中に avast! が検査する圧縮ファイルを設定します。 デフォルトの設定は 自己解凍式実行ファイル のみです。 もちろん検査は遅くなりますが、追加圧縮ファイルを設定して処理することができます。 すべての圧縮形式 オプションをチェックすると avast! は処理することができるすべての圧縮ファイルを検査します。

avast! は 次の圧縮ファイルを処理することができます。

自己解凍式 DOS 実行ファイル

自己解凍式 Win32 実行ファイル (UPX, AsPack, PEShield, ...)

7ZIP 圧縮ファイル

ACE 圧縮ファイル

ARC 圧縮ファイル

ARJ 圧縮ファイル

BZIP2 圧縮ファイル

CAB 圧縮ファイル

CHM 圧縮ファイル

CPIO 圧縮ファイル

DBX 圧縮ファイル (Outlook Express)

GZIP 圧縮ファイル

Installer 圧縮ファイル (Wise, ...)

ISO 圧縮ファイル

LHA 圧縮ファイル

MAPI ファイル (*.pst)

MIME

NTFS ストリーム

OLE 圧縮ファイル (DOC, XLS, MSI, ...)

RAR 圧縮ファイル

RPM 圧縮ファイル

SIS 圧縮ファイル

TAR 圧縮ファイル

TNEF ストリーム

ZIP 圧縮ファイル

ZOO 圧縮ファイル

常駐保護：標準シールド - Virus

このページではタスクがウィルスを発見した時、とるべき行動を指示できます。デフォルトの設定は **choose action** です。演算命令 "...and..." と "...if failed, then..." を使用して、ひとつだけでなくたくさんの行動を定義することができます。

演算命令 "...and..."

選択した動作のすべてを指示した順番(左から右へ)に行います。

演算命令 "...if failed, then..."

avast! は指示された最初の動作を試みます。成功すれば他のものはすべて無視します。しかしその動作に失敗すると avast! はそれに続く動作を処理しようとします。

ウィルスについての動作

Choose action

ウィルスが見つかったとタスクは一時的に停止します。ウィンドウが表示され、ウィンドウ内で取るべき動作が選択できます。対話 ボタンを押してこのウィンドウ内に提示される 可能な動作を選択してください。

Repair

avast! は感染したファイルの修復を試みます。これを選択するとファイルを修復する方針を記述したウィンドウを表示します。このウィンドウですべてのマクロを Word 6 文書から削除するかどうかを選ぶことができます。ウィルスが正確に鑑定されないときは Word 6 文書からマクロのすべてが自動的に削除されます。Word97, Excel95 および Excel97 文書については、この選択によりマクロのすべてが削除されます。実行型ファイルのウィルス の場合、avast! は ウィルス修復データベース に保存されている情報を基にして 削除しようとします。ウィルス修復データベース に全く記録がないファイルは修復することができません！ ブート・ウィルス の場合、avast! は フロッピーディスク の ブートセクタに書き込んでウィルスを除去します。

Move / Rename

感染したファイルを移動するか名前を書き換えます。ファイルを移動するフォルダを指示できません。

Move to Chest

感染したファイルを ウィルス・チェスト に移動します。

Delete

感染したファイルを削除します。削除の追加オプションを設定することができます。デフォルトの設定は delete file() permanetly で、ファイルはお使いのコンピュータ (ハードディスク, フロッピーディスク, ...) から 完全に削除されます。この選択では、再起動が組込まれていれば OS を再起動したときにファイルを削除するように指示することができます。現在実行中のウィルス (感染)ファイルがすぐ削除されませんのでとても便利な設定です。そして、avast! はそれがどの

ファイルが"記憶"します。 次のオペレーション・システム起動時に（即ち、ウイルスが再び活動する前に）該当ファイルをできるだけ早く削除します。” Delete file(s) to recycle bin” オプションはファイルを物理的に削除するのではなく、代わりに「ごみ箱」に移動します。

Stop

最初のウイルス本体が見つかったときにタスクを停止します。 ウィルスに対して何も動作しません。

7.5 Outlook/Exchange" - プロバイダの設定

この設定は MS Outlook および MS Exchange メール・クライアントのみ影響あります。 Outlook Express, Eudora 等、他のメール・クライアントの設定については インターネット・メール プロバイダ をご覧ください。

Normal

デフォルト設定

High

デフォルトの設定に加えて、既読メッセージさえも開封時に検査し、ヒューリスティック感度は「高」に設定。

常駐保護 : Outlook/Exchange - Scanner

Scan inbound messages

e-mail メッセージを受信時に、先ずウイルスを検査します。 感染していれば、ウィンドウが現れ、そのメッセージをどうするか（例えば感染した添付ファイルを削除する）を指示できます。

Scan outbound messages

送信メッセージがウイルス検査されます。

Scan archived messages on open

ディスクに保存した e-mail メッセージが開封時に検査されます。

Unread messages only

既読メッセージは検査されません（未読限定）。

Scan message bodies

e-mail の添付ファイル（もっとも一般的なウイルス・キャリア）検査だけでなく、メッセージ本体も検査されます。 その結果ウイルス検出の効果がより高く得られます。

常駐保護 : Outlook/Exchange - Inbound Mail

このページでは感染メッセージに対する avast! の対応を設定します。 更に、avast! がショートノートを受信メッセージに添付するよう指示できます。 そのメッセージにより、ウイルスを含んでいるか表示します。

avast ! が感染した受信メッセージを発見したとき

let it be delivered to your inbox ウィルス感染メッセージに手を付けず、そのまま受信トレイに届けられます。恐らくウィルスの添付ファイルを含んだままです。

Discard it unconditionally

ウィルスの添付ファイルは破棄されます。仮にウィルスがメッセージ本体に直接埋め込まれた場合、メッセージ全体が削除されます。

Move it to the following Outlook folder

感染メッセージを下記で選択した Outlook フォルダに移動します。

以下のオプションで E-Mail メッセージに挿入する記録(メモ)を作成します。

Insert notes to infected messages

ショートノートが感染メッセージに添付されます。

Insert notes to clean (uninfected) messages

ショートノートがクリーン (感染していない) メッセージにも添付されます。

Format of the notes...

挿入するノートの 書式 を変更できます。

感染メッセージに添付される記録の例 :

avast!: Inbound message INFECTED BY A VIRUS!

File EICAR.SCR (infection EICAR Test-NOT virus!!) (BEWARE!!)

left intact in the message.

Date and time of the test: 22.10.2002 13:10:07

Virus database (VPS) date: 17.10.2002

avast! antivirus by Alwil Software

常駐保護 : Outlook/Exchange - Outbound Mail

Insert notes to clean (uninfected) messages

avast! は感染していないメッセージにノートを挿入してウィルスがないことを知らせます。 avast! は感染メッセージの送信を全て許可しません。

Format of the notes...

挿入されるノートの 書式 を 変更できます。

Scan attachments when attaching

e-mail に同封する添付ファイルを、送信時ではなく、添付処理する間に、添付物を即座に検査します。

常駐保護 : Outlook/Exchange - Signature

署名を使用することで、検査を要するメッセージ数を大きく減らすことができます。 署名は小さな "スタンプ" です。 avast! (それがセットアップされる場合) が感染していないメッセージ添付されます。 個々の署名それぞれに日付と時間が含まれます。

重要なことは、MS Outlook/Exchange プロバイダの署名は 例えば avast!, Exchange Server Edition の 署名と完全に互換性があるということです。 ですから、Exchange サーバー が avast! を実行しているのであれば、MS Exchange サーバー プロバイダ により検査されたメッセージはクライアントの MS Outlook/Exchange プロバイダにより再び検査されることはないので、署名の追加は "スピード・アップ" に繋がります。

Insert signatures into clean messages

このオプションをチェックすると署名入りメッセージに変わります。 チェックしなければ、メッセージに署名は付きません。

Always trust signed messages

このオプションはどの程度署名を信用するかを明記します。 チェックすると正しく署名されたメッセージをプロバイダは信用し、例えどんなに古い署名であっても (オプション "現在のウィルス・データベースより古い署名を常に無視する" にチェックしているときを除いて) メッセージを検査しません。

Trust signatures only up to

ここでは信用する署名の最大年数を設定することができます。 ここで設定された値は オプション "現在のウィルス・データベースより古い署名を常に無視する" により常にマスクされます。

Ignore all signatures (no trust)

このオプションは署名を全く信用しないことを明記します。 プロバイダはいかなる署名も信用することは無く、各メッセージを無条件に検査します。

Always ignore signatures older than current virus database

このオプションをチェックすると、署名が現在の avast! ウィルス・データベース よりも古い場合、プロバイダは常に 有効な署名のあるメッセージだとしても検査します。 このオプションが有益なのは、元の検査と今日との間、その間に新しいウィルス・パターンが ウィルス・データベースに追加され、まさしくそれと同じウィルスがそのメッセージに含まれているということがあり得るからです。 avast! が古い署名を信用すると、有効な署名の存在により メッセージを検査されません。 その結果、既にウィルス・データベースに入っているにもかかわらずウィルスの 検出に失敗することになります。

常駐保護 : Outlook/Exchange - Virus Storing

ここではウィルスが発見されたときに、avast! が その感染メッセージをディスクにバックアップをとるかどうかを指示します。

Store infected items in a folder

このオプションをチェックすると、avast! 感染した目的ファイルをディスクの指定したフォルダに保存します。 フォルダを指定するには、Folder ボックス に入力してください。 また Browse ボタンを利用して、ディスクのツリー構造を表示できます。 そのボタンはローカル・コンピュータのタスクを編集するときだけ有効です。

Overwrite existing items

既にフォルダに同じ名前のファイルがあるにも関わらず、avast! が 感染ファイルを指定フォルダ

に保存しようとする場合に指示します。このオプションをチェックすると、元のファイルは上書きされます。チェックしなければ元のファイルは何もされません。

常駐保護 : Outlook/Exchange - Advanced

Show detailed info on performed action

このオプションをチェックすると、プロバイダは検査対象の各オブジェクトについて知らせます。情報はスクリーンの右下の角、システムトレイのすぐ上に表示されます。

Show tray icon when scanning mail

チェックすると、すべての動作の間、小さなアイコンがシステムトレイに表示されます。

Show splash screen when the provider is loading

チェックすると、プロバイダはサポートしている e-mail クライアント (MS Exchange クライアントおよび MS Outlook 95/97/98/2000) が起動したときにスプラッシュ・スクリーンを表示します。e-mail が保護されることを知らせるものとして有益です。

Profile と **Password** のフィールドには MAPI プロファイルと e-mail クライアントにログオンするために使用するパスワードを指示します。受信メール ページの "閲覧" ボタンを押したときにご覧になるフォルダの階層を表示するために、avast! はこれらの情報を使用します。しかしながら、そのデータはプロバイダ自信にとって重要ではありません。つまり、そのフィールドが空のままであってもプロバイダは正しく動作します。

常駐保護 : Outlook/Exchange - Heuristic

受信メールに対して avast! が検査可能であるのは既知のウィルスだけではありません。ヒューリスティック分析によりメッセージを確認し、場合によっては ウィルス・データベース にまだ登録していないウィルスを明らかにできます。このページでヒューリスティック分析の設定を変更することができます。

感度設定

Low

Basic attachments check

添付ファイルは名称とコンテンツの種類により認証されます。avast! は添付ファイルの名前が2つの拡張子を含んでいるか検査します。(2つ目は "危険" と考えられます。) 例えば、添付ファイルの名前が "Patch.jpg.exe" であれば、avast! は (そのファイルを) 潜在的に危険性があるとして扱い、警告を表示します。加えて、avast! は添付ファイルの拡張子が実際のファイル・タイプに対応しているか検査します。違う場合、警告が表示されます (例えば、ファイル "Pamela.jpg" が画像でなければ、想像されるように、名前を替えた COM ファイルかも知れません)。

Check whitespaces sequence

あるウイルスが使うトリック： 感染ファイルの名前のひとつの拡張子の後ろに、2番目の本当に危険な拡張子まで、大量のスペース(または他の表示できない "白い" 文字) を追加します。ユーザーには2番目の拡張子は見えません (それは数行下にあるか または 名前を表示する ウィンドウに収まりません)。ヒューリスティック分析はこのトリックを摘発してユーザーに警告します。デフォルトで許可されている連続長は5です。従って、5つよりも多い白い文字があれば警告メッセージが表示されることになります。

HTML part check

あるウイルスは特定のメールプログラムのバグを利用します。(特に安全でない MS Outlook と Outlook Express) このバグにより、単にプレビュー画面でメッセージを表示するだけのウイルスを起動させます。avast! はメッセージの HTML コードがそのようなトリックを実行するタグを含んでいないか検査します。もし含んでいれば、警告メッセージが表示されます。

Meidum 上記に加えて

Thorough check of attachments

添付ファイルの名前に実行型ファイルの拡張子 (EXE, COM, BAT 等) が含まれていれば、警告メッセージが表示されます。

High 上記に加えて

Subject structure check

avast! は、e-mail の件名が常に怪しい大量の無意味な文字を含んでいないかどうか検査します。例えば、件名が連続した文字列 "<?*&\$^(^%#\$_)" を含んでいれば警告が表示されます。

Outbound messages Time period check

ほとんどの最新のウイルスは e-mail によって広がり、自分自身を Windows のアドレス帳に保存されているアドレスに送ります。この拡散には典型的な症状があり、それは、非常に短い時間内に大量のアドレスにメッセージを送り、そして更にこれらのメッセージは 件名 および/または添付ファイル が同じであるということです。avast! はこれらの症状を監視して警告を發します。詳細に付いては ヒューリスティック - 追加 をご覧ください。

Outbound messages Mass messages

上記の症状の他にも、次から次へと素早く送る多くのメッセージにウイルス自身が拡散していく時、もう一つ似たような方法があります。それはウイルスが、あるメッセージの中の自分自身を、項目 To, Carbon Copy (CC) または Blind Carbon Copy (BCC) にある多くの受信者に送る ということです。avast! はこの動作の監視も行い、危険性を警告します。詳細な情報と可能な設定については ヒューリスティック - 追加 をご覧ください。

Custom

Cutomize ボタンを押すことで、ヒューリスティック分析をあなたの望むように設定することができます。お使いになりたい上記のヒューリスティック分析の部分を選んでください。

常駐保護 : Outlook/Exchange - Heuristic Advanced

このページでは送信メールに対するヒューリスティック分析の変更を行います。 "Heuristic" の感度が high または custom に 設定されている時（ および それらが custom 感度設定によってのみ変更できる時 ） 限定で、この設定を使用します。

e-mail により自分自身を拡散するウィルスは、短い時間でそのコードを含む 大量 のメッセージを送ります。 これらのメッセージは通常、同じ 件名 であるか、および/または 同じ 添付ファイルを含んでいます。 avast! により その4つの要素を検査することができ、ウィルスのような動作が検出されると警告が表示されます。 このページでは個々の値を指示することができます。

Checked time

avast! は特定時間内で、送信されたメッセージを算出します。 デフォルトの値は 30 秒 です。 30 秒以内に 5つ以上のメッセージ（ もうひとつのデフォルトの値 ） が 送られ、同じ件名を持ち、および/または 同じ添付ファイルを含んでいると、警告が表示されます。

Warnig count

同じ件名であり および/または 同じ添付ファイルを含んでいても avast! が何の警告も無しに通過させてしまったメッセージの数。 件数が超過したときに警告が表示されます。

Check subject

設定すると、ヒューリスティック分析の間 avast! が email の "件名" を 考慮します。

Check attachments

設定すると、ヒューリスティック分析の間 avast! が email の 添付 ファイルを考慮します。 ウィルスが拡散するために用いるもうひとつの手段は大量メッセージです。 先ほどの場合は、たくさんのアドレスにたくさんの e-mail を素早く送ることによりウィルスが拡散するだろうと考えました。 ここでは、ウィルスは たった一つのメッセージですが自分自身を、多数の受信者に同時に送ることを想定します。 これは avast! が 確認できるもうひとつのことであり、パラメータをここで変更することができます。 メッセージの受信者の全てを、つまり、To, Carbon copy(CC) および Blind carbon copy(BCC) のフィールドにあるアドレスを数えます。

Absolute count

デフォルトで 10 に設定されています。 この値は1件のメッセージの 受信者数であり、超過すると警告が表示されます。

Relative count (Address book)

これも1件のメッセージの受信者数が超過したときに警告が表示されます。 しかしながら、この値は Windows アドレス帳にアドレスが保存されているユーザー数のパーセント として入力されます。 デフォルトの値は 20% です。

Minimal count

ここでは、相対カウント数に対応するユーザーの最小カウント数 を設定できます。 例えば、その 20% が 10 アドレス未満である人数のユーザーが Windows アドレス帳に 含まれているときは、avast! は受信者が 10 人を超えるまでその相対数を無視します。

常駐保護 : Outlook/Exchange - Packers

このページでは タスクの処理中に avast! が検査する圧縮ファイルを設定します。デフォルトの設定は 自己解凍式実行ファイル のみです。もちろん検査は遅くなりますが、追加圧縮ファイルを設定して処理することができます。すべての圧縮形式 オプションをチェックすると avast! は処理することができるすべての圧縮ファイルを検査します。

avast! は 次の圧縮ファイルを処理することができます。

自己解凍式 DOS 実行ファイル

自己解凍式 Win32 実行ファイル (UPX, AsPack, PEShield, ...)

7ZIP 圧縮ファイル

ACE 圧縮ファイル

ARC 圧縮ファイル

ARJ 圧縮ファイル

BZIP2 圧縮ファイル

CAB 圧縮ファイル

CHM 圧縮ファイル

CPIO 圧縮ファイル

DBX 圧縮ファイル (Outlook Express)

GZIP 圧縮ファイル

ISO 圧縮ファイル

LHA 圧縮ファイル

MAPI ファイル (*.pst)

MIME

NTFS ストリーム

OLE 圧縮ファイル (DOC, XLS, MSI, ...)

RAR 圧縮ファイル

RPM 圧縮ファイル

SIS 圧縮ファイル

TAR 圧縮ファイル

TNEF ストリーム

ZIP 圧縮ファイル

ZOO 圧縮ファイル

7.6 インターネット・メール - プロバイダの設定

インターネット・メール プロバイダ は MS Outlook 及び MS Exchange 以外のメール・クライアントで処理される e-mail を保護に使用します。

Normal

デフォルトの設定。

Hign

ヒューリスティック感度を「高」に設定する。

常駐保護 : インターネット・メール - POP

受信 e-mail を検査するときの avast! の動作をこのページで設定します。

Scan Inbound mail

POP プロトコルで受信した e-mail メッセージを avast! が検査します。

Insert note in to clean message

avast! は感染メッセージに記録を挿入します。 このオプションを設定すると、感染していない (ウイルスの全く無い) メッセージにも記録が挿入されます。

常駐保護 : インターネット・メール - SMTP

送信 e-mail を検査するときの avast! の動作をこのページで設定します。

Scan outbound mail

SMTP プロトコル で送信された e-mail メッセージを avast! が検査します。

Allow sending of infected mail

avast! はウイルスを含んだメッセージを送ることもあります。 例えば、解析のために感染したファイル弊社 (Alwil a.s.) に送信、等に利用します。

Insert note into clean message

avast! は感染メッセージに記録を挿入します。 このオプションを設定すると、感染していない (ウイルスの全く無い) メッセージにも記録を挿入します。

常駐保護 : インターネット・メール - IMAP

IMAP は POP や POP3 同様、インターネット e-mail サーバーと通信する最近のプロトコルのひとつです。 e-mail 受信に IMAP プロトコルを使用されているのであれば、e-mail 検査を行うか、感染していないメッセージにも記録を添付するか、を設定できます。

Scan inbound mail

IMAP プロトコルで受信した e-mail メッセージを avast! が 検査します。

Insert note into clean message

avast! は 感染したファイルに記録を挿入します。 このオプションを設定すると、感染していない (ウイルスが全く無い) メッセージにも記録を挿入します。

常駐保護 : インターネット・メール - NNTP

このページでは、送受信するニュース、即ち Usenet ニュースグループ (NNTP プロトコル) を検査するときの avast! の 動作をセットアップします。

Scan inbound news

avast! は 購読 (受信) する全てのニュースを検査します。

Scan outbound news

avast! は 送信 (送る) 全てのニュースを検査します。

Allow posting of infected news

設定すると、avast! は ウイルスを含んだメッセージの送信を許可します。

Insert note into clean inbound news

avast! は 感染しているメッセージに記録を挿入します。 このオプションを設定すると、感染していない (ウイルスの無い) 受信メッセージにも記録を挿入するようになります。

Insert note into clean outbound news

上記と同様のオプションで、送信するメッセージに対するものです。

Format of the notes.

挿入する記録の書式を変更することができます。

常駐保護 : インターネット・メール - Redirect

このページでは 透過 e-mail 検査の設定が可能です。 この機能は NT 系 のオペレーティング システム (Windows NT/2000/XP/2003/Vista/2008) においてのみ有効です。 リダイレクト ポートの接続が avast! に送られます (即ち、ウイルスについて検査を行います) 。

Redirected ports

通常の e-mail プロトコル用のポート番号をここに入力してください。 デフォルトでは、avast! は 4 つの基本 e-mail プロトコルに対して標準のポート番号を使用します。 異なるポート (または追加のポート) を 使用する場合には、その番号を対応するボックスに記入してください。 複数の値を指定する場合にはカンマで区切る必要があります。

POP

受信メール用のポート番号。 標準ポートは 110。

SMTP

送信メール用のポート番号。 標準ポートは 25。

IMAP

IMAP ポート番号。 標準ポートは 143。

NNTP

送受信するニュース用のポート番号。 標準ポートは 119。

Ignored addresses

avast! の検査から除外したい メール サーバー の アドレス を ここに入力することができます。 無視したいポート番号を指定することもできます。 特定のアカウントからのメッセージを avast! に 検査させ (残りを無視させ) たい時に、この機能をご利用下さい。 smtp.server.com と 入力すると、avast! は 対応するアカウントの送信 (SMTP) メッセージを検査しません。

Ignore local communication

このオプションは常にオンにして下さい。 無効にすると avast! は (常に安全である) ローカ

ル通信さえも検査し、コンピュータがいくらか遅くなるでしょう。

注意: 実際に e-mail トラフィック用に使用している他のポート番号を入力しないで下さい。 そうしないと予期せぬ問題 (タイムアウト etc) が 生じるかもしれません。

常駐保護 : インターネット・メール - Advanced

Show detailed info on performed action

このオプションを設定すると、常駐保護は現在検査しているファイルについて知らせます。 情報はスクリーンの右下の角、システムトレイのちょうど上に表示されます。

"Silent" mode

サーバー・オペレーティング・システムで主に用います。 このオプションにより常駐保護はユーザーとの対話を 確実に要求しなくなり、ウィンドウを表示しなくなります。 このため、対話型の動作の選択は勿論 ユーザーとの対話を要求しますので サイレント・モードの **ウィルス** の ページで "行動を選択する" を設定することはお勧めしません。 ファイルの削除や チェスト への移動といったいくつかの特別な動作を予め設定された方が宜しいでしょう。

With answer Yest (OK)

普通の環境下でスクリーンに表示される avast! のすべての質問に対して 「はい」 を返します。 選択した動作が 結局 **choose action** である場合は、OK ボタンを 押したのと同じこととなります。

With answer No (Cancel)

普通の環境下でスクリーンに表示される avast! のすべての質問に対して 「いいえ」 を返します。 選択した動作が 結局 **choose action** である場合は、Delete ボタンを 押したのと同じこととなります (即ち、感染したファイルは削除されます。)。

Timeout for Internet communication

この値はメールサーバから返事を待つための秒数です。 デフォルトの値は 120 秒です。 時間内にサーバーの返事を受取らなければ、avast! は下の設定に従って行動します。

Shutdown communication

インターネット接続を閉じます。

ask

時間経過後、待ち続けるか切断するかを尋ねるウィンドウが表示されます。 これがデフォルトのオプションです。

常駐保護 : インターネット・メール - Heuristis

受信メールに対して avast!が検査可能であるのは既知のウィルスだけではありません。 ヒューリスティック分析によりメッセージを確認し、場合によっては ウィルス・データベース にまだ登録していないウィルスを明らかにできます。 このページで ヒューリスティック分析の設定を変更することができます。

感度設定

Low

Basic attachments check

添付ファイルの名前と内容の型式により認証されます。 avast! は 添付ファイルの名前が 2 つの拡張子を含んでいるか検査します。(2 つ目は "危険" と考えられます。) 例えば、添付ファイルの名前が "Patch.jpg.exe" であれば、avast! は (そのファイルを)潜在的に危険性があるとして扱い、警告を表示します。 加えて、avast! は 添付ファイルの 拡張子が実際のファイル・タイプに対応しているか検査します。 違う場合、警告が表示されます (例えば、ファイル "Pamela.jpg" が 画像でなければ、想像通り、名前を替えた COM ファイルかも知れません)。

Check whitespaces sequence

あるウイルスはトリックを使います。 感染したファイルの名前のひとつの拡張子の後ろに、2 番目の危険な実際の拡張子まで、大量のスペース (または他の表示できない "白い" 文字) を追加します。 ユーザーには2番目の拡張子は見えません (それは数行下にあるか名前を表示するウィンドウに 収まりません)。 ヒューリスティック分析はこのトリックを摘発してユーザーに警告します。 デフォルトで許可されている連続長は5です。 従って、5つよりも多い白い文字があれば 警告メッセージが表示されることとなります。

HTML part check

あるウイルスは特定のメールプログラムのバグを利用します。(特に安全でない MS Outlook と Outlook Express) このバグにより、単にプレビュー画面でメッセージを表示するだけのウイルスを起動させます。 avast! は メッセージの HTML コードがそのようなトリックを実行するタグを含んでいないか検査します。 もし含んでいれば、警告メッセージが表示されます。

Medium 上記に加えて

Thorough check of attachments

添付ファイルの名前に実行型ファイルの拡張子 (EXE, COM, BAT 等) が含まれていれば、警告メッセージが表示されます。

High 上記に加えて

Subject structure check

avast! は、e-mail **件名**が 怪しい大量の無意味な文字を含んでいないかどうか常に検査します。 例えば、件名が 連続した文字 "<?*&\$^(^%#\$_())" を 含んでいれば警告が表示されます。

Outbound messages Time period check

ほとんどの最新のウイルスは e-mail によって広がり、自分自身を Windows のアドレス帳に保存されているアドレスに送ります。 この拡散には典型的な症状があり、それは、非常に短い時間内に 大量のアドレスにメッセージを送り、そして更にこれらのメッセージは 件名 および/または添付ファイル が 同じであるということです。 avast! はこれらの症状を監視して警告を發します。 詳細に付いては ヒューリスティック - 追加 を ご覧ください。

Outbound messages Mass messages

上記の症状の他にも、次から次へと素早く送る多くのメッセージにウイルス自身が拡散していく時、

もう一つ似たような方法があります。それはウィルスが、あるメッセージの中の自分自身を、項目 To, Carbon Copy (CC) または Blind Carbon Copy (BCC) にある多くの受信者に送る というものです。avast! はこの動作の監視も行い、危険性を警告します。詳細な情報と可能な設定については ヒューリスティック - 追加 をご覧ください。

Custom

Customize ボタンを押すことで、ヒューリスティック分析をあなたの望むように設定することができます。お使いになりたい上記のヒューリスティック分析の部分を選んでください。

常駐保護 : インターネット・メール - Heuristic Advanced

このページでは送信メールに対するヒューリスティック分析の設定を行います。"ヒューリスティック" の感度が High または Custom に設定されている時 (および それらが カスタム 感度設定によってのみ変更できる時) にだけこの設定を使用します。

e-mail により自分自身を拡散するウィルスは、短い時間 に そのコードを含む大量のメッセージを送ります。これらのメッセージはいつも同じ 件名であるか、および/または 同じ 添付ファイルを含んでいます。avast! により その4つの要素を検査することができ、ウィルスのような動作が検出されると警告が表示されます。このページでは個々の値を指定することができます。

Checked time

avast! は与えられた時間の間、送信メッセージを数えます。デフォルトの値は 30 秒 です。30 秒以内に5つ以上のメッセージ (もうひとつのデフォルトの値) が 送られ、同じ件名を持ち および/または 同じ添付ファイルを含んでいると、警告が表示されます。

Warning count

同じ件名を持ち および/または 同じ添付ファイルを含んでいても avast! が何の警告も無しに通過させてしまった メッセージの数。件数が超過したときに警告が表示されます。

Check subject

設定すると、ヒューリスティック分析の間 avast! が email の "件名" を 考慮します。

Check attachments

設定すると、ヒューリスティック分析の間 avast! が email の 添付ファイルを考慮します。

ウィルスが拡散するために用いるもうひとつの手段は大量メッセージです。先ほどの場合は、たくさんのアドレスにたくさんの e-mail を素早く送ることによりウィルスが拡散するだろうと考えました。ここでは、ウィルスは たった一つのメッセージですが自分自身を、多数の受信者に同時に送ることを想定します。これは avast! が 確認できるもうひとつのことであり、パラメータをここで変更することができます。メッセージの受信者の全てを、つまり、To, Carbon copy(CC) および Blind carbon copy(BCC) のフィールドにあるアドレスを数えます。

Absolute count

デフォルトで 10 に設定されています。この値は1件のメッセージの 受信者数であり、超過すると警告が表示されます。

常駐保護 : インターネット・メール - Packers

このページでは タスクの処理中に avast! が検査する圧縮ファイルを設定します。デフォルトの設定は **自己解凍式実行ファイル** のみです。もちろん検査は遅くなりますが、追加圧縮ファイルを設定して処理することができます。 **すべての圧縮形式** オプションをチェックすると avast! は処理することができるすべての圧縮ファイルを検査します。

avast! は 次の圧縮ファイルを処理することができます。

自己解凍式 DOS 実行ファイル

自己解凍式 Win32 実行ファイル (UPX, AsPack, PEShield, ...)

7ZIP 圧縮ファイル

ACE 圧縮ファイル

ARC 圧縮ファイル

ARJ 圧縮ファイル

BZIP2 圧縮ファイル

CAB 圧縮ファイル

CHM 圧縮ファイル

CPIO 圧縮ファイル

DBX 圧縮ファイル (Outlook Express)

GZIP 圧縮ファイル

ISO 圧縮ファイル

LHA 圧縮ファイル

MAPI ファイル (*.pst)

MIME

NTFS ストリーム

OLE 圧縮ファイル (DOC, XLS, MSI, ...)

RAR 圧縮ファイル

RPM 圧縮ファイル

SIS 圧縮ファイル

TAR 圧縮ファイル

TNEF ストリーム

ZIP 圧縮ファイル

ZOO 圧縮ファイル

常駐保護 : インターネット・メール - Virus

このページではタスクがウィルスを発見した時、とるべき行動を指示できます。デフォルトの設定は **動作を選ぶ** です。演算命令 "...and..." と "...if failed, then..." を使用して、ひとつだけでなくたくさんの行動を定義することができます。

演算命令 "...and..."

選択した動作のすべてを指示した順番(左から右へ)に行います。

演算命令 "...if failed, then..."

avast! は指示された最初の動作を試みます。成功すれば他のものはすべて無視します。しかしその動作に失敗すると avast! はそれに続く動作を処理しようとします。

ウイルスについての動作

Choose action

ウイルスが見つかりとタスクは一時的に停止し、ウィンドウが表われます。ウィンドウ内で取るべき動作が選択できます。対話 ボタンを押してこのウィンドウ内に提示される 可能な動作を選択してください。

Repair

avast! は感染したファイルの修復を試みます。これを選択するとファイルを修復する方針を記述したウィンドウを表示します。このウィンドウですべてのマクロを Word 6 文書から削除するかどうかを選ぶことができます。ウイルスが正確に鑑定されないときは Word 6 文書からマクロのすべてが自動的に削除されます。Word97, Excel95 および Excel97 文書については、この選択によりマクロのすべてが削除されます。実行型ファイルのウイルス の場合、avast! は ウィルス修復データベース に保存されている情報を基にして 削除しようとします。ウイルス修復データベース に全く記録がないファイルは修復することができません！ ブート・ウイルス の場合、avast! は フロッピーディスク の ブートセクタに上書きしてウイルスを除去します。

Move / Rename

感染したファイルを移動するか名前を書き換えます。ファイルを移動するフォルダを指示することができます。

Move to Chest

感染したファイルを ウィルス・チェスト に移動します。

Delete

感染したファイルを削除します。削除の追加オプションを設定することができます。デフォルトの設定は delete file(s) permanently で、ファイルはお使いのコンピュータ (ハードディスク, フロッピーディスク, ...) から 完全に削除されます。この選択では、再起動が組込まれていれば OS を再起動したときにファイルを削除するように指示することができます。現在実行されているウイルスのファイルをすぐに削除することができませんのでとても 便利な設定です。ですから、avast! はそれがどのファイルであり、次のオペレーション・システム起動時に (即ち、ウイルスが再び活動する前に) どのファイルをできるだけ早く削除しなければならないのかを "覚えています"。delete file(s) to recycle bin オプションは ファイルを物理的に削除するのではなく、代わりに「ごみ箱」に移動します。

Stop

最初のウイルス本体が見つかったときにタスクを停止します。ウイルスに対して何も動作しません。

7.7 スクリプト・ブロック - プロバイダの設定

スクリプト・ブロック プロバイダは WEB ページのスクリプト・ウイルスからご利用中のコンピュータを保護するモジュールです。 特定 WEB ページにはスクリプト・ウイルスを含んでいると思われる。 通常、そのようなウイルスの活動は重要ではありません。 いかなるファイルにもアクセスさせない保護モードでスクリプトが動いているからです。 とはいえ、理論的に、この方法で感染させられる可能性があります (誰かがウイルスにより不当に利用できるブラウザのバグを見つけるかも知れません)。 それが avast! が WEB ページのスクリプトを検査する理由です。

Normal

このプロバイダに対してこの設定は何の意味もありません。

Hign

このプロバイダに対してこの設定は何の意味もありません。

常駐保護： スクリプト・ブロック - Protected Programs

スクリプト検査を行いたい WEB ブラウザを選択してください。

常駐保護： スクリプト・ブロック - Advancced

Show splash window on startup

このオプションを設定すると、スクリプト・ブロック プロバイダは毎回起動毎に数秒間 スプラッシュ・スクリーン を表示します。プロバイダがアクティブであることを知らせます。

Show detailed info on pereformed action

このオプションをチェックすると、プロバイダは各オブジェクトの検査について知らせます。 情報はスクリーンの右下の角、システムトレイのちょうど上に表示されます。

Silent mode

サーバー・オペレーティング・システムで主に用います。 このオプションにより確実に、常駐保護はユーザーとの対話要求を行わなくなり、ウィンドウを表示しなくなります。 このため、サイレント・モードの ウィルス のページで "行動を選択する" を設定することはお勧めしません。 対話型アクションの選択は当然ユーザーとの対話を要求するからです。 ファイルの削除や チェストへの移動といったいくつかの特別なアクションを予め設定された方が宜しいでしょう。

With answer No (Cancel)

通常的环境下でスクリーンに表示される avast! のすべての質問に対して No を返します。 選択した動作が Choose action である場合は、Delete ボタンを押したのと同じこととなります (即ち、感染したファイルは削除されます)

このプロバイダでは「はい」という答えをサイレント・モードに設定することはできません。

常駐保護： スクリプト・ブロック - Virus

このページではタスクがウイルスを発見した時、とる行動を指示できます。 デフォルトの設定は動作を選ぶ です。 演算命令 "...and..." と "...if failed, then..." を使用して、ひとつだけでなく

たさんの行動を定義することができます。

演算命令 "...and..."

選択した動作のすべてを指示した順番(左から右へ)に行います。

演算命令 "...if failed, then..."

avast! は指示された最初の動作を試みます。成功すれば他のものはすべて無視します。しかしその動作に失敗すると avast! はそれに続く動作を処理しようとします。

ウィルスについての動作

Choose action

ウィルスが見つかったとタスクは一時的に停止しウィンドウが開いて採用する動作を選ぶことができます。 **Interactive** ボタンを押してこのウィンドウ内に提示される 可能な動作を選択してください。

Repair

avast! は感染したファイルを修復しようとします。 これを選択するとファイルを修復する方針を記述したウィンドウを表示します。 このウィンドウですべてのマクロを Word 6 文書から削除するか、選択可能になります。 ウィルスが正確に鑑定されないときは Word 6 文書から全てのマクロが自動的に削除されます。 **Word97, Excel95** および **Excel97** 文書については、この選択によりマクロのすべてが削除されます。 **実行型ファイルのウィルス** の場合、avast! は ウィルス修復データベース に保存されている情報を基にして 削除しようとします。 ウィルス修復データベース に全く記録がないファイルは修復することができません！ **ブート・ウィルス** の場合、avast! は フロッピーディスク の ブートセクタに書き込んでウィルスを除去します。

Move / Rename

感染したファイルを移動するか名前を書き換えます。 ファイルを移動するフォルダを指示することができます。

Move to Chest

感染したファイルを ウィルス・チェスト に移動します。

Delete

感染したファイルを削除します。 削除の追加オプションを設定することができます。 デフォルトの設定は **delete file(s) permanently** で、ファイルはお使いのコンピュータ (ハードディスク、フロッピーディスク、...) から 完全に削除されます。 この選択では、再起動が組込まれていれば OS を再起動したときにファイルを削除するように指示することができます。 現在実行されているウィルスのファイルをすぐに削除することができませんのでとても 便利な設定です。 ですから、avast! はそれがどのファイルであり、次のオペレーション・システム起動時に (即ち、ウィルスが再び活動する前に) どのファイルをできるだけ早く削除しなければならないのかを "覚えています"。 **delete file(s) to recycle bin** オプションは ファイルを物理的に削除するのではなく、代わりに「ごみ箱」に移動します。

Stop

最初のウィルス本体が見つかったときにタスクを停止します。 ウィルスに対して何も動作しません。

7.8 インスタント・メッセージ - プロバイダの設定

インスタント・メッセージ プロバイダはあなたの通信プログラムを保護します。 たくさんの通信プログラムが他のユーザーとのファイルの送受信が可能です。 このように、感染したファイルを手に入れて更にそれを拡散することはかなり簡単なのです。 あるウイルスはユーザーの知らないところで通信プログラムを使って拡散することさえできるのです。 **インスタント・メッセージ** プロバイダはこの種の感染を回避します。 受信または送信ファイルを保存するフォルダを監視します。 そのフォルダの内容が変われば（新しいファイルが現れる、ファイルが編集される等）いつでも avast! は すぐに検査を行います。 Windows NT/2000/XP/2003/Vista/2008 オペレーティング システムでは、（指定されたフォルダの外であっても）通信プログラムによって変更されたすべてのファイルが検査されます。

次の通信プログラムをサポートしています。

AIM (AOL Instant Messenger)

Gadu-Gadu*

gaim*

Google Talk*

ICQ

IM2 Messenger*

Miranda*

mIRC*

MSN / Windows Messenger

Odigo*

PalTalk Messenger*

Psi Jabber Client*

SIM (Simple Instant Messenger)*

Skype*

Tlen*

Trillian

WengoPhone*

Yahoo! Messenger

注意: アスタリスク (*) のついているプログラムの保護は Windows NT, 2000, XP, 2003, Vista および 2008 においてのみ有効です。

常駐保護 : インスタントメッセージング - Program

このページでは、常駐プロバイダにより保護されるべき通信プログラムを明記できます。

Windows 95/98/ME の Trillian プログラム を 保護するのであれば、環境設定ファイル talk.ini にそのパスを入力しなければなりません（ **Browse** ボタンを使用することができます ）。

一部のプログラムは Windows NT, 2000, XP, 2003, Vista または 2008 においてのみ 保護することができます。

常駐保護：インスタントメッセージング - Archives

このページでは タスクの処理中に avast! が検査する圧縮ファイルを設定します。デフォルトの設定は **自己解凍式実行ファイル** のみです。もちろん検査は遅くなりますが、追加圧縮ファイルを設定して処理することができます。 **すべての圧縮形式** オプションをチェックすると avast! は処理することができるすべての圧縮ファイルを検査します。

avast! は **次の圧縮ファイルを処理することができます。**

自己解凍式 DOS 実行ファイル

自己解凍式 Win32 実行ファイル (UPX, AsPack, PEShield, ...)

7ZIP 圧縮ファイル

ACE 圧縮ファイル

ARC 圧縮ファイル

ARJ 圧縮ファイル

BZIP2 圧縮ファイル

CAB 圧縮ファイル

CHM 圧縮ファイル

CPIO 圧縮ファイル

DBX 圧縮ファイル (Outlook Express)

GZIP 圧縮ファイル

ISO 圧縮ファイル

LHA 圧縮ファイル

MAPI ファイル (*.pst)

MIME

NTFS ストリーム

OLE 圧縮ファイル (DOC, XLS, MSI, ...)

RAR 圧縮ファイル

RPM 圧縮ファイル

SIS 圧縮ファイル

TAR 圧縮ファイル

TNEF ストリーム

ZIP 圧縮ファイル

ZOO 圧縮ファイル

常駐保護：インスタントメッセージング - Virus

このページではタスクがウィルスを発見した時、とるべき行動を指示できます。デフォルトの設定

は **choose action** です。演算命令 "...and..." と "...if failed, then..." を使用して、ひとつだけでなくたくさんの行動を定義することができます。

演算命令 "...and..."

選択した動作のすべてを指示した順番(左から右へ)に行います。

演算命令 "...if failed, then..."

avast! は指示された最初の動作を試みます。成功すれば他のものはすべて無視します。しかしその動作に失敗すると avast! はそれに続く動作を処理しようとします。

ウィルスについての動作

Choose action

ウィルスが見つかるとタスクは一時的に停止しウィンドウが開いて採用する動作を選ぶことができます。 **Interactive** ボタンを押してこのウィンドウ内に提示される 可能な動作を選択してください。

Repair

avast! は感染したファイルを修復しようとします。 これを選択するとファイルを修復する方針を記述したウィンドウを表示します。 このウィンドウですべてのマクロを Word 6 文書から削除するかどうかを選ぶことができます。 ウィルスが正確に鑑定されないときは Word 6 文書からマクロのすべてが自動的に削除されます。 **Word97, Excel95** および **Excel97** 文書については、この選択によりマクロのすべてが削除されます。 **実行型ファイルのウィルス** の場合、avast! はウィルス修復データベース に保存されている情報を基にして 削除しようとします。 ウィルス修復データベース に全く記録がないファイルは修復することができません！ **ブート・ウィルス** の場合、avast! は フロッピーディスク の ブートセクタに上書きしてウィルスを除去します。

Move / Rename

感染したファイルを移動するか名前を書き換えます。 ファイルを移動するフォルダを指示することができます。

Move to Chest

感染したファイルを ウィルス・チェスト に移動します。

Delete

感染したファイルを削除します。 削除の追加オプションを設定することができます。 デフォルトの設定は **delete file(s) permanently** で、ファイルはお使いのコンピュータ (ハードディスク, フロッピーディスク, ...) から 完全に削除されます。 この選択では、再起動が組込まれていれば OS を再起動したときにファイルを削除するように指示することができます。 現在実行されているウィルスのファイルをすぐに削除することができませんのでとても 便利な設定です。 ですから、avast! はそれがどのファイルであり、次のオペレーション・システム起動時に (即ち、ウィルスが再び活動する前に) どのファイルをできるだけ早く削除しなければならないのかを "覚えています"。 **delete file(s) to recycle bin** オプションは ファイルを物理的に削除するのではなく、代わりに「ごみ箱」に移動します。

Stop

最初のウィルス本体が見つかったときにタスクを停止します。 ウィルスに対して何も動作しません。

7.9 P2P シールド - プロバイダの設定

P2P シールド は (P2P プログラム, Peer-To-Peer と呼ばれる) 多くのファイル共有プログラムを保護します。 P2P ネットワーク上の管理されていないデータの流れにより、P2P ネットワークから感染したファイルを受取るリスクはむしろ高いのです。 あるウィルスは自分自身を拡散するためにユーザーに気付かれることなく P2P プログラムを乱用する能力さえあります。 P2P シールド 常駐プロバイダはファイル共有を安全にします。

次のファイル共有プログラムをサポートしています。

ABC*

Ares*

BearShare

BitComet*

BitLord*

BitPump*

BitTorrent*

CZDC++*

Direct Connect

Direct Connect++

eDonkey*

eMule*

iDC++*

iMesh

Kazaa

Kazaa Lite

KCeasy*

LimeWire*

Morpheus*

Opera's DC++*

Overnet*

Shareaza*

SoulSeek*

StrongDC++*

uTorrent*

WinMX*

Winny2*

Zultrax*

注意: アスタリスク (*) のついているプログラムの保護は Windows NT, 2000, XP, 2003,

Vista および 2008 においてのみ有効です。

常駐保護 : P2P シールド - Program

このページでは、P2P シールド により、どの P2P プログラムを保護するのか を 指定します。

一部のプログラムは Windows NT, 2000, XP, 2003, Vista または 2008 においてのみ 保護
することができます。

常駐保護 : P2P シールド - Archives

このページでは タスクの処理中に avast! が検査する圧縮ファイルを設定します。 デフォルトの
設定は **自己解凍式実行ファイル** のみです。 もちろん検査は遅くなりますが、追加圧縮ファイル
を設定して処理することができます。 **すべての圧縮形式** オプションをチェックすると avast! は
処理することができるすべての圧縮ファイルを検査します。

avast! は 次の圧縮ファイルを処理することができます。

自己解凍式 DOS 実行ファイル

自己解凍式 Win32 実行ファイル (UPX, AsPack, PEShield, ...)

7ZIP 圧縮ファイル

ACE 圧縮ファイル

ARC 圧縮ファイル

ARJ 圧縮ファイル

BZIP2 圧縮ファイル

CAB 圧縮ファイル

CHM 圧縮ファイル

CPIO 圧縮ファイル

DBX 圧縮ファイル (Outlook Express)

GZIP 圧縮ファイル

ISO 圧縮ファイル

LHA 圧縮ファイル

MAPI ファイル (*.pst)

MIME

NTFS ストリーム

OLE 圧縮ファイル (DOC, XLS, MSI, ...)

RAR 圧縮ファイル

RPM 圧縮ファイル

SIS 圧縮ファイル

TAR 圧縮ファイル

TNEF ストリーム

ZIP 圧縮ファイル

ZOO 圧縮ファイル

常駐保護 : P2P シールド - Virus

このページではタスクがウィルスを発見した時、とるべき行動を指示できます。デフォルトの設定は **choose action** です。演算命令 "...and..." と "...if failed, then..." を使用して、ひとつだけでなくたくさんの行動を定義することができます。

演算命令 "...and..."

選択した動作のすべてを指示した順番(左から右へ)に行います。

演算命令 "...if failed, then..."

avast! は指示された最初の動作を試みます。成功すれば他のものはすべて無視します。しかしその動作に失敗すると avast! はそれに続く動作を処理しようとします。

ウィルスについての動作

Choose action

ウィルスが見つかりとタスクは一時的に停止しウィンドウが開いて採用する動作を選ぶことができます。 **Interactive** ボタンを押してこのウィンドウ内に提示される 可能な動作を選択してください。

Repair

avast! は感染したファイルを修復しようとします。 これを選択するとファイルを修復する方針を記述したウィンドウを表示します。 このウィンドウですべてのマクロを Word 6 文書から削除するかどうかを選ぶことができます。 ウィルスが正確に鑑定されないときは Word 6 文書からマクロのすべてが自動的に削除されます。 **Word97, Excel95** および **Excel97** 文書については、この選択によりマクロのすべてが削除されます。 **実行型ファイルのウィルス** の場合、avast! はウィルス修復データベース に保存されている情報を基にして 削除しようとします。 ウィルス修復データベース に全く記録がないファイルは修復することができません！ **ブート・ウィルス** の場合、avast! は フロッピーディスク の ブートセクタに上書きしてウィルスを除去します。

Move / Rename

感染したファイルを移動するか名前を書き換えます。 ファイルを移動するフォルダを指示することができます。

Move to Chest

感染したファイルを ウィルス・チェスト に移動します。

Delete

感染したファイルを削除します。 削除の追加オプションを設定することができます。 デフォルトの設定は **delete file(s) permanently** で、ファイルはお使いのコンピュータ (ハードディスク, フロッピーディスク, ...) から 完全に削除されます。 この選択では、再起動が組込まれていれば OS を再起動したときにファイルを削除するように指示することができます。 現在実行されているウィルスのファイルをすぐに削除することができませんのでとても 便利な設定です。 ですから、avast! はそれがどのファイルであり、次のオペレーション・システム起動時に (即ち、ウィルスが再び活動する前に)どのファイルをできるだけ早く削除しなければならないのかを "覚えています

" 。 delete file(s) to recycle bin オプションは ファイルを物理的に削除するのではなく、代わりに「ごみ箱」に移動します。

Stop

最初のウイルス本体が見つかったときにタスクを停止します。ウイルスに対して何も動作しません。

7.10 ネットワーク・シールド - プロバイダの設定

ネットワーク・シールド プロバイダ はインターネット ワームの攻撃からお使いのコンピュータを保護します。完全に置き換わるものではありませんが、ファイアウォールと似たような動作をします。ネットワーク・シールドはユーザーとの対話を全く必要としません。

注意：この常駐プロバイダは Windows NT, 2000, XP, 2003, Vista および 2008 においてのみ有効です。

・Normal この設定はこのプロバイダに対して何の意味もありません。

・High この設定はこのプロバイダに対して何の意味もありません。

常駐保護： ネットワーク・シールド - Settings

Show warning messages このオプションをオンにすると、avast! が インターネット ワーム の 攻撃を検出するたびに毎回システム領域（システム時計の上）に 警告メッセージを表示します。

Logging 全ての攻撃が ログ ファイル に 記録されるので、その履歴や頻度などを詳細に調べる事ができます。最後に検出された攻撃は Last attacks のページに表示されます。

常駐保護： ネットワーク・シールド - Last attacks

(もし "設定" の ページ で この機能がオンにされていれば) このページは ネットワーク ワーム による 最後の 10 件 の 攻撃リストを表示します。各攻撃について、日時、タイプ および 攻撃元の IP アドレス と ポート を 見ることができます。

7.11 Web シールド - プロバイダの設定

Web シールド プロバイダ は インターネットの閲覧、特に web ページからファイルをダウンロードするとき、お使いのコンピュータをウイルスの感染から保護します。

誤って感染しているファイルをダウンロードし、起動しようとする、avast! は（ファイルを開くときに全てのファイルを検査する）標準シールド プロバイダ によって感染を防ぎます。Web シールド は より早く、ファイルのダウンロード中にウイルスを検出します。その為、Web シールド により 以前よりもお使いのコンピュータはより安全になります。

このプロバイダは指定した URL アドレスをブロックすることも可能です。

このプロバイダはローカル・プロキシ・サーバーとして働きます。 NT 系 の オペレーティング システム (Windows NT/2000/XP/2003/Vista/2008) では 保護は完全に透過で、特別な設定は必要ありません。 Windows 9x/ME オペレーティング システム で Web シールドを有効にするには、インターネットオプションの設定を、特に ローカル プロキシ の アドレス と ポート を 変更する必要があります。 ですから、古い オペレーティング システム で Web シールド を お使いになる場合には、次のようにしてください。 :

ローカル エリア ネットワーク (LAN) を 使用する Windows 95, 98, および Millennium の プロキシ サーバー の 設定:

Internet Explorer:

Internet Explorer を 起動

ツール インターネット オプション... を メイン・メニューから選択

接続 ページ を 開く

LAN の設定... ボタン を クリック

LAN にプロキシ サーバーを使用する オプション に チェック を 入れる

アドレス フィールドに localhost (もしくは localhost と 同じ IP アドレス 127.0.0.1 を入力しても構いません) と 入力

ポート フィールド に 12080 を 入力

OK ボタン により決定

ダイヤルアップ接続 (モデム) を 使用する Windows 95, 98, および Millennium の プロキシ サーバー の 設定:

Internet Explorer を 起動

ツール **インターネット オプション...** を メイン・メニューから選択

接続 ページ を 開く

リストからお使いのダイヤルアップ接続を選択し **設定...** ボタン を クリック

この接続にプロキシ サーバーを使用する オプション に チェック を 入れる

アドレス フィールドに localhost (もしくは localhost と 同じ IP アドレス 127.0.0.1 を入力しても構いません) と 入力

ポート フィールド に 12080 を 入力

OK ボタン により決定

注意: 複数の接続を使用する場合にはそれぞれの接続に対して別々に ローカル プロキシ の アドレス と ポート を 設定する必要があります。

(訳注) プロキシ サーバー には HTTP プロトコルのみを設定しなければなりませんので御注意ください。 HTTPS や FTP といったほかのプロトコルはプロキシを介さずに通信するように、ダイアログ の フィールド を ブランクのままにしておかなければなりません。

(avast! support forums, avast! 4.x Home/Pro を 参照のこと)

常駐保護 : Web シールド - Basic

Enable Web scanning

チェックボックスにより web 検査機能を オン / オフして下さい (URL ブロックには影響しません)。勿論、このオプションはデフォルトでオンになっています。Web シールド プロバイダを使いたくない場合には、ここでオフにしてください。

Use intelligent stream scanning

このオプションによりどのようにダウンロードするファイルを検査するかを指定します。このオプションが有効になっていると、ダウンロードされるファイルはほとんどリアルタイムに検査されます。データの断片が到着するとすぐに検査され、前の部分にウイルスが無いことを確認して次をダウンロードします。このオプションをオフにすると、初めにファイル全体を一時フォルダにダウンロードし、その後 avast! により検査します (そしてウイルスが検出されなければ、要求をした web ブラウザに引き渡します。)。

次のオプションは Windows 95, 98 および Millennium ではご利用できません:

Redirected HTTP port(s)

avast! プロキシにリダイレクトしたい HTTP ポートの番号をここで指定することができます。数種類のプロキシ・サーバーを使用してインターネットにアクセスし、サーバーとコンピュータの間の通信を検査したいときにはこの設定が重要です。ですから、例えばポート 3128 を使用してプロキシ・サーバーに接続する場合には、この数字をボックスに入力してください。そうでない場合には、avast! はポート 80 (デフォルト) による接続を想定して他のものは無視します。

注意: HTTP 以外のポート(例えば ICQ, DC++ 等のポート)を入力しないで下さい。

複数のポート番号はカンマで区切ってください。

Ignored addresses

このアドレスには avast! プロキシにリダイレクトしない URL または IP アドレスを入れます。複数のアドレスはカンマで区切ってください。

Ignore local communication

(デフォルトでは有効になっている) このオプションは avast! が全てのローカル通信を即ち、お使いのコンピュータ上で動いているプログラム間の通信を無視することを意味します。

(訳注) HTTPS や FTP の使用するポート番号も指定しないで下さい。

(avast! support forums, avast! 4.x Home/Pro を参照のこと)

常駐保護 : Web シールド - Web Scanning

このページでは、ダウンロード中に avast! が検査するファイルを指定することができます。

ほとんどの場合デフォルトの設定が適切です。

Scan all files

avast! は ダウンロードする全てファイルを検査します。これはデフォルトで選択されています。

Scan files with these extensions

このオプションを選択すると、検査するファイルの拡張子を入力することができます。拡張子リストはカンマで区切らなければなりません。

And files of the following MIME-types

ここには検査すべきオブジェクトの MIME タイプを入力することができます。

常駐保護 : Web シールド - Exceptions

Web シールドにより検査しないオブジェクトを指定することができます。例えば、1 つの（信頼できるもの！）アドレス、サーバーからたくさんのファイルをダウンロードする時に便利です。

URLs to exclude:

Add ボタンにより無視する URL アドレスを入力してください。ひとつのページだけを指定したい場合には、全てのパスを入力する必要があります。例えば、`http://www.yahoo.com/index.html` を追加すると、`index.html` のみを検査から除外します。しかし `http://www.yahoo.com/*` と入力すると、`http://www.yahoo.com` で始まるページは検査されません。同様に、特別なファイル・タイプの検査をしたくない場合には、例えば拡張子 `txt` を持つものであれば、単に `txt` と入力してください。

MIME Types to exclude:

ここでは検査から除外したい MIME タイプ / サブタイプ を 指定することができます。

常駐保護 : Web シールド - URL Blocking

Web シールドは一定の web ページ への アクセスをブロックすることもできます。このオプションはデフォルトではオフですが便利な機能です。例えば、ご家族が "悪い" web ページ (ポルノ、不法なソフトウェア 等 を含む) へ アクセスすることを防ぐことができます。そのようなブロック ページ が web ブラウザから要求された場合には、avast! antivirus によりブロックされたページにアクセスしたことを知らせるページが表示されます。

Enable URL Blocking

このチェックボックスは URL ブロック 機能を有効にし、ブロックするアドレスの入力できるようになります。

Block URLs based on the following masks

Add ボタンを使用して、ブロックするアドレスのマスクを入力することができます。? および * の ワイルドカードを使用することができます。例えば、`http://www.penthouse.com/*` と入力すれば、`http://www.penthouse.com` から始まるページは表示されません。

avast! は 次にルールに従って入力された URL を完成させます。

アドレス が `http://` または ワイルドカード * 若しくは ? で開始しない場合には、avast! は そ

のアドレスの前に http:// を 加えて末尾にアスタリスクを付加します。 ですから、www.yahoo.com と 入力されると、avast! は http://www.yahoo.com* に 修正します。そのアドレスが http:// で 開始されていれば、avast! は そのアドレスを修正しません。

常駐保護 : Web シールド - Advanced

ここでは他の Web シールド の オプション を 設定することができます。

Show detailed info on performed action

このオプションを設定すると、今検査したファイルについての情報を常駐保護が知らせます。 お知らせは画面の右下角に、システムトレイの右上に表示されます。

Silent mode

有効にすると、Web シールドはユーザーとの対話を要求しなくなります。 ファイルのダウンロード中にウイルスが発見された時には、Web シールド は いつも表示する ウイルス ダイアログ を表示する代わりに、直ちに接続を中止します。 勿論、この時ウイルスはダウンロードされません。

常駐保護 : Web シールド - Packers

このページでは タスクの処理中に avast! が検査する圧縮ファイルを設定します。 デフォルトの設定は **自己解凍式実行ファイル** のみです。 もちろん検査は遅くなりますが、追加圧縮ファイルを設定して処理することができます。 **すべての圧縮形式** オプションをチェックすると avast! は 処理することができるすべての圧縮ファイルを検査します。

avast! は 次の圧縮ファイルを処理することができます。

自己解凍式 DOS 実行ファイル

自己解凍式 Win32 実行ファイル (UPX, AsPack, PEShield, ...)

7ZIP 圧縮ファイル

ACE 圧縮ファイル

ARC 圧縮ファイル

ARJ 圧縮ファイル

BZIP2 圧縮ファイル

CAB 圧縮ファイル

CHM 圧縮ファイル

CPIO 圧縮ファイル

DBX 圧縮ファイル (Outlook Express)

GZIP 圧縮ファイル

ISO 圧縮ファイル

LHA 圧縮ファイル

MAPI ファイル (*.pst)

MIME

NTFS ストリーム
OLE 圧縮ファイル (DOC, XLS, MSI, ...)
RAR 圧縮ファイル
RPM 圧縮ファイル
SIS 圧縮ファイル
TAR 圧縮ファイル
TNEF ストリーム
ZIP 圧縮ファイル
ZOO 圧縮ファイル

8 メール保護のセットアップ

8.1 概要

MS Outlook または Exchange クライアントは avast! によって自動的に保護され設定はまったく必要ありません。 Outlook Express や Eudora のような他の e-mail クライアントを保護するためには、いくつかの設定を変更してメール保護を完全に機能させる必要があります。これは avast! 4.5 までの事です。もし avast! 4.5 以上を使用し オペレーティング システムが Windows NT, 2000, XP または 2003 であれば、他の e-mail クライアントであっても、特別な設定をする必要は全くありません。 avast! 4.5 は ユーザーにとって非常に使いやすい、完全全自動の、新しい方法の e-mail 保護を 特徴としています。

avast! パッケージにはメールプロテクションの簡単設定に使用する Mail Protection Wizard が含まれています。このプログラムは Windows タスクバーのスタートボタン 経由で スタート → プログラム → avast! Antivirus → Mail Protection Wizard で 起動することができます。

後でメール保護の設定を変更したいときには、常駐保護タスク と 適切なプロバイダ を編集してください。 MS Outlook と Exchange プログラムについては Outlook/Exchange プロバイダであり、他のメール・クライアントについては インターネット・メール プロバイダです。

Mail Protection Wizard は MS Outlook, Exchange, Outlook Express, Eudora, Pegasus Mail, Netscape Mail, Mozilla Mail および IncrediMail の メール クライアントに有効です。また、その他のクライアントのメール トラフィックを保護することもできます。avast! の設定と サポートしていないメール クライアント についての詳細な情報は メール保護のマニュアル設定 のページをご覧ください

Mail Protection Wizard を実行する前に全てのメール クライアントを閉じる必要があります！
(そうしないと設定できません。)

8.2 基本設定

Automatically protect all my accounts

このオプションを選択すると、avast! は サポートしている全ての e-mail クライアントにある 全てのアカウントに対して e-mail 保護 を設定します。 Outlook Express, Eudora, Pegasus Mail, Netscape (version 6 まで) の クライアント が サポートされます。 更に新しいアカウントを保護することも確実にするために 将来作成する全てのアカウントを自動的に保護します チェックボックスを選択することもできます。 この選択の後、自動設定が実行されてウィザードを閉じます。

Automatically remove protection from all my accounts

このオプションの選択により、avast! が サポートしている全ての e-mail クライアントにある全てのアカウントの保護を停止します。

メール保護は削除されて ウィザード を 閉じます。

Set up the protection manually

いくつかのアカウントだけを保護したいとか e-mail 保護の微調整をしたいときにこのオプションを選択してください。

このオプションは avast! 4.5 より前の プログラム バージョン、または オペレーティング システム Windows 95, 98 および Millennium においてのみ 有効です。

8.3 MS Outlook / Exchange

このページでは メール処理に MS Outlook または Exchange を使用しているかどうかを指示します。 これらのクライアントのひとつが使われていれば、継続の必要はまったくありませんのでウィザードは 完了します。 avast! はデフォルトで (はじめから) これらの e-mail クライアントをサポートしています。

別のプログラムを使う場合や、設定を継続する時は第2のオプションを選択して下さい。 複数のメール・クライアント (MS Outlook / Exchange と Outlook Express や Eudora のような別のクライアント) を使われているときもこのオプションを選んで下さい。

8.4 サービスの一時停止

このページではメール保護サービスの一時停止について告知します。 先に進む前にこのサービスを停止しなければなりません。 設定ページの最後にこのサービスは再開可能になります。 Next ボタン をクリック して続けてください。

8.5 e-mail アカウントの選択

このページにはコンピュータで使われる e-mail アカウントのリストが表示されます。 隣にあるチェックボックスにチェックを入れて検査するアカウントを選択して下さい。 各アカウントについて、**受信**、**送信** または 全ての e-mail を検査しなければならないか、指定することができます。

Account details

このボタンをクリックすると、選択したアカウントの詳細な情報が現れます (SMTP および POP サーバー アドレス、ユーザー アドレス)。

Select all

このボタンにより全てのアカウントが検査されるようになります。

Deselect all

検査のための全てのアカウントの選択がキャンセルされます。

Show mailers for all users of this computer

このコンピュータで使用する全てのアカウントが表示されます。 チェックボックスがチェックされていないと記録されたユーザーのアカウントだけが表示されます。

My account is not in the list

このテキストをクリックすると、サポートしていない メール クライアント の メール保護のマニュアル設定を記載しているページが 表示されます。

8.6 サービスの設定

SMTP Server

メールを送るために最も頻繁に使われる SMTP サーバー (送信メール メッセージ用サーバー) を 選択してください。 リストから選択するかサーバー アドレスを直接入力します。

Default POP3 Server

メールを受けるために最も頻繁に使われる POP3 サーバー (受信メール メッセージ用サーバー) を選択してください。 お使いのメール クライアントがこの情報を提供しない場合に avast! が使用します。

Show taskbar icon when processing mail

このボックスにチェックを入れると、メール検査 を意味するアイコンがメール処理中に avast! システム アイコンの隣に表示されるようになります。 このオプションはプログラムの機能に影響を与える事はなく、メール検査の確認表示に過ぎません。

8.7 タスクの設定

Enable automatic start of the service

このオプションはログオン時にメール検査サービスが自動的に開始されることを保証します。 御社のメール トラフィックがコンピュータ による作業の非常に早い段階から保護されます。 このサービスを実行しないと avast! はあなたのメールをチェックすることができませんので、この設定をお勧めします。 e-mail を 通じて多くのウィルスが拡散しますので、このサービスが ON になっている事は極めて重要であるということに 注意してください。

Enable mail protection in default resident task

メール検査サービス が 常駐保護機能の一部になります。 このオプションを有効化することをお勧めします。

8.8 サービスの開始

(2 ページ目で中断した) サービスの再開について告げられます。(可能ならば) **Start now** ボタンをクリックして保護機能を始動してください。 **Next** ボタン そして **Finish** ボタン と 続けてください。そして、お使いの e-mail クライアントを起動することができます。

8.9 メール保護のマニュアル設定

メール スキャナ は SMTP/POP/IMAP プロトコルを使用する任意のメール プログラムと共に動作します。 Mail Protection Wizard によりサポートされていないメール プログラムを使用した場合や、メール スキャナ に送受信メッセージを確認させたい時は、マニュアル設定で行えます。 avast4.ini ファイルを変更し そして あなたのメール プログラムの アカウント プロパティを修正しなければならない という、2 つのステップからこの操作は成ります。

avast! Antivirus Version 4.5 は 新しい e-mail 保護の方法を採用しました。 マニュアル設定 (更に、e-mail プログラムのアカウントは維持されます。) を 全く必要としません。 ですから、avast! 4.5 以上をお使いになり オペレーティング・システム が Windows NT, 2000, XP または 2003 で あれば、以下の説明をお読みにならなくても構いません - ちょうど MS Outlook や MS Exchange のように あなたの e-mail は 自動的に保護されます。

ステップ 1 : AVAST4.INI ファイルの変更

avast4.ini ファイルを Notepad エディタで開いてください。このファイルは avast! をインストールした フォルダ の Data フォルダ、例えば C:\Program Files\ALWIL Software\avast4\Data にあります。

[MailScanner] というセクションを探します。以下の行をこのセクションに挿入します(もし既に存在しているようであれば変更してください)。

```
DefaultSmtpServer=smtp.server.com
```

```
DefaultPopServer=pop.server.com
```

```
DefaultImapServer=imap.server.com ( 受信メールに IMAP を使っているときだけ )
```

smtp.server.com を お使いの SMPT サーバーに、例えば smtp.tiscali.com のように置き換えてください。 POP (および IMAP) サーバー も 同様に (例えば pop3.tiscali.com のように) 行なってください。

お使いの e-mail プログラムが SMPT 認証を備えていて、更に POP と 異なるログイン名を SMPT に 設定する事もできるのであれば、UseDefaultSmtp=0 の行を挿入してください。

お使いの e-mail プログラムが SMPT 認証を備えていなければ UseDefaultSmtp=1 の行を挿入してください。

変更を保存して Notepad エディタを閉じてください。

ステップ 2 : メール プログラム の アカウント プロパティ を 編集

メール プログラムを起動してください。

アカウントの設定画面を表示。

送信メッセージを検査したい場合、SMTP サーバーのアドレスを ローカル コンピュータのアドレス、つまり 127.0.0.1 に変更してください。

受信メールを検査したい場合、POP (IMAP) サーバーのアドレスを ローカル コンピュータのアドレス、つまり 127.0.0.1 に変更してください。

ユーザー (ログイン) 名 に 記号 # (ダブルハッシュ) と あなたの POP (IMAP) サーバー アドレス (ステップ 1 で avast4.ini に明記したのと同じもの) を付け加えて、変更してください。 よってログイン名はこのようになります。

Ann.Jones#pop3.tiscali.com

お使いの e-mail プログラムが SMTP 認証を備えていて、更に POP と異なるログイン名を SMTP に設定する事もできる時 SMTP 認証が可能であれば、記号 # とあなたの SMTP サーバーのアドレスをログイン名に付け加えます。(例えば annie2#smtp.tiscali.com) SMTP 認証ができなければ、これを可能にしてログイン名として記号 # を 御社の SMTP サーバーの アドレスと一緒に使います。(例えば #smtp.tiscali.com) 変更を保存してください。

これで メール スキャナ のマニュアル設定は完了です。

メールの送信と受信

始動に成功すれば メール スキャナ を直ぐに使い始める事ができます。 e-mail をあなた自身に送ってみてください。 受信後、ヘッダを見て下さい。 こう書いてあるはずで

X-Antivirus: avast! (VPS 4.7.2003), Outbound message

X-Antivirus-Status: Clean

X-Antivirus: avast! (VPS 4.7.2003), Inbound message

X-Antivirus-Status: Clean

はじめの 2 行はメッセージ送信に対する参照です。 1 行目には ウィルス・データベース のバージョン と 送信メッセージか受信メッセージかの情報があります。 2 行目はファイルスキャンの内容です。 感染していなければ 感染していません と表示され、感染していれば 感染しています と 代わりに表示されます。 検査されなかったときは "検査されませんでした" と表示されま

メール スキャナ が感染メッセージを発見したときは、"ウィルス" ページの インターネット・メール プロバイダ の設定に従って動作します。 動作を選択(対話)を選択することにより、侵入したウィルスについて即座に知らされる事になります。 感染についての情報はヘッダのほかにメッセージ本体にも書き出されます。 ある e-mail プログラムはウィルスの情報を含んでいるメッセージの部分の正しく示すことができません。 ですから、最初にテキストの添付ファイルのすべてを見るのが良いでしょう。 というのも、その中のひとつは メール スキャナ からの物かも知れ

ないからです。

メール スキャナ は BASE64, UU-encode および BinHex で エンコードしたメッセージ本体と添付ファイルを検査します。メール スキャナ は添付ファイルを 修復 または 削除 することができます。メッセージ本体にウイルスが発見されたときはその本体を削除してインフォメーション・テキストで置き換えます。ヘッダは残りますので、誰がそのメッセージを送ったかがわかり、もう一度メッセージを要求することもできますし、また送信者にその人がウイルスを散布していることを知らせる事もできます。

もしお使いのメール プログラムがメール サーバーに接続できないといった場合には、ashMaiSv.exe プログラムが動作しているかどうか確認してください。もし動いていなければ、動かしてもう一度試してください。インストール プログラムはコンピュータ起動時の ashMaiSv.exe の自動起動を設定します。まだ起動していなければ、スタートメニュー の "スタートアップ" フォルダ に ショートカット を追加してください。

INI ファイル

メール スキャナ によって取り込まれた項目は Avast4¥Data¥Avast4.ini ファイルの [MailScanner] セクションの下にあります。メール スキャナ の実行中に項目を変更すると、avast4.ini ファイルを保存した直後に新しい値がロードされ使用されることになります。

SMTP, POP3 および IMAP トラフィックが向かう (転送される) アドレスは DefaultSmtServer , DefaultPopServer および DefaultImapServer という項目によって定義されます。サーバー アドレスは ドット付き IP アドレス か DNS 名 で記入されます。もしポート番号も使用したければ、記号 : (コロン) の後に書いてください。デフォルトのポート番号は SMTP については 25, POP3 については 110, IMAP については 143 です。

DefaultSmtServer, DefaultPopServer および DefaultImapServer の値は、e-mail プログラムに設定されたログイン名がサーバー アドレスを含んでいないときに参照されます。POP サーバーの ログイン名 が、例えば Ann.Jones であれば、メール スキャナ は e-mail を DefaultPopServer の値によって与えられたサーバーからダウンロードします。しかしながら、ログイン名 が Ann.Jones#pop3.tiscali.com であれば、メール スキャナ は pop3.tiscali.com サーバーに接続し、Ann.Jones というユーザーのメールをダウンロードすることになります。同じルールが IMAP プロトコルに対しても適用されます。SMTP プロトコルについても同様に同じルールが適用されます。加えて、ログイン名 を #smtp.tiscali.com の形式で設定することができ、これは何の証明も無しに smtp.tiscali.com サーバーを使ってメールが送られることを意味します。e-mail の送信は UseDefaultSmt の値にも依存します。

例 :

DNS 名 とポートにより指定された SMTP サーバー アドレス

```
DefaultSmtServer=oursmt.domain.com:25
```

デフォルト ポートを選択した、数字により指定された POP サーバー アドレス

DefaultPopServer=192.168.1.1

数字とポートにより指定された IMAP サーバー アドレス

DefaultImapServer=192.168.1.1:143

項目 ShowTrayIcon は、メール スキャナ がメール サーバーに接続したときにタスクバーのトレイにアイコンを見せるかどうかを指示します。 値 1 は yes, 値 0 は no を意味します。

項目 Log は記録するレベルを指示します。 値 0 は記録がアクティブでないことを意味します。 値 1 は単に基本情報がログファイルに書き出されることを意味します。 もし値 20 が使われると メール スキャナ とメール サーバーとの間のすべての通信が記録されます。 情報は Avast4¥Data¥LOG ディレクトリにある AshMaiSv.log ファイルに書き出されます。

項目 PassThrough はメッセージを検査できなかったときの メール スキャナ の動作を指示します。 この項目の値が 1 に設定されていれば、メール スキャナ は 検査せずにメッセージを通過させます。 値が 0 に設定されていれば、メール スキャナ は常駐タスクが実行されるまではいかなるメッセージも通過させません。 従って、e-mail は 常駐タスク が 実行中 か ポーズ のときに通過することができます。 その他のすべての場合において、メール スキャナ はメール プログラムがメール サーバーに接続することを許可しませんので、お使いのメール プログラムからの エラー メッセージ に遭遇することになるでしょう。

項目 Smtplisten, Poplisten および Imaplisten には メール スキャナ が接続する(接続を受け入れる、"listen") ネットワーク インターフェースを指定します。 コンピュータに複数のネットワークカード アダプタ があれば、メール スキャナ に必要なひとつだけを指定する事ができます。 ポート番号を指定する事もできます。

例 :

ポート 110 ですべてのネットワーク インターフェースからの接続を受け入れる

Poplisten=:110

ポート 110 で1つのネットワーク インターフェースからの接続を受け入れる (192.168.1.208 はあなたのコンピュータ・アドレスのひとつであるとする)

Poplisten=192.168.1.208:110

この項目のデフォルト設定 :

Smtplisten=127.0.0.1:25

Poplisten=127.0.0.1:110

Imaplisten=127.0.0.1:143

項目 Trust には メール スキャナ にアクセスすることが許されたコンピュータを指定します。 アドレスは ドット付き IP アドレス か DNS 名 で定義することができます。 IP アドレス/有効ビット数 の書式で、IP アドレスのグループも 定義することができます。 Trust 項目が空白のままならば、どのアドレスからのアクセスも許可します。 127.0.0.1:PORT の書式に *listen の項目を設定すれば、ローカルアドレス (127.0.0.1) からの接続だけを受け入れますので、Trust 項目はまったく効果を及ぼしません。

例 :

Trust=127.0.0.1,server.domain.com,192.168.1.0/24

Trust=

項目 StartSmtp, StartPop, StartImap は メール スキャナ が保護することができるプロトコルを定義することができます。 値 1 は、個々のプロトコルに対する デーモン が 開始されて 値 'Listen' により決定されたポートをふさぐことを意味します。 値 0 の使用は、使わないプロトコルの検査を停止することができます。

項目 UseDefaultSmtp は e-mail を送る 2 つの可能な方法のうちの 1 つを選択します。 値 1 は、すべての e-mail が DefaultSmtpServer の値により与えられたサーバーを利用して送付されることを示します。 この値は、SMTP サーバー上で (ログイン) 認証をサポートしていない、または SMTP に POP と異なるログイン名を設定できない e-mail プログラムのためにあります。 値 0 は 色々な SMTP サーバー を通して e-mail を送ることを可能にします。 この場合、SMTP サーバーのアドレスは e-mail プログラムに設定されたログイン名から取得します (アドレスは記号 # により区切られます。)

他のソフトウェアとの連携

メール スキャナ は単純な SMTP/POP3/IMAP プロキシ サーバーとして働きます。 これは、お使いのメール プログラムが メール スキャナ へ リクエストを送り、そして メール スキャナ はそれを 適切な SMTP (POP3, IMAP) サーバーへ転送するように、お使いのメール プログラムが環境設定されなければならないことを意味します。

メール スキャナ はコンピュータのポート 25, 110 および 143 を使用します。 もしもこれらのポートを利用する別のプログラムを更にインストールしたときは、どちらか一方のポート番号を変更しなければなりません。 メール スキャナ の場合は、項目 Smtplisten, Poplisten および Imaplisten の設定によって行うことができます。

例 :

```
Smtplisten=127.0.0.1:26
```

```
Poplisten=127.0.0.1:111
```

```
Imaplisten=127.0.0.1:144
```

その結果、お使いのメールプログラムに同じポート番号を設定する必要があります。

コンピュータにインストールされている他の SMTP/POP3/IMAP - プロキシ/サーバー型 プログラムと一緒に メール スキャナ を 使用したいときは、当然のことながら項目 DefaultSmtpServer, DefaultPopServer および DefaultImapServer を設定する必要があります。 例えば、メール スキャナ を 同じコンピュータの上で動いているお使いのメール プログラム と SMTP/POP3 サーバーとの " 間に置く " ように設定したいときは、上の項目 *Listen を設定し次の項目を追加してください。

```
DefaultSmtpServer=127.0.0.1:25
```

```
DefaultPopServer=127.0.0.1:110
```

メール スキャナ に 他のコンピュータのメールも検査させたいのならば、ローカルではなく他のアドレスからの接続の受け入れを許すことが必要です。 項目 *Listen の変更と項目 Trust の設定によりこれを行います。

例 :

192.168.1.10 はアドレス 192.168.1.20 および 192.168.1.21 のコンピュータが接続されているサーバー上の 1 つのネットワーク カードのアドレスです。

PopListen=192.168.1.10:111

Trust=192.168.1.20,192.168.1.21

コマンドライン パラメータ

ashMaiSv.exe /i - "avast! メール スキャナ" サービスを作成します。このサービスはコンピュータが起動されていればいつでもメール スキャナを起動します。誰もログオンしていないときにさえメール スキャナ を動かしておきたいときに役立ちます。

ashMaiSv.exe /u - サービスを取りやめます。

ashMaiSv.exe /e - メール スキャナ の 進行中の作業 (訳注: current instance) を中断して抜け出します。

ashMaiSv.exe (パラメータなし) - ユーザーがログオフするときに終了する通常のアプリケーションとして メール スキャナ を起動します。

既知の問題

お使いの e-mail プログラム (例えば Eudora) が、SMTP サーバー上での (ログイン) 認証をサポートしていなければ、また POP と異なるログイン名を SMTP に設定することができないならば、メール スキャナ は e-mail を色々な SMTP サーバー経由で送ることができません。その場合、UseDefaultSmtp=1 という設定を使用することで、ちょうど avast! version 4.0.235 以前のように単一の SMTP サーバーのみを経由して e-mail が送られます。

インターネット接続が遅すぎる場合や、送信中のメッセージが長すぎる場合は、お使いのメールプログラムの応答待ち時間が終了します。時間の経過により自動的に切断するメール プログラムはこのようなメッセージを送ることができません。SMTP の特性からこのエラーは修正されません。インターバルをできるだけ大きな値に設定する必要があります。POP3 サーバーから長いメッセージをダウンロードすると、タイムアウトで終了したメッセージがなくなっているはずで、このインターバルをできるだけ大きな値に設定することが、なおさら推奨されます。

お使いのメール プログラム (例えば Eudora) が IMAP サーバーから メッセージ テキストと 添付ファイル を分けてダウンロードするときには、ヘッダやメッセージのテキストに一切の補足情報が挿入されません。インターネット・メール 環境設定の "IMAP" ページにある "感染していないメッセージに記録を挿入する" チェックボックスが、その場合は働きません。

メール スキャナ は SSL (TLS) 接続をサポートしていません。

8.10 挿入される記録の書式

もし送受信メッセージに記録を挿入することを選択すると、どのように表示するか、これらの記録の書式を指示することができます。まず、あなたが変更したい挿入記録のタイプを選び出します。次の 4 つの中からひとつを選ぶことができます。

Tag for clean messages HTML version

HTML 形式のクリーン(感染していない)メッセージに挿入する情報の書式を変更。

Tag for clean messages TXT version

純粋なテキスト形式のクリーン(感染していない)メッセージに挿入する情報の書式を変更。

Tag for infected messages HTML version

感染した HTML 形式のメッセージに挿入する情報の書式を変更します。

Tag for infected messages TXT version

感染した純粋なテキスト形式のメッセージに挿入する情報の書式を変更します。

変更したい記録のタイプを選んで、適切な記録を Notepad エディタで表示します。

クリーン・メッセージに対する HTML 形式の記録の変更

以下のテキストがデフォルトです。

```
<html>
<BR><BR>
<TABLE width=400><HR>
<P style="FONT: 9pt/11pt verdana"><a href="http://www.avast.com">avast!
Antivirus</a>: %TYPE% メッセージは感染していません。
<P style="FONT: 8pt/11pt verdana">ウイルス・データベース (VPS):%VPS%<BR>検査日
時: %TIMEDATE%<BR><FONT color=gray>avast! - copyright (c) 1988-2007 ALWIL
Software.</FONT></P>
<TBODY></TBODY></TABLE>
<BR></html>
```

%INBOUND=受信%

%OUTBOUND=送信%

HTML コードに精通されていれば、ほとんどすべてを変更することができます。上で使用された変数は以下の意味を持っています。

%TYPE% - メッセージ・タイプにより置換されます。"受信" と "送信" がデフォルトの値です。

変数 %INBOUND% と %OUTBOUND% によりその値を変えることができます(以下参照)。

%VPS% - メッセージの検査に使われた ウィルス・データベースのバージョンにより置換されます。

%TIMEDATE% - メッセージを検査した時間と日付により置換されます。

%INBOUND=受信% - 単語 "受信" を、例えば "received message" に変更することができます。

ここで定義した単語や表現が 変数 %TYPE% の代わりに表示されます。

%OUTBOUND=送信% - 変数 %INBOUND=受信% に同じです。

感染メッセージに対する HTML 形式の記録の変更

以下のテキストがデフォルトです。

```
<html>
<BR><BR>
<TABLE width=400><HR>
```

```
<P style="FONT: 9pt/11pt verdana"><a href="http://www.avast.com">avast!
Antivirus</a>: %TYPE% メッセージは「感染」しました:<br>%ATTACH%
<P style="FONT: 8pt/11pt verdana">ウイルス・データベース (VPS):%VPS%<BR>検査日
時: %TIMEDATE%<BR><FONT color=gray>avast! - copyright (c) 1988-2007 ALWIL
Software.</FONT></P>
<TBODY></TBODY></TABLE>
<BR></html>
%INBOUND=受信%
%OUTBOUND=送信%
%CLEANED=は駆除に成功しました。%
%DELETED=はメッセージから削除されました。%
%LEFT=は(御注意ください!!!) 無傷のままメッセージに残りました。%
上で使用された変数は以下の意味を持っています。
%TYPE% - メッセージ・タイプにより置換されます。 "受信" と "送信" がデフォルトの値です。
変数 %INBOUND% と %OUTBOUND% によりその値を変えることができます(以下参照)。
%ATTACH% - 感染した添付ファイルの名前により置換されます。
%TIMEDATE% - メッセージを検査した時間と日付により置換されます。
%INBOUND=受信% - 単語 "受信" を、例えば "received message" に変更することができます。
ここで定義した単語や表現が 変数 %TYPE% の代わりに表示されます。
%OUTBOUND=送信% - 変数 %INBOUND=受信% に同じです。
%CLEANED=は駆除に成功しました。% - 感染したファイルからウイルス・コードを取り 除くことに成
功したときに記録に表示されるテキストを定義することができます。
%DELETED=はメッセージから削除されました。% - メッセージから感染したファイルを削除するこ
とに 成功したときに記録に表示されるテキストを定義することができます。
%LEFT=は(御注意ください!!!) 無傷のままメッセージに残りました。% - ウィルスがメッセージの中
に相変わらず残っているときに記録に表示されるテキストを定義することができます。
```

感染していないメッセージに対する 純粋なテキスト形式の記録の変更

以下のテキストがデフォルトです。

```
avast! Antivirus: %TYPE% メッセージは感染していません。
ウイルス・データベース (VPS):%VPS%
検査日時: %TIMEDATE%
avast! - copyright (c) 1988-2007 ALWIL Software.
http://www.avast.com
%INBOUND=受信%
%OUTBOUND=送信%
変数は HTML 形式のものと同じです。
```

感染メッセージに対する純粋なテキスト形式の記録の変更

以下のテキストがデフォルトです。

avast! Antivirus: %TYPE% メッセージは「感染」しました:
%ATTACH%

ウイルス・データベース (VPS):%VPS%

検査日時: %TIMEDATE%

avast! - copyright (c) 1988-2007 ALWIL Software.

<http://www.avast.com>

%INBOUND=受信%

%OUTBOUND=送信%

%CLEANED=は駆除に成功しました。%

%DELETED=はメッセージから削除されました。%

%LEFT=は(御注意ください!!!) 無傷のままメッセージに残りました。%

変数は HTML 形式のものと同じです。

9 ウィルス・チェスト

9.1 概要

チェスト はお使いのコンピュータ上にある安全で隔離された特別なフォルダとして扱われます。特別なファイルを 保存 するのに適した場所です。多少の制約はありますが チェス 内でそのファイルを扱う ことができます。

主な特徴

オペレーティング・システムの他の部分から完全に **隔離**。

チェスト 内のファイルにはどんな外部プロセスも影響を及ぼせません。つまりウィルスが外部プロセスに感染することも全くありません。

チェスト 内のファイルを **実行することはできません**。

この "制約" は ウィルスを実行しコンピュータの他の部分や チェスト 内の他のファイルに 感染することができないようにするために設けられています。

9.2 チェスト・ファイル の 取扱い

チェスト の中のファイルに対して次のアクションをとることができます。

Add file

"ユーザ・ファイル" カテゴリ にだけ ファイルを加えることができます。

Delete file

ファイルを削除し元に戻せません。つまり「ごみ箱」に移動しません！

Restore file

ファイルを元の場所に、つまり チェスト に 移動される前のディスク上のフォルダに移動します。同時にそのファイルは チェスト から削除されます。

Extract file

ファイルを選択したフォルダにコピーします。

Scan file

ウイルスについてファイルを検査します。

Show file properties

ファイルのプロパティを表示し、コメントをファイルに加えることができます。

Email to ALWIL Software

選択したファイルを (e-mail で) ALWIL Software に送ります。 avast! の誤報に気付いた場合のような特別な 場合にだけこのオプションを使ってください。 そのファイルを送る理由、お使いのウイルス・データベース の バージョン 等 といった、できるだけたくさんの情報を添付することを忘れないで下さい。 そうすることにより、お客様へのサービスをよりよいものになります。

(訳注: 追加情報等は必ず英語で書いてください。)

以下、3つの方法で操作できます: ファイルを選択して対応するアイコンをクリックしてツールバーから操作を選ぶ、 オブジェクトを選択してメイン・メニューからアクションを選ぶ、 ファイルを右クリックしてポップアップメニューからアクションを選ぶ、

注意

ファイルをダブル・クリックしてもそのファイルが起動されることはなく、代わりにそのプロパティが表示されます。 これは チェスト 内での予期しない感染から あなたを更に保護するための手段です。

9.3 チェスト の 使用

チェスト は - その 特性 のため - 次の目的に適しています。

Storing the viruses

avast! がウイルスを発見し、何かの理由であなたがそれを削除しないと決定するときは、チェストにウイルスを 移動するのが良いでしょう。 チェスト の中のウイルスが何かのきっかけで実行されることは決してありません。

Storing the suspicious files

後で解析するために疑わしいファイル (拡張子が 2 つあるようなファイル) の各々を チェスト に保存するのに用います。

Backup of the system files

インストール中に avast! はいくつかの重大なシステム・ファイルを チェスト の中に、 "システム・ファイル"のカテゴリ下にコピーします。 それらのファイルはウイルスによって感染させられた場合にオペレーティング・システムをクラッシュさせるかもしれません。 必要であれば、それらのファイルを チェスト から元の場所に戻すことができます。 もし avast! アンチ・ウイルス・パッケージからの広範囲な保護にもかかわらず未知のウイルスがコンピュータに 感染し重要なシステム・ファイルを部分的に変えてしまっても、それを簡単に元の状態に戻すことができます。

9.4 チェストのファイル・カテゴリ

チェストのファイルは3つのカテゴリに分けられます。

Infected file

ファイルを直接削除しなければ、avast! は感染したファイルをこの区分に入れます。

User file

これはユーザーがファイルを入れておくことができる唯一の区分です。

System files

avast! はインストールしている間に重要なシステム・ファイルをこのカテゴリにコピーします。

9.5 使用方法

ファイルを追加

Virus Chest で user file カテゴリに切り替えてください。

メイン・メニューで File Add を選択してください。

フォルダを閲覧して追加したいファイルを選択してください。

Open を選んでください。

または

Virus Chest で user file カテゴリに切り替えてください。

ファイル・リスト・ウィンドウを右クリックしてポップアップメニューから Add を選んでください。

フォルダを閲覧して追加したいファイルを選択してください。

Open を選んでください。

または

Virus Chest で user file カテゴリに切り替えてください。

ツールバーの Add アイコンをクリックしてください。

フォルダを閲覧して追加したいファイルを選択してください。

Open を選んでください。

ファイルを削除

Virus Chest で 削除するファイルを選択してください。

メイン・メニューで ファイル Delete を選択してください。

または

Virus Chest で 削除するファイルを右クリックしてください。

ポップアップメニューから Delete を選択してください。

または

Virus Chest で 削除するファイルを選択してください。
ツールバー の Delete アイコンをクリックしてください。

ファイルを復帰させる

Virus Chest で 復帰させるファイルを選択してください。
メイン メニューで、ファイル Restore を選択してください。

または

Virus Chest で 復帰させるファイルを右クリックしてください。
ポップアップ メニューから Restore を選んでください。

または

Virus Chest で 復帰させるファイルを選んでください。
ツールバー の Restore アイコンをクリックしてください。

ファイルを抽出

Virus Chest で 抽出するファイルを選択してください。
メイン・メニューで ファイル Extract を選択してください。
Explorer 風のダイアログが表示されます。 ファイルの移動先を選択してください。
OK をクリックしてください。

または

Virus Chest で抽出するファイルを右クリックしてください。
ポップ・アップ・メニューから Extract を選択してください。
Explorer 風 のダイアログが表示されます。 ファイルの移動先を選択してください。
OK をクリックして下さい。

または

Virus Chest で 抽出したいファイルを選択してください。
ツールバー の Extract アイコンを選択してください。
Explorer 風 のダイアログが表示されます。 ファイルの移動先を選択してください。
OK をクリックしてください。

ファイル・プロパティを表示

Virus Chest で プロパティを表示するファイルを選択してください。
メイン メニューで File Properties を選択してください。

または

Virus Chest で プロパティを表示するファイルを右クリックしてください。
ポップアップ メニューから Properties を選択してください。

または

Virus Chest で プロパティを表示するファイルを選択してください。
ツールバーの Properties アイコンをクリックしてください。

または

Virus Chest で プロパティを表示するファイルを選択してください。
Enter キー を押してください。

または

ウィルス・チェスト で プロパティを表示するファイルをダブル・クリックしてください。

ファイル検査

Virus Chest で 検査するファイルを選択してください。
メイン メニューで File Scan を選択してください。

または

Virus Chest で 検査するファイルを右クリックしてください。
ポップアップ メニューから Scan を選択してください。

または

Virus Chest で 検査するファイルを選択してください。
ツールバー の Scan アイコンを選んでください。

内容をリフレッシュ

メイン メニューで、File Refresh all files を選択してください。

または

ファイル・リスト・ウィンドウを右クリックしてください。
ポップアップ メニューから Refresh all files を選んでください。

または

ツールバー の Refresh アイコンをクリックしてください。

10 拡張エクスプローラ - ashQuick プログラム

10.1 概要

ashQuick プログラムは、avast! や ashCmd のようなウイルススキャナです。 エクスプローラ からするように、ローカル・コンテキスト・メニュー からファイルを検査するのにいつも使われます。他の場合には avast! や ashCmd を使う方が良いです。

(訳注)コンテキスト・メニュー :ファイルやフォルダを選択、マウスを右クリックすると表示されるメニュー

10.2 拡張エクスプローラ の セットアップ

拡張エクスプローラ の設定は "拡張エクスプローラ" タスクを 編集 することにより直接行う事ができます。 追加設定は avast! プログラムの 設定 にあります。

注意 : "拡張エクスプローラ" タスクの編集を可能にするためには、("高機能インターフェース" のページで) avast! の 設定 の 特別なタスクを表示できるようにしなければなりません。

11 ashCmd プログラム

11.1 概要

ashCmd プログラムはちょうど avast! のようにすべてのタイプのウイルスを検索するために使われます。 ashCmd は avast! と同じ検査カーネルを使いますので、検査結果は全く同じです。違いはインターフェースだけであり、ユーザー・フレンドリーな avast! とは対比的に、ashCmd は コマンドライン だけを使います。

コンソール(コマンドライン)で ashCmd を直接取扱うか、その出力をファイルにリダイレクトするかの 2 つのモードの操作があります。 これは パラメータ "/_>" により行われ、例えば "ashCmd.exe c:¥windows /_> test.txt" は C:¥Windows フォルダを検査してその結果を avast! がインストールされているディレクトリに作成される test.txt ファイルに保存します。

(訳注) kernel: the central, most important part of something; core; essence (何かの主要な、最も重要な部分; 芯; 本質) (Webster's New World Dictionary of American English, Third College Edition より)

11.2 ashCmd

多数の **スイッチ** と **パラメータ** を利用し、ashCmd はコマンドラインのみで制御されません。 ashCmd のコマンドラインは下記の通りです。

ashCmd /@=<タスク名> | <領域名> [<パラメータ>]

avast! タスクを起動させたいときは、記号 "@" の後にその名前を入れてください。 タスク名がスペースを含んでいるときは引用符で囲まなければいけません。 引用符を忘れるとタスクは動きません! avast! タスクが走ると他のコマンドラインのパラメータはすべて無視されます。

タスク名を指定しないと avast! は 与えられた領域を検査します。 どのように検査を行うかは他のパラメータによって制御します。

検査の実行はエスケープ・キーによって中断できます。

検査が終了すると、例えば感染したファイルの数などの様々な有益な情報が印刷されます。 ashCmd は リターン・コード も設定し、他のプログラムや BAT ファイル の IF ERRORLEVEL コマンドにより検査することもできます。

11.3 ashCmd の パラメータ と スイッチ

例 : "C:\Program files" /p /u=virus@avast.com --soundoff /v="key kapt"

d:\%path

このパラメータは検査すべきドライブとディレクトリを指定します。 パラメータが与えられなければカレント・ドライブのルート・ディレクトリにあるファイルを検査します。 いくつかのドライブを同時に指定することができます。

d:\%path\%file

ファイルのフル・パス名が与えられると ashCmd はそのファイルだけを検査します。 ファイルは存在していなければなりません！

/H または /? (または --help)

簡単なヘルプと可能なスイッチのリストを印刷します。

/# (または --remote)

リモート・ディスクを検査します。

/* (または --local)

ローカル・ハード・ディスクを検査します。

/_> (または --console)

アプリケーションは STDIN/STDOUT について準備をします。 出力のすべての出力が標準出力 (STDOUT) に リダイレクトされます。 つまり 出力は個々の UNIX スタイルのコマンドライン・ツールで処理することができます。

/A (または --testall)

すべてのファイルを検査します。

/@=<タスク名> (または **--task**)

与えられた名前の avast! タスクを起動します。他のパラメータはすべて無視されます。タスク名にスペースが含まれるときは引用符で囲まなければなりません。

/C (または **--testfull**)

ファイル全体を検査します。デフォルトによりファイルの重要な部分だけが検査され、かなり早いです。ウィルスが見つかったとプログラムはファイル全域を検査するように自動的に切り替わりません。

/I (または **--ignoretype**)

すべてのファイルのすべてのウィルスを検索します (例えば、EXE ファイルの中でもブート・ウィルスを探す等)。

/J (または **--paging**)

プログラムが STDOUT モードになればラインを呼び出します (即ち、それぞれの結果のページを満たした後に停止します)。

/M (または **--boot**)

ブートセクタとオペレーティング・メモリを検査します。

/P (または **--continue**)

このスイッチは、ウィルスが見つかったとディスクのシステム領域を検査した後すぐに、かつ、ユーザーとの対話することなくプログラムを実行するように指示します。検査の結果を確認するために予め定義したリターン・コードまたはレポート・ファイルに保存された情報を使うことができます。感染したファイルに対する自動処理を指定するには **/P=[1234]** を使用します。ここで 1 = ファイルを削除, 2 = チェストへ移動, 3 = 修復, 4 = 停止 を意味します。

/R:[*] [ファイル名] (または **--report**)

発見されたウィルスのリストとまとめの表(レポート・ファイル)でテキストファイルを作成することをこのスイッチで指示します。ファイル名が与えられないと、カレント・ディレクトリの ASHCMD.RPT が出力に利用されます。スイッチ **/R** の後に記号 "*" があるときは、検査されたすべてのファイルが (ウィルスが全く検出されなかったものでさえ) レポート・ファイルに書き出されます。

/S (または **--soundoff**)

このスイッチはウィルス警告音を off にします。デフォルトではウィルスが発見されるとピープ音により知らせます。

/U=<アドレス> (または **--sendmessage**)

ウィルスが発見されると、警告メッセージを与えられたアドレスに送ります。

/V=[**ウイルス名の最初の文字**] (または --viruslist)

ashCmd プログラムは 現在の ウィルス・データベース (即ち、発見可能なウィルスのリスト) を 印刷して終了します。

/T:[**JZIMXRSTGCBWOEQHFVKPY7D6UAN**] (または --archivetype)

検査する圧縮ファイルのタイプを指定します。

(J:ARJ, Z:ZIP, I:MIME, M:MAPI, X:Exec, R:RAR, S:Streams, T:TAR, G:GZ, C:CAB, B:BZIP2, W:WinExec, O:ZOO, E:ACE, Q:ARC, H:LHA, F:TNEF, V:CPIO, K:CHM, P:RPM, Y:ISO, 7:7ZIP, D:DBX, 6:SIS, U:OLE, A:All, N:none)

11.4 リターン・コード

ashCmd が終了するとリターン・コードをオペレーティング・システムに返信します。 他のプログラムや BAT ファイル の IF ERRORLEVEL コマンドによりこのコードを後から検査することができます。 リターン・コードは次の値を持っています。

0 - 正しくプログラムが終了し、ウィルスは発見されなかった。

1 - ウィルスが発見された。

> 1 - 検査中にエラーが発生した。

12 avast! の設定

幅広い設定により avast! を 御社の必要に応じて調整できます。設定のほとんどは 基本機能および 高機能ユーザ・インターフェース で全く同じですが、それでもいくつかは 有料の avast! Professional の 高機能ユーザ・インターフェース 特有のものです。

基本機能ユーザ・インターフェース の設定へは **メニュー** → **設定**、高機能ユーザ・インターフェース の設定へは **ファイル** → **設定** または ツールバーの対応するボタンをクリックすることにより到達することができます。

12.1 Common (一般)

・ Test memory during application start-up

avast! を起動する時に RAM メモリのウィルス検査をします。このチェックを off にすることができ、avast! の起動をわずかに早くしますが、avast! が メモリに常駐するウィルスを 破壊的になる前に捕らえる 機会は減少します。

・ Check floppy disks in drive when logging off

ドライブにフロッピーディスクがあるときに avast! はコンピュータをシャットダウンしたり 再起動したりしません。ブート・ウィルスについて保護します。

・ Chek CDs in drive when logging off

フロッピーディスクの場合と同じ意味です。

- **Check other removal media when logging off**

上の2つの機能と同じです。 ZIPドライブ等の他のリムーバブル・ディスクを確認します。

- **Enable skins for Explorer Extension**

このオプションの使用により拡張エクスプローラ用のウィンドウを標準 (Windows) の方法で描画するのか、対応するスキンを使うのかを指定できます。 スキンを off にするとクイック・スキャンの初期化が若干早くなります。

- **Exit Explorer Extension when first virus is found**

複数のファイルに同時にクイック・スキャンを実行すると、最初のウイルス発見時にスキャンは停止します。 このオプションを off にすると選択した全てのファイルを検査します。

- **Show results of Explorer Extension**

クイック・スキャン実行時にウイルスが見つからなくても結果を表示します。

- **Show Explorer Extension icon**

このオプションにチェックを入れると、コンテキストメニューの avast! の項目に小さいアイコンが表示されます。

12.2 Appearance (外観)

このページには avast! antivirus の表示に関する多くの設定があります。

Show avast! Tray icon

"a" という文字の青いアイコンをシステムトレイ (時計のそば) に表示し、avast! antivirus の状態を示します。

Animate the icon when scanning

avast! 常駐保護が何かを (例えば、送受信するメール、アクセスするディスク上のファイル、ブラウザにダウンロードする Web ページ を) 検査しているときに、avast! が活動していることを示すためにアイコンが回転します。

Use translucent effects

このオプション (Windows 2000 以上で有効) は 基本機能ユーザ・インターフェースの特別な表示効果を ON にします。

12.3 Enhanced Interface (拡張インターフェイス)

Show Special tasks

このタスク・リストはスクリーン・セーバーや拡張エクスプローラといった特別なタスクを含んでいます。タスクを表示するので編集することができます。

Scroll session results

セッションの結果は自動的にスクロールされて常に最新の結果を表示します。

Automatically delete sessions

与えられた日数経過後に削除する保存したセッションを指定します。

12.4 Chest (チェスト)

このページでは、**チェスト** から ALWIL Software へファイル送付するときのオプションを指定します。**チェスト** から送信可能なファイルサイズの最大値を選択し、e-mail を送るために使用する SMTP の設定を指定してください。

12.5 Confirmation (確認)

このページでは avast! の実行中に表示すべき質問と警告を選択することができます。チェックされていない項目については確認ウィンドウが表示されません。熟練ユーザーに限り、確認ウィンドウのスイッチを切ることをお勧めします。ただし、処理のいくつかは取り消すことができません！

12.6 Language (言語)

ここでは avast! に使いたい言語を指定することができます。変更はプログラムを再起動した後に有効になります。

12.7 Sounds (サウンド)

avast! は行っていることについて知らせるためにサウンドを使うことができます。**設定**をクリックすると、Windows の標準のサウンド設定が表示されます。厳密に言えば**イベント**のページです。イベント間で "avast! antivirus" と呼ばれるセクションがあります。ここでは、個々の avast! イベントに割り振られたサウンドを知ることができます。お好みに合わせて、同じようにして他の Windows のサウンドに変えることができます。

avast! サウンドを完全に off にしたければ、単に **avast! のサウンドを使用しない** にチェックを入れてください。

12.8 Logging (記録)

実行中に、avast! に関するいくつかのイベントについての情報を保存するファイル(ログ)を avast! は作成します。このページではログに保存されるイベントの **タイプ** を設定することができます。快適な **ログ・ビューア** を avast! ではお使いになれます。

12.9 Exclusion (例外)

avast! はそれが1つのファイルであっても検査から一部の領域を除外することができます。つまり avast! はそこではウィルスを検索しません。それは様々な場合に利用されます。

Avoiding false alarms

avast! がファイル内のウィルスの感染を報告したとしても、それが誤報であることが確かであれば、そのファイルを検査から除外して更なる誤報を回避することができます。しかし、我々が問題を解決することができるよう、そのようなファイルを送っていただければ幸いです。

Speeding up the processing

例えばイメージだけを含んでいるようなディレクトリがハードディスク上にあるのなら、それを例外リストに追加することで検査から除外することができます。その結果ファイルの検査に要する時間が短縮されます。

重要な事ですので、覚えておいて下さい。これらの**例外**は全てのタスクに影響を及ぼします。ひとつのタスクにだけ例外を設定したい場合、個々のタスクを編集しなければなりません。

設定

Add

除外するフォルダやファイル記載用のリストに空アイテムを加えます。すべてのサブフォルダを含むフォルダを選択したければ、"C:¥Windows¥*" のように "¥*" を付け足さなければなりません。

Remove

例外リストから選択したフォルダやファイルを削除します。

Browse

Explorer 風のウィンドウが開きます。ここではパスの全部をタイプする必要なく、希望するフォルダやファイルを選択することができます。

注意：以下に述べられているいくつかの項目は Professional バージョンでのみ有効です！

12.10 Update-Basic (更新 - 基本)

注記：以下に記されたいくつかの項目は Professional 版に限り有効です。

ウィルス保護の確実性を最大限にするには、最新の ウィルス データベース (VPS ファイル) を備える必要があります。avast! は インターネット接続を利用したデータベースのオンラインによる更新をお約束します。このページでは更新を実行する方法を設定します。

avast! プログラム自身を更新することができます。より新しいバージョンはいつも新しい機能を備えており、既知の問題を解決します。一般的に、年2回プログラムを更新されることをお勧めします。プログラム更新中は ウィルス データベース も更新されます。

更新は両方とも差分、つまり足りない部分だけをダウンロードします。更新のダウンロードに要

する時間はかなり短く、時間とお金を節約します。

はじめて更新を開始するときに、avast! は インターネット接続について尋ねます。プロキシ サーバーを用いてインターネットにアクセスする場合、ここで設定して下さい。そうでない場合、アップデート サーバーへの接続に失敗します。

Automatic

この選択により確実にデータベースとプログラムは最新のものになります。 インターネットに接続すると毎回、avast! は ウィルス データベース (プログラム) が我々のサーバーにある利用可能なものより 古いかどうかを確認します。両者が異なれば、現在足りないデータをお使いのコンピュータにダウンロードします。

Ask when update is available

原則的に上記と同じですが、更新は自動的に開始しません。より新しいバージョンが利用可能である事を知らされる だけであり、すぐにダウンロードするか後で行なうかどうかはあなたに委ねられます。これがデフォルトの設定です。

Manual

更新は自動化されず常にマニュアルで行わなければなりません。

Update now

このテキストをクリックするとデータベースやプログラムの更新がすぐに開始されます。

Details

詳細な設定 (および プロキシ サーバー) をここで設定します。

Running mode

ここでは マニュアル 更新 の設定を行いません。自動更新は常に "サイレント" です。

•Normal

更新が行なわれると、avast! は 要約を表示します。 オプションで、更新の進行状況を表示することもできます。

•Silent

更新は完全にバックグラウンドで行なわれ、メッセージは何も表示されません。

Update options:

• Show update progress

更新している間、小さなウィンドウが表示され進捗状況を見ることができます。

•Show icon in task tray bar

更新の間アイコンがシステムトレイに表示されます。

•Ask for reboot when needed

一部の更新はそれを有効にするために再起動が必要です。このオプションをチェックすることでオペレーティング システムの再起動が自動的に起こらないように設定されます。今再起動したいのか後でしたいのかを尋ねるポップ アップ ウィンドウが表示されます。

・**Show sliding box after automatic update**

自動更新が行なわれると、小さなお知らせウィンドウがシステム時計の上に表示されます。

・**Show sliding box on error**

自動更新中にエラーが発生した場合に、小さなお知らせウィンドウがシステム時計の上に表示されます。

Auto update interval

自動更新の間隔をここで設定することができます。(つまり、新しい更新が可能か、どのくらい頻繁に avast! に確認させるか)

Push iAVS

特別な更新の方法です。時として、早急に更新を行うことが非常に重要になります(例えば、新しいウィルスが蔓延し始めるとき)。Push iAVS により、ALWIL Software スペシャリストの要請により遠隔操作で更新を開始することができます。要請は特別な e-mail メッセージにより行われます。avast! は受信 e-mail を検査しており、メッセージを認識して更新を自動的に開始します。

・**Enable**

Push iAVS 機能を有効にします。

・**Add information about performed action into e-mail**

このオプションを選択すると、avast! は、更新が行われたかどうか、そしてどのようにして行われたかを告げるメッセージを記録します。

・**Registration**

登録により Push iAVS サービス (Professional バージョンのみ) を始動しなければなりません。リンクをクリックするとオンライン フォームがお使いのブラウザで開かれます。ここで、iAVS を開始するためのメッセージを送る e-mail アドレスを入力しなければなりません。

12.11 Update-Connections (更新 – 接続)

ここではお使いのコンピュータがインターネットに接続する方法を指示できます。これらの設定により avast! が新しい更新を確認する方法を改善し、自動更新のプロセスをより信頼できるものにします。

Proxy

このボタンをクリックするとプロキシ サーバーの設定を入力するウィンドウを表示します。詳細は"Proxy"のページをご参照下さい。

12.12 Alerts (警告)

avast! は ウィルスの発生について警告メッセージを送ることができます。例えばネットワーク管理者が管理しているコンピュータのどれかにウィルスが存在すると知らされた場合にこの機能

が役立ち、その結果、素早く対応することができます。

警報を次のような方法で送ることができます。

・SMTP

SMTP プロトコルを使って e-mail で警報を送ります。 SMTP サーバー、即ちメッセージが通過するメールサーバ (例えば smtp.company.com または 192.168.1.1) を定義する必要があります。 更に使用する ポート を指定しなければなりません(標準値は 25 です)。 最後に送信者アドレス("From", つまりユーザー・アドレス) を入力してください。

・MAPI

MAPI プロトコルを使って e-mail として 警報を送ります。 MAPI プロファイル名を対応する利用パスワードと一緒に入力してください。

・WinPopup

net send コマンドを使って警報を送ります。 警報を送る相手のコンピュータの IP アドレスまたはネットワークアドレスを入力してください。

・ICQ

警報を ICQ メッセージとして送ります。 警報を送る相手の ICQ クライアントの UIN を入力してください。

・Windows Messenger

警報を Windows Messenger プログラムのメッセージとして送ります。 警報を受信する人が Windows Messenger サービスにログインするために使用している e-mail アドレスを入力してください。

・Add

そのボタンを押して使用するプロトコル(SMTP/MAPI/ICQ...) を選択します。 更に、対応する設定(上記参照)を入力することができます。

・Remove

選択したアドレスを削除します。

・Edit

選択したアドレスを編集します。

・Test

テスト・メッセージを選択したアドレスに送ります。

・Test All

テスト・メッセージをリスト上のすべてのアドレスに送ります。

12.13 SMTP

このページでは、SMTP サーバーのパラメータを指定できます。 特に次のような場合に、avast! は e-mail メッセージを送るためにこの設定を使用します。

- ・Sending warning messages (ウィルスが発見されたとき)
- ・Sending files from the Chest (ALWIL Software に)
- ・Sending avast! Crash report (ALWIL Software に)

次の情報を入力しなければなりません。

- ・ **Server address** - 送信 e-mail サーバー のアドレス (例えば smtp.server.com または 192.168.1.25)
- ・ **Port** - ポート番号 (デフォルトは 25 です)
- ・ **From address** - 送る人のアドレス ("From")

12.14 Trouble shooting (トラブルシューティング)

このページには特定の問題を解決するための、特別な設定があります。もっともな理由も無いのにそれらを変更すべきではありません。疑問があるときは、最初にテクニカルサポートにお問い合わせ下さい。

・ **ポップアップを表示する前にフルスクリーン アプリケーションについてチェックする**

avast! の 環境設定に従って、コンピュータの動作中に様々なメッセージが表示されます (例えば、ウイルス データベースが更新されたとき、受信メールをウイルスに関して検査するとき等)。通常は、関連するイベントによってメッセージが表示されます。しかし このことによりフルスクリーン アプリケーション (例えばゲーム) が中断され、メッセージを表示するときに Windows が フルスクリーン モードから普通のウィンドウ モードに切り替えます。

このオプションにチェックを入れると、avast! は メッセージを表示する前に フルスクリーン モードかどうかを確認します。アクティブなフルスクリーンが見つければ、avast! は メッセージを**表示しません**。

・ **カーネルモードでのスキャンを無効化**

NT ベースの OS を利用する avast! ユーザーは "カーネルモードでのスキャンを無効化" をチェックします。検査性能に影響はありませんが、不完全なハードウェア上の安定性が向上すると考えられます。(例えば;テクニカルサポートにより)指示を受けない限り、このオプションに変更すべきではありません。

13 ログ・ビューア

12.1 概要

プログラムの活動、エラーまたは警告についての情報を保存するいくつかのログファイルを avast! は動作中に作成します。インストールやプログラムの情報および ウィルス・データベース の更新はそこでも見ることができます。これらのログは統合した **ログ・ビューア** で閲覧することができます。全ての記録が検索可能な区分に分けられます。ログ・ビューア は 基本機能ユーザ・インターフェース から **Menu → Log Viewer** を介して起動されます。

12.2 ログ・ビューアの取扱い

付属のビューアを使いログファイルの情報によりいくつかの基本的な操作を行うことができます。例えばフィルタをかけたり、検索したり、出力したりすることができます。

検索

キーワードを使って特定の記録を見つけたければ、CTRL+F を押す、またはメニューから Edit Find を選択、またはツールバーの Find アイコンをクリックしてください。現行のリストを右クリックしてポップアップメニューから Find を選択することもできます。キーワード、例えば "boot"、をタイプできるところにダイアログが表示されるので OK により追認してください。1 番目の記録が表示されます。CTRL+F キーをもう一度押すと次のものが見つかります。

フィルタ

フィルタリングが用いられるのは与えられた基準による現行の選択リストを特に絞り込むためです。たくさんの行があるログについては、キーワードを含む数行を表示することができます。フィルタリングは CTRL+R キーを押すことで開始され、上にある検索方法と同じように使います。フィルタの特性を設定するダイアログが表示されます。

Include

閲覧、選択する行に含めるキーワードを入力して下さい。ワイルドカード * を使用することができます。複数のキーワードはセミコロンで区切って下さい。

Exclude

閲覧、選択する行から除外するキーワードを入力して下さい。

Time range

一定の期間から記録を篩分けしたいだけであればここで期間を指定してください。

Select defined lines

このオプションにより一致した行を選択することになります。選択したものをエクスポートする場合に便利です。

Show only defined lines (hide the rest)

このオプションを選択すると一致した行だけが表示されます。

出力

検索またはフィルタリングされた記録はテキストファイルに出力することができます。更に記録リストのすべてをファイルに出力することができます(例えば全カテゴリリスト)。そうするためにはすべての行を選択してメインメニューで File Export current list を選ぶか、行だけを

出力する為 **File** **Export Selected Lines** を使用して下さい。
新たに表示されたウィンドウで、出力ファイルの名前とディスク上のフォルダを選択してください。

並べ替え

現在のリストの並べ替えをしたいときは、適切な列の見出しをクリックしてください。項目を並べ替えます。再度同じことをすると反対に昇順から降順に並び替えられます。

12.3 イベントのカテゴリ

ログファイルに保存されたイベントをより読みやすくする為、いくつかのカテゴリに分けられます。以下、リストと説明です。

緊急 コンピュータ全体にとって危険 (セキュリティ, システム・ファイル削除)。

警報 コンピュータ全体にとって危険になりうる。

深刻 深刻なプログラムエラー、プログラムが終了する。

エラー エラー発生、プログラムが動作しない。

警告 エラー発生、で `sy` がプログラムは動作する、または問題を解決。

注意 重要な情報、すべて正常。

情報 単なる情報、すべて OK。

13 復旧

13.1 avast! ウィルス・クリーナーで復旧

avast! ウィルス・クリーナー は 選択したウィルスをコンピュータから削除するツールです。avast! 自身で殆ど全ての既知ウィルスを検出して削除することができます。avast! ウィルス・クリーナー は最も一般的なウィルスのごく一部を処理することができます。"About" ボタンをクリックすると (avast! ウィルス・クリーナー・ツールに) すべてのリストが表示されます。

avast! ウィルス・クリーナー は avast! アンチウィルスに直接組込まれています。必要ならば、avast! ウィルス・クリーナー の スタンド・アローン・バージョンを ALWIL Software のウェブ・ページから無料でダウンロードすることができます。両方のバージョン(ダウンロード可能なものと avast! アンチウィルスに統合されているもの)は同じです。

avast! が avast! ウィルス・クリーナー を使って削除することができるウィルスを検出すると、ツールを起動するための特別なボタンを表示します。("ウィルスをシステムから完全に除去します"と書かれた)ボタンがウィルス警告ウィンドウに直接表示されます。ボタン右上より、感染したファイル削除、名前を変更、移動です。avast! ウィルス・クリーナー を起動するオプションが可能なときは、それを使用されることをお勧めします！

長所

avast! ウィルス・クリーナー は御社システムから完全にウィルス感染を除去するツールです。感染したファイルを (可能なときは何時でも) 修復してウィルス本体を削除します。その為、システムを再インストールやバックアップから回復させる必要はありません。更に、それだけではありません。システム・レジストリからウィルスの項目をも取除き (それはある場合には非常に重要です)、破壊された環境設定ファイルを修復し、そしてウィルスが作成した一時ファイルを削除します (そのようなファイルはウィルス・コードを全く含んでいませんので avast! によって検出されませんが、ハードディスクのスペースを消費します)。簡単に言えば、avast! ウィルス・クリーナー はシステムから可能な限り、全てのウィルスの痕跡を取除きます。Safe Mode で 駆除する必要は全くありません。ウィルスがメモリに発見されると、最初にそれを不活性化します。

avast! ウィルス・クリーナー 起動

高機能ユーザ・インターフェースから、File Start avast! Virus Cleaner を選択

"ウィルスが発見されました" ウィンドウから、ボタン "ウィルスをシステムから完全に除去します" を使用

ALWIL Software ページからダウンロードした スタンド・アローン・アプリケーションを実行する。この場合、ツールを起動する前にすべての常駐アンチウィルス保護を停止したことを確認してください。

使用法

デフォルトで、avast! ウィルス・クリーナー は 自動的にすべての作業を行います。起動すると次のことを行います。

1. オペレーティング・システム・メモリを検査します。既知のウィルスが発見されると、ウィルスの実行を停止 これにより、更なる拡散を回避。 感染による処理を停止させられないときは (例えば、他のプロセスの内部で実行するために 偽のライブラリを使用する Nimda ワーム によって 生じるかもしれません)、その拡散を停止するためにメモリ内のウィルスを不活性化します。
2. ローカル・ハードディスクを検査。
3. "スタートアップ項目" (システム・レジストリ、スタートアップ・フォルダ 等) を検査します。メモリやディスクに見つかった感染したファイルのリファレンスが削除され修正されます。
4. 2 番目の項目で確認した感染したファイルを削除し修正します (必要に応じて)。
5. 識別されたウィルスが作成した、 付加的な作業/一時ファイルを削除します。
6. ウィルス感染除去処理を完了させるのにコンピュータの再起動が必要なときは (例えば、その時使用されていてファイルを削除できない時や、不活性化したウィルスがまだメモリに存在している場合)、ユーザーに通知して直ちに再起動するかどうかを尋ねます。

重要事項

1. 検査中は、いかなるアプリケーションも起動しないでください。 一部のウィルスやワームは他のアプリケーションが起動されると、自動的に開始されます。 avast! ウィルス・クリーナー 検査

の第1段階においてのみ活性なウイルスを停止・不活性化します。検査過程の途中で (Notepad, Explorer, ... のような他のアプリケーションを起動して) ウィルスを再び活性化すると、ウイルスは恐らくコンピュータから削除されないでしょう！

2. 正しく機能させるために、avast! ウィルス・クリーナー を Windows NT/2000/XP/2003 オペレーティング・システム上で実行するときには管理者権限を必要とします。この条件が満たされないと一部のウイルスを正しく検出または削除することができません！

VRDB

VRDB の意味は "Virus Recovery Database(ウイルス修復データベース)" です。以前の avast! のバージョンでは "Integrity Database" として知られていました。VRDB の目的はすべてのセキュリティ対策にもかかわらずウイルスがコンピュータ内部に侵入してファイルが感染したときに助けることです。VRDB の助けにより、感染したファイルを修復すること(まさしく元の状態に戻すこと)が可能になります。VRDB は システムトレイに文字 "i" のアイコンで(時計の隣に)現れます。アイコンが動いていると、ちょうどその時にデータベースが作成されています。

VRDB の原理

avast! は無傷のデータベースを作成します。つまりそのファイルの実際の状態についての情報を保存し、各ファイルの **3バージョン** 前までを保存しています。データベースの作成/メンテナンスはコンピュータがアイドルのとき、またはスクリーン・セーバー(avast! のものだけではなく、すべてのスクリーン・セーバー)が動いているときに行います。一度作成されると、このデータベースは **3週間**に1度、更新されます。(この値は avast4.ini を編集して変更できます)

ファイルがウイルスに感染すると、VRDB に保存された情報を利用して修復可能です。例えば、オリジナルの状態に戻す、等。データベースに複数のバージョンのファイルがあるときは、戻したいバージョンを選択できます。

設定

VRDB の設定は システムトレイのアイコンをマウスの右ボタンでクリックして変更することができます。3つのオプションがあります。

コンピュータがアイドルの時に VRDB を作成

avast! はコンピュータがアイドル状態の時、例えば使われていないときにのみデータベースを作成します。

スクリーン・セーバー実行時に VRDB を作成

avast! スクリーン・セーバーが動いているときにデータベースを作成します。avast! に限らず、どのスクリーン・セーバーでもかまいません。

VRDB を作成しない

avast! はデータベースの作成も更新もしません。このオプションを選択すると将来ウイルスに感染したファイルを修復することができなくなります！

(訳注) integrity : the quality or state of being complete; unbroken condition: wholeness; entirety (質や状態の完璧であること ; 壊れていない状態 ; すべて ; 完全に) (Webster's New World Dictionary of American English, Third College Edition より)

13.2 スプラッシュ・スクリーン

avast! 起動中、しばらくの間 スプラッシュ・スクリーンが表示されます。このウィンドウはむしろ情報を与えるものであり、avast! が起動されていることを知らせ News を提供します。起動中にメモリを検査し、avast! は実行中のプロセス全てについてウィルスの有無を検査します。メモリ検査の進捗状況もスプラッシュ・スクリーンに示されます。 **Stop Memory Test** ボタンを押すとこの検査を中断できます。 **Registration** ボタンはライセンスキーを入力できるようにします（登録 参照）。このボタンを押すとプログラムの起動が一時停止されます。ライセンスキーを入力して "続ける" ボタンで継続してください。

13.3 よくある質問

最新の FAQ は以下のページにあります。：

<http://www.avast.com/jpn/faq-avast-4-home-professional.html>

Q: avast!4 と Outlook Express 6 を使用すると、なぜ E-メールの添付ファイルを開けなかったり、保存できなかったりするのでしょうか。

A: これは Outlook Express 6 のセキュリティの新機能です（avast! 側の問題ではありません）。添付ファイルを「保存」と「開く」がデフォルトでは無効になるからです。

次の手順に従って添付ファイルを「保存」と「開く」を有効にできます：

Outlook Express を起動します。

ツール オプション セキュリティ を選択。

「ウィルスの可能性がある添付ファイルを保存したり開いたりしない」のチェックをはずします。

[OK] をクリックします。

Q: avast! 4 をファイアウォールと一緒に使う際に注意する点は何ですか？

A: 一度 avast! 4 をインストールすると、お使いのファイアウォールによる警告を受ける事があるかもしれません。ウィルス定義ファイルの更新とプログラムの更新を探すために avast! が弊社サーバーに接続しようとするからです。avast! の接続を許可しなければ更新は機能しません。次の情報を活用してください：

avast!が接続するサーバー：

URL: <http://www.asw.cz/iavs4pro>

IP: 195.70.130.34

URL: <http://www.avast.com/iavs4pro>

IP: 64.246.6.135

URL: http://www.iavs.net/iavs4pro

IP: 204.44.156.15

URL: http://www.iavs.cz/iavs4pro

IP: 62.168.45.69

2) 接続を許可すべき avast! 4 の コンポーネント:

avast.setup

avastXX.setup ("XX" は任意の数字)

aswUpdSv.exe

ashServ.exe

ashWebSv.exe

3) 更新サービスの稼働方法

最初に avast! は、弊社サーバーに 'パケット' (メッセージ) を送り返事を待つことで、コンピュータがインターネットに接続しているかどうかを検査します。'パケット' が受信されれば、コンピュータが接続していて更新が始められることを avast! は "確認します"。もし送ったパケットに対して返事がなければ avast! は 40 秒ごとにサーバーに ping を送信 (接続) します。ping が成功すると、avast! は弊社サーバーに接続し、利用可能な新しいアップデートがあるかどうかを確認します。もしあれば avast! はそれをダウンロードしてインストールします。なければ、avast! は 4 時間 待機して再び接続しアップデートを確認します。つまり avast! は 40 秒ごとにインターネットへの接続を検出して、4 時間ごとに新しいアップデートを探します。

4) ダイアルアップ接続の最適化

もしダイアルアップ接続 だけ をご利用であれば、コンピュータがインターネットに接続しているかどうかを検出する別の方法があります。avast! はモデムのステータスから接続状況を知ることができます。40 秒ごとに ping を送信するものではありません。以下の手順で avast! を設定してください:

"設定"プログラムを開く "更新(接続)"ページをを選択 "インターネット接続をダイアル-アップもでのみで行う"オプションをチェック

5) 常時接続の最適化

コンピュータがインターネットへ常時接続している場合、avast! にこの事実を知らせることで接続確認をバイパスすることができます。次の手順に従ってください:

"設定"プログラムを開く "更新(接続)"ページをを選択 "このコンピュータはインターネットに常時接続しています"オプションをチェック

Q: avast! 4 Home を使用するために登録し登録番号を受け取りました。残念なことに、その登録番号をどうして良いのか分かりません。

A: まず avast! 4 をダウンロードしてインストールして下さい。次にコンピュータを再起動して下さい。再起動後、青い丸いアイコンが表れます。これでライセンスキーと一緒にお送りした作業手順を続けることができます。

Q: avast!4 が POP3 と SMTP の設定を 127.0.0.1 に変更しようとしています。同時に電子メールのアカウント名も変更してしまうのでメールが送信できません。何故ですか？

A: avast! では電子メールのメッセージを検査するために、この設定を変更する必要があります。しかしメッセージの送信・受信になんら影響を与えないはずですが、もし問題が生じるようなら次の手順に従ってください:

Outlook Express における、サーバーに対するメッセージの送受信をデフォルトに設定
Eメールの送受信をテスト。今なら、全てうまく行くはずですが、avast!の防御はありません。
Outlook Express を閉じる (重要です!!!)。

avast! Mail Protection Wizard を起動します。(スタート プログラム avast! Antivirus
Mail Protection Wizard)画面の指示に従ってください。

再度 Outlook Express を起動します。

Q: avast! をダウンロードしたら "無効なファイル署名です。エラー 2000000B" ... というエラーが表示されました。問題は何でしょうか。

A: ダウンロードしたプログラムが壊れています。再度ダウンロードして下さい。

Q: 'avast! 4 Home' をインストールしましたが起動するたびに "未知のエラーメッセージ", "アプリケーションはスキンを読み込めません。関数 usiGetSkin は失敗しました" と表示されます。どうやって直したらよいのでしょうか？

A:

スタート -> ファイル名を指定して実行... を選択します

次のコマンドを入力してください:

Windows NT または 2000 をお使いのとき:

C:\WINNT\SYSTEM32\REGSVR32.EXE ACTSKIN4.OCX

Windows 95, 98 または ME をお使いのとき:

C:\WINDOWS\SYSTEM\REGSVR32.EXE ACTSKIN4.OCX

Windows XP をお使いのとき:

C:\WINDOWS\SYSTEM32\REGSVR32.EXE ACTSKIN4.OCX

OK (または Enter) を押します

ファイルの登録に成功したというメッセージが表示されるはずですが

Q: avast! をインストールする前に他社のアンチウイルスソフト (Norton Antivirus, McAfee, AVG, Kaspersky Antivirus など) をアンインストールする必要がありますか?

A: はい。2 つ以上のアンチウイルスプログラムを同時に使用すると問題が発生、オペレーティング・システムが不安定になったりする可能性があります。その為、最初に(avast!インストール前)他社製品のプログラムをアンインストールすることを推奨します。

Q: Microsoft Outlook を起動すると "avoutext.dll がロード/開始できません" というメッセージが表示されます。どうすればいいですか?

A:

MS Outlook を閉じます。

REGEDIT.EXE を利用して、avast32 に関する項目を削除します。この項目はレジストリ HKLM¥Software¥Microsoft¥Exchange¥Client¥Extensions 内にあります。

ハードディスクの、全ての extend.dat ファイルを検索し、削除してください。(ハードディスク内にファイルが隠されている可能性があります)

Q: avast! アンチウイルスプログラム使用のための登録に成功し、何の問題もなくライセンスキーを受け取りました。しかし、ライセンスキーを入力しようとするとプログラムが "無効なライセンス番号です" と言ってきます。なぜですか?

A: ライセンスキーは有効です。コピー & ペースト で avast! に入力してください。以下、ご注意下さい。この数字はサーバー・オペレーティング・システム上では使うことはできません。その為、(キーを入力するには) 管理者権限で Windows にログインしなければなりません。

Q: 新しい avast! のセットアップが ODBC ドライバ がインストールされていないと警告します。どうしたら取得できますか?

A: ODBC ドライバは Microsoft 社のウェブサイト からダウンロードできます。

Q: 'Outlook/Exchange' オンアクセス・スキャナ' のプロバイダがサブシステムの起動を待っています。何か問題があるのでしょうか?

A: いいえ。このプロバイダは MS Outlook (Outlook Express ではありません!) または MS Exchange が稼働しているときにだけ実行します。これらのプログラムを使っていなければプロバイダも稼働しません。

Q: avast!をインストール後、インターネットオプションが "ダイアルしない" に設定され、変更しても元に戻ってしまいます。どうしたらいいでしょうか?

A: インターネットをダイアルアップのみで接続している場合、プログラム設定画面を開く 更新 (接続) ページを選択 "ダイアルアップモデムを使用してインターネット接続に限定" オプションを

チェックします。

Q: avast! HOME と avast! PROFESSIONAL は何が違うのでしょうか?

A: バージョンの比較は最終ページ、avast! アンチウィルス-バージョン比較をご参照下さい。

Q: avast! をアンインストールできません。そのほかに方法はありますか?

A: AvClear または AvClear4 (コンピュータにインストールされている avast! のバージョンによる) というアンインストール用ユーティリティをダウンロードできます。詳しくはウェブページ <http://www.avast.com/jpn/avast-uninstall-utility.html> をご参照下さい。

Q: ライセンスキーを受け取っていません。なぜですか?

A:

- ・ お客様が入力した電子メールのアドレスが無効である。この場合、メールはおそらく私たちの所に戻ってきています。
- ・ お使いのメールサーバが利用不可能、または、ライセンスキーの入っているメールを受け取る間にエラーレポートが発生。このメールはのちほど配信されることが可能です。大抵は数日間 4 時間ごとに配信を試みます。
- ・ 受信メールボックスが一杯で、そのためにライセンスキーの入ったメールの配信ができない。
- ・ ある種のスパム保護をご使用になっており、ライセンスキーの入ったメールが何らかの理由で拒絶されている。

もしライセンスキーの入ったメールを 1 日以内に受け取らないときは、他のメールアドレスやメールサーバで再登録されることをお勧めします。

13.4 ウィルスについての情報

avast! はデータベースにあるウィルスの基本的な情報を表示することができます。 広範囲に拡散したウィルスについて、avast! の接続を介して、Alwill 社の WEB ウィルス・データベースにて、きわめて包括的な情報を得ることができます。

ウィルスについての情報を閲覧/検索は基本機能ユーザ・インターフェースのメニュー - **ウィルス・データベース** で行ってください。 **高機能ユーザ・インターフェース** では、**ウィルス・データベース** フォルダを選択してツールバーの **フィルタ** アイコンをクリックするだけです。

ウィルス情報を検索

リスト内のウィルスは多数のパラメータを使って検索できます。 ウィルス名称が判明している、特定ウィルスについての情報を表示したいときは、名前を入力して **検索** ボタンをクリックしてください。 名前が判らないときには、ワイルドカード "*" と "?" を使えます。 記号 "*" (アスタリスク) はいくつもの文字と置き換わり、記号 "?" (クエスチョン マーク) は 1文字の代わりをします。

例 : Klez virus を検索します。 データベース内の実際の名前は Win32:Klez-H [WRM] です。 その為、ワイルドカードを用います。 : *klez*。 文字列 "klez" を含むすべてのウィルスがこの方法で見つかります。

検索範囲を狭めるために、それぞれのウィルスの特徴に隣接する 3 段階のチェックボックスを利用できます。 各々の状態は次のような意味を持ちます。

薄暗い色 (ウィルスがこの特徴を有するか有しないかという)検索中に、ウィルスのこの特徴は無視されます。 チェックボックスのステータスはデフォルト。

チェックあり 検索されたウィルスはこの条件を満たしています。

チェック無し 検索されたウィルスはこの条件を満たしません。

ウィルスの特徴の意味

ITW - 非常に活発なウィルス性質

ITW ("In The Wild") と呼ばれるウィルスは世界中のユーザー間で広く拡散します。

Worm - ファイルに感染しません

特殊なウィルスでファイルに感染しませんが、e-mail を経由して拡散したり、パスワードを盗んだり ... というような悪いことをします。

マクロ

マクロウィルスで、特に Microsoft の製品 (Word, Excel, ...) のマクロ言語を利用するウィルス。

Rep - 修復可能

avast! はこれらのファイルを修復できます。 感染したファイルを感染前の元の状態に戻せます。

Care - 削除にあたり特別な注意が必要です

これらのウイルスについては削除するために特別な手順を踏まなければなりません（特別な注意を払わないと、ウイルス自体より更に大きなダメージを受けます！）。

Boot - ブートセクタに感染

このタイプのウイルスはハードディスクやフロッピーディスクのブートセクタに感染します。

MBR - MBR セクタに感染

このタイプのウイルスはハードディスクの マスター ブートセクタ に感染します。

COM - COM ファイルに感染

このタイプのウイルスは拡張子に .com を持つ実行型ファイルに感染します。

EXE - EXE ファイルに感染します

このタイプのウイルスは拡張子に .exe を持つ実行型ファイルに感染します。

RES - メモリに常駐します

このウイルスは RAM メモリに留まり起動されたファイルに感染します。

13.5 avast! iNews

avast!ユーザーに対する通知を継続する為、最新ニュースを受信します。 ニュースはプログラムの更新と同じ方法で配布されます。 ユーザーに新しいウイルスの危険性、重要なプログラムの変更や改良 等 についてお知らせします。 最新のニュースは受信後 7 日間 avast! スプラッシュ・スクリーンに表示されます。

ニュースをご覧になりたいときは次のようにして下さい。

基本機能ユーザ・インターフェース で **Menu** ボタンをクリックし、avast! iNews を選択してください。 ニュースが2つに区切られた分割ウィンドウに表示されます。 左の部分にはニュースのリストが、右の部分には対応する内容が入ります。 左の部分でご覧になりたいニュースをクリックするとすぐに表示されます。 **Close** ボタンはニュースの閲覧を終了します。

高機能ユーザ・インターフェース では avast! iNews フォルダをクリックしてください。 ニュースのリストが右上の部分に、対応する内容が右下の部分に表示されます。 ニュースを選択すると内容が表示されます。

13.6 登録

avast! アンチ・ウィルス・パッケージはインストール後に登録しなければなりません。登録は個別のライセンスキーの入力により完了します。ライセンスキーは多数の文字や数字で構成されます。キーを入手するには、適切なライセンスの avast! プログラムを購入して下さい。ホーム・ユーザーは ALWIL Software の WEB ページにあるオンライン・フォームに記入してキーを入手することができます（下記参照）。

次の方法でああなたのライセンスキーを入力してください。

最初のプログラム起動

最初のプログラム起動で avast! はあなたのライセンスキーを入力する小さなウィンドウが表示されます。

基本機能ユーザー・インターフェース・メニュー

基本機能ユーザー・インターフェース で Menu About avast! を選択。表示された ウィンドウの一番下にある License key ボタンを押してください。

常駐保護メニュー から

システムトレイにある 文字 "a" のアイコンをマウスの右ボタンでクリックしてください。ポップアップメニューから About avast! を選択して "License key ライセンスキー" ボタンをクリックして下さい。

高機能ユーザー・インターフェース・メニューから

高機能ユーザー・インターフェース・メニューで Help Regisatration を選択してください。

上記全てのケースで、小さなウィンドウが現れます。ライセンスキーをラインに入力して OK ボタンを押してください。ありがちなタイピング・エラー（例えば、文字 0 (zero) を O (大文字の "o") に変えてしまう）を避けるために、コピー&ペースト の手法 を使ったキーの入力をお勧めします。（マウスでライセンスキーを選択、Ctrl+C を使い Windows のクリップボードにコピー、Ctrl+V を使い 登録ダイアログ にペーストします）。

avast! がキーを受け入れないときは、たぶん間違ってタイプされたか(再度、コピー&ペースト の手法 をお使いになるようにお勧めします)、またはライセンスが適切ではありません(例えば、ワークステーション用のライセンスキーはサーバー・オペレーティング・システム上にインストールされた avast! には 入力することができません)。そのような場合は avast! プログラムの販売者が ALWIL Software のサポートにご連絡下さい。

