G DATA Total Security

ユーザーマニュアル

目次

はじめに	4
ユーザーサポートについて	4
インストール	4
セキュリティセンター	13
ステータス	13
ライセンス	13
ソフトウェアの機能	13
アンチウイルス	22
ウイルススキャン	22
隔離されたファイル	22
ブートメディア	22
ファイアウォール	26
ステータス	26
ネットワーク	26
ルールセット	26
バックアップ	38
バックアップと復元	38
パスワードマネージャー	55
ブラウザプラグインの使用方法	55
チューナー	60
復元	60
ブラウザクリーナー	60
フィルタリング	63
新規ユーザー	63
禁止するコンテンツ	63
許可するコンテンツ	63
インターネット利用時間の監視	63
コンピュータ利用時間の監視	63
パーソナルフィルタ	63
設定 ログ	63
データセーフ	75
データセーフ作成ウィザード	75
モバイルデータセーフを作成	75
モバイルデータセーフを開く	75
オートスタートマネージャー	86
プロパティ	86
デバイスコントロール	88

設定	89
一般 アンチウイルス	89 89
ファイアウォール	89
チューナー	89
デバイスコントロール	89
バックアップ	89
ログ <u></u>	139
アンチウイルスのログ	139
ファイアウォールのログ	139
バックアップのログ	139
アンチスパムのログ	139
フィルタリングのログ	139
デバイスコントロールのログ	139
FAQ: ブートスキャン	141
ブートスキャンの準備	141
ブートスキャンの流れ	141
FAQ: 各種機能について	145
G DATA アイコン	145
ウイルススキャンの流れ	145
ウイルス検出時の対応	145
ファイアウォールアラート	145
ウイルススキャンで「not-a-virus」が表示される	145
アンインストールの方法	145
USB キーボードを間違ってブロックした場合	145
FAQ: ライセンスについて	154
複数台用ライセンスを所有している場合	154
ライセンスの期限が切れた場合	154
コンピュータを買い替えたり、クリーンインストールした場合	154
データ保護に関する声明	154
コピーライト	154

はじめに

この度はG DATA 製品をお買い求めいただき、誠にありがとうございます。本マニュアルでは、 製品のインストール、コンピュータを不正プログラムから効果的に保護するためのヒントが分か りやすく纏められています。本製品を操作する上でわからないことがでてきたら、まずは、マ ニュアルやG DATA ウェブサイトのFAQなどでご確認ください。

このマニュアルでは、製品のインストール方法と実用的なヒントをまとめています。



プログラム バージョン: 25.1.0.4	TRUST IN GERMAN SICHERHEIT.

*スクリーンショットに関して: 本マニュアルで使用されている画像は、開発中のトータ ルセキュリティもしくはインターネットセキュリティを使用しています。

メモ: 各機能の使用方法を簡単に調べたい場合はオンラインヘルプが便利です。オンラインヘルプは各画面にあるヘルプボタンを押すことで表示できます。

ユーザーサポートについて

操作方法など、ご購入後の製品に関するお問い合わせは、ユーザーサポートで受付いたします。 ※体験版の場合は、ユーザーサポートのご利用はできません。予めご了承ください。

ユーザーサポートの連絡先

問い合わせ先については、登録後のメールをご確認ください。

1. サポート期間

ライセンス有効期間内

2. サポート範囲

製品のご利用の説明、疑問点にお答えするサービスとさせていただきます。 以下の場合には、お問い合わせに対してのご回答ができませんので、予めご了承ください。

a) 本製品で保証している動作環境外でのお問い合わせ

- b) 本製品ではないもの(ハードウェア・他社製品)に関するお問い合わせ
- c) サポート時間外のサポートおよび、指定された方法以外の方法でのサポートのご依頼

3. ユーザーサポートをお受けになる際に

お問い合わせの際は、お客様番号または、レジストレーション番号をご用意いただき、更に質問 要点を整理していただいた上で、お問い合わせいただきますようお願いいたします。

インストール

まず本製品をインストールする環境についてご確認ください。本製品を正常に機能させるために は、以下の**動作環境**を満たす必要があります。

動作環境

対応OS	Windows 10 (32bit/64bit) Windows 8/8.1 (32bit/64bit) Windows 7 (32bit/64bit) ※インストールには管理者(Administrator)権限でログインする必要があ ります。 ※日本語OS環境のみサポート。 ※最新のサービスパックを推奨。
CPU	各OSが推奨するCPU
メモリ	2GB以上

	※グラフィックメモリとの共用は除きます。
ハードディスク	1GB以上の空き容量
デバイス装置	DVD-ROMドライブ(パッケージ版のみインストール時に必要) ※ブートCDの作成・バックアップ時には書き込み可能なCD/DVDドライ ブが必要です。
ディスプレイ	解像度1024×768ドット、High Color(16ビット、65,536色)以上
その他	InternetExplorer8以上 インターネットに接続可能な環境[ブロードバンド以上を推奨]

※他のウイルス対策ソフトとは併用できません。

※ユーザー登録するためにはPCのメールアドレス(携帯メール不可)が必要です。 ※オンライン上へのバックアップ機能を利用する場合は、ブロードバンド以上のインターネット 接続環境が必要です。

新品のコンピュータ、もしくは本製品インストール前に他のウイルス対策ソフトで保護されてい たコンピュータでは、次のステップを参考に本製品をインストールしてください。それ以外の場 合やコンピュータがウイルスに感染している疑いがある場合は、インストール前にブートスキャ ンを実行することをお勧めします。 ブートスキャンの方法については、プートスキャンの流れ を参照してください。

注意: 本製品をインストールしようとしているコンピュータに、他社製のウイルス対策 ソフトがインストールされている場合は、必ず他社製品をアンインストールした後で、 本製品をインストールしてください。ウイルス対策ソフトは Windows のシステム深く に配置されて動作するため、複数の製品を同時に使用すると深刻な問題が出る場合があ ります。

なお、他社製品をアンインストールする場合、通常アンインストールではデータのゴミ が残る場合がほとんどで、動作不良の原因となります。製品ごとに用意されている、完 全アンインストールツールを使用してアンインストールする事で、コンピュータをクリ ーンな状態にでき、その上で本製品をインストールする事で最適な動作をさせることが できます。他社製品の完全アンインストールツールに関しては、各社のユーザーサポー トをご利用ください。

ステップ1-インストールの開始

本製品はCD/DVD版もしくは、ダウンロード版として販売されています。それぞれのインストール方法は次の通りです:

- CD/DVD 版の場合:本製品CD/DVDをドライブにセットします。
- ダウンロード版の場合: ダウンロードしたファイルをダブルクリックします。

しばらくすると、自動的にインストール開始画面が開きます。

注意: インストール起動画面が自動表示されない場合は、Windowsの自動再生機能が無効になっている可能性があります。

- 自動再生の画面が表示される場合は、AUTOSTRT.EXE の実行 をクリックしてく ださい。
- 自動再生の画面が開かない場合は、Windows 上で本製品のディスクを探して開き、Setup もしくは Setup.exe をダブルクリックしてください。

ステップ2-インストール方法の選択

ウィザードに沿ってインストールを行います。まず、**標準インストール**もしくはユーザー自身で インストール内容を決定できる**カスタムインストール**を選択する画面が表示されるので、希望す るインストール方法を選択してください。(推奨:標準インストール)

カスタムインストールでは、プログラムの保存場所やインストールする機能を任意で選 択できます。

G	G DATA インターネットセキュリティ
	G DATA 製品をご利用いただき、ありがとうございます。
	このウィザードでは、G DATA インターネットセキュリティ のインストールをご案内します。インストール方法を選択し てください:
	標準インストール 標準的な構成で G DATA インターネットセキュリティをインストールします。 (推奨)(5)
	カスタムインストール 構成を望快して G DATA インターネットセキュリティをインストールします。 (上級者向け)(U)
	✓ <u>マルウェア債報(ニシアデブ</u>) = 参加(推奨)(<u>M</u>)
	< 戻る(B) 次へ(<u>N</u>) > キャンセル
	G DATA SIMPLY SECURE

- 標準インストールを選択した場合 ステップ3の画面が表示されます。
- カスタムインストールを選択した場合

使用許諾契約の画面が表示されるので、**使用許諾契約の条項に同意します**にチェックを入れて**[次へ]**を選択します。ステップ4のカスタムインストール用の画面が表示されます。

マルウェア情報イニシアチブとは

G DATA セキュリティラボでは、G DATA 製品の利用者をコンピュータの安全性を脅かす脅威か ら保護するため、保護・対策の研究や分析に絶え間なく励んでいます。 マルウェア研究では、マ ルウェアに関する情報が多ければ多いほど、効果的な保護メカニズムの開発をいち早く進めるこ とができます。これらの情報をG DATAの研究・分析・開発に効率的に取り入れることを可能に するための取り組みが、G DATA マルウェア情報イニシアチブです。 これにより、マルウェア に関するデータをG DATA セキュリティラボに送信することができます。 より多くのユーザー 様に参加頂くことで、他のG DATA 製品をご利用の方々もインターネットをより安全に利用でき るようになります。このインストール方法の選択画面にあるチェックボックスで、このデータを 提供するかどうかの選択ができます。

ステップ3 - 使用許諾契約

使用許諾契約書をご確認いただき、同意できる場合は**[同意してインストール]**をクリックして ください。インストールが始まります。

6	G DATA ተンターネ	ットセキュリティ
	マルウェア情報・	イニシアチブ
	協力のお願い未知の脅威へのレスポンス向上のた 置名のユーザーデータと統計情報の提供にご協力く	-ル方法を選択し た ださい。
	情報の取り扱いに関する誓約書 G DATA のアンチウイルス機能には、特定の条件下には 信する保護コンポーネントが含まれています。保護コンポ 必要な特定データは、常に同サーバーへ送信されます。 ウエヴサイルのアドレス送信が必須となります。また、別の パンキング茶トロイの木馬の適別や駆除のために、チェッ 検知にピヘイピアゴロカーンの機能は、クランドからの情情	★ SUTCG DATAのクラウドサーパーへデータを送 ニーネントのコア機能を正常に機能させるために 保護コンボーネントの10、ウゴア保護(は、 保護コンボーネントの10、ウゴア保護(は、 保護コンボーネントの10、ウゴア保護(は、 を取得することにおり、コンピュータをよりの効果 を取得することにおり、コンピュータをよりの効果
	印刷(P)	参加します(Y) 参加しません(N)
		< 戻る(<u>B</u>) 次へ(<u>N</u>) > キャンセル
		G DATA SIMPLY SECURE

ステップ4 - カスタムインストール (オプション)

カスタムインストールを選択した場合は、次の2つの画面でインストール先フォルダとインスト ールする機能の範囲を指定します。 標準インストールを選択した場合は、この手順は省略されます。

あらかじめ設定されているインストール範囲には以下の違いがあります。

- ユーザー定義: この設定ではソフトウェアの機能(例: アンチウイルス、アンチスパムなど)の横にあるボックスをチェックして、インストールする機能を自分で指定することができます。G DATA アンチウイルス、G DATA インターネットセキュリティ、またはG DATA トータルセキュリティ、それぞれの製品に応じて、ここで選択できる機能の種類は変わります。
- 完全: 製品に含まれる全ての機能がインストールされます。
- **最小**: ウイルス対策に最低限必要な、アンチウイルス機能のみがインストールされます。

本製品のインストール後に、あとからインストールされている機能を変更する事も可能 です。セットアップを起動し、**変更**を選択すると、カスタムインストールの要領で機能 の追加や削除を行う事ができます。

ステップ5 - 製品種類の選択

この手順では、本製品を製品版として使用するか、体験版として試用するかを選択します。

G	G DATA インターネットセキュリティ		
ワクチン更新を利用するためにユーザー登録を行ってください。			
	G DAIA SIMPLY SECURE		

- 製品版として登録:製品版を購入した場合は、ここを選択します。
- 体験版として登録: 無料体験版として利用する場合は、ここを選択します。なお、体験版 を利用するには、氏名とメールアドレスの入力が必要です。入力されたメールアドレスに は、アクセスデータが送付されるので、必ず有効なPC用メールアドレスを入力してください。

ステップ6 - ライセンスの認証

インストール中に**ライセンスの認証**を行い、プログラムの機能をすべて使用できるようにしま す。

レジストレーション番号を入力:製品を新規購入された方は、ここを選択し、購入した製品のレジストレーション番号を入力してください。パッケージ版を購入された場合は、レジストレーション番号は同梱の用紙に記載されています。ダウンロード版を購入された場合は、レジストレーション番号はメールなどで送信されています(購入したWEBストアによって異なります)。

注意: レジストレーション番号を入力して、製品が正常に認証されると、更新ファイル をロードできるようになります。複数台版やライセンスの移行で必要になるアクセスデ ータは、認証後に G DATA から送付されるメールに記載されています。アクセスデータ は厳重に保管してください。

入力したレジストレーション番号で認証できない場合は、まず入力ミスの可能性がない か確認してください。それでも問題が解決できない場合は、ユーザーサポート にお問い 合わせください。

 アクセスデータを入力: アクセスデータ(ユーザー名とパスワード)を使って、認証します。本製品を再インストールしたり、他のコンピュータでライセンスを認証したい場合 (複数ユーザー版の場合など)は、ここを選択してアクセスデータを入力してください。

注意: アクセスデータは初回認証(レジストレーション番号を入力)後に G DATA から 送付されたメールに記載されています。製品には同梱されていません。

アクセスデータを紛失したり忘れた場合は、**アクセスデータの確認**をクリックしてくだ さい。ブラウザが自動的に起動して G DATA のサポートページが開きます。サポートペ ージに記載されている手順に沿って手続きをし、アクセスデータを再確認してくださ い。※アクセスデータの再確認では、レジストレーション番号が必要です。またレジス トレーション番号の登録時に使用したメールアドレスを変更した場合は、ユーザーサポ ートへお問い合わせください。

・後で認証を行う:後で製品を認証する場合はここを選択します。認証を行わない場合はワクチン更新が行われないため、最新の脅威に対して適切な保護を提供する事ができなくなります。インストール後はできるだけ早く認証の手続きをしてください。インストール後の認証は、ワクチン更新を実行しようとした際に表示されるウインドウか、設定アイコンをクリックして、アンチウイルスの更新領域などから行う事ができます。

G	G DATA インターネットセキュリティ
	 レジストレーション番号を入力 G DATA インターネットセキュリティ のライセンスを新規購入した場合、ここからレジストレーション番号の登録を行います。(血)
	アクセスデータを入力 ライセンスの初回登録後に発行されたアクセスデータで認証を行います。(d)
	後で認証を行う インストール後に認証を行います。(A)
	< 戻ō(B) 次へ(N) > 終了(E)
	G DATA SIMPLY SECURE

ステップ7 - インストールの完了

最後に、インストールを完了するためにコンピュータを再起動してください。再起動が完了する と本製品が使用可能になります。

インストール後

インストール後には、ショートカットやタスクバーのアイコンから本製品を起動できるようになり、各種セキュリティ機能が利用可能になります。



G DATA アイコン: ユーザーの操作が必要になると、タスクバーのG DATA アイコンからお知らせします。このアイコンを右クリックして起動を選択する事で G DATA のインターフェイスを開く事ができます。その他の情報は、G DATA アイコンの項を参照してください。



G DATA シュレッダー: インストールでシュレッダーを選択すると、デスクトップ上に シュレッダーアイコンが作成されます。シュレッダーを使ってファイルを完全に削除す るには、ファイルをシュレッダーのアイコン上に移動するか、ファイルの上で右クリッ クして、シュレッダーを選択します。一旦シュレッダーでファイルを削除すると、ファ イルは復元不可能になります。※シュレッダー機能は、G DATA アンチウイルスには 含まれていません。

クイックスキャン: 特定のファイルやフォルダだけをウイルススキャンしたい場合は、 プログラム画面を起動する必要はありません。対象の上で右クリックし、**ウイルスス キャン**を選択すると、スキャンが実行されます。

本製品をインストールしてコンピュータを再起動した際に、Windows が起動しない 場合: まずCD/DVDドライブに本製品CDが挿入されたままではないか確認してください。本製品CDは、ブートスキャン機能を搭載しているので、コンピュータの設定によっては、Windows 起動前にブートCD が起動している可能性があります。製品CDがCD/ DVDドライブに挿入されていた場合は、CDを取り出し、コンピュータを再起動してください。Windows が通常通りに起動します。

ブートスキャンに関する詳細は、**ブートスキャンの流れ**の項を参照してください。

セキュリティセンター

本製品を起動すると立ち上がるセキュリティセンター画面では、各機能のステータスを確認した り、操作を実行できます。ウイルスなどの脅威に対する保護は、通常バックグラウンドで動作し ますが、利用者の判断が必要になる場合はタスクバー上にその情報が表示されます。

GDATA	G DATA トータルプロデクション			? _ ×		
5	A 🖗	* ¢ 4	. 2	: 🐌 🖓	4	
	セキュリティセン	ター				0
\bigotimes	このコンビュータは保護され	れています	\bigotimes	ワクチンは最新の状態です	ŧ.	C
	 ○ リアルタイム意味(E): ○ アイドリングスキャン(L): ○ フナイアウォール(E): ○ ウェブ保積(Y): ○ メール保護(M): ○ アンチスパム(S): 	有効(すべてのモジュール) 一時停止中 ユーザー定義 有効 有効		 ※ 新日のフクチン英新(以): ※ 次回のフクチン支新(点): プラウザ/アブリ保護 ジノンクカード(G): ※ キーロカー対策(な): ※ エクスプロイト対策(x): 	2015/06/08 59 分	
\otimes	ライセンス: 有効期限 : 201 ライセンス有効期間について	6/09/08 アクセスデータ(<u>)</u> て	\square	メッセージはありません		۵
J0756.K-	Say: 25.1.0.4			TRUST IN GE	RMAN SICH	ERHEIT.

セキュリティステータス

セキュリティステータスのアイコンを使用すると、ボタン操作ひとつでコンピュータの保護状況 を簡単に改善できます。

このアイコンをクリックすると、コンピュータを守るための対策が提案されます。全てのセキュ リティステータスが再び緑色に戻るまで対策を行い、保護レベルを改善してください。セキュリ ティステータスが全て緑色になれば、コンピュータの保護は最新の状態であり、セキュリティセ ンターでの作業も終了です。

赤色のマーク=今すぐに改善が必要(システムが危険にさらされている可能性があります)

● 灰色のマーク=このセキュリティ機能は無効(例 アンチスパム機能を停止している)

① 黄色のマーク=近いうちに改善が必要(例 ソフトウェアアップデートが利用可能)

本製品の全ての機能は、必要に応じて設定変更する事ができます。機能や設定の詳細については

このオンラインヘルプの各項目をご覧ください

ステータス

以下の項目から現在のセキュリティステータスの確認ができ、それぞれの項目をクリックし操作 を実行することで、コンピュータの保護状況を改善できます:

リアルタイム保護

ウイルスガードはウイルスを常時監視するリアルタイムスキャン機能で、書き込みおよび読み取 り処理を監視します。あるプログラムが不正な機能を実行したり、不正ファイルを拡散しようと すると、ウイルスガードがこれを防ぎます。ウイルスガードは最も重要なウイルス対策の1つで すので、特別な理由が無い限り、常に有効にしておいてください。

 ウイルスガードを無効にする:必要に応じてウイルスガードを無効化できます。例えば、 大量のデータをハードディスク上のある場所から別の場所にコピーしたり、多くのメモリ を必要とする演算プロセス(DVDのコピーなど)を実行する時には、ウイルスガードを 無効にするとコンピュータのパフォーマンスが向上します。 ただし、パフォーマンスのためにウイルスガードを無効化したい場合は、ウイルスガード を無効化する際や、アンチウイルスの設定画面から設定できる、セキュリティ /パフォ ーマンスのオプションを調整する事で、納得行くパフォーマンスを出せるか先に確認す ることをお勧めします。

注意: ウイルスガードは必要な時だけ無効化してください。また、ウイルスガードが無効 に設定されている間は、できるだけインターネットには接続しないようにし、CD、 DVD、メモリカードまたは USB メモリなどに保存されている、スキャンをしたことのな いデータにはアクセスしないように注意してください。

- ふるまい検知を無効にする:ふるまい検知(ビヘイビアブロッキング)は、ワクチンによる検出とは独立した、未知のウイルスを検出するための機能です。この機能は特別な理由が無い限り、常に有効にしておいてください。
- 詳細設定: この機能に関する設定画面、設定 | アンチウイルス | リアルタイム保護 を開きます。

前回のアイドリングスキャン

前回コンピュータをアイドリングスキャンによってスキャンした日時が表示されます。この項目 が赤色で表示されている場合は、できるだけ早くウイルススキャンを実行してください。※アイ ドリングスキャンが無効になっている場合は**前回のウイルススキャン**と表示されます。

コンピュータをスキャン: コンピュータを数時間使わなくてもいい場合や、ウイルス感染の疑いがあり、すぐに結果を確認したい、といった場合には、ここからすぐにコンピュータ全体をスキャンできます。この全体スキャンの間もコンピュータは使用できますが、こ

こで実行されるスキャンはコンピュータの最大パフォーマンスを利用するため、他のアプ リケーションのパフォーマンスにも影響を与えます。この機能の詳細は ウイルススキャ ンの流れの項を参照してください。

・ 今すぐ実行: アイドリングスキャンは、ウイルススキャンがユーザーの作業の邪魔にならないように、コンピュータが使われていない状態にのみ自動的に起動するスキャン機能です。アイドリングスキャン中にユーザーがコンピュータを利用すると、実行中のスキャンはすぐに休止状態となります。次のアイドリングスキャン実行日よりも先にスキャンを行いたい場合は、今すぐ実行を選択してください。 仕事の休憩中などにアイドリングスキャンを自動実行したくない場合は、アイドリングスキャンを振動にするを選択して機能を無効化してください(非推奨)。

ファイアウォール

ファイアウォールは、外部の不正侵入からコンピュータを防御するため防御する機能で、インタ ーネットやネットワークとコンピュータとの間で送受信されるデータを監視します。許可されて いないデータの書き込みやダウンロードを検知すると、ファイアウォールが警告を発し、それら のデータ通信を阻止します。 ※この機能はG DATA インターネットセキュリティ、G DATA トータルセキュリティで利用でき ます。

- ファイアウォールを無効にする:必要に応じて、ファイアウォールを無効にします(非推奨)。コンピュータがインターネットやネットワークと接続されている環境では、不正な 攻撃や侵入から保護されなくなりますのでご注意ください。
- オートパイロットを無効にする:オートパイロットは、ファイアウォールが許可/拒否するアプリケーションを自動的に判断し制御する機能です。通常は、この機能を有効にしてファイアウォールを利用することをお勧めします。オートパイロットを無効にした状態でファイアウォールを使用する場合は、プログラムにルールを学習させ、ネットワーク環境に合わせて設定していく必要がありますので、上級者ユーザー以外は、オートパイロットを無効にしないでください。
- 詳細設定: この機能に関する設定画面、設定|ファイアウォール|自動を開きます。

ウェブ保護

インターネット利用中の保護を提供する**ウェブ保護**の有効/無効を切り替えます。ウェブ経由で の感染が増加している現在、ウェブ保護は感染防止のための重要な機能です。ウェブ機能を有効 にすると、ウェブサイト経由の感染やフィッシング詐欺などの脅威をアクセス前に未然に防ぎま す。

インターネット閲覧中にウェブサイトが本製品によって脅威として検出されると、サイトの閲覧 はブロックされ、ブラウザ画面に警告が表示されます。

- ・ウェブ保護を無効にする: ウェブ保護を無効にすると、ウェブサイトのチェックが無効に なるため、ウェブサイトから大量にデータをダウンロードする際などにダウンロード時間 を省略できます。また、ウェブ保護が無効中の状態も、ウイルスガードがコンピュータを 感染から守ります。しかし、例外的ケースを除いては、ウェブ保護は有効に設定すること をお勧めします。
- ・ 例外を設定: ウェブ保護は、不正コードが仕掛けられたウェブサイト、またはフィッシン グなどの詐欺サイトからコンピュータを保護する機能です。しかし場合によっては、ウェ ブ保護を有効にすると、安全なサイトであるにも関わらず、ウェブページが正しく表示さ れないことがあります。そのような場合は、対象ページのアドレスをホワイトリストに例 外登録してください。これにより、ウェブ保護がブロックしていたページが閲覧できるよ うになります。詳細については、例外の項を参照してください。
- 詳細設定: この機能に関する設定画面、設定 | アンチウイルス | ウェブ保護 を開きます。

メール保護

メール保護機能は、送受信されるメールの内容や添付ファイルをスキャンし、ウイルス感染を防 ぎます。ウイルスが検出された場合は添付ファイルを削除、もしくはウイルスの駆除を行いま す。

- メール保護を無効にする:メールのスキャンを行いたいくない場合は、ここを選択してください。ただし、その場合はメール経由のセキュリティリスクが大きく増えますので、特別な場合を除いてメール保護は有効に設定しておくことをお勧めします。
- 詳細設定: この機能に関する設定画面、設定 | アンチウイルス | メールスキャン を開きます。

Microsoft Outlook: Microsoft Outlook には、専用プラグインがインストールされます。この プラグインは、メールスキャンで設定できる POP3/IMAP ベースの保護を提供し、これにより、 Outlook 上でのウイルスチェックがより簡単に行えます。メールまたはフォルダのスキャンを実 行するには、Outlook メニューバーの [G DATA] > [フォルダをスキャン] を選択します。 ※通常のメールスキャンと併用すると送受信に問題が出る場合がありますので、その際はPOP/ IMAP/SMTPのスキャンを無効にしてください。

アンチスパム

スパム保護は、迷惑な広告メールや大量のスパムメールに対する対策機能です。G DATA のスパム保護は、緻密に設定された判断基準をもとにスパム判定を行い、迷惑メールや迷惑メール送信者を効果的にブロックします。

※この機能はG DATA インターネットセキュリティ、G DATA トータルセキュリティで利用でき ます。 ログ:スパム:スパムと判断されたメールに関する情報が一覧で表示されます。 [更新] をクリックすると、ステータス情報を更新できます。対象を選択して [削除] をクリック すると、指定したメールのログを削除できます。なお、ここで削除しても、メールプログ ラムで受信した実際のメールは削除されません。

[ホワイトリストに登録] では、選択したメールの送信者をホワイトリストに入れ、それ以降はこの送信者からのメールに対するスパムチェックは省略されるようになります。 逆に [プラックリストに登録] へ移動すると、この送信者に対するメールは、以降、より入念なスパムチェックが行われるようになります。

 ログ:スパム以外:スパムではないと判断されたメールに関する情報が一覧で表示されます。
 [更新]をクリックすると、ステータスを更新できます。対象を選択して
 [削除] を押すと、指定したメールのログを削除できます。なお、ここで削除しても、メールプロ グラムで受信した実際のメールは削除されません。

[ホワイトリストに登録] では、選択したメールの送信者をホワイトリストに入れ、それ以降はこの送信者からのメールに対するスパムチェックは省略されるようになります。 逆に [ブラックリストに登録] へ移動されると、この送信者に対するメールは、以降、 より入念なスパムチェックが行われるようになります。

ホワイトリストを編集: 特定の送信者からのメールアドレスやドメインをスパム扱いしないように設定できます。ホワイトリストに登録するには、[新規作成] ボタンをクリックし、スパム扱いしたくないメールアドレス(例:newsletter@gdata.co.jp) またはドメイン(例:gdata.co.jp)を送信者アドレス/ドメインの欄に入力します。すると、入力された送信者またはドメインからのメールは、スパムではないと判定されるようになります。

また、【インポート】をクリックすると、既存のメールアドレスまたはドメインのリスト をホワイトリストに追加できます。インポートするリストには、アドレスおよびドメイン が1件1行ずつ、上から順に入力されている必要があります。データフォーマットは、 Windows の「メモ帳」で作成できるようなテキスト形式(txt ファイル)を使用しま す。【エクスポート】からは、上述のホワイトリストをテキスト形式で書き出すことがで きます。

- ブラックリストを編集: 特定の送信者からのメールアドレスやドメインをスパム扱いする ように設定できます。ホワイトリストに登録するには、[新規作成] ボタンをクリック し、スパム扱いしたいメールアドレス(例: newsletter@gdata.co.jp) またはドメイン (例: gdata.co.jp)を送信者アドレス/ドメインの欄に入力します。すると、入力された 送信者またはドメインからのメールは、スパムと判定されるようになります。 また、[インポート]をクリックすると、既存のメールアドレスまたはドメインのリスト をブラックリストに追加できます。インポートするリストには、アドレスおよびドメイン が1件1行ずつ、上から順に入力されている必要があります。データフォーマットは、 Windowsの「メモ帳」で作成できるようなテキスト形式(txt ファイル)を使用しま す。[エクスポート]からは、上述のブラックリストをテキスト形式で書き出すことがで きます。
- アンチスパムを無効にする: アンチスパムを無効します。コンピュータでメールを利用しない場合などに、この機能を利用してください。
- **詳細設定**: この機能に関する設定画面、<u>設定 | アンチスパム | スパムフィルタ</u> を開きます。

前回のワクチン更新

ここでは、最後にインターネットからワクチンをダウンロードした日時が表示されます。ステー タス情報が赤色で表示される場合には、できるだけ近いうちに、ワクチン更新を実行してくださ い。ワクチンを更新するには、この項目をクリックし、プルダウン表示される**ワクチンの更新**を 選択します。

- **ワクチンの更新**: デフォルト設定では、ワクチンの自動更新が行われように設定されていま す。今すぐに更新を手動実行する場合は、ここをクリックします。
- 自動更新を無効にする: ワクチンの自動更新を無効にする場合はここをクリックします。 特種なケースを除いて、自動更新は常に有効にしておいてください。
- 詳細設定: この機能に関する設定画面、設定 | アンチウイルス | 更新 を開きます。

次回のワクチン更新

ここには、次回のワクチン更新までの時間が表示されます。ワクチンを更新するには、この項目 をクリックし、プルダウン表示される**ワクチンの更新**を選択します。

- **ワクチンの更新**: デフォルト設定では、ワクチンの自動更新が行われように設定されています。今すぐに更新を手動実行する場合は、ここをクリックします。
- 自動更新を無効にする: ワクチンの自動更新を無効にする場合はここをクリックします。 特種なケースを除いて、自動更新は常に有効にしておいてください。
- 詳細設定: この機能に関する設定画面、設定|アンチウイルス|更新 を開きます。

バンクガード

G DATA のオンラインバンキング対策機能「**バンクガード**」は、ネットバンキングを標的とす るバンキング系トロイの木馬による中間者攻撃(man-in-the-middle攻撃)を検出し、リアルタ イムで保護します。

バンキング系トロイの木馬は、金銭的被害をもたらす悪質な不正プログラムで、現在、世界各国 で猛威を振るっています。銀行サイトがオンライン取引の暗号化をしていても、攻撃は復号化さ れたブラウザ上で行われるため、通常のウイルス対策ソフトでは攻撃の回避が困難でした。G DATA 製品に搭載されているバンクガードは、ネットワークライブラリをリアルタイムでチェッ クすることにより、man-in-the-middle攻撃によるブラウザの不正操作を防止します。

キーロガー対策

コンピュータで入力したキー入力を不正に記録するプログラムを監視します。 ※キーロガー対策は、文字入力にIMEを使用していない場合のみ効果があります。 IMEを使用しない文字入力を行うには、「テキストサービスと入力言語」(Windowsの言語バー を右クリックして設定を選択することで開くことができます)を開き、「全般」画面で追加ボタ ンをクリックし英語(米国)などの英語入力を選択、適用して文字言語を追加します。 その後、言語バーの言語設定をJPからENに変更する事でIMEを使用しない文字入力が行えるよ うになります。

エクスプロイト対策

アプリケーション(PDFビューア、ブラウザなど)の脆弱性を突くエクスプロイト攻撃により、 あなたのPCが不正侵入を受けないように保護します。

ー般的なエクスプロイト対策としてはアプリケーションを最新の状態に更新することが非常に重要ですが、未知のエクスプロイト攻撃があった場合、更新を行っているだけでは完全に防げない可能性があります。G DATA のエクスプロイト対策機能は、そのような未知の攻撃にも対応できるプロアクティブ技術を搭載しています。

ライセンス

ワクチン更新が利用できるライセンスの有効期限を確認できます。

ウイルス対策ソフトにおいて、更新は非常に重要です。インターネット更新は必ず定期的に実行 し、製品を常に最新の状態に保つように心がけてください。本製品はお手元のライセンスの有効 期間が切れる前に、自動的にライセンス延長についてお知らせします。ライセンスの延長は、以 下の手順で簡単に手続きできます。

ライセンスの有効期間が切れた場合

ライセンス期限が切れる数日前から、タスクバーにその旨を知らせるバルーンが表示されます。 このバルーンをクリックすると、ダイアログが開くので、ダイアログの説明に従い、簡単に更新 をインターネット経由でできます。

保護する台数を増やす

使用中の製品の登録可能ユーザー数をさらに増やしたい場合は、更新時に別製品へと切り替える ことができます。この項目をクリックすると手続き用のウェブページが開きますので、そこで詳 細をご確認ください。

ソフトウェアの機能

本製品では以下の機能が利用できます(製品により使用できる機能が異なります):

 \odot

ð

セキュリティセンター: セキュリティーセンターでは、利用者がマルウェアなどの脅威 に素早く簡単に対応できるよう、コンピュータの保護に必要な情報を一目で確認できま す。

アンチウイルス: アンチウイルス機能は、お使いのコンピュータをウイルスガードによ り常時リアルタイムスキャンを行ったり、指定した方法に従ってコンピュータ全体のス キャンを行い、感染を防ぎます。スキャンにより隔離したファイルの確認や、Windows を起動せずにマルウェアをスキャンできるブートメディアの作成も、この機能から行え ます。



ファイアウォール:ファイアウォールは、外部の不正侵入からコンピュータを防御する ため防御する機能で、インターネットやネットワークとコンピュータとの間で送受信さ れるデータを監視します。許可されていないデータの書き込みやダウンロードを検知す ると、ファイアウォールが警告を発し、それらのデータ通信を阻止します。 ※この機能はG DATA インターネットセキュリティ、G DATA トータルセキュリティで 利用できます。



バックアップ: バックアップは、シンプルかつ簡単な操作で、大切な書類やデータを バックアップする機能です。日常生活は、オンライン音楽サービス、デジタルカメラや 電子メールの活用など、ますますデジタル化しており、個人的なデータのバックアップ の重要度も増しています。

ハードウェアの故障、過失によるデータ消失、あるいはウイルスやハッカーによるデー タ損害に備え、コンピュータに保存されている音楽データ、写真/動画データ、メール データなどのデータを定期的にバックアップしましょう。

※この機能はG DATA インターネットセキュリティ、G DATA トータルセキュリティで 利用できます。

※G DATA インターネットセキュリティではクラウドストレージへのファイルバック アップ機能のみ利用できます。



※この機能は G DATA トータルセキュリティで利用できます。



(A

チューナー: チューナーを使用すると、簡単な操作で OS を最適化できます。チューナ ーは Windows Update の自動確認をはじめ、定期的なデフラグ、レジストリと一時 ファイルの定期的なクリーンアップに至るまで、Windows システム内を整理し、処理 速度を向上させるツールです。

※この機能は G DATA トータルセキュリティで利用できます。

フィルタリング:フィルタリング機能は、お子様がコンピュータを使用する際などに、 ウェブサイトを一定の基準で評価判別して排除したり、コンピュータの利用時間に制限 をかける機能です。 ※この機能はG DATA インターネットセキュリティ、G DATA トータルセキュリティで 利用できます。



9

<u>アータセーフ</u>: データセーフは個人情報等の機密データを保護するための金庫のような 機能です。ハードディスクの追加パーティションのような感覚で簡単に利用できます。 ※この機能は G DATA トータルセキュリティで利用できます。



<u>オートスタートマネージャー</u>:オートスタートマネージャーは、Windowsの起動時に 自動起動するプログラムを管理する機能です。通常、それらのプログラムは OS 起動時 に読み込まれます。オートスタートマネージャーを使用すると、各プログラムごとに自 動起動のタイミングを遅らせたり、起動を防いだり、システムやハードディスクの負荷 に応じて設定を調整することができます。この調整により、OS のより高速な起動や、 パフォーマンス向上を実現する事が可能となります。



<u>デパイスコントロール</u>: デバイスコントロールは、コンピュータに接続済みのリムーバブ ルデバイス(例: USBスティック)やCD/DVDドライブやフロッピードライブの利用権 限をユーザー単位で管理できる機能です。望ましくないデータのインポート/エクスポー トやプログラムのインストールなどを防ぎ、情報漏洩やデータ詐取などの被害を未然に 防ぐことができます。 ※この機能は G DATA トータルセキュリティで利用できます。

アンチウイルス

この機能を使用して、コンピュータや記録メディアのウイルス感染が無いか、指定した方法でス キャンすることができます。例えば、友人や家族、職場の同僚から借りたUSBメモリや、CD/ DVDなどの感染チェック。インターネットからダウンロードしたソフトの感染チェックにも効 果を発揮します。

GDATA	G Data トータルプロデクション		
5	👰 🚸 🏥 🤄 🔧 😫	🍾 🔶 🕰	
-	ウイルス対策	۵ 🕲	
Q	ウイルススキャン:	塙越中のファイル: 1	
	コンピュータ内の全線紙 もしくは想ました機械をスキャン:	電器機械では、株式された構成フライルボコンとユータに発展を加え ないように、操作化した状態で安全に発展されます。 Ⅲ (単純体的な状況の)	
		ブートメディア	
		ウイルススキャンを実行できるブート可能なメディア (例: CD, USB メモリなど) を作成します。	
		ジートメディアを作成(B)	
		TRUST IN GERMAN SICHERHEIT.	

注意: コンピュータや記録メディアのウイルススキャンは追加的な保護機能です。普段は アイドリングスキャンとウイルスガードが常にバックグラウンドで動作しており、マル ウェアの脅威に対して最適な保護を維持します。G DATA 製品をインストールする前 や、ウイルスガードが無効になっていた間コンピュータにコピーされたウイルスを検出 するには、ウイルススキャンを使用してください。

ウイルススキャン

以下の項目からコンピュータやメディアのスキャンを行えます:

- コンピュータをスキャン(すべてのローカルドライブ):ウイルス感染の疑いがある場合 など、アイドリングスキャンやスケジュールスキャンとは関係なく、今すぐにコンピュ ータをスキャンする必要がある時は、ここをクリックします。クリック後は、ただちに スキャンが開始されます。ウイルススキャンの流れの項も参照してください。
- メモリとスタートアップをスキャン:実行中のすべてのプロセスに対して、プログラム ファイル および DLL(プログラムライブラリ)をスキャンします。不正プログラムが見 つかった場合は、メモリとスタートアップ領域から不正プログラムをすぐに除去しま す。このスキャンは比較的短時間で完了できるため、自動ウイルススキャンなどと一緒

に定期的に実行することをお勧めします。

この機能は、データの定期的なウイルススキャンに代わるものではなく、それを補完す るものです。

<u>.</u>.

フォルダ/ファイルをスキャン: 選択したドライブ、フォルダ、またはファイルがウイル スに感染していないか調べます。この操作をクリックすると、フォルダとファイルの一 覧が表示されます。個々のファイルにターゲットを絞ってスキャンしたり、フォルダ全 体のウイルススキャンを行うことができます。

フォルダツリーでは、「+」をクリックするとそのフォルダが展開し、フォルダの内容 がファイルビューに表示されます。ウイルススキャンは、チェックボックスにチェック が入っているフォルダまたはファイルに対して、行われます。一部スキャンされない ファイルがあるフォルダには、グレーのチェックマークが表示されます。



••

リムーバブルメディアをスキャン: CD/DVD-ROM、フロッピーディスク、メモリカード、USB メモリなどをスキャンします。この機能を選択すると、コンピュータに接続されているすべてのリムーバブルメディア(トレイに挿入済みのCD/DVD-ROM、メモリカード、または USB経由で接続中の外付けハードディスクやUSB メモリ)をスキャンします。ただし、本製品は書き込み不可のメディアに対してウイルス除去できません。スキャン結果にウイルス検出のログが作成されるだけですので、ご注意ください。

ルートキットをスキャン: ルートキットとは、従来のウイルス検出方法では検出が困難 な不正プログラムです。この機能を使うと、ハードディスク内の全データすべてをス キャンすることなく、ターゲットをルートキットに絞ってスキャンします。

隔離されたファイル

ウイルス検出時の処理方法の1つに**隔離**という処理方法があります。この操作を行うと、検出さ れたファイルが他のファイルに危害を及ぼさないように、コンピュータ上に作成された暗号化領 域に保存されます。

ます。

G mm	_	_	_	_
\$-04	ス感染ファイルは増勢化されば	職績成に保存されます。	職種されたウイルスがコンピュータに被害を考	読ることはありません
白付/時刻	ワイルス	オプジェクト	フォルダ	
2013/06/1	1 EICAR-Test-File (not a	vir eicarcom2.zip	C:#Users#test64#Desktop##fl.4137	1ルダ
	100 Lat-1-			
	ian i			
	オブジェク eloarco	m2.zip		
	場所: C:¥Use	rs¥test64¥Desktop¥新し	いフォルダ	
	ウイルス: ESCAR	Test-File (not a virus) (I	>5> A)	
		St. March 1996	million and	

隔離領域に移動したファイルは、検出された時の状態で保存されます。隔離されているファイル には次の操作が可能です。

- **更新**:隔離情報を更新します。隔離画面を開いてから時間が経過し、他にもウイルスが検 出された場合、それらが表示されます。
- 送信: 感染ファイルを G DATA に送信します。感染ファイルが新種の不正ファイルである場合は、その後のワクチン開発に活用されます。ユーザーが送信した情報は匿名情報として処理されます。詳細は、マルウェア情報イニシアチブ を参照してください。

マルウェア情報イニシアチブとは

G Data セキュリティラボでは、G DATA 製品をご利用のユーザー様を、コンピュータ の安全性を脅かす脅威からから保護するため、保護・対策の研究や分析に絶え間なく励 んでいます。マルウェア研究では、マルウェアに関する情報が多ければ多いほど、効果 的な保護メカニズムの開発をいち早く進めることができます。これらの情報をG DATA の研究・分析・開発に効率的に取り入れることを可能にするための取り組みが、G DATAマルウェア情報イニシアチブです。これにより、マルウェアに関するデータをG DATAセキュリティラボに送信することができます。より多くのユーザー様に参加頂く ことで、他のG DATA製品をご利用の方々もインターネットをより安全に利用できるよ うになります。

• **ウイルス駆除**: 感染ファイルから感染部分のみを駆除し、ファイルを元の場所に戻しま す。場合によっては、駆除はできない場合もあります。

- 元に戻す:隔離ファイルを元に戻します。この処理は例外ケースを除き利用しないでください。利用する場合は、コンピュータのネットワーク/インターネット接続を切断し、未感染データをバックアップするなどした上で、実行してください。
- 削除:感染ファイルが不要な場合は、隔離領域から削除できます。

ブートメディア

プートメディアは、Windows 起動前にスキャンを実行できるブートスキャン機能が搭載しており、本製品のインストール前からコンピュータに感染し、本製品のインストールを妨害する可能性のあるウイルスを駆除するのに役立ちます。詳細は、<u>プートスキャン</u>の項を参照してください。



ブートメディアを作成する場合は、アンチウイルス画面から**ブートメディアを作成**ボタンをクリックし、ウィザードの指示に従ってください。このウィザードでは、最新の最新のワクチンのダウンロードや、作成メディア種類(CD/DVD/USB)を選択できます。

ブートメディア ウィザード
ブートメディアウィザードを使うと、ブート可能な CD/DVD や USB の作成ができます。 すートメディアウィザードで作成したブートメディアをコンピュータにセットしてコンピ ュージを起動すると、ディモンピュータにインストールだれているOSを起動すること なく、お使いのコンピューダに不正プログラムが潜んでいないがスキャンできます。
サポートされているメディアやブートメディアの使用については、ヘルプを参照してくだ さい。
<原る(B) 次へ(N) キャンセル

復元: G DATA トータルセキュリティを使用している場合は、ブートメディアからバック アップイメージをシステムボリュームへ復元、もしくはファイルバックアップを任意の ドライブへ復元する事が可能です。復元機能を利用する場合はブートメディアをコン ピュータへ挿入し、**G DATA バックアップ(復元)**を選択してください。

ファイアウォール

ファイアウォールは、外部の不正侵入からコンピュータを防御するため防御する機能で、インタ ーネットやネットワークとコンピュータとの間で送受信されるデータを監視します。ファイア ウォールには以下の3つの領域が存在します。

- ステータス:ステータス領域では、使用中のコンピュータでの一般的なファイアウォール 動作状況を確認する事ができます。
- <u>ネットワーク</u>: ネットワーク領域では、コンピュータが接続しているネットワークが表示 されます(例: ローカルエリア接続、ワイヤレスネットワーク接続など)。
- <u>ルールセット</u>: ルールセット領域では、ネットワークごとにルールセットを作成し、ファ イアウォールの動作を最適化できます。

<u>ファイアウォールの設定</u>

画面右上に配置された (歯車ボタン)からは、ファイアウォールの細かな設定を行う 設定画面を開くことができます。

ステータス

ステータスでは、ファイアウォールの状態に関する基本情報が項目ごとに表示されます。項目を クリックしてそれぞれの操作を選択すると、機能の切り替えや、設定の編集を行えます。

GDATA		G Da	ta トータルプロ	テクション			? _ X
5		<u> </u>	3	2	6		
フ	アイアウォール	0	*	§			0 🖻
A 75	ータス						
27* 00 00 00 00 00	イアウォールの状態を表示しま (195-209-2(5)) モード(2): ネットワーク(3): 参差した改革(3): アプリケーション レーダー(4)	 (基準セキュロジー 白倉 (オートル・ すべてのネット) ジニ プロック揺去はよ 	イ (ロット) ワークが保護されて(らりません	۸ŦŦ	→ セキュリディ L ウォールのルー 定できます。	-ベルを満留することで、 ルの掲かさや、アラート	, ファイア -03度を殺

TRUST IN GERMAN SICHERHEIT.

警告マークの付いた項目の設定が最適化されると、マークは再び緑色のチェックマークに戻りま す。

- セキュリティ: ファイアウォールは、インターネットに接続したり、コンピュータに悪影響を及ぼすアプリケーションを自己学習していきます。ファイアウォールに関する知識レベルに応じてファイアウォールの設定を変えることも可能です。ユーザーへの確認の頻度を減らしつつ、セキュリティレベルの高い基礎的保護がなされるように設定することもできれば、コンピュータの使用状況に合わせた高水準の保護が得られるように詳細設定することも可能です。ただし、詳細設定を利用するには、ファイアウォールに関する高度な知識が必要です。セキュリティをクリックしてセキュリティを編集を選択すると、設定画面の設定|ファイアウォール|自動が開きます。
- モード: 作動中のファイアウォール設定を確認できます。設定は、自動(オートパイロット)と手動でルールを作成のいずれかから選択できます。

オートパイロット:ファイアウォールがアプリケーションの許可/拒否を自動判断で制 御し、コンピュータを保護します。この機能は全般的な状況に対応できるため、通常は この機能を使用することを推奨します。デフォルト設定ではオートパイロットはオンに なっています。

詳細設定: ファイアウォールをネットワーク環境に合わせて設定したい場合、あるいは 特定のアプリケーションにオートパイロットモードを適用したくない場合には、ルール を手動で作成するように設定を変更できます。この機能の詳細は 設定 | ファイアウォ ール | 自動の項を参照してください。

- ネットワーク:ファイアウォールが監視しているネットワークの状況を表示します。この 機能の詳細はファイアウォール | ネットワークの項を参照してください。
- 撃退した攻撃: コンピュータへの攻撃が検知されると、ファイアウォールはこれをブロックし、ログとして記録します。この項目をクリックし、システムメッセージを表示を選択すると、ブロックした攻撃に関する詳細な情報を見ることができます。
- アプリケーションレーダー: アプリケーションレーダーでは、ファイアウォールが起動を ブロックしているプログラムを表示できます。ブロックされたアプリケーションのうち ネットワーク使用を許可したいものがあれば、そのアプリケーションを選択して【許 可】をクリックします。

🔽 アプリケーション レーダー	×
ブロックされたアプリケーションを選択して [許可] をクリックすると、アプリケーショ ンを起動できるようになります。	
アプリケーション 理由	
ブロックされているアブリケーションはありません	
(例許可) 閉じる	

ネットワーク

ネットワークでは、コンピュータが接続しているネットワーク (LAN接続、DTN (ダイヤル アップ接続)など)の一覧、適応されている**ルールセット**、IPアドレスが表示されます。

この画面では使用されているネットワークと、それに使用されているルールセットが一覧表示されます。ネットワーク名の横にあるチェックを外すと、そのネットワークに対するファイアウォールによる保護が解除されます。※特別な理由がない限り、ファイアウォールの保護は解除しないようにしてください。

表示されている設定を確認したり、編集したりするには、対象を選択してダブルクリック(もし くは対象を選択して【**編集】**をクリック)します。



PCが接続しているすべてのネットワークの一覧です。G Data ファイアウォールはチェックマークの付いているネットワークのみ保護します。

5a)	ルールセット	サデドレス
2 上がイヤルテッジ ネットワーク	「自然」キットに素持視識	
◎ 上ローカル エリア構築	信頼性の高いマットワーク	A REAL POINT OF A REAL CONTRACTOR AND A

補柴(主)

TRUST IN GERMAN SICHERHEIT.

ネットワークの編集

ネットワーク画面で編集を選択すると、選択されたネットワークの各種情報が表示されます:

5 ネッ	トワークの編集		×
ネットワ	ワークについて		ОК
<u>.</u>	名前:	ローカル エリア接続	++2>,+21
<i>a a</i>	IPv4 アドレス:		+1720
	IPv6 アドレス:		
	サブネット マスク:		
	デフォルト ゲートウェイ:		
	優先 DNS サーバー:		
	代替 DNS サーバー:		
	WINS サーバー:		
V 20	のネットワークでファイアウ	オールを有効にする	
☑自	動設定 (DHCP) を有効にする		
ルール	レセット		
信頼	性の高いネットワーク	•	
		ルールセットを編集	

- ネットワークについて: IP アドレス、サブネットマスク、デフォルトゲートウェイ、DNS および WINS サーバーなどのネットワークに関する情報がある場合、それらを表示しま す。
- このネットワークでファイアウォールを有効にする: チェックを外すと、ネットワークに 対してファイアウォールを無効にできます。特別な理由がない限り、有効にしておいてく ださい。
- インターネット接続共有: インターネットに直接接続している場合、ネットワーク内のすべてのコンピュータに対して、インターネットアクセスの許可または禁止を設定できます。このインターネット接続共有(ICS)は通常、ホームネットワークでのみ有効にできます。
- 自動設定を有効にする(DHCP): DHCP(Dynamic Host Configuration Protocol) を使用したネットワークでは、コンピュータを接続すると動的に IP アドレスが割り当て られます。このネットワークに接続している場合は、設定を有効にしてください。
- ルールセット:信頼性の高い、信頼性の低い、またはアクセスを拒否するネットワーク といった複数のルールセットから選択し、ファイアウォールルールを素早く設定できま す。さらに【ルールセットを編集】をクリックすると、これらのルールセットを編集して 独自のルールを作ることもできます。詳細ついては、ルールセットの項を参照してください。

ルールセット

ファイアウォールの細かいルール郡から構成されているルールのまとまりをルールセットといい ます。ルールセット領域では、それぞれのネットワークに応じた固有のルールを作成できます。 作成されたルールセットは、ルールセット領域にすべて表示されます。

本製品にプリセットされているルールセットには、アクセスを拒否するネットワーク、インタ ーネットに直接接続、信頼性の低いネットワーク、信頼性の高いネットワークがあります。そ れぞれのルールセットの内容を確認や修正するには、ルールセットを選択して[編集]を押しま す。新規ルールを作成するには、[新規作成]のボタンを押し、ダイアログに沿ってルールを作 成してください。

GDATA		G Data	トータルプロ	テクション				? _ X
5	👰 🚸 🏥	¢	∢	2	6	ዋ		
	ファイアウォール	0	*	ş				0 🗈
§	ルールセット							
	東なる原則していことに専用ルールを作成し、 な市 10 70005486513-3-000-0 10 609-3-4465484 10 508-4-44554 10 508-4-4455 10 688455824-4-50-5 10 688455824-4-50-5	***	「通切に存毀しま	γ.				
					8	新統件成(因)	❀ 削除(D)	· 編集(E)

TRUST IN GERMAN SICHERHEIT.

メモ: ユーザーによって作成されたルールセットは削除できますが、本製品に前もって 設定されているルールセットは削除できません。

新規作成

ネットワークごとに異なる設定のルールセットを割り当てる事で、ファイアウォールは様々なセ キュリティレベルのネットワークに対応できます。例えば、一般的に、ホームネットワークに接 続している場合は、インターネットに直接接続している場合よりも緩めのルールで十分効果を発 揮します。

GDATA	G Data トータルプロテクション							
5	(* ¢	×	9	🍗	2		
	ファイアウォール	0	*	§		0	Ê	
§	ルールセット							
	異なる危険レベルごとに専用ルー.	ルを作成し、ネットワーク	を適切に保護しま	g.				
	名目 							
					🦉 新統作成(N)	※ 形除(D))	

TRUST IN GERMAN SICHERHEIT.

ルールセットは自分で作成する事も可能です。新規ルールを作成するには、**[新規作成]**のボタンを押してください。

▶ 新規ルールセット	×
新規ルールセット	
ルールセット名	
新規ルールセット	
◎ 空のルールセットを生成	
◎ 推奨ルールを含むルールセットを生成	
ルールセットの選択	
信頼性の低いネットワーク用のルールセット	
OK キャンセル	-

- ルールセット名: ルールセットの名前を入力します。
- **空のルールセットを生成**: 空のルールセットを作成しておいて、ルールを自身で定義して 追加します。

- 推奨ルールを含むルールセットを生成: G DATA のプリセットルールの信頼性の高い ネットワーク、信頼性の低いネットワーク、アクセスを拒否するネットワークから選択 してルールを作成します。作成されたルールセットは、必要に応じて後からカスタムでき ます。 ファイアウォールには、ネットワークの種類ごとに以下のデフォルトルールセットが用意 されています:
- インターネットに直接接続:インターネットに直接接続している環境用のルールセットです。
- 信頼性の低いネットワーク: ダイヤルアップネットワークやその他のインターネット接続 するオープンネットワーク用のルールセットです。
- 信頼性の高いネットワーク:ホームネットワークや企業ネットワークなどの信頼できる ネットワーク用のルールセットです。
- アクセスを拒否するネットワーク:あるネットワークへの接続を一時的または常時ブロックするためのルールセットです。この設定は、セキュリティのレベルが不明なネットワーク(例:他社の企業ネットワーク、公共ネットワークなど)に接続する時に適用してください。

新規作成されたルールセットは、ルールセット領域に表示されます。作成したルールセットを変 更するには、そのルールセットを選択して【編集】を押してください。設定|ファイアウォー ル|その他のデフォルトで使用するウィザードの種類で定義されている方法でルールセットを を編集できます。

> 新規ルールの作成方法は、<mark>ルールウィザード</mark> もしくは <u>拡張ルールセットエディタ</u> の 項を参照してください。

オートパイロットを使用していない場合、新規ルールをポップアップで表示されるア ラートからも作成できます。詳細は ファイアウォールアラート の項を参照してくだ さい。

ルールウィザード

ルールウィザードは、既存のルールセットに特定のルールを追加したり、既存のルールを編集する際に、ユーザーをサポートするウィザード形式の設定アシスタントです。ファイアウォール上 級者以外は、**拡張ルールセットエディタ**よりも**ルールウィザード**を利用することをお勧めしま す。

> ルールウィザードを使用すると、選択したルールセットに含まれるルールを簡単に編 集できます。

> ネットワークごとに適用したルールセットの種類によって、アプリケーションは遮断 されたり、許可されたりします。例えば、ホームネットワークでネットワーク接続を 許可する一方で、ダイヤルアップ接続では拒否するといった設定も可能です。

§	ルールウィザードは、ファイアウォールのルール将成をサポートします。
ta.	
-00	アプリケーションのネットワークアクセスを利用してください。(A)
	ネットワークサービスを許可/拒否
-	特定ネットワークサービスとアプリケーションへのアクセスを制限してください。(別)
12	ファイルおよびプリンタ共有を許可/拒否
40.00	ネットワーク共有とプリンタへのアクセスを影響してください。(ビ)
E.	ドメインサービスを許可/拒否
-	ネットワーク ドメインへのアクセスの許可/拒否を設定してください。(2)
Q.	インターネット接続共有を許可/拒否
	インターネットへの共有アクセスを制飾してください。(1)
	VPN サービスを許可/拒否
-	VPN サービスへのアクセスの評可/拒否を設定してください。(V)
	拡張ルールセットエディタ (エキスパートモード)
3	詳細なルールの作成、編集ができます。(E)
	進用 キャンセル

ルールウィザードでは次の基礎ルールを選択できます:

アプリケーションを許可/拒否: インストールされているアプリケーションを選択し、ルールセットで指定したネットワークへのアクセスを許可/拒否します。目的のアプリケーションのある場所を示す文字列(パス)を選択して、接続の方向でそのプログラムにインバウンド接続(着信接続)、アウトバウンド接続(発信接続)のどちらを許可するか、あるいはイン/アウトバウンド接続の両方を許可するかどうかを設定します。例えば、音楽再生ソフトの場合では、次のような利用ができます。

アウトバウンド接続を拒否して、ユーザーの音楽嗜好データを自動送信するのを防止 インバウンド接続を拒否して、プログラムの自動更新を遮断

- ・ネットワークサービスを許可/拒否:ポートとは、外部とデータを入出力するため、アプリケーションによって使用されるネットワークアドレスの一部です。例えば、ウェブページの閲覧ではポート80、メール送信にはポート25、メールの受信にはポート110が割り当てられています。ファイアウォールを使用しない場合には、すべてのポートが開放状態になっているので、外部の第三者から攻撃を仕掛けられる可能性があります。ルールウィザードを使用すると、特定のアプリケーションに必要なポートのみ許可し、その他のポートは遮断します。
- ファイルおよびプリンタ共有を許可/拒否: 主にNetBIOSに関する設定です。NetBIOSとはLANでネットワークを利用する際の通信規約で、TCP/IP プロトコルなどを使用せずに、コンピュータ間で直接ファイルやプリンタを共有するのに利用されています。これは、一般的なホームネットワークではほぼ不要ですが、ハッカーが NetBIOS を使ってコンピュータを攻撃する可能性もあるので、信頼性の低いネットワークに対しては共有を拒否してください。
- ドメインサービスを許可/拒否:ドメインはあるネットワーク内にあるコンピュータを整理して一覧できるようにするためのもので、ネットワークに接続しているコンピュータを1か

所で管理できるように割り当てられています。ドメインサービスを許可(もしくは拒否) します。信頼できないネットワークでのドメインサービスの共有は拒否してください。

- インターネット接続共有を許可/拒否: インターネットに直接接続している場合、ネットワーク内のすべてのコンピュータに対して、インターネットアクセスの許可または禁止を設定します。このインターネット接続共有(ICS)は通常、ホームネットワークでのみ有効にするものです。
- VPNサービスを許可/拒否: VPNはVirtual Private Networkの略で、別ネットワークにあるコンピュータ同士を接続し、あたかも直接接続しているかのように動作させることのできる技術です。VPN接続を利用している場合は、この設定を許可する必要があります。
- 拡張ルールセットエディタへ切換え(エキスパートモード):ファイアウォールのルール ウィザード(ルールセットの作成モード)から拡張ルールセットエディタへ切換えます。

拡張ルールセットエディタ

ネットワークセキュリティに関してある程度の知識があるユーザーは、拡張ルールセットエディ タを使ってルールセットを更に詳細に設定できます。このエディタでは、ルールウィザードでは 難しい高度な設定が可能です。

ラル-	ールセット						×
名前 信頼性 ルールに	の高いネットワーク ないアクセスが検知された場合の処	理方法] ステルス モード	<u> 1291</u>		開じる
8 <u>8</u> 2-	サーに確認		- V	アダプティブ モード			
ルール							
名前		∋	アクセス	接続の方向	コメント	^	ルール
7	MpCmdRun.exe	1	許可	アウトバウ	オートパイロ		新規作成
7	POWERPNT.EXE	2	許可	アウトバウ	オートパイロ	=	續集
1	sftlist.exe	3	許可	アウトバウ	オートパイロ		- monte
7	X16-57071_2M2JX-CVT3	4	許可	アウトバウ	オートパイロ		削除
7	Remotedesktop	5	許可	アウトバウ	デフォルト ル		
1	Sidebar	6	許可	アウトバウ	デフォルト ル		7-7-1
7	Media Player	7	許可	アウトバウ	デフォルト ル		表示
7	Media Player Setup	8	許可	アウトバウ	デフォルト ル		雨46
7	Media Center	9	許可	アウトバウ	Windows Me		,C.#/1
7	IE RSS Feed	10	許可	アウトバウ	デフォルト ル		=`.h
7 🚺	Internet Explorer	11	許可	アウトバウ	デフォルト ル		
7	Windows Problem Repor	12	許可	アウトバウ	デフォルト ル		$ \langle \rangle \rangle$
7	Windows Reability Analy	13	許可	アウトバウ	デフォルト ル	-	

拡張ルールセットエディタでは次の設定ができます:

- 名前: 選択したルールセットの名前を変更できます。ルールセットはこの名前でルール セット領域に表示され、ファイアウォールが識別したネットワークに結び付けられます。
- **ステルスモード**: ステルスモードを使用すると、コンピュータで使用しているポートの確認に対して応答せず、ハッカーなどがシステム情報を取得するのを困難にします。
- ルールにないアクセスが検知された場合の操作: ネットワークのアクセスをすべて許可/

拒否するか、あるいはユーザーへの確認で決めるかを設定できます。ファイアウォールの 学習機能で個々のアプリケーションに専用ルールを設定している場合は、そのルールが適 用されます。

・アダプティブモード:フィードバックチャネル技術を使用するアプリケーション(FTPや 各種オンラインゲームなど)をサポートします。この種のアプリケーションはリモートコ ンピュータに一旦接続し、その後、リモートコンピュータがユーザーのアプリケーション に逆接続するフィードバックチャネルを確保します。アダプティブモードを有効にしてお くと、ファイアウォールがこのフィードバックチャネルを検出し、確認を求めることなく 接続を許可します。

ルール

ルール領域には、ルールセットに含まれるに細かなルールが登録されています。

ルールセットは以下の3種類の方式で作成されます。

- <u>ルールウィザード</u>
- <u>拡張ルールセットエディタ</u> (エディタ内の**新規作成**ボタンを押して新しいルールを作成 できます)
- <u>アラート</u>(アラートダイアログ経由でルールが作成された場合は、エディタ内のコメント 欄に「アラートにより作成」と表記されます)

これらの方法で作成されたルールセットには、それぞれ独自のルールが含まれています。

ファイアウォールルールは、一部が階層構造でまとめられているため、場合によってはルールの **ランク順**に注意する必要があります。例えば、ポートを開放しているにもかかわらず、そのポー トを利用しているアプリケーションが遮断される可能性があります。このような場合は、ルール のランク順を変更するとアクセスが許可されるようになります。ランク順を変更するには、目的 のルールをマウスで選択して **ランク**の欄の矢印ボタンでリストの上位または下位へ移動してくだ さい。

名前 新しいルール		変育効なルール	OK
4486			4420
編織の方向		アクセス	
the second se	22.4VP	4626	
	₩ ₩ •	◎ 拒益	•
ТСР -	我校 ・ アプリケーション	◎ 拒否 は、 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	● サービス制造て
■ プロトコル TCP ・	まだ ・	◆ #書 #2番目で インターネット 校7 22:59:59 日	サービス制造で

拡張ルールセットエディタで**[新規作成]**から新規ルールを作成したり、**[編集]**ボタンから 既存ルールを変更すると、**ルールを編集**ダイアログが表示されます。

このダイアログでは、以下の項目を設定できます:

- **名前**: デフォルトルールおよび自動的に作成されたルールの場合、アプリケーション名が 入ります。名前は自由に変更できます。
- **有効なルール**: ルールの有効/無効を切り替えます。ルールを無効にするには、チェック を外します。ルール自体の削除はされせん。
- コメント: ルールを作成した方法が表示されます。ルールセットに対するデフォルトルールにはデフォルトルール、アラートから作成したルールにはアラートにより作成と自動的に入力され、ユーザーが詳細設定ダイアログで作成したルールの場合にはユーザーが自分でコメントを入力できます。
- 接続の方向: ルールをインバウンド接続(着信接続)とアウトバウンド接続(発信接続)のどちらに適用するかを指定します。
- アクセス: ルールセットに関連するプログラムに対してアクセスを許可するかどうかを設定します。
- プロトコル: アクセスを許可または禁止する接続プロトコル を選択できます。このとき、 プロトコルを原則として停止または許可する、またはプロトコルの使用を1つのアプリケ ーションまたは複数のアプリケーションと組み合わせる(アプリケーション割当て)こ とができます。同様に、許可するポートとブロックするポートを【インターネットサービ ス割当て】から厳密に定義できます。
- 時間: ネットワークリソースへのアクセス時間を設定できます。例えば、アクセス許可を 業務時間内に限定して、それ以外の時間はアクセスできないように設定できます。
- IP アドレス範囲: 固定 IP アドレスを持ったネットワークでは、IP アドレス範囲を限定し
て使用方法も可能です。IP アドレス範囲を厳密に定義すれば、ハッカーから攻撃を受ける 危険性を大幅に低減できます。

バックアップ

G DATA バックアップは、シンプルかつ簡単な操作で、大切な書類やデータを保護できます。ハードウェアの故障、過失によるデータ消失、あるいはウイルスやハッカーによるデータ損害に備え、コンピュータに保存されている音楽データ、写真/動画データ、メールデータなどのデータを定期的にバックアップしましょう。

バックアップと復元

バックアップジョブは**新規ジョブ**ボタンから作成できます。作成されたジョブは以下の項目から 編集や操作を行えます:



復元: 保存したバックアップからファイルを復元できます。詳しい手順は<u>復元</u>を参照し てください。

 パックアップ:手動バックアップを開始したり、スケジュールを無視してバックアップを 実行できます。

設定: <u>新規ジョブ</u>で作成したバックアップジョブの詳細設定を確認したり、編集できま す。

ログ:バックアップ、管理および復元プロセスのログを閲覧できます。 このログには、手動またはスケジュールバックアップジョブ、復元に関する情報の記録。場合によってはエラーメッセージ(例:バックアップが実行されているため、保存先に十分な空き容量が無かった場合など)が記録されます。

Ś

Ö

新規ジョブ G+ **新規ジョブ**ボタンから新しいバックアップジョブを作成できます。

😈 バックアッフ	での練頭	\times
まず作成するバッ	クアップの種様を盛んでください。	
¢	© ファイルバックアップ 痛欲したファイル(フォルダをバックアップ	
¢	④ イメージ バックアップ パードディスクまたはパーディション全体をバックアップ	
	ок <i>+</i> т>tz	14

ファイル/ハードディスク/パーティションの選択 バックアップジョブの作成では、まず実行するバックアップの種類を選択を行います。

C ファイル バックアップ: ユーザーが指定した特定のファイルやフォルダをアーカイブ ファイルにバックアップします。

K +5 ク >7 3→3 0 4 2 D 7+ A -04英 B (新元の曲代 B (不分25=-/k B (オプ25=2) B (オプ2=2)	■ ■ ■ ■ ■ ■ ■ ■ ■ □ ■ □ □ □ □ □ □ □	ファイル名 □ ぱつつビーデイ □ 品ローカルティス □ cabedopti (00) □ cabedopti (01) □ cabedopti (12) □ cabedopt	9 42	使効 フロッピーチー、 ローカルディー ローカルディー ローカルディー ローカルディー ロトライブ ローカルディー	
					,

まず、ファイルの選択画面で、バックアップしたいフォルダやファイルを選択します。 通常、ファイルバックアップでは自分用のファイルをバックアップする事をお勧めしま す。インストールされたプログラムのバックアップとしての使用はお勧めしません。 フォルダツリーの各アイコンの横にある「+」をクリックするとそのフォルダが展開 し、フォルダの内容が右側のファイルビューに表示されます。チェックを入れたフォル ダやファイルは、すべてバックアップの対象になります。選択されていないファイルが 含まれているフォルダは、グレーのチェックマークで表示されます。



イメージ バックアップ: ハードディスクやパーティションのデータをアーカイブファイ ルに完全にバックアップします。

👽 バックアップ ジョブの識	走 八一ドディスク/バーティションの迎訳	×
代9クアップ ジョブの起流 ▶ パードディスタ/パーティシ =>0確訳 ▶ 終わら道訳 ▶ スタシニール ▶ スタシニール ▶ スクシュン	B: Un-France 2770005 I: I: I:	
	QK #ャンセ	r.

※インターネットセキュリティではファイルバックアップのみ使用できます。

保存先の選択

バックアップの保存先を指定します。G DATA のバックアップでは、CD/DVD ドライブやリム ーバブルメディアの他、オンラインストレージサービス(DropboxやGoogle ドライブ)へも バックアップできます。 ※インターネットセキュリティではオンラインストレージサービス上へ の保存のみ使用できます。

😈 バックアップ ジョフ	「の論定 保存先の選択			×
 バックアップ ショブの設定 > ファイルの温保 タイルの温保 タイルの温保 スクジュール スクジュール オプション 	⇒■ デスクトップ ○ ポ コンピュー ※ 色 D ーが ※ D ーが ※ D ーが ※ 受 date ※ 受 date ※ 受 date ※ 受 date ※ マトンー	9− 1.∓< 7.9 (C.) 1.9 < 7.0 (E) WitherverLighta.de) (S.) WitherverLighta.de) (T.) 2		
	図オンライン ストレー	ジサービス上に保存	-	
	ジアーカイブを FTP 5	ナーバーにコピーする		新しいフォルダ
	アーカイブ名:	ファイル バックアップ_1	ê tit 5년~	ネットワーク ログイン データ
				OK キャンセル

オンライン ストレージ サービス上に保存: Dropbox や Google ドライブにアーカイブを保存 します。バックアップ先として利用するサービスを選択してください。オンラインストレージサ ービス上に初めてバックアップする場合は、まずG DATA バックアップとクラウドサービスの認 証を行う必要があります。オンライン ストレージ サービス上に保存新規アカウントにチェッ クが入っている事を確認し、利用するサービスを選択してから**雲のアイコン** ▲を押します。プ ルダウン表示で新規アカウントが表示されるので、これを選択し、利用するサービスを選択し ます。ポップアップメッセージが表示されるので、 [OK] を押します。G DATA のブラウザが 開き、アカウント情報を入力すると、G DATA バックアップとの認証が行われます。これで、ク ラウド上にバックアップを作成する準備が整いました。

メモ: オンライン ストレージ サービスのアカウントをお持ちでない場合、Dropbox の アカウントはG DATA のブラウザ経由で簡単に新規作成できます。G DATA のブラウザ 上で Dropbox の新規ユーザーです。アカウントを作成 を選択してください。Google ドライブを利用したい場合、別途 Google のアカウントを新規作成してください。

メモ: バックアップをクラウドストレージ上に保存する場合、パスワードを掛けて暗号化 することをお勧めします。暗号化は、バックアップジョブ設定のオプション から設定 できます。

アーカイブ名: 作成するアーカイブファイルに名前を付けることができます。例: 毎週のバック アップ、MP3バックアップ など。

新しいフォルダ: バックアップ先として新しいフォルダを作成したい場合は、**新しいフォルダ**ボ タンをクリックすると、選択したフォルダ内にフォルダが作成されます。

注意: オリジナルデータが保存されているハードディスク上にバックアップを保存する と、ハードディスクに問題が発生した場合、オリジナルデータとバックアップデータの 両方が消失してしまいます。バックアップは、オリジナルデータが保存されているハー ドディスク上に保存せず、オリジナルデータの保存場所以外の外付けハードディスクへ の保存、またはCD/DVDに書き込むことをお勧めします。

スケジュール

スケジュール画面では、バックアップを特定の日時に定期的に自動実行するように設定できま す。指定できるバックアップの種類には、選択された全てのデータをバックアップする**フルバッ クアップ**、過去のバックアップからの変更点のみをバックアップする**部分バックアップ**、という オプションがあります。

フルバックアップの実行

フルバックアップの実行頻度(**手動、1回のみ、毎日、毎週、毎月、曜日、時間**)を設定できます。ここで指定した頻度で、ファイル/ハードディスク/パーティションの選択画面で選んだ全てのファイルがバックアップされます。

手動を選択した場合は、バックアップは自動実行されません。実行するためにはバックアップの 画面上から、バックアップボタンをクリックする必要があります。**毎日**を選択した場合は、一日 おきに行う、週末だけ行う、といったように、曜日を指定して自動実行できます。この他にも毎 週、毎月実行させることも可能です。

バッテリーモードでは実行しない: バックアッププロセスがノートPCのバッテリー不足で意図 せず終了することを防ぎます。このオプションが有効な場合、ノートPCが電源に接続されてい る状態でのみバックアップが実行されます。



注意: スケジュール設定された自動バックアップでは、CD/DVD-ROM にはバックアッ プを保存できません。

古いアーカイブを削除では、フルバックアップを実行する際に、既存のフルバックアップデータの取扱いについて設定します。(拡張子 ARC で保存されるファイルがバックアップによって作成されるファイルです)

デフォルト設定で選択されているフルバックアップ後に自動的に削除では、保存するフルバック アップの数を定義します。例えば、データの破損に備えて、フルバックアップを2回分保存して おきたい時は、__**回までフルバックアップを保存**に2と入力します。3回目のフルバックアップ が実行された場合は、1回目のバックアップデータは削除されます。

削除しないを選択した場合は、既存バックアップデータは削除されずにそのまま保存領域に保存 され続けます。この設定は、バックアップをとった直後に何らかの理由でアーカイブが破損した 場合、前回保存したアーカイブを利用できるメリットがあります。一方で、保存するアーカイブ が増えればデータ容量がコンピュータ内の保存領域を圧迫して、コンピュータのパフォーマンス に悪影響を及ぼす可能性もありますので、バックアップアーカイブは貯めすぎないように注意し てください。

部分バックアップの作成にチェックを入れると、部分バックアップが実行されバックアップに掛かる時間を大幅に短縮できます。部分バックアップはすべてのデータをバックアップする代わり に、既存のフルバックアップをもとに、前回のフルバックアップ以降に変更されたデータだけを バックアップします。

ただし、バックアップを復元する際は時間がかかります。また、この方式ではフルバックアップ のファイルが削除されないため、バックアップにより大きな空き容量が必要となります。その場 合でも、次にフルバックアップを実行すればフルバックアップと部分バックアップの内容が同期 され、一つのフルバックアップのファイルとなります。

差分 / 増分: 差分では、常に前回のフルバックアップ時点からの変更点をすべてバックアップします。フルバックアップに比べ、バックアップの所要時間やディスク容量の面で効率的なバック アップ方法です。増分では、前回の部分バックアップからの変更点をすべてバックアップするの で、バックアップの所要時間が差分バックアップより早くなります。但し、バックアップを復元 する際は、フルバックアップとフルバックアップ移行のすべての部分バックアップが必要とな り、差分で復元する場合に比べ、復元に時間が掛かります。

部分バックアップの実行

部分バックアップの実行頻度(手動、1回のみ、毎日)を設定できます。

オプション

オプション領域では、バックアップの一般的なオプションを変更できます。G DATA のデフォル ト設定は幅広い状況を想定していますので、ほとんどの場合ここで設定を変更する必要はありま せん。

ファイルの遊祝	11 アーカイブのファイルサイズを制度 650 MB *	o Tringt
様がたの単図 > スがジュール → オプション	マルチセッション CD/DVO の作成 マーカイブを始発 空 一切イブを参称とつイルススキャンを現在 アーカイブを参称と アーカイブを考れ 国 二カイブを考れ 国 二カイブを考れ 国 二カイブを考れ 国 二カイブを考れ 国 二カイブを考れ 国 二カーカイブを考れ 国 二カイブを考れ 国 二カイジを考れ 国 二カイブを考れた 国 二カナイルの表表しまえ出をチェック 一売フナイルの表表しまえルグ 二 Windows ポリュームシャドウコビーを使用する 高心をファイルの義慧	 ○ 和三田平 ○ 中臣婦童 ● 常熟地理(正確なし) ○ 中古フォルダ ○ インラーネットー費フォルダ ○ Thurits.db ○ 中古ファイル(ファイルの間性) ② システム ファイル(ファイルの間性) 豚外下るファイルあれ(コットルの間性)
	ユーザー情感	

一般的なアーカイブオプション

ここでは以下の設定を利用できます。

※インターネットセキュリティでは使用できる機能が制限されます。灰色で表示された選択でき ない項目は使用できません。

- アーカイブのファイルサイズを制限:アーカイブを CD/DVD または他の書き込み可能な メディアに保存する場合には、バックアップでアーカイブファイルのサイズを制限することが重要です。この機能で、アーカイブデータを CD、DVD または Blu-ray ディスクに 保存するデフォルトサイズを選択できます。アーカイブがここで指定した最大サイズに達 するとアーカイブが分割され、バックアップ情報が複数のアーカイブファイルに配分され ます。
- マルチセッション CD/DVD の作成: 追記可能な方式でCD/DVDを作成します。このオプションを選択して書き込みを行っても古いデータは削除されず、新しいデータが追記されます。
- 一時的なアーカイブを削除: バックアップ作成時に自動的に作成された一時アーカイブを 削除します。バックアップの実行回数が増えるに従って、一時アーカイブの領域は増えま す。一度利用した一時アーカイブは不要になるため、通常、このオプションは有効にして おいてください。
- 復元プログラムのコピー: バックアップデータ保存先にアーカイブデータの他に、G DATA バックアップをインストールしていなくても、バックアップデータを復元できるようにバックアッププログラムを一緒にコピーします。この機能を利用するには、バック アップ先の CD/DVD-ROM から次のプログラム(AVKBackup または AVKBackup. exe)を起動してください。

復元プログラムは CD/DVD-ROM ヘバックアップする場合のみコピーされます。USB メモリや外付けハードディスクなどにはコピーされません。

バックアップデータを復元するコンピュータに本製品がインストールされている場合、復元プログラムを CD/DVD-ROM から実行するのではなく <u>アーカイブのインポ</u> <u>ート</u>機能から実行してください。

- アーカイブする前にウイルススキャンを実行:データがバックアップアーカイブに保存される前にウイルススキャンを実行します。
- アーカイブを作成後にチェック:アーカイブ作成後にバックアップデータの完全性を チェックします。
- アーカイブを暗号化: アーカイブファイルにパスワードを掛けて保護します。パスワード 保護すると、データ復元の際にパスワードが必要になります。パスワードは忘れないよう にメモして安全な場所に保管してください。
 ※パスワードがない場合は、アーカイブデータは復元できなくなります。
- 差分バックアップ時にデータを検証: 部分バックアップの作成後にデータの完全性を チェックします。
- ハードディスク復元時に完全性をチェック:復元後に、復元されたデータの完全性を チェックします。

- 一時ファイル用フォルダ: この一時ファイルは、バックアップ機能が一時的にコンピュー タの保存領域内に書き込むデータのことです。ハードディスクの空き容量が不足している 場合には、ここでバックアップ用一時ファイルの保存先を変更できます。
- ボリュームシャドウコピーを使用: この機能が無効になっていると、OSが稼働している間 は、システムパーティションのイメージは作成されません。

ユーザー情報

設定したスケジュールでバックアップを自動実行するには、ジョブ実行ユーザーにチェックを入 れ、[...] をクリックすると表示される画面で、Windows ユーザーアカウントのログインデー タ (ユーザー名、パスワード、ドメイン/コンピュータ名)を入力します。このログインデータ は、ユーザー本人が実際にログインしないで、プログラムが設定時間にバックアップを実行する ために必要です。

圧縮

圧縮領域では、アーカイブの圧縮率を設定できます。

- **高圧縮率**: データを高圧縮率で圧縮します。高圧縮でバックアップすると、バックアップ 容量を小さくできますが、バックアップ処理に時間がかかります。
- **中圧縮率**: データを中圧縮率で圧縮します。バックアップは通常の処理速度で処理されます。
- **高速処理(圧縮なし)**: データは圧縮されませんが、バックアップの処理時間は短くなり ます。

除外するファイル

ファイルのバックアップは、ファイル形式をもとにバックアップしますが、バックアップする必要のない領域に、バックアップ対象のファイル形式があります(例:ウェブページの表示速度を向上させるために一時的に保存されたファイルなど)。バックアップがこれらのファイルを一緒に圧縮しないように、特定のファイルやファイル形式を除外できます。

- 一時フォルダ:一時フォルダとそのサブフォルダに含まれるファイルをバックアップしません。
- インターネットー時フォルダ: ウェブページのキャッシュ保存用フォルダとそのサブフォ ルダに含まれるファイルをバックアップしません。

- Thumbs.db: Windows Explorer が自動的に作成したファイル「Thumbs.db」をバック アップしません。Thumbs.db は、スライドショーのサムネールを管理するために使わ れ、オリジナル画像から自動的に生成されます。
- **一時ファイル(ファイルの属性)**:システムによって**一時ファイル**属性を付けられたファ イルをバックアップしません。
- システムファイル(ファイルの属性):システムによってシステムファイル属性を付けられたファイルをバックアップしません。
- 除外するファイル形式: バックアップから除外する拡張子を入力できます。設定するには、ファイル形式の欄に拡張子もしくはファイル名を入力し、【追加】をクリックします(例:*.txt)。除外するすべてのファイル形式やを上述の手順で設定してください。なお、アスタリスク(*)と疑問符(?)は、ワイルドカードとして利用できます。

ワイルドカードの機能は次のとおりです。

- 疑問符(?):任意の1文字に代わるワイルドカード
- アスタリスク(*): 文字列全体に代わるワイルドカード

例えば、拡張子が「**.exe**」のファイルをすべてスキャンするには、「***.exe**」と入力 します。また、「**xlr**」と「**xls**」 などの複数のスプレッドシート形式のファイル をス キャンするには、「***.xl?**」と入力します。また、ファイル名の始まりが同一で形式の 異なるファイルをスキャンするには、「**text*.***」のように入力します。

バックアップジョブ用デフォルト設定にリセット

オプションをデフォルト設定に戻します。誤った設定をうっかり選択し、訂正方法がわからなく なった場合には、【バックアップジョブ用デフォルト設定にリセット】をクリックしてくださ い。



復元では、バックアップされたファイルを復元する事ができます。実行するには**復元**ボ タンをクリックしてください。

ダイアログが開き、保存されたバックアップファイルが表示されます。

(W7FWJEIR	バックアップ	ファイル教	94%	
013年6月11日 15:41	ファイノルペタ	3	16.57 MB	
013年6月11日 15:33	ファイルバッ	3	16.57 MB	

復元したいバックアップファイル(例:アクシデントが起きる直前に取ったバックアップファイル)を選択し、**復元**ボタンをクリックします。

(ックアップ日時	バックアップ・・・	ファイル数	サイズ	
1013年6月11日 15:41	ファイルバッ	3	16.57 MB	
1013年6月11日 15:33	ファイルバッ・・・	3	16.57 MB	

以下の中から復元方法を選択します。

• アーカイブの全ファイルを復元: 選択したバックアップファイルに含まれるすべてのファ

イルが復元されます。

 アーカイブの選択したファイルのみ復元:特定ファイルのみ復元したい場合には、ここを クリックして復元したいフォルダやファイルを選択します。フォルダツリーの各アイコン の横にある「+」をクリックするとそのフォルダが展開し、フォルダの内容が右側のファ イルビューに表示されます。チェックを入れたフォルダやファイルは、すべてバックアッ プの対象になります。選択されていないファイルが含まれているフォルダは、グレーの チェックマークで表示されます。

🌀 ファイルの選択				×
◎ ア~カイブの金ファイルを廃元				
● アーカイブの遅択したファイルのみ寝光				
 ○ ● Ard、ファイルバックアップ、2012.06_111_15_41_34 ○ ○ ← C: ▲ ○ ○ ● ○ ○ ■ ○<th> ファイル& ✓ ▲ Kalimba.mp3 ▲ Maid with the Fl ▲ Sleep Avey.mp3 </th><th>サイズ 8218 KB 4016 KB 4730 KB</th><th>産族 MPI 形式サラ MPI 形式サラ MPI 形式サラ</th><th>変更日 2009/C 2009/C 2009/C</th>	 ファイル& ✓ ▲ Kalimba.mp3 ▲ Maid with the Fl ▲ Sleep Avey.mp3 	サイズ 8218 KB 4016 KB 4730 KB	産族 MPI 形式サラ MPI 形式サラ MPI 形式サラ	変更日 2009/C 2009/C 2009/C
x[] x	e [etti		
	< 興高(B) (N) >	. ;	57 47 2	セル

最後に、ファイルを元のフォルダに復元するかどうかを選択します。別の場所へ復元したい場合 は、フォルダを選択するか、新しいフォルダボタンでフォルダを作成してください。パスワード (暗号化)をかけてバックアップを行った場合はパスワードの入力も必要です。

G DATA USER MANUAL

12633030969933555998	6		新法27434基	
回 👹 デスクトップ				
8 🧶 3>82-9-				
è 🚽 20 y 2−	- ディスク ドライブ (A:)			
💮 🏯 🖾 …カル 🕈	ディスク (C:)			ŧ
H to backup01	(D:)			
D 👝 beckup02	(E:)			
B tackupus	(F) # - 7 # (D)			
8-94 ネットワーク	74 X7 (9)			~
ロファイル後光病にかくルス2	2年42を実行			
スワード				
統存2元4元への上書を―				
网络定主要 者				
※登美市地のお上書	12			
※登美芝時のみ上書 ※アーカイブの更新日時	特許新しい場合のあ上書を			
※ 容量定定時のき上者 ※ アーカイブの更新日時 ※ 更新日時が変更され	∲を 物解しい場合のみ上書き 応増合のみ上書き			
 日登えてありのき上書 アーカイクの連結日時 更新日時が変更され 	#2 新新しい協会なみ上書き た場合のみ上書き			
言 容量定意時のき上書 言 アーカイクの更新日時 言 更新日時が変更され 二 更新日時が変更され	#2 約時にい場合のみ上書き 之場合のみ上書き			
※日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日	#2 約4時にい場合のみ上書き 定場合のみ上書き			
 留意文度時の当上者 アーカイクの運転日時 更新日時が変更され 	#2 初新しい協会のみ上書き 定場合のみ上書き			
 	#2 新新しい場合のみ上書き た場合のみ上書き			
■ 容量支援時の市上者 ■ アーカインの運転日時 ■ 運転日時が変更おい	43 初新して場合のみ上書き 之場合のみ上書き			
■営業実践時のも上書 ■ アーカインの運転日時 ■ 更新日時が実定され	#2 新新にい場合のみ上書き 定場合のみ上書き			
■ 容量変更ものも上当 ■ アーカイクの運転日時 ■ 運転日時が変更され	42 日本時日に増加めたまま と増合のみ上書き			
■ 容差式数478±48 ■ アーカインの運転日時 ■ 更新日時が変更され	42 日本時には強迫のあた書き 上時合のみ上書き			
■ 全容式だから上述 ■ アーカインの運転日時 ■ 東市日時が変更ない	42 日本時には強いのあた書き 上時合のみ上書き			

バックアップしたファイルを元の場所に復元する場合は、保存先に存在するファイルを以下の方 法で処理します。

- 常に上書き: 既存ファイルはアーカイブ内のファイルで置き換えられます。バックアップ されたデータが既存のファイルよりも重要な場合などに有効な設定です。
- 容量変更時のみ: 既存ファイルが変更されている場合にのみ上書きします。ファイルサイズが変わっていないファイルは上書きされません。また、この設定では復元速度も向上します。
- アーカイブの更新日時が新しい場合のみ: 元フォルダのファイルがアーカイブのファイル よりも新しい場合には、元フォルダのファイルをアーカイブデータで上書きします。また、この設定では復元速度も向上します。
- 更新日時が変更された場合のみ: 元フォルダ内のファイルの変更日時がアーカイブファイルの変更日時と異なる場合に、元フォルダ内のデータを上書きします。

[完了]をクリックすると、データが指定した場所に復元されます。

操作

操作領域では、バックアップデータの管理とメンテナンスを行います。

	らファイルを懐 ックアップ ァイルバッ アイルバッ	光します。 ファイル教 3 3	サイズ 16.57 MB 15.57 MB
バックアップ日時 バ 2013年6月11日 15:41 フ 2013年6月11日 15:33 フ	ックアップ ァイルバッ ァイルバッ	ファイル数 3 3	サイズ 16.57 MB 16.57 MB
2013年6月11日 15:41 2 2013年6月11日 15:53 7	ァイルバッ アイルバッ	3 3	16.57 MB 16.57 MB
2013年6月11日 15:33 フ	アイルバツー	3	16.57 MB
			模元

以下のオプションを使用できます。 ※インターネットセキュリティでは、アーカイブのインポート機能以外は使用できません。

CD/DVD へのアーカイブ書き込み

バックアップデータは、CDやDVDに保存することもできます。ダイアログに表示されたバック アッププロジェクトの中からディスクに書き込むデータを選択して、 [次へ] をクリックしま す。次に、バックアップデータの書き込みを実行するドライブを選択します。 ※インターネッ トセキュリティでは本機能は使用できません。

アーカイブ名	ファイル	メデニーサイズ		
Arch 77476/00707 1 201-	DING DATAN	 1		5.57 MB
Wch_ファイルバックアップ_2013	DING DATAK	 1	199-199-199-1	16.57 MB
4ch_ファイルバックアップ_2013	DING DATAN	1		16.57 MB

次に、どのドライブでバックアップデータを書き込むかを選択します。

G:# HL-DT-ST DVDRAM GS	A-H42N		 *	
送菜	11 1 12	>後にデータを検証		
•	復元プロ	ログラムのコピー		
マルチセッション	[] tost	コンの緒子		
ドライブ内のメディア:				
メディアが薄入されていません				
遗行状况 0 %				
●行状党 0 % パッファ 0 %				
連行状態 0 % バップナ 0 %				

ここでは以下のオプションを選択できます。

書き込み後にデータを検証:書き込み終了後にデータを検証します。この設定を有効にすると、検証を省略した書き込みよりも時間が掛かりますが、通常はこの設定を有効にしておくことをお勧めします。

復元プログラムのコピー: G DATA のバックアッププログラムがインストールされていない環境でも、バックアップデータを復元できるように、バックアップの保存先にプログラムをコピーします。
 データを復元するには、CD/DVDから次のプログラム (AVKBackup またはAVKBackup.exe)を起動します。

[書き込み] ボタンをクリックして書き込みを開始します。書き込みが終了したら、バックアップ CD/DVD が自動的に排出されます。

書き込みが完了しても、バックアップ対象ファイルは元の保存先にそのまま残ります。CD/DVDへの書き込みは、追加的なバックアップです。

アーカイブのインポート機能で、CDやDVDなどのメディアに保存されているアーカ イブを、再びバックアップのファイル管理システムに取り込むこともできます。

アーカイブのインポート

本製品のバックアッププログラムで管理しているドライブ以外にあるアーカイブやバックアップ データを復元するには、**アーカイブのインポート**機能を使用します。

このダイアログで、アーカイブファイル (拡張子「**ARC**」) をCD、DVD またはネットワークか ら探し出します。希望するアーカイブが見つかったら、これにチェックを付け、 **[OK]** をク リックします。 ウインドウが開いて、アーカイブが正常にインポートされた事を表す通知が表示 されます。

このアーカイブをデータの復元に使用する場合には、バックアップの**復元**領域で、目的のバック アップを選択して復元を開始します。

バックアップで作成したアーカイブファイルの拡張子は、「ARC」です。

ブートメディアの作成

バックアップ機能では、イメージバックアップしたデータをシステムの存在するドライブへ復元 する場合や、ファイルを復元したい場合に、ブート可能なCD/DVD/USBメモリを使用します。 機能を使用するには、ブートメディアを挿入し、**復元を開始**を選択します。

ブートCDを挿入時に、G DATA アンチウイルスを選択した場合は、ブートCD版のアンチウイ ルス機能が起動します。この機能では Windows 起動前の状態でウイルススキャンを実行し、起 動中では検出しにくいウイルスなども見つけることができます。特に G DATA をインストールす る前にウイルス対策ソフトをインストールしていなかったコンピュータ(新品のコンピュータは 除く)では、この機能を使用してブートスキャンを実行することをお勧めします。 ※インター ネットセキュリティでは本機能は使用できません。

ブートCDの作成方法は、**ブートメディア**の項を参照してください。

ブートメディアの機能が見つからない場合

この機能をインストール時に選択しなかったため、コンピュータにインストールされていない可能性があります。その場合は、製品CD(もしくはセットアップ)からイン

ストールウィザードを開始し、ダイアログに従って、ブートCDを作成機能を追加して ください。

パスワードマネージャー

パスワードマネージャーは専用のブラウザ用プラグインを使用し、ウェブサイト上で使用するパ スワードや個人情報などの管理を行うための機能です。



プログラム バージョン: 25.3.0.1

パスワードマネージャーは以下のブラウザをサポートしています:

- Google Chrome
- Mozilla Firefox
- Microsoft Internet Explorer

メモ: ブラウザの設定によってはパスワードマネージャープラグインを使用できない場合があります(例: シークレットモードを使用している場合や、プライバシー、セキュリティのレベルが高く設定されている場合など)。 プラグインの動作に問題が出る場合はブラウザの設定(シークレットモード、プライバシー、セキュリティに関わる設定)を確認し、関連すると思われる設定を一時的にオフにする、設定のレベルを一時的に下げるなどをお試しください。

パスワードマネージャーを使用する際は、まずパスワードセーフを作成し、次に、サポートされているブラウザへプラグインをインストールしてください。

パスワードセーフの作成とプラグインのインストール

まず、パスワードマネージャーの画面内にある、**パスワードセーフ**をクリックします。すると メニューが開きますので、**新しいセーフを作成**を選択してください。

👽 新しいセーフを作成				
パスワード:				
パスワード再入力:				
パスワードのヒント:				
パスワードの強度:	I			
		セーフの作成	キャンセル	

パスワードセーフ作成用のダイアログが開きますので、パスワードとその再入力、パスワードを 思い出すために表示させるパスワードのヒントを入力し、**セーフの作成**をクリックします。

これでパスワードセーフが作成されました。パスワードマネージャーの画面右にあるブラウザ名 を選択し、インストールを選択することでブラウザ用プラグインのインストール処理を始めるこ とができます。

プラグインのインストール処理が開始されると、説明用のダイアログが表示される、もしくは、 自動的に対象ブラウザが開きます。ダイアログの内容や、各ブラウザのプラグイン導入手順に 従って G DATA Password Manager をブラウザにインストールしてください。

⑦ 合 プラグインのインストールが完了すると、これらいずれかのアイコンがブラウザのツー ルバーに表示されます。アイコンをクリックすることでパスワードマネージャーを開く ことができます。(ブラウザにより表示されるアイコンが異なります)



パスワードマネージャーを開く際は、パスワードセーフ作成時に設定したパスワードの入力が必要になります。パスワードの入力を行った後、**ロック解除**をクリックして機能選択画面に進んで

ください。

ここで選択できるパスワードマネージャープラグインの各種機能の詳細は<u>プラウザプラグインの</u> 使用方法のページでご確認いただけます。

ブラウザプラグインの使用方法

 プラグインがインストールされたブラウザでは、これらいずれかのアイコンがツ ールバーに表示されます。アイコンをクリックすることでパスワードマネージャ ーを開くことができます。(ブラウザにより表示されるアイコンが異なります)

メモ: ブラウザの設定によってはパスワードマネージャープラグインを使用できない場合があります(例: シークレットモードを使用している場合や、プライバシー、セキュリティのレベルが高く設定されている場合など)。 プラグインの動作に問題が出る場合はブラウザの設定(シークレットモード、プライバシー、セキュリティに関わる設定)を確認し、関連すると思われる設定を一時的にオフにする、設定のレベルを一時的に下げるなどをお試しください。



パスワードセーフ作成時に設定したパスワードの入力を行い、**ロック解除**をクリックすると機能 選択画面に進みます。

機能選択画面では以下の機能を利用できます:

☆

お気に入り: ログイン情報の管理画面でお気に入りとして設定した、パスワード保護されたウェブサイトを呼び出すことができます。

圜 **ログイン情報**:パスワード保護されたウェブサイト用のログイン情報を管理できます。

連絡先情報:連絡先情報を登録して、ネットショップの配達住所などのウェブフォーム を自動的に入力させることができます。

阍 メモ: その他のメモを登録することができます。

ツール:パスワードマネージャーを閉じるにはこの機能を選択しロックをクリックしてください。設定をクリックすると、各種機能の設定画面を開くことができます。 パスワード生成では安全性の高いパスワードを自動的に生成でき、それをコピー貼り付けして使用できます。この機能は、パスワード保護されたウェブサイトでアカウントを作成する際など、新しいパスワードを設定する際に便利です。

管理	管理
ロック	バスワード生成
設定	h05wggSsyzXm5dJvwu
パスワード生成	
	□ 特殊文字
	クリップホードにコピー 新規作成

パスワードマネージャーに登録した各項目は以下の方法で編集、削除することができます:

+ **新規作成**: このボタンをクリックすると、選択した機能の新しい項目を作成できます。 情報を編集: このボタンをクリックすると、現在選択、編集している項目を保存できま す。

情報を削除: このボタンをクリックすると、選択した項目を削除できます。

	-	
CON BREEN XC	**	
GDATA	⊇~9 ⁻ 8*: com.	
	/12/2-F ¹⁴ :	
	21%	
	(約数に入た: 個)	
	tates N	
	EU-CO-1 www.gitta.de	
	2°F6/21 https://www.glata.de/nlop	
	7K32	
	2=40	
	「いたいはいと思想するです」というくどうという。	

メモ: 管理画面でログイン情報を設定する際は、ドメイン欄には、パスワードを登録するウェブ サイトのドメインを記入「例: gdata.co.jp」、アドレス欄には、登録するウェブサイトのアカ ウント入力ページのURLを http:// や https:// を含めて入力してください。

メモ:ログイン情報を登録してもアカウント入力ページ上に情報が入力されない場合は、ログイン情報の登録画面で「お気に入り」に設定してください。その後、パスワードマネージャーのプラグインのお気に入り画面から登録情報を選択することで、ページが開き自動的にアカウントが入力されます。

チューナー

チューナーを使用すると、簡単な操作で OS を最適化できます。チューナーは Windows Update の自動確認をはじめ、定期的なデフラグ、レジストリと一時ファイルの定期的なクリー ンアップに至るまで、Windows システム内を整理し、処理速度を向上させるツールです。



手動で各チューニングを実行できるほか、スケジュール化されたチューニングジョブを設定する 事もできます。

- 前回のチューニング: ここには最後にチューニングを行った日時が表示されます。新し くチューニングジョブを開始したい場合は、今すぐチューニングをクリックすると、す ぐにチューニング作業が開始されます。チューニング作業中は進行状況を示すプログレ スバーが表示されます。
- スケジュールチューニング: チューニングジョブを自動的に行いたい場合は、スケジュ ールチューニングを有効にするをクリックしてください。スケジュールの設定を変更したい場合は詳細設定で調整することができます。
- 構成: ここでは、チューナーが実行する設定項目を指定できます。選択した設定項目は、スケジュールもしくは、手動実行の際に実行されるようになります。各設定項目の有効/無効の切換えは、チェックボックスで行います。

チューナーの設定項目は次の3つのカテゴリに分類されています。

セキュリティ:セキュリティ用モジュールは、OS、各種ソフトウェアの更新や設定など、コンピュータに害を及ぼす可能性のある脆弱性をチューニングで解消し、コンピュータを適切に保護します。

- パフォーマンス:不要になったバックアップファイル、ログファイル、インストー ル済みプログラムのインストールファイルなどの一時ファイルは、ハードディスク へのアクセス速度に影響し、貴重な空き領域を圧迫する原因の1つです。さらに、 不要になったプロセスやショートカットはシステムの動作速度に大きな影響を及ぼ します。パフォーマンス用モジュールは、コンピュータに無駄な負荷をかけず、ス ピードアップするためのツールです。
- データ保護: データ保護用モジュールは、インターネットの閲覧やコンピュータの 通常利用している間に、意図せずコンピュータに残った履歴、ユーザーの利用傾 向、重要なファイル、パスワードを消去します。

後元: チューナーは変更したすべての項目が復元ができるように、項目ごとに復元ポイ ントを作成します。 もしチューニング実行後に問題が発生した場合には、ここから実行したチューニング項 目を取り消してシステムを変更前の状態に復元できます。復元を実行するには、復元領 域で表示される実行済み項目にチェックを入れてから、復元をクリックしてください。

この項目に関しての詳しい説明は<u>復元</u>の項で覧いただけます。

復元

チューナーは変更したすべての項目が復元ができるように、項目ごとに復元ポイントを作成しま す。もしチューニング実行後に問題が発生した場合には、ここから実行したチューニング項目を 取り消してシステムを変更前の状態に復元できます。





すべて選択: チューナーで変更したすべての項目を復元したい場合は、このボタンを選 択し**復元**ボタンをクリックしてください。



復元: チューナーで変更した項目を実際に復元する場合は、復元したい項目を選択し、 このボタンをクリックします。

選択した項目を削除:不要になった復元ポイントは、このボタンをクリックすると削除できます。

ブラウザクリーナー

ブラウザクリーナーを使うと、しばしばフリーウェア(無料ソフト)と一緒にインストールさ れ、ブラウザ設定やPC内のデータを盗み出すPUP (悪意のある有害な可能性のあるプログラムや アドオン)をブロック・取り除くことができます。

ブラウザクリーナーは、Microsoft インターネットエクスプローラー、Mozilla Firefox、 Google Chromeの各ブラウザごとに PUP を一覧表示し、更に無効化や削除などの操作ができ ます。無効化したアドオンはいつでも元の状態 (有効化の状態) に戻す事ができます。

GDATA		G DATA トータル	プロテクション	v		? _ X
5	⊉ 🖗 些	&	8	8	P	
	チューナー		2			۵ 🗘
E	Mozilla Firefox					₹ 5
	♂ このブラウザはサポートされています。					
	インストール済みブラウザ拡張機能					ステータス / 操作
e	🗉 💁 Adblock Plus					有効 ヘ
						→ 変更なし(K)
U						
9						(1) (1)((1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)
						変更を適用(A)
プログラム バージ	ョン: 25.1.0.4				TRUS	IN GERMAN SICHERHEIT.

メモ: ブラウザクリーナーは G DATA トータルセキュリティにのみ含まれる機能です。

ブラウザクリーナーは、Microsoft Internet Explorer、Mozilla Firefox および Google Chrome ブラウザに対応し、インストール済みの拡張機能を簡単に管理できます。無効 化・削除の操作は、対象を選択してクリックします。また、インストール済みのプラグ インはフィルタを適用でき、カテゴリに分類して表示させる事ができます。

フィルタリング

フィルタリング機能は、お子様がコンピュータを使用する際などに、ウェブサイトを一定の基準 で評価判別して排除したり、コンピュータの利用時間に制限をかける機能です。



🦉 新規ユーザー(N)

TRUST IN GERMAN SICHERHEIT.

ユーザーでコンピュータに登録されているユーザーアカウントを選択し、以下の項目か らそれぞれに適した設定を行ってください。Windows の新規ユーザーアカウント(例: 子供用アカウントなど)を作成したい場合は、<u>新規ユーザー</u>ボタンから作成する事がで きます。

- このユーザーのフィルタリング: ここでフィルタリングのオン/オフを切り替えられます。
- 禁止するコンテンツ: 編集をクリックするとダイアログが開き、指定したユーザーに対してブロックするウェブコンテンツを指定できます。
- 許可するコンテンツ: 編集をクリックするとダイアログが開き、指定したユーザーに対して許可するウェブコンテンツを指定できます。
- インターネット利用時間の監視: 編集をクリックするとダイアログが開き、指定したユー ザーに対してどれくらいの期間(またはどの時間帯)インターネットの接続を許可するか を設定できます。
- コンピュータ利用時間の監視: 編集をクリックするとダイアログが開き、指定したユーザーに対してどれくらいの期間(またはどの時間帯)インタコンピュータの使用を許可するかを設定できます。
- 設定:フィルタリング機能のログに関する動作を設定できます。

新規ユーザー

【新規ユーザー】をクリックすると、ダイアログが開きます。ここでユーザー名とパスワードを 入力してください。

▶ 新規ユーザーを	×	
ユーザー名(<u>B</u>):	test	作成(A)
パスワード(<u>P</u>):	•••••	閉じる(E)
パスワード再入力(<u>W</u>):	•••••	ヘルプ

安全のため、パスワードは、『8文字以上(大文字と小文字、数字を含む)』で構成す るようにしてください。

各項目を入力した後に**[作成]** をクリックするとWindows ユーザーアカウントが作 成され、ステータス領域のユーザーに新しく追加したユーザー名が表示されるように なります。Windows起動時に作成したユーザー名でログインすると、そのユーザー用 に設定したフィルタリングの設定が有効になります。ユーザー用のフィルタリング設 定を変更したり確認するには、禁止するコンテンツ、許可するコンテンツ、インター ネット利用時間の監視、コンピュータ利用時間の監視選択して**[編集]** をクリックし てください。

禁止するコンテンツ

ダイアログ画面で、ユーザーが閲覧することを禁止するコンテンツを設定します。禁止するコン テンツを有効にするには、禁止したいカテゴリにチェックを入れます。[OK]をクリックする と、**禁止する基準**を満たすウェブサイトを表示できなくなります。

🔽 禁止するコン	テンツを選択	×
選択したユー 注: [新規作版 注: [例外] を す。	ゲーに対してブロックするカテゴリを選択します。 対 を使用すると、個人用のブラックリストを作成できます。 使用すると、ブロックする必要がないページとして許可できま	
カテゴリ名	情報	
☑ 暴力	ブラックリスト 暴力 武器	
☑ 薬物	ブラックリスト 薬物	
☑ 過激表現	ブラックリスト 過激な表現	
📝 アダルト向けポ	ブラックリスト ポルノ アダルトサイト	
📝 八ッカー・クラ	ブラックリスト ハッカー 違法コピー	
新規作成(<u>N</u>)	例外(A) OK(Q) キャンセル(A) ヘルプ(H)	

[新規作成] をクリックするとダイアログ画面が開き、禁止するコンテンツを独自に作成できま す。コンテンツを作成するには、パーソナルフィルタを作成の画面で、名前の欄に入力し(必要 であれば情報欄に説明を入力して)、[OK] をクリックしてください。

😈 パーソナ	・ル フィルタを作成 プロパティ	×
説明		
名前(<u>N</u>):	test	
'情報(<u>I</u>):		
カテゴリ		
許可するコ <u>禁止するコ</u>	コンテンツ コンテンツ	
-		
L	OK キャンセル 適用(A))

[OK] をクリックすると、禁止するコンテンツの編集の画面が開きます。

J1709(<u>E</u>).	快赤灯象(0).)追加(H)
virus	検索対象の領域	
vinue	URL III	<u>変更(№)</u>
VII US		尚(1月全(1))
	✓ ★X	
] [
	OK キャンセ	ル 適用(A)

- URL: ウェブアドレス内の文字列を検索します。例えば、<u>www.chatcity.co.jp</u>、<u>www.crazychat.co.jp</u> などのサイトを禁止したい場合、フィルタ欄に「chat」と入力し、 URLにチェックを入れて【追加】をクリックします。この設定が有効になると、URLに「chat」という文字列が含まれているページがすべて閲覧できなくなります。
- タイトル: ウェブサイトのタイトルの文字列を検索します。ここでいうタイトルとは、ウェ ブページをブックマークに追加する時に表示されるウェブサイトに付与されている名前で す。例えば、Chat City Japan、Teenage Chat などのサイトを禁止したい場合、フィル 夕欄に「chat」と入力し、タイトルにチェックを入れて【追加】をクリックします。こ の設定が有効になると、タイトルに「chat」という文字列を使用しているページはすべ て閲覧できなくなります。
- メタタグ: メタタグ(検索エンジンによる検索結果を上げるために利用されるタグです))に記載されている文字列を検索します。例えば、メタタグ内のどこかに文字列「chat」が記述されているページを閲覧禁止にするには、フィルタ欄に「chat」と入力し、メタタグにチェックを入れて[追加]をクリックします。この設定が有効になると、メタタグ内に「chat」という文字列が含まれているページがすべて閲覧できなくなります。
- 本文:フィルタ欄に「chat」と入力し、次に本文にチェックを入れて、【追加】をクリックします。この設定が有効になると、本文内に「chat」という文字列が含まれているページがすべて閲覧できなくなります。 通常利用されるキーワードをフィルタに設定すると、無害なウェブページを閲覧できなくなることもあります。例えば、禁止キーワードに「cash」を登録すると、「Cashew」という文字列を含むウェブページの閲覧も禁止されかねません。

フィルタに引っ掛かりやすいウェブページを許可するには、**例外**機能を使って例外扱いします。 例外を追加するには、まず作成したブラックリストを選択し、**[例外]**をクリックします。例外 リストの画面が開くので、上述の例であれば、「Cashew」をフィルタに入力して、**[追加]**を クリックします。

> 禁止するコンテンツで追加したフィルタは、**パーソナルフィルタ**領域では、種類の列 に**ブラックリスト**と表示されます。作成済みフィルタは、自由に編集したり削除でき ます。詳細については、<u>パーソナルフィルタ</u>の項を参照してください。

許可するコンテンツ

ダイアログ画面で、ユーザーが閲覧することを許可するコンテンツを設定します。許可するコン テンツを有効にするには、許可したいカテゴリにチェックを入れます。[OK]をクリックする と、**許可するコンテンツの編集**で設定したウェブサイトの表示が許可されます。

許可するコン	テンツを選択 メ
選択したユー 注: 〔新規作]	ザーにアクセスを許可するコンテンツを選択します。 成] を使用すると、個人用のホワイトリストを作成できます。
カテゴリ名	情報
	小学生向けニュース
新規作成(<u>N</u>)	ОК(<u>0</u>) ≠ヤンセル(<u>A</u>) へルプ(<u>H</u>)

[新規作成] をクリックするとダイアログ画面が開き、許可するコンテンツを独自に作成できま す。コンテンツを作成するには、パーソナルフィルタを作成の画面で、名前の欄に入力し(必要 であれば情報欄に説明を入力して)、[OK] をクリックしてください。

じ パーソナ	ルフィルタ	▶を作成 プロ♪	パティ	×
説明				
名前(<u>N</u>):	kids			
情報(<u>I</u>):				
カテゴリ				
許可するコ 禁止するコ	ンテンツ ンテンツ			
	ОК	キャンセル	適用(A)	

[OK] をクリックすると、許可するコンテンツの編集の画面が開きます。

odata			etn(u)
+			19)11(<u>F</u>)
兄明(<u>5</u>):			変更(<u>N</u>)
			削除(A)
ታイトへのリン	ック(<u>L</u>):		
www.gdata.c	o.jp		
jdata			

次に、フィルタの欄に許可するドメイン名の一部入力します。(例: nickjapan)。説明の欄 には、ウェブページの内容(前述の例の場合、「nickjapan:子供向けウェブページ」など)を 入力します。サイトへのリンクの欄には、ウェブサイトの正確なアドレス(例: www.nickjapan. com)を入力します。説明とサイトへのリンクに情報を入力すると、ユーザーが禁止されたサ イトにアクセスしようとした場合に、許可するリストに登録されたウェブサイトがブラウザ上に 表示されます。すべての情報を入力して[追加]をクリックすると、情報が許可するコンテンツ に登録されます。

> フィルタやドメインの入力が間違っているとウェブサイトの表示ができませんのでご 注意ください。また、説明はアクセス可能なインターネットサイトのリストにリンク 名として表示されますので、お子様などの使用者を想定して設定してください。

> フィルタはドメイン名に含まれる文字を検索します。入力する文字によって表示基準 の厳密さを調整する事も可能です。

> 許可するコンテンツで追加したフィルタは、**パーソナルフィルタ**領域では、種類の列 に**ホワイトリスト**と表示されます。作成済みフィルタは、自由に編集したり削除でき ます。詳細については、<u>パーソナルフィルタ</u>の項を参照してください。

インターネット利用時間の監視

ユーザーのインターネット利用時間を設定します。まずは、ステータス領域でユーザーを選択 し、次にインターネット利用時間の監視、編集をクリックします。インターネット利用時間の 設定画面が現れるので、そこでインターネット利用時間を監視にチェックを入れます。許可す る時間は、月次、週次、曜日ごとに設定できます。許可する時間は、日/時:分の欄に入力す るか、マウスを使ってバーをスライドさせて設定します。例えば、「04/20:05」と入力す ると、インターネットの利用時間は「4日間、20時間と5分」となります。



インターネット利用時間の設定では、常に最小値が適用されます。例えば、1か月の時間制限を4日間と設定する一方で1週間の時間制限を5日間と設定した場合、ソフトウェアはこのユーザーのインターネット利用時間を自動的に4日間に制限します。

ユーザーが許可された制限時間を超えてインターネットにアクセスしようとすると、ブラウザに 利用制限時間を超過したことを知らせるメッセージが表示されます。

禁止する時間

【禁止する時間】をクリックしてダイアログを呼び出し、インターネットにアクセスできる時間 の量的制限に加えて、週のうちの特定の時間帯にインターネットにアクセスできないように設定 できます。

禁止する時間帯は赤色、許可する時間帯は緑色で表示されます。 許可または禁止する時間を指 定するには、マウスで時間帯を選択し、マウスポインタの横に表示されるコンテキストメニュー で**許可する時間**もしくは**禁止する時間**のいずれかを選択します。ユーザーが禁止時間にインタ ーネットにアクセスしようとすると、ブラウザに利用できない時間帯である事を知らせるメッセ ージを表示されます。

	月	火	*	木	숲	±	B
0:00					_		
1:00							
2:00							
3:00							
4:00							
5:00							
6:00							
7:00							
8:00							
9:00 10:00							
11.00							
12.00							
13:00							
14:00							
15:00							
16:00							
17:00							
18:00							
19:00							
20:00							
21:00							
22:00							
29.00							

コンピュータ利用時間の監視

ユーザーのコンピュータ利用時間を設定します。まずは、ステータス領域でユーザーを選択し、次にコンピュータ利用時間の監視、編集をクリックします。コンピュータ利用時間の設定画面が現れるので、そこでコンピュータ利用時間の監視にチェックを入れます。許可する時間は、 月次、週次、曜日ごとに設定できます。許可する時間は、日/時:分の欄に入力するか、マウスを使ってバーをスライドさせて設定します。例えば、「04/20:05」と入力すると、インターネットの利用時間は「4日間、20時間と5分」となります。

時間切れの前に警告を表示にチェックをいれると、コンピュータが自動的にシャットダウンさ れる前に、ユーザーにその旨を知らせることができます。コンピュータが事前の警告なしに シャットダウンされると、データの消失などの原因になります。

🔽 コンピュータ利用時間	×
ユーザーのコンピュータ操作を許可する時間と時刻を選択します。 注: [禁止する時間] からは、インターネット利用時間をより詳細に設定できます。 ます。	
☑ コンピュータ利用時間の監視	
□時間切れの前に警告を表示	
	日/時:分
週	02/14:30
月	18/12:30
	時:分
月曜日	00:00
火曜日	00:00
水曜日	00:00
木曜日	00:00
金曜日	00:00
	14:00
日曜日	14:00
禁止する時間(Z) OK(Q) キャンセル(r)	A) ヘルプ(<u>H</u>)

メモ: コンピュータ利用時間の設定では、常に最小値が適用されます。例えば、1か月の時間制限を4日間と設定する一方で1週間の時間制限を5日間と設定した場合、 ソフトウェアはこのユーザーのコンピュータ利用時間を自動的に4日間に制限します。

禁止する時間

【禁止する時間】をクリックしてダイアログを呼び出し、コンピュータを使用できる時間の量的 制限に加えて、週のうちの特定の時間帯にコンピュータを使用できないように設定できます。

禁止する時間帯は赤色、許可する時間帯は緑色で表示されます。 許可または禁止する時間を指 定するには、マウスで時間帯を選択し、マウスポインタの横に表示されるコンテキストメニュー で**許可する時間**もしくは**禁止する時間**のいずれかを選択します。


パーソナルフィルタ

自分で作成した**許可するコンテンツ(ホワイトリスト)と禁止するコンテンツ(ブラックリス** ト)の新規作成や変更ができます。

GDATA			G Data トータル	プロデクション				? _ X
6		*	& \	2	6	ዋ	£	
_	フィルタ	リング			ig.	*		۵ 🗘
4	パーソナルフィ	イルタ						
	(MOY HURN (肝町するコンチンツ)] と [ブラ	ックリスト (禁止するコ	ンテンツ)] の作成。	変更、および病害	業を行います。		
	名明	推动	()) 年代					
	ing test	ホワイトリスト						
	TR orace	228992AF						
	L							
						剂除(L) 🐐	新規作款(N)	👰 端隽(皇)
					TRUS	T IN GERM	AN SICH	ERHEIT.

パーソナルフィルタには以下の種類が利用できます:

- ・許可するコンテンツ(ホワイトリスト):選択したユーザーに対してホワイトリストを選択すると、このユーザーはそのホワイトリストに登録されているウェブページにしかアクセスできません。管理者はホワイトリストをそれぞれのユーザーにカスタマイズしたり、既存のホワイトリストからそれぞれのユーザーに合ったリストを選択できます。ホワイトリストは、特に幼少の子供へのインターネットアクセス制限を行いたい場合に有効で、教育上有益なウェブページのみ利用させるために役立ちます。
- ・禁止するコンテンツ(プラックリスト): ブラックリストはユーザーに特定サイトへのアクセスを禁止します。ブラックリストで指定した以外のコンテンツには自由にアクセスできます。 例えば、ブラックリストで指定したサイトと類似したコンテンツを含むサイトにはアクセスできます。 きます。もし制限をより確実にしたい場合は、URL 以外の別要素を禁止項目に含むか、ホワイトリストをご利用ください。
- 各リストの編集には以下のボタンを使用できます:
- 削除: 選択したリストを削除します。
- 新規作成: ブラックリストまたはホワイトリストを新規作成します。詳細は、禁止するコンテンツ および 許可するコンテンツ の項を参照してください。
- 編集: 既存リストの内容を変更します。

設定|ログ

この画面では、ログ取得に関する基本設定を変更でき、各違反ごとにログを記録するかどうかを 設定できます。ログは各ユーザーごとに保存され、ログ画面でユーザーごとのログを確認できま す。

🕞 設定 ログ	×			
 ☑ [許可するコンテンツ]の違反を記録(<u>5</u>) ☑ [禁止するコンテンツ]の違反を記録(V) 				
 ▼ [ポエキョン・フラブ いかはてもお客(王) ▼ [インターネット利用時間]の違反を記録(I) 				
 ☑ 「コンビュータ利用時間」の違反を記録(C) □ ファイルが 1000 KB に達した時にメッセージを表示 				
OK キャンセル 適用(A) ヘルプ				

使用環境によっては、ログファイルの容量が非常に大きくなります。ログファイルがディスク容量を圧迫するようであれば、ファイルが__KBに達したときにメッセージを表示にチェックを入れて、適当な数値を入力してください。ログのファイルサイズが設定された数値に到達すると、ユーザーに通知します。ログを削除したい場合は、ログ領域の[ログを削除]から削除できます。

データセーフ

データセーフは、個人情報などの重要なデータを暗号化して保護する機能です。ハードディスク の追加パーティションのような感覚で簡単に利用できます。

GDATA			G Data トータルプロテクション			? _ X
5	(G 🔧	2	ቀ 🚆	
	データセーフ					۵ 🗘
	管理					
	暗号化されたフォルダの最	新ステータスが確認でき、	、ここから暗萼化の作成や前	味を行うことができます。		
	說明	スデータス	ドライブ パス			
	My Safe	<i>0</i> ⊐-X	C:¥Users¥115	Honor Honor Honor	ents¥tsmxg_disc.ts4	
				受新	データセーフを新規作成	図く 削除
				TRU	ST IN GERMAN SI	CHERHEIT

データセーフ領域では、以下の操作が可能です。

- 更新: データセーフ領域からデータセーフを開閉した場合は、常時ステータスが更新され ますが、その他の方法でデータセーフを開閉した場合は、[更新] ボタンを押すとステータ スを更新できます。
- 開く/閉じる:お使いのコンピュータもしくは接続した記録メディア上にあるデータセーフ を開くいたり、閉じます。データセーフを開く際には、データセーフ作成時に設定したパ スワードの入力を求められます。一方、閉じる時にはパスワード入力は必要ありません。
- データセーフを作成: ここからデータセーフを新規作成できます。このボタンをクリック すると、データセーフ作成ウィザードが立ち上がり、ウィザードの指示に従って、データ セーフを簡単に作成できます。
- モバイル データセーフを作成: 作成したデータセーフを、リムーバブルメディアやメール で送信可能なモバイル データセーフに変換します。詳細は、モバイルデータセーフを作 成で確認してください。
- **削除**: 作成済みのデータセーフを削除します。削除操作では、パスワード入力は求められ ませんので、過って削除しないように注意してください。

データセーフ作成ウィザード

ウィザードを使って、データセーフの作成ができます。[次へ]ボタンで手順を進めてください。



データセーフの保存場所と容量

データセーフの保存先とサイズを指定します。

メモ: ローカルストレージ上にデータセーフを作成した場合は、データセーフがオープンの状態になると、データセーフはハードディスクのⅠパーティションとして認識され、保存されているファイルの編集・削除・コピーができます。データセーフ内のファイルは、暗号化して保存されます。

データセーフの保存場所

データセーフの保存先(例:**ローカルディスク(C:)**)を指定します。データセーフファイルは ドキュメントフォルダまたは任意の場所に保存できます。

> メモ:本製品をアンインストールしてから再インストールを行った場合、アンインストール前に作成されたデータセーフはデータセーフの管理画面に表示されなくなります。 その場合でも、Windows上でデータセーフファイル自体をダブルクリックもしくはコ ンテキストメニューから開けば、データセーフを開く事ができます。データセーフファ イルの拡張子は.ts4 です。(ファイル名の例: tsnxg_disc1.ts4)

データセーフの容量

スライダを調整することで、データセーフで使用できる容量を設定できます。セーフのサイズ は、設定可能な最大容量から 2GB 以上少なくなるように設定してください。最大容量でデータ セーフを作成すると、コンピュータの処理速度が低下する恐れがあります。

メモ:スライダの左側にあるボタンを使用すると、より正確に容量を設定する事ができます。例えばCDやDVDなどに書き込む際などに便利です。

設定が完了したら【次へ】ボタンで手順を進めてください。

セーフの保存場所と容量 データセーフを保護されたフォルダ、もしくは任意の保存場所に作成できます。
データセーフファイルが作成されます。他のユーザーがデータセーフを消してしまう等の事故をあたために、ファイ ルをドキュメントフォルダに保管する事をお勧めします。もちろん別のフォルダに保管する事も可能です。
保存場所
データセーブは、指定の保存場所に作成されます。 注意・セーファイルは消去の危険から保護されていません。 セーフの容量は1MBと2TBの間です(データフォーマット及び利用可能なメモリ容量に依存)。
データセーフの保存場所
C:¥Users¥shinsuke.kishimoto¥Documents¥tsnxg_disc3.ts4
データセーフの容量(少なくとも1 MB - 最大 49.4 GB)
現在の容量: 49.4 GB
< 戻る(B) 次へ(N) > キャンセル

データセーフのパラメータ

データセーフの各種項目を設定します。

- データセーフの名称: データセーフの名前を設定します。
- 説明: 補足情報などを記載します。(例: 個人情報用 など)
- ファイルシステム: データセーフを作成する仮想ドライブで使用するファイルシステムとして、FAT もしくは NTFS を指定できます。通常は自動選択を指定する事をお勧めします。
- データセーフのドライブを自動選択: データセーフは、ドライブ文字が割り当てられて表示されます。ここではデータセーフに、固定のドライブ文字を指定するか、自動割当てするかを選択できます。通常は自動選択(はい)を指定する事をお勧めします。
- ドライブの割り当て: このオプションは、ドライブ文字を自動割当てを選択しなかった場合に選択できます。

設定が完了したら [次へ]を押して進めてください。

G DATA USER MANUAL

図 セーフを作成	
データセーフのパラメータ データセーフの各種パラメーターを設定してください。	
データセーフの名前とデータセーフに適用するパラメータを入力してください	•
日 一般	
データセーフの名称	My Safe
1.20月	
ファイルシステム	自動選択
□ データセーフのドライブ	
データセーフのドライブを自動選択	(tt)
ドライブの割り当て	割り当てのないドライブのみ
選択:	H:¥
データセーフの名称 システム上でデータセーフを表示する際の名前を決めてください。	
< 戻る(B)	次へ(N) > キャンセル

データセーフへのアクセス

この画面でデータセーフにパスワードを設定します。[追加]ボタンをクリックしてください。

🗐 セーフを作成						
データセーフへのア ク データセーフのアク	性ス セス方法とアクセス権を定めてください。					
データセーフへのアクセスは、パスワードを使って行います。 データセースには複数のパスワードを割り当てることができ、それぞれのパスワードに異なった権利を付与できま す。						
- '	《スワードを追加するには、「追加」を押してください。複数入力可能です。					
追加	名前 /					
道去	パスワード: 1					
検閲付ち						
	< 戻る(B) 次へ(N) > キャンセル 					
18 I + -						

パスワード入力のダイアログが表示されます。名前の欄には適当な名称を入力し、パス ワードとパスワードを再入力のこの欄に同一のパスワードを入力します。

100	新しいパスワード	×
	データセーフアクセス用の新し パスワードは、少なくとも8つの 字、数字を含むから構成す く例: 10f%L1#39)。	いパスワードを入力してください。 0文字(大文字、小文字、特殊文 る必要があります。
	名前: パスワード: パスワードを再入力:	パスワード: 1 •••••
	❸ 推測ビットレート: 10	追加 キャンセル

[追加]ボタンをクリックするとパスワードが設定されます。その後、必要に応じて以下の項目を設定し[次へ]を選択します。

メモ: データセーフには、異なる権限を持った複数のパスワードを設定できます(例: パスワードA: ファイルの変更が可能、パスワードB: ファイルの読み込みのみ可 能)。

パスワード追加した後は、[権限付与]をクリックすることで以下の権限を設定できます。

- 自動起動を行う: データセーフ内には Autostart フォルダが作成されます。このオプションを「はい」に設定した場合、データセーフを開いた際に Autostart 内の実行可能ファイルが自動的に起動します。
- 「読み取りモード」で開く: このオプションを設定すると、データセーフ内のファイルの 保存や変更ができない、読み取り専用のモードになります。
- リムーバブルメディアとして開く: データセーフは通常、ハードディスクとして認識され ます。リムーバルディスクとして認識させる場合は、このオプションを「はい」に設定し てください。
- 共同利用: この設定を有効にするとネットワーク内の他のコンピュータからもデータセーフが利用できるようになります。※この設定を有効にすると、データセーフへのアクセス時にパスワード入力が不要になります。全ユーザーがアクセスできるネットワークで利用した場合、データセーフの意味をなさなるので、この機能の利用には注意してください。
- ログアウト時にセーフを閉じる: この設定は通常、有効にしておく必要があります。ユー ザーがデータセーフを閉じないままログオフした場合、他のユーザーがデータセーフの中 身を見ることができるためです。
- 自動データセーフ: この設定を有効にすると、自動データセーフ属性を持つ複数のデータ セーフを複数のデータセーフを一度に開く事ができます。※ この機能は今後のアップデートにより追加される可能性があります。初期状態では選択しても動作しませんのでご了承 ください。

G DATA USER MANUAL

データセーフへのフ	アクセスと権限		x	
アクセス方: 各アクセス	法: パスワード: 1 方法に対して別々の権限	見を割り当てられます。		
□ データセーフ^	のアクセス権限			
自動起動を行	3	はい		
「読み取り専用	リモードで開く	いいえ		
リムーバブルメラ	「ィアとして開く	いいえ		
共同利用		いいえ		
ログアウト時にも	2ーフを閉じる	はい		
自動データセー	7	いいえ		
データセーフへのアクセス権限				
		閉じる		

データセーフの設定

データセーフ作成ウィザードの最後の手順です。作成されるデータセーフの概要をここで確認 し、もし変更を加えたければ [戻る] ボタンをクリックして必要な項目を修正してください。設 定に問題が無い場合は [作成] ボタンをクリックし、次の画面で [完了] をクリックしてくださ い。



作成したデータセーフを開くにチェックが入っていれば、作成したデータセーフが読み 込まれます。



モバイルデータセーフを作成

モバイルデータセーフでは、リムーバブルメディア上でデータセーフを使用したり、メールで送 信可能なモバイルデータセーフを設定できます。

モバイルデータセーフを作成するには、まず**データセーフ**の画面を表示させ、作成されたデータ セーフを選択します。次に、画面下に[**モバイルデータセーフを作成]**ボタンが表示されるの で、これをクリックします。[次へ]を押して手順を進めてください。



データセーフのパラメータ

通常のデータセーフ作成と同じ要領で、データセーフの各種項目を設定します。モバイルデータ セーフでは、以下のパラメータが設定できます。

- データセーフのドライブを自動選択: データセーフは、ドライブ文字が割り当てられて表示されます。ここではデータセーフに、固定のドライブ文字を指定するか、自動割当てするかを選択できます。通常は自動選択(はい)を指定する事をお勧めします。
- データセーフを記憶媒体と結合する: 作成先のメディア(例: USBメモリやハードディスク) でのみデータセーフを利用できるように紐付けることができます。記憶メディアに結合しない場合は、データセーフのファイル(拡張子: tsnxg) は自由にコピーや移動できます。

G DATA USER MANUAL

データヤーフのパラメータ			
モバイルデータゼーフのパラメータを入力してください			
作成するモバイルデータセーフのパラメータを設定してくださ	5(1.5		
日一般			
データセーフの名称		My Safe	
□ データセーフのドライブ			
データセーフのドライブを自動選択		(t ()	Ξ
ドライブの割り当て		割り当てのないドライブのみ	
	選択:	H¥	
□ データセーフへのアクセスの制限			
データセーフを記録媒体と結合する		いいえ	- -

媒体

モバイルデータセーフの保存先メディアを指定します。

メモ:読み取り専用モードの設定されたパスワードを使用している場合や、CD/DVD に作成されたモバイルデータセ−フを利用している場合は、データを書き込む事はでき ませんのでご注意ください。

モバイルデータセーフを作成	-	×
媒体 記録媒体を選択してください。		
データセーフのコピー先メディアを選択	してください	
◎ リムーバブルメディアを選択		
名前	空き保存領域	
りムーバブル ディスク (H:)	1.84 GB	
		*
	< 戻る(B) 次へ(N)	> ++>セル

データセーフの容量

保存先メディア上で必要になる容量が表示されます。保存先メディアが容量不足の場合は、モバ イルデータセーフの作成をキャンセルすることもできます。

> メモ: モバイルデータセーフの容量には、データセーフの実際の容量の他、ドライバ (約6MB)も含まれます。ドライバは、G DATA トータルセキュリティが未インスト ールの環境でデータセーフを開くために必要です。



完了

[完了] を押すと、モバイルデータセーフの作成が完了します。保存されたファイルを表示する にチェックを入れたままにしておくと、モバイルデータセーフのフォルダが自動的に開きます。

🗐 モバイルデータセーフを作成	1	-	I	x
	完了			
		ファイルの保存に対 マ 保存されたファ	は功しました。 ・イルを表示する	5
			完了	**ンセル



モバイルデータセーフを開く

G DATA トータルセキュリティが未インストールの Windows PC上でモバイルデータセーフを開 くには、モバイルデータセーフの保存先に移動し、**TSNxG_4** フォルダ内の **Start.exe** を実行 します。次に、モバイルデータセーフのダイアログボックスが開くので、**[セーフを開く]** をク リックしてください。

G Data TotalProtection - モバイルデー	-9t-7				
データセーフのファイル: FYITSNYG 4¥data¥isnyn disc2 ts4					
セーフを開く	セーフを閉じる				
	開じる ヘルプ				

メモ: モバイルセーフを始めて利用する際は、対応ドライバのデータとプログラムが読み込んだ後、再起動が必要になる場合があります。コンピュータを再起動した後は、 再度 **Start.exe** を実行してください。

厕」G Data データセーフ - データセーフを開く	×
データセーフを開く データセーフを開くには、アクセス方法を選択して有効なアクセスラ し、「データセーフを開く」をクリックしてください。	产-梦起力
パスワードを用いたデータセーフへのみ	りりセス
パスワードを使用してデータセーフを開 正しいパスワードを入力し「データセーフを開く」を	きます。 クリックしてください。
パスワード	
データヤーフロ情報を確認するには ここをわいが	カリ・アください。
データセーフを開くキャンセル	

データセーフ用のパスワードを求められるので、データセーフに設定したパスワードを入力します。データセーフを開くをクリックすると、実際にデータセーフがコンピュータに読み込まれます。

読み込み処理が完了すると、通常のデータセーフのようにハードディスクもしくはリムーバブル メディアとして読み込まれ、Windows エクスプローラー上で表示されます。

モバイルデータセーフを閉じるには、開いた時と同様の手順で行います。モバイルデータセーフの保存先に移動し、TSNxG_4 フォルダ内の Start.exe を実行して表示されるダイアログで [セーフを閉じる] を選択してください。

メモ: リムーバブルメディアをコンピュータから取り外す際は、データセーフが閉じられていることを確認してから実行してください。

オートスタートマネージャー

オートスタートマネージャーは、Windows 起動時に自動起動するプログラムを管理するモジュ ールです。通常、自動起動プログラムは Windows のスタートアップにロードされますが、オー トマネージャーを使うと、任意の自動起動プログラムの起動を指定した時間で遅らせて起動で き、Windows の起動を高速化できます。

GDATA	G Dat	a 1	タルフ	ロテクション			? _ X
5 🖳 🕫	t 🏥 🤤	•	╲	2 `	•	A	
オートスター	-トマネージャー			_			0 🖻
オートスタート (3)	(風なし)			7-10	スタート (遅延あり)		
アプリケーション	鑽從元	0		アプリケーション	刷完元	<u>385</u>	
⊜ すべてのユーザー		-		◎ ログイン ユーザー			
Tintel(R) USB 3.0 Monitor	Intel Corporation			400.付蕪	Microsoft Corporation	2 59	-
Apple Push	Apple Inc.						
FreePDF Assistent für Fre	shbox.de	8					
Adobe Reader and Acroba	Adobe Systems Incorporated		-				
🕝 iTunesHelper	Apple Inc.		-				
ightTray Module	Intel Corporation						
bkcmd Module	Intel Corporation						
persistence Module	Intel Corporation						
🖯 ログインユーザー							
👩 Google Chrome	Google Inc.	¥					
						保存(3)	光に関す(R)

TRUST IN GERMAN SICHERHEIT.

オートスタートマネージャーを初めて開くと、画面左側にコンピュータにインストール済みの自 動起動プログラムの一覧が表示されます。これらは Widows の起動直後に起動されるため、起 動所要時間に直接の影響を及ぼします。

自動起動プログラムを遅らせて起動するには、まず対象のプログラムを選択して矢印ア イコンをクリックし、右側の領域**スタートアップ(遅延あり)**に移動させます。

遅らせて起動している自動起動プログラムを再び遅延なしで起動するには、対象のプロ グラムを選択して矢印アイコンをクリックし、左側の領域スタートアップ(遅延なし) に移動します。

遅延の設定

オートスタート(遅延あり)のプログラムは、起動を指定した時間で遅らせて起動できます。遅 延時間を変更するには、対象プログラムの**遅延カラム**上でクリックします。プルダウン表示され るオプションから、選択してください。

アプリケーション	開発元	遅延
すべてのユーザー		· ·
vm VMware Tools Co	VMware, Inc.	2分 🔻
		起動しない 自動 1 分
		2 分
		3分 4分 5分
		6分
		7分
		8ヵ 9分
		10分

以下のオプションが選択できます。

- 起動しない: Windows の次回起動時から起動されなくなります。
- 1-10分: ここで指定する時間に準じてアプリケーションが起動されます。
- 自動: CPUと保存領域の負荷状況を判断しながら自動起動します。

プロパティ

オートスタートマネージャーで表示されるプログラム上でダブルクリックすると、対象の自動起 動プログラムのプロパティを表示させることができます。

G Adobe ARM	วือパ ร า X
() 20	アプリケーションは、G Data によって管理されています
IKEY_LOCAL_MA	CHINE¥Software¥WOW6432Node¥Microsoft¥Windows¥Current¥Run
アプリケーション:	Adobe ARM
説明:	Adobe Reader and Acrobat Manager
開発元:	Adobe Systems Incorporated
ファイル バージョン:	1.7.2.0
対象:	"C:¥Program Files (x86)¥Common Files¥Adobe¥ARM¥1.0¥AdobeARM
引数:	

["	閉じる(<u>s</u>)	ヘルプ

デバイスコントロール

デバイスコントロールを使うと、コンピュータに接続したCD/DVDドライブやリムーバブルメ ディアなどを、ユーザーおよびデバイス単位でアクセス権限を細かく管理できます。これによ り、コンピュータから情報が不正に抜き取られる被害やバックアップ用の外付けディスクへ特定 ユーザーのみアクセスできるように設定するなどして、データ欠損事故やデータ漏洩の被害を未 然に防ぐ事ができます。

この画面では、管理対象のデバイス一覧が表示されます。どのユーザーに対して、どのような権限が付与されているか確認できます。 [ルールを編集] ボタンからは、デバイスまたはユーザーに対してのルールを設定する事ができます。

GDATA		G Data	トータルプロデクション		? _ X
5	Q	¢	🔧 👱 🍗 🖓		
	デバイス コン	ントロール			•
	管理対象のデバイス	一覧を表示します。			
Barrad at	ユーザーに適用するルー	ル老磯源してください。			
	ユーザー: <u>SKIS</u>				
	デバイス / ドライブ	アクセス	デバイスの説明		
	E:¥	70*0	Elements 1000 GB (Western Digital Technologies, Inc.)		
				🦉 ルールを端集	要新
			TOUGT IN OFF		
			I RUST IN GER	MAN SICHER	meil.

設定

設定領域では、本製品に搭載されている機能の設定項目を確認したり変更ができます。設定領域の左上アイコンからは、次の機能が利用できます。



設定をエクスポート:設定ファイルを作成します。複数のコンピュータに製品をインス トールして共通の設定でコンピュータを管理する場合、この機能を利用すると便利で す。



設定をインポート: ここから設定ファイルをインポートします。インポートを実行する には、ここをクリックし、設定ファイルを指定してインポートを実行します。設定のイ ンポートは、チェックマークを操作して、設定をインポートするモジュールや各モジュ ールの項目を選択します。



設定をリセット: 何らか理由で現在の設定をデフォルトの状態に戻したい場合は、この アイコンから簡単にリセットできます。リセットは、インポートの操作と同じ様にモ ジュールやモジュールに含まれる設定項目単位でリセットすることが可能です。

▶ 設定をインポート	×
インポートする設定領域を選択してください。	
□-図 <u>すべての設定</u> □-図一般	
■ ■ ウイルスガード	=
 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	
 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	
■ ■ ファイアウォール	~
ОК ‡ †	ンセル

一般

セキュリティ/パフォーマンス

ここでは、コンピュータの性能に応じて簡易的にセキュリティ設定を最適化できます。下のメー ターでは、それぞれの設定が及ぼすパフォーマンスやセキュリティ性能への影響を確認できま す。まず簡単に動作の調整を行いたい、という場合にはこの機能を使用すると便利です。

標準スペックのコンピュータ用(推奨):2種類のエンジンを使い、最適な保護を提供します。この設定では、ウイルスガード(オンアクセス機能)はすべての読み取り/書き込みアクセスをチェックします。

エンジン: G DATA には、2種類のエンジンが搭載されています。コンピュータの保護 レベルを最適に保つためにも、この設定を利用することをお勧めします。

 低スペックのコンピュータ用: 低スペックのコンピュータでは、コンピュータの処理速度 が遅くなることがあります。その場合は、1つのエンジンのみを利用することで、パフォ ーマンス低下を回避することができます。この設定では、ウイルスガード(オンアクセス 機能)は実行アクセスのみをチェックします。

市販の大部分のウイルス対策ソフトには1種類のみのエンジンが搭載されていることか らも、1種類のエンジンのみで稼動したとしても、セキュリティ保護レベルが大幅に低 下することはありません。

ユーザー定義: エンジンとウイルスガード(オンアクセス機能)の設定をお好みでカスタマイズできます。モードでは、無効(非推奨)以外のオプションを選択してください。無効(非推奨)を選択すると、セキュリティレベルが著しく低下するので、推奨されません。

◆ 設定 一般 セキュリラ ◆ 全 そ	ティ / パフォーマンス			×
 ごまた ごまた ごまた このののののののののののののののののののののののののののののののののののの	 設定の最適化: ● 標準スペックのコン ● 低スペックのコン ● ユーザー定義 エンジンの理算: 	ンピュータ用 (推 ビュータ用 2つのエンジ	(夏高映出力)推奨)	•
 ▶ アンチスパム ▶ ファイアウォール ▶ チューナー ▶ デバイス コントロール ▶ バックアップ 	t-r:	読み取り/音	さんが初にスキヤン	•
	セキュリティ: スピード: メモリ使用量:	低 	良 	最高
		ок	キャンセル 適用(目	き) へいて

USB キーボードガード

本機能は、USB端末がキーボードになりすましてコンピュータを不正操作する攻撃(BadUSBと呼ばれる脆弱性を悪用する攻撃手法の1つ)からコンピュータを保護します。

機能を有効にすると、新しいUSBキーボードもしくは、キーボードになりすました機器がコン ピュータに接続された際にポップアップが表示されます。

🔽 US	GB キーボードガード	×
⚠	新たに検出されたキーボード: HID キーボード デバイス Sold Year 掲線した提供器がキーボードでない」場合は、「キーボードを のうた道理ルにでない。安全のため、プロゥウした機器は は感 キーボードがインストールされていないユージョージ 環境したいなど見ててたない。 対応方法を選択して、統行してください。	ブルに
	キーボードを計可 キーボードをブロック	

接続されたUSB機器が自分の接続したキーボードの場合はポップアップ内の**キーボードを許可** を選択してください。

もし、キーボードではない機器を接続したにも関わらず、このポップアップが表示される場合 は、その機器がキーボードになりすましている可能性がありますので、**キーボードをブロック**を 選択し、ブロックした機器をコンピュータから取り外してください。

注意:不正操作を防ぐため、ブロックした機器は別のコンピュータにも接続しないでください。

😈 USB +-	ボードル	2 - 12		×
10255	01.0 .117	の数字列	を入力して(ださい)	
	7	0 6	5	
	Ζ	<u>8</u>	2	
	4	5	6	
	1	2	3	
		0		
		中止 (24)		

キーボードを許可を選択した後は確認のため認証番号の入力画面が表示されますので、マウス などで画面に表示された番号を入力してください。入力成功すると接続したキーボードの使用が 許可されます。

パスワード

本製品では、設定にパスワード保護を行うことができます。パスワード設定により、別のユーザ ーが本製品の設定を不正操作することを防ぐことができます。

設定	役定やセキュリティ機連	後作のパスワード保護:
→ 一般		
> セキュリティ / パフォー マンス	パスワード(K):	1
▶ バスワード	パスワード再入力(w);	
> アンチウイルス	パフワードのというの	
▶ アンチスパム	CONTRACTION.	
シ ファイアウォール		推進ったバスリードかん力された際に、パスワードのセンドが表示されま す。自分だけがわかるパスワードのセントを入力してください。
▶ チューナー		
▶ デバイス コントロール		
Ҍ バックアップ	パスワードの削除(e)	
	※パスワード保護は、ソ	フトウェアのセキュリディを責に強化します。

パスワードを設定するには、設定画面の左側の領域で**パスワード**を選択し、画面右側の**パスワー** ドと**パスワードの再入力**の2箇所のフィールドで、パスワード入力を行います。**パスワードのヒ** ントでは、万一パスワードを忘れた際に表示するヒントを入力します。

パスワードの設定後に各設定を変更したい場合は、設定画面の右下に表示されるボタンをクリッ クし、パスワードを入力してください。

> **メモ**:パスワードのヒントは、間違ったパスワードが入力された場合に表示されます。 パスワードを設定した本人だけがわかるヒントを指定してください。

> メモ:パスワード保護は、セキュリティレベルをアップさせるための有効な手段ですが、1台のコンピュータを複数ユーザーで共同利用する環境では、各ユーザーに専用のアカウントを作成することをお勧めします。これにより、管理者権限を持つユーザーのみが変更することが許可され、制限された権限を持つコンピュータの利用者は変更ができないようになります。

メモ: コンピュータの各ユーザーにユーザーアカウントをセットアップしたなどして、 パスワードが不要になった場合は、**パスワードの削除**のボタンからパスワードを削除 できます。

注意: パスワードの設定後は、**パスワードの削除**を行わない限り、設定変更を行いたい場合に毎回パスワード入力が必要になりますのでご注意ください。

アンチウイルス

リアルタイム保護

本製品では、リアルタイム保護を継続的に提供するウイルスガード(オンアクセススキャン)機 能を提供しています。この機能は、コンピュータ上で行われる読み取り/書き込み処理を常時 チェックし、 マルウェアの実行や拡散を未然に防ぎます。ウイルスガードは、アンチウイルス機 能で最も重要な機能の1つです。通常は、この機能は無効にしないようにしてください。

1. 1. ¢				
 設定 > アッチウイルスガード > マンチウイルス > ビ塔奈道建美近3 > アンチウイルス エンジンの建築D: > ウイルススキャン > マボススキャン > マボススキャン > スールススキャン > シスールススキャン > シスールススキャン > シスールススキャン > シスールススキャン > シストルススキャン > シストルスストャン > シストルスストャン > シストルスストャン > シストルススキャン > シストルスストャン > シストルスストキャン > シストルススキャン > シストルストャン > シストルストッシュ > シストルストッシュ > シストルストッシュ > シストルストッシュ > シストルストッシュ > シストルストッシュ > シストッシュ > シストルストッシュ > シストルストッシ	ウイルスガード (注意)(注意)(13 エンジンの運動(D): 感染したフナイル(D): 変染したアーカイブ(C):	2001ンジン(推奨) 3-ガーの操作を持つ 3-ダーの操作を持つ		-
	 つう「ルス鉄上時に巻で通知 込みたい時知(ビハイビアブロッキ 図 有効(推測) 図 有効(推測) 図 オットバイロット(確認) 	「回」 ング ラセージの表示調動を搭載	詳細設定(<u>A</u>))(E)	制化
 ▶ デューナー ▶ デバイス コントロール 	ランサムウェア対策 (衛等化機能) 図 複助 (推薦)	定持ったトロイロ木馬に対す	る漆縷機能)	
 Norral 	1937日イト対策(ソフトウェアの 図 有助(推美))続荷住を専用する攻撃に)	対する保護機能)	

リアルタイム保護で利用できる項目です。

- 有効(推奨):このチェックマークボックスから、ウイルスガードのオン/オフを切換えできます。
- エンジンの種類: ウイルススキャンに使用するエンジンを選択します。G DATAには、2 種類の高性能ウイルス検索エンジンを搭載し、世界最高レベルのウイルス検出率を実現しています。通常は、2つのエンジン(最高検出力/推奨)に設定してください。もしコン ピュータの処理速度に問題がある場合は、1種類のエンジンのみを使用することにより、 パフォーマンスを改善することもできます。
- 感染したファイル: 感染ファイルが検出された場合の処理方法を設定します。デフォルト 設定では、感染ファイルの処理方法をユーザーに確認します。なお、データを最高セキュ リティで保護するには、ウイルス駆除(不可能な場合は隔離)に設定します。
- 感染したアーカイブ: アーカイブファイル(RAR、ZIP または PST などの拡張子を持つ ファイル)を通常ファイルと別扱いするかどうかを設定します。なお、隔離されたアーカ イブファイルは、元に戻す場合に破損する場合があります。感染したアーカイブは、ユー ザーの操作を待つを選択し、検出の度に処理方法をユーザーに選択させることをお勧めし ます。
- ふるまい検知: コンピュータ上のWindows のレジストリやHOSTSファイルへのアクセス

やネットワークアクティビティを監視します。これにより、通常のウイルススキャンで検 出できなかった不正プログラムを検出します。

- ランサムウェア検知: ランサムウェアの攻撃からファイルやシステムを保護する機能です。ランサムウェアの多くは暗号化機能を持ったトロイの木馬の一種であり、暗号化したファイルと引き換えに身代金を要求します。本機能はランサムウェアの動作を検知し被害を最小限に防ぎます。
- エクスプロイト対策: アプリケーション(PDFビューア、ブラウザなど)の脆弱性を突く エクスプロイト攻撃により、あなたのPCが不正侵入を受けないように保護します。
 一般的なエクスプロイト対策としてはアプリケーションを最新の状態に更新することが非常に重要ですが、未知のエクスプロイト攻撃があった場合、更新を行っているだけでは完全に防げない可能性があります。G DATA のエクスプロイト対策機能は、そのような未知の攻撃にも対応できるプロアクティブ技術を搭載しています。

例外

ウイルスガードによるスキャンが不要なドライブ、ファイル、およびフォルダをスキャン対象か ら除外する設定を行います。

Щ	定義	新規作成(<u>N</u>)
フォルダ	C:¥PerfLogs	編集(E)
		削除(D)

例外を設定するには、以下の手順に沿って行います。

[例外]を選択します。

2 ウイルスガード用の例外設定のダイアログ画面で、[新規作成] を選択します。

3 次の**例外設定**の画面で、除外対象をドライブ、フォルダ、ファイルを選択できます。

ドライブまたはフォルダを指定する場合は、対象を入力欄に直接入力、もしくは、[…]
 をクリックして対象を指定します。ファイルを指定するには、完全なファイル名もしくはワイルドカードを含むファイル名を設定します。

メモ: ワイルドカードの機能について

- 疑問符(?):任意の1文字を表すためのワイルドカード
- アスタリスク(*):文字列全体を表すためのワイルドカード

例: 拡張子「.sav」のファイルをすべて対象に設定するには、「*.sav」と入力しま す。連続性のある名前のファイル (text1.doc、text2.doc、text3.doc など) などを 保護するには、「text?.doc」と入力します。

この手順を繰り返して例外設定行うことにより、自身の環境に適したウイルスガード用例外をカ スタマイズできます。また、作成した例外設定は、**ウイルスガード用の例外設定**画面の**例外**で 表示され、編集や削除の操作は、それぞれ [**編集**] と [**削除**] から可能です。

詳細設定

[詳細設定] からは、ウイルスガードによるスキャンの設定確認や変更ができます。

ウイルスガー।	ş		×
€-ド(<u>o</u>):	読み取り/書き込み	時にスキャン	•
	🗹 重要なフォルダを領	集中的に監視(<u>₭</u>)	
設定			
☑ ネットワーク	アクセスのスキャン(工)		
✓ ビューリスティ	ック(<u>H</u>)		
🗹 アーカイブの	スキャン(<u>A</u>)	(300KB 以下)(<u>D</u>)	
ロメールァ	′ーカイブのスキャン(⊻)		
☑ システム起動	り時にシステム領域をスキ	ヤン(<u>S</u>)	
☑ メティア交換	時にシステム領域をスキャ	ッン(<u>M</u>)	
☑ 怪しいプログ	ラムのスキャン(<u>U</u>)		
☑ 新しいファイノ	レと変更したファイルのみ	スキャン(<u>n</u>)	
		OK 4	キャンセル

以下の項目を設定できます。

- モード:スキャンするタイミングを設定します。設定は、読み取り/書き込み時にスキャン、読み取り時にスキャン、もしくは実行時にスキャンから選択します。なお、読み取り時にスキャンが行われた場合は、不明なプロセスによる感染があったかどうかを、新規ファイルもしくは新たなファイルバージョンの作成時にスキャンします。その他のケースでは、プログラムが読み取りを行う際にファイルをスキャンします。
- 重要なフォルダを集中的に監視: このオプションを有効にすると、共有フォルダやコン ピュータ上のユーザーデータ、またはクラウドサービス(DropboxやGoogle ドライブ)

などを常時、読み取り/書き込み時にスキャンするようになります。スキャンのモード に、実行時にスキャン以外が設定されている場合、このオプションは灰色で表示されま す。

- ・ネットワークアクセスのスキャン:ネットワークアクセスで不正プログラムをスキャンします。自身のコンピュータを、ネットワーク経由でウイルス対策がなされていない第三者のコンピュータと接続する場合には、この機能を有効にしてください。一方、スタンドアロン(ネットワークに未接続)環境、またはネットワーク内の全コンピュータにウイルス対策ソフトがインストールされている環境では、この機能は無効にしておいてください。これらの環境でこの設定を有効のままにしておくと、、重複スキャンが発生することがあり、コンピュータの動作速度の低下につながります。
- ヒューリスティック: ワクチンに情報がないウイルス特有の特徴をもつ新種ウイルスを検出します。この検出手法では、保護率を大幅に向上できますが、一方で、未感染ファイルを感染ファイルと判断することもあります。
- アーカイブのスキャン: アーカイブ(ZIP、RAR、またはPSTなどの拡張子を持つファイル)をスキャンします。アーカイブのスキャンには、多くの時間を要します。ウイルスガードが常時システムを監視している場合には、アーカイブを解凍する時にアーカイブ内のウイルスを検出するので、この機能は無効にして問題ありません。使用頻度が低い容量の大きなアーカイブのスキャンによるコンピュータの処理速度低下を防止するには、スキャンするアーカイブのサイズを制限します。
- メールアーカイブのスキャン:メールアーカイブをスキャンします。なお、本製品では、 メールの送受信時にスキャンを実行しているので、通常はこの機能は無効にしていても問 題はありません。メールアーカイブのスキャンは、アーカイブのサイズによっては数分間 かかることがあります。
- システム起動時にシステム領域をスキャン:システム領域のスキャン実行タイミングをシ ステム起動時に設定します。この設定、もしくはメディアの交換時にシステム領域をス キャンのいずれかは常に有効にし、スキャン対象から除外しないでください。
- メディアの交換時にシステム領域をスキャン:システム領域のスキャン実行タイミングを メディア(CD/DVDなど)の交換時に設定します。この設定もしくはシステム起動時に システム領域をスキャンのいずれかは常に有効にし、スキャン対象から除外しないでくだ さい。
- ・ 怪しいプログラムのスキャン:ダイヤラ、スパイウェア、アドウェア、リスクウェアなどの不正プログラムをスキャンします。これらの不正プログラムは、望ましくないインターネット接続を勝手に確立したり、ブラウザの閲覧履歴やキーボードへの入力(パスワードなど)を不正に盗みだし、情報漏洩や金銭的な被害に発展する恐れがあります。
- 新しいファイルと変更したファイルのみスキャン: この機能を有効にすると、以前実行したスキャンにおいて、安全と判断されているファイルで、かつしばらくの間、変更されていないファイルのスキャンをスキップします。スキャンの対象は、新規作成ファイルや変更されたファイルのみがスキャンされるようになり、スキャン速度を大幅に向上できます。

ウイルススキャン

オンデマンドスキャン用のスキャン設定を行います。

リアルタイム保護で利用できる項目です。

- エンジンの種類: ウイルススキャンに使用するエンジンを選択します。G DATAには、2 種類の高性能ウイルス検索エンジンを搭載し、世界最高レベルのウイルス検出率を実現しています。通常は、2つのエンジン(最高検出力/推奨)に設定してください。もしコン ピュータの処理速度に問題がある場合は、1種類のエンジンのみを使用することにより、 パフォーマンスを改善することもできます。
- 感染したファイル:感染ファイルが検出された場合の処理方法を設定します。デフォルト 設定では、感染ファイルの処理方法をユーザーに確認します。なお、データを最高セキュ リティで保護するには、ウイルス駆除(不可能な場合は隔離)に設定します。
- 感染したアーカイブ: アーカイブファイル(RAR、ZIP または PST などの拡張子を持つ ファイル)を通常ファイルと別扱いするかどうかを設定します。なお、隔離されたアーカ イブファイルは、元に戻す場合に破損する場合があります。感染したアーカイブは、ユー ザーの操作を待つを選択し、検出の度に処理方法をユーザーに選択させることをお勧めし ます。
- 高システム負荷時にはウイルススキャンを停止: ユーザーがコンピュータ上で作業しない 状態になると、スキャンが自動で実行されます。スキャン実行中にコンピュータを使用す ると、スキャンは中断されます。中断されたスキャンは、再びコンピュータで作業をしな い状態になった場合に再開されます。

👽 設定 アンチウイルス ウイルススキャン					
11 C					
識定	エンパンの種類(症):	2001ンタン(商業)	输出力/推奨)		*
▶ 一般	感染したファイル(D):	ウイルス懸録(不明	能な場合は隠謬)		*
 ▶ アンチウイルス ▶ リアルタイム保護 ▶ ウイルススキャン 	厳築したアーカイブ(C): 	ログを残すのみ ウイルススキャンを停止(5)		-	
▶ 英新 ▶ ウエブ俘援					6191(N)
 ▶ メールスキャン ▶ 自動ウイルススキャン 					算稿設定(<u>w</u>)
▶ アンチスパム					
♪ ファイアウォール					
♪ チューナー					
≬ デバイス コントロール					
トバックアップ					
		OK	キャンセル	濾用(8)	~H.I

例外

ウイルススキャンによるスキャンが不要なドライブ、ファイル、およびフォルダをスキャン対象 から除外する設定を行います。

種類	定義	新規作成(<u>N</u>)
		編集(E)
		削除(D)

例外を設定するには、以下の手順に沿って行います。

- [例外]を選択します。
- 2 ウイルススキャン用の例外設定のダイアログ画面で、[新規作成]を選択します。
- 3 次の**例外設定**の画面で、除外対象をドライブ、フォルダ、ファイル拡張子を選択できます。
- 4 ドライブまたはフォルダを指定する場合は、対象を入力欄に直接入力するか、もしくは [...]をクリックして対象を指定します。拡張子を指定するには、拡張子を入力して [OK]を選択します。(例:拡張子「iso」を持つファイルを例外設定するには、「.iso」 もしくは「iso」と入力)

この手順を繰り返して例外設定行うことにより、自身の環境に適したウイルススキャンをカスタマイズできます。作成した例外設定は、**ウイルススキャン用の例外設定**画面の**例外**で表示され、編集や削除の操作は、それぞれ [編集] と [削除] から可能です。

アイドリングスキャンでも例外を有効にする:アイドリングスキャンは、ユーザーがコンピュー タを利用しない時に自動的に起動するスキャン機能です。アイドリングスキャン中に、ユーザー が再び作業をはじめると、実行中のスキャンは中断されます。ユーザーはスキャンによるコン ピュータ速度の低下に悩まされることはありません。ここではアイドリングスキャンでスキャン 対象から除外するファイルやフォルダを指定します。

詳細設定

[詳細設定] からは、**ウイルススキャン**によるスキャンの詳細内容を確認したり、変更したりでき ます。

ファイルの種類(F): すべてのファイル 🗸
設定
アーカイブのスキャン(A) (サイズ制限なし)(B)
☑ ダイヤラ/スパイウェア/アドウェア/リスクウェアのスキャン(0)
ルートキットのスキャン(K)
☑新しいファイルと変更したファイルのみスキャン(n)
マログの作成(L)
🔲 リムーバブル メディアをスキャン(W)
OK キャンセル

以下の項目を設定できます。

- ファイルの種類: ウイルススキャンの対象になるファイルの種類を指定します。プログラムファイルとドキュメントのみを選択すると、速度優先でウイルススキャンします。
- ヒューリスティック: ウイルスデータベースに情報がないウイルス特有の特徴をもつ新種 ウイルスを検出します。この検出手法では、保護率を大幅に向上できますが、一方で、未 感染ファイルを感染ファイルと判断してしまう誤検出のケースもあります。
- アーカイブのスキャン: アーカイブ(ZIP、RAR、またはPSTなどの拡張子を持つファイル)をスキャンします。アーカイブのスキャンには、多くの時間を要します。ウイルスガードが常時システムを監視している場合には、アーカイブを解凍する時にアーカイブ内のウイルスを検出するので、この機能は無効にしておいてください。使用頻度が低い容量の大きなアーカイブのスキャンによるコンピュータの処理速度低下を防止するには、スキャンするアーカイブのサイズを制限します。
- メールアーカイブのスキャン: メールアーカイブをスキャンします。
- システム領域のスキャン: システム領域をスキャンします。この設定は常に有効にしてお いてください。
- ダイヤラ/スパイウェア/アドウェア/リスクウェアのスキャン:ダイヤラ、スパイウェア、アドウェア、リスクウェアなどの不正プログラムをチェックします。これらの不正プログラムは、望ましくないインターネット接続を勝手に確立したり、ブラウザの閲覧履歴やキーボードへの入力(パスワードなど)を不正に盗みだし、情報漏洩や金銭的な被害に発展する恐れがあります。

- **ルートキットのスキャン**: 従来型のウイルス対策ソフトによる検出方法では検出が困難な ルートキットをスキャンできます。
- 新しいファイルと変更したファイルのみスキャン: この機能を有効にすると、以前スキャンしたことがあり、その際に安全と判断されたファイルのスキャンを省略します。スキャンの対象は、新規作成ファイルや変更されたファイルのみがスキャンされるようになり、スキャン速度を向上させることができます。
- ログの作成: ウイルススキャンのログを記録します。ログを閲覧するには、起動画面の右 上のログアイコンをクリックします。
- リムーバブルメディアをスキャン: このチェックボックスを有効にすると、リムーバブル メディア(例: USBメモリ、USB外付けハードディスクなど)がコンピュータに接続され た際に、ウイルススキャンを実行するかを確認するメッセージボックスが表示されます。

更新

ワクチンやプログラム更新が機能しない場合には、この領域で設定を確認してください。更新を 利用するには、有効な**アクセスデータ(ユーザー名**と**パスワード)**が入力されている必要があ ります。アクセスデータは、製品の初回認証時に登録先メールアドレスに送信されています。

🍹 設定 アンチウイルス 更	鏩			;
± ± €				
設定 ▶ 一般 ▶ アンチウイルス	初回登録時に受け うイセンスをまだ <u>登</u>	/取ったアクセスデータを入力して、【連) 縁していない場合は、【ユーザー館延信	粗】 老クリックしてください。 小田用()】 老クリックしてください。	
> リアルタイム保護			ユーザー網羅(初期用)(1)
▶ ウイルススキャン ▶ 学新	ユーザー名(辺):		インターネッ	N設定()
▶ ウェブ保護	122-H000:	*******	キットワーク アク	ttスを管理(A)
> メールスキャン > 自動ウイルススキャン	ライセンス。	有助期間: 2016/07/03	755001011-	- ト/エクスポ ート
▶ 72FZパム	アクセスデータを 初	夫した場合(逆)	◎パージョン確認凶	
▶ ファイアウォール				
) ₹1-+-				
> 97(12 DVHD-W				
▶ バックアップ	☑ 自動的に229	シ更新を実行 (搭載)		課細設定创
		OK	キャンセル 適用(別)	へルプ

初めて認証を行う場合は、[ユーザー認証(初回用)]</u>を選択します。 <u>インターネット設定</u>で は、プロキシサーバーや更新ファイル用のサーバーを指定できます。

> 更新ネットワークを管理: ワクチンやソフトウェアアップデートのダウンロードを許 可するネットワークを選択できる機能です。Wi-Fiやモバイルネットワークでインター ネットに接続している環境でワクチンやプログラム更新を行うと、そのネットワーク でのダウンロードを許可するかどうか選択するダイアログが表示されます。そこで選 択した設定を、この機能で後から変更することができます。 例えば、外出時にモバイルネットワークを使用中に大量のデータ通信を行いたくない 場合、そのネットワークをブロック登録するのがお勧めです。

ワクチンのインポート/エクスポート(オフライン更新用): インターネット接続に制 約がある環境用のワクチンをインポート/エクスポートする機能です。ワクチンのイン ポート/エクスポートは、インターネットでG DATAのライセンス登録を行ったコン ピュータ上でのみ可能です。オフライン更新を利用する場合は、セキュリティの観点 から、できるだけ頻繁に更新することをお勧めします。

設定画面でインポートかエクスポートを選択し、ワクチン保存先フォルダを選択した 後でワクチン更新を行うと、指定したフォルダ内にワクチンデータが保存される、も しくは、フォルダ内からワクチンデータが読み込まれます。ワクチンデータをエクス ポートする際、使用中のワクチンがすでに最新の場合はエクスポートされませんので ご注意ください。

バージョンチェック: ワクチンファイルの差分更新を実行するかについて、設定できます。エンジンの破損や誤ってワクチンファイルを削除した場合以外は、通常、この設定は有効にしておいてください。

自動的にワクチン更新を実行: デフォルト設定の自動更新を利用しない場合にチェックを外しま す。なお、ワクチンが長期間更新されないと、コンピュータの保護レベルが著しく低下します。 この設定は、特殊なケースを除き無効化しないでください。もし更新間隔が短すぎる場合は、必 要に応じて実行頻度を調節してください。

実行頻度内の、毎日(インターネット接続時)、もしくは毎時(インターネット接続時)という 設定は、コンピュータがインターネット接続中かどうかを判断し、インターネットに接続してい る場合のみ更新処理を行う設定です。これはコンピュータを外へ持ち出している場合などに適し た設定で、不必要な処理を減らす事ができます。

ログを作成: ワクチン更新やウイルス検出などをログとして記録します。起動画面の右上にある ログアイコンをクリックすると、ログを閲覧できます。

ユーザー認証(初回用)

ユーザー認証が完了していない場合は、ここから**レジストレーション番号**を入力して認証を行う ことができます。ボックス製品を購入された場合は、レジストレーション番号はユーザー登録用 紙に記載されています。ダウンロード版を購入された場合は、メールで送信されています。

製品を認証するには、【ユーザー認証(初回用)】をクリックすると現れる画面に、レジストレ ーション番号、姓、名、メールアドレス(PC用)を入力し、[登録] をクリックします。認証が 正常に行われると、「登録に成功しました。アクセスデータは自動的に本製品に登録され、メ ールでもアクセスデータが送信されます。」というメッセージが表示されます。[OK] をクリッ クして、この画面を閉じます。

注意: アクセスデータは、ここで登録したメールアドレスに送信されます。メールアドレス入力の際は、誤入力のないようにご注意ください。アクセスデータは、再インストールまたは2台目以降のPCを認証する際(複数台版を購入の場合)に必要です。

認証後は、ユーザー名とパスワードの入力欄に生成されたアクセスデータが自動的に入力されま す。これで更新を実行できるようになります。

認証に失敗する場合

まず、ブラウザを使ってインターネットに正常に接続されているか確認してくださ い。ブラウザでインターネット閲覧できるにもかかわらず更新できない場合は、プロ キシサーバーに問題がある可能性があります。この場合は、<u>インターネット設定</u>を選 択して、プロキシサーバーに入力されている情報を確認してください。

レジストレーション番号と連絡先を入力してください。アクセスデータは、自動的に G Data トータル プロテクション 2014 に登録され、入力したメールアドレスにも送信されます。
レジストレーション番号(R)
 クイック登録(必須項目のみ) 詳細登録
ユーザーデータ
姓:*(N)
名:*(V)
メールアドレス:*(E)
メールアドレス再入力:*(B)
☑ G Data から製品やサービス情報が提供されることに同意します。
登録 単立とリレー

インターネット設定

プロキシサーバー を使用する環境では、プロキシサーバーを使用にチェックを入れてください。この設定は、インターネット更新が正常に機能しない場合にのみ変更します。プロキシサーバーの入力欄で入力する情報については、システム管理者またはインターネット接続プロバイダに確認してください。アクセスデータは必要に応じて入力してください。

インターネット設定	Ē	
プロキシ サーバー	使用(S)	
アドレス(A)	ポート(0)	80 (標準: 80)
アクセスデータ ユーザー名(E): パスワード(W)		
地域 アジア (日本)		•
	ОК	キャンセル

プロキシサーバー: プロキシサーバーは、ネットワーク内のPCからのリクエストを束 ねてインターネットに接続します。社内ネットワークなどにプロキシサーバーが導入 されている場合は、プロキシサーバーを使用にチェックを入れ、必要な情報を入力す ることで、更新が利用にできるようになります。

ウェブ保護

ウェブ保護を有効にすると、ウェブ閲覧中もコンピュータをマルウェアから保護することができ ます。ウェブ保護では次の設定が可能です。

 インターネットコンテンツ(HTTP)のスキャン: インターネット閲覧するだけで感染す る危険がある、ウェブページ経由のウイルスをスキャンします。ユーザーが閲覧しようと したコンテンツで不正プログラムを検出すると、そのコンテンツの実行をストップして、 コンピュータを感染から守ります。なお、ウイルスが検出された場合、ウェブページは表 示されません。この設定を有効にするには、インターネットコンテンツ(HTTP)のス キャンにチェックを入れます。

ウェプコンテンツのスキャンを無効にした場合は、ウイルスガードは必ず有効にしてく ださい。不正プログラムの実行時に、ウイルスガードがこれを検出します。

特定サイトを例外に設定するには、例外の項を参照してください。 [詳細設定] から は、インターネットコンテンツ関連の設定を行うことができます。

- フィッシング保護: オンラインバンキング、オンラインショップ、ネットオークションの 偽サイトに誘導し、顧客データやログイン情報を盗むフィッシングサイトやその他の詐 欺、悪質サイトをブロックします。インターネットを閲覧する時は、常時有効化すること をお勧めします。
- 感染したウェブページのアドレスを送信: 危険と判断されたウェブページの情報をG
 DATA へ自動送信します。なお、このアドレスの送信は、匿名で処理されます。送信元が 特定できるデータは送信されません。収集データは、ユーザーがインターネットをより安 全に利用できるために役立てられます。
- ・オンラインバンキング対策: G DATA のオンラインバンキング対策機能「バンクガード」は、ネットバンキングを標的とするバンキング系トロイの木馬による中間者攻撃(man-in-the-middle攻撃)を検出し、リアルタイムで保護します。バンキング系トロイの木馬は、金銭的被害をもたらす悪質な不正プログラムで、現在、世界各国で猛威を振るっています。銀行サイトがオンライン取引の暗号化をしていても、攻撃は復号化されたブラウザ上で行われるため、通常のウイルス対策ソフトでは攻撃の回避が困難でした。G DATA 製品に搭載されているバンクガードは、ネットワークライブラリをリアルタイムでチェックすることにより、man-in-the-middle攻撃によるブラウザの不正操作を防止します。

キーロガー対策: コンピュータで入力したキー入力を不正に記録するプログラムを監視します。この機能は常時有効にしておく事をお勧めします。
 ※キーロガー対策は、文字入力にIMEを使用していない場合のみ効果があります。
 IMEを使用しない文字入力を行うには、「テキストサービスと入力言語」(Windowsの言語バーを右クリックして設定を選択することで開くことができます)を開き、「全般」画面で追加ボタンをクリックし英語(米国)などの英語入力を選択、適用して文字言語を追加します。
 その後、言語バーの言語設定をJPからENに変更する事でIMEを使用しない文字入力が行え、

その後、言語バーの言語設定をJPからENに変更する事でIMEを使用しない文字入力が行え るようになります。

1. 1. C		
 扱定 ▶ 一般 ▶ リアルタイム保護 ▶ リアルタイム保護 ▶ ウイルススキャン ▶ 要新 ▶ フェブ保護 ▶ メールスキャン ▶ 首加ウイルススキャン ▶ 首加ウイルススキャン ▶ コウイズびた ▶ ファゲイズの本 	インダーネット コンダング (HTTP)	0 :(E)
▶ デューナー ▶ デバイス コントロール ▶ パックアップ	OK キャンセル 透用(の) A	1.J

例外

ウェブサイトを例外として設定するには、次の手順に沿って行います。

【例外】をクリックします。そうすると、**ウェブ保護用の例外設定**の画面が開きます。 この画面では、ユーザーが安全なサイトとして登録したページが表示されます。

ップできます。		19 るととて、ワエノ休護の	CPT-CA	
ウェブアドレス (URL)	追加済み	説明		新規作成(<u>N</u>)
gdata.co.jp	2013/05/14			編集(B)
				削除(L)
			>	

- 2 例外のウェブサイトをウェブ保護用例外に追加するには、[新規作成] をクリックします。入力画面が開くので、URL の欄にウェブページのアドレス(例: www.gdata.co. jp)と、必要に応じて説明の欄に登録の理由などを入力します。
- **3** [OK] をクリックすると、ウェブページが例外サイトとして追加され、ウェブ保護の対象から除外されます。

例外に登録したウェブページの編集や編集は、登録した項目を選択し、編集の場合は[編集] を、削除の場合は[削除]をクリックします。

詳細設定

ウェブ保護が監視するサーバーポート番号を設定します。デフォルト設定では、通常のインター ネット閲覧に使用する 80 が設定されています。

 ブラウザのタイムアウトを防止: インターネットコンテンツ(HTTP)のスキャンに チェックを入れた場合、ウェブコンテンツをブラウザに表示する前に不正ルーチンの チェックが行われます。この処理はデータ量によっては処理時間がかかり、ブラウザが表 示データをすぐに受信できないため、エラーメッセージが表示されることがあります。ブ ラウザのタイムアウトを防止にチェックを入れると、このエラーメッセージが表示され ず、コンテンツ全体のチェックが終了するとウェブページが通常どおり表示されるように なります。

 ダウンロードの容量制限:指定したサイズを超過したダウンロードファイルでのインター ネットコンテンツ(HTTP)のスキャンを解除します。この容量制限を利用することで、 インターネットコンテンツ(HTTP)のスキャンによるインターネットの通信速度低下 を回避できるます。なお、容量制限した場合は、ウイルスガードは必ず有効にしておいて ください。

▼ インターネット コンテンツ(HTTP)	X
サーバー ポート番号 (複数の番号を入力する場合は、コンマ (,) で区切ってください)(S):	
80,443 標準	
☑ ブラウザのタイムアウトを防止(Z)	
ダウンロード	
ダウンロードの容量制限(G)	
次の容量までのダウンロードをスキャン(D): 2 MB	
ок <i>キャン</i> セル	,

メールスキャン

メールスキャンは、送受信メールや添付ファイルでウイルススキャンする機能です。メールス キャンで検出した添付ファイルは、削除や修復の操作ができます。

7 設定 アンチウイルス	メールスキャン)
±. ±. €	
SIR ⇒ 一版 ⇒ リアルタイム保護 ⇒ リアルタイム保護 ⇒ リアルススキャン ⇒ 発照 ⇒ ウエブ環想 ⇒ メールスキャン ⇒ 回動ウイルススキャン ⇒ 回動ウイルススキャン ⇒ アンチスパム ⇒ ファイアウォール ⇒ チューナー > デパイスコントロール	登電メール 協迎した特徴(1): (ワイルス群隊(不可能な場合は歩付ファイル / 本文を制除) ◆ 図 受電メールのスキャン(P) 図 医強メールへのレポート沖付(F)
	送燈メール 図 送儀券のメールスキャン(M)
	スキャンオブション エンジンの確認(F): 2つのエンジン(推発) ・ 図 アウトブレイクシールド(0)
▶ バックアップ	計冊時年 (\overline{n})
	OK キャンセル 適用(8) ヘルプ

メモ: Microsoft Outlook には、専用プラグインがインストールされます。このプラ

グインは、Outlook 上でより簡単なウイルスチェックを実現するツールです。メール スキャンで設定できる POP3/IMAP ベースの保護と全く同じ機能を提供します。メー ルまたはフォルダのスキャンを実行するには、Outlook メニューバーの [ツール] > [フォルダのウイルスをスキャン] を選択します。

受信メール

受信メールでは、次の設定が可能です。

- 感染した場合: 感染メールが検出された場合の処理方法を設定します。コンピュータ環境に応じて、最適な設定を選択してください。通常は、ウイルス駆除(不可能な場合は添付ファイル/メール本文を削除)の使用をお勧めします。
- 受信メールのスキャン: インターネット接続中の全受信メール に対して、ウイルススキャンを実行します。
- ・感染メールへのレポート添付:ウイルスが検出された場合、感染メールの件名欄に「ウイルス」という警告を挿入します。また、メール本文の先頭に「注意!このメールはウイルスに感染しています」というメッセージ、ウイルスの名称、ウイルスの駆除または感染ファイルを修復したなどの情報を表示します。

送信メール 送信メールでは、次の設定が可能です。

 送信前のメールスキャン: ウイルス添付メールの外部送信を防ぐために、送信前にチェックします。この機能が有効な場合に、ウイルス添付メールを送信しようとすると、「メール [件名] には次のウイルスがあります: [ウイルス名]」というメッセージが表示され、メールの送信はブロックされます。

スキャンオプション

スキャンオプションでは、基本的なウイルススキャンの基本的な設定を行います。次の設定が可 能です。

- エンジンの種類: ウイルススキャンに使用するエンジンを選択します。G DATAには、2 種類の高性能ウイルス検索エンジンを搭載し、世界最高レベルのウイルス検出率を実現しています。通常は、2つのエンジン(最高検出力/推奨)に設定してください。もしコン ピュータの処理速度に問題がある場合は、1種類のエンジンのみを使用することにより、 パフォーマンスを改善することもできます。
- アウトブレイクシールド:パンデミック型のウイルス感染メールを常時監視してブロック するクラウド型機能、アウトブレイクシールド (OutbreakShield)を有効/無効を設定し ます。アウトブレイクシールドを有効にすると、受信メールにチェックサムが作成され、 クラウド上のアンチスパムブラックリストと照会が行われます。これにより、ワクチンに

依存することなく、ウイルスが最初に発見された時点から数十秒から数分内でウイルスメ ールとして検出できます。

暗号化された接続

メールやメールアカウントのセキュリティを高めるため、メールプロバイダによってはSSLを採 用していますが、SSLメールでもウイルス対策ソフトによるチェックをすることをお勧めしま す。

G DATA はSSL通信でのメールチェックを可能にする**暗号化された接続 (SSL) モジュール**を提 供しています。この機能を使うには、G DATA の証明書をエクスポートし、その後、メールプロ グラム側にインポートする必要があります。

このモジュールは、証明書のインストールもしくは Windows 証明書ストアへのアクセスが可能 なすべてのメールプログラムで利用できます。

本機能を利用可能なメールプログラムの一例:

- Outlook 2003 or higher
- Thunderbird
- The Bat
- Pegasusmail

G DATA 証明書が自動インストールされていない場合は、以下の手順に沿ってください:

- 1. 証明書のインストール中は、メールプログラムは非アクティブである必要があります。証 明書の生成・インストール時には、必ずすべてのメールプログラムを閉じてください。
- 2. G DATA の起動画面の右上の歯車アイコンを押し、表示された画面の左側領域でメールス キャンを選択します。
- 3.「証明書をエクスポート」ボタンを押して、証明書の保存場所を指定し、「OK」を選択 します。証明書ファイルは GDataRootCertificate.crt という名前で保存されます。
- 4. GDataRootCertificate.crt ファイルを開いてください。PC に証明書をインストールする ためのダイアログが表示されます。
- 5. ダイアログ画面内の「**証明書のインストール**」を押し、ウィザードに従ってインストール を進めます。
- これで作業は完了です。Outlook および Windows 証明書ストアにアクセスできるすべてのメー
ルプログラムにSSLを利用する受信メールでスキャンする設定を完了しました。

メモ: Thunderbird (Portable)の環境下で証明書が自動インポートされない場合は、以下の方法で後から証明書をインポートして、G DATA 証明書を信頼する認証局に設定する必要があります。

- 1. Thunderbird (Portable) で「**証明書を表示」 (オプション > 詳細 > 証明書**) を押しま す。
- 2. ここを押すと、証明書マネージャが表示されます。認証局証明書タブを選択し、次に「インポート」ボタンを押します。
- 3. **証明書のインポート**ダイアログが表示されるので、上で作成した GdataRootCertificate を選択します。
- 4. 続いて、"G DATA Mail Scanner Root" が行う認証のうち、信頼するものを選択します。

以下の項目の横にあるボックスにチェックを入れて「OK」を押すと、Thunderbird (Portable) は G DATA で保護されるようになります:

- この認証局による Web サイトの識別を信頼する
- この認証局によるメールユーザの識別を信頼する
- この認証局によるソフトウェア製作者の識別を信頼する

他のメールプログラムでも、Thunderbird と似たような証明書のインポート機能がありま す。設定方法がわからない場合は、メールプログラムのヘルプファイルを参照してください。

詳細設定

メールプログラムに標準ポートを割り当てていない場合には、メールの送受信に使用するポート をサーバーポート番号の欄に入力してください。[標準] をクリックすると、自動的に標準のポ ート番号にリセットされます。複数のポートをスキャンさせたい場合は、コンマ(,) でそれぞ れのポート番号を区切って入力してください。

メモ: Microsoft Outlook には、専用プラグインがインストールされます。このプラ グインは、Outlook 上でより簡単なウイルスチェックを実現するツールです。 Outlook プラグインを使うと、Outlook 上で簡単な操作でメールスキャンができるよ うになります。スキャンを実行するには、スキャンする対象のメールまたはフォルダ を選択し、G DATA アイコンをクリックして実行する操作を選択します。

G DATA のメールスキャンは、メールプログラムが実際にメールを受信する以前に処理を行うた

め、大量のメールを受信する場合やインターネット回線速度が遅い環境では、メールプログラム がタイムアウトのエラーメッセージを表示することがあります。この原因は、メールスキャンに よるスキャンで、メールプログラム側でのメール受信で遅延が発生するためです。メールクライ アントのタイムアウトを防止にチェックを入れると、タイムアウトエラーが表示されなくなりま す。受信メールは、スキャン完了次第、メールプログラムに引き渡されます。

	-	
図 愛信メールの処理(POP3)	(P)	
サーバーボート番号(複数	教入力する場合は、コンマ()で区切ってくださ	(V):
110	(A) (A)	
図メール クライアントの	タイムアウトを防止(Z)	
受信メール (IMAP)		
■受信×ールの処理(IMAP)	(1)	
サーバーボート番号(複数	取入力する場合は、コンマ(,)で区切ってくださ	(N):
143	雪莲(D)	
マメール クライアントの	タイムアウトを防止(1)	
送信メール(SMTP)		
送信メール(SMTP) 夏送信メールの処理(SMTP)	(5)	
送信メール(SMTP) 図送信メールの処理(SMTP) サーバー ポート番号(接) (5) 原入力する場合は、コンマ(。)で送切ってくださ	(U) (M):
送信メール (SMTP) 図送信メールの処理 (SMTP) サーバー ボート番号 (御日 25) (5) 取入力する場合は、コンマ(。)で巡切ってくださ 篠座(<u>5</u>)	(VI) (M):
送徳メール (SMTP) 図 送徳メールの処理 (SMTP) サーバー ポート番号 (被引 25 図 メール サーバーのタイ)(5) (5) (京入力する場合は、コンマ()で空切ってくださ (標準(<u>5</u>) ムアウトを防止(U)	(M):

自動ウイルススキャン

ユーザーがコンピュータを使用していない時にスキャンが自動実行されるアイドリングスキャン 機能やスキャン対象、スキャン実行日時や頻度、エンジンの種類などをカスタムしたスケジュー ルスキャンを設定できます。

ウイルススキャンのスケジュール設定で、[新規作成] をクリックします。ダイアログ画面が開く のでまず名前を入力し、必要な項目を設定してください。例えば、ダウンロードしたファイルを 毎日特定の時間にスキャンする場合は、スキャン範囲の次のフォルダとファイルをスキャンを 選択し、[選択] ボタンから対象フォルダを選択します。次にスケジュールの実行頻度で毎日を 選択、そして時間を設定して、[OK] をクリックすれば設定は完了です。

激定 ▶ 一級 ▶ アンチウイルス	アイドリングスキャン システムザアイドリング状態になった場合に、目動的にスキャンを行います。 図目物(性質)(5)			
▶ リアルタイム保護 ▶ ウイルススキャン	ウイルススキャ	ンのスケジュール被走(G)		
 ▶ 更新 ▶ ウェブ深淡 ▶ メールスキャン ▶ 自動ウイルススキャン 	名前	業行	次照の起動	新聞の起動
> アンチスパム > ファイアウォール				
#2-+-	4			5
デバイス コントロール バックアップ	今日く間治(3) 新規	作成(因) プロバラ	イ(E) 別除(L)

一般

新規作成する自動ウイルススキャンジョブに名前をつけます。ジョブにはわかりやすい名前をつ けてください。

🔽 自動ウイルススキャン	-般 ×
 日勤ウイルススキャン ー般 スキャン範囲 スキャン範囲 スキャン範囲 スキャン範囲 スキャン範囲 スキャン総理 スキャン総定 スキャン設定 ユーザーアカウント 	名前(1): 定照スキャン1 スキャン終了後にコンピュータの重度を切る(ユーザーがログインしていない場合)
	OK キャンセル ヘルプ

スキャン終了後にコンピュータの電源を切る(ユーザーがログインしていない場合)にチェックを入れると、スキャン後にコンピュータを自動的にシャットダウンします。

ジョブ:実行されるウイルススキャン処理の単位をジョブと呼びます。

スキャン範囲

ウイルススキャンを実行する対象を設定します。スキャンの対象は、ローカルのハードディスク ドライブ、メモリとスタートアップ、次のフォルダとファイルをスキャンから選択できます。 次のフォルダとファイルをスキャンを選択した場合は、[選択]をクリックすると対象を指定しま す。

自動ウイルススキャン	● ローカル ハードディスク ドライブをえ	(キャン(L))	例外(因)
一般	③ メモリとスタートアップをスキャン(M)	
スキャン範囲	⑦ 次のフォルダとファイルをスキャン(別)):	递织(S)
スケジュール			
> スキャン設定			
ユーザー アカウント			
			hand the second
自動ウイルススキャン 例外	ン用の例外設定	×	
自動ウイルススキャン 例外 種類 反 例	ン用の例外設定 外設定 X	X 新規作成(<u>N</u>)	
自動ウイルススキャン 例外 種類 反例	ン用の例外設定 外設定 X	★ 新規作成(N) ^{运使(F)}	
自動ウイルススキャン 例外 種類 反 例	ン用の例外設定 外設定 X ト ドライブ(R)	新規作成(<u>U</u>) 編集(E)	
自動ウイルススキャン 例外 種類	ン用の例外設定 外設定 X ト ドライブ(R) フォルダ(T)	新規作成(<u>U</u>) 編集(E) 削除(D)	
自動ウイルススキャン 例外 種類 の の の の の の の の の の の の の	ン用の例外設定 外設定 X ト ドライブ(R) フォルダ(T) ファイル応選子(D)	新規作成(<u>U</u>) 編集(E) 別除(D)	
自動ウイルススキャン 例外 種類 の外 の の の の フ フ	>用の例外設定 外設定 X トライブ(R) フォルダ(T) ファイル辺張子(D) オルダ(D):	X 新規作成(1) 編集(E) 削除(D)	
自動ウイルススキャン 例外 種類 で 例 の の こ て こ	ン用の例外設定 外設定 × トライブ(R) ・フォルタ(T) ファイル辺張子(D) オルダ(I): :WProgram Files (x86) …	× 新規作成(<u>))</u> 編集(E) 削除(D)	
自動ウイルススキャン 例外 種類 又 例 の の フ て C	ン用の例外設定 外設定 × トライブ(R) フォルタ(T) ファイルが感子(D) オルダ(D): :¥Program Files (x86) …	新規作成(1) 編集(E) 削除(D)	
自動ウイルススキャン 例外 種類 の外 の の つ こ こ こ	ン用の例外設定 外設定 X ト ドライブ(R) フォルダ(T) ファイル応選子(D) オルダ(I): :¥PPogram Files (x86) OK キャンセル	新規作成(1) 編集(E) 削除(D)	

フォルダとファイルの選択: フォルダのツリー構造で「+」をクリックするとそのフォルダが展開し、フォルダの内容がファイルビューに表示されます。チェックが入っているフォルダまたはファイルがスキャンの対象になります。なお、フォルダ内ですべてのファイルがマークされるとチェックマークは黒で表示されます。一部のファイルが選択されていないフォルダは、グレーのチェックマークで表示されます。

日 🗹 💼 デスクトップ	ファイル名	サイズ 種類
◎ 団 帰 コンピューター	🕑 📴 お気に入り	ファイル フォ.
申日書 フロッピー ディスクドライフ (A:)	🕑 📑 マイ ビデオ	ファイル フォ.
③ (二) 急 pup ドライゴ (p)	🕑 📓 マイ ビクチャ	ファイル フォ.
	🕑 🐞 ダウンロード	ファイル フォ.
a 🖓 🎽 Test Account & Deta	🖃 🕌 マイ ミュージック	ジァイル ジ オ・
- 二 参しいフォルダー	🖃 🎒 保守したゲーム	ファイル フォ
	☑ ≧アドレス様	ファイル フォ
	🗔 🎉 純常	ファイル フォ
	📋 🍡 デスクトップ	
	📋 🌒 リンク	ファイル フォ
	📋 📑 マイ ドキュメント	ファイル フォ.
	4 30	,

スケジュール

ジョブを実行するタイミングを設定します。実行のタイミングは、**実行頻度と時間**を組み合わせ て設定します。**実行頻度でシステム起動時**を選択した場合は、**時間**は非表示となります。

- スケジュール実行後にコンピュータの電源が切れていた場合、次回の起動時にジョブを 実行: コンピュータを起動していなかったため実行できなかったスキャンジョブを、コン ピュータの次回起動した時に自動的に実行します。
- バッテリモードでは実行しない: ノートパソコン用の設定です。バッテリー駆動時はス キャンジョブを実行せずに、AC電源での駆動時にスキャンジョブを実行します。

🔽 自動ウイルススキャン	スケジュール X
 自動ウイルススキャン ▶ 一般 ▶ スキャン範囲 ▶ スケジュール ▶ スキャン設定 ▶ ユーザー アカウント 	実行頻度 1 回のみ(Q) 毎月(M) ● 毎時(H) ● システム起動時(U) ● 毎日(D) ● 無運(W) ● 無運(W) ● ● ● ● 無運(W) ● ● ●
	OK キャンセル ヘルプ

スキャン設定

自動ウイルススキャン用のスキャン設定について定義します。

🔽 自動ウイルススキャン	スキャン設定				×
自動ウイルススキャン → 一般 → スキャン範囲 > スキャン範囲 > スキャン設定 > ユーザー アカウント 	エンジンの種類(E): 感染したファイル(D): 感染したアーカイブ(<u>C</u>): 回高システム負荷時には	2つのエンジン(信用 ウイルス駆除(不可) ログを残すのみ ウイルススキャンを併	i検出力/推奨) 能な場合は隔離) 章止(<u>5</u>)		・ ・ 詳細設定(<u>w</u>)
			ОК	キャンセル	ヘルプ

- エンジンの種類: ウイルススキャンに使用するエンジンを選択します。G DATAには、2 種類の高性能ウイルス検索エンジンを搭載し、世界最高レベルのウイルス検出率を実現し ています。通常は、2つのエンジン(最高検出力/推奨)に設定してください。もしコン ピュータの処理速度に問題がある場合は、1種類のエンジンのみを使用することにより、 パフォーマンスを改善することもできます。
- 感染したファイル: 感染ファイルが検出された場合の処理方法を設定します。デフォルト 設定では、ウイルスが検出されるとウイルスと感染ファイルについてのログが残されま す。最高セキュリティで保護するには、ウイルス駆除(不可能な場合は隔離)に設定し ます。
- ・感染したアーカイブ: アーカイブファイル(RAR、ZIP または PST などの拡張子を持つ ファイル)を通常ファイルと別扱いするかどうかを設定します。なお、アーカイブファイ ルを隔離すると、元に戻す場合にファイルが破損する場合があります。感染したアーカイ ブは、ログを残すのみを選択し、検出の度に処理方法をユーザーが選択することをお勧め します。
- 高システム負荷時にはウイルススキャンを停止: ユーザーがコンピュータ上で作業しない 状態になると、スキャンが自動で実行されます。スキャン実行中にコンピュータを使用す ると、スキャンは中断されます。中断されたスキャンは、再びコンピュータで作業をしな い状態になった場合に再開されます。

[詳細設定]からはスキャン詳細設定の編集や確認ができます。

ファイルの種類(F):	すべて	のファイル	1	•
設定				
☑ ヒューリスティッ	ク(H)			
🔽 アーカイブのスキ	-ヤン(A)	(サイス	ズ制限なし)(<u>B)</u>
👿 メール アーカ	コイブのスキ	ヤン(M)		
☑ システム領域の2	(キャン(S)			
☑ ダイヤラ/スパイ	ウェア/アド	ウェア/リス	マクウェアのス	ペキャン(0)
ℤルートキットのフ	(キャン(K)			
☑ 新しいファイルと	変更したフ	アイルのみ	スキャン(n)	

次の設定が可能です。

- ファイルの種類: スキャン対象とするファイルの種類を選択します。
- ヒューリスティック: ウイルスデータベースに情報がないウイルス特有の特徴をもつ新種 ウイルスを検出します。この検出手法では、保護率を大幅に向上できますが、一方で、未 感染ファイルを感染ファイルと判断してしまう誤検出のケースもあります。
- アーカイブのスキャン: アーカイブ(ZIP、RAR、またはPSTなどの拡張子を持つファイル)をスキャンします。アーカイブのスキャンには、多くの時間を要します。ウイルスガードが常時システムを監視している場合には、アーカイブを解凍する時にアーカイブ内のウイルスを検出するので、この機能は無効にしておいてください。使用頻度が低い容量の大きなアーカイブのスキャンによるコンピュータの処理速度低下を防止するには、スキャンするアーカイブのサイズを制限します。
- メールアーカイブのスキャン: メールアーカイブをスキャンします。
- システム領域のスキャン: システム領域をスキャンします。この設定は常に有効にしてお いてください。
- ダイヤラ/スパイウェア/アドウェア/リスクウェアのスキャン:ダイヤラ、スパイウェア、アドウェア、リスクウェアなどの不正プログラムをチェックします。これらの不正プログラムは、望ましくないインターネット接続を勝手に確立したり、ブラウザの閲覧履歴やキーボードへの入力(パスワードなど)を不正に盗みだし、情報漏洩や金銭的な被害に発展する恐れがあります。
- **ルートキットのスキャン**: 従来型のウイルス対策ソフトによる検出方法では検出が困難な ルートキットをスキャンできます。
- **ログの作成**: ウイルススキャンのログを記録します。ログを閲覧するには、起動画面の右 上のログアイコンをクリックします。

ユーザーアカウント

コンピュータがネットワークに接続されている環境で、接続先もスキャン対象とする場合は、接 続先へのアクセス権が必要となります。アクセスに必要な**ユーザー名、パスワード、ドメイン**を 入力してください。

自動ウイルススキャン スキャン対象のネッ クセス権限が必要で ネットワークドライ ト 一般 ネットワークドライ ト スキャン範囲 ト スケジュール ユーザー名(U): [
・ユーザーアカウント パスワード(<u>₩</u>): ドメイン(<u>D</u>):

アンチスパム

スパムフィルタ

スパムフィルタは、スパムメールが持つ特長をもとに数値を算出し、スパムメールを効果的にブロックする機能です。スパムフィルタを有効にするには、**スパムフィルタを使用**にチェックを入れます。

🔽 設定 アンチスパム ス	マパムフィルタ	×
⊥ ⊥ ∉		
設定	☑ 受信メールのフィルタ(E)	
▶ 一般	☑ スパムフィルタを使用(F)	
▶ アンチウイルス	☑ スパム アウトブレイクシールド(0)	
▶ アンチスパム	☑ ホワイトリストを使用(₩)	
▶ スパムフィルタ	☑ ブラックリストを使用(៤)	
▶ フィルタの追加	図 リアルタイム ブラックリスト(デフォルト設定)を使用(<u>t</u>)	
▶ その他	☑ キーワード (メール本文) を使用(≦)	
▶ ファイアウォール	☑ キーワード (件名) を使用(<u>S</u>)	
▶ チューナー	図 コンテンツ フィルタを使用(I)	
▶ デバイス コントロール		
▶ バックアップ	处理方法(<u>R</u>)	
	上級者用設定(<u>P</u>)	
	OK キャンセル 適用(<u>B</u>) ヘルプ	

スパムフィルタの項目の有効/無効の切換えはチェックボックスで行います。各スパムフィルタ 項目の設定を変更するには、項目をクリックすると表示される画面から行います。スパムフィル タには、次の項目があります。

- スパム アウトブレイクシールド:パンデミック型のウイルス感染メールを常時監視してブロックするクラウド型機能、アウトブレイクシールド (OutbreakShield)を有効/無効を設定します。アウトブレイクシールドを有効にすると、受信メールにチェックサムが作成され、クラウド上のアンチスパムブラックリストと照会が行われます。これにより、ワクチンに依存することなく、ウイルスが最初に発見された時点から数十秒から数分内でウイルスメールとして検出できます。プロキシサーバーを使用している環境では、[インターネット設定]をクリックし、設定の変更を行ってください。この設定はアウトブレイクシールドが機能しない場合にのみ変更してください。
- ホワイトリストを使用:特定のメールアドレスやドメインから送信されるメールを、スパムとして判定しないように設定できます。ホワイトリストに登録するには、ホワイトリストを使用を選択すると表示されるウィンドウ上の[新規作成]をクリックし、送信者アドレス/ドメインの欄にスパム判定から除外するメールアドレス(例:newsletter@gdata.co.jp)またはドメイン(例:gdata.co.jp)を入力して、[OK]をクリックします。そうする

と、入力された送信者またはドメインからのメールを、スパムではないと判定されるよう になります。

また、【インポート】をクリックすると、既存のメールアドレスまたはドメインのリストを ホワイトリストに追加できます。インポート用のリストを作成するには、Windows の「メ モ帳」などのテキストエディタプログラムを利用し、テキスト形式(txt ファイル)で作成 します。また、キーワードリストは、必ず1件1行ずつ、上から順に入力してください。 【エクスポート】からは、ホワイトリストをテキスト形式で書き出します。

ブラックリストを使用:特定のメールアドレスやドメインから送信されるメールを、スパムとして判定するように設定できます。ブラックリストに登録するには、ブラックリストを使用を選択すると表示されるウィンドウ上の[新規作成]をクリックし、送信者アドレス/ドメインの欄にスパム判定するメールアドレス(例:newsletter@spam.co.jp)またはドメイン(例:spam.co.jp)を入力して、[OK]をクリックします。そうすると、入力された送信者またはドメインからのメールは、自動的にスパムと判定されるようになります。

また、【インポート】をクリックすると、既存のメールアドレスまたはドメインのリストを ブラックリストに追加できます。インポート用のリストを作成するには、Windows の「メ モ帳」などのテキストエディタプログラムを利用し、テキスト形式(txt ファイル)で作成 します。また、キーワードリストは、必ず1件1行ずつ、上から順に入力してください。 【エクスポート】からは、上述のブラックリストをテキスト形式で書き出します。

- リアルタイムブラックリストを使用: スパム送信に使用されているサーバーのブラックリストをもとに、受信メールがスパムメールであるかどうかを確かめます。サーバーがリストに掲載されていれば、スパムの可能性は高くなります。この設定はデフォルト設定のままでの使用をお勧めますが、カスタムも可能です。
- キーワード (メール本文)を使用:メール本文に使用されている単語をもとに、スパムメ ールかどうかを判断します。リスト内の1 個以上の単語がメール本文に使用されている と、スパムの可能性が高まります。キーワードのリストは、[新規作成]、[編集]、[削除] が可能です。また、[インポート]をクリックすると、自身で作成したキーワードリスト を追加できます。インポート用のリストを作成するには、Windowsの「メモ帳」などの テキストエディタプログラムを利用し、テキスト形式(txt ファイル)で作成します。ま た、キーワードリストは、必ず1 件1行ずつ、上から順に入力してください。[エクスポ ート] からは、既存のキーワードリストをテキスト形式で書き出します。完全なキーワ ードのみ検索にチェックを入れると、完全に一致する単語だけを検索します。
- キーワード(件名)を使用:メールの件名に使用されている単語をもとに、スパムメール かどうかを判断します。リストの1 語以上が件名に使用されていると、スパムの可能性 が高まります。キーワードの編集は、キーワード(メール本文を使用)と同様の操作で 行います。
- コンテンツフィルタを使用: コンテンツフィルタは自己学習型フィルタで、メール本文の 単語を基準にしてスパムの可能性を計算します。このフィルタは、変更できない単語リストだけを基準にして機能するのではなく、新着メールが届くたびに学習してリストを拡張していきます。[テーブルコンテンツを検索]をクリックすると、メールをスパムに分類するコンテンツフィルタが使用している単語リストを表示できます。[テーブルをリセット]をクリックすると学習したテーブルの内容がすべて削除され、自己学習型コンテンツフィルタが学習プロセスを最初からやり直します。

<u>処理方法</u>

スパムフィルタによるスパムメールへの応答方法を定義します。スパムの疑いがあるメールの処 理方法は、スパム判定された3種類の段階で設定できます。

5	処理方法		×
	一処理方法		
	スパムの可能性: メールを受信; スパム警告を挿入; メールを移動	変更(<u>N</u>)	
	スパムの可能性が高い: メールを受信; スパム警告を挿入; メールを移動	変更(<u>D</u>)	
	スパムの可能性が非常に高い: メールを受信; スパム警告を挿入; メールを移動	変更(<u>E</u>)	
	0K キャンセル	へレプ(<u>H</u>)	

- スパムの可能性があるメール:スパムの特徴を持つメールが検出された場合の処理ルール を設定します。ここに振り分けられたメールには、受信者が配信を希望するニュースレタ ーが紛れ込むこともあります。そのため、受信者にはスパムの可能性を通知する設定をお 勧めします。
- スパムの可能性が高いメール:スパムの要素を多数持っているメールが検出された場合の 処理ルールを設定します。この中にはまれに受信者が配信を希望するメールが含まれることもあります。
- スパムの可能性が非常に高いメール: スパムメールの要件をすべて満たすメールが検出された場合の処理ルールを設定します。ここに配信を希望するメールが紛れ込むことはほとんどありません。ここに振り分けられたメールは受信拒否することをお勧めします。

この3 種類の処理方法は、それぞれ独自にカスタマイズできます。変更を行うには、**[変更]** をク リックします。

[変更] を押すと表示される画面内にあるメールを拒否にチェックを入れると、スパムと判断されたメールを受信トレイに入れません。また、メールの件名と本文にスパム警告を挿入に チェックを入れると、スパムと判断されたメールに警告を挿入します。Microsoft Outlook を 利用している場合は、メールをフォルダに移動からスパムの疑いのあるメールを受信フォルダ内 の任意のフォルダ(デフォルト設定:アンチスパム)に移動できます。

> メモ:メーラーの仕分ルールを使用する事で、Microsoft Outlook を使用していない 場合でも、スパムと判断されたメールをフォルダに移動できます。メールを移動する には、件名欄に警告([Spam] など)を挿入し、使用しているメールプログラムで、警 告が挿入されたメールを別のフォルダに移動させるルールを作成します。

上級者用設定

スパム検出の基準として使用されるスパムインデックス値を詳細にカスタマイズできる上級者用 の設定です。専門知識を必要とする設定のため、通常はデフォルト設定のままで使用する事をお 勧めします。

フパムと認定する甘進	フパルわた除めする甘油
 (JーDiole's ジョンクリスト	✓ (Д) Skirts Back ☑ メールサイズ(Z)
1件名(J) 3 メール本文(T) ■ 最初のスパム可能性が確認される を使用しない(V)	5までリアルタイム ブラックリス

フィルタの追加

デフォルト設定では次のフィルタが有効になっていますが、チェックを外すことで無効にできま す。

- HTMLスクリプトの無効化: このフィルタは、メールのHTML部分のスクリプトを無効にします。HTMLスクリプトは、ウェブページで利用されるスクリプトですが、コンピュータを感染させるためにメールに埋め込まれて悪用されることがあります。
- 有害な添付ファイルのフィルタ:メールに添付されている危険な添付ファイルをフィルタします。多くのメールウイルスは、EXEファイルや画像(動画または音楽)ファイルに仕掛けられたVBスクリプトや隠し実行ファイルが含まれる添付ファイルを通して広がります。メールの添付ファイルを実行する際は、十分に注意してください。場合によっては、送信者に確認するのも感染から有効な手段の1つです。

設定 ▶ 一般	図HTMLスクリプトの無効化(H) 図 有書な添付ファイルのフィルタ(A) ○ フィルタ リスト(D)		
 ▶ アンチジイルス ▶ アンチスパム ▶ スパムフイルタ ▶ フィルタの追加 	名前 ☑ スクリプト ☑ 有害な添付ファイルの名前を変更 ■ 言語フィルタ	 種類 HTML スクリプトの無効化 添付ファイルのフィルタ 	説明 必要としない言語ℓ
 ▶ その他 ▶ ファイアウォール ▶ チューナー ▶ ディーナー 			
▶ テハイス コントロール ▶ バックアップ	C m		>
	新規作成(<u>N</u>)	プロパティ(E) 削除(<u>L</u>)	統計情報(S)

新規フィルタを追加するには、**[新規]** をクリックし、表示されたダイアログ画面でフィルタの種 類を選択して**[OK]** をクリックしてください。続いて選択したフィルタの設定アシスタント画面 が開くので、必要な情報を入力して **[OK]** をクリックします。フィルタを削除するには、対象の フィルタを選択して、**[削除]** をクリックします。

以下が選択可能なフィルタの種類です。各フィルタの設定方法を解説します。

添付ファイルのフィルタ:メールに添付されている危険な添付ファイルをフィルタします。

ファイル拡張子では、フィルタに適応する拡張子を指定します。指定できる拡張子の種類 は、実行ファイル(EXEファイルやCOMファイルなど)の他、画像/動画/音楽ファイル (MPEG/AVI/MP3/JPEGなど)や圧縮ファイル(ZIP/RAR/CABなど)の拡張子も フィルタできます。複数の拡張子を指定する際は、それぞれの拡張子をコンマ(,)で区切 ります。

添付ファイルのみ名前を変更にチェックを入れると、フィルタする添付ファイルは自動削除されずに、ファイル名が変更されます。ファイル名を変更すると、実行ファイルや実行可能なスクリプトやマクロを含む Microsoft Office 形式のファイルをクリックしただけでは実行できないので、誤ってクリックしての感染などを未然に防ぐことができます。ファイル名が変更されたファイルを実行するには、ユーザーはファイルを任意の場所に保存し、本製品によって付与された拡張子(デフォルト設定では_danger)を消去する必要があります。危険とみなされたファイルに付与する拡張子はユーザーが自由に設定できます。添付ファイルのみ名前を変更にチェックを入れない場合は、フィルタされたファイルはすぐに削除されます。

メール本文にメッセージを挿入にチェックを入れると、危険な添付ファイルが含まれていた場合、判断されたメールにテキストを挿入し、添付ファイルが削除された(もしくは名前が変更された)ことをユーザーに知らせます。

コンテンツフィルタ: コンテンツフィルタは、特定のテーマまたはテキストを含むメールの受信をブロックします。コンテンツフィルタを設定するには、まず検索基準に、フィルタするキーワードと表現を入力します。論理演算子 AND および OR を使うと、キーワードや表現を複数入力できます。

検索範囲では、メールのどの部分でこの表現を検索するかを指定します。**ヘッダ**では、送 信者および受信者のメールアドレス、件名、メールプログラムの情報、プロトコル、送信 者情報がフィルタの対象となります。**件名**では、件名欄の内容だけをチェックします。

メール本文では純粋なテキストメール、**HTML テキスト**ではHTMLメールをチェックします。**埋め込みメール**では、コンテンツフィルタの対象を受信メールの本文に添付ファイルが埋め込まれているメールをフィルタ対象とするかどうかを指定します。

処理方法では、スパムと判断されたメールの処理方法を設定します。メールの件名と本文 に警告を挿入にチェックを入れると、疑わしいメールの件名欄の件名の前に「スパム」ま たは「注意」などの警告([件名に追加する文字])を挿入できます。

メールを拒否を有効にすると、メールプログラムはこの警告が件名欄に挿入されたメール を受信しません。スパムの疑いがある場合には、件名欄ではなく実際のメール本文の前に テキストを挿入することもできます(**[本文中のメッセージ])**。

Microsoft Outlook (※Outlook Express や Windows Mail では不可)を使用している 場合、スパムの疑いのあるメールを受信トレイ内の任意のフォルダに移動できます ([メ ールをフォルダに移動])。移動先のフォルダは、フォルダ名に入力すると新規作成でき ます。

送信者フィルタ:送信者フィルタは、特定の送信者から送られてきたメールの受信をブロックします。送信者フィルタを設定するには、送信者 / ドメインに、ブロックする送信者のメールアドレス とドメイン名 を入力します。複数の送信者を登録する場合には、メールアドレスをセミコロン (;) で区切ります。

処理方法では、スパムと判断されたメールの処理方法を設定します。メールの件名と本文 に警告を挿入にチェックを入れると、疑わしいメールの件名欄の件名の前に「スパム」ま たは「注意」などの警告(件名に追加する文字)を挿入できます。

メールを拒否を有効にすると、メールプログラムはこの警告が件名欄に挿入されたメール を受信しません。スパムの疑いがある場合に、件名欄ではなく実際のメール本文の前にテ キストを挿入することもできます**(本文中のメッセージ)**。

Microsoft Outlook を使用している場合(※Outlook Express または Windows Mail で は不可)、スパム疑惑のあるメールを受信トレイ内の自由に定義できるフォルダに移動す ることができます(メールをフォルダに移動)。本製品は、フォルダ名の欄にフォルダを 定義すれば直接フォルダを作成する機能を備えています。 **処理方法**では、スパムと判断されたメールの処理方法を設定します。メールの件名と本文 に警告を挿入にチェックを入れると、疑わしいメールの件名欄の件名の前に「スパム」ま たは「注意」などの警告(件名に追加する文字)を挿入できます。

メールを拒否を有効にすると、メールプログラムはこの警告が件名欄に挿入されたメール を受信しません。スパムの疑いがある場合に、件名欄ではなく実際のメール本文の前にテ キストを挿入することもできます(本文中のメッセージ)。

Microsoft Outlook を使用している場合(※Outlook Express または Windows Mail で は不可)、スパムの疑いのあるメールを受信トレイ内の自由に定義できるフォルダに移動 することができます(メールをフォルダに移動)。本製品は、フォルダ名の欄にフォルダ を定義すれば直接フォルダを作成する機能を備えています。

その他

ここでは次の設定を行うことができます。

🔽 設定 アンチスパム そ	Eの他 X
🛓 🏦 🤤	
設定	- Microsoft Outlook のみ ■プログラム起動時に受信トレイの未読メールをスキャン(U)
▷ ⁻ ¹ / ₁ / ₁	~他のメール クライアント(POP3 を使用)
 アンチスパム スパムフィルタ スパムフィルタ 	受信拒否された場合は、代替メールが配信されます。 メール クライアントでルールを定義 し、メールを完全に削除するか、別のフォルダに移動するか指定してください。
▶ フィルタの追加 ▶ その他	
▶ ファイアウォール ▶ チューナー	
▶ デバイス コントロール	メール本文(M): アンチスパムによってメッセージが拒否されました。
▶ ハックアッノ	送信者: %s 作名: %su ~
	ワイルドカード: %s = 送信者, %u = 件名
	OK キャンセル 適用(<u>B</u>) ヘルプ

 プログラム起動時に受信トレイの未読メールをスキャン(Microsoft Outlook のみ): Outlook を起動するとすぐに、受信トレイとそのサブフォルダにあるすべての未読メール をチェックします。

- 他のメールプログラム (POP3 を使用): POP3 で受信したメールは、POP3の仕様による制限で、すぐには削除できないことがあります。フィルタがメールの受信を拒否すると、このメールは下の代替テキストで書き換えられます。受信拒否メールの代替テキストは「メッセージが拒否されました」と表示されます。この代替テキストは自由に編集できます。件名とメール本文のテキストを、以下のワイルドカード(「%」記号に続けて小文字1文字)を使って自由に作成できます。
 - %s 送信者

%u 件名

ここで設定したテキストを自動的に削除するルールをメールプログラムで設定できます。

ファイアウォール

自動

ファイアウォールは外部からの不正侵入からコンピュータを保護します。G DATA のファイア ウォールには、オートパイロットモードからマニュアルでのルール設定まで、初心者から上級者 のニーズに応えることができる様々な設定が搭載されています。

後定	オートバイロット	
	● オート/ (イロット モード (進度	(A)
-61	④ 手動でルールを作成(M)	
アンチウイルス アンチスパム	回 フルスクリーン アプリケー	ション実行時にオートパイロット実行 (ゲーム モード)(V)
ファイアウォール	③ ユーザー定義セキュリアイ (上)	使售的(计)(d)
▶ 自動	● 容勢セキュリティ レベル(S)	
▶ アワート	1 - ##### 1072	送 明
▶ デェックサム デスト	COM CHELDING	概算セキュリティ:
▶ その個	・ 病セキュリティ	アプリターもあり単位で低中的に整想します。
チューナー		
デバイス コントロール	一 植巣セキュリアイ	
バックアップ	. 低セキュリティ	
	. ファイアウォール県効	

ファイアウォール設定の自動は、以下の2つの領域から構成されています。

オートパイロット

ファイアウォールの作動方式を選択します。モードでは、オートパイロットモード(推奨)と 手動でルールを作成から選択できます。

- オートパイロットモード:ファイアウォールが許可、またはブロックするアプリケーションを自動制御するので、ユーザーを煩わすことなく、コンピュータを最適に保護できます。(推奨設定)
- ・手動でルールを作成:ファイアウォールをネットワーク環境に合わせて設定したり、特定のアプリケーションにオートパイロットモードを適用しない場合には、この設定を選択して、ルールを手動で作成します。
- フルスクリーンアプリケーション実行時にオートパイロットを実行(ゲームモード): ゲームやフルスクリーン表示のアプリケーションを起動した際に、ファイアウォールが自 動的にオートパイロットモードに切り替わるように設定します。この設定は、オートパイ ロットを通常は使用しない場合にのみ選択できます。

ユーザー定義セキュリティ

上級者向けのユーザー定義セキュリティ(上級者向け)とGDATAが定義した自動セキュリ ティレベルから選択できます。自動セキュリティレベルを使用すると、ネットワークセキュリ ティの専門知識がなくてもユーザーを煩わせることなく、ファイアウォールを環境に応じて設定 できます。自動セキュリティレベルの設定は、非常にシンプルで、希望するセキュリティレベ ルにスライダを合わせて設定するだけです。設定レベルには以下の5種類があります。

- 最高セキュリティ: ファイアウォールのルールを非常に細かく設定します。ネットワークの専門用語(TCP、UDP、ポートなど)に精通している必要があります。ファイアウォールは微小な不一致も検知するため、学習段階では非常に頻繁に確認が行われます。
- 高セキュリティ: ファイアウォールのルールを細かに設定します。ネットワークの専門用
 語(TCP、UDP、ポートなど)に精通している必要があります。ファイアウォールが、学習段階で頻繁に確認が行われます。
- 標準セキュリティ: ファイアウォールのルールをアプリケーションレベルで設定します。
 ネットワークの専門知識がなくても、ウィザードで簡単に設定できます。学習段階での確認頻度も最小限です。
- 低セキュリティ:ファイアウォールのルールをアプリケーションレベルで設定します。 ネットワークの専門知識がなくてもウィザードで簡単に設定できます。また、学習段階での確認もほとんどありません。このセキュリティレベルでも、着信する接続要求に対して は最高レベルのセキュリティが適用されます。
- ファイアウォール無効: ファイアウォールを無効にします。ファイアウォールを無効にしても、インターネットや他のネットワークとの接続は維持されます。外部からの攻撃やスパイウェアの防御が機能しなくなるので、ファイアウォールを無効にする際は注意ください。

ファイアウォールを細かく設定するには、**ユーザー定義セキュリティ(上級者向け)**にチェックを入れます。この設定は、ネットワーク知識のある上級者にのみお勧めします。

アラート

ユーザー定義セキュリティ(上級者向け)にチェックを入れた場合、この領域の設定ができる ようになります。アラートでは、このプログラムがインターネットやネットワークと接続を確立 する時に、ファイアウォールがユーザーに確認を求めるタイミング、処理方法、確認の有無など を設定します。

fbrar	
are > 一般 > アンチウイルス > アンチスパム > フッイアウォール	 プライアジュールルールの存成基準: アプリケーションごと(A) プロトコルボート/アプリケーションごと(P) アフートの停留数を接定(n)
> 自動 ▶ プリート ▶ チェックサム チスト > その他	 不場なサーバー アプリケーション ● 不易なサーバー アプリケーションが配置したらすぐに留点する(5) ◎ 不易なサーバー アプリケーションがネットワーク接続を確立しようとする終意告する(E)
> チューナー > デバイス コントロール > バックアップ	保護されていないネットワーク 一変保護されていないネットワークが発見されたらすぐに整合する(f)
	アプリケーション アラートのキャッシュ アラートのキャッシュ 参照(れ): 20 点 数

ルールの作成

ファイアウォールがネットワークとの接続を検知すると、ポップアップが表示されます。この画 面で、当該アプリケーションを許可/禁止するなどの処理方法を指定します。

- **アプリケーションごと**:表示されたアプリケーションに対して、許可/拒否するポートお よびプロトコルを設定します。
- プロトコル/ポート/アプリケーション: ネットワーク接続を要求するアプリケーション に、要求されたポート(またはプロトコル)だけを使用したアクセスを許可します。この アプリケーションがさらに別のポート(またはプロトコル)でネットワーク接続を要求し た場合は、追加ルールを作成するために、ユーザーに再度確認が行われます。
- アラートの保留数を指定 __アラートまで保留: 一部のアプリケーション (Microsoft Outlook など) は、ネットワークへのアクセス時に同一のリクエストを複数ポートへ送信 したり、複数のポートやプロトコルを同時使用しています。このようなアプリケーション を使用している環境でプロトコル / ポート / アプリケーションごとを設定すると、ユーザーへの確認が複数回行われますが、特定回数以上、ユーザーへの確認があった場合は、アプリケーションごとに切換え、当該アプリケーションに対して許可 / 拒否を行うこと ができます。

不明なサーバーアプリケーション

ルールにないサーバーアプリケーションが起動した場合、もしくはサーバーアプリケーションが 接続状態に入った時に、報告を発します。

保護されていないワイヤレスネットワーク

ファイアウォールが適切に機能するには、コンピュータが接続しているネットワークが認識され、かつファイアウォールによって監視されている必要があります。このため、通常はデフォルト設定の**保護されていないワイヤレスネットワークが発見されたらすぐに警告する**からは チェックを外さないでください。

アプリケーションアラートのキャッシュ

ルールで定義されていない接続要求において、繰り返し行われる接続確認を特定の間隔で行うように設定できます。デフォルトでは、20秒に設定されています。

チェックサムテスト

チェックサムテストでは、ファイアウォールがネットワークアクセスを許可したアプリケーションに対して、ファイル容量などの判断基準から構成されるチェックサムを使い、その信頼性を チェックします。アプリケーションのチェックサムが一致しない時は、アプリケーションが改変 された可能性があるので、アラートが発せられます。

チェックサムテストの実行: アプリケーションに加えてモジュール(例:DLL)も監視します。 モジュール変更や新たなモジュールのロードは頻繁に行われるため、モジュール変更と不明なモ ジュールを完全に管理するのは手間がかかります。モジュールチェック機能は非常に高レベルの セキュリティが必要な場合にのみ使用してください。

👽 設定 ファイアウォー	ルーチェックサム テスト	×
116		
 細次 一級 アンテンパム アンテスパム アンデスパム ラクボウスール ト (2) アクラント チェックサムアスト チスの位 アニートー アニートー アバイスコントロール バックフップ 	 ビチェックサム デストの演行(4) この機能を負効にすると、快か込まれたアプリケーションに交受があるかチェックします。 金盤 れたアプリケーションに使するフィイアウォールの回答: コーザーによってな際(A) G Data のウイルススキャンで能够(推測(V)) 図 和目的のウイルススキャンで能够(推測(V)) 図 ロード選 かモジュールのプエックサム デスト(M) ロード選 かモジュールの またい 勉強で キジュールをチェック(5) 会 変更されたモジュールの不明なモジュールをチェック(6) 	
	OK オヤンセル 通用(当) ヘルプ	

その他

他にも以下のような設定も可能です。

ŧ	テフォルト設定ウィザード
一府	ファイアウォール ルール補助時のデフォルト設定:
	④ ルール ウィザードを使用(R)
アンチスパム	○ 詳細設定ダイアログを使用 (上或容用)(w)
ファイアウォール > 自動 > アラート > チェックサムチスト > その機	プログラム起動物のチェック 図 プログラム起動時に不苟なサーバー アプリケーションをスキャンする(u)
チューナー	接続ログの保存
デバイス コントロール バックアップ	接成ログの保存時載(2): 1 高 時発まで

デフォルトで使用するウィザードの種類

新規ルールの生成方法を**ルールウィザード**もしくは**詳細設定ダイアログ**から選択します。**詳細 設定ダイアログ**は上級者向けの設定モードです。

プログラム起動時のチェック

アプリケーション起動の度に、ファイアウォールが不明なサーバーアプリケーションをチェック します。この設定は、クローズドネットワークを除くすべてのネットワーク環境で有効にしてお く事をお勧めします。

接続ログの保存

Ê

ファイアウォールのログを保管する期間を設定します。期間は1~60時間の中から選択 できます。ログは、ファイアウォール領域に移動して、ログアイコンを押すと表示でき ます。

的题的操作	390-010	アポリケーション	ローカル ホート	機能の方向	北井 十子社	ひをート ポート	現由
1018/26/17 10:26/11	UDP	System	nerbios-don (18.	<-	18231.3842	netbios-den (.	達用されたルール
2010/85/17 1925/0	UDP	Spoten	inertico-no (107)	÷	19,218,19,47	netbios-no (12.,	適用されたルール
2018/06/17 16.26.02	UOF	evolucituse	Gear (3355)	6+	IE/258	17347	漫明されたルール
2010/25/17 19:29:22	UDP	sive#yostenie	Sizer (\$155)	100	E)/296	\$0,239	通用されたルール
2018/85/97 95:24:59	UDP	skipstere	Since (\$255)	6	18/215.12/248	\$3567	適用されたルール
2018/26/17 18:24:59	UDF	availout ave	Binar (3385)	10×	fel9.sccted1d_	18186	連用されたルール
2010/15/17 192459	UDP	svokostere	liene (5355)	4.4	ID216	12765	適用対わたルール
2018/05/17 16:24:59	UDP	evoluciase	Geor (3885)	6-	IE258	80459	漫明かれたルール
S 2010/26/17 19:24:86	UDP		57421	194	18211.12211	\$7521	存在。如此证明本不必
2010/85/17 153445	UDP	sychostere	1980) (1980)	1-	10:211.11.49	56911	適用されたルール
2018/85/17 18:24:14	UDF	reduction	iner (3381)	6.	18211.1148	19771	連用されたルール
2010/15/17 19:2454	UDP	svokostere	itere (5:55)		fel@t6c3e782_	81911	適用されたルール
2018/06/17 16:34:34	UDP	evoluciave	Unar (\$255)	(-	18/211.18.47	57488	適用されたルール
2018/86/17 10:24:54	UDP	cychoct exe	Stree (\$365)	¥-	fe10-1d211e62_	51588	達用されたルール
\$ 2010/25/17 15:34:36	UDP		bactpe (87)	4-	ID459	86	容易L4A1122米本化A
0 2018/06/17 18:24:22	UDP		Lautes (87)	6-	IE:258	83	存在しな、エントキイン
02010/26/17 19:24:19	UDP		beolos (\$2)	14	EDADA	10	存起,从111/14本心力
A NATION OF THE AND A NATION	1.015	Husten	mathing days \$16	1	MI-164	weather share f	and the second s

チューナー

一般

次の設定が利用できます。

18 ie	後先ゲータを削除する期間(<u>W</u>)	E	
一般	古いデータを新除する期間(D)	14 8	
アンテウイルス	デスクトップ ショートカットを利益する問題(V)	160 1	
アンテスパム		161	
ファイアウォール	図 Microsoft Update の株素中に Office のアップゲー	- トを検索する(図)	
チューナー	ご 相称とイルに項目の非確認能を含むログ ファイルを 同一時つきメリカ完全に能称する(T)	PROVED (U)	
*	※一句ンアマルを元金に始けるの(1) ※ コンピュータの開発教をチューナーに許可しないの	N	
▶ 级定	逆 備々の壊死ポイントの作成を許可する(E)		
> フォルダ保護	※ デンラク時にドライブの確実 リュードディスク/55	(1) をチェックしない	
» ファイル保護			
▶ スケジュール			
デバイス コントロール			
バックアップ			

- 復元データを削除する期限: 作成した復元ファイルを削除するタイミングを設定します。
- 古いデータを削除する期限: Tempフォルダにある不要なファイルを削除するタイミングを設定します。
- デスクトップショートカットを削除する期限: 使用されていないデスクトップ上のショー

トカットを削除するタイミングを設定します。

- Microsoft Update の検索中に Office のアップデートを検索: Microsoft Update の 確認と一緒に、Microsoft Office の更新も確認します。この機能は Microsoft Office が コンピュータにインストールされている場合にのみ実行されます。
- **削除された項目の詳細情報を含むログファイルを作成しない**: チューナーで実行した変 更のログを記録しません。
- **コンピュータの自動再起動をチューナーに許可しない**:スケジュールチューニング実行後に要求される再起動(ログインユーザーがいない場合にのみ)を実行しません。
- 個々の復元ポイントの作成を許可: ここを有効にしない場合、チューナーの復元ができな くなります。
- アフラグ時にドライブの種類(SSD/ハードディスク)をチェックしない: 大部分のSSD 製造メーカーはSSDのデフラグを推奨していないため、チューナーもデフォルトではSSD をデフラグしない設定になっています。使用しているコンピュータにSSDが搭載されてい ないことが確実な場合は、この設定を有効にすることで、ドライブの種類をチェックせず に全てのハードドライブのデフラグを実行させる事ができます。

設定

設定では、チューナー用の設定項目を細かく定義できます。ここで選択した設定項目は、スケ ジュール もしくは手動でチューナーを実行した際に実行されます。各項目の有効/無効の切換 えは、チェックボックスで行います。

チューナーの設定項目は次の3つのカテゴリに分類されています。

- セキュリティ: OS、各種ソフトウェアの更新や設定など、コンピュータに害を及ぼす可能 性のあるセキュリティリスクをチューニングで解消し、コンピュータを適切に保護しま す。
- パフォーマンス:不要になったバックアップファイル、ログファイル、インストール済み プログラムのインストールファイルなどの一時ファイルは、空きスペースの減少や保存領 域へのアクセス速度低下の原因となります。さらに、不要になったプロセスやファイルの リンクはシステムの動作速度に大きな影響を及ぼします。パフォーマンス用モジュール は、コンピュータに無駄な負荷をかけず、スピードアップするためのツールです。
- データ保護: データ保護用モジュールは、インターネットの閲覧やコンピュータの通常利用している間にに、意図せずコンピュータに残った履歴、ユーザーの利用傾向、重要なファイル、パスワードを消去します。

安定	チューニングに使用する機能を選択します。	
	817 セキュリティ	-
アンチウイルス	(梁) シスデム設定の影響スデータスを確認	
> アンチスパム	 図 整整のインターネット セキュリディ ゾーン設定を有効化 図 Internet Endorer のフィッシング フィルタを参加化 	
ファイアウォール	Internet Explorer のフォームデータの記録を集効化	
チューナー	図 Outlook, Outlook Express, Windows Mail, Windows Live Mail の時付ファイ	ルに来
> 一般	図 OsBook Express, Windows Mail, Windows Live Mail のプレビュー ウインドウ	アを重
· 57	「 Outbook, Outbook express, windows Mail, Windows Live Mail での外部デー	9000
5 7+1.43/93#	[1] おいファイルとファイル必要する次本を有効化 (1) コービー ウカウントを使きたみた。	
- The du Alter	(M) ペーシーアカンノンで構成であるい。 (M) がついだいがしゃつきだいがのますはない、ボナックを算続からのです。	
* JANANA	(1) Modia Dever の運転半十小力を制いた	
▶ スケジュール	III Madia Pinyer でのスクリプト面行を豊か化	
テバイス コントロール	② Media Player での新しいコーデックの目動ダウンロードを算効化	
バックアップ	100 dalaha filandan di tana 10 ki 1993 (2000 ki 19	•
	ソフトウェアを機断に伴っことによって説知の過替性を排除します	

フォルダ保護

フォルダ保護は、特定フォルダをチューナーの削除対象から除外したい場合に設定します。

設定	…・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	
⊅ ──穀		
b アンデウイルス	2 C: WerfLogs	
D アンテスパム		
> ファイアウォール		×
・ チューナー		
▶ ──般		
▶ 證范		
▶ フォルダ保護		
▶ ファイル保護		
V X2/2/2-10		
> デバイスコントロール		
> バックアップ		

٠

ファイルやドライブをフォルダ保護に設定するには、【追加】アイコンをクリックし、

対象を選択して [OK]をクリックします。



設定済みのフォルダ保護を解除するには、表示された一覧から選択し、[削除] アイコン をクリックします。

ファイル保護

ファイル保護は、特定ファイルをチューナーの削除対象から除外したい場合に設定します。

論定	傍ファイルの標案対象から以下のファイルが除外されます。 チェックポックスをオンにすると、米型ナガナフォル与内のファイルのみ保障されます。	
▷ 一般		
▶ アンテウイルス	meret	
> アンテスパム	iiii text?.doc	
> ファイアウォール		×
チューナー		
▶ 一般		
▶ 股定		
▶ フォルダ保護		
▶ ファイル保護		
▶ スケジュール		
デバイス コントロール		
バックアップ		

٠

特定のファイルを保護するには、左の**[追加]**アイコンをクリックし、ファイル名を入力 します。ファイル名にはワイルドカードを利用できます。

ワイルドカードの機能は次のとおりです。

- 疑問符(?): 任意の1文字に代わるワイルドカード
- アスタリスク(*): 文字列全体に代わるワイルドカード

例: 拡張子「.sav」のファイルをすべて対象に設定するには、「*.sav」と入力しま す。連続性のある名前のファイル(text1.doc、text2.doc、text3.doc など)などを 保護するには、例えば「text?.doc」と入力します。

[...] ボタンからは、保護対象のフォルダを選択できます。保護したいファイルの保存 場所を選択してください。



追加したフォルダ保護を解除するには、一覧から選択し、**[削除]** アイコンをクリックします。

スケジュール

スケジュールでは、スケジュールチューニング(自動実行されるチューニング)の実行間隔を設 定します。

(シー情報、およびセ	システムの/ (フォーマンス、コンピュータに保存されている) ユリティの最適化を信定した時間に目動共行します。 (2) 有効	。 … 検 アンチウイルス っ、 ユマ バル
 第日 2 月場日 2 火曜日 2 水曜日 2 水曜日 2 土曜日 2 日曜日 2 日曜日 	高行領度 ① 1 回のみ(E) ① 毎月(M) ② 町時(5) ③ 町日(7) ④ 町田(7) ④ 町田(7) ④ 町田(7) ④ 町田(7) ④ 町田(7) 〇 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二	ファイアウォール テ 二 - デー ・ 一 岩 シ フェーノノ保護 シ ファイル保護 シ ファイル保護 ・ スタジョール デバイス コントロール ミックアップ
	 ● 申請(5) ● 申目(T) ● 申述(W) 時間 日曜日の 12:00 ▲ 次の曜日 	 一般 放定 フォルダ保護 ファイル保護 スクジュール ボイス コントロール ミックァップ

実行頻度では、チューニングを実行する頻度を入力します。ここ選択した設定によって、次に選択できる項目が自動的に展開します(例:毎日にチェックを入れると、右側に曜日が表示されるので、ここで曜日を選択します。その次に、時間で時間を指定します)。

スケジュールチューニングをしない場合は、**有効**のチェックボックスからチェックを外してくだ さい。

デバイスコントロール

デバイスコントロールでは、コンピュータに接続(または搭載)されたデバイスへのアクセスを 細かく管理できます。この機能を使うことで、USBメモリを使った不正データ詐取を未然に防ぐ ことができます。

コール ルール	×
アクセスを割限する対象のデバイスを選択してください。	
	_
☑ リムーバブル ディスク(W) (例: USBメモリ) ルールを編集(e)	
フロッピードライブ(D) ルールを編集(r)	
☑ デバイスへのアクセスをブロックする時、メッセージを表示	
OK キャンセル 道用(B) へ	ルプ
	 コール ルール ビデバイスコントロールを有効にする(G) アクセスを制限する対象のデバイスを選択してください。 ビリムーバブルディスク(W) (例: USBメモリ) ルールを構集(e) CD/DVD ドライブ(C) ルールを構集(c) フロッピー ドライブ(D) ルールを構集(r) ビデバイスへのアクセスをブロックする時、メッセージを表示 OK キャンセル 適用(6) へ

デバイスコントロールを使うには、**デバイスコントロールを有効にする**にチェックを入れ、管理したいデバイスの種類を以下から選択します。

- リムーバブル ディスク (例: USBメモリ)
- CD/DVD ドライブ
- フロッピー ドライブ

次に、選択したデバイスに対して適用するルールを設定します。[**ルールを編集**] をクリックして ください。

一般ルール

対象デバイスに適用するアクセスルールを選択します。ここで選択できるアクセスの種類は、以下の3種類です。ここで設定するルールは、コンピュータの全ユーザーに適用されます。

• アクセスをブロック: 読み取り/書き込みの両方をブロックします。

- 読み取り: 読み取りアクセスのみを許可します。
- 読み取り/書き込み: 読み取り/書き込みアクセスの両方を許可します。

- ゲーシーシン(まかパイス曲号のジールによらいジャーロン ジェーフンシンメナイナー出版 5 のシール ● アクセスをプロック(Z) ◎ 読み取り(L) ◎ 音さ込み(読み取り(V) - ザー面積のルール(D)				
通知(A) バイス国際のルール(端菜(+) G)	取り除く[n]		
	11-11	ルールの種類	有功明期	ルールが避用され
デバイスの説明	10-10	ALC: 1 1. 1987	11212	
デバイスの説明 IV Elements 1000 (28 (… 有効	#810/P/80/P-		
デバイスの統明 IV Elements 1000 C IV Kingston DetaTr	メレール 28 (… 有効 svol 有効	書き込み/助み. 書き込み/読み.	期限切れ	

ユーザー固有のルール

特定ユーザーにおいてのみアクセス制限を設定することもできます。

🔽 ユーザーを選択	×		
ローカル ユーザーを選択(L):			
VMware_Conv_SA			
admin			
	·	コーザー の選択	9
		+ サミシートル 通知 (2)	
		ユーザー ユーザー	オブジェクトの種類
		場所の指定(F):	
-		ID333	场/ff(L)
別のユーザー(<u>A</u>)…		選択するオブジェクト名を人力してください (例)(E):	名前の確認の
OK キャンセ	ιL		
		I詳細設定(A)	OK +++>d

2-9-8				
admin				
ルールの構成				
© アクセスをプロッ	· ク(Z)			
※読み取りアクセス	:(L)			
◎ 光金なアクセス[a			
的动物制造				
@ 加利税(u)				
◎ 乾了(b)	2013年 5月24日	8*	13:11:16	
				101

このような設定を行うには、まず [追加] をクリックし、ユーザー名を選択して [OK] を押しま す。次のウィンドウで、アクセスルールの種類(必要に応じて有効期限も)を設定してくださ い。[OK] を押すと、設定完了です。

> **メモ: ユーザー固有のルール**は、**一般ルール**より優先されます。例えば、一般ルール でUSBメモリへの**アクセスをブロック**と設定した場合でも、ユーザー固有のルールを 設定することで、特定ユーザーを一般ルールから除外対象とすることができます。ま た、**有効期限**を設けたユーザー固有のルールは、期限終了後に一般ルールが適用され ます。

デバイス固有のルール

リムーバブルディスクのルール設定では、特定のUSBデバイスのみ使用できるように設定できま す。これを行うには、USBデバイスをコンピュータに接続してから、[追加]を押します。表示さ れるウィンドウで、対象のデバイスを選択して [OK]を押します。次の画面で、アクセスルール の種類(必要に応じて有効期限と適用されるユーザー)を設定してください。[OK]を押して設 定完了です。

デバイスの説明	ドライブ	
IM20337 HI-Speed USB to SATA _PATA Combo Bridge (JMi	F:¥	

INTERTO IN COMM	ISTR BA EATA & DATA CAUSAN BALAN	(INTERNA Technology Core /
umzuaav mi-apeed	USE to SAIA & PAIA Compo Bridge	(anacran recritiology Corp. /
一ルの種類		
⑦ アクセスをブロッ	ク(2)	
(8) 読み取りアクセス	(L)	
◎ 完全なアクセス[V)	
交通 通		
● 未設定(U)		
◎ 精细核了(B)	2013年 5月17日	16:36:01
レールが適用されるユ	-9-	
@ すべてのユーザー	(A)	
◎ 特定ユーザー		ユーザーを選択(図)

バックアップ

バックアップでは、バックアップ機能の設定を行います。

- ・一時ファイルの保存先フォルダ:バックアップ用の一時ファイル保存先フォルダを変更できます。この設定は、現在設定されているフォルダの保存先ドライブに、十分な保存領域が確保されていない場合にのみ変更してください。一時ファイルは、バックアップ中もしくは復元中に作成され、処理完了後に自動削除されます。一時ファイル用フォルダの保存先ドライブに十分な保存領域がないと、バックアップおよび復元プロセスの処理速度低下の原因となります。
- バックアップの対象と保存先が同一ドライブ上にないか確認する: ここにチェックを入れると、保存対象と保存先が同一ドライブにある場合、それをユーザーに通知します。これは、万一のデータ消失の際、いずれのデータも利用できなくなる可能性があることをユーザーに通らせるためです。特別な理由がない限り、このオプションは無効にしないことをお勧めします。



ログ

本製品に搭載されている各機能には、保護などを行った際の動作を記録、確認するためのログ機 能が搭載されています。

アンチウイルスのログ

アンチウイルスを選択した状態でログアイコンを選択すると、ウイルスからの保護状況や、ワク チンのアップデート状況が記録されます。

列見出しの 開始時刻、種類、内容 もしくはステータスをクリックすると、ログを並び替えることができます。 [名前を付けて保存] では、ログをテキストファイルに保存し、 [印刷] ではログを印刷できます。ログを削除するには、対象を選択してから、 [削除] ボタン(もしくはキーボードの Delete キー)を押してください。

ファイアウォールのログ

ファイアウォールを選択した状態でログアイコンを選択すると、ファイアウォールが許可/拒否 した接続がすべて表示されます。

任意の列の見出しをクリックすると、その項目に従って並び替えができます。また、行を選択し て【**詳細**】をクリックすると、その接続について詳細情報が表示できます。ログの保存期間を変 更したい場合は<u>設定 | その他</u>の項に従って変更してください。

バックアップのログ

バックアップを選択した状態でログアイコンを選択すると、すべての操作やバックアップジョブ の結果を確認できます。

各ログの詳細情報を確認するには、対象をダブルクリックするか**[開く]**ボタンを押します。開いたログは印刷やテキスト形式での保存が可能です。詳しくは<u>パックアップと復元</u>の項をご覧ください。

アンチスパムのログ

セキュリティセンターのアンチスパム、ログ:スパム(スパム以外)を選択すると、スパムメール の判定を手動で行うための特別なログを確認できます。

それぞれのログにはアンチスパム機能で処理したメールの一覧が表示され、ユーザーの判断に基づいて、各メールをホワイトリストもしくはブラックリストに登録することができます。

ログ

フィルタリングのログ

フィルタリングを選択した状態でログアイコンを選択すると、管理者は各ユーザーの接続履歴、 拒否されたコンテンツの内容やブロックした理由などの情報を確認できます。詳細は、フィルタ リングの設定:ログの項をご覧ください。

デバイスコントロールのログ

デバイスコントロールを選択した状態でログアイコンを選択すると、デバイスコントロールに関するイベントのログが表示されます。

イベントログは期間を絞って表示させることもできます。右下の**表示期間**で表示させるイベント の期間を選択してください。デバイスコントロールの詳細は、設定:デバイスコントロール を参 照してください。

FAQ: ブートスキャン

本製品には、Windows 起動前にスキャンを実行できる**ブートスキャン**機能が搭載されていま す。 ブートスキャンは、本製品をインストールする前からコンピュータに感染し、本製品のイン ストールを妨害する可能性のあるウイルスの駆除をするのに役立ちます。

ブートとは: コンピュータの電源を入れると、通常は自動的に Windows OS が起動します。このプロセスを「ブート」と呼びます。このプロセスでは Windows OS だけでなく代わりに別のOSを自動的に起動させることもできます。本製品のブートメディアを使用すると、ブートの際、 Windows の代わりに専用OSでコンピュータを起動することができ、そのOS上でウイルススキャンを行う事ができます。

ブートスキャンの準備

ブートスキャンは、本製品をインストールする前からコンピュータに感染し、本製品のインスト ールを妨害する可能性のあるウイルスの駆除をするのに役立ちます。このブートスキャン機能 は、Windows を使用せずにコンピュータをブートメディアから起動してスキャンを行う機能で す。

CD/DVD からのブート: コンピュータが、ブートCD/DVD から起動できない場合は、以下の手順をお試しください。

(この作業は、コンピュータの操作に慣れた上級者が設定されることをお勧めします)

- **]** コンピュータをシャットダウンします。
- 2 コンピュータを起動し、BIOS 設定画面を表示します。通常 BIOS 設定を行うには、コンピュータの起動(=ブート)時に Delete キーを押します。

BIOS 設定画面が Delete キーで表示されない場合: コンピュータのメーカーによっては、**F2 キー、F10 キー**、または**その他のキー**が割り当てられている場合もあります。コンピュータの取扱説明書もしくはホームページなどでご確認ください。

- 3 次に、BIOS 設定画面で、ブートデバイスの優先順位を変更します。BIOS の各設定項目 をどのように変更するかはコンピュータによって異なりますので、コンピュータの取扱 説明書をお読みください。変更後のブート順は CD/DVD:, C: にします。具体的には、 CD/DVD ドライブを [1st Boot Device] (第1ブートデバイス)とし、Windows OS がインストールされているハードディスクパーティションを [2nd Boot Device] (第2 ブートデバイス)とします。
- **4** 変更を保存して、コンピュータを再起動します。これでブートメディアからブートできる状態になりました。

ブートスキャンを中断するには:通常、コンピュータに起動中にブートメディアが挿入 されているとブートスキャンの画面が表示されます。Windows 起動画面を表示したい 場合は、ブートスキャンのメニュー画面で矢印キーを使い、**Microsoft Windows** を 選択し、**Enter** キーを押します。すると、Windows が通常通り起動します。

USBメモリからのブート: USBメモリのブートメディアからブートする場合も、CD/ DVDと同じ要領で 1st Boot Device として認識されるように設定してください。それ でも起動時に認識されない場合は、コンピュータの起動時に**ブートメニュー**を使用 し、対象のUSBメモリを選択して、ブートを行ってください。

ブートスキャンの流れ

ブートスキャンを実行するには、以下の手順に沿って行ってください:

CD版製品でのブートスキャン:製品CD/DVD をCD/DVDドライブに挿入します。表示 された起動ウインドウで、[キャンセル] をクリックし、コンピュータをシャットダ ウンします。

ダウンロード版製品でのブートスキャン: G DATA を起動し、**ウイルス対策**タブを選択 します。次に、右下の【ブートメディアを作成】 を選択して、ブートメディア を作成 します。作成が完了したら、作成したブートメディアをコンピュータに挿入して、コン ピュータをシャットダウンします。 ※ブートメディアを挿入後に起動画面が表示された場合は、【キャンセル】をクリック してコンピュータをシャットダウンします。

メモ: Windows XP 上では、ブートメディア作成時に「IMAPI 2.x がインストールされていません」というメッセージが表示されることがあります。これは、古いOSでデータをメディアにコピーするために必要な Microsoft の更新プログラムです。Microsoftのサイトからダウンロードしてインストールしてください。

USBメモリを利用したブートスキャン: G DATA を起動し、**ウイルス対策**タブを選択し ます。次に、右下の【**ブートメディアを作成】**を選択して、ブートUSB を作成しま す。作成が完了したら、作成したブートUSB をPCに差し込み、コンピュータをシャッ トダウンします。 ※ブートUSBの挿入後に起動画面が表示された場合は、【キャンセル】をクリックして コンピュータをシャットダウンします。

注意: ブートUSBから起動する場合は、コンピュータがUSBメモリからブートできる状態でなければなりません。多くの場合は、起動時にコンピュータのブートメニューを使用する事でブート可能です。詳しい解説は、ブートスキャンの準備の項のUSBメモリからのブートを確認ください。

2 コンピュータを再起動します。G DATA ブートスキャンのスタートメニューが表示されます。



3 矢印キーで G Data AntiVirus(もしくはG Data AntiVirus + Backup) を選択し、 Enter キーで確定してください。自動的に Linux OS が起動し、ブートスキャン用画面 が表示されます。

メモ: プログラム画面が正常に表示されない場合には、コンピュータを再起動して G Data AntiVirus - Alternative (もしくはG Data AntiVirus + Backup -Alternative) を選択してください。

メモ:トータルセキュリティ を使用している場合、この画面の後にダッシュボード画面 が表示されます。AntiVirus を起動もしくは復元を開始を選択してください。

- 4 ワクチン更新を実行するよう促されます。
- 5 [はい] をクリックし、次の画面で [スタート] ボタンを押すと更新が始まります。ワ クチンデータが更新されると、「更新できました」というメッセージが表示されます。

★モ:自動インターネット更新機能は、IP アドレスを自動割当機能(DHCP)を持つル ータを使用している場合にのみ、利用できます。インターネット更新が利用できなくて も、古いワクチンを利用して、ブートスキャンを実行できます。ただし、この場合に は、本製品のインストール後できるだけ早いうちに、更新したワクチンを使って、ブー トスキャンを実行してください。

6 スキャンのタブを選択して、スキャン領域に移動します。[コンピュータ]をクリックすると、コンピュータ全体のスキャンが開始されます。一般的に、コンピュータ全体のスキャンを行った場合は、スキャン終了まで数時間以上の時間を要します。一部のフォルダのみのスキャンで十分な場合は、[ファイルとフォルダ]を押して、対象のフォルダを選択してスキャンすると、スキャン時間も短く済み、効率的です。

7 ウイルスが検出されたら、本製品が提案する処理方法から適当なものを選択して、ウイルス駆除を行ってください。ウイルスを駆除できたら、オリジナルファイルが再び使用可能な状態になります。なお、ファイルがシステムファイルや重要なファイルと思われる場合は、削除しないことをお勧めします。

メモ: 削除を選択する場合は、対象のファイルが削除されてもシステムに問題を引起さないことを確かめてから、操作を実行してください。

- 8 ウイルススキャンが完了したら、画面右上のXマークをクリックします。ダッシュボード画面が表示されるので、[終了]をクリックし、再起動またはシャットダウンを選択します。
- 9 ドライブのトレイが開いたら、ブートCDを取り出します。(USBメモリを使用して ブートスキャンしている場合は、コンピュータのUSBスロットに差し込まれているUSB メモリを抜きます。)
- 10 コンピュータを再起動し、通常通り Windows OS を起動します。(CDやUSBメモリ が挿入されている場合は、すぐに取り出してください)
FAQ: 各種機能について

G DATA アイコン

本製品の保護機能が有効に機能しているかどうかは、タスクバー上の G DATA アイコンで確認 できます。

- Cのアイコンが表示されている時は、G DATA によるセキュリティ保護が有効で、コン ピュータが適切に保護されていることを意味しています。
- 窊

警告マーク付きのアイコンが表示される時には、セキュリティ保護が有効になっていな いことを意味しています。このアイコンは、ウイルスガードを無効にしたり、セキュリ ティ保護に問題がある場合に表示されます。



このアイコンが表示されている時は、本製品がインターネットから更新ファイルをダウ ンロードしています。

G DATA アイコン上で右クリックをすると、右クリックメニューが表示されます。右クリックメ ニューからは、ユーザーがよく使用する操作が選択できます。



画像はトータルセキュリティのものです。

ここでは以下の操作を選択できます:

- G DATA(製品名)を起動:本製品プログラムのセキュリティセンターを呼び出します。
 セキュリティセンターに関する詳細は、セキュリティセンター
- ウイルスガードを無効にする: ウイルスガードの有効/無効を切り替えます。大容量のファイルをコピーしたりする際にウイルスガードを無効にすると処理がより高速に行われますが、ウイルスガードを無効にする期間は最小限に抑えてください。またウイルスガードが無効な間は、インターネットやスキャン未実行のメディア(CD/DVDやUSBメモリなど)と接続しないようにしてください。

- ファイアウォールを無効にする: ファイアウォールが搭載されている製品では、右クリックメニューからファイアウォールの有効/無効を切り替えることができます。インターネット接続環境では、ファイアウォールを無効にした後も、コンピュータは引き続きインターネットに接続されます。このとき外部からの攻撃から保護されませんので、ファイアウォールを無効にする際は注意してください。
- オートパイロットを無効にする: ファイアウォールのオートパイロット機能の有効/無効 を切り替えます。オートパイロットはファイアウォールの処理をユーザーに代わって自動 的に判断する機能で、これを無効にすると、ネットワーク接続についてユーザーへ確認が 行われるようになります。通常はオートパイロットを有効にした状態で利用することをお 勧めします。
- **ワクチンを更新**: 今すぐにワクチン更新を手動実行します。コンピュータの適切な保護に は、ワクチン更新は非常に重要です。ワクチン更新は通常、自動更新に設定しておいてく ださい。インターネット更新に関する詳細は、更<u>新</u>の項を参照してください。
- データセーフを開く:トータルセキュリティを使用している場合は、データセーフ作成後 にここから任意のデータセーフを開く事ができます。
- 統計情報:メール、ウェブ、ウイルスガードなどのスキャン統計を確認できます。

ウイルススキャンの流れ

ウイルススキャンは、コンピュータ上のマルウェアをスキャンする機能です。ウイルススキャン 中にウイルスが検出されると、検出されたウイルスへの対処方法を選択できます。

スキャン: C:¥Windo	ws¥SoftwareDistrib	ution¥Do	wnload¥243	3163bf0db40854fe2c	38a32 C
スク	進行状況				キャンセル
システム領域	スキャン済み:	2441	開始時刻:	2013/06/19 17:21:11	一時信止
メモリとスタートアップ	検出:	0	経過時間: 産り時間:	00:00:52	비가
ルートキットスキャン		0	78 7 KUBI	00.00.57	○○へ 操作の ○○○ 実行
ウイルススキャン					
- 67					
テータ人					
₽ヤン: C:¥Windows¥Softv	wareDistribution¥Download	¥243163bf0c	lb40854fe2c38a	3293f15f9432c918e	
アイル/オブジェクト ガ	カテゴリ 操	/ ⊫		説明	フォノ
					· · · · · ·
		ш			
プション	1	詳細表示			
システム負荷が高い時はウ	イルススキャンを停止]パスワード	保護されたアーナ	 コイブ	
フナャン放了浴についだっ	- 々の重源を切る	■ マクセフ 15	不さわたフラノル		
ハイヤノペリ ほにコノヒエ	2007-Ellion C -50 G		出て1 いこ ノア 1 ハ		

検出されたウイルスには、それぞれの検出ごとに、削除、駆除、隔離といった対処が可能です。

- ウイルススキャンを開始します。ウイルススキャンの開始方法は、アンチウイルスの各 項目を参照してください。
- 2 コンピュータ上でスキャンが始まると、スキャンのステータス情報を表示する画面が開きます。

画面上部のステータス表示バーには、スキャンの進捗状況が表示されます。ウイルス スキャンのプロセスに関する設定は、スキャン中に行うことができます。設定できる 項目は次の通りです。

• システム負荷が高い時はウイルススキャンを停止: ユーザーがコンピュータで作業 を行っている間は、ウイルススキャンを自動的に停止します。

- スキャン終了後にコンピュータの電源を切る: ウイルススキャン終了後に、コン ピュータが自動的にシャットダウンします。例えば、一日の作業終了時にスキャン を行う場合などに使用すると便利です。
- パスワード保護されたアーカイブ:アーカイブがパスワードで保護されている場合、このアーカイブはスキャンされません。ここにチェックを入れると、スキャンできなかったパスワード保護されたアーカイブを表示します。これらのアーカイブにウイルスが潜んでいたとしていても、解凍しない限り、ウイルスがシステムに感染する可能性はありません。
- アクセス拒否されたファイル: Windowsでは、通常、アプリケーションが自身の動作のために使用するファイルを、そのアプリケーションの実行中にスキャンできません。スキャン実行中は、可能な限り、他のプログラムを実行しないようにしてください。ここにチェックを入れると、スキャンできなかったデータが表示されます。
- 3a ウイルススキャン結果が画面に表示されます。ウイルスが検出されなければ、【閉じる】をクリックして画面を閉じます。
- **3b ウイルスが検出された場合**は、 [操作の実行] をクリックして感染ファイルの処理を行います。

デフォルト設定(設定|アンチウイルス|ウイルススキャンで、何も変更しなかった 場合)では、感染ファイルからウイルスを駆除します。ウイルスを駆除に成功した ファイルは再び普通に使用してもコンピュータに支障をきたしません。

駆除できない場合には、ファイルは隔離領域に移動されます。隔離されたファイル は、暗号化して保存されるので、コンピュータに問題を引起すことはありません。こ の感染ファイルが必要にな場合は、隔離領域から元の場所に戻して使用できます。

3c 感染ファイルやオブジェクトが、必要か不要がを判別できる場合には、スキャン結果1 件ごとに操作を実行することもできます。

スキャン結果一覧の操作領域で、感染ファイル1件ごとに処理方法を決めます。

- ログを残すのみ: 感染したファイルをログとして記録します。感染ファイルのウイ ルス駆除やファイル削除はされません。※ウイルスをログに残すだけの場合、ウイ ルスは活動を続けるため危険です。
- ウイルス駆除(不可能な場合はログを残すのみ): 感染ファイルからウイルスを 駆除できない場合には、ファイルを検出時のままの状態でログに残し、このログ を基に後で処理方法を決めることができます。※ウイルスをログに残すだけの場 合、ウイルスは活動を続けるため危険です。
- ウイルス駆除(不可能な場合は隔離):感染ファイルからウイルスを駆除できない場合には、ファイルを検出時のままの状態でログに残し、隔離します(推奨設定)。隔離に関する詳細は、隔離されたファイルを参照してください。

- ウイルス駆除(不可能な場合はファイルを削除): 感染ファイルからウイルスを 駆除できなかった場合は、ファイルを削除します。この処理方法は、コンピュー タ上に重要なデータが無い場合にのみ選択してください。※感染ファイルを完全に 削除すると、場合によっては、Windowsの動作に影響を与える可能性がありま す。対象のファイルが、削除しても問題ないファイルの時にのみ、選択してください。。
- ファイルを隔離: 感染ファイルを暗号化して、隔離領域に移動します。隔離領域に 移動した感染ファイルは、後で修正できるように暗号化して保管され、有害な活動 ができないように暗号化されます。隔離に関する詳細は、隔離されたファイル を 参照してください。
- 削除:ファイルを削除します。※感染ファイルを完全に削除すると、場合によっては、Windowsの動作に影響を与える可能性があります。対象のファイルが、削除しても問題ないファイルの時にのみ、選択してください。

【操作を実行】をクリックすると、検出されたウイルスごとに、ユーザーが設定した処理が行われます。

これでスキャン終了です。ログを残すのみにしていた検出がある場合は、マルウェアはまだコン ピュータに残った状態になっていますので、ご注意ください。

ウイルス検出時の対応

ウイルスまたは他の不正プログラムが発見された場合、感染ファイルを以下の方法で処理できます。

▶ ウイルス警告	x
感染したアーカイブにアクセスしようとしました。	
ウイルス: EICAR-Test-File (not a virus) (エンジン A) ファイル: eicarcom2.zip リスト: E:¥test プロセス: explorer.exe	
٠	- F
操作:	
ファイルアクセスをブロック	-
🔲 すべてのアーカイブに適用	
OK	

感染ファイルにアクセスしようとした際に表示されるダイアログで、以下の処理方法を選択でき ます:

ファイルアクセスをブロック: 感染したファイルへのアクセスをブロックします。感染ファイルのウイルス駆除やファイル削除はされません。※一時的にアクセスはブロックされますが、ウイルスはコンピュータに残るため危険です。

- ウイルス駆除(不可能な場合はアクセスをブロック): 感染ファイルからウイルスを駆除できない場合には、ファイルへのアクセスをブロックします。※一時的にアクセスはブロックされますが、ウイルスはコンピュータに残るため危険です。
- ウイルス駆除(不可能な場合は隔離): 感染ファイルからウイルスを駆除できない場合には、 ファイルを検出時のままの状態でログに残し、隔離します(推奨設定)。隔離に関する詳細 は、隔離されたファイルを参照してください。
- ファイルを隔離: 感染ファイルを暗号化して、隔離領域に移動します。隔離領域に移動した感染ファイルは、後で修正できるように暗号化して保管され、有害な活動ができないように暗号化されます。隔離に関する詳細は、隔離されたファイルを参照してください。
- 感染ファイルを削除: ファイルを削除します。※感染ファイルを完全に削除すると、場合に よっては、Windowsの動作に影響を与える可能性があります。対象のファイルが、削除して も問題ないファイルの時にのみ、選択してください。

メールボックスの隔離に関しての注意: ※電子メールのメールボックス用のアーカイ ブは隔離しないでください。メールボックスのアーカイブ(拡張子.pst のファイルな ど)が隔離されると、メールプログラムはメールデータにアクセスできなくなり、メー ルプログラムは適切に機能しなくなります。

ファイアウォールアラート

オートパイロットを使用せずに**手動でルールを作成**モードを使用すると、未知のアプリケーショ ンやプロセスがネットワークへのアクセスを試みた際に、アクセスの許可/拒否について、ユー ザーに確認が行われます。

確認は、画面の右下からのポップアップで行われます。このポップアップでは、ユーザーは、ア プリケーションに対して、ネットワークアクセスを**一時的に許可/拒否**または**常に許可/拒否**と いう処理方法から選択できます。アプリケーションにアクセスを**常に許可/拒否**すると、操作が アクセスするネットワークのルールセットに取り込まれ、以降はアラートが表示されなくなりま す。

> ネットワークのルールセットに取り込まれたルールは、**ルールセット**の**コメントでア ラートにより作成**と表示されます。

下 G Data トータルプロテクション 2014				
3	アウトパウンド接続			
アプリケーション	🚺 setup_wm.ex	æ		
起動元:	🚺 wmplayer.ex	е		
ネットワーク:	ローカル エリア接続			
プロトコル:	TCP			
ポート:	http (80)			
IP ΣΚυλ:	157.56.59.199			
	許可しますか?			
		😡 一時的に許可		
1	拒否	💫 一時的に拒否		

アラートのポップアップ画面では、次の選択操作が可能です:

- 常に許可:アプリケーションに対して、表示されたネットワーク内でのネットワークまたはインターネットへのアクセスを常に許可します。ルールセット領域には、アラート経由で作成されたルールとして表示されます。
- 一時的に許可: アプリケーションに対して、ネットワークアクセスを1回だけ許可します。アプリケーションが再度ネットワークへアクセスを試みると、ファイアウォールが改めてアクセスの可否を問い合わせます。
- 常に拒否:アプリケーションに対して、表示されたネットワーク内でのネットワークまたはインターネットへの接続を常に拒否します。ルールセット領域には、アラート経由で作成されたルールとして表示されます。
- 一時的に拒否: アプリーションに対して、ネットワークアクセスを1回だけ拒否します。アプリケーションが再度ネットワークへアクセスを試みると、ファイアウォールが改めてアクセスの可否を問い合わせます。

アプリケーションが利用しようとしているロトコル、ポート、IPアドレスなどの情報もここのア ラート画面で確認できます。

ウイルススキャンで「not-a-virus」が表示される

「not-a-virus」 と表示されるファイルは、ファイル自身は不正機能を持っていませんが、ある 状況においては攻撃者によって不正利用され、コンピュータに危害を加えられる可能性があるア プリケーションです。

not-a-virus カテゴリには、キー配列自動変更ツール、IRCクライアント、FTPサーバー、プロセ ス作成(または隠す)ツールなどあります。

アンインストールの方法

本製品をアンインストールする場合は、以下の手順でアンインストールが可能です。

- Windows 10: Windows タスクバーで [ウインドウズロゴ] (通常はディスプレイの左下に 配置)を右クリックし、[コントロールパネル] を選択します。そこで [プログラム] > [プロ グラムのアンインストール] を選択します。表示されたリストから本製品を選択し、[アンイ ンストール] をクリックしてアンインストールを実行します。
- Windows 8.x: スタート画面(Modern UI)から、本製品のアイコンを右クリックし、画面下の[アンインストール]を選択します。表示された[プログラムと機能]ウインドウから、本製品を選択し、[アンインストール]をクリックしてアンインストールを実行します。
- Windows Vista, Windows 7: Windows タスクバーで [スタート] (通常はディスプレイの 左下に配置)をクリックし、[コントロールパネル] を選択します。そこで [プログラム]> [プログラムのアンインストール] を選択します。表示されたリストから本製品を選択し、 [アンインストール]をクリックしてアンインストールを実行します。
- Windows XP: Windows タスクバーの [スタート] をクリックして [設定] > [コントロール パネル] > [プログラムの追加と削除]</u>を選択します。表示された [プログラムの追加と削除] ウインドウから、本製品をマウスで選択します。そして [変更と削除] をクリックしてアンイ ンストールを実行します。

隔離済みファイルが隔離領域に残っていると、アンインストール中に、これらファイルを削除す るかどうかを確認されます。隔離ファイルを削除しない場合は、当該ファイルは暗号化されてコ ンピュータ上に保存され、アンインストール後もコンピュータ内に残ります(これらのファイル は本製品を再インストールしないと使用できません)。また、アンインストール中に、**設定とロ グ**を削除するかどうかについても確認されます。これらのファイルを削除せずにコンピュータに 残しておくと、ソフトウェアを再インストールした場合、保存されたログと設定が再び使用でき るようになります。

[終了]をクリックすると、アンインストールを終了します。これでソフトウェアがシステムか ら完全にアンインストールされます。

USB キーボードを間違ってブロックした場合

USBキーボードガードを使用中、接続したUSBキーボードを間違ってブロックもしくは許可した 場合は、以下の方法で該当キーボードの情報を削除することができます。

- 方法1: インストールされているG DATA製品をアンインストール、再インストールすると、 USBキーボードガードで設定したキーボードの情報は削除されます。 再度USBキーボードを接続すると、USBキーボードガードのポップアップが表示されますの で、そこで正しい設定を行ってください。
- 方法2(上級者向け): G DATA製品をインストールしたままで、レジストリエディタを使用 し、以下のレジストリキーを開いてください。

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\GDKeyboard Guard

このレジストリキー内に [HID\VID_…]で始まる値がありますので、これを削除してPCを再 起動すると、USBキーボードガードで設定したキーボードの情報は削除されます。 再度USBキーボードを接続すると、USBキーボードガードのポップアップが表示されますの で、そこで正しい設定を行ってください。

※方法2はシステムのレジストリを編集する方法ですので、操作を間違えるとシステムの動作 に影響を及ぼす可能性があります。この方法を実行する場合は、上記の説明が理解できるユー ザーが実行してください。

FAQ: ライセンスについて

複数台用ライセンスを所有している場合

複数台用ライセンスをご購入いただくと、取得したライセンスと同数のコンピュータに本製品を インストールして使用できます。1 台目のコンピュータへのインストールとインターネット更新 が終了すると、メールでアクセスデータが送信されます。2 台目のコンピュータにもソフトウェ アをインストールする時には、1台目の登録の際に発行されたユーザー名とパスワードを入力し ます。3 台目以降のコンピュータにもこの作業を繰り返します。

複数台用ライセンスの製品を複数のコンピュータで使用する際は、初回登録時にレジストレー ション番号を登録して発行された、インターネット更新用の**アクセスデータ**(ユーザー名とパス ワード)を、すべてのコンピュータで使用します。手順は以下のとおりです。

- 本製品を起動します。
- 2 セキュリティセンター画面で [前回のワクチン更新] をクリックし、プルダウンメニュ ーから [今すぐワクチン更新] をクリックします。
- 3 表示されるウィンドウに、初回登録時にG DATA から送られてきたメールに記載されているアクセスデータを入力します。[OK]をクリックすると、更新ができるようになります。

※複数台用ライセンスは、1台目コンピュータでレジストレーション番号を初回登録した段階から、購入したライセンスの年数分使用できるようになります。2台目以降のコンピュータでも、 その最初に登録したコンピュータと共通の期限が使用されますのでご注意ください。

例:1年/3台版のライセンスを購入した場合

2014/7/1 に1台目のコンピュータでレジストレーション番号を初回登録、 2014/10/1 に2台目のコンピュータにアクセスデータを登録したとすると、全てのコ ンピュータのライセンス有効期限は、1台目のコンピュータで初回登録を行ってから1 年後の 2015/7/1 までになります。

これは、もし 2015/7/1 以降に3台目のコンピュータにアクセスデータを登録して も、期限切れになる、という事も意味します。

そのため、複数台用のライセンスを使用する場合は、初回のレジストレーション番号 の登録が終わり次第、速やかに残り全ての対象コンピュータでアクセスデータの登録 を済ませるのが、ライセンスの効率的な使用方法となります。

Android版について

複数台用ライセンスを所有している場合はライセンスをAndroid版でも使用することができま す。その際はAndroid版1台につき、1台分のライセンスが使用されます。ライセンスの使用方法 は購入したライセンスにより異なりますので、初回登録時に送付された「認証処理完了のお知ら せ」メールに記載された説明をご覧ください。

※マルチライセンスを含む一部ライセンスではAndroid版は利用できません。

ライセンスの期限が切れた場合

ライセンスの期限切れが近づくとポップアップのメッセージでお知らせします。このポップアッ プメッセージをクリックすると、ダイアログが開き、ここから更新の手続きを行うことができま す。

> **メモ**: 法人向け販売パートナーから購入したライセンスの場合(マルチライセンス製品 など)は、お買い上げいただいた販売パートナーへお問い合せください。

コンピュータを買い替えたり、クリーンインストールした場合

コンピュータを買い換えたり、クリーンインストールした場合は、本製品をコンピュータにイン ストールし、初回登録時に G DATA から送付されたアクセスデータを入力します。アクセスデ ータの入力は、インストールもしく更新の項を参照してください。

> メモ: ライセンスの移行には回数制限が設定されています。この回数を超えた場合は、 更新期限が有効でも更新がロードできなくなりますので、ユーザーサポートに問い合 わせください。

データ保護に関する声明

本ソフトウェアのデータ保護に関する声明

G DATA製品には、特定条件下においてデータをG DATAのクラウドサーバーへ送信する保護コンポーネントが 含まれています。保護コンポーネントのコア機能を正常に機能させるために必要な特定データは、常に同サーバ ーへ送信されます。保護コンポーネントの1つ、ウェブ保護には、ウェブサイトのアドレス送信が必須となりま す。また、別の保護コンポーネント、バンクガードでは、新種のバンキング系トロイの木馬の特定・削除のた めに、チェックサムの送信が必要となります。更に、ふるまい検知(ビヘイビアブロッカー)の機能は、クラウ ドからの情報を取得することにより、コンピュータをより効果的に保護できますが、これには、不審なファイ ルに関する特定の情報をクラウドサーバーへ送信する必要があります。

また、送信されるデータは、他のコンポーネントにおいても重要な意味を持っています。ユーザー様から送信さ れたデータは、G DATAのセキュリティラボで有書なファイルを検証や挙動の分析に使用されます。検証結果 は、G DATAの保護コンポーネントの改善やG DATA製品のユーザーへの有害プログラムに関する情報やその影 響を提供します。詳細は、マルウェア情報イニシアチブ(MII)のデータ保護に関する声明をご覧ください。な お、MIIへの参加は任意です。MIIへの参加を無効化しても、G DATAによる保護メカニズムは、その効果を制限 されません。

<u>重要: これらの機能で収集される情報には、個人情報は含まれません。また、取得した情報を使って個人の</u> 特定を行うことはありません。

・ウェブ保護によるデータ収集

G DATA ウェブ保護とは?

インターネットには、数多くの有害サイトや詐欺サイトが存在しています。これらのサイトは、マルウェア配布 や適切な保護が施されていないコンピュータを感染させるための感染経路(Drive-By-Infection)として使われ ており、個人情報を盗み出したり(例: PaypalやFacebookのサイトフィッシング)、スキャムなどの詐欺と して使用されている可能性があります。G DATAは、有害サイトへのアクセスを遮断するブラックリストを独自 に管理・保守しています。G DATAウェブ保護は、次の2種類のテクノロジーがベースとなっています。

1. HTTPスキャン。この機能は、既知の有害コードがないか、ウイルススキャナでスキャンしてHTTPトラ フィックをチェックする機能です。有害コードが見つかった場合、G DATAが警告を発します。なお、警告が表 示された場合、ユーザーが安全性に関する判定情報を、任意で送信できるケースがあります。

2.フィッシング保護。この機能は、リクエストされたアドレスがフィッシングサイトではないか、G DATA が管理・保守するブラックリストと照合し、フィッシングサイトであった場合は警告を発する機能です。このURL ブラックリストには、無数の有害サイトや詐欺サイトの情報が保存されています。なお、フィッシング警告が表示された場合、ユーザーが安全性に関する判定情報を、任意で送信できるケースがあります。

収集される情報の種類は?

リクエスト先のウェブサイトがG DATAのURLブラックリストに存在するかチェックするため、ウェブサイトの アドレスをクラウドサーバーに送信します。

収集された情報の使用方法は?

リクエスト先のアドレスは、G DATAのデータベースに保存されますが、リクエスト送信元のユーザーもしくは PC情報は保存されません。ウェブサイトのアドレスは、まずG DATAの分析システムに転送され、次のステッ プで、有害もしくは不審な構成部分をチェックします。不審なウェブサイトのアドレスは、G DATAセキュリ ティラボの分析システムに転送されます。分析によって不審サイトと確認された場合は、このサイトはブラック リストに追加されます。

G DATAのクラウドサーバーとリクエスト送信元コンピュータの間の接続中は、送信元コンピュータのIPアドレ スが送信されますが、通常、このIPアドレス情報はG DATA側では保存されません。ウェブサイトがブロックさ れた場合は、IPアドレスをもとに国情報を識別しますが、IPアドレスは識別後に破棄します。そのため、G DATA側でリクエスト送信元の個人を特定することはできません。

・G DATA バンクガードによるデータ収集

G DATA バンクガードとは?

G DATA バンクガードは、ブラウザのメモリ領域が破損状況やマルウェアによる改竄など、ブラウザが暗号化 された情報の送信に使用するシステムライブラリを監視する機能です。G DATA バンクガードがこの領域への 攻撃を検出すると、保護メカニズムが作動し、攻撃されたブラウザを通常ステータスに戻します。その後、攻 撃を引き起こした有害ファイルをシステムから見つけ出し、除去します。

収集するデータの種類は?

ブラウザのメモリが攻撃された場合、次の情報が送信されます。

バージョン番号

- G DATA 製品および同コンポーネント
- ブラウザおよび同コンポーネント
- OS情報

チェックサム

- 攻撃元および攻撃に関わったファイル
- 削除されたファイル

匿名 GUID

 発生した事象を特定のコンピュータを関連付けるため、コンピュータのGUID情報を取得します。なお、 GUIDは同一の情報が存在する可能性は非常に低く、GUIDからコンピュータの場所や個人の特定はできません。

攻撃時のアクティビティ情報

- 攻撃を特定マルウェアに関連付けるため、攻撃種類をもとにマルウェアを特定するフィンガープリントを取得します。フィンガープリントはシステムライブラリの呼び出しに基づくもので、これには個人情報は含まれません。
- 各システムライブラリで危険にさられている機能の名称

マルウェア除去時のアクティビティ情報

- 削除されたレジストリエントリ
- 削除時: ルートキットの種類(例: Watchdog/Versteck via Hook)

収集された情報の使用方法は?

バージョン番号は、発生した事象とプログラムバージョンを関連付けるために使用します。これは、エラー発生 数の減少と脆弱なシステムの特定に役立ちます。

関連付けられたファイルのチェックサムは、G DATAのデータベース内の有害ファイルとの照合やさらに詳しい 分析を行う上で、役立ちます。G DATAが保しない新たな脅威が発生した場合、この脅威は、リクエストリスト へと入れられます。そして、次にこの脅威へのリクエストが確認された場合、実際にファイルが転送されます。 このリクエストは、同じコンピュータから複数回送信されることはほぼありません。このリクエストは、実行 可能なファイルの場合にのみ、送信されます。ドキュメント、画像、またはその他の個人情報を含むファイルな どは、送信されません。

フィンガープリントで、マルウェアを特定の系種に識別できます。同じ系種に属するマルウェアは同様の手法を 用いて駆除できます。

クラウドサーバーとリクエストされたコンピュータ間の接続中は、リクエストされたコンピュータのIPアドレス 情報が取得されますが、これは保存されません。ウェブサイトが有害と判定された場合、このIPアドレスを用い て、リクエスト元の国情報を取得します。このプロセスの後、IPアドレスは破棄されるため、G DATA でユー ザー情報の詳細を特定することはできません。

攻撃時のアクティビティ、更に攻撃に関わったり、削除されたファイルおよびレジストリエントリの情報は、削 除ルーチンの分析・開発に役立ちます。これらのデータを使うと、新たな脅威や攻撃に迅速に対応できるよう になります。

特定のデータは統計に使用されます。系種別の出現頻度などはG DATAのホワイトペーパーやマルウェアレポートで使用されます。また、これらの情報は、作業プロセスの優先度の決定や自動化にも使われています。

・ふるまい検知およびファイルクラウドセキュリティによるデータ収集

ふるまい検知とは?

ふるまい検知は、コンピュータ上のすべてのアクティブなプログラムによる不審な動きを監視する機能です。ふ るまい検知では、プログラムによる挙動がすべてポイントで計算され、特定の値を超えると、当該プログラムを 終了に導きます。特定の条件下においては、ふるまい検知は不審なファイルのチェックサムをG DATAのサーバ ーへと送信し、既知のマルウェアファイルと照合します。チェックサム送信の条件は、プログラムのダウンロー ド時、プログラムの初回起動時、プログラムによるある程度の不審な動きが実行された場合などがあります。 ファイルが有害であると判断された場合は、プログラムの実行を中止するかどうか、ユーザーに確認します。

収集するデータの種類は?

ファイルをチェックする場合、チェックサム情報を取得し、サーバーに送信します。更に、ふるまい検知が有害 度評価のために取得されたパラメーター(例:有害度(0-1)、評価したルールのID番号)が送信されます。 ファイルが有害と判定された場合、プログラムの呼び出しパラメーターが取得されます。警告メッセージに対す るユーザーの操作情報も送信されます。また、ログ、ルールセット、G DATA製品のバージョン番号も送信され ます。

収集された情報の使用方法は?

有害度の数値(チェックサムによって識別)は、有害なファイルをG DATAが保するマルウェアデータベースでの照合に使用します。このファイルは、ピンポイントで分析され、場合によっては、ブラックリストでブロック されます。ユーザーの操作情報は、誤検出の発見や修正に役立ちます。

・G DATA マルウェア情報イニシアチブの収集データのデータ保護に関する声明

上で述べた保護コンポーネントで必要なデータを除き、マルウェアイニシアチブでは、参加に協力頂いたユーザ ー様から、以下の情報を収集しています。これらの情報は、保護メカニズムの分析・開発の迅速化に役立つの で、ぜひ参加にご協力ください。

G DATA マルウェア情報イニシアチプとは?

G DATA セキュリティラボでは、G DATA 製品をご利用のユーザー様を、コンピュータの安全性を脅かす脅威 からから保護するため、保護・対策の研究や分析に絶え間なく励んでいます。 マルウェア研究では、マルウェ アに関する情報が多ければ多いほど、効果的な保護メカニズムの開発をいち早く進めることができます。これ らの情報をG DATA の研究・分析・開発に効率的に取り入れることを可能にするための取り組みが、G DATAマ ルウェア情報イニシアチブです。 これにより、マルウェアに関するデータをG DATAセキュリティラボに送信 することができます。 より多くのユーザー様に参加頂くことで、他のG DATA製品をご利用の方々もインター ネットをより安全に利用できるようになります。

収集される情報の種類は?

原則として、次の3種類のデータ収集方法があります。

- 1.G DATAの保護メカニズム(ウイルススキャナ、ふるまい検知、バンクガードなど)が、ユーザー様のコン ビュータ上で有害ファイルが検出された場合(送信する情報は保護メカニズムによって異なります)
- 2. ウェブサイト上で有害なコンテンツが発見された場合
- 3. ユーザー様自身が任意でG DATA セキュリティラボにデータを送信した場合

ユーザー様がマルウェアファイルをG DATA セキュリティラボへ送信すると、システムは送信されるファイルの ほかに、ワクチン情報、スキャンエンジンのバージョン番号、発見場所、オリジナルのファイル名、作成日とい う情報が一緒に送信されます。

有害なインターネットコンテンツを検出した場合は、次のデータが送信されます。

- マルウェア情報のバージョン
- G DATA 製品および使用スキャンエンジンのバージョン番号

G DATA USER MANUAL

- 使用しているOSの言語
- コンピュータのIPアドレス匿名化のためのハッシュ
- ブラウザのユーザーエージェント
- アクセスを遮断したURLと遮断した理由(マルウェアサイト、フィッシングサイトなど)
- マルウェア名

不審な実行可能ファイルが検出された際は、次の情報を取得します。また、検出したファイルは、送信すること もできます。

- 有害または不審なファイルのチェックサム
- ファイルサイズ
- ファイルに署名されている場合は、証明書の情報
- 攻撃に関わった有害または不審なファイルの検出場所
- 使用しているOSの言語
- コンピュータのIPアドレス匿名化のためのハッシュ
- 攻撃後に削除されたファイルの匿名パス
- 特定の条件下(GDATAが未所の新たな脅威が発生した場合)では、攻撃に関わったファイルのダウンロードをGDATAが要求することができます。送信されるファイルは、攻撃に関わっている実行可能なファイルのみです。

重要: 収集される情報には、個人情報は含まれません。また、取得した情報を使って個人の特定を行うこと はありません。

収集したデータの利用方法は?

データの処理および保存にあたっては、各国で適用されるデータ保護ならび開示に関する法規が適用されます。GDATAは、すべてのデータを不正アクセスから保護するため、厳重にデータを管理します。

ウェブサイトのアドレス情報は、まず選定が行われますが、有害または詐欺サイトの共通点を突き止める用途に 使用されます。分析結果はURLブラックリストやG DATA の他の保護メカニズムにも反映されます。特定のデ ータは、統計分析や開発などに使用されます。

不審なファイルに関する情報は、G DATA で関連ファイルとの照合や有害プログラムの挙動を分析に使用しま す。取得した情報は、詳しい分析を行うためのベースとなる重要な要素です。目的は、保護メカニズムによる保 護や駆除機能の改善となります。

有害プログラムの挙動を検証するには、有害ファイルが必要です。このため、ファイルをG DATAに送付するこ

とができます。送信するファイルは、実行可能なファイルのみです。文書やデータベースなど個人情報を含む ファイルは送信されません。更に、ファイルは2つのステップを踏んで送信されます。まず、最初のステップで は、チェックサムもしくは他の共通プロパティを用い、ファイルをリクエストリストに入れられます。ファイル が再びリクエストされると、アップロードが開始されます。これが第2のステップです。このリクエストが同じ コンピュータから発生するケースはほぼありません。ファイルは、その後G DATA セキュリティラボで詳しく 検証されます。統計データは、優先度の決定(例:頻度が高いほど、優先的に処理)、またはG DATAが作成す るレポートに活用されます。マルウェアを削除するツールも、同様となります。

データの評価はG DATAセキュリティラボ内で行われ、評価結果はITセキュリティ分野の研究事案の解明にのみ 利用されます。 収集データ利用における最大目標は、安全上のリスクの研究と保護メカニズムの開発です。 収 集したデータの評価結果は例えば、ブラックリストの作成、専門記事発表のための統計、セキュリティ技術用 ルールの開発などに利用されます。 このイニシアチブへの参加は任意であり、参加されなくてもご利用頂く製 品の機能に影響がでることはありません。 G DATAマルウェア情報イニシアチブにご参加頂くことにより、今 後すべてのG DATAユーザーがコンピューターへの脅威について、より詳細な情報を得ることができるようにな るとともに、ご利用のコンピュータの保護精度が向上します。

G DATA製品によるデータ収集へのご理解とマルウェア情報イニシアチブ参加へのご協力頂きますよう、何卒宜 しくお願い申し上げます。

コピーライト

Copyright © 2018 G DATA Software AG Engine: The Virus Scan Engine and the Spyware Scan Engines are based on BitDefender technologies © 1997-2018 BitDefender SRL. OutbreakShield: © 2018 CYREN Ltd. [G DATA – 2018/03/08, 15:45]

G DATA USER MANUAL

索引

Г

「読み取りモード」で開く 78

1

1 - 10 分 86 1st Boot Device 141

2

2nd Boot Device 141 2つのエンジン (推奨) 93

Α

AUTOSTRT.EXE の実行 5 AVKBackup 44 AVKBackup.exe 44

В

BIOS 141

С

CD/DVD からのブート 141 CD/DVD ドライブ 134 CD/DVD ヘのアーカイブ書き込み 52 CD/DVD-ROM:, C: 141 CD/DVDへのアーカイブ書き込み 51 CD/DVD版 5 CD/DVD版 5 CD版製品でのブートスキャン 142 Copyright 162

D

Dropbox 41

E

Enter キー 141

F

FAQ 4 FAQ: ブートスキャン 141 FAQ: プログラムの機能 145 FAQ: ライセンスについて 154

G

G Data AntiVirus 142 G Data AntiVirus - Alternative 142 G Data AntiVirus - Alternative 142 G Data AntiVirus + Backup - Alternative 142 G DATA アイコン 12,145 G DATA ウェブサイト 4 G DATA ウェブサイト 4 G DATA ショートカット 12 G Data ブートスキャン 142 G DATA を起動 145 G DATA (製品名)を起動 145 G Data Boot-Medium 142 G Data Boot-Medium - alternative 142 Google ドライブ 41

Η

HTMLスクリプトの無効化 120

I

IMAPI 2.x がインストールされていません 142 IP アドレス範囲 35

Μ

Microsoft Outlook 14, 106, 109, 119 Microsoft Update の検索中に Office のアップデートを検索 129 Microsoft Windows 141

Ν

NetBIOS 32 not-a-virus 151

0

OK 154

Ρ

PST拡張子ファイル 149

S

Setup 5 Setup.exe 5 SSD 129 start.exe 84

Т

Thumbs.db 44 tsnxg 81 TSNxG_4 84

U

URL 64,105,140 USB からのブート 141 USB キーボードガード 91,152 USB キーボードを間違ってブロックした場合 152 USBメモリを利用したプートスキャン 142

V

VPN 32 VPNサービスを許可/拒否 32

W

Windows ボリューム シャドウ コピーを使用 44 Windows ユーザー アカウント 64 www.gdata.co.jp 4

Other

アーカイブ 44 アーカイブする前にウイルススキャンを実行 44 アーカイブのインポート 44,51,53 アーカイブのオンライン管理 51 アーカイブのスキャン 95,99,114 アーカイブのファイルサイズを制限 44 アーカイブの全ファイルを復元 48 アーカイブの更新日時が新しい場合のみ上書き 48 アーカイブの選択したファイルのみ復元 48 アーカイブを作成後にチェック 44 アーカイブを暗号化 44 アーカイブ名 41 アイドリングスキャンでも例外を有効にする 98 アイドリングスキャンを使用 14 アイドリングスキャンを無効にする 14 アウトブレイクシールド 107 アクセス 35 アクセスデータ 5.154 アクセスデータの確認 5 アクセスデータを入力 5 アクセスをブロック 134 アクセスを拒否するネットワーク 30.31 アクセス拒否されたファイル 147 アスタリスク 44 アダプティブ モード 34 アプリケーション レーダー 26 アプリケーションアラートのキャッシュ 126 アプリケーションごと 126 アプリケーションを許可/拒否 32 アプリケーション割当て 35 アラート 35.126 アラートにより作成 35 アラートの保留数を指定 126 アンインストール 152 アンインストールの方法 152 アンチウイルス 13, 20, 22, 93 アンチウイルスのログ 139 アンチスパム 14.117 アンチスパムを無効にする 14 イメージ バックアップ 39 インストール 5.63 インストールの完了 5 インストールの開始 5 インストール後 12 インストール手順 5 インストール方法の選択 5 インターネットコンテンツ (HTTP) のスキャン 103 インターネットサービス割当て 35 インターネットに直接接続 30,31 インターネット一時フォルダ 44 インターネット利用時間の監視 63,69 インターネット接続共有 29 インターネット接続共有を許可/拒否 32 インターネット設定 100,101,103,117 インポート 14,117 ウイルス 107 ウイルス アラート 149 ウイルスガード 14,93 ウイルスガードを無効にする 14,145 ウイルスガード用の例外設定 94 ウイルスが検出されたら 142 ウイルスが検出された場合 147

ウイルススキャン 12.14.22.145 ウイルススキャンで「not-a-virus」が表示される 151 ウイルススキャンのスケジュール設定 110 ウイルススキャンの流れ 147 ウイルススキャンを実行 147 ウイルススキャン用の例外設定 98 ウイルス保護 147 ウイルス対策 13,20 ウイルス検出時の対応 149 ウイルス駆除 24 ウイルス駆除(不可能な場合は隔離) 93,97,149 ウイルス駆除(不可能な場合はアクセスをブロック) 149 ウイルス駆除(不可能な場合はファイルを削除) 147 ウイルス駆除(不可能な場合はログを残すのみ) 147 ウイルス駆除(不可能な場合は添付ファイル / メール本文を削除) 107 ウイルス駆除(不可能な場合は隔離) 114,147,149 ウェブサイト アドレス (URL) 105 ウェブ保護 14,103 ウェブ保護を無効にする 14 ウェブ保護用の例外設定 105 エクスプロイト対策 93 エクスポート 14.117 エンジンの種類 90,93,97,107,114 オートスタート(遅延あり) 86 オートスタート(遅延なし) 86 オートスタートマネージャー 20.86 オートパイロット 14,26,124 オートパイロット モード 124 オートパイロットを無効にする 14,145 オプション 44 オフライン更新 100 オンライン ヘルプ 4 オンラインストレージサービスへのバックアップ 41 オンラインバンキング対策 14.103 お気に入り 57 カスタムインストール 5 キーボード 152 キーボードをブロック 91 キーボードを許可 91 キーロガー対策 103 キーワード (メール本文)を使用 117 キーワード(件名)を使用 117 キャンセル 142 クイックスキャン 12 このネットワークでファイアウォールを有効にする 29 このユーザーのフィルタリング 63 コピーライト 162 コメント 35 コンテンツフィルタ 120 コンテンツフィルタを使用 117 コントロールパネル 152 コンピュータの自動再起動をチューナーに許可しない 129 コンピュータをスキャン 14.22 コンピュータをスキャン (すべてのローカルドライブ) 22 コンピュータを買い替えたり、クリーンインストールした場

コンピュータ利用時間の監視 63.70 サーバー ポート番号 105.109 サイズ 139 サイトへのリンク 67 サポート期間 4 システム ファイル 44 システム ファイル(ファイルの属性) 44 システム負荷が高い時はウイルススキャンを停止 147 システム起動時 113 システム起動時にシステム領域をスキャン 95 システム領域のスキャン 99.114 シュレッダー 12 ジョブ 111 ジョブの種類 139 ジョブ実行ユーザー 44 スキャン オプション 107 スキャン範囲 112 スキャン終了後にコンピュータの電源を切る 147 スキャン終了後にコンピュータの電源を切る(ユーザーがロ グインしていない場合) 111 スキャン設定 114 スケジュール 42, 113, 130, 133 スケジュール チューニング 60.133 スケジュール チューニングを有効にする 60 スケジュール実行後にコンピュータの電源が切れていた場合 、次回の起動時にジョブを実行 113 スタート 142 ステータス 14.26.139 ステップ1-インストールの開始 5 ステップ2-インストール方法の選択 5 ステップ3-使用許諾契約 5 ステップ4-カスタムインストール(オプション) 5 ステップ5-製品種類の選択 5 ステップ6 - ライセンスの認証 5 ステップ7-インストールの完了 5 ステルス モード 34 スパム アウトブレイクシールド 117 スパム フィルタ 117 スパムの可能性があるメール 119 スパムの可能性が非常に高いメール 119 スパムの可能性が高いメール 119 スパムフィルタを使用 117 すべて選択 61 セーフの作成 55 セーフの保存場所と容量 76 セキュリティ 26.130 セキュリティ / パフォーマンス 14 セキュリティ アイコン 145 セキュリティ ステータス 13 セキュリティ センター 13 セキュリティ/パフォーマンス 90 セキュリティセンター 20,100,145,154 セキュリティを編集 26 その他 123,128 タイトル 64

ダイヤラ/スパイウェア/アドウェア/リスクウェアのスキャン 95, 99, 114 ダウンロードの容量制限 105 ダウンロード版 5 ダウンロード版製品でのブートスキャン 142 チェックサムテスト 127 チェックサムテストの実行 127 チューナー 20,60,129 ツール 57.106 データセーフ 20.75 データセーフのドライブを自動選択 77.81 データセーフのパラメータ 81 データセーフの名称 77 データセーフの容量 76.83 データセーフの設定 80 データセーフへのアクセス 78 データセーフを新規作成 75,76 データセーフを記憶媒体と結合する 81 データセーフを開く 145 データセーフ作成ウィザード 76 データ保護 130 データ保護に関する声明 156 テーブルコンテンツを検索 117 テーブルをリセット 117 デスクトップ ショートカットを削除する 129 デバイス コントロール 134 デバイス コントロールのログ 140 デバイス コントロールを有効にする 134 デバイス/ドライブ 140 デバイスコントロール 20.88 デバイスの説明 140 デバイス固有のルール 134 デフォルトで使用するウィザードの種類 128 デフォルトルール 35 デフラグ時にドライブの種類をチェックしない 129 ドメインサービスを許可/拒否 32 ドライブの割り当て 77 ネットワーク 26.28 ネットワークアクセスのスキャン 95 ネットワークサービスを許可/拒否 32 ネットワークについて 29 バージョンチェック 100 パーソナル フィルタ 64 パーソナル フィルタを作成 64 パーソナルフィルタ 73 パーソナルフィルタを作成 67 ハードディスク 129 ハードディスクのクローン 51 ハードディスク復元時に完全性をチェック 44 はじめに 4 パス 32 パスワード 48.78.92 パスワード(暗号化) 48 パスワードセーフ 55 パスワードのヒント 92 パスワードの削除 92 パスワードマネージャー 55.57 パスワードを歳入両k 78

パスワード保護 92 パスワード保護されたアーカイブ 147 パスワード再入力 92 パスワード生成 57 バックアップ 20.38.137 バックアップ(復元) 25 バックアップ/復元 25 バックアップジョブ用デフォルト設定にリセット 44 バックアップと復元 38.139 バックアップのログ 139 バックアップの対象と保存先が同一ドライブ上にないか確認 する 137 バックアップを復元 48 バックアップ日時 139 バッテリーモードでは実行しない 42 バッテリモードでは実行しない 113 パフォーマンス 130 バンクガード 14,103 ビヘイビア ブロッキング 93 ヒューリスティック 95,99,114 ファイアウォール 14, 20, 26, 124 ファイアウォール | ネットワーク 26 ファイアウォール アラート 31, 35, 150 ファイアウォールのログ 139 ファイアウォールを無効にする 14,145 ファイアウォール無効 124 ファイル システム 77 ファイル バックアップ 39 ファイル/ハードディスク/パーティションの選択 39.42 ファイルアクセスをブロック 147.149 ファイルおよびプリンタ共有を許可/拒否 32 ファイルが KBに達したときにメッセージを表示 74 ファイルの種類 99.114 ファイルの選択 39 ファイルを元のフォルダに復元 48 ファイルを削除 147 ファイルを隔離 93.97.147.149 ファイル保護 132 ファイル名 132 ファイル形式 44 ファイル拡張子 120 ファイル数 139 フィッシング保護 103 フィルタ 64.67 フィルタリング 20.63 フィルタリングのログ 140 ブート 141 ブートスキャン 25.141 ブートスキャンの流れ 5.142 ブートスキャンの準備 141 ブートスキャンを中断するには 141 ブートメディア 25.141 ブートメディアの作成 51,53 ブートメディアを作成 25.142 フォルダ/ファイルをスキャン 22 フォルダツリー 48 フォルダをスキャン 14

フォルダ保護 131 フォルダ名 119.120 ブラウザのタイムアウトを防止 105 ブラウザプラグインの使用方法 57 ブラウザ保護 103 プラグイン 57 ブラックリスト 73 ブラックリストに登録 14 ブラックリストを使用 117 ブラックリストを編集 14 フル バックアップ 42 フル バックアップの実行 42 フル バックアップを復元 48 フル バックアップ後に自動的に削除 42 フルスクリーンアプリケーション実行時にオートパイロット を実行(ゲームモード) 124 ふるまい検知 93 ふるまい検知を無効にする 14 プロキシ サーバー 103 プロキシ サーバーを使用 103 プログラムと機能 152 プログラムの追加と削除 152 プログラム起動時に受信トレイの未読メールをスキャン 123 プログラム起動時に受信トレイの未読メールをスキャン (Mi crosoft Outlook のみ) 123 プログラム起動時のチェック 128 ブロックの理由 140 フロッピー ドライブ 134 プロトコル 35 プロトコル/ポート/アプリケーションごと 126 プロパティ 87 ヘッダー 120 ヘルプを表示 13 ポート 32 ホワイトリスト 67.73 ホワイトリストに登録 14 ホワイトリストを使用 117 ホワイトリストを編集 14 マニュアル 4 マルウェア情報イニシアチブ 5,156 マルウェ情報イニシアチブ 24 マルチセッション CD/DVD の作成 44 マルチユーザーライセンス 154 メール [件名] には次のウイルスがあります: [ウイルス名] 107 メール アーカイブのスキャン 95, 99, 114 メールアドレス (PC用) 101 メールスキャン 14,106 メールの件名と本文にスパム警告を挿入 119 メールボックスの隔離に関しての注意 149 メールをフォルダに移動 119.120 メールを拒否 119.120 メール保護 14 メール保護を無効にする 14 メール本文 120,123

メール本文にメッセージを挿入 120 メタタグ 64 メッセージが拒否されました 123 メディア 82 メディアの交換時にシステム領域をスキャン 95 XŦ 57 メモリおよびスタートアップをスキャン 22 モード 26.95 モジュール 20 モバイル データセーフを作成 75 モバイルデータセーフを作成 81 モバイルデータセーフを開く 84 ユーザー 63.64 ユーザーアカウント 116 ユーザーサポート 4 ユーザーの接続履歴 140 ユーザー名 140 ユーザー名とパスワード 154 ユーザー固有のルール 134 ユーザー定義 5.90 ユーザー定義セキュリティ 124 ユーザー定義セキュリティ(上級者向け) 126 ユーザー情報 44 ユーザー認証(初回用) 100 ユーザー認証(初回用) 101 ライセンス 19 ライセンスの更新 19 ライセンスの有効期間が切れた場合 19 ライセンスの期限が切れた場合 155 ライセンスの移行 155 ライセンスの認証 5 ライセンス更新 155 ランク 35 ランク順 35 リアルタイムブラックリストを使用 117 リアルタイム保護 14,93 リムーバブル ディスク (例: USBメモリ) 134 リムーバブル メディアをスキャン 22 リムーバブルメディアとして開く 78 リムーバブルメディアをスキャン 99 ルートキットのスキャン 99,114 ルートキットをスキャン 22 ルール 31,35 ルールウィザード 32,35 ルールセット 26, 28, 29, 30, 31, 34 ルールセットを作成 29 ルールセットを編集 29 ルールセット名 31 ルールにないアクセスが検知された場合の操作 34 ルールの作成 126 ルールの作成基準 126 ルールを編集 35 レジストレーション番号 5,101 レジストレーション番号を入力 5 ロード済みモジュールのチェックサムテスト 127 ログ 13, 35, 38, 74, 100, 139, 140, 147 ログ: スパム 14

ログ: スパム以外 14 ログアウト時にセーフを閉じる 78 ログイン情報 57 ログに残すのみ 147 ログの作成 99.114 ログを作成 100 ログを削除 74.140 ログを残すのみ 149 ロック 57 ロック解除 55 ワイルドカード 44 ワクチンのインポート/エクスポート 100 ワクチンの更新 14 ワクチンを更新 142,145 ワクチン更新 145,154 一時ファイル 44 一時ファイル(ファイルの属性) 11 一時ファイルの保存先フォルダ 137 一時ファイルを完全に削除 129 一時ファイル用フォルダ 44 一時フォルダ 44 一時的なアーカイブを削除 44 一時的に拒否 150 一時的に許可 150 一般 90,111,129 一般ルール 134 一般的なアーカイブ オプション 44 上級者用設定 120 不明なサーバー アプリケーション 126 中圧縮率 44 今すぐチューニング 60 今すぐ実行 14 今すぐ購入 19.155 他のメールプログラム (POP3 を使用) 123 代替メール 123 件名 120,123 低スペックのコンピュータ用 90 低セキュリティ 124 体験版として登録 5 作成 80 使用許諾契約 5 例外 64, 94, 98, 103 例外を設定 14 保存先の選択 41 保存場所 76 保護されていないワイヤレス ネットワーク 126 保護する台数を増やす 19 信頼性の低いネットワーク 30,31 信頼性の高いネットワーク 30,31 個々の復元ポイントの作成を許可 129 停止 142 元に戻す 24 共同利用 78 共通機能 13 内容 139 処理方法 119,120 削除 14, 24, 30, 73, 75, 105, 131, 132, 139, 147 削除された項目の詳細情報を含むログファイルを作成しない 129 削除しない 42 前回のアイドリングスキャン 14 前回のウイルススキャン 14 前回のチューニング 60 前回のワクチン更新 14 動作環境 5 印刷 139 受信トレイをスキャン 106.109 受信メール 107 受信メールのスキャン 107 古いアーカイブを削除 42 古いデータを削除する 129 名 101 名前 34.35 名前をつけて保存 139 回までフルバックアップを保存 42 圧縮 44 埋め込みメール 120 埋め込みメールの添付ファイルもフィルタ 120 増分 42 変更 5 姓 101 媒体 82 完了 48.83 完全 5 完全アンインストールツール 5 実行頻度 113.133 容量変更時のみ上書き 48 差分 42 差分バックアップ時にデータを検証 44 常に上書き 48 常に拒否 150 常に許可 150 後で認証を行う 5 復元 25.38.48.53.60.61 復元データを削除する 129 復元プログラムのコピー 44.52 復元を開始 53 情報 13.140 感染したアーカイブ 93.97.114 感染したウェブページのアドレスを送信 103 感染したファイル 93,97,114 感染した場合 107 感染ファイルを削除 149 感染メールへのレポート添付 107 手動 42 手動スキャン (オンデマンド スキャン) 97 手動でルールを作成 26,124 拒否されたコンテンツ 140 拡張ルールセット エディタ 34.35 拡張ルールセットエディタ 32 拡張ルールセットエディタへ切換え(エキスパートモード) 32 接続の方向 32,35 接続ログの保存 128 推奨ルールを含むルールセットを生成 31

撃退した攻撃 26 操作 51.147 操作の実行 147 操作を実行 147 新しいセーフを作成 55 新しいファイルと変更したファイルのみスキャン 95,99 新しいフォルダ 41,48 新規 14 新規ジョブ 38.39 新規バックアップ ジョブ 38.39 新規ユーザー 63.64 新規ユーザーを追加 64 新規作成 30, 31, 35, 67, 73, 94, 98, 105, 110 日付 140 日付/時刻 140 時刻 140 時間 35.113.133 時間切れの前に警告を表示 70 時間枠 35 暗号化された接続 (SSL) 108 更新 5, 13, 14, 24, 75, 100, 142 更新できました 142 更新日時が変更された場合のみ上書き 48 書き込み後にデータを検証 52 最小 5 最高セキュリティ 124 有効 133 有効なルール 35 有効期限 134 有害な添付ファイルのフィルタ 120 期限切れ 134 本文 64 本製品をインストールしてコンピュータを再起動した際に、 Windows が起動しない場合 12 検索マスク 132 検索基準 120 検索対象 64 検索対象の領域 64 検索範囲 120 構成 60 標準 109 標準インストール 5 標準スペックのコンピュータ用(推奨) 90 標準セキュリティ 124 権限付与 78 次のフォルダとファイルをスキャン 112 次回のワクチン更新 14 毎日 42.133 注意!このメールはウイルスに感染しています 107 添付ファイルのフィルタ 120 添付ファイルのみ名前を変更 120 無制限 134 理由 140 疑問符 44 登録 101 登録に成功しました 101 登録日 105

禁止するコンテンツ 63.64.73 禁止する基準 64 禁止する時間 70.72 種類 139.140 空のルールセットを生成 31 第1ブートデバイス 141 第2ブートデバイス 141 終了 142 統計 145 統計情報 145 編集 28, 30, 31, 35, 63, 73 自動 86,124 自動(オートパイロット) 26 自動ウイルススキャン 110 自動再生 5 自動制御 124 自動更新を無効にする 14 自動的にワクチン更新を実行 100 自動設定を有効にする(DHCP) 29 自動起動を行う 78 表示期間 140 製品版として登録 5 製品種類の選択 5 複数台用ライセンス 154 複数台用ライセンスを所有している場合 154 言語フィルタ 120 設定 13, 14, 26, 38, 57, 89, 130 設定|アンチウイルス|ウェブ保護 14 設定 | アンチウイルス | メールスキャン 14 設定 | アンチウイルス | リアルタイム保護 14 設定 | アンチウイルス | 更新 14 設定|アンチスパム|スパムフィルタ 14 設定 | その他 31 設定|ファイアウォール|自動 14,26 設定: デバイス コントロール 140 設定: ログ 140 設定: 手動ウイルススキャン 147 設定:ログ 74 設定をインポート 89 設定をエクスポート 89 設定をリセット 89 設定を保存 89 許可 26 許可するコンテンツ 63,67,73 許可する時間 70,72 証明書のインストール 108 詳細 74,139 詳細設定 14, 26, 95, 99, 103, 105, 109, 114 認証に失敗する場合 101 説明 67,77,105 読み取り 88,134 読み取り/書き込み 88,134 起動しない 86 追加 64, 67, 78, 117, 131, 132, 134 送信 24 送信メール 107 送信前のメールスキャン 107

送信者/ドメイン 120 送信者アドレス/ドメイン 117 送信者フィルタ 120 連絡先情報 57 遅延 86 選択 112 選択したパーティション/ファイルのみ復元 48 選択した項目を削除 61 部分バックアップ 42 部分バックアップの作成 42 部分バックアップの実行 42 重要なフォルダを集中的に監視 95 閉じる 147 開く/閉じる 75 開始時刻 139 除外するファイル 44 除外するファイル形式 44 隔離 24.147 隔離されたファイル 24 隔離したファイル 149 隔離ファイル 147 隔離領域 147.149 隔離領域を表示 24 駆除できない場合 147 高システム負荷時にはウイルススキャンを停止 97,114, 147 高セキュリティ 124 高圧縮率 44 高速処理(圧縮なし) 44