ドキュメントの補遺

Zone Alarm セキュリティ ソフトウェア バージョン 7.1

このドキュメントには、ローカライズ版のユーザ ガイドに収録されていない新機能を掲載されています。下のリスト内で希望の項目をクリックすると、詳細が表示されます。

- **ZoneAlarm ID 保護センター**－個人情報盗難の防止と検出、および必要に応じてそれからの回復を手助けします。
- **ゲーム モード**－Zone Alarm セキュリティ ソフトウェア のほとんどのスキャン、製品アップデート、および警告を一時的に抑制することにより、コンピュータでゲームをしているときに邪魔されることが少なくなります。
- **OSFirewall 特殊システム保護**－コンピュータ上のプログラムが特定のアクション（Internet Explorer のホーム ページを変更したり ActiveX コントロールをインストールするなど）を実行できるかどうかを決定します。
- **ウイルス スキャン オプション**－指定したサイズより大きいファイルのバイパス機能、および拡張不正プログラム データベースを提供します。
- **システム メモリ スキャン**－コンピュータの RAM をスキャンします。
- **例外リスト**－Zone Alarm セキュリティ ソフトウェア ウイルススキャンが無視するアイテムのリストの管理機能を提供します。
- **プログラム コントロール レベル**－Zone Alarm セキュリティ ソフトウェアがお使いのコンピュータを学習する間、プログラム警告の数を最少化する自動学習モードを提供します。
- **ネットワーク セキュリティ オプションの設定**－IPv6（Internet Protocol version 6）を使用するインターネット トラフィックのアクセスを許可または拒否する機能を提供します。
- **ドキュメントの訂正とアップデート**

ZoneAlarm ID 保護センター

近年、E コマース、電子記録保持、および大量の金融メール送付の台頭に伴い、個人情報盗難が増加しています。悪意のあるプログラムによって、個人情報がオンラインでハッカーに傍受される可能性があります。また、顧客情報を収めた CD やラップトップが盗まれたり、個人データを含んだ機密メール項目（事前承認されたクレジット カードのオファーなど）が傍受される可能性もあります。-

ZoneAlarm ID 保護センターは、個人情報盗難の防止と検出、および必要に応じて、個人情報盗難からの回復を手助けする Web サイトです。ID 保護センターには、ID 保護のヒントに加えて、個人情報の使用をモニタリングしたり個人情報盗難からの回復を行うためのリソースがあります。

ID 保護センターへのアクセスは、ZoneAlarm Pro および ZoneAlarm Security Suite で行えます。

ID 保護センターにアクセスするには：

1. ［**ID 保護**］｜［**メイン**］に移動します。
2. ［ID 保護センター］エリアで、［**ZoneAlarm ID 保護センターにアクセスする**］をクリックします。

ゲーム モード

ゲーム モードでは、Zone Alarm セキュリティ ソフトウェア のほとんどのスキャン、製品アップデート、および警告を一時的に抑制することにより、コンピュータでゲームをしているときに邪魔されることが少なくなります。ゲーム モードでは、すべてのプログラム許可要求を一時的に許可または拒否できます。すると Zone Alarm セキュリティ ソフトウェア は、警告を表示することなく、そのような要求に自動的に応答します。自動スキャンと製品アップデートは、ゲーム モードを無効にするまで延期されます。ゲーム モードは、ゲーム モードをオフにするまで、または Zone Alarm セキュリティ ソフトウェア やコンピュータをオフにするまでは有効なままとなります。

ゲーム モードは、すべての情報警告と意思決定を求めるすべての警告を抑制します。これには、プログラム一覧内の［問い合わせ］設定によって引き起こされる警告（メールを送信しようとしたりサーバとして機能しようとしているプログラムによって引き起こされる許可警告など）が含まれます。また、OSFirewall 警告（異常と思われる動作や疑わしいと思われる動作を許可するか拒否するかを尋ねる）も含まれます。ゲーム モード設定は、プログラム一覧内の［ブロック］設定や［許可］設定を上書きしません。Zone Alarm セキュリティ ソフトウェア で特定のプログラムを常にブロックするように設定されている場合は、ゲーム モードを［許可］設定下で有効にしても、そのプログラムは引き続きブロックされます。

ゲーム モードを使用すると、システムのセキュリティが低下する可能性があります。すべての許可要求を許可することを選択した場合は、悪意のあるプログラムがコンピュータに危害を加えたり個人データにアクセスする

危険性が高くなります。他方、すべての要求を拒否することを選択した場合は、正当なプログラムの機能が妨害される可能性があります。したがって、ゲーム モードを有効にするのは、ゲーム中に限定する必要があります。

ゲーム モードをオンにするには：

1. システム トレイ アイコンを右クリックし、[**ゲーム モード...**] を選択します。-
2. 表示された [ゲーム モードを有効にする] ダイアログで、次のいずれかをクリックします。

   [**すべての警告に「許可」で応答する**] －許可要求は許可されます。

   [**すべての警告に「拒否」で応答する**] －許可要求は拒否されます。
3. [ゲーム モードを有効にする] ダイアログを開いたままにします。または、閉じずに最小化しておきます。(ウィンドウを閉じると、ゲーム モードがオフになります。)

   ゲーム モードがオンの間、Zone Alarm セキュリティ ソフトウェア はシステム トレイに特殊なアイコン を表示します。

ゲーム モードをオフにするには：

次のいずれかを行います。

- [**キャンセル**] をクリックするか、右上にある [閉じる] アイコン (x) をクリックして、[ゲーム モードを有効にする] ダイアログを閉じます。
- [ゲーム モードを有効にする] ダイアログで、[**ゲーム モードを停止する**] をクリックします。
- システム トレイ アイコンを右クリックし、[**ゲーム モードを停止する**] を選択します。-

コンピュータをオフにしたり Zone Alarm セキュリティ ソフトウェア をオフにすると、ゲーム モードは自動的に無効になります。

OSFirewall 特殊システム保護

デフォルトで有効になる OSFirewall 保護は、プログラムがオペレーティング システムを利用してコンピュータに対して疑わしいアクションを実行しようとするのを検出します。さまざまな OSFirewall 特殊システム保護を設定することにより、コンピュータ上のプログラムが特定のアクション (Internet Explorer のホーム ページを変更したり ActiveX コントロールをインストールするなど) を実行できるかどうかを決定することもできます。

OSFirewall 特殊システム保護は、付録「プログラム動作」に説明されている中レベルの疑わしい動作のいくつかを防止できます。-

OSFirewall 設定を行うには：

1. ［**プログラム コントロール**］｜［**メイン**］を選択します。
2. ［プログラムのコントロール］エリアで、［**カスタム**］をクリックします。
3. 表示された［カスタム プログラム コントロール設定］ダイアログボックスで、[OSFirewall] タブを選択します。
4. 希望に応じて、[OSFirewall を有効にする］を選択または選択解除します。（次のステップで OSFirewall 特殊システム保護を設定するには、最初にこのチェック ボックスを選択する必要があります。）
5. オプションで、OSFirewall 特殊システム保護を設定します。リスト内のアクションの［状態］フィールドをクリックし、［**許可**］、［**拒否**］、［**問い合わせ**］、または［**プログラム設定を使用する**］を選択します。［プログラム設定を使用する］を選択した場合、Zone Labs セキュリティ ソフトウェア は SmartDefense Advisor の設定やユーザの手動設定に委ねます。
6. ［**適用**］をクリックすると、設定が保存され、ダイアログが開いたままとなります。[OK] をクリックすると、設定が保存され、ダイアログが閉じます。

ウイルス スキャン オプション

指定したサイズ以上のファイルを無視するようにウイルス スキャンを設定できます（デフォルト設定は 8 MB です）。ウイルス ファイルのサイズは通常 8 MB 未満なので、このオプションはリスクを高めることなくスキャン時間を向上します。スキャンで無視されたサイズの大きいファイルにウイルスが含まれている場合は、アクセス スキャンが有効であればコンピュータは保護されます。

拡張データベースを有効にすることもできます。このデータベースには、標準ウイルス リストに加えて不正プログラムの包括的なリストが含まれます。ただし、拡張データベースにリストアップされる一部の不正プログラムは標準のアンチスパイウェア データベースにもリストアップされることがあります。このため、疑わしい不正プログラムが 2 回スキャンされることがあります。また、拡張データベースの不正プログラム リストには、ユーザにより良性とみなされるプログラムも含まれる場合があります。

ウイルス スキャン オプションを指定するには、次のようにします。

1. ［**アンチウイルス / アンチスパイウェア**］|［**メイン**］を選択し、［**詳細オプション**］をクリックします。

   ［詳細オプション］ダイアログが表示されます。

2. ［**ウイルス管理**］で、［**スキャン オプション**］を選択します。

3. ［**オブジェクトが次のサイズより大きい場合はスキップ**］チェックボックスをオンまたはオフにしてください。

   オンにした場合、[MB] フィールドにオブジェクトの最大サイズを入力してください。

4. ［**拡張データベースを有効にする**］チェックボックスをオンまたはオフにして、[OK] をクリックします。

システム メモリ スキャン

. システム メモリをスキャンするには、次の手順を実行します。

システム メモリをスキャンするには、次のようにします。

1. ［**アンチウイルス / アンチスパイウェア**］|［**メイン**］を選択します。
2. ［**詳細オプション**］をクリックします。

   ［詳細オプション］ダイアログが表示されます。

3. ［ウイルス管理］で、［**スキャン ターゲット**］を選択します。
4. スキャンするドライブ、フォルダ、およびファイルを選択してください。
5. ［**すべてのローカル ドライブのブート セクタをスキャンする**］チェックボックスをオンまたはオフにしてください。
6. ［**システムメモリのスキャン**］チェックボックスをオンまたはオフにして、[OK] をクリックします。

例外リスト

拡張データベースによって疑わしいとみなされる一部のプログラムはコンピュータに危害を加えたり、データをハッカーに対して脆弱にしたりする可能性がありますが、多くの潜在的に良性のアプリケーションもスキャン時にウイルスとして検出されます。こうしたアプリケーションを使用している場合は、例外リストに追加することにより、スパイウェア スキャンから除外できます。［スキャン結果］リスト内の項目を右クリックし、メニューから［常に 無視］を選択して、プログラムを例外リストに追加できます。

プログラムが例外リストに含まれると、ウイルス スキャン中に検出されません。ウイルスが誤って例外リストに追加された場合は、手動で削除できます。

ウイルスを例外リストから削除するには、次のようにします。

1. ［**アンチウイルス / アンチスパイウェア**］|［**メイン**］を選択し、［**詳細オプション**］をクリックします。
2. ［ウイルス管理］で、［**例外**］を選択します。

3. ［ウイルス処理の例外］エリアで、削除するウイルスを選択し、［**リストから削除する**］をクリックします。
4. ［OK］をクリックします。

プログラム コントロール レベル

Zone Alarm セキュリティ ソフトウェア は、プログラム コントロールの方法を複数提供します。基本的なプログラム コントロールにより、個々のプログラムに対するアクセスおよびサーバ権限を確認できます。アドバンスプログラム コントロールにより、不正プログラムが信頼できるプログラムを悪用するのを防止します。プロセスが別のプロセスを使用しようとしたり、またはプログラムが別のプログラムを開始しようとしたりした場合、アプリケーション対話コントロールがユーザに警告します。OSFirewall 保護は、プログラムがオペレーティング システムを利用してコンピュータに対して疑わしいアクションを実行しようとするのを検出します。

表示する警告数を制限するには、次の機能を使用します。

- Zone Alarm セキュリティ ソフトウェア をアンチウイルスと共に使用する場合は、自動学習プログラム コントロール レベルを使用してください。Zone Alarm セキュリティ ソフトウェア使用開始後の最初の 7 ～ 21 日間は、自動学習が中程度の保護を提供します。Zone Alarm セキュリティ ソフトウェアがユーザのコンピュータを学習すると、プログラム コントロール レベルを最大に再設定します。
- Zone Alarm が推奨するプログラム設定を活用するには、SmartDefense Advisor をプログラム コントロールと共に使用します。

プログラム コントロール レベルを設定するには、次のようにします。

1. ［**プログラム コントロール**］｜［**メイン**］を選択します。
2. ［プログラム コントロール］エリアで、スライダをクリックして希望の設定になるようにドラッグします。

最大（アンチウイルス含むバージョン） 高 （アンチウイルスを含まないバージョン）	この設定では、多数の警告が表示されることがあります。 ◆ プログラムがインターネット アクセスおよびサーバ権限を要求します。 ◆ OSFirewall が疑わしい動作を監視します。 ◆ アドバンス プログラム コントロールおよびアプリケーション対話コントロールが有効になります。 ◆ デフォルトでは、コンポーネント コントロールは無効になります。*

自動 （アンチウイルスを含むバージョン）	このモードは警告数を最小化します。 ◆ 最初の 7 ～ 21 日間は、このコントロール レベルのセキュリティが低下します。 ◆ ネットワークおよび OSFirewall が複数のプログラムをスクリーンします。
中 （アンチウイルスを含まないバージョン）	これは、デフォルトの設定です。 ◆ プログラムがインターネット アクセスおよびサーバ権限を要求します。 ◆ OSFirewall が疑わしい動作を監視します。 ◆ デフォルトでは、コンポーネント コントロールは無効になります。*
最小 （アンチウイルスを含むバージョン）	◆ OSFirewall は無効になります。 ◆ デフォルトでは、コンポーネント コントロールは無効になります。* ◆ サーバ コントロールおよびステルス モードが利用できます。
低 （アンチウイルスを含まないバージョン）	◆ OSFirewall は無効になります。 ◆ デフォルトでは、コンポーネント コントロールは無効になります。* ◆ サーバ コントロールおよびステルス モードは利用できません。
オフ	プログラム コントロールは無効になります。 ◆ プログラムおよびコンポーネントは認証も学習もされません。 ◆ プログラム許可は施行されません。 ◆ すべてのプログラムにアクセス/サーバ権限が与えられます。 ◆ すべてのプログラムが疑わしい動作実行できます。 ◆ プログラム警告は表示されません。

* デフォルトでは、コンポーネント コントロールは無効になります。コンポーネント コントロールをオンにすると、プログラム コントロールが「高」、「中」、または「低」に設定されている限りは、コンポーネント コントロールが有効のままになります。

ネットワーク セキュリティ オプションの設定

自動ネットワーク検出機能を利用すると、ファイルおよびプリンタの共有などの従来のローカル ネットワーク アクティビティを中断せずに、トラスト ゾーンを簡単に設定することができます。Zone Alarm セキュリティ ソフトウェアは、物理的に接続しているネットワークだけを検出します。

ルーテッド ネットワークまたは仮想ネットワークの接続は検出されません。

Zone Alarm セキュリティ ソフトウェアの設定では、警告を表示せずに検出したネットワークすべてをトラスト ゾーンに追加するように、または、新しく検出したネットワークを追加するかどうかをそのたび尋ねる警告を表示するように指定できます。

ネットワークの設定を指定するには、次のようにします。

1. ［ファイアウォール］|［メイン］を選択します。
2. ［詳細設定］をクリックします。
3. ［ネットワーク設定］エリアで、セキュリティ設定を指定します。

新しく検出したネットワークをトラスト ゾーンに含める	新しいネットワークを自動的にトラスト ゾーンに追加します。この設定は最低限のセキュリティを提供します。
新しく検出したネットワークをトラスト ゾーンに含めない	新しいネットワークをトラスト ゾーンに追加せずに、インターネット ゾーンに追加します。この設定は最大のセキュリティを提供します。
新しく検出したネットワークを含めるゾーンを問い合わせる	Zone Alarm セキュリティ ソフトウェアが新しいネットワーク警告またはネットワーク設定ウィザードを表示します。これらを利用して、ゾーンを指定することができます。
新しく検出した保護されていないワイヤレス ネットワーク（WEP または WPA）をインターネット ゾーンに自動的に含める	保護されていないワイヤレス ネットワークをインターネット ゾーンに自動的に追加するので、他者がネットワークにアクセスし、許可を得ずにユーザのデータにアクセスすることを防ぎます。
IPv6 ネットワーキングを有効にする	IPv6 ネットワーク トラフィックがご使用のコンピュータにアクセスするのを許可します。

ドキュメントの訂正とアップデート

以下のセクションには、ローカライズ版のオンライン ヘルプやユーザ ガイドの本文に収録されなかった訂正とアップデートが掲載されています。

- 9 ページの「スパイウェアのスキャン」
- 9 ページの「スキャンからのスパイウェアの除外」
- 9 ページの「スパイウェアおよびウイルス スキャンの結果」
- 9 ページの「コンポーネント コントロール」
- 10 ページの「設定の保存に関する新しい動作」
- 10 ページの「［ファイアウォール］パネル内の名称変更」
- 10 ページの「新しいシステム トレイ アイコン」

スパイウェアのスキャン
以前のバージョンの Zone Alarm セキュリティ ソフトウェア のドキュメントには、ファイルを開くか、ファイルを右クリックしてスキャン オプションを選択することにより、スパイウェア スキャンを開始できると記載されていましたが、これは誤りでした。

スパイウェア スキャンを開始するには、以下の 2 とおりの方法があります。

- ［**アンチウイルス/アンチスパイウェア**］パネルの［メイン］タブにある［アンチスパイウェア］エリアの［**スパイウェアのスキャン**］をクリックできます。
- システム スキャンを 1 回のみ、あるいは一定の間隔で実行するようスケジュールできます。（このオプションの設定の詳細については、関連のオンライン ヘルプを参照してください。）

スキャンからのスパイウェアの除外
以前のバージョンのドキュメントでは、特定のプログラムをスキャンから除外する方法に関して、若干の詳細が抜け落ちていました。以下に訂正されたテキストを示します。

一部のスパイウェア プログラムはコンピュータに危害を加えたり、データをハッカーに対して脆弱にしたりする可能性がありますが、多くの良性のアプリケーションがスキャン時にスパイウェアとして検出されます。こうしたアプリケーション（音声認識ソフトウェアなど）を使用している場合は、例外リストに追加することにより、スパイウェア スキャンから除外できます。［スキャン結果］リスト内の項目を右クリックし、メニューから［常に無視］を選択して、スパイウェアを例外リストに追加できます。

スパイウェアおよびウイルス スキャンの結果
ウイルスおよびスパイウェア スキャンの結果を表示する［スキャン結果］ダイアログ ボックスに、［詳細］エリアが追加されました。スパイウェア スキャンの場合、［詳細］エリアにはすべてのスパイウェア痕跡（レジストリ キーや Cookie など）のフル パスが一覧表示されます。この情報は、Zone Alarm セキュリティ ソフトウェア によって自動的に処理されないスパイウェア プログラムを突き止めようとする上級ユーザに役立ちます。ウイルス スキャン結果の場合、［詳細］エリアは空のままとなります。

コンポーネント コントロール
ドキュメントは、プログラム コントロールとコンポーネント コントロールの間の連係をより正確に記述するように更新されました。以下に更新されたテキストを示します。

プログラム コントロール設定に関わらず、コンポーネント コントロールはデフォルトで無効になります。プログラム コントロール レベルを変更しても、コンポーネント コントロールは自動的にオンになりません。ただし、コンポーネント コントロールをオンにすると、プログラム コントロールが

「高」、「中」、または「低」に設定されている限りは、コンポーネント コントロールが有効なままとなります。

設定の保存に関する新しい動作
バージョン 6.5 では、プログラム警告の［**この設定を保存**］チェックボックスに関して、新しい動作が導入されます。以下に新しい説明を示します。

SmartDefense Advisor が「自動」に設定されている場合、Zone Labs セキュリティ ソフトウェア は自動設定が存在しない場合に限ってプログラム警告を出します。プログラム アクセスを許可または拒否するときにプログラム警告の［**この設定を保存**］を選択した場合、SmartDefense Advisor が別の設定を提示しない限り、またはユーザが［プログラム］タブで手動で設定を変更するまで、Zone Labs セキュリティ ソフトウェア は設定を保持します。［**この設定を保存**］を選択しない場合、プログラムが次回に同じアクションを試みたときに、Zone Labs セキュリティ ソフトウェア は再びプログラム警告を出します。

［ファイアウォール］パネル内の名称変更
［ファイアウォール］パネルの［メイン］タブにある［インターネット ゾーン セキュリティ］および［トラスト ゾーン セキュリティ］設定の 1 つが名称変更されました。「低」設定が「オフ」に名称変更されました。

新しいシステム トレイ アイコン

以下のシステム トレイ アイコンがバージョン 6.5 に追加されました。

アイコン	説明
	Zone Alarm セキュリティ ソフトウェア は、スパイウェア スキャンやウイルス スキャンを実行しています。ウイルス スキャンやスパイウェア スキャンの詳細については、関連のオンライン ヘルプと、このドキュメントの 8 ページの「ドキュメントの訂正とアップデート」に記載されているスパイウェア セクションを参照してください。このアイコンが表示されているときは、それを右クリックして［**スキャンを表示**］-を選択すると、［スキャン ステータス］ダイアログが表示されます。
	ゲーム モードがアクティブになっています。その場合、Zone Alarm セキュリティ ソフトウェア は、アップデート、スキャン、およびほとんどの警告を抑制します。ゲーム モードの詳細については、2 ページの「ゲーム モード」. を参照してください。
	Zone Alarm セキュリティ ソフトウェア は、アップデート（新しいスパイウェア定義やウイルス定義のアップデートなど）を受け取っています。