

- ▶ [FirewallとDefense+について](#)
- ▶ [設定をする場所は？](#)
- ▶ [Firewallの設定](#)
 - ▶ [Firewallとは](#)
 - ▶ [基礎的な事項](#)
 - ▶ [設定は大きく分けて3つある](#)
 - ▶ [Firewall全体の通信の流れ](#)
 - ▶ [発信元アドレスとあて先アドレス](#)
 - ▶ [ルールについて](#)
 - ▶ [全般ルールについて](#)
 - ▶ [セキュリティの強度](#)
 - ▶ [ステルスポート機能](#)
 - ▶ [ステルスポートウィザードを使ってLANとの接続を許可する](#)
 - ▶ [ステルスポートウィザードを使って外部からのアクセス\(Incoming\)を許可する](#)
 - ▶ [攻撃検知設定](#)
 - ▶ [攻撃検出タブ](#)
 - ▶ [その他タブ](#)
- ▶ [Defense+の設定](#)
 - ▶ [Defense+とは](#)
 - ▶ [Defense+のセキュリティ強度](#)
 - ▶ [コンピューターセキュリティポリシー](#)
 - ▶ [アクセス特権](#)
 - ▶ [保護設定](#)
 - ▶ [実行イメージコントロール設定](#)
- ▶ [その他の設定](#)
 - ▶ [Threatcast](#)
 - ▶ [設定管理](#)
 - ▶ [テーマ](#)
- ▶ [tips](#)
- ▶ [アラートの対処](#)
 - ▶ [Firewall アラート](#)
 - ▶ [Defense+ アラート](#)

Firewall と Defense+ について

Comodo Firewallのセキュリティは **Firewall** と **Defense+** から主に成り立っています。
 FirewallとDefense+は互いに独立した機能で、Firewallは外部(インターネット等)との通信を、Defense+は内部(ユーザのPC)で実行されるプログラムを監視しています。
 Firewallの目的は情報流出やハッキングの抑止で、ファイアウォールソフトの基本機能です。
 さらにDefense+ではウイルスやスパイウェアなどのマルウェアによる、ユーザの意図しない振る舞いを抑止することで更なるセキュリティの向上を果たしています。

設定をする場所は？

Firewallのアプリケーションルールと、全般ルールを設定する。

Defense+のルール設定を変更する。

DEFENSE+セクション 詳細設定 コンピューター セキュリティ ポリシー

Defense+のオン・オフ

DEFENSE+セクション 詳細設定 Defense+ 設定 全般設定 Defense+ を完全に停止するチェックボックス
(チェック外すとオン、チェックするとオフ)

アプリ全体的な設定をする所。

その他セクション 設定で。

Firewallの設定

Firewallとは

Comodo Firewallは、**Firewall** と **Defense+** の別々の二つの機能で主に構成されている。

ここでいうFirewallは、補助的なDefense+と違って、本来の、コンピュータ間の通信を監視したり遮断する機能であるFirewallをさす。

Firewallはルール単位で管理されていて、ルールを追加、編集したり削除することで通信の許可、ブロックを制御している。

Firewallが判断しきれない、ユーザの判断が必要なものはアラートとしてポップアップで表示され、アラートで設定された内容のルールがFirewallに追加される。

ルールを設定する場所は [上記項目](#) を参照。

Firewallのアラートについては [Firewall アラート](#) を参照。

アラートの頻度やセキュリティレベル等の設定は [セキュリティの強度](#) を参照。

基礎的な事項

Firewallのルールを理解する上での基本的な事柄。ルールを理解したい人用。

設定は大きく分けて3つある

- ▶ アプリケーション ルール

アプリケーション個々の通信を制御する。

- ▶ 全般ルール

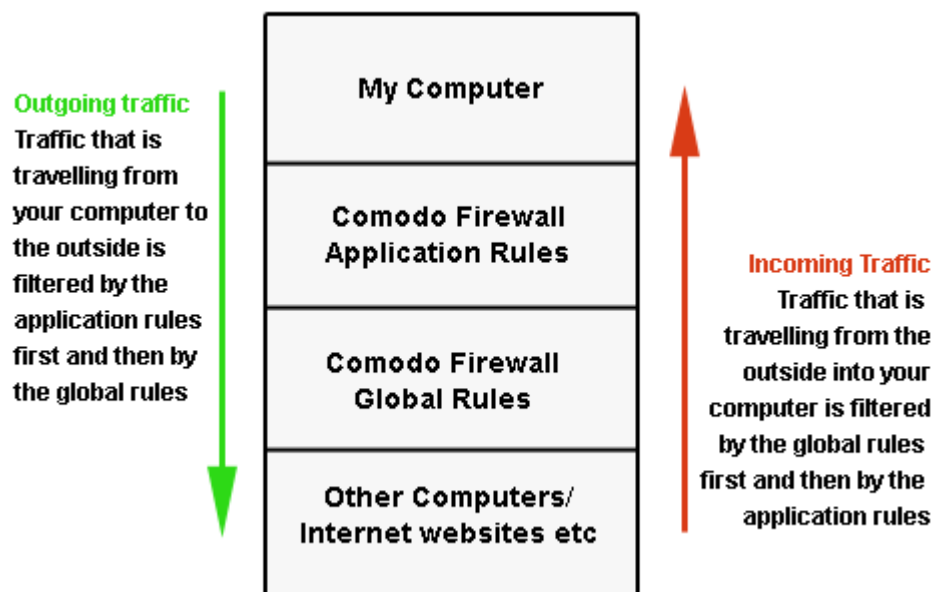
コンピュータと外部との通信を一括制御する。二重チェックの役割を果たす。ルータの簡易ファイアウォールのような振る舞いをする。

- ▶ その他の設定。 [ファイアウォール動作設定](#)、[攻撃検出設定](#) など。

Firewall全体の通信の流れ

下の図のようにOutgoing、Incomingは2回フィルターされる。

例えば、Comodo Firewall Application Rules(アプリケーション ルール)で許可していても、Comodo Firewall Global Rules(全般ルール)で拒否していればブロックされてしまう。



Comodo Firewall Proのヘルプより。

発信元アドレスとあて先アドレス

例えば、

192.168.x.xが発信元、74.125.67.100(google)があて先だったらOutgoing

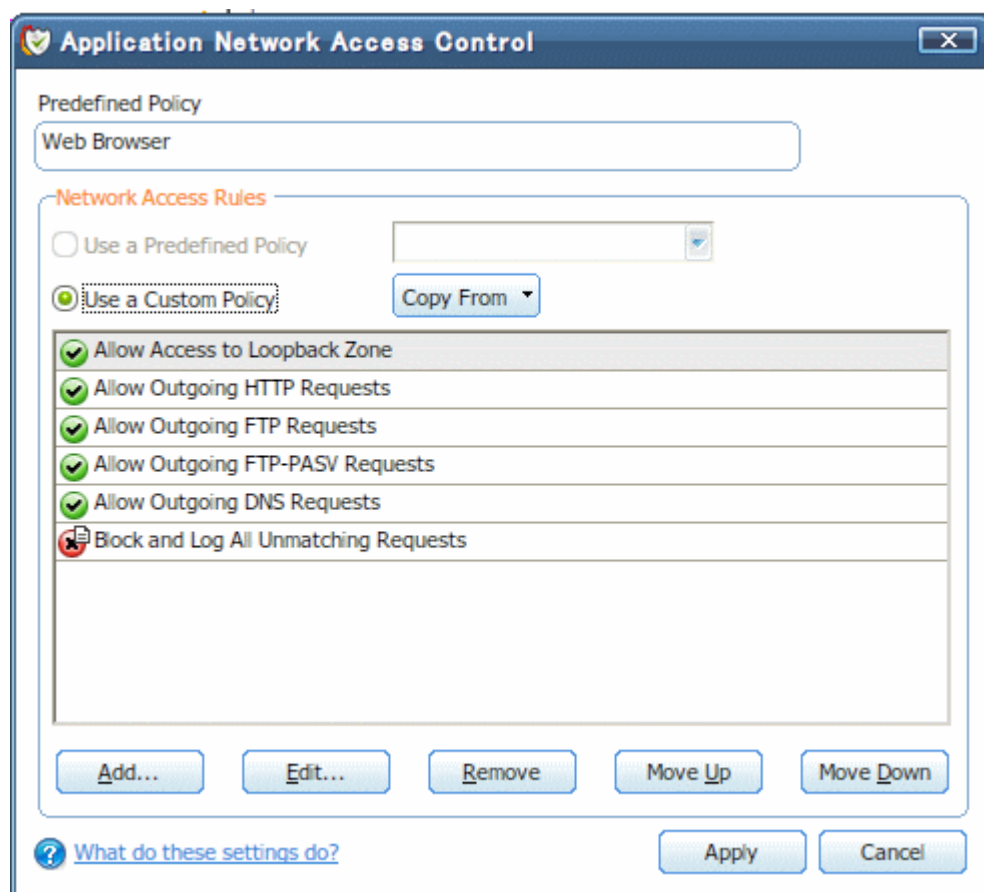
74.125.67.100(google)が発信元、192.168.x.xがあて先だったらIncoming

となる。

ルールについて

複数のルールがリスト状になっている画面では、ルールは上から順に適用されていく。

例：



上のルールの場合、Allow Access to Loopback Zone（ループバックゾーンのアクセスを許可する）が最初に適用され、下へ順々にルールが適用されていく。

最後のBlock and Log All Unmatching Requests（すべての整合しないリクエストをブロックし、ログする）で、適用されてきたルール以外のすべての通信が遮断される。

全般ルールについて

全般ルールではブロックのルールに引っ掛からなければ、明示的に許可のルールを作らなくても通信は許可される。

セキュリティの強度

全体的なセキュリティの強度を決める。インストール時に選択できる大まかな強度を自分で設定しなおすことが出来る。

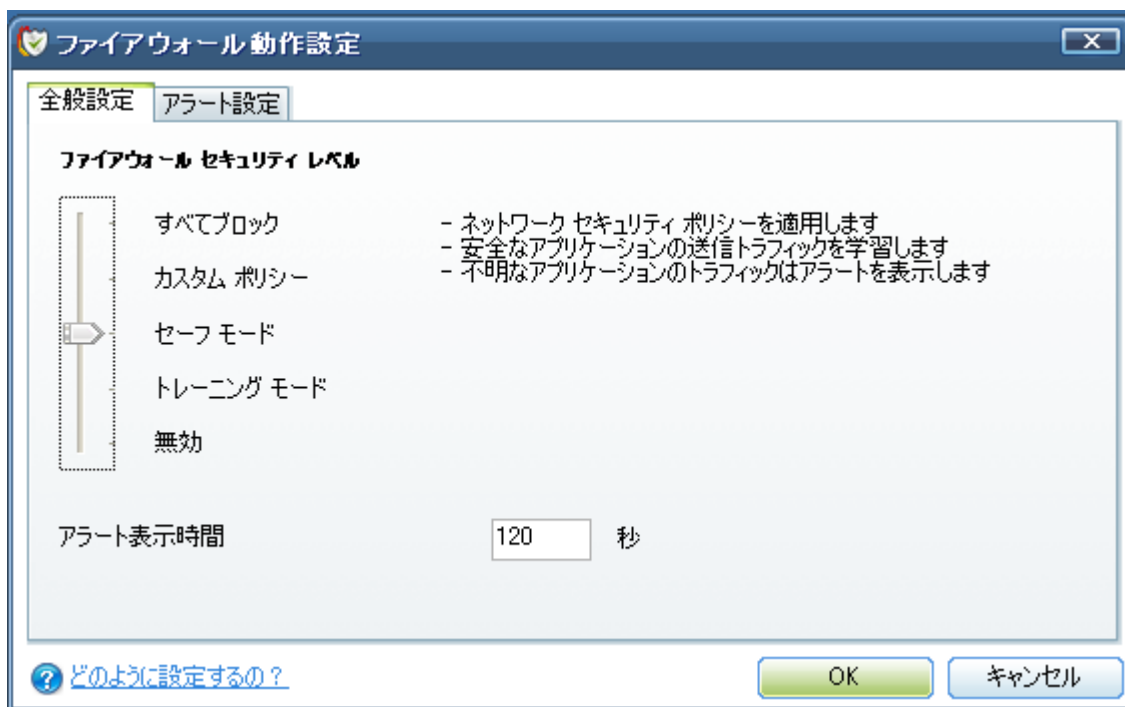
自分の今の設定と見比べて、自分の技量やセキュリティ意識の高さ、利便性などを考えて調整していくのが良いと思う。

しかし、ファイアウォールセキュリティレベルは基本的にはセーフモードで問題ないと思われる。

FIREWALL -> 詳細設定 -> ファイアウォール動作設定 でFirewallの基本設定が出来る。

▶ 全般設定タブ

ファイアウォールセキュリティレベル



すべてブロック

Firewallはユーザが設定したルールや設定に構わず、すべてのinとoutの通信をブロックする。Firewallはアプリケーションの振る舞いを学習しようと試みないし、アプリケーションの通信ルールを自動で作成しない。このオプションを選択するとインターネットを含むどんなネットワークからのアクセスも効果的に防止する。

カスタムポリシー

Firewallは定義されたセキュリティ設定と、ユーザが指定したネットワークセキュリティポリシーのみを適用する。新しいユーザはこれを「学習しない」設定と考えるとよいだろう。なぜならFirewallはどんなアプリケーションの振る舞いも学習しようと試みないからだ。また、それらのアプリケーションのネットワーク通信ルールも自動で作成されない。アプリケーションが接続を試みると常にアラートが出るだろう。それは例えComodoのセーフリストに載ったアプリケーションだとしてもだ。もちろんアプリケーションの通信の試みを信用したと、Firewallに指示して出来たルールとポリシーを以前に指定していないかぎりは、

もしアプリケーションが外部と接続を試みようとしたら、Firewallはすべてのロードされたコンポーネントを監査し、すでに許可あるいはブロックされたコンポーネントのリストに対してそれぞれをチェックする。もしブロックされるべきコンポーネントが見つかったら、全アプリケーションがインターネットアクセスを拒否され、アラートが出る。この設定は最大限の、鮮明度とinとoutの通信のコントロールを望む熟練のFirewallユーザに勧められる。

セーフモード

Firewallが安全と判断したアプリケーションの通信を自動で許可、学習する。未知のアプリケーションの通信はアラートで知らせ、許可/不許可をユーザにせまる。ほぼすべてのユーザに推薦される。体感ではこの設定をする前にコンピュータに存在したプログラムを起動したとき自動学習されて、セーフモード設定後インストールされたプログラムは、ポップアップが出るようだ。信頼するソフトウェアベンダのソフトは自動学習される。

トレーニングモード

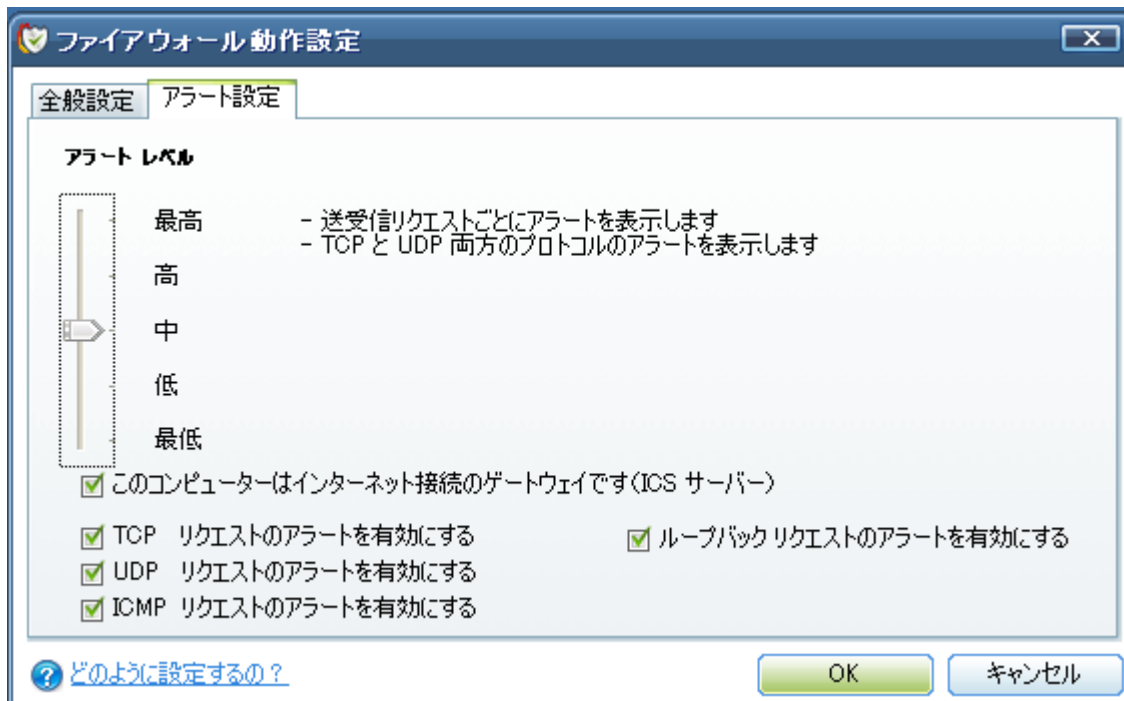
すべてのアプリケーションの通信を学習する。常用は推薦されない。

無効

Firewallを停止する。

▶ アラート設定タブ

アラートレベル



最高

高に加え、IPアドレスごとに許可/拒否する。JeticoやKerioと同じアラートを求めるなら、これを選択すると良いだろう。

高

中に加え、ポートを **個別に** 許可/拒否する。ポートを個別設定したい人はこれ。

中

低に加え、TCPとUDPを **別に** 許可/拒否する。まあまあ。

低

最低に加え、incoming/outgoingを **別に** 許可/拒否する。TCPとUDPを **一緒に** 許可/拒否する。Windows Firewallよりちょい上なレベル。

最低

アプリごとに通信を許可/拒否するだけ。Windows Firewall以下なレベル。

このコンピュータはインターネット接続のゲートウェイです(ICS サーバー)

ICS(Internet Connection Sharing:インターネット接続共有) サーバーとは、自身のインターネットコネクションをLANで接続された別のコンピュータと共有しているコンピュータのことです。言い換えれば、その別のコンピュータはICSサーバーを介してインターネットに接続します。

複数のコンピューターが有るにもかかわらずインターネット接続が1つしか張れない環境の会社や家庭においては、ICS サーバを立てると便利です。例えば、家に2台のコンピューターが有るのに接続権が1つしかない場合に、1台をICSサーバに設定すると2台共インターネットにアクセスできます。

- ▶ コネクションを共有するためにLANを通じて接続している他のコンピューターが存在しない場合は、このチェックボックスはチェックせずにおいてください。大多数のユーザーはこちらに該当するでしょう。
- ▶ コンピューターがICSサーバとして設定されていて他のコンピューターがこのコンピューターを介してインターネットに接続している場合は、このチェックボックスをチェックしてください。

注：コンピューターが実際にICSサーバーとして機能しているにもかかわらず、このチェックボックスをチェックしていない場合、ファイアウォールが出すアラートが増大することが想定されます。このチェックボックスをチェックしてもセキュリティが低下する様なことはありませんが、ファイアウォールがICS リクエストにも対処するようになります。つまり、いくつかの追加機能が有効になってアラートの数を減らす手助けをするだけです。

Q：2台のコンピュータを所有していて両方ともインターネットに接続している場合、このチェックボックスをチェックしておく必要がありますか？

A：大抵の場合、チェックする必要はありません。2台のコンピュータを所有してそれぞれがルーターや無線を介してネットに接続している場合は、ここで述べているコネクション「共有」とは意味が異なります。真にコンピューターをICSサーバーとして使用する場合にこのチェックボックスをチェックしてください。

ステルスポート機能

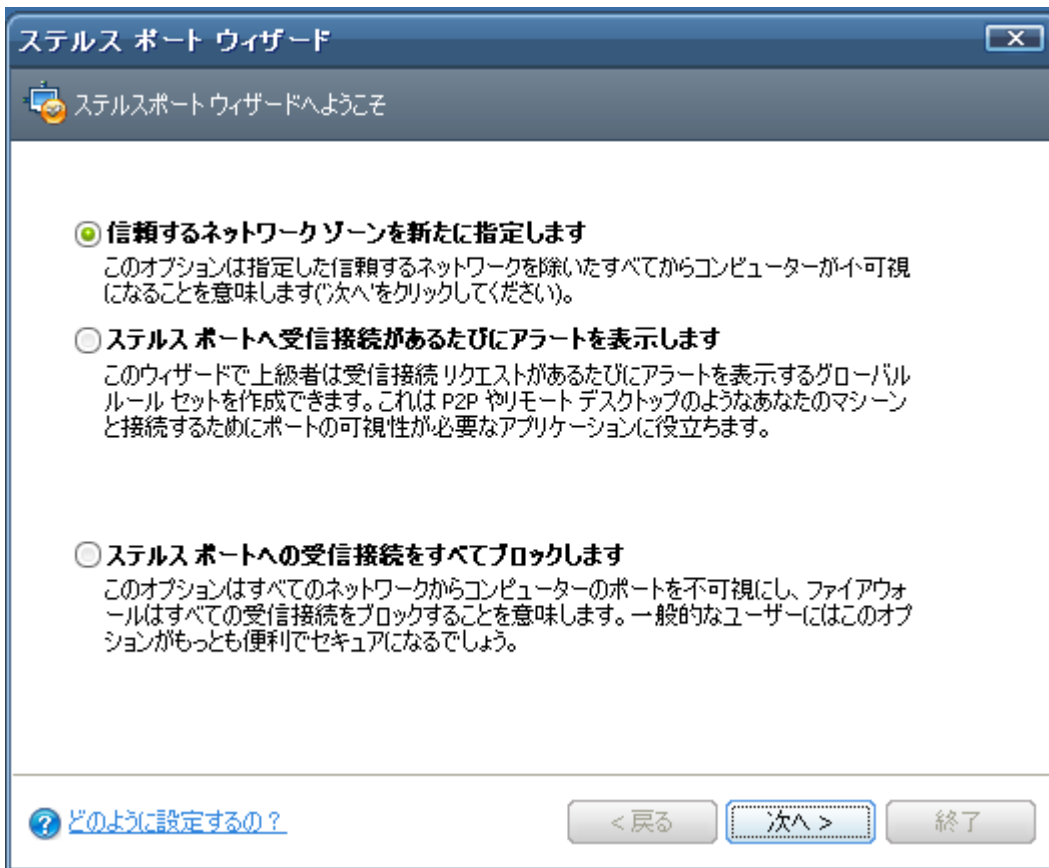
ステルスポート機能は、ポートスキャンに対して応答を返さないことによりインターネットに接続しているPCのポートを(外部から)隠蔽するセキュリティ機能です。

ステルスポート機能はポートスキャンから'不可視'にします。'不可視'は、ポートが'閉じている'のとは異なります。ポートが'閉じている'状態では、'閉じている'という応答を返してしまいIPCが実際に存在していることが侵入者にばれてしまいます。一方、'不可視'の場合は応答を一切返しません。

Comodo Firewallは順応性のあるステルスポート機能の選択肢を提供します。

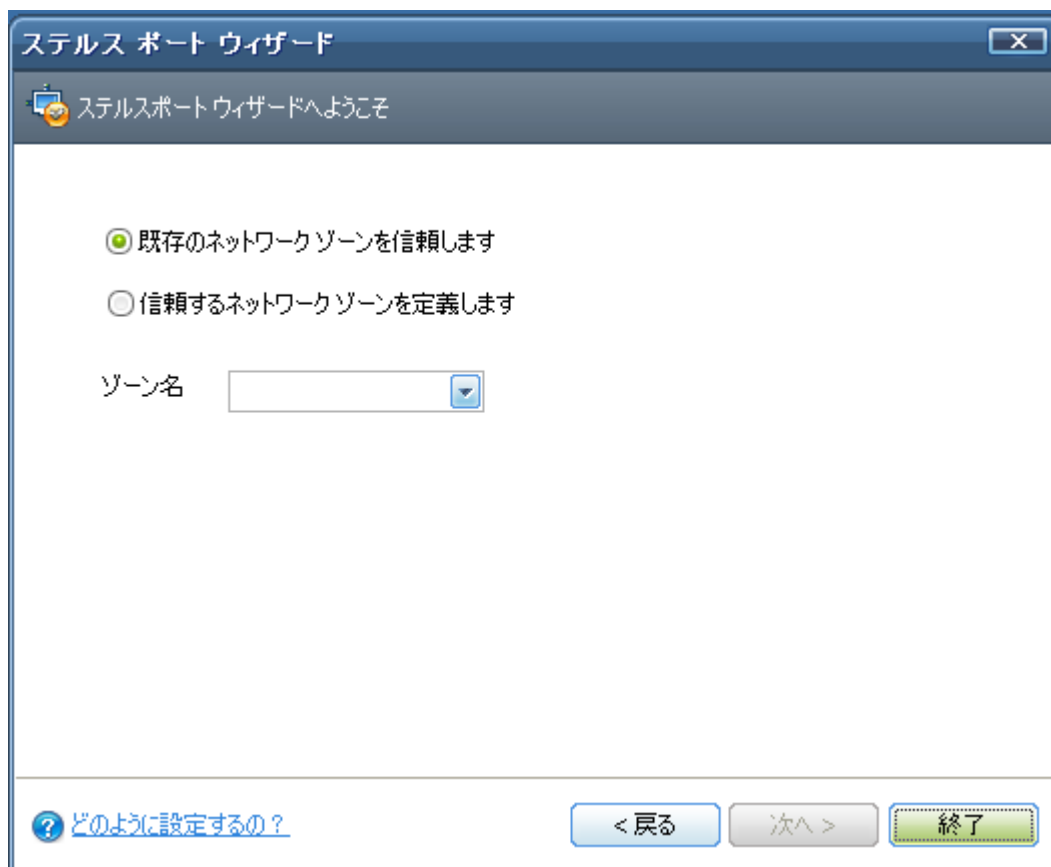
ステルスポートウィザードは具体的にはFirewallの全般ルールとアプリケーションルールのSYSTEMにルールを追加します。

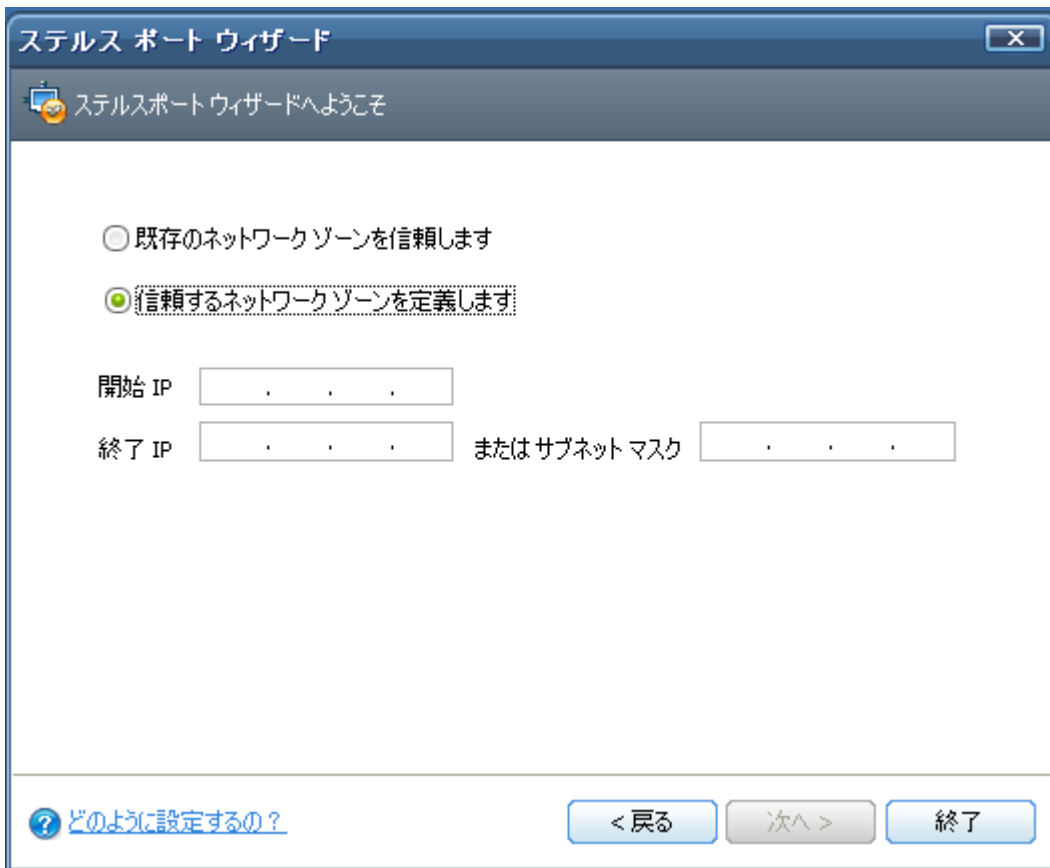
1. FIREWALL -> 共通タスク -> ステルスポートウィザード
- 2.



信頼するネットワークゾーンを新たに指定します

この選択肢では、信頼すると指定されたネットワーク以外からPCのポートを不可視にします。信頼するネットワークを指定します。





以下のルールが'全般ルール'に追加されます。

許可	IP	Out	From Any IP Address	To <ZONE>	Where Protocol is ANY
許可	IP	In	From <ZONE>	To Any IP Address	Where Protocol is ANY

ステルスポートへ受信接続があるたびにアラートを表示します

この選択肢では、外部からのリクエストを受信する度にアラートを出すようにします。アラートにより、当該リクエストの続行を許可するかどうかを尋ねられます。この選択肢はP2PやRemote Desktop等の外部から接続される必要のあるアプリケーションに有用です。

以下のルールが'全般ルール'に追加されます。(P2P、サーバ等でincoming通信を制御したい場合これを選択)

Block	ICMP	In	From Any IP Address	To Any IP Address	Where Message is ECHO REQUEST
-------	------	----	---------------------	-------------------	-------------------------------

ステルスポートへの受信接続をすべてブロックします

この選択肢では、信頼すると指定されているかどうかにかかわらず、すべてのネットワークからPCのポートを不可視にします。普通に家庭で使用する場合はこの選択肢が便利で安全です。リクエストをブロックしたときアラートは出ませんがイベントログに記録されるようになります。

以下のルールが'全般ルール'に追加されます。

Block And Log	IP	In	From Any IP Address	To Any IP Address	Where Protocol is Any
---------------	----	----	---------------------	-------------------	-----------------------

以下は具体的な操作例。

ステルスポートウィザードを使ってLANとの接続を許可する

- ▶ FIREWALL -> 共通タスク -> ステルスポートウィザード

「信頼するネットワークゾーンを新たに指定します」にチェックを入れ次へ進む。

- ▶ 「信用するネットワークゾーンを定義します」を選択する。
- ▶ 許可したいネットワークの範囲を指定する。

例：

LANが192.168.11.***（11は環境によって変わる）なら
開始 IP：192.168.11.1
サブネット マスク：255.255.255.0
とする。

- ▶ ウィザードに従って終了する

ステルスポートウィザードを使って外部からのアクセス（Incoming）を許可する

ファイル共有ソフトやサーバー機能のあるアプリケーションを使用する場合、この操作が必要になる場合がある。

- ▶ FIREWALL -> 共通タスク -> ステルスポートウィザード
- ▶ 「ステルスポートへ受信接続があるたびにアラートを表示します」にチェックを入れ次へ進む。
- ▶ ウィザードに従って終了する

攻撃検知設定

Comodo Firewall には、高度な攻撃検知を設定ができる機能があります。ユーザーのコンピューターを、一般的なタイプのサービス妨害 (DoS) 攻撃から保護するのに役に立ちます。サービス妨害攻撃または 'フラッド' 攻撃を始めるとき、攻撃者はターゲットのマシンに大量のコネクション要求を一斉に発行します。そうすると、コンピューターは正当なコネクションを受け入れることができなくなります。そうやって、ウェブサーバー、または、メールサーバー、FTPサーバー、VPNサーバーを事実上ダウンさせます。

攻撃検出 タブ

攻撃検出設定

攻撃検出 その他

TCP フラッド

トラフィック レート パケット / 秒

継続時間 秒

UDP フラッド

トラフィック レート パケット / 秒

継続時間 秒

ICMP フラッド

トラフィック レート パケット / 秒

継続時間 秒

疑わしいホストからポートスキャンを試行された後、どのくらいの間
自動でブロックしますか？ 分

DOS 攻撃を受けている間、ファイアウォールはどのくらいの間
緊急事態モードにすべきですか？ 秒

ARP キャッシュを保護する

不当な ARP フレームをブロックする

[? どのように設定するの？](#)

TCP フラッド / UDP フラッド / ICMP フラッド

フラッド攻撃は、何千ものパケットデータがスプーフィングされた送信元 IP アドレスを使って被害者のマシンに送信されることで起こります。被害者のマシンは、自動的にこれらのリクエストへの応答 (SYN パケット) を返して、肯定応答 (ACK パケット) を待ちます。しかしスプーフィングされた IP アドレスが使われているので、被害者のマシンが何らかの応答や肯定応答パケットを受け取ることはありません。この結果、応答の無い要求が滞って、被害者のマシンのコネクションテーブルが満杯になってしまいます。コネクションテーブルが満杯になると、被害者のマシンは新たなコネクションの受け入れを拒否します。それは、コンピューターを使ってのインターネット接続や電子メール送信、FTP の使用などができなくなることを意味します。これが複数の発信元から何度も実行されると、被害者のマシンは大量のリクエストを送りつけられて、クラッシュしてしまう可能性があります。

デフォルトでは、Comodo Firewall は TCP ・ UDP ・ ICMP のアクセスを受け入れるのに、一定の時間連続して 1 秒あたりのパケット数の最大値を超えるかどうかで設定されます。上記の 3 プロトコルに対するデフォルト値は、20 秒間連続して 20 パケット / 秒 に設定されています。ファイアウォールの 1 秒あたりのパケット数および最大連続時間は、ユーザーが適当なフィールドを変更することで再設定できます。もし最大値を超えたときは、Dos 攻撃として Firewall は緊急事態モードになります。

ファイアウォールは、ユーザーが設定した時間、緊急事態モードの状態を継続します。デフォルトでは、これは 120 秒間に設定されています。ユーザーは「How long should the firewall stay in emergency mode while the host is under DOS attack?」を設定して、この時間を変更することができます。緊急事態モードにおいては、これまでに確立されて今も使用中のコネクションを除いて、入ってくるデータは全てブロックされます。一方、出て行くデータはすべて許可されたままです。

疑わしいホストからポートスキャンを施行された後、どのくらいの間自動でブロックしますか？

コンピューター・クラッカーがよくやる手段ですが、ポートスキャンをすることで脆弱性を探り出すことができます。基本的に、ポートスキャンとは 1 つ 1 つのポートに対してメッセージを送信することです。受け取った応答の種類によって、当該ポートが使用されていて、かつ、脆弱性があることが分かります。

Comodo Firewall は最も一般的なポートスキャンの形態を検知します。そして、ユーザーにアラートを出して、一時的に犯人の IP アドレスからのアクセスを禁止します。こうすることで、ユーザのシステムに関する有益な情報を手にする前に犯人を遮断して安全を確保します。

ユーザーは、ポートスキャンを実行している疑いのあるホストからのアクセスをブロックする期間を設定することができます。ポートスキャンを検知すると、ファイアウォールは犯人を特定して自動的に一定期間アクセスをブロックします。デフォルトでは 5 分です。この時間中、当該ホストからのアクセスは一切受け入れられません。この 5 分間、犯人からはユーザーのシステムにアクセスできませんが、ユーザー側からは犯人のシステムにアクセスすることができます。

DOS 攻撃を受けている間、ファイアウォールはどのくらいの間緊急事態モードにすべきですか？

DoS が検知されると、ファイアウォールは一定期間緊急事態モードになります。デフォルトでは 120 秒間です。ユーザーは期間を設定することができます。

ARP キャッシュを保護する

このオプションにチェックを入れると、Comodo Firewall は、ARP (アドレス解決プロトコル: Address Resolution Protocol) コネクションの処理状態検査を開始します。こうすることで、偽装された ARP リクエストはブロックされて、ユーザのコンピューターは ARP キャッシュポイズニングから保護されます。

ARP キャッシュ (ARP テーブル) は、コンピューターに保管されている IP アドレスの履歴です。それは、IP アドレスを MAC アドレスに対応づけるために使用されます。処理状態検査は、プロトコルスタック下層のデータを分析します。そして、現行のセッションを以前のものと比較して、怪しい行動を検知します。

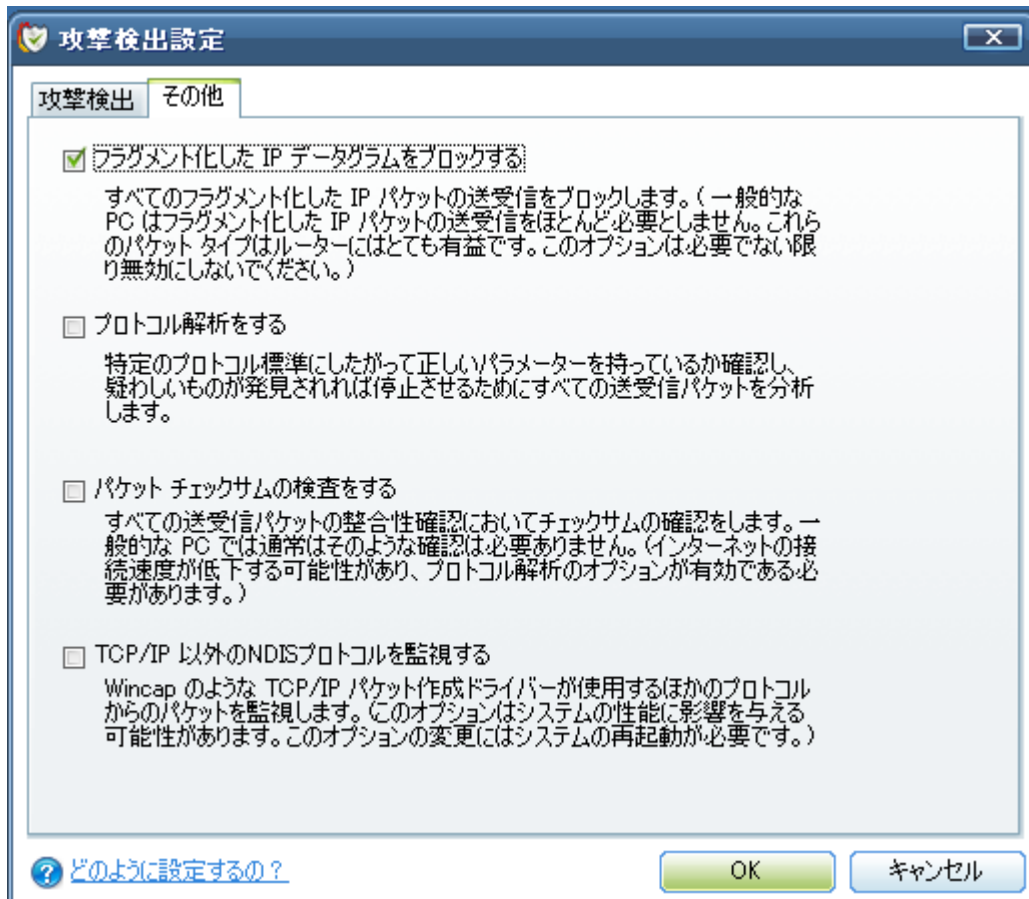
背景 - ネットワーク装置はそれぞれ 2 つのアドレスを持っています。すなわち、MAC (Media Access Control) アドレスと IP (Internet Protocol) アドレスです。MAC アドレスは、装置内の物理的なネットワーク・インターフェース・カードのアドレスであり、変更することはできません (つまり、PC 内のネットワーク・カードは決め打ちされた MAC アドレスを持っていて、別のマシンに付け替えても同じ MAC アドレスのままです)。その一方で、IP アドレスは変更されることがあります。例えば、マシンが別のネットワークに移設したとき、または、ネットワークが DHCP を使用して IP アドレスを動的に割り当てている場合です。ホストから宛先ネットワーク・カードまで正確にパケットをルーティングするために、IP アドレスと MAC アドレスの相関関係の情報を保持することは不可欠です。アドレス解決プロトコルは、IP アドレスをしかるべき MAC アドレスに適合させる (またはその逆) ことで機能を実現します。ARP キャッシュは、当該コンピューターが今までに適合させてきた IP アドレスと MAC アドレスの履歴です。

DoS 攻撃や中間者攻撃、MAC アドレス・フラッド、ARP リクエスト偽装など何らかの方法で、ハッカーがコンピューターの ARP キャッシュを変更し得る可能性があります。注意してほしいのは、ARP 攻撃が成功するには、大抵ハッカーが当該ネットワークへ物理的に接続できるか当該ネットワーク上のマシンを直接操作する必要があります。それ故にこの設定項目はホームユーザーよりむしろネットワーク管理者にとって意義があります。

不当な ARP フレームをブロックする

gratuitous ARP frame は全てのマシンにブロードキャストされているにもかかわらず、いずれかの ARP 要求の応答ではない ARP 応答です。ARP 応答がブロードキャストされると、全てのホストはローカルに保持している ARP キャッシュを更新することが求められます。ARP 応答が、それまでに発行された ARP 要求に対する応答であるかどうかにかかわらずです。ネットワーク上の別のマシンに変更があった場合すぐにユーザーマシンの ARP キャッシュを更新するために Gratuitous ARP frames は重要です (例えば、ネットワーク上のマシンのネットワーク・カードが付け替えられた場合、gratuitous ARP frame によってこの変更を知ることができユーザーマシンの ARP キャッシュが更新されることでデータが正しくルーティングされます)。この設定を有効にすると、これらのリクエストをブロックします。そして、ARP キャッシュが悪意によって更新されることを保護します。

その他 タブ



フラグメント化した IP データグラムをブロックする

2つのコンピュータ間でコネクションが確立された場合、MTU(Mass Transmission Unit)について合意する必要があります。ユーザーが使用しているよりも小さい MTU のルーターをデータが通過した場合、IPフラグメンテーション (IP Datagram fragmentation) が起こります。すなわち、送信経路のネットワークの MTU よりもデータグラムが大きい場合、データグラムは「フラグメント」に分割されてそれぞれ別々に送信されます。フラグメント化された IP パケットは、DOS 攻撃に似た脅威を作り出します。さらに、フラグメント化は 1 パケット送信に掛かる時間を倍増させます。その結果、ダウンロードに掛かる時間を遅らせます。

Comodo Firewall はデフォルトでフラグメント化された IP データグラムをブロックするように設定されています。すなわち、Block Fragmented IP datagrams はデフォルトでチェックが入れられています。

プロトコル解析をする

プロトコル分析はサービス妨害攻撃に使用される偽装パケットを検知するための手掛かりです。このオプションにチェックを入れると、Comodo Firewall は各パケットがプロトコル標準に従っているか検査します。従っていない場合、当該パケットはブロックされます。

パケット チェックサムの検査をする

パケットデータはそれぞれシグニチャーを持っています。このオプションにチェックを入れると、Comodo Firewall は入ってくるパケットのチェックサムを再計算して、シグニチャーで提示されているチェックサムと比較します。それらが一致しない場合は、送信後にパケットが改ざんされたということで、Comodo Firewall は当該パケットをブロックします。この機能を使用することでセキュリティ上の恩恵がありますが、同時に全てのパケットのチェックサム検証を実行すると、リソースを消費してインターネット接続速度は大きく低下します。この機能は上級ユーザー向けです。Comodo としては、大抵のホームユーザにはこの機能を無効にすることをお勧めします。

TCP/IP 以外の NDIS プロトコルを監視する

このオプションにチェックを入れると、Comodo Firewall は TCP/IP 以外のプロトコルドライバに属するパケットをキャプチャーします。トロイの木馬は、パケットのやり取りに独自のプロトコルドライバを使用する場合があります。このオプションは、そのような攻撃を捕捉するのに有用です。このオプションはデフォルトでは無効になっています。なぜなら、システムのパフォーマンスが低下しますし、一部のプロトコルドライバと相性が悪い可能性があ

るからです。

Defense+の設定

Defense+とは

Firewallは外部との通信を見張っていますが、Defense+はコンピュータの動作を見張るものです。ファイルやレジストリの書き換え、プロセス間通信等を監視します。

CISにFirewallだけの機能を期待してる人、特にアンチウイルスソフトと併用してる人はDefense+の必要性をあまり感じないかもしれません。

しかしDefense+は、アンチウイルスソフトが検出できないような、企業が製作した行儀の悪いソフトや、未知のウイルスやマルウェア等の振る舞いを抑制、遮断することに対しては有効だと言えます。

セキュリティレベルを変更するには [Defense+のセキュリティ強度](#) を参照、ポップアップアラートが出る頻度を調節できます。

Defense+のルールの設定、編集は [コンピューター セキュリティ ポリシー](#) で行えます。

exeファイル等の実行時のポップアップアラートの出方は [実行イメージ コントロール設定](#) で調節できます。実行イメージ コントロールは、Defense+ のセキュリティ強度が「セーフ モード」または「クリーン PC モード」に設定されている場合のみ有効です。

保護されてるファイル

ここに載ってる項目が書き換えられようとしてるとDefense+が警告を出す。マルウェア(ウイルス/スパイウェアなど)が勝手にファイルを書き換えようとする時など。

My Quarantined Files (隔離されてるファイル)

保留中のファイル

新しく作られたり変更されたりした、.exeや.dllファイルが登録される。気付かない内に、ここに大量のファイルが登録されている場合があるので、時々チェックするのがよい。

信用できるソフトベンダーのリスト

.exeの右クリック プロパティ デジタル署名で信用出来るベンダー製かどうかを判断

保護されてるレジストリキー

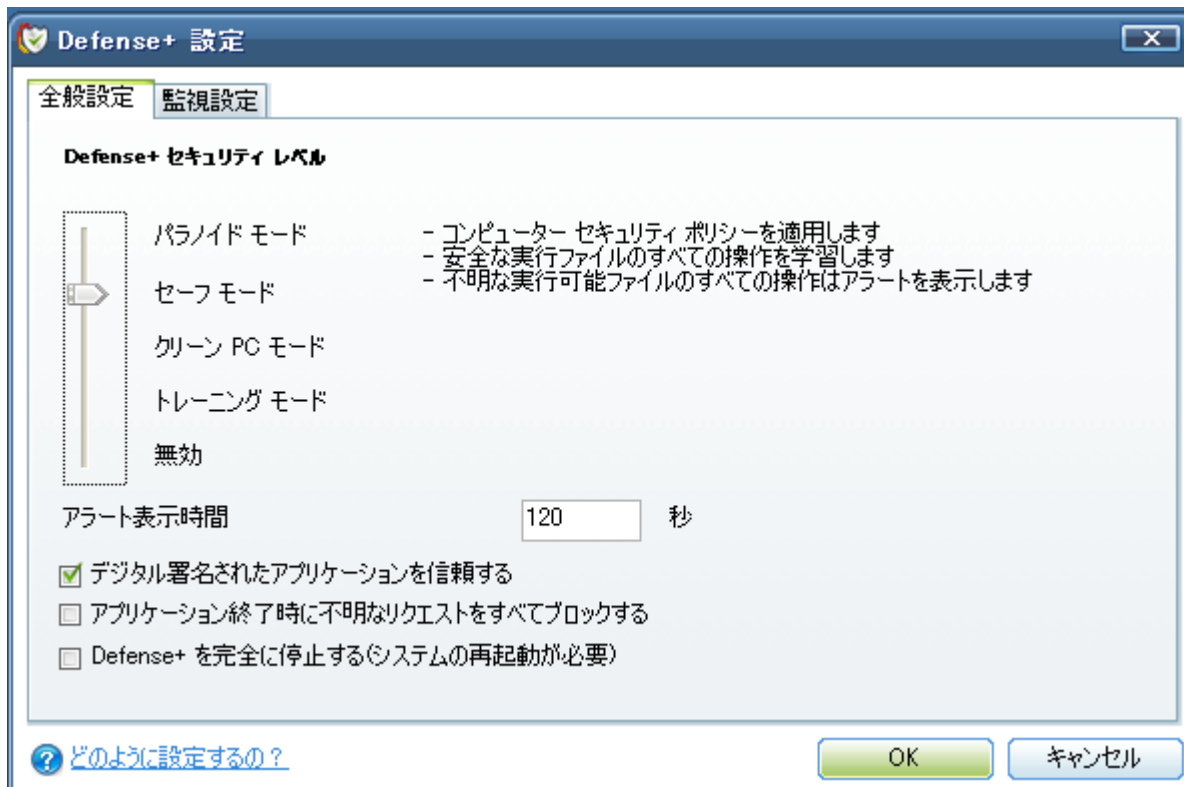
ここに載ってるレジストリ項目が書き換えられようとしてるとDefense+がアラートを出す。マルウェア(ウイルス/スパイウェアなど)が勝手にレジストリを書き換えようとする時など。

保護されてるComponent Object Model(COM)

プロセス間通信を利用して情報を横取りしたり、ハッキングを掛けるソフトを監視する。しかし健全なマウスジェスチャーソフト (プロセス間通信を利用してマウスフックを掛ける)

Defense+のセキュリティ強度

▶ DEFENSE+ -> 詳細設定 -> Defense+ 設定



パラノイドモード

これは最も高いセキュリティレベルの設定です。Defense+は、あなたが安全であると判断したファイルを除き、すべての実行ファイルを監視・制御します。Defense+はあらゆるアプリケーションの動作を学習しません(Comodoの安全リストにあるアプリケーションも同様です)。システムの危険な活動をフィルタリングする際、ユーザの環境設定だけを唯一使用します。同様に、Defense+は、あらゆるアプリケーションに対し、勝手に"許可(Allow)"ルールを作成しません。とはいえ、Defense+がアラートを出した際、当該アプリケーションを"信頼(Trusted)"として取り扱う選択肢を選ぶことができます。パラノイドモードはDefense+がアラートをもっと多く出す選択肢であり、システムの活動を完全に認識したいと願う上級ユーザに推奨します。

セーフモード

システムの危険な活動を監視すると同時に、Comodoの安全リストにあるアプリケーションの活動を学習します。そして、それらのアプリケーションの活動に対して、"許可(Allow)"ルールを作成します。それ以外のアプリケーションを実行しようとした際、アラートを出します。アラートが出た際、"Treat this application as a Trusted Application"を選択することで当該アプリケーションを安全リストに追加することができます。それにより、当該アプリケーションが次に実行された際、Defense+がアラートを出さなくなります。"クリーン PC モード"の様にあなたのPCが新品であるかマルウェア等の脅威がないとわかっているわけではない場合は、大部分のユーザに"セーフモード"を推奨します。高いセキュリティレベルと手頃なアラート頻度を兼ね備えています。

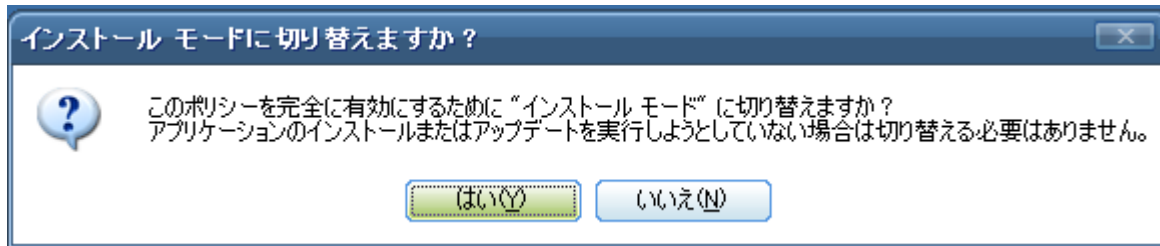
クリーン PC モード

Defense+はすべて新しい実行ファイルを監視・制御すると同時に、現在PCにインストールされているアプリケーションの活動を学習します。この特許出願中の選択肢は、PCが新品であるかマルウェア等の脅威がないとわかっている場合に推奨されます。以降、新しく未承認のアプリケーションをインストールするとDefense+がアラートを出します。このモードでは、「保留中のファイル」に入っているファイルは、安全とはみなされず監視・制御の対象になります。

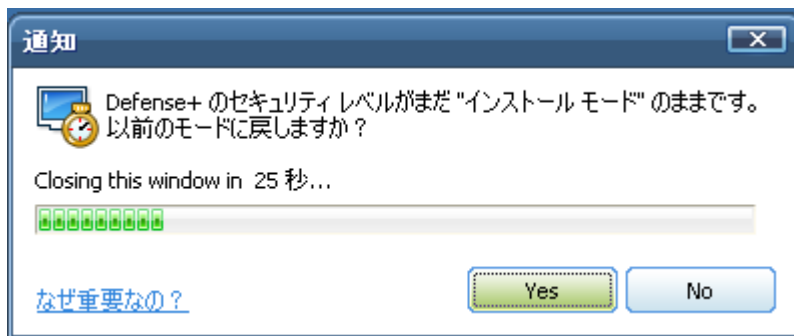
インストールモード

インストーラや更新プログラムは実行時に他のプロセスを立ち上げることがあります。いわゆる"子プロセス"です。「パラノイド」「セーフ」「クリーン PC」のそれぞれのモードにおいては、それらの子プロセスが実行しようとするたびにDefense+はアラートを出すでしょう。なぜなら、それらの子プロセスはアクセス権をDefense+から与えられていないからです。そこで「パラノイド」「セーフ」「クリーン PC」のそれぞれのモードにおいては、COMODOは一時的にインストールモードに変更するように提案することで信頼できるアプリケーションのインストールを容易にすることができます。インストールモードでは、子プロセスは親プロセスと同じアクセス権を与えられます。そうすることでアラートが頻発することなくインストールを行うことができます。

新しい未知のアプリケーションをインストールしようとする時、Defense+はポップアップのアラートを出します。このアプリケーションのインストールを継続したいときは、ポップアップアラート上の" Treat this application as an Installer or Updater"を選択してください。すると次のようなポップアップが出ます。



「Yes」を選択するとインストールモードに変更され、子プロセスは親プロセスと同じアクセス権を与えられます。インストールモードに変更すると元のモードに戻すことを忘れないように次のような注意喚起がなされます。



トレーニングモード

Defense+はすべての実行ファイルの活動を監視し学習します。そして当該実行ファイルの活動に対して、勝手に"許可(Allow)"ルールを作成します。Defense+はアラートを出しません。トレーニングモードを選択する場合は、PCにインストールされている実行ファイルとアプリケーションが実行しても安全であることを100%確信しているようにしてください。

無効

Defense+の保護を無効化します。すべての実行ファイルとアプリケーションが実行許可されます。他の不正侵入防止システムをインストールしていて確信があるとき以外はこのモードを選択しないように強く勧告します。

アラート表示時間

ユーザの操作がない場合に、どれだけの時間アラートを表示しておくかを決定します。デフォルトは120秒です。

デジタル署名されたアプリケーションを信頼する

これをチェックしておく、信頼できる認証局を使って署名されたアプリケーションは自動的に安全リストに追加されます。Comodoはこのオプションを有効にしておくことを推奨しています。

アプリケーション終了時に不明なリクエストをすべてブロックする

これをチェックしておく、Comodo Firewallが起動していないか、シャットダウンされている場合に、未知の(コンピューターセキュリティポリシーに定義されていない)要求を全てブロックします。

Defense+ を完全に停止する(OSの再起動が必要)

Basicで入れた後でDefense+の全機能を使いたいなら

DEFENSE+ 詳細設定 Defense+ 設定 全般設定 の
Defense+ を完全に停止する のチェックを外す必要がある

でも、普通はDefense+使ってもウザイだけだろうから、Basicで入れた後にスライダーでセキュリティレベルを上げる程度で良いと思う

コンピューターセキュリティポリシー

コンピューターセキュリティポリシーではアプリケーションに適用されたDefense+のポリシーの管理や編集ができる。

設定はDEFENSE+ 詳細設定 コンピューターセキュリティポリシー から行える。

アクセス特権

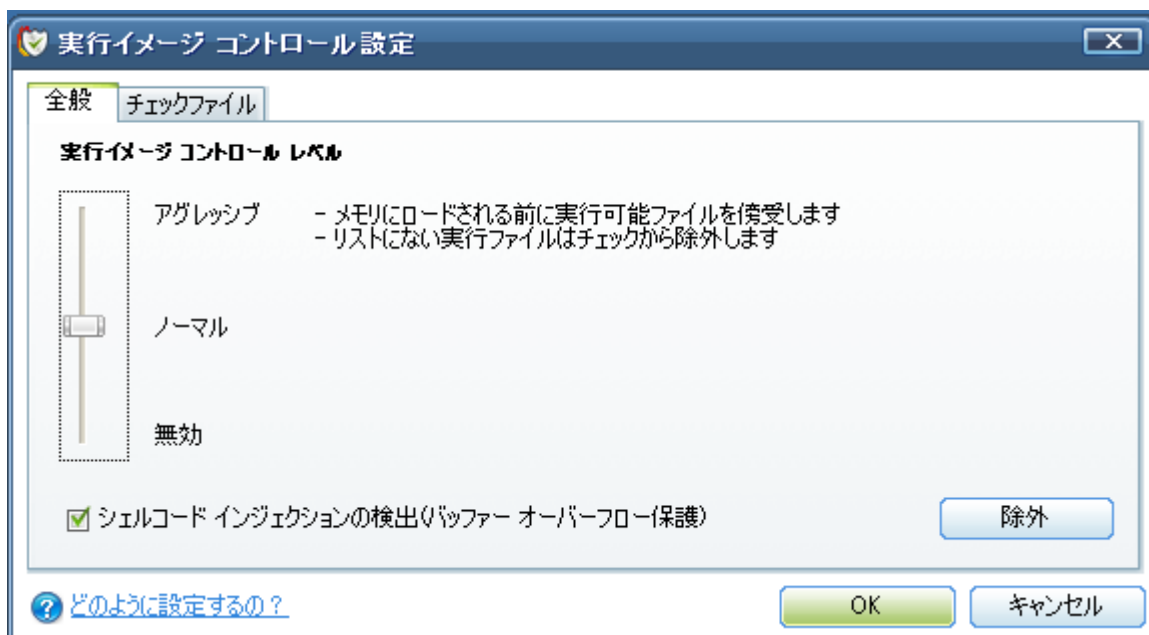
アクセス特権では対象のアプリケーションの活動の種類ごとに実行を制限できる。設定により活動がブロックされるとDefense+ のイベントログを表示 にログが残る。

保護設定

保護設定では他のプロセスからどのように対象のアプリケーションやファイルグループを保護するか設定できる。設定により他のプロセスからのアクセスがブロックされると Defense+ のイベントログを表示 にログが残る。

実行イメージ コントロール設定

Defense+ のセキュリティ強度が「セーフ モード」または「クリーン PC モード」に設定されている場合、メモリーにロードされる EXE イメージが信頼できるかどうかを Defense+ は毎回確認します。Comodo Internet Security は、実行プログラムがメモリーにロードされようとしている時点で実行プログラムのハッシュ値を算出します。そして、算出したハッシュ値と既知のアプリケーションのリストと照合します。照合する既知のアプリケーションは Comodo 安全リストに保持されています。ハッシュ値がリストの実行プログラムのいずれかと一致した場合は当該アプリケーションは安全と判断されます。ハッシュ値に一致するものが安全リストに無かった場合は、実行プログラムの安全が確認できないとしてアラートを表示します。ユーザーは、どこまで監視するか、どの種類のファイルをチェックするかを設定することができます。



アグレッシブ

これに設定すると「Files to Check」タブで指定されたファイルがメモリーにロードされる場合に加えて、プリフェッチやキャッシュされる場合にも遮断して確認ようになります。

ノーマル

Aggressive と同様ですが、プリフェッチやキャッシュされる場合にはチェックされません。これはデフォルトであり、お勧めする設定です。

無効

実行制御は作動しません。

シェルコード インジェクションの検出(バッファ オーバーフロー保護)

この設定にチェックを入れるとバッファオーバーフロー保護が有効になります。

バッファオーバーフローはプロセス/実行プログラムが固定長バッファ領域を超えてデータを格納しようとして起こる変則的な状態です。結果として、はみ出たデータで隣接するメモリ領域を上書きしてしまいます。上書きされたデータに別のバッファや変数、プログラムフローデータが含まれていた場合、プロセスがクラッシュし

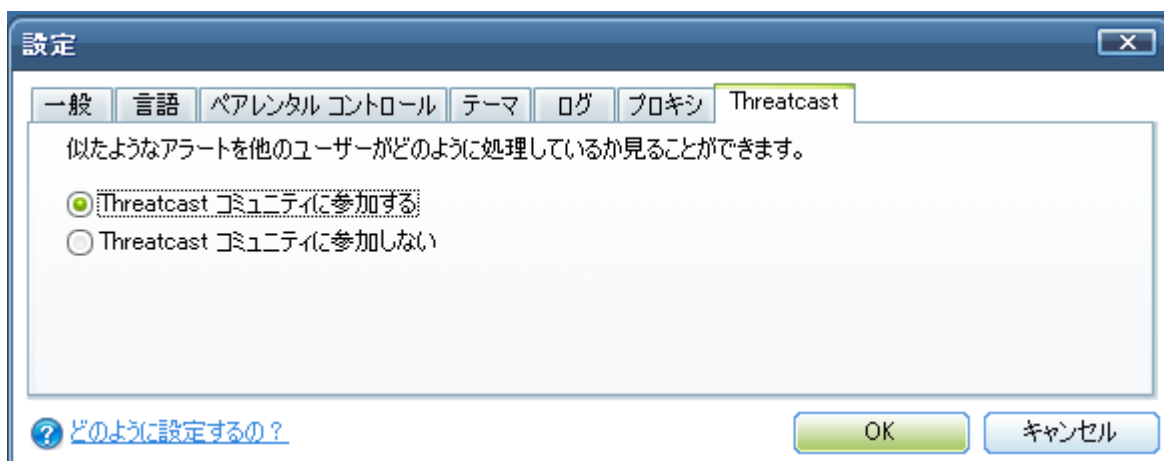
たり間違った結果を返したりする可能性があります。悪意のあるコードが実行されたりプログラムに意図しない動きをさせたりするように仕向けられたデータが、バッファオーバーフローを引き起こす場合があります。そのようにして、バッファオーバーフローはソフトウェアの脆弱性の原因になったり、弱点を突く手段になってしまいます。バッファオーバーフロー保護を有効にすると、バッファオーバーフロー攻撃の可能性がある Comodo Internet Security はアラートを表示するようになります。ユーザーはアラートで要求された動作を許可するか拒否することができます。

Comodo はこの設定を常に有効にしておくことをお勧めします。

その他の設定

Threatcast

Comodo Internet Security の Threatcast を使用すると、CIS のアラートに対する対応を、世界中の何百万人という CIS ユーザのコミュニティで共有することができます。すなわち、あるアラートに対して許可したのか拒否したのかという情報を共有できます。Threatcast を使用している各ユーザがアラートに対して許可/拒否の対応をする度にその情報が Comodo サーバーにアップロードされます。そしてアラートが表示されたときには、他の人が同様のアラートに対してどう対応したかというパーセンテージが棒グラフでアラート上に表示されます。これにより、ユーザがアラートにどう対応するかの指針を得ることができます。Comodo Internet Security のユーザには、技術に精通した方が多数います。したがって、Comodo Internet Security の多くのユーザの対応を知ることは、初心者ユーザにとって手助けになります。Threatcast を有効にすると、自身の応答もサーバーにアップロードされ、他の人の助けになります。



Threatcast コミュニティに参加する

何百万人という CIS ユーザのコミュニティに参加して CIS のアラートに対する対応を共有する場合には選択してください。

Threatcast コミュニティに参加しない

参加したくない場合に選択してください。

設定管理

設定環境をそのままエクスポート、インポートできる。ただ、アップデート時に CIS を再インストールする時は設定のアップデートも行われるので、旧バージョンでエクスポート後、新バージョンにインポートすることは推薦されない。プリセットが初めからいくつか用意されていて、インストール時の構成選択に合った初期設定が保存されているプリセットがインストール時に自動で選択される。

COMODO - Internet Security

Firewall と Antivirus をインストール時、

COMODO - Proactive Security

究極のプリセット。インストール時にも選べる。

COMODO - Antivirus Security

Antivirusのみをインストール時。

COMODO - Firewall Security

Firewallのみをインストール時。

テーマ

Comodo Internet Security のルックアンドフィールをカスタマイズすることができます。

1. *.msstyles ファイルを入手または作成します。(Windows標準のものは C:\WINDOWS\Resources\Themes\???\???.msstyles にあります。)
2. *.msstyles ファイルを C:\Program Files\COMODO\COMODO Internet Security\Themes にコピーします。
3. ファイルの拡張子を *.msstyles から *.theme に変更します。
4. その他セクション 設定 テーマ のプルダウンメニューからテーマを選択します。
5. Comodo Internet Securityを再起動します。

tips

[tips](#) を参照。

アラートの対処

アラートで許可、ブロックすると、Firewallのアラートならネットワーク セキュリティ ポリシー、Defense+のアラートなら コンピュータ セキュリティ ポリシー にルールが追加される。

アラートの振る舞いや頻度の設定はFirewallについては [セキュリティの強度](#)、Defense+については [Defense+のセキュリティ強度](#) で説明がある。

アラートの色

黄色

リスクレベル：低

オレンジ

リスクレベル：中

赤

リスクレベル：高

アラートの色によってコンピュータに及ぼすリスクが表わされるが、アラートが赤だろうと安全なプログラムの場合には許可して全く問題ないと言える。判断材料としてThreatcastが、完全ではないが役に立つだろう。

Firewall アラート

▶ Web Browser

FirefoxとかOperaとかChromeなど。

ループバック、HTTP、FTP、DNS、ポート843が許可される。ポート843は で使われる。

▶ Email Client

▶ Ftp Client

▶ Trusted Application

in, out共に全通信が許可される。

▶ Blocked Application

全通信がブロック、ログされる。

▶ Outgoing only

outのみ通信可。P2Pでなければ大方のソフトがoutgoing通信を許可すれば動作するだろう。

Defense+ アラート

▶ Installer or Updater

インストール、アップデート、アンインストールみたいな場面で選択する。インストールモードに移行するか、ダイアログが出るのでYes。数分後インストールモード解除するか、ダイアログがまだ出るのでYesで解除。

▶ Trusted Application

信用できて、変なことしないとわかってるアプリケーションの場合、選択する。

▶ Windows System Application

Windowsにもともと入ってるアプリケーションの場合、選択する。

▶ Isolated Application

隔離目的で選択する。むやみにこれを選択するとアプリケーションの不具合につながるかもしれない。

▶ Limited Application

限定的にアプリケーションを動作させたい場合、選択する。得体の知れないアプリケーションをとりあえず動かしてみる時などに有効かもしれない。

参考？ URL:

http://forums.comodo.com/help_for_v3/a_few_questions_please_help-t24602.0.html;msg176307

<http://www.google.com/search?aq=f&num=50&hl=en&newwindow=1&safe=off&q=site%3Acomodo.com+%22limited+application&btnG=Search&lr=>