

2chのコモドスレによる、cpf3.0を日本語化する活動のページです。
日本語化に関する情報を書いてください。

スレで訳文を見たら張りましょう。
誤訳、わかりにくい表現など見つけ次第直してください。

翻訳規則

- ▶ Boldの文は？ ->
- ▶ Defense+はどう訳す？ -> Defense+で。

編集記録や意見など。

- ▶ ここまではお疲れ様。ところで書き込み規則を決めないとこの先厳しい気がする。出来ればツリー形式が使いたいね。 -- 名無しさん
- ▶ 確かにDefence+のままでもいいかもしれんね - 名無しさん 2008-02-03 15:27:51
- ▶ Defense+ SettingsのMonitor Settingsがそれぞれ何を指すのか解説頂けると助かります。 - 名無しさん 2008-07-21 18:35:01
- ▶ Interprocess Memory Access を不自然ながら訳した。 - 名無しさん 2008-07-28 16:55:00
- ▶ これってむしろ意識のほうがいいんじゃない？ってことで手直し - 名無しさん 2008-10-08 19:04:06
- ▶ ファイアーよりもファイアウォールの方が良い - 名無しさん 2009-03-16 18:42:28
- ▶ loopback network interfaceの訳は？ - 名無しさん 2009-03-17 00:47:21
- ▶ windows system application - 名無しさん 2009-03-26 17:27:10
- ▶ Defense+ga - 名無しさん 2009-05-23 16:43:04
- ▶ Defense+が英語ならFWも英語でいいと思うけど - 名無しさん 2009-05-23 16:43:32
- ▶ Defense+は固有名詞だからカナ表記すると変だがファイアウォールは一般名詞だからカナにするべき - 名無しさん 2010-03-14 02:42:12

名前:

書き込む

- ▶ メインウィンドウ
 - ▶ summary : 概要
 - ▶ firewall : ファイアウォール
 - ▶ common tasks : 一般
 - ▶ advanced : 詳細
 - ▶ defense+ : ディフェンス+
 - ▶ common tasks : 一般
 - ▶ advanced : 詳細
 - ▶ miscellaneous : 他
- ▶ Defense+ Alert :
 - ▶ access the loopback network interface
 - ▶ exeute
 - ▶ access xxx.exe in memory
- ▶ Firewall Alert
- ▶ Help (Comodo Firewall User Guide)
 - ▶ Defense+ Task > Advanced
 - ▶ Defense+ Settings
- ▶ Ver.3.xのインストールウィザードの文を訳してみよう。

メインウィンドウ

summary : 概要

system status : システムの状況

all systems are active and running.
you do not need to perform any actions at this time.
システムはすべて有効に作動しています。
現在すぐに処置する必要はありません。

network defence : ネットワークの防御

the firewall blocked intrusion ~ attempt(s) sofar
the firewall security level is set to ~
これまでファイアウォールにより~の侵入を遮断しました。
ファイアウォールのセキュリティのレベルは~に設定されています。

proactive defense : ディフェンス+ (proactiveは予防的などという意味だろうがこの場合はディフェンス+を指すのだろう)

defence+ has blocked ~ suspicious attempt(s) so far
defence+ security level is set to ~
これまでディフェンス+により疑わしい接続を遮断しました。
ディフェンス+のセキュリティのレベルは~に設定されています。

highlights : 広告 (ハイライトは重要な場面とかいう意味で使うが文を見る限りコモドに関するニュースだろう) 表示される文章はインストールフォルダ内cfpinfo.iniに記述されている

traffic : トラフィック

tips of the day : 今日のワンポイント (did you know ~ の形でファイアウォールにこういう機能があることを表示する) 表示される文章はインストールフォルダ内cfpinfo.iniに記述されている (文字化けている気がしますが)

firewall : ファイアウォール

common tasks : 一般

view firewall events : ファイアウォールの記録を見る

This section allows you to view a record of the events and alerts triggered by possible attacks on your computer.
コンピュータに対する攻撃によるイベント(このままでいいかな?)と警告の記録を見ます。

define a new trusted application : 信頼するアプリケーションを指定する

This shortcut represents a convenient way to create an automatic shortcut 'Allow' rule for applications that you trust.
信頼するアプリケーションを自動的に許可するルールを作成します。

define a new blocked application : 遮断するアプリケーションを指定する

This shortcut represents a convenient way to create an automatic shortcut 'Deny' rule for applications that you do not trust.

信頼しないアプリケーションを自動的に拒否するルールを作成します。

stealth ports wizard : ステルスポート・ウィザード

This wizard allows you to create a set of global firewall rules, which will affect your computer's visibility from other computers.

あなたのコンピュータが他のコンピュータからどう見えるかに関わる全般的なファイアウォールのルールの一部を設定します。

view a active connections : 現在の接続を見る

view which application are currently connecting to the Internet along with the IP, Port, Protocol and Traffic level of the connection.

どのアプリケーションが現在インターネットに接続しているかを、IPアドレス、ポート、プロトコル、転送量と共に表示します。

my port sets : ポートの編集

my network zones : ネットワークゾーンの編集

my blocked network zones : 遮断するネットワークゾーンの編集

advanced : 詳細

network security policy : ネットワーク・セキュリティー・ポリシー

predefined firewall policies : 予め指定したファイアウォールのポリシー

attack detection settings : 攻撃の検知に関する設定

firewall behavior settings : ファイアウォールの作動に関する設定

defense+ : ディフェンス+

common tasks : 一般

view defense+ events : ディフェンス+の記録を見る

my protected files : 保護するファイル

my quarantined files : 隔離するファイル

my pending files : 保留しているファイル

my own safe files : 安全な実行ファイル

view active process : 現在のプロセス見る

my trusted software vendor : 信頼するソフト会社

my protected registry keys : レジストリキー

my protected com interfaces : 保護するCOM インターフェイス

advanced : 詳細

computer security policy : コンピューター・セキュリティー・ポリシー

This section is all about Defense+ rules. Advanced users can use this section to manage the Defense+ rules to exploit the full power of the Defense+ engine.

ディフェンス+の全てのルールに関する項目です。上級者はこの項目でディフェンス+のルールを定義することによってディフェンス+エンジンを最大限に活用できます。

Predefined Security Policy : 予め指定したセキュリティー・ポリシー

You can create a set of Defense+ rules which can be shared of by more than one application. Such a set is called a Predefined Security Policy

あなたは複数のアプリケーションで共有することの出来るディフェンス+のルールのセットを設定出来ます。そのようなセットは予め指定したセキュリティー・ポリシーから呼び出されます。(もっと上手く訳して)

Image Execution Control Settings : 画像の実行の制御に関する設定(ファイルの実行制御、あたりのほうがいい気が、少なくともImageは画像ではない、)

Image Execution Control Settings is an integral part of Defense+ engine. It is responsible for authenticating every executable image being loaded into the memory.

ファイルの実行制御はディフェンス+エンジンの不可欠な部分です。これはあらゆる実行可能なイメージがメモリに読み込まれることに対して責任を持ちます。(責任でいいのかな?)

Defense+ Settings : ディフェンス+の設定

Defense+ has many options which affect its defense mechanisms. You can easily modify these options to make Defense+ operate according to the specific defense requirements of your computer.

ディフェンス+には防御の体系に影響する多くの設定があります。Defense+をコンピュータの個々の防御の必要性に沿うように動作させるために、これらのオプションを簡単に変更できます。

miscellaneous : 他

settings : 設定

this section lets you configure general settings like password protection, update options, language, theme, etc.

パスワード、アップデート、言語、スキンなどの一般的な設定を行います。

manage my configurations : 設定情報の編集

this section allows you to import/export/delete your firewall's configuration settings

ファイアーウォールの設定のインポート、エクスポート、削除を行います。

diagnostics : 診断

did your firewall report an error? this tool may help you to identify the problem.

ファイアーウォールからエラーが出た場合に問題の特定を補助します。

check for updates : アップデートの確認

check for the latest updates for your fire wall to make sure it is to up-to-date.

ファイアーウォールの最新のアップデートを確認します。

submit suspicious files : 疑わしいファイルの情報の送信

did your firewall report suspicious files?

you can submit as many files as you wish to COMODO for analysis by using this section

ファイアウォールにより疑わしいファイルを検出した場合に、コモド社での分析のための情報としてファイルの情報を送信します。

browse support forums : サポートフォーラムを見る

Need help? find answer to your question in COMODO forums,
our developers regularly post and we would love to hear from you.

コモド・フォーラムを表示します。

(そのまま訳するなら「お困りでしょうか? コモド・フォーラムで疑問の答えを探してみましょう。
開発者も定期的に投稿し、ユーザーのご意見をお待ちしています。」のようになるけれども、端折ってみた。)

help : ヘルプ

do you want to learn more about your firewall?

you can use this section to view the help file.

ファイアウォールについて知りたいときにヘルプファイルを見ることができます。

about : このソフトについて

view the copyright and version information about your firewall

商標登録およびこのファイアウォールのバージョン情報を表示します。

Defense+ Alert :

Defense+のAlertはいくつかパターンがある。

access the loopback network interface

xxx.exe is trying to **{access the loopback network interface}**. What would you like to do?

xxx.exeはループバックインターフェイス(*)にアクセスを試みています。どうしますか?

(* 自ホストで動くプロセスとの通信やソフトのテストのために使われるネットワーク、IPアドレス127.0.0.1が一般的)

Security Consider actions:

xxx.exe **{could not be recognized}** and it is **{about to access the loopback network interface.}** The IP address range **{127.0.0.0.1/127.255.255.255}** belongs to a special network zone called the loopback network interface. Although it is a pseudo-network zone i.e. no real network traffic occurs to/from your computer, it allows an application to communicate with other applications such as local proxy servers installed in the same computer. If xxx.exe is one of your everyday applications, you can safely allow this request.

xxx.exeのループバックインターフェイスへのアクセスは承認されていません。その(ループバックインターフェイスの)IPアドレスの範囲は127.0.0.1から127.255.255.255でループバックインターフェイスと呼ばれる特別なネットワークゾーンに属しています。たとえそれが疑似的なネットワーク、つまりパケットのやりとりがないもので

あっても、アプリケーションに他のアプリケーションとコミュニケーションを取るための、媒体をインストールする事を許可するようなものです。もしxxx.exeが信頼できるアプリケーションの一つなら、あなたはこの要求を安全に許可できます。

Allow this request : 許可する

Block this request : 拒否する

Treat this application as : プリセットから指定(超意識)

-Installer or Updater : インストーラまたはアップデータ

-Trusted Application : 信頼するアプリケーション

-Windows System Application : ウィンドウズのシステムアプリケーション

-Isolated Application : 隔離するアプリケーション(or 信頼しない、拒否する のほうがいいのかも)

-Limited Application : 動作を制限するアプリケーション

Remember my answer

exeute

xxx.exe is trying to execute yyy.exe. What would you like to do?

xxx.exeはyyy.exeを実行しようとしています。どうしますか？

Security Consider actions:

access xxx.exe in memory

Firewall Alert

xxx.exe is trying to **{connect to the internet}**. What would you like to do?

xxx.exeはインターネットに接続しようとしています。処理の選択

Application:

Remote:

Port:

Security Consider actions:

xxx.exe **{could not be recognized}** and it is about to connect the internet. If it is one of your everyday applications, you can allow this request.

xxx.exeのインターネット接続は承認されていません。もしxxx.exeが信頼できるアプリケーションの一つなら、この要求を許可できます。

Allow this request : (接続を)許可する

Block this request : 拒否する

Treat this application as : プリセットから指定(超意識)

-Web Browser : Webブラウザ

-Ftp Client : FTPクライアント

-Trusted Application : 信頼するアプリケーション
-Blocked Application : 信頼しないアプリケーション
-Outgoing Only : 外向きの接続のみ受け付ける
Remember my answer

Help (Comodo Firewall User Guide)

Defense+ Tasks > Advanced

Defense+ Settings

'Monitor Settings' tab

The 'Monitor Settings' tab allows you configure which activities, entities and objects should be monitored by Defense+.

「モニター設定」タブは各部の動作や、Defense+によってモニターするオブジェクトを設定します。

Note: The settings you choose here are universally applied.

ここで選択された設定は全体に適用されます。

If you disable monitoring of an activity, entity or object using this interface it will completely switch off monitoring of that activity on a global basis - effectively creating a universal 'Allow' rule for that activity . This 'Allow' setting will over-rule any policy specific 'Block' or 'Ask' setting for that activity that you may have selected using the 'Access Rights' and 'Protection Settings' interface.

もし、いずれかのモニタリングを無効にした場合、完全にそれらのモニタリングは基本的に無効にされます。これは普遍的な'許可(Allow)'のルールです。この'許可'するルールは'Access Rights'や'Protection Settings'の画面から設定できる'不許可(Block)'や'確認(Ask)'より優先順位が高いルールとなるでしょう。

Activities To Monitor:

Interprocess Memory Access - Malware programs use memory space modification to inject malicious code for numerous types of attacks, including recording your keyboard strokes; modifying the behavior of the invaded application; stealing confidential data by sending confidential information from one process to another process etc. One of the most serious aspects of memory-space breaches is the ability of the offending malware to take the identity of the invaded process, or 'impersonate' the application under attack. This makes life harder for traditional virus scanning software and intrusion-detection systems. Leave this box checked and Defense+ will alert you when an application attempts to modify the memory space allocated to another application.

Interprocess Memory Access - マルウェアは多種多様な攻撃用の悪意のあるコードを注入するためにメモリスペース改変を用います。攻撃の種類は、キーロガー、進入されたアプリケーションのふるまいの制限、あるプロセスから他のプロセスに内部情報を送ることによる内部情報の窃盗、などを含みます。もっとも深刻なメモリスペース違反のひとつは、進入されたプロセスのアイデンティティを維持したり、攻撃下にあるアプリケーションの「ふり

をする」、問題のあるマルウェアの能力です。これらは伝統的なウイルスをスキャンするソフトウェアと進入検知システムを動作させにくくします。ボックスのチェックを残すことで、Defense+はあるアプリケーションが他のアプリケーションに割り当てられたメモリスパースの改変を企てた時、あなたに知らせます。

Windows/WinEvent Hooks - In the Microsoft Windows operating system, a hook is a mechanism by which a function can intercept events (messages, mouse actions, keystrokes) before they reach an application. The function can act on events and, in some cases, modify or discard them. Originally developed to allow legitimate software developers to develop more powerful and useful applications, hooks have also been exploited by hackers to create more powerful malware. Examples include malware that can record every stroke on your keyboard; record your mouse movements; monitor and modify all messages on your computer; take over control of your mouse and keyboard to remotely administer your computer. Leaving this box checked means that you are warned every time a hook is executed by an untrusted application.

Windows/WinEvent Hooks - Windowsにはアプリケーションに届く前にメッセージやマウスの動き、キーボード入力を傍受する関数(システム)があります。この関数が作動すると、時としてそれらが改竄されたり捨てられたりすることがあります。元々はソフトウェア開発者により有用でパワフルなアプリケーションの開発のために開発されましたが、これはより強力なマルウェアを作成するハッカー達の攻撃手段になっています。たとえば、あなたの全てのキー入力、マウス操作の記録、画面の監視、改竄ができるマルウェアが含まれていれば、マウスやキーボードのコントロールは間接的なあなたのパソコンの管理者(攻撃者)に乗っ取られます。このボックスのチェックを残すことは、常に信頼できないアプリケーションによってこの関数が実行されることを、あなたに警告することを意味します。

Device Driver Installations - Device drivers are small programs that allow applications and/or operating systems to interact with a hardware device on your computer. Hardware devices include your disk drives, graphics card, wireless and LAN network cards, CPU, mouse, USB devices, monitor, DVD player etc.. Even the installation of a perfectly well-intentioned device driver can lead to system instability if it conflicts with other drivers on your system. The installation of a malicious driver could, obviously, cause irreparable damage to your computer or even pass control of that device to a hacker. Leaving this box checked means Defense+ will alert you every time a device driver is installed on your machine by an untrusted application.

Loopback Networking - Loopback connections refer to the internal communications within your PC. Any data transmitted by your computer through a loopback connection is immediately also received by it. This involves no connection outside your computer to the internet or a local network. The IP address of the loopback network is 127.0.0.1, which you may have heard referred to under its domain name of '<http://localhost>' i.e. the address of your computer. Loopback channel attacks can be used to flood your computer with TCP and/or UDP requests which can smash your IP stack or crash your computer. Leaving this box checked means Defense+ will alert you every time a process attempts to communicate using the loopback channel.

Process Terminations - A process is a running instance of a program. (for example, the Comodo Firewall Pro process is called 'cfp.exe'. Press 'Ctrl+Alt+Delete' and click on 'Processes' to see the full list that are running on your system). Terminating a process will, obviously, terminate the program. Viruses and Trojan horses often try to shut down the processes of any security software you have been running in order to bypass it. With this setting enabled, Defense+ will monitor and alert you to all attempts by an untrusted application to close down another application.

Window Messages - This setting means Comodo Firewall Pro will monitor and detect if one application attempts to send special Windows Messages to modify the behaviour of another application (e.g. by using the WM_PASTE command).

DNS Client Service - This setting alerts you if an application attempts to access the 'Windows DNS service' - possibly in order to launch a DNS recursion attack. A DNS recursion attack is a type of Distributed Denial of Service attack

whereby an malicious entity sends several thousand spoofed requests to a DNS server. The requests are spoofed in that they appear to come from the target or 'victim' server but in fact come from different sources - often a network of 'zombie' pc's which are sending out these requests without the owners knowledge. The DNS servers are tricked into sending all their replies to the victim server - overwhelming it with requests and causing it to crash. Leaving this setting enabled will prevent malware from using the DNS Client Service to launch such an attack.

Note for beginners: DNS stands for Domain Name System. It is the part of the Internet infrastructure that translates a familiar domain name, such as 'example.com' to an IP address like 123.456.789.04. This is essential because the Internet routes messages to their destinations on the basis of this destination IP address, not the domain name. Whenever you type a domain name, your internet browser contacts a DNS server and makes a 'DNS Query'. In simplistic terms, this query is 'What is the IP address of example.com?'. Once the IP address has been located, the DNS server replies to your computer, telling it to connect to the IP in question.

Entities To Monitor Against Modifications:

- ▶ Protected COM Interfaces enables monitoring of COM interfaces you specified here.

- ▶ Protected Registry Keys enables monitoring of Registry keys you specified here.

- ▶ Protected Files/Folders enables monitoring of files and folders you specified here.

Objects To Monitor Against Direct Access:

Determines whether or not Comodo Firewall Pro should monitor access to system critical objects on your computer.. Using direct access methods, malicious applications can obtain data from a storage devices, modify or infect other executable software, record keystrokes and more. Comodo advise the average user to leave these settings enabled:

- ▶ Physical Memory

Monitors your computer's memory for direct access by an applications and processes. Malicious programs will attempt to access physical memory to run a wide range of exploits - the most famous being the 'Buffer Overflow' exploit. Buffer overruns occur when an interface designed to store a certain amount of data at a specific address in memory allows a malicious process to supply too much data to that address., This overwrites its internal structures and can be used by malware to force the system to execute its code.

- ▶ Computer Monitor

Comodo Firewall Pro will raise an alert every time a process tries to directly access your computer monitor. Although legitimate applications will sometimes require this access, there is also an emerging category of spyware-programs that use such access to monitor users' activities. (for example, to take screenshots of your current desktop; to record your browsing activities etc)

- ▶ Disks

Monitors your local disk drives for direct access by running processes. This helps guard against malicious software that need this access to, for example, obtain data stored on the drives, destroy files on a hard disk, format the drive or corrupt the file system by writing junk data.

- ▶ Keyboard

Monitors your keyboard for access attempts. Malicious software, known as 'keyloggers', can record every stroke you make on your keyboard and can be used to steal your passwords, credit card numbers and other personal data. With this setting checked, Comodo Firewall Pro will alert you every time an application attempts to establish direct access to your keyboard.

Ver.3.xのインストールウィザードの文を訳してみよう。

in case you have any third party personal firewall installed,
please uninstall that before installing COMODO firewall Pro. Would you like to continue?
他社製のパーソナル・ファイアウォールをインストールしている場合には
コモド・ファイアウォール・プロをインストールする前にそちらをアンインストールしてください。続けますか？

welcome to the Comodo Firewall Pro Installer.
This will install COMODO Firewall Pro on your computer.
to continue,please click "Next" button.
コモド・ファイアウォール・プロインストーラーを起動しました。
これよりコンピューターにコモド・ファイアウォール・プロをインストールします。
続けるには「Next」をクリックしてください。

do you accept all the terms of the proceeding licence agreement?
If you choose "I DECLINE" the set up will close.
To install the COMODO Firewall Pro, you must accept this agreement.
使用許諾契約書のすべての項目に同意しますか？
「I DECLINE」を選択すると、インストールせずに終了します。
コモド・ファイアウォール・プロをインストールするには、この契約書に同意しなければなりません。

Setup will install COMODO Firewall Pro in the following folder.
to install to this folder click next. To install to a different folder,
click Browse and select another folder.
以下のフォルダにコモド・ファイアウォール・プロをインストールします。
このフォルダにインストールする場合は「next」をクリックしてください。
異なるフォルダにインストールする場合には、「Browse」をクリックして他のフォルダを選択してください。

Welcome to the Comoco Firewall Configuration Wizard.
This wizard will help you to configure you firewall in the couple of steps.
During this process,please do not close the wizard or power off on your computer
The installation may cause your internet connection to be temporarily dropped.
please save all your work before continuing.
To continue,please press "Next" button.

コモド・ファイアウォール設定ウィザードへようこそ。
このウィザードによってファイアウォールをかんたんに設定することができます。
設定中は、このウィザードを閉じたりコンピューターの電源を切らないでください。
インストールにより、一時的にインターネットの接続が切断されることがあります。
このウィザードを続ける前に作業中のものをすべて保存しておいてください。
続けるには「Next」を押してください。

COMODO Firewall Pro has many powerful features which affect the number of popup alerts you may see while it is installed.
コモド・ファイアウォール・プロではポップアップ・アラートを出す有用な機能が多く装備されています。

▶ advanced Firewall with Defence+ (ディフェンス+付き 上級モード)

this option is recommended for experienced users.in addition to the firewall engine, it is going to activate the Defence+ to cope with malware by protecting more resorces than just your internet connection.

The number of popup alerts may increase depending on your configuration.

こちらは熟練したユーザーにおすすめです。ファイアウォール・エンジンに加えてインターネット接続よりも多くのリソースを保護することで、悪質なソフトウェア（マルウェア）の活動に対処する「Defence+」を有効にします。
ただし、設定によってはポップアップ警告が多くなることがあります。

▶ Basic Firewall (基礎モード)

this option is recommended if you are not familiar with computer too much or you do not want to see frequent alerts from your firewall.

It will not activate Defence+ to fight with malware but your computer still be secured with an industry strength firewall engine.

こちらはあまりコンピューターに詳しくない人、頻繁なポップアップ警告に悩まされたくない人におすすめです。悪質なソフトウェア（マルウェア）に対処するための「Defence+」は有効になりませんが、セキュリティーは有料のファイアウォールなみのエンジンによって保護されます。

COMODO Firewall Pro has been installed succesfully.

Please restart the system for installation to complete

コモド・ファイアウォール・プロが正しくインストールされました。

システムを再起動しインストールを完了してください。