HAGIWARA Solutions

コピーガード設定ソフト
IC Manager For Device
マニュアル

この度は SecurityUSB Manager(以下、本ソフトウェア)をご購入いただき誠にありがとうございます。このマニュアルではコピーガード設定ソフト：IC Manager For Device の使用方法を説明しています。本ソフトウェアを正しくご利用いただくために、使用開始前に、必ずこのマニュアルを必ずお読みください。

1 ソフトウェア使用許諾契約書

本契約は、お客様（以下「お客様」とします）とハギワラソリューションズ株式会社（以下「弊社」とします）との間で弊社がお客様へ提供するソフトウェア（以下「許諾ソフトウェア」とします）の使用権許諾に関して次のように条件を定めます。

弊社は、お客様に対して、以下の条件に従って許諾ソフトウェアの使用を許諾いたします。お客様は、本契約書の内容をしっかりとお読みになり、本契約書の内容に同意できる場合に限り、お客様の責任で許諾ソフトウェアを使用してください。許諾ソフトウェアを使用することによって、お客様は本契約の各条項に同意したものとみなされます。本契約の各条項に同意されない場合、弊社はお客様に対し、許諾ソフトウェアのご使用を許諾できません。

第１条（総則）

許諾ソフトウェアは、日本国内外の著作権及びその他知的財産権に関する諸法令及び諸条約によって保護されています。許諾ソフトウェアは、本契約の条件に従い弊社からお客様に対して使用許諾されるもので、許諾ソフトウェアの著作権等の知的財産権は弊社に帰属し、お客様に移転いたしません。

第２条（使用権）

1. 弊社は、許諾ソフトウェアの非独占的な使用権をお客様に許諾します。
2. 本契約によって生ずる許諾ソフトウェアの使用権とは、お客様が取得または購入された許諾ソフトウェアがインストールされている電子機器上において、許諾ソフトウェアをお客様の機器等に対して使用する権利をいいます。
3. お客様は、許諾ソフトウェアの全部又は一部を複製、複写、並びに、これに対する修正、追加等の改変をすることが

できません。

第３条（権利の制限）

1. お客様は、許諾ソフトウェアを再使用許諾、譲渡、貸与又はリースその他の方法で第三者に使用させてはならないものとします。
2. お客様は、許諾ソフトウェアを用いて、弊社又は第三者の著作権等の権利を侵害する行為を行ってはならないものとします。
3. お客様は、許諾ソフトウェアに関しリバースエンジニアリング、逆アセンブル、逆コンパイル等のソースコード解析作業を行ってはならないものとします。
4. お客様は、本契約に基づいて、許諾ソフトウェアがインストールされている電子機器と一体としてのみお客様の許諾ソフトウェアに関する権利の全てを、譲受人が本契約の条項に同意することを条件に譲渡することができます。但しその場合、お客様は許諾ソフトウェアの複製物を保有することはできず、許諾ソフトウェアの一切（全ての構成部分、媒体、電子文書及び本契約書を含みます）を譲渡しなければなりません。

第４条（許諾ソフトウェアの権利）

許諾ソフトウェアに関する著作権等一切の権利は、弊社または、本契約に基づきお客様に対して使用許諾を行うための権利を弊社に認めた原権利者（以下原権利者とします）に帰属するものとし、お客様は許諾ソフトウェアに関して本契約に基づき許諾された使用権以外の権利を有しないものとします。

第５条（責任の範囲）

1. 弊社及び原権利者は、第６条２項に定義するアップデートデータが正常にインストールできることを保証いたしません。また、弊社及び原権利者は、当該アップデートデータのインストールによってお客様に損害が発生しないことを保証いたしません。
2. 弊社及び原権利者は、許諾ソフトウェアにエラー、バグ等の不具合がないこと、若しくは許諾ソフトウェアが中断なく稼動すること又は許諾ソフトウェアの使用がお客様及び第三者に損害を与えないことを保証しません。また、弊社及び原権利者は、許諾ソフトウェアが第三者の知的財産権を侵害していないことを保証いたしません。
3. 許諾ソフトウェアの稼動が依存する、許諾ソフトウェア以外の製品、ソフトウェア又はネットワークサービス（第三者が提供する場合に限られず、弊社又は原権利者が提供する場合も含みます）は、当該ソフトウェア又はネットワークサービスの提供者の判断で中止又は中断する場合があります。弊社及び原権利者は、許諾ソフトウェアの稼動が依存するこれらの製品、ソフトウェア又はネットワークサービスが中断なく正常に作動すること及び将来に亘って正常に稼動することを保証いたしません。
4. お客様に対する弊社及び原権利者の損害賠償責任は、当該損害が弊社又は原権利者の故意又は重過失による場合を除きいかなる場合にも、お客様に直接且つ現実に生じた通常の損害に限定され且つお客様が証明することのできる許諾ソフトウェアの購入代金を上限とします。
5. 弊社又は原権利者は、債務不履行及び不法行為等の理由の如何にかかわらず、如何なる場合においても、お客様に生じた逸失利益、結果的損害、間接損害、若しくは、データ消失及び破損における損害については、一切賠償する責を負わないものとする。
6. 弊社は、弊社ウェブページにて定めるお問合わせ窓口（許諾ソフトウェア購入ページからリンクしてご確認ください。）に限り、お客様が弊社から使用許諾を受けた許諾ソフトウェアに関する技術的サポートを提供します。但し、弊社は、お客様の同意を得ることなく、当該窓口の受付時間及び当該サポートの提供の有無について随時変更することができるものとします。なお、弊社は、お客様との間で、別途契約を締結しないかぎり、当該サポートをお客様に提供及び

継続する義務を一切負うことはありません。

第６条（著作権保護及び自動アップデート）

1. お客様は、許諾ソフトウェアの使用に際し、日本国内外の著作権及びその他知的財産権に関する諸法令及び諸条約に従うものとします。
2. お客様は、弊社又は弊社の指定する第三者がウェブ上に、許諾ソフトウェアのセキュリティ機能の向上、エラーの修正、アップデート機能の向上等の目的で許諾ソフトウェアが適宜にアップデートデータ（以下「アップデートデータ」とします）を公開する場合は、アップデートデータ公開後 90 日以内に許諾ソフトウェアをアップデートしなければなりません。また、お客様は、アップデートデータ公開後 90 日を経過した場合は、旧許諾ソフトウェアを、アップデートをする目的以外で使用することができません。お客様は、(ⅰ)当該許諾ソフトウェアのアップデートに伴い、許諾ソフトウェアの機能が追加、変更又は削除されることがあること、及び(ⅱ)アップデートされた許諾ソフトウェアについても本契約が適用されることに同意するものとします。

第７条（契約の解約）

1. 弊社は、お客様が本契約に定める条項に違反した場合、直ちに本契約を解約することができるものとします。
2. 前項の規定により本契約が終了した場合、お客様は契約の終了した日から ２週間以内に許諾ソフトウェアの全てを廃棄するか、弊社に対して返還するものとします。お客様が許諾ソフトウェアを廃棄した場合、直ちにその旨を証明する文書を弊社に差し入れるものとします。
3. 本条１項の規定により本契約が終了した場合といえども、第４条、第５条、第７条第２項及び第３項並びに第８条第１項及び第３項乃至第５項の規定は有効に存続するものとします。

第８条（その他）

1. 本契約は、日本国法に準拠するものとします。
2. お客様は、許諾ソフトウェアを国外に持ち出して使用する場合、適用ある条例、法律、輸出管理規制、命令に従うものとします。
3. 本契約に関連する一切の紛争については、弊社本店所在地の地方裁判所または簡易裁判所を第一審の専属管轄裁判所とします。
4. 本契約の一部条項が法令によって無効となった場合でも、当該条項は法令で有効と認められる範囲で依然として有効に存続するものとします。
5. 本契約に定めなき事項又は本契約の解釈に疑義を生じた場合は、お客様及び弊社は誠意をもって協議し、解決するものとします。

2 本ソフトウェアについて

本ソフトウェアは、ウイルス対策 USB シリーズ（トレンドマイクロ・シマンテック・マカフィ）、パスワードロッカー３のコピーガード設定を行うソフトウェアです。

コピーガード機能について

コピーガード機能とは自宅 PC 等で USB メモリ内のファイルを編集する際に、USB メモリから外部にファイル操作を制限する機能です。USB メモリ内であればファイルの編集は可能なため、データの不正流出を防ぎ、社外での作業を可能にします。
ユーザ様の自宅でも仕事がしたいという要望と管理者様のデータ流出を防ぎたいという要望にお答えします。

本ソフトウェアでできること

■コピーガードの設定
- 通常 USB メモリ(オフィスモード)として使用可能な PC の登録、登録クリア
- 印刷禁止設定
- スクリーンキャプチャ禁止設定
- クリップボード使用禁止設定
- ネットワーク共有フォルダへのアクセス禁止設定
- インターネットアクセス禁止設定
- エンドポイント監視設定
- ファイルアクセスログの取得
- 印刷ログの取得

製品仕様

USB インターフェース	USB1.1(Full Speed)/USB 2.0（High Speed/Full Speed）USB3.0(Super Speed)
動作環境*1*2	USB インターフェイス(USB2.0 必須)を搭載した DOS/V 機器 Pentium4 1.4GB 以上の CPU 物理空きメモリ容量 512MByte 以上 ハードディスク空き容量 500MB 以上
対応 OS	Windows XP withSP3 Windows VISTA withSP2 Windows 7 with SP1 Windows 8/8.1 ※日本語 OS 場合、日本語表示になります
対応ユーザアカウント	コンピュータの管理者（Administrator）※制限ユーザには対応しておりません
対象 USB メモリ	・ウイルス対策 USB MF-PUVT**GM*/ MF-PUVT3**GM* ・ウイルス対策 USB HUD-PUVS**GM/USB HUD-PUVS3**GM* ・ウイルス対策 USB HUD-PUVM**GM*/ USB HUD-PUVM3**GM* ・パスワードロッカー3/4(HUD-PL**GM/ HUD-PL3**GM)

*1　拡張ボードで増設した USB インターフェースには対応していません。
*2　USB Mass Storage Class ドライバ、HID Class ドライバ、CD-ROM ドライバがあらかじめ組み込まれている必要があります。

その他制限事項

システムご利用上の注意・制限事項

1.コピーガード機能利用後、ログオフ・シャットダウン時にアプリケーションエラーが表示される場合があります。
通常、ユーザプロセスのエラーのため、システムやアプリケーションに重大な異常が発生するものではありません。引き続きご利用いただいても、問題はありません。

2. コピーガード機能利用時、SecurityUSB 以外のアプリケーションを終了させるときにアプリケーションエラーが表示される場合があります。
アプリケーションに異常が発生するものではありません。引き続き利用していただいても、問題はありません。

3.プリンタ・スキャナなどの周辺機器について
モバイルモード中はローカル HDD へのアクセスが制限されるため、プリンタやスキャナ等の周辺機器が正常に動作しない場合があります。

4.日本語変換ソフトウェアについて
モバイルモードでサポートしている日本語変換ソフトウェアは、OS 付属の日本語変換ソフトウェア（MS-IME）、Microsoft Office（2007、2010、2013）付属の日本語変換ソフトウェア、ATOK（2011～2013）となります。
ローカル HDD の書き込み制御の影響で、ユーザー辞書やオプションの辞書は利用できない場合があります。
・Google IME、Baidu IME、ATOK スマイル等はサポートしていません。
ユーザー辞書機能が利用できないなど、動作に制限が発生する場合があります。

5.Windows8/8.1 では「Windows ストアアプリ」の動作をサポートしていません。
拡張子に関連付けられたアプリケーションが Windows ストアアプリに設定されている環境ではファイルが実行されません。予め、拡張子の関連付けをデスクトップアプリケーションに設定してご利用ください。
（PDF の閲覧は Adobe Reader をご利用ください。）

6.ユーザー切り替えは、ご利用頂けません。

7.一部のウイルス対策ソフトで、コピーガード機能の動作に対して警告と動作制限が加えられる場合があります。
SecurityUSB のプログラムモジュールを除外設定することで回避できる場合があります。

8.SecurityUSB メモリを利用中に Windows が休止/スリープ状態になると、休止/スリープ状態からの復帰時、専用 USB メモリが切り離されていて、動作中のアプリケーションなどが誤動作する場合があります。
SecurityUSB メモリの利用中は、休止/スリープ状態にならないようにしてください。

9.他社の暗号化ソフトウェア・ログ取得ソフトウェア・デバイス制御ソフトウェアなどが動作している PC では、コピーガード機能が利用している基本技術と競合して、正常に動作しない場合があります。

10.USB 接続ケーブルや、USB ハブを経由して専用 USB メモリを接続すると、正しく動作しないことがあります。このような場合には、USB 接続ケーブルや USB ハブを取り外して、動作が改善するかご確認ください。

11.Office 2007（IME 2007）を使用中に漢字変換すると Office 2007 が強制終了する場合があります（IME 2007 の不具合です）。
IME 2007 をご利用の場合は、IME 2010 にアップデートしてご利用ください。
（KB938574）

12. コピーガード機能の動作中は、アプリケーションのインストールが正常にできない場合があります。

インターネットアクセス禁止関連の注意・制限事項

1.インターネットアクセス制限を利用したとき、Internet Explorer コンポーネントを利用しているアプリケーションの動作が極端に遅くなる場合があります。

2.Internet Explorer 10 及びそれ以降のバージョンをご利用時に
「この Web サイトのセキュリティ証明書には問題があります。」のメッセージが表示されるサイトで閲覧を続行するとページが表示されない場合があります。
その際は Internet Explorer の保護モード機能を無効に設定してご利用ください。

モバイルモードでの注意・制限事項

1.モバイルモードは全てのシステム構成での動作を保証するものではありません。
一般に利用されるアプリケーションでも、モバイルモードで正常に動作しない場合があります。
また、セキュリティ上の理由から、コントロールパネルや管理ツール等の動作も抑止されます。
※ローカル HDD への書き込み制御だけでなく、レジストリや環境変数に対するアクセス制御や内容の一時的な入れ替え、OS システムコール等へのアクセス制御や介在を行っているため、アプリケーションの各種機能が通常通り動作しない場合があります。

2.動作確認済みのアプリケーションは以下の通りです。括弧内のファイル形式以外のファイルは利用できない場合があります。
- Microsoft Word 2007/2010/2013（.doc, .docx のみ）
- Microsoft Excel 2007/2010/2013（.xls, .xlsx のみ）
- Microsoft PowerPoint 2007/2010/2013（.ppt, .pptx のみ）
- 一太郎 2011/2012/2013（.jtd のみ）
- メモ帳
- ペイント
- Adobe Reader 9/X/XI(ドキュメントの表示のみ)
- Internet Explorer 9/10/11（ページの閲覧のみ）

※アプリケーションの起動・ファイルを開く・閉じる・ファイルの保存・文字の入力といった基本動作以外は、通常時と動作が異なる場合があります。
※上記アプリケーションが標準とは異なる場所にインストールされていると、正常に動作しない場合があります。
※各種アドインがインストールされている環境や、マクロが含まれるファイルの編集・利用時は、正常に動作しない場合があります。
※アドインやマクロの誤動作によって、利用中のファイルが破損・消失する可能性がありますので、適宜バックアップを行うなど、運用にはご注意ください。
※Office2007 以降は 32bit 版での動作確認を行っております。

3.プリンタ・スキャナなどの周辺機器について
モバイルモード中はローカル HDD へのアクセスが制限されるため、プリンタやスキャナ等の周辺機器が正常に動作しない場合があります。

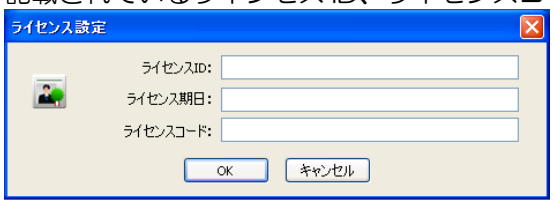
4.モード起動中に強制電源断などの方法でコンピューターの電源を落とした場合
コピーガード機能によってユーザー設定情報等が変更されたままになる場合があります。
原則としては正規の手順でシャットダウンを行っていただくことを強く推奨
いたしますが、予期せぬ問題等により強制的に電源断を行った場合は、
再度モバイルモードの起動をしていただくことで、一時的に書き換えられた
ユーザー設定等が復旧します。

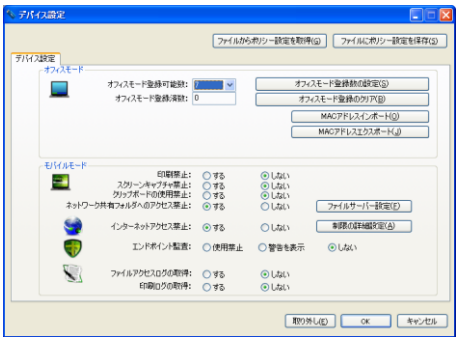
5.Windows8/8.1 の「Windows ストアアプリ」の動作をサポートしていません。
そのため拡張子に関連付けられたアプリケーションが Windows ストアアプリに
設定されている環境ではファイルが実行されません。予め、拡張子の関連付けを
デスクトップアプリケーションに設定してご利用ください。
（PDF の閲覧は、Adobe Reader をご利用ください。）

6.Internet Explorer から Active X コンポーネントのダウンロード、インストール
に失敗する場合があります。
モバイルモード移行前にダウンロード、インストールをお願い致します。

7.モバイルモードではローカル HDD への書込みを行えないようにしていますが、
アプリケーションによっては一時ファイルを書き込めないと不具合が発生する
場合があるため、これを防ぐために、書き込めたように振る舞います。
このため、あたかもファイルが書けたようにみえる場合がありますが、
モバイルモード終了後は、ローカル HDD に作成したファイルが残ることは
ありません。

3 コピーガード機能の運用開始までの流れ

[管理者] 通常 USB メモリ(オフィスモード)で使用する PC の MAC アドレスを収集する。 	通常 USB メモリ(オフィスモード)で使用する PC の MAC アドレスを収集し、ファイルへリスト化します。 **MACアドレス** **11-22-33-44-55-66**
[管理者] SecurityUSB Manager でコピーガード機能を有効にする 	SecurityUSB Manager(別ソフト)でコピーガード機能を有効にします。 
[管理者] IC Manager For Device を起動しライセンス設定を行います。 	IC Manager For Device を起動し、同封されているライセンス ID 用紙に記載されているラインセス ID、ライセンスコードを入力してください。 

[管理者] IC Manager For Device でオフィスモード使用 PC、コピーガード設定を書き込みます。 	IC Manager For Device でオフィスモードコンピュータ、コピーガード設定を書き込みます。   **設定書き込み**
[ユーザ] 対象 USB メモリの運用 	対象 USB メモリを入手し、使用します。コピーガード機能がご使用になれます。 

4 ご使用方法

本章では、本ソフトウェアの使用方法などを説明しております。

ご使用にあたって

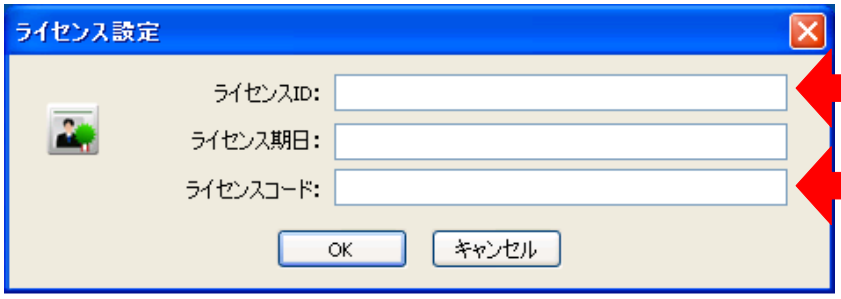
・対象製品を接続した状態でパソコンを起動した場合、これまでに接続したことのある対象 USB メモリであっても新たに認識する表示が出ることがあります。
・対象製品を接続してから認識されるまでに 5 分ほど時間がかかる場合があります。パソコンの再操作が可能になるまでお待ちください。
・パソコンの電源が入った状態で、対象製品をパソコンから取り外す際には、タスクトレイ（通知領域）上で、「ハードウェアの安全な取り外し」を行ってください。無理に取り外しますと、ファイルが消失したり、故障の原因になります。
・消失・破損したデータに関しては、当社は一切の責任を負いません。
・対象製品は、正しい向きでまっすぐ抜き差ししてください。
・本ソフトウェアはスタンバイや休止状態、スリープ状態には対応しておりません。
・対象製品を複数台接続している場合、本ソフトウェアは使用することはできません。

IC Manager For Device のインストール及び起動

SecurityUSB Manager CD-ROM の[SecurityUSB_Manager]内にインストーラファイル：setup.exe があります。
setup.exe を実行し、インストーラに従い PC へ SecurityUSB Manager をインストールしてください。
インストール途中にシリアル番号入力画面が表示されます。同封のシリアル番号用紙に記載されているシリアル番号を入力してください。
インストールが開始され、デスクトップへショートカットができるので実行してください。

ライセンス設定

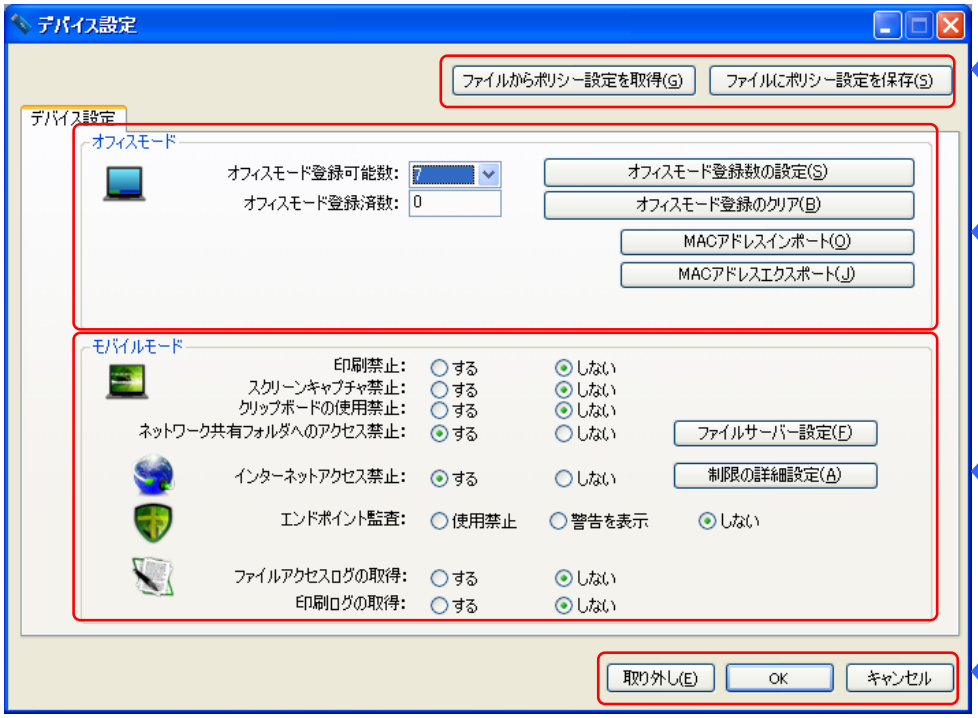
本ソフトウェア起動時にライセンス登録を行う必要があります。同封されているライセンス証書を確認し
ラインセス ID、ライセンスコードを入力してください。
※ライセンス期日には何も入力しないでください。



ライセンスIDとライセンスコードを
入力してください。

メイン画面

本ソフトウェアのメイン画面は以下になります。



現在表示されている設定をファイルに保存します。

通常のUSBとして動作するPCの登録を行います。

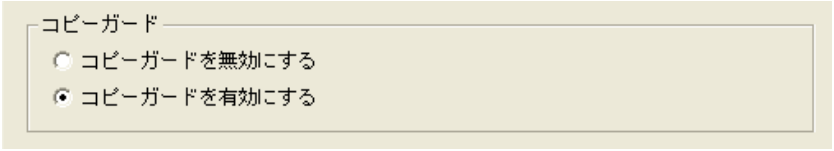
コピーガード有効PC上での制限を設定します。

OKボタンでデバイスへ設定書き込みを行います。

コピーガード設定を行う USB メモリの接続

コピーガード設定を行う USB メモリを接続してください。

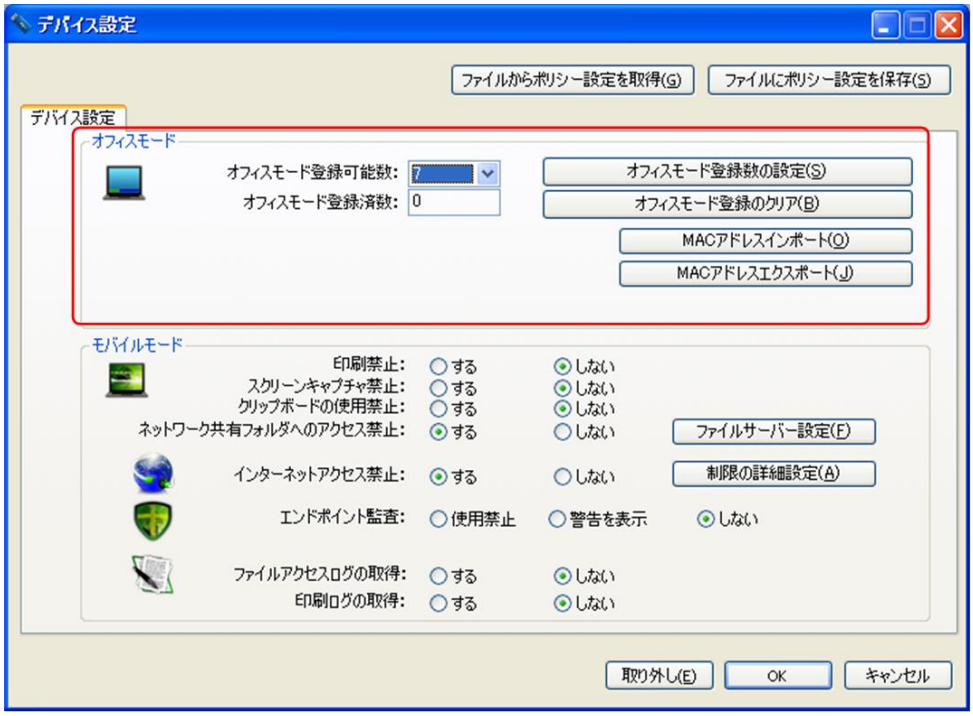
注意；IC Manager For Device でコピーガード設定を行う USB メモリ事前に SecurityUSB Manager でコピーガードを有効にしてください。有効にして無い場合、コピーガード機能は使用できません。
設定方法は SecurityUSB Manager のマニュアルを確認ください。



SecurityUSB Manager の設定項目

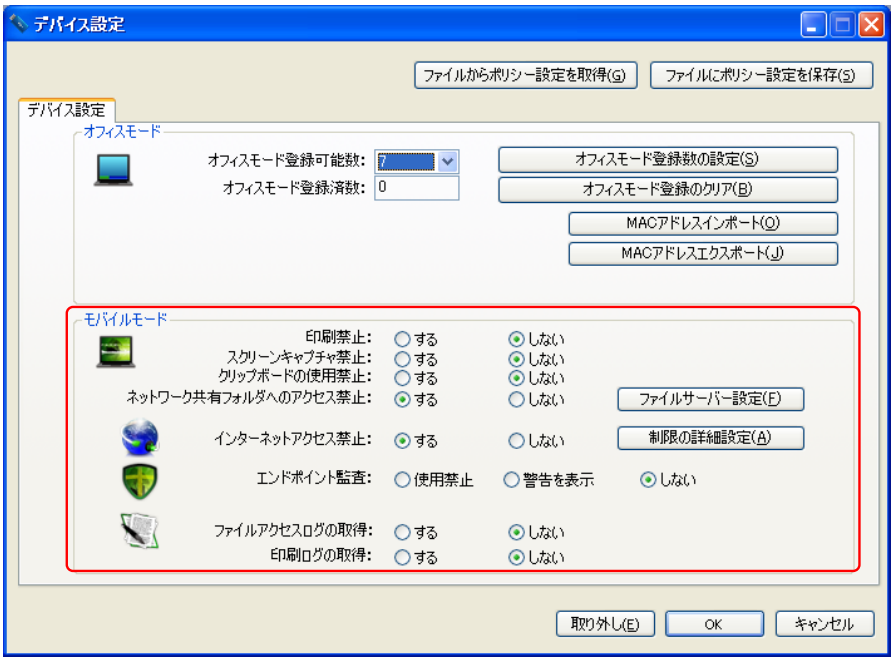
オフィスモード設定

コンピュータに USB メモリを挿入したときに、オフィスモードコンピュータとして動作させる設定を行います。



項目	内容
オフィスモード登録可能数	オフィスモードとして動作させるコンピュータをいくつまで専用 USB メモリに記憶させるか指定します。0～1000 まで入力できます。 登録可能数を入力後は、必ず「オフィスモード登録数の設定」ボタンをクリックしてください
オフィスモード登録数	現在専用 USB メモリに登録されているオフィスモードとして動作するコンピュータの数が表示されます。（変更不可） 登録済みのオフィスモードコンピュータをクリアするときは、「オフィスモード登録のクリア」ボタンをクリックしてください。
MAC アドレスインポート	オフィスモードで動作さえるコンピュータを登録します。 コンピュータは MAC アドレスで登録します。 インポートファイルフォーマットは CSV ファイル形式で MAC アドレスの列挙をしてください。 例： 11.22.33.44.55.66 22.33.44.55.66.77 33.44.55.66.77.88 MAC アドレスは「ピリオド」区切りで指定してください。 Windows の ipconfig コマンドでは、「ハイフン」区切りで表示されますので注意してください。
MAC アドレスエクスポート	USB メモリに登録されているコンピュータの MAC アドレスを出力します。画面の指示に沿ってファイルに保存してください。

モバイルモード設定



モバイルモード項目ではコピーガード機能を有効にした PC での動作設定を行うことが可能です。
USB メモリへ設定できるポリシーは以下になります。

設定項目	説明		デフォルト値
印刷禁止	印刷を禁止するか選択します。禁止するときは、「する」を選択します		する
スクリーンキャプチャ禁止	スクリーンキャプチャを禁止するか選択します。禁止するときは、「する」を選択します。		する
クリップボードの使用禁止	クリップボードの使用を禁止するか選択します。禁止するときは、「する」を選択します。		しない
ネットワーク共有フォルダへのアクセス禁止	ファイルサーバー、NAS 等のネットワーク共有フォルダへのアクセスを禁止するか選択します。禁止するときは、「する」を選択します。 ネットワーク共有フォルダの暗号化・復号化を行うときは、「ファイルサーバーの設定」ボタンをクリックして個別に設定してください。		する
インターネットアクセス禁止	インターネットのアクセスを禁止するか選択します。インターネットのアクセスを禁止するときは、「する」を選択します。 インターネットのアクセスを禁止を「する」に設定したとき、「制限の詳細設定」で設定されるドメインのみアクセスを許可することができます。		する
エンドポイント監査	USB メモリが挿入されたコンピュータのウイルス対策ソフトの状態・リムバブルメディアの自動再生設定状態を監査します。 ウイルス対策ソフトの状態は、Windows のセキュリティセンターおよびアクションセンターの情報を参照しています。 ※セキュリティセンター・アクションセンターの情報は、WMI の「root¥SecurityCenter」および「root¥SecurityCenter2」から情報を取得しています。 ※ SSO オプションを利用しているコンピュータでは利用できません。		警告を表示
	使用禁止	ウイルス対策ソフトが最新の状態で動作していないときは、USB メモリは利用できません。	
	警告を表示	ウイルス対策ソフトが最新の状態で動作していないと警告のみ表示します。	
	しない	エンドポイント監査をしません。	
ファイルアクセルログの取得	USB メモリ内のファイルアクセスのログを保存するか設定します。 ログを保存する場合は「する」を選択します。		しない
印刷ログの取得	USB メモリ内のファイルの印刷を実行した時のログを保存するか設定します。ログを保存する場合は「する」を選択します。		しない

■ファイルアクセスログ/印刷ログについて

モバイルモードの設定によってファイルアクセスログ、印刷ログを取得することができます。
不正アクセス防止に使用することができます。以下に各ログについて説明致します。

項目	内容
ログファイル保存場所	セキュリティ USB のリムーバブルディスク領域(パスワードロック) 内の「a1fd5b43.$$$」フォルダ下に保存されます a1fd5b43.$$$ 　　|-iss_log_host 	|- 0000000000000000 	|- 0000000000000001 　　|-iss_log_print 　　|- 0000000000000000 　　|- 0000000000000001 iss_log_host：ファイルアクセスログ格納フォルダ iss_log_print：印刷ログ格納フォルダ
ファイルアクセスログ	コピーガード機能を有効時に取得できるファイルアクセスログです。 **ファイル形式**：XML **ファイル名**； 0000000000000000/0000000000000001/0000000000000002... セキュリティ USB 内のファイルにアクセスする度にログを残します。 詳細なログ内容については次ページを確認ください。
印刷ログ	コピーガード機能を有効時に取得できる印刷ログです。 **ファイル形式**：XML **ファイル名**； 0000000000000000/0000000000000001/0000000000000002... セキュリティ USB 内のファイルを印刷する度にログを残します。 詳細なログ内容については次ページを確認ください。
保存されたログへのアクセス権	セキュリティ USB 内へ保存されているログはアクセス制限が掛かっており、ユーザーは保存されているログの読み書き、削除することができません。 ログの中身を確認するためには SecurtyUSB Manager の [デバイス内のログ収集]機能を使用してログを収集してください。 注意；セキュリティ USB によって製品の初期化を行うとログを削除されてしまいます。ユーザーにログを消されたくない場合は SecurityUSB Manager によってデバイスの初期化機能を無効にしてください。

■ファイルアクセスログ内容

項目	内容
time	ファイルアクセスが行われた時間(エポック時間)
localtime	ファイルアクセスが行われた時間(ローカル時間)
process	ファイルへアクセスを行ったプロセス名
function	ファイルへ行った処理 ・Open：ファイルを開く ・Create：ファイルを作成 ・Access:：ファイルをアクセス ・Copy：ファイルをコピー ・Move：ファイルを移動 ・Execute：ファイルを実行 ・Delete：ファイルを削除
target	ファイル操作元のファイルパス/ファイル名
destination	ファイルコピー、移動などを行った際のコピー・移動先ファイルパス/ファイル名
serverSource※1	転送元サーバー名
serverDest※1	転送先サーバー名
flagSourceFile※1	転送元にファイル名が存在する場合「1」が記載。
flagDestFile※1	転送先にファイル名が存在する場合「1」が記載。
deviceID	製品の USB シリアル番号
loginName	PC のログインユーザ名
uniqID	ID 番号。1 ログ毎に異なる番号が割り当てられます。
fileByte	アクセスしたファイルのファイルサイズ[byte]
vendorID	PC に他の USB メモリから取得するベンダーID
productID	PC に他の USB メモリから取得するプロダクト D
deviceType	PC に他の USB メモリから取得するデバイスタイプ
Dup	弊社管理情報
userID	
fingerNumber	
ipAddress	
macAddress	
HostID	
operationMode	
accessType	

※1：ファイル操作対象がネットワークドライブにある場合に記載されます。

■印刷ログ内容

項目	内容
Time	ファイル印刷が行われた時間(エポック時間)
localtime	ファイル印刷が行われた時間(ローカル時間)
process	ファイル印刷を行ったプロセス名
function	“print”固定
target	印刷されたファイルのファイルパス/ファイル名
destination	プリンタ名
Dup	印刷枚数
loginName	PC のログインユーザ名
deviceID	製品の USB シリアル番号
uniqID	ID 番号。1 ログ毎に異なる番号が割り当てられます。
HostID	弊社管理情報
userID	
fingerNumber	
operationMode	
vendorID	本項目は記録されません。
productID	
deviceType	
AccessType	
serverDest	

■ファイルサーバの設定

ネットワーク共有フォルダの暗号化あるいは、アクセス禁止のときの例外設定を行います。「ファイルサーバー設定」ボタンをクリックすると、ファイルサーバー設定画面が表示されます

新規に、ネットワーク共有フォルダの設定を追加するときは、「追加」ボタンをクリックして次の項目を入力します。

設定項目	説明
アドレス（必須）	ネットワーク共有フォルダを指定します。 書式は必ず、「¥¥ファイルサーバーアドレス¥共有フォルダ名」で指定してください。
コメント	一覧画面でわかりやすいようにコメントを入力します。
暗号化	暗号化するかどうか選択します。暗号化するときは、「する」を選択します。
アクセスユーザー名	ファイルサーバーへアクセスするためのユーザー名を指定します。
パスワード	ファイルサーバーへアクセスするためのユーザーに設定されているパスワードを指定します。

ネットワーク共有フォルダへのアクセスが禁止されているときでも、ここで設定されている共有フォルダにはアクセス可能となります。

■制限の詳細設定

インターネットアクセスが禁止されているときの、例外設定を行います。

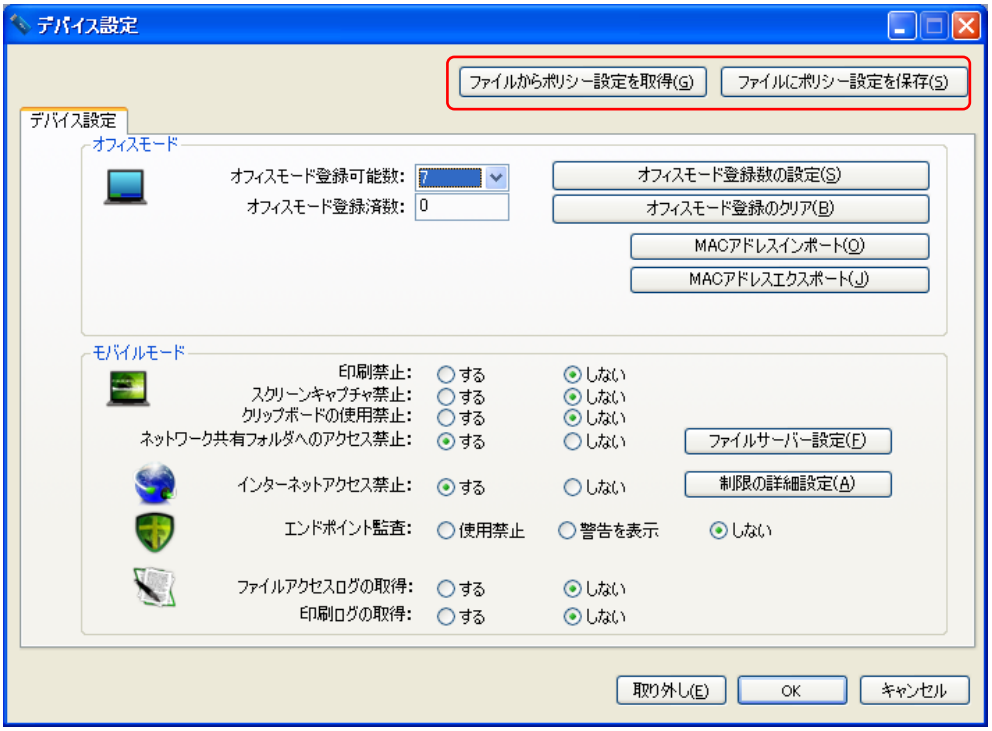
「制限の詳細設定」ボタンをクリックすると、インターネットアクセス制限の詳細設定画面が表示されます。

新規に、インターネットアドレスの設定を追加するときは、「追加」ボタンをクリックして次の項目を入力します。

設定項目	説明
FQDN/IP アドレス（必須	ドメイン名あるいはドメインの IP アドレスを指定します。 例）intelligent.jp 「http://www.hagisol.co.jp/」を指定しても有効に働きません。サブドメイン名などは入力しないでください。同様に URL などを指定しても有効に働きません。
ポート番号	ポート番号を指定するときは、許可するポート番号を指定してください。 入力がないときは、すべてのポートに対してアクセス可能となります。

モバイルモード　ポリシー設定の管理

モバイルモード項目で設定したポリシーの保存、保存されたポリシーの取得について説明します。
複数の専用 USB メモリに同じ設定を行うときなどに、設定情報をファイルに保存しておくと便利です。



■ファイルに設定を保存

現在表示されている内容をファイルに保存します。
[ファイルにポリシー設定を保存]ボタンを押し、画面の指示に沿ってファイルに保存してください。

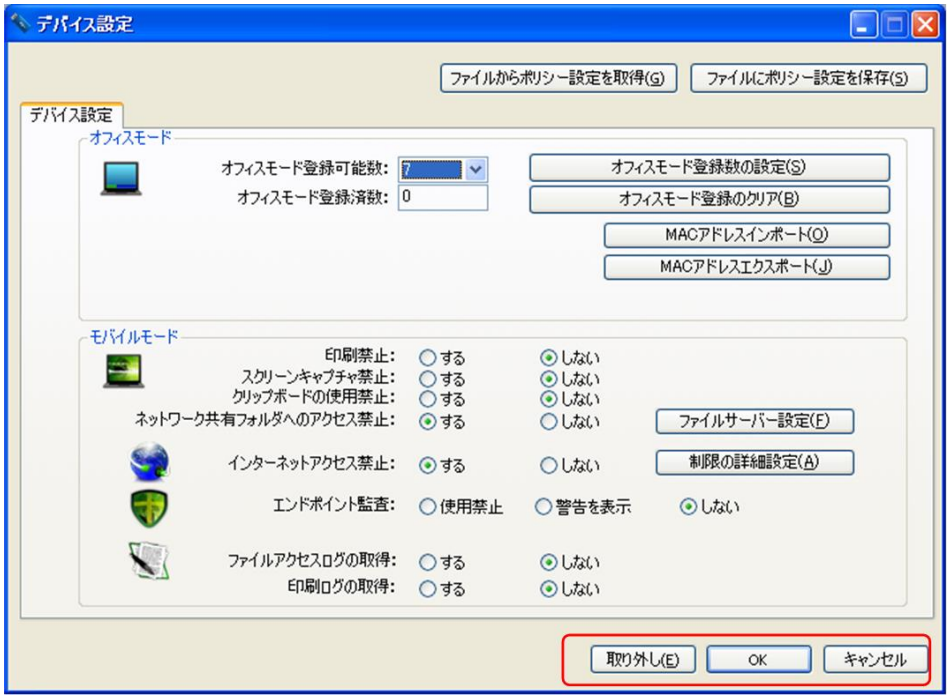
■ファイルから設定を取得

ファイルに設定してある情報を読み込むときに利用します。
[ファイルからポリシー設定を取得]ボタンを押し、画面の指示に沿ってファイルを読み込んでください。

ファイルの読み込みは専用 USB メモリ 1 本 1 本実施してください。専用 USB メモリを変更すると
初回は、専用 USB メモリ内の情報を表示します。

USB メモリへの設定書き込み

オフィスモード設定、モバイルモード設定項目で設定した内容を USB メモリへ書き込みます。
各種設定後、[OK]ボタンを押してください。



ウイルス対策ソフトとの共存について

ウイルス対策ソフトとの共存についての注意事項を説明します。

※各ソフトウェアで有効なライセンスをお持ちで、最新のものを利用されていることを前提としています。
※いずれの製品もデフォルト設定の状態で確認しています。

■利用開始時にメッセージが表示される、あるいは例外設定が必要なもの

メーカー	ソフトウェア名	表示されるメッセージ/設定など	32bit 版で確認済みバージョン	64bit 版で確認済みバージョン
F-Secure	エフセキュア インターネットセキュリティ	こちらを参照	2011/2012	2011/2012
Kingsoft	Kingsoft Internet Security	こちらを参照	2011	2011
AVG	AVG インターネットセキュリティ	こちらを参照	2011/2012	2011/2012

各ソフトウェアの「表示されるメッセージ/設定など」を参照して適切に操作してください。

■メッセージなどの表示はなく、そのまま利用できるもの

メーカー	ソフトウェア名	32bit 版で確認済みバージョン	64bit 版で確認済みバージョン
トレンドマイクロ	ウイルスバスター	2010※1/2011/2012	2010/2011/2012
シマンテック	ノートン インターネットセキュリティ	2011/2012	2011/2012
マカフィー	インターネットセキュリティ/ トータルセキュリティ	2011/2012	2011/2012
ESET	ESET Smart Security	4.2	4.2
ソースネクスト	ウイルスセキュリティ ZERO	2011/5	2011/5
カスペルスキー	Kaspersky Internet Security	2011/2012	2011/2012
G DATA	G DATA　インターネットセキュリティ	2011/2012※2	2011/2012※2
マイクロソフト	Microsoft Security Essentials	2011/5_	2011/5
Avira	Avira Premium Security Suite	2011/5	2011/5
Avast	Avast! インターネットセキュリティ	2011/5_	2011/5
BitDefender	BitDefender インターネットセキュリティ	2011	2011

※1 必ず最新のものにアップデートしてください。一度もアップデートされていない環境では、起動できない場合があります。
※2 モバイルモード時、HDD ドライブもエクスプローラー上に表示されますがファイルの読み込み、書き込みはできません。

法人向けの対策ソフトについては、上記製品を参考にして管理者の方が検証および例外設定してください。
それぞれの例外設定方法などは、各製品のマニュアルあるいは各メーカーにお問い合わせください。

エフセキュア クライアント セキュリティ/インターネット セキュリティ

専用 USB メモリ起動時に、次の設定をします。

■2011 の場合

2 種類の画面が表示されます。

システム変更の試行画面では、「プログラムを信頼しています。プログラムを許可します。」を選択して、「OK」ボタンをクリックします。
新しいサーバーアプリケーション画面では、「今後、このプログラムでこのダイアログを表示しない」をチェックして、「許可」ボタンをクリックします。

2012 の場合

以下の画面が表示されます。

システム変更の試行画面では、「プログラムを信頼しています。プログラムを許可します。」を選択して、「OK」ボタンをクリックします。

※エフセキュア　クライアント　セキュリティの使用方法は、エフセキュア　クライアント　セキュリティの説明書をご覧ください

Kingsoft Internet Security

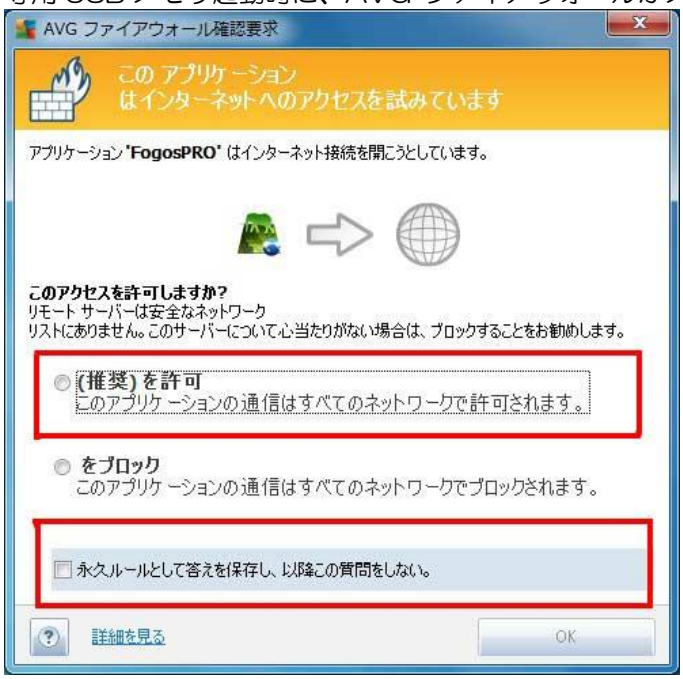
専用 USB メモリ起動時に、PersonalFirewall がメッセージを表示します。

「いつでも許可」を選択して、「信用認証したプログラムのアクセスをいつも許可」にチェックをいれて「OK」ボタンをクリックします。

※Kingsoft Internet Security の使用方法は、Kingsoft Internet Security の説明書をご覧ください

AVG インターネットセキュリティ

専用 USB メモリ起動時に、AVG ファイアウォールがメッセージを表示します。



アプリケーションが「FogosPRO」とあるとき、「(推奨)を許可」を選択し、「永久ルールとして答えを保存し、以降この質問をしない」にチェックを入れて「OK」ボタンをクリックします。

※AVG Internet Security の使用方法は、AVG Internet Security の説明書をご覧ください

5 サポート・メンテナンス・ライセンス

お問い合わせ窓口

ご連絡先		受付
サポートセンター※	TEL：0570-080-900	10:00～19:00 （年中無休）

※内容を正確に把握するため、通話を録音させていただいております。個人情報に関する保護方針はホームページをご参照ください。ハギワラソリューションズ株式会社ホームページ：http://www.hagisol.co.jp

ナビダイヤルについて

弊社ではサービスサポートお問い合わせ窓口にナビダイヤルを採用しています。
全国の固定電話から1分間10円の通話料（発信者のご負担）でご利用いただける「全国統一番号」で、NTTコミュニケーションズ（株）が提供するサービスのひとつです。
ダイヤルQ2などの有料サービスではなく、ナビダイヤル通話料から弊社が利益を得るシステムではありません。
※携帯電話からは20秒10円の通話料でご利用いただけます。※PHS・一部のIP電話からはご利用いただけません。
※お待ちいただいている間も通話料がかかりますので、混雑時はしばらくたってからおかけ直しください。

コピーガード設定ソフト
IC Manager For Device
マニュアル
2019 年 1 月