

InfoCage モバイル防御 インストールガイド

InfoCage モバイル防御 Version 3.62 インストールガイド

はじめに

このたびは、NECのInfoCage モバイル防御をお買い求めいただき誠にありがとうございます。InfoCage モバイル防御は、 パソコンからの情報漏洩を防止するセキュリティソフトウェアです。 ご使用になる前に本書をよくお読みになり、製品の取り扱いを十分にご理解ください。

● 商標について

- ・Microsoft および Windows は米国 Microsoft Corporationの米国およびその他の国における登録商標または商標です。
- ・ InfoCage は日本電気株式会社の登録商標です。
- ・その他、本マニュアルに記載されている会社名、商品名は各社の商標または登録商標です。
- ・このマニュアルの一部、又は全部を流用・複写することはできません。
- ・本マニュアル中のサンプル画面で使用している名称は、すべて架空のものです。実在する品名、団体名、個人 名とは一切関係ありません。

● 免責事項

本書及び本システムは、ライセンス契約に基づいて使用することができます。ライセンス契約で明示的に定められて いないかぎり、日本電気株式会社は製品、及びその関連文書について、明示的にも暗黙的にも、商品性に関する 保証、特定目的への適合性に関する保証、取り扱い、使用、または取引行為に伴う保証について一切の責任を負 いません。

本書について

本書は、InfoCage モバイル防御を導入する手順を記載しています。InfoCage モバイル防御を導入する際に ご利用ください。

また本ソフトウェアの使用に関する注意点などを記載している「2.2 注意事項」は必ずお読みください。 セットアップが完了した後は、『InfoCage モバイル防御 ユーザーズガイド』を参照してください。

本文中の記号について

本文中では、説明、操作手順の他に以下の記号を利用しています。これらの記号の意味を正しくご理解になり、本書をお読みください。

項目	説明	
▲ Notice	システムの取り扱いで守らなければならない事柄や特に注意すべき点、確認す べき点を説明します。	
参照	関連する内容が記載されているページを紹介しています。	

用語の定義

本書では、システム操作の説明に以下のような用語を用いています。 本書を確認するにあたって前提としてご理解ください。

項目	説明
InfoCage モバイル防御	パソコンからの情報漏洩を防止するため、認証を受けていない人がそのパソ コンを使うことを防止したり、データを暗号化して読めないようにしたりするこ とができる情報漏洩対策セキュリティソフトウェアです。
暗号化	第三者の解読・利用を防ぐために、デジタル情報を組み替えることです。組 み替えの際に用いられる特定の情報を「鍵」と呼びます。InfoCage モバイル 防御はパソコンのドライブまたはフォルダを暗号化します。 メディア鍵認証方式では、鍵または合鍵などがパソコンに装着された状態、 またはネットワーク鍵にアクセスできる状態のいずれかでなければ、暗号化 されたハードディスクドライブの中を閲覧することはできません。 パスワード認証方式では、ユーザパスワードを認証しない限り、暗号化され たハードディスクドライブの中を閲覧することはできません。 ただし、Windows へのログオンは、InfoCage モバイル防御以外の認証方法 と併用することも可能です。
復号	暗号化したファイルを元に戻すことです。
セキュリティ認証	パソコンを操作可能な状態にする際に、アクセスする権利があるかどうかを確認することです。セキュリティ認証を行うと、Windows ヘログオンしてパソコンを操作できるようになります。これによって、パソコンの不正利用やなりすまし利用を防止します。セキュリティ認証が行われないとパソコンはロックされた状態のため、パソコン内の暗号化されたデータは読み取ることができません。
InfoCage モバイル防御ユ ーティリティ	InfoCage モバイル防御を使ってパソコンの保護設定を行うためのアプリケ ーションです。InfoCage モバイル防御をパソコンにインストールして使用し ます。この InfoCage モバイル防御ユーティリティを起動して、パソコンの保 護設定やパスワードの変更、鍵の作成(メディア鍵認証方式)の操作を行い ます。
メディア鍵認証方式/ パスワード認証方式	InfoCage モバイル防御の運用方式です。 インストールの際に、外部メディアを鍵としてパソコンの認証を行うメディア鍵 認証方式か、またはパスワードにてパソコンの認証を行うパスワード認証方 式を選択します。

項目	説明
スーパーバイザパスワード /ユーザパスワード	InfoCage モバイル防御ユーティリティ起動時などに必要なパスワードです。 メディア鍵認証方式で運用する場合はスーパーバイザパスワードを、パスワ ード認証方式で運用する場合はユーザパスワードを使用します。
管理者	InfoCage モバイル防御の管理者をさします。InfoCage モバイル防御のセッ トアッププログラムのカスタマイズを行います。
クライアント	InfoCage モバイル防御のシステム上で管理者が管理を行うパソコンをさします。
利用者	クライアントを利用する人をさします。
保護対象	暗号化によりデータを保護するパソコンの内蔵ドライブをさします。鍵を作成 する際に設定します。(メディア鍵認証方式)
メディア暗号ユーティリティ	USBメモリなどのメディアの中に暗号化したファイルを保存し、これらのファイ ルを InfoCage モバイル防御のインストールされていないパソコンで復号し、 使用するためのユーティリティです。
外部メディア自動暗号	許可された外部メディア(許可外部メディア)へ書き出すときに自動的に暗 号化を行う機能です。許可外部メディアは、同じグループ名とキーワードが 設定されているパソコンでのみデータを読み書き可能で、許可されていない メディアや他のグループのパソコンではデータの読み書きはできません。
外部メディア	OSがリムーバブルメディアと認識するメディア、フロッピーディスクおよび許可 外部メディアのことをさします。
許可外部メディア	外部メディア自動暗号機能によりグループ内で使用が許可されたメディア (CD-R/RW、DVD-R/+R/RW/RAM は対象外)をさします。

目 次

第1章	InfoCage モバイル防御について	1
1.1	InfoCage モバイル防御の特徴	2
1.2	鍵とは	5
1.3	鍵情報とは	
1.4	運用モード	6
1.5	初期暗号化モード	7
第2章	インストールの前にお読みください	8
2.1	インストールの流れ	
2.2	注意事項	9
2.3	【導入前の注意事項】確認チェックシート	
第3章	インストール	17
3.1	インストールの前に	
3.2	パソコンの環境チェック	
3.2.1	環境チェックユーティリティ	
3.2.2	SYSTEMアカウントの変更方法	
3.3	Step1	
3.4	Windows ヘログオン	
3.5	Step2	
3.5.1	メディア鍵認証方式の場合	
3.5.2	パスワード認証方式の場合	
第4章	個別暗号モードインストール	
4.1	メディア鍵認証方式の場合	
4.2	パスワード認証方式の場合	
第5章	アップグレードインストール	54
第6章	ログオン方法	60
6.1	メディア鍵認証方式の場合	
6.2	パスワード認証方式の場合	
第7章	特定のFeliCaカードの設定	67
第8章	ユーティリティの起動方法	68
第9章	時限消去機能について	69
第 10 章	セキュリティチップ(TPM)搭載のパソコンをお使いの場合	70
第 11 章	トラブルシューティング	71

第1章 InfoCage モバイル防御について

InfoCage モバイル防御は、パソコンからの情報漏洩を防止するため、認証を受けていない人がそのパソコンを使う ことを防止したり、データを暗号化して読めないようにしたりすることができる情報漏洩対策セキュリティソフトウェアです。 InfoCage モバイル防御では、インストール時にパソコンを使用する人を認証する「鍵」の作成、または「パスワード」の 設定を行い、保護が必要なドライブまたはフォルダの暗号化を行います。

本インストールガイドにしたがってそれぞれ設定を行ってください。

インストール後はパソコンを再起動する必要があります。他のプログラムを実行中の場合は、終了させてからインストール してください。

🛕 Notice

InfoCage モバイル防御には、メディア鍵でセキュリティ認証を行う「メディア鍵認証方式」と、パスワードでセキュリティ認証 を行う「パスワード認証方式」があります。

「メディア鍵認証方式」と「パスワード認証方式」の併用はできません。

1.1 InfoCage モバイル防御の特徴

InfoCage モバイル防御は、以下の機能で情報を強固に保護します。





● パソコンのロック

メディア鍵認証方式の場合

鍵となるメディア等をパソコンから抜くことでパソコンをロックし、操作ができないようにします。 また、鍵をパソコンに装着することでセキュリティ認証が行われ、パソコンのロックを解除できます。



パスワード認証方式の場合

InfoCage モバイル防御のユーザパスワードが正しく入力された場合にセキュリティ認証が行われ、 Windows にログオン可能になります。

また FeliCa カードで認証することもできます。(WindowsXP/2000のみ)



※ Windows へのログオンは、InfoCage モバイル防御以外の認証方法と併用することも可能です。

● ドライブ、フォルダの暗号化

InfoCage モバイル防御は、ドライブおよびフォルダ単位で一括して内蔵ドライブ内のデータの暗号化を 行います。セキュリティ認証が行われないとパソコン内のデータは暗号化されたままのため、読み取ることが できません。

メディア鍵認証方式の場合

鍵となるメディアが装着された場合にセキュリティ認証が行われ、暗号化されたファイルへアクセスが可能になります。

パスワード認証方式の場合

パスワードを正しく入力した場合にセキュリティ認証が行われ、暗号化されたファイルへアクセスが可能になります。



※ Windows へのログオンは、InfoCage モバイル防御以外の認証方法と併用することも可能です。

● 外部メディア自動暗号 (InfoCage モバイル防御の管理者による設定が必要)

外部メディア内のデータの暗号化を自動的に行います。所属するグループ内でのみ使用が許可される 外部メディア(許可外部メディア)を設定し、この許可外部メディアへはデータは自動的に暗号化されて 書き込まれ、読み込むときには自動的に復号されます。







● セキュリティチップ(TPM)でのセキュリティ強化 (InfoCage モバイル防御の管理者による設定が必要)

InfoCage モバイル防御をパスワード認証方式で運用し、セキュリティチップ(TPM)搭載のパソコンを お使いの場合、セキュリティチップ(TPM)と連携し、より強固なセキュリティを実現します。 (WindowsXPのパスワード認証方式のみ)

1.2 鍵とは

InfoCage モバイル防御 メディア鍵認証方式で使用する鍵には以下の3種類があります。

●鍵

鍵とは、パソコンにログオンする際や暗号化されたデータにアクセスする際などに必要な認証情報をメディア等に 作成したものです。

鍵がなければドアが開かないのと同様に、鍵として設定したメディアがなければ、セキュリティ認証が行われず、 パソコンの情報にアクセスできません。

鍵はメディアやネットワークの共有フォルダに作成できます。



● 合鍵

合鍵とは、スペアキーのことです。

万が一の鍵の紛失等に備えて、パソコンの保護対象ごとに1つの鍵に対して合鍵を2つまで作成できます。 鍵または合鍵のうちどれか1つで、パソコンやメディアの保護と解除ができます。



合成鍵(WindowsXP/2000のみ)

異なるメディアに作成した鍵を2つ組み合わせて使用するダブルロックキーのことです。 組み合わせることができるのは2つまでです。 鍵が2つそろわなければパソコンや外部メディアの保護を解除できません。



1.3 鍵情報とは

鍵のバックアップデータを鍵情報といい、鍵となるメディアとは別のメディアに保存しておきます。 鍵となるメディア内のデータを紛失した場合等は、鍵情報を元に鍵を復旧します。



🛕 Notice

鍵情報を紛失すると鍵の復旧ができません。鍵情報を保存したメディア内のデータを絶対に紛失しないように注意してく ださい。

1.4 運用モード

運用モードには、クライアント単体で運用するスタンドアローンモードと、InfoCage モバイル防御の管理者が InfoCage モ バイル防御サーバを使ってクライアントの設定などを管理するネットワークモードがあります。 インストール後に運用モードを変更する場合は、運用モード設定ユーティリティを使います。

● スタンドアローンモード

クライアント単体で運用します。



● ネットワークモード

スタンドアローンモードの機能に加え、InfoCage モバイル防御サーバと連携する運用モードです。 InfoCage モバイル防御の管理者が InfoCage モバイル防御サーバにてユーザ登録やポリシー設定を行い、クライ アントの管理などを行います。



初期暗号化モード 1.5

InfoCage モバイル防御をインストールした後に実行される暗号化は、通常は「ドライブー括暗号モード」によりドライブ 単位で行われます。

ただし、InfoCage モバイル防御の管理者により「個別暗号モード」に設定されている場合は、指定したドライブおよび フォルダのみ暗号化を行います。

インストールする InfoCage モバイル防御の初期暗号化モードをあらかじめ InfoCage モバイル防御の管理者に確認して ください。

● **ドライブー括暗号モード** (デフォルト)



ドライブ単位で暗号化

● 個別暗号モード



指定したドライブ・フォルダを暗号化



InfoCage モバイル防御は以下の流れでインストールします。



🛕 Notice

InfoCage モバイル防御の管理者によってセットアッププログラムがカスタマイズされた場合は、上記の手順と異なる場合があります。

2.2 注意事項

● お願い

- インストールを行う前に、「2.3【導入前の注意事項】確認チェックシート」を使用して、インストール環境の確認 を行ってください。
- 万が一に備え、大切なデータはバックアップを取ってから使用してください。

● 動作環境

オペレーティングシステム (*1)(*2)	システムメモリ	ハードディスクの空き容量 (インストール時)	
Windows Vista Ultimate		本製品のインストールドライブには 50MB 以上の空き容量が必要です	
Windows Vista Business	IGD KL	インストールの際にはセットアップ情報	
Windows Vista Home Basic	512MB 以上	を展開するために、さらに 30MB 以上の 空き容量が必要です。	
Windows XP Professional			
Windows XP Home Edition		本製品のインストールドライブには 50MB以上の空き容量が必要です。 インストールの際にはセットアップ情報	
Windows XP Tablet PC Edition	128MB以上		
Windows XP Tablet PC Edition 2005		を展開するために、さらに 20MB 以上の 空き容量が必要です。	
Windows 2000 Professional			
ハードディスクの空き容量(暗号化時)			
暗号化する際には、以下の空き容量が必要です。 必要な空き容量 = 暗号化対象ファイルの中で最大のファイルと同等の容量 + (ドライブ容量×0.02)			

必要な空き容量 = 暗号化対象ファイルの中で最大のファイルと同等の容量 + (ドライブ容量×0.02) (上記は最低限必要な容量です。暗号化処理は十分な空き容量がある状態で行ってください。) メディア鍵認証方式の場合、初めて暗号化処理を行う場合は、保護対象に指定したドライブのごみ箱を暗 号化するため、暗号化指定していないドライブにも上記の空き容量が必要となりますのでご注意ください。

(*1) 32bit 版の日本語オペレーティングシステムをサポートしています。

(*2) Microsoft 社から提供される最新セキュリティパッチの適用をお奨めします。

● インストール前の注意事項

- InfoCage モバイル防御をWindows XPまたはWindows2000で使用している場合、Windows Vista用のセット アッププログラムを使用してアップグレードインストールすることはできません。また、その逆も同様です。
- ・ InfoCage モバイル防御と共存できないアプリケーションと併用すると、正しく動作しない場合があります。イン ストール前に「アプリケーション競合問題について」を必ず確認してください。
- インストールは、コンピュータの管理者権限を持つユーザで、日本語または英語以外の文字を含まないユー ザ名で行ってください。
 InfoCage モバイル防御 ユーティリティの操作もコンピュータの管理者で行ってください。
 また、Windows XPの[別のユーザとして実行]機能、Windows Vistaの[管理者として実行]機能は、使用しないでください。
- Windows Vista の場合、インストールの前にユーザアカウント制御(UAC)は有効にしてください。
 ユーザアカウント制御(UAC)の設定は、コントロールパネルの[ユーザアカウントの変更]より[ユーザアカウント制御の有効化または無効化]で行います。
 また、インストール後もユーザアカウント制御(UAC)は常に有効にしてください。

- ・プロダクト ID はライセンス証書に記載されています。
- ・NTFS ファイルシステムの暗号化、または圧縮されたファイルは InfoCage モバイル防御では暗号化できない ため、NTFS ファイルシステムの暗号化、または圧縮している場合は、InfoCage モバイル防御をインストール する前に解除してください。
- 仮想ドライブの割り当ては行わないでください。
 (SUBSTコマンドおよび MOUNTVOLコマンドを使用、または[コンピュータの管理]-[ディスクの管理]でドラ イブ文字またはパスの変更より[次の空の NTFS フォルダにマウントする]を使用など)
- ・ InfoCage モバイル防御をインストール後は、コントロールパネル等からユーザのログオンやログオフの方法を 変更することができなくなります。セキュリティ強化のため、[Ctrl+Alt+Del]キーを押下する画面を表示するよう に設定を変更する場合は、インストール前に設定変更してください。

● インストール後の注意事項

- ・スーパーバイザパスワード/ユーザパスワードは、InfoCage モバイル防御 ユーティリティの起動時、鍵の復 旧時、アンインストール時に必要になりますので、絶対に忘れないように注意してください。
- ・ InfoCage モバイル防御を正常にインストールした後に同じバージョンの setup.exe を実行すると、アンインスト ールのウィザードが起動しますので実行しないでください。
- Windows XP/2000の場合、InfoCage モバイル防御の管理者の設定によっては、InfoCage モバイル防御を インストール後、Windowsのセーフモードでの起動ができなくなる場合があります。
- Windows XP に InfoCage モバイル防御をインストールすると、OS 標準のバックアップ機能が使用できなくなります。バックアップを行う場合は、InfoCage モバイル防御のインストールフォルダ(通常は ¥Program Files¥NEC¥InfoCageCE)内の ¥tools¥MPBackup.exe を使用してバックアップを行ってください。操作方法については、「InfoCage モバイル防御 ユーザーズガイド」の「バックアップツールの利用」の項を参照してください。
- Windows XP に InfoCage モバイル防御をインストールすると、ユーザ選択画面が表示されなくなり、[簡易ユ ーザ切り替え]ができなくなります。また、シャットダウン時の画面が[コンピュータの電源を切る](ボタン選択) 画面から、[Windows のシャットダウン](プルダウンメニュー選択)画面に変更されます。また、[Windows へよ うこそ]画面が通常のログオン画面に変更されます。
- InfoCage モバイル防御インストール後は ファイルシステムの変更(FAT および FAT32 からNTFS へのコンバート)は行えません。コンバートを行う場合は、いったん InfoCage モバイル防御をアンインストールしてから行ってください。
- InfoCage モバイル防御インストール後は、OSの再インストールおよびリカバリ、または内蔵ハードディスクの フォーマットは行わないでください。これらを行う場合は、いったん InfoCage モバイル防御をアンインストール してから行ってください。
- ・Windows XP/2000にInfoCage モバイル防御をインストールすると、OS標準の[システムの復元]が使用できなくなります。
- Windows Vista標準の[バックアップと復元センター]でバックアップを行う場合は、ファイルとフォルダのバック アップのみ行ってください。[Windows Complete PC バックアップ]は復元前と復元後で鍵やユーザパスワード が異なると、Windows へのログオンやファイルの参照ができなくなりますので使用しないでください。

● 暗号化について

- ・暗号化を実行する前に、常駐プログラムを含むすべてのアプリケーションを必ず終了させてください。アプリケ ーションが使用しているファイルは、暗号化できない場合があります。
- ・暗号化や暗号化解除(復号)を行う場合、暗号化/復号処理の途中で、強制終了、Windowsのロック、スクリ ーンセーバの設定の変更を行うとファイルが不正になりますので、絶対に行わないでください。
- ・以下の操作を行うとデータを正しく参照できなくなりますので、絶対に行わないでください。OS にログオンでき なくなった場合などでデータを退避させたい場合でも、何も操作を行わず速やかに InfoCage モバイル防御 製品保守担当までご相談ください。
 - * 暗号化したハードディスクを別のパソコンに接続し、データを移動する
 - * セーフモードで起動し、暗号化したハードディスクから別のドライブにデータを移動する
 - * Windows Vista 用の InfoCage モバイル防御 ユーティリティで暗号化したハードディスクドライブを、 Windows XP/2000 用の InfoCage モバイル防御をインストールしたパソコンに装着する。またはその逆を 行う。
- ・NTFS ファイルシステムの場合、暗号化するファイルとフォルダは、SYSTEM アカウントの変更権限が必要です。

■ SYSTEMアカウントの変更方法は、「3.2.2 SYSTEMアカウントの変更方法」を参照してください。

- ・ NTFS ファイルシステムで暗号化または圧縮されたファイルは暗号化できません。
- ・暗号化指定したフォルダを共有設定しないでください。
- ・ 旧バージョンの InfoCage モバイル防御で暗号化した外部メディアおよびハードディスクドライブを本バージョンの InfoCage モバイル防御がインストールされているパソコンに装着した場合、一部のファイルが正常に読み込みできないことがあります。
- ・万が一、使用中に次のような現象が発生した場合は、大切なデータを損失する可能性がありますので、現象が 発生した状態のまま何も操作を行わず、速やかに InfoCage モバイル防御製品保守担当までご相談ください。
 - * 暗号化したはずのファイルが読み書きできない(文字化けなど)
 - * OS にログオンできない
 - * 作成した鍵が使用できない(メディア鍵認証方式の場合)

● アップグレードインストールの注意事項

- アップグレードインストールを行う場合、すでにインストール済みの InfoCage モバイル防御をアンインストール する必要はありません。
- ・暗号化した外付けハードディスクドライブおよびリムーバブルディスクがある場合は、必ずパソコンに装着した 状態でアップグレードインストールを行ってください。パソコンから取り外した状態でアップグレードした場合、 一部のファイルが正常に読み込みできないことがあります。
- ・お使いのバージョンによってはアップグレードインストールの途中で数回再起動を行う場合があります。メッセージにしたがって操作してください。
- ・外部メディア自動暗号機能や FeliCa カードでの認証機能については、セットアッププログラムのカスタマイズ を行い、アップグレードインストールすることで、各機能が有効になります。カスタマイズ方法については、 「InfoCage モバイル防御 管理者ガイド」を参照してください。
- ・バージョンにかかわらずアップグレードインストール後も設定を引き継ぐものは以下の通りです。
 - * スーパーバイザパスワード/ユーザパスワード
 - * 鍵および鍵情報(InfoCage モバイル防御 Ver1.0 で鍵情報をネットワーク共有フォルダに作成している 場合もそのまま引き継がれます。)
 - * 暗号化指定されたドライブ/フォルダ
 - *管理サーバでの設定内容(ネットワークモードで運用している場合)
 - * インストール先のフォルダ

- * クライアント初期設定ツールでセットアッププログラムをカスタマイズしてインストールした設定内容
- * その他のユーティリティでの設定内容 (InfoCage モバイル防御ユーティリティおよびメディア暗号ユーティリティ)
- ・ Ver3.5より以前のバージョンからアップグレードインストールを行った場合に変わるものは以下の通りです。
 - * プログラム名 [MobileProtect] ↓ [InfoCage モバイル防御]
 - * スタートメニューからの起動方法 [すべてのプログラム]-[MobileProtect] ↓ [すべてのプログラム]-[NEC]-[InfoCage モバイル防御]
 - * ユーザーズガイド [MobileProtect オンラインマニュアル] ↓ 「InfoCage モバイル防御 ユーザーズガイド]

● メディア鍵認証方式の注意事項

 ・事前に準備していただくもの インストールには外部メディアが2個必要です。
 ご使用にあたっては、鍵を作成するメディア(*1)と、鍵情報を作成するためのメディア(*2)が必要です。
 各メディアはインストール前にフォーマットしておいてください。

🛕 Notice

メディアをフォーマットせずに使用した場合、鍵の作成や復旧ができない場合があります。

- *1:鍵は、USBメモリ、フラッシュメモリカード、フロッピーディスク (Windows XP/2000の場合のみ)、モバイル ディスク等の他、サーバの共有フォルダに作成できます。(推奨:USBメモリ) *2:フロッピーディスク、USBメモリ、フラッシュメモリカード、モバイルディスク等が使用できます。
- 注意事項
 - 鍵について InfoCage モバイル防御で保護されたパソコンを使用する際には、必ず鍵を作成したメディアを装着した状態で使用してください。
 - (2) 鍵情報について
 - ・「鍵情報」を紛失すると「鍵」の復旧ができませんので、「鍵情報」を保存したメディア内のデータを絶 対に紛失しないように注意してください。
 - ・スタンドアローン運用時、鍵情報は鍵を作成したメディアには保存できません。

● パスワード認証方式の注意事項

- ・セキュリティチップ(TPM)を使用している場合、以下の操作を行うと、暗号化されたファイルにアクセスできな くなりますので絶対に行わないでください。これらを行う場合は、いったん InfoCage モバイル防御をアンイン ストールしてから行ってください。
 - * セキュリティチップ(TPM)は Windows XP でパスワード認証方式を導入する場合のみ使用可能です。
 - * BIOS でセキュリティチップを[使用しない]に設定を変更する
 - * BIOS のアップデートなどで設定値を初期化する
 - * セキュリティチップユーティリティをアンインストールする

● ハードウェア/アプリケーション競合問題について

次のハードウェアおよびアプリケーションソフトは、InfoCage モバイル防御と同時に利用、またはInfoCage モバイル 防御がインストールされた環境で利用すると、問題が発生することがあります。 これらは InfoCage モバイル防御をインストールする前にアンインストール、または取り外しておいてください。 アプリケーションをアンインストールできない場合は使用しないでください。

🛕 Notice

- ・下記はこれまで報告のあったハードウェアおよびアプリケーションソフトの一覧を記載しております。記載のない ハードウェアおよびアプリケーションソフトの動作を保証するものではありません。(2008年1月現在)
- 最新情報は以下に掲載しております。 http://www.nec.co.jp/cced/infocage/m_defense/env.html

InfoCage モバイル防御と共存できないハードウェア/アプリケーション

× ・・・共存できないことを確認済みのハードウェア/アプリケーション

空欄 ・・・OS 未対応または未確認のハードウェア/アプリケーション

ハードウェア/アプリケーションの種類	Windows Vista	Windows XP/2000	
・ハードウェア			
I/O データ UIDE-133R2(RAID ボード)		×	
 他のファイル暗号化ソフト、一部の独自のログオン認証を行うソフト、BitLocker ドライブ暗号化(Windows Vistaの統合セキュリティ機能) 	×	×	
Pointsec Media Encryption		×	
・ 仮想マシン環境構築ソフト(Microsoft VirtualPC など)	×	×	
 データバックアップ、リカバリソフト 			
(PowerX StandbyDisk4、FINALDATA2007、Acronis True Image LE、Acronis True Image 10 など)	×		
(StandbyDisk、StandbyDisk Solo、StandbyDisk Solo RB、FINALDATA、Acronis True Image LE、Acronis True Image 8.0 など)		×	
・一部のディスクイメージ(HDD バックアップ)作成ソフト(V2i Protector など)		×	
 ・ティアック株式会社 Swipe FINGERPRINT USB メモリ および NEC 製ノートパソコン内蔵の指紋センサ以外を使用する指紋認証システム (NEC 製ノートパソコン内蔵の指紋センサを使用した認証システムと、InfoCage モバイル防御の認証システムとの併用が可能です。ただし、Swipe FINGERPRINT USB メモリのように連携させることはできません。) 			
・一部のライティングソフト(B's CLiP など)		×	
・一部の PC プレインストールソフト			
(IBM/レノボ製 PC に付属のバックアップソフト「Rapid Restore Ultra/Rescue and Recovery」	×	×	
松下電器製 PC に搭載されている「オプティカルディスク省電力ユーティリティ」 など)		×	
・ McAfee プライバシーサービス		×	
Acronis True Image LE, True Image 8.0		×	
Acronis DriveCleanser		×	

ハードウェア/アプリケーションの種類	Windows Vista	Windows XP/2000
• DiskXtender		×
• PartitionMagic		×
• Windows ReadyBoost	×	
・一部のウイルス対策ソフト (Symantec Endpoint Protection 11.0、Norton Internet Security 2008、Norton AntiVirus 2008 、GRISOFT AVG Anti-Virus 、eTrust Antivirus 、McAfee Managed Total Protection 4.x (4.0.0.395 以降)、Eset NOD32 など)		×
・ Google パック(Norton SecurityScan Ver.1.1.0.27)		×
 Google ハック(Norton SecurityScan Ver.1.1.0.27) Norton SystemWorks (Norton Utilities)のNorton Protection (ごみ箱機能) 使用している場合は InfoCage モバイル防御をインストールする前に解除してください。 <解除方法> 1.デスクトップの[Norton ごみ箱]のアイコンを右クリックし、[プロパティ]をクリックして ください。 2.[Norton Protection]タブを選択してください。 3.プルダウンメニュー[ドライブ]で、ドライブを選択し、[保護を有効にする]チェックを 外してください。 ※必ず全ドライブ無効にしてください。 4.[OK]をクリックしてください。 		×

使用に制限のあるハードウェア/アプリケーション(Windows XP/2000)

ハードウェア/アプリケーションの種類	対策	
ハードウェア		
SOTEC Winbook WV730 (PC 本体)	BIOS をアップグレードすることにより利用可能 (Ver は 1.03ST → 1.05ST)	
独自のセキュリティ機能を持つ USB メモリ (IO Data EasyDisk for Security など)	鍵以外では利用可能。(鍵メディアとして利用不可)	
CD-R 等ライティングソフト (*)		
・Windows XP 標準の CD 書き込み機能	ファイルを書き込みする場合は、暗号化されていないフォルダに	
• DirectCD	ファイルをコピーもしくは移動した後に操作を行うことで利用可能	
ウイルス対策ソフト		
・SymantecAntiVirusCorprateEdition10.0 (MR2 MP2 より以前のバージョン)	0 パッチ適用により利用可能	
・Symantec Client Security 3.0.2 (MR2 MP2 より以前のバージョン)		
• Norton AntiVirus2006		
その他ソフト		
• Symantec pcAnywhere	 ・pcAnywhere→モバイル防御の順でインストールすることで利用 可能 ・モバイル防御→pcAnywhere の順でインストールする際は、パッ チ適用で利用可能 	
• Pointsec	・ディスク暗号による暗号化環境での利用不可。	
• NETWIZARD	・[ReachOut サービスを停止しました]エラーを閉じてログオンす ることで利用可能。閉じずにログオンした場合は Ctrl+Alt+Del を	

ハードウェア/アプリケーションの種類	対策
	押下してエラーを再表示し閉じることにより利用可能。 ・閉じずにログオンした場合は Ctrl+Alt+Del を押下してエラーを 再表示し閉じることにより利用可能。
・BIGLOBE リモートアクセスサービス VPN クライアント	・VPN ソフト→モバイル防御の順番でインストールすることで利用 可能
・ローミングクライアント	以下のどちらかで利用可能 ・ローミングクライアント→モバイル防御の順でインストール。 ・ローミングクライアントのレジストリを編集。
	ただし、ドメイン環境使用時には上記回避策のみではドメインログ オンができなくなります。モバイル防御の初期設定ファイルを置換 することで利用可能。
• WebSAM WinShare	・WebSAM WinShare→モバイル防御の順でインストールすること で利用可能。
・Socia 給与システム	以下のどちらかで利用可能。 • Oracle9.2i以上を利用する。 • Oracle インストールフォルダ(データベース格納フォルダ含む) を暗号化対象外とすることで回避可能。
・InfoCage 持ち出し制御 クライアント	以下の手順で利用可能 (1)InfoCage 持ち出し制御をアンインストールする。 (2)InfoCage モバイル防御をインストールし、再起動後に暗号化 を行う。 (3)InfoCage 持ち出し制御 クライアントをインストールする。
・4thEye Professional++ クライアント版	※4hEyeとの共存については、別途お問い合わせください。

(*) 下記のライティングソフトは InfoCage モバイル防御とは併用が可能であることを確認しています。

RecordNow

• B's Recorder Gold

• Easy CD Creator

2.3 【導入前の注意事項】確認チェックシート

InfoCage モバイル防御をインストールする前に、以下の項目をチェックしてください。

			チェック欄	
	確認事項	メディア鍵	パスワード	
		認証方式	認証方式	
1	重要なデータは、念のためバックアップを取ること。			
2	鍵用のメディア、あるいはサーバを用意すること。			
	十分な空き容量が各ドライブにあること。			
3	 ※暗号化を実行する際、テンポラリ(一時作業スペース)として以下の空き容量がドラ イブごとに必要になります。 必要な空き容量 = 暗号化対象ファイルの中で最大のファイルと同等の容量 + (ド ライブ容量×0.02) (上記は最低限必要な容量です。暗号化処理は、十分な空き容量がある状態で行っ てください。) ※ただし、初めて暗号化処理を行う場合はすべてのドライブのごみ箱を暗号化するた め、暗号化指定していないドライブにも上記の空き容量が必要となりますのでご注 			
	意ください。			
4	共存不可のアプリケーションの確認・対策を行うこと。 ※「アプリケーション競合問題について」を参照			
5	暗号化するフォルダやファイルに SYSTEM アカウントの変更権限があることを確認すること。			
6	デュアルブートマシンでないこと。			
7	仮想ドライブを割り当てていないこと。			



InfoCage モバイル防御のインストールを行います。

🛕 Notice

アップグレードインストールを行う場合は、「第5章 アップグレードインストール」を参照してください。

3.1 インストールの前に

■ 確認事項

インストールの前に次のことを確認してください。

□ 注意事項はすべて確認しましたか?

▶ 注意事項は「2.2注意事項」を参照してください。

□ 「【導入前の注意事項】確認チェックシート」を実施しましたか?

● 確認チェックシートは「2.3 【導入前の注意事項】確認チェックシート」を参照してください。

□必要なものは揃っていますか?

InfoCage モバイル防御の管理者から次のものが配布または通知されているか確認してください。

運用方法の通知(メディア鍵認証方式またはパスワード認証方式) ※
プロダクト ID の通知
「鍵および鍵情報を保存するメディアの配布(メディア鍵認証方式の場合)
暗号化するドライブ/フォルダの通知(個別暗号モードインストールの場合) 💥
許可外部メディアの配布(許可外部メディアを利用する場合)

(※) InfoCage モバイル防御の管理者より、あらかじめセットアッププログラムに設定されている場合があります。

3.2 パソコンの環境チェック

インストールを行う前に、InfoCage モバイル防御を使用するパソコンの環境をチェックしてください。

3.2.1 環境チェックユーティリティ

🗞 Operation

 InfoCage モバイル防御が格納されているメディア(例 CD-ROM)内の以下のファイルを実行してください。 Windows Vista の場合 ¥Vista¥Tools¥環境チェックUTL¥MPEnvChk.exe
 Windows XP/2000 の場合 ¥2K_XP¥Tools¥環境チェックUTL¥MPEnvChk.exe

```
▲ Notice
CD-ROMからコピーして使用する場合は、環境チェックUTLフォルダをデスクトップなどにコピーしてから
実行してください。(MPEnvChk.exe は実行ファイルのみをコピーしても動作しません。)
```

2. 環境チェックユーティリティの説明が表示されます。 [OK]をクリックして、起動しているアプリケーションや常駐プログラムを必ず終了してください。



3. [ドライブ]に表示されているドライブのうち、暗号化するドライブにチェックを入れ、[開始]をクリックしてください。

P InfoCage モバイル約朝 間後チェックユー	74974
BR1201R1910071201. (Blue	9048#UE0880%
IZ C#	
7#65-7+16&	mana
	19 100

4. 環境をチェックしています。しばらくお待ちください。

* InfoCage モバイル的師 環境チェックユーディリ	194
IRRESOLUTION COMPL. (MILLING)	PLEORNA
P347	
R CH	
RADADP	
7855-7+158	Mag-rus
C#SetsRepoten01	7963/8

5. 問題が見つかった場合は、[フォルダ・ファイル名]に表示されているファイルを選択し、[対処方法]をクリックします。

* DeliCage モバイル的群 環境チェックユーティリティ	
使用チェンクを用けずるとうくさを追加し、「読む」がたくを押していたた。	
1917	
IE CH IE DH	
NAMES OF A CONTRACT OF A DESCRIPTION OF	
2007 21100	
Caldukovendt	79628
Canada da C	The second se
CHOssuments and SettingsRuseOVHy DocumentsRomath	24150000
CROscurents and SettingsRuseOVRIy DocumentsRomatic	291.605899
Concerning and Delivery Accessible Decementation Accession and Concerning and Delivery and Deliv	10.00
Comparison of Second Contract of Second Contract Second	1NEVOE
Concentration and the second state of the seco	0.000

6. 対処方法が表示されます。内容を確認し、[OK]をクリックします。

▶ アクセス権に関する対象方法については、「3.2.2 SYSTEMアカウントの変更方法」を参照してください。



7. ファイルを選択している状態で[開く]をクリックすると、ファイルのあるフォルダが開きます。 対処方法に表示されていた内容にしたがって、対処してください。

♪ DrivCage モバイル的群 環境チェックユーディリティ	(c) 0 📰
環境を200年度です3月9日の大阪業所に、「開発」が30年時にこの2015	
8947	
R CH	
THE REPORTS AND A DESCRIPTION OF THE PROPERTY	
Contractored	70024
Giloconents ed Serregikar/PMI Doument/Aprof. Giloconents ed Serregikar/PMI Doument/Aprof. Giloconents ed Serregikar/PMI Doument/ADChatektekte/de/ Giloconents ed Serregikar/PMI Doument/ADChatektekte/de/ Giloconents ed Serregikar/PMI Doument/ADChatektekte/de/ Giloconents ed Serregikar/PMI Doument/ADChatektekte/de/ Giloconents ed Serregikar/PMI Doument/ADChatektekte/ Doument/ADChatektekte/ Giloconents ed Serregikar/PMI Doument/ADChatektekte/ Doument/ADChatektektekte/ Doument/ADChatektektektektektektektektektektektektekt	2+(4)代期中 2+(4)代期中 75月 75月 75月 75月 75月
PROFILED	AMINO MITOD

8. 環境チェックユーティリティを終了する場合は、[終了]をクリックします。

the second	
株チェンクを用いするとうくうを確認し、「数回」が30.4月していたさい。	
H7	
é ca	
8.0 W	
Cope Envisioner(2017-54104-2010-000-000-000-0	
1+55-7+(58	1200-102
California (200.28
Contraction of the second se	10000
(Manufacetore))	7582.0
(Administration) (Administration)	75±3月 2×64月前中
Resulty-steel2 Wite-sense and Seming-Rase(1999; Document/Abra)1 Wite-sense and Seming-Rase(1999; Document/Abra)2	7953篇 2+(A世間中 2+(A世間中
Didonalisysteel2 Didonalisysteel2 Didonalisessa aid SemingsRuse01999 Document/Admitt Didonalises aid SemingsRuse01999 Document/Admittable Didonalises aid SemingsRuse01999 Document/AdmittableDidonalistoch4	79世3月 2年(永徳明中 3年(永徳明中 103月
Debustystend2 EROssuents and Semagakaer01999 DocumentAtasid Robustents and SettingeRear01999 DocumentAtasid2 Robustents and SettingeRear01999 DocumentAtaSid2RearAtasidaetAtadebit Robustents and SettingeRear01999 DocumentAtaSid2RearAtasidaetAtadebit Robustents and SettingeRear01999 DocumentAtaSid2RearAtasidaetAtadebit	75年3月 7年1月世界中 7年1月世界中 701月 701月
Cadenakysteeli2 Cadenakysteeli2 Cadenakers and Serregikaand'HMy Document/Abrahit Discounters and Serregikaand'HMy Document/Abrahitakkoolek Discounters and Serregikaand'HMy Document/Abrahitakkoolek Discounters and Serregikaand'HMy Document/Abrahitakkoolek Discounters and Serregikaand'HMy Document/Abrahitakkoolek	79年2月 2年6月世界 2年6月世界 7月3月 7月3月 1月3月 1月3月 1月3月
Descriptional Colonaments and SettingsRead/1999; Documents/Settill Colonaments and SettingsRead/1999; Documents/MCRestational/adocting Colonaments and SettingsRead/1999; Documents/MCRestational/adocting CROssuments and SettingsRead/1999; Documents/MCRestational/adocting CROssuments and SettingsRead/1999; Documents/Adocting	75523編 29438世界中 29438世界中 2938年 2038年 1038年 1038年
Charakoponinti Okonamis ad Simopikaad/199, poolentikkisti Siloonenis ad Simopikaad/199, poolentikkisti Okonamis ad Simopikaad/199, poolentikkistaataote Okonamis ad Simopikaad/199, poolentikkistaataote Okonamis ad Simopikaad/199, poolentikkista	7963月 2968世紀 2968世紀 2968世紀 208 208 208 208 208 208 208 208 208 208
Celebrationell Octowers ed Sampskastfrith, Douenskindt Octowers ed Sampskastfrith, Douenskindt Octowers ed Sampskastfrith, Douenskittickeldodt Octowers ed Sampskastfrith, Douenskittickeldodt Octowers ed Sampskastfrith, Douenskittickt	796238 294(A世間中 294(A世間中 H346 H346 H346 H346 H346 H346 H346 H346

9. 問題の一覧を保存する場合は[はい]をクリックします。



10.保存する場所を指定し、[保存]をクリックします。

10129400	F#3.5	04	-	000	-
8,81	更新日時	121	サイズ	99	
				_	
7(483)	214/05/23	07770280		-6	100

以上で環境チェックは完了です。

見つかった問題の対処が完了したら、InfoCage モバイル防御をインストールします。

3.2.2 SYSTEM アカウントの変更方法

NTFS ファイルシステムの場合、暗号化するファイルとフォルダは、SYSTEM アカウントのフルコントロール権限または変更 権限が必要です。

(Windows Vista および Windows XP Professional 、Windows 2000 のみ変更可能です。) ここでは D:¥Data¥Data1 フォルダの SYSTEM アカウントを変更する方法を説明します。

■ Windows Vista の場合

🗞 Operation

1. SYSTEM アカウントを変更したいフォルダを右クリックし、表示されるメニューの中から[プロパティ]を クリックしてください。フォルダのプロパティ画面が表示されます。

9710 9710	
5710 5710	
9710 9710	
яю	
Nr. 0	
-00	
UTABD	kato).
	icoo Diriedd

2. [セキュリティ]タブを選択し、[編集]をクリックしてください。アクセス許可の編集画面が表示されます。 [グループ名またはユーザ名]から[SYSTEM]を選択し、[アクセス許可]の[フルコントロール]の[許可]に チェックを入れ、[OK]をクリックしてください。

これで SYSTEM アカウントが変更されました。[OK]をクリックして画面を閉じます。

Data1のアクセス許可		
04:3994		
オブジェクト名 DXData#Data1		
グルーナ名またはユーザー名(①)		
S2 CREATOR OWNER		
2 aut (FOUR and		
Luser1 (PC014User1)	(material)	-
*	are or a	
	iBttp(_)_	ARKB)
SYSTEM のアクセス非可(E)	19-17	推造
SYSTEM のPかセス体可(例) フル コントロール	19-27 19-27	相當
SISTEM のPかセスは中可(日) フル エントロール 基本 読みまたいと思い	(回) (回) (日) (日) (日) (日) (日) (日) (日) (日) (日) (日	103
SYSTEM のからせいみ中の(引) フルコントロール また 読み取りと実行 フォルダの内容の一覧表示	N N N N	165
SYSTEM のひかせつお中の(E) フル コントロール 本来 読み取りと用いう フォルダの内容の一覧表示 読み取り	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	#65
SYSTEM のアクセン非可(2) 2月 コントロール 次度 読み取りますう 2月 小がらの下部の一覧 読み取ります。 読み取り 2月 小がらの下部の一覧 表示 読み取り 2月 ついます。 2月 小がらの下部の一覧 また。 2月 小がらの一部であります。 2月 小がらの一覧 2月 小がらの 2月 小がらの 2日 小がらの 2月 小からの 2月 小 2月 小からの 2月	1947 20 20 20 20 20 20 20 20 20 20 20 20 20	163

🛕 Notice

[グループ名またはユーザ名]内に[SYSTEM]が表示されていない場合は、次の方法で表示させてください。

- 1. [グループ名またはユーザ名]の下の[編集]をクリックし、[アクセス許可]の画面で[追加]をクリックします。
- 2. 表示された画面の[選択するオブジェクト名を入力してください]に[SYSTEM]と入力し、[名前の確認]を クリックします。
- 3. [選択するオブジェクト名を入力してください]に[SYSTEM]と表示されますので、[OK]をクリックします。

■ Windows XP/2000の場合

🗞 Operation

1. SYSTEM アカウントを変更したいフォルダを右クリックし、表示されるメニューの中から[プロパティ]を クリックしてください。フォルダのプロパティ画面が表示されます。

Detail@2015	14	2 🛙
全統 共主	1042094 209947	
	Deta1	
1618	7+15 7+55	
471	DWDeta	
913	2.00 MB (2000,000 /5(1))	
8922	2.00 MB (2.000,000 /1/11)	
内容	ファイル数 10.7#ルダ数 0	
nusee	2006年4月6日、000000	
腐壮	 読み取り専用(2) (第し7)・(ルージ) 	Indike ga
	OK #+	254 8763

🛕 Notice

[セキュリティ]タブが表示されていない場合は、次の方法で表示させてください。

- 1. SYSTEM アカウントを変更したいフォルダを開きます。
- 2. [ツール]-[フォルダオプション]-[表示]-[簡易ファイルの共有を使用する]のチェックを外して、[OK]をクリック してください。

[セキュリティ]タブを選択してください。 [グループ名またはユーザ名]から[SYSTEM]を選択し、[アクセス許可]の[フルコントロール]の[許可]に チェックを入れ、[OK]をクリックしてください。 これで SYSTEM アカウントが変更されました。

载 [共有] 10年107-4 525247	()	
グループ名またはユーザー名(公)		
Administrators (PODIVAdminist COREATOR OWNER	rators)	
SYSTEM		
Cover a compositio		
Coers (PC01#Users)		
	1870 Q/.	8488/89
CONTRA A REPORT OF THE PARTY OF	19.27	162
7% 32/10-%	. EI	8 1
読み取りと用け		ö
フォルダの内容合一覧表示		
書き込み		ŏ,
接接なアクセス非可または認識記定を表	EFFECT OF	Indiana
AND A REAL AND AVAILABLE		Baseline (C.C.)

🛕 Notice

[グループ名またはユーザ名]内に[SYSTEM]が表示されていない場合は、次の方法で表示させてください。

- 1. [グループ名またはユーザ名]の下の[追加]をクリックします。
- 2. 表示された[ユーザまたはグループの選択]画面の[選択するオブジェクト名を入力してください]に[SYSTEM]と 入力し、[名前の確認]をクリックします。
- 3. [選択するオブジェクト名を入力してください]に[SYSTEM]と表示されますので、[OK]をクリックします。

3.3 Step1

InfoCage モバイル防御をインストールします。下記の手順で操作してください。

🏷 Operation

1. InfoCage モバイル防御が格納されているメディア(例 CD-ROM)内の setup.exe を実行し、[次へ]をクリック してください。

InfoCage	モバイル防御 インストーラ	
	このたいは、krisCage モバイルが利用もご購入いただき、 まことに知りがたいこといせず。	
	helocare モバイル防御は、パンプレクロック、デーの回帰号化を行うことで、 パンプンからの補助業業を防止すると気の効果造です。 利潤、公司需求に合わせて、LEGNを印成とのパムーパブル・ディアを提出して使用する。 ドンジング通び起きたでし、または、専用的パンジードを使用するパンジラート回転方式にを 運行することができます。	
	インストールを開始するにはり次へ」を押してください。	
	(第3日) (78人285) キャンセン	

2. [「メディア鍵認証方式の InfoCage モバイル防御」をインストール]または[「パスワード認証方式の InfoCage モバイル防御」をインストール]のいずれかを選択し、[次へ]をクリックしてください。

8	InfoCase モバイム防御のインストールを行います。 インストール学るInfoCase モノイム防御を輩択し、「次へ」を押してく たたい。
	メディア雑習証方式のわれてare モバイル防御」をインストール USBメモリなどのリムーバブルメディアを練たして使用します。
0	バスワード認証方式のShifeCage モバイル防御」をインストール 専用のパスワードを使用します。

🛕 Notice

InfoCage モバイル防御の管理者によって運用形態が設定されている場合は、この画面は表示されません。

3. [導入前の注意事項] 画面が表示されます。

各項目をクリックすると詳細な説明が表示されますので、必ずすべての注意事項を確認し、チェックを付けて ください。

すべての確認が終わりましたら、[閉じる]をクリックしてください。



A Notice

画面はメディア鍵認証方式のものです。パスワード認証方式の場合は一部異なります。

4. すべての項目がチェックされていない場合は、下記のメッセージが表示されます。 インストールを続ける場合は[はい]をクリックしてください。 インストールを中止する場合は[いいえ]を、**3** の画面に戻る場合は[キャンセル]をクリックしてください。

	TATONE	はチェックされ)	CIVETA.
-	インストール	、を続けますか?	
		`	

5. [次へ]をクリックしてください。



6. 使用権許諾契約をすべて確認し、同意する場合は[使用権許諾の条項に同意します]を選択し、[次へ]を クリックしてください。

[使用権許諾の条項に同意しません]を選択した場合はインストールできません。

使用權許認知的		No.	
2次の使用権許認契約の書を注意:深くおき	(153)をあ		
お客様へのお願い			-
このソフトウェアパッケージを	インストールされる前に	こ必ずお読みくだ	1
この度は、本製品をお求めいた: 物料では本製品のお客様による	だき、まことにありがと	とうございます。	
スについて、下記の「ソフトウ	エア使用権許諾契約書」	を設けさせてい	
本契約書を充分にお読みくださ! い場合は、本製品をお求めにな	い。本契約書の条件にこ った取扱序にご返却くた	(同意いただけな)	
・ 使用権許認知的の条項に同意します(Al		
D (ENHIBITERATIOR/ALITERUS/EA	w(D)		
stalSheld	20100		
	Comment of the second	a hard beau	-

7. ユーザ情報を入力します。

ユーザ名、会社名、プロダクトID、スーパーバイザパスワード/ユーザパスワードを入力します。 (確認のため、スーパーバイザパスワード/ユーザパスワードは2回入力してください。) すべての入力が終わりましたら、[次へ]をクリックしてください。

ユーザ情報		- 4
情報を入力してください。		
2-4800:		
1 余社名(2):		
1 プロダクトロタ): 		
スーパーバイザパスワード入力確認	(<u>v</u>):	
traffound.		
	- WR (0)	- 00

ユーザ名、会社名	半角 40 文字以内、または全角 20 文字以内で入力してください。
プロダクト ID	ライセンス証書に記載されているものを半角文字で入力してください。 (大文字小文字は区別しません)。
スーパーバイザパスワード	8 文字以上 64 文字以内の半角英数および記号を指定してください。 (大文字小文字を区別します)。
ユーザパスワード	8 文字以上 32 文字以内の半角英数および記号を指定してください。 (大文字小文字を区別します)

A Notice

- ・ 画面はメディア鍵認証方式版のものです。パスワード認証方式版の場合は、[スーパーバイザパスワード]の欄は[ユーザパスワード]と表示されます。
- スーパーバイザパスワード/ユーザパスワードとは InfoCage モバイル防御ユーティリティを起動すると きなどに必要なパスワードです。忘れないよう注意してください。

8. [運用形態の選択] 画面で、運用形態の選択をします。 [スタンドアローンモード]または[ネットワークモード]を選択し、[次へ]をクリックしてください。

運用影響を選択してください。	
* Z3X#70-XE-P(3)	
◎ ネットワークモード(2)	
110	
ないアップ調査キットワークモードからスタンドアローンモードに移	
料行するためには、一旦アンインストールする必要 があります。	

🛕 Notice

- 別売の InfoCage モバイル防御 管理サーバが導入されていない環境では、スタンドアローンモードを 選択してください。
 また、InfoCage モバイル防御管理サーバが導入されている環境では、InfoCage モバイル防御の管理
 - 者に問い合わせて運用形態を選択してください。
- InfoCage モバイル防御の管理者によって運用形態が設定されている場合は、この画面は表示されません。
- ・ スタンドアローンモードを選択した場合は 10 へ進んでください。
- **9.** 8でネットワークモードを選択した場合、クライアント認証画面が表示されます。 クライアントID、管理サーバのURLを入力して、「次へ」をクリックしてください。

A Notice

- ・ スタンドアローンモードの場合、この画面は表示されません。
- ・認証に失敗した場合は、クライアントA、クライアントID、管理サーバの URL を確認後、InfoCage モバイル防御の管理者に問い合わせてください。
- ・ InfoCage モバイル防御の管理者がクライアント登録をしていない場合は認証されません。
- ・ その他の理由で認証に失敗した場合は、以下を参照してください。

参照 第11章トラブルシューティング(2)

10. インストール先のフォルダ選択画面で InfoCage モバイル防御のインストールフォルダを選択します。 通常はそのまま[次へ]をクリックしてください。



🛕 Notice

日本語または英語以外の文字を含むフォルダにインストールすることはできません。

11. [インストール]をクリックしてインストールを開始してください。



12. インストール中です。しばらくお待ちください。

D InfoCag	e モバイル防御 - InstaliShield Wizard	
InfoCage 7075/	モバイル病効率 をインストールしています 、をインストールしています。	1
13	InstalSheid ウィザードは、InfoCage モバイル防御 をイン す。しばらくお何ちらだだい。 ステータス:	ストールしていま
bristaliShield -	< 戻る(目) 沈へ(日	p>

13.インストールが完了すると下記の画面が表示されます。 [完了]をクリックしてください。

14. InfoCage モバイル防御を使用可能にするためには、パソコンを再起動する必要があります。 他のプログラムを実行中の場合は、終了させてください。 [OK]をクリックすると、パソコンが再起動します。



再起動後の操作は、次章以降を参照してください。

3.4 Windows ヘログオン

InfoCage モバイル防御をインストールすると、Windows のログオン方法が変わります。 再起動後は以下の手順で Windows ヘログオンします。

```
■ Windows Vista の場合
```



1. InfoCage モバイル防御のボタンをクリックします。



2. Windows のユーザ名およびパスワードを入力し、 ● をクリックするか Enter キーを押すと、 Windows ヘログオ ンすることができます。

パスワード認証方式の場合は[InfoCage モバイル防御 パスワード]に、インストール時に設定したユーザパ スワードを入力してください。



A Notice

- ・ 画面はメディア鍵認証方式のものです。
- ドメインに参加している場合は[ワークグループ名/ドメイン名]にドメイン名を入力してください。 (ワークグループの場合は空欄でも可。)

●ユーザ情報エラーの場合

メディア鍵認証方式の場合は鍵を抜いた状態、パスワード認証方式の場合は誤ったユーザパスワードでログ オンしようとすると、[Windows のユーザ情報、または InfoCage モバイル防御の認証情報が違います。] と 表示され、Windows ヘログオンできません。

[OK]をクリックして、2に戻って操作してください。



■ Windows XP/2000 の場合

- メディア鍵認証方式の場合
 - 再起動後に[Windows へようこそ]画面が表示されます。 Ctrl+Alt+Delキーを押してください。



🛕 Notice

Windows の設定によっては、[Windows へようこそ]画面は表示されません。

2. [Windows ヘログオン] 画面が表示されます。

正しいパスワードを入力して[OK]をクリックするとWindows ヘログオンすることができます。



● パスワード認証方式の場合

 再起動後に[Windows へようこそ]画面が表示されます。 Ctrl+Alt+Delキーを押してください。



🛕 Notice

Windowsの設定によっては、[Windows へようこそ] 画面は表示されません。

2. ユーザパスワード入力画面が表示されます。 インストール時に設定したユーザパスワードを入力し、[OK]をクリックしてください。



🛕 Notice

```
ユーザパスワードを5回連続で誤って入力すると、[OK]がクリックできなくなります。
その場合は[シャットダウン]をクリックしていったんシャットダウンした後、再度パソコンを起動してパスワード入力画面が有効になるまでしばらくお待ちください。
(すぐにパソコンを起動しても一定時間パスワードの入力はできません。)
```

3. [Windows ヘログオン] 画面が表示されます。 正しいパスワードを入力して[OK]をクリックすると Windows ヘログオンすることができます。

	👭 Win	dows ^{xp}	
2-9-80	User1	Allow	seeff
パスワード(1)	[

続いて次章「3.5 Step」へ進み、それぞれの認証方式の項を参照してください。

3.5.1メディア鍵認証方式の場合

3.5.2パスワード認証方式の場合

InfoCage モバイル防御の管理者の設定により、個別暗号モードでインストールした場合は、「第4章 個別暗号モードインストール」へ進んでください。
3.5 Step2

再起動後、暗号化ウィザードが起動します。

それぞれの認証方式の説明にしたがって、暗号化を行ってください。

🗛 Notice

```
何らかの理由で暗号化ウィザートを終了した場合、再度暗号化ウィザードを起動するには、スタートメニューから
[すべてのプログラム]-[NEC]-[InfoCage モバイル防御]-[InfoCage モバイル防御 ユーティリティ]をクリックします。
```

3.5.1 メディア鍵認証方式の場合

🗞 Operation

1. Windows Vista の場合は再起動後に、以下の画面が表示されます。 [OK]をクリックしてください。

InfoCage/モバイル防御	
InfoCage/モバイル称加 コ よろしいですか?	レーティリティを起動します。
	at a state of
(OK	447214

A Notice

[キャンセル]をクリックすると、本プログラムが終了します。その場合は、後で必ず再度暗号化ウィザードを 起動して、パソコンの鍵を作成および暗号化を行ってください。

2. 鍵を格納するメディアと鍵情報を格納するメディアを装着し、インストール時に設定したスーパーバイザ パスワードを入力して[次へ]をクリックしてください。

鍵を作成し、暗号化を実行します。	E)
構わよび創始期を結めするパディアを装置して、 スーパーパイサリマスワードを入力し、「ホペンポのいを 使してくどあい。	
2-11-11190(29-10)	
· · · · · · · · · · · · · · · · · · ·	_

🛕 Notice

他のパソコンの InfoCage モバイル防御 ユーティリティまたはメディア暗号ユーティリティで暗号化した外部メディアは、暗号化を実行する前に必ず抜いてください。

装着したまま暗号化を開始すると上図と異なる画面が表示されますので、いったん [キャンセル] をクリックし、外部メディアを抜いてから再度暗号化ウィザードを起動してください。

3. 鍵および鍵情報を作成します。

鍵を格納するメディア および 鍵情報を格納するメディアのドライブを選択してください。 格納するメディアが表示されないときは、[更新]をクリックします。 [次へ]をクリックしてください。

えます.	1
「ライブを雇用」、	
6	
(F.	
(151)ないた()。 (ますう)	
	礼ます。 19(22編8)。 (6) (5) (8) (8) (8) (8) (8) (8) (8) (8) (8) (8

🛕 Notice

- ・ ネットワークモードの場合や InfoCage モバイル防御の管理者によりあらかじめ鍵および鍵情報の格納 先が設定されている場合は上記の画面が一部異なります。
- ここではネットワークの共有フォルダに鍵を作成することはできません。共有フォルダに鍵を作成する 場合はいったん外部メディアに鍵を作成し、暗号化終了後に合鍵として作成してください。
- ネットワークモードの場合で管理サーバと通信できないときは、以下を参照してください。
 第 11 章 トラブルシューティング (2)

4. 常駐アプリケーションや起動しているアプリケーションがあれば必ず終了してください。 [はい]をクリックすると暗号化が開始されます。



🛕 Notice

- ・ アプリケーションが使用しているファイルは、暗号化できない場合があります。
- ・ 暗号化するフォルダ内のファイル数が多い場合、暗号化に時間がかかる場合があります。
 またごみ箱に大量のファイルが入っている場合は暗号化に時間がかかることがありますので、あらかじめごみ箱を空にしておくことをお奨めします。

5. 暗号化処理中です。しばらくお待ちください。

BIRDER INFORMATION	
RARAGA CARCEMPERSO	
	500 / 1
成立の影響	
31823w645: GWhojectWowal	
8810: 870.	

6. 暗号化を完了しました。 [完了]をクリックしてください。



以上で暗号化は完了しました。

その他の設定については、「InfoCage モバイル防御 ユーザーズガイド」を参照してください。

🛕 Notice

この段階では、Program Files やアプリケーションのインストールフォルダ以下は暗号化されていません。 Program Files やアプリケーションのインストールフォルダ以下にあるデータファイルを個別に暗号化するには、 「InfoCage モバイル防御 ユーザーズガイド」の「アプリケーションのフォルダを暗号化指定する」の項を参照してください。(Windows XP/2000のみ)

3.5.2 パスワード認証方式の場合

● セキュリティチップ(TPM)搭載のパソコンをお使いでセキュリティチップ(TPM)が有効になっている場合

Windows XP の場合、InfoCage モバイル防御の管理者の設定によっては、再起動後にユーザパスワードを 入力して Windows にログオンすると、下記の画面が表示される場合があります。



セキュリティチップ(TPM)を使用する場合は[使用する]を、使用しない場合は[使用しない]を、後で選択する場合は [キャンセル]をクリックしてください。

ただし、[キャンセル]をクリックした場合、TPMの使用を選択するまで InfoCage モバイル防御 ユーティリティの起動 時にメッセージが表示されます。

セキュリティチップ (TPM) に関しては、「第 10 章 セキュリティチップ (TPM) 搭載のパソコンをお使いの 場合」を参照してください。 ● ログオン認証にパスワードを使用する場合



1. Windows Vista の場合は再起動後に、以下の画面が表示されます。 [OK]をクリックしてください。

InfoCage/モノミイル数 よろしいですか?	河即 ユーティリティを起動します
ROK	キャンセル

🛕 Notice

[キャンセル] をクリックすると、本プログラムが終了します。その場合は、後で必ず再度暗号化ウィザード を起動して、パソコンの鍵を作成および暗号化を行ってください。

2. ユーザパスワードを入力して[次へ]をクリックしてください。

de Contration de Sales - 19 - 1	
暗号化を実行します。	E
3-9039-PEX5L Davidson RUT058 V	
2-9/12/9-1/(8)	
	NAMES IN COMPANY

🛕 Notice

他のパソコンの InfoCage モバイル防御 ユーティリティまたはメディア暗号ユーティリティで暗号化した外 部メディアは、暗号化を実行する前に必ず抜いてください。 装着したまま暗号化を開始すると上図と異なる画面が表示されますので、いったん [キャンセル] をクリッ クし、外部メディアを抜いてから再度暗号化ウィザードを起動してください。

3. 暗号化を実行します。[次へ]をクリックしてください。

InfoCage/モバイル防御 暗号化ウィザード	
暗号化を実行します。	1
「ホッ」が少く生ます。 毎年位に当時間がかから用金があります。	
-1×-193	4+2/56

▲ Notice	
暗号化するフォルダ内のファイル数が多い場合、暗号化に時間がかかる場合があります。	

4. 常駐アプリケーションや起動しているアプリケーションがあれば必ず終了してください。 [はい]をクリックすると暗号化が開始されます。



🛕 Notice

アプリケーションが使用しているファイルは、暗号化できない場合があります。 暗号化するフォルダ内のファイル数が多い場合、暗号化に時間がかかる場合があります。 またごみ箱に大量のファイルが入っている場合は暗号化に時間がかかることがありますので、あらかじめ ごみ箱を空にしておくことをお奨めします。

5. 暗号化処理中です。しばらくお待ちください。

1HbCage/モバイル時間	0-00-0
処理中です。 しばら(法特ち下さい ー	
	500 / 100
R208月	
708246-5: OilhoactWonal	
永陽内容) 現今化	
-1094. 8101	

6. 暗号化を完了しました。 [完了]をクリックしてください。



以上で暗号化は完了しました。

その他の設定については、「InfoCage モバイル防御 ユーザーズガイド」を参照してください。

🛕 Notice

この段階では、Program Files やアプリケーションのインストールフォルダ以下は暗号化されていません。 Program Files やアプリケーションのインストールフォルダ以下にあるデータファイルを個別に暗号化するには、 「InfoCage モバイル防御 ユーザーズガイド」の「アプリケーションのフォルダを暗号化指定する」の項を参照してください。(Windows XP/2000のみ) ● ログオン認証に FeliCa カードを使用する場合 (Windows XP/2000 のみ)



1. インストール時に設定した InfoCage モバイル防御のユーザパスワードを入力して Windows にログオンすると、 下記の画面が表示されます。

ユーザパスワードを入力して[次へ]をクリックしてください。

Intellines / EDI (A時間 株式化力パテード	8
暗号化を実行します。	Ð
ユーザンワワードを入力し、「ホヘルギジンを 際していためい	
3-5107-10	
	4+200

🛕 Notice

他のパソコンの InfoCage モバイル防御 ユーティリティまたはメディア暗号ユーティリティで暗号化した 外部メディアは、暗号化を実行する前に必ず抜いてください。 装着したまま暗号化を開始すると上図と異なる画面が表示されますので、いったん[キャンセル] をクリック し、外部メディアを抜いてから再度スタートメニューから[すべてのプログラム] – [NEC] – [InfoCage モバイル防御] – [InfoCage モバイル防御 ユーティリティ]をクリックし、暗号化ウィザードを起 動して操作してください。

2. FeliCaカードをカードリーダにセットして[次へ]をクリックしてください。



FeliCa のカードリーダを使用可能な状態にしてから操作してください。

3. 常駐アプリケーションや起動しているアプリケーションがあれば必ず終了してください。 [はい]をクリックすると暗号化が開始されます。



A Notice

- ・ アプリケーションが使用しているファイルは、暗号化できない場合があります。
- ・ 暗号化するフォルダ内のファイル数が多い場合、暗号化に時間がかかる場合があります。 またごみ箱に大量のファイルが入っている場合は暗号化に時間がかかることがありますので、ごみ箱を 空にしておくことをお奨めします。
- 4. 暗号化処理中です。しばらくお待ちください。



5. 暗号化を完了しました。 [完了]をクリックしてください。



以上でインストールは完了しました。

その他の設定については、「InfoCage モバイル防御 ユーザーズガイド」を参照してください。

🛕 Notice

この段階では、Program Files やアプリケーションのインストールフォルダ以下は暗号化されていません。 Program Files やアプリケーションのインストールフォルダ以下にあるデータファイルを個別に暗号化するには、 「InfoCage モバイル防御 ユーザーズガイド」の「アプリケーションのフォルダを暗号化指定する」の項を参照してください。(Windows XP/2000のみ)



個別暗号モードインストール

InfoCage モバイル防御は、インストール後の暗号化モード(ドライブー括暗号モード または 個別暗号モード)を InfoCage モバイル防御の管理者により選択することができます。

「個別暗号モード」に設定されたセットアッププログラムを使用した場合、インストールを完了し再起動した後は、本章の それぞれの認証方式の説明にしたがって操作してください。

🗛 Notice

何らかの理由で暗号化ウィザートを終了した場合、再度暗号化ウィザードを起動するには、スタートメニューから [すべてのプログラム]-[NEC]-[InfoCage モバイル防御]-[InfoCage モバイル防御 ユーティリティ]をクリックします。

4.1 メディア鍵認証方式の場合

🗞 Operation

 Windows Vista の場合は再起動後に、以下の画面が表示されます。 [OK]をクリックしてください。

nfoCage/モバイル防	9		
htoCage/モバイル	防御 ユーラ	ィリティを起動	りします。
\$0000C97P1			
	_		
(CON		赤いたり	

A Notice

[キャンセル] をクリックすると、本プログラムが終了します。その場合は、後で必ず再度暗号化ウィザード を起動して、パソコンの鍵を作成および暗号化を行ってください。

2. スーパーバイザパスワード入力画面が表示されます。 インストール時に設定したスーパーバイザパスワードを入力し、[OK]をクリックしてください。

	2			
6	InfoCage/モ	パイル本法律 Ve	rsion	
スーパー	544127-	ドを入力してく	だおい	

3. 設定のご案内が表示されます。[次へ]をクリックしてください。

[Step1、パソコンの鍵を作成
l	
[Step2. パソコンの保護設定
	Step3. 暗号化の設定

パソコンの鍵の作成に関する説明が表示されます。
 内容を確認して準備ができたら、[次へ]をクリックしてください。

Step1Jでソコンの構を	ag		
パンロントの観察的のない	\$ 7 .		
公司·均规数10.5	3/7:75.898	目前するシア・アガモりそれ。	ALL A
NTL BYTER	CERL TOTAL	L	rymy yme
and the second state			
		28-480	キャンセル

5. [パソコン用の鍵を新規作成] が選択されています。ドライブ一覧に、内蔵ハードディスクドライブ以外のドラ イブが表示されている場合はチェックをはずしてください。 鍵を作成するメディアを装着し、[次へ]をクリックしてください。

(第四十三十四日年119年119年11月)	0. 0.
* (C/C/HOM/HOM/HOM/	No two-rg

🛕 Notice

- システムドライブのチェックは外せません。
- 内蔵ハードディスクドライブは必ずチェックしてください。
 内蔵ハードディスクドライブのチェックを外すと、その内蔵ハードディスクドライブへのデータのコピー、
 移動およびファイルの新規作成ができなくなったり、その内蔵ハードディスクドライブにインストールされたアプリケーションが正しく動作しなくなったりする場合があります。
- 内蔵ハードディスクドライブではないドライブのチェックは必ずはずしてください。
 内蔵ハードディスクドライブではないドライブにチェックをつけると、そのドライブを取り外した際に動作が不正になる場合があります。

6. [鍵を格納するメディアまたは共有フォルダ]の[選択]をクリックしてください。

MONE .	
#E00170/F472	または非有フォルダを推定してくだろい。
menon roof of	P\$151\$F\$\$12+1-0
	Aller()
~	THORE AND AND

🛕 Notice

以下では1つの鍵を作成する方法を説明します。 合成鍵を作成する場合は、「InfoCage モバイル防御 ユーザーズガイド」の「合成鍵を作成する」の項を 参照してください。(合成鍵は Windows XP/2000 のみ作成できます。) 7. [メディア(ドライブ)の選択]を選択し、ドライブー覧から鍵を作成するメディアのドライブを選択して[OK]を クリックしてください。

(ここでは例として E ドライブとします)

メディアの温沢	
● 29-771F9-F3Xの撮評(M) E× -	
② キットワークの共有フォルダの運搬(S)	
	(例题(B)
0K +>ttp/]

8. [次へ]をクリックしてください。

illonit.			
#850H752947	または本州和フォルダを取取してい	58. v	
#850#75/94	「または同胞フォルダ		
E¥.		-C.912	6
	<用6(8)	31-130	ADA

9. 内容を確認後、[作成]をクリックしてください。

stores	
holderetend.tr.	
(実践り)協となるメディア PC[ORDH]	
線を局約するパディアまた13月有フォルグ モモ目リムーバブル ディスク (1月)	
(Roup)	4+5456

10. 鍵の作成が完了しました。[OK]をクリックしてください。



11. 続いて鍵情報を保存します。

```
<スタンドアローンモードの場合>
鍵情報を保存するメディアを装着してください。
(ここでは例としてFドライブに保存します)
外部メディア(ドライブ)一覧に鍵情報を保存するメディアが見つからない場合は、 [更新] をクリックして
ください。
```

鍵情報の保存先メディアを選択し、[次へ]をクリックしてください。



<ネットワークモードの場合>

鍵情報をサーバに保存します。保存場所を確認して、[次へ]をクリックしてください。



12. 鍵情報の保存が完了しました。[OK]をクリックしてください。

<スタンドアローンモードの場合>

A Notice

InfoCage/モバイル防御	
() Fドライブに動物	を保存しました。
	ОК

<ネットワークモードの場合>



13.パソコンの保護に関する設定画面が表示されます。

<Windows Vista の場合>

データの抜き取り防止設定をする場合は、[メディアへのコピーを禁止する]のチェックを入れて[次へ]を クリックしてください。

WP2パンコンの保護	10
パールンの理由ことで、説明します。 これらの説明主張からあらGan、キバイル目前国ユーティリティ	TREFSCEPTERT.
109777-002-88215	
24-0	4+545A

A Notice

- ・ InfoCage モバイル防御の管理者の設定により外部メディア自動暗号が有効になっている場合、[メディアへのコピーを禁止する]は操作できません。
- ・ 外部メディア自動暗号が無効になっている場合、ここにチェックをするとすべての外部メディアへの データのコピーができなくなります。

<Windows XP/2000の場合>

あらかじめ[パソコンの鍵がないときはパソコンをロックする]にチェックが入っています。 データの抜き取り防止設定をする場合は、[認証されていないメディアへのコピーを禁止する]のチェックを 入れて[次へ]をクリックしてください。

Step? パソコンの目調	8
パンピンの保護について、設定します。 これられ後期140からからのロングパイルが加ユーティリティで設定することができます。	
○正立の規模など表示して、地方力学を ○正規約れたもいディアへのピーを集まする	
3080 4+206)

A Notice

- ・ 通常は[パソコンの鍵がないときはパソコンをロックする]のチェックを入れて使用してください。
 このチェックを外す場合は、「InfoCage モバイル防御 ユーザーズガイド」の「パソコンのロック」の項を 参照してください。
- ・ InfoCage モバイル防御の管理者の設定により外部メディア自動暗号が有効になっている場合、[認証 されていないメディアへのコピーを禁止する]はチェックできません。

14. 設定内容の確認画面が表示されます。[OK]をクリックしてください。



A Notice

- ・ 設定内容によっては、上記の画面に表示される内容が異なる場合があります。
- これ以降、設定内容が適用されます。
 Windows Vista の場合、メディアへのコピーを禁止した場合は、メディアへの書き込みができません。
 Windows XP/2000 の場合、パソコンをロックする設定をした場合は、鍵を抜くとパソコンがロックされます。ロックを解除し、ログオンするには鍵を装着してください。
 また、認証されていないメディアへのコピーを禁止した場合は、認証されていないメディアへの書き込みができません。

15. 暗号化指定に関する説明が表示されます。 内容を確認して準備ができたら、[次へ]をクリックしてください。

Step3.增考化推定	4
haceae/モレイム結構ユーティンティを使って様常な加定をします。 様式のコンドログロクターをつかり、そく加工法の内容でわられないと、 などのコンドログロクターをつかったが、していた。 などのクログロクターをつくためでは、ことになった。	7058.5
	4+5454

16. [暗号化指定]タブが表示されます。[追加]をクリックしてください。

<Windows Vista の場合>

#書記を記録の読得するのです。通知になる意思の公式(Main excent)での 通用できませんでいるつきからな	0 0
■単化注意用用していらう+ルメダ	
電電電路電影等語法 編集等を確認系統的escence	
THE AND THE SALE AND THE T	1000
基金融新活动的名词复数 建型合体建立合体的 escoment	29(2)
BREAM STREET BERTS (BREAM) over om o	
電能設施設時外設計。編集的多確認為認識in extenut	
REALTING REST CONTRACTOR	
REALTHYSE RESS COMMENCE.	
REFERENCEST FOR A REFERENCE FOR THE FOURIER STATES	
	0036.6
	417

A Notice

- ・ InfoCage モバイル防御の管理者によって暗号化するドライブやフォルダがあらかじめ設定されている 場合は、そのドライブやフォルダが[暗号化を指定しているフォルダ]に表示されています。
- ・ 他に暗号化設定するドライブやフォルダがない場合は、18へ進んでください。

<Windows XP/2000の場合>

日本日本日本日本日本1140つ。	M	
	me.	() () () () () () () () () () () () () (
		829.0
		Die D
AND REAL PROPERTY AND INCOME.	出版物	いたまし、 からの時間の年3にき用していたれ、
制品的研究		
単年に日本部では年7年で 単年にと知识するフォル ロザスクトップ	0 DV/P#asC#	0-0-9-3-1-402-0

以下のフォルダを暗号化する場合は、[暗号化を推奨するフォルダ]内のチェックボックスにチェックを入れ てください。

・デスクトップ ・マイドキュメント ・インターネットー時ファイル

🛕 Notice

- デスクトップを暗号化または復号した場合、デスクトップの表示が不正になる場合があります。その場合 はデスクトップの任意の場所をクリックし、[F5]キーを押すと正常に戻ります。また、アイコンの並びが 変更される場合がありますが、その場合は手動で並び替えてください。
- ・ InfoCage モバイル防御 管理サーバが導入されている環境で、InfoCage モバイル防御の管理者によって暗号化するドライブやフォルダがあらかじめ設定されている場合は、そのドライブやフォルダが [暗号化を指定しているフォルダ]に表示されています。
- ・ 他に暗号化設定するドライブやフォルダがない場合は、18へ進んでください。

17.暗号化したいドライブまたはフォルダを選択し、[OK]をクリックしてください。



18. [暗号化を指定しているフォルダ]に選択したフォルダが追加されます。 複数のフォルダを指定したい場合は、*16 ~ 17* を繰り返してください。 また、暗号化したいドライブおよびフォルダを解除する場合は、[解除]をクリックしてください。 ドライブやフォルダを指定し終わったら[適用]をクリックしてください。

InfoCage/モバイル防御 ユーディリティ	
金統 網の保護 程序化指定	
相号化学相信U、C1-0Da 6-5 ⁴ Definition	87930. 629(2)
	ส่งระสะบารสา
	#+5±50 . #7

A Notice

- すでに暗号化したドライブやフォルダがある場合、そのドライブやフォルダ名も表示されていますが、それらを[解除]後、[適用]または[終了]を実行するとそれらのフォルダは復号されますのでご注意ください。
- ・ [適用]をクリックすると、暗号化処理が終了するまで暗号化指定しているドライブおよびフォルダには アクセスできなくなります。([一時停止]をクリックしても同様です)
- ・ ここで[終了]をクリックすると、指定したドライブおよびフォルダの暗号化を実行後に、InfoCage モバイル防御ユーティリティが終了します。

19. 暗号化処理に関する注意事項が表示されます。

常駐アプリケーションや起動しているアプリケーションがあれば必ず終了し、[はい]をクリックしてください。



A Notice

アプリケーションが使用しているファイルは、暗号化できない場合があります。

20.ごみ箱の暗号化に関する注意事項が表示されます。 内容を確認して、[OK]をクリックしてください。

128	
「ごみ場」を増考化します。	
パンコンに初めて暗号をファルタが落空されましたので、同時にごみ 化します、ごみ幅に大量のファイルが入っている場合は暗号にに開始 ことがありますので、ここで見にしておくことを影響のします。 ごろ幅を思いまるとは、デスクトップのごみ得アイコンをおクリック(み得を思いする)を選択してください。	#を増号 がかめる して「ご
	OK

🛕 Notice

・ 暗号化するフォルダ内のファイル数が多い場合、暗号化に時間がかかる場合があります。
 またごみ箱に大量のファイルが入っている場合は暗号化に時間がかかることがありますので、あらかじめごみ箱を空にしておくことをお奨めします。

21. [開始]をクリックすると、暗号化処理が始まります。

設定したり目を対象フォルテに反映します。	開始がおった押してのだちり。
82088	
円塗りまんり:	
0810	
	44

A Notice

暗号化するフォルダ内のファイル数が多い場合、暗号化に時間がかかる場合があります。

22. 暗号化処理中です。しばらくお待ちください。

P InfoCage./1E/11/1.858	-0-10014
思想中です。 しばらは持ち下さいー	
	500 / 100
85088	
1世間フォルボ: GWhojactWDatel	
思想内容: 暗号化	
-4944_ 2001	

23.暗号化処理が終了しました。暗号化できなかったファイルがある場合はウィンドウ内に表示されます。 [終了]をクリックしてください。

@InfoCage/%/11/1888	-ce00 -
Million,	
10.000	
Fim 200.7:	
56742	
48412/18428535-229-1628081846.	1
MY NUCT	

🛕 Notice

・ 暗号化できなかったファイルがあった場合は、起動しているアプリケーションがあれば終了し、[再試行]をクリックしてください。

すべての起動中のアプリケーションを終了して[再試行]をクリックしても暗号化できなかったファイルが ある場合、そのファイルはオペレーティングシステムのサービス等で優先的に使用されているため、暗 号化できません。これらのファイルは本ソフトウェア内で暗号化できなかったファイルとして登録される ため、暗号化対象フォルダ内にあっても、動作に問題はありません。

- ・ 暗号化対象外ファイルについては、暗号化できなかったファイルの一覧には表示されません。
- ・ 暗号化対象外ファイルについては、「InfoCage モバイル防御 ユーザーズガイド」の「「暗号化指定」 タブ」の項を参照してください。



24. [暗号化を指定しているフォルダ]に暗号化されたフォルダが表示されます。 これで暗号化の作業は終了です。[終了]をクリックしてください。

その他の設定に関しては、「InfoCage モバイル防御 ユーザーズガイド」を参照してください。

4.2 パスワード認証方式の場合



Windows Vista の場合は再起動後に、以下の画面が表示されます。
 [OK]をクリックしてください。

InfoCage/モバイル防御	
InfoCage/モノ「イル版方面: よろしいですか?	ユーティリティを起動します。
С	キャンセル

🛕 Notice

[キャンセル] をクリックすると、本プログラムが終了します。その場合は、後で必ず再度暗号化ウィザード を起動して、パソコンの鍵を作成および暗号化を行ってください。

Windows XP の場合、セキュリティチップ(TPM)搭載のパソコンをお使いでセキュリティチップ(TPM)が有効になっていると、InfoCage モバイル防御の管理者の設定によっては、下記の画面が表示される場合があります。



セキュリティチップ(TPM)を使用する場合は [使用する] を、使用しない場合は [使用しない] を、後で 選択する場合は[キャンセル]をクリックしてください。

[キャンセル] をクリックした場合、TPM の使用を選択するまで InfoCage モバイル防御ユーティリティの 起動時にメッセージが表示されます。

A Notice

セキュリティチップ(TPM)に関しては、本ガイドの「第10章セキュリティチップ(TPM)搭載のパソコンをお 使いの場合」を参照してください。

3. 暗号化処理に関する説明が表示されますので、必ず内容を確認し、[OK]をクリックしてください。



4. [暗号化指定]タブが表示されます。[追加]をクリックしてください。

<Windows Vista の場合>

1127-ド 相考と指定		
増考化を推定しているフォルダ		
		385000
		#29(2)
		12
#\$9246/28000000	「日本のため」のである。	
ALAICEMPTOR OF STOL	100.141.9 200.4 20-0 0600	POCARCIOSAL

🛕 Notice

 InfoCage モバイル防御の管理者の設定により外部メディア自動暗号機能が有効の場合、システムドラ イブを除く暗号化フォルダの指定がない内蔵ハードディスクドライブは、外部メディアと同じ扱いとなり、 その内蔵ハードディスクドライブへはデータのコピー、移動およびファイルの新規作成ができなくなりま す。

また、その内蔵ハードディスクドライブにインストールされたアプリケーションが正しく動作しない場合がありますので、すべての内蔵ハードディスクドライブに暗号化フォルダを作成してください。

- ・ InfoCage モバイル防御の管理者によって暗号化するドライブやフォルダがあらかじめ設定されている 場合は、そのドライブやフォルダが[暗号化を指定しているフォルダ]に表示されています。
- ・他に暗号化設定するドライブやフォルダがない場合は、6へ進んでください。

<Windows XP/2000 の場合>

/ Mobile Protect 2039	- FBI 1-94974	
1032-F1 (00000) 10 - 0 9 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	4tax	(영영). (2010)
 ・ ・ ・	503. (#8145,498,7 037. 1999: 0.0448,7 0 07474x354	1140
	49.9	(

以下のフォルダを暗号化する場合は、[暗号化を推奨するフォルダ]内のチェックボックスにチェックを入れ てください。

・デスクトップ ・マイドキュメント ・インターネットー時ファイル

A Notice

- InfoCage モバイル防御の管理者の設定により外部メディア自動暗号機能が有効の場合、システムドラ イブを除く暗号化フォルダの指定がない内蔵ハードディスクドライブは、外部メディアと同じ扱いとなり、 その内蔵ハードディスクドライブへはデータのコピー、移動およびファイルの新規作成ができなくなりま す。また、その内蔵ハードディスクドライブにインストールされたアプリケーションが正しく動作しない場 合がありますので、すべての内蔵ハードディスクドライブに暗号化フォルダを作成してください。
- デスクトップを暗号化または復号した場合、デスクトップの表示が不正になる場合があります。その場合 はデスクトップの任意の場所をクリックし、[F5]キーを押すと正常に戻ります。また、アイコンの並びが 変更される場合がありますが、その場合は手動で並び替えてください。

- ・ 管理サーバが導入されている環境で、InfoCage モバイル防御の管理者によって暗号化するドライブ やフォルダがあらかじめ設定されている場合は、そのドライブやフォルダが[暗号化を指定しているフォ ルダ]に表示されています。
- ・ 他に暗号化設定するドライブやフォルダがない場合は、6へ進んでください。

5. 暗号化したいドライブまたはフォルダを選択し、[OK]をクリックしてください。



6. [暗号化を指定しているフォルダ]に選択したフォルダが追加されます。
 複数のフォルダを指定したい場合は、4~5 を繰り返してください。
 暗号化したいドライブおよびフォルダを解除する場合は、[解除]をクリックしてください。
 すべて指定し終わったら[適用]をクリックしてください。

12.0-F 様年と指定 様年化活発記しているフォルグ	
An Angelon (476(5). 629(5)
REALSON CONTRACTOR	ROCENTURES 6

A Notice

- すでに暗号化したドライブやフォルダがある場合、そのドライブやフォルダ名も表示されていますが、 それらを[解除]後、[適用]または[終了]を実行するとそれらのフォルダは復号されますのでご注意 ください。
- ・ [適用]をクリックすると、暗号化処理が終了するまで暗号化指定しているフォルダにはアクセスできなくなります。(暗号化処理を実行中に[一時停止]をクリックしても同様です)
- ・ ここで[終了]をクリックすると、指定したフォルダの暗号化を実行後に、InfoCage モバイル防御ユーティリティが終了します。

7. 暗号化処理に関する注意事項が表示されます。 常駐アプリケーションや起動しているアプリケーションがあれば必ず終了し、[はい]をクリックしてください。



🛕 Notice

アプリケーションが使用しているファイルは、暗号化できない場合があります。

8. ごみ箱の暗号化に関する注意事項が表示されます。 内容を確認して、[OK]をクリックしてください。

18	
「ごみ福」を除きたします。	
Cドライブに初めて線号をフォル 化します。ごみ場に大量のファイ ことがありますので、ここで至ら ごみ場を型にするには、デスクト み場を型にする」を選択してくた	ダが後生されましたので、高時にごみ場を接号 小が入っている場合は障害化に時間がかかる いておくことをお知らします。 ップのごみ場アイコンを取りリックして「ご さい。
	OK

🛕 Notice

- ・ 暗号化するフォルダ内のファイル数が多い場合、暗号化に時間がかかる場合があります。
 またごみ箱に大量のファイルが入っている場合は暗号化に時間がかかることがありますので、あらかじめごみ箱を空にしておくことをお奨めします。
- 9. [開始]をクリックすると、暗号化処理が始まります。

MoCage/E/14/L898	-c0- -
設定した内容を対象つきんがに影映します。 IN	除されたこを押していたちに、
Raced	
月童296年:	
8/8/10:	
	Access .

🛕 Notice

暗号化するフォルダ内のファイル数が多い場合、暗号化に時間がかかる場合があります。

10.暗号化処理中です。しばらくお待ちください。

InfoCage./1E/14/1488	0-0-0-0
影躍中です。 しばら(法領ち下さ)	
	500 / 1000
82088	
月豊から方: GithspectWorld	
机槽内容	
the second se	

11. 暗号化処理が終了しました。

暗号化できなかったファイルがある場合はウィンドウ内に表示されます。 [終了]をクリックしてください。

anotage Entritate		
	利了しました。	
Ranse		
31歳2まんが:		
8/8/101		
4442/4428555227	H.6280#16	

🛕 Notice

・ 暗号化できなかったファイルがあった場合は、起動しているアプリケーションがあれば終了し、[再試 行]をクリックしてください。

すべての起動中のアプリケーションを終了して[再試行]をクリックしても暗号化できなかったファイル がある場合、そのファイルはオペレーティングシステムのサービス等で優先的に使用されているため、 暗号化できません。これらのファイルは本ソフトウェア内で暗号化できなかったファイルとして登録され るため、暗号化対象フォルダ内にあっても、問題はありません。

- ・暗号化対象外ファイルについては、暗号化できなかったファイルの一覧には表示されません。
- ・ 暗号化対象外ファイルについては、「InfoCage モバイル防御 ユーザーズガイド」の「「暗号化指定」 タブ」の項を参照してください。

12. [暗号化を指定しているフォルダ]に暗号化されたフォルダが表示されます。 これで暗号化の作業は終了です。[終了]をクリックしてください。

線号化を設定しているフォルダ Accord	4700
	A29H2J
WERKSPECTE	FSC-EIFUTCEELL

その他の設定に関しては、「InfoCage モバイル防御 ユーザーズガイド」を参照してください。



A Notice

Windows XP/2000 の場合、アップグレードインストールを行う前に、InfoCage モバイル防御を使用するパソコンの環境を チェックしてください。

菱瓢◯ 環境のチェック方法は、「3.2.1 環境チェックユーティリティ Windows XP/2000 の場合」を参照してください。

● ご注意

すでにインストールされている InfoCage モバイル防御と同じバージョンの setup.exe を実行するとアンインストールのウィ ザードが起動しますのでご注意ください。その際は下記の手順にしたがって操作してください。



1. setup.exe を実行すると、[InstallShield(R)ウィザードを使うと、InfoCage モバイル防御を削除することができます。]と表示された場合は、[キャンセル]をクリックしてください。



2. [はい]をクリックしてください。



3. [完了]をクリックしてください。操作は以上です。



アップグレードインストールを行います。



1. InfoCage モバイル防御が格納されているメディア(例 CD-ROM)内の setup.exe を実行し、[次へ]をクリック してください。

2	このたびは、broCage モバイル部制御をご購入いただき、 まことに取りがたっこでいます。
Inte /C/J	age モディイル系列的は、パンパン・クロック、データの標準号化を行うことで、 ンからの情報業実体的上するための政治です。
わざい 東京	の明治に合わせて、USBメモルなどのリムーバブルメディアを継として使用する の確認な方式し、または、専用的バリワードを使用するバリバワード回望方式した なくシリボできます。
102	トールを開始するにはり次へ」を押してください。

2. インストールする InfoCage モバイル防御のプログラムの確認画面が表示されます。 [次へ]をクリックしてください。

は8日メモリなどのリムーリブルメディアを描述して使用する。 ドメディア機能量力気な高からCage モディル約増加のデップラレードインストールを行いま す。 専用的ロセワードを使用する 「パスワード気管力力」のAnoname モディル約増加、モインストールを打ち込め会社、 をいずれしていることのためのane モディル約増加、サインストールを打ち込め会社、 をいずれしていることのためのane モディルがありませいで、ストールを		《 · · · · · · · · · · · · · · · · · · ·
専用ないいつードを使用する 「パスワード問題を方式のからGase モリビイル形成の」をインストールされる場合は、 をいくからしていていたいの意味をとし、backGase モリビーの話録を見ていていた。 によ		USBメモル広とのリムーバラルメディアを開たして使用する 「メディア構築型は方式の自体のGase モドバネ活動的のアップラレードインストールを行いま す。
高価、インストールを行っていために		■用心にワードを使用する 「パレワード型協力式のAndocare Uドム新知道」をインストールされる場合は、 キャンセルドノマストールを中止し、Encoare Uドム新知道をアンインストール後、 構成、インストールを行ってたたい。
< 開め田 (液へ取り) キャンセル	1	< 第8(日) (二次へびの) キャンセル

画面はメディア鍵認証方式版です。

3. 確認メッセージが表示されます。[はい]をクリックしてください。

InfoCage モバイル的師	
② このセットアップは、Findcage モバー を見行します。他行しますか?	イル動動」のアップグレード
	and marked
▲ Notice	
アップグレードする InfoCage モバイル防御のバ	ージョンによっては、この画面は表示されませ

【導入前の注意事項】画面が表示されます。
 各項目をクリックすると詳細な説明が表示されますので、必ずお読みの上、チェックを付けてください。
 すべての確認が終わりましたら、[閉じる]をクリックしてください。

No. P A	
□ データがトックアップ ● 出来的の・ゲイオとはサートな事後 □ 年月ライジの没を含 □ 日本ではアシワテーションの確認った後 日本ではアンワテーションの確認った後 □ 日本ではアンワテーションの確認 □ 5% アッパートでないこと ■ 本部分のより後 □ 本が、クェンレートでないこと	

🛕 Notice

画面はメディア鍵認証方式の場合です。パスワード認証方式の場合は一部異なります。

5. すべての項目がチェックされていない場合は、下記のメッセージが表示されます。 インストールを続ける場合は [はい] を、インストールを中止する場合は [いいえ] を、**4** の画面に戻る場 合は [キャンセル]をクリックしてください。

1 1	ての項目がチ	エックされて	WETL-
- 12	AP-WER	12. 9.17.1	
_			

6. [次へ]をクリックしてください。



🛕 Notice

お使いのバージョンによっては[InfoCage モバイル防御用のInstallShieldウィザードを続行しています]と 表示されますので、7 または9 または10 へ進みます。 7. [運用形態の選択] 画面で、運用形態の選択をし、[次へ]をクリックします。

運用影響の灌漑		
運用影響を選択してください。		
■ スタンドアローンモード(S) ○ ネットワークモード(S)	1	
注意 セットアップ(動まキットワー 行することはできません。 移行するためコよ、一旦7 があります。	- クモードからスタンドアローンモードに移 アンインストールする必要	
InstallShield	< 80.00 \ 260.00 \	dan't da

🛕 Notice

- ・ アップグレードする InfoCage モバイル防御のバージョンによっては、この画面は表示されません。
- スタンドアローンモードを選択した場合は 9 へ。
- 8. 《ネットワークモード》を選択した場合、クライアント認証画面が表示されるので、クライアント ID、管理 サーバの URL を入力して、「次へ」をクリックしてください。

InfoCage モバイル初即 - Inst	tallShield Wizard	
使理サーバでクライアントを認証し	±7.	
InfoCage も/パル防御管理者た よびサーバのJALを入力してくささ ※クライアントIDはクライアントごと	時入手したクライアントのお くし に見たります。	
クライアント名:		
からアントDQ:		
管理サーバのURL(U);		
[
altheid		
	< 戻る(8) 次へ	(N) > #width

🛕 Notice

- ・ アップグレードする InfoCage モバイル防御のバージョンによっては、この画面は表示されません。
- ・ スタンドアローンモードの場合、この画面は表示されません。
- ・ InfoCage モバイル防御の管理者がクライアント登録をしていない場合は認証されません。 認証に失敗した場合は、クライアント名、クライアント ID、管理サーバの URL を確認後、InfoCage モバイル防御の管理者に問い合わせてください。
- ・ その他の理由で認証に失敗した場合は、以下を参照してください。

参照 第11章 トラブルシューティング (2)

9. [インストール]をクリックしてインストールを開始してください。



10. インストール中です。しばらくお待ちください。



11. インストールが完了すると下記の画面が表示されます。 [完了]をクリックしてください。



12. InfoCage モバイル防御を使用可能にするためには、パソコンを再起動する必要があります。 他のプログラムを実行中の場合は、終了させてください。 [OK]をクリックすると、パソコンが再起動します。

1 InfoCag	e モバイル防御 セットアップ	
⚠	コンピュータを再起動します。 他のプログラムを実行中の場合は「OK」をグリックする 朝に林了させてびたい。 OK	5

13. Windows XP/2000 の場合、お使いのバージョンによっては、再起動後に表示されるパスワード入力画面で スーパーバイザパスワードまたはユーザパスワードを入力すると、下記のメッセージが表示される場合があ ります。内容を確認し、[はい]をクリックしてください。



🛕 Notice

暗号化を後で行う場合は[いいえ]をクリックしてください。 [いいえ]をクリックした場合、暗号化が完了するまでは InfoCage モバイル防御 ユーティリティを起動する ごとにメッセージが表示されます。

14. 暗号化が完了すると下記のメッセージが表示されますので、[OK]をクリックし、InfoCage モバイル防御 ユーティリティを終了してください。

暗号化の	完了 🔀
()	暗号化が完了しました。
	OK

以上で操作は完了です。

第6章 ログオン方法

InfoCage モバイル防御をインストールすると、Windows のログオン方法が変わります。 以下を行うことでセキュリティ認証を行い、Windows ヘログオンしてパソコンを操作できるようになります。

● メディア鍵認証方式の場合

鍵となるメディア等をパソコンに装着することでセキュリティ認証を行います。 (鍵となるメディア等は、鍵の作成の完了後に装着が必要となります。 InfoCage モバイル防御のインストール後に初めてWindows にログオンする際は、通常のログオンとなります。)

● パスワード認証方式の場合

InfoCage モバイル防御のユーザパスワードを入力することでセキュリティ認証を行います。

以下の手順で Windows ヘログオンします。

6.1 メディア鍵認証方式の場合

起動しているパソコンから鍵を抜いた場合、または鍵を抜いたままパソコンを起動した場合は、パソコンがロックされた 状態になります。

🛕 Notice

- ・ 鍵を作成していない場合は、パソコンをロックできません。
- ・ パソコンのロック機能のみでは情報漏洩対策は万全ではありません。重要なファイルは必ず暗号化してください。
- ネットワークの共有フォルダの鍵を使用する場合は、InfoCage モバイル防御のセキュリティ認証からWindows ヘログオンしてください。他の認証方法でWindows ヘログオンした場合はいったんログアウトし、InfoCage モバイル防御のセキュリティ認証からログオンしなおすと、シャットダウン時までネットワークの共有フォルダの鍵が有効になります。

■ Windows Vista の場合

🗞 Operation

1. InfoCage モバイル防御のボタンをクリックします。



2. 鍵となるメディアをパソコンに装着して Windows のユーザ名およびパスワードを入力して ● をクリック、 または Enter キーを押すと、Windows ヘログオンすることができます。



A Notice

ドメインに参加している場合は[ワークグループ名/ドメイン名]にドメイン名を入力してください。 (ワークグループの場合は空欄でも可。)

●ユーザ情報エラーの場合

メディア鍵認証方式の場合は鍵を抜いた状態、パスワード認証方式の場合は誤ったユーザパスワードでログ オンしようとすると、[Windows のユーザ情報、または InfoCage モバイル防御の認証情報が違います。] と表 示され、Windows ヘログオンできません。

[OK]をクリックして、2に戻って操作してください。



■ Windows XP/2000の場合

● 起動しているパソコンから鍵を抜いた場合

1. 起動しているパソコンから鍵を抜くと、[コンピュータのロック] 画面が表示され、パソコンがロックされた状態になります。

	Windows ^{xp}
Ř	progra c. proc. del Microsoft Innell Corporation Microsoft
3	このコンピューダはロックされています。 Group1¥Uper1(Uper1)または管理者のみがこのコンピュータのロックも解除できます
	このコンパッーカのロックを検討をするには Carle Alle Dail キーを押してくだろい。

▲ Notice Windows の設定によっては、[コンピュータのロック]画面は表示されない場合があります。

2. 鍵を抜いた状態でログオンしようとすると、以下の画面が表示され、ログオンできません。

Ì	コンピュータのロック
	コンピュータはロックされています。 鍵を使ってロックを解除してください
	再試行 キャンセル

3. 鍵を装着して[再試行]をクリックすると、[コンピュータのロックの解除]画面が表示され、パスワードを入力 するとロックが解除され、ログオンすることができます。



● 鍵を抜いた状態でパソコンを起動した場合

1. パソコンを起動すると[Windows へようこそ] 画面が表示されます。



🛕 Notice

Windowsの設定によっては、[Windows へようこそ]画面は表示されない場合があります。

2. 鍵を抜いた状態でログオンしようとすると、以下の画面が表示され、ログオンできません。



3. 鍵を装着して[再試行]をクリックすると、[Windows ヘログオン]画面が表示され、パスワードを入力すると ロックが解除され、ログオンすることができます。

Windows A D	A Wind	ows ^{xp}
ユーザー名(2) パスワード(2) ログオン(40)	Res 2001	Microsoft
arriver.	OK 4+545	2001372/00 (17902/00 ()



■ Windows Vista の場合

🗞 Operation

1. InfoCage モバイル防御のボタンをクリックします。



2. Windows のユーザ名およびパスワード、InfoCage モバイル防御のユーザパスワードを入力して Seply クするか、Enter キーを押すと、Windows ヘログオンすることができます。



🛕 Notice

ドメインに参加している場合は[ワークグループ名/ドメイン名]にドメイン名を入力してください。 (ワークグループの場合は空欄でも可。) ●ユーザ情報エラーの場合

誤ったユーザパスワードを入力すると、[Windows のユーザ情報、または InfoCage モバイル防御の 認証情報が違います。] と表示されログオンできません。 [OK]をクリックして、**2** に戻って操作してください。



🛕 Notice

ユーザパスワードを5回誤って入力すると、パソコンがロックアウトされます。その場合はパスワード入力 画面が有効になるまでしばらくお待ちください。

■ Windows XP/2000の場合

1. 再起動後に、通常のログオン画面が表示されます。 Ctrl+Alt+Delキーを押してください。



A Notice

Windows の設定によっては、[Windows へようこそ] 画面は表示されない場合があります。

2. ユーザパスワード入力画面が表示されます。 インストール時に設定したユーザパスワードを入力し、[OK]をクリックしてください。

InfoGage/	E八子赤肋御
2	httoCage/モバイル防御のバスワードを 入力してください。
]
	0K キャンセル

A Notice

ユーザパスワードを5回連続で誤って入力すると、[OK]がクリックできなくなります。 その場合は [シャットダウン] をクリックしていったんシャットダウンした後、再度パソコンを起動してパスワ ード入力画面が有効になるまでしばらくお待ちください。 (すぐにパソコンを起動しても一定時間パスワードの入力はできません。)

3. [Windows ヘログオン] 画面が表示され、ユーザ名と Windows ログオンパスワードを入力すると ログオンすることができます。

	💾 Win	dows ^{xp}
2-7-800	Set of the	Microsoft
パスワード(12)		

第7章 特定の FeliCa カードの設定

Windows XP/2000 の場合、InfoCage モバイル防御をパスワード認証方式で運用しログオン認証に特定の FeliCa カード を使用するためには、システムコード(FeliCa カードに割り当てられている固有のコード)を適用する必要があります。 インストール後にシステムコードを適用する場合は、システムコード適用ツールを使用します。 本設定は InfoCage モバイル防御の管理者の指示にしたがって操作してください。

🛕 Notice

- 本ツールは Windows XP/2000 用の InfoCage モバイル防御 Ver3.5 以降がインストールされたパソコンで動作します。
 Windows Vista 用 InfoCage モバイル防御には FeliCa 認証機能はありません。
- ・ InfoCage モバイル防御の管理者によって FeliCa カードのシステムコードが設定されたセットアッププログラムでインストールした場合は、本設定は不要です。
- ・ システムコード適用ツールは、コンピュータの管理者のユーザで実行してください。
- ・ FeliCa カード認証は InfoCage モバイル防御をメディア鍵認証方式で運用している場合は使用できません。

🏷 Operation

- InfoCage モバイル防御の管理者から配布された mbscd.dat ファイルを、InfoCage モバイル防御をインストールしたフォルダ(通常は ¥Program Files¥NEC¥InfoCageCE)内の¥Tools フォルダ内にある NmlStScd.exe と同じ場所に保存してください。
- 2. NmlStScd.exe を実行し、[OK]をクリックします。



3. システムコードが適用されました。[OK]をクリックしてください。

システムコード連用ツール 🔀
道用に成功しました。
ОК

以上で終了です。

FeliCa カードの設定方法は、「InfoCage モバイル防御 ユーザーズガイド」の「「認証設定」タブ」の項を 参照してください。(パスワード認証方式のみ)


InfoCage モバイル防御 ユーティリティの起動方法を説明します。

🗞 Operation

- 1. スタートメニューから、[すべてのプログラム] [NEC] [InfoCage モバイル防御] [InfoCage モバイル防御 ユーティリティ]をクリックします。
- **2.** Windows Vista の場合は以下の画面が表示されます。 [OK]をクリックしてください。

ioCage/モバイル防御	
InfoCage/モバイル防御 よろしんいですか?	ユーティリティを起動します。
(ROK	キャンセル

3. メディア鍵認証方式の場合は、鍵をパソコンに装着してからスーパーバイザパスワードを入力し、[OK]を クリックしてください。

パスワード認証方式の場合は、ユーザパスワードを入力し、[OK]をクリックしてください。 InfoCage モバイル防御ユーティリティが起動します。



A Notice

上記の画面はメディア鍵認証方式のものです。パスワード認証方式の場合は一部表記が異なります。

● InfoCage モバイル防御 ユーザーズガイドを参照するには

スタートメニューから、[すべてのプログラム] – [NEC] – [InfoCage モバイル防御] – [InfoCage モバイル防御 ユーザーズガイド]をクリックしてください。

第9章 時限消去機能について

時限消去機能を使用するためには[時限消去機能設定ツール]で有効にする必要があります。 以下の手順にて有効にしてください。

🛕 Notice

- 時限消去機能は Windows XP/2000 のみの機能です。
- ・ InfoCage モバイル防御がインストールされたパソコン上での操作手順です。

🗞 Operation

- **1.** クライアントCD-ROM内の¥2K_XP¥Tools¥時限消去機能設定ツール フォルダにあるEnableTBM.exeを実行してください。
- 2. メッセージが表示されますので[はい]をクリックしてください。

時限消去機能設定ツール 🔣		
時限済去様能を有効にします。 よろしいですか?		
ແທນ	000200	

3. [OK]をクリックしてください。

局限消 法	機能設定ウール	
1	時限消去標範を有効に設定	しました。
	OK	

以上で終了です。

時限消去機能の設定方法は、「InfoCage モバイル防御 ユーザーズガイド」の「「時限消去設定」タブ」の項を参照してください。

第10章 セキュリティチップ(TPM)搭載のパソコンをお使いの場合

セキュリティチップ(TPM: Trusted Platform Module)とは、PC プラットフォームにおけるセキュリティ技術の業界団体 TCG (Trusted Computing Group)が策定した仕様に準拠した IC チップで、これを使用することにより、様々なセキュリティ機能 を利用することが可能になります。

Windows XP をお使いの場合は、InfoCage モバイル防御のパスワード認証方式でセキュリティチップ(TPM)の機能を使用することにより、さらに強固なセキュリティを実現できます。

セキュリティチップ(TPM)を使用する場合は、InfoCage モバイル防御の管理者がカスタマイズしたセットアッププログラム を使ってインストールしてください。

■ セキュリティチップ(TPM)の使用について

セキュリティチップ(TPM)を有効に設定したセットアッププログラムを使ってインストールした場合は、セキュリティチップ (TPM)を使用するかを選択することができます。

セキュリティチップ (TPM)を有効にするには、BIOS セットアップでセキュリティチップを [使用する] にし、セキュリティチッ プユーティリティをインストールしてください。

🛕 Notice

セキュリティチップ(TPM)の設定方法についてはお使いのパソコンのマニュアルを参照してください。

InfoCage モバイル防御のパスワード認証方式をインストール後、InfoCage モバイル防御 ユーティリティの起動時に下記 のメッセージが表示されます。

セキュリティチップ(TPM)を使用する場合は[使用する]を、使用しない場合は[使用しない]を、後で選択する場合は [キャンセル]をクリックしてください。

[キャンセル]をクリックした場合、TPMの使用を選択するまで InfoCage モバイル防御 ユーティリティの起動時にメッセージが表示されます。



注意事項

- ・セキュリティチップ(TPM)を使用するには、InfoCage モバイル防御のパスワード認証方式をインストールする前に セキュリティチップ用ドライバおよびユーティリティがインストールされている必要があります。
- ・BIOSのアップデートなどで設定値を初期化した場合、アップデート後にセキュリティチップの値を必ず元に戻して ください。
- ・セキュリティチップ(TPM)を使用している場合、セキュリティチップユーティリティをアンインストールしないでください。 アンインストールすると暗号化されたファイルにアクセスできなくなります。
- ・セキュリティチップ(TPM)を使用している場合、BIOSでセキュリティチップを [使用しない] に設定を変更したり、設 定値の初期化をしたりすることは絶対にしないでください。これらの操作を実行した場合、暗号化されたファイルに アクセスできなくなります。

第11章 トラブルシューティング

(1)	インストール時に「1607:InstallShield Scripting Runtime をインストールできません。」というメッセージが表示され、 インストールできない。		
この	このエラーは、InstallShield が次のような原因で正常に動作していないときに表示されます。		
1.	管理者権限のないユーザでログオンしている。 インストールする際のユーザ権限は、コンピュータの管理者(Administrator 権限)で行ってください。		
2.	IDriver.exe が正しく登録されていない。 Windows のコマンドプロンプトから以下のコマンドを実行して、IDriver.exe を登録しなおしてください。 ¥Program Files¥CommonFiles¥InstallShield¥ <u>Driver¥7¥Intel32</u> ¥IDriver.exe/REGSERVER(注1) ※ Windows が Cドライブにインストールされている場合の例です。 それ以外のドライブにインストールされている場合には、該当するドライブ文字に置き換えてください。 ※ 下線部はお使いの環境によって異なる場合があります。		
3.	同時に複数のインストーラが起動している。 誤って setup.exe を複数実行してしまった場合、いったんすべてのインストーラを終了してから、再度インストールを 行ってください。		
4.	 Windows インストーラ(msiexec.exe)が正しく登録されていない。 任意の場所(デスクトップ等)に[新規作成]でテキストファイルを作成し、ファイルの拡張子を.txt から.msi に変更してください。 アイコンがインストーラのアイコンに変わるか確認します。アイコンがインストーラのアイコンに変わらない場合は、コマンドプロンプトで以下のコマンドを実行してください。 C:¥Windows¥System32¥msiexec.exe /REGSERVER ※ Windows XP が C ドライブにインストールされている場合の例です。 それ以外のドライブにインストールされている場合には、該当するドライブ文字に置き換えてください。 また、OS が異なる場合はシステムフォルダ名を置き換えてください。 		
5.	「SUBST」コマンドで作成した仮想ドライブからインストールを実行している。 SUBST コマンドによる仮想ドライブを解除してください。		

(2) ネットワークモードの場合、管理サーバと通信できない、または管理サーバのクライアント認証に失敗する。

- 1. インストール時に使用したクライアント名、クライアント ID、管理サーバの URL が正しいか確認してください。
- 2. コマンドプロンプトで管理サーバに ping コマンドを実施してください。ping コマンドでエラーが発生した場合は、管理 サーバとの通信が行われていない可能性があります。
 - ※ ping についてはオペレーティングシステムのマニュアル等を参照してください。ネットワークで ping コマンド が禁止されている場合がありますのでご注意ください。また、OS が異なる場合はシステムフォルダ名を置き 換えてください。
- 3. DNS 設定していない可能性があります。設定していない場合は、ネットワーク管理者に管理サーバの IP アドレスを DNS 設定してもらってください。
- 4. URLの管理サーバ名部分をIPアドレスに変更して接続すると、接続できる場合があります。

▶ その他については「InfoCage モバイル防御 ユーザーズガイド」のトラブルシューティングを参照してください。

InfoCage モバイル防御 Ver 3.62 インストールガイド

日本電気株式会社 東京都港区芝5丁目7番1号 TEL(03)3454-1111(大代表)

Copyright© NEC Corporation 2007, 2008.

日本電気株式会社の許可なく複製・改変等を行うことはできません。