

Driverware

4thEye Professional Ver. 4.5

製品のご紹介



サイエンスパーク株式会社
営業部 セキュリティ製品営業課

目 次

- 0. 4thEye Professionalとは
- 1. ファイルの持ち出し禁止
- 2. 印刷禁止
- 3. マスターキー
- 4. 持ち出し許可デバイスの作成
- 5. 禁止操作メッセージ表示
- 6. ログ取得
- 7. 導入手順
- 8. 対応環境
- 9. 暗号Liteとの連携
- 10. お問い合わせ

0. 4thEye Professionalとは

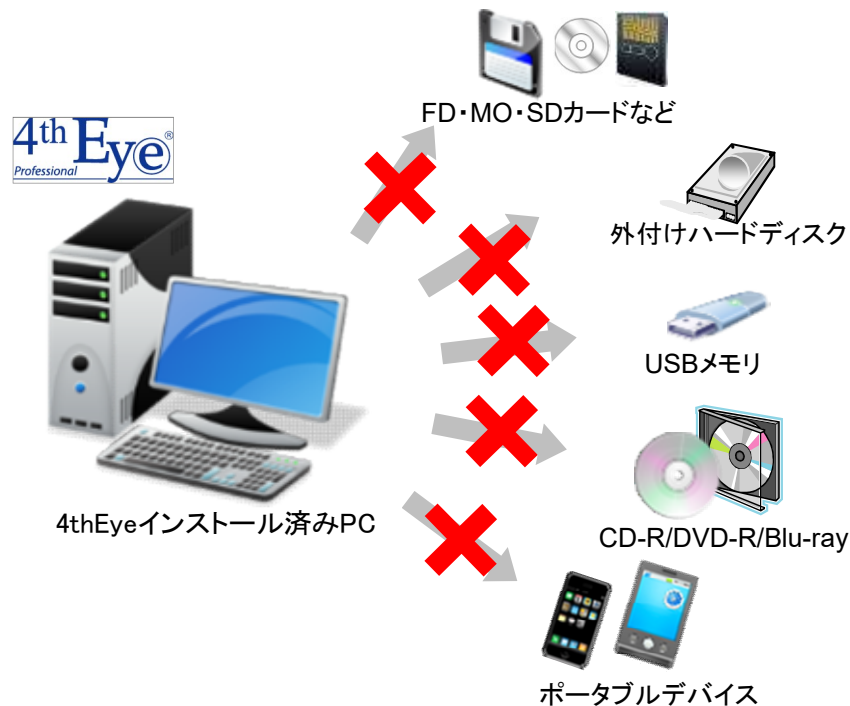
4thEye Professional(以下4thEye)は、PCから外部接続デバイス(USBメモリなど)へファイルの持ち出しを禁止する情報漏えい防止ソフトウェアです。

4thEyeの特長

サーバー不要の 簡単運用	サーバーがなくても導入が可能です。 PCに4thEyeをインストールするだけで、すぐに各機能が有効になります。 (サーバーがあるとログの管理がさらに簡単になります。詳しくはP10へ)
マスターキーを挿す だけの制御解除	4thEyeをインストールしたPC(クライアントPC)にマスターキー(USBトークン)を接続中はファイルの持ち出しができるようになります。 「金庫の鍵」のような直感的で分かりやすい運用を実現しています。 (詳しくはP7へ)
Windows 10 対応	最新のOS、Windows 10に対応済みです。

1. ファイルの持ち出し禁止① ～機能概要～

- 4thEyeをインストールしたPC(クライアントPC)から、各種デバイスへのファイルの持ち出しを禁止します。



多数のインターフェイスに対応

USB、IEEE1394、SCSI、シリアルポートなど

多彩なメディアに対応

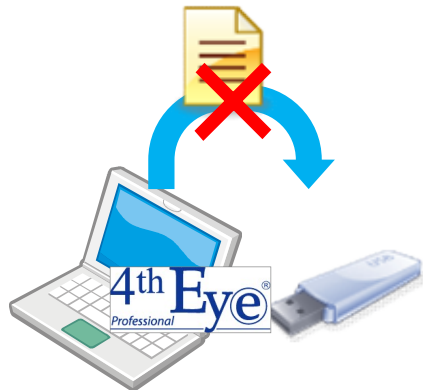
USBメモリ、SDカード、FD、SSD等

Androidのデバッグモードに対応

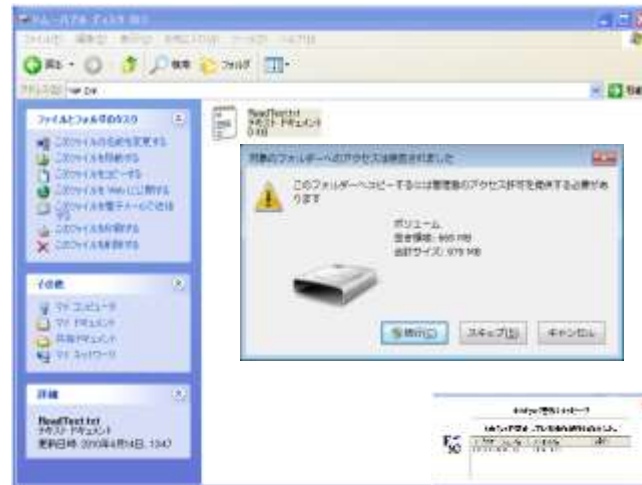
スマートフォン(Android)のUSBデバッグモード経由のファイル持ち出しも禁止します。

1. ファイルの持ち出し禁止② ～機能詳細～

ファイルの持ち出し禁止



4thEyeインストール済みPC



クライアントPCからリムーバブルディスク／ポータブルデバイスへファイルの持ち出しを禁止します。

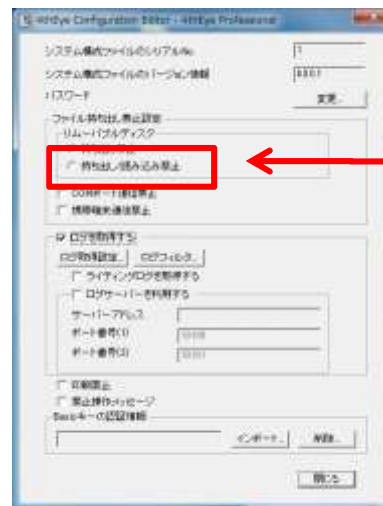
持ち出し操作をした場合はデスクトップ上に禁止メッセージを表示し、ファイルの持ち出しはできません。

※ライティングソフトによるCD/DVD/BDへの書き込みも禁止します。

ファイルの読み込み禁止(オプション)



4thEyeインストール済みPC



リムーバブルディスクからクライアントPCへのファイルの読み込みを禁止します。

設定は、読み込み禁止にチェックを付けてインストールするだけです。

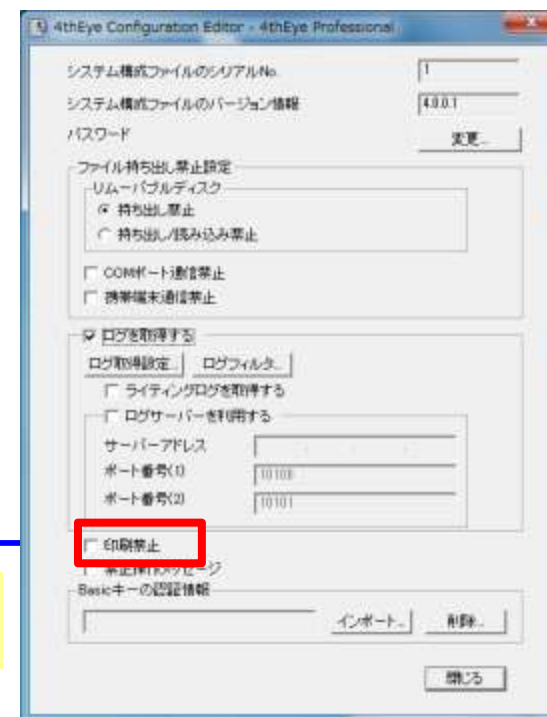
リムーバブルディスクからのウィルス混入やCD-ROMからの不要なソフトウェアのインストールなどを防止できます。

2. 印刷禁止

- 印刷禁止設定を行うことでアプリケーションからの印刷を禁止します(Windows 8以降のOSを除きます)
- パラレルポートやUSB、ネットワーク等の各種インターフェイスを持つプリンタに対応し、印刷物による情報漏えいを防止することができます。



「印刷禁止」にチェックをいれてインストールするだけで、印刷を禁止します。



3. マスターキー

■ マスターキー機能

USBポートにマスターキーを挿している間だけ、4thEyeの禁止機能を解除します。



マスターキーで解除される機能

ファイルの持ち出し禁止機能

PCから各種デバイスへのファイル持ち出しが可能になります。
持ち出し／読み込み禁止設定の場合、各種デバイス内のファイルが読み込めるようになります。

印刷禁止機能

印刷ができるようになります。

部門毎に使用可能なマスターキーを設定できます。

	部門AのPC	部門BのPC
マスターキーA	○	×
マスターキーB	×	○

○: 機能解除可能

×: 機能解除不可能

※マスターキーの紛失対策として特定のマスターキーをブラックリストに登録して使用不可にすることができます。

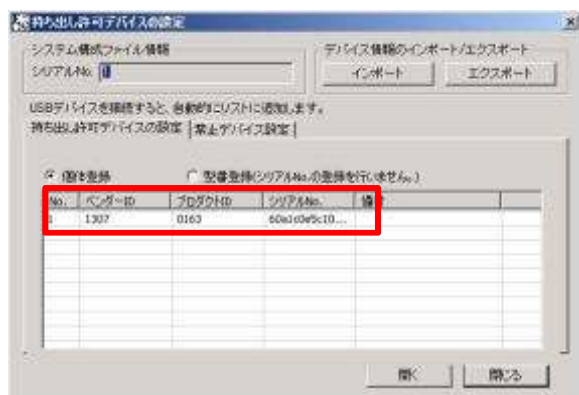
4.持ち出し許可デバイスの作成

- 管理者が許可したUSBメモリのみ、ファイルの持ち出しが可能になります。

設定方法

設定は、管理者が専用ツールを使って行います。

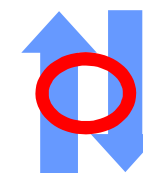
USBメモリのベンダーID、プロダクトID、シリアルIDを取得し、持ち出し許可デバイスの設定ファイル(NIJIWL.bin)を作成します。



持ち出し許可デバイスの
設定ファイル



4thEyeのインストール



使用可能



持ち出し許可デバイス



使用禁止

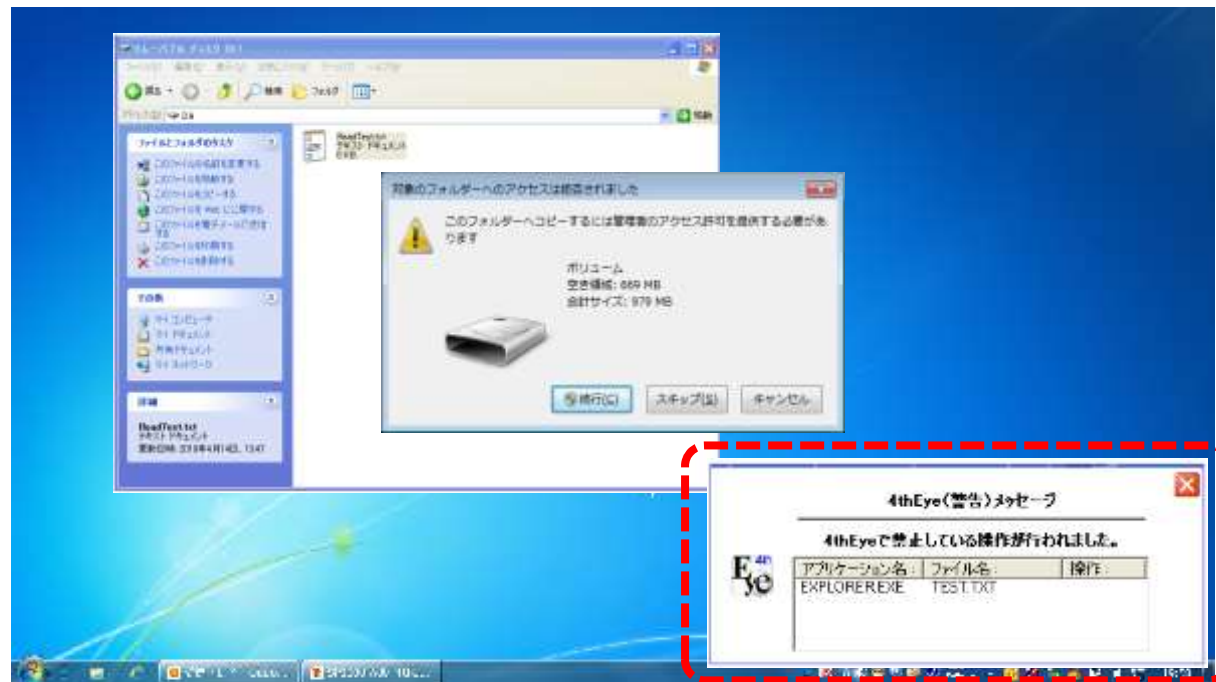


未許可デバイス

※指定USBメモリは10,000本まで登録できます。
※ウイルス対策・暗号機能付USBメモリにも対応しております。
動作確認済USBメモリにつきましては、当社Webサイトをご確認ください。

5. 禁止操作メッセージ表示

- ファイルを持ち出そうとした場合、ユーザーに禁止操作であることを知らせるメッセージを表示します。



6.ログ取得 ① ～設定画面と表示例～

■ クライアントPCでのファイルアクセスログを取得します

<ログ取得の設定画面>



設定画面で取得するログの種類を選べます。

※ポータブルデバイスのログ取得設定は固定です。
「読み込み」「書き込み」「削除」「改名」ログを取得します。

<取得したログの表示例(ログサーバー運用の場合)>



「いつ」「どのPC」で「誰」が「何のファイル」を
「どう扱ったのか」のファイル操作のログを
取得可能です。

6.ログ取得 ② ～運用例～

- サーバーを構築しないスタンドアロン型でも、クライアントPCのファイルアクセスログの取得、閲覧が可能です。

ログサーバー運用

ログ閲覧ソフトを利用して、各クライアントPCからサーバー上に収集されたファイル操作ログを一括で閲覧できます。



OR

スタンドアロン運用

専用ツールを利用して、各クライアントPCのファイル操作ログを「CSVファイル」に変換し、個別に閲覧することができます。



CSVファイル

※ログ取得に必要なディスク容量について

ログデータは、1件あたり約580byte(弊社平均値)です。保存するログの量により、必要な空き容量を確保してください。

7.導入手順

- 4thEye の基本的な導入手順は以下の通りです。

セキュリティポリシーの決定

マスターキーの運用方法、ログ取得や印刷制御の有無等



インストール準備

社内セキュリティポリシーを反映した設定ファイルの作成、
持ち出し許可デバイスの設定ファイルの作成



インストール

ユーザーのPCへ4thEye のインストール

8.対応環境

■ 4thEye Professional 対応OS(日本語のみ)

- Windows Vista(SP2)
- Windows 7(SP1)
- Windows 8.1(Update1)
- Windows 10(Ver.1511及び1607対応)

※Vista(SP2)のみ32bit版対応、他のOSは32bit、64bit対応

■ 4thEye Professional LogServer 対応OS (日本語のみ)

- Windows Server 2008 [Standard /Enterprise (SP2)]
- Windows Server 2008 R2 [Standard / Enterprise (SP1)]
- Windows Server 2012 [Standard / Datacenter]
- Windows Server 2012 R2 [Standard / Datacenter (Update1)]

※別途Microsoft SQL Server 2008、2008 R2、2012 (Express Edition含む)が必要です。

最新の対応OS、動作確認済アプリケーションにつきましては弊社WEBページをご確認ください。

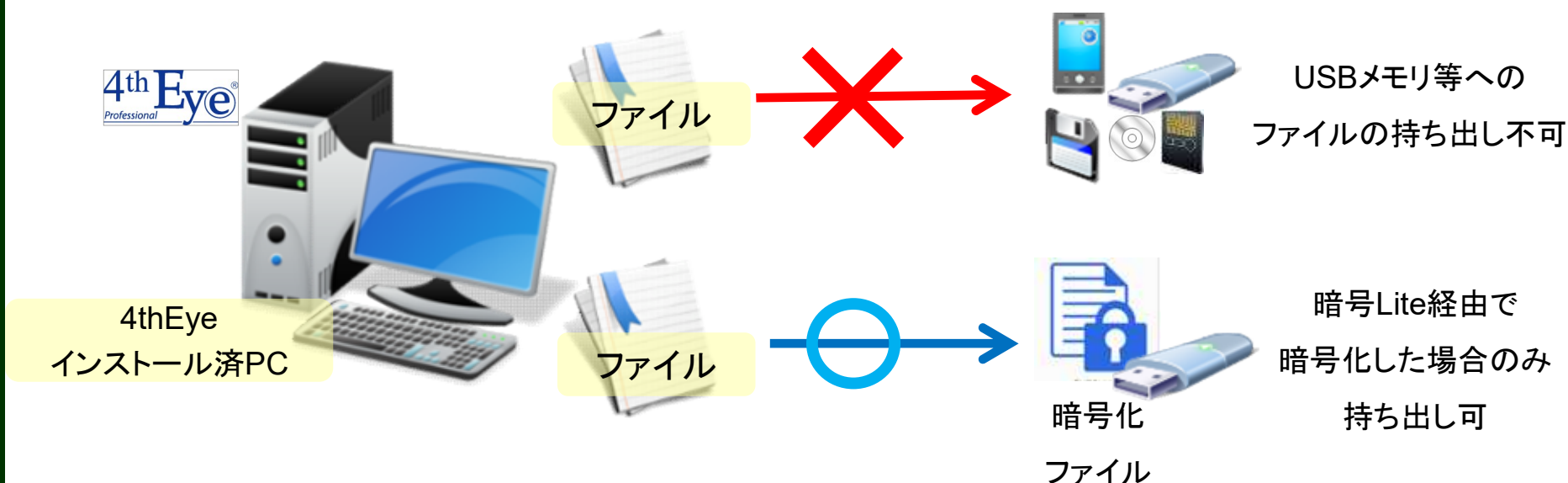
「動作環境 | 4thEyeProfessional | サイエンスパーク株式会社」

http://www.sciencepark.co.jp/information_security/4theye/operation.html

9.暗号Liteとの連携

- 暗号Liteで暗号化する場合のみ、ファイルの持ち出しが可能です。

※「暗号Lite」のライセンス(別売)が必要です。



「暗号Lite」とは
ファイルを自己復号型暗号ファイルに変換するソフトウェアです。

10.お問い合わせ

サイエンスパーク株式会社 営業部 セキュリティ製品営業課

Tel:046-255-2544

E-Mail:sales-products@sciencepark.co.jp

弊社WEBページで製品紹介資料・販売代理店をご案内しております。
是非一度ご覧ください。

http://www.sciencepark.co.jp/information_security/4theye/