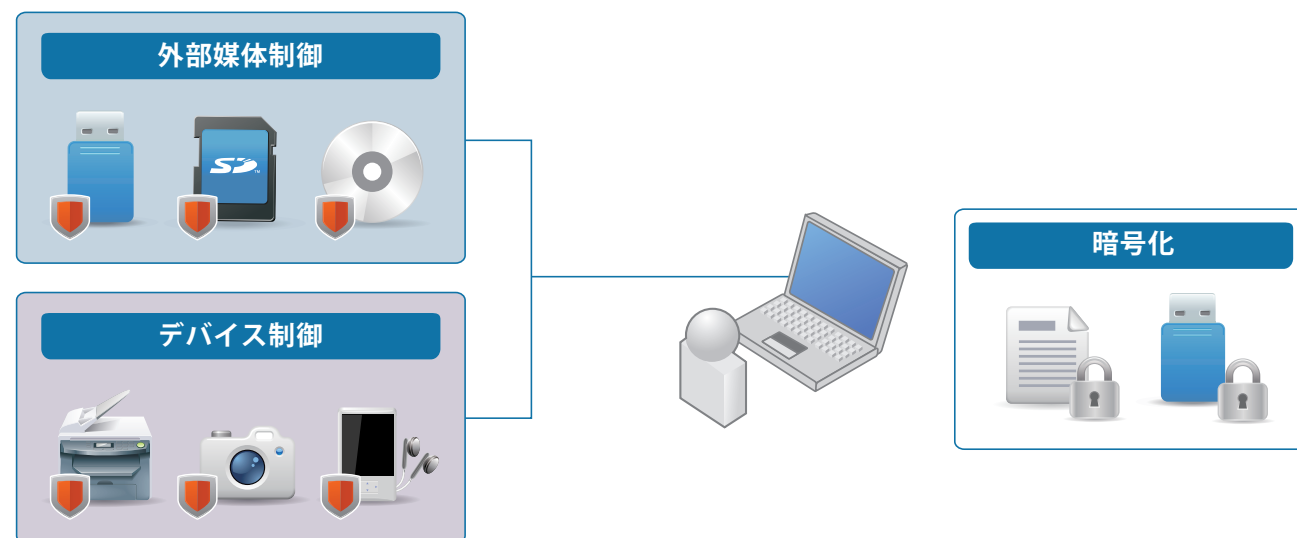


SecureCore RSS



外部記録媒体の利用を制限する、情報漏洩対策ソリューション

- USBメモリなど外部記録媒体の利用制御
- ハードウェアやポートの制御
- 外部記録媒体の暗号化
- ファイル単位での暗号化



情報漏洩のリスク

個人情報や企業の知的情報が流出する事件・事故が多く報告されています。情報システムの大容量化に伴い、事故一件あたりの被害は飛躍的に増大しております。また、自社内で全ての業務を完結する事は困難な時代であり、派遣先、委託先や請負先など、社外のルートから情報が流出するリスクも高まっております。

SecureCore RSSによる対策

- ・協力会社や取引先との安全なデータ受け渡し
- ・データ暗号化による個人情報や営業情報の漏洩対策
- ・私物 USB メモリ、オーディオプレーヤーやスマートフォンの接続禁止
- ・デバイス利用申請から承認のルールによる、社員のセキュリティ意識の向上
- ・盗難や紛失時の二次被害防止

イージーモードによるシンプルな管理機能と簡単な操作性

管理画面はイージーモードとプロフェッショナルモードから選択できます。
メディアの【登録】→【配布】や、ユーザーからの【申請】→【承認】の操作をウィザード形式でシンプルに行えます。
SecureCore RSSでは、業務の生産性を妨げず、シンプルで柔軟な管理と、簡単な操作性を実現しています。

SecureCore RSSの機能

メディア本体の暗号化フォーマット 暗号化されたメディアは組織外で利用不可能	コンピュータ別による管理 コンピュータ単位でのポリシー配布による利用制限が可能	ファイルの暗号化や自己復号暗号 パスワードを掛けることでファイル単位での暗号化が可能
ユーザーや組織別による管理 ユーザーや組織単位でのポリシー配布による利用制限が可能	メディアの利用期間制限 利用期限が過ぎたメディアは利用不可能	ウィザード形式による承認処理 時間と手間をかけない簡単な承認処理
組織に合わせた管理権限の委任 部や課などの組織に合わせた管理者の権限委任が可能	業務フローの簡略化を実現 管理者の仕事を増やさない簡略化された業務フロー	社外オフライン PC の利用も可能 出張時など、社外にPCを持ち出した時でも安全に利用可能
ポリシー変更も即座に反映 ユーザーがメディアを挿入した瞬間にポリシー反映	メディアの個体管理による履歴追跡 メディア固有のID情報を管理し利用履歴を全て記録	オプション 内蔵HDDのアクセス証跡を記録 内蔵HDDの読み/書き/ファイル名変更などの操作を全て記録

製品仕様

	サーバー動作環境
サポートOS	Windows 2000, XP, Vista, 7 (32bit / 64bit) Windows 2003, 2008 Server
CPU	Pentium 500MHz以上
メモリ	64MB以上
ハードディスク	1GB以上 (標準インストールの場合)
DB	Microsoft SQL Server 2005以上 (Express Edition でも可)
	クライアントおよびコンソール動作環境
サポートOS	Windows 2000, XP, Vista, 7 (32 / 64bit) Windows 2003, 2008 Server
CPU	Pentium 500MHz以上
メモリ	64MB以上
ハードディスク	32MB以上

詳しくは、WEBサイトでもご覧頂けます。 <http://www.ftsafe.co.jp/>