

HDD暗号化ソフトウェア
SecureDocのご紹介

クロス・ヘッド株式会社

成長するネットワークを創造する



CROSS HEAD

SecureDocの概要と販売実績

■ 開発元

- **WinMagic Inc.**(カナダ トロント)

■ 日本発売

- **2004年5月**

■ 実績

- **SecureDocは2013,2014年度の国内のHDD暗号化製品新規導入でシェアNo.1を達成**
- **世界で1,000万クライアントの実績**
- **日本:約200万ライセンス**
(大手商社様、官公庁、警察、文教、業種を問わず実績有り)
- **海外:米国防総省、カナダ最大手銀行、北米/西欧の政府組織、米最大手ISP業者**

■ 製品体系

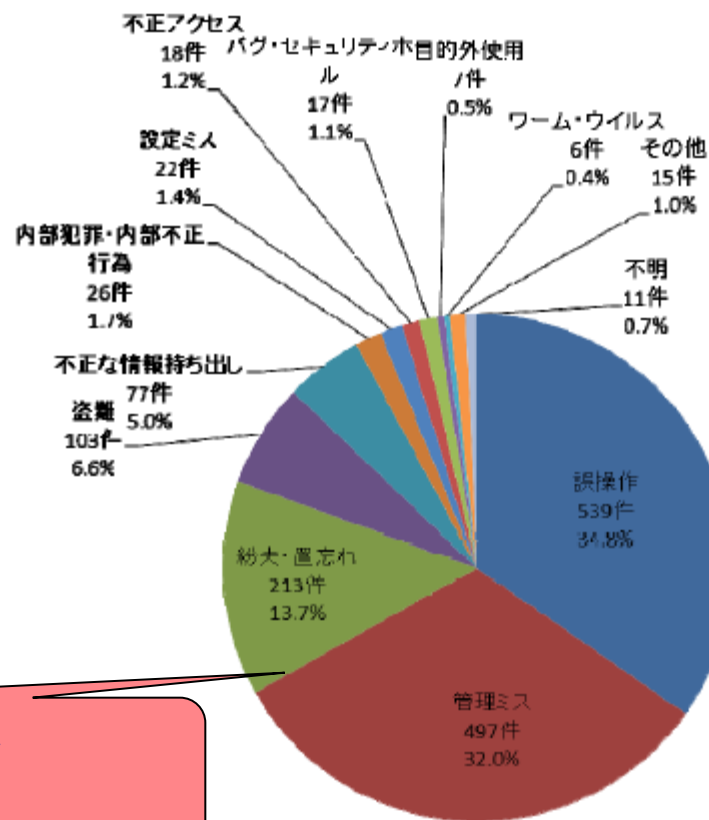
- **SecureDoc Standalone Edition**
- **SecureDoc Enterprise Edition**

報道は減っても、まだまだ多発

管理ミス、紛失・置忘れなどのヒューマンエラーは組織としてルールが整備されていない、もしくはルールが存在しているものの、遵守されていないために社内や主要な流通経路で発生するインシデントである。

ヒューマンエラーは必ず起こることを前提として暗号化などの情報漏えい対策や、紛失しても被害が拡大しない対策もあわせて行うことも検討に値する。

情報漏洩経路・原因比率(発生件数)



情報漏洩経路の原因は約52.3%が紛失や盗難、管理ミスです

(参考)「情報セキュリティマネジメントに関する調査報告書」

経済産業省のガイドラインより

安全管理措置ガイドラインより

METI 経済産業省

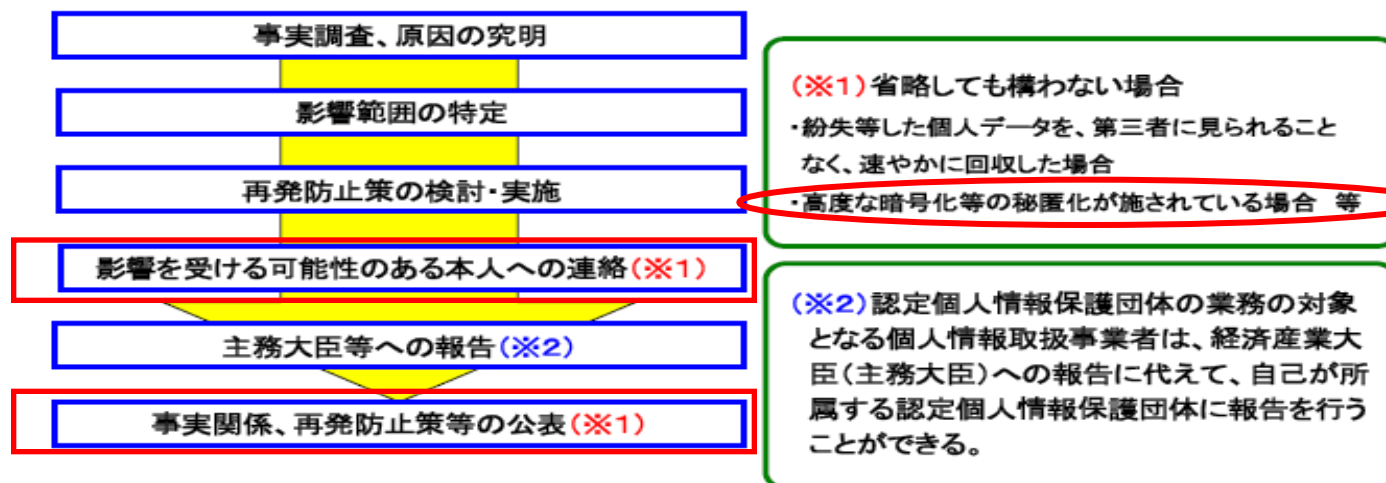
～ 「安全管理措置」⑥ ～

～ 「組織的安全管理措置」(ガイドライン26ページ以下) ～

【講じなければならない事項】

⑤事故又は違反への対処

＜事故又は違反が発覚した場合の対処の手順等(例)＞



30

高度な暗号化技術を持つSecureDocなら、大きなリスクを回避することができます

他社との優位点

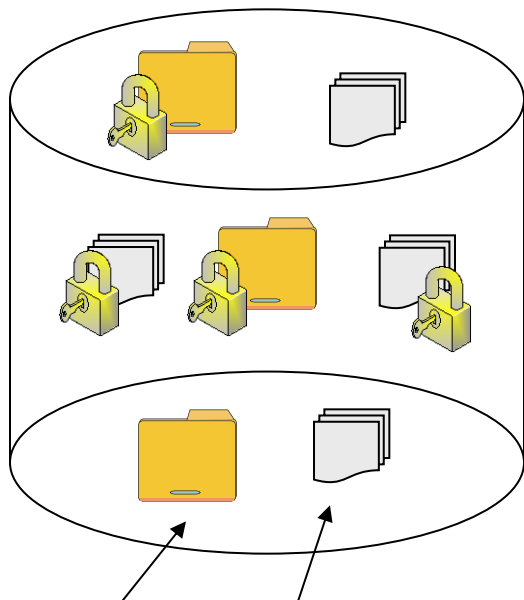
- ・ **オンラインにならないPCの管理も可能**
 - 完全にオフラインのPCにもインストール可能
 - ActiveDirectoryに参加していないPCにもインストール可能
- ・ **データ救済方法が簡単**
 - 鍵を持たせることで、HDDを抜き出してデータを救済することが可能
 - OSクラッシュ時にSecureDocが持つOSで起動させることで、データ救済が可能
- ・ **最新技術に対応している**
 - OPAL3.0以降
 - Windows10
 - 第6世代Intel Coreプロセッサ「Skylake」
- ・ **SESの機能**
 - ActiveDirectory情報のインポート
 - PreBootNetwork
 - エマージェンシーディスク、暗号鍵の管理
 - BitLockerの管理
 - FileVault2の管理

HDDを丸ごと暗号化



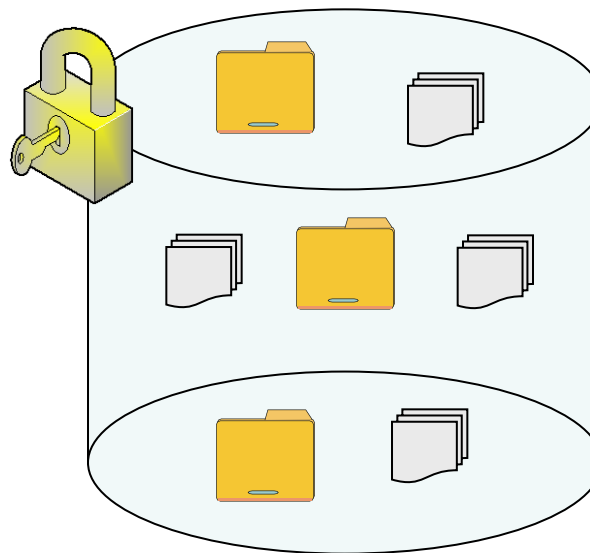
SecureDocは、セクタ単位でHDDすべての領域を暗号化

一般的なファイル単位の
暗号化ソフト



暗号化されない領域があります。
ユーザはそれを意識する必要があります

VS



HDDは、まるごと暗号化されているので
ユーザは暗号化を意識する必要がない

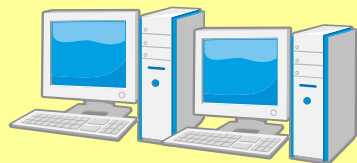
暗号化のアルゴリズムは、
「電子政府推奨暗号リスト」
にも記載されているディスク
暗号製品の中で最高位の
AES 256bitを使用しており
ます。

多様な運用方法

- 「スタンドアロン運用・オフライン運用・オンライン運用」の3つの運用に対応
- お客様のニーズによって選択可能（混在可能）

スタンドアロン運用

- 小規模ユーザ向け
- 管理サーバ不要
- キitting時に、Diskイメージの複製も可能



サーバ運用

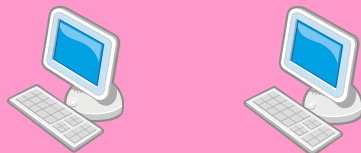
- 大規模ユーザ向け
- パスワード忘却時にも、チャレンジアンドレスポンス機能でログイン可
- オンラインとオフラインの併用が可能
- ウィザードに添ってクリックしていくだけで、暗号化まで完了

SecureDoc
Enterprise Server



社内LAN、VPNなど

オンライン運用



- 暗号化状況の把握・監査レポートの作成
- パスワードルールや暗号鍵などのユーザプロファイルや許可済みのUSBデバイスリストなどポリシーの配布がリモートで可能

オフライン運用



- ネットワークに接続できない端末でもインストール可能
- キitting時に、Diskイメージの複製も可能

暗号化時、運用時共に通信は必要ありません。

ポート・外部記録媒体



ポートコントロール

許可したUSBデバイスしか使用させない

使用許可済



プリンタ



社用USBメモリ
(製造番号:ABC)



デジタルカメラ

使用未許可



MP3プレイヤー



私用USBメモリ
(製造番号:XYZ)



携帯電話

❖USBメモリからの
ウイルス感染防止にも役立ちます



使用可
使用不可



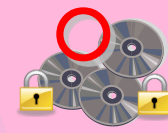
メディア暗号化・デバイスコントロール

暗号化したメディアしか使用させない

暗号化済



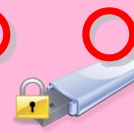
CD/DVD



FD

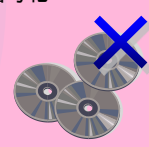


SDカード

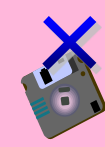


USBメモリ

非暗号化



CD/DVD



FD



SDカード



USBメモリ

ビルドインSDカードリーダーにも対応
CD/DVDからの情報漏えいを防止

- ❖ 外付けHDDも暗号化出来ます
- ❖ 自動暗号だから、ユーザの操作は必要なし



SecureDoc導入端末

標準機能で外部メディアの制御が可能です。

AutoBoot機能

社内では自動起動、社外ではPre-Boot認証となります。

オンライン

SecureDocのプリブート認証時に、有線LANが接続されていて、SecureDoc Enterprise Serverに接続が可能な場合に、認証画面をスキップし、自動的にOSが起動します。

端末の電源を入れる
※手動あるいは、WakeOnLAN



※自動認証が完了するまで
10秒かかります。



OS起動



有線LANを事前に接続しておけば、
ユーザの操作が一切不要で起動可能

オフライン

有線LANが未接続な状態や、SecureDoc Enterprise Serverに対して接続ができない場合には、プリブート認証を実施します。

端末の電源を入れる



SD認証画面
※OS起動前認証



OS起動



登録されているアカウントでログインする。
ID: SecureDoc01
PW: password

固定のID、PW以外に、Tokenを使用での
ログインも可能です。

※プリブートネットワーク(PBN)機能は、パソコンのネットワークカードとの相性があるため、必ず事前に動作確認をお願いします。

BitLocker Managementとは



Windows 7 Enterprise/Ultimate、Windows 8/8.1に搭載されているBitLockerの

- ・初回暗号化処理
- ・認証方法の決定
- ・リカバリーキー

を、SecureDocのサーバで一元管理します。

Microsoft社が用意している、以下の運用方法に比べて

非常に手軽に実施できます。

- ・Active Directoryのスキーマ拡張での管理
- ・Microsoft社の管理ツールでの管理



なお、本運用を実施するには、SecureDocの**オンライン運用が必須**となります。

■ BitLocker Management導入時の制限事項

- ・OS起動前認証画面はBitLocker固有のものを利用致します。
- ・**PBNによる自動起動**はご利用頂くことが出来ません。
- ・**トークンによる起動**をすることが出来ません。

FileVault2 Managementとは

Apple Mac OSに搭載されているFileVault2の

- ・初回暗号化管理
- ・リカバリーキー

を、SecureDocのサーバで一元管理します。



なお、本運用を実施するには、SecureDocの**オンライン運用が必須**となります。

■ FileVault2 Management導入時の制限事項

- ・OSは、10.9.5～10.10.5までが対応となります。
※10.11.x(EI Capitan)は、次期バージョンでの対応予定です。
- ・OS起動前認証画面はFileVault2固有のものを利用致します。
- ・**トークンによる起動**をすることが出来ません。

OPALへの対応

SecureDocがOPAL規格の自己暗号HDD（FDE：Full Disk Encryption）に対応することにより、OPAL規格HDDの認証管理をサポート

FDEのメリットとデメリット

• メリット

- ✓ 導入時のディスク暗号作業が不要
- ✓ 高いパフォーマンス
- ✓ 完全暗号
- ✓ 導入時の障害の可能性が極めて低い

• デメリット

- 起動認証の管理不可
- 管理不可（スタンドアロンのみ可能）



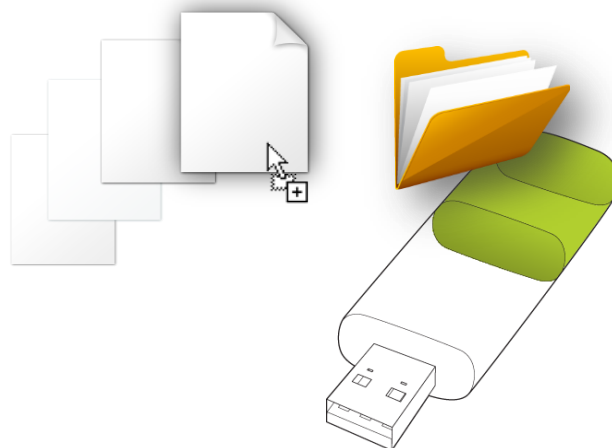
ドライブ上の
鍵とチップで
暗号処理



SecureDocとFDEの統合によりFDEのデメリットを解消
パフォーマンスを下げないディスク暗号の実現

USBコンテナ暗号化機能

- 市販のUSB内領域に、SecureDocが暗号化領域を作成します。
- 同じ暗号鍵を所持している環境では、ユーザはパスワードを使用することなく、媒体の読み書きが可能
- オプションにて、パスワード保護の設定をすることで、SecureDoc未導入端末でも暗号領域に格納されたデータの読み書きが可能



ファイル/フォルダ暗号機能(FFE)

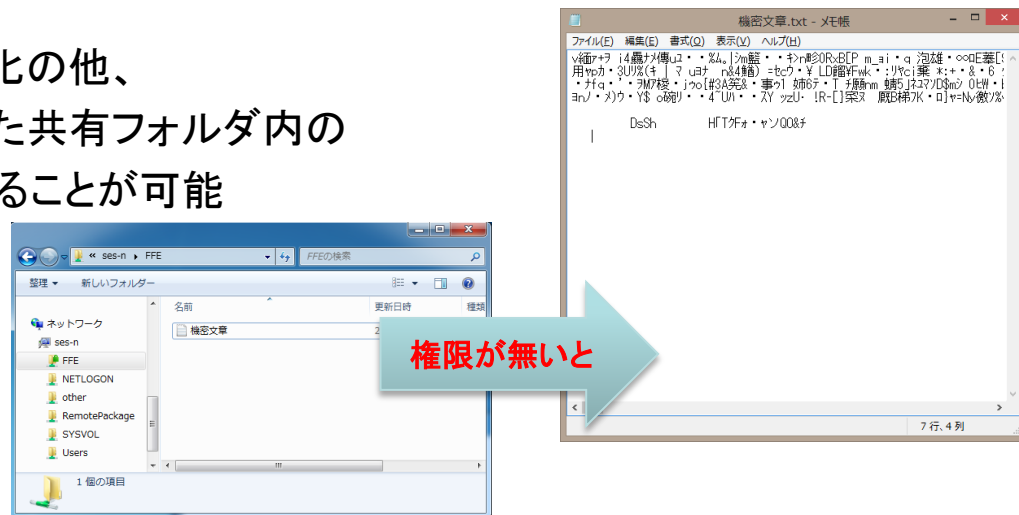
- ハードディスクのセクター単位での暗号化の他、事前にSecureDoc管理サーバで設定した共有フォルダ内のファイルを指定した暗号鍵で暗号化をすることが可能
- ローカルの特定のフォルダに対して設定することも可能
- ユーザは意識することなく暗号化設定されたフォルダにファイルを保存することで自動暗号
- CloudSync機能を使用して、パソコンからクラウド上へアップロードされるファイルを自動で暗号化することが可能

※v7.1では、CloudSyncはDropBox、Box、Google Drive、One Driveに対応となります。

CloudSyncでの暗号化には、各クラウドベンダーが提供するアプリケーションの導入が必須です。



※FFE機能はオプションとなり、別途有償となります。
※CloudSync機能はオプションとなり、別途有償となります。



OSが破損してもデータ救済が可能

SecureDocは、暗号鍵の概念を持っているため、復号化せずにデータ救済が可能です。

1. 事前準備

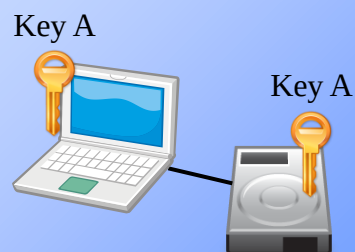
- 復旧用端末にSecureDocをインストールします。
- 復旧用端末にクラッシュした端末の暗号カギを付与します。

2. データ救済作業

1.OSがクラッシュしたHDDを抜く



2.セカンダリ・外付けHDDとして 復旧用PCにデータ抽出対象の HDDを接続する。



3.必要な場所にデータの コピーを実施



※事前に復旧用端末を用意しておくことで、おおよそ30分以内にデータ救済開始が可能となります。

OSが破損してもデータ救済が可能2

メーカー提供のCD起動OSを使用することで、内蔵ドライブを取り出すことなくデータ救済が可能です。

1. 事前準備

-CD-ROMドライブ

2. データ救済作業

1.OSがクラッシュしたパソコンを
SDRecovery Mediaで起動



2.SDRecovery Media内で、
SecureDocのアカウントでログイン実施



3.USBメモリや外付けHDDに
必要なデータを退避実施



※おおよそ30分以内にデータ救済開始が可能となります。

SecureDocの仕様と機能(v7.1)

■ 動作環境

OS	Microsoft Windows 10 Microsoft Windows 8/8.1 Microsoft Windows 7 SP1 Microsoft Windows Vista SP2 Mac FileVault2(オンライン運用時) Mac FileVault2 X10.11.1 El Capitan対応 (v7.1SR1より)
CPU	Intel互換CPU(1 GHz 以上) Intel Skylake対応 (v7.1SR1より)
RAM	512MB 以上
HDD	800MB 以上の空き容量 ※インストールドライブに10%以上の空き容量があること

HDD暗号化ソフトは、機種依存が発生するケースがあるため、必ず事前検証をお願いします。

■ その他の特徴

- ・ 暗号アルゴリズム AES256bit
- ・ FIP S 140-1&2
- ・ 休止モードサポート(対応OS全て)
- ・ 通信によるSESとのポリシー同期
- ・ スタンドアロンモード
- ・ 一般ユーザによる復号化、アンインストールの禁止
- ・ パスワードルールの強制
- ・ USBトークン、ICカード、指紋認証、TPMを利用した二要素認証によるログイン
- ・ 設定変更等ログのサーバーへのアップデート

SecureDoc Enterprise Serverの仕様と機能(v7.1)

■動作環境

OS	Microsoft Windows Server 2008 Microsoft Windows Server 2008 R2 Microsoft Windows Server 2012
プロセッサ	Intel互換 1GHz以上
メモリ	512MB以上 * オンライン運用の場合1GB以上
スクリーン解像度	横幅1200ピクセル以上
HDD	4GB以上の空き容量 40GB以上推奨
データベース	Microsoft SQL Server 2008 (Express Edition) Microsoft SQL Server 2008 R2 (Express Edition) Microsoft SQL Server 2012 (Express Edition) Microsoft SQL Server 2014 ※SESの運用にはデータベースが必要です

■ポリシー管理方法

- ・ オフライン管理
- ・ オンライン管理

■その他の管理機能（一部オンラインでのみ提供）

- ・ クライアントの端末の暗号化状況の追跡機能（コンピューターIDによる表示）
- ・ Active Directoryユーザ情報のインポート
- ・ クライアント端末の設定の一元管理（オフライン運用、オンライン運用共に可能）
- ・ チャレンジ&レスポンス方式によるパスワードリカバリ
- ・ 一時的なパスワードの発行（トークンユーザがトークンを紛失した際などに有効）
- ・ 複数端末からのデータベースへの同時アクセス

お問合せは. . . 、



成長するネットワークを創造する



CROSS HEAD

クロス・ヘッド株式会社
NCLC事業部

Tel : 03-5447-8514
Mail : security@crosshead.co.jp

