

USBトークン認証ハードディスク暗号

Windows7対応USBトークンでOS起動前（プリブート）認証ハードディスク暗号



WindowsXPからWindows7にPC環境を移行させるお客様に、これまで同様にハードディスク暗号をUSBトークンで起動前に認証するソリューションをご提供いたします。社員が携帯する持ち出しPCをパスワードで起動するのではなく、起動用の証明書を含むUSBトークンを認証して起動させる安全な運用にできます。社員も定期的にパスワードを変更する煩わしさから解放されます。

パスワードでなくUSBトークンで起動前認証 利用者の頻繁なパスワード更新から解放

ハードディスク暗号利用者は暗号化ハードディスクの起動に、起動用パスワードを利用するのが一般的ですが、これではせっかくの暗号化ハードディスクもパスワード流布によって重要情報の漏洩に直結してしまいます。このような事態を防止するため、パスワードを頻繁（2～3ヶ月に1度程度）に変更するポリシーで運用します。この事がかえってパスワードを記憶できずメモに書き留めるなどにつながって情報管理に逆効果な場合があります。



USBトークンを紛失しても認証局から再発行 認証局で鍵を保管するから再発行可能で安全

USBトークンに暗号化を解く復号鍵（暗号鍵証明書）を格納し、起動前PCにUSBトークンを挿入し起動前認証します。USBトークンが無いと暗号化されたディスクを復号できないので大変安全です。暗号鍵証明書を保管するのは、Pentio ADCS認証局パッケージです。認証局に保管された証明書は、USBトークンを紛失した場合に新しいUSBトークンに証明書を格納することで、鍵の再発行ができます。これにより管理者はPCの回収設定作業から解放されます。



緊急時は管理者USBトークン（管理者鍵） でプリブート認証起動。暗号ツールには利用 者証明書と管理者証明書を登録。

起動前認証用の鍵は、複数登録できます。各PCの暗号ツールには復号鍵（暗号鍵証明書）を複数登録します。利用者の暗号鍵証明書と、管理者の暗号鍵証明書との二つを登録してハードディスク暗号し、万一の緊急時は必要に応じて管理者USBトークンで起動させることもできます。また、管理者は使用済みPCを別の利用者に再配布する初期化作業などでも管理者鍵を利用することができます。



USBトークンを持参忘れてはワンタイム パスワード生成認証。遠隔の場合はワン タイムパスワード生成し携帯電話へ。

出張などの遠隔地で暗号化ハードディスクPCを起動する復号鍵USBトークンを忘れてきた場合は、管理者に連絡してください。管理者はPCを特定した後、Secure Docサーバで生成した一時利用パスワード（ワンタイムパスワード）パスフレーズを利用者携帯電話に送ります。携帯電話で受け取ったパスフレーズを緊急起動操作から入力することで一時的に起動前認証させPCを利用することができます。ただしこのパスフレーズは次回に利用することができないので安全は確保されます。



SecureDoc™ の主な機能

SecureDoc Disk Encryptionは、WinMagic Inc.が開発したPCの盗難や紛失から機密情報を守るソフトウェアソリューションです。SecureDocをインストールすると、PCのハードディスク全体が暗号化され、Windowsが起動する前に認証を要求するようになります。SecureDocにより暗号化されたPCが盗難にあっても、パスワードがなければWindowsは起動しません。ハードディスクを抜いて他のPCに接続しても、ディスク全体が暗号化されているため、データ復元ツールを使って内部のデータを読み取ることはできません。更にパスワードの代わりに、ハードウェアトークンを使うことで、「トークンがなければ、起動しない」PCを構築することができます。全ての暗号は自動的に行われるため、ユーザは起動時の認証さえ行えば、暗号を意識することなく通常と同じ操作で暗号化されたPCを利用することができます。また、標準機能として、同じソフトウェアで外部メディアのフル暗号、書き出し制御、使用制御を行えるのもSecureDocの特長です。これらの設定やポリシーは、全てSecureDoc Enterprise Server (SES)と呼ばれる管理サーバで管理されます。SESは、Windowsのみならず、Mac、Linux、自己暗号ドライブを搭載したPC等、様々なプラットフォームにおけるユーザ・PC・暗号鍵の管理を一元的に行います。

SecureDoc™ の特長

- PCのOSやシステム領域を含めたハードディスク（HDD）を丸ごと暗号化。
- プリブート（Windows起動前）のユーザ認証（パスワード、トークン、ICカード等）。
- リムーバブルメディアの丸ごと暗号化、使用制御（私有USBメモリの使用禁止等）を標準搭載。
- SESによる一元的なポリシー、ユーザ、PC、暗号鍵の管理。PCが暗号化されていることの証跡も保存。
- SESを利用したPCの遠隔ロック、データ消去（業界初）。
- Macや自己暗号ディスク等、これまで管理できなかったプラットフォームの暗号化を一元管理（業界初）。
- LANに接続しているPCは認証不要、LANに接続していないPCは認証を要求する設定等、きめ細かなニーズに応じたPC起動認証を実現（業界初）。
- 自己暗号ハードディスクにインストールすることで、一般的に数時間かかるフルディスク暗号のインストールを、数分で完了（業界初）。※トークン連携時は未検証

USBトークン認証ハードディスク暗号 構成図



※あくまでも概念構成図になります。

SecureDoc構築スタイル別メリット

	スタンドアロン運用	管理サーバ運用	管理サーバ・証明書併用
			
①セキュリティ限界	▲ 起動パスワードのみ	○ USBトークン+PIN	○ USBトークン+PIN
②起動鍵の複製	▲ パスワードを記憶に頼る	× 複製はできない	○ 新USBトークンにバックアップ証明書を格納
③起動鍵紛失の場合	▲ PC回収と再設定	▲ PC回収と再設定 (管理者鍵で再設定)	○ 新USBトークン送付 (PC回収なし継続可)
総合判定	C せっかくの暗号化PCだがセキュリティ限界が低い	B USBトークン併用でセキュリティは高いが鍵紛失の運用が管理者には高負荷	A セキュリティ限界も高く、導入後の運用も管理者には安心

商品パッケージ

必要製品群	製品名	数量	標準料金
USBトークン	Pentio PKI USB Token™ 3300	100個	700,000円
クライアントPC用暗号化ツール※1	WinMagic SecureDoc™ DiskEncryption 5.2J	100ライセンス	1,650,000円
暗号化クライアント管理用サーバ※2	WinMagic SecureDoc™ Enterprise Server	1ライセンス	0円
証明書発行認証局パッケージ※3	Pentio AD CS認証局 パッケージ	一式	1,220,000円
		合計	3,570,000円

※1 別途、設定設置、年間アップデートサービス(技術サポート、パッチ提供、バージョンアップサービス)費用がかかります。
 ※2クライアントが50ライセンス以上のご購入は初回導入時のSecureDoc Enterprise Server 1ライセンスが無償になります。
 ※3 別途、設置、保守費用がかかります。

SecureDoc™ 技術仕様

動作環境
クライアント:SecureDoc Disk Encryption
 OS:Windows 7, Windows Vista SP1/SP2, XP SP2/SP3
 プロセッサ:Pentium互換(1GHz 以上)
 メモリ:128MB以上
 HDD:128MB以上の空き容量
 ※インストールするドライブには10%の空き容量が必要です

管理サーバ:SecureDoc Enterprise Server
 OS:Windows Server 2003 SP1/SP2, Server 2003 R2 SP1/SP2, XP Pro SP2/SP3
 ※オンライン運用の場合サーバOSのみ対応
 プロセッサ:Pentium互換(1GHz 以上)
 メモリ:256MB以上 オンライン運用の場合512MB以上
 HDD:100MB以上の空き容量(20GB 以上推奨)
 データベース:Microsoft SQL Server 2005, Microsoft SQL Server 2005 Express edition, Microsoft SQL Server 2008, Microsoft SQL Server 2008 Express

主な機能
 ディスク暗号化/複合化・PCブート制御・スクリーンロック・未暗号化デバイスの使用制御・USBデバイス制御

暗号アルゴリズム
 AES256bit

標準規格への準拠
 ・Common Criteria EAL-4
 ・FIPS 140 level 2
 ・NISTによるAES認定

クライアント認証方法
 ・パスワード
 ・USBトークン、ICカード、バイオ認証
 - Pentio PKI USB Token 3300, 2050 / Pentio IC Card 3300C, 2600FC, 2300 / UPEK 製指紋認証デバイス
 - RSA 個人鍵、デジタル証明書
 - PKCS#11 準拠

対応認証局
 ・CyberTrust CA, Digital Signature Trust, Entrust, Identrus, Microsoft, Pentio, RSA, Verisign, その他のPKIベンダー

SecureDoc™については下記お問い合わせください。
ウインマジック・ジャパン株式会社
<http://www.winmagic.com/>



ペンティオ株式会社

[PKIソリューション事業部]
 〒160-0004 東京都新宿区四谷2-4 久保ビル3F
 Tel.03-5919-0971 Fax.03-5919-0980 <http://www.pentio.com/>

2011年4月