HDD暗号化のご提案

JBService

株式会社ジェー・ビー・サービス

IBM Business Partner

NO.2080420

パソコン紛失・盗難による個人情報漏洩

日本は今でも安全・安心？
セルフサービスの店で、カバン（ノートPCが入っている）を席に置いたままチョッと離席したら・・・・。
最近ではノートパソンだけでなく、オフィス内のデスクトップパソコンも狙われている！

2005/06/11, 日本経済新聞　朝刊, 11ページ
PHS最大手　10日、同社社員や顧客企業の連絡先などが保存された業務用パソコンを盗まれたと発表した。パソコンは発見されていないが、現時点では情報漏洩（ろうえい）による被害は確認されていない。ウィルコムの社員が九日、帰宅途中に電車内でパソコンを盗まれた。パソコンには顧客企業など約二千社分の連絡先と担当者名に加えて、同社社員のPHS電話番号、自宅番号など五十九人分が入っている。個人顧客の情報は入っていないという。

2005/06/29, 日本経済新聞　北海道朝刊 (社会面), 38ページ
某医科大（旭川市）の三十代の女性医師が二百十九人分の患者の個人情報を記録したノートパソコンを盗まれていたことが二十八日、分かった。ノートパソコンには患者の氏名や病名など診療情報が入っており、医師は旭川東署に被害届を出した。
大学によると、二十三日午後八時四十五分ごろ、医師が帰宅途中に保育園に子供を迎えに行った際、路上に止めていた乗用車の窓ガラスが割られ、ノートパソコンを盗まれたという。
医師は臨床研究の基礎資料として使用している患者の情報を整理するために、病院から持ち出していた。

2005/06/03, 日本経済新聞　大阪朝刊 (社会面), 16ページ
二日午前八時十分ごろ、大阪市阿倍野区松崎町一、某ビル管理会社の営業所で、現金約十六万円などが入った金庫と顧客など約六百人の個人情報が記録されたパソコン五台が盗まれているのが見つかった。阿倍野署は窃盗事件として捜査している。
調べによると、ビル一階のシャッターとガラス製のドアが、バールのようなものでこじ開けられていた。
同社はJR西日本の子会社で介護サービスも手掛けている。盗まれたパソコン五台のうち三台に、同サービスの利用者約五百人と介護ヘルパー約百人の氏名、住所、電話番号、口座番号などが保存されていた。パスワードなどの設定はなく、誰でも見られるという。

2005/08/06, 日本経済新聞　西部朝刊 (社会面), 17ページ
某エアコンメーカー　五日、九州・沖縄の八県でエアコンの修理を同社に依頼した顧客の個人データ九千七百八十件が入ったパソコン三台が盗まれた、と発表した。
同社によると、盗まれたのは「鳥栖サービスステーション」（佐賀県鳥栖市）で使用していたデスクトップ型のパソコン三台。七月二十六日、廃棄のため福岡県志免町にある同社の九州・沖縄地区のサービス拠点に配送中、運送会社の集配所（福岡県粕屋町）で盗難に遭ったという。

職場外で使用するPCのHDD暗号化

報道資料

実はここにも 総務省
MIC Ministry of Internal Affairs and Communications

平成18年4月28日

「職場外のパソコンで仕事をする際のセキュリティガイドライン」の公表

情報通信技術の進歩により、今日の企業活動においては、企業は様々な情報資産を電子データとして保有し、従業員はそれを職場外に持ち出して仕事をする機会が増えています。そして職場外のパソコンで企業データを取り扱ったり、インターネットでそうしたデータをやり取りする機会は今後ますます増えることが予想されます。

しかし、それに伴って、情報の改ざん・紛失など様々な情報セキュリティ上の被害も拡大しています。特に、インターネットに接続する機能を持つコンピュータが大勢を占める中で、ウィニーなどのファイル交換ソフトを介した暴露ウィルスによる機密情報や個人情報の漏えいは、企業に甚大な損失を与えています。

これらの情報セキュリティリスクに対処するために、総務省ではこの度、情報セキュリティ対策をこれから行おうとする組織・企業を対象に、「職場外のパソコンで仕事をする際のセキュリティガイドライン」を策定しましたので、ここに公表します。

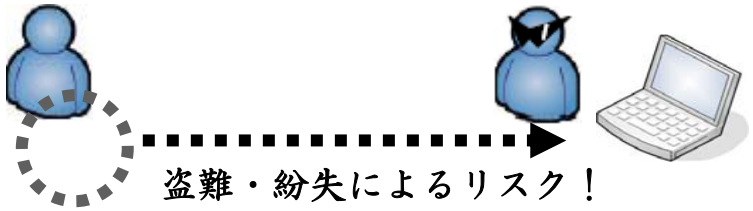
＜職場外のパソコンで仕事をする際のセキュリティ対策18 か条＞

① 情報セキュリティ管理体制（管理者の選任、情報資産の管理方法の策定等）を構築する。
② 職場外でパソコンが使用される場合でも、情報セキュリティポリシーが正しく遵守されているか、定期的なチェック（監査）を実施する。
：

⑯ 機密性の高いデータを保存・送信する際には 必ず暗号化する。
⑰ 社内システムと持ち出し用パソコンの環境の境界線にはファイアウォールやルータなどを設置し、不必要なアクセスを遮断する。
⑱ 社内システム内にある重要データは、安全な領域に格納するとともにアクセス権限の付与は必要最低限とする。

パソコンのハードディスク暗号化

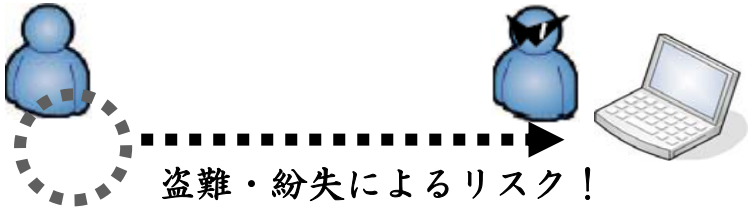
Ⅰ. 暗号化されていないPC



内蔵ハードディスクを取出して別のPCに接続すると・・・。

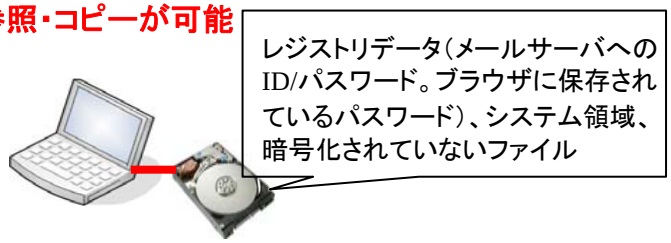
ディスク上の全てのデータの参照・コピーが可能

Ⅱ. ドライブ暗号/ファイル暗号PC



内蔵ハードディスクを取出して別のPCに接続すると・・・。

レジストリ、システム領域、非暗号のデータの参照・コピーが可能



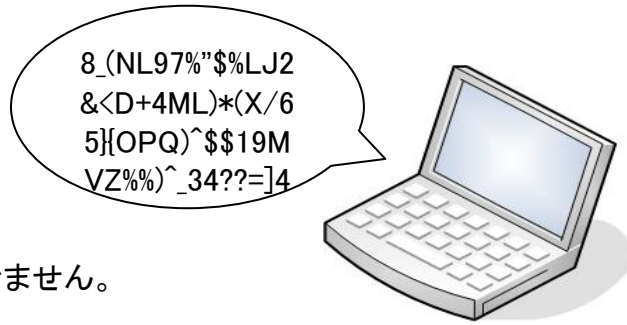
Ⅲ. ハードディスク丸ごと暗号PC

内蔵ハードディスクを取出して別のPCに接続すると・・・。

ディスクへのアクセス、あらゆるデータの参照・コピーは不可能

SecureDocとは

PCのハードディスクを丸ごと暗号化するソフトです。



- ユーザの暗号化／復号化の操作は必要ありません。
  （PCの外部へ持ち出すデータは、暗号化操作が必要です）
- ディスクが暗号化されているため、PCが盗まれてもデータを読み取る事はできません。

【主な機能】

1. ハードディスク暗号化
   ハードディスクを丸ごと暗号化します。
2. ブート制御（BIOSレベルでのユーザ認証）
   PC起動時にパスワードを要求することができます。
3. ファイル暗号化機能
   ファイル/フォルダ単位に、明示的に暗号化することが可能です。
4. 外部媒体使用制限・暗号化
   リムーバブルメディアの暗号化・使用制限が可能です。

【主な特徴】

1. 優れたパフォーマンス
   ・標準的なPCで初回暗号は、3~6分/GB程度
   ・日常運用時のCPUへの負荷は、10%未満
2. PCの機能を下げない
   ・「休止モード」、「スタンバイモード」は、従来通り
   そのまま使うことができる
3. Windows上での操作が不要
   ・今までと違うのは、PC起動時の認証だけ
   ・認証以外の操作は何も変わらない

【運用管理形態】

ニーズに合わせた運用管理形態をご提供します。

鍵の管理は暗号化製品の重要ポイントです！
・スタンドアロン
・オフライン管理（ネットワークなしのデータベース管理）
・オンライン管理（ネットワーク経由の集中管理）

SecureDoc
WINMAGIC DATA SECURITY

SecureDocの機能

クライアントPC上のデータをディスクごと暗号化し、情報を保護します。

ハードディスクの暗号化

PCのハードディスクをOSごと自動的に暗号化することにより、第三者による情報データの漏えいを防ぎます。ハードディスクが抜き取られても、他のPCから認識する事はできません。
暗号化・復号化の処理は、ハードディスクアクセスの都度、自動的に行いますので、ユーザーは操作を意識する必要がありません。

BIOSレベルの認証とハードウェアトークンによる認証強化

Windows起動前に認証（BIOSレベルの認証）を要求することで、PCの不正使用防止が可能です。また、USBトークン、ICカード内の鍵を利用してPC起動時の認証強化が可能です。

ファイル／フォルダ単位の暗号化とアクセスコントロール

共有ファイルやPC外部に保管するデータを暗号化することが可能です。個人鍵/グループ鍵により暗号化することで、特定ユーザのみ復号可能とすることができます。

外部媒体の使用制限と暗号化

リムーバブルメディアの丸ごと暗号化と使用制限を行うことが可能です。但し、CD-Rなどのライティングソフトを利用する媒体は対象外です。

Enterprise Server によるクライアント管理

・ユーザ情報集中管理

ユーザの作成、SecureDoc（クライアント）上での権限を決定できます。
管理要件により、集中管理・分散管理の構成をとることが可能です。

・KeyFileの発行、管理

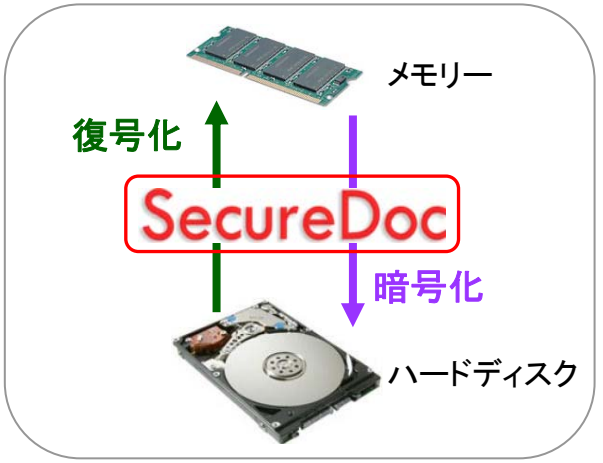
EnterpriseServerにより、暗号化の鍵（KeyFile）の発行管理を行います。
クライアントユーザの権限に応じた、共有鍵の割当てが可能です。

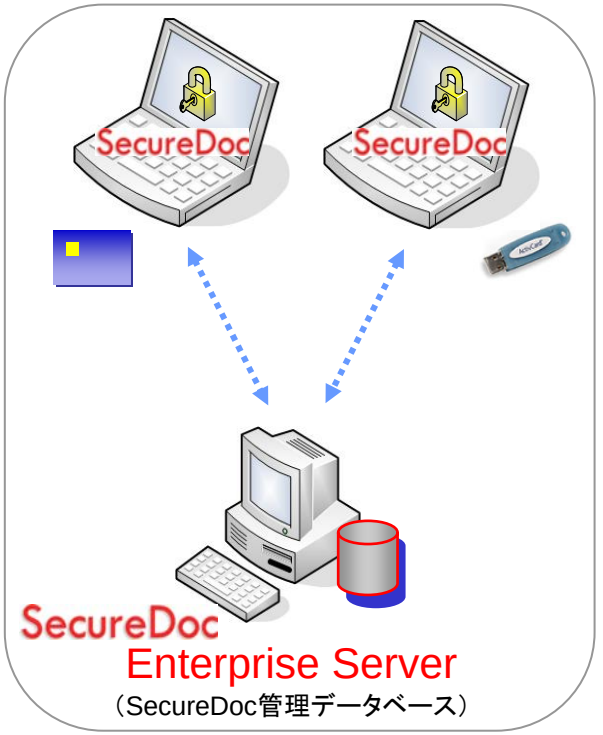
・ユーザがトークンやパスワードを忘れた場合の運用性

管理機能により、チャレンジ＆レスポンスによるパスワードリカバリを行います。
Key Fileを再発行することができます

・通信環境に応じた運用性（PCとの日常的な通信は不要）

社内PCやモバイルPCなど、クライアントPCとの通信の有無に応じた運用が可能です





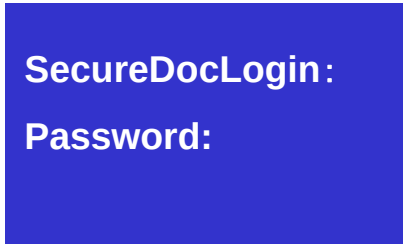
モバイルセキュリティを強化　SecureDocとActivCard等のUSBトークンとの組み合せ例

BIOSレベルでのトークン認証を行います。

多様なUSBトークン、ICカードによる認証
（多様なUSBトークン、ICカードに対応可能です。）

PCを起動

→



SecureDoc 認証画面
（BIOS上）

→ OS起動

※ Windowsログイン画面の省略可能

＜対応トークン、ICカード （例）＞

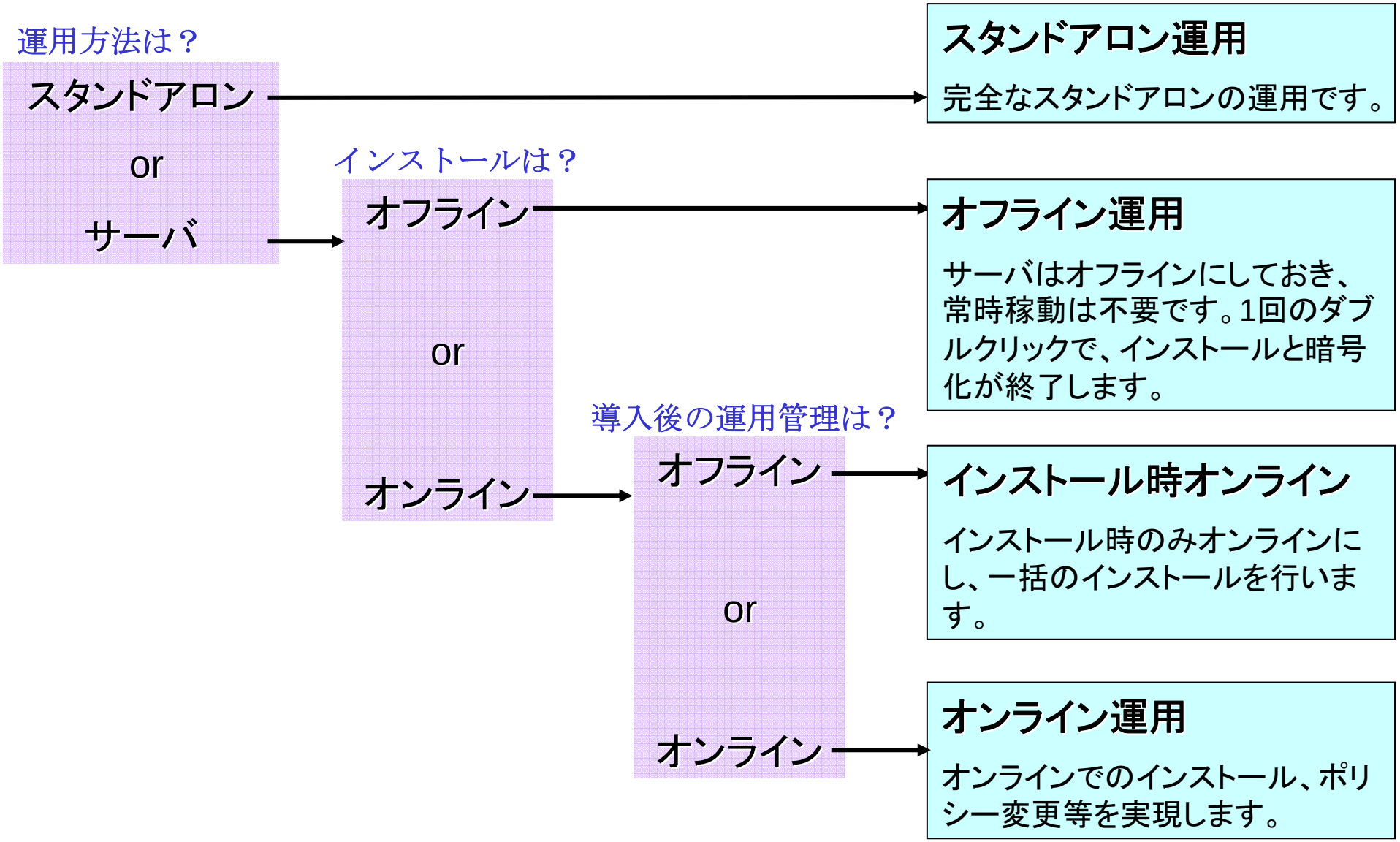
ActivCard

JUJO

Aladdin
SECURING THE GLOBAL VILLAGE

※システム構成により、VPNや無線LAN認証に使用するものと同一のUSBトークン、ICカードにより認証することが可能です。

運用方法の選択


運用方法は？
スタンドアロン
or
サーバ
スタンドアロン運用
完全なスタンドアロンの運用です。
インストールは？
オフライン
or
オンライン
オフライン運用
サーバはオフラインにしておき、常時稼動は不要です。1回のダブルクリックで、インストールと暗号化が終了します。
導入後の運用管理は？
オフライン
or
オンライン
インストール時オンライン
インストール時のみオンラインにし、一括のインストールを行います。
オンライン運用
オンラインでのインストール、ポリシー変更等を実現します。

運用管理形態

①スタンドアロン型

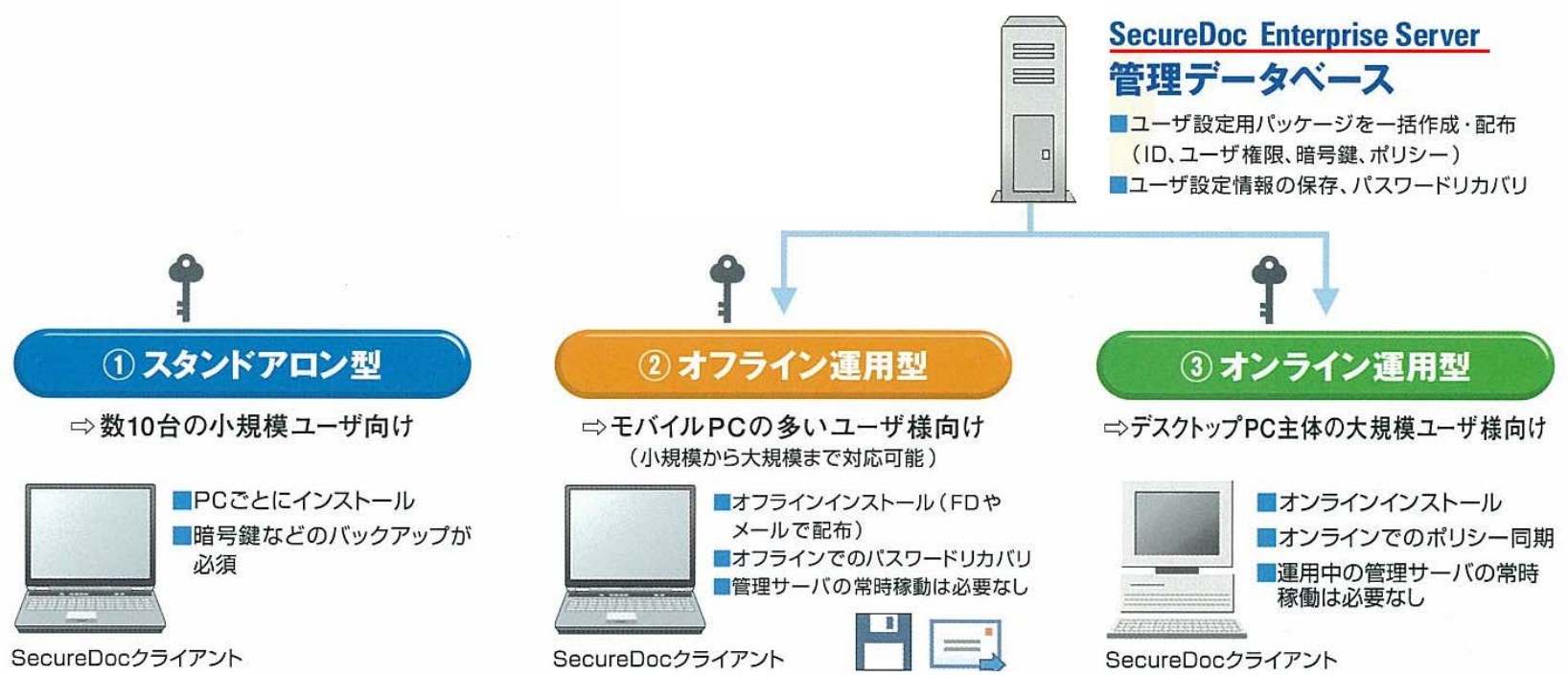
インストールウィザードによって各PCごとにインストールを行います。ユーザー名などの入力が必要です。「NEXT」をクリックし続けることで、基本的な設定がなされ、インストールが完了します。運用はPC単体ごとになり、暗号鍵などユーザー設定情報のバックアップが必要です。主に小規模向けです。

②オフライン運用型

クライアントPC上での一回のダブルクリックだけで、インストール、設定、初回暗号化が行われます。サーバをネットワークに接続する必要はありません。サーバ上で作成された鍵はネットワークを介さず配布することができます。ネットワークを使用しないため、導入展開・運用の設計が容易です。

③オンライン運用型

クライアントPC上での一回のダブルクリックだけで、インストール、設定、初回暗号化が行われます。インストール中に自動的に生成された鍵がサーバに送信されます。また、ユーザー名はWindowsから自動取得することもできます。サーバでのユーザー登録や鍵作成が自動化されるため、データベースを作成する手間がなくなります。各PCは定期的に管理サーバ(SecureDoc Enterprise Server)と通信を行い、ネットワーク経由でのセキュリティポリシーの適用やログの収集を行うことができます。



SecureDoc EnterpriseServerによる運用方法（オフライン、オンライン）

項目	オフライン運用	Connex オンライン運用
利用サーバ	共通のEnterprise Server	
クライアントインストール時のネットワーク接続	不要	必要
KeyFile作成場所	SESサーバ上	クライアント上（クライアントからSESへ送信）
個別ファイルの配布の有無	必要	不要
DB（データベース）作成方法	手作業（ユーザIDなどは、CSVからのインポート化）	クライアントが自動的にSESに書き込むことで作成
管理者のタスク（導入時）	SES上でのユーザIDの作成、Keyの作成、KeyFileの作成、ユーザ個別ファイルの配布	Connexのセットアップ、ネットワーク接続環境の構築
クライアントでのインストール作業	①RemotePackageをCドライブ直下にコピー ②Setup.exeをダブルクリック	①ネットワークへの接続 ②Setup.exeの実行 ③登録シートへの記入（Windowsログイン名を利用する場合は不要）
クライアントでの設定変更	可（要管理者権限）	
オンラインでの設定変更	不可	可
復号化とアンインストール	クライアント上で操作（要管理者権限）	
パスワード リカバリ	チャレンジ&レスポンス、管理者用FD、マスターUSBトークン	
メリット	インストール時にネットワーク接続が不要 複数の端末を共通の鍵で暗号化できる	管理者がデータベースを作成するコストを省く 設定変更が自動的に行われるため容易 暗号が終了した端末がリスト化される
デメリット	データベース作成の手間がかかる 各クライアント上で設定変更する必要がある	少なくともインストール時にネットワーク接続が必要（常時接続は不要）

パスワードリカバリ　チャレンジレスポンスによる復旧

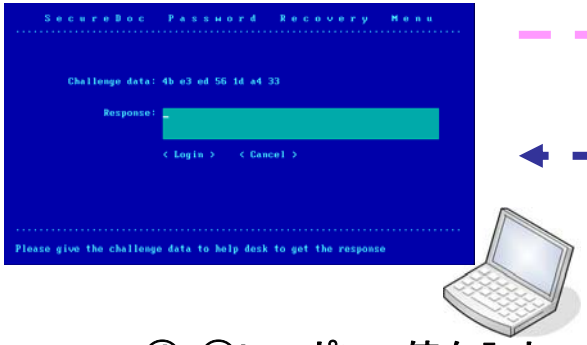
■SecureDoc EnterpriseServer により、ユーザ認証の復旧を、次のような形で実現します。
- ・SecureDoc認証パスワードを、ユーザが忘れた場合
- ・認証トークンを無くした場合

■復旧手順（例）

①クライアントPCを起動します。
②BIOS起動後に、認証画面でユーザIDを入力し、「F8」を押します。チャレンジ値をSES管理者に伝えます（電話やFAX等）。
③SESにて当該ユーザプロファイル上でレスポンス値を発生させて、SES管理者がユーザへ伝えます。
④ユーザは、レスポンス値を入力して、ログインを実施します。
⑤ログイン後、パスワードを変更するよう要求されますので、変更をします（パスワード認証の場合）。

※一度、利用したレスポンス値を使うことはできません。
※チャレンジ値は、起動の度に変わります。

①・②チャレンジ値を管理者に連絡



チャレンジ値

電話、FAXなどによる連絡

レスポンス値

④・⑤レスポンス値を入力（PCは起動したまま）

③チャレンジ値をユーザのプロファイルを管理クライアントへ指定・入力し、レスポンス値を回答

KeyFileの配布による暗号鍵とポリシーの管理

KeyFileによるポリシー管理

・KeyFileは、Key（暗号鍵）と、ポリシー情報（ユーザ権限情報など）をユーザごとに束ねたものです。
・SecureDocはこのKeyFileをユーザ毎に設定することで、ユーザポリシーや暗号鍵の管理を行います。
（SecureDoc EnterpriseServerでは、このKeyFileを一元的に管理します。）

Key

・Keyとは、HDDまたはファイルの暗号・復号を行う暗号鍵（Key）のことです。

ユーザ権限情報

・ユーザがクライアント上のSecureDocユーティリティ上で、設定を変更できる権限を決定します
・管理者権限を持ったKeyFileでログインすると、ローカル上に存在する他のKeyFileの設定の変更、
PCの暗号化の設定の変更等を行うことができます
・ユーザ権限を持ったKeyFileでログインすると、SecureDocユーティリティ上では何もできません

有効期限

・KeyFileには有効期限を設定することができます（V4.2)

	KeyFile	Key	ユーザ権限
ユーザ101	USER101	Key101 Key_ITS admin_1	管理者
⋮			
ユーザ201	USER201	Key_201 Sales_1	一般ユーザ（営業担当）
ユーザ202	USER202	Key_202 Sales_1	一般ユーザ（営業担当）

SecureDoc仕様（スペック）

■SecureDoc Disk Encryption Ver.4.3（クライアント）

暗号化アルゴリズム
- AES（256bit）

動作環境
- OS:Windows 2000 Pro SP4 、XP Pro SP2、
  Vista（Homeを除く）
- CPU：Pentium互換CPU
- メモリ：64MB以上
- 64MB以上の空容量
  （インストールするドライブの10%以上）

標準規格への準拠
- Common Criteria
- FIPS 140-1　Level 2
- NISTによるAES認定

認証方法
- パスワード
- USBトークン、ICカード、指紋認証ICカード
  －ActivKey　－HardKey（十条電子）　－eToken －iKey
- 指紋認証デバイス
  －Puppy
- ICカード
  －ActivCard　－Axalto
- PKI
  －RSA個人鍵、トークン内プロファイル、デジタル証明書
  －PKCS#11準拠
- 対応認証局
  －Entrust, identrus, Microsoft, RSA, VeriSign等

■SecureDoc Enterprise Server Ver.4.3（サーバ）

動作環境（オフライン運用）
- Windows 2000 Pro SP4 ／ XP Pro SP2
  2000 Server SP4／ 2003 Server
- CPU：Pentium互換CPU
- メモリ：64MB以上
- 64M以上の空容量
- DB：MSDE (Microsoft SQL Desktop Engine)／ SQLServer

動作環境（オンライン運用）
- Windows 2000 Server SP4／ 2003 Server
- CPU：Pentium互換CPU
- メモリ：512MB以上
- 64M以上の空容量
- DB：MSDE (Microsoft SQL Desktop Engine)／ SQLServer

SecureDoc 開発元

- **開発元**
  - WinMagic Inc.（カナダ トロント）
- **実績**
  - 世界で100万クライアントの実績
  - 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
- **製品ラインナップ**
  - SecureDoc クライアント
  - SecureDoc Enterprise Server
- **セキュリティレベル**
  - 世界ではじめてAES暗号を取得したディスク暗号化製品（2002年）
  - 下記認定を全て取得している唯一のディスク暗号化製品
  - Common Criteria（ISO策定の情報セキュリティ国際標準規格）
  - FIPS 140-1/-2 Level 2（北米政府機関への暗号化製品調達における必要条件）
  - NSA（米国国家安全保障局）認定

国内総代理店：NCLC
エヌ・シー・エル・コミュニケーション株式会社

何故SecureDocが選ばれるのか？

1. パフォーマンスが高い
- 競合製品と比較したところ初回暗号、暗号化後のPCのパフォーマンスが最も高かった。

2. 使いやすい
- ファイル暗号やドライブ暗号製品と比較したところ、ユーザの操作が必要なく、暗号化できない領域もないのでも使い安いと判断した。
- 休止モードをサポートしているので、パソコンの利便性を損なわないと判断した。
- 暗号化を途中で停止しても、途中から再開できる。

3. 運用しやすい
- 運用の際、拠点ごとに異なる環境に順応できるソリューションが必要だった。ネットワークを利用した運用と、ネットワークを利用しない運用が併用できるのはSecureDocだけだったので、SecureDocを選定した。
- ユーザデータや鍵データが、クライアントから自動的に収集される機能に魅力を感じた。

4. トークンサポート
- ICカードでPC起動、PC使用を制御したかった。Windowsログイン制御だけでは、モバイルPCのセキュリティにはならないと考えていた。
- 既に導入していたUSBトークンに対応していた。

5. 製品体系が分かりやすい
- オプション機能などがなく、全ての機能がクライアントに含まれているので分かりやすかった。

SecureDoc主な導入実績（日本国内）とユーザの声（海外）※原文はwww.winmagic.comにてご覧いただけます。

【金融】
- A証券：600ライセンス
- B証券：50ライセンス
- C保険：850ライセンス
- D保険：750ライセンス

【商社】
- A社：5000ライセンス
- B社：500ライセンス

【小売】
- A社：7000ライセンス
- B社：100ライセンス

【人材派遣】
- A社：130ライセンス

【法人】
- A弁護士法人：170ライセンス

【医療】
- A社：3000ライセンス
- B社：550ライセンス

【製造】
- A社：450ライセンス
- B社：400ライセンス

【通信】
- A社：350ライセンス
- B社：150ライセンス

【システムインテグレータ】
- A社：450ライセンス
- B社：150ライセンス
- C社：1800ライセンス

【その他】
- A社：約15000ライセンス

「いくつかの製品を評価しましたが、SecureDocのパフォーマンス、使いやすさ、セキュリティの高さは圧倒的でした。
また、集中管理の運用方法も大きな優位点でした。」
～ Michael Scott, Manager, Network Infrastructure and Security, Witness Systems, Inc.（米国）～

「弊社は、自社で販売するモバイルユーザー向けのVPN機器“Thales Trusted VPN”との組合せ販売の製品として、慎重にHDD暗号化製品の検証を実施しました。国際的なセキュリティスタンダードへの準拠、機能、ユーザーの使い勝手、価格など、組合せに必要な要件を厳しくテストした結果、WinMagic社のSecureDocの採用を決定しました。弊社は現在、モバイルユーザーやSOHOユーザーに、より完全なセュリティソリューションの提供が可能となりました。」
～ Nils Klippenberg, Director e-Security, THALES Communication（ノルウェイ）～

「SecureDocのセクターレベルでの暗号化技術は大変すばらしい。一番下位の階層で読み込み書き込みのリスエストすべてに対応するためHDD全体の暗号化が可能となり、セクター単位でも暗号化の漏れがありません。強力で信頼性の高い暗号化アルゴリズムでSecureDocはわかりやすい製品デザインに仕上がっています。」
～ Bruce Schneier, world renowned cryptographer, author of “Applied Cryptography”, CTO of Counterpane Internet Security, Inc（米国）～

SecureDoc FAQ

1. マルチOSに対応していますか？
- 対応しています。但し、Windowsのみです。

2. Windowsへのシングルサインオンには対応していますか？
- 対応しています。（Vistaは不可）

3. ユーザにパスワードルールを強制させることができますか？
- できます。
  例えば、XX桁以上、大文字をXX桁以上使う、以前使用したパスワードを禁止する、等のパスワードを強制させることができます。

4. ユーザはPCの復号化ができますか？
- 権限によって、復号化の禁止、許可が選択できます。

5. クライアントPCのロギング機能はありますか？
- あります。
  SecureDoc上の動作（設定変更、認証の可否）を記録します。

6. PKI対応とはどのようなものですか？
- 認証デバイス内のデジタル証明書を利用して、PCを起動することができます。通常、認証デバイスにはSecureDoc独自の鍵を格納しますが、既存のデジタル証明書を利用することができます。

7. SD Connex（オンライン運用）の場合は常にネットワーク接続は必要ですか？
- いいえ、オンライン接続はインストールの瞬間か、インストール直後のみです。

8. ディスクが暗号化されたことはサーバなどで確認することができますか？
- はい、できます。ログを参照することができます。また、Connexを使うとSecureDocをインストールしたコンピュータ名が自動的にサーバに登録されます。

SecureDocライセンス料金

SecureDoc （クライアントライセンス）

型番	ライセンス数	標準単価(税別)
WMUS-SD4-405	5-24	25,000
WMUS-SD4-425	25-49	22,500
WMUS-SD4-450	50-99	21,000
WMUS-SD4-4100	100-499	16,500
WMUS-SD4-4500	500-999	15,000
WMUS-SD4-41000	1000-	CALL

※初回ご注文時に、インストールCD（プログラム、マニュアル）を1セットご提供致します。
※最低販売ライセンス数は5ライセンスです。
※50ライセンス以上をご注文頂いた場合は、SecureDocEnterpriseServerを初回1ライセンス分のみ無償でご提供致します。
（但し、年間アップデートサービスは有償になります）

- クライアント及びサーバーライセンスともに、標準価格の１５％が年間アップデートサービスとして初年度より発生します。
- 年間アップデートサービスの内容は、SecureDocソフトウェアのパッチ、マイナーバージョンアップのご提供です。また、優待価格でメジャーバージョンアップをご提供します。

SecureDoc EnterpriseServer （サーバライセンス）

型番	ライセンス数	標準単価（税別）
WMUS-CDBV4	1	160,000

※1ライセンスには、管理者1名分の使用権、500クライアントユーザまでのデータベース使用権が含まれます。
※データベースの数に応じて、サーバライセンスの追加が必要です。
例）100ユーザのデータベースを3つ構築する場合は3つのサーバライセンスが必要になります。

【お問い合わせ・評価用貸出CDのお申し込みをお待ちしております】

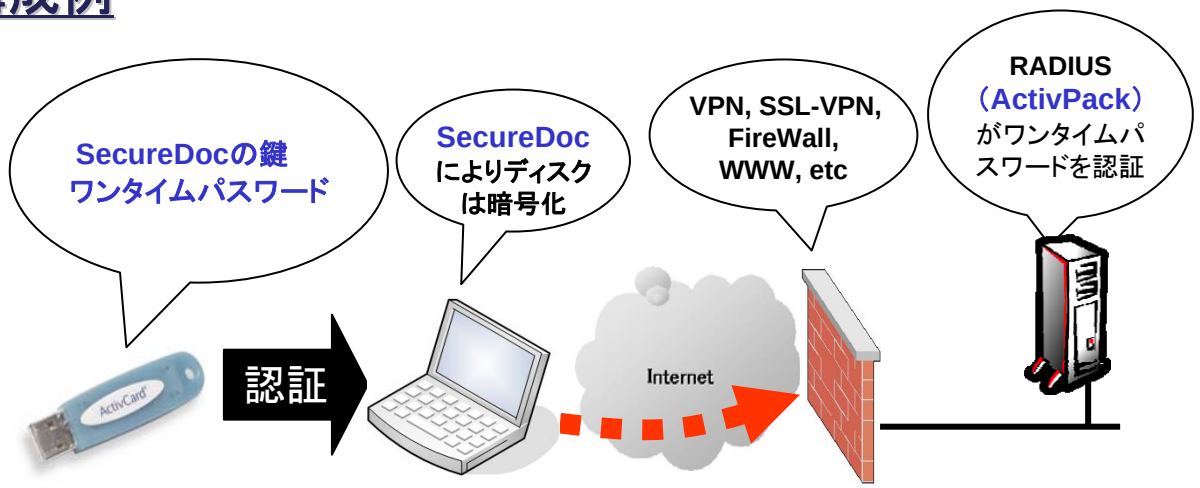
JBService
株式会社ジェー・ビー・サービス
IBM Business Partner
URL http://www.jbservice.co.jp
E-mail sales@jbservice.co.jp
電話 03-3837-9226

お断り無く本製品の使用及び製品内容や標準価格を変更する場合がございますので、予めご了承下さい。

その他Solutionの組み合わせ：モバイル統合セキュリティ（SecureDoc+ActivCard）

モバイルには、PCの保護だけではなく、リモートユーザの認証が必要です

構成例



①USBトークンでPC起動　②同じトークが生成するワンタイムパスワードによるSSL、VPNなどの認証

必要な製品：

- SecureDoc
- ActivKey（USBトークン）
- ActivPack（ワンタイムパスワード認証サーバ）

※ ActivKeyだけでもPC起動は可能です。ActivPackはワンタイムパスワードを利用する場合のみ必要です。

（オプション）

- SecureDoc EnterpriseServer

対象になる情報漏えい経路は？

・モバイルPCのディスク
・リモートアクセス可能なサーバ

今まではこんな問題がありました：

・モバイルPCユーザの多くがリモートアクセスを利用しているが、リモートアクセス認証ができる製品でPCのディスクを守る製品が見つからなかった。

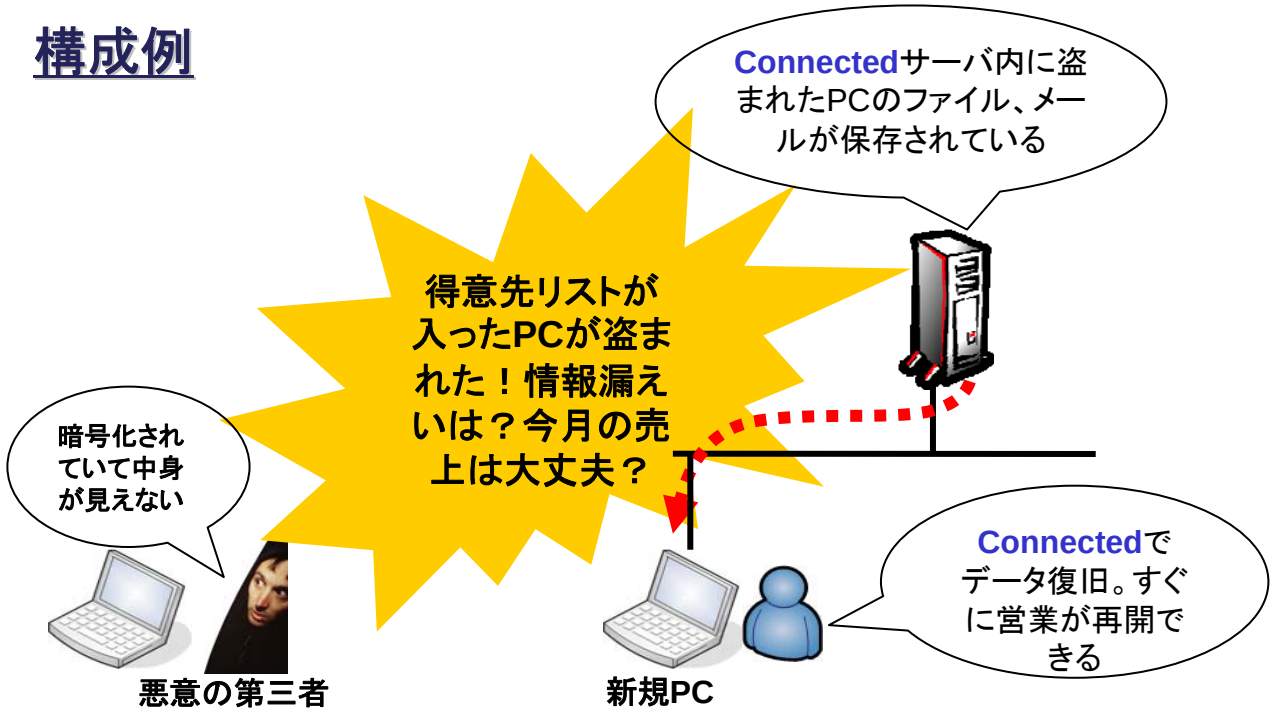
メリット：

・ワンタイムパスワードで、安全なリモートアクセス
・USBトークン1本でPC起動からVPN認証まで、ユーザへの負荷を削減
・USBトークンがなければ、「PCが使えない」「リモートアクセスができない」簡単で高いセキュリティが構築される

その他Solutionの組み合わせ： 暗号化の上にバックアップすれば更に安心（SecureDoc+Connected）

PCが盗まれた・・・SecureDocならデータは盗まれませんが、なくしたデータはどうしますか？

構成例



必要な製品：

- SecureDoc
- Connectedクライアント（バックアップ）
- Connected（サーバ）

（オプション）

- SecureDoc EnterpriseServer

対象になるリスクは？

・PC盗難、紛失の際の情報漏えい
・PC盗難、紛失、破損の際のデータ損失（機会損失）

今まではこんな問題がありました：

・ファイル毎の暗号化はユーザにとって大きな負担
・ファイル毎のバックアップはユーザにとって大きな負担
・手動でファイルサーバに保存しても差分管理はできない

メリット：

・Connectedは全てをバックアップ、SecureDocは全てを暗号化、ユーザに負荷をかけさせません
・PC内のデータの安全と保全を確実にします

SecureDoc v4.3 ハイライト（クライアント）

Vista対応

■ 他社製品のVista対応

– 国内でVista対応を発表しているディスク暗号化製品はありません（2007年7月現在）

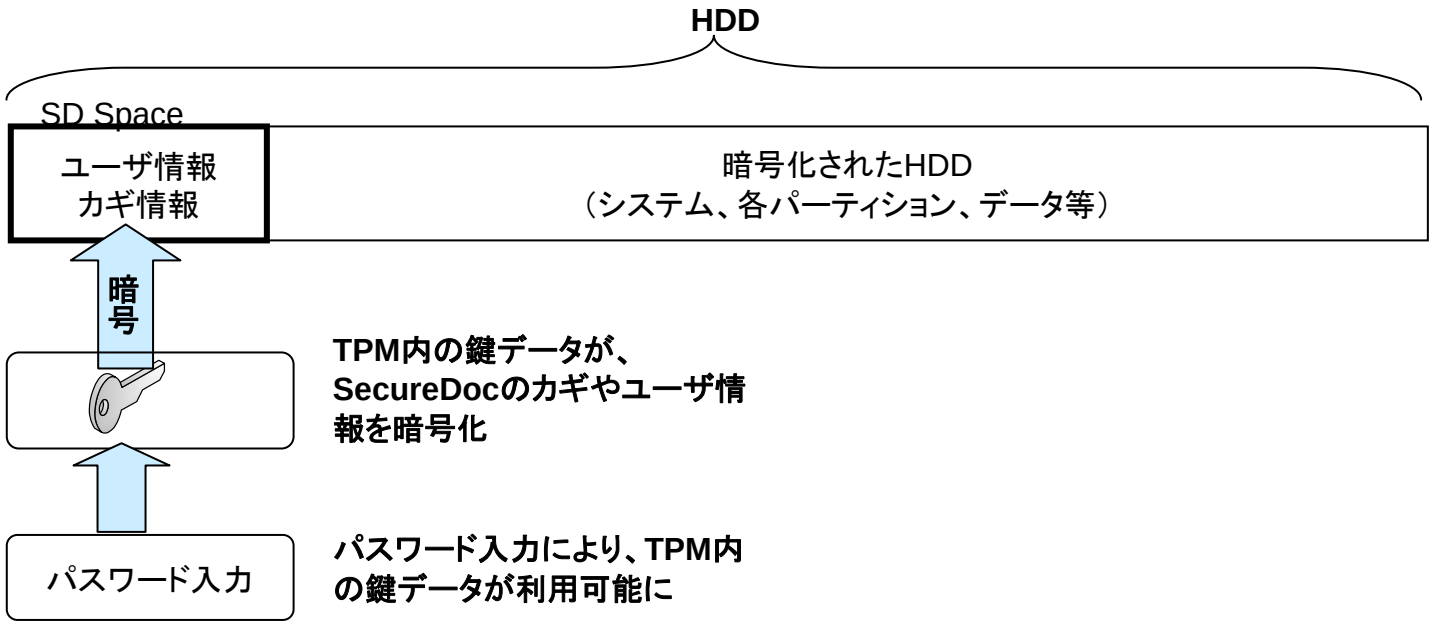
■ Vistaで利用する場合の注意点

– USBトークン、ICカード製品がVistaに対応していないため、トークン連携をご希望されるお客様の場合は、対応状況を弊社にご確認ください。

– Vistaに関する制限事項があります。詳細は Vistaでの「SecureDocv4.3Jの注意事項.doc」をご参照ください

TPM1.2対応

TPM1.2内の鍵データが、KeyFileを保護します。
使い勝手は、パスワードを利用して認証するのと同じです。



SecureDoc v4.3 ハイライト（クライアント）

パスワードによるメディア暗号とMedia Viewer

■ パスワードによるメディア暗号

- これまでは、暗号化されたメディアを閲覧するには、SecureDocの「カギ」の共有が必要でした。カギの共有には、サーバを介して行うため、手間がかかりました。
- パスワードで暗号化すれば「カギ」の共有は不要です。
- これまで通り、共有「カギ」を使った暗号も可能です。

■ 暗号化方法の簡易化

- USBメモリを接続すると、自動的に暗号化する機能が付加されました。
- マイコンピュータ上のアイコンを右クリックすることでも、暗号化を行うことができます（これまでは、SecureDoc Control Centerにログインする必要がありました）。

■ Media Viewerによる暗号メディア閲覧

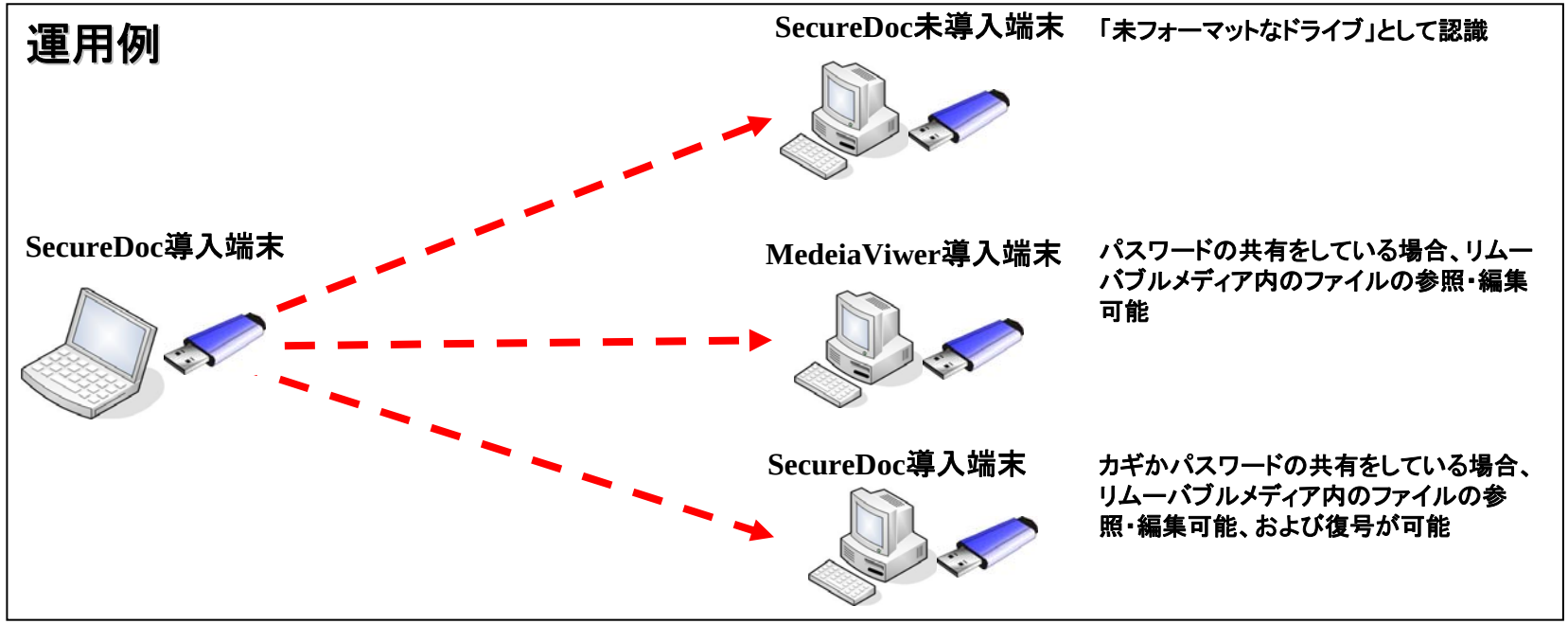
- これまでは、暗号化されたメディアを閲覧したり、データを書き込むには、SecureDocのインストールが必要でした。v4.3のMedia Viewerをインストールすれば、暗号化メディアの読み込み/書き込みができるようになります。
- MediaViewerでアクセスできるのは、暗号化の時に、パスワードが設定されたメディアだけです。カギによって暗号化されたメディアは、MediaViewerはサポートしません。
- MediaViewerは、Vistaに対応していません。

SecureDoc v4.3 ハイライト（クライアント）

パスワードによるメディア暗号とMedia Viewer

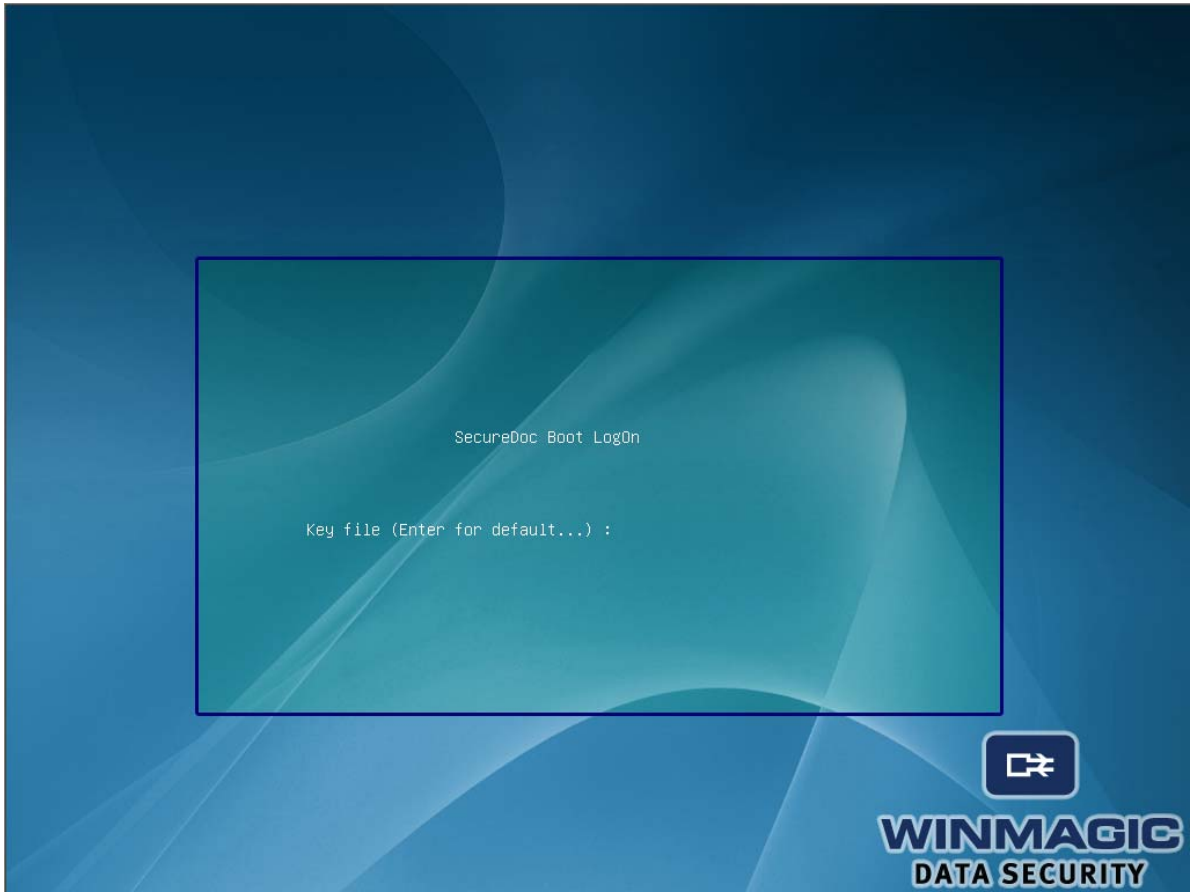
SecureDocとMediaViewerの比較

	SecureDoc	MediaViewer
メディアの暗号化	○（要権限）	×
メディアの復号状態への変換	○（要権限）	×
暗号化メディアへの読み込み/書き込み	○	○



SecureDoc v4.3 ハイライト（クライアント）

ブートログオンのグラフィック化



- ブートログオン起動直前で、[Back space]を押し続けることで、以前のブートログオン画面に、戻すことができます。この設定は、再び同じ操作をするまで反映されます。
- チャレンジ&レスポンス実行時に、ユーザIDがクライアント画面に表示されるようになりました。

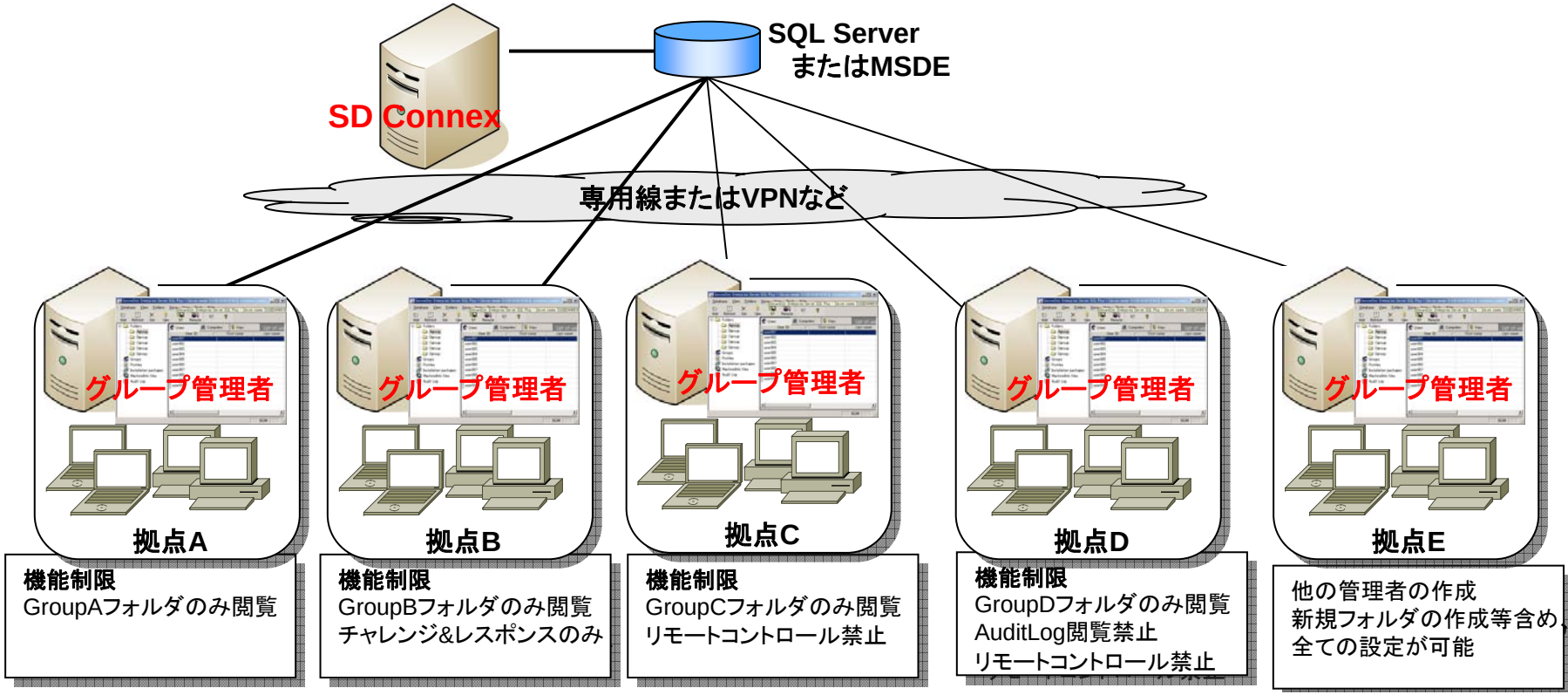
SecureDoc v4.3ハイライト（ SecureDocEnterpriseServer）

グループ管理者の作成

グループ管理者とは対象のグループのみを閲覧し、管理できる管理者のことです。SESで追加の管理者を作成する時に、対象のグループを指定することができます。

■ 管理者権限の種類

- パスワードリカバリー（チャレンジ&レスポンス）のみ操作可能
- SESの操作ログの閲覧権限
- クライアントのリモートコントロール（強制シャットダウン等）の実行権限
- 他のSES管理者ユーザの作成権限



SecureDoc v4.3ハイライト（ SecureDocEnterpriseServer）

暗号化状況のモニタリング

- 暗号化状況の把握が容易になりました
  - オンライン運用時に、
    - 暗号化が開始されていない、
    - 暗号化途中である、
    - 暗号化が完了している、
    - という状況が明示的にSESに表示されます。

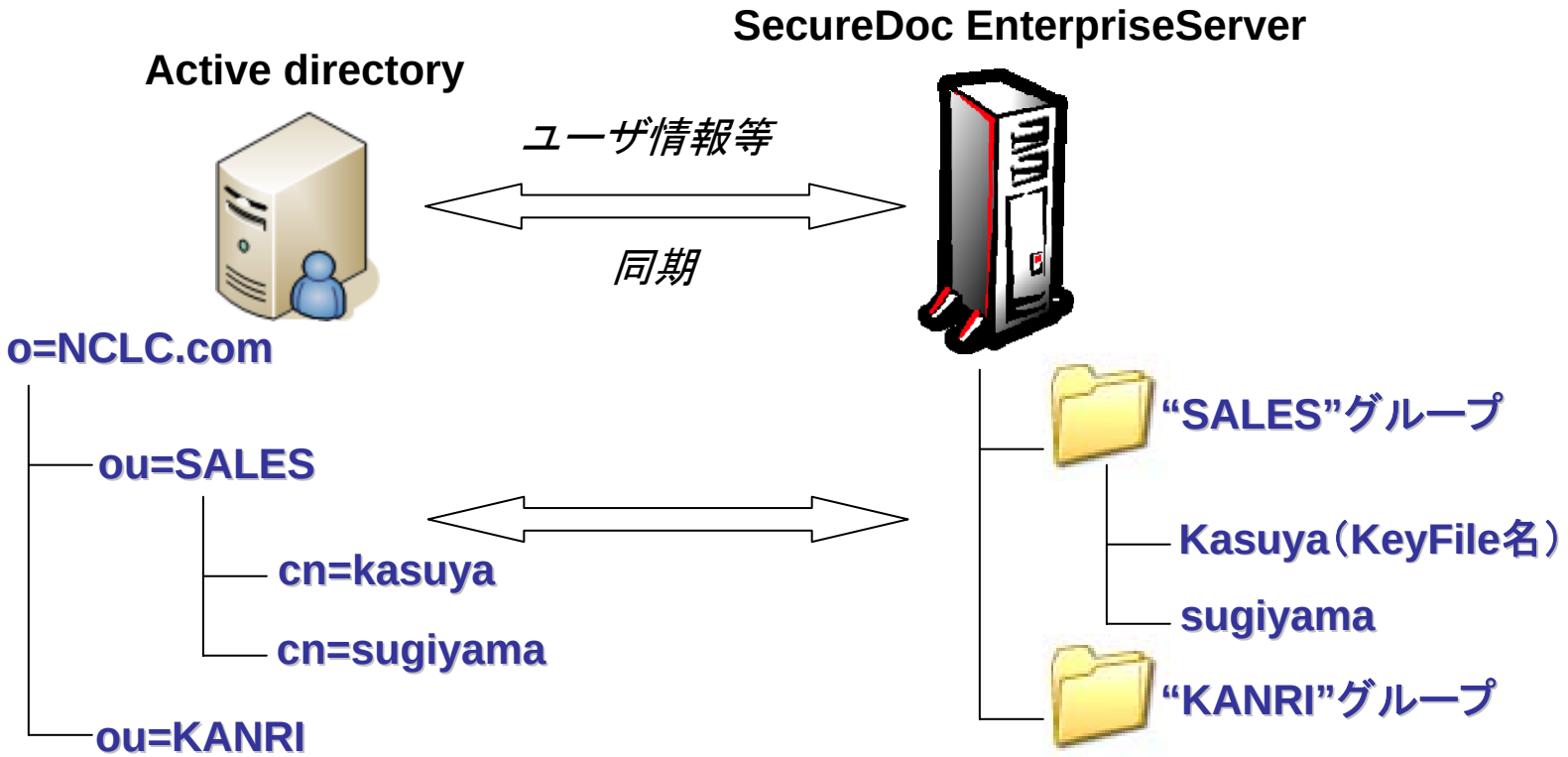
SD Connexの強化

- SD Connexの処理能力向上
  - Windowsサービスとしての安定稼動
  - 帯域の狭い環境からのアクセスでも対応可能
- SD Connex管理機能
  - サーバ障害発生時のメール通知機能
  - Connex専用証明書が標準で付属
- アクセス管理
  - 「〇〇日間」サーバにアクセスしていないユーザの端末へのログインを禁止することができます

SecureDoc v4.3ハイライト（ SecureDocEnterpriseServer）

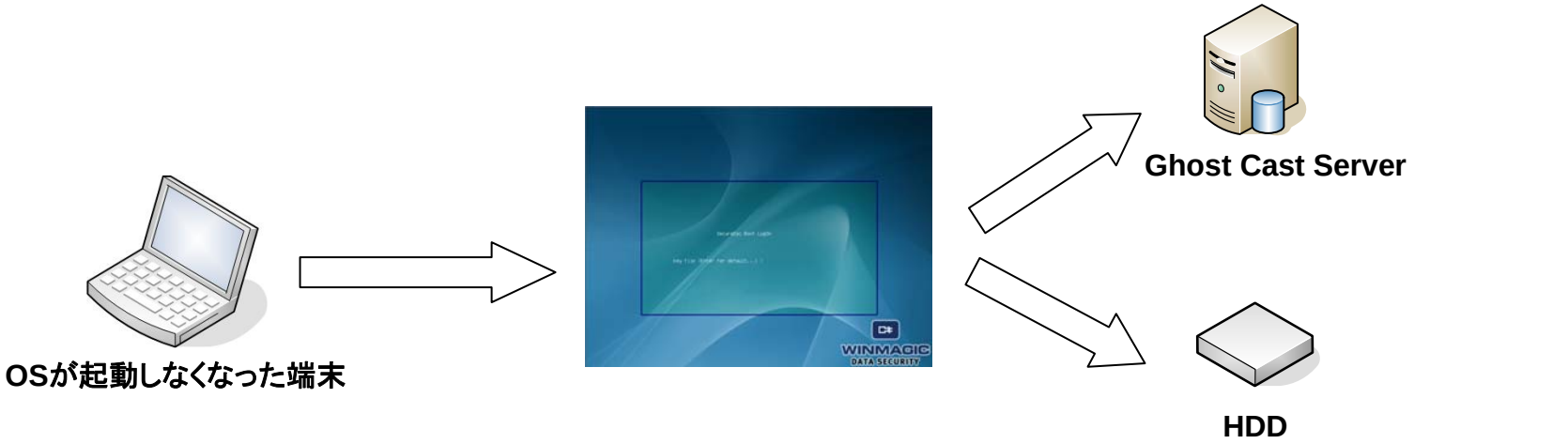
ActiveDirectory連携

- ActiveDirectoryとSESがユーザデータベースを共有し、ユーザデータ管理の一元化を実現します



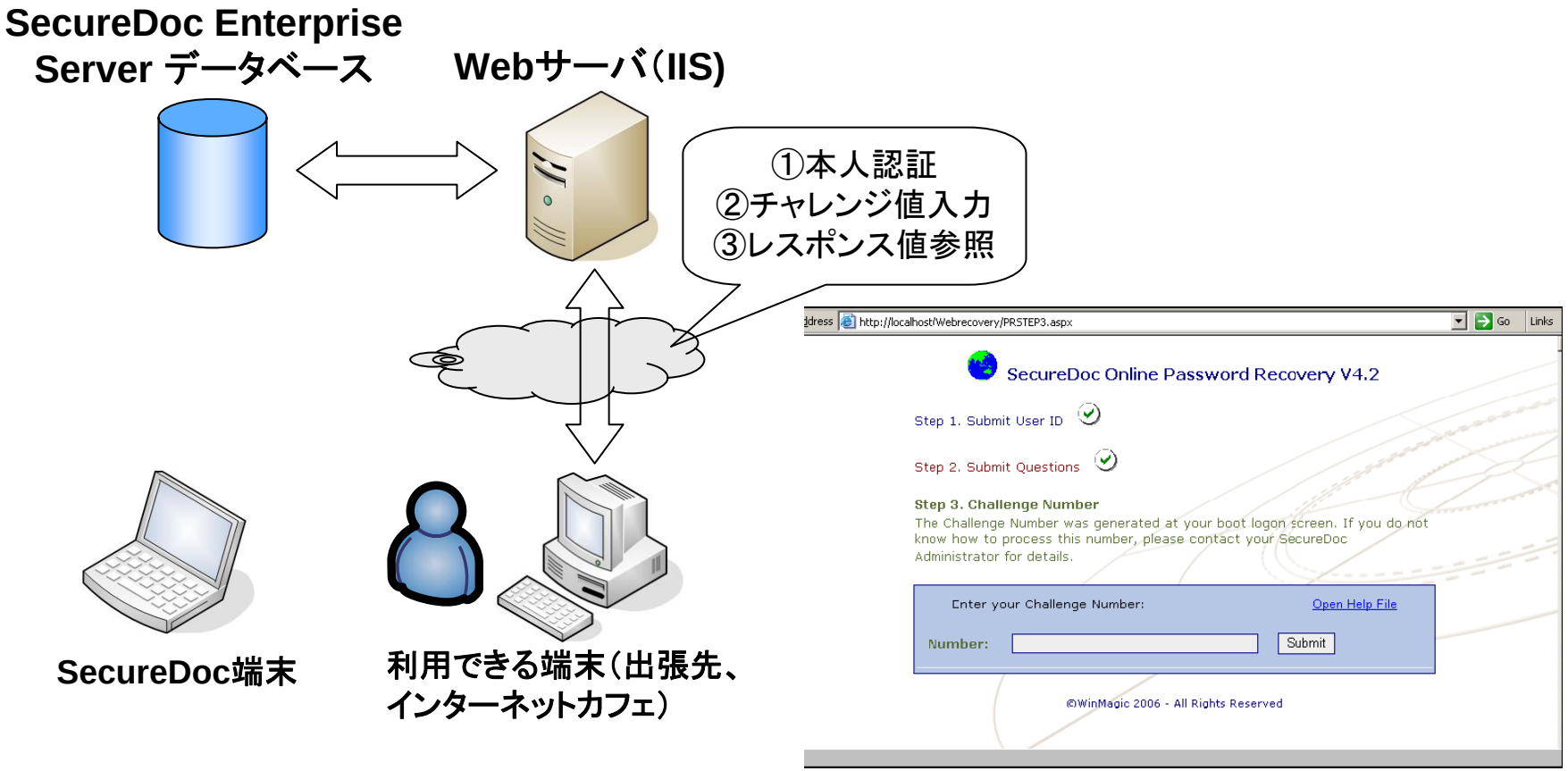
SecureDoc v4.3でこんなこともできます　：　暗号化ディスクのイメージバックアップ

- 暗号化した端末のOSが起動しなくなった!?
  - PE BuilderやGhostを使えば、即時データを救済することができます



SecureDoc v4.3でこんなこともできます　：　オンラインパスワードリカバリ

- オンラインパスワードリカバリ
  - チャレンジ&レスポンスのWeb化



Contact us

株式会社ジェー・ビー・サービス

Contact us
〒110-0016 東京都台東区台東2－29－12　ｻﾝｹｴﾎﾜｲﾄﾋﾞﾙ
TEL : 03-3837-9226　FAX : 03-3837-9236
ホームページ : http://www.jbservice.co.jp
E-mail : sales@jbservice.co.jp