XXXXXXXXXXXXXXXX 様

暗号技術導入計画書（雛形）

― モバイル PC に対する EFS／BitLocker の導入 ―

（2012/xx/xx）

XXXXXXXXXXXXXXXX

本雛形をご利用される前に、以下の事項をお読み下さい。

本雛形の利用方法

本雛形は、「暗号技術導入に関するコンサルティング手引書- Windows EFS／BitLocker 編-」に沿って PC の暗号化を導入支援する上で必要となる「暗号技術導入計画書」を作成するためのベースとなる資料です。導入する暗号技術は、Windows OS に標準で搭載されている EFS（ファイル暗号化システム）および BitLocker（ディスクボリューム暗号化機能）を対象としており、それぞれの機能が搭載された PC に対してその機能を有効化する際に事前に整理すべき情報や基本的な導入手順のモデルを示したものです。
試験的に暗号化する対象となる PC の情報や暗号化に利用する機能（EFS および BitLocker）などの情報は、導入対象となる企業の状況に合わせて修正してご利用下さい。

修正のポイント

「暗号技術導入計画書」を作成するにあたって、以下の点を考慮して本雛形を修正してください。

- 上記利用方法でも述べたとおり、暗号化する対象となる PC や暗号化に利用する機能、あるいは暗号化するフォルダやドライブ等の運用形態については、導入対象となる企業の状況に合わせて修正してください。
- 本雛形は、コンサルタントが導入対象となる企業に提示することを想定して作成されたものです。巻末の付録 1 および付録 2 に記載されている内容は、「暗号技術導入に関するコンサルティング手引書- Windows EFS／BitLocker 編-」に記載されている内容と同様です。

ご利用にあたっての注意事項

ご意見等連絡先

本雛形に関するご意見・ご感想・ご質問等がありましたら、以下の E-mail までご連絡下さい。
E-mail：ango_info@iisec.ac.jp

はじめに

本書は XXXXXXXX 様（以下、御社）に対する暗号技術導入コンサルティングの一環として、御社で実施される Windows ノート PC への暗号システムの導入に関する手順や導入後の進め方等を記述したものです。

本書で対象としている暗号システムは、Windows OS に標準で搭載されている EFS（暗号化ファイルシステム）および BitLocker です。EFS や BitLocker の詳細については本書の付録をご参照ください。

本書の構成は以下の通りです。

1. 暗号技術導入の流れ
2. 暗号技術導入の概要
3. 試験導入の手順
4. 試験運用時のチェック項目
5. 社内展開に向けて

付録１：EFS に関する技術情報
付録２：BitLocker に関する技術情報

1. 暗号技術導入の流れ

暗号技術導入の全体の流れを下図に示します。

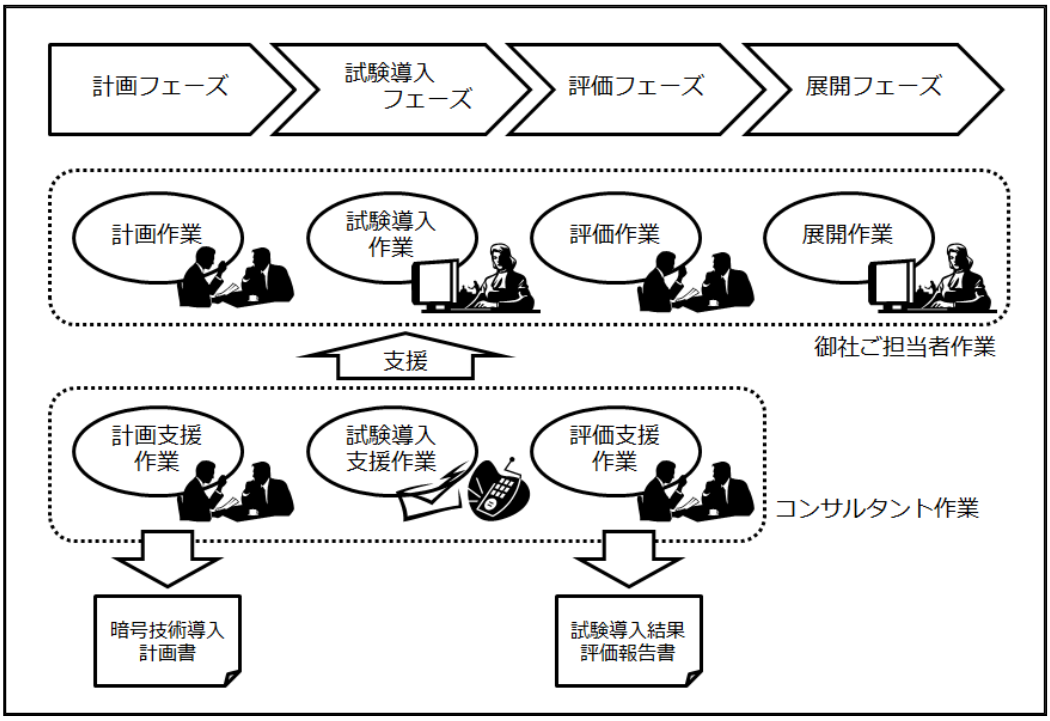


図　暗号技術導入の流れ

- 計画フェーズ
  計画フェーズでは御社のご担当者と打ち合わせを持ちながら暗号技術導入に関する基本的な考え方を整理し、暗号技術の試験導入対象とするコンピュータ（1～3 台程度）の選定や暗号対象データの決定、今後の進め方の検討などを行います。コンサルタントはその結果を「暗号技術導入計画書」（本書）としてまとめます。

- 試験導入フェーズ
  試験導入フェーズでは計画書に基づいてコンピュータに対する暗号技術の試験的な導入を行った後、一定期間運用することで暗号技術導入に起因する問題点を顕在化させます。導入や運用に関わる作業は御社にて実施し、コンサルタントは電子メールや電話による導入支援を行います。

- 評価フェーズ
  ここでは前フェーズにおける試験導入および一定期間の運用後、導入過程や試験運用時における問題点などをヒアリングして評価を実施します。コンサルタントはその結果を「試験導入結果評価報告書」としてまとめます。今回のコンサルティング作業は基本的にはこの時点で完了となります。

- 展開フェーズ
  導入計画書および評価報告書を基に、御社内部で社内的に暗号技術の展開（他のコンピュータへの導入、Windows ドメインへの統合など）を進めるフェーズです。

2. 暗号技術導入の概要

ここでは御社における暗号技術の導入に関する概要を述べます。

A) 試験導入対象のコンピュータ

試験導入フェーズにて暗号技術を導入するコンピュータは以下の 2 台とします。

メーカー名、機種名	IBM ThinkPad X31
社内における識別情報（ホスト名等）	XXXXXXXX
OS 種類、エディション、サービスパック	Windows XP Professional
Windows ドメイン環境	スタンドアローン
備考	（使用形態、ハードウェア構成、その他特記すべき事項を記載）

メーカー名、機種名	Toshiba Dynabook R731/C
社内における識別情報（ホスト名等）	XXXXXXXX
OS 種類、エディション、サービスパック	Windows 7 Ultimate
Windows ドメイン環境	スタンドアローン
備考	（使用形態、ハードウェア構成、その他特記すべき事項を記載）

B) 使用する暗号技術と暗号化の対象

ThinkPad については OS が XP（Professional）であるため、導入する暗号技術は EFS とします。暗号化が必要な情報は一時的に使用するパワーポイント資料等であることから、該当ユーザの「マイドキュメント」フォルダを EFS で暗号化し、常にマイドキュメントにそれらのデータを格納するような運用形態を採用します。

Dynabook については OS が Windows 7 Ultimate であり、かつ TPM が装備されているので、BitLocker で OS ドライブ（C ドライブ）全体を暗号化し、暗号鍵は TPM に格納するような運用形態を採用します。また第三者による不正な OS 起動を避けるために TPM には PIN（暗証番号）を設定します。

C) データ回復に関する方針

暗号技術を導入する上で非常に重要になるのが「データ回復」です。暗号化された情報は「鍵」がなければ読み出すことができません。つまり鍵を安全に管理することによって暗号技術は情報の機密性を確保しているわけですが、一方でこの鍵はコンピュータのハードウェア障害やユーザの誤操作などにより消失してしまう危険性があります。また組織内における監査等のために、権限の与えられたシステム管理者がユーザの暗号化情報にアクセスしなければならない場合も考えられます。

このような事態に備え、暗号技術を導入する際には事前に確実なデータ回復の手段を検討し、用意しておく必要があります。データ回復を行うことでユーザは万一鍵を失った場合でも確実に自分の機密情報へのアクセスを取り戻すことができ、またシステム管理者は業務上必要な範囲でユーザの機密情報へアクセスすることが可能になります。

今回導入する EFS および BitLocker のデータ回復方法については、基本方針として以下の考え方に基づくこととします。（データ回復に関する詳細については付録資料を参照してください）

- システム管理者はすべてのコンピュータ／ユーザの暗号化データを回復することができる
- EFS の場合、ユーザは自分が暗号化したデータを回復することができる
- BitLocker の場合、ユーザは自分のコンピュータの暗号化データを回復することができる

D)　試験導入および評価フェーズのスケジュール

試験導入フェーズはおおむね xx 月 xx 日までと考え、その結果を受けて xx 月末までを評価フェーズとして位置づけます。

E)　連絡体制

御社のご担当者および担当コンサルタントの連絡先を以下に示します。

- 御社ご担当者

株式会社 XXXXXXXX	XXXX 部　XXXX 課　XXXXXXXX 様
	電話：xx-xxxx-xxxx　E-Mail：xxxx@xxxx.xx.xx
株式会社 XXXXXXXX	XXXX 部　XXXX 課　XXXXXXXX 様
	電話：xx-xxxx-xxxx　E-Mail：xxxx@xxxx.xx.xx

- 担当コンサルタント

株式会社 XXXXXXXX	XXXX 部　XXXX 課　XXXXXXXX
	電話：xx-xxxx-xxxx　E-Mail：xxxx@xxxx.xx.xx
株式会社 XXXXXXXX	XXXX 部　XXXX 課　XXXXXXXX
	電話：xx-xxxx-xxxx　E-Mail：xxxx@xxxx.xx.xx

3. 試験導入の手順

ここでは試験導入の際の具体的手順について、導入対象のコンピュータごとに記述します。

A) IBM ThinkPad X31

IBM ThinkPad X32 には EFS を導入し、該当ユーザの「マイドキュメント」フォルダを暗号化します。そのための EFS 導入手順の流れを下図に示します。図中の網掛け部分はシステム管理者の作業手順を、それ以外はユーザの作業手順を表しています。

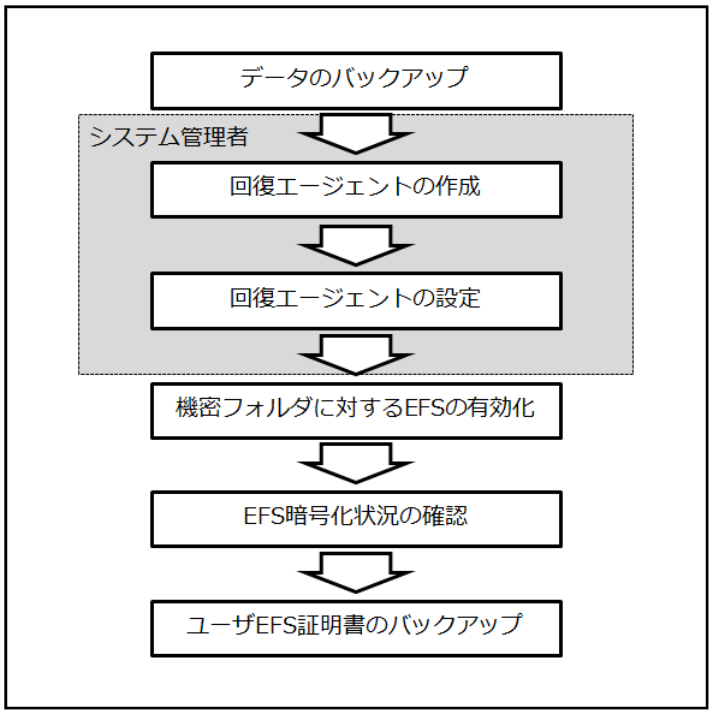


図　EFS 導入手順の流れ

- データのバックアップ【ユーザが実行】
  万一の場合に備え、暗号化対象ファイルのデータバックアップを取得する

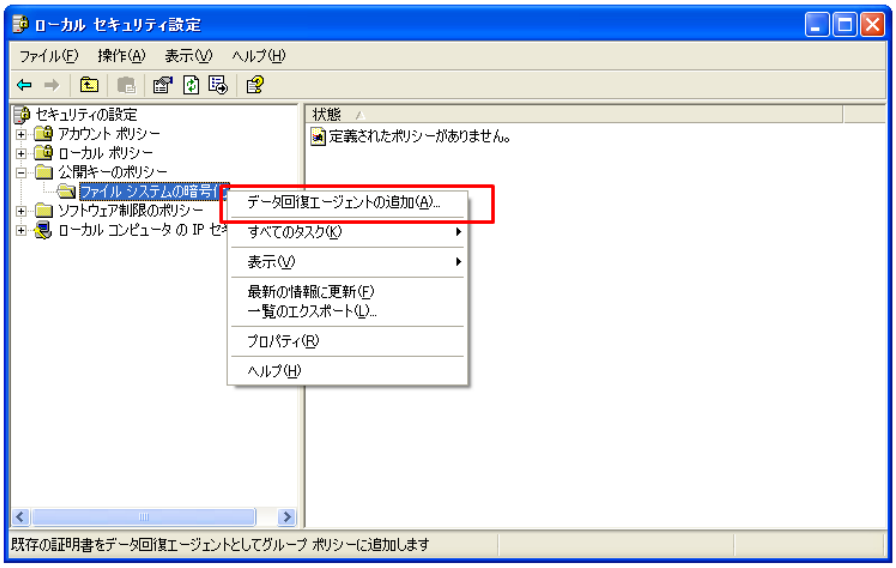
- 回復エージェントの作成【システム管理者が実行】
  システム管理用のコンピュータ上（XP 以降）で以下のコマンドを実行し、回復エージェントの EFS 証明書を作成する

  cipher /R:EFSRecover　　（注：「EFSRecover」は任意のファイル名）

  カレントフォルダに回復エージェント証明書のファイル「EFSRecover.PFX（証明書と秘密鍵）」および「EFSRecover..CER（証明書のみ）」が生成される

  EFSRecover.PFX は別メディアへバックアップするとともにシステム管理者のみがアクセスできるよう厳重にアクセス制限を設定し、入力した保護パスワードも安全に記録しておく

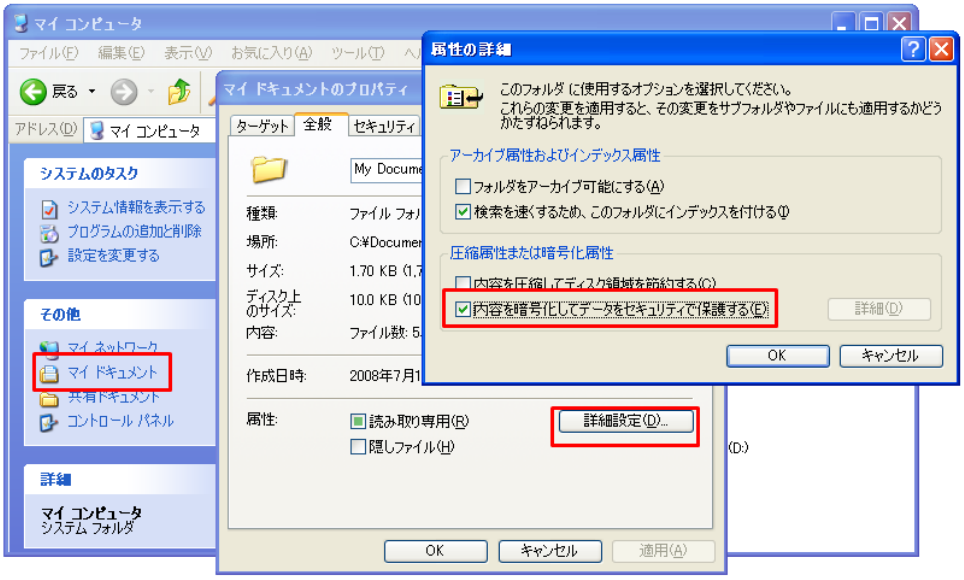
- 回復エージェントの設定【システム管理者が実行】
  EFS で暗号化するコンピュータに管理者権限でログオン、「コントロールパネル」の「管理ツール」から「ローカルセキュリティポリシー」を開き、「公開キーのポリシー」の中にある「ファイルシステムの暗号化」を右クリック、メニューから「データ回復エージェントの追加」を選択



  システム管理用コンピュータで作成した「EFSRecover..CER」を当該コンピュータへコピーし、「回復エージェントの追加ウィザード」でそのファイルを指定することによりデータ回復エージェントとして登録

  EFSRecover.CER ファイルを当該コンピュータ上から削除し、ログアウト

- 機密フォルダに対する EFS の有効化【ユーザが実行】
  当該コンピュータを利用するユーザのアカウントでログオンした後、EFS で暗号化する対象の機密フォルダ（マイドキュメント）についてエクスプローラでプロパティを開き、「全般」タブの「詳細設定」ボタンで「属性の詳細」ウィンドウを表示させ、「内容を暗号化してデータをセキュリティで保護する」にチェックを入れる

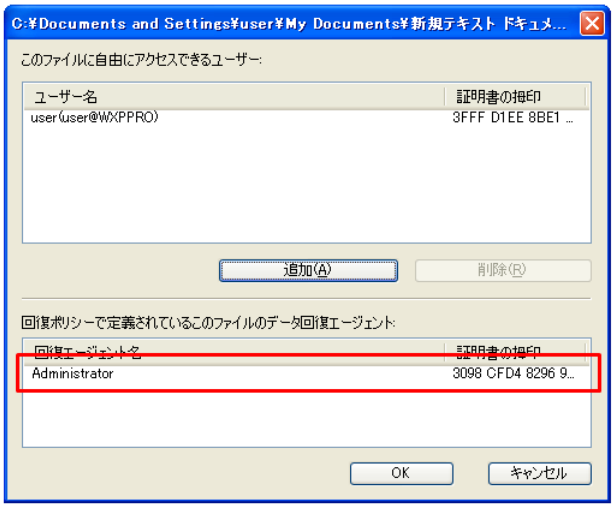


「属性変更の確認」ウィンドウが表示された場合は「このフォルダー、サブフォルダーおよびファイルに変更を適用する」を選択する

この時点で当該ユーザの EFS 証明書が自動生成されると同時に、マイドキュメントフォルダ以下のファイルが EFS で暗号化される

EFS で暗号化されると、エクスプローラ上では暗号化フォルダやファイルの名称が緑色で表示されるようになる
※　圧縮属性のついているフォルダやファイルは EFS では暗号化できないので注意

- EFS 暗号化状況の確認【ユーザが実行】
  暗号化された任意のファイルについてエクスプローラでプロパティを開き、「属性の詳細」ウィンドウで「詳細」を押して当該ファイルにアクセスできるユーザ証明書と回復証明書の一覧を表示させ、回復エージェントの証明書が下の段に存在することを確認する



もし存在しない場合は、前述の「回復エージェントの設定」手順を再確認する

- ユーザ EFS 証明書のバックアップ【ユーザが実行】
  生成されたユーザの EFS 証明書は、以下のコマンドによりユーザ自身でバックアップを行う

  cipher /X EFSBackup　　（注：「EFSBackup」は任意のファイル名）

  カレントフォルダにユーザ証明書のバックアップファイル「EFSBackup.PFX（証明書と秘密鍵）」が生成されるので、このファイルを別メディアへ移動するとともにユーザのみがアクセスできるよう厳重にアクセス制限を設定し、入力した保護パスワードも安全に記録しておく

NTFS でフォーマットされていれば USB メモリ等のリムーバブルメディア内のファイルを EFS で暗号化することもできます。暗号化の操作方法は上記を参考にしてください。EFS で暗号化した USB メモリのファイルを他のコンピュータ上で読み書きしたい場合は、そのコンピュータにユーザの EFS 証明書をインポートする必要があります（「付録：EFS に関する技術情報」参照）。

B)　Toshiba Dynabook R731/C

Toshiba Dynabook R731/C には BitLocker を導入し、OS ドライブ（C ドライブ）全体を暗号化します。暗号鍵は TPM に格納するとともに、OS 起動時に PIN（暗証番号）が要求されるような運用形態とします。そのための BitLocker 導入手順の流れを下図に示します。図中の網掛け部分はシステム管理者の作業手順を、それ以外はユーザの作業手順を表しています。

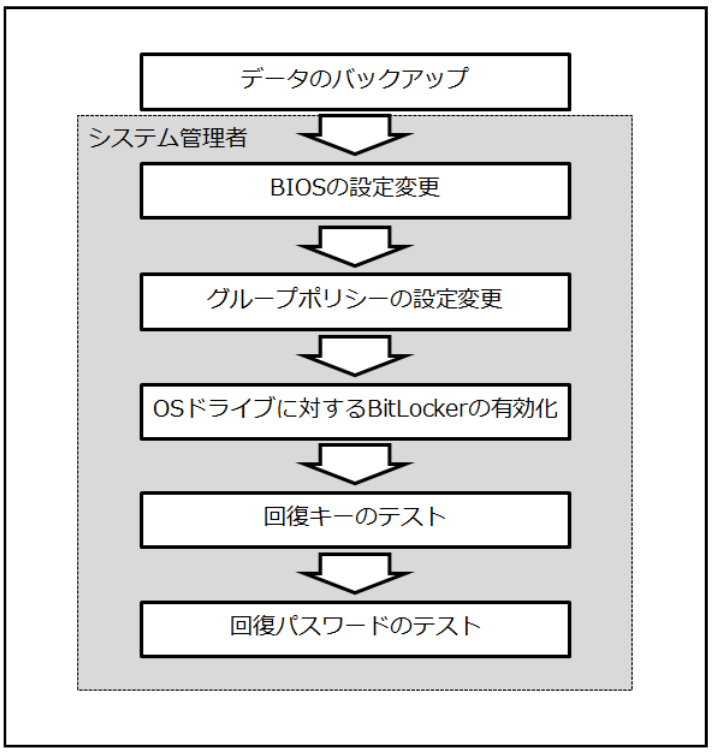


図　BitLocker 導入手順の流れ

- データのバックアップ【ユーザが実行】
  万一の場合に備え、暗号化対象ドライブのデータバックアップを取得する

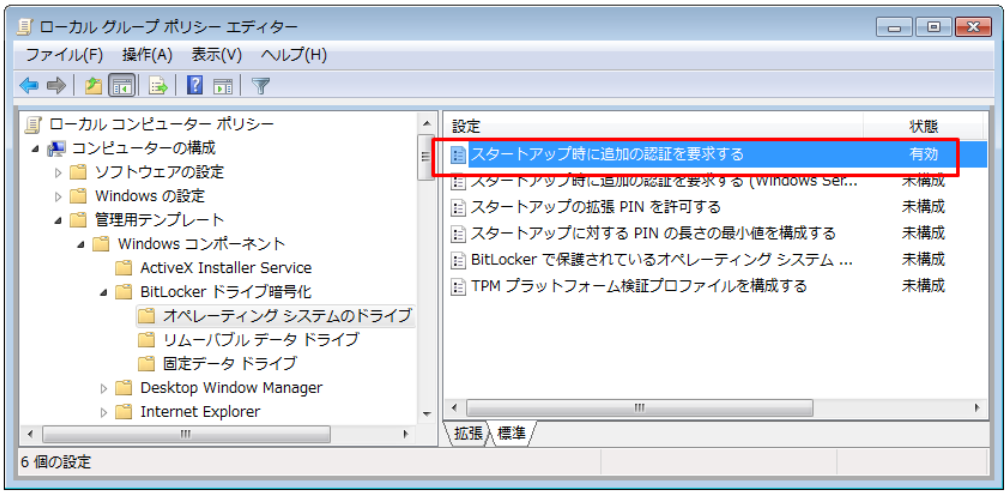
- BIOS の設定変更【システム管理者が実行】
  USB メモリからの OS 起動を優先するように設定されている場合は、BIOS の設定を変更し、ハードディスクからの OS 起動が最優先となるようにする

  BIOS 設定で TPM が無効になっている場合は、BIOS の設定を変更し、TPM を有効にする

- グループポリシーの設定変更【システム管理者が実行】
  管理者権限でコマンドプロンプトを起動し、以下のコマンドにより「ローカル グループポリシー エディター」を実行

  ```
  gpedit.msc
  ```

  「コンピューターの構成」→「管理用テンプレート」→「Windows コンポーネント」→「BitLocker ドライブ暗号化」→「オペレーティングシステムのドライブ」を開き、「スタートアップ時に追加の認証を要求する」を「有効」にする（これにより PIN の使用が可能になる）



- OS ドライブに対する BitLocker の有効化【システム管理者が実行】
  「コントロールパネル」の「BitLocker ドライブ暗号化」で OS ドライブ（通常は C:）について「BitLocker を有効にする」を選択

  BitLocker ドライブ暗号化のウィザードに従い「次へ」をクリックしていき、「再起動」ボタンが表示されれば指示に従って再起動する

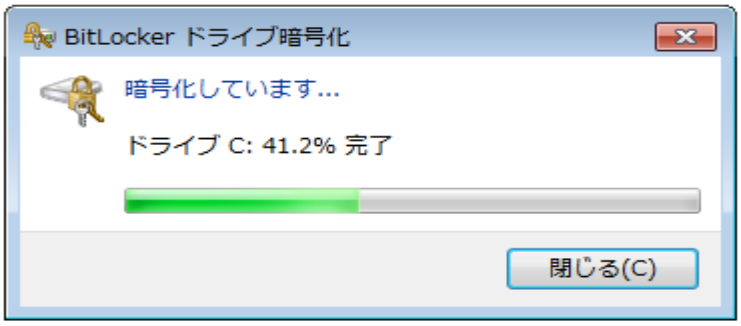
  再起動の過程で TPM の初期化へ移行する場合は、指示に従って TPM の初期化を行う（TPM 初期化処理は BIOS の種類に依存）

  再起動後、BitLocker のセットアップが継続され、「BitLocker のスタートアップ設定を設定する」という画面が表示されたら「毎回のスタートアップ時に PIN を要求する」をクリックし、4~20 桁の数字の暗証番号を設定する

  「回復キーの保存方法を指定してください」という画面が表示されたら回復キー保存用として使用する USB メモリを挿入し、「回復キーを USB フラッシュドライブに保存する」をクリック、回復キーを USB メモリに保存（拡張子 BEK のキーファイルと回復パスワードが記載されたテキストファイルが保存される）

  ウィザードに従って「次へ」→「続行」ボタンを押し、「今すぐ再起動する」で再起動

  OS 起動時に PIN が要求されるので正しく入力、起動後、再びシステム管理者でログオンし、OS ドライブの暗号化が完了するのを待つ（通知領域のアイコンクリックで進捗が表示）

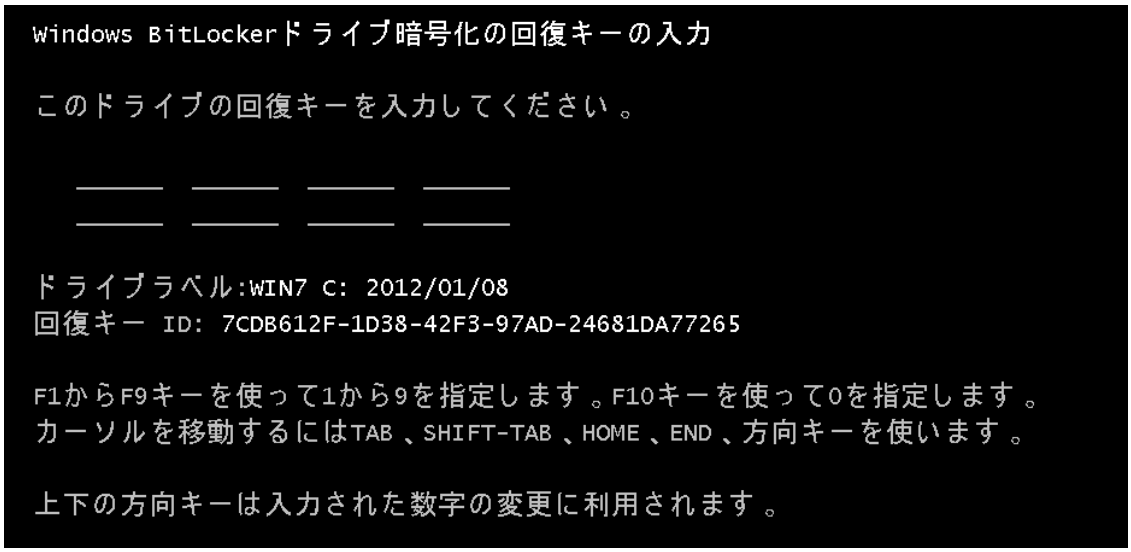


以上で OS ドライブへの BitLocker 導入は完了
※　ドライブ暗号化の実行中も通常の作業を行うことは可能

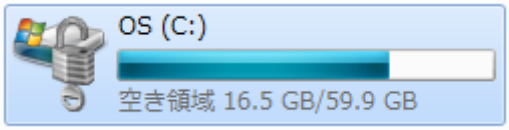
- 回復キーのテスト【システム管理者が実行】
  再起動時に回復キーを保存した USB メモリを挿入して OS が正常に起動することを確認

- 回復パスワードのテスト【システム管理者が実行】
  再起動時に表示される PIN 入力画面で ESC キーを押すと USB メモリの回復キーを挿入するように表示されるので、さらに Enter キーを押して回復パスワード入力画面へ移行

  48 桁の回復キー入力エリアに回復パスワード（48 桁の数字）を入力し OS が正常に起動することを確認



正常に暗号化されるとエクスプローラ上での OS ドライブのアイコン表示に「錠前」のマークが表示されます。



設定した PIN は当該コンピュータのユーザにのみ伝えます。ユーザは PIN が第三者の手に渡らないように管理する必要があります。回復キーを保存した USB メモリは内容を別のメディアにバックアップするとともに、システム管理者が厳重に保管します。

4. 試験運用時のチェック項目

暗号技術を導入したコンピュータを試験運用する際には、以下のチェック項目について確認を行います。

- 暗号化の対象は適切か？
  EFS は暗号化対象をフォルダ（あるいはファイル）単位で指定します。そのため暗号化の設定をしていないフォルダ内に機密ファイルを格納した場合、そのファイルは暗号化されません。試験運用時には暗号化設定したフォルダ以外に機密ファイルを格納していないかどうかを確認します。

- データバックアップシステムは正常に動作するか？
  暗号技術を導入したコンピュータ上でデータバックアップシステムが正常に動作するかどうかを確認します。

- ウイルス対策ソフトは正常に動作するか？
  下記の文字列を含むファイル（EICAR ウイルステストファイル）を暗号化した領域に拡張子「.com」として作成し、ウイルス対策ソフトがテストウイルスとして正しく検出するかどうかを確認します。（注：3 文字目の「O」は英大文字の「オー」）

  X5O!P%@AP[4¥PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

  この文字列は Web サイト「http://www.eicar.org/86-0-Intended-use.html」のページ下部からコピーすることができます。これはウイルス対策ソフトのテスト用ですので害はありません。

- その他の既存のアプリケーションソフトは正常に動作するか？
  暗号技術を導入したコンピュータ上でその他の既存のアプリケーションソフトウェアが正常に動作するかどうかを確認します。

- 社内システムとの連携上に問題はないか？
  暗号技術を導入したコンピュータで必要とされる社内業務システムを使用し、問題が発生しないことを確認します。

- その他、運用上の不具合は発生しないか？
  その他、パフォーマンスの著しい低下や操作性の悪化等、運用上の不具合が発生しないことを確認します。

5. 社内展開に向けて

試験導入フェーズ終了後、評価フェーズでは暗号技術の導入過程や運用上の問題点などを整理し、「試験導入結果評価報告書」としてまとめます。EFS や BitLocker の社内展開（社内の他のコンピュータへの導入）は、本書（導入計画書）および評価フェーズで作成される評価報告書の両方を参考にしながら行います。

EFS の試験導入時に作成／使用した回復エージェントの証明書（データ回復用の鍵）は、他の PC に EFS を導入する際にも同じものを使用することができます。そうすることにより、社内のすべての PC に導入した EFS のデータ回復を一つの回復エージェント証明書で管理することが可能です。BitLocker の回復キーおよび回復パスワードは、基本的に BitLocker を導入したそれぞれの PC ごとに生成されます。つまり例えば 10 台の PC に BitLocker を導入した場合、10 の回復キー／回復パスワードのセットが生成されることになります。

Windows ドメイン環境では EFS の回復エージェントや BitLocker の回復パスワードをドメインコントローラで管理することができます。EFS／BitLocker のデータ回復方法やドメイン環境での設定、その他の詳細な技術情報については付録資料を参照してください。

暗号技術は機密情報を保護する上で大いに役立ちますが、その効果を最大限に発揮させるためには導入する暗号技術の特性を理解し、残存リスク（暗号技術の導入のみでは解決されないリスク）への適切な対処が求められます。以下に EFS および BitLocker を運用していく際の注意点や、より安全な使用に向けての推奨事項を述べます。

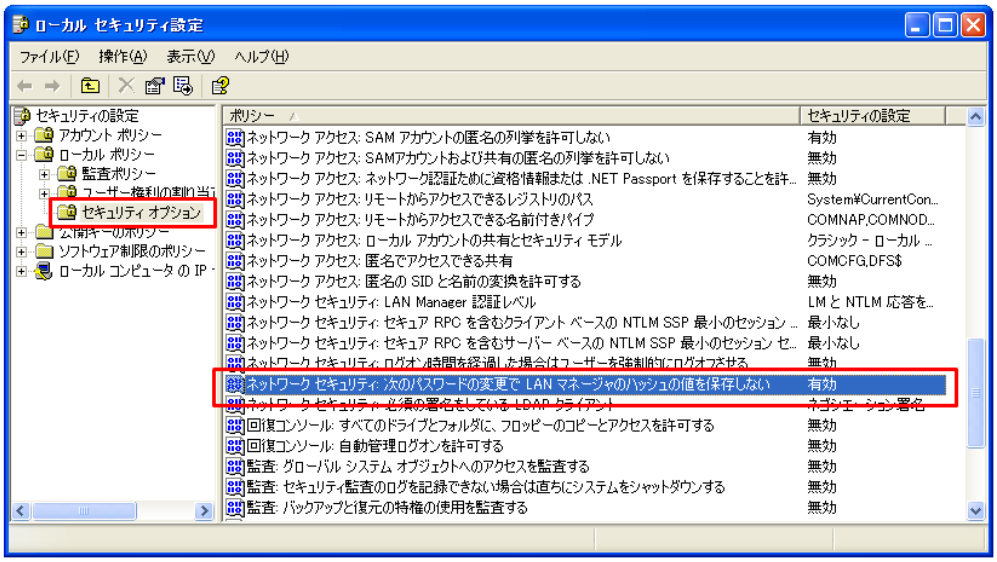
- コンピュータを持ち運ぶ際の注意点
  EFS を導入したコンピュータを持ち運ぶ際は、シャットダウンした状態で持ち運ぶことがセキュリティ上最も安全です。ユーザがログオンしたまま「スタンバイ」や「休止状態」で盗難にあうと、さまざまな攻撃手法を使用してコンピュータの状態をユーザのログオン状態に復帰させることにより、暗号化した情報に不正にアクセスされてしまう危険性があります。一方 BitLocker で OS ドライブを暗号化している場合はコンピュータを「休止状態」にして安全に持ち運ぶことが可能です。ただし PIN（暗証番号）や USB メモリ・キーの管理を厳重に行わなければ BitLocker を安全に運用することはできませんので注意が必要です。

- ウイルスや不正アクセスへの対策
  コンピュータウイルスに感染したり、ネットワーク経由で不正アクセスされたりした場合、いかに暗号技術を導入していてもコンピュータ内のデータの機密性を確保することはできません。暗号技術の導入とともに、ウイルス対策ソフトの適切な利用、ファイアウォールの設定、定期的なアップデートによるコンピュータの脆弱性（セキュリティ・ホール）の解消、その他のセキュリティ強化策の導入といった一般的なセキュリティ対策を併せて行うことが重要になります。

- 複雑なログオンパスワードの設定
  EFS の暗号鍵情報はそのユーザのログオンパスワードによって保護されていますので、ログオンパスワードが容易に推測可能な場合、EFS は暗号システムとしての効果を発揮することができません。ユーザは他者が推測することの困難なログオンパスワードを設定し、それが第三者に漏れないように秘匿する必要があります。

- パスワード情報の保護の強化
  ユーザのパスワード情報（パスワード・ハッシュ）はコンピュータのハードディスク上に保護された形で記録されていますが、攻撃者はハードディスクから直接その情報を抜き出し、時間をかけてパスワードを解析することを行います。BitLocker で OS ドライブ（C ドライブ）を暗号化している場合はパスワード情報も暗号化されるためこのような攻撃は不可能ですが、EFS ではパスワード情報が格納されたシステムファイル（レジストリ・ハイブファイル）を暗号化することができません。そのため BitLocker を導入していないコンピュータでは以下の手順によりパスワード情報の保護強化（LAN マネージャ・ハッシュを保存しない）を行い、このような攻撃に対する耐性を高めることが推奨されます。

  管理者権限でログオン、「コントロールパネル」の「管理ツール」から「ローカルセキュリティポリシー」を開き、「ローカルポリシー」の中にある「セキュリティオプション」で「ネットワークセキュリティ：次のパスワードの変更で LAN マネージャのハッシュの値を保存しない」を「有効」に設定した後、OS を再起動し、パスワードを再設定



※　Windows 95 や 98 が混在する環境では相互接続に問題が発生する場合があります。
※　Vista や Windows 7 はデフォルトでこの設定が有効になっています。

付録１：EFS に関する技術情報および導入手順

A)　EFS の基本

EFS（Encrypting File System：暗号化ファイルシステム）は Windows 2000 から Windows OS に導入されたファイル暗号化機構です。EFS はユーザごとに保有する「鍵」によって特定のファイルやフォルダを暗号化します。

EFS はシステムが自動生成する「ファイル暗号化鍵」でファイル内容を暗号化し、当該ユーザの「EFS 証明書」の公開鍵でファイル暗号化鍵を暗号化します。

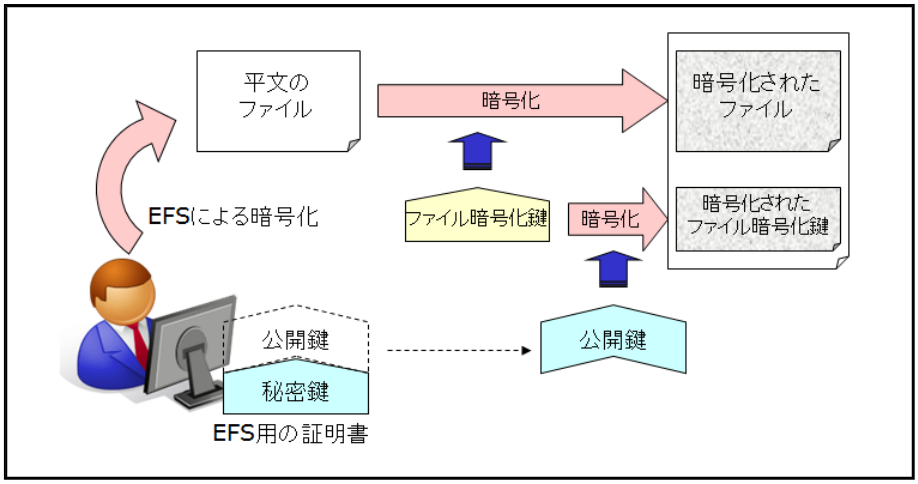


図　EFS によるファイル暗号化の仕組み

EFS 証明書（ユーザの秘密鍵／公開鍵ペア）は、そのユーザが最初に当該コンピュータ上で EFS 暗号化を行った際にシステムにより自動的に生成されます（社内の CA（認証局）から発行することもできますが、ここではそのような環境を想定していません）。

EFS の特徴の一つとしてアクセスの透過性があります。EFS で暗号化されたファイルは、ユーザが正しい証明書（秘密鍵）を持っていれば通常のアクセスにより自動的に復号されてアプリケーションプログラムに読み込まれます。当該ファイルは、ハードディスクの中では暗号化されたままの状態が保たれます。フォルダに対して EFS を適用させる（フォルダを EFS で暗号化する）と、そのフォルダ内に新たに作られるファイルは自動的に EFS で暗号化されます。つまり一度 EFS で暗号化する設定をしておけば、ユーザは特に暗号化／復号を意識することなくファイルの作成や読み書きを行うことができます。

EFS で暗号化したファイルを同一コンピュータ上でコピーや移動した場合、基本的には暗号化されたままコピー／移動されますが、コピーや移動先が別ドライブでかつ NTFS 以外の場合は復号された状態でのコピー／移動となります。またネットワーク経由でのファイルサーバへのコピー／移動も、特別に設定されたサーバ以外は基本的には復号された状態になります。

EFS 証明書の秘密鍵はユーザのログオンパスワードによって保護された状態でハードディスク内に格納されます。正しいログオンパスワードを入力してログオンした正当なユーザのみが、そのユーザの EFS 証明書を使用して暗号化ファイルにアクセスすることができます。逆に言うと、ユーザのログオンパスワードが第三者に漏洩することで暗号化ファイルへの不正なアクセスを許してしまうため注意が

必要です。

B) EFS 導入に関する注意事項

- 対象 OS
  - XP Professional（サービスパック 3）
  - Vista Business／Enterprise／Ultimate（サービスパック 2）
  - 7 Professional／Enterprise／Ultimate
  - ※ 上記以前のバージョンやサービスパックでも EFS は使用可能であるが、マイクロソフトのサポートが終了しているためここでは上記のみを対象 OS とする

- ディスクフォーマット
  EFS で暗号化する場合、ハードディスクは NTFS でフォーマットされている必要がある

- 暗号化できないファイル／フォルダ
  - ルートフォルダ直下のブート関連ファイル
  - %Windir%フォルダおよびその子オブジェクト
  - ユーザプロファイル関連のファイル（つまり、Ntuser.*）
  - %APPDATA%フォルダ
  - ¥Boot（Vista の場合）
  - ¥$Recycle.Bin（ゴミ箱）
  - システム属性がマークされたファイルまたはフォルダ
  - 休止状態ファイル

- 暗号化すべきでないファイル／フォルダ
  - ¥Program Files フォルダおよびそのサブフォルダ
  - システムのサービスがアクセスするファイルやフォルダ
  - 他のユーザもアクセスするファイルやフォルダ（他ユーザと EFS 共有する場合を除く）

- 暗号化する場合に注意が必要なファイル／フォルダ
  - %TEMP%フォルダ（インストールやアップデートの際に不具合が発生する可能性あり）
  - デスクトップフォルダ（ログオン中には暗号化できない可能性あり）

- その他の注意事項
  データバックアップシステムによっては EFS で暗号化したファイルをバックアップできない場合がある（Windows 標準のバックアップユーティリティは OK）

C) EFS データ回復の考え方

EFS ではデータ回復の手段として「回復エージェント（データ回復用の証明書）」という機能が用意されています。EFS 証明書はコンピュータ上に保存されたファイルですので、ハードウェア障害や誤操作等により消失する危険性があります。また社内監査等のためにシステム管理者がユーザの暗号化ファイルを復号する必要性も考えなければなりません。そのような場合に備え、EFS を使用するコンピュータでは回復エージェントを設定しておく必要があります。回復エージェントの秘密鍵はシステム管理者が厳重に管理し、データ回復の必要性が発生した段階で使用します。

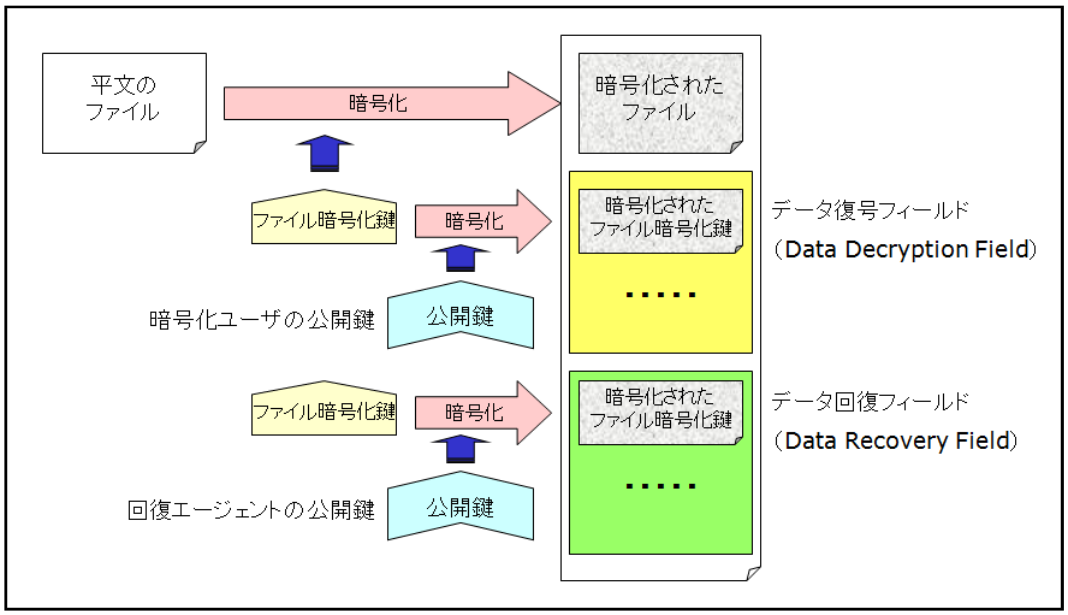


図　EFS における回復エージェントの仕組み

またユーザの EFS 証明書もユーザ自身の手でバックアップを取得しておくことが必要です。そうすることでハードウェア障害等により鍵情報が失われた場合でも、バックアップファイルからユーザの EFS 証明書をインポートして復元することが可能になります。

D)　EFS の導入手順

ここではスタンドアローンコンピュータへ EFS を導入する際の一般的な手順について記述します。

- データのバックアップ【ユーザが実行】
  万一の場合に備え、暗号化対象ファイルのデータバックアップを取得する

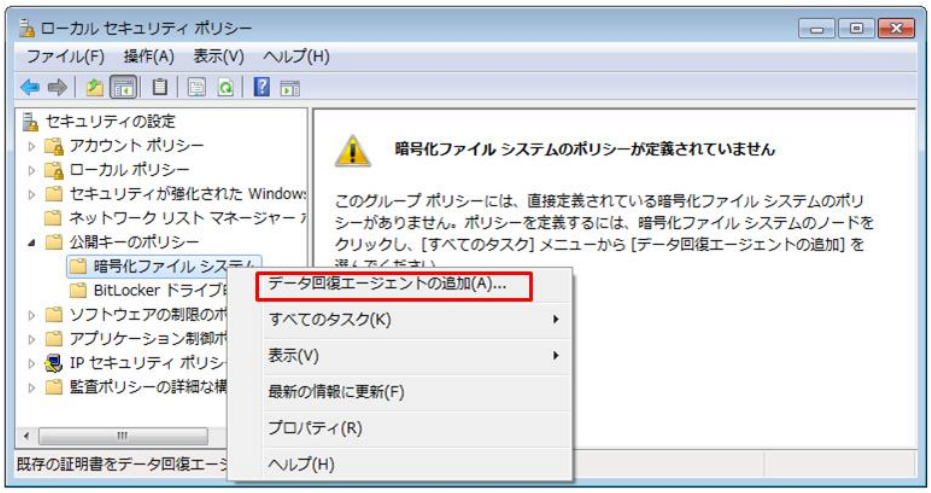
- 回復エージェントの作成【システム管理者が実行】
  システム管理用のコンピュータ上（XP 以降）で以下のコマンドを実行し、回復エージェントの EFS 証明書を作成する

  cipher /R:EFSRecover　　（注：「EFSRecover」は任意のファイル名）

  カレントフォルダに回復エージェント証明書のファイル「EFSRecover.PFX（証明書と秘密鍵)」および「EFSRecover..CER（証明書のみ)」が生成される

  EFSRecover.PFX は別メディアへバックアップするとともにシステム管理者のみがアクセスできるよう厳重にアクセス制限を設定し、入力した保護パスワードも安全に記録しておく

- 回復エージェントの設定【システム管理者が実行】
  EFS で暗号化するコンピュータに管理者権限でログオン、「コントロールパネル」の「管理ツール」から「ローカルセキュリティポリシー」を開き、「公開キーのポリシー」の中にある「暗号化ファイルシステム」を右クリック、メニューから「データ回復エージェントの追加」を選択



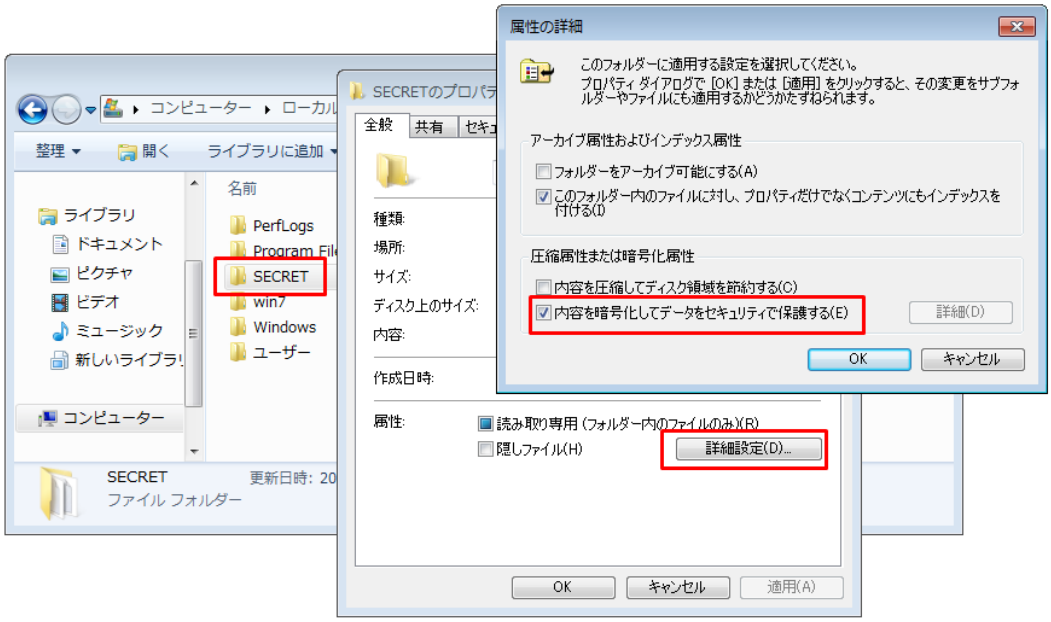
  システム管理用コンピュータで作成した「EFSRecover..CER」を当該コンピュータへコピーし、「回復エージェントの追加ウィザード」でそのファイルを指定することによりデータ回復エージェントとして登録

  EFSRecover.CER ファイルを当該コンピュータ上から削除し、ログアウト

- 機密フォルダに対する EFS の有効化【ユーザが実行】
  当該コンピュータを利用するユーザのアカウントでログオンした後、EFS で暗号化する対象の機密フォルダ（ここでは「C:¥SECRET」とする）についてエクスプローラでプロパティを開き、「属性の詳細」ウィンドウで「内容を暗号化してデータをセキュリティで保護する」にチェックを入れる

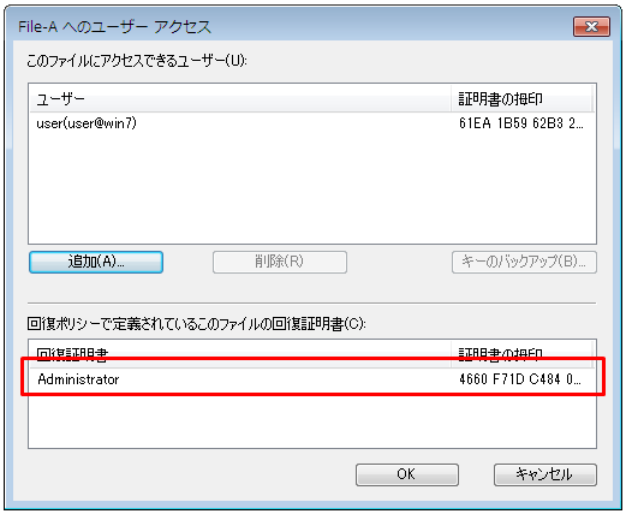
  「属性変更の確認」ウィンドウが表示された場合は「変更をこのフォルダー、サブフォルダーおよびファイルに適用する」を選択する

  この時点で当該ユーザの EFS 証明書が自動生成されると同時に、SECRET フォルダ以下のファイルが EFS で暗号化される



EFS で暗号化されると、エクスプローラ上では暗号化フォルダやファイルの名称が緑色で表示されるようになる
※　圧縮属性のついているフォルダやファイルは EFS では暗号化できないので注意

- EFS 暗号化状況の確認【ユーザが実行】
  暗号化された任意のファイルについてエクスプローラでプロパティを開き、「属性の詳細」ウィンドウで「詳細」を押して当該ファイルにアクセスできるユーザ証明書と回復証明書の一覧を表示させ、回復エージェントの証明書が下の段に存在することを確認する



もし存在しない場合は、前述の「回復エージェントの設定」手順を再確認する

- ユーザ EFS 証明書のバックアップ【ユーザが実行】
  生成されたユーザの EFS 証明書は、以下のコマンドによりユーザ自身でバックアップを行う

  cipher /X EFSBackup　　（注：「EFSBackup」は任意のファイル名）

カレントフォルダにユーザ証明書のバックアップファイル「EFSBackup.PFX（証明書と秘密鍵）」が生成されるので、このファイルを別メディアへ移動するとともにユーザのみがアクセスできるよう厳重にアクセス制限を設定し、入力した保護パスワードも安全に記録しておく
※ Vista 以降は「ファイル暗号化キーのバックアップ」というバルーンメッセージが表示されるので、それをクリックしてウィザードに従いバックアップを行っても良い

NTFS でフォーマットされていれば USB メモリ等のリムーバブルメディア内のファイルを EFS で暗号化することもできます。暗号化の操作方法は上記を参考にしてください。EFS で暗号化した USB メモリのファイルを他のコンピュータ上で読み書きしたい場合は、そのコンピュータにユーザの EFS 証明書をインポートする必要があります（後述の「EFS の回復手順」参照）。

E) EFS の回復手順

ハードウェア障害等でユーザの鍵情報が失われてしまいユーザ自身が自分で暗号化したデータにアクセスできなくなった場合には、バックアップしておいたユーザの EFS 証明書をインポートして回復することができます。他のコンピュータで EFS の暗号化を行ったファイルにアクセスしたい場合も同様です。

- ユーザ EFS 証明書のインポート【ユーザが実行】
  バックアップしておいたユーザ証明書ファイル（EFSBackup.PFX）をハードディスク上へコピーし、ダブルクリックして「証明書のインポートウィザード」を開始、バックアップ時に指定した保護パスワードを入力してユーザ証明書をインポートする

またユーザの退職やシステム監査等の事由によりシステム管理者がユーザの暗号化ファイルへアクセスする必要が生じた場合には、システム管理者が回復エージェントの EFS 証明書をインポートしてユーザの EFS ファイルへのアクセスを可能にすることができます。

- 回復エージェント EFS 証明書のインポート【システム管理者が実行】
  回復エージェント証明書ファイル（EFSRecover.PFX）をハードディスク上へコピーし、ダブルクリックして「証明書のインポートウィザード」を開始、作成時に指定した保護パスワードを入力して回復エージェント証明書をインポートする

F) EFS の解除手順

EFS で暗号化したファイル／フォルダについて、ハードディスク上の暗号化を解除し元の状態へ戻したい場合、以下の手順で EFS の解除を行うことができます。

- 暗号化ファイル／フォルダに対する EFS の解除【ユーザが実行】
  EFS で暗号化しているファイルやフォルダについてエクスプローラでプロパティを開き、「属性の詳細」ウィンドウで「内容を暗号化してデータをセキュリティで保護する」のチェックをはずす

  「属性変更の確認」ウィンドウが表示された場合は「変更をこのフォルダー、サブフォルダーおよびファイルに適用する」を選択する

回復エージェントの証明書をインポートしたシステム管理者は、ユーザの EFS ファイルの暗号化を解除することが可能です。

G) ドメイン環境での展開

EFS の回復エージェントをドメインのグループポリシーで設定しておくことにより、回復エージェントをドメインコントローラで統合的に管理できます。

- 「コンピュータの構成」→「Windows の設定」→「セキュリティの設定」→「公開キーのポリシー」の「暗号化ファイルシステム」を右クリックして「データ回復エージェントの追加」で回復エージェントを追加

すべてのユーザの「マイドキュメント」フォルダ以下を EFS で暗号化するようにしたい場合は、ドメインのグループポリシーで以下の設定を行います（Windows Server 2008 ドメインコントローラ）。

- 「コンピュータの構成」→「Windows の設定」→「セキュリティの設定」→「公開キーのポリシー」の「暗号化ファイルシステム」を右クリックして「プロパティ」を開き、「ユーザーのドキュメントフォルダーの内容を暗号化する」を ON

付録２：BitLocker に関する技術情報および導入手順

A)　BitLocker の基本

BitLocker は Windows Vista から導入され、Windows 7 で機能拡張されたディスク・フルボリューム暗号化機構です。BitLocker は TPM（セキュリティチップ）または USB メモリ内部に格納した「鍵」によってハードディスクの OS ドライブ（C ドライブ）全体を暗号化します。また OS ドライブ以外のデータドライブ（D ドライブ等）を暗号化することもできます。ここでは基本的に Windows 7 の BitLocker の機能について解説します。

BitLocker で OS ドライブを暗号化することにより、「鍵」がないと OS を起動したり OS ドライブ上のファイルにアクセスしたりすることができなくなります。例えば TPM に鍵を格納した場合、その TPM を搭載したコンピュータ以外では当該 OS ドライブへのアクセスはできません。TPM と PIN（暗証番号）を併用することでさらにセキュリティを高めることも可能です。OS 起動時に適切な鍵が与えられると、後は自動的にディスク上のデータの復号が行われ、通常の Windows システムと同様に使用することができます。

EFS はユーザ単位でのファイル暗号化の機能を提供しますが、EFS ではシステム関連のファイル（レジストリ・ハイブファイル、ハイバネーションファイル、OS コマンドファイル等）を暗号化することができません。一方 BitLocker は OS ドライブ全体を暗号化しますので、システム関連ファイルからの情報取得やシステムファイルの書き換えといった攻撃に対抗することが可能となります。

また BitLocker を TPM で使用する場合、コンピュータ上に存在する以下のブート情報の書き換えを検査し、もし変更があると OS の起動をロックする「ブート情報の整合性検査機能」が提供されます。

- BIOS 設定情報
- マスターブートレコード（MBR）
- ブートセクター
- ブートマネージャ、等

BitLocker で OS ドライブのハードディスク・セクタを暗号化する際に使用される鍵は「FVEK（Full-Volume Encryption Key）」と呼ばれます。FVEK は「VMK（Volume Master Key）」という別の鍵で暗号化して保存されます。TPM や USB メモリ・キー（スタートアップキー）はこの VMK を暗号化して保護するために使用されることになります。VMK の保護には、コンピュータのハードウェア機能や求められるセキュリティレベルに応じて以下のオプションが用意されています。

- TPM のみ
  TPM に鍵を格納
- TPM ＋ PIN
  TPM に鍵を格納、PIN（暗証番号またはパスワード）により保護
- USB メモリのみ
  USB メモリに鍵を格納
- TPM ＋ USB メモリ
  TPM の鍵と USB メモリの鍵とを併用
- TPM ＋ USB メモリ ＋ PIN

TPM の鍵と USB メモリの鍵とを併用、PIN（暗証番号またはパスワード）により保護

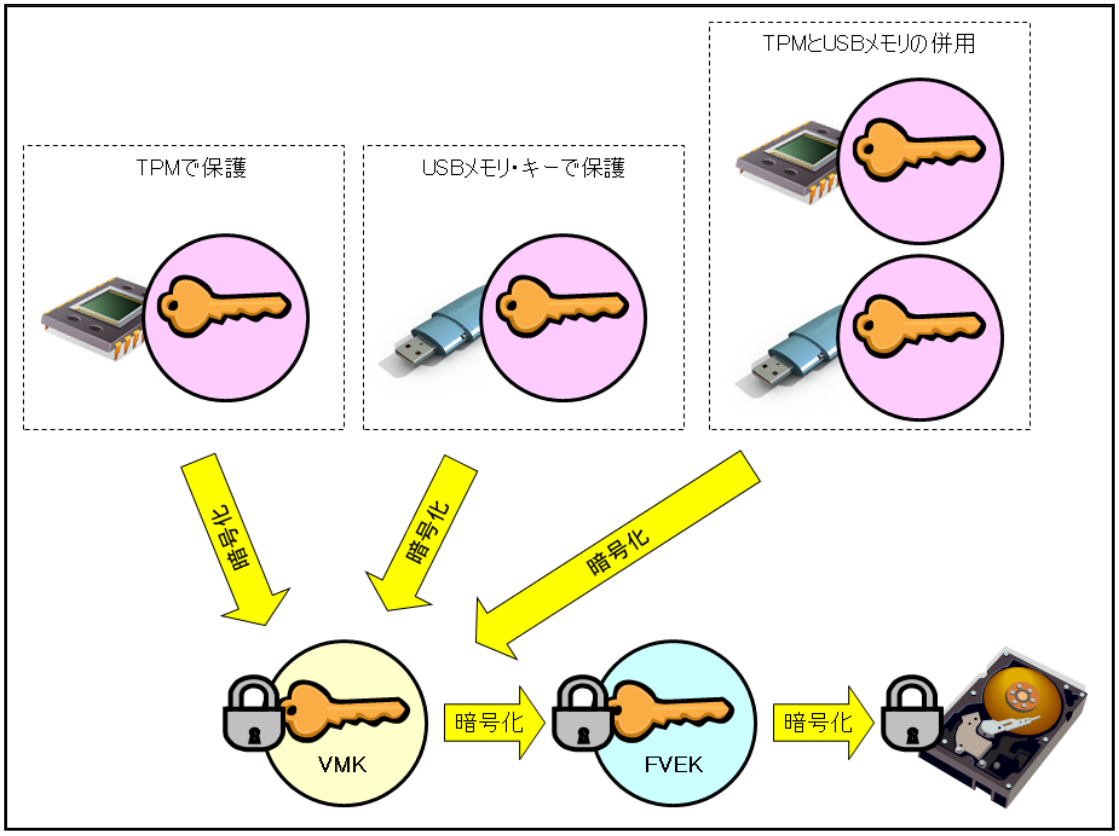


図　BitLocker における鍵の関係のイメージ

BitLocker は OS ドライブ以外の固定ハードディスク・ドライブや USB メモリ等のリムーバブルメディアを暗号化することもできますが、その場合はパスワードを用いて保護することが可能です。

B)　BitLocker 導入に関する注意事項

- 対象 OS
  - Vista Enterprise／Ultimate（サービスパック 2）
  - 7 Enterprise／Ultimate
  - ※　上記以前のサービスパックでも BitLocker は使用可能であるが、マイクロソフトのサポートが終了しているためここでは上記のみを対象 OS とする

- ディスクフォーマット
  BitLocker で暗号化する場合、OS ドライブは NTFS でフォーマットされている必要がある
  OS ドライブ以外のデータドライブは exFAT、FAT16、FAT32、NTFS いずれでもよい

- ディスク空き容量
  Vista の場合、OS ドライブに 1.5GB の空き容量が必要（起動ボリュームとして分割）

- ハードウェア要件
  - TPM v1.2 以降（TPM を使用する場合）
  - ※　他のアプリケーションですでに TPM を使用している場合は、そのアプリケーションの製造元に BitLocker との併用について確認

- BIOS の USB メモリサポート（USB メモリ・キーを使用する場合）

C) BitLocker データ回復の考え方

BitLocker にはデータ回復用として「回復キー」や「回復パスワード」が用意されています。回復キーは USB メモリに保存するファイル（拡張子が BEK）で、回復パスワードは 48 ケタの数字からなるパスワードです。このいずれかを使用することにより、BitLocker で暗号化した OS ドライブのデータ回復を行うことが可能です。

BitLocker で暗号化した OS ドライブにアクセスできなくなる原因として、以下のようなケースがあげられます。

- TPM の PIN を忘れた
- USB メモリ・キーを紛失した
- BIOS アップデート等によりブート関連情報を更新した
- 悪意のある第三者がブート関連情報を書き換えた
- 故障のためハードディスクを別のコンピュータへ移行した

いずれの場合でも回復キーまたは回復パスワードがあれば VMK を復号して OS ドライブへのアクセスを回復することができます。ドメインメンバの BitLocker 回復パスワードは、Active Directory へ自動的にバックアップされるように設定することも可能です。

本書では回復キーおよび回復パスワードの両方を作成し、システム管理者が厳重に保管するという運用方法を採用します。

D) BitLocker の OS ドライブへの導入手順（TPM 使用の場合）

ここでは TPM がサポートされているスタンドアローンの Windows 7 コンピュータへ BitLocker を導入して OS ドライブを暗号化する際の一般的な手順について記述します。セキュリティを強化するために PIN（暗証番号）による保護を追加しています。
※ Vista では OS ドライブに対して BitLocker を有効化する前に、「BitLocker ドライブ準備ツール」を使用してハードディスクの構成を変更し、起動ボリュームを別途作成する必要があります。

- データのバックアップ【ユーザが実行】
  万一の場合に備え、暗号化対象ドライブのデータバックアップを取得する

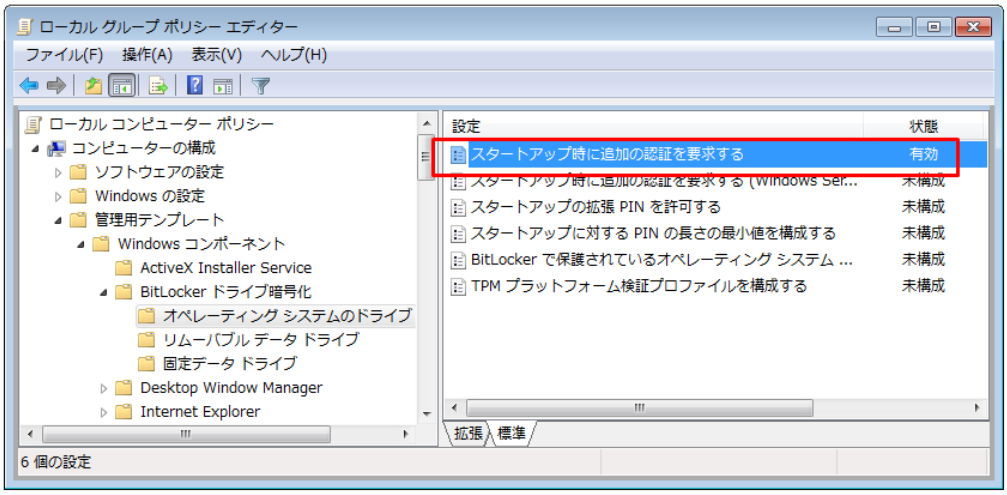
- BIOS の設定変更【システム管理者が実行】
  USB メモリからの OS 起動を優先するように設定されている場合は、BIOS の設定を変更し、ハードディスクからの OS 起動が最優先となるようにする

  BIOS 設定で TPM が無効になっている場合は、BIOS の設定を変更し、TPM を有効にする

- グループポリシーの設定変更【システム管理者が実行】
  管理者権限でコマンドプロンプトを起動し、以下のコマンドにより「ローカル グループポリシー エディター」を実行

gpedit.msc

「コンピューターの構成」→「管理用テンプレート」→「Windows コンポーネント」→「BitLocker ドライブ暗号化」→「オペレーティングシステムのドライブ」を開き、「スタートアップ時に追加の認証を要求する」を「有効」にする（これにより PIN の使用が可能になる）



- OS ドライブに対する BitLocker の有効化【システム管理者が実行】
  「コントロールパネル」の「BitLocker ドライブ暗号化」で OS ドライブ（通常は C:）について「BitLocker を有効にする」を選択

  BitLocker ドライブ暗号化のウィザードに従い「次へ」をクリックしていき、「再起動」ボタンが表示されれば指示に従って再起動する

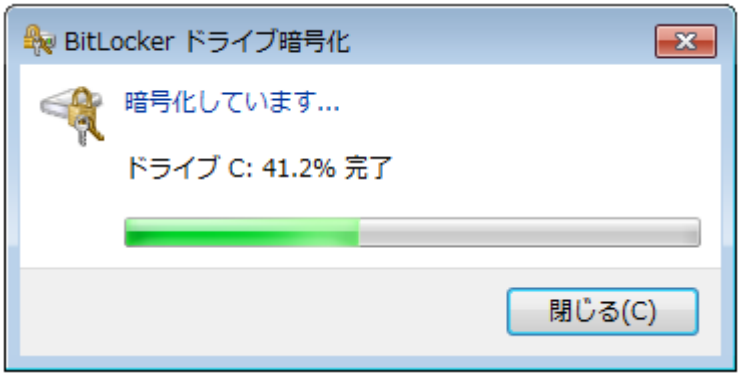
  再起動の過程で TPM の初期化へ移行する場合は、指示に従って TPM の初期化を行う（TPM 初期化処理は BIOS の種類に依存）

  再起動後、BitLocker のセットアップが継続され、「BitLocker のスタートアップ設定を設定する」という画面が表示されたら「毎回のスタートアップ時に PIN を要求する」をクリックし、4~20 桁の数字の暗証番号を設定する

  「回復キーの保存方法を指定してください」という画面が表示されたら回復キー保存用として使用する USB メモリを挿入し、「回復キーを USB フラッシュドライブに保存する」をクリック、回復キーを USB メモリに保存（拡張子 BEK のキーファイルと回復パスワードが記載されたテキストファイルが保存される）

  ウィザードに従って「次へ」→「続行」ボタンを押し、「今すぐ再起動する」で再起動

  OS 起動時に PIN が要求されるので正しく入力、起動後、再びシステム管理者でログオンし、OS ドライブの暗号化が完了するのを待つ（通知領域のアイコンクリックで進捗が表示）

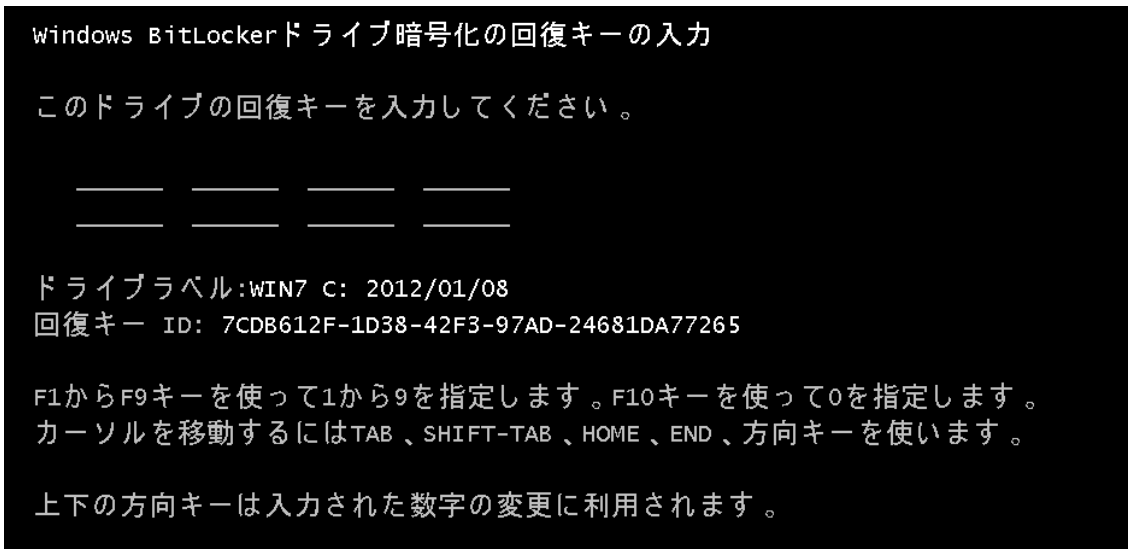


以上で OS ドライブへの BitLocker 導入は完了
※　ドライブ暗号化の実行中も通常の作業を行うことは可能

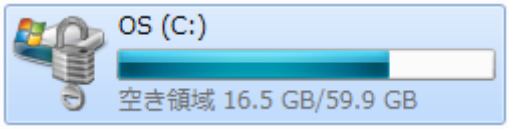
- 回復キーのテスト【システム管理者が実行】
  再起動時に回復キーを保存した USB メモリを挿入して OS が正常に起動することを確認

- 回復パスワードのテスト【システム管理者が実行】
  再起動時に表示される PIN 入力画面で ESC キーを押すと USB メモリの回復キーを挿入するように表示されるので、さらに Enter キーを押して回復パスワード入力画面へ移行

  48 桁の回復キー入力エリアに回復パスワード（48 桁の数字）を入力し OS が正常に起動することを確認



正常に暗号化されるとエクスプローラ上での OS ドライブのアイコン表示に「錠前」のマークが表示されます。



設定した PIN は当該コンピュータのユーザにのみ伝えます。ユーザは PIN が第三者の手に渡らないよ

うに管理する必要があります。回復キーを保存した USB メモリは内容を別のメディアにバックアップするとともに、システム管理者が厳重に保管します。

E)　BitLocker の OS ドライブへの導入手順（USB メモリ・キー使用の場合）

TPM がサポートされていないコンピュータでも、USB メモリの中に鍵を保存することで OS ドライブの暗号化が可能です。その場合、OS 起動時や休止状態からの復帰時には毎回この USB メモリ・キーを挿入する必要があります。ここでは TPM がサポートされていないスタンドアローンの Windows 7 コンピュータへ BitLocker を導入する際の一般的な手順について記述します。

- データのバックアップ【ユーザが実行】
  万一の場合に備え、暗号化対象ドライブのデータバックアップを取得する

- BIOS の設定変更【システム管理者が実行】
  USB メモリからの OS 起動を優先するように設定されている場合は、BIOS の設定を変更し、ハードディスクからの OS 起動が最優先となるようにする

- グループポリシーの設定変更【システム管理者が実行】
  管理者権限でコマンドプロンプトを起動し、以下のコマンドにより「ローカル グループポリシー エディター」を実行

  ```
  gpedit.msc
  ```

  「コンピューターの構成」→「管理用テンプレート」→「Windows コンポーネント」→「BitLocker ドライブ暗号化」→「オペレーティングシステムのドライブ」を開き、「スタートアップ時に追加の認証を要求する」を「有効」にする（これにより USB メモリ・キーの使用が可能になる）

- OS ドライブに対する BitLocker の有効化【システム管理者が実行】
  「コントロールパネル」の「BitLocker ドライブ暗号化」で OS ドライブ（通常は C:）について「BitLocker を有効にする」を選択

  BitLocker ドライブ暗号化ウィザードで「BitLocker のスタートアップ設定を設定する」という画面が表示されたら「毎回のスタートアップ時にスタートアップキーを要求する」をクリックし、鍵を保存する USB メモリを挿入してスタートアップキーを保存（拡張子 BEK のキーファイルが保存され、これが USB メモリ・キーとなる）

  「回復キーの保存方法を指定してください」という画面が表示されたら回復キー保存用として使用する別の USB メモリを挿入し、「回復キーを USB フラッシュドライブに保存する」をクリック、回復キーを USB メモリに保存（拡張子 BEK のキーファイルと回復パスワードが記載されたテキストファイルが保存される）

  ウィザードに従って「次へ」→「続行」ボタンを押し、「今すぐ再起動する」で再起動

  OS 起動後、再びシステム管理者でログオンし、OS ドライブの暗号化が完了するのを待つ（OS

の起動が開始すれば USB メモリ・キーは取り外してかまわない）

以上で OS ドライブへの BitLocker 導入は完了
※　ドライブ暗号化の実行中も通常の作業を行うことは可能

- 回復キーのテスト【システム管理者が実行】
  再起動時に回復キーを保存した USB メモリを挿入して OS が正常に起動することを確認

- 回復パスワードのテスト【システム管理者が実行】
  再起動時に USB メモリを挿入しないと画面上に USB メモリの回復キーを挿入するように表示されるので、Enter キーを押して回復パスワード入力画面へ移行

  48 桁の回復キー入力エリアに回復パスワード（48 桁の数字）を入力し OS が正常に起動することを確認

USB メモリ・キーは当該コンピュータのユーザに渡します。ユーザは USB メモリ・キーが第三者の手に渡らないように管理する必要があります。回復キーを保存した USB メモリはデータを別のメディアにバックアップするとともに、システム管理者が厳重に保管します。

F)　BitLocker の固定データドライブへの導入手順

ここでは OS ドライブ以外の固定ハードディスク・データドライブへ BitLocker を導入する際の一般的な手順について記述します。OS ドライブはすでに BitLocker で暗号化されているという前提です。固定ハードディスクのデータドライブでは、そのドライブへのアクセス時にパスワードを要求するように設定することも可能ですが、ここでは利便性を考慮し、当該コンピュータに接続されている限りログオン時に自動的にロックが解除されるオプションを選択します。

- データのバックアップ【ユーザが実行】
  万一の場合に備え、暗号化対象ドライブのデータバックアップを取得する

- 固定データドライブに対する BitLocker の有効化【システム管理者が実行】
  「コントロールパネル」の「BitLocker ドライブ暗号化」で該当する固定データドライブについて「BitLocker を有効にする」を選択

  BitLocker ドライブ暗号化ウィザードで「このドライブのロック解除方法を選択する」という画面が表示されたら「このコンピュータでこのドライブのロックを自動的に解除する」をチェックし、「次へ」をクリックする（当該コンピュータ上であれば自動的にアクセス可能になる）

  「回復キーの保存方法を指定してください」という画面が表示されたら回復キー保存用として使用する USB メモリを挿入し、「回復キーを USB フラッシュドライブに保存する」をクリック、回復キーを USB メモリに保存（拡張子 BEK のキーファイルと回復パスワードが記載されたテキストファイルが保存される）

  ウィザードに従って「次へ」→「暗号化の開始」ボタンを押し、暗号化を開始する

回復キーを保存した USB メモリはデータを別のメディアにバックアップするとともに、システム管理者が厳重に保管します。

G) BitLocker のリムーバブルデータドライブへの導入手順

ここでは USB メモリ等のリムーバブルデータドライブへ BitLocker を導入する際の一般的な手順について記述します。リムーバブルデータドライブでは、そのドライブへのアクセス時（USB メモリ挿入時等）にパスワードを要求するように設定します。BitLocker によるリムーバブルドライブの暗号化の機能は「BitLocker To Go」と呼ばれます。この機能は一般ユーザで利用することも可能ですが、ここではシステム管理者が暗号化リムーバブルデータドライブを作成してユーザへ配布するケースを想定します。（※ Vista は BitLocker To Go をサポートしていません）

- リムーバブルデータドライブに対する BitLocker の有効化【システム管理者が実行】
  「コントロールパネル」の「BitLocker ドライブ暗号化」で該当するリムーバブルデータドライブについて「BitLocker を有効にする」を選択

  BitLocker ドライブ暗号化ウィザードで「このドライブのロック解除方法を選択する」という画面が表示されたら「パスワードを使用してドライブのロックを解除する」をチェック、ドライブの保護パスワードを入力し、「次へ」をクリックする

  「回復キーの保存方法を指定してください」という画面が表示されたら「回復キーをファイルに保存する」をクリック、回復キーをハードディスク上に保存（回復パスワードが記載されたテキストファイルが保存される）

  ウィザードに従って「次へ」→「暗号化の開始」ボタンを押し、暗号化を開始する

設定したパスワードは当該メディアの使用ユーザにのみ伝えます。ユーザはパスワードが第三者の手に渡らないように管理する必要があります。回復キーのファイル（回復パスワードが書かれたテキストファイル）は別のメディアにバックアップするとともに、システム管理者が厳重に保管します。

H) BitLocker の回復手順

ユーザが TPM の PIN を忘れてしまったり、USB メモリ・キーを紛失してしまったりした場合、システム管理者に 48 桁の回復パスワードを問い合わせてユーザがそれを入力することにより OS を起動することが可能です。ユーザからの問い合わせに迅速に対応できる体制（24 時間のヘルプデスク体制等）がない場合は、あらかじめ回復パスワードのメモをユーザに渡しておく等、リスク回避手段を検討する必要があります。

ユーザからの問い合わせに応じて回復パスワードを知らせる際には、電話や対面によって確かに正当なユーザであることを確認します。また回復パスワードは BitLocker で暗号化したドライブごとに異なりますので、正しい回復パスワードを知らせるために回復パスワード入力画面に表示される「回復キーID」の情報をユーザから伝えてもらいます。回復パスワードの入力手順については前述の「BitLocker の導入手順」の「回復パスワードのテスト」を参照してください。

システム管理者は回復キーが保存された USB メモリを使用することで、PIN や USB メモリ・キーな

しで OS を起動することができます。使用方法は OS 起動時に回復キーUSB メモリを挿入するだけです。

ユーザが TPM の PIN を忘れてしまった場合は、システム管理者によって PIN のリセットを行い、新たに設定した PIN をユーザに伝えます。

- PIN のリセット【システム管理者が実行】
  「コントロールパネル」の「BitLocker ドライブ暗号化」で OS ドライブについて「BitLocker の管理」を選択

  「暗証番号（PIN）のリセット」をクリックし、新しい PIN を入力して「暗証番号（PIN）の設定」を押す

ユーザが USB メモリ・キーを紛失した場合は、第三者による不正な利用を防ぐため現在のキーを無効にしてキーを再生成する必要があります。後述する「BitLocker の解除手順」で OS ドライブの暗号化を一旦解除し、再び OS ドライブの暗号化を行います。

BitLocker To Go で暗号化したリムーバブルデータドライブ（USB メモリ）についても、ユーザがパスワードを忘れた場合はシステム管理者が回復パスワードを知らせることでアクセスを回復することができます。

I)　BitLocker の解除手順

BitLocker で暗号化したドライブについて、ハードディスク上の暗号化を解除し元の状態へ戻したい場合、以下の手順で BitLocker の解除を行うことができます。

- 暗号化ドライブに対する BitLocker の解除【システム管理者が実行】
  「コントロールパネル」の「BitLocker ドライブ暗号化」で暗号化を解除したいドライブについて「BitLocker を無効にする」を選択

続いて表示されるウィンドウで「ドライブの暗号化解除」をクリックし BitLocker の解除を実行

J)　BitLocker の保護中断手順

BitLocker で TPM を使用している場合、OS 起動時にブート情報が不正に書き換えられていないかどうかを検査し、異常が認められると回復モード（回復キーや回復パスワードが要求される）へと移行します。これは第三者が不正にブート情報を書き換えて攻撃することを防ぐためです。

一方でブート情報の変更は BIOS アップデートや OS 起動設定の変更といった通常のメンテナンス作業でも行われる可能性があります。そのため BitLocker には一時的に保護を中断するという機能があります。システム管理者が BIOS アップデートや OS 起動設定の変更の作業を行う際には、BitLocker の保護を一時的に中断し、作業終了後に保護を再開することが求められます。BitLocker の保護の中断は OS ドライブに対してのみ実行できます。

- 暗号化ドライブに対する BitLocker の保護中断【システム管理者が実行】
  「コントロールパネル」の「BitLocker ドライブ暗号化」で保護を中断したいドライブについて「保護の中断」を選択

- 暗号化ドライブに対する BitLocker の保護再開【システム管理者が実行】
  「コントロールパネル」の「BitLocker ドライブ暗号化」で保護を再開したいドライブについて「保護の再開」を選択

K)　ドメイン環境での展開

BitLocker の回復パスワードをドメインコントローラへ自動的にバックアップするように設定しておくことにより、回復パスワードをドメインコントローラで統合的に管理できます（Windows Server 2008 R2 ドメインコントローラ）。

- 「コンピュータの構成」→「管理用テンプレート」→「Windows コンポーネント」→「BitLocker ドライブ暗号化」→「オペレーティングシステムのドライブ」を開き、「BitLocker で保護されているオペレーティング システム ドライブの回復方法を選択する」を「有効」に設定
  （Windows 7 はこれにより回復パスワードがドメインコントローラへバックアップされる）
  ※ OS ドライブ以外についても適用したい場合は「固定データドライブ」や「リムーバブルデータドライブ」以下にある同様のポリシーを有効にする

ドメインコントローラにバックアップされた回復パスワードは、「Active Directory ユーザーとコンピューター」ウィンドウ上の該当するコンピュータのプロパティで表示させることができます。そのためにはドメインコントローラに「BitLocker ドライブ暗号化管理ユーティリティ」がインストールされている必要があります。

- 「BitLocker ドライブ暗号化管理ユーティリティ」のインストール
  サーバーマネージャで「機能の追加」により「リモートサーバー管理ツール」の「BitLocker ドライブ暗号化管理ユーティリティ」の機能をインストール

- BitLocker の回復パスワードを表示
  「Active Directory ユーザーとコンピューター」ウィンドウで該当するコンピュータのプロパティを表示、「BitLocker 回復」タブを選択

商品名称等に関する表示

Active Directory、BitLocker、BitLocker To Go、Microsoft、Windows、Windows Server、Windows Vista は Microsoft Corporation の米国およびその他の国における登録商標または商標です。本書に記載されている会社名、製品名は、それぞれの会社の商標もしくは登録商標です。

暗号技術導入計画書（雛形）
― モバイル PC に対する EFS／BitLocker の導入 ―
（初版）

平成２４年４月

著作・発行　情報セキュリティ大学院大学
〒221-0835
神奈川県横浜市神奈川区鶴屋町 2-14-1
＜URL＞ http://www.iisec.ac.jp/

- 本書は、文部科学省「私立大学戦略的研究基盤形成支援事業」に採択された研究プロジェクトの一環として作成されたものです。