明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

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 ―

（2012/03/29 版）

情報セキュリティ大学院大学

はじめに

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である「暗号技術の導入による機密情報の適切な保護方式の研究」の中で実施される「モバイル PC[1]の暗号化導入支援」において、コンサルタントが顧客企業に対し暗号技術導入のコンサルティングを行う際に参照する手引書として書かれたものです。本書で取り扱う暗号技術は、Windows OS に標準的に備わっている「EFS（暗号化ファイルシステム）」および「BitLocker」を対象としています。

ここでのコンサルティング対象企業は中小企業をターゲットとしているため、高度に統合化された Active Directory 環境やスマートカードによる認証インフラ等は想定していません。ただし将来的な Windows ドメインでの運用については考慮を加えています。

本書の構成は以下の通りです。

1 暗号技術導入の流れ
2 コンサルティング作業の概要
3 導入計画作成の考え方
4 EFS に関する技術情報
5 BitLocker に関する技術情報

[1] 社外に持ち出す機会のある PC を特にターゲットとしているためモバイル PC としているが、社外に持ち出す機会のないデスクトップ PC を対象外とするものではない。

1　暗号技術導入の流れ

顧客に対する暗号技術導入の流れを下図に示します。

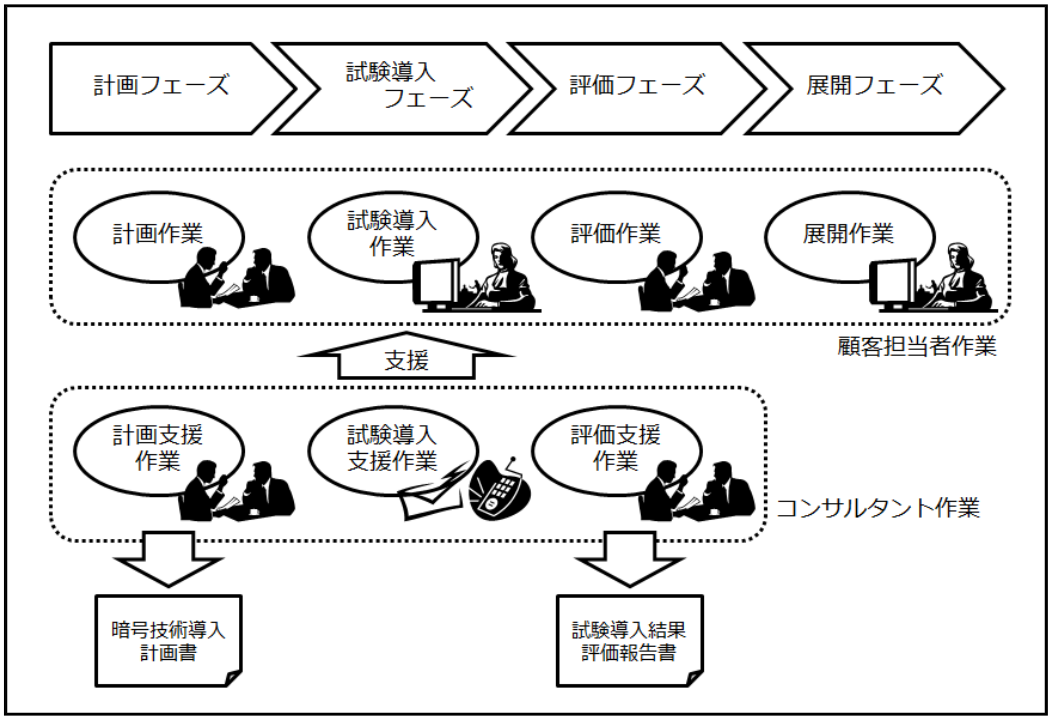


図　暗号技術導入の流れ

- 計画フェーズ
  計画フェーズでは顧客の担当者と打合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う。コンサルタントはその結果を「暗号技術導入計画書」としてまとめる。

- 試験導入フェーズ
  試験導入フェーズでは計画書に基づき、顧客企業内部において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る。導入や運用に関わる作業は顧客担当者にて実施し、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う。

- 評価フェーズ
  評価フェーズ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する。コンサルタントはその結果を「試験導入結果評価報告書」としてまとめる。コンサルティング作業は基本的にはこの時点で完了とする。

- 展開フェーズ
  顧客内部で社内的に暗号技術の展開（他の PC への導入、Windows ドメインへの統合など）を進めるフェーズ。追加的なコンサルティングが必要な場合は別途調整する。

2　コンサルティング作業の概要

A)　計画支援作業

「計画支援作業」は計画フェーズにおけるコンサルティング作業です。計画支援作業の全体像を下図に示します。

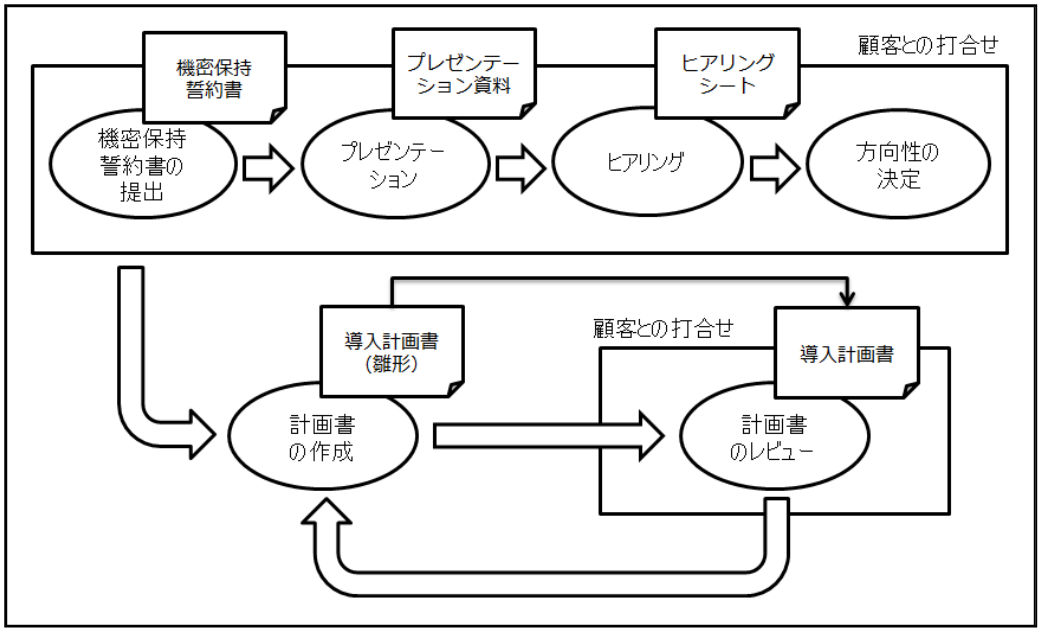


図　計画支援作業の全体像

- 機密保持誓約書の提出
  初回の顧客との打合せの冒頭において、参加する各コンサルタントは「機密保持誓約書」に署名し、顧客へ提出する。

- プレゼンテーション
  プレゼンテーション資料「モバイル PC の暗号技術導入について」を使用し、顧客に対してなぜ暗号技術を導入する必要があるのか、どのような暗号技術を導入するのか、今後の作業の進め方等を説明する。(1 時間程度)

- ヒアリング
  「ヒアリングシート」に沿って、顧客の情報システム環境、保護対象となる機密情報の種類や保存場所、モバイル PC の運用形態など、必要となる情報の聞き取りを行う。(30 分程度)
  ※　事前にヒアリングシートを顧客へ送付し、ヒアリング内容を通知しておくこと

- 方向性の決定
  ヒアリング結果に基づき、暗号化対象とする具体的な PC や使用する暗号技術、暗号化するデータや万一の場合のデータ回復方法などを顧客と協議し、暗号技術導入の方向性について決定する。(1 時間程度、ここまでを初回の打合せにおいて実施)

- 計画書の作成
  上記の打合せ結果を持ち帰り、「暗号技術導入計画書（雛形)」をベースに顧客に適した「暗号

技術導入計画書」を作成する。

- 計画書のレビュー
  導入計画書を顧客へ提出し、打合せにて内容を説明、顧客のレビューおよび承認を受ける。計画書の内容について大幅な見直しが必要な場合は、持ち帰って再度作成を行う。

計画書レビューにて顧客の承認が得られた段階で計画フェーズは完了し、試験導入フェーズへと移行することになります。

B)　試験導入支援作業

試験導入フェーズでは顧客企業が計画書に基づいて、暗号技術の試験的な社内導入および運用を実施します。このフェーズではコンサルタントは「試験導入支援作業」として電子メールや電話による支援を行い、原則、訪問コンサルティングは実施しません。

C)　評価支援作業

1～2 か月程度の試験導入フェーズにおける試験的な暗号技術の運用の後に、評価フェーズとして導入／運用状況に関する評価を行います。ここではコンサルタントは「評価支援作業」として客先へ訪問し、導入過程や試験運用時における問題点などについてヒアリングを実施、「試験導入結果評価報告書」としてまとめ提出します。

3　導入計画作成の考え方

導入計画の作成は本コンサルティングにおける最も重要な作業として位置づけられます。ヒアリングで顧客から聞き取った情報に基づき、初回の打合せ時に以下の事項について方向性を決定した後、持ち帰って具体的な計画書を作成することになります。

- 試験導入対象のコンピュータ
- 使用する暗号技術と暗号化の対象
- データ回復に関する方針
- 試験導入および評価フェーズのスケジュール
- その他必要事項

A)　試験導入対象のコンピュータ

本コンサルティングのフレームワークでは、まず「試験導入フェーズ」として 1～3 台のコンピュータに暗号技術を導入し、試験的に運用してから「展開フェーズ」で社内展開を図るという流れになります。最初に試験導入するコンピュータはシステム管理者等、ある程度の問題に自ら対応できるユーザのノート PC を選択することが推奨されます。そうでない場合はユーザからの問合せに迅速に対応できる体制が必要となります。

導入計画書には試験導入フェーズで暗号技術を導入するコンピュータを識別するため、メーカー、機種名、社内における識別情報（管理番号やホスト名等）、OS の種類、エディション、サービスパックレベルといった情報を記述します。

B)　使用する暗号技術と暗号化の対象

基本的に OS およびハードウェアの要件が満たされていれば、使用する暗号技術として BitLocker を採用します。もし BitLocker が使用できない場合は EFS による暗号化を選択します。EFS／BitLocker それぞれの要件については後述の技術情報を参照してください。BitLocker と EFS の両方を併用することも可能です。現在すでにサードパーティの暗号化ソリューションを導入して運用している場合、また特殊なユーザ認証機構を導入している場合などは、EFS や BitLocker との運用上の整合性について確認します。

BitLocker を利用する場合はどのディスクドライブを暗号化するか決定します。通常、OS ドライブ（一般的には C ドライブ）は原則として暗号化対象となります。他にデータドライブが存在する場合、必要に応じてそれらも暗号化対象とします。BitLocker では OS ドライブの保護方法として TPM か USB メモリ・キーのいずれかを使用しますが、TPM が使用可能な場合は TPM を選択し、PIN（暗証番号）を組み合わせてセキュリティを強化します。

EFS を利用する場合は、機密情報が格納されているフォルダや、機密情報のファイルを個別に暗号化対象として指定する必要があります。ヒアリングの時点で暗号化する具体的なフォルダ名やファイル名が判ればそれを記録します。BitLocker と EFS を併用する、つまり BitLocker でドライブ全体を暗号化し、さらに機密情報を EFS で暗号化することにより、そのコンピュータを使用可能な他のユーザからの不正なアクセスを防ぐことが可能になります。

導入計画書には各コンピュータごとに EFS／BitLocker いずれを使用するのか、また暗号化対象は何かについて具体的に記述します。

C)　データ回復に関する方針

顧客と協議して万一の際のデータ回復方法に関する方針を決定します。基本方針として以下の考え方に基づくことが一般的に行われます。

- 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

事実上システム管理者とユーザが同一人物である場合でも役割としてはそれぞれを分けて考え、後述の技術情報を参考にデータ回復方針を検討します。

D)　試験導入および評価フェーズのスケジュール

試験導入フェーズおよび評価フェーズについて、おおよそのスケジュールを決定します。

E)　その他必要事項

相互の担当者の連絡先等、その他の必要事項について検討／調整を行います。

4　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。

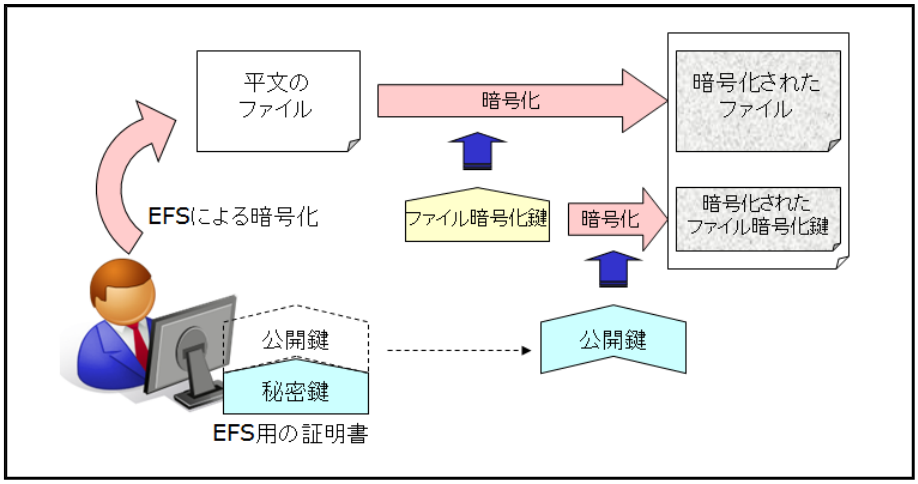


図　EFS によるファイル暗号化の仕組み

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。

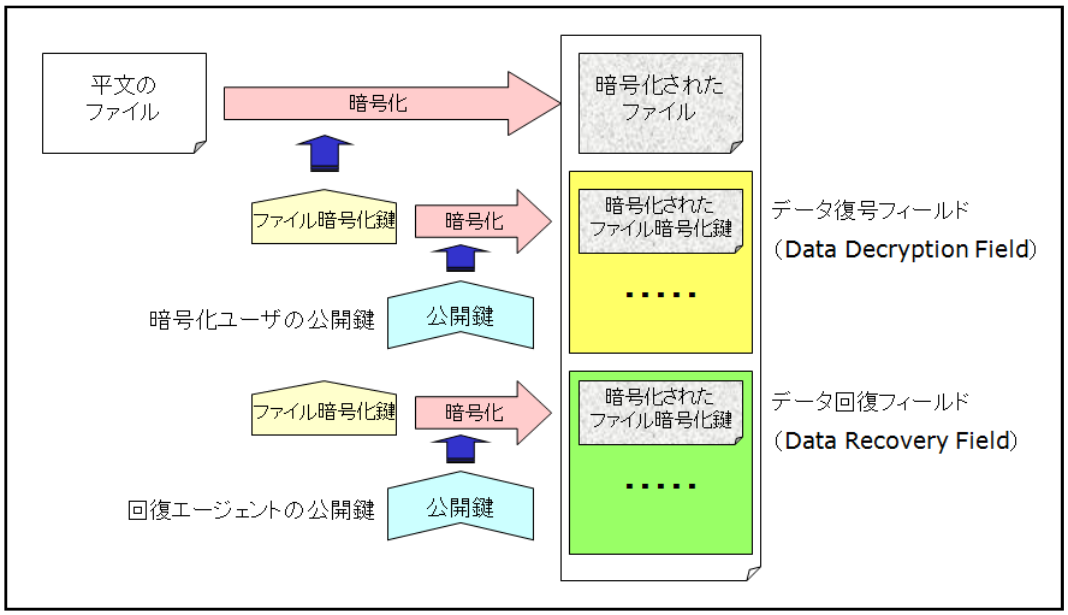


図　EFS における回復エージェントの仕組み

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

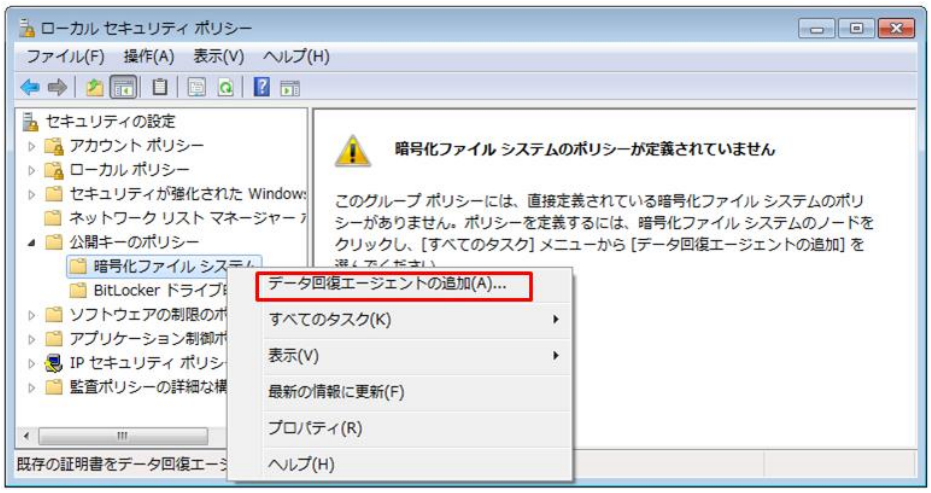
- 回復エージェントの作成【システム管理者が実行】
  システム管理用のコンピュータ上（XP 以降）で以下のコマンドを実行し、回復エージェントの EFS 証明書を作成する

  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



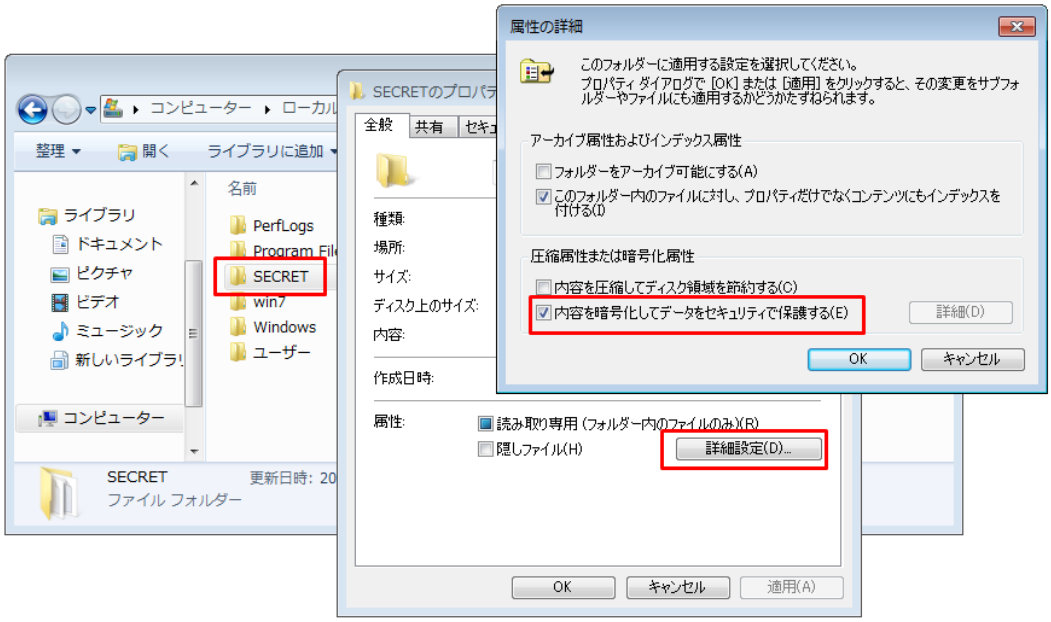
  システム管理用コンピュータで作成した「EFSRecover..CER」を当該コンピュータへコピーし、「回復エージェントの追加ウィザード」でそのファイルを指定することによりデータ回復エージェントとして登録

  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

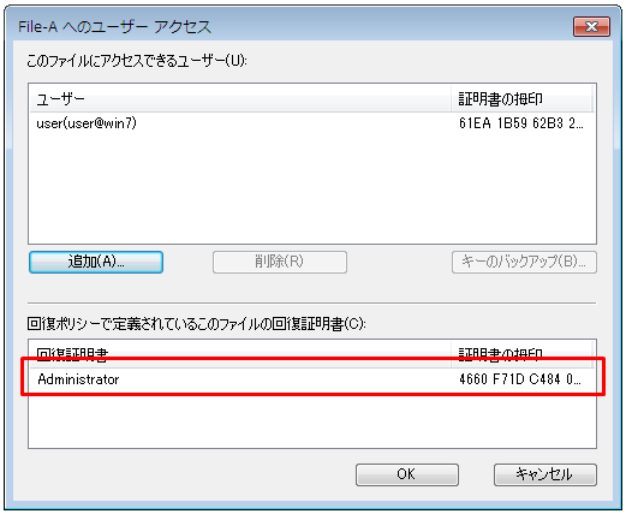
  「属性変更の確認」ウィンドウが表示された場合は「変更をこのフォルダー、サブフォルダーおよびファイルに適用する」を選択する

  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

5　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

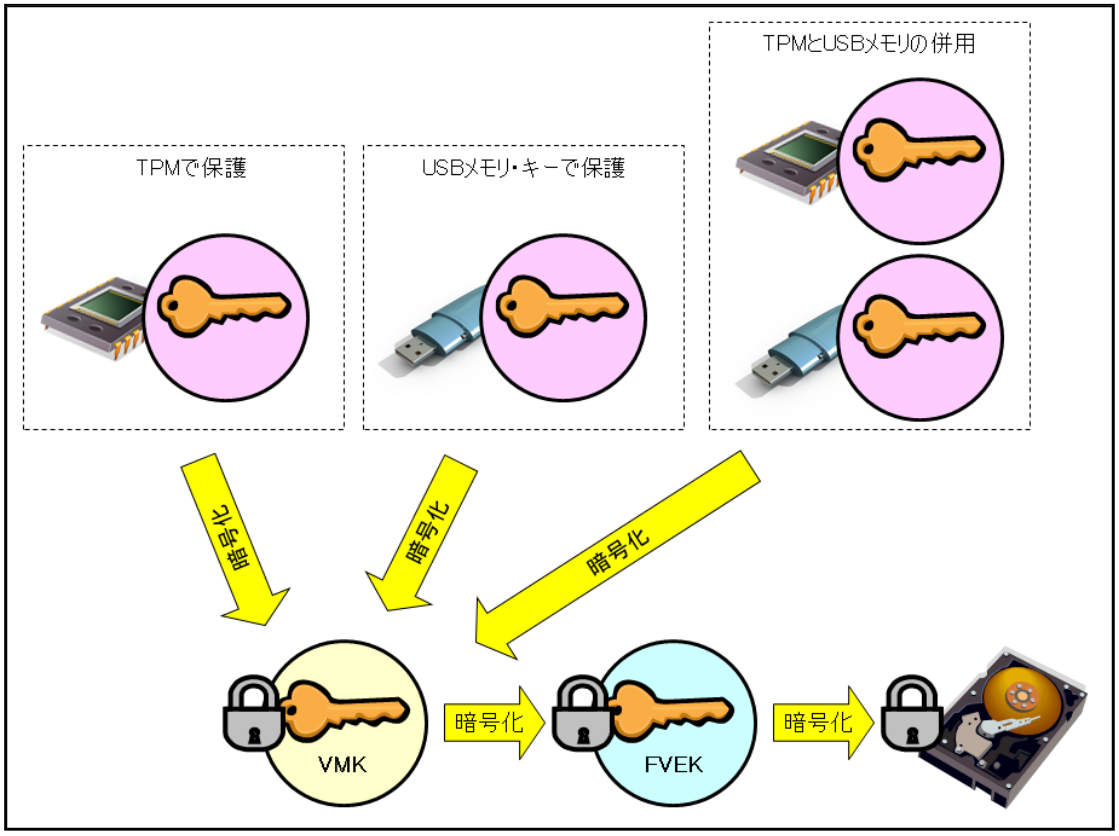


図　BitLocker における鍵の関係のイメージ

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

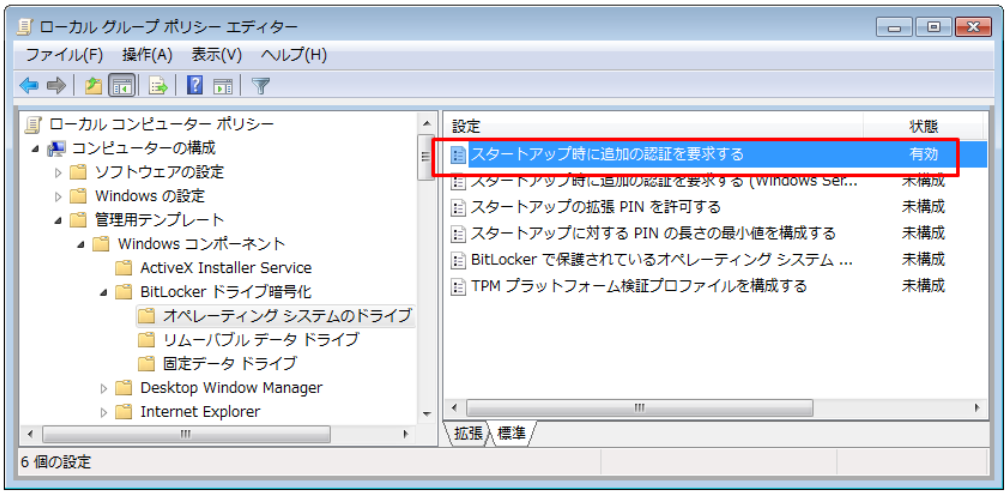
- BIOS の設定変更【システム管理者が実行】
  USB メモリからの OS 起動を優先するように設定されている場合は、BIOS の設定を変更し、ハードディスクからの OS 起動が最優先となるようにする

  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

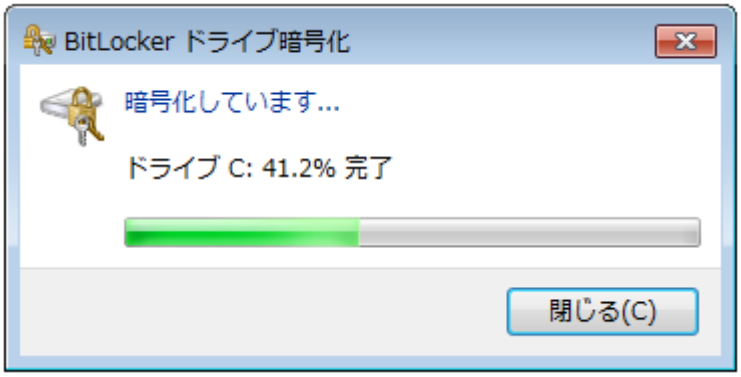
  再起動の過程で TPM の初期化へ移行する場合は、指示に従って TPM の初期化を行う（TPM 初期化処理は BIOS の種類に依存）

  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）

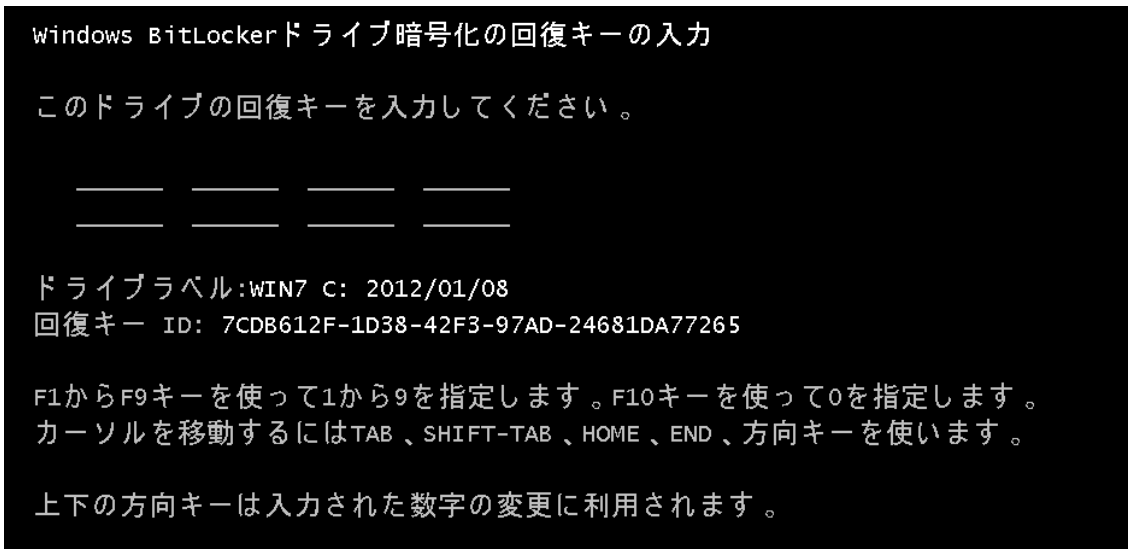


以上で OS ドライブへの BitLocker 導入は完了
※　ドライブ暗号化の実行中も通常の作業を行うことは可能

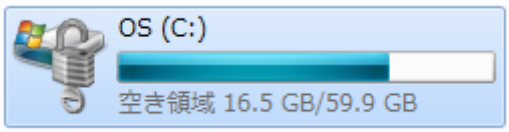
- 回復キーのテスト【システム管理者が実行】
  再起動時に回復キーを保存した USB メモリを挿入して OS が正常に起動することを確認

- 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

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 ―
（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。