Appleテクニカルホワイトペーパー

FileVault 2の導入に関するベストプラクティス

OS Xディスク全体の暗号化テクノロジーの導入

2012年8月 – OS X 10.7.4

目次

概要

企業のデータセキュリティが侵害されると、顧客、信用、多額の罰金や損害など、悪影響を及ぼす恐れがあります。貴重品を金庫に保管して大切に保護するのと同じ原則が機密性の高いコンピュータファイルにも適用されます。ただし、コンピュータファイルは、物理的な金庫ではなくファイルの金庫に保管されます。

ユーザーがコンピュータに機密情報を保管する場合、企業の将来が危険にさらされる可能性があります。たとえば、社員がポータブルコンピュータに機密性の高い財政データを保存し、そのコンピュータを紛失してしまうと、第三者がこのデータを悪用して組織に大きな損害を与えかねません。強力な暗号化を使用することで、こうしたファイルを保護し、情報を安全に保つことができます。

特別なアクセス権がユーザーに付与されている場合や、保護された領域のみへのデータ保存を許可するポリシーがない場合は、不注意によるデータ漏洩の危険性があります。ディスク全体を暗号化することで、不注意によるデータ漏洩の危険性をなくし、確実にすべての情報が保護されるようになります。FileVaultを有効にすると、ハードドライブ上でも組織の情報を安全に保存できます。

第2世代のFileVault、FileVault 2は、OS Xに組み込まれているディスク全体の暗号化（FDE）により、すべてのボリュームの保存データを保護します。コンピュータの紛失や盗難時も、FileVault 2はディスクレベルでのXTS-AES-128データ暗号化により、ハードドライブ上のすべてのファイルを安全に保ちます。Apple製ハードウェアとソフトウェアの統合により、組織は、企業のIT部門がアクセス可能なテクノロジーにより、社内外のディスクドライブに保存されているすべてのユーザーデータを、ユーザーに意識させず、必要な時に保護できます。

企業のIT部門にはさまざまな機密データの保護オプションがありますが、各オプションのトレードオフを理解することにより、最適なアプローチを確実に導入できるようになります。考慮すべきトレードオフの1つとして、FileVault 2がパスワードベースの認証に制限される点が挙げられます。

OS Xの強力なFileVault 2によって、組織の機密データを悪意のある不正なアクセスから確実に保護できます。管理者は基盤となる要素を基にさまざまな方法でFileVault 2を導入および使用して、本書では取り上げられていないさらに複雑なデータ保護を実現できます。

保護を実現。シンプルさを維持。

内蔵の保護機能

OS Xに組み込まれている管理しやすい暗号化テクノロジー、FileVault 2はボリューム全体を保護します。FileVault 2を使うと、専門のITスタッフがいなくとも、だれでも簡単にボリューム全体の暗号化を使用できます。

FileVault 2ではボリューム全体のすべてのデータが暗号化されるため、個々のファイルを暗号化したり、暗号化された特定のコンテナにファイルを保存したりする必要はありません。バックグラウンドで行われるこの保護機能により、ユーザーはデータ保護について心配することなく、重要なタスクや通常のワークフローに集中できます。

本書の内容

FileVault 2の効果とシンプルさを十分に理解するには、そのアーキテクチャ、さまざまな設定の意味、ユーザーとサポートの特定のニーズを満たすためにこうした暗号化ボリュームを管理する最良の方法を理解することが重要です。

大規模組織にとっては、FileVault 2の基盤について、またIT部門による保護ストレージの操作を可能にするFileVaultマスターアイデンティティ（FVMI）の使い方を理解することが鍵となります。エンタープライズにおける効果的な導入では、FVMIの適切なプロビジョニングと使用が非常に重要です。

高レベルでのサポートテクノロジーについての説明も同様に重要です。CoreStorageの詳細、キーチェーンの操作、暗号化アルゴリズムなど複雑なテクノロジーについては、明確化を目的として説明しますが、本書では詳しく取り上げません。

設計方法

信頼性の高い安全なアーキテクチャを提供するだけでなく、個人の使用から企業の管理下でのアクセスなど、さまざまな状況に適合させる必要性があるため、FileVault 2はいくつかの重要な要素を考慮して設計されました。

使いやすさ

FileVault 2では、エンドユーザーによる使いやすさを重視しています。セキュリティのエキスパートではないエンドユーザーでも、データを保護できるようにしなければなりません。また、個人の復元に対する安全策（Appleのサーバに保護された復旧キーを保管するなど）が組み込まれていることも、エンドユーザーにとっては重要です。複雑な手順が増えることなく、どこからでもこの保護を使用できることが求められます。

FDEの使いやすさという点では、エンドユーザーの2回にわたる認証に従来依存してきたことが障害となります。ユーザーは、一度「プリブート認証」を行って暗号化された起動ボリュームをロック解除してから、ディレクトリサービスアカウントにもう一度ログインする必要があります。何らかの理由で資格情報の不一致が生じれば、ユーザー体験は不快なものとなります。何度も認証を行ったり、パスワードを変更するたびに一致させたりすることなく、ユーザーの安全なアクセスを確実にすることで、使いやすさを向上することができます。ユーザーは、ボリュームを再暗号化することなく、いつでもパスワードをリセットできる必要があります。

ITによるアクセス

管理者はデータがコントロールできなくなることを恐れています。パスワードを忘れた場合など単純な状況から、ボリュームへの法的アクセスが関与する複雑な状況まで、管理者が、エンドユーザーのボリュームへの認証済みアクセスを有効にするメカニズムを配備することが重要です。承認済み管理者によるアクセスと変更に関する最小限かつ具体的な条件を加え、FVMIを使った団体の復元方法に対するサポートを強化することで、個人のセルフサービス復元方式を超えて機能を拡張できます。大規模組織におけるFVMIの導入でのベストプラクティスは、エンドユーザーとITサポートの機能と制限によって異なります。

パフォーマンス

FileVault 2でのユーザーのメリットは、アーキテクチャ設計における最適化、暗号化アルゴリズム、ハードウェアアクセラレーションの使用（可能な場合）にあります。ブロック暗号化で使用されるXTS-AES-128アルゴリズムは、512バイトブロックのために最適化されています。標準テキストから暗号テキストへの変換はバックグラウンドで行われ、ユーザータスクに処理サイクルを譲るため、ユーザー体験に対する影響はほとんどありません。Intel Core i5とi7が搭載されたシステムでは、内蔵のAES-NI命令セットを使ったハードウェアアクセラレーションにより、ソフトウェアの最適化がさらに高速になります。

導入に関するベストプラクティス

多様なデータ保護のエンタープライズポリシーやアプローチの選択肢の中から、すべてのユーザーに合う導入シナリオを1つに絞ることは最良のアプローチとは言えません。FileVault 2の最良の導入方法を特定するには、使用環境、IT部門がどのようにエンドユーザーをサポートし、必要に応じて暗号化ボリュームへのアクセスを復元するかを考慮することが重要です。

以下の導入方法には、設定、毎日の使用、そして最大の課題である必要に応じた復元という点で、それぞれ利点と欠点があります。

ほとんどの大規模組織では、組織全体に1つのアプローチを適用して、1つの方法を標準化する代わりに、ユーザーのさまざまなカテゴリのニーズに合った方法を組み合わせています。組織のユーザー層ごとの用途のほか、ITスタッフのサービス、能力、制限を把握することが重要です。

導入

以下の3通りの導入方法を考慮できます。

セルフサービス—エンドユーザーが各自のシステム設定、使用、個人の復元を完全にコントロールする1対1の導入方式。

- **利点**：ITリソースにほとんど負担がかからない。完全なオフラインでの復元が可能。
- **欠点**：エンドユーザー側での責任と理解を要する。企業キーエスクローでの問題。コンプライアンスの徹底とモニタリングに追加のリソースが必要となる。

カフェ—セルフサービスに類似するが、オプションのメニュー、初期設定時のサービス、日常の使用、ボリュームの復元についてITがエンドユーザーをサポートする。

- **利点**：ITによる管理、専門的なガイダンス、必要に応じた実証済みツールの使用。
- **欠点**：コンプライアンスの徹底とモニタリングに追加のリソースが必要となる。

一元管理型—すべてのデータを保護し、常に復元可能な状態にしながら、ITスタッフがユーザーシステムの設定と管理を厳格に管理する。

- **利点**：ITがコンプライアンスとキーエスクローを保証する。
- **欠点**：導入と復元計画でITリソースに大きな負担がかかる。

セルフサービス方式

1対1の導入

セルフサービス方式は1対1の導入方法で、エンドユーザー自身がシステム設定、使い方、復元の管理を行う環境でのFileVault 2の使用に重点を置きます。この場合、システムが企業の一元管理型ディレクトリサービスから独立して機能するだけでなく、単一のシステムで1人のユーザーがFileVault 2を使用します。

ターゲット環境

この方法は、組織のデータセンターとネットワークサービスに適切な管理体制が配備され、個人で使用できることがユーザーにとってメリットとなる場合に適切です。この導入方法では通常、エンドユーザーがすべての操作を管理し責任を持ちます。必要に応じてITスタッフがガイダンスを提供できますが、ほとんど介入しません。

各自のシステムで完全な管理者権限を持つユーザー、復元サポートを必要とするがネットワークアクセスがないユーザーに適しています。

導入

セルフサービス導入では、エンドユーザーが自由かつフレキシブルに、各自のワークフローとニーズに合った状況と方法で、FileVault 2を有効化、変更、無効化することができます。

この導入の要件は、各ユーザーがシステム設定の変更と、FileVault 2設定のためのローカル権限を持っていることです。こうした変更はすべて「システム環境設定」>「セキュリティとプライバシー」>「FileVault」で行います。

FileVault 2を有効にするには、承認権限（`system.preferences.security`）を取得可能なアカウントでシステム環境設定をロック解除する必要があります。

承認権限は、認証データベース（/etc/authorization）で定義され、ローカルの管理者グループのメンバーにデフォルトで付与されます。エンドユーザーにシステムの完全な管理者権限がない場合は、「セキュリティとプライバシー」環境設定での設定変更を許可することができます。ただし、これを許可すると、ユーザーがシステム上のあらゆるセキュリティ設定を変更できることになります。権限のないユーザーに付与できる、FileVault管理専用の権限はありません。ただし、権限を持つユーザーが資格情報を入力して1回限りの認証を行うことで、FileVaultを有効にするエンドユーザーを支援できます。

個人の復旧キー（PRK）

企業における制限事項と復元の状況に応じて、オフラインでPRKを保管する設定と、Appleサーバに保管する設定のいずれかを選択できます。企業によっては、企業が管理するインフラストラクチャ内ですべての暗号化キーと復旧キーの保管を管理することが規則で定められている場合があります。一方、特にネットワークリソースへの接続が完全に切断された場合など、いつでもどこでも復元できる必要性を重視する企業もあります。

オフラインでの保管を選択した場合は、ランダムに生成されたPRKを書き留めるかスクリーンショットを撮って、コンピュータ以外の場所で保護することになります。この場合、PRKを保持できる自動化システム方法はありません。また、FileVaultの有効化プロセスでPRKを書き留めないと、永久的に紛失してしまう可能性があります。

AppleサーバにPRKを保管することを選択した場合、ユーザーは、保管前にPRKのWrapに使用する対称鍵を生成するために、3つのセキュリティ質問に答えます。対象鍵は、エンドユーザーだけが知っているこれらの質問への正確な答えを入力しない限りWrap解除できません。必要な時にユーザーが思い出せるように、答えが複雑すぎないように注意します。

復元

FileVault 2を有効にしても、毎日のワークフローは変わりません。ユーザーはディレクトリサービスのアカウントパスワードを使って定期的にログインします。プリブートEFIログインでパスワードを入力すると、オペレーティングシステムが起動し、ログインの資格情報が求められた時にシステムがパスワードの転送を開始します。パスワードの転送により、コールドブート時に2回ログインする必要がなくなります。

ユーザーがアカウントパスワードを忘れてしまった場合や、承認済みFileVaultユーザーの不在時にIT部門がシステムにアクセスする必要が生じた場合はどうすればよいでしょうか？PRKの使用は、こうした場合での安全策となります。

プリブート時のログインで誤ったパスワードを3回入力すると、「パスワードを忘れた場合は、復旧キーを使ってパスワードをリセットできます」というメッセージがパスワードフィールドの下に表示されます。ユーザーはこのメッセージの横にある三角形をクリックして「復旧キー」フィールドを表示し、コンピュータのシリアル番号とレコード番号も入力する必要があります。エンドユーザーはAppleCareに電話して、設定時に提供した3つのセキュリティ質問への答えなど、必要な情報を提供します。エンドユーザーにAppleCareのサポートを提供することで、IT部門は毎日の電話対応に追われることなく、企業インフラストラクチャ全体の向上に集中できます。

利点

セルフサービス方式の最大の利点は、ITコストの削減とエンドユーザーへの権限の付与にあります。ポジティブなユーザー体験は、企業セキュリティの遵守に大きく貢献します。複雑な規制やリソースに負担のかかるタスクからネガティブな体験をすると、エンドユーザーは保護に対する安全策を回避するようになってしまいます。

オフラインでの保管を選択すると、PRKを書き留めて安全な場所に保管するという簡単な方法から、ウェブフォームや電話を通じてヘルプデスクサービスにPRKを提出するというさらに統合的なアプローチまで、さまざまなシナリオが可能です。オフラインでの保管の場合、組織はどのような状況でも自社の管理下でPRKを保持および取得できます。

AppleサーバでのPRKの保管を選択すると、エンドユーザーがいつでもどこでもシステムを復旧できるという柔軟性が生まれ、キーの強力な保護も提供できます。エンドユーザーがFDEプリブート認証に失敗した場合、コンピュータではOSが実行されず、リモートアクセスサービスを使用できないため、ヘルプデスクスタッフはサポートを必要とするユーザーにネットワーク経由で連絡できなくなります。AppleサーバにPRKを保管すると、エンドユーザー側の柔軟性が高まるだけでなく、キーが厳重に保護されます。専任の企業ITリソースは必要ありません。

短所

セルフサービス方式での最大の課題は、PRKのエスクローの自動化と、ユーザーによる遵守の徹底です。

オフラインでの保管方法を選択すると、組織はPRKを後で取得できるよう中枢サーバにPRKを再エスクローするための自動化プロセスを使用できません。PRKの高度なエスクローと取得方法を希望する場合は、クライアント管理サービスまたは自社のツールセットへの統合が必要になります。既存のエンタープライズエスクローサービスへのPRKの統合にかかる追加の時間とコストが、このアプローチの妨げとなる可能性もあります。

経験の少ないユーザーやOS Xをはじめて使うユーザーは、各自での管理と取得に不安を感じるかもしれません。多くのユーザーは、ほかのプラットフォームに移行する場合、テクニカルサポートのためにヘルプデスクに電話で問い合わせることが当然だと思っています。このようなエンドユーザーに責任を移すことは、最良のユーザー体験とは言えません。

セルフサービスの導入を行うと、企業は団体の復旧キー（IRK）を使用する一元管理型方式を活用できません。これら2つの方法は排他的です。

セルフサービスの導入の欠点がエンドユーザーにとっての利点よりも大きい場合は、カフェまたは一元管理型方式を検討すべきです。

まとめ

セルフサービス方式では、設定、管理、復元の責任がエンドユーザーに移行されます。これにより、ITコストの大幅削減と、ユーザー体験の向上が可能です。ユーザーが満足すると規則を遵守する傾向が高まり、その結果ITコストはさらに削減されます。

経験の少ないユーザーがほかのプラットフォームから移行する場合は、各自での管理と復元に不安を感じるかもしれません。エンドユーザーに完全に責任を移すことは、こうしたユーザーにとって最良のユーザー体験とは言えません。この方式では、FileVault 2の有効化と無効化に管理者権限が必要となるため、企業の管理下にあるアセットには適切ではない、または許可されない可能性があります。

ユーザーがネットワークから完全に切断されている場合など、必要な場合はいつでもアカウントパスワードをリセットして、認証済みアクセスを確実にすることは、ユーザーと企業ITの両方にとって大きなメリットとなります。

このセルフサービス方式は、組織のデータセンターとネットワークサービスに適切な管理体制が配備され、個人で使用できることがユーザーにとってメリットとなる場合に適切です。

カフェ方式

サポート付き導入

カフェ方式はサポート付きの導入方法で、ユーザーコミュニティが自らの使用の大部分のコントロールを求める一方、エンドユーザーの確実なデータ保護についてはITスタッフがサポートすることが企業または業界で要件化されているような組織に適しています。このアプローチでは、IT管理者は必要に応じてセキュリティの専門性、導入オプション、復元サポートを提供できますが、有効化と使用に関するタスクはエンドユーザーに任せます。

ターゲット環境

この方式は、ユーザーによる管理、企業ポリシーの遵守、ユーザーアカウントの安全な保護と復元のバランスを考慮した最善の妥協案と言えます。ITスタッフとエンドユーザーの両方がプロセスに介入し、責任を分担しながら企業または業界の各種要件の遵守を徹底させることができます。

専門的な知識を持つITスタッフは、トレーニングと、エンドユーザーが必要に応じて参照できるガイダンス資料を作成できます。ITスタッフは、暗号化の状態をモニタリングし、適宜ユーザーにアクションを求めるためのローカルのツールやサービスを作成して提供することもできます。

プラットフォームをはじめて使用する大規模組織はこの方式を採用して、ポジティブなユーザー体験を提供しながら、管理された環境に移行することができます。比較的自由なIT環境のユーザーは、企業のIT部門による厳しい管理に抵抗を示すかもしれません。責任を分担することで、エンドユーザーとITの懸念を軽減し、エンドユーザーの体験を向上しながら、インフラストラクチャ側の改善に時間を割くことができるようになります。

導入

サポート付き導入でも、エンドユーザーには自由と柔軟性がありますが、FileVaultの有効化、変更、無効化に対する責任は企業のIT部門と分担します。自由と責任の分担には、エンドユーザーと企業のIT部門との協力が必要となります。

完全なシステムアクセスと断続的なネットワークアクセスを持つ管理ユーザーが、一般的にこの方法に適しています。組織のIT管理者は、大きな責任を持たない、または責任を持ちたくないというユーザーをサポートできます。責任を分担することで、セルフサービス方式または一元管理型方式にはない設定と復元における柔軟性が高まります。

導入設定での要件は、ユーザーのワークフロー（個人または団体）に最適な復元方法によって異なります。個人と団体の両方の復元方法を一度に有効にすることはできませんが、この2つの方法を切り替えることはできます。切り替えを可能にするには、1つの方法でボリュームを復号化し、別の方法で再暗号化することが必要となります。

復元

復元方法では、個人の復旧キー（PRK）と団体の復旧キーを使った個人の復元が可能で、ユーザーは標準のログインウインドウ（プリブートログインではなく）でロックされたシステムでアカウントパスワードをリセットできます。

PRKを使うと、保管や、必要に応じた企業のIT部門の介入に関する詳細を設定できます。PRKに関する詳細は、「セルフサービス方式」セクションと、本書全体の情報を参照してください。

パスワードのリセット

IRKの使用は、企業のIT部門がパスワードのリセット操作全体を管理することなく、エンドユーザーをサポートできる効果的な方法です。ただし、システムはIRKの保管ボリュームにアクセスできないため、エンドユーザーはプリブート復元でIRKを使用できません。ヘルプデスクなどのITスタッフは、標準ログインウインドウのテキストフィールドに入力する、事前設定のマスターパスワードをエンドユーザーに提供できます。IRKがあり、ユーザーが標準ログインウインドウでログインに失敗した場合は、通常のサポート電話として電話でマスターパスワードを提供するか、保護された企業ウェブサイトへの安全な認証アクセスに制限することもできます。これにより、エンドユーザーはITスタッフと協力して自分のパスワードをリセットできます。この方法は、オフライン環境では特に便利です。

マスターパスワードは、完全なFileVaultマスターアイデンティティ（FVMI）を含むFileVaultマスターキーチェーン（FVMK）を保護するパスワードです。

エンドユーザーは非表示の復元用HDを使って、企業の保護されたウェブサイトからPRKに安全にアクセスして取得することもできます。FileVault 2を実行しているシステムには、この目的のために特別に設計された非表示の復元用HDパーティションがあります。このパーティションは、「起動ディスク」環境設定にも表示されず、ディスクユーティリティアプリケーションでも表示できません。エンドユーザーはMacを再起動してすぐにキーボードのCommand+Rキーを押します。Macが復元モードに起動を開始したら、キーを放します。復元によって、限定的なゲスト専用のアクセス環境が読み込まれ、ユーザーはSafariを開いて企業の保護されたウェブポータルにアクセスして認証できます。認証が完了すると、企業の安全な保管場所からPRKを取得できます。

利点

カフェ方式の最大の利点は、エンドユーザーと企業のIT部門で責任を分担できることにあります。ポジティブなユーザー体験は、企業セキュリティの遵守に大きく貢献します。このアプローチでは、エンドユーザーとITスタッフの両方のニーズと能力に応じて選択的に責任を割り当てることができます。

IT部門は、重点的なガイダンスと復旧キーポータルを作成し、エンドユーザーが各自でタスクを行えるように、管理および保護されたアクセスを与えることで、リソースにかかる負担の大部分に事前に対処できます。また、ITスタッフは企業のインフラストラクチャ外で保管場所やキーを使用することなく、機密情報を保持しながら、ガイダンス、復元、モニタリングを向上することもできます。

内蔵の復元用HDと、限定的なゲスト専用アクセスにより、機密情報を開示したり、システムの整合性または暗号化ボリュームを危険にさらしたりすることなく、エンドユーザーは企業の保護されたコンテンツに安全にアクセスすることができます。

短所

カフェ方式での最大の課題は、エンドユーザーとIT部門にどの責任を割り当てるかを判断すること、また安全なキーエスクローと取得用ポータルを使ったウェブベースのガイダンスコンテンツの作成でITリソースが必要となることにあります。

多くの組織では、トレーニング、テクノロジーに関する説明やガイダンスの提供にすでにウェブベースコンテンツを使用しているため、FileVaultに関するユーザーコンテンツを追加してもリソースに大きな負担はかからないと考えられます。安全なキーエスクローと取得用ポータルは、PRK自体またはIRKのためのマスターパスワードのいずれかを取得・配布できるよう特別に作成する必要があります。

IT側が分担する責任への対処にはリソースと開発が必要となることが主な欠点です。強固なOS X統合を備えたクライアント管理ソリューションを使っている組織は、ベンダのツールセット内ですべての、あるいはほとんどのITタスクを頻繁に実行できます。

まとめ

カフェ方式は、組織のユーザーコミュニティにある程度の能力があるが、限定的なITスタッフの介入が必要となる場合に適しています。このアプローチを用いると、実際の有効化と復元はエンドユーザーに任せ、IT部門はセキュリティに関する専門性、導入オプション、復元に関するサポートを提供できます。

知識の豊富なITスタッフが、トレーニング、ガイダンス、またエンドユーザーが安全にアクセスできる復旧キーエスクロー／取得用ポータルを作成できます。復旧キーの作成と取得は、各ユーザーの導入方式によって異なり、柔軟性のあるアプローチを提供します。経験の少ないユーザーがほかのプラットフォームから切り替える場合は、管理と復元をITスタッフに任せる方が安心かもしれません。

カフェ方式は、組織が強力なITリソースプールを持つが、FileVault 2の使用の大部分を管理するエンドユーザーのニーズや需要とITリソースとのバランスが求められる場合に最適です。IT部門は、エンドユーザーの体験を制限することなく、エンドユーザーにアドバイスやガイダンスを提供する専門家として機能できます。

一元管理型方式

ITが管理する導入

一元管理型方式は、ITスタッフにユーザーシステムの厳格な管理を任せ、ユーザーデバイス上のすべてのデータをディスク全体の暗号化（FDE）で保護しながら、復元にはITの介入を必要とする組織に最適です。この導入方式では、ITスタッフが暗号化ボリュームの作成、管理、復元のすべての局面をコントロールする必要があります。ITの完全な介入により、適切な導入、システムの監査、企業または業界の規則の遵守の徹底を確実にします。

ターゲット環境

この方式は、規制の厳しい環境または安全性の高い環境に適しています。エンドユーザーによる失敗を防ぎ、常にすべての規制の準拠を確実にするために、導入プロセスのすべての段階が認定ITスタッフによってコントロールおよび実行されます。

プラットフォーム関する知識が豊富な大規模組織は、厳格に管理された環境でこの方式を採用し、一般的に強力なクライアント管理ツールを使用します。多くのクライアント管理ツールが、FileVaultマスターキーチェーン（FVMK）、FileVaultマスターアイデンティティ（FVMI）の導入と管理、およびOS Xに組み込まれている`security`コマンドなど、Appleが提供するコマンドラインインターフェイス（CLI）をサポートします。

FDEソリューションの導入では、FMVIのプロビジョニングとエスクローにエンタープライズの認証局（CA）が不可欠です。セキュリティに重点を置く管理者、ワークグループマネージャ、ヘルプデスクスタッフ間で責任が分担されるため、機密情報への認証とアクセスも管理が必要です。

導入

一元管理型方式では、ITスタッフが完全な暗号化ボリュームへのアクセスを設定する上で、FVMIの適切な生成、保護、管理が非常に重要です。これは3つの方式のうち最も複雑な方式で、通常、エンドユーザーの代わりにITスタッフまたは上級OS Xユーザーがすべてのプロセスを実行します。OS Xによる特定の条件を満たしている限り、組織では多様なツールセットを使用できます。

FVMIと、関連する各コンポーネントの目的をよく理解することで、FDEの保護とアクセスの成功を確実にし、管理が容易になります。FVMIは、暗号化ボリュームへの認証済みアクセスのための鍵暗号鍵（KEK）のWrapとWrap解除に使用する一組の非対称鍵（公開鍵と秘密鍵）を提供します（詳しくは、「付録A：アーキテクチャの概要」を参照してください）。このITによるアクセス方法は、完全な暗号化ボリュームのロック解除に承認済みユーザーの資格情報を必要としないという点で特に興味深い方法です。

組織は、独自のエンタープライズCA、「マスターパスワード設定」のための内蔵GUIによる方法、またはFVMIが入力するFileVaultMaster.keychainを作成するためのCLIの`security`コマンドのいずれかを使って最初にFVMIをプロビジョニングする必要があります。

FVMIのプロビジョニング

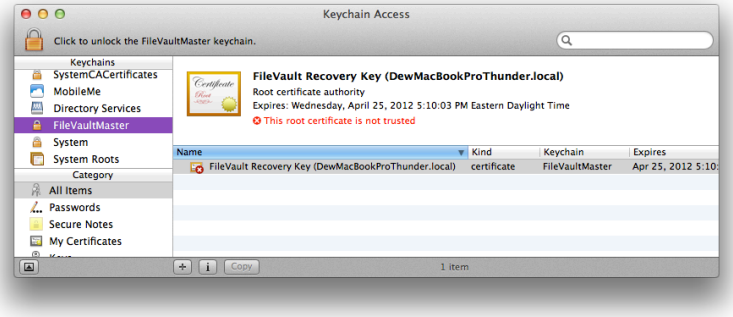
FVMIの適切なプロビジョニングには、組織が独自のエンタープライズCAを使用することが推奨されます。主なメリットは秘密鍵のエスクローです。「付録A：アーキテクチャの概要」の要件にそって、FVMIをプロビジョニングする必要があります。必須の属性と属性値に従わないと、キーのWrapとWrap解除でFVMIを適切に使用できなくなります。

組織のインフラストラクチャとITリソースが複雑さと詳細さに対応できる場合は、FileVault 2を有効にするすべてのシステムでFVMIをプロビジョニングすることが推奨されます。これは、FileVault 2の技術的な条件ではありませんが、このレベルでプロビジョニングすることにより、組織は各システムの鍵を選択的に管理できるようになります。さらには別の中間CAからも管理できる可能性があります。これと反対のアプローチは、FileVaultを有効にするすべてのシステムで1つのFVMIを発行することです。この場合は、何らかの理由で1つのFVMIが侵害されると、組織全体のシステムが危険にさらされることになります。同じFVMIを使って有効にしたすべてのコンピュータを1つのアイデンティティでロック解除または復号化できるためです。

FVMIの導入

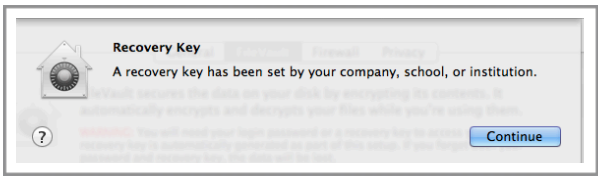
FileVault 2を有効にするには、承認権限（`system.preferences.security`）を取得可能なアカウントでシステム環境設定のロックを解除する必要があります。こうした権限は、認証データベース（`/etc/authorization`）で定義され、ローカルの管理者グループのメンバーにデフォルトで付与されます。

「FileVaultMaster.keychain」というキーチェーンファイル（FVMIの証明書コンポーネントのみを含む）を、クライアント管理ツールを使って既存のクライアントにプッシュし、新しいシステムのイメージング時にディスクイメージ内に含める必要があります。パス「/ライブラリ/Keychains/FileVaultMaster.keychain」のファイルシステム上に配置します。



含まれるのは証明書だけです。ITが管理するFileVault 2の有効化に必要なのは、証明書に埋め込まれている公開鍵のみだからです。最も機密性の高いコンポーネントである秘密鍵を含めないことで、FVMIの悪質な侵害の可能性が軽減されます。秘密鍵は、暗号化ボリュームで復元を行う時に必要です。システム上に完全なFVMIが含まれる場合、不正なユーザーがこれにアクセスすると、そのシステムと、同じFVMIを使って有効にしたほかのシステムをロック解除または復号化できるようになります。

OS Xでは、GUIを使ったFileVault 2の設定と、システム設定の変更権限を持つ管理者がFileVault 2をオン／オフにする必要があります。これは、「システム環境設定」>「セキュリティとプライバシー」>「FileVault」で「FileVaultを入にする」をクリックして行います。特殊な資格情報の保管場所であるFVMKには証明書のみが入力され、「/ライブラリ/Keychains/FileVaultMaster.keychain」ですでに設定されているため、管理者には次のスクリーンショットのような通知が表示されます。



この通知は、FVMKがIRKとして適切に導入されたこと、KEKのWrapには証明書の公開鍵が使用されること、認定ITスタッフが後でアクセスして使用する時のために保管することをOS Xが認識していることを示します。「`Library/Keychains/FileVaultMaster.keychain`」が導入されていない場合や、キーチェーンに完全なFVMIが含まれている場合、「セルフサービス方式」セクションの説明の通り、デフォルトでPRKの設定になります。FileVault 2はPRKまたはIRKのいずれかを認識しますが、両方は認識しません。

マスターパスワードの設定

組織は、「マスターパスワードの設定」を使ってデバイス上に直接FVMIをプロビジョニングして導入することもできます。「マスターパスワードの設定」とは、ランダムなFVMIを生成し、新しく作成した「FileVaultMaster.keychain」キーチェーン内にこれを保管して、FVMKのパスワードを、「マスターパスワード」で入力したパスワードに設定するようOSにリクエストすることを指します。キーチェーンまたはマスターパスワードのエスクローを希望または必要とする場合は、マスターパスワードの設定後に行うことができます。

FVMIプロビジョニングのスクリプティング

FVMIをプロビジョニングするもう1つの方法として、CLIの`security`コマンドを使用します。`security`コマンドの使い方については、このセクションの後半で詳しく説明します。

代替管理者アカウント

代替の管理者アカウントを設定して、FileVault 2を有効にすることが推奨されます。このアカウントは、管理者がアカウントパスワードをリセットして、完全な暗号化ボリューム上で復元を行わずにボリュームをロック解除できるもう1つの方法です。これにより、FileVault 2の知識があまりないITスタッフでも、パスワードのリセットについてエンドユーザーをサポートできます。

復元

ユーザーはディレクトリサービスのアカウントパスワードを使ってシステムにログインするため、FileVault 2を有効にしても毎日のワークフローに影響はありません。プリブートEFIログインでパスワードを入力すると、オペレーティングシステムが起動し、ユーザーのログイン資格情報の入力が求められた時にシステムがパスワードの転送を開始します。パスワードの転送により、コールドブート時に2回ログインする必要がなくなります。

承認済みFileVaultユーザーの不在時にIT部門がシステムにアクセスする必要が生じた場合はどうすればよいでしょうか？IRKの使用は、こうした場合での安全策となります。

パスワードのリセット

アカウントパスワードをリセットするには、暗号化された起動ボリュームを最初にロック解除してアクティブにする必要があります。これはユーザーが1人だけの場合は不可能です。コンピュータは最初にEFIを使ってプリブートを行うため、承認済みユーザーがボリュームをロック解除して、ブートプロセスを続けることが必要となります。パスワードリセットを行うために、代替の管理者アカウントを設定して、FileVault 2を有効にすることが重要なのはこのためです。

代替の管理者がボリュームをロック解除してシステムにアクセスすると、ユーザーのアカウントで標準のパスワードリセット（「ユーザとグループ」環境設定から）が行われます。OS Xからパスワードをリセットすると、FileVault 2にアクセスする対応ユーザーもリセットされ、ユーザーのパスワードから生成された新しいパスワード（派生暗号鍵（DEK））を使用しなければならなくなります。

外部のディレクトリサービス側（Active Directoryなど）からユーザーのパスワードをリセットすると、ユーザーの新しいパスワードではプリブート時にボリュームをロック解除できません。この場合も、代替の管理者がボリュームをロック解除し、ログアウトしてから、システムのログインウインドウでユーザーに新しい資格情報を入力してもらうことが必要となります。

FVMIベースの復元

完全な暗号化ボリュームを復元したり、法的なアクセスが必要となったりする場合は必ず、完全なFVMI、つまり証明書（埋め込まれている公開鍵）と、有効なキーチェーン（FVMI.keychainなど）に保存された秘密鍵の両方が必要となります。これは、エンタープライズCAからFVMIを取得するためのすべての手順が、認定IT管理者によって行われていることを前提とします。空のキーチェーンファイルを作成して、FVMIの読み込みを自動化する方法が最も簡単です。キーチェーンを作成してFVMIを読み込む方法には、securityコマンドを使用した完全なスクリプト化を含め数通りの方法があります。ターミナルアプリケーションとCLIコマンドを使った方法は以下の通りです。

1. 新しいFVMIキーチェーンを作成して、USBメモリスティックに保存します。
    a. `# security create-keychain -P /Volumes/<ファイルパス>/FVMI.keychain`
    b. これにより、FVMI.keychainというキーチェーンが入力したパスに作成されます。
    c. プロンプトが表示されたら、キーチェーンを保護する希望のパスワードを入力します。
2. エンタープライズCA（FVMI.p12）から書き出したFVMIを読み込みます。
    a. `# security import /PathTo/FVMI.p12 -k /Volumes/<ファイルパス>/FVMI.keychain -f pkcs12 -P`
    b. プロンプトが表示されたら、キーチェーンと.p12ファイルを保護するパスワードを入力します。
3. 復元対象のコンピュータを復元用HDに起動します。
    a. キーボードでCommand+Rキーを押して、復元用HDに起動します。
4. 「ユーティリティ」メニューから「ターミナル」を開きます。
5. 暗号化ボリュームの論理ボリュームUUID（LvUUID）を特定します。

a. CoreStorageボリュームの管理について詳しくは、「付録A：アーキテクチャの概要」を参照してください。

6. USBメモリスティックを挿入します。
7. FVMIキーチェーンのロックを解除します。
   a. `# security unlock-keychain -p <パスワード>`
      `/Volumes/<ファイルパス>/FVMI.keychain`
8. CoreStorageが暗号化したターゲットボリュームのロックを解除してマウントします。
   a. `# diskutil cs unlockVolume <LvUUID>`
      `-recoverykeychain`
      `/Volumes/<ファイルパス>/FVMI.keychain`

これらの手順が完了すると、ボリュームがロック解除およびマウントされ、あらゆるツールやサービスがアクセスできるようになります。これにより、ボリューム上のファイルのアップデートや変更（システムまたはアプリケーションファイルのパッチ適用など）が可能になります。

同じ暗号化ボリュームから起動を試みる場合は、FVMIを使ったロック解除はできません。内蔵の復元用HDなど、代替ドライブから最初に起動する必要があるのはそのためです。復元用HDは不変イメージで、整合性が検証され、読み取り専用起動ボリュームとしてマウントされます。整合性に問題がある場合は使用できず、最新のOS Xベースシステムで、ファームウェアでのインターネット復元がサポートされる場合は、デフォルトでインターネット復元になります。また、ほかのユーザーによるソフトウェアのインストールや設定変更により、非表示の復元用HDを改ざんすることも防ぎます。

利点

一元管理型方式は、ITスタッフがFVMIの事前設定と、暗号化ボリュームへの常時アクセスを完全に管理できるという点が最大の利点です。ポジティブなユーザー体験は企業のセキュリティ規定の遵守に貢献しますが、この場合は、IT部門がFileVault 2の使用におけるすべての段階を厳格に管理します。通常ユーザーは、日常の使用以外では、FileVault 2のどの管理段階にも介入しません。

FVMIのプロビジョニングと秘密鍵のエスクローに独自のエンタープライズCAを使用するという点が、IT部門にとってこのアプローチが魅力的な理由です。CAが、「付録A：アーキテクチャの概要」に記載されている要件を満たすアイデンティティを発行できる限り、各組織のニーズとITリソースに合った詳細レベルを選択できます。FileVault 2を使うと、組織は1つのアプローチや1つのキーエスクロー方法に限定されません。

新しいシステムに復元されるイメージ上でFVMIを設定したり、すべての既存OS Xシステムにプッシュアウトしたりすることで、IT部門は承認済みユーザーの資格情報がなくてもこうしたボリュームに常にアクセスできます。プロセスの大部分をスクリプト化し、イメージングと導入の既存のワークフローに統合できます。

短所

これは、3つの方式のうち最も複雑です。FileVault 2管理のすべての段階でITスタッフまたは上級OS Xユーザーの介入が必要となります。組織が使用するツールセットも役には立ちますが、エンドユーザーがアカウントパスワードを入力することなくFileVault 2を完全に有効にするソリューションはありません。

OS Xでは、ボタンを押すだけで、1個所から複数のシステム間でFVMIを生成しエスクローできる自動化機能はありません（つまり、データセンターに対する内蔵コンソールサポートもありません）。ベストプラクティスでは、組織が複数のエンタープライズサービスを使用し、内部導入または追加のITリソースを通じて機能を統合することが必要となります。

まとめ

一元管理型方式は、ITスタッフがユーザーシステムを厳格に管理し、ITの管理下でのみFDEの復元を可能にすることを望む組織に最適です。この導入方式では、ITスタッフが暗号化ボリュームの作成、管理、復元のすべての局面を行う必要があります。

完全なITの介入により、適切な導入、システムの監査、企業または業界の規定の遵守が確実にはなりますが、ITコストは増加し、計画と実行はさらに複雑になります。

ITスタッフは、プロビジョニング、エスクロー、IRKを使った適切な設定と復元について知識を深めることが必要です。

コンプライアンス

組織では一般的に、コンピュータの配備と保存データの保護に関して数種類の規制を適用しています。そのうち最も頻繁に議論される要件は、FIPS 140-2適合性検証の必要性と支援テクノロジー（通称第508条またはアクセシビリティ）の対応の2つです。

FIPS 140-2適合性検証

米国およびカナダ政府は、製品で使用される暗号モジュールの適切な確認と検証を目的として、米国の国立標準技術研究所（NIST）とカナダの通信セキュリティ機関（CSEC）内で暗号モジュール検証プログラム（CMVP）という検証プログラムを運営しています。暗号モジュール自体で行われる検証、検証済み暗号モジュールを使用しているオペレーティングシステム、サービス、アプリケーションは「FIPS 140-2準拠」と呼ばれます。

OS X Lion 10.7では、OSリリースではじめてFileVault 2（FDE）が導入されました。FileVault 2の基盤にもなっている、新しいカーネルベースの暗号モジュールCoreCryptoは、OS X LionではFIPS 140-2適合性検証に提出されていません。

OS X Snow Leopard 10.6が暗号化ディスクイメージ、S/MIME、SecureTransportなどのサービスで使用している暗号モジュールは、2011年3月9日にFIPS 140-2検証に合格しました。Appleは、OS X Lionにも搭載されているこのモジュールの再検証にも合格しています。OS X LionでレガシーFileVaultのみを使用する場合でも、FileVault 2と共に使用する場合でも、再検証済みモジュールの使用と、FIPS 140-2準拠を実現できますが、パフォーマンスに影響が生じます。

以来、OS Xの暗号モジュールは検証のために提出され、OS X Mountain Lion 10.8リリースでも検証に合格することが予測されています。OS X Mountain Lion 10.8のFileVault 2はFIPS 140-2準拠になる見込みです。

第508条（アクセシビリティ）

プリブート時の認証を使用したFDEの設計上のアプローチにより、アクセシビリティの対応が妨げられ、障害を持つユーザーがFDEサービスを使用できなくなる可能性があります。プリブート時にはデバイスでOSが実行されていないため、OSに依存するテクノロジー（アクセシビリティなど）をデバイスで使用することができません。アクセシビリティの対応を必要とする組織が、アクセシビリティサービスの使用を有効にしながら、ユーザーのホームディレクトリを保護するには、OS X LionのレガシーFileVaultを引き続き使用することが推奨されます。

結論

データセキュリティにおける違反はさまざまな面で組織に損害を及ぼします。個人および企業の機密データの保護は不可欠であり、データを暗号化し、未承認ユーザーによる入手を防ぐことで保護を強化できます。特別なアクセス権がユーザーに付与されている場合や、保護された領域のみへのデータ保存を許可するポリシーがない場合は、組織は暗号化の領域外でのファイル保存による不注意のデータ漏洩の危険にさらされます。ディスク全体を暗号化することで、すべての情報が確実に保護されます。FileVault 2を有効にすると、ハードドライブ上ですべての情報を安全に保存できます。

Appleは、使いやすさ、ITによるアクセス、パフォーマンスという3つの設計上の主要な目標の下、FileVault 2の機能を開発し、向上に取り組んでいます。

FileVault 2はAppleのハードウェアとソフトウェアとの統合の良い例として、個人と組織による社内外の保管場所でのすべてのユーザーデータ保護を可能にします。実行をユーザーに意識させることなく、場合によってはITリソースも必要としません。セキュリティのエキスパートではないエンドユーザーでも、データを保護できるようにしなければなりません。

エンドユーザーと管理者はデータのコントロールを失うことを恐れています。暗号化ボリュームへの制限的な認証済みアクセスのための個人および団体の復元方法により、だれもが必要とする安全性が実現します。IT部門があらゆる状況でエンドユーザーのボリュームにアクセスできることは非常に重要です。団体の復旧キー（IRK）とFileVaultマスターアイデンティティ（FVMI）との統合のサポートにより、個人の復旧キー（PRK）を使った個人のセルフサービス方式を超えて機能が拡張されます。

これまでのパフォーマンスでは、保存データに対するソリューションは限定されていましたが、FileVault 2は、アーキテクチャ設計、最適化された暗号化、ハードウェアアクセラレーションの使用といった最も重要な点において優れています。FileVault 2は、個人および組織の体験を向上しながら、強力な保護を提供します。この事実だけでも、他社製品に十分差をつけています。

企業のIT部門にはさまざまな機密データの保護オプションがありますが、各オプションのトレードオフを理解することにより、確実に最適なアプローチの導入できるようになります。FileVault 2、適切にプロビジョニングおよびエスクローされた復旧キー、導入方式に関する実用的な知識を用いることで、組織は機密データを常に不正なアクセスから確実に保護できるようになります。

付録A：アーキテクチャの概要

FileVault 2は、完全な暗号化ボリューム（起動ボリュームとデータボリューム）へのユーザーおよび管理者アクセスのシステム全体にわたる管理と定義されます。単一のプロセスでもコンポーネントでもなく、OS Xに1つの機能として搭載されている複数のコンポーネント管理です。そのため、各コンポーネントがどのようなものか、コンポーネントが1つの機能としてどのように関連し合うかを理解することが重要です。

FileVault 2は、3つの重要なコンポーネントで構成されており、大規模な導入のための全体的な機能を提供します。

- CoreStorage
- 鍵管理
- 復元方法

CoreStorage

CoreStorageアーキテクチャの図では、各論理ボリュームグループ（LVG）に複数の物理ボリューム（PV）が内在し、複数の論理ボリューム（LV）があることを示しています。各ボリュームを選択的に暗号化できます。

CoreStorageは、高度な論理ボリュームマネージャ（LVM）のためのAppleのアーキテクチャです。CoreStorageはFileVaultと同じではなく、暗号化ビットの保存と取得のためにFileVaultで採用されている論理ボリューム管理機能です。OS GUIでは、FileVaultのCoreStorageサポートは、CoreStorageディスク全体暗号化（CSFDE）とも呼ばれます。

本書ではCoreStorageの詳細は取り上げませんが、そのアーキテクチャとFileVaultとの関係をよく理解することが重要です。

CoreStorageのコンポーネント：

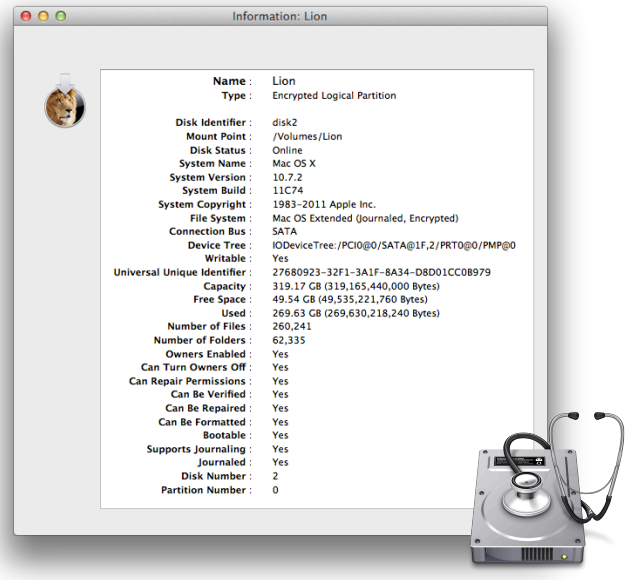
- 物理ボリューム (PV)
- 論理ボリュームグループ (LVG)
- 論理ボリュームファミリー (LVF)
- 論理ボリューム (LV)

物理ボリューム（PV）は論理ボリュームグループ（LGV）の一部で、論理ボリューム（LV）の属性を説明する、論理ボリュームファミリー（LVF）を含みます。

CoreStorageアーキテクチャは複数のLVG、LVF、LVを呼び出しますが、ここでは簡単にするために、結果的に1つの暗号化論理ボリューム（LV）となる1つの論理ボリュームグループ（LVG）の1つの物理ボリューム（PV）に重点を置きましょう。

各CoreStorageボリュームは、128ビット値（空間と時間を通して一意性が保証済み）でフォーマットされた独自の汎用一意識別子（UUID）を使って個別に参照されます。UUIDの標準フォーマットは、ハイフンで区切られたASCII文字列で表記されます（例：486E9812-167F-4129-B1AA-E6A041C69EA6）。

CoreStorageオブジェクトは、ディスクユーティリティアプリケーションまたはdiskutilというコマンドラインインターフェイス（CLI）ツールのいずれかを使って表示および操作できます。




```
Usage:  diskutil [quiet] coreStorage|CS <verb> <options>
       where <verb> is as follows:

list                (Show status of CoreStorage volumes)
info[rmation]       (Get CoreStorage information by UUID or disk)
convert                   (Convert a volume into a CoreStorage volume)
revert              (Revert a CoreStorage volume to its native type)
create              (Create a new CoreStorage logical volume group)
delete              (Delete a CoreStorage logical volume group)
createVolume        (Create a new CoreStorage logical volume)
unlockVolume        (Attach/mount a locked CoreStorage logical volume)
changeVolumePassphrase(Change a CoreStorage logical volume's passphrase)

diskutil CoreStorage <verb> with no options will provide help on that verb
```

既存のCoreStorageボリュームに関する情報を収集するには、ターミナルウインドウで次のdiskutilコマンドを実行します。

```
$ diskutil cs list
+-- Logical Volume Group 486E9812-167F-4129-B1AA-E6A041C69EA6
    =========================================================
    Name:         Lion
    Sequence:     1
    Free Space:   0 B (0 B)
    |
    +-< Physical Volume ABF9FDE7-8481-43FB-A9BB-1E316C182DC1
    |   ----------------------------------------------------
    |   Index:    0
    |   Disk:     disk0s2
    |   Status:   Online
    |   Size:     319484211200 B (319.5 GB)
    |
    +-> Logical Volume Family 02064501-2BE1-442E-B317-C21379CE5DD2
        ----------------------------------------------------------
        Sequence:                 13
        Encryption Status:        Unlocked
        Encryption Type:          AES-XTS
        Encryption Context:       Present
        Conversion Status:        Complete
        Has Encrypted Extents:    Yes
        Conversion Direction:     -none-
        |
        +-> Logical Volume F9EC4CFD-9440-4A43-A3F9-83F670153DFC
            ---------------------------------------------------
            Disk:                 disk2
            Status:               Online
            Sequence:             4
            Size (Total):         319165440000 B (319.2 GB)
            Size (Converted):     -none-
            Revertible:           Yes (unlock and decryption required)
            LV Name:              Lion
            Volume Name:          Lion
            Content Hint:         Apple_HFS
```

FileVaultの暗号化では、NIST SP 800-38EのNISTガイダンスに準拠する256ビットキーを使ったAES-XTS-128暗号化アルゴリズムを採用しています。

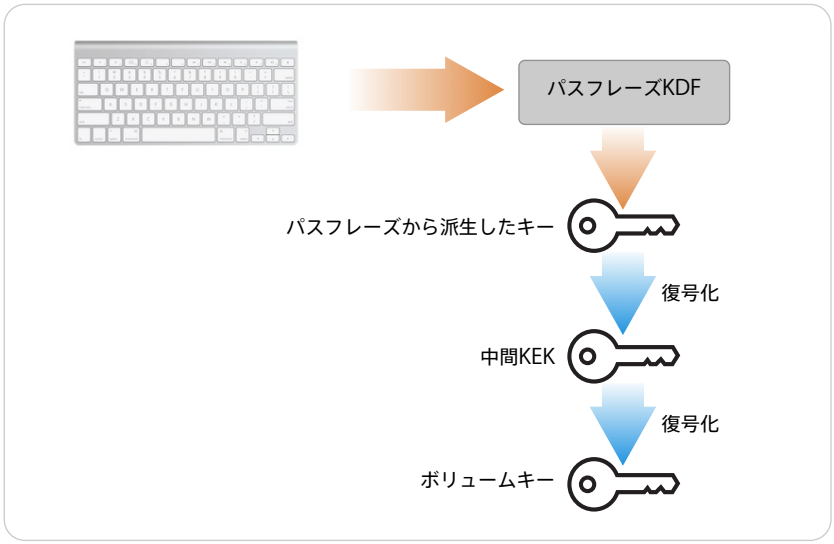
次のコマンドに正しいUUIDを挿入して実行すると、ボリュームの暗号化の状況や存在を取得できます。

```
$ diskutil cs info 02064501-2BE1-442E-B317-C21379CE5DD2
      CoreStorage Properties:
   Role:                     Logical Volume Family (LVF)
   UUID:                     02064501-2BE1-442E-B317-C21379CE5DD2
   Parent LVG UUID:          486E9812-167F-4129-B1AA-E6A041C69EA6
   LVF Encryption Status:    Unlocked
   LVF Encryption Type:      AES-XTS
```

このサンプルボリュームは、AES-XTSで完全に暗号化され、現在マウントされロックは解除されています。

LVF UUIDでdiskutil cs infoを実行すると、親LVG UUIDを見つけて特定できます。LV UUIDで同じコマンドを実行すると、LV UUIDから親LVF UUID、親LVG UUIDまでのUUIDの完全なチェーンと、暗号化ボリュームへの変換ステータス（ここでは「Complete」）が表示されます。

```
$ diskutil cs info F9EC4CFD-9440-4A43-A3F9-83F670153DFC
      CoreStorage Properties:
   Role:                     Logical Volume (LV)
   UUID:                     F9EC4CFD-9440-4A43-A3F9-83F670153DFC
   Parent LVF UUID:          02064501-2BE1-442E-B317-C21379CE5DD2
   Parent LVG UUID:          486E9812-167F-4129-B1AA-E6A041C69EA6
   Device Identifier:        disk2
   LV Status:                Online
   Conversion Status:        Complete
   Content Hint:             Apple_HFS
   LV Name:                  Lion
   Volume Name:              Lion
   LV Size:                  319165440000 B
```



鍵の管理

このセクションでは、OSでのFileVault 2の鍵管理について説明します。組織での復旧キーの管理には触れません。団体の復旧キーのプロビジョニングと管理についての詳細は、付録の後半部分で説明します。

CoreStorageを使った暗号化ボリュームでは、データ保護と、認証アクセス、ユーザーパスワードのリセット、復元へのアクセスサポートのための、Wrapされた暗号キーの文字列があります。ここでは、起動ボリュームでのFileVaultの使用を重点的に取り上げますが、CoreStorageは、データボリュームにおけるディスクパスワードも提供します。データボリュームの導入には、1つの一意のパスワードが便利な場合があります。

鍵管理には、暗号化キーと復旧キーの両方の管理と使用が関与します。3レベルの暗号化キーと、2種類の復旧キーがあります。

この3つのレベルのキーラッピングアーキテクチャの目的と柔軟性を理解するには、まず関連する3つのキーについて理解することが重要です。

- ボリューム暗号化キー (VEK)
- 鍵暗号鍵 (KEK)
- 派生暗号鍵 (DEK)

ボリューム暗号化キー

最低レベルで、CoreStorageは対象ボリューム暗号化キー（VEK）を使って512バイトの論理ブロックで動作します。各VEKは独立した論理ボリュームにそれぞれランダムに生成されるため、論理ボリューム上でのすべての暗号化操作は、各ボリュームに固有のものです。この一意のVEKとブロック単位での微調整を組み合わせると、すべてのデータブロックの暗号化がさらに強力になります。ボリューム上でのデータへのアクセスはVEKに依存するため、VEKは常に不変でなければなりません。最終的に、CoreStorageが実際必要とするキーは、このVEKだけであるということができます。

このブロックレベルで実行される暗号化はAES-XTS-128で、256ビットVEKを使用します。XTSは、ストレージデバイス上での機密性のために米国の国立標準技術研究所（NIST）が推奨する新しいAESブロック暗号モードです。XTSは、XEX Tweakable Block Cipher with Ciphertext Stealingの略語です。NISTは、「認証またはアクセス制御が適用されていない場合、その他の承認済みの機密性専用モードと比較し、XTS-AESは暗号化データの不正な操作に対してより強力な保護を提供します」としています。XTS-AESについて詳しくは、http://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf を参照してください。

3つのレベルのキーによる間接参照アプローチにより、組織では、これまでほかのプラットフォームで必要とされたように、ボリュームのキーを再作成する必要がなくなります。組織がこの低レベルでボリュームのキーを再作成する場合は、ボリューム全体を完全に復号化してから暗号化し直す必要があります。通常この概念は、ボリュームでFileVaultが使用されている場合は、「un-vaulting」「re-vaulting」と呼ばれます。

鍵暗号鍵

暗号化ボリュームの初期化中、ランダムで対称的な中間鍵暗号鍵（KEK）が生成され、VEKが暗号化（Wrap）され、CoreStorageメタデータに保存されます。この中間キーにより、間接参照が前述の設計方法の要件をサポートできるようになります。また、この間接化により、派生暗号鍵（DEK）を個別に、VEKから切り離して変更できるようになります。また、VEKをDEKから切り離して変更できるようになります。VEKがKEKでWrapされると、その結果暗号化されたblobは、データの取得と復号化のために、ボリュームのCoreStorageメタデータ内に保存されます。

派生暗号鍵

最上レベルで、ほかの2つのキーのロック解除チェーンを開始し、その結果復号化と暗号化ボリュームへのアクセスが可能になるように、派生暗号鍵（DEK）を使用できる必要があります。DEKは、KEK自体またはVEKにも影響を及ぼすことなく単独で変更できます。この違いは、鍵に関するマテリアルを開示することなく（団体の復旧キーの場合は、特定のユーザーの資格情報を知る必要もありません）、同じ暗号化ボリュームへのさまざまなアクセス方法を有効にするという点で重要な意味を持ちます。

特定のCoreStorageボリュームでは、固有のDEKを持つ複数の暗号化ユーザーをサポートする必要があります。暗号化ユーザーは、OSの認証済みユーザーと同じである場合がありますが、必ずしも同じである必要はありません。暗号化ユーザーとは、特定の鍵がボリュームのロック解除で必要とするすべてのパラメータを指します。特定のボリュームに対して保存されている有効な暗号化ユーザー資格情報のいずれかを入力して、そのボリュームをロック解除できます。

この最上レベルの鍵の派生方法は以下の2通りです。

- パスフレーズベースDEK
- X.509アイデンティティベースDEK

パスフレーズベースDEK

パスフレーズを入力すると、PKCS#5 v2.0およびRFC2898で定義された擬似ランダム関数を内部的に使用するSHA256-HMACを用いたRSAパスワードベースの鍵派生関数（PBKDF2）に基づく鍵に変換されます。その結果生成された鍵がDEKとして使用されます。

DEKの生成では2回パスフレーズが使用されます。

- ログインパスワードベースDEK
- ディスクパスワードベースDEK

暗号化されたボリュームへのオフラインのパスフレーズ推測攻撃を防止することが、システムの主な目標です。ユーザーのパスフレーズが簡単にハッシュ化されると、攻撃者は特殊なハードウェアを使って、事前計算攻撃または総当たり攻撃をマウントする可能性があります。この攻撃を困難にするために、パスフレーズでハッシュ関数を何度も繰り返し、その結果を混合して並列化を難しくする一般的な暗号化手法が使用されます。

ログインパスワードベースDEK

OSの認証済みユーザーとは、暗号化ボリュームのロック解除を許可されたユーザーです。ユーザーのログインパスワードは、各自のディレクトリサービスアカウントのパスワードです。FileVaultでは、複数のOSの認証済みユーザーによるロック解除をサポートする必要があるため、各ログインパスワードは固有の一意のDEKに変換され、KEKを個別にWrapし、後で取得できるようにボリュームのCoreStorageメタデータ内のユーザーのバンドルに保存されます。

複数のOSの認証済みユーザーをサポートすると、予想どおり、FileVaultを有効にしているすべてのユーザーがボリューム全体をロック解除できることになります。ただし、システム環境で追加の暗号化分離とユーザーファイルの含有が許可される場合は、レガシーFileVault（FileVault 1）を同時に使用することを検討してください。FileVault FDEを使った、OS Xシステムでのレガシー FileVaultについては本書では取り上げません。簡単に言うと、ディスク全体の暗号化を提供するFileVault 2のほか、ユーザーのホームディレクトリのコンテナベースの暗号化であるFileVault 1を引き続き使用することです。

ディスクパスワードベースDEK

1つのパスフレーズの使用は、1つのパスフレーズを使用して1つのDEKを生成し、対応KEKまたはボリュームをWrapおよびロック解除する特殊な使用法であると考えてください。この方法で保護されたボリュームは、1人のOSの未認証ユーザーを持つ、FileVaultが有効なボリュームとみなされます。ディスクパスワードは、異なるユーザーが独自のパスワードでボリュームをロック解除することを禁じ、IRKを使用してそのボリュームにアクセスすることを防ぎます。

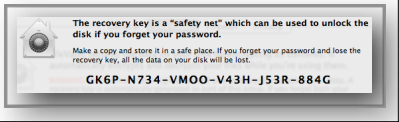
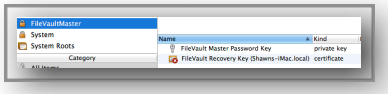
X.509アイデンティティベースDEK

組織では、FileVaultが有効なユーザーのパスワードを使用せずに、暗号化ボリュームをロック解除するための方法が必要になります。その場合は、公開鍵インフラストラクチャ（PKI）が効果を発揮します。一元的なITパスフレーズを複数のデバイスでシンクする代わりに、より安全性が高くプロビジョニングされたX.509ベースアイデンティティ（FVMI）を使用できます。PBKDF2を使ってパスフレーズをDEKに変換したり、PRKを使用したりする代わりに、FileVaultはFVMIの非対称の公開／秘密鍵の組み合わせを使用します。KEKのWrapには公開鍵が、KEKのWrap解除には秘密鍵が使用されます。

復元方法

個人と組織の両方にとって復元は非常に重要です。場合によっては、復元のためのリソースの制限、アクセスできずネットワーク上で孤立しているシステムにより、すべての要素において最適な導入方式が決まることがあります。特定のシステム上でFileVaultを有効にしているユーザーがパスワードを忘れた場合、また資格情報や復旧キーを使用できない場合は、暗号化ボリュームはロック解除できず、データにアクセスすることができません。データが永久的に失われる可能性があるため、適切な復元計画は不可欠です。

検討の対象となる2つの復元方法には、1つ以上の導入方法が関与する場合がありますが、本書では導入方法と復元方法の最も一般的な組み合わせを説明します。

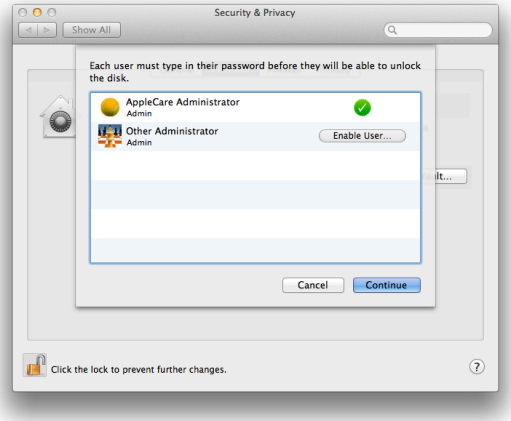
	**個人の復元** 個人の安全策としてランダムな対称鍵を生成して使用する。
	**団体の復元** X.509ベースの非対称鍵のペアを使用して企業の安全策および個人キーエスクローを行う。

個人の復元

個人の復元では、個人の復旧キー（PRK）を使った安全策を提供します。「セキュリティとプライバシー」の「FileVault」パネルから直接始めます。

注意：FileVaultの有効化には権限取得（`system.preferences.security`）のためのアクセス権が必要です。このアクセス権は、ローカルの管理者グループにデフォルトで付与されます。

「FileVault機能を入にする」をクリックすると、Macに複数のユーザーアカウントが設定されている場合は、管理者が（コンピュータの起動またはスリープ／休止状態からの復帰のための）暗号化ドライブのロック解除を許可するユーザーアカウントを指定するように求められます。デフォルトでは現在ログインしているユーザーが有効化済みとマークされ、緑のチェックマークが付きます。



すべてのユーザーアカウントでFileVaultが有効になっている場合は、環境設定パネルに「ユーザを有効にする」ボタンが表示されません。その後作成されるすべてのアカウントで、自動的にFileVaultが有効になります。

FileVaultのロック解除が有効になっていないユーザーは、FileVault 2が有効になっているユーザーがドライブをロック解除した後でのみ、そのMacにログインできます。一度ロック解除されたドライブはそのままの状態を保ち、コンピュータがシャットダウンするか休止状態に入らない限り、すべてのユーザーが使用できます。

管理者は、ボリュームのロック解除機能が必要なすべてのアカウントでパスワードを入力するか、ユーザーにパスワードを入力してもらう必要があります。

ユーザーのディスクのロック解除を有効にすると、PRKが表示されます。

「復旧キーの保管をAppleに依頼しない」を選択した場合、24桁の英数字の復旧キーを取得してコンピュータの外に保管する必要があります。つまり、個人でシステムを設定してキー値を書き留め、コンピュータ以外に安全に保管します。個人または組織が、有効時にランダムに生成される復旧キーを紛失してしまった場合、Appleが復元についてサポートできる方法はなく、すべてのデータが失われます。

この方法では、インフラストラクチャ側にコストや変更は一切必要ありません。PRKを適切に保護すれば、エンドユーザーにとって迅速で簡単な安全策となります。ただし、エンドユーザーが復旧キーを適切に保護しない場合（たとえば、キーを付箋紙に書き留めて職場のデスクに貼り付けるなど）、復旧キーは簡単に見つけられ、侵入者がアクセス権を得てしまいます。

ユーザーが「復旧キーの保管をAppleに依頼」を選択した場合のキーの保護と取得方法については、次のセクションで説明します。

個人の復旧キーの保護

PRKを保護し、反復可能な方法でこのキーを取得およびWrap解除するには、対称のPRKラッピングキーが必要です。このPRKラッピングキーは、選択した3つすべてのセキュリティ質問に対する答えのハッシュにより派生されます。答えのハッシュによりこのキーが派生されるため、PRKを取得するには正確な答えを提供する必要があります。答えが少しでも違っていると、有効な対称キーが派生されません。質問に対する答えはFileVaultを有効にしているユーザーのみが知っているため、これを提供できない場合、Appleが復元についてサポートできる方法はなく、すべてのデータが失われてしまいます。

Appleからの個人の復旧キーの取得

ユーザーがアカウントパスワードを忘れてしまった場合や、ITスタッフが代替のアカウントを有効にすることなく、保護されたボリュームにアクセスする必要がある場合は、PRKが必要となり、Appleからこれを取得できます。

誤ったログインパスワードを3回入力すると、パスワードフィールドの下に「パスワードを忘れた場合は、復旧キーを使ってリセットできます」というメッセージが表示されます。ユーザーはメッセージの横にある三角形をクリックして、「復旧キー」フィールド（「パスワード」フィールドに代わって表示されます）とAppleCareの連絡先、コンピュータのシリアル番号とレコード番号を表示する必要があります。レコード番号は、PRKを最初にAppleに送信した際に生成されます。

AppleからPRKを取得するには、AppleCareに連絡し、シリアル番号とレコード番号を含む必要な情報を提供します。その後、AppleCare担当者がPRKを提供できます。復旧キーを取得して正確に入力すると、ユーザーにはログインパスワードの変更を求めるプロンプトが表示されます。ログインパスワードのリセットでは、新しいログインキーチェーンの作成を求めるプロンプトも表示されます。以前のログインキーチェーンは、デフォルトでアカウントと同じパスワードに設定されます。アカウントをリセットすると、OS Xは以前のパスワードを記憶したり保存したりしていないため、以前のログインキーチェーンをロック解除することはできません。キーチェーンに保存されているパスワードで保護されていないコンテンツだけを新しいキーチェーンに移行できます。

ログインパスワードの変更後、FileVault Recovery Keyも変更して新しいキーをAppleにアップロードすることが推奨されます。

復旧キーの変更

「セキュリティとプライバシー」環境設定の「FileVault」パネルで「FileVaultを切にする」をクリックしてFileVaultを無効にします。オフになると、FileVaultがドライブの復号化を開始します。復号化が完了すると、「FileVaultを入にする」ボタンがクリック可能になります。管理者はこれをクリックしてロック解除可能なユーザーを有効にし、新しい復旧キーを表示して、この新しいキーをAppleに送信するオプションを提供できるようになります。Appleに送信した古いキーを使って、新しく暗号化されたディスクをロック解除することはできません。Appleから復旧キーを取得する必要がある場合は、ログインウインドウに表示されるシリアル番号とレコード番号に基づいて最新のキーのみを取得できます。

団体の復元

団体の復元は企業のIT部門に安全策を提供するとともに、X.509アイデンティティと非対称の公開／秘密鍵のペアを使って秘密鍵エスクローを有効にします。

団体の復旧キー

IRKは、FileVaultマスターアイデンティティ（FVMI）と呼ばれる、企業のプロビジョニング済みX.509ベースアイデンティティを指します。FVMIは、公開鍵と対応する秘密鍵を含むX.509証明書で構成されます。FileVaultはアイデンティティの証明書に記載されている公開鍵を使ってKEKをWrap（暗号化）し、秘密鍵を使ってKEKをWrap解除（復号化）します。

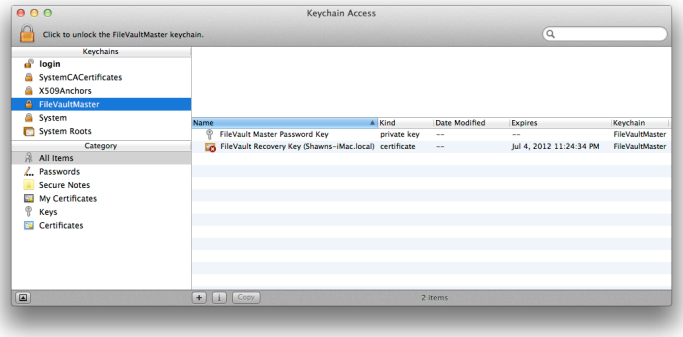
FileVaultマスターアイデンティティ

FVMIは、FileVaultで暗号化されたボリュームへのITアクセスにおいて不可欠なコンポーネントです。このアイデンティティにより、システム管理者またはITスタッフは、承認済みユーザーのパスワードを知らなくとも、代替の方法でユーザーの暗号化ボリュームにアクセスすることができます。

1つのホストにつき1つのFVMIのみを使用できます。組織は、FVMIプロビジョニングの詳細を選択できます。シンプルさを求める場合は、会社全体で1つのFVMIをプロビジョニングできますが、アイデンティティが侵害されると、システム全体が悪質なエンティティの危険にさらされることになります。各コンピュータにそれぞれFVMIをプロビジョニングすることにより、そのリスクを軽減できますが、FVMIと各コンピュータ間の関連付けの管理が複雑になります。組織は安全な管理を可能にする最高のレベルを決定すべきですが、その他に必須の詳細レベルに対する明確なベストプラクティスはありません。

FVMIは3つのコンポーネントで構成されており、これらを組み合わせてX.509デジタルアイデンティティを構成します。

- 自己署名のX.509ルート証明書
- 公開鍵（証明書に埋め込まれている）
- 秘密鍵



デフォルトでは、FVMIはOS Xが生成し管理するFileVaultMasterというキーチェーン内で保護されています。このキーチェーンは「/ライブラリ/Keychains/FileVaultMaster.keychain」にあります。

これはOS Xが管理するキーチェーンの1つで、キーチェーンリストに表示される必要がありません（キーチェーンアクセスユーティリティで表示できます）。ただし、ユーザーまたは管理者がこのキーチェーンの内容を表示したい場合は、このキーチェーンをキーチェーンリストに手動で追加できます。キーチェーンファイルをダブルクリックするか、「ファイル」>「キーチェーンを追加」を選択して、以前のパスに移動し、「開く」をクリックしてキーチェーンを有効なリストに追加します。

キーチェーンの内容を表示するために、キーチェーン保護の資格情報は必要ありません。ただし、キーチェーンの内容を操作する場合は（削除、秘密鍵の書き出し、アイデンティティの置換など）、FileVaultMaster.keychainを保護するパスフレーズ（最初にユーザーまたは管理者が入力したもの）が必要です。保護されたFVMIの使用により、完全な暗号化ボリュームにアクセスできるため、不正なアクセスと使用からアイデンティティを保護することが重要です。

自己署名のX.509ルート証明書

管理者が「ユーザとグループ」環境設定で「マスターパスワードを設定／マスターパスワードを変更」、またはCLIの`security`コマンドの2つの内蔵サービスのいずれかを使用すると、ランダムなX.509アイデンティティが生成されます。FileVault 2はどのような環境でもあらゆるユーザーで機能するよう設計されているため、生成されたアイデンティティ証明書は自己署名です。つまり、完全な公開鍵インフラストラクチャ（PKI）を持っていなくとも、FileVault 2を活用できます。また、このアーキテクチャにより、組織は独自のエンタープライズ認証局（CA）で指定したアイデンティティを使用できます。

どのようなアプローチ（OS Xで直接またはエンタープライズCAからプロビジョニング）を取るかに関係なく、OS XではFileVaultのアイデンティティ証明書のトラストアンカーへの信頼パスを検証する必要はありません。OS Xが生成したアイデンティティの場合、証明書は自己署名ルートCA証明書です。エンタープライズCAが発行した証明書では、信頼できるルートCA証明書、中間証明またはリーフ証明書のいずれかです。公開鍵／秘密鍵（Key Sizeが1K、2Kまたは4K）のペアが適切にプロビジョニングされたアイデンティティの存在と、Key Usageの記載が必要ですが、信頼パスまたは失効の検証は必要ありません。

Subject Name		
Common Name	FileVault Recovery Key	Required
Description	MySystem.local	Optional

Issuer Name		
Common Name	FileVault Recovery Key	Required
Description	MySystem.local	Optional
Signature Algorithm	SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)	Required

証明書には、特定の値を必要とする数個の属性があります。その他の属性はOptionalの値に設定できます。

「Common Name」は「FileVault Recovery Key」に設定されています。FileVaultが正しく認識して

使用するには、この名前を必要とし、正確である必要があります。FVMIを組織独自のCAからプロビジョニングする場合は、この属性を正しく設定するよう十分注意してください。

「Description」はデフォルトで「MySystem.local」に設定されています。FVMKでマスターパスワードを設定する場合、「システム環境設定」>「共有」で設定されているコンピュータ名を基に生成されます。「Description」フィールドには特別な値は必要ありませんが、アイデンティティが組織独自のCAから発行された場合は、証明書内の別のアイデンティティのために、組織はこの属性をホストの完全修飾ドメイン名（FQDN）に設定できます。

OS Xが生成したこの証明書は自己署名ルート証明書です。Subject NameとIssuer Nameにはどちらも、OS XのFileVaultで使用される特殊ケースのCAである「FileVault Recovery Key」に設定されます。この証明書では証明書の失効確認は行われないため、証明書の期限を心配する必要はありません。この証明書は、このプロセスで当初から信頼済みであるため、それが信用済みであることを明示的に指定する必要もありません。

公開鍵

公開鍵は、非対称（公開／秘密）鍵ペアの最初の半分にあたり、KEKのEncrypt／Wrapに使用されます。名前が示す通り、保護策を必要とせずに一般に公開されます。公開鍵はX.509証明書に埋め込まれており、異なるオブジェクトとして抽出または保存する必要がありません。

Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Key Usage	Encrypt, Verify, Wrap
Key Size	1024, 2048, or 4096; default = 1024

「FileVault Recovery Key」アイデンティティの実際の公開鍵は、「Encrypt」「Verify」「Wrap」に設定する必要があります。システムが生成したアイデンティティを置き換える場合は、対応するPublic Key Infoで、少なくとも同じExtension—Key Usageが定義されていることが必要です。

Extension—Key Usage (2.5.29.15)	
Critical	No
Usage	Digital Signature, Key Encipherment, Data Encipherment, Key Cert Sign

「FileVault Recovery Key」アイデンティティの公開鍵についての記載では、「Digital Signature」「Key Encipherment」「Data Encipherment」「Key Cert Sign」の4つすべての機能についてExtension—Key Usageを定義する必要があります。

Extension—Basic Constraints (2.5.29.19)	
Critical	Yes
Certificate Authority	Yes

これは自己署名ルート証明書であるため、CriticalおよびCertificate Authorityとして指定する必要があります。

秘密鍵

秘密鍵は非対称（公開／秘密）鍵ペアのもう1つの重要な半分で、鍵暗号鍵（KEK）の復号化（Wrap解除）に使用されます。秘密鍵は公開されず、常に保護される必要があります。保護されないと、FileVault 2保護が危険にさらされることになります。暗号化ボリュームを安全に復元する機能と、FVMIの適切な管理が、不正なアクセスからシステムを安全に保護する上で非常に重要です。

このX.509ベースアイデンティティの適切な使用と保護は、OS Xの制御とFileVaultアーキテクチャにあまり精通していないユーザーにとって誤解しやすい点です。

FVMIの作成、使用、管理にあたってOS Xが使用するプロセスをしっかりと理解することが重要です。

注意：スタンバイによって、カーネル電源管理が一定の時間スリープ状態にあるコンピュータを自動的に休止状態にします。これにより、スリープ時の電力を節約します。サポートされるハードウェアでは、この設定がデフォルトでオンになっています。この機能がサポートされるコンピュータでは、pmset -gでスタンバイ設定を表示できます。スタンバイは、休止状態モード3または25に設定されている場合のみ機能します。

マスターパスワード

マスターパスワードとは、FileVaultマスターキーチェーン（FileVaultMaster.keychain）で設定されるパスワードを指します。OS Xキーチェーンパスワードは、キーチェーン内に保存されている非公開データのEncrypt（Wrap）に使用されます。FVMIの秘密鍵コンポーネントのロック解除と復号化（Wrap解除）には、マスターパスワードが必要です。対応する証明書は公開情報であるため、保護は必要ありません。

このマスターパスワードは、FileVaultマスターキーチェーンの内容またはKEKの実際の保護に直接的な関連性はありません。キーチェーンに保存されている場合は、秘密鍵へのアクセスのロック解除に直接的に関連します。パスワードは、有効であればどのようなパスワードにも設定できます。導入および保護されているFVMIが、導入されているすべてのシステムで同一の場合でも、多くの場合1台のコンピュータ／1人のユーザーに一意なパスワードが設定されます。

マスターパスワードの差し替え

キーチェーン内で完全なFVMIを保持するよう選択した場合、FileVaultMaster.keychainパスワードを定期的にリセットすることを検討するかもしれません。この場合は、マスターパスワードの定期的な差し替えにより、アイデンティティが危険にさらされるリスクを軽減できます。FVMIが侵害され、不正なユーザーが証明書と秘密鍵の両方にアクセスした場合、FileVaultが有効で、そのFVMIに関連付けられている場合は、承認済みユーザーの資格情報がなくとも、保護されたボリュームへのアクセスをロック解除できます。

ファームウェア

スタンバイモード

ハードウェアコンポーネントの検出、最終的には希望のOSインスタンスを使ったコンピュータの適切なブートストWrapを支援するために、あらゆるコンピュータに、EFI、BIOSなどある種のファームウェアが搭載されています。Apple製ハードウェアでEFIを使用する場合、OS Xの機能性を支援するためにAppleはEFI内に関連情報を保存します。たとえば、スタンバイモードから透過的に復帰できるように、FileVault鍵はEFIに保存されています。

攻撃を受けやすい環境や、デバイスがスタンバイモード時にデバイスが完全なアクセスにさらされることに対して特に敏感な組織は、ファームウェアでFileVaultキーを破棄すると、このリスクを軽減することができます。FileVaultキーを破棄してもFileVaultを使用できなくなるわけではありません。システムのスタンバイモードを解除する時にユーザーがパスワードを入力する必要が生じるだけです。

スタンバイモードに入る時にFileVaultキーを破棄するには、`pmset`コマンドを使って特定の電源管理環境変数を設定します。対象システムで操作中、または自動化または導入のスクリプト実行中に次のコマンドを実行すると、破棄のキーが設定されます。

```
# pmset destroyfvkeyonstandby 1
```

同じ変数を0に設定すると、スタンバイモードに入る時にFileVaultキーが保持される原因となります。

pmsetコマンドdestroyfvkeyonstandbyの詳細と、使用可能なその他の変数は、次のコマンドを実行すると表示できます。

```
# man pmset
```

destroyfvkeyonstandbyの説明は次のように記載されています。

> destroyfvkeyonstandby - スタンバイモードに入る時にFileVaultキーを破棄します。システムがスタンバイに入る時も、デフォルトでFileVaultキーは保持されます。キーが破棄された場合、スタンバイモードの解除時にパスワードの入力が求められます。（値：1 – 破棄、0 – 保持）

destroyfvkeyonstandby、その他の環境変数の現在の状況を特定するには、次のコマンドを実行します。

```
# pmset -g
```

このコマンドの結果は、以下のようになります。

```
bash-3.2# pmset -g
System-wide power settings:
 DestroyFVKeyOnStandby          0
Active Profiles:
Battery Power           -1
AC Power                -1*
Currently in use:
 standbydelay         4200
 standby              0
 womp                 1
 halfdim              1
 hibernatefile        /var/vm/sleepimage
 gpuswitch            2
 sms                  1
 networkoversleep     0
 disksleep            10
 sleep                0
 hibernatemode        3
 ttyskeepawake        1
 displaysleep         60
 acwake               0
 lidwake              1
```

ファームウェアパスワード

OS Xシステムは、現在のファームウェア設定を無効にして、特定のシステムでファームウェアに予期しない変更を加えることを防ぐためのパスワードの使用をサポートします。これは、ハードドライブ上にインストールされている項目の変更には適用されません。このファームウェアパスワードは、多くの場合、厳格な管理下にあるユーザーが代替システムボリュームから起動できないようにしたり、「キャッチキー」を使用して起動プロセスのフローを変更（シングルユーザーモードへの起動など）できないようにしたりするために使用されます。また、組織で許可されない場合、未承認ユーザーが非表示の復元パーティションに起動することを防ぎます。ファームウェアパスワードは、FireWireなどのインターフェイス経由の ダイレクトメモリアクセス（DMA）も防止します。ターゲットディスクモードではDMAを必要とするため、ファームウェアパスワードを使用するとシステム上でターゲットディスクモードを使用できなくなります。

ファームウェアパスワードを知っている承認済みユーザーが、起動時にキーボードでOptionキーを押したままにして、プロンプトに従ってパスワードを入力し、システムの「ブートピッカー」インターフェイスを使って別の起動ボリュームを選択できます。

この操作により、オリジナルの起動ボリュームにさまざまな変更（ディスク修復ツールを実行する、法的な目的のために暗号化ボリュームへのアクセスをロック解除するなど）を加えることができるようになります。

ファームウェアパスワードはホストコンピュータに付属するため、1つのシステムから別のシステムに暗号化ドライブを移動する場合、ファームウェアパスワードは付随しません。ただし、ターゲットディスクモードを使って別のコンピュータからボリュームをマウントしようとする場合は、ターゲットシステムからボリュームをマウントする前にファームウェアパスワードを入力する必要があります。

Boot Camp

Boot Campは、サポートされるApple製ハードウェアでMicrosoft Windowsの標準実行を可能にするAppleテクノロジーです。すべての新しいMacで、Boot Campという内蔵ユーティリティを使って、Windowsをインストールして、直接ディスクパーティションから同等の速度で実行できます。設定は簡単で、WindowsはOS X起動パーティションとは完全に異なるパーティションにあるため、Macファイルにとっても安全です。Boot Campを使ってWindowsをインストールすると、ユーザーはOS XまたはWindowsのいずれかにMacを起動できます。

Microsoft Windowsと、Windows用のサードパーティFDEのソリューションには、CoreStorageの管理下にあるボリュームを解釈および利用する機能がありません。これにより、FileVault 2 FDEテクノロジーを使用するOS Xシステム上では、Boot CampとWindowsを使用できなくなります。

代わりに、複数のオペレーティングシステムを同時に実行している（Apple製ハードウェア上でOS XとWindowsを使用している場合など）組織では、VMwareやParallelsといった仮想化ソフトウェアを使ってWindowsをインストールできます。

Boot Campと、Apple製ハードウェア上でのWindowsの実行に関する詳細は、OS X互換性ウェブページ、およびBoot Campサポートページを参照してください。

- http://www.apple.com/jp/macosx/what-is/compatibility.html
- http://www.apple.com/jp/support/bootcamp/

2要素認証

前述の通り、FileVault 2（FDE）を使用すると、EFIプリブート認証プロセスの一部として初期認証が行われます。OSに依存するサービスはOSの実行が必要となるため、起動段階の初期段階ではこれらのサービスを読み込むことができません。つまり、パスワードによる認証以外の認証方法は、この時点ではサポートされないことになります。

スマートカードやワンタイムパスワード（OTP）など、その他の2要素認証方法をサポートするには、厳しく制限された環境でEFIを実行することによって、これらのサービスをさらに開発することが必要となります。組織が認証および暗号化ストレージへのアクセスのロック解除のためにスマートカードを使用する必要がある場合は、コンテナベースのレガシーFileVaultの使用について詳しく検討してみることが推奨されます。

レガシーFileVaultと、スマートカードのサポートに関する詳細は、
http://www.apple.com/jp/supportで検索して参照してください。

付録B：FileVault 2プロセスの流れ

ユーザーアクセスの流れ

1. ユーザーがデバイスの電源を入れる
2. EFI
   - 2.1. 起動ボリュームから承認済みFDEユーザーの情報を読み込む
   - 2.2. EFIベースのログインに、アイコンと名前で承認済みユーザーが表示される
   - 2.3. ユーザーを選択した場合はパスワード認証が必要
3. ユーザー
   - 3.1. アカウントパスワードを入力する
4. FileVault
   - 4.1. PBKDF2を使ってパスワードを鍵に変換する
     - 4.1.1. PBKDF2—RSAパスワードベースの鍵派生関数
   - 4.2. CoreStorageメタデータから取得したユーザーバンドルにあるKEK鍵のロック解除によりパスワードを検証する
   - 4.3. 成功は、KEK鍵が正常にWrap解除されたことを示す
5. OSカーネルが読み込まれる
6. 後でカーネルを取得できるように、AppleKeyStoreに起動パラメータを保存する
   - 6.1. 取得したKEKを使ってVEKをWrap解除する
   - 6.2. 認証済みユーザーを特定するトークン
   - 6.3. ユーザーのパスワード
7. カーネルにコントロールを移行する
8. ボリュームをロック解除する
   - 8.1. Apple_CoreStorageパーティションとAppleKeyStoreリファレンス
   - 8.2. Apple_CoreStorageパーティション（起動ボリューム）のロック解除に使用されるVEK
9. オペレーティングシステムが起動する
   - 9.1. システムが通常どおりルートボリュームを検出する
   - 9.2. ログイン
     - 9.2.1. ユーザーがプリブート時に入力したパスワード転送を試みる
       - 9.2.1.1. 権限system.login.consoleで、認証データベース /etc/authorizationで参照した認証メカニズムエントリ builtin:forward-login,privilegedでパスワード転送を有効にする
     - 9.2.2. ディレクトリサービスがユーザー／パスワードを認証する
     - 9.2.3. ユーザーのアクセスが許可され、個人のデスクトップが表示される

付録C：補足資料

関連記事

FileVault 2の設定と使用については、Appleサポートウェブサイトからさまざまな記事を参照できます。以下の内容を含む詳細については、apple.com/jp/support/を参照してください。

- OS X：FileVault 2 について
- OS X Lion：FileVault 2 と Lion 復元機能を使う
- Lion 復元ディスクアシスタント
- MacBook Air (Original), MacBook Air (Late 2008), and MacBook Air (Mid 2009)：紛失した EFI ファームウェアパスワードを回復する
- Mac OS X：シングルユーザモードまたは verbose モードで起動する方法

関連ウェブページ

- OS Xの復元機能があなたのMacを数クリックで元通りに。

セキュリティ設定ガイド

Appleは、Macセキュリティを強化するためのその他のベストプラクティス、および米国の国家安全保障局（NSA）、国立標準技術研究所（NIST）、国防情報システム局（DISA）など世界的な評価の高いセキュリティ組織との長年にわたるコラボレーションから生まれた詳細のガイダンスを提供しています。Apple製品に関する最新のガイダンスについては、www.apple.com/support/security/guides（英語）を参照してください。

トレーニングと認定資格

Apple公認トレーニングセンターでは、OS X、OS X Server、その他のAppleソリューションのエンタープライズ環境への統合、計画、管理に関心を持つプロフェッショナル向けに幅広いITトレーニングと認定資格を提供しています。インストラクター主導のコースでは、実践的で現実的なラボと演習を取り入れたデモや講義で、ITプロフェッショナルのための包括的なトレーニングを実施しています。Appleのトレーニングと認定資格に関する詳細は、http://www.apple.com/jp/training/を参照してください。

8/17/12