ESET Full Disk Encryption
機能紹介資料

第11版

2025年5月

キヤノンマーケティングジャパン株式会社

0 目次

1 はじめに（本資料について）

本資料は暗号化製品「ESET Full Disk Encryption」の機能を紹介した資料です。

- 本資料で使用している画面イメージは使用するOSにより異なる場合があります。また、今後画面イメージや文言が変更される可能性があります。
- ESET PROTECTソリューションではクライアントOSおよびサーバーOSの端末に導入する プログラムとしてWindows、Mac、Linux、Android OS向けのプログラムをご使用いただけます。 また、上記のプログラムを管理するセキュリティ管理ツールをご使用いただけます。各プログラムの機能紹介は別資料でご用意しています。
- ESET Full Disk Encryptionのご利用には、クラウド型セキュリティ管理ツールであるESET PROTECT、または、オンプレミス型セキュリティ管理ツールであるESET PROTECT On-Premでの管理が必要です。
- Windowsは、米国Microsoft Corporationの、米国、日本およびその他の国における登録商標または商標です。
- macOSは、米国およびその他の国で登録されている Apple Inc. の商標です。

ESET Full Disk Encryption（EFDE）とは

2 ESET Full Disk Encryption（EFDE）とは

(1)EFDEとは

クライアント端末のディスク全体、またはブートディスク(※)を暗号化します。暗号化実施後、クライアント端末にはプリブート認証が付与されるため、端末の紛失・盗難時の情報漏洩対策を行うことができます。また、 ESET PROTECTソリューションのセキュリティ管理ツールであるESET PROTECT(EP)、ESET PROTECT on-prem(EP on-prem)を使用して、各クライアント端末の暗号化状況の確認や復号、プリブート認証パスワードの回復などを行うことができます。

持ち出し端末の情報漏洩対策

セキュリティ管理ツールによる一元管理

※ブートディスク…Windowsのブートドライブとして使用される物理ディスクです。同一ディスク内にWindowsのブートドライブとその他のドライブが存在する場合は、そのディスク全体が暗号化されます。

2 ESET Full Disk Encryption（EFDE）とは

(2)EFDEの特長

1. **ESET Full Disk Encryptionの強固な暗号化**
   EFDEはAES256を使用したソフトウェアでの暗号化、または、OPAL2.0準拠の自己暗号化ドライブを使用したハードウェアでの暗号化が可能なため、高い暗号化強度を実現しています。さらに、暗号化キー保護に対するセキュリティ強化として、Trusted Platform Module 2.0（TPM2.0）の使用も可能です。

2. **セキュリティ管理ツールを使用した一元管理**
   EFDEはESET PROTECTソリューションによるウイルス・スパイウェア対策プログラムと同一のセキュリティ管理ツールで一元管理が可能です。EFDEの展開や暗号化状況の確認だけではなく、ポリシーやタスク、レポート機能を使用した柔軟な管理が可能です。

3. **セキュリティ管理ツールを使用したリカバリー対応**
   ユーザがEFDEのプリブート認証パスワードを忘れてしまった場合や、Windowsが起動しなくなった場合は、セキュリティ管理ツールを使用した迅速なプリブート認証パスワードの回復や、セキュリティ管理ツールで作成したリカバリーデータを元に用意した復号USBドライブを使用することで、ディスクの復号を行うことができます。

ESET Full Disk Encryptionの構成について

3 ESET Full Disk Encryptionの構成について

(1)システム要件/動作環境

ESET Full Disk Encryptionの利用にあたっては、以下の環境が必要です。

①クライアント端末のOSがMicrosoft Windows10以上であること
②クライアント端末のハードウェアはUEFIと物理キーボードを利用していること
③WDDM 1.0以上のドライバーを搭載したDirectX 9グラフィックスデバイスの利用していること
④セキュリティ管理ツールが構築されていること
⑤セキュリティ管理ツールでエンドポイントの管理が行われていること
⑥セキュリティ管理ツールがインターネット接続が可能であるこ
※32bit版のOSはEFDE2.0以降ではサポートされません。
※TPM2.0やOPAL2.0を使用した暗号化もサポートされています。
※オフライン環境でクライアントにEFDEをインストールするときはオールインインストーラーでのみインストール可能です。

プログラム名		
ESET Endpoint アンチウイルス（EEA）	WindowsクライアントOS向け　ウイルス・スパイウェア対策プログラム	○(必須ではない)
ESET Endpoint Security（EES）	WindowsクライアントOS向け　総合セキュリティプログラム	○(必須ではない)
ESET PROTECT（EP）または ESET PROTECT on-prem（EP on-prem）	セキュリティ管理ツール	○(※)
ESET Management エージェント（EMエージェント）	クライアント管理用のエージェントプログラム	○

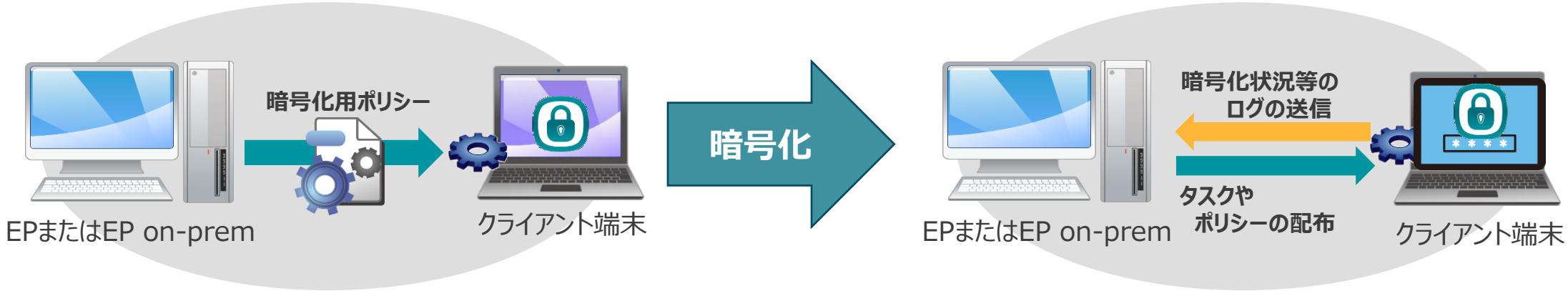
※サポート対象のセキュリティ管理ツールのバージョンは、下記の[要件とサポート対象の製品]よりご確認ください。
https://eset-info.canon-its.jp/files/user/pdf/support/EFDE_support_document_for_online_help.pdf

3 ESET Full Disk Encryptionの構成について

(2)コンポーネント

ESET Full Disk Encryptionは以下のコンポーネントから構成されています。

コンポーネント	
ESET Full Disk Encryption（EFDE）	クライアント端末にインストールし、暗号化を行うプログラムです。暗号化後はクライアント端末の起動時にプリブート認証パスワードの入力が必要になります。
ESET PROTECT（EP）または ESET PROTECT on-prem（EP on-prem）	タスク機能によるクライアント端末へのEFDEのインストールをはじめ、ポリシー機能を使用したクライアント端末の暗号化/復号や暗号化状況の確認、プリブート認証パスワードの回復などが可能です。
ESET Management エージェント（EMエージェント）	EPまたはEP on-premで作成した暗号化/復号のポリシーやクライアントタスクをクライアント端末へ配布します。また、クライアント端末の暗号化状況などの情報をEPまたはEP on-premへ送信します。



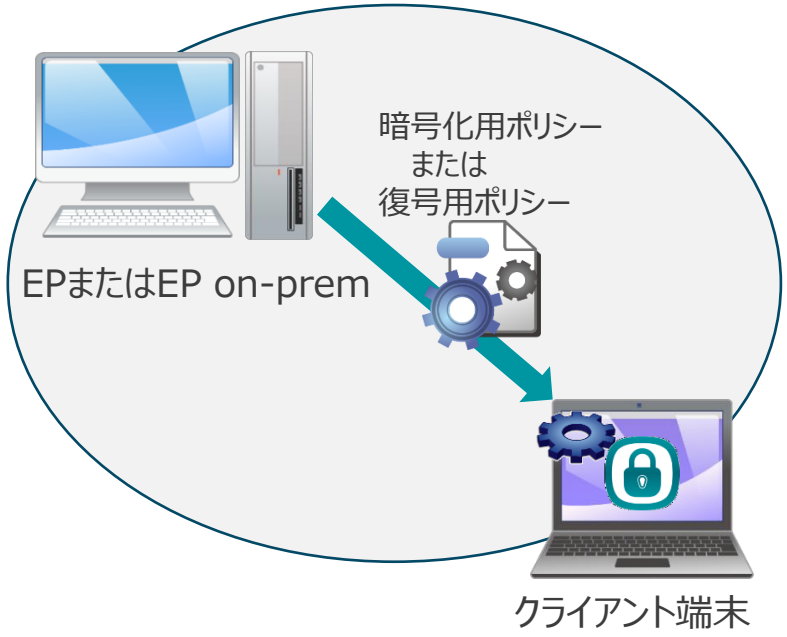
ESET Full Disk Encryptionの機能について

4 ESET Full Disk Encryptionの機能について

(1)ディスクの暗号化と復号

EFDEではセキュリティ管理ツールESET PROTECTまたは、ESET PROTECT on-premのポリシー機能を使用することで、リモートでクライアント端末のディスクの暗号化および復号を行うことができます。V2.1以降では、使用済み領域のみを暗号化/復号することも可能です。クライアント端末の暗号化/復号はユーザー自身で行うことはできません。ディスクが暗号化されたクライアント端末は起動時にプリブート認証パスワードの入力が必要になります。

※暗号化実施前に再起動を行い、安全に暗号化が行われるセーフスタートを実施しています。
※パーティション単位の暗号化には対応していません。



暗号化開始

暗号化中のEFDEのユーザーインターフェース

4 ESET Full Disk Encryptionの機能について

(1)ディスクの暗号化と復号(プリブート認証画面)

EFDEにより暗号化を行うと、端末の起動後、以下の通りプリブート認証画面が表示されるようになります。プリブート認証パスワードを入力するとOSが起動するようになります。

パスワードを入力

OS起動画面

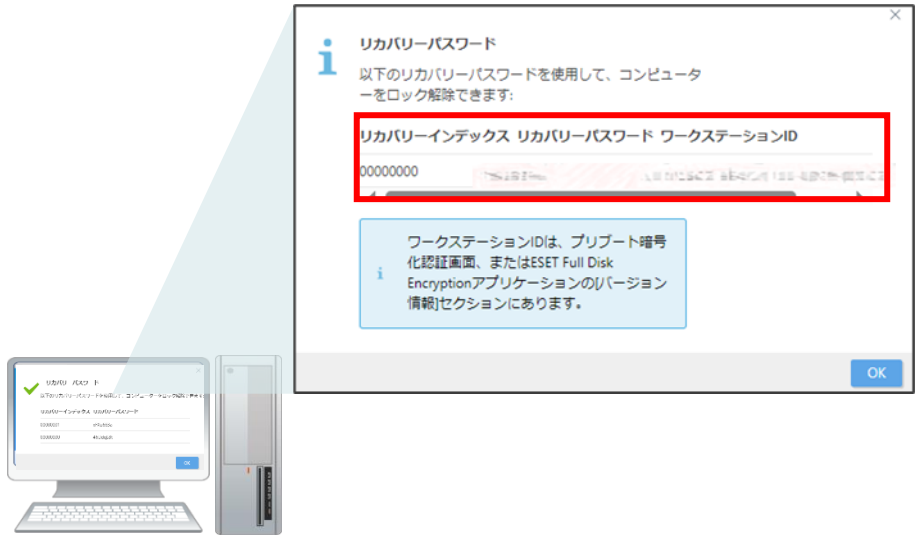
4 ESET Full Disk Encryptionの機能について

(2)プリブート認証パスワードの管理

プリブート認証パスワードを忘れてしまった場合は、セキュリティ管理ツールで確認できるリカバリーパスワードをクライアント端末で入力することでプリブート認証パスワードを回復（再設定）することができます。

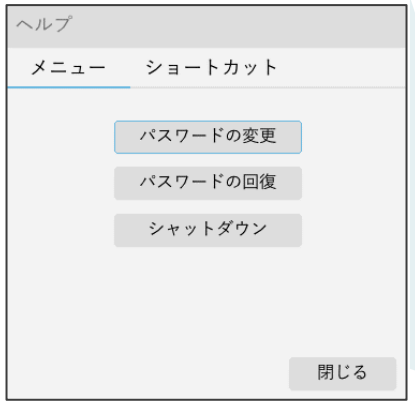
※ポリシーで設定したパスワード期限が切れた場合やクライアントタスクを利用することでユーザ自身でパスワードを変更することが可能です。

※プリブート認証パスワードはTPMやOPALの使用に関わらず、パスワードによる認証のみです。



EP または EP on-prem

リカバリー
パスワードを共有



プリブート認証
パスワードの変更

クライアント端末

4 ESET Full Disk Encryptionの機能について

(3)リカバリーデータを使用した復号

Windowsが起動できなくなり、ディスクの復号が行えなくなってしまった場合には、セキュリティ管理ツールで作成したリカバリーデータをUSBブートすることでディスクの復号を行うことできます。

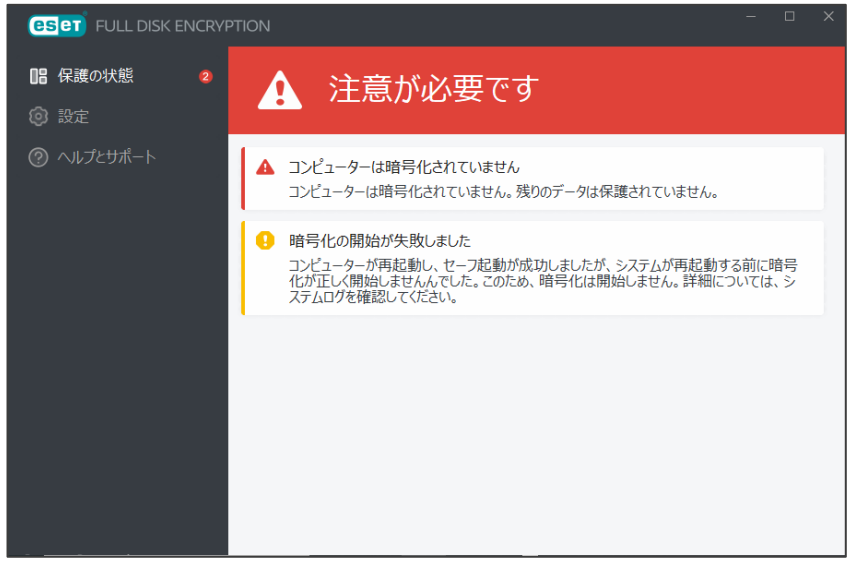
No.	手順	備考
1	セキュリティ管理ツールでリカバリーデータを作成してダウンロードする	セキュリティ管理ツールからダウンロード
2	セキュリティ管理ツールで暗号化回復ユーティリティをダウンロードする	セキュリティ管理ツールからダウンロード
3	手順「1」と手順「2」でダウンロードしたリカバリデータと暗号化ユーティリティで復号USBドライブを作成する	-
4	手順「3」で作成した復号USBドライブを使用してPCを起動し、ディスクを復号する	USBドライブから起動する際、「セキュアブート」を無効にする（※）

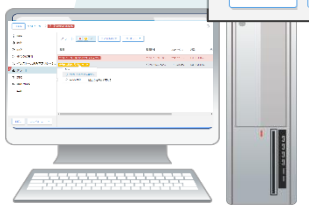
※本機能を利用する場合、UEFIの設定で「セキュアブート」を無効にする必要があります。

4 ESET Full Disk Encryptionの機能について

(4)Webコンソールからの暗号化再試行

クライアント側で暗号化に失敗してしまった場合、セキュリティ管理ツールのWebコンソールから暗号化の再試行が可能です。





EP または EP on-prem

失敗した暗号化を再試行

暗号化の再試行

4 ESET Full Disk Encryptionの機能について

(5)リカバリーデータの移行とバックアップ

EFDEを使用した管理端末の暗号化回復データとパスワードを含む暗号化されたバックアップファイルエクスポートし、他のEPまたはEP on-premにインポートすることで、復号の必要なく端末を他のEPまたはEP on-premに移行できます。

4 ESET Full Disk Encryptionの機能について

(6)セキュリティ管理ツールで可能なこと(クライアントタスク一覧)

セキュリティ管理ツールでは以下のクライアントタスクが使用できます。

クライアントタスク名	説明
FDEログインパスワードのブロック	プリブートログインが無効になります。パスワードリカバリーを使用し、アクセスを復元して新しいパスワードを設定することでシステムを起動できます。あるいは、リカバリーツールを使用して、システムを復元することもできます。
FDEログインパスワードのワイプ	パスワードリカバリー情報を含むパスワード暗号化情報がクライアント端末から削除されます。システムは起動できず、リカバリーツールを使用した方法でのみ復号できます。
FDEログインパスワードの無効化	ユーザーは、クライアント端末にインストールされたEFDEで、パスワードを変更するように指示されます。パスワードが変更されないか、ユーザーがログオンしていない場合、クライアント端末のプリブートログイン中にパスワードを変更する必要があります。
FDE認証を一時停止する	FDE認証を一時停止すると、ユーザーがパスワードを入力しなくても、クライアント端末を自動的に起動できます。（長期的にFDE認証を無効化する場合は、ポリシーでも設定が可能です。）
FDE認証を再開する	FDE認証を再開すると、元のプリブート認証動作が復元され、ユーザーはシステム起動時にパスワードの入力が必要になります。
新しいFDEリカバリーパスワードの生成	新しいFDEリカバリーパスワードを生成します。生成後は既存のリカバリーパスワードは利用できなくなります。

4 ESET Full Disk Encryptionの機能について

(6)セキュリティ管理ツールで可能なこと

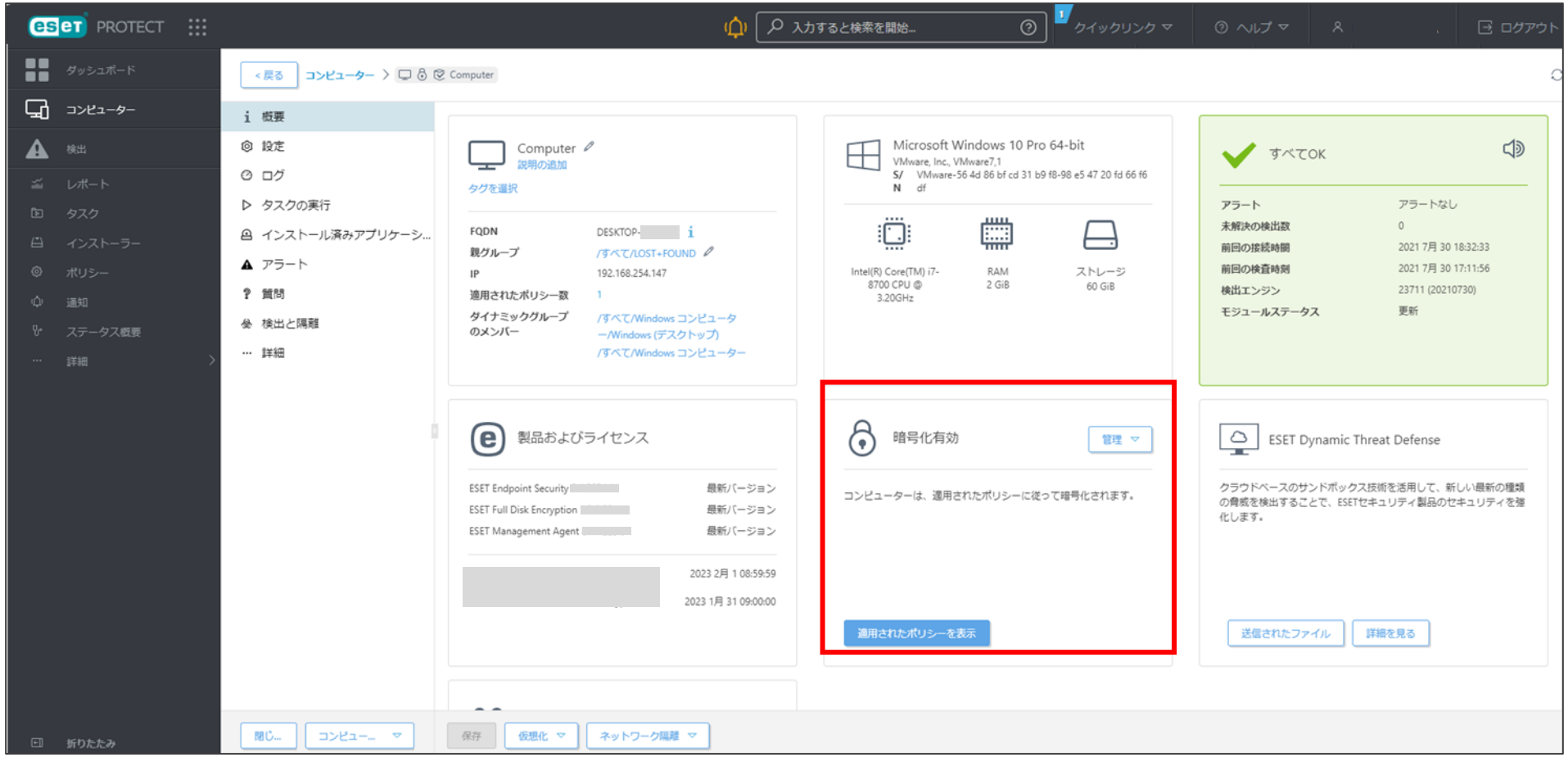
EFDEの利用には、 ESET PROTECTソリューションのセキュリティ管理ツールであるESET PROTECTまたはESET PROTECT on-premが必須です。セキュリティ管理ツールでは主に以下の機能が使用可能です。

項目	説明
暗号化状況の確認 （P18にイメージ画像があります）	セキュリティ管理ツールの「コンピューター」欄の詳細情報より確認可能です。また、レポートテンプレートを作成することで、クライアント端末の暗号化状況についてレポートを作成することが可能です。
EFDEの設定変更	セキュリティ管理ツールのポリシー機能を使用することで、暗号化または復号をはじめ、プリブート認証パスワードの期限や文字数などのパスワードポリシーを設定することができます。
リカバリーパスワードの確認や リカバリーデータの作成	クライアント端末のプリブート認証パスワードの回復のためのリカバリーパスワードや、ディスクの復元を行うことができるリカバリーデータの作成が可能です。
暗号化されていない端末の グルーピング	セキュリティ管理ツールで動的グループのルールを作成することで、EFDEをインストールしているのに暗号化を行っていない端末をグルーピングすることが可能です。
クライアントタスク （P16にクライアントタスク一覧があります）	（例）【FDEログインパスワードの無効化タスク】 強制的にプリブート認証パスワードを変更させることができます。
	（例）【FDE認証を一時停止するタスク】 クライアント端末のプリブート認証を一時的に無効にすることができます。
EFDEのインストール	セキュリティ管理ツールでクライアント端末の管理を行っている場合は、タスク機能を使用しリモートでEFDEのインストール/アンインストールが可能です。また、セキュリティ管理ツールでインストーラーを作成することで、EFDE/EMエージェント/EESまたはEEAを同時にインストールすることが可能です。

4 ESET Full Disk Encryptionの機能について

(6)セキュリティ管理ツールで可能なこと（参考）

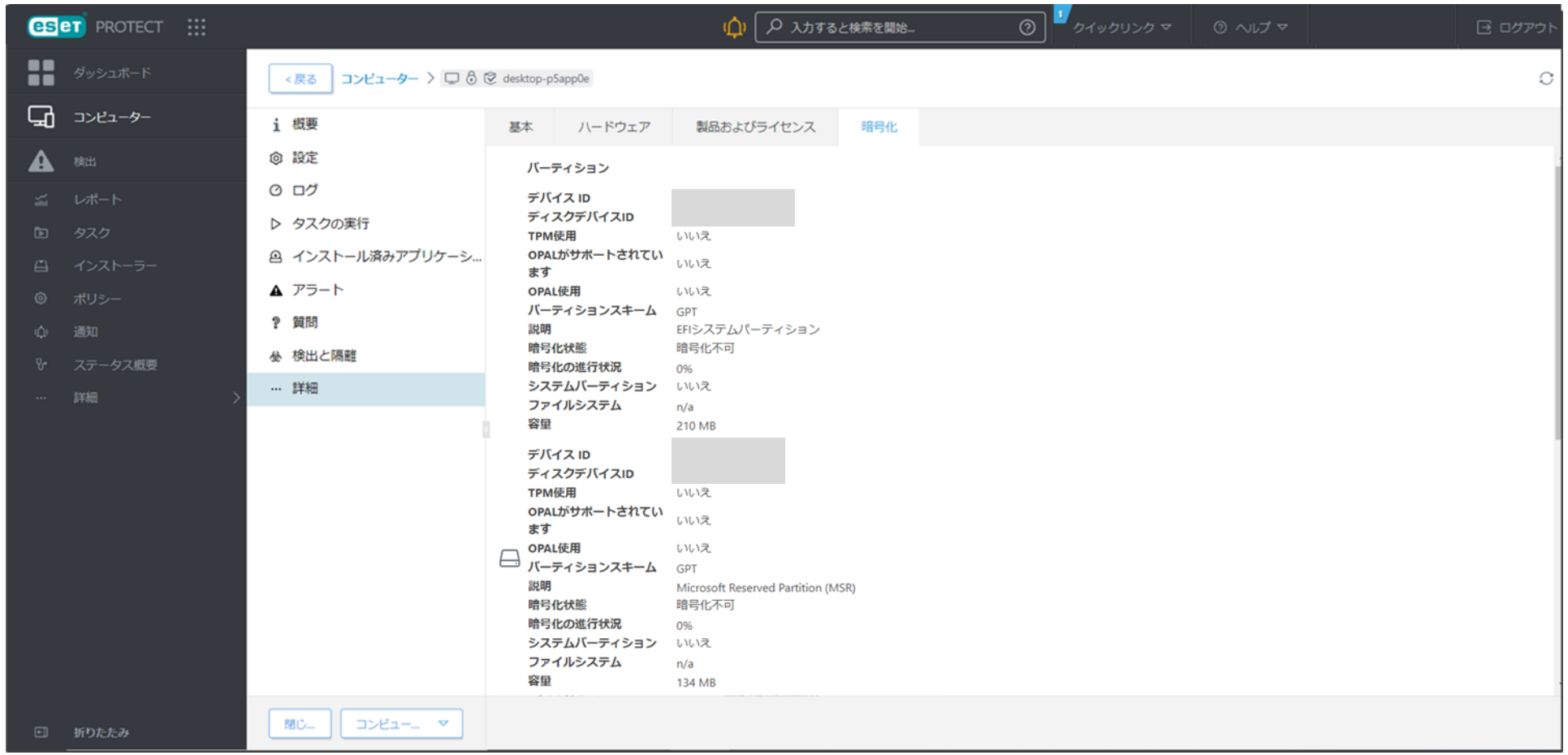
コンピューターの詳細(暗号化確認画面)



4 ESET Full Disk Encryptionの機能について

(6)セキュリティ管理ツールで可能なこと（参考）

コンピューターの詳細(暗号タブ)



5 導入・展開方法について

(6)セキュリティ管理ツールで可能なこと（参考）

「ESET Full Disk Encryption」ポリシーにて、シングルサインオン(SSO)の設定ができます。
「シングルサインを有効にする」を有効にすると、WindowsパスワードによるSSOによるログインができるようになります。
※Microsoft Azureドメインはサポートしていません。
※標準のWindows ログインパスワードのみをサポートしています。
　(Windows Hello、PIN、または Microsoft アカウントはサポートしていません)

Windows パスワードでログイン

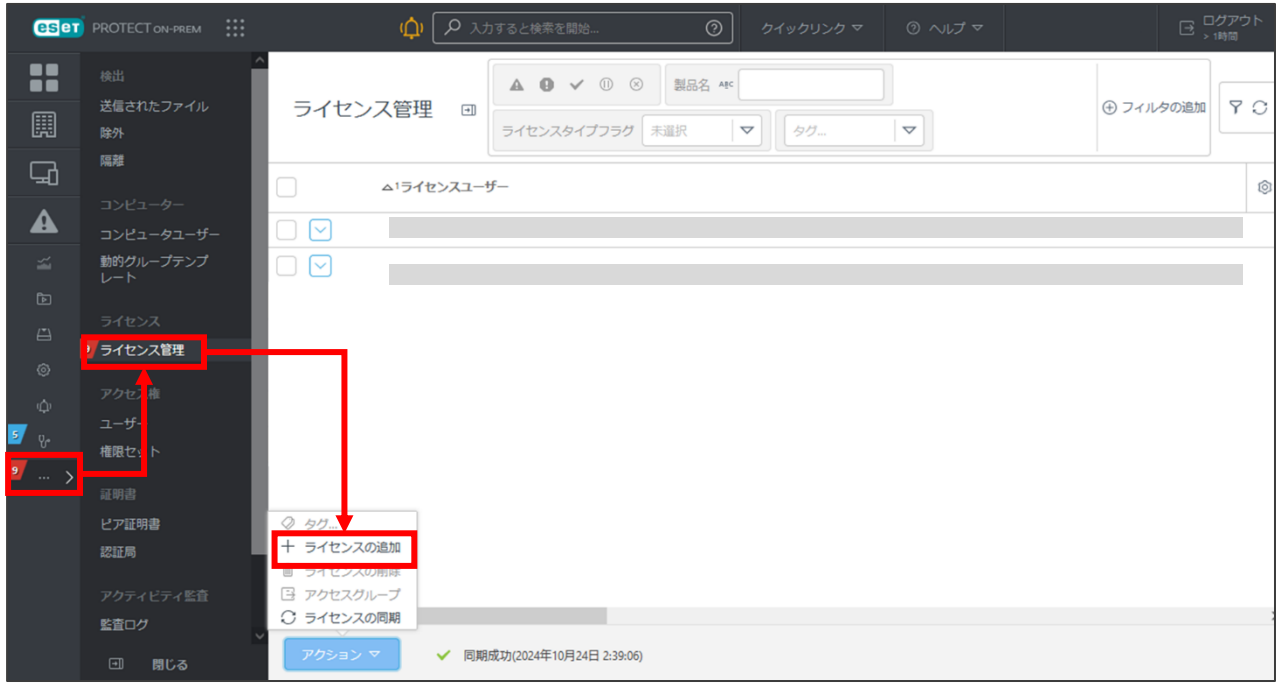
導入・展開方法について

5 導入・展開方法について

EFDEの導入・展開方法（1）

セキュリティ管理ツールにログインしEFDEのライセンス（製品認証キー）を登録します。
※ライセンスを登録することでセキュリティ管理ツール上でEFDE用の項目が表示されるようになります。
※製品認証キーはユーザーズサイトで確認可能です。
※EPをご利用の場合はESET Business AccountまたはESET PROTECT Hubにてライセンスの追加を実施ください。

EP on-premのライセンス管理画面



5 導入・展開方法について

EFDEの導入・展開方法（2）

セキュリティ管理ツールでEFDE用のポリシーを作成します。暗号化を有効にする設定やTPM、OPALに関する設定、プリブート認証パスワードのパスワードポリシーなどの設定が可能です。ポリシーはライブインストーラー(EPの場合)やオールインワンインストーラー(EP on-premの場合)に組み込んだり、コンピューターやグループに対し配布すること可能です。

セキュリティ管理ツールのポリシー作成画面

5 導入・展開方法について

EFDEの導入・展開方法（3）

EFDEをクライアント端末に展開します。セキュリティ管理ツールでクライアント端末を管理済みかどうかで展開方法が変わります。
※インストール後、端末の再起動が必要です。

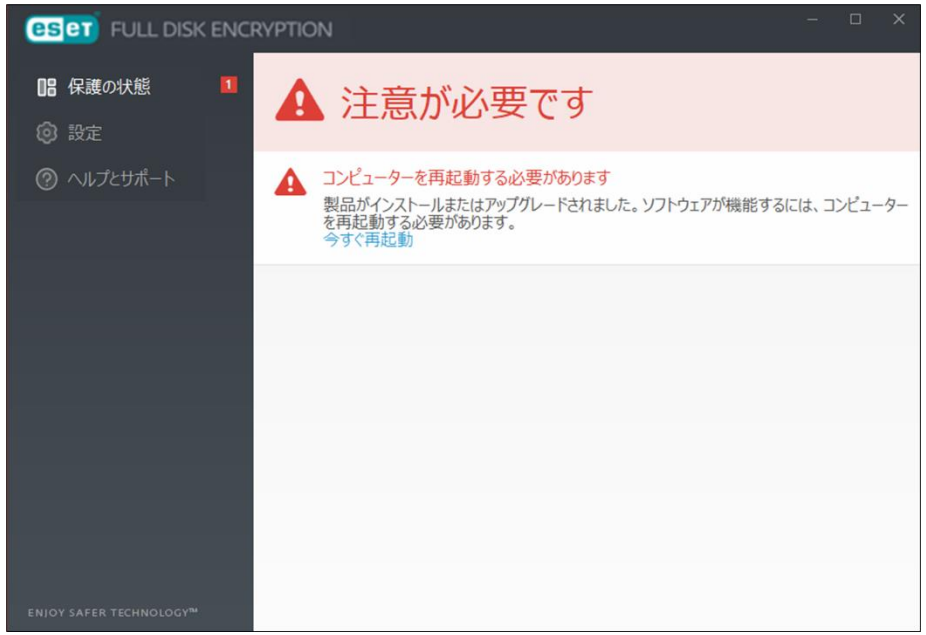
【クライアント端末を管理している場合】

ソフトウェアインストールタスクを使用して、
リモートでEFDEをインストールします。
※ネットワーク負荷を考慮し、グループごとにインストールする等のご対応をお願いいたします。

【クライアント端末を管理していない場合】

セキュリティ管理ツールで作成したインストーラーを使用します。EPではライブインストーラー、 EP on-premではオールインワンインストーラーを使用してEFDEとEMエージェントをインストールします。 EEA/EESも同時にインストール可能です。
※オフライン環境ではこちらの方法でのみ展開できます。

EFDEインストール直後のGUI



5 導入・展開方法について

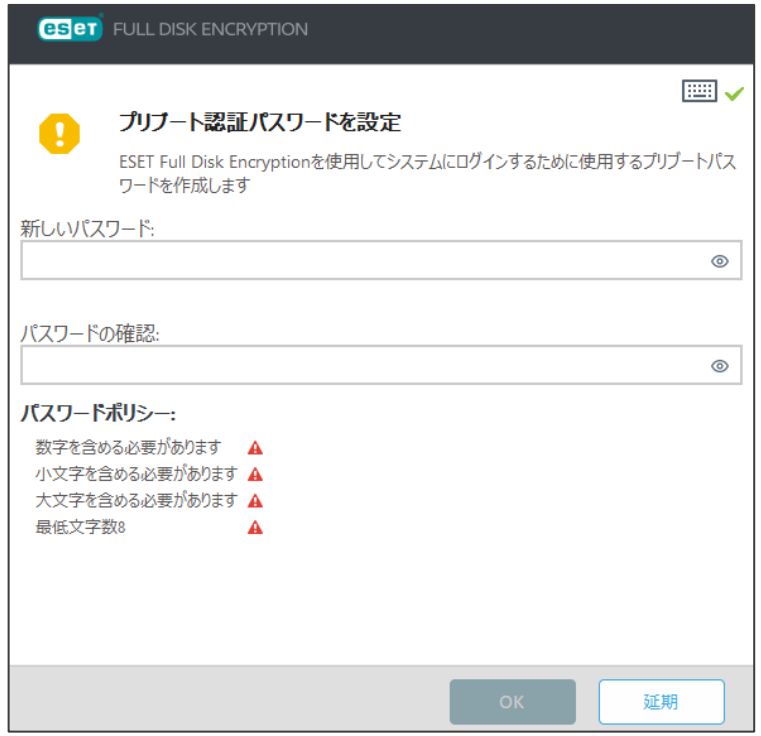
EFDEの導入・展開方法（4）

セーフスタートのための再起動後、ユーザ自身がプリブート認証パスワードを作成します。
【手順２】で作成したパスワードポリシーを満たす必要があります。

セーフスタートのための再起動待機画面

再起動

プリブート認証パスワード設定画面



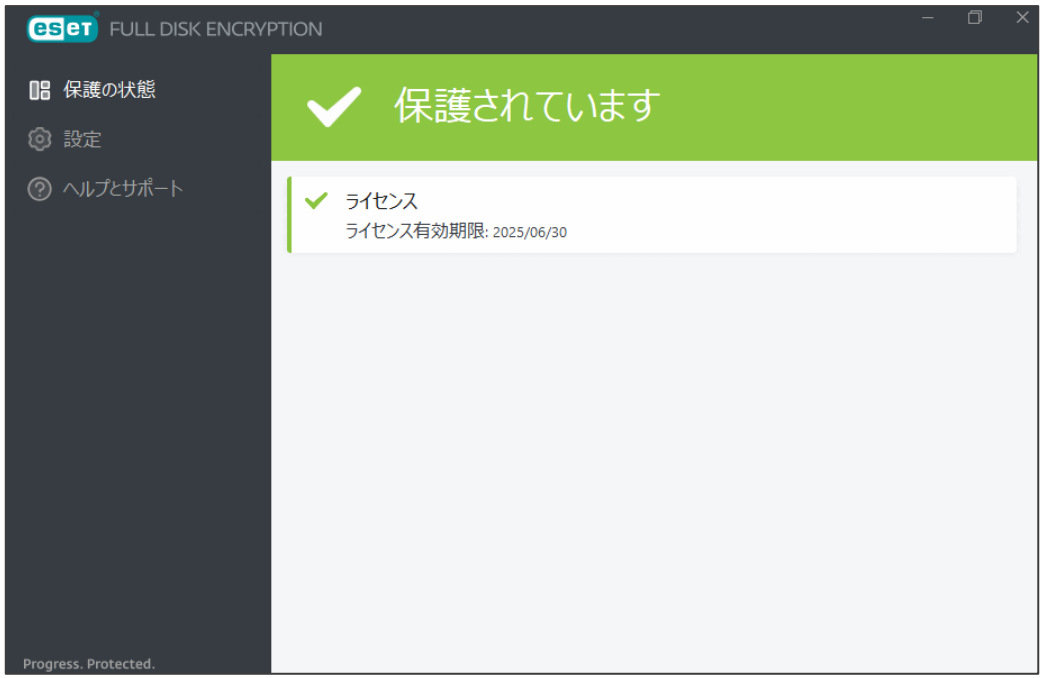
5 導入・展開方法について

EFDEの導入・展開方法（5）

ユーザによるパスワード設定後、HDD/SSDの暗号化が開始されます。
※暗号化中でもクライアント端末のシャットダウンや再起動は可能です。

暗号化進行中のGUI

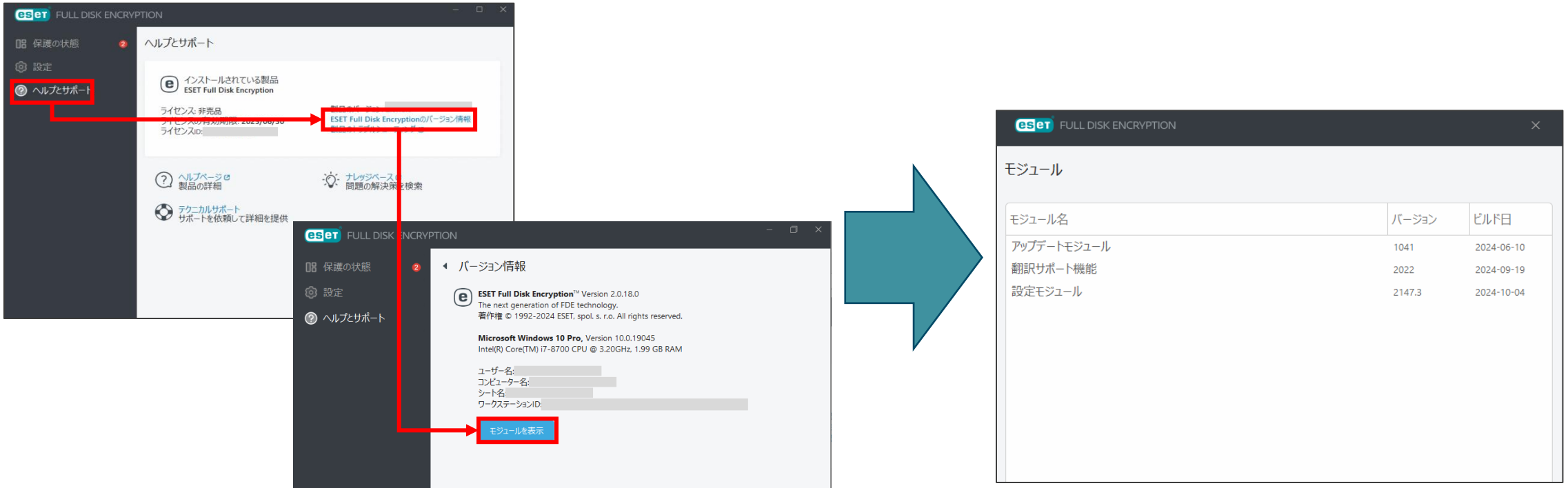
暗号化完了時のGUI



5 導入・展開方法について

EFDEの導入・展開方法（参考）

「ヘルプとサポート」内の「ESET Full Disk Encryptionのバージョン情報」>「モジュールを表示」から、EFDEのモジュール情報が確認できます。



導入時の注意事項について

6 導入時の注意事項について

EFDE導入時の注意事項

- クライアントPCがマルチブートで構成されている場合、ESET Full Disk Encryptionの導入はできません。
- クライアントPC内のストレージがソフトウェアRAID構成の場合、ESET Full Disk Encryptionの導入はできません。
- クライアントPCでBitLockerおよびBitLocker機能を利用したデバイスの暗号化機能を利用してる場合、ESET Full Disk Encryptionの導入はできません。
- OPAL以外の暗号化機能付きストレージはESET Full Disk Encryptionで暗号化することはできません。
- 他社製暗号化ソフトウェアが導入されている場合、ESET Full Disk Encryptionの導入はできません。
- BIOSファームウェアのあるクライアントPCへのESET Full Disk Encryptionの導入はサポートされていません。
- 仮想化された環境へのESET Full Disk Encryptionの導入はサポートされていません。
- ESET Full Disk Encryption for Macはサポートしていません。

EFDE導入時の注意事項の詳細についてはWebページをご確認ください。
https://eset-info.canon-its.jp/business/efde/spec.html
https://eset-info.canon-its.jp/files/user/pdf/support/EFDE_support_document_for_online_help.pdf