ESET Full Disk Encryption 機能紹介資料

第11版

2025年5月

Canon 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)
- 2. ESET Full Disk Encryption (EFDE) とは
 - (1) EFDEとは
 - (2) EFDEの特長
- 3. ESET Full Disk Encryptionの構成について
 - (1) システム要件/動作環境
 - (2) コンポーネント
- 4. ESET Full Disk Encryptionの機能について
 - (1) ディスクの暗号化と復号
 - (2) プリブート認証パスワードの管理
 - (3) リカバリーデータを使用した復号
 - (4) Webコンソールからの暗号化再試行
 - (5) リカバリーデータの移行とバックアップ
 - (6) セキュリティ管理ツールで可能なこと
- 5. 導入・展開方法について
- 6. 導入時の注意事項について



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。



※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。





(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。

クライアント端末のOSがMicrosoft Windows10以上であること
 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
 WDDM 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
 セキュリティ管理ツールが構築されていること
 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
 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	፟ጛፚ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	O(*)
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	0

※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





(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。



(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。





10





(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。

ESET FULL DISK ENCRYPTION		
システムの起動 パスワード ● F5 ログイン	パスワード を入力	OS起動画面



12

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。 リカバリーパスワード ヘルプ 以下のリカバリーパスワードを使用して、コンピュータ ーをロック解除できます: メニュー ショートカット リカバリーインデックス リカバリーバスワード ワークステーションID パスワードの変更 AUNUSCI ABACA IN ADDR. パスワードの回復 フリブート認証 ワークステーションIDは、プリブート暗号 シャットダウン 化認証画面、またはESET Full Disk リカバリー パスワードの変更 Encryptionアプリケーションのバージョン 情報」セクションにあります。 パスワードを共有 閉じる * * * * EP または EP on-prem クライアント端末





(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。



©Canon Marketing Japan Inc.



(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。

	< 戻る コンピューター > 8 0 0	desktop-r6bpbtv				C		rion – 🗆 ×
	i 概要 ③ 設定	アラート 🛕 🔍 ノイルタの追加 ブリセット マ]				□: 保護の状態2◎: 設定	▲ 注意が必要です
	② ログ	問題	問題詳細	ステータ ス	製品	٢	⑦ ヘルプとサポート	▲ コンピューターは暗号化されていません
	▶ タスクの実行	コンピューターは暗号化されていません	コンピューターは	セキュリテ	ESET Full Dis			コンピューターは暗号化されていません。残りのデータは保護されていません。
		暗号化の開始が失敗しました	ポリシーによると	セキュリテ	ESET Full Dis			9 暗号化の開始が失敗しました
	≟ ▲ アラート	 答告 〇 失敗した暗号化を再試行 〇 						コンピューターが再起動し、セーフ起動が成功しましたが、システムが再起動する前に暗号 化が正しく開始しませんんでした。このため、暗号化は開始しません。詳細については、シ
	? 質問	✓ Webを検索 失敗した暗号化を再試行						ステムログを確認してください。
	◎ 検出と隔離							
		₹				4		
		失敗した暗	音号化を	と再試	行			
EP または EP	on-prem							号化の再試行



(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。





(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。

(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	(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。
(P16にクライアントタスク一覧があります)	(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。

eset



(6)セキュリティ管理ツールで可能なこと(参考)

eset protect :::	コンピューターの	<u>詳細(暗号化確認画面)</u> ゆ ア 入力すると検索を開始… ⑦] ¹ カイックリンク マ ③ へル	プマ & 、⊡ ⊡775ト
ダッシュボード ゴンピューター ゴ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	< 戻る コンピューター 〉 □ ③ ⓒ Computer 版要 ゆ 設定 ログ タスクの実行 インストール済みアプリケーシ… アラート アラート 後出と隔離 後出と隔離 け細 Pin Total and a state of the state of	i i i i i i i i i i i i i i	o 64-bit ¹⁹ f8-98 e5 47 20 fd 66 f6	マラートなし 検出数 0 検出数 0 続時間 2021 7月 30 18:32:33 査時刻 2021 7月 30 17:11:56 ジン 23711 (20210730) ルステータス 更新
	ESET Endpoint Security ESET Full Disk Encryption ESET Management Agent	 	管理 マ つつつ つつつ つうつド の角成を 化します。	ESET Dynamic Threat Defense ペースのサンドボックス技術を活用して、新しい最新の種類 検出することで、ESETセキュリティ製品のセキュリティを弾 ・
ロ 折りたたみ	閉じ… □ンピュー… マ 保存 仮想化 マ ネットワーク隔離 <	7		



- **>** 1 °



(6)セキュリティ管理ツールで可能なこと(参考)

eset protect :::		ログアウト
● ● ダッシュボード	<戻る コンビューター > ロ ⁶ [©] desitop-pSapp0e	C
□ >ピュ-タ-	i 概要 基本 ハードウェア 製品およびライセンス 暗号化	
 ▲ 株田 ゴ レポート ト ケスク ゴ インストーラー ◎ ポリシー ゆ 通知 ♥ ステータス概要 … 詳細 	・ ジェレール ・ ブーク ・ ・ ・	
・ 折りたたみ	容量 134 MB	

©Canon Marketing Japan Inc.



(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)

ESET Full Disk Encryption		Q 入力すると検索を開始	
暗号化オプション 2	- フルディスク暗号化モード	E (0 • 4
パスワードポリシー	○ ● ≁ 暗号化を有効にする		0
ユーザーインターフェース	 ○ ● ✓ 暗号化設定アクションを実行することをユーに再確認するまでの時間(時間) 	Lーザ 4	6
接続	○ ● ∮ 暗号化オプション	すべてのディスク	を暗号化 🖌 🚺
	○ ● ∮ シングルサインオンを有効にする 🛛 🖲	≥ 2.0	0
	シングルサインオン(SSO)が有効な場合、ユーザー ではなく、Windowsポリシーによって強制されま できる」、「パスワードの文字教」、「パスワー し、回復パスワードが生成されるとき、パスワー パスワードの無効化タスクは適用されません。代 ーは次回ログオン時にパスワードを変更する必要	-のパスワード要件は、ESET Full [す。これには、「ユーザーはパス ドの有効期限」のポリシーが含ま ドの文字設定は引き続き適用され わりに、Active Directory内のWinu がある]オプションを使用してくた	Disk Encryption Rワードを変更 れます。ただ れます。また、 dowsの[ユーザ ささい。
	○ ● ∮ FDE認証を無効にする		0



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。

eset		① 入力すると検索を開始… ② ⑦ クイックリンク マ ③ ヘルプ マ ③ ヘルプ マ ③ ○ □ ○ □ ○ □ ○ □	7F
	へ 検出 送信されたファイル 除外	ライセンス管理 □ ライセンス管理 □ ライセンスタイプフラグ 未進択 マ タグ マ	0
	₩# コンピューター コンピュータユーザー	▲157te>スユーザー ✓	0
e 	動的グループテンプ レート ライセンス		
ല ⊚ ഗ	ライセンス管理 アクセン 権		
5 >	ユーザ- 権限セット		
	証明書 ピア証明書 認証局	 	
	アクティビティ監査 <u> 監査</u> ロ グ ~	 ● アクセスグループ ○ ライセンスの周期 	
		アクション マ 同期成功(2024年10月24日 2:39:06)	

<u>EP on-premのライセンス管理画面</u>



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。

ESET Full Disk Encryption	~	Q、入力すると検索を開始	
暗号化オプション	- フルディスク暗号化モード		0 • +
パスワードポリシー	 ● ✓ 暗号化を有効にする 		(
ユーザーインターフェース	○ ● 🔸 使用済み領域のみを暗号化および復号化	(€) ≥ 2.1	
拉注	データを含むディスク領域のみをターゲットにすることで、暗	号化と復号化を高速化します。新しいシステムにのみ推奨されます。	
はない	○ ● ∮ 暗号化設定アクションを実行することをユーザーに再 での時間(時間)	確認するま 🧉 4	
	○ ● 🗲 暗号化オプション	すべてのディスクを暗号化する	~ (
	○ ● 🗲 シングルサインオンを有効にする	€ ≥ 2.0	
	シングルサインオン(SSO)が有効な場合、ユーザーのパスワード ます。これには、「ユーザーはパスワードを変更できる」、「 し、回復パスワードが生成されるとき、パスワードの文字設定! わりに、Active Directory内のWindowsの(ユーザーは次回ログオ	、要件は、ESET Full Disk Encryptionではなく、Windowsポリシーによっ パスワードの文字数」、「パスワードの有効期限」のポリシーが含ま は引き続き適用されます。また、パスワードの無効化タスクは適用さ *ン時にパスワードを変更する必要がある]オプションを使用してくだ;	って強制され れます。ただ れません。代 さい。
	○ ● ∮ FDE認証を無効にする		
	TRUSTED PLATFORM MODULEサポート		
	○ ● ∮ TPMを使用する		(
	TPMの使用を有効にし、Trusted Platform Module (TPM)の所有権 れていないことを確認してください。他のソフトウェアで使用	権を取得します。お客様の責任において、TPMが他のソフトウェアに、 されていると、データが損失する可能性があります。	よって使用さ
	○ ● ≁ TPMモード	可能な場合にはTPMを使用する	~ (

セキュリティ管理ツールのポリシー作成画面



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。



©Canon Marketing Japan Inc.





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。

ESET FULL DISK ENCRYPTION **ESET** FULL DISK ENCRYPTION - IIII 🗸 || 保護の状態 注意が必要です A プリブート認証パスワードを設定 Ω 設定 ESET Full Disk Encryptionを使用してシステムにログインするために使用するプリブートパス ワードを作成します ▲ コンピューターは暗号化されていません 新しいパスワード: コンピューターは暗号化されていません。残りのデータは保護されていません。 0 デバイスを再起動する必要があります 再起動 Safe startを開始して、ハードウェアおよびファームウェアの互換性を開始し、初期化を実行する には、コンピューターの再起動が必要です。 パスワードの確認: \odot 今すぐ再起動 パスワードポリシー: 数字を含める必要があります 小文字を含める必要があります 🗛 大文字を含める必要があります 🗛 最低文字数8 A 延期

セーフスタートのための再起動待機画面

プリブート認証パスワード設定画面





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。

<u>暗号化進行中のGUI</u>

暗号化完了時のGUI

 品 保護の状態 2 3 3 3 5 5 5 5 7 7 7 8 7 7 8 8 7 8 7 8 7 8 7 8 7 8 7 8 7 8 7 8 7 8 7 8 7 8 7 8 7 8 7 8 7 8 7 8 7 8 7 8 7 8 8 7 8 8 7 8 8 7 8 8 8 8 8 9 8 9 8 9 9 9 9 9 9	日 暗号化が進行中です	旧 保護の状態 ③ 設定	✔ 保護されています
⑦ ヘルプとサポート	コンピューターを暗号化しています 処理が開始し、10%未満完了しました 詳細の表示	⑦ ヘルプとサポート	✓ ライセンス ライセンス有効期限: 2025/06/30
ENJOY SAFER TECHNOLOGY™		Progress. Protected.	



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。



バージョン

1041

2022

2147.3

ビルド日

2024-06-10

2024-09-19

2024-10-04

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。 <u>https://eset-info.canon-its.jp/business/efde/spec.html</u> <u>https://eset-info.canon-its.jp/files/user/pdf/support/EFDE_support_document_for_online_help.pdf</u>