

ESET PROTECTソリューション オンプレミス型セキュリティ管理ツール ESET PROTECT V 9 レポート機能紹介資料

> 第1版 2021年12月15日

**Canon** キヤノンマーケティングジャパン株式会社



#### もくじ

#### 1. はじめに

2. レポートとは?

- 3. 運用に役立つレポートテンプレートの紹介
- 4. レポートのスケジュール機能
- 5. レポートテンプレートの作成手順
- 6. 参考情報

#### 1.はじめに(本資料について)



本資料はセキュリティ管理ツールのレポート機能を紹介している資料です。セキュリティ管理ツールに関する機能紹介は別資料 でご用意しています。本資料は、オンプレミス型セキュリティ管路ツールであるESET PROTECT(以降、EP)V9を例に、セキュ リティ管理ツールのレポート機能を紹介しています。

※EP V8以上とEPCではEES/EEA V6.6以下、EFSW V6.5以下を管理することはできません。

フログラム名	略称	備考
ESET PROTECT	EP	オンプレミス型セキュリティ管理ツール ※ESET Security Management Centerの後継
ESET PROTECT Cloud	EPC	クラウド型セキュリティ管理ツール

※セキュリティ管理ツールのバージョンによって管理できるクライアント用プログラムに差異があります。 詳細は以下サポートページをご参照ください。 <u>https://eset-support.canon-its.jp/faq/show/143?site\_domain=business</u>

#### 1.はじめに(本資料について)



- 本資料で使用しているESET製品の画面イメージは使用するバージョン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ございます。
- ESET、NOD32、ThreatSense、LiveGrid、ESET Endpoint Security、ESET Endpoint アンチウイルス、ESET File Security、ESET NOD32アンチウイルス、ESET Security Management Center、ESET PROTECT、 ESET Dynamic Threat Defense、ESET Enterprise Inspector、ESET Full Disk Encryption は、 ESET,spol. s. r. o.の商標です。
- Windows、Windows Server、Microsoft Edge、Internet Explorerは、米国 Microsoft Corporation の米国、 日本およびその他の国における商標登録または商標です。macOS、OS X および iPhone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。



# 2.レポートとは?







クライアントから収集した情報やセキュリティ管理ツールの情報をもとにレポートを作成することができます。 既に定義されているレポートテンプレートは約110種類あり、テンプレートをもとに独自にレポートを作成することもできます。





## 3.運用に役立つレポートテンプレートの紹介



#### 3.過去7日間に検出イベントがあった上位のコンピューター



「過去7日間に検出イベントがあった上位のコンピューター」レポートはデータ※「ウイルス対策検出」の情報をもとに<mark>ウイルス警告の多いコンピューターを抽出し、レポート化します。</mark>

ウイルス警告の多いクライアントを把握することで、ウイルスの感染・標的型攻撃の可能性が無いかなど、問題の早期発見に役 立ちます。

※レポートで表示させるデータを指しております。データはレポート作成時に設定することができます。データの設定につきましては本資料の「P25 5.レポートテンプ レートの作成手順」をご参照ください。



©Canon Marketing Japan Inc.

#### 3.スキャナー別過去30日のウイルス対策の検出



「スキャナー別過去30日のウイルス対策の検出」レポートはデータ「ウイルス対策検出」の情報をもとに<mark>ウイルス検出した保護機能を抽出し、レポート化します。</mark>

保護機能ごとの比率を出すことで、ウイルスの侵入経路の割合を確認することができます。

HTTPフィルタであればインターネット経由、POP3フィルタであればメール経由、リアルタイムファイルシステム保護であれば外部ストレージ経由など、推測することが可能です。



### 3. 過去7日間のアクティブな高重要度検出イベント



「過去7日間のアクティブな高重要度検出イベント」レポートはデータ「ウイルス対策検出」の情報をもとにウイルス検出後の処理 が未解決のクライアントを抽出し、レポート化します。 抽出されたクライアントは、脅威が駆除/削除されずにクライアント内に存在している可能性があります。その場合、該当のクライア ントの調査又はレスキューCDを利用した検査※の実施を検討ください。 ※レスキューCDを利用した検査につきましては以下をご参照ください。 ▽レスキューメディア(レスキューCD)にてコンピューターの検査を実施する手順 https://eset-support.canon-its.ip/fag/show/3639?site\_domain=business

	コンピュー ター名	扬 重大度	脅威タイプウイルス名。 脅威フラ	グスキャナ	検出エンジ ン	オブジェク トの種類	オブジェク実行され トURI アクショ	ıたアクション処玛 ıンエラー 脅威	星された 減	再起動が必 <sub>史</sub>	プロセス名	状況	
脅威タイプや マイルス名が	2021年 12日 15:46:4	E 4月 🛕 重大 4 <u>1</u>	テストファ Eicar イル	リアルタイ ムファイル システム保 護	23117 (20210412)	ファイル	file:///C:/U 保持 sers/ESET/ Desktop/新 しいテキス ト ドキュ メント.txt	L^L	いえ	いいえ	C:\Window s\System3; \notepad.e xe	変更された ファイルで イベントが 発生しまし た。	脅威検出状確認できます
筆認できます。 	2021年 9日 16:38:2	E 4月 🛕 重大 23	テストファ Eicar イル	リアルタイ ムファイル システム保 護	23103 (20210409)	ファイル	file:///C:/U 保持 sers/ESET/ Desktop/ei car.txt	ι.ι	いえ	いいえ 	C:\Window s\System32 \notepad.e xe	ファイルに アクセスし ようとした ときにイベ ントが発生 しました。	
	2021年 9日 16:38:1	E 4月 🛕 重大 16	テストファ Eicar イル	リアルタイ ムファイル システム保 護	23103 (20210409)	ファイル	file:///C:/U 保持 sers/ESET/ Desktop/ei car.txt	L\L	いえ	いいえ	C:\Window s\System32 \notepad.e xe	変更された ファイルで イベントが 発生しまし た。	

#### 3. 検出エンジンの更新ステータスの割合



「検出エンジン更新状況の割合」レポートはデータ「検出エンジン」の情報をもとに、アップデート状況を抽出し、レポート化します。 セキュリティレベルを高めるためには、検出エンジンが最新である必要があります。 アップデートがされていないクライアントが存在する場合は、検出エンジンのアップデートタスクを配信することを検討します。 ※検出エンジンのアップデートタスクを配信する手順につきましては以下をご参照ください。 ▽クライアント管理用プログラムから、クライアント用プログラムの検出エンジン(ウイルス定義データベース)をアップデートするには ? https://eset-support.canon-its.jp/faq/show/13247?site\_domain=business



## 3. OS



「OS」レポートはデータ「OSエディション」の情報をもとに、クライアントのOS情報を抽出し、レポート化します。

クライアントのOSを把握することで、レガシーOSの有無を確認することができます。レガシーOSは脆弱性を悪用した攻撃の対象 になりやすいため、把握しておくことが重要です。また、クライアントで使われているOSを確認することで、クライアント用プログラムの

バージョンアップ計画の参考にすることができます。

※レガシーOSの注意点につきましては以下をご参照ください。

ママイクロソフト社のサポートが終了したOSの利用を継続する場合の注意事項

https://eset-support.canon-its.jp/faq/show/303?site\_domain=business



4.前回の検査



「前回の検査」レポートはデータ「前回の検査」の情報をもとに、クライアントが前回の検査のタイミングをレポート化します。長期 間検査を実施していないクライアントを確認することができます。定期的に検査を行うことでセキュリティを保つことができます。長 期的に検査を実施していないクライアントがある場合は該当のクライアントに対して検査を実施するなど検討してください。

※クライアントに対して検査をさせる設定手順につきましては以下をご参照ください。
 ▽クライアントに対して定期的にファイルの検査をさせるには?
 <a href="https://eset-support.canon-its.jp/faq/show/100?site\_domain=business">https://eset-support.canon-its.jp/faq/show/100?site\_domain=business</a>







「監査ログ」レポートはデータ「監査ログ」の情報をもとに、EPのログインユーザーの動作を抽出し、レポート化します。各ログイン ユーザーがEP Webコンソール上で行った操作(ログイン情報、ポリシーの作成や変更、タスクの実行など)を確認することがで きます。管理者は、拠点ごとに複数のログインユーザーいる場合などはEP Webコンソールで実行されたアクティビティを検査するこ とで、各ログインアカウントに対するユーザーの権限設定の見直しに役立てることが可能です。

※監査ログは「監査ログ」機能でも確認することができます。(監査ログのデータを出力することはできません。)監査ログのデータを出力する場合はレポート機能をご利用 ください。

発生時刻	ドメイン	アクション	アクション詳細	結果	ユーザー氏名	ユーザー名	ローカルユーザー
2020 7月 21 17:01:55	シングルサインオントークン	シングルサインオントークンの 発行	ネイティブユー ザー'administrator'のシン グルサインオントーク ン'********が発行されまし た。	<u>i</u> 成功	「EPのログインユーザーの実」 アクションを確認 できます。	行した	
2020 7 <b>月</b> 21 17:01:55	ローカルユーザー	ログイン試行	ネイティブユー ザー'administrator'を認証 しています。	<u>i</u> 成功			
2020 7月 21 16:59:54	モジュールの更新	アップテート	モジュールが更新されまし た。	1 成功	System user	system	はい
2020 7月 21 16:58:54	ローカルユーザー	ログアウト	ネイティブユー ザー'Administrator'をログ アウトしています。	<u>i</u> 成功	Administrator	Administrator	はい
2020 7 <b>月</b> 21 16:15:56	サーバータスク	削除	タイプ・レポートの作成'のサー パータスク'レポートの生成: OS, (2020 2月 28 16:06:13)'を削除していま す。	1 成功	Administrator	Administrator	はい
2020 7月 21 16:15:19	サーバータスク	開始日時	タイブ・コンピューター名の変 更・のサーバータスク・同期さ れたコンピュータの名前を自 動的にFQDN形式に変更・を 開始しています。	1 成功	Administrator	Administrator	はい

©Canon Marketing Japan Inc.



# 4.レポートのスケジュール機能



#### 4.レポートのスケジュール機能



「レポートのスケジュール」では指定したレポートテンプレートを定期的に作成することができます。 定期的に作成するタイミングは時間やイベント(動的グループのクライアントが変更されたタイミングなど)で設定することができます。 また、作成したレポートは「電子メールで送信」「フォルダに保存」ができます。



※EPCでは「フォルダに保存」はできませんが、「電子メールの送信」は可能です。「ESETクライアント管理 クラウド対応オプション」および「ESETクライアント管理 クラウド対応オプション Lite」では、「フォルダに 保存」および「電子メールでの送信」はできませんが、ブラウザよりダウンロード が可能です。

©Canon Marketing Japan Inc.



「1日1回レポートをメールで送信する」場合を例に、レポートのスケジュール設定手順を紹介します。

①EP Webコンソール を起動して、ESET PROTECT に接続します。 ユーザー名とパスワードを入力し、「ログイン」をクリックします。

※ EP Webコンソールには以下のURLよりアクセスできます。

https:// <セキュリティ管理ツールのサーバー名、または、IPアドレス>/era/

②EP Webコンソールの画面左のメインセクションの [レポート] より、 [スケジュールされたレポート] 、[スケジュール…]の 順にクリックします。

<ol> <li>①の画面</li> </ol>	②の画面
(eser) PROTECT	ダッシュポード     カナゴリをテップレーズグジュールされたレポート       コンピューター     スグジュールされたレポート   アクセスグループ 選択 意 タグニ マ フィルタ
ログイン	kiti     タグ     タグ     レポート省     トリガー     ゴ レポート     タスク
A Administrator	<ul> <li>         インストーラー         ③ ポリシー         ゆ 通知         %         ステータス標準     </li> </ul>
<ul> <li>● 日本語</li> <li>▼</li> <li>● ドメインユーザーとしてログイン</li> <li>マレチタブでのセッションを有効化</li> <li>ログイン</li> <li>パスワードの変更</li> </ul>	<ul> <li>メントーラスム型</li> <li>デオル</li> <li>ジントーラスム型</li> <li>ジストーター</li> <li>ジュント ゴムビタングのジストを確認し、 オムビタンジングできます。</li> <li>マーク</li> </ul>



# ③「テンプレート」ではレポートテンプレートを設定します。 設定したいレポートテンプレートを [レポートテンプレートの追加] で選択します。必要に応じて [タグ] を選択してください。 テンプレートの設定が終わりましたら、 [続行] をクリックします。 例) 名前 : 接続していないコンピューター

レポート 〉レポートのスケジュ	-JL		下記のように一覧で表示されます。
テンプレート	レポートテンプレート		テンプレートを選択してください
スケジュール	接続していないコンピューター	<del></del>	
詳細設定 - 調整	レポートテンプレートの追加		
▲ 配信	タヴ		③ 上位のコンピューターの問題 オペレーティングシステムまたは管理製品によって報告された最も頻繁な問題
	タグを選択		③ 上位のモバイルデバイスの問題 オペレーティングシステムまたは管理製品によって報告された最も頻繁な問題
			田信頼できないハードウェアの検出があったコンビュータ 信頼できるハードウェア検出のために十分な情報を提供していないコンピュータのリスト。ハードウェア検出は無効に
			囲 接続していないコンピューター 14日間以上接続していないコンピューターの概要
			(2) 前回のコンビューター接続 前回接続時刻によってグループ化されたコンピューターの概要
			(2) 前回のモバイルデバイス更新 最後の検出エンジンによってグループ化されたモバイルデバイス
			③ 前回のモバイルデバイス接続 前回接続時間でグループ化されたモバイルデバイスの概要
			(2) 前回の更新 最後の検出エンジン更新によるコンピュータグループ
	↓		用  十鬼はうなどう家庭

④「スケジュール」ではレポートの作成タイミングを設定します。
 [トリガータイプ]を選択して、レポートが作成されるタイミングを設定ください。
 トリガー毎に設定項目がことなります。任意の設定を行います。
 テンプレートの設定が終わりましたら、 [続行]をクリックします。
 例)トリガータイプ:毎日

テンプレート	i トリガータイプ
スケジュール	
詳細設定 - 調整	田口操り次()
▲ 配信	1 開始日時 ⑦
	2021 4月 22 09:00:00
	終了条件 ⑦
	<ul> <li>終了なし</li> </ul>
	○ 終了日 10 発生
	() 終了日
	スケジュール ③
	● 毎週土曜日と日曜日
	ランダム遅延間隔 ③
	0 秒 🗸
	設定した時間に失行されなかった場合は即時失行 ②
	1 サーハーのローカル時刻を使用

#### ●トリガータイプ※

	一度だけ実行	~
Γ	スケジュール済み	
	一度だけ実行	
	毎日	
	毎週	
	毎月	
	毎年	
	動的グループ	
	動的グループメンバーが変更	
	しきい値に従って動的グループサイズが変更	
	期間中に動的グループサイズが変更	
	比較グループを基準に動的グループサイズが変更	
	その他	
	サーバーが起動	
	イベントログトリガー	
	CRONE	

※トリガータイプつきましては以下をご参照ください。 マタスクトリガータイプ ESET PROTECT オンラインヘルプ <u>https://help.eset.com/protect\_admin/80/ja-JP/?admin\_st\_triggers.html</u>



⑤「配信」ではレポート配信の設定をします。
 [電子メール] [ファイルに保存]を選択して、レポートの出力方法を設定ください。
 レポートの出力設定が終わりましたら、[終了] をクリックします。
 以上で設定手順は終了です。
 (例) レポート配信

例)レポート配信

: 電子メールに送信 : test@test.com

送信先 メッセージをカスタマイズ

- : チェックなし
- レポートが空の場合にメールを送信: チェックあり



©Canon Marketing Japan Inc.



## 4.(補足)レポートのスケジュール機能設定手順

eser

フォルダにレポートを保存する際に設定する[ファイルに保存]について案内します。

- [相対ファイルパス] ではレポート保存時のフォルダの設定をします。(必ず相対パスでしてください) 以下の形で設定をします。
  - [保存先フォルダ※1] ¥ [保存時のフォルダ名※2]
  - 例)./TEST/%DATE%
- [レポートが空の場合にファイルを保存]ではレポートが作成できない場合の動作を指定します。
  - ※1 既定フォルダ配下であれば任意の場所に設定できます。
    - 既定のフォルダは以下となります。
    - Windowsの場合
    - C:/ProgramData/ESET/RemoteAdministrator/Server/EraServerApplicationData/Data/GeneratedReports
    - Linuxの場合 /var/opt/eset/RemoteAdministrator/Server/GeneratedReports/
  - ※2 保存時のフォルダのフォルダ名は「任意の文字列」+「パス変数」で設定できます。

	ファイルオプション	●パス変数	
設定例) ./TEST/%DATE% 上記の設定では既定のフォルダ 配下の「フォルダ名: TEST」へ 保存し、レポート保存時に作成 されるフォルダ名は「現在の日 時」となります。(レポート自体は レポート保存時に作成されるフォ ルダに保存されます。)	<ul> <li>i レポート配信</li> <li>◎ 電子メールを送信</li> <li>マァイルレオプション</li> <li>i 相対ファイルパス</li> <li>/TEST/%DATE%</li> <li>レポートが空の場合にファイルを保存 ⑨</li> </ul>	パス変数の追加         現在の日付(YYYY-MM-DD')         現在の時間('HH-MM-SS')         現在の日付と時間('YYYY-MM-DD HH-MM-SS')         現在の時間、詳細形式('HHMMSS')         現在の時間、詳細形式('HHMMSS')         年('YYY')         ク月('mm')         日 ('dd')         時間('HH')         ミュート('MM')	パス変数は 左記より指定 できます。
		秒(~55~)	



# 5.レポートテンプレートの作成手順



#### 5. レポートテンプレートの作成手順



「検出エンジンのバージョンの一覧表を出力する」場合を例に、レポートテンプレートの作成手順を紹介します。

①EP Webコンソール を起動して、ESET PROTECT に接続します。 ユーザー名とパスワードを入力し、「ログイン」をクリック します。

※ EP Webコンソールには以下のURLよりアクセスできます。

https:// <セキュリティ管理ツールのサーバー名、または、IPアドレス> /era/

②EP Webコンソールの画面左のメインセクションの [レポート] より、 [新しいレポートテンプレート] をクリックします。

<ul> <li>▲ レポート</li> <li>▶ タスク</li> <li>□ インストーラー</li> </ul>		
<ul> <li>③ ポリシー</li> <li>ゆ 通知</li> <li>&amp; ステータス概要</li> <li>… 詳細</li> </ul>		ログイン 冬 Administrator 合 パスワード ● 日本語
>	··· 詳細 >	
	G ホリシー 中 ゆ 通知 ♥ ステータス概 … 詳細	· ↓ 通知 · ↓ 通知 · ↓ 通知 · ↓ 詳細 · · · 詳細

5. レポートテンプレートの作成手順

eser

③「基本」ではレポートの基本情報を設定します。 作成するレポートテンプレートの〔名前〕を入力し、〔カテゴリ〕を選択します。 必要に応じて〔説明〕を入力し、〔タグ〕を選択してください。基本の設定が終わりましたら、〔続行〕をクリックします。 例)名前 :検出エンジンのバージョンの一覧 カテゴリ: TEST

※名前に「:」「\*」「<」「>」「/」「¥」「?」を含めないようにしてください。含めると正常にレポートが保存できないケースがありますのでご注意ください。

基本	基本		名前 説明
🔺 グラフ	名前		
データ	検出エンジンのパージョンの一覧		
並べ替え	14.00		
フィルタ	150 499		
サマリー			
	タグ	( 既定のカテゴリも用意されて	
	タヴを選択	いますが、任意のカテゴリも	
	カテゴリ	追加できます。	
	TEST	独自のカテゴリを追加するこ	
		とで既定のテンフレートと分	
		けることかできます。	
			元全ナイ人ク暗亏化

5. レポートテンプレートの作成手順

#### ④「グラフ」では表示させるデータを設定します。 テーブルを表示させる場合は [表示テーブル] にチェックをいれます。 グラフの設定が終わりましたら、 [続行] をクリックします。

例) 表示テーブル : チェックあり

グラフの表示

:チェックなし







5. レポートテンプレートの作成手順

⑤「データ」では表示するデータを設定します。 [列の追加]より、表示させるテーブル列のデータを設定します。データの設定が終わりましたら、[続行]をクリックします。 例) テーブル列:コンピューター,コンピューター名,コンピューター名 検出エンジン,データベースのバージョン 検出エンジン,データベース日付





ese

5. レポートテンプレートの作成手順

eser

⑥「並び替え」では表示させるデータの順番を設定できます。

[並び替えの追加]をクリックして、データの並び替えを行います。データの並び替えが終わりましたら、 [続行]を クリックします。

例) 並び替え:コンピューター,コンピューター名,昇順

新しいレポートテンプレート レポート > 検出エンジンのパージョンの一覧	昇順、降順より、表示させる結果 を並び変えることができます。
<ul> <li>基本</li> <li>グラフ</li> <li>データ</li> <li>並べ替え</li> <li>コンピューター、コンピューター名</li> <li>原順</li> <li>並べ替えの追加</li> <li>プィルタ</li> <li>サマリー</li> <li>印刷プレビュー</li> </ul>	
戻る 統行 終了 キャンセル	

#### 5. レポートテンプレートの作成手順



⑦「フィルタ」ではレポートに表示させる情報にフィルタをかけることができます。フィルタによりレポートで抽出するデータの範囲 指定することができます。

[フィルタの追加] よりフィルタの設定を行います。フィルタの設定が終わりましたら、 [続行] をクリックします。

例) フィルタ条件:静的グループ,静的グループ,=(等しい),TEST

※上記の例は静的グループ「TEST」よりデータを抽出するフィルタの設定です。

⑧「サマリー」レポートテンプレートの設定内容を確認できます。内容を確認し、 [終了] をクリックします。 以上で設定手順は終了です。

基本	フィルタ条件	
グラフ データ	静的グループ · 静的グルー = (等しい) TEST プ	Ŵ
並べ替え フィルタ		
-U\$ <del>U</del>	ロ刷プレビュー	
	戻る 統行 終了 キャンセル	

©Canon Marketing Japan Inc.

### 5. (補足)レポートテンプレートの作成手順



レポートテンプレートより、レポートをダウンロードする方法について案内します。

①EP Webコンソール を起動して、ESET PROTECT に接続します。 ユーザー名とパスワードを入力し、「ログイン」をクリック します。

※ EP Webコンソールには以下のURLよりアクセスできます。

https:// <セキュリティ管理ツールのサーバー名、または、IPアドレス>/era/

②EP Webコンソールの画面左のメインセクションの [レポート] より、ダウンロードしたレポートのテンプレートを選択し、[歯車 マーク] をクリックします。

③[ダウンロード]を選択し、ダウンロードしたいレポート形式([PDF]または[CSV(表データのみ)])をクリックします。その後、指 定した形式でレポートがダウンロードされます。

<sup>2</sup> 🛦	検出	Dynamic Threat Defense	TEST		検出エンジンのバージョンの一覧 ▶ 今すぐ生成	形式を指定してダウンロード
	レポート	Enterprise Inspector			<ul> <li></li></ul>	
Þ	タスク			★出エンジンのバ ージョンの一覧		
	インストーラー	ワイルス対策検出	└⊕ 新しいレポートテ		<ul> <li>国 監査ログ</li> <li>「 複製…</li> </ul>	
ø	ポリシー	サーバーパフォーマンス	ンプレート		<b>〕</b> 削除	
φ	通知	ネットワーク			▶ エクスボート	
ъ	ステータス概要	ハードウェアインベントリ				











レポートテンプレートカテゴリの「ESET Dynamic Threat Defense※1」「ESET Enterprise Inspector※2」「完全ディスク暗号化(ESET Full Disk Encryption)※3」は ESET Endpoint Protection シリーズと別製品に関するものです。このレポートテンプレートを利用するには、ESET Endpoint Protection シリーズのライセンスとは別に該当の製品のライセンスを購入する必要があります。

※1 ESET Dynamic Threat Defense 未知のマルウェアに対する検出・防御の即時性を高め、ESET PROTECTソリューションの検出力・防御力を高めるクラウドサービスです。 製品の特長・動作環境・価格については以下のWebページをご参照ください。 <u>https://eset-info.canon-its.jp/business/edtd/</u>

※ 2 ESET Enterprise Inspector 組織内の端末から収集したさまざまなアクティビティをもとに、端末上の疑わしい動きを検出・分析・調査し、組織内に潜む脅威をいち早く割り出し、封じ込めることが できるEDR製品です。

製品の特長・動作環境・価格については以下のWebページをご参照ください。

https://eset-info.canon-its.jp/business/eei/

※3完全ディスク暗号化(ESET Full Disk Encryption) リモートワークや社内で利用するクライアントPCのディスクを暗号化し、PC紛失・盗難時の情報漏えいから、お客さまの機密情報を守る暗号化製品です。 製品の特長・動作環境・価格については以下のWebページをご参照ください。 <u>https://eset-info.canon-its.jp/business/efde/</u>