

# Dell Data Security

EnCase 統合ガイド



## メモ、注意、警告

① | **メモ:** 製品を使いやすくするための重要な情報を説明しています。

△ | **注意:** ハードウェアの損傷やデータの損失の可能性を示し、その問題を回避するための方法を説明しています。

⚠ | **警告:** 物的損害、けが、または死亡の原因となる可能性があることを示しています。

© 2012-2018 Dell Inc. 無断転載を禁じます。Dell、EMC、およびその他の商標は Dell Inc. またはその子会社の商標です。その他の商標は、それぞれの所有者の商標である可能性があります。

Dell Encryption、Endpoint Security Suite Pro、Endpoint Security Suite Enterprise、および Data Guardian スイートのドキュメントに使用されている登録商標および商標 ( Dell™、Dell のロゴ、Dell Precision™、OptiPlex™、ControlVault™、Latitude™、XPS®、および KACE™ ) は、Dell Inc. の商標です。Cylance®、CylancePROTECT、および Cylance のロゴは、米国およびその他の国における Cylance, Inc. の登録商標です。McAfee® および McAfee のロゴは、米国およびその他の国における McAfee, Inc. の商標または登録商標です。Intel ®、Pentium ®、Intel Core Inside Duo®、Itanium®、および Xeon ® は米国およびその他の国における Intel Corporation の登録商標です。Adobe®、Acrobat®、および Flash® は、Adobe Systems Incorporated の登録商標です。Authen Tec® および Eikon® は、Authen Tec の登録商標です。AMD® は、詳細設定 Micro Devices, Inc. の登録商標です。Microsoft®、Windows®、および Windows Server®、Internet Explorer®、MS-DOS®、Windows Vista®、MSN®、ActiveX®、Active Directory®、Access®、ActiveSync®、BitLocker®、BitLocker To Go®、Excel®、Hyper-V®、Silverlight®、Outlook®、PowerPoint®、Skydrive®、SQL Serve®、および Visual C++® は、米国および / またはその他の国における Microsoft Corporation の商標または登録商標です。VMware® は、米国およびその他の国における VMware, Inc. の登録商標または商標です。Box® は、Box の登録商標です。DropboxSM は、Dropbox, Inc. のサービスマークです。Google™、Android™、Google™ Chrome™、Gmail™、YouTube®、および Google™ Play は、米国およびその他の国における Google Inc. の商標または登録商標のいずれかです。Apple®、Aperture®、App StoreSM、Apple Remote Desktop™、Apple TV®、Boot Camp™、FileVault™、 iCloud®SM、iPad®、iPhone®、iPhoto®、iTunes Music Store®、Macintosh®、Safari®、および Siri® は、米国またはその他の国あるいはその両方における Apple, Inc. のサービスマーク、商標、または登録商標です。GO ID®、RSA®、および SecurID® は Dell EMC の登録商標です。EnCase™ および Guidance Software® は、Guidance Software の商標または登録商標です。Entrust® は、米国およびその他の国における Entrust®, Inc. の登録商標です。InstallShield® は、米国、中国、欧州共同体、香港、日本、台湾、および英国における Flexera Software の登録商標です。Micron® および RealSSD® は、米国およびその他の国における Micron Technology, Inc. の登録商標です。Mozilla® Firefox® は、米国およびその他の国における Mozilla Foundation の登録商標です。IOS ® は同社の商標または米国およびその他の特定の国で Cisco Systems, Inc. の登録商標であり、ライセンスに使用されます。Oracle® および Java® は、Oracle および / またはその関連会社の登録商標です。その他の名称は、それぞれの所有者の商標である場合があります。SAMSUNG™ は、米国およびその他の国における SAMSUNG の商標です。Seagate® は、米国および / またはその他の国における Seagate Technology LLC の登録商標です。Travelstar® は、米国およびその他の国における HGST, Inc. の登録商標です。UNIX® は、The Open Group の登録商標です。VALIDITY™ は、米国およびその他の国における Validity Sensors, Inc. の商標です。VeriSign® およびその他の関連標章は、米国およびその他の国における VeriSign, Inc. またはその関連会社あるいは子会社の商標または登録商標であり、Symantec Corporation にライセンス供与されています。KVM on IP® は、Video Products の登録商標です。Yahoo!® は、Yahoo! Inc. の登録商標ですこの製品は、7-Zip プログラムの一部を使用しています。このソースコードは、[7-zip.org](http://7-zip.org) に掲載されています。ライセンス供与は、GNU LGPL ライセンス + unRAR 制限 ( [7-zip.org/license.txt](http://7-zip.org/license.txt) ) の対象です。

### EnCase 統合ガイド

2018 - 03

Rev. A01

<b>1 はじめに</b> .....	<b>4</b>
Dell ProSupport へのお問い合わせ.....	4
<b>2 EnCase との統合</b> .....	<b>5</b>
EnCase API の有効化.....	5
EnCase 統合アダプタのインストール.....	5
<b>3 EnCase が統合された Dell Data Security の使用方法</b> .....	<b>6</b>
<b>4 Dell Data Security に統合された EnCase の使用方法</b> .....	<b>8</b>
CEGetBundle.....	8



# はじめに

Dell Data Security は、デル暗号化ファイルのオンライン調査に対応できるように、Guidance Software, Inc. の EnCase v6.15 デジタルフォレンジック製品と統合されます。この統合により、フォレンジック調査担当者は、デルで保護されたデータの表示、エクスポート、検索ができるようになります。適切なフォレンジック管理者資格情報を有していれば、暗号化の際に使用したキーにかかわらず、デルで保護されたすべてのデータが復号化されて調査担当者に表示されます。余分な操作は一切必要ありません。EnCase の Secure Storage にフォレンジック管理者の資格情報が太文字小文字を区別して格納保存されるため、再入力の必要はありません。

EnCase v6.15 ( 32 ビット ) フォレンジック統合のサポート対象は次のとおりです。

- Dell Data Security Encryption Enterprise for Windows v7.0.x 以降
- Dell Security Management Server v7.0.1 以降

① **※E: Dell Data Security Encryption Enterprise for Mac は EnCase フォレンジック調査をサポートしません。**

## Dell ProSupport へのお問い合わせ

デル製品向けの 24 時間 365 日対応電話サポート ( 877-459-7304、内線 4310039 ) にご連絡ください。

さらに、デル製品のオンラインサポートも [dell.com/support](https://dell.com/support) からご利用いただけます。オンラインサポートでは、ドライバ、マニュアル、テクニカルアドバイザー、よくあるご質問 ( FAQ )、および緊急の問題を取り扱っています。

適切なサポート担当者に迅速におつなぎするためにも、お電話の際はお客様のサービスタグまたはエクスプレスサービスコードをご用意ください。

米国外の電話番号については、[Dell ProSupport の国際電話番号](#)をチェックしてください。

## EnCase との統合

### EnCase API の有効化

- ① **メモ:** DMZ に展開している Dell デバイスサーバには、この API を使用しないでください。セキュリティ維持のため、内部で使用する Dell デバイスサーバでは、統合した EnCase へのアクセスを制限してください。

#### v7.7 より前の Security Management Server の場合

- 1 <Dell install dir>\Enterprise Edition\Device Server\conf\context.properties を開きます。
- 2 フォレンジック統合 API を有効化します。

```
service.forensic.enable=true
```

- 3 スタートメニューから、Dell デバイスサーバを停止して再起動します。

フォレンジック統合を無効化するには、次のように指定します : set service.forensic.enable=false。

#### v7.7 以降の Security Management Server の場合

- このサービスは、Dell サーバでデフォルトで有効になっています。
- フォレンジック統合を無効化するには、次のように指定します : set xapi.service.forensic.enable=false。

スタートメニューから、Dell デバイスサーバを停止して再起動します。

### EnCase 統合アダプタのインストール

- 1 EnCase を実行しているコンピュータで、**CMGEnCaseIntegration.exe** をダブルクリックします。
- 2 ライブラリインストーラのダイアログが表示されたら、ターゲットの EnCase フォルダが正しいことを確認します。
- 3 **終了** をクリックして、CEGetBundle ファイルと統合アダプタファイルを \Program Files\EnCase6\Lib\Credant Technologies\CMG に解凍します。



# EnCase が統合された Dell Data Security の使用方法

## 暗号化キーの取得

EnCase Enterprise ユーザーインターフェースを使用して Dell リモート管理コンソールから暗号化キーを取得し、このコンピュータまたはエビデンスファイルのためにデル暗号化データを復号化します。

- 1 **オンライン** チェックボックスを選択します。
- 2 フォレンジック管理者の **ユーザー名** を入力します。
- 3 フォレンジック管理者の **パスワード** を入力します。
- 4 EnCase API が有効化されている Dell サーバの URL を入力します。次に例を示します。

https://cred01.somedomain.com:8443/xapi/ ( Security Management Server が v7.7 以降の場合 )

https://cred01.somedomain.com:8081/xapi ( Security Management Server が v7.7 より前の場合 )

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet で、Dell サーバ URI を見つけます。

**① メモ:** キーをエクスポートするため、Dell サーバでは EnCase API が有効化されている必要があります。オプションとして、EnCase 統合専用を使用する Dell デバイスサーバを別にもう 1 台用意する方法もあります。

- 5 ターゲットコンピュータまたはエビデンスファイルのマシン ID ( MCID またはユニーク ID とも呼ぶ ) を入力します。

Dell リモート管理コンソールで、HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield のターゲットコンピュータのレジストリにある MCID を見つけます。

左のペインで、**ポピュレーション > エンドポイント** をクリックします。

- 適切なデバイスの **詳細** アイコンをクリックします。
- 上部のメニューで、**詳細およびアクション** をクリックします。
- エンドポイントの詳細 エリアでユニーク ID を見つけます。

- 6 ターゲットコンピュータまたはエビデンスファイルのシールド ID ( デバイス ID、DCID、リカバリ ID、SCID とも呼ぶ ) を入力します。

Dell リモート管理コンソールで、HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield のターゲットコンピュータのレジストリにある DCID を見つけます。

左のペインで、**ポピュレーション > エンドポイント** をクリックします。

- 適切なデバイスの **詳細** アイコンをクリックします。
- 上部のメニューで、**詳細およびアクション** をクリックします。
- シールド エリアでリカバリ ID を見つけます。

**① メモ:** MCID、DCID、または両方の ID を指定します。インポートしたケースには、指定したマシン ID、シールド ID、またはその両方の ID のすべてのキーマテリアルが含まれています。

- 7 **OK** をクリックします。

復号化が進行します。

復号化が完了すると、ファイルのフォレンジック調査が可能になります。復号化されたファイルは、EnCase モジュールを介してのみ表示できます。元のソースファイルは変更されず、暗号化されたままです。



# Dell Data Security に統合された EnCase の使用方法

## CEGetBundle

CEGetBundle は、フォレンジック管理者が Dell サーバからキーマテリアルを取得するためのユーティリティです。このユーティリティは Dell ProSupport から入手できます。

次の表は、インストールで使用できるパラメータの詳細です。

### パラメータ

-L = レガシーモード ( CMG 5.3.x サーバからキーをエクスポートするときに使用 )

URL = デバイスサーバの URL ( <securityserver.organization.com> )

AdminName = 管理者ユーザー名

AdminPwd = 管理者パスワード

AdminDomain = 管理者ドメイン

MCID = ターゲットデバイスのマシン ID ( ユニーク ID またはホスト名とも呼ぶ )

SCID = ターゲットシールドのシールド Credant ID ( DCID またはリカバリ ID とも呼ぶ )

Username = キーマテリアルをエクスポートするユーザー ( レガシーモードのみ )

OutputFile = エクスポートしたキーバンドルのファイル名

OutputPwd = エクスポートしたキーバンドルのパスワード

-R = ユーザーバックアップファイルモード

BackupFile = バックアップキーを含む実行可能ファイル

BackupPwd = バックアップファイルに使用する管理者パスワード

- ① **メモ:** AdminDomain パラメータは、複数ドメインをサポートするように設定された CMG Enterprise Edition 6.0 以降のサーバからキーをエクスポートする場合にのみ指定します。
- ① **メモ:** レガシーモードでは、MCID、SCID、Username の指定は必須です。出力ファイルに追加されるキーマテリアルは、指定したユーザーのものに限られます。ユーザーまたはユーザーローミング暗号化が有効になっている場合、復号化対象デバイスでユーザーごとに同じ出力ファイル名でこのツールを実行する必要があります。各ユーザーのキーマテリアルは出力ファイルに追加されます。

### コマンドラインの例

- 次の例では、MCID、SCID、またはその両方を使用しています。指定したマシン( MCID )、SCID、またはその両方に関連付けられたすべてのキー材料が出力ファイルに保存されます。すでに出カファイルが存在している場合は上書きされます。

```
CEGetBundle [-L] -XURL -aAdminName -AAdminPwd [-DAdminDomain] [-dMCID] [-sSCID] [-uUsername] -oOutputFile -iOutputPwd
```

- 次の例では、インストーラによってエクスポートされたバックアップファイルからキー材料が抽出されます。

```
CEGetBundle -R -bBackupFile -ABackupPwd -oOutputFile -iOutputPwd
```

