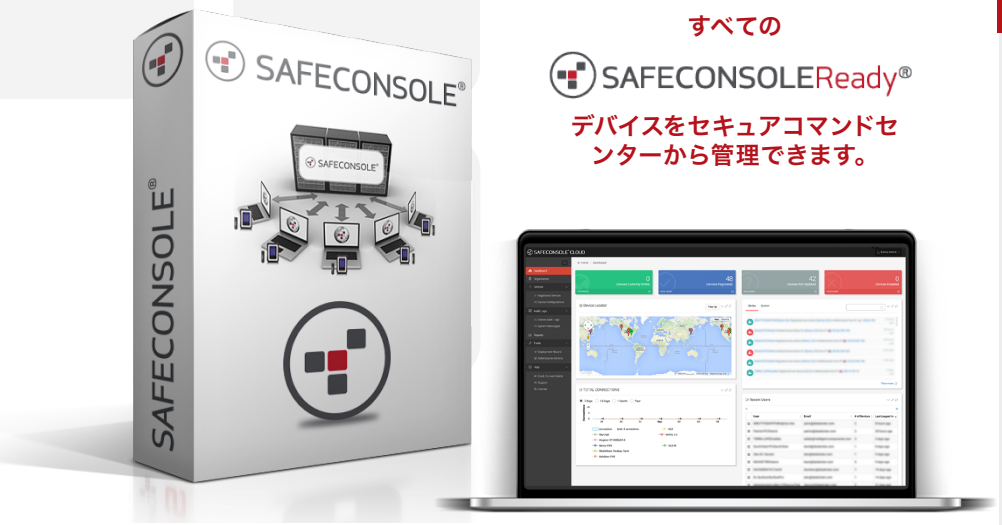
SAFECONSOLE®
クラウド型暗号化デバイス管理プラットフォーム



すべての
SAFECONSOLEReady®
デバイスをセキュアコマンドセンターから管理できます。

機密データの追跡を見失わない

DataLocker 暗号化ソリューションは、セキュアデータの持運び、保管と共有を簡単にします。SafeConsoleは、たとえどこにエンドポイントデバイスが行こうとも、それらを中央管理することができます。

SafeConsoleは、DL3/DL3FEの外部ハードディスク、DataLocker Sentry®3FIPSのフラッシュドライブ、SafeCrypt®のクラウド暗号ゲートウェイとEncryptDisc®の暗号化光学メディアなどのエンドポイントデバイスのためのセキュアストレージ管理センターです。他のSafeConsole対応®製品は、Kingston®とCardWave®のような我々のパートナーのデバイスを含みます。

SafeConsoleは、複数の場所で機密データや知的財産を処理しているデータを運ぶ従業員にとって理想的です。 SafeConsoleは、数百または数千の暗号化されたエンドポイントデバイスを効率的、視覚的に制御して管理することができます。

SAFECONSOLE の仕様

インベントリ: 暗号化されたすべての（場所を含む）エンドポイントデバイスを監視します。 Active Directoryと統合して、ユーザ、割り当てられたデバイスおよび接続されたコンピュータを容易に追跡します。

監査: 暗号化されたエンドポイントに保存または削除されたファイルを確認できます。監査証跡は、接続、ログイン失敗、リセット、および紛失レポートを含むユーザのアクティビティを監視します。

コントロール: パスワードルール、ファイルタイプ制限、地理的境界などのポリシーを強制適用できます。 パスワードをリセットし、エンドポイントを読み取り専用モードに切り替え、紛失や盗難の際にリモートで消去することもできます。

レポート: 世界中の暗号化されたエンドポイントを地図上で把握できます。設定、地理的な場所、状況、更新、最近の活動などのレポートにアクセスできます。

*SafeCrypt とEncryptDisc のサポートは間もなく提供されます。

追加機能

ジオロケーションとジオフェンシング
IPベースのロケーショントラッキングを使用して、世界中の暗号化されたエンドポイントのおおよその位置を特定します。 SafeConsoleは、特定の地理的境界内でのみアクセスできるように、デバイスを「ジオフェンシング」することもできます。

簡単で迅速な展開
SafeConsoleは、Active Directory（AD）に接続している小規模および大規模組織で簡単に利用可能です。管理者は、AD証明書でSafeConsoleにアクセスするための認証を行うことができます。 サーバーにSafeConsoleをインストールし、ドライブをユーザに展開します。 各デバイスは、SafeConsoleの特定のユーザに登録され、社内ディレクトリ（利用可能な場合）にユーザにリンクされています。オールインワンのインストールでは、必要に応じて数千台の大規模なデバイスの導入に対応する能力があります。

パブリッシャ
この機能により、管理者はポータブルアプリケーションとコンテンツをデバイスのセキュアストレージボリュームに展開/プッシュできます。 これにより、たとえば、 オプションのAntiVirusサービスの使用が可能になります。

ゾーンビルダー
これにより、安全な証明書に基づいて、信頼できるマシン上および/または信頼ゾーン内のみでデバイスのロックを解除することができます。たとえば組織ネットワーク（オンプレミスのみ）

制限: デバイスは、信頼ゾーン内のコンピュータへアクセスできます。

自動ロック解除: パスワードを入力する必要がなくなります。 この機能は、認証にRSAクライアント証明書を使用します。

アンチマルウェアサービス
DataLockerは、McAfeeと協力してデバイスのバックグラウンドで動作するアンチマルウェアソフトを提供します。McAfeeアプリケーションは各々の使用と同時にデバイスをスキャンしてマルウェアソフトを見つけて削除します。そして、どのデバイスが感染していたか、そして、それらがどのように除去されたか正確にわかるように、SafeConsoleへレポートされます。
デバイスにシームレスに統合されたMcAfeeを使用することで、お客様とお客様の組織はコンプライアンスを維持し、高いメンテナンスやサービスコストによる事故を避けることができます。

Powered by McAfee

SAFECONSOLE®
暗号デバイス管理プラットフォーム

パスワードなどの利用を中央管理します。

幅広い柔軟なポリシーとパスワードのコントロールを活用して、デバイスの使用とアクセスを管理する。

- パスワードの長さと複雑さ、パスワードの変更頻度、再試行回数などのデバイス固有のルールを強制します。
- ヘルプデスクの管理者は、パスワードを忘れたユーザを簡単かつ遠隔操作で支援できます。
- 特定のIPアドレスまたはアドレス範囲をホワイトリストに登録することにより、特定のコンピュータでドライブを使用する機能を制限できます。
- リモートでデバイスをリセットしたり、パスワードをリセットしたり、ポリシーを更新したり、読み取り専用モードを強制したり、世界中のどこからでもデバイスを無効にしたり、データを消去することさえできます。
- 管理しているデバイスの一部またはすべてで、オプションのMcAfee Anti-Virus保護ソフトウェアをアクティブ化して管理できます。
- いかなる場合でも暗号化されたエンドポイントからどのファイルが保存または削除されたかを確認できます。
- 管理しているデバイスに保存できるファイルの種類を制限できます。

デバイス管理

Kingston DataTraveler Vault Privacy 3.0 and DataTraveler 4000 G2

256ビットAES暗号化で企業の機密データを保護し機密データを保護します。

DataLocker DL3 and DL3 FE External Hard Drives

両方のDataLocker外付けハードディスクは、暗号化されたポータブルストレージの新しい標準を設定しています。ハードディスクを管理、暗号化、または展開するためのソフトウェアは必要ありません。

DataLocker Sentry 3 FIPS Flash Drive

Sentry 3 FIPSは、DataLockerの認定および実証済みのテクノロジ、FIPS 140-2レベル3認定、ハード256ビットAES暗号化を使用しています。

柔軟な展開オプション

クラウドホスティングサービス

- 数分で実行可能
- どこからでもログイン、管理が可能
- メールと電話のサポート
- エンドポイント/年当たりの価格と1回限りの初期基本料金

オンプレミス

- 専用のWindowsベースのサーバーが必要
- どこからでもログインして管理可能
- 適度のスペックのハードとネットワーク帯域が必要です。
- 300以上のエンドポイントの導入に最適

詳細、デモ、価格については販売元にお問い合わせください。

PCI コンプライアンス

SafeConsole Cloudの場合、当社のデータセンターは国内および/または国際的なセキュリティ基準によって認証されています。 また、SafeConsole Cloudは単一のテナントソリューションです。つまり、会社のサービスのみがその特定の仮想サーバーをホストしています。 また、ストレージ製品の実際のデータはクラウドに保存されません。 管理コンソールであるSafeConsoleだけがクラウド上でホストされます。

販売元

WEBSITE
datalocker.com

米国、カナダ
sales@datalocker.com
+1 913 310 9088

ヨーロッパ
emea@datalocker.com

アジア
apac@datalocker.com

日本
sol_sales@e-it.co.jp
www.datalocker.jp