

WinMagic SecureDoc Linux for Servers

WinMagic SecureDoc Linux for Servers は、Linux サーバ向けの市場で唯一のエンタープライズクラスのフルディスク暗号化ソフトウェアです。ネイティブの暗号化ツールの dm-crypt を置換するのではなく、dm-crypt の上層で動作するため、暗号化の管理を容易にし、Linux の暗号化管理を新しいレベルへと移行し、大規模でグローバルなテクノロジー企業が実際に直面している課題を解決します。

サーバ保護については、多くの企業が物理的なセキュリティリスクを見逃しがちです。よくある誤解は、「サーバがデータセンターにあるか、あるいは鍵が適用されロックされているため」、そして「データが常に使用されデータが決して静止することがないため」、ドライブの暗号化は不要という考えです。Linux デバイスを暗号化するための作業は複雑化しており、多くの組織が「これで十分」というアプローチになるのも不思議ではありませんが、これが問題を引き起こす原因となることは多くあります。すべてのドライブは修理や廃棄のために最終的にはデータセンターを離れることになります。このような意図しないところでデータが漏洩するリスクを回避するためには、ドライブを暗号化しておくことが最良の方法になります。

暗号化と鍵管理の分離

暗号化製品が優れた効果を発揮するためには、暗号化と鍵管理の 2 つのコンポーネントに分ける必要があります。これらの 2 つのコンポーネントで必要となる専門知識が大きく異なるためです。これこそが、WinMagic SecureDoc Linux for Servers が採用している仕組みです。WinMagic SecureDoc Linux for Servers は、Linux サーバ向けの市場で唯一のエンタープライズクラスのフルディスク暗号化ソフトウェアです。このソリューションは、ネイティブの暗号化ツールである dm-crypt を置換するのではなく、dm-crypt の上層で動作するため、暗号化の管理を容易にし、Linux の暗号化管理を新しいレベルへと移行し、大規模でグローバルなテクノロジー企業が実際に直面している課題を解決します。

- Linux 環境を保護しながら、システムのセキュリティを管理および監査できるようにします。
- すべてのオペレーティングシステムのネイティブなソフトウェア暗号化（Linux、Windows、Mac OS）または自己暗号化ドライブを管理します。
- 最も高度なストレージ手法との互換性を確保しています。

堅牢な認証

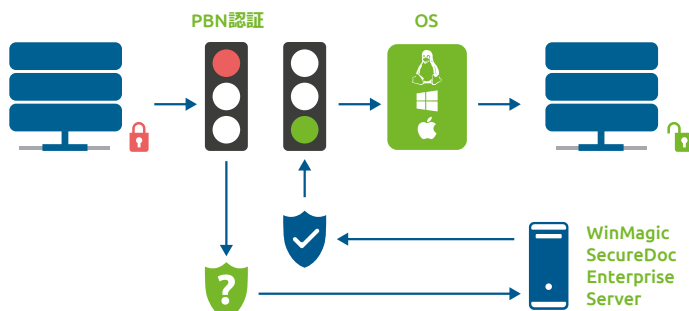
アイデンティティとアクセスコントロールが現在重視されている中で、サーバの堅牢な認証を実現し、データが確実に悪用されないようにする暗号化ソリューションを導入することが重要です。Linux で現在利用されている暗号化機能である dm-crypt と LUKS を併用することで、パスワード認証されるシンプルな「スタンドアロン」のハードディスク暗号化（FDE）アプリケーションの基盤を形成することは可能です。しかし、これらのツールは特にサーバ環境に対応するエンタープライズクラスのソリューションではなく、管理者が常駐していない環境では利便性が大きく低下します。

WinMagic SecureDoc Linux for Servers は、ウインマジックのプリブートネットワーク認証機能である PBConnex を使用して、リモートから安全にサーバを自動的に起動 / 再起動できるようにして、IT 管理者の大きな悩みを解決します。

- プリブートネットワークベースの認証による認証のセキュリティの向上 - OS の起動前にセキュリティを確保します。
- Active Directory のユーザ名とパスワードを使用したプリブート環境での認証を可能にします。通常 Linux ではプリブートパスワードや各ボリュームに異なるパスワードが必要になります。また AD はサポートされません。



サーバ向けネットワークベースの自動認証



ディスク全体とルートボリュームの暗号化

ルートボリュームの暗号化、データボリュームの暗号化、およびスワップパーティションの暗号化は、ほぼすべての組織が必要です。しかし、Linux ネイティブの FDE を使用してルートボリュームを保護することは非常に複雑な作業になります。WinMagic SecureDoc Linux for Servers は、Linux サーバを暗号化するための優れた仕組みを提供します。

- RAID アレイ、ディスク、リモート管理、およびマルチ OS 対応といった課題を解決できるよう最適化されています。

初回暗号時のライブコンバージョン

ダウンタイムを最小限にすることは、変化の激しい市場で業務を行っている組織にとって極めて重要です。暗号化のためにサーバを数時間または数日ダウンさせることは、業務に大きな影響を与えることになります。そのため、WinMagic SecureDoc Linux for Servers では、お客様に以下のような機能を提供しています。

- 暗号化を開始する前にディスクを完全に消去したり、暗号化を有効にした上で Linux を再インストールする必要がなく、インストールされている Linux サーバを暗号化できます。
- 貴重な時間と費用を節約して暗号化導入の失敗を回避できます。

暗号化されたシステムのパスワードと鍵管理を一元化

シンプルなパスワード管理、暗号化された Linux デバイスの運用と管理は非常に重要です。さらに重要なのは、このような機能を一元的なコンソールで提供でき、コンソールから暗号鍵と復旧に必要な情報のバックアップを提供できるようにすることです。

- WinMagic SecureDoc Enterprise Server (SES) によるすべてのサーバとデバイスの一元的な管理。
- デバイスのセキュリティが侵害された場合やデバイスの利用目的を変更する場合、暗号鍵を削除します。(この操作は、コンプライアンス上の理由から記録する必要があります)

コンプライアンス対応の強化

GDPR や HIPAA などのデータ保護規制のもとでコンプライアンスを遵守できない場合に極めて重大なペナルティが科せられる企業には、Linux ベースおよび Windows ベースのサーバのすべてについてシームレスで統合された鍵管理ソリューションが不可欠です。WinMagic SecureDoc を使用すると、暗号化されたサーバの運用、管理、および復旧のすべてが単一のコンソールから可能になります。単一の画面で各サーバの暗号化のステータスを確認してデータが保護されていることを確認できるため、監査担当者や経営幹部は確実にコンプライアンス監査に合格できる確信を得ることができます。

- データ暗号化によりコンプライアンス対策を強化。
- わかりやすい単一画面で、サーバ、エンドポイント、仮想マシンの暗号化のステータスを即座に可視化。
- 扱いやすい監査およびレポートツールによってコンプライアンスニーズに迅速に対応。

SD Linux for Servers の機能

- 暗号化の処理中に管理者とユーザがログインしてマシンで作業できるようにするライブコンバージョン
- 暗号化を開始する前にディスクを消去して OS を再インストールする必要性を排除するシンプルな暗号化
- データを安全に維持するために必要な追加のセキュリティ対策であるネットワークベースのプリブート認証
- Linux デバイスの運用、管理、および復旧のすべてを単一のコンソールから可能にするエンタープライズクラスの管理機能

暗号化対象 Linux ディストリビューション



WINMAGIC®

ウインマジック・ジャパン株式会社

〒105-0022 東京都港区海岸 1-2-3 汐留芝離宮ビルディング 21 階

TEL.03-5403-6950 FAX.03-5403-6953



sales.jp@winmagic.com | www.winmagic.com/jp