



ローカルアカウントのパスワード管理

問題発生：第三者のログインによる PC 情報漏えい

社内のPCには重要な情報が含まれています。

未使用時にはスクリーンセーバを起動するよう設定する、離席の際にはログアウトを義務付けるなどを行っても強力なパスワードを使用していない限り第三者からログインされる危険性は常に存在します。

アクティブディレクトリなどの普及によりドメインのパスワードポリシーは容易に一元管理できるようになりましたが、ローカルのアカウントに対しても同様の管理が求められます。



対策

第三者に容易にログインされないようにするには、ローカルのアカウントにも以下のようなパスワードポリシーを適用する必要があります。

- 複雑なパスワード使用の徹底
- 定期的なパスワードの変更
- パスワード再利用の回避



LANDeskだと実現できます

LANDesk® Security Suiteはローカルアカウントのパスワードを一元管理するための機能を提供します。管理者は次の項目においてローカルアカウントのポリシー定義することが可能となります。定義に準じていないクライアントを検出し、ポリシーを強制適用することでローカルのアカウントの安全性を維持します。

- パスワードの履歴を記録する
 - 履歴の数(過去のパスワード再利用の制限)
- パスワードの有効期間
 - 日数
- パスワードの長さ
 - 文字数
- パスワードが要求する複雑さを満たす
 - 有効かどうか