

機密保持サーバ保護を見直しませんか？

多くの企業では、個人情報等のデータが存在する特権アカウントでしかアクセスできない機密性の高いサーバを所有しています。ただ、ID・PWのみで制限するだけでは安心はできません。

不正アクセス防止の為に、UserLockのMFAで機密保持サーバの保護をはじめませんか？

重要な情報等を格納している機密保持サーバを保護して安全に運用したい皆様にUserLockはお勧めです。

UserLockはActiveDirectoryと連携し、Windowsアカウントにログインする際に、MFAをはじめとした各種ログイン制御を行うことができます。

機密保持サーバの業界別利用シーン

医療業界



電子カルテ

会計システム

研究データ

製造業界



新製品の情報

製品の機密情報

顧客情報

金融業界



顧客情報

企業情報

クレジットカード情報

簡単に導入可能な『UserLock』の
導入ステップ・ユースケースを裏面で確認



UserLock導入ステップ

Step1

インストール

メンバーサーバーにUserLockをインストール。
最小構成だと最短5分でセットアップ可能です。

Step2

機密保持サーバへUserLockエージェントを配布

管理コンソールから対象サーバを選択し、
ワンクリックでエージェントを配布できます。

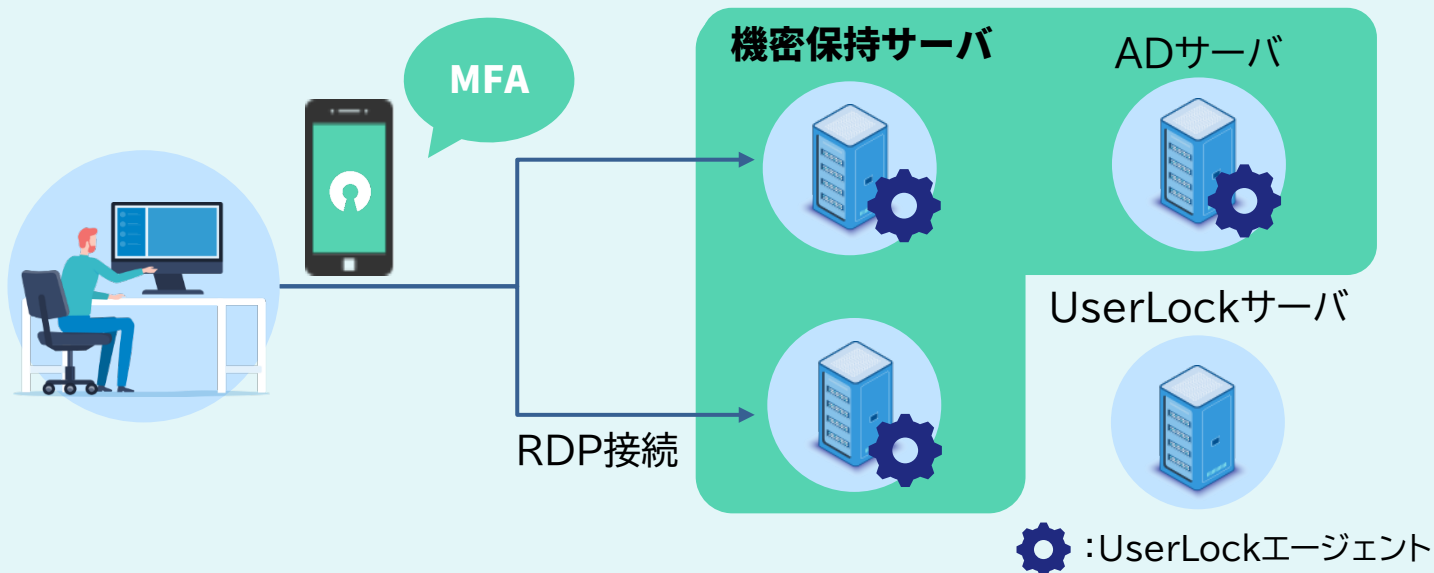
Step3

グループへのアクセスポリシーの設定

管理コンソールから対象サーバへログインするADグループ
(OU, アカウトも可)に対して多要素認証等のアクセス
ポリシーを設定します。



UserLockのユースケース



直接ログインもRDP接続も
まとめてMFAを提供

許可された時間帯以外の
ログインを禁止

ユーザ毎に機密保持サーバへ
ログインできる端末を制限

ログイン失敗を繰り返すユーザーを
ハイリスクユーザーとして検知

参考価格(年間サブスクリプション形式)

※その他レンジの価格や詳細については別途お問い合わせください。

20ライセンス	¥137,400
50ライセンス	¥316,000
100ライセンス	¥550,000

OCEANBRIDGE

株式会社オーシャンブリッジ

〒107-0051 東京都港区元赤坂1-5-12 住友不動産元赤坂ビル7F

<https://www.isdecisions.jp/>

userlock@oceanbridge.jp