いまサイバー攻撃・内部不正の標的としてRDPが狙われている!!

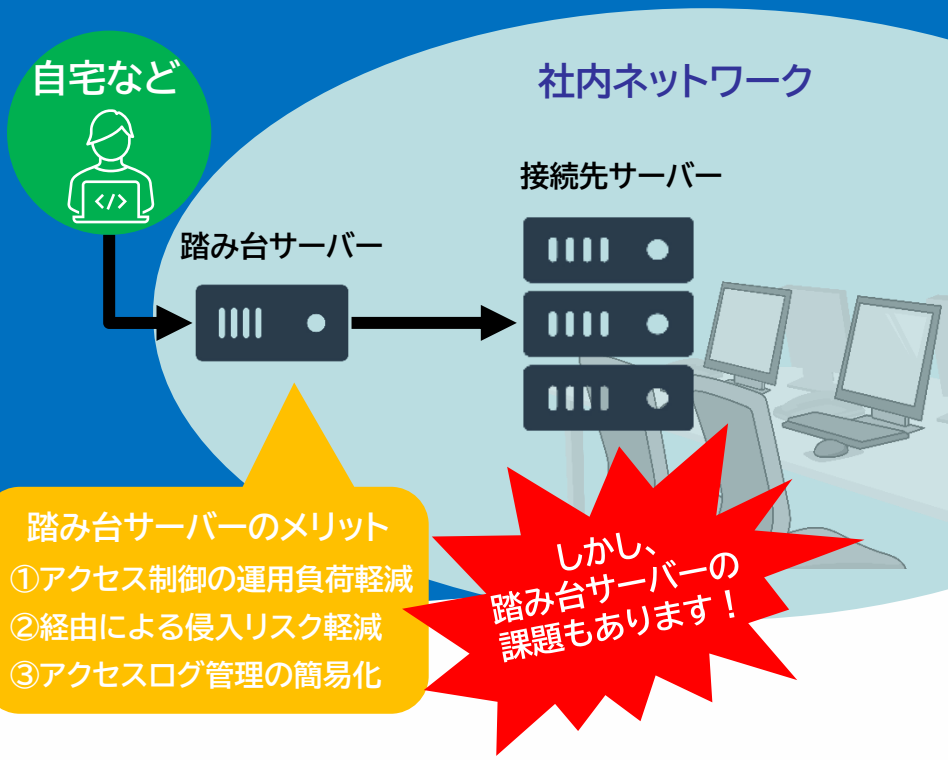
UserLock

踏み台サーバーを経由したRDP接続のセキュリティリスクをゼロトラスト視点で強化

リモートデスクトップ

リモートワークの増加により、企業の利用が急拡大しているのがリモートデスクトップ(RDP)サービスです。
RDPでは目的のサーバーに接続する際に、不正アクセスのターゲットとなるリスクを避けるため、
踏み台サーバーと呼ばれる中継サーバーを経由する方法が推奨されています。
この踏み台サーバーを活用することで、
①アクセス制御の運用負荷軽減
②経由による侵入リスク軽減
③アクセスログ管理の簡易化
といったメリットがあります。

しかし、年々高度になるサイバー攻撃や、
情報漏洩の主な要因となる内部不正の
リスクを考えた場合、
ゼロトラスト視点、つまりネットワークの外部、内部を問わずアクセスを脅威と捉え、認証を強化するセキュリティが求められています。



踏み台サーバーのメリット
①アクセス制御の運用負荷軽減
②経由による侵入リスク軽減
③アクセスログ管理の簡易化

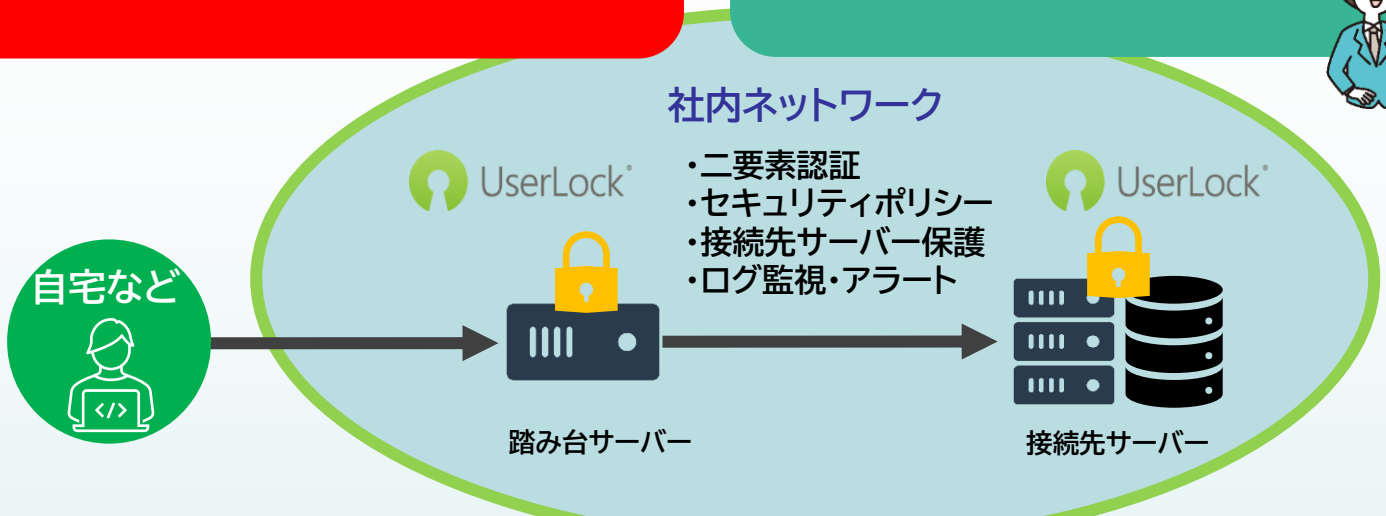
しかし、踏み台サーバーの課題もあります！

踏み台サーバーの課題

△ID・パスワード認証のみでは不十分
△深夜・休日など業務時間外のアクセス拒否ができない
△アクセス状況の可視化ができない
△なりすまし・内部不正対策が不十分

UserLockのソリューション

◎多要素認証や柔軟なセキュリティポリシー設定
◎踏み台だけではなく、接続先サーバーも保護
◎アクセス状況のリアルタイム監視
◎不審なアクセス検知とアラート発出



認証強化・アクセス管理ツール「UserLock」が解決します。裏面をチェック！

UserLock

Windows Active Directoryと連携するログイン管理ツール
既存のセキュリティ環境を変更せずに、セキュリティを強化！

二要素認証や柔軟なセキュリティポリシー設定

スマホアプリやハードウェアトークンによる多要素認証や、さまざまな条件による柔軟なアクセス制御が可能です。
企業のセキュリティポリシーや利用状況に合わせて、安全性と業務効率のトレードオフを調整することが可能です。

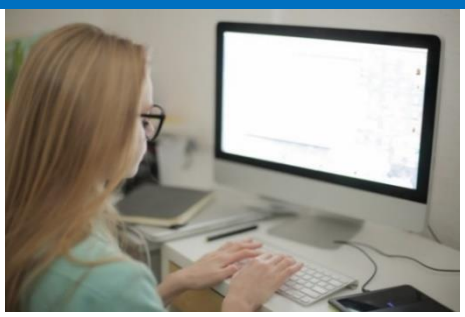
- ◎ 同時ログイン制御（複数人による同一ID利用禁止）
- ◎ 接続種類（社内外・ローカル・RDPなど）
- ◎ 接続元（端末・IPアドレス・組織・国）
- ◎ 時間（曜日・時間帯・接続時間）

踏み台だけではなく、接続先サーバーも保護

踏み台サーバーはもちろん、標的となりうる接続先サーバーにも多要素認証やセキュリティポリシーを設定し、保護することが可能です。
仮に踏み台サーバーなどを経由して異なる経路で接続先サーバーに同時アクセスがあった場合や攻撃対象となり易い放置セッションがあった場合の対応も可能です。

アクセス状況のリアルタイム監視と緊急時のアラート

踏み台サーバーだけでなく、その先にある接続先サーバー、さらにネットワーク全体で発生しているログイン状況をリアルタイムで把握することができます。
複数の端末やサーバーを経由したアクセスのトラッキング、不正が疑われるログイン試行の検知やアラート発出、アクセス遮断や強制ログオフなど、不正の被害を最小限に抑える機能を搭載しています。



※踏み台サーバー(Windowsサーバー)の代替として、RD-WebやRD-Gatewayを利用する場合も、多要素認証のカスタマイズ等、UserLockでセキュリティを強化できます。

参考価格（年間サブスクリプション形式）

10ライセンス	￥68,700
50ライセンス	￥316,000
100ライセンス	￥550,000

※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。

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/
fileaudit@oceanbridge.jp