UserLock® ホワイトペーパー

近年急増するリモート接続(VPN/RDPなど)を狙ったサイバー攻撃に、既存インフラを極力変えず、サクッと対応するには？

OCEANBRIDGE

急増するリモート接続（VPN/RDPなど）のセキュリティリスク

リモートワークのセキュリティ

新型コロナウイルスによる感染症に拡大により、世界規模でリモートワークの必要性が大きく高まり、これまでリモートワークを行っていなかった数多くの企業でも実施されています。しかし緊急的に十分な準備なしでリモートワークを導入することは、セキュリティ上の大きな懸念となります。

MicrosoftのRDP（リモートデスクトッププロトコル）は、PC端末へのリモートデスクトップを許可するために使用されます。このプロトコルは 非常に使いやすく、ほとんどのバージョンのMicrosoft Windowsに組み込まれているため、リモートデスクトップツールの中で、もっとも広く実装されているといえます。 リモートワークを実現するための強力かつ便利なビジネスツールではありますが、セキュリティ面を考慮すれば、RDPだけでは十分とは言えません。

まず、リモートデスクトップが安全な仮想プライベートネットワーク（VPN）経由で行われることで、アクセスの制限が可能です。 次に、RDP、VPNと併用可能な二要素認証（2FA）を導入することで、従来のパスワード認証よりもセキュリティ強化が可能となります。

リモートワークのリスクとは？

IT部門は、専門家として、リモートワークが非常に有益であることを理解していますが、同時にリモートワークによって起こるリスクがあるということもわかっています。

ある調査によれば、IT部門の92%がリモートワークのメリットよりも、リスクの方が上回っていると考えています。回答者の90%がリモートワークの導入にあたり、リモートワークを行う従業員によるセキュリティリスクが発生すると考えており、54%は出社して働く場合よりセキュリティリスクが高いと考えています。

安全性が未確認のネットワークや、産業スパイやハッキングのリスク、さらには従業員による内部不正のリスクなど、リモートワークに関わるリスクは、最終的に、ITが企業ネットワークと機密情報へのアクセスを安全に確立できる方法に関係します。

リモートワークを保護するためのステップ

まずはITに関わるセキュリティリスクについて、従業員の知識と意識を高めることが重要です。
そして具体的には、各従業員が遵守すべき下記の5つのステップがあります。

1

VPNの使用

VPNを使用することで、リモートデスクトップと企業ネットワークの間に安全なトンネルを開くことが可能です。

2

VPN接続への安全なアクセス

IT部門の管理者は指定された社用端末以外のVPNアクセスを制限できるようにして、社外からの安全な接続を可能にする必要があります。

3

VPNセッションの二要素認証

VPN経由で機密性の高いデータへのアクセスを許可する際に、二要素認証（２FA）で本人確認を強化することは、なりすましなどで、ハッカーが企業ネットワーク内にアクセスするのを防ぐための重要なポイントとなります。

4

すべてのRDPセッションの監視と管理

すべてのRDPセッションを監視できるソリューションを導入することで、不正アクセスを検知した場合に、リアルタイムのアラートと自動対応が実行され、実害が起こる前に対処することが可能となります。

5

RDPセッションの二要素認証

二要素認証（2FA）は、Windows環境へのユーザーアクセスを保護するのに有効な手段であり、リモート環境ではさらに重要性が高くなります。ネットワーク上の端末にRDPまたはVPNで接続するユーザーは2FAを使用して本人確認を行う必要があります。

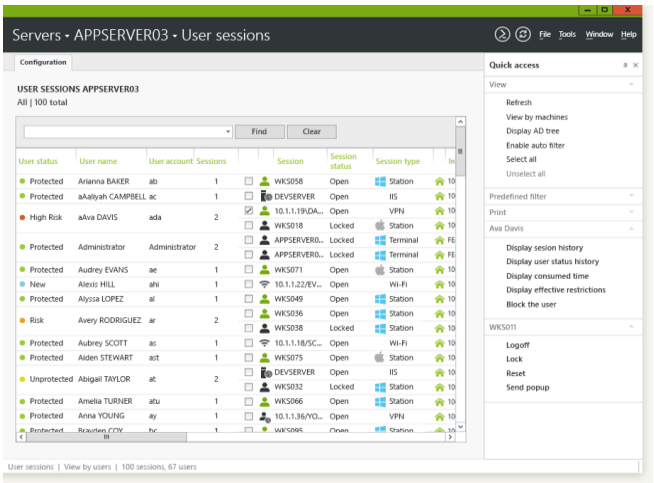
RDP & VPNセッションを保護するソリューション

リモートワークやモバイル端末での社内ネットワークへのアクセスはすでに一般化しつつあります。これに伴い、セキュリティのリスクは増大し続けていますが、UserLockはこのようなリスクを軽減し、不正なアクセスや怪しいアクセスから社内ネットワークを保護します。

既存のインフラを活用して導入できるUserlock

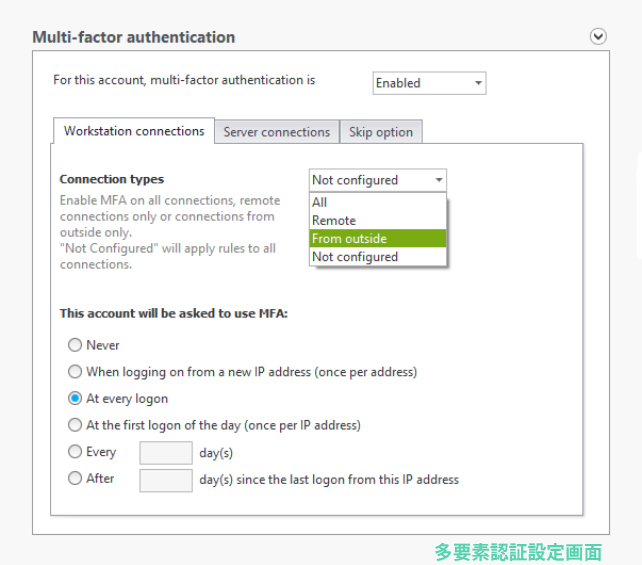
UserLockのソリューションは、Windows Active Directoryと連携、既存のインフラを活用することで、従業員の業務の妨げにならず、そしてIT部門にも混乱を招かないように導入が可能です。リモートワークを行うユーザーだけでなく、オンプレミスのアクセスを含むすべてのユーザーログインの管理と保護を実現します。

- 特定の許可された端末へのユーザーアクセスのみを許可することにより、VPN接続を保護を実現
- UserLockコンソールから直接ユーザーセッション（RDP / VPNを含む）を監視して対応



Userlockコンソール

- すべてのWindowsログインとRDPおよびVPNセッションで2要素認証を有効化
- 社内ネットワーク外部からのRDP接続、もしくは内部または外部からのRDP接続に2要素認証を適用

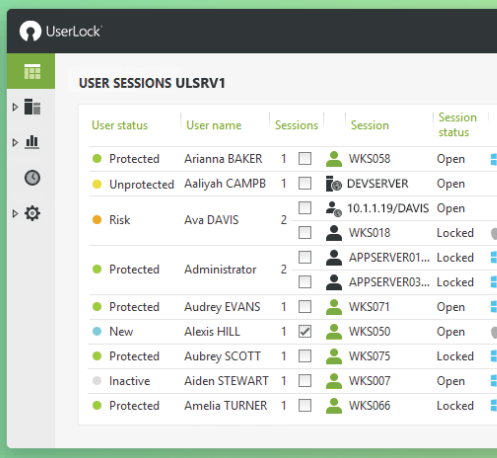


多要素認証設定画面

OceanBridge

UserLock®

UserLockは、社内ネットワーク（LAN）に接続しているユーザーと端末を一元管理するActive Directoryと連携して、ユーザーのログインを簡単に管理できるログイン見える化ソリューションです。
使いやすいインターフェイスと、さまざまな機能で簡単にセキュアなログイン管理を実現します。



UserLockの主な特長と機能

二段階認証の簡単導入

通常のログインやリモートデスクトップ接続で、二段階認証を簡単に導入にできます。

多重ログインの制限

多重ログインはセキュリティ上の問題の要因となります。同一アカウントの同時ログインを制限します。

ログイン端末の制限

ログインを端末やIPアドレスなどで制限してグループ全体を一元的に管理します。

ログイン時間の設定

ログイン可能な時間帯や曜日、上限時間の設定など、個別の業務形態、時間に合わせた運用を行うことが可能です。

接続方式によるログイン制限

Wi-Fi、VPN、IISなどのさまざまな接続方式によるログインの制御が行えます。

ログイン状況の監視

すべてのユーザーのログイン状況をモニタリングして、ログインの挙動に関してアラートを設定することも可能です。

強制ユーザーログオフ

社内ネットワークやリモート接続上で不審なログインや放置されたログインなどを強制的にログオフできます。

ログイン履歴の監査レポート

パスワードのリトライや正規ルールではないログイン試行などを含むアクセスイベントの監査レポートを提供します。

フル機能を無料で30日間お試しいただける体験版もご用意しております。
下記サイト、またはuserlock@oceanbridge.jp (UserLock担当)まで
お気軽にお問い合わせください。

■製品情報サイト　：https://www.isdecisions.jp/userlock/
■体験版お申込み　：https://www.isdecisions.jp/trial
■製品お問い合わせ：https://www.isdecisions.jp/contact

OCEANBRIDGE
つかえるITを、世界から。

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