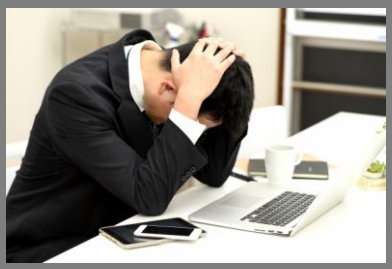
UserLock® ITガバナンスを支援するアクセスセキュリティ強化ツール

# テレワーク×VPNを狙った
# 不正アクセスによる情報漏洩事故が多発！
# 急務となる二段階認証導入＋αとは？

VPN接続はインターネット経由で社内ネットワークにアクセスできる非常に便利な方法です。しかし、利便性がある反面、VPNのIDやパスワードが流出した途端にどこからでも、誰でも社内ネットワークに侵入できてしまうという危険性もあります。実際に、多くの日本企業のVPN接続情報が大量に流出していることが発覚し、多くの報道機関で取り上げられました。テレワークでのVPN需要が高まる中、VPNに対する信頼性とセキュリティ対策が急務となっています。

## VPNの認証情報が流出してしまうと…

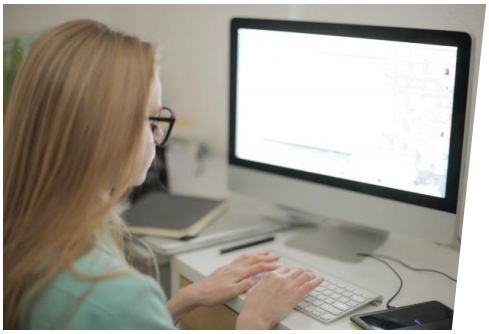
侵入者は盗んだ『IDとパスワード』を利用し、社内の端末やサーバーへのアクセスが可能となるため、企業の営業秘密や個人情報の窃取、業務の妨害を引き起こし、想像できないほどの莫大な損害を企業に与えます。



## セキュアなVPN接続を実現するための条件とは？

### 二段階認証

VPN接続の利便性を維持しつつ、セキュリティを強化するためには、モバイル端末を活用した二段階認証の導入が有効です。通常のIDとパスワードによる認証に二段階認証を追加することで、仮にアカウント情報が流出しても、不正ログインを防ぐことが可能となります。



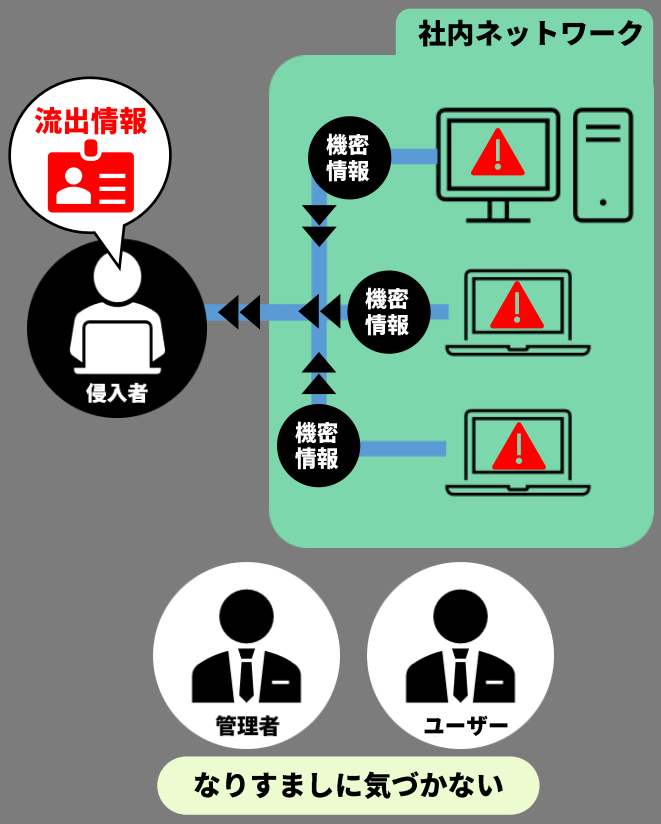
### アクセス管理とアラート通知

社内の端末やサーバーへのアクセス管理機能により、不正ログインが起こった場合、対象の端末へのアクセス制限や強制ログオフなどを行うことで、被害を最小限に留めることができます。
また、不審なアクセスがあった場合にアラートを通知する機能があることで迅速な初期対応が可能となります。

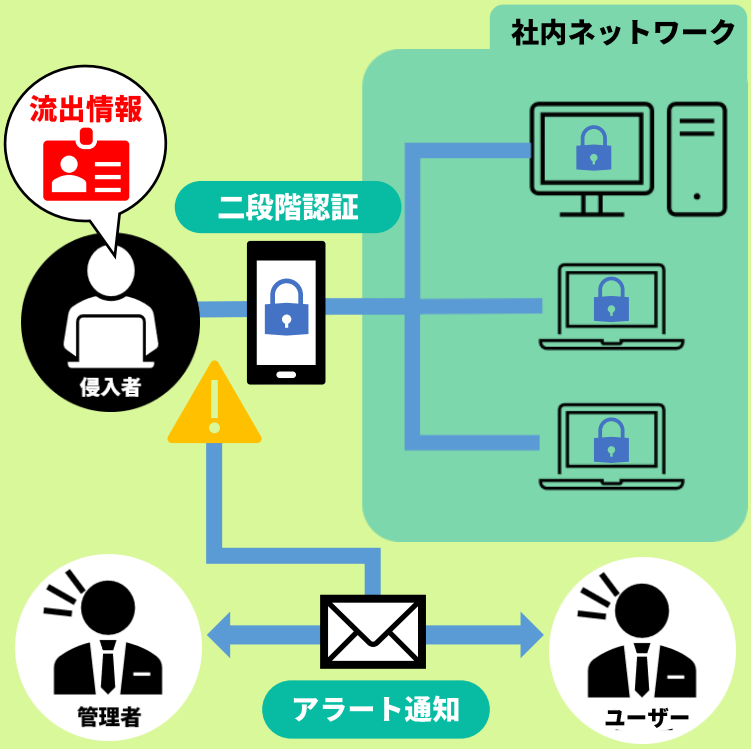
UserLock® ITガバナンスを支援するアクセスセキュリティ強化ツール

# UserLockで安全なネットワーク利用を実現

## 通常のVPN




## UserLock




# UserLock独自の【予防・確認・対応】で多層的に保護

## 【予防】


VPN経由の社内ネットワークへのログインに二段階認証を簡単に付加することが可能で、アクセス管理機能と組み合わせることで、強固な認証ルールが設定可能です。

## 【確認】


端末や時間、接続方法（RDPやVPN）によってユーザーアカウントの利用を管理できます。社外からの不正アクセスだけでなく、内部でおきるアカウントの不正利用にも有効です。

## 【対応】


パスワード間違いや許可されていないアクセスがあった場合にアラートを通知します。ユーザーアカウントの利用状況をリアルタイムで通知することで特権IDの不正利用にも対応できます。

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