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

Windowsログインソリューション
UserLock®

テレワーク環境を守る4つのセキュリティチェックポイント

狙われる脆弱なテレワーク環境

国内では依然として新型コロナウィルス第二波の脅威が高まっており、企業においてテレワーク環境の構築は喫緊の課題となっています。ただ、業務の遂行を最優先にした急場のテレワーク環境では、セキュリティリスクにさらされるケースが多くなります。このような隙を狙ってサイバー犯罪者は社内ネットワークに入り込むためのログイン認証情報を盗み、システムからシステムへ横移動しながら価値あるデータを探します。ある海外セキュリティ機関の調べでは、実際に不正アクセスを受けてからその侵入に気付くまで平均して191日もの時間がかかっているとの報告があり、このような攻撃には気付きにくいのが実情です。

Active Directoryは“セキュリティツール”ではない

長く利用されているログイン基盤のActive Directoryだけでは、テレワークのセキュリティが万全とは言えません。実際に「新型コロナ感染症に関する重要なお知らせ」や「新型コロナ感染地域マップ」といった件名のフィッシングメールでログイン情報を盗もうとする事件も起こっています。しかし、多くの企業のActive Directoryのログインは、『IDとパスワード』だけでしか守られていない状態です。テレワーク環境と社内ネットワークの守るためには、外部からのアクセスに二段階認証を追加する、不審なログインが起きていないかをチェックする、といったことが非常に重要になってきます。

テレワーク環境を守る４つのチェックポイントとは？（裏面へ）

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

テレワーク環境を守る４つのチェックポイント

テレワーク環境における４つセキュリティチェックポイント	セキュリティポイントを遵守できるUserLockの機能
① 許可されてない端末のVPN接続を制限 VPN接続を許可する端末をしっかりと管理することで、ID・パスワードが漏れたときにも、ネットワーク内に侵入されるリスクを低減することが可能です。	端末のログインコントロール  ログインを端末や接続方式、時間帯などで制御することでグループ全体を一元的に管理します。
② リモート接続に二段階認証を追加する サイバー犯罪者が巧妙な手口で社内ネットワークにアクセスできるようになったとしても、二段階認証があれば最終的に不正ログインされるリスクは大幅に軽減できます。また、同僚のアカウントを利用し不正アクセスを行う内部不正に対しても有効です。	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。
③ アクセスログの記録と監査を可能にする ネットワーク全体に渡ってアクセスの履歴を日常的に取得することで、どの端末から、どのアカウントを利用して、最終的にどのサーバーに不正にアクセスされたのか、などを把握することができます。	ログイン履歴の監査  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。
④ 外部からのアクセスや重要な端末へのアクセスを監視する 「いつもと違うPCからアクセスしている」、「ログインのときに何度もパスワードを間違えている」など、不審なアクセスがあった場合に自動でアラートを発報し、すぐに接続を遮断できる体制を作ることで不正アクセスの被害を未然に防ぐことができます。	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。

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