UserLock

リリースノート

Version 12.1

IS Decisions

UserLock リリースノート

バージョン：12.1

2024/7/8 版

株式会社オーシャンブリッジ

製品紹介ページ： https://www.isdecisions.jp/userlock/
技術情報ページ： https://ulsupport.oceanbridge.jp/portal/ja/home/
営業担当連絡先： userlock@oceanbridge.jp
技術サポート連絡先： ul-support@oceanbridge.jp

目次

1. 本書について....3
2. 新機能/廃止機能....3
2-1. 新機能....3
2-2. 廃止機能....4
3. 既知の問題と制限事項....4
3-1. 既知の問題....4
3-2. 制限事項....4
3-2-1. IIS セッションに関する制限事項....4
3-2-2. VPN セッションに関する制限事項....5
3-3-3. Wi-Fi セッションに関する制限事項....6
3-3-4. SaaS セッション（SSO セッション）に関する制限事項....7
3-3-5. MFA に関する制限事項....8
3-3-6. その他の制限事項....8

1. 本書について

本書は、IS Decisions 社製品「UserLock」バージョン番号：12.1 にて新規追加/廃止される機能、および既知の問題と制限事項をオーシャンブリッジ社にてまとめたものです。

2. 新機能/廃止機能

2-1. 新機能

以下の機能が新しく追加されました。

- **RemoteApp に対する MFA とアクセス管理**
  RemoteApp セッションへの保護が正式リリースとなりました。

- **セッションタイプ別の MFA**
  12.0 まではワークステーション・サーバー接続の二種類での MFA の設定が可能でしたが、12.1 からセッションタイプ（ワークステーション・サーバー・IIS・VPN・SaaS）ごとに MFA の設定を行えるようになりました。

- **日・時・分単位での MFA の頻度設定**
  MFA の頻度設定が、日・時・分単位で行えるようになりました。

- **新しい構成ウィザード**
  構成ウィザードのデザインが変更され、より簡単に Web アプリケーション・
  IIS MFA 機能・UserLock Anywhere の設定を行えるようになりました。

- **コンピュータコマンドの追加**
  Agent Distribution メニューでマシンに対して実行できるコマンドとして「Check agent status（エージェントステータスの確認）」と「Check machine（マシンの確認）」が追加されました。

- **IIS イベントの記録**
  UserLock サーバーに接続できない場合、IIS のイベントログをデスクトップエージェントログに記録するようになりました。

- **UserLock Anywhere のプロキシ経由での接続のサポート**
  プロキシ経由で UserLock Anywhere に接続する場合、以前まではプロキシの IP が取得されていましたが、詳細設定の「IISProxyList」にプロキシサーバーのアドレスを設定することで、クライアントの IP を取得できるようになりました。

- **【UserLock Push アプリ】プッシュ通知の履歴表示**
  プッシュ通知の承認・拒否の履歴が確認できるようになりました。本機能を利用する場合はお手持ちのスマートフォンの「UserLock Push」を最新版（1.3.0 以降）にアップグレードしてください。

2-2. 廃止機能

廃止された機能はありません。

3. 既知の問題と制限事項

3-1. 既知の問題

- **Web アプリケーション（Web 版コンソールアプリ） インストール時の問題**
  WEB アプリケーションは専用の構成ツールでインストールすることができますが、特定の条件にあてはまると正しく動作しなくなります。
  問題の詳細と回避方法は以下のナレッジベース記事をご覧ください。
  https://ulsupport.oceanbridge.jp/portal/ja/kb/articles/webapp-internal-server-error

- **時間割り当て制限のキャリーオーバーに関する問題**
  時間割り当て制限（Time quotas）では、定められた期間内に割り当て時間を消費しきれない場合に次の期間に持ち越すことを可能にするオプションがあります。しかし現在はこのオプションを有効化しても、持ち越し対象の期間が正しく算出されない問題が報告されています。

3-2. 制限事項

UserLock では計 5 種類のセッション（対話型、IIS、VPN、Wi-Fi、SaaS）を監査対象とすることができますが、すべてのセッション種別ですべての監査項目やオプション機能が同じように有効になるわけではありません。セッション毎の性質や、ご使用のインフラ機器によっては有効にならない監査項目やオプション機能がある点にご注意ください。

なお、ここでは主要な制限事項のみをまとめて把握できるよう、各ドキュメント内で提示されている制限事項をピックアップしています。各セッション/各機能の細かい制限事項は他にもありますので、実際にご利用になる際は各ドキュメントを参照してください。

3-2-1. IIS セッションに関する制限事項

- 接続元情報の取得
  接続元マシンのホスト名が取得できるケースは限定されています。ホスト名が取得できない場合、ワークステーション制限は IP アドレスベース制限のみが有効となります。

- セッションログオフとセッションタイムアウト
  明示的なログオフ操作のある WEB アプリケーションでない限り、UserLock は IIS セッションのログオフを検出できません（単に Web ブラウザを閉じた場合はログオフにはなりません）。
  ログオフに対応していない IIS のセッションは、規定のタイムアウト時間に達した時にクローズされます。このタイムアウト値の変更方法はリファレンスガイドを参照してください。

- 監査対象アプリケーションの指定
  IIS Web サイトで UserLock IIS エージェントを構成する際、デフォルトではサイト上のすべてのアプリケーションが監査対象となります。監査の対象を Web アプリケーション単位で設定する方法は、リファレンスガイドを参照してください。

- 監査対象ユーザーの指定
  IIS Web サイトで UserLock IIS エージェントを構成する際、デフォルトではアプリケーションのすべてのユーザーが監査されます。監査の対象を Web ユーザー単位で設定する方法は、リファレンスガイドを参照してください。

- 時間経過による強制ログオフ
  時間帯制限でログオンを許可された時間枠を逸脱した場合や、時間割り当て制限で割り当て時間に到達した場合のために、強制的にセッションをログオフさせるためのオプションがあります。これらは対話型セッションでのみ有効であり、IIS セッションでは時間経過に伴う強制的な自動ログオフを行うことはできません。

※IIS セッションに関する制限について、詳しくは「UserLock リファレンスガイド」の「5-3-4. 既知の制限事項と追加設定」をご参照ください

3-2-2. VPN セッションに関する制限事項

- 接続元情報の取得
  一般的に RADIUS プロトコルでは、接続元クライアント名を復元することはできません。その結果、クライアント名を使用したワークステーションの制限を適用することはできません。この名前を使用できる唯一の既知のケースは、RRAS サーバーが RADIUS 認証と RADIUS アカウンティングで構成されている場合です。
  また、VPN クライアントの IP アドレスは、すべての RADIUS クライアント（ハードウェアルータ）から提供されるわけではないため、IP アドレスによる制限を実施できない場合もあります。

- 複数の RADIUS サーバーの使用
  1 つの RADIUS クライアント（ハードウェアルータ）に対して複数の RADIUS サーバーを使用すると、ログオフとは別のエージェントでログオンが管理される可能性があるため、対応していません。

- ログオン不可時のメッセージ
  VPN セッションのログオンが UserLock によって拒否されると、ユーザーは新しい認証情報の入力を求められます。現在のところ、ユーザーに対してより分かりやすいメッセージを表示する方法はありません。

- 強制ログオフ
  VPN セッションは強制ログオフに対応していません。

- UserLock と互換性のあるハードウェアルーター
  現在のところ、UserLock と互換性のあるすべてのハードウェア ルーターを示すハードウェア互換性リストはありません。そのため、ご使用のハードウェアデバイスを UserLock でテストすることをお勧めします。

※VPN セッションに関する制限について、詳しくは「UserLock リファレンスガイド」の「1-2. VPN セッション」をご参照ください。

3-3-3. Wi-Fi セッションに関する制限事項

- 接続元情報の取得
  一般的に RADIUS プロトコルでは、クライアント名を復元することはできません。そのため、クライアント名を使用してワークステーションの制限を適用することはできません。

- セッションクローズを検知できない場合の制限
  Wi-Fi セッションを適切に閉じずに Wi-Fi クライアントの電源が切れたときに、Wi-Fi アクセスポイントが RADIUS サーバーにセッションの終了を正しく通知しないと、Wi-Fi セッションの制御が信頼できなくなることがあります。

- コンピューターアカウントによる認証
  Wi-Fi クライアントが Active Directory ドメインのメンバーである場合、Wi-Fi セッションはユーザーアカウントではなくコンピューターアカウントで認証されることがあります。この場合、UserLock はセッションを管理しません。UserLock はユーザーアカウントのセッションのみを管理し、コンピューターアカウントのセッションは管理しません。

- 複数の RADIUS サーバーの使用
  1 つの RADIUS クライアント（ハードウェアルーター）に対して複数の RADIUS サーバーを使用することはサポートしていません。ログオフとは別のエージェントでログオンが管理される可能性があるためです。

- ログオン不可時のメッセージ
  Wi-Fi セッションのログオンが拒否されると、ユーザーは新しい認証情報の入力を求められます。

現在のところ、ユーザーにより分かりやすいメッセージを表示する方法はありません。

- UserLock と互換性のあるハードウェアルーターと Wi-Fi アクセスポイント
  以下の通りです：
  ・Wi-Fi アクセスポイント： Cisco Aironet 1700(AIR-CAP1702I-E-K9)
  ※このリストは、特定のデバイスとの互換性を確認できた場合に追加されるものであり、すべてを網羅しているわけではありません。そのため、ご使用のハードウェアデバイスを UserLock でテストすることをお勧めします。

※Wi-Fi セッションに関する制限について、詳しくは「UserLock リファレンスガイド」の「1-2. Wi-Fi セッション」および「5-2-4. 既知の制限事項と追加設定」をご参照ください。

3-3-4. SaaS セッション（SSO セッション）に関する制限事項

- ログオフの検知
  SaaS セッションはログオフを検知できません。SaaS アプリケーションで明示的にログオフ操作をした場合でもログオフイベントは記録されません。

- レポートに関する制限
  SaaS セッションに接続された時間は、「労働時間レポート」「同時接続セッションの履歴レポート」には含まれません。

- 同時接続セッション数の制限
  同時接続を許可するか否かの設定はできますが、他のセッション種別のように接続許可セッション数を指定することはできません。

- 時間経過による強制ログオフ
  IIS セッションと同じく、時間経過に伴う強制的なログオフを行うことはできません。

- 接続元情報の取得
  クライアント名を復元することはできないため、ワークステーション制限は IP アドレスによる制限のみ行えます。

- 時間割り当て制限
  Saas アプリケーションに接続している時間は含まれません。

※SaaS セッションに関する制限について、詳しくは「UserLock リファレンスガイド」の「1-5. SaaS セッション」をご参照ください。

3-3-5. MFA に関する制限事項

- MFA の対象セッション種別
  MFA では対象のセッション種別を指定することはできません。

- MFA 認証にハードウェアトークンを使用する場合の制限
  ハードウェアトークン（Token2、YubiKey）の MFA 認証の構成は RDP セッションでは行えません。コンピュータへの物理接続が必要です。また、仮想マシンに関しても使用制限があります。
  詳細は「UserLock ユースケース」の「1. Multi-factor Authentication (MFA:多要素認証)」内、ユーザーオンボーディングについての案内をご参照ください。

- MFA と他の監査項目が同時に有効化されているときの制限
  MFA コードが正しく入力されているにもかかわらず、別の UserLock 制限が接続を拒否している場合、UserLock MFA レポートで MFA コードが正しく入力されたというイベントを確認することはできません（これは UserLock サービスのログでのみ確認できます）。

- バックアップ手段にプッシュ通知を指定した場合の制限
  MFA の認証手段のうち、プッシュ通知による認証をバックアップ手段として指定した場合、MFA コードの入力を求められるたびにプッシュ通知アプリに通知が届きます。これは止めることができません。
  MFA のバックアップ手段にはプッシュ通知を指定しないことをお勧めいたします。

- VPN セッションの MFA
  VPN セッションに MFA を構成すると、VPN を介して共有フォルダーにアクセスするときに、ユーザーは資格情報の入力を求められます。
  詳細は、「UserLock ユースケース」の「1-3-2. RRAS 方式による VPN/MFA」を参照してください。

- スタンドアロンモードでの MFA
  スタンドアロンモードでお使いの場合は、プッシュ通知機能はご利用いただけません。

3-3-6. その他の制限事項

- ActiveDirectory によるログオン拒否
  Active Directory によって拒否されたログオンは一部検出できないものがあります。詳細は「UserLock リファレンスガイド」の「7-3. Active Directory によるログオン拒否」を参照してください。