重要

2022 年 01 月 28 日　更新

WinKeeper TB v1.8（利用シーン機能）運用注意事項

本紙では、WinKeeper TB において「利用シーン」機能をご利用されるお客様へ、運用・設定の際の注意事項をご説明します。
本紙は以下で構成されております。

・はじめに
・事前準備について
・機能一覧と初期設定内容について
・「システム監視」各設定項目の注意事項
・制限事項

はじめに

WinKeeper TB では、「利用シーン」機能においてセキュリティ対策の設定を行います。
ポリシー違反によりアクションが発動する機能が搭載されていますが、通常運用ではアクションが発動しないよう、また不意の出来事でアクションが発動した際は適切に解除／対処ができるようユーザ様と認識を合わせておく必要があります。
基本的に、【ポリシー違反の抑止効果を高めるような設定／環境づくり】を行うことが重要となります。
※ユーザ様の環境に合わせ、運用に即した各「利用シーン」の設定をしてご利用下さい。

事前準備について

■　利用シーンの設定と WinKeeper の保護環境の関係について

「利用シーン」の設定は、WinKeeper の保護機能と連動しておりません。
このため、以下の点についてご注意ください。
・WinKeeper の保護状態に関係なく、「利用シーン」が適用されている場合、該当のポリシー監視が作動しています。
※「USB デバイス接続管理」機能は除く。

■　アクションが発動する仕組みについて

デバイス端末で設定したポリシーが、適用されている「利用シーン」の設定項目に対して違反を検知すると設定したアクションが発動します。マニュアルや本紙の情報を参考に、各機能のポリシー設定の内容をご理解ください。
※検知のタイミングは、利用する機能や設定により、多少の時間差があります。

■　発動したアクションの解除方法について

設定により発動したアクションは、以下の 2 つの方法で解除することが可能です。
・ポリシー違反状態からの回復
・解除キーのパスワードを記述した解除設定ファイルを USB メモリのドライブ直下へ配置し、アクションを発動しているデバイスに認識させます。

＜USB メモリ 設定例＞
(ルート)
|-- unlock.txt [※ファイルの最上段にパスワード 4 桁のみ一行記載]
|--

※認証を要する、またドライブが自動認識されないような USB メモリではアクションは解除されません。
※解除設定ファイルの名前は、”unlock.txt”として配置して下さい。[※全て小文字]
※専用の USB メモリをご用意いただき、アクションが解除できる USB メモリかどうか、事前に検証されることを強く推奨いたします。
※解除パスワードは、[利用シーン設定の編集] ＞ [システム監視ポリシーの設定] ＞ [設定] ＞ アクション タブにて 4 ケタの数字にて設定します。
※解除パスワードは、必ずデフォルトの初期パスワードから変更してご利用ください。

■ 解除キーを保存した USB メモリにて解除できない場合について

デバイスの稼働状態により、上記の解除手順を実行しても適切にアクションが解除できない場合があります。
このような際は、以下の手順での解除をご確認下さい。

＜WinKeeper TB Server からのアクション解除＞

・デバイスを、ポリシー違反状態から回復される状態にして、WinKeeper TB Server に認識させます。
・WinKeeper TB Server で、該当デバイスを認識できたら、利用シーンで該当デバイスを選択し、「クリア」を適用します。
・デバイスのウィンドウで反応があるようであれば、そのまま WinKeeper TB Server から OS 再起動をかけます。

■ 利用シーンで設定した内容について、事前に動作確認をする

事前に運用に入る前に、実際に何らかのポリシーで機能が有効であることをご確認下さい。
アクション発動の動作検証は、「AC アダプターの有無を監視する」設定での検証が容易です。
※SSID 関連の設定は、デバイスが SSID を認識する/しないのタイミング(OS 仕様に基づく)にてアクションが発動する為、発動のタイミングに時間を要する場合があります。自動接続される SSID をご利用ください。

■ 利用シーン設定とネットワーク監視ポリシーについて

利用シーン設定で指定した SSID はネットワーク監視ポリシー＞「指定の SSID 以外への接続を検出した場合、接続を許可する」を設定する際、必ず指定の SSID として追加することを推奨いたします。

機能一覧と初期設定内容について

■ 利用シーンの各機能と設定内容について

以下のように、初期セットアップ時には 3 つの利用シーン設定が、以下の通り用意されております。
該当の利用シーンを編集して機能・設定を追加、または利用シーン設定自体を追加／削除してご利用できます。

設定項目一覧	コンピューター室	普通教室	校外持ち出し
壁紙の設定	○	○	○
ショートカットの設定			
メッセージ設定 [デスクトップにメッセージを表示]			
プログラムの実行制限設定			
USBデバイスの利用制限設定★ [USBメモリ/HDDの利用制限]			
その他機能の利用制限設定 [カメラの使用を禁止する/PrtScnキーの使用を禁止する]			
※以下は「システム監視ポリシーの設定」			
オフライン			
ネットワークの接続先を監視			
無線LANの監視 1 [指定SSID圏外ロック]			
無線LANの監視 2 [指定SSID以外接続不可]			
ネットワークの接続状態を一定時間監視			
ACアダプターの有無を監視			
Windowsログオンパスワードの監視 [初期値3回]			
(コンピューターの)利用エリアの監視			
操作ロック中に表示されるメッセージ			
アラーム			
操作ロックの解除キーを指定 [ロック解除キー初期値 : 0000]	○	○	○
ディスクの全消去(自動) [初期値96時間]			

※★「USB デバイスの利用制限設定」機能を使うと、解除キーが入った USB メモリでのアクション解除ができなくなりますので、設定・運用時にはご注意下さい。
※初期設定では、「システム監視」の設定は全て”解除”状態となります。

「システム監視」各設定項目の注意事項

■ 「オフライン(ネットワーク接続がない)時はアクションを実行する」に関して

本設定では、無線／有線 LAN の切断、Wi-Fi スイッチのオフ、機内モードのオンによるネットワークの切断が発生した場合にアクションが発動します。
アクションの発動は、デバイス端末機器の種類／設定等で時間が掛かる場合があります。
【注意】
- 無線／有線 LAN の 2 つのネットワークがある場合に、どちらにも接続されている場合には片方を切断しても、アクションは発動しません。両方の接続が切断された場合にアクションが発動します。
- 無線 LAN では、SSID を認識しても非接続状態の場合はアクションが発動します。
- ネットワークアダプターを無効にした場合もアクションが発動します。非接続のときにネットワークアダプターを無効にした場合も、検知され次第アクションが発動します。

■ 「ネットワークの接続先を監視する」に関して

本設定では、指定されたデフォルトゲートウェイ以外のアドレスが存在した場合にアクションが発動します。デフォルトゲートウェイのアドレスをチェックし、違反した監視ポリシーの条件が満たされるまでアクションが発動します。
【注意】
- IPv4 のみの対応となり、IPv6 には対応していません。
- 設定したアドレスを TCP/IPv4 の設定によってデフォルトゲートウェイとして直接指定すると、そのアドレスがデフォルトゲートウェイとして固定されてしまうため、端末を指定外のネットワークに接続してもアクションは実行されません。
- ネットワーク接続が無い状態ではアクションは働きません。ネットワークを無効にした場合、Wi-Fi、有線 LAN の切断、Wi-Fi スイッチのオフ、機内モードをオンにされることによるネットワークの切断が発生した場合にはアクションは発動しません。 ネットワークのオフラインも監視したい場合は【オフライン(ネットワーク接続がない)時はアクションを実行する】を組み合わせてご利用ください。

■ 「指定の無線 LAN の圏外ではアクションを実行する」に関して

本設定では、登録された SSID の範囲から外れて、その SSID が無線 LAN のリスト表示できない場合にアクションが発動します。
【注意】
- 「,」(カンマ)、「 」(スペース)、日本語などのダブルバイトを含む SSID は使用できません。
- SSID の登録は 10 個まで有効です。11 個以上登録しても有効になりません。
- 無線 LAN アダプターが存在しない場合には、SSID を登録してもアクションは発動されません。
- 無線 LAN の SSID 監視では、その SSID に接続されている必要はありません。無線 LAN の SSID のリストが取れる状態ではアクションが発動されず、SSID がリストから取れない場合にアクションが発動します。
- ネットワークアダプターを無効にした場合、アクションは発動しません。
- Wi-Fi をオフ、もしくは機内モードをオンにした場合、アクションは発動します。
- ネットワークのオフラインも監視したい場合には【オフライン(ネットワーク接続がない)ときはアクションを実行する】を組み合わせてご利用ください。
- SSID の隠ぺい(ステルス、ブロードキャストオフも同じ)を使用している場合、SSID の判定が行えません。（接続している状態では SSID が取得できる場合があります。）

■ 「指定の SSID 以外への接続を検出した場合、接続を切断する」に関して

本設定では、指定の SSID 以外への接続を検出した場合、接続を切断します。
【注意】
- 監視の対象は Wi-Fi のみです。

- この監視が違反を検出して行うアクションは違反 SSID の切断のみで、ロックのアクションは発動しません。
- 解除キーを使用してこの監視ポリシーを一時的に停止することはできません。
- 他、クラス制御メニューの「Wi-Fi 接続制限」機能とは併用して設定しないよう十分ご注意ください。

■ 「ネットワークの接続状態を監視する」に関して

本設定では、登録されたホストに対して OS 起動時または前回の疎通確認を参照し、指定された期間で疎通確認を行えない場合にアクションを発動します。

【注意】

- IPv4 のみ対応しており、IPv6 には対応していません。
- 対象先のホストに対して、ファイアウォールやネットワーク等で ICMP がブロック場合は、疎通確認ができませんのでご注意ください。
- 対象先のホストは構内のゲートウェイや管理されているサーバーなど、適切に選択する必要があります。

■ 「AC アダプターの有無を監視する」に関して

本設定では、端末から AC アダプターを取り外された場合にアクションが発動します。端末に AC アダプターが接続されるまでアクションは発動します。

【注意】

- 端末に接続している AC アダプターは電源コンセントに差し込まれて通電している必要があります。

■ 「利用エリアを監視する」に関して

【注意】

- 取得される位置情報には、精度と呼ばれる誤差が存在します。位置情報は GPS や Wi-Fi の位置情報を利用します。場所により正確な位置情報を取得できない場合があります。

■ 発動するアクションのロックについて

監視ポリシー違反によって発動するアクションのロック処理では以下の注意事項があります。

・操作をロックする： マウス、キーボード、タッチパッドやタッチパネルなどの入力デバイスを無効化して端末の入力操作を不能にします。

【注意】

- 操作ロックを解除するためには次の方法があります。
  ・ポリシー違反状態からの回復
  ・ロック解除キーの使用
- 端末に USB 解除キーが挿入されている場合にはロックのアクションは発生しませんが、USB 解除キーを端末に挿した状態で Windows を起動した場合は、ロックのアクションが発動します。
- 操作ロックの発動中に強制的にシャットダウンを行っても、次回 OS 起動したときにロックがかかります。

■ ロック画面上で表示されるメッセージに関して

操作ロックが発動した際に、設定したメッセージを画面に表示することができます。「アクション」画面で、操作ロック発動時に表示させたい文字列を設定することができます。

メッセージ 1(大)：最大 50 文字
メッセージ 2(小)：最大 50 文字

操作ロックが発動すると、背景色が青色の全画面になり、設定したメッセージが表示されます。メッセージ横にはロック発動要因の違反ポリシー名が英字で表示されます。

※複数のポリシーを同時に違反した場合でも、表示される違反したポリシー名は 1 つのみとなります。

【注意】

- メッセージ 1(大)の入力なしに、メッセージ 2(小)のみ入力設定した場合は、ロック中のメッセージスクリーンは表示されません。

- 設定したメッセージ文字列の長さによっては、表示されるメッセージが端末の画面内に収まらない場合があります。
- デバイス端末の状態により、操作ロック中のメッセージスクリーンが表示されないことがあります。

■ アラームに関して

監視ポリシー違反が発生した際、ロックと同時にアラームを鳴らすことができます。アラームを鳴らすことによって、持ち出しへの警告を行い、周囲に知らせることができます。

【注意】

- サウンドアラームは、USB 解除キーで解除ができます。
- アラームが実行された後の端末は、音量設定値が最大音量になっている場合がありますのでご注意ください。
- ログオフ時にもサウンドアラームは鳴ります。一部機種では鳴らない場合があります。

制限事項

■ [有線 LAN 接続時利用シーン使用]監視例外時間帯について

- 監視例外時間帯を設定する場合、疎通先確認にチェックをいれ IP を入力しないと、機能が使用出来ません。

■ 利用シーンの切り替えに関して

- 利用シーンの切り替えを行う際は、前回の適用から２分ほど間隔をあける必要があります。

■ ロック画面に関して

- ロック画面が表示される状態でタブレット画面を回転させるとロック画面が全体画面に表示されないことがあります。

■ USB 解除キーに関して

- 解除用に作成した解除設定ファイル (unlock.txt)は、必ず USB メモリのルート(最上階層)へ保存して下さい。USB メモリのフォルダー内に保存した場合、その USB 解除キー(USB メモリ)を使用してロック解除することはできません。
- 利用シーンを設定後に解除キーを変更した場合は、必ずクライアント側へ適用する必要があります。
- 解除パスワードを失念された場合は、WinKeeper TB Server の「利用シーン設定」にてご確認下さい。
- USB 解除キーが接続されている間のみロックが解除されます。

■ 運用に関する注意事項

- 保護対象の端末デバイスの設定ファイルの改変を行うと設定ファイルの不正操作に対する操作ロックが発動します。
- 上記の操作ロックに対しては、解除キー(unlock.txt)を使用してロック解除することはできません。

■ 「USB デバイス接続管理」機能と USB 解除キーでの解除に関して

「USB デバイス接続管理」機能を使うと、解除キーが入った USB メモリでのポリシー解除ができません。

■ IPv6 について

IPv6 はサポートしておりません。IPv4 環境でご利用いただけます。

■ SSID の認識に関して

アクションの発動、解除は OS でのアクセスポイントの認識に左右されます。できる限り”自動接続”の設定が有効な状態でご活用ください。

■ アクション実行／解除時のロック画面に関して

アクションが実行され画面ロックがかかる際、デバイスの稼働状態等により、正常にロック画面が表示されない、もしくは逆に、完全にアクションが解除されない場合があります。タイミングにより正常にロック画面が表示できず、黒画面の状態や、デスクトップ表示のまま（操作ロック状態）になる場合があります。

現時点では、以下のような動作を確認しておりますので、運用の際に本情報をご活用ください。

―アクション実行状態のデスクトップ画面―

・青いロック画面が正常に表示される
・コマンドプロンプトのウィンドウが半分表示された状態でフリーズしたような状態となる

―アクション解除時の Windows ロック画面―

・正常にロック等が解除され、Windows サインイン画面が表示され、
サインインができる
※この後は OS 再起動することで正常にご利用が可能となります。
※デバイスの種類により、外部キーボードをさして、操作を実行下さい。

■　端末デバイスによる「アクション」発動に関して

端末デバイスの種類（特にドッキングステーションタイプ）により、ロック画面が正常に表示できない場合があります。

■　「ディスクの全消去」機能に関して

本機能が発動した場合、OS の再インストールが必要となります。
ロック発動からの経過時間で発動しますが、OS が起動しない場合には、次回起動時に 3 分程度の猶予時間後に消去が発動します。
UEFI ファームウェアの一部をディスク内に持っている場合には、ロック発動後にはこれらの情報も消去するため、万が一発動してしまった場合の復旧に関してはハードウェアメーカー様へご相談ください。

以上