2023 年 3 月 29 日

お客様各位

リコージャパン株式会社

クラウドサービス for サーバーセキュリティ
Windows 最小バージョン要件に関するご案内

拝啓 貴社ますますご清栄のこととお慶び申し上げます。
平素よりリコー製品及びサービスをご愛顧賜り、誠にありがとうございます。

標記の件、「クラウドサービス for サーバーセキュリティ（本サービス）」で採用している「Trend Micro Cloud One Endpoint and Workload Security」の提供元であるトレンドマイクロ株式会社より「Windows の最小バージョン要件」についての告知を受けました。
つきましては、本サービスをご利用中の端末において Windows のバージョンに応じた対応が必要となる為、トレンドマイクロ株式会社からの告知内容を下記にご案内いたします。

― 記 ―

１． 概要

Microsoft 社では、セキュリティ対策の一環として Windows プラットフォーム上で動作するアプリケーションに対して Azure Code Signing(以降、ACS と略す）での製品モジュールの認証（署名）強化により Windows 端末におけるセキュリティ信頼性の向上を進めております。
Microsoft 社からトレンドマイクロ社が本要請を受け、「クラウドサービス for サーバーセキュリティ」で採用している「Trend Micro Cloud One Endpoint and Workload Security」に関しても、今後 ACS で署名された製品モジュール（以降、ACS 対応エージェントと略す）が配信されます。
ACS 対応エージェントのアップデートはお客様のご都合に合わせて実施いただけます。ご利用端末における ACS 対応として、Windows の OS バージョンに応じた最小バージョン要件のセキュリティパッチとルート証明書を適用いただく必要がございます。

＜Windows 最小バージョン要件＞

OS バージョン	Windows 最小バージョン要件（MICROSOFT の KB へのリンク）	
	セキュリティパッチ	ルート証明書
Windows Server 2022	OS Build 20348.261	「Microsoft Identity Verification Root Certificate Authority 2020」

Windows Server 2019	OS Build 17763.2210	※左記のセキュリティパッチが適用されていますと、自動的に証明書も適用されます。 但し、「信頼されたルート証明書」の自動更新を無効化している場合は手動での適用が必要となります。
Windows Server 2016	OS Build 14393.4704	
Windows Server 2012 R2	2021-10 マンスリー ロールアップセキュリティのみの更新プログラム	
Windows Server 2012	2021-10 マンスリー ロールアップセキュリティのみの更新プログラム	
Windows Server 2008 SP2	2021-10 マンスリー ロールアップセキュリティのみの更新プログラム Windows Server 2008/2008 R2 （Azure でない） をご利用のお客様は、Microsoft と ESU 契約を結んでいる必要があります。ESU の正式な期限は 2023 年 1 月までとなります。	

※上記セキュリティパッチは、2021 年 9 月または 10 月に最初に公開され、その後 Microsoft の毎月の累積更新プログラムに含まれています。その為、定期的にセキュリティパッチの更新を実施されている場合は、上記セキュリティパッチはすでに適用済みの場合があります。

※ご利用端末の OS ビルドバージョンが、[セキュリティパッチ]欄に記載された OS ビルドバージョン未満の場合は、上記のセキュリティパッチ適用が必要となります。

2． 対象サービス

ITKeeper クラウドサービス for サーバーセキュリティ

3． 適用開始日

2023 年 4 月上旬（※）以降に、トレンドマイクロ社から ACS 対応エージェントが配信されます。

但し、エージェントのアップデートは、お客様のご都合に合わせて実施いただけます。

※配信時期はトレンドマイクロ社の都合により変更になる可能性があります。

配信日が確定しましたら、以下リコーセンターサービスにてご案内いたします。

https://itkeeper.service.ricoh.co.jp/isp2/

※現在ご利用いただいている ACS 非対応のエージェントでも、パターンファイルやセキュリティルールは更新され、セキュリティ機能は動作します。

※サポート終了バージョンのエージェントをご利用いただいている場合は、サポート対象バージョンのエージェントへのアップデートを合わせてご検討ください。

４．お客様へのお願い事項

①　Windows セキュリティパッチの適用

ご利用端末の Windows のバージョンに応じた Microsoft Windows セキュリティパッチの適用をお願いいたします。

※ご確認方法と適用方法の詳細は別紙１をご参照ください。

②　ルート証明書の適用

「信頼されたルート証明機関」にルート証明書「Microsoft Identity Verification Root Certificate Authority 2020」が適用されていることが必要です。ルート証明書が適用されていない場合は手動での適用をお願いいたします。

※上記４．①のセキュリティパッチが適用されていますと、自動的に証明書も適用されます。
但し、「信頼されたルート証明書」の自動更新を無効化している場合は手動での適用をお願いいたします。

※ご確認と適用方法の詳細は別紙２をご参照ください。

③　エージェントのアップデート

・最新エージェントへのアップデートは管理コンソールより、お客様のご都合に合わせて実施してください。

※管理コンソールへのログオン方法については、別紙 3 をご参照ください。

※アップデート手順は、別紙 4 をご参照ください。

※エージェントのアップグレード完了時に、稀に OS 側が再起動を求める場合がございます。その為、エージェントのアップデートはメンテナンス時間を設けてご対応ください。

・ACS 対応エージェントの最新バージョンは以下の通りです。

エージェントバージョン ※1	ACS 非対応エージェントの 最新バージョン	ACS 対応エージェント ※2
バージョン 20	20.0.0.6313	左記以降のバージョン
バージョン 12	12.0.0.2626	左記以降のバージョン
バージョン 11	11.0.0.2549	左記以降のバージョン

※1 バージョン 11 未満のエージェントは、サポートが終了しております。

※2 ACS 対応エージェントのバージョンは、配信時に確定します。確定しましたら、以下リコーセンターサービスにてご案内いたします。
https://itkeeper.service.ricoh.co.jp/isp2/

５． ACS 非対応の端末における影響について

- ACS 対応要件を満たさない環境においても、パターンファイルやルールの更新などのセキュリティ機能は、継続してご利用いただけますので、ご安心ください。ただし、ACS 対応エージェントのバージョン以降へ更新ができません。
- 最新エージェントへの更新ができないことにおける留意事項は以下となります。

＜留意事項＞

① 製品の脆弱性が見つかった場合は、エージェントの更新にて修正するため、脆弱性が修正されません。

② エージェントの新バージョンで提供される新機能はご利用いただけません

③ 今後、ご利用のバージョンがサポート期限を迎えた場合、サポート対象外となります。

６． 本件に関する問合せ先

«クラウドサービス for サーバーセキュリティ ヘルプデスク»

0120-722-213（受付：月曜日-金曜日 9 時-17 時）

※祝日、弊社が定める指定日（年末年始等）は除きます。

※お電話の際は、お掛け間違えの無いようにご注意ください。

※本メールアドレスは送信専用アドレスとなります。本メールの返信によるお問合せはできませんので、ご注意ください。

以上

別紙目次

	概要	詳細
別紙１	Windows セキュリティパッチの最小バージョン要件について	１　ご利用端末の Windows のバージョン確認方法 ２　最小バージョン要件について
別紙２	ルート証明書の確認方法と適用方法について	１　証明書の確認方法 ２　証明書の適用方法
別紙３	管理コンソールへのログオン方法について	はじめに 1.【アカウント作成済みの場合】ログオン方法 2.【アカウントが不明の場合】招待メールの受信～アカウントの作成～ログオン
別紙４	エージェントのアップデート方法について	１エージェントバージョンの確認方法 ２【ACS 対応端末】最新のエージェントバージョンへのアップデート方法 ３【ACS 非対応端末】バージョンを指定したエージェントアップデート方法

別紙１．**Windows セキュリティパッチの最小バージョン要件について**

1. ご利用端末の Windows のバージョン確認方法

Windows キー+R にて「ファイル名を指定して実行」のポップアップ画面が表示されますので、「名前」の欄に「winver」と入力し、OK をクリックしてください。
ご利用端末で実行中の Windows バージョンを確認できます。

※詳細については、Microsoft 社の下記サイトをご参照ください。
『使用中の Windows オペレーティング システムのバージョンを確認する』

2. 最小バージョン要件について

適用が必要な Windows の最小バージョン要件については、トレンドマイクロ社の下記サイト記載の「Windows の最小バージョン要件（Microsoft の KB5022661 を反映）」より抜粋し、ご案内いたします。
詳細についてはトレンドマイクロ社サイトおよび Microsoft 社の KB のサイトをご参照ください。

『重要なお知らせ：2023 年 2 月以降に公開されるトレンドマイクロのサーバおよびエンドポイント製品、および関連モジュールに関する Windows の最小バージョン要件について』
https://success.trendmicro.com/jp/solution/000291910

OS バージョン	最小バージョン要件（Microsoft の KB へのリンク）
Windows Server 2022	OS Build 20348.261
Windows Server 2019	OS Build 17763.2210
Windows Server 2016	OS Build 14393.4704
Windows Server 2012 R2	2021-10 マンスリー ロールアップ セキュリティのみの更新プログラム
Windows Server 2012	2021-10 マンスリー ロールアップ セキュリティのみの更新プログラム
Windows Server 2008 SP2	2021-10 マンスリー ロールアップ セキュリティのみの更新プログラム ※Windows Server 2008/2008 R2（Azure を除く） をご利用のお客様は、Microsoft と ESU 契約を結んでいる必要があります。ESU の正式な期限は 2023 年 1 月までとなります。

以上

別紙２．**ルート証明書の確認方法と適用方法について**

1. 証明書の確認方法

① 「ファイル名を指定して実行」に「certlm.msc」と入力して実行します。
（Windows キー+R にて「ファイル名を指定して実行」のポップアップ画面が表示されますので、「名前」の欄に「certmgr.msc」と入力し、OK をクリックしてください）

② [信頼されたルート証明書機関] - [証明書]を選択します。

③ 表示された証明書に「Microsoft Identity Verification Root Certificate Authority 2020」があるか確認します。

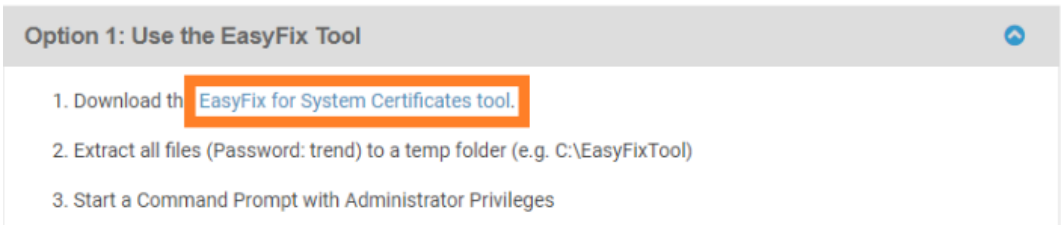
2. 証明書の適用方法

適用方法については、トレンドマイクロ株式会社の下記 Q&A 記載の「方法 1:ツールによる証明書のインストール」より抜粋しご案内いたします。詳細についてはトレンドマイクロ社サイトをご参照ください。
※Apex One SaaS の製品 Q&A となりますが、製品に関わらずご利用いただけます。

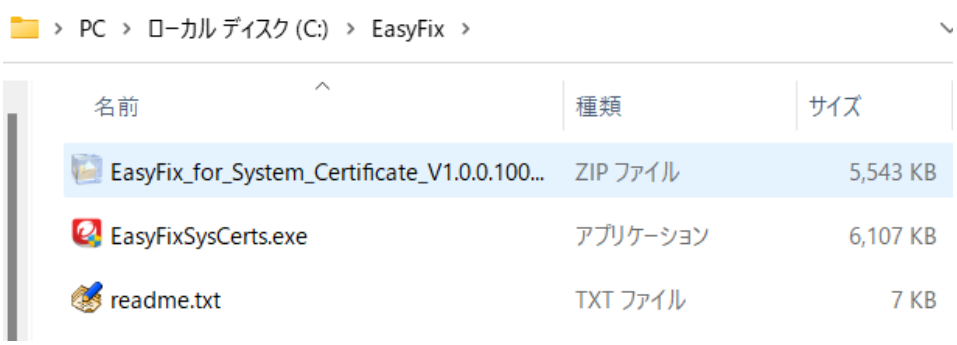
『 [Apex One SaaS] セキュリティエージェントが正常に動作しない場合 - デジタル署名関連』
https://success.trendmicro.com/jp/solution/000291489

① 以下の製品 Q&A にアクセスします。
◆ Resolving certificate-related issues in Apex One

② 「Option 1: Use the EasyFix Tool（日本語：「オプション 1: EasyFix ツールを使用する」）のセクションを開き、"EasyFix for System Certificates tool" のリンクをクリックし、ツールをダウンロードします。
※ ツールのご利用にあたっては下記サイトの「Free Tools Terms and Conditions」に同意のうえご利用ください。
Legal - License Agreements

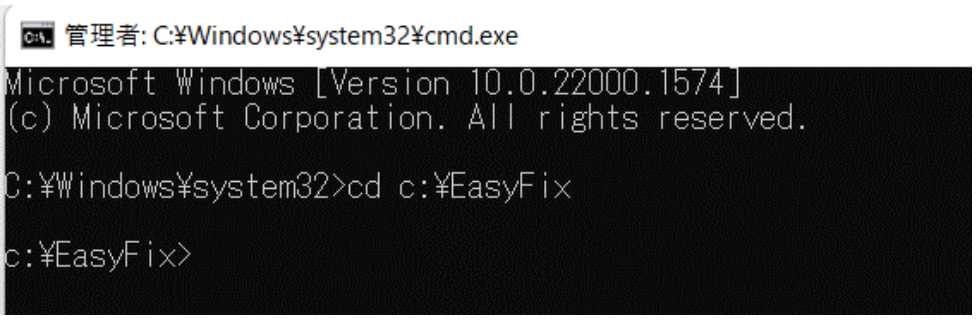


③ ダウンロードしたツールをご利用端末上の任意（c:¥EasyFix）の場所に解凍して配置します。(解凍時のパスワードを聞かれた場合は trend です)

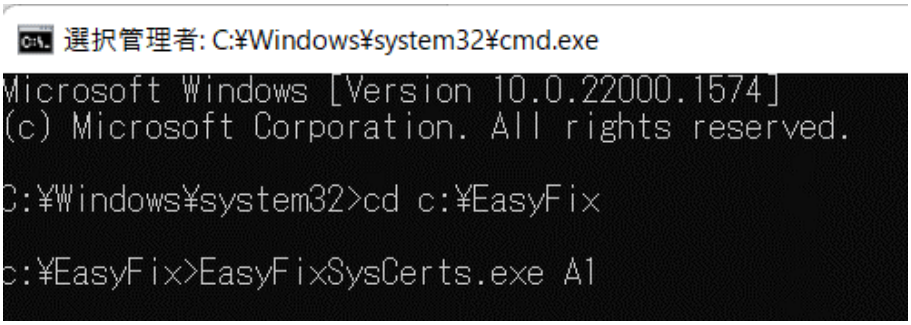


④ コマンドプロンプトを "管理者として実行" して起動します。
（Windows キー+R にて「ファイル名を指定して実行」のポップアップ画面が表示されますので、「名前」の欄に「cmd」と入力して CTRL キー+SHIFT キーを押しながら OK をクリックしてください）

⑤ コマンドプロンプトが表示された後③の任意のフォルダ（c:¥EasyFix）に移動（Enter をクリック）します。
（cd▲c:¥EasyFix）
※ ▲ は半角スペースを示します



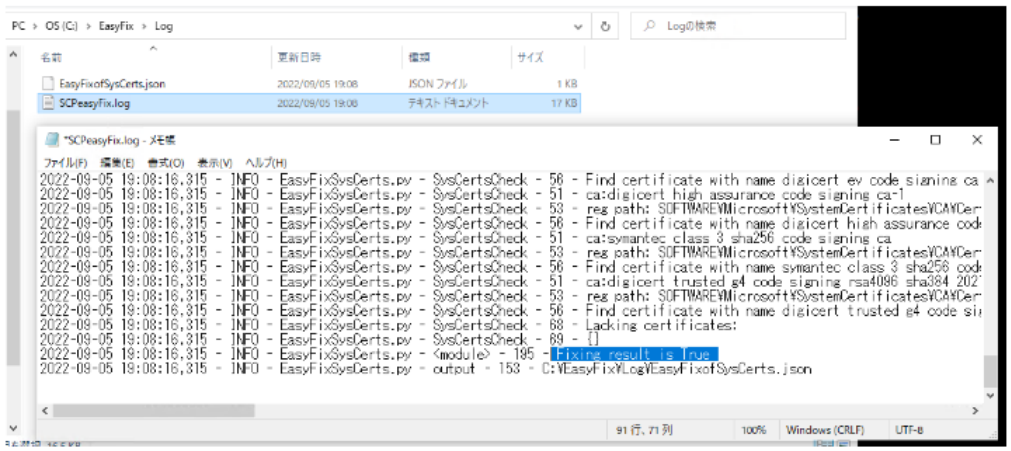
⑥　手順 ③で配置した任意の場所に移動し、以下のコマンドを実行（Enter をクリック）します。
（EasyFixSysCerts.exe▲A1）
※ ▲ は半角スペースを示します



以上で操作は終わりです。
本サービスのセキュリティエージェントに必要なルート証明書や中間証明書がなかった場合は、バックグラウンドで自動的にインストールされます。

[オプション]
お客様側でツールの実行結果を確認されたい場合は、手順 ③で配置した任意の場所の Log フォルダ内にあります SCPeasyFix.txt ファイルに記録されている処理の最後を確認してください。
”Fixing result is True” の文字列が確認できれば、ツールの処理はすべて成功しています。

既に必要な証明書を端末が持っている場合は、"No missing system certificate" の文字列が確認できます。



前項「1．証明書の確認方法」にて証明書を確認ください。

以上

別紙３．**管理コンソールへのログオン方法について**

はじめに

管理コンソールへログオンするためには、メールアドレスを用いたアカウントが必要です。

アカウントを作成するための「Trend Micro Cloud One 招待メール」（有効期限：2 週間）は、お申込時に受領したお客様のメールアドレス宛に送信（※）され、お客様にてアカウントを作成いただきます。

アカウントを作成されていない場合は、本紙 2 項に記載のとおり、「Trend Micro Cloud One 招待メール」の送信依頼をリコージャパンへご連絡のうえ、アカウントを作成してください。

※招待メールの送信時期は、アカウントシステムの変更に伴い、お申込時期により異なります。

・2021 年 8 月 1 日以降にお申込のお客様：お申込時に送信されます。

・2021 年 7 月 31 日以前にお申込のお客様：2022 年 6 月に、事前のメールによるご案内とともに送信されています。

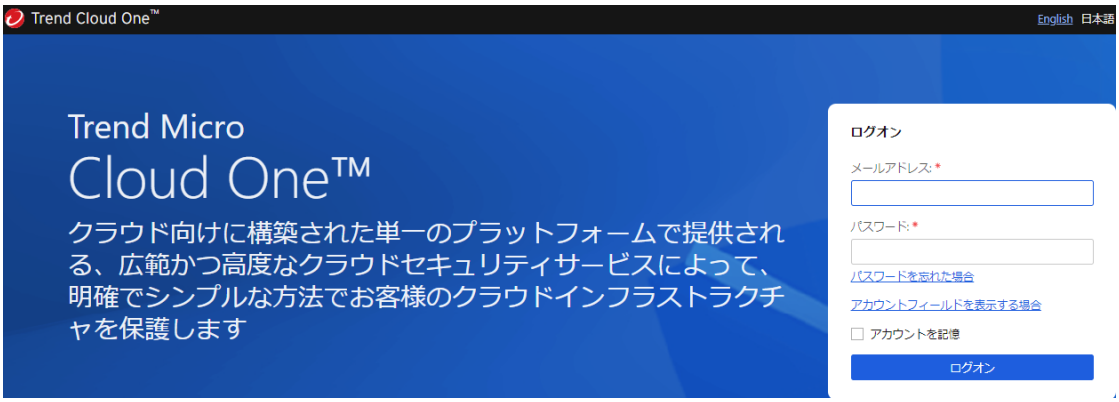
1.【アカウント作成済みの場合】ログオン方法

管理コンソール URL へ、メールアドレスとパスワードを入力しログオンします。

■管理コンソール URL

https://cloudone.trendmicro.com/

※パスワードを忘れた場合は、[パスワードを忘れた場合]をクリックし、パスワードのリセットを実施してください。



2. 【アカウントが不明の場合】招待メールの受信～アカウントの作成～ログオン

① 「招待メール」の送信依頼をお客様管理者様メールアドレスから、リコーIT コンタクトセンター宛てに以下の内容をメールにてご連絡ください。

＜ご連絡方法＞

・件名：サーバーセキュリティ ログオンアカウントの連絡

・宛先：zjc_netsupport@jp.ricoh.com

・送信元メールアドレス：お客様管理者メールアドレス

※第三者からの成りすましを防ぐため、お客様管理者様メールアドレスからの依頼のみ、受付いたします。

・本文に記載いただきたいこと

(ア)　お客様名（会社名）

(イ)　サーバーセキュリティ契約 ID

(ウ)　お客様管理者　メールアドレス　※送信元メールアドレスを記載してください。

(エ)　お客様管理者　氏名

※お申込み受付け次第、順次、TrendMicro Cloud One 招待メールを送信します。

招待メール記載のサインアップページへのリンクの有効期限はメール受信日を含み 14 日間です。お客様のご都合に合わせて送信依頼をご連絡ください。

② **招待メールを受信し、開きます。**招待メール本文に記載されている URL をクリックします。

メールの件名および送信元アドレスは以下です。

・メールの件名

「TrendMicroCloudOne に招待されました」

・送信元アドレス

「Trend Micro Cloud One <no-reply@notifications.cloudone.trendmicro.com>」

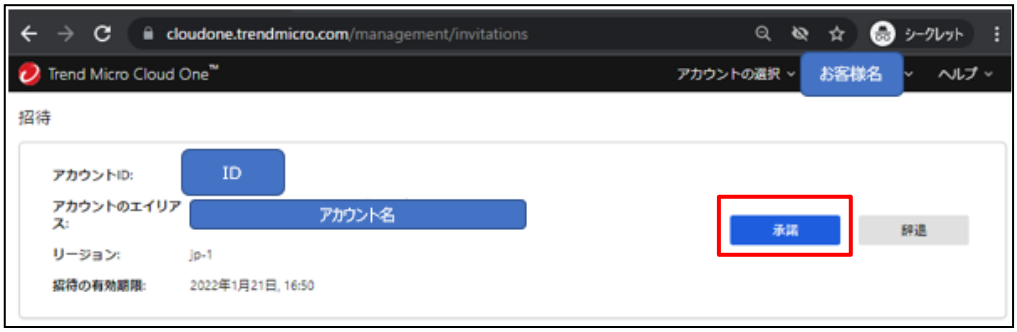
※件名およびアドレスは予告なく変更となる可能性があります。

③ [Trend Micro Cloud One にサインインアップ]画面が開きますので、ページのフィールドにメールアドレス、お名前、国（Japan）、新しいパスワードを入力し、reCAPTCHA 認証、使用条件をそれぞれチェックし、[サインアップ]をクリックします。

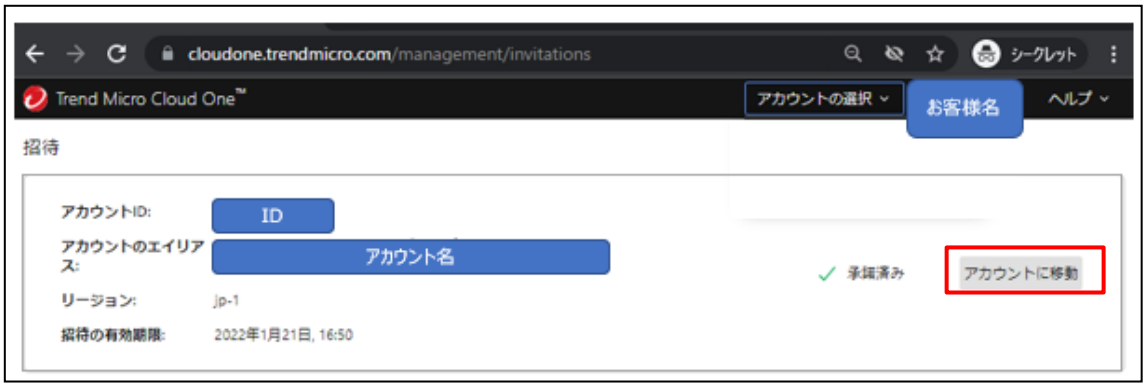
④ ユーザアカウント作成完了画面が開きますので、[Cloud One にログオン]をクリックします。

⑤ Trend Micro Cloud One ログオン画面が開きます。メールアドレス・パスワード（前項にて設定したもの）を入力し、[ログオン]をクリックします。

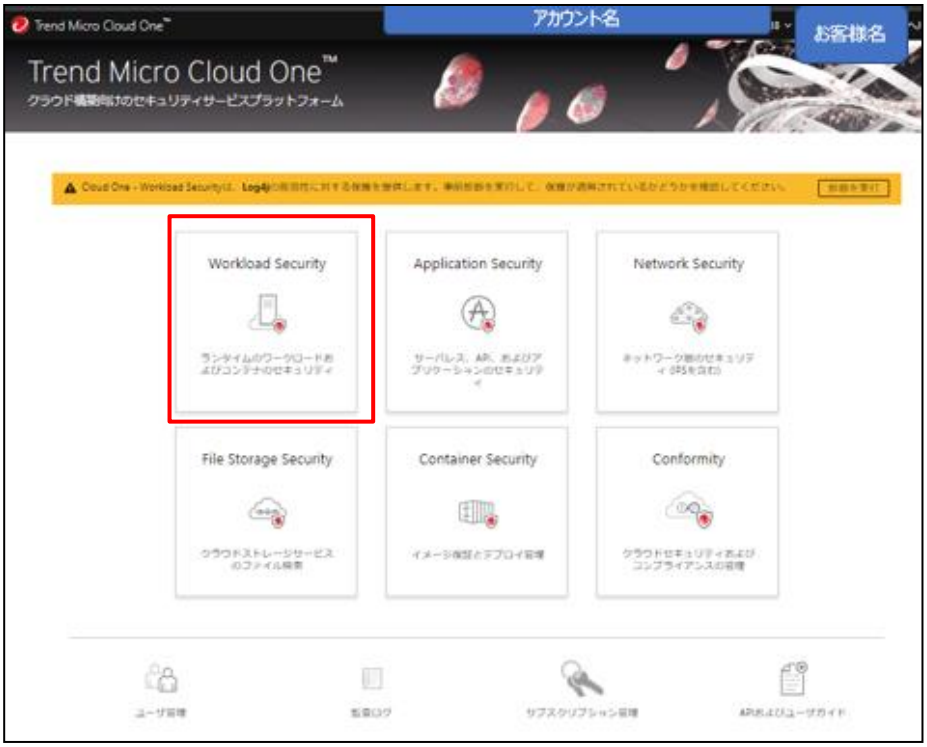
⑥ ログオンすると、Trend Micro Cloud One アカウントへの招待を受け入れるように求められます。[承諾]（Accept）をクリックします。



⑦ [承諾済み]となりますので、[アカウントに移動]をクリックします。



⑧Trend Micro Cloud One 画面が開きます。（通常のログオン後に表示される画面です。）
[Workload Security]をクリックすると、管理コンソールが表示されます。



※お願い
「RJAdmin」アカウントは、本サービスを提供する為のリコージャパン専用アカウントです。
削除しないようお願いいたします。

以上

別紙４．**エージェントのアップデート方法について**

はじめに

ご利用端末が、ACS 対応端末か、ACS 非対応端末かにより、エージェントのアップデート方法が異なります。

端末	エージェントのアップデート方法	手順
ACS 対応端末	最新のエージェントバージョン（下表の赤枠）へアップデート可能です	本紙２項
ACS 非対応端末	ACS 非対応エージェントの最新バージョン（下表の青枠）へバージョンを指定してアップデートすることを推奨します。	本紙３項

※エージェントバージョン 11 未満をご利用されている端末においても、ACS 対応端末か、ACS 非対応端末かにより、バージョン 11 以降へのエージェントアップデート手順をご確認ください。

ACS 非対応端末の場合　　ACS 対応端末の場合

エージェントバージョン	ACS 非対応エージェントの最新バージョン	ACS 対応エージェント※
バージョン 20	20.0.0.6313	左記以降のバージョン
バージョン 12	12.0.0.2626	左記以降のバージョン
バージョン 11	11.0.0.2549	左記以降のバージョン

手順は、トレンドマイクロ社の Workload Security ユーザガイドより抜粋しご案内いたします。

『Workload Security のアップグレード エージェントをアップグレードする』

https://cloudone.trendmicro.com/docs/jp/workload-security/agent-upgrade/

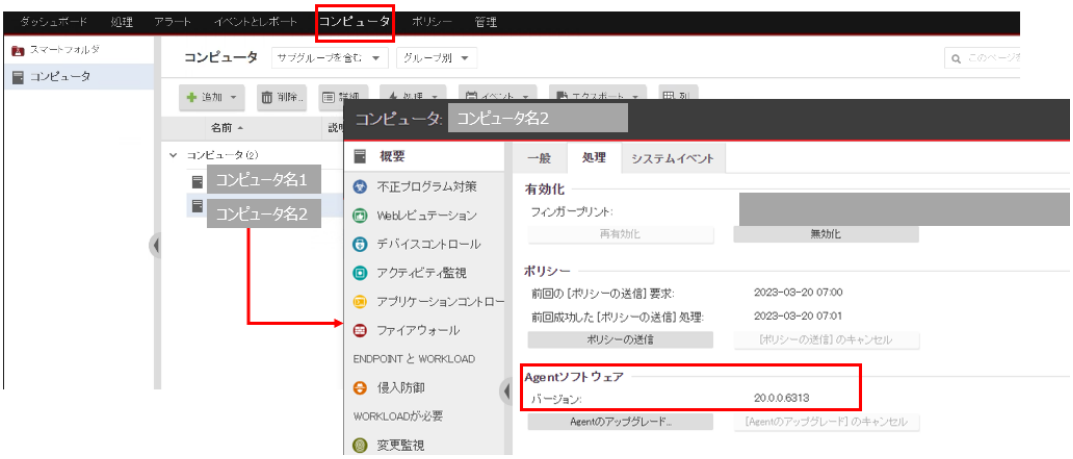
※ご注意：事前にご確認ください。

エージェントのアップグレード完了時に、稀に OS 側が再起動を求める場合がございます。その為、エージェントのアップデートはメンテナンス時間を設けてご対応ください。

再起動の要求がなければ、再起動をご実施いただく必要はございません。

1. ご利用端末のエージェントバージョンの確認方法

管理コンソールにログオンし[コンピュータ]画面で、対象のコンピュータを選択し右クリックすると詳細画面が表示されます。[Agent ソフトウェア]欄のバージョンで、ご利用端末のエージェントバージョンをご確認いただけます。



2. 【ACS 対応端末】最新のエージェントバージョンへのアップデート方法

管理コンソールにログオンし[コンピュータ]画面で、対象のコンピュータを右クリックすると詳細画面が表示されます。[Agent ソフトウェア]欄の[Agent のアップグレード]ボタンをクリックします。最新のエージェントバージョンへアップデートされます。

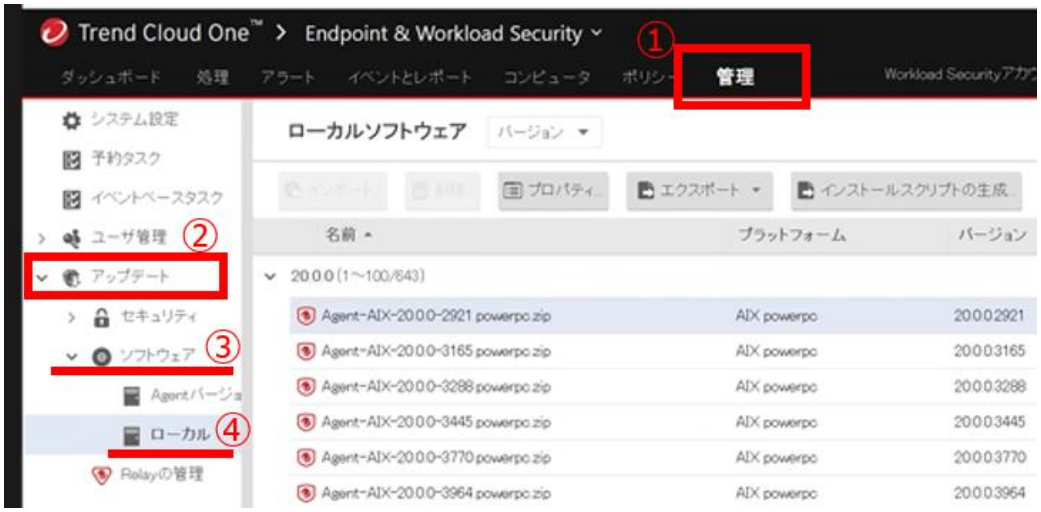
3. 【ACS 非対応端末】バージョンを指定したエージェントアップデート方法

トレンドマイクロ社の Workload Security ユーザガイドのうち、[Windows でエージェントをアップグレードする]より抜粋し、手順をご案内いたします。
『Workload Security のアップグレード エージェントをアップグレードする』
https://cloudone.trendmicro.com/docs/jp/workload-security/agent-upgrade/

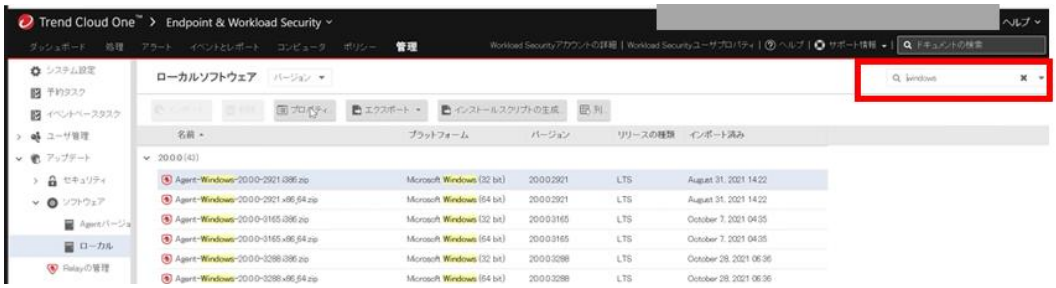
① エージェントのバージョンを指定してアップデートするため、対象バージョンのエージェントインストーラをダウンロードして実行します。事前に、[エージェント自己保護]を無効にして、インストーラがエージェントを変更できるようにします。自己保護を無効にするには、管理コンソールにログオンし[コンピュータ]画面で対象のコンピュータを選択し、[詳細]を選択します。

② コンピュータ詳細画面の[設定]→[一般]の順に選択します。[Agent セルフプロテクション]欄の[ローカルのエンドユーザによる Agent のアンインストール、停止、または変更を拒否]を［いいえ］を選択し、保存します。
※初期設定は［いいえ］です。

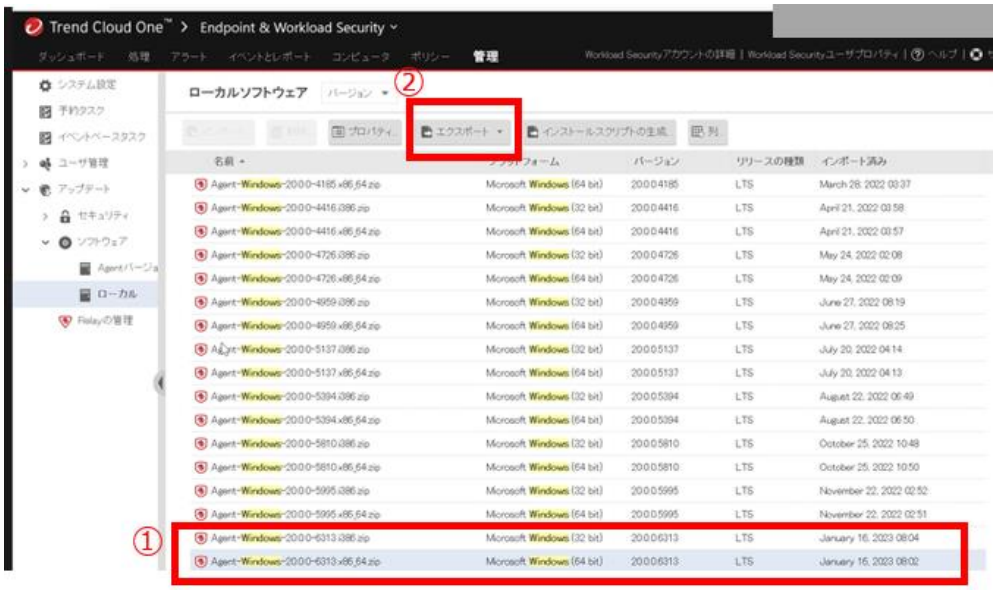
③ インストールするエージェントのインストーラを管理コンソールよりエクスポートします。
管理コンソールで、[管理]→[アップデート]→[ソフトウェア]→[ローカル]の順に選択します。



④ 右上の検索画面に「Windows」と入力し Enter キーをクリックすると Windows のエージェントに絞られてリストが表示されます。



⑤ リストからアップデート対象のバージョンのエージェントを選択し、[エクスポート]をクリックします。



⑥ [エクスポート]→[インストーラのエクスポート] をクリックします。
※これにより、インストーラ（MSI ファイル）がエクスポートされます。[パッケージのエクスポート]を選択した場合は、Zip ファイルがエクスポートされますので、ファイルを展開し、MSI ファイルを実行してください。

⑦ 前項でエクスポートしたインストーラファイルをクリックし実行するとエージェントがアップデートされます。

⑧ アップデート完了後、ご利用端末のエージェントバージョンがアップデートしたバージョンとなっていることをご確認ください。
エージェントのバージョンは、管理コンソールの[コンピュータ]画面で、対象のコンピュータを右クリックし詳細画面を表示し、[Agent ソフトウェア]欄のバージョンにてご確認いただけます。

以上