NEC

文書管理番号：SND-SEC-MI-21004-1.7

Deep Security Agent 20.0
アップグレード手順書
(Linux)

2024 年 10 月 21 日

【第 1.7 版】

日本電気株式会社

更新履歴

項番	版数	更新日	更新内容	更新箇所	更新区分	備考
1	1.0	2021/09/27	―	―	新規	
2	1.1	2023/01/17	対応 OS を更新	1.2 動作環境	更新	
3	1.2	2023/10/10	サポート期間が終了した OS の Deep Security Agent 20.0 でのサポート内容が変更されます	1.2 動作環境	更新	
4	1.2	2023/10/10	サポート対象の OS 追加	1.2 動作環境	更新	追加された OS Amazon Linux 2 (AWS ARM-Based Graviton 3) Amazon Linux 2023 (64-bit) Amazon Linux 2023 (AWS ARM-Based Graviton 2) Red Hat Enterprise Linux 9 (64-bit) Rocky Linux 8 (64-bit) Rocky Linux 9 (64-bit) AlmaLinux 8 (64-bit) AlmaLinux 9 (64-bit) Ubuntu 22.04 (64-bit) Ubuntu 18.04 (AWS ARM-Based Graviton 2) Ubuntu 20.04 (AWS ARM-Based Graviton 2) Ubuntu 22.04 (AWS ARM-Based Graviton 2) Debian 11 (64-bit) Oracle Linux 9 (64-bit)
5	1.2	2023/10/10	サポート対象の Web ブラウザを記載	2.3 管理サーバログイン	更新	
6	1.3	2023/12/21	サポート対象の OS 追加	1.2 動作環境	更新	追加された OS Miracle Linux 8 (64-bit) Miracle Linux 9 (64-bit) Debian 12 (64-bit)
7	1.4	2024/01/23	以下の内容を追記 ※対応プラットフォームに「Oracle Linux」が含まれていますが、Oracle Exadata などのアプライアンス製品の場合はサポート対象外となります。 ※Deep Security Agent 20.0 未満はサポート対象外です。	1.2 動作環境	更新	
8	1.4	2024/01/23	"https://success.trendmicro.com/jp/" で始まる URL を最新のものに変更	1.2 動作環境	更新	
9	1.5	2024/06/25	限定サポート対象 OS の制限事項について記載	1.2 動作環境	更新	
10	1.5	2024/06/25	記載内容を修正	1.1	更新	
11	1.6	2024/08/14	製品 Q&A の URL を更新	1.2	更新	
12	1.6	2024/08/14	記載内容を修正	2.1, 2.2, 2.3, 2.4, 3	更新	
13	1.7	2024/10/21	サポート対象の OS 追加	1.2 動作環境	更新	追加された OS SUSE Linux Enterprise Server 12 (PowerPC little-endian) SUSE Linux Enterprise Server 15 (PowerPC little-endian) Red Hat Enterprise Linux 8 (AWS Arm-based Graviton2) Red Hat Enterprise Linux 8.6 (PowerPC little-endian)

目 次

1 はじめに

1.1 本資料に関して

本資料は、Linux 環境において「Deep Security Agent 20.0」をご利用のお客様が、バージョンアップを行う方法を記載しています。

1.2 動作環境

（1）Deep Security Agent 20.0 は、以下の動作環境を満たしている必要があります

メモリ	最小 RAM 2GB ※5GB 以上を推奨
ハードディスク	1GB 以上を推奨
OS	Red Hat Enterprise Linux 6 (32- and 64-bit) Red Hat Enterprise Linux 7 (64-bit) Red Hat Enterprise Linux 8 (64-bit) Red Hat Enterprise Linux 8 (AWS Arm-based Graviton2) Red Hat Enterprise Linux 8.6 (PowerPC little-endian) Red Hat Enterprise Linux 9 (64-bit) Rocky Linux 8 (64-bit) Rocky Linux 9 (64-bit) AlmaLinux 8 (64-bit) AlmaLinux 9 (64-bit) Miracle Linux 8 (64-bit) Miracle Linux 9 (64-bit) Ubuntu 16.04 (64-bit) Ubuntu 18.04 (64-bit) Ubuntu 18.04 (AWS ARM-Based Graviton 2) Ubuntu 20.04 (64-bit) Ubuntu 20.04 (AWS ARM-Based Graviton 2) Ubuntu 22.04 (64-bit) Ubuntu 22.04 (AWS ARM-Based Graviton 2) CentOS 6 (32- and 64-bit) CentOS 7 (64-bit) CentOS 8 (64-bit) Debian 8 (64-bit) Debian 9 (64-bit) Debian 10 (64-bit) Debian 11 (64-bit) Debian 12 (64-bit) Amazon Linux (64-bit) Amazon Linux 2 (64-bit) Amazon Linux 2 (AWS ARM-Based Graviton 2) Amazon Linux 2 (AWS ARM-Based Graviton 3) Amazon Linux 2023 (64-bit) Amazon Linux 2023 (AWS ARM-Based Graviton 2) Oracle Linux 6 (32- and 64-bit) Oracle Linux 7 (64-bit) Oracle Linux 8 (64-bit) Oracle Linux 9 (64-bit) SUSE Linux Enterprise Server 12 (64-bit) SUSE Linux Enterprise Server 12 (PowerPC little-endian) SUSE Linux Enterprise Server 15 (64-bit) SUSE Linux Enterprise Server 15 (PowerPC little-endian) CloudLinux 7 (64-bit) CloudLinux 8 (64-bit)

※ 2024 年 1 月 1 日より OS ベンダーが定めるサポート終了後、原則 1 年間の通常サポートを提供した上で、「限定サポート」の提供へと移行します。詳細は以下の製品 Q&A をご参照ください。
[参照先]：https://success.trendmicro.com/ja-JP/solution/KA-0014849

※ 限定サポート対象 OS の制限事項
限定サポート対象となっているレガシーOS は、次回の改訂した新しい DSA 20.0.x から
システム要件外になります。

例)
2024 年 1 月以降にリリースされた DSA 20.0.1-xxx は、2023/12/31 時点での
限定サポート OS 上では、ご利用いただけません。(システム要件外となります。)
※誤ってアップグレードおよび新規インストールを行った場合は、不可である旨のエラー/警告
が出力されます。

現在の限定サポート対象 OS は以下の製品 Q&A をご参照ください。
[参照先]：https://success.trendmicro.com/ja-JP/solution/KA-0015528

※ Linux 版 Agent では、ご利用のカーネルもサポート対象である必要があります。サポートするカーネルバージョンについては、以下の製品 Q&A をご参照ください。
[参照先]：https://success.trendmicro.com/ja-JP/solution/KA-0003667

※ 対応プラットフォームに「Oracle Linux」が含まれていますが、Oracle Exadata などの
アプライアンス製品の場合はサポート対象外となります。

※ Deep Security Agent 20.0 未満はサポート対象外です。
Deep Security Agent 20.0 は、リリース日から 5 年後の 12 月 31 日でサポート終了します。
[参照先]：https://success.trendmicro.com/ja-JP/solution/KA-0009810#ds20

（2）本製品の利用には下記の要件を満たす必要があります。

- インターネット接続が可能
- TCP443 で通信が可能
- プロキシ経由する場合は、プロキシの認証無し、もしくは Basic 認証で通信が可能（Digest 認証と NTLM 認証は未サポート。）
- 保護対象サーバが以下の URL にアクセスできる必要があります。
- 保護対象サーバから対象 URL への通信経路に FW やロードバランサなどの通信機器が存在する場合は、SSL を含む送信、受信が共に可能な設定となっていることをご確認ください。
- 「仮想パッチ&アンチウイルスライセンス」のライセンスをご利用で、機械学習型検索をご利用の場合は以下 URL の「Smart Protection Network -Global Census サービス」「Smart Protection Network - Good File Reputation サービス」「Smart Protection Network -機械学習型検索」の項目に記載の URL にアクセスできる必要があります。(https://help.deepsecurity.trendmicro.com/20_0/on-premise/ja-jp/communication-ports-urls-ip.html)

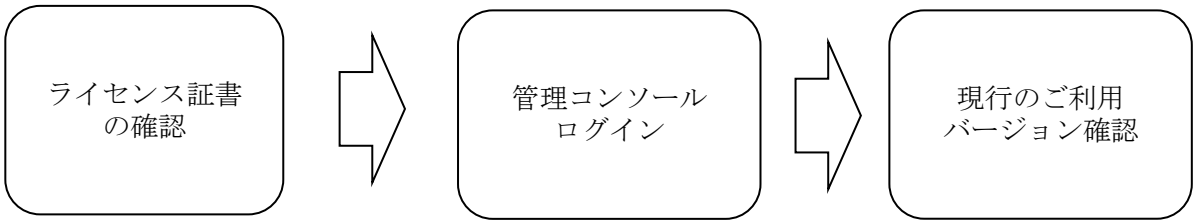
URL	用途	補足
serversecurity-nec.jp:443	管理コンソール URL	保護対象サーバ上で管理コンソールにアクセスしない場合は不要です。
hb.serversecurity-nec.jp:443	管理サーバとの疎通確認、イベントログの送信等	
reray.serversecurity-nec.jp:443	セキュリティアップデート ソフトウェアアップデート	
iaus.trendmicro.com:443	セキュリティアップデート	Trend Micro 社 Active Update サーバ。 アクセス可能にすることで可用性が向上します。
iaus.activeupdate.trendmicro.com:443		
ipv6-iaus.trendmicro.com:443		
ipv6-iaus.activeupdate.trendmicro.com:443		

2 事前準備

2.1 事前準備

【注意事項】
・事前準備作業は、保護対象サーバ以外のお客様のクライアント PC や端末機でも実施可能です。

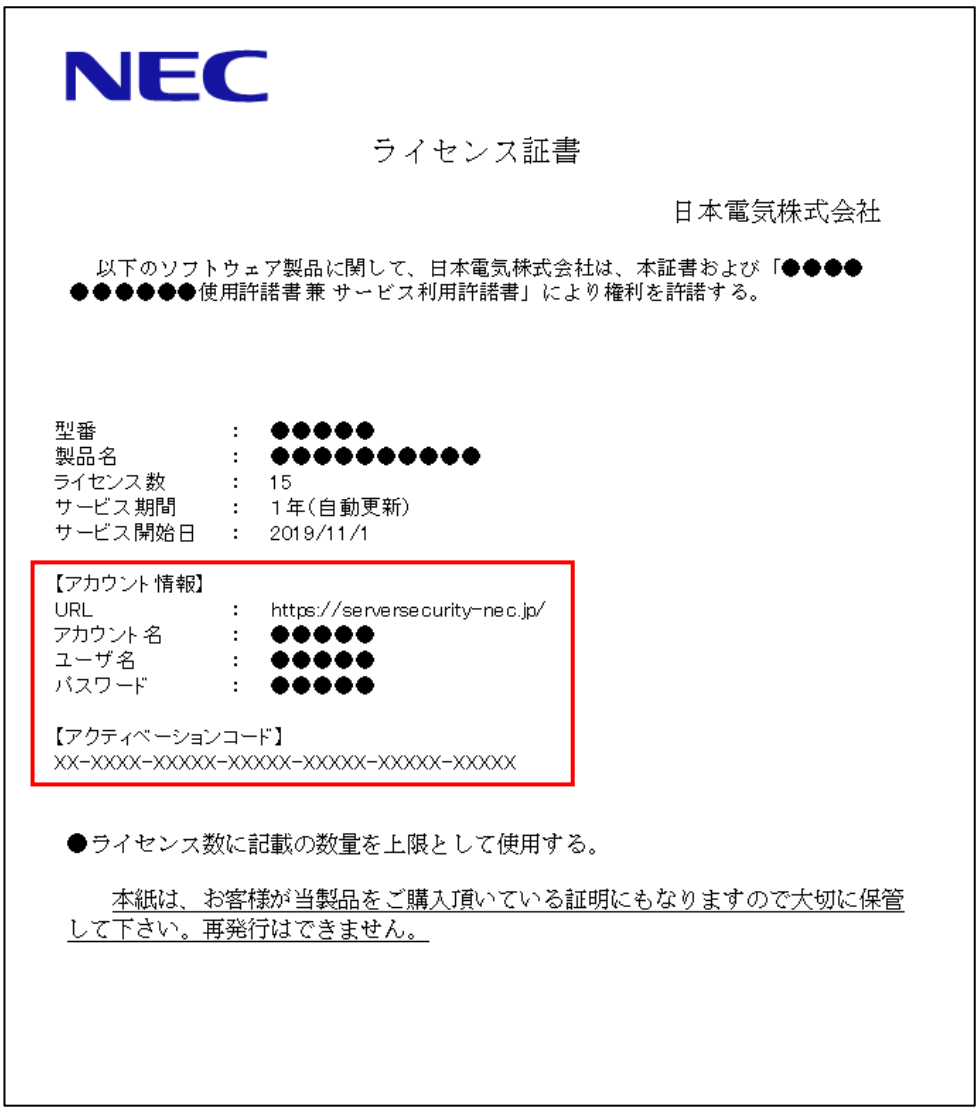
Agent 導入前に管理コンソール上で、Agent インストールの事前準備を行います。



2.2 ライセンス証書の確認

【注意事項】
・この情報は、管理コンソールログイン等に使用します。
・外部に公開しない様、慎重にお取り扱いください。

別途送付したライセンス証書より、アカウント情報（赤枠部分）を確認してください。



NEC

ライセンス証書

日本電気株式会社

以下のソフトウェア製品に関して、日本電気株式会社は、本証書および「●●●●
●●●●●●使用許諾書 兼 サービス利用許諾書」により権利を許諾する。

型番　：　●●●●●
製品名　：　●●●●●●●●●●
ライセンス数　：　15
サービス期間　：　1年(自動更新)
サービス開始日　：　2019/11/1

【アカウント情報】
URL　：　https://serversecurity-nec.jp/
アカウント名　：　●●●●●
ユーザ名　：　●●●●●
パスワード　：　●●●●●

【アクティベーションコード】
XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

●ライセンス数に記載の数量を上限として使用する。

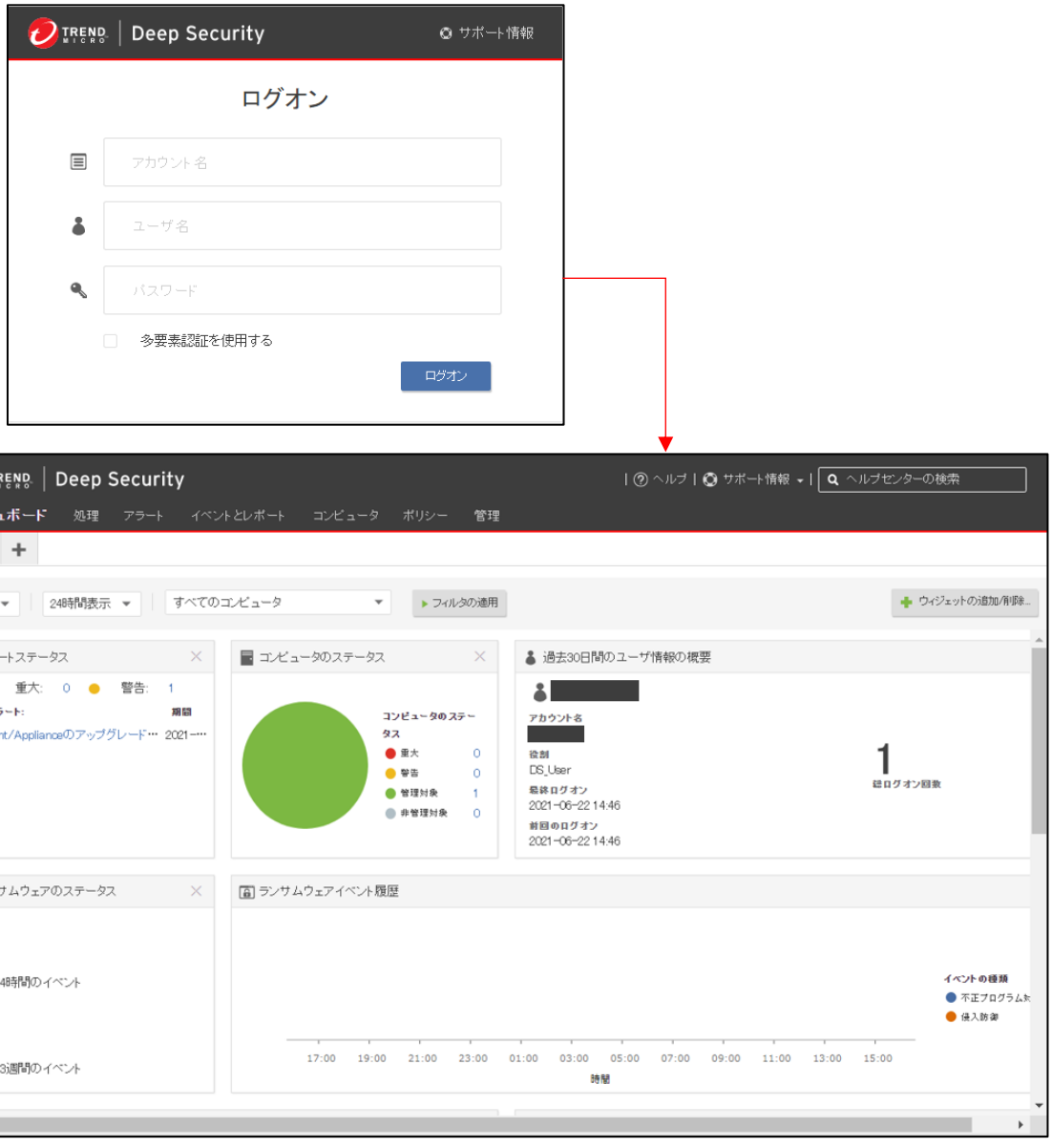
本紙は、お客様が当製品をご購入頂いている証明にもなりますので大切に保管して下さい。再発行はできません。

2.3 管理コンソールログイン

【注意事項】
管理コンソールは以下の Web ブラウザで動作を保証します。
- Mozilla Firefox (Cookie を有効にする)
- Microsoft Edge (Cookie を有効にする)
- Google Chrome (Cookie を有効にする)
- Safari (Cookie を有効にする)

（1）ライセンス証書の[アカウント情報] > [URL] に記載してある URL にアクセス

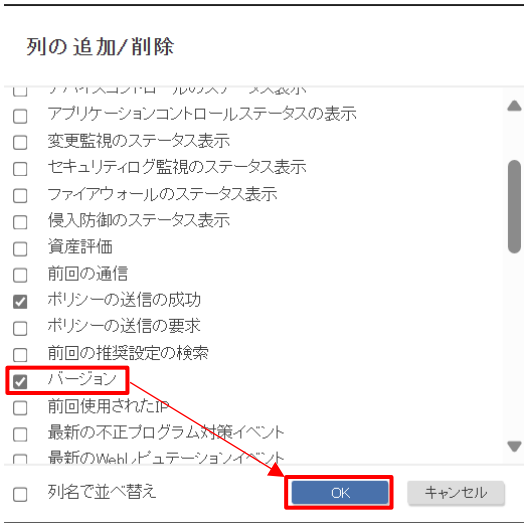
（2）ライセンス証書の[アカウント情報] > [アカウント名/ユーザ名/パスワード]を入力してログイン



2.4 現行のご利用バージョンの確認

（1）[コンピュータ] > [列]を選択

（2）[バージョン」にチェックボックスを入れ、「OK」ボタンをクリック



（3）[バージョン]列から確認

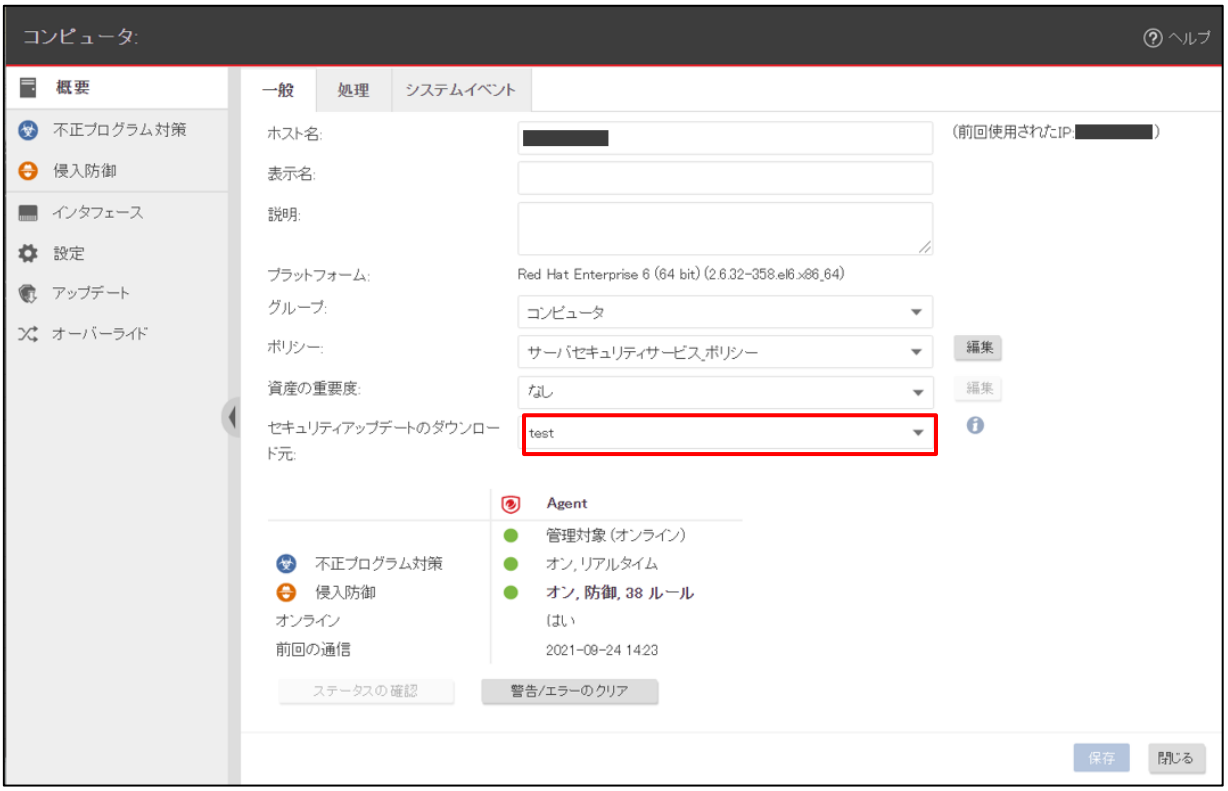
2.5 セキュリティアップデートのダウンロード元の変更

【注意事項】
※プロキシを経由しない環境の場合、本手順は不要です

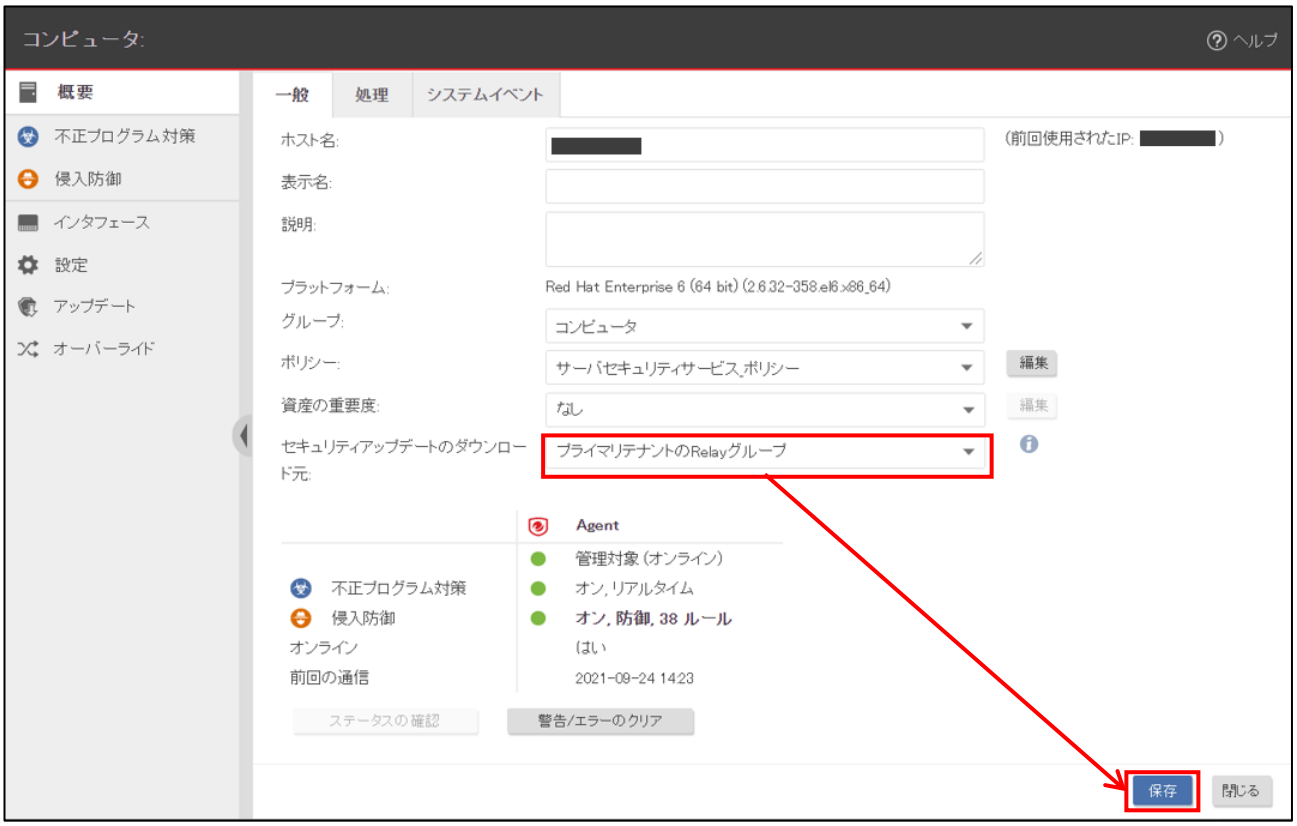
(1) 管理コンソールにログイン

(2) [コンピュータ]タブを選択

(3) 対象のコンピュータの詳細画面を表示し、[概要]の[一般]タブで、[セキュリティアップデートのダウンロード元:]に、”プライマリテナントの Relay グループ”以外が設定されていることを確認する。
※”プライマリテナントの Relay グループ”が設定されている場合は以降の手順は不要です。



（4）[セキュリティアップデートのダウンロード元:]のプルダウンリストから”プライマリテナントの Relay グループ”を選択し、[保存]をクリックする。



2.6 Relay への接続に使用するプロキシの設定

【注意事項】
※既に Relay のプロキシ設定をしている場合やプロキシを使用しない場合は本手順は不要です。

（1）以下のコマンドを管理者権限で実行し、Relay へ接続するためのプロキシを設定する。
/opt/ds_agent/dsa_control -y relay_proxy://*プロキシサーバの URL:ポート*//

プロキシで認証（Basic 認証のみ対応）を行う場合、
「/opt/ds_agent/dsa_control -y relay_proxy://*プロキシサーバの URL:ポート*/」行の次行に、

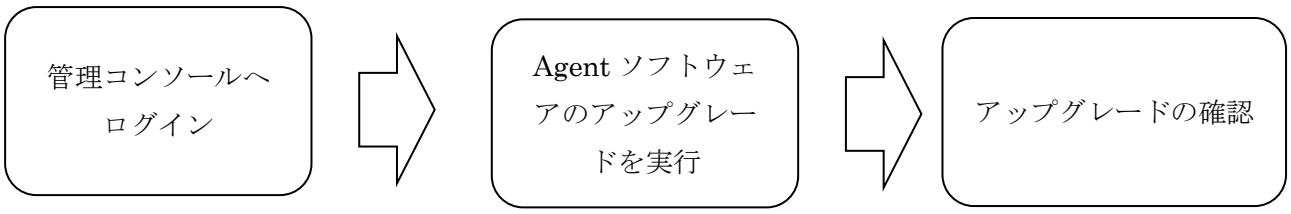
「/opt/ds_agent/dsa_control -w *ユーザ名:パスワード*」

と入力してください。

例）「ユーザ名：root、パスワード：Password」の場合、以下のように入力
/opt/ds_agent/dsa_control -w root:Password

3 アップグレードする手順

管理コンソールにログインし、Agent ソフトウェアのアップグレードを行います。

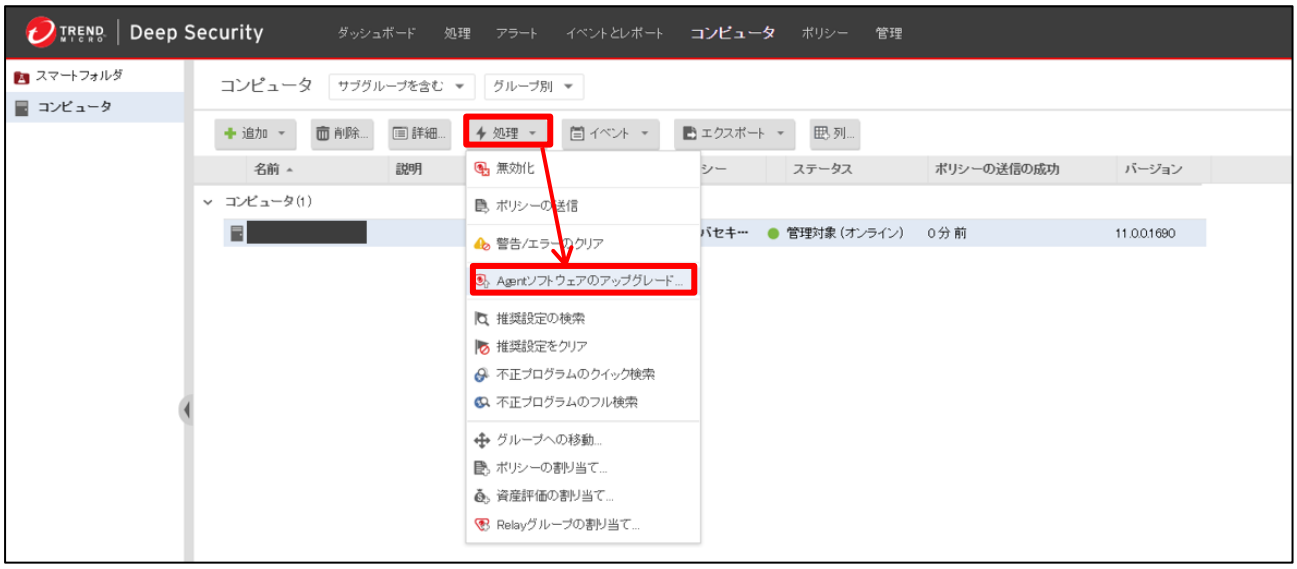


3.1 Agent ソフトウェアのアップグレードを実行する

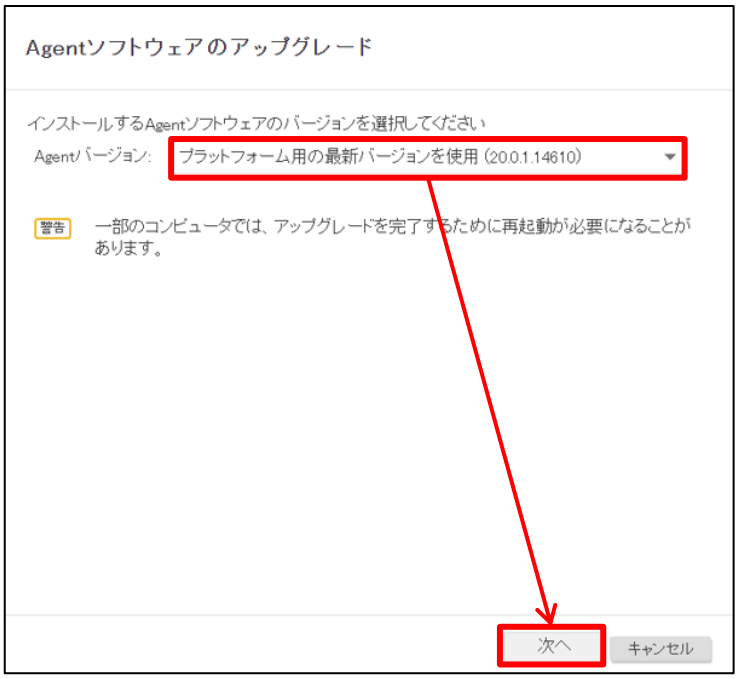
（1）管理コンソールへログイン

（2）[コンピュータ]タブを選択

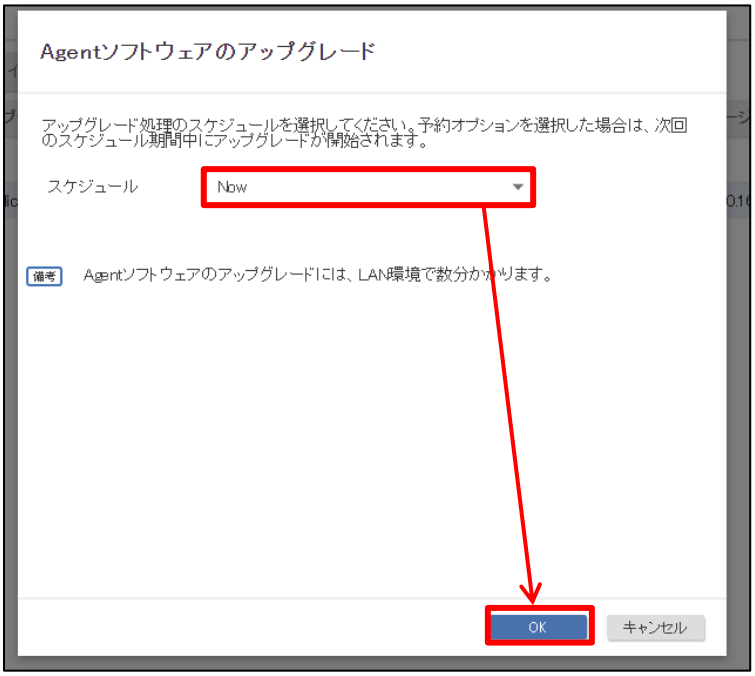
（3）[処理] > [Agent ソフトウェアのアップグレード]をクリック



（4）[20.0.1-]に続く数値が一番大きなバージョンを選択して、[次へ]をクリック



（5）スケジュールは[Now]を選択し、[OK]をクリック



（6）アップグレードの完了を待ち。最新のバージョンになっていることを確認する。

（参考）モジュールのインストール失敗のエラーが発生した場合

アップグレード処理時、一時的に「ソフトウェアアップデート：〇〇モジュールのインストール失敗」のエラーが発生することが確認されています。

当該エラーはアップグレード処理における一時的なものですので、警告/エラーのクリアを押下し、しばらく後に状況をご確認ください。