



インテル®vPro®プラットフォーム× インテル®EMA

～PC 管理の救世主～

内容

1. はじめに.....	3
2. 検証環境.....	4
3. 利便性.....	7
4. インテル®VPRO®プラットフォームで実現する機能(インテル® EMA) と HP WOLF SECURITY FOR BUSINESS を利用した制御.....	10
4.1 運用管理	12
4.1.1 PC 統合管理.....	12
4.1.1.1 ユーザ管理とグループ管理.....	19
4.1.1.2 ユーザ作成.....	20
4.1.1.3 ユーザグループ作成.....	23
4.1.1.5 エンドポイント (クライアント PC) 導入	31
4.1.1.6 ユーザグループとエンドポイントグループの関連付け	44
4.1.2 リモート電源制御	46
4.1.2.1 リモート電源一括制御	46
4.1.2.2 リモート電源個別制御	51
4.1.2.3 Hardware Manageability タブからのリモート電源個別制御.....	54
4.1.3 ハードウェアアラームクロック機能.....	61
4.1.4 ハードウェア KVM 機能.....	68
4.1.4.1 「Desktop」タブからの操作	68
4.1.4.2 「Hardware Manageability」タブからの操作	74
4.1.4.3 BIOS 画面操作	78
4.1.5 HP PC Hardware Diagnostics UEFI 機能	84
4.1.5.1 問題のテスト	92

4.1.5.2 システムテスト.....	97
4.1.5.3 コンポーネントテスト.....	102
4.1.5.4 テストログ	107
4.1.5.5 システム情報	109
4.1.5.6 終了	111
4.1.6 クライアント PC に対してのファイル転送機能	113
4.1.6.1 クライアント PC のフォルダ内容表示	113
4.1.6.2 ファイルのアップロード機能	118
4.1.6.3 ファイルのダウンロード機能	121
4.2 セキュリティ.....	123
4.2.1 ハードウェア支援型 AI による検知.....	123
4.2.2 自己回復型 BIOS によるファームウェア攻撃からの防御	125
4.2.3 HP Secure Erase 機能.....	129
4.2.4 HP Sure Recover 機能	139

1. はじめに

コロナ禍で今まで当たり前だった通勤・客先訪問・出張などの活動が減り、代わりにオンライン会議の増加、テレワークによる働く場所の多様化などにより、セキュリティリスクとIT管理者のPC管理の負担が増大しています。

今回のホワイトペーパーは、HP vPro PC を使用してテレワークなどの社外に持ち出されたPCを管理・サポートする為の具体的な設定・運用方法を説明したわかりやすい資料ですので、これからの時代に合ったビジネスPCをどう選ぶべきか悩んでいるIT管理者に向けて発信し、「思ったより簡単そうだから、問い合わせして詳しく説明を聞いてみたい」と思って頂きたいと思っています。

2. 検証環境

今回、インテル®EMA とインテル®vPro®プラットフォーム搭載 PC を利用しての利便性や管理性そしてセキュリティに対してどのように対応できるかの検証を行いました。

これらの機能を確認するため、今回、検証環境として利用した環境は、Azure 環境と インテル®vPro®プラットフォーム搭載 PC を利用して検証を実施いたしました。

以下は検証環境の図になります。（図 2-①）

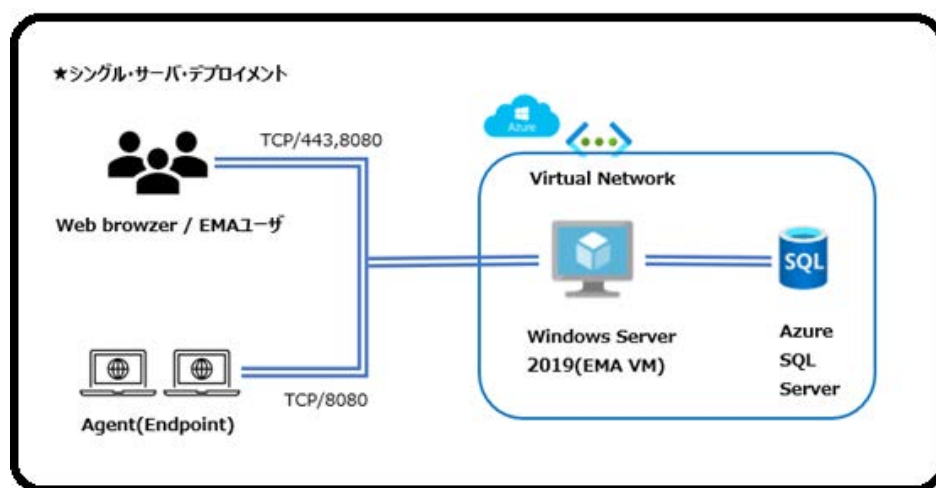


図 2-① 検証環境

今回の検証で利用した端末は日本 HP 社より提供されている、HP Elite x2 G4 と HP Elite Dragonfly G2 Notebook PC の2つのデバイスを利用して検証を行いました。（表 2-①）

インテル®EMA エージェントは2台とも、リモート接続時にユーザへの同意が不要となる ACM（Admin Control Mode）でセットアップしています。

表 2-① 検証端末一覧表

デバイス名称	OS	CPU	メモリ	HDD
HP Elite x2 G4	Windows 10 Pro (64bit)	インテル®Core™ i7- 8665U プロセッサ	16GB	512GB SSD
HP Elite Dragonfly G2	Windows 10 Pro (64bit)	インテル®Core™ i5- 1145G7 プロセッサ	8GB	256GB SSD



HP Elite x2 G4



HP Elite Dragonfly G2

インテル®EMA のバージョンは下記になります。

バージョン情報	インテル®エンドポイント・マネジメント・アシスタント (インテル®EMA) 1.5.0
---------	---

各ファームウェアおよびドライバのバージョンは以下になります。(表 2-②)

表 2-② 各種バージョン一覧

デバイス名称	HP BIOS およびシステムファームウェア	Intel Management Engine(ME)ドライバ	Intel WLAN ドライバ
HP Elite x2 G4	01.09.00	2105.15.0.2157	22.40.0.7
HP Elite Dragonfly G2	01.04.01	2117.15.0.2272	22.30.0.11

インテル®EMA サーバを構築する際に使用した Azure テンプレートは以下になります。

<参考 URL>

<https://www.intel.co.jp/content/www/jp/ja/download/19738/30201/intel-endpoint-management-assistant-intel-ema-cloud-start-tool-for-azure.html>

<今回使用した Azure テンプレート>

<https://portal.azure.com/#create/Microsoft.Template/uri/https%3A%2F%2Fintelema.z22.web.core.windows.net%2Fematemplate.json/createUIDefinitionUri/https%3A%2F%2Fintelema.z22.web.core.windows.net%2FcreateUiDefinition.json>

3. 利便性

現在、在宅勤務を多くの企業が実施している中、在宅勤務を実施している社員や IT 管理者は、以下のような悩みを抱えています。

－在宅勤務の社員

会社から支給された PC のスペックがあまり良くないため、Web 会議やリモート作業に支障をきたしている。

－IT 管理者

在宅勤務のクライアント PC が故障した際、会社に出勤して対応する必要がある。また、在宅勤務のクライアント PC はインターネットに直接つながっているためセキュリティ面で不安がある。

インテル®vPro®プラットフォームには上記の悩みを解決する、4 つの機能が組み込まれています。（図 3-①）



図 3-① インテル®vPro®プラットフォームの 4 つの機能

－パフォーマンス

インテル®vPro®プラットフォーム搭載ビジネス PC は、高いパフォーマンスを発揮するインテル®Core™ i5 / i7 vPro™プロセッサ、インテル®Xe グラフィックス、高速ネットワークカード、サンダーボルトなどビジネスに必要なハードウェアを内蔵し、どこで仕事しても生産性を向上させます。

－安定性

インテル®ステイブル IT プラットフォーム・プログラムにより、高い品質のドライバ及び長期間の Windows OS サポートを提供、また少なくとも 15 カ月または次世代リリースまで、ハードウェアの変更をゼロにすることで、IT 業務をサポートします。

－セキュリティ

インテル®vPro®プラットフォームでは「ハードウェアシールド」機能により、ハードウェアベースのセキュリティが可能になり、進化する攻撃に対して防御することができます。また、HP 社のビジネス PC には「HP Wolf Security for Business」機能が搭載されており、ハードウェアシールドと組み合わせることで、より強固なセキュリティ対策を実現することができます。

－リモート管理

今までの IT 管理者はクライアント PC を「いつでも、どんな時でもリモート管理ができる」ことが困難な部分が多くありました。例えば、クライアント PC がブルースクリーンとなった場合は、リモートから接続ができず対応できませんでした。インテル®vPro®プラットフォームでは、以下の 2 つの機能を利用して「いつでも、どんな時でもリモート管理」を実現します。

・管理コンソール(インテル®エンドポイント・マネジメント・アシスタント (インテル®EMA))

インテル®vPro®プラットフォームはインテル®アクティブ・マネジメント・テクノロジー (インテル®AMT) 機能を利用してクライアント PC のリモート管理が可能でしたが、インテル®AMT は社内ネットワークに接続されていることが前提のため、インテル®AMT で在宅勤務のクライアント PC をリモート管理するのが難しくなりました。そのような状況を打破するため、2019 年にインテル® エンドポイント・マネジメント・アシスタント (インテル®EMA) がリリースされました。インテル® EMA とインテル® AMT を組み合わせることで、インターネット環境に存在するクライアント PC をリモートから管理することが可能となりました。また、ブルースクリーンなどのトラブル時でも、リモートからの接続が可能になりました。

- ・ハードウェア KVM 機能

インテル®vPro®プラットフォームでは「ハードウェア KVM」機能により、他のアプリケーションにあるリモート操作機能では操作や画面表示できなかった BIOS 設定やブルースクリーン時のリモート操作が可能になりました。

本資料ではインテル®vPro®プラットフォームに組み込まれている機能の中で、「リモート管理」と「セキュリティ」について、詳しく紹介していきます。

4. インテル®vPro®プラットフォームで実現する機能(インテル® EMA) と HP Wolf Security for Business を利用した制御

HP Wolf Security for Business は HP のビジネス PC に実装されている、OS の下・中・上（図 4-①参照）から PC を守る各種のセキュリティ機能の総称です。



図 4-① PC の基本構造

HP Wolf Security for Business とインテル®vPro®プラットフォームのリモート運用管理機能を組み合わせることで、システム担当者は場所や時間にとらわれることなく、あたかも目の前に従業員のデバイスがあるかのようなサポートが実現します。

HP Wolf Security for Business の中には下記の機能があります。(各章をご参照ください)

- HP Sure Start

⇒[4.2.2BIOS によるファームウェア攻撃からの防御]

- HP PC Hardware Diagnostics UEFI

⇒[4.1.5HP PC Hardware Diagnostics UEFI 機能]

- HP Secure Erase

⇒[4.2.3 HP Secure Erase 機能]

- HP Sure Recover

⇒[4.2.4 HP Sure Recover 機能]

各機能に対して、リモート PC がシャットダウンしている状態でも、インテル®EMA のリモートデスクトップ機能

「ハードウェア KVM」を通じ、リモート PC を起動させてアクセスできます。

以降では、主にインテル®EMA の使用方法、各機能について説明します。

4.1 運用管理

本章ではインテル®EMA サーバでインテル®vPro®プラットフォーム搭載の端末を管理する機能について説明します。

4.1.1 PC 統合管理

インテル®エンドポイント・マネジメント・アシスタント（インテル®EMA）を利用することで、遠隔地にあるパソコンでもインターネットを経由して、さまざまな操作を行うことができます。以下にインテル®EMA の接続からインテル®EMA 管理画面について説明します。

※手順①～④はログインする URL に必要な DNS 名（FQDN）を調べる手順になりますので、接続する URL を把握している場合はスキップして手順⑤から参照してください。

- ① Azure ポータルに接続し、ログインします。(図 4-1-1-①)

[URL:https://portal.azure.com](https://portal.azure.com)

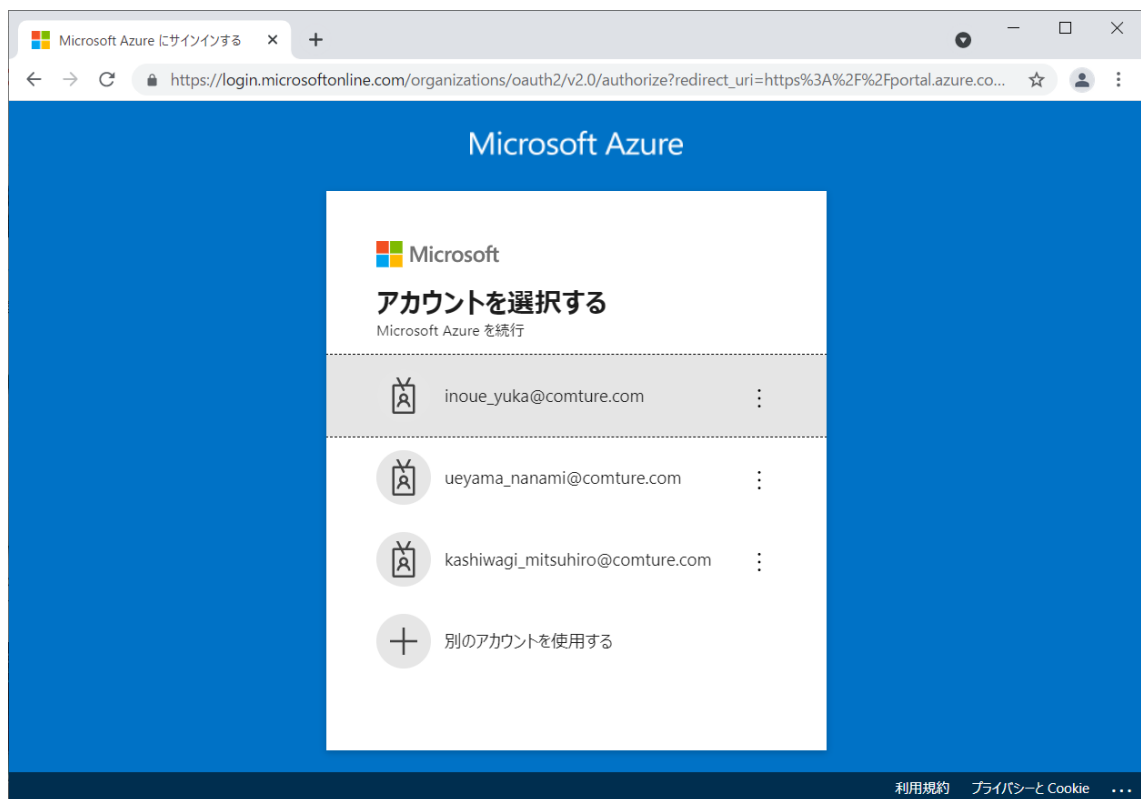


図 4-1-1-① Azure ログイン画面

② Azure サービス画面にて「Virtual Machines」を選択します。(図 4-1-1-②)



図 4-1-1-② Azure サービス画面

③ Azure ポータルにて、お客様で作成された対象インテル®EMA サーバを選択します。(図 4-1-1-③)



図 4-1-1-③ Azure Virtual Machines 画面

④ DNS 名を確認し、コピーします。(図 4-1-1-④)



図 4-1-1-④ Azure 仮想マシン画面

- ⑤ ブラウザにてインテル®EMA サーバの DNS 名を入力し、インテル®EMA へ接続します。
(URL:https://[インテル®EMA サーバの DNS 名]) (図 4-1-1-⑤)

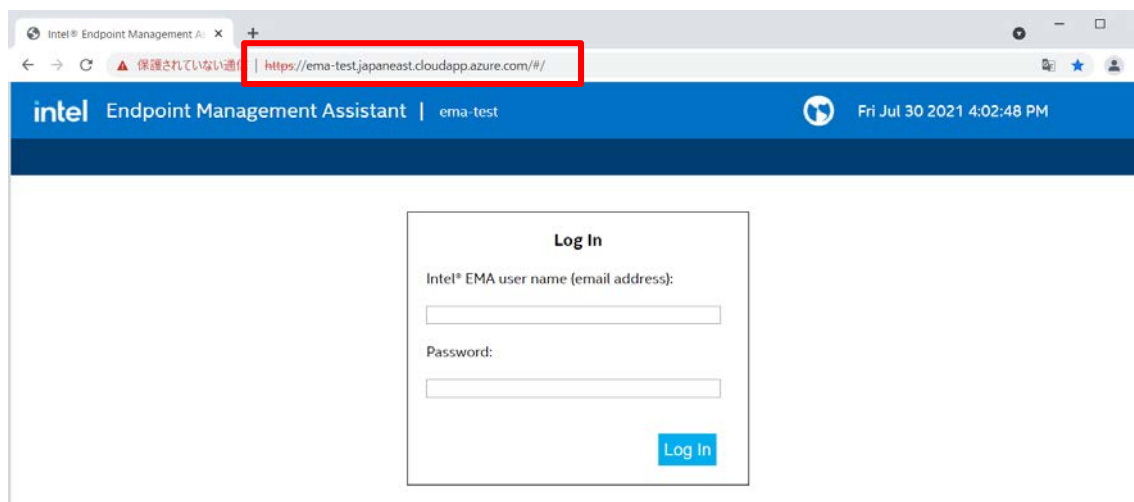


図 4-1-1-⑤ ログイン画面

- ⑥ インテル®EMA サーバ作成時に設定した user name と Password を入力、Log In ボタンをクリックしログインします。
※テナント管理者またはエンドポイント管理者でログインします。

⑦ インテル®EMA のダッシュボードが表示されます。(図 4-1-1-⑥)

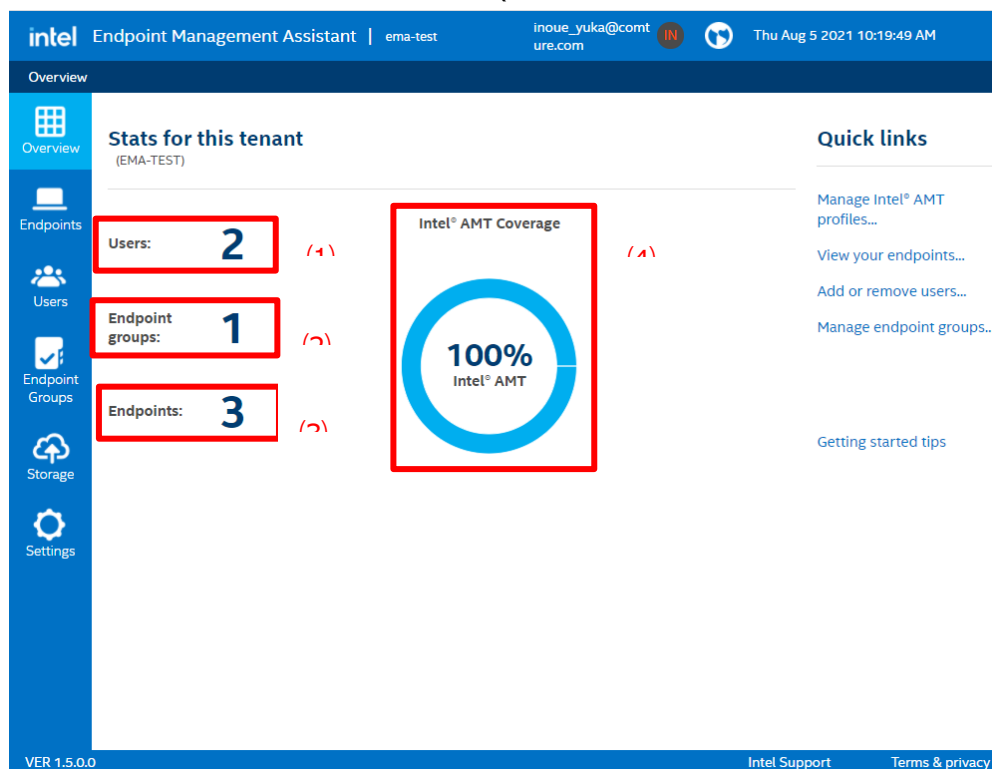


図 4-1-1-⑥ ダッシュボード画面

ダッシュボードでは、下記の情報を確認することができます。

- (1) テナント内で管理しているユーザ数
- (2) エンドポイントグループ数
- (3) 管理しているエンドポイント(クライアント PC) 数
- (4) 管理しているエンドポイントでインテル®vPro®プラットフォーム搭載 PC の割合

<管理についての注意事項>

- ・クライアント側 PC がインテル®vPro®プラットフォーム搭載 PC であること (第 7 世代以降)
- ・クライアント側 PC がノートパソコンである場合は、充電用の AC アダプターが接続されていること
- ・クライアント側 PC に第 7 世代以降の Core プロセッサが搭載されていること

- ⑧ 左メニューから「Endpoints」を選択し、「Load all Endpoints」をクリックします。(図 4-1-1-⑦)

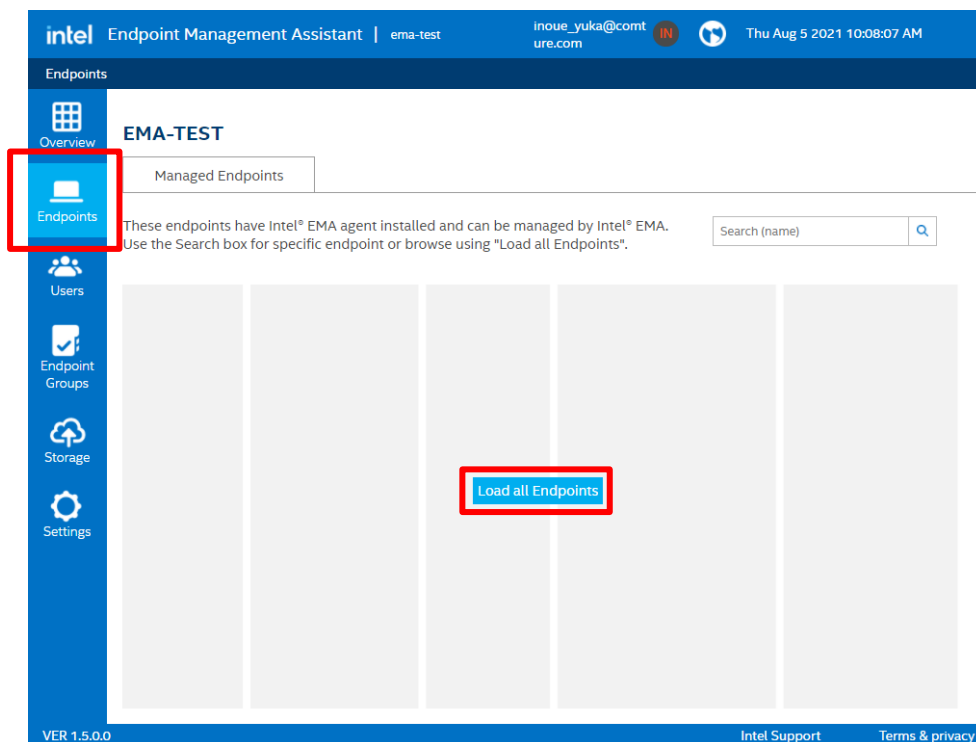


図 4-1-1-⑦ Endpoints 画面

- ⑨ エンドポイント一覧が表示されますので、確認したい対象のエンドポイントの横にある「view」をクリックします。(図 4-1-1-⑧)

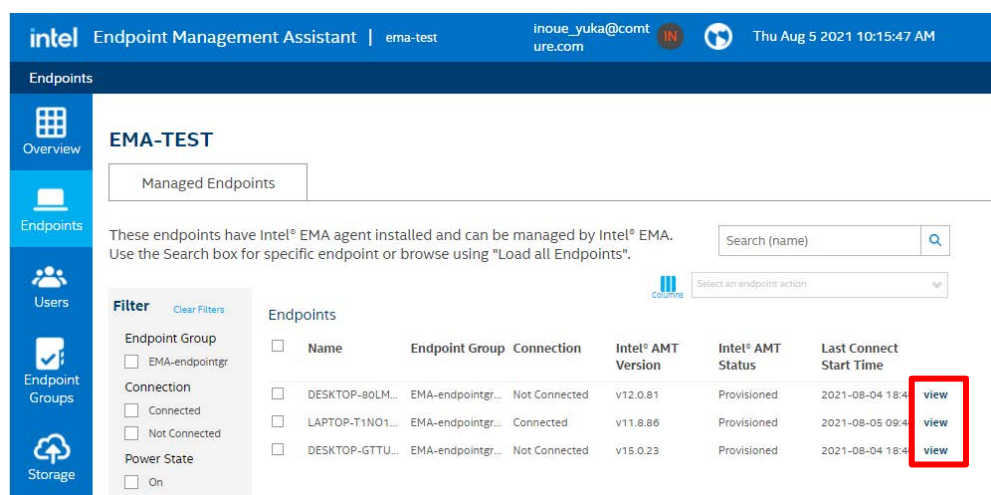


図 4-1-1-⑧ Endpoints 一覧画面

- ⑩ 現在の PC の状況を確認することができます。(図 4-1-1-⑨)

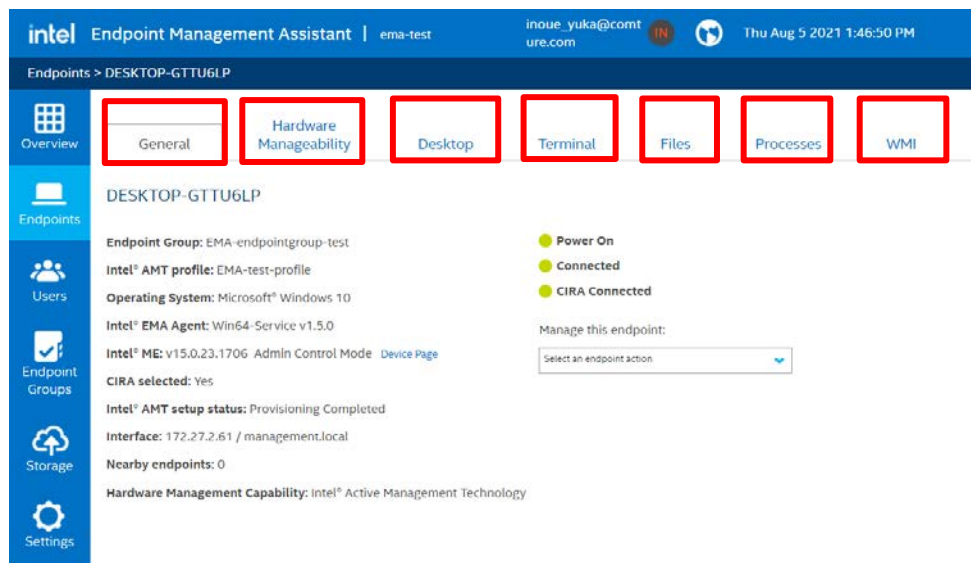


図 4-1-1-⑨ Endpoints 詳細画面

※各タブ機能について、以下に説明します。(表 4-1-1-①)

表 4-1-1-① Endpoints タブ機能説明

機能	機能説明
General	選択したエンドポイントについて全般的情報を表示
Hardware Manageability	インテル®AMT の操作(リモートデスクトップ、アラームクロック等)を実行
Desktop	リモートデスクトップの実行 ※ここからの電源操作は不可
Terminal	AMT リモートターミナル機能の実行 コマンドのみで PC/OS を操作可能
Files	リモートファイル参照 ファイルのアップロード、ダウンロードが可能
Processes	リモートプロセス管理 エンドポイントのプロセス一覧表示、削除が可能
WMI	Windows Management Instrumentation(WMI) クエリーまたはアクションの実行

4.1.1.1 ユーザ管理とグループ管理

インテル®EMA 管理画面でエンドポイント（クライアント PC）を部署ごとに管理したい場合にグループ管理を実施することが出来ます。

グループ管理設定をすることにより、部署ごとにエンドポイント（クライアント PC）を分けることが可能です。

(図 4-1-1-1-①)

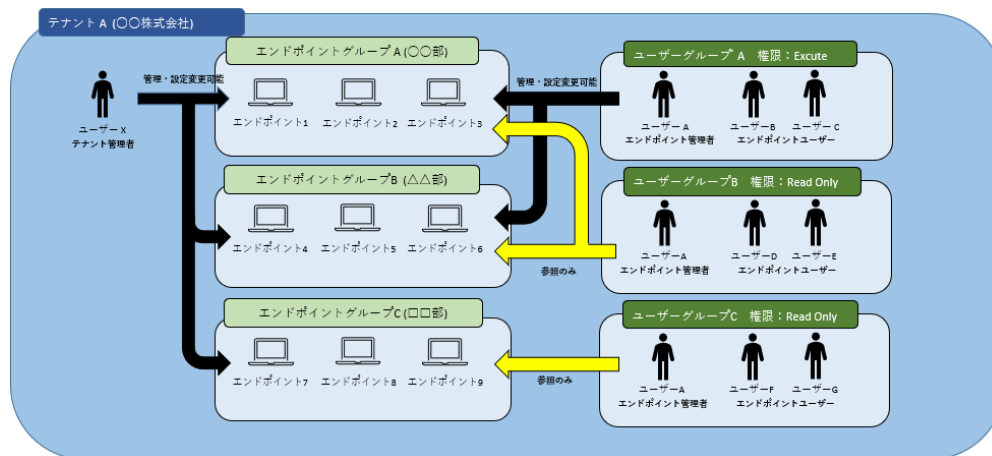


図 4-1-1-1-① 部署ごとの管理例

ユーザ管理とグループ管理を実施するために、下記の作業手順を記載します。(各章をご参照ください)

- ユーザの作成

⇒[4.1.1.2 ユーザ作成]

- ユーザグループの作成

⇒[4.1.1.3 ユーザグループ作成]

- エンドポイントグループの作成

⇒[4.1.1.4 エンドポイントグループの作成]

- エンドポイントの導入

⇒[4.1.1.5 エンドポイント導入]

- ユーザグループとエンドポイントグループの関連付け

⇒[4.1.1.6 ユーザグループとエンドポイントグループの関連付け]

4.1.1.2 ユーザ作成

インテル®EMA 管理画面にログインできるユーザの作成や権限を付与することが可能です。まず、管理を実施するにあたり、グローバル管理者でログインし、ユーザ作成してください。

本手順ではユーザの作成と権限の付与の手順を記載します。

- ① グローバル管理者またはテナント管理者権限のユーザでログイン後、Overview 画面が表示されるので、左側メニューにある「Users」を選択します。（図 4-1-1-2-①）

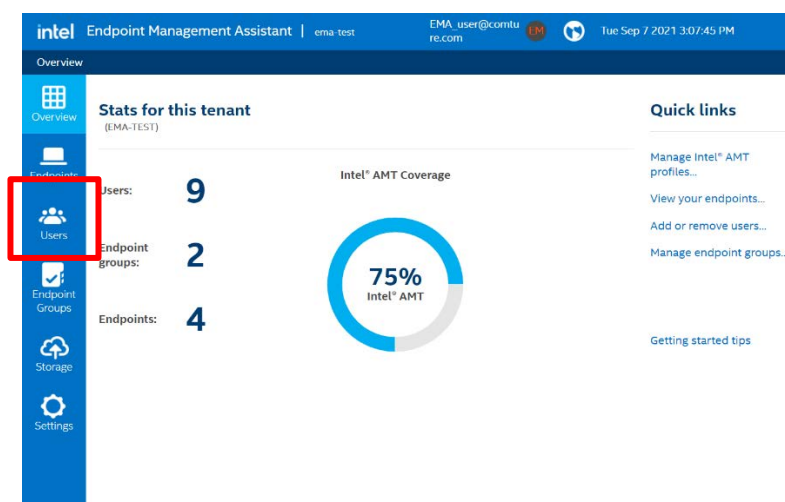


図 4-1-1-2-① OverView 画面

- ② Users 画面が表示されるので、「New User...」をクリックします。（図 4-1-1-2-②）

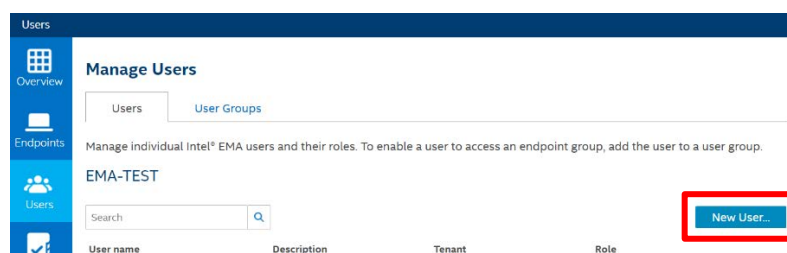


図 4-1-1-2-② ユーザ管理画面

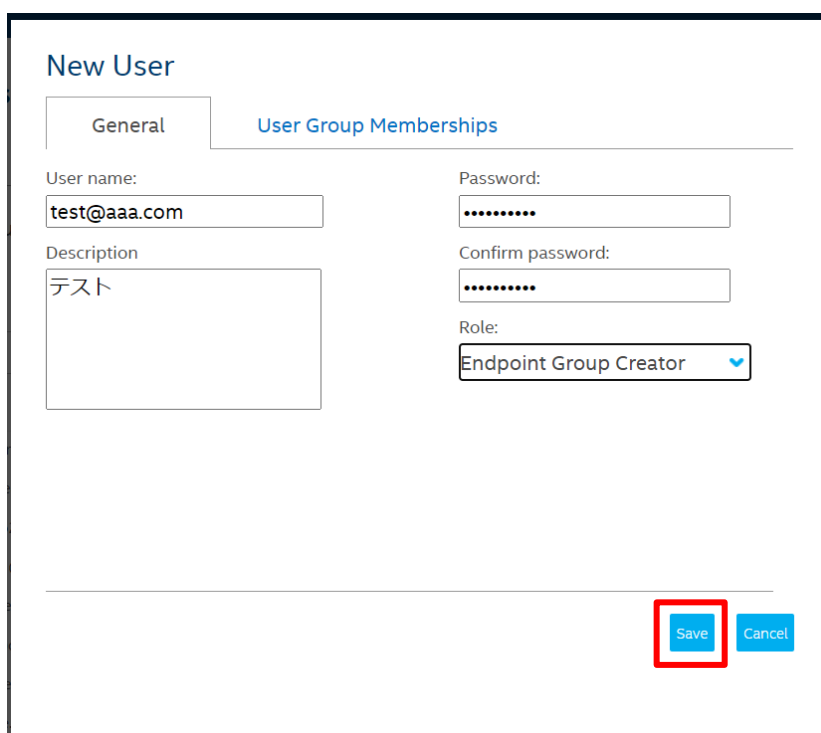
③ 新しいユーザを作成するため、各項目を入力後に「Save」をクリックします。（図 4-1-1-2-③）

User name・・・ログイン名（メールアドレス形式で入力）

Description・・・説明（参照用など、用途に合わせて記載下さい）

Password・・・ログインパスワード（大文字小文字含む英字＋数字＋記号の 8 文字以上）

Role・・・権限の付与（表 4-1-1-2-①）



New User

General User Group Memberships

User name: test@aaa.com

Password:

Confirm password:

Description テスト

Role: Endpoint Group Creator

Save Cancel

図 4-1-1-2-③ ユーザ作成画面

・Role 部分に付与できる権限は、以下種類があります。（表 4-1-1-2-①）

表 4-1-1-2-① 選択可能なロールの種類

ロール名	名称	役割	特徴
Global Administrator	グローバル管理者	テナント・ユーザの全ての管理が可能 エンドポイント（クライアント PC）管理は実施不可	・ロール最上位権限を持ち、作成後に変更が出来ない ・エンドポイントグループ・ユーザグループに属さない
Tenant Administrator	テナント管理者	テナント内の全ての操作が可能	・エンドポイントグループ・ユーザグループに属さない ・ユーザ作成時に設定したテナント内のみ管理が可能
Account Manager	アカウントマネージャー	ユーザ作成・ユーザグループ作成のみ可能	・上位ロール （Global Administrator、Tenant Administrator）はユーザ管理不可 ・エンドポイントグループ・ユーザグループに属することは出来ない ・ユーザ作成時に設定したテナント内でのみ管理が可能
Endpoint Group Creator	エンドポイントグループ作成者	エンドポイントグループの作成、エンドポイントの管理、AMT プロファイルの管理が可能	・複数のユーザグループに属した際、属しているグループの管理が可能 ・ユーザ管理は不可 ・ユーザ作成時に設定したテナント内でのみ管理が可能
Endpoint Group User	エンドポイントグループユーザ	エンドポイント管理のみ実行	・複数のユーザグループに属することが可能 ・ユーザ管理は不可 ・ユーザ作成時に設定したテナント内でのみ管理が可能

4.1.1.3 ユーザグループ作成

インテル®EMA で作成したユーザをグループ化する為には、ユーザグループを作成します。ここではユーザグループの作成から作成したユーザグループにユーザを登録する手順までを記載します。

- ① グローバル管理者またはテナント管理者権限のユーザでログイン後、Overview 画面が表示されるので、左側メニューにある「Users」を選択します。（図 4-1-1-3-①）

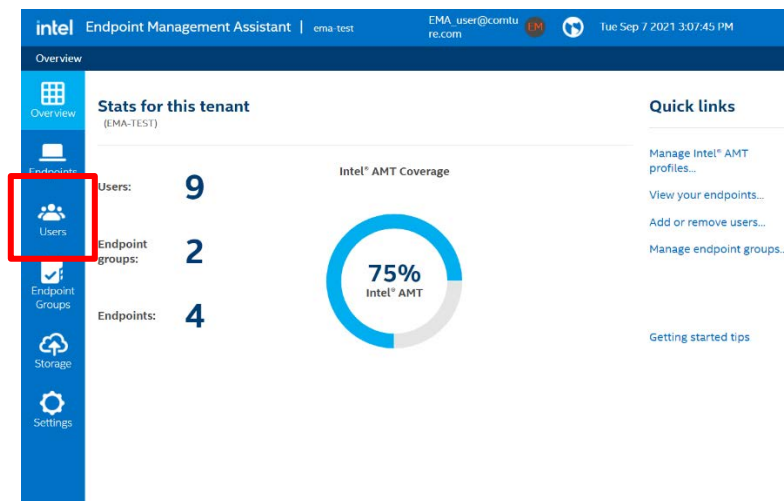


図 4-1-1-3-① OverView 画面

- ② Users 画面が表示されるので、「User Groups」タブを選択し、「New Group...」をクリックします。（図 4-1-1-3-②）

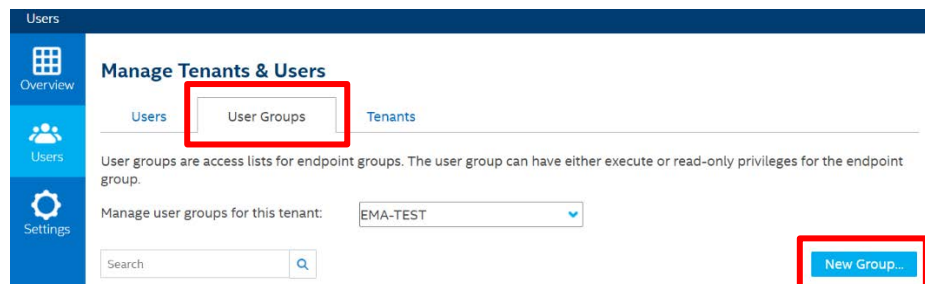


図 4-1-1-3-② ユーザグループ管理画面

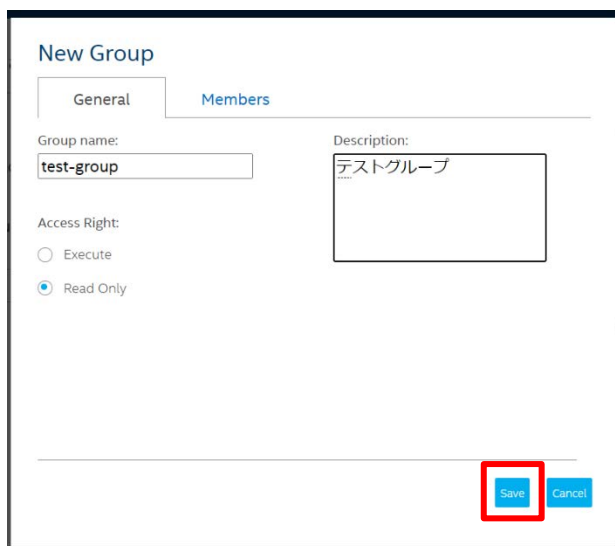
- ③ 新しいユーザグループを作成するために、各項目を入力後に「Save」をクリックします。（図 4-1-1-3-③）

Group name・・・ユーザグループ名

Access Right・・・実行権限（Execute）、参照権限（Read Only）いずれかを選択

- 実行権限・・・General タブや Hardware Managebility タブなど
（【Endpoints】-【Load all Endpoint】-【View】をクリックした後の画面）全て
実行可能
- 参照権限・・・General タブ（【Endpoints】-【Load all Endpoint】-【View】をク
リックした後の画面）のみ閲覧可能

Description・・・説明（任意：参照用など、用途に合わせて記載下さい）



The screenshot shows a web form titled "New Group". It has two tabs: "General" and "Members". Under the "General" tab, there is a "Group name:" label followed by a text input field containing "test-group". To the right is a "Description:" label followed by a text area containing "テストグループ". Below the name field is an "Access Right:" section with two radio buttons: "Execute" (unselected) and "Read Only" (selected). At the bottom right, there are two buttons: "Save" (highlighted with a red rectangle) and "Cancel".

図 4-1-1-3-③ ユーザグループ作成画面

- ④ 「User」タブを選択し、ユーザの右側にある「…」をクリックし、「Group memberships…」を選択します。(図 4-1-1-3-④)

※グループメンバーに加える前提条件として Role 部分が「Endpoint Group User」または「Endpoint Group Creator」であることを確認下さい。その他のロールの場合は次画面に遷移しませんのでご注意下さい。

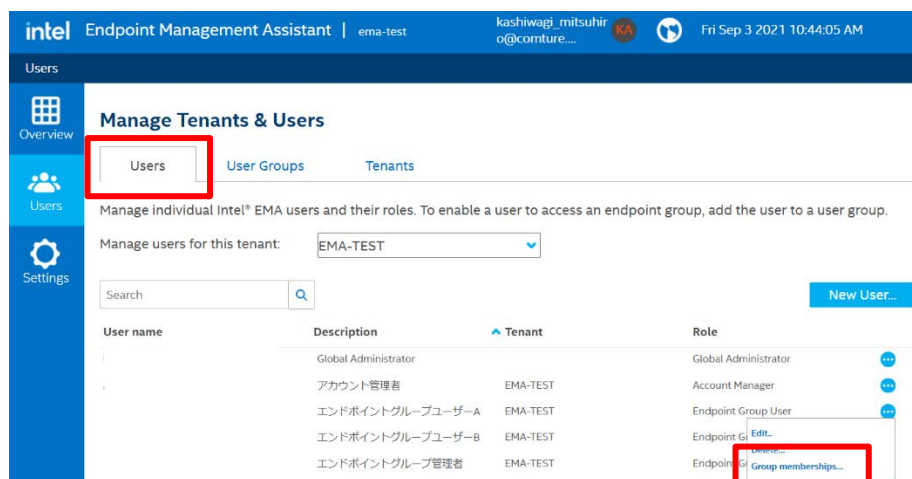


図 4-1-1-3-④ ユーザグループ選択画面

- ⑤ 手順④で選択したユーザを登録させたいユーザグループの左側にあるチェックボックスにチェック入れ、「Save」をクリックします。（図 4-1-1-3-⑤）

※複数のユーザグループに登録する場合は複数選択下さい。

※その他のユーザを登録する場合は手順④へ戻り、繰り返し作業願います。

The screenshot shows the 'Edit User' dialog box with the 'User Group Memberships' tab selected. The instruction 'Select the user groups where this user is a member:' is displayed above a table. The table has three columns: 'Name', 'Description', and 'Access Right'. There are two rows of data. The first row, 'test-groupA1', has a checked checkbox in the first column, '実行権限あり' (Execute permission) in the second column, and 'Execute' in the third column. The second row, 'test-groupA2', has an unchecked checkbox, '参照のみ' (Read only), and 'Read Only'. Below the table is a pagination bar showing 'Page 1 of 1' with 'Previous' and 'Next' buttons. At the bottom right, there are 'Save' and 'Cancel' buttons, with the 'Save' button highlighted by a red rectangle.

☐	Name	Description	Access Right
☒	test-groupA1	実行権限あり	Execute
☐	test-groupA2	参照のみ	Read Only

図 4-1-1-3-⑤ ユーザグループ選択画面

4.1.1.4 エンドポイントグループの作成

部署ごとにクライアント PC を管理する為に、エンドポイントグループ作成が必要です。ここではエンドポイントグループ作成からエンドポイント(クライアント PC)をエンドポイントグループに認識させる設定手順を記載します。

- ① テナント管理者権限のユーザでログイン後、Overview 画面が表示されるので、左側メニューにある「Endpoint Groups」を選択します。(図 4-1-1-4-①)

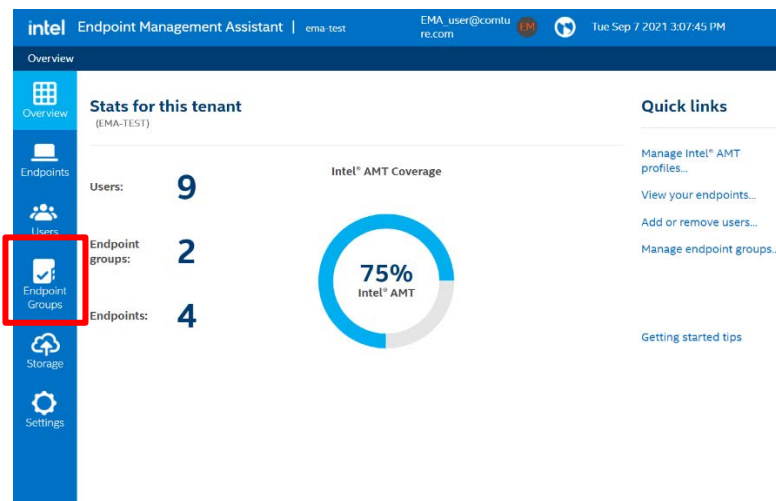


図 4-1-1-4-① Over View 画面

- ② Endpoint Group 画面が表示されるので、「Endpoint Groups」タブを選択し、「New endpoint group...」をクリックします。(図 4-1-1-4-②)

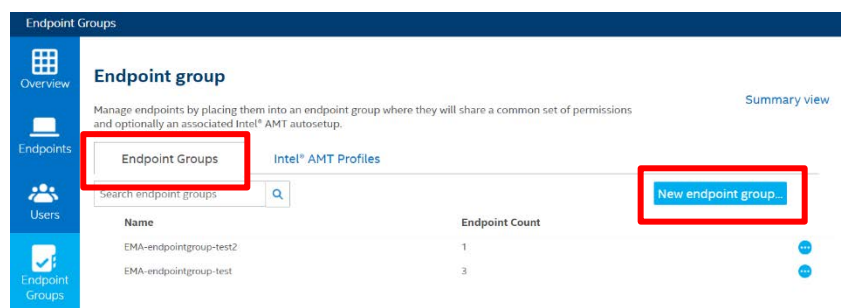


図 4-1-1-4-② Endpoint Groups 画面

③ Endpoint Group Setup 画面に移動しますので、必要事項を記載します。（図 4-1-1-4-③）

1. Create a new Group

- Group Name・・・エンドポイントグループ名
- Group Description・・・説明（任意：参照用など、用途に合わせて記載下さい）
- Password・・・再設定用パスワード（大文字小文字含む英字＋数字＋記号の 8 文字以上）

2. Group Policy

「Select all」をクリックし、「user consent for in-band KVM」のみチェックを外します。

（この場合、Desktop タブ経由のリモートデスクトップ開始時にユーザ同意コードの入力が省略されます）

Endpoint Group Setup

Define the policy and enable Intel® AMT auto-setup (optional) -- for a group of endpoints.

1 Define the group 2 Generate agent installation files

1 Create a new group

Group Name: EMA-endpointgroup-test3

Group Description: エンドポイントグループテスト3

Password (required to change the policy later):

Save & Intel® AMT autosetup

2 Group Policy

Enable Intel® EMA users with execute rights to use these capabilities on the group:

Power operations

- ☒ Wakeup
- ☒ Sleep
- ☒ Turn off or restart

Messaging and alerts

- ☒ TCP traffic relay
- ☒ Alert messages
- ☒ Console prompts
- ☒ Location information
- ☒ Peer-to-peer communication

Remote control

- ☒ Remote KVM
- ☒ Remote file access
- ☒ Remote management (vmm)
- ☐ User Consent for In-Band KVM

Select all

Generate agent installation files

図 4-1-1-4-③ Endpoint Group Setup 画面

- ④ 入力完了後、「Save & Intel® AMT autosetup」をクリックします。（図 4-1-1-4-④）

Endpoint Group Setup

Define the policy and enable Intel® AMT auto-setup (optional) -- for a group of endpoints.

1 Define the group 2 Generate agent installation files

1 Create a new group

Group Name
EMA-endpointgroup-test3

Group Description
エンドポイントグループテスト3

Password (required to change the policy later)

Save & Intel® AMT autosetup

2 Group Policy

Enable Intel® EMA users with execute rights to use these capabilities on the group:

Power operations

- ☒ Wakeup
- ☒ Sleep
- ☒ Turn off or restart

Messaging and alerts

- ☒ TCP traffic relay
- ☒ Alert messages
- ☒ Console prompts
- ☒ Location information
- ☒ Peer-to-peer communication

Remote control

- ☒ Remote KVM
- ☒ Remote file access
- ☒ Remote management (WMI)
- ☐ User Consent for In-Band KVM

Select all

Generate agent installation files

図 4-1-1-4-④ Endpoint Group Setup 画面

- ⑤ Intel®AMT autosetup 画面に移動したら、「Enabled」にチェックを入れ、以下設定を入力し、「Save」をクリックします。(図 4-1-1-4-⑤)
- Intel®AMT profile・・・既存のプロファイルを選択
 - Activation method・・・「Certificate Provisioning (TLS-PKI)」を選択
 - Administrator Password : 8 文字以上、大文字小文字数字特殊文字をいずれも 1 つ以上含む文字列を入力
 - Intel® MEBX Password Configuration・・・「Do not set the password」にチェック
(今回の実証実験ではこちらを選択しております)

Intel® AMT autosetup (EMA-endpointgroup-test3)

After setting up, any endpoint joining this group and supporting Intel® AMT will automatically be activated. Need to have at least 1 Intel® AMT profile.

☒ Enabled

Intel® AMT profile: EMA-test-profile

Activation Method: Certificate Provisioning (TLS-PKI)

Administrator Password: [password field] ☐ display

Intel® MEBX Password Configuration

☐ Set a random password per endpoint (recommended)

☒ Do not set the password (not recommended)

Certificates Details:

Available Certificates: ema-certificate_test

Domain: intel.vprodemo.com

Save

図 4-1-1-4-⑤ Intel®AMT autosetup 画面

- ⑥ 作成したエンドポイントグループ名が表示されることを確認します。(図 4-1-1-4-⑥)

Endpoint group

Manage endpoints by placing them into an endpoint group where they will share a common set of permissions and optionally an associated Intel® AMT autosetup.

Endpoint Groups Intel® AMT Profiles

Search endpoint groups [search icon]

New endpoint group...

Name	Endpoint Count	
EMA-endpointgroup-test3	0	...
EMA-endpointgroup-test4	1	...
EMA-endpointgroup-test	3	...

図 4-1-1-4-⑥ Endpoint Group 管理画面

4.1.1.5 エンドポイント（クライアント PC） 導入

前述(4.1.1.4)で作成したエンドポイントグループにエンドポイント(クライアント PC)を認識させる手順を記載します。また、エンドポイント（クライアント PC）を別のエンドポイントグループに入れ替えする場合もこちらの手順で実施出来ます。

- ① 作成したエンドポイントグループ右側にある「…」をクリックし、「Create Agent Files」をクリックします。
(図 4-1-1-5-①)

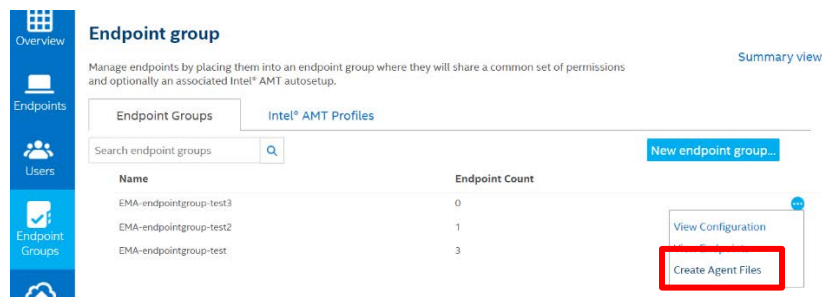


図 4-1-1-5-① Endpoint Group 管理画面

② Generate Agent Installation Files 画面に移動しますので、以下手順にてエージェントをインストールする為のファイルをダウンロードします。(図 4-1-1-5-②)

(1) エージェント端末の Windows OS によって、ダウンロードするエージェントファイルを選択します。

・Windows OS が 32bit の場合、「Windows (32-bit) Service」にチェック

・Windows OS が 64bit の場合、「Windows (64-bit) Service」にチェック

(2) チェックした項目の右側に表示される「Download」ボタンをクリックします

(3) Agent policy file 右側の「Download」ボタンをクリックします

※特にダウンロード先の設定を行っていない場合は、ダウンロードフォルダにダウンロードされます

(4) ダウンロードが完了したら、「Done」をクリックします

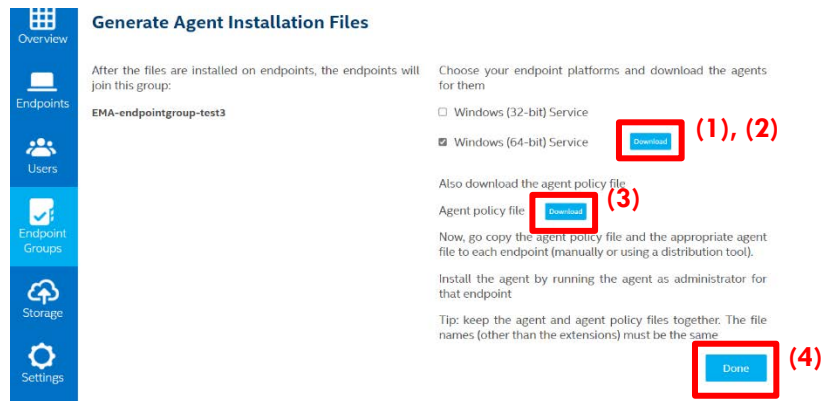


図 4-1-1-5-② Generate Agent Installation Files 画面

- ③ ダウンロードした拡張子が「.exe」「.msh」のファイルを USB メモリなどの外部記憶媒体にコピーします。

【ダウンロード詳細手順】

※以下は「Microsoft Edge」での画面になります。ダウンロードの画面はブラウザによって異なります。

・右上の「↓」ボタンでダウンロードの進捗が確認できます。（図 4-1-1-5-③）



図 4-1-1-5-③ ダウンロード画面

・「ファイルを開く」との文言が出ていればダウンロード完了しています。（図 4-1-1-5-④）

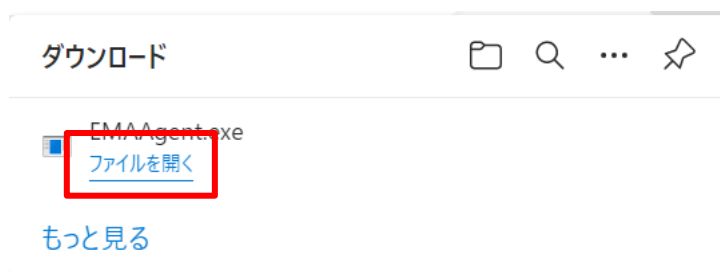


図 4-1-1-5-④ ダウンロード完了画面

・危険なファイルとしてブロックされる場合は右にある「…」をクリックします。（図 4-1-1-5-⑤）

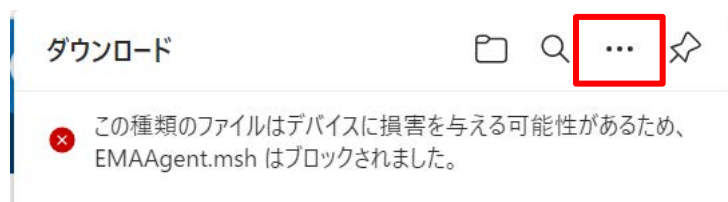


図 4-1-1-5-⑤ ダウンロードエラー画面

・メニューが表示されますので、「保存」をクリックします。（図 4-1-1-5-⑥）

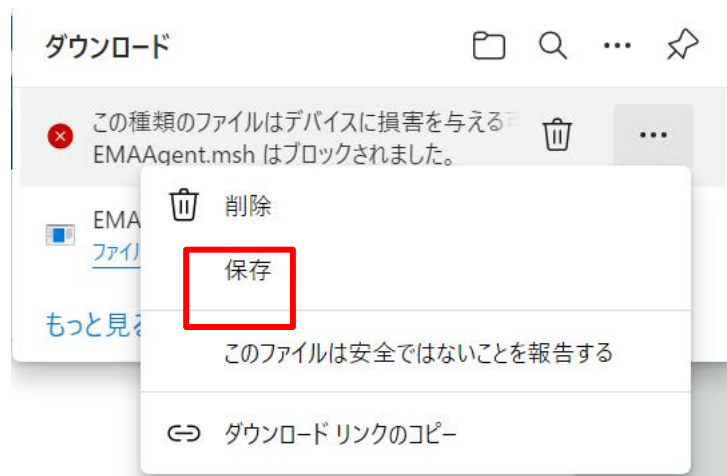


図 4-1-1-5-⑥ ダウンロードエラー画面

・ダウンロードされたファイルは通常「ダウンロード」フォルダに格納されます。（図 4-1-1-5-⑦）

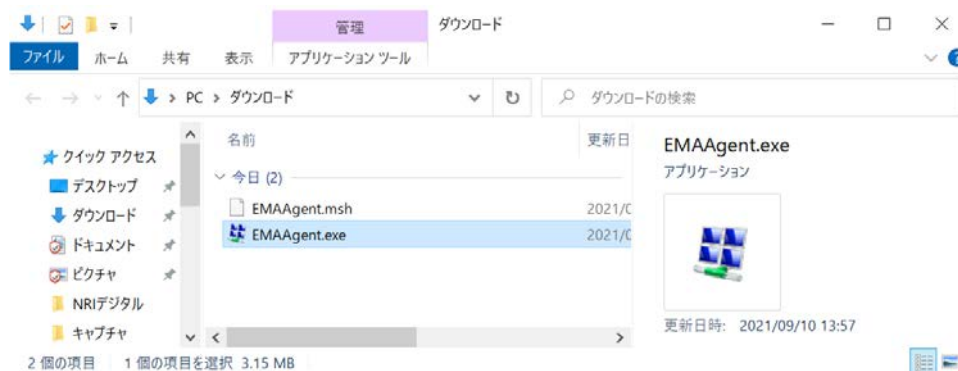


図 4-1-1-5-⑦ ダウンロード確認画面

※項番④～⑫までの設定は Wifi ネットワーク接続環境で Admin Control Mode モード（管理者による強制リモート接続設定）で運用する為に必要な設定ですので Client Control Mode モード（リモート接続時にユーザ側の同意が必要な設定）の場合、不要になります。

- ④ インテル®EMA で管理を行いたいクライアント PC をシャットダウンから起動または、再起動をします。起動中、HP のロゴが表示された際に以下操作を行い、MEBx 画面に入ります。

操作は以下になります。

・起動時[F6]、または起動時[ESC]、スタートアップメニューで[F6]

- ⑤ MEBx メニュー画面が表示されますので、「MEBx Login」を選択し「Enter」キーを押下します。（図 4-1-1-5-③）

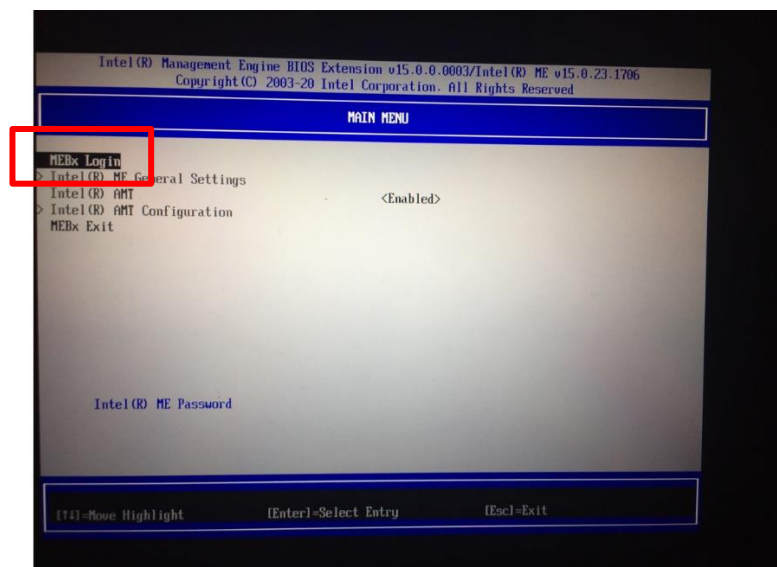


図 4-1-1-5-③ MEBx メニュー画面

- ⑥ MEBx のパスワードを入力します。初期パスワードは「admin」ですが、パスワード変更を求められた場合は、前述（図 4-1-1-4-⑤ Intel®AMT autosetup 画面）で設定した Administrator Password を入力します。（図 4-1-1-5-④）

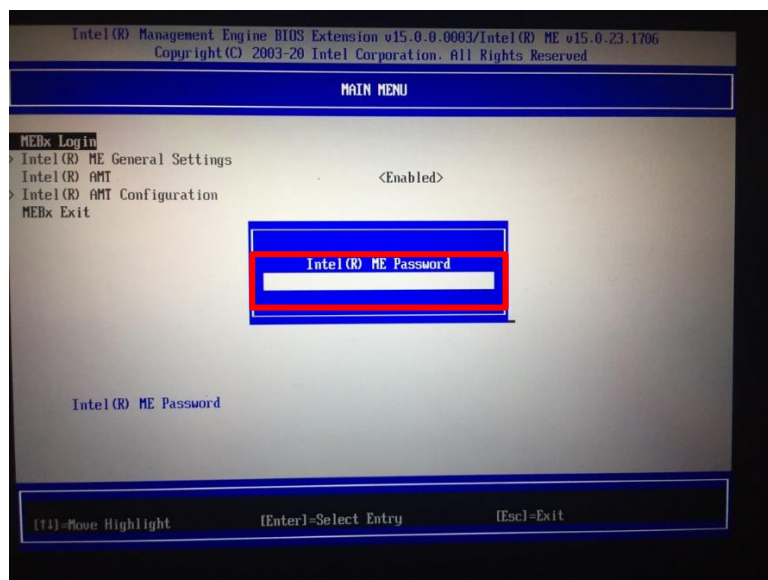


図 4-1-1-5-④ MEBx メニュー画面

- ⑦ 「Intel® AMT Configuration」にカーソルを合わせ、「Enter」キーを押下します。（図 4-1-1-5-⑤）

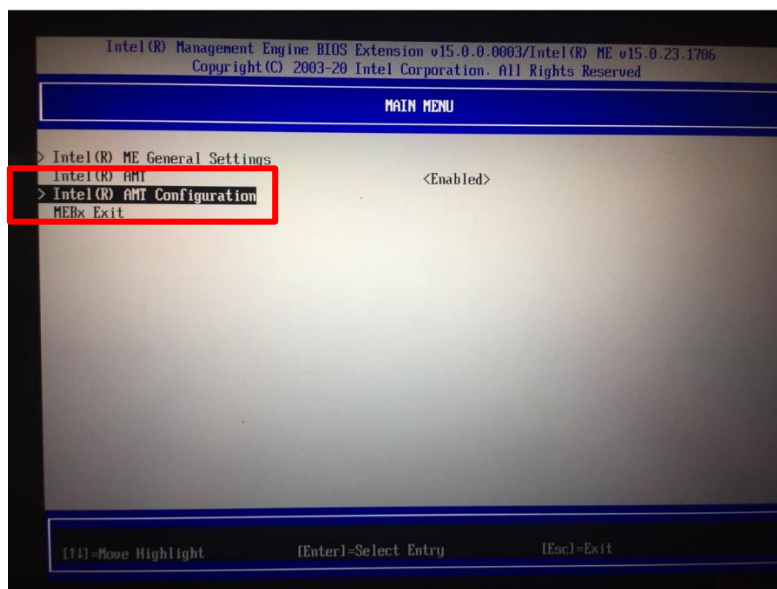


図 4-1-1-5-⑤ MEBx メニュー画面

- ⑧ 「Remote setup and configuration」にカーソルを合わせ、「Enter」キーを押下します。(図 4-1-1-5-⑥)

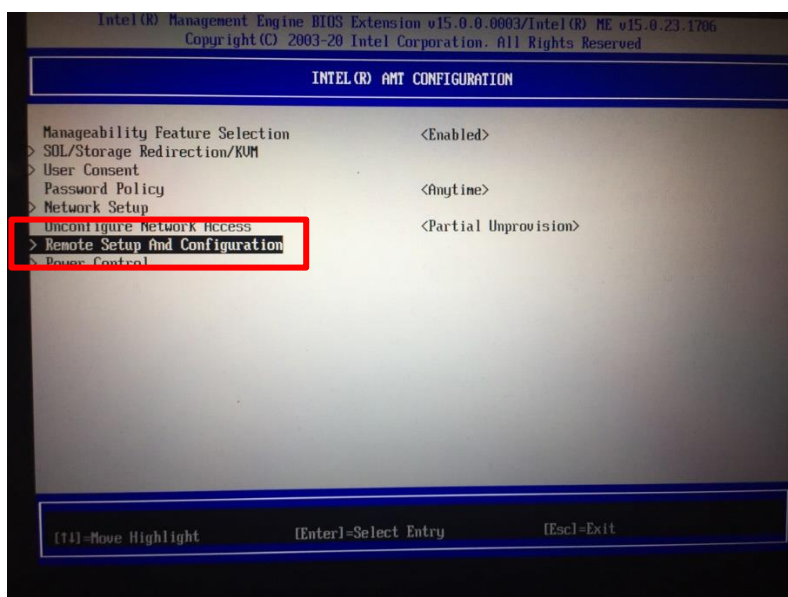


図 4-1-1-5-⑥ MEBx メニュー画面

- ⑨ 「TLS PKI」にカーソルを合わせ、「Enter」キーを押下します。(図 4-1-1-5-⑦)

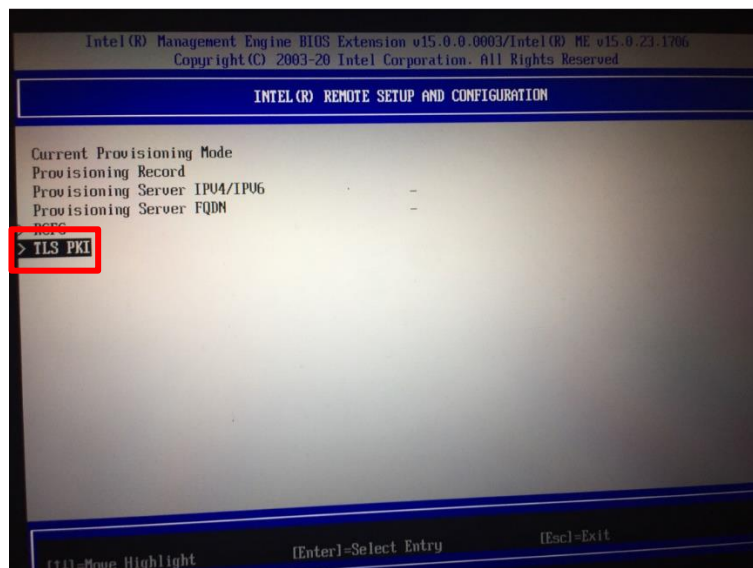


図 4-1-1-5-⑦ MEBx メニュー画面

- ⑩ 「PKI DNS suffix」にカーソルを合わせ、「Enter」キーを押下します。（図 4-1-1-5-⑧）

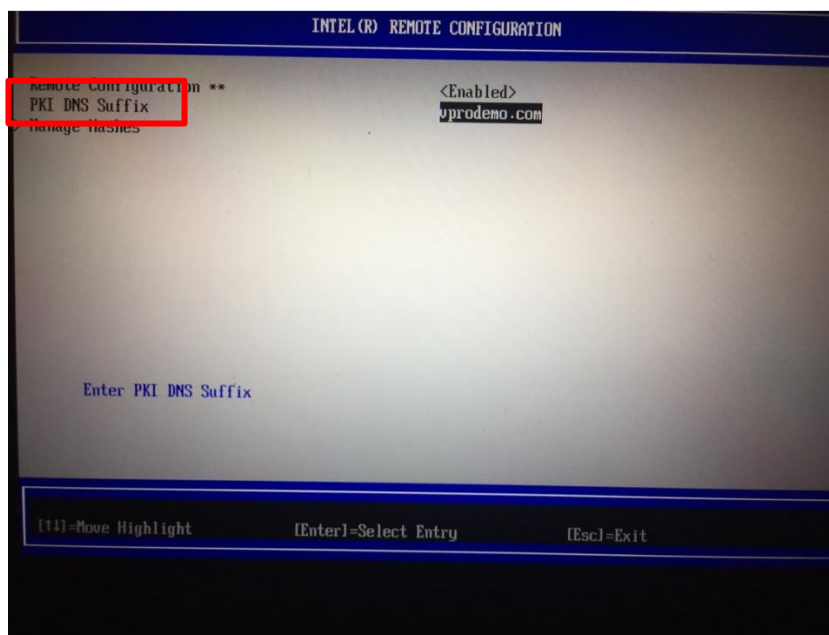


図 4-1-1-5-⑧ MEBx メニュー画面

- ⑪ 表示された入力欄に、証明書(※1)のドメインを入力し、「Enter」キーを押下します。(図 4-1-1-5-9) (例 : vprodemo.com)

※1 ユーザの同意なくリモート接続可能な管理者コントロール・モード (ACM) でインテル® AMT をエンドポイントにプロビジョニングするには、インテル® AMT PKI 証明書が必要です。PKI 証明書がない場合、インテル® EMA はインテル® AMT をクライアント・コントロール・モード (CCM) でプロビジョニングします。CCM では、各エンドポイントにおいてリモート操作についてユーザの同意が必要になります。

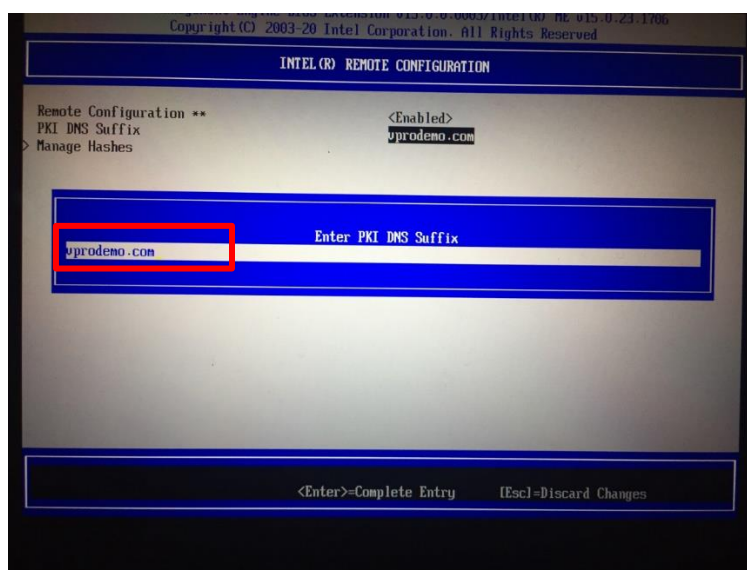


図 4-1-1-5-9 MEBx メニュー画面

- ⑫ ESC キーを 3 回押下して、「Are you sure you want to exit? (Y/N) 」と表示されますので「Y」キーを押下して MEBx 画面を終了します。(図 4-1-1-5-⑩)

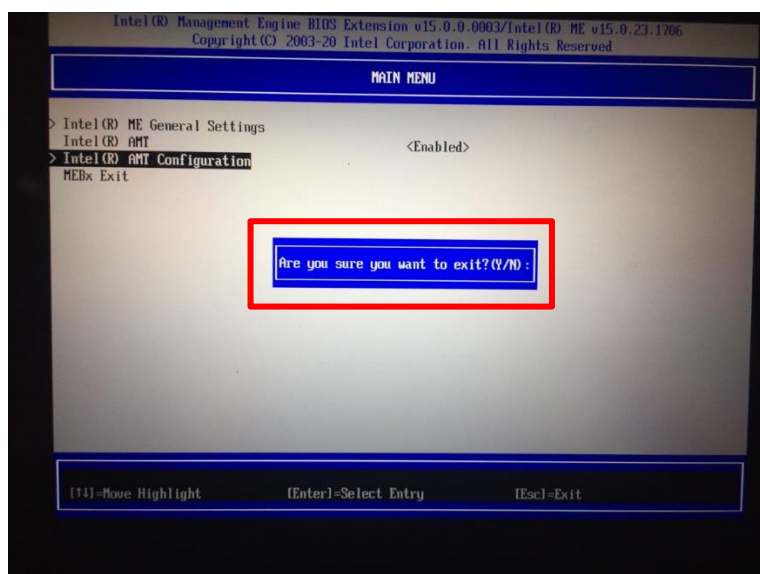


図 4-1-1-5-⑩ MEBx メニュー画面

- ⑬ クライアント PC に戻り、C ドライブに「EMAAgent」という名前のフォルダを作成します。(図 4-1-1-5-⑪)

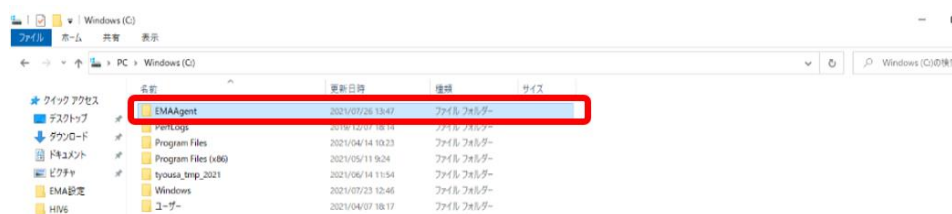


図 4-1-1-5-⑪ フォルダ作成画面

- ⑭ 手順③で外部媒体に保存したファイルを「EMAAgent」フォルダにコピーします。(図 4-1-1-5-⑫)



図 4-1-1-5-⑫ ファイルコピー画面

- ⑮ 「EMAAgent.exe」を右クリックし、管理者として実行をクリックします。(図 4-1-1-5-⑬)

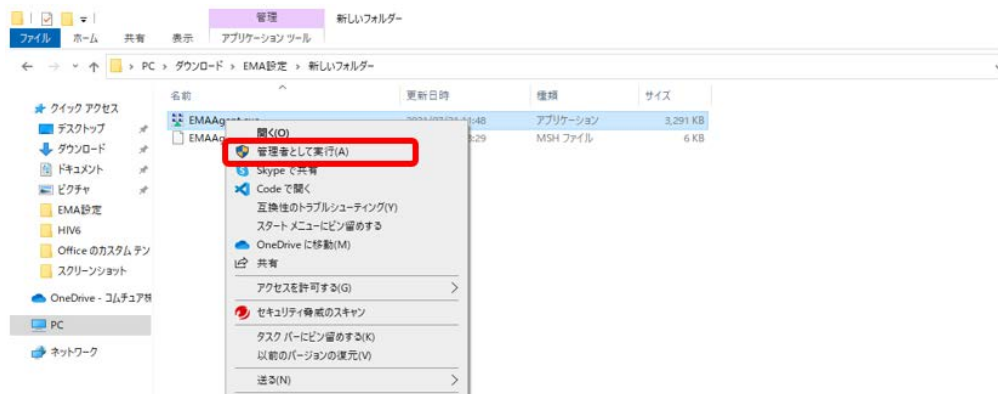


図 4-1-1-5-⑬ ファイル実行画面

- ⑯ 「このアプリがデバイスに変更を加えることを許可しますか？」というポップアップが表示された場合、「はい」をクリックします。(図 4-1-1-5-⑭)



図 4-1-1-5-⑭ ファイル実行確認画面

- ⑰ Intel®EMA Agent Installer が開きますので、「Install/Update」をクリックします。完了したら、自動で画面が閉じます。（図 4-1-1-5-⑮）

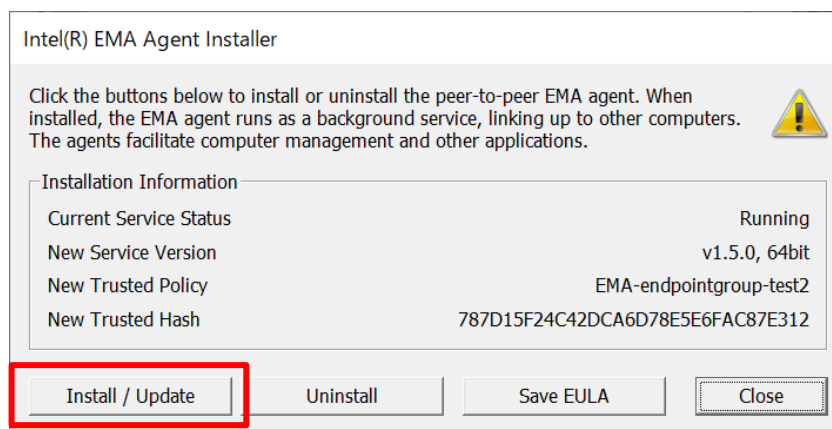


図 4-1-1-5-⑮ Intel®EMA Agent Installer 画面

- ⑱ インテル®EMA 管理画面に戻り、「EndPoint Groups」をクリック後、「View Endpoints」をクリックします。（図 4-1-1-5-⑯）

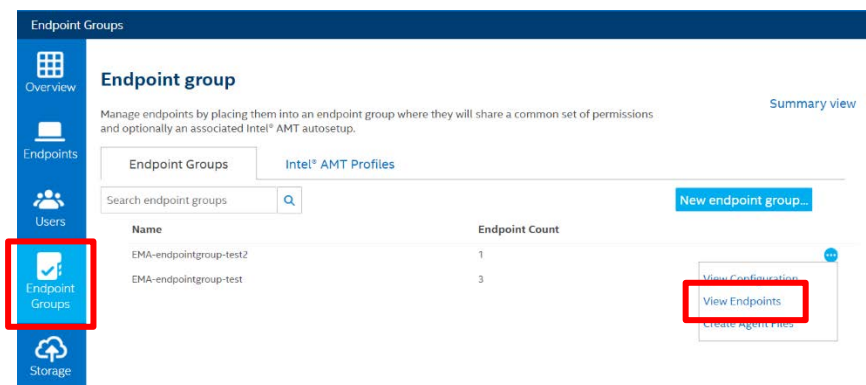


図 4-1-1-5-⑯ Endpoint Groups 画面

- ①⑨ 「Load all Endpoints」をクリックします。(図 4-1-1-5-①⑨)

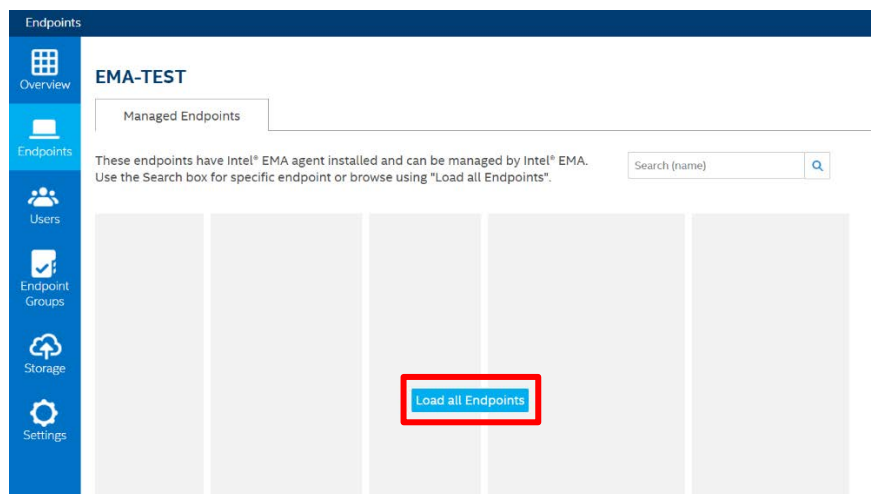


図 4-1-1-5-①⑨ Endpoints 画面

- ②⑩ エージェントをインストールしたクライアント PC が Endpoint メニューへ登録されたことを確認します。(図 4-1-1-5-②⑩) ※反映に 5 分ほど掛かります。

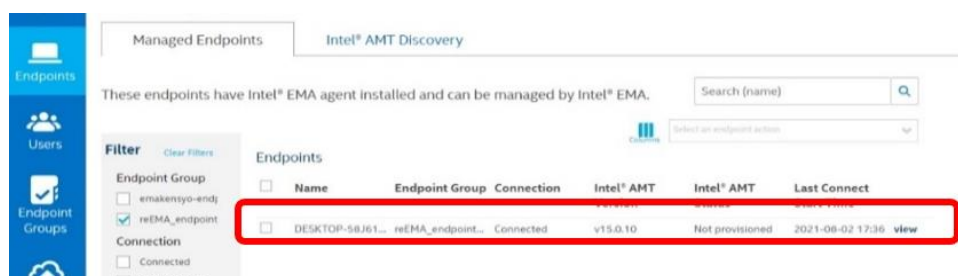


図 4-1-1-5-②⑩ Endpoint 管理画面

4.1.1.6 ユーザグループとエンドポイントグループの関連付け

インテル®EMA 管理画面より前述で作成したユーザグループとエンドポイントグループを関連付ける必要がありますので、以下に手順を記載します。

- ① テナント管理者権限のユーザでログイン後、Overview 画面が表示されるので、左側メニューにある「Users」を選択します。（図 4-1-1-6-①）

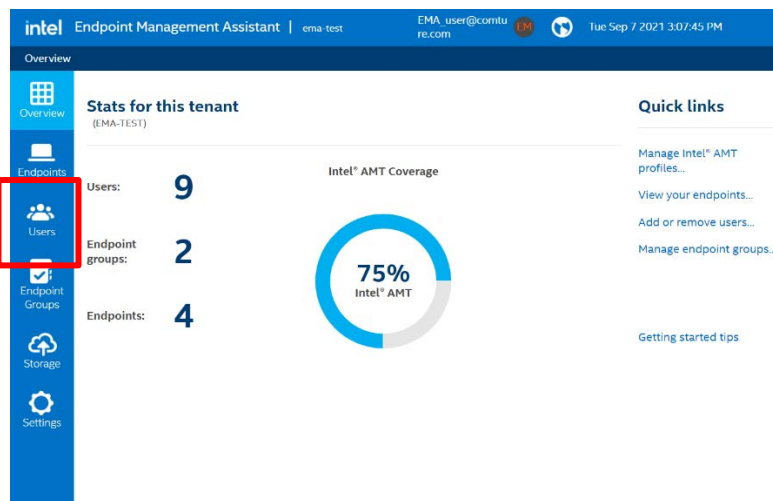


図 4-1-1-6-① Over View 画面

- ② Users 画面が表示されるので、「User Groups」タブを選択します。エンドポイントグループと関連のづけたいユーザグループの右側の「...」ボタンをクリックし、メニューが表示されるので、「Assign Endpoint Groups...」を選択します。（図 4-1-1-6-②）

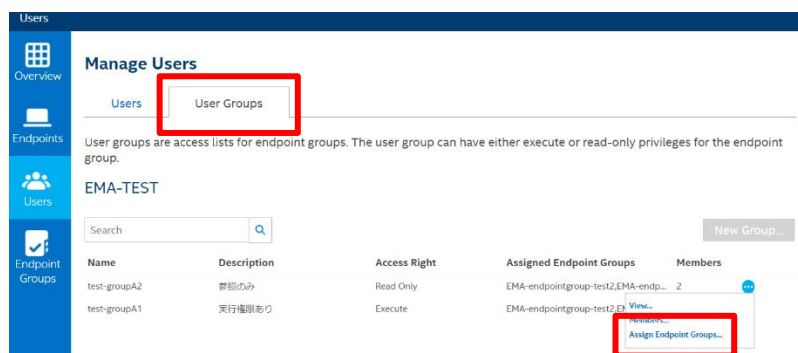


図 4-1-1-6-② ユーザグループ選択画面

- ③ Edit Group 画面が表示されるので、関連付けを行う、エンドポイントグループを選択し、「Save」をクリックします。(図 4-1-1-6-③)

Edit Group

General **Members** **Endpoint Groups**

Select the endpoint groups for this user group:

☒ **Endpoint Groups**

- ☒ EMA-endpointgroup-test2
- ☒ EMA-endpointgroup-test

Previous Page 1 of 1 Next

Save Cancel

図 4-1-1-6-③ エンドポイントグループ選択画面

4.1.2 リモート電源制御

この章ではインテル®EMA からの電源制御(一括制御および個別での制御)について説明します。

4.1.2.1 リモート電源一括制御

ここで複数台のエンドポイント (クライアント PC) の電源を一括で制御する方法を以下に記載します。

- ① ブラウザにてインテル®EMA サーバの DNS 名を入力し、インテル®EMA へ接続 (URL:https://[インテル®EMA サーバの DNS 名]) し、インテル®EMA サーバ作成時に設定した user name と Password を入力、Log In ボタンをクリックしログインします。(図 4-1-2-1-①)

※「テナント管理者」または「エンドポイント管理者」権限が設定されているユーザでログインします。

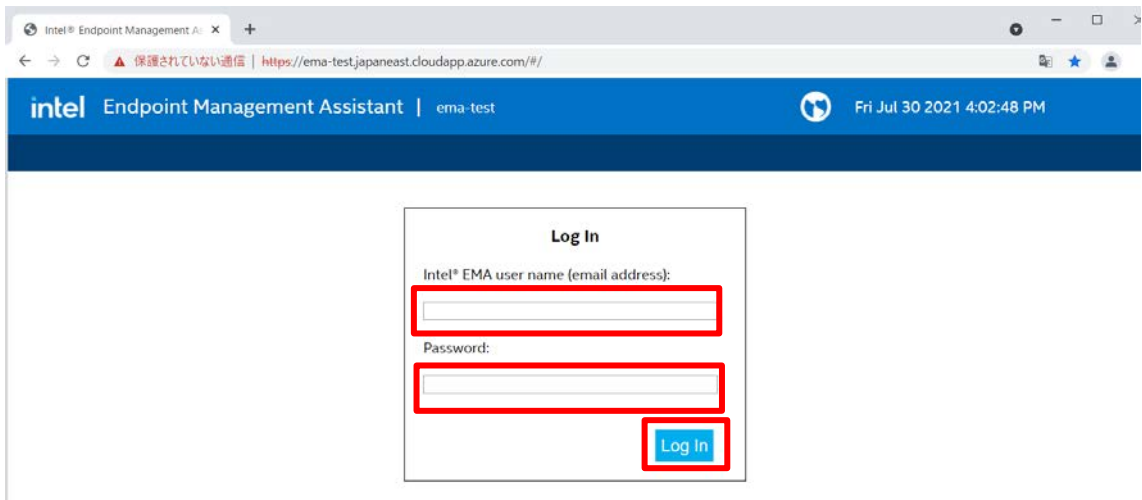


図 4-1-2-1-① ログイン画面

② OverView 画面が表示されるので、左側メニューから「Endpoints」を選択します。(図 4-1-2-1-②)

※現在管理されているクライアント PC の一覧とその状態が確認できます。

intel Endpoint Management Assistant | ema-test inoue_yuka@comt ure.com Thu Jul 29 2021 12:13:46 PM

Endpoints

Overview
Endpoints
Users
Endpoint Groups
Storage
Settings

EMA-TEST

Managed Endpoints Intel® AMT Discovery

These endpoints have Intel® EMA agent installed and can be managed by Intel® EMA.

Search (name) []

Select an endpoint action []

Filter Clear Filters

Endpoint Group
☐ EMA-endpointgr

Connection
☐ Connected
☐ Not Connected

Power State
☐ On
☐ Off
☐ Sleep
☐ Hibernating
☐ Unknown

Intel® AMT Status
☐ Provisioned
☐ Not provisioned
☐ Provisioning
☐ None

Name	Endpoint Group	Connection	Intel® AMT Version	Intel® AMT Status	Last Connect Start Time
DESKTOP-80LM...	EMA-endpointgr...	Connected	v12.0.49	Provisioned	2021-07-29 11:34 view
DESKTOP-8VH4...	EMA-endpointgr...	Connected	v15.0.10	Provisioned	2021-07-29 11:07 view
LAPTOP-T1NO1...	EMA-endpointgr...	Connected	v11.8.86	Provisioned	2021-07-29 09:07 view

Previous Page 1 of 1 Next

VER 1.4.0.0 Intel Support Terms & privacy

図 4-1-2-1-② エンドポイント一覧画面

- ③ 電源を制御したいエンドポイント(クライアント PC) のチェックボックスにチェックを入れます。そして画面右上の「Select an endpoint action」をクリックすると、実行できる制御リストが表示されます。(図 4-1-2-1-③)

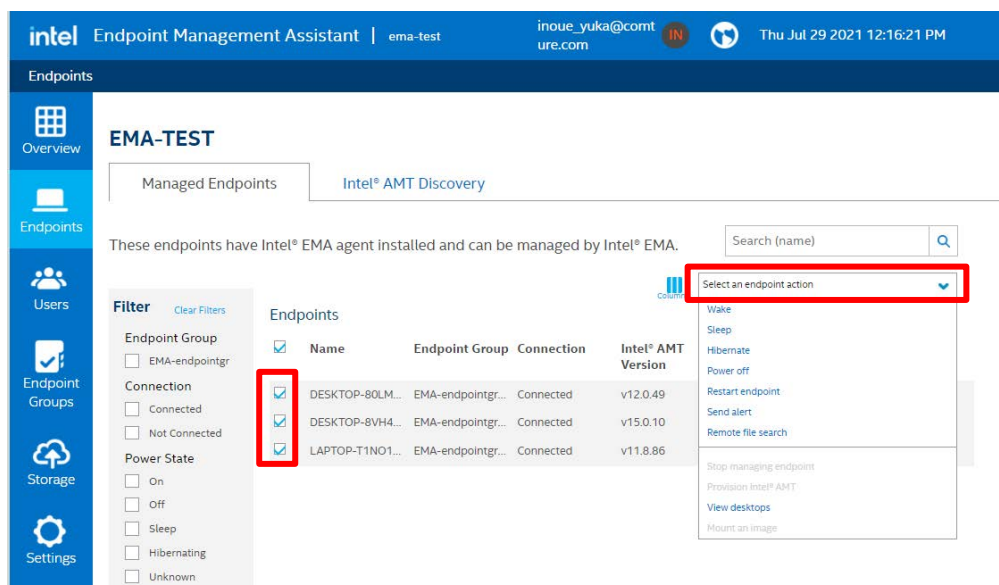


図 4-1-2-1-③ Endpoints 画面からの「Select an endpoint action」一覧

※以下に「select an endpoint action」で実行できる機能を紹介します。（表 4-1-2-1-①）

表 4-1-2-1-① Select an endpoint action 一覧と機能

制御一覧	機能
Wake	PC の起動
Sleep	スリープ状態への移行
Hibernate	休止状態への移行
Power off	PC の電源切断
Restart endpoint	PC の再起動
Send alert	アラートの送信 アラートメッセージをポップアップ・ウィンドウとして送信する
Remote file search	指定フォルダに対して、ファイルの検索実施 ダウンロードも可能
Stop managing endpoint	エンドポイントの管理の停止 インテル® EMA から削除する
Provision intel AMT	インテル® AMT のプロビジョニング情報を開く
View desktops	デスクトップ表示
Mount an image	イメージのマウント

※画面の左側に「Filter」部分があります。これは選択した状態のエンドポイントのみを表示することが可能になります。(図 4-1-2-1-④)

Filter [Clear Filters](#)

(1) **Endpoint Group**
☐ EMA-endpointgr

Connection
 (2) ☐ Connected
☐ Not Connected

Power State
 (3) ☐ On
☐ Off
☐ Sleep
☐ Hibernating
☐ Unknown

Intel® AMT Status
☐ Provisioned
☐ Not provisioned
☐ Provisioning
☐ None

図 4-1-2-1-④ Filter 一覧

<Filter について>

	フィルタ名	説明
(1)	Endpoint Group	選択したエンドポイントグループに所属しているエンドポイント（クライアント PC）を表示する
(2)	Connect	選択した接続状態のエンドポイント（クライアント PC）を表示する
(3)	Power State	選択した電源の状態のエンドポイント（クライアント PC）を表示する
(4)	Intel AMT Status	インテル®AMT の状態のエンドポイント（クライアント PC）を表示する

4.1.2.2 リモート電源個別制御

ここで個別にエンドポイント（クライアント PC）の電源を制御する方法を以下に記載します。個別に電源を制御する方法は以下の 2 つになります。

- 「General」タブからの電源制御方法
- 「Hardware Manageability」タブからの電源制御方法

●「General」タブからの電源制御方法

- ① ブラウザにてインテル®EMA サーバの DNS 名を入力し、インテル®EMA へ接続（URL:https://[インテル®EMA サーバの DNS 名]）し、インテル®EMA サーバ作成時に設定した user name と Password を入力、Log In ボタンをクリックしログインします。（図 4-1-2-2-①）

※テナント管理者またはエンドポイント管理者でログインします。

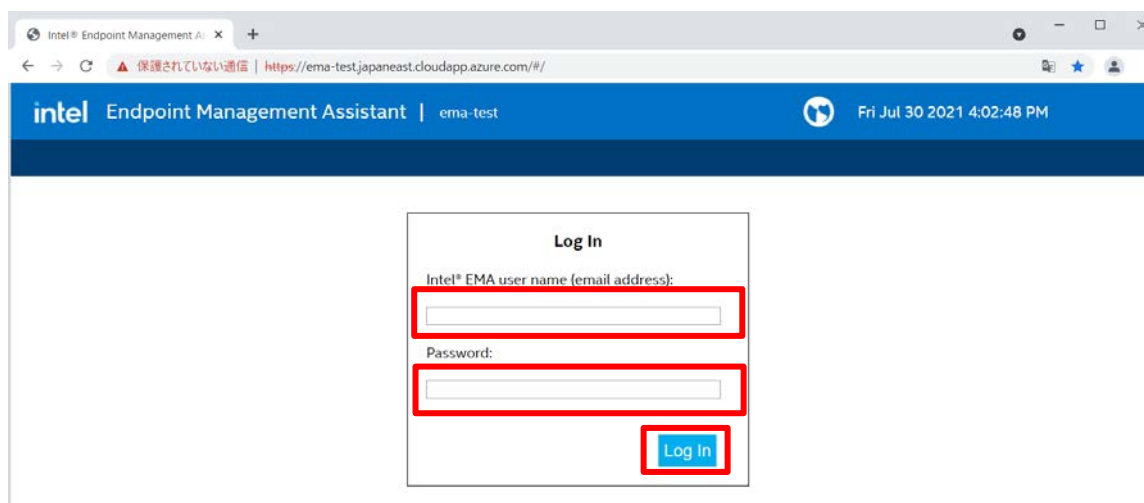


図 4-1-2-2-① ログイン画面

- ② 左メニューから「Endpoints」を選択します。(図 4-1-2-2-②)

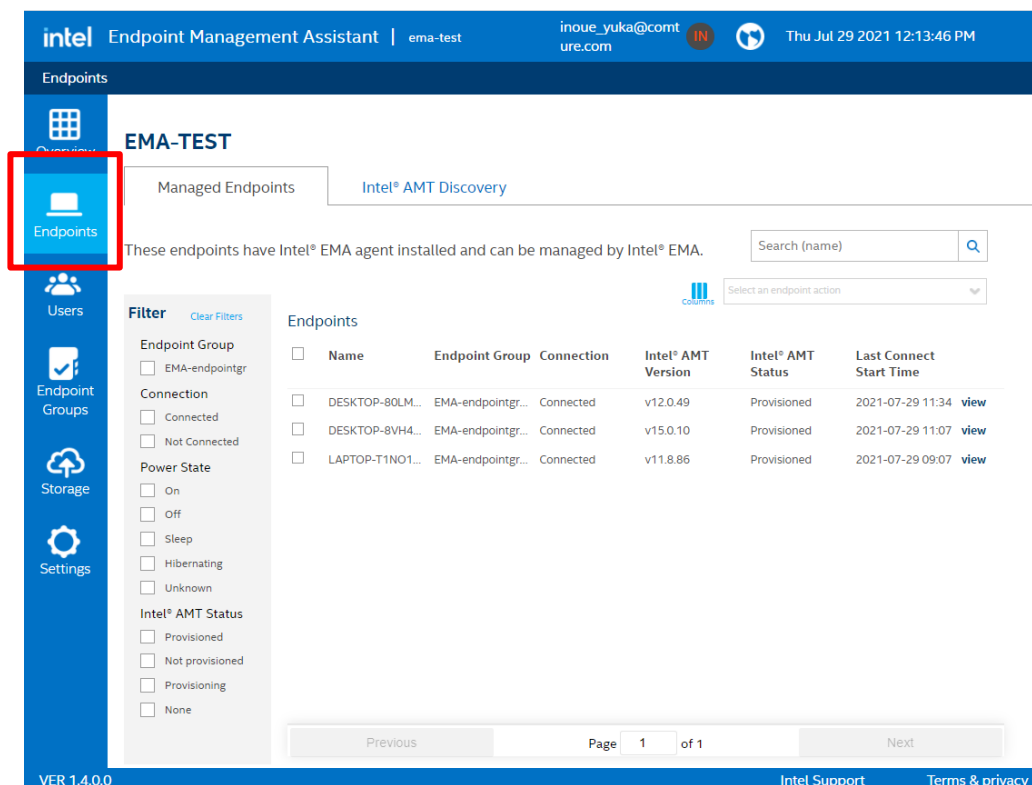


図 4-1-2-2-② Endpoints 一覧画面

- ③ 電源を制御したいエンドポイント(クライアント PC) の右側の「view」ボタンをクリックします。(図 4-1-2-2-③)

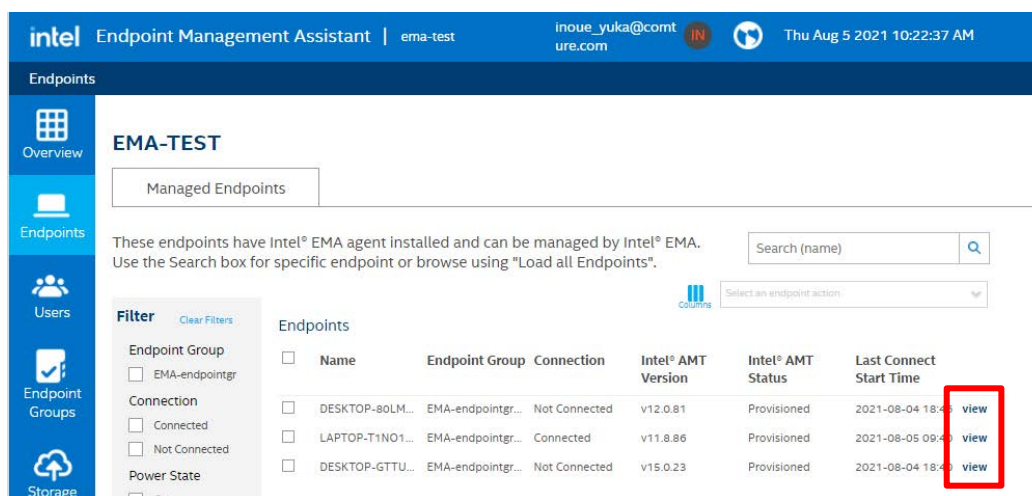


図 4-1-2-2-③ Endpoints 一覧画面

- ④ 現在の電源の状態が確認できます。(図 4-1-2-2-④)

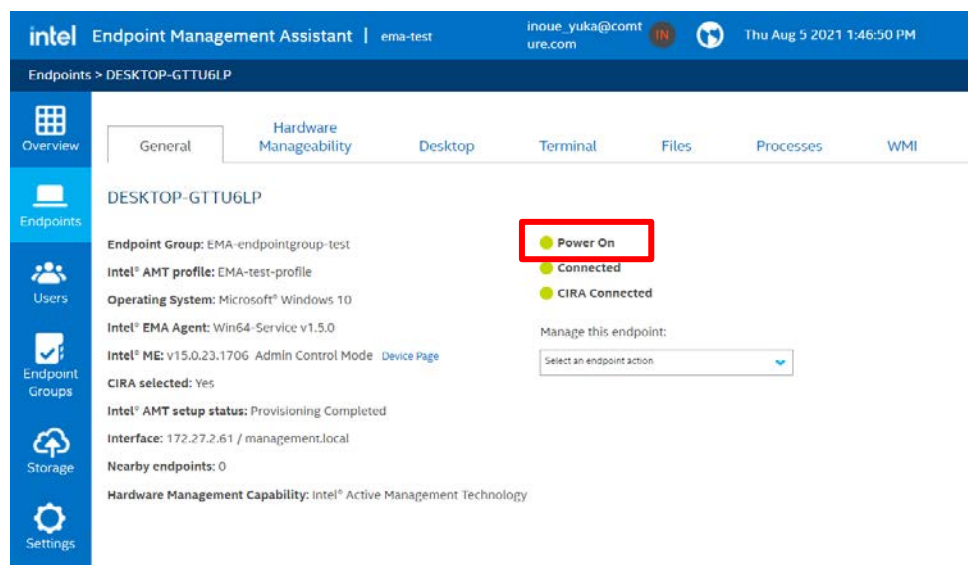


図 4-1-2-2-④ Endpoints 詳細画面

- ⑤ 画面右側にある「Manage this endpoint」-「Select an endpoint action」をクリックすると、制御リストが表示されますので、そこから実施したい制御を選択します。(図 4-1-2-2-⑤)
※制御内容は「4.1.2.1 リモート電源一括制御」の手順③と同様になります。

Manage this endpoint:

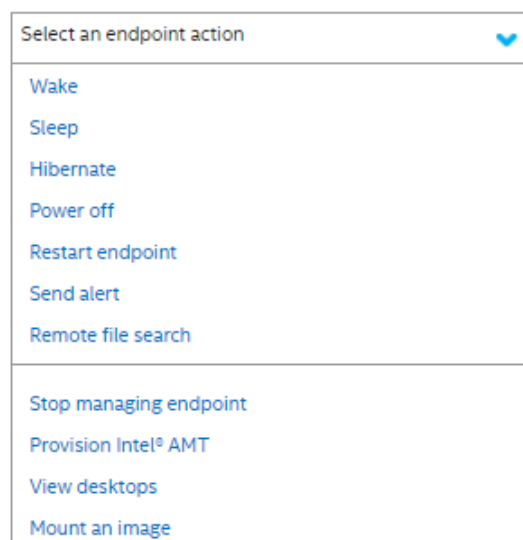


図 4-1-2-2-⑤ Manage this endpoint メニュー一覧

4.1.2.3 Hardware Manageability タブからのリモート電源個別制御

- ① ブラウザにてインテル®EMA サーバの DNS 名を入力し、インテル®EMA へ接続（URL:https://[インテル®EMA サーバの DNS 名]）し、インテル®EMA サーバ作成時に設定した user name と Password を入力、Log In ボタンをクリックしログインします。（図 4-1-2-3-①）

※テナント管理者またはエンドポイント管理者でログインします。

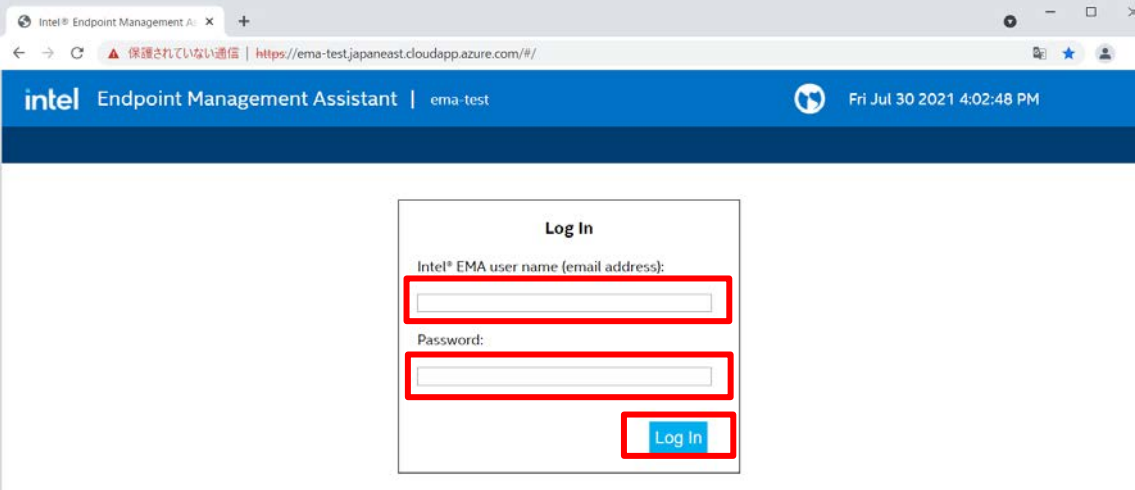


図 4-1-2-3-① ログイン画面

- ② 左メニューから「Endpoints」を選択します。(図 4-1-2-3-②)

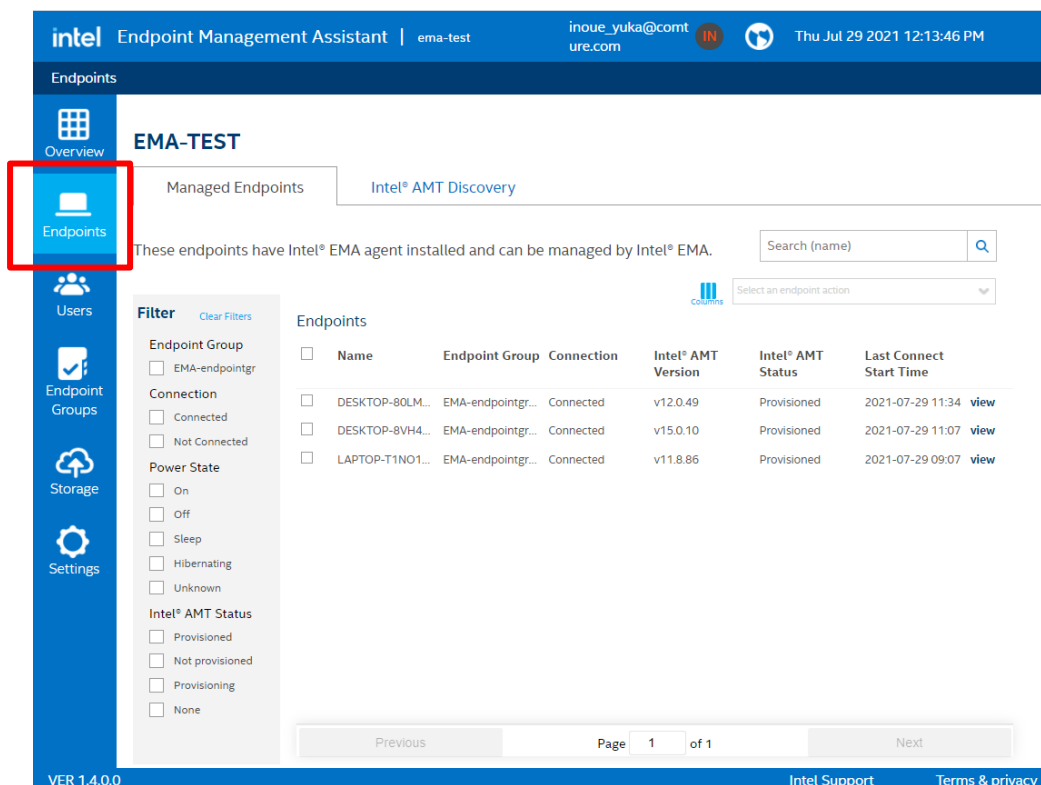


図 4-1-2-3-② Endpoints 一覧画面

- ③ 電源制御したエンドポイント(クライアント PC) の右側の「view」ボタンをクリックします。(図 4-1-2-3-③)

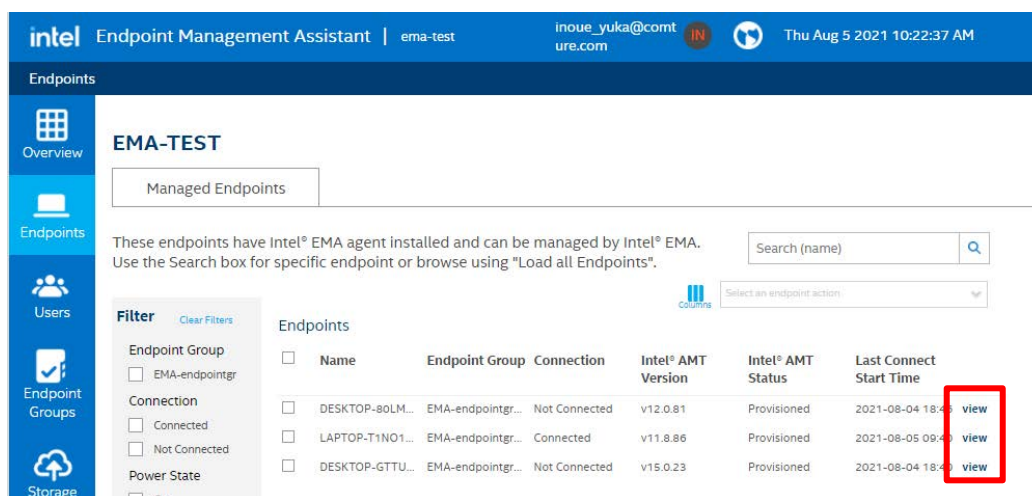


図 4-1-2-3-③ Endpoints 一覧画面

- ④ 「Hardware Manageability」タブをクリックします。(図 4-1-2-3-④)

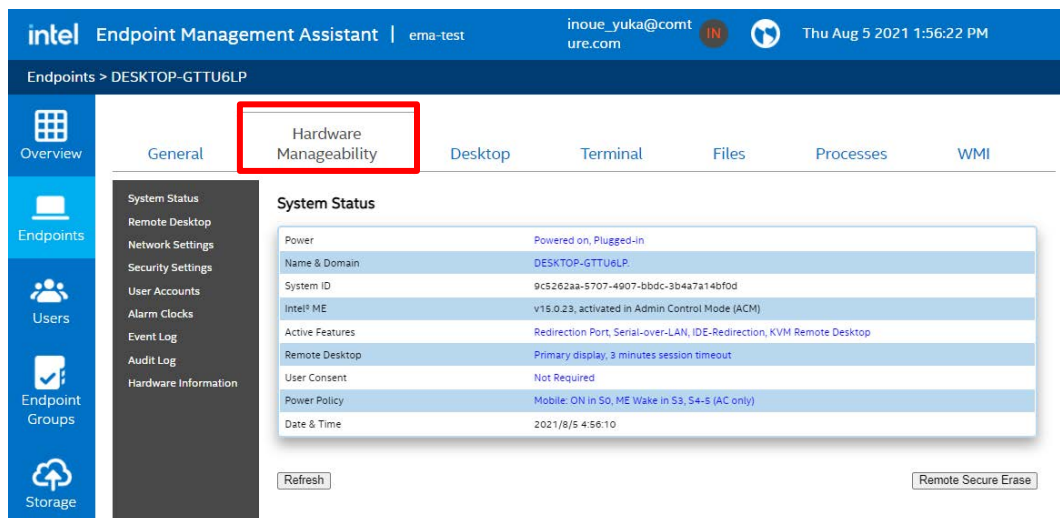


図 4-1-2-3-④ Hardware Manageability 画面

- ⑤ 左側のメニューにある「Remote Desktop」をクリックし、左上の「Power Actions」ボタンをクリックします。(図 4-1-2-3-⑤)

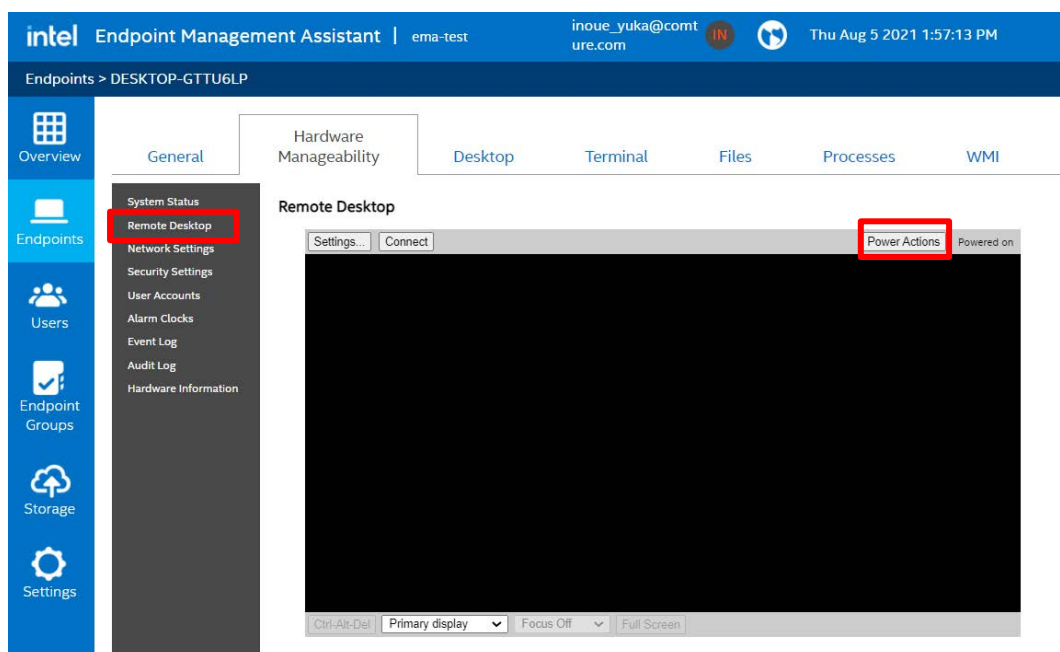


図 4-1-2-3-⑤ Remote Desktop 画面

- ⑥ 「PowerCommand」部分をクリックすると、制御リストが表示されますので、そこから実施したい制御を選択します。図 4-1-2-3-⑥)

※制御内容は「4.1.2.1 リモート電源一括制御」の手順③と同様になります。

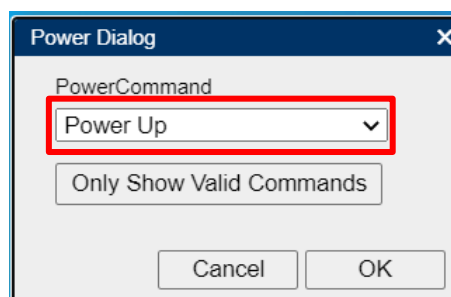


図 4-1-2-3-⑥ Power Dialog 初期画面

※「Power Command」それぞれの機能の説明は以下になります。（表 4-1-2-3-①）

表 4-1-2-3-① Only Show Valid Command 一覧と機能

制御一覧	機能
Power UP	PC の起動
Sleep	スリープ状態への移行
Hibernate	休止状態への移行
Power Down	PC の電源切断
Force Reset	PC の強制再起動
Soft off	間隔を置いての PC の電源切断
Reset	PC の再起動
Power up to BIOS	BIOS の起動
Reset to BIOS	PC 再起動からの BIOS 起動
Reset to IDE-R image	リモートのイメージからの再起動
Power on to IDE-R image	リモートのイメージからの起動
Reset to IDE-R CDROM	リモートの CD ドライブからの再起動
Power on to IDE-R CDROM	リモートの CD ドライブからの起動

※「Show All Power Actions」をクリックすると、「Only Show Valid Commands」に切り替わり
ます。(図 4-1-2-3-⑦-1)

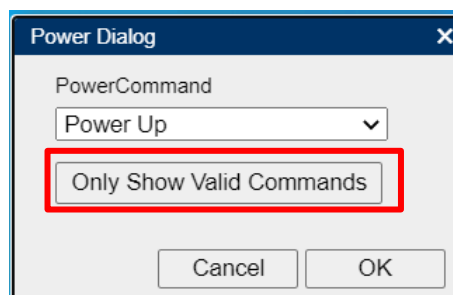


図 4-1-2-3-⑦-1 Power Dialog 初期画面

※「Only Show Valid Commands」をクリックすると、「Show All Power Actions」に切り替わり
ます。(図 4-1-2-3-⑦-2)

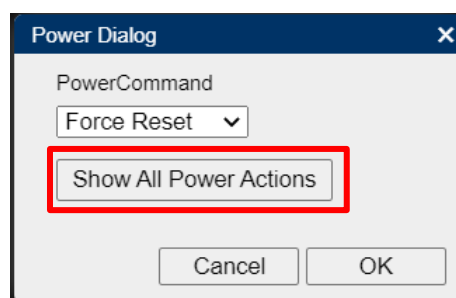


図 4-1-2-3-⑦-2 Only Show Valid Commands クリック時画面

「PowerCommand」は、上記「Only Show Valid Commands」(図 4-1-2-3-⑦-2) の状況から実行可能なパワーアクションが表示されます。(表 4-1-2-3-②)

(表示されるコマンドは、エンドポイント (クライアント PC) の状況によって表示内容は変わります)

表 4-1-2-3-② Show All Power Actions 一覧と機能

制御一覧	機能
Force Reset	PC の強制再起動
Power Down	PC の電源切断
Sleep	スリープ状態への移行
Hibernate	休止状態への移行
Reset	PC の再起動
Soft off	間隔を置いての PC の電源切断
Power Down	PC の電源切断
Reset to BIOS	PC 再起動からの BIOS 起動

4.1.3 ハードウェアアラームクロック機能

本章ではエンドポイント（クライアント PC）の起動時間をスケジュールできる、ハードウェアアラームクロック機能の設定手順を記載します。

- ① ブラウザにてインテル®EMA サーバの DNS 名を入力し、インテル®EMA へ接続（URL:https://[インテル®EMA サーバの DNS 名]）し、インテル®EMA サーバ作成時に設定した user name と Password を入力、Log In ボタンをクリックしログインします。（図 4-1-3-①）

※「テナント管理者」または「エンドポイント管理者」権限が設定されているユーザでログインします。

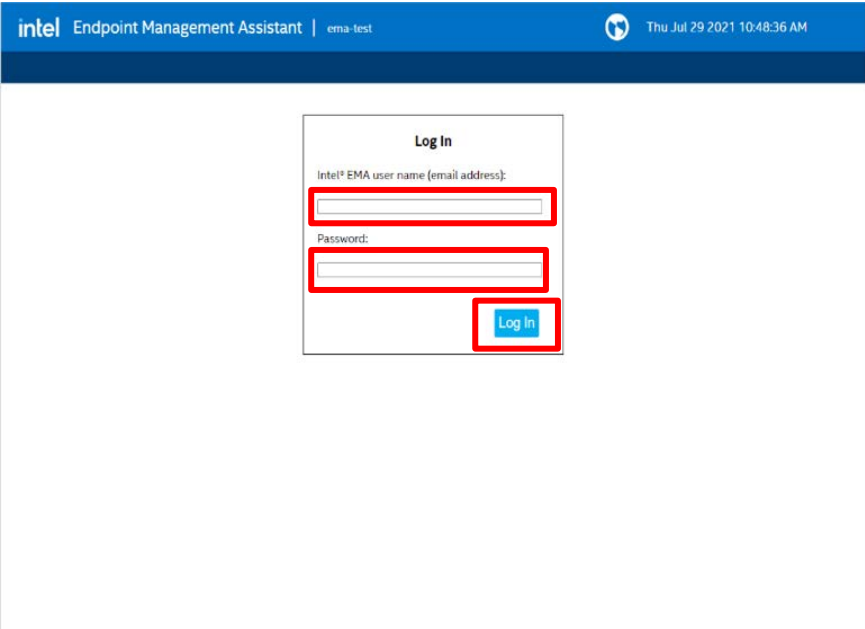


図 4-1-3-① ログイン画面

- ② Overview 画面が表示されるので、左側のメニューにある「Endpoints」を選択します。（図 4-1-3-②）

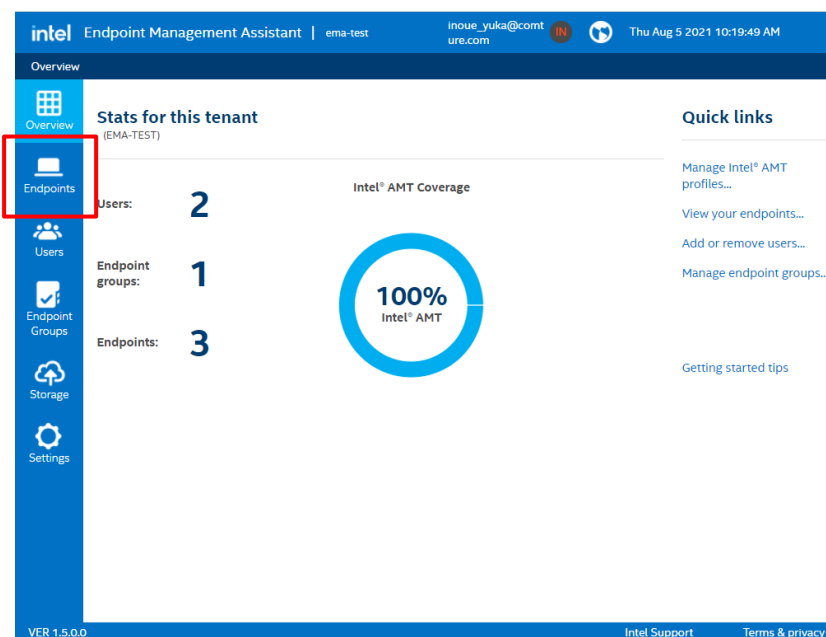


図 4-1-3-② ログイン後のトップ画面

- ③ 「Load all Endpoints」をクリックします。（図 4-1-3-③）

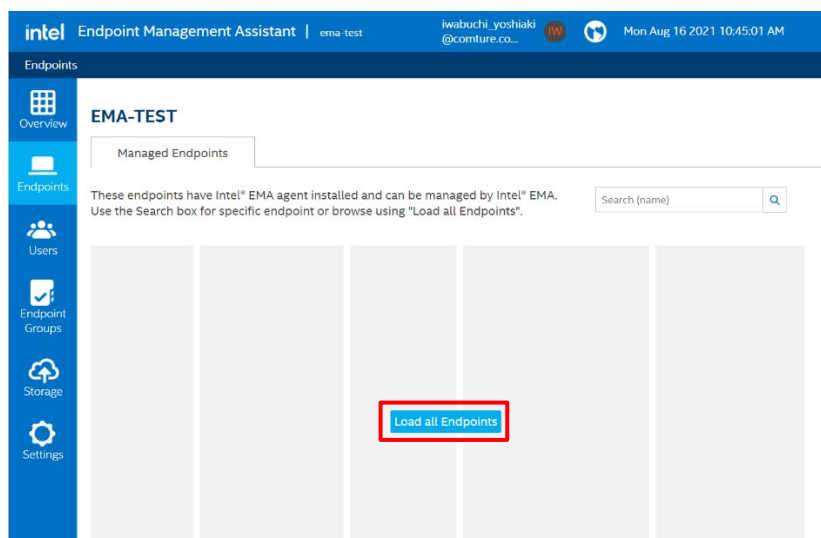


図 4-1-3-③ Endpoint 選択画面

- ④ ハードウェアアラームクロック機能を設定したい、エンドポイント（クライアント PC）の「View」をクリックします。（図 4-1-3-④）

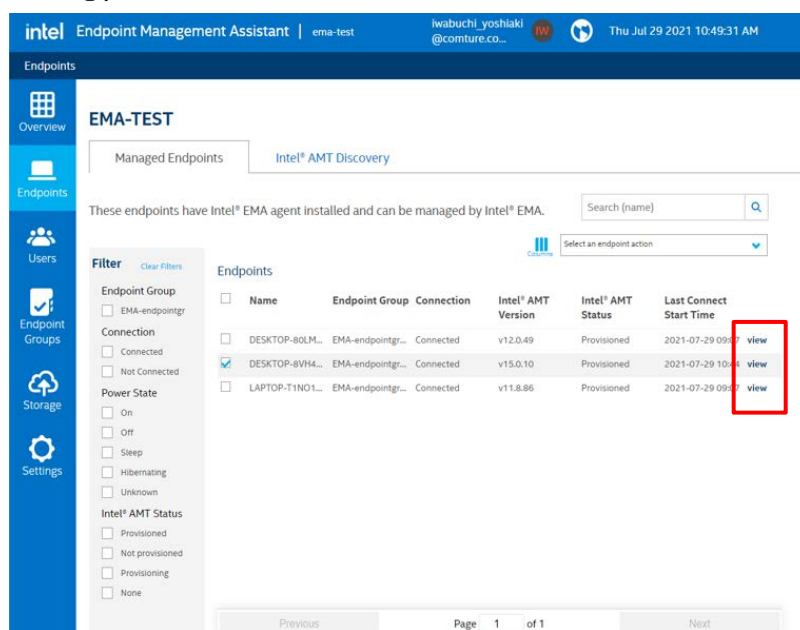


図 4-1-3-④ Endpoint 選択画面

- ⑤ General タブの画面が表示されるので、エンドポイント（クライアント PC）の状態が「CIRA Connected」であることを確認した後、「Hardware Manageability」タブを選択します。（図 4-1-3-⑤）

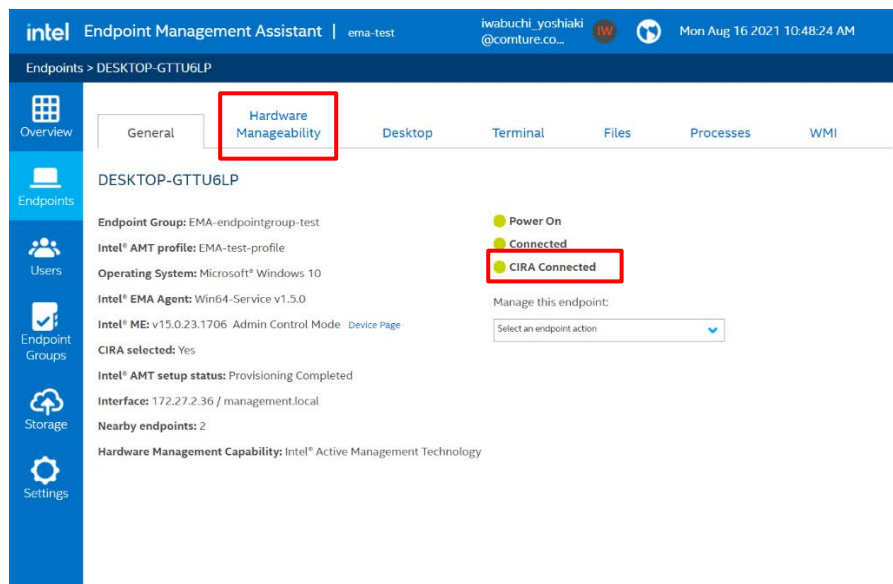


図 4-1-3-⑤ Endpoint 状態確認画面

- ⑥ Hardware Manageability 画面が表示されますので、左側のメニューの「Alarm Clocks」をクリックします。(図 4-1-3-⑥)

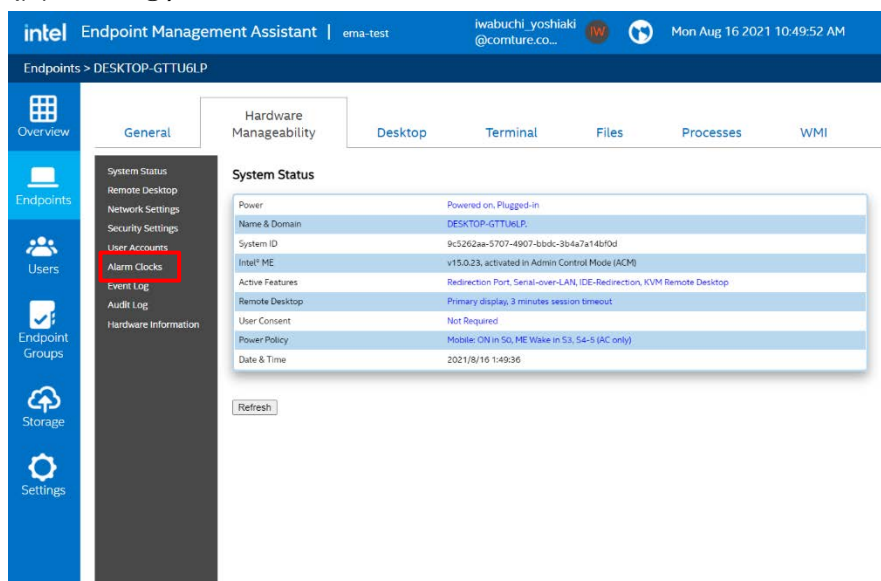


図 4-1-3-⑥ Hardware Manageability 詳細画面

- ⑦ 「Add Alarm」ボタンをクリックします。(図 4-1-3-⑦)

※「No Alarm Clocks are present」と表示されている場合はハードウェアアラームクロック機能が未設定であることを意味しています。

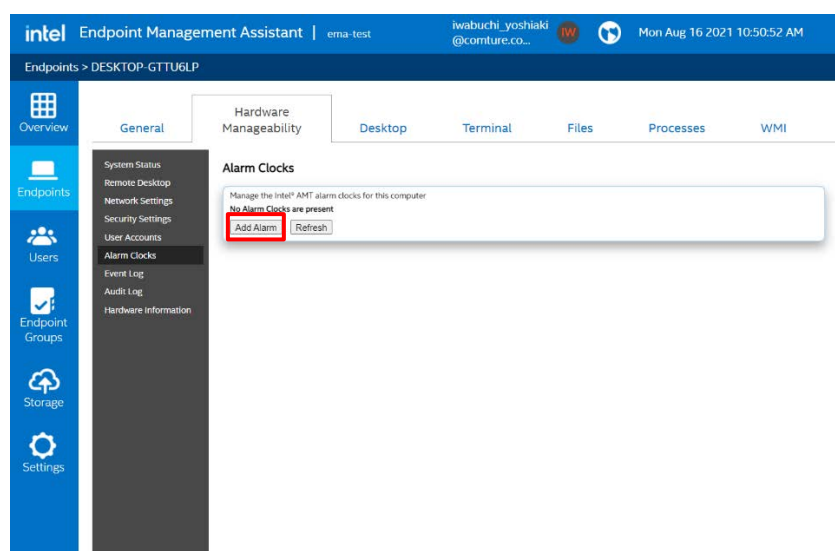
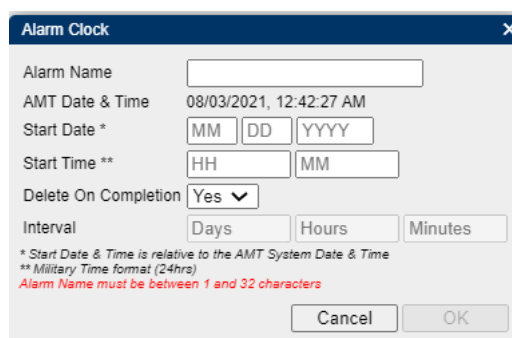


図 4-1-3-⑦ Alarm Clocks 詳細画面

- ⑧ 以下ウィンドウが表示されますので、各項目を設定しハードウェアアラームクロック機能を設定します。(図 4-1-3-⑧)



The image shows a software window titled "Alarm Clock" with a close button (X) in the top right corner. The window contains the following fields and controls:

- Alarm Name:** A text input field.
- AMT Date & Time:** A text field displaying "08/03/2021, 12:42:27 AM".
- Start Date *:** Three input fields labeled "MM", "DD", and "YYYY".
- Start Time **:** Two input fields labeled "HH" and "MM".
- Delete On Completion:** A dropdown menu currently set to "Yes".
- Interval:** Three input fields labeled "Days", "Hours", and "Minutes".

Below the input fields, there is a small text note: "* Start Date & Time is relative to the AMT System Date & Time". Below that is another note: "** Military Time format (24hrs)". At the bottom of the window, there is a red text warning: "Alarm Name must be between 1 and 32 characters". At the very bottom, there are two buttons: "Cancel" and "OK".

図 4-1-3-⑧ 自動起動設定画面

※各項目の説明については以下に記載します。（表 4-1-3-①）

表 4-1-3-① Add Alarm 各項目の詳細

項目	説明
Alert Name	アラート名（任意）
AMT Data & Time	現在の AMT の日付・時刻（仕様により設定変更は不可）
Start Date ※ 1	起動する日付の設定
Start Time ※ 1	起動する時間の設定（24 時間形式で入力） 例）PM6:00 の場合、18:00 と入力する
Delete On Completion	完了時に本設定を削除する場合は「Yes」、削除しない場合は「No」を選択
Interval	繰り返し設定 各項目に設定する値ごとに起動する設定が可能 設定しない場合は「0」を入力 例 1）起動時間は 9 時で 1 日ごとに起動設定する場合 Start Time 09:00 に設定後 Days : 1 Hours : 0 Minutes : 0 で設定 例 2）起動時間は 9 時で 1 時間ごとに起動設定する場合 Start Time 09:00 に設定後 Days : 0 Hours : 1 Minutes : 0 で設定

※ 1 AMT Data & Time の日時を基準で設定します。

（例：5 時間後に設定する場合は AMT Data & Time の時刻の + 5 時間で設定します）

⑨ 手順⑧で設定した Alert Name が表示されていることを確認します。(図 4-1-3-⑨)

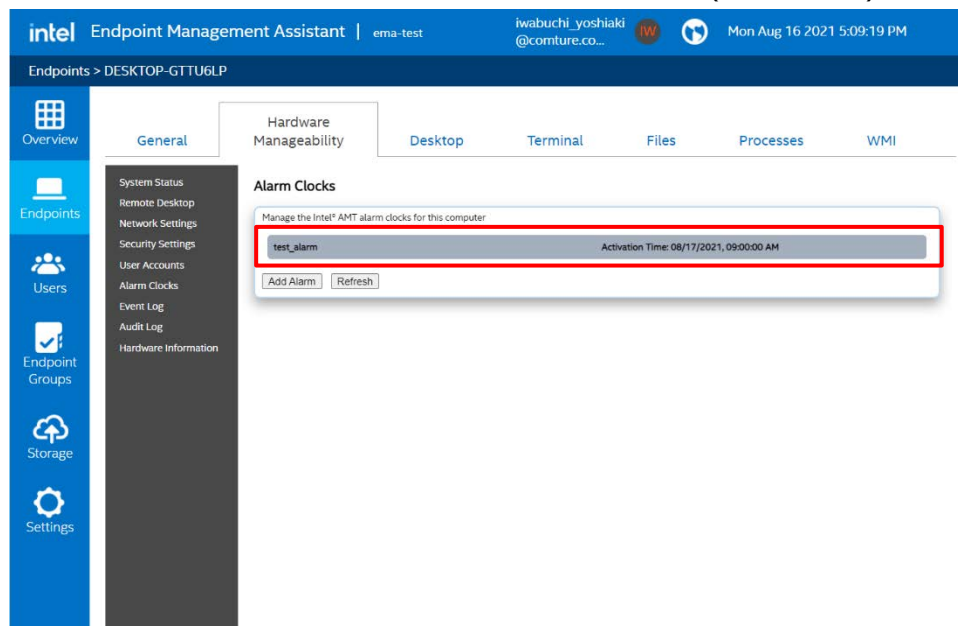


図 4-1-3-⑨ 設定完了画面

4.1.4 ハードウェア KVM 機能

本章でインテル®EMA の、ハードウェア KVM（キーボード/ビデオ/マウス（KVM）機能により、手元のキーボード、ビデオ、マウスがエンドポイント（クライアント PC）に物理的に接続されているかのようにリモートから操作が可能になります。ハードウェア KVM 機能を利用してリモート操作ができる方法は以下の 3 点ありますので、それぞれ説明していきます。

- 「Desktop」タブからの操作
- 「Hardware Manageability」タブからの操作
- BIOS 画面の操作

4.1.4.1 「Desktop」タブからの操作

- ① ブラウザにてインテル®EMA サーバの DNS 名を入力し、インテル®EMA へ接続（URL: [https://\[インテル®EMA サーバの DNS 名\]](https://[インテル®EMA サーバの DNS 名])）し、インテル®EMA サーバ作成時に設定した user name と Password を入力、Log In ボタンをクリックしログインします。（図 4-1-4-1-①）

※「テナント管理者」または「エンドポイント管理者」権限が設定されているユーザでログインします。

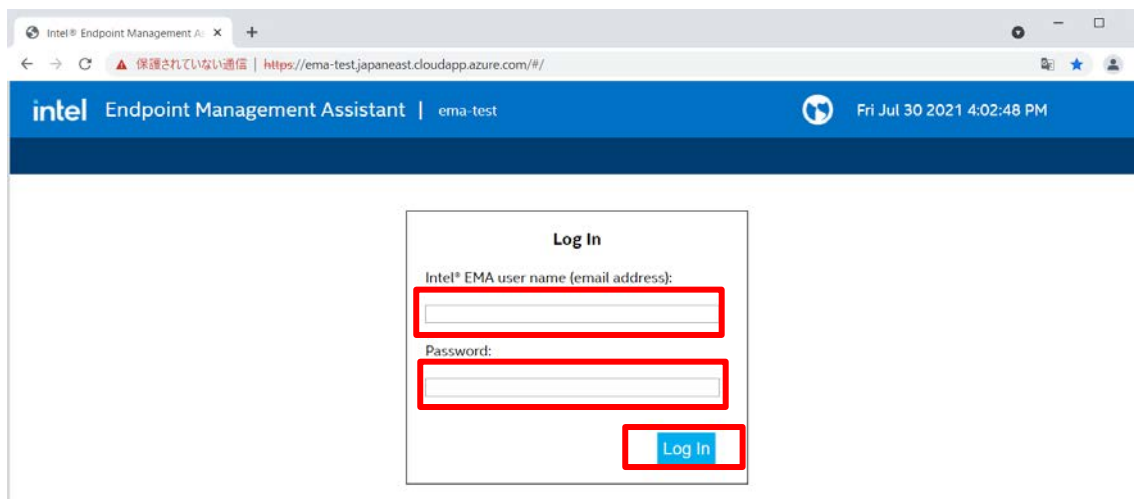


図 4-1-4-1-① ログイン画面

- ② Overview 画面が表示されるので、左側のメニューから「Endpoints」を選択します。（図 4-1-4-1-②）

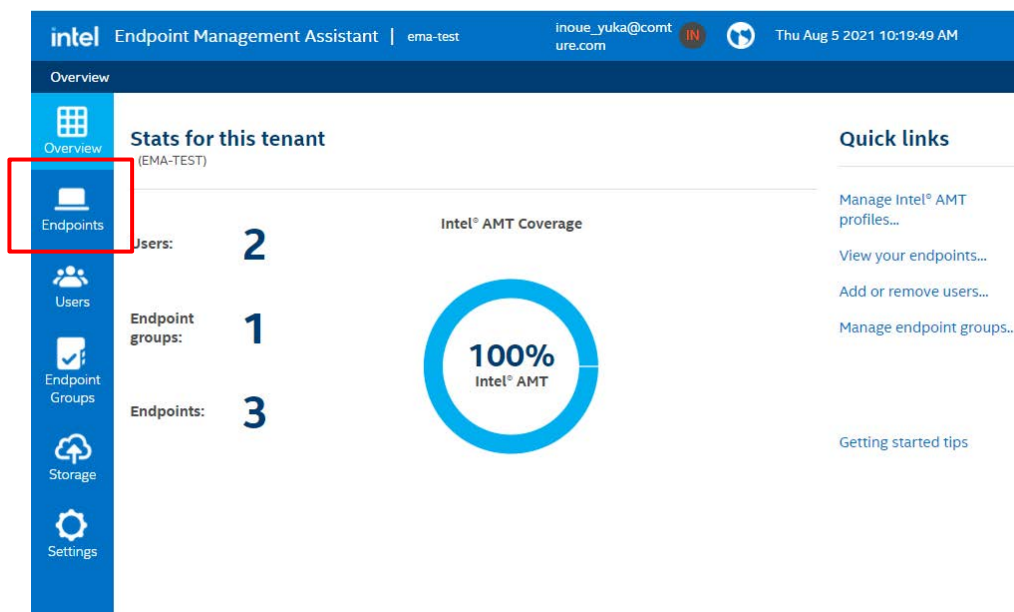


図 4-1-4-1-② ログイン後のトップ画面

- ③ 「Load all Endpoints」をクリックします。（図 4-1-4-1-③）

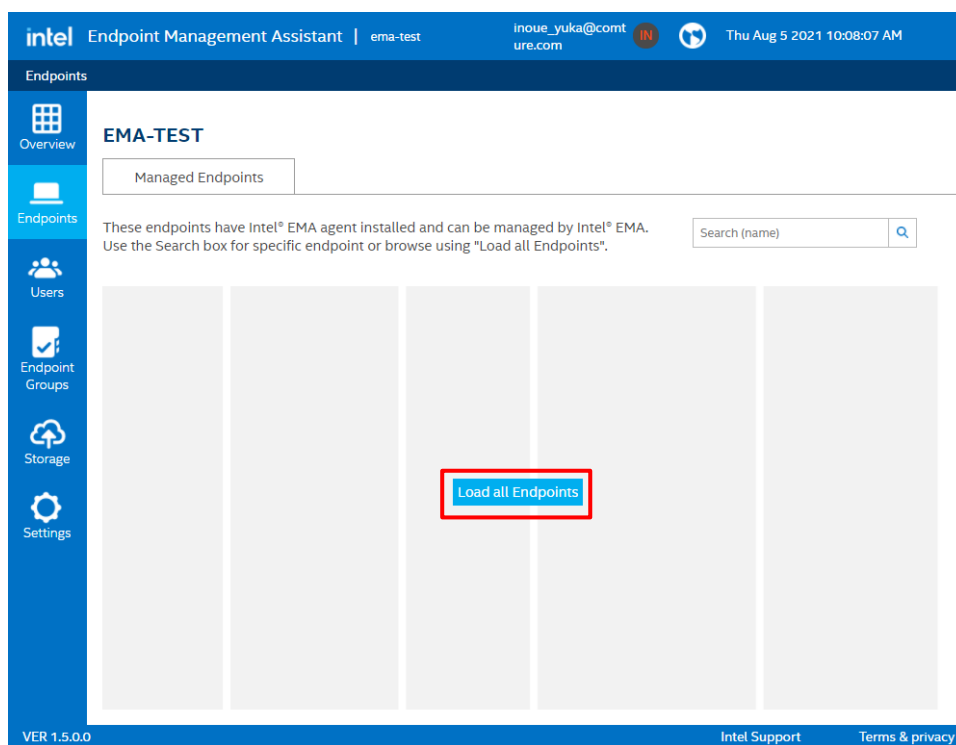


図 4-1-4-1-③ Endpoint 選択画面

- ④ リモートから操作したいエンドポイント（クライアント PC）の右側にある「view」をクリックします（図 4-1-4-1-④）

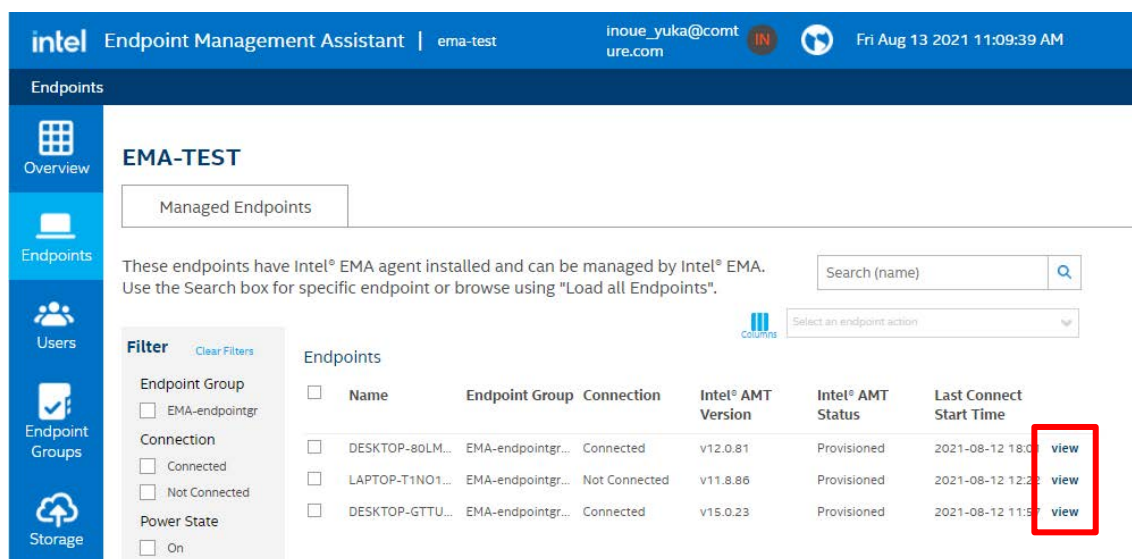


図 4-1-4-1-④ Endpoints 一覧画面

- ⑤ 「Desktop」タブをクリックし、画面左上にある「Connect」ボタンをクリックします。（図 4-1-4-1-⑤）

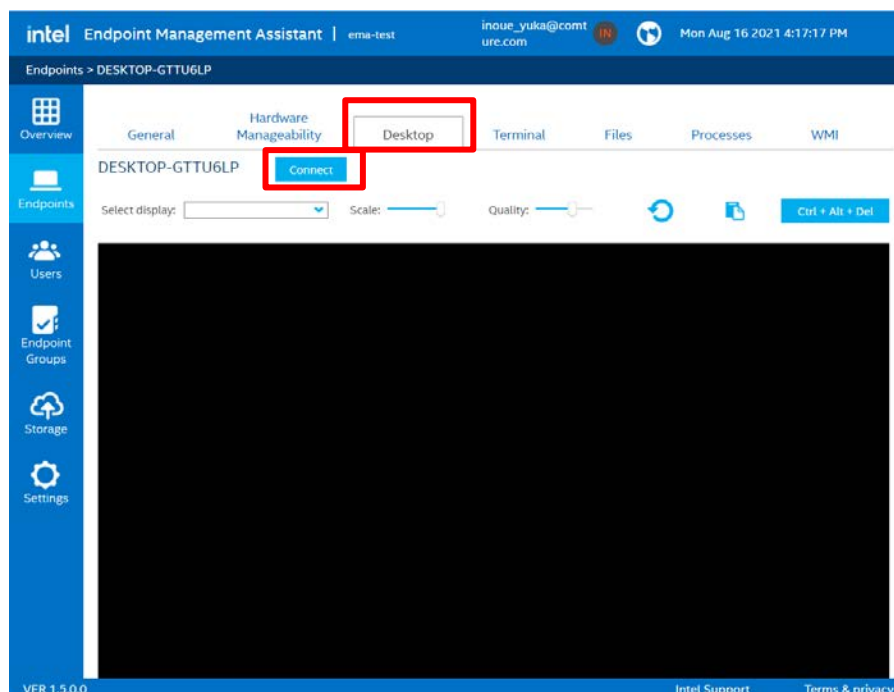


図 4-1-4-1-⑤ Desktop 画面

- ⑥ 対象のエンドポイント（クライアント PC）へ接続され、リモート操作することが可能になります。（図 4-1-4-1-⑥）

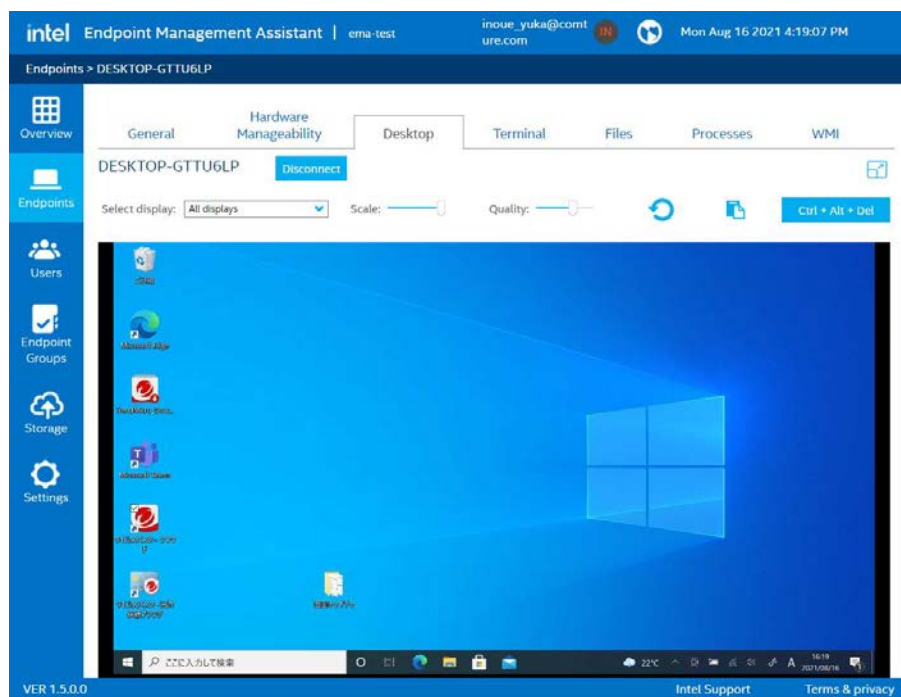


図 4-1-4-1-⑥ Desktop 画面

※Desktop 画面の上部にある各項目の機能の説明をします。（表 4-1-4-1-①）

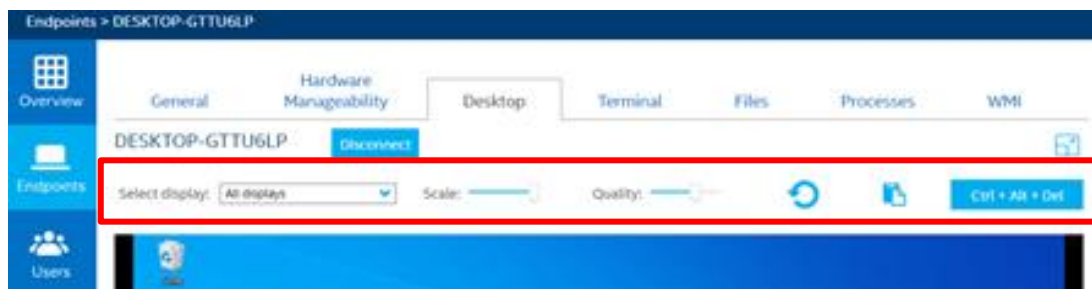


表 4-1-4-1-① Desktop 機能

項目	機能
Select display	エンドポイントにディスプレイが複数ある場合、表示するターゲット・ディスプレイを選択できる
Scale	レンダリング解像度のパーセント値 値が小さいほど、解像度は低くなる 50%（半分）または 100%（フルスケール）を使用すると最良の結果が得られる
Quality	ビットマップ圧縮のレベル 値が小さいほど、圧縮率は高くなるが、解像度が低下する
	表示するディスプレイの回転する
	エンドポイント上へのテキストの貼り付ける
	Ctrl + Alt + Del キーをリモートのシステムに送信する
	リモート KVM を全画面モードに拡大する。このモードを解除するには、ウェブブラウザの制御（Esc キーなど）を使用する

注意事項

- 前の同意リクエストが有効な場合、ユーザの同意は再度リクエストされません。
- マウスとキーボードの入力について、すべてのセッションが競合します。
- スケール、ビットマップ品質、ディスプレイの選択はすべてのセッションに影響します。
- 回転は現在のブラウザのみに影響します。

4.1.4.2 「Hardware Manageability」タブからの操作

- ① ブラウザにてインテル®EMA サーバの DNS 名を入力し、インテル®EMA へ接続（URL:https://[インテル®EMA サーバの DNS 名]）し、インテル®EMA サーバ作成時に設定した user name と Password を入力、Log In ボタンをクリックしログインします。（図 4-1-4-2-①）

※「テナント管理者」または「エンドポイント管理者」権限が設定されているユーザでログインします。

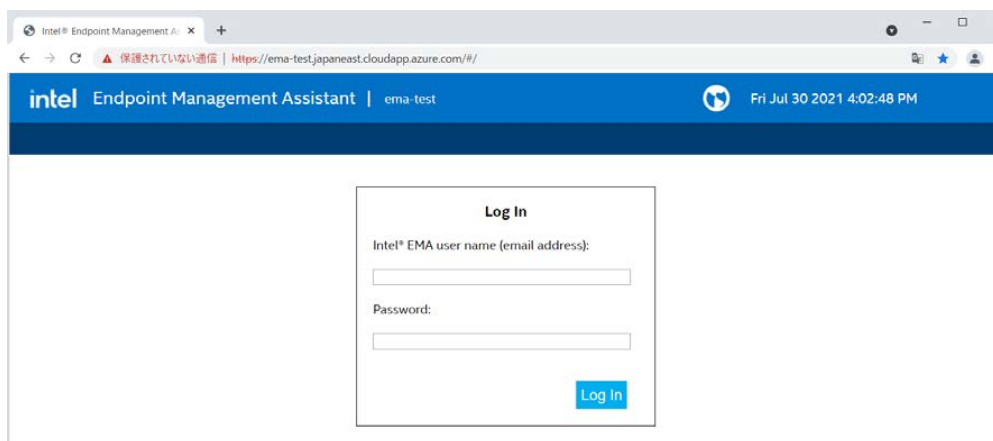


図 4-1-4-2-① ログイン画面

- ② OverView 画面が表示されるので、左側のメニューから「Endpoints」を選択します。（図 4-1-4-2-②）

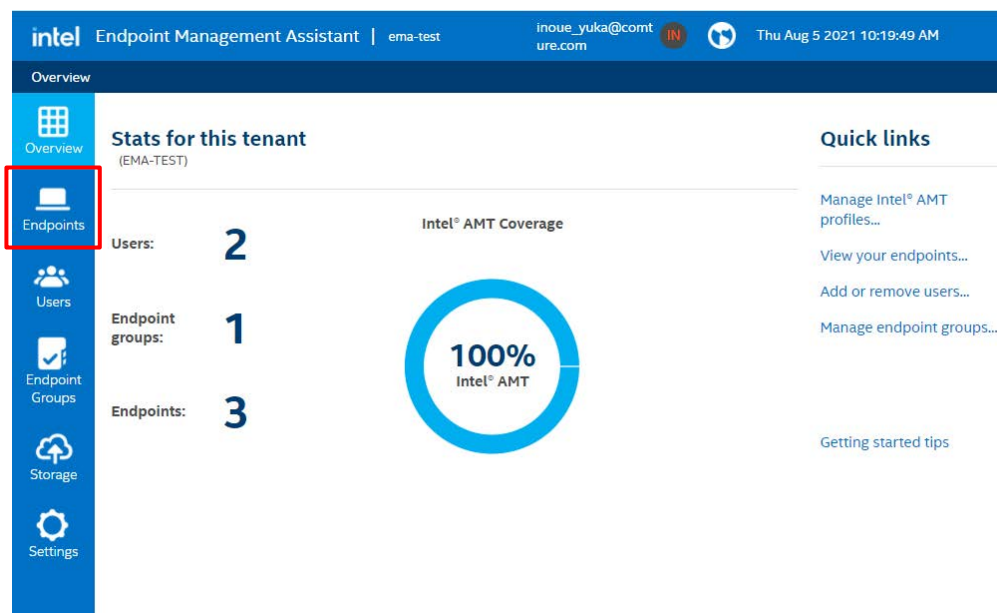


図 4-1-4-2-② ログイン後のトップ画面

- ③ 「Load all Endpoints」をクリックします。(図 4-1-4-2-③)

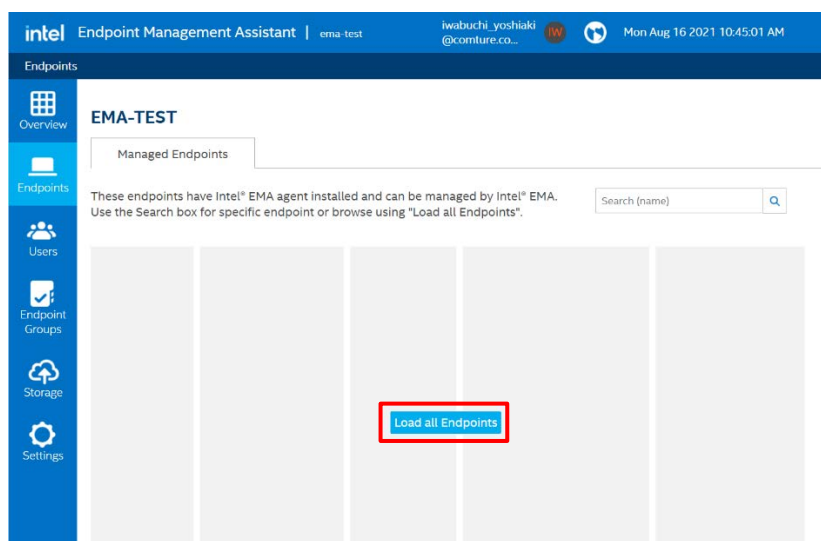


図 4-1-4-2-③ Endpoint 画面

- ④ リモートから操作したいエンドポイント（クライアント PC）の右側にある「view」をクリックします（図 4-1-4-2-④）

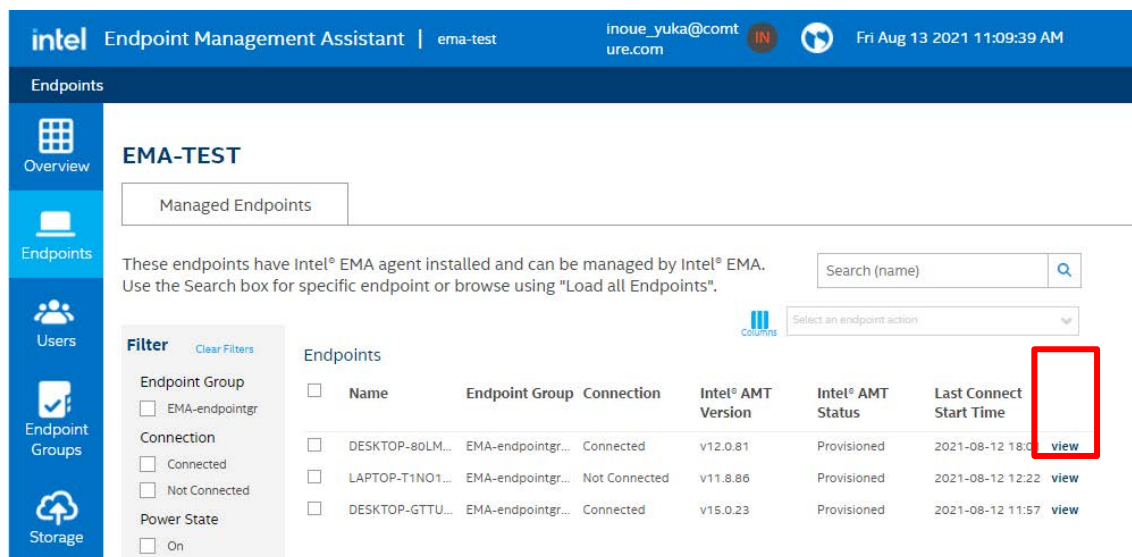


図 4-1-4-2-④ Endpoints 画面

⑤ 「Hardware Manageability」タブをクリックします（図 4-1-4-2-⑤）

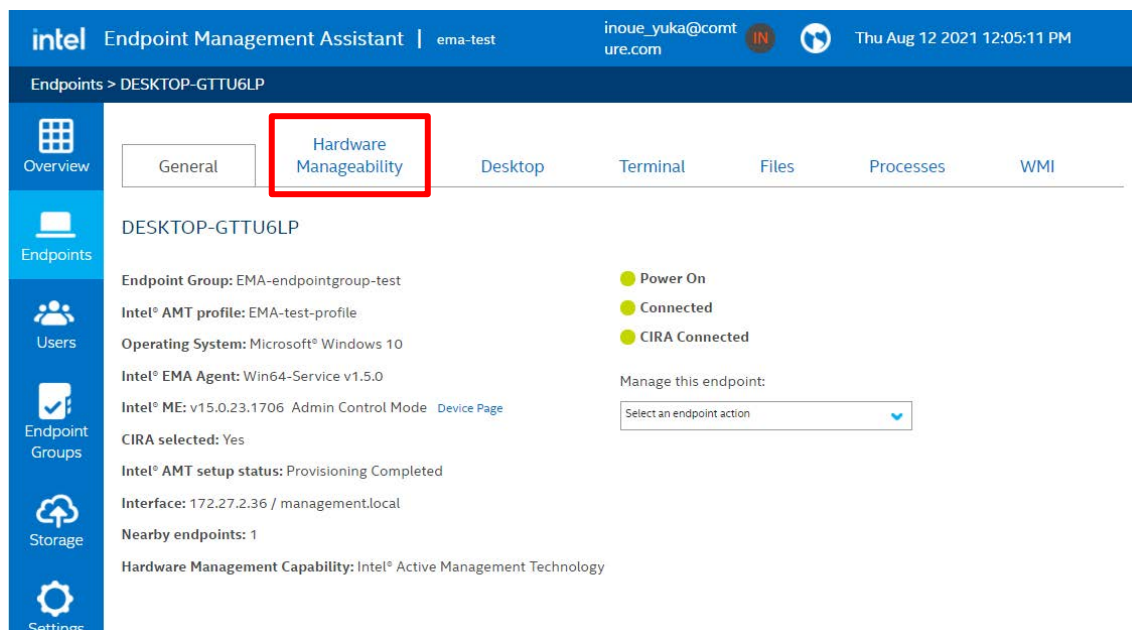


図 4-1-4-2-⑤ General タブ画面

⑥ 左側にある「Remote Desktop」を選択します（図 4-1-4-2-⑥）

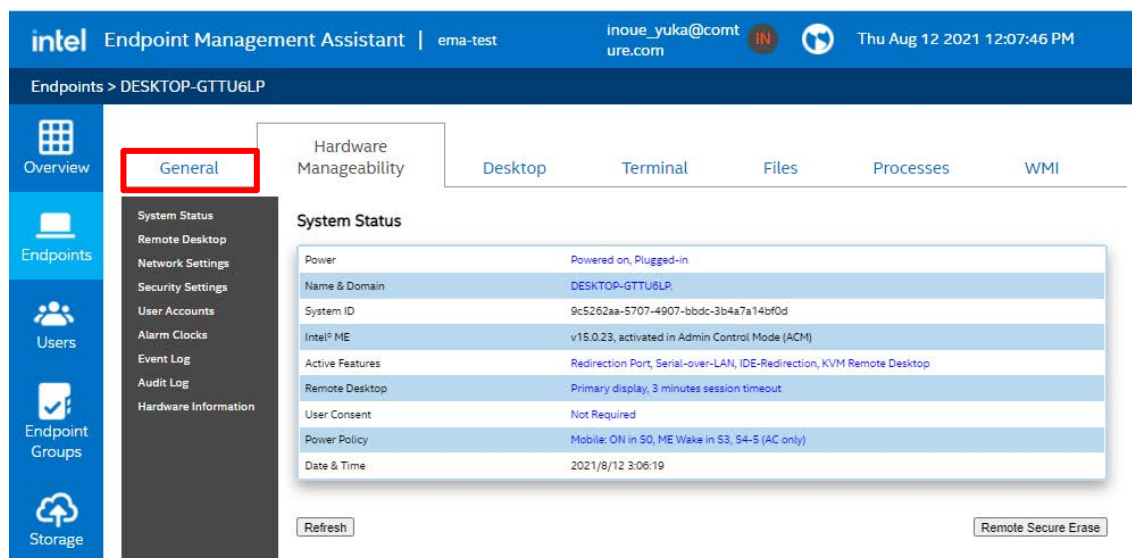


図 4-1-4-2-⑥ Hardware Manageability タブ画面

- ⑦ 左上にある「connect」ボタンをクリックします。(図 4-1-4-2-⑦)

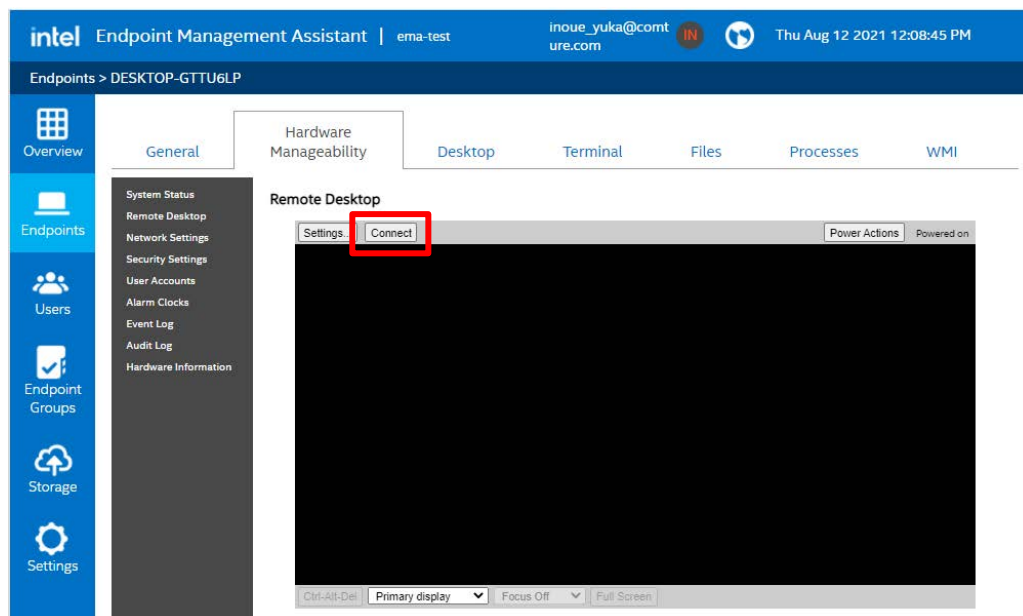


図 4-1-4-2-⑦ Remote Desktop 画面

- ⑧ 対象のエンドポイント（クライアント PC）へ接続され、リモート操作することが可能になります。(図 4-1-4-2-⑧)

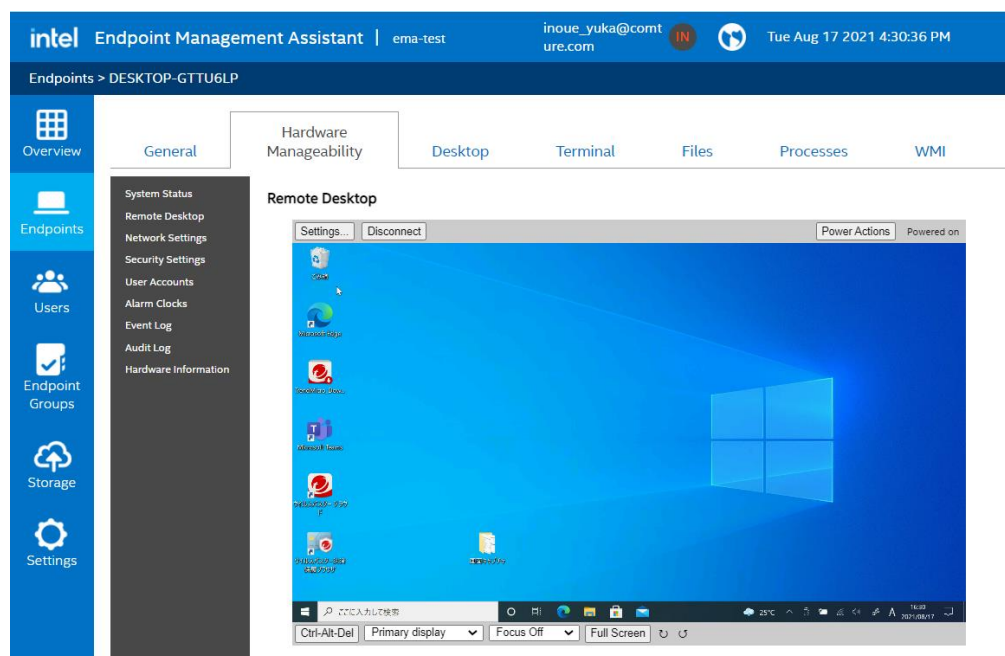


図 4-1-4-2-⑧ connect 後 Remote Desktop 画面

4.1.4.3 BIOS 画面操作

エンドポイント（クライアント PC）がブルースクリーンなどのトラブルが発生した場合や OS が起動してなくても、リモートから操作することが可能になります。

- ① ブラウザにてインテル®EMA サーバの DNS 名を入力し、インテル®EMA へ接続（URL:https://[インテル®EMA サーバの DNS 名]）し、インテル®EMA サーバ作成時に設定した user name と Password を入力、Log In ボタンをクリックしログインします。（図 4-1-4-3-①）

※「テナント管理者」または「エンドポイント管理者」権限が設定されているユーザでログインします。

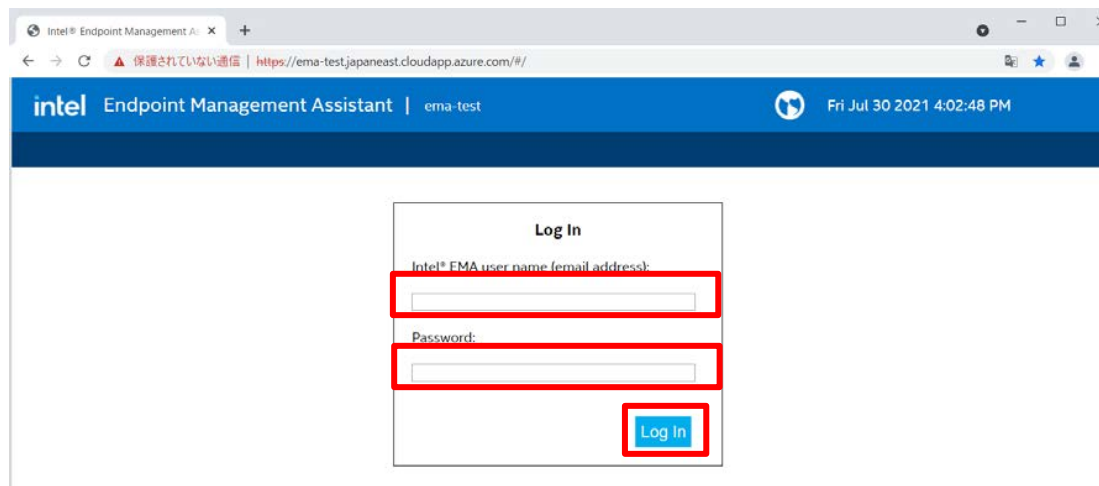


図 4-1-4-3-① ログイン画面

- ② Overview 画面が表示されるので、左側のメニューから「Endpoints」を選択します。（図 4-1-4-3-②）

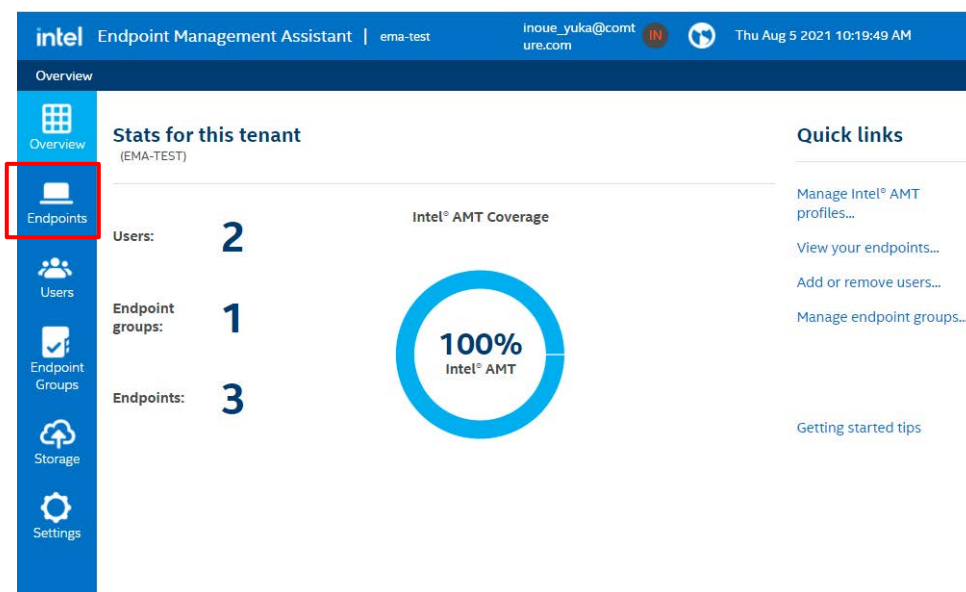


図 4-1-4-3-② ログイン後のトップ画面

- ③ 「Load all Endpoints」をクリックします。（図 4-1-4-3-③）

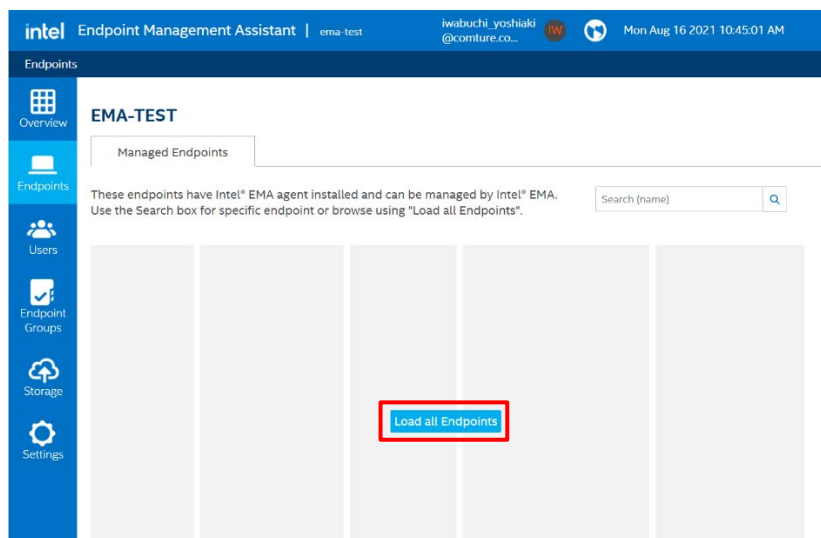


図 4-1-4-3-③ Endpoint 画面

- ④ リモートから操作したいエンドポイント（クライアント PC）の右側にある「view」をクリックします。（図 4-1-4-3-④）

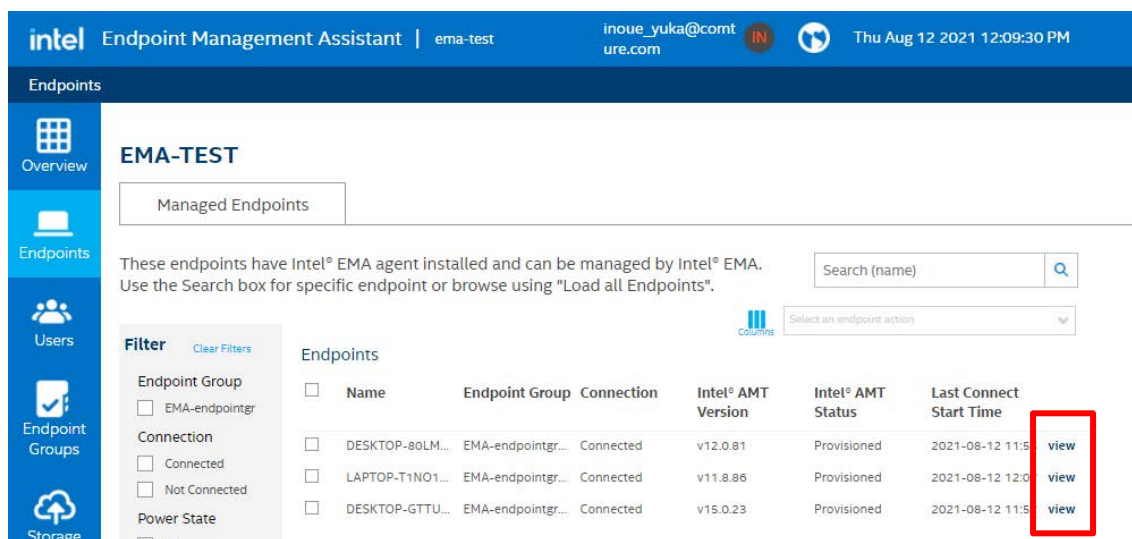


図 4-1-4-3-④ Endpoints 画面

- ⑤ 「Hardware Manageability」タブをクリックします。（図 4-1-4-3-⑤）

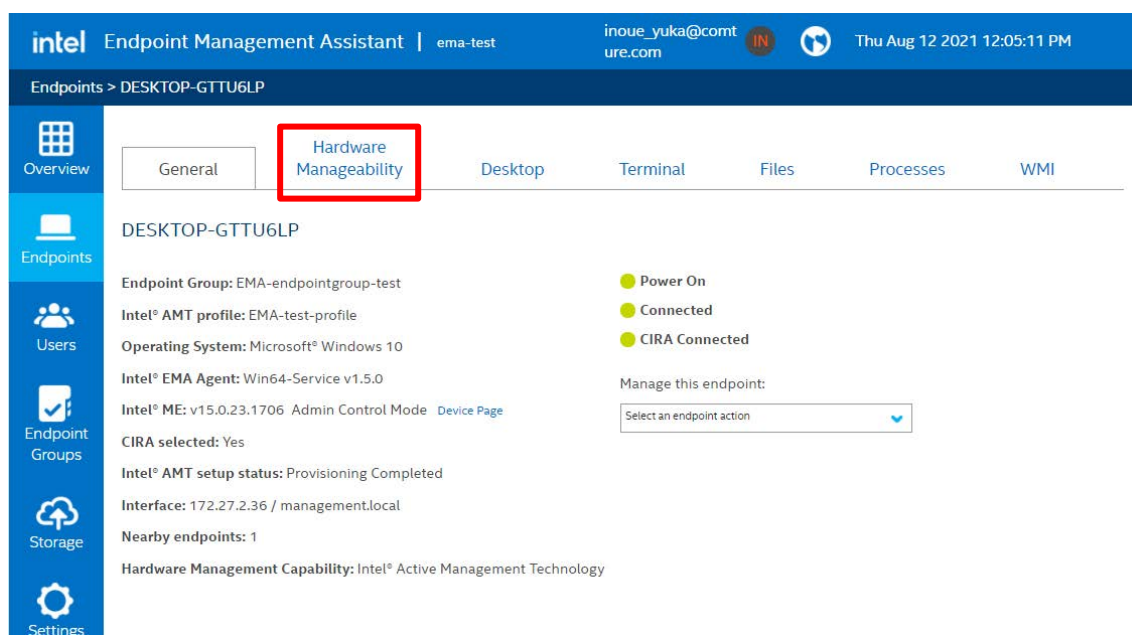


図 4-1-4-3-⑤ General タブ画面

- ⑥ 左側にある「Remote Desktop」を選択します。(図 4-1-4-3-⑥)

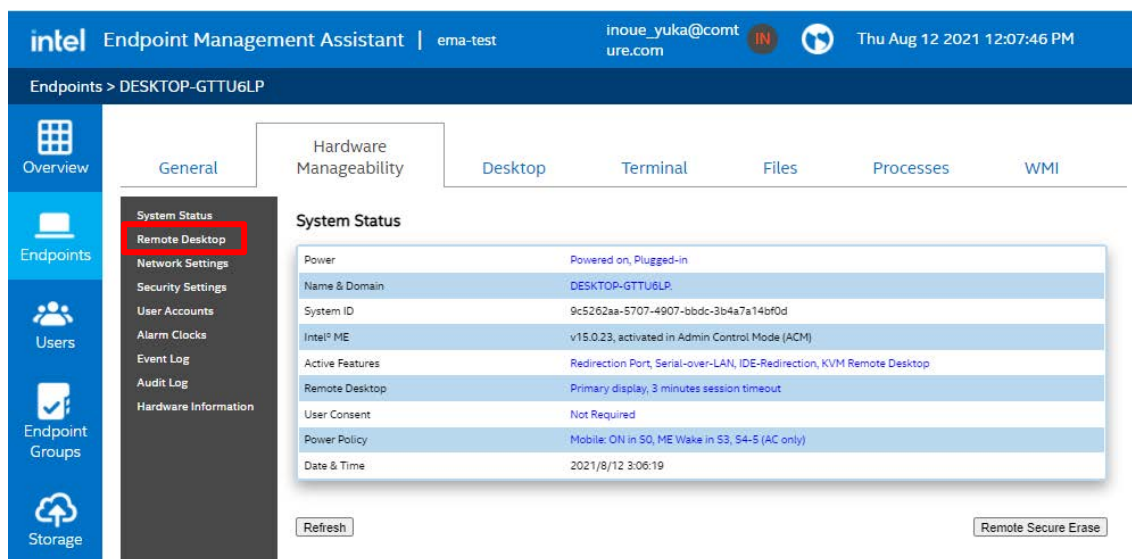


図 4-1-4-3-⑥ Hardware Manageability タブ画面

- ⑦ 左上にある「connect」ボタンをクリックすると、エンドポイント（クライアント PC）へ接続されます。(図 4-1-4-3-⑦)

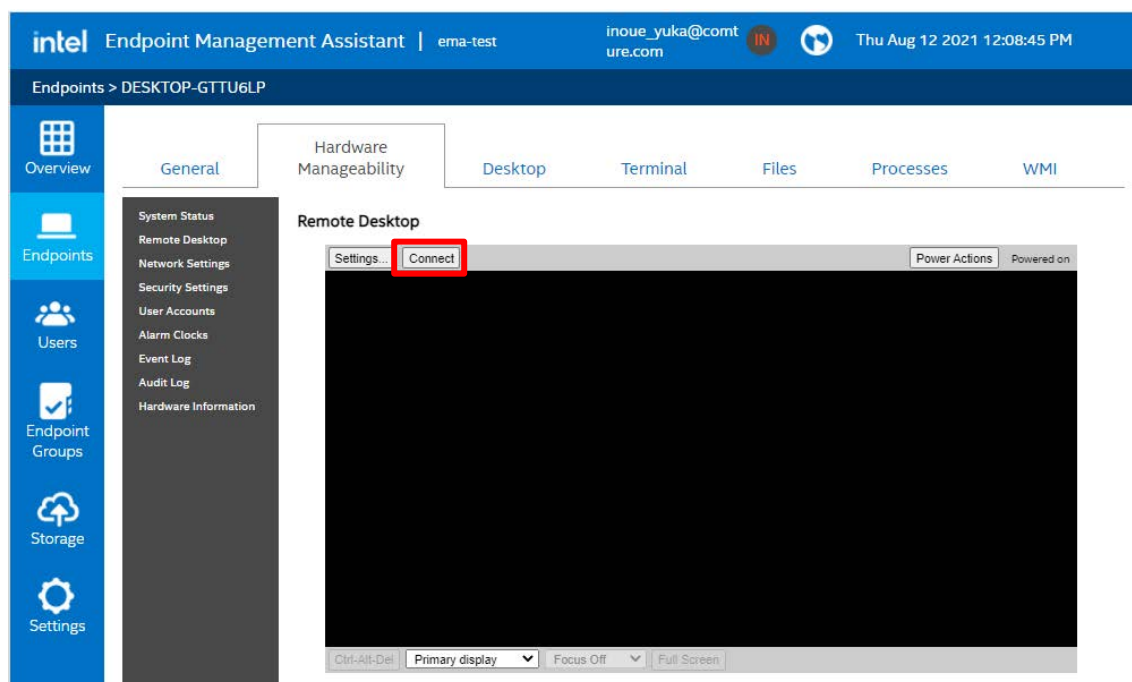


図 4-1-4-3-⑦ Remote Desktop 画面

- ⑧ 以下のようにブルースクリーン画面であっても、画面を表示することができます。(図 4-1-4-3-⑧)

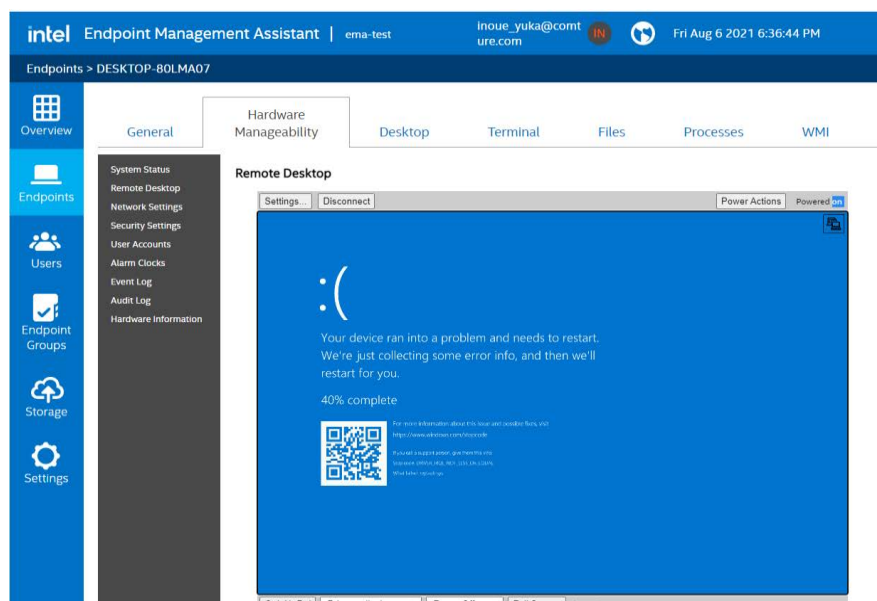


図 4-1-4-3-⑧ エンドポイントデスクトップ画面

- ⑨ 画面右上の「Power Actions」ボタンをクリックし、Power Dialog 画面を表示されますので、「Reset to BIOS」を選択後、「OK」ボタンをクリックし BIOS 画面を起動させます。(図 4-1-4-3-⑨)

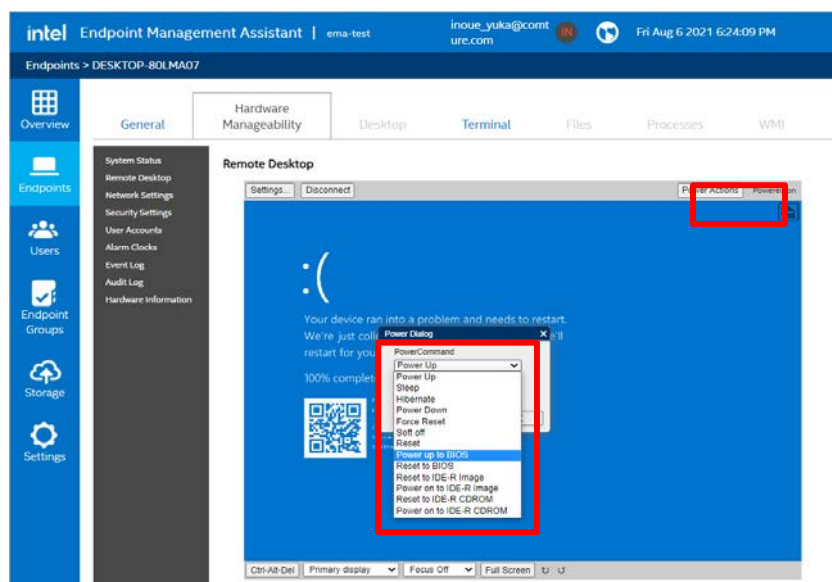


図 4-1-4-3-⑨ Power Dialog 表示画面

※BIOS からのシステム診断につきましては、【4.1.4 HP PC Hardware Diagnostics UEFI 機能】の項目をご参照ください。

- ⑩ 対象のエンドポイント（クライアント PC）の BIOS 画面が表示され、BIOS 画面のリモート操作をすることが可能になります。（図 4-1-4-3-⑩）

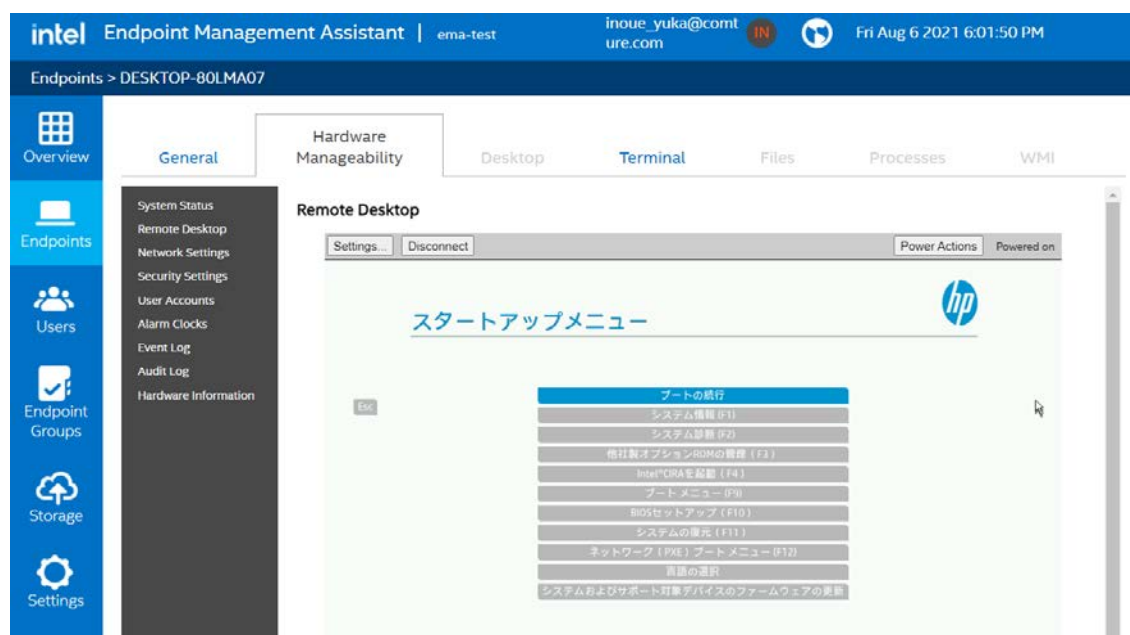


図 4-1-4-3-⑩ BIOS 画面（スタートアップメニュー）

4.1.5 HP PC Hardware Diagnostics UEFI 機能

本章ではエンドポイント（クライアント PC）のハードウェア診断を実施することができる HP PC Diagnostics UEFI 機能をリモートから実行する操作手順について記載します。

- ① ブラウザにてインテル®EMA サーバの DNS 名を入力し、インテル®EMA へ接続（URL:https://[インテル®EMA サーバの DNS 名]）し、インテル®EMA サーバ作成時に設定した user name と Password を入力、Log In ボタンをクリックしログインします。（図 4-1-5-①）

※「テナント管理者」または「エンドポイント管理者」権限が設定されているユーザでログインします。

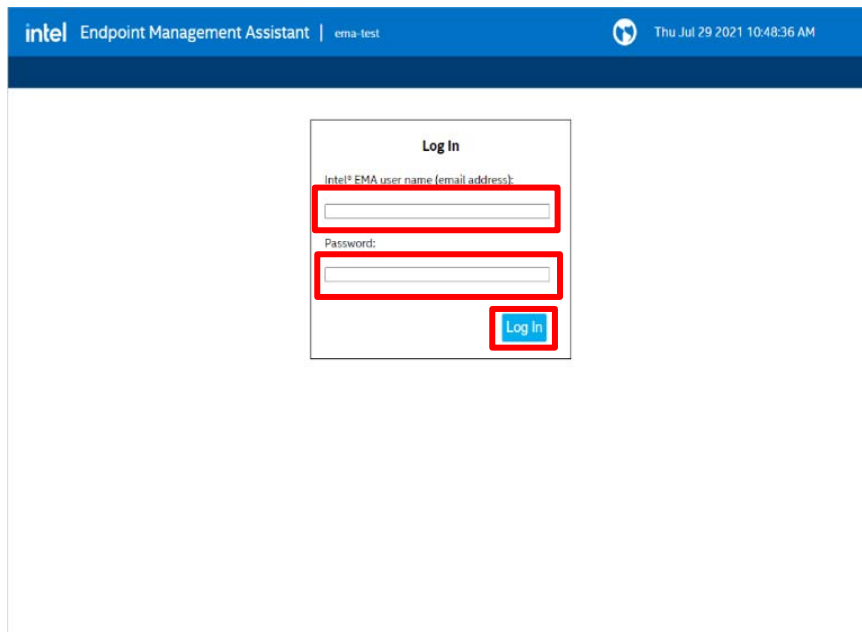


図 4-1-5-① ログイン画面

- ② Overview 画面が表示されるので、左側のメニューから「Endpoints」を選択します。(図 4-1-5-②)

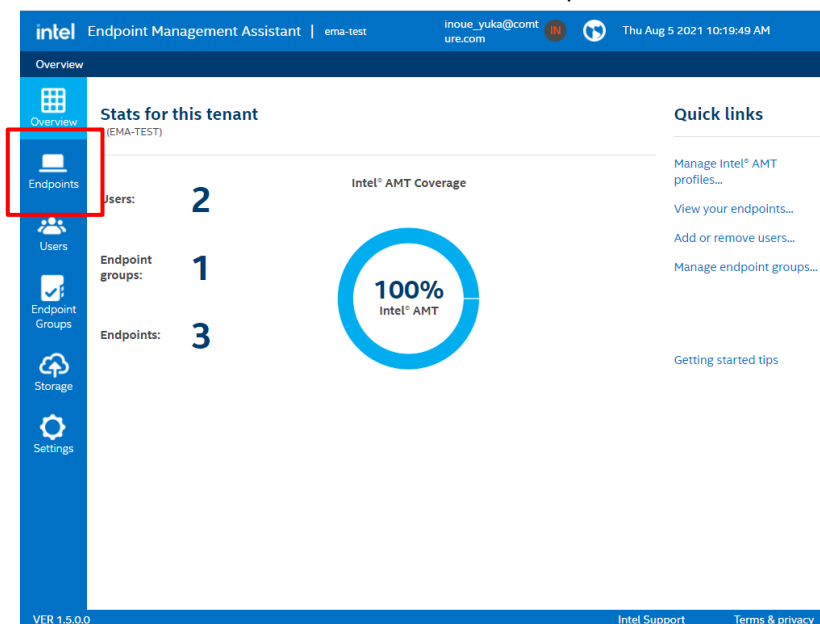


図 4-1-5-② ログイン後のトップ画面

- ③ 「Load all Endpoints」をクリックします。(図 4-1-5-③)

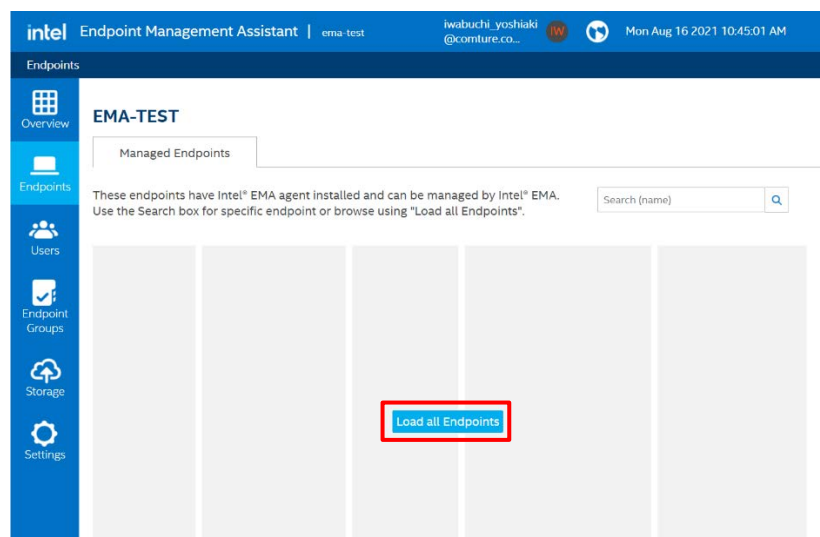


図 4-1-5-③ Endpoint 選択画面

- ④ リモートから操作したいエンドポイント（クライアント PC）の右側にある「View」をクリックします。（図 4-1-5-④）

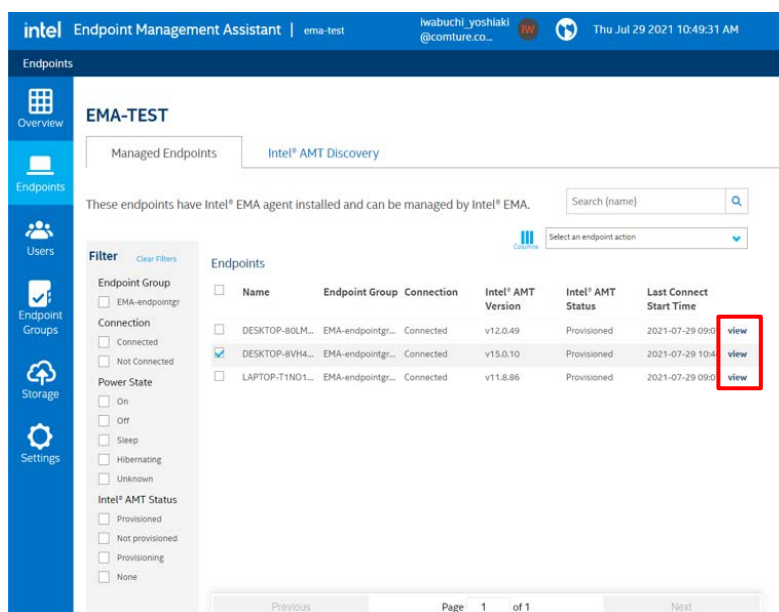


図 4-1-5-④ Endpoint 選択画面

- ⑤ General タブ画面が表示されるので、画面右側にある「CIRA Connected」であることを確認した後に「Hardware Manageability」タブを選択します。（図 4-1-5-⑤）

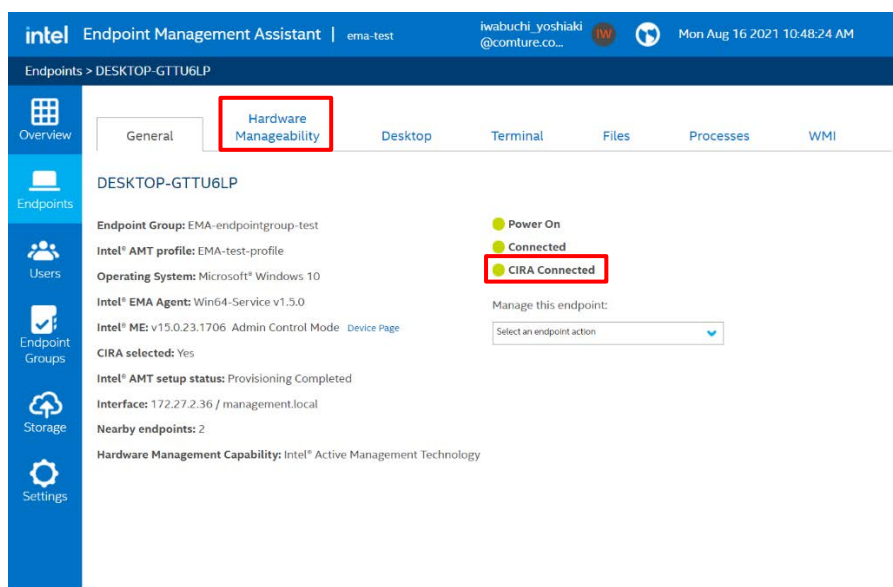


図 4-1-5-⑤ Endpoint 状態確認画面

⑥ 「Remote Desktop」をクリックします。(図 4-1-5-⑥)

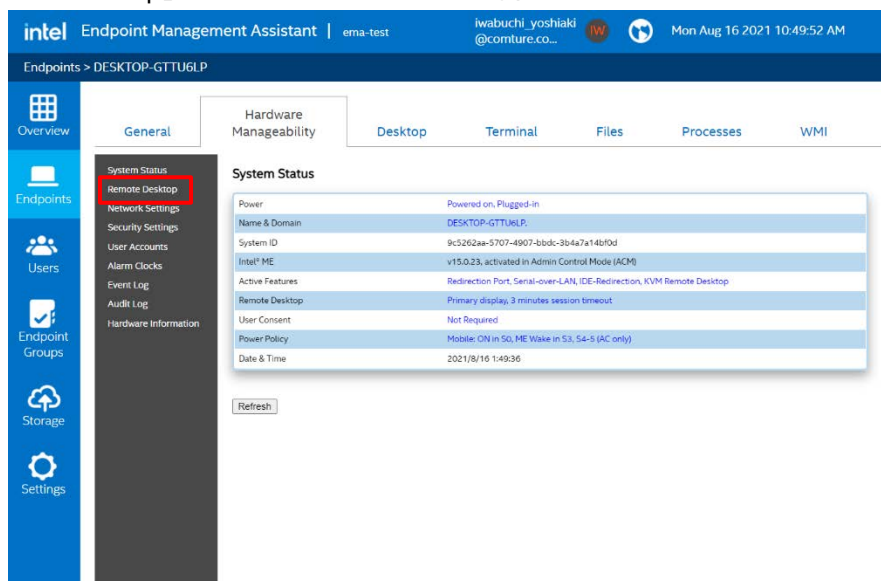


図 4-1-5-⑥ Hardware Manageability 詳細画面

⑦ 「Connect」ボタンをクリックします。(図 4-1-5-⑦)

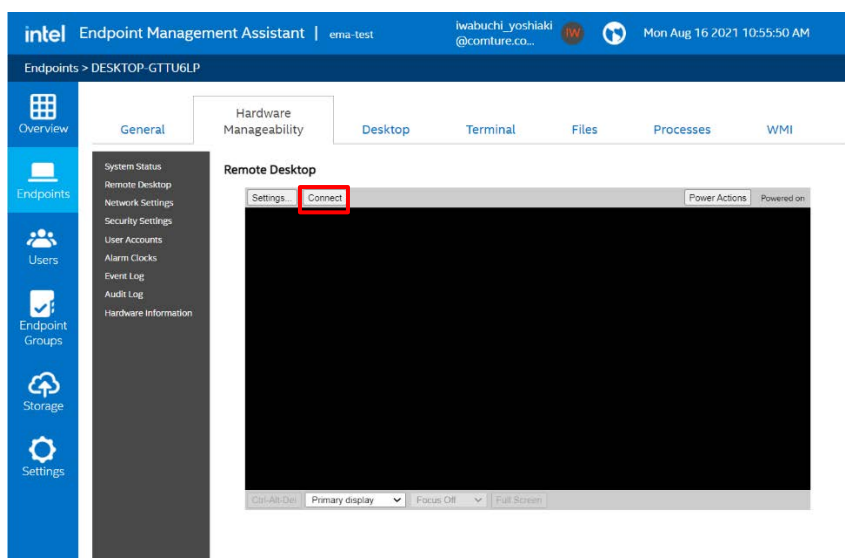


図 4-1-5-⑦ Remote Desktop 画面

⑧ 電源の状態に合わせてエンドポイント（クライアント PC）の BIOS 画面を起動させます。（または再起動させます）

（ア） エンドポイント（クライアント PC）が電源 OFF の場合は、「Power Actions」→「Power Up to BIOS」を選択します。（図 4-1-5-⑧）

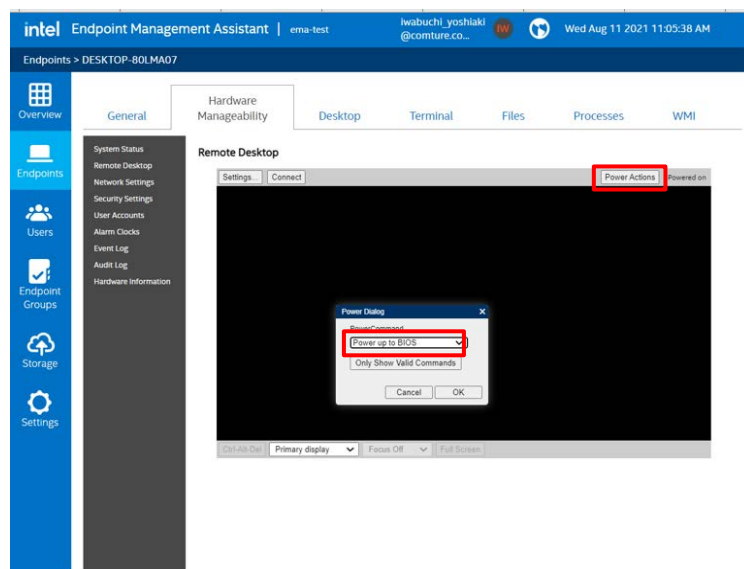


図 4-1-5-⑧ 電源状態が電源 OFF の場合の操作画面

（イ） エンドポイント（クライアント PC）が電源 ON の場合は「Power Actions」→「Reset to BIOS」を選択します。（図 4-1-5-⑨）

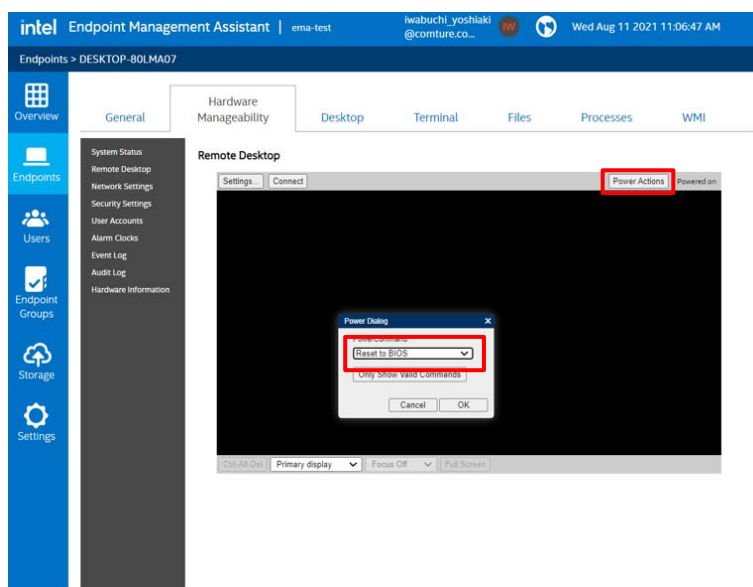


図 4-1-5-⑨ 電源状態が電源 ON の場合の操作画面

⑨ BIOS 画面（スタートアップメニュー画面）が表示されます。（図 4-1-5-⑩）

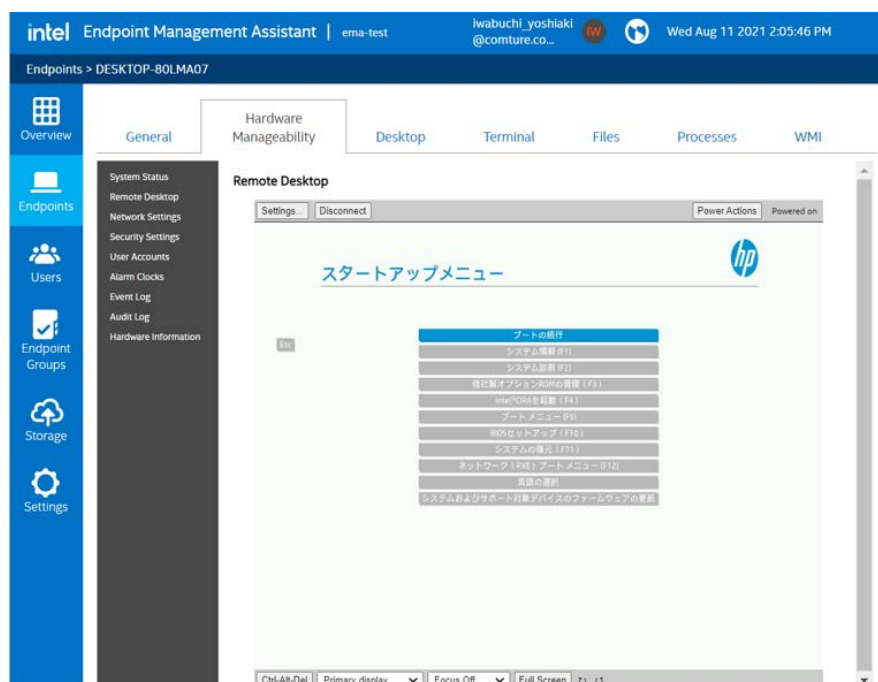


図 4-1-5-⑩ HP スタートアップメニュー画面

⑩ スタートアップメニュー画面から「システム診断（F2）」を選択します。（図 4-1-5-⑪）

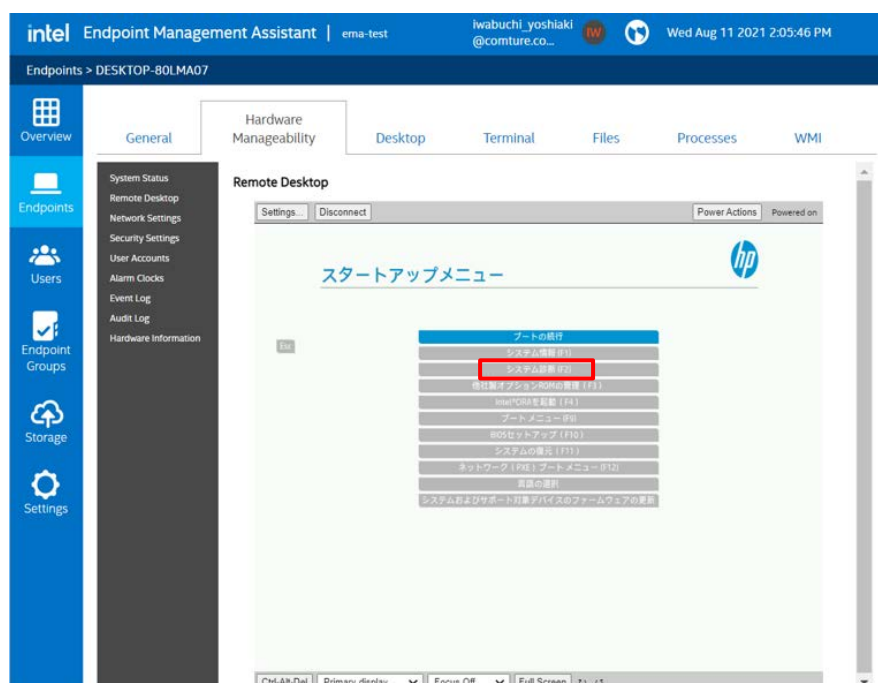


図 4-1-5-⑪ HP スタートアップメニュー選択画面

- ⑪ 初期起動時には言語を選択する画面になりますので、「日本語」を選択します。(図 4-1-5-⑫)

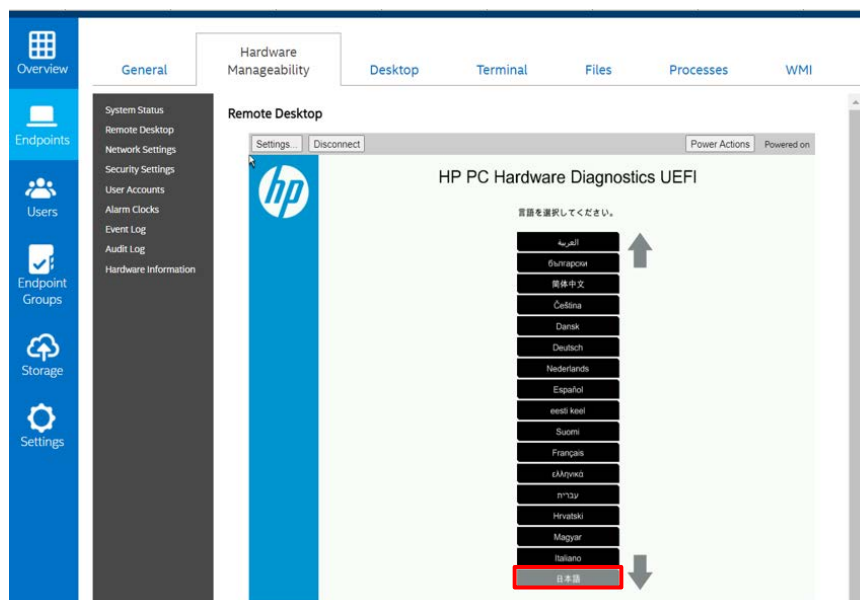


図 4-1-5-⑫ 言語選択画面

- ⑫ HP PC Hardware Diagnostics UEFI 画面が表示されますので、実施したいテストを選択します。
(図 4-1-5-⑬)

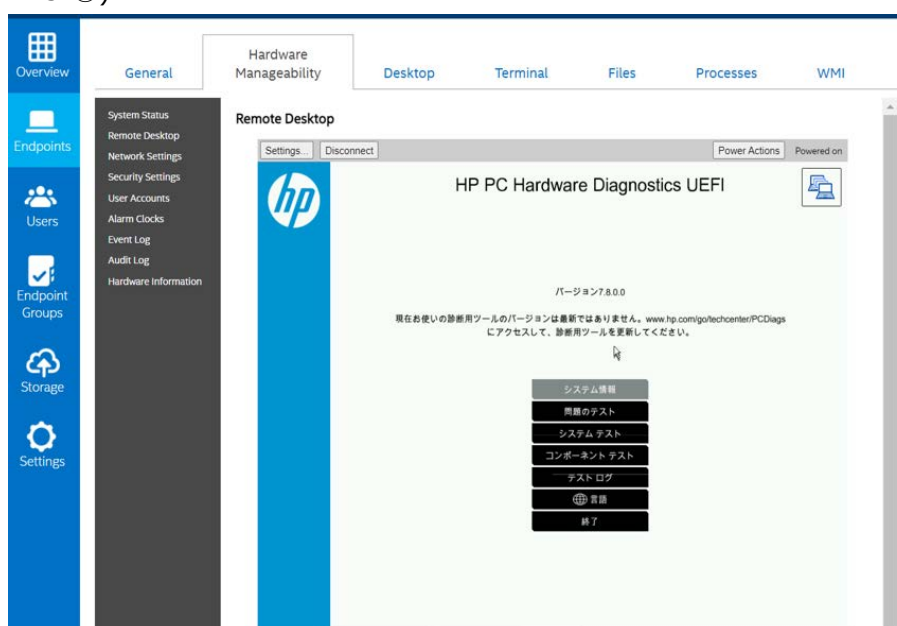


図 4-1-5-⑬ HP PC Hardware Diagnostics UEFI 画面

※HP PC Hardware Diagnostics UEFI 画面の各項目については、表 4-1-5-①に記載します。

表 4-1-5-① 各項目の詳細

項目	概要	機能説明
システム情報	端末情報	エンドポイント（クライアント P C）の詳細情報を表示 (4.1.5.5)
問題のテスト	ハードウェア診断	「起動時」や「ブルースクリーン」など、各項目別で問題点のチェックを実施（4.1.5.1）
システムテスト	ハードウェア診断	システム全般のテストを実施（4.1.5.2）
コンポーネントテスト	ハードウェア診断	各デバイスのチェックを実施（4.1.5.3）
テストログ	結果のアウトプット	各項目のテスト結果のアウトプットの実施（4.1.5.4）
言語	—	使用する言語を選択
終了	—	終了する場合に選択（4.1.5.6）

4.1.5.1 問題のテスト

※本手順では「問題のテスト」の中の「起動に関する問題」の手順について紹介しますが、他の項目についても同様の手順であるため、他の項目を実施する場合も本手順を参考にしてください。

① 「問題のテスト」を選択します。（図 4-1-5-1-①）

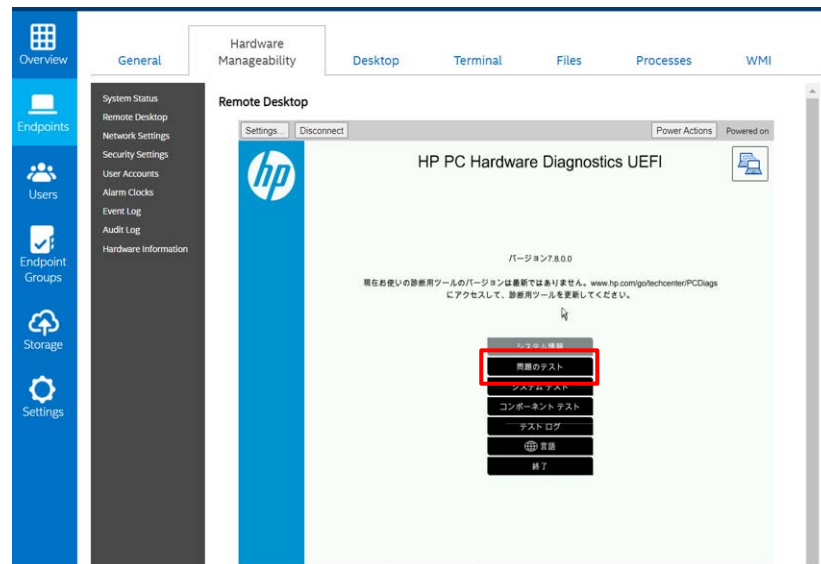


図 4-1-5-1-① 問題のテスト画面

② 「一般的な問題」に記載されている各項目の番号を画面下の空白欄に入力します。（図 4-1-5-1-②）

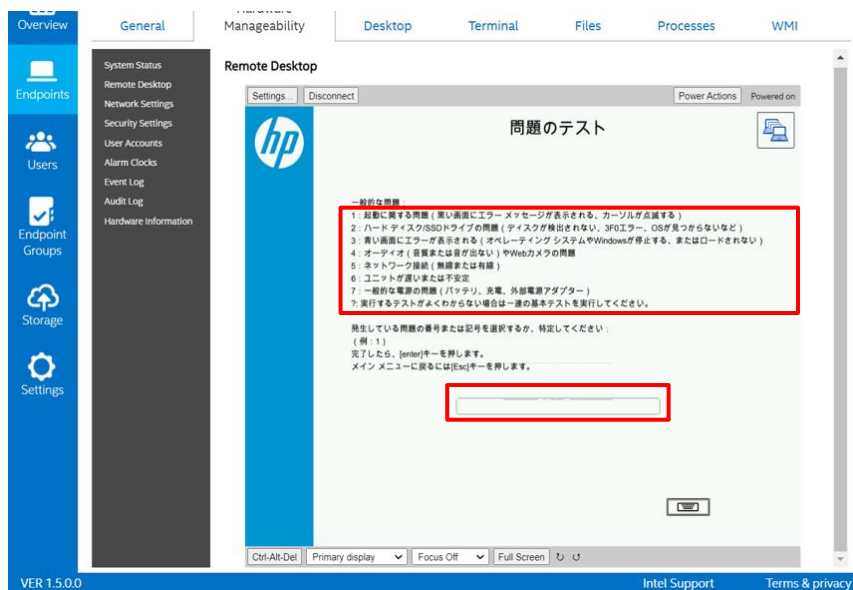


図 4-1-5-1-② 問題のテスト表示画面

※「一般的な問題」の各項目については、以下の表 4-1-5-1-①に示します。

表 4-1-5-1-① 問題のテスト 各チェック項目詳細

項目	操作	チェック内容
起動に関する問題	1を入力	起動時に異常がある場合に選択
ハードディスク(SSD)ドライブの問題	2を入力	ディスクが検出しないなどディスクに異常がある場合に選択
青い画面にエラーが表示される	3を入力	ブルースクリーンエラーが出る場合に選択
オーディオ（音楽または音が出ない） や Web カメラの問題	4を入力	音やカメラに異常がある場合に選択
ネットワーク接続	5を入力	ネットワークに繋がらないなどネットワークに異常がある場合に選択
ユニットが遅いまたは不安定	6を入力	PC の動作が不安定な場合に選択
一般的な電源の問題	7を入力	バッテリーやアダプターに異常がある場合に選択
実行するテストが分からない場合	?を入力	ハードウェア全般のチェック（後述のシステムテストと同様）

③ テキストボックス欄に「1」と入力し、Enter キーを押下します。（図 4-1-5-1-③）

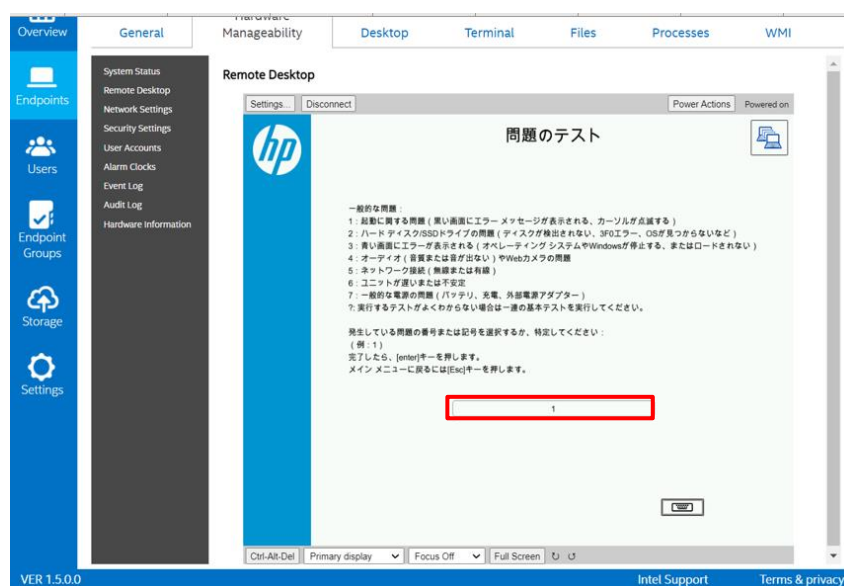


図 4-1-5-1-③ 起動に関する問題 入力画面

- ④ 以下の画面が表示されるので、「1 回実行」を選択して Enter キーを押下します。（図 4-1-5-1-④）
- ※テスト内容は画面の中央に記載されています。

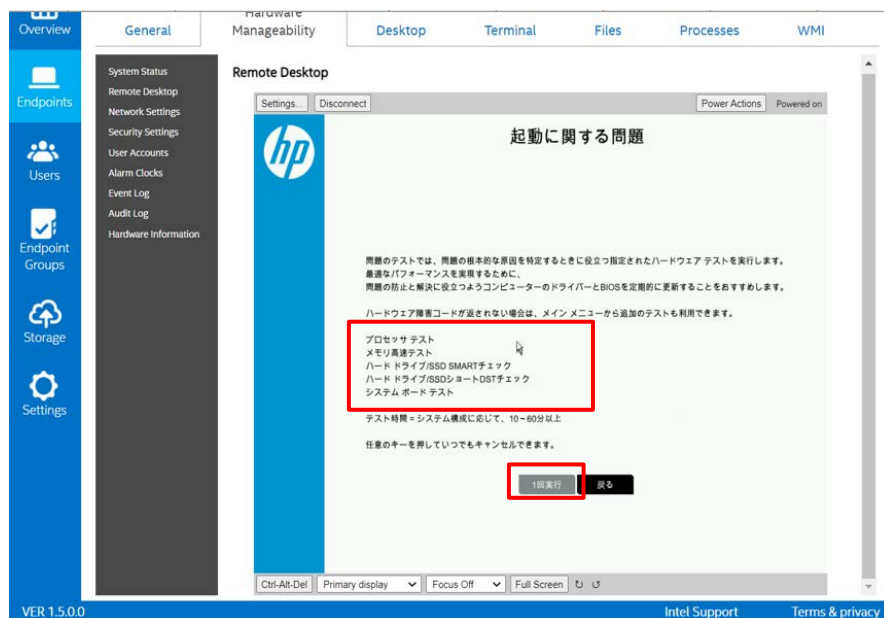


図 4-1-5-1-④ 起動に関する問題 実行画面

- ⑤ 以下の画面が表示され、「残り時間」と「進行状況」が表示されます。（図 4-1-5-1-⑤）

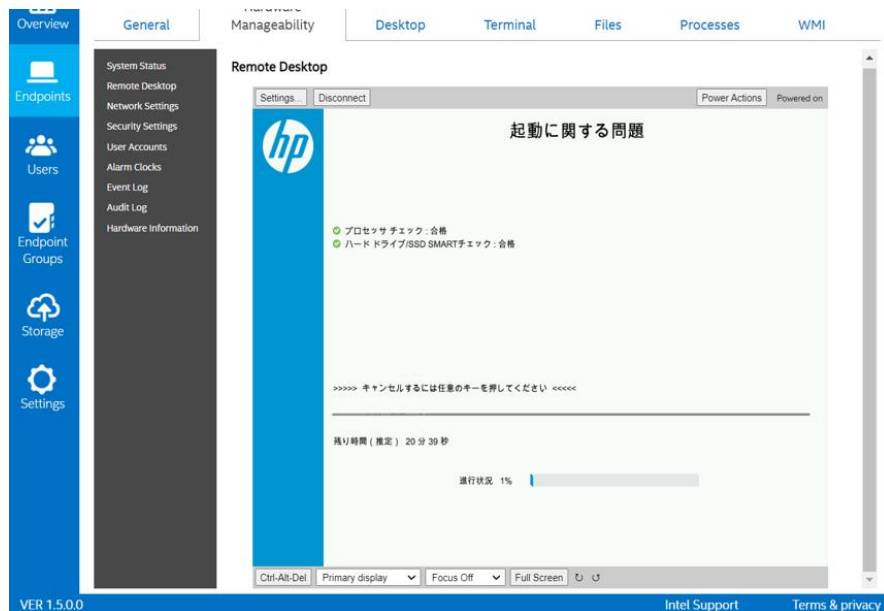


図 4-1-5-1-⑤ 起動に関する問題 処理中画面

⑥ 結果画面が表示されますので、結果内容を確認します。（図 4-1-5-1-⑥）

※本画面には 2 つのパターンがあります。

・「メインメニュー」ボタンしかない場合 → （ア）へ移動

・「メインメニュー」と「続行」ボタンの複数ボタンが表示される場合 → （イ）へ移動

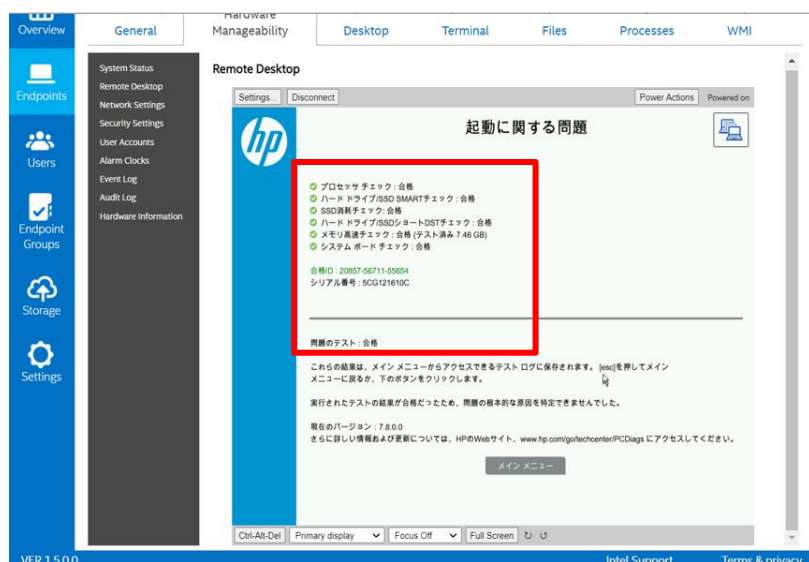


図 4-1-5-1-⑥ 起動に関する問題 結果画面

(ア) 「メインメニュー」ボタンしかない場合は、「メインメニュー」をクリックし、問題のテストが終了になります。(図 4-1-5-1-⑦)

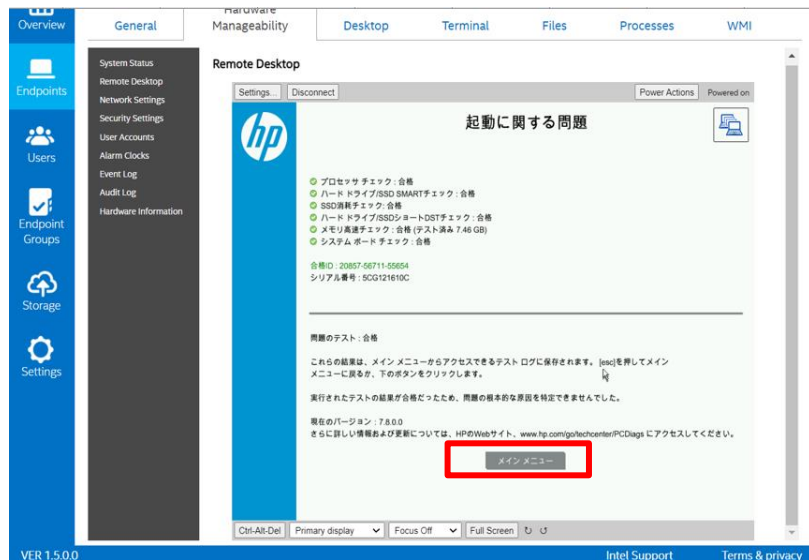


図 4-1-5-1-⑦ 起動に関する問題 結果画面 (パターン 1)

(イ) 「メインメニュー」と「続行」ボタンの複数ボタンが表示される場合は、「続行」ボタンをクリックし、手順⑤へ戻ります。(図 4-1-5-1-⑧)

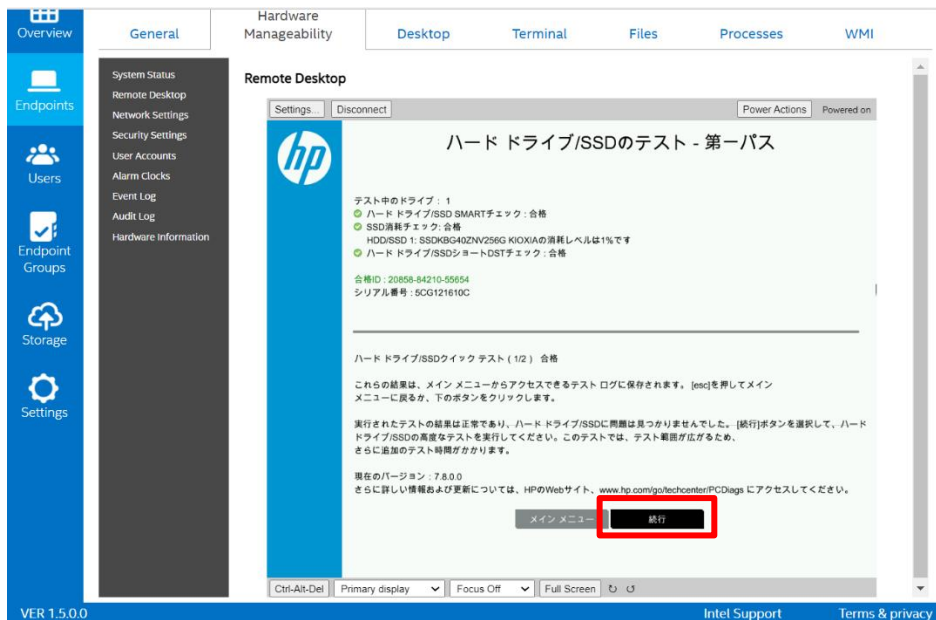


図 4-1-5-1-⑧ 起動に関する問題 結果画面 (パターン 2)

4.1.5.2 システムテスト

※本手順では「システムテスト」の中の「高速テスト」の手順について紹介しますが、他の項目についても同様の手順であるため、他の項目を実施する場合も本手順を参考にしてください。

① 「システムテスト」を選択します。(図 4-1-5-2-①)

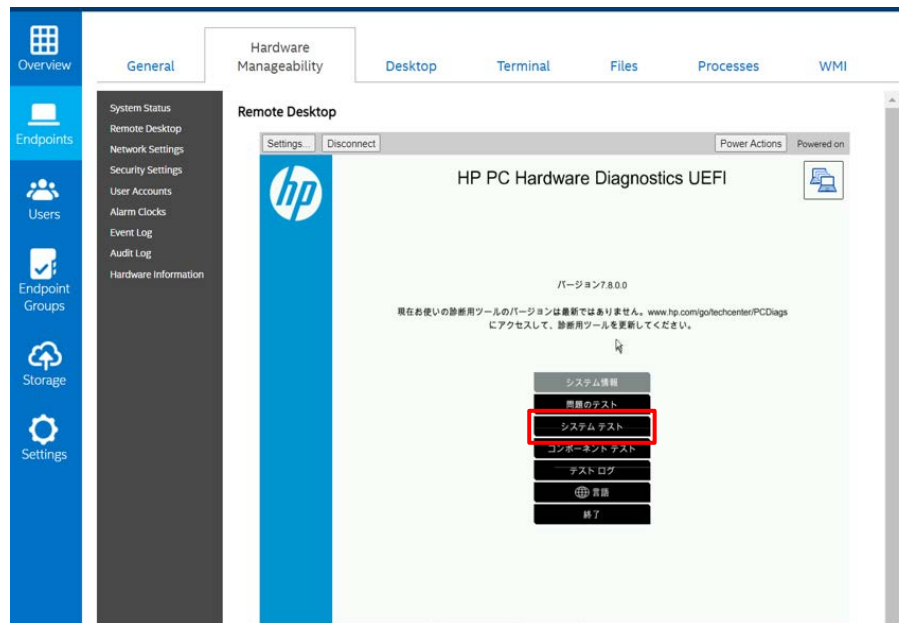


図 4-1-5-2-① システムテスト選択画面

② 以下の画面が表示されるので、「高速テスト」を選択します。（図 4-1-5-2-②）

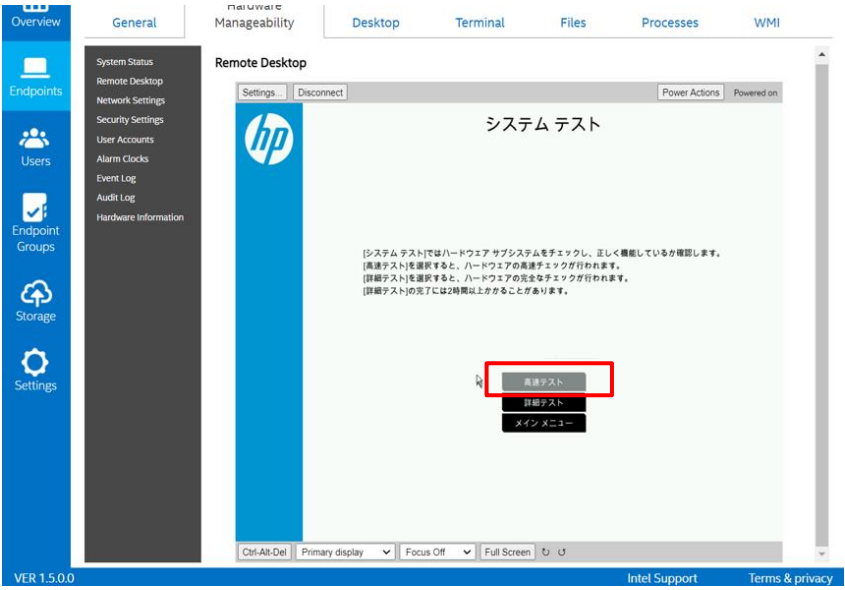


図 4-1-5-2-② システムテスト画面

※システムテストの各項目については、以下の表 4-1-5-2-①に示します。

表 4-1-5-2-① システムテスト 各チェック項目詳細

項目	内容
高速テスト	システム全般(ハードウェア)の高速テストを実施
詳細テスト	システム全般(ハードウェア)の完全テストを実施
メインメニュー	メインメニューへ戻る

- ③ 以下の画面が表示されるので、「1 回実行」を選択します。(図 4-1-5-2-③)

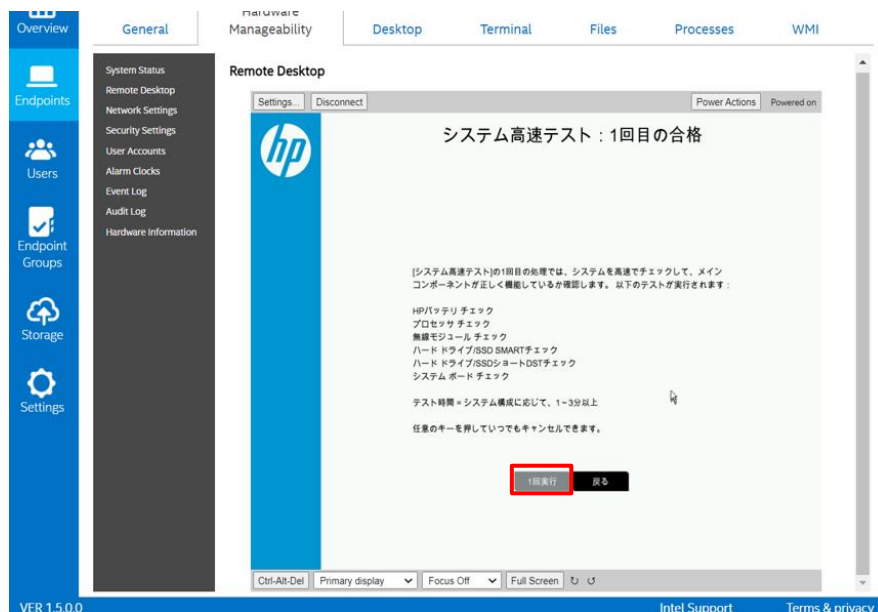


図 4-1-5-2-③ システム高速テスト(1 回目)実行画面

- ④ 結果画面が表示され、結果を確認します。(図 4-1-5-2-④)

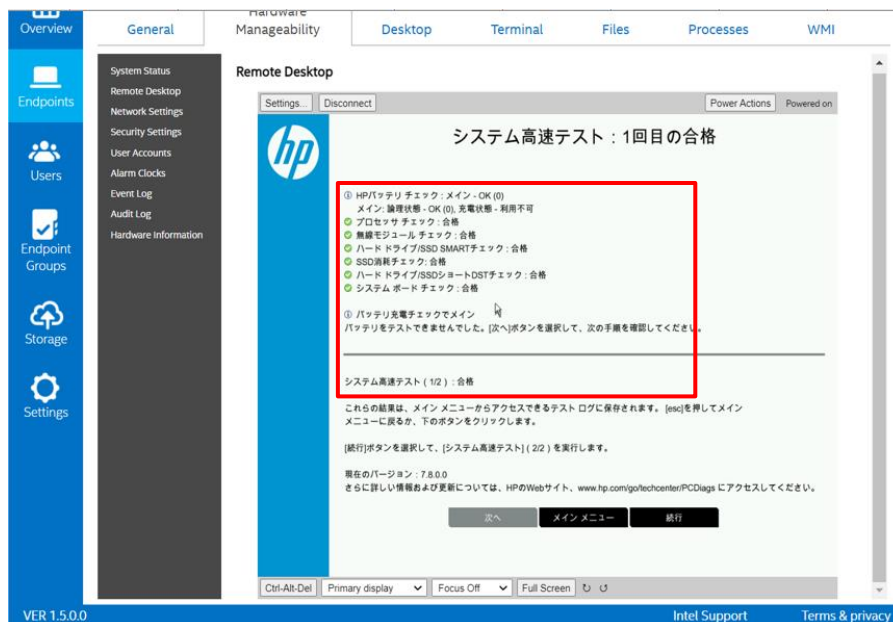


図 4-1-5-2-④ システム高速テストの実行結果画面

⑤ テストを実施した結果や画面の表示から、以下の3つのパターンになります。

ーテスト結果が全て「合格」であった場合 → (ア) へ移動

ーテスト結果に「不合格」があった場合 → (イ) へ移動

ーテスト結果が全て「合格」で「メインメニュー」ボタンしかない場合 → (ウ) へ移動

(ア) 「続行」を選択する場合は、1 回目のシステムテストが「合格」だった場合に選択します。(図 4-1-5-2-⑤)

※以降の基本的な操作の流れとしては、手順③に戻ります。

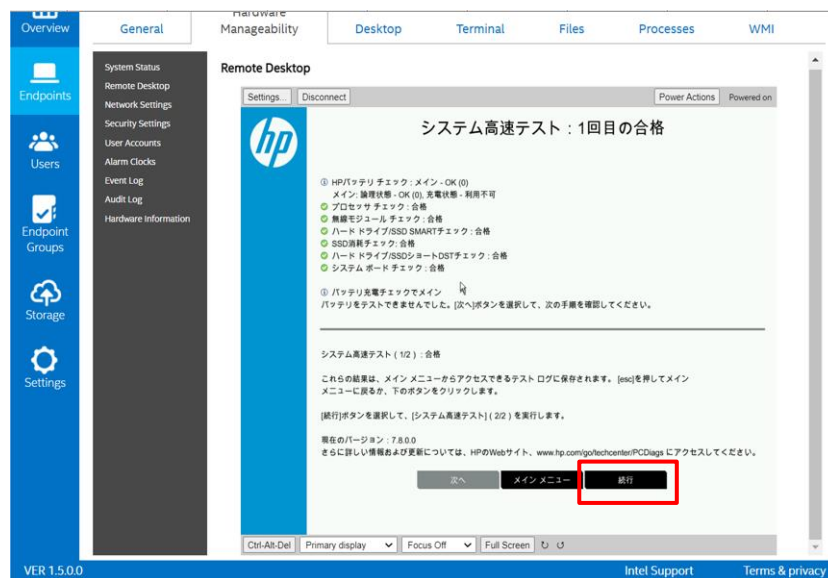


図 4-1-5-2-⑤ システム高速テスト(1 回目)結果画面

(イ)「次へ」を選択する場合は、システムテストのテスト項目の中で、「不合格」あった場合に選択します。(図 4-1-5-2-⑥)

※以降の基本的な操作の流れとしては、手順③に戻ります。

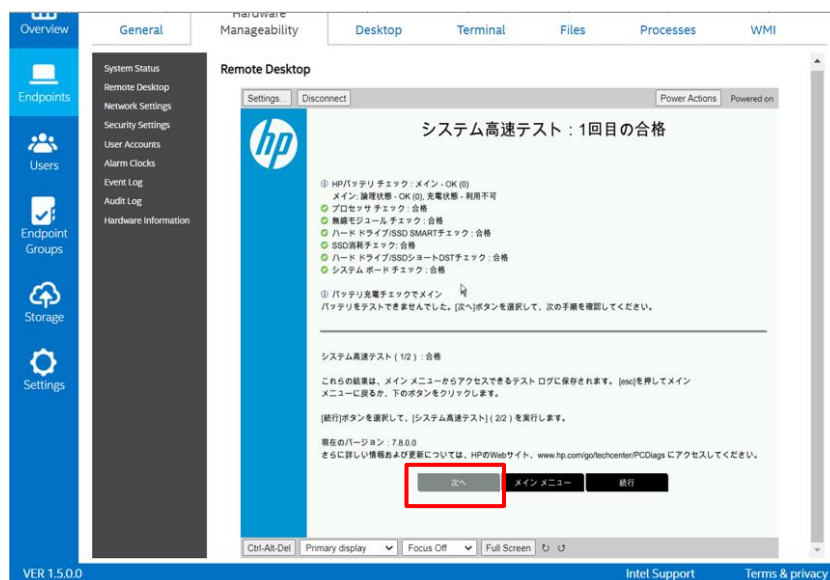


図 4-1-5-2-⑥ システム高速テスト結果画面

(ウ)「メインメニュー」ボタンしかない場合は、「メインメニュー」ボタンをクリックし、システムテストを終了します。(図 4-1-5-2-⑦)

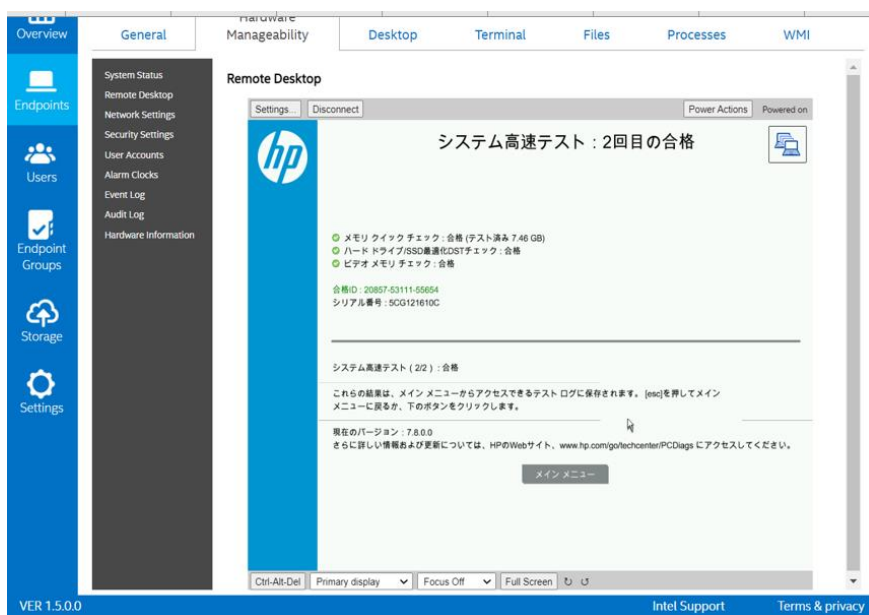


図 4-1-5-2-⑦ システム高速テスト実行画面

4.1.5.3 コンポーネントテスト

※本手順では「コンポーネントテスト」の中の「プロセッサ」の手順について紹介しますが、他の項目についても同様の手順であるため、他の項目を実施する場合も本手順を参考にしてください。

- ① 「コンポーネントテスト」を選択します。（図 4-1-5-3-①）

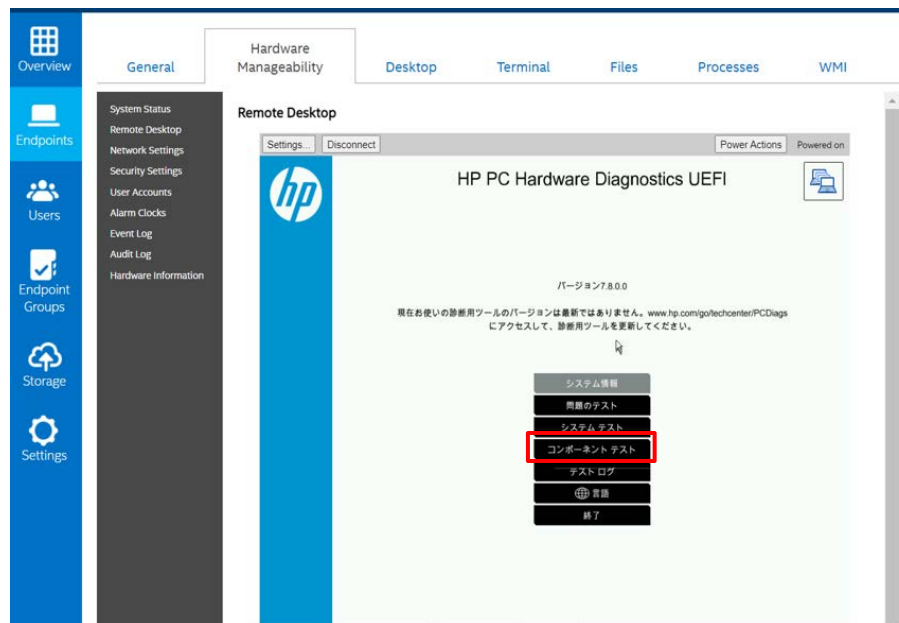


図 4-1-5-3-① コンポーネントテスト選択画面

- ② コンポーネントテスト画面が表示されます。（図 4-1-5-3-②）

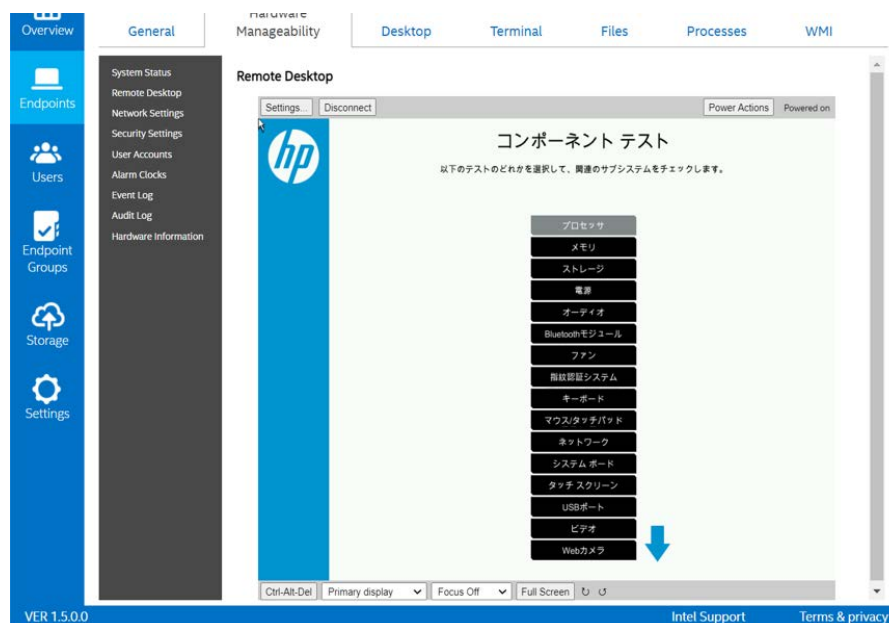


図 4-1-5-3-② コンポーネントテスト画面

※コンポーネントテストの各項目の説明については、以下の表図 4-1-5-3-①に示します。

表 4-1-5-3-① コンポーネントテスト 各チェック項目詳細

項目	テスト内容
プロセッサ	CPU の正常性確認
メモリ	メモリの正常性確認
ストレージ	HDD、SSD などの正常性確認
電源	バッテリーの正常性確認
オーディオ	オーディオの動作率
Bluetooth モジュール	Bluetooth、無線モジュールの確認
ファン	ファンの正常性
指紋認証システム	指紋認証が出来るかの確認
キーボード	キーボードの反応チェック
マウス／タッチパッド	マウス／タッチパッドの反応チェック
ネットワーク	ネットワークの正常性確認
システムボード	マザーボードの正常性確認
タッチスクリーン	タッチスクリーンの反応チェック
USB ポート	USB ポートの正常性確認
ビデオ	ビデオメモリの正常性確認
Web カメラ	Web カメラの正常性確認
メインメニュー	メインメニューに戻る

③ 「プロセッサ」を選択します。(図 4-1-5-3-③)

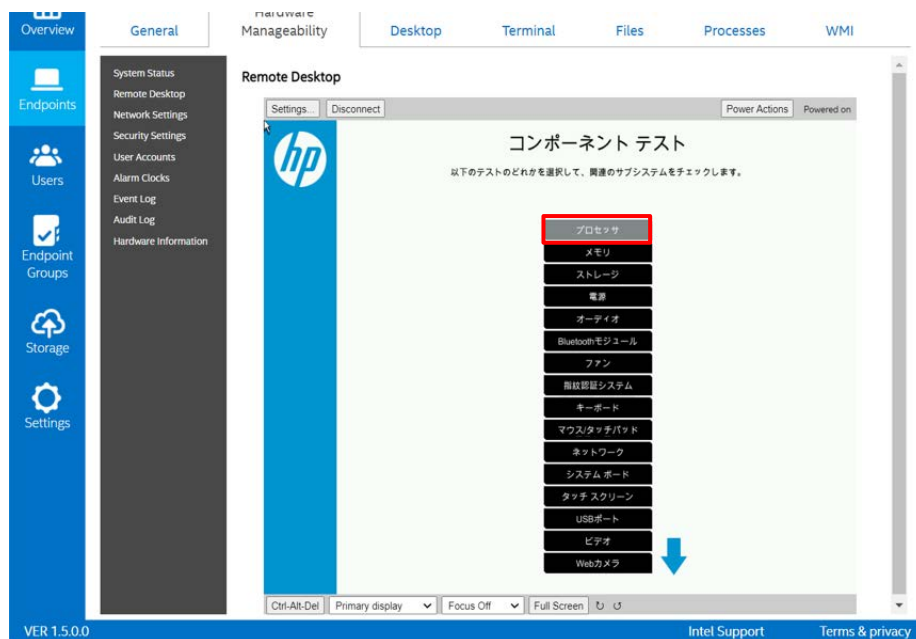


図 4-1-5-3-③ コンポーネントテスト選択画面

④ 以下の画面が表示されるので、「1 回実行」を選択します。(図 4-1-5-3-④)

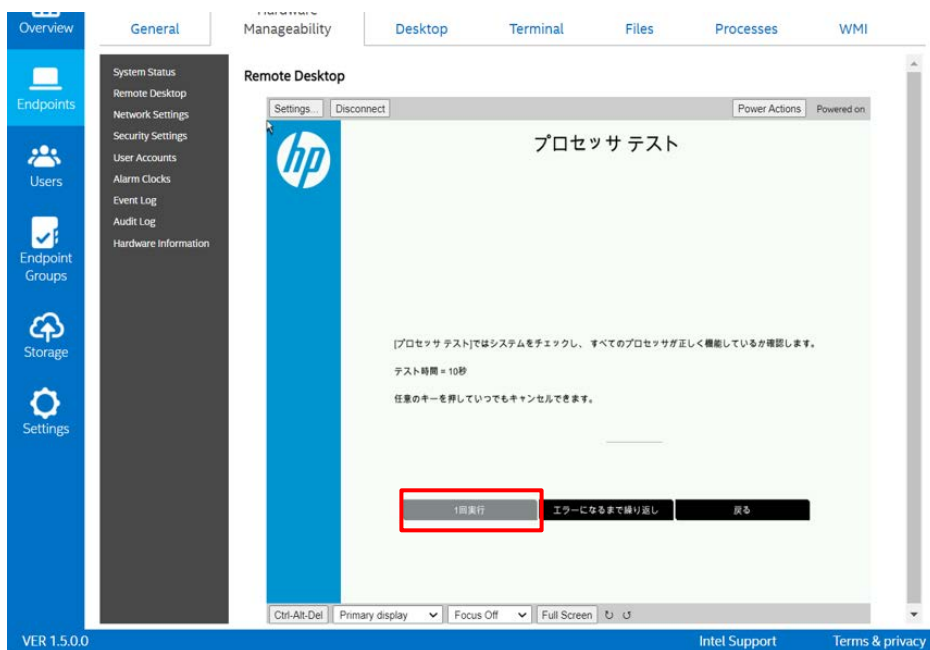


図 4-1-5-3-④ プロセッサテスト実行画面

⑤ テストを実施した結果や画面の表示から、以下の2つのパターンになります。(図 4-1-5-3-⑤)

–「メインメニュー」ボタンしかない場合 → (ア) へ移動

–「メインメニュー」と「続行」が表示されている場合 → (イ) へ移動

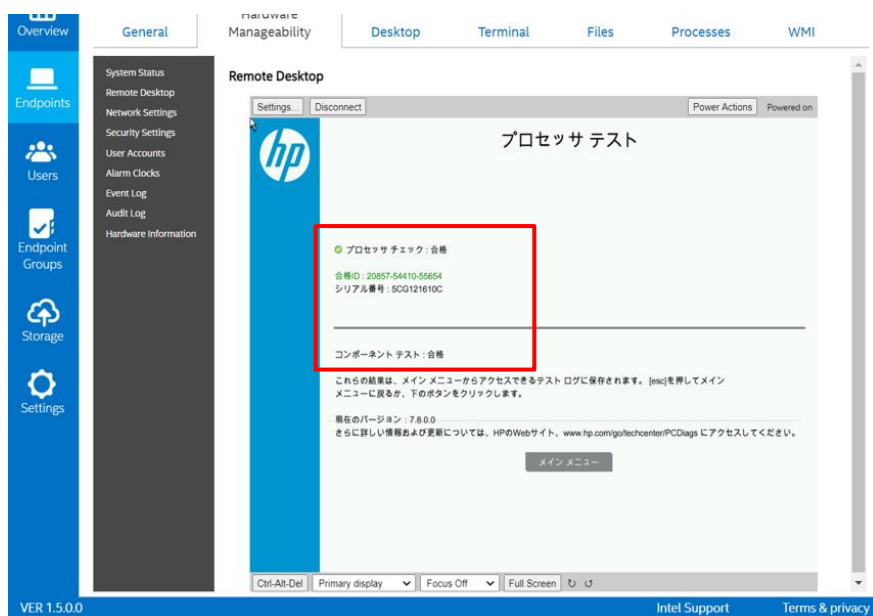


図 4-1-5-3-⑤ プロセッサテスト結果画面

(ア) 「メインメニュー」ボタンしかない場合、「メインメニュー」ボタンをクリックしテストを終了します。

(図 4-1-5-3-⑥)

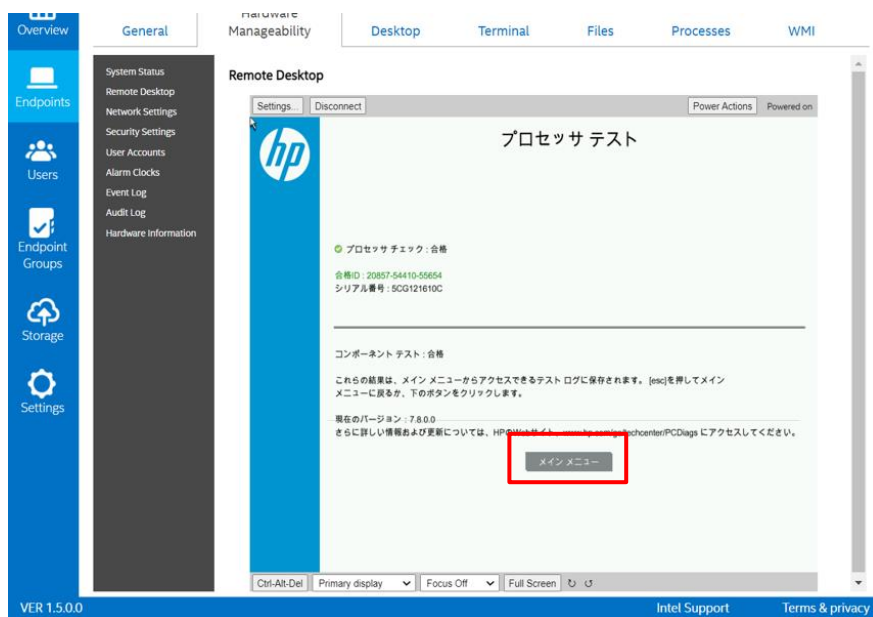


図 4-1-5-3-⑥ プロセッサテスト結果画面

(イ)「メインメニュー」と「続行」が表示されている場合は、「続行」ボタンをクリックし、手順③に戻ります。(図 4-1-5-3-⑦)

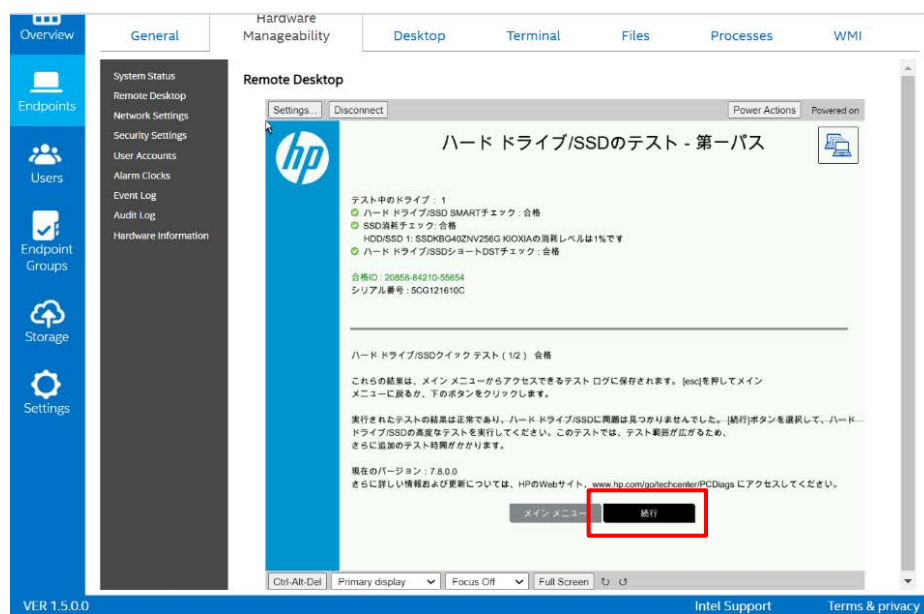


図 4-1-5-3-⑦ プロセッサテスト結果画面

4.1.5.4 テストログ

以下の手順で各テスト実施した結果の表示やログ保存が可能になります。

- ① 「テストログ」を選択します。(図 4-1-5-4-①)

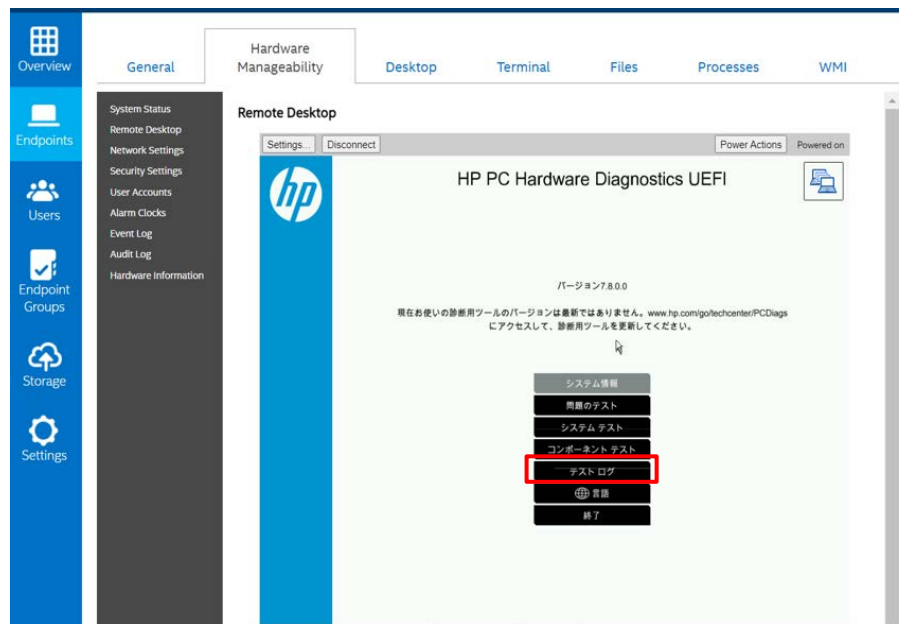


図 4-1-5-4-① テストログ選択画面

② これまでチェックしたテストの結果が表示されます。(図 4-1-5-4-②)

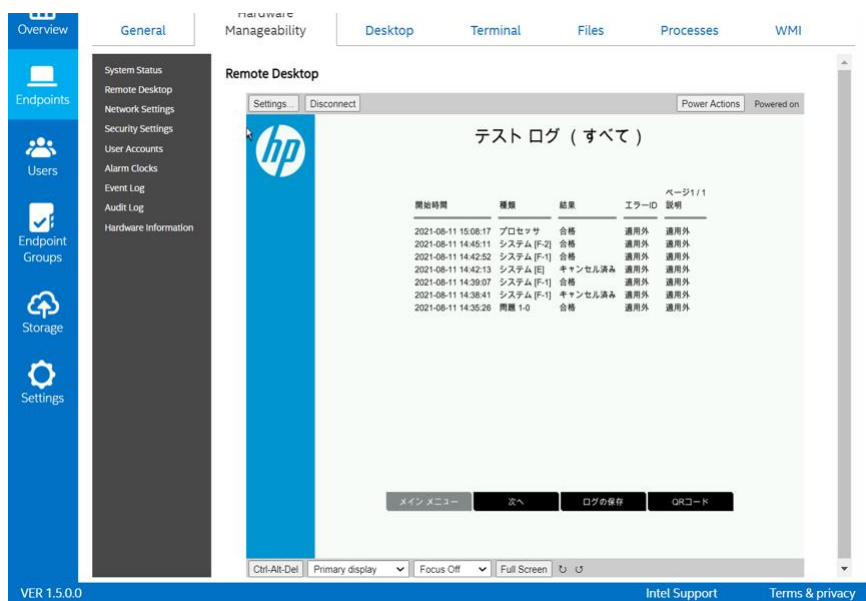


図 4-1-5-4-② テストログ画面

※テストログの各項目の説明については以下の表 4-1-5-4-①に示します。

表 4-1-5-4-① テストログ 各項目詳細

項目	表示内容
メインメニュー	メインメニューに戻る
次へ	次ページを表示
ログの保存	外付けの媒体（USB フラッシュメモリ）へ保存
QR コード	QR コードの表示

4.1.5.5 システム情報

※本手順では、「システム情報」の中の「システム」部分を閲覧する手順を記載しているが、その他の項目についても同様の手順のため、本手順を参考にしてください。

- ① 「システム情報」を選択します。(図 4-1-5-5-①)

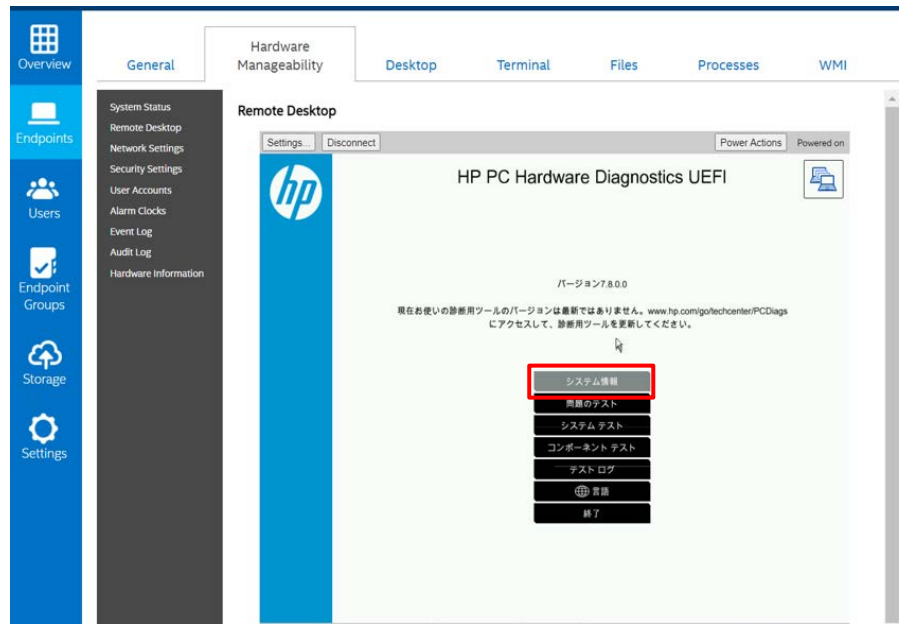


図 4-1-5-5-① システム情報 選択画面

- ② 以下のようにシステム情報の画面が表示される。(図 4-1-5-5-②)

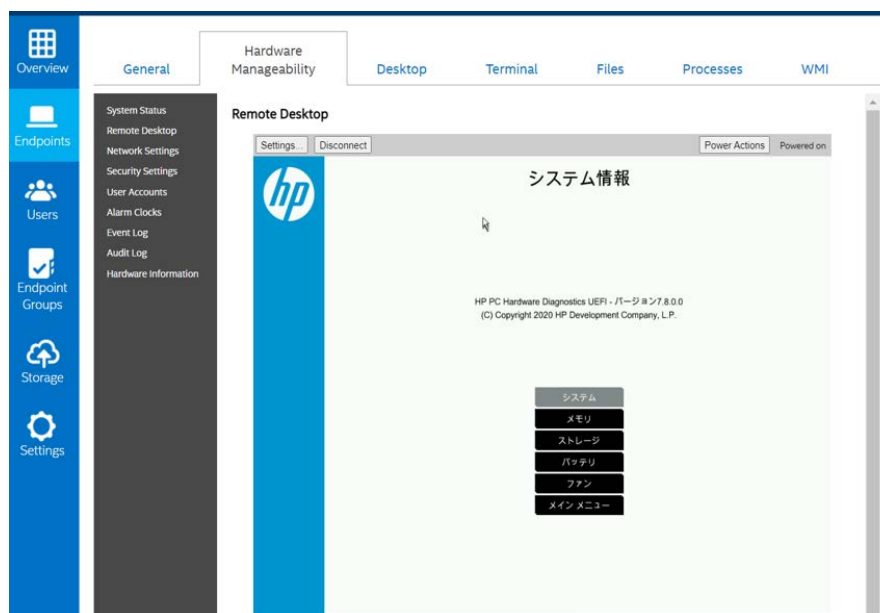


図 4-1-5-5-② システム情報画面

※システム情報の各項目について、以下の表 4-1-5-5-①に示します。

表 4-1-5-5-① システム情報 各項目詳細

項目	表示内容
システム	製造元、製造日、メモリサイズ、プロセッサタイプの情報が閲覧可能
メモリ	スロットごとのメモリの情報が閲覧可能
ストレージ	HDD、SSD の容量、温度の情報が閲覧可能
バッテリー	バッテリーの状況（電圧、温度など）の情報が閲覧可能
ファン	ファンの動作率、速度などの情報が閲覧可能
メインメニュー	メインメニューに戻る

4.1.5.6 終了

- ① 「終了」を選択します。(図 4-1-5-6-①)

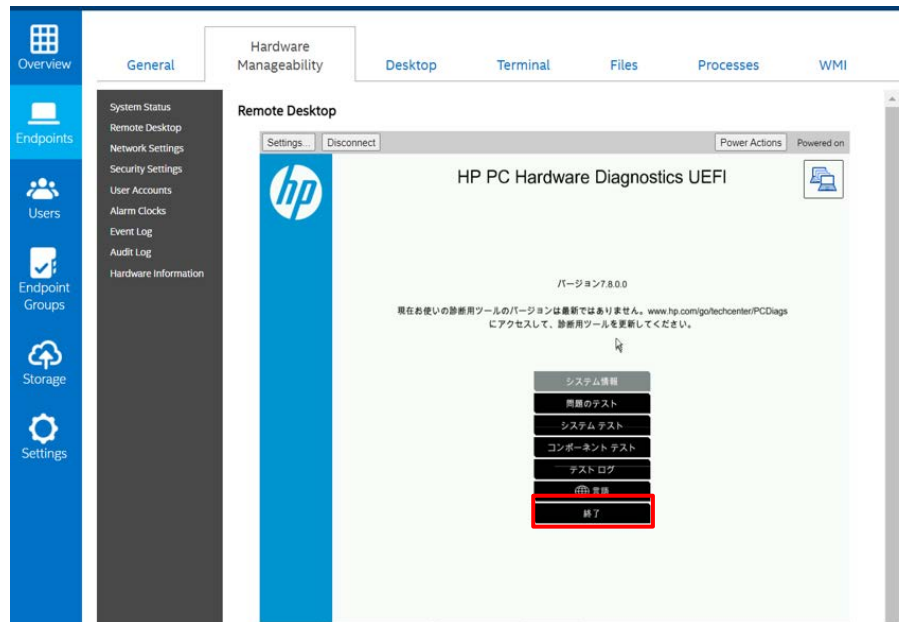


図 4-1-5-6-① 終了選択画面

- ② 以下の画面が表示され「よろしいですか？」と画面に表示されますので、「はい」選択します。(図 4-1-5-6-②)

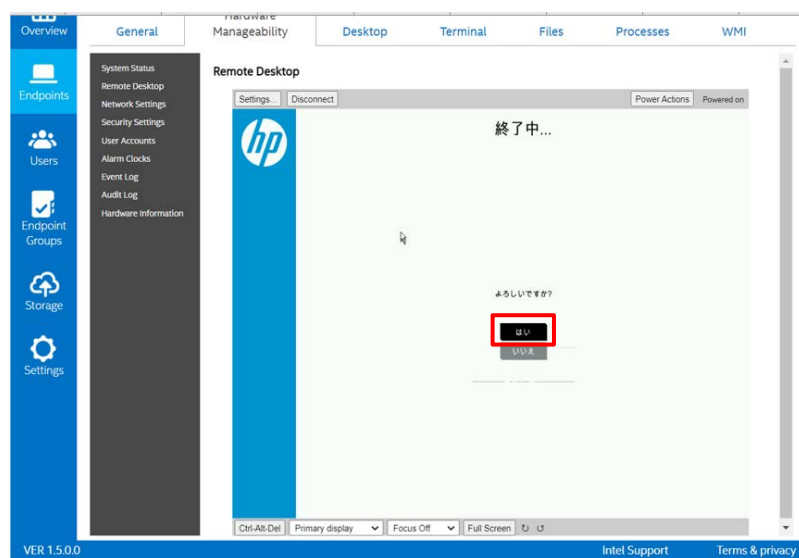


図 4-1-5-6-② 終了中画面

※終了の各項目については、以下の表 4-1-5-6-①に示します。

表 4-1-5-6-① 各項目詳細

項目	内容
はい	メインメニューに戻る
いいえ	HP PC Hardware Diagnostics UEFI 画面へ戻る

4.1.6 クライアント PC に対してのファイル転送機能

ファイル転送機能では、リモートからエンドポイント（クライアント PC）上にあるファイルのデータをダウンロードする機能やインテル®EMA 管理画面の操作端末（コンソール PC）上にあるファイルをアップロードするための操作手順を記載します。その他にもフォルダ作成やファイル名変更、ファイル削除も可能となっております。

本章では、エンドポイント（クライアント PC）側のフォルダを表示するまでの手順を記載します。

※ファイルのアップロード手順は「4.1.6.2」に記載、ファイルのダウンロード手順は「4.1.6.3」に記載します。

4.1.6.1 クライアント PC のフォルダ内容表示

- ① ブラウザにてインテル®EMA サーバの DNS 名を入力し、インテル®EMA へ接続（URL:https://[インテル®EMA サーバの DNS 名]）し、インテル®EMA サーバ作成時に設定した user name と Password を入力、Log In ボタンをクリックしログインします。（図 4-1-6-1-①）

※「テナント管理者」または「エンドポイント管理者」権限が設定されているユーザでログインします。

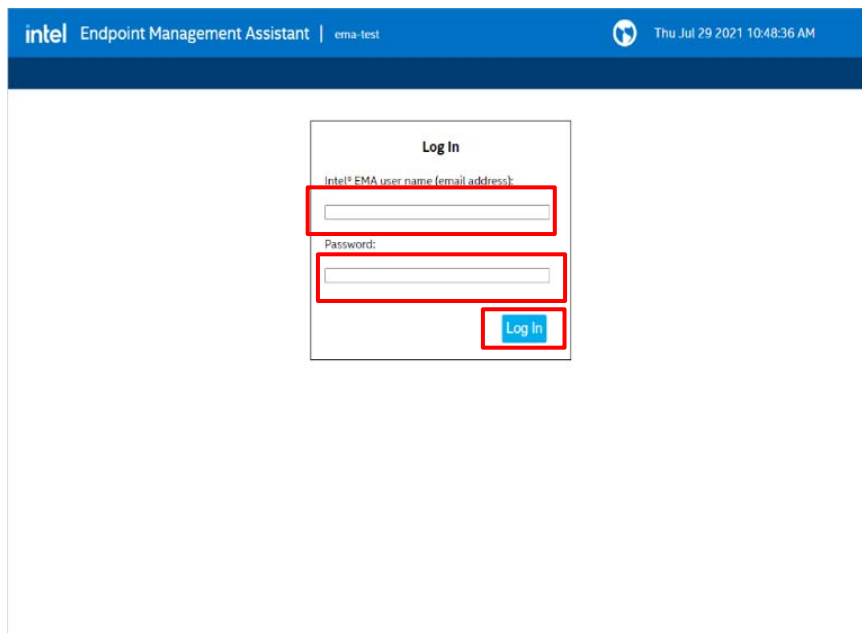


図 4-1-6-1-① ログイン画面

- ② Overview 画面が表示されるので、左側のメニューから「Endpoints」を選択します。（図 4-1-6-1-②）

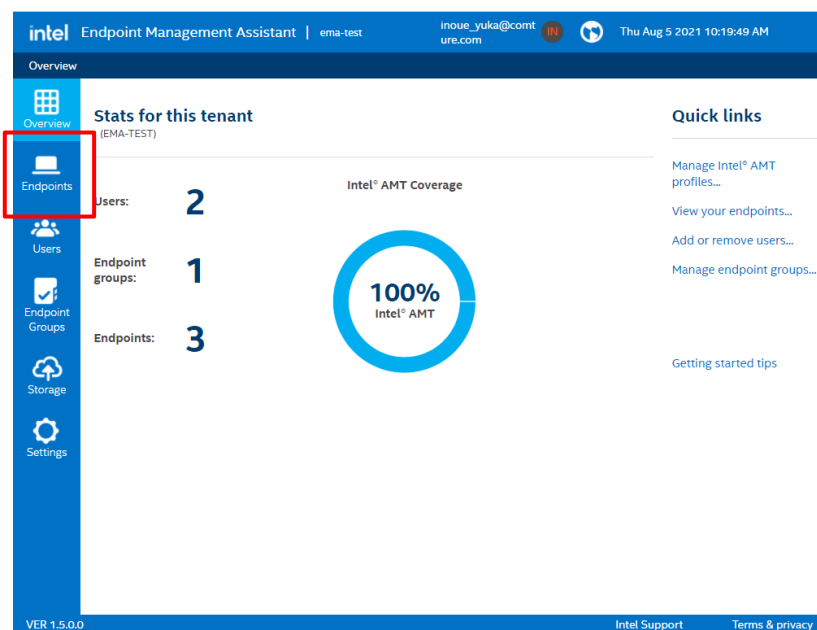


図 4-1-6-1-② ログイン後のトップ画面

- ③ 「Load all Endpoints」をクリックします。（図 4-1-6-1-③）

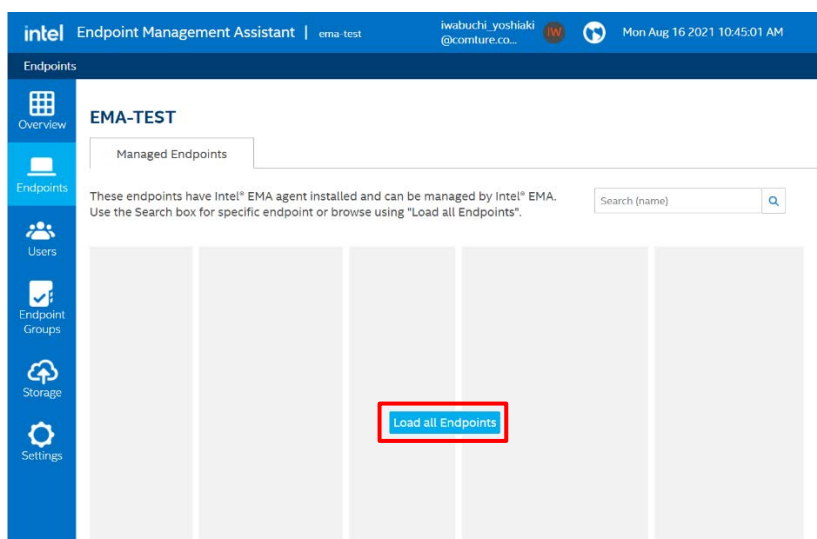


図 4-1-6-1-③ Endpoint 選択画面

- ④ ファイル操作を行うエンドポイント（クライアント PC）の右側にある「view」をクリックします。（図 4-1-6-1-④）

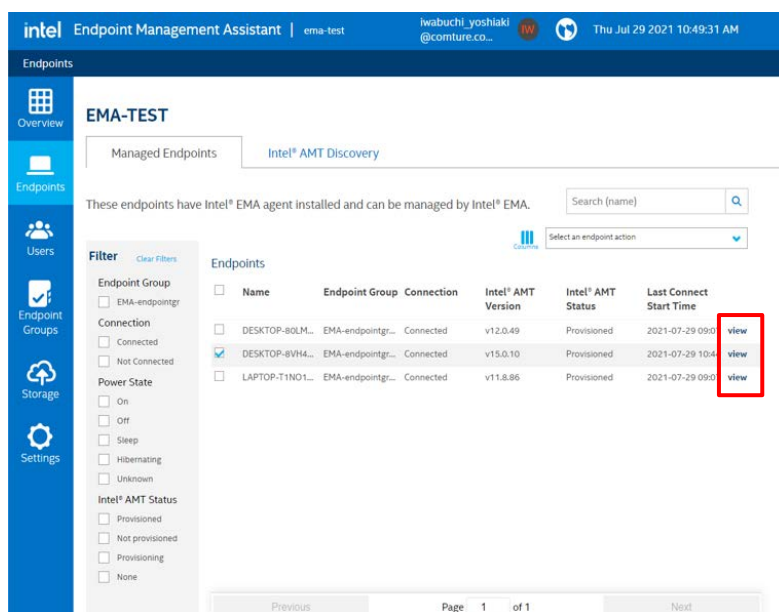


図 4-1-6-1-④ Endpoint 選択画面

- ⑤ General タブの画面の右側にある「Connected」であることを確認した後、「Files」タブを選択します。（図 4-1-6-1-⑤）

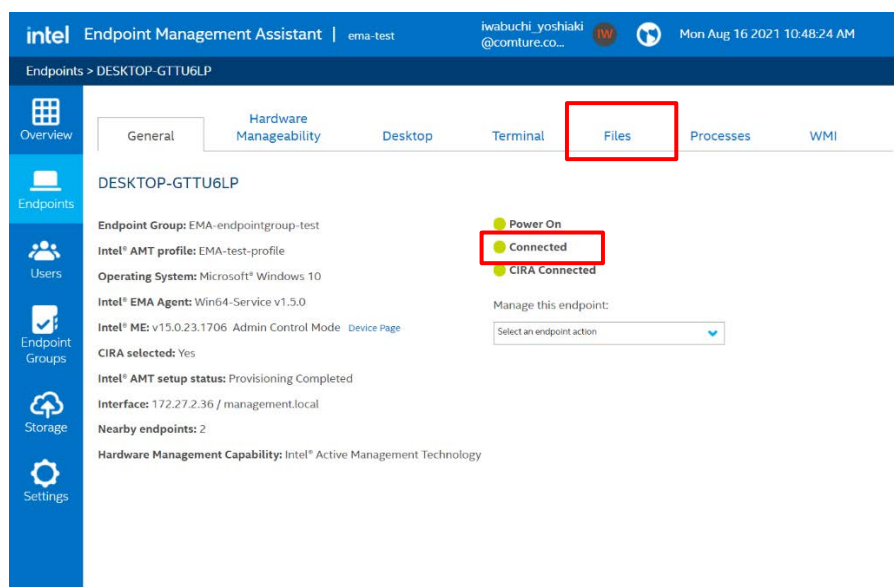


図 4-1-6-1-⑤ Endpoint 状態確認画面

⑥ 「Connect to Files」をクリックします。(図 4-1-6-1-⑥)

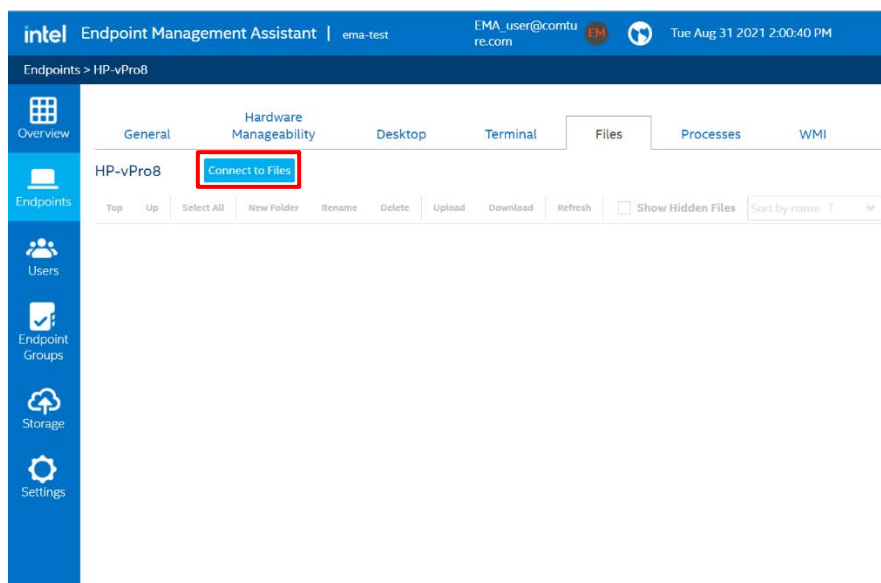


図 4-1-6-1-⑥ Files 詳細画面

⑦ クライアント PC のディレクトリが表示されることを確認します。(図 4-1-6-1-⑦)

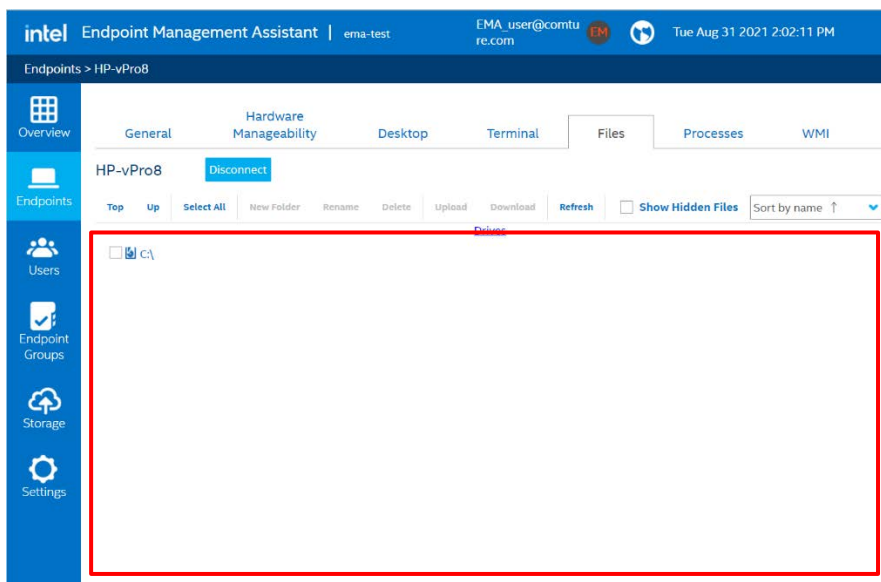


図 4-1-6-1-⑦ Connect to Files クリック後画面

※下記赤枠部分の各機能については以下表 4-1-6-1-①で説明します。

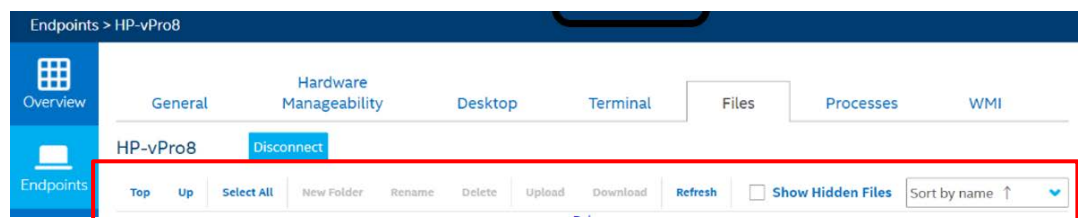


表 4-1-6-1-① Files 機能説明

機能	機能説明
Top	一番上のディレクトリへ移動
Up	一つ上のディレクトリへ移動
Select All	現在のディレクトリの全ファイルを選択
New Folder	現在のディレクトリに新しいフォルダを作成
Rename	ファイル名の変更
Delete	選択したファイルの削除
Upload	ファイルのアップロード
Download	選択したファイルのダウンロード
Refresh	ディレクトリ状態の更新
Show Hidden Files	隠しファイルの有効／無効
Sort By (name/size/date)	ファイル名・サイズ・更新日付の昇順または降順

4.1.6.2 ファイルのアップロード機能

ファイルのアップロード機能とは、インテル®EMA 管理画面の操作端末（コンソール PC）の「C ドライブ」や「デスクトップ」などにあるファイルをエンドポイント（クライアント PC）へアップロードする機能になります。共有したいファイルをクライアント PC に置きたい場合や、バッチファイルなどをクライアント PC 上で実行したい場合などに活用できます。本章ではファイルのアップロード機能の操作手順について記載します。

- ① ファイルをアップロードしたいフォルダの場所まで移動し、「Upload」ボタンをクリックします。（図 4-1-6-2-①）

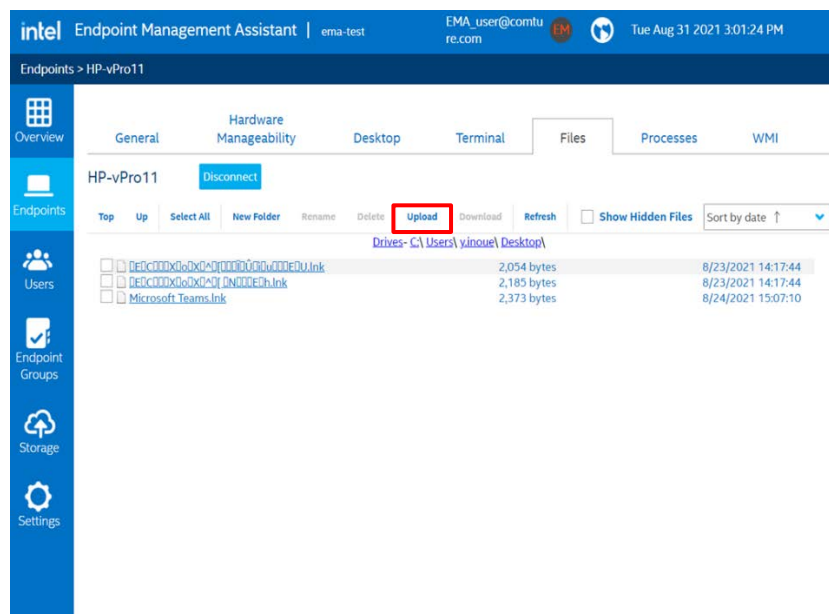


図 4-1-6-2-① Files タブ操作画面

- ② 以下のような画面が表示されるので、「Select files to upload」をクリックします。（図 4-1-6-2-②）

※手順②・③については「Select files to upload」ボタンの下にある点線の四角枠にドラッグ＆ドロップでも同様にアップロードするファイルを指定可能です。

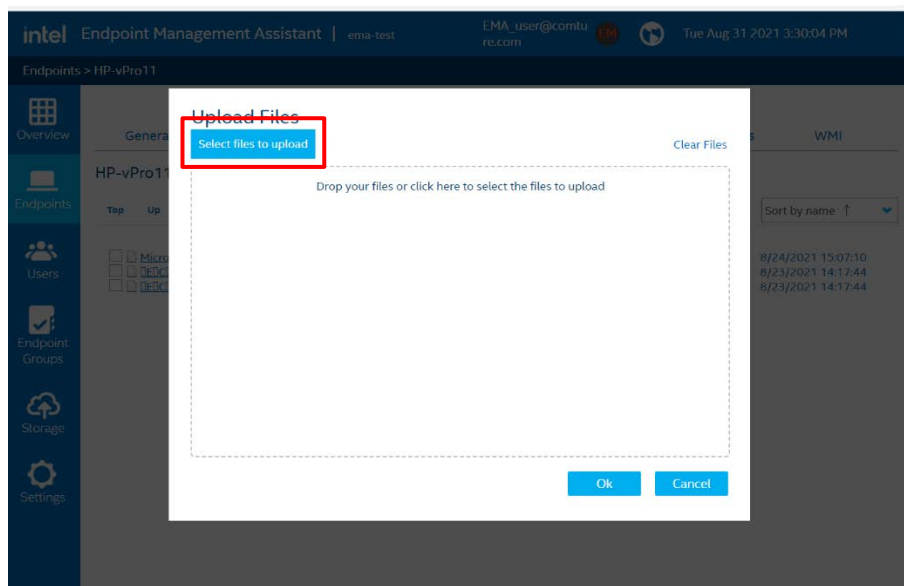


図 4-1-6-2-② アップロード画面

- ③ アップロードしたいファイルを選択し、「開く」をクリックします。（図 4-1-6-2-③）

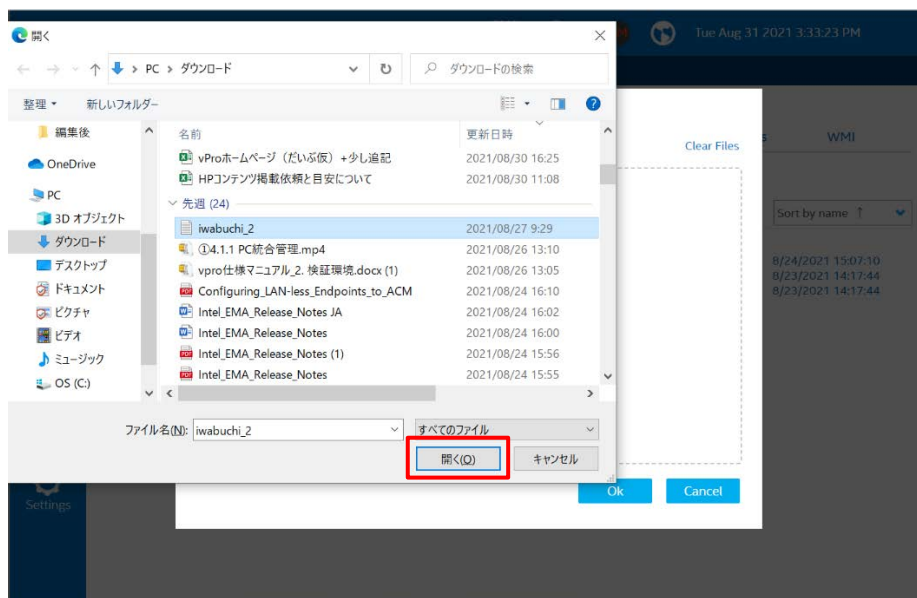


図 4-1-6-2-③ アップロードファイル選択画面

- ④ アップロードを予定しているファイルが表示されていることを確認後、「OK」をクリックします。（図 4-1-6-2-④）

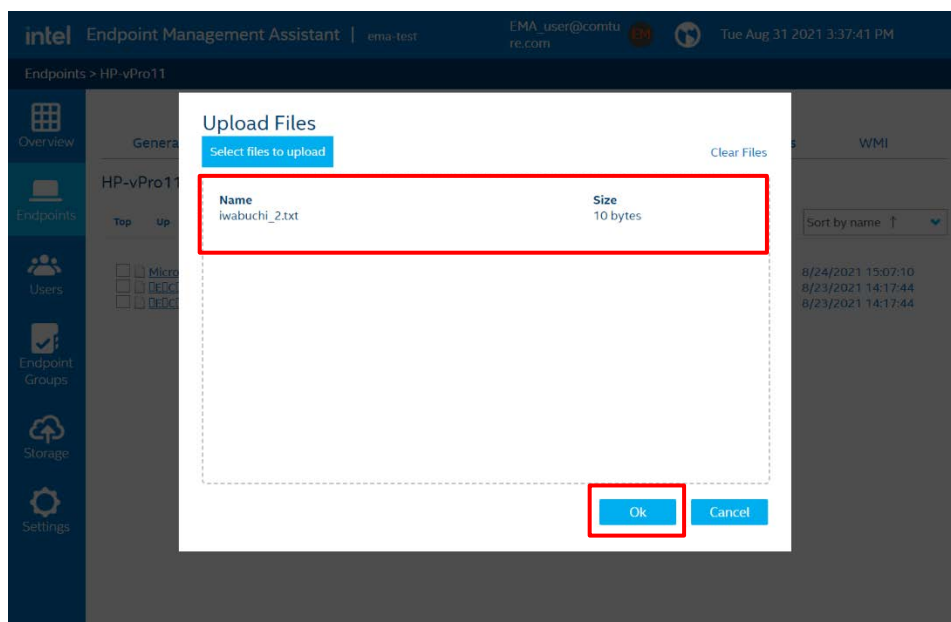


図 4-1-6-2-④ アップロードファイル確認画面

- ⑤ アップロードしたファイルがあることを確認します。（図 4-1-6-2-⑤）

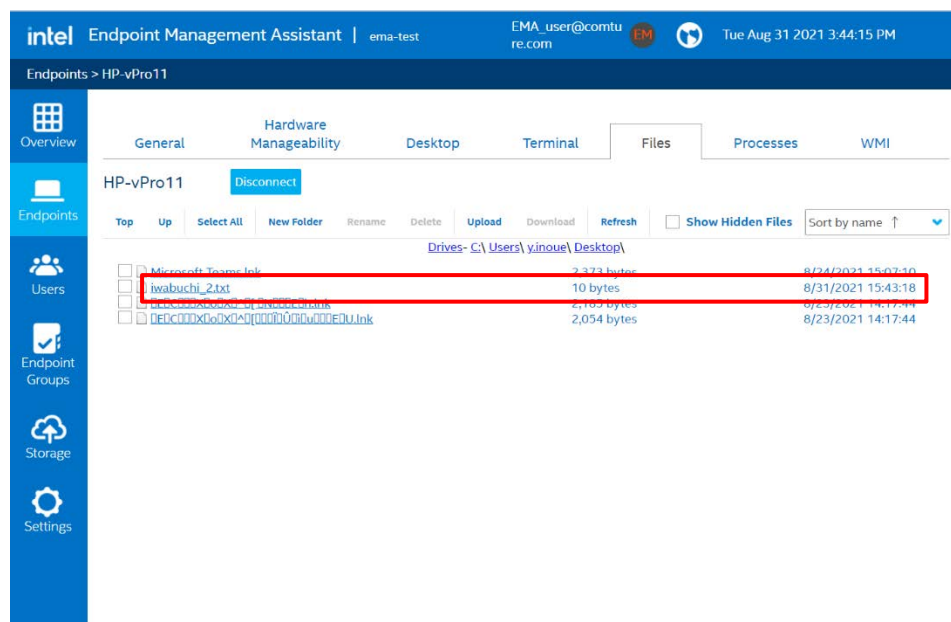


図 4-1-6-2-⑤ アップロード確認画面

4.1.6.3 ファイルのダウンロード機能

ファイルのダウンロード機能とは、エンドポイント（クライアント PC）から EMA 管理画面の操作端末（コンソール PC）にファイルをダウンロードする機能になります。クライアント上にあるファイルを効率良く自端末でファイル編集したい場合などに活用できます。本章ではファイルのダウンロードの操作手順について記載します。

- ① ダウンロードファイルが保存されているフォルダまで移動し、ダウンロードしたいファイルのチェックボックスにチェックを入れて「Download」ボタンをクリックします。（図 4-1-6-3-①）

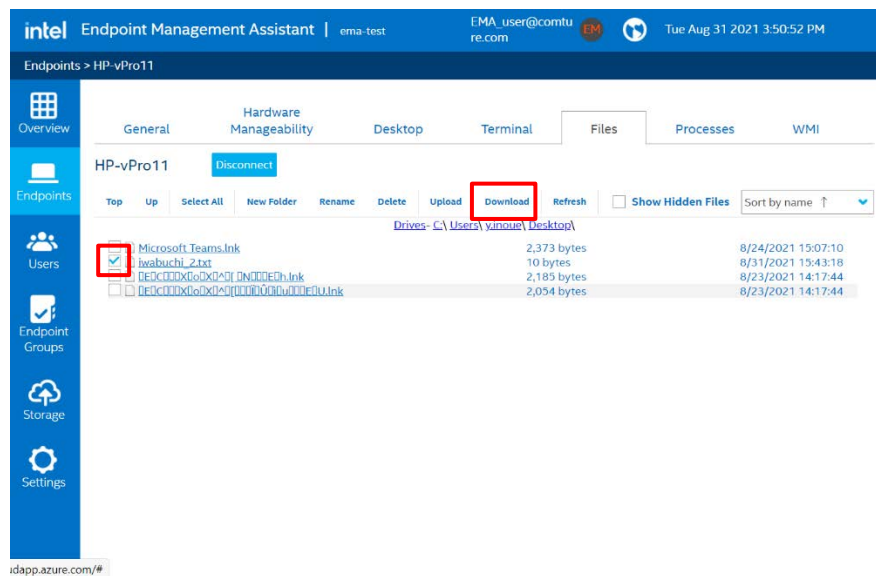


図 4-1-6-3-① ファイル選択画面

- ② コンソール PC の「ダウンロード」フォルダに該当のファイルがダウンロードされていることを確認します。（図 4-1-6-3-②）

※通常であれば「ダウンロード」フォルダに格納されます。

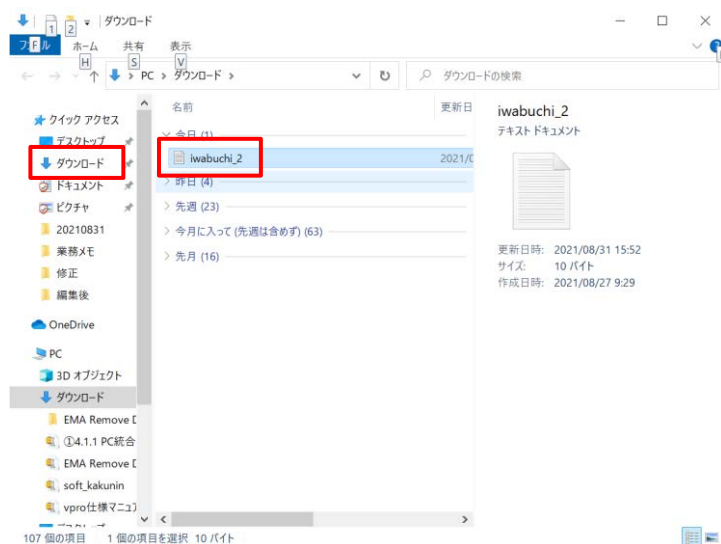


図 4-1-6-3-② ダウンロードファイル確認画面

4.2 セキュリティ

インテル® vPro® プラットフォームには、インテル® vPro® プラットフォームのみで利用可能なインテル® ハードウェア・シールドという包括的なハードウェア・ベースのセキュリティ機能を搭載しており、OS 下層のセキュリティ、アプリケーションとデータの保護、高度な脅威検出機能を提供します。

また、HP 社のインテル®vPro®プラットフォーム搭載端末には HP Wolf Security for Business があり、本機能と組み合わせることで、よりセキュリティの強化を実現しています。

本章では様々なセキュリティ機能についてご説明します。

4.2.1 ハードウェア支援型 AI による検知

ハードウェア支援型の AI 検知では機器の状態を監視し、脅威からの保護と検知をすることが可能になります。現在、ほとんどの企業ではソフトウェアベースのセキュリティ対策を実施していますが、近年の悪意あるユーザから攻撃は高度になり PDos 攻撃のようにハードウェアへの攻撃を実施されることがあります。PDos 攻撃から守るためにもハードウェアベースのセキュリティ対策を実施することが必要になります。インテル®vPro®プラットフォームでは、「インテル®ハードウェア・シールド」によってハードウェアベースのセキュリティを実現しています。インテル®ハードウェア・シールドは OS よりも下位レイヤである BIOS、ファームウェアへの攻撃から防御が可能になります。（図 4-2-1-①）

これにより、ファームウェアやデバイスドライバなどの脆弱性をついたリスクから軽減することが可能になります。



図 4-2-1-① インテル®ハードウェア・シールド

また、インテル®ハードウェア・シールドでは、高度な攻撃を検知するために、ヒューリスティック型（挙動検知）の機械学習で「リアルタイム」や「継続的」両方の攻撃を検知します。

このようにセキュリティを向上させると利便性・生産性が低下するトレードオフになるのが一般的ですが、インテル®vPro®プラットフォームではマルウェアのスキャンをオンボードのインテル・グラフィックエンジンにオフロードすることができますので、生産性の低下を抑えながら、マルウェアのスキャンを実施することが可能になります。

4.2.2 自己回復型 BIOS によるファームウェア攻撃からの防御

自己回復型 BIOS によるファームウェア攻撃からの防御はファームウェアの攻撃や破損を自動的に検知しリカバリを実施します。これは HP Wolf Security for Business のセキュリティ機能の 1 つである「HP Sure Start」で実現しています。

HP Sure Start は、HP の PC のマザーボード上に搭載された HP 独自のセキュリティハードウェアである HP エンドポイントセキュリティコントローラを利用して起動時および実行中に BIOS を監視し、攻撃による改ざんや破損が発生した際に保護されたバックアップコピーを利用して自己修復します。

最新バージョンの HP Sure Start Gen6 では保護対象を BIOS だけでなく PC のシステムフラッシュ全体に拡張しています。PC のシステムフラッシュには BIOS だけでなく、PC の起動に必要なコンポーネントが含まれています。フラッシュの一部または全体が消去されてしまうと PC が起動できなくなってしまうので、このような攻撃からも PC を守ることができます。

- HP Sure Start の主な機能

HP Sure Start には以下の主要な機能があります。

- HP フォームファームウェアの真正性と改ざん防止

PC の起動時に HP ファームウェアと BIOS の真正性チェックを行い、正規の改ざんされていない HP ファームウェアと BIOS のみがロードされます。

- ランタイム侵入検知

OS を起動させる前に BIOS コードはメインメモリにロードされます。その後、OS が正常に起動し、OS 稼働している間も BIOS コードの一部がメインメモリに残っています。この部分が改竄されるとセキュリティ上、大きな問題となるため、OS が稼働中でもメインメモリを継続的な監視しています。

- BIOS 設定保護

すべてのユーザまたは管理者が変更した BIOS 設定をバックアップします。起動時に整合性のチェックが実行され BIOS の設定が変更されていないことを確認しています。

ー 自己回復

BIOS、ファームウェア、メインメモリの改ざんを検出した場合、保護されたバックアップコピーを使用して自動回復を行います。

ー インテル® マネジメントエンジンファームウェア保護

PC のシステムフラッシュには vPro プラットフォームで使用されるインテル® マネジメントエンジンファームウェアが含まれています。BIOS と同様にインテル® マネジメントエンジンファームウェアの保護と回復を行います。

- HP Sure Start のランタイム侵入検知

メールの添付ファイルなどからウイルス感染し、ファームウェア攻撃を受けた際、Hp Sure Start が不正動作を検知します。(図 4-2-2-①)

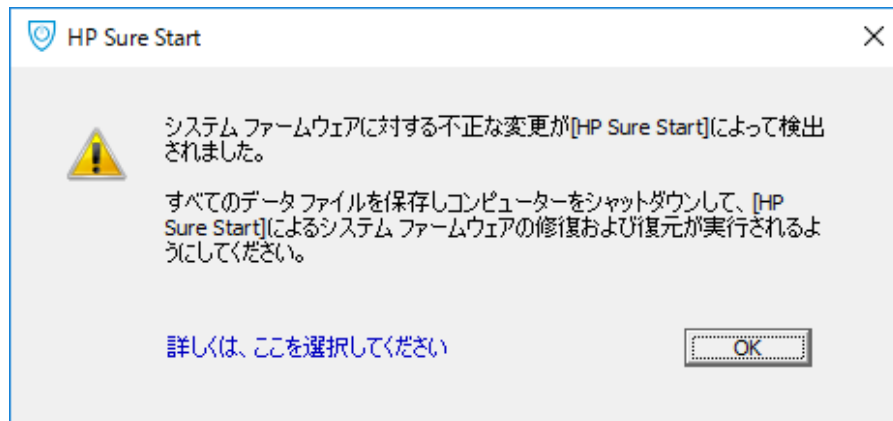


図 4-2-2-① 検知時のポップアップ画面

- HP Sure Start の通知機能について

HP Sure Start はユーザには見えない設定になっており、HP Sure Start が問題を特定した場合、管理者側で特別な操作を実施することなくリカバリ操作は自動的に行われます。

また、重大なイベントが検出された場合や処置がとられた場合、HP Sure Start は、次の起動時に Windows の通知で警告メッセージを表示します。

※Windows 通知を表示するには、HP Notifications ソフトウェアが別途必要になりますのでご注意ください。

- HP Sure Start のリカバリ

不正な変更を検出したメッセージを確認した後、再起動を行うと HP Sure Start が自動で BIOS の修復を実施します。（図 4-2-2-②）

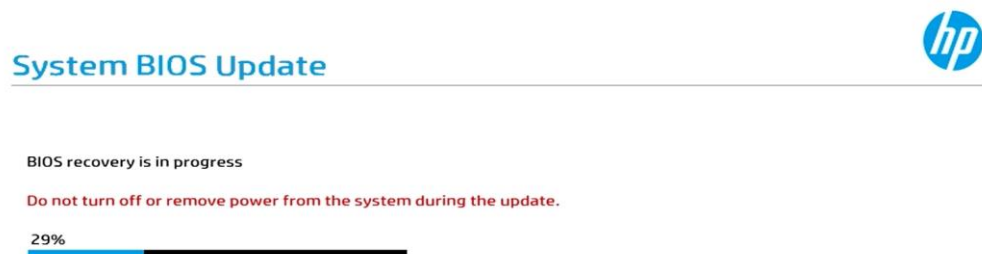


図 4-2-2-② BIOS 自動修復画面

4.2.3 HP Secure Erase 機能

本章では、ハードディスクや SSD のデータを完全消去する HP Secure Erase の機能をリモートから実行する操作手順を記載します。

- ① ブラウザにてインテル®EMA サーバの DNS 名を入力し、インテル®EMA へ接続（URL:https://[インテル®EMA サーバの DNS 名]）し、インテル®EMA サーバ作成時に設定した user name と Password を入力、Log In ボタンをクリックしログインします。（図 4-2-3-①）

※「テナント管理者」または「エンドポイント管理者」権限が設定されているユーザでログインします。

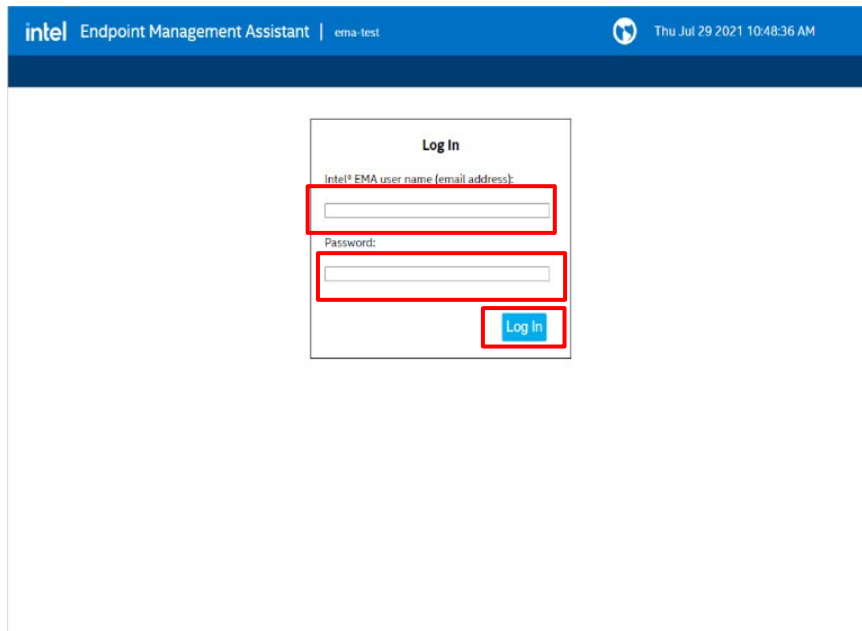


図 4-2-3-① ログイン画面

- ② Overview 画面が表示されるので、左側のメニューから「Endpoints」を選択します。（図 4-2-3-②）

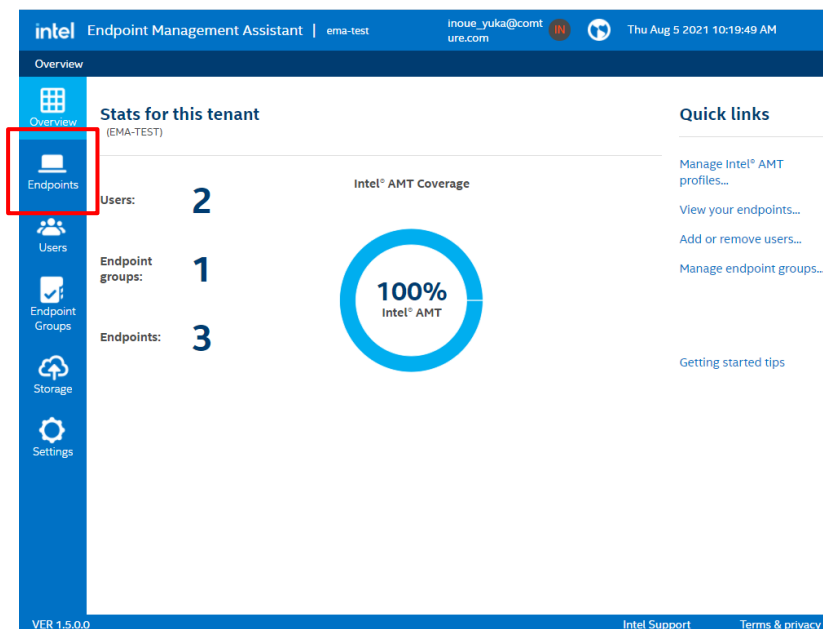


図 4-2-3-② ログイン後のトップ画面

- ③ 「Load all Endpoints」をクリックします。（図 4-2-3-③）

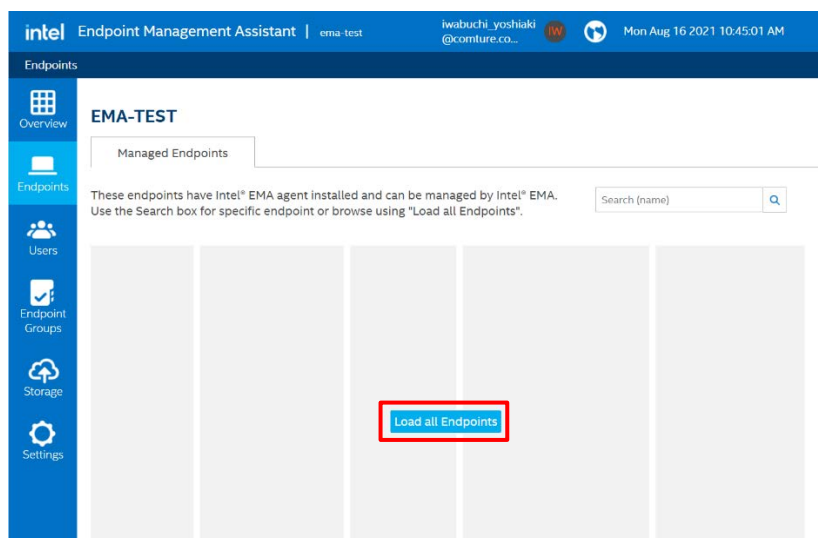


図 4-2-3-③ Endpoint 選択画面

- ④ ハードディスクまたは SSD のデータを完全消去したいエンドポイント（クライアント PC）の右側にある「view」をクリックします。（図 4-2-3-④）

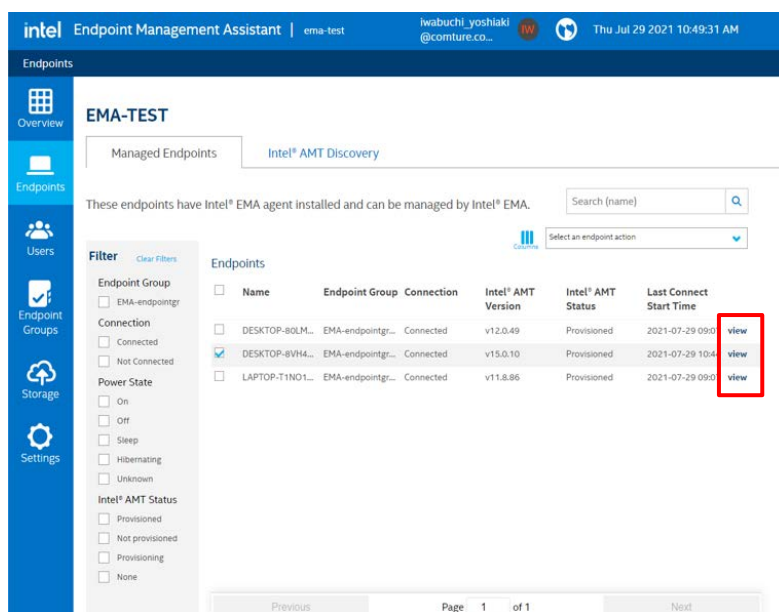


図 4-2-3-④ Endpoint 選択画面

- ⑤ General タブの画面の右側にある「CIRA Connected」であることを確認した後、「Hardware Manageability」タブを選択します。（図 4-2-3-⑤）

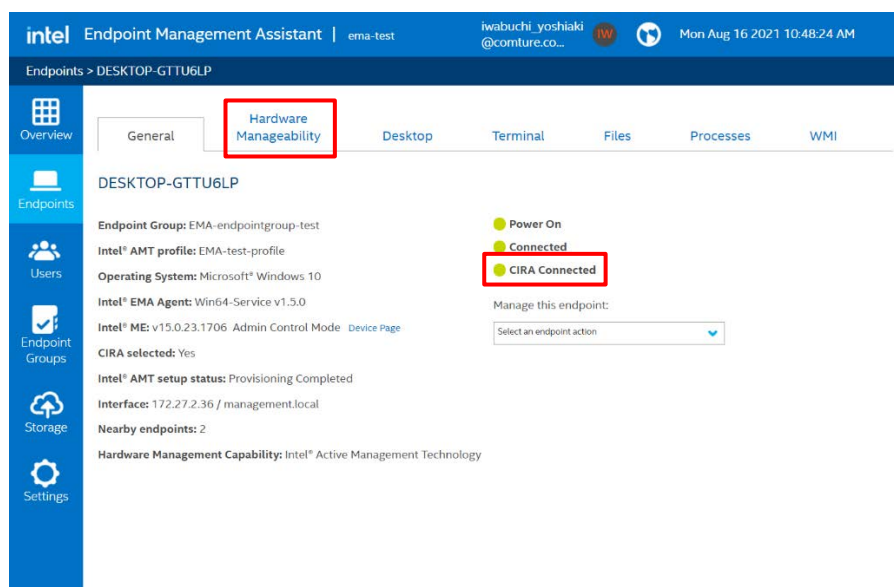


図 4-2-3-⑤ Endpoint 状態確認画面

⑥ 「Remote Desktop」をクリックします。(図 4-2-3-⑥)

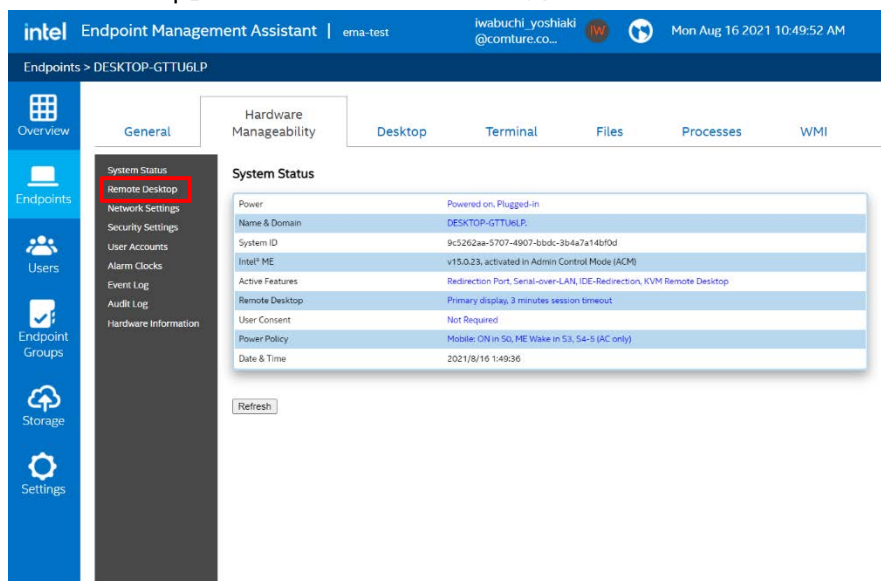


図 4-2-3-⑥ Hardware Manageability 詳細画面

⑦ 「Connect」ボタンをクリックします。(図 4-2-3-⑦)

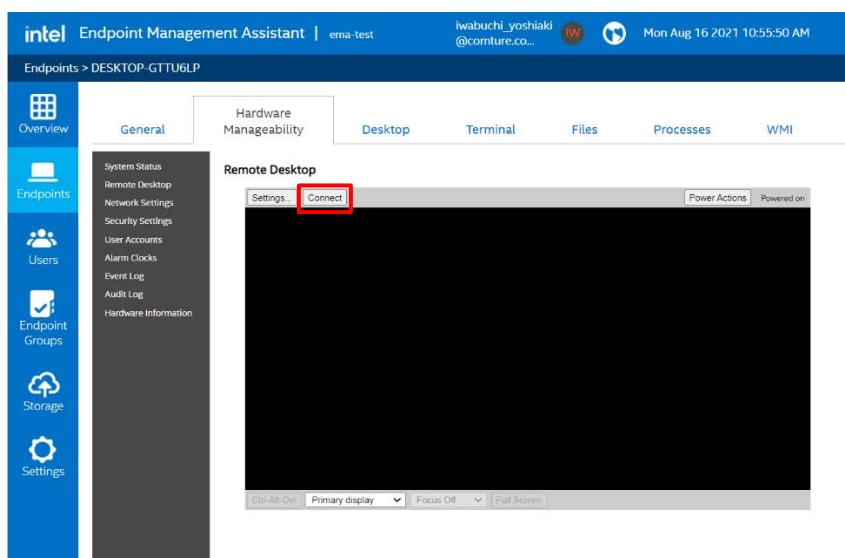


図 4-2-3-⑦ Remote Desktop 画面

- ⑧ 電源の状態に合わせて BIOS 画面の画面を起動させます。(または再起動させます)
- (ア) エンドポイント (クライアント PC) の電源が OFF の場合、「Power Actions」→「Power Up to BIOS」を選択します。(図 4-2-3-⑧)

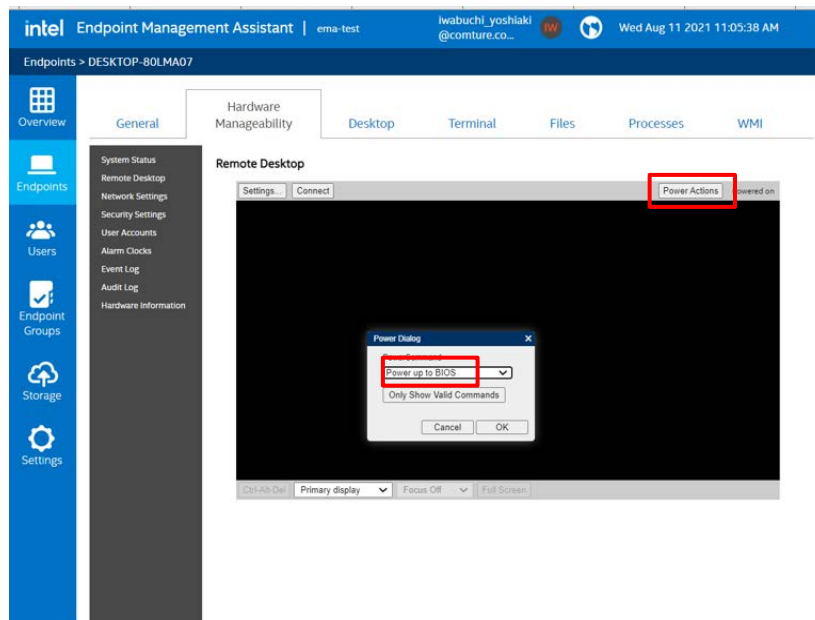


図 4-2-3-⑧ 電源状態が電源 OFF の場合の操作画面

- (イ) エンドポイント (クライアント PC) が電源 ON の場合、「Power Actions」→「Reset to BIOS」を選択します。(図 4-2-3-⑨)

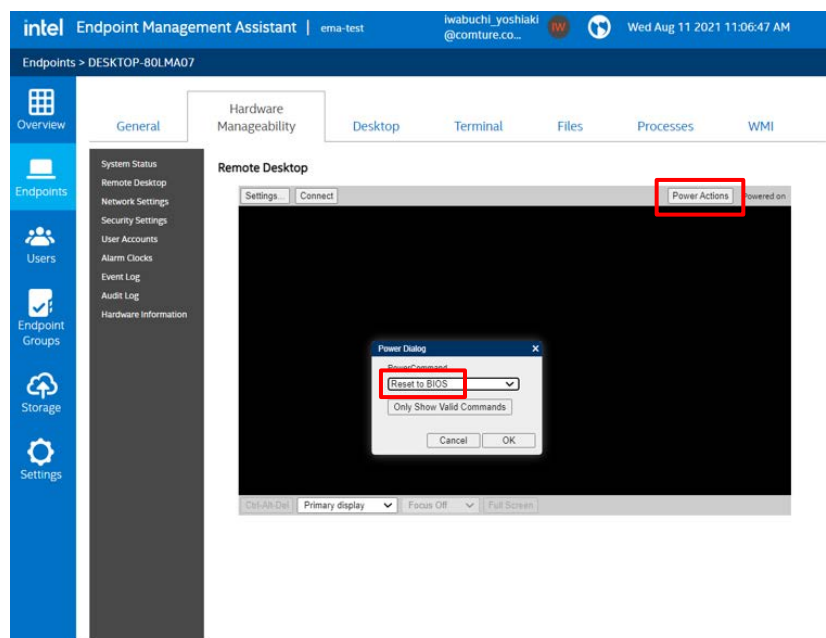


図 4-2-3-⑨ 電源状態が電源 ON の場合の操作画面

- ⑨ BIOS 画面（スタートアップメニュー画面）が起動したことを確認します。（図 4-2-3-⑩）

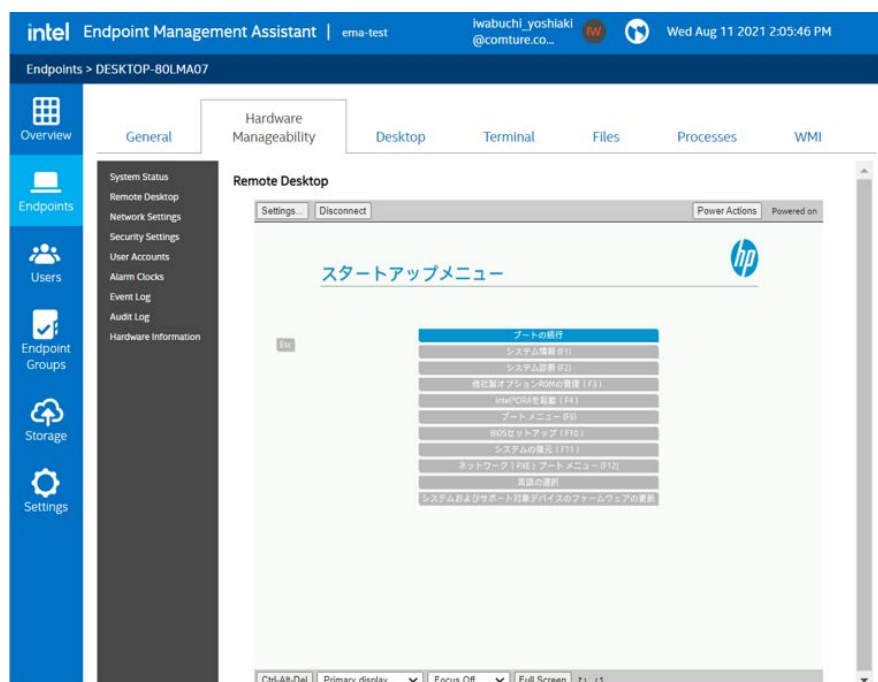


図 4-2-3-⑩ HP スタートアップメニュー画面

- ⑩ スタートアップメニューから「BIOS セットアップ（F10）」を選択します。（図 4-2-3-⑪）

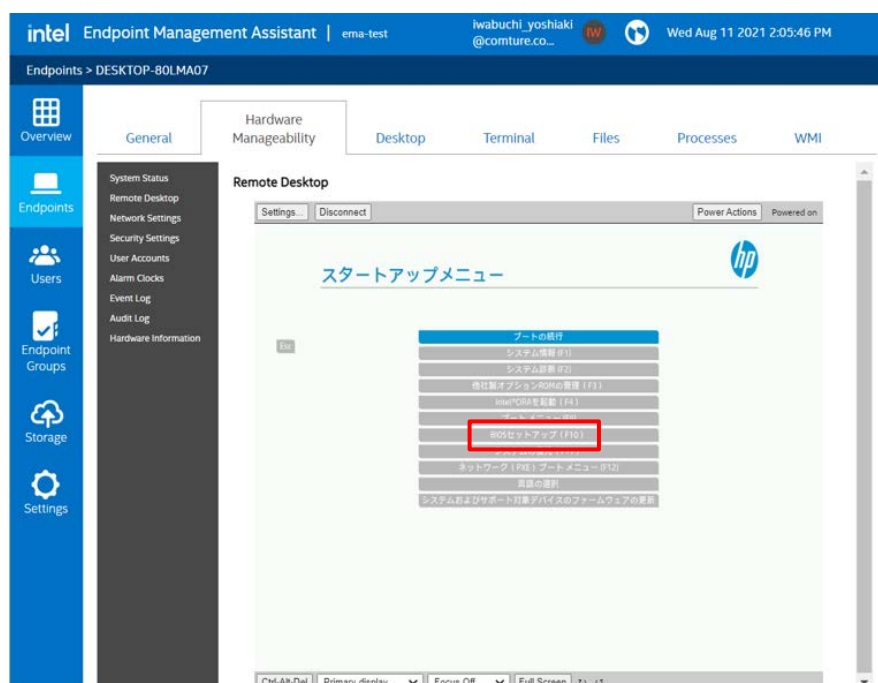


図 4-2-3-⑪ HP スタートアップメニュー選択画面

- ⑪ 「セキュリティ」タブを選択し、「ハードドライブユーティリティメニュー」から「セキュリティ保護された消去」をクリックします。(図 4-2-3-⑫)

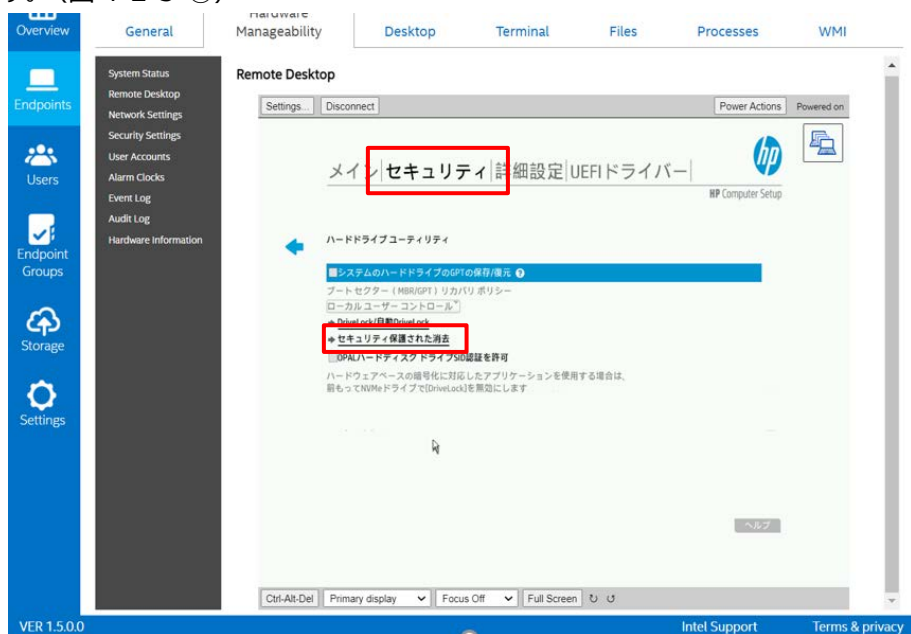


図 4-2-3-⑫ セキュリティタブ画面

- ⑫ 消去したいハードドライブをクリックします。(図 4-2-3-⑬)

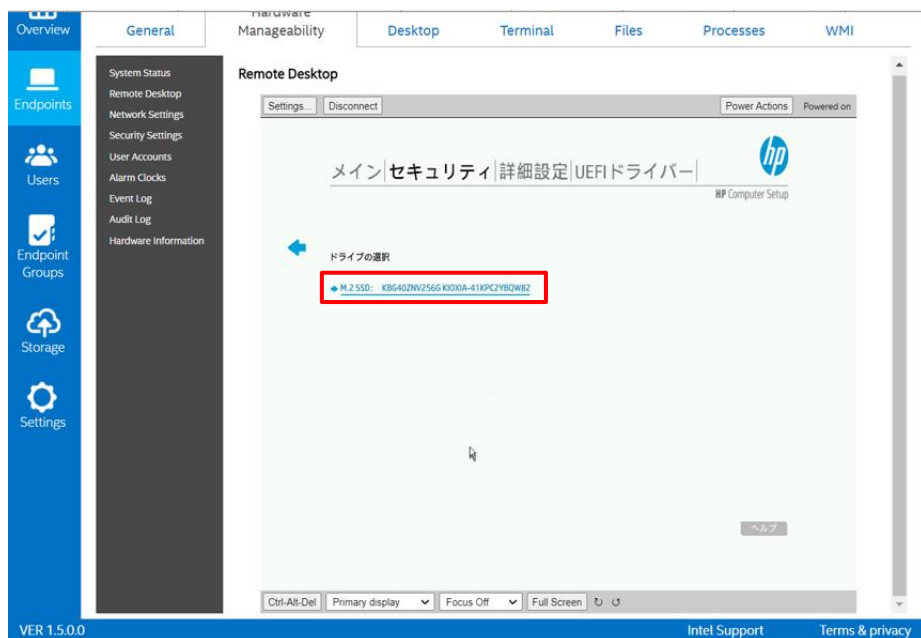


図 4-2-3-⑬ ドライブ選択画面

- ⑬ 以下のような画面が表示されるので、「続行」をクリックします。（図 4-2-3-⑭）

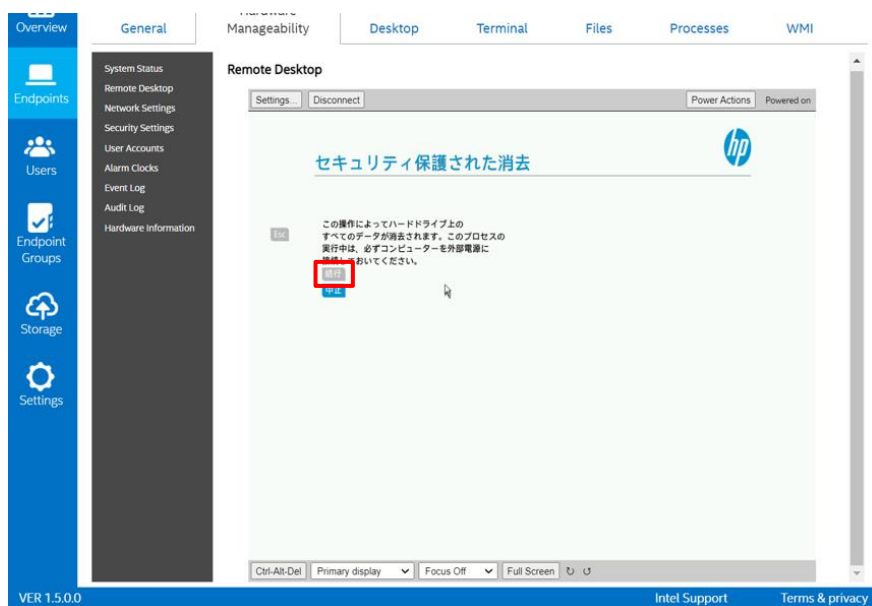


図 4-2-3-⑭ ドライブ選択画面

- ⑭ 以下の画面が表示された場合は「続行」をクリックします。（図 4-2-3-⑮）

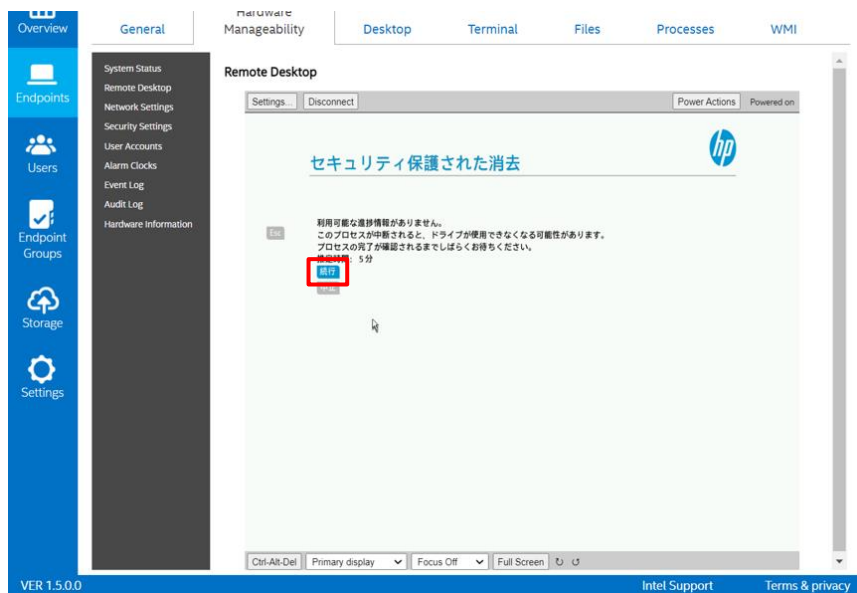


図 4-2-3-⑮ プロセス完了待機画面

- ⑮ 以下のように削除中の画面が表示されます。(図 4-2-3-⑮)

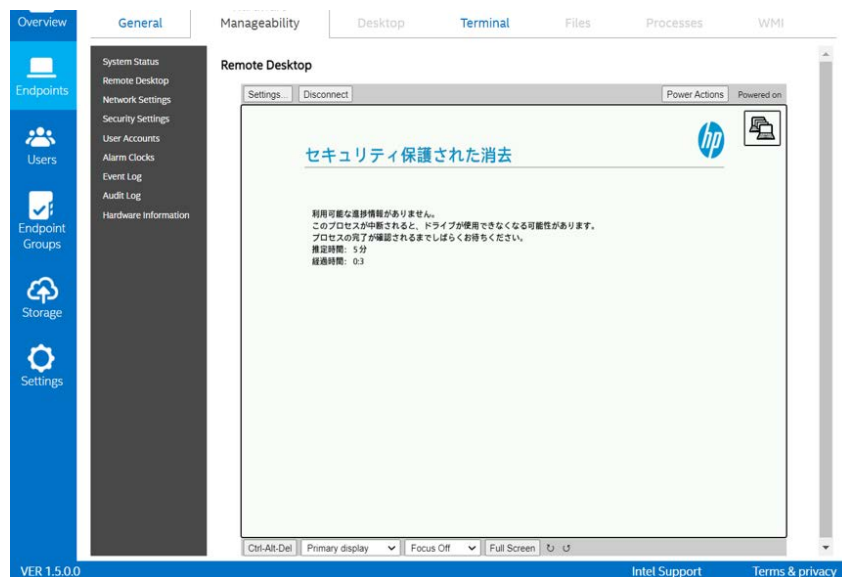


図 4-2-3-⑮ データ削除画面

- ⑯ 画面に「セキュリティ保護された消去が完了しました。」とメッセージが表示されることを確認し、「続行」をクリックします。(図 4-2-3-⑯)

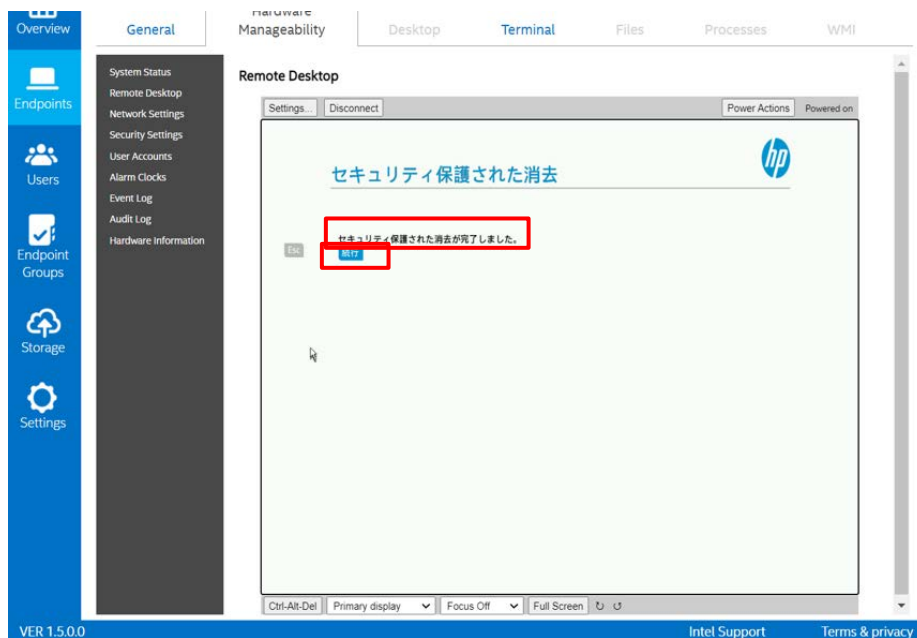


図 4-2-3-⑯ データ削除完了画面

- ⑰ 3回 Esc キーを押下すると、以下のように画面が表示されますので、「変更を保存しますか？」質問に対して「はい」ボタンをクリックします。（図 4-2-3-⑱）

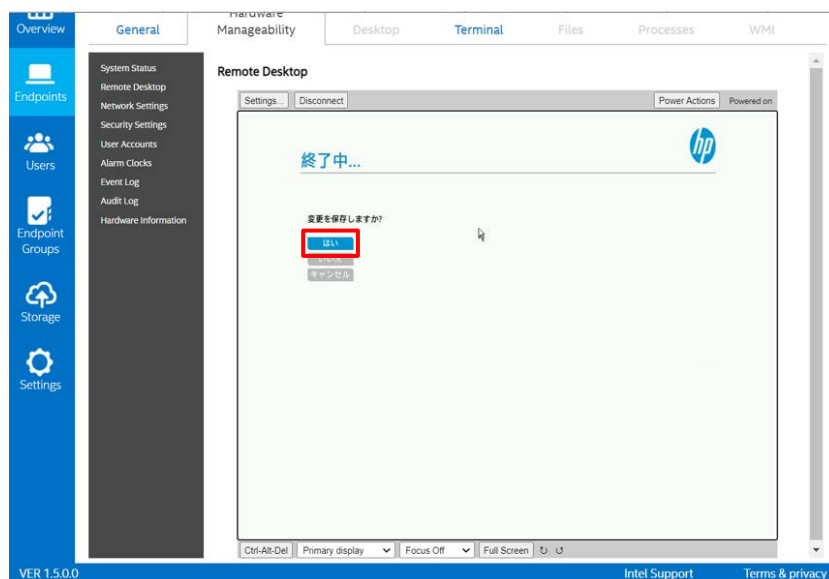


図 4-2-3-⑱ 終了画面

- ⑱ 終了後、自動で再起動され、OS が起動しないことを確認します。（図 4-2-3-⑲）

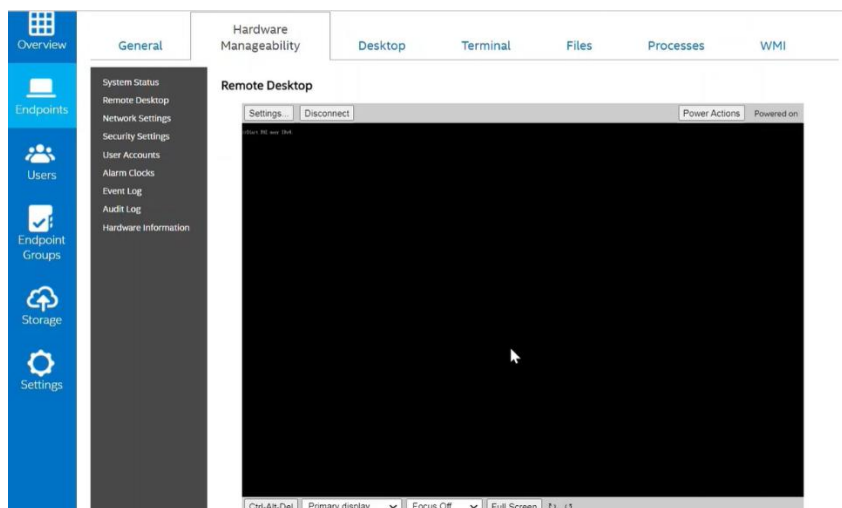


図 4-2-3-⑲ OS 起動エラー画面

4.2.4 HP Sure Recover 機能

本章ではインターネット接続経由で OS イメージ（OS + デバイスドライバー）をインストールする HP Sure Recover 機能をリモートから実行する手順について記載します。

◆本作業に対する注意事項

・本作業はエンドポイント（クライアント PC）が HP Sure Recover に対応かつ有線 LAN 接続されていることが条件になります。エンドポイント（クライアント PC）に有線 LAN 接続のインターフェースが無い場合は、別途、ドッキングステーション（※ 1）が必要となります。

※ 1 ノート PC に接続して機能拡張などを行う機器

●ドッキングステーション製品一覧は以下 URL をご参照下さい。

https://jp.ext.hp.com/directplus/keyword/main_docstation/

- ① ブラウザにてインテル®EMA サーバの DNS 名を入力し、インテル®EMA へ接続（URL: [https://\[インテル®EMA サーバの DNS 名\]](https://[インテル®EMA サーバの DNS 名])）し、インテル®EMA サーバ作成時に設定した user name と Password を入力、Log In ボタンをクリックしログインします。（図 4-2-4-①）

※「テナント管理者」または「エンドポイント管理者」権限が設定されているユーザでログインします。

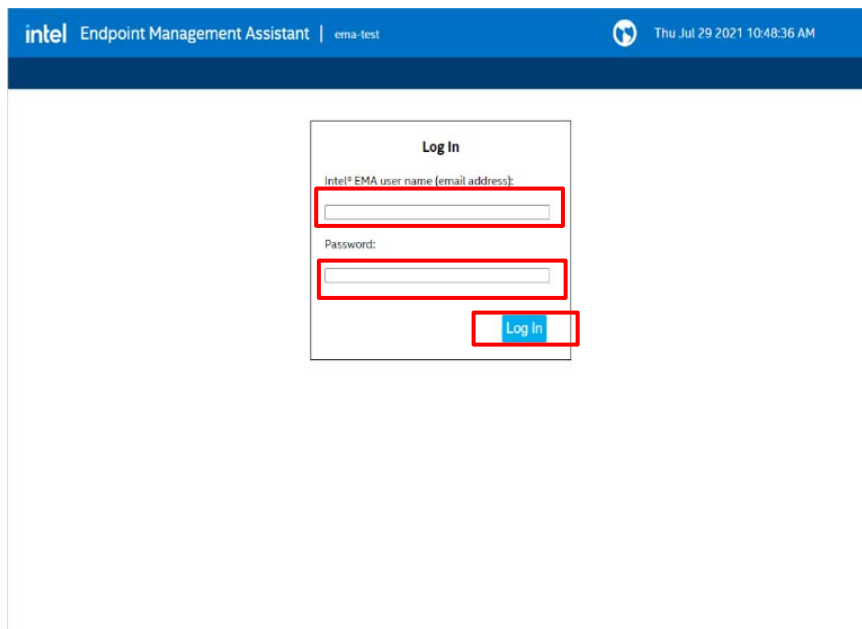


図 4-2-4-① ログイン画面

- ② Overview 画面が表示されますので、左側のメニューから「Endpoints」を選択します。（図 4-2-4-②）

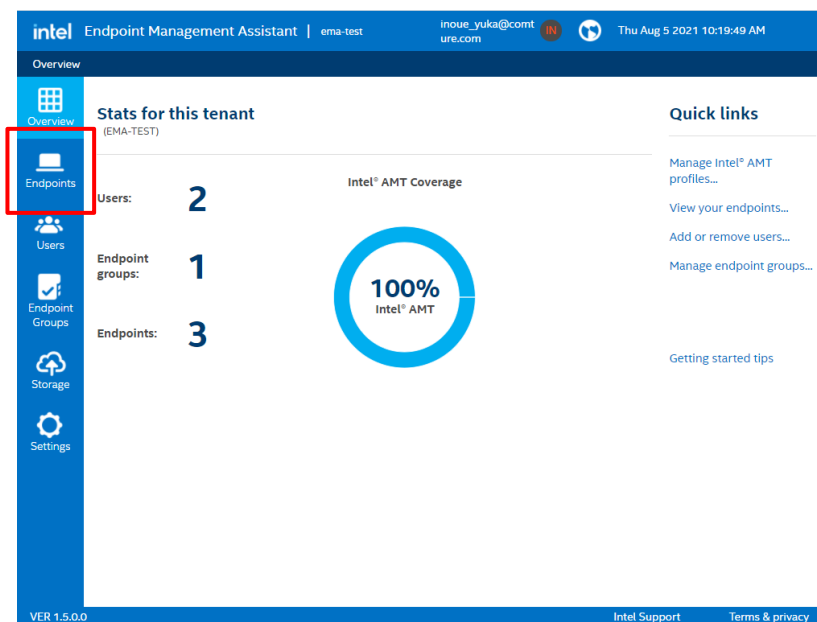


図 4-2-4-② ログイン後のトップ画面

- ③ 「Load all Endpoints」をクリックします。（図 4-2-4-③）

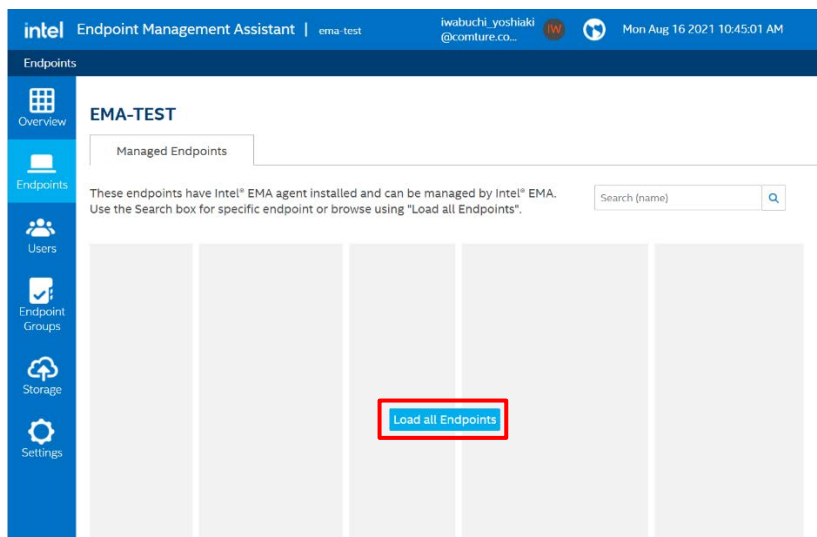


図 4-2-4-③ Endpoint 選択画面

- ④ 工場出荷状態にしたいエンドポイント（クライアント PC）の右側にある「view」をクリックします。（図 4-2-4-④）

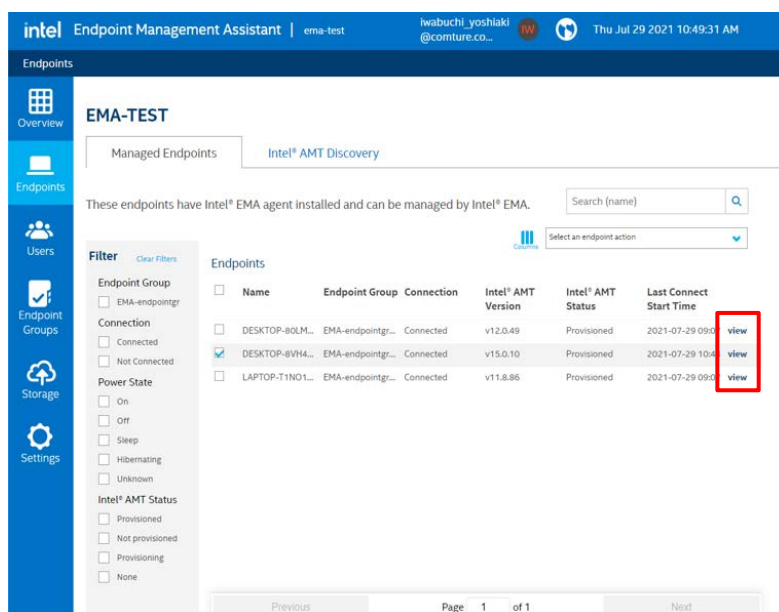


図 4-2-4-④ Endpoint 選択画面

- ⑤ General タブの右側にある「CIRA Connected」であることを確認した後、「Hardware Manageability」タブを選択します。（図 4-2-4-⑤）

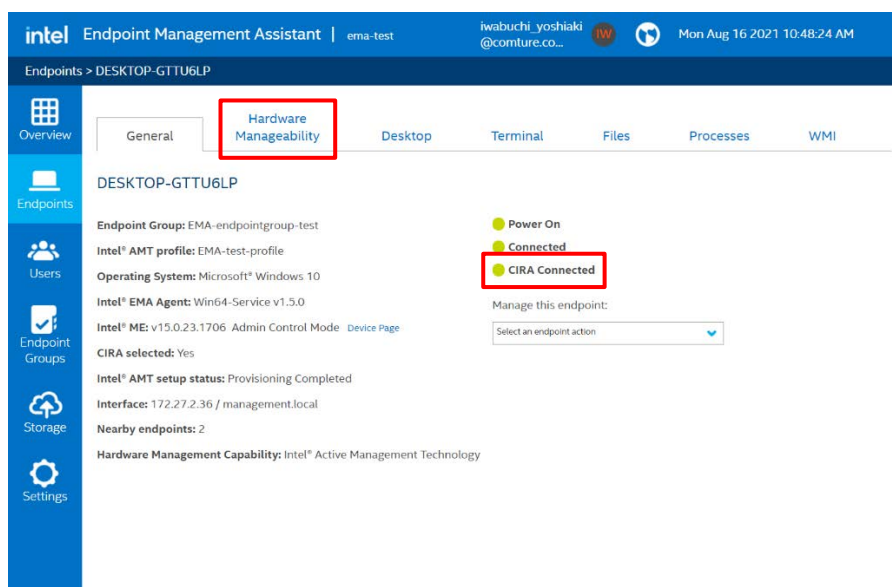


図 4-2-4-⑤ Endpoint 状態確認画面

⑥ 「Remote Desktop」をクリックします。(図 4-2-4-⑥)

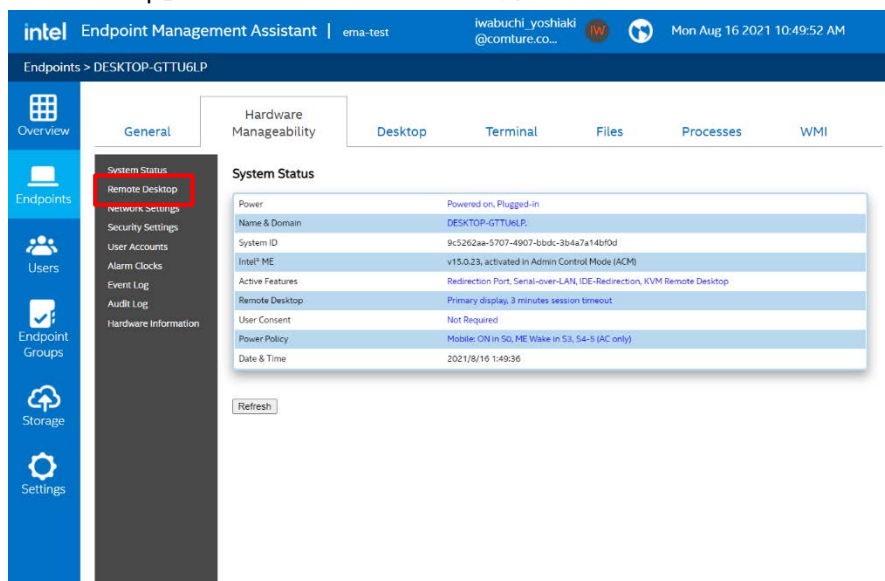


図 4-2-4-⑥ Hardware Manageability 詳細画面

⑦ 画面左上ある「Connect」ボタンをクリックします。(図 4-2-4-⑦)

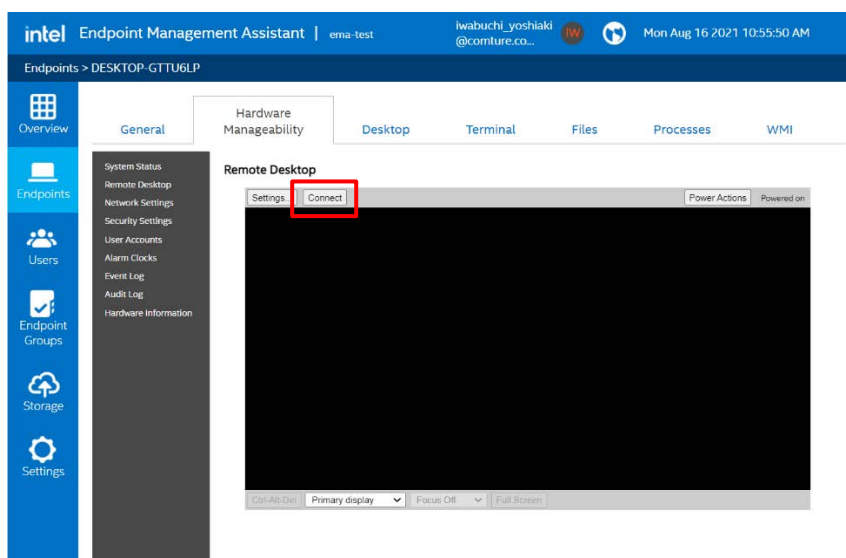


図 4-2-4-⑦ Remote Desktop 画面

- ⑧ エンドポイント（クライアント PC）は電源 OFF の状態から BIOS 画面を起動させるために、画面右上の「Power Actions」ボタンをクリックし「Power UP」を選択します。（（図 4-2-4-⑧））

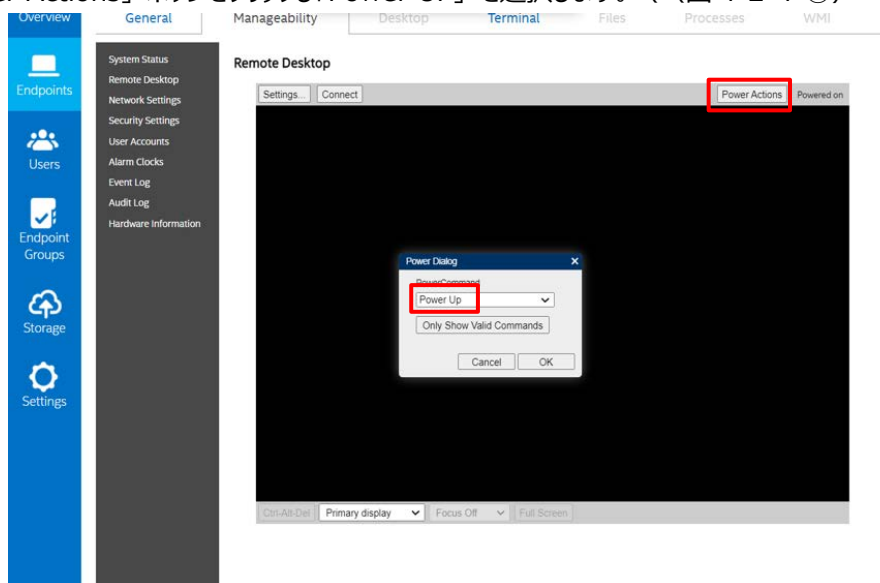


図 4-2-4-⑧ PC 起動操作画面

- ⑨ HP ロゴ表示時に「F11」キーを押下します。（図 4-2-4-⑨）

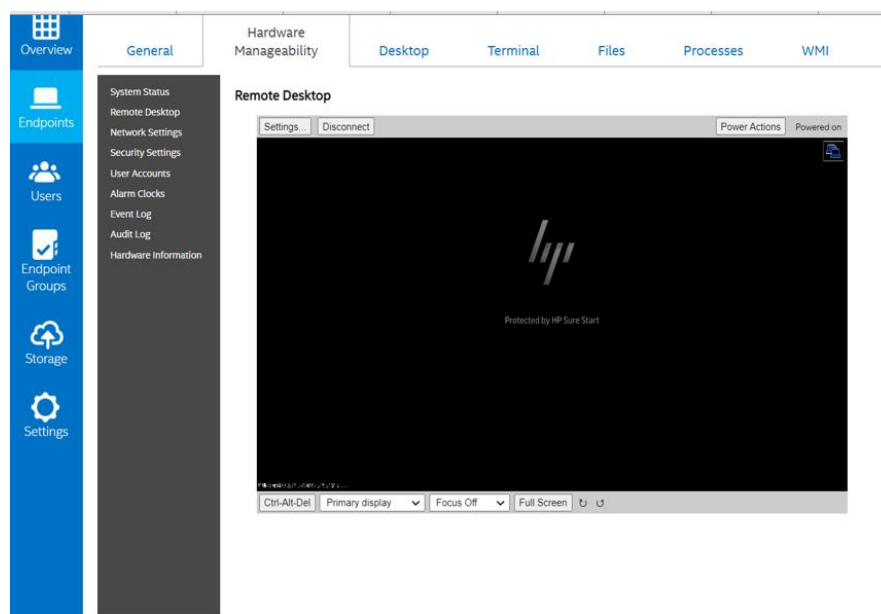


図 4-2-4-⑨ HP ロゴ表示画面

⑩ 「ネットワークからの復元」をクリックします。(図 4-2-4-⑩)

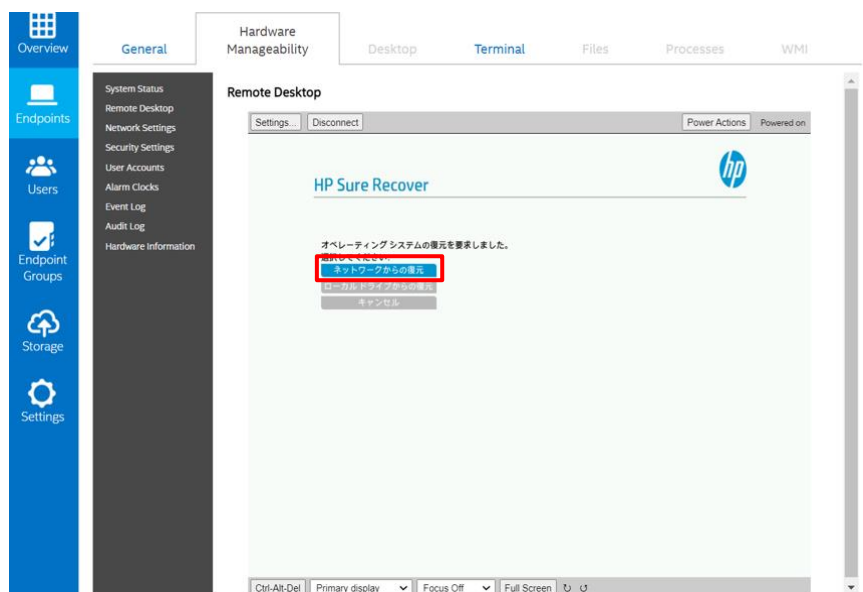


図 4-2-4-⑩ ネットワークからの復元選択画面

⑪ リカバリソフトウェアのダウンロードが開始されます。(図 4-2-4-⑪)

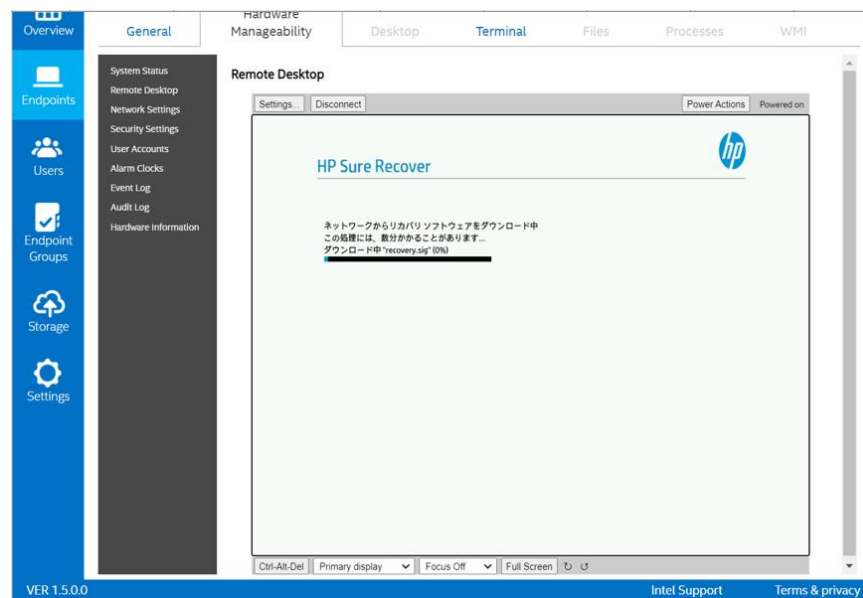


図 4-2-4-⑪ リカバリソフトウェアのダウンロード画面

- ⑫ OS インストールに必要なデータと OS のイメージやドライバなどがダウンロードされ、ダウンロード完了すると、再起動を実施するポップアップ画面が表示され、自動的に再起動が実施されます。（図 4-2-4-⑫・⑬・⑭）

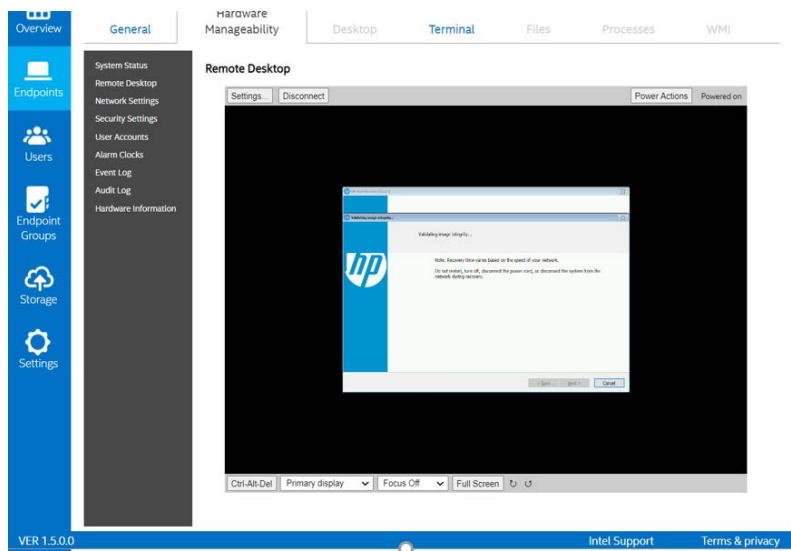


図 4-2-4-⑫ データダウンロード画面①

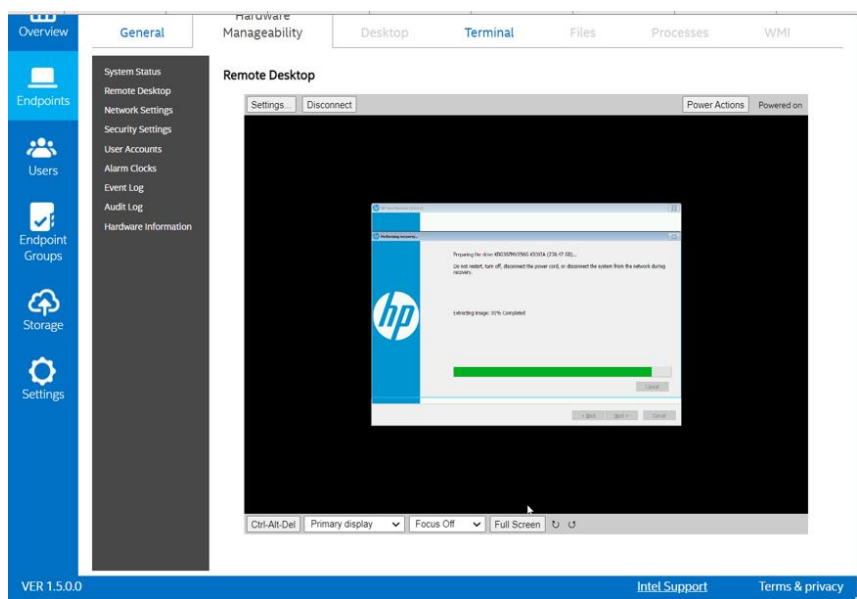


図 4-2-4-⑬ データダウンロード画面②

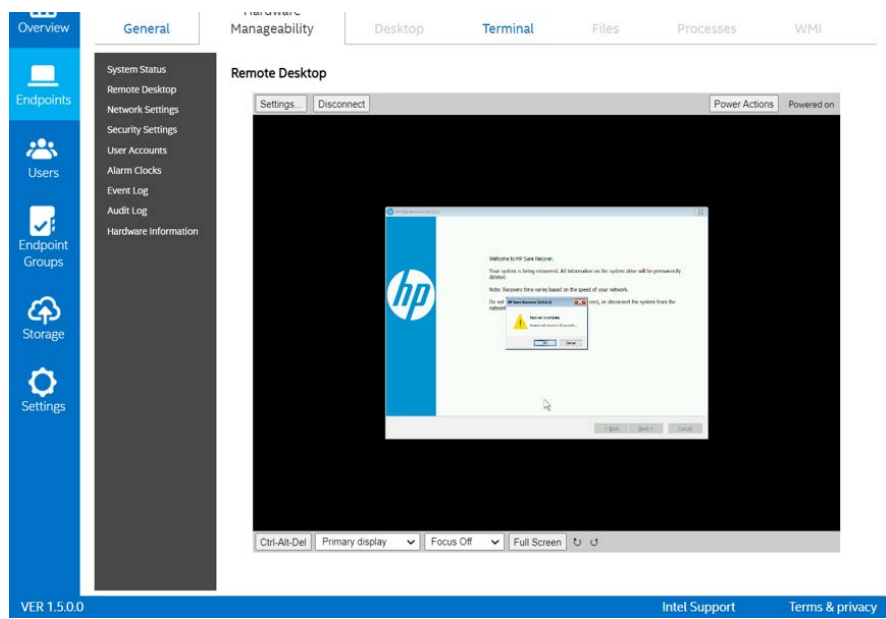


図 4-2-4-⑭ データダウンロード画面③

- ⑬ 再起動を実施すると OS セットアップ画面が表示されます。(図 4-2-4-⑮)

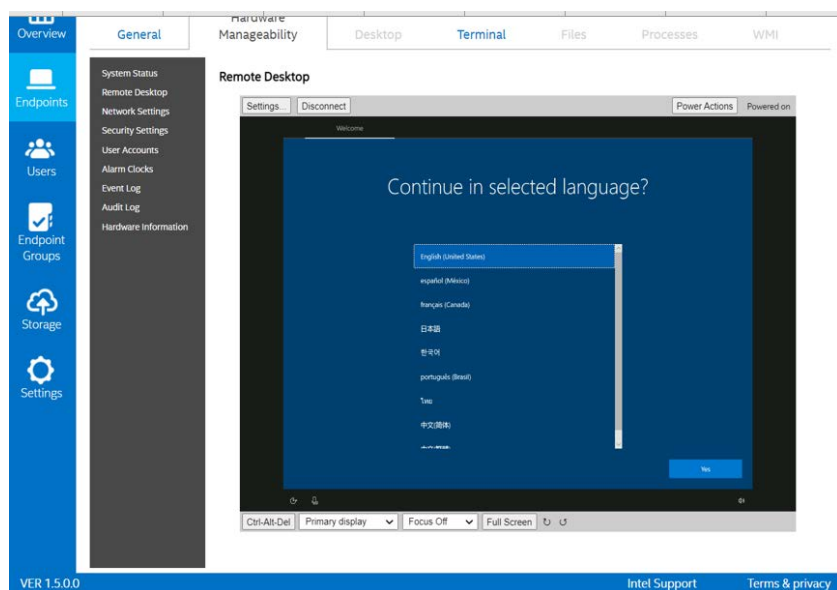


図 4-2-4-⑮ OS セットアップ画面

- ⑭ Continue in selected language?画面が表示されるので、「日本語」を選択し、「はい」ボタンをクリックします。(図 4-2-4-⑯)

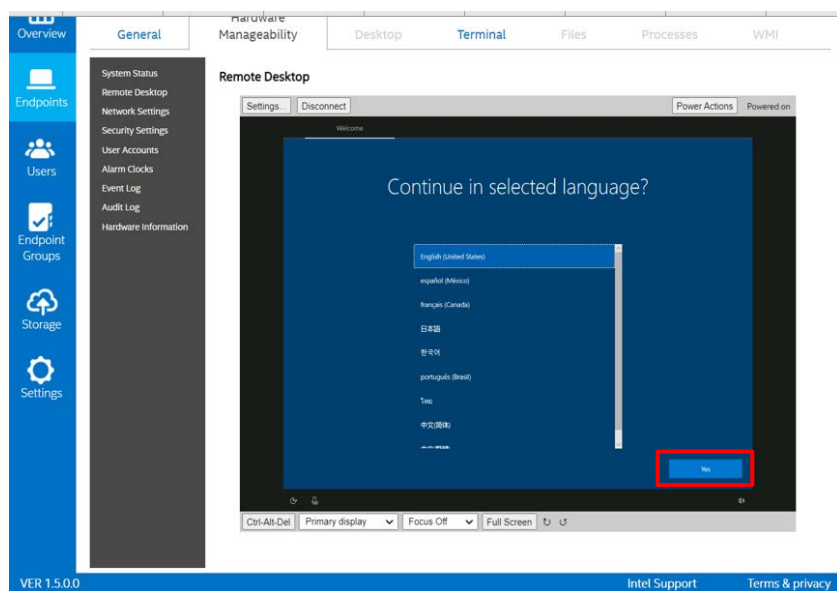


図 4-2-4-⑯ 言語設定画面

- ⑮ お住まいの地域はこちらでよろしいですか？画面が表示されるので、「日本」を選択し、「はい」を選択します。（図 4-2-4-⑰）

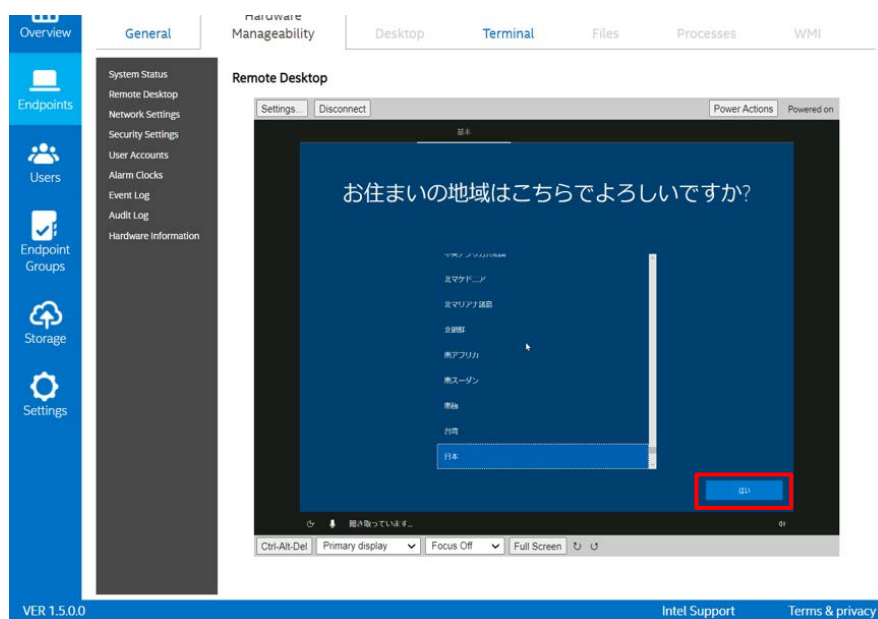


図 4-2-4-⑰ 地域設定画面

- ⑩ キーボードレイアウトを選択して、「はい」を選択します。(図 4-2-4-⑩)
- ※通常は「Microsoft IME」を選択します。

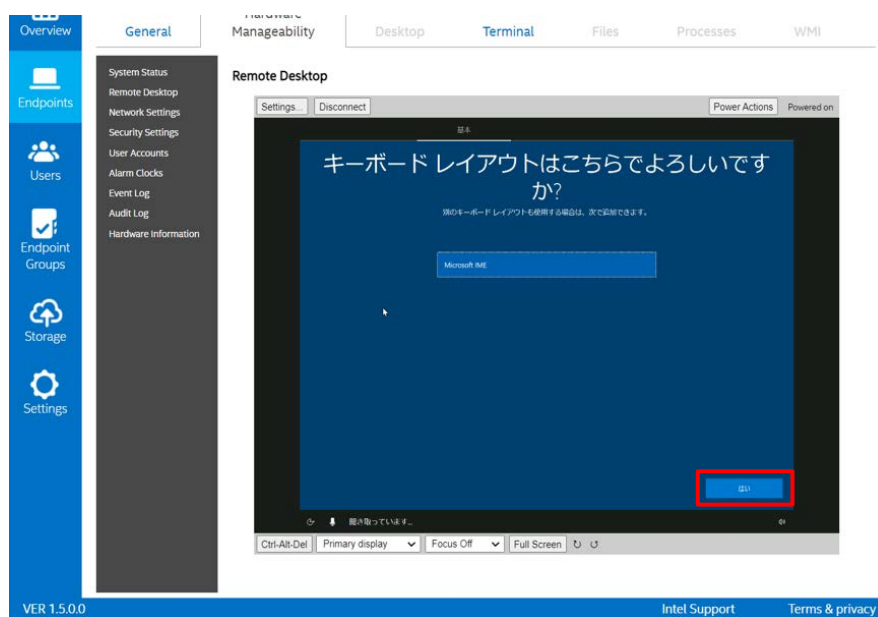


図 4-2-4-⑱ キーボードレイアウト設定画面①

- ⑰ 以下の画面が表示されるので、「レイアウトの追加」を選択し、「日本語」を追加します。（図 4-2-4-⑰）

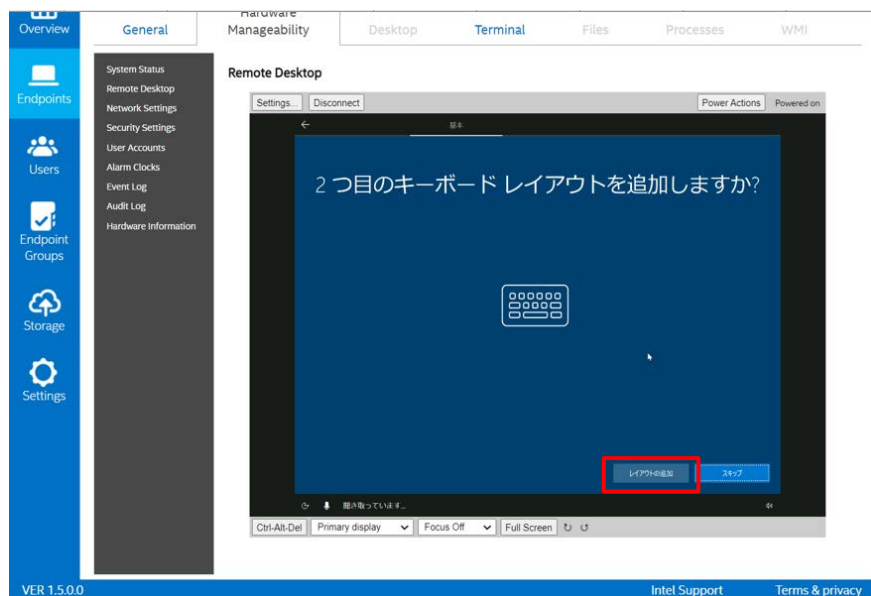


図 4-2-4-⑰ キーボードレイアウト設定画面②

- ⑱ Windows10 使用許諾契約画面が表示されるので、「同意」をクリックします。（図 4-2-4-⑱）

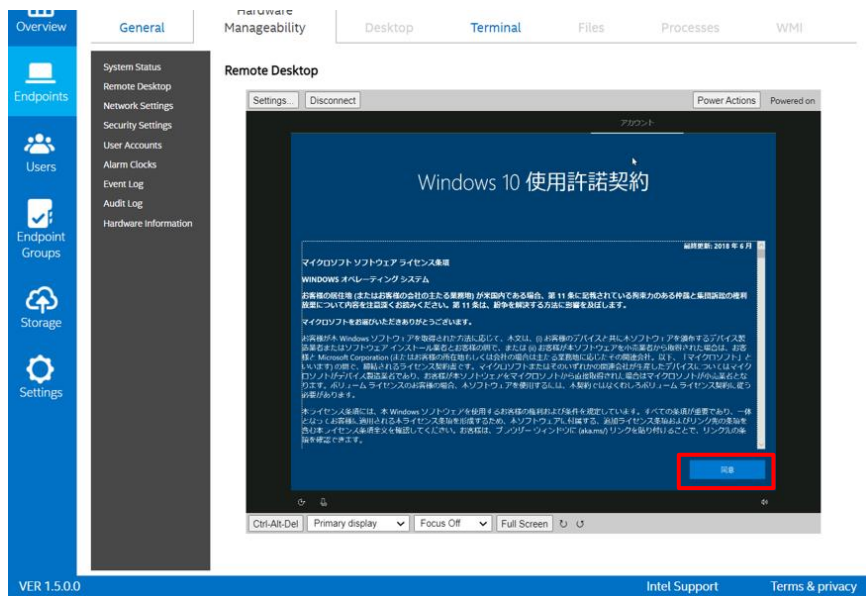


図 4-2-4-⑱ Windows10 使用許諾契約画面

- ⑱ ご使用の環境によって設定方法が変わりますので任意で以下の条件に合った環境を選択して「次へ」ボタンをクリックします。(図 4-2-4-⑱)

個人用に設定・・・個人的に使う PC のための設定します。

組織用に設定・・・「〇〇@組織名.co.jp」などの Office 365 や Microsoft 365、Microsoft Azure の Azure AD、Windows Server などで管理されているアカウントを使う場合に設定します。

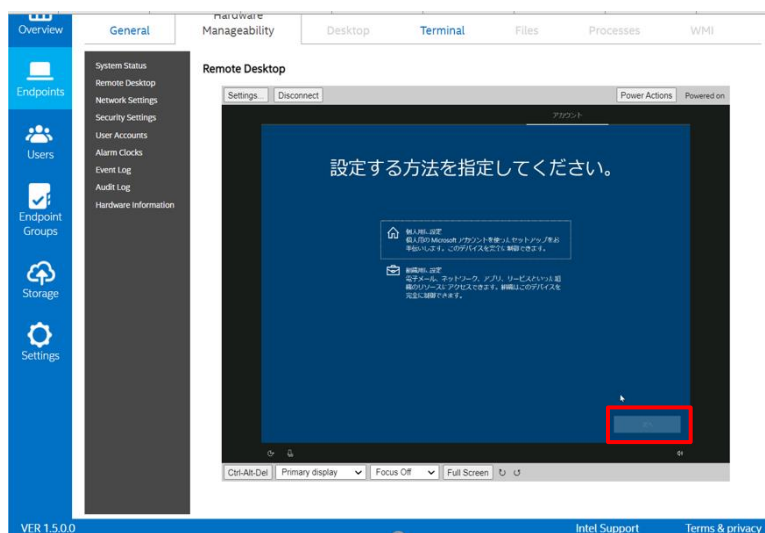


図 4-2-4-⑱ アカウント設定画面

- ⑳ 使用するメールアドレス、パスワード、秘密のパスワードなどを設定します。(図 4-2-4-㉔)

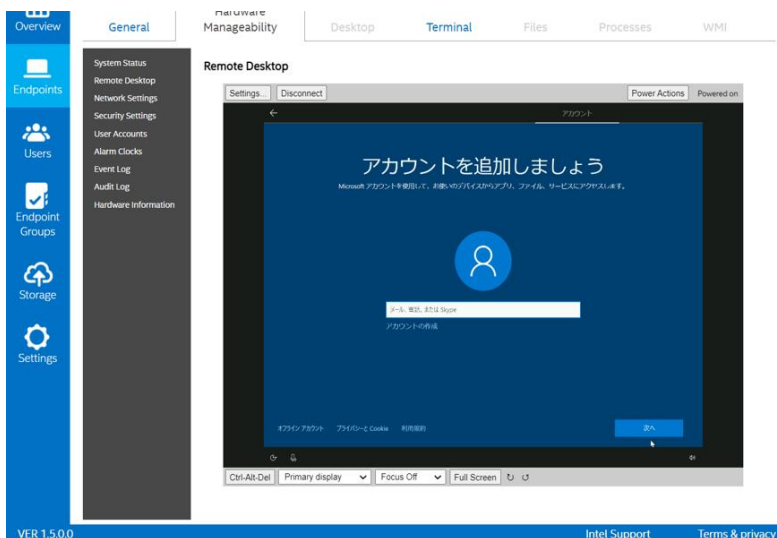


図 4-2-4-㉔ アカウント設定画面

② Windows Hello(顔認証、指紋認証)が不要であれば「今はスキップ」をクリックします。

※後から変更できます。(図 4-2-4-②)

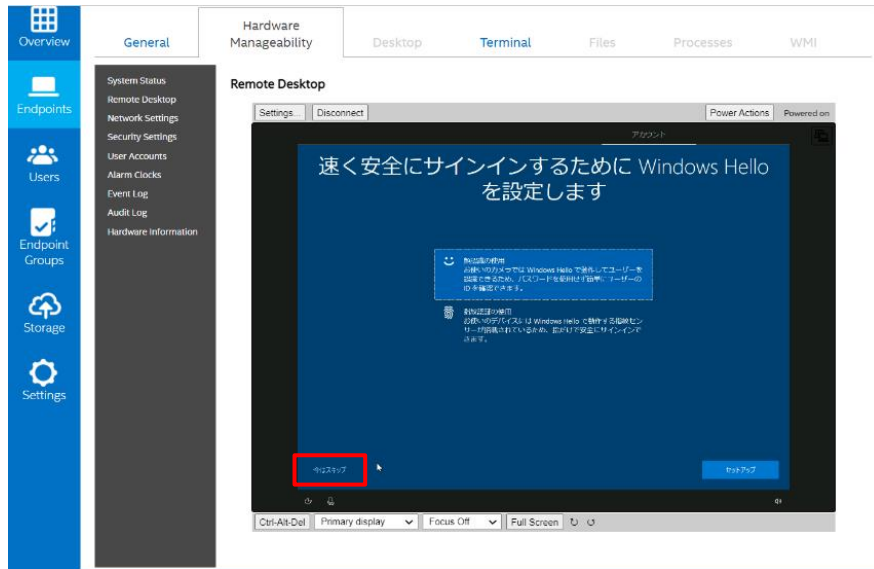


図 4-2-4-② Windows Hello 設定画面

② 使用履歴を他のデバイスでも使えるようにする設定となりますので、環境に合わせて「はい」または「いいえ」をクリックします。※後から変更できます。(図 4-2-4-④)

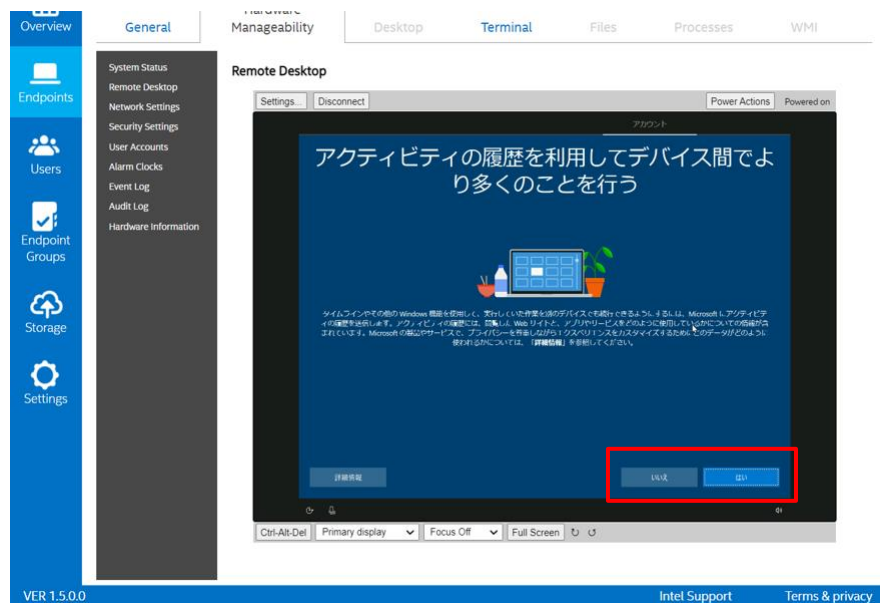


図 4-2-4-④ 他デバイス使用履歴設定画面

② 以下の画面が表示されるので、デジタルアシスタント（Cortana : コルタナ）を利用する場合は「同意」ボタンをクリックし、不要であれば「拒否」ボタンをクリックします。（図 4-2-4-②）

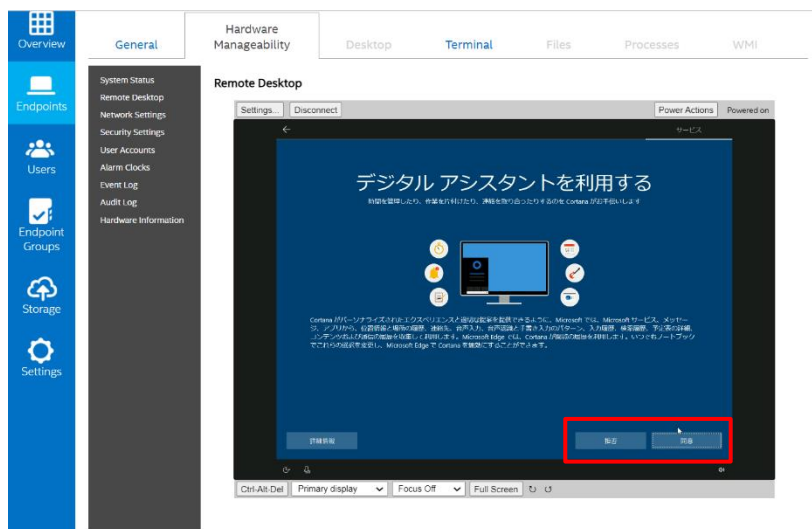


図 4-2-4-② Cortana 設定画面

③ 以下の画面が表示されるので、「同意する」をクリックします。（図 4-2-4-③）

※ご使用の環境に合わせて各設定のカスタマイズが可能です。通常はそのまま「同意する」で問題ありません。

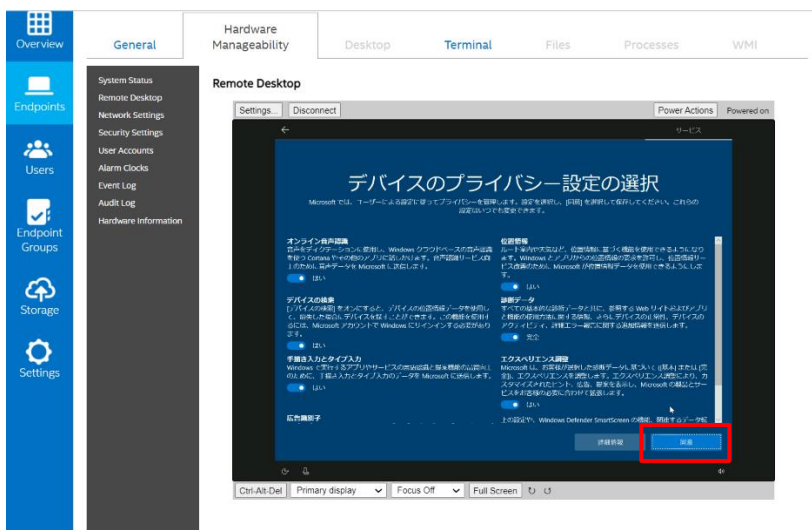


図 4-2-4-③ デバイスのプライバシー設定の選択画面

- ⑳ 全て設定完了したら、エンドポイント（クライアント PC）は起動準備の画面が表示されます。（図 4-2-4-㉑）

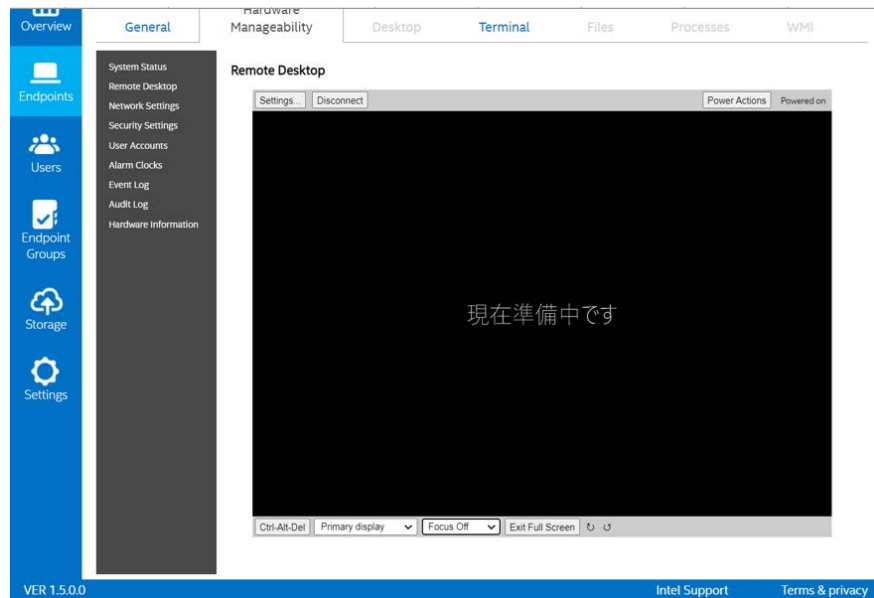


図 4-2-4-㉑ PC 起動準備画面

- ㉒ デスクトップ画面が表示されることを確認します。（図 4-2-4-㉓）

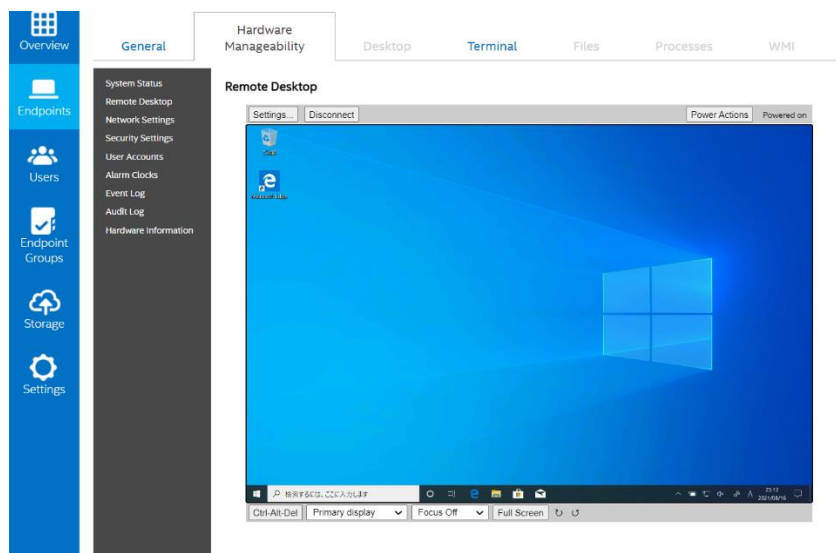


図 4-2-4-㉓ デスクトップ画面