

Intel® Unite™ ソリューション

保護されたゲストアクセス用プラグインガイド



法務情報および免責事項、著作権

本資料に記載されたすべての情報は、予告なく変更されることがあります。インテル® 製品の最新の仕様およびロードマップをご希望の場合は、インテルの担当社員までご連絡ください。

インテル® テクノロジーの機能と利点はシステム構成によって異なり、対応するハードウェアやソフトウェア、またはサービスの有効化が必要となる場合があります。実際の性能はシステム構成によって異なります。絶対的なセキュリティーを提供できるコンピューター・システムはありません。詳細については、各システムメーカーまたは販売店にお問い合わせいただくか、www.intel.co.jp を参照してください。

ここに記載されているインテル製品に関する侵害行為または法的分析に関連して、本書を使用または使用を促すことはできません。インテルに対し、ここで開示された内容を含む特許クレームについて非独占的かつロイヤルティー・フリーの実施権を許諾することに同意したものとみなされます。

本資料は、（明示されているか否かにかかわらず、また禁反言によるとよらずにかかわらず）いかなる知的財産権のライセンスを許諾するためのものではありません。

インテル® 製品には、エラッタと呼ばれる設計上の不具合が含まれている可能性があります。公表されている仕様とは異なる動作をする場合があります。現在確認済みのエラッタについては、インテルまでお問い合わせください。

インテルは、明示たると黙示たるとを問わず、商品性、特定の目的に対する適合性、法律違反のないこと、履行の過程、商取引上の取り扱いもしくは利用の慣例の黙示の保証を含むが、これらに限定しないすべての保証を否認します。

インテルは、本資料で参照している第三者のベンチマーク・データまたは Web サイトについて管理や監査を行っていません。本資料で参照している Web サイトを参照し、本資料で参照しているデータが正確かどうかを確認してください。

Intel、インテル、Intel ロゴ、Intel Unite は、アメリカ合衆国および / またはその他の国における Intel Corporation またはその子会社の商標です。

この文書はローカライズされることにより、一部の画像の表示が異なることがあります。

*その他の社名、製品名などは、一般に各社の表示、商標または登録商標です

© 2016 Intel Corporation.無断での引用、転載を禁じます。



1.	はじめに	4
1.1	対象	4
1.2	概要	4
1.3	推奨されているセキュリティー・コントロール.....	6
2.	プラグインのインストールとコンポーネント.....	7
2.1	プラグイン・コンポーネント	7
2.2	プラグインのインストール.....	7
2.2.1	エンタープライズ・バージョン.....	8
	証明書ハッシュの値の取得.....	8
	管理者 Web ポータルでプロファイルを作成する	10
	保護されたゲスト・アクセス・プラグインのレジストリー・キー	11
2.2.2	スタンドアロン・バージョン	12
3.	保護されたゲスト・アクセス・プラグインのフロー	13
4.	クライアント・デバイスでゲストアクセスを有効にする方法.....	14
	付録 A : ファイアウォールの例外.....	19
	付録 B : トラブルシューティング	20

□. はじめに

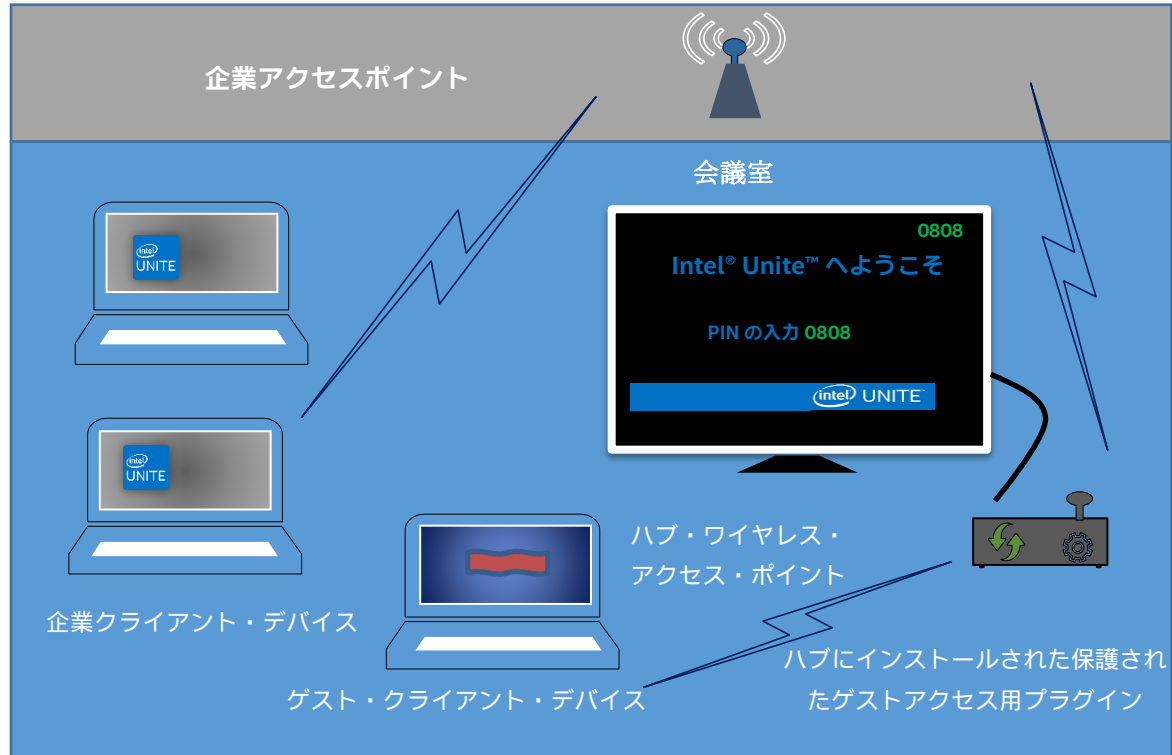
このドキュメントでは、Intel® Unite™ ソリューション上での保護されたゲストアクセス用 Intel® Unite™ プラグインのインストールおよび使用方法について説明します。

□.□ 対象

このドキュメントは、Intel® Unite™ ソフトウェアのインストールやビジネス向けゲストアクセスの有効化などアプリケーションへのオプション機能追加を担当する、企業環境内で作業を行う IT スタッフを対象としています。

□.□ 概要

保護されたゲストアクセス用 Intel® Unite™ プラグインを使用すると、ゲスト・クライアント・デバイスがエンタープライズ・ネットワークになくてもハブに接続できるようになります。これはなぜ可能かというと、ゲスト・クライアント・デバイスがクライアント・デバイス用の Intel® Unite™ アプリケーションを接続、ダウンロード、参加できるよう、ハブがアドホック/ホスト・ネットワーク (アクセスポイント) を作成するからです。



□.3 推奨されているセキュリティ・コントロール

IT 担当者が以下の推奨セキュリティ・コントロールに従うことを推奨します。

- ゲストアクセス実行中のハブのネットワーク・ブリッジをオフにします。
- Active Directory 環境では、ハブにアプリケーションとユーザーを制限するグループ・ポリシー・オブジェクト (GPO ポリシー) を設定します。
- 許可されていないトラフィックを制限するため、ゲスト・アクセス・マシンと企業接続の間にファイアウォールを導入します。
- 未使用のポートにファイアウォールが設定されていることを確認します。
- 許可されていない実行ファイルがゲスト・アクセス・マシンで実行されないよう、ソフトウェア・ベースのソリューション (McAfee* Application Control や Windows* AppLocker* など) を導入します。
 - McAfee* Application Control の詳細については、
<http://www.mcafee.com/us/products/application-control.aspx> にアクセスしてください。
 - Windows* AppLocker* の詳細については、
<https://technet.microsoft.com/itpro/windows/whats-new/whats-new-windows-10-version-1507-and-1511> にアクセスしてください。
- 許可されていない実行ファイルがゲスト・アクセス・マシンで実行されないよう、ハードウェアおよびソフトウェア・ベースのソリューション (Windows® 10 デバイスのデバイス ガード* など) を導入します。
 - デバイス ガード* の詳細については、<https://technet.microsoft.com/ja-jp/itpro/windows/keep-secure/device-guard-deployment-guide> にアクセスしてください。
- ネットワーク・ブリッジを無効にする方法：
 - [https://technet.microsoft.com/en-us/library/cc732103\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc732103(v=ws.10).aspx) (英語) にアクセスしてください。

□. プラグインのインストールとコンポーネント

□.□ プラグイン・コンポーネント

以下のコンポーネントは保護されたゲスト・アクセス・プラグインの一部です。

- ゲスト・アクセス・クライアント・プラグイン (dll)
 - これはハブによってロードされるプラグインです。CFCPlugin.dll で定義される機能を実装します。
- ゲスト・アクセス・サービス (Windows* サービス)
 - これはアドホック/ホスト・ネットワーク (アクセスポイント) の作成と構成を行う Windows* サービスです。GuestAccessClientPlugin.dll は、このサービスによって受信および処理されるコマンドを送信します。
- クライアント・ダウンロード・ページ
 - クライアント向け Intel® Unite™ アプリ v3.0 が必要です。アドホック・ネットワークをホストするハブを実行して接続するよう構成されている必要があります。ネットワークを作成したら、ダウンロードができるようになります。

□.□ プラグインのインストール

保護されたゲストアクセス用 Intel® Unite™ プラグインをインストールするには、管理者権限が必要です。また、Intel® Unite™ ソリューションのターゲットバージョンとの互換性を確認する必要があります。Intel® Unite™ ソフトウェアのバージョン 1.0 および 2.0 は、最新リリースバージョンのプラグインには対応していません。



LAN ケーブルが必要：ハブの最低条件に加えて、ネットワーク構成では、ハブが有線接続を通して企業ネットワークに接続されていること、およびワイヤレス・ネットワーク・アダプターが別のアクセスポイントに接続されていないことが必要です。

保護されたゲスト・アクセス・プラグインをインストールする前に、最新のインテル® ワイヤレスドライバーがインストールされていることを確認します。ドライバーがインストールされていない場合は、インストールする必要があります。

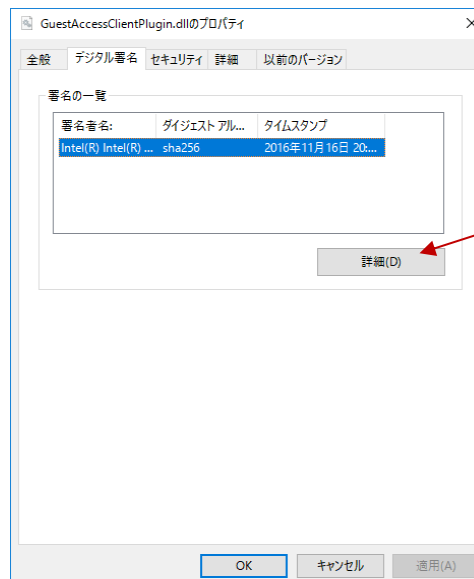
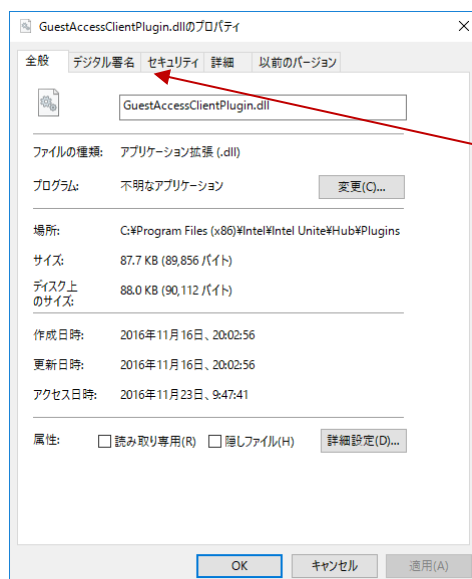
□.□.□ エンタープライズ・バージョン

1. **保護されたゲストアクセス用 Intel® Unite™ プラグインのインストーラー** (Windows* インストーラー パッケージ) を実行します。
2. Program Files (x86) \Intel\Intel Unite\Hub\Plugins にあるプラグインフォルダーに移動します。ここに、GuestAccessClient Plugin.dll がインストールされています。
3. 次に、ゲスト・アクセス・クライアント・プラグインの証明書ハッシュの値 (キー値) を取得します。デフォルト値 (デフォルト値 = 空白) ではなく、プラグインのキー値を取得して使用することをお勧めします。キー値を使用することによって、セキュリティが強化され、悪意のあるプラグインがハブにインストールされ実行されることを防ぐことができます。

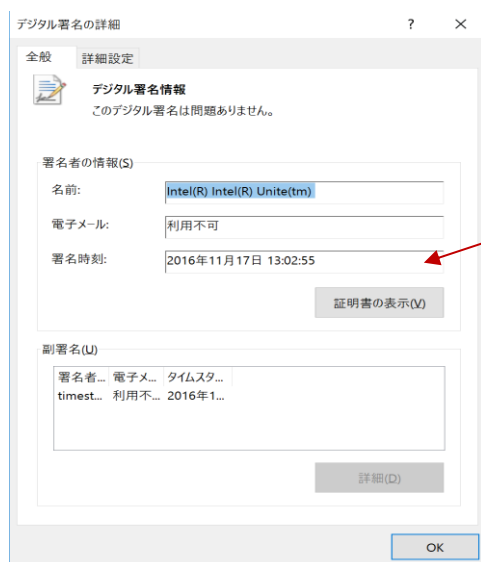
注：テスト環境ではデフォルトのキー値を使用できますが、実稼働環境では使用しないことをお勧めします。

証明書ハッシュの値の取得

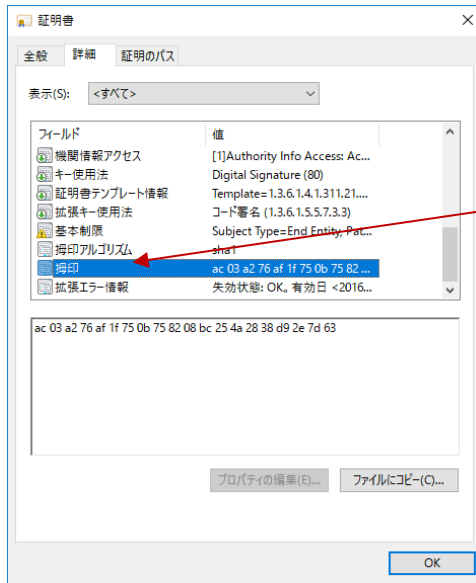
1. Intel Unite\Hub\Plugins フォルダーで、**GuestAccessClientPlugin.dll** を右クリックして [プロパティ] を選択します。
2. プラグインの [プロパティ] ウィンドウが表示されたら、[デジタル署名] タブを開きます。



4. [Intel® Unite™ プラグイン] を選択し、[詳細] をクリックします。
5. [デジタル署名の詳細] ウィンドウで、[証明書の表示] をクリックします。



6. [証明書] ウィンドウで [詳細] タブを選択し、[拇印] が表示されるまで下にスクロールします。
7. [拇印] を選択します。値が表示されたら、コピーしてメモ帳またはテキストファイルに貼り付け、スペースを削除して保存します。

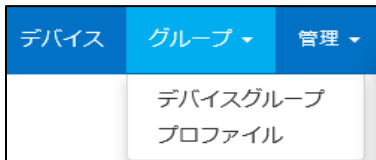


値をコピーしてメモ帳またはテキストファイルに貼り付け、スペースを削除して保存します。

- この情報は、管理者 Web ポータルでプラグインのプロファイルを作成する際に使用されます。また、プロファイルの作成後に、キー値を作成して入力することもできます。

管理者 Web ポータルでプロファイルを作成する

- 管理者 Web ポータルに移動して、[グループ] の [プロファイル] を選択します。



- [作成] をクリックしてゲストアクセスのプラグイン証明書ハッシュキーを作成し、[プロファイルのプロパティ] ウィンドウが表示されたら次の情報を入力します。



- キー : PluginCertificateHash_GuestAccessPlugin

(形式は PluginCertificateHash_XXXX です。X には、プラグインに付ける名前を指定します)

- **データ型** : テキスト
- **値** : 「証明書ハッシュの値の取得」のセクションでメモ帳またはテキストファイルに保存した値 (拇印値) を貼り付けます。このデータはキーの作成後に入力することもできます。

3. [作成] をクリックしてプロファイルを保存します。
4. [プロファイルの詳細] ウィンドウに、プラグインの新しいプロファイルおよび入力したキー値が表示されます。



5. また、[プロファイルの詳細] ウィンドウの [プラグイン証明書ハッシュの確認] キーが有効 (緑色) であることを確認する必要があります。有効になっていない場合は、赤から緑に切り替えて有効にします。



注 : テスト環境では証明書チェックを無効にすることができますが、実稼働環境ではお勧めできません。

保護されたゲスト・アクセス・プラグインのレジストリー・キー

レジストリー・キーで定義されるデータは以下のとおりです。

- a. HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\SSID
- b. HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\PSK

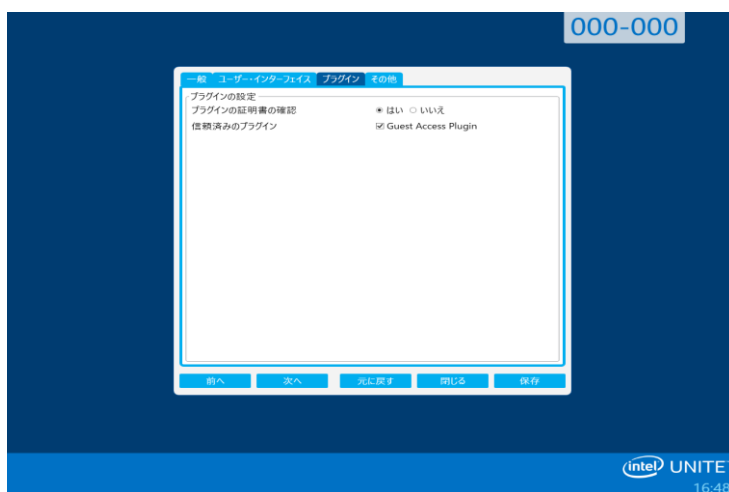
重要 : パスワードを指定する場合は、8 文字以上にする必要があります。8 文字未満のパスワードを指定すると、ゲストアクセスが開始されないことがあります。

- c. HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\Download

□.□.□ スタンドアロン・バージョン

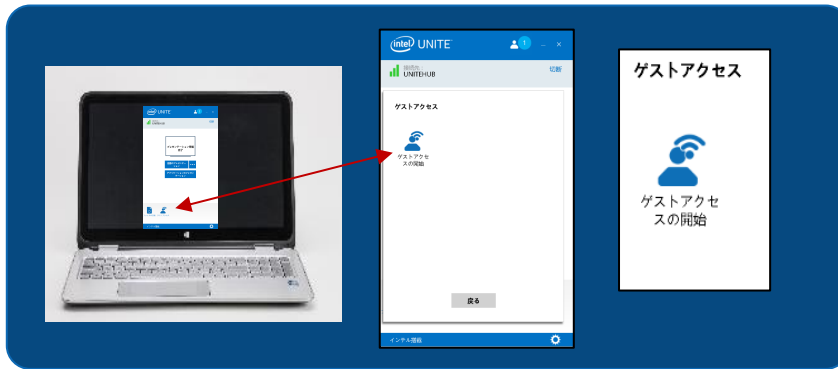
スタンドアロン・バージョンでは、ハブで実行している Intel® Unite™ アプリケーションを終了し、デスクトップのランチャーをクリックするか [スタート] メニューから Intel® Unite™ アプリケーションの**設定**を開く必要があります。

1. 設定ウィンドウで、**[プラグイン]** タブに移動します。

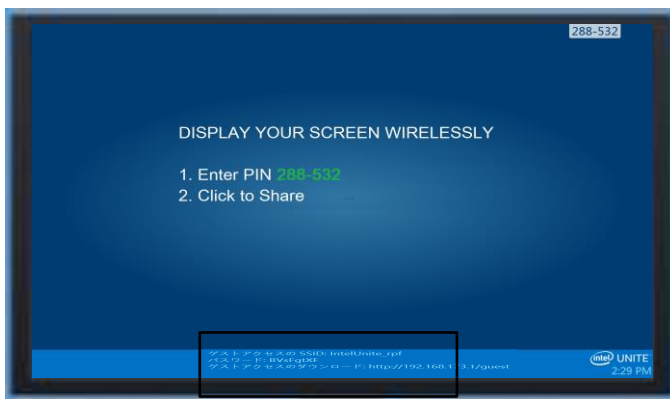


2. **[プラグインの証明書の確認]** で **[はい]** を選択します。これで、信頼済みのプラグインのみが読み込まれます。
 - 信頼済みのデジタル署名されたプラグインのみを読み込む場合は、**[はい]** に設定します。**[いいえ]** に設定した場合は、インストール済みのあらゆるプラグインの読み込みが許可されます。
3. **[信頼済みのプラグイン]** で、ゲスト・アクセス・プラグインのボックスをオンにして有効にし、**[保存]** をクリックします。このオプションは、**[プラグインの証明書の確認]** が **[はい]** に設定されている場合にのみ表示されます。**[信頼済みのプラグイン]** リストが空の場合、デジタル署名されたプラグインはインストールされていません。

3. 保護されたゲスト・アクセス・プラグインのフロー



クライアント・デバイスは、モニターに表示された PIN を入力して、Intel® Unite™ アプリケーション内でセッションを開始し、ゲストアクセスを開始します。



ハブで、インストールされているプラグインとサービスが開始します。

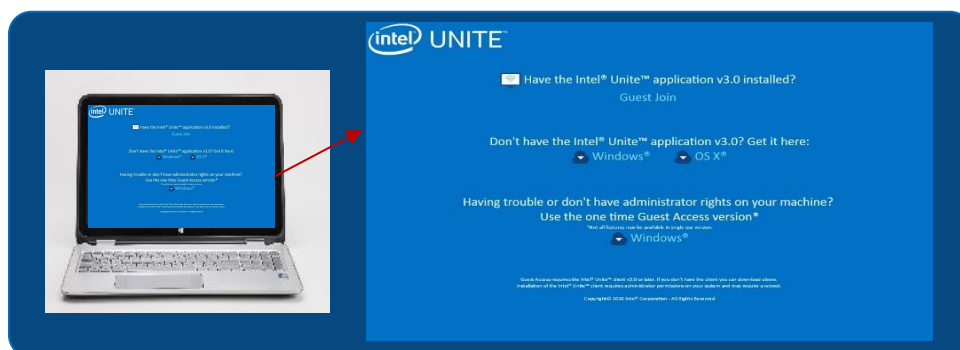
ゲスト・アクセス・サービスは、ホストされているネットワークを開始します。SSID、パスワード、ダウンロードのリンクがモニターに表示されます。



ゲストアクセスの SSID: IntelUnite_rpf
パスワード: BVsFgDXF
ゲストアクセスのダウンロード: <http://192.168.173.1/guest>



ゲスト (ユーザー) は、関連付けられているパスワードを使用して SSID に接続し、アプリケーションに参加するか、ダウンロードします。

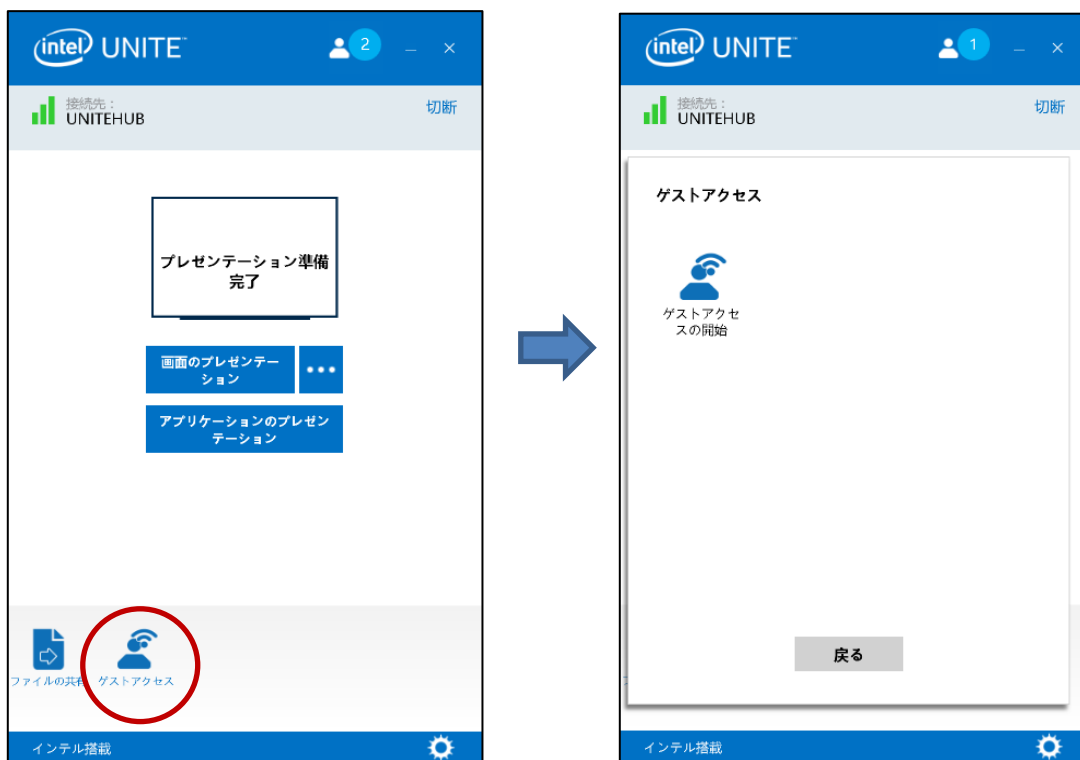


□. クライアント・デバイスでゲストアクセスを有効にする方法

ユーザーは、ゲスト・アクセス・クライアントが接続できるモニターあるいはディスプレイに表示されている PIN を使用し、ローカルでハブ (室内の参加者) に接続されたクライアント・マシンを用意します。

ゲストアクセスが許可されているクライアント・マシンで、次の手順を実行します。

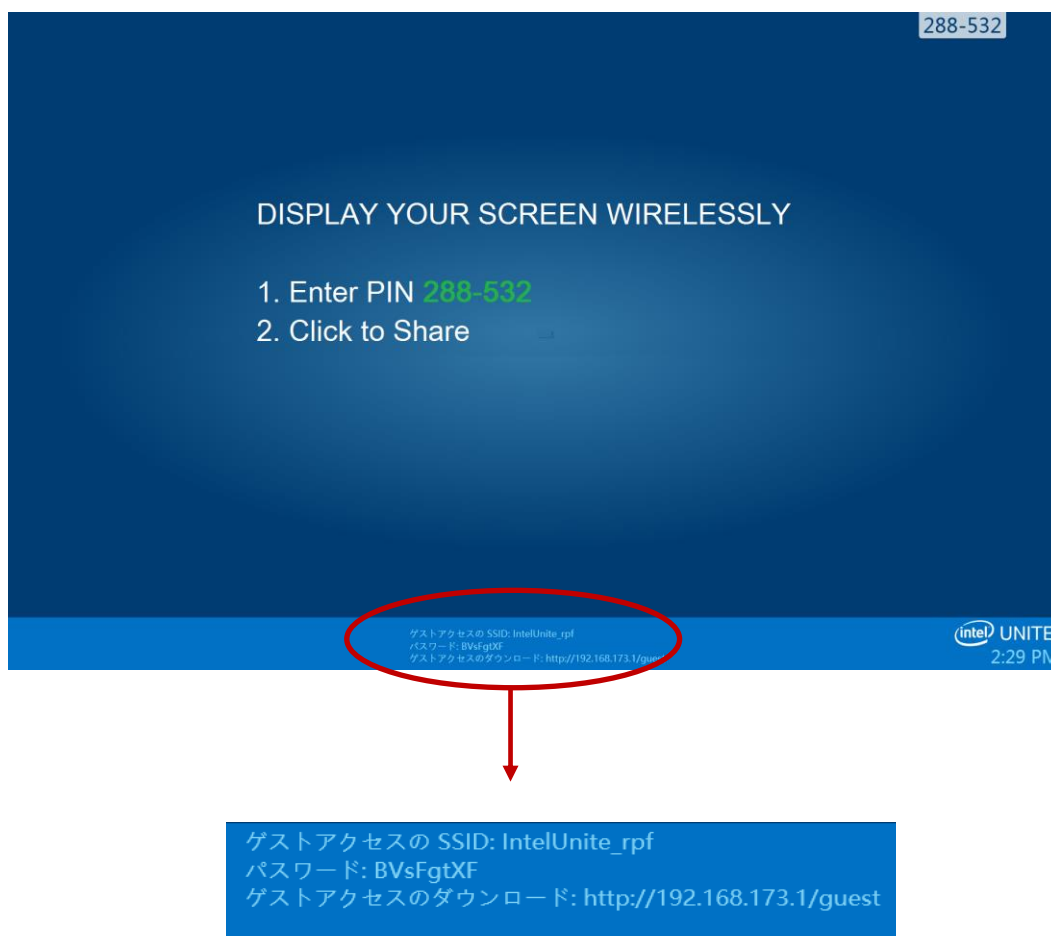
1. ハブに表示されている PIN を使用して Intel® Unite™ アプリケーションに接続します。
2. 接続したら、ウィンドウに表示される [ゲストアクセス] アイコンをクリックします。



3. [ゲストアクセス] ウィンドウが表示されます。[ゲストアクセスの開始] をクリックして、参加するゲストのローカルの Wi-Fi アクセスを有効にします。

4. 会議室内のモニターまたはディスプレイであるハブには次の内容が表示されます。

- **ゲストアクセスの SSID** 「独自のネットワーク名」
- 使用するパスワード
- [ゲストアクセスのダウンロード] リンク



ゲストアクセスから接続しているクライアント・マシン (セッションゲスト) :

1. **ゲストアクセスの SSID** に接続して、ハブに表示されるパスワードを入力します。
2. ブラウザーで、モニターに表示される [ゲストアクセスのダウンロード] リンクに移動します。表示されている形式 <http://<hostIP>/guest> を使用します。

3. 次の Web ページが表示されます。

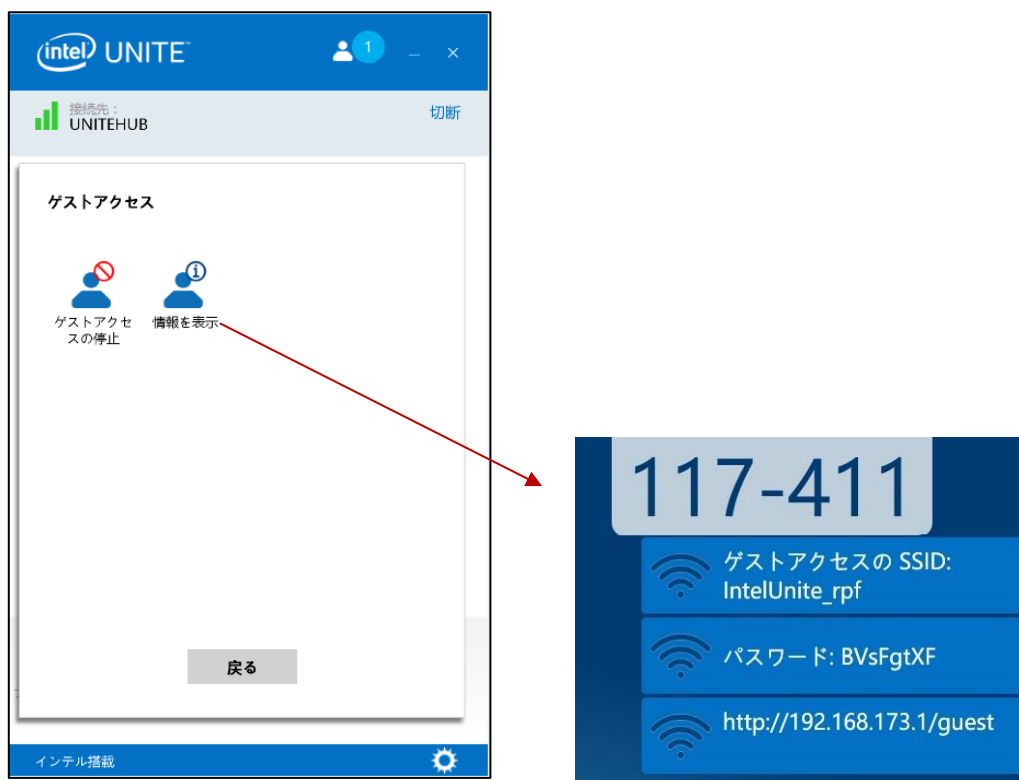


4. 次の 3 つのオプションに従って選択します。

- **Intel® Unite™ アプリケーション v3.0 をインストールしていますか？**
 - このオプションは、クライアント・マシンに Intel® Unite™ アプリケーションがすでにインストールされている場合に使用します。接続するには、**[ゲスト参加]** (v3.0 が必要) をクリックしてください。
- **Intel® Unite™ アプリケーション v3.0 を所有していませんか？こちらでダウンロード：**
 - このオプションはクライアント・マシンに Intel® Unite™ アプリケーションがインストールされていない場合に使用します。お使いの OS に応じて **[Windows*]** または **[OS X*]** をクリックし、アプリケーションをダウンロードして接続します。
- **マシンに問題があったり、管理者権限を持っていませんか？**
ワンタイム・ゲスト・アクセス・バージョンを使用
 - このオプションは、Intel® Unite™ アプリケーションがマシンにない場合、および/またはアプリケーションのダウンロードに問題があるか (前述

の2 オプション)、アプリをダウンロードしてインストールする権限がない場合に使用します。ワンタイムのゲスト・アクセス・バージョンを使用できます。このオプションでは、Intel® Unite™ アプリケーションが1 回のみ起動し、クライアント・マシンには常駐しません。このオプションは、**Windows* OS** のみで使用できます。

5. 選択に従って、インストーラーをダウンロードし、実行します。
6. インストールの完了後、クライアント・マシンに **[接続]** ウィンドウが表示され、ゲストが PIN を入力してセッションに接続できます。
7. **[ゲストアクセス]** ウィンドウで、**[情報を表示]** アイコンが表示されている場合は、セッションに接続しているユーザーを表示できます。**[情報を表示]** をクリックすると、ゲストが使用しているゲストアクセス情報のトーストメッセージがモニター (ハブ) に表示されます。





8. すべてのユーザーがセッションから切断されると、ゲストアクセスを使用しているクライアント・デバイスが切断されます。ハブ (モニターまたはディスプレイ) に、ゲストアクセスで接続しているユーザーがいないことを示すトーストメッセージが数秒間表示されます。

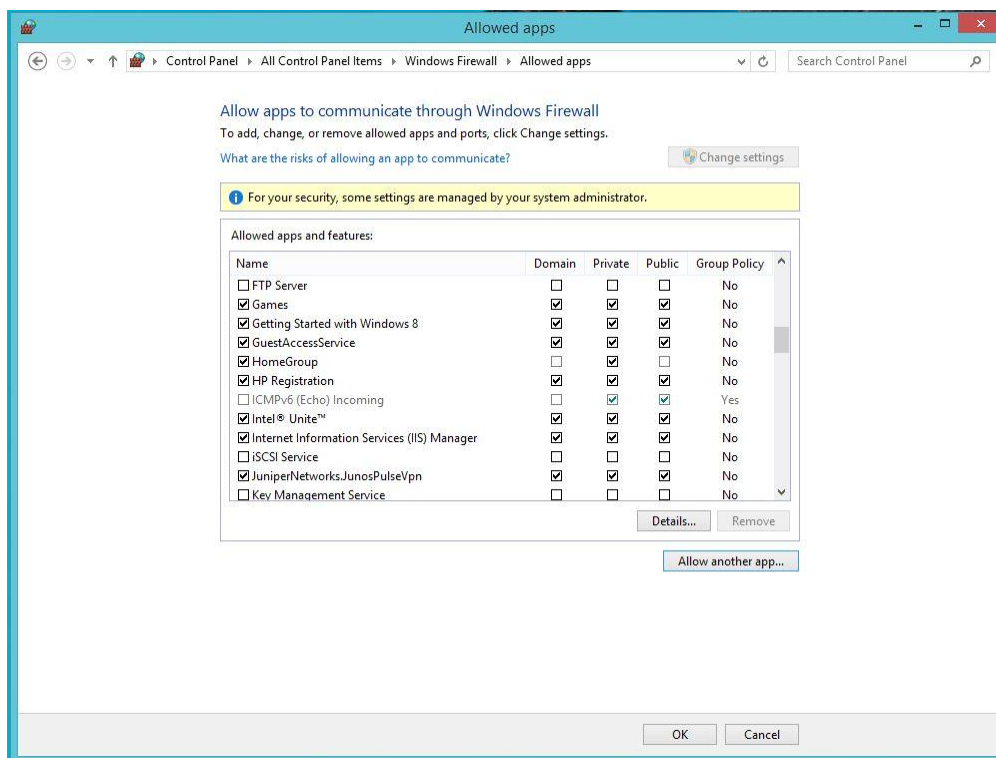
ゲストアクセスが停止しました。接続しているユーザーは...

付録 A : ファイアウォールの例外

ファイアウォール設定で、Intel® Unite™ アプリケーションと GuestAccessService が [許可されたアプリ] リストに追加されていることを確認および検証してください。

以下の例のように次のボックスをチェックする必要があります。

1. インターネット インフォメーション サービス (IIS)
2. マネージャーおよび WWW (HTTP)
3. GuestAccessService



付録 B : トラブルシューティング

Windows* イベント ログでも詳細情報が確認できます。

ゲストアクセスが開始しない (または表示されない)

- プラグインの動作を妨げる証明書ハッシュが入力されていないことを管理ポータルで確認します。
- 自分の組織の GPO ポリシー (グループ・ポリシー・オブジェクト) が仮想ホスト・ネットワークを許可しない場合は、システム管理者に連絡してください。
- 管理者 Web ポータル (エンタープライズ・バージョン) に、保護されたゲストアクセスのプラグイン証明書ハッシュのキー値が入力されていることを確認します。
- 管理者 Web ポータルで、プラグイン証明書ハッシュが有効になっていることを確認します。
- ハブが有線接続で企業ネットワークに接続されていることを確認します。
- スタンドアロン・バージョンの場合、[信頼済みのプラグイン] チェックボックスをクリックして、[設定] - [プラグイン] タブでプラグインを有効にしていることを確認します。
- レジストリー・キー HKCU/software/intel/unite/guestaccess/PSK でパスワード値を変更した場合 (デフォルト値を使用していない場合) は、そのパスワード値が 8 文字以上であることを確認します。
- 最新のインテル® ワイヤレスドライバーがインストールされていることを確認します。