ATENジャパン株式会社　技術部　製品戦略課　2021-09-02版

CC2000簡易セットアップガイド

目次

【必ずお読みください】ご注意

- 当ガイドはCC2000 / v3.2.312をベースにした内容となります
    - 2021年9月現在、最新バージョンはv3.2.315となりますがセットアップ方法は同一です
    - CC混在した説明がございますが、適宜最新バージョンとしてお読み替えください
- 当ガイドは「CC2000を最低限セットアップして使用開始するまでのガイド」として作成しています
- 手順の詳細を確認する場合は、製品マニュアルをご参照ください
- 弊社製のKVM製品やマニュアルは、予告なく仕様変更などが行われます
- 弊社の技術サポートの提供は最新版のファームウエアでのご利用が前提条件です。過去バージョンで発生する不具合はサポート外のためご注意ください
- 過去バージョンの機器を使用している発生している問題・障害に対してはまず最新版へアップグレードしてからご確認ください
    - 過去のバージョンで発生している不具合に対しては、サポート外となります
    - 同様に既存のKVMデバイスに対して増設する時も必ずJDK、デバイスならびに各機器をアップグレードしてください
    - **使用するCC2000とKVMデバイスが最新バージョン同士でない組み合わせでは、認識・検出されない、画面が表示できない、操作ができないなど予期しない不具合の原因となることがあります。そのため構築・増設する前には必ずCC2000とKVMデバイス両方が最新バージョンに更新されているか確認してから、構築してください**
- 仕様変更によって、最新のハードウエアでは過去バージョンのファームウエアに書き換え出来ない場合がございます
    - 強制的にダウングレードした場合に動作しないおそれがございます。弊社では同製品内の過去互換性についてはサポート外のため、ご理解いただきますようお願い申し上げます
- ご利用から3年以上経過した製品については、仕様変更に伴い最新のファームウエアはご利用いただけない可能性がございます。保証期間を満了した旧バージョンのハードウェアに対し、現行バージョン同等に使用するための技術サポートは提供できません。
    - 保証期間が満了したハードウェアで相性問題などの不具合が発生した場合、使用しているバージョンに近いバージョンへアップグレードできるかお試しください。(例・v1.1.102を使用していればv1.1.103に上げられるかお試しください)その後、アップグレードできるバージョンまで更新し、不具合が解消できるかお試しください
    - 改善が見られなかった場合は、製品リプレースでの解決による方法をご検討いただきますようお願い申し上げます。
- 製品のファームウエアは製造時点では最新バージョンにて製造されていますが、物流などの都合によりさらにに新しいバージョンが公開されていることがあります。利用の際は最新バージョンにアップグレードしてご利用ください
- 本製品は、すべての接続機器、ネットワーク機器の動作を保証するものではありません。ご使用の際には、事前の段階で十分に評価していただき、お客様の責任においてご利用頂きますようお願い致します。最終システムに対しても本機器の機能が満足するかどうかを事前に評価などにてご確認頂きますようお願いします
- v2.8.274以前のバージョンへの技術サポートは2020年12月31日に終了しています。弊社技術サポートは最新バージョンのCC2000が必須となるため、ご注意の上、アップグレードしてから問題点の切り分けを進めていただきますようお願い申し上げます

- 各OSや機器のIPアドレスのセットアップ、VPNを使用したリモートからの接続方法などについては割愛します。弊社製品であれば製品マニュアルをご確認いただき、他社製品については各ベンダーへお問合せください

改定

- 2021年03月10日 : 初版公開
- 2021年03月11日 : 1. リモート端末でIE11を使用するケースを加筆 / 2.各項目の加筆修正
- 2021年03月12日 : 各項目の加筆修正
- 2021年03月18日 : 加筆 / 1.リモート端末でIEを使用したログイン方法 / 2.冗長構成のセットアップ方法の加筆修正
- 2021年09月02日 : 各項目の加筆修正

推奨事項

事前検証

- 弊社製品各OSやミドルウェアに応じた製品づくりをしていますが、すべてのサーバーやミドルウェア/仮想環境での動作を保証するものではありません。ご使用の際には、事前の段階で十分に評価していただき、お客様の責任においてご利用頂きますようお願い致します。
- 各KVM製品のマニュアルに記載されている動作対象OSでの基本的な動作の確認を実施しておりますが、各ビルドおよびバージョンと、それらにて提供されるドライバーの完全な動作を保証するものではありません。又お客様のご使用になるソフトウェアとの相性および完全な動作を保証するものではありません。充分に事前評価していただきますようお願いします。
- 最終システムに対して本機器の機能が満足するかどうかを事前に評価してご導入いただきますようお願い申し上げます。
- 実機検証する前の段階で、弊社営業でも構成相談を承れます。
  詳細につきましては、弊社お問い合わせフォームをご利用の上、弊社営業までお気軽にお問合せください。
  https://atenjapan.satori.site/contactus
- 営業までご相談をいただく場合に具体的な構成図などをご提示いただくことで、より早い構成提案なども可能になります。
  お急ぎの場合は、弊社営業窓口03-5615-5810までご連絡ください。
    - 受付時間：午前9時～午後6時(土・日・祝日・お盆・正月期間・弊社指定の休日を除く)

障害発生時・故障に備えて

- USBキーの故障に関しては、メーカー保証(3年)はセンドバック保守となります
    - 修理の受付には製品のシリアル番号が必須となります。本体裏面のシール部分にバーコード下の英数字がシリアル番号となります
    - シリアル番号から保証期間内の判定と、有償オプションに加入しているか照合します
    - 本体底面に養生用シールなどが貼られて見えない、シールがはがされている、汚損などによってシリアル番号がご提示頂けないなどの場合は、有償での修理対応となります
    - 保証期間内は無償修理となりますが、修理品の送料につきましては相互元払いとなります
- 障害の切り分けや早期対応(代替機の先出しを希望)が必要なお客様向けに、弊社では製品購入時のみにご契約いただける有償オプションプラン「先出保守センドバックサービス」を提供しております
- 併せて、最大5年までの保証期間の延長プランもございます
- https://www.aten.com/jp/ja/supportcenter/product-warranty/product-warranty-options/
- ご加入内容によって保守サービスの価格が変わるため、詳細については弊社営業までお問い合わせください
    - ご契約を頂いた製品保守発生時、弊社技術サポート(03-5615-5811または弊社技術サポートサイト「esupport」へご依頼ください。電話応対による障害切り分けをして、保守対象機器が故障と判断された場合には、交換部材（又は代替機）を先に

指定頂いたお送り先へ発送するサービスとなります。故障した部品(機器）はお客様による交換作業実施後、弊社に発送していただきます

- 誠に恐れ入りますが弊社では、弊社によるオンサイトの保守交換サービスは提供していないため、ご対応が出来かねることをご容赦頂きますようお願い申し上げます

CC2000とは何か

- CC2000はネットワークを利用して弊社製KVMスイッチを統合管理するソフトウェアです
    - 次のような用途に対しての利点があります
        - 複数のKVM overIP製品を所有していて、管理が煩雑になってしまった
        - 複数のKVM overIP製品を使っているが、どのサーバーがどのKVMスイッチにあるのか分からなくなってしまった
        - 複数のKVM overIP製品を使っているが、それぞれのKVMスイッチにアクセスする時、都度ログインするのに手間がかかる
- CC2000は、Windowsまたは対応するLinuxOS環境にインストールするとサービスとして動作します
- 無償版と有償版がありますがプログラムは同一で、ライセンスキーで制限が解除されます
    - 無償版 : アクセスできるポート数(ノード)が16台までの制限があります。また、CC2000を冗長構成で構築できません
    - 有償版 : ライセンス形態によって、アクセスできるポート数(ノード)が増えます。また、CC2000を冗長構成で構築できるようになります
- CC2000は仮想OSで利用する場合、VMware(VMwareをサポートする物理サーバーと対応サーバーOSでの稼働が必須です)のみ動作を確認しています。Hyper-V、XenServer、コンテナー型仮想環境(Dockerなど)での動作はサポート外となります。
    - 理由として仮想環境下でUSBデバイスが利用できるミドルウェアはVMwareであることを確認しています
    - 2021年現在、ESXi6.7 + WindowsServer2019 standard + ZuluOpenJDK8にて動作を確認しています
    - 仮想環境は、物理環境よりもパフォーマンスが低下するためハードウェア要件よりも高い、処理能力に余裕を持ったサーバーを用意することを推奨します
- CC2000はJDK8シリーズを利用し、JAVA VM(Virtual Machine)環境下で動作します
    - CC2000(v3.2.315)が対応するOpenJDKビルドは、ZuluOpenJDKとなります
    - 過去のOracle Javaで動作を確認しているのは、JavaRunTime Edition 8 update 202となります。
    - OpenJDKの11以降での動作サポートは2021年2月現在、対応検討中となります(使用した時に発生する不具合はサポート外となります)
- CC2000はUSBライセンスキーがなくても、機能制限の無償版として利用は可能です
    - 登録できるデバイスは16台まで、CC2000サーバーの冗長化機能が利用できないという制限がございます
- CC2000のライセンスキーは初回購入時、USBキー形態での販売となります
    - 機器の増設によるライセンスキーのボリュームを増やす場合は、購入時USBキーに記録されるライセンスデータを書き換えることでアップグレードができます。詳細は弊社営業までお問合せください
- 別売の「CCVSR」(KVM操作録画サーバー)と組み合わせてご利用いただけます
- プライマリーサーバーとセカンダリーサーバーは異なるネットワークセグメントにあっても利用できます

CC2000の仕組み

- CC2000はJava Virtual Machine(JVM)で動作するサービスとして実行されます

    - CC2000をインストールする前には、JVMを起動するためのJava Runtime EditionまたはZulu OpenJDKのインストールが必須です
    - 現在、CC2000はOracle Javaバージョン8またはZulu OpenJDK8での動作を確認しています
- CC2000をインストールした後、OSを再起動することで自動的にCC2000のサービスが自動的に起動します
    - 外部からのアクセスを必須とするため、ファイヤウォールの解放設定が必須となります
    - 機器の各通信によってポート番号が異なります。詳細はマニュアルをご参照ください
- リモートPCのブラウザから、CC2000がインストールされたサーバーの8443番ポートにアクセスすることで、管理画面にログインができます

過去バージョンについて

- 2021年3月時点で、最新バージョンはv3.2.312です
- このバージョンをことを示す時に「3.0」「3.x」「CC2000 3.0」と指しますが、同じバージョンのものを示します
- その前のバージョンを指す時には「2.x系」「2.x」と称することがあります。このガイドでは、特定の話題が出ない限りは言及しません

対応スペック

サーバー機

ハードウエア

- サーバーまたは、24時間365日連続稼働に対応する、サーバーOSの利用をサポートする機器でご利用ください
- OA用のデスクトップPCやノートPCでの利用は以下の理由でサポート外となります
    - 24時間365日連続稼働に対応するよう、設計されていない
    - 高速かつ大量のネットワーク処理が行えるサーバー用途クラスのネットワークインターフェイスがオンボードで搭載されていない
        - リモートユーザーのログインや切り替えが頻繁に発生する環境では高負荷となるため、サーバーのハングアップ、パフォーマンス低下のほか予期しない不具合の可能性が考えられます
- 最小CPU : Intel Xeon E-2226G以上
- 最小メモリ : 8GB以上(CC2000の稼働にて必要となるメモリサイズです)
- 最小ストレージ : 480GB以上 (CC2000は数百MB程度の使用となります)
- 最小ネットワークインターフェイス : 1000Base-T以上の能力を持っていること

ソフトウエア

- WindowsOS : WindowsServer2012R2、2016または2019 (メインストリームサポート期間内の製品であること)
    - OSはクライアントOSではなく、サーバーOSをご利用ください。
    - クライアントOSでの稼働を想定した設計開発はされていません
- LinuxOS : RHEL 7.0以降
- LinuxOS : CentOS 7.0以降
- Zulu OpenJDK 8に対応すること
    - https://jp.azul.com/products/zulu-embedded/zuluembeddedfaq/

クライアントOSを敢えて使用した時に予想されること

- ネットワークに接続する台数や方法に依存しますが、次のような不具合の発生するおそれがあります

> - KVMデバイスが突然オフラインになってしまう
> - ブラウザなどからCC2000の管理画面にアクセス出来なくなる
> - 複数人が表示操作の切り替えをするとサーバーがハングアップする

- 理由としては以下の仕様から制限として発生します

> - 一時的にクライアントOSが対応するネットワーク接続台数が超過した
> - Windows updateが実行されて、強制的にCC2000のサービスを停止される

        - Windows updateはユーザーによる手動設定で停止してもOSが強制的に起動させるケースがあります。潜在的なネットワーク障害の要素となります
    - 処理能力を超える接続変更により、転送処理ができなくなる

クライアント機(リモートアクセス用端末)

ハードウエア

- CPU : Intel Core i5 6600以上
- メモリ : 最低8GB以上
- グラフィックス : Intel HDgraphics 530以上
- ストレージ : 20GB以上の空き容量があるSSDやHDD
- モニター : 1920x1080または1920x1200
- ネットワークインターフェイス : 1000Base-T以上の能力を持っていること

ソフトウエア

- Windows OS : Windows 10(すべて64bit版 / メインストリームサポート期間内の製品であること)
- macOS : Mojave, Sierra and High Sierra and above
- Linux : Ubuntu LTS (メインストリームサポート期間内の製品であること)
- Zulu OpenJDK 8 + Iced-teaに対応すること
    - https://jp.azul.com/products/zulu-embedded/zuluembeddedfaq/
- 対応ブラウザ
    - Microsoft Internet Explorer 11
    - Microsoft Edge (chromium版)
    - Mozilla Firefox
    - Google chrome
    - Apple Safari

使用するJavaのバージョン、種類

- CC2000は2021年3月現在の時点で、以下のJDKで動作を確認しています。共に64bitにて動作を確認しています。
    - Oracle Java version 8 runtime edition update202(通称 : jre8u202)
        - Java version8 update 202以降はOracle社のサポートポリシーが変更され、商業用途では有償となります。そのため、無償で利用できる最終バージョンにて動作を確認しております
    - Zulu Open JDK 8 update 282 b08 (別称 : 8u282b08)
        - Zulu OpenJDK11、15に対しては現時点では動作保証外となります
- 以下のバージョンではJava内部の仕様が大幅に変更されていることから、CC2000が動作しないことを確認しています
    - Java9、Java10

マルチホーム構成(複数NIC)での利用

- 1台のサーバーに複数のネットワークワークアダプター(NIC)があるマルチホーム環境での利用は、すべての環境に対しての保証ができない内容となります。
    - 理由として、CC2000はJavaにて動作していますが、JavaとWindowsにはそれぞれプログラムに対して特定のNICを固定使用する設定がありません。サーバーの構成やネットワーク環境で依存するため起動するタイミングなどによってデバイスと通信できなくなるなど、挙動の変わる可能性があります。
    - 後述の方法でデバイスを登録まで行った場合、通信できることは確認しています。しかし、再起動やネットワーク構成変更が発生した場合は、想定外の挙動に陥る可能性があります。事前の段階で十分に評価していただき、お客様の責任においてご利用頂きますようお願い致します。
- より確実なネットワークの問題を回避させる場合は、物理サーバーで複数NICを搭載している場合はVMware ESXiなどUSB接続に対応する仮想環境を構築し、ゲストOS内に1つNICが搭載された環境でCC2000を構築してください。
- マルチホーム環境にてCC2000を構築する場合は、OSのバージョンや仕様を確認してから、必ずネットワーク設計・構築できる方がしてください。
    - マルチホーム環境を使用するには、各OSのバージョンやNICごとにDNSの設定、メトリック値、バインドの設定方法などルーティング方法が異なります。このような環境に対しての設計・構築は弊社では行いません。お客様にて設定・構築してください。
- 以下の方法で導入の報告はございますが、以下はお客様にて評価を行い、障害復旧にも問題がないことを確認の上、行ってください。
    - 1つのOSで複数のNICが稼働している環境の場合は、1つのNICだけが起動している状態で、CC2000のネットワーク環境を構築する。CC2000の冗長環境を構築して、KVMデバイスの通信、挙動が確認されて、システムの構築が完了してから他のNICを起動する。ネットワークの復旧時も同様に、1つだけのNICを起動させ、KVMデバイスとの通信ができたことを確認してから他のNICを起動させる。

セットアップの流れ

1. CC2000をインストールするサーバー機ですること

1. クリーンインストールされたWindows server / Linux Serverを準備する
2. サーバーのドライバー類を最新版へアップデートする
3. Zulu Open JDKをインストールする
4. CC2000をインストールする
5. 起動したCC2000でATEN製KVMデバイスを登録する
6. 一般ユーザーアカウントを作成する

2. KVMデバイスですること

1. CC2000と通信するため、「CCマネージメント」の設定変更する

3. CC2000にアクセスするリモート端末ですること

1. クリーンインストールされたWindows 10端末を準備する
    2. (以下はIE11が利用できない環境に対しての手順)
    3. OpenJDK Zuluをインストールする
    4. Java webサービス起動用プラグインZulu製「Iced-tea」をインストールする
2. ブラウザからアクセスする

テスト構成

- Windows Server 2019 Standard (デスクトップエクスペリエンス)を使用した場合のインストール方法を紹介します
- このマニュアルでは、下図の構成を想定して紹介します
- テストシナリオは次のとおりです
    - 当初はCN9600を1台だけ使ってリモート端末から社内でアクセスして利用できるようにしていた
    - 将来的にCN9600を増設したり、ATEN製のKVMスイッチも追加してサーバーを統合管理したいという話になった
    - まずはCC2000をインストールして、CN9600を登録することで、評価環境を構築する計画となった
- この冊子では「CN9600」をKVMスイッチの例として手順を紹介しますが、他のKVMスイッチなどもほぼ共通の設定となるため、必要に応じて読み替えてご参照ください。

実施要領

1. サーバーにCC2000をインストールする
2. CN9600をCC2000に登録する
3. リモート端末からCC2000にアクセスしてCN9600にアクセスする

テスト構成図

テスト時の周囲

- Windows Serverは自機の設定やロールやタスク設定を行っていないこと、Active Directoryなどで他ドメインなどに登録などがされていない、クリーンインストールされた状態で行ってください

ZuluOpenJDKをサーバーにインストールする

- OpenJDKのJREパッケージをダウンロードします
- Zulu Open JDKのページへアクセスします

https://jp.azul.com/downloads/zulu-community/?package=jdk

- 「Download Zulu」をクリックします
- 各エディションが多くあるため、ダウンロードページの検索フィルターで「Java 8」と「JRE」を選択すると探しやすくなります
- CC2000はJava version8に対応していますので、Java 8 (LTS)の最新バージョン「8u282b08(Zulu: 8.52.0.23)」の64ビット版、JREパッケージ版のmsi形式のファイルをダウンロードします
    - もしも動作異常などが確認された場合、安定動作を確認している「8u212b04(Zulu: 8.38.0.13)」にて動作が改善されるかお試しください
        - 弊社他ソフトウェアのCCKMでは、u271以降ではTLSなど通信仕様のセキュリティを変更しているため、通信不具合を確認しています。回避策として、Oracle Java Runtime Edtion version8 update202環境での動作改善を確認しています。
- Java11以降への対応は2021年3月現在、検討中となります。使用した場合による不具合はサポート外となります
- ダウンロードしたmsiファイルをサーバーにコピーします
- コピーしたファイルを右クリックして「インストール」を選択します
- 起動すると次のような画面が表示されるので、「Next」をクリックします
- インストール先を確認してから「Next」をクリックします
- 「Install」をクリックします
- インストールするデータコピーが完了するまで、しばらく待ちます
- データコピーが完了すると自動的に次の表示になります「Finish」をクリックして終了します
- 次のインストール確認をして正しく実行されたら、OSを再起動します
- 再起動したらJDKのインストールは完了です

JDKがインストールできたかを確認する

- コマンドプロンプトを起動して「java -version」と入力し、Javaが正しくインストールできているか確認してください
- ファイル名に記載されているバージョンと同じ値が表示されているか確認してください

注意：環境変数について

- Oracle Javaによる、Java8の初期バージョン以前では環境変数を登録しないと、上記プロンプトのプログラム実行やCC2000がインストールできないという不具合が確認されていました。OpenJDK Zuluのこのバージョンでは環境変数を登録しなくても利用できることを確認しています。また、敢えて環境変数にpathを登録しないでください。CC2000が誤動作する原因になります。

CC2000をダウンロードする

- CC2000は他製品とは異なり、データ入手方法はKVM製品ファームウェアと異なります
- サポートサイトにアカウントを作成し、製品登録をするとCC2000のインストール用プログラムをダウンロードできます
- インストール完了時にOS再起動を必須としますので、ご注意ください

KVM製品をATEN技術サポートサイト「サポートセンター」に登録する

- ATENジャパンの公式ページにアクセスします
- 右上にある「サポート情報」から「サポートセンター」を選択します
- メニュー表示ができない場合は「https://eservice.aten.com/eServiceCx」から直接サイトへアクセスできるかお試しください

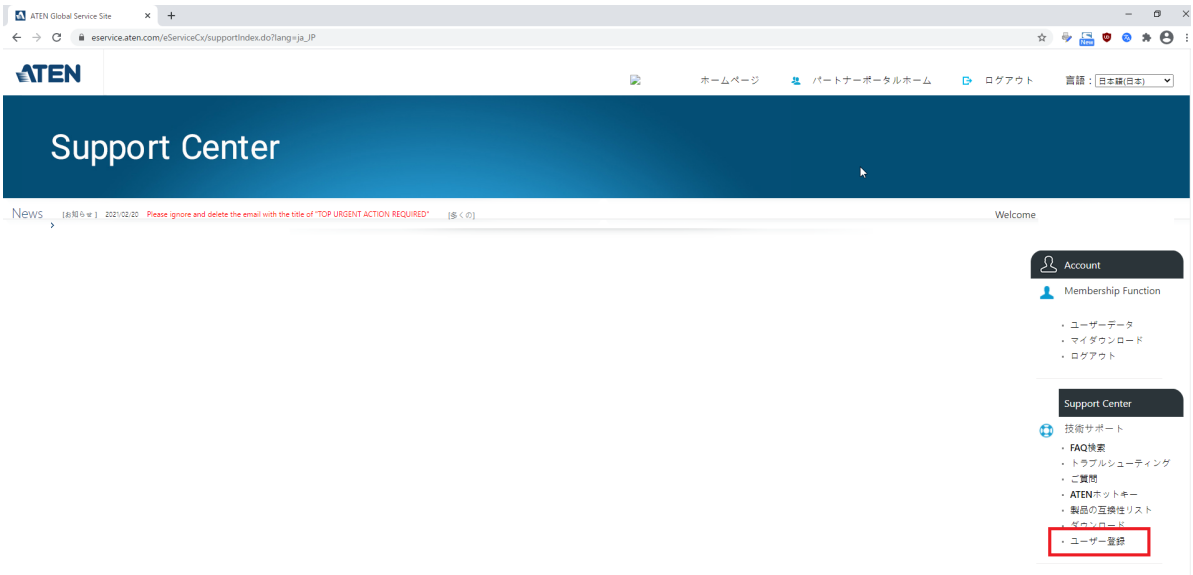
  ※画像は2021年3月時点のスクリーンショットです
- KVM製品を登録していなければ、「アカウントの新規作成」をクリックし、すでに登録済ならば「ログインをクリックしてください」

サポートセンターでアカウントを作成する

- サポートセンターでアカウントを作成し、ご購入いただきました製品を登録することで、製品によっては専用のアプリケーションプログラムやドキュメントなどがダウンロードできます。ほかにも技術的なご質問のお問合せのほか、保証期間の照会や修理サービスの提供スピードが向上しますのでぜひともご活用ください
- 「アカウントの新規作成」をクリックしたら、「個人情報の取り扱いについて」にチェックして必要事項を入力してください
    - チェック入れないと各項目が入力できません
- 送信を押して、本人確認のアクティベーションを実施したら完了です

サイトにログインし、KVM製品を登録する

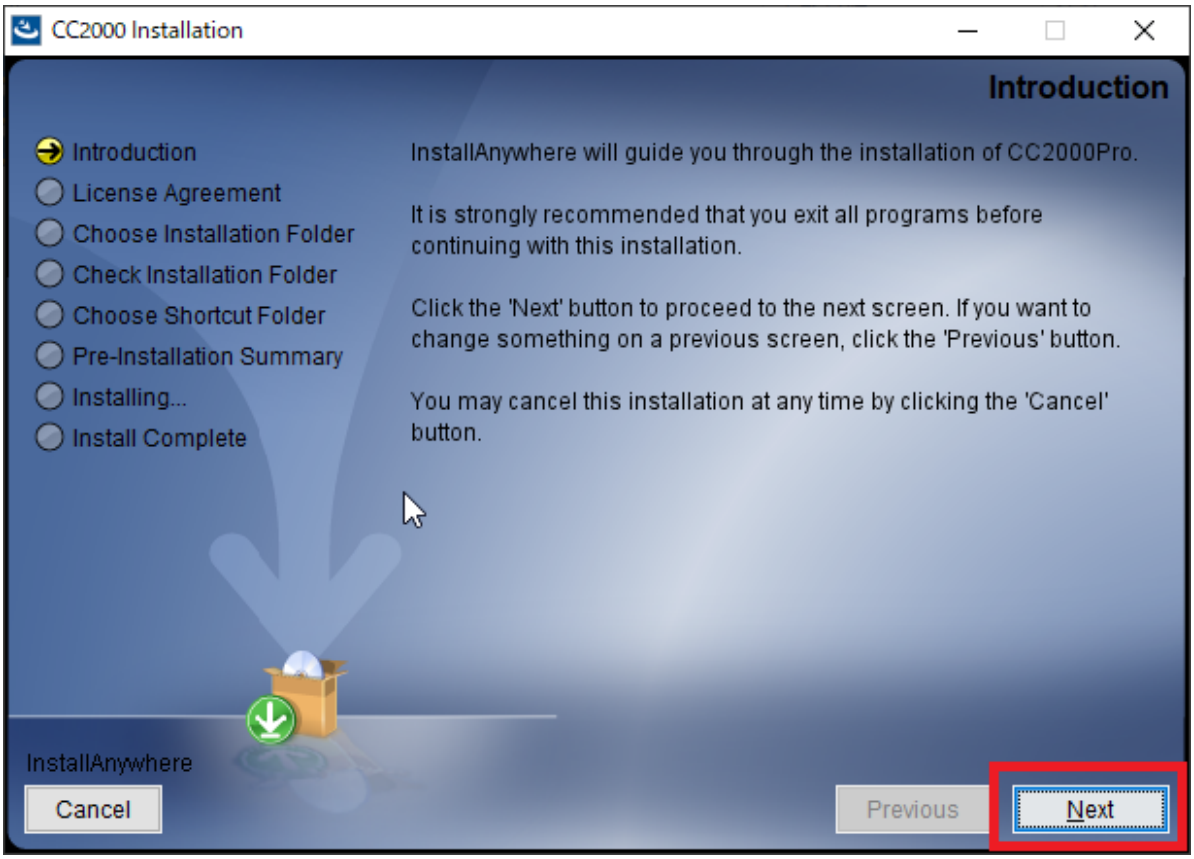
- ログインしたら、右にある「ユーザー登録」をクリックします



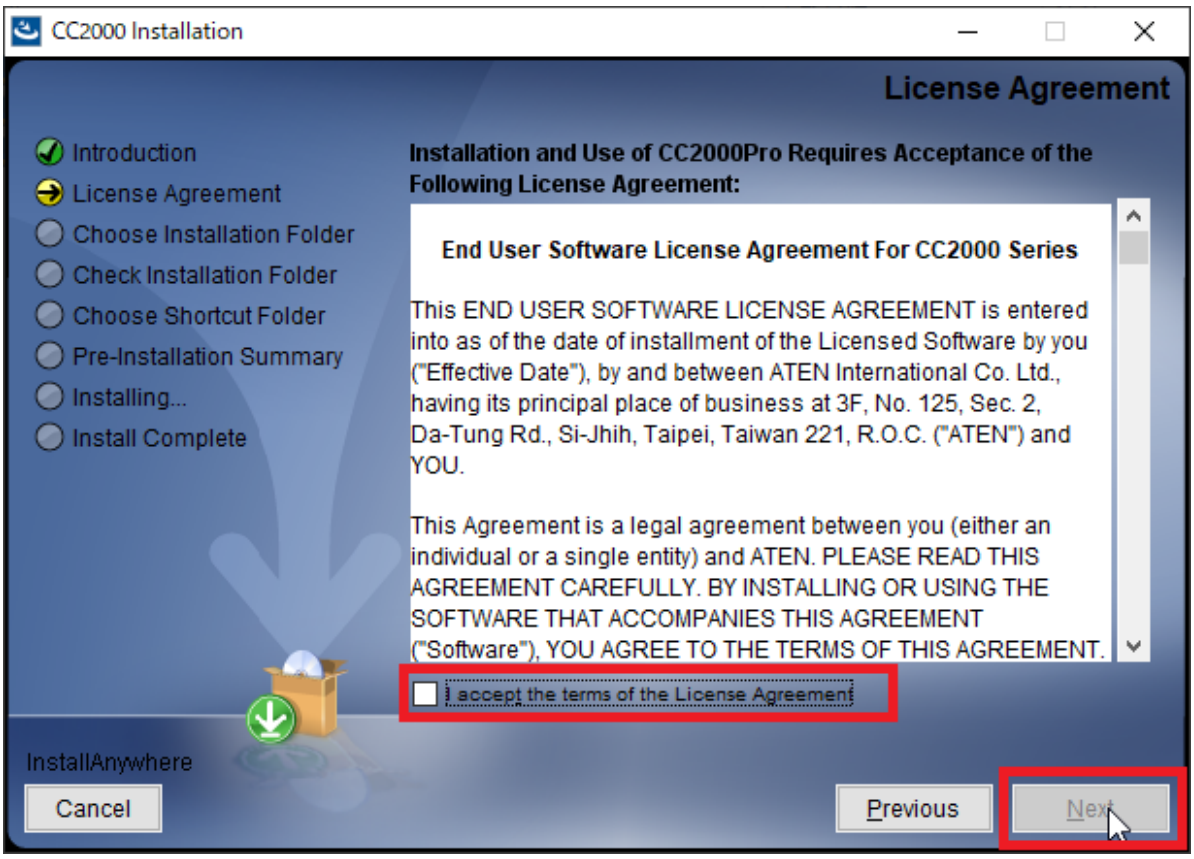
- この画面では、今までに登録済みのATEN製品がリストに表示されます
- 新規登録するため「挿入」をクリックします
- 必要事項を入力します
- **CC2000のセットアップ用プログラムを入手するには、CC2000に対応するKVM製品のシリアル番号を登録します。**今回はCN9600がCC2000に対応しているので、CN9600のシリアル番号を入力します
    - 2021年現在、CC2000 / v3.2.315は次のATEN製品を管理できます。最新の対応状況はCC2000の製品ページをご確認ください
        - KL1108V, KL1116V, KL1508Ai, KL1516Ai, KH1508Ai, KH1516Ai, KN1000, KN1000A, KN1108v, KN1116v, KN1108VA, KN1116VA, KN2124VA, KN2140VA, KN4124VA, KN4140VA, KN1132V, KN2116VA, KN2132VA, KN4116VA, KN4132VA, KN4164V, KN8132V, KN8164V, KN2116A, KN2132, KN4132, CN8000A, CN8000, CN8600, CN9000, CN9600, CN9950, CS1708i, CS1716i, IP8000
        - SN0148CO, SN0132CO, SN0116CO, SN0108CO, SN9116CO, SN9108CO, SN0148, SN0132, SN0116A, SN0108A, SN9116, SN9108, SN3101
        - PE8324, PE8216, PE8208, PE8108, PE7208, PE7108, PE6324, PE6216, PE6208, PE6108, PE5208, PE5108, EC2004, EC1000.
- 「添付」には、購入(納品)した日付と型番がわかる領収書のpdfファイルまたは画像ファイルを添付してください
- 保証期間の根拠として利用します。金額の箇所のみ黒塗りなどで読めないように処理したものを利用しても問題ありません
- 「保存」をすると登録が完了します
- シリアルナンバーは、製品底面シールのバーコード下に記載されている英数字を確認の上、登録してください。下図はサンプルとなります。
- 入力が完了したら、次は「マイダウンロード」をクリックします
- 対応機種を製品登録するとマイダウンロードに関連する製品のソフトウェアなどがリストされます。
- 今回は現時点でのWindows用CC2000の最新バージョンv3.2.315を「ファイルのダウンロード」のアイコンをクリックしてダウンロードします
- ダウンロードしたファイルは任意のフォルダーに保存してください

CC2000をインストールする

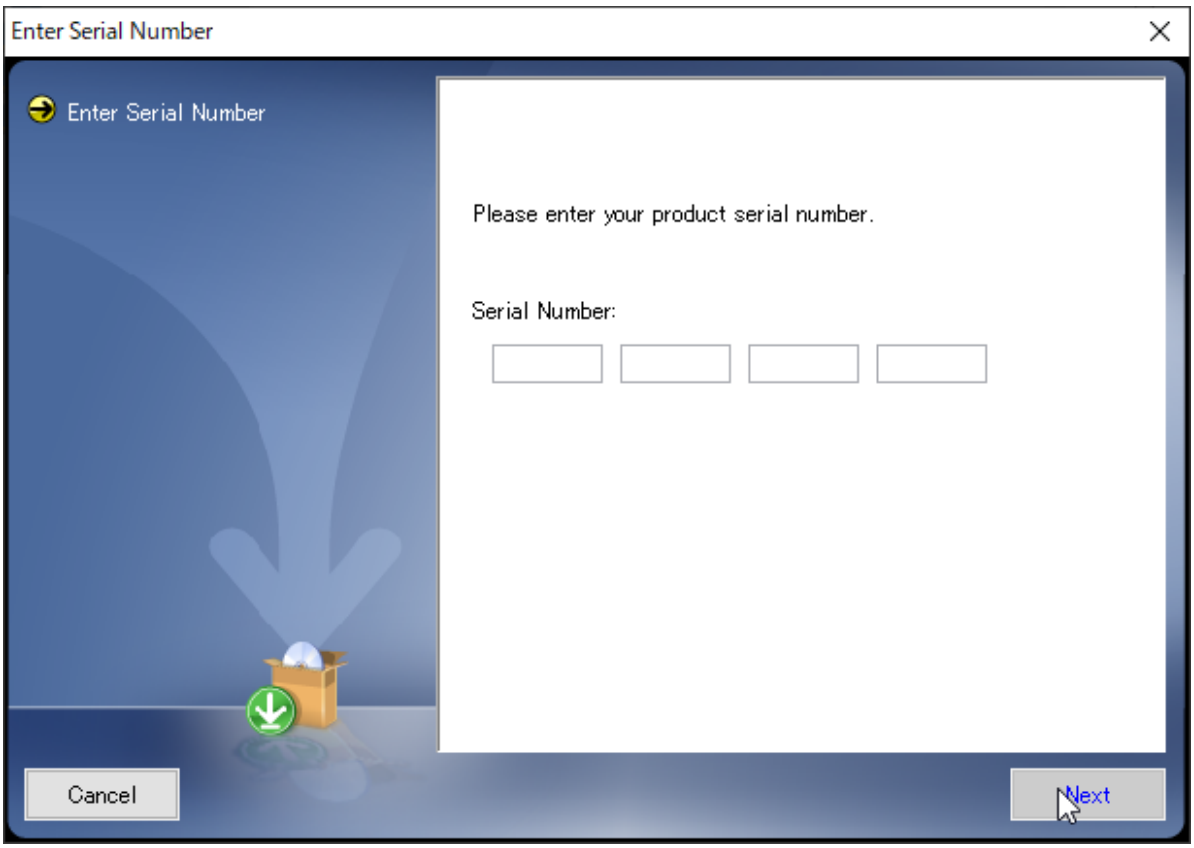
- ダウンロードしたファイルの中から、「CC2000V3-Setup-ForWindows_V3.2.315.exe」とセットアップ用ファイルを使ってインストールします
    - ファイル名に「Migration Utility」があるファイルは、v2.x系(過去バージョン)を利用していたユーザー向けのデータベースコンバーターです
    - 「Upgrade」とはv3.1.304などv3.x系で使用していたユーザー向けのアップグレード向けプログラムです
- 右クリックで「管理者として実行」でインストールを開始します
- JDKが正しくインストールできていると下図の準備画面が表示されます
- OpenJDK Zuluがインストールされていないと次のようなエラー表示がされているので、正しくインストールされているか確認してください
- 「Next」をクリックします



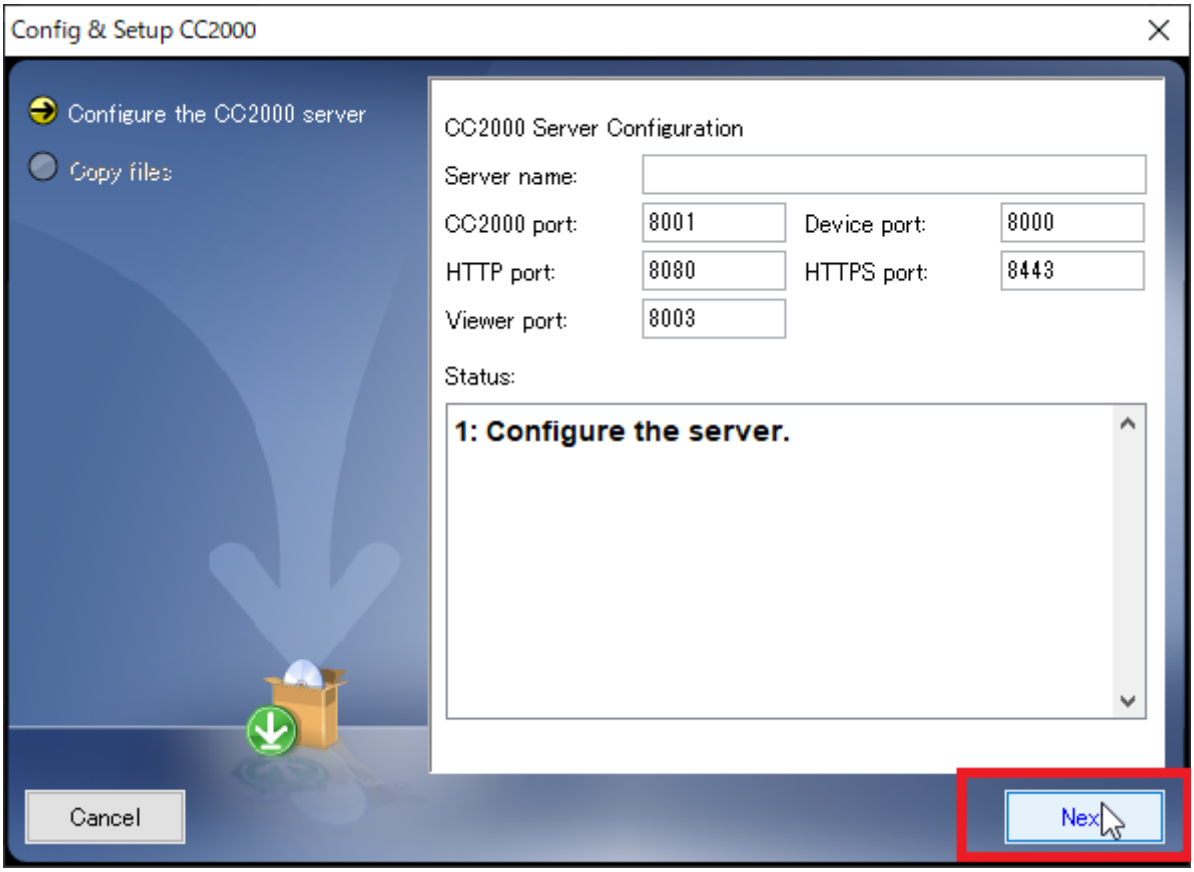
- ライセンス契約の条項を確認したら、チェックを入れて「Next」をクリックします



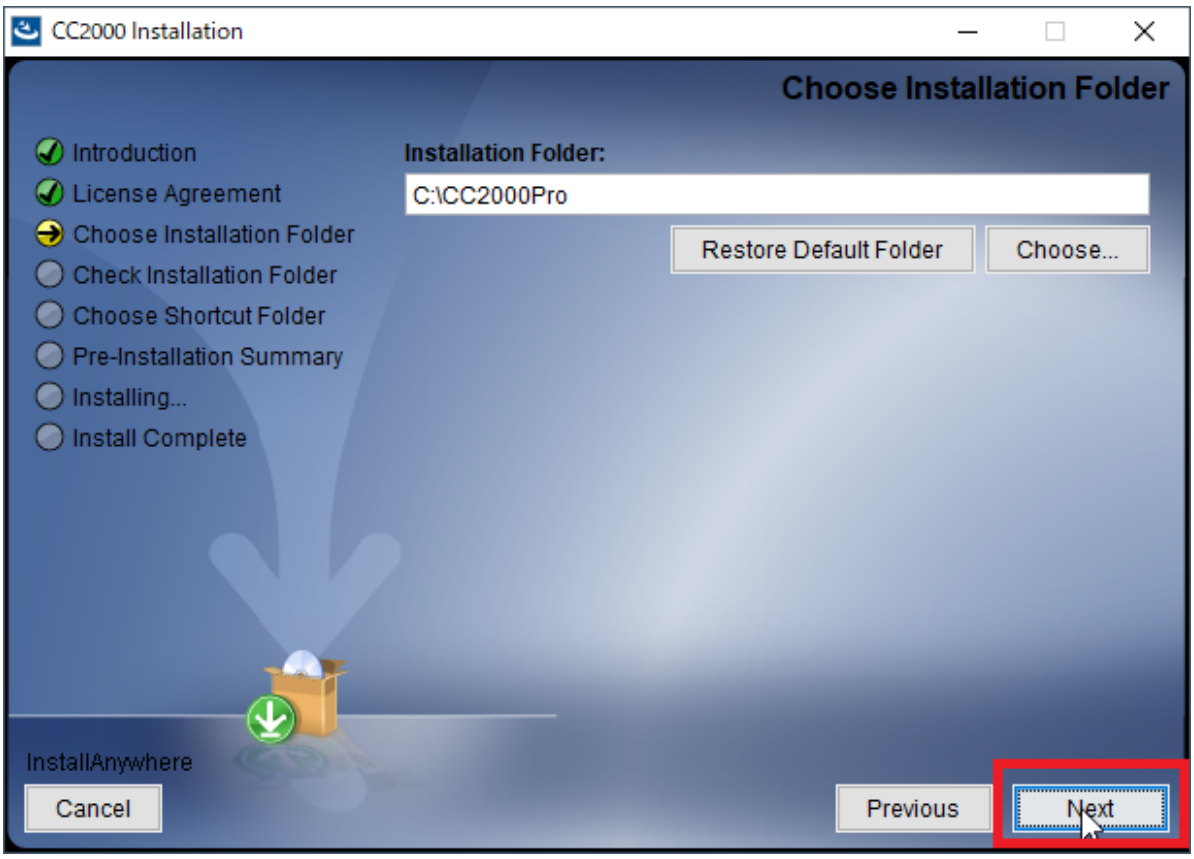
- インストールシリアルを入力します
- デモ用途で利用する場合は「01CF3-DGXU9-LJLFL-23T4P」と入力してインストールしてください
- このインストールライセンスは、デモ評価用の入力キーとなります
    - デモ版は機能的な制限として以下の点があります
        - CC2000サーバーの冗長化機能は利用できません
        - 登録できるデバイスの制限はありませんが、利用できるノード数は16個です
            - 備考「ノード」：KVMなどのポート数の総称を指します。たとえば、CN9600はPCに1台のみ接続するので、CC2000で管理する時には1ノードを使用します。KN4140VAは最大で40ポートを必要とします。デモ版では16ポート登録できますが、残りの24ポートはデモライセンスではノードが不足するため利用できない、という制限が発生します。
        - CC2000の正式版はノード数によってライセンス価格が異なりますため、システムの規模に応じたライセンスをお求めください
- 正式版を購入した場合は、次の正式なインストールライセンスキーを使ってインストールしてください
    - 購入後に正規ライセンスを使用せずにデモキーで使用し続けた場合、以下の制限が発生します
        - 機能的な制限はございませんが、CC2000にて発生した技術的な問題や不具合が発生した場合、すべてサポート外となります



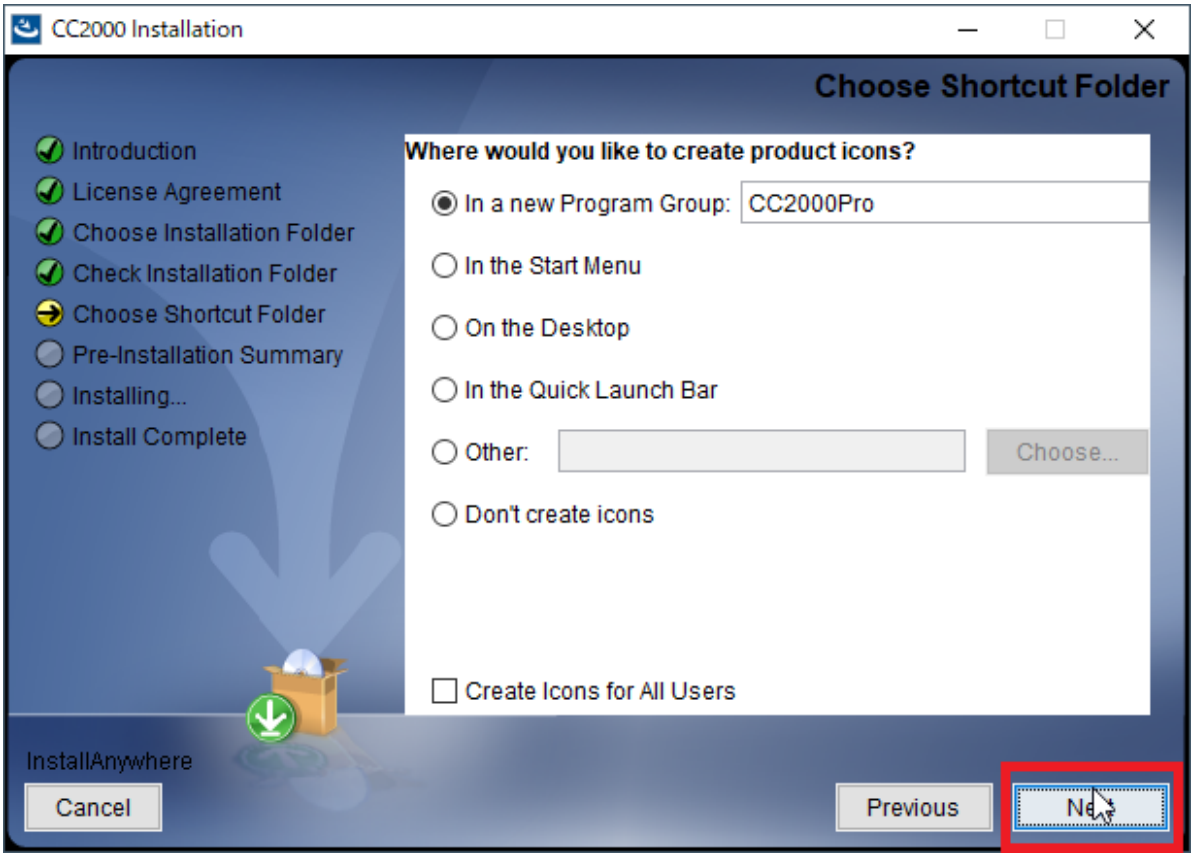
- 正規のインストールライセンスキーは、製品購入時に同梱されるCDの盤面にシール添付されています
- 決して廃棄や紛失しないよう保管してください
- CC2000にて他の機器などに接続するためのネットワークポートの番号を確認して、「Next」をクリックします



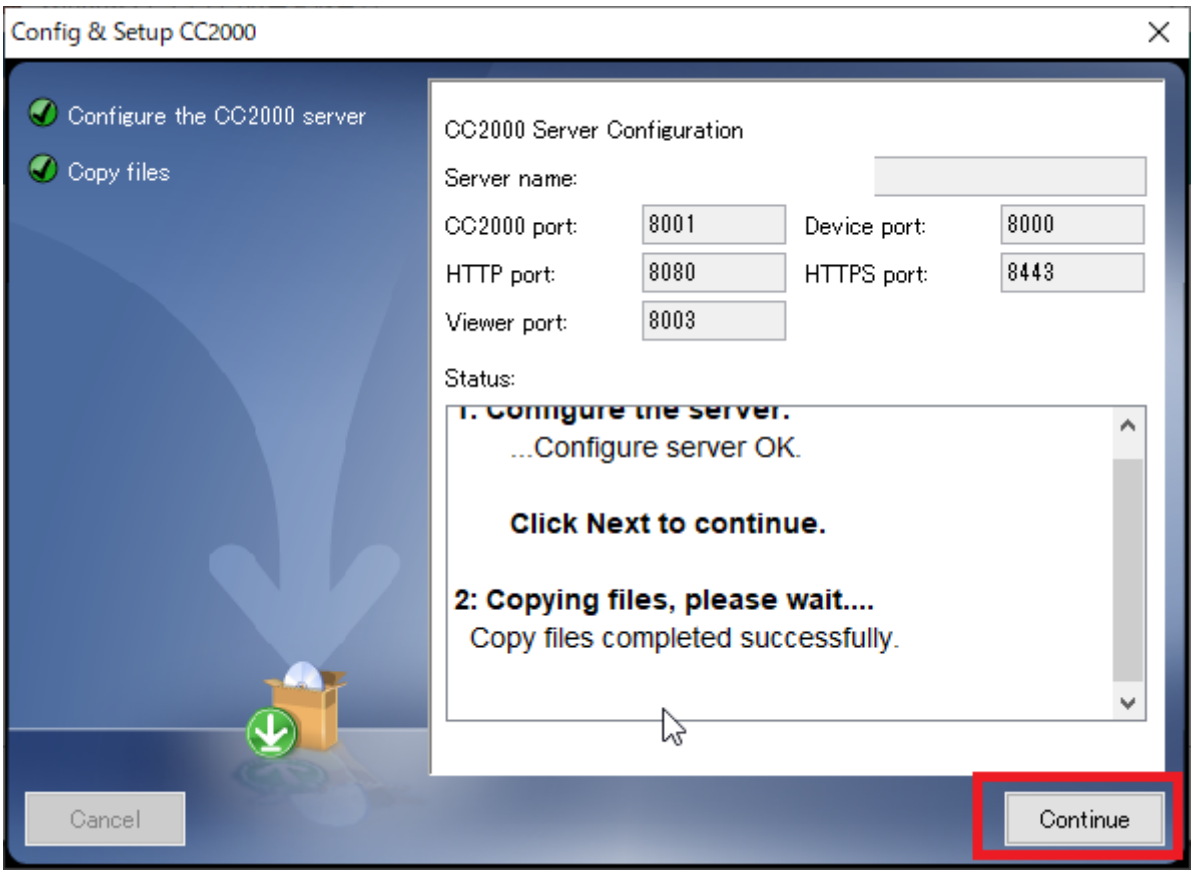
- インストール先を確認して、「Next」をクリックします



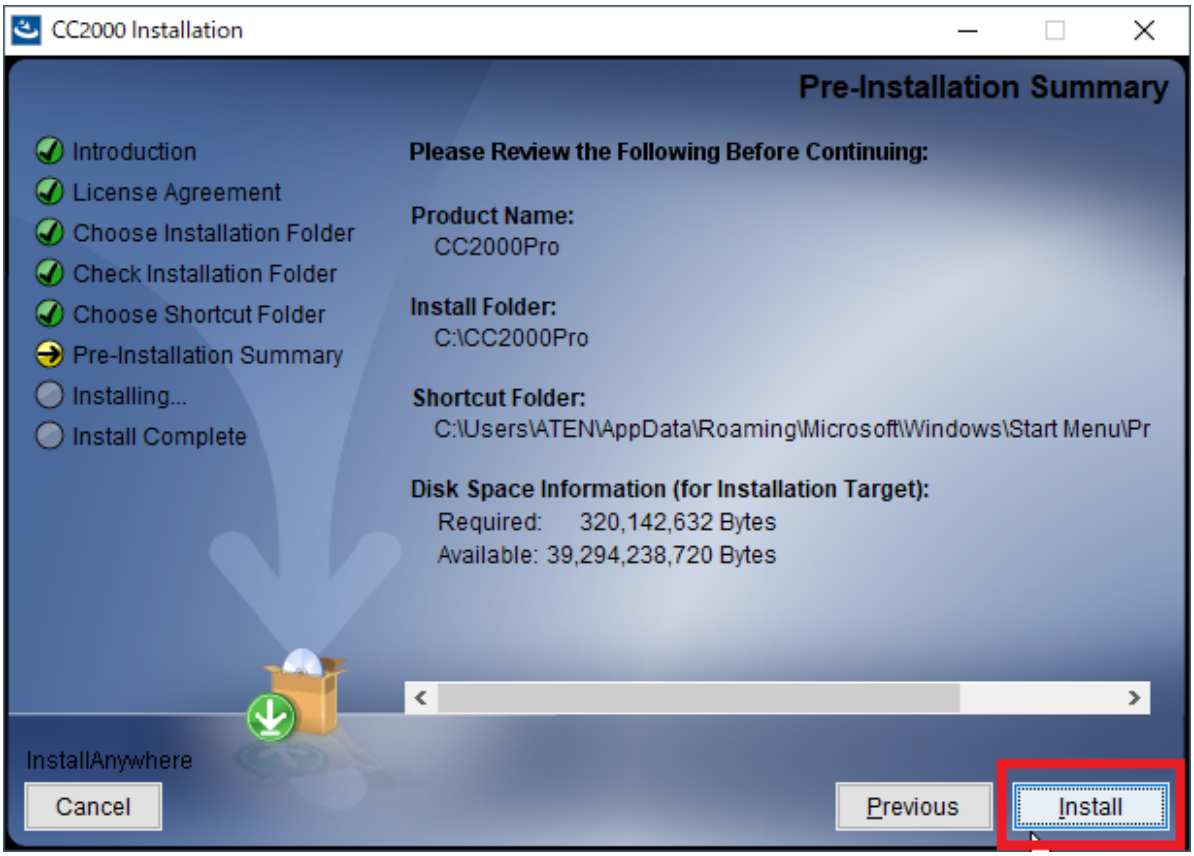
- ショートカットアイコンの作成先を確認して、「Next」をクリックします



- 各ネットワークで使用するポートを確認して、「Continue」をクリックします

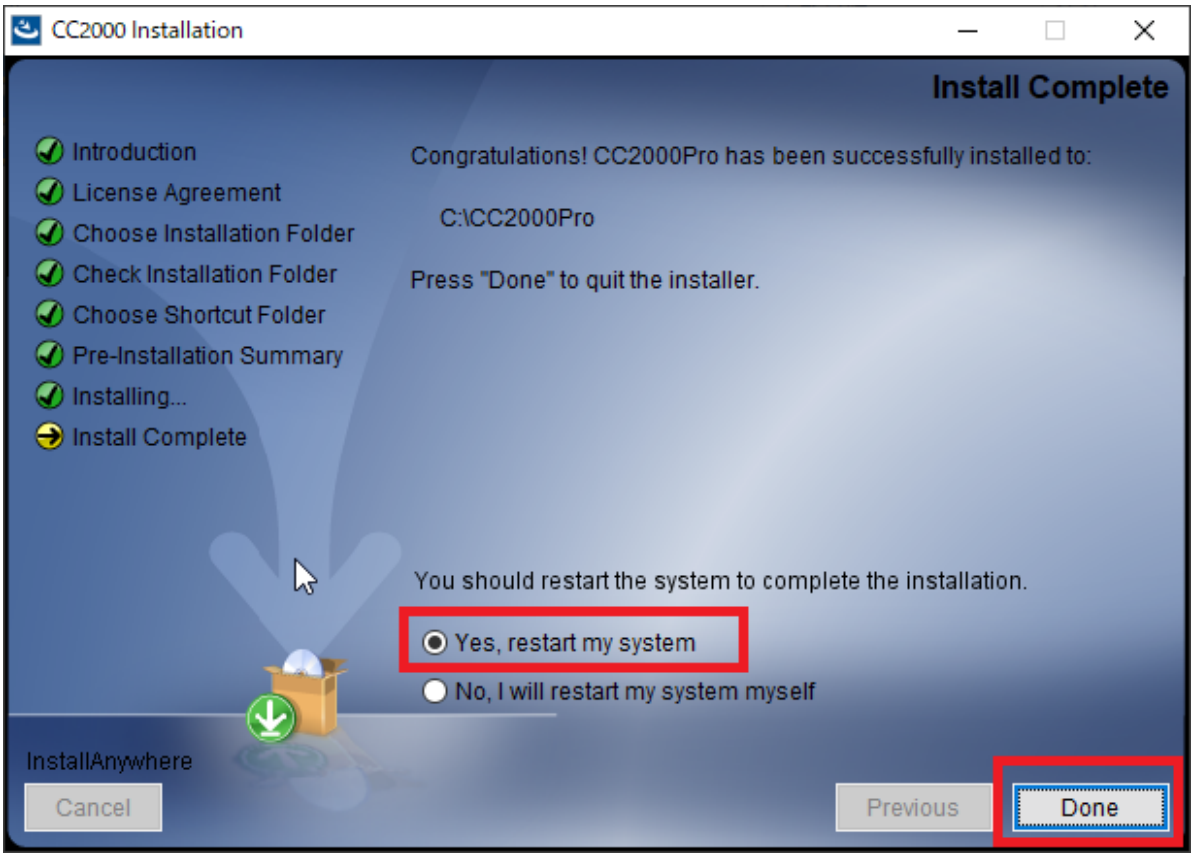


- 「Install」をクリックします



- CC2000のデータコピーとセットアップが完了するまで、しばらく待ちます

- セットアップが完了したら、「Yes, restart my system」を選択して「Done」をクリックし、OS再起動してください
    - サーバーで稼働しているシステムによっては再起動できないケースがあります。その場合は、他のシステムをシャットダウンしてからOSを再起動させてください
    - 再起動していない状態でCC2000は利用できません
- 「No, I will restart my system syself」を選択して「Done」をクリックした場合は、手動でOS再起動してください



- 再起動が完了したら、CC2000のインストール完了です

ファイヤーウォールの設定をする

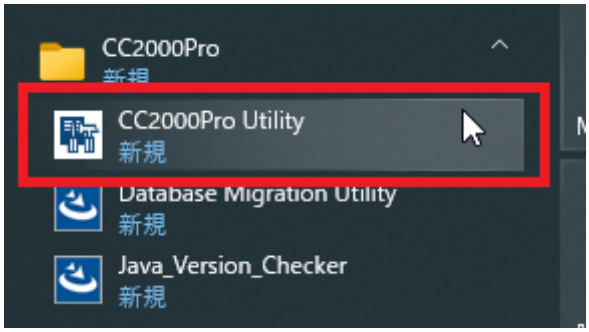
- Windows server 2019は初期設定でファイヤーウォールは有効になっており、外部との通信許可設定が必要になります
- テスト段階ではまず、マイクロソフトのファイヤーウォールをすべて無効にした状態で利用できることを確認してください。通信ができることを確認してから、必要なポート以外は無効にするなど設定されることを推奨します
- 詳細の設定方法は割愛します
    - ネットなどで公開されている方法を参考する前に、まずはネットワーク管理者の方に相談してください。

CC2000を起動させる

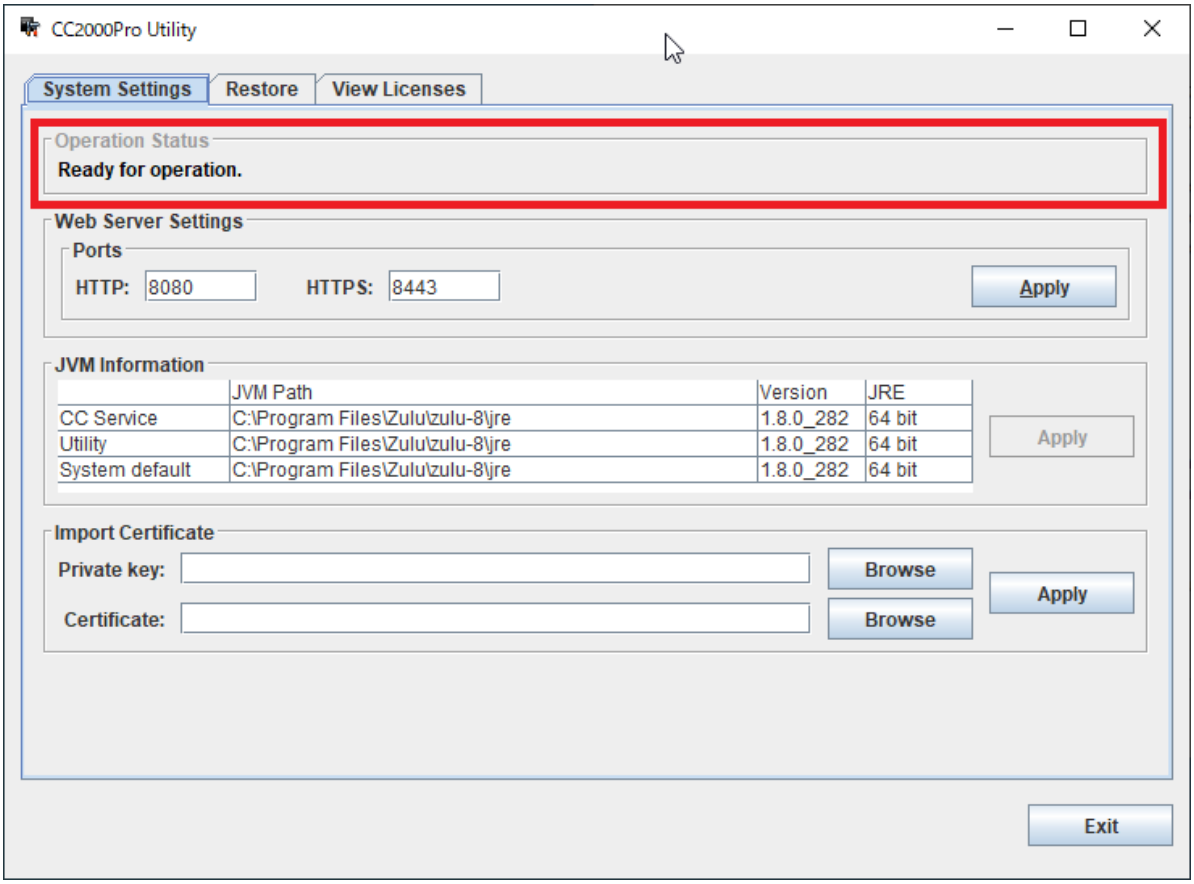
- CC2000はWindowsサービスとして登録され、自動的に起動するようになっています
- サーバーの処理能力や状況によっては、CC2000の起動に数分以上かかることがございます
- 以下は、タスクマネージャーから起動状況や強制的に起動させることはできますが、可能な限り強制的な起動は行わずOSによる自動かつ安全な起動を強く推奨します
- サービスで実行しても反応しないなど、フリーズしている可能性が考えられる場合は、次の方法で動作を確認できます

CC2000の稼働ステータスを確認する

- windowsのスタートをクリックして「CC2000 Pro」にある「CC2000 Pro Utility」を起動します



- CC2000Pro Utilityにある「Operation Status」で「Ready for Operation」と表示していれば、プログラムとしては稼働し、問い合わせに反応していると確認できます
- 「Ready for Operation」と表示しているにもかかわらずリモート端末からアクセスできない場合は、ネットワークに不具合がないかご確認ください



CN9600を設定する

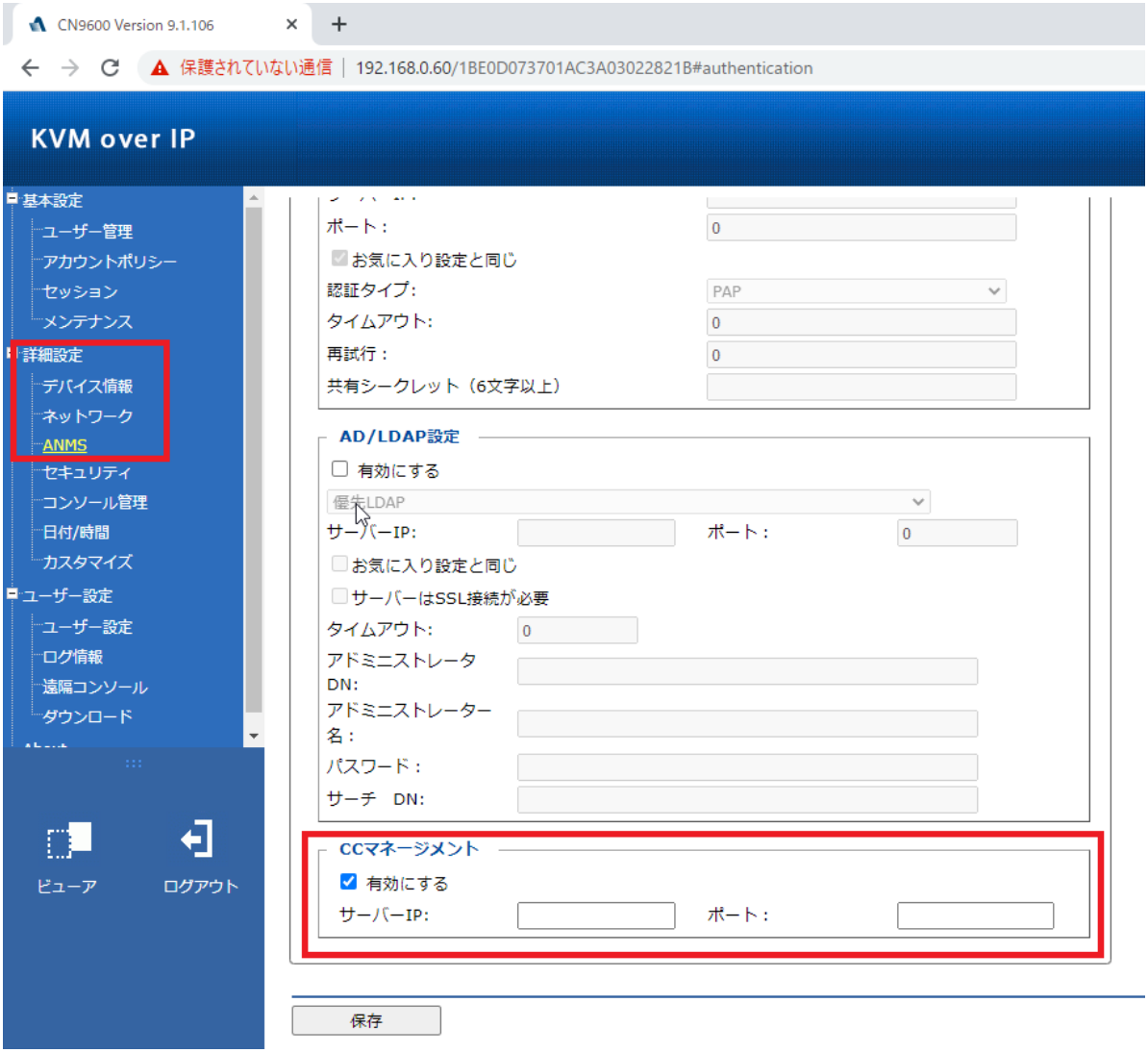
- CC2000で登録するKVM製品を設定します
- この設定をしないと、CC2000の管理画面からデバイスが発見できません

CN9600にログインする

- リモート端末から、ブラウザーを利用してCN9600にログインします
- テスト構成ではCN9600のIPアドレスは192.168.0.60ですので「https://192.168.0.60」でアクセスします
- 初回ログイン、パスワード変更についてはCC2000の初回ログイン時と同じため割愛します

「CCマネジメント」の項目を変更する

- 左メニューにある詳細設定 > ANMSの「認証」タブで、CCマネージメントの項目を設定します
- 「有効にする」でチェックを入れます
- 「サーバーIP」には、CC2000がインストールされたサーバーのIPアドレス、今回は「192.168.0.100」と入力します
- 「ポート」には初期設定の「8000」と入力します
    - このポートは、CC2000のインストール時に確認する「Device Port」がこの設定に該当します
- 画面下の「保存」ボタンをクリックして設定を反映させます。保存直後からCC2000がデバイスを検出できます。



KNシリーズの場合

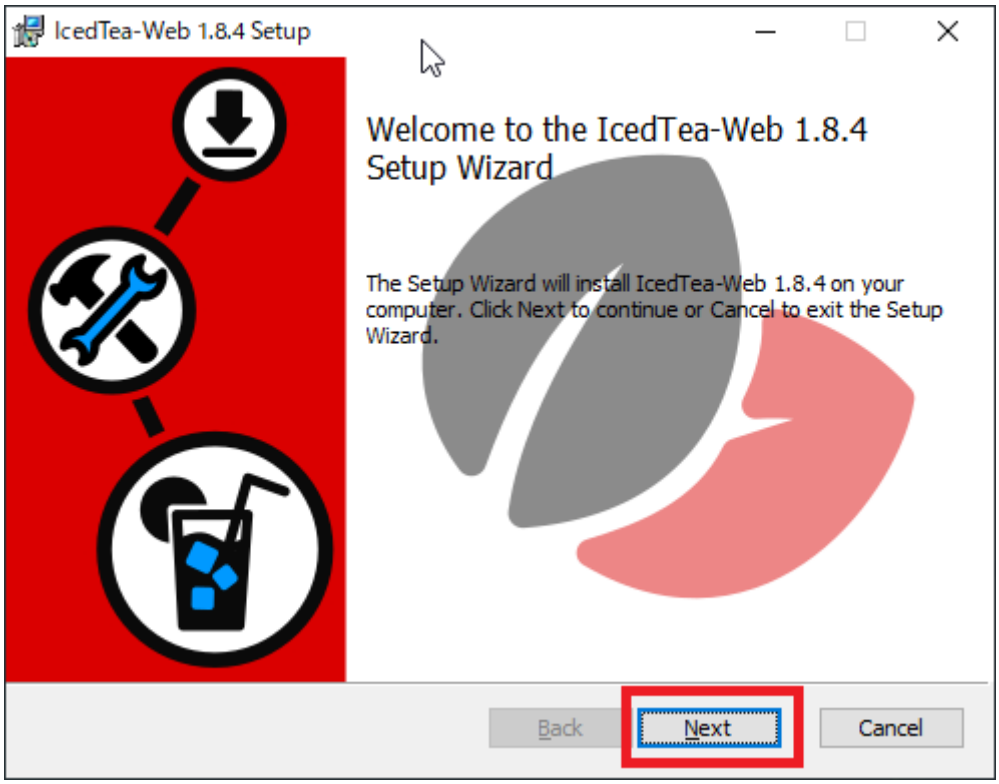
- KNシリーズでも同様の項目があります
- リモート端末でログイン後、「Device Management > AMNS >認証」にて、CCマネージメントの項目があります
- 入力する内容はCN9600と同じで、IPアドレスとポートを登録して「保存」ボタンをクリックすると準備が完了します

リモート端末をセットアップする

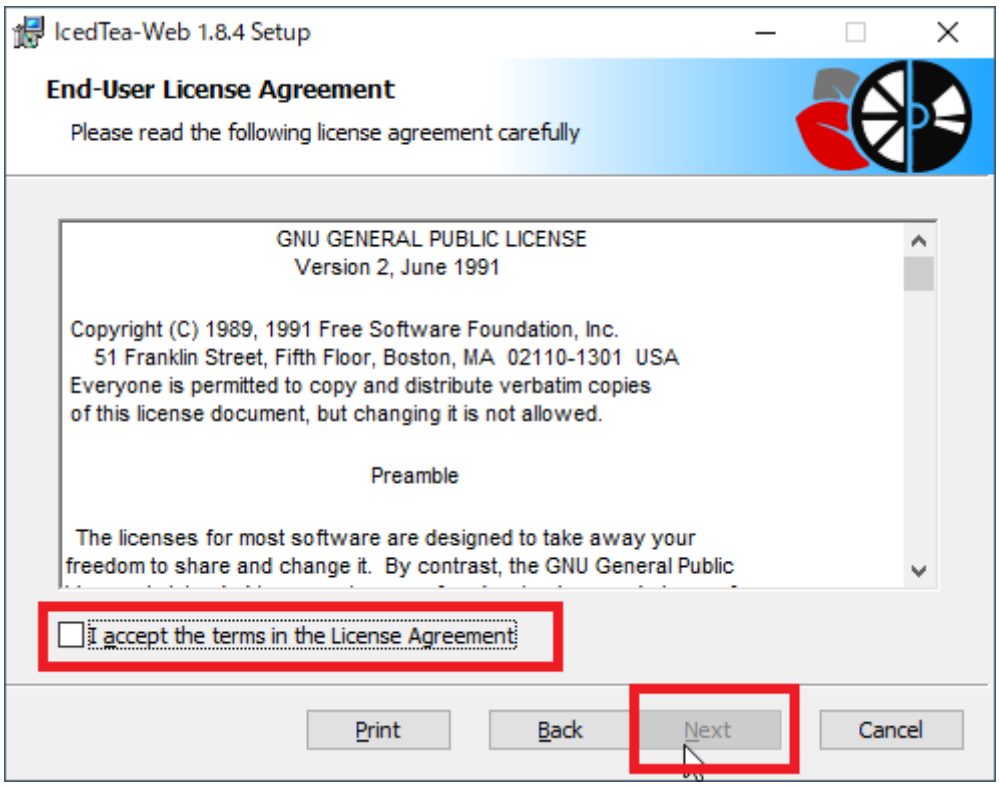
- IE11が利用できない場合は、「Iced-Teaをインストールする」を参照しセットアップしてください
- IE11が利用できる場合、事前の設定は不要です。「リモート端末でCC2000へログインする」以降を参照して進めてください

Iced-Teaをインストールする

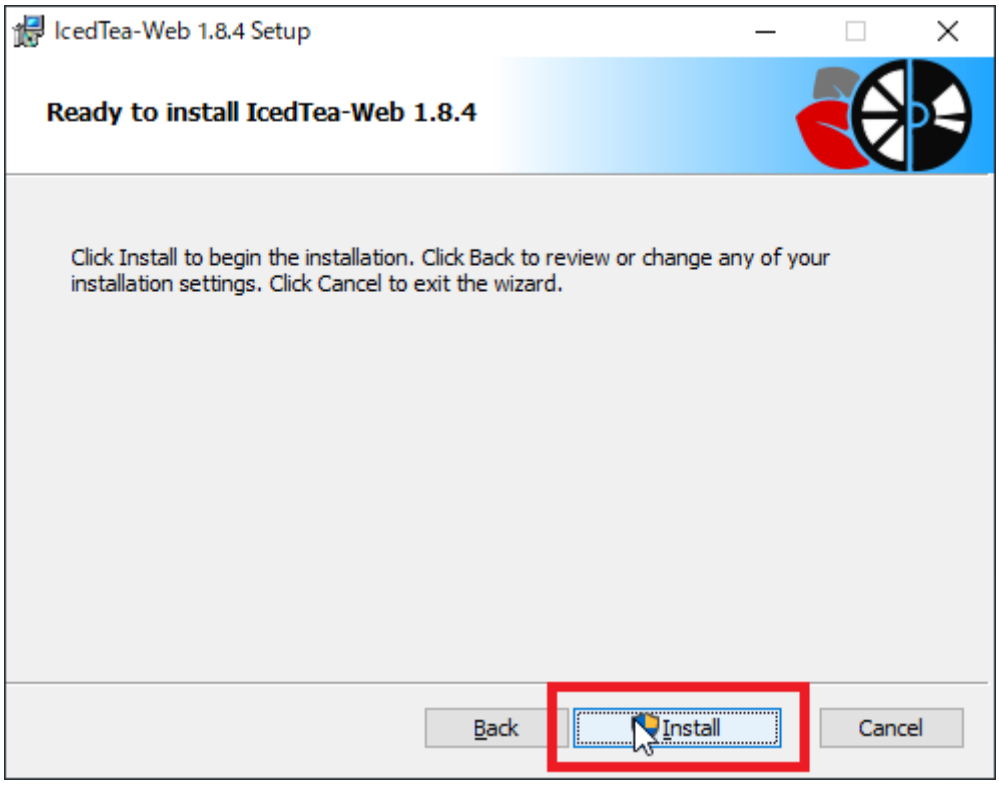
- IE11が利用できない場合は、以下の手順でセットアップしてください
- Iced-Teaとは、ブラウザと連携してJavaのプログラムを実行させるランタイムです(Oracle Java / web startのオープンソース版です)
    - **Iced-Teaをインストールする前に必ずZulu OpenJDKをインストールしてください**
    - 詳細は「ZuluOpenJDKをインストールする」をご参照ください
- Azul Zuluのページにある「Iced-tea」をダウンロードします
- https://www.azul.com/downloads/icedtea-web-community/
- 2021年3月時点で1.8.4が最新版なので、x86_64bit版のmsiファイルをダウンロードします
- ダウンロードしたmsiファイルを右クリックで「インストール」を選択します
- 「Next」をクリックします



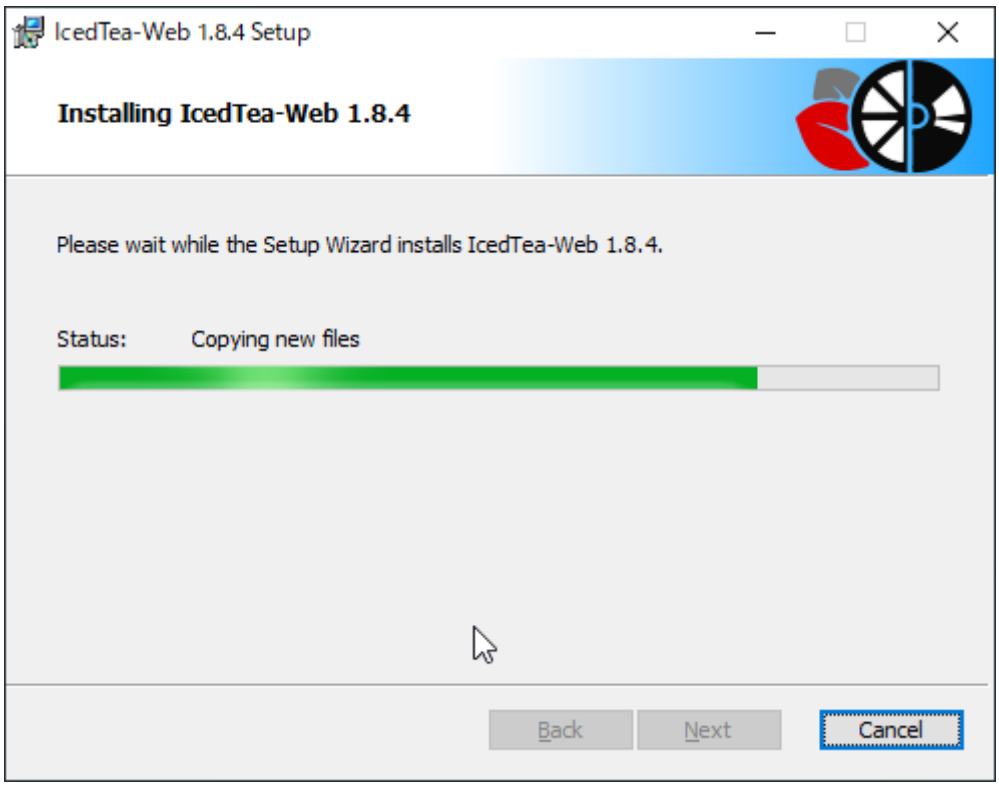
- ライセンス契約を確認し、チェックを入れたら「Next」をクリックします



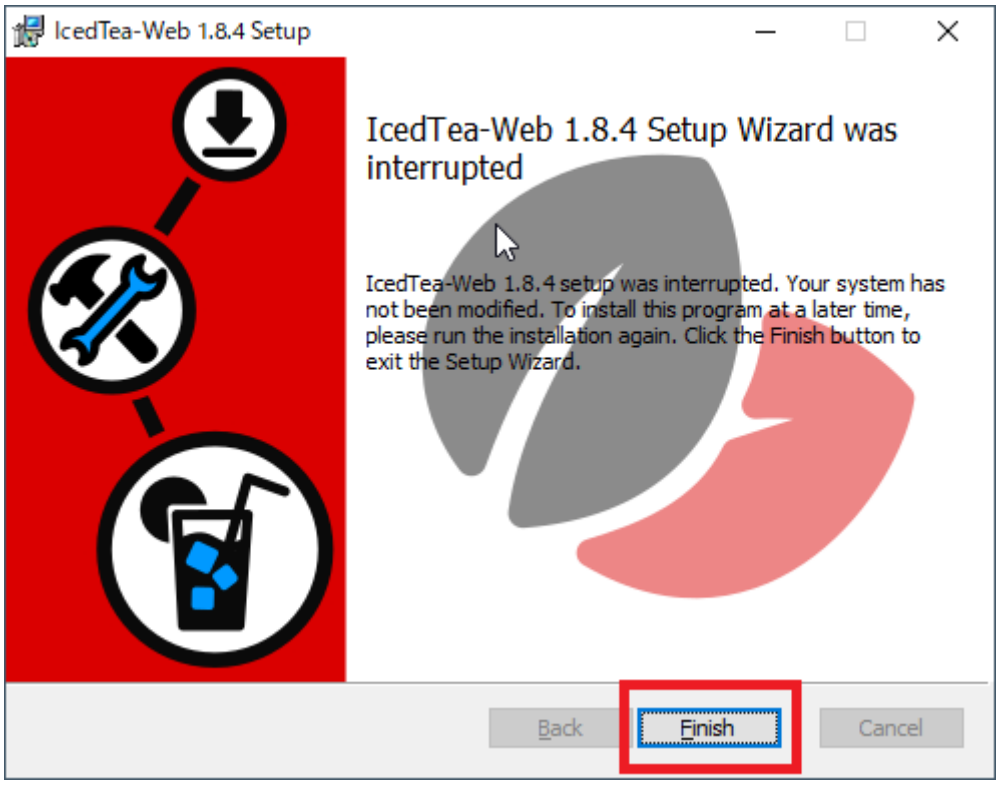
- 「Install」をクリックします



- データコピー/セットアップが完了するまで待ちます



- セットアップが完了したら「Finish」をクリックします



- これでリモート端末のセットアップは完了しました

リモート端末でCC2000へログインする

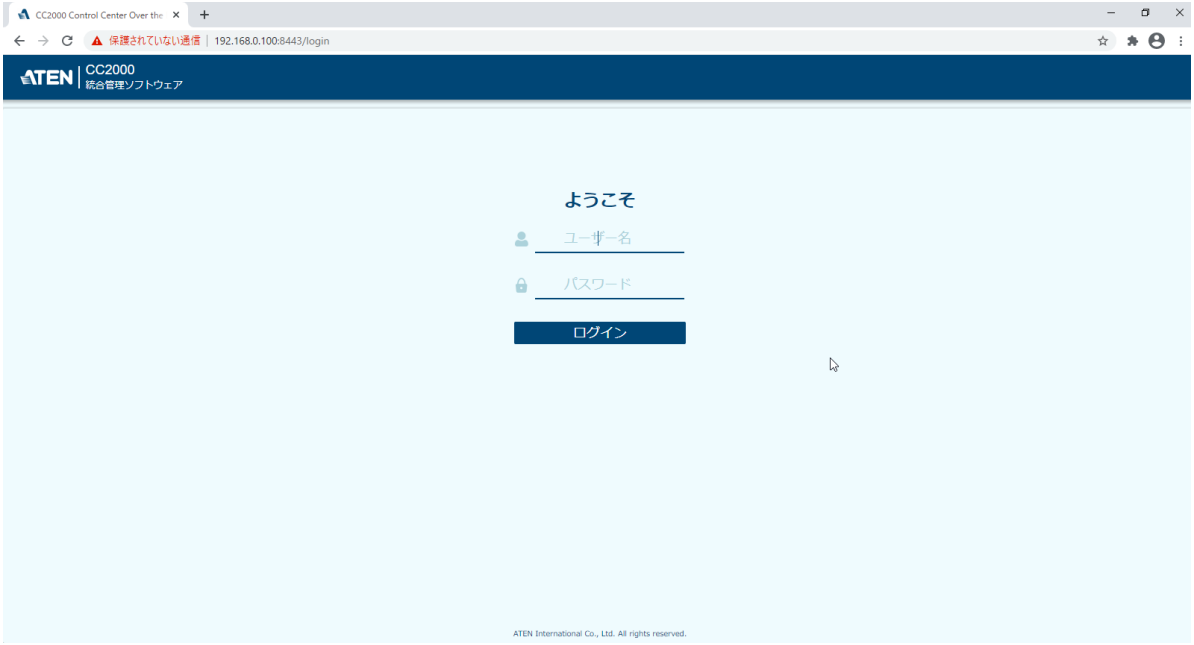
- リモート端末のブラウザは以下のいずれかをご利用ください
    - Microsoft Internet Explorer : バージョン11
    - Google chrome : バージョン56以降
    - Mozilla Firefox : バージョン60以降
- Microsoft chromium版Edge : バージョン79以降

CC2000へのアクセス方法

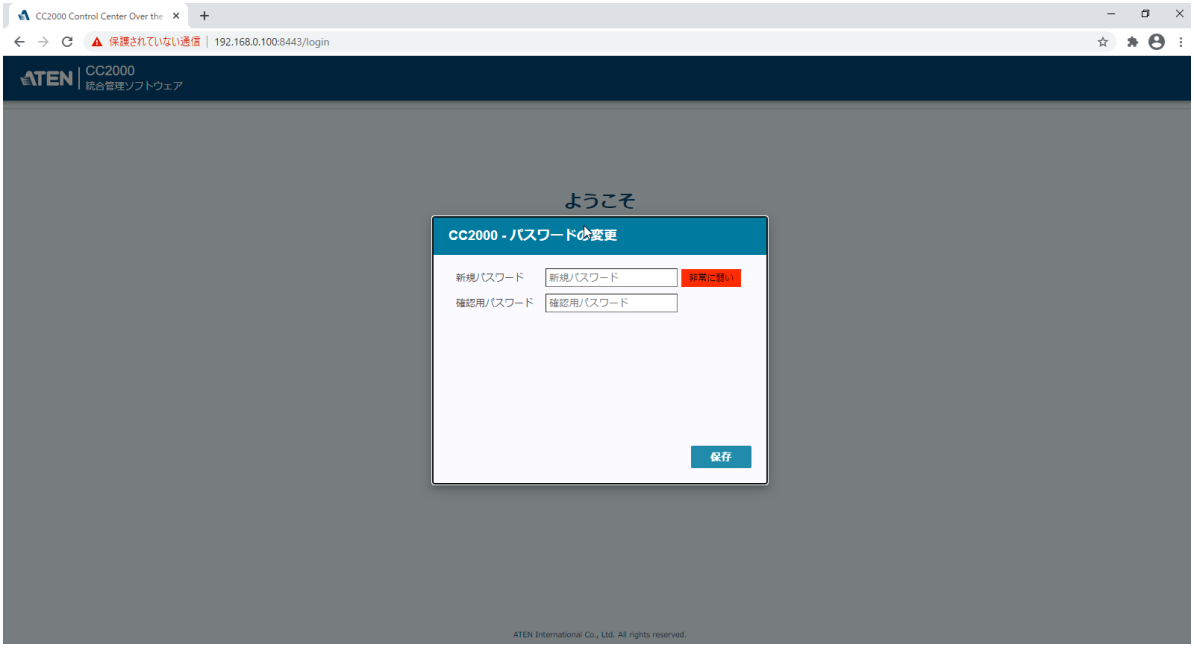
- リモート端末からアクセスする場合、今回のテスト構成ではCC2000がインストールされたサーバーのIPアドレス「https://192.168.0.100:8443」でアクセスできます
- CC2000が正しく起動した状態でアクセスすると「この接続ではプライバシーが保護されません」と警告されます
    - CC2000は初期設定では通信においてセキュリティを掛けていないため、このような警告が表示されますが問題ありません
        - 必要に応じてサーバー証明書をCC2000サーバーに組み込むことで、よりセキュアな接続が可能になります。詳細は製品マニュアルをご確認ください
- 「詳細設定」をクリックしてから「192.168.0.100にアクセスする(安全ではありません)」をクリックしてください

CC2000にログインする

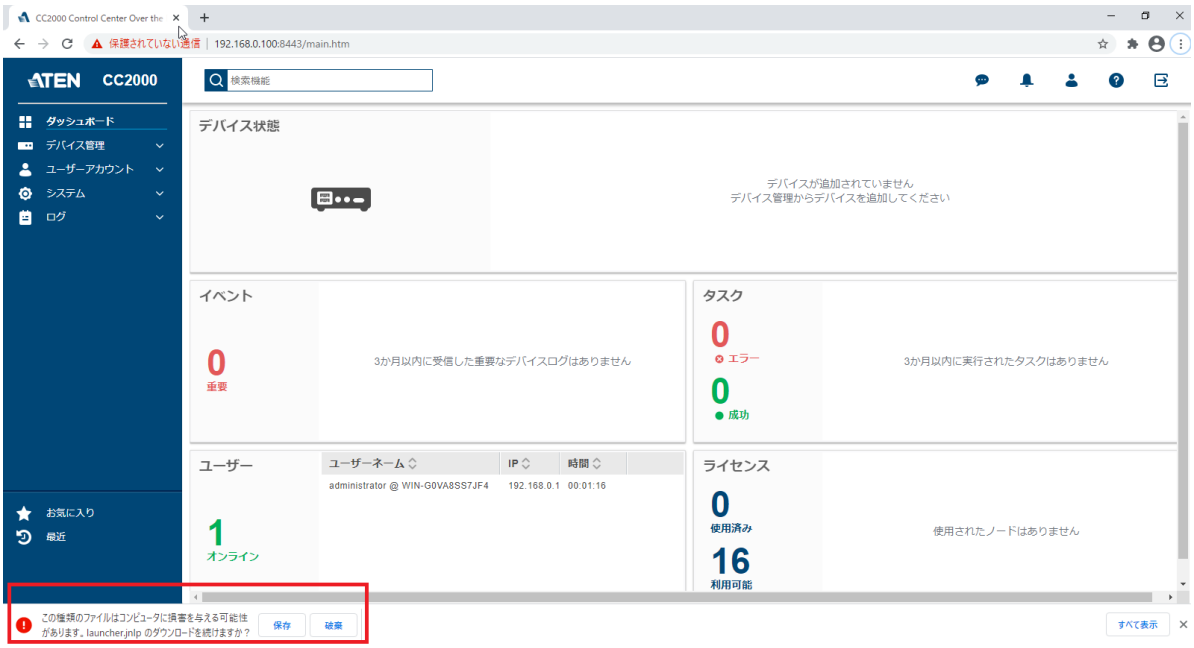
- 初期設定ではユーザー名は「administrator」、パスワードは「password」でログインできます



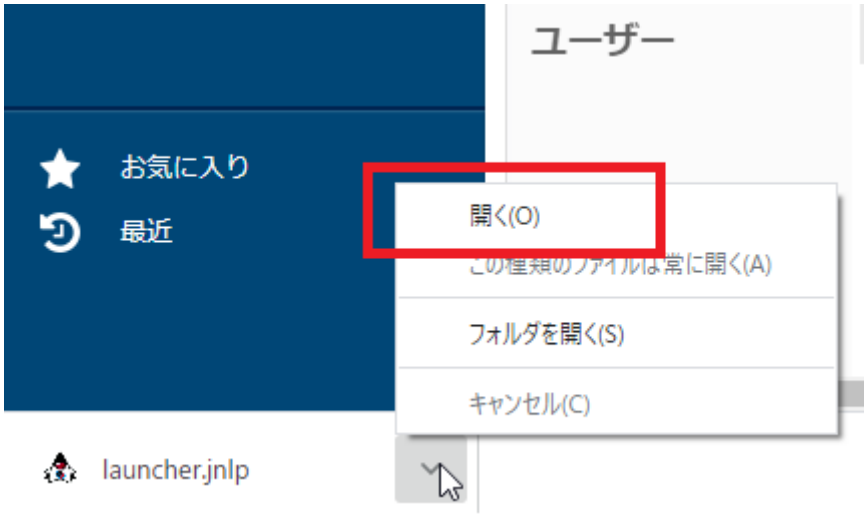
- GPDR/CCPA(カリフォルニア州消費者プライバシー法)に準拠するため、初回ログイン時にはパスワードを必ず変更する必要があります
- 任意のパスワードに変更してから「保存」をクリックします



- ログインに成功すると、ダッシュボード画面に進みます。この画面はCC2000の稼働状態のサマリを表示しています
- 管理画面にて動作に必要なプログラム「launcher.jnlp」を自動的にダウンロードします
- このプログラムはログインに成功するとそのログインごとにプログラムを生成するので、セッションが終了したら削除してください
    - 削除しないでも継続して利用は可能ですが、その場合は必ずログイン時にダウンロードしたlauncher.jnlpを起動させてください

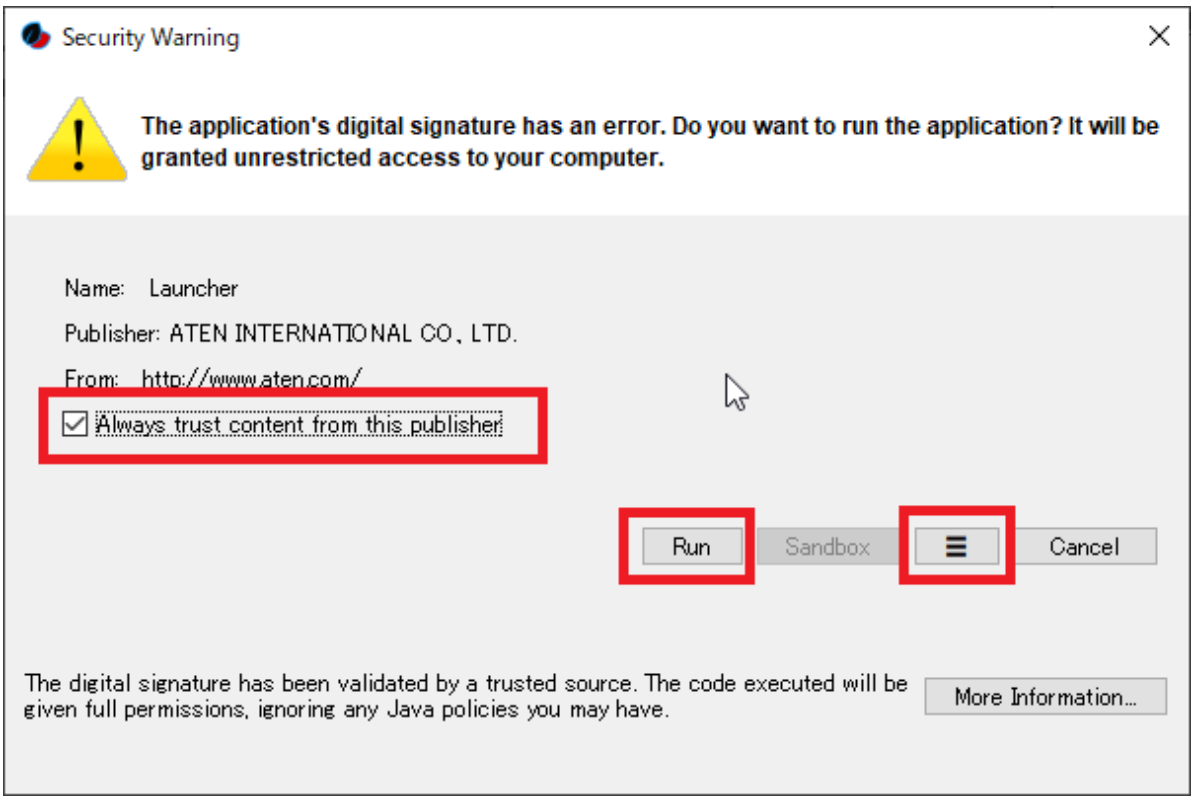


- ダウンロードしたら、「開く」を選択します

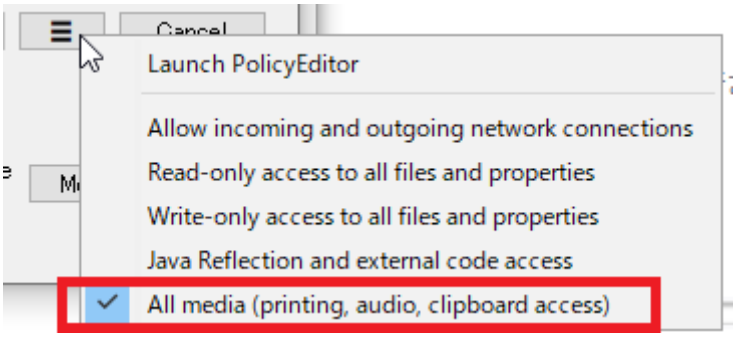


- Iced-teaを正しくインストールできているとプログラムの起動画面が表示されます
- 「起動できない」、「起動するためのプログラムを要求された」場合は、リモート端末にIced-Teaをインストールされていません。
    - Iced-Tea単体ではなく、Zulu OpenJDKもインストールが必要です

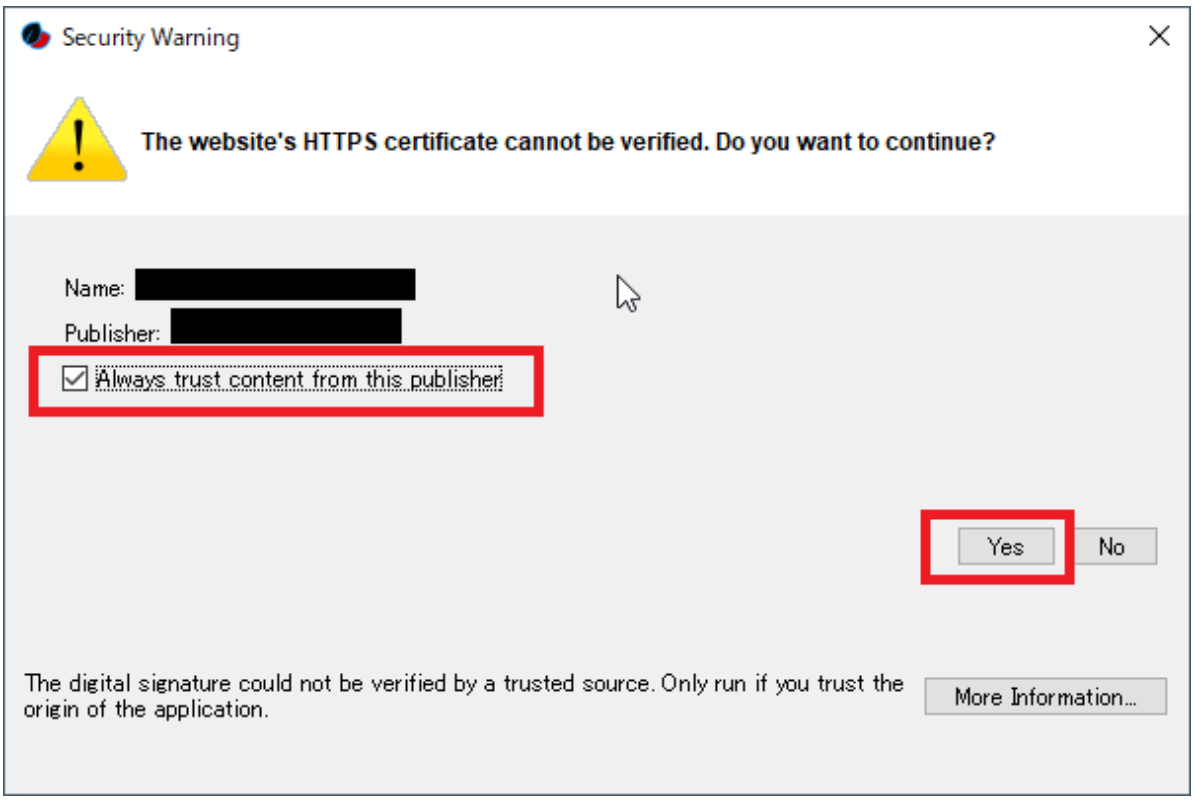
- 起動時にセキュリティ警告が表示されます
- この時、「Always trust content from this publisher(発行元を常に信頼する)」にチェックを入れておくと次回以降の起動でこの確認画面を回避できます
    - リモート端末のセキュリティ設定によっては、チェックを入れてもこの確認画面を表示することがあります
- 起動時の設定をするため「 ☰ 」をクリックします



- 起動時のオプションで「All media」を選択します。これをチェックしない場合、CC2000専用リモートデスクトップクライアント「CCviewer」利用時に映像音声が出力できない、各機能が利用できない不具合の原因となります
- 選択した後に「Run」をクリックします



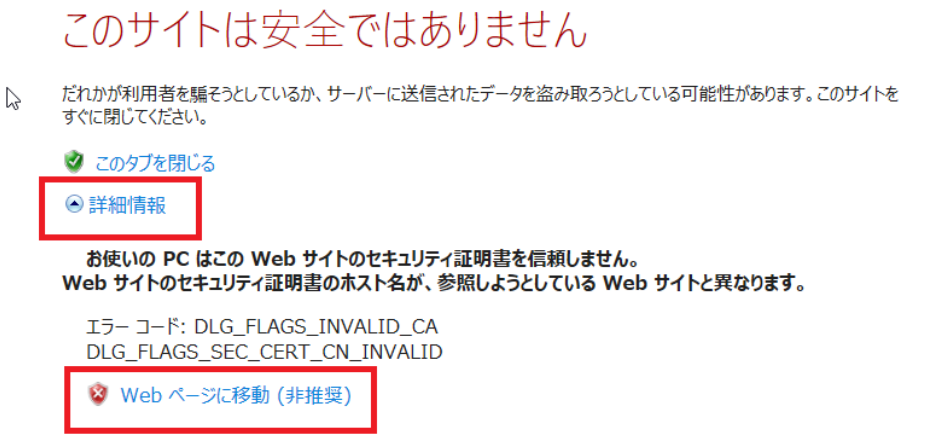
- 環境によって、通信先にセキュリティがないという警告が表示されます。この場合は、「Always trust content from this publisher(発行元を常に信頼する)」をチェックして、「Yes」をクリックします



- 起動が完了すると、バックグラウンドで管理画面などの処理をするため、画面は消えます
- これで、管理画面を操作する準備が完了しました

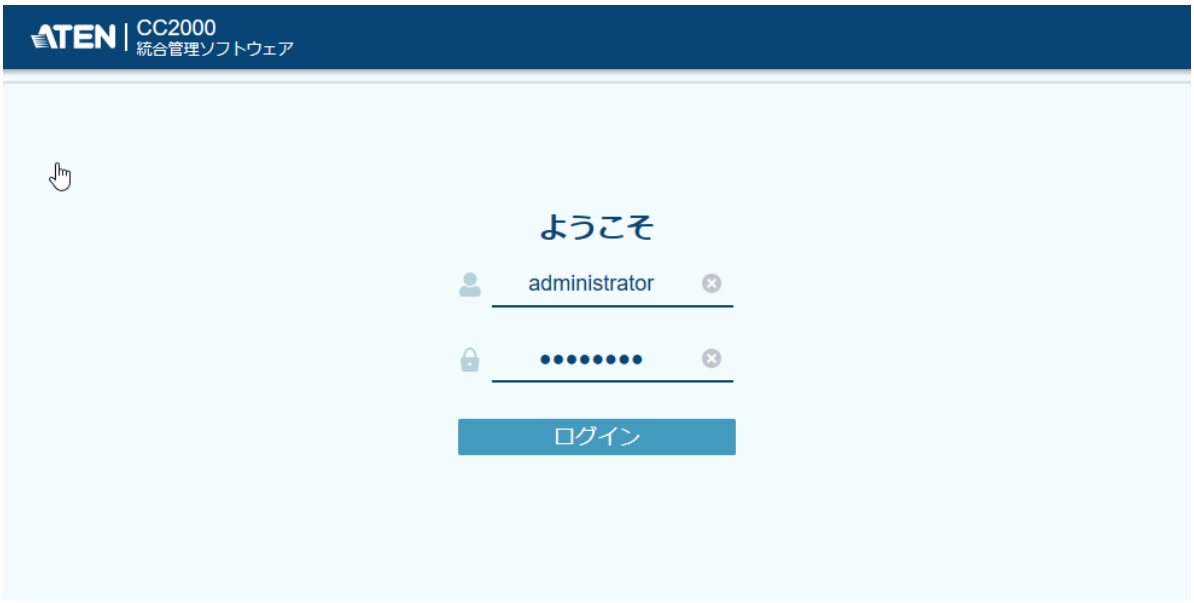
Internet Explorer11を使用した場合

- 今回のテスト構成で使用するCC2000がインストールされたサーバーのIPアドレス「https://192.168.0.100:8443」へアクセスします
- 「このサイトは安全ではありません」の「詳細情報」をクリックします
- 次に、「Webページに移動(非推奨)」をクリックします

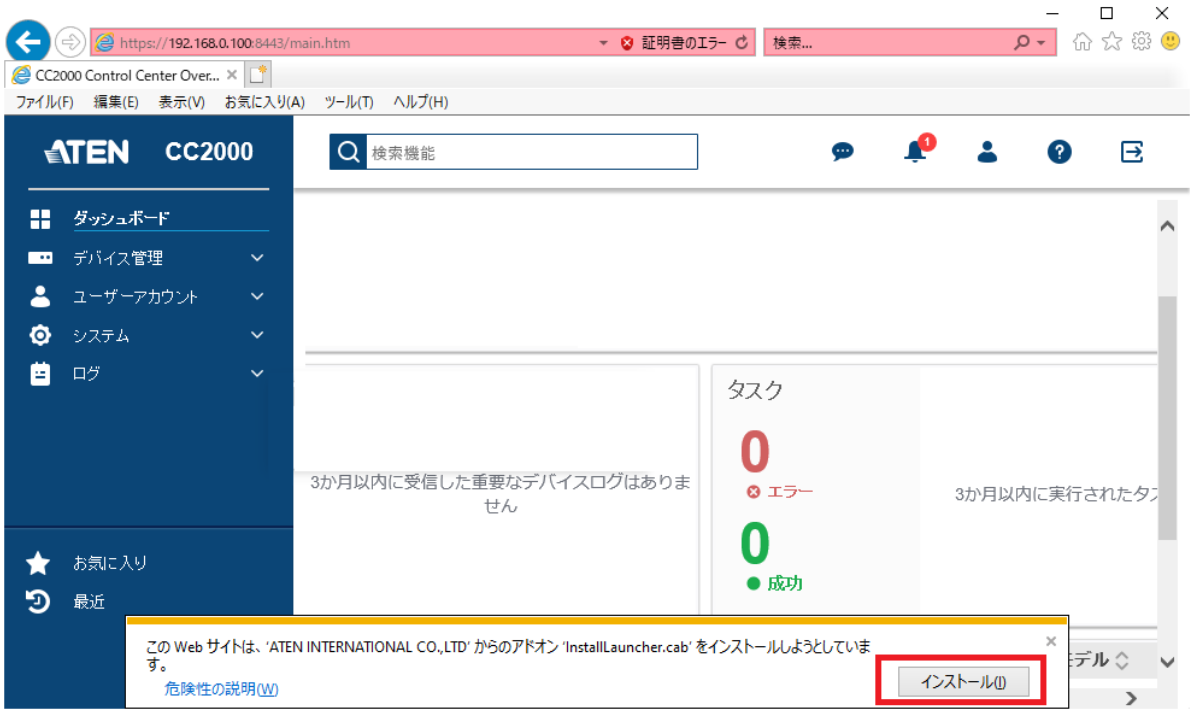


- CC2000は初期設定では通信においてセキュリティを掛けていないため、このような警告が表示されますが問題ありません
    - 必要に応じてサーバー証明書をCC2000サーバーに組み込むことで、よりセキュアな接続が可能になります。詳細は製品マニュアルをご確認ください
- 初期設定ではユーザー名は「administrator」、パスワードは「password」でログインできます

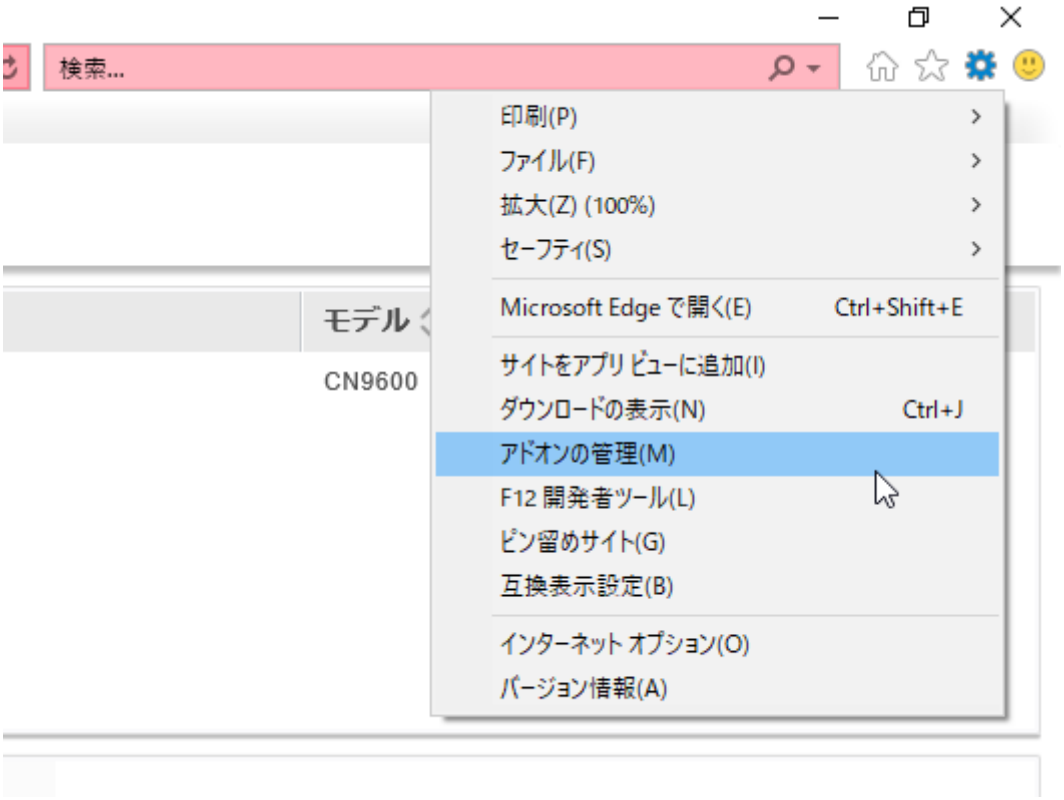
- GPDR/CCPA(カリフォルニア州消費者プライバシー法)に準拠するため、初回ログイン時にはパスワードを必ず変更する必要があります
- 任意のパスワードに変更してから「保存」をクリックします



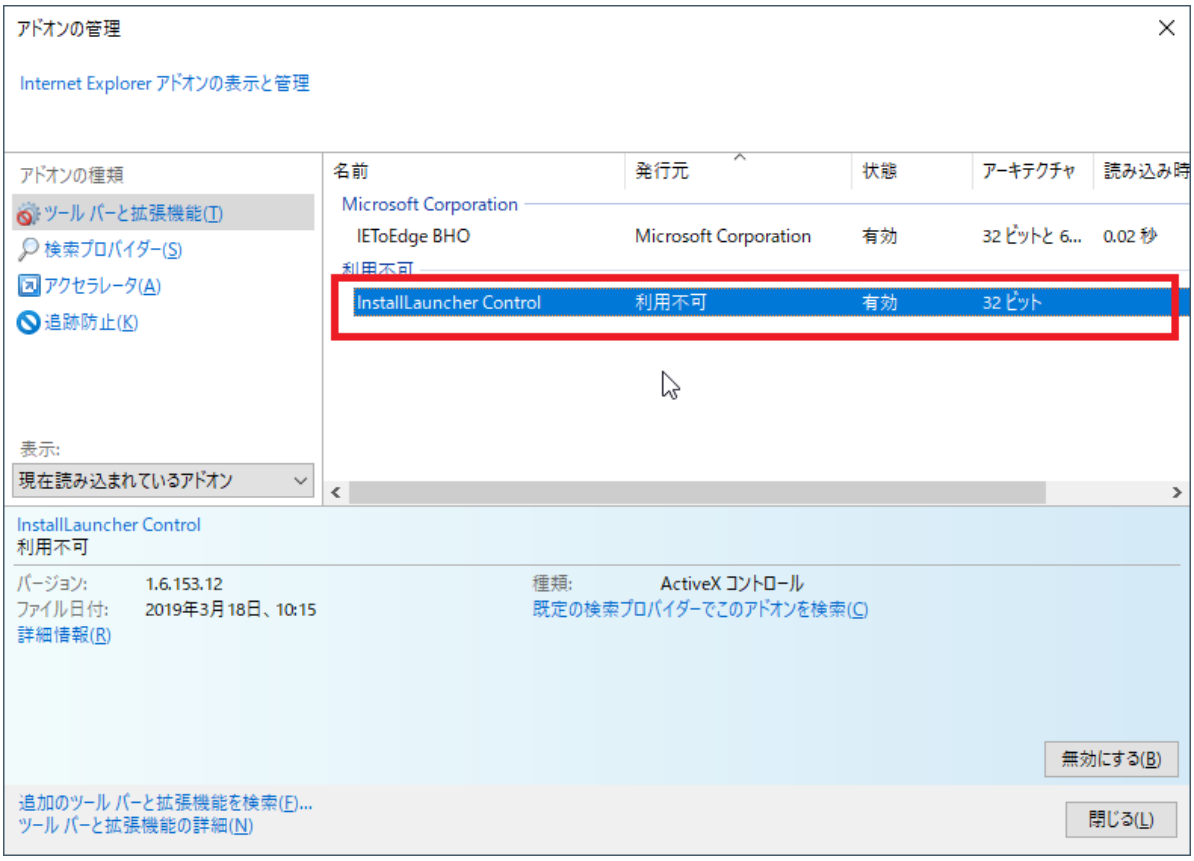
- 初回アクセスには、ActiveXアドオンのインストールを求められるので「インストール」をクリックします
- インストールが完了しても完了メッセージは表示されません。CC2000をログアウトして、Internet Explorerを再度立ち上げてログインしなおしてください



- 正しくインストールすると、「アドオンの管理」から確認できます。Internet Explorerのの設定から選択します



- 「InstallLauncher Control」の状態が「有効」になっていたら、リモート端末のInternet Explorer利用準備が完了です
    - リモート端末のセキュリティによってはActiveXのアドオンをインストールするには「Internet Explorerを管理者権限で実行する」「ドメイン管理者にインストール権限の許可をもらう」などの準備が必要なケースもございます

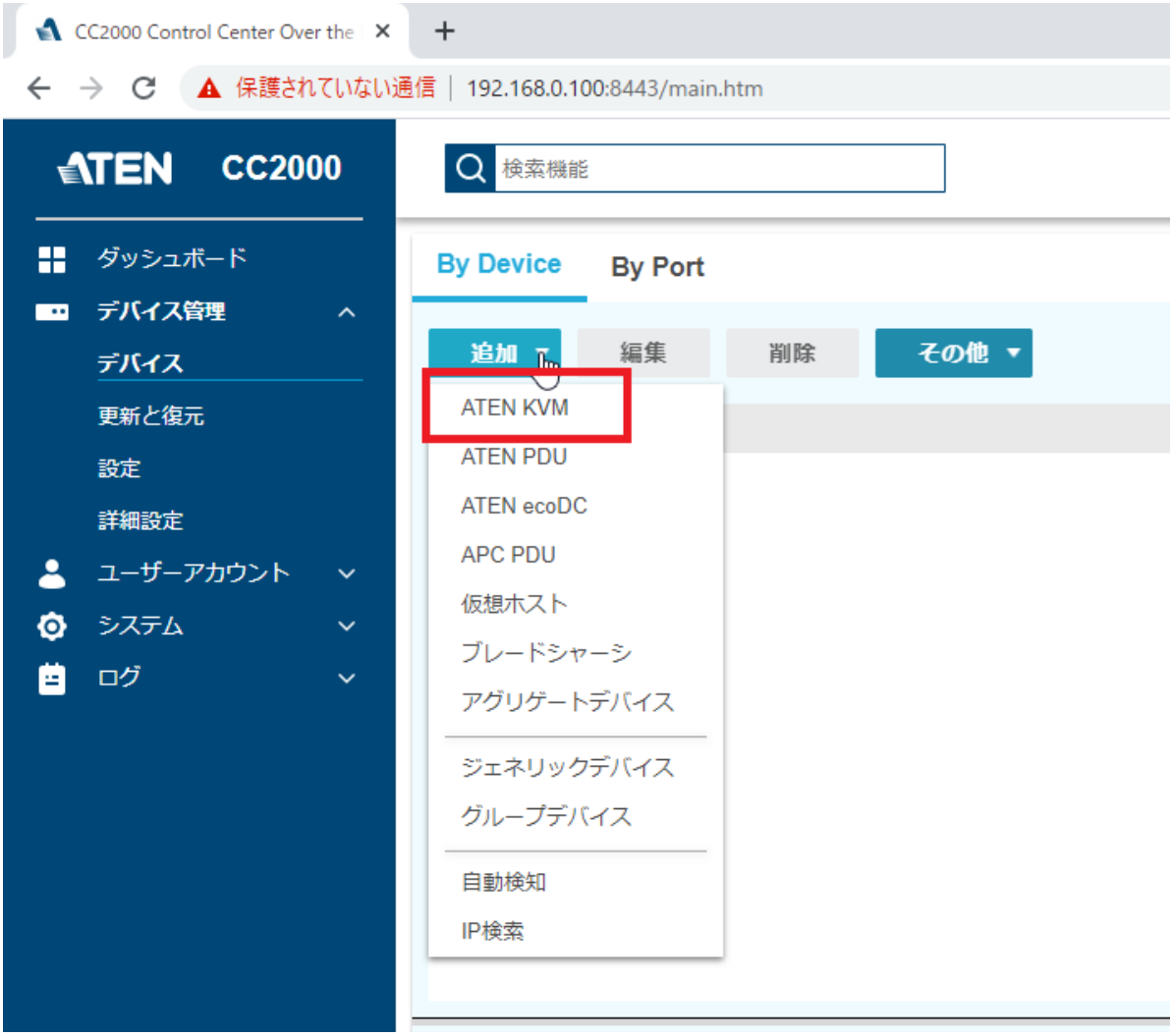


CC2000でCN9600を登録する

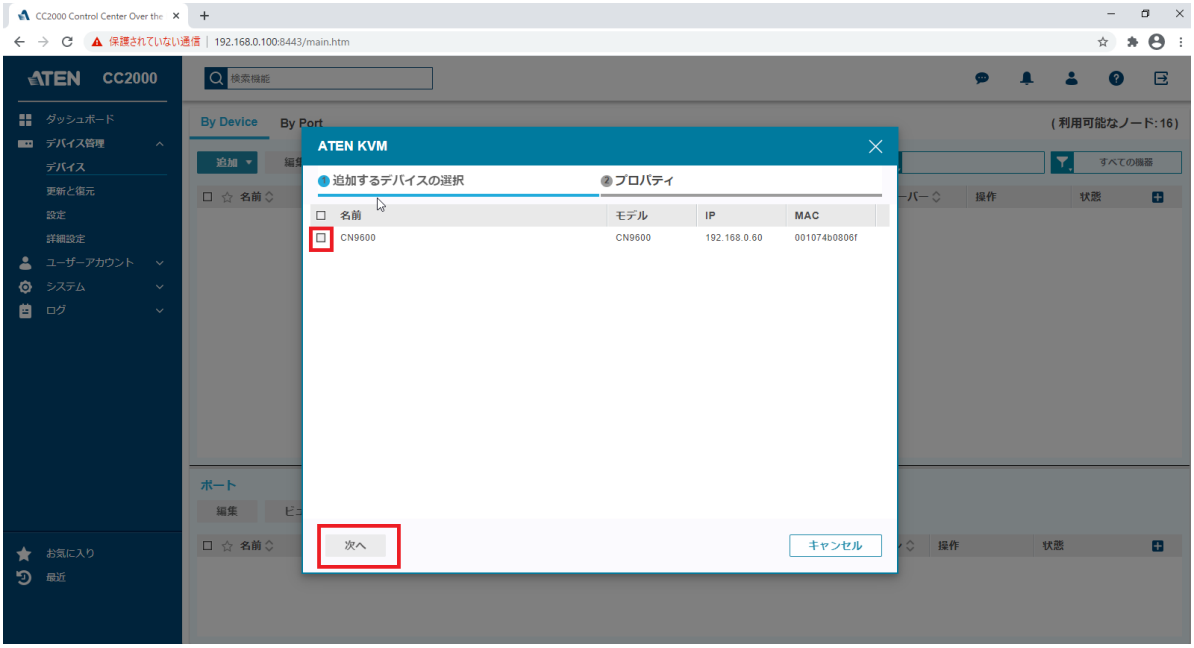
- ここからの手順は必ず、「CN9600を設定する」をしてから開始してください
- KVMスイッチを設定していない場合、登録できません

CN9600を検索して登録する

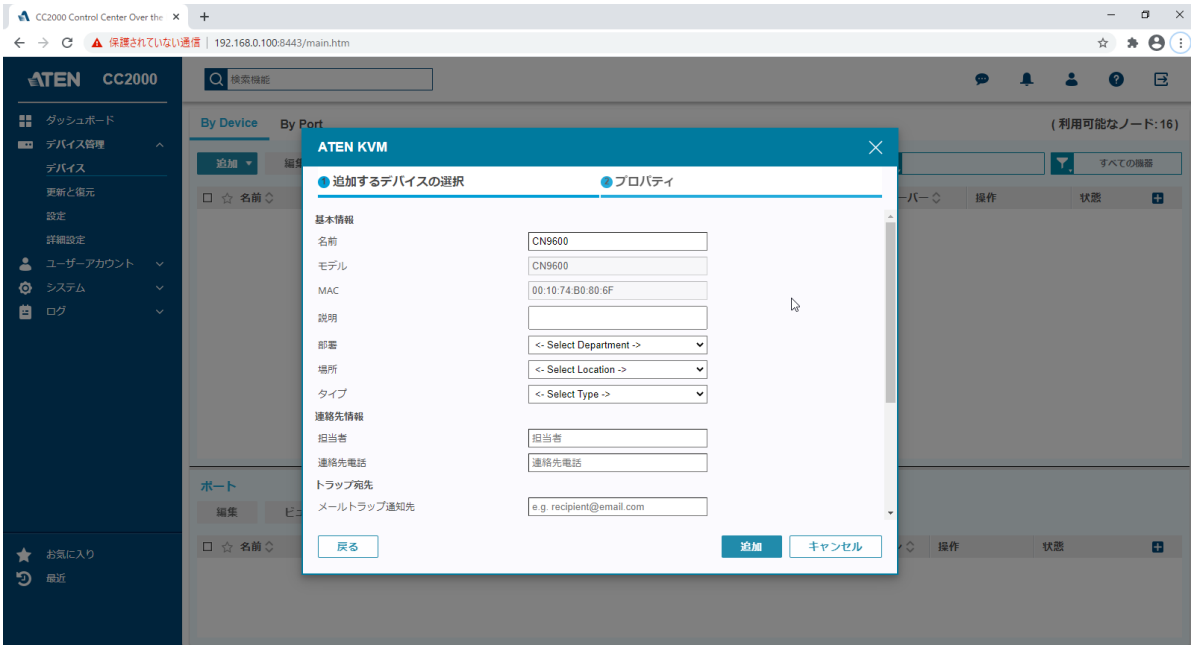
- リモート端末からCC2000の管理画面にログインします
- 左メニューの「デバイス管理 > デバイス」にある「By Device」の追加ボタンから「ATEN KVM」をクリックします
    - 対応機種を一括して登録する場合は「自動検知」からも対応デバイスを検出できます



- CN9600を設定していると、ここでリストに表示されます
    - CN9600の設定しているにもかかわらずCC2000から検出できない場合、CC2000をインストールしたサーバーやネットワーク機器のファイヤーウォールで8000番ポートを許可しているかご確認ください
- デバイス名の左にチェックを入れたら「次へ」をクリックします

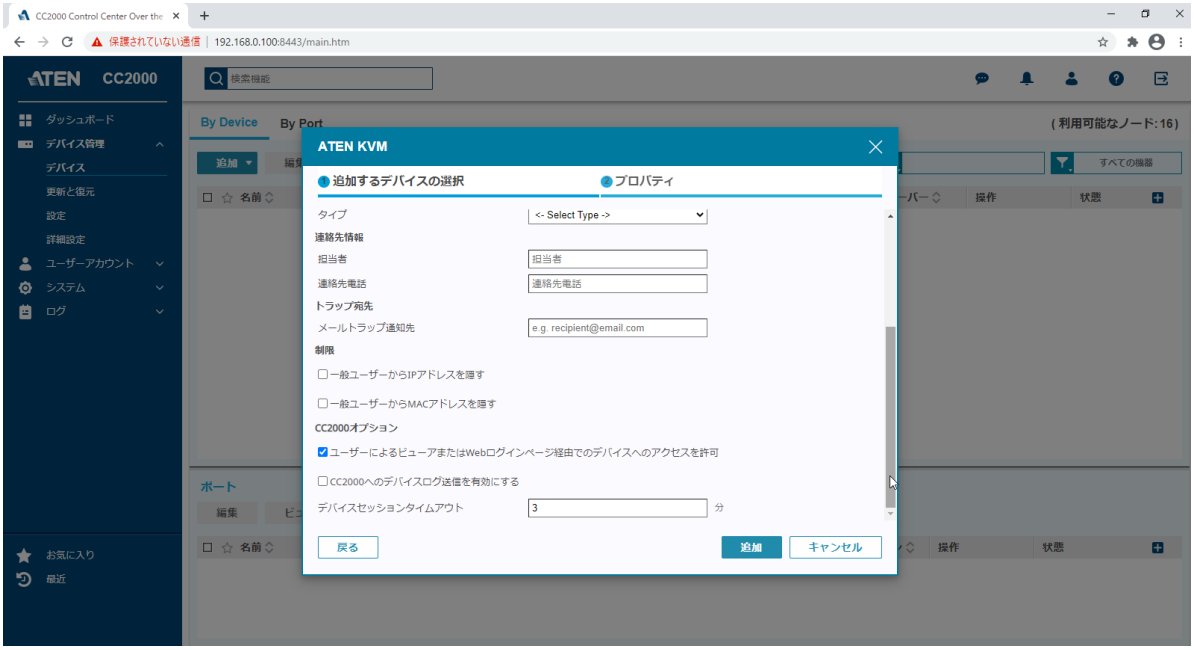


- 「追加するデバイスの選択」では、KVMデバイスの詳細情報を登録します
- この項目は割愛しても問題はありません
- 複数の機器を管理する場合は判別しやすくなるため、入力することを推奨します
- 下の設定項目を確認するため、画面をスクロールします

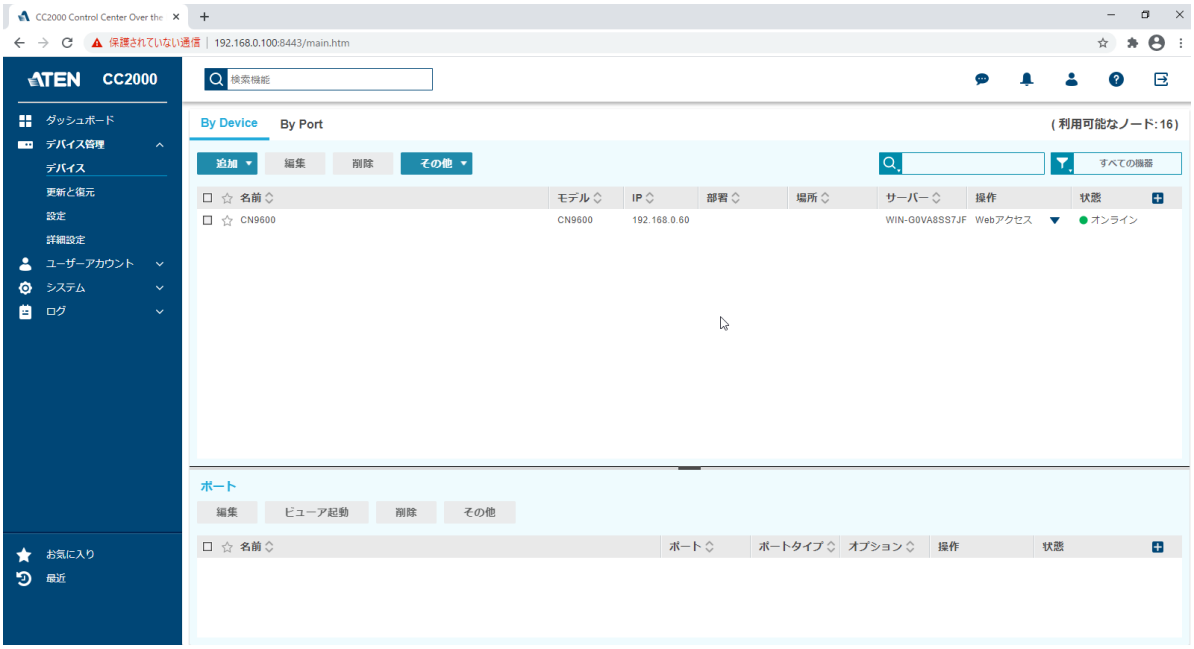


- 「CC2000オプション」の設定は次の通りです
    - 「ユーザーによるビューアまたはweb...」はリモート端末から、ブラウザーで直接CN9600へアクセスを許可するかの設定です
        - 直接アクセスを許可する場合は、チェックを入れます
        - CC2000からのアクセスだけを許可する場合は、チェックを外してください
    - 「CC2000へのデバイスログ送信を有効にする」は、KVMデバイスのログをCC2000へ自動的に送信する機能です
        - CC2000が各KVMデバイスのログサーバーの機能を持つことができます
        - ログをCC2000で保管する場合は、チェックを入れます
- 「デバイスセッションタイムアウト」はKVMにアクセスしているにもかかわらず無操作の状態が続いたら、自動的にビューワーを終了させて終了させる機能です。無効にする場合は「0」と数値を変更します

- 情報の入力が完了したら、「追加」をクリックします



- これで、CN9600のデバイス登録が完了しました
- KVMスイッチを追加登録する場合は、この操作を繰り返し行ってください



CN9600のロック解除をする

「ロック」の概念

- CC2000のライセンスの概念で「ロック(Lock)」というものがあります
- デバイスを登録やユーザーアカウントを作成するだけなら、制限はありません
- CC2000で「KVMスイッチにリモートからアクセスする」という機能に制限を掛けており、ライセンスキーを使って1つずつ制限を解除する必要があります。この制限を「ロック」を呼びます
- 評価版では「16ノード」分のライセンスがあり、KVMスイッチなら「1ノード = KVMスイッチの1ポート」という数値で換算されます。VMwareの仮想デバイスなら「物理サーバーで1ノード、ゲストOSひとつごとに1ノード」とライセンスを使用してロック解除できます。
- デバイス1台のポートをすべて開放する必要はありません。たとえば40ポートのKVMで10ポートしかサーバーに接続していない場合、評価版ライセンスで10ポート分のライセンスを使用し、残り6ノード分のライセンスをサーバーやKVMの増設時に使えます。
- CC2000は複数ライセンスがあるので、構築するシステムに応じたボリュームをお求めください
- 有償版は以下のライセンス形態があります

CC2000有償ライセンス形態

名称	型番	ノード数	プライマリサーバー数	セカンダリサーバー数
タイニー・パック	CC2000TN	32	1	なし
エクストラ・ライト・パック	CC2000XL	64	1	なし
ライト・パック	CC2000LE	128	1	なし
ライト・プラス・パック	CC2000LS	256	1	なし
スタンダード・パック	CC2000SD	512	1	1
プラス・パック	CC2000PS	2048	1	5
プレミアム・パック	CC2000PM	5120	1	9
プラチナム・パック	CC2000PL	無制限	1	15
マキシマム・パック	CC2000MX	無制限	1	31

- これらのライセンスを1つ購入するごとに、専用のUSBキーがお客様のお手元へ発送されます
- CC2000のサーバーにUSBキーを接続して、ライセンスを認証してください
    - リモート端末に接続してもライセンス認証はできないためご注意ください
    - 仮想環境では、VMware esxiではUSBデバイスが利用できることから認証できることを確認しています
    - しかし、Hyper-VのゲストOSそのままでは、ホストサーバーのUSBデバイスが利用できないため、CC2000のライセンスを認証できないことを確認しています。海外

では他社製のソフトウェア「USB redirector」を使用することで、Hyper-VのゲストOSでも認証ができたことを確認していますが、この方法につきましては、弊社ではサポート外、お客様の責任と判断にてご利用いただきますようお願い申し上げます。

- ライト・プラス・パック以下のライセンスそのままでは、CC2000を冗長サーバーに構築できません。オプションで1セカンダリー・サーバーライセンスを追加購入し、USBキーにデータを書き込むことで、利用が可能になります。USBキーは1つで、プライマリーとセカンダリーをそれぞれ認証できます
- 「ノード数」とは利用できるATEN製KVMのポート数または、APC製PDU、仮想サーバーなどの総称です
    - 例1 : CC2000の無償評価版ライセンスでは16ノードあり、次のような使い方ができます
        - CN9600を最大16台まで登録して使う
        - KN2116VAの全ポートを登録して使う
            - 合計16ポートが利用できるのでKN2116VAは4ポート、CN9600は3台、KN2132VAは5ポート、PE8108Aでは4ポート、といった使い方もできます

CC2000ライセンスアドオン形態

名称	型番	ノード数	プライマリサーバー数	セカンダリサーバー数
1セカンダリー・サーバー ライセンス	CCS1	なし	なし	1
1ノード ライセンス	CCN1	1	なし	なし
10ノード ライセンス	CCN10	10	なし	なし
50ノード ライセンス	CCN50	50	なし	なし
100ノード ライセンス	CCN100	100	なし	なし
500ノード ライセンス	CCN500	500	なし	なし
1000ノード ライセンス	CCN1000	1000	なし	なし
10000ノード ライセンス	CCN10000	10000	なし	なし
無制限ノード ライセンス	CCNU	無制限	なし	なし

- このライセンスアドオンは有償ライセンスの追加オプションとしての販売となります。単体での販売はできません
- すでに有償ライセンスを購入している場合は、ライセンスアドオンを購入して追加できます
    - 購入方法は弊社営業までお問合せください
- これらの追加ライセンスは、以下の用途にてご利用いただけます
    - CC2000で管理するKVMデバイスの数が少なくても、CC2000のサーバーは冗長構成にしたい
    - ライト・パックを使っていたのだが、KVMスイッチを増設する計画になり、ノード数が不足した

ロックを解除する

- リモート端末からCC2000の管理画面にログインします
- 「デバイス管理 > デバイス > By device」で、任意のデバイスの右通りにある「 ⋮ 」をクリックして「ロック解除」を選択します

- CN9600には、内部ポートでは「画面表示操作用ポート」と「シリアル通信ポート」の合計2つのポートがあるので、デバイスの全ポートのロックを解除すると2ポート使用します。
- 「利用可能なノード」として、現時点で利用できる残りの14ノード分を画面右上から確認できます
- もしもCN9600を使用しなくなった場合や、KVMスイッチを増設してノードが一時的に不足した場合には、**<u>同じ操作で「ロック」すると使用したノード数が返却されるため、他のKVMデバイスへ再利用できます</u>**

- ロック解除してからはじめて、ターゲットのサーバーへリモートアクセスができるようになります

特定のポートだけをロック解除する/ロックを掛け直す

- 「By Device」にて任意のデバイスをクリックすると、下の「ポート」に各デバイスで利用できるポートがリスト表示されます
- CN9600は「ポート1(KVM用途)」と「COM1(シリアル接続)」の、2ノードがリストに表示されます

- ポート名の右隣にある「 ⋮ 」をクリックして「ロック解除」を選択すると、1つずつロック解除できます
- ロック解除済のデバイスを選択すると「ロック」が選択できるので必要に応じて再度ロックを掛けてください

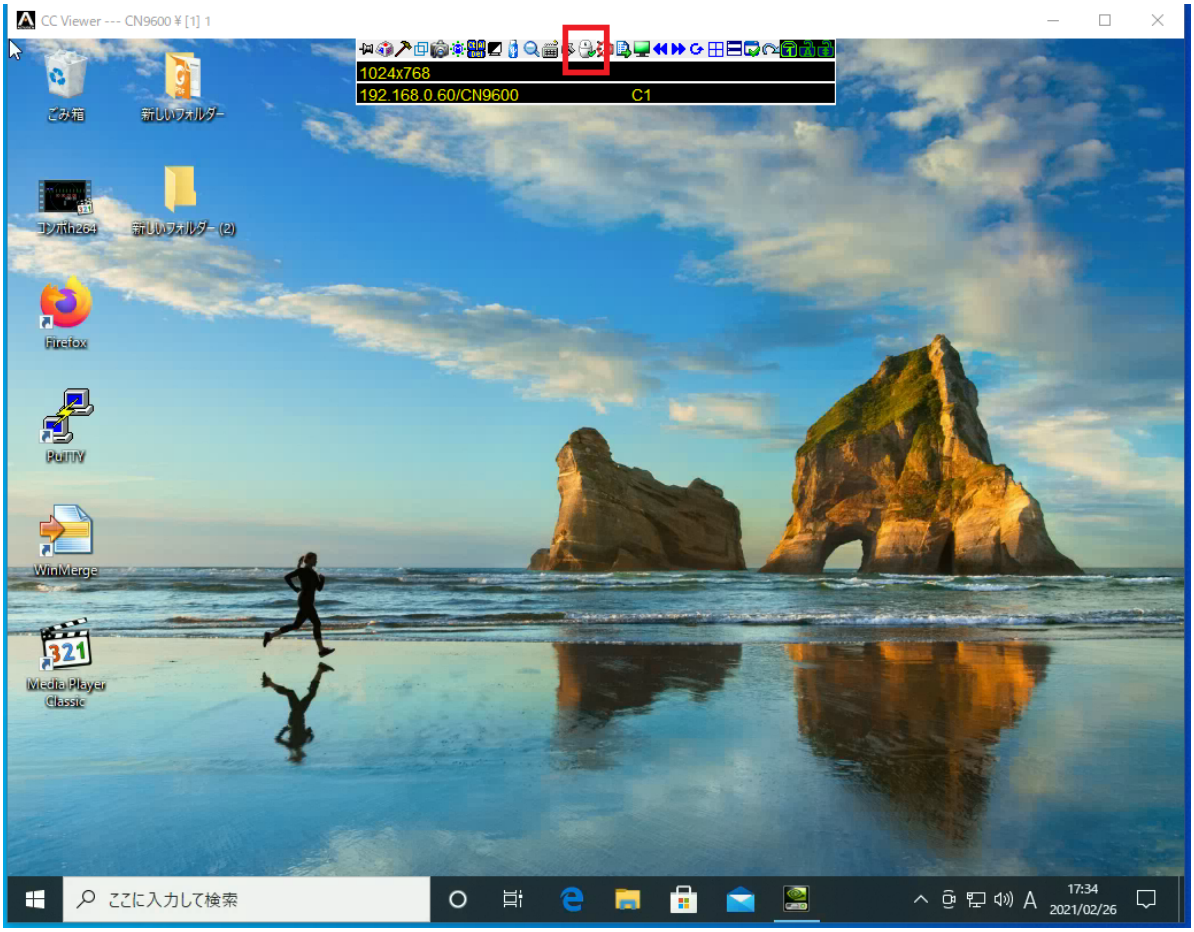
登録したKVMをリモートからアクセスする

- これまでにリモート端末から、CC2000経由でアクセスするには以下を設定しました
    - CN9600をCC2000に接続できるように設定する
    - CC2000でCN9600を登録する
    - CN9600のロックを解除する
- これ以降からは、リモート端末からアクセスする手順を紹介します
- 一般ユーザーアカウントでは、この段階ではまだ各KVMスイッチへのアクセス権限が設定されていないので、管理者権限でログインしてから各アカウントのアクセス権限を付与してください
    - 詳細の手順は「一般ユーザーアカウントを追加する」以降をご参照ください

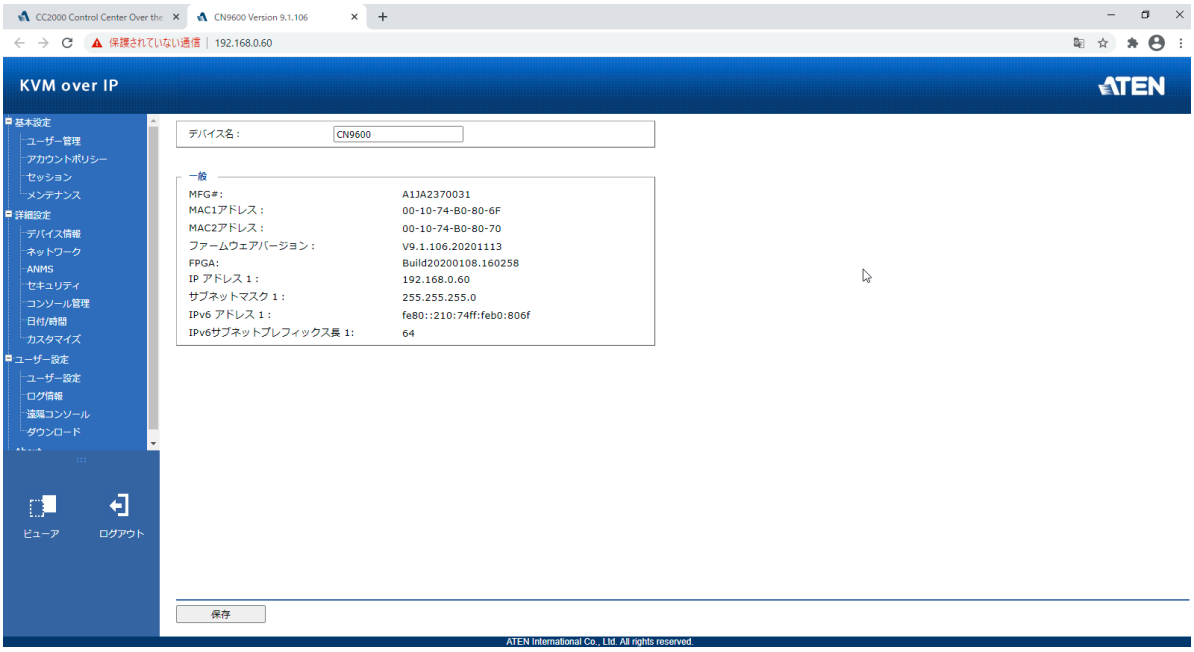
「デバイス管理」からデバイスの画面にアクセスする

- CN9600とDVI+USBケーブルで接続しているターゲットPCにアクセスするには、「デバイス管理 > デバイス > By Device」にある「操作」から「KVMビューワ」を選択します
- 操作の項目で「webアクセス」しかない場合、デバイスがロック解除されていないおそれがあります。解除してからアクセスしてください

- Iced-Teaが正しくインストールされ、ログイン時に「launcher.jnlp」を起動していれば、CN9600本体にアクセスして、次のようなリモート操作画面に進めます
- もしも、接続先のマウスカーソルが「ずれて移動する」「縦方向または横方向しか進まない」「反応しない」場合は、ウインドウ中央上部にあるツールバーの「  」をクリックし、マウスの動作モードを変更して改善されるかお試しください



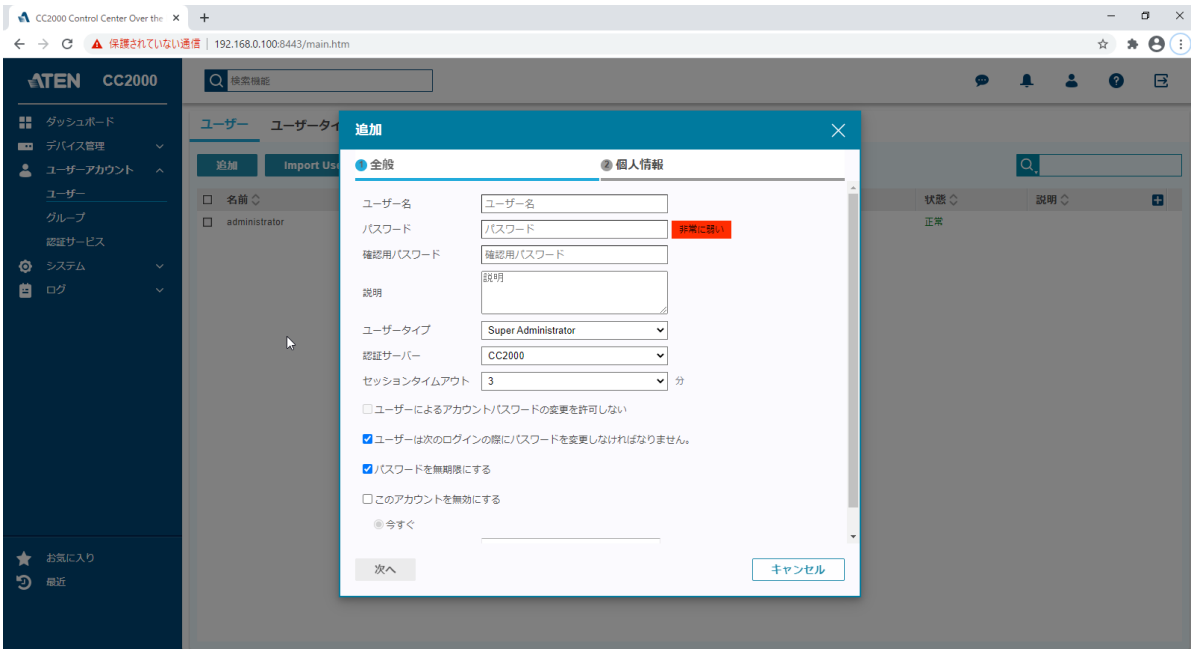
- CC2000の管理画面で「Webアクセス」を選択するとCN9600本体の設定画面に進めます
- この画面は、リモート端末から直接CN9600にブラウザーでアクセスした時と同じ画面です



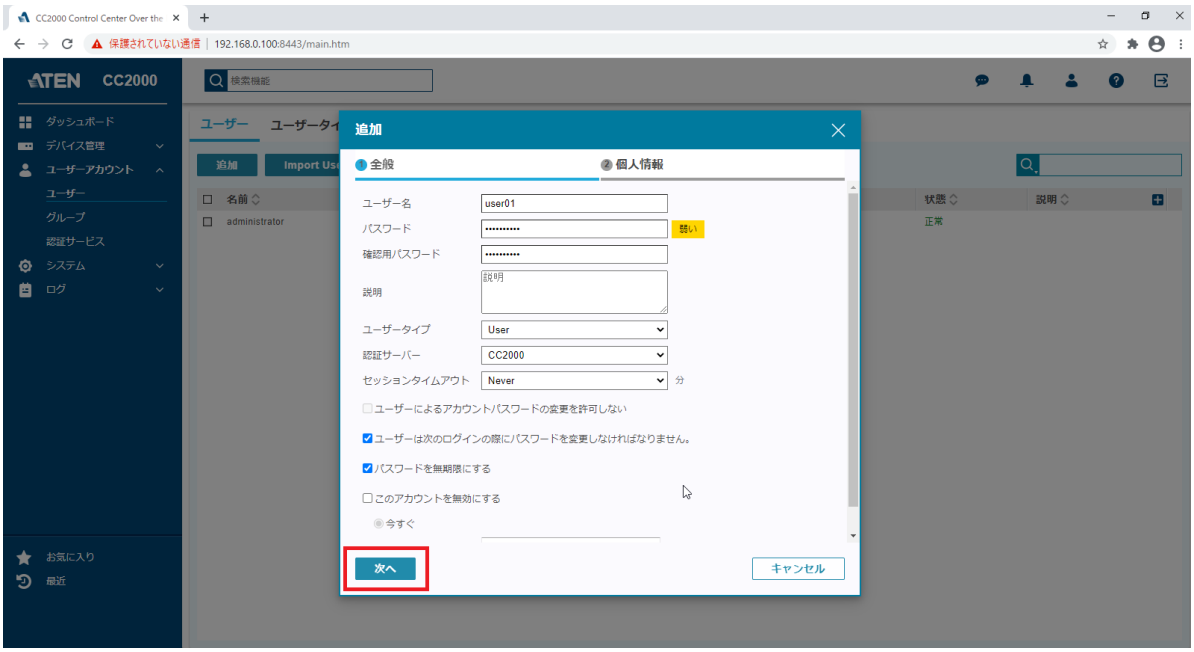
一般ユーザーアカウントを追加する

- 管理者アカウントでCC2000にログインします
- 「ユーザーアカウント > ユーザー」から「追加」をクリックします

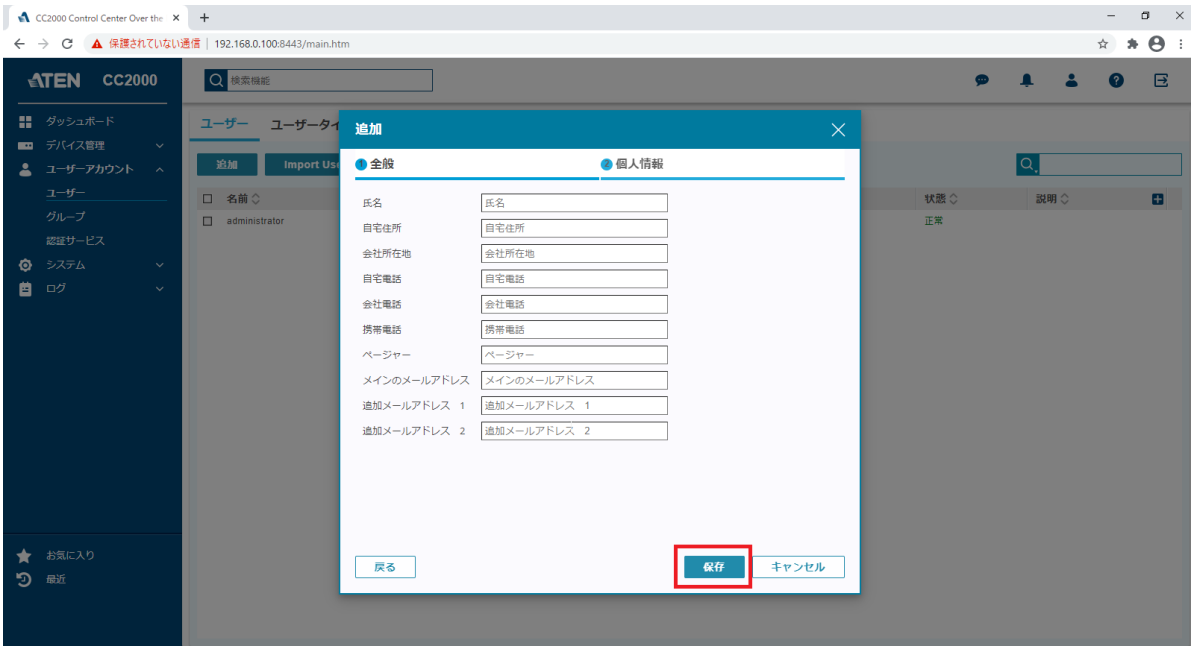
- 必須となる情報を入力します
    - ユーザー名(ログイン時に使用する文字列となります)
    - パスワード
    - ユーザータイプ
        - CC2000の各システム設定変更の操作権限を付与できます。初期状態では6種類のテンプレートがあり、独自の権限設定のテンプレート作成もできます
    - 認証サーバー
        - ユーザーアカウントを認証するサーバーを選択します。
            - CC2000 : CC2000に登録されているアカウント情報でアカウントを認証確認します(初期値)。外部認証サーバーを使用しない場合は、この設定のままで問題ありません
            - 「ユーザーアカウント > 認証サービス」にて登録すると、この項目にその認証サーバーを利用できます。認証サービスには、ActiveDirectlyなどが利用できます
    - セッションタイムアウト
        - 無操作の状態で設定した時間を超過すると自動的にCC2000からログアウトします。無効にする場合は「Never」とプルダウンから選択します



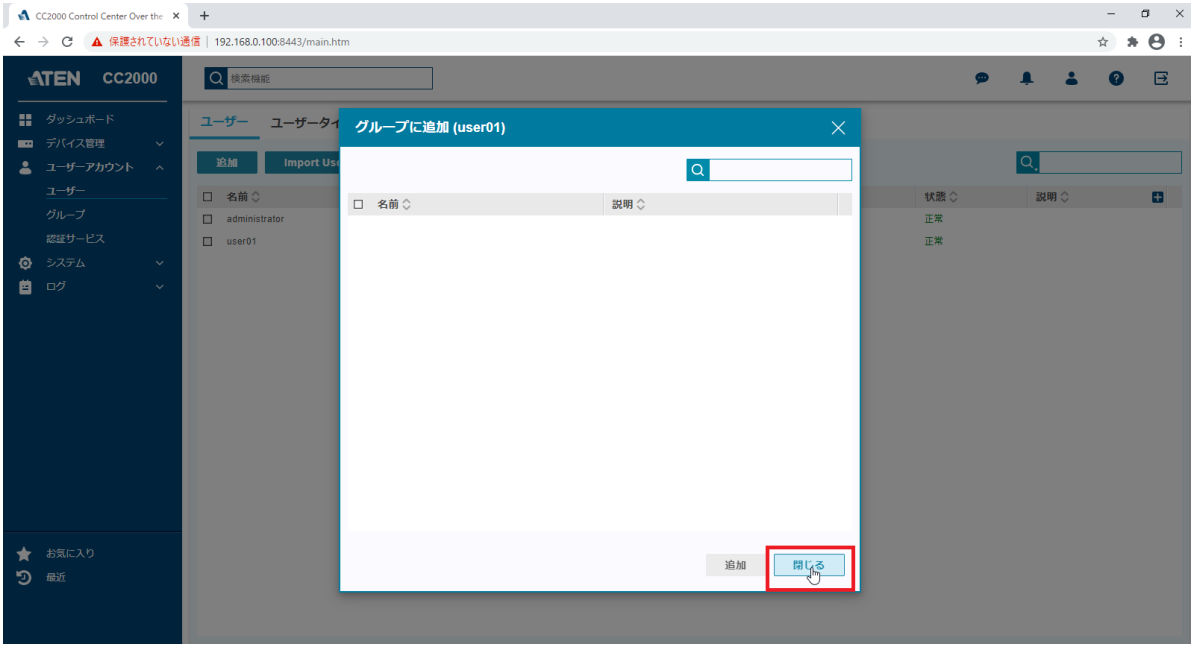
- 下図では例として「user01」というアカウントを作成しました
- 「次へ」をクリックします



- アカウントに追加の情報を付与する項目です
- 「個人情報」は必要に応じてデータを入力してください。入力しなくても問題ありませんが、多くのアカウントを作成する場合は、アカウントの取り違いや誤った設定変更などを抑止できるため入力することを推奨します。
- 保存ボタンをクリックします



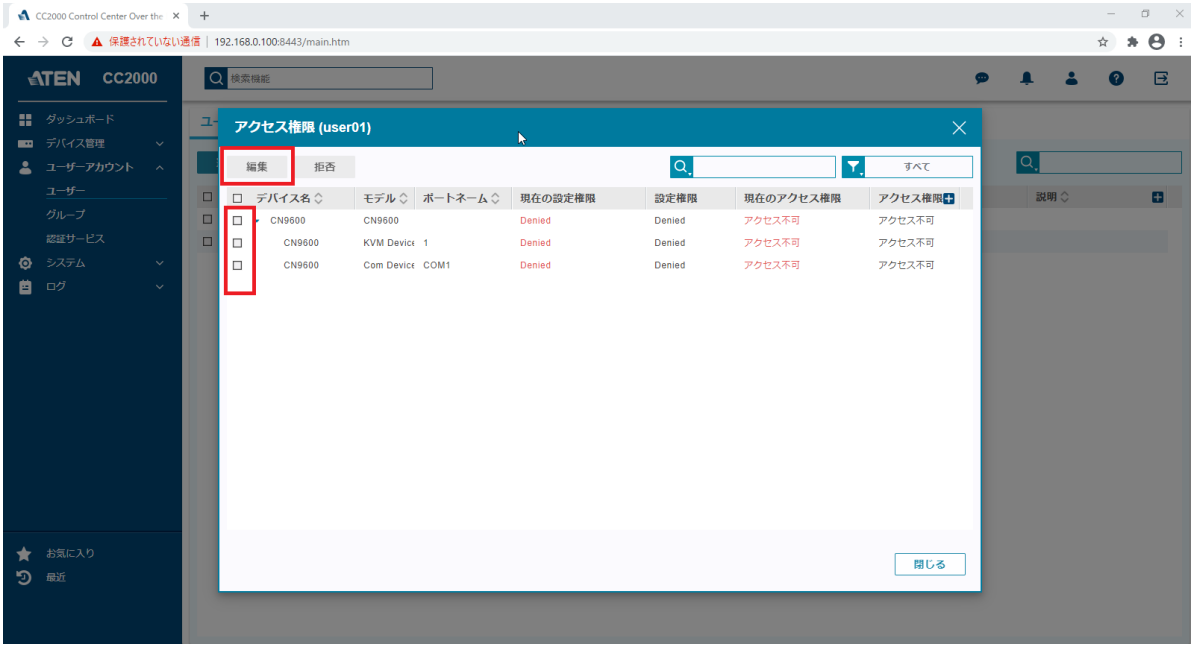
- 別途ユーザーグループがすでに作成されていると、この項目でどのグループに属するかを設定できます
- ユーザーグループは、複数のアカウントに同一の権限を付与できる設定です
- 「閉じる」をクリックすると、設定が完了します



アカウントにデバイスのアクセス権限を付与する

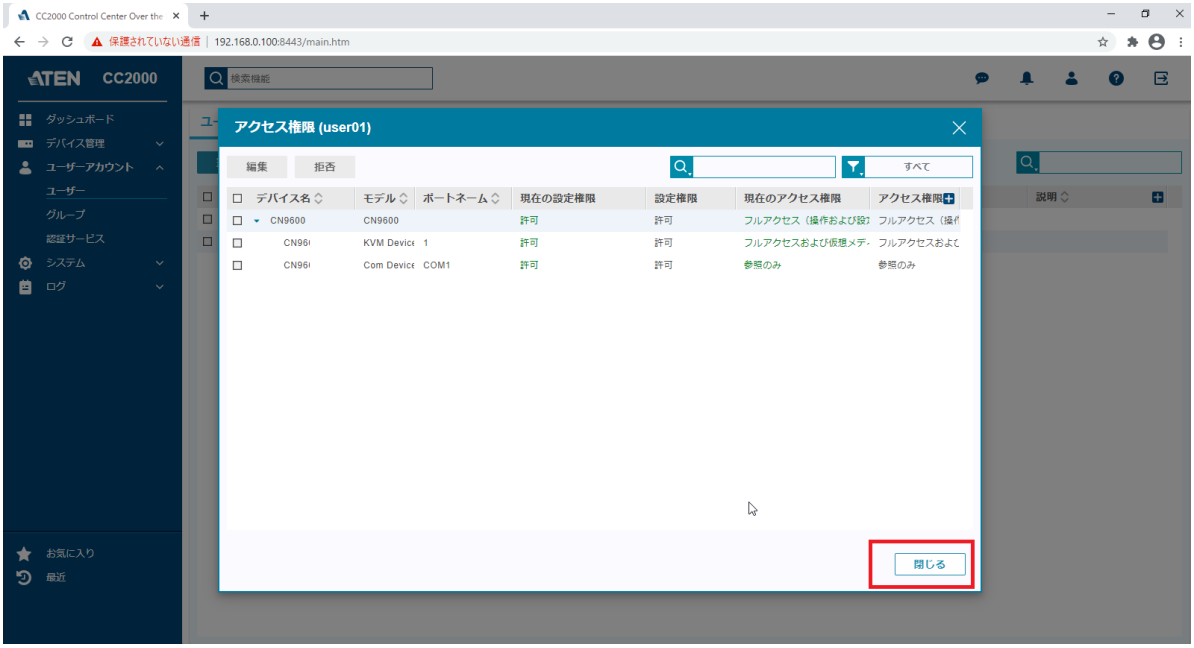
- アカウントを作成したら、アカウントごとにデバイスのアクセス権限を設定します
- 「ユーザーアカウント > ユーザー」で、任意のユーザーの項目にマウスカーソルを合わせると表示される「 」をクリックし、「アクセス権限」をクリックします

- アクセス権限を設定するデバイスがリスト表示されます
- 権限を開放する場合は、デバイス名の左をチェックして、「編集」をクリックします



- アクセスを許可する時にどの権限までを許可するか設定します
    - 設定権限 : KVMデバイス本体の設定権限を付与するかの項目です
    - フルアクセス : 画面表示 + キーボード + マウス操作
    - 仮想メディア : リモート端末に接続しているUSBメモリやHDD内のISOファイルなどを接続先のサーバーへマウントする機能
        - ストレージデバイスのみ対応です。タッチパネルや指紋認証デバイスなどはマウントして利用できません
- 設定が完了したら、「保存」クリックします

- 各ポートに対して設定が完了したら、「閉じる」をクリックします

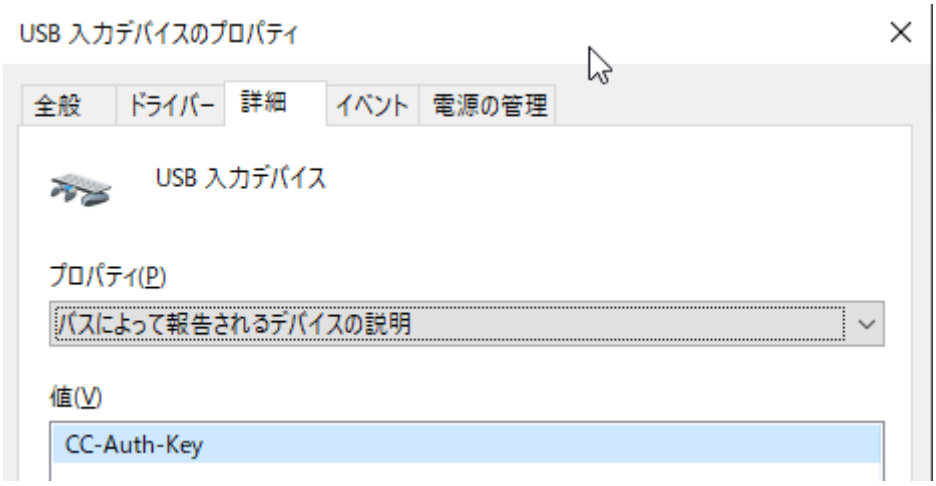


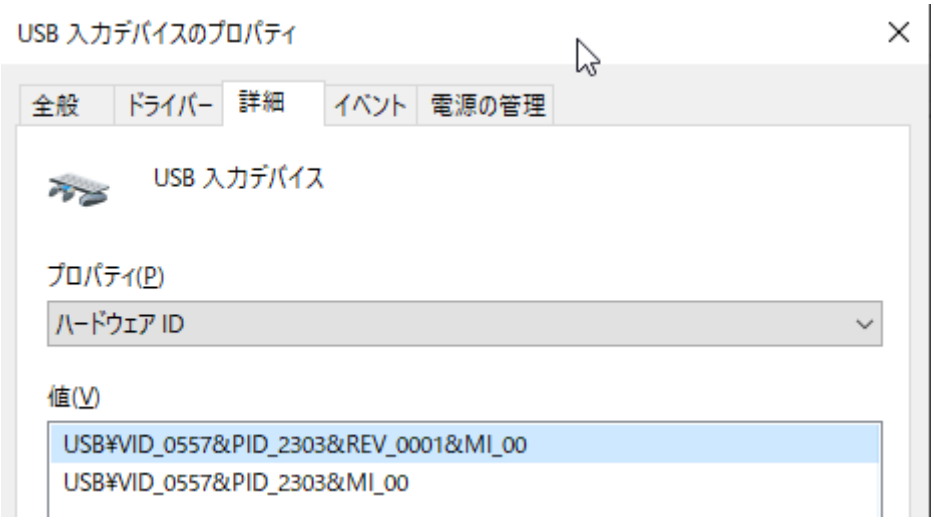
- 接続しているKVMデバイスごとに設定したら完了です

補足

有償ライセンス認証方法

- CC2000がインストールされたサーバー本体にUSBキーを接続してください
    - リモート端末にUSBキーを接続してもご利用いただけないためご注意ください
- リモート端末からCC2000にログインしてください
- 「システム>ライセンス」の画面では、ライセンスの認証状況を確認できます
    - 下図では、「CC2000-Demo-License」と評価版を利用していることが確認できます
- 有償ライセンスを認証するには、「アップデート」ボタンをクリックします
- 認証には数秒かかります。この時、他のユーザーのリモートアクセスに影響はありません
- ライセンスキーによる認証に成功すると、次のような画面が表示されます
- 「シリアルナンバーを入力してください」という項目には、USBライセンスキーの背面にあるシリアル番号が記載されます
    - 技術的な問題が発生し、ATENへ問い合わせる場合はこのシリアル番号をご提示ください
- 認証に失敗した場合、CC2000がインストールされたサーバーにUSBキーが接続されていない可能性があります。しっかり接続できているか確認してから再認証してください
- USBキーはデバイスマネージャーから見た場合、キー次のように認識されます
    - USBキーはコンポジットデバイスに区分けされ「USBハブ+HID(USB入力デバイス)」と認識されます





冗長サーバー構成構築方法

- CC2000のサーバーは1つのセグメントに1台のプライマリーサーバーだけが存在することを前提に設計されています
- 冗長構成を構築する場合は以下の手順で構築し、同じネットワークセグメント内にプライマリーサーバーが複数稼働した状態にしないでください
    - プライマリーサーバーにCC2000をインストールする
    - プライマリーサーバー(物理サーバー)にUSBキーを接続して、ライセンス認証を行う
    - 「システム > 冗長サーバー」でプライマリーサーバーとしてオンラインになっていることを確認します

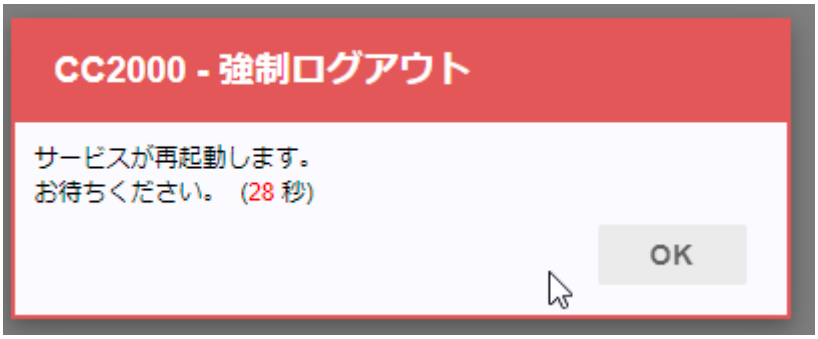
    - セカンダリーサーバーにCC2000をインストールする
    - セカンダリサーバーにログインします。この時、プライマリーサーバーが複数ある状態では、上図のリストにはプライマリーサーバーが複数出てこないようになっています。「サーバー名」にそれぞれの名前が表示されます
    - セカンダリーサーバーの「システム > 冗長サーバー」で「登録」をクリックすると、プライマリーサーバーの登録をします

- 今回のモデル構成に準じた設定であれば
  - プライマリーサーバーは「192.168.0.100」
  - プライマリーサーバーのHttpsポートは標準では「8443」
  - ユーザーネームと管理者パスワードは任意で設定した値を入力します
  - OTP(OneTime Password)は利用している場合は入力します
    - 使用していない、OTPが分からない方は空欄のままで登録します

- 「登録」をクリックすセカンダリーサーバーのデータをすべて消去し、プライマリーサーバーのデータをコピーする確認が表示します
  - もしもセカンダリーサーバーは別途稼働していた場合は、必要に応じてバックアップを取得してから、冗長構成を構築してください

- 「はい」をクリックすると、セカンダリーサーバーのデータが消去され、プライマリーサーバーからデータコピーが開始します

- セカンダリーサーバーとして動作モードが変更するため、サービスが再起動し、ブラウザーから強制的にログアウトします



- セカンダリーサーバーのCC2000が再起動したら、冗長構成が構築できました。
- この後は、「タスク」で「データベース同期」タスクを作成してください
    - 「毎日xx時」などデータベースを同期させると、障害発生時にセカンダリーサーバーは最終の同期したデータベースをもとに稼働します
- 冗長構成のセットアップはこれで完了です

設定反映の遅延について

- 弊社製KVM OverIP製品とCC2000は、複数のユーザーが同時にリモートからアクセスし、設定変更が行われることを想定しています
- 複数ユーザーによるリアルタイムで設定を反映した場合、デッドロックなど不具合が発生するケースもあることから、各製品では設定反映するまで約2~3分の遅延を意図的に設けています
- そのためログインのタイムアウト設定は変更し、数分してからでないと反映されないため反映前の設定で自動的にログアウトすることがございます。これは正しい動作となります
- 即座に設定を反映させる方法としては、CC2000のサービスを再起動させることで強制的に設定を反映させることは可能です