

ホワイトペーパーシリーズ：

Windows Server IoT 2019 for Storage で構築する企業向け最新ファイルサーバー

1. インフラ編
2. 運用管理編
- 3. 集中管理編**
4. ハイブリッドクラウド編

2019年6月30日

内容

1 概要	2
1.1 このガイドについて	2
1.2 複数の LAN DISK Z に適した集中管理環境.....	2
1.3 実施環境について	4
2 Windows Admin Center の導入	6
2.1 Windows 10 へのデスクトップモードでの導入.....	6
2.2 LAN DISK Z へのゲートウェイモードでの導入.....	12
3 アイ・オー・データのクラウドサービス NarSuS の活用	20
3.1 サービスへの NAS デバイスの登録	20
3.2 専用ポータルでのステータス監視	22

本文書は、株式会社アイ・オー・データ機器（以下、「アイ・オー・データ」とします。）が、アイ・オー・データの特定の商品に関する機能・性能や技術についての説明を記述した参考資料となります。当該商品の利用という目的の範囲内で自由に使用、複製をしていただけますが、アイ・オー・データの事前の書面による承諾なしに、改変、掲示、転載等の行為は禁止されます。また、あくまで参考資料として提供いたしますので、内容については一切保証を致しかねます。アイ・オー・データサポートセンターでは内容に関するお問い合わせは承っておりません。以下の内容をご了承いただいた場合のみご利用ください。(1)アイ・オー・データは、本文書によりいかなる権利の移転もしくはライセンスの許諾、またはいかなる保証を与えるものではありません。(2)アイ・オー・データは、本文書について、有用性、正確性、特定目的への適合性等のいかなる保証をするものではありません。(3)アイ・オー・データは、本文書を利用したこと、または利用しなかったことにより生じるいかなる損害についても責任を負うものではありません。(4)アイ・オー・データは、本文書の内容を随時、断りなく更新、修正、変更、削除することがあります。最新の商品情報については、<https://www.iodata.jp/>をご覧ください。

1 概要

1.1 このガイドについて

このガイドは、Windows Server IoT 2019 for Storage Standard または Workgroup を搭載する LAN DISK Z LAN DISK Z の NAS デバイスを導入するにあたり、ファイルサーバーとしての運用管理を効率化するための集中管理環境について説明します。このガイドが想定しているのは、他の運用管理システムを導入していない小規模なワークグループ環境であり、1 台以上の LAN DISK Z と Windows Server を実行する既存のサーバーを含めた集中管理環境を追加コストなしで実現します。LAN DISK Z の Windows Storage Server 2016 搭載もまた、同様の方法で管理することができます。

1.2 複数の LAN DISK Z に適した集中管理環境

このガイドでは小規模なワークグループ環境に追加コストなしで導入できる集中管理環境として、以下の2つの管理ツールおよびサービスを利用します。このガイドではワークグループ環境での利用を想定していますが、Active Directory ドメイン環境での利用を排除するものではありません。

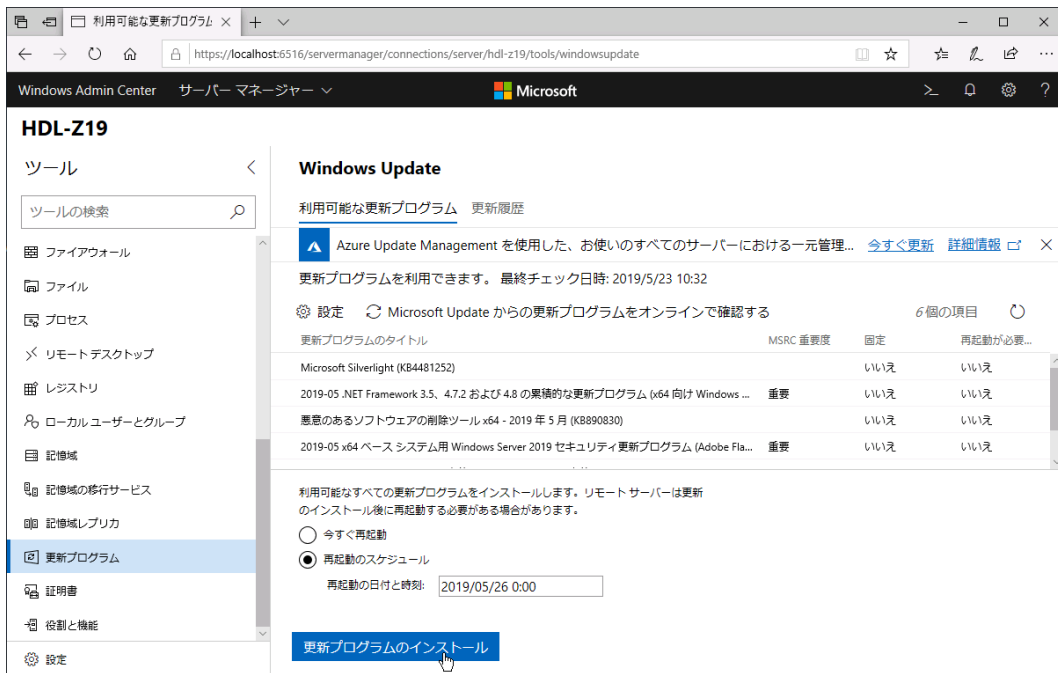
- Windows Admin Center
- NarSuS

Windows Admin Center

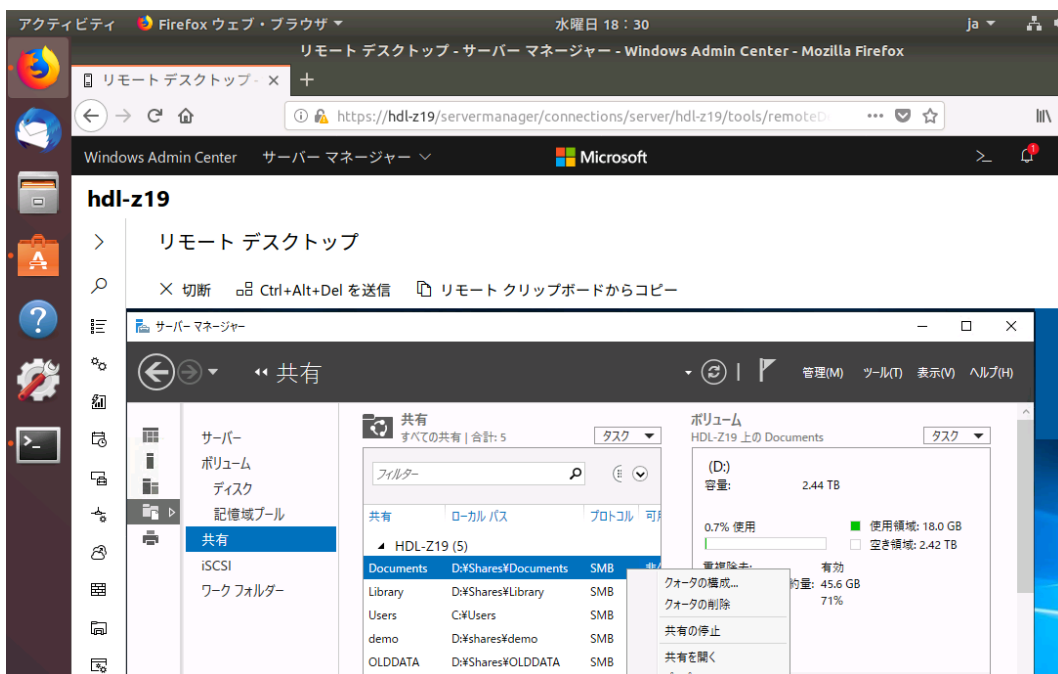
Windows Admin Center はマイクロソフトが無料提供する HTML5 ベースの管理アプリです。Project Honolulu という開発コード名で開発され、2018 年 4 月に最初のバージョン 1804 がリリースされました。このツールは、半期チャネルで 1 年に 2 回 (4 月頃と 9 月頃)、新しいメジャーバージョンがリリースされ、機能強化や改善が行われます。このガイドの制作時点の最新のメジャーバージョンは 2019 年 4 月にリリースされたバージョン 1904 です (6 月に更新バージョン 1904.1 がリリースされています)。

Windows Admin Center は、Windows 10 (バージョン 1709 以降) に導入することができます。Windows Server 2016 以降の Windows Server の管理に最適化されていますが、Windows Server 2008 R2 以降の Windows Server (Windows Server 2008 R2 の管理は機能制限あり)、および Windows 10 (バージョン 1709 以降) クライアントのローカルおよびリモート管理に対応しています。

Windows Admin Center が提供する管理コンソールは HTML5 ベースの Web アプリであり、Microsoft Edge、Google Chrome、および Mozilla Firefox ブラウザーだけで利用できるのが特徴です。コンピューターの管理やタスクスケジューラ、エクスプローラー、デバイスマネージャー、レジストリエディター、Windows Update といった Windows 標準の管理ツールと同等の機能を備えるほか、サーバーマネージャーの管理機能やサーバーの役割や機能に対応した管理機能、Microsoft Azure の各種サービスとの連携機能を提供します (Microsoft Azure との連携機能については、このガイドのシリーズの『4. ハイブリッドクラウド編』で説明します)。また、Windows Admin Center にはマイクロソフトやサードベンダーが開発・提供する拡張機能で管理機能を追加することができます。



Windows Admin Center は、リモートサーバーにリモートデスクトップ接続や Windows PowerShell を使用して対話的に接続する機能も備えています。このガイドのシリーズの『2. 運用管理編』では、Windows だけでなく、Android、iOS、macOS、または Linux からのリモートデスクトップ接続のための RDP 対応クライアントについて紹介しました。Windows Admin Center を使用すると、ローカルに RDP 対応クライアントを準備しなくても、さまざまなプラットフォームから Web ブラウザーだけでサーバーのコンソールに対話的に接続できます。



Windows Admin Center について詳しくは、以下の公式ドキュメントで確認してください。

Windows Admin Center の概要 (Microsoft Docs)

<https://docs.microsoft.com/ja-jp/windows-server/manage/windows-admin-center/overview>

NarSuS

NarSuS（ナーサス）は、アイ・オー・データのNAS製品の状態をリモート管理できる、アイ・オー・データ独自のクラウドベースの管理機能です。登録済み NAS デバイスからクラウドへのステータス情報の定期通知および機器の異常のイベント通知（送信方法のHTTPSのみを使用）により、NASデバイスのステータスや異常を監視し、登録ユーザーに対して電子メールで定期レポートや異常時のアラート通知を行います。また、管理者は時と場所を選ばずに Web ベースの管理コンソールにログインして、1 台以上の登録済み NAS デバイスの状態や統計情報を参照することができます。

The screenshot shows the NarSuS web interface for a device with model number HDL-Z2WM4.0. The status is 'Normal' (通常). The interface includes sections for power unit status, device temperature (46°C), fan speed (3069rpm), and disk RAID mode (RAID1) with usage percentages. A table lists internal disk models and their usage. There is also a section for external connected devices, showing a UPS device (OMRON BY80S) connected via USB port 5.

電源ユニット稼働時間	ステータス	状態
電源ユニット稼働時間	稼働中	●
装置稼働時間	稼働中	●
FAN稼働時間	稼働中	●

ディスク RAIDモード	使用量/全容量(残量)	状態
C: RAID1	20.26 / 97.66GB (79.25%)	●
D: RAID1	0.44 / 1,765.36GB (99.98%)	●

内蔵ディスク情報	HDD番号	内蔵ディスクモデル名	内蔵ディスク稼働時間	解決策	HDD状態	SMART状態
	1	WDC WD20EADS-22FR60	23,164時間		●	●
	2	WDC WD20EFRX-68EUZN0	10,844時間		●	●

外付接続機器	接続先	ポート	種別	製品名 / ミラー設定	使用量 / 全容量 (残量)	状態	解決策
	USB	5	UPS	OMRON BY80S	100.00%	●	UPSステータス画面を見る

NarSuS について詳しくは、アイ・オー・データの NarSuS 特集サイトで確認してください。

ビジネス NAS 入門 | NarSuS (I-O DATA)

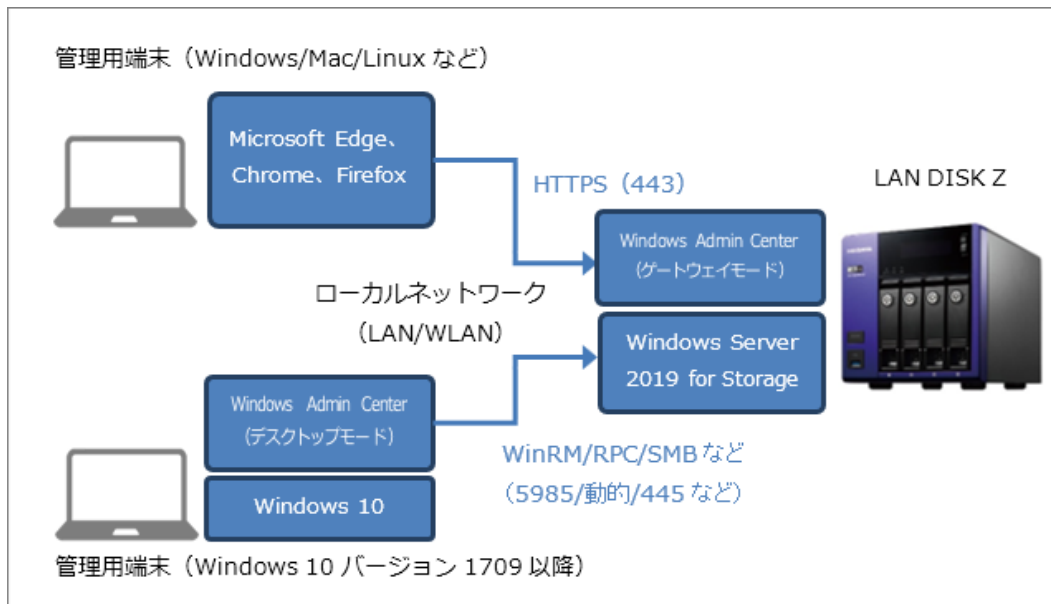
<https://www.iodata.jp/ssp/nas/biznas/narsus.htm>

1.3 実施環境について

Windows Admin Center の導入形態には、Windows 10（バージョン 1709 以降）にインストールしてローカルの Web ブラウザーから利用する形態の「デスクトップモード」と、Windows Server 2016 以降のサーバーにインストールしてリモートの Web ブラウザーから利用する形態の「ゲートウェイモード」の 2 種類があります。このガイドでは、その両方について説明します。利用環境に合わせて、いずれかの形態で導入してください。2 種類の導入形態の両方を導入することも可能です。

Windows Server IoT 2019 for Storage は、Windows Server 2019 がベースとなっています。そのため、Windows Server IoT 2019 for Storage を搭載する LAN DISK Z の NAS デバイスのローカルに Windows Admin Center をゲートウェイモードとしてインストールすることができ、リモートから以下のいずれかの Web ブラウザー（最新バージョンを推奨）を使用して管理することができます。Internet Explorer はサポートしていないため、Windows Server のローカルの Internet Explorer 11 からは利用できません。

- Microsoft Edge (Windows 10 のみ)
- Google Chrome
- Mozilla Firefox (正式にはテストされていませんが、動作します)



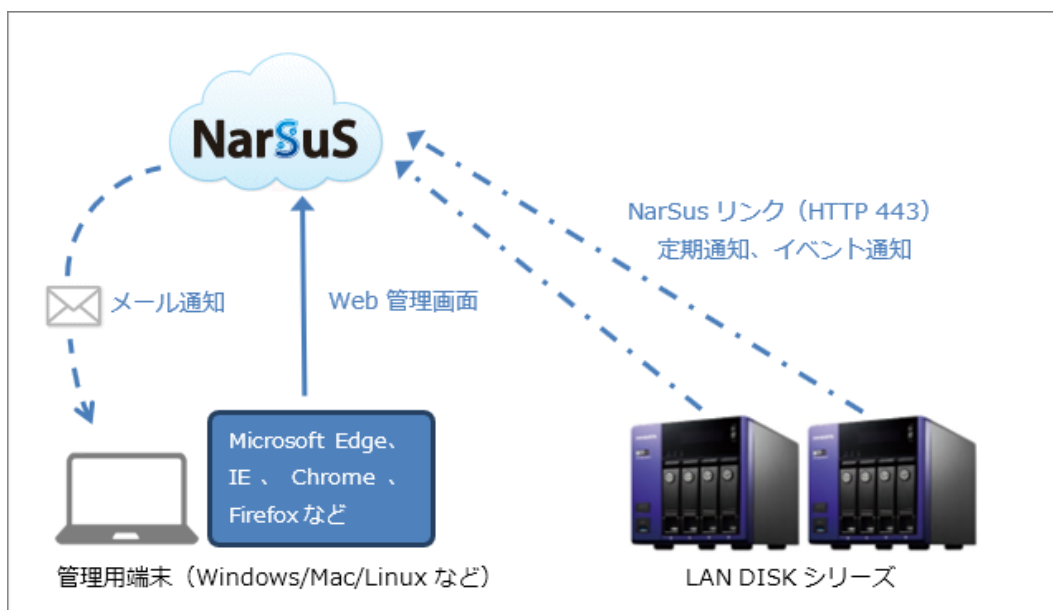
NarSuS は、NAS デバイスがインターネットに HTTPS で接続可能なネットワーク（プロキシ経由を含む）に接続されている環境で利用できます。インターネットに接続できない環境にある場合は、アイ・オー・データが提供するネットワーク管理ソフト「IO Navi」を導入することで NAS を含むネットワーク機器が正常に動作しているかを監視することが可能です。また、機器を個別に設定したり、グループに登録した機器をまとめて設定したりできます。IO Navi については以下のサイトで確認してください。

IO Navi

<https://www.iodata.jp/product/app/network/ionavi/>

NarSuS の Web 管理コンソールにアクセスする管理端末はインターネットにアクセス可能であればよく、設置場所は問いません。社外からアクセスすることもできます。以下の Web ブラウザー（最新バージョンを推奨）がサポートされ、Google Chrome と Mozilla Firefox はプラットフォームを問いません。

- Internet Explorer (Windows のみ)
- Microsoft Edge (Windows 10 のみ)
- Google Chrome
- Mozilla Firefox
- Apple Safari (iOS および macOS)



2 Windows Admin Center の導入

Windows Server 2019 の [サーバーマネージャー] を初めて開くと、最初に [Windows Admin Center でのサーバー管理を試してみる] のダイアログボックスを目にするはずですが、このダイアログボックス内のリンク先は前述の「Windows Admin Center の概要」(Microsoft Docs) 内の「今すぐダウンロード」のページになっています。



Windows Admin Center を導入する前に、このページから一般公開リリースの最新バージョンの Windows インストーラーパッケージ (このガイドの制作時点では WindowsAdminCenter1904.1.msi) をダウンロードしてください。日本語サイトは最新情報が反映されるまでタイムラグがある場合がありますが、[こちらで入手します] は最新バージョンである以下の URL にリンクされています。

Windows Admin Center 最新バージョンのダウンロード

<https://aka.ms/WACDownload>

2.1 Windows 10 へのデスクトップモードでの導入

Windows 10 を実行するコンピューターに、デスクトップモードの Windows Admin Center をインストールする手順を説明します。

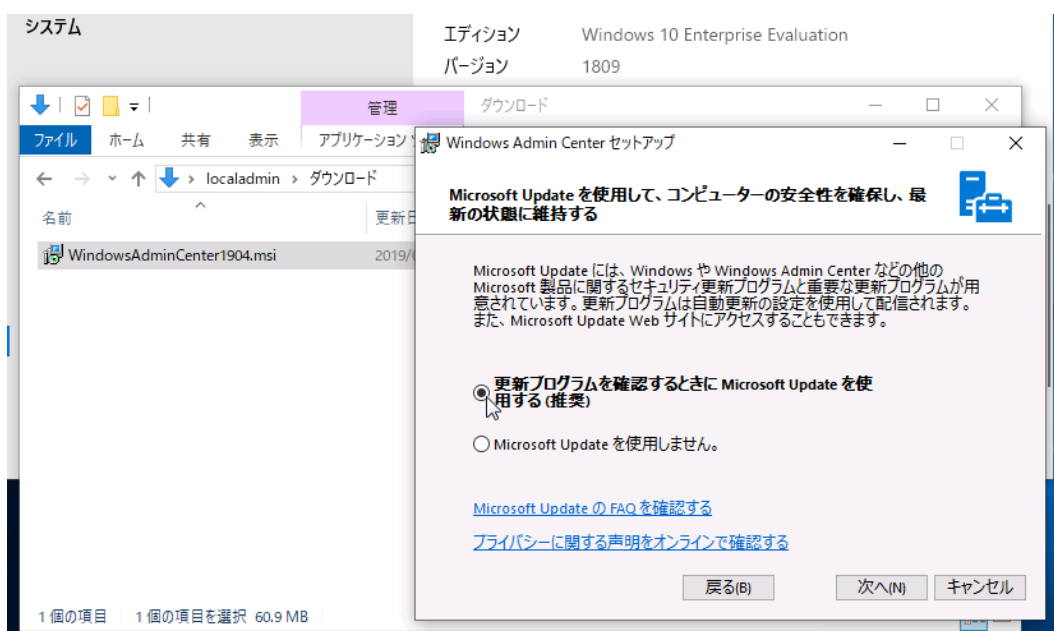
Windows Admin Center (デスクトップモード) のインストール

デスクトップモードの Windows Admin Center は、64 ビット (x64) Windows 10 バージョン 1709 以降を実行するコンピューターにインストールできます。32 ビット (x86) Windows 10 にはインストール

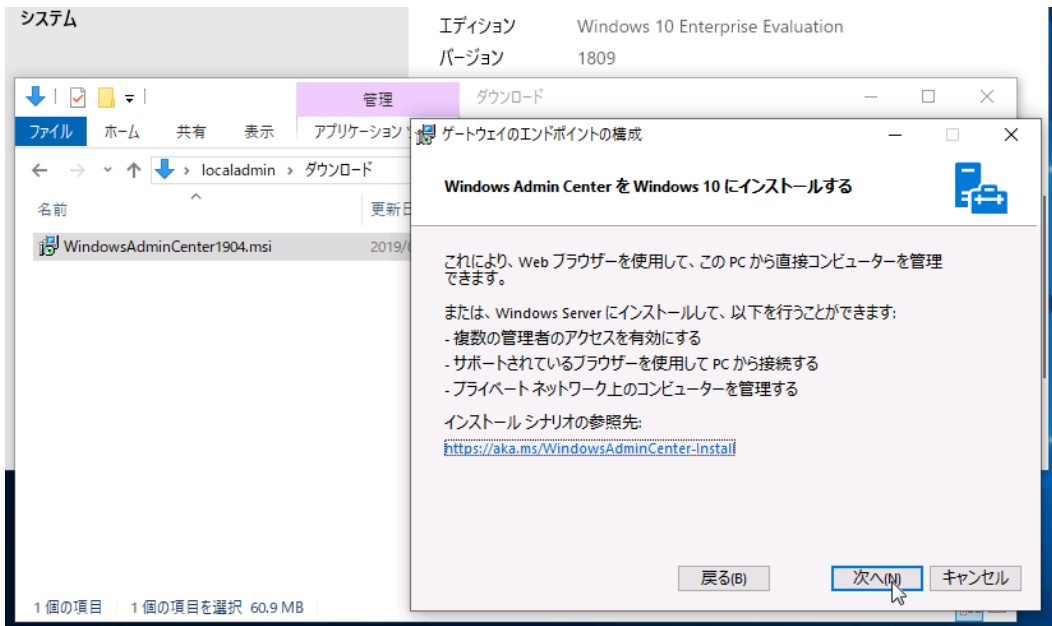
できません。Home エディションにもインストールできますが、Home エディションでの利用は想定されていないため、正しく動作しない可能性があります。

デスクトップモードの Windows Admin Center をインストールするには、次の手順で操作します。

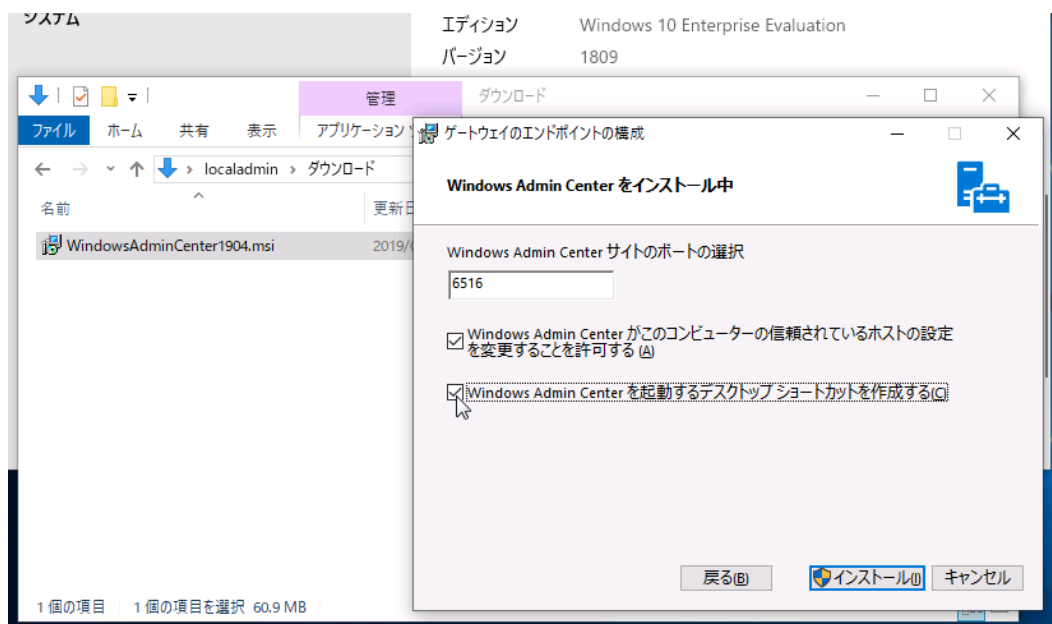
1. Windows 10 にローカル管理者ユーザー（Microsoft アカウント、ローカルアカウント、または Active Directory ドメインアカウント）でサインインします。事前にダウンロードしておいた Windows Admin Center の Windows インストーラーパッケージ（WindowsAdminCenterXXXX.msi、XXXX はバージョン）を実行して [Windows Admin Center セットアップ] を開始します。最初の画面では、使用許諾契約書の内容を確認し、問題がなければ [使用許諾契約書に同意します] をチェックして [次へ] をクリックします。
2. 次の画面で [更新プログラムを確認するときに Microsoft Update を使用する (推奨)] を選択して、[次へ] をクリックします。これにより、Windows Admin Center の更新バージョンが Windows Update で提供されるようになります。



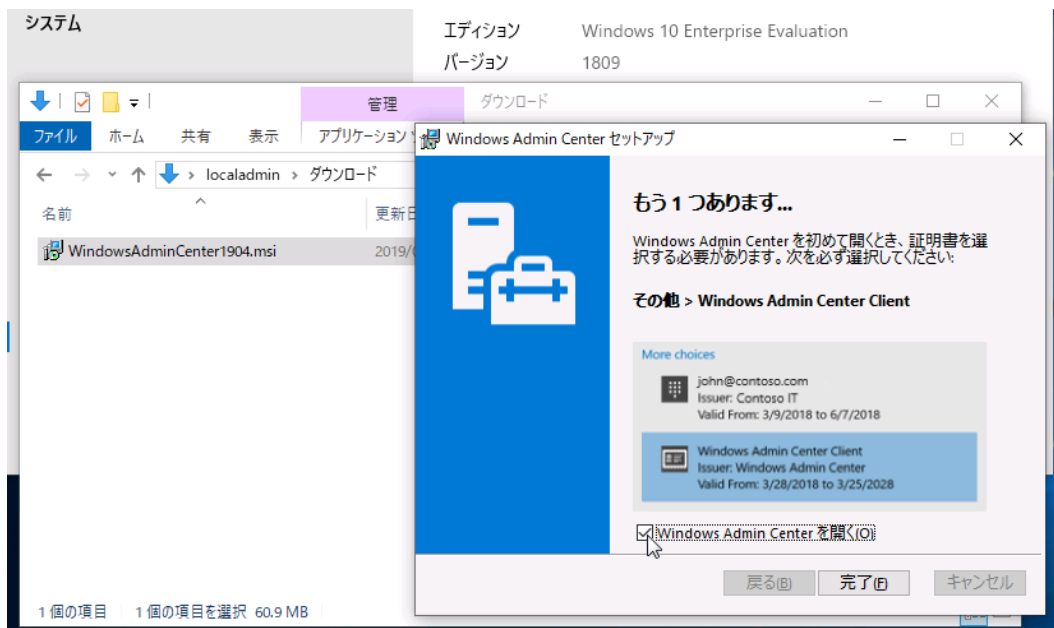
3. [Windows Admin Center を Windows 10 にインストールする] の画面にデスクトップモードの Windows Admin Center についての説明が表示されるので、確認して [次へ] をクリックします。



4. [Windows Admin Center をインストール中] の画面で、Windows Admin Center サイト用のローカルポート（既定は 6516）を確認し、必要に応じて [Windows Admin Center を起動するデスクトップショートカットを作成する] をチェックして [インストール] をクリックします。既定でチェックされる [Windows Admin Center がこのコンピューターの信頼されているホストの設定を変更することを許可する] は、ワークグループ環境での Windows リモート管理 (WinRM) に必要な TrustedHosts の構成を行うものです。Active Directory ドメイン環境の場合はオフにすることができます。



5. [ユーザーアカウント制御] の昇格ダイアログボックスが表示されるので、[はい] をクリックします。
6. セットアップが完了し、[もう 1 つあります...] という最後の画面が表示されます。すぐに Windows Admin Center を開く場合は、ここで [Windows Admin Center を開く] をチェックし、[完了] をクリックします。すぐに開始しない場合は、そのまま [完了] をクリックしてください。



Windows Admin Center が行う TrustedHosts の構成について

[Windows Admin Center がこのコンピューターの信頼されているホストの設定を変更することを許可する] をチェック (既定) して Windows Admin Center をセットアップで行う場合、TrustedHosts の構成は管理者として開いた Windows PowerShell で次のコマンドラインを実行したのと同じ設定になります。

```
Set-Item WSMAN:¥localhost¥Client¥TrustedHosts "*" -Force
```

既に別の設定を行っている場合は、[Windows Admin Center がこのコンピューターの信頼されているホストの設定を変更することを許可する] をオフにしてセットアップを進め、管理対象のサーバーのコンピューター名または IP アドレスを既存の設定に追加してください。現在の設定の確認と、新しい管理対象の追加は、次のコマンドラインを実行することで確認することができます。

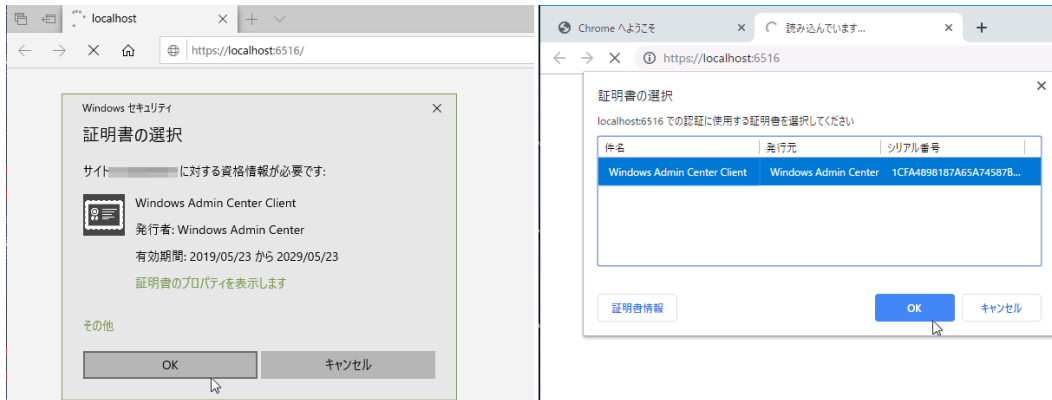
```
Get-Item WSMAN:¥localhost¥Client¥TrustedHosts
```

```
Set-Item WSMAN:¥localhost¥Client¥TrustedHosts "追加する管理対象のコンピューター名または IP アドレス" -Concatenate -Force
```

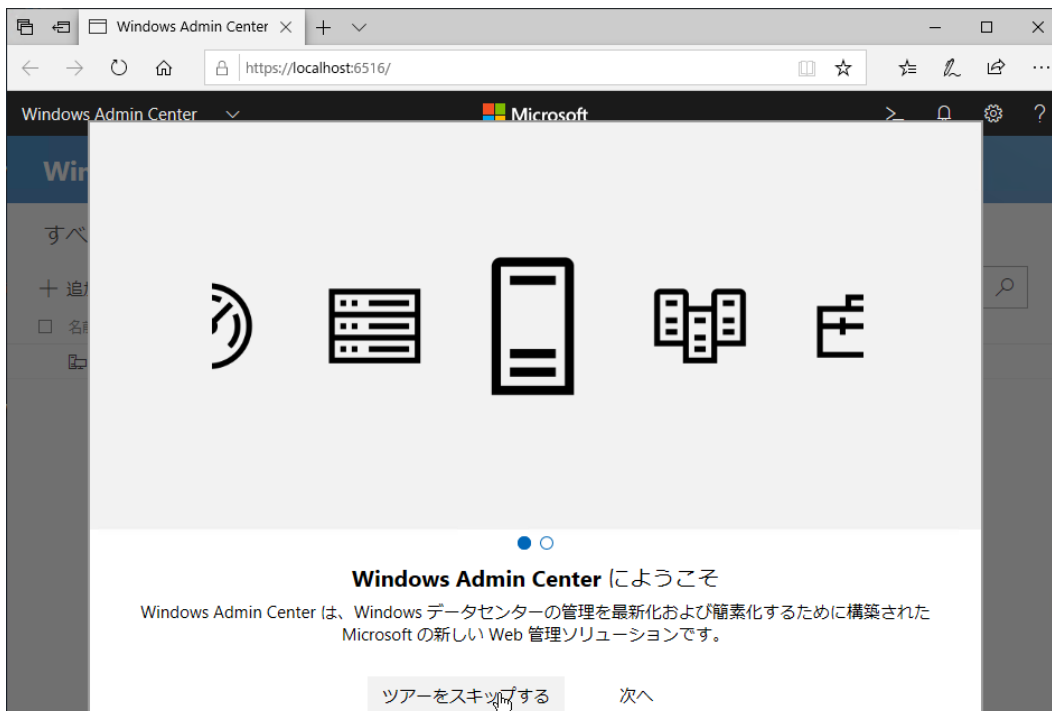
Windows Admin Center サイトの開始

[Windows Admin Center セットアップ] の最後の画面で [Windows Admin Center を開く] をチェックした場合、[完了] をクリックすると、Windows Admin Center アプリが開始され、既定の Web ブラウザーで「https://localhost:6516/」が開きます。初めて起動した際には、Web ブラウザーで証明書の選択が求められるので、[OK] をクリックしてください。なお、Windows Admin Center に対応していない Web

ブラウザ（Internet Explorer など）が既定のブラウザとして設定されている場合、[別のブラウザでお試してください] と表示され、対処方法が示されます。その際、ページが文字化けする場合は、エンコードを Unicode（UTF-8）に変更してください。



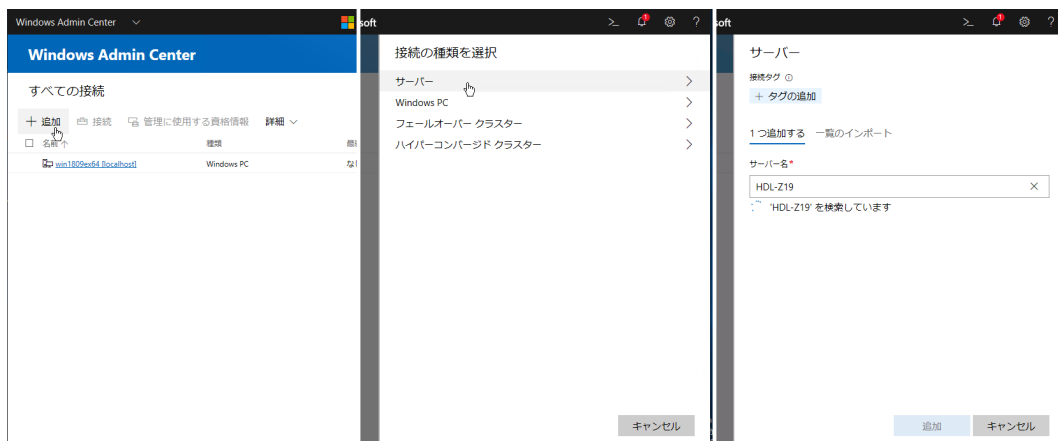
続いて [Windows Admin Center による] の解説ツアーが表示されるので、[次へ] をクリックしてツアーを一通り参照するか、[ツアーをスキップする] をクリックして Windows Admin Center のトップページに移動します。インストール直後および運用中に Windows Admin Center の拡張機能の更新がある旨の通知がある場合があります。通知メッセージに従って [拡張機能] に移動し、インストール済みの拡張機能を更新してください。



Windows Admin Center サイトの「https://localhost:6516/」は常に稼働しているわけではありません。[スタート] メニューやデスクトップに登録された Windows Admin Center アプリ (C:\Program Files\Windows Admin Center\SmeDesktop.exe) を開始することでサイトが利用可能になり、既定のブラウザで Windows Admin Center サイトが開きます。Windows Admin Center サイトを開始したあとは、Windows Admin Center 対応のローカルの別のブラウザでも「https://localhost:6516/」にアクセスすることができます。リモートコンピュータからは接続できません。

管理対象サーバーの登録

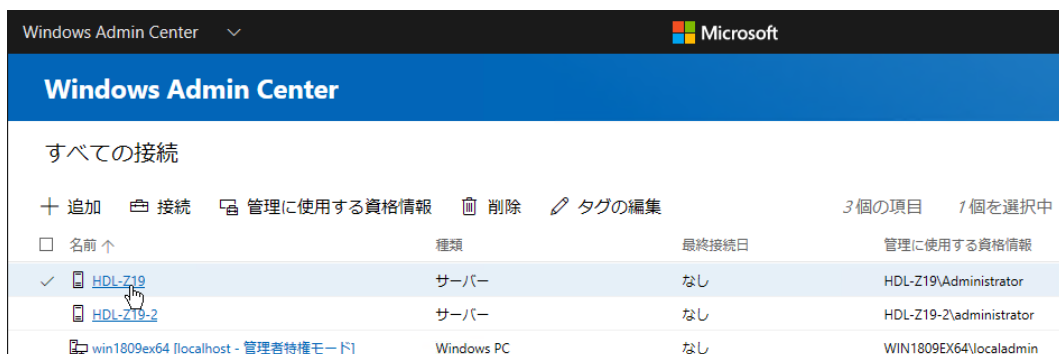
デスクトップモードの Windows Admin Center には、既定でローカルの Windows 10 コンピューターが管理対象として登録されます。LAN DISK Z の NAS デバイスを管理するには、[+追加] をクリックして、[接続の種類を選択] で [サーバー >] をクリックし、[サーバー名] に LAN DISK Z のコンピューター名または IP アドレスを入力します。



管理対象のサーバーが検出されると、資格情報が要求されるので、サーバーのローカル管理者の資格情報（<コンピューター名>¥Administrator とそのパスワード）を入力して追加します。



管理対象が複数台ある場合は、サーバーの登録を繰り返します。Windows Admin Center のトップページで管理対象をクリックすると、管理対象のサーバーの管理ページが開きます。





リモートサーバーへのシングルサインオン (SSO) 接続について (デスクトップモード)

デスクトップモードの Windows Admin Center をワークグループ環境に導入する場合、CredSSP 認証 (NTLM 認証) が使用されるため、管理対象のサーバーへの接続ごとに資格情報の入力が必要です。

デスクトップモードの Windows Admin Center を Active Directory ドメインメンバーの Windows 10 にインストールした場合、Kerberos 認証が使用されるため、適切な権限を持つドメインアカウント (管理対象のローカル Administrators の権限のあるアカウント) でサインインすれば、同じく Active Directory ドメインメンバーであるリモートサーバーにシングルサインオン接続できます。

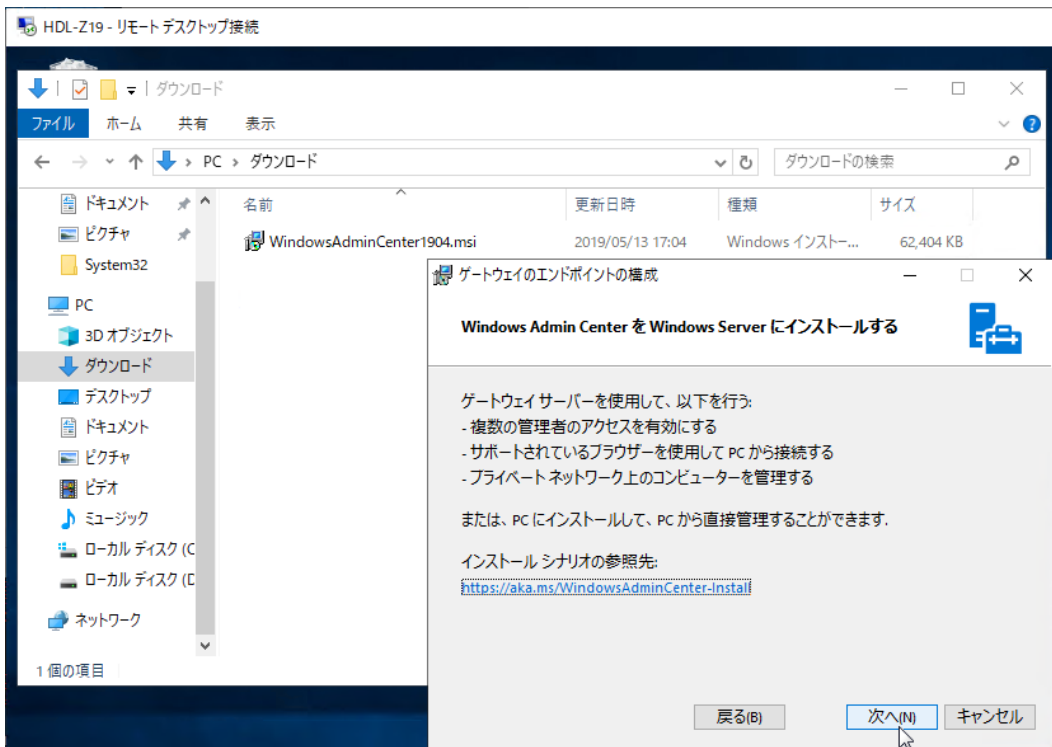
2.2 LAN DISK Z へのゲートウェイモードでの導入

Windows Admin Center は、Windows Server 2016 以降の Windows Server にゲートウェイモードでインストールすることができます。Windows Server IoT 2019 for Storage や Windows Storage Server 2016 を搭載する LAN DISK Z には、ゲートウェイモードの Windows Admin Center をインストールすることができ、Windows Admin Center 対応の Web ブラウザーを使用してリモートから接続して管理することができます。デスクトップモードの Windows Admin Center をインストールできる環境が無い場合は、この方法による Windows Admin Center の導入がおすすめです。

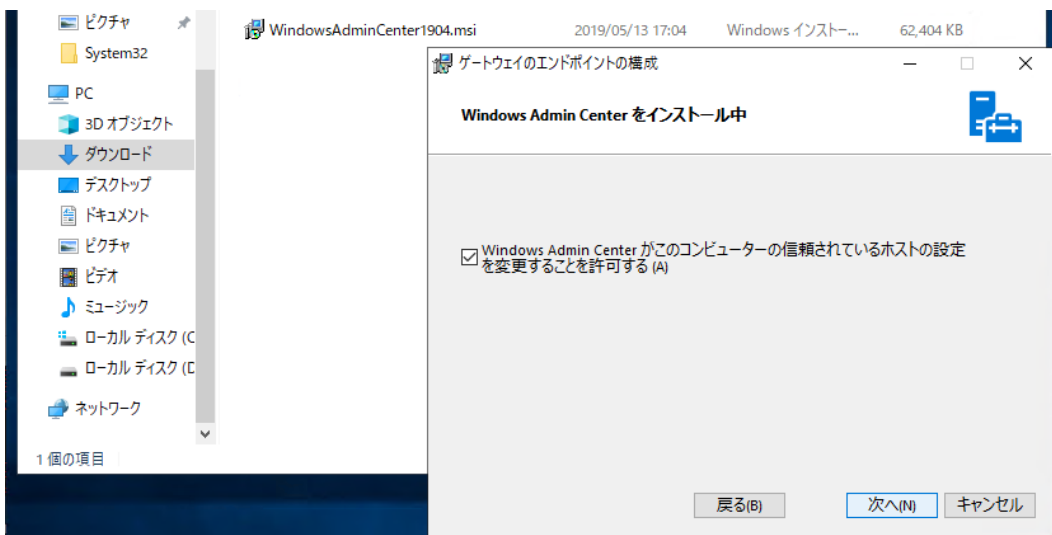
Windows Admin Center (ゲートウェイモード) のインストール

LAN DISK Z にゲートウェイモードの Windows Admin Center をインストールするには、次の手順で操作します。

1. LAN DISK Z に、ローカル管理者アカウントの資格情報でリモートデスクトップ接続します。
2. 事前にダウンロードしておいた Windows Admin Center の Windows インストーラーパッケージ (WindowsAdminCenterXXXX.msi、XXXX はバージョン) を実行して [Windows Admin Center セットアップ] を開始します。最初の画面では、使用許諾契約書の内容を確認し、問題がなければ [使用許諾契約書に同意します] をチェックして [次へ] をクリックします。
3. 次の画面で [更新プログラムを確認するときに Microsoft Update を使用する (推奨)] を選択して、[次へ] をクリックします。これにより、Windows Admin Center の更新バージョンが Windows Update で提供されるようになります。
4. [Windows Admin Center を Windows Server にインストールする] の画面にゲートウェイモード (ゲートウェイサーバー) についての説明が表示されるので、確認して [次へ] をクリックします。

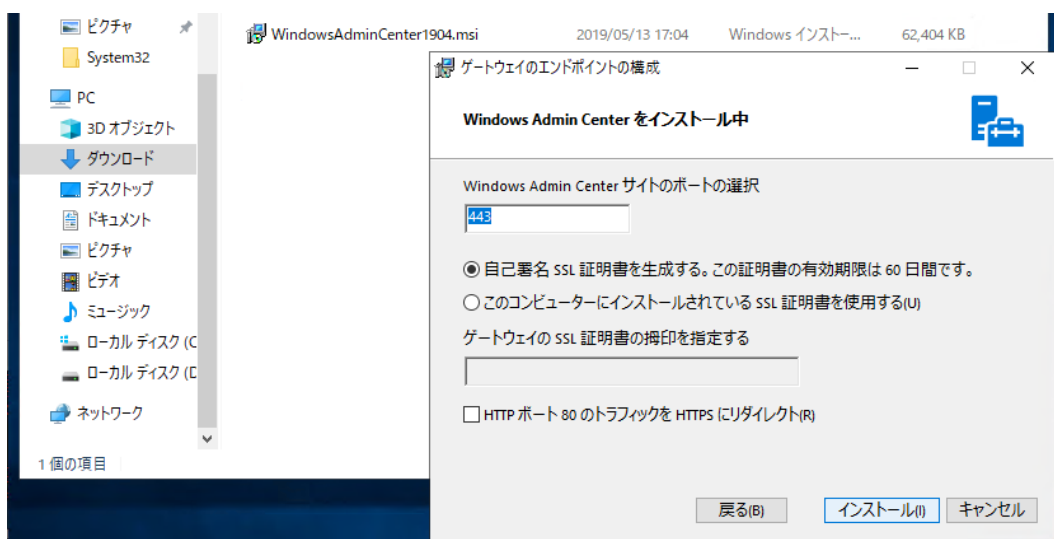


5. [Windows Admin Center をインストール中] の画面で、[Windows Admin Centerがこのコンピューターの信頼されているホストの設定を変更することを許可する] がチェックされていることを確認し、[次へ] をクリックします。このオプションは、ワークグループ環境での Windows リモート管理 (WinRM) に必要な TrustedHosts の構成を行うものです。Active Directory ドメイン環境の場合はオフにすることができます。この設定については、「2.1 Windows 10 へのデスクトップモードでの導入」で説明しました。

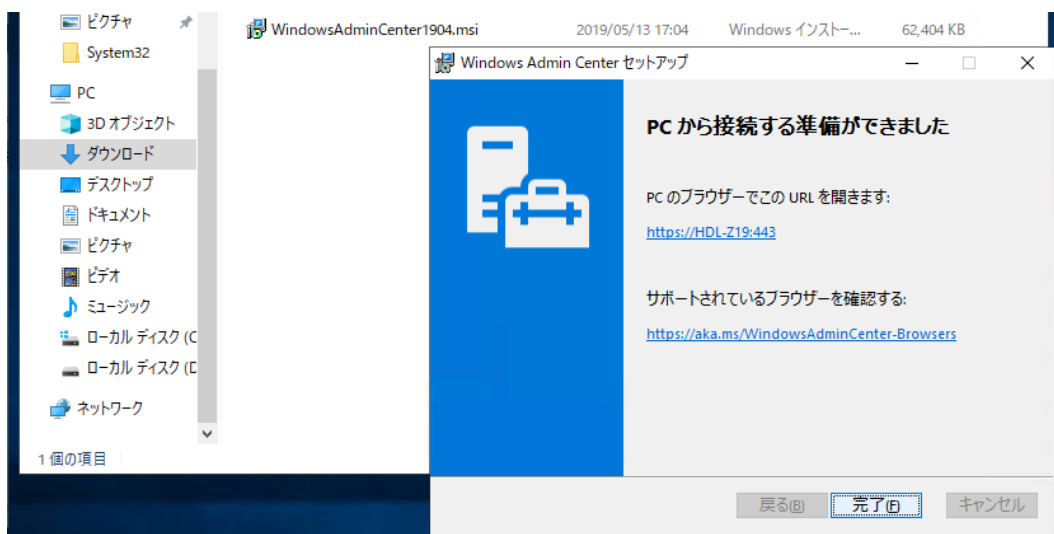


6. 次の [Windows Admin Center をインストール中] の画面では、リモートからのアクセスを受け付ける Windows Admin Center サイトのポート (既定は 443) を確認し、[自己署名 SSL 証明書を生成する] を選択して、[インストール] をクリックします。[自己署名 SSL 証明書を生成する] を選択してセットアップするのが簡単ですが、インストール済みの有効な証明書を利用できる場合は、ここで [このコンピューターにインストールされている SSL 証明書を使用する] を選択し、証明書の拇印を指定しま

す。証明書の拇印は、証明書のプロパティなどから確認できます（説明は省略します）。



7. セットアップが完了すると、[PC から接続する準備ができました] の画面に接続用の URL が示されるので、確認して [完了] をクリックします。また、リモートデスクトップ接続のセッションからログオフします。



Windows Admin Center サイトへの接続

Windows Admin Center アプリを使用して Windows Admin Center サイトを開始する必要があるデスクトップモードの Windows Admin Center とは異なり、ゲートウェイモードの Windows Admin Center は Windows のサービス（サービス名「ServerManagementGateway」、表示名「Windows Admin Center」）として常に稼働しており、いつでもリモートの Web ブラウザーから接続することができます。

ゲートウェイモードの Windows Admin Center の既定のインストール（ポート 443）の場合は、「**https://<コンピューター名>:443/**」または「**https://<コンピューター名>/**」でリモートコンピューターから接続することができます。インストール直後および運用中に Windows Admin Center の拡張機能の更新がある旨の通知がある場合があります。通知メッセージに従って [拡張機能] に移動し、インストール済みの拡張機能を更新してください。

ゲートウェイモードの Windows Admin Center を自己署名証明書でセットアップした場合、Web ブラウザーは証明書の有効性を確認できないため、安全でない接続として接続前にブロックします。Microsoft Edge の場合は「このサイトは安全ではありません」、Google Chrome の場合は「この接続ではプライバシーが保護されません」、Mozilla Firefox の場合は「安全な接続ができませんでした」と表示します。これは、Web ブラウザーのセキュリティ機能の正常な動作です。

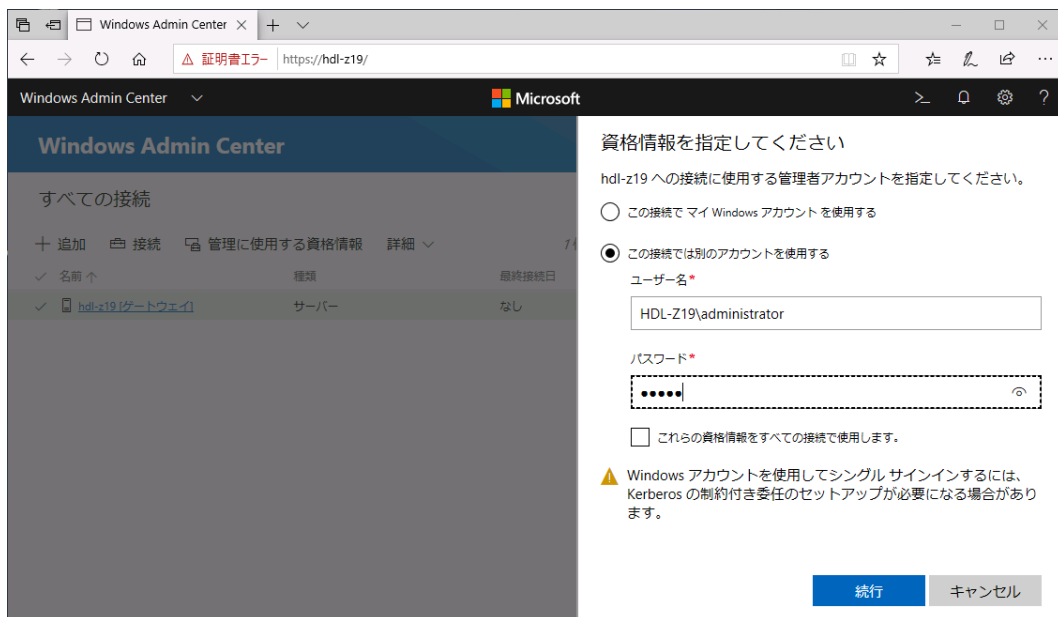


ここでは自己署名証明書の使用が理由であることがわかっているので、接続を続行してください。その方法は使用中の Web ブラウザーによって異なります。Microsoft Edge の場合は、[詳細] をクリックして詳細情報を表示させ、[Web ページへ移動 (非推奨)] をクリックします。



ゲートウェイモードの Windows Admin Center サイトにアクセスするには、ゲートウェイサーバーのローカル管理者の資格情報 (<コンピューター名>¥Administrator とそのパスワード) を入力する必要があります。ユーザー認証が完了すると、Windows Admin Center のトップページにアクセスすることができます。はじめて接続したときにはデスクトップモードの場合と同様に、解説ツアーが表示されます。

ゲートウェイモードの Windows Admin Center サイトには、ゲートウェイのサーバーが管理対象として登録済みになっているので、クリックしてローカル管理者の資格情報 (<コンピューター名>¥Administrator とそのパスワード) を入力し、管理ページを開きます。



ゲートウェイモードの Windows Admin Center は、デスクトップモードの Windows Admin Center と同様に、他の Windows Server および Windows 10（バージョン 1709 以降）を管理対象として追加して、同じ管理コンソールから管理することができます。その方法は、「1.2 Windows 10 へのゲートウェイモードでの導入」で説明した手順と共通です。

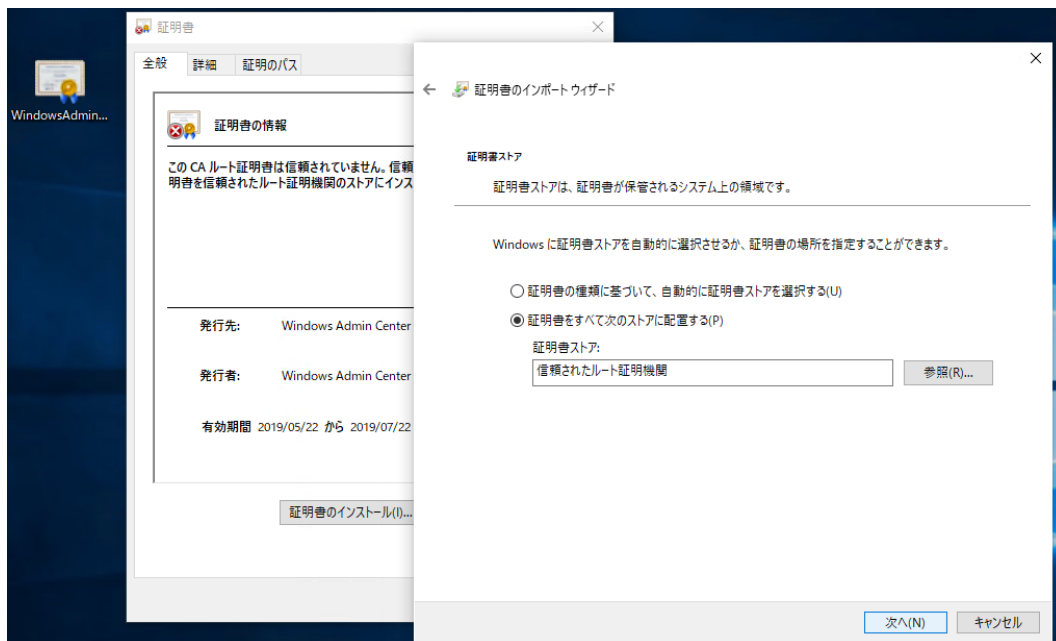
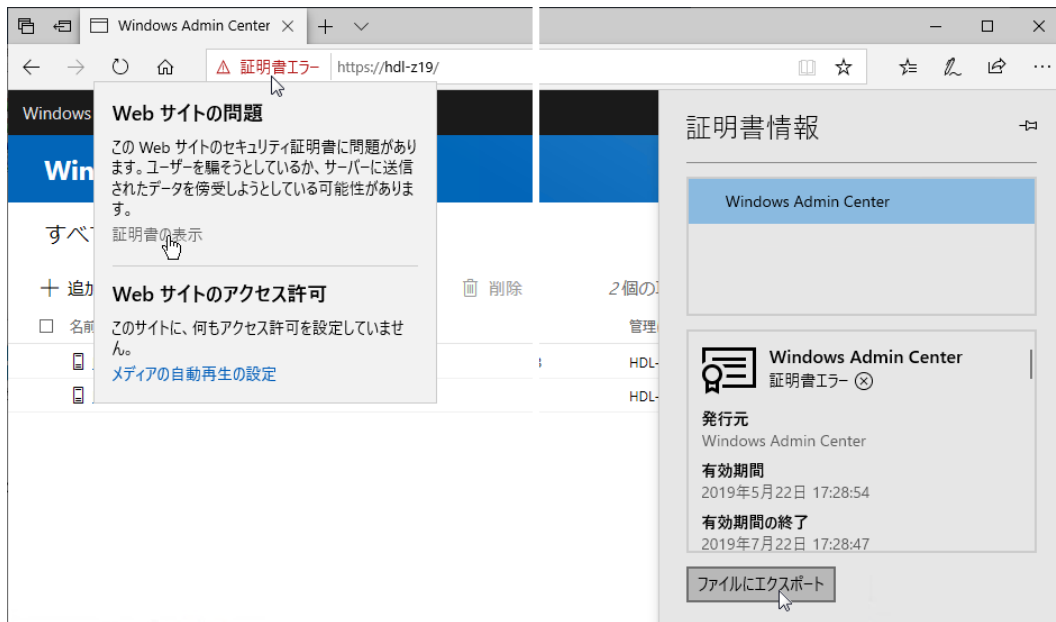


証明書のエラーを回避するには

ゲートウェイモードの Windows Admin Center を自己署名証明書でセットアップした場合、証明書エラーが表示されますが、使用される自己署名証明書をローカル（現在のユーザーまたはコンピューター）の [信頼されたルート証明機関] にインストールすることで、自己署名証明書を信頼し、証明書エラーを回避することができます。

Windows 10 の Microsoft Edge の場合は、次の手順で証明書をインストールします。

1. Windows Admin Center サイトに接続し、アドレスバーにある [証明書エラー] をクリックして、[証明書の表示] をクリックします。
2. [証明書情報] が表示されるので、[ファイルにエクスポート] をクリックして、デスクトップまたは任意の場所に WindowsAdminCenter.crt という X.509 証明書ファイルにエクスポートします。
3. エクスポートした WindowsAdminCenter.crt をダブルクリックして開き、[証明書のインストール] をクリックします。
4. [証明書のインポートウィザード] が開始するので、保存場所として [現在のユーザー] を選択し、証明書ストアとして [信頼されたルート証明機関] を選択して証明書をインストールします。
5. Web ブラウザーをいったん閉じ、再び開始して、Windows Admin Center サイトに接続し、証明書エラーが解消されたことを確認します。

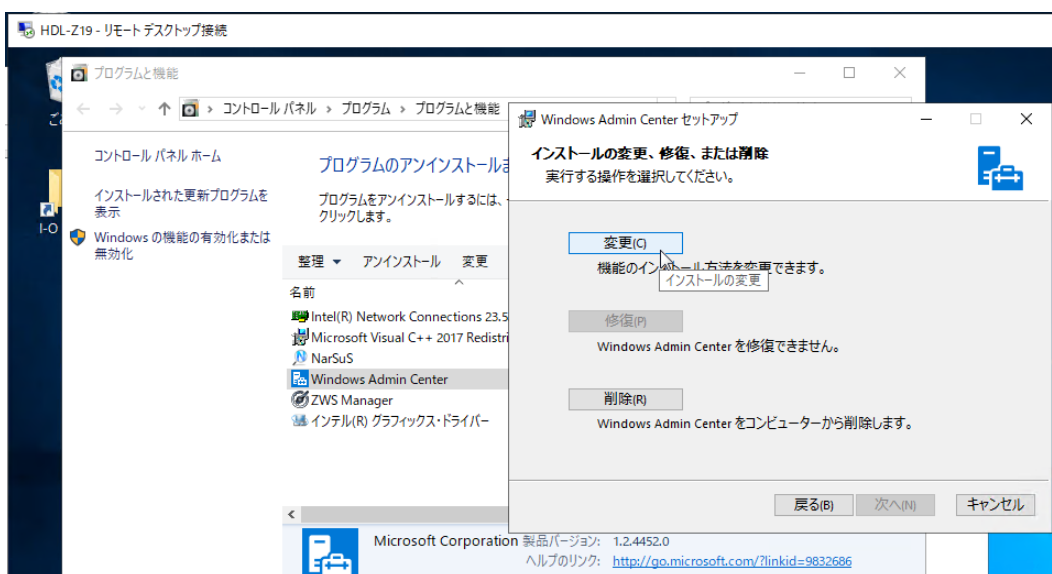


自己署名証明書の再生成について

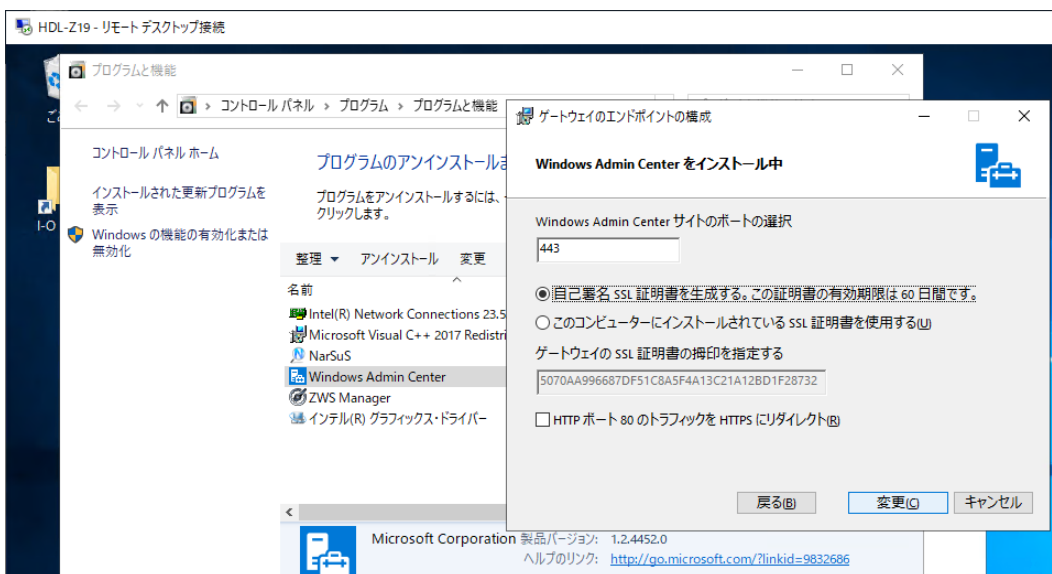
Windows Admin Center のセットアップで生成される自己署名証明書の有効期間は 60 日間であり、60 日後に期限切れとなります。現在の自己署名証明書が期限切れになった場合は (あるいは期限切れになる前に)、次の手順で再生成させることができます。自己署名証明書を有効な証明書と入れ替える場合も、同じ手順で行うことができます。

1. LAN DISK Z の NAS デバイスに、ローカル管理者アカウントの資格情報でリモートデスクトップ接続します。
2. [スタート] メニューの [Windows システムツール] からコントロールパネルを開き、[プログラムのアンインストールまたは変更] を開きます。[ファイル名を指定して実行] で **appwiz.cpl** と入力するとすばやく開くことができます。

3. プログラムの一覧から Windows Admin Center を選択し、[変更]をクリックします。[Windows Admin Center セットアップ] が起動し、[インストールの変更、修復、または削除] の画面が開くので、[変更] をクリックします。



4. [Windows Admin Center をインストール中] の画面で [自己署名 SSL 証明書を生成する。この証明書の有効期限は 60 日間です。] を選択し、[変更] をクリックします。



5. セットアップが完了したら [完了] をクリックして終了します。また、リモートデスクトップ接続のセッションからログオフします。
6. Web ブラウザーでゲートウェイモードの Windows Admin Center サイトに接続します。以前の自己署名証明書を [信頼されるルート証明機関] にインストールして信頼していた場合は、証明書が再生成されたことで再び証明書エラーが発生するようになります。必要に応じて、現在のユーザーの証明書ストアの [信頼されるルート証明機関] に新しい自己署名証明書をインストールしてください。

7.



リモートサーバーへのシングルサインオン (SSO) 接続について (ゲートウェイモード)

ゲートウェイモードの Windows Admin Center をワークグループ環境に導入する場合、管理対象のサーバーへの接続ごとに資格情報の入力が必要です。シングルサインオン接続には対応していません。

ゲートウェイモードの Windows Admin Center を Active Directory ドメインメンバーの Windows Server にインストールした場合は、Kerberos の委任設定を行うことでゲートウェイに接続する際の資格情報によるシングルサインオン接続を実現することができます。これを可能にするには、Active Directory のドメインコントローラーの Windows PowerShell で以下のコマンドラインを実行します。管理対象が複数の場合は、管理対象ごとに \$node のコンピューター名を変更して実行してください。

```
$gateway = "<Windows Admin Center のゲートウェイのコンピューター名>"  
  
$node = "<管理対象のコンピューター名>"  
  
$gatewayObject = Get-ADComputer -Identity $gateway  
  
$nodeObject = Get-ADComputer -Identity $node  
  
Set-ADComputer -Identity $nodeObject -PrincipalsAllowedToDelegateToAccount $gatewayObject
```

詳しくは、以下のドキュメントで説明されています。

Configure User Access Control and Permissions | Configure single sign-on

<https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/configure/user-access-control#configure-single-sign-on>

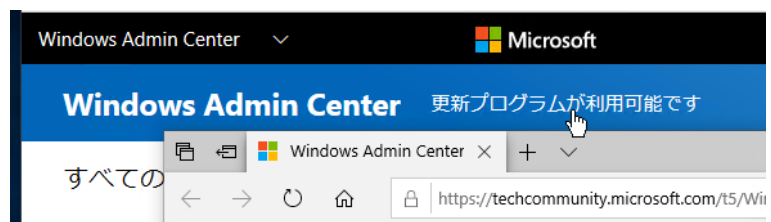


Windows Admin Center のメジャーバージョンアップとサポート期間について

Windows Admin Center は半期チャネル (4 月頃と 9 月頃) で新しいバージョンがリリースされます。また、メンテナンスのために、マイナーバージョンが提供される場合があります (例えば、バージョン 1904 に対するバージョン 1904.1)。Microsoft Update を使用するように構成されている場合 (推奨)、Windows Admin Center は Windows Update を通じて最新バージョンに更新されます。

新バージョンがリリースされると、Windows Admin Center のトップやバージョン情報の下に**“更新プログラムが利用可能です”**と通知

されるので、手動で更新することもできます。なお、メジャーバージョンが利用可能になると、以前のバージョンは 30 日でサポート終了になることに注意してください。



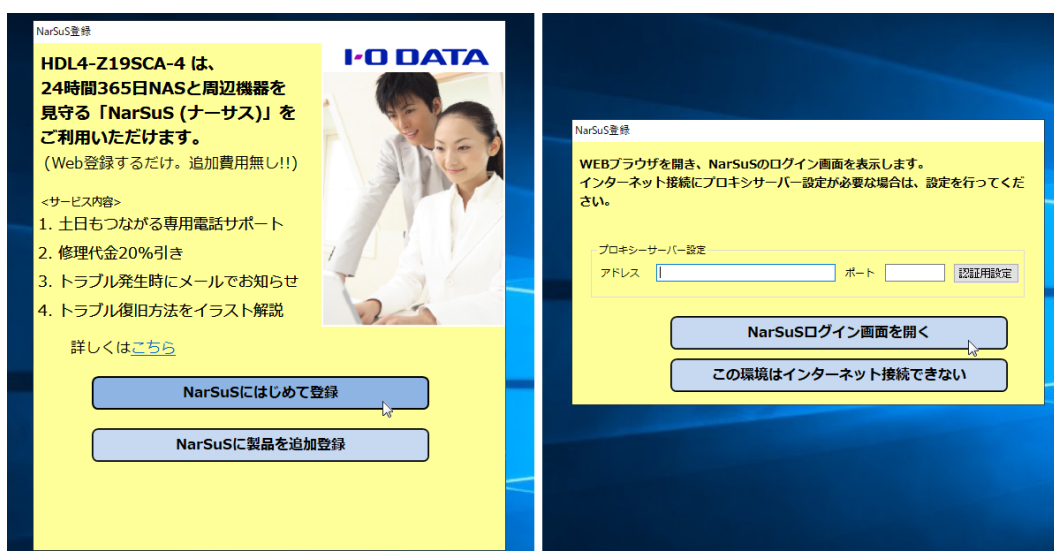
3 クラウド管理機能 NarSuS の活用

アイ・オー・データの NarSuS は、NarSuS に対応する NAS デバイスの購入者に無料で提供されるクラウドベースの管理機能です。ここではサービスへの NAS デバイスの登録手順と管理ポータルへのアクセス方法について説明します。

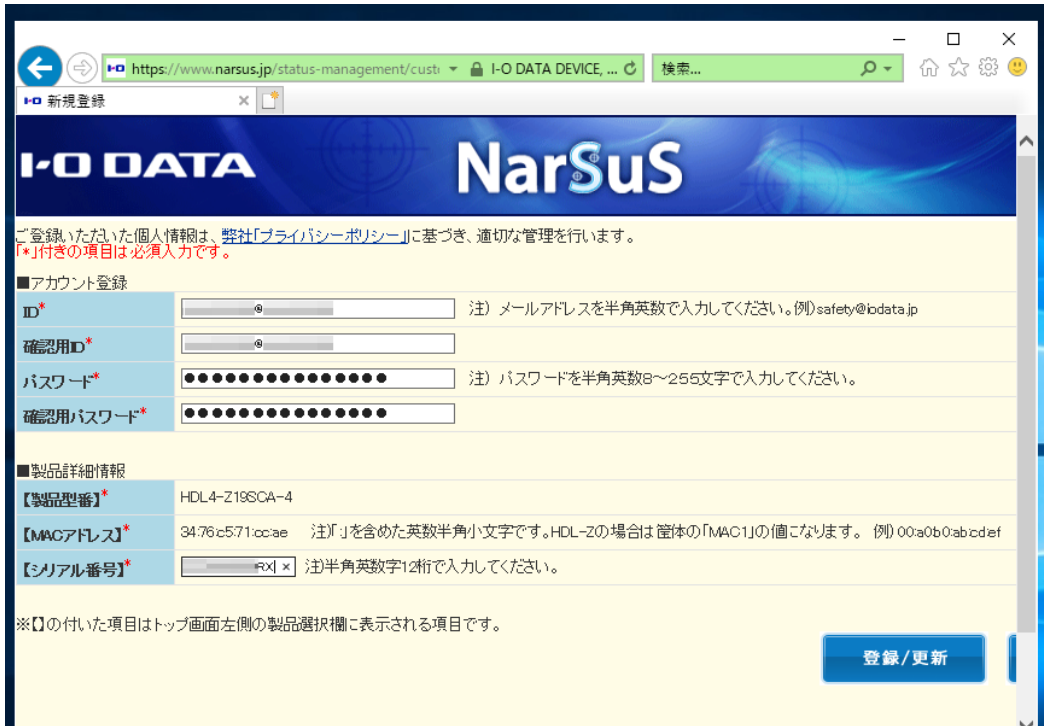
3.1 サービスへの NAS デバイスの登録

LAN DISK Z を導入し、NarSuS への登録をまだ行っていない場合は、リモートデスクトップ接続によるログイン時に [NarSuS 登録] ウィンドウが表示されます。登録を開始するには、次の手順で操作します。

1. [NarSuS 登録] ウィンドウで [NarSuS にはじめて登録] をクリックし、次の画面で [NarSuS ログイン画面を開く] をクリックします。



2. 既定の Web ブラウザー (Internet Explorer 11) で「NarSuS ご登録案内」ページが開くので、重要なお知らせを確認した上で、[同意/新規登録] をクリックします。
3. 「新規登録」ページが開くので、有効な電子メールアドレスを入力し、NarSuS の管理ポータルにログインするために使用するパスワードを設定します。製品のシリアル番号を入力したら [登録/更新] をクリックします。



- 「登録確認」ページが開くので、登録内容に問題がなければ[この内容で登録する]をクリックします。
- NarSuS の管理ポータルトップページに移動します。NAS デバイスからの通知が受信され、情報が取得されるまでしばらく時間がかかるため、ページ右上の[ログアウト]をクリックして管理ポータルを閉じます。



- 他にも未登録のNASデバイスがある場合は、NASデバイスごとに[NarSuS登録]ウィンドウで[NarSuSに製品を追加登録]をクリックして、登録済みのユーザーID（メールアドレス）とパスワードを使用してNASデバイスを登録してください。

3.2 専用ポータルでのステータス監視

NarSuS に NAS デバイスを登録したら、NarSuS の管理ポータルにいつでも、どこからでもログインして 1 台以上の NAS デバイスのステータスを確認することができます。NarSuS の管理ポータルにアクセスするには、Web ブラウザーで次の URL にアクセスし、ユーザー ID として登録したメールアドレスとパスワードを入力します。

クラウド状態管理 NarSuS (ログイン)

<https://www.narsus.jp/>

