



# クラウドネイティブの**SAP** **HANA**データベースをバックアップ BlueXP backup and recovery

NetApp  
April 18, 2024

# 目次

クラウドネイティブのSAP HANAデータベースをバックアップ .....	1
クイックスタート .....	1
Azure NetApp Files を設定します .....	2
SnapCenter Plug-in for SAP HANAをインストールし、データベースホストを追加します .....	2
クラウドネイティブのSAP HANAデータベースをバックアップ .....	8

# クラウドネイティブのSAP HANAデータベースをバックアップ

## クイックスタート

これらの手順を実行すると、すぐに作業を開始できます。

1

構成がサポートされていることを確認します

- オペレーティングシステム
  - RHEL 7.6以降
  - SAP-HANA SPS07の場合はRHEL 8.1以降
  - SLES 12 SP5以降および15 SPXプラットフォームは、SAP HANAによって認定されています
- ネットアップクラウドストレージ：Azure NetApp Files
- ストレージレイアウト：データファイルとログファイルについては、AzureでサポートされるのはNFSv4.1のみです。
- データベースレイアウト：
  - シングルテナントまたは複数テナントのSAP HANAマルチテナントデータベースコンテナ（MDC）2.0SPS5、2.0SPS6、2.0SPS7
  - SAP HANAシングルホストシステム、SAP HANAマルチホストシステム、HANAシステムレプリケーション
- データベースホスト上のSAP HANAプラグイン

2

BlueXPにサインアップします

BlueXPにはWebベースのコンソールからアクセスできます。BlueXPの利用を開始するには、まず既存のNetApp Support Site クレデンシャルを使用するか、ネットアップクラウドログインアカウントを作成して登録します。詳細については、[を参照してください "BlueXPにサインアップします"](#)。

3

BlueXPにログインします

BlueXPに登録すると、Webベースのコンソールからログインできます。詳細については、[を参照してください "BlueXPにログインします"](#)。

4

BlueXPアカウントを管理します

ユーザー、サービスアカウント、ワークスペース、コネクタを管理することで、アカウントを管理できます。詳細については、[を参照してください "BlueXPアカウントを管理します"](#)。

# Azure NetApp Files を設定します

BlueXPを使用してAzure NetApp Files 作業環境を作成し、ボリュームや追加のデータサービスを追加および管理する必要があります。Azureでコネクタを作成して、パブリッククラウド環境内のリソースとプロセスをBlueXPで管理できるようにすることも必要です。

## Azure NetApp Files 作業環境を作成します

データベースがホストされているAzure NetApp Files 作業環境を作成する必要があります。詳細については、を参照してください ["Azure NetApp Files の詳細をご覧ください"](#) および ["Azure NetApp Files 作業環境を作成します"](#)。

### コネクタを作成します

BlueXPのアカウント管理者は、Azureにコネクタを導入して、パブリッククラウド環境内のリソースとプロセスをBlueXPで管理できるようにする必要があります。

詳細については、を参照してください ["BlueXPからAzureにコネクタを作成します"](#)。

- コネクタからデータベースホストへの接続が確立されていることを確認します。
- Azure NetApp Files の作業環境とデータベースが同じ仮想ネットワーク（VNet）にある場合は、コネクタを同じVNetに導入できます。
- Azure NetApp Files 作業環境とデータベースが異なるVNetにあり、Azure NetApp Files でNAS（NFS）ワークロードが設定されている場合は、どちらかのVNetにコネクタを作成できます。

コネクタを作成したら、[ストレージ]>\* Canvas >[マイ作業環境]>[作業環境の追加]\*をクリックして作業環境を追加します。

## SnapCenter Plug-in for SAP HANAをインストールし、データベースホストを追加します

各SAP HANAデータベースホストにSnapCenter Plug-in for SAP HANAをインストールする必要があります。SAP HANAホストでSSHキーベースの認証が有効になっているかどうかに応じて、いずれかの方法でプラグインをインストールできます。

- データベース・ホストでSSHが有効になっている場合は、SSHオプションを使用してプラグインをインストールできます。 [詳細はこちら](#)。。
- SSHが無効になっている場合は、プラグインを手動でインストールします。 [詳細はこちら](#)。。

### 前提条件

ホストを追加する前に、前提条件を満たしていることを確認する必要があります。

- 各SAP HANAデータベースホストにJava 11（64ビット）Oracle JavaまたはOpenJDKがインストールされていることを確認します。

- 作業環境を追加し、コネクタを作成しておく必要があります。
- コネクタがSAP HANAデータベースホストに接続されていることを確認します。

接続問題を解決する方法については、を参照してください ["BlueXP Connectorホストからアプリケーションデータベースホストへの接続を検証できませんでした"](#)。

コネクタが失われた場合、または新しいコネクタを作成した場合は、コネクタを既存のアプリケーションリソースに関連付ける必要があります。コネクタを更新する手順については、を参照してください ["コネクタの詳細を更新します"](#)。

- BlueXPユーザーに「アカウント管理者」の役割があることを確認します。
- SnapCenter ユーザを作成し、root以外（sudo）ユーザにsudoを設定しておく必要があります。詳細については、を参照してください ["SnapCenter ユーザにsudoを設定します。"](#)
- データベースホストを追加する前に、SnapCenter Plug-in for SAP HANAをインストールしておく必要があります。
- SAP HANAデータベースホストを追加する場合は、HDBユーザストアキーを追加する必要があります。HDBセキュアユーザストアキーは、SAP HANAデータベースホストの接続情報をクライアントにセキュアに格納し、HDBSQLクライアントでセキュアなユーザストアキーを使用してSAP HANAデータベースホストに接続するために使用されます。
- HANA System Replication（HSR；システムレプリケーション）の場合、HANAシステムを保護するには、プライマリとセカンダリの両方のHANAシステムを手動で登録する必要があります。



ホスト名は、HSRレプリケーションで使用するホストのホスト名と同じである必要があります。

- SSHベースのインストールを実行する場合は、コネクタでSSHポートへの通信が有効になっていることを確認します（デフォルト：22）。
- データ保護処理が機能するように、コネクタがプラグインポート（デフォルト：8145）との通信が有効になっていることを確認します。
- 最新バージョンのプラグインがインストールされていることを確認します。プラグインをアップグレードするには、を参照してください [SnapCenter Plug-in for SAP HANA Databaseをアップグレードします](#)。

## SnapCenter ユーザにsudoを設定します

プラグインをインストールするには、root以外のユーザ（sudo）を作成してください。

### 手順

1. Connector VMにログインします。
2. SnapCenter Linuxホストプラグインバイナリをダウンロードします。  

```
sudo docker exec -it cloudmanager_scs_cloud curl -X GET 'http://127.0.0.1/deploy/downloadLinuxPlugin'
```
3. `/var/lib/docker/volumes/service-manager-2_cloudmanager_SCS_cloud_volume/_data/$`（`sudo docker ps | grep -PO "cloudmanager_SCS_cloud:.*" | sed -e 's/.$//' | cut -f2 -d ':'`）にある `sudoer.txt` の内容をコピーします。`"|sed -e 's/.$//' | cut -f2 -d ':'`） `/sc-linux-host-plugin`
4. rootユーザアカウントを使用してSAP HANAシステムホストにログインします。
5. 手順3でコピーしたテキストを `/etc/sudoers.d/snapcenter_file` にコピーして、root以外のユーザにsudoアク

セスを設定します。

/etc/sudoers.d/snapcenter\_fileに追加した行で、<LINUXUSER>\_をroot以外のユーザに、<USER\_HOME\_DIRECTORY>\_を\_HOME /<non-root-user>\_に置き換えます。

## スクリプトを使用してプラグインをインストールします

SAP HANAホストのroot以外のユーザアカウントに対してSSHキーベースの認証を設定し、次の手順を実行してプラグインをインストールします。

始める前に

コネクタへのSSH接続が有効になっていることを確認します。

手順

1. コネクタVMにログインします。
2. コネクタに付属のスクリプトを使用してプラグインをインストールします。  

```
sudo bash /var/lib/docker/volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port>
```

古いコネクタを使用している場合は、次のコマンドを実行してプラグインをインストールします。

```
sudo /var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port>
```

名前	説明	必須	デフォルト
plugin_hostの略	SAP HANAホストを指定します	はい。	-
host_user_nameを指定します	SAP HANAホストに対するSSH権限を持つSnapCenter ユーザを指定します	はい。	-
host_ssh_keyを指定します	SnapCenter ユーザのSSHキーを指定します。このキーは、SAP HANAホストへの接続に使用されます	はい。	-
PLUGIN_PORT	プラグインで使用されるポートを指定します	いいえ	8145
host_ssh_portを指定します	SAP HANAホストのSSHポートを指定します	いいえ	22

たとえば、'sudo bash /var/lib/docker/volumes/service-manager-2\_cloudmanager\_SCS\_cloud\_volume/\_data/scripts/linux\_plugin\_copy\_and\_install.sh --host 10.0.1.1 --username SnapCenter --sshkey/keys/netapp-ssh.ppk'と入力します

プラグインをインストールしたら、インストールする必要があります [SAP HANAデータベースホストを追加します](#)。

## プラグインを手動でインストールします

HANAホストでSSHキーベースの認証が有効になっていない場合は、以下の手順を実行してプラグインをインストールする必要があります。

### • 手順 \*

1. コネクタVMにログインします。

2. SnapCenter Linuxホストプラグインバイナリをダウンロードします。

```
sudo docker exec -it cloudmanager_scs_cloud curl -X GET  
'http://127.0.0.1/deploy/downloadLinuxPlugin'
```

プラグインのバイナリは次の場所にあります。cd /var/lib/docker/volumes/service-manager-2\_cloudmanager\_SCS\_cloud\_volume/\_data/\$ (sudo docker ps | grep -po "cloudmanager\_SCS\_cloud:.? " | sed -e 's/[/]/ cut-f2-d' : ") /sc-linux-host-plugin

3. scpまたはその他の方法を使用して、各<non root user (sudo)> HANAデータベースホストの\_/home/sapan/.sc\_netapp\_pathに上記のパスから\_snapcenter\_linux\_host\_plugin\_sc.bin\_をコピーします。

4. root以外のアカウント (sudo) を使用してSAP HANAデータベースホストにログインします。

5. ディレクトリを\_/home/home /<non root user> /.sc\_netapp/\_に変更し、次のコマンドを実行してバイナリの実行権限を有効にします。

```
chmod +x snapcenter_linux_host_plugin_scs.bin
```

6. sudo SnapCenter ユーザとしてSAP HANAプラグインをインストールします。

```
./snapcenter_linux_host_plugin_scs.bin -i silent -DSPL_USER=<non-root>
```

7. コネクタVMのcopy\_certificate.pem\_from\_certificate/client/certificate/path <base\_mount\_path>をプラグインホストの/var/opt/snapcenter/spl/etc/にコピーします。

8. /var/opt/snapcenter/spl/etcに移動し、keytoolコマンドを実行して証明書をインポートします。

```
keytool -import -alias agentcert -file certificate.pem -keystore  
keystore.jks -deststorepass snapcenter -noprompt
```

9. SPLを再起動します。systemctl restart spl

10. コネクタから次のコマンドを実行して、コネクタからプラグインに到達できることを確認します。

```
docker exec -it cloudmanager_scs_cloud curl -ik https://<FQDN or IP of the  
plug-in host>:<plug-in port>/PluginService/Version --cert  
config/client/certificate/certificate.pem --key  
/config/client/certificate/key.pem
```

プラグインをインストールしたら、インストールする必要があります [SAP HANAデータベースホストを追加します](#)。

## SnapCenter Plug-in for SAP HANA Databaseをアップグレードします

最新の新機能や機能拡張を利用するには、SnapCenter Plug-in for SAP HANAデータベースをアップグレードする必要があります。

- 始める前に \*
  - ホストで実行中の処理がないことを確認します。
  - 手順 \*
1. SnapCenter ユーザにsudoを設定します。詳細については、を参照してください [SnapCenter ユーザにsudoを設定します](#)。
  2. 次のスクリプトを実行します。

```
/var/lib/docker/volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port> --upgrade
```

古いコネクタを使用している場合は、次のコマンドを実行してプラグインをアップグレードします。

```
/var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port> --upgrade
```

## SAP HANAデータベースホストを追加します

ポリシーを割り当ててバックアップを作成するには、SAP HANAデータベースホストを手動で追加する必要があります。SAP HANAデータベースホストの自動検出はサポートされていません。

- 手順 \*
1. BlueXP \* UIで、[保護]>[アプリケーション]\*を選択します。
  2. [アプリケーションの検出]\*を選択します。
  3. Cloud Native > SAP HANA を選択し、Next \*を選択します。
  4. [アプリケーション]ページで、\*[システムの追加]\*を選択します。
  5. [システムの詳細\*]ページで、次の操作を実行します。
    - a. [System Type]で、[Multi-tenant database container]または[Global Non-Data Volumes]を選択します。
    - b. SAP HANAシステムの名前を入力します。
    - c. SAP HANA システムの SID を指定します。
    - d. (任意) OSDBユーザを変更します。
    - e. HANAシステムがHANAシステムレプリケーションで構成されている場合は、\* HANA System Replication (HSR) System \*を有効にします。
    - f. [HDB Secure User Store Keys]\*テキストボックスを選択して、ユーザストアキーの詳細を追加します。



キー名、システムの詳細、ユーザー名、パスワードを指定し、\*キーの追加\*をクリックします。

ユーザストアキーは削除または変更できます。

6. 「\*次へ\*」を選択します。
7. [ホストの詳細]\*ページで、次の操作を実行します。
  - a. または[既存のホストを使用]\*を選択します。
  - b. または[Manual]\*を選択します。

[Manual]に、ホストのFQDNまたはIP、コネクタ、ユーザ名、SSHポート、プラグインポートを入力します。必要に応じて、SSH秘密鍵を追加して検証します。

SSHの場合は、ホストのFQDNまたはIP、コネクタ、ユーザ名、およびプラグインポートを入力します。

- a. 「\*次へ\*」を選択します。
  1. [ホスト設定]ページで、設定要件を満たしているかどうかを確認します。

確認するチェックボックスをオンにします。

2. 「\*次へ\*」を選択します。
  3. [ストレージフットプリント]ページで\*[ストレージの追加]\*を選択し、次の手順を実行します。
- b. 作業環境を選択し、ネットアップアカウントを指定します。

左側のナビゲーションペインで、BlueXP \* Canvas \*を選択して新しい作業環境を追加します。

- c. 必要なボリュームを選択します。
- d. [ストレージの追加]\*を選択します。
  1. すべての詳細を確認し、\*[システムの追加]\*を選択します。

UIからSAP HANAシステムを変更または削除できます。

SAP HANAシステムを削除する前に、関連付けられているバックアップをすべて削除し、保護を解除する必要があります。

非データボリュームを追加します

マルチテナントデータベースコンテナタイプをSAP HANAシステムに追加したら、HANAシステムのデータボリューム以外のボリュームを追加できます。

使用可能な SAP HANA データベースを検出したあと、それらのリソースをリソースグループに追加してデータ保護処理を実行できます。

• 手順 \*

1. BlueXP\* UIで、[保護>\*バックアップとリカバリ\*>\*アプリケーション\*]をクリックします。
2. [アプリケーションの検出]をクリックします。
3. Cloud Native > SAP HANA を選択し、Next \*をクリックします。

4. [アプリケーション]ページで、をクリックします ... 非データボリュームを追加するシステムに対応し、システム管理>\*非データボリューム\*を選択します。

## グローバル非データボリュームの追加

マルチテナントデータベースコンテナタイプがSAP HANAシステムの追加後に、HANAシステムのグローバルデータボリューム以外のボリュームを追加できます。

### • 手順 \*

1. BlueXP\* UIで、[保護>\*バックアップとリカバリ\*>\*アプリケーション\*]をクリックします。
2. [アプリケーションの検出]をクリックします。
3. Cloud Native > SAP HANA を選択し、Next \*をクリックします。
4. [アプリケーション]ページで、[システムの追加]をクリックします。
5. [システムの詳細\*]ページで、次の操作を実行します。
  - a. System Type (システムタイプ) ドロップダウンから、\* Global Non-Data Volume (グローバル非データボリューム) \*を選択します。
  - b. SAP HANAシステムの名前を入力します。
6. 。[ホストの詳細]\*ページで、次の操作を実行します。
  - a. SAP HANAシステムの関連付けられたSIDを指定します。
  - b. プラグインホストを選択します
  - c. 「\* 次へ \*」をクリックします。
  - d. すべての詳細を確認し、\*システムの追加\*をクリックします。

## クラウドネイティブの**SAP HANA**データベースをバックアップ

組み込みのポリシーまたは作成したポリシーを割り当てることで、バックアップを作成できます。

### **SAP HANA**データベースを保護するポリシーを作成します

組み込みポリシーを使用または編集しない場合は、ポリシーを作成できます。

1. [アプリケーション]ページの[設定]ドロップダウンリストから、[ポリシー]を選択します。
2. [ポリシーの作成] をクリックします。
3. ポリシー名を指定します。
4. (オプション) Snapshotコピー名の形式を編集します。
5. ポリシータイプを選択します。
6. スケジュールと保持の詳細を指定します。
7. (任意) スクリプトを指定します。 **"プリスクリプトとポストスクリプト"**
8. [作成 (Create) ] をクリックします。

## プリスクリプトとポストスクリプト

ポリシーの作成時にプリスクリプト、ポストスクリプト、および終了スクリプトを指定できます。これらのスクリプトは、データ保護処理中にHANAホストで実行されます。

サポートされているスクリプトの形式は、.sh、Pythonスクリプト、perlスクリプトなどです。

プリスクリプトとポストスクリプトは、ホスト管理者がに登録する必要があります  
/opt/NetApp/snapcenter/scc/etc/allowed\_commands.config ファイル。

```
[root@scspa2622265001 etc]# cat allowed_commands.config
command: mount
command: umount
command: /mnt/scripts/pre_script.sh
command: /mnt/scripts/post_script.sh
```

## 環境変数

バックアップワークフローでは、プリスクリプトとポストスクリプトで次の環境変数を使用できます。

環境変数	説明
SID	リストア用に選択したHANAデータベースのシステムID
BackupNameの略	リストア処理用に選択されたバックアップ名
UserStoreKeyNames	HANAデータベース用にユーザストアキーを設定しました
OSDBUser	HANAデータベース用にOSDBUserを設定
実行します	スケジュールされたバックアップの場合のみ
schedule_type	スケジュールされたバックアップの場合のみ

## SAP HANAデータベースのバックアップを作成します

組み込みポリシーを割り当てるか、ポリシーを作成してデータベースに割り当てることができます。ポリシーを割り当てると、ポリシーで定義されたスケジュールに従ってバックアップが作成されます。

- 始める前に \*

SAP HANAデータベースホストを追加しておく必要があります。  
["SAP HANAデータベースホストを追加します"](#)

- このタスクについて \*

HANAシステムレプリケーション（HSR）の場合、スケジュールされたバックアップジョブはプライマ

リHANAシステムに対してのみトリガーされ、システムがセカンダリHANAシステムにフェイルオーバーすると、既存のスケジュールによって現在のプライマリHANAシステムでバックアップがトリガーされます。ポリシーがプライマリとセカンダリの両方のHANAシステムに割り当てられていないと、フェイルオーバー後にスケジュールが失敗します。

複数のポリシーがHSRシステムに割り当てられている場合、プライマリとセカンダリの両方のHANAシステムでスケジュールされたバックアップトリガーと、セカンダリHANAシステムのバックアップは失敗します。

• 手順 \*

1. [アプリケーション]ページで、データベースがポリシーを使用して保護されていない場合は、[ポリシーの割り当て]をクリックします。

データベースは1つ以上のポリシーを使用して保護されていますが、必要に応じてをクリックして、さらにポリシーを割り当てることができます ... >\*ポリシーの割り当て\*。

2. ポリシーを選択し、\* assign \*をクリックします。

バックアップは、ポリシーで定義されたスケジュールに従って作成されます。



スケジュールされたバックアップ処理の実行には、サービスアカウント（\_SnapCenter-account-<account\_id>\_）を使用します。

## SAP HANAデータベースのオンデマンドバックアップを作成する

ポリシーを割り当てたら、アプリケーションのオンデマンドバックアップを作成できます。

• 手順 \*

1. [アプリケーション]ページで、をクリックします ... アプリケーションに対応して、\*オンデマンドバックアップ\*をクリックします。
2. オンデマンドバックアップタイプを選択します。
3. ポリシーベースのバックアップの場合、ポリシーと保持階層を選択し、\*バックアップの作成\*をクリックします。
4. Snapshotコピーベースを1回選択するか、ファイルベースを選択して、次の手順を実行します。
  - a. 保持値を選択し、バックアップ名を指定します。
  - b. （任意）スクリプトおよびスクリプトのパスを指定します。

詳細については、を参照してください ["プリスクリプトとポストスクリプト"](#)

- c. [バックアップの作成 \*] をクリックします。

## 著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。