



VERITAS™

Veritas NetBackup 10.4

セキュリティ・認証 利用ガイド MFA編

(Multi-Factor Authentication)

ベリタステクノロジーズ合同会社

Veritas テクニカルガイド

免責事項

- ベリタステクノロジーズは、この文書の著作権を留保します。また、記載された内容の無謬性を保証しません。
- 当ガイドは代表的な構成方法や操作の一般的な手順をご紹介することを目的としています。
- 機能の全ての範囲を網羅した説明を行うものではありません。詳細な情報は、製品マニュアルを参照ください。
- NetBackupは将来に渡って仕様を変更する可能性を常に含み、これらは予告なく行われることもあります。
- なお、当ドキュメントの内容は参考資料として、読者の責任において管理/配布されるようお願いいたします。

当資料の コンテンツ

1. 機能紹介
2. MFAの設定手順
3. 全ユーザーに対するMFAの設定

1. 機能紹介

1. 機能紹介

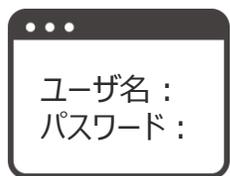
NetBackupにおけるMFA (Multi-Factor Authentication) とは

インターネット接続不要な多要素認証

(RFC-6238に準拠した時間ベースのワンタイムパスワード)

- ✓ システムへ接続する際、ユーザ名 / パスワードに加えて追加の認証手順が必要となる機能。
- ✓ MFAは不正なアカウントアクセスを防止します。
- ✓ 各コンポーネントのSSH/WebUI接続に対応。
- ✓ 全ユーザにMFAを強制させることが可能です。

1段階目の認証



ユーザ名:
パスワード:

ユーザ名/パスワード
による認証

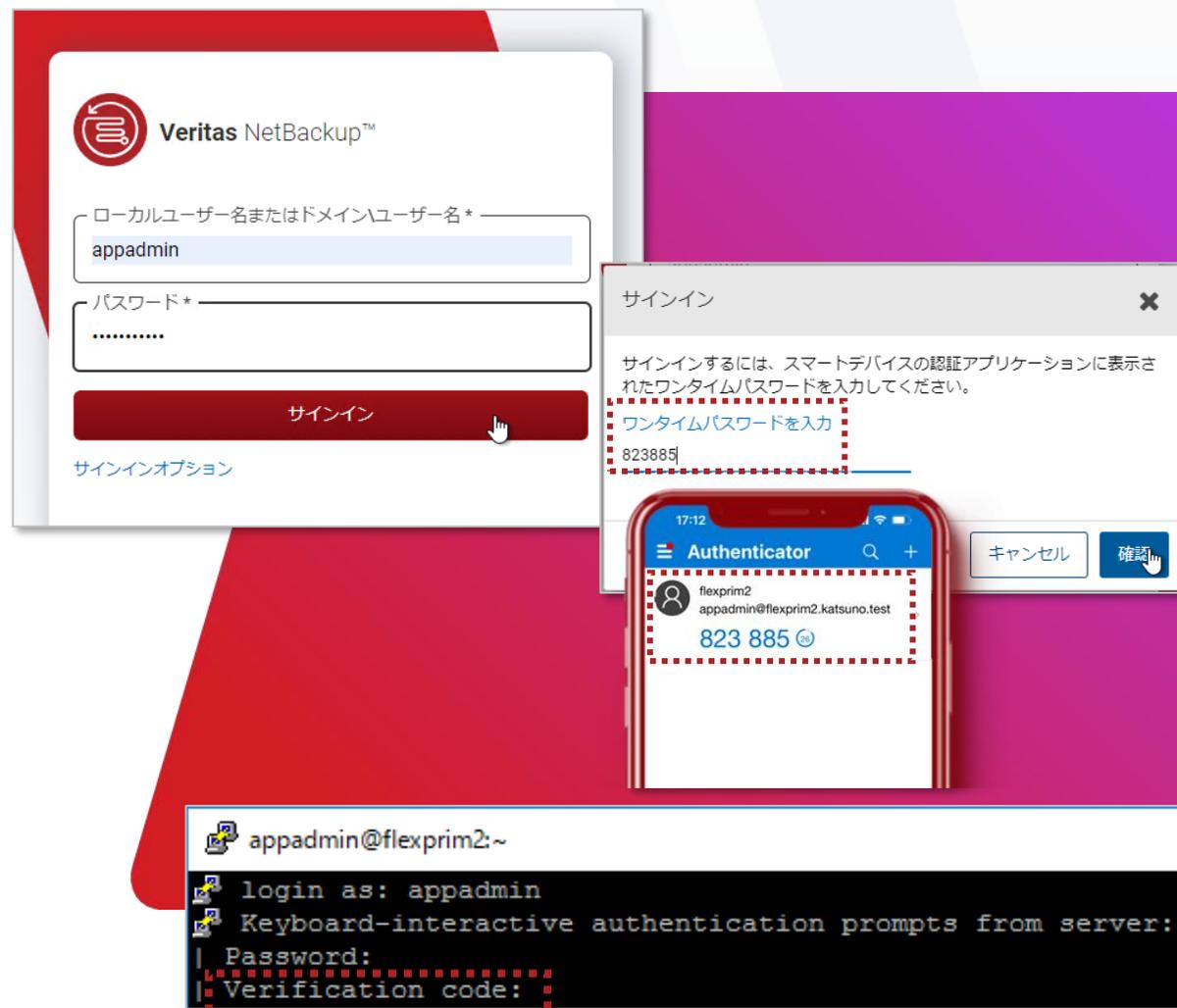
2段階目の認証



6桁の認証コード



認証完了!!



1. 機能紹介

前提条件

- MFAの機能を利用する場合、NetBackupのバージョンは10.3以降でサポートされています。
 - リスクエンジンによるMFAの再認証については、10.4以降からのサポートとなります。（P.9 参照）
- サポートされているTOTP（Time-Based One-Time Password Algorithm）アプリケーション
 - Microsoft Authenticator
 - Google Authenticator
 - Okta Authenticator
 - 上記以外にも、RFC-6238に準拠したTOTPアプリケーションであれば使用可能です。
- 参考情報
 - NetBackup セキュリティおよび暗号化ガイド バージョン10.4 - 多要素認証の構成
https://sort.veritas.com/doc_viewer/#/content?id=32258597-164728727-0%2Fv162211621-164728727
 - NetBackup Web UI 管理者ガイドバージョン10.4 - 多要素認証の構成
https://sort.veritas.com/doc_viewer/#/content?id=152422053-164219671-0%2Fv162561429-164219671
 - Setting up multi-factor authentication for NetBackup on user's authenticator application.
https://www.veritas.com/support/en_US/article.100060168

1. 機能紹介

Flex Applianceの管理コンソールにも対応

Flex Applianceの管理コンソールにも対応しています。

Veritas™ Flex Appliance Console

Username *
admin

Password *
.....

Sign in

Sign-in options

Product information
Documentation
SORT (Veritas Services and Operations Readiness Tools)
Terms and Conditions
Copyright © 2023 Veritas Technologies LLC. All rights reserved.

Veritas™ Flex Appliance Console

Enter the 6-digit confirmation code from the authenticator app.

Code
998213

Cancel Submit

Authenticator

Flex
998213
admin@flex02.lab.local

Okta

Veritas™ Flex Appliance Console

Home

Storage
Allocated Total TIB
0 % TIB Allocated TIB Available

Instances
Online Offline Faulted
0 0 0

Security meter
Good Excellent

Call Home
Not configured
Configure now to:
Proactively monitor appliance components
Autogenerate a support case when a hardware alert occurs
Improve error analysis

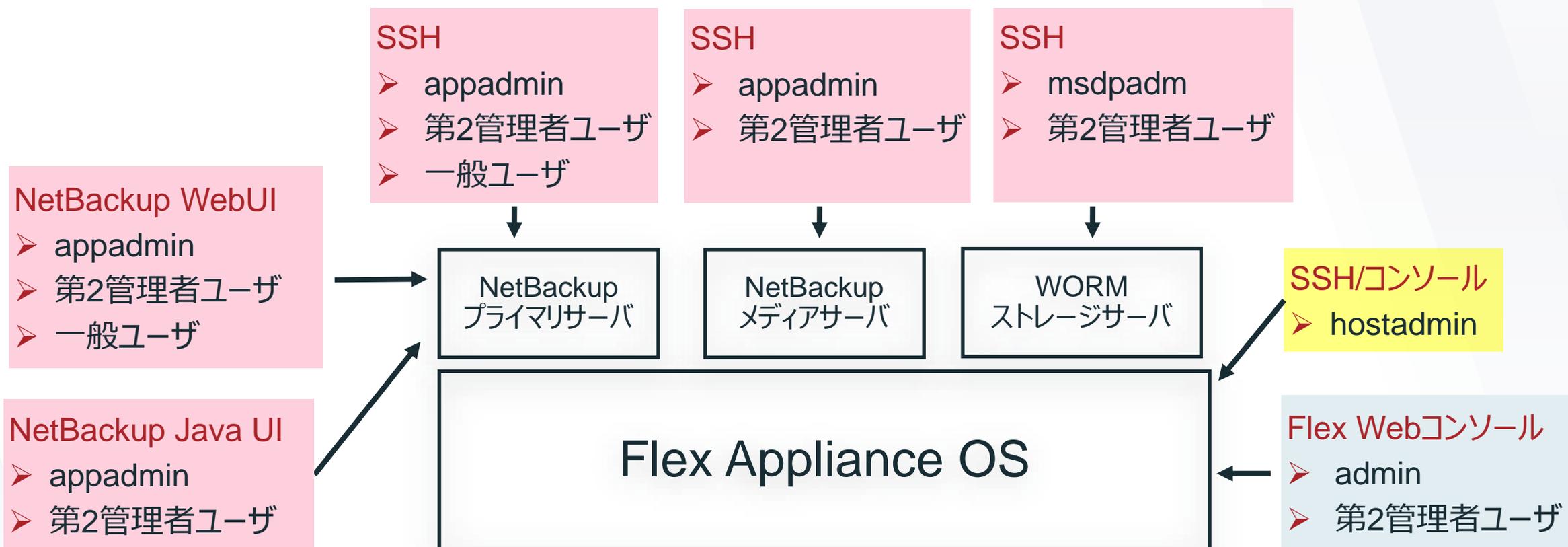
Performance
Nodes
Timeframe Last 24 hours Metrics 3 of 3 metrics Nodes 1 of 1 nodes Last updated 14:07:47 03/04/2024 Refresh

多要素認証により、特定のデバイスで示されるワンタイムコードを必須とします。

1. 機能紹介

Flex Applianceの管理コンソールにも対応

Flex Applianceは基盤のみならず、NetBackupのコンテナの部分に関しても、WebUI、Javaコンソール、SSHと全面的に多要素認証の構成が可能です。

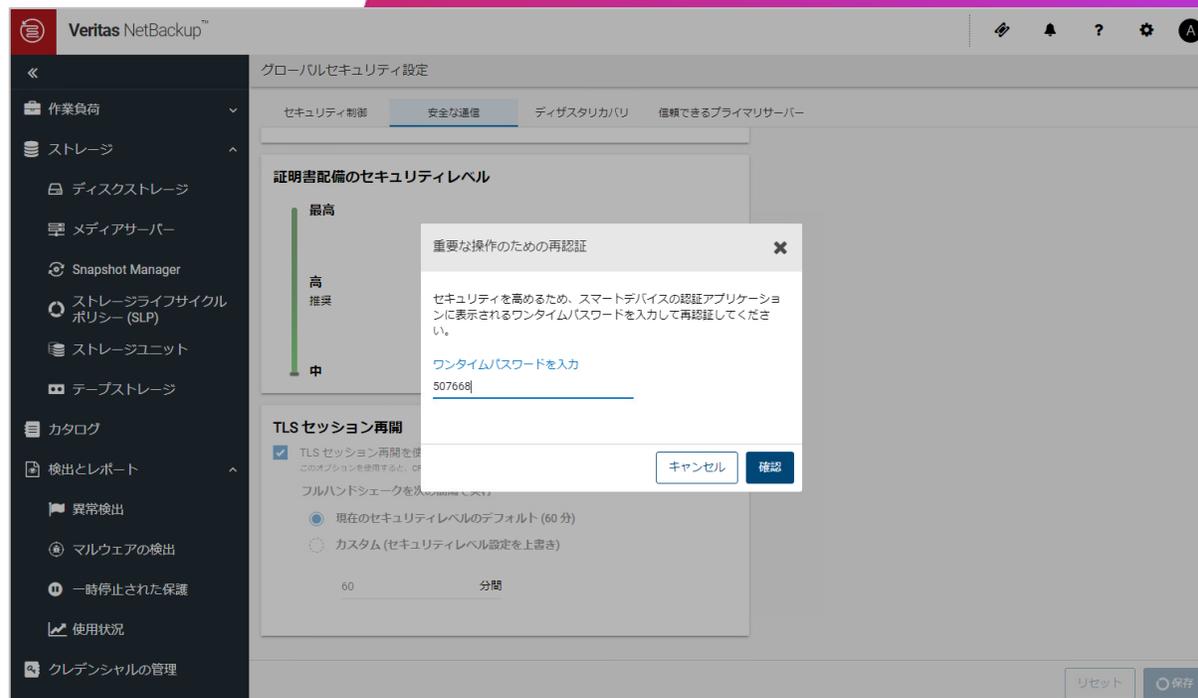


1. 機能紹介

NetBackup 10.4での機能強化

リスクエンジンによるMFAの再認証

- 自己学習型ユーザー行動監視により、リスクの高い異常な操作に対して、ワンタイムパスワードによる再認証が必要となる機能。
 - MFAが構成されているユーザーアカウントが対象となります。
 - MFAが構成されていない場合、再認証を求めるメッセージは表示されません。
- 以下ケースでワンタイムパスワードの再入力が必要となります。
 - グローバルセキュリティの変更時
 - APIキーの作成時



1. 機能紹介

NetBackup 10.4での機能強化 - グローバルセキュリティ変更時のワンタイムパスワード再認証

- グローバルセキュリティ変更時のワンタイムパスワード再認証を有効化する場合、以下を実施してください。
 - [検出とレポート] - [異常検出] - [Secure critical operations]に を入れる。
 - デフォルトで有効になっているため、MFAを設定したタイミングで自動的に有効化されることとなります。

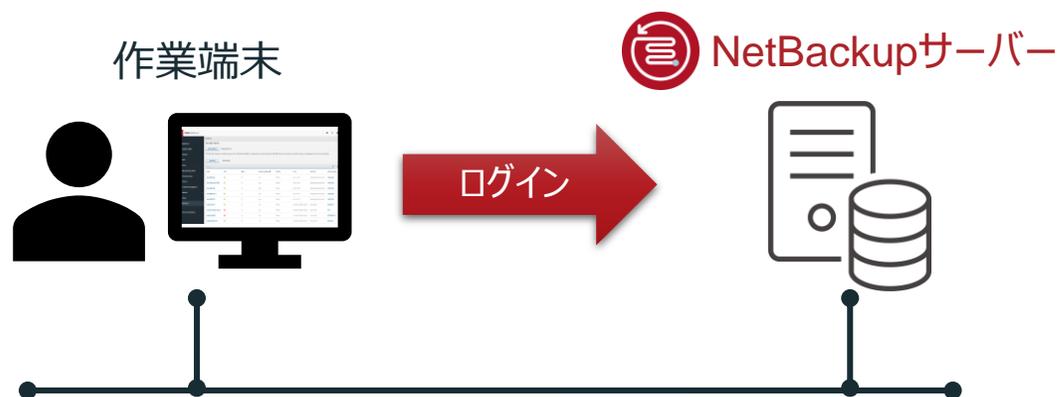
The screenshot shows the Veritas NetBackup console interface. On the left is a dark navigation sidebar with a red header containing the Veritas logo and the text 'Veritas NetBackup™'. The sidebar menu items are: '作業負荷' (Job Load), 'ストレージ' (Storage), 'カタログ' (Catalog), '検出とレポート' (Detection and Reports), '異常検出' (Anomaly Detection), and 'マルウェアの検出' (Malware Detection). The '検出とレポート' item is highlighted with a red border. The main content area is titled 'システムの異常検出の構成' (System Anomaly Detection Configuration) and contains a section for 'リスクエンジンベースの異常検出' (Risk Engine Based Anomaly Detection). This section lists three detection rules, each with a checked checkbox and an '編集' (Edit) button: 'Detect suspicious image expiration' (Detect when images are expired in an unusual or a suspicious manner.), 'Secure critical operations' (Protect global security settings and API key generation with multifactor authentication.), and 'Detect possible session hijack' (Detect if there is a possible user session hijack by a malicious source.). The 'Secure critical operations' rule is highlighted with a red border.

2. MFAの設定手順

2. MFAの設定手順

本ドキュメントにおける環境構成図

- 本ドキュメントで設定手順を紹介するシステム構成は以下のとおりです。



| | |
|------------|-----------------------|
| ホスト名 | prod-primary |
| 役割 | NetBackup サーバー |
| OS | Windows 2022 |
| NetBackup | 10.4 (プライマリ兼メディアサーバー) |
| 管理者ユーザー | veritas01 |
| MFAテストユーザー | tanaka01 |

2. MFAの設定手順

設定手順の流れ



1. MFA（多要素認証）の構成



2. TOTP（Time-based One-Time Password）アプリケーションとの連携



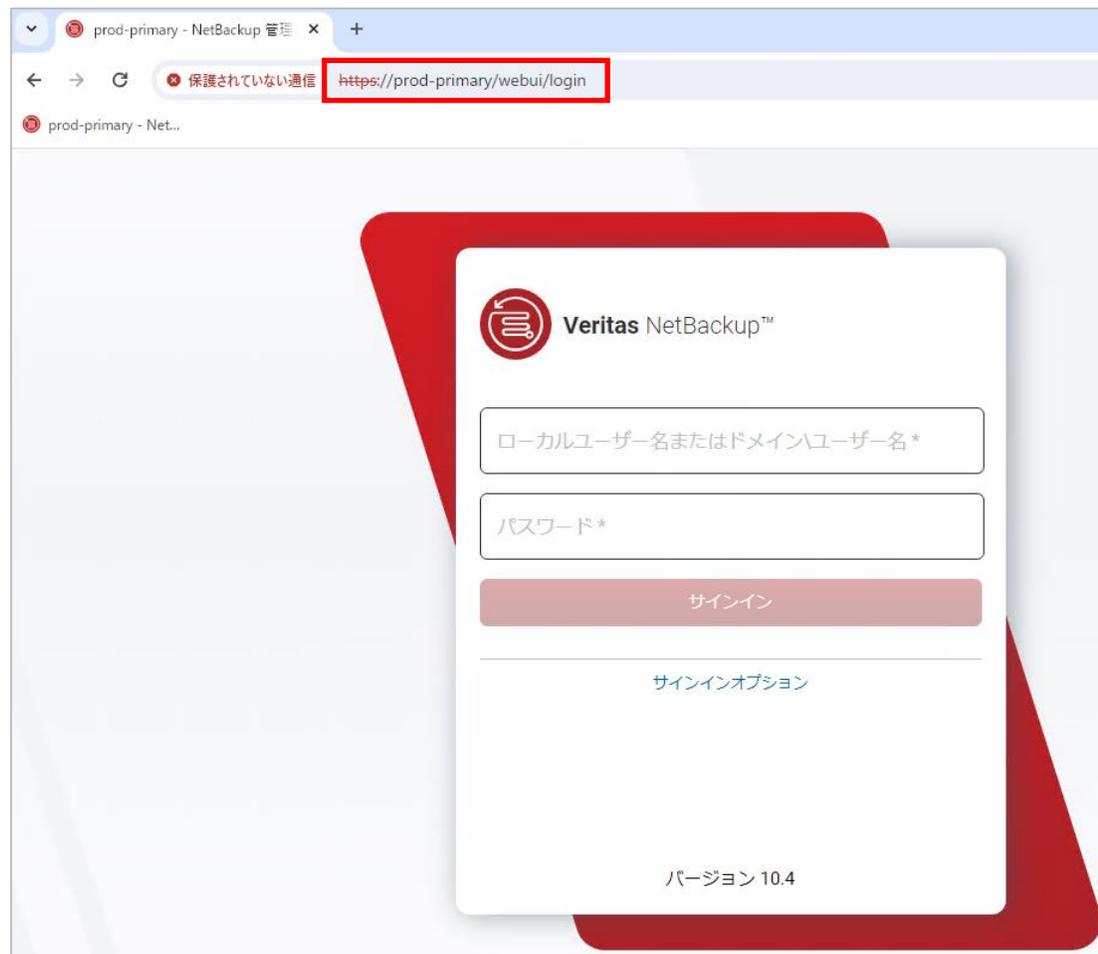
3. NetBackup WebUIを用いた動作確認



4. NetBackup Java管理コンソールを用いた動作確認

2. MFAの設定手順

2-1. MFA（多要素認証）の構成



まず、NetBackup WebUIにログインして、MFAの構成を行います。

- ブラウザを起動し、プライマリサーバーのNetBackup WebUIにアクセスします。
 - 本ドキュメントの場合ですと、以下となります。
<https://prod-primary/webui/login>
 - [prod-primary]がプライマリサーバー名となり、NetBackupインストール時に指定したサーバー名を入力してください。

備考)
プライバシーエラーが発生した場合は次スライドの手順を実施ください。

2. MFAの設定手順

2-1. MFA（多要素認証）の構成

この接続ではプライバシーが保護されません

prod-primary では、悪意のあるユーザーによって、パスワード、メッセージ、クレジットカードなどの情報が盗まれる可能性があります。詳細

NET::ERR_CERT_AUTHORITY_INVALID

Chrome の最高レベルのセキュリティで保護するには、保護強化機能を有効にしてください。

[詳細設定](#)

この接続ではプライバシーが保護されません

prod-primary では、悪意のあるユーザーによって、パスワード、メッセージ、クレジットカードなどの情報が盗まれる可能性があります。詳細

NET::ERR_CERT_AUTHORITY_INVALID

Chrome の最高レベルのセキュリティで保護するには、保護強化機能を有効にしてください。

[詳細情報を表示しない](#) [セキュリティで保護されたページに戻る](#)

このサーバーが **prod-primary** であることを確認できませんでした。このサーバーのセキュリティ証明書は、ご使用のパソコンのオペレーティング システムによって信頼されているものではありません。原因としては、不適切な設定や、悪意のあるユーザーによる接続妨害が考えられます。

[prod-primary にアクセスする \(安全ではありません\)](#)

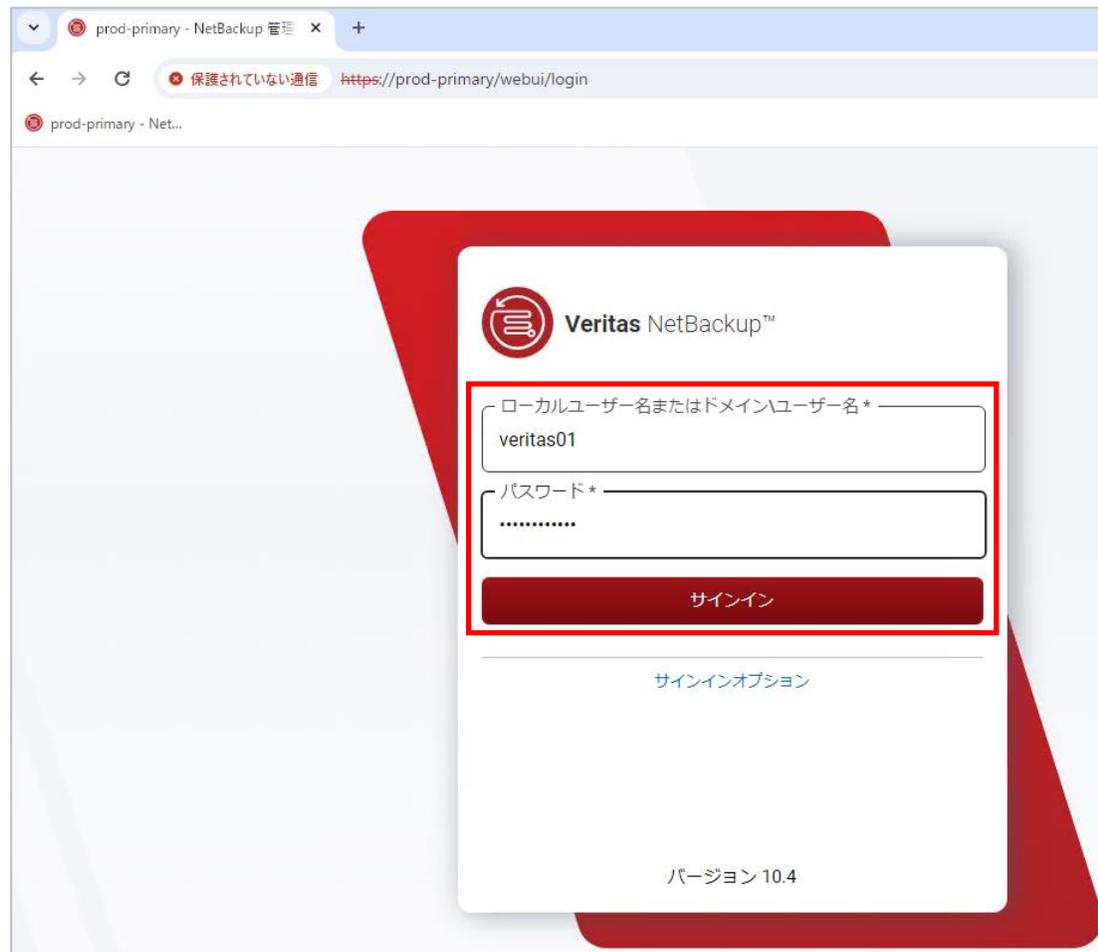
- プライバシーエラーの画面が表示された場合、[詳細設定]をクリックします。

- [prod-primaryにアクセスする（安全ではありません）]をクリックします。

備考)
プライバシーエラーが発生した場合のみ本手順を実施ください。

2. MFAの設定手順

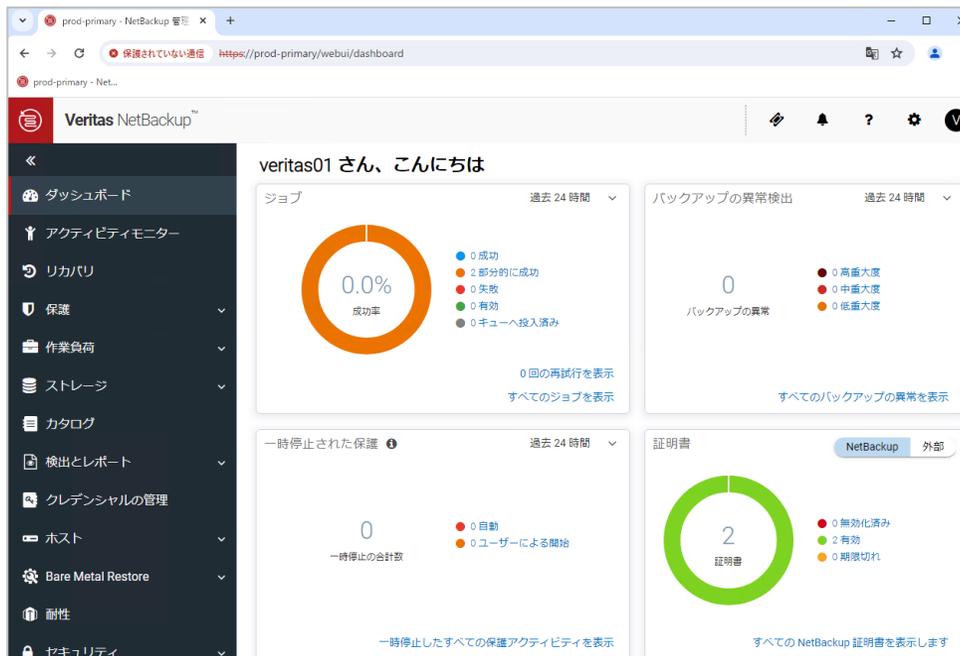
2-1. MFA（多要素認証）の構成



- NetBackup WebUIのログイン画面が表示されるので、[ユーザー名]と[パスワード]を入力します。
 - NetBackupインストール時に使用した管理者権限を持ったユーザーを指定してください。
 - 本ドキュメントでは、[veritas01]ユーザーでログインを行います。
- [サインイン]をクリックして、NetBackup WebUIにログインします。

2. MFAの設定手順

2-1. MFA (多要素認証) の構成



- ダッシュボードが表示されます。



- ようこそ画面が表示された場合は、右上の[×]をクリックしてウィンドウを閉じて下さい。

2. MFAの設定手順

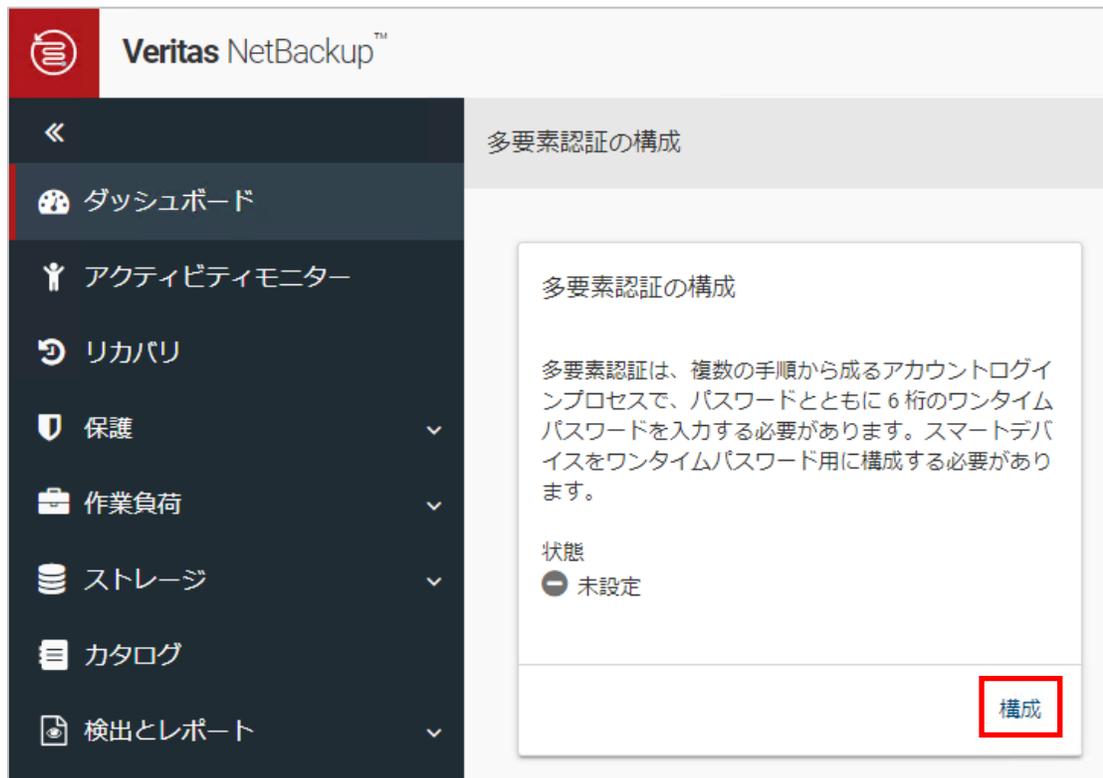
2-1. MFA (多要素認証) の構成



- 画面右上の[プロフィール]をクリックします。
- メニューが表示されるので、[多要素認証の構成]をクリックします。

2. MFAの設定手順

2-1. MFA（多要素認証）の構成



- [構成]をクリックします。

2. MFAの設定手順

2-1. MFA（多要素認証）の構成

多要素認証の構成

アカウントのセキュリティを保護するために多要素認証を構成することを強くお勧めします。

次の手順に従って、認証アプリケーションをスマートデバイスにインストールし、構成します。 [サポートされている認証アプリケーション](#)

- サポートされている認証アプリケーションをスマートデバイスにインストールして、構成手順を実行します。
- 認証アプリケーションで QR コードをスキャンするか、手動でキーを入力します。



イメージをスキャンできない場合、認証アプリケーションで次のキーを入力します。

キー
*****  | 

- スマートデバイスの認証アプリケーションに表示されたワンタイムパスワードを入力してください。

6桁のワンタイムパスワード

このフィールドに値を指定してください。

キャンセル 構成

- 多要素認証を行うための、QRコードが表示されることを確認します。

2. MFAの設定手順

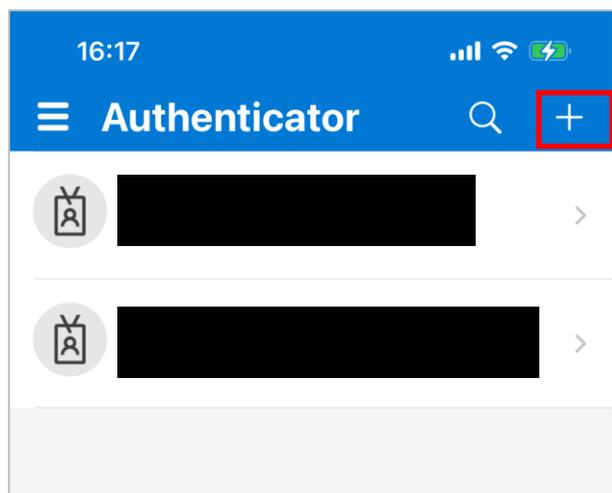
2-2. TOTP（Time-based One-Time Password）アプリケーションとの連携



TOTPアプリケーションから、先ほど表示されたQRコードのスクリーンを行います。

事前にiPhoneなどのモバイルデバイスに、TOTPアプリケーションをインストールしておきます。

- 本ドキュメントでは、Microsoft Authenticatorを用いて説明を行います。



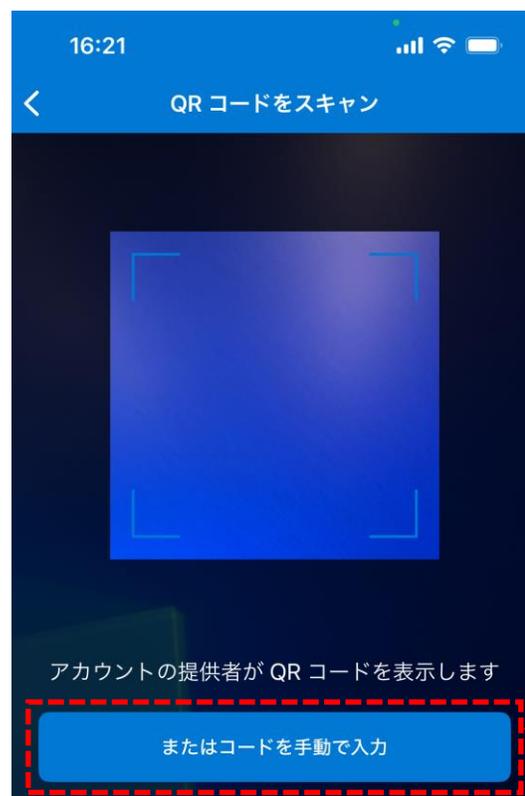
- Microsoft Authenticatorを起動し、右上の（+）をタップします。

2. MFAの設定手順

2-2. TOTP (Time-based One-Time Password) アプリケーションとの連携



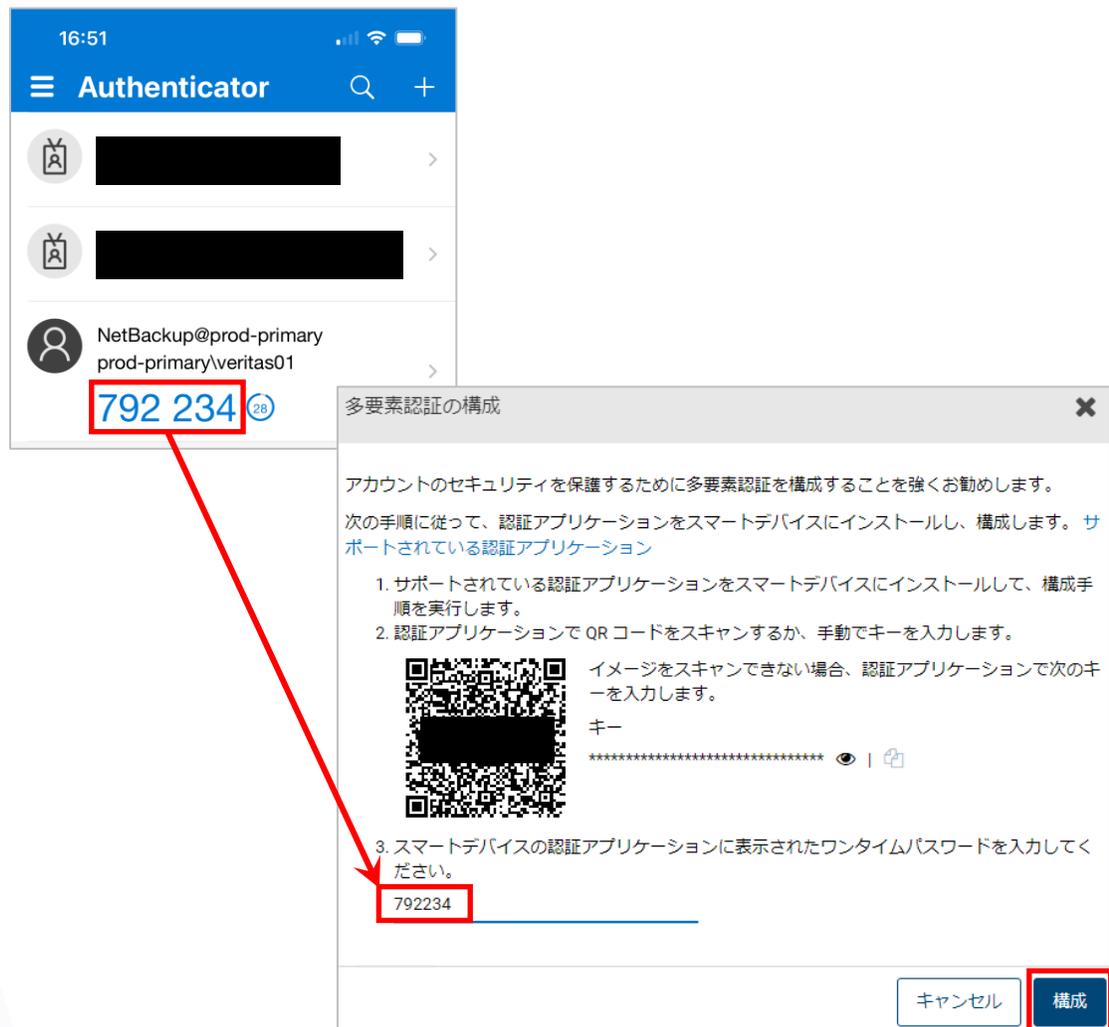
- [その他 (Google、Facebookなど)] をタップします。



- カメラが起動するので、プライマリサーバーに表示されているQRコードを読み取ります。
 - もし、カメラの起動が許可されていない場合、手動でコードを入力することも可能です。
 - 設定手順については、以下のTechnoteを参照してください。
 - [Setting up multi-factor authentication for NetBackup on user's authenticator application.](https://www.veritas.com/support/en_US/article.100060168)
 - https://www.veritas.com/support/en_US/article.100060168

2. MFAの設定手順

2-2. TOTP (Time-based One-Time Password) アプリケーションとの連携



- プライマリサーバー用のワンタイムパスワードが表示されることを確認します。

- 表示されているワンタイムパスワードを、[多要素認証の構成ウィンドウ]に入力します。
- [ワンタイムパスワード]入力後、[構成]をクリックします。

2. MFAの設定手順

2-2. TOTP（Time-based One-Time Password）アプリケーションとの連携



The screenshot displays the '多要素認証の構成' (MFA Configuration) page. At the top, a green banner contains a success message: '多要素認証が正常に構成されました。' (MFA has been configured normally). Below this, a white box contains the title '多要素認証の構成' and a paragraph explaining that MFA requires a password and a 6-digit one-time password. A '状態' (Status) section shows '構成済み' (Completed) with a green checkmark. A '無効化' (Deactivate) button is located at the bottom right of the white box.

- MFAが正常に構成されたことを確認します。

2. MFAの設定手順

2-2. TOTP（Time-based One-Time Password）アプリケーションとの連携

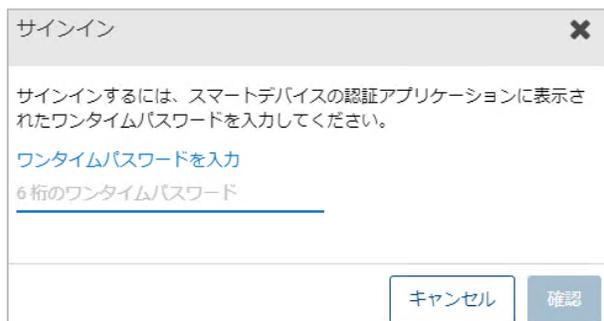
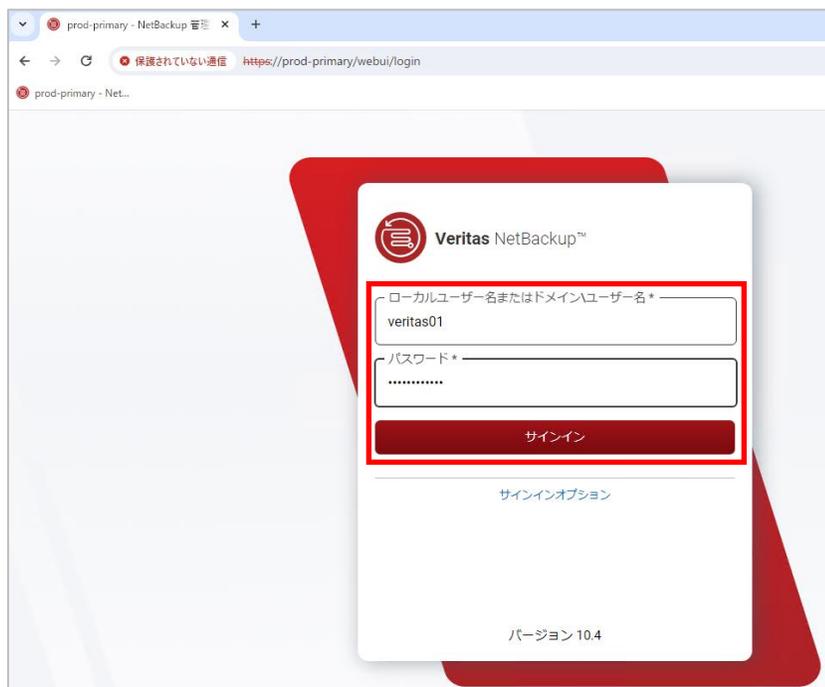


動作確認のため、NetBackup WebUIからサインアウトします。

- 画面右上の[プロフィール]をクリックします。
- メニューが表示されるので、[サインアウト]をクリックします。

2. MFAの設定手順

2-3. NetBackup WebUIを用いた動作確認

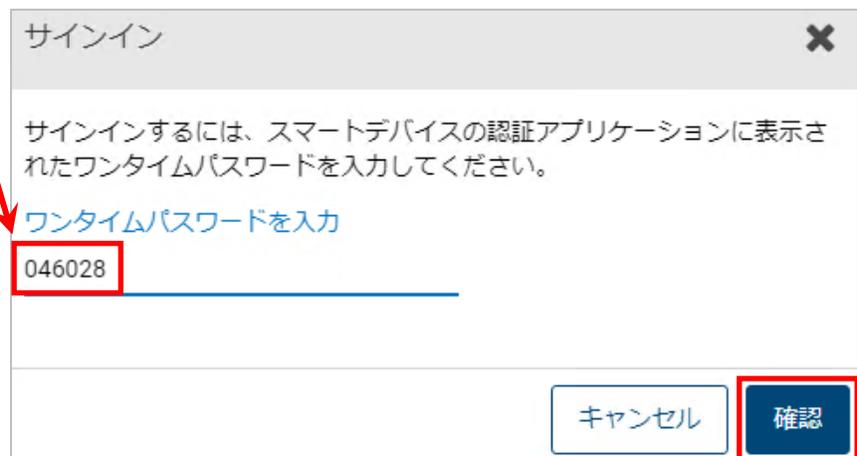
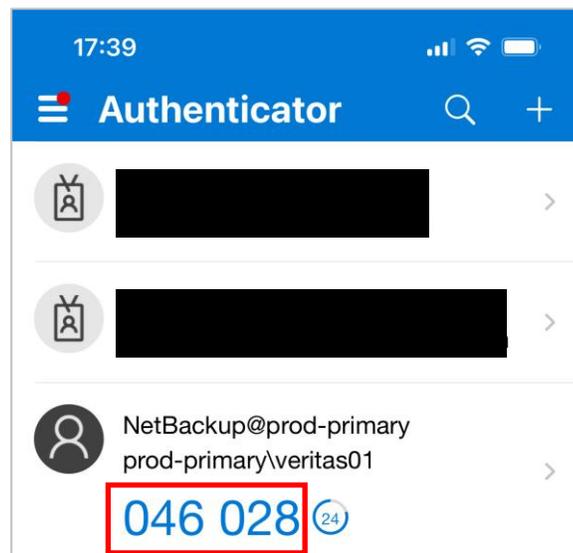


MFAが正常に機能するか、NetBackup WebUIを用いて確認を行います。

- プライマリサーバーのNetBackup WebUIにアクセスします。
- [ユーザー名]と[パスワード]を入力後、[サインイン]をクリックします。
 - 本ドキュメントでは、先ほどMFAの設定を行った、[veritas01]ユーザーでログインを行います。
- ワンタイムパスワードを入力を促すウィンドウが起動します。

2. MFAの設定手順

2-3. NetBackup WebUIを用いた動作確認

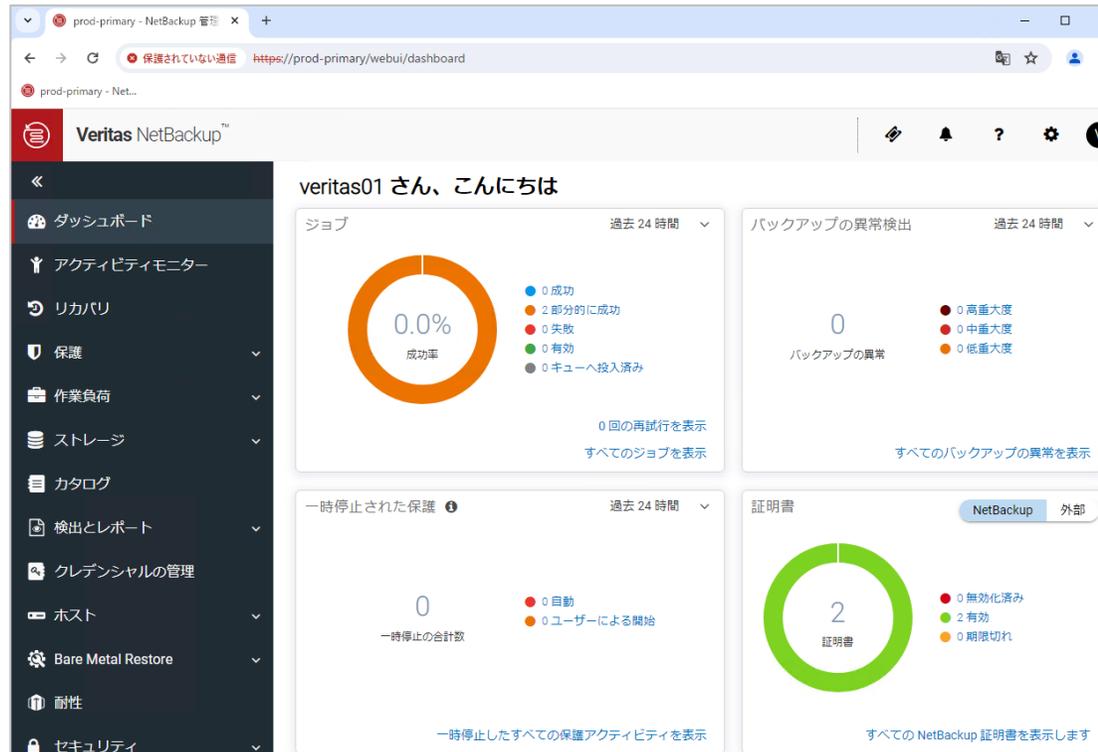


- Microsoft Authenticatorを起動し、プライマリサーバー用のワンタイムパスワードを確認します。

- 表示されているワンタイムパスワードを、[サインインウィンドウ]に入力します。
- ワンタイムパスワード入力後、[確認]をクリックします。

2. MFAの設定手順

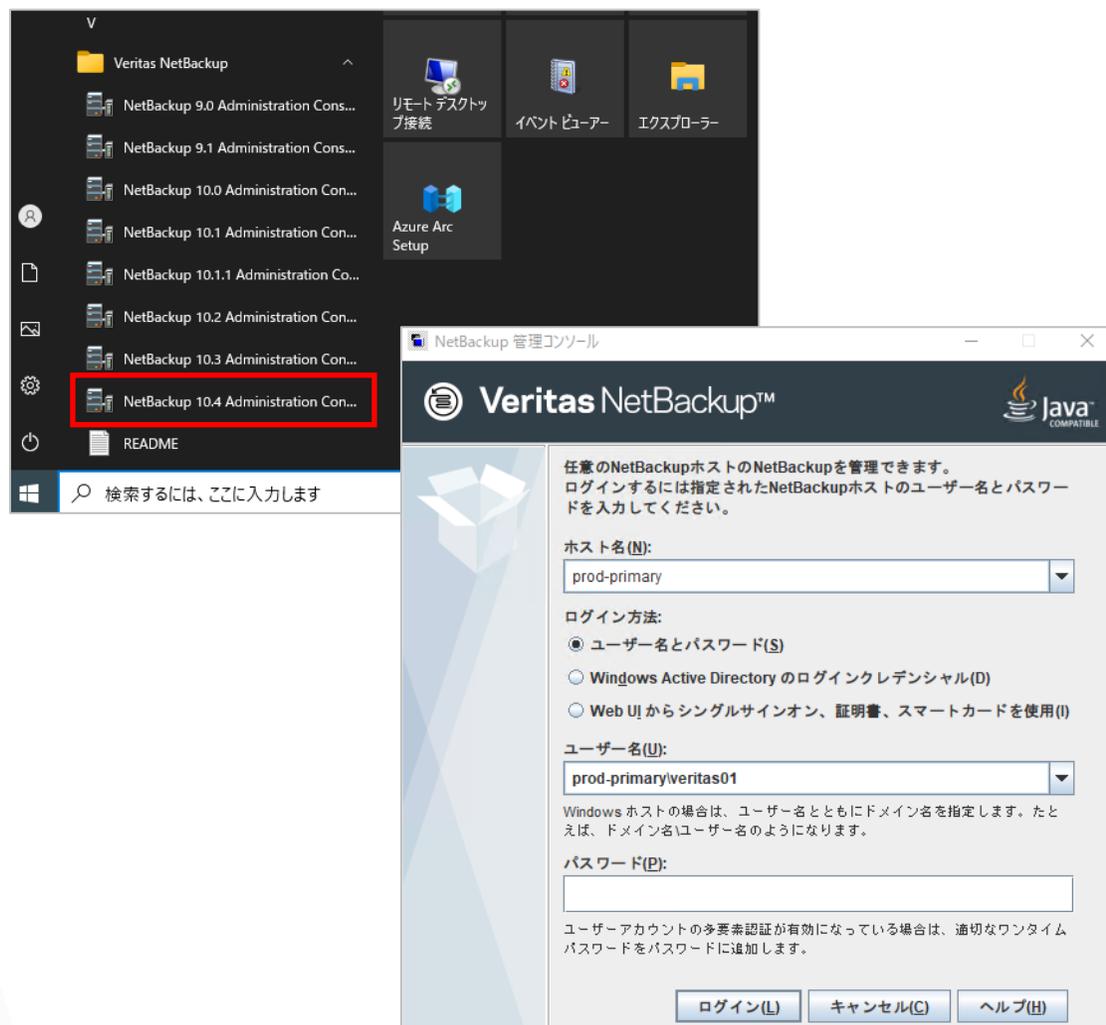
2-3. NetBackup WebUIを用いた動作確認



- NetBackup WebUIに正常にログイン出来ることを確認します。

2. MFAの設定手順

2-4. NetBackup Java管理コンソールを用いた動作確認



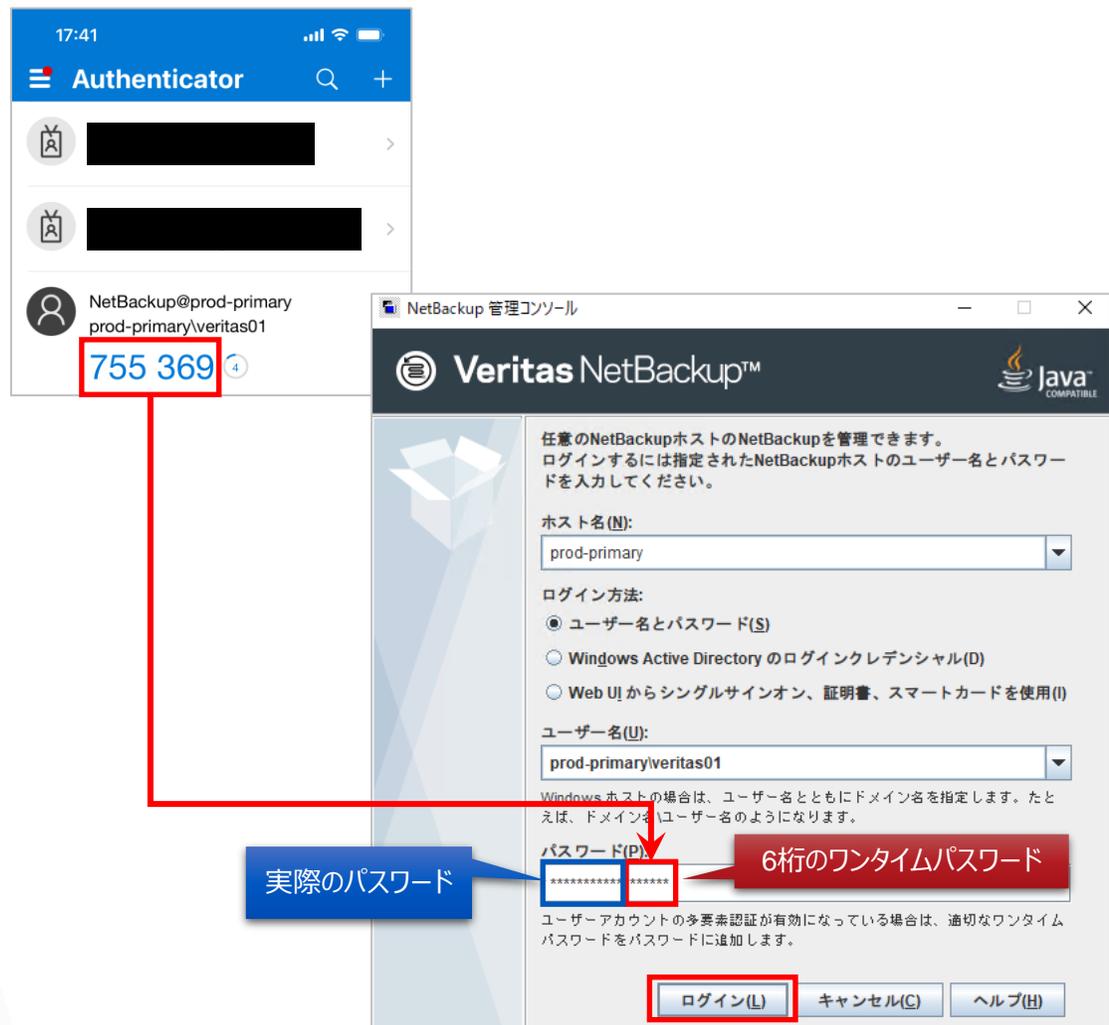
NetBackup Java管理コンソールにログインする際も、MFAが正常に機能するか確認を行います。

NetBackup Java管理コンソールの場合、新たなウィンドウが起動する仕組みではなく、パスワードを入力する際、実際のパスワードに続けて、6桁のワンタイムパスワードを入力する仕組みとなっています。

- Windowsのスタートメニューから、NetBackup Java管理コンソールを起動します。

2. MFAの設定手順

2-4. NetBackup Java管理コンソールを用いた動作確認

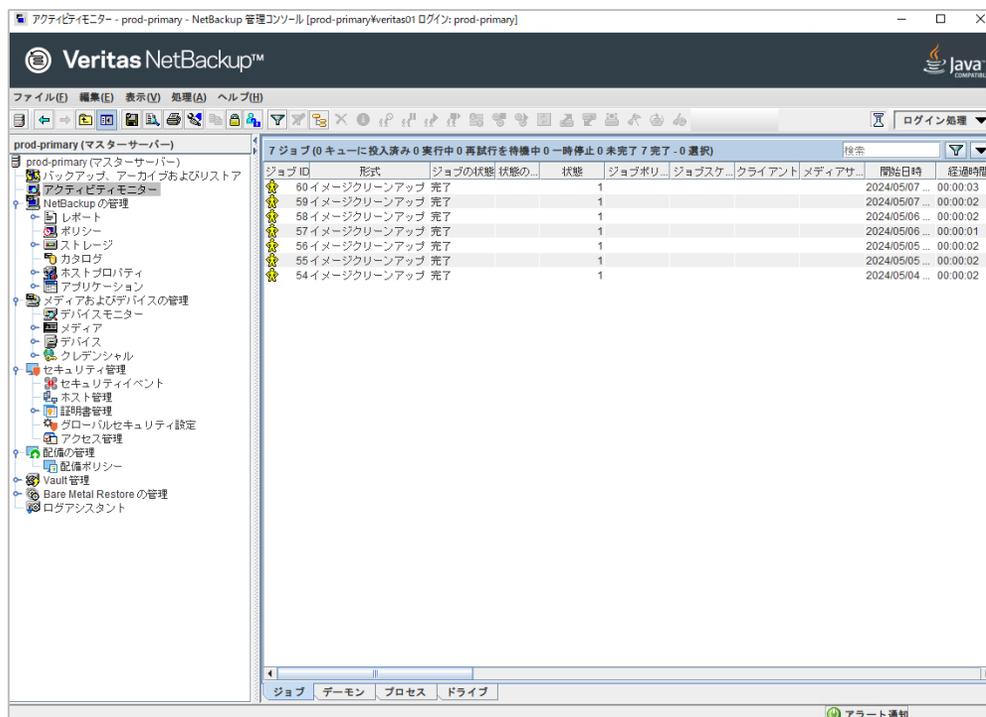
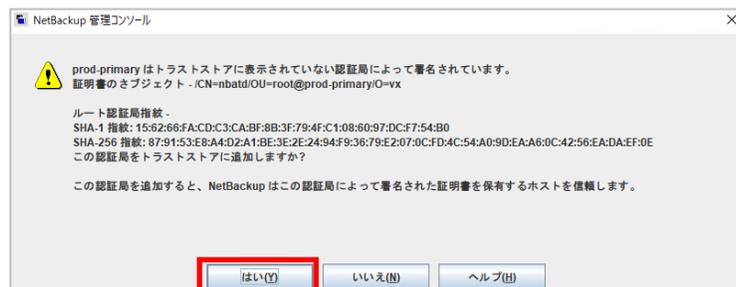


- Microsoft Authenticatorを起動し、プライマリサーバー用のワンタイムパスワードを確認します。

- パスワードを入力する際、[実際のパスワード]に続けて、[6桁のワンタイムパスワード]を入力します。
- パスワード入力後、[ログイン]をクリックします。

2. MFAの設定手順

2-4. NetBackup Java管理コンソールを用いた動作確認



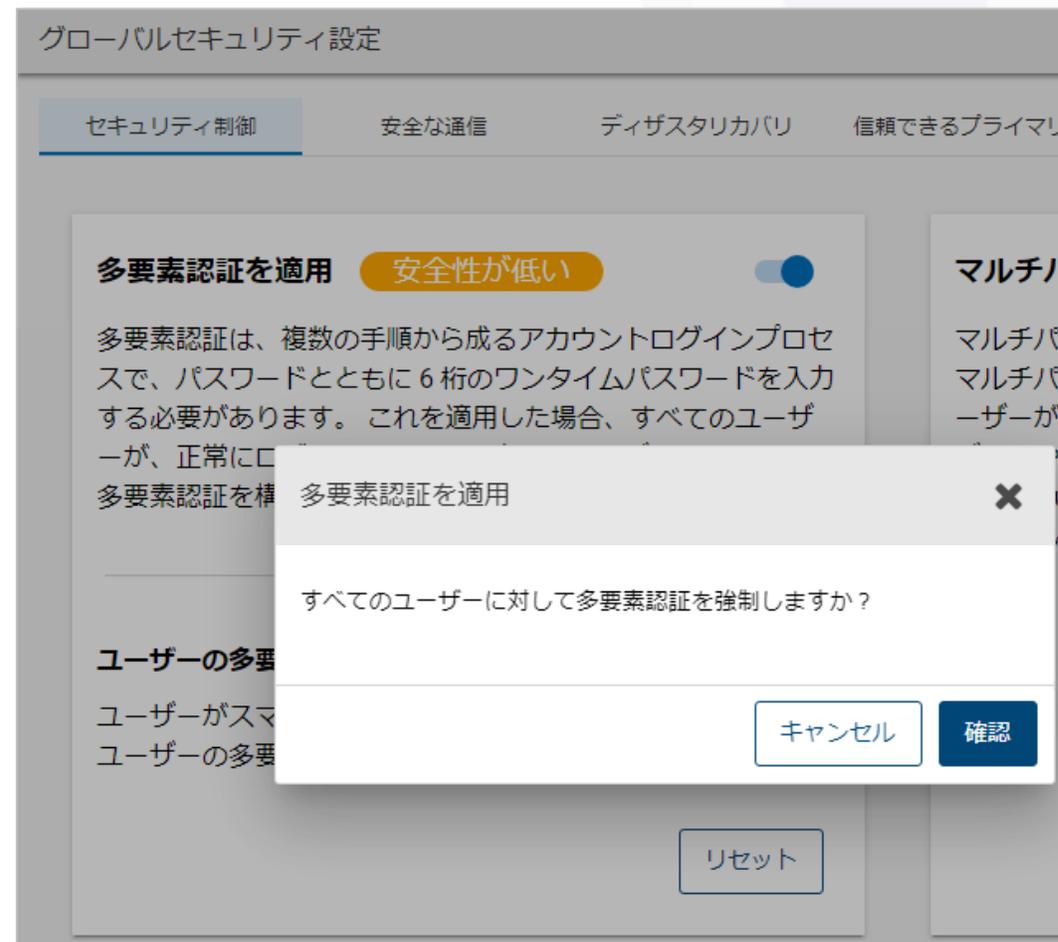
- **初回ログイン時のみ実施)**
- NetBackup Java管理コンソールによる初回ログイン時には証明書の確認を行うウィンドウが起動しますので、[はい]で先に進めてください。
- NetBackup Java管理コンソールに正常にログイン出来ることを確認します。

3. 全ユーザーに対するMFAの設定

3. 全ユーザーに対するMFAの設定

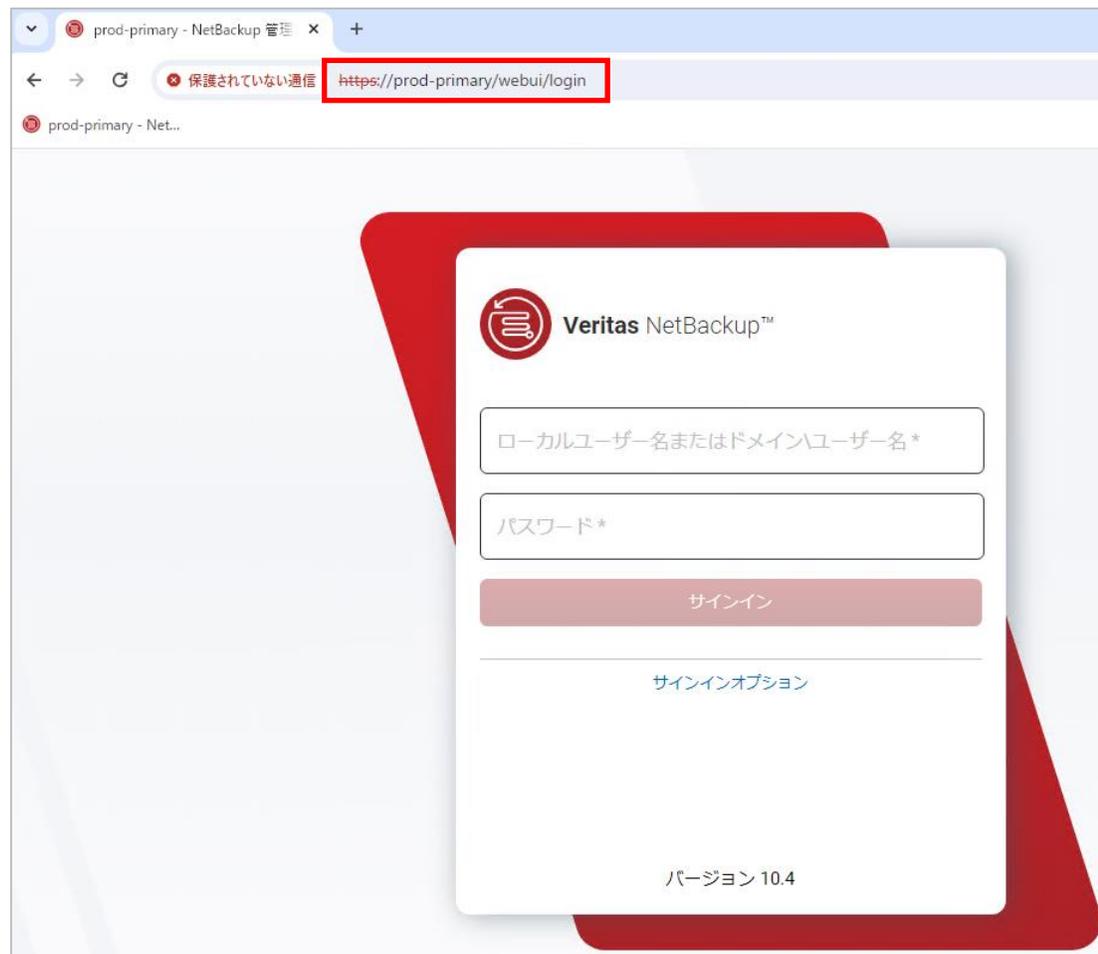
注意事項

- MFAを全ユーザーに強制した場合の注意事項
 - 全ユーザーにMFAを強制する設定も可能ですが、その際には管理者権限のユーザを複数人設定したうえで実施いただくことを推奨します。
 - 管理者権限ユーザーが1人の場合で、MFAを構成した後、スマートフォンの紛失やスマホアプリからアカウント情報を削除してしまうと、NetBackupに管理者権限でログインできるユーザーがいなくなります。
 - 管理者権限ユーザーが複数人いる場合、正常にログインできる管理者ユーザーが問題となった管理者ユーザーのMFA構成をリセットすることが可能です。



3. 全ユーザーに対するMFAの設定

3-1. MFAを設定していないユーザーによるNetBackup WebUIログイン時の動作確認



項番2ではログインユーザーに対するMFAの設定となっていました
が、本項番では全ユーザーに対してMFAを強制化する設定
を行います。

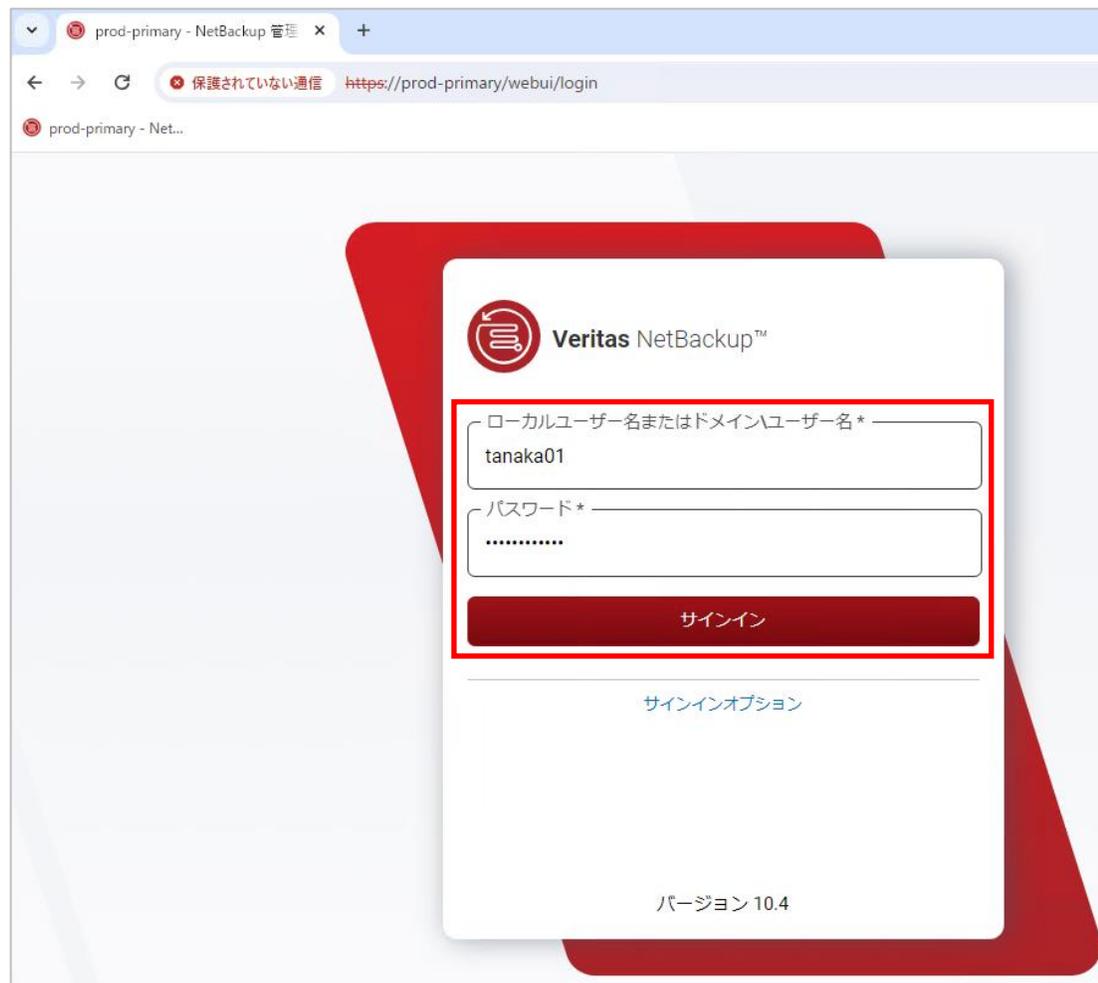
まず、MFAを設定していないユーザーである[tanaka01]にて、
NetBackup WebUIにログインした際の動作を確認します。

- ブラウザを起動し、プライマリサーバーのNetBackup WebUI
にアクセスします。
 - 本ドキュメントの場合ですと、以下となります。
<https://prod-primary/webui/login>
 - [prod-primary]がプライマリサーバー名となり、NetBackupイン
ストール時に指定したサーバー名を入力してください。

備考)
プライバシーエラーが発生した場合はP.15の手順を実施ください。

3. 全ユーザーに対するMFAの設定

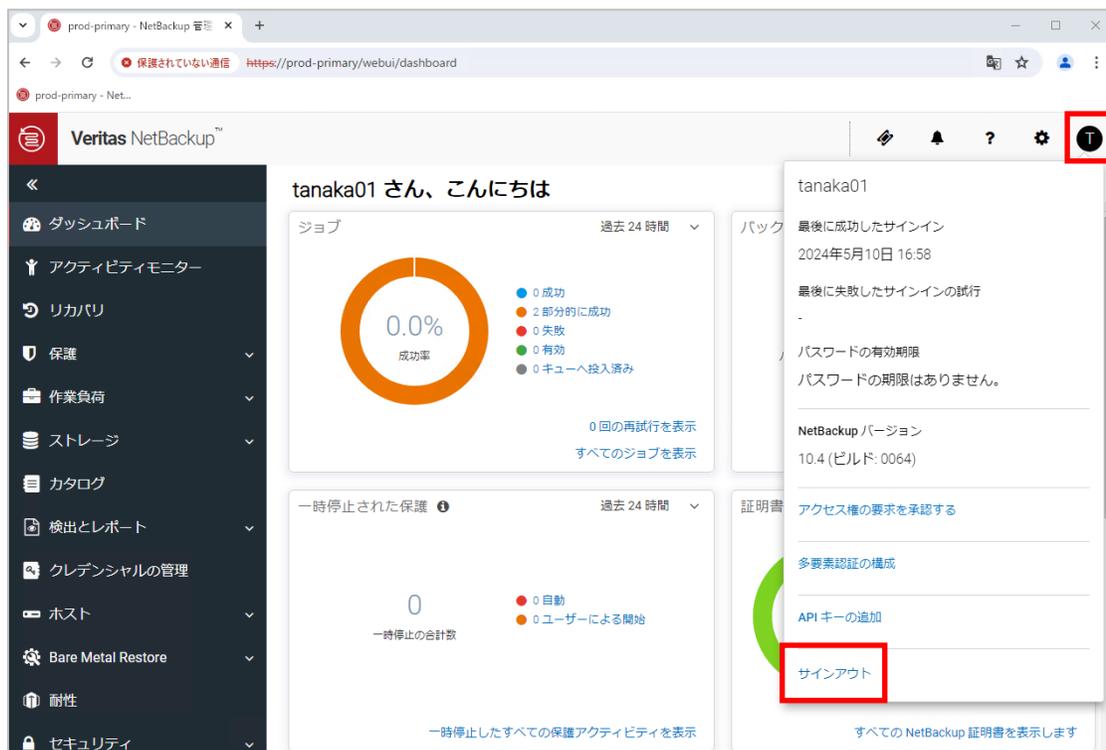
3-1. MFAを設定していないユーザーによるNetBackup WebUIログイン時の動作確認



- NetBackup WebUIのログイン画面が表示されるので、[ユーザー名]と[パスワード]を入力します。
 - 今回ログインするユーザーは事前にRBACで権限を付与しています。
 - また、今回ログインするユーザーはMFAを設定していないユーザーを指定してください。
 - 本ドキュメントでは、[tanaka01]ユーザーでログインを行います。
- [サインイン]をクリックして、NetBackup WebUIにログインします。

3. 全ユーザーに対するMFAの設定

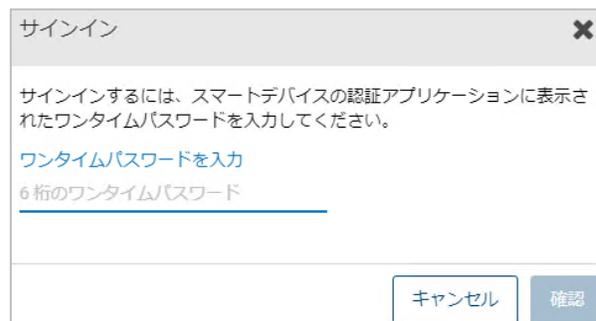
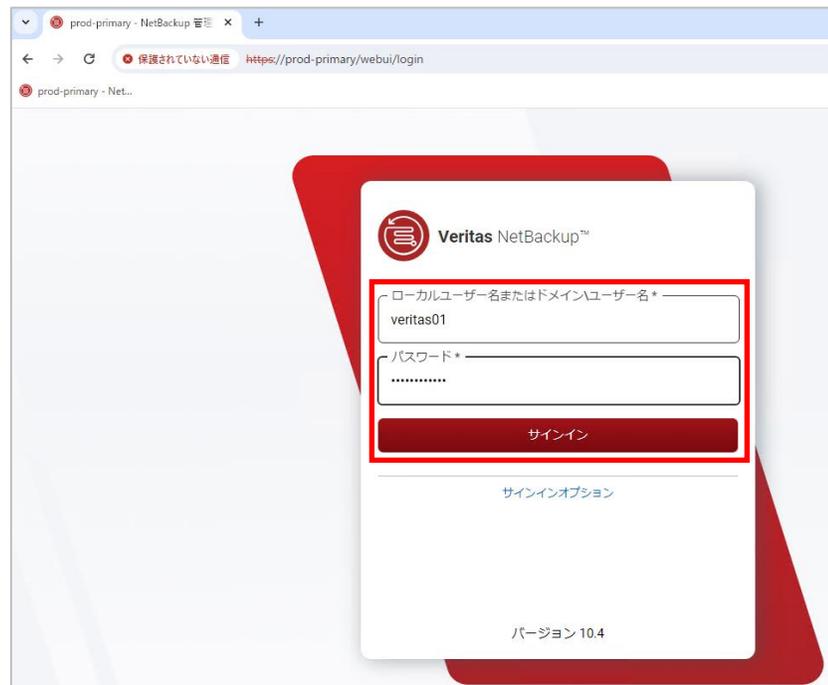
3-1. MFAを設定していないユーザーによるNetBackup WebUIログイン時の動作確認



- MFAの設定を実施していないので、ワンタイムパスワードを尋ねられることなく、ダッシュボードが表示されることを確認します。
- 確認後、画面右上の[プロフィール]をクリックします。
- メニューが表示されるので、[サインアウト]をクリックします。

3. 全ユーザーに対するMFAの設定

3-2. 全ユーザーに対するMFAの設定

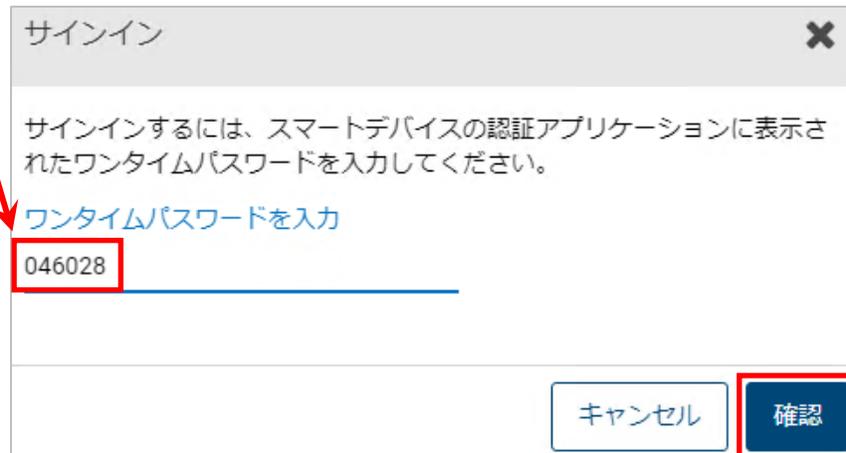
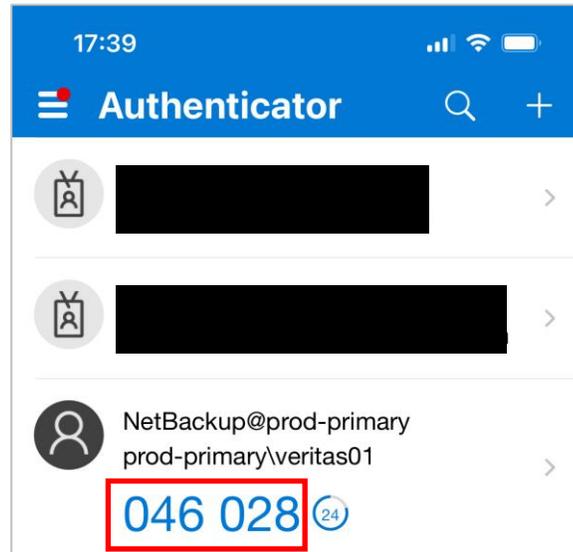


続いて、全ユーザーに対するMFAの設定を行います。

- プライマリサーバーのNetBackup WebUIにアクセスします。
- [ユーザー名]と[パスワード]を入力後、[サインイン]をクリックします。
 - NetBackupの管理者権限を持ったユーザーを指定してください。
 - 本ドキュメントでは、先ほどMFAの設定を行った、[veritas01]ユーザーでログインを行います。
- ワンタイムパスワードを入力を促すウィンドウが起動します。

3. 全ユーザーに対するMFAの設定

3-2. 全ユーザーに対するMFAの設定

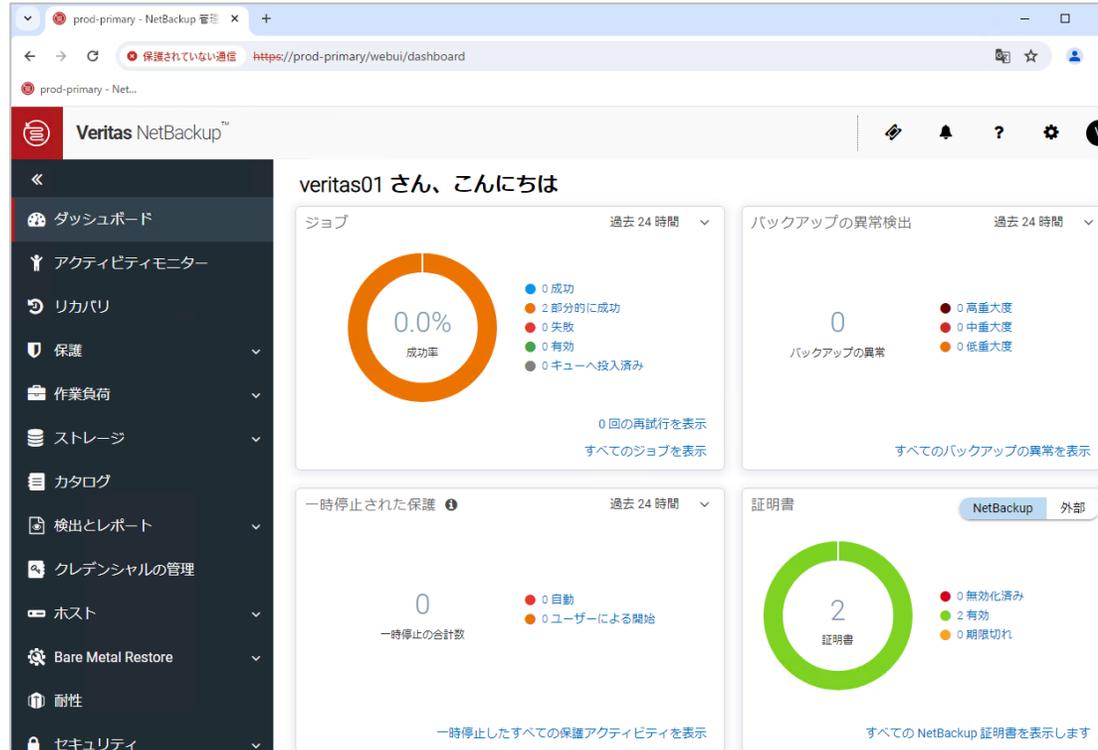


- Microsoft Authenticatorを起動し、プライマリサーバー用のワンタイムパスワードを確認します。

- 表示されているワンタイムパスワードを、[サインインウィンドウ]に入力します。
- ワンタイムパスワード入力後、[確認]をクリックします。

3. 全ユーザーに対するMFAの設定

3-2. 全ユーザーに対するMFAの設定



- NetBackup WebUIに正常にログイン出来ることを確認します。

3. 全ユーザーに対するMFAの設定

3-2. 全ユーザーに対するMFAの設定



- 画面右上の[歯車アイコン]をクリックします。
- メニューが表示されるので、[グローバルセキュリティ]をクリックします。



- グローバルセキュリティ設定のセキュリティ制御タブの項目である[多要素認証を適用します]のスイッチアイコンをクリックします。

3. 全ユーザーに対するMFAの設定

3-2. 全ユーザーに対するMFAの設定

多要素認証を適用します

すべてのユーザーを対象に多要素認証を適用しますか?

キャンセル 確認

- [多要素認証を適用します]ウィンドウがウィンドウが表示されるので、[確認]をクリックします。

重要な操作のための再認証

セキュリティを高めるため、スマートデバイスの認証アプリケーションに表示されるワンタイムパスワードを入力して再認証してください。

ワンタイムパスワードを入力
259068

キャンセル 確認

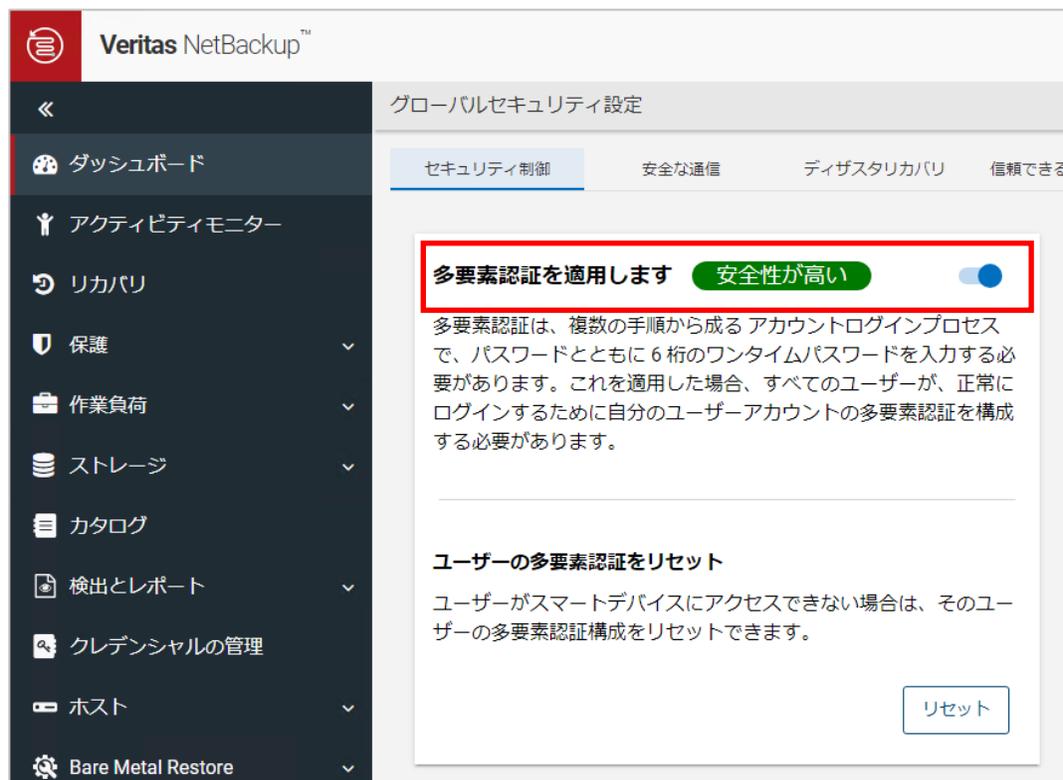
- もし、[重要な操作のための再認証]ウィンドウが起動した場合、Microsoft Authenticatorを起動して、[ワンタイムパスワード]を入力してください。
- 入力後、[確認]をクリックします。

3. 全ユーザーに対するMFAの設定

3-2. 全ユーザーに対するMFAの設定

✔ 多要素認証の適用が正常に有効化されました。

- [多要素認証の適用が正常に有効化されました]と表示されることを確認します。



- [多要素認証を適用します]にて、[安全性が高い]になっていること、スイッチアイコンが有効状態（青色）になっていることを確認します。

3. 全ユーザーに対するMFAの設定

3-3. 動作確認

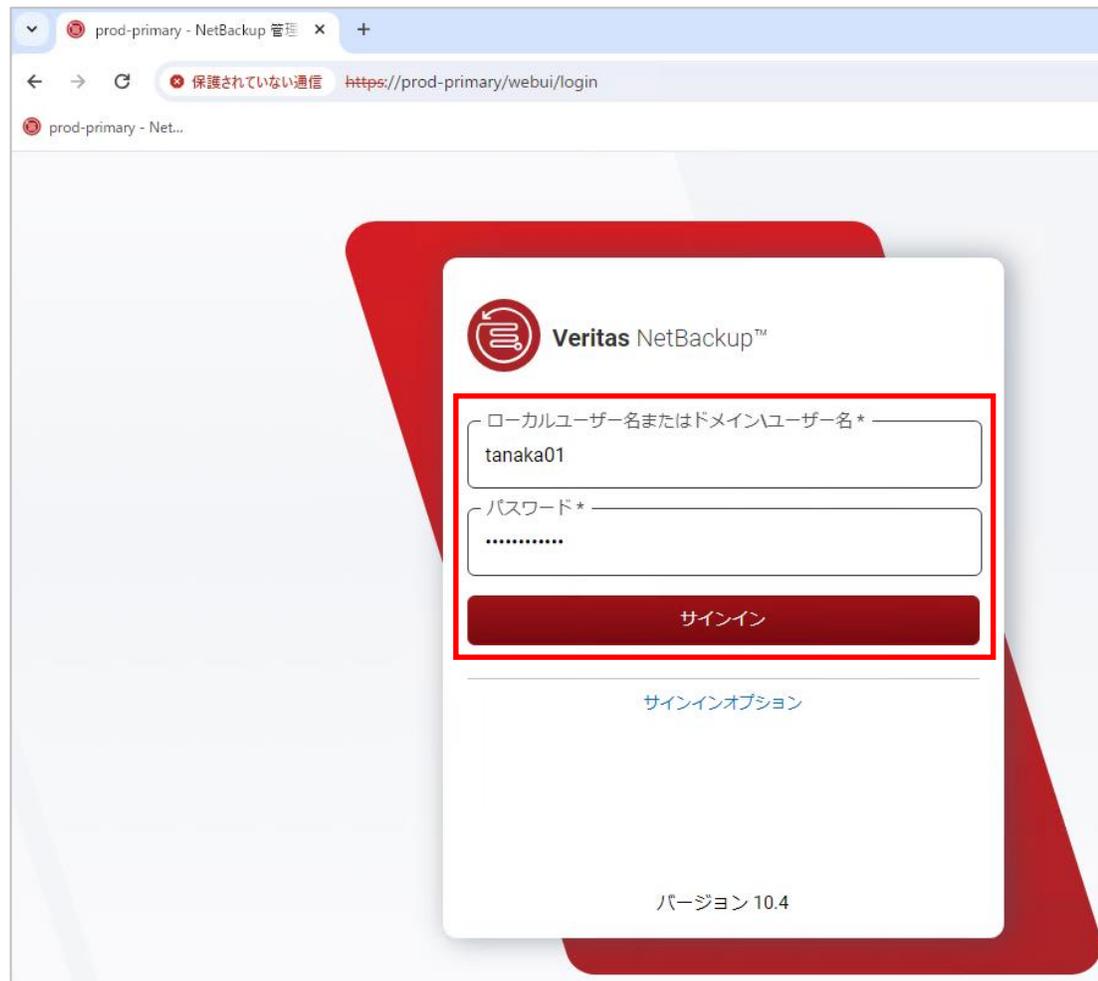


MFAを構成していない[tanaka01]ユーザーで改めてログインして、どのような変化があるかを確認します。

- 画面右上の[プロフィール]をクリックします。
- メニューが表示されるので、[サインアウト]をクリックします。

3. 全ユーザーに対するMFAの設定

3-3. 動作確認



- プライマリサーバーのNetBackup WebUIにアクセスします。
- [ユーザー名]と[パスワード]を入力後、[サインイン]をクリックします。
 - 本ドキュメントでは、[tanaka01]ユーザーでログインを行います。

3. 全ユーザーに対するMFAの設定

3-3. 動作確認

多要素認証の構成

アカウントのセキュリティを保護するには、多要素認証を構成する必要があります。3分以内に構成プロセスを完了してください。

次の手順に従って、認証アプリケーションをスマートデバイスにインストールし、構成します。 [サポートされている認証アプリケーション](#)

- サポートされている認証アプリケーションをスマートデバイスにインストールして、構成手順を実行します。
- 認証アプリケーションでQRコードをスキャンするか、手動でキーを入力します。



イメージをスキャンできない場合、認証アプリケーションで次のキーを入力します。

キー
***** | 

- スマートデバイスの認証アプリケーションに表示されたワンタイムパスワードを入力してください。

6桁のワンタイムパスワード

- 項番3-1では[ユーザー名]と[パスワード]を入力した直後に、NetBackup WebUIにログイン出来ていましたが、今回は[多要素認証の構成]ウィンドウが表示されることを確認します。
- **このウィンドウが表示されていれば、全ユーザーの多要素認証の構成が正常に設定出来ていることとなります。**
- **この後、このユーザーでログインする場合は、項番2-2の手順に従い、MFAの設定を改めて実施してください。**

VERITAS™

ありがとうございました！

Copyright © 2024 Veritas Technologies, LLC. All rights reserved.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.