



2023年10月3日

データ保護に必要なNextcloudの セキュリティ機能解説



partner
network



自己紹介

□大島 皐 (Satsuki Oshima)

□株式会社スタイルズ

- ▶ NextcloudやRancherなどの
商用オープンソースプロダクトの導入サポートチーム



ドイツ Nextcloud GmbH
Premium Partner

<https://nextcloud.com/partners/>

本日の内容

□対象

- ▶ Nextcloudに興味がある方
- ▶ Nextcloudを利用している方

□ゴール

- ▶ Nextcloudのセキュリティ機能を知る

本日の内容

□ Nextcloudとは

□ Nextcloudのセキュリティ機能

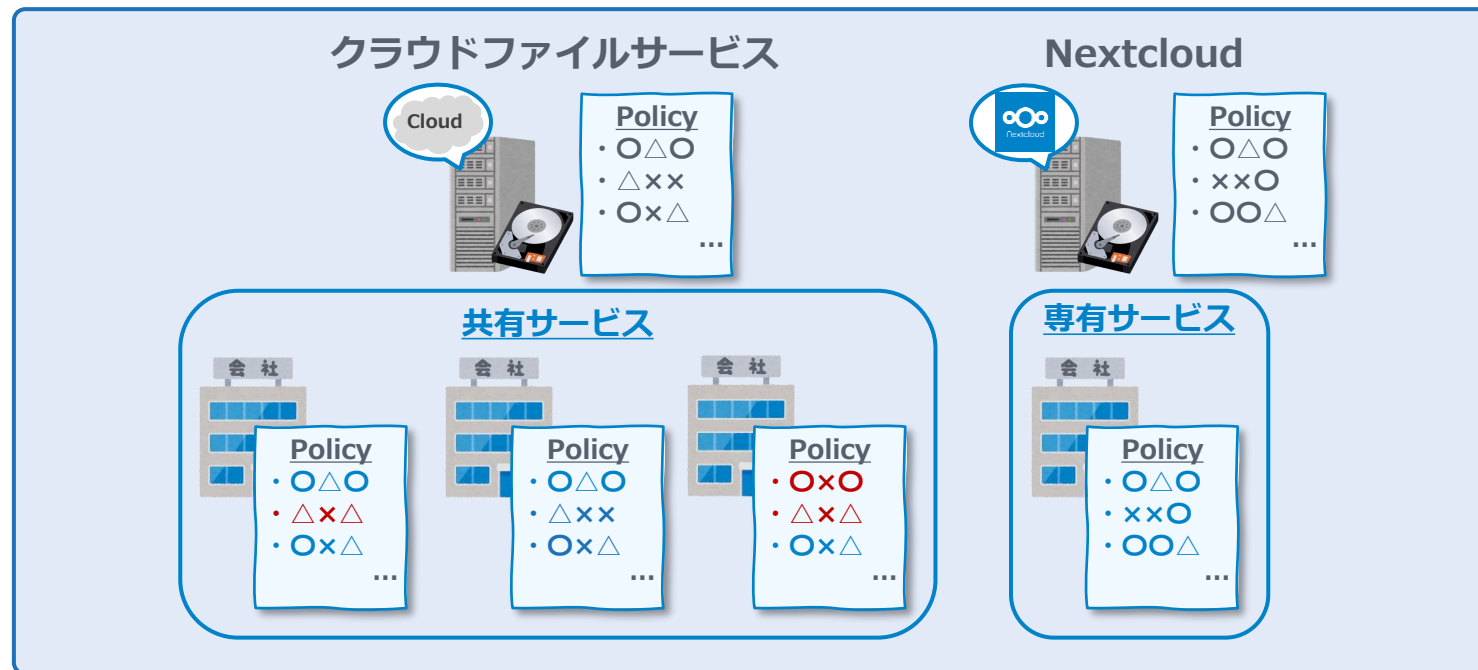
- ▶ 認証
- ▶ 保護
- ▶ 運用

Nextcloudとは

- Nextcloudはオープンソースで提供される、企業や大学向けのオンラインストレージ製品です
- 他のオンラインストレージと比較して、次のような特徴があります
 - ▶ オンプレミスでも利用できる
 - ▶ 既存のファイルサービスとの高い融和性
 - ▶ 多彩なファイル共有機能

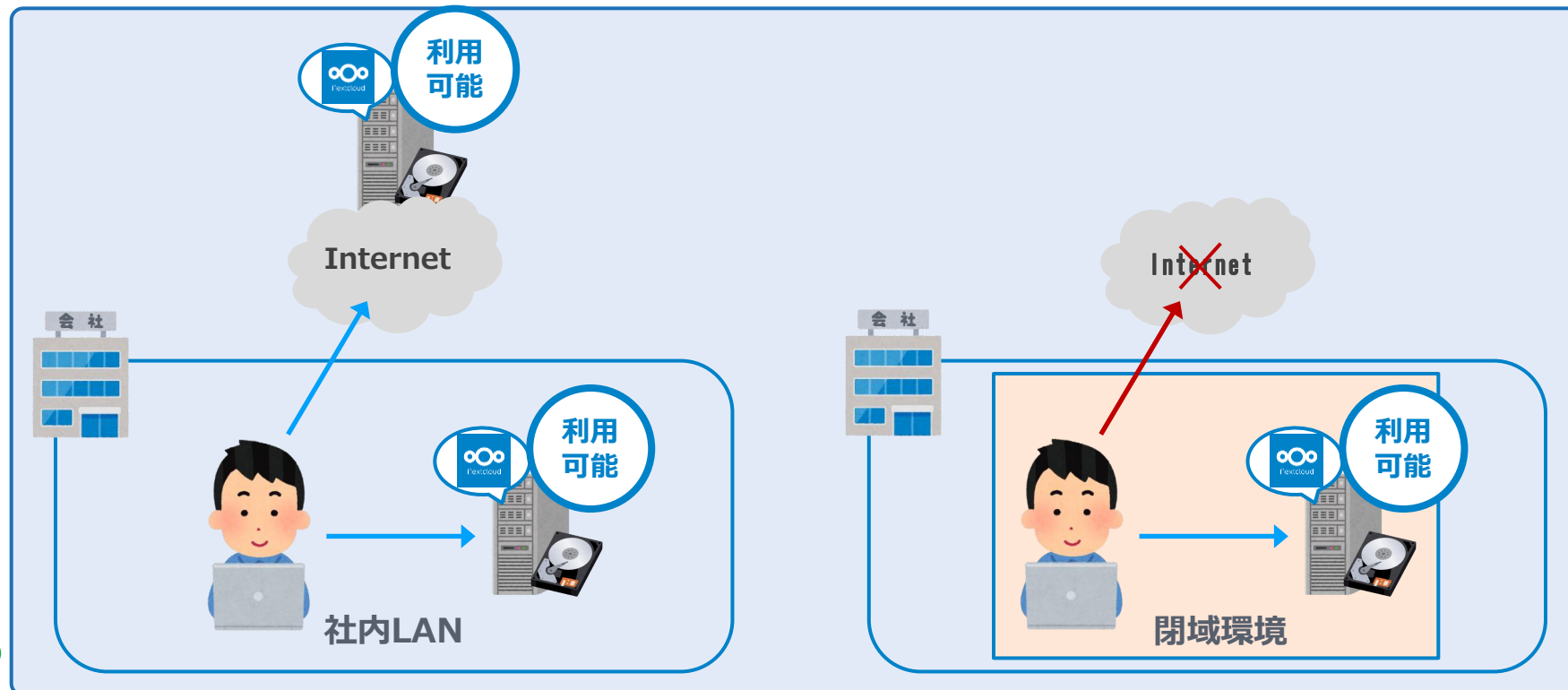
オンプレミスでも利用できる

- Nextcloudは、サーバーにインストールして使用するソフトウェア製品です
- 自社の管理するサーバーにNextcloudを導入することにより、自社専用のオンラインストレージとして利用できます
- 他社と一切を共有しませんので、セキュリティや設定、保存されるデータなどを含めて**全て自社で管理**ができます



オンプレミスでも利用できる

- Nextcloudは、クラウドサービスではありません
- 例えば、セキュリティの確保やアクセス回線などの環境を理由に、LAN内に導入することができます
- また、インターネットと接続されていない、機密性の高い環境にも導入できます



Nextcloudのセキュリティ機能

□認証

- ▶ Nextcloudの認証の種類
- ▶ パスワードポリシー
- ▶ 二要素認証

□保護

- ▶ 保管データの暗号化
- ▶ ブルートフォース保護
- ▶ アンチウィルス
- ▶ CSRF Token

□運用

- ▶ 監査ログ
- ▶ グループフォルダ

Nextcloudで利用できる認証方式

認証方式	概要
ID/PW認証 (通常ログイン)	Nextcloudの通常のログイン方法
統合認証 (シングルサインオン)	外部認証プロバイダなどを利用したログイン方法 例: ▪ LDAP/AD認証 ▪ SAML認証
二要素認証	複数の認証方式を組み合わせたログイン方法 例: ▪ TOTP ▪ U2F ▪ WebAuthn

ID/PW認証(パスワードポリシー)

□ Nextcloudのローカルユーザーに対してパスワードポリシーを設定できます。

□ 設定できる項目

- パスワードの最小の長さ
- 一定数世代前のパスワードを再利用禁止
- パスワードの有効期間
- ユーザーアカウントがブロックされるまでのログイン試行回数
- 一般的なパスワードの禁止 (例 : 「password123」)
- 大文字と小文字を必ず含む
- 数字を必ず含む
- 記号を必ず含む
- haveibeenpwned.comの侵害されたパスワードと比較してパスワードをチェックする

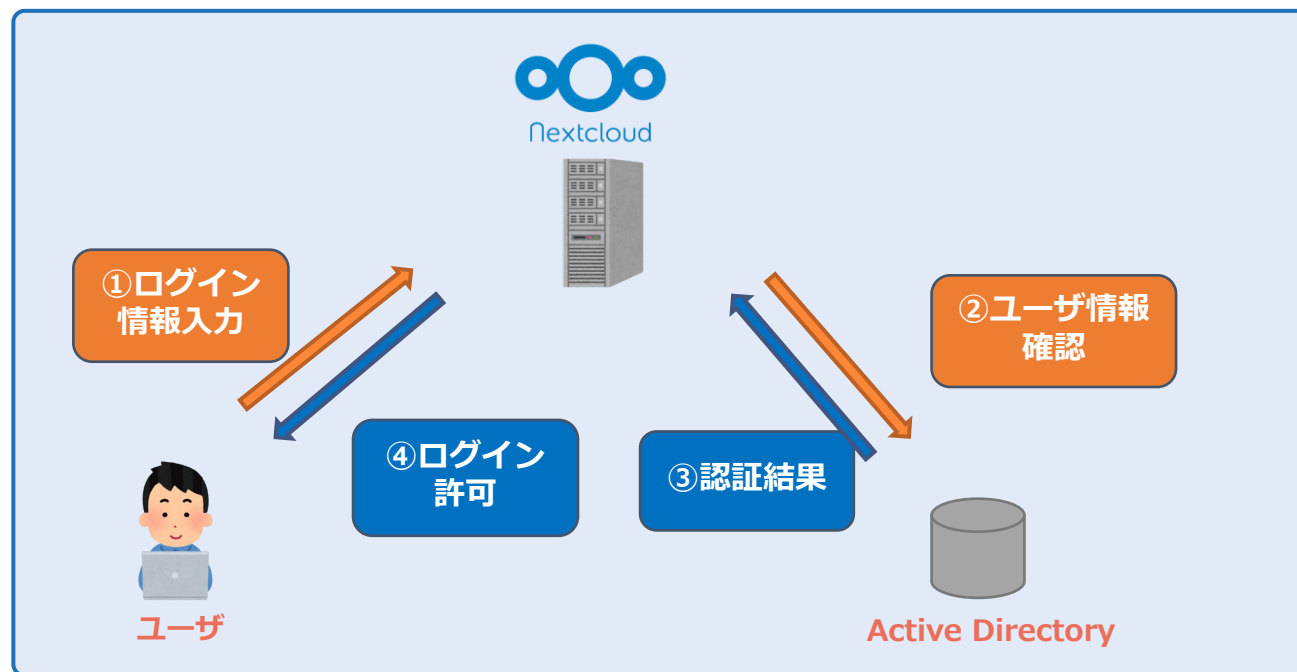
統合認証

□ LDAP/AD認証

ユーザがNextcloudにログインする際、LDAP/ADサーバへ連携して認証する仕組みです

□ 統合認証のメリット

既存の認証基盤を再利用することで、ユーザが複数のシステムで異なるID/PWを持つ必要がなくなり、管理の手間やセキュリティリスクを減らすことができます



二要素認証

- Nextcloudでは以下の二要素認証が利用できます
 - TOTP (Time-based One-Time Password)
 - Google Authenticator、Microsoft Authenticator等を利用
 - U2F (Universal 2nd Factor)
 - USB dongles等の物理デバイスを利用
 - WebAuthn
 - FIDO2デバイス(顔認証、指紋認証)を利用

ワンタイムパスワード

□ Google Authenticatorを利用する例

1. ユーザが、個人設定画面のQRコードをGoogle Authenticatorアプリでスキャンし、アカウントをアプリに登録
2. 次回からのログイン時、まずID/PWを入力
3. Nextcloudがワンタイムパスワードの入力をユーザに要求
4. ユーザはアプリで表示されるワンタイムパスワードを入力
5. 正しいパスワードが入力されれば、ユーザは認証されてログイン

ワンタイムパスワード

二要素認証 i

アカウントのセキュリティを強化するには、パスワード以外に2番目の要素を使用してください。
サードパーティのアプリケーションを使用してNextcloudに接続する場合は、二要素認証を有効にする前に必ずそれぞれのアプリパスワードを作成して設定してください。

TOTP (Authenticator app)

☐ TOTP有効化

新しいTOTP秘密鍵は次のとおりです： XXXXXXXXXX

クイックセットアップでは、このQRコードをTOTPアプリでスキャンしてください：



スキャン

アプリを設定したら、以下のテストコード

認証コード

検証

ワンタイムパスワード
を入力して検証

とを確認します。

ワンタイムパスワード

1つ目の認証 (ID/PW)



Nextcloud ログイン

アカウント名またはメールアドレス

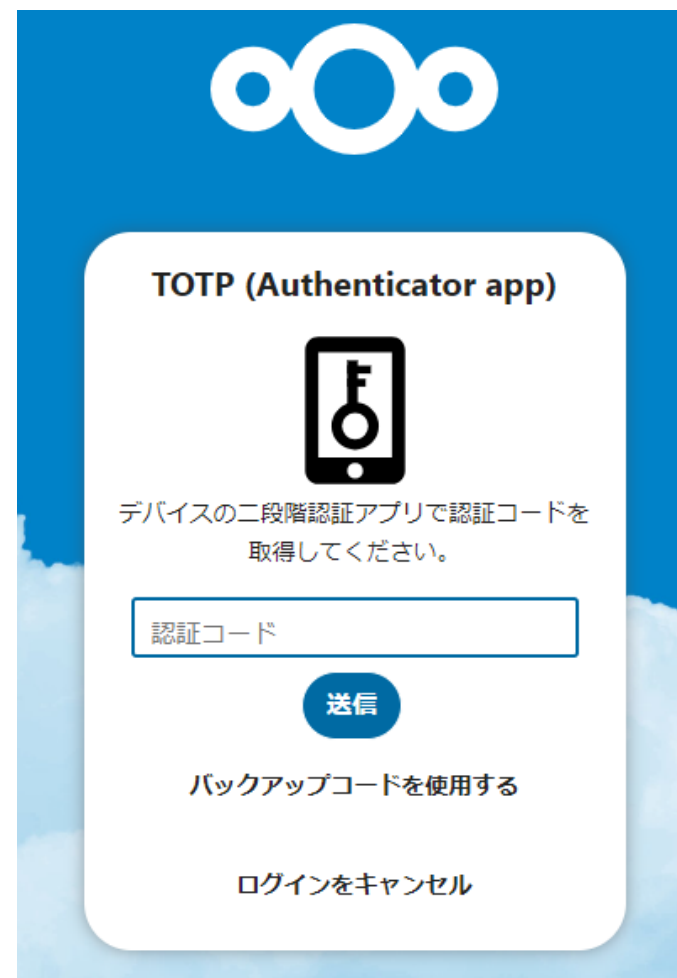
パスワード

→ ログイン

パスワードをお忘れですか?

デバイスを使ってログインする

2つ目の認証 (ワンタイムパスワード)



TOTP (Authenticator app)



デバイスの二段階認証アプリで認証コードを取得してください。

送信

バックアップコードを使用する

ログインをキャンセル

Nextcloudのセキュリティ機能

□認証

- ▶ Nextcloudの認証の種類
- ▶ パスワードポリシー
- ▶ 二要素認証

□保護

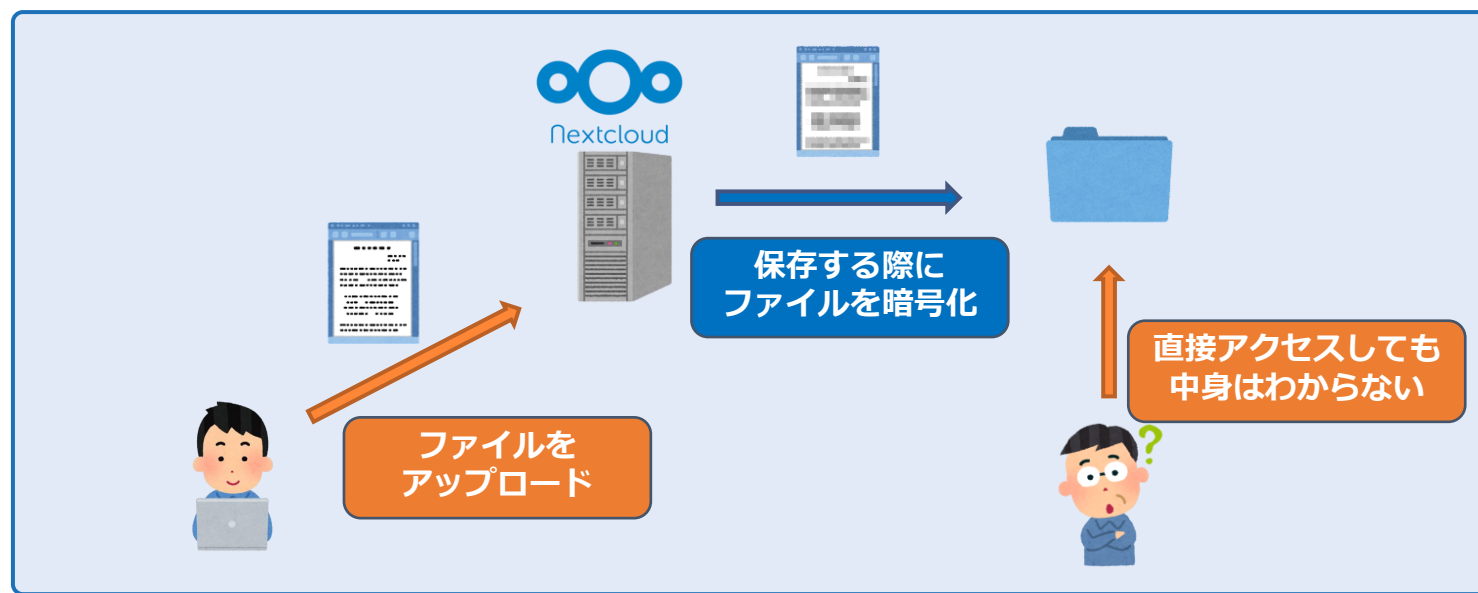
- ▶ サーバーサイド暗号化
- ▶ ブルートフォース保護
- ▶ アンチウィルス
- ▶ CSRFトークン

□運用

- ▶ 監査ログ
- ▶ グループフォルダ

サーバーサイド暗号化

- Nextcloudにアップロードされたファイルがストレージに保存される際に暗号化されます
- ストレージに直接アクセスされても、ファイルの中身を把握することはできなくなります
- サーバーサイド暗号化機能は、AmazonS3やFTPサーバー等の外部ストレージを利用する際に特に有効です



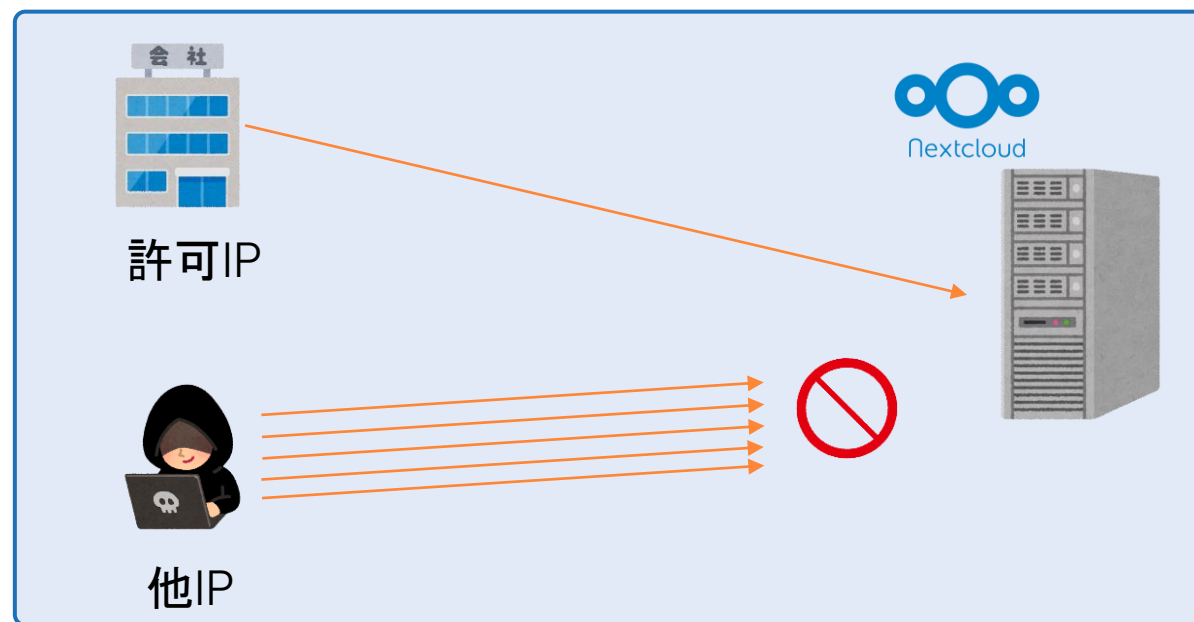
サーバーサイド暗号化

- Nextcloudに連携したファイルサーバーを直接操作したい、というケースもあります
- その場合は、暗号化を有効にしてしまうと、ファイルサーバーのファイルが暗号化されてしまい操作が難しくなるため、暗号化を無効にする必要があります



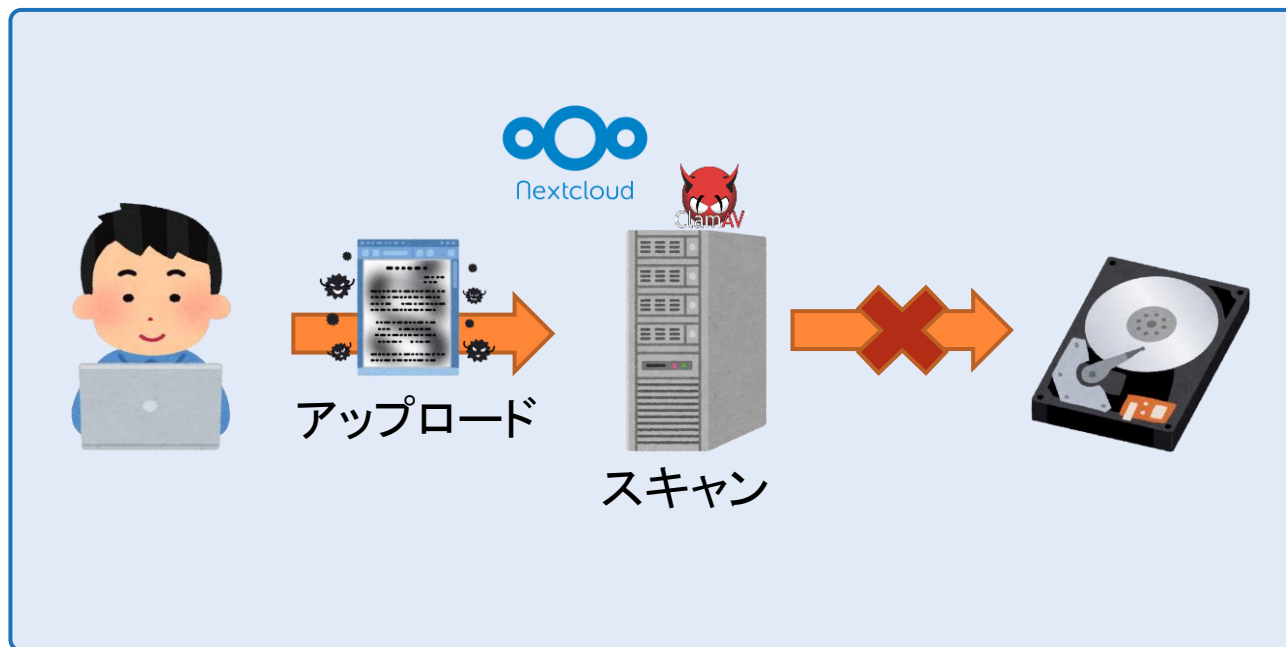
ブルートフォース保護

- ブルートフォース攻撃は、ユーザー名とパスワードの組み合わせを繰り返し試行することによって、アカウントに不正アクセスを試みる攻撃手法です
- ログインに複数回失敗した場合、ログインを試行してきたIPに対してアクセスを一時的に制限することができます
- ホワイトリストでIPアドレスを指定すると、指定したIPアドレスでログインに複数回失敗してもアクセスが制限されることはありません



ウイルススキャン

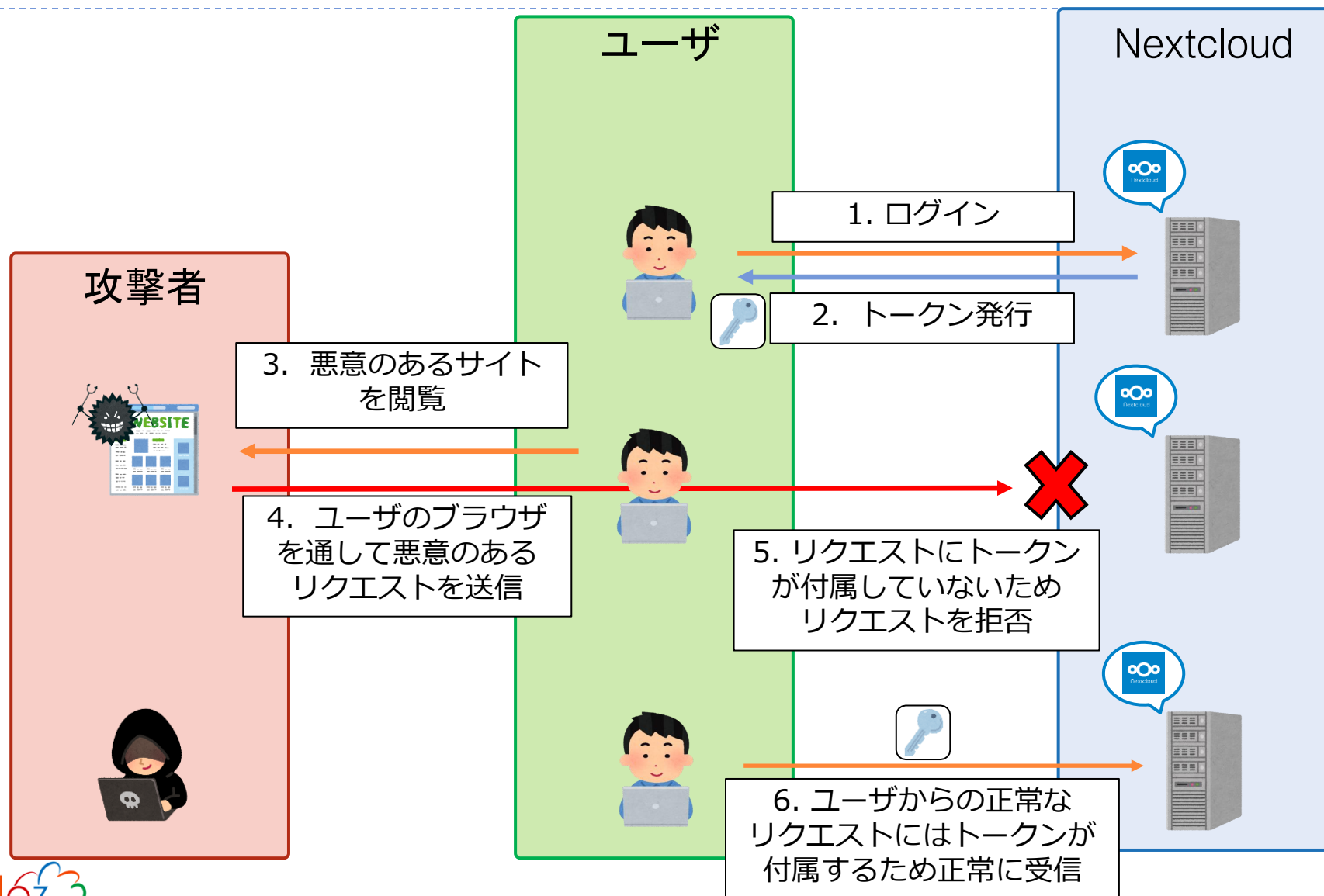
- Nextcloudにアップロードされたファイルを、ウイルス対策ソフトを利用しNextcloudのストレージに保存される前にウイルス検査します
- ファイルがウイルスと判定された場合ファイルは削除され、通知がユーザに送信されます



CSRFトークン

- ❑ Cross-Site Request Forgery(CSRF)は、ユーザがログインした状態のWebサイトに対して、ユーザ意図しないリクエストを送信させる攻撃です
- ❑ Nextcloudでは攻撃を防ぐためにCSRFトークンを使用しています
ユーザからの各リクエストに一意的トークンを含めることで、そのリクエストが本当にユーザ自身によるものであることを確認します

CSRFToken



Nextcloudのセキュリティ機能

□認証

- ▶ Nextcloudの認証の種類
- ▶ パスワードポリシー
- ▶ 二要素認証

□保護

- ▶ サーバーサイド暗号化
- ▶ ブルートフォース保護
- ▶ アンチウィルス
- ▶ CSRFトークン

□運用

- ▶ 監査ログ
- ▶ アクセス権限管理

Nextcloudで取得できる監査ログ

ログイン、ファイルアップロード/ダウンロード/更新/削除を記録できます

項目	詳細
日時	操作日時
IPアドレス	操作元のIPアドレス
ユーザー名	操作したユーザー名
操作内容	ログイン、ファイル操作など
環境	利用者の操作環境 (ブラウザ、デスクトップ)

Nextcloud監査ログの例

```
{  
  "reqId": "1R7QNTtwVThLZMR77baE",  
  "level": 1,  
  "time": "2022-12-23 14:55:47",  
  "remoteAddr": "10.10.10.25",  
  "user": "taro.yamada",  
  "app": "admin_audit",  
  "method": "PUT",  
  "url": "/remote.php/webdav/sample-pdf.pdf",  
  "message": "File written to: ¥\"//sample-pdf.pdf¥\"",  
  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,  
like Gecko) Chrome/108.0.0.0 Safari/537.36",  
  "version": "24.0.8.2",  
  "data": {  
    "app": "admin_audit"  
  }  
}
```

操作日時

アクセス元IPアドレス

ユーザー名

操作内容

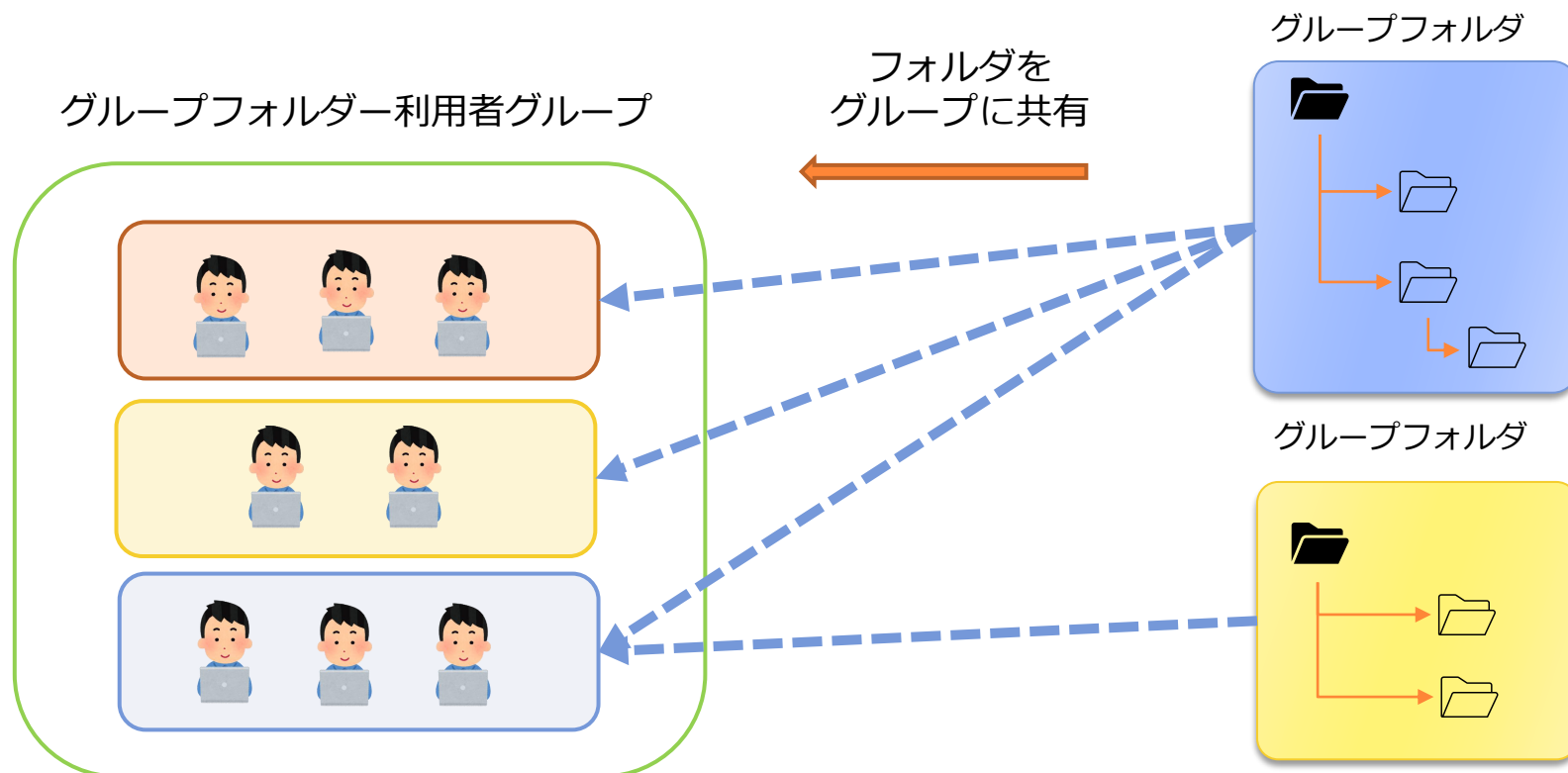
環境

アクセス権限の管理

機能	概要
ファイル共有時の アクセス権限管理	ファイルやフォルダを共有する際に、共有先のユーザーやグループに編集の許可や再共有の許可を設定する機能
グループフォルダ	特定のグループのみがアクセスできる共有フォルダを作成する機能 グループ単位だけでなく、グループ内のユーザーに対して細かい権限管理が可能
ファイルアクセス コントロール	特定の条件やルールに基づいてファイルやフォルダへのアクセスを制限する機能 例： ・ 特定のIPアドレスからのみアクセスを許可 ・ 特定のファイルタイプへのアクセスを制限

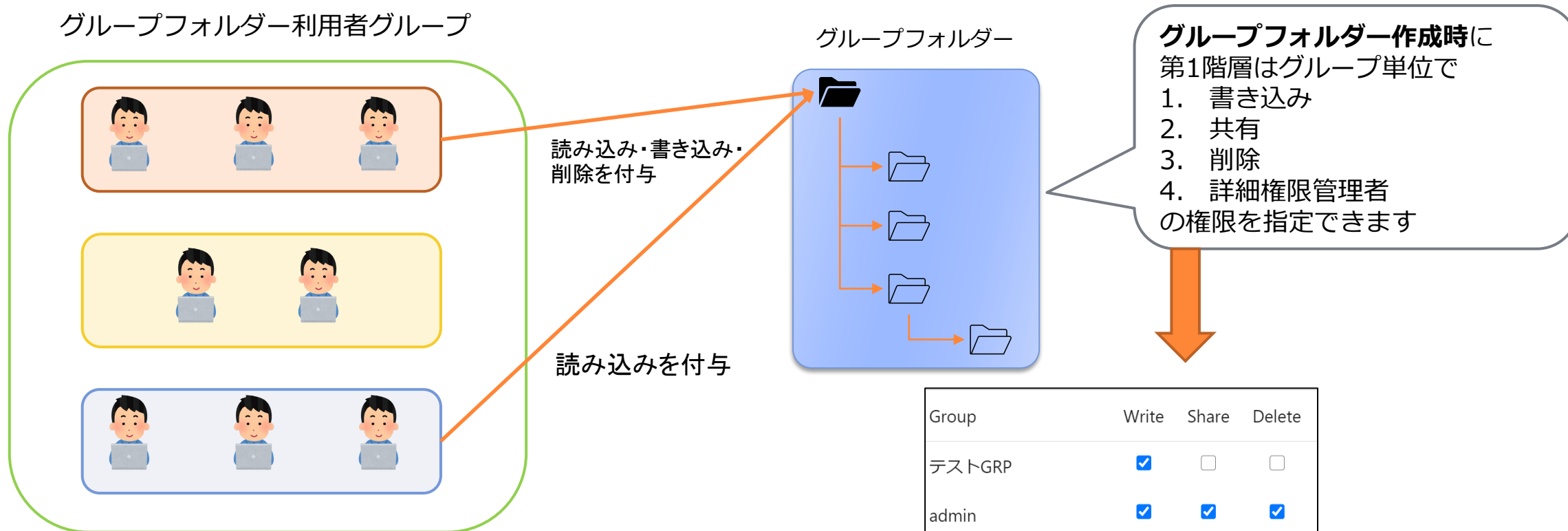
グループフォルダ

- グループフォルダは、特定のユーザーグループのみがアクセスできる共有フォルダを作成する機能です
- グループフォルダには、共有先グループに対しての権限管理と、グループフォルダ内での個別の権限管理の、2つの権限管理があります



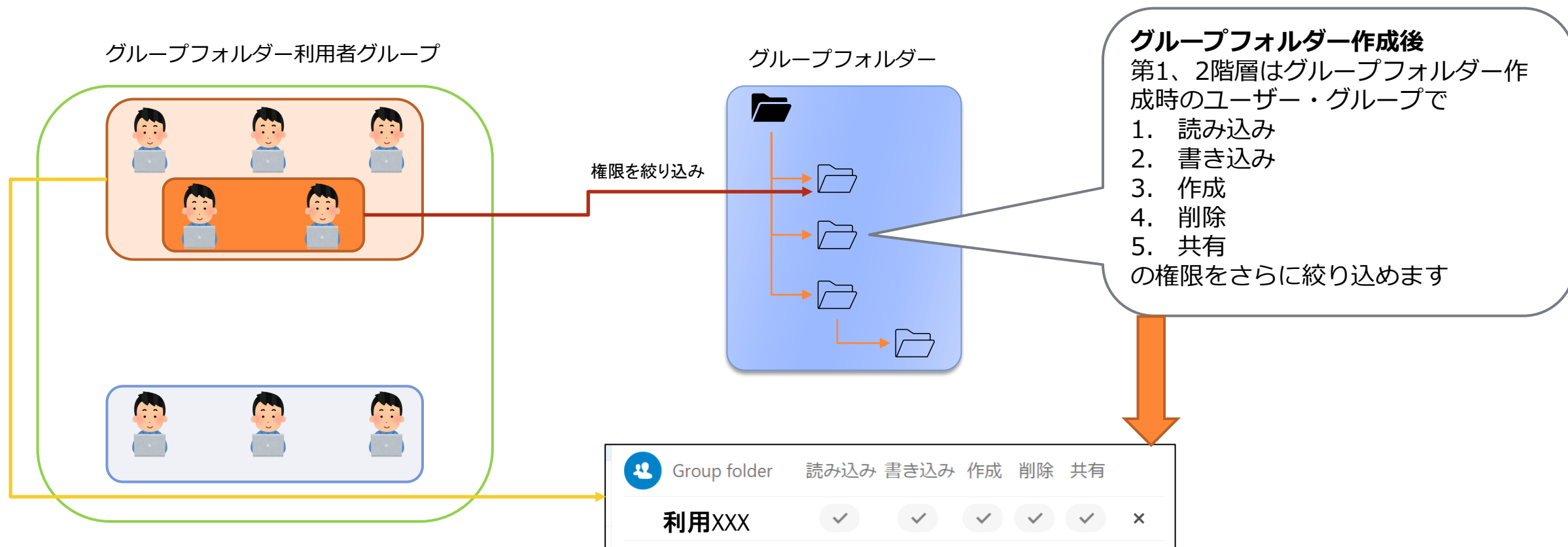
グループフォルダの権限管理①

1. Nextcloudの管理者が、共有先グループへの権限と、グループフォルダの詳細権限管理者を指定します



フォルダーと指定できる利用者の関係について②

2. さらに詳細に設定したい場合は、詳細権限管理者に指定された人が、第1階層と第2階層フォルダー権限を、利用者グループ、またはグループ内のユーザを指定して権限を絞り込めます



グループフォルダの権限管理

- Nextcloudの管理者が、共有先グループに対して以下の制限をかけられます
 - ▶ 書き込み
 - ▶ 共有
 - ▶ 削除

- グループフォルダー作成後、詳細権限管理者がフォルダー第1階層とその配下のフォルダーに対してユーザやグループを指定して以下の権限を制限することができます
 - ▶ 読み込み
 - ▶ 書き込み
 - ▶ 作成
 - ▶ 削除
 - ▶ 共有

まとめ

- 二要素認証に対応しており、TOTPを用いることで導入の手間が少なくセキュリティを高めることができます
- サーバーサイド暗号化はデータ保護に有効ですが、実際の運用方法に応じて有効・無効は適切に選択する必要があります
- グループフォルダを利用することで、ファイルへのアクセス権限をグループ単位からユーザ単位まで細かく管理することができます

スタイルズ Nextcloud ホームページ

製品資料、サービス案内、ブログなど、Nextcloudのお問合せは以下弊社WEBサイトより

<https://nextcloud.stylez.co.jp/>





**実績豊富なエンジニア集団の技術と開発ツールで
「開発期間/コスト削減」「品質向上」を実現**

株式会社スタイルズ

<https://www.stylez.co.jp>

東京都千代田区神田小川町1-2 風雲堂ビル6階

Tel:03-5244-4111

オープンソースソフトウェア推進

