


# セキュリティガイド

---

NASを安全に保つための保護ガイドライン

# 安全シート - 無視できない基本事項


## FIRST TIME INITIATING NAS



**Administrator**  
Don't use default settings!  
Create a new admin



**Passwords**  
Use secure Password policies




**2FA**  
Enhances the security  
of user accounts



**UPnP**  
Turn off Plug and Play  
to avoid attackers


## EVERYDAY / REGULAR TASKS




**Backup**  
More than one backup location!  
Use 3-2-1 Backup Strategy



**Snapshots**  
Capture data constantly  
to present data lost



**Updates**  
Keep software  
up-to-date automatically



**VPN**  
Establish a VPN connection  
for remote access

## ONE TIME TASK - ENABLE & BE SAFE PERMANENTLY



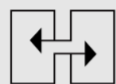
**QuFirewall**  
Download from APP center  
and enable it



**Security Counselor**  
Download from APP center  
and enable it

# 安全シート - **IT**の詳細設定

## FOR PEOPLE WITH A BIT MORE KNOW HOW



### Ports

Change the standard Ports



### Encryption

Use encrypted connections  
(HTTPS)

# 導入

## セキュリティガイド

この短いセキュリティガイドでは、データを最適に保護するための設定について説明を行います。快適さとセキュリティの間には常にトレードオフがあり、すべてのユーザーが自分で決定する必要があります。

このガイドでは、最も重要なトピックの概要を説明します。

詳細情報と手順については、<https://www.qnap.com/en>をご覧ください。

## ランサムウェアとは何ですか？

ランサムウェアは、コンピュータをロックしたりファイルを暗号化したりして、皆様のデータへのアクセスをブロックする悪意のあるプログラムです。被害者は、影響を受けたファイルを復号化するために身代金を要求される、または影響を受けたファイルを再び開くことができなくなります。

## ランサムウェアから身を守るにはどうすればよいですか？

ランサムウェアは、コンピュータとネットワークベースのデバイスを標的とし、ビジネスユーザーとホームユーザーの両方に対して増大している脅威です。ハッカーは、悪意のあるソフトウェアを配置する新しい方法を常に見つけています。

QNAPはこの危険性の高まりを認識しており、マルウェアに対する最善の保護を提供するために絶えず取り組んでいます。

本資料にて、皆様のニーズに応じて皆様自身のデータを保護する方法を示します。

# 初めて**NAS**を使用するとき

## 管理者アカウント

QTSの管理者アカウントはデフォルトで「admin」です。セキュリティ上の理由から、システムクリティカルなアカウントに対して、一般的で簡単に推測できる名前を使用することはお勧めしません。このような場合、ハッカーは正しいパスワードを推測するだけで、システムを完全に制御することができてしまいます。このような危険から身を守るために、別のシステム管理者アカウントを作成し、デフォルトの「admin」アカウントを無効にすることを強くお勧めします。さらに、管理者アカウントは、メンテナンスタスクなどの管理タスクにのみ使用する必要があります。QNAP NASを使用する際には、管理者機能とユーザー機能を完全に分けることをお勧めします。

注：「admin」アカウントを無効にするオプションは、QTS4.1.2以降のバージョンでのみ使用できます。



**CREATE NEW  
ADMINISTRATOR  
ACCOUNT**



**DISABLE THE  
ADMINISTRATOR  
ACCOUNT „ADMIN“**



**USE ADMINISTRATOR  
ACCOUNT ONLY FOR  
ADMINISTRATIVE TASKS**

# 初めてNASを使用するとき

## 「管理者」ユーザーアカウントを無効にする方法

QNAP NASのパスワードには、システムのセキュリティを大幅に向上させる、いくつかのセットアップオプションがあります。もちろん、QNAP NASをご自身だけで使用する場合、パスワードの推奨ルールに従うことに対して責任があるのはご自身だけです。安全なパスワードを実現する基本的な手順は単純です。

### 新しい管理者アカウントの作成

1. 「admin」アカウントを使用してQTSにログインします。
2. [コントロールパネル] > [ユーザー]を選択します。
3. ユーザー（この例では「Ben」）を作成し、「Administrators」ユーザーグループに割り当てます。

### 「管理者」アカウントの無効化

1. 「Ben」としてQTSにログインします。
2. [コントロールパネル] > [ユーザー]を選択し、「admin」アカウントプロファイルを編集します。
3. [このアカウントを無効にする]をクリックして、[OK]を選択します。

# 初めて**NAS**を使用するとき

## パスワードポリシー

QNAP NASのパスワードには、システムのセキュリティを大幅に向上させる、いくつかのセットアップオプションがあります。

もちろん、QNAP NASをご自身だけで使用する場合、パスワードの推奨ルールに従うことに対して責任があるのはご自身だけです。安全なパスワードを実現する基本的なルールは単純です。



十分に長い



特殊文字を含む

aA

大文字と小文字を使用する



複数のアプリケーションに対して  
同じパスワードの使用を避ける



定期的なパスワード変更

他のユーザーもQNAP NASを利用できる場合、管理者はパスワードに特定のルールを設定し、QNAP NASに対してルールを適用する必要があります。

これにより、上記のルールが確実に守られます。簡単な説明は次のページにあります。

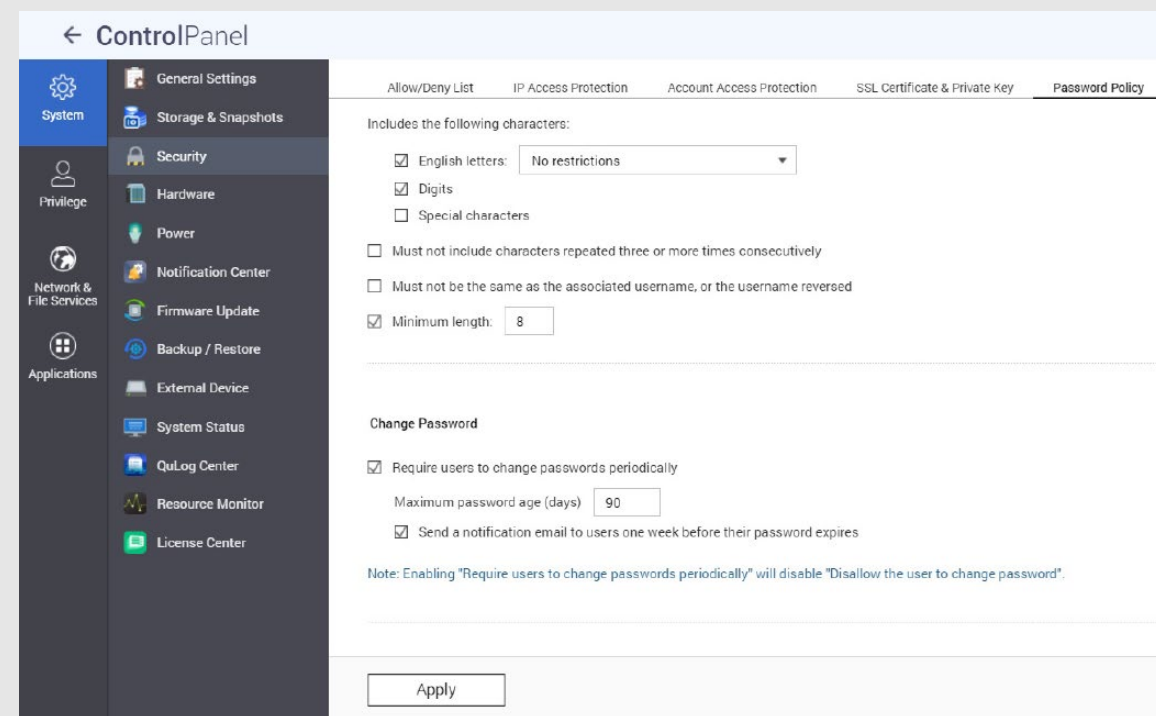
# 初めてNASを使用するとき

## パスワードポリシー

- 1.[コントロールパネル]>[システム]>[セキュリティ]>[パスワードポリシー]に移動します。
  2. [パスワード強度]で、条件を選択します。
    1. 新しいパスワードには、大文字、小文字、数字、特殊文字の中で少なくとも**3種類**の文字を含めます。
    2. 新しいパスワードには、文字を**3回**（またはそれ以上）繰り返すことはできません（例：**AAA**）。
    3. パスワードは、対応するユーザー名と同じであってはならず、また、逆にしたものであってもいけません。
  3. [パスワードの変更]で、**[NASユーザーにパスワードを定期的に変更させる]**を選択します。

重要：この設定を有効にすると、**[ユーザーによるパスワード変更を禁止]**設定が無効になります。

    - 1.パスワードが有効な最大日数を指定します。
    - 2.オプション：**[パスワード失効の1週間前にユーザーに通知メールを送信する]**を選択します。
  - 4.[適用]をクリックします。





# 初めてNASを使用するとき

## 2FA

2FA = 2段階認証プロセスにより、ユーザーアカウントのセキュリティが強化されます。

有効にすると、NASにサインインするたびに、パスワードに加えてワンタイムの

セキュリティコード (6桁) を入力する必要があります。2段階認証プロセスには、

Time-based One-Time Password (TOTP) プロトコルをサポートする認証システムアプリを  
備えたモバイルデバイスが必要です。サポートされているアプリには、Google Authenticator

(Android / iPhone / BlackBerry) または Authenticator (Windows Phone) が含まれます。

この機能を使用するには、次の手順に従います。

1. モバイルデバイスに Authenticator アプリをインストールします。

2. [パスワード強度] で、条件を選択します

3. [オプション] > [2段階認証] に移動し、[使用開始] をクリックします。

1. QRコードをスキャンするか、アプリにセキュリティキーを入力して、

Authenticator アプリを構成します。

2. アプリから生成されたコードを NAS に入力して、正しい構成を確認します。

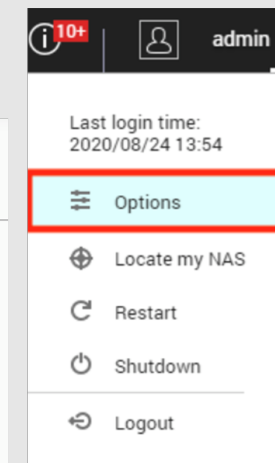
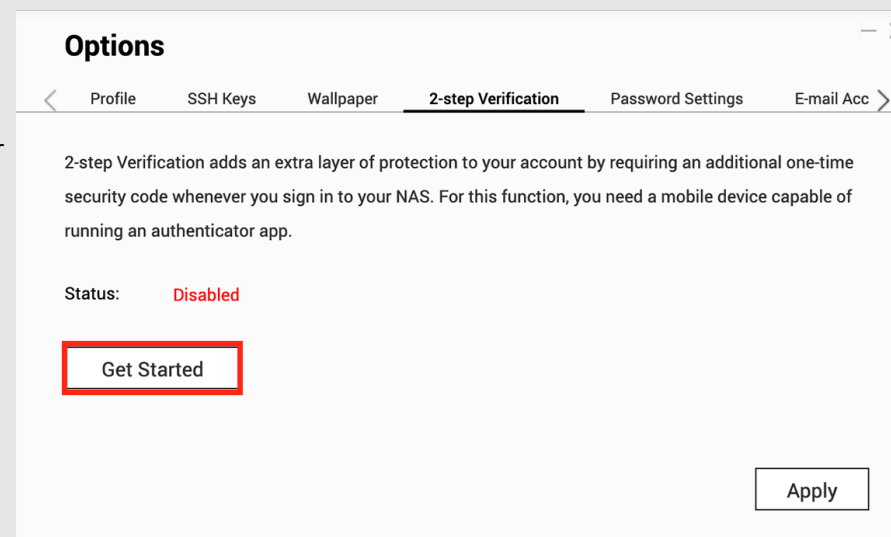
3. セキュリティコードを電子メールで受け取るか、モバイルデバイスを使用できない場合はセキュリティ質問に答えて、

別の確認方法を選択します。セキュリティコードを電子メールで送信するには、SMTPサーバーが

[コントロールパネル] > [通知センター] > [電子メール] で適切に構成されている必要があります。

セットアップの詳細な説明は、チュートリアル Web サイトにあります。

<https://www.qnap.com/ja-jp/how-to/tutorial/article/2-段階検証を利用してアカウントのセキュリティを強化する方法とは>



# 日常/定期的なタスク

## 3-2-1バックアップ戦略

### バックアップ

データをどこで、どのように、どのくらいの頻度でバックアップするかといった、別のトピックがあります。ここでの決定的な要因は、セキュリティのニーズ、データの関連性、利用可能なオプションです。ただし、重要なデータを確実にバックアップするために従うべき経験則があります。

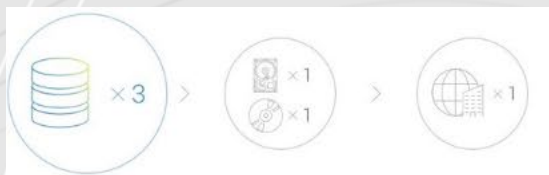
**重要**：RAIDはバックアップではなく、ハードディスクの障害から保護します。スナップショットは、ローカルコンピュータからのランサムウェア攻撃からユーザーのデータを保護します。

### 3-2-1バックアップ戦略

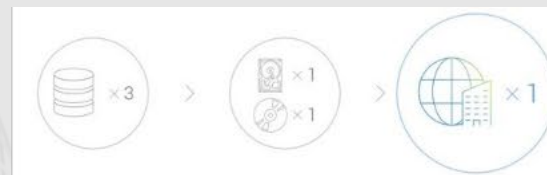
悪意のあるソフトウェアからの影響に対する最初の防衛線は、慎重で賢明な使用習慣（ソフトウェアを定期的に更新する、信頼できない電子メールを開かない、不明なWebサイトにアクセスしないなど）を実践することですが、常にデータをバックアップすることを忘れないでください。

完璧なバックアップ計画はありませんが、**3-2-1**バックアップは良いスタートです。重要なファイルのコピーを**3**つ保持し、ファイルを少なくとも**2**種類のストレージメディアに保存し、**1**つのコピーをオフサイトに保存します。

Important data should be backed up at least  
**3 copies**: 1 main file and 2 backup files.



**One** of the backups is to be stored offsite  
(outside the home or business).



Archives are stored on **2 different** backup media  
to protect against various types of hazards.



# 日常/定期的なタスク

## スナップショット

スナップショットとは何ですか？

スナップショットは、QNAP NASに保存したデータの画像です。初めてスナップショットを作成すると、すべてのストレージがキャプチャされます。その後のすべてのスナップショットは、最後のスナップショット以降に変更されたコンテンツのみを記録します。スナップショットはブロックベースであるため、スペースを大幅に節約できます。

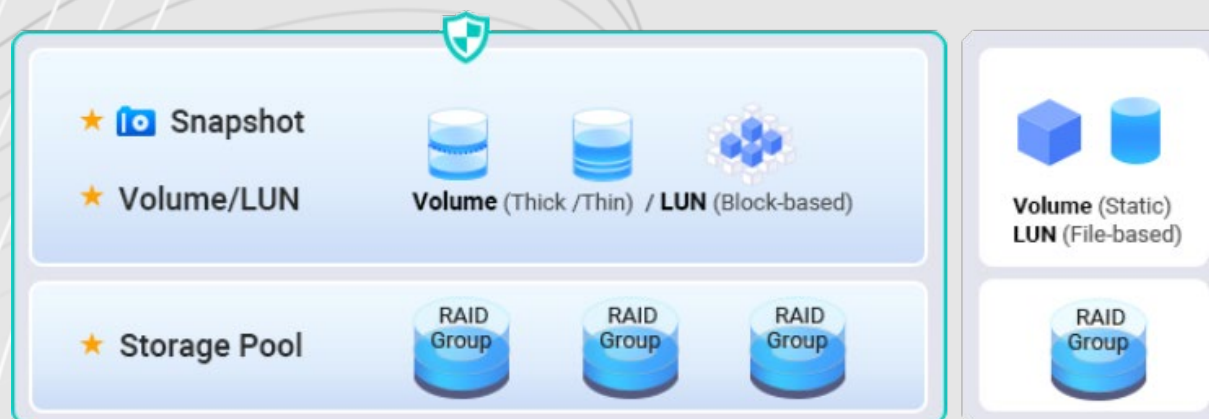
**重要：**

スナップショットはバックアップではありません。以前のバージョンが誤って削除された場合や、コンテンツが誤って変更された場合に、以前のバージョンにアクセスできます。

このトピックの詳細な説明は、当社のWebサイトにあります。

<https://www.qnap.com/ja-jp/software/snapshots>

スナップショットの設定



# 日常/定期的なタスク

## 自動アップデート

### アップデート

NASでは、最新のシステムソフトウェアが重要です。QNAPは常に、新たなセキュリティギャップが発生しないよう、必要に応じてシステムに新しい機能を追加します。したがって、データを可能な限り保護するために、常に迅速にアップデートを行う必要があります。

QNAP NASがインターネットに接続されていて、デフォルト設定を変更していない場合、デバイスは自動的に最新のシステムソフトウェアをチェックし、警告を發します。その後、必ずアップデートを行ってください。QNAP NASをアップデートするには再起動で、これにより5~10分間利用できなくなることに注意してください。

最新のシステムソフトウェアを手動でインストールするオプションもあります。これは、QNAP NASがインターネットに接続されておらず、自動的にアップデートを確認・更新できない場合に必要です。

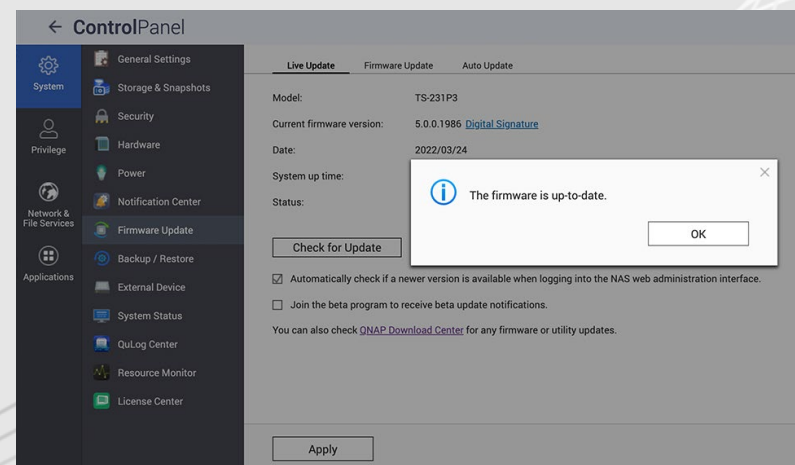
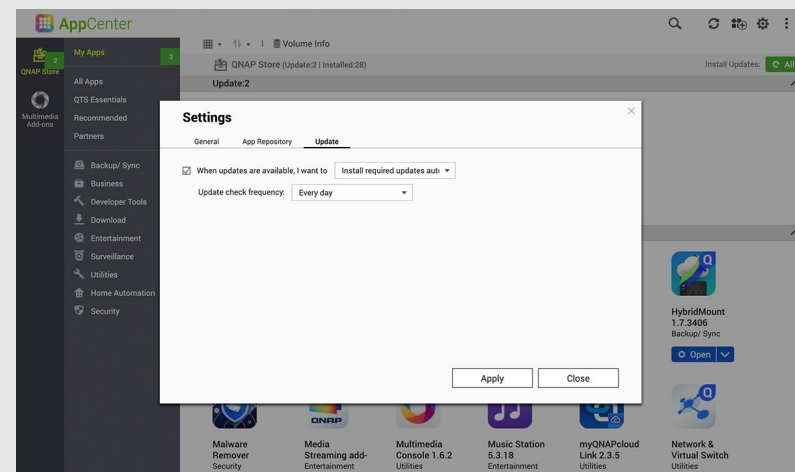
ファームウェアが最新か確認するには、次のようにしてください。

### リアルタイムファームウェアアップデート

1. 「管理者」としてログインします
2. [コントロールパネル]> [ファームウェア更新]を開きます
3. ライブアップデートを開きます
4. [更新の確認]をクリックします

### アプリを自動的に更新する

1. AppCenterに移動します
2. 設定に移動します
3. 更新を開きます
4. 「更新が利用できるとき...」を選択します
5. [すべての更新を自動的にインストールする]を選択します



# 日常/定期的なタスク

## VPN

### VPNとは何ですか？

VPNは仮想プライベートネットワークです。私たちは、これによって外出中にQNAP NASへの安全なアクセスを確立することを目的としています。

VPNサーバーはQNAP NASで実行され、特別なVPNソフトウェアは外出先のデバイスで実行されます。これら2つの間には、インターネットを介してトンネルが設定されます。この利点は、接続が認証と暗号化によって保護され、許可された人だけが使用できることです。したがって、このようなVPN接続は、両方のデバイスが同じネットワークにログインしているかのように動作し、ローカルリソースにこれ以上の手間をかけずにアクセスできます。一度設定すると、VPN接続を何度でも簡単に使用でき、ホームネットワークへの安全なアクセスが保証されます。

外出中は常にVPN経由で接続を確立することをお勧めします。データ転送の速度は多少低下しますが、接続は安全です。

### VPNを設定して使用するにはどうすればよいですか？

セットアップの詳細な説明は、チュートリアルWebサイトにあります。

<https://www.qnap.com/ja-jp/how-to/tutorial/article/qvpn-のセットアップ方法と使用方法>

### リモートアクセスの推奨事項

myQNAPcloud Link & VPN (ポートフォワーディングVPNサービスポートが必要です。保護を強化するためにQuFirewallを有効にすることをお勧めします)



# ワンタイムタスク

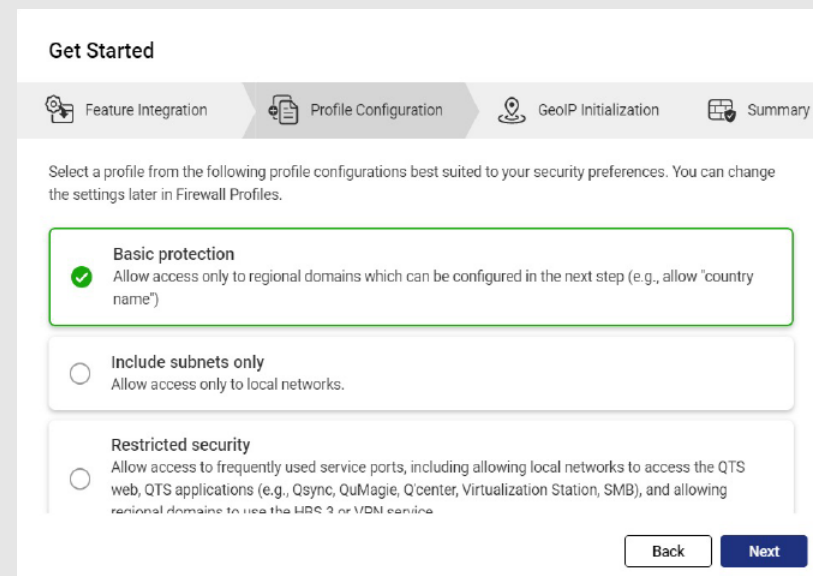
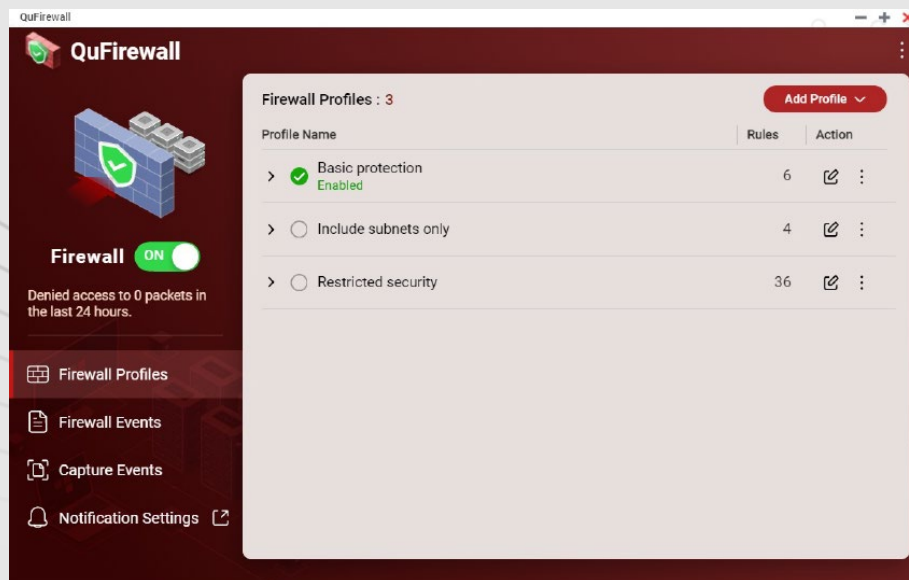
## QuFirewall

### QuFirewallとは何ですか？

QuFirewallは、QNAPデバイス用のファイアウォール管理アプリケーションです。強力で使いやすいプロファイリングシステムを統合することにより、デバイスへの接続を制御および検証できます。QNAPは、QNAP NASにQuFirewallをインストールし、許可するIPアドレスを特定のリージョンまたはサブネットに制限することをお勧めします。

### QuFirewallをセットアップする

- 1.AppCenterからQuFirewallをインストールします
- 2.プロファイル構成を選択します
- 3.お住まいの地域を選択してください
- 4.[完了]をクリックします



# ワンタイムタスク

## Security Counselor

「**Security Counselor**」とは何ですか？

Security Counselorは、QNAP NASのセキュリティポータルです。システムの脆弱性をスキャンし、さまざまな攻撃方法からデータを保護するための推奨事項を提供します。ネットワーク環境のセキュリティ要件に基づいて、3つのデフォルトのセキュリティポリシー（基本/中級/上級）のいずれかを選択できます。セキュリティチェック機能は、システムをスキャンするときに、選択したポリシーを使用します。カスタムセキュリティポリシーを選択して、独自のポリシーを構成することもできます。



基本



中級



上級



カスタム

セキュリティスキャンは、手動またはスケジュールに従って実行し、最大限の保護を確保できます。

スケジュールはさまざまな方法（毎日/平日/週末/特定の曜日）に設定して、作業が中断されないようにすることができます。

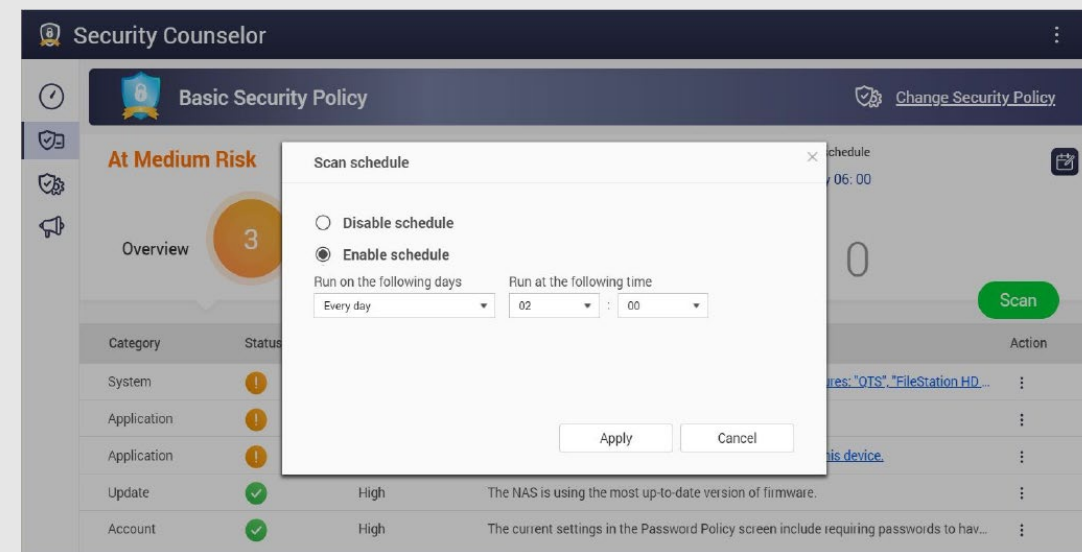
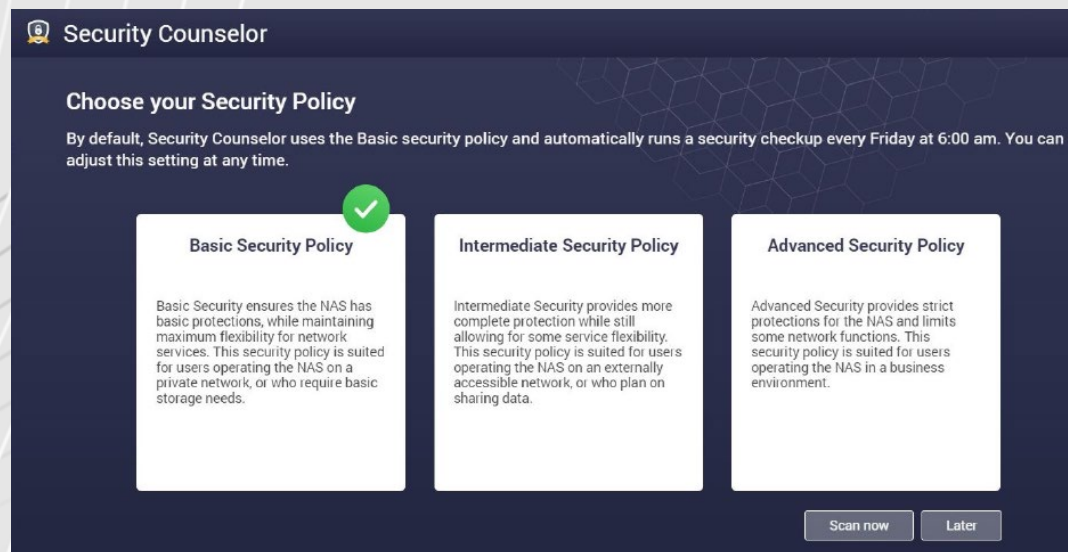
スキャン結果をクリックすると、Security Counselorが適切なシステムセクションに案内し、NASを保護するための関連設定を変更します。

# ワンタイムタスク

## Security Counselor

「Security Counselor」のセットアップ

- 1.AppCenterからSecurity Counselorをダウンロードします
- 2.セキュリティポリシーを選択し、[今すぐスキャン]をクリックします
- 3.スケジュールを作成するには、セキュリティチェックアップ(緑)に移動します
- 4.スキャンスケジュール(赤)に移動します
- 5.希望の時間を選択し、[適用]をクリックします





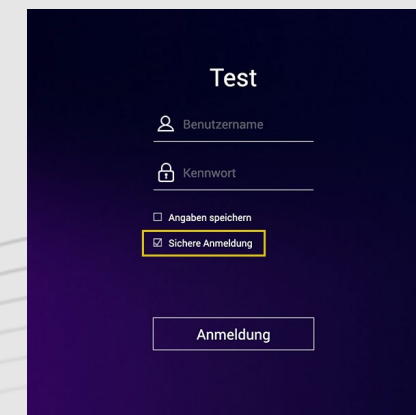
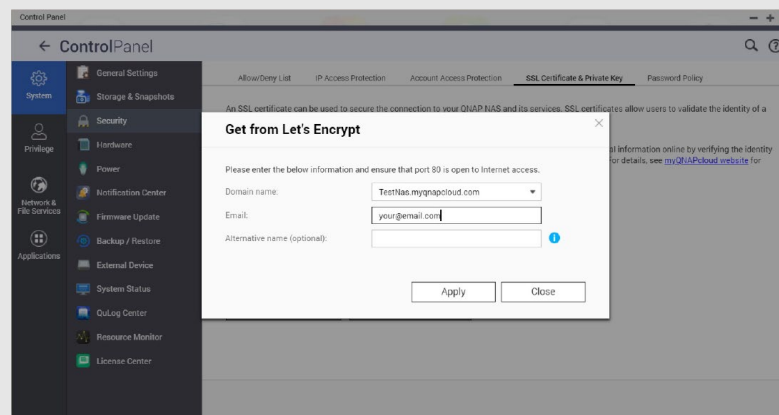
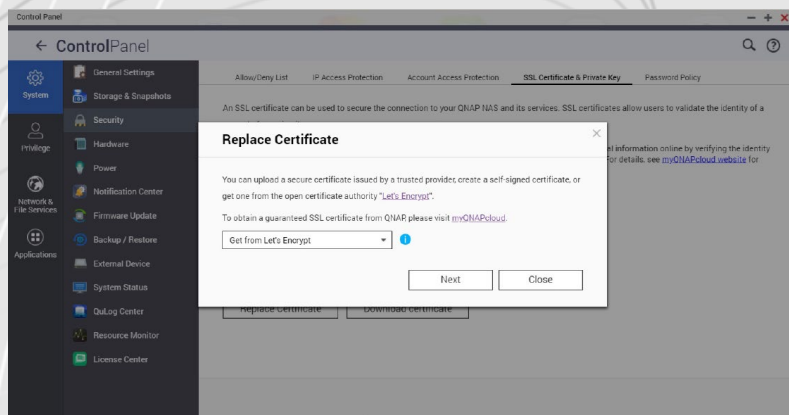
# 高度な設定

## 暗号化された接続

### 暗号化されたHTTPS接続を使用

独自のネットワークの外部からQNAP NASに接続する場合は、データが暗号化されていることを確認する必要があります。これにより、第三者がデータを「読み取る」ことができなくなります。保護された接続を使用することで、これを確実に行うことができます。たとえば、HTTPの代わりにHTTPS、FTPの代わりにFTPSです。Sは「セキュア」の略で、データ転送は証明書で暗号化されるようになり、それぞれの当事者の信頼性が保証されます。

- 1.[コントロールパネル]> [システム]> [セキュリティ]を開き、[SSL証明書と秘密鍵]に移動します。
- 2.[証明書の置換]をクリックします。
3. Let'sEncryptからGetを選択します。
4. [ドメイン名]に、NASにアクセスできる名前またはDDNSを入力します。
5. Lets'sEncryptに登録するための電子メールアドレスを入力します。
- 6.Webインターフェースにログインするときに[セキュアログイン]を選択します



# 高度な設定

## ポート

### ポートとは何ですか？

ポートを使用すると、コンピュータと別のコンピュータ、およびインターネット間の通信が可能になります。ファイアウォールは未使用のポートを閉じて、マルウェアのコンピュータへの侵入を防ぎます。ポートフォワーディングを設定することにより、インターネットからの接続を受け入れるオンラインサービスやその他のインターネットアプリケーションを使用したり、インターネット上のユーザーがホームネットワーク上のWebサーバーやリモートサーバーやその他のサービスにアクセスできるようにしたりできます。

### デフォルトポートの変更

21、22、80、443、8080、8081など、ルーターの構成のデフォルトポートをランダムなカスタムポート番号に変更する必要があります。たとえば、ポート番号8080を9527に変更します。これを行う方法については、ルーターの製造元にお問い合わせください。

### 「システムポート」/不要なサービスポート (SSH、Telnetなど) を転送しないでください

不要なサービスポートでポート転送を無効にすると、攻撃対象となる領域を減らすことができます。

ポート転送後、これらのサービスポートにはインターネット経由で誰でもアクセスできます。

# 補足資料

- バックアップ：<https://www.qnap.com/ja-jp/how-to/tutorial/article/hybrid-backup-sync>
- 管理者アカウント：<https://www.qnap.com/ja-jp/how-to/faq/article/既定のadminアカウントの名前を変えることはできますか>
- パスワードポリシー：<https://www.qnap.com/en/how-to/knowledge-base/article/setup-the-password-policy-to-require-the-change-periodically>
- UPnP：<https://docs.qnap.com/nas-outdated/QTS4.3.5/en/GUID-907F01D9-68D9-4449-A4D1-3213E19D0124.html>
- 暗号化：<https://www.qnap.com/ja-jp/how-to/tutorial/article/ssl-証明書を使用しqnap-nas-接続のセキュリティを強化する>
- VPN：<https://www.qnap.com/ja-jp/how-to/tutorial/article/qvpn-のセットアップ方法と使用方法>
- ポートフォワーディング：<https://www.qnap.com/en/how-to/faq/article/how-do-i-set-up-port-forwarding-on-the-nas>
- QuFirewallの使用方法：<https://www.qnap.com/ja-jp/how-to/tutorial/article/qufirewall-の使用方法>
- アップデート：<https://www.qnap.com/en/how-to/tutorial/article/how-to-update-your-qnap-nas-firmware>
- Security Counselor：<https://www.qnap.com/solution/security-counselor/ja-jp/>