



2023

# セキュリティガイド

2 0 2 3

## セキュリティガイド

# 目次

- 1 はじめに
- 2 よくある攻撃
- 3 ネットワーク機器の基本概念
- 4 Internet から NAS に接続するための種々の方法

## NAS をインターネットから見えないようにする

- 8 NAS を正しく接続する
- 9 ルーター設定を確認する
- 12 NAS 設定を確認する
- 15 ネットワーク関連設定のチェックリスト

## NAS のセキュリティ設定

- 17 システム通知の設定
- 24 ファームウェア (QTS / QuTS hero) の自動更新を有効にする
- 25 アプリの更新設定
- 27 不要な機能の無効化や削除
- 29 Telnet / SSH の無効化
- 30 システムアカウントセキュリティの強化
- 34 パスワードポリシーの設定
- 35 アクセス保護の有効化 (IP / アカウント)
- 36 2 段階認証 (2SV) の有効化
- 39 デフォルトポートの変更
- 40 アクセスログを表示
- 41 セキュリティアプリのインストールと有効化
- 42 セキュリティカウンセラー
- 45 Malware Remover
- 46 QuFirewall
- 51 スケジュールしたスナップショットの有効化
- 53 スナップショットの削除ポリシーを設定する
- 54 NAS のセキュリティ設定のチェックリスト



# はじめに

QNAP はセキュリティに最大限の配慮をしています。高まり続ける脅威に直面しながら、QNAP は休むことなくハードウェアとソフトウェアの設計を改善し続け、ユーザーにセキュアで便利なソリューションの提供を目指しています。

QNAP の Product Security Incident Response Team (PSIRT) は、QNAP の製品に関連するセキュリティ上の問題に対応する責任をもっています。サイバーセキュリティに関連したインシデントの対応に加え、PSIRT はさまざまな製品における脆弱性の報告、調査、改善、公表も担当しています。

QNAP はまた、製品セキュリティの強化にも取り組んでいます。従来は、製品をユーザーがセットアップし、利用する際の利便性と使い勝手を重視して設計されていました。近年、ネットワークにつながれたデバイスへのサイバー攻撃の増加により、QNAP の製品設計理念も変化し、製品設計は、ユーザーのために防御をし、関連する脅威にユーザーが対処できるよう、セキュリティを設計段階で確保するようになりました。

このチュートリアルを、ユーザーが NAS を正しく設定し、セキュリティを高めるために役立ててください。ご質問の際は、弊社の技術サポートまでお問い合わせください。



製品の脆弱性やセキュリティ関連のインシデント情報については、QNAP セキュリティアドバイザリを参照および購読してください。

<https://www.qnap.com/go/security-advisories/>



QNAP カスタマーサービス :

<https://service.qnap.com/>



# よくある攻撃

サイバー攻撃に対する防御方法を知るためには、攻撃がどのように行われるかを知る必要があります。NAS に対する攻撃では、そのほとんどがインターネット経由で行われます。攻撃には大別して 2 つのタイプがあります。「パスワードクラッキング」と「脆弱性攻撃」です。ここで、「脆弱性攻撃」は、「N デイ」と「0 デイ」に分けられます。

「N デイ」とは、攻撃をする際にパッチされた脆弱性を悪用するもので、現在のほとんどの攻撃はこの種類に該当します。そういった攻撃に対しては、最新のパッチと更新を常にインストールしておくことで効果的な防御が可能です。

「0 デイ」は、未知の脆弱性を悪用して攻撃をしかけるもので、ベンダーがセキュリティパッチを出すのは事後になります。そういった攻撃に対しては、攻撃者がデバイスに接続できないようにするしか、効果的な防御方法はありません。

次の表は、参考のために攻撃別に対応方法を示しています。

対応	攻撃		
	パスワードクラッキング	脆弱性攻撃 (N デイ)	脆弱性攻撃 (0 デイ)
インターネットから見えないようにする	V	V	V
ソフトウェアを更新する (システムおよびアプリ)	X	V	Δ
自動更新を有効にする (システムおよびアプリ)	X	V	Δ
全アカウントで強力なパスワードを使用する	V	X	X
デフォルトの「admin」アカウントを無効にする	V	X	X
2 段階検証を有効にする	V	X	X
アクセス保護を有効にする	Δ	X	X
ファイアウォールを有効にする	Δ	Δ	Δ
システム通知を受け取る	Δ	Δ	Δ
デフォルトポートを変更する	Δ	Δ	Δ
不要な機能を無効化 / 削除する	Δ	Δ	Δ

V: 効果的 X: 効果なし Δ: 一定の効果 ( 攻撃を緩和できる、あるいは攻撃されるリスクを低められる )

「インターネットから見えないようにする」ことで、攻撃者がデバイスに接続し、攻撃を行うことを効果的に防げます。このチュートリアルではまず始めに、「インターネットから見えないようにする」方法を解説し、次に NAS の防御力を高めるために「NAS のセキュリティ設定」を詳述します。

# ネットワーク機器の基本概念

ネットワークデバイスの一種である NAS は、2 つの接続方向をもっています。

## 01 | NAS の外部接続



NAS は通常、適切な動作のために外部接続を必要とします。たとえば、自動更新や通知の設定といった基本的なシステム機能です。それに加えて、NAS データをパブリッククラウドにバックアップする、あるいは NAS を他のデバイスやパブリッククラウド（仮想マシン、Google Workspace、Microsoft 365 など）、コンピューターやサーバーからのデータをバックアップするために使用が必要があれば、NAS は相手への接続ができなければなりません。

## 02 | NAS に接続するその他のデバイス（コンピューター、モバイル機器、その他のサーバー）



ファイルへのアクセスや設定インターフェースの表示など、NAS が提供する機能やサービスを使用する必要がある場合は、NAS への接続ができなければなりません。

ルーターが DMZ やポートフォワーディング、UPnP 機能をもっていない場合、ルーターはインターネットからのトラフィックをブロックします。ローカル ネットワーク上のデバイスだけが、NAS にアクセスできるようになります。

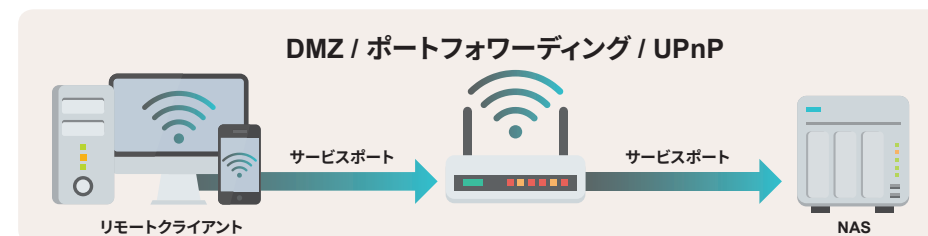
ルーターが有効で上記の機能が設定されている場合、オープンポートにはインターネットから誰でも接続ができ、ルーターのルールに従って NAS に転送され、ログインし、関連機能を通常通り使用することができます。しかし、これはハッカーがパスワードクラッキングやソフトウェア脆弱性の悪用を行う余地を与えることになり、セキュリティリスクとなります。

# リモートから NAS に接続するいくつかの方法

## 01 | ルーター上で、DMZ やポートフォワーディング、UPnP を有効にし、設定する

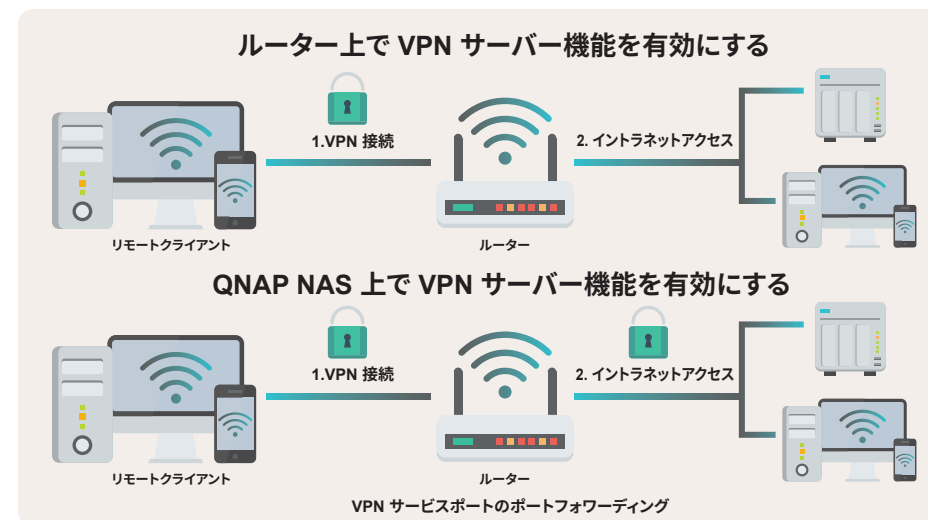
この方法にはセキュリティリスクがあります。ネットワーク設定についての深い知識があり、これに伴うリスクを理解している人でない限り、**QNAP ではこの方法の利用をお勧めしません**\*。ルーターはトラフィックをイントラネット デバイスに渡してしまうため、悪意のあるトラフィックをブロックするファイアウォールがルーターと NAS の間に設置されていなければ、ハッカーは容易にネットワーク攻撃を行えるようになります。ただし、ファイアウォールが設置されていたとしても（基本的なファイアウォールの利用や企業グレードのファイアウォールの購入で）、すべての攻撃をブロックできる保証はありません。

\* QNAP では、比較的低リスクの低い VPN サービスポートのみをインターネットに開き、システム管理、SMB、SSH サービスなどの高リスクサービスポートはインターネットから容易にアクセスできないようにすることをお勧めします。



## 02 | ルーターまたは QNAP NAS で VPN サーバー機能を有効にする

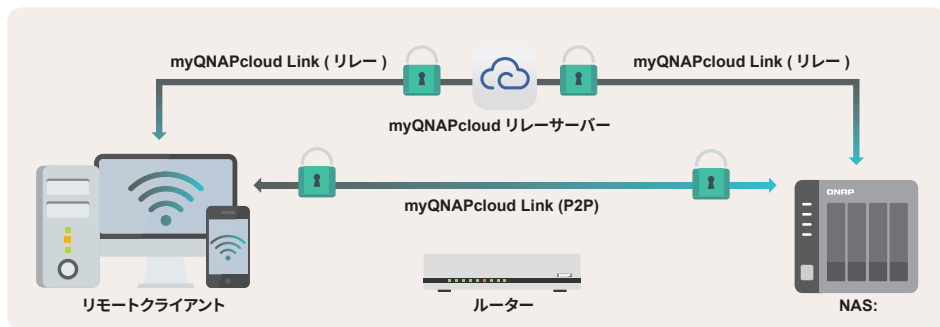
ルーターの中には、VPN サーバー機能をサポートするものがあり（QNAP QHora や QMiro シリーズルーター）、QNAP NAS も複数の VPN サーバーをサポートします。有効化されて適切に設定されれば、インターネットから VPN サーバーへの VPN 暗号化接続によって、イントラネット上の各デバイスにアクセスすることができ、高いレベルのセキュリティが実現できます。





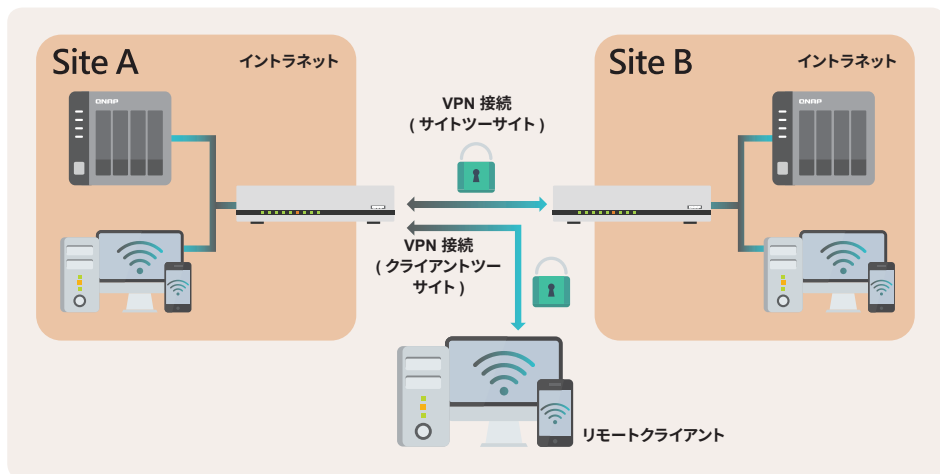
### 03 | myQNAPcloud Link のセキュア接続を利用

NAS への接続に myQNAPcloud Link を利用する場合は、それが直接 NAS サービスをインターネットに開くため、ルーターの設定は不要です。myQNAPcloud Link は、ネットワーク環境に応じてリレーサービスまたはピアツーピア テクノロジー (P2P) で接続を確立します。接続全体がセキュリティ確保のために暗号化されます。



### 04 | SD-WAN またはサイトツーサイト VPN 製品を使用する

上述の VPN サーバー機能 (クライアントツーサイト VPN) と異なり、SD-WAN またはサイトツーサイト VPN は、異なる場所にある 2 台あるいはそれ以上のルーター間でセキュアな暗号化 VPN 接続を確立します。デバイスをサイトツーサイト VPN ネットワークにつなぐだけで、あたかも同じイントラネットにあるように接続できるため、複数の場所があるユーザーには理想的です。クライアントツーサイト VPN を使うと、どこからでも NAS にアクセスできます。



比較表を参照し、ご自身に合った接続方法をお選びください。QNAP では、ユーザーニーズに合わせて、複数のセキュアな接続ソリューションを用意しています。

接続方法	長所	短所	適するユーザー
ルーター DMZ/ポートフォワーディングを UPnP で有効にして設定	• 接続がもっとも早い	• サイバー攻撃に弱い • 0 デイ脆弱性攻撃に対する防御がない	• 関連リスクに対する明確な理解をもつ • ネットワーク設定を理解している • 重要なデータに対し複数のバックアップをとる • ディザスタリカバリプランをもつ
ルーターで VPN サーバーを有効にする*	• 設定が比較的シンプル	• ログイン失敗通知、オートブロック、ファイアウォールの機能がない • サポートされる VPN プロトコルが少ない • 性能はルーターのハードウェアによって制限される	• ネットワーク設定に不案内 • 転送速度は気にしない
QNAP NAS 上で VPN サーバー機能を有効にする*	• 複数の VPN プロトコルをサポート • NAS ファイアウォールに対応 (QuFirewall) • ログイン失敗とオートブロックをサポート	• 設定は若干複雑	• ネットワーク設定を理解している • 多くのファイルにインターネットから頻繁にアクセスが必要
myQNAPcloud Link のセキュアな接続を利用	• セットアップが非常に簡単 • アクセス制御をサポート • NAS をインターネットに見せる必要がない	• 接続が低速	• ネットワーク設定に不案内 • インターネットからの NAS へのアクセスが頻繁でない • WAN IP アドレスを取得できないネットワーク環境
SD-WAN またはサイトツーサイト VPN 製品を使用する*	• 一度設定すると、イントラネットユーザーは違いを意識せずに使用できる • クライアントツーサイト VPN もサポートする	• 追加の機器が必要	• マルチポイントアクセスとリモートバックアップが必要 • 付加価値アプリケーションが必要

\* QNAP NAS がサポートする機能 :  
myQNAPcloud Link / VPN Servers (L2TP/IPsec, OpenVPN, WireGuard, QBelt) / QuWAN SD-WAN

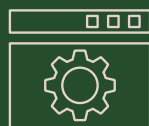
\* QNAP ルーターがサポートする機能 :  
QuWANSD-WAN / VPN Servers (L2TP/IPsec, OpenVPN, WireGuard, QBelt)

# 一般的なホームルーターを参照

# 01

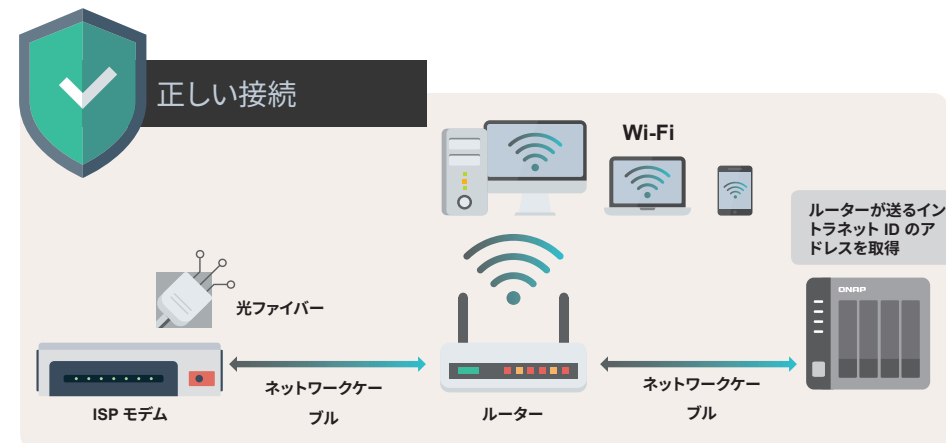
## NAS セキュリティ設定ガイド

### NAS をインターネットに見せないようにする

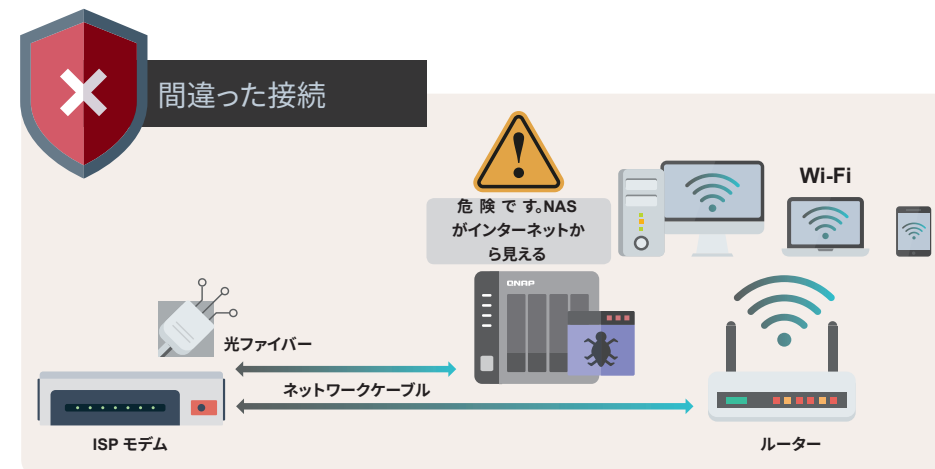


## NAS を正しく接続する

お使いの NAS がルーターに接続されていることを確認してください。設定が正しければ、ルーターはインターネットからの接続をブロックし、NAS をインターネットから隠すことでサイバー攻撃を防止します。



NAS を ISP 提供のモデムに接続する場合、NAS は直接 WAN IP アドレスを取得します。その場合、ハッカーを含むだれでも、インターネット経由で NAS に接続、さらには攻撃や侵入を試みる可能性があります。

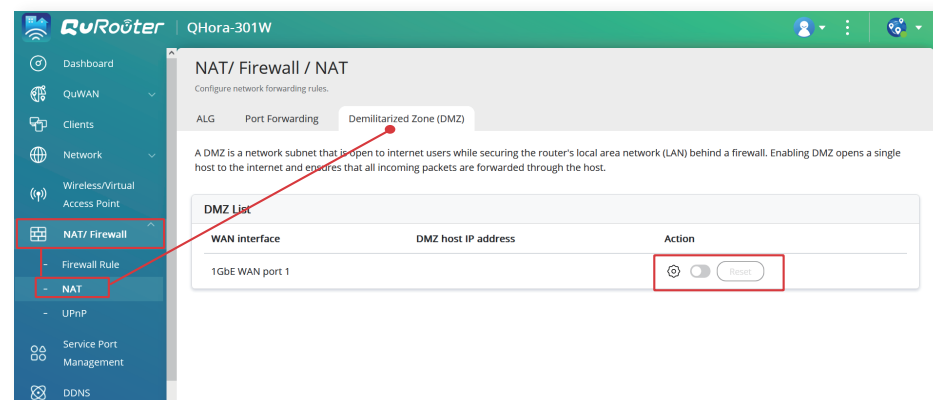
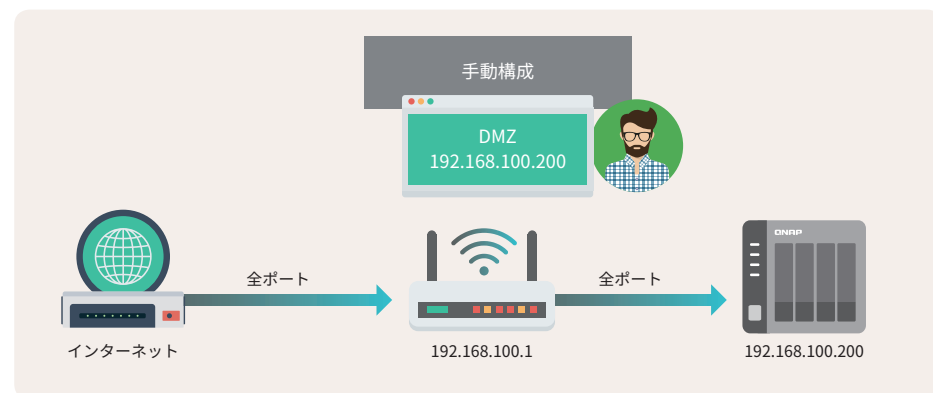


# ルーター設定を確認する

デフォルトでは、ルーターの背後にあるデバイスにインターネットから直接接続することは理論的にできませんが、「DMZ (Demilitarized Zone)」、「ポートフォワーディング」または「UPnP (Universal Plug and Play)」を有効にしていると、ルーターはルールに従ってユーザーが選択したデバイスにパケットを転送するため、デバイスがインターネットから見えることになります。必要に応じて、転送機能が**無効になっていること**をチェックし、確認してください。

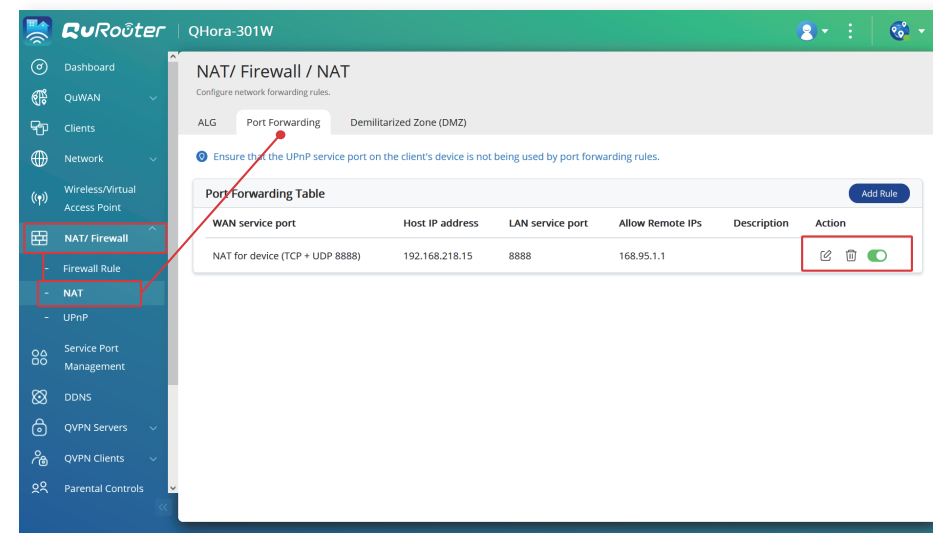
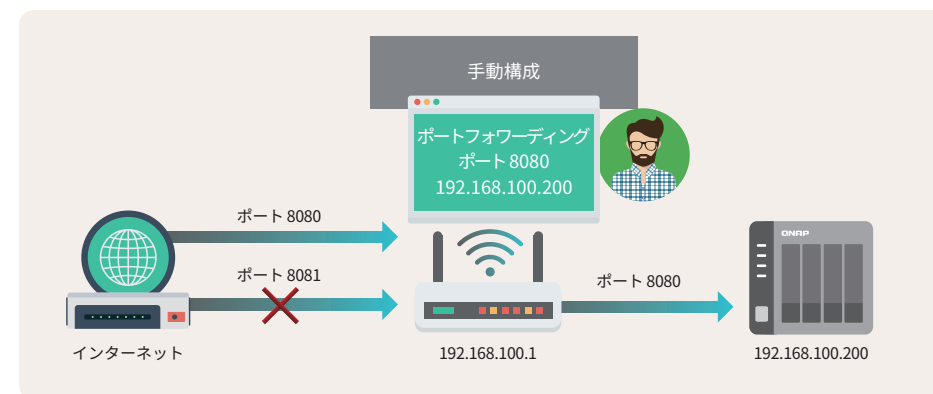
## 01 | DMZ (Demilitarized Zone) をチェックする

この機能を有効にした後、選択したデバイスの全サービスポートは、インターネットから直接開かれ、インターネットから見えるようになります。セキュリティリスクを下げるために、この機能は無効にしてください。



## 02 | ポートフォワーディングをチェックする

この機能は、デバイス上の特定のサービスポートをインターネットに対して開くことができ、だれもがインターネット経由で関連サービスにアクセスできるようにします。ただし、開かれているサービスにインターネットからハッカーが攻撃を仕掛けることもできます。そのため、この機能を使って求められるサービスをインターネットに対して開く前に、まずすべてのポートでフォワーディングルールを無効にしてから、NAS のセキュリティを設定し、重要データをバックアップすることをお勧めします。



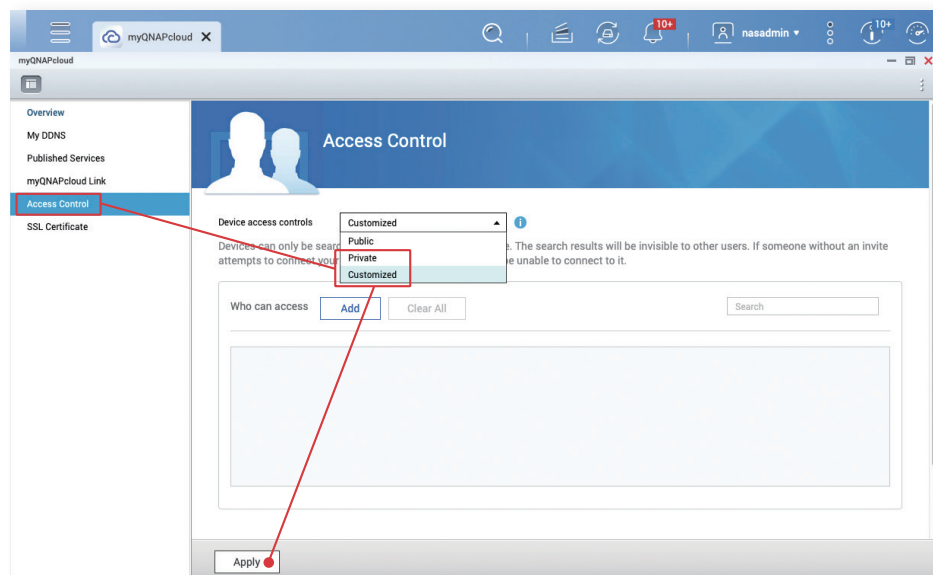
4. 「自動ルーター構成」設定ページで、[UPnP ポートフォワーディング]のチェックを外し、[適用]をクリックします。

## 02 | myQNAPcloud Link アクセス制御

myQNAPcloud Link は、QNAP が提供するセキュア接続クラウドサービスです。ユーザーは、自身の QNAP NAS を自分で選んだ myQNAPcloud デバイス名で接続できます。myQNAPcloud Link は、アクセス制御設定を提供します。アクセス制御が「パブリック」に設定されている場合、デバイス名を知っている人は誰でも myQNAPcloud Link を使用して NAS に接続できます。そのため、**アクセス制御は「パブリック」または「カスタマイズ」に設定することをお勧めします**。いずれのモードでも、myQNAPcloud Link を使用できるようになる前に、ユーザーはクラウドサービスに安全に接続するために、アクセス許可リスト内にある自分の QNAP ID にログインする必要があります。

★ Q TS 4.5.0 / Qu TS hero h4.5.3 (またはそれ以降) でデフォルト設定は、「カスタマイズ」です。

1. 管理者アカウントで、QTS / QuTS hero Web 管理インターフェイスにログイン
2. 管理インターフェイスの左上隅にあるメニューをクリック、[myQNAPcloud]をクリック
3. 左側メニューの[アクセス制御]をクリック
4. 「アクセス制御」設定ページで、[デバイスアクセス制御]を[プライベート]または[カスタマイズ]に設定し、[適用]をクリックします。



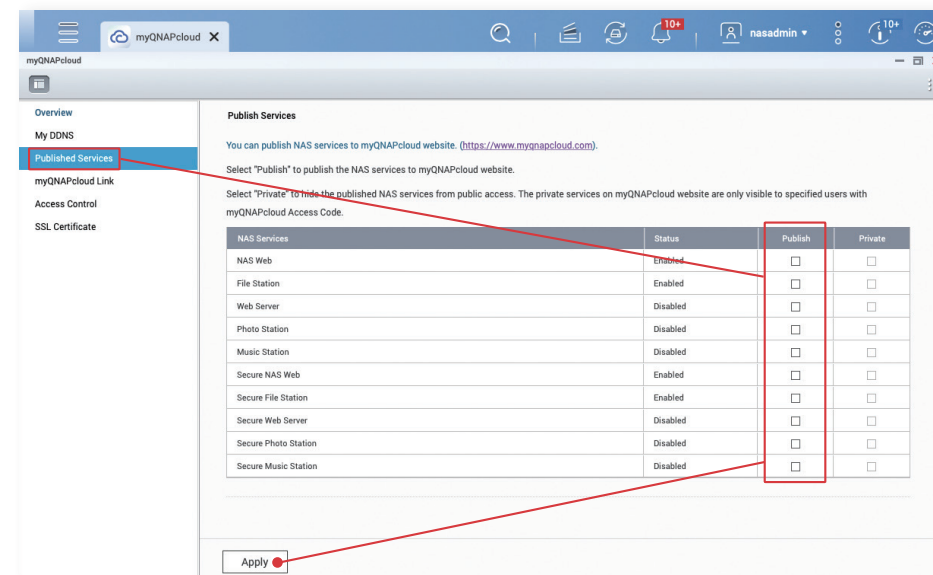
## 03 | 公開サービス

公開サービスは、ユーザーが myQNAPcloud Web サイトにある関連機能を使いやすくしますが、セキュリティリスクも増加します。この機能を使う必要がなければ、無効にしてセキュリティを高めておくことをお勧めします。

★ この機能は、QTS 4.5.0 / QuTS hero h4.5.3 以降からはデフォルトで無効になっています

### 「公開サービス」機能：

1. 管理者アカウントで、QTS / QuTS hero Web 管理インターフェイスにログイン
2. 管理インターフェイスの左上隅にあるメニューをクリック、[myQNAPcloud]をクリック
3. 左側メニューの[公開サービス]をクリック
4. [公開]フィールドで、すべてのチェックを外し、[適用]をクリックします。



# ネットワーク設定チェックリスト

## ハードウェア関連

- ☐ NAS がルーターの背後に接続されている
- ☐ NAS がイントラネットの IP アドレスを取得している

## ルーター

- ☐ ルーターの「DMZ」機能を無効にしている
- ☐ ルーターの「ポートフォワーディング」ルールを無効にしている
- ☐ ルーターの「UPnP」機能を無効にしている

## NAS:

- ☐ NAS の「自動ルーター構成 UPnP ポートフォワーディング」機能を無効にしている
- ☐ NAS の「myQNAPcloud Link アクセス制御」を[プライベート]または[カスタマイズ]に設定している
- ☐ 「公開サービス」機能を無効にしている

上記の設定を確認し、適用した後は、QNAP NAS はインターネットから見えなくなり、ハッカーによって攻撃されるリスクが大きく減少します。QNAP NAS を強化するために、残りの設定を読み、確認してください。

インターネット越しに NAS にアクセスする必要がある場合は、以下の 3 つのセキュアな方法を検討できます。



myQNAPcloud Link



詳細



QVPN Service



詳細



QuWAN SD-WAN



詳細

# 02

## NAS セキュリティ設定ガイド



# NAS セキュリティ設定



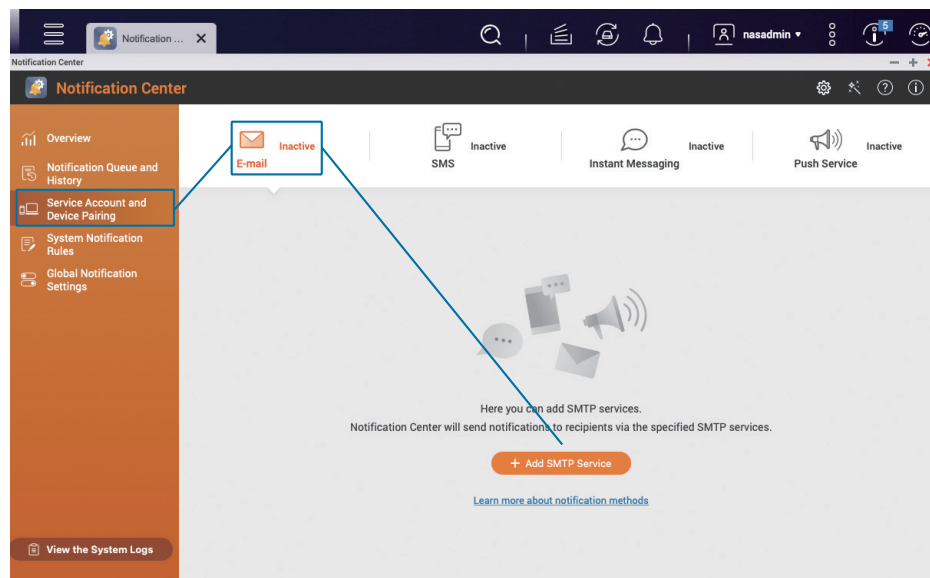
# システム通知の設定

内蔵の通知センターは、設定に応じてプッシュ通知が行なえ、ユーザーは NAS ステータスを常に注意を払い、異常が検出されたらすぐに対応できます。

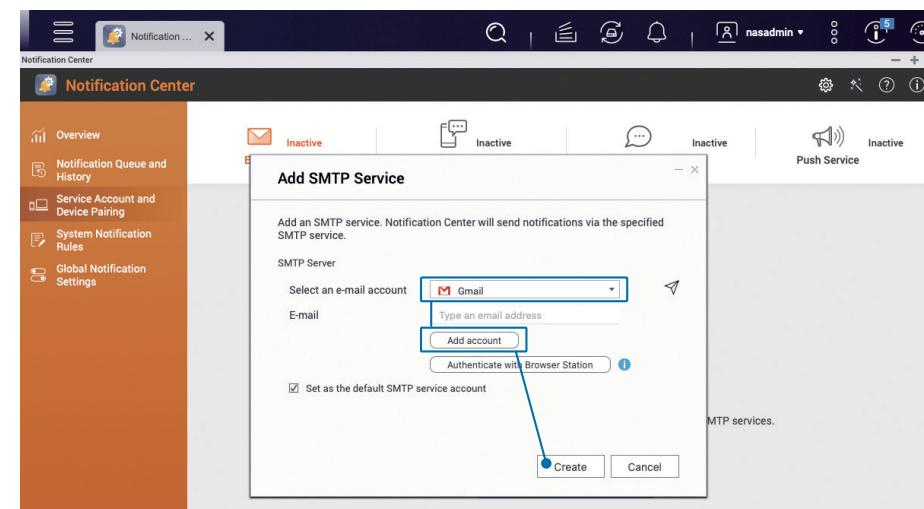
次のチュートリアルでは、「警告通知」と「ファームウェア更新」を送信するために、メール用の 2 つの基本ルールを作成し、必要があればさらにルールを追加する方法を説明します。

## 01 | 「メール」通知方法の追加

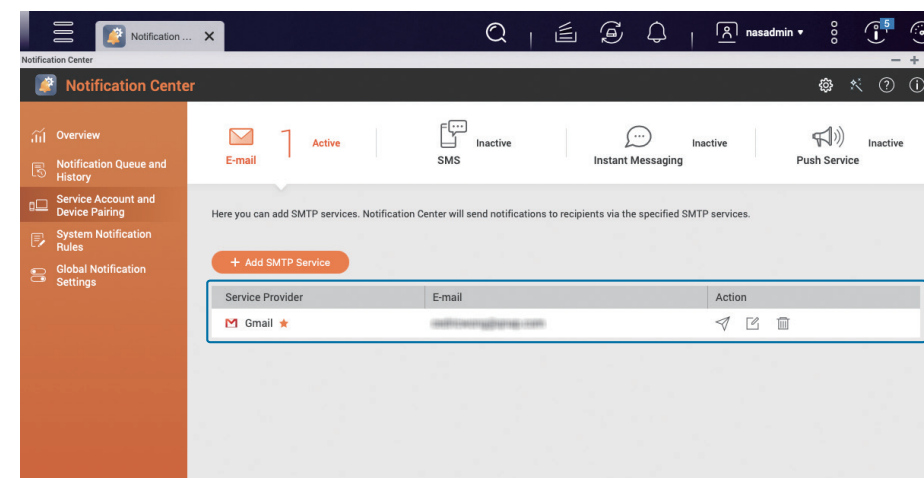
[通知センター]を開き、左側メニューの[サービスアカウントとデバイスのペアリング]をクリックし、[メール]を選択してから、[SMTP サービスの追加]をクリックします。



メールアカウントを選択し (ここでは例として Gmail を使用) 。[アカウントの追加]をクリックし、指示に沿って Gmail の確認プロセスを完了させ、検証完了後に[作成]をクリックします。



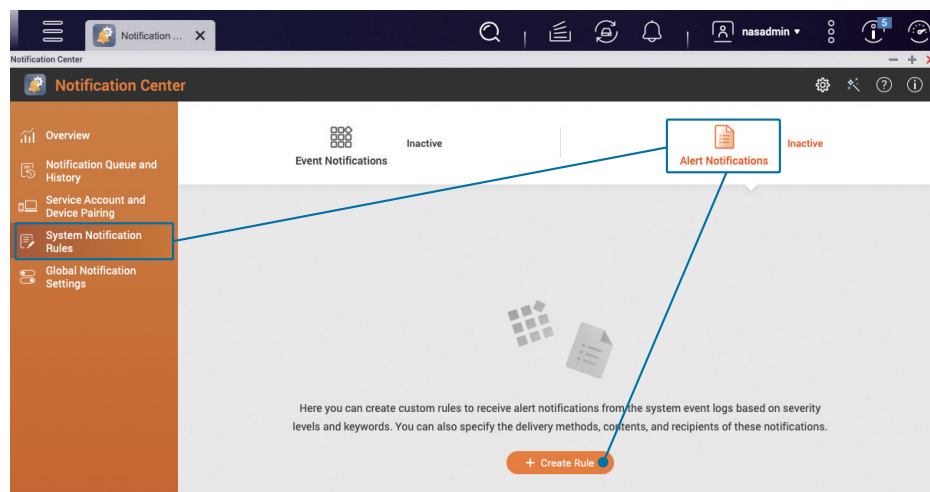
⇓ 作成が終わると、追加したメールアカウントがリストに現れます。



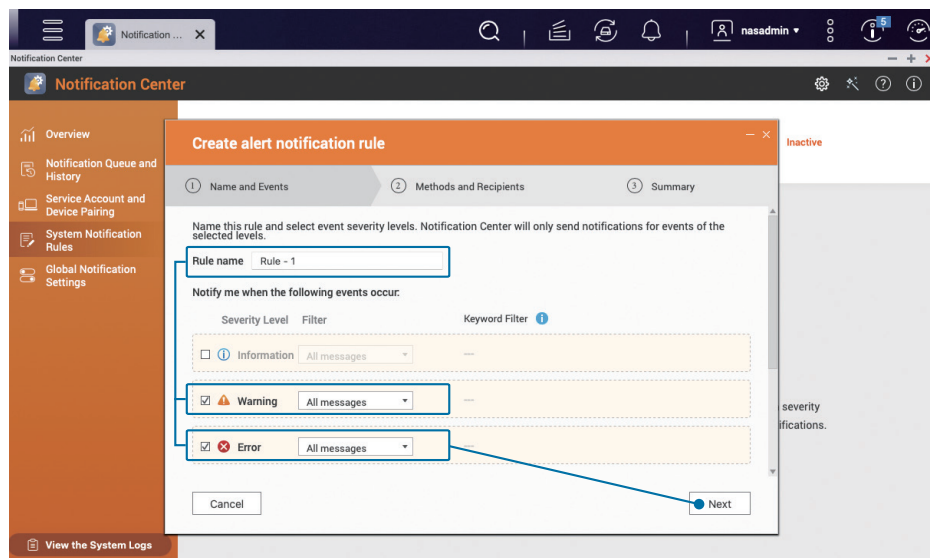


## 02 「警告通知」の設定

「通知センター」の左側メニューで、[システム通知ルール] をクリックし、[警告通知] を選んで [ルールを作成] をクリックします。

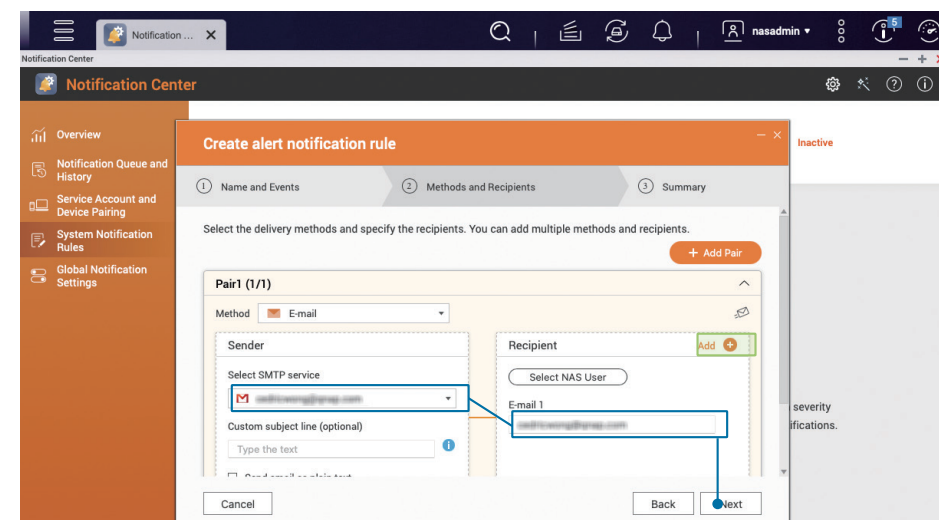


ニーズに応じて「ルール名」を変更し、[警告] と [エラー] の2つの重大度レベルにチェックを入れ、[次へ] をクリックします。

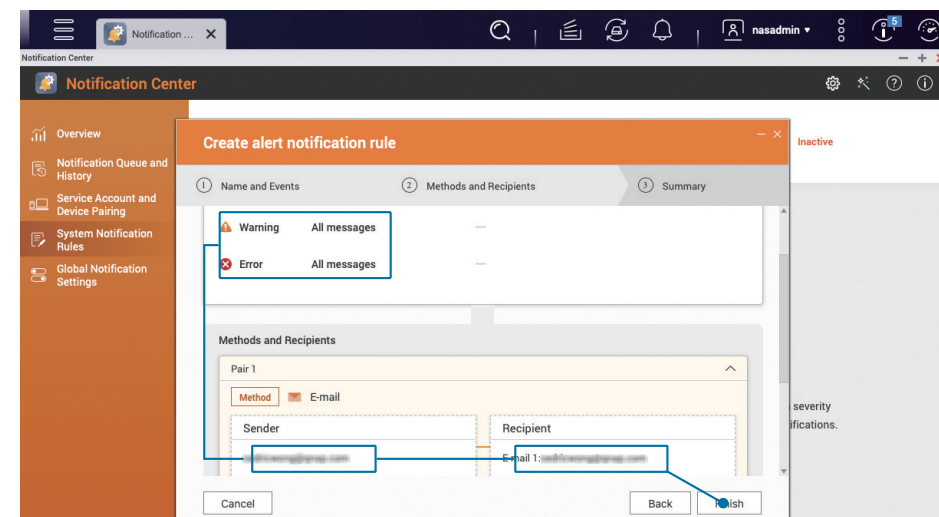


配信方法をセットし、受信者をセット、ペアリングで[送信者]として追加したメールアカウントを選択してから、[受信者]の[メールアドレス]を入力し、[次へ]をクリックします。

必要であれば、[受信者]の横の[追加 +] をクリックして複数の受信者を入力できます。[ペアの追加] で、複数の方法で通知を同時に送信させることもできます。



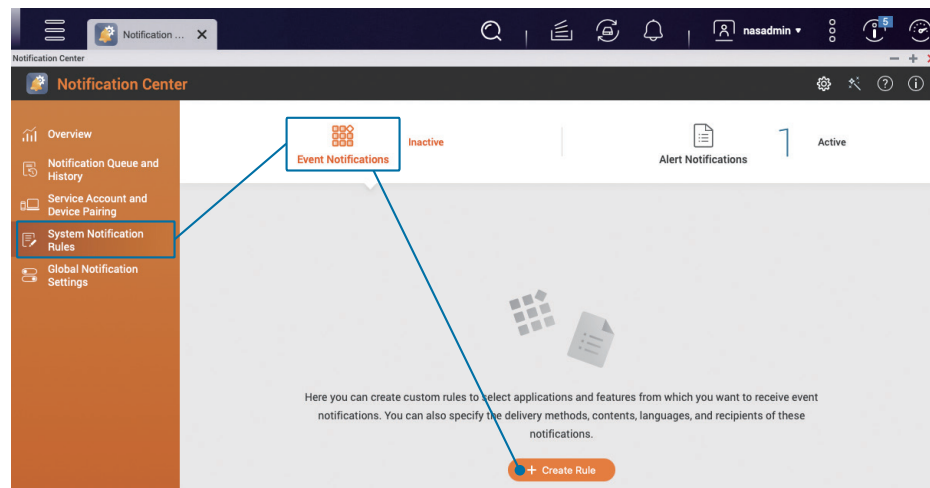
設定が正しいことを確認した後、[終了] をクリックして「警告通知」設定が完了です。



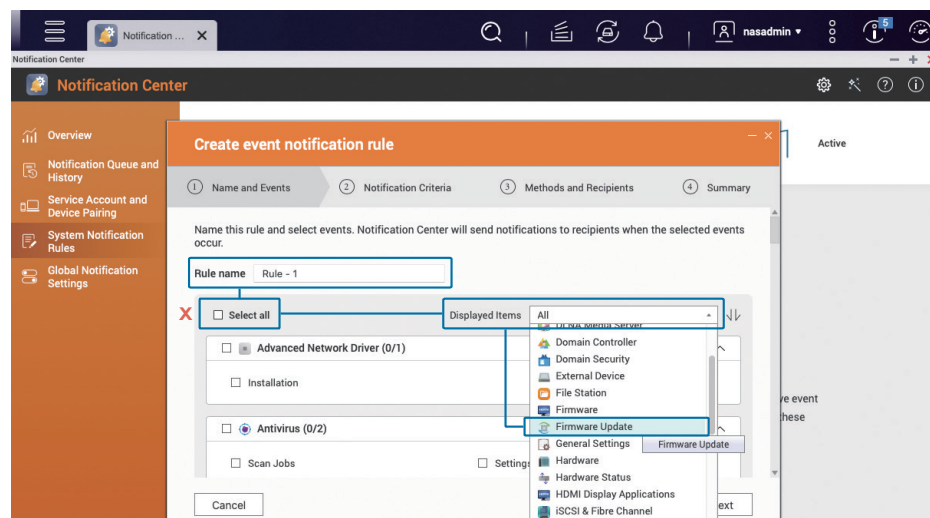


### 03 | 「ファームウェア更新」通知の設定

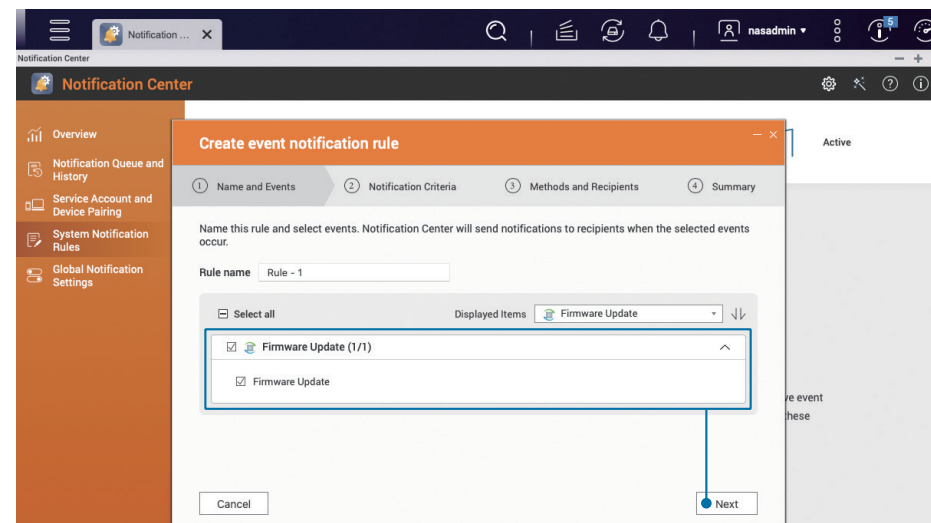
「通知センター」の左側メニューで、[システム通知ルール]をクリックし、[イベント通知]を選択してから、[ルールを作成]をクリックします。



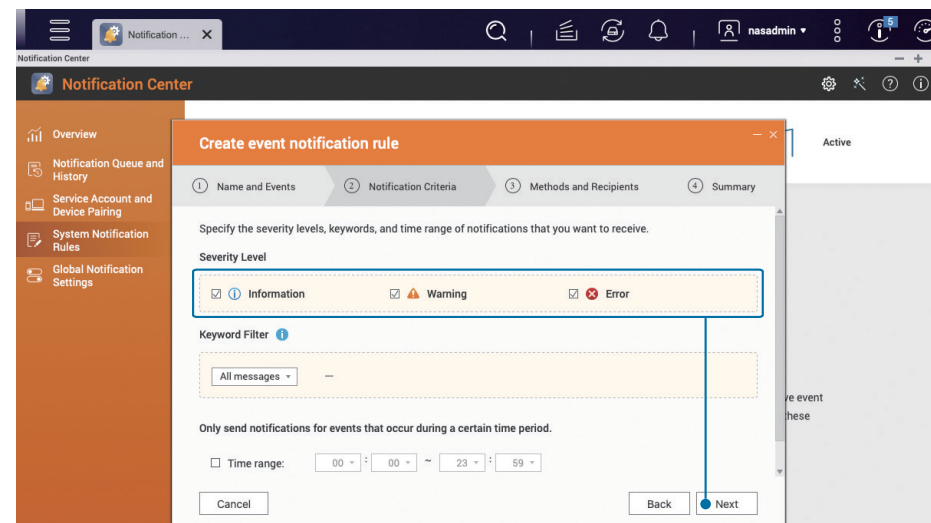
必要に応じて[ルール名]を変更し、[すべてを選択]のチェックを外してから、左側の[表示されたアイテム]にある[ファームウェア更新]を選んでから、下の[ファームウェア更新]を選択します。



[ファームウェア更新]オプションにチェックを入れ、[次へ]をクリックします。



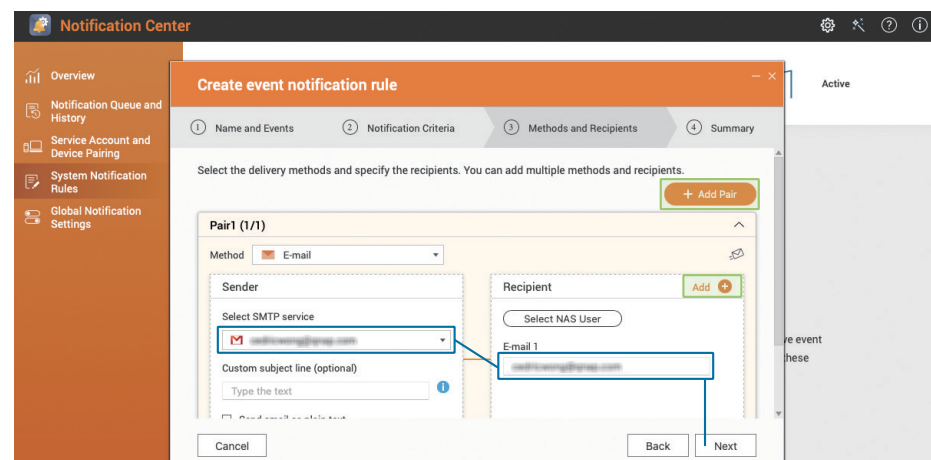
[情報]、[警告]、[エラー]を含むすべての重大度レベルをチェックし、[次へ]をクリックします。



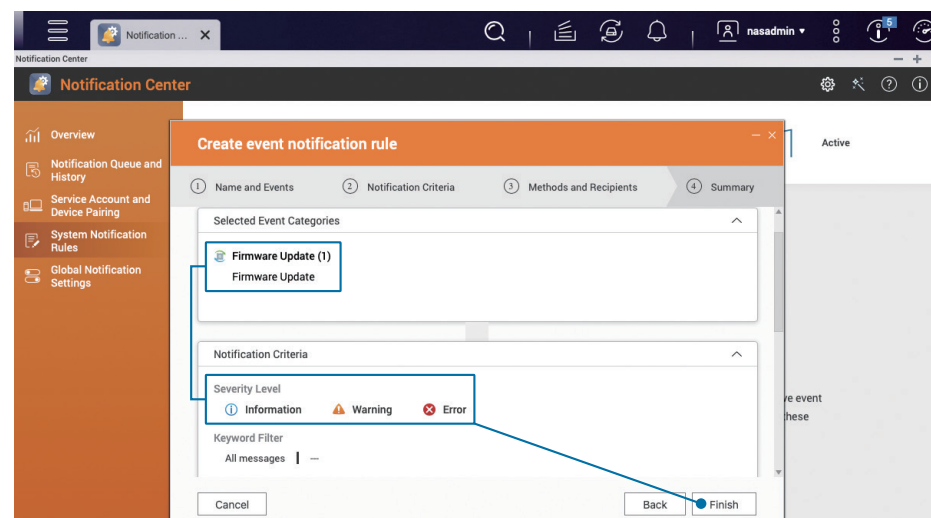
# ファームウェア (QTS / QuTS hero) の自動更新を有効にする

配信方法をセットし、受信者をセットします。[メール]通知だけが設定されているため、ペアリングで[送信者]として追加したメールアカウントを選択し、[受信者]の[メールアドレス]を入力してから、[次へ]をクリックします。

必要であれば、[受信者]の横の[追加 +]をクリックして複数の受信者を入力できます。[ペアの追加]で、複数の方法で通知を同時に送信させることもできます。

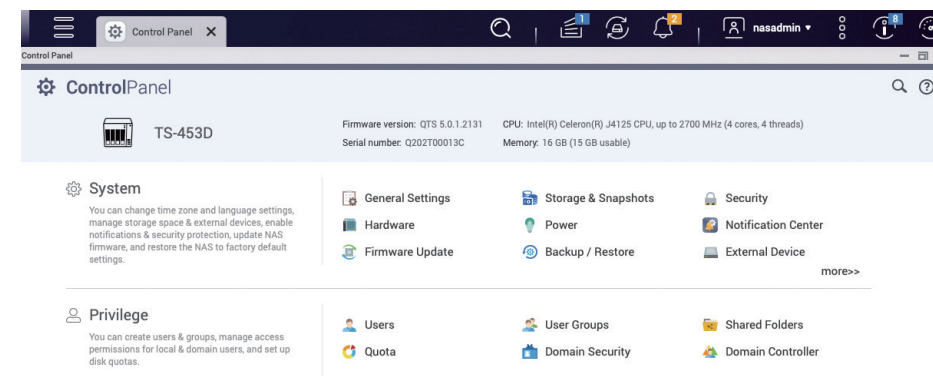


設定が正しいことを確認した後、[終了]をクリックして「ファームウェア更新」の設定が完了です。



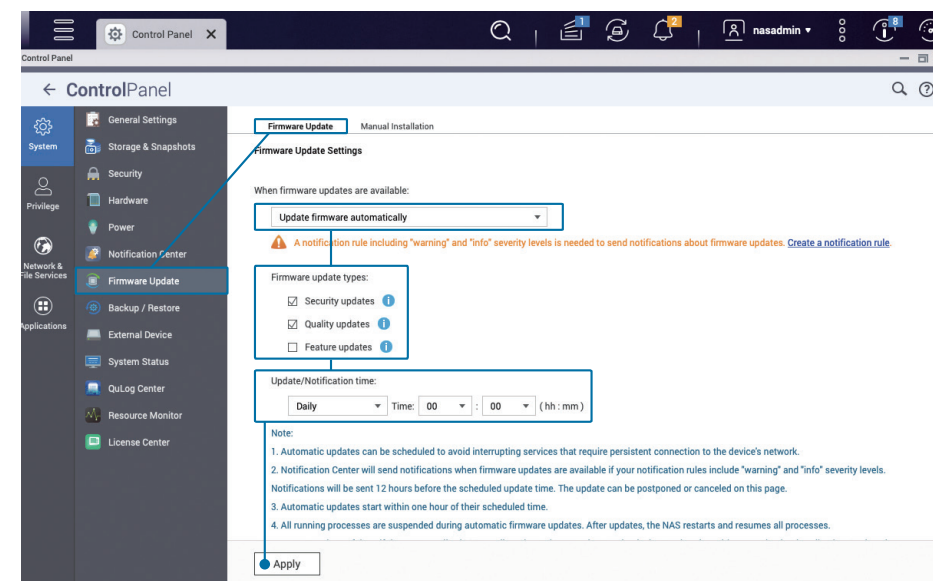
自動更新機能により、新機能やバグ修正、脆弱性に対する更新をより容易にインストールできるようになります。

[コントロールパネル]を開き、[ファームウェア更新]をクリックします。




[ファームウェア更新設定]で、[ファームウェアの自動更新]を選択し、[セキュリティ更新]と[品質更新]にチェックを入れます。[更新 / 通知時間]は、「00 : 00」などのオフピーク時間を設定するようにしてから、[適用]をクリックします。

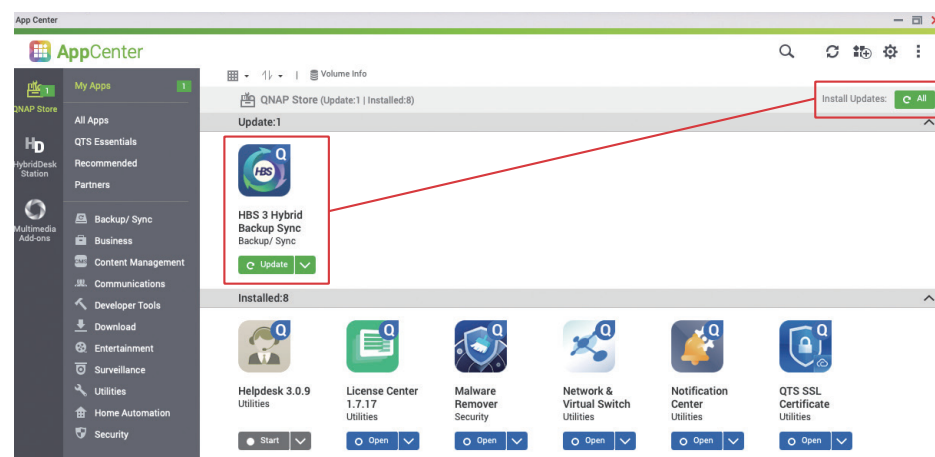
★ QTS 5.0.0 / QuTS hero h5.0.0 (またはそれ以前) に対しては、「自動更新」ページの「推奨バージョン」をご確認ください。



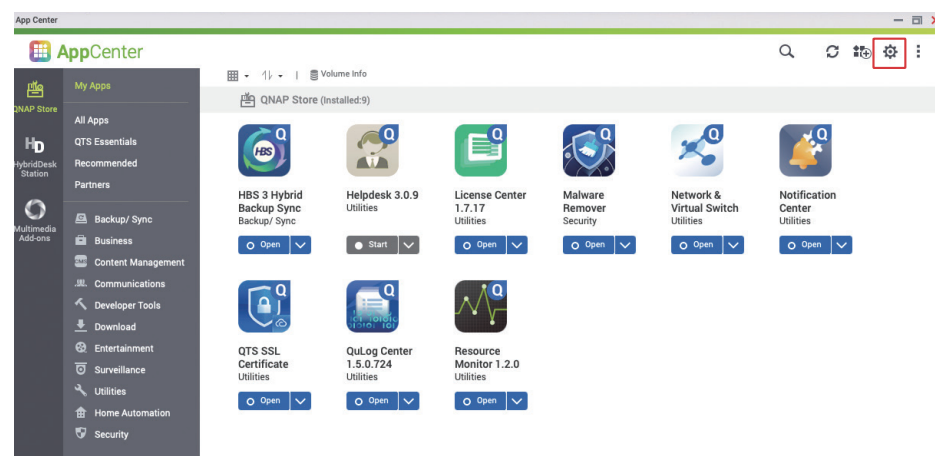
# アプリの更新設定

App Center は、より多くの機能を QNAP NAS に追加するために複数のアプリを提供しますが、それらのアプリに対しても、アプリの機能を強化し、問題や脆弱性を解消し、ユーザー体験を向上させるための更新が必要です。

[App Center] を開いて、更新が必要なアプリがあるかどうかを確認します。もしあれば、右上の[すべて]  ボタンをクリックしてすべてのアプリを更新します。

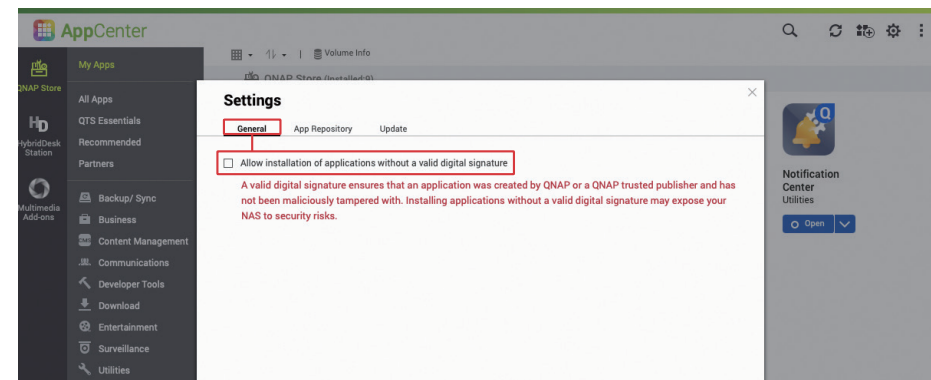


更新完了後、右上隅にある[設定]  アイコンをクリックして、App Center の設定ページにはいります。



QNAP または QNAP が信頼する開発者は、それが本物であることを確認するためにデジタル署名を追加します。セキュリティを高めるために、[正しいデジタル署名なしでのアプリケーションを許可する]のチェックは外すことをお勧めします。

★ デフォルトではこのチェックは外れており、正しいデジタル署名なしではアプリをインストールできないようになっています

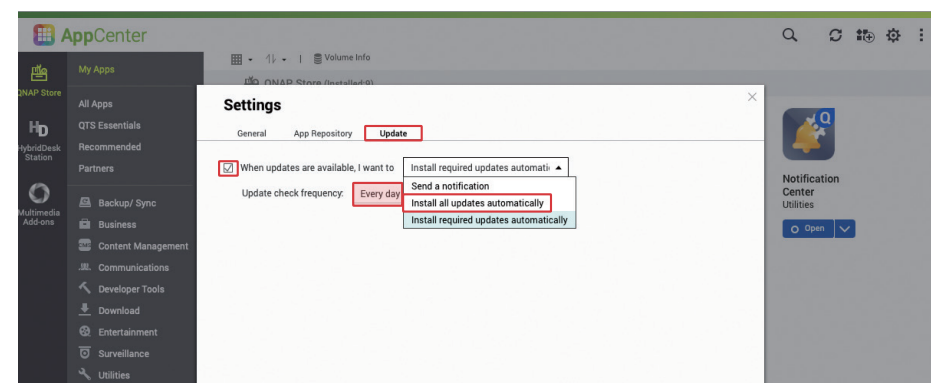


[更新]タブをクリックし、特別な必要がなければ、[すべての更新を自動的にインストールする]を選択し、周期を[毎日]に設定し、[適用]をクリックして設定を完了します。

⇒[必須の更新]は主に、アプリとファームウェアの依存関係を保つために使われ、[重大な脆弱性の更新]も含まれます。

⇒[すべての更新]には、あらゆる機能改善、バグ修正、すべての脆弱性パッチが含まれます。更新頻度は短くなります。

★ デフォルトは、[すべての更新を自動的にインストール]です



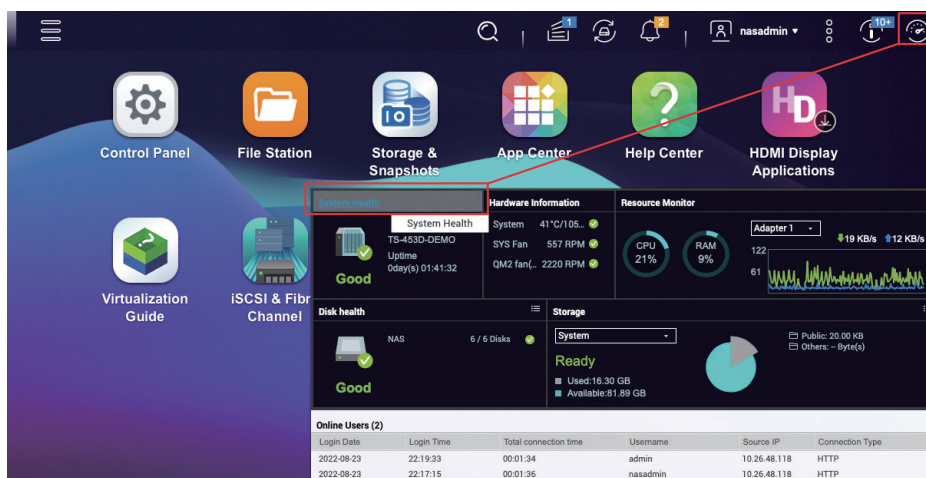


# 不要な機能の無効化や削除

QNAP NAS はさまざまな機能とアプリを提供していますが、多くの機能を有効にするほど、潜在的な攻撃ベクトルが増えます。セキュリティを高め、システムがスムーズに動作するよう、定期的に不要な機能をチェックし、無効に（あるいは削除）するようにしてください。

★ 製品のセキュリティを強化するために、QTS 5.0.0 / QuTS hero h5.0.0 以降では、必須でない機能はシステム初期化時にデフォルトで無効化されるようになり、App Center は必須でないアプリをデフォルトでインストールしないようになりました。システムが、QTS 5.0.0 / QuTS hero h5.0.0 にアップデートする前に初期化された場合は、インストールされているアプリを確認してください。

右上隅の「😊」ボタンをクリックしてシステム「ダッシュボード」を開き、[システム健全性]をクリックして[システムステータス]ウィンドウを開きます。



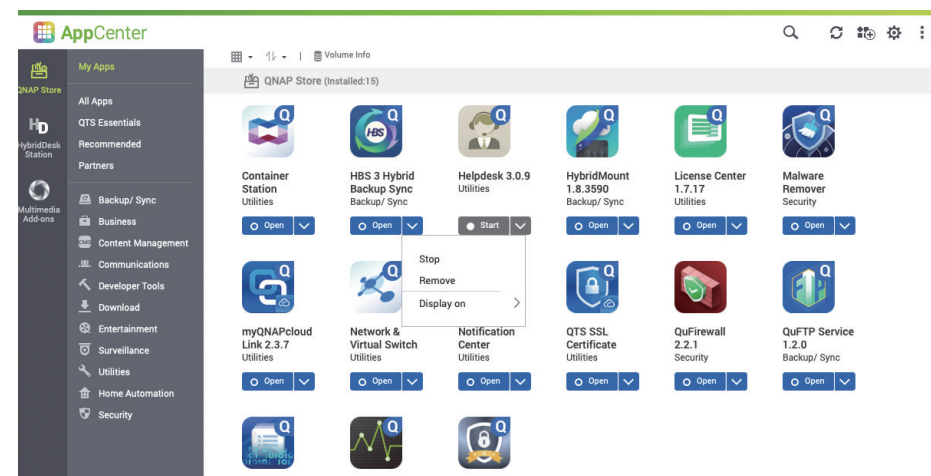
[システムサービス]をクリックし、有効なシステム機能を表示します。コントロールパネルに進み、不要なシステム機能を無効にします。

System Status

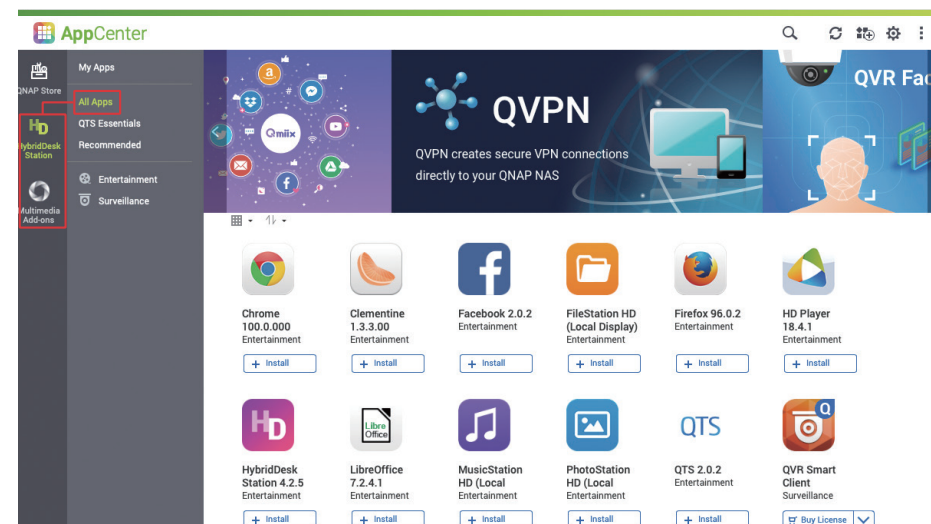
System Information   Network Status   **System Service**   Hardware Information

Service	Status	Port	Description
Antivirus	Disabled	-	
Apple Networking	Disabled	-	
DDNS Service	Disabled	-	
Disk Management	Disabled	3260	
Domain Controller	Disabled	-	
FTP Service	Disabled	21	Maximum connections:30
LDAP Server	Disabled	-	
Microsoft Networking	Enabled	-	Server type :Standalone server Workgroup:WORKGROUP Enable WINS server:Disabled

システム組み込み機能に加え、App Center に何がインストールされているかをチェックする必要もあります。



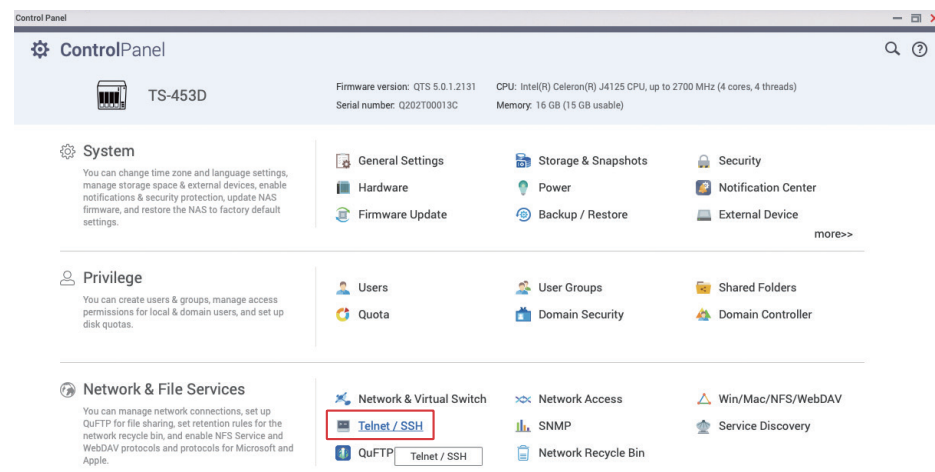
左側端で、[HybridDesk Station]と[マルチメディア アドオン]をクリックし、対応するアプリの状態を見ます。



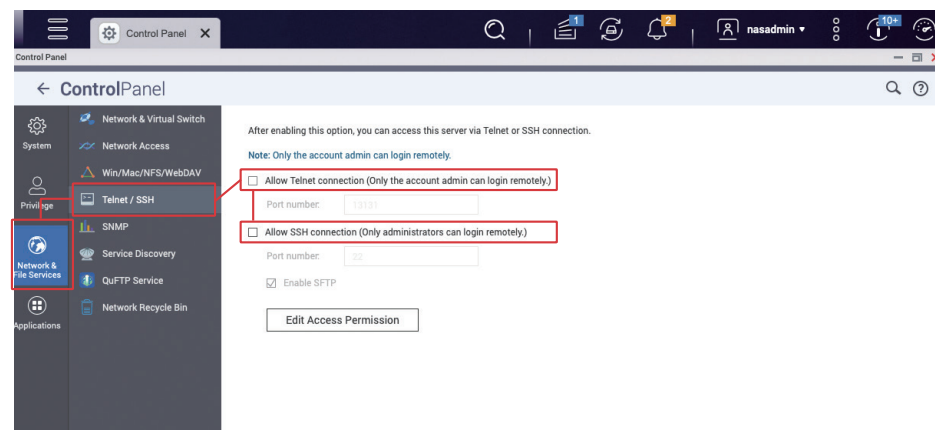
# Telnet / SSH の無効化

使用していないのであれば、**Telnet および SSH** は無効にすることを強くお勧めします。これら 2 つの機能は一般的に、システムの保守のために QNAP カスタマーサービスや IT の専門家によって使われています。一般の利用者は不要ですので、無効にすることをお勧めします。

[コントロールパネル]を開き、[Telnet/SSH]をクリックします。



[Telnet 接続を許可する]と[SSH 接続を許可する]のチェックを外し、[適用]をクリックします。

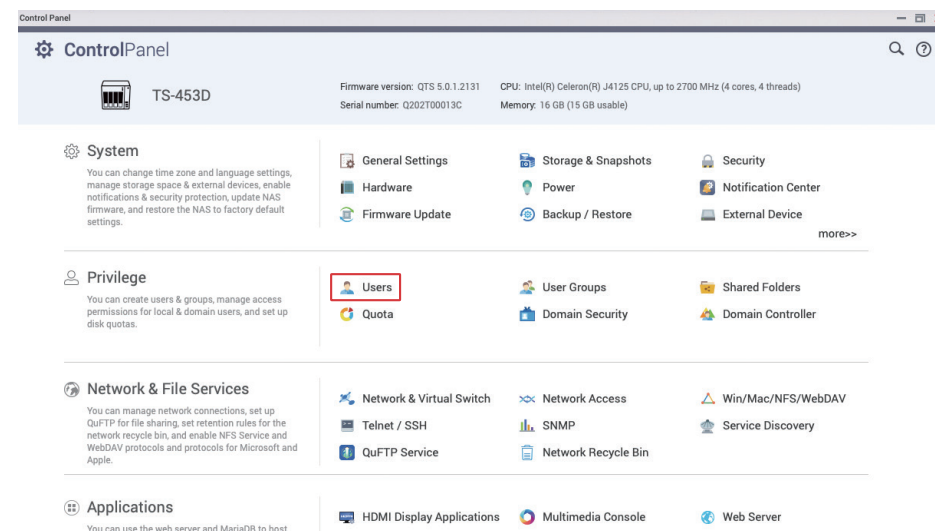


# システムアカウントセキュリティの強化

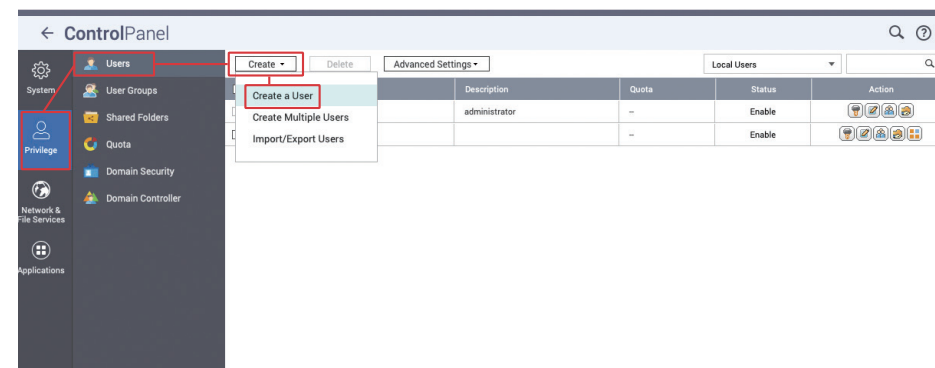
## デフォルトの管理者アカウント「admin」の無効化

総当たり攻撃によりパスワード破りを行うハッカーは通常、デフォルトの管理者アカウント「admin」を狙います。システムが QTS 4.5.4 / QuTS hero h4.5.4 (またはそれ以前) で初期化された場合、デフォルトの管理者アカウント「admin」はアクティブになります。以下の手順で新しい管理者アカウントを作り、「admin」アカウントを無効にしてください。

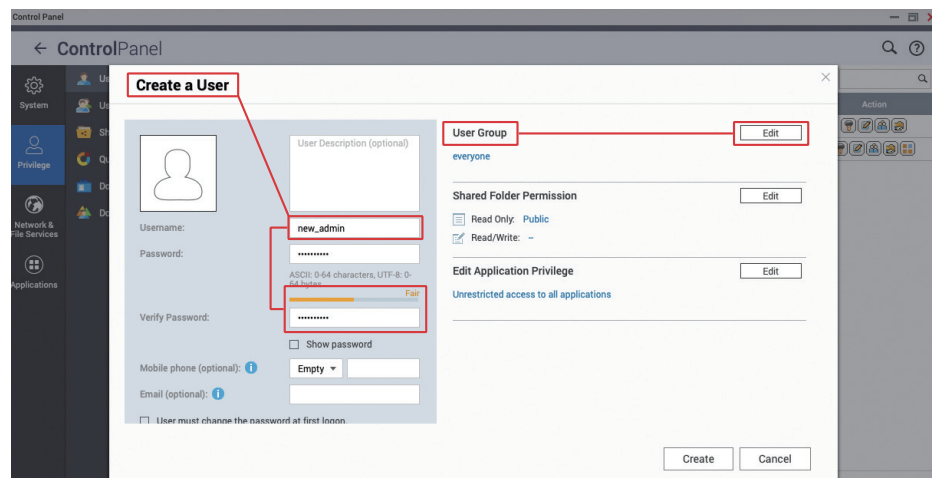
[コントロールパネル]を開き、[ユーザー]をクリックします。



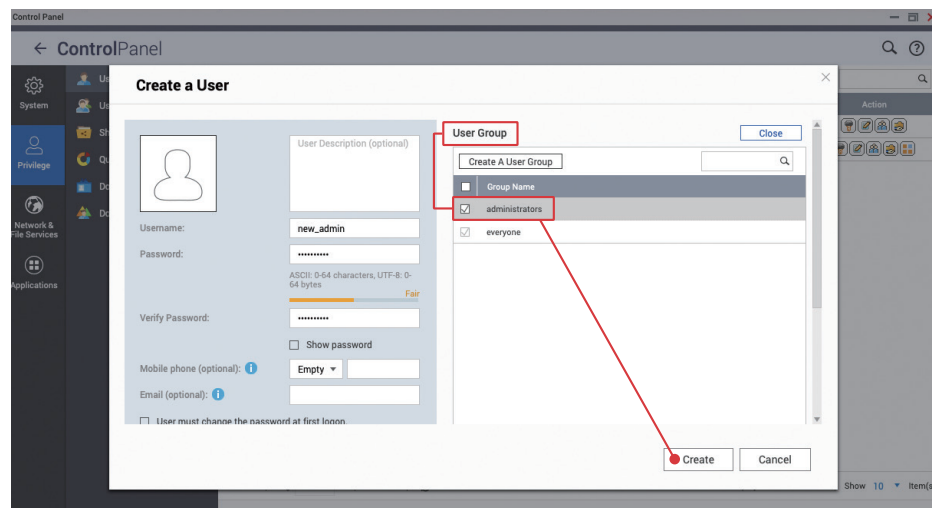
[作成] > [ユーザーの作成]をクリックします。



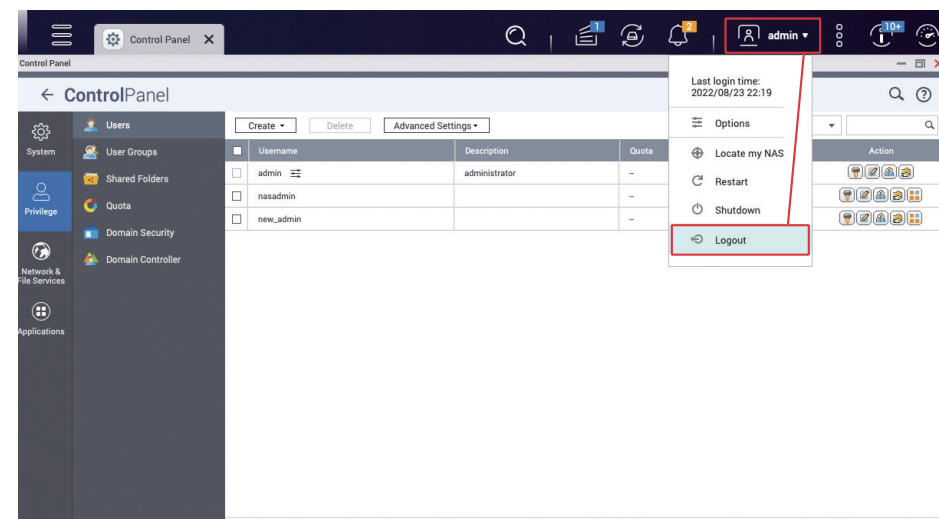
管理者アカウントのユーザー名 (たとえば「new\_admin」など) を入力し、強力なパスワードを設定します。



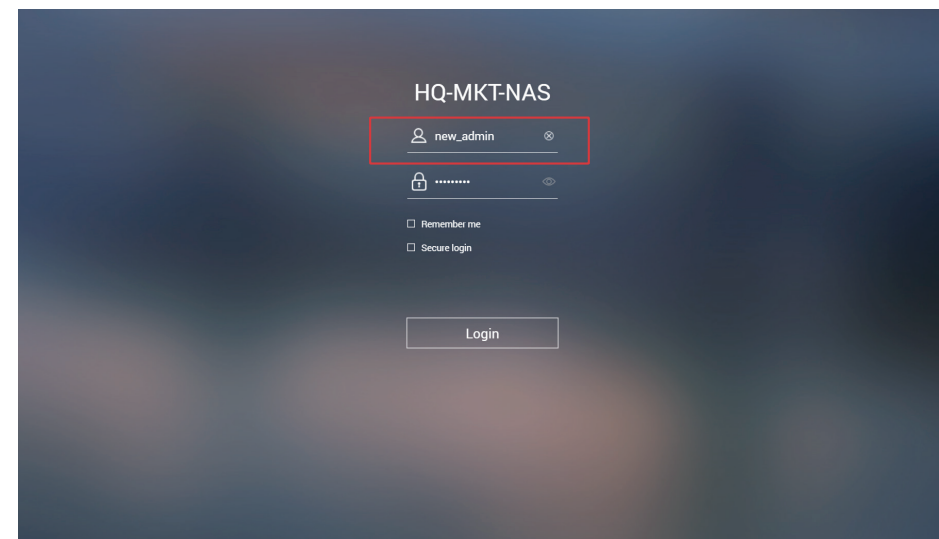
[ユーザーグループ] セクションで、[編集] をクリックし、[管理者] グループであることを確認してから、[作成] をクリックして新しいユーザーを追加します。



一番上で [admin] をクリックしてメニューを開き、[ログアウト] をクリックして QTS Web 管理インターフェイスからログアウトします。

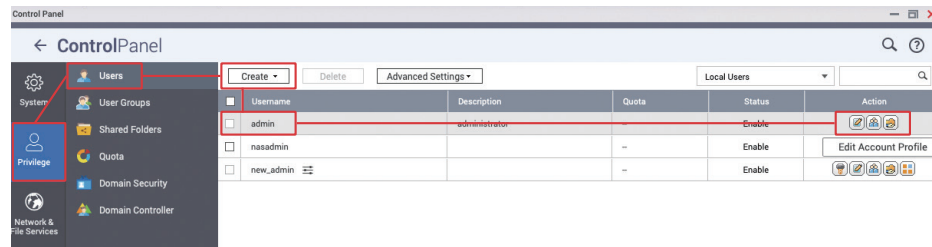


作成した [管理者アカウント] を使用して、QTS Web 管理インターフェイスにログインします。

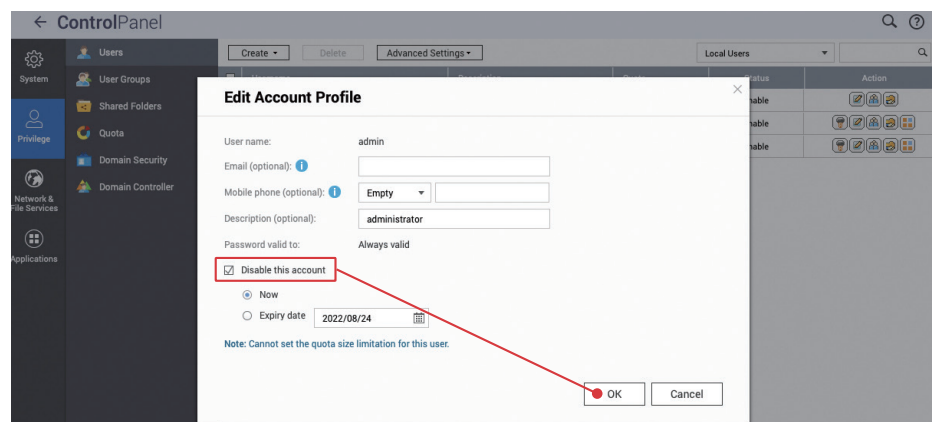


# パスワードポリシーの設定

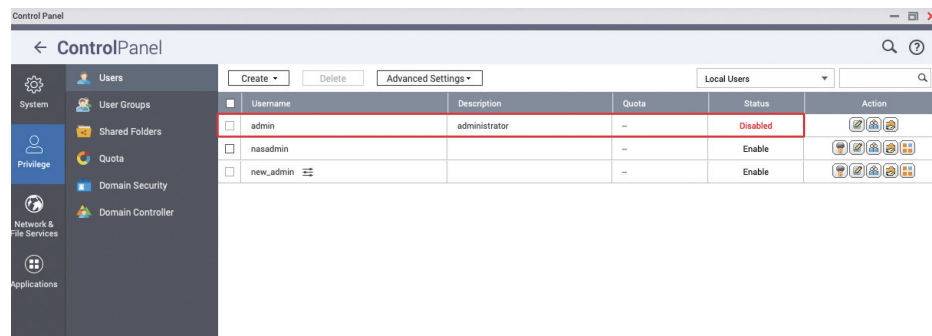
再度[コントロールパネル]を開き、[ユーザー]をクリックし、[admin]行で[アカウントプロファイルの編集]をクリックします。



[このアカウントを無効にする]にチェックを入れ、[OK]を押して終了します

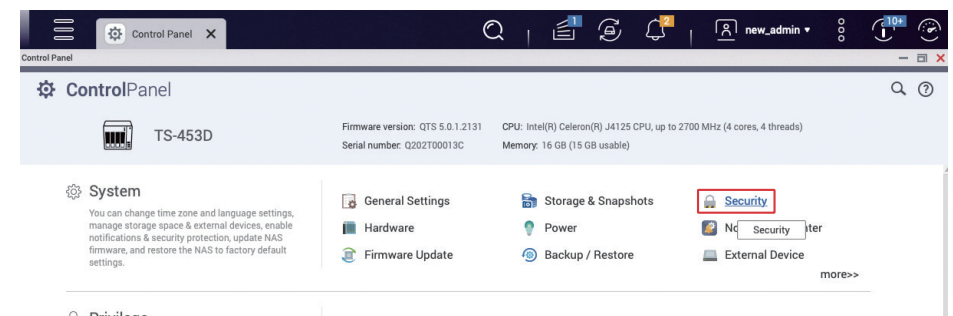


完了後、「admin」のステータスが「無効」になっています。

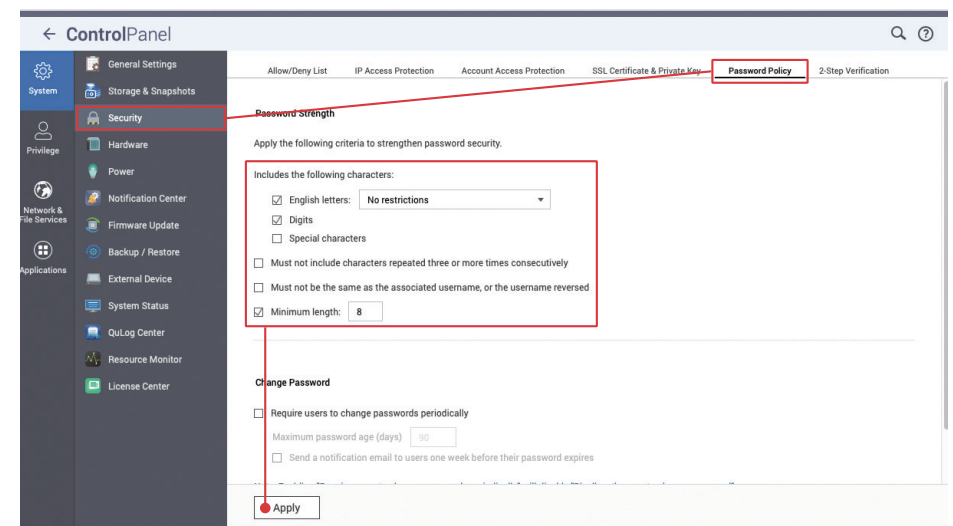


デフォルトの管理者アカウント「admin」の無効化に加え、すべてのアカウントに強力なパスワードがついていることも必ず確認してください。[アクセス保護]をつけることで、悪意のあるログイン試行のブロックに役立ちます。さらにセキュリティを高めるために、すべてのアカウントに対し「2段階認証 (2SV)」を必須にし、パスワードクラッキングや悪意のあるログインを防止します。

[コントロールパネル]を開き、[セキュリティ設定]をクリックします。



[パスワードポリシー]をクリックして設定ページにはいります。システムが QTS 5.0.0 / QuTS hero h5.0.0 (またはそれそれ以降) で初期化された場合、基本的なパスワード強度の状態はデフォルトで有効になっています。ニーズに応じて強力なパスワード条件を設定できます。パスワードには、「大文字と小文字の英字」と「数字」を含むことができ、パスワード長は少なくとも「10文字」で、完了後に[適用]をクリックします。





# アクセス保護の有効化 (IP / アカウント)

「IP アクセス保護」と「アカウントアクセス保護」は、総当たり攻撃によってパスワードが盗まれることの防止に役立ちます。特定の IP またはアカウントでのログインが何度も失敗している場合、IP のブロックやアカウントの無効化が起動され、攻撃者が何度もパスワードを試すのを防止します。

[IP アクセス保護]をクリックして設定ページにはいり、全サービスにチェックを入れ、必要に応じて[時間間隔]、[ログイン失敗回数]、[IP ブロック長]をセットし、[適用]をクリックして設定を完了します。

Allow/Deny List **IP Access Protection** Account Access Protection SSL Certificate & Private Key Password Policy 2-Step Verification

Automatically block client IP addresses after too many failed login attempts within the specified time period. You can view blocked IP addresses in [QuFirewall](#).

Service	Time interval	Failed login attempts	IP block length
<input checked="" type="checkbox"/> SSH	1 minute(s)	5	5 minutes
<input checked="" type="checkbox"/> Telnet	1 minute(s)	5	5 minutes
<input checked="" type="checkbox"/> HTTP(S)	1 minute(s)	5	IP
<input checked="" type="checkbox"/> FTP	1 minute(s)	5	IP
<input checked="" type="checkbox"/> SAMBA	1 minute(s)	5	IP
<input checked="" type="checkbox"/> AFP	1 minute(s)	5	IP
<input checked="" type="checkbox"/> RTTR	1 minute(s)	5	IP
<input checked="" type="checkbox"/> Rsync	1 minute(s)	5	IP

**★ 一般ユーザーの IP アドレスが誤ってブロックされてしまった場合は、次のようにブロックリストを調整できます。**

- 別のコンピュータから、QTS / QuTS hero の管理インターフェイスにログイン
- IP アドレスを変更し、QTS / QuTS hero の管理インターフェイスにログイン
- モバイルブラウザで、QTS / QuTS hero の管理インターフェイスにログイン
- QManager アプリを利用

**Apply**

[アカウント アクセス保護]をクリックして設定ページにはいり、関連するサービスにチェックを入れ、必要に応じて「時間間隔」、「ログイン失敗回数」をセットし、[適用]をクリックして設定を完了します。

Allow/Deny List IP Access Protection **Account Access Protection** SSL Certificate & Private Key Password Policy 2-Step Verification

Disable accounts automatically when they fail too many login attempts within a specified time period. You can view the disabled accounts in [Users](#).

Users: All users not in the administrators group

Service	Time interval	Failed login attempts
<input type="checkbox"/> SSH	5 minute(s)	5
<input type="checkbox"/> Telnet	5 minute(s)	5
<input type="checkbox"/> HTTP(S)	5 minute(s)	5
<input type="checkbox"/> FTP	5 minute(s)	5
<input type="checkbox"/> SAMBA	5 minute(s)	5
<input type="checkbox"/> AFP	5 minute(s)	5
<input type="checkbox"/> RTTR	5 minute(s)	5
<input type="checkbox"/> Rsync	5 minute(s)	5

**★ 管理者アカウントに対して[アカウントアクセス保護]が有効になっている場合、パスワードクラッキング攻撃によってすべての管理者アカウントが無効になる可能性があります。その場合、リセット機能で再度有効化できるのは[admin]アカウントだけで、[admin]アカウントのパスワードもリセットされます。リセット後にパスワードを変更することを忘れずに。**

**Apply**

# 2 段階認証 (2SV) の有効化

[2 段階認証]をクリックして設定ページにはいり、「ユーザー」や「ユーザーグループ」に対し 2 段階認証 (2SV) の利用を必須とすることができます。[管理者グループ]のアカウントに対しては、2SV を有効にすることを強くお勧めします。その他のアカウントに対しては、リスクを勘案し、適切な設定を適用してください。

[ローカルユーザー]をクリックして、メニューを開き、[ローカルグループ]を選択します。

Control Panel

← ControlPanel

Allow/Deny List IP Access Protection Account Access Protection SSL Certificate & Private Key Password Policy **2-Step Verification**

**2-Step Verification**

2-Step Verification (2SV) adds an extra layer of protection to a user's account by requiring an additional one-time security code whenever a user signs in to your NAS. You can enforce 2-step verification for specific users and groups.

Note: The configuration of "Enforce 2SV" between the group and users in the group may not be consistent. See "Status" to check the final 2SV status of users.

Enforce 2SV	Username	Description
<input type="checkbox"/>	admin	administrator
<input type="checkbox"/>	nasadmin	
<input type="checkbox"/>	new_admin	

Local Users

Local Users

Local Users

Domain Users

Domain Groups

Disabled

[管理者]で[2SVを強制する]にチェックを入れ、[適用]をクリックして設定を完了します。

← ControlPanel

Allow/Deny List IP Access Protection Account Access Protection SSL Certificate & Private Key Password Policy **2-Step Verification**

**2-Step Verification**

2-Step Verification (2SV) adds an extra layer of protection to a user's account by requiring an additional one-time security code whenever a user signs in to your NAS. You can enforce 2-step verification for specific users and groups.

Note: The configuration of "Enforce 2SV" between the group and users in the group may not be consistent. See "Status" to check the final 2SV status of users.

Enforce 2SV	Group Name	Description	Status
<input checked="" type="checkbox"/>	administrators		--
<input type="checkbox"/>	everyone		--

Local Groups

Page 1 / 1

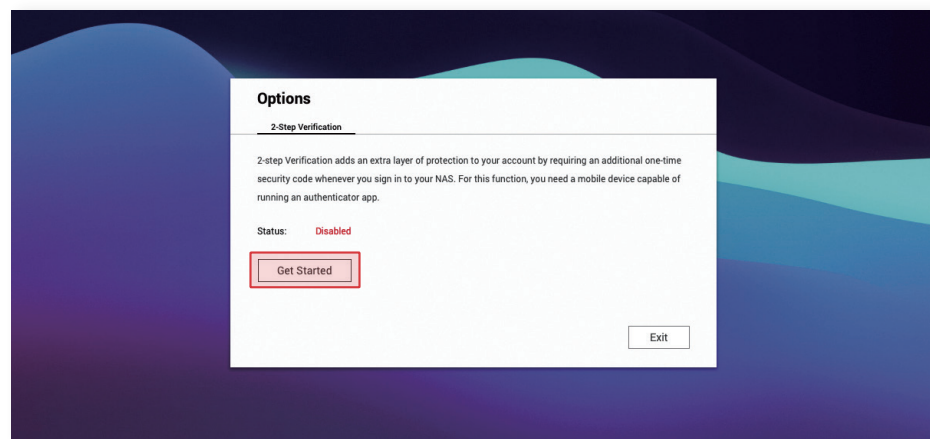
Display item: 1-2, Total: 2 | Show 10 | Item(s)

**Apply**

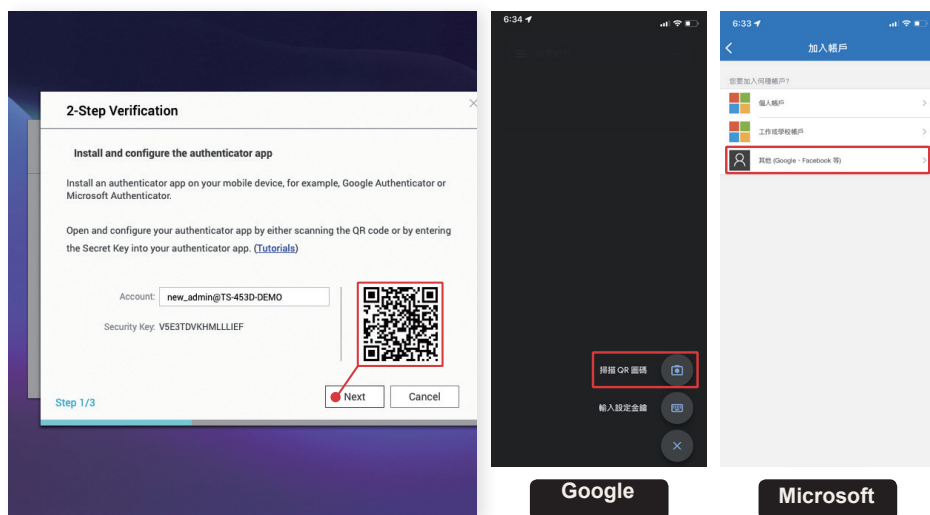


[2SVを強制する]を有効にした後、[管理者]アカウントで[2段階認証(2SV)]が有効化されていない場合、次のログイン時に強制的に「2段階認証(2SV)」設定ページに飛び、アカウントを設定するよう求められます。

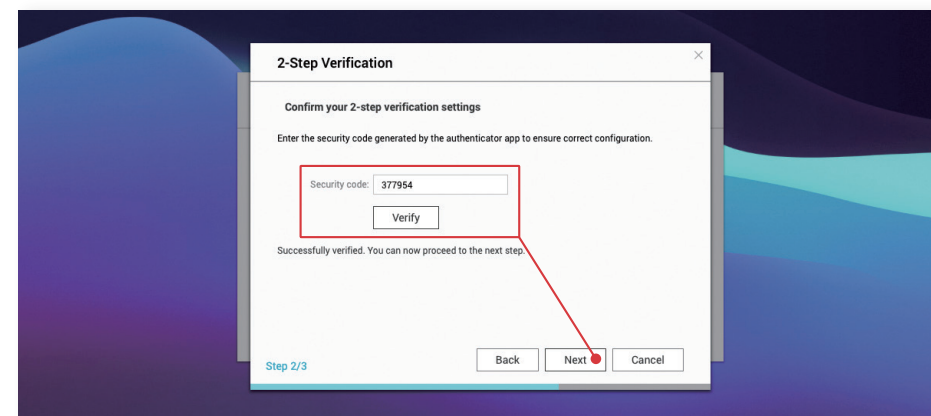
[システム管理者]アカウントに再ログインし、[開始]をクリックして設定を始めます。



モバイルデバイスに[Google Authenticator]または[Microsoft Authenticator]をインストールし、プログラムのQRコードをスキャンしてデバイスを追加してから、[次へ]をクリックします。

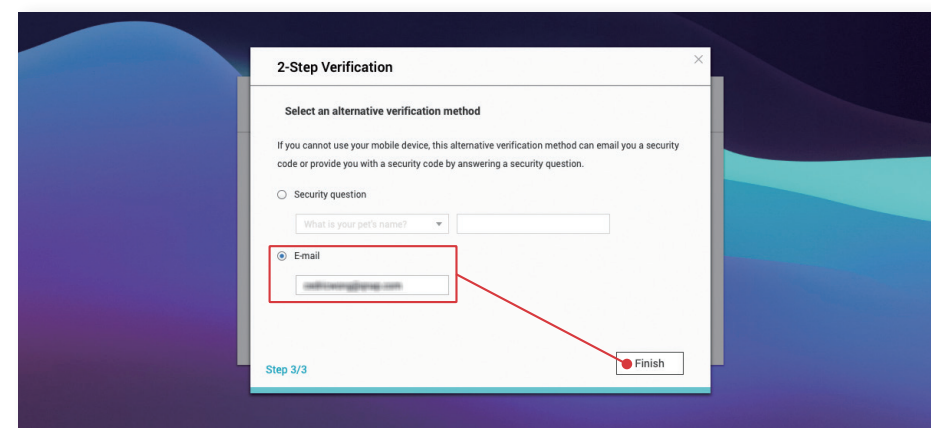


[Google Authenticator]または[Microsoft Authenticator]で生成された6桁の[セキュリティコード]を入力し、[検証]をクリックします。検証後、[次へ]をクリックして続行します。



別の検証方法\*を設定するには[セキュリティ質問]\*\* または[メール]\*\*を選択入力後に[終了]をクリックして[2段階認証(2SV)]を有効にします。

- \* 認証アプリから[セキュリティコード]を取得できない場合は、[セキュリティ質問]に答えるかまたは[メール]を使用して[セキュリティコード]を取得できます。
- \*\* [セキュリティ質問]に正しく答えることで、2段階認証を通過します。簡単すぎる、または推測しやすい質問は避けてください。
- \*\*\* この機能を使うには、[通知センター]に[メール]通知方法を追加する必要があります。



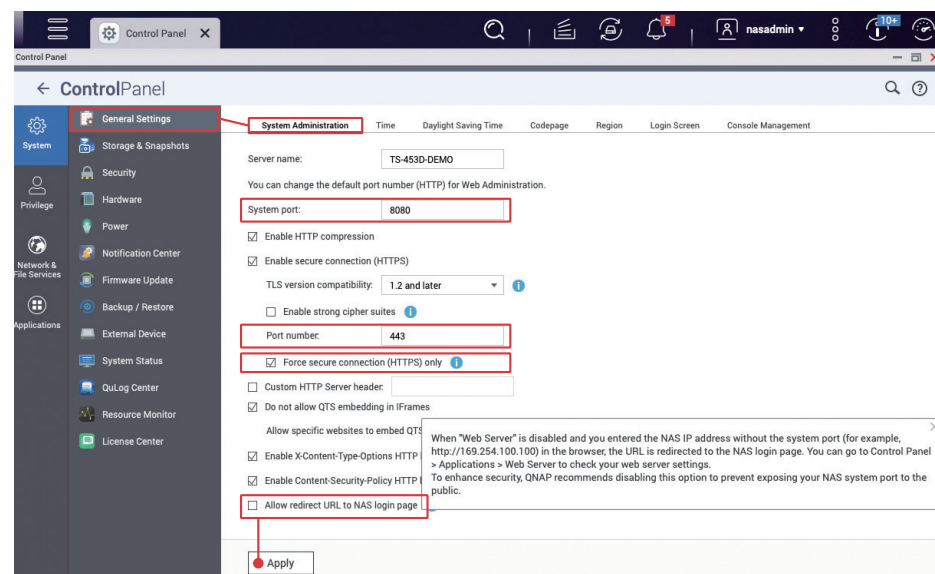
# デフォルトポートを変更する

NAS で実行中の各サービスには、それぞれ対応するサービスポートがあります。変更ができない標準のサービスポート以外は、ユーザーによって定義できます。

ハッカーが攻撃対象を探している際、あるいはハッカーがよく使用する IoT 検索エンジンを使用している場合、デフォルトポートがまず試されます。攻撃されるリスクを下げるには、よく使われるサービスのデフォルトポートを変更する必要があります。NAS に対する攻撃で言えば、もっともよく狙われる対象は「システムポート」です。「システムポート」の変更方法を次に示します。他の機能用のポートは、対応する設定ページで変更できます。その変更は、セキュリティのために、関連するサービスを使う前にしてください。

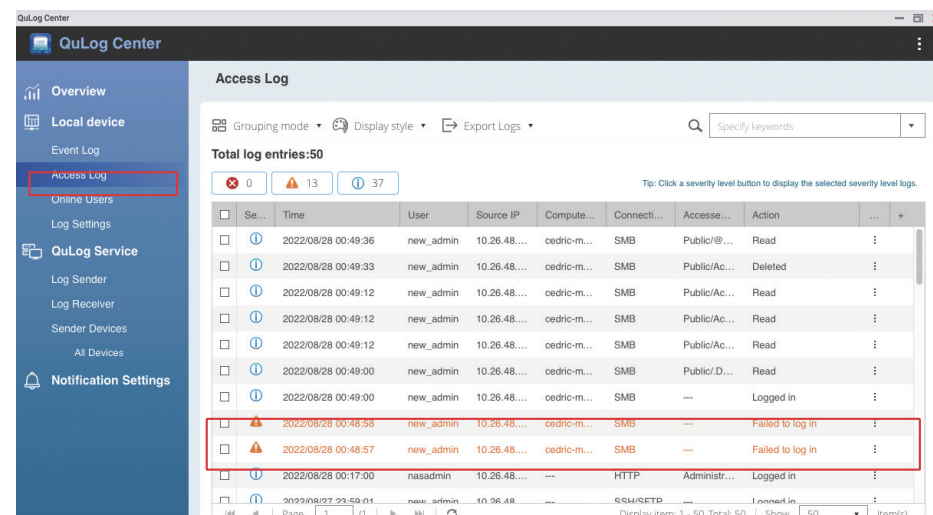
[コントロールパネル]を開いて[一般設定]をクリックし、デフォルトが「8080」の[システムポート (HTTP)]に、1 ～ 65535 の間でポート番号を入力（たとえば 56789）します。さらに「セキュア接続」機能をもつ[システムポート (HTTPS)]では、**システムポートはデフォルトが「443」で、これも変更することを推奨します。**同時に、**セキュア接続 (HTTPS) だけを強制する**にチェックを入れて、全ユーザーがデータを HTTPS で送信するようにし、ハッカーがアカウントのパスワードなどの重要情報が盗まれるのを防ぐことをお勧めします。

さらに、**NAS ログインページへのリダイレクト URL を許可のチェックを外し**、自動リダイレクションによって「システムポート」が露出してしまふのを防ぐことをお勧めします。変更後、**[適用]**をクリックして設定を完了します。

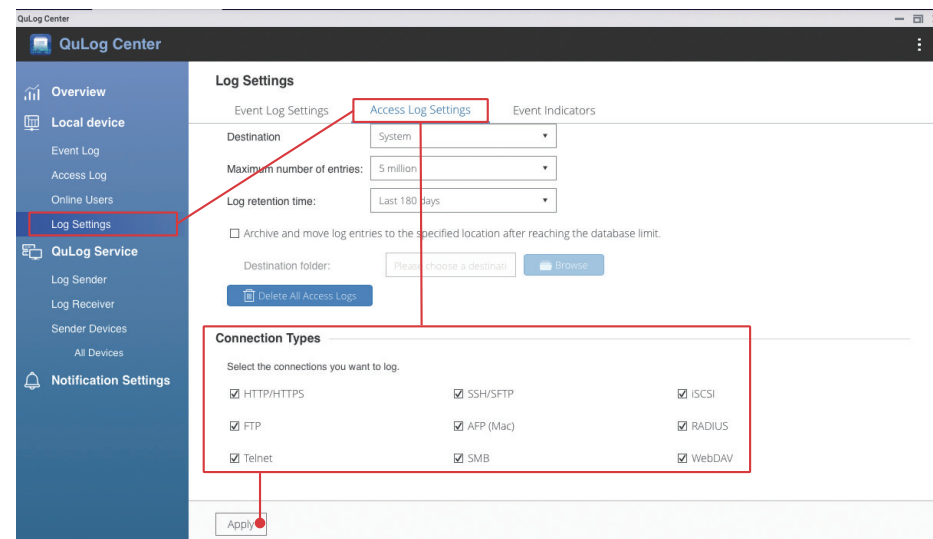


# アクセスログを表示

アクセスログは、ユーザーのファイルアクセス、操作、ログイン履歴を見るのに役立ちます。問題発生時には、まず最初にアクセスログをチェックして根本的な問題を診断します。



[QuLog Center]を開き、左側メニューの[ログ設定]をクリックし、[アクセスログ設定]ページに移り、[接続タイプ]ですべての接続にチェックを入れてから、**[適用]**をクリックして設定を完了します。



# セキュリティアプリのインストールと有効化

QNAP では、NAS のセキュリティを向上させるセキュリティアプリをいくつか提供しています。これらのアプリを設定することで、NAS のセキュリティを向上させることができ、ユーザーに安心してもらえます。



Security Counselor は、NAS 設定のセキュリティを定期的にチェックし、潜在的なリスクを通知します。



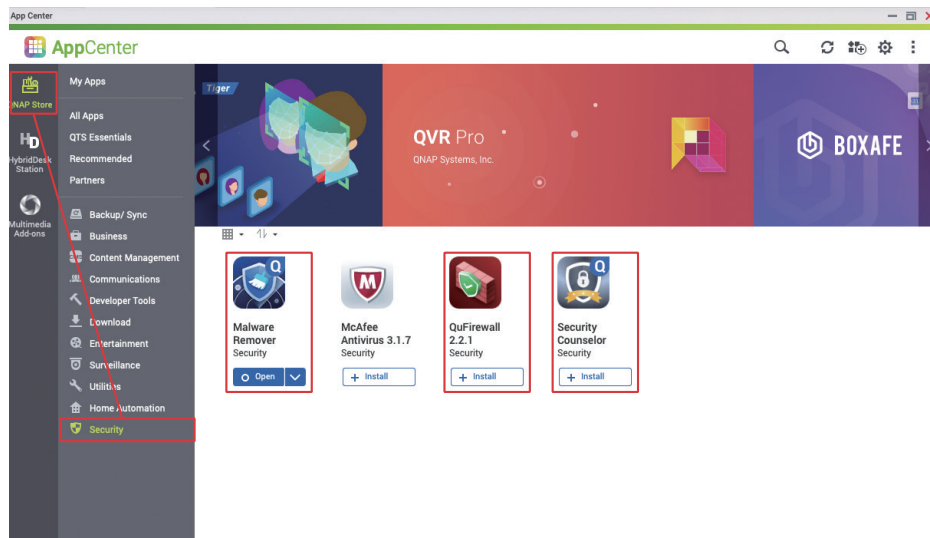
Malware Remover は、スキャンを行い、検出されたマルウェアを NAS から削除します。



QuFirewall は、QNAP NAS に対し基本的なファイアウォール機能を提供し、NAS に接続する際に極力多くのハッカーをブロックします。

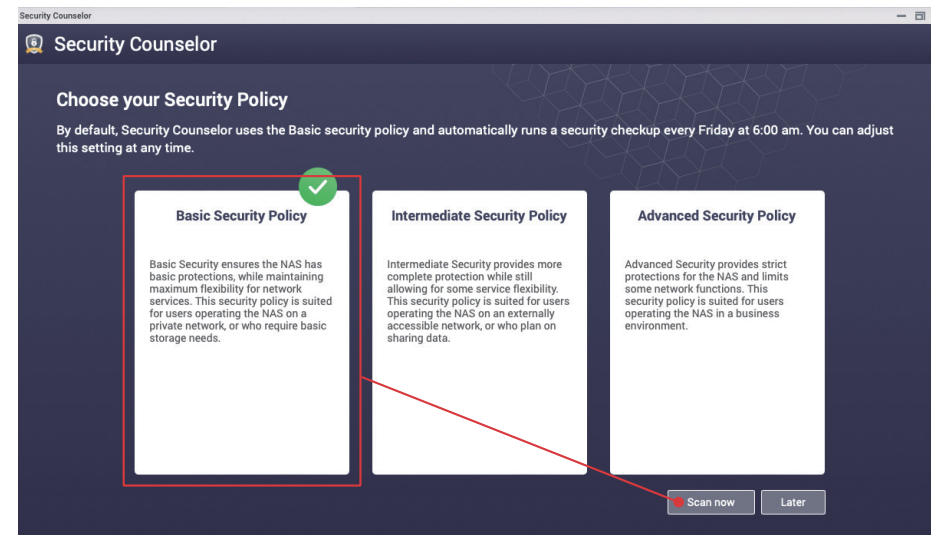
[App Center] を開いて左側の [セキュリティ] をクリックし、Security Counselor、Malware Remover\*、QuFirewall をインストールします。

\* Malware Remover は、QTS 4.4.3 (およびそれ以降) と QuTS hero にはプリロードされています。

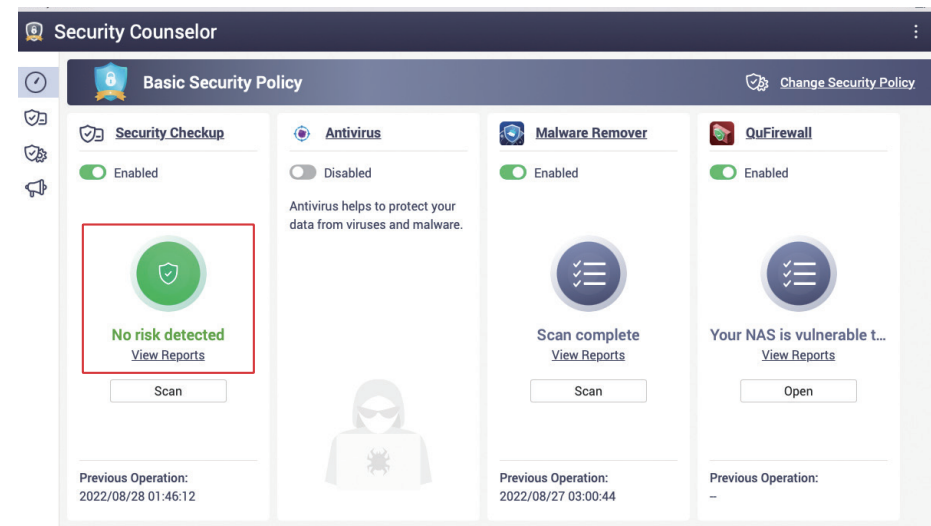


# Security Counselor

[Security Counselor] を開き、[基本セキュリティポリシー] を選択して、[今すぐスキャン] をクリックします。



スキャンが完了すると、通常は [検出リスクなし] という結果になります。リスクが検出された場合は、[レポートを表示] をクリックして詳細を見て、指示に従って設定を変更します。





以下は、意図的に誤った設定にして「高リスク」を起こさせたスキャン結果です。[推奨される設定アシスタント]をクリックして、設定を調整します。

**Security Counselor**

**Basic Security Policy** Change Security Policy

**At High Risk** Last scan status: Finished Last scan time: 2022/08/28 01:53:30 Scan schedule: Friday 06: 00

Overview **1** High **1** Medium **0** Low **0** Scan

Category	Status	Risk	Result	Action
Account	❌	High	Either this setting is deselected in the Password Policy screen or the current required mini...	⋮
Update	✅	High	The	⋮
Account	✅	High	The	⋮
Network	✅	High	Either this setting is deselected in the Password Policy screen or the current required minimum length for passwords is below 8 characters.	⋮
Network	✅	High	The web server on your device cannot be directly accessed from the internet using the foll...	⋮
Network	✅	High	The NAS doesn't allow Telnet connections.	⋮
System	✅	High	Run user defined processes during startup is disabled.	⋮

[推奨される設定アシスタント]が関連する推奨内容を列挙します。読んでから確認し、[推奨事項を適用]をクリックすると、システムが自動的に関連する設定を適用します。手動で変更が必要な設定があります。左側の[手動]タブをクリックし、指示通りに設定を調整します。変更を適用後、スキャンが自動的に再開します。再度スキャン結果をチェックし、NAS にセキュリティリスクが検出されなかったことを確認します。

**Security Counselor**

**Suggested Settings Assistant**

The Suggested Settings Assistant offers suggestions that help improve NAS security.

Automatic Adjustment: There are **1** at-risk settings. Select the risk items below to automatically adjust the related settings.

At-risk User Settings	Suggestion
❌ Either this setting is deselected in the Password Policy screen or the current required minimum length for passwords is below 8 characters.	✅ Configure the settings in the Password Policy screen and require the use of passwords with a minimum of 8 characters.

Apply suggestion Close

左側の[セキュリティ診断]をクリックしてセキュリティ結果画面にはいり、右側の[スキャンスケジュール] をクリックしてスキャンスケジュール設定画面を開きます。

**Security Counselor**

**Basic Security Policy** Change Security Policy

**No risk detected** Last scan status: Finished Last scan time: 2022/08/28 02:08:53 Scan schedule: Friday 06: 00 Scan schedule

Overview **0** High **0** Medium **0** Low **0** Scan

Category	Status	Risk	Result	Action
Update	✅	High	The NAS is using the most up-to-date version of firmware.	⋮
Account	✅	High	The current settings in the Password Policy screen include requiring passwords to have a ...	⋮
Account	✅	High	The default administrator password is not the default password.	⋮
Network	✅	High	The system administration service on your device cannot be directly accessed from the int...	⋮
Network	✅	High	The web server on your device cannot be directly accessed from the internet using the foll...	⋮
Network	✅	High	The NAS doesn't allow Telnet connections.	⋮
System	✅	High	Run user defined processes during startup is disabled.	⋮

[スキャンスケジュール]は少なくとも**ひと月に1回**は行うように設定し、システムが定期的に設定とシステムステータスをチェックできるようにしてください。リスクが検出され、通知センターが正しく設定されていれば、素早い対応が可能な通知を受けることができます。

**Security Counselor**

**Basic Security Policy** Change Security Policy

**No risk detected** Last scan status: Finished Last scan time: 2022/08/28 02:08:53 Scan schedule: Friday 06: 00

Overview **0** High **0** Medium **0** Low **0** Scan

**Scan schedule**

☐ Disable schedule

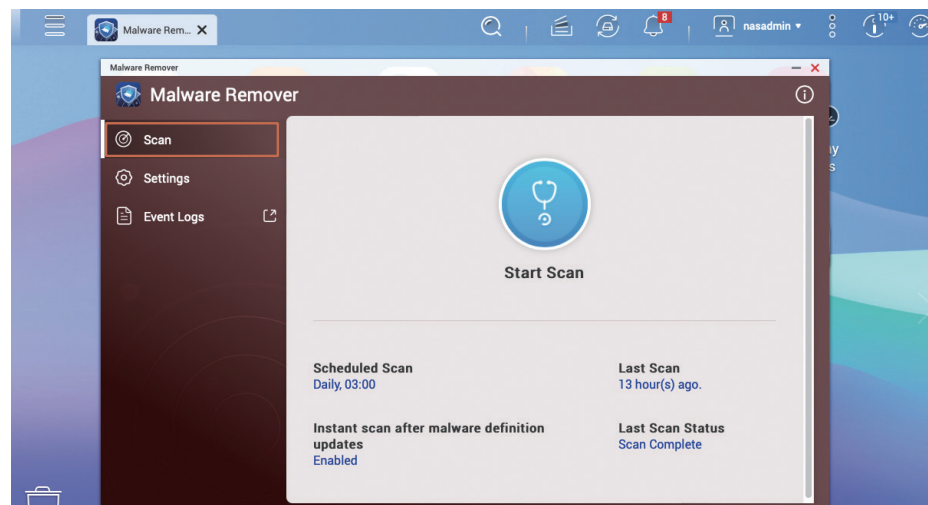
☒ Enable schedule

Run on the following days: Friday Run at the following time: 06 : 00

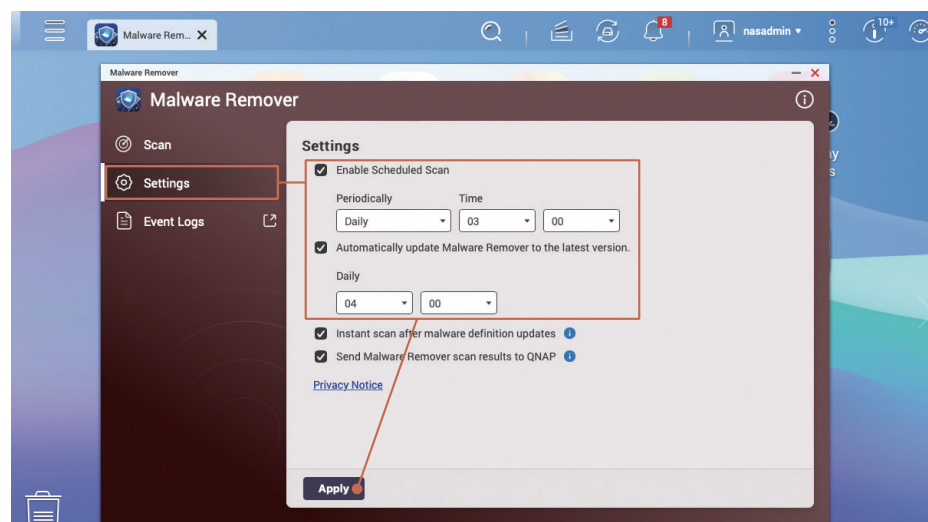
Apply Cancel

# Malware Remover

[Malware Remover]を開き、最後のスキャンのステータスが表示されたら、左側の[設定]をクリックします。

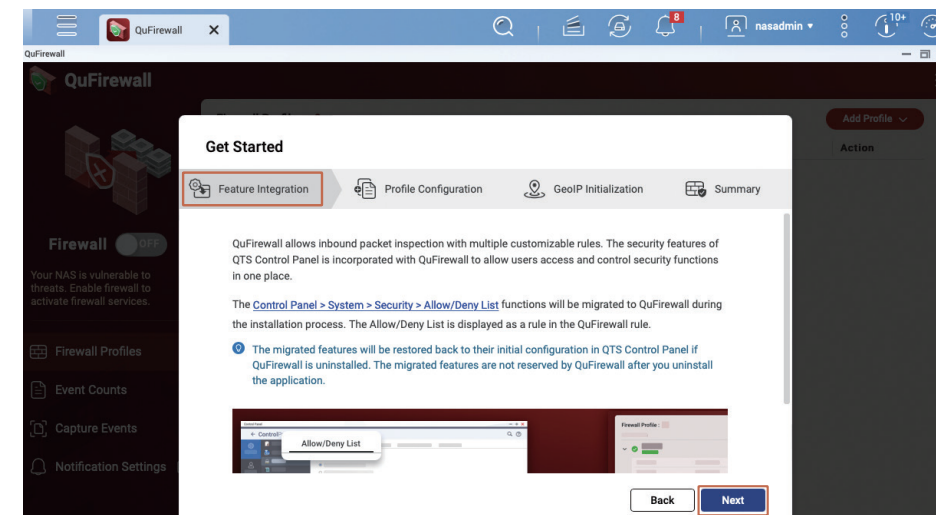


[スキャンスケジュール]は少なくとも **1 日に 1 回**は行うように設定し、[Malware Remover]が定期的にシステムステータスをチェックできるようにしてください。さらに、[Malware Remover を自動的に最新バージョンに更新]にチェックが入っていることを確認してください。

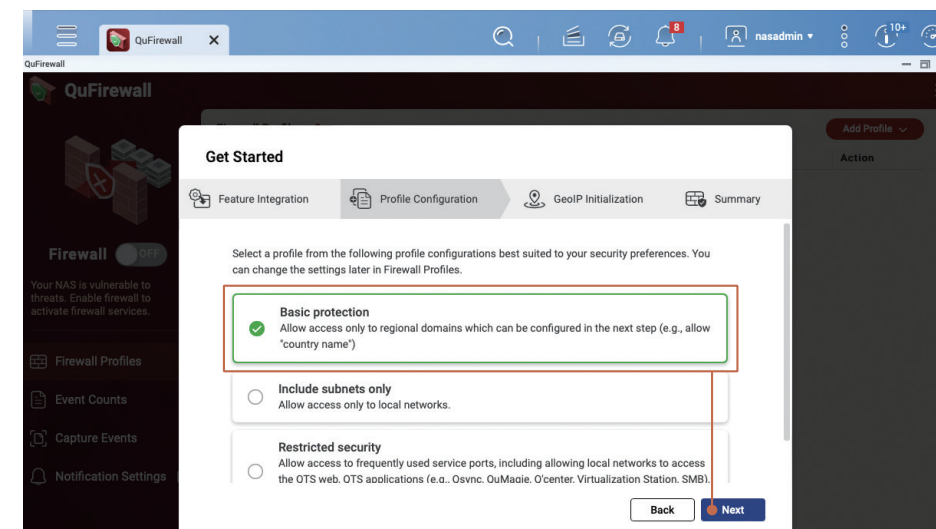


# QuFirewall

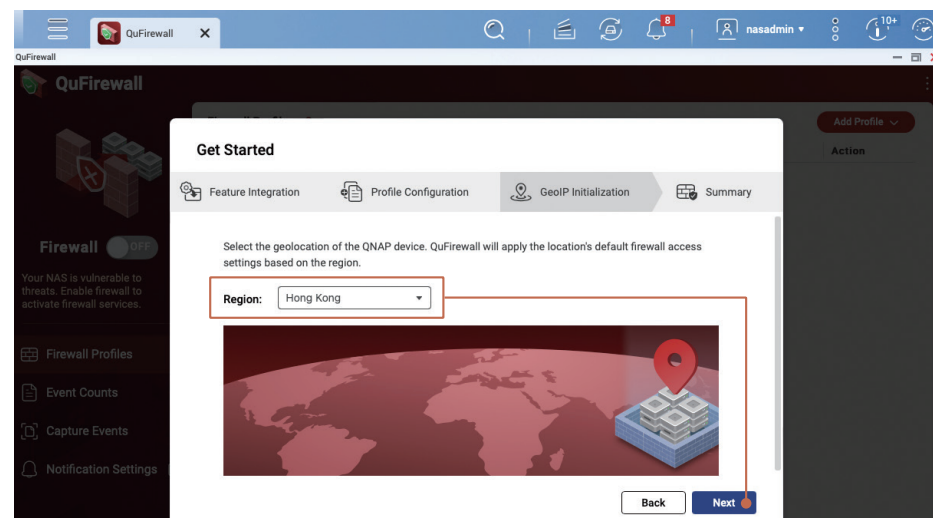
「QuFirewall」を開きます。初めて QuFirewall を使う場合は、開始画面が表示されます。それを読んだ後、[次へ]をクリックして続行します。



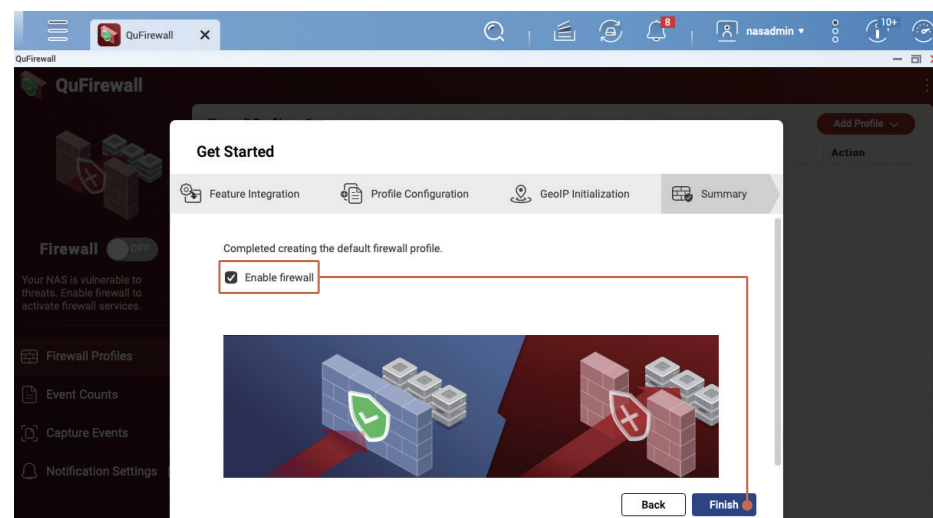
ネットワークに特別のニーズがない場合は、[基本的な保護]を選択し、[次へ]をクリックして続行することをお勧めします。



お住まいの地域を設定します。たとえば、台湾にいる場合は[Taiwan]を、香港にいる場合は[Hong Kong]を、マカオにいる場合は[Macao]を選択します。地域は後で追加できます。[次へ]をクリックして続行します。

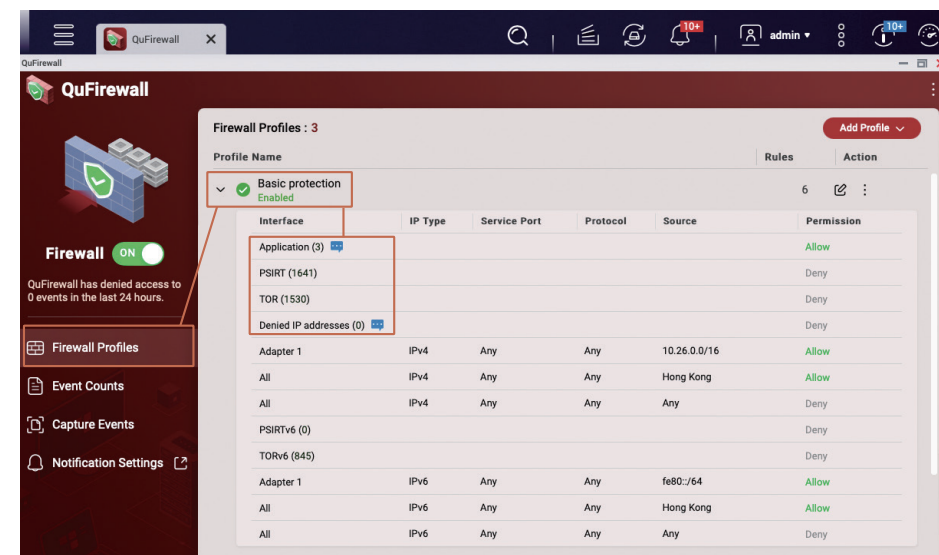


[ファイアウォールを有効にする]にチェックを入れてから、[終了]をクリックして設定を適用し、ファイアウォールを有効にします。




QuFirewall のプロフィールページに進み、[基本的な保護]が有効になっていることを確認します。[基本的な保護]をクリックして拡張させ、対応するファイアウォールルールを表示します。ルールは、受信パケットの情報に基づいてチェックされ、ファイアウォールルールに従って通過されるかブロックされます。ファイアウォールルールは順番に実行されます。条件に適合しない場合、次の行のルールがチェックされます。どれも適合しない場合は、最後の[deny all]ルールに到達し、ファイアウォールが対応する接続をブロックします。

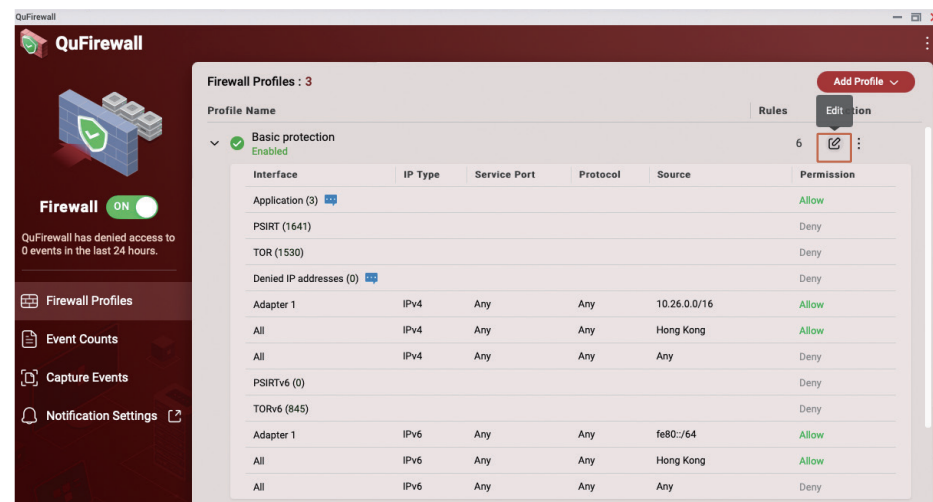
- [アプリケーション]ルールは、システムによって作成されるもので、システムが適切に機能するようにします。
- [PSIRT]ルールは、QNAP PSIRT によってまとめられるブラックリストです。これには QNAP NAS を攻撃することが知られている IP アドレスが含まれます。
- [TOR]ルールは、TOR ネットワークからの接続をブロックするために用いられます。TOR ネットワークは、その匿名性のために犯罪によく使われており、これをブロックすることで攻撃のリスクを減らすことができます。
- [拒否された IP アドレス]は、[IP アクセス保護]機能でブロックされたものかまたは、ユーザーによって手動でブラックリストに追加された IP アドレスです。



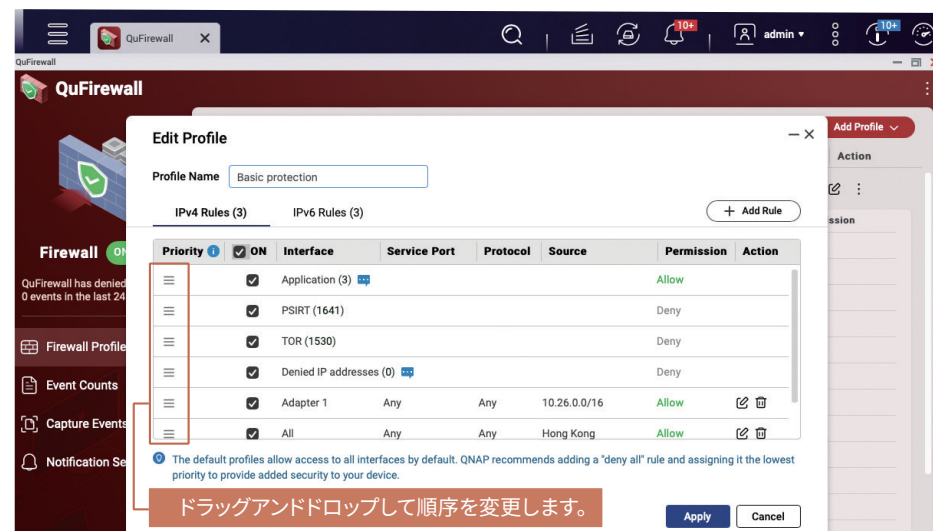
その他のルールはユーザーがカスタマイズすることが可能で、基本的な保護設定においては、同じイントラネットおよび同じ地域からのインターネット接続だけが許可 (allowed) されます。QNAP は、NAS に接続できる IP アドレスを厳密に制限するために、お客様のカスタムルールを管理する「ホワイトリスト」の考え方を推荐使用します。



ファイアウォールルールの編集方法を以下に示します。[編集 ] ボタンをクリックし、ファイアウォールプロフィール画面を編集します。

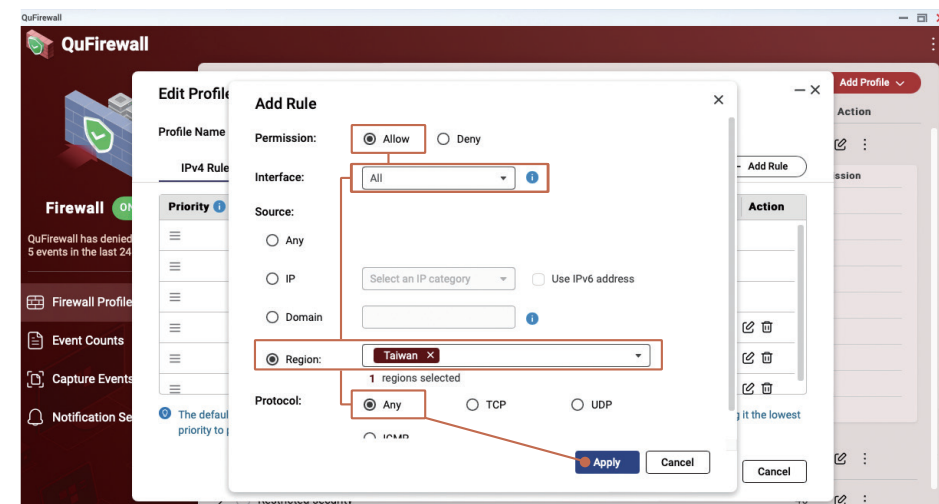


編集プロフィール画面では、ルールの順序変更や新しいルールの追加が行なえます。次の例では、接続が許可される地域を追加するもので、[ルールを追加]をクリックして設定画面にはいります。

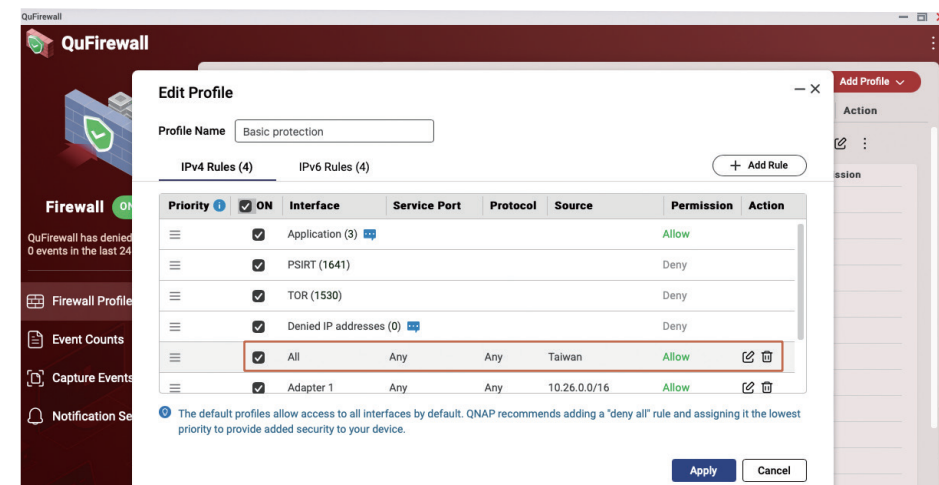


ドラッグアンドドロップして順序を変更します。

たとえば、台湾からの接続を許可するには、[Permission]を[Allow]に、[Interface]を[All]に、[Source]を[Region]に設定してから、[Taiwan]を選択し、[Protocol]を[Any]にしてから、[適用]をクリックすることで終了後にルールが追加されます。



新しく追加されたルールは、[プロフィールの編集] ページで見ることができます。必要であれば、ルールの順序を調整できます。すべてが正しいことを確認した後、[適用]をクリックします。



# スケジュールしたスナップショットの有効化

スナップショット機能は、復元ポイントを複数バージョン作成することで重要なデータを保護します。基本データ保護としてのスケジュールに従い、システムが自動的にスナップショットを作成できるよう、QNAP NAS でスナップショットのスケジュールを設定できます。

- ★ スケジュールしたスナップショットは、デフォルトでは、QTS 5.0.0 で作成された「フル/シン ボリューム」に対して有効です。
- ★ QTS 5.0.1 (およびそれ以降) では、デフォルトでは「シン ボリューム」だけでスケジュールしたスナップショットが有効です。
- ★ QuTS hero h5.0.1 (およびそれ以降) で作成された「共有フォルダー」は、デフォルトでは、スケジュールしたスナップショットが有効です。

[ストレージ&スナップショット]を開き、左側の[ストレージ/スナップショット]をクリックし、[ストレージ領域]が[ストレージプール] 構造で、[ストレージプール] にスナップショット機能のために十分な空き領域があることを確認します。ボリュームタイプが「フルボリューム」の場合、スナップショット機能のために[ストレージプール] 領域を空けるために、[ボリュームのサイズ変更\*]と[シンボリュームに変換]を検討できます。

- ★ データ損失が起きないように、ボリュームを変換する前にデータをバックアップしてください。

NAS の[ストレージプール]に十分な領域があることを確認した後、まず[ボリューム]をクリックしてから、上にある[スナップショット]をクリックし、メニューの[スナップショットマネージャー]をクリックします。

「ボリューム」の[スナップショットマネージャー]設定ページに進み、右上の[スナップショットをスケジュール]をクリックします。

[スナップショットマネージャー]を[有効]な状態に切り替えてから、必要に応じてスケジュールを変更します。  
[毎日]または[毎週]を使用することをお勧めします。

スナップショット保持ポリシーを設定して、スナップショットの数を制限し、スナップショットによって過大な領域が占められてしまうのを防止できます。

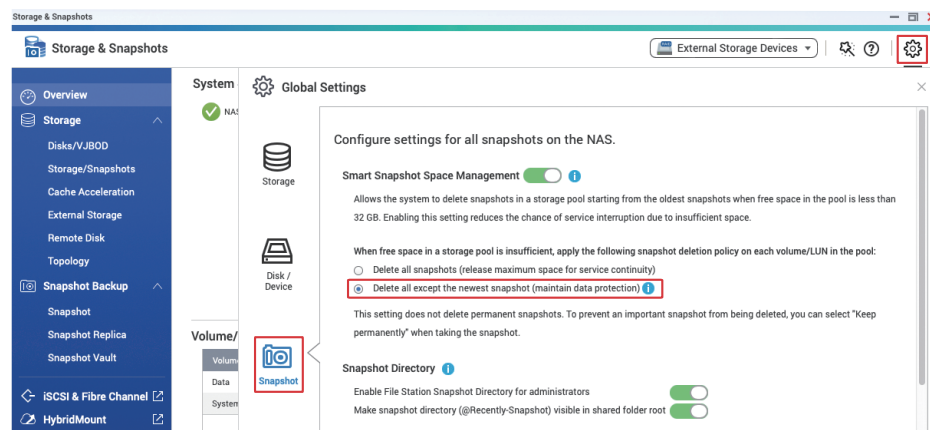
[スマートバージョンング]を設定し、GFS ルール (Grandfather-Father-Son) によってデータ保護のために十分なバージョンを保持することをお勧めします。完了したことを確認後、[OK]をクリックして設定を適用します。



# スナップショットの削除ポリシーを設定する

ストレージプールの領域が十分でない場合、システムは通常のシステムサービスを維持し、領域不足によってサービス停止が起こらないよう、設定に応じてスナップショットを削除します。

[ストレージ&スナップショット]で、右上隅の[設定]ボタンをクリックし、[グローバル設定]を開いて[スナップショット]をクリックします。すべてのスナップショットが削除されて、保護ができなくなるのを防ぐため、**[最新のスナップショット以外を削除]**に設定することをお勧めします。

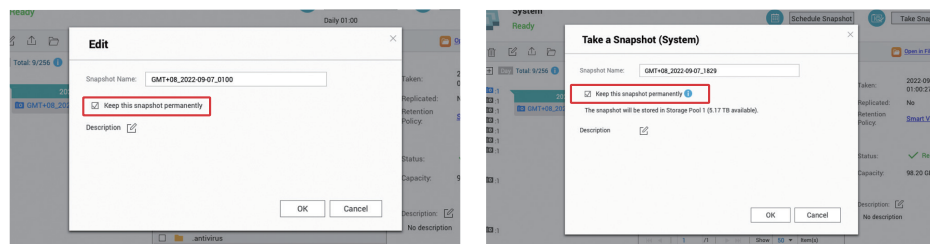


[ストレージプール]の領域が不足した時でもシステムがすべてのスナップショットを保持するようにしたい場合は、[スマートスナップショット領域管理]を無効にします。この場合、[ストレージプール]が不足した場合には、[ストレージプール]が[読み取り / 削除]モードになりますのでご注意ください。[ストレージプール]を通常の動作に戻すには、スナップショットを手動で削除する必要があります。この機能を無効にした場合は、領域を定期的にチェックしてください。



スナップショットの削除ポリシーによって保護に問題が生じないよう、大量のデータを保存した後は、スナップショットのすべてあるいは一部に[スナップショットを永続的に保持]\*を設定し、システムによってスナップショットが再利用されないようにすることをお勧めします。

\* 領域を空けるために手動で削除する必要があります。定期的に手動で作成および削除することをお勧めします



# NAS セキュリティ設定チェックリスト

## 通知センターを設定する

- ☐ 少なくともひとつの通知方法を設定する
- ☐ 「アラート通知」ルールを作成する
- ☐ 「ファームウェア更新」通知ルールを作成する

## ファームウェア 自動更新 (QTS / QuTS hero) を有効にする

## App Center を設定する

- ☐ すべてのアプリケーションを最新バージョンに更新する
- ☐ 正しいデジタル署名を持たないアプリケーションのインストールを禁止する
- ☐ 自動更新を有効にする

## 不要な機能を無効化または削除する

- ☐ 有効化しているサービスの必要性を確認する
- ☐ 有効化した **App Center** アプリが必要かどうか確認する
- ☐ SSH を無効にする
- ☐ Telnet を無効にする

## システムアカウントセキュリティを強化する

- ☐ デフォルトの「admin」アカウントを無効にする
- ☐ パスワードポリシーを設定する
- ☐ IP アクセス保護を有効にする
- ☐ 2段階認証 (2SV) を有効化する

## デフォルトシステムポートを変更する

## アクセスログを有効にする

## セキュリティアプリをインストールし有効にする

- ☐ **Security Counselor**
  - ☐ スケジュールスキャンを開始する
- ☐ **Malware Remover**
  - ☐ スケジュールスキャンを開始する
- ☐ **QuFirewall**
  - ☐ ファイアウォールを有効にする
  - ☐ Geo-IP 地域を設定する
  - ☐ PSIRT ルールを有効にする
  - ☐ TOR ルールを有効にする

## スケジュールしたスナップショットを有効にする

- ☐ 定期的に[スナップショットを永続的に保持]を設定する

**Q NAS をインターネットから切断すると、安全性が増しますか？**

**A** いいえ。NAS の「切断」は一般的に、NAS をネットワークから切断し、外の世界に接続できないようにします。いくつかのマルウェアでは、実行に外部接続が必要なものの、外部接続がなくても悪意ある行動を行えるマルウェアも存在します。そのため、ハッカーの違法な行動の防止ができないだけでなく、自動ソフトウェア更新や通知など、システム機能のいくつかが正しく動作しないことになります。正しいアプローチは、インターネットから見えないようにして NAS へのトラフィックを制限してセキュリティを高めることです。

**Q 使っているハードディスクは RAID で構成されているので、バックアップは不要ですか？**

**A** いいえ。RAID はバックアップ手法ではありません。レベル 0 より上の RAID レベルは、ディスク障害に対する冗長性のためのものです。RAID は、データの削除や暗号に対する保護機能はありません。そのため、**3-2-1 バックアップ原則に従ってデータを適切にバックアップすることをお勧めします。**

**Q 「スナップショット」を設定してあるので、バックアップは不要ですか？**

**A** いいえ。「スナップショット」は、同じハードドライブにデータとして保存されるため、RAID 障害があるとデータは失われてしまいます。さらに、ハッカーが必要十分な権限を得てしまうと（管理者アカウントのクラッキングに成功するなどして）、「スナップショット」も削除されてしまいます。そのため、3-2-1 バックアップ原則に従ってスナップショットファイルを適切にバックアップすることをお勧めします。

**Q 私の NAS はインターネットから見えないようになっているので、攻撃は不可能と考えていいですか？**

**A** いいえ。大半のサイバー攻撃はインターネットからのものですが、それでも NAS はイントラネットでも攻撃されるリスクがあります。たとえば、イントラネット上の別のコンピューターやデバイスがハックされた、あるいはマルウェアに感染した場合、イントラネットの他のデバイスへの攻撃や感染拡大に使われる可能性があります。コンピューターにアンチウイルスソフトウェアをインストールし、ネットワークセキュリティ製品をデプロイすることで、関連する脅威に対応することができます。たとえば、QNAP ADRA NDR は疑わしいイントラネット上の活動を検出し、それを自動的に隔離します。同時に、3-2-1 バックアップ原則に従ってデータを適切にバックアップすることをお勧めします。

**Q 私の NAS は長い間使用していますが、マルウェアがインストールされていないかはどうしたらチェックできますか？**

**A** プロセッサの負荷が異常に高い、ソフトウェアの更新が失敗する、あるいは App Center に見知らぬアプリがあるといったことに気づいた場合は、悪意あるプログラムがインストールされている可能性があります。最新版の Malware Remover をインストールして動作させることが推奨されます。その問題を解決できない場合は、QNAP テクニカルサポートチームに支援を求めてください。

**Q インターネットにサービスを開く必要がある場合は、どのようにしてセキュリティを確保したらよいでしょうか？**

**A** NAS に最新のファームウェアとアプリがインストールされていることを確認してください。基本的なファイアウォール保護のために、QuFirewall を有効にすると同時に、「PSIRT」と「TOR」ルールがハッカーの接続をブロックする役に立ちます。ビジネスユーザーあるいは企業ユーザーの場合は、より高いレベルのファイアウォールソリューションを使われることをお勧めします。さらに、ストレージプールに余裕があれば、基本的なデータ保護のために「スナップショット」を作成できます。最悪の事態に備え、データ損失の可能性をなくすために、3-2-1 バックアップ原則に従ってデータを適切にバックアップすることをお勧めします。

**Q 私の NAS は古く、QTS の最新バージョンをサポートしていません。まだ安全に使えますか？**

**A** レガシーモデルやライフサイクル終了 (EOL) モデルに対するサポートは限定的で、イントラネットやオフラインバックアップ目的にのみ使用すべきです。

**Q NAS ログイン失敗警告が出続けるのはなぜですか？**

**A** 失敗ログインの IP アドレスがインターネットからのものであれば、NAS が総当たり攻撃によるパスワードクラッキング攻撃を受けています。NAS がインターネットから見えないようにすべきで、このチュートリアルで NAS を強化してください。ログイン失敗の IP アドレスがイントラネットからのものであれば、その IP アドレスのデバイスにマルウェアがインストールされていないかを調べてください。

## Q ファイルにおかしなファイル名がついているのはなぜですか？

**A** これは、ランサムウェアに感染している兆候です。NAS のアクセスログをチェックして、別のコンピューターまたは NAS 自身で暗号化アクションがないかどうか調べてください。NAS がランサムウェアに感染していた場合、感染拡大を止めるための適切な行動をとる必要があります。必要であれば、QNAP テクニカルサポートチームに支援を求めてください。

## Q 使っている NAS がランサムウェアに感染した場合どうしたらいいですか？

**A** 大半のランサムウェアは、解読不能な暗号方法を用います。正しい鍵がなければ、ファイルはロック解除することができないため、ファイルはバックアップまたはスナップショットでしか復元できません。

すぐにこのチュートリアルに従ってルーター設定を変更し、NAS がインターネットから見えるようになるのを防ぎ、二次的攻撃を防いでください。もうひとつ、直ちに同期タスクをすべて停止させ、スナップショットが永続的に保持されるようにしてバックアップファイルが失われないようにします。データを復元できるバックアップやスナップショットがある場合には、NAS ファームウェアとアプリを更新し、Malware Remover のスキャンを完了させてからファイルを復元します。データがバックアップされていない場合は、ランサムウェアが残したランサムノートと身代金を支払う方法をバックアップしてから、データを復元すべくデータ復元などの方法を試みてください。必要であれば、QNAP テクニカルサポートチームに支援を求めてください。

## Q QNAP パッチング製品の脆弱性に関するメディアレポートが続いています。これは、QNAP 製品がセキュアでないということですか？

**A** 世の中に完璧なソフトウェアやハードウェアはありません。さまざまなメーカーによって開発された独自ソフトウェアやオープンソースソフトウェア、あるいはハードウェアであれ、脆弱性はいつも見られ、メーカーによってパッチが出されます。他の主要なテクノロジー企業と同じように、QNAP は既知の脆弱性に対するパッチを出し続け、できるだけ早くユーザーに更新をリリースしてユーザーのデバイスやデータのセキュリティを確保しています。QNAP PSIRT は、顕在化する問題に対してユーザーが対応できるよう、サイバーセキュリティの外部への通知も行っています。QNAP は、オープンで透明性のある形で脆弱性に取り組むことにより、ユーザーの知る権利を守り、製品の安全性を向上できると考えています。ユーザーに対しては、QNAP セキュリティアドバイザリに参加し、メディアが報道する前に、関連する正確で完全な情報を取得するよう呼びかけています。

### QNAP セキュリティアドバイザリ:

<https://www.qnap.com/go/security-advisories/>



## Q 3-2-1 バックアップ原則とは何ですか？

**A** 3-2-1 バックアップ原則は、IT 業界ではよく知られたバックアップ原則です。これは、最悪の自体に備えるものです。これは、災害発生時に、データを復元し、損失を避け、安全性を確保するためのバックアップファイルをもつようにします。

バックアップ 3-2-1 の「3」はバックアップコピーを 3 つもつことを、「2」は少なくとも 2 つのストレージメディアを、「1」は少なくとも 1 つのオフサイトバックアップをもつことを意味しています。

3-2-1 バックアップ原則に基づくことで、偶発的な変更や削除、ハードウェアの損傷、ウイルス感染、火災や洪水などの災害に遭っても、復元可能なバックアップファイルが確保されます。

この原則を満足させるために、QNAP NAS には Hybrid Backup Sync 3 (HBS3)、スナップショットレプリカ、SnapSync (QuTS hero のみサポート) が含まれ、NAS 上のデータをオフサイトの NAS、パブリッククラウド、外部ストレージ、その他のファイルサーバー、その他のデバイスにバックアップすることでデータ損失をなくします。

### Hybrid Backup Sync 3 (HBS3) 関連のチュートリアル:

<https://www.qnap.com/go/how-to/tutorial/article/hybridbackup-sync>



### スナップショットレプリカ関連のチュートリアル:

<https://www.qnap.com/go/how-to/tutorial/article/savesnapshots-to-other-qnap-nas-with-snapshot-replica>



### SnapSync のチュートリアル:

<https://www.qnap.com/go/how-to/tutorial/article/bestpractices-for-the-configuration-of-realtime-snapsync>



セキュリティを高めるためには、オフラインバックアップを追加するか、QuTS hero の WORM (Write Once Read Many) ストレージ領域にバックアップして、データの改ざんを防止してください。

MEMO

2 0 2 3

セキュリティガイド

# QNAP



## QNAP SYSTEMS, INC.

電話: +886-2-2641-2000 FAX: +886-2-2641-0555 電子メール: [qnapsales@qnap.com](mailto:qnapsales@qnap.com)

アドレス: 3F, No.22, Zhongxing Rd., Xizhi Dist., New Taipei City, 221, Taiwan

QNAP はいつでも、事前の通知なしに仕様と製品説明を変更することができます。

Copyright © 2023 QNAP Systems, Inc. All rights reserved.

QNAP® および QNAP 製品の名前は QNAP Systems, Inc. の独占所有権のある商標または登録商標です。

ここで述べられたその他の製品と会社名は、それぞれの所有者の商標です。