

QNAP NAS

情報セキュリティマニュアル



QNAP SYSTEMS, INC.

QNAP 製品のご利用、そしてデータを QNAP NAS にお任せいただき、ありがとうございます。お客様のサポートに感謝すると共に、お客様の信頼は私たちにとって最も大切なことだと考えます。そのために、絶えず製品とセキュリティの改善を続け、努力しております。

世界的に増え続けている攻撃、マルウェア、セキュリティへの懸念を踏まえ、お客様自身およびお客様のデジタル資産を積極的に保護していただけるよう、以下の情報を提供する必要性を認識しています。本ガイドのアドバイスと正しい IT 利用習慣を組み合わせ、ユーザーの皆様がご自身のデバイスとデータを差し迫る脅威から保護できることを願っています。

QNAP Systems, Inc.

張明智

ジェネラルマネージャー

www.qnap.com

セキュリティ向上のためのベストプラクティス

データ保護手法は、変化し続けるハッキングテクニックに遅れを取らないよう、進化しています。データおよびデバイスを保護し続けるために、NAS ユーザーは数多くのツールを自由に選べます。たとえば、パスワード保護、権限設定、ファイルレベルの暗号化、オペレーティングシステムおよびソフトウェアの更新、ネットワーク接続設定、データバックアップとディザスタリカバリ用アプリなど。QNAP 製品は、多角的で強力な情報セキュリティ機能を有しています。以下は、情報セキュリティに関する基本的理解を素早く得るために役立つ 9 つの情報セキュリティポイントを示しています。

1. 不明なアカウントや疑わしいユーザアカウントを削除する
2. 不明な、あるいはめったに使わない NAS アプリケーションを削除する
3. myQNAPcloud で自動ルーター設定を無効にする
4. デバイスアクセス制御を設定する
5. インターネットでデフォルトのポート番号を開示しない
6. 最新版の Malware Remover をインストールして実行する
7. 全ユーザーアカウントのパスワードを定期的に変更する
8. インストールされているアプリケーションを最新版に更新する
9. ネットワーク接続したデバイスのオペレーティングシステムやシステムソフトウェアが常に更新されているようにする

後に、QNAP のさまざまな情報セキュリティ設計をひとつずつ説明し、さらに包括的な NAS 保護計画の構築についても説明します。

強力なパスワードを使用する

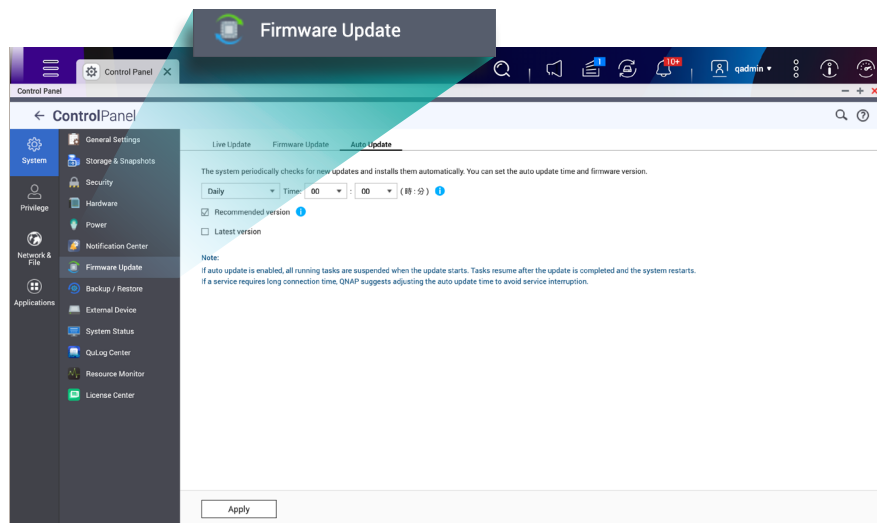
ユーザーのアカウントにアクセスを試みることは、ハッカーにとって最も一般的な攻撃ベクトルです。これは通常ハッカーによってデフォルトあるいは一般的なパスワードが試される、あるいはソーシャルエンジニアリング（たとえば、ペットや子供の名前をパスワードに使っていると推測されやすくなります）を使って行われます。ユーザーアカウントが破られてしまう脅威を緩和するには、デフォルトの admin アカウントを無効にし、すべてのユーザーに対して以下に述べるような強力なパスワードの設定を義務付けることをお勧めします。

条件	説明
英文字	大文字と小文字を含めてください
数字	少なくとも 1 つの数字を含めてください
特殊文字	少なくとも 1 つの特殊文字を含めてください (<ADD SPECIAL CHARACTERS HERE>など)
繰り返しをしない	同じ文字を繰り返し使わないでください (AAA や 111)
ユーザー名を含めない	パスワード内にいかなる形でも（逆向きにも）ユーザー名を使わないでくださいたとえば、ユーザー名が W user1 で、パスワードが 1resu。
最小長	パスワードには最低 8 文字を使用することを推奨します。パスワードの最大長は 64 文字です。

強力なパスワードの使用に加え、ユーザーは自分のパスワードを定期的に変更すると良いでしょう。ユーザーのパスワードが有効な日数をシステム設定で指定することができます。

ソフトウェアアップデートは重要です

NAS やその他のネットワーク接続されたデバイスで、古くなったソフトウェアを実行すると、ネットワーク全体がリスクにさらされます。QNAP の開発チームは、常に監視し、脆弱性の可能性が見つかったとすぐにパッチを作成して、可能な限り早くオペレーティングシステムおよびアプリのアップデートをリリースします。ユーザーは App Center でアプリを常に最新に保ち、さらに QTS システムのファームウェアアップデートセクションで自動更新を有効にすることをお勧めします。QNAP Web サイトには、新しいソフトウェアバージョンに加えられた修正と改善に関する情報が掲載されているリリースノートがあります。



QTS 4.5.3 からは、App Center はデフォルトで、新しいバージョンのアプリに自動的にアップデートするようになります（QTS 4.5.3 より後のバージョンにアップグレードできない NAS は、コンソールインターフェースを用いて自動更新を有効にできます）。お使いの NAS がインターネットに接続されていない場合は、QNAP Download Center からアップデートをダウンロードし、それを手動で NAS にインストールできます。

2 段階認証を有効にする

2 段階認証は、ユーザーアカウントのセキュリティを大幅に高めます。有効にすると、ユーザーは、アカウントへのログインの際に自分のモバイルデバイスの認証アプリからコードを入力するよう求められます。これはユーザーアカウントに追加のセキュリティレイヤを追加するもので、ご自分のアカウントへのハッカーによる不正なアクセスの可能性を大幅に減らします。

2 段階認証を使用するには、お使いのモバイルデバイスに検証アプリをインストールする必要があります。このアプリは、認証サービスを構築するためにタイムベースドワンタイムパスワード (TOTP) アルゴリズムを使用する必要があります。QTS では 2 段階認証用に、Google Authenticator (Android、iOS、BlackBerry) および Authenticator (Windows Phone) に対応しています。



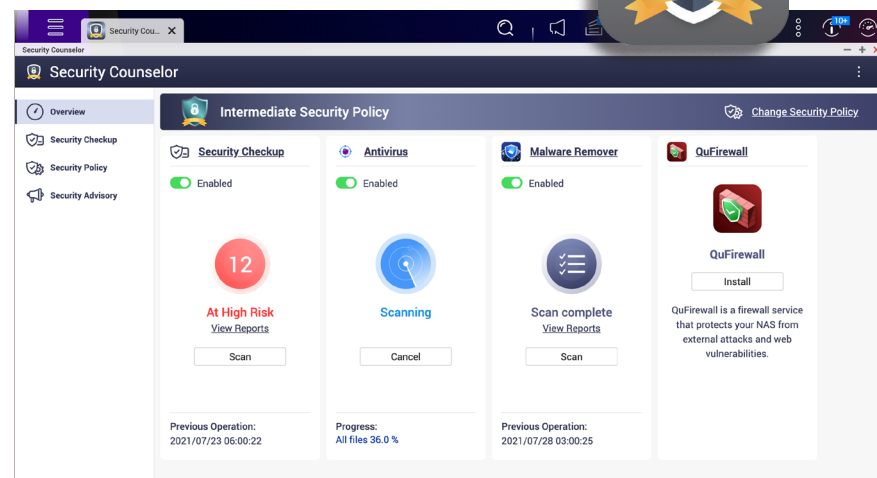
認証アプリを入れたモバイルデバイスを紛失、あるいはユーザーが 2 段階検証用のモバイルデバイスを使えない場合、セキュリティ質問に回答する別の認証方法やメールでセキュリティコードを受け取る選択を設定できます。

セキュリティを評価する

デバイスをインターネットに接続する際はセキュリティリスクを避けられないため、QNAP ではセキュリティカウンセラーアプリを提供しています。このアプリは、お使いの NAS での潜在的なセキュリティ脆弱性を監査し、NAS が危険にさらされるのを防止するために推奨のシステム設定調整を提供します。

セキュリティカウンセラーでは、NAS の使用要件に基づいてそれぞれのセキュリティレベルの推奨を指定できます。定期的にスキャンも行われます。その他の設定、たとえば IP ブロッキング、セキュリティ資格情報、パスワードポリシーなども調整が可能です。

セキュリティカウンセラー



簡単に脅威を除去

定期スキャンにより、お使いの NAS がマルウェアに感染していないかを確認でき、検出されたマルウェアは削除されます。また、Malware Remover は最新のマルウェア定義を自動的にダウンロードし、新たに現れるマルウェアの脅威に対してもしっかり保護を提供します。

Malware Remover



Malware Remover のスキャン結果を QNAP に送るような設定も可能で、これにより QNAP は自社のマルウェア定義を更新でき、QNAP NAS ユーザーのセキュリティを強化するのに役立てられます。

セキュリティファイアウォールを NAS にインストール

ネットワーク上のセキュリティ脅威は、内部ネットワークと外部ネットワークを区別しないため、ネットワークベースのファイアウォール（バウンダリ）をローカルネットワークのエッジに設置するだけでは、全体のセキュリティを確保するには不十分です。現在では、ゼロトラストネットワークが主流となっており、QNAP デバイスに QuFirewall をインストールして有効化し、ホストベースのファイアウォール（マイクロバウンダリ）を作成すると、重要なデータやサービスを保護することができます。

QuFirewall



QuFirewall は無料の QNAP NAS アプリで、受信ネットワークトラフィックに対して接続を許可 / 拒否する設定により、インターネットに接続された NAS のセキュリティを向上させます。QuFirewall は GeolIP もサポートしています。これによって、特定の地理的エリアからの接続を検出して拒否することができます。さらに保護機能を高めるために、Virtualization Station の Virtual Machine Marketplace から、利用者の多いオープンソースのファイアウォールである pfSense をインストールすることもできます。

NAS を脅威にさらさない

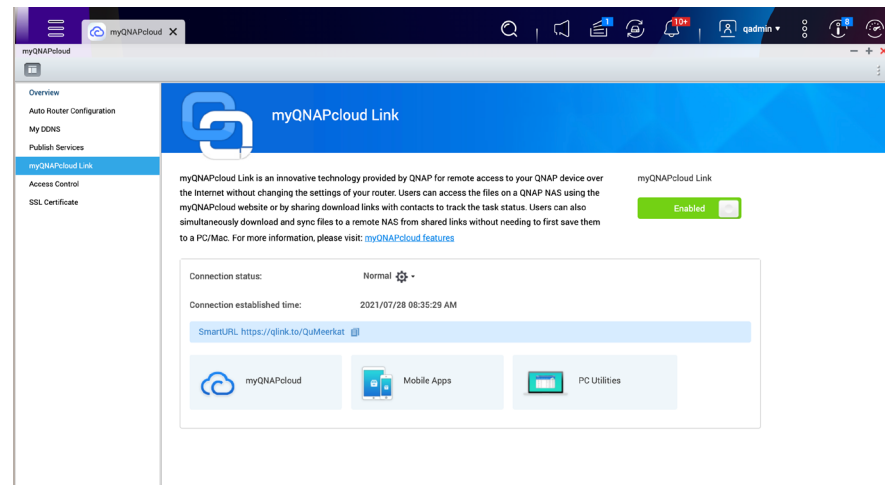
QNAP NAS は、保護せずにインターネットに直接接続すると、スヌーピングに対する脆弱性を抱える可能性があります。攻撃者は、ボットネットや Shodan などのウェブサイトを利用して、デバイスをロックダウンさせたり、攻撃を仕掛ける可能性があります。これは、ルーターやモデムのポートフォワーディング設定によって制御されます。手動フォワーディング、自動ポートフォワーディング (UPnP、Universal Plug and Play) または非武装地帯 (DMZ) を有効にした場合、QNAP NAS はインターネットに直接接続されます。QNAP NAS が直接パブリック IP アドレスを取得する場合 (スタティック / PPPoE / DHCP) も、インターネットへの直接接続となります。

NAS にリモートアクセスする際、最も安全な方法は、セキュアな VPN 接続を確立するか、あるいは myQNAPcloud Link アプリケーションを使用することです。これらの接続方法以外の接続をする場合には、QNAP NAS をルーターやファイアウォールの背後に設置する必要があります。NAS がルーターの背後にあっても、ポートフォワーディングでインターネットに接続されている場合は、ルーターで新しいポート番号を指定してください。22、443、80、8080、8081 というポート番号は使用しないでください。

リモート接続でセキュリティを高めるヒント

NAS の良い点のひとつは、ファイルやサービスをいつでもどのデバイスからでも広くアクセスできるという点です。リモート接続をより簡単に、よりセキュアにするために開発された myQNAPcloud Link アプリケーションは、ファイアウォールを別途設定したり NAS を直接脅威にさらすことなく安全に NAS に接続できます (P2P 接続)。

DDNS サービスでリモート接続するには面倒な設定が必要ですが、myQNAPcloud Link であれば、どこにいてもシンプルなりモート接続が可能です。まるで QNAP NAS を持ち運んでいるかのような接続が可能です。

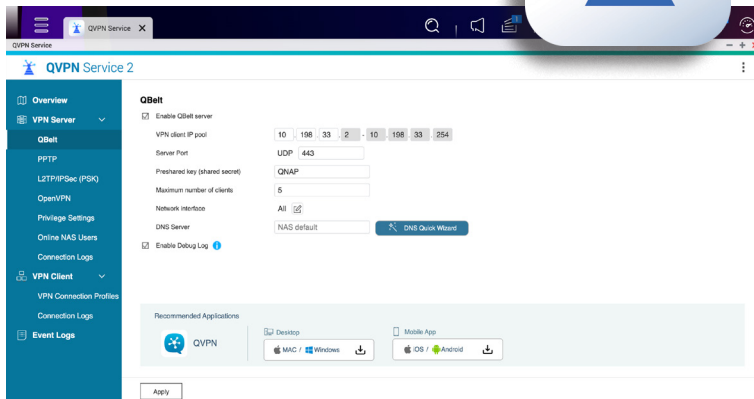


セキュアな VPN 接続を確立する

myQNAPcloud Link リモート接続に加えて、QVPN Service を利用した Virtual Private Network (VPN) サーバーを QNAP NAS に設定することで、デバイスと NAS の間の接続をより安全にする高度なセキュア接続が可能になります。さらに、QNAP NAS を別の VPN サーバーに接続することもできます。

QNAP 独自の QVPN VPN プロトコルである QBelt は、VPN 接続が見つかる可能性をさらに減らすことができます。コンピュータやモバイルデバイスは、QVPN Device Client を使用して、QNAP NAS または QuWAN サーバーの VPN サーバーに接続できます。

QVPN サービス



組み込みセキュリティ機能

ここまで述べてきたような多くのセキュリティ強化アプリケーションに加え、QNAP の NAS オペレーティングシステム (QTS および QuTS hero) には、NAS を保護するためのさらなるレイヤを追加する広範な組み込みセキュリティ機能が備わっています。

- IP ブラックリストとホワイトリスト：ホワイトリストを使用することで認証された IP アドレスだけに接続を制限でき、一方ブラックリストは特定の IP アドレスからの NAS への接続を自動的にブロックします。
- オートブロッキング：NAS へのログインに失敗したユーザー / IP アドレスを、一定回数の試行後ブロックするように設定します。これは、総当たり攻撃を防止するのに有効で、デバイスのセキュリティを高めます。
- HTTPS 接続：NAS への HTTPS 接続を有効にすることで、自己署名 / myQNAPcloud/Let's Encrypt TLS 証明書を使って接続を暗号化し、セキュリティを高めます。
- 複数のバックアップソリューション：スナップショットやバックアップ / 同期など複数の方法により、NAS をリモートサーバーやクラウドストレージサービスにフルバックアップできます。
- 権限の管理：情報セキュリティの制御に加えて、フォルダ権限を設定することでユーザーのプライバシーを高め、秘密情報のセキュリティを確保するだけでなく、規制要件への準拠が可能になります。
- ログおよび通知：システムには、充実したイベントログと通知が内蔵されており、操作の詳しい追跡が可能で、IT メンテナンスの時間節約にもなります。

アンチウイルスソフトウェアのインストール

QTS に組み込まれている無料の ClamAV アンチウイルスに加えて、より高度な保護のために、よく知られているアンチウイルスソフトウェアの McAfee Antivirus を購入できます。QNAP ユーザーは、ウイルスからのデータの保護、感染してしまったファイルの修復、感染ファイルの隔離、そして新しく現れるウイルスに対抗するための最新のウイルス定義の受信を、手動あるいは定期的にスキャンできます。McAfee Antivirus ライセンスは、QNAP Software Store から 3 年までの期間で購入可能です。

未知のリスクの除去

ユーザーアカウントは、組織の要件に基づいて監視および修正されなければなりません。不要になったアカウントは削除し、またはそのアカウントが後で必要になる場合は、権限を取り消しておく必要があります。これは、[コントロールパネル] > [権限] > [ユーザー] から可能です。さらに、ユーザーがインストールしたアプリの監視や、ユーザーアカウントが削除された後に、そのアカウントの必要性の検証も必要です。認識していない、あるいは作成した記憶のないユーザーアカウントを発見した場合は、いつでも削除しなければなりません。



必須	Pro	プレミアム
1年ごとのアンチウイルスNAS用サブスクリプション	2年ごとのアンチウイルスNAS用サブスクリプション	3年ごとのアンチウイルスNAS用サブスクリプション
USD \$25.00 /年	USD \$50.00 /2年	USD \$70.00 /3年
購読する	購読する	購読する

常時待機している QNAP のセキュリティチーム

QNAP は 2018 年に、国際的な非営利組織である MITRE によって、CVE Numbering Authority として認定されました。これにより、QNAP は QNAP 製品のセキュリティ問題に対し、CVE 識別子を割り当てることができます。QNAP の Product Security Incident Response Team (PSIRT) は、世界中からリアルタイムで情報セキュリティ通知、脆弱性、一般に開示された脅威を事前に調査し、脆弱性通知に対して受信後 24 時間以内に対応します。

QNAP ではお客様に対し、QNAP のセキュリティ掲示板を定期的にチェックすること、および QNAP 情報セキュリティニュースレターを購読して最新の情報と更新を入手していただくようお勧めしております。セキュリティ上の問題が発生した場合、QNAP PSIRT チームの推奨案に従い、お客様の NAS にセキュリティの被害が及ばないようにしてください。

Advisory		Status	Impact	CVE	Last Updated	Affected Product(s)
Improper Access Control Vulnerability in Legacy HBS 3 (Hybrid Backup Sync)		Resolved	Critical	CVE-2021-28809	2021-07-06	Certain QNAP NAS
QNAP SA ID: QSA-21-19 First Published: 2021-07-06		Summary: An improper access control vulnerability has been reported to affect certain legacy versions of HBS 3 (Hybrid Backup Sync). If exploited, this vulnerability allows attackers to compromise the security of the operating system. We have already fixed this vulnerability in the following versions of HBS 3 QTS 4.3.6... Learn More				
Multiple Command Injection Vulnerabilities in QTS and QUTS hero		Resolved	Medium	CVE-2021-28802 CVE-2021-28804	2021-06-25	Certain QNAP NAS
Stored XSS Vulnerability in QLog Center		Resolved	Medium	CVE-2020-36196	2021-06-25	Certain QNAP NAS
Stored XSS Vulnerability in Qcenter		Resolved	Medium	CVE-2021-28803	2021-06-25	Certain QNAP NAS
XSS Vulnerability in QTS and QUTS hero		Resolved	Medium	CVE-2020-36194	2021-06-25	Certain QNAP NAS
DNSSpoof Vulnerabilities in QTS		Resolved	Medium	CVE-2020-25684 CVE-2020-25685 CVE-2020-25686	2021-06-28	Certain QNAP NAS



使っている NAS が暗号化攻撃に遭った場合の対処法

ランサムウェア攻撃にはさまざまな被害と攻撃ベクトルがあり、ひとつの攻撃に対して推奨できる一般的な対応を見出すのは困難です。潜在的な攻撃に対する備えとして、毎日のバックアップ、バックアップを複数デバイスに保存、スナップショットとスナップショットバックアップの使用といったバックアップとディザスタリカバリのベストプラクティスに従うことを強くお勧めします。また、最新情報を入手するために、QNAP の情報セキュリティニュースレターを購読するのを忘れなきようご注意ください。

ご自身の NAS やその他のネットワークデバイスが被害を受けている（心当たりのないアプリケーション / サービスによる異常に高い CPU 利用、ログインの失敗、フォルダに不明なファイルがある、あるいはファイルが勝手に暗号化されているなど）ことが疑われる場合、お使いの NAS を直ちにネットワークから切り離し、ネットワークをインターネットから切断してください。NAS を直ちにシャットダウンし*、QNAP Helpdesk から最新情報を受け取ってください。さらに、バックアップの整合性を確認し、被害を受けていないかどうかを確認します。

システムからマルウェアを消去できる可能性があるため、Malware Remover アプリが使用できます。最新バージョンの Malware Remover を使用していることを確認してください。

スナップショットを使用されており、ご自身のスナップショットファイルに影響が及んでいないことが確認できた場合は、スナップショット復元機能を使用してお客様の大事なデータを復元していただけます。

* 多くの場合、最初に攻撃に気づいた時点で NAS をすぐシャットダウンすることが最良の方法です。ごく稀に暗号化攻撃では、NAS のシャットダウン後に解読キーが失われる場合があります。QNAP のセキュリティ掲示に目を配っていただくようお勧めします。

情報セキュリティは QNAP の最優先事項です

QNAP がお約束する情報セキュリティには隙がありません。QNAP は情報セキュリティを積極的に維持し、同社のパートナーやコミュニティの強みを取り入れ、QNAP 製品のセキュリティを高めてお客様の安心に繋がります。

QNAP SYSTEMS, INC.

電話: +886-2-2641-2000 FAX: +886-2-2641-0555 電子メール: 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 © 2021 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。

ここで言及し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。

オランダ (倉庫サービス)

電子メール: nlsales@qnap.com

電話: +31(0)107600830

中国

メール: cnsales@qnap.com

電話: +86-400-028-0079

日本

メール: jpsales@qnap.com

FAX: 03-6435-9686

米国

メール: usasales@qnap.com

電話: +1-909-595-2782

インド

電子メール: indiasales@qnap.com

フランス

電子メール: Frsales@qnap.com

タイ

メール: thsales@qnap.com

電話: +66-2-5415988

ドイツ

電子メール: desales@qnap.com