



# ファイアウォールを制御します

## StorageGRID 11.7

NetApp  
April 12, 2024

# 目次

ファイアウォールを制御します .....	1
外部ファイアウォールでアクセスを制御します .....	1
内部ファイアウォールコントロールを管理します .....	2
内部ファイアウォールを設定します .....	5

# ファイアウォールを制御します

## 外部ファイアウォールでアクセスを制御します

外部ファイアウォールで特定のポートを開いたり閉じたりできます。

StorageGRID 管理ノード上のユーザインターフェイスと API へのアクセスは、外部ファイアウォールで特定のポートを開くか、または閉じることで制御できます。たとえば、システムアクセスを制御する他の方法に加えて、ファイアウォールでテナントが Grid Manager に接続できないようにすることができます。

StorageGRID 内部ファイアウォールを設定する場合は、を参照してください "[内部ファイアウォールを設定します](#)"。

ポート	説明	ポートが開いている場合
443	管理ノードのデフォルトの HTTPS ポート	Web ブラウザと管理 API クライアントは、Grid Manager、Grid 管理 API、Tenant Manager、およびテナント管理 API にアクセスできます。  • 注：* ポート 443 は一部の内部トラフィックにも使用されます。
8443	管理ノード上の制限された Grid Manager ポート	• Web ブラウザと管理 API クライアントは、HTTPS を使用して Grid Manager とグリッド管理 API にアクセスできます。  • Web ブラウザおよび管理 API クライアントは、Tenant Manager またはテナント管理 API にアクセスできません。  • 内部コンテンツに対する要求は拒否されます。
ポート 1	管理ノード上の制限された Tenant Manager ポート	• Web ブラウザと管理 API クライアントは HTTPS を使用して Tenant Manager とテナント管理 API にアクセスできます。  • Web ブラウザおよび管理 API クライアントは、Grid Manager またはグリッド管理 API にアクセスできません。  • 内部コンテンツに対する要求は拒否されます。



シングルサインオン (SSO) は、制限された Grid Manager ポートまたは Tenant Manager ポートでは使用できません。ユーザをシングルサインオンで認証する場合は、デフォルトの HTTPS ポート (443) を使用する必要があります。

### 関連情報

- "[Grid Manager にサインインします](#)"
- "[テナントアカウントを作成する](#)"

## 内部ファイアウォールコントロールを管理します

StorageGRID には、各ノードに内部ファイアウォールがあります。このファイアウォールを使用すると、ノードへのネットワークアクセスを制御できるため、グリッドのセキュリティが強化されます。ファイアウォールを使用して、特定のグリッド環境に必要なポートを除くすべてのポートでネットワークアクセスを禁止します。[Firewall]コントロールページで行った設定変更は、各ノードに展開されます。

Firewallコントロールページの3つのタブを使用して、グリッドに必要なアクセスをカスタマイズします。

- 特権アドレスリスト：このタブを使用して、選択したポートへのアクセスを許可します。[Manage external access]タブを使用して閉じたポートにアクセスできるIPアドレスまたはサブネットをCIDR表記で追加できます。
- 外部アクセスの管理：このタブを使用して、デフォルトで開いているポートを閉じるか、以前閉じていたポートを再度開きます。
- 信頼されていないクライアントネットワーク：このタブを使用して、ノードがクライアントネットワークからのインバウンドトラフィックを信頼するかどうかを指定します。

このタブでは、信頼されていないクライアントネットワークが設定されている場合に開く追加のポートを指定することもできます。これらのポートから、Grid Manager、Tenant Manager、またはその両方へのアクセスを提供できます。

このタブの設定は、[外部アクセスの管理]タブの設定よりも優先されます。

- 信頼されていないクライアントネットワークを使用するノードは、そのノードに設定されているロードバランサエンドポイントポート（グローバル、ノードインターフェイス、およびノードタイプにバインドされたエンドポイント）の接続のみを受け入れます。
- 信頼されていないクライアントネットワークでは、ロードバランサエンドポイントが設定されていない場合でも、[Untrusted Client Network]タブで開いている追加のポートがすべて開いています。
- 信頼されていないクライアントネットワークでは、[Manage external networks]タブの設定に関係なく、ロードバランサエンドポイントのポートと選択された追加ポート\_のみが開いています。
- 信頼されている場合は、[Manage external access]タブで開いたすべてのポートおよびクライアントネットワークで開いているロードバランサエンドポイントにアクセスできます。



あるタブで行った設定は、別のタブで行ったアクセス変更に影響を与える可能性があります。すべてのタブの設定を確認して、ネットワークが想定どおりに動作することを確認してください。

内部ファイアウォールコントロールを設定するには、を参照してください ["ファイアウォールコントロールを設定します"](#)。

外部ファイアウォールとネットワークセキュリティの詳細については、を参照してください ["外部ファイアウォールでアクセスを制御します"](#)。

## [Privileged address list]タブと[Manage external access]タブ

特権アドレスリストタブでは、閉じられているグリッドポートへのアクセスを許可する1つ以上のIPアドレスを登録できます。[Manage external access]タブでは、選択した外部ポートまたは開いているすべての外部ポート（デフォルトではグリッド以外のノードからアクセス可能なポート）への外部アクセスを閉じることができます。多くの場合、この2つのタブを一緒に使用して、グリッドに必要な正確なネットワークアクセスをカスタマイズできます。



特権IPアドレスには、デフォルトで内部グリッドポートへのアクセスはありません。

### 例1: メンテナンスタスクにジャンプホストを使用します

ネットワーク管理にジャンプホスト（セキュリティ強化ホスト）を使用するとします。次の一般的な手順を使用できます。

1. 特権アドレスリストタブを使用して、ジャンプホストのIPアドレスを追加します。
2. [Manage external access]タブを使用して、すべてのポートをブロックします。



ポート443と8443をブロックする前に、特権IPアドレスを追加してください。ブロックされたポートに現在接続されているユーザ（ユーザを含む）は、自分のIPアドレスが特権アドレスリストに追加されていないかぎり、Grid Managerにアクセスできません。

設定を保存すると、グリッド内の管理ノードのすべての外部ポートが、ジャンプホストを除くすべてのホストに対してブロックされます。これにより、ジャンプホストを使用して、グリッドでより安全にメンテナンスタスクを実行できるようになります。

### 例2: Grid ManagerとTenant Managerへのアクセスを制限する

セキュリティ上の理由から、Grid ManagerとTenant Managerへのアクセスを制限するとします。次の一般的な手順を使用できます。

1. [Manage external access]タブのトグルを使用して、ポート443をブロックします。
2. [Manage external access]タブのトグルを使用して、ポート8443へのアクセスを許可します。
3. [Manage external access]タブのトグルを使用して、ポート9443へのアクセスを許可します。

設定を保存すると、ホストはポート443にアクセスできなくなりますが、引き続きGrid Managerにはポート8443経由で、Tenant Managerにはポート9443経由でアクセスできます。

### 例3: 敏感なポートをロックダウンします

機密性の高いポートとそのポート上のサービス（たとえば、ポート22のSSH）をロックダウンするとします。次の一般的な手順を使用できます。

1. サービスへのアクセスを必要とするホストにのみアクセスを許可するには、特権アドレスリストタブを使用します。
2. [Manage external access]タブを使用して、すべてのポートをブロックします。



ポート443と8443をブロックする前に、特権IPアドレスを追加してください。ブロックされたポートに現在接続されているユーザ（ユーザを含む）は、自分のIPアドレスが特権アドレスリストに追加されていないかぎり、Grid Managerにアクセスできません。

設定を保存すると、特権アドレスリストのホストでポート22とSSHサービスを使用できるようになります。要求の送信元インターフェイスに関係なく、他のすべてのホストはサービスへのアクセスを拒否されます。

#### 例4：未使用のサービスへのアクセスを無効にします

ネットワークレベルでは、使用する予定のない一部のサービスを無効にすることができます。たとえば、Swiftアクセスを許可しない場合は、次の一般的な手順を実行します。

1. [Manage external access]タブのトグルを使用して、ポート18083をブロックします。
2. [Manage external access]タブのトグルを使用して、ポート18085をブロックします。

設定を保存すると、ストレージノードでSwift接続は許可されなくなりますが、ブロックされていないポートで他のサービスへのアクセスは引き続き許可されます。

### [信頼されていないクライアントネットワーク]タブ

クライアントネットワークを使用している場合は、明示的に設定されたエンドポイントまたはこのタブで選択した追加のポートでのみインバウンドクライアントトラフィックを受け入れることで、StorageGRID を悪意のある攻撃から保護できます。

デフォルトでは、各グリッドノードのクライアントネットワークは *trusted\_* です。つまり、StorageGRID はデフォルトで、すべてののグリッドノードへのインバウンド接続を信頼します "[使用可能な外部ポート](#)"。

各ノードのクライアントネットワークを「*untrusted\_*」に指定することで、StorageGRID システムに対する悪意ある攻撃の脅威を軽減できます。ノードのクライアントネットワークが信頼されていない場合、ノードはロードバランサエンドポイントとして明示的に設定されたポートと、[Firewall]制御ページの[Untrusted Client Network]タブを使用して指定した追加のポートでのみインバウンド接続を受け入れます。を参照してください "[ロードバランサエンドポイントを設定する](#)" および "[ファイアウォールコントロールを設定します](#)"。

#### 例 1：ゲートウェイノードが HTTPS S3 要求のみを受け入れる

ゲートウェイノードで、HTTPS S3 要求を除くクライアントネットワーク上のすべてのインバウンドトラフィックを拒否するとします。この場合、次の一般的な手順を実行します。

1. から "[ロードバランサエンドポイント](#)" ページで、HTTPS経由のS3用のロードバランサエンドポイントをポート443に設定します。
2. [Firewall control]ページで、[Untrusted]を選択して、ゲートウェイノードのクライアントネットワークを信頼されていないネットワークとして指定します。

設定を保存すると、ポート 443 での HTTPS S3 要求と ICMP エコー（ping）要求を除き、ゲートウェイノードのクライアントネットワーク上のすべてのインバウンドトラフィックが破棄されます。

#### 例 2：ストレージノードが S3 プラットフォームサービス要求を送信する

あるストレージノードからのアウトバウンドS3プラットフォームサービストラフィックは有効にするが、クライアントネットワークではそのストレージノードへのインバウンド接続は禁止するとします。この場合は、次の手順を実行します。

- [Firewall]制御ページの[Untrusted Client Networks]タブで、ストレージノード上のクライアントネットワークが信頼されていないことを指定します。

設定を保存すると、ストレージノードはクライアントネットワークで受信トラフィックを受け入れなくなりますが、設定されているプラットフォームサービスのデスティネーションへのアウトバウンド要求は引き続き許可します。

### 例3：Grid Managerへのアクセスをサブネットに制限する

Grid Managerに特定のサブネットに対するアクセスのみを許可するとします。次の手順を実行します。

1. 管理ノードのクライアントネットワークをサブネットに接続します。
2. [Untrusted Client Network]タブを使用して、クライアントネットワークを信頼されていないものとして設定します。
3. タブの\*[信頼されていないクライアントネットワークで開くポートの追加]\*セクションで、ポート443または8443を追加します。
4. [Manage external access]タブを使用して、すべての外部ポートをブロックします（サブネット外のホストに対して特権IPアドレスが設定されているかどうかに関係なく）。

設定を保存すると、指定したサブネットのホストだけがGrid Managerにアクセスできるようになります。他のすべてのホストはブロックされます。

## 内部ファイアウォールを設定します

StorageGRID ノードの特定のポートへのネットワークアクセスを制御するようにStorageGRID ファイアウォールを設定できます。

作業を開始する前に

- を使用して Grid Manager にサインインします "[サポートされている Web ブラウザ](#)"。
- これで完了です "[特定のアクセス権限](#)"。
- の情報を確認しておきます "[ファイアウォールコントロールを管理します](#)" および "[ネットワークのガイドライン](#)"。
- 管理ノードまたはゲートウェイノードが明示的に設定されたエンドポイントでのみインバウンドトラフィックを受け入れるように設定する場合は、ロードバランサエンドポイントを定義しておきます。



クライアントネットワークの設定を変更する際、ロードバランサエンドポイントが設定されていないと、既存のクライアント接続が失敗することがあります。

このタスクについて

StorageGRID には、各ノードに内部ファイアウォールがあります。このファイアウォールを使用して、グリッドのノードの一部のポートを開いたり閉じたりできます。[Firewall]制御タブを使用して、グリッドネットワーク、管理ネットワーク、およびクライアントネットワークでデフォルトで開いているポートを開いたり閉じたりできます。閉じているグリッドポートにアクセスできる特権IPアドレスのリストを作成することもできます。クライアントネットワークを使用している場合は、ノードがクライアントネットワークからのインバウンドトラフィックを信頼するかどうかを指定できます。また、クライアントネットワークの特定のポートへのアクセスを設定できます。

グリッドの外部のIPアドレスに対して開くポートの数を絶対に必要なポートだけに制限すると、グリッドのセキュリティが強化されます。3つのファイアウォールコントロールタブのそれぞれの設定を使用して、必要なポートだけが開いていることを確認します。

ファイアウォールコントロールの使用法（例を含む）の詳細については、を参照してください ["ファイアウォールコントロールを管理します"](#)。

外部ファイアウォールとネットワークセキュリティの詳細については、を参照してください ["外部ファイアウォールでアクセスを制御します"](#)。

## ファイアウォールコントロールにアクセスします

### 手順

1. \* configuration > Security > Firewall control \*を選択します。

このページの3つのタブについては、を参照してください ["ファイアウォールコントロールを管理します"](#)。

2. 任意のタブを選択して、ファイアウォールコントロールを設定します。

これらのタブは任意の順序で使用できます。1つのタブで設定した設定では、他のタブで実行できる操作は制限されません。ただし、1つのタブで設定を変更すると、他のタブで設定されたポートの動作が変更される可能性があります。

## 特権アドレスリスト

特権アドレスリストタブを使用して、デフォルトで閉じられているポート、または外部アクセスの管理タブの設定によって閉じられているポートへのアクセスをホストに許可します。

権限付きIPアドレスとサブネットには、デフォルトで内部のグリッドアクセスはありません。また、[Manage external access]タブでブロックされていても、ロードバランサエンドポイントと、[Privileged address list]タブで開いている追加のポートにアクセスできます。



[特権アドレスリスト]タブの設定は、[信頼されていないクライアントネットワーク]タブの設定を上書きすることはできません。

### 手順

1. 特権アドレスリストタブで、閉じたポートへのアクセスを許可するアドレスまたはIPサブネットを入力します。
2. 必要に応じて、\*[Add another IP address or subnet in CIDR notation]\*を選択して、権限付きクライアントを追加します。



特権リストにできるだけ少ないアドレスを追加します。

3. 必要に応じて、\*[特権IPアドレスによるStorageGRID 内部ポートへのアクセスを許可する]\*を選択します。を参照してください ["StorageGRID の内部ポート"](#)。



このオプションを使用すると、内部サービスの保護が一部解除されます。可能であれば無効のままにしておきます。



4. [保存 ( Save ) ] を選択します。

## 外部アクセスの管理

[Manage external access] タブでポートを閉じると、特権アドレスリストにIPアドレスを追加しないかぎり、グリッド以外のIPアドレスからポートにアクセスすることはできません。閉じることができるのは、デフォルトで開いているポートだけです。また、閉じたポートのみを開くことができます。



[外部アクセスの管理] タブの設定は、[信頼されていないクライアントネットワーク] タブの設定を上書きすることはできません。たとえば、ノードが信頼されていない場合、クライアントネットワークでポートSSH/22が[外部アクセスの管理] タブで開いていてもブロックされます。[Untrusted Client Network] タブの設定は、クライアントネットワークの閉じているポート（443、8443、9443など）よりも優先されます。

### 手順

1. [外部アクセスの管理]\* を選択します。タブには、グリッド内のノードのすべての外部ポート（デフォルトではグリッド以外のノードからアクセス可能なポート）が表示されます。
2. 次のオプションを使用して、開いたり閉じたりするポートを設定します。
  - 各ポートの横にあるトグルを使用して、選択したポートを開いたり閉じたりします。
  - 表にリストされているすべてのポートを開くには、\*表示されているすべてのポートを開く\* を選択します。
  - 表に示されているすべてのポートを閉じるには、\*[表示されているすべてのポートを閉じる]\* を選択します。



Grid Managerポート443または8443を閉じると、ブロックされたポートに現在接続しているユーザ（ユーザを含む）は、ユーザのIPアドレスが特権アドレスのリストに追加されていないかぎり、Grid Managerにアクセスできなくなります。



テーブルの右側にあるスクロールバーを使用して、使用可能なすべてのポートが表示されていることを確認します。検索フィールドを使用して、ポート番号を入力して外部ポートの設定を検索します。ポート番号の一部を入力できます。たとえば、\*2\* と入力すると、名前に文字列「2」が含まれるすべてのポートが表示されます。

3. [保存 ( Save ) ] を選択します

## Untrusted Client Networkの略

ノードのクライアントネットワークが信頼されていない場合、ノードはロードバランサエンドポイントとして設定されたポート、およびオプションでこのタブで選択した追加のポートでのみインバウンドトラフィックを受け入れます。このタブを使用して、拡張時に追加する新しいノードのデフォルト設定を指定することもできます。



ロードバランサエンドポイントが設定されていないと、既存のクライアント接続が失敗する可能性があります。

タブで設定を変更すると、[外部アクセスの管理]\* タブの設定が上書きされます。

## 手順

1. [信頼されていないクライアントネットワーク]\*を選択します。
2. [Set New Node Default]セクションで、拡張手順 で新しいノードをグリッドに追加する際のデフォルト設定を指定します。

- \* Trusted \* (デフォルト) : 拡張でノードを追加すると、そのクライアントネットワークが信頼されます。
- \* Untrusted \* : 拡張でノードが追加されるときに、そのクライアントネットワークは信頼されません。

必要に応じて、このタブに戻って特定の新しいノードの設定を変更できます。



この設定は、StorageGRID システム内の既存のノードには影響しません。

3. 次のオプションを使用して、明示的に設定されたロードバランサエンドポイントまたは選択した追加のポートでのみクライアント接続を許可するノードを選択します。

- テーブルに表示されたすべてのノードを信頼されていないクライアントネットワークのリストに追加するには、\*[表示されたノードで信頼されていないクライアントネットワーク]\*を選択します。
- テーブルに表示されたすべてのノードを信頼されていないクライアントネットワークのリストから削除するには、\*[表示されたノードで信頼する]\*を選択します。
- 各ポートの横にある切り替えボタンを使用して、選択したノードのクライアントネットワークを[Trusted]または[Untrusted]に設定します。

たとえば、\*表示されているノードで[Untrust on displayed nodes]\*を選択してすべてのノードを[Untrusted Client Network]リストに追加し、個々のノードの横にある切り替えを使用してその1つのノードを[Trusted Client Network]リストに追加できます。



テーブルの右側にあるスクロールバーを使用して、使用可能なすべてのノードが表示されていることを確認します。検索フィールドにノード名を入力して、任意のノードの設定を検索します。名前の一部を入力できます。たとえば、「\* gw \*」と入力すると、名前に文字列「gw」を含むすべてのノードが表示されます。

4. 必要に応じて、信頼されていないクライアントネットワークで開く追加のポートを選択します。これらのポートから、Grid Manager、Tenant Manager、またはその両方へのアクセスを提供できます。

たとえば、メンテナンス目的でクライアントネットワークからGrid Managerにアクセスできるようにする場合にこのオプションを使用します。



これらの追加ポートは、[Manage external access]タブで閉じているかどうかに関係なく、クライアントネットワークで開いています。

5. [保存 ( Save ) ] を選択します。

新しいファイアウォール設定がすぐに適用され、適用されます。ロードバランサエンドポイントが設定されていないと、既存のクライアント接続が失敗する可能性があります。

## 著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。