SonicOS 7

一致オブジェクト

管理者ガイド

SONICWALL®

目次

1

ゾーン

ゾーンとは、アクセス ルールの定義と適用などの管理作業を行うために、1 つ以上のインターフェースを論理的にグループ化したものです。このグループ化は、物理インターフェースのみによる方法よりも単純でより直感的なプロセスです。ゾーン ベース セキュリティは、内部および外部のネットワーク セグメントを強力かつ柔軟に管理する方法であり、これを利用して未承認アクセスや攻撃から内部の重要ネットワーク リソースを切り離し、保護することができます。

ネットワーク セキュリティ ゾーンは、扱いやすくユーザにも設定可能な名前で 1 つ以上のインターフェースを簡単にグループ化し、ゾーン間をトラフィックが通過する際にセキュリティ規則を適用する論理的な手法です。セキュリティ ゾーンによって、ファイアウォール用により柔軟なセキュリティ層が追加されます。ゾーン ベース セキュリティを使用することで、管理者は類似するインターフェースをグループ化して同じポリシーを適用できるので、各インターフェースについて同じポリシーを作成する必要がなくなります。インターフェースの設定方法については、「**ネットワーク > インターフェース**」を参照してください。

SonicOS のゾーンを利用して、ネットワーク内部にセキュリティ ポリシーを適用できます。これにより、ネットワーク リソースを別々のゾーンに分類し、ゾーン間のトラフィックを許可または制限することができます。この方法によって、給与支払いサーバやエンジニアリング コード サーバなどの重要な内部リソースへのアクセスを厳格に制御することができます。

ゾーンでは NAT テーブルを完全に公開でき、トラフィックがゾーン間で転送されるときに送信元アドレスと送信先アドレスを制御することで、インターフェース全体でトラフィックを制御することができます。つまり、NAT を内部で適用することも、VPN トンネルを経由して適用もできます。これはユーザが以前から要望していた機能です。またファイアウォールでは、VPN が VPN ゾーンに論理的にグループ化されたため、NAT ポリシーおよびゾーン ポリシーを使って VPN トラフィックを管理できるようになりました。

トピック:

ゾーンの動 作

セキュリティ ゾーンの動作をわかりやすく模式化して説明してみましょう。複数の部屋がある大きな新築ビルと、ビル内の通路を知らない新入社員のグループがいるとします。このビルには 1 つ以上の出口があります。これは WAN インターフェースと見なすことができます。ビル内の部屋には 1 つ以上のドアがあります。これはインターフェースと見なすことができます。部屋はゾーンと考えられます。各部屋にはたくさんの人がいます。人々は分類さ

れ、ビル内の別々の部屋に割り当てられます。各部屋にいる人は、別の部屋に行くときやビルを出るときに、各部屋の出口に立っている門番に話しかける必要があります。この門番が、ゾーン間/ゾーン内セキュリティ ポリシーです。門番の仕事は、リストを参照して、その人物が別の部屋への通行を許可されているか、またはビルを出ることが許可されているかを確かめることです。その人物は許可されていれば（たとえば、セキュリティ ポリシーで許可されていれば）、ドア（インターフェース）から部屋の外に出ることができます。

廊下に出ると、目的の部屋がどこにあるのか、またはビルの外に出るドアがどこにあるのかを警備員に確認する必要があります。警備員はすべての部屋の場所と、ビルから出入りする方法を知っているため、経路を教えることができます。また、警備員はすべての支店の住所を知っています。これはVPN と見なすことができます。ビルに複数の出入口（WAN インターフェース）がある場合、警備員は指示に応じて（たとえば、緊急の場合や、出入口の通行量を分散する目的のために）第 2 の出入口を使用するように人々を誘導できます。この働きは、WAN 負荷分散と見なすことができます。

ビル内の部屋には複数のドアがあることもあれば、部屋の中にいるグループ同士が親しくないこともあります。例えば、同じ部屋のグループでも、あるグループと別のグループが別々のドアを使用する場合があります。この 2 つのグループは互いを認識しないため、ユーザは門番（セキュリティ ポリシー）に依頼して、別のグループ内にいる話しかけたい人物を指し示してもらう必要があります。門番は、あるグループの人が同じ部屋の別のグループの人に話しかけられないようにすることもできます。これは、ゾーンに複数のインターフェースが関連付けられており、ゾーン内トラフィックが許可されていない場合の例です。

ときおり、人々は支店に出向くこともあれば、支店からやってきてビル内の特定の部屋にいる人を訪問することもあるでしょう。これは VPN トンネルと見なすことができます。警備員と門番は許可されているかどうかを確認してから、トラフィックの通過を許可します。また門番は、別の部屋に行く人やビルを出る人、また別の支店に行く人に、衣装を着るように強制することもできます。これにより、その人物の本当の身分を隠し、別人に見せかけます。このプロセスは、NAT ポリシーと見なすことができます。

事前定義ゾーン

ⓘ | **補足:** ファイアウォールには、デバイスに応じた事前定義ゾーンがあります。

SonicWall セキュリティ装置の事前定義セキュリティ ゾーンは変更できません。

ゾーン	機能
DMZ	通常はパブリックアクセス可能なサーバで使用され、ネットワークの設計に応じて 1 ～ 4 個のインターフェースで構成できます。
LAN	ネットワークの設計に応じて複数個のインターフェースで構成されます。各インターフェースには別々のネットワーク サブネットが接続されますが、グループ化することで 1 つのエンティティとして管理することができます。
MGMT	装置管理に使用され、管理インターフェースだけを含みます。他のゾーンのインターフェースも SonicOS 管理用に有効化できますが、MGMT ゾーン/インターフェースを使用すると、管理専用の独立したゾーンによるセキュリティ強化を図ることができます。
マルチキャスト	IP マルチキャストをサポートします。IP マルチキャストとは、1 つの送信元から同時に複数のホストに IN パケットを送信する手法です。
SSLVPN	SonicWall NetExtender クライアントを使用してリモート アクセスを保護する場合に使用されます。
VPN	安全なリモート接続を簡単に実現するために使用される仮想ゾーンです。

WLAN	SonicWall SonicPoint および SonicWave に対するサポートを提供します。このゾーンを Opt ポートに割り当てると、SonicPoint の規制が適用され、SonicPoint 非対応デバイスから受信されたパケットがすべて自動的に削除されます。WLAN ゾーンでは、以下がサポートされます。 • 接続された SonicPoint および SonicWave を自動的にポーリングして識別する Discovery Protocol (SDP) • プロファイルを使用して SonicPoint および SonicWave を構成するための SonicPoint Simple Provisioning Protocol • 無線とゲスト サービスの設定。
WAN	複数のインターフェースで構成できます。セキュリティ装置の WAN フェイルオーバー機能を使用する場合、WAN ゾーンに 2 つ目のインターネット インターフェースを追加する必要があります。

ⓘ **補足:** インターフェースを 1 つのセキュリティ ゾーンにグループ化しても、そのゾーン内に 1 つのインターフェースを割り当てる必要はあります。

セキュリティ種 別

ⓘ **補足:** ゾーンのセキュリティ種別はデバイスに依存します。

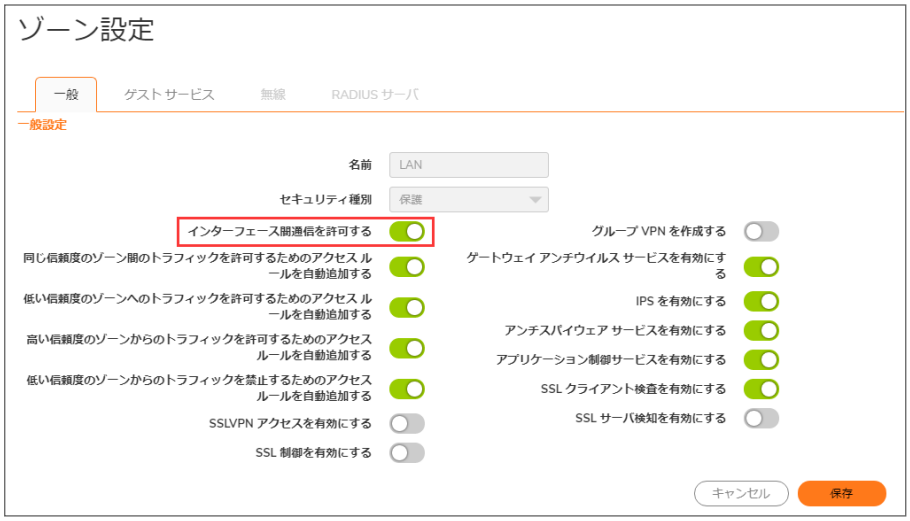
各ゾーンには、そのゾーンの信頼レベルを定義するセキュリティ種別があります。

信頼	最も高い信頼レベルを提供します。これは、保護ゾーンから送信されたトラフィックには、最小限の調査しか行われないことを意味します。保護セキュリティは、セキュリティ装置の LAN (保護) 側であると考えることができます。LAN ゾーンは常に信頼されています。
管理	管理ゾーンおよび管理インターフェースに固有のものであり、これもまた最高レベルの保護を提供します。
暗号化	VPN および SSL VPN ゾーンのみで使用されます。暗号化ゾーンで送受信されるトラフィックはすべて暗号化されます。
無線	ネットワークへの唯一のインターフェースが SonicWall SonicPoint および SonicWave デバイスで構成されている WLAN ゾーンまたはその他のゾーンに適用されます。無線セキュリティ タイプは、SonicPoint および SonicWave のみで使用することが前提となっています。無線ゾーンにインターフェースを配置すると、そのインターフェースで SDP (SonicWall ディスカバリ プロトコル) および SSPP (SonicWall シンプル プロビジョニング プロトコル) が有効になり、SonicPoint および SonicWave の自動検出とプロビジョニングが実行されます。SonicPoint または SonicWave を通過するトラフィックのみが無線ゾーンの通過を許可されます。それ以外のトラフィックはすべて破棄されます。
公開	「信頼されていない」ゾーンよりも高く、「信頼された」ゾーンよりは低い保護レベルを提供します。公開ゾーンは、セキュリティ装置の LAN (保護) 側と WAN (非保護) 側の中間にある安全領域であると考えることができます。例えば、DMZ は公開ゾーンです。DMZから送信されたトラフィックは LAN と WAN の両方に送られるためです。既定では、DMZ からLAN へのトラフィックは拒否されますが、LAN から ANY (すべて) へのトラフィックは許可されます。つまり、LAN 側から開始された接続のみによって DMZ と LAN の間のトラフィックが生成されます。DMZ から既定でアクセスできるのは LAN ではなく、WAN のみです。

非保護	最も低い保護レベルを表します。これは WAN および仮想マルチキャスト ゾーンで使用されます。非保護ゾーンは、セキュリティ装置の WAN（非保護）側と考えることができます。既定では、非保護ゾーンからのトラフィックは明示的なルールがない限り他のゾーン タイプへの入力が許可されませんが、他のゾーン タイプから非保護ゾーンへのトラフィックは入力が許可されます。

インターフェース間通信を許可する

「**ゾーンの追加**」ダイアログの「**インターフェース間通信を許可する**」設定を使用して、ゾーン インスタンスのインターフェース間でトラフィックの通過を許可するアクセス ルールを自動的に作成できます。例えば、LAN ゾーンに **LAN** インターフェースと **X3** インターフェースの両方が割り当てられている場合、LAN ゾーンで「**インターフェース間通信を許可する**」をオンにすることで、これらのインターフェース上のホストに相互通信を許可するために必要なアクセス ルールが作成されます。



ゾーンでの SonicWall セキュリティ サービスの有効化

ゾーン間を通過するトラフィックに対して、SonicWall セキュリティ サービスを有効にすることができます。例えば、WLAN ゾーンで入出力されるトラフィックに対して SonicWall 侵入防御を有効にすることで、内部ネットワーク トラフィックのセキュリティを高めることができます。以下の SonicWall セキュリティ サービスをゾーンで有効にできます。

SSLVPN アクセスを有効にする	このゾーンで SSL VPN セキュア リモート アクセスを有効にします。
SSL 制御を有効にする	このゾーンで SSL 制御を有効にします。これで、このゾーンから開始されるすべての新しい SSL 接続に対して検査が実行されるようになります。「**ポリシー > ファイアウォール > SSL 制御**」ページでまず SSL 制御を全体で有効化しておく必要があります。SSL 制御の詳細については、『*SonicOS 7 セキュリティ設定*』を参照してください。
グループ VPN を作成する	ゾーンの グループ VPN ポリシーを作成すると、「**ネットワーク > SSL VPN > サーバ設定**」の「VPN ポリシー」テーブルに表示されます。「**ネットワーク > SSL VPN > サーバ設定**」で、グループ VPN ポリシーをカスタマイズできます。「**グループ VPN を作成する**」の選択を解除すると、グループ VPN ポリシーは「**ネットワーク > SSL VPN > サーバ設定**」から削除されます。VPN ポリシー作成の詳細については、『*SonicOS 7 接続*』を参照してください。
ゲートウェイ アンチウイルス サービスを有効にする	WLAN ゾーンの同じ「保護」および「公開」セキュリティ種別の複数のインターフェースにゲートウェイ アンチウイルス保護を適用します。
IPS を有効にする	WLAN ゾーンの同じ「保護」および「公開」セキュリティ種別の複数のインターフェースに侵入検知と侵入防御を適用します。
アンチスパイウェア サービスを有効にする	WLAN ゾーンの同じ「保護」および「公開」セキュリティ種別の複数のインターフェースにアンチスパイウェア検出とスパイウェア防御を適用します。
アプリケーション制御サービスを有効にする	WLAN ゾーンの同じ「保護」および「公開」セキュリティ種別の複数のインターフェースにアプリケーション制御ポリシー サービスを適用します。
SSL クライアント検査を有効にする	DPI-SSL クライアントに対してグローバル ベースではなく、ゾーンごとにきめ細かく DPI-SSL を有効にします。
SSL サーバ検知を有効にする	DPI-SSL サーバに対してグローバル ベースではなく、ゾーンごとにきめ細かく DPI-SSL を有効にします。

無線および非無線コントローラ モードの効果

トピック:

- 非無線コントローラ モードを有効にした場合の影響
- 無線コントローラ モードを有効にした場合の影響

非無線コントローラ モードを有効にした場合の影響

非無線コントローラ モードを有効にすると、「**オブジェクト > 一致オブジェクト > ゾーン**」ページが影響を受けます。影響を受ける機能を有効または削除しようとする試みは拒否されます。

- 無線ゾーンの「**編集**」および「**削除**」アイコンが、「**オブジェクト > 一致オブジェクト > ゾーン**」ページで淡色表示になります。
- 内部無線ゾーンは無効になっています。

無線コントローラ モードを有効にした場合の影響

無線コントローラ モードを有効にすると、「**オブジェクト > 一致オブジェクト > ゾーン**」ページが影響を受けます。影響を受ける機能を有効または削除しようとする試みは拒否されます。

- VPN および SSL VPN ゾーンの**編集**および**削除**アイコンが、「**オブジェクト > 一致オブジェクト > ゾーン**」ページで淡色表示になります。
- VPN または SSL VPN、あるいはその両方でゾーンを有効にしようとすると、エラーになります。

一致オブジェクト > ゾーン

トピック:

- ゾーンの設定テーブル
- 新しいゾーンの追加
- ゲスト アクセス用ゾーンの設定
- オープン認証およびソーシャル ログイン用ゾーンの設定
- RADIUS によるキャプティブ ポータル認証用のゾーンの設定
- ユーザ定義ポリシー メッセージ用のゾーンの設定
- ユーザ定義ログイン ページ用ゾーンの設定
- WLAN ゾーンの設定
- ゾーンの削除

ゾーンの設定テーブル

「**ゾーンの設定**」テーブルには、ユーザが作成したゾーンだけでなくSonicWall セキュリティ装置の既定の事前定義ゾーンもすべて表示されます。このテーブルには、各ゾーンの設定に関する以下の状況情報が表示されます。

名前	ゾーンの名前。事前定義されているゾーン名である「**LAN**」、「**WAN**」、「**WLAN**」、「**VPN**」、「**SSLVPN**」、「**MGMT**」、「**MULTICAST**」、「**暗号化**」は変更できません。
セキュリティ種別	セキュリティ種別: セキュリティ タイプは、「**保護**」、「**非保護**」、「**公開**」、「**無線**」、または「**暗号化**」です。
メンバー インターフェース	ゾーンのメンバーであるインターフェース。
インターフェース間通信	チェック マークがある場合、そのゾーンで「**インターフェース間通信を許可する**」設定が有効になっています。
クライアント AV	チェック マークがある場合、そのゾーンに入出力されるトラフィックに対してSonicWall クライアント アンチウイルスが有効になっています。SonicWall クライアント アンチウイルスにより、ゾーン内のすべてのクライアントのアンチウイルス クライアント アプリケーションが管理されます。
クライアント CF	チェック マークがある場合、クライアント コンテンツ フィルタ サービスが有効になっています。
ゲートウェイ AV	チェック マークがある場合、そのゾーンに入出力されるトラフィックに対してSonicWall ゲートウェイ アンチウイルスが有効になっています。SonicWall ゲートウェイ アンチウイルスにより、ファイアウォールのアンチウイルス サービスが管理されます。
アンチスパイウェア	チェック マークがある場合、そのゾーン内のインターフェースを通過するトラフィックに対して SonicWall アンチスパイウェア検出およびスパイウェア防御が有効になっています。
IPS	チェック マークがある場合、そのゾーンに入出力されるトラフィックに対してSonicWall 侵入防御サービスが有効になっています。
アプリケーション制御	チェック マークがある場合、そのゾーンに入出力されるトラフィックに対してアプリケーション制御サービスが有効になっています。
SSL 制御	チェック マークがある場合、そのゾーンに入出力されるトラフィックに対して SSL 制御が有効になっています。これで、このゾーンから開始されるすべての新しい SSL 接続に対して検査が実行されるようになります。
SSL VPN アクセス	チェック マークがある場合、そのゾーンに入出力されるトラフィックに対してSSLVPN セキュア リモート アクセスが有効になっています。
DPI-SSL クライアント	チェック マークがある場合、DPI-SSL クライアントに対して、グローバル ベースではなく、ゾーンごとのきめ細かな DPI-SSL が有効になっています。
DPI-SSL サーバ	チェック マークがある場合、DPI-SSL サーバに対して、グローバル ベースではなく、ゾーンごとのきめ細かな DPI-SSL が有効になっています。

コメント	「**コメント**」アイコンにマウス カーソルを合わせると、ゾーンの構成時に入力したコメントが表示されます。
構成	**編集**アイコンを選択すると、「ゾーンの編集」ダイアログが表示されます。**削除**アイコンを選択すると、ゾーンが削除されます。事前定義ゾーンについては、削除アイコンが淡色表示になっています。こうしたゾーンは削除できません。

新しいゾーンの追加

新しいゾーンを追加するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > ゾーン**」に移動します。
2. **追加**アイコンをクリックします。

3. 新しいゾーンの名前を「**名前**」フィールドに入力します。
4. 「**セキュリティ種別**」で、以下の選択を行います。

保護	信頼レベルが最も高いゾーン（内部 LAN セグメントなど）。
公開	要求される信頼レベルがより低いゾーン（DMZ インターフェースなど）。
無線	WLAN インターフェース。
SSLVPN	コンテンツ フィルタ、クライアント AV 強制、およびクライアント CF サービスが有効なインターフェース。 ⓘ **補足:** このセキュリティ種別を選択すると、このダイアログで「**SSLVPN アクセスを有効にする**」および「**グループ VPN を作成する**」オプションが無効になります。

5. ゾーン内通信を許可する場合は、「**インターフェース間通信を許可する**」を選択します。ゾーン インスタンスのインターフェース間のトラフィック フローを許可するアクセス ルールが自動的に作成されます。このオプションは、既定では選択されています。
6. このゾーンと同じ信頼度の他のゾーンとの間のトラフィックを許可するアクセス ルールを SonicOS に自動的に作成させる場合は、「**同じ信頼度のゾーン間のトラフィックを許可するためのアクセス ルールを自動追加する**」を選択します。例えば、*CUSTOM_LAN -> CUSTOM_LAN または CUSTOM_LAN -> LAN*。このオプションは、既定では選択されています。

   ⓘ **補足:** このオプションと以下のアクセス ルール オプションについては、『*SonicOS ポリシー*』でアクセス ルールに関する情報を参照してください。

7. このゾーンと信頼度の低い他のゾーンとの間のトラフィックを許可するアクセス ルールを SonicOS に自動的に作成させる場合は、「**低い信頼度のゾーンへのトラフィックを許可するためのアクセス ルールを自動追加する**」を選択します。例えば、*CUSTOM_LAN -> WAN または CUSTOM_LAN -> DMZ*。このオプションは、既定では選択されています。
8. このゾーンと信頼度の高い他のゾーンとの間のトラフィックを許可するアクセス ルールを SonicOS に自動的に作成させる場合は、「**高い信頼度のゾーンからのトラフィックを許可するためのアクセス ルールを自動追加する**」を選択します。例えば、*LAN -> CUSTOM_DMZ または CUSTOM_LAN -> CUSTOM_DMZ*。このオプションは、既定では選択されています。
9. このゾーンと信頼度の低いゾーンとの間のトラフィックを禁止するアクセス ルールを SonicOS に自動的に作成させる場合は、「**低い信頼度のゾーンからのトラフィックを拒否するためのアクセス ルールを自動追加する**」を選択します。例えば、*WAN -> CUSTOM_LAN* または *DMZ -> CUSTOM_LAN*。このオプションは、既定では選択されています。
10. ネットワーク ホストのクライアント アンチウイルス サービスを使用して、同じ保護ゾーン、公開ゾーン、または WLAN ゾーンの複数のインターフェースに接続されたクライアントに管理されたクライアント アンチウイルス保護を適用する場合は、「**クライアント AV 強制サービスを有効にする**」を選択します。このオプションは、既定では選択されていません。

    ⓘ **補足:** このオプションは、「セキュリティ種別」からセキュリティ種別を選択するまで、淡色表示で使用できない状態になっています。このオプションと以下のセキュリティ サービス オプションについては、『*SonicOS セキュリティ設定*』でこれらのサービスに関する情報を参照してください。
11. DPI-SSL 強制や SentinelOne AV 強制などの強化された NGAV (Next Generation AV) を実施するには、「DPI-SSL 強制サービスを有効にする」を選択します。このオプションは、既定では選択されていません。NGAV の詳細については、『*SonicOS セキュリティ設定*』を参照してください。
12. このゾーンで SSL VPN セキュア リモート アクセスを有効にする場合は、「**SSLVPN アクセスを有効にする**」を選択します。このオプションは、既定では選択されていません。

    ⓘ **補足:** 「**セキュリティ種別**」で **SSLVPN** を選択すると、このオプションは淡色表示になります。
13. このゾーンに対して、SonicWall グループ VPN ポリシーを自動的に作成する場合は、「**グループ VPN を作成する**」を選択します。「**ネットワーク > SSLVPN > サーバ設定**」で、グループ VPN ポリシーをカスタマイズできます。このオプションは、既定では選択されていません。このオプションは、「セキュリティ種別」として SSLVPN を選択するまで使用でき、このセキュリティ種別をそれ以外のいずれかの種別に変更した後は淡色表示となって使用できない状態になります。

    △ **注意:** **「グループ VPN を作成する」を無効にすると、対応するグループ VPN ポリシーはすべて削除されます。**

    ⓘ **補足:** 「**セキュリティ種別**」で **SSLVPN** を選択すると、このオプションは淡色表示になります。接続オプションの詳細については、『*SonicOS 接続*』を参照してください。

    WAN/WLAN VPN ポリシーのグループ VPN を無効にすると、すべての VPN ポリシーが削除されます。「グループ VPN を作成する」オプションを再度有効にすると、新しい有効な VPN ポリシーが自動的に作成されます。VPN ポリシーをグローバルに無効にしても、自動ルールは削除されません。VPN ポリシーをまったく使用したくない場合は、VPN をグローバルに無効にしてから、VPN 関連のポリシーをすべて削除します。

    グループ VPN ポリシーは、「**ネットワーク > SSLVPN > サーバ設定**」の「VPN ポリシー」テーブルに表示されます。ファイアウォールが工場出荷時の既定の設定で起動されたとき、WAN/WLAN GroupVPN ポリシーは既定で無効になっています。
14. このゾーンで SSL 制御を有効にする場合は、「**SSL 制御を有効にする**」を選択します。これで、このゾーンから開始されるすべての新しい SSL 接続に対して検査が実行されるようになります。このオプションは、既定では選択されていません。

    ⓘ **補足:** SSL 制御は最初に「**ポリシー > ファイアウォール > SSL 制御**」で全体的に有効にしておく必要があります。

15. このゾーンに接続されたすべてのクライアントに対して、セキュリティ装置上でゲートウェイ アンチウイルス保護を適用する場合は、「**ゲートウェイ アンチウイルス サービスを有効にする**」を選択します。SonicWall ゲートウェイ アンチウイルスにより、セキュリティ装置のアンチウイルス サービスが管理されます。このオプションは、既定では選択されていません。
16. 同じ保護ゾーン、公開ゾーン、または WLAN ゾーンの複数のインターフェースに侵入検知と侵入防御を適用する場合は、「**IPS を有効にする**」を選択します。このオプションは、既定では選択されていません。
17. WLAN ゾーンと同じ信頼または公開セキュリティ種別の複数のインターフェースにアンチスパイウェア検出とスパイウェア防御を適用する場合は、「**アンチスパイウェア サービスを有効にする**」を選択します。このオプションは、既定では選択されていません。
18. WLAN ゾーンと同じ信頼または公開セキュリティ種別の複数のインターフェースにアプリケーション制御ポリシーを適用する場合は、「**アプリケーション制御サービスを有効にする**」を選択します。このオプションは、既定では選択されていません。アプリケーション制御の詳細については、『*SonicOS ポリシー*』を参照してください。
19. DPI-SSL クライアントに対してグローバル ベースではなく、ゾーンごとのきめ細かな DPI-SSL を有効にするには、「**SSL クライアント検査を有効にする**」を選択します。このオプションは、既定では選択されていません。
20. DPI-SSL サーバに対してグローバル ベースではなく、ゾーンごとのきめ細かな DPI-SSL を有効にするには、「**SSL サーバ検査を有効にする**」を選択します。このオプションは、既定では選択されていません。
21. 「**保存**」をクリックします。これで、新しいゾーンが セキュリティ装置 に追加されます。

ゲスト アクセス用ゾーンの設定

ⓘ | **重要: 非保護、暗号化、SSL VPN** または **管理**のゾーンをゲスト アクセス用に構成することはできません。

SonicWall ユーザ ゲスト サービスは、訪問者や信頼されていないネットワーク ノード用に無線ゲスト パスおよびロックダウンされたインターネット専用のネットワーク アクセスを簡単に作成できるソリューションを提供します。この機能は、WLAN、LAN、DMZ、または任意の公開/半公開ゾーンの無線ユーザまたは有線ユーザにまで拡張できます。

ゲスト サービス機能を構成するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > ゾーン**」に移動します。
2. ゲスト サービスを追加したいゾーンの「**編集**」をクリックします。「**ゾーンの設定**」ダイアログが表示されます。
3. 「**ゲスト サービス**」タブをクリックします。

4. 「**ゲスト サービスを有効にする**」オプションを選択します。その他すべてのオプションが使用可能になりますが、これらは既定では選択されていません。
5. ゲスト サービスについて、以下の設定オプションを選択します。

ゲスト間の通信を有効にする	ゲストがこのゾーンに接続している他のユーザと直接通信することを許可します。
外部ゲスト認証を有効にする	選択したデバイスまたはネットワークから接続するゲストを、アクセスに先立って認証する必要があります。このオプションを選択すると、「**構成**」が使用可能になります。 ⓘ **補足:** このオプションを選択すると、次の 4 つのオプションが淡色表示になり、使用できなくなります。
キャプティブ ポータル認証を有効にする	RADIUS 認証によってカスタマイズされたログイン ページを作成できます。このオプションを選択すると、「**構成**」が使用可能になります。このオプションの設定については、「RADIUS によるキャプティブ ポータル認証用のゾーンの設定」を参照してください。
認証なしにポリシー ページを有効にする	WLAN ゾーンで SonicPoint または SonicWave に初めて接続するユーザに対して、ゲスト サービスの利用に関するポリシー ページが表示されます。ゲスト ユーザは、ユーザ名とパスワードの入力ではなく、ポリシーの承諾によって認証されます。このオプションを選択すると、「**構成**」が使用可能になります。HTML カスタマイズ可能なポリシーの使用に関するページを設定するには、「**構成**」を選択します。このオプションの設定については、「ユーザ定義ポリシー メッセージ用のゾーンの設定」を参照してください。
個別認証ページ	ユーザがネットワークに最初に接続するときに、ユーザを個別認証ページにリダイレクトします。このオプションを選択すると、「**構成**」が使用可能になります。個別認証ページを設定するには、「**構成**」をクリックします。このオプションの設定については、「ユーザ定義ログイン ページ用ゾーンの設定」を参照してください。

認証後に表示するページを有効にする	認証が成功した直後にユーザを指定のページに振り向けます。このオプションを選択すると、「**認証後に表示するページ**」フィールドが使用可能になります。
認証後に表示するページ	認証後に表示されるページの URL をフィールドに入力します。
ゲスト認証のバイパス	何らかのユーザレベル認証が既に使用されている環境に、ゲスト サービス機能を統合することを許可します。この機能によって認証プロセスが自動化され、認証を要求することなく無線ユーザに無制限の無線ゲスト サービスを割り当てることができます。選択すると、このオプションのドロップダウン メニューが使用可能になります。以下から選択します。 • **すべての MAC アドレス**（既定） • アドレス オブジェクト • アドレス グループ • MAC オブジェクトの作成 ⓘ **補足:** この機能は、無制限のゲスト サービス アクセスが必要な場合、またはアップストリームにある別のデバイスによって認証が適用される場合にのみ使用してください。
SMTP トラフィックのリダイレクト先	このゾーンに入ってくる SMTP トラフィックを指定の SMTP サーバにリダイレクトします。選択すると、このオプションのドロップダウン メニューが使用可能になります。以下から選択します。 • アドレス オブジェクト • アドレス オブジェクトの作成
通信を禁止するネットワーク	指定されたネットワークへのトラフィックを遮断します。選択すると、このオプションのドロップダウン メニューが使用可能になります。以下から選択します。 • アドレス オブジェクト • アドレス オブジェクト グループ • アドレス オブジェクトの作成 • アドレス オブジェクト グループの作成
通信を許可するネットワーク	選択したネットワークへのトラフィックが、ゲスト サービスが有効になっているゾーンを通過することを自動的に許可します。選択すると、このオプションのドロップダウン メニューが使用可能になります。以下から選択します。 • アドレス オブジェクト • アドレス オブジェクト グループ • アドレス オブジェクトの作成 • アドレス オブジェクト グループの作成
最大ゲスト数	このゾーンへの接続を許可されるゲスト ユーザの最大数を指定します。最小値は 1、最大値は 4500 で、既定の設定は **10** になっています。

6. 「**保存**」をクリックすると、これらの設定がこのゾーンに適用されます。

ⓘ **補足:** アドレス オブジェクトおよびアドレス オブジェクト グループの作成については、SonicOS の「**オブジェクト > 一致オブジェクト > アドレス**」を参照してください。

オープン認証およびソーシャル ログイン用ゾーンの設定

SonicOS はオープン認証 (OAuth) とソーシャル ログインをサポートしています。

- OAuth は、ユーザによるアプリケーション間でのデータの共有を支援します。
- ソーシャル ログインは、さまざまなソーシャル メディアでのログイン処理を簡素化します

RADIUS によるキャプティブ ポータル認証用のゾーンの設定

RADIUS によるキャプティブ ポータル認証を構成するには、以下の手順に従います

1. 「**ゾーンの設定**」ダイアログで、「**ゲスト サービス**」タブをクリックします。

2. 「**ゲスト サービスを有効にする**」オプションを選択します。オプションが使用可能になります。
3. 「**キャプティブ ポータル認証を有効にする**」を選択します。「**構成**」が使用可能になります。
4. 「**構成**」をクリックします。

5. 「**ユーザ定義ポータル認証設定**」セクションで:
    a. 内部キャプティブ ポータル ベンダーの URL を「**内部キャプティブ ポータル ベンダー URL**」フィールドに入力します。
    b. 外部キャプティブ ポータル ベンダーの URL を「**外部キャプティブ ポータル ベンダー URL**」フィールドに入力します。
6. 「**RADIUS サーバ属性の設定**」セクション:
    a. 「**キャプティブ ポータル ウェルカム URL 送信元**」からキャプティブ ポータル ウェルカム URL のソースを選択します。
        - **RADIUS から**（既定）。ステップ *c* に進みます。
        - **ユーザ定義**。次のオプションが使用可能になります。
    b. ウェルカム URL を「**ユーザ定義キャプティブ ポータル ウェルカム URL**」フィールドに入力します。
    c. セッション タイムアウト制限の送信元を「**セッション タイムアウト送信元**」から選択します。
        - **RADIUS から**（既定）。ステップ *f* に進みます。
        - **ユーザ定義**。次のオプションが使用可能になります。
    d. 「**ユーザ定義無動作時 タイムアウト送信元**」からセッション タイムアウト期間のタイプを選択します。
        - 分
        - 時間
        - 日（既定）
    e. 制限値をフィールドに入力します。
    f. 無動作時タイムアウトの送信元を「**無動作時タイムアウト送信元**」から選択します。
        - **RADIUS から**（既定）。ステップ 7 に進みます。
        - **ユーザ定義**。次のオプションが使用可能になります。
    g. 「**ユーザ定義無動作時 タイムアウト送信元**」から無動作時タイムアウト期間のタイプを選択します。
        - 分
        - 時間
        - 日（既定）
    h. 期間の制限値をフィールドに入力します。
7. 「**RADIUS 認証設定**」セクションで、「**RADIUS 認証方式**」から認証方式を選択します。
    - CHAP（既定）
    - PAP – 暗号化

- PAP –平文

8. 「**保存**」をクリックします。

ユーザ定義ポリシー メッセージ用のゾーンの設定

ユーザ定義ポリシー メッセージを構成するには、以下の手順に従います

1. 「**ゾーンの設定**」ダイアログで、「**ゲスト サービス**」タブをクリックします。
2. 「**ゲスト サービスを有効にする**」オプションを選択します。オプションが使用可能になります。
3. 「**認証なしにポリシー ページを有効にする**」を選択します。「**構成**」が使用可能になります。
4. 「**構成**」をクリックします。

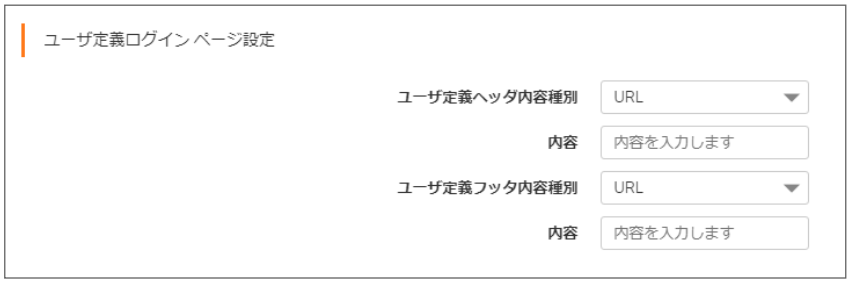
5. ゲストが利用する場合のポリシーを「**ゲスト使用ポリシー**」フィールドに入力します。テキストには HTML フォーマットを含めることができます。
6. 入力したポリシー メッセージをプレビューするには、「**プレビュー**」を選択します。
7. 無動作タイムアウトを指定するには、「**無動作時タイムアウト**」フィールドにタイムアウト値を入力します。
8. タイムアウトのタイプを選択します。
    - 秒
    - 分（既定）
    - 時間
    - 日
9. 「**ポリシー ページを自動的に承諾する**」を選択します。このオプションは、既定では選択されていません。
10. 「**保存**」をクリックします。

ユーザ定義ログイン ページ用ゾーンの設定

ユーザ定義ログイン ページを構成するには、以下の手順に従います

1. 「**ゾーンの設定**」ダイアログで、「**ゲスト サービス**」タブをクリックします。

2. 「**ゲスト サービスを有効にする**」オプションを選択します。オプションが使用可能になります。
3. 「**ユーザ定義認証ページ**」オプションを選択します。
4. 「**構成**」ボタンをクリックします。



5. 「**ユーザ定義ヘッダ内容種別**」について、以下を選択します。
   - URL
   - テキスト
6. URL またはテキストを「**内容**」フィールドに入力します。
7. 「**ユーザ定義フッタ内容種別**」について、以下を選択します。
   - URL
   - テキスト

8. URL またはテキストを「**内容**」フィールドに入力します。
9. 「**保存**」をクリックします。

WLAN ゾーンの設定

WLAN ゾーンを構成するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > ゾーン**」に移動します。
2. 次の手順を実行します。
   - 新規のゾーンを設定する場合は、「**追加**」をクリックします。
   - 既存のゾーンを設定する場合は、WLAN ゾーンの**編集**アイコンを選択します。

   「**ゾーンの設定**」ダイアログが表示されます。

   ⓘ **補足:** ゾーンによっては、「**ゲスト サービス**」、「**無線**」、および「**RADIUS サーバ**」のビューも表示されます。「**一般**」ビューの構成方法については、「新しいゾーンの追加」を参照してください。
3. 新しいゾーンを作成する場合は、「**セキュリティ種別**」から「**無線**」を選択します。「**ゲスト サービス**」、「**無線**」、および「**RADIUS サーバ**」が表示されます。
4. ゾーン インスタンスのインターフェース間でトラフィックの通過を許可するアクセス ルールの作成を自動化するには、「**インターフェース間通信を許可する**」を選択します。例えば、LAN ゾーンに LAN インターフェースと X3 インターフェースの両方が割り当てられている場合、LAN ゾーンで「**インターフェース間通信を許可する**」を有効にすることで、これらのインターフェース上のホストに相互通信を許可するために必要なアクセス ルールが作成されます。このオプションは、既定では選択されていません。
5. 「**無線**」タブを選択します。

6. 「**SonicPoint/SonicWave 設定**」セクションで、このゾーンに接続されるすべての SonicPoint/SonicWave に適

用するプロファイルを「**SonicPoint/SonicWave プロビジョニング プロファイル**」で選択します。個別に異なる設定を構成していない限り、このゾーンに接続する SonicPoint/SonicWave は、SonicPoint/SonicWave プロビジョニング プロファイルの設定によって自動的にプロビジョニングされます。SonicPoint/SonicWave プロビジョニング プロファイルについては、『*SonicOS 接続ガイド*』を参照してください。

ⓘ **補足:** 自動プロビジョニングの設定では、必要に応じて、「**自動プロビジョニング**」フィールドを選択すると、プロファイルに関連付けられた SonicPoint/SonicWave が、プロファイルの変更時に自動的にプロビジョニングされるようになります。このオプションは、既定では選択されていません。

7. このゾーンに接続されるすべての SonicPointN/Ni/Ne にプロファイルを適用するには、「**SonicPointN/Ni/Ne プロビジョニング プロファイル**」を選択します。個別に異なる設定を構成していない限り、このゾーンに接続される SonicPointN/Ni/Ne は、SonicPoint プロビジョニング プロファイルの設定によって自動的にプロビジョニングされます。既定のプロビジョニング プロファイルは「**SonicPointN**」です。
8. このゾーンに接続されるすべての SonicPointNDR にプロファイルを適用するには、「**SonicPoint N Dual Radio プロビジョニング プロファイル**」を選択します。個別に異なる設定を構成していない限り、このゾーンに接続される SonicPointNDR は、SonicPointNDR プロビジョニング プロファイルの設定によって自動的にプロビジョニングされます。既定のプロビジョニング プロファイルは「**SonicPointNDR**」です。
9. このゾーンに接続されるすべての SonicPointACe/ACi/N2 にプロファイルを適用するには、「**SonicPointACe/ACi/N2 プロビジョニング プロファイル**」を選択します。個別に異なる設定を構成していない限り、このゾーンに接続される SonicPointACe/ACi/N2 は、SonicPointACe/ACi/N2 プロビジョニング プロファイルの設定によって自動的にプロビジョニングされます。既定のプロビジョニング プロファイルは「**SonicPointACe/ACi/N2**」です。
10. このゾーンに接続されるすべての SonicPointNDR にプロファイルを適用するには、「**SonicWave プロビジョニング プロファイル**」を選択します。個別に異なる設定を構成していない限り、このゾーンに接続される SonicPointNDR は、SonicPointNDR プロビジョニング プロファイルの設定によって自動的にプロビジョニングされます。既定のプロビジョニング プロファイルは「**SonicWave**」です。
11. SonicWall SonicPoints からのトラフィックのみ WLAN ゾーンのインターフェースへの入力を許可するには、「**SonicPoint/SonicWave により生成された通信のみ許可する**」を選択します。これにより、WLAN のセキュリティが最大限に高められます。このオプションは、既定では選択されています。トラフィックの送信元が無線接続かどうかに関係なく、WLAN ゾーンですべてのトラフィックを許可する場合は、このオプションをオフにしてください。

   ⓘ **ヒント:** 送信元が無線接続かどうかに関係なく、WLAN ゾーンですべてのトラフィックを許可するには、「**SonicPoint/SonicPointN により生成された通信のみ許可する**」をオフにします。

   ⓘ **補足:** ゲスト サービスの設定については、「ゲスト アクセス用ゾーンの設定」を参照してください。RADIUS サーバの設定情報については、「RADIUS サーバの設定」を参照してください。
12. オプションで、「**SonicPoint/SonicWave 2.4Hz 自動チャンネル選択として 1、6、および 11 のみを優先する**」を選択します。このオプションは、既定では選択されていません。

    ⓘ **重要:** このオプションは、SonicPointN/AC 2.4Hz 自動チャンネル選択として 1、6、および 11 を優先する場合にのみ有効にします。
13. 「**保護された信頼できるライセンス マネージャからの SonicWave ライセンス有効化を強制する**」を選択します。

    △ **注意: このオプションは、安全で信頼できるライセンス マネージャからのライセンス アクティベーションを強制します。ライセンス キーセットの手動入力は許可されません。この設定は、テクニカル サポートから指示された場合にのみ変更してください。**
14. 「**SonicPoint/SonicWave 管理を無効にする**」を選択して、この WLAN のすべての管理機能を無効にします。
15. 適宜、以下の操作を行います。
    - RADIUS サーバを構成する場合は、「RADIUS サーバの設定」に進みます。
    - これらの設定を WLAN ゾーンに適用する場合は、「**保存**」をクリックします。

RADIUS サーバの設定

ⓘ | **補足:** 「RADIUS サーバ」タブは、デバイスによって有効/無効になります。

RADIUS サーバを構成するには、以下の手順に従います

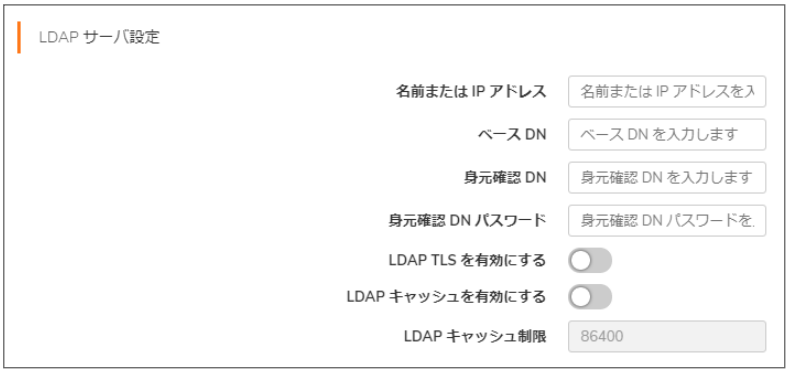
1. 「**オブジェクト > 一致オブジェクト > ゾーン**」に移動します。
2. 次の手順を実行します。
   - 新規のゾーンを設定する場合は、「**追加**」をクリックします。
   - 既存のゾーンを設定する場合は、WLAN ゾーンの**編集**アイコンを選択します。

   「**ゾーンの設定**」ダイアログが表示されます。

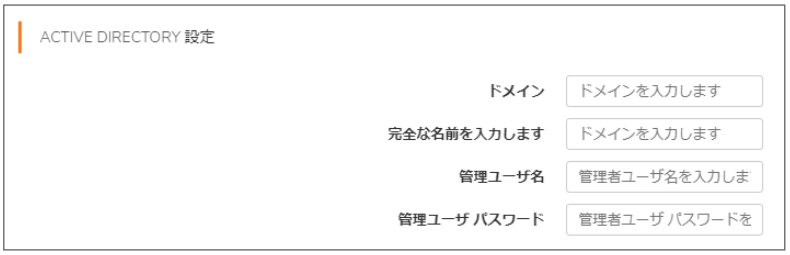
   ⓘ | **補足:** ゾーンによっては、「**ゲスト サービス**」、「**無線**」、および「**RADIUS サーバ**」のビューも表示されます。「**一般**」ビューの構成方法については、「新しいゾーンの追加」を参照してください。
3. 新しいゾーンを作成する場合は、「**セキュリティ種別**」から「無線」を選択します。「**ゲスト サービス**」、「**無線**」、および「**RADIUS サーバ**」が表示されます。
4. 「**RADIUS サーバ**」タブをクリックします。

5. 「**ローカル RADIUS サーバを有効にする**」を選択します。他のオプションが使用可能になります。
6. 「**インターフェース毎のサーバ数**」に、インターフェースあたりの RADIUS サーバ番号の数を入力します。最小値は 1、最大値は 512、既定値は **2** です。

7. 「**RADIUS サーバ ポート**」フィールドに RADIUS サーバのポートを入力します。既定値は **1812** です。
8. 「**RADIUS クライアント パスワード**」フィールドに RADIUS クライアントのパスワードを入力します。
9. 必要に応じて、「**ローカル RADIUS サーバ TLS キャッシュの持続時間を有効にする**」を選択します。このオプションは、既定では選択されていません。「**キャッシュの持続時間 (h)**」フィールドが使用可能になります。
    - 「**キャッシュの持続時間 (h)**」フィールドに存続期間を時間単位で入力します。最小 (既定値) は **1** 時間、最大は 99999 時間です。
10. 「**データベース アクセス設定**」からデータベース アクセス方法を選択します。
    - **LDAP サーバ** – さらにオプションが表示されます。*ステップ 11* に進みます。



    - **Active Directory** – さらにオプションが表示されます。*ステップ 18* に進みます。



11. 「**名前または IP アドレス**」フィールドに LDAP サーバの名前または IP アドレスを入力します。
12. 「**ベース DN**」フィールドに基本識別名を入力します。
13. 「**身元確認 DN**」フィールドに本人識別名を入力します。
14. 「**身元確認 DN パスワード**」フィールドに識別名パスワードを入力します。
15. LDAP Transport Layer Security (TLS) を有効にするには、「**LDAP TLS を有効にする**」を選択します。このオプションは、既定では選択されていません。
16. LDAP キャッシュを有効にするには、「**LDAP キャッシュを有効にする**」を選択します。「LDAP キャッシュ制限」フィールドが使用可能になります。
    - 「LDAP キャッシュ制限」フィールドに存続期間を秒単位で入力します。最小値は 1、最大値は 99999、既定値は **86400** です
17. *ステップ 22* に進みます。
18. 「**ドメイン**」フィールドに、ドメイン名を入力します。
19. 「**完全な名前を入力します**」フィールドに Active Directory で使用するフルネーム (氏名) を入力します。
20. 「**管理ユーザ名**」フィールドに管理者ユーザのユーザ名を入力します。
21. 「**管理ユーザ パスワード**」フィールドに管理者ユーザのパスワードを入力します。
22. 「**保存**」をクリックします。

DPI-SSL をゾーン単位できめ細かく制御する設定

DPI-SSL をきめ細かく制御する設定では、グローバル ベースではなくゾーン単位で DPI-SSL を有効化することができます。ゾーンごとに DPI-SSL クライアントと DPI-SSL サーバの両方を有効にできます。詳細については、『*SonicOS セキュリティ設定ガイド*』を参照してください。

ユーザポリシー ページへの自動リダイレクトを有効にする

SonicOS を使用すると、ゲストを自動的にゲスト使用ポリシー ページにリダイレクトできます。この機能（ゼロタッチ ポリシー ページのリダイレクトとも呼ばれる）を有効にすると、ゲスト ユーザは自動的に guest-user ポリシー ページにリダイレクトされます。この機能を無効にした場合、ゲストは「**適用**」をクリックする必要があります。

ユーザ ポリシー ページへの自動リダイレクトを有効にするには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > ゾーン**」に移動します。
2. 次のいずれかをクリックします。
   - 新しいゾーンを追加する**追加**アイコン。
   - 既存ゾーンの**編集**アイコン。

   「**ゾーンの設定**」ダイアログが表示されます。
3. 新しいゾーンの名前を「**名前**」フィールドに入力します。
4. ドロップダウン メニューから「**セキュリティ種別**」を選択します。
5. 「**ゲスト サービス**」タブをクリックします。

6. 「**ゲスト サービスを有効にする**」オプションをクリックします。

7. 「**認証なしにポリシー ページを有効にする**」オプションをクリックします。
8. 「**構成**」ボタンをクリックします。「**個別認証ページの設定**」ダイアログが表示されます。

9. 「**ポリシー ページを自動的に承諾する**」オプションを選択します。このオプションは、既定では選択されていません。
10. 「**保存**」をクリックします。

ゾーンの削除

ユーザが作成したゾーンを削除するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > ゾーン**」に移動します。

   ⓘ **補足:** 事前定義ゾーンについては、**削除**アイコンは使用できません。このようなゾーンを削除することはできません。ユーザが作成したゾーンはすべて削除できます。
2. 削除するゾーンの「構成」列で、**削除**アイコンをクリックします。

ユーザが作成した 1 つまたは複数のゾーンを削除するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > ゾーン**」に移動します。

   ⓘ **補足:** これらのチェックボックスは事前定義ゾーンでは使用できません。このようなゾーンを削除することはできません。ユーザが作成したゾーンはすべて削除できます。
2. 削除するゾーンのチェックボックスを選択し、「**ゾーンの削除**」をクリックします。

2

アドレス

アドレス オブジェクトを使用することで、一度定義したエンティティを SonicOS インターフェース全体の複数の参照インスタンスで再利用することができます。アドレス オブジェクトの作成は単に IP アドレスを入力するよりも手間がかかりますが、アドレス オブジェクトは SonicOS の管理機構を補完する目的で実装されており、それによって以下の特徴が実現されています。

- **ゾーンの関連付け** — ホスト、MAC、および FQDN のアドレス オブジェクトを定義する際は、明示的にゾーンを指定する必要があります。インターフェースのほとんどの領域（アクセス ルールなど）では、指定されたゾーンは参照のためにしか使われません。指定されたゾーンが機能上の目的で使用されるのは、「アドレス オブジェクト」ドロップダウン リストの項目をコンテキストに合わせて正確に表示するために利用される場合と、ユーザおよびグループに割り当てる VPN アクセスを定義する場合です。アドレス オブジェクトを使用して VPN アクセスを定義する際には、アクセス ルール自動作成プロセスによってアドレス オブジェクトのゾーンが参照され、そのルールを割り当てるべき VPN [ゾーン] の共通部分が適切に決定されます。例えば、LAN ゾーンに属する *192.168.168.200* というホスト アドレス オブジェクトが *Trusted Users* ユーザ グループの VPN アクセスに追加された場合、自動的に作成されるアクセス ルールは VPN LAN ゾーンに割り当てられます。
- **管理と処理** – 多用途向けの一群のアドレス オブジェクト種別を SonicOS インターフェース全域で簡単に使用できるため、（アクセス ルールを定義する場合など）処理の定義や管理を素早く行うことができます。また、アドレス グループのメンバーは単純な操作によって簡単に追加または削除できるので、それを参照するルールやポリシーを直接操作する必要なしに、ルールやポリシーの内容を効率的に変更することができます。
- **再利用性** — オブジェクトを定義する必要があるのは一度だけで、定義したオブジェクトは必要に応じて何度でも容易に参照できます。

例えば、IP アドレスが *67.115.118.80* の内部ウェブ サーバがあるとします。アクセス ロールや NAT ポリシーを作成する際に IP アドレスを繰り返し入力するのではなく、アドレス オブジェクトを使用して、例えば *マイ ウェブ サーバ* という 1 つのエンティティを IP アドレス *67.115.118.80* のホスト アドレス オブジェクトとして作成します。この**マイ ウェブ サーバ**アドレス オブジェクトは、アドレス オブジェクトを定義条件として使用する任意の設定画面で、ドロップダウン メニューから簡単に選択できます。

トピック:

アドレス オブジェクトの種別

ネットワーク アドレスの表現にはさまざまな種類があるため、下の表に示す複数のアドレス オブジェクト種別が用意されています。

種別	定義
ホスト	IP アドレスとゾーン関連によって 1 つのホストを定義します。ホスト アドレス オブジェクトのサブネット マスクは、単独のホストを識別できるように自動的に 32 ビット (*255.255.255.255*) に設定されます。例えば、マイ ウェブ サーバの IP アドレスは *67.115.118.110* であり、既定のネットマスクは *255.255.255.255* です。
範囲	連続する IP アドレスの範囲を定義します。範囲アドレス オブジェクトにはサブネット マスクは関連付けられませんが、内部ロジックでは通常、指定範囲の各アドレスは32 ビットでマスクされたホスト オブジェクトとして扱われます。例えば、*公開サーバ*の開始 IP アドレスは *67.115.118.66*、終了 IP アドレスは *67.115.118.90* です。この範囲内の 25 個の個々のホストアドレスはすべてこのアドレス オブジェクトに含まれます。
ネットワーク	複数のホストを構成するという点で範囲オブジェクトと似ていますが、アドレスの上限と下限を指定するのではなく、有効なサブネット マスクによってアドレスの境界を定義します。ネットワーク アドレス オブジェクトは、ネットワークのアドレスとそれに対応するサブネット マスクによって定義する必要があります。例えば、ネットワーク値が *67.115.118.64*、サブネット マスクが *255.255.255.224* の *公開ネットワーク*のアドレスは、*67.115.118.64* ～ *67.115.118.95* になります。一般的なルールとして、ネットワークの最初のアドレス (ネットワーク アドレス) およびネットワークの最後のアドレス (ブロードキャスト アドレス) はホストに割り当てることはできません。
MAC	ハードウェア アドレスまたは IPv4/IPv6 MAC (メディア アクセス コントロール) アドレスによってホストを識別できます。MAC アドレスは、ハードウェアの製造元によって有線または無線のすべてのネットワーク デバイスに個別に割り当てられており、変更できないようになっています。MAC アドレスは、6 バイト 16 進数形式で表記される 48 ビット値です。例えば、*アクセス ポイント*の MAC アドレスは *00:06:01:AB:02:CD* です。MAC アドレスは、セキュリティ装置の ARP キャッシュを参照することにより、IP アドレスに解決されます。MAC アドレス オブジェクトは、SonicPoint や SonicWave ID などの

	SonicOS 全体の無線構成のさまざまなコンポーネントによって使用され、無線スキャン中に検出された無線アクセス ポイントの BSSID (Basic Service Set Identifier または WLAN MAC) を認証します。MAC アドレス オブジェクトを使用して、ホストがゲストサービス認証をバイパスできるようにすることもできます。
FQDN	例えば *www.sonicwall.com* など、ホストの IPv4/IPv6 による完全修飾ドメイン名 (FQDN) を使ってホストを識別できます。FQDN は、セキュリティ装置の構成で指定されている DNS サーバを使用して IP アドレスに解決されます。ワイルドカード エントリは、DNS サーバに送信されたクエリに対する応答によってサポートされます。

アドレス グループについて

SonicOS には、アドレス オブジェクトと他のアドレス グループをアドレス グループにグループ化する機能があります。アドレス グループを定義することで、参照の効率を向上させることができます。アドレス グループは、ホスト アドレス オブジェクト、範囲アドレス オブジェクト、ネットワーク アドレス オブジェクトを任意に組み合わせて構成できます。例えば、「*公開グループ*」にはホスト アドレス オブジェクトである「 ウェブ サーバ」と、範囲アドレス オブジェクトである「*公開サーバ*」を含められるので、実質的に IP アドレス *67.115.118.66*～*67.115.118.90*、および IP アドレス *67.115.118.110* を表すことができます。

動的アドレス オブジェクト (MAC および FQDN) は別にグループ化する必要がありますが、IP ベースのアドレス オブジェクトのグループに MAC アドレス オブジェクトを追加すること自体は安全です。IP アドレス オブジェクトのグループに追加された MAC アドレス オブジェクトは、処理のコンテキストにおいてその参照が無意味なとき (NAT ポリシーの場合など) には無視されます。

アドレス グループは、*RADIUS プール* アドレス グループとして WLAN ゾーン設定の「**ローカル RADIUS サーバを有効にする**」オプションをオンにするなど、特定の機能を有効にすると自動的に作成され、その機能を無効にすると削除されます。

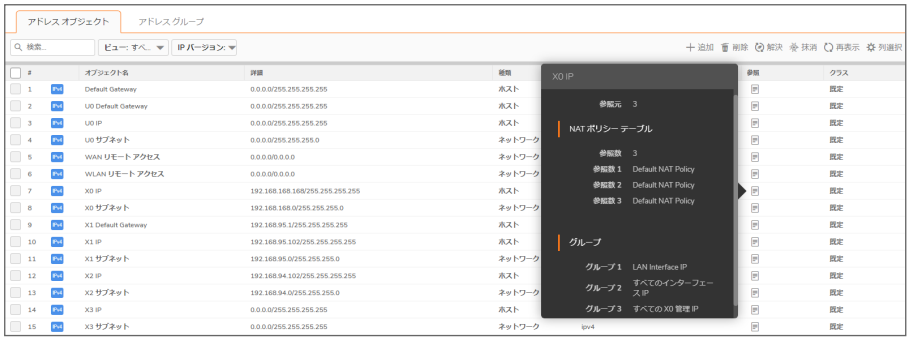
アドレス オブジェクト/グループの UUID について

UUID (Universally Unique Identifier) は、36 文字の文字列 (32 文字の英数字と 4 つのハイフン) です。SonicWall ネットワーク セキュリティ装置上でアドレスオ ブジェクト/グループなどのエンティティを一意に識別するために使用されます。SonicOS UUID は、システムによって生成される読み取り専用の内部値です。以下の性質があります。

- UUID はネットワーク全体で SonicWall エンティティを一意に表します。
- UUID は、エンティティの作成時に生成され、エンティティの削除時に削除されます。削除されると再利用されません。
- エンティティが変更されても、UUID は変わりません。
- UUID は、装置を工場出荷時の既定の設定で再起動すると再生成されます。

既定では、UUID は表示されません。UUID の表示は、内部的な設定によってコントロールされます。内部設定の詳細については、SonicWall テクニカル サポートまでお問い合わせください。

表示状態になると、UUID は各オブジェクト/グループの種別に対応するテーブルに現れます。



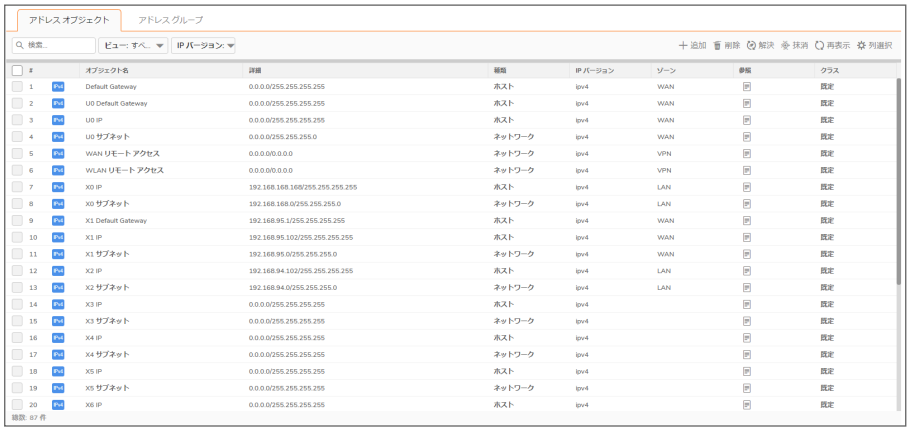
UUID のおかげで次の機能が促進されます。

- 管理インターフェースのグローバル検索機能で UUID を使用してアドレス オブジェクト/グループを検索できます。
- UUID 付きのオブジェクト/グループが UUID 付きの別のエンティティから参照されている場合、参照カウントと参照元のエンティティを表示するには、「**アドレス**」ページの「**オブジェクト**」の下にある「**コメント**」列にマウスカーソルを重ねます。

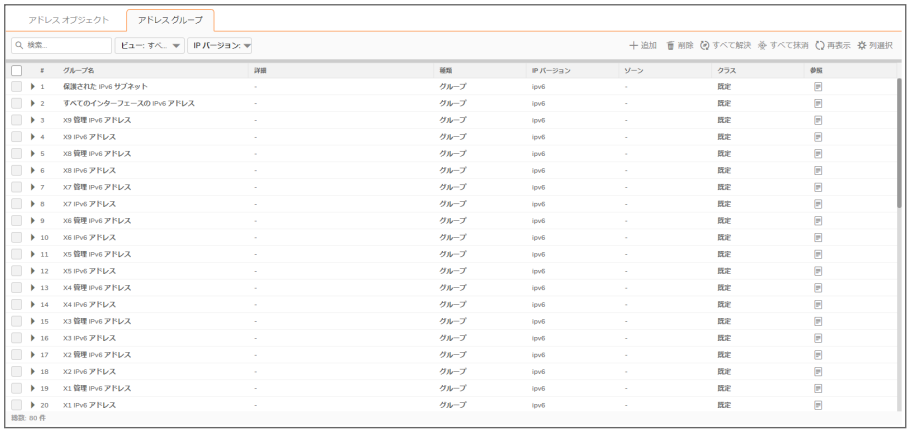
アドレス ページ

アドレス ページには 2 つのタブがあります。

アドレス オブジェクト



アドレス グループ



この 2 つの画面は似ており、同じような機能を備えていますが、いくつかの違いがあります。

このページで使用できる機能の詳細については、以下を参照してください。

- 共通の機能
- エントリの並べ替え

共通の機能

「**アドレス オブジェクト**」および「**アドレス グループ**」画面には共通の機能が含まれ、各テーブルには同じ列見出しが含まれます。

それぞれのテーブルの下部には、テーブル内のエントリ数が表示されます。

トピック:

- 共通の機能
- 共通の列見出し

共通の機能

機能	説明
検索	検索文字列を入力すると、その文字列を含むエントリのみが表示されます。検索文字列の大文字と小文字は区別されます。
ビュー	「**既定**」を選択してシステムで作成された既定のエントリのみを表示するか、「**ユーザ定義**」を選択してユーザ定義エントリのみを表示するか、あるいは「**すべて**」を選択してすべてのエントリを表示します。既定で選択されている表示種別は「**すべて**」

機能	説明
	です。
IP バージョン	IPv4 エントリだけを表示するには「**IPv4**」、IPv6 エントリのみを表示するには「**IPv6**」、すべてのエントリを表示するには「**IPv4 と IPv6**」を選択します。既定で選択されている IP バージョンは「**IPv4 と IPv6**」です。
追加	アドレス オブジェクトまたはアドレス グループを追加する場合にクリックします。
削除	「**削除**」を選択すると、選択したユーザ定義エントリがテーブルから削除されます。既定のエントリは削除できません。
すべて削除	「**すべて削除**」を選択すると、すべてのユーザ定義エントリがテーブルから削除されます。既定のエントリは削除できません。
すべて解決	「**すべて解決**」を選択すると、テーブル内のすべての MAC または FQDN アドレス オブジェクトが解決されます。
すべて抹消	「**すべて抹消**」を選択すると、MAC または FQDN エントリから古い情報が削除されます。MAC アドレス オブジェクトの場合は ARP 情報、FQDN アドレス オブジェクトの場合は DNS TTL 値です。
再表示	「**再表示**」をクリックすると、表示が更新されます。

共通の列見出し

列見出し	説明
チェックボックス	クリックして個別エントリを選択します。 ⓘ | **補足:** 既定のアドレス オブジェクトと既定のアドレス グループは削除できません。
#	テーブル内のエントリの番号。この番号は、列を降順と昇順のどちらで並べ替えるかに応じて変化します。「**アドレス グループ**」画面には、そのグループのエントリを展開または折りたたむことができる小さな三角形が表示されます。
名前	アドレス オブジェクトまたはアドレス グループ エントリの一意の名前。アドレス グループ エントリが展開されている場合、この列に次の情報が表示されます。 • アドレス グループの各メンバーの一意の名前。 • アドレス グループにメンバーがない場合は、「登録がありません」という文字列。
詳細	アドレス オブジェクトの詳細として該当するアドレスやマスクが表示されます。アドレス グループ エントリでは、この列は空白になります。ただし、エントリを展開すると、グループのメンバーの詳細が表示されます。
種別	「**ホスト**」、「**ネットワーク**」、「**範囲**」、「**MAC アドレス**」、「**FQDN**」など、アドレス オブジェクトの種別が表示されます。アドレス グループでは、種別は「**グループ**」です。エントリを展開すると、各メンバーの種別が表示されます。
IP バージョン	アドレス オブジェクトまたはアドレス グループのメンバーの IP バージョンが表示されます。**IPv4**、**IPv6**、または**混在**
ゾーン	アドレス オブジェクトまたはアドレス グループ メンバーの割り当てられたゾーンが表示されます。

列見出し	説明
クラス	アドレス オブジェクトまたはアドレス グループが**既定**（システム定義）または**個別**（ユーザ定義）のいずれであるかが表示されます。
コメント	**コメント** アイコンにマウス カーソルを重ねると、エントリに関する次のような詳細を示すポップアップ情報が表示されます。

- **アドレス オブジェクト** – 以下の情報が表示されます。

  - アドレス オブジェクトの名前
  - 参照元: – アドレス オブジェクトの参照元と、参照された回数。参照されたことのないアドレス オブジェクトの場合は、このセクションに「*0*」と表示されます。
  - グループ: – アドレス オブジェクトが所属するグループのリスト。
  - 構成: – アドレス オブジェクトにマウス カーソルを重ねると、各エントリの**編集**および**削除**アイコンが表示されます。削除できるのは、ユーザ定義アドレス オブジェクトのみです。また、編集できるのは、個別エントリと一部の既定のエントリのみです。編集または削除できないエントリのアイコンは淡色表示になります。
- **アドレス グループ** – 以下の情報が表示されます。

列見出し	説明

- アドレス グループの名前
- 参照元: – アドレス グループの参照元と、参照された回数。参照されたことのないアドレス グループの場合は、このセクションに「0」と表示されます。
- グループ: – アドレス グループが所属するグループのリスト。
- 構成: – アドレス グループにマウス カーソルを重ねると、各エントリの**編集**および**削除**アイコンが表示されます。削除できるのは、ユーザ定義アドレス グループのみです。また、編集できるのは、個別エントリと一部の既定のエントリのみです。編集または削除できないエントリのアイコンは淡色表示になります。

エントリの並べ替え

「**アドレス オブジェクト**」画面と「**アドレス グループ**」画面には、アドレス オブジェクトとアドレス グループを見やすくするためのテーブルが表示されます。

テーブルのエントリを並べ替えるには、列見出しを選択します。登録は昇順または降順で並べ替えられます。列登録の右側にある矢印が、並べ替え状況を示します。下向きの矢印は昇順を意味します。上向きの矢印は、降順（アルファベット A–Z または上から 0 から始まる数字）を示します。

既定のアドレス オブジェクトおよびアドレス グループ

「**既定**」表示には、ファイアウォールの既定のアドレス オブジェクトおよびアドレス グループが表示されます。一方の画面で「**既定**」表示を選択すると、他方の画面でもこの表示が選択されます。既定のアドレス オブジェクトのエントリは変更や削除ができませんが、既定のアドレス グループは変更や削除が可能です。そのため、次のようになっています。

- 「**アドレス オブジェクト**」画面では、**編集**アイコンと**削除**アイコンは淡色表示になっています。
- 「**アドレス グループ**」画面では、**編集**アイコンはほとんどのエントリで、**削除**アイコンは少数を除くすべてのエントリで淡色表示になっています。編集または削除が可能なエントリでは、そうした操作に必要なアイコンが使用可能になっています。

既定の Pref64 アドレス オブジェクト

NAT64 機能をサポートするために、SonicOS では既定のネットワーク アドレス オブジェクトである *Pref64* が提供されています。これは NAT64 ポリシーのための変換前の送信先であり、常に *pref64::/n* となります。**ネットワーク**種別のアドレス オブジェクトを作成すると、すべてのアドレスを *pref64::/n* で表して、NAT64 を実行できるすべての IPv6 クライアントを表すことができます。例:

よく使用されるプレフィックスの *64:ff9b::/96* は、SonicOS によって自動的に作成されます。Pref64 に関する詳細は、「**ポリシー > NAT ルール**」セクションを参照してください。

既定の、悪意のあるアドレス グループ

SonicOS は、悪意のある無線アクセス ポイントとデバイスに対応する 2 つの既定のアドレス グループを提供しています。

- すべての悪意のあるアクセス ポイント
- すべての悪意のあるデバイス

無線侵入検知と防御 (WIDP) が有効になっている場合、SonicWave 装置はアクセス ポイントとしても、SonicWall ネットワークに接続された不正アクセス ポイントを検知するセンサーとしても機能します。検出された悪意のあるアクセス ポイントを「すべての悪意のあるアクセス ポイント」アドレス グループに自動的に追加できます。また、検出された悪意のあるデバイスを「すべての悪意のあるデバイス」アドレス グループに自動的に追加できます。悪意のあるアクセス ポイントに関連するオプションを有効にする方法については、『*SonicOS 接続管理ガイド*』の「*高度な IDP の設定*」を参照してください。

アドレス オブジェクトの追加

アドレス オブジェクトは、NAT ポリシー、アクセス ルール、サービスを設定する前に定義する必要があります。

アドレス オブジェクトを追加するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > アドレス > アドレス オブジェクト**」ページに移動します。
2. 「**アドレス オブジェクト**」画面で、ページの上部にある「**追加**」を選択して、「アドレス オブジェクトの追加」ダイアログを表示します。

3. 「**名前**」フィールドに、ネットワーク アドレス オブジェクトのわかりやすい一意の名前を入力します。
4. 「**ゾーンの割り当て**」ドロップダウン リストからアドレス オブジェクトのゾーンを選択します。
5. 「**種別**」ドロップダウンリストから次のいずれかを選択し、「**種別**」を選択すると表示される関連フィールドを入力します。

- **ホスト** – 「**IP アドレス**」フィールドに IP アドレスを入力します。

- **範囲** – 「**開始アドレス**」フィールドと「**終了アドレス**」フィールドに開始アドレスと終了アドレスを入力します。

- 「**ネットワーク** – 「**ネットワーク**」および「**ネットマスク/接頭辞長**」フィールドに、ネットワーク IP アドレスとネットマスク（255.255.255.0 など）または接頭辞長（24 など）を入力します。

- **FQDN** – 「**FQDN ホスト名**」フィールドに、個々のサイトまたはサイトの範囲（ワイルドカード ‘*’ を使用）のドメイン名を入力します。必要に応じて、「**DNS 登録の TTL の手動設定**」を選択し、「**TTL**

(120 ～ 86400s)」フィールドに存続時間を秒単位で入力します。最小値は 120、最大値は 86400 です。

- MAC－「**MAC アドレス**」フィールドに MAC アドレス（00:11:f5:1b:e3:cf など）を入力します。既定では、「**マルチホーム**」オプションが選択されています。

6. 「**保存**」をクリックします。

アドレス オブジェクトの編集

ⓘ | **補足:** 編集できるのは、ユーザ定義アドレス オブジェクトと一部の既定のアドレス オブジェクトのみです。

アドレス オブジェクトを編集するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > アドレス > アドレス オブジェクト**」ページに移動します。
2. アドレス オブジェクトの「**構成**」列で**編集**アイコンをクリックします。「アドレス オブジェクトの編集」ウィンドウが開き、「**アドレス オブジェクトの追加**」ウィンドウと同じ設定項目が表示されます（「アドレス オブジェクトの追加」を参照してください）。
3. 「**OK**」をクリックします。

ユーザ定義アドレス オブジェクトの削除

ⓘ | **補足:** 削除できるのは、ユーザ定義アドレス オブジェクトのみです。

ユーザ定義アドレス オブジェクトを削除するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > アドレス > アドレス オブジェクト**」ページに移動します。
2. アドレス オブジェクトの「**構成**」列で**削除**アイコンをクリックします。
3. 確認のダイアログ ボックスで「**OK**」を選択し、アドレス オブジェクトを削除します。

1 つ以上のユーザ定義アドレス オブジェクトを削除するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > アドレス > アドレス オブジェクト**」ページに移動します。
2. 削除するエントリのチェックボックスを選択します。

3. ページ上部にある「**削除**」をクリックします。
4. 確認のダイアログ ボックスで「**OK**」をクリックし、アドレス オブジェクトを削除します。

すべてのユーザ定義アドレス オブジェクトを削除するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > アドレス > アドレス オブジェクト**」ページに移動します。
2. ページ上部にある「**すべて削除**」を選択します。
3. 確認のダイアログ ボックスで「**OK**」をクリックし、すべてのユーザ定義アドレス オブジェクトを削除します。

MAC または FQDN アドレス オブジェクトの消去

「抹消」は、MAC または FQDN アドレス オブジェクトから古い ARP または DNS 情報を削除するために使用します。

MAC または FQDN アドレス オブジェクトを抹消するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > アドレス > アドレス オブジェクト**」ページに移動します。
2. ページの上部にある「**消去**」をクリックします。

すべての MAC または FQDN アドレス オブジェクトを抹消するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > アドレス > アドレス オブジェクト**」ページに移動します。
2. ページの上部にある「**すべて消去**」をクリックします。

アドレス グループの作成

ファイアウォールに追加されたアドレス オブジェクトの数が増えてきたら、アドレスのグループを作成することで、アドレスやアクセス ポリシーの管理を容易にすることができます。グループに加えた変更は、アドレス グループ内の各オブジェクトに適用されます。アドレス グループには、アドレス オブジェクトだけでなく、他のアドレス グループも含めることができます。

アドレス オブジェクトを追加するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > アドレス**」ページに移動します。
2. ページの上部にある「**アドレス グループ**」タブをクリックします。
3. 「**アドレス グループ**」画面で「**追加**」をクリックすると、「**アドレス グループの追加**」ダイアログが表示されます。

4. グループに付ける説明的な一意の名前を「**名前**」フィールドに入力します。
5. リストから目的のアドレス オブジェクトまたはグループを選択し、右矢印をクリックします。選択した項目が右側のリストに移動します。**Ctrl** キーまたは **Shift** キーを押しながら複数の項目を選択します。

   グループから項目を削除するには、右の列で項目を選択し、左矢印を選択します。選択した項目は、右側のリストから左側のリストに移動します。グループからすべての項目を削除するには、「**すべての項目の選択解除**」アイコンをクリックします。
6. 「**保存**」をクリックします。

アドレス グループの編集

ⓘ **補足:** 編集できるのはユーザ定義および一部の規定のアドレス グループのみです。削除できるのはユーザ定義アドレス グループのみです。

アドレス グループを編集するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > アドレス**」ページに移動します。
2. ページの上部にある「**アドレス グループ**」タブをクリックします。
3. アドレス グループの「**構成**」列で、**編集**アイコンをクリックします。「アドレス グループの編集」ウィンドウが表示されます。
4. 名前を変更するには、「**名前**」フィールドを編集します。
5. リストから目的のアドレス オブジェクトまたはグループを選択し、右矢印をクリックします。選択した項目が右側のリストに移動します。**Ctrl** キーまたは **Shift** キーを押しながら複数の項目を選択します。

   グループから項目を削除するには、右の列で項目を選択し、左矢印を選択します。選択した項目は、右側のリストから左側のリストに移動します。グループからすべての項目を削除するには、「**すべての項目の選択解除**」アイコンをクリックします。
6. 「**保存**」をクリックします。

アドレス グループの削 除

ⓘ | **補足:** カスタム アドレス グループだけを削除できます。

カスタム アドレス グループを削除するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > アドレス >アドレス グループ**」ページに移動します。
2. アドレス グループの「**構成**」列で、**削除**アイコンをクリックします。
3. 確認のダイアログ ボックスで「**OK**」を選択し、アドレス グループを削除します。

1 つ以上のカスタム アドレス グループを削除するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > アドレス >アドレス グループ**」ページに移動します。
2. 削除するエントリのチェックボックスを選択します。
3. ページ上部にある「**削除**」をクリックします。
4. 確認のダイアログ ボックスで「**OK**」をクリックし、アドレス グループを削除します。

すべてのカスタム アドレス グループを削除するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > アドレス >アドレス グループ**」ページに移動します。
2. ページ上部にある「**すべて削除**」を選択します。
3. 確認のダイアログ ボックスで「**OK**」をクリックし、すべてのカスタム アドレス グループを削除します。

動 的アドレス オブジェクトの使 用

SonicOS では初期のバージョンから常に、ユーザ インターフェースのほとんどの領域において、IP アドレスを表すためにアドレス オブジェクトが使われてきました。アドレス オブジェクトの種別については、「アドレス オブジェクトの種別」を参照してください。

SonicOS は、2 種類の動的アドレス オブジェクトをサポートします。

- **MAC** – SonicOS では、ファイアウォールの ARP キャッシュを参照することにより、MAC AO を IP アドレスに対して解決します。
- **FQDN** – 完全修飾ドメイン名 (例えば "www.reallybadwebsite.com" など) は、ファイアウォールの構成で指定されている DNS サーバを使用して (1 つまたは複数の) IP アドレスに対して解決されます。'*' を使用するワイルドカード エントリもサポートされており、ワイルドカードを指定すると、承認済み DNS サーバへの問い合わせに対する応答が収集されるようになります。

トピック:

- 動的アドレス オブジェクトの主要な機能
- ネットワーク上の承認済みサーバの使用の強制
- MAC および FQDN 動的アドレス オブジェクトの使用

動的アドレス オブジェクトの主要な機能

動的アドレス オブジェクト（DAO）とは、MAC AO および FQDN AO の使用を可能にする基幹フレームワークのことを表す用語です。アクセス ルールは、アドレス オブジェクトを静的な構造から動的な構造に変換することによって、ネットワークの変化に自動的に対応できます。

下の表には、DAO の詳細と例が示されています。

動的アドレス オブジェクト: 機能と利点

機能	利点
FQDN ワイルドカードのサポート	FQDN アドレス オブジェクトでは**.somedomainname.com*のようなワイルドカード エントリがサポートされています。ワイルドカード エントリが指定された場合は、まず基本ドメイン名が解決されて、それに対して定義されているすべてのホスト IP アドレスに変換され、その後、ファイアウォールを通過する DNS 応答のアクティブな収集が継続的に行われます。例えば、**.myspace.com* の FQDN AO を作成すると、まずファイアウォールの構成で指定されている DNS サーバを使用して、*myspace.com* を *63.208.226.40*、*63.208.226.41*、*63.208.226.42*、*63.208.226.43* に対して解決します（このことは nslookup myspace.com、またはそれと同等のコマンドによって確認できます）。ほとんどの DNS サーバではゾーン転送は許可されないので、通常はドメイン内のすべてのホストを自動的に列挙することはできません。それに代わる方法として、ファイアウォールは、ファイアウォールを通過する DNS 応答を監視して、承認済み DNS サーバから発信された DNS 応答を探します。そのため、ファイアウォールの背後のホストが外部 DNS サーバに対して問い合わせを行った場合、そのサーバがファイアウォール上の構成済み/定義済み DNS サーバであるときには、その応答がファイアウォールによって解析され、いずれかのワイルドカード FQDN AO のドメインに一致するかどうかが調べられます。 ⓘ **補足:** 承認済み DNS サーバとは、ファイアウォールが使用する DNS サーバとして構成されている DNS サーバのことです。承認済み DNS サーバからの応答のみをワイルドカードの学習プロセスで使用する理由は、意図的に不正なホスト エントリが設定された未承認 DNS サーバの使用によって FQDN AO のポイズニングが発生する危険を防止するためです。SonicOS の将来のバージョンでは、すべての DNS サーバからの応答をサポートするオプションが提供される可能性があります。アクセス ルールを使うと、承認済み DNS サーバの使用を強制することができます。その方法については、この後の「ネットワーク上の承認済みサーバの使用の強制」で説明します。

機能	利点
	ⓘ **補足:** 例として、*4.2.2.1* と *4.2.2.2* の DNS サーバを使用するようにファイアウォールが構成されていて、ファイアウォールで保護されているすべてのクライアントに対して DHCP 経由でこれらの DNS サーバが提供されている場合を考えてみましょう。ファイアウォールで保護されているクライアント A が *vids.myspace.com* に対応するアドレスの DNS クエリを *4.2.2.1* または *4.2.2.2* に対して実行する場合、ファイアウォールでは、それに対する応答が検査され、定義済みの **.myspace.com* FQDN AOに一致するものと判断されます。そして、その問い合わせの結果 (*63.208.226.224*) は、**.myspace.com DAO* に対応する解決済みの値として追加されます。 ⓘ **補足:** 上記の例で、**.myspace.com* AO が作成される前に、クライアント A のワークステーションが *vids.myspace.com* を解決して、その結果をキャッシュしていたとすると、クライアントは新しい DNS要求を発行する代わりにリゾルバのキャッシュを使用するので、ファイアウォールによる *vids.myspace.com* の解決は行われません。そのため、別のホストによって vids.myspace.com の解決が行われない限り、ファイアウォールは *vids.myspace.com* について学習する機会を得られないことになります。Microsoft Windows を使用しているワークステーションでは、**ipconfig /flushdns** コマンドを使用して、ローカル リゾルバのキャッシュを消去することができます。このキャッシュの消去を行うと、クライアントはすべての FQDN を解決するようになるので、それらのアクセス時にファイアウォールがその解決の情報を取得することが可能になります。 ⓘ **補足:** ワイルドカード FQDN エントリは、そのドメイン名のコンテキストに含まれるすべてのホスト名に解決されます (アドレス オブジェクトあたり最大 256 エントリまで)。例えば、**.sonicwall.com* と指定されている場合、*www.sonicwall.com*、*software.sonicwall.com*、*licensemanager.sonicwall.com* は、それぞれの IP アドレスに解決されますが、*sslvpn.demo.sonicwall.com* は別のコンテキストのドメイン名であるため解決されません。ワイルドカード FQDN AO によって *sslvpn.demo.sonicwall.com* を解決するには、**.demo.sonicwall.com* というエントリを指定する必要があります。このエントリを指定した場合は、*sonicos-enhanced.demo.sonicwall.com*、*csm.demo.sonicwall.com*、*sonicos-standard.demo.sonicwall.com* などのドメイン名も解決されます。 ⓘ **補足:** ワイルドカードは、部分一致ではなく完全一致のみをサポートします。つまり、**.sonicwall.com* は正当な入力ですが、*w*.sonicwall.com*、**w.sonicwall.com*、および *w*w.sonicwall.com* は違います。ワイルドカードはエントリごとに 1 つしか指定できないので、例えば **.*.sonicwall.com* は機能しません。
DNS の使用による FQDN の解決	FQDN アドレス オブジェクトは、ファイアウォールの「**ネットワーク > DNS**」ページで構成された DNS サーバを使用して解決されます。DNS 登録は複数の IP アドレスに解決される場合が多いので、FQDN AO 解決プロセスは、AO あたり最大 256 個の登録までの範囲で、ホスト名に対応するアドレスをすべて取得します。解決プロセスでは、FQDN の IP アドレスへの解決だけでなく、DNS 管理者による構成に基づいて、登録の TTL (存続期間) の関連付けも行われます。この TTL は、古くなった FQDN 情報が

機能	利点
	使われることを防ぐために利用されます。
動的 ARP キャッシュ データの使用による MAC アドレスの解決	ファイアウォールのいずれかの物理セグメントにおいて、ARP (Address Resolution Protocol) メカニズムによってノードが検出されると、ファイアウォールの ARP キャッシュが更新され、そのノードの MAC アドレスと IP アドレスが追加されます。この更新が発生した場合、そのノードの MAC アドレスを参照する MAC アドレス オブジェクトが存在するときには、解決されたアドレスのペアを使用して、そのアドレス オブジェクトが直ちに更新されます。ノードが使われなくなって、そのノードの ARP キャッシュがタイムアウトした場合 (ホストとファイアウォールの L2 接続が切断された場合など) には、その MAC AO は未解決状態に移行します。
MAC アドレス オブジェクトによるマルチホームのサポート	MAC AO ではマルチホームのノードをサポートする構成を使用できます。マルチホームのノードとは、物理インターフェースごとに複数の IP アドレスが割り当てられているノードのことです。各 AO では最大256 個の解決済みエントリを指定できます。この方法を使用すると、1 つの MAC アドレスが複数の IP アドレスに解決される場合でも、そのすべての IP アドレスに対して、その MAC AO を参照するアクセス ルールなどが適用されるようになります。
自動と手動の更新処理	MAC AO エントリはファイアウォールの ARP キャッシュに自動的に同期され、FQDN AO エントリには DNS エントリの TTL 値が適用されるため、解決済みの値は常に新しい状態に保たれます。これらの自動的な更新処理に加えて、個々の DAO または定義済みのすべての DAO を対象として手動で更新および抹消を実行することもできます。

ネットワーク上の承認済みサーバの使用の強制

ネットワーク上の承認済みサーバ (許可されたサーバ) の使用を強制することは必須ではありませんが、そのような設定を行うことをお勧めします。この設定は不正なネットワーク活動の抑止に有効であるだけでなく、FQDN ワイルドカードの解決プロセスの信頼性を確保するためにも役立ちます。一般に、既知のプロトコルによる通信のエンドポイントは可能な限り明確に定義することが望ましいと言えます。例を以下に示します。

- 承認済みサーバ (SMTP サーバ、DNS サーバなど) のアドレス グループを作成します。
- 該当するゾーンのアクセス ルールを作成して、内部ネットワーク上の承認済み SMTP サーバにのみ SMTP 通信の発信を許可し、それ以外のすべての SMTP 発信トラフィックを遮断することにより、意図的または意図しないスパムの送信を防止します。
- 該当するゾーンのアクセス ルールを作成して、内部ネットワーク上の承認済み DNS サーバに対して、すべての宛先ホストとの DNS プロトコル (TCP/UDP 53) による通信を許可します。

  ⓘ **重要:** 内部ネットワーク上に DNS サーバを設置している場合は、必ずこのルールを定義したうえで、アクセスを制限する次の DNS ルールを設定する必要があります。
- 該当するゾーンのアクセス ルールを作成して、ファイアウォールで保護されたホストからの DNS (TCP/UDP 53) 通信を承認済み DNS サーバに対してのみ許可し、それ以外のすべてのDNS アクセスを遮断することにより、未承認の DNS サーバとの通信の発生を防止します。
- 上記のルール設定後に、許可されていないアクセスが試行された場合は、ログの表示によってそのことを確認できます。

MAC および FQDN 動的アドレス オブジェクトの使用

MAC および FQDN の動的アドレス オブジェクトを使用すると、アクセス ルールを非常に柔軟な形で作成できるようになります。MAC アドレス オブジェクトおよび FQDN アドレス オブジェクトの構成は、静的アドレス オブジェクトの場合と同じ方法で「**オブジェクト > 一致オブジェクト > アドレス > アドレス オブジェクト**」ページから行います。動的アドレス オブジェクトの作成後に、その表示項目にマウスを合わせると、そのオブジェクトの状況が表示されます。また、動的アドレス オブジェクトの追加や削除を行うと、その操作がイベントとしてログに記録されます。

動的アドレス オブジェクトは、さまざまな用途に使用できます。以下に示す例は、可能な活用方法のごく一部にすぎません。

トピック:

- FQDN DAO の使用による、ドメインに対するすべてのプロトコルのアクセス遮断
- FQDN ベースのアクセス ルールに適した内部 DNS サーバの使用
- MAC アドレスによる動的ホストのネットワーク アクセスの制御
- ドメイン全体へのアクセスの帯域幅管理

FQDN DAO の使用による、ドメインに対するすべてのプロトコルのアクセス遮断

非標準ポートを使った処理や、未知のプロトコルの使用、暗号化やトンネル化（またはその両方）によるトラフィックの意図的な不明瞭化などを行っているという理由から、特定の送信先 IP アドレスへのすべてのプロトコルのアクセスを遮断することが望ましい場合があります。具体的な例としては、ホーム ネットワークのトンネルを通すことによってトラフィックを不明瞭化するという目的で、DSL モデムまたはケーブル モデムに接続されたホーム ネットワーク上に HTTPS プロキシ サーバを設定した場合（あるいはその他の方法で、53、80、443 などの“信頼できる”ポート、および 5734、23221、63466 などの非標準ポートのポート転送/トンネル化を行っている場合）などが考えられるでしょう。このようなネットワークではポートが予測不能であるだけでなく、多くの場合、IP アドレスも動的に設定されるため同様に予測不能となり、状況はさらに複雑化します。

これらのシナリオでは、通常、ユーザによるホーム ネットワークの特定ができるように動的 DNS（DDNS）登録が利用されるので、FQDN AO を積極的に使えば DDNS レジストラに登録されているすべてのホストへのアクセスを遮断できます。

ⓘ **補足:** ここでは例として DDNS ターゲットの場合を示しています。非 DDNS ターゲット ドメインも同様に使用できます。

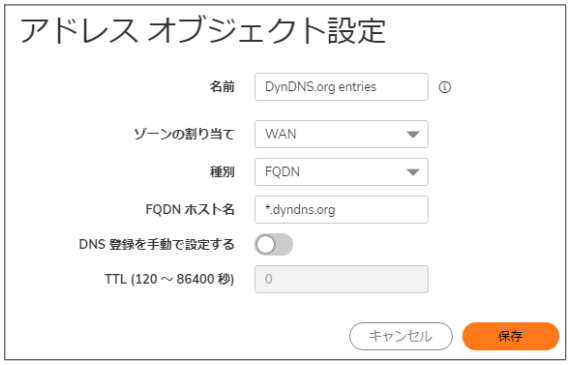
想定条件

- *10.50.165.3* と *10.50.128.53* の DNS サーバを使うようにファイアウォールが構成されているとします。
- ファイアウォールは、ファイアウォールで保護されているすべてのユーザに対して DHCP リースを提供しているものとします。ネットワーク上のすべてのホストは上記の構成済み DNS サーバを使用して解決を行います。
  - 未承認 DNS サーバへの DNS 通信を遮断したければアクセス ルールを使います。「ネットワーク上の承認済みサーバの使用の強制」を参照してください。
- DSL ホーム ネットワークのユーザが DDNS プロバイダ DynDNS に登録しているホスト名が moosifer.dyndns.org であるとします。このセッションで ISP がこの DSL 接続に割り当てたアドレスは、*71.35.249.153* であるとします。

- 同じ IP アドレスに対して別のホスト名を登録することは容易なので、後からホスト名が追加されることを想定して FQDN AO を使用しています。必要に応じて、別の DDNS プロバイダに対応するエントリを追加することもできます。

手順 1 ー FQDN アドレス オブジェクトの作成:

1. 「**オブジェクト > ー致オブジェクト > アドレス > アドレス オブジェクト**」ページに移動します。
2. 「**追加**」をクリックし、次の FQDN アドレス オブジェクトを作成します。



最初に作成された時点では、*dyndns.org* のアドレス（例えば、63.208.196.110）のみがこのエントリの解決先になります。ファイアウォールで保護されているホストが承認済み DNS サーバを使用して *moosifer.dyndns.org*の解決を試行した場合、その問い合わせに対する応答として返された（1 つまたは複数の）IP アドレスが FQDN AO に動的に追加されます。

手順 2 ー アクセス ルールの作成:

1. 「**ポリシー > アクセス ルール**」ページに移動します。
2. 「**追加**」をクリックし、次のアクセス ルールを作成します。

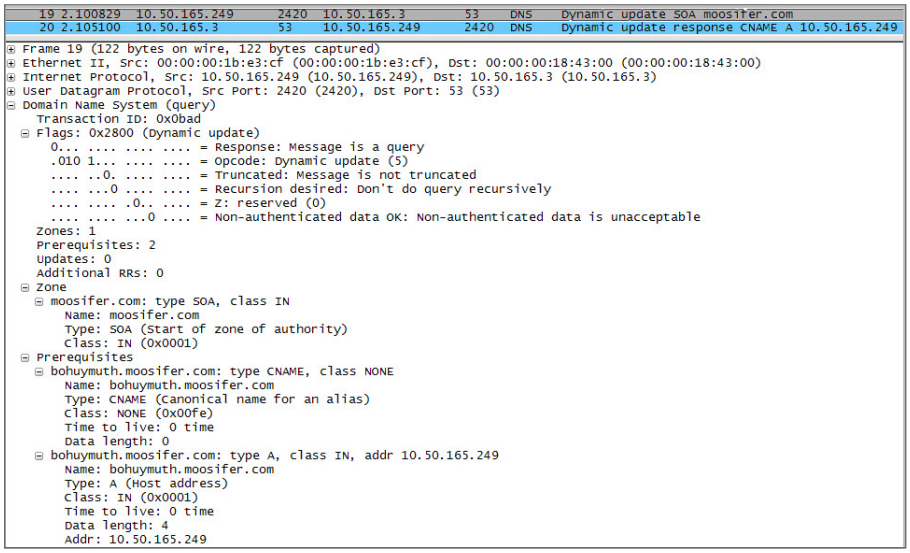
この FQDN に含まれるターゲット ホストへのアクセスはプロトコルに関係なく遮断され、アクセスが試行された場合は、そのイベントがログに記録されます。

FQDN ベースのアクセス ルールに適した内 部 DNS サーバの使 用

DHCP で動的に構成されるネットワーク環境は、内部ホストの登録を動的に行うために、内部 DNSサーバと組み合わせて運用されるのが一般的であり、広く使われている Microsoft の DHCP サービスと DNS サービスもその一例です。このようなネットワークでは、ネットワーク上のホストを構成することによって、適切に構成された DNS サー

バ上の DNS レコードの動的更新を容易に実現することができます（詳細については、Microsoft のサポート技術情報「*Windows Server 2003 で DNS 動的更新を構成する方法*」(http://support.microsoft.com/kb/816592/ja) などを参照してください）。

次の図は、典型的な DNS 動的更新プロセスのパケットの詳細情報を示したものです。この例では、動的に構成されたホスト（*10.50.165.249*）が、（DHCP で提供された）DNS サーバ（*10.50.165.3*）に対して、完全なホスト名（*bohuymuth.moosifer.com*）を登録していることがわかります。



このような環境では、FQDN AO を利用して、ホスト名によるアクセス制御を行うことが有益な場合があります。この方法が最も有効に適用できるのは、ネットワーク内のホスト名が既知の場合（ホスト名のリストが保持されている場合や、一貫した名前付け規則が使用されている場合など）です。

MAC アドレスによる動的ホストのネットワークアクセスの制御

ほとんどのネットワークでは静的なアドレス設定よりも DHCP が利用されることの方がはるかに多いため、特に、動的な DNS 更新が行われていない場合や、ホスト名が常に確定しているとは言えない環境では、動的に構成されるホストの IP アドレスを予測するのが困難な場合があります。このような状況では、MAC アドレス オブジェクトを使用することにより、ほぼ不変の MAC（ハードウェア）アドレスに基づいてホストのアクセスを制御することができます。

その他のほとんどのアクセス制御方法と同様、MAC アドレスによるアクセス制御も、アクセスを原則的に許可して特定のホストまたはホストのグループを送信先/送信元とするアクセスのみを禁止する方法と、アクセスを原則的に禁止して特定のホストまたはホストのグループに対してのみアクセスを許可する方法のどちらでも利用できます。ここでは、例として後者の場合を示します。

DHCP 対応の複数の無線クライアントがあり、それらのクライアントで独自のオペレーティング システムが実行されているため、ユーザ レベルの認証は一切利用できないと仮定します。このとき、それらのクライアントに LAN 上のアプリケーション固有のサーバ（例えば、10.50.165.2）へのアクセスのみを許可することを考えます。WLAN セグメントではセキュリティのために WPA-PSK が使用されていますが、これらのクライアントからのアクセスを許可する対象は 10.50.165.2 のサーバのみであり、LAN 上のそれ以外のリソースへのアクセスはすべて禁止しなければなりません。また、その他のすべての無線クライアントに対しては、*10.50.165.2* へのアクセスのみを禁止し、それ以外の場所へのアクセスはすべて許可する必要があります。

ステップ 1 – MAC アドレス オブジェクトの作成:

1. 「**オブジェクト > 一致オブジェクト > アドレス > アドレス オブジェクト**」ページに移動します。
2. 「**追加**」をクリックし、次の MAC アドレス オブジェクトを作成します（マルチホームのオプションは必要に応じて選択します）。

3. アドレス オブジェクトの作成完了時点において、対象のホストがファイアウォールの ARP キャッシュに含まれている場合は、直ちにその解決が行われます。ARP キャッシュ内にホストの情報が存在しない場合は、ホストが有効化されて ARP によって検出されるまでの間、「*アドレス オブジェクト*」テーブルにはそれらのアドレスが「**未解決**」状態として表示されます。
4. ハンド ヘルド デバイス用のアドレス グループを作成します。

ステップ 2 – アクセス ルールの作成:

1. 「**ポリシー > アクセス ルール**」ページに移動します。
2. 「**追加**」をクリックし、下の表に示されている設定で 4 つのアクセス ルールを作成します。

サンプルのアクセス ルール

設定	アクセス ルール1	アクセス ルール2	アクセス ルール3	アクセス ルール4
許可 / 拒否	許可	禁止	許可	禁止
送信元ゾーン	WLAN	WLAN	WLAN	WLAN
送信先ゾーン	LAN	LAN	LAN	LAN
サービス	MediaMoose サービス	MediaMoose サービス	すべて	すべて
送信元	ハンドヘルド デバイス	すべて	ハンドヘルド デバイス	すべて
送信先	10.50.165.2	10.50.165.2	すべて	すべて
許可ユーザ	すべて	すべて	すべて	すべて
スケジュール	常に有効	常に有効	常に有効	常に有効

ⓘ **補足:** この例では、ハンドヘルド デバイスによって使用される特定のアプリケーションを表すために「MediaMoose サービス」というサービスを使用しています。固有サービスの宣言はオプションであり、必要に応じて行ってください。

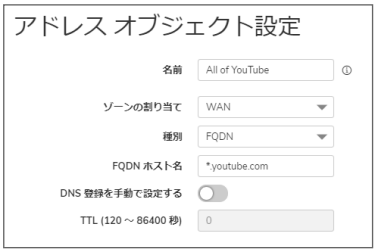
ドメイン全体へのアクセスの帯域幅管理

ストリーミング メディアは、ネットワークの帯域幅を最も大量に消費するサービスの 1 つです。ストリーミング メディアを配信しているサイトでは、ほとんどの場合、多数のサーバからなるサーバ ファームが利用されているため、これらのサイトへのアクセスを制御したり、サイトへの接続に割り当てられる帯域幅を管理したりすることは容易ではあ

りません。さらに、これらのサイトではメディアが再エンコードされてから HTTP で送信される場合が多いので、種別による分類や分離を行うことはいっそう難しくなっています。これらのサイトを構成しているサーバのリストを手動で管理するのは困難な仕事ですが、ワイルドカード FQDN アドレス オブジェクトを使用すると、その作業を簡単化することができます。

ステップ 1 ー FQDN アドレス オブジェクトの作成:

1. 「**オブジェクト > 一致オブジェクト > アドレス > アドレス オブジェクト**」ページに移動します。
2. 「**追加**」をクリックし、次のアドレス オブジェクトを作成します。



アドレス オブジェクトが最初に作成された時点では、**.youtube.com* は *208.65.153.240*、*208.65.153.241*、*208.65.153.242* の IP アドレスに解決されますが、内部ホストが youtube.com ドメイン内のすべての要素に対応する各ホストの解決を開始した後は、*v87.youtube.com* サーバ (*208.65.154.84*) のエントリなど、内部ホストからの問い合わせによって取得されたホスト エントリが追加されていきます。

ステップ2 – 帯域幅オブジェクトを作成する

1. 「**オブジェクト > プロファイル オブジェクト > 帯域幅**」ページに移動します。
2. 「**追加**」をクリックし、次の帯域幅オブジェクトを作成します。

ステップ 3 ー アクセス ルールの作成:

1. 「**ポリシー > アクセス ルール**」ページに移動します。
2. 「**追加**」をクリックし、次のアクセス ルールを作成します。

アクセス ルールが作成された後、「アクセス ルール」テーブル内に、帯域幅管理が有効であることを示す帯域幅管理アイコンと統計情報が表示されるようになります。マウス ポインタをアイコンの上に移動すると、帯域幅管理設定が表示されます。

*.youtube.com のすべてのホストに対するアクセスは、どのプロトコルを使用している場合でも、設定した速度（すべてのユーザ セッションで利用可能な合計帯域幅の低率）に累積的に制限されます。

3

サービス

サービス オブジェクトとサービス グループは、「**オブジェクト > 一致オブジェクト > サービス**」ページで構成します。

SonicOS では拡張 IP プロトコルがサポートされており、ユーザはこれらのカスタム プロトコルに基づいてサービス オブジェクト、サービス グループ、およびアクセス ルールを作成できます。定義済みのプロトコルの一覧は、「ユーザ定義サービス オブジェクト用の 定義済み IP プロトコル」を参照してください。ネットワークに必要な固有の IP プロトコルを追加するには、「カスタム IP 種別サービスの追加」を参照してください。

SonicWall セキュリティ装置では、ネットワークへのトラフィックの許可または拒否を決定するアクセス ルールを構成するために、サービスを使用します。SonicWall セキュリティ装置には、事前定義された既定のサービス オブジェクトと既定のサービス グループが用意されています。既定のサービス オブジェクトとサービス グループは編集可能ですが、削除することはできません。特定の業務上の要件に合わせてユーザ定義サービス オブジェクトやユーザ定義サービス グループを作成することができます。

ページの上部にある「**ビュー**」ドロップダウン リストを使用すると、規定およびユーザ定義サービス オブジェクトおよびグループの表示を制御できます。「**すべて**」を選択してユーザ定義エントリと既定のエントリを表示し、「**ユーザ定義**」を選択してユーザ定義のみを表示するか、「**既定**」を選択して既定のサービス エントリのみを表示します。

既定のサービス オブジェクトおよびグループ

既定のサービス オブジェクトとグループはSonicOSであらかじめ定義されており、削除はできませんが編集することはできます。既定のサービスではポートのみを編集できます。既定のサービスグループでは、含まれているサービスまたは除外されているサービスを変更できます。

「**サービス オブジェクト**」および「**サービス グループ**」テーブルには、サービス オブジェクトとサービス グループに関する以下の属性が表示されます。

名前	サービスの名前
プロトコル	サービスのプロトコル
開始ポート	サービスの開始ポート番号。
終了ポート	サービスの終了ポート番号。
クラス	エントリが「**既定**」(システム) のサービスか「**ユーザ定義**」(ユーザ) サービスかを示します。
コメント	コメント アイコンの上をマウスでポイントすると、サービス オブジェクトまたはグループに関する情報が表示されます。ポップアップには以下の各項目が表示されます。 • 「**参照先**」 – サービス オブジェクトまたはグループを使用するファイアウォー

名前	サービスの名前
	ルに構成されているルールまたはポリシーのタイプのリストが、各種別の参照の数とともに表示されます。ルールまたはポリシーの種別は、「**アクセスルール**」、「**NAT ポリシー**」などのリンクとして表示されます（利用可能な場合）。リンクをクリックするとページが開き、サービス オブジェクトまたはグループを使用して特定のルールまたはポリシーのリストを表示できます。 • 「**グループ（所属先）**」 – サービス オブジェクトまたはグループを含むサービス グループまたは他の種別のグループのリストが表示されます。
構成	サービスの**編集**アイコン、**表示**アイコン、**削除**アイコンが表示されます（既定のサービスは削除できず、それに対応する**削除**アイコンは淡色表示になっています）。「**編集**」アイコンを選択すると、「**サービスの編集**」ダイアログが表示されます。既定のサービスではポートのみを編集できます。既定のサービスグループでは、含まれているサービスまたは除外されているサービスを変更できます。

既定のサービス グループは、既定のサービス オブジェクトおよび/または他の既定のサービス グループのグループです。グループ名表示の左側にある三角形をクリックすると、グループに含まれているすべての既定のサービスとグループが表示されます。例えば、「**AD ディレクトリ サービス**」の既定のグループには、いくつかのサービスオブジェクトとサービスグループが含まれています（「下の画像を参照」参照）。これらの複数のエントリをまとめてグループ化することで、SonicOS 全体のルールとポリシーで単一のサービスとして参照できます。

AD ディレクトリ サービス グループの詳細

ユーザ定義サービス オブジェクト用の定義済み IP プロトコル

ICMP (1)	インターネット制御メッセージ プロトコル。エラー メッセージと制御メッセージの送信に使用される TCP/IP プロトコルです。
IGMP (2)	インターネット グループ管理プロトコル。TCP/IP ネットワークにおけるマルチキャスト グループの管理を制御するプロトコルです。
TCP (6)	転送制御プロトコル。TCP/IP の TCP 部分です。TCP は TCP/IP の転送プロトコルです。TCP により、メッセージが正確に、欠けることなく送信されます。
UDP (17)	ユーザ データグラム プロトコル。TCP/IP プロトコル スイートに含まれるプロトコル

	です。信頼性の高い送信が不要な場合に、TCP の代わりに使用されます。
6over4 (41)	(明示的なトンネルのない IPv6 over IPv4 ドメインの送信) 6over4 トラフィックは、IP ヘッダーの IP プロトコル番号が 41 に設定された IPv4 パケット内で送信されます。
GRE (47)	汎用ルーティング カプセル化。IP トンネル内のさまざまな種類のプロトコル パケットをカプセル化するために使用されるトンネル プロトコルです。ファイアウォールへの仮想ポイントツーポイント リンクの作成や、IP インターネットワーク経由でのデバイスのルーティングに使用されます。
ESP (50)	カプセル化セキュリティ ペイロード。IPSec による柔軟なデータ転送手段として使用される、別のデータグラム内の IP データグラムをカプセル化する手法です。
AH (51)	認証ヘッダー。データ認証に加え、オプションでアンチリレー サービスを提供するセキュリティ プロトコルです。AH は保護するデータに埋め込みます (完全な IP データグラム)。
ICMPv6/ND (58)	(インターネット メッセージ制御プロトコル バージョン 6 向けの近隣者発見) 近隣者発見は、次の 5 種類の ICMP パケット タイプを定義します。ルータ要請メッセージとルータ通知メッセージのペア、近隣者要請メッセージと近隣者通知メッセージのペア、およびリダイレクト メッセージ。
EIGRP (88)	拡張内部ゲートウェイ ルーティング プロトコル。IGRP を拡張したプロトコルです。優れた収束特性と動作効率を実現し、リンク状態プロトコルの利点と距離ベクトル プロトコルの利点を同時に備えています。
OSPF (89)	オープン ショーテスト パス ファースト。ノード間の距離およびいくつかの品質パラメータに基づいて、TCP/IP ネットワークにおける IP トラフィックのルーティングに最適なパスを決定するルーティング プロトコルです。OSPF は内部ゲートウェイ プロトコル (IGP) の 1 つであり、自律システムの内部で動作するように設計されています。また、OSPF は RIP プロトコルを置き換えるために開発されたリンク状態プロトコルであり、RIP プロトコル (距離ベクトル プロトコル) よりも少ないルータ数でトラフィックを更新できます。
PIM (103)	(プロトコル非依存マルチキャスト) 2 つある PIM 動作モードの 1 つです。 • PIM スパース モード (PIM-SM) では、ネットワーク内の最小限のルータがデータを受け取るように、データの配信が制限されます。パケットは、RP (ランデブー ポイント) で明示的に要求された場合にのみ送信されます。スパース モードでは、受信側が広く分散しているため、ダウンストリームのネットワークに送信されたデータグラムは必ずしも使用されないと想定されます。スパース モード使用の代償としては、明示的な Join メッセージの定期更新に依存していることと、RP が必要であることです。 • PM デンス モード (PIM-DM) では、下流側のすべてのルータおよびホストが送信者からのマルチキャスト データグラムを受信すべきであると仮定し、ネットワーク全域にマルチキャスト トラフィックのフラッドを発生させます。ダウンストリームに近隣ルータがないルータは、不要なトラフィックを削除します。データグラムの反復的なフラッドとその後の削除を最小限に抑えるために、PIM DM では、送信元に直接接続しているルータによって送信される状態の再表示メッセージを使用します。 ⓘ **補足:** ファイアウォールは、マルチキャスト トラフィックがアップ/ダウンストリーム インターフェースを通過できるように、マルチキャスト プロトコルとしてのみ構成できます。ファイアウォールは PIM ルータの役割を果たすことができません。

L2TP (115)	レイヤ 2 トンネリング プロトコル。PPP セッションをインターネット経由で実行するためのプロトコルです。L2TP には暗号化機能はありませんが、リモート ユーザから企業 LAN への仮想プライベート ネットワーク (VPN) 接続を確立するために既定で IPsec が使用されます。

定義済みプロトコルを使用したサービス オブジェクトの追加

任意の定義済みプロトコルまたはサービス タイプに、ユーザ定義サービスを追加できます。

定義済みサービス タイプ

プロトコル	IP 番号
ICMP	1
IGMP	2
TCP	6
UDP	17
6over4	41
GRE	47
IPsec ESP	50
IPsec AH	51
ICMPv6/ND	58
EIGRP	88
OSPF	89
PIM	103
L2TP	115

これらのプロトコルの定義については、「ユーザ定義サービス オブジェクト用の 定義済み IP プロトコル」を参照してください。

作成したユーザ定義サービスは、すべて「**サービス オブジェクト**」テーブルに一覧表示されます。ユーザ定義サービス グループを作成してユーザ定義サービスをグループ化することで、より簡単にポリシーを適用することができます。既定のサービス オブジェクトにリストされていないプロトコルは、ユーザ定義サービス オブジェクトに追加できます。

定義済みプロトコルを使用してユーザ定義サービス オブジェクトを追加するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > サービス >サービス オブジェクト**」ページに移動します。
2. 「**追加**」ボタンを選択します。「**サービス オブジェクト**」ダイアログが表示されます。

3. このサービス オブジェクトに付ける説明的な名前を「**名前**」フィールドに入力します。
4. 「**プロトコル**」ドロップダウン メニューで、IP プロトコルの種類を選択します。ダイアログのフィールドが変更されることがあります。
5. 次に入力する内容は、選択した IP プロトコルによって異なります。
   - **TCP** プロトコルと **UDP** プロトコルの場合、**ポート範囲**を指定します。
   - **ICMP**、**IGMP**、**OSPF**、および **PIM** プロトコルの場合、「**サブ種別**」ドロップダウン メニューからサブ種別を選択します。

   ⓘ **補足:** PIM のサブ種別は、PIM SM 専用である以下のものを除き、PIM-SM と PIM-DM の両方に適用されます。

   - 種別 1: 登録
   - 種別 2: 登録停止
   - 種別 4: ブートストラップ
   - 種別 8: 候補 RP 通知
   - その他のプロトコルの場合、それ以上の指定を行う必要はありません。
6. 「**保存**」をクリックします。

カスタム IP 種別サービスの追加

定義済み IP プロトコル種別のみを使用している場合、セキュリティ装置でその他の IP プロトコル種別のトラフィックが検出されると、そのトラフィックは「*識別不能*」として破棄されます。ただし、その他の登録済み IP 種別の膨大なリストが存在し、IANA (Internet Assigned Numbers Authority) (http://www.iana.org/assignments/protocol-numbers) によって管理されるため、共通点の少ない (識別不能) IP 種別を破棄するという厳格な手続きが設けられている間は、機能的に制約されます。

SonicOS では、任意の IP 種別を表すサービス オブジェクトを作成できます。これにより、任意の種別の IP トラフィックを認識および制御するファイアウォール アクセス ルールを作成できます。

ⓘ **補足:** 汎用サービス「**すべて**」では、カスタム IP 種別サービス オブジェクトが処理されません。つまり、IP 種別 126 のカスタム IP 種別サービス オブジェクトを定義しただけでは、IP 種別 126 トラフィックは既定の「**LAN > WAN 許可**」ルールで許可されません。

カスタム IP 種別のサービス オブジェクトを含むアクセス ルールを作成し、その認識と処理を提供する必要があります。「設定例」で説明しています。

設定例

管理者が、RSVP（リソース予約プロトコル – IP 種別 46）および SRP（Spectralink™ 無線プロトコル – IP 種別 119）を WLAN ゾーン（WLAN サブネット）の全クライアントから LAN ゾーン（例えば *10.50.165.26* など）のサーバまで許可する必要があるとします。管理者は、この 2 つのサービスを扱うユーザ定義 IP 種別 サービス オブジェクトを定義できます。

ユーザ定義 IP 種別サービス オブジェクトと関連する構成を定義するには、以下の手順に従います:

1. 「**オブジェクト > 一致オブジェクト > サービス >サービス オブジェクト**」ページに移動します。
2. 「**追加**」ボタンを選択します。「**サービス オブジェクト**」ダイアログが表示されます。

3. このサービス オブジェクトに付ける説明的な名前を「**名前**」フィールドに入力します。
4. 「**プロトコル**」ドロップダウン メニューから、「**カスタム IP 種別**」を選択します。

5. 「**プロトコル**」ドロップダウン リストの右側のフィールドに、「**カスタム IP 種別**」のプロトコル番号を入力します。

ⓘ **補足:** 「**ポート範囲**」と「**サブ種別**」フィールドは、「カスタム IP 種別」として定義、適用されません。

ⓘ **補足:** 定義済み IP 種別に対してカスタム プロトコル種別サービス オブジェクトを定義しようとすると、許可されず、エラー メッセージが表示されます。

6. 「**保存**」をクリックします。
7. 定義するユーザ定義サービスごとに **ステップ 3 ～ステップ 6** を繰り返します。
8. 「**オブジェクト > 一致オブジェクト > サービス >サービス グループ**」ページに移動します。
9. 「**追加**」ボタンを選択します。「**サービス グループ**」ダイアログが表示されます。

10. 「**名前**」フィールドに、サービス グループのわかりやすい名前を入力します (例: *myServices*)。
11. 左側のリストから作成したユーザ定義サービス オブジェクトを選択し、**右矢印**ボタンをクリックして右側のリストに移動します。

    ⓘ **補足:** **Ctrl** または **Shift** キーを押しながら複数のサービス オブジェクトを選択し、**右矢印**ボタンをクリックすると、一度にすべてのサービスを移動できます。
12. 「**保存**」をクリックします。
13. 「**オブジェクト > 一致オブジェクト > サービス >サービス オブジェクト**」ページに移動します。
14. 「**追加**」ボタンを選択します。「**サービス オブジェクト**」ダイアログが表示されます。
15. WLAN サブネットが *myServices* を使用してアクセスできるホスト用のアドレス オブジェクトを作成します。
16. 左側のリストから作成したユーザ定義サービス オブジェクトを選択し、**右矢印**ボタンをクリックして右側のリストに移動します。

    ⓘ **補足:** **Ctrl** または **Shift** キーを押しながら複数のサービス オブジェクトを選択し、**右矢印**ボタンをクリックすると、一度にすべてのサービスを移動できます。
17. 「**保存**」をクリックします。
18. 「**ポリシー > ルールとポリシー > アクセス ルール**」ページに移動して、「**WLAN > LAN**」ルールを作成します。
19. *myServices* に **WLAN サブネット**から *10.50.165.26* アドレス オブジェクトへのアクセスを許可するアクセス ルールを定義します。

    ⓘ **補足:** 双方向トラフィックのためにアクセス ルールを作成する必要がある場合もあります。例えば、*myServices* に *10.50.165.26* から WLAN サブネットへのアクセスを許可する、「**LAN > WAN**」からアクセス ルールを追加する場合も考えられます。
20. 「**保存**」をクリックします。

    これで、IP プロトコル 46 および 119 のトラフィックが認識され、WLAN サブネットから *10.50.165.26* への転送が許可されるようになります。

ユーザ定義サービス オブジェクトの編集

「**構成**」列の下にある**編集**アイコンをクリックして、サービス オブジェクトを編集します。このオブジェクトには、「**サービスの追加**」ダイアログと同じ構成設定項目があります。「定義済みプロトコルを使用したサービス オブジェクトの追加」または「カスタム IP 種別サービスの追加」を参照してください。

ユーザ定義サービス オブジェクトの削除

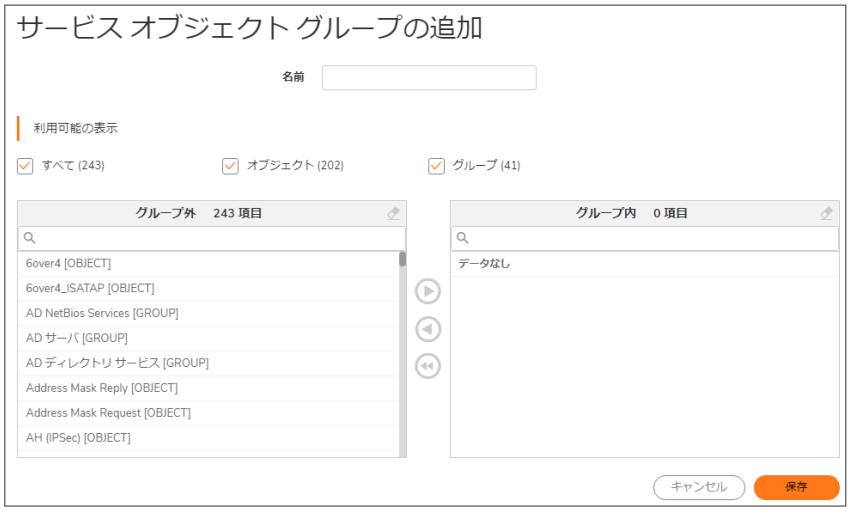
削除するサービス オブジェクトの行で、「**構成**」行の下の「**削除**」アイコンをクリックして、個々のカスタム サービス オブジェクトを削除します。1 つまたは複数のカスタム サービス オブジェクトを削除するには、目的のエントリのチェックボックスをオンにし、テーブル上部の「**削除**」をクリックします。

ユーザ定義サービス グループの追加

ユーザ定義サービスを追加した後で、サービス（既定のサービスを含む）のグループを作成し、グループ内のサービスに同じポリシーを適用することができます。例えば、特定の時刻または曜日にのみ SMTP トラフィックと POP3 トラフィックを許可するには、この 2 つのサービスをユーザ定義サービス グループとして追加します。

ユーザ定義サービス グループを作成するには、以下の手順に従います

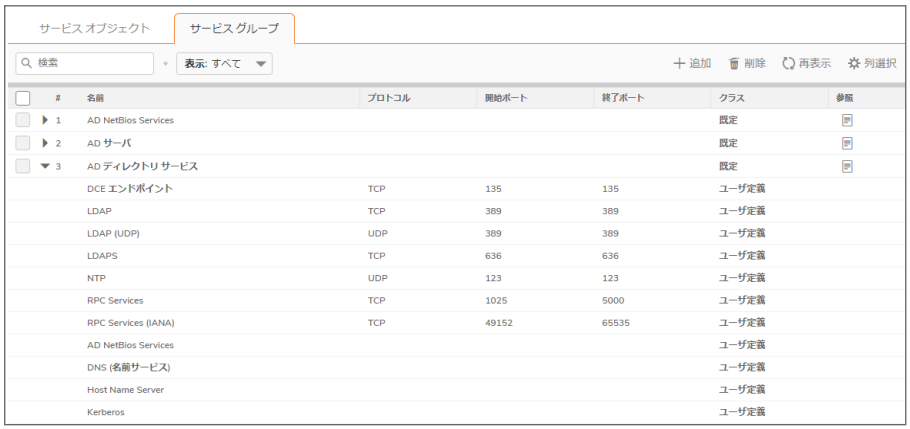
1. 「**オブジェクト > 一致オブジェクト > サービス > サービス グループ**」ページに移動します。
2. 「**追加**」ボタンを選択します。「**サービス グループ**」ダイアログが表示されます。



3. ユーザ定義グループに付ける名前を「**名前**」フィールドに入力します。
4. 左側のリストから作成したユーザ定義サービス オブジェクトを選択し、**右矢印**ボタンをクリックして右側のリストに移動します。

   ⓘ **補足:** Ctrl または Shift キーを押しながら複数のサービス オブジェクトを選択し、**右矢印**ボタンをクリックすると、一度にすべてのサービスを移動できます。
5. 「**保存**」をクリックします。

ユーザ定義サービス グループの名前の左側にある三角形を選択すると、そのユーザ定義サービス グループ登録に含まれている個々のユーザ定義サービス、既定のサービス、ユーザ定義サービス グループがすべて表示されます。



ユーザ定義サービス グループの編集

「**構成**」列の**編集**アイコンをクリックし、ユーザ定義サービス グループを編集します。これには、「**サービス グループの追加**」ダイアログと同じ構成設定項目があります。詳細については、「ユーザ定義サービス グループの追加」を参照してください。

ユーザ定義サービス グループを展開し、個々のサービスの**編集**アイコンを選択して、グループの個々のサービスを編集することもできます。

ユーザ定義サービス グループの削除

削除するサービス グループの行で、「**構成**」の下の「**削除** 」アイコンをクリックして、個々のユーザ定義サービス グループを削除します。1 つ以上のカスタム サービス グループを削除するには、目的のエントリのチェックボックスを選択し、テーブル上部の「**削除**」をクリックします。

4

URI リスト

URI リスト オブジェクトは、許可または禁止としてマーク可能な URI (Uniform Resource Identifiers) またはドメインのリストを定義します。この URI リストは、外部のファイルにエクスポートしたり、別の URI リストにインポートしたりすることもできます。

ⓘ | **補足:** URI リストの処理は、URI の種別よりも優先されます。

URI リスト オブジェクトには次の要件があります。

- 最大で 128 個の URI リスト オブジェクトが設定可能です。
- URI リスト オブジェクトは、1 個で最大 5000 の URI をサポートします。最小値は 1 です。
- 各 URI リスト オブジェクトには、最大 100 個のキーワードを構成できます。最小値はゼロです。

URI と URI リストについて

各**URI リスト オブジェクト**は、「**URI リスト**」に少なくとも 1 つの URI を持たなければなりません。「**URI リスト**」に手動でエントリを入力または貼り付けたり、テキスト (*.txt*) ファイルから URI リストをインポートすることができます。このファイルは、手動で作成することも、以前に装置からエクスポートされたものを使用することもできます。ファイル内の各 URI はそれ自身の行にあります。

URI リストの内容をテキスト (.txt) ファイルにエクスポートしておくと、後でこのファイルからオブジェクトをインポートすることができます。

URI とURI リストには次の要件があります。

- URI は最大 255 文字です。
- 1 つのURI リスト内のすべての URI の長さの合計は、URI 間の各改行 (復帰) コード用の 1 文字を含めて、最大 131,072 (1024*128) です。
- 定義上、URI とはホストとパスが含まれている文字列です。ポートなどのコンテンツは現在サポートされていませんが、キーワードを使用してこれらのコンテンツに一致させることができます。
- URI のホスト部分には、IPv4 または IPv6 のアドレス文字列を指定できます。
- 各 URI には、最大で 16 個のトークンを含むことができます。URI 内のトークンは、次の文字からなる文字列です。

  0 ～ 9
  a ～ z
  A ～ Z
  $ - _ + ! ' ( ) , .

- 各トークンの長さは、トークンを囲む区切り文字（. または /）用の 1 文字を含めて、最大 64 文字です。
- 1 つ以上の有効なトークンの列を表すワイルドカードとして、アスタリスク（*）が使用できます。アスタリスクは、1 つ以上の文字は表しません。

有効な URI の例	無効な URI の例
• *news.example.com* • *news.example.com/path* • *news.example.com/path/abc.txt* • *news.*.com/*.txt* • *10.10.10.10* • *10.10.10.10/path* • *[2001:2002::2003]/path* • *[2001:2002::2003:*:2004]/path/*.txt*	ワイルドカード文字（*）を誤って使用すると、次のような無効な URI になることがあります。 • *example*.com* • *exa*ple.com* • *example.*.*.com* ⓘ **補足:** ワイルドカード文字は、1 つ以上の文字ではなく、1 つ以上のトークンの系列を表します。

URI リスト グループについて

SonicOS 6.5.2 以降から URI リスト グループがサポートされるようになりました。これで URI リスト オブジェクト（CFS プロファイルの許可/禁止リストなど）を柔軟かつ手軽に管理でき、また Websense 除外リストを実現できます。1 つのグループに複数の URI リスト オブジェクトを割り当て、他のモジュール内でそのグループを直接参照できます。URI リスト グループはネストされた包含をサポートし、1 つの URI リスト グループに他の URI リスト グループを含めることができます。URI リスト グループは、URI リスト オブジェクトを使用できる場所であればどこでも使用できます。

最大 128 個の URI リスト グループを構成でき、URI リスト グループ名の最大長は 49 文字です。URI リスト グループには、最大 128 個の URI リスト オブジェクトや URI リスト グループを割り当てることができます。一意の URI の最大数は 5000、一意のキーワードの最大数は 100 です。

キーワードとキーワード リストについて

URI リスト オブジェクトは、URI リストを使用してウェブ トラフィックをスキャンするときに URI を照合します。これは、torrent.comがseedtorrent.comと一致しないことを意味するトークン ベースの一致アルゴリズムを使用します。キーワード リストは、URI 一致をより柔軟にし、URI リスト オブジェクトを URI の他の部分と一致させることによってトラフィックを照合できるようにします。

ウェブ トラフィックの URI 文字列（ホスト+パス+クエリ文字列）にキーワードリストのサブストリングがある場合、URI リストオブジェクトは一致します。たとえば、「sports」と「news」がキーワード リストにある場合、URI リスト オブジェクトは、www.extremsports.com、news.google.com/news/headlines?ned=us&hl=en、または www.yahoo.com/?q=sports と一致させることができます。

URI リストと同様に、**キーワード リスト**に入力または貼り付けすることで手動でエントリを追加することも、テキスト（*.txt*）ファイルからキーワード リストをインポートすることもできます。このファイルは、手動で作成することも、以前に装置からエクスポートされたものを使用することもできます。ファイル内の各キーワードはそれぞれの行にあります。

キーワード リストの内容を後でインポートできるテキスト ファイルにエクスポートできます。

キーワードとキーワード リストの用件:

- 各キーワードは、最大で 255 文字の印刷可能な ASCII 文字を含むことができます。
- 1 つの**キーワード リスト**内のキーワードの最大結合長は、キーワード間の改行（改行）ごとに 1 文字を含む 1024 * 2 に制限されています。

URI リスト オブジェクトの照合

URI リスト オブジェクトの照合処理は、トークンに基づいています。有効なトークン系列は、"." または "/" のような特定の文字で結合された 1 つ以上のトークンで構成されます。URI は 1 つのトークン系列を表しています。例えば、*www.example.com* という URI は "www"、"example"、"com" が "." で結合されたトークン系列です。通常、ある URI に URI リスト オブジェクト内の URI のいずれかが含まれている場合、このリスト オブジェクトはその URI に一致します。

標準一致

リスト オブジェクトに *example.com* のような URI が含まれている場合、そのオブジェクトは次のように定義された URI に一致します。

[<token sequence>(.|/)]example.com[(.|/)<token sequence>]

例えば、この URI リスト オブジェクトは次の URI のいずれにも一致します。

- *example.com*
- *www.example.com*
- *example.com.uk*
- *www.example.com.uk*
- *example.com/path*

この URI リスト オブジェクトは、*specialexample.com* という URI には一致しません。*specialexample* の部分が *example* とは異なるトークンであると認識されるからです。

ワイルドカード一致

ワイルドカード一致がサポートされています。アスタリスク (*) がワイルドカード文字として使用され、この文字はトークンの有効な系列を表します。リスト オブジェクトに *example.*.com* のような URI が含まれている場合、そのリスト オブジェクトは次のように定義された URI に一致します。

[<token sequence>(.|/)]example.<token sequence>.com[(.|/)<token sequence>]

例えば、URI リスト オブジェクト*example.*.com* は次の URI のいずれにも一致します。

- *example.exam1.com*
- *example.exam1.exam2.com*
- *www.example.exam1.com/path*

この URI リスト オブジェクトは次の URI には一致しません。

- *example.com*

これは、ワイルドカード文字 (*) が *example.com* に存在しない有効なトークン系列を表しているためです。

IPv6 アドレスの照合

IPv6 アドレス文字列の照合もサポートされています。IPv4 アドレスは標準のトークン系列として処理できますが、IPv6 アドレス文字列は特別な処理を必要とします。URI リスト オブジェクトに *[2001:2002::2008]* のような URI が含まれている場合、この URI リスト オブジェクトは次のように定義された URI に一致します。

[2001:2002::2008][/<token sequence>]

例えば、この URI リスト オブジェクトは次の URI のいずれにも一致します。

- *[2001:2002::2008]*
- *[2001:2002::2008]/path*
- *[2001:2002::2008]/path/abc.txt*

IPv6 のワイルドカード照合

IPv6 アドレス文字列ではワイルドカード照合がサポートされています。リスト オブジェクトに *[2001:2002:*:2008]/*/abc.mp3* のような URI が含まれている場合、このリスト オブジェクトは次のように定義された URI に一致します。

[2001:2002:<token sequence>:2008]/<token sequence>/abc.mp3

例えば、この URI リスト オブジェクトは次の URI のいずれにも一致します。

- *[2001:2002:2003::2007:2008]/path/abc.txt*
- *[2001:2002:2003:2004:2005:2006:2007:2008]/path/path2/abc.txt*

URI リスト オブジェクトの使用

現在、URI リスト オブジェクトは、次のフィールドで使用できます。

- CFS プロファイルの許可 URI リスト
- CFS プロファイルの禁止 URI リスト
- Websense の除外するウェブ ドメイン

CFS URI リスト オブジェクトの使用法はこれらのフィールドで異なります。CFS プロファイルの許可または禁止 URI リストで使用する場合、CFS URI リスト オブジェクトは通常どおりに動作します。例えば、URI リスト オブジェクトに *example.com/path/abc.txt* のような URI が含まれている場合、そのリスト オブジェクトは、

[<token sequence>(.|/)] example.com/path/abc.txt[(.|/)<token sequence>] のように定義された URI に一致します。

Websense の除外するウェブ ドメインで使用される場合は、URI のホスト部分のみが有効です。例えば、URI リスト オブジェクトに上記のものと同じ *example.com/path/abc.txt* という URI が含まれている場合、そのリスト オブジェクトはトークン系列 *example.com* が含まれているすべてのドメインに一致します。URI のパス部分は無視されます。

URI リスト オブジェクトの管 理

トピック:

URI リスト オブジェクト テーブルについて

URI リスト オブジェクトを表示するには、「**オブジェクト > 一致オブジェクト > URL リスト > URL リスト オブジェクト**」タブに移動します。

名前	**URI リスト オブジェクトの名前。**
URI リスト	URI リスト オブジェクトの URI を指定します。
キーワード リスト	URI リスト オブジェクトで構成されたキーワードを指定します。
構成	テーブルには各項目の「**編集**」、「**クローン**」、「**削除**」アイコンがあります。

URI リスト オブジェクトの設 定

URI リスト オブジェクトを構成するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > URL リスト > URI リスト オブジェクト**」タブに移動します。
2. ページの上部にある「 **追加**」を選択します。

3. この URI リスト オブジェクトに付けるわかりやすい名前を「**名前**」フィールドに入力します。
4. URI を追加するか、ファイルから URI をインポートすることができます。適宜、以下の操作を行います。
    - URI を追加する場合は、*ステップ 6* に進みます。
    - URI をインポートする場合は、*ステップ 10* に進みます。

5. URI を手動で追加するには、「**追加**」をクリックします。「**URI の追加**」ダイアログが表示されます。

6. URI を入力し、「**OK**」をクリックします。URI 要件については、「 URI と URI リストについて」を参照してください。
7. すべての URI を追加するまで、*ステップ 5* と*ステップ 6* の操作を繰り返します。
8. インポートの手順をスキップするには、*ステップ 13* に進みます。ファイルから URI をインポートすると、手動で追加された URI はすべて上書きされます。
9. 「**インポート**」をクリックして、テキスト ファイルから URI のリストをインポートします。確認メッセージが表示されます。

   ⓘ **重要:** ファイルは、「 URI と URI リストについて」に記載されている条件に準拠している必要があります。

   テキスト ファイル内の URI は、次の区切り文字のいずれかで区切ることができます。追加するには、**Enter** または **Return** キーを押します。

区切り文字	スタイル
¥r¥n	Windows スタイルの改行文字
¥r	Mac OS スタイルの改行文字
¥n	UNIX スタイルの改行文字

   ファイル内の最初の 2000 件の有効な URI だけがインポートされます。無効な URI はスキップされ、1 つの **URI リストオブジェクト**につき 2000 件という URI の最大数にはカウントされません。
10. 「**確認**」をクリックします。「**ファイルのアップロード**」ダイアログが表示されます。
11. ファイルを選択し、「**開く**」を選択します。「URI リスト」テーブルに情報が設定されます。「**追加**」ボタンを使用して既に追加されていた URI は、インポートされたファイルの URI に置き換えられます。
12. 「**URI リスト**」に URI を追加し終えたら、必要に応じて「**種別**」ドロップダウンから「**キーワード**」を選択してキーワードを追加します。

   ⓘ **重要:** キーワードと**キーワード リスト**の詳細については、「キーワードとキーワード リストについて」を参照してください。
13. 手動でキーワードを追加するには、「**追加**」をクリックします。「**キーワードの追加**」ダイアログが表示されます。

14. フィールドにキーワードを入力または貼り付け、「**OK**」をクリックします。
15. すべてのキーワードを追加するまで、*ステップ 13* と*ステップ 14* の操作を繰り返します。

16. 手動でキーワードを追加するのではなく、テキスト ファイルからキーワード リストをインポートするには、「**インポート**」を選択します。確認メッセージが表示されます。
17. 「**確認**」をクリックします。「**ファイルのアップロード**」ダイアログが表示されます。
18. ファイルを選択し、「**開く**」を選択します。「キーワード リスト」テーブルが読み込まれます。「**追加**」ボタンを使用して既に追加されたキーワードは、インポートされたファイルのキーワードに置き換えられます。
19. URI とキーワードの追加が終了したら、「**CFS URI リスト オブジェクトの追加**」ダイアログで「**OK**」を選択します。
20. 「**追加**」を選択します。「**URI リスト オブジェクト**」テーブルに情報が設定されます。

    または

    「**キャンセル**」をクリックして、「**URI リスト オブジェクト**」ダイアログを閉じます。

URI リスト オブジェクトのエクスポート

URI リスト オブジェクトをエクスポートするには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > URL リスト > URI リスト オブジェクト**」タブに移動します。
2. 「**構成**」列で、エクスポートするリスト オブジェクトの**編集**アイコンをクリックします。

   「**URI リスト オブジェクト**」ダイアログが表示されます。

3. URI リストをエクスポートするには、「**URI リスト**」ボタンをクリックしてから、「**エクスポート**」をクリックします。

URI リスト オブジェクトの編集

URI リスト オブジェクトを編集するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > URL リスト > URI リスト オブジェクト**」タブに移動します。
2. 「**構成**」列で、編集するリスト オブジェクトの**編集**アイコンをクリックします。
3. ボタンを選択して、「URI リスト」または「キーワード リスト」を選択します。次の選択が可能です。
   - 「URI リスト」テーブルまたは「キーワード リスト」テーブル内のエントリを削除するには、エントリの削除アイコンをクリックします。
   - テーブル内のエントリを選択し、「**削除**」ボタンをクリックします。確認のダイアログで、「**OK**」を選択します。

     「**URI リスト オブジェクト**」ダイアログで「OK」を選択すると、「URI リスト」テーブルに少なくとも 1 つのエントリが残っている必要があることを示すメッセージが表示されます（「キーワード リスト」テーブルでは必要ない）。次のどちらかを行います。
     - 1 つ以上のエントリをテーブルに追加します。
     - ファイルからエントリをインポートします。
     - 「**キャンセル**」をクリックし、別の方法を試みてください。

- 「**編集**」アイコンをクリックして、エントリを編集します。このステップで選択した画面に応じて、「URI の編集」または「キーワードの編集」ダイアログが表示されます。
    - URI またはキーワードに変更を加えます。
    - 「**保存**」をクリックします。「URI リスト」テーブルまたは「キーワード リスト」テーブルの情報が更新されます。

4. 「**URI リスト オブジェクト**」ダイアログで「**OK**」をクリックします。

URI リスト オブジェクトの削除

URI リスト オブジェクトを削除するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > URL リスト > URI リスト オブジェクト**」タブに移動します。
2. 次のいずれかを行います。
    - 削除するリスト オブジェクトの「**構成**」列で**削除**アイコンを選択します。
    - 削除する 1 つ以上のリスト オブジェクトのチェックボックスをオンにします。テーブル上部の「**削除**」ボタンをクリックします。

URI リスト グループの管理

トピック:

- URI リスト グループ テーブルについて
- URI リスト グループの追加
- URI リスト グループの編集
- URI リスト グループの削除

URI リスト グループ テーブルについて

名前	URI リスト グループの名前。
URI リスト	URI リスト グループの URI を指定します。
キーワード リスト	URI リスト グループで構成されたキーワードを指定します。
構成	テーブルには各項目の「**編集**」、「**クローン**」、「**削除**」アイコンがあります。

URI リスト グループの追加

URI リスト グループ を追加するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > URL リスト > URI リスト グループ**」タブに移動します。
2. ページの上部にある「 **追加**」を選択します。
   「**URI リスト グループ**」ダイアログが表示されます。構成されたすべての URI リスト オブジェクトと URI リスト グループのリストが、ダイアログの左側に表示されます。

3. この URI リスト グループに付けるわかりやすい名前を「**名前**」フィールドに入力します。
4. 左側のリストで URI リスト グループに含める項目を選択します。
5. 右矢印ボタンを選択して、選択した項目を右側のフィールドに移動します。
6. 「**保存**」をクリックし、右側のリストを使用して URI リスト グループを作成します。

URI リスト グループの編集

URI リスト グループを編集するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > URL リスト > URI リスト グループ**」タブに移動します。
2. 「**構成**」列で、編集するグループの**編集**アイコンをクリックします。
3. いずれかの側の項目を選択し、左または右矢印ボタンを使用して、項目を反対側に移動します。右側の項目は、URI リスト グループの一部です。URI リスト グループからすべての項目を削除する場合は、「**すべての項目の選択解除**」アイコンをクリックして、すべての項目を右側から左側に移動できます。
4. 「**保存**」をクリックします。

URI リスト グループの削除

URI リスト グループを削除するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > URI リスト > URI リスト グループ**」タブに移動します。
2. 次のいずれかを行います。
   - 削除するグループの「**構成**」列で「**削除**」アイコンを選択します。
   - 削除する 1 つ以上のグループのチェック ボックスをオンにします。テーブル上部の**削除**アイコンをクリックします。

5

一致オブジェクト

このセクションでは、一致オブジェクトおよびアプリケーション リスト オブジェクトの概要と、それらを作成および構成する方法について説明します。

トピック:

一致オブジェクトについて

一致オブジェクトは、動作を実行するために満たす必要がある条件のセットを表します。これには、オブジェクト種別、一致する種別 (完全、部分、正規表現、前方、または後方)、入力形式 (テキストまたは16 進)、および照合する実際のコンテンツが含まれます。一致オブジェクトは、以前のリリースではアプリケーション オブジェクトと呼ばれていました。

実行可能ファイルなどのバイナリ コンテンツを照合する場合は 16 進入力形式を使用し、ファイルや電子メールのコンテンツなどを照合する場合は英数字 (テキスト) 入力形式を使用します。また、16 進入力形式は、グラフィック イメージ内のバイナリ コンテンツに対しても使用できます。グラフィックのいずれかのプロパティ フィールドに特定の文字列が含まれている場合は、テキスト入力形式を使用して同じグラフィックを照合することもできます。正規表現 (regex) は、特定の文字列や値ではなくパターンを照合するためのもので、英数字入力形式を使用します。

ファイル内容一致オブジェクト種別は、ファイル内のパターンやキーワードを照合するための方法を提供します。この種別の一致オブジェクトは、FTP データ転送、HTTP サーバ、またはSMTP クライアント ポリシーでのみ使用できます。

アプリケーション リストおよびアプリケーション種別リストの一致オブジェクト種別は、アプリ ベースのルート ポリシーで使用できます。これは、「**ポリシー > アプリケーション ルール**」ページでサポートされ、構成されます。

当該オブジェクトを作成するには、「**オブジェクト > 一致オブジェクト**」ページで「**追加**」または「**アプリケーションの追加**」オプションをクリックします。アプリ ベースのルート ポリシーについては、『*SonicOS システム セットアップ管理ガイド*』を参照してください。

下の表に、サポートされている一致オブジェクト種別を示します。

サポートされている一致オブジェクト種別

オブジェクト種別	説明	一致する種別	不一致検索	追加のプロパティ
ActiveX クラス ID	ActiveX コンポーネントのクラス ID。例えば、Gator ActiveXコンポーネントのクラス ID は“c1fb8842-5281-45ce-a271-8fd5f117ba5f”です。	完全	無	なし
アプリケーション種別リスト	アプリケーション種別 (マルチメディア、P2P、ソーシャル ネットワーキングなど) を指定できます。	該当なし	無	なし
アプリケーション リスト	選択したアプリケーション種別内で個々のアプリケーションを指定できます。	該当なし	無	なし
アプリケーション シ	選択したアプリケー	該当なし	無	なし

オブジェクト種別	説明	一致する種別	不一致検索	追加のプロパティ
グネチャリスト	ションや種別に対して個々のアプリケーションを指定できます。			
個別オブジェクト	IPS 形式の条件の個別セットを指定できます。	完全	無	4 つのオプション パラメータを追加で設定できます。それらはオフセット、深度、最小ペイロード サイズ、最大ペイロード サイズです。オフセットは、パケット ペイロード内のどのバイトからパターンの照合を開始するかを指定します（値は 1 から始まり、照合における誤検出を最小限にする働きをします）。深度は、パケット ペイロード内のどのバイトでパターンの照合を終了するかを指定します（値は 1 から始まります）。
電子メール本文	電子メール本文内のすべての内容。	処理中	無	なし
電子メール CC の送信先（MIME ヘッダー）	CC MIME ヘッダー内のすべての内容。	完全、部分、前方、後方	有	なし
電子メール送信元（MIME ヘッダー）	From MIME ヘッダー内のすべての内容。	完全、部分、前方、後方	有	なし
電子メール サイズ	送信を許可する最大電子メール サイズを指定できます。	該当なし	無	なし
電子メール件名（MIME ヘッダー）	Subject MIME ヘッダー内のすべての内容。	完全、部分、前方、後方	有	なし
電子メール送信先（MIME ヘッダー）	To MIME ヘッダー内のすべての内容。	完全、部分、前方、後方	有	なし
MIME 個別ヘッダー	MIME 個別ヘッダーを作成できます。	完全、部分、前方、後方	有	個別ヘッダー名を指定する必要があります。
ファイル内容	ファイル内容で照合するパターンを指定できます。パターンは、ファイルが圧縮されている場合でも照合されます。	処理中	無	このオブジェクトには“添付ファイルを無効にする”動作を適用しないでください。
ファイル名	電子メールの場合、これは添付ファイルの名前です。HTTP	完全、部分、前方、後方	有	なし

オブジェクト種別	説明	一致する種別	不一致検索	追加のプロパティ
	の場合、これはウェブ メール アカウントにアップロードされた添付ファイルの名前です。FTP の場合は、アップロードまたはダウンロードされたファイルの名前です。			
ファイル拡張子	電子メールの場合、これは添付ファイルのファイル拡張子です。HTTP の場合、これはウェブ メール アカウントにアップロードされた添付ファイルのファイル拡張子です。FTP の場合は、アップロードまたはダウンロードされたファイルのファイル拡張子です。	完全	有	なし
FTP コマンド	特定の FTP コマンドを選択できます。	該当なし	無	なし
FTP コマンド + 値	特定の FTP コマンドと値を選択できます。	完全、部分、前方、後方	有	なし
HTTP Cookie ヘッダー	ブラウザから送信される Cookie を指定できます。	完全、部分、前方、後方	有	なし
HTTP Host ヘッダー	HTTP Host ヘッダー内の内容。HTTP 要求における送信先サーバのホスト名を表します（例えば、*www.google.com*）。	完全、部分、前方、後方	有	なし
HTTP Referrer ヘッダー	ブラウザから送信される Referrer ヘッダーの内容を指定できます。この機能は、ユーザがどのウェブ サイトから顧客のウェブ サイトにリダイレクトされたかの統計情報を制御または収集するのに	完全、部分、前方、後方	有	なし

オブジェクト種別	説明	一致する種別	不一致検索	追加のプロパティ
	便利です。			
HTTP Request 個別ヘッダー	個別 HTTP Request ヘッダーを処理できます。	完全、部分、前方、後方	有	個別ヘッダー名を指定する必要があります。
HTTP Response 個別ヘッダー	個別 HTTP Response ヘッダーを処理できます。	完全、部分、前方、後方	有	個別ヘッダー名を指定する必要があります。
HTTP Set Cookieヘッダー	Set-Cookie ヘッダー。ブラウザに特定の Cookie を設定できないようにするための方法を提供します。	完全、部分、前方、後方	有	なし
HTTP URI 内容	HTTP 要求の URI 内のすべての内容。	完全、部分、前方、後方	無	なし
HTTP User-Agent ヘッダー	User-Agent ヘッダー内のすべての内容。例を以下に示します。User-Agent: Skype。	完全、部分、前方、後方	有	なし
ウェブ ブラウザ	特定のウェブ ブラウザを選択できます (MSIE、Netscape、Firefox、Safari、Chrome)。	該当なし	有	なし
IPS シグネチャ種別リスト	1 つ以上の IPSシグネチャ グループを選択できます。各グループに複数の定義済み IPSシグネチャが含まれます。	該当なし	無	なし
IPS シグネチャ リスト	粒度を高めるために 1 つ以上の特定の IPSシグネチャを選択できます。	該当なし	無	なし

使用できる一致オブジェクトの種別は、「**一致オブジェクトの設定**」ダイアログのドロップダウン メニューで確認できます。

- 「**一致オブジェクトの設定**」ダイアログでは、複数のエントリを追加して、照合するコンテンツ要素のリストを作成できます。一致オブジェクトで指定したすべての内容は、照合の目的で大文字と小文字が区別されることはありません。バイナリ内容を照合するには 16 進形式を使用します。16 進エディタや、Wiresharkのようなネットワーク プロトコル アナライザを使用すると、バイナリ ファイルの 16 進形式を取得できます。これらのツールの詳細については、「**ポリシー > アプリケーション ルール**」の Wireshark および Hex Editor セクションを参照してください。

(ファイルからロード) アイコンを使用すると、照合する一致オブジェクトの複数のエントリを含む定義済みのテキスト ファイルから内容をインポートできます。ファイル内のエントリは、それぞれ 1 行に 1 つずつ記述されている必要があります。「ファイルからロード」機能を使用すると、ファイアウォール間でアプリケーション ルールの設定を容易に移行できます。

複数のエントリ (テキスト ファイルから読み込まれたエントリまたは手動で入力されたエントリ) は「リスト」領域に表示されます。リストされたエントリは論理和を使用して照合されるため、リスト内のいずれかのアイテムが一致すると、当該ポリシーの動作が実行されます。

1 つの一致オブジェクトには、合計で 8000 文字まで含めることができます。一致オブジェクト内の各要素に含まれる文字数が約 30 である場合、約 260 個の要素を入力できることになります。最大要素サイズは 8000 バイトです。

トピック:

- 正規表現について
- 不一致検索について

正規表現について

アプリケーション ルール ポリシーで使用するため、特定の一致オブジェクト種別に正規表現を構成できます。「一致オブジェクトの設定」オプションでは、個別正規表現を構成したり、あらかじめ定義された正規表現から選択したりできます。SonicWall セキュリティ装置は、ネットワークトラフィックに対して再組み立て不要の正規表現による照合をサポートしています。このため、入力ストリームのバッファリングが不要で、パターンはパケット境界をまたがって照合されます。

SonicOS には、以下の定義済み正規表現が用意されています。

VISA CC	VISA クレジット カード番号
US SSN	米国の社会保障番号
CANADIAN SIN	カナダの社会保険番号
ABA ROUTING NUMBER	米国銀行協会のルーティング番号
AMEX CC	American Express クレジット カード番号
MASTERCARD CC	Mastercard クレジット カード番号
DISCOVER CC	Discover クレジット カード番号

正規表現を使用するポリシーは、ネットワークトラフィック内の該当するパターンのうち、最初に出現するものに一致します。そのため、一致に対して可能な限り速やかに動作できます。照合は、人間が読み取れるテキストだけではなくネットワークトラフィックに対しても実行されるので、照合可能な英字には ASCII 文字セット全体（全 256 文字）が含まれます。

'.'、(任意の文字ワイルドカード)、'*'、'?'、'+'、繰り返しカウント、代替、および否定などの一般的な正規表現の基本命令がサポートされています。構文とセマンティクスは Perl や vim などの一般的な正規表現の実装と似ていますが、わずかな違いがあります。例えば、行頭演算子 (^) と行末演算子 ($) はサポートされていません。また、'¥z' は、PERL のように文字列の終わりを指すのではなく、0 以外の数字、すなわち [1-9] を指します。詳細については、「正規表現の構文」を参照してください。

Perl 正規表現エンジンとの大きな違いの 1 つは、後方参照と置換がサポートされていないことです。これらの機能は実際には正規表現に無関係で、調べているデータについて線形時間では実行できません。したがって、最高のパフォーマンスを維持するため、これらの機能はサポートされていません。置換または変換機能がサポートされていないのは、ネットワークトラフィックを検査するだけで、変更はしないからです。

よく使用されるパターン (米国の社会保障番号や VISA のクレジットカード番号など) 向けにあらかじめ定義された正規表現は、一致オブジェクトの作成時に選択できます。ユーザは、同じ一致オブジェクト内に独自の表現を記述することもできます。ユーザが入力した表現は解析され、正しく解析されなかった表現があれば、「一致オブジェクトの設定」ウィンドウの下部に構文エラーが表示されます。解析が正しく完了した後、正規表現はコンパイラに渡され、ネットワークトラフィックをリアルタイムでスキャンするのに必要なデータ構造が作成されます。

決定性有限オートマトン (DFA) というデータ構造を作成することによって、正規表現が効率的に照合されます。DFA のサイズはユーザが入力した正規表現によって決定され、デバイスのメモリ容量によって制約を受けます。複雑な正規表現のコンパイル処理には長い時間がかかり、装置のメモリを大量に消費することがあります。含まれる表現によっては、DFA の作成に最大 2 分かかることもあります。

装置管理の応答性に対する影響が大きすぎるだけでなく、悪用やサービス拒否攻撃を防ぐため、コンパイラは処理を中止し、データ構造がデバイスに対して大きくなりすぎる正規表現を拒否できます。ウィンドウの下部に、"悪用を検出しました" というエラー メッセージが表示されます。

ⓘ **補足:** 長時間のコンパイル中、装置管理セッションが一時的に反応しなくなることがありますが、ネットワークトラフィックは装置に送信され続けています。

大きなカウンタを含む表現の DFA を作成すると、多くの時間とメモリが消費されます。そのような表現は、'*' 演算子と '+' 演算子などの無制限のカウンタを使用する表現よりも拒否される可能性が高くなります。

同様に、拒否されるおそれがある表現としては、文字範囲や文字クラスよりも多数の文字を含む表現があります。つまり、'(a|b|c|d|. . .|z)' という表現は、同等の文字クラス '¥l' よりも拒否される可能性が高くなります。'[a-z]' という範囲を使用すると、内部的に '¥l' に変換されます。ただし、

'[d-y]' または '[0-Z]' という範囲は、文字クラスに変換できず、長いので、この断片を含む表現は拒否される可能性があります。

表現が拒否されたときはいつでも上記のヒントを利用して、拒否されないように、より効率的な方法で書き直すことができます。構文の詳細については、「正規表現の構文」を参照してください。ユーザ定義正規表現の作成方法に関する例は、「**ポリシー > アプリケーション ルール**」の「*一致オブジェクトにおける正規表現の作成*」セクションを参照してください。

正規表現の構文

このセクションでは、正規表現の作成に使用する構文について説明します。

正規表現の構文: 単一文字

入力形式	定義
.	'¥n' 以外の任意の文字。'¥n' も照合するには、/s (ストリーム モード、または 1 行モードとも呼ばれる) 修飾子を使用します。
[xyz]	文字クラス。エスケープ文字も指定できます。かっこ ([ ]) で囲まれた特殊文字は

入力形式	定義
	特別な意味を持たないので、エスケープする必要はありません。
¥xdd	16 進入力。"dd" は文字の 16 進値です。2 つの数字が必須です。例えば、¥r は ¥x0d で、¥xd ではありません。
[a–z][0–9]	文字範囲。

正規表現の構文: 複合

入力形式	定義
xy	x に y が続く
x|y	x または y
(x)	x と同等です。優先をオーバーライドするのに使用できます。

正規表現の構文: 繰り返し

入力形式	定義
x*	0 個以上の x
x?	0 または 1 個の x
x+	1 個以上の x
x{n, m}	最小 n 個、最大 m 個の x。すべての数字の分だけ繰り返しが拡張されます。そのため、不当に大きい m を使用することは賢明ではありません。
x{n}	正確に n 個の x
x{n,}	最小 n 個の x
x{,n}	最大 n 個の x

正規表現の構文: エスケープ シーケンス

入力形式	定義
¥0、¥a、¥b、¥f、¥t、¥n、¥r、¥v	C プログラミング言語のエスケープ シーケンス (¥0 は NULL 文字 (ASCII 文字のゼロ))。
¥x	16 進値。¥x とそれに続く 2 つの 16 進数字は、対象の文字の 16 進値を示します。
¥*, ¥?, ¥+, ¥(, ¥), ¥[, ¥], ¥{, ¥}, ¥¥, ¥/, ¥<space>, ¥##	特殊文字をエスケープします。 ⓘ **補足:** 処理されないコメントの前には、任意の数のスペースと 1 個のポンド記号 (#) が付きます。そのため、スペースまたはポンド記号 (#) を照合するには、エスケープ シーケンス ¥ および ¥# を使用する必要があります。

正規表現の構文: PERL に似た文字クラス

入力形式	定義
¥d、¥D	数字、数字以外。
¥z、¥Z	0 以外の数字 ([1–9])、それ以外のすべての文字。
¥s、¥S	空白、空白以外。[¥t¥n¥f¥r] と同等。¥v は Perl 空白には含まれません。
¥w、¥W	単語文字、単語文字以外。[0–9A–Za–z_] と同等です。

正規表現の構文: その他の ASCII 文字クラスの基本命令

文字クラス	表現	
[:cntrl:]	¥c、¥C	制御文字。[¥x00 – ¥x1F¥x7F]。
[:digit:]	¥d、¥D	数字、数字以外。Perl 文字クラスと同じです。
[:graph:]	¥g、¥G	スペース以外の任意の印刷可能文字。
[:xdigit:]	¥h、¥H	任意の 16 進数。[a–fA–F0–9]。水平スペースを意味する Perl の ¥h とは異なります。
[:lower:]	¥l、¥L	任意の小文字。
[:ascii:]	¥p、¥P	正または負の ASCII 数字。[0x00 – 0x7F]、[0x80 – 0xFF]。
[:upper:]	¥u、¥U	任意の大文字。

その他の一般的な文字クラスの一部は、上記の基本命令から作成できます。以下の文字クラスに関しては、使用できる残りの文字に適切なニーモニックがないため、独自の簡略表現はありません。

正規表現の構文: 複合文字クラス

文字クラス	表現	
[:alnum:]	= [¥l¥u¥d]	すべての文字と数字のセット。
[:alpha:]	= [¥l¥u]	すべての文字のセット。
[:blank:]	= [¥t<space>]	空白文字のクラス: タブとスペース。
[:print:]	= [¥g<space>]	すべての印刷可能文字のクラス: スペースを含むすべてのグラフィカル文字。
[:punct:]	= [^¥P¥c<space>¥d¥u¥l]	すべての句読文字のクラス: 否定 ASCII 文字、制御文字、スペース、数字、大文字または小文字を含みません。
[:space:]	= [¥s¥v]	すべての空白文字。Perl の空白と垂直タブ文字を含みます。

正規表現の構文: 修飾子

入力形式	定義
/i	大文字と小文字を区別する
/s	入力を 1 行として扱います。ストリームモードと考えることもできます。つまり、'.' は '¥n' にも一致します。

正規表現の構文: 演算子の優先順位 (降順)

演算子	結合規則
[ ], [^]	左から右
()	左から右
*, +, ?	左から右
. (連結)	左から右
|	左から右

正規表現でのコメント

SonicOS は、正規表現でコメントをサポートしています。コメントの前には、任意の数のスペースと 1 個のポンド記号 (#) を付けます。スペースとポンド記号の後のテキストはすべて、表現の終わりまで破棄されます。

不一致検索について

不一致検索は、遮断するコンテンツを指定するための別の方法を提供します。不一致検索は、特定のコンテンツ種別を除くすべてのコンテンツを遮断する場合に、一致オブジェクト内で有効にできます。この一致オブジェクトをポリシー内で使用すると、そのポリシーは、一致オブジェクトに指定されているコンテンツの欠如に基づいて動作を実行します。不一致検索オブジェクト内にある複数のリスト登録が論理条件 AND を使用して照合されます。つまり、ポリシーの動作は、指定された不一致検索登録のすべてが一致した場合に限り実行されます。

すべてのアプリケーション ルール ポリシーは禁止ポリシーですが、不一致検索を使用することで許可ポリシーを再現できます。例えば、*.txt* 形式の電子メール添付ファイルは許可しつつ、その他すべてのファイル種別の添付ファイルを遮断できます。また、いくつかの種別を許可してその他すべてを遮断することもできます。

すべての一致オブジェクト種別で不一致検索を利用できるわけではありません。不一致検索が可能なオブジェクトについては、「**一致オブジェクトの設定**」ダイアログで「**不一致検索を有効にする**」チェックボックスが表示されます。

アプリケーション リスト オブジェクトについて

アプリケーション リスト オブジェクトを作成するには、「**オブジェクト > 一致オブジェクト**」ページの「**アプリケーションの追加**」をクリックします。ダイアログには 2 つの選択肢があります。

- **アプリケーション** – この画面ではアプリケーション フィルタ オブジェクトを作成できます。この画面では、アプリケーション種別、脅威度、技術の種類、属性を選択できます。選択が終わると、それらの条件に一致するアプリケーションのリストが表示されます。「**アプリケーション**」画面は、**アプリケーション リスト** タイプの一致オブジェクトを作成する 1 つの方法を提供します。
- **種別** – この画面では種別フィルタ オブジェクトを作成できます。アプリケーション種別のリストが表示され、マウスを種別に移動すると説明が表示されます。「**種別**画面で、「**アプリケーション種別リスト**」タイプの一致オブジェクトを作成することができます。

トピック:

- アプリケーション フィルタについて
- 種別フィルタについて

アプリケーション フィルタについて

「**アプリケーション**」画面は、選択するアプリケーションのリストを提供します。表示するアプリケーションは、1 つ以上のアプリケーション種別、技術、リスク、指向、方向を選択することによって制御できます。また、あるキーワードをすべてのアプリケーション名から検索するには、「**検索**」フィールドにそのキーワードを入力します。例えば、「**検索**」フィールドに "bittorrent" と入力すると、名前に "bittorrent" (大文字と小文字の区別なし) が含まれる複数のアプリケーションが見つかります。

アプリケーション リストが適切に絞り込まれたリストに縮小されると、アプリケーションの隣にある**プラス** (+) アイコンによってフィルタ向けに個々のアプリケーションを選択して、選択結果をアプリケーション フィルタ オブジェクトとして個別の名前または自動的に生成された名前で保存できます。以下の図に示すダイアログでは、個々のアプリケーションを選択する前に、すべての種別、技術、リスク、指向、方向が選択されています。

フィルタ向けに選択したアプリケーションは、右側の「**選択済み**」ペインに表示されます。このフィールド内のリストを編集するには、**削除**アイコンをクリックしてアプリケーションを削除します。下の画像は、「**選択済み**」ペインのいくつかのアプリケーションを示しています。また、左側のアプリケーション リストの選択されているアプリケーションには緑色のチェックマークが付いています。

対象として含めるアプリケーションの選択が終了したら、「**一致オブジェクト名**」フィールドにオブジェクトの名前を入力し（最初に「**一致オブジェクト名を自動生成する**」チェックボックスをオフにする）、「**保存**」オプションをクリックします。「**オブジェクト > 一致オブジェクト**」ページに、オブジェクト種別が「アプリケーション リスト」であるオブジェクト名のリストが表示されます。その後、アプリケーション ルール ポリシーまたはアプリ ベースのルート ポリシーを作成するとき、このオブジェクトを選択できます。

「**一致オブジェクト名を自動生成する**」オプションを使用して作成されたアプリケーション リスト オブジェクトには、オブジェクト名の最初の文字としてチルダ (~) が表示されます。

種別フィルタについて

「**種別**」画面は、選択するアプリケーション種別のリストを提供します。種別の任意の組み合わせを選択し、選択結果を種別フィルタ オブジェクトとして個別の名前で保存できます。以下の図に示すダイアログには、アプリケーション種別の説明が表示されています。

ユーザ定義種別フィルタ オブジェクトを作成するには、以下の順に従います:

1. 「**一致オブジェクト名を自動生成する**」チェックボックスをオフにして、「**一致オブジェクト名**」フィールドにオブジェクトの名前を入力します。
2. 1 つまたは複数の種別のチェックボックスを選択します。
3. 「**保存**」をクリックします。

   「**オブジェクト > 一致オブジェクト**」ページには、オブジェクト種別が「アプリケーション種別リスト」であるオブジェクト名が表示されます。アプリケーション ルール ポリシーまたはアプリ ベースのルート ポリシーを作成するとき、このオブジェクトを選択できます。

「**一致オブジェクト名を自動生成する**」オプションを使用して作成されたアプリケーション リスト オブジェクトには、オブジェクト名の最初の文字としてチルダ (~) が表示されます。

一致オブジェクトの設定

一致オブジェクトを構成するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト**」ページに移動します。

2. 「**追加**」を選択します。「**一致オブジェクトの設定**」ダイアログが表示されます。

3. 「**オブジェクト名**」フィールドにわかりやすいオブジェクト名を入力します。
4. ドロップダウン メニューから「**一致オブジェクト種別**」を選択します。ここでの選択内容はこの画面に表示されるオプションに影響します。一致オブジェクト種別の説明については、「一致オブジェクトについて」を参照してください。
5. ドロップダウン メニューから「**一致種別**」を選択します。一致オブジェクトの種別によって選択肢が変わります。
6. 「**入力形式**」で、照合するテキスト パターンとして「**英数字**」を選択します。バイナリ コンテンツを照合する場合は、「**16 進数**」を選択します。
7. 「**内容**」テキスト ボックスに、照合するパターンを入力します。
8. **追加**アイコンをクリックします。「リスト」フィールドに内容が表示されます。同じ手順を繰り返して、照合する他の要素を追加します。

   「**一致種別**」が「**正規表現一致**」の場合、あらかじめ定義されている正規表現のいずれかを選択し、種別をクリックして「リスト」に追加します。個別正規表現を「**内容**」フィールドに入力し、「**追加**」をクリックして「リスト」に追加することもできます。

または、「**ファイルからロード**」アイコンをクリックして、テキスト ファイルから要素のリストをインポートすることができます。ファイル内の各要素は、1 行に 1 つずつ記述されている必要があります。

9. 「**保存**」をクリックします。「**オブジェクト > 一致オブジェクト**」ページに、オブジェクト種別が「アプリケーション リスト」であるオブジェクト名のリストが表示されます。その後、アプリケーション ルール ポリシーまたはアプリ ベースのルート ポリシーを作成するとき、このオブジェクトを選択できます。

アプリケーション リスト オブジェクトの設定

このセクションでは、アプリケーション リスト オブジェクトの作成方法を説明します。これは、「**一致オブジェクトの作成**」ダイアログで作成されるアプリケーション リスト オブジェクトと同じように、アプリケーション ルール ポリシーまたはアプリ ベースのルート ポリシーで使用できます。

アプリケーション リスト オブジェクト種別の詳細（「種別」画面に関する情報を含みます）については、「アプリケーション リスト オブジェクトについて」を参照してください。

アプリケーション リスト オブジェクトを構成するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト**」に移動します。
2. ページ上部の「**アプリケーションの追加**」オプションを選択します。「**一致オブジェクトの作成**」ダイアログが開き、「アプリケーション」画面が表示されます。

表示するアプリケーションは、1 つ以上のアプリケーション種別、脅威度、技術を選択することによって制御できます。アプリケーション リストが縮小されて適切なリストに絞り込まれると、フィルタに対して個々のアプリケーションを選択できます。

3. 「**検索**」フィールドでは、必要に応じて、アプリケーション名の一部を入力し、名前にそのキーワードが含まれるアプリケーションを検索できます。
4. 「**種別**」ペインで、1 つ以上のアプリケーション種別のチェックボックスをオンにします。
5. 「**技術**」ペインで、1 つ以上の技術のチェックボックスをオンにします。
6. 「**リスク**」ペインで、1 つ以上のリスク レベルのチェックボックスをオンにします。
7. 「**指向**」ペインで、1 つ以上の指向種別のチェックボックスをオンにします。
8. **方向**」ペインで、1 つ以上の方向種別のチェックボックスをオンにします。
9. フィルタ オブジェクトを追加するそれぞれのアプリケーションの隣にある**プラス記号**を選択します。アプリケーションの説明を表示するには、「**名前**」列内の三角をクリックします。フィルタに対してアプリケーションを選択すると、**プラス記号**が**緑色のチェックマーク** アイコンになり、選択したアプリケーションが右側の「**選択済み**」ペインに表示されます。このフィールド内のリストは、個々のアイテムを削除したり、**削除**アイコンをクリックしてすべてのアイテムを削除したりして、編集することができます。

10. 対象として含めるアプリケーションの選択が終了すると、最初に「**一致オブジェクト名を自動生成する**」チェックボックスをオフにし、「一致オブジェクト名」フィールドにオブジェクトの名前を入力します。また、自動生成された名前を使用することもできます。
11. 「**保存**」をクリックします。「**オブジェクト > 一致オブジェクト**」ページに、オブジェクト種別が「アプリケーション リスト」であるオブジェクト名のリストが表示されます。その後、アプリケーション ルール ポリシーまたはアプリベースのルート ポリシーを作成するとき、このオブジェクトを選択できます。

6

スケジュール

SonicOS では、セキュリティ機能やポリシーと組み合わせてスケジュール オブジェクトを使用します。スケジュール オブジェクトを作成するには、「**オブジェクト > 一致オブジェクト > スケジュール**」に移動します。特定のセキュリティ機能やポリシー（ルール）にスケジュール オブジェクトを適用できます。例えば、「**ポリシー > ルールとポリシー > アクセス ルール**」ページでアクセス ルールを追加すると、「**ルールの追加**」ダイアログに、すべての使用可能な定義済みスケジュール オブジェクトおよび「**スケジュール**」ページで作成したスケジュール オブジェクトが表示されます。1 つのスケジュールでのルール適用に複数の日付および時刻の追加を含めることができます。

「**スケジュール**」ページでは、SonicWall Security Appliance のさまざまな機能のスケジュール時刻を設定する既定および個別のスケジュール オブジェクトを作成および管理できます。

ⓘ | **補足:** 既定のスケジュールは編集できますが、削除することはできません。

「**スケジュール**」テーブルには、定義済みのスケジュールと個別スケジュールがすべて表示されます。既定のスケジュールとして以下のものがあります。

勤務時間	時間外
週末時間	AppFlow 報告時間
アプリケーション可視化報告時間	TSR 報告時間
クラウド バックアップ時間	ゲスト サイクル クォータ更新

個別スケジュールの追加

個別スケジュールを作成するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > スケジュール**」に移動します。
2. 「**追加**」を選択します。「**スケジュールの追加**」ダイアログが表示されます。

3. 「**スケジュール名**」フィールドにスケジュールの名前を入力します。
4. 「**スケジュール種別**」に次のいずれかのラジオ ボタンを選択します。

1 回	「**開始**」と「**終了**」の時刻および日付を構成し、その間に一度発生するスケジュールです。これを選択すると「**1 回**」の各フィールドが使用可能になり、「**繰り返し**」の各フィールドが淡色表示になります。
繰り返し	開始と終了の日時は設定せず、時刻と曜日を構成し、その同じタイミングで繰り返し発生するスケジュールです。これを選択すると「**繰り返し**」の各フィールドが使用可能になり、「**1 回**」の各フィールドが淡色表示になります。
混合	開始と終了の日時を構成し、時刻と曜日も構成して、その期間に同じタイミングで繰り返し発生するスケジュールです。これを選択すると、ページ内のすべてのフィールドが有効になります。

ⓘ **補足:** 時刻は 24 時間形式 (5 p.m の場合は 17:00) にする必要があります。

5. 「**1 回**」の各フィールドが使用可能な場合、以下を構成します:
   - 「**開始**」行のドロップダウン メニューから「**年**」、「**月**」、「**日**」、「**時**」、「**分**」を選択して開始日時を設定します。時間は 24 時間形式で入力してください。
   - 「**終了**」行のドロップダウン メニューから「**年**」、「**月**」、「**日**」、「**時間**」、「**分**」を選択して終了日時を設定します。時間は 24 時間形式で入力してください。
6. 「**繰り返し**」の各フィールドが使用可能な場合:
   - スケジュールに適用する曜日をチェックボックスで選択するか、「**すべて**」を選択します。
   - スケジュールを開始する時刻を「**開始時刻**」フィールドに入力します。
   - スケジュールを終了する時刻を「**終了時刻**」フィールドに入力します。
7. 「**追加**」を選択して、スケジュールを「**スケジュール リスト**」に追加します。
8. 「**保存**」をクリックします。「**スケジュール**」が作成されます。

スケジュールの変更

既定と個別の両方のスケジュールを変更するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > スケジュール**」に移動します。
2. マウス カーソルを編集したいスケジュールに重ね、**編集**アイコンをクリックします。「**スケジュールの編集**」ダイアログが表示されます。

3. スケジュールの各種構成要素（時刻、種別、日など）を変更できます。ただし、既定のスケジュールの名前を変更することはできません。このフィールドは淡色表示になっています。変更を行うには、「個別スケジュールの追加」の手順に従ってください。
4. 「**保存**」をクリックします。

個別スケジュールの削除

個別スケジュールは削除できますが、既定のスケジュールを削除することはできません。

スケジュール オブジェクトを削除するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > スケジュール**」に移動します。
2. マウス カーソルを削除したいスケジュールに重ね、**削除**アイコンをクリックします。

複数のスケジュール オブジェクトを削除するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > スケジュール**」に移動します。
2. 「スケジュール」テーブルで、複数のユーザ定義スケジュールを選択し、ページ上部の「**削除**」をクリックします。

7

動的グループ

動的グループは、動的外部アドレス グループ（DEAG）と動的外部アドレス オブジェクト（DEAO）で構成されます。動的外部アドレス グループは、メンバーが動的なアドレス グループです。動的外部アドレス オブジェクトは、動的外部アドレス グループ ファイルがダウンロードされたときに動的に作成され、動的外部アドレス グループの下に配置される中間の内部オブジェクトです。動的外部オブジェクト機能を使用すると、メンバーを追加または削除するためにアドレス グループを手動で変更する必要がなくなります。

「動的グループ」ページ

DEAG エントリの多くのフィールドにマウスを移動すると、ポップアップ ツールチップが表示されます。複数の動的外部アドレス グループを構成でき、アクセス ルールまたはポリシーでこれらの DEAG を使用できます。たとえば、特定のアクセス ルールが適用されるすべてのパートナー IP アドレスのグループを維持する場合、動的外部アドレス グループ/動的外部オブジェクトを作成できます。

動的外部オブジェクトの作成は、2 つの部分で構成されます。

- FTP サーバまたは特定の URL のウェブ ページにおける外部動的アドレス グループ ファイルの作成
- SonicOS の「**オブジェクト > 動的グループ**」ページにおける動的外部アドレス グループの設定（DEAG ファイル内の情報のダウンロードおよび使用）

動的外部アドレス グループ ファイルについて

動的外部アドレス グループ ファイル（DEAG ファイル）には、IP アドレスまたは完全修飾ドメイン名（FQDN）（DEAG のメンバーである DEAO を定義する）のリストが含まれます。DEAG ファイルは、外部の FTP アクセス用サーバまたは HTTPS アクセス用特定 URL のウェブ ページに保存されます。この IP アドレスまたは FQDN のリストは、外部で変更可能です。定期的にファイルをダウンロードするように構成されている場合、変更に伴い関連する DEAO および DEAG は SonicOS で動的に更新されます。

DEAG ファイルには、以下の形式のの IP アドレスまたは FQDN のテキスト リストを格納できます。

- 1 行に 1 個の IP アドレスのリスト。CIDR 形式で指定されたサブネットを含めることができます。
- 1 行に 1 個の FQDN のリスト。FQDN は **www.example.com** などの文字列です。ワイルドカード（*）文字を含めることはできません。
- 1 行に 1 個の FQDN および IP アドレス/サブネットの混合リスト。これは FQDN 型 DEAG のみでサポートさ

れます。非 FQDN 型 DEAG は DEAG ファイル内で FQDN を受け入れません。

ただし、DEAG ファイル内で IP アドレスと FQDN を混在および照合することはお勧めしません。このリスト内の IP アドレスは FQDN としても処理され、SonicOS がその問題を解決しようとするからです。これらの入力タイプを混在させるには、FQDN 型および非 FQDN 型の DEAG を個別に作成してから、両方の DEAG をアクセス ルールで使用する個別のアドレス グループに追加することを推奨します。

それぞれの DEAG において、IP アドレス (*0.0.0.0*) のDEAO が自動的に作成されます。例えば、DEAG が 1 つしかない場合、DEAG ファイル内の IP アドレスの最大数は、「DEAG および DEAO の最大数」で定義される DEAO の許容最大数 − 1 となります。

DEAG および DEAO の最大数

最大 DEAG:

- IP アドレスと FQDN 種別を両方含む DEAG の最大数は、デバイスによってサポートされるアドレス グループの合計数の 25% です。
- 作成可能な DEAG の最大数は、ファイアウォール上でサポートされる合計数を超過するまでに残っているアドレス グループの数を超えることはできません。

  たとえば、デバイスが 1024 個のアドレス グループをサポートし、20 個のアドレス グループのみを使用している場合、256 個の DEAG (1024 個の 25%) を作成できます。ただし、既に 1000 個のアドレス グループを手動で作成している場合は、24 個の DEAG のみを作成できます。

最大 DEAO:

- *IP アドレス種別* DEAO の最大数は、デバイスによってサポートされるアドレス オブジェクトの合計数の 25% です。
- *FQDN* 種別 DEAO の最大数は、デバイスによってサポートされるアドレス オブジェクトの合計数の 50% です。
- 作成可能な DEAO の最大数は、ファイアウォール上でサポートされる合計数を超過するまでに残っているアドレス オブジェクトの数を超えることはできません。

高可用性の要件

高可用性ペアとして展開する場合、IP アドレスまたは FQDN のリストを含むファイルをダウンロードするには、アクティブ ファイアウォールとスタンバイ ファイアウォールの両方にサーバまたは URL への接続が必要です。これには、スタンバイ装置で監視 IP アドレスを設定する必要があります。

動的外部オブジェクトの追加

動的外部オブジェクトを追加するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > 動的グループ**」ページに移動します。
2. 「**追加**」ボタンを選択します。「**動的外部オブジェクトの追加**」ダイアログが表示されます。

3. 「**名前**」フィールドに、動的外部アドレス グループの一意のわかりやすい名前を入力します。「DEAG_」は保存時に名前の前に自動的に追加されます。
4. 「**種別**」フィールドは「*アドレス グループ*」に設定されます。他のオプションはありません。
5. 「**ゾーンの割り当て**」ドロップダウン リストで、動的外部アドレスグ グループのゾーンを選択します。
6. 動的アドレス グループ ファイルの定期ダウンロードを継続するには、「**定期的なダウンロードを有効にする**」オプションを選択します。
7. 「**定期的なダウンロードを有効にする**」が有効になっている場合、「ダウンロード間隔」フィールドでダウンロード間の分または時間を選択します。次のいずれかを選択できます。

   - 5 分
   - 15 分
   - 1 時間
   - 24 時間

8. 「**プロトコル**」ドロップダウン リストから、DEAG ファイルのダウンロードに使用するプロトコルの種別を選択します。選択肢は FTP または HTTPS です。ダイアログの残りのフィールドは、FTP と HTTPS で異なります。
9. **プロトコル**として「**FTP**」を選択した場合、以下を指定します。

   - **サーバ IP アドレス** – DEAG ファイルが保存されている FTP サーバの IP アドレス

     DEAG ファイルの詳細については、「動的外部アドレス グループ ファイルについて」を参照してください。
   - **ログイン ID** – FTP サーバにログインするためのユーザ名
   - **パスワード** – FTP サーバにログインするためのパスワード
   - **ディレクトリ パス** – FTP サーバ上で DEAG ファイルが保存されるフォルダ
   - **ファイル名** – FTP サーバ上の DEAG ファイルの名前

10. **プロトコル**として「**HTTPS**」を選択した場合、以下を指定します。
    - **URL 名** – IP アドレスまたは FQDN のリストが含まれる URL

    URL 名は、*https://* で始まり、ページ名が続く必要があります。このページには、IP アドレスまたは FQDN のリストが含まれています。
11. 「**保存**」をクリックします。

設定に基づいて、ファイアウォールはファイルまたは URL から IP アドレスまたは FQDN のリストを読み取ります。その後、SonicOS は次を自動的に作成します。

- 「**動的外部オブジェクトの追加**」ダイアログで指定された名前のアドレス グループ。このアドレス グループは読み取り専用です。つまり、編集または削除することはできません。
- ファイル内のすべての有効な一意の IP アドレスまたは FQDN のアドレス オブジェクト。これらのアドレス オブジェクトも読み取り専用です。

次に、個々のアドレス オブジェクトが動的外部アドレス グループ/動的外部オブジェクトに追加されます。これはアクセス ルールとポリシーで使用できます。

動的外部オブジェクトの編集

編集する動的外部オブジェクトの「**構成**」列で**編集**アイコンをクリックします。構成の設定は、「**動的外部オブジェクトの追加**」ダイアログと同じです。

動的外部オブジェクトの編集中に、DEAG の「**名前**」または「ゾーンの割り当て」を変更することはできません。

動的外部オブジェクトの削除

動的外部オブジェクトを削除するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > 動的グループ**」ページに移動します。
2. 以下のいずれかを実行します。

- 削除するオブジェクトの「**構成**」列で「削除」アイコンを選択します。
- 削除する 1 つ以上のオブジェクトのチェックボックスをクリックし、ページ上部の「**削除**」をクリックします。

ⓘ **補足:** アクセス ルールが使用している場合など、動的外部アドレス グループが使用されている場合、削除は失敗します。

8

電子メール アドレス

アプリケーション制御では、電子メール アドレス オブジェクトとして個別電子メール アドレス リストを作成できます。「**ポリシータイプ**」が「**SMTPクライアント**」の場合、アプリケーション ルールポリシーで電子メール アドレス オブジェクトのみを使用きます。電子メール アドレス オブジェクトは、個別ユーザまたはドメイン全体を表すことができます。さらに、個別アドレスのリストをオブジェクトに追加することで、グループを表す電子メール アドレス オブジェクトを作成することもできます。これにより、SMTP クライアントのアプリケーション ルールを作成するときに、ユーザ グループを容易に対象に含めたり対象から除外したりできます。詳細は、「**ポリシー > アプリケーション ルール**」を参照してください。

例えば、サポート グループを表す電子メール アドレス オブジェクトを作成できます。

電子メール アドレス オブジェクトにグループを定義した後、そのグループを対象として含める SMTP クライアント ポリシーまたは対象から除外する SMTP クライアント ポリシーを作成します。

「**ポリシー > アプリケーション ルール > 追加**」に移動し、送信電子メールへの実行可能ファイルの添付を禁止するポリシーからサポート グループが除外されています。電子メール アドレス オブジェクトは、SMTP クライアント ポリシーの「**メール送信者包含**」、「**メール送信者除外**」、「**メール受信者包含**」、または「**メール受信者除外**」フィールドで使用できます。「**メール送信者**」フィールドは、電子メールの送信者を表します。「**メール受信者**」フィールドは、電子メールの受信者を表します。

アプリケーション ルールでは Outlook Exchange または類似のアプリケーションからグループ メンバーを直接抽出することはできませんが、Outlook のメンバー リストを使用して、グループ メンバーがリストされたテキスト ファイルを作成することはできます。その後、このグループの電子メール アドレス オブジェクトを作成するとき、**アップロード**

アイコンをクリックしてテキスト ファイルからリストをインポートします。テキスト ファイル内で電子メール アドレスが 1 行に 1 つずつ記述されていることを確認してください。

電子メール アドレス オブジェクトの設定

電子メール アドレス オブジェクトの設定を構成するには、以下の手順に従います

1. 「**オブジェクト > 一致オブジェクト > 電子メール アドレス**」に移動します。
2. ページの上部にある「**追加**」をクリックします。「**電子メール アドレス オブジェクトの設定**」ダイアログが表示されます。

3. 「**電子メール ユーザ オブジェクト名**」フィールドに電子メール アドレス オブジェクトに対するわかりやすい名前を入力します。
4. 「**一致種別**」で、以下のいずれかを選択します。
   - 「**完全一致**」– 入力した電子メール アドレスとの厳密な照合を行う場合に使用します。
   - 「**部分一致**」– 入力した電子メール アドレスの任意の部分で照合を行う場合に使用します。
   - 「**正規表現一致**」– 正規表現と電子メール アドレスとの照合を行う場合に使用します。
5. 「**内容**」フィールドで、電子メール ID の**追加**アイコンをクリックします。
   - 例えば、ドメインに対して照合を行うには、前の手順で「**部分一致**」を選択し、「**内容**」フィールドでドメイン名を @ に続けて入力します（例: **@sonicwall.com**）。個々のユーザに対して照合を行うには、前の手順で「**完全一致**」を選択し、「**内容**」フィールドに完全な電子メール アドレスを入力します（例: **jsmith@sonicwall.com**）。

- 要素のリストをテキスト ファイルからインポートするには、**アップロード**アイコンをクリックします。ファイル内の各要素は、1 行に 1 つずつ記述されている必要があります。

  ユーザのリストを含む電子メール アドレス オブジェクトを定義することで、アプリケーション ルールを使用してグループをシミュレートできます。

6. 「**保存**」をクリックします。

   電子メール アドレス オブジェクトが作成され、テーブルに表示されます。

9

SonicWall サポート

有効なメンテナンス契約が付属する SonicWall 製品をご購入になったお客様は、テクニカル サポートを利用できます。

サポート ポータルには、問題を自主的にすばやく解決するために使用できるセルフヘルプ ツールがあり、24 時間 365 日ご利用いただけます。サポート ポータルにアクセスするには、次の URL を開きます:
https://www.sonicwall.com/ja-jp/support

サポート ポータルでは、次のことができます。

- ナレッジ ベースの記事や技術文書を閲覧する。
- 次のサイトでコミュニティ フォーラムのディスカッションに参加したり、その内容を閲覧したりする:
  https://community.sonicwall.com/technology-and-support
- ビデオ チュートリアルを視聴する。
- https://mysonicwall.com にアクセスする。
- SonicWall のプロフェッショナル サービスに関して情報を得る。
- SonicWall サポート サービスおよび保証に関する情報を確認する。
- トレーニングや認定プログラムに登録する。
- テクニカル サポートやカスタマー サービスを要請する。

SonicWall サポートに連絡するには、次の URL を開きます: https://www.sonicwall.com/ja-jp/support/contact-support

このドキュメントについて

補足: メモ アイコンは、補足情報があることを示しています。

重要: 重要アイコンは、補足情報があることを示しています。

ヒント: ヒント アイコンは、参考になる情報があることを示しています。

注意: 注意アイコンは、手順に従わないとハードウェアの破損やデータの消失が生じる恐れがあることを示しています。

警告: 警告アイコンは、物的損害、人身傷害、または死亡事故につながるおそれがあることを示します。

SonicOS 一致オブジェクト 管理者ガイド
更新日 – 2021 年 4 月
ソフトウェア バージョン – 7
232-005639-10 Rev B

エンド ユーザ製品利用規約

SonicWall エンド ユーザ製品利用規約を参照する場合は、次に移動してください: https://www.sonicwall.com/ja-jp/legal

オープン ソース コード

SonicWall Inc. では、該当する場合は、GPL、LGPL、AGPL のような制限付きライセンスによるオープン ソース コードについて、コンピュータで読み取り可能なコピーをライセンス要件に従って提供できます。コンピュータで読み取り可能なコピーを入手するには、「SonicWall Inc.」を受取人とする 25.00 米ドルの支払保証小切手または郵便為替と共に、書面によるリクエストを以下の宛先までご送付ください。

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035