SonicOS 7
ダッシュボード

管理ガイド

--- TZ シリーズ用

SONICWALL®

目次

1

ダッシュボード

ダッシュボードには、システム、アクセス ポイント、キャプチャ ATP、WWAN、トポロジ用の監視表示が含まれています。

- 「システム」では、「**サマリ**」タブに「**ネットワーク**」、「**脅威**」、「**デバイス**」の詳細情報の概要が表示されます。「**サマリ**」モジュールが、これらの各特性に関するデータ レポートを提供します。
- 「**アクセス ポイント**」オプションは、接続されているオンラインおよびオフラインのすべてのアクセス ポイントからなるアクセス ポイント スナップショット、アクセス ポイントに関連付けられているクライアント、帯域幅消費量、クライアント報告、リアルタイム クライアント監視を提供します。
- 「**キャプチャ ATP**」は、疑わしいコードを分析するクラウドベースのネットワーク サンドボックスを提供します。

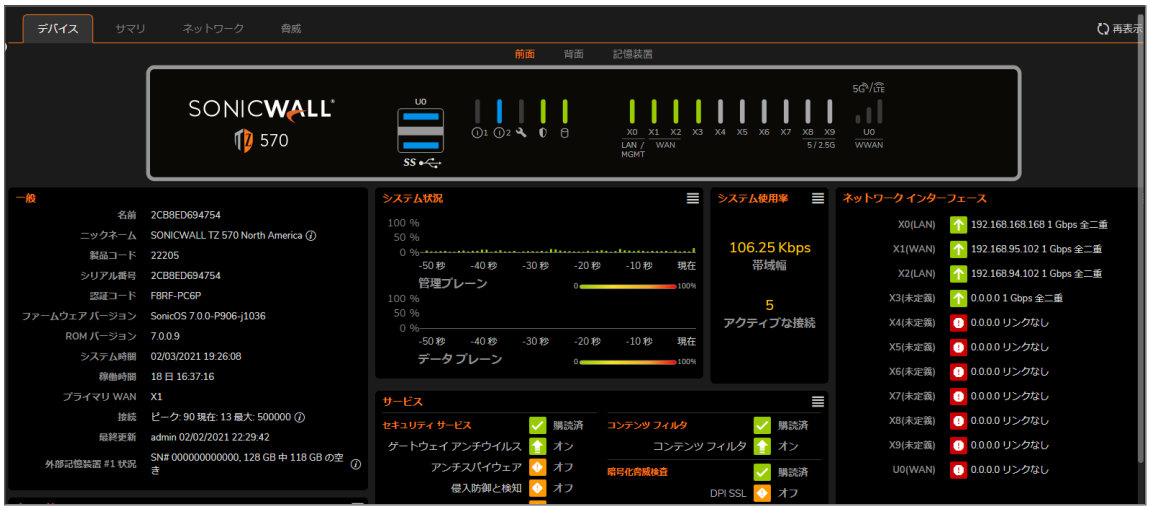
  「**WWAN**」は、使用環境に接続されている3G/4G/LTE デバイスを視覚化します。

  「**トポロジ**」は、ネットワーク マッピングと接続デバイスを表示し、関連付けられているシステムの概要を示します。

2

システム

「**ホーム | ダッシュボード > システム | デバイス**」表示は、SonicOS への初回ログイン時に表示される既定の表示です。ここでは、状況の概要と、インフラ内に含まれるデバイスに関して「**ネットワーク**」表示と「**脅威**」表示で設定されたレポートを確認できます。「**ホーム**」表示は、以下を含む大部分の作業の出発点と考えてください。



トピック:

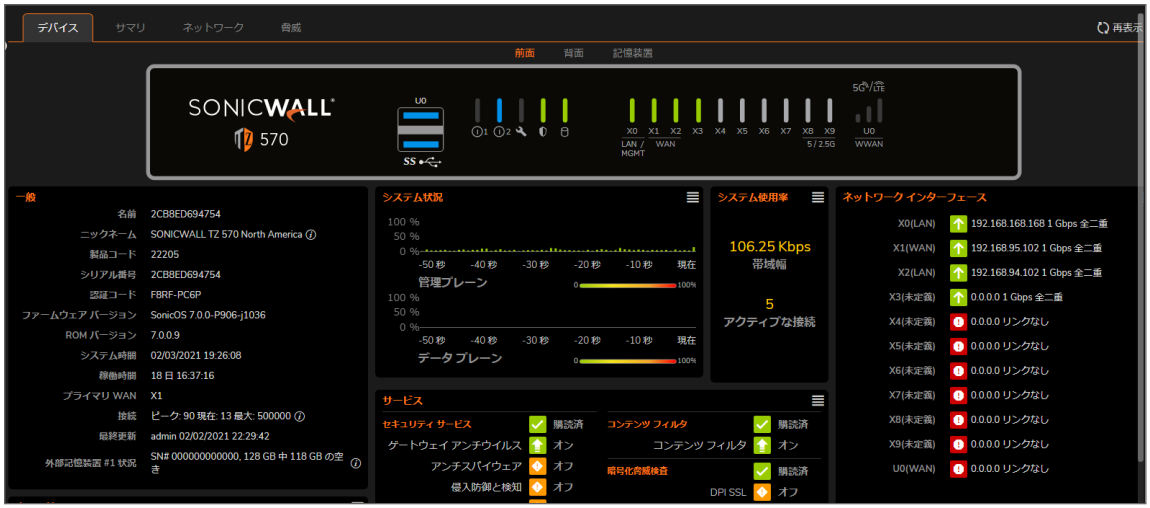
- サマリ
- ネットワーク
- 脅威
- デバイス

ⓘ | **重要:** オンプレミスの Analytics に実装されている場合、SonicOS でゼロ タッチはサポートされません。

ⓘ | **補足:** 「**概要**」セクションで使用可能な情報は、他の表示で選択した表示種別によって異なります。

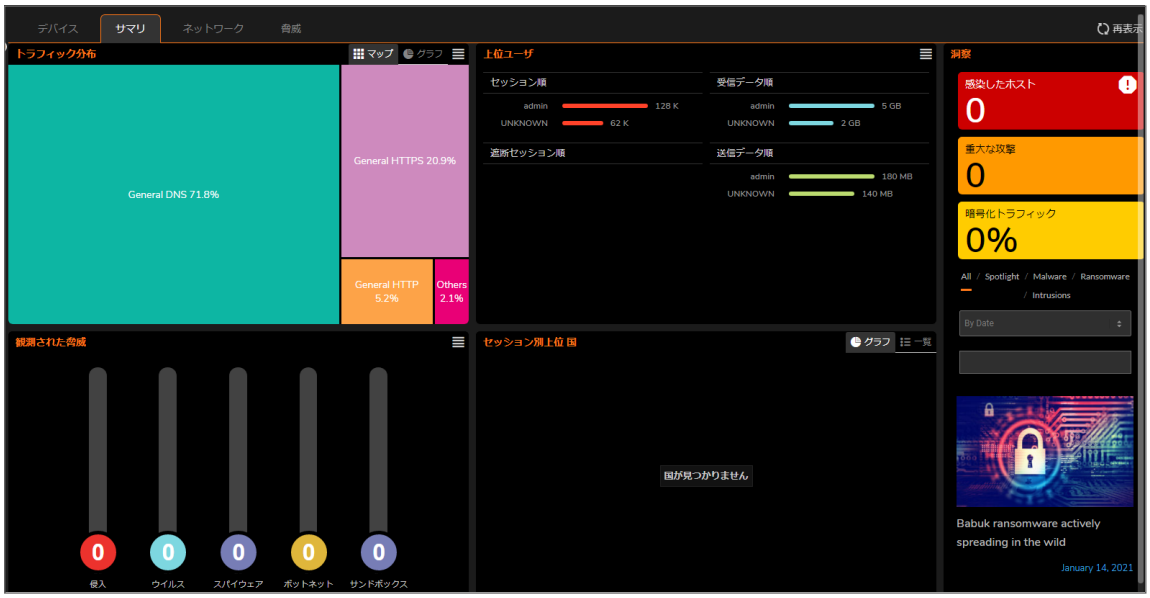
デバイス

「**ホーム | ダッシュボード > システム | デバイス**」表示には、システムに接続されている装置の関連情報が表示されます。デバイスに関する一般的な詳細情報を示すウィンドウ サマリが、テーブルのグループとして表示されます。これらの表示内では、デバイスの前面、背面、ストレージの表示だけでなく、ライセンス、高可用性データ、システム状況なども確認できます。



サマリ

「**ホーム | ダッシュボード > システム | サマリ**」にある「**システム サマリ**」は、セキュリティ インフラの状態の概要を提供します。見やすく、色分けされたインジケータでアクティビティを要約しています。「システム サマリ」を確認すると、調査が必要な問題の有無が一目でわかります。



「**システム サマリ**」には、デバイスと、生成されているトラフィックを表したものが表示されます。また、拡大/縮小できる地図を使用して、デバイスを地理的に表示することができます。デバイスは地図上にマークされます。

次の表に、「**システム サマリ**」を構成する要素を示します。

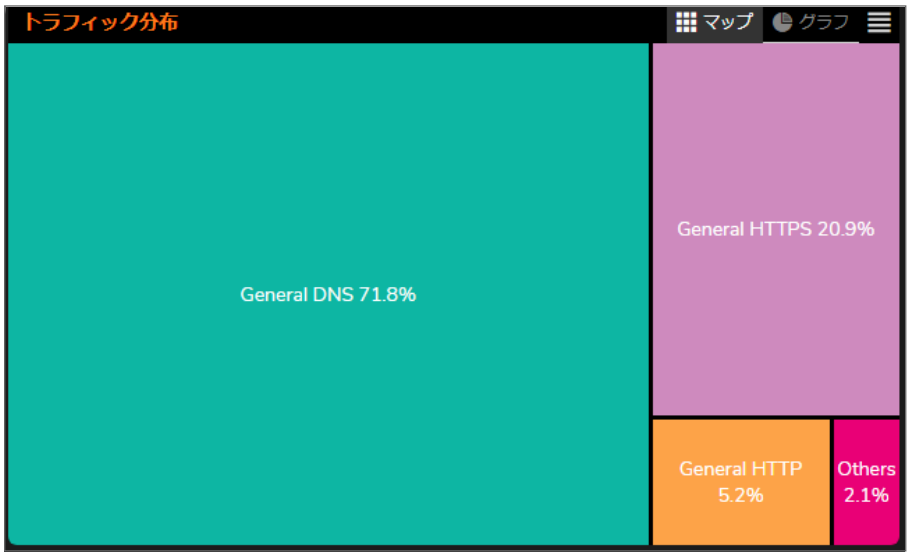
サマリの概要

機能	説明
トラフィック分布	脅威とその位置を含む、インフラ内のすべてのトラフィックを表示します。

機能	説明
上位ユーザ	システムに接続しているユーザに関するデータを提供します。
観測された脅威	システム接続レポートが開始された脅威の数を追跡します。
サービス サマリ	ネットワーク内で使用できる（または使用できない）すべての動作中/停止中および購読済/未購読のサービスの概要を提供します。

トラフィック分布

「**トラフィック分布**」ウィンドウは、脅威とその位置を含む、インフラ内のすべてのトラフィックを表示します。脅威は、世界地図の上に視覚的に配置されます。マウスのローラーを使用して、脅威を拡大/縮小することができます。この種のデータを使用して、利用できるすべての情報を深く掘り下げて調べることができます。



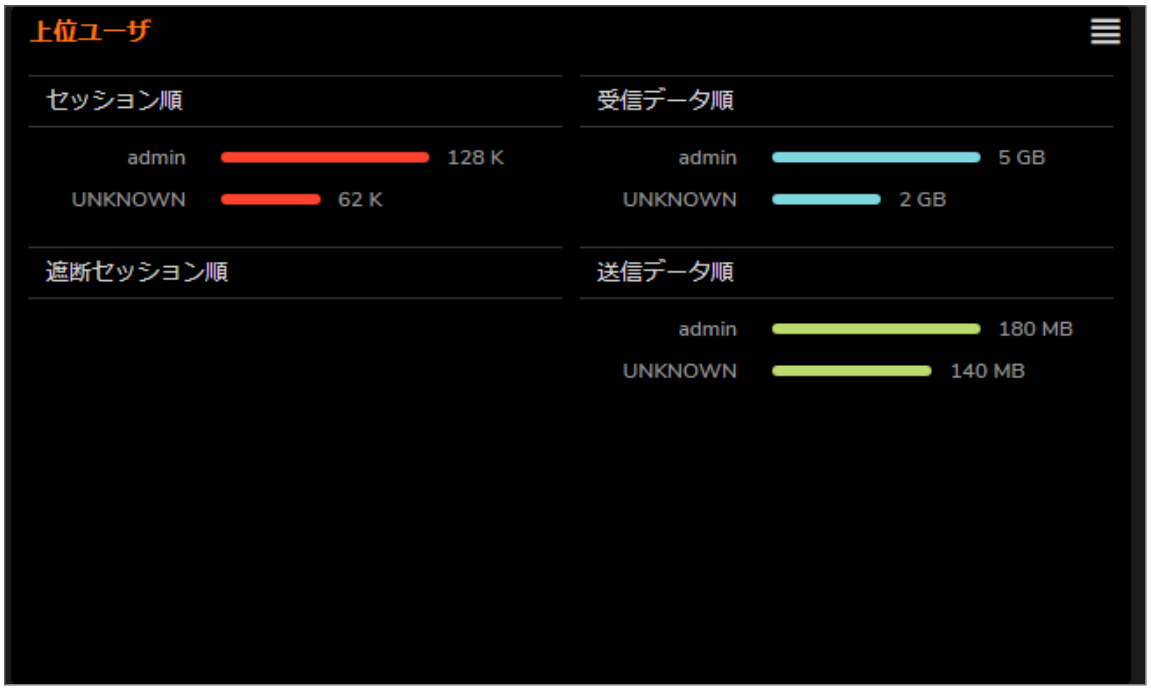
「**トラフィック分布**」には、デバイスと、生成されているトラフィックを表したものが表示されます。このウィンドウでは、拡大/縮小できる地図を使用して、デバイスを地理的に表示することができます。デバイスは地図上にマークされます。

この地図は、プライベート IP、ファイアウォール、脅威、受信トラフィック、送信トラフィックに関する情報を提供します。

「トラフィック マップ」セグメントでも、詳細情報をドリルダウンすることができます。拡大/縮小を行うには、世界地図上でマウス ホイールを使用するか、地図の左側にある縦方向の + と − のスライダーを使用します。その他の詳細情報をドリルダウンするには、地図上の旗やアイコンを選択します。

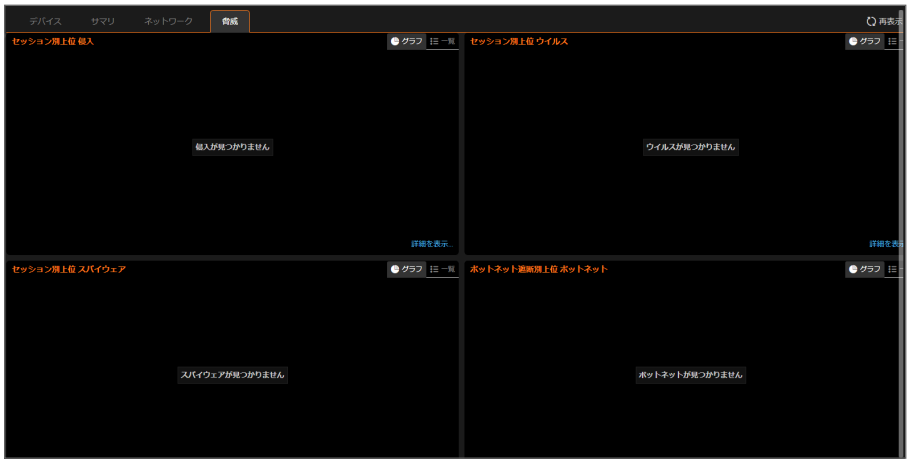
上位ユーザ

「**上位ユーザ**」レポート ウィンドウは、システムに接続しているユーザに関するデータを提供します。セッション、受信バイト、送信バイト、遮断バイトなど、数種類のオプションでフィルタすることによって、ユーザ レベルのトランザクションとアクティビティを追跡できます。



観測された脅威

「**観測された脅威**」は、システム接続レポートが開始された脅威の数を追跡します。既定の表示は「接続の総数」ですが、「脅威」ドロップダウン リストの上位の侵入、ウイルス、スパイウェア、ボットネットでフィルタすることができます。使用可能な各種脅威レポートを確認するには、「**ホーム | ダッシュボード > システム | 脅威**」に移動します。使用可能なフィルタ オプションを展開するには、各ウィンドウの**オプション** アイコンを選択します。

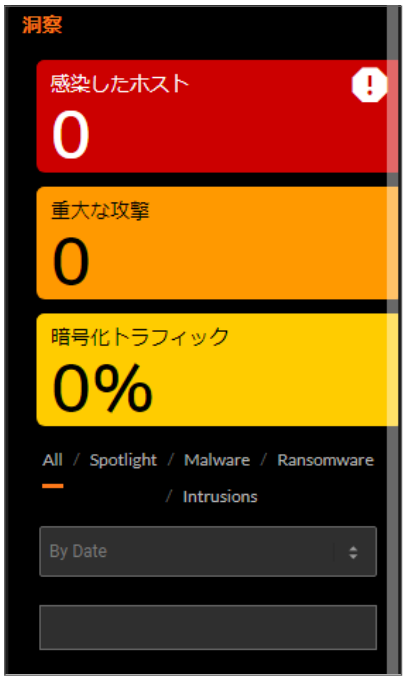


サービス サマリ

「**サービス サマリ**」ウィンドウは、ネットワーク内で使用できる（または使用できない）すべての動作中/停止中および購読済/未購読のサービスの概要を提供します。

洞察

「洞察」ウィンドウは、セキュリティ インフラ全体の状況の概要を提供します。このウィンドウは、見やすく、色分けされたインジケータでアクティビティを要約しています。「洞察」を確認すると、調査が必要な問題の有無や、スポットライティング、マルウェア、ランサムウェア、侵入、またはこれらすべてを使用した追加のフィルタリングが一目でわかります。



ネットワーク

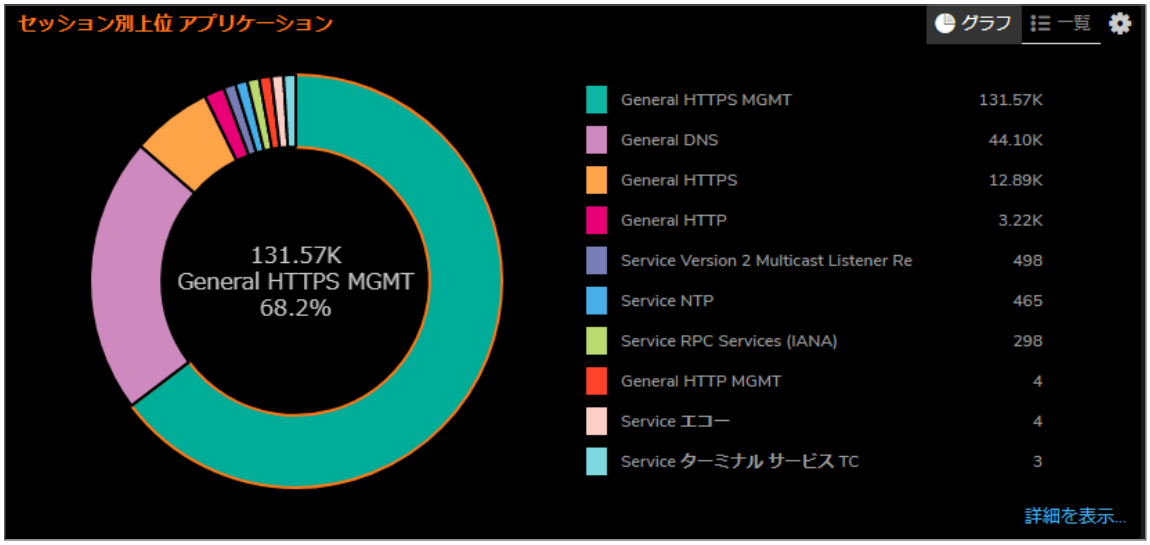
「**ネットワーク**」表示は、上位のアプリケーション、アドレス、ユーザ、ウェブサイト格付け、国などを表示するセッション レポート ウィンドウを提供します。

トピック:

- 上位アプリケーション
- 上位アドレス
- 上位ユーザ
- 上位ウェブサイト格付け
- 上位国

上位アプリケーション

「**上位アプリケーション**」ウィンドウは、ファイアウォールを流れるすべてのアプリケーションを 1 秒あたりのビット数で示します。



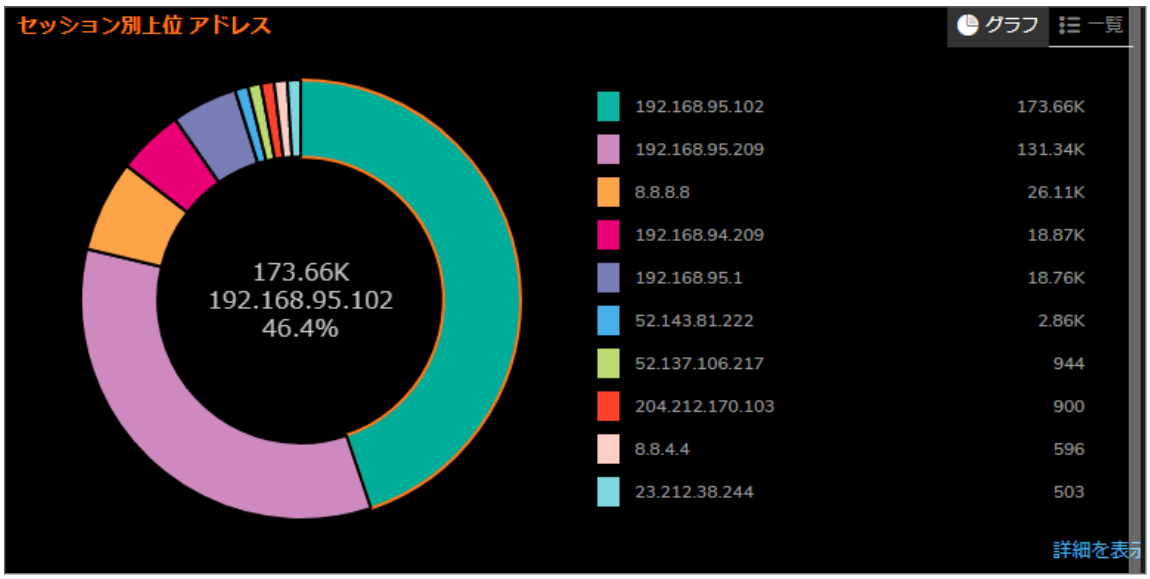
以下の項目別の「**上位アプリケーション**」を含む数種類のオプションでフィルタすることによって、他のアプリケーション レベルのトランザクションとアクティビティも追跡できます。

- 始動バイト
- 応答バイト
- アクセス ルール遮断
- アプリケーション ルール遮断
- 位置
- ボットネット遮断
- ウイルス
- 侵入
- スパイウェア

「**監視 | AppFlow > AppFlow 報告 | アプリケーション**」にあるすべてのアプリケーション フィルタリングに関する詳細なレポートを確認するには、「**詳細を表示**」を選択します。

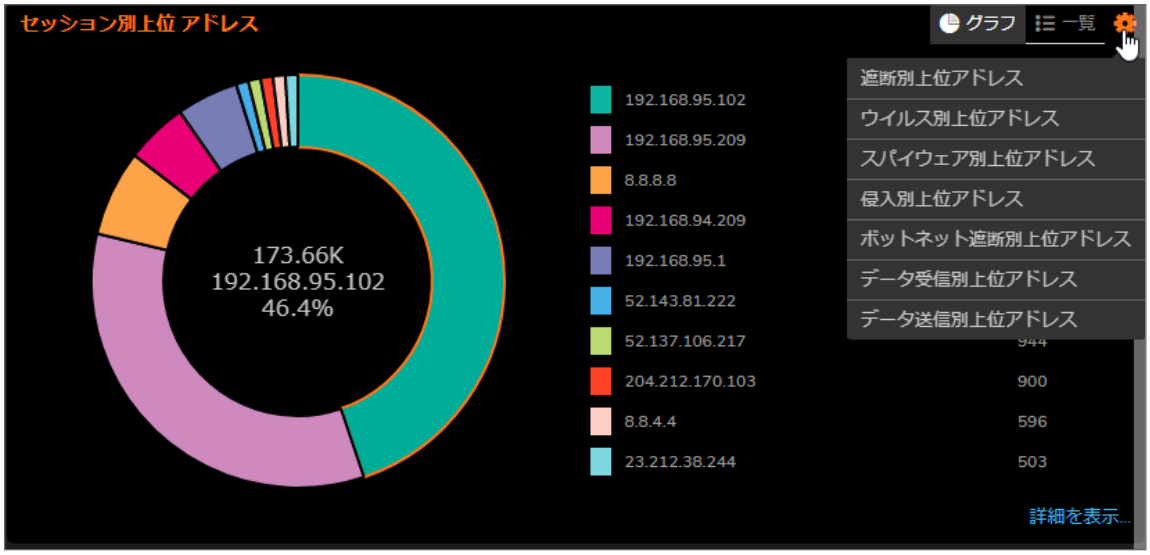
上位アドレス

「**セッション別上位アドレス**」レポートは、システムに接続している IP アドレスに関するデータを提供します。



以下の項目別の「**上位アドレス**」を含む数種類のオプションでフィルタすることによって、IP アドレス レベルのトランザクションとアクティビティを追跡できます。

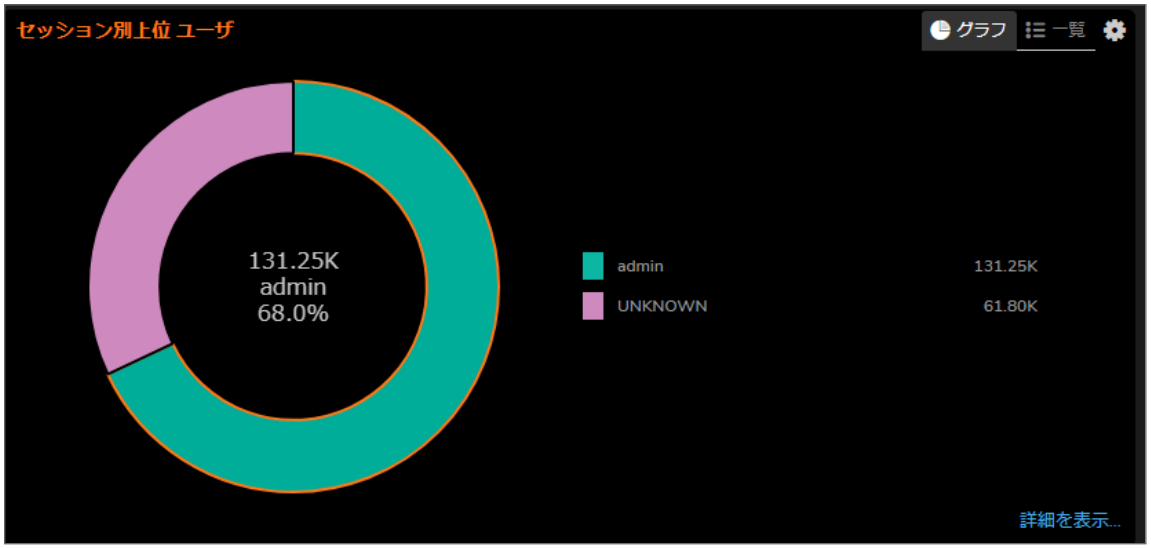
- 遮断
- ウイルス
- スパイウェア
- 侵入
- ボットネット遮断
- 受信バイト数
- 送信バイト数



「**監視 | AppFlow > AppFlow 報告 | IP**」にあるすべての IP アドレスに関する詳細なレポートを確認するには、「**詳細を表示**」を選択します。

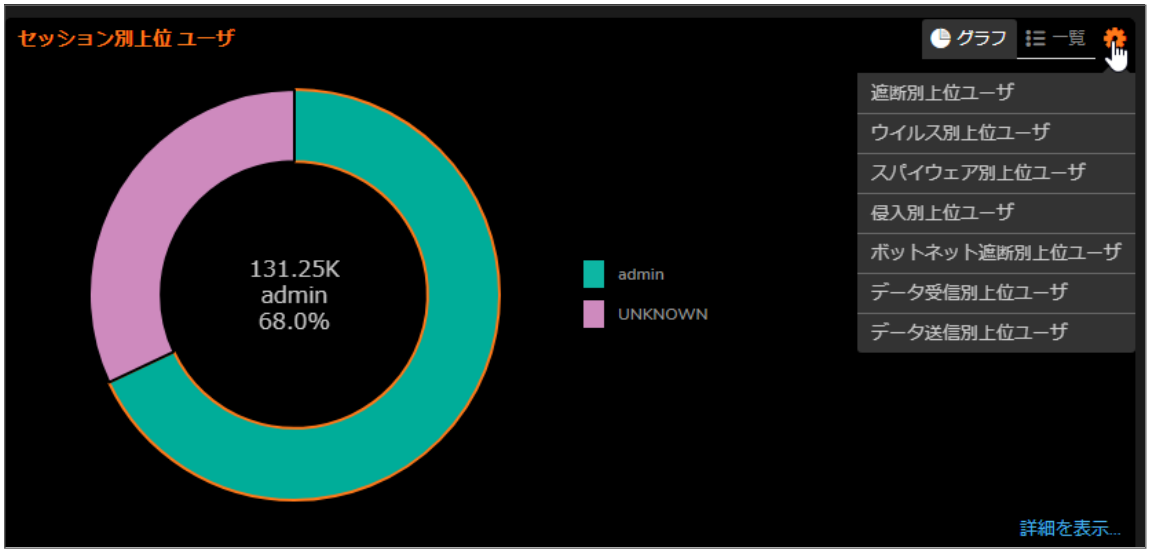
上位ユーザ

「**セッション別上位ユーザ**」レポートは、システムに接続している上位ユーザに関するデータを提供します。



以下の項目別の「**上位ユーザ**」を含む数種類のオプションでフィルタすることによって、ユーザ レベルのトランザクションとアクティビティを追跡できます。

- 遮断
- ウイルス
- スパイウェア
- 侵入
- ボットネット遮断
- 受信バイト数
- 送信バイト数



「**監視 | AppFlow > AppFlow 報告 | ユーザ**」にあるすべてのユーザに関する詳細なレポートを確認するには、「**詳細を表示**」を選択します。

上位ウェブサイト格付け

「**セッション別上位ウェブサイト格付け**」レポートは、システムによって処理された URL に関するデータを提供します。

以下の項目別の「**上位ウェブサイト格付け**」を含む数種類のオプションでフィルタすることによって、URL レベルのトランザクションとアクティビティを追跡できます。

- 個数
- 割合

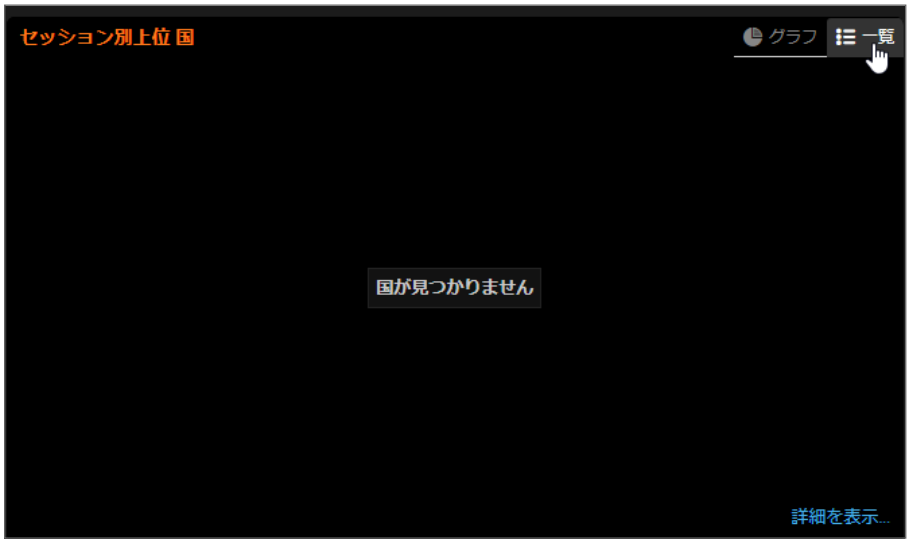
「**監視 | AppFlow > AppFlow 報告 | URL 格付け**」にあるすべてのウェブサイト格付けに関する詳細なレポートを確認するには、「**詳細を表示**」を選択します。

上位国

「**セッション別上位国**」レポートは、システムに接続している国の位置に関するデータを提供します。

以下の項目別の「**上位国**」を含む数種類のオプションでフィルタすることによって、位置レベルのトランザクションとアクティビティを追跡できます。

- 破棄
- 受信バイト数
- 送信バイト数



「**監視 | AppFlow > AppFlow 報告 | 位置**」にあるすべての国に関する詳細なレポートを確認するには、「**詳細を表示**」を選択します。

脅威

以下のレポートは、脅威によって影響を受けた接続の数を追跡します。ドロップダウン メニューにリストされている他のオプションでフィルタすることもできます。

トピック:

- 上位ウイルス
- 上位侵入
- 上位スパイウェア
- 上位ボットネット

上位ウイルス

「**セッション別上位ウイルス**」レポートは、システムによって処理されたウイルス脅威に関するデータを提供します。以下の項目別の「**上位ウイルス**」を含む数種類のオプションでフィルタすることによって、ウイルス レベルのトランザクションとアクティビティを追跡できます。

- 個数
- 割合

「**監視 | AppFlow > AppFlow 報告 | ウイルス**」にあるすべてのウイルスに関する詳細なレポートを確認するには、「**詳細を表示**」を選択します。

上位侵入

「**セッション別上位侵入**」レポートは、システムによって処理された侵入に関するデータを提供します。

以下の項目別の「**上位侵入**」を含む数種類のオプションでフィルタすることによって、侵入レベルのトランザクションとアクティビティを追跡できます。

- 個数
- 割合

「**監視 | AppFlow > AppFlow 報告 | 侵入**」にあるすべての侵入に関する詳細なレポートを確認するには、「**詳細を表示**」を選択します。

上位スパイウェア

「**セッション別上位スパイウェア**」レポートは、システムによって処理されたスパイウェア脅威に関するデータを提供します。

以下の項目別の「**上位スパイウェア**」を含む数種類のオプションでフィルタすることによって、スパイウェア レベルのトランザクションとアクティビティを追跡できます。

- 個数
- 割合

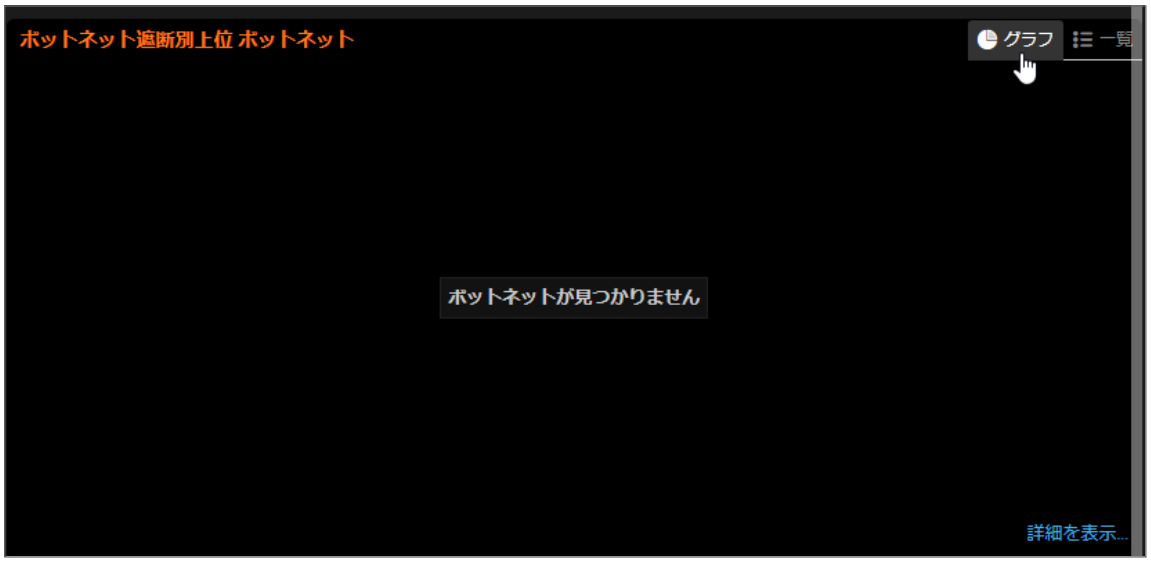
「**監視 | AppFlow > AppFlow 報告 | スパイウェア**」にあるすべてのスパイウェアに関する詳細なレポートを確認するには、「**詳細を表示**」を選択します。

上位ボットネット

「**遮断ボットネット別上位ボットネット**」レポートは、システムに接続しているボットネット脅威に関するデータを提供します。

以下の項目別の「**上位ボットネット**」を含む数種類のオプションでフィルタすることによって、ボットネット レベルのトランザクションとアクティビティを追跡できます。

- 遮断
- ウイルス
- スパイウェア
- 侵入
- 受信バイト数
- 送信バイト数



「**監視 | AppFlow > AppFlow 報告 | IP**」にあるすべてのボットネットに関する詳細なレポートを確認するには、「**詳細を表示**」を選択します。

パケット フィルタリング

パケット フィルタリングは、システムへのネットワーク アクセスを制御するためのファイアウォール手法です。送受信パケットを監視し、送信元および送信先のインターネット プロトコル (IP) アドレス、プロトコル、ポートに基づいて通過または停止させることができます。パケット フィルタリングは、以下のフィルタのいずれかを使用して強制することができます。

アクセス ルール遮断

「**アクセス ルール遮断**」レポートは、適用するアクセス ルールによって遮断された接続の数を追跡します。

アプリケーション ルール遮断

「アプリケーション ルール遮断」レポートは、アプリケーション ルールによって遮断された接続の数を追跡します。ドロップダウン メニューからオプションを選択できます。

遮断

このレポートは、遮断された接続の数を追跡します。

ボット ネット

このレポートは、システム内で検出されたボットネットのアドレスを追跡します。

受信バイト数

受信バイト数フィルタは、ホストから受信した合計バイトをレポートします。受信バイト数と送信バイト数を合わせると、サーバとホスト コンピュータ間の通信リンク上の総データ転送量になります。

送信バイト数

送信バイト数フィルタは、ホストに送信した合計バイトをレポートします。受信バイト数と送信バイト数を合わせると、サーバとホスト コンピュータ間の通信リンク上の総データ転送量になります。

破棄

「**破棄**」フィルタは、破棄されたインターフェース上で送信された（「送信」テーブル内）または受信された（「受信」テーブル内）パケットまたはバイトの総数を示します。インターフェースが飽和状態になると、サーバのメカニズムによって破棄されたパケットごとに 1 回、この数字がインクリメントされます。

始動者バイト

「**始動者バイト**」レポートには、送信元の場所に基づいて接続数が表示されます。ドロップダウン メニューにリストされている接続種別でフィルタすることができます。ドロップダウン メニューから、追加の送信元 IP レポートをタイトルで選択することができます。

侵入

「侵入」サマリには、2 種類のレポートが含まれます（別々のタブで表示されます）。侵入に対するセッション/接続/始動/応答の数と、統計上の割合です。

場所

このレポートには、送信先の国に基づいて接続数が表示されます。ドロップダウン メニューから、追加の送信先 IP レポートをタイトルで選択することができます。

応答者バイト

「**応答者バイト**」レポートには、送信元の IP アドレスに基づいて接続数が表示されます。ドロップダウン メニューにリストされている送信元種別でフィルタすることができます。ドロップダウン メニューから、追加の送信先 IP レポートをタイトルで選択することができます。

スパイウェア

このレポートは、システム内で検出されたスパイウェアを追跡します。スパイウェアが検出された接続、または遮断されたスパイウェア（名前）でフィルタすることができます。

ウイルス

このレポートは、システム内で検出されたすべてのウイルスを追跡します。ウイルスが検出された接続、または遮断されたウイルスに基づいてフィルタすることができます。詳細情報はテーブルに表示されます。

3

アクセス ポイント

SonicWave および SonicPoint AC 機器に対して、「**ホーム | ダッシュボード > アクセス ポイント**」は、表やグラフを使って、インフラに接続しているアクセス ポイントに関連したデータを視覚化できます。リアルタイムの状態および状態の履歴を両方とも表示できるほか、個別のクライアントの速度、OS の種類およびホスト名も表示します。また、SonicWave および SonicPoint 機器の状態も表示し、さらに監視と問題の診断を支援する情報も提供します。

トピック:

- 機能上の制限
- アクセス ポイント スナップショット
- リアルタイム帯域幅
- クライアント報告
- リアルタイム クライアント監視
- クライアント報告とクライアント監視フィルタリング

機能上の制限

SonicWave および SonicPoint AC 機器の状態は、機器が SonicWallファイアウォールによって管理されている場合に表示されます。ファイアウォールとアクセス ポイントの両方が機能している必要があります。そうでない場合、有

効なデータが交換されません。SonicWave アクセス ポイントは、常時、ダッシュボード データの 7 日間の履歴を保持します。ただし、メモリの制限により、SonicPoint AC 機器は再起動されるとすべての履歴データを失います。

アクセス ポイント スナップショット

「**ホーム | ダッシュボード > アクセス ポイント | アクセス ポイント オンライン/オフラインおよびクライアント参加**」の「**アクセス ポイント スナップショット**」セクションには、2 つのグラフが表示されます。右の方で、これらの表を更新する間隔を指定できます。ドロップダウン メニューから分数を選択してください。オプション範囲は 5～10 分です。

アクセス ポイント オンライン/オフライン

「**アクセス ポイント オンライン/オフライン**」グラフは、インフラ内のアクセス ポイントの状態を短くまとめて表示します。データはドーナツ グラフで表示されます。オンラインは緑色、オフラインは赤色です。グラフの右側には、アクセス ポイントの数と状態も表示されます。

オンライン ステータスには、利用可能、無効、再起動中、IDS スキャン モードが含まれます。

オフライン ステータスには、無応答および初期化状態が含まれます。

クライアント参加

「**クライアント参加**」グラフは、構成内の個別のアクセス ポイントに関連付けられたクライアントの数を表示します。ユーザ数は棒グラフ形式で表示されます。

リアルタイム帯域幅

「**ホーム | ダッシュボード > アクセス ポイント**」の「**リアルタイム帯域幅**」セクションには、選択されたアクセス ポイントで使用されている帯域幅のグラフが表示されます。

ⓘ **補足:** SonicPoint ACe/ACi/N2 および SonicWave 機器だけが、「**リアルタイム帯域幅**」機能をサポートしています。

SonicOS は、選択されたアクセス ポイントのリアルタイム トラフィックの積み上げグラフを示します。Y 値は、受信および送信の両方の合計トラフィックです。既定では、すべてのアクセス ポイントが表示用に選択されています。

更新間隔を選択するには、グラフのタイトルの近くにあるドロップダウン メニューから更新間隔を選択してください。オプションは、1 分、2 分、5 分、10 分、60 分 です。

表示するアクセス ポイントを変更するには、「**アクセス ポイント**」ドロップダウン メニューに移動して、別の機器を選択してください。グラフは、当該のアクセス ポイントに対するデータに更新されます。

クライアント報告

「**ホーム | ダッシュボード > アクセス ポイント**」の「**クライアント報告**」セクションには、3 つのグラフが表示されます。「**OS 種別**」、「**無線**」、「**上位クライアント**」です。

ⓘ | **補足:** SonicPointクライアント レポートSonicWave機能をサポートするのは、**ACe / ACi / N2 および** 機器のみです。

OS 種別

OS 種別円グラフには、接続されている Windows クライアント、Macintosh クライアント、Linux クライアント、iPhone、Android などの割合が表示されます。クライアントが HTTP トラフィックを生成していない場合、「**不明**」と表示されることがあります。

ⓘ | **補足:** SonicPointOS 種別SonicWave機能をサポートするのは、**ACe / ACi / N2 および** 機器のみです。

無線

クライアント報告は**無線**チャートも提供します。**無線**チャートには、2.4GHz 無線と 5GHz 無線に接続されているクライアントの割合が表示されます。

ⓘ | **補足:** SonicPoint無線SonicWave機能をサポートするのは、**ACe / ACi / N2 および** 機器のみです。

上位クライアント

「**上位クライアント**」グラフは、誰が一番帯域幅を使用しているかを表示します。「上位」フィールドに移動してドロップダウン メニューから数を選択します。帯域幅使用者のトップ 5、トップ 10、トップ 15、またはトップ 20 を表示できます。上位ユーザについて、送信および受信データの数値が表示されます。

ⓘ | **補足:** SonicPoint上位クライアントSonicWave機能をサポートするのは、**ACe / ACi / N2 および** 機器のみです。

リアルタイム クライアント監視

「**ホーム | ダッシュボード > アクセス ポイント**」の「**リアルタイム クライアント監視**」セクションには、クライアント接続状況の詳細グラフが表示されます。アクセス ポイントを通じて接続している個別のユーザの詳細を提供します。MAC アドレス、ホスト名、OS 種別、受信 (Rx) トラフィック量、および送信 (Tx) トラフィック量が表示できます。

ⓘ | **補足:** SonicPoint ACe/ACi/N2 および SonicWave 機器だけが、**リアルタイム クライアント監視**機能をサポートしています。

クライアント報告とクライアント監視フィルタリング

「**クライアント報告**」セクションと「**リアルタイム クライアント監視**」セクションの両方で出力をフィルタリングできます。具体的には、「**すべて**」または特定のアクセス ポイントを「**アクセス ポイント**」ドロップダウン メニューで選択します。あるいは、「**すべて**」または特定の SSID を「**SSID**」ドロップダウン メニューで選択します。

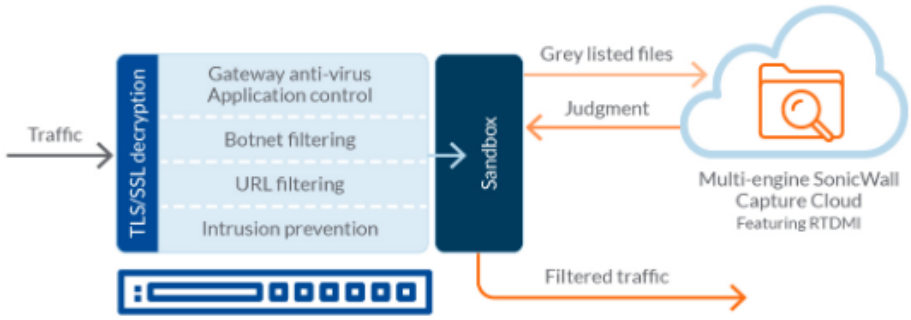
ⓘ **補足:** SonicPoint ACe / ACi / N2 および SonicWave 機器のみがクライアント詳細フィルタリングをサポートします。

4

キャプチャ ATP

「**ホーム**」表示の「**SonicWall キャプチャ ATP (高度脅威防御)**」セクションは、疑わしいコードを分析するクラウドベースのネットワーク サンドボックスを提供します。これにより、判定が下るまでゲートウェイでランサムウェア、高度で継続的な脅威 (APT)、ゼロデイ攻撃を発見し、ネットワークへの侵入を阻止することができます。このセクションには、防御のためのバックエンドへのファイル送信に使用されているファームウェアの状況が表示されます。

キャプチャ ATP は、疑わしいコードの動作を分析するため、SonicWall の Real-Time Deep Memory Inspection (RTDMI)、システム全体のエミュレーションおよび仮想化手法などの多層型サンドボックスを提供します。キャプチャ ATP は、トラフィック、疑わしいコード、幅広いサイズおよび種別のファイルをスキャンします。



キャプチャ ATP のダッシュボード

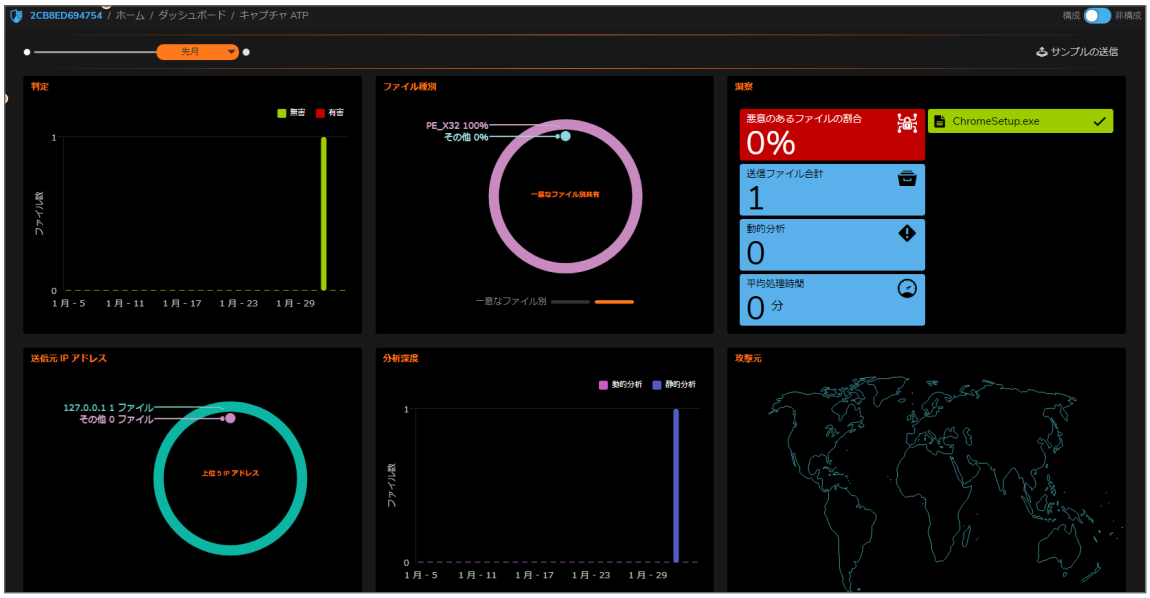
キャプチャ ATP ダッシュボード (「**ホーム | ダッシュボード > キャプチャ ATP**」) を使用して、スキャンのためにバックエンドに送信されているファイルや遮断されているファイルを 1 つの場所で確認することができます。青色のボックスはスキャンされたファイルの総数を示し、赤色のボックスは見つかった有害ファイルの総数を示します。ファイルのスキャン期間には、前月、前週、または最新 24 時間を指定できます。

キャプチャ ATP ダッシュボードは、ファイアウォールが作業を行った日付と、スキャンされたファイルの数についての情報も提供します。色付きの棒グラフで、有害ファイルが見つかった割合と日数を示します。

このセクションでは、他のレポートも利用できます。また、「**ユーザ定義**」ドロップダウン メニューを使用して、カスタマイズされたレポート ウィンドウを作成できます。「**列選択**」ドロップダウン メニューでスキャン対象のファイルにフィルタを追加し、ファイルの特性、ファイル名、ファイル ハッシュ、種別、送信者、日付、時間別にリストしてファイルを表示することもできます。キャプチャ ATP は、「**ポリシー | キャプチャ ATP > 設定**」でも設定できます。

詳細については、『*SonicWall 管理サービス キャプチャ ATP 管理ガイド*』を参照してください。

キャプチャ ATP はゲートウェイ アンチウイルス（GAV）と同様に、ファイアウォールに対するアドオン セキュリティ サービスであり、システムで有害ファイルを識別するために使用します。このサービスを有効にするには、ライセンス、GAV サービス、クラウド アンチウイルス データベース サービスが必要です。



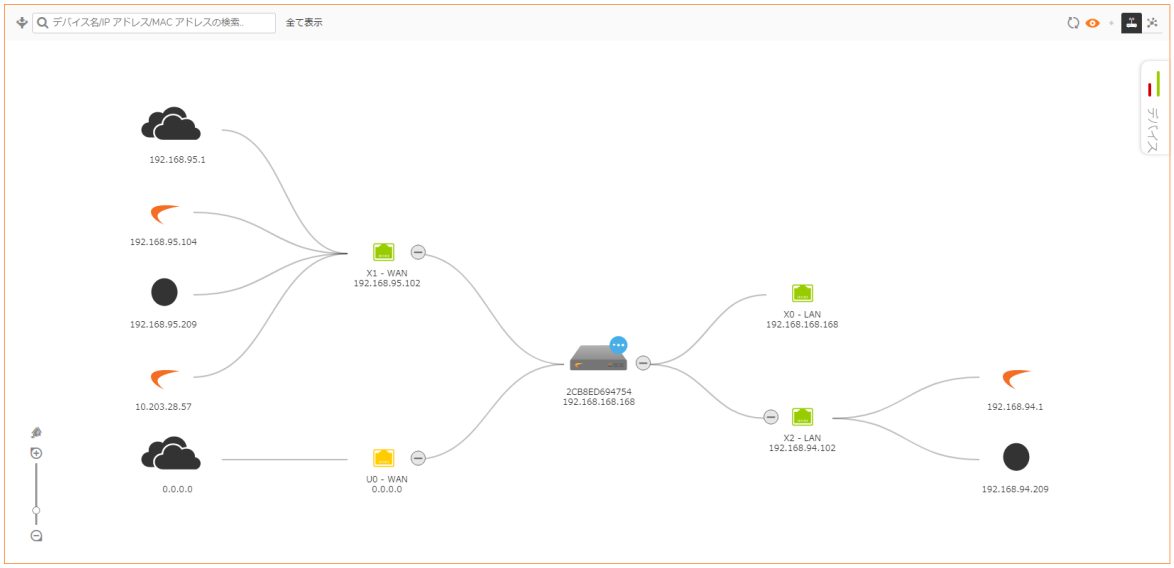
5

トポロジ

「**ホーム | ダッシュボード > トポロジ**」ページで、トポロジ機能を使用してデバイスを管理できます。トポロジは、SonicWall ファイアウォールから無線アクセス ポイントまでのネットワークトポロジを表示します。アクセス ポイントのリアルタイムの状態を監視できます。コンテキスト メニューは、設定オプションも提供します。

この機能により、すべての WAN、LAN、WLAN ゾーンのデバイス間の論理的な関係を表示し、トポロジでデバイスを直接管理できるようになります。

「**ホーム | ダッシュボード > トポロジ**」ページには、ファイアウォールが認識している接続デバイスとそれらの関係を示す、樹形または網目状の図が表示されます。以下の図と同様なものです。



トピック:

- トポロジ表示の管理
- トポロジ表示でのアクセス ポイントの管理

トポロジ表示の管理

トポロジ表示はシンプルなインターフェースです。表示を最新に維持し、インフラ内の物理機器を変更する手段を提供します。

トポロジ表示内で、個々の機器の詳細情報を得ることもできます。カーソルを機器の上に重ねると、ツールチップがポップアップします。機器の種別によって、名前、IP アドレス、インターフェース、モデルなどの情報を表示します。アクセス ポイントに対しては、状況やクライアント数など、追加情報が表示されます。

個々のアクセス ポイントは、状況を示すために色分けされています。

- 緑 = オンライン
- 赤 = オフライン
- 黄 = ビジー

トポロジ表示でのアクセス ポイントの管理

トポロジ表示にはコンテキスト メニューがあり、その中にはアクセス ポイントの管理に使用できる命令があります。

ⓘ **補足:** コンテキスト メニューはアクセス ポイントのみに適用されます。トポロジ マップ上の他の機器にはコンテキスト メニューはありません。

トピック:

- アクセス ポイントの編集
- 統計の表示
- アクセス ポイントの監視状況
- アクセス ポイントの削除

アクセス ポイントの編集

アクセス ポイントをトポロジ表示内で編集するには、以下の手順に従います。

1. 「**ホーム | ダッシュボード > トポロジ**」に移動します。
2. マウスを編集したいアクセス ポイントに重ねます。
3. アクセス ポイントを右クリックします。
4. 「**このアクセス ポイントを編集する**」を選択します。
5. 必要に応じて、オブジェクト設定に変更を加えます。
6. 新しい設定を保存するために「**OK**」をクリックします。

統計の表示

アクセス ポイントの統計を表示するには、以下の手順に従います。

1. 「**ホーム | ダッシュボード > トポロジ**」に移動します。
2. マウスを表示したいアクセス ポイントに重ねます。
3. アクセス ポイントを右クリックします。
4. 「**アクセス ポイント統計の表示**」を選択します。
5. 統計を再表示するには、「**再表示**」をクリックします。
6. 完了したら「**OK**」を選択します。

アクセス ポイントの状況の監視

アクセス ポイントをトポロジ表示内で監視するには、以下の手順に従います。

1. 「**ホーム | ダッシュボード > トポロジ**」に移動します。
2. マウスを監視したいアクセス ポイントに重ねます。
3. アクセス ポイントを右クリックします。
4. 「**アクセス ポイント監視状況**」を選択します。
   アクセス ポイント監視は、アクセス ポイントの状況を表示します。CPU 使用率、メモリ使用率、受信速度と送信速度を含みます。
5. データを再表示するには、「**再表示**」をクリックします。
6. アクセス ポイントの詳細を表示するには、**詳細**アイコンをクリックします。
7. 完了したら「OK」を選択します。

アクセス ポイントの削除

アクセス ポイントをトポロジ表示内で削除するには、以下の手順に従います。

1. 「**ホーム | ダッシュボード > トポロジ**」に移動します。
2. マウスを削除したいアクセス ポイントに重ねます。
3. アクセス ポイントを右クリックします。
4. 「**アクセス ポイントの削除**」を選択します。
5. アクセス ポイントを削除する場合には確認を、そうでない場合にはキャンセルを行います。

6

法的情報

SonicOS に関する法的情報は、「**ホーム | 法的情報**」に記載されています。

本製品のダウンロードおよび使用に適用される条件は、https://www.sonicwall.com/ja-jp/legal/#tab-id-3（"契約書"）をご覧ください。本契約書には、貴方（貴社）が本製品を使用する方法や関連する制限、保証および保証の否認、損害賠償の制限および請求される可能性のある救済措置、監査権などの条項が含まれているため、よくお読みください。本製品をダウンロード、インストール、又は利用することにより、貴方（貴社）は本契約の条件を承諾しこれに同意します。本契約の条件に同意しない場合は、本製品に対するライセンスがないため、本製品のダウンロード、インストール、又は利用はお控え下さい。

7

API

SonicWall API の利用に関する契約は、「**ホーム | API**」で確認できます。

SonicOS API をご利用になる前に本契約を熟読して下さい。本 API をダウンロード、インストール、又は利用することにより、貴方（貴社）は本契約の条件を承諾しこれに同意します。HTTPS://SONICOS-API.SONICWALL.COM にアクセスして、製品の API の該当するバージョンをご覧ください。本契約の条件に同意しない場合は、本 API のダウンロード、インストール、又は利用はお控え下さい。

8

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 サービスを要求する。

SonicWall サポートに連絡するには、次の URL にアクセスします。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 ダッシュボード 管理ガイド 目的:対象:TZ シリーズ
更新日 – 2021 年 3 月
ソフトウェア バージョン – 7
232-005436-10 Rev B

エンドユーザ製品契約

SonicWall エンドユーザ製品契約を参照する場合は、以下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、書面による要求を以下の宛先までお送りください。

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