PRTG Network Monitor – リモートプローブと複数プローブ

この資料では、PRTG Network Monitor のリモートプローブの概要について説明します。

情報源

この資料の情報源は以下のとおりです：

メーカーマニュアル：PRTG Manual: Remote Probes and Multiple Probes
https://www.paessler.com/manuals/prtg/remote_probes_and_multiple_probes

本資料は Paessler AG 作成の資料/ナレッジベースをジュピターテクノロジー株式会社（以下当社と略記）が独自で翻訳したものです。ベストエフォートの翻訳であるため、最新情報ではない可能性があります。最新情報は情報源をご確認ください。

リモートプローブと複数プローブ

PRTG をインストールすると、最初のプローブ（PRTG Network Monitor の場合はローカルプローブ、PRTG Hosted Monitor の場合はホステッドプローブ）が自動的に作成されます。これらのプローブは PRTG コアサーバーシステム上で動作し、システムから到達可能なデバイス、サーバー、サービスをセンサーで監視します。

PRTG Network Monitor で LAN や 1 つの場所のみを監視する場合は、ローカルプローブだけで十分です。PRTG Hosted Monitor のホステッドプローブはインターネット経由で一般に公開されている対象にのみ到達可能なため、PRTG Hosted Monitor で LAN を監視する場合は、少なくとも 1 つのリモートプローブが必要です。

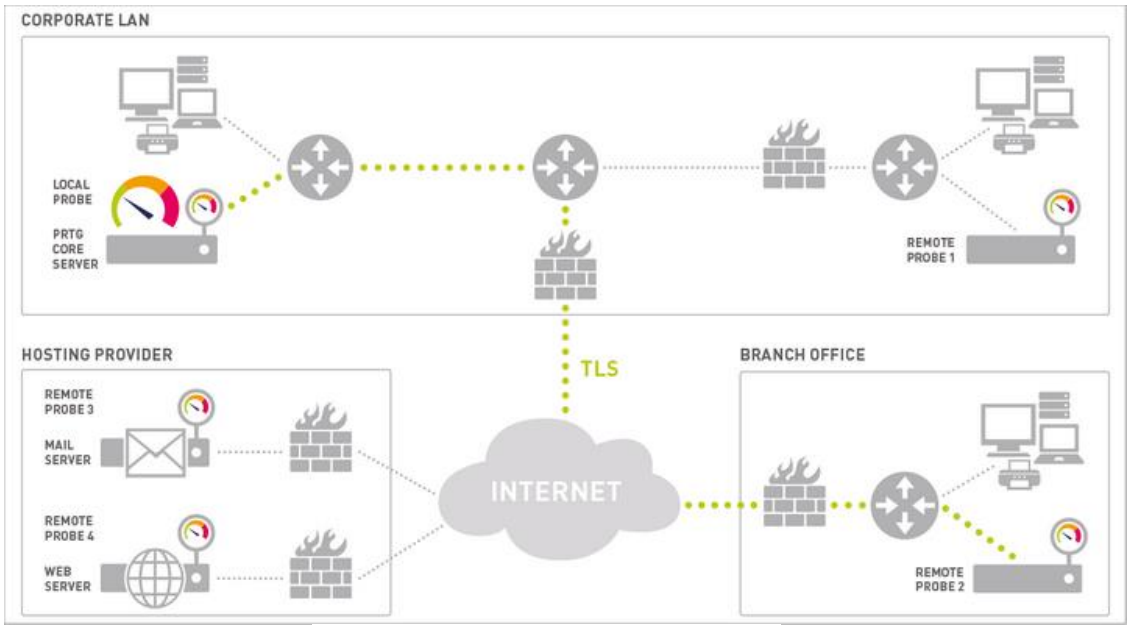
リモートプローブが必要になるシナリオ

同一 LAN 内、または遠隔地でリモートプローブが必要になる状況がいくつかあります。次のような状況です。

- PRTG Hosted Monitor を使用しており、ローカルネットワークを監視したい。
- 複数の拠点があり、すべての拠点からサービスの可用性を確認する必要がある。
- ネットワークがファイアウォールで区切られた複数の LAN に分割されていて、ローカルプローブがファイアウォールを超えて特定のサービスを監視できない。

- セキュリティ保護されたネットワーク内のシステムを監視するために、PRTG コアサーバーとそのネットワーク間で安全な接続が必要。
- 別のコンピューターをパケットスニファーしたい。
- 別のコンピューターで NetFlow データを監視したい。
- パケットスニファーや NetFlow センサーのような CPU 負荷の高いセンサーでパフォーマンスの問題が発生し、複数のコンピューターで負荷分散する必要がある。

次の図は、リモートプローブのシナリオの例を示しています。



PRTG による分散ネットワークの監視

社内 LAN 内の PRTG コアサーバー（左上）で次の監視が可能になっています：

- ローカルプローブを使用した社内 LAN 内のサービス
- リモートプローブ 1 を使用した、社内 LAN のファイアウォールの背後にあるサービス
- リモートプローブ 2 を使用した、別拠点（右下）のセキュリティ保護されたサービス
- サーバーに直接インストールしたリモートプローブ 3、4 を使用した、セキュリティ保護されたメールサーバーと Web サーバーのサービス
- いずれかのプローブを使用したインターネット上のパブリックサービス

プローブの仕組み

プローブは起動するとすぐに、自動的に PRTG コアサーバーに接続し、センサー設定をダウンロードし、監視タスクを開始します。ユーザーが監視設定を変更すると、PRTG コアサーバーは新しい設定データをプローブに送信します。プローブは自律的に監視を行い、実行したチェックごとに監視結果を PRTG コアサーバーに送ります。

PRTG コアサーバーとプローブ間の接続が何らかの理由（PRTG コアサーバーシステムの再起動など）

で切断されても、プローブは監視を継続し、結果を保存します。接続が切断されている間はリモートプローブシステムの RAM に最大 50 万件のセンサー結果を保存します（最大 50～200MB）。つまり、100 個のセンサーでスキャン間隔が 1 分の場合、プローブは最大 3 日分（10,000 個のセンサーでスキャン間隔が 1 分の場合は 52 分）の監視結果を保存しておくことができます。プローブは、PRTG コアサーバーが使用可能になると自動的にすぐ再接続し、切断中に収集したすべての監視結果を送信します。

プローブと PRTG コアサーバー間の接続はプローブから開始され、その通信は SSL（Secure Sockets Layer）/TLS（Transport Layer Security）で保護されています。つまり、PRTG コアサーバーとプローブの間で送受信されるデータは、データパケットをキャプチャーしても見ることはできません。PRTG コアサーバーは TCP/IP ポートをオープンし、プローブからの接続試行を待ちます。新しいプローブが初めて接続されると、ToDo チケットを発行し、デバイスツリーに新しいプローブを表示します。

セキュリティ対策として、センサーを作成する前に、デバイスツリーでプローブを手動で承認する必要があります。プローブを拒否し、切断することもできます。その場合、PRTG はそれ以降の接続試行を受け付けず、設定の「接続を拒否する IP アドレス」リストにプローブの IP が追加されます。これにより、不正なプローブが PRTG コアサーバーに接続できないようにします。

プローブが接続を開始するには、外部からコアサーバーへ接続できることを確認する必要があります。このプロセスは、ポート 80 または 443 を介して PRTG コアサーバーの Web サーバーにアクセスする場合と同様です。ほとんどの場合、プローブが TCP（Transmission Control Protocol）ポート 23560 経由で PRTG コアサーバーに到達できるようにする許可、または NAT ルールが必要になります。なお、プローブは送信接続の際はハイポート範囲（49152～65535）の動的ポートを使用します。

ⓘ PRTG Hosted Monitor インスタンスへのリモートプローブ接続の場合も上記が適用されますが、PRTG Hosted Monitor インスタンス（DNS 名または基になる IP アドレス）への送信接続が可能で、この特定のポートで到達可能であることを、リモートプローブ側でのみ確認すればよいという点が主な違いになります。

クラスターで PRTG を実行する場合、リモートプローはすべてのクラスターノードに接続し、監視データを送信します。この動作は上記の一台のコアサーバーの場合と同様です。マスターノードに障害が発生しても、フェイルオーバーノードで監視データを確認できます。各プローブの「クラスター接続状況」はプローブの設定の「プローブ管理設定」で定義できます。

プローブの自動アップデート

新しい PRTG バージョンをコアサーバーにインストールし、アップデートされたコアサーバーにリモートプローブが再接続すると、すべてのリモートプローブはすぐにアップデートされたバージョンを自動的にダウンロードしてインストールします。

PRTG コアサーバーをアップデートすると、PRTG はローカルプローブをアップデートします。すべてのリモートプローブは SSL/TLS で保護されたプローブ接続または PRTG コアサーバー接続を介して、新しいバイナリを自動的にダウンロードします。4MB のファイルのダウンロードには、利用可能な帯域幅にもよりますが、数秒（LAN 内）から数分（インターネット接続経由）かかります。アップデートがダウンロードされるとすぐに、リモートプローブは接続を切断し、アップデートをインストールし、

PRTG コアサーバーに再接続します。これには 20～100 秒かかります。アップデート中は、ダウンロードに必要な帯域幅のため、ローカルプローブによる監視に影響が出る可能性があることに注意してください。

ⓘ アップデート後にリモートプローブの切断が続く場合は、リモートプローブを使用しているサーバーに異なる IP アドレスを持つ 2 つのネットワーク接続がないか確認してください。これらのアドレスが「コア&プローブ」設定の「接続を許可する IP アドレス」のリストにあることを確認してください。

リモートプローブの削除

接続済みのリモートプローブをデバイスツリーで削除すると、リモートプローブシステム上の「PRTG Probe Service」が停止し、スタートアップの種類が「手動」に設定されます。リモートプローブシステム上のリモートプローブを別途アンインストールすることをお勧めします。

未接続状態のリモートプローブを削除した場合、リモートプローブシステム上の「PRTG Probe Service」は停止せず、スタートアップの種類も変更されません。リモートプローブは「PRTG Probe Service」を停止するか、リモートプローブをアンインストールするまで、PRTG コアサーバーへの再接続を試みつづけます。

参考情報

■ PAESSLER WEBSITE

How to connect PRTG through a firewall in 4 steps

https://www.paessler.com/support/how-to/firewall

■ VIDEO TUTORIAL

Distributed monitoring with PRTG

https://www.paessler.com/support/videos-and-webinars/videos/distributed_monitoring

免責事項・使用限定事項

ジュピターテクノロジー株式会社（以下当社と略記します）が作成した本ドキュメントに関する免責事項および本ドキュメント使用に関する限定事項は以下の通りです。

本ドキュメントに関する免責事項

本ドキュメントは作成時点においてメーカーより提供された情報および当社での検証結果により作成されたものですが、当社は本ドキュメントの内容に関していかなる保証をするものではありません。万一、内容についての誤りおよび内容に基づいて被った損害が発生した場合でも一切責任を負いかねます。本ドキュメントの内容によりなされた判断による行為で発生したいかなる損害に対しても当社は責任を負いません。

本ドキュメント使用に関する限定事項

別に定める場合を除いて、本ドキュメントの取り扱いは当社より提供を受けたお客様による私的かつ非営利目的での使用に限定されます。お客様は、本ドキュメントについて、変更、コピー、頒布、送信、展示、上映、複製、公開、再許諾、二次的著作物作成、譲渡、販売のいずれも行うことができません。

お問い合わせ

PRTG Network Monitor について、ご不明な点などございましたらお問い合わせください：

ジュピターテクノロジー株式会社（Jupiter Technology Corp.）

住所：　〒183-0023　東京都府中市宮町一丁目 40 番地　KDX 府中ビル 6F

URL：　https://www.jtc-i.co.jp/

電話番号：　042-358-1250

購入前のお問い合わせ先：　https://www.jtc-i.co.jp/contact/scontact.php

購入後のお問い合わせ先：　https://www.jtc-i.co.jp/support/customerportal/

発行日　2023 年 12 月 07 日
修正日　2023 年 12 月 07 日
ジュピターテクノロジー株式会社