

Network Traffic Guide

2013 年 3 月

概要

- SiteAuditのトラフィックへの影響
- SiteAudit検索のメカニズム
- トラフィック計測方法
- ネットワークトラフィック例

このドキュメントでは、SiteAudit のデータ収集方法と、ネットワークへの負荷を最低限に抑えるためのメカニズムをご説明します。実装者、IT 管理者を対象読者に想定しています。

ネットワークトラフィック

ネットワークトラフィック は、ネットワークのデザイン、ネットワーク数、サブネット/ルーティングなどによって変化します。SiteAuditは、ネットワークトラフィックに与える影響を最低限に抑えることをモットーとしています。

●SiteAuditのネットワークトラフィックへの影響は？

SiteAuditの通常の動作中、ネットワークトラフィックへの影響はほとんどありません。ネットワークの回線容量、サービスの質への影響もほとんどありません。「ネットワークを自動的に検索」オプションが選択されている場合、SiteAuditはブロードキャストを実行し、ネットワークやデバイスを検索します。ご使用の環境に応じてブロードキャストを無効にすることも、検索範囲を狭めることもできます。検索サイクル中のネットワークトラフィックは約3~5%になります。SiteAuditではこの時点でネットワークトラフィックに与える影響が最大になります。SiteAuditでは、セットアップを簡易化するため、IPネットワーク検索データの自動インポートを許可しています。（Knowledge Base内の「データのインポート」の記事をお読みください。）

検索のメカニズム

SiteAuditではすべてのプリンタ資産が検索可能です。ブロードキャストが有効になっている場合、検索サイクル中にのみブロードキャストが送信されます。以下の2種類のブロードキャストパケットを送信します。

- SNMP
- ICMP

検索は以下の手順で実行されます。

- 1) リスト上の各ネットワークのアドレスを確認。
- 2) 検索対象から除外するアドレスがあるかないか確認（他のネットワークまたは領域経由）。
- 3) 検索対象に含めるアドレスに対してICMPパケットを送信。
- 4) ICMPパケットに応答があった場合
- 5) SNMPに対応しているかどうか確認。指定の各コミュニティストリングを試行。
- 6) 以下のポートをスキャンし、プリンタを検出。
 - 161 SNMP: SNMP が使用可能かどうか確認（データ収集に使用）
 - 80 HTTP: 組込み web サーバーがあるかどうか確認（データ収集に使用）
 - 9100 プリンタ用プリントプロトコル向け（データ収集に使用）
 - 1650 同上
 - 631 IPP: プリントプロトコル（データ収集に使用）
 - 135 RPC: 以前は直接接続されたプリンタの Windows ホスト検出に使用
- 7) 標準プリンタMIBがサポートされている場合、プリンタはネットワークプリンタ。
- 8) SNMPがサポートされているが標準プリンタMIBはサポートされておらず、9100番ポート（または同等）がサポートされている場合もプリンタはネットワークプリンタ。
- 9) ICMPに回答するものの、ネットワークプリンタではない場合、135番ポートがサポートされているかどうか確認。
- 10) 135番ポートがサポートされている場合、WMIとクレデンシャルの1つを使って接続を試行。
- 11) クレデンシャルが正しかった場合、そのホストにローカルプリンタまたはプリントキューがあるかどうか確認。
- 12) 検索プロセスはマルチスレッドにも対応しています（ただし、ホストマシンとリソースによって対応状況は異なる可能性があります）。

検索スキヤンのタイミング

検索にかかる時間は、以下の条件によって異なります。

- 1) SiteAuditが動作しているホストとホスト上のリソース（プロセッサ、メモリ、ネットワーク回線容量など）
- 2) スキヤン対象となるネットワークアドレスの数
- 3) スキヤン対象となるすべてのネットワークを含めたネットワーク回線容量
- 4) スキヤン対象となるネットワークの密度

注：ネットワーク密度が低い場合、アドレスの中にICMPに応答しないものがあり、タイムアウト後に再試行しなければならないため、検索時間が長くなります。

検索スキヤンは7日おきに実行されます。検索スキヤンの終了に丸2日かかる場合、次のスキヤンはスキヤン終了後5日目に実行されます。検索スキヤンの終了に7日以上かかる場合は、スキヤン終了後ただちに次のスキヤンが実行されます。

ネットワークトラフィックへの影響がほぼ0の理由

SiteAuditのデータ収集は、「ゆっくりと安定したペースのパケット受信」と説明できます。そのため、ネットワークの回線容量をほとんどとりません。Web JetAdminのようなアプリケーションでは、「データブラスト」を送信するため、データ収集をオフピーク時にスケジューリングする必要があります。データがいつ使用可能になるか、ネットワークトラフィックにどれだけの影響があるかという点が競合製品とSiteAuditが最も大きく異なる点と言えます。

収集データ形式

SiteAuditは変化（volatile）データと安定（stable）データの2種類のプリンタデータを収集します。デフォルト値を以下に示します。

- 変化（Volatile）データ：頻繁に変化するデータ
 - ページ数：1時間ごとに収集
 - プリントジョブ：4時間ごとに収集
 - 消耗品情報：40分ごとに収集
 - スレッショルド情報：30分ごとに収集
 - デバイスステータス：10分ごとに収集
 - MAC（移動・追加・変化）
- 安定（Stable）データ（頻繁に変化しないデータ）
 - ネットワーク、ID情報：7日間ごとに収集
 - 設定情報（入出力オプション）：12時間ごとに収集

SiteAuditでは、検出したアドレスで、プリンタではないもののデータも保管します。その例を以下に示します。

- ・ SNMP情報、ポート情報
- ・ Windowsホスト：メーカー、型番、最後にリポートした日時、ログインユーザ（設定されている場合）
- ・ プリントサーバーであるWindowsホストでキューがあるもの：ジョブデータ（設定されている場合）

ネットワークトラフィック量

ネットワークトラフィックはSiteAuditがモニタしているデバイスの数によって異なります。パケット数を計算する場合の条件を以下に示します。

検索トラフィック

- ICMP: 検索設定されている各ネットワークの各IPアドレスに対してICMPパケットを送信します。ネットワークに対するブロードキャストアドレスが含まれている場合、そのネットワークに対してICMPブロードキャストを送信します。デバイスが応答しない場合、3度再試行します。

- SNMP: 検索設定されている各ネットワークの各IPアドレスに対してSNMPパケットを送信します。ネットワークに対するブロードキャストアドレスが含まれている場合、そのネットワークに対してICMPブロードキャストを送信します。デバイスが応答しない場合、3度再試行します。パケットは各コミュニティストリングに対して再試行されます。このパケットは、デフォルトで提供されているコミュニティストリングの中から、頻繁に使用しないコミュニティストリングを削除することで数を減らすことができます。

- ポートスキャン：ICMPパケットに回答するデバイスに対してはポートスキャンパケットも送信します。各デバイスの161番、80番、8080番、9100番、1650番、631番、135番のポートをスキャンします。UDPポートである161番ポートを除き、いずれもTCPポートです。スキャンは3度再試行します。

トラフィックのモニタ

- 変化データ：デバイスの種類と各デバイスのカウンタ、消耗品データによって異なります。高性能のデバイスは通常20個程度のカウンタをサポートしていますが、各カウンタに対して1つのパケットが必要になります。普通のデバイスは3個から4個のカウンタをサポートしています。各パケットは512バイトです。再試行は行いません。

消耗品データは、高性能のデバイスは3個から4個の消耗品をサポートしており、各消耗品は6種類の異なる情報を伴っています。そのため、高性能のデバイスの場合、パケットは18から24個必要になります。

アラートはアラートテーブルの内容をチェックしてからポーリングを行います。アラートテーブルに変更がない場合は取得しません。アラートテーブルには7種類の取得可能なデータが入っています。

- 安定データ：一日に約100個のパケット分のデータを取得します。

ローカルプリンタとキューデータ

-すべてのデータの取得にWMIを使用します。WMIはRPCおよびWindows認証を利用します。ポーリング対象となるホストに対して5つの異なるクエリを発行します。パケットはTCPで、パケット数およびサイズはネットワークパケットサイズ、認証の種類、クエリの種類によって異なります。

SQLトラフィック

SQLトラフィックはデータが変更になり、データベースをアップデートする際に発生します。サーバに対するTCPトラフィックとなります。また、SiteAuditのビューアアプリケーションとデータベース間のクエリにおいても発生します。トラフィックの量はデバイス数、ネットワークパケットの最大サイズ、認証の種類によって異なります。尚、トラフィックはSiteAuditが動作しているとホストとSQLサーバー間で発生します。

その他のトラフィック

メールでの通知を発行する場合、トラフィックが発生する可能性があります。また、定期レポートがスケジュール設定されている場合、レポートのメール送信時にも発生します。その場合、SMTPサーバー上のトラフィックになります。

ネットワークトラフィックの測定方法

ネットワークトラフィックの測定、予測は、各環境によって異なるため容易ではありません。ネットワーク設定、デバイスの種類などによっても大きく異なります。たとえば、高性能の複合機の場合、ローエンドのデスクトップ用モノクロプリンタよりもはるかに多い数のメッセージを発行します。

SiteAudit では今までネットワークトラフィック過多の問題が報告されたことはありませんが、各環境でネットワークトラフィックを知ることは重要です。簡単な方法として、ネットワークアナライザを使ってトラフィックを測定する方法が挙げられます。

Netaphor では次のフリーアプリの使用をお勧めしています。 www.wireshark.com/

ネットワークトラフィックの例

4つの異なるフリートサイズによって発生するネットワークトラフィックの例を以下に示します。

- フリートサイズがプリンタ250台の場合

パケットの種類	数	備考
・ 検索パケット	40500	1 サイクル中のパケット数
・ モニタリングパケット	19016	1 時間のモニタリングパケット数
・ ネットワーク回線容量	9	1 時間の平均ネットワーク回線容量 (MB)
・ 回線容量/秒	0.003	1 秒の平均ネットワーク回線容量 (MB)
・ GB のネットワークの回線容量使用率	0.000293	1GB のネットワークにおける平均回線容量使用率 (%)
・ 100MB のネットワークの回線容量使用率	0.003	100MB のネットワークにおける平均回線容量使用率 (%)

- フリートサイズがプリンタ1000台の場合

パケットの種類	数	備考
・ 検索パケット	1159200	1 サイクル中のパケット数
・ モニタ用パケット	75920	1 時間のモニタリングパケット数
・ ネットワーク回線容量	37	1 時間の平均ネットワーク回線容量 (MB)
・ ネットワーク回線容量/秒	0.01	1 秒の平均ネットワーク回線容量 (MB)
・ GB のネットワークの回線容量使用率	0.000977	1GB のネットワークにおける平均回線容量使用率 (%)
・ 100MB のネットワークの回線容量使用率	0.001	100MB のネットワークにおける平均回線容量使用率 (%)

- フリートサイズがプリンタ10000台の場合

パケットの種類	数	備考
・ 検索パケット	5025000	1 サイクル中のパケット数
・ モニタ用パケット	762038	1 時間のモニタリングパケット数
・ ネットワーク回線容量	372	1 時間の平均ネットワーク回線容量 (MB)
・ ネットワーク回線容量/秒	0.103	1 秒の平均ネットワーク回線容量 (MB)
・ GB のネットワークの回線容量使用率	.010058594	1GB のネットワークにおける平均回線容量使用率 (%)
・ 100MB のネットワークの回線容量使用率	0.103	100MB のネットワークにおける平均回線容量使用率 (%)

- フリートサイズがプリンタ25000台の場合

パケットの種類	量	備考
・ 検索パケット	5025000	1 サイクル中のパケット数
・ モニタ用パケット	1901550	1 時間のモニタリングパケット数
・ ネットワーク回線容量	928	1 時間の平均ネットワーク回線容量 (MB)
・ ネットワーク回線容量/秒	0.258	1 秒の平均ネットワーク回線容量 (MB)
・ GB のネットワークの回線容量使用率	0.025195313	1GB のネットワークにおける平均回線容量使用率 (%)
・ 100MB のネットワークの回線容量使用率	0.258	100MB のネットワークにおける平均回線容量使用率 (%)

注：上記のトラフィック量は、典型的な環境で予測したものです。実際には、ローカルプリンタ、ネットワークプリンタの数、アドレスのスペーシング、IP アドレス数などによって異なる場合があります。