



FUJITSU Software ServerView Suite

# ServerView Suite 製品での SNMPv3 の 使用

(Windows と Linux)

## **DIN EN ISO 9001:2015 に準拠したドキュメントの作成**

高い品質とお客様の使いやすさが常に確保されるように、

このマニュアルは、DIN EN ISO 9001:2015

基準の要件に準拠した品質管理システムの規定を

満たすように作成されました。

cognitas. Gesellschaft für Technik-Dokumentation mbH

[www.cognitas.de](http://www.cognitas.de)

## **著作権および商標**

Copyright 1998 - 2019 FUJITSU LIMITED

All rights reserved.

お届けまでの日数は在庫状況によって異なります。技術的修正の権利を有します。

使用されているハードウェア名とソフトウェア名は、各メーカーの商標名および商標です。

---

# 目次

<b>1 ServerView Suite 製品での SNMPv3 の使用</b>	<b>7</b>
1.1 新機能	8
1.2 本マニュアルの対象者および目的	8
1.3 ServerView Suite のマニュアル	9
1.4 本書の表記	9
<b>2 SNMPv3: 新機能</b>	<b>11</b>
2.1 起源	11
2.2 SNMPv3: 新機能	11
2.3 SNMP のアーキテクチャ	11
2.3.1 SNMP マネージャと SNMP エージェント	12
2.4 セキュリティの問題	13
2.4.1 SNMPv3: 脅威	13
2.4.2 SNMPv3: セキュリティモデルとアクセス制御	15
2.4.3 ユーザベースセキュリティモデル( USM)	15
2.4.4 ビューベースアクセス制御モデル( VACM)	15
2.5 ユーザ管理	16
<b>3 ServerView Agents での SNMPv3 の使用</b>	<b>17</b>
3.1 アーキテクチャと要件	17
3.1.1 エージェントのアーキテクチャ	17
3.1.2 ServerView Agents の技術的要件	19
3.2 Windows ベースのサーバ: 処理の概要	20
3.2.1 SNMPv3 への切り替え	20
3.2.2 管理対象サーバの初期インストール	21
3.2.3 アップデート	22
3.3 Linux ベースのサーバ: 処理の概要	22
3.3.1 SNMPv3 への切り替え	22
3.3.2 管理対象サーバの初期インストール	23
3.3.3 アップデート	24
3.4 手順	24

3.4.1 Microsoft Windows SNMP サービスのインストールまたは有効化 (Windows)	24
3.4.2 ServerView Agents のインストール (Windows/Linux)	25
3.4.3 Windows SNMP サービスの無効化とNet-SNMP (Windows) のインストール	25
3.4.3.1 Net-SNMP Installer for Windows	26
3.4.3.2 段階的	27
3.4.4 Net-SNMP の設定 (Windows/Linux)	29
3.4.4.1 snmpd.conf の設定	30
3.4.5 Net-SNMP マスターエージェントによる ServerView Agents のアップデート (Windows/Linux)	32
3.4.5.1 Linux	32
3.4.5.2 Windows	32
<b>4 Operations Manager での SNMPv3 の使用</b>	<b>34</b>
4.1 アーキテクチャと要件	34
4.1.1 Operations Manager と ServerView Agents との間の SNMPv3 通信	34
4.1.1.1 SNMPv3 通信の共通ユーザ	34
4.1.1.2 Windows: 2 つの SNMP サービスの共存: UDP ポートの再構成	34
4.1.2 Operations Manager の技術的要件	35
4.1.2.1 管理対象サーバ: ServerView Agents	35
4.1.2.2 中央管理用サーバ: Operations Manager	35
4.2 中央管理用サーバ (CMS) での設定	36
4.2.1 Windows ベースのシステム: 処理の概要	36
4.2.1.1 SNMPv3 への切り替え	36
4.2.1.2 初期インストール	37
4.2.2 Linux ベースのシステム: 処理の概要	38
4.2.2.1 SNMPv3 への切り替え	38
4.2.2.2 初期インストール	39
4.2.3 Operations Manager のインストール (Windows/Linux)	40
4.2.4 Microsoft Windows SNMP サービスのインストールまたは有効化 (Windows)	40
4.2.5 Windows SNMP サービスの無効化 (Windows)	40
4.2.6 Net-SNMP のインストール (Windows)	40
4.2.6.1 Net-SNMP のソース	41
4.2.6.2 インストール	41
4.2.7 CMS 上の Windows: UDP ポートの再構成、snmptrapd.conf の登録と設定	42

4.2.7.1 UDP ポートの再構成 .....	42
4.2.7.2 Net-SNMP Service を Windows サービスとして登録する .....	43
4.2.7.3 snmptrapd.conf の設定 .....	43
4.2.7.4 snmptrapd.conf ファイルの例 .....	44
4.2.8 CMS 上の Linux: snmptrapd.conf の設定 .....	45
4.2.8.1 snmptrapd.conf の設定 .....	45
4.2.8.2 snmptrapd.conf ファイルの例 .....	46
4.2.9 Operations Manager での SNMPv3 の有効化 .....	47
4.2.9.1 「V3 Setting」設定ウィンドウで Operations Manager の SNMPv3 を有効にする .....	47
4.2.9.2 snmp.conf による Operations Manager の SNMPv3 の有効化 .....	50
4.3 管理対象サーバでの設定 .....	51
4.3.1 Windows ベースのサーバ: 処理の概要 .....	51
4.3.1.1 SNMPv3 への切り替え .....	51
4.3.1.2 管理対象サーバの初期インストール .....	52
4.3.1.3 アップデート .....	53
4.3.2 Linux ベースのサーバ: 処理の概要 .....	53
4.3.2.1 SNMPv3 への切り替え .....	53
4.3.2.2 管理対象サーバの初期インストール .....	53
4.3.2.3 アップデート .....	54
4.3.3 管理対象サーバ上の Windows: UDP ポートの再構成、snmpd.conf の登録と設定 .....	54
4.3.3.1 UDP ポートの再構成 .....	54
4.3.3.2 Net-SNMP Service を Windows サービスとして登録する .....	55
4.3.3.3 snmpd.conf の設定 .....	55
4.3.3.4 snmpd.conf 設定ファイルの例: .....	57
4.3.4 管理対象サーバの Linux: snmpd.conf の設定 .....	58
4.3.4.1 snmpd.conf 設定ファイルの例: .....	60
4.4 Net-SNMP 実装とテスト手順 .....	61
4.4.1 Windows SNMP サービスの設定 .....	61
4.4.2 Net-SNMP サービスの基本設定 .....	64
4.4.2.1 エージェント (snmpd) .....	64
4.4.2.2 トラップリスナー (snmptrapd) .....	66
4.4.3 SNMP 環境のテスト .....	67

---

4.4.3.1 SNMP クライアントのシミュレーション .....	67
4.4.3.2 テストトラップの送信と到着の確認 .....	68
4.5 アイテムの操作 .....	68
4.5.1 SNMPv3 を有効にしたサーバでブラウザ操作が失敗する .....	68
4.5.2 Operations Manager での CMS の可視性 .....	69
<b>5 iRMC での SNMPv3 の使用 .....</b>	<b>70</b>
5.1 アーキテクチャと要件 .....	70
5.1.1 iRMC のアーキテクチャ .....	70
5.1.1.1 リモートマネジメントコントローラ - iRMC S4 .....	70
5.1.1.2 ServerView Integration .....	71
5.1.1.3 ServerView Agentless Service を使用したエージェントレスモード .....	71
5.1.1.4 iRMC S4 上の SNMP サービス .....	72
5.1.1.5 iRMC S4 上のユーザ権限 .....	73
5.1.2 技術的要件 .....	73
5.2 「iRMC S4 ユーザ情報」ページの SNMPv3 .....	74
5.3 処理の概要 .....	74
5.3.1 SNMP バージョンの設定 .....	75
5.3.2 SNMPv3 のユーザ固有の設定の指定 .....	77
5.3.2.1 サポートされる認証/プライバシー設定 .....	79

---

# 1 ServerView Suite 製品での SNMPv3 の使用

FUJITSU Software ServerView® Suite には、サーバシステムのライフサイクル全体にわたって専門家が管理するために必要なすべての要素が備えられています。

ServerView Suite の基本プロトコルは SNMP です。SNMPv1 セキュリティはコミュニティ文字列を基盤としており、エージェント側と管理用サーバ側の両方に設定する必要があります。SNMP バージョン 3 は、新しいコンセプトを定義するセキュリティモデルを実装し、古いコミュニティベースの疑似認証を置き換え、暗号化を使用して通信のプライバシーを確保します。詳細は、[11 ページの SNMPv3: 新機能](#)を参照してください。

以下の ServerView Suite 製品は SNMPv3 をサポートします。

## ServerView Agents

ServerView でシステムを管理するためには、SNMP サービスと ServerView Agents をこのシステムにインストールする必要があります。ServerView Agents はシステムから管理データを取得し、SNMP 経由でこの情報の要求側 (ServerView Operations Manager など) に転送します。

SNMPv3 を ServerView 通信に使用するためには、Net-SNMP マスターエージェントを推奨します。

詳細は、[17 ページの ServerView Agents での SNMPv3 の使用](#)を参照してください。

## ServerView Operations Manager

ServerView Suite の中央管理用コンポーネントである ServerView Operations Manager (略して「Operations Manager」) は、物理サーバ、仮想サーバ、関連するインフラストラクチャコンポーネントをネットワーク内のストレージ拡張装置として監視し、分析します。

ネットワーク内のサーバの検出は SNMP および IPMI ベースで、サーバリストへの登録はシンプルです。バージョン 7.10 以降では、ServerView も SNMPv3 をサポートします。

SNMPv3 を ServerView 通信に使用するためには、Net-SNMP マスターエージェントを推奨します。

詳細は、[34 ページの Operations Manager での SNMPv3 の使用](#)を参照してください。

## iRMC

ServerView integrated Remote Management Controller iRMC S4 は、システムのステータスにかかわらず、Out-Of-Band 操作であっても、Fujitsu サーバを広範囲にわたって監視および管理できます。マザーボードのチップに実装され、さまざまなリモート管理機能を基本システム管理機能に統合します。

iRMC S4 は SNMP サービスを提供し、一連の SNMP MIB の GET 要求をサポートします。

詳細は、[70 ページの iRMC での SNMPv3 の使用](#)を参照してください。

## ServerView RAID Manager

ServerView RAID Manager では、各種 Fujitsu PRIMERGY プラットフォームに異なるベンダが提供した、ホストベースのハードウェアおよびソフトウェア RAID ソリューションを均一に管理および監視できます。

ServerView RAID は Net-SNMP スタックをサポートします。これは ServerView 通信で SNMPv3 を使用する場合に推奨されます。

詳細は、[9 ページの ServerView Suite のマニュアル](#)から『ServerView RAID Manager』マニュアルを参照してください。

# 1.1 新機能

本マニュアルのこのエディションは、オンラインマニュアル『FUJITSU Software ServerView Suite, Using SNMPv3 with ServerView Suite products (Windows and Linux)』(2016 年 5 月版)の更新版です。

このマニュアルでは、以下の変更と追加について主に説明します。

- Net-SNMP Installer for Windows([26 ページの Net-SNMP Installer for Windows](#)を参照)

Net-SNMP Installer for Windows ノパッケージには、Windows オペレーティングシステム(64 ビットシステムのみ)向けの SNMPv1、SNMPv2、SNMPv3 のサポート機能が搭載されています。

# 1.2 本マニュアルの対象者および目的

本書はシステム管理者、ネットワーク管理者、およびハードウェアやソフトウェアの十分な知識をもったサービス技術者を対象としています。

ServerView Agents、Operations Manager、および ServerView integrated Remote Management Controller iRMC S4 で SNMPv3 を使用する方法について説明します。





## 1.3 ServerView Suite のマニュアル

マニュアルはインターネットから無料でダウンロードできます。インターネットのオンラインドキュメントは、<http://manuals.ts.fujitsu.com>の「x86 Servers」リンクをクリックすると入手できます。

ServerView Suiteにあるマニュアルの概要およびファイル構造については、ServerView Suite サイトマップを参照してください( ServerView Suite - ServerView Suite マニュアルアップデートリスト)。

## 1.4 本書の表記

以下の表記規定を使用します。

表記	説明
	データの損失やデバイスの損傷の可能性があるリスクを表示します。
	追加関連情報とヒントを表示します。
<b>太字</b>	インターフェース要素の名前を示します。
<code>monospace</code>	パスおよびファイル名など、出力やシステム要素を示します。
<b><code>monospace semibold (やや太字)</code></b>	キーボードを使用して入力するテキストを示します。
<a href="#">青字の文字列</a>	関連するトピックへのリンクを示します。
<a href="#">ピンク字の文字列</a>	すでに表示したリンクを示します。
<abc>	実際の値に置き換える必要のある変数を示します。
[abc]	オプション(構文)を示します
[key]	キーボード上のキーを示します。大文字のテキストを入力する場合、[Shift] キーを指定します。たとえば、Aを入力する場合 [Shift] + [A] を押します。2つのキーを同時に押す場合は、2つのキーをプラス記号で連結して示します。

テーブル 1: 本書の表記

### 画面

いくつかの画面はシステムに依存しているため、表示される詳細はシステムによって異なります。メニューオプションとコマンドには、システム固有の違いがある場合もあります。

---

## 2 SNMPv3: 新機能



この項で扱っていない詳細については、IETF の SNMPv3 に関する RFC ([www.ietf.org](http://www.ietf.org) - 特に RFC 3411、RFC 3414、RFC 3415) を参照してください。

### 2.1 起源

SNMP( Simple Network Management Protocol) は 1990 年代の初めに登場し、簡単で安定性に優れていることから、すぐに普及しました。

ただし、後に SNMPv1 と呼ばれる SNMP は、データを保護することなく転送し、実際にはフレームワークを提供しません。このような理由で、後のバージョンが拡張されました。

### 2.2 SNMPv3: 新機能

SNMPv3( 1998 ~ 2002 年) には、新しい形式の SNMP メッセージ、セキュリティの問題、アクセス制御、SNMP パラメータのリモート設定を備えた新しいフレームワークが導入されています。

この新しいフレームワークは以下のセキュリティ要件を満たします。

- 認証 - 送信者と受信者は本当に要求されたエンティティなのか
- プライバシー - 不正なサードパーティはメッセージを読み取れるか
- 整合性 - メッセージは変更されずに通信経路を通過したか



SNMPv3 は SNMPv1 または SNMPv2c をスタンドアロンで置き換えるものではありません。SNMPv2c( または一定の制限付きで SNMPv1) と併用してセキュリティ機能を定義します。

### 2.3 SNMP のアーキテクチャ

SNMP のアーキテクチャは、SNMP プロトコルデータユニット( PDU) の生成と受信のために、以下のインスタンスを定義します。

- Command generator
- Command responder
- Notification originator

- Notification receiver
- Proxy forwarder

このアーキテクチャでは、次のサービスを提供する SNMP エンジンも定義されます。

- メッセージを送受信するサービス
- メッセージの承認と暗号化を行うサービス
- 管理対象オブジェクトへのアクセスを制御するサービス

SNMP エンジンには以下のコンポーネントを含められます。

- ディスパッチャ
- メッセージ処理サブシステム
- セキュリティサブシステム
- アクセス制御サブシステム

SNMP アーキテクチャの実装は、SNMP エンティティと呼ばれます。SNMP エンティティは、SNMP エンジンと、関連する 1 つ以上のアプリケーションで構成されます。

### 2.3.1 SNMP マネージャと SNMP エージェント

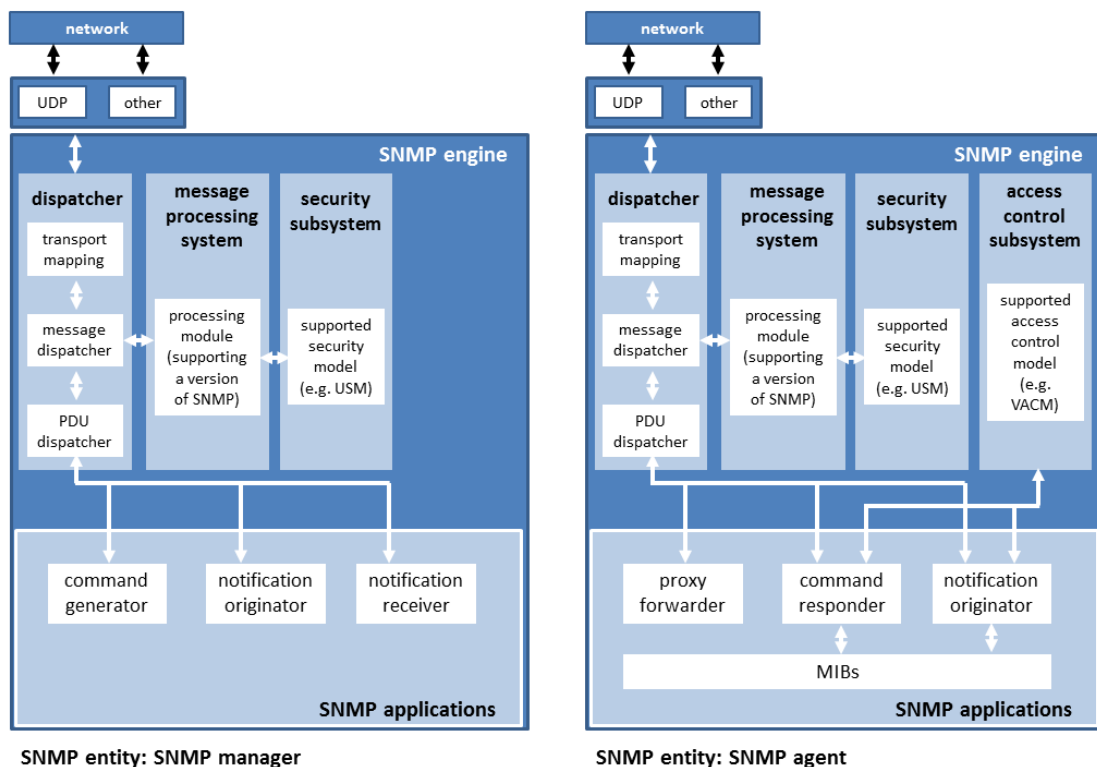


図 1: SNMP マネージャと SNMP エージェントのアーキテクチャ

### SNMP マネージャ

1 つ以上の command generator または notification receiver アプリケーションを含む SNMP エンティティは、SNMP マネージャと呼ばれます。

従来の SNMP マネージャでは、SNMP エンジンには以下のものが含まれます。

- ディスパッチャ  
ディスパッチャは、トラフィックマネージャです。
- メッセージ処理サブシステム  
メッセージ処理サブシステムは、ディスパッチャからの発信 PDU を受信します。メッセージヘッダでラッピングして、ディスパッチャに戻します。
- セキュリティサブシステム  
セキュリティサブシステムは認証および暗号化機能を実行します。

### SNMP エージェント

1 つ以上の command responder または notification originator アプリケーションを含む SNMP エンティティは、SNMP エージェントと呼ばれます。

従来のエージェントの SNMP エンジンには、従来のマネージャの SNMP エンジンが持つすべてのコンポーネントに加えて、アクセス制御サブシステムが含まれます。

- アクセス制御サブシステム  
アクセス制御サブシステムは認証サービスを実行して、管理オブジェクトの読み取りと設定のために MIB へのアクセスを制御します。

## 2.4 セキュリティの問題

### 2.4.1 SNMPv3: 脅威

SNMPv3 は、以下のような主な脅威に対する保護を実現するように設計されています。

- 情報の改変  
エンティティは、認証されたエンティティから生成された転送中の SNMP メッセージを改変して、不正な管理操作を行うことがあります。
- なりすまし  
特定のエンティティに対して承認されていない管理操作が、認証されたエンティティの ID を装ってエンティティに対して試行されます。

- **メッセージストリーミングの改変**

SNMP は接続のない転送プロトコルで運用するように設計されています。このため、SNMP メッセージの順序変更、遅延や再生(重複)が発生し、不正な管理操作が行われます。

- **開示**

エンティティはマネージャとエージェントの間のやりとりを観察できます。このとき、管理対象オブジェクトの値が認識され、通知されるイベントの情報が知られてしまいます。

## 2.4.2 SNMPv3: セキュリティモデルとアクセス制御

SNMPv3 は、セキュリティに関連する 2 つの機能を定義します。1 つ以上のサポートされる異なるセキュリティモデル(認証用)を持つセキュリティサブシステムと、1 つ以上のサポートされる異なるアクセス制御モデル(承認用)を持つアクセス制御サブシステムです。現時点では、定義されるモデルはユーザベースのセキュリティモデル(USM)とビューベースのアクセス制御モデル(VACM)のみです。

- ユーザベースセキュリティモデル(USM)
  - 認証とプライバシー(暗号化)機能を提供します。
  - メッセージレベルで動作します。
- ビューベースアクセス制御モデル(VACM)
  - 指定されたプリンシパルが特定の機能を実行するために特定の MIB オブジェクトへのアクセスが許可されているか、判定します(承認)。
  - PDU レベルで動作します。

## 2.4.3 ユーザベースセキュリティモデル(USM)

セキュリティサブシステムでのセキュリティモデルは、これらの脅威から保護しなければなりません。

現時点では、ユーザベースセキュリティモデル(USM)のみが、SNMPv3 に定義されたセキュリティモデルです。USM は認証とプライバシー(暗号化)機能を提供します。

このモデルは以下のような通信メカニズムを提供します。

- 認証とプライバシーのない通信(NoAuthNoPriv)
- 認証はあるがプライバシーのない通信(AuthNoPriv)
- 認証とプライバシーがある通信(AuthPriv)

USM は以下の目的で設計されています。

- 受信 SNMP メッセージがネットワーク処理中に改変されていないことを確認する
- 送信者の ID を確認する
- 管理情報を要求する、または含む古い受信メッセージをフィルタリングする
- 受信メッセージが開示から保護されるようにする

## 2.4.4 ビューベースアクセス制御モデル(VACM)

ビューベースアクセス制御モデル(VACM)は、アプリケーション(command responder や notification originator アプリケーションなど)がアクセス権の確認に使用できる一連のサービスを定義します。

VACM は以下の目的で設計されています。

- MIB を使用して、エージェントのアクセス制御の調整を定義する
- リモートエントリにローカル MIB の管理対象オブジェクトにアクセスを許可するかどうかをチェックする

## 2.5 ユーザ管理

SNMPv3 の認証および承認メカニズムを使用するためには、以下のフィールドを各ユーザに対して設定する必要があります。

- **securityName**  
ユーザ名
- **authProtocol**  
認証プロトコル。MD5 または SHA の 2 つのプロトコルを使用できます。
- **privProtocol**  
プライバシープロトコル。AES または DES の 2 つのプロトコルを使用できます。
- **authKey**  
パスフレーズから生成された認証キーで、8 文字以上が必要です。
- **privKey**  
パスフレーズから生成されたプライバシーキーで、8 文字以上が必要です。
- **securityLevel**  
以下の値を指定できます。
  - NoAuthNoPriv  
メッセージは、認証も暗号化もされずに送信されます。
  - AuthNoPriv  
メッセージは、認証され、暗号化されずに送信されます。
  - AuthPriv  
メッセージは、認証および暗号化されて送信されます。



この項で扱っていない詳細については、IETF の SNMPv3 に関する RFC ([www.ietf.org](http://www.ietf.org) - 特に RFC 3411、RFC 3414、RFC 3415) を参照してください。



---

## 3 ServerView Agents での SNMPv3 の使用



SNMPv3 は、ユーザ固有の総合的なセキュリティコンセプトおよびセキュリティ管理計画の一部として実装する必要があります。

本書で説明する手順とメカニズムは、単独では総合的な保護には不十分です。全体的なセキュリティコンセプトに合わせて統合する必要があります。

### 3.1 アーキテクチャと要件

#### 3.1.1 エージェントのアーキテクチャ

ServerView SNMP エージェントはサブエージェントとして実装されます。各エージェントは特定のタスク専用です。リーンプログラミングのコンセプトに従って、すべてのサブエージェントへの中央コンポーネントは適切に設定され、メッセージングやアクセス制御などの中央サービスを実行します。

SNMPv3 を ServerView Agent 通信に使用するためには、Net-SNMP マスターエージェントを推奨します。

## Net-SNMP マスターエージェントのアーキテクチャ / ServerView SNMP サブエージェントシナリオ

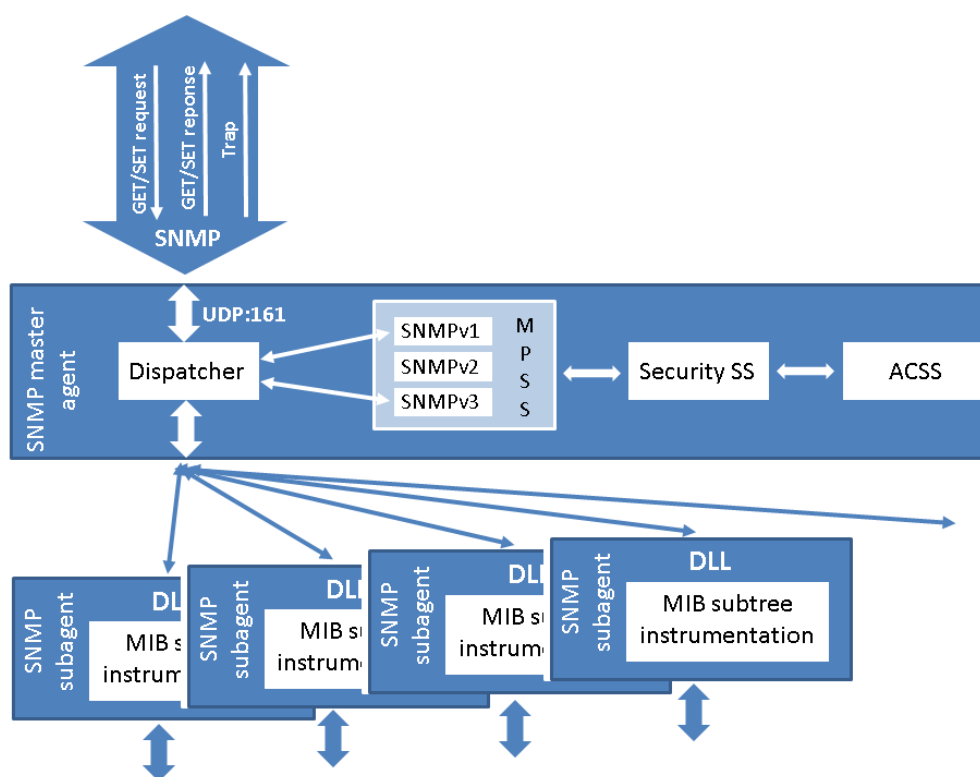


図 2: エージェントのアーキテクチャ

このアーキテクチャでは、サブエージェントには SNMP の情報がありません。メッセージ処理(どのバージョンのどのプロトコルか)とセキュリティおよびアクセス制御は、マスターエージェントで処理されます。

### Windows

SNMP バージョン 1 および 2c では、Microsoft は Microsoft Windows SNMP サービスを Microsoft Windows に統合しています。ServerView SNMP エージェントがサブエージェントとして実装され、DLL 情報がこのサービスによってアップロードされます。

しかし、Microsoft Windows SNMP サービスでは SNMP バージョン 3 をサポートしていません。SNMPv3 を使用して Windows ベースのサーバを管理するためには、Net-SNMP マスターエージェントを追加する必要があります。

**i** Microsoft Windows SNMP サービスでは SNMPv3 をサポートしていませんが、必要な Windows SNMP サービス拡張 DLL および Windows SNMP API を **snmpapi.dll** から提供するためには、インストールする必要があります。



Microsoft Windows SNMP サービスに必要なアドオンとして、Net-SNMP マスターエージェントを推奨します( [27 ページの Windows SNMP サービスの無効化 \(Windows\)](#) を参照)。

## Linux

Net-SNMP マスターエージェントは、大部分の Linux ディストリビューションに付属しています。

### 3.1.2 ServerView Agents の技術的要件

ServerView Agents は以下の製品で使用できます。

#### Windows

- Windows Server 2008 / 2008 x64 / 2008 R2
- Windows Server 2012 Datacenter / Standard / Foundation
- Windows Server 2012 R2 Datacenter / R2 Standard / R2 Foundation
- Windows Storage Server 2012 Standard

#### Linux

- SUSE( SLES 11) : SP3 および SP4
- SUSE( SLES 12) : GA および SP1
- Red Hat Enterprise Linux 5.10 / 5.11
- Red Hat Enterprise Linux 6.6 / 6.7
- Red Hat Enterprise Linux 7.1 / 7.2

#### Windows ベースのサーバ: シナリオ

指定された状況と目的によって、手順は異なります。

個々の手順の詳細については、[51 ページの Windows ベースのサーバ: 処理の概要](#)を参照してください。

- **SNMPv3 への切り替え**

状況: Windows ベースのサーバを ServerView Agents で監視している。

目的: SNMPv3 を使用する。

- **管理対象サーバの初期インストール**

状況: Windows ベースのサーバは ServerView Agents で監視されていない。

目的: サーバを SNMPv3 を使用して ServerView Agents で監視する。

- **アップデート**

状況: Windows ベースのサーバを SNMPv3 を使用して ServerView Agents で監視している。

目的: ServerView Agents をアップデートする。

**Linux ベースのサーバ: シナリオ**

指定された状況と目的によって、手順は異なります。

個々の手順の詳細については、[53 ページの Linux ベースのサーバ: 処理の概要](#)を参照してください。

- **SNMPv3 への切り替え**

状況: Linux ベースのサーバを ServerView Agents で監視している。

目的: SNMPv3 を使用する。

- **管理対象サーバの初期インストール**

状況: Linux ベースのサーバは ServerView Agents で監視されていない。

目的: サーバを SNMPv3 を使用して ServerView Agents で監視する。

- **アップデート**

状況: Linux ベースのサーバを SNMPv3 を使用して ServerView Agents で監視している。

目的: ServerView Agents をアップデートする。

## 3.2 Windows ベースのサーバ: 処理の概要

指定された状況と目的によって、手順は異なります。

### 3.2.1 SNMPv3 への切り替え

状況: Windows ベースのサーバを ServerView Agents で監視している。

目的: SNMPv3 を使用する。

手順:

1. **ServerView Agents の V7.01 へのアップデート**

Net-SNMP のインストール前のアップデートは、通常通り実行できます(アップデート管理の ServerView のマニュアルを参照)。

## 2. Microsoft Windows SNMP サービスの無効化

Microsoft Windows SNMP サービスでは SNMP バージョン 3 をサポートしていません。SNMPv3 を使用して Windows ベースのサーバを管理するためには、Microsoft Windows SNMP サービスを無効にしてから SNMP マスターエージェントを別の SNMPv3 対応スタックに置換する必要があります。

詳細については、[17 ページのエージェントのアーキテクチャ](#)を参照してください。

手順については、[25 ページの Windows SNMP サービスの無効化と Net-SNMP \(Windows\) のインストール](#)を参照してください。

## 3. Net-SNMP のインストール

手順については、[25 ページの Windows SNMP サービスの無効化と Net-SNMP \(Windows\) のインストール](#)を参照してください。

## 4. 新規 SNMP マスターエージェントの設定 - Net-SNMP の例を使用

少なくとも USM ユーザを作成し、アクセス制御を定義してトラップを構成する必要があります。

詳細は、[11 ページの SNMPv3: 新機能](#)を参照してください。

手順については、[29 ページの Net-SNMP の設定 \(Windows/Linux\)](#)を参照してください。

## 3.2.2 管理対象サーバの初期インストール

状況 : Windows ベースのサーバは ServerView Agents で監視されていない。

目的 : サーバを SNMPv3 を使用して ServerView Agents で監視する。

手順 :

### 1. Microsoft Windows SNMP サービスのインストールまたは有効化

手順については、[24 ページの Microsoft Windows SNMP サービスのインストールまたは有効化 \(Windows\)](#)を参照してください。

### 2. ServerView Agents V7.01 以上のインストール

手順については、[25 ページの ServerView Agents のインストール \(Windows/Linux\)](#)を参照してください。

### 3. Microsoft Windows SNMP サービスの無効化

Microsoft Windows SNMP サービスでは SNMP バージョン 3 をサポートしていません。SNMPv3 を使用して Windows ベースのサーバを管理するためには、Microsoft Windows SNMP サービスを無効にしてから SNMP マスターエージェントを別の SNMPv3 対応スタックに置換する必要があります。

詳細については、[17 ページのエージェントのアーキテクチャ](#)を参照してください。

手順については、[25 ページの Windows SNMP サービスの無効化と Net-SNMP \(Windows\) のインストール](#)を参照してください。

#### 4. Net-SNMP のインストール

手順については、[25 ページの Windows SNMP サービスの無効化と Net-SNMP \(Windows\) のインストール](#)を参照してください。

#### 5. 新規 SNMP マスターエージェントの設定 - Net-SNMP の例を使用

少なくとも USM ユーザを作成し、アクセス制御を定義してトラップを構成する必要があります。

詳細は、[11 ページの SNMPv3: 新機能](#)を参照してください。

手順については、[29 ページの Net-SNMP の設定 \(Windows/Linux\)](#)を参照してください。

### 3.2.3 アップデート

**状況** : Windows ベースのサーバを SNMPv3 を使用して ServerView Agents で監視している。

**目的** : ServerView Agents をアップデートする。

**手順** : 手順については、[32 ページの Net-SNMP マスターエージェントによる ServerView Agents のアップデート \(Windows/Linux\)](#)を参照してください。

## 3.3 Linux ベースのサーバ: 処理の概要

指定された状況と目的によって、手順は異なります。

### 3.3.1 SNMPv3 への切り替え

**状況** : Linux ベースのサーバを ServerView Agents で監視している。

**目的** : SNMPv3 を使用する。

**手順** :

#### 1. ServerView Agents の V7.01 へのアップデート

このアップデートは、Net-SNMP のインストール前に実行できます(アップデート管理の ServerView のマニュアルを参照)。

#### 2. SNMP マスターエージェントの設定

少なくとも USM ユーザを作成し、アクセス制御を定義してトラップを構成する必要があります。

詳細は、[11 ページの SNMPv3: 新機能](#)を参照してください。

手順については、[29 ページの Net-SNMP の設定 \( Windows/Linux\)](#)を参照してください。

### 3.3.2 管理対象サーバの初期インストール

状況 : Linux ベースのサーバは ServerView Agents で監視されていない。

目的 : サーバを SNMPv3 を使用して ServerView Agents で監視する。

手順 :

1. ServerView Agents V7.01 以上のインストール

手順については、[25 ページの ServerView Agents のインストール\( Windows/Linux\)](#)を参照してください。

## 2. SNMP マスターエージェントの設定

少なくとも USM ユーザを作成し、アクセス制御を定義してトラップを構成する必要があります。

詳細は、[11 ページの SNMPv3: 新機能](#)を参照してください。

手順については、[29 ページの Net-SNMP の設定 \(Windows/Linux\)](#)を参照してください。

### 3.3.3 アップデート

**状況** : Linux ベースのサーバを SNMPv3 を使用して ServerView Agents で監視している。

**目的** : ServerView Agents をアップデートする。

**手順**: 手順については、[32 ページの Net-SNMP マスターエージェントによる ServerView Agents のアップデート \(Windows/Linux\)](#)を参照してください。

## 3.4 手順



SNMPv3 は、ユーザ固有の総合的なセキュリティコンセプトおよびセキュリティ管理計画の一部として実装する必要があります。

本書で説明する手順とメカニズムは、単独では総合的な保護には不十分です。全体的なセキュリティコンセプトに合わせて統合する必要があります。

オペレーティングシステム、指定された状況および目的によって、手順は異なります。

個々のシナリオの詳細については、[51 ページの Windows ベースのサーバ: 処理の概要](#)または [53 ページの Linux ベースのサーバ: 処理の概要](#)を参照してください。

### 3.4.1 Microsoft Windows SNMP サービスのインストールまたは有効化 (Windows)



Microsoft Windows SNMP サービスでは SNMPv3 をサポートしていませんが、必要な Windows SNMP サービス拡張 DLL および Windows SNMP API を `snmpapi.dll` から提供するためには、インストールする必要があります。



ServerView Agents をインストールするためには、Microsoft Windows SNMP サービスを有効にして、正しいインストールプロセスを実施する必要があります。



Windows ベースのサーバを Net-SNMP マスターエージェントで監視している場合、Microsoft Windows SNMP サービスを無効にして、SNMPv3 通信を確保する必要があります ([27 ページの Windows SNMP サービスの無効化 \(Windows\)](#)を参照)。



1. Microsoft Windows SNMP サービスをインストールおよび有効にします。

このサービスのインストールおよび有効化の詳細については、『**ServerView Agents for Windows**』マニュアルか、Microsoft の該当するマニュアルを参照してください。

### 3.4.2 ServerView Agents のインストール(Windows/Linux)

1. ServerView Agents をインストールします。

ServerView Agents のインストールの詳細については、『**ServerView Agents for Windows**』または『**ServerView Agents for Linux**』のマニュアルを参照してください。

### 3.4.3 Windows SNMP サービスの無効化と Net-SNMP(Windows) のインストール

Microsoft Windows SNMP サービスでは SNMP バージョン 3 をサポートしていません。SNMPv3 を使用して Windows ベースのサーバを管理するためには、Microsoft Windows SNMP サービスを無効にしてから SNMP マスターエージェントを別の SNMPv3 対応スタックに置換する必要があります。SNMPv3 を使用して Windows ベースのサーバを管理するためには、Net-SNMP マスターエージェントを追加する必要があります。

Windows SNMP サービスを無効化して Net-SNMP をインストールするには、2 つのオプションがあります。

- **FUJITSU Net-SNMP Installer for Windows** を使用できます。
- Microsoft Windows SNMP サービスを手動で無効化して、Net-SNMP を段階的にインストールできます。

#### FUJITSU Net-SNMP Installer for Windows

**FUJITSU Net-SNMP Installer for Windows** を使用できます。

Windows SNMP サービスを無効化して Net-SNMP をインストールする最も効率的な方法  
詳細な情報と手順については、[26 ページの Net-SNMP Installer for Windows](#)を参照してください。

#### 段階的な手動操作

Microsoft Windows SNMP サービスを手動で無効化して、Net-SNMP を段階的にインストールできます。

- **Microsoft Windows SNMP サービスの無効化**

手順については、[27 ページの Windows SNMP サービスの無効化 \(Windows\)](#) を参照してください。

- **Net-SNMP のインストール**

手順については、[28 ページの Net-SNMP のインストール \(Windows\)](#) を参照してください。

### 3.4.3.1 Net-SNMP Installer for Windows

Net-SNMP Installer for Windows パッケージには、Windows オペレーティングシステム( 64 ビットシステムのみ) 向けの SNMPv1、SNMPv2、SNMPv3 のサポート機能が搭載されています。

パッケージは Net-SNMP Windows バイナリをベースとし、Net-SNMP エージェントおよび Net-SNMP トラップハンドラに必要なすべてのアイテムと SNMP プロトコル向けの一部のクライアントツールを提供するよう変更されています。

Net-SNMP サービスは Windows SNMP サービスを置き換えることも、並行して実行(別のネットワークポート上)することもできます。

このパッケージには OpenSSL の一部も含まれているので、暗号化を使用するために OpenSSL を別にインストールする必要はありません。

#### 提供

Net-SNMP Installer for Windows は、以下の手順で取得できます。

- FUJITSU サポート Web サイト( <http://support.ts.fujitsu.com/>) からダウンロードします。
  1. 「**Search**」フィールドに「**Net-SNMP**」と入力します。
  2. 「**Search result**」リストで「**Tools and Utilities**」を選択します。

「**Tools and Utilities**」リストで、項目「**Net-SNMP Installer for Windows**」を見つけます。
- ServerView Suite DVD からダウンロードします。

#### 要件

サポートされる OS : x64 Windows システム

#### インストール

インストーラによって、ネイティブ SNMP サービスが停止し、無効になります。Net-SNMP エージェントと Net-SNMP トラップハンドラが Windows システム上のサービスとして登録され、起動されます。



インストーラは Net-SNMP サービスを設定しません。サービスは手動で設定する必要があります( [29 ページの Net-SNMP の設定 \(Windows/Linux\)](#) を参照)。

パッケージのファイル:

- 0x0409.ini
- Data1.cab

- Net-SNMP\_x64.msi
- Setup.exe
- Setup.ini
- THIRDPARTYLICENSEREADME.txt

Net-SNMP Installer for Windows をインストールする際に入力は不要です。ただし、Net-SNMP Installer for Windows は著作権および国際条約で保護されているため、利用規約に同意する必要があります。

1. ファイル **Setup.exe** をダブルクリックします。  
Net-SNMP Installer for Windows が起動します。「ようこそ」ページが表示されます。
2. 「次へ」をクリックします。  
ライセンス契約書が表示されます。
3. 「**ライセンス契約に同意します。**」を選択して「次へ」をクリックします。  
サードパーティーライセンス契約書が表示されます。
4. 「**ライセンス契約に同意します。**」を選択して「次へ」をクリックします。  
「プログラムのインストール準備をする」ページが表示されます。
5. 「**インストール**」をクリックします。  
プログレスバーが表示されます。  
インストールが終了すると、「**Setup Wizard Completed**」ページが表示されます。
6. 「**終了**」をクリックします。  
Net-SNMP パッケージはディレクトリ `C:\usr` にインストールされます。



インストーラは Net-SNMP サービスを設定しません。サービスは手動で設定する必要があります( [29 ページの Net-SNMP の設定 \(Windows/Linux\)](#) を参照)。

### 3.4.3.2 段階的

#### Windows SNMP サービスの無効化 (Windows)

1. Microsoft Windows SNMP サービスが実行されている場合は、停止します。
2. Windows SNMP サービスを無効にするか、起動タイプを「**手動**」にします。





そうしないと、システムの次回起動時に Windows SNMP サービスが再起動してしまいます。

2 つのマスターエージェントの共存については、Net-SNMP のマニュアルを参照してください。

Microsoft Windows SNMP サービスの処理の詳細については、『**ServerView Agents for Windows**』マニュアルか、Microsoft の該当するマニュアルを参照してください。



### Net-SNMP のインストール(Windows)

-  SNMPv3 を ServerView Agent 通信に使用するためには、Net-SNMP マスターエージェントを推奨します。
-  **Linux:** Net-SNMP マスターエージェントは、大部分の Linux ディストリビューションに属しています。

### Net-SNMP のソース


Net-SNMP は Simple Network Management Protocol に関連するツールとライブラリを提供します。拡張可能なエージェント、SNMP ライブラリ、SNMP エージェントから情報を要求または設定するツール、SNMP トラップを生成および処理するツールなどが含まれます。

Net-SNMP は <http://www.net-snmp.org/download.html> を参照してください。

-  Net-SNMP はオープンソースフレームワークなので、予期しない変更が行われる可能性があります。
-  お使いの Windows プラットフォームのリリースと Windows 向け Net-SNMP に互換性があることを確認してください。


Windows が Win64 プラットフォームベースで Win32 プラットフォーム向けの Net-SNMP をインストールした場合、Windows サービス拡張 DLL に互換性はありません。この場合、Net-SNMP マスターエージェントは ServerView Agents と通信できません。

### インストール

-  Net-SNMP のマニュアル:  
Net-SNMP はインストールパッケージで配布された **INSTALL** ファイルを参照します。  
その他のマニュアルについては、<http://www.net-snmp.org/docs/> を参照してください。

1. Net-SNMP のマニュアルに従って Net-SNMP パッケージをインストールします。

以下の事項を考慮する必要があります。

-  v5.4 以降では、Net-SNMP エージェントは Windows SNMP サービス拡張 DLL を Net-SNMP winExtDLL 拡張を使用して読み込みます。



暗号化を使用できるようにするためには、OpenSSL (<https://www.openssl.org>) をインストールする必要があります。

**Net-SNMP バージョン 5.7.3(LTS)、5.6.2.1、5.5.2.1、5.4.4(LTS) :**

Net-SNMP Windows バイナリは OpenSSL バージョン 0.9.8r で作成されています。OpenSSL 0.9 および 1.0 DLL は互換性がないため、Net-SNMP を OpenSSL 1.0 がインストールされているシステムにインストールしようとしても失敗します。

- a. Net-SNMP インストールウィザードの「**Choose Components**」ウィンドウで次の手順に従います。

「**Net-SNMP Agent Service**」コンポーネントで、「**With Windows Extension DLL support**」設定を有効にします。

- b. 暗号化を使用できるようにするためには、次の手順に従います。

Net-SNMP インストールウィザードの「**Choose Components**」ウィンドウで、「**Encryption support (openssl)**」コンポーネントを有効にします。

2. **Net-SNMP Agent Service** を Windows サービスとして登録します。

推奨: Net-SNMP インストールディレクトリにあるバッチファイル **registeragent.bat** を使用します。

### 3.4.4 Net-SNMP の設定 (Windows/Linux)



SNMPv3 は、ユーザ固有の総合的なセキュリティコンセプトおよびセキュリティ管理計画の一部として実装する必要があります。

本書で説明する手順とメカニズムは、単独では総合的な保護には不十分です。全体的なセキュリティコンセプトに合わせて統合する必要があります。



Net-SNMP はオープンソースフレームワークなので、予期しない変更が行われる可能性があります。

その他のマニュアルについては、<http://www.net-snmp.org/docs/> を参照してください。



このアーキテクチャ( [17 ページのエージェントのアーキテクチャ](#)を参照) では、サブエージェントには SNMP の情報がありません。メッセージ処理(どのバージョンのどのプロトコルか)とセキュリティおよびアクセス制御は、マスターエージェントで処理されます。

SNMPv3 セキュリティのサポートは Net-SNMP マスターエージェント設定の一般タスクで、サブエージェントとは関係ありません。

Net-SNMP の設定にはいくつかの方法があります。以降では、Net-SNMP は設定ファイル **snmpd.conf** によって設定されます。

情報については、<http://www.net-snmp.org/docs/> を参照してください。

## Windows

Windows で **snmpd.conf** ファイルを見つけます。

1. **snmpd.conf** ファイルは <net-snmp installdir>\etc\snmp ディレクトリにあります。

## Linux

Linux で **snmpd.conf** ファイルを見つけます。

**snmpd.conf** ファイルを見つける方法は複数あります。1 つは、Net-SNMP マスターエージェントの出力をデバッグする方法です。

1. 次のパラメータで **snmpd** デーモンを呼び出します。

```
snmpd -f -Lo -Dread_config -H 2>&1 | grep "config path" |
head -1
```

出力は以下ようになります。

```
config path used for
snmpd:/etc/snmp:/usr/share/snmp:/usr/lib64/snmp:/root/.snmp:
(persistent path:/var/lib/net-snmp)
```

2. **snmpd.conf** ファイルは **/etc/snmp** ディレクトリにあります。

### 3.4.4.1 snmpd.conf の設定

1. **snmpd.conf** 設定ファイルを開きます。



**snmpd.conf** パーシステントファイルの内容は、Net-SNMP マスターエージェントが停止されるたびに上書きされます。Net-SNMP マスターエージェントが実行されているときは、**snmpd.conf** パーシステントファイルを編集しないことを推奨します。

2. ユーザを作成します。

**snmpd.conf** 設定ファイルに **createUser** ステートメントを追加します。

```
createUser [-e ENGINEID] <username> [(MD5|SHA)
<authpassphrase> [DES|AES] [<privpassphrase>]]
```




例：

- **createUser adminA MD5 adminAdminA**

**adminA** というユーザを定義します。このユーザを、認証付きでプライバシーのない要求に使用できます。パスワードは **adminAdminA** で、使用するハッシュアルゴリズムは **MD5** です。

- **createUser adminP MD5 adminAdminA DES adminAdminP**

**adminP** というユーザを定義します。このユーザをプライバシー付きの要求に使用できます( 認証付きでもある、[11 ページの SNMPv3: 新機能](#)を参照)。認証プロセスのパスワードは **adminAadminA** で、使用するハッシュアルゴリズムは **MD5** です。暗号化手順のパスワードは **adminPadminP** で、使用するハッシュアルゴリズムは **DES** です。

-  認証とプライバシーに同じパスワードを使用するためには、暗号アルゴリズムの後のステートメントを省略します。
-  USM( [11 ページの SNMPv3: 新機能](#)を参照) は認証のないプライバシーを定義しません。
-  SNMPv3 パスフレーズは 8 文字以上にしてください。

### 3. アクセス制御を定義します。

読み取り専用アクセスに **rouser**、または読み書きアクセスに **rwuser** を **snmpd.conf** ファイルに追加します。

```
rouser <username> secLevel:{noauth|auth|priv} [restriction_
mibtree]
```

```
rwuser <username> secLevel:{noauth|auth|priv} [restriction_
mibtree]
```

例：

- `rouser adminA auth`

上記で定義した SNMPv3 ユーザ **adminA** に、フル MIB ツリーへの読み取り専用アクセスを付与します。

- `rwuser adminA auth .1.3.6.1.4.1.231.2`

**adminA** に個々のサブツリー **1.3.6.1.4.1.231.2** への選択的読み書きアクセスを付与します。

### 4. Net-SNMP サービスを再起動します。

デーモンを再起動すると、**snmpd.conf** パーシステントファイルに **usmUser** エントリが作成されます。

例：

```
usmUser 1 3 0x80001f88800706b92268f4934900000000
0x61646d696e4100 0x61646d696e4100 NULL .1.3.6.1.6.3.10.1.1.2
0x60c245359704f595b1af164a411d299d .1.3.6.1.6.3.10.1.2.1 ""
""
```

基本的に、**usmUser** ステートメントには **createUser** エントリと同じ情報が含まれます。主な違いは、読み取り可能なパスワードがローカライズされたキーに置換されていることです( Net-SNMP のマニュアルを参照)。

以降は、**snmpd** デーモンは **usmUser** 情報を使用します。

5. セキュリティ上の理由から、**snmpd.conf** 設定ファイルから元の **createUser** エントリを削除します。
6. オプション: より複雑なアクセス制御 - VACM

ビューベースのアクセス制御 (VACM) は SNMPv3 標準の一部で、フレームワークの実装面を担当します。VACM の主な特長は、セキュリティ名 (SNMPv3 のユーザ名) を専用 MIB ツリーのアクセス権に割り当てることです。

詳細は、Net-SNMP のマニュアルを参照してください。

7. トラップを設定します。

トラップ/インフォーム通知のターゲットを指定するためには、**snmpd.conf** に以下の行を追加します。

```
trapsess [-e ENGINEID] -v 3 -l  
(noAuthNoPriv|authNoPriv|authPriv) -u <username> <target>
```

例:

```
trapsess -v 3 -l authNoPriv -u adminA 10.172.103.139:162
```

これにより、認証された、暗号化されていないトラップが IP アドレス 10.172.103.139 ポート 162 に送信されます。

8. Net-SNMP サービスを再起動します。

## 3.4.5 Net-SNMP マスターエージェントによる ServerView Agents のアップデート (Windows/Linux)

### 3.4.5.1 Linux

ServerView Agent 通信を SNMPv3 で設定すると、通常のすべてのアップデート手順を実行できます。

### 3.4.5.2 Windows

Net-SNMP と Microsoft Windows SNMP サービスの関係には以下が必要です。

- Microsoft Windows SNMP サービスでは SNMPv3 をサポートしませんが、サーバ監視のその他の機能をサポートするためには、インストールする必要があります。

さらに、ServerView Agents バージョン < 7.20 からバージョン ≤ 7.20 にアップグレードした場合は、以下が該当します。

- ServerView Agents をインストールするためには、Microsoft Windows SNMP サービスを有効にして、正しいインストールプロセスを実施する必要があります。
- Windows ベースのサーバを Net-SNMP マスターエージェントで監視している場合、



Microsoft Windows SNMP サービスを無効にするか、SNMPv3 通信を確保するために起動タイプを「手動」に設定する必要があります。そうしないと、システムの次回起動時に Windows SNMP サービスが再起動してしまいます。



2つのマスターエージェントの共存については、Net-SNMP のマニュアルを参照してください。

このため、ServerView Agents のバージョンによってアップデートプロセスは異なります。

#### ServerView Agents バージョン < 7.20 からバージョン ≤ 7.20 へのアップデート

ServerView Agents をアップデートするためには、次の手順に従います。

1. Microsoft Windows SNMP サービスが無効になっている場合は、有効にします(起動タイプを「手動」に設定する必要はありません)。

Microsoft Windows SNMP サービスの処理の詳細については、『**ServerView Agents for Windows**』マニュアルか、Microsoft の該当するマニュアルを参照してください。

2. Microsoft Windows SNMP サービスを有効にします。
3. 通常の手順で ServerView Agents をアップデートします(アップデート管理の ServerView のマニュアルを参照)。
4. Microsoft Windows SNMP サービスを停止します。

Microsoft Windows SNMP サービスの処理の詳細については、『**ServerView Agents for Windows**』マニュアルか、Microsoft の該当するマニュアルを参照してください。

5. Windows SNMP サービスを無効にするか、起動タイプを「手動」にします。
6. Net-SNMP サービスを再起動します。


#### ServerView Agents バージョン ≥ 7.20 からバージョン > 7.20 へのアップデート

ServerView Agents をアップデートするためには、次の手順に従います。


1. 通常の手順で ServerView Agents をアップデートします(アップデート管理の ServerView のマニュアルを参照)。

---

## 4 Operations Manager での SNMPv3 の使用


 SNMPv3 は、ユーザ固有の総合的なセキュリティコンセプトおよびセキュリティ管理計画の一部として実装する必要があります。

本書で説明する手順とメカニズムは、単独では総合的な保護には不十分です。全体的なセキュリティコンセプトに合わせて統合する必要があります。

 Operations Manager バージョン 7.0x およびそれ以前は SNMPv3 をサポートしません。

### 4.1 アーキテクチャと要件

#### 4.1.1 Operations Manager と ServerView Agents との間の SNMPv3 通信

 Operations Manager バージョン 7.0x およびそれ以前は SNMPv3 をサポートしません。


##### 4.1.1.1 SNMPv3 通信の共通ユーザ

Operations Manager の中央管理用サーバと管理対象ノード上の ServerView Agents との間で SNMP バージョン 3 の通信を行うためには、通信エンドポイントで共通ユーザを設定する必要があります。

##### 4.1.1.2 Windows: 2 つの SNMP サービスの共存: UDP ポートの再構成

SNMP バージョン 1 および 2c では、Microsoft は Microsoft Windows SNMP サービスを Microsoft Windows に統合しています。しかし、Microsoft Windows SNMP サービスでは SNMP バージョン 3 をサポートしていません。

SNMPv3 を使用して Windows ベースのサーバを管理するためには、Net-SNMP サービスを追加する必要があります。

 Microsoft Windows SNMP サービスに必要なアドオンとして、Net-SNMP サービスを推奨します。

- ❶ Microsoft Windows SNMP サービスでは SNMPv3 をサポートしていませんが、必要な Windows SNMP サービス拡張 DLL および Windows SNMP API を `snmpapi.dll` から提供するためには、インストールする必要があります。
- ❷ 2 つの SNMP サービスの共存については、Net-SNMP のマニュアルを参照してください。

トラフィックを Windows SNMP サービスに転送するためには、Windows SNMP サービスの UDP ポートを再構成する必要があります(図を参照)。

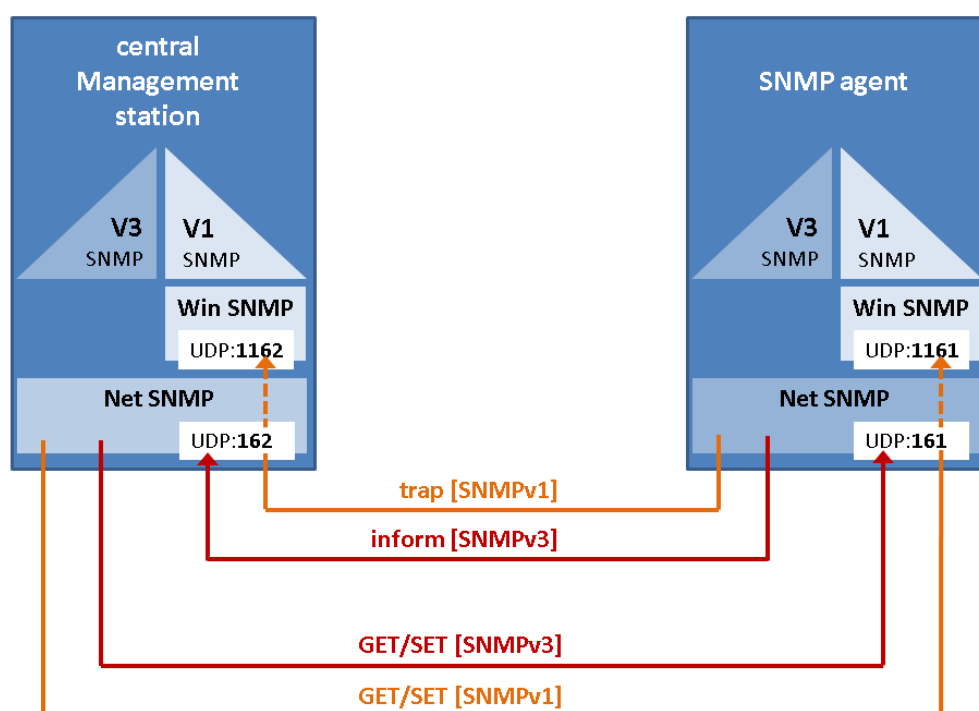


図 3: Operations Manager 通信の SNMP エージェント/中央管理用サーバのポート

## 4.1.2 Operations Manager の技術的要件

### 4.1.2.1 管理対象サーバ: ServerView Agents

ServerView Agents の技術的要件については、[19 ページの ServerView Agents の技術的要件](#)を参照してください。

### 4.1.2.2 中央管理用サーバ: Operations Manager

Operations Manager は以下で使用できます。

### Windows

- Microsoft Windows® Server 2012 の全エディション  
(ただし Server Core インストール以外)
- Microsoft Windows® Server 2012 R2 の全エディション  
(ただし Server Core インストール以外)
- Microsoft Windows® Server 2008 の全エディション  
(ただし Server Core インストール以外)
- Microsoft Windows® Server 2008 R2 の全エディション  
(ただし Server Core インストール以外)

Operations Manager の技術的要件の詳細については、『ServerView Operations Manager - Installing ServerView Operations Manager Software under Windows』マニュアルを参照してください。


### Linux

- SUSE( SLES 11) : SP2 および SP3
- Red Hat Enterprise Linux 5.9 / 5.10
- Red Hat Enterprise Linux 6.4/6.5
- Red Hat Enterprise Linux 7.0

Operations Manager の技術的要件の詳細については、『ServerView Operations Manager - Installing ServerView Operations Manager Software under Linux』マニュアルを参照してください。

## 4.2 中央管理用サーバ(CMS)での設定

### 4.2.1 Windows ベースのシステム: 処理の概要

 Operations Manager バージョン 7.0x およびそれ以前は SNMPv3 をサポートしません。

指定された状況と目的によって、手順は異なります。

#### 4.2.1.1 SNMPv3 への切り替え

**状況** : Operations Manager が Windows ベースのシステムにインストールされ、この監視ソリューションは SNMPv1 を使用している。

**目的** : SNMPv3 を使用する。

手順:

1. **Operations Manager を V7.1x 以上にアップデートする**

Net-SNMP のインストール前のアップデートは、通常通り実行できます(アップデート管理の ServerView のマニュアルを参照)。

2. **Microsoft Windows SNMP サービスの無効化**

Microsoft Windows SNMP サービスでは SNMP バージョン 3 をサポートしていません。SNMPv3 を使用して Windows ベースのシステムを管理するためには、Microsoft Windows SNMP サービスを無効にしてから SNMP マスターエージェントを別の SNMPv3 対応スタックに置換する必要があります。

詳細は、[34 ページの Operations Manager と ServerView Agents との間の SNMPv3 通信](#)を参照してください。

手順については、[40 ページの Windows SNMP サービスの無効化 \(Windows\)](#)を参照してください。

3. **Net-SNMP のインストール**

手順については、[40 ページの Net-SNMP のインストール\(Windows\)](#)を参照してください。

4. **新規 SNMP デーモンの設定 - Net-SNMP の例を使用**

少なくとも USM ユーザを作成し、アクセス制御を定義して、トラップと Windows SNMP サービスへのトラップ転送を構成する必要があります。

詳細は、[11 ページの SNMPv3: 新機能](#)と[34 ページの Operations Manager と ServerView Agents との間の SNMPv3 通信](#)を参照してください。

手順については、[42 ページの CMS 上の Windows: UDP ポートの再構成、snmptrapd.conf の登録と設定](#)を参照してください。

5. **snmp.conf による Operations Manager の SNMPv3 の有効化**

手順については、[47 ページの Operations Manager での SNMPv3 の有効化](#)を参照してください。

#### 4.2.1.2 初期インストール

状況 : Operations Manager を Windows ベースのシステムにインストールする。

目的 : 新規インストールした監視ソリューションで SNMPv3 を使用する。

手順:

1. **Microsoft Windows SNMP サービスのインストールまたは有効化**

手順については、[40 ページの Microsoft Windows SNMP サービスのインストールまたは有効化 \(Windows\)](#)を参照してください。

## 2. Operations Manager V7.1x 以上をインストールする

手順については、[40 ページの Operations Manager のインストール\(Windows/Linux\)](#) を参照してください。

## 3. Microsoft Windows SNMP サービスの無効化

Microsoft Windows SNMP サービスでは SNMP バージョン 3 をサポートしていません。SNMPv3 を使用して Windows ベースのサーバを管理するためには、Microsoft Windows SNMP サービスを無効にしてから SNMP マスターエージェントを別の SNMPv3 対応スタックに置換する必要があります。

詳細は、[34 ページの Operations Manager と ServerView Agents との間の SNMPv3 通信](#) を参照してください。

手順については、[40 ページの Windows SNMP サービスの無効化\(Windows\)](#) を参照してください。

## 4. Net-SNMP のインストール

手順については、[40 ページの Net-SNMP のインストール\(Windows\)](#) を参照してください。

## 5. 新規 SNMP デーモンの設定 - Net-SNMP の例を使用

少なくとも USM ユーザを作成し、アクセス制御を定義して、トラップと Windows SNMP サービスへのトラップ転送を構成する必要があります。


詳細は、[11 ページの SNMPv3: 新機能](#)と[34 ページの Operations Manager と ServerView Agents との間の SNMPv3 通信](#) を参照してください。

手順については、[42 ページの CMS 上の Windows: UDP ポートの再構成、snmptrapd.conf の登録と設定](#) を参照してください。

## 6. snmp.conf による Operations Manager の SNMPv3 の有効化

手順については、[47 ページの Operations Manager での SNMPv3 の有効化](#) を参照してください。

## 4.2.2 Linux ベースのシステム: 処理の概要

 Operations Manager バージョン 7.0x およびそれ以前は SNMPv3 をサポートしません。

指定された状況と目的によって、手順は異なります。

### 4.2.2.1 SNMPv3 への切り替え

「状況」: Operations Manager が Linux ベースのシステムにインストールされ、この監視ソリューションは SNMPv1 を使用している。

「目的」: SNMPv3 を使用する。

手順:

1. Operations Manager を V7.1x 以上にアップデートする

Net-SNMP のインストール前のアップデートは、通常通り実行できます(アップデート管理の ServerView のマニュアルを参照)。

2. 新規 SNMP デーモンの設定 - Net-SNMP の例を使用

少なくとも USM ユーザを作成し、アクセス制御を定義してトラップを構成する必要があります。

詳細は、[11 ページの SNMPv3: 新機能](#)を参照してください。

手順については、[42 ページの CMS 上の Windows: UDP ポートの再構成、snmptrapd.conf の登録と設定](#)を参照してください。

3. snmp.conf による Operations Manager の SNMPv3 の有効化

手順については、[47 ページの Operations Manager での SNMPv3 の有効化](#)を参照してください。

#### 4.2.2.2 初期インストール

状況 : Operations Manager を Linux ベースのシステムにインストールする。

目的 : 新規インストールした監視ソリューションで SNMPv3 を使用する。

手順:

1. Operations Manager V7.1x 以上をインストールする

手順については、[40 ページの Operations Manager のインストール\(Windows/Linux\)](#)を参照してください。

2. 新規 SNMP デーモンの設定 - Net-SNMP の例を使用

少なくとも USM ユーザを作成し、アクセス制御を定義してトラップを構成する必要があります。


詳細は、[11 ページの SNMPv3: 新機能](#)を参照してください。

手順については、[45 ページの CMS 上の Linux: snmptrapd.conf の設定](#)を参照してください。

3. snmp.conf による Operations Manager の SNMPv3 の有効化

手順については、[47 ページの Operations Manager での SNMPv3 の有効化](#)を参照してください。


### 4.2.3 Operations Manager のインストール(Windows/Linux)


 Operations Manager バージョン 7.0x およびそれ以前は SNMPv3 をサポートしません。

1. Operations Manager バージョン 7.1x 以上をインストールします。

Operations Manager のインストールの詳細については、『ServerView Operations Manager - Installation Guide』マニュアルを参照してください。

### 4.2.4 Microsoft Windows SNMP サービスのインストールまたは有効化 (Windows)

 Microsoft Windows SNMP サービスでは SNMPv3 をサポートしていませんが、必要な Windows SNMP サービス拡張 DLL および Windows SNMP API を `snmpapi.dll` から提供するためには、インストールする必要があります。


 Operations Manager をインストールするためには、Microsoft Windows SNMP サービスを有効にして、正しいインストールプロセスを実施する必要があります。

1. Microsoft Windows SNMP サービスをインストールおよび有効にします。

このサービスのインストールと有効化の詳細については、Microsoft の該当するマニュアルを参照してください。

### 4.2.5 Windows SNMP サービスの無効化 (Windows)


1. Microsoft Windows SNMP サービスが実行されている場合は、停止します。
2. Windows SNMP サービスを無効にするか、起動タイプを「手動」にします。


 そうしないと、システムの次回起動時に Windows SNMP サービスが再起動してしまいます。

2 つのデーモンの共存については、Net-SNMP のマニュアルを参照してください。

Microsoft Windows SNMP サービスの処理の詳細については、Microsoft の該当するマニュアルを参照してください。

### 4.2.6 Net-SNMP のインストール(Windows)

 SNMPv3 を ServerView 通信に使用するためには、Net-SNMP サービスを推奨します。

 **Linux:** Net-SNMP サービスは、大部分の Linux ディストリビューションに付属しています。



#### 4.2.6.1 Net-SNMP のソース

Net-SNMP は Simple Network Management Protocol に関連するツールとライブラリを提供します。拡張可能なエージェント、SNMP ライブラリ、SNMP エージェントから情報を要求または設定するツール、SNMP トラップを生成および処理するツールなどが含まれます。

Net-SNMP は <http://www.net-snmp.org/download.html> を参照してください。



Net-SNMP はオープンソースフレームワークなので、予期しない変更が行われる可能性があります。



お使いの Windows プラットフォームのリリースと Windows 向け Net-SNMP に互換性があることを確認してください。

Windows が Win64 プラットフォームベースで Win32 プラットフォーム向けの Net-SNMP をインストールした場合、Windows サービス拡張 DLL に互換性はありません。この場合、Net-SNMP マスターエージェントは ServerView Agents と通信できません。

#### 4.2.6.2 インストール



Net-SNMP のマニュアル:

Net-SNMP はインストールパッケージで配布された **INSTALL** ファイルを参照します。  
その他のマニュアルについては、<http://www.net-snmp.org/docs/> を参照してください。

1. Net-SNMP のマニュアルに従って Net-SNMP パッケージをインストールします。

以下の事項を考慮する必要があります。



暗号化を使用できるようにするためには、OpenSSL (<https://www.openssl.org>) をインストールする必要があります。

**Net-SNMP バージョン 5.7.3(LTS)、5.6.2.1、5.5.2.1、5.4.4(LTS):**

Net-SNMP Windows バイナリは OpenSSL バージョン 0.9.8r で作成されています。OpenSSL 0.9 および 1.0 DLL は互換性がないため、Net-SNMP を OpenSSL 1.0 がインストールされているシステムにインストールしようとしても失敗します。


- a. Net-SNMP インストールウィザードの「**Choose Components**」ウィンドウで次の手順に従います。  
「**Net-SNMP Agent Service**」コンポーネントで、「**With Windows Extension DLL support**」設定を有効にします。
- b. 暗号化を使用できるようにするためには、次の手順に従います。

Net-SNMP インストールウィザードの「Choose Components」ウィンドウで、「Encryption support (openSSL)」コンポーネントを有効にします。

2. Net-SNMP Agent Service を Windows サービスとして登録します。


推奨: Net-SNMP インストールディレクトリにあるバッチファイル `registeragent.bat` を使用します。

## 4.2.7 CMS 上の Windows: UDP ポートの再構成、snmptrapd.conf の登録と設定

 要件: Operations Manager をインストールする必要があります。40 ページの [Operations Manager のインストール \(Windows/Linux\)](#) を参照してください。


### 4.2.7.1 UDP ポートの再構成


SNMPv3 を使用して Windows ベースのサーバを管理するためには、Net-SNMP サービスを追加する必要があります。

 Microsoft Windows SNMP サービスでは SNMPv3 をサポートしていませんが、必要な Windows SNMP サービス拡張 DLL および Windows SNMP API を `snmpapi.dll` から提供するためには、インストールする必要があります。

トラフィックを Windows SNMP サービスに転送するためには、Windows SNMP サービスの UDP ポートを再構成する必要があります( 34 ページの [Operations Manager と ServerView Agents との間の SNMPv3 通信](#) を参照)。

1. ファイル `C:\Windows\<Systems32>\drivers\etc\services` を開きます。
2. `snmpd` で始まる行を見つけます。
3. 値 `162/udp` を変更します( `1162/udp` など)。
4. 変更を保存します。
5. Windows SNMP サービスを再起動します。

 2 つの SNMP サービスの共存については、Net-SNMP のマニュアルを参照してください。

 トラフィックを Windows SNMP サービスに転送するためには、`snmptrapd.conf` ファイルで転送コマンドを設定する必要があります( 以下を参照)。

### 4.2.7.2 Net-SNMP Service を Windows サービスとして登録する

1. Net-SNMP のインストール場所で **snmpd.exe** ファイルを見つけます。
2. コマンドラインを開きます。
3. 次のコマンドを実行します。

```
snmpd -register -Lf"C:\usr\LOG_AGENT" -I-  
udp,udpTable,tcp,tcpTable,icmp,ip,interfaces,system_  
mib,sysORTable
```

### 4.2.7.3 snmptrapd.conf の設定

1. Windows で **snmptrapd.conf** ファイルを見つけます。  
**snmptrapd.conf** ファイルは <net-snmp installdir>\etc\snmp ディレクトリにあります。
2. **snmptrapd.conf** 設定ファイルを開きます。
3. トラフィック転送と共通ユーザの設定を指定します。
  - ユーザを作成します。



Operations Manager の中央管理用サーバと管理対象ノード上の ServerView Agents との間で SNMP バージョン 3 の通信を行うためには、通信エンドポイントで共通ユーザを設定する必要があります。

**snmptrapd.conf** ファイルに **createUser** ステートメントを追加します。

```
createUser [-e ENGINEID] <username> [(MD5|SHA)  
<authpassphrase> [DES|AES] [<privpassphrase>]]
```

例：

- **createUser adminA MD5 adminAadminA**

**adminA** というユーザを定義します。このユーザを、暗号化なしの認証済み SNMPv3 メッセージに使用できます。パスワードは **adminAadminA** で、使用するハッシュアルゴリズムは **MD5** です。

- **createUser adminP MD5 adminAadminA DES adminPadminP**

**adminP** というユーザを定義します。このユーザを認証済みで暗号化された SNMPv3 メッセージに使用できます( [11 ページの SNMPv3: 新機能](#) を参照)。認証プロセスのパスワードは **adminAadminA** で、使用するハッシュアルゴリズムは **MD5** です。暗号化手順のパスワードは **adminPadminP** で、使用するハッシュアルゴリズムは **DES** です。



認証とプライバシーに同じパスワードを使用するためには、暗号アルゴリズムの後のステートメントを省略します。



USM( 11 ページのSNMPv3: 新機能 を参照 ) は認証のないプライバシーを定義しません。



SNMPv3 パスフレーズは 8 文字以上にしてください。

- トラップに回答して実行されるプログラムを定義します。

**snmptrapd.conf** ファイルに **traphandle** ステートメントを追加します。

```
traphandle default "<file path>"
```

特定のトラップ OID に回答して実行されるプログラムを定義します。**default** は、これまで定義されていないすべてのトラップ OID を対象とします。

- トラップの転送を Windows SNMP サービスに設定します。

**snmptrapd.conf** ファイルに **forward** ステートメントを追加します。

```
forward default localhost:1162
```

特定の OID のトラップを宛先 IP アドレスに転送します。**default** は、これまで定義されていないすべてのトラップ OID を対象とします。

4. Net-SNMP サービスを再起動します。

#### 4.2.7.4 snmptrapd.conf ファイルの例

```
authCommunity net public
authUser log,execute testuser
createUser testuser MD5 testuser AES testuser
traphandle default "C:\Program Files
(x86)\Fujitsu\ServerView Suite\ServerView\ServerView
Services\scripts\ServerView\SnmpTrap\SnmpTrapListen3"
forward default localhost:1162
```

##### 説明

- **authCommunity/authUser**

特定のユーザまたはコミュニティ文字列が所有するクレデンシャルを定義します。

- **net**

通信を転送します。

- **log**

トラップをログに記録します。

- **execute**

トラップに回答して実行可能ファイルを実行します。

## 4.2.8 CMS 上の Linux: snmptrapd.conf の設定



要件 : Operations Manager をインストールする必要があります。 [40 ページの Operations Manager のインストール\(Windows/Linux\)](#) を参照してください。

### 4.2.8.1 snmptrapd.conf の設定

1. Linux で **snmptrapd.conf** ファイルを見つけます。

**snmptrapd.conf** ファイルを見つける方法は複数あります。1 つは、Net-SNMP マスターエージェントの出力をデバッグする方法です。

- 次のパラメータで **snmpd** デーモンを呼び出します。

```
snmpd -f -Lo -Dread_config -H 2>&1 | grep "config path" | head -1
```

出力は以下ようになります。

```
config path used for
snmptrapd:/etc/snmp:/usr/share/snmp:/usr/lib64/snmp:/root
/.snmp: (persistent path:/var/lib/net-snmp)
```

- **snmptrapd.conf** ファイルは **/etc/snmp** ディレクトリにあります。

2. **snmptrapd.conf** 設定ファイルを開きます。
3. トラフィック転送と共通ユーザの設定を指定します。
  - ユーザを作成します。



Operations Manager の中央管理用サーバと管理対象ノード上の ServerView Agents との間で SNMP バージョン 3 の通信を行うためには、通信エンドポイントで共通ユーザを設定する必要があります。

**snmptrapd.conf** ファイルに **createUser** ステートメントを追加します。

```
createUser [-e ENGINEID] <username> [(MD5|SHA)
<authpassphrase> [DES|AES] [<privpassphrase>]]
```

例 :

- **createUser adminA MD5 adminAadminA**

**adminA** というユーザを定義します。このユーザを、認証付きでプライバシーのない要求に使用できます。パスワードは **adminAadminA** で、使用するハッシュアルゴリズムは **MD5** です。

- **createUser adminP MD5 adminAadminA DES adminPadminP**

**adminP** というユーザを定義します。このユーザをプライバシー付きの要求に使用できます( 認証付きでもある、 [11 ページの SNMPv3: 新機能](#) を参照)。認証プロ

セスのパスワードは **adminAadminA** で、使用するハッシュアルゴリズムは **MD5** です。暗号化手順のパスワードは **adminPadminP** で、使用するハッシュアルゴリズムは **DES** です。



認証と暗号化に同じパスワードを使用するためには、暗号アルゴリズムの後のステートメントを省略します。



USM( [11 ページの SNMPv3: 新機能](#) を参照) は認証のない暗号化を定義しません。



SNMPv3 パスフレーズは 8 文字以上にしてください。

- トラップに回答して実行されるプログラムを定義します。

**snmptrapd.conf** ファイルに **traphandle** ステートメントを追加します。

```
traphandle default "<file path>"
```

特定のトラップ OID に回答して実行されるプログラムを定義します。**default** は、これまで定義されていないすべてのトラップ OID を対象とします。

4. Net-SNMP サービスを再起動します。

#### 4.2.8.2 snmptrapd.conf ファイルの例

```
authCommunity net public
authUser log,execute testuser
createUser testuser MD5 testuser AES testuser
traphandle default "C:\Program Files
(x86)\Fujitsu\ServerView Suite\ServerView\ServerView
Services\scripts\ServerView\SnmpTrap\SnmpTrapListen3"
```

##### 説明

- **authCommunity/authUser**

特定のユーザまたはコミュニティ文字列が所有するクレデンシャルを定義します。

- **net**

通信を転送します。

- **log**

トラップをログに記録します。

- **execute**

トラップに回答して実行可能ファイルを実行します。

## 4.2.9 Operations Manager での SNMPv3 の有効化

管理対象ノード(51 ページの管理対象サーバでの設定を参照)と中央管理用サーバ(36 ページの中央管理用サーバ(CMS)での設定を参照)を準備してある場合、Operations Manager で SNMPv3 を有効にできます。

SNMPv3 を Operations Manager で有効にするには、2 つの方法があります。

- 「V3 Setting」設定ウィンドウを使用する

47 ページの「V3 Setting」設定ウィンドウで Operations Manager の SNMPv3 を有効にするを参照

または

- 設定ファイル `snmp.conf` を使用する

50 ページの `snmp.conf` による Operations Manager の SNMPv3 の有効化を参照

### 4.2.9.1 「V3 Setting」設定ウィンドウで Operations Manager の SNMPv3 を有効にする

Operations Manager V7.10 以上では、「V3 Setting」設定ウィンドウで Operations Manager の SNMPv3 を有効にできます。

#### 「V3 Setting」設定ウィンドウを開く

Operations Manager の「V3 Setting」設定ウィンドウは、中央管理用サーバの Web アドレスを直接入力して開くことができます。

1. 以下の Web アドレスを入力します。

`https://<server_name>.<domain_name>:3170/SNMPv3Settings/Settings`

「V3 Setting」設定ウィンドウが開きます。

SNMPv3 Settings - Mozilla Firefox

https://...:3170/SNMPv3Settings/Settings

V3 Setting

After any change you must restart the ServerView service in order to see changes.

Enable V3 ☐

Security Name

Authentication Password

Privacy Password

Security level

Authentication algorithm

Privacy algorithm

Note: Password must have more than 8 characters

図 4: 「V3 Setting」設定ウィンドウ



## 設定

### 説明



Operations Manager の中央管理用サーバと管理対象ノード上の ServerView Agents との間で SNMP バージョン 3 の通信を行うためには、通信エンドポイントで共通ユーザを設定する必要があります。

- **Enable V3**

SNMP バージョン 3 プロトコルを設定します。

- **Security Name**

Operations Manager に定義されたユーザ名。[42 ページの CMS 上の Windows: UDP ポートの再構成、snmptrapd.conf の登録と設定](#) または [45 ページの CMS 上の Linux: snmptrapd.conf の設定](#) を参照してください。

- **Authentication Password**

認証用パスワードです。

- **Privacy Password**

暗号化用パスワードです。

- **セキュリティレベル**

セキュリティレベルです。

可能な値: 「None」、「authNoPriv」、「authPriv」。詳細は、[11 ページの SNMPv3: 新機能](#) を参照してください。

- **Authentication algorithm**

ユーザが使用する認証アルゴリズムです。

可能な値: 「MD5」、「SHA」。詳細は、[11 ページの SNMPv3: 新機能](#) を参照してください。

- **Privacy algorithm**

ユーザが使用する暗号化アルゴリズムです。

可能な値: 「DES」、「AES」。詳細は、[11 ページの SNMPv3: 新機能](#) を参照してください。

設定を保存します。

1. 「V3 Setting」設定ウィンドウで「Save」ボタンをクリックします。

#### 4.2.9.2 snmp.conf による Operations Manager の SNMPv3 の有効化

##### snmp.conf の場所

SNMPv3 は、設定ファイル **snmp.conf** を追加で作成して、Operations Manager で有効にできます。このファイルは以下のディレクトリにあります。

##### Windows

C:\usr\etc\snmp\snmp.conf

##### Linux

/usr/local/etc/snmp/snmp.conf

##### snmp.conf の内容

snmp.conf には以下の記述があります。

```
defVersion 3
defSecurityName testuser
defSecurityLevel authNoPriv
defPassphrase testuser
defAuthType MD5
defPrivType AES
```

##### 説明



Operations Manager の中央管理用サーバと管理対象ノード上の ServerView Agents との間で SNMP バージョン 3 の通信を行うためには、通信エンドポイントで共通ユーザを設定する必要があります。

- **defSecurityName**

Operations Manager に定義されたユーザ名。[42 ページの CMS 上の Windows: UDP ポートの再構成、snmptrapd.conf の登録と設定](#)または[45 ページの CMS 上の Linux: snmptrapd.conf の設定](#)を参照してください。

- **defPassphrase**

認証と暗号化のパスワードです。

パスワードが異なる場合は、**defAuthPassphrase** と **defPrivPassphrase** の設定を使用します。

- **defSecurityLevel**

セキュリティレベルです。

可能な値:「noAuthNoPriv」、「authNoPriv」、「authPriv」。詳細は、[11 ページの SNMPv3: 新機能](#)を参照してください。

- **defAuthType**

ユーザが使用する認証アルゴリズムです。

可能な値:「MD5」、「SHA」。詳細は、[11 ページの SNMPv3: 新機能](#) を参照してください。

- **defPrivType**

ユーザが使用する暗号化アルゴリズムです。

可能な値:「DES」、「AES」。詳細は、[11 ページの SNMPv3: 新機能](#) を参照してください。

## 4.3 管理対象サーバでの設定

### 4.3.1 Windows ベースのサーバ: 処理の概要

指定された状況と目的によって、手順は異なります。

#### 4.3.1.1 SNMPv3 への切り替え

**状況** : Windows ベースのサーバを ServerView Agents で監視している。

**目的** : SNMPv3 を使用する。

**手順** :

1. **ServerView Agents の V7.01 へのアップデート**

Net-SNMP のインストール前のアップデートは、通常通り実行できます( アップデート 管理 の ServerView のマニュアルを参照 )。

2. **Microsoft Windows SNMP サービスの無効化**

Microsoft Windows SNMP サービスでは SNMP バージョン 3 をサポートしていません。SNMPv3 を使用して Windows ベースのサーバを管理するためには、Microsoft Windows SNMP サービスを無効にしてから SNMP マスターエージェントを別の SNMPv3 対応スタックに置換する必要があります。

詳細については、[17 ページのエージェントのアーキテクチャ](#)を参照してください。

手順については、[25 ページの Windows SNMP サービスの無効化と Net-SNMP \(Windows\) のインストール](#)を参照してください。

3. **Net-SNMP のインストール**

手順については、[25 ページの Windows SNMP サービスの無効化と Net-SNMP \(Windows\) のインストール](#)を参照してください。

#### 4. 新規 SNMP マスターエージェントの設定 - Net-SNMP の例を使用

少なくとも USM ユーザを作成し、アクセス制御を定義してトラップを構成する必要があります。

詳細は、[11 ページの SNMPv3: 新機能](#)を参照してください。

手順については、[29 ページの Net-SNMP の設定 \(Windows/Linux\)](#)を参照してください。

#### 4.3.1.2 管理対象サーバの初期インストール

状況：Windows ベースのサーバは ServerView Agents で監視されていない。

目的：サーバを SNMPv3 を使用して ServerView Agents で監視する。

手順：

##### 1. Microsoft Windows SNMP サービスのインストールまたは有効化

手順については、[24 ページの Microsoft Windows SNMP サービスのインストールまたは有効化 \(Windows\)](#)を参照してください。

##### 2. ServerView Agents V7.01 以上のインストール

手順については、[25 ページの ServerView Agents のインストール \(Windows/Linux\)](#)を参照してください。

##### 3. Microsoft Windows SNMP サービスの無効化

Microsoft Windows SNMP サービスでは SNMP バージョン 3 をサポートしていません。SNMPv3 を使用して Windows ベースのサーバを管理するためには、Microsoft Windows SNMP サービスを無効にしてから SNMP マスターエージェントを別の SNMPv3 対応スタックに置換する必要があります。

詳細については、[17 ページのエージェントのアーキテクチャ](#)を参照してください。

手順については、[25 ページの Windows SNMP サービスの無効化と Net-SNMP \(Windows\) のインストール](#)を参照してください。

##### 4. Net-SNMP のインストール

手順については、[25 ページの Windows SNMP サービスの無効化と Net-SNMP \(Windows\) のインストール](#)を参照してください。

##### 5. 新規 SNMP マスターエージェントの設定 - Net-SNMP の例を使用

少なくとも USM ユーザを作成し、アクセス制御を定義してトラップを構成する必要があります。

詳細は、[11 ページの SNMPv3: 新機能](#)を参照してください。

手順については、[29 ページの Net-SNMP の設定 \(Windows/Linux\)](#)を参照してください。

#### 4.3.1.3 アップデート

状況：Windows ベースのサーバを SNMPv3 を使用して ServerView Agents で監視している。

目的：ServerView Agents をアップデートする。

手順：手順については、[32 ページの Net-SNMP マスターエージェントによる ServerView Agents のアップデート \(Windows/Linux\)](#) を参照してください。

### 4.3.2 Linux ベースのサーバ: 処理の概要

指定された状況と目的によって、手順は異なります。

#### 4.3.2.1 SNMPv3 への切り替え

状況：Linux ベースのサーバを ServerView Agents で監視している。

目的：SNMPv3 を使用する。

手順：

1. ServerView Agents の V7.01 へのアップデート

このアップデートは、Net-SNMP のインストール前に実行できます(アップデート管理の ServerView のマニュアルを参照)。

2. SNMP マスターエージェントの設定

少なくとも USM ユーザを作成し、アクセス制御を定義してトラップを構成する必要があります。

詳細は、[11 ページの SNMPv3: 新機能](#) を参照してください。

手順については、[29 ページの Net-SNMP の設定 \(Windows/Linux\)](#) を参照してください。

#### 4.3.2.2 管理対象サーバの初期インストール

状況：Linux ベースのサーバは ServerView Agents で監視されていない。

目的：サーバを SNMPv3 を使用して ServerView Agents で監視する。

手順：

1. ServerView Agents V7.01 以上のインストール

手順については、[25 ページの ServerView Agents のインストール \(Windows/Linux\)](#) を参照してください。

## 2. SNMP マスターエージェントの設定

少なくとも USM ユーザを作成し、アクセス制御を定義してトラップを構成する必要があります。

詳細は、[11 ページの SNMPv3: 新機能](#)を参照してください。

手順については、[29 ページの Net-SNMP の設定 \(Windows/Linux\)](#)を参照してください。

### 4.3.2.3 アップデート

状況 : Linux ベースのサーバを SNMPv3 を使用して ServerView Agents で監視している。

目的 : ServerView Agents をアップデートする。

手順: 手順については、[32 ページの Net-SNMP マスターエージェントによる ServerView Agents のアップデート \(Windows/Linux\)](#)を参照してください。

### 4.3.3 管理対象サーバ上の Windows: UDP ポートの再構成、snmpd.conf の登録と設定



要件 :

管理対象サーバが SNMPv3 を使用するように準備すること。詳細は、[17 ページの ServerView Agents での SNMPv3 の使用](#)を参照してください。

以下は、Operations Manager の中央管理用サーバと管理対象ノード上の ServerView Agents が SNMPv3 で通信できるようにする追加設定です。

#### 4.3.3.1 UDP ポートの再構成

SNMPv3 を使用して Windows ベースのサーバを管理するためには、Net-SNMP サービスを追加する必要があります。





Microsoft Windows SNMP サービスでは SNMPv3 をサポートしていませんが、必要な Windows SNMP サービス拡張 DLL および Windows SNMP API を `snmpapi.dll` から提供するためには、インストールする必要があります。

トラフィックを Windows SNMP サービスに転送するためには、Windows SNMP サービスの UDP ポートを再構成する必要があります([34 ページの Operations Manager と ServerView Agents との間の SNMPv3 通信](#)を参照)。

1. ファイル `C:\Windows\<Systems32>\drivers\etc\services` を開きます。
2. `snmpd` で始まる行を見つけます。
3. 値 `161/udp` を変更します(`1161/udp` など)。

4. 変更を保存します。
5. Windows SNMP サービスを再起動します。

 2つのSNMPサービスの共存については、Net-SNMPのマニュアルを参照してください。

 トラフィックをWindows SNMPサービスに転送するためには、**snmpd.conf**ファイルでプロキシコマンドを設定する必要があります(以下を参照)。


#### 4.3.3.2 Net-SNMP Service を Windows サービスとして登録する

1. Net-SNMP のインストール場所で **snmpd.exe** ファイルを見つけます。
2. コマンドラインを開きます。
3. 次のコマンドを実行します。

```
snmpd -register -Lf"C:\usr\LOG_AGENT" -I-
udp,udpTable,tcp,tcpTable,icmp,ip,interfaces,system_
mib,sysORTable
```

#### 4.3.3.3 snmpd.conf の設定

1. Windows で **snmpd.conf** ファイルを見つけます。  
**snmpd.conf** ファイルは <net-snmp installdir>\etc\snmp ディレクトリにあります。
2. **snmpd.conf** 設定ファイルを開きます。

 **snmpd.conf** パーシステントファイルの内容は、Net-SNMP マスターエージェントが停止されるたびに上書きされます。Net-SNMP マスターエージェントが実行されているときは、**snmpd.conf** パーシステントファイルを編集しないことを推奨します。

3. トラフィック転送と共通ユーザの設定を指定します。

- アクセス制御を定義します。

読み取り専用アクセスに **rouser**、または読み書きアクセスに **rwuser** を **snmpd.conf** ファイルに追加します。

```
rouser <username> secLevel:{noauth|auth|priv}
[restriction_mibtree]

rwuser <username> secLevel:{noauth|auth|priv}
[restriction_mibtree]
```

例：

- `rouser adminA auth`

上記で定義した SNMPv3 ユーザ **adminA** に、フル MIB ツリーへの読み取り専用アクセスを付与します。

- `rwuser adminA auth .1.3.6.1.4.1.231.2`

**adminA** に個々のサブツリー `1.3.6.1.4.1.231.2` への選択的読み書きアクセスを付与します。

- ユーザを作成します。



Operations Manager の中央管理用サーバと管理対象ノード上の ServerView Agents との間で SNMP バージョン 3 の通信を行うためには、通信エンドポイントで共通ユーザを設定する必要があります。

**snmpd.conf** 設定ファイルに **createUser** ステートメントを追加します。

```
createUser [-e ENGINEID] <username> [(MD5|SHA)
<authpassphrase> [DES|AES] [<privpassphrase>]]
```

例：

- **createUser adminA MD5 adminAadminA**

**adminA** というユーザを定義します。このユーザを、暗号化なしの認証済み SNMPv3 メッセージに使用できます。パスワードは **adminAadminA** で、使用するハッシュアルゴリズムは **MD5** です。

- **createUser adminP MD5 adminAadminA DES adminPadminP**

**adminP** というユーザを定義します。このユーザを認証済みで暗号化された SNMPv3 メッセージに使用できます( [11 ページの SNMPv3: 新機能](#) を参照)。認証プロセスのパスワードは **adminAadminA** で、使用するハッシュアルゴリズムは **MD5** です。暗号化手順のパスワードは **adminPadminP** で、使用するハッシュアルゴリズムは **DES** です。



認証とプライバシーに同じパスワードを使用するためには、暗号アルゴリズムの後のステートメントを省略します。



USM( [11 ページの SNMPv3: 新機能](#) を参照) は認証のないプライバシーを定義しません。



SNMPv3 パスフレーズは 8 文字以上にしてください。

- SNMPv1 通信の転送を Windows SNMP サービスに設定します。

**snmpd.conf** 設定ファイルに **proxy** ステートメントを追加します。

```
proxy -v 1 -c public localhost:1161 .1.3
```

4. Net-SNMP サービスを再起動します。



デーモンを再起動すると、**snmpd.conf** パーシステントファイルに **usmUser** エントリが作成されます。

例：

```
usmUser 1 3 0x80001f88800706b92268f4934900000000
0x61646d696e4100 0x61646d696e4100 NULL .1.3.6.1.6.3.10.1.1.2
0x60c245359704f595b1af164a411d299d .1.3.6.1.6.3.10.1.2.1 ""
""
```

基本的に、**usmUser** ステートメントには **createUser** エントリと同じ情報が含まれます。主な違いは、読み取り可能なパスワードがローカライズされたキーに置換されていることです( Net-SNMP のマニュアルを参照)。

以降は、**snmpd** デーモンは **usmUser** 情報を使用します。

#### 4.3.3.4 snmpd.conf 設定ファイルの例:

```
agentaddress udp:161
agentaddress udp6:161

com2sec public default public
com2sec6 public default public

group MyGroup v1 public
group MyGroup v2c public

view all included .1

access MyGroup "" any noauth exact all all all

rwuser testuser auth .1

createUser testuser MD5 testuser AES testuser

proxy -v 1 -c public localhost:1161 1.3

proc mountd

proc ntalkd 4
```

```
proc sendmail 10 1
```

#### 4.3.4 管理対象サーバの Linux: snmpd.conf の設定



要件：

管理対象サーバがSNMPv3を使用するように準備すること。詳細は、[17 ページの ServerView Agents での SNMPv3 の使用](#)を参照してください。

以下は、Operations Manager の中央管理用サーバと管理対象ノード上の ServerView Agents がSNMPv3 で通信できるようにする追加設定です。

1. Linux で **snmpd.conf** ファイルを見つけます。

**snmpd.conf** ファイルを見つける方法は複数あります。1 つは、Net-SNMP マスターエージェントの出力をデバッグする方法です。

- 次のパラメータで **snmpd** デーモンを呼び出します。

```
snmpd -f -Lo -Dread_config -H 2>&1 | grep "config path" | head -1
```

出力は以下ようになります。

```
config path used for
snmpd:/etc/snmp:/usr/share/snmp:/usr/lib64/snmp:/root/.snmp: (persistent path:/var/lib/net-snmp)
```

- **snmpd.conf** ファイルは **/etc/snmp** ディレクトリにあります。

2. **snmpd.conf** 設定ファイルを開きます。



**snmpd.conf** パーシステントファイルの内容は、Net-SNMP マスターエージェントが停止されるたびに上書きされます。Net-SNMP マスターエージェントが実行されているときは、**snmpd.conf** パーシステントファイルを編集しないことを推奨します。

3. 共通ユーザの設定を指定します。

- アクセス制御を定義します。

読み取り専用アクセスに **rouser**、または読み書きアクセスに **rwuser** を **snmpd.conf** ファイルに追加します。

```
rouser <username> secLevel:{noauth|auth|priv}
[restriction_mibtree]

rwuser <username> secLevel:{noauth|auth|priv}
[restriction_mibtree]
```

例：

- `rouser adminA auth`

上記で定義した SNMPv3 ユーザ **adminA** に、フル MIB ツリーへの読み取り専用アクセスを付与します。

- `rwuser adminA auth .1.3.6.1.4.1.231.2`

**adminA** に個々のサブツリー 1.3.6.1.4.1.231.2 への選択的読み書きアクセスを付与します。

- ユーザを作成します。



Operations Manager の中央管理用サーバと管理対象ノード上の ServerView Agents との間で SNMP バージョン 3 の通信を行うためには、通信エンドポイントで共通ユーザを設定する必要があります。

**snmpd.conf** 設定ファイルに **createUser** ステートメントを追加します。

```
createUser [-e ENGINEID] <username> [(MD5|SHA)
<authpassphrase> [DES|AES] [<privpassphrase>]]
```

例：

- **createUser adminA MD5 adminAadminA**

**adminA** というユーザを定義します。このユーザを、暗号化なしの認証済み SNMPv3 メッセージに使用できます。パスワードは **adminAadminA** で、使用するハッシュアルゴリズムは **MD5** です。

- **createUser adminP MD5 adminAadminA DES adminPadminP**

**adminP** というユーザを定義します。このユーザを認証済みで暗号化された SNMPv3 メッセージに使用できます( [11 ページの SNMPv3: 新機能](#) を参照)。認証プロセスのパスワードは **adminAadminA** で、使用するハッシュアルゴリズムは **MD5** です。暗号化手順のパスワードは **adminPadminP** で、使用するハッシュアルゴリズムは **DES** です。



認証とプライバシーに同じパスワードを使用するためには、暗号アルゴリズムの後のステートメントを省略します。



USM( [11 ページの SNMPv3: 新機能](#) を参照) は認証のないプライバシーを定義しません。



SNMPv3 パスフレーズは 8 文字以上にしてください。

#### 4. Net-SNMP サービスを再起動します。

デーモンを再起動すると、**snmpd.conf** パーシステントファイルに **usmUser** エントリが作成されます。

例：

```
usmUser 1 3 0x80001f88800706b92268f4934900000000
0x61646d696e4100 0x61646d696e4100 NULL .1.3.6.1.6.3.10.1.1.2
0x60c245359704f595b1af164a411d299d .1.3.6.1.6.3.10.1.2.1 ""
""
```

基本的に、**usmUser** ステートメントには **createUser** エントリと同じ情報が含まれます。主な違いは、読み取り可能なパスワードがローカライズされたキーに置換されていることです( **Net-SNMP** のマニュアルを参照)。

以降は、**snmpd** デーモンは **usmUser** 情報を使用します。

#### 4.3.4.1 **snmpd.conf** 設定ファイルの例：

```
agentaddress udp:161
agentaddress udp6:161

com2sec public default public
com2sec6 public default public

group MyGroup v1 public
group MyGroup v2c public

view all included .1

access MyGroup "" any noauth exact all all all

rwuser testuser auth .1

createUser testuser MD5 testuser AES testuser

proc mountd

proc ntalkd 4

proc sendmail 10 1
```

## 4.4 Net-SNMP 実装とテスト手順

この章では、Windows ディストリビューションに含まれる SNMP サービスおよび SNMP トラップと、オープンソースコミュニティが作成し、Windows と Linux システムの両方に使用できる Net-SNMP パッケージという、SNMP ツールの 2 つの実装を説明します。

Windows SNMP サービスは、SNMP プロトコルバージョン 1 と 2 をサポートし、次の 3 つの主要部分で構成されます。

- SNMP クエリの応答サービスと、他のステーションへのトラップの送信 (SNMP サービス)
- 外部トラップからの取得サービス (SNMP トラップ)
- ダイナミックリンクライブラリの形式の、サービスへの API (snmpapi.dll)

ServerView ソフトウェアと Windows SNMP の連携により、Fujitsu 固有の部分によって API を使用して SNMP エージェントがサービスを提供する情報量を増加し (ServerView Agents)、収集されたトラップを取得します (Operations Manager)。SNMP サービスはクエリの作成 (Operations Manager による) には使用されないため、同期監視にはサービスの有効化は必須ではありません。

Net-SNMP は、Windows サービスの同等機能である snmpd (SNMP エージェント) と snmpttrapd (SNMP トラップレシーバ) を含むパッケージです。さらに、Net-SNMP には SNMP インフラストラクチャの診断に使用できる一連のツールも含まれています。Net-SNMP の最大の利点は、SNMPv3 をサポートすることです。

### Windows

- 両方のツールをインストールできますが、制限事項が 1 つあります。標準 SNMP ポート (エージェントは 161、トラップレシーバは 162) を待機できるのは、1 つのエージェントプロセスと 1 つのトラップレシーバだけです。たとえば、Net-SNMP サービスを標準ポートで使用する場合、Windows SNMP を別のポートを使用するように再設定する必要があります。Windows SNMP で使用するポート番号を大きくする方法は、[55 ページの Net-SNMP Service を Windows サービスとして登録する](#)を参照してください。

### Linux

- 大半の Linux ディストリビューションには Net-SNMP パッケージが搭載され、SNMP サポートが必要な場合に通常最初に選択されます。

### 4.4.1 Windows SNMP サービスの設定

Windows SNMP の設定は、サービス管理画面 (services.msc) で実行できます。

ServerView ソフトウェアと連携している場合、以下に示すように、監視システム (「エージェント」タブの「連絡先」と「場所」、取得するデータの範囲 (「エージェント」タブの「サービス」) に表示された ID データを確認できます。

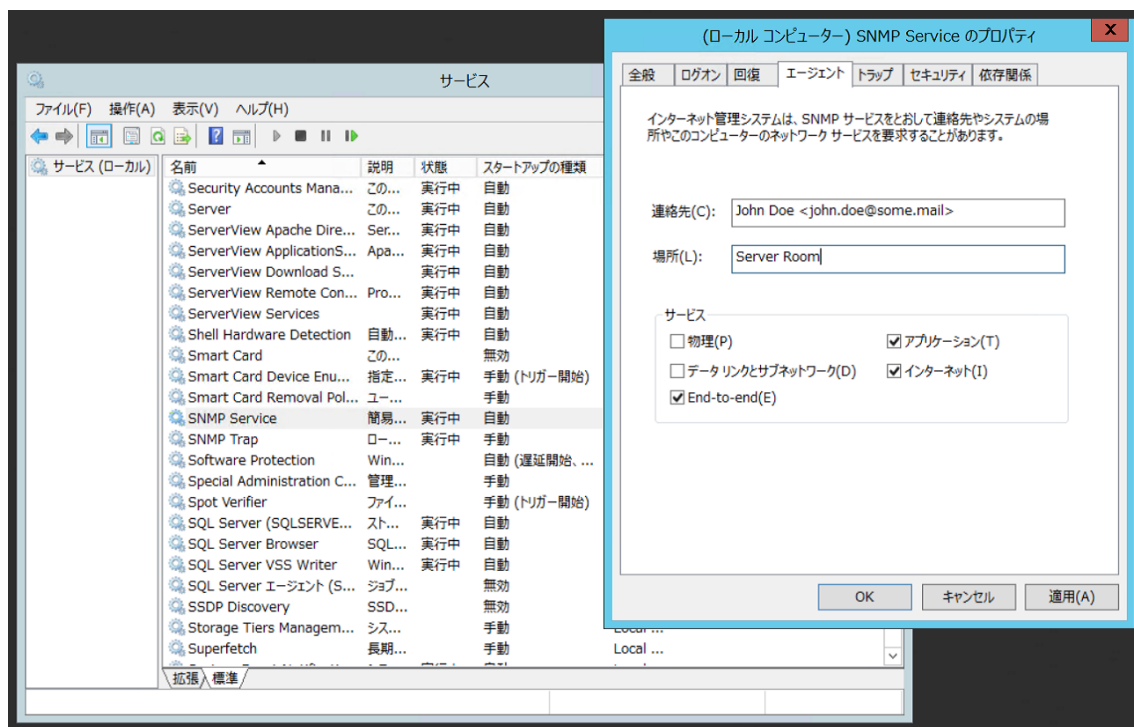


図 5: 「(ローカルコンピュータ) SNMP Service のプロパティ」ウィンドウ

別の設定オプションとして、マシンから生成されたトラップの送信先があります。システム内で発生したイベントに関する情報が送信される、多数の送信先(ネットワークアドレス)を定義できます。ここで最も一般的なシナリオは、システムからトラップを受信するすべての Operations Manager インスタンス(IP)のリストを指定することです。

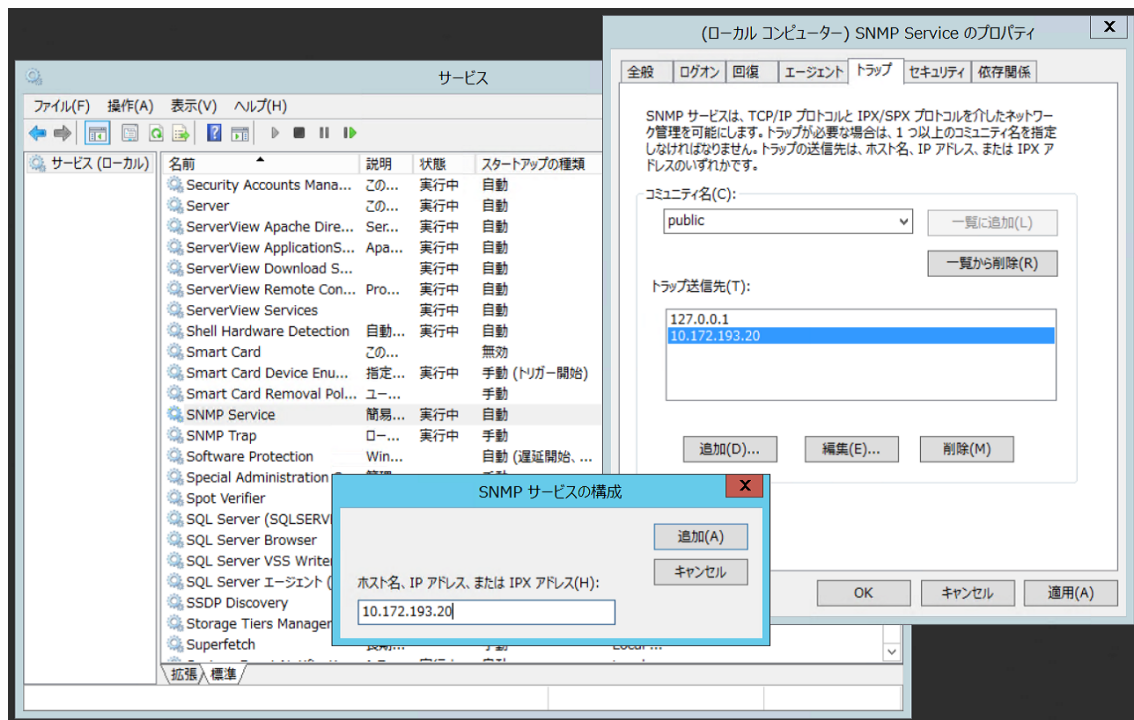




図 6: 「SNMP サービスの構成」画面

-  ホストの Operations Manager の「接続テスト」「テストトラップ」の機能を動作させるには、「トラップ送信先」リストで Operations Manager IP を設定しておく必要があります。
-  SNMP サービスを再起動すると、トラップ「Agent cold start/Station reinitialized」が送信されます。ホストと任意の Operations Manager インスタンス間で、トラップ通信のテストに簡単に使用できます。

SNMP サービスの最も重要な部分は、どのホストがエージェントにクエリでき、どのコミュニティ文字列を受理するかを決定することです(「セキュリティ」タブ)。通常は、「読み取り」以上の権限のコミュニティ「public」を使用して、ServerView Manager IP を受理されたホストとして設定(または「すべてのホストから SNMP パケットを受け付ける」を設定)する必要があります(サーバーの識別 LED のオン/オフを切り替える場合などは、「読み書き」権限が必要です)。

Net-SNMP 設定に直接表示される一部の設定オプションの設定には、注意が必要です。たとえば、Windows SNMP サービスで待機するポートを変更するには、[55 ページの Net-SNMP Service を Windows サービスとして登録する](#)の章で示すように、必要なポート番号をファイル C:\Windows\<Systems32>\drivers\etc\services で設定する方法しかありません。

## 4.4.2 Net-SNMP サービスの基本設定

Net-SNMP の設定はテキストファイルに保存され、必要に応じて、最適化やセキュリティの目的で変換され、他のフォルダにコピーされます。設定の主な場所は、Windows の場合はフォルダ C:\usr\etc\snmp、多くの Linux ディストリビューションの場合は 2 つのフォルダ /etc/snmp と /usr/share/snmp です。本書では、3 つのファイルの内容を検討します。

snmp.conf	すべての SNMP アプリケーションの設定
snmpd.conf	SNMP エージェントの設定 ( snmpd)
snmptrapd.conf	SNMP トラップリスナーの設定 ( snmptrapd)

該当するサービスの起動または再起動が成功すると、ファイルが変換され、/usr/snmp/persist( Windows) または /var/lib/net-snmp( Linux) にコピーされます。これらの場所のファイルは、特に目的がない限り、直接編集してはいけません。

### 4.4.2.1 エージェント( snmpd)

SNMP エージェント( snmpd.conf) の最小動作設定は、どのネットワーク接続が受理され ( 1)、SNMP ツリーのどの部分がクライアントからアクセス可能で ( 2)、データを取得するためにどのパラメータをクライアントが使用する必要があるか ( 3) を指定します。

1. agentAddress は、待機に使用するアドレスとポートのペアを定義します。代表的な設定は以下のとおりです。

```
agentAddr udp:161
```

エージェントは、任意のインターフェースに接続したすべてのクライアントに回答し、ポート 161/udp にリクエストを送信することを示します。



ファイアウォール設定に注意してください。agentAddress ディレクティブに使用された udp ポートを、選択したネットワークからの受信接続に対して開いておく必要があります。

2. アクセス可能なツリーの名前付きルートを定義しておくと便利です。ツリー全体は、ディレクティブで「all」などと定義できます。

```
view all included .1
```

ビューへのアクセスは、クライアントパラメータ/ID との関係で定義されます。次のような、さまざまな方法で実行できます。

```
authcommunity read public default -V all
```

任意のネットワーク( "default") から送信された「コミュニティクライアント」( v1 および v2c クライアント、コミュニティ「public」を使用) を指し、ツリー全体のデータ( "-V all") を読み取れます( "read") 。

3. SNMPv3 クライアントを設定するには、どの程度のセキュリティが必要かをまず検討する





必要があります。レベル名は、noAuth、authNoPriv、authPriv で、名前から機能がわかります。noAuth では、少なくとも 1 つのユーザ名を定義する必要があります。authNoPriv では、少なくとも 1 つのユーザ名と、認証プロトコルとパスワードを定義する必要があります。authPriv では、少なくとも 1 つのユーザ名と、認証プロトコルと認証パスワードと、プライバシープロトコルとプライバシーのパスワードを定義する必要があります。

```
createUser someUser1
createUser someUser2 MD5 "Password2"
createUser someUser3 MD5 "Password3" DES "OtherPassword3"
```

ユーザを作成してセキュリティのレベルを決定した後、次のように、読み取り/読み書き権限を割り当てます。

```
rouser someUser2 authNoPriv -V all
```

 MD5 ハッシュを使用せずに、SHA を使用してセキュリティを強化できます。同様に、DES プロトコルの代わりに強力な AES を使用できます。プロトコルには、クライアントから対応するプロトコルを使用する必要があることに注意してください。

 snmpd.conf ファイルにプレーンテキストでパスワードを残さないようにするには、再設定したサービスを初めて起動した後に、createUser ディレクティブで行を削除します。暗号化されたパスワードは、フォルダ /usr/snmp/persist( Windows) または /var/lib/net-snmp( Linux) の "シャドウ" snmpd.conf II に保存されます。

まとめると、エージェントデータの設定を検討して、クライアントがホストと連絡先担当者を識別できるようにすることが重要です。ディレクティブを次のように設定できます。

```
sysName someHostName
sysDescr Some words about the system
sysLocation Where we can physically find the host
sysContact The administrator <some@mail.domain>
```

Net-SNMP エージェントは、多数のトラップリスナーのトラップ送信元としても機能できます。ハードウェアまたはソフトウェアから生成された場合、snmd はトラップを設定にリストされたすべての送信先に送信します。2 つの独立したディレクティブで、トラップ送信先として v1 トラップ (trapsink) と v3 トラップ (trapsess) を個別に設定します。場合によっては、snmd が、該当するパラメータを使ったバイナリ snmptrap の実行と同等の機能を実行することがあります。設定で、トラップリスナーのアドレスと SNMP セッションのパラメータを定義する必要があります。v1 トラップの送信は、以下の形式のディレクティブで有効になります。

```
trapsink someHost1 public
trapsink someHost:1162 private
```

v3 トラップを使用するには、snmpd.conf ファイルを別のディレクティブに追加します(他のオプションについては、[67 ページの SNMP クライアントのシミュレーション](#)および [68 ページのテストトラップの送信と到着の確認](#)を参照)。

```
trapsess -l authPriv -u someUser3 -a MD5 -A "Password3" -x DES -X "OtherPassword3"
someHost3:1162
```



暗号化されていないパスワードが一般に読み取れる設定に保存されないようにするには、createUser ディレクティブでユーザを作成し、trapsess でオプション(-a -A -x -X)を使用せずにユーザ(-u userName)を作成し、サービスが正常に起動したら、元の snmpd.conf ファイルから createUser 行を削除します。

#### 4.4.2.2 トラップリスナー( snmptrapd)

SNMPトラップリスナーの基本設定( snmptrapd.conf) は、エージェントの設定と類似のパラメータを定義します。snmpTrapdAddr ディレクティブは agentAddress と同等で、トラップ上の待機には一般にポート 162/udp を使用します。指定されたコミュニティのトラップを制限するには、以下の形式で authCommunity ディレクティブを使用できます。

```
authCommunity log,execute,net public
```

"public" は他のコミュニティに置換できます。SNMP v3トラップを使用する場合、セキュリティレベルと、必要に応じて認証およびプライバシーパラメータも定義します。

```
createUser someUser3 MD5 "Password3" DES "OtherPassword3"
authUser log,execute,net someUser3
```

認証のないトラップも取得するには、上記の代わりに以下を使用します。

```
authUser log,execute,net someUser3 noAuth
```

プレーンテキストのパスワードを設定ファイルに保存しないようにする方法は、前章の説明と同じです。

### 4.4.3 SNMP 環境のテスト

Operations Manager は、リモートシステムを直接監視する機能をサポートしていません。エージェントからデータを取得するので、監視対象のホストに追加のソフトウェアがインストールされます。データは Operations Manager や、その他の監視プロトコルのクライアントと同一です。SNMP の場合、データを Operations Manager だけでなく、よりシンプルなツールからも収集できます。

#### 4.4.3.1 SNMP クライアントのシミュレーション

Net-SNMP パッケージには、SNMP 設定のテストに使用できる、便利なツールセットが付属しています。SNMP エージェントにクエリするには、通常は `snmpget` または `snmpwalk` ツールを実行します。最初のツールは 1 つの SNMP 変数を調査し、2 つ目は指定されたツールからサブツリーを再帰的に調べます。



ツールは Linux システムの `/usr/bin` フォルダにあるので、シェルから直接使用できます。Windows の場合は `C:\usr\bin` にあり、フルパスを使用するか、フォルダを環境変数 `PATH` に手動で追加して実行できます。



`snmpwalk` で `.1` などの非常に短いルートを使用すると、`.1` で始まる OID で各 SNMP 変数の値を取得できる保証がないことに注意してください。サブツリーはループ内の次の値を取得する場合、一定する必要はありません。

ツールの使用方法はシンプルです。パラメータで使用する必要があるバージョンのプロトコル、必要に応じてコミュニティまたはユーザ、パスワードとプロトコル、クエリされるエージェントのアドレス(標準以外のポートを使用する場合は、該当するポートに続けてコロン)、OID(1 つまたは複数)を指定します。

v1 でのツールの使用例を以下に示します。

```
snmpget -v1 -c public someHost1 .1.3.6.1.2.1.1.5.0
.1.3.6.1.2.1.1.1.0
```

```
snmpwalk -v1 -c public someHost1:1161 .1
```

v3 の使用はもう少し複雑です。

```
snmpwalk -v3 -l authPriv -u someUser3 -a MD5 -A "Password3" -x
DES -X "OtherPassword3" someHost3 .1.3.6.1.2.1.1
```

### 4.4.3.2 テストトラップの送信と到着の確認

snmptrap コマンドを使用して、明示的に定義されたトラップを送信できます。

```
snmptrap -v 1 -c public someHost1 .1.3.6.1.6.3.1.1.5.1.0 "" 0 0 ""
```

someHost1 トラップリスナーを、1 つの *coldStart* トラップに送信します。最初の空文字列 ("" ) は、送信先のエージェント名 ( デフォルトではホスト名と同一 ) を示し、2 つ目は現在のタイムスタンプ ( 空文字列は「現在」を示す ) を示します。

v3 の snmptrap の構文は以下のように、違いがあります。

```
snmptrap -v3 -l authPriv -u someUser3 -a MD5 -A "Password3" -x DES -X "OtherPassword3" someHost1 "" .1.3.6.1.6.3.1.1.5.1.0
```

上記の例の空文字列は、現在のタイムスタンプをデコードします。

低レベルの診断ツール ( tcpdump、Wireshark ) を使用して、トラップの到着をテストできます。しかし暗号化を使用する場合、検出できるのは、一部のネットワークデータが送信先に到着したことだけです。データを分析するには、データを復号する必要があります。最も簡単な方法は、traphandle ディレクティブを snmptrapd.conf に追加することです ( ただし、Net-SNMP でのみ可能 ) 。一部のトラップが到着したとき、アプリケーションを呼び出すことができます。最もシンプルな設定の例を以下に示します。

```
traphandle default path-to-application
```

"default" は「任意のトラップ」を示します。トラップで実行されたアプリケーションは、標準入力にトラップコンテンツを受け取ります。メカニズムの代表的な使用法は、以下のコードを含む、実行可能シェルスクリプトの作成です。

```
#!/bin/bash
date >> /tmp/trapdump.log
cat >> /tmp/trapdump.log
```

Windows では、対応するスクリプトは以下ようになります。

```
@date /t >> C:\trapdump.log
@more >> C:\trapdump.log
```

traphandle でスクリプトを使用すると、トラップリスナーに到着したトラップを、可読形式で表示できます。

## 4.5 アイテムの操作

### 4.5.1 SNMPv3 を有効にしたサーバでブラウズ操作が失敗する

CMS で SNMPv3 が有効にされたサーバをブラウズしようとする、サブネットに数台の ( SNMPv3 が有効な ) サーバしかない場合、ブラウズがタイムアウトすることがあります。

SNMPv3 ホストをサーバリストに追加することを推奨します。

推奨します。

このホスト構成で自動ブラウズが必要な場合、以下の手順を実行してください。

- \* CMS で SNMPv3 を無効にする
- \* SNMPv3 ホストが SNMPv1 でも通信することを確認する
- \* サブネットを参照する
- \* サーバリストに必要なすべてのサーバを追加する
- \* CMS で SNMPv3 を有効にする
- \* 必要に応じてサーバで SNMPv1 を無効にする

## 4.5.2 Operations Manager での CMS の可視性

Operations Manager で CMS を自動で表示するためには、CMS で SNMP サービスを正しく構成する必要があります。

### Windows

1. 「サービス」に移動します。
2. SNMP サービスのプロパティで「セキュリティ」タブに移動します。
3. 「受け付けるコミュニティ名」で、「追加」ボタンをクリックして「Public」を挿入します。

### Linux

1. `snmpd.conf` ファイルで、次の行 `rwcommunity public default` を追加します。
2. これらの変更を行ったら、すぐに SNMP サービスを再起動します。

## 5 iRMC での SNMPv3 の使用

**i** SNMPv3 は、ユーザ固有の総合的なセキュリティコンセプトおよびセキュリティ管理計画の一部として実装する必要があります。

本書で説明する手順とメカニズムは、単独では総合的な保護には不十分です。全体的なセキュリティコンセプトに合わせて統合する必要があります。

**i** iRMC S4 は、ファームウェア V7.8 以上で SNMPv3 サービスを提供します (SNMPv3 サービスのみ、SNMPv3 トラップなし)。

### 5.1 アーキテクチャと要件

#### 5.1.1 iRMC のアーキテクチャ

##### 5.1.1.1 リモートマネジメントコントローラ - iRMC S4

iRMC (integrated Remote Management Controller) は、統合された LAN 接続と拡張機能を持つ BMC です。このように、iRMC S4 は PRIMERGY サーバをシステムの状態に関係なく包括的に制御する機能を提供します。特に、iRMC S4 では、PRIMERGY サーバの Out-Of-Band 管理 (Lights Out Management - LOM) が可能です。Out-Of-Band 管理では、サーバの電源がオンになっているかどうかに関係なくシステム管理者がリモート制御を使用してサーバを監視および管理できるようにする専用の管理チャネルを使用します。

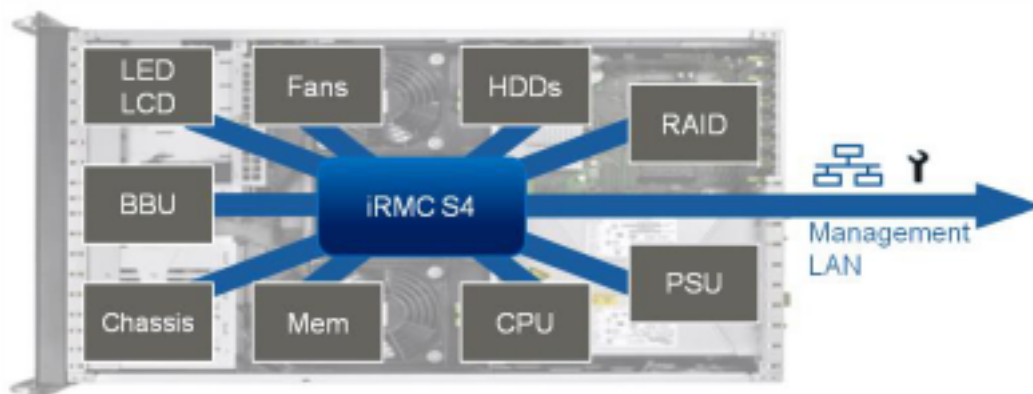


図 7: iRMC S4 のアーキテクチャ

### 5.1.1.2 ServerView Integration

ServerView Agents は、iRMC S4 を検出し、関連するサーバに自動的に割り当てます。これは、Operations Manager から直接 ServerView Remote Management Frontend を使用して iRMC S4 Web インターフェースおよびテキストコンソールリダイレクションを開始することが可能なことを意味します。

Operations Manager は、iRMC S4 の SNMP スタックを使用して主要なすべての内部サブシステムを監視します。

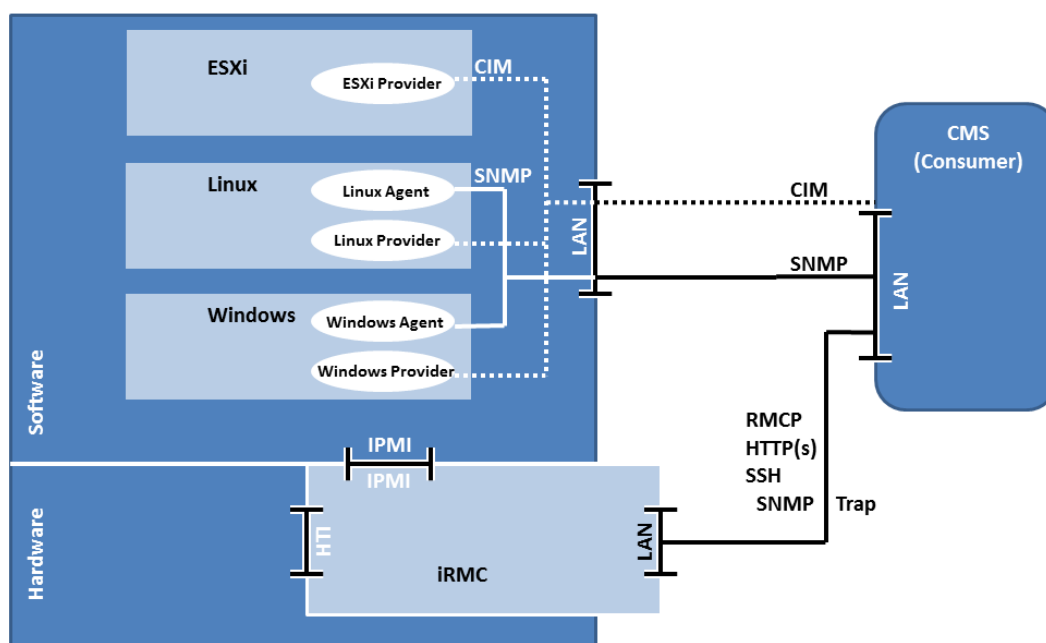


図 8: ServerView のアーキテクチャ

### 5.1.1.3 ServerView Agentless Service を使用したエージェントレスモード

ServerView Agentless Service を使用するエージェントレスモードでは、サーバは管理対象サーバの iRMC S4 のみで管理されます。ServerView Agentless Service と iRMC S4 との間の通信は、HTI (High Speed Transfer Interface) を通じて行われます。SNMP は、管理対象サーバ上ではなく、iRMC S4 上で実行されます。

Operations Manager などのコンシューマは、専用の管理 LAN ポート経由でのみ iRMC S4 と通信します。

マザーボード、メモリモジュール、電源、特定の RAID などの複数のシステムコンポーネントに関する情報と同様に、Agentless Service を使用するエージェントレスモードの ServerView エージェントレス管理は、OS イベントログを含む PrimeCollect データなどのオペレーティングシステムベースの情報を提供します。

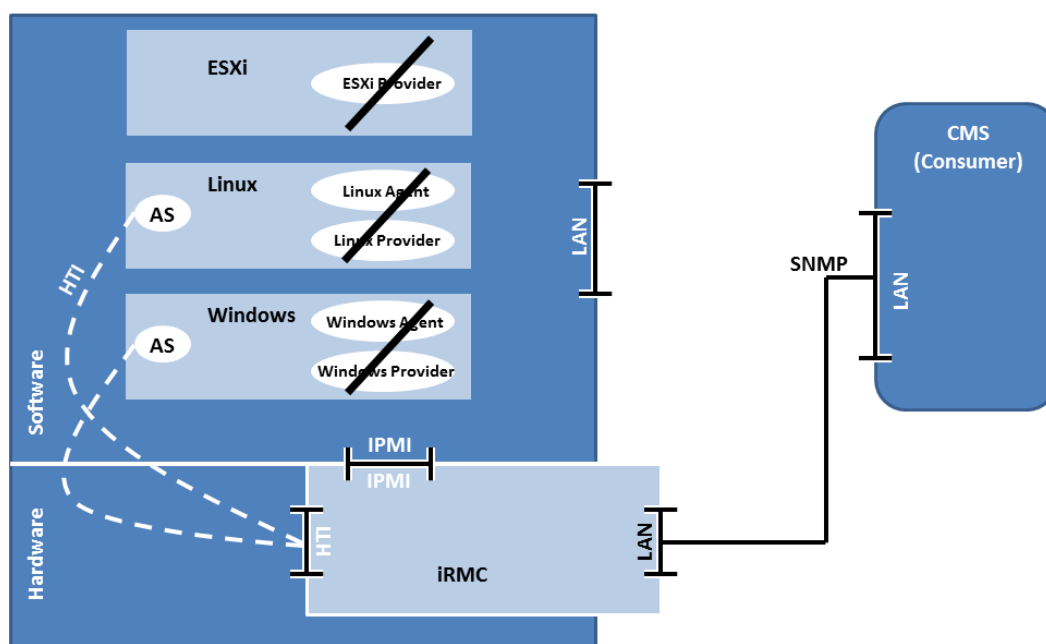


図 9: ServerView Agentless Service を使用したエージェントレスモードのアーキテクチャ

#### 5.1.1.4 iRMC S4 上の SNMP サービス

デフォルトで、SNMP サービスは iRMC S4 では無効になっています。

iRMC S4 の SNMP サービスは、以下の SNMP MIB での GET 要求をサポートします。

- SNMP STATUS.MIB
- SNMP OS.MIB
- SNMP SC2.MIB
- SNMP MIB-2.MIB

SNMP サービスが有効な場合、これらの MIB によって提供される情報を SNMP マネージャを実行中のシステムで使用できます。



### 5.1.1.5 iRMC S4 上のユーザ権限

iRMC S4 は以下の 2 つの相互補完的なユーザ権限を区別します。

- チャンネル固有の特権
- iRMC S4 独自の機能によるアクセス許可

iRMC S4 はチャンネル固有を基本にして許可を割り当てるので、ユーザが iRMC S4 に LAN インターフェースを経由して接続したか、シリアルインターフェースを経由して接続したかにより、ユーザの権限は異なります。

LAN チャンネルまたはシリアルモデムチャンネルは、セッションベースのチャンネルです。セッションのコンセプトは、ユーザ認証のコンセプトです。

## 5.1.2 技術的要件

### リモートワークステーション

- ブラウザ:

ブラウザ	バージョン	エンジン	注意事項
Firefox	4x.x	Gekoa/ Mozilla	
Internet Explorer	11	Trident MS Edge 1.0	EdgeHTMLNo Browser Helper Objects (1)
Chrome	4x.x	Blink	

- コンソールリダイレクションの場合:

Sun Java Virtual Machine バージョン 1.6 以降

### ネットワーク内

- ネットワークに DHCP サーバが必要です。
- IP アドレスの代わりに具体的な名前を使用して iRMC Web インターフェースにログインする場合、ネットワークの DHCP サーバを動的 DNS に設定する必要があります。
- DNS を設定する必要があります。設定しない場合は、IP アドレスを要求する必要があります。

## 5.2 「iRMC S4 ユーザ情報」ページの SNMPv3

「iRMC S4 ユーザ情報」ページには、設定されたすべてのユーザが表に示されています。各行には、設定された1名のユーザのデータが表示されます。ユーザ名はリンク形式で実装されています。ユーザ名をクリックすると「ユーザ“<name>”構成」画面が開き(77ページの[SNMPv3のユーザ固有の設定の指定](#)を参照)、そのユーザの構成を表示したり変更したりすることができます。

「iRMC S4 ユーザ情報」ページを開くには

1. iRMC S4 Web インターフェースのナビゲーションツリーで、「ネットワーク設定」-「SNMP」の順に選択します。

「iRMC S4 ユーザ情報」ページが表示されます。



図 10: 「iRMC S4 ユーザ情報」ウィンドウ

このページには、「SNMPv3 有効」という列があります。この列は、SNMP がグローバルで無効にされていても表示されます(75ページの[SNMP バージョンの設定](#)を参照)。

## 5.3 処理の概要



iRMC S4 は、ファームウェア V7.8 以上で SNMPv3 サービスを提供します( SNMPv3 サービスのみ、SNMPv3トラップなし)。

デフォルトで、SNMP サービスは iRMC S4 では無効になっています。

SNMP サービスの有効化は2段階で設定します。

1. 「ネットワーク設定」で SNMP バージョンを設定します。
2. 「iRMC S4 ユーザ情報」設定 ページで SNMPv3 のユーザ固有の設定を指定します。

### 5.3.1 SNMP バージョンの設定

デフォルトで、SNMP サービスは iRMC S4 では無効になっています。

iRMC S4 の SNMP サービスは、以下の SNMP MIB での GET 要求をサポートします。

- SNMP STATUS.MIB
- SNMP OS.MIB
- SNMP SC2.MIB
- SNMP MIB-2.MIB

SNMP サービスが有効な場合、これらの MIB によって提供される情報を SNMP マネージャを実行中のシステムで使用できます。

手順:

1. iRMC S4 Web インターフェースのナビゲーションツリーで、「ネットワーク設定」-「SNMP」の順に選択します。  
「SNMP 一般構成」ページが表示されます。
2. このページで目的のパラメータを設定します。



SNMPv3 は、SNMPv1 や SNMPv2c にはないセキュリティ機能を定義します。  
設定「全プロトコルサポート (SNMPv1/v2c/v3)」では、システム全体は最も弱いプロトコルバージョンに合わせたセキュリティになります。



SNMPv3 は、ユーザ固有の総合的なセキュリティコンセプトおよびセキュリティ管理計画の一部として実装する必要があります。

本書で説明する手順とメカニズムは、単独では総合的な保護には不十分です。全体的なセキュリティコンセプトに合わせて統合する必要があります。

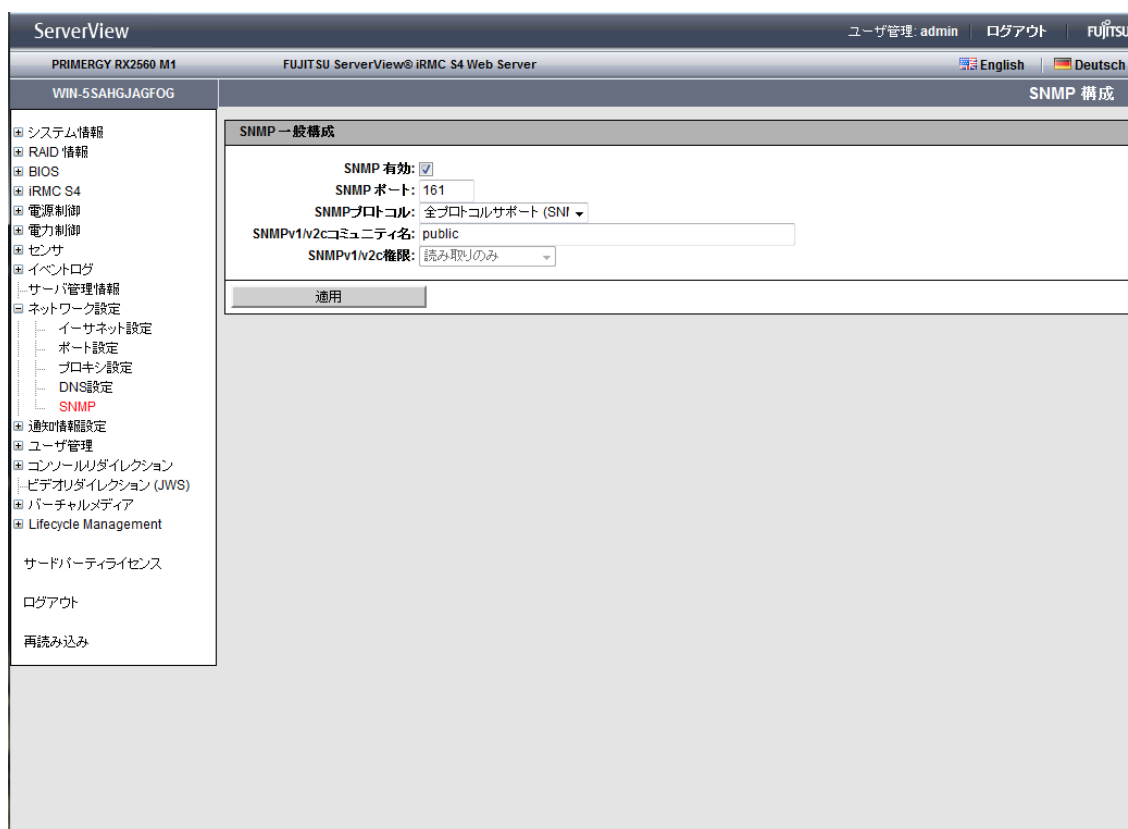


図 11: 「SNMP 一般構成」ページ

- **SNMP 有効**

iRMC S4 で SNMP サービスを有効にします( デフォルト: 無効)。

- **SNMP ポート**

SNMP サービスが待機しているポート( 通常は UDP 161)。

- **SNMP プロトコル**

使用する SNMP プロトコルバージョン

- **全て(SNMPv1/v2c/v3)**

SNMP サービスをすべての SNMP プロトコルバージョン( SNMP v1/v2c/v3) で使用できます。

- **SNMPv3 のみ**

SNMPv3 のみ使用できます。

- **「SNMPv1/v2c コミュニティ名」および「SNMPv1/v2c 権限」**

この 2 つのオプションは、SNMP プロトコルに「全プロトコルサポート

( SNMPv1/v2c/v3)」が選択されている場合にのみ表示されます( 詳細は『Remote Management. iRMC S4 - integrated Remote Management Controller』マニュアルを参照)。

3. 「適用」ボタンをクリックして、設定を保存してください。

iRMC S4 のユーザ管理のコンセプトに従って( 70 ページの iRMC のアーキテクチャを参照)、SNMPv3 のユーザ固有の設定を「iRMC S4 ユーザ情報」設定ページで指定します( 77 ページの SNMPv3 のユーザ固有の設定の指定を参照)。

## 5.3.2 SNMPv3 のユーザ固有の設定の指定

iRMC S4 ではチャンネル固有で権限が割り当てられるので、ユーザには異なる権限が付与されることがあります。

SNMP ユーザ構成は、IPMI ユーザ構成に追加して実装されます。このため、IPMI が有効で SNMP が有効、いずれかが有効でいずれかが無効、または両方とも無効という構成がユーザに指定されます。

「iRMC S4 ユーザ情報」で定義されたユーザ名とパスワードが、IPMI と SNMP の両方に適用されます。

手順：

1. iRMC S4 Web インターフェースのナビゲーションツリーで、「ユーザ管理」-「iRMC S4 ユーザ情報」の順に選択します。

「ユーザ'xx' 構成」ページが表示されます。

ServerView

PRIMERGY RX2560 M1 FUJITSU ServerView® iRMC S4 Web Server

WIN-5SAHGJAGFOG

ユーザ管理: admin ログアウト

English Deutsch

新規ユーザの構成

新規ユーザの構成

名前: user5

パスワード: .....

確認用パスワード: .....

ユーザの説明: NewUser Description

IPMI設定

IPMIユーザ有効: ☒

LANアクセス権限: ユーザ管理

シリアルアクセス権限: ユーザ管理

ユーザアカウント変更権限: ☐

iRMC S4設定変更権限: ☐

AVR使用権限: ☐

リモートストレージ使用権限: ☐

使用シェル(Textアクセス): Remote Manager

SNMPv3構成

SNMPv3有効: ☐

アクセス権: 読み取りのみ

認証: SHA

暗号化: AES

適用 キャンセル

① 注: SNMPv3ユーザを作成/変更するときは、ネットワーク設定 -> SNMPにてSNMPを有効にする必要があります。  
② 注: SNMPv3を使用するときは最低8文字のパスワードを設定する必要があります！

図 12: 「ユーザ'xx' 構成」ページ

SNMP を構成するには、「iRMC S4 ユーザ情報」と「SNMPv3 構成」の2つのグループが重要です。

## 2. iRMC S4 ユーザ情報

SNMPv3 には認証とプライバシーにパスワードが必要です。パスワードはここと「iRMC S4 ユーザ情報」で設定できます。



ユーザに SNMPv3 を有効にするためには、8 文字以上のパスワードが必要です。

## 3. SNMPv3 構成



「SNMP 一般構成」ページで「SNMP 有効」オプションが無効な場合 (75 ページの SNMP バージョンの設定を参照) は、「SNMPv3 構成」のパラメータが無効です (グレー表示)。

### • SNMP 有効

ユーザに対して SNMPv3 サポートを有効にします (デフォルト: 無効)。

### • アクセス権

ユーザのアクセス権限現在、「読み取りのみ」があらかじめ設定されています (デフォルト: 「読み取りのみ」、グレー表示)。

### • 認証



サポートされる認証/プライバシー設定の詳細は、79 ページのサポートされる認証/プライバシー設定を参照してください。

SNMPv3 が認証に使用する認証プロトコルを選択します (デフォルト: SHA)。

#### • SHA

セキュアハッシュアルゴリズム (SHA) が認証に使用されます。

#### • MD5

メッセージダイジェストアルゴリズム 5 (MD5) が認証に使用されます。

### • プライバシー

SNMPv3 が SNMPv3 トラフィックの暗号化に使用するプライバシープロトコルを選択します (デフォルト: AES)。

#### • DES

SNMPv3 トラフィックの暗号化にデジタル暗号化標準が使用されます。

#### • AES

Advanced Encryption Standard( AES) 128ビット 暗号化を SNMPv3トラフィックの暗号化に使用します。

- 「適用」ボタンをクリックして、設定を保存してください。

#### 5.3.2.1 サポートされる認証/プライバシー設定

認証プロトコル	プライバシープロトコル	サポート
なし	なし	今後サポート予定
なし	AES	非サポート
なし	DES	非サポート
MD5	なし	今後サポート予定
MD5	AES	サポート
MD5	DES	サポート
SHA	なし	今後サポート予定
SHA	AES	サポート
SHA	DES	サポート