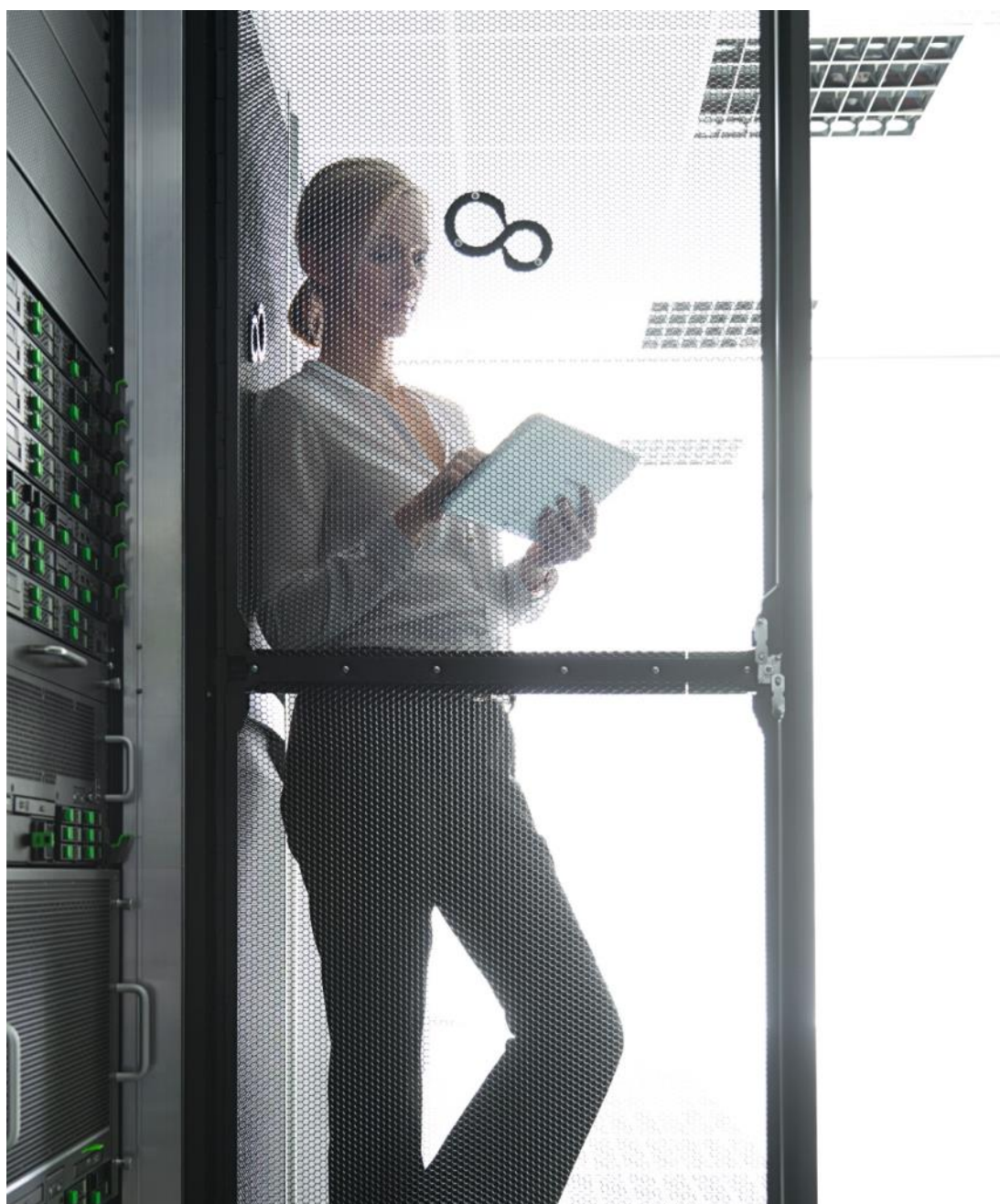


# ホワイトペーパー セキュアな PRIMERGY サーバ管理 エンタープライズセキュリティ

セキュアな高可用性プラットフォームのための PRIMERGY サーバ管理



## 目次

1.	はじめに	5
2.	「セキュリティ管理はプロセスである」	5
2.1.	セキュリティコンセプトの確立	5
2.2.	継続的な調整の必要性	6
3.	一般的な問題	8
3.1.	通信パス	8
3.1.1.	iRMC ファミリで使用されるネットワークポート	17
3.2.	ファイアウォールによる保護	18
3.3.	開いているポート	18
3.4.	管理 LAN の分離	19
3.5.	SSL 証明書の管理	20
3.5.1.	ServerView の証明書	20
3.5.2.	証明書のフィンガープリント	21
3.6.	ディレクトリサービスへのアクセス	22
3.7.	ブラウザの設定	23
3.7.1.	Cookie	23
3.7.2.	スクリプト	23
3.7.3.	証明書の管理	23
3.8.	セキュアブート	25
4.	PRIMERGY サーバの設定、インストール、およびデプロイメント	26
4.1.	RAID Manager	26
4.2.	Installation Manager を使用したリモートインストール	27
4.2.1.	デプロイメントコンポーネントのインストール	28
4.2.2.	Installation Manager によるリファレンスインストール	28
5.	ユーザ管理	30
5.1.	中央認証サービスとシングルサインオン	30
5.2.	統合ロールベースのアクセス制御 (URBAC)	30
5.2.1.	ユーザ、ユーザ役割、権限	30
5.2.2.	ユーザ役割の割り当て	31
6.	管理対象サーバ上の ServerView Agents と CIM Provider	32
6.1.	SNMP サービス	32
6.1.1.	SNMP v3	33
6.1.2.	MMB と CPU ブレード間の通信	33
6.2.	ServerView Agents	34
6.3.	IPSec を使用した SNMP メッセージのセキュリティ保護	34
6.4.	ServerView CIM Provider	35
6.4.1.	ServerView ESXi CIM Provider	35
6.4.2.	Windows 用 ServerView CIM Provider	35
6.4.3.	Linux 用 ServerView CIM Provider	35
6.5.	ServerView Connector Service	36
6.6.	ServerView System Monitor	36
7.	管理 (Operations Manager)	37

7.1.	SNMP サービス	37
7.2.	Operations Manager 環境への Web サーバのインストール	37
7.3.	Operations Manager の SSL 証明書の交換	38
7.4.	Operations Manager 向け TLS/SSL 暗号スイートの制限	38
7.4.1.	BEAST 攻撃に対抗する暗号スイート設定	41
7.4.2.	Operations Manager バージョン 8.00 以降のセキュリティ設定	41
7.4.3.	Operations Manager バージョン 9.00 以降のセキュリティ設定	42
7.5.	ユーザ認証を使用する 設定操作	42
7.6.	Event Manager とアンチウイルスプログラム	43
7.7.	変更可能な SNMP ポート	43
8.	メンテナンス	45
8.1.	アップデート管理	45
8.2.	PrimeCollect	47
8.3.	リポジトリサーバ	48
9.	Out-of-band 管理用 SNMP エージェント	49
9.1.	iRMC	49
9.2.	マネジメントブレード	49
10.	特別な設定	51
10.1.	DMZ (Demilitarized Zone) のサーバを管理するためのオプション	51
11.	まとめ	52
12.	ログファイル	55
13.	ServerView のデフォルトの証明書	56
13.1.	マネジメントコントローラ/マネジメントブレード	56
13.1.1.	ルート CA	56
13.1.2.	iRMC のデフォルトの証明書	56
13.1.3.	MMB のデフォルトの証明書	56
13.2.	ServerView Connector Service (SCS)	57
13.2.1.	ルート CA	57
13.2.2.	SCS のデフォルトの証明書	57
14.	エンタープライズセキュリティに関する詳細情報	58
15.	付録: iRMC S4 の概要/暗号技術のサポート	59
15.1.	IPMI	59
15.1.1.	RMCP	59
15.1.2.	RMCP+	59
15.1.3.	IPMI でサポート暗号スイートのリスト	59
15.2.	OpenSSH	60
15.3.	SNMPv3	61
15.4.	Web、KVM、VMEDIA、Redfish (iRMC S5 のみ)	62
15.4.1.	SSLv3 の暗号リスト	62
15.4.2.	TLSv1.2 の暗号リスト	63
15.5.	CIM/SMASH (iRMCS4 のみ)	64
15.6.	Linux カーネル暗号	64
16.	用語集	65



## 1. はじめに

本書の最初の章で、品質管理と同様に、セキュリティ管理が永続的なプロセスであることを説明します。本書はセキュリティ分析およびセキュリティポリシー確立のためのガイドではありません。それらは重要なステップですが、本書の範囲よりも一般性が高く、包括的です。

本書のアプローチでは、サーバ管理ツールを使用せずに既にセキュアなシステムが構成されているものとします。新たに PRIMERGY サーバ管理コンポーネントを追加する場合、本書にシステムをセキュアに維持する方法、および管理操作のセキュリティを向上させる方法についての多くのヒントが記載されています。当然、セキュリティを增強すると、計画や構成などの作業が増加します。どのルールとヒントを使用するかは、セキュリティポリシー全体に照らして決定してください。

本書で検討するセキュリティの範囲は、ライフサイクル全体に対応します。

- インストールとデプロイメント（第 4 章）
- 監視と管理（第 5、6、7 章）
- 保守（第 8 章）
- 修復および out-of-band 管理（第 10 章）

## 2. 「セキュリティ管理はプロセスである」

セキュリティは、製品やソリューションによって実現することはできません。永続的なセキュリティ管理プロセスによってのみ、セキュリティは実現します。これは、永続的な品質管理プロセスと同じです。

また、予防だけではセキュリティを実現することもできません。予防システムは決して完璧ではありません。セキュリティポリシーには、予防、検出、対応を含める必要があります。

### 2.1. セキュリティコンセプトの確立

堅牢で機密性の高い IT システムのセキュリティは、矛盾なく定義されたセキュリティポリシーを正しく実装して保守することによって実現します。このようなセキュリティポリシーでは、技術的な問題の他に、組織に関する問題、人的な側面、リスク発生確率、リスク評価といった多くのさまざまな側面を考慮する必要があります。

基本的には以下のステップを行い、矛盾なく定義されたセキュリティポリシーを確立します。

- 保護する財産と資産の分析
- 脅威の分析
- リスクの評価
  - 損失、破壊、財務的影響などの一次的な影響
  - 遅延、ビジネス損失などの二次的影響
  - 信頼喪失、顧客喪失などの二次的影響
- 特定の脅威から保護するための決定
- 数々の適切な対策の選択
- コスト計算
- 残存リスクの評価

これらのステップのいくつかを複数回行う必要があることはほぼ確実です。つまり、単純なシーケンスではなく、サイクルになる可能性があります。たとえば、「コスト計算」でコストが損害を上回ることがわかった場合、「数々の適切な対策の選択」ステップを繰り返す必要があります。

## 2.2. 継続的な調整の必要性

これらのステップのすべてを行うと、最初のステップ「保護する財産と資産の分析」を行った時点の状況に対してセキュリティポリシーを確立したことになります。極端な場合、新しいセキュリティポリシーは、すでに陳腐化している可能性があります。通常はこのようなことはありませんが、セキュリティポリシーは定期的に、また、資産に関する大きな変化があった場合、新しい潜在的脅威が発生した場合、新しい対策を実施できるようになった場合などに、調整する必要があることを示しています。

本書では次の状況を例として取り上げます。セキュリティポリシー全体がすでに IT ビジネスに対して設計されているとします。つまり、セキュリティ目標を達成するためのルールとそれらの実装の枠組みができています。新しいコンポーネントの追加、プロセスの変更、組織の変更などが行われるたびに、セキュリティポリシーの調整も行う必要があります。また、このような調整を必要とするイベントとして、サーバ管理ツールの配備を挙げることもできます。

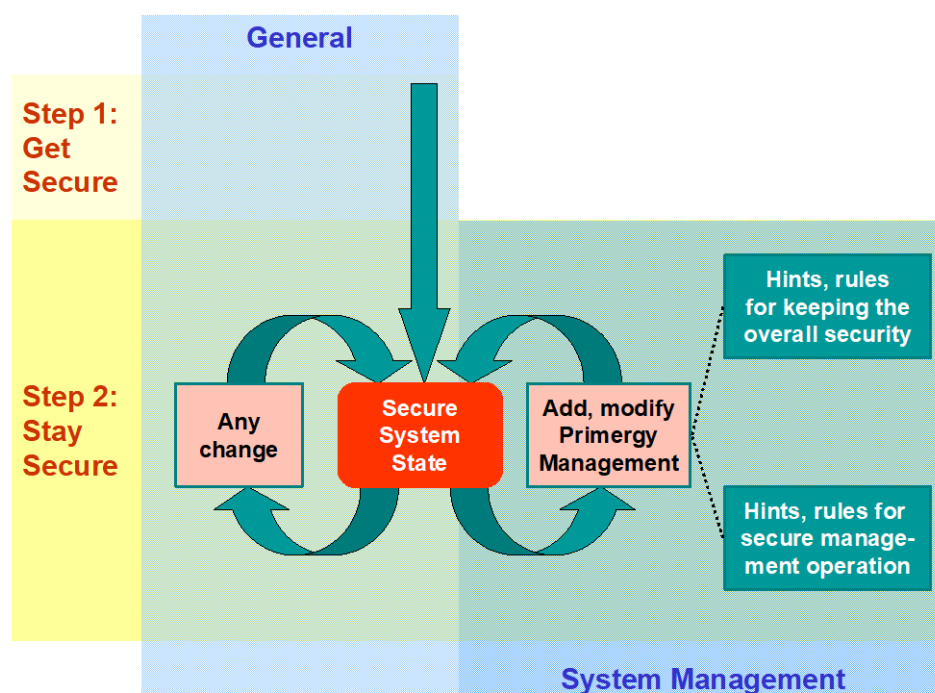


図 1: セキュリティのアプローチ

図 1 はこのアプローチを説明しています。一般的なアプローチは、「Get Secure」と「Stay Secure」の 2 つのステップで構成されます。

このドキュメントは次のアプローチに従います。ユーザは、すでに最初のステップを終えています。つまりセキュアなシステム構成を実現できており、次に PRIMERGY サーバ用の ServerView Suite コンポーネントを追加または変更しようとしています。本書では、「Stay Secure」ステップでユーザを支援する 2 種類のヒントを紹介します。

- システム全体をセキュアに維持することを支援するヒントとルール。たとえば、Web サーバをインストールするときに特定のルールを適用しないとセキュリティホールが生じる可能性があります。
- サーバ管理操作のセキュリティを強化するヒントとルール。たとえば、権限のないユーザが管理操作を行えないようにするなどです。

サーバ管理ツールを使用する際は、既存の IT 構成および既存のセキュリティポリシーに対するセキュリティ上の問題および影響を評価する必要があります。両者は関連性がないため、本書ではサーバ管理に関するセキュリティソリューションは扱いません。

せん。ここでは、PRIMERGY サーバの ServerView Suite を使用する場合にセキュリティポリシーを調整するための情報と支援を提供します。

上述のように、予防システムは完璧ではありません。潜在的な脆弱性が非常に多く、サイバー攻撃者は、最も容易で最も手軽な手段に便乗します。彼らは、最も効果的で広まっている攻撃ツールを使用して、最もよく知られた弱点につけ込みます。有効な戦略は、セキュリティホールを塞ぐことです。

これらは、後項の各所で参照しています。



## 3. 一般的な問題

### 3.1. 通信パス

この項では、PRIMERGY ServerView Suite の各種コンポーネント/ツールで使用するすべての通信パスについて説明します。『ServerView Suite: Basic Concepts』マニュアルに記載されているように、ServerView Suite のコンポーネントは次の 4 つのカテゴリに分類できます。

- 管理コンソール
- 管理アプリケーション
- ヘルパー
- 管理対象ノード

図 2 は、これらのサーバ管理コンポーネントが属するカテゴリと、相互の通信方法について図示したものです。これらのコンポーネントは別々のコンピュータにインストールすることができますが、異なるカテゴリの複数のコンポーネントを 1 台のコンピュータにインストールすることもできます。

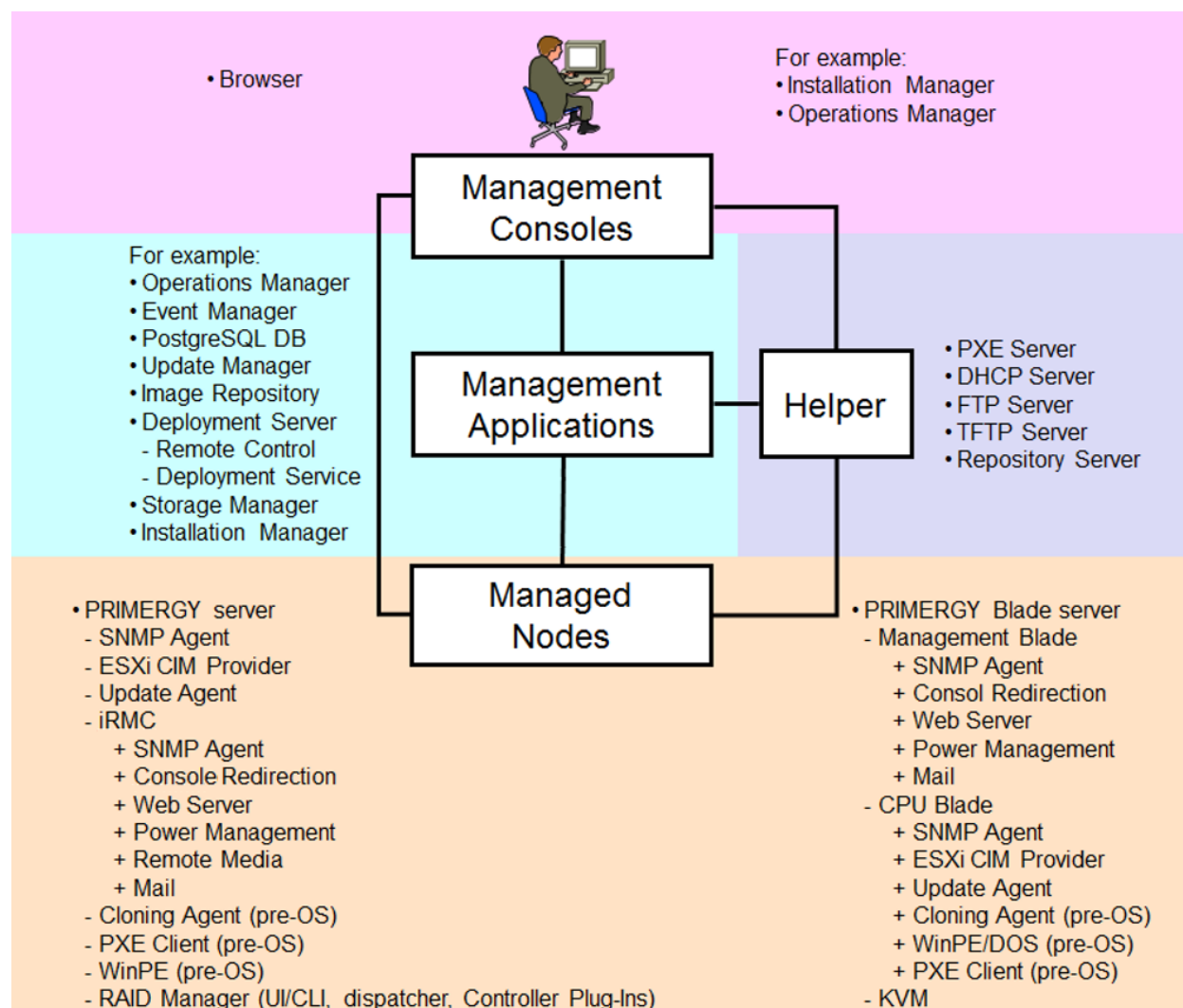


図 2：PRIMERGY サーバの ServerView Suite で使用される通信パス



iRMC は、PRIMERGY ServerView Suite で一部使用されない通信パスを提供します。

- IPMI
- SSDP
- eLCM
- 仮想メディア
- AIS Connect
- USB Host LAN
- AVR

iRMC のセキュリティ面の詳細については、10.3.1 項を参照してください。

次の表に、デフォルトで使用される通信プロトコルとポートを示します。デフォルトでは、主に well-known ポート（0 ～ 1023）および IANA 登録ポート（1024 ～ 49151）が使用されます。3169 ～ 3173、3789、4178、9212、9213 のポートは、PRIMERGY サーバ専用に IANA で登録されています。

詳細については次を参照してください。

<http://www.iana.org/assignments/port-numbers>

ただし、ほとんどのポートは他のポート番号へ個別に設定できます。

↔：双方向の通信パス

← または →：単方向の通信パス

通信	ポート：プロトコル 目的
<b>管理コンソール - 管理アプリケーション</b>	
ブラウザ ↔ Operations Manager	3169 (IANA 登録ポート) : UDP/TCP
ブラウザ ↔ Event Manager	TomEE Application Server
ブラウザ ↔ Update Manager	3170 (IANA 登録ポート) : UDP/TCP
ブラウザ ↔ Remote Management/ Web フロントエンド	TomEE Application Server over SSL
ブラウザ ↔ Deployment Manager	3172 (IANA 登録ポート) : UDP/TCP
ブラウザ ↔ Virtual I/O-Manager	SV Connector Service (SCS)
ブラウザ ↔ Installation Manager	3169 (IANA 登録ポート) : UDP/TCP
	ServerView Application Service
	3170 (IANA 登録ポート) : UDP/TCP
	ServerView Application Service over SSL
Mailserver ← Event Manager	25: UDP/TCP
	SMTP メール (設定可能)

通信	ポート：プロトコル 目的
vCenter Plugin ↔ vCenter ServerView Plugin Appliance	3170: HTTPS <a href="http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&amp;cmd=displayKC&amp;externalId=1012382U6T">http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&amp;cmd=displayKC&amp;externalId=1012382U6T</a> を参照してください。 で、その他の vCenter 関連のポートの使用状況に関するリストと説明を参照してください。 9092 (localhost 上のみ、外部アクセスはファイアウォールで拒否できます)：内部データベース H2  5480: Plugin アプライアンスの設定ポート
vRealize Orchestrator ↔ vCenter ServerView Plugin Appliance	3170: HTTPS
vRealize Operations ↔ vCenter ServerView Plugin Appliance	3170: HTTPS
NAGIOS Plugin スクリプトは可変ポートパラメータを受け付ける。使用されるデフォルト値:  スクリプト ↔ SNMP  スクリプト ↔ CIM-XML  スクリプト ↔ WS- MAN  スクリプト ↔ REST  CIM インジケーション - リスナー	161  https: 5989, http: 5988  ESXi https: 8888, http: 8889, その他 https: 5986, http: 5985  SCS: 3172 iRMC https: 443, http: 80  https および http: 3169
ブラウザ <- -> System Monitor	3172: SV Connector Service (SCS) (IANA 登録ポート) : UDP/TCP
管理コンソール - 管理対象ノード	
ブラウザ (Advanced Video Redirection) ↔ iRMC Web サーバ ブラウザ ↔ マネジメントブレード : Web サーバ	80: UDP/TCP Web HTTP (設定可能) 443: UDP/TCP HTTP over TLS/SSL (設定可能)

通信	ポート : プロトコル 目的
Administrator ↔ Linux CIM Agent	5989: 受信および送信 TCP HTTPS 経由の CIM-XML トランザクション 5988: 受信および送信 TCP HTTP 経由の CIM-XML トランザクション 5986: 受信および送信 TCP HTTPS 経由の WS-MAN トランザクション 5985: 受信および送信 TCP HTTP 経由の WS-MAN トランザクション
Administrator ↔ Windows CIM Agent	5986 / 443: 受信および送信 TCP HTTPS 経由の WS-MAN トランザクション 5985 / 80: 受信および送信 TCP HTTP 経由の WS-MAN トランザクション
クライアント ↔ iRMC Remote Manager/ SMASH CLP	22: TCP (SSH、設定可能) 3172: TCP (Telnet、設定可能)
クライアント ↔ IPMI-over-LAN	623: UDP (RMCP+/LAN 上のシリアル通信)
ブラウザ/S3 クライアント SW ↔ 外部 KVM KVM S2-1611/KVM S2-0411/KVM S3-1621	3211: UDP/TCP 独自プロトコル 2068: TCP キーボードとマウスの暗号化されたデータ、デジタルビデオデータ、仮想メディア 8192: TCP デジタルビデオデータ 389: UDP LDAP (非セキュア) 636: UDP LDAP (セキュア)
Administrator ← iRMC/マネジメントブレード : 電子メールアラート	25: UDP/TCP SMTP メール (設定可能)
ブラウザ ↔ RAID Manager	3173 (IANA 登録ポート) : UDP/TCP HTTP over SSL
Configuration Manager ↔ PRIMERGY サーバ Configuration Manager ↔ CPU ブレード	3172 (IANA 登録ポート) : UDP/TCP SV Connector Service (SCS)
Installation Manager ↔ Installation エージェント	9213 (IANA 登録ポート) : UDP/TCP Installation Manager のリモート制御 (設定可能)
Installation Manager → Installation エージェント	5001 : TCP Installation Manager のリモート制御 (設定不可能)

通信	ポート：プロトコル 目的
ServerView Tomcat ↔ ESXi, MMB	3170: TCP (cim.listening.port) 3169: Indication listener 161: UDP/TCP SNMP 162: UDP/TCP SNMP トラップ  5989: ESXi 上の CIM サービス  <a href="http://pubs.vmware.com/vsphere-55/index.jsp?topic=%2Fcom.vmware.vsphere.security.doc%2FGUID-ECEA77F5-D38E-4339-9B06-FF9B78E94B68.html">http://pubs.vmware.com/vsphere-55/index.jsp?topic=%2Fcom.vmware.vsphere.security.doc%2FGUID-ECEA77F5-D38E-4339-9B06-FF9B78E94B68.html</a> および <a href="http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&amp;cmd=displayKC&amp;externalId=1012382U6T">http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&amp;cmd=displayKC&amp;externalId=1012382U6T</a> を参照してください で、その他の vCenter 関連のポートの使用状況に関するリストと説明を参照してください。
Redfish Client ↔ iRMC	iRMC S5 443: TCP (設定可能) Redfish サービス
ISM ↔ iRMC	iRMC S5 1900: UPNP SSDP での自動検出用の UDP (SSDP が無効の場合は閉じる) 50000: UPNP SSDP 記述用の TCP/UDP (SSDP が無効の場合は閉じる)
管理コンソール - 管理コンソール (SVOM V7.11 以上)	
TomEE	8005 シャットダウンポート
TomEE	8009 Apache JServ Protocol (AJP) ポート
TomEE	その他のすべてのポートは、RFC 6335 で定義される「動的ポート」範囲で動的に割り当てられます。
管理コンソール - 管理コンソール (SVOM V7.20 以上)	
TomEE	31705 シャットダウンポート
TomEE	その他のすべてのポートは、RFC 6335 で定義される「動的ポート」範囲で動的に割り当てられます。
ポート 1325、1445、4713、8009、8090、9443、9990、9999 は使用されなくなりました	

管理アプリケーション - ディレクトリサービス	
中央認証サービス ↔ ディレクトリサービス	389: LDAP デフォルトポート (非セキュア) 636: LDAP SSL デフォルトポート 1473: ServerView の ApacheDS/OpenDJ の LDAP ポート (非セキュア) 1474: ServerView の ApacheDS/OpenDJ の LDAP SSL ポート
管理アプリケーション - 管理アプリケーション	
OpenDJ コントロールパネル ↔ OpenDJ	4444: ServerView の OpenDJ の管理ポート (IP アドレス 127.0.0.1 でのみ)
Operations Manager ↔ PostgreSQL DB (Linux のみ)	9212 (IANA 登録ポート) : UDP/TCP
Event Manager ↔ PostgreSQL DB (Linux のみ)	
Event Manager → Operations Manager	動的: UDP SNMP: Operations Manager から Operations Manager への通知
Operations Manager ↔ Storage Manager	4178 (IANA 登録ポート) : UDP/TCP StorMan
管理アプリケーション - 管理アプリケーション (SVOM V9.00 以上)	
Operations Manager ↔ JMX bean	9876 (IANA 登録ポート) : Session Director (IP アドレス 127.0.0.1 でのみ)
管理アプリケーション - 管理対象ノード	
Operations Manager ↔ SNMP エージェント Event Manager ↔ SNMP エージェント Operations Manager ↔ SNMP エージェント (CPU ブレード) Event Manager ↔ SNMP エージェント (CPU ブレード) リモート制御 (Deployment サーバ上の DLL) ↔ SNMP エージェント (CPU ブレード) Operations Manager ↔ SNMP (マネジメントブレード) Event Manager ↔ SNMP (マネジメントブレード)	161: UDP/TCP SNMP 623: UDP IPMI over LAN/RMCP
Operations Manager ← SNMP エージェント Event Manager ← SNMP エージェント Event Manager ← SNMP トラップ (iRMC) Operations Manager ← SNMP エージェント (CPU ブレード) Event Manager ← SNMP エージェント (CPU ブレード) Operations Manager ← SNMP (マネジメントブレード) Event Manager ← SNMP (マネジメントブレード)	162: UDP/TCP SNMP トラップ

Operations Manager ← エージェント (パフォーマンス管理 & 電力監視 & Online Diagnosis & PrimeCollect & Configuration Manager & ServerListService & TestConnectivity & VME Services - 結果)	3172 (IANA 登録ポート) : UDP/TCP SV Connector Service (SCS)
Operations Manager ↔ ESXi CIM Provider	5989: 受信および送信 TCP HTTPS 経由の CIM-XML トランザクション 5988: 受信および送信 TCP HTTP 経由の CIM-XML トランザクション
Update Manager ↔ Update エージェント Update Manager ↔ Update エージェント (CPU ブレード) Update Manager ↔ Update エージェント プロバイダ (SOAP)	3171 (IANA 登録ポート) : TCP ファームウェアフラッシュ (設定可能) 3172 (IANA 登録ポート) : UDP/TCP SV Connector Service (SCS) (証明書チェック)
Update Manager ↔ マネジメントブレード/ コネクションブレード	161: UDP/TCP SNMP トラップ (読み取り専用) 22: TCP (SSH、設定不可能) 80: UDP/TCP Web HTTP
Operations Manager ↔ iRMC	161: UDP/TCP SNMP トラップ (読み取り専用) 623: UDP RMCP/IPMI over LAN 80: UDP/TCP Web HTTP 443: HTTPS
Installation Manager ↔ Installation エージェント (WinPE)	9213 (IANA 登録ポート) : UDP/TCP Installation Manager のリモート制御 (設定可能)
Installation Manager → Installation エージェント (WinPE)	5001 : TCP Installation Manager のリモート制御 (設定不可能)
Remote Management/Web Frontend ↔ マネジメントブレード テキストコンソールリダイレクション Remote Management/Web Frontend ↔ iRMC テキストコンソールリダイレクション	623: UDP: IPMI over LAN/RMCP 3172 (IANA 登録ポート) : UDP/TCP (SSL) Telnet : コンソールリダイレクション リモートマネージャインターフェース (設定可能)
Operations Manager ↔ VMware ホスト	443: UDP/TCP HTTP over TLS/SSL (SOAP)
Operations Manager ↔ Xen ホスト	9363: TCP XML-RPC

Operations Manager ↔ Hyper-V ホスト	135: WMI/DCOM、リモートプロシージャ呼び出し。 動的: RPC エフェメラル範囲 3172: (Hyper-V ホスト) パフォーマンスおよびスレッシュホールドデータ。
Operations Manager ↔ KVM ホスト	16509: TCP 16514: TLS
Virtual-IO Manager ↔ マネジメントブレード	3172: (IANA 登録ポート) : TCP (Telnet、設定可能) 22: TCP (SSH、設定可能)
Virtual-IO Manager ↔ Intelligent Blade Panel (IBP)	23: (IANA 登録ポート) : TCP (Telnet、設定可能) 22: TCP (SSH、設定可能)
Virtual-IO Manager ↔ iRMC	623: UDP: RMCP (LAN 上の IPMI ) 162: iRMC から管理用サーバへの SNMP トラップ
vRealize Orchestrator → iRMC	623: UDP: RMCP (LAN 上の IPMI ) 80/443: HTTP (S) eLCM REST API への通信
vCenter Plugin → iRMC	623: UDP: RMCP (LAN 上の IPMI ) 80/443: HTTP (S) eLCM REST API への通信
vCenter ServerView Plugin Appliance ↔ iRMC	623: UDP: RMCP (LAN 上の IPMI ) 80/443: HTTP (S) eLCM REST API への通信 162: iRMC から管理用サーバへの SNMP トラップ
vCenter Plugin → ESXi CIM Provider	5989 : HTTPS 経由の CIM-XML トランザクション (5988 : HTTPS 経由の CIM-XML トランザクション)
vCenter ServerView Plugin Appliance ↔ ESXi CIM Provider	5989 : HTTPS 経由の CIM-XML トランザクション (5988 : HTTPS 経由の CIM-XML トランザクション) 3169/3170 : HTTP(S) (ホストから管理用 サーバへの Indication)
vCenter ServerView Plugin Appliance ↔ SNMP (マネジメントブレード)	161: UDP/TCP SNMP
vCenter ServerView Plugin Appliance ← SNMP (マネジメントブレード)	162: UDP/TCP SNMP トラップ



管理アプリケーション - 管理アプリケーション	
Virtual-IO Manager ↔ Virtual-IO Manager	50042: 管理用サーバ内部通信
管理アプリケーション - ヘルパー	
Update Manager ↔ PXE サーバ (アップデートプロキシ) Update Manager ↔ TFTP サーバ (アップデートプロキシ)	3171 (IANA 登録ポート) : TCP ファームウェアフラッシュ (設定可能)
デプロイメントサービス ↔ PXE サーバ	ローカル
管理対象ノード - ヘルパー	
Update エージェント ↔ PXE サーバ (アップデートプロキシ)	3171 (IANA 登録ポート) : TCP ファームウェアフラッシュ (設定可能)
Update エージェント ↔ PXE サーバ (PXE ブート)	67: UDP/TCP Bootstrap Protocol サーバ (bootps)
PXE クライアント ↔ PXE サーバ WinPE ↔ PXE サーバ PXE クライアント (CPU ブレード) ↔ PXE サーバ WinPE (CPU ブレード) ↔ PXE サーバ Update エージェント ↔ PXE サーバ (PXE ブート)	4011: UDP/TCP 代替サービスのブート
PXE クライアント ↔ TFTP サーバ WinPE ↔ TFTP サーバ PXE クライアント (CPU ブレード) ↔ TFTP サーバ WinPE (CPU ブレード) ↔ TFTP サーバ Update エージェント ↔ PXE サーバ (PXE ブート) マネジメントブレード ↔ TFTP サーバ	69: UDP/TCP Trivial File Transfer (TFTP)
マネジメントブレード ↔ TFTP サーバ	161: UDP/TCP SNMP 80: UDP/TCP Web HTTP
Update エージェント ↔ SwitchBlade	22 SSH (Plink) ConnectionBlade FW フラッシュ

### 3.1.1. iRMC ファミリで使用されるネットワークポート

理解しやすいように、次の表に iRMC S4 / S5 で使用されるすべてのポートを示します。

http :	80、iRMC へのインバウンド（設定可能）
https :	443、iRMC へのインバウンド（設定可能）
SSH :	22、iRMC へのインバウンド（設定可能）
Telnet :	3172 (/23) 、iRMC へのインバウンド（設定可能）
SMTP :	25、iRMC からのアウトバウンド（設定可能）
SNMP :	161、iRMC からのアウトバウンド（設定可能）
SNMP トラップ :	162、iRMC からのアウトバウンド（固定）
LDAP :	389（非セキュア） 636（セキュア） iRMC からのアウトバウンド（設定可能）
CAS/シングルサインオン	3170、iRMC からのアウトバウンド（設定可能）
RMCP :	623、iRMC へのインバウンド（IPMI 1.5/2.0 仕様に従い、固定）
iRMC S1（AVR およびリモートメディア）:	
AVR（ビデオ）:	5900、iRMC へのインバウンド（設定可能）
AVR（セキュア）:	5910、iRMC へのインバウンド（設定可能）
リモートメディア:	5901、iRMC からアプレットへのアウトバウンド（設定可能）
リモートメディア:	5901、iRMC スタンドアロンストレージサーバからのアウトバウンド（設定可能、アプレットと共有）
iRMC S2（AVR およびリモートメディア - FW version 5.0x まで）	
AVR（ビデオ）:	80、iRMC へのインバウンド（設定可能、http ポートと共有）
AVR（セキュア）:	443、iRMC へのインバウンド（設定可能、http ポートと共有）
リモートメディア:	5901、iRMC からアプレットへのアウトバウンド（設定可能）
リモートメディア:	5901、iRMC スタンドアロンストレージサーバからのアウトバウンド（設定可能、アプレットと共有）
iRMC S4 / S5	
tftp :	69、iRMC からのアウトバウンド（固定） ...
iRMC S5	
Redfish :	443、iRMC へのインバウンド（設定可能）
SSDP :	1900、iRMC へのインバウンド（SSDP が有効な場合のみ） 50000、iRMC へのインバウンド（SSDP が有効な場合のみ）

## 3.2. ファイアウォールによる保護

ファイアウォールは、インターネットからの攻撃の防止に使用されます。PRIMERGY 管理製品のすべてのコンポーネント/ツールと管理対象のシステムがファイアウォールの内側にある場合、すべての通信パスがインターネットからの攻撃から保護されます。しかし、管理者は、ブラウザを使用してインターネット経由でいつでもどこからでも管理作業を行います。つまり、この理想的な状況においては、

- Java フロントエンド（管理コンソール）を搭載したブラウザと、Operations Manager などのアプリケーション間および
- Java フロントエンド（管理コンソール）を搭載したブラウザと、iRMC およびマネジメントブレード上の Web サーバ間

の通信パスのみがファイアウォールを通過する必要があります。これらの通信パスは後で示すように、SSL で保護することができます。

### Recommendation 1

PRIMERGY 管理スイートのすべてのコンポーネント/ツールと管理対象のシステムをファイアウォールの内側に配置します。Web ベースのツールには、ブラウザを使用してインターネット経由でアクセスできます。この通信パスは SSL で保護する必要があります（Recommendation 30 も参照）。

ただし、場合によりファイアウォール内で発生した特定のイベントに関する情報を取得するために、ファイアウォールを通じて SNMP トラップを送信するよう設定すると便利な場合があります。この場合、ファイアウォールを UDP ポート 162 に対して開いてください。開かれていない場合、SNMP トラップがブロックされます。

## 3.3. 開いているポート

正規ユーザと攻撃者の両方が、開いているポートからシステムに接続できます。開いているポートが多いほど、システムへの接続を可能にする手段が多くなります。そのため、システムが適切に稼働するのに必要な最低限数のポートしか開かないことが重要です。他のすべてのポートは閉じてください。

上の表に、PRIMERGY サーバ管理のために開く必要のあるポートを決定する際に必要な情報を示します。図に示すように、これはシステムによって異なり、さらに、構成およびシステムに配置されるコンポーネント/ツールによって異なります。

### Recommendation 2

各システムで開くポートの数を最小限にします。上の表に、PRIMERGY ServerView Suite でどのポートを開く必要があるかを示します。

### 3.4. 管理 LAN の分離

ファイアウォールの実装、および開いているポート数を最小限にする目的は、管理コンポーネントを不正アクセスから保護するためです。この目標は、サーバ管理用の VLAN を設定して、管理 LAN と運用 LAN を切り離すことによって実現することもできます。これにより、論理層の運用 LAN のトラフィックから管理 LAN のトラフィックが遮断されます。PRIMERGY の管理に使用される通信パスについて説明する図 2 と表に基づいて、管理用の通信全体、または選択したセキュリティに関連するパスに対して、VLAN トポロジを計画できます。

#### Recommendation 3

LAN 上の管理トラフィックと運用トラフィックを切り離すことにより、セキュリティを著しく改善できます。これを実現するには、PRIMERGY の管理に使用される通信パスについて説明する図 2 と表に基づいて、管理トラフィックの VLAN トポロジを設定します。

リモートマネジメントコントローラ (iRMC) およびマネジメントブレードには、固有の物理ネットワークインターフェースがあります。これにより、これらのコンポーネントとそれに対応するフロントエンド間で物理的に切り離された管理 LAN を構築することができます。その結果、多少の作業が必要となりますが、非常にセキュアな PRIMERGY 管理が実現します。

#### Recommendation 4

iRMC およびマネジメントブレードにはそれぞれ固有の物理ネットワークインターフェースがあり、それを使用して、物理的に切り離された管理 LAN を構築することができます。これにより、物理ベースでは、これらのコンポーネントから実行できる、セキュリティに影響するすべての操作は、この物理的に切り離された管理 LAN に接続されたノードからしか開始できなくなります。

## 3.5. SSL 証明書の管理

ServerView 製品へのすべての HTTP 接続は、SSL (Secure Sockets Layer) を使用して保護されます。このプロトコルを使用すると、サーバからクライアントへ証明書が転送されます。

「暗号技術において、公開鍵証明書（こうかいかぎしょうめいしょ）とは、公開鍵と、その所有者の同定情報（その他に有効期間、発行者、署名アルゴリズムなどの情報も含む）を結びつける証明書である。デジタル証明書とも呼ばれる。」（引用：『フリー百科事典 ウィキペディア日本語版』より。）

クライアントは、この証明書を信頼するか、接続の確立を拒否する必要があります。そのために、各クライアントは信頼する証明書のリストを保有します。このリストは、トラストストアと呼ばれています。通常、証明書はいわゆる認証局

(Certificate Authority : CA) によって署名され、これは別の証明書によって証明されます。クライアントがある CA を信頼する場合、この CA が署名したすべての証明書を信頼する必要があります。CA を証明する証明書に、別の CA が同時に署名することができます。このようにして、1 つの証明書は、証明書チェーンによって信頼されます。このようなチェーンの最上位の証明書を証明する CA をルート CA といいます。Internet Explorer と Firefox ブラウザがデフォルトで信頼するルート CA は多数あります。このリストは、各ブラウザのプロパティ設定にあります。

### 3.5.1. ServerView の証明書

次の表に、証明書が使用される ServerView 製品と、その用途を示します。

SV 製品	用途	注記
Operations Manager	暗号化、識別、認証	インストール時に作成
Agents	暗号化	製造時に作成
ServerView Raid	暗号化	インストール時に作成
iRMC	暗号化	製造時/オンラインに作成
MMB	暗号化	製造時に作成

セットアップ時にインストールされた証明書しか持たない ServerView Web サーバにブラウザを接続すると、このような証明書はまだ CA に署名されていないため、ブラウザからの警告が表示されます。そのとき、証明書を各ブラウザのトラストストアに恒久的にインポートして、今後警告が表示されないようにすることができます。これを行うときは十分に注意し、サーバ証明書の「フィンガープリント」（または「サムプリント」）をチェックします。ServerView Operations Manager のサーバ証明書の場合にフィンガープリントを取得する方法については、7.3 項「Exchanging SSL certificates for the Operations Manager」で説明します。

すべての ServerView 製品では、サーバ証明書をユーザ指定の証明書と交換できます。CA に署名された証明書を適用する可能性がある場合、インストールされた証明書を CA が署名した証明書に交換することを推奨します。証明書の交換方法の詳細については、各製品のマニュアルを参照してください。署名された証明書を商用 CA またはそれらの販売業者から購入したくない場合でも、自己署名証明書を使用して固有の CA を作成し、この CA からサーバ証明書を取得することができます。これには、取得した証明書は自動的に信頼されるため、CA の証明書をブラウザに一度インポートするだけでよいという利点があります。このようにすると、新しい HTTPS 接続を開くときに、フィンガープリントのチェックをせずに未知の証明書を即座に受け入れてしまうことが少なくなります。

## Recommendation 5

すでにブラウザから信頼されている（商用）CA に署名された証明書を購入しない場合は、自己認証局（CA）を作成します。次に、自己 CA の証明書を、ServerView 製品の操作に使用するすべてのブラウザにインポートします。

管理ノードなどにすでにインポートされている証明書を交換する場合、交換される証明書をもう一度インポートする必要があります。そのため、インストールされている証明書はできるだけ早く交換してください。

## Recommendation 6

セキュリティ上の理由で、ServerView 製品の Web インターフェースの SSL オプションを使用すること、および、事前に定義されている証明書を認証局（CA）の証明書にできるだけ早く交換することを推奨します。

### ヒント

ServerView Operations Manager (SVOM) の自己署名証明書の交換方法については、『ServerView でのユーザ管理』マニュアルの 4.2.4 項の「中央管理用サーバ (CMS) での証明書の交換」を参照してください。このマニュアルは、[Manuals Download Page](#) からダウンロードできます。

### 3.5.2. 証明書のフィンガープリント

Operations Manager の以前のバージョンと異なり、バージョン 5.00 以上では、サーバ証明書は暗号化に使用されるだけでなく、サーバの識別にも使用されます。そのため、秘密鍵とサーバ証明書はインストールメディアで配布されず、インストールタスクが行われるときにのみ個別に作成されます。その結果、証明書は認証局によって署名されず、自己署名のみになります。そのため、ブラウザには ServerView の開始ページは表示されませんが、「この接続は信頼されません」や「Web サイトのセキュリティ証明書に問題があります」などの警告が表示され、ページのロードを続行するかどうかについて尋ねられます。この状態で続行して、接続先のサーバに心当たりがない場合、パスワードなどの機密データを発行してはいけません。先に、「フィンガープリント」や「サムプリント」をサーバの秘密鍵の 1 つと比較して、サーバ証明書を慎重にチェックしてください。管理者アカウント（または JBoss の起動に使用したアカウント）を使用して以下のコマンドを発行することにより、CMS のフィンガープリントを取得します。

Linux :

```
{JAVA_BIN_PATH}keytool -keystore ${PKI_PATH}keystore -storepass ${STOREPASS} -list -v
```

Windows :

```
%JAVA_BIN_PATH%keytool -keystore %PKI_PATH%keystore -storepass %STOREPASS% -list -v
```

プレースホルダの意味は次の通りです。

JAVA\_BIN\_PATH: Java のインストール先の bin ディレクトリへのパス。例 :

C:\Program Files (x86)\Java\jre6\bin\

PKI\_PATH: ServerView Suite のインストール先の pki ディレクトリへのパス。

例 :C:\Program Files (86)\Fujitsu\ServerView Suite\jboss\server\serverview\conf\pki\

STOREPASS : キーストアのパスワード。現在、これは常に changeit です。

このコマンドの長い出力の中で Certificate Fingerprints という見出しの後の行に、要求した情報が次の例のように表示されます。

**証明書のフィンガープリント**

```
MD5: B9:6E:38:F4:B6:9C:80:0D:79:C4:ED:D4:FC:92:69:E4
SHA1: 58:DE:5C:0B:62:E2:94:77:51:09:40:9C:0A:6D:99:B1:0C:53:B5:C5
```

このフィンガープリントは、CMS のサーバ証明書をブラウザのトラストストアにインポートするときに必要になります。そのため、後で比較するために、プリントアウトするか、安全なメディアにコピーしてください。

**Recommendation 7**

サーバ証明書のフィンガープリントは、SSL によるセキュアな HTTP 接続を確立するときにブラウザから提供された値と比較する可能性があるため、プリントアウトするか、USB スティックなどのメディアへコピーします。

ServerView の事前に作成された証明書は、特定の Web サーバの識別には適していませんが、完全を期するために本書ではそのフィンガープリントをリストします（140 項「ServerView Default Certificates」を参照）。

## 3.6. ディレクトリサービスへのアクセス

ServerView では、ユーザの認証と許可のためにディレクトリサービスを利用します（5 項「User Management」を参照）。ディレクトリサービスには、LDAP（Lightweight Directory Access Protocol）を使用してアクセスします。ServerView の組み込みディレクトリサービスは LDAP のセキュアバージョン（LDAPS）を使用して自動的に設定されますが、外部ディレクトリサービスを設定するときに LDAP を選択できます。ただし、ユーザの資格情報は復号化されて LDAP 接続を介して転送されるため、これは実験環境以外では推奨されません。

**Recommendation 8**

SSL によるセキュアな LDAP を設定して外部のディレクトリサービスへアクセスします。

ディレクトリサービスでユーザデータにアクセスするには、ディレクトリサービスのユーザアカウントを設定する必要があります。セキュリティ上の理由から、このユーザアカウントには最小限（読み取り専用）のユーザ権限のみ付与します。

**Recommendation 9**

最小限のユーザ権限を持つユーザアカウントを使用して、外部のディレクトリサービスへの LDAP アクセスを設定します。



## 3.7. ブラウザの設定

ブラウザは今では、インターネットからの攻撃の主な標的の 1 つとなっています。したがって、セキュリティギャップを回避するために、ブラウザの設定と操作は慎重に行ってください。これは、インターネットのブラウズにブラウザを使用する場合にも効果的です。ブラウザの考えられるセキュリティ問題とその解決策の説明は、インターネットのさまざまなサイトで紹介されています。Internet Explorer を使用するとき、標準のセキュリティ設定でブラウザを運用している場合、ServerView 製品の Web サーバを実行しているすべてのホストを信頼済サイトのリストに追加する必要があることに注意してください。さらに「InPrivate」ブラウズは、ServerView の Web ページではサポートされないことも注意してください。以下に、ServerView の Web ページに関連する特別なヒントをいくつか紹介します。

### 3.7.1. Cookie

Cookie の設定はブラウザで慎重に制御してください。これに関連して、ServerView の Web ページでは次の Cookie を設定しており、これは正常に機能するために必要であることに注意してください。

JSESSIONID: これは、[Java™ Servlet Specification](#) に規定されるセッショントラッキング Cookie です。ServerView は、JBoss Application Server に含まれる Apache Tomcat Java コンテナを利用するので、ServerView の Web ページが適切に動作するように、この Cookie を設定する必要があります。

AURA: これは、ServerView Raid によってのみ使用されるもう 1 つのセッショントラッキング Cookie です。

CASTGC: これは、ServerView の Central Authentication Service (CAS) のチケット認可チケット Cookie です。サービスがこの Cookie を設定しないようにすると、シングルサインオン機能を利用できなくなります。つまり、ServerView 製品のあらゆる Web サーバごとにログインしなければならなくなります。

org.springframework.web.servlet.i18n.CookieLocaleResolver.LOCALE: この Cookie は、GUI で使用する言語を保存するために、ServerView の CAS で使用される [Spring フレームワーク](#) によって設定されます。使用する言語は、HTTP パラメータ Lang によって常に追加して提供されるので、この Cookie の設定を拒否しても機能面での不都合は生じません。

さらに、ServerView Operations Manager が適切に動作するように、Firefox の Cookie の設定では、「サードパーティの Cookie も保存する」オプションをオンにする必要があります。

### 3.7.2. スクリプト

スクリプト言語の使用もできる限り制限します。ただし、ServerView の Web ページを操作するために、JavaScript および Java アプレットの使用を有効にする必要があります。

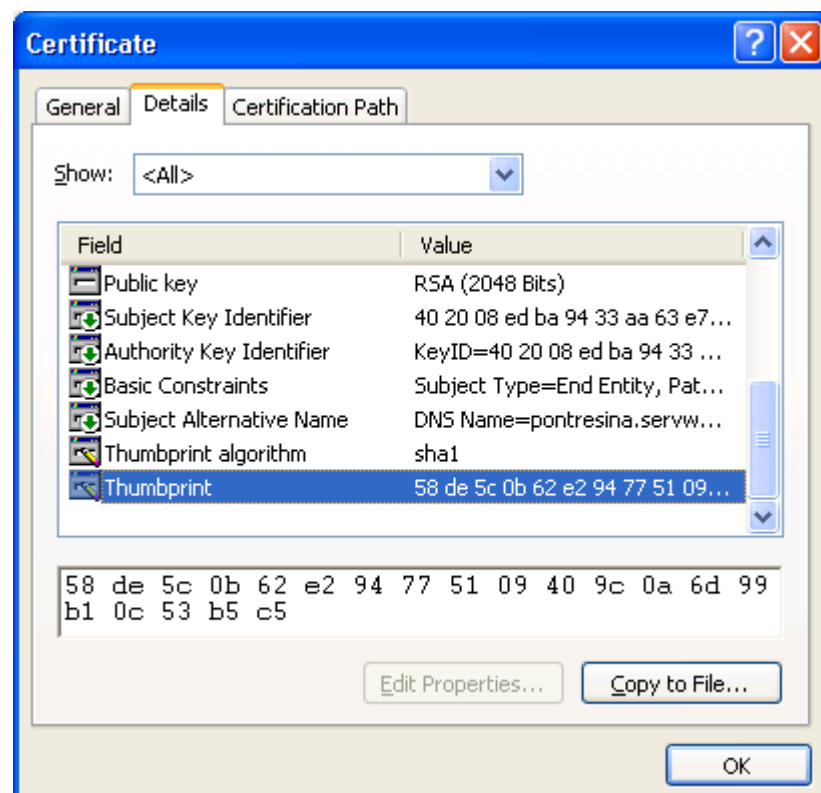
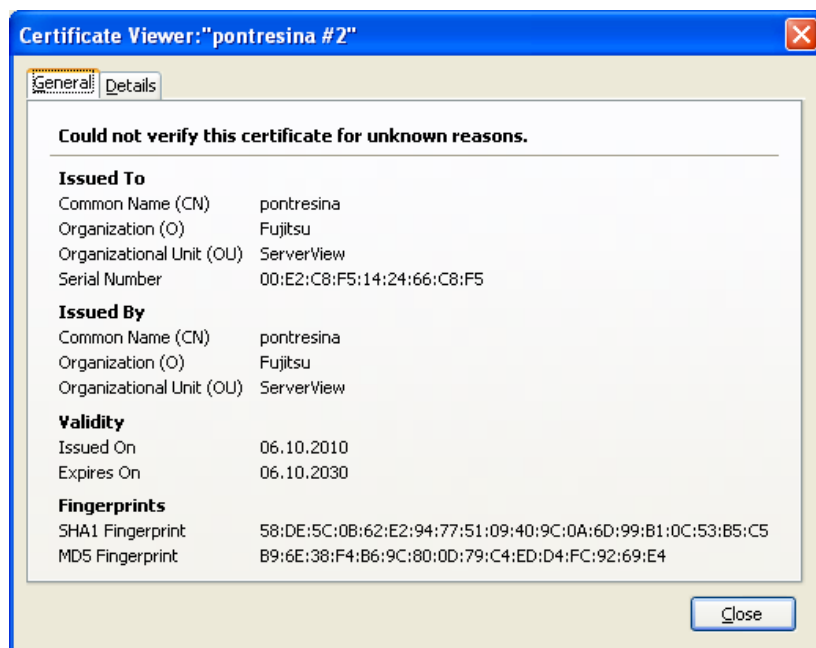
### 3.7.3. 証明書の管理

Operations Manager 内の Web ベースの通信は SSL 接続によってセキュリティ保護されます。Operations Manager の以前のバージョンでは、オプションとして、SSL (Secure Socket Layer) によってセキュリティ保護された接続でのセキュアなアクセスを提供していました。バージョン 5.00 以上では、これがセキュリティ上の理由から必須になり、SSL でセキュリティ確保された接続を使用しないと Operations Manager にアクセスできなくなりました。これは、ユーザパスワードが接続時にクリアテキストとして送信されますが、これらの認証情報はファイアウォール保護されたイントラネット内であっても見られないようにする必要があるためです。

SSL でセキュリティ保護された接続を確立するには、データの暗号化および復号化のための秘密鍵をクライアントとサーバ側で交換する必要があります。これは SSL ハンドシェイクプロトコルを使用した接続開始時に行われ、最初にサーバが鍵のペアの公開部分を含む証明書を公表します。秘密鍵はこの交換にサーバ自体が使用し、クライアントは公開鍵を使用します。

3.5 項の「SSL Certificate Management」に示されるように、サーバ証明書や自己 CA の証明書をブラウザのトラストストアにインポートすることができます。ただし、Web サーバによって提供される証明書が、本当に期待する証明書であることを確認する必要があります。これを行うには、証明書のフィンガープリントを、サーバ上のサーバ証明書から取得したフィンガープリントと比較します（3.5.2 項の「Certificate Fingerprints」を参照）。

Mozilla Firefox や Microsoft Internet Explorer など、どのブラウザも証明書のフィンガープリントを少なくとも 1 つ表示することができます。



ほとんどのブラウザでは、ページを右クリックしてそのページのプロパティを選択するとサーバ証明書が表示されます。証明書の情報は、プロパティから簡単に見つけられます。

#### Recommendation 10

目的の中央管理用サーバ（CMS）に接続されていることが完全には確実でない場合、CMS のサーバ証明書のフィンガープリントをよく確認する必要があります。

ブラウザの「トラストストア」に「インポート」または「インストール」することにより、同じ証明書を何度もチェックしなくて済みます。Firefox の場合、「信頼されない接続」を確立するために「例外を追加」して、「次回以降にもこの例外を有効にする」チェックボックスをオンにすることによって、簡単に実現できます。Internet Explorer の場合は、「証明書」ウィンドウの「全般」の「証明書のインストール」ボタンをクリックすることにより、同様のことを行うことができます。細心の注意を払い、証明書のフィンガープリントを常にチェックしてください。それでもなお誤って不要な証明書をインポートしてしまった場合は、ブラウザの証明書マネージャを使用して、ブラウザのトラストストアからその証明書を削除します。

Firefox の場合、証明書マネージャは、メインメニューで「ツール」->「オプション」を選択し、「詳細」ウィンドウの「暗号化」タブを選択し、そこで「証明書を表示」ボタンをクリックすると表示されます。

#### Recommendation 11

ブラウザのトラストストアにインポートした証明書は、頻繁にチェックしてください。ストアのサイズはできる限り小さくしておくようにし、サーバおよび認証局のエントリは、必要なくなった場合は削除します。

3.5.1 項の ServerView Certificates ですでに示したように、ブラウザに信頼される CA が署名した証明書を CMS にインストールした場合、証明書をインポートせずに済みます。

## 3.8. セキュアブート

最新の PRIMERGY Server は、UEFI ブートモードを標準としてリリースされています。これにより、自動的によりセキュアなシステムを実現するセキュアブートを選択できます。以下の点に注意してください。

- ブートは、署名されたドライバでのみ成功します
- UEFI（レガシーではない）モードでのみ使用可能
- BIOS に署名する必要があります
- アダプタカードのドライバに署名する必要があります
- 古い OS ではサポートされません

## 4. PRIMERGY サーバの設定、インストール、およびデプロイメント

PRIMERGY サーバの設定、インストール、およびデプロイメントには、以下のツールを使用できます。

- Installation Manager - ローカルまたはリモートインストール用のツール
- ServerView RAID Manager - 複数の RAID コントローラを同じ Web ベースのユーザインターフェースを使用して管理するためのツール
- Multi-Deployment Platform (MDP) - ターゲットサーバにてローカルまたはリモートのデプロイメントプロセスの機能が動作するサービスプラットフォームを提供するツール

オペレーティングシステムをインストールする前に、Bootable Update DVD を使用して、各種サーバコンポーネントのファームウェアおよびサーバの BIOS を管理対象サーバでローカルでアップデートできます。

詳細については、8.1 項を参照してください。

上述したように、Download Manager の目的は、管理用サーバのリポジトリを最新状態に維持することです。適切に設定した場合、Download Manager は新しいアップデートパッケージがないか Fujitsu Web サーバを定期的にチェックし、新しいパッケージを中央管理用サーバ (CMS) のアップデートリポジトリにダウンロードします。

指定された Web サイトからダウンロードされるファイルには、技術的な理由から署名されていないものがあります。バージョン 5.0 以降、ダウンロード中にこれらのファイルが改ざんされないように、セキュアな HTTPS プロトコルがサポートされています。

ダウンロードされるファイルの一部は関連する署名ファイルを持ち、それらは、取得するプログラムによって検証されます。たとえば、UMEiRMC.tar をダウンロードする場合、変更を回避するために暗号化されている署名ファイルが付属し、UMEiRMC.tar は使用前に iRMC で検証できます。

### Recommendation 12

可能であれば、Download Manager 機能には HTTPS プロトコルを選択してください。

### 4.1. RAID Manager

ServerView RAID Manager を使用すると、同じ Web ベースのユーザインターフェースを使用して複数の RAID コントローラを設定および管理することができます。ServerView RAID Manager は、ローカルでもリモートでも起動できます。各通信は、HTTPS および SV 登録ポートである 3173 を使用して実行され、TLS/SSL によって暗号化されます。

ServerView RAID Manager を使用する前に、管理者はアカウントとパスワードの入力が必要です。

アカウントとパスワードが通常の文字列として送信されるため、SSL によるセキュアな接続から非セキュアな HTTP 接続へ変更されないことを強く推奨します。

RAID Manager ネットワーク接続のセキュリティ設定は、amDPatch.ini ファイルで設定できます。

このファイルは、RAID Manager bin ディレクトリに配置されています。

Windows : C:\Program Files\Fujitsu\ServerView Suite\RAID Manager\bin\amDPatch.ini

Linux : /opt/fujitsu/ServerViewSuite/RAIDManager/bin/amDPatch.ini

推奨されるデフォルト SSL セキュリティオプションは、TLSv1.1 以上で使用します。

カスタムセキュリティ選択を有効にするには、ClientSecurity の行の値を次のように調整する必要があります。

`ClientSecurity = 4` (カスタムセキュリティ選択を有効化)

許可しないプロトコルは SSLSecurityOptions の行にリストされます。

```
SSLSecurityOptions = SSL_OP_ALL:!SSL_OP_DONT_INSERT_EMPTY_FRAGMENTS:SSL_OP_
NO_SSLv2:SSL_OP_NO_SSLv3:SSL_OP_NO_TLSv1
```

オプションの定義：

```
SSL_OP_NO_SSLv2
SSL_OP_NO_SSLv3
SSL_OP_NO_TLSv1
SSL_OP_NO_TLSv1_2
SSL_OP_NO_TLSv1_1
```

例：TLSv1.1 を無効にするには、SSL\_OP\_NO\_TLSv1\_1 をこの行に追加します。

```
SSLSecurityOptions = SSL_OP_ALL:!SSL_OP_DONT_INSERT_EMPTY_FRAGMENTS:SSL_OP_
NO_SSLv2:SSL_OP_NO_SSLv3:SSL_OP_NO_TLSv1:SSL_OP_NO_TLSv1_1
```

変更を有効にするには、RAID Manager を再起動する必要があります。

## 4.2. Installation Manager を使用したリモートインストール

PRIMERGY サーバのローカルインストールの他に、Installation Manager では、リモートインストールを行うこともできます。Installation Manager のリモートインストールは、ローカル準備フェーズとそれに続くレプリケーションフェーズとしてのリモートインストールで構成されます。

リモートインストールには、デプロイメントサーバの準備が必要です。

この準備中に、Installation Manager DVD のコンテンツツリーがデプロイメントサーバのハードディスクへネットワーク共有としてコピーされます。デプロイメントサーバへの Installation Manager のインストール中、このネットワーク共有へのアクセスは、ユーザ名とパスワードで保護できます。

リモートインストールをターゲットシステムに対して開始するときに、管理者はこの名前とパスワードを入力する必要があります。そうしないと、ターゲットシステムでのインストールプロセスが Installation Manager のコンテンツにアクセスできません。Installation Manager での不正なリモートインストールは、このメカニズムで回避されます。

Installation Manager は、リモートインストールに、Installation Manager - OS (WinPE) との別のネットワーク共有を使用します。このネットワーク共有には、TFTP 経由で読み取り専用アクセス権限を使用してアクセスします。これが危険と見なされる場合は、Installation Manager をローカルモードでのみ使用することを推奨します。

### Recommendation 13

セキュリティポリシーに従ってアカウントを使用して、Installation Manager のコンテンツとのネットワーク共有を保護してください。これで、Installation Manager での不正なリモートインストールを防止できます。読み取り専用アクセス権限での OS 共有への TFTP アクセスが危険と見なされる場合は、Installation Manager をローカルモードでのみ使用することを推奨します。

Installation Manager は、PRIMERGY サーバをローカルまたはリモートでインストールすることを主眼に置いています。基本的には、セキュリティの検討対象となる、以下の 4 つのフェーズがあります。

- Installation Manager を使用するためのコンポーネントのインストール
- リファレンスインストールセッション

ブレードサーバのデプロイメントに関しては特に、マネジメントブレードが Installation Manager の運用において重要な役割を果たします。Recommendation 4 も考慮してください。

#### 4.2.1. デプロイメントコンポーネントのインストール

2 つのインストールプロセスがあります。

- リモートインストールエージェントを含む Web ベースの SV Installation Manager フロントエンドは通常、Operations Manager として同じマシンにインストールされます。これらのコンポーネントを提供するこのマシンは、CMS（中央管理用サーバ）と呼ばれます。
- PXE サービス、TFTP サービス、およびインストールサービスを含むプラットフォームを「デプロイメントサーバ」と呼びます。これは、CMS の役割でもあることがあります。

#### リモートインストールエージェント

インストールエージェントは Fujitsu ServerView アプリケーションサービス (Tomcat) を使用し、SV Operations Manager と同じマシンにインストールすることができます。正常にインストールされた後、Installation Manager のグラフィカルユーザインターフェース (GUI) を起動できます。Web ブラウザは通常は同じマシンで起動されます。つまり一般には、Web ブラウザと ServerView アプリケーションサービス間の通信はローカルで行われます。

この場合、ローカルの HTTP リクエストのみ許可するように Tomcat アプリケーションサーバを設定すると、セキュリティを強化できます。

ただし、Installation Manager が SSL を使用するように設定されている場合（も参照）、Web ベースのアクセスが自動的に SSL で保護されます。

インストールエージェントへのアクセス方法に関係なく、デプロイメントセッションはログイン操作によって開始されます。インストールサービスはインストールエージェントからアクセスされるので、認証/許可は、このサービスのインストール時に指定されるアカウント（管理者アカウント）に基づきます。認証されていない状態でのアクセスはできません。

#### Recommendation 14

デプロイメントセッションの認証/許可は、インストールサービスのインストール時に定義されるユーザアカウントに基づくインストールエンジンによって行われます。必要に応じて、ローカルの HTTP 要求のみ許可するように Tomcat アプリケーションサーバを設定することにより、セキュリティを強化できます。

#### インストールサービス

インストールサービスのセットアッププロセス中に、インストールサーバセッションにアクセスするためのユーザアカウントを指定します。このアカウントは後で、インストールエンジンを使用してデプロイメントセッションを開始するときの、認証/許可に使用します。

#### 4.2.2. Installation Manager によるリファレンスインストール

リファレンスインストールの実行方法には、ローカルインストールとリモートインストールの 2 通りがあります。

ローカルインストールでは、USB インターフェースを使用してターゲットサーバを CD-ROM ドライブおよびフロッピーディスクドライブに接続する必要があります。また、モニタ、キーボード、マウスをブレードサーバキャビネットの背面に接続し、内部 KVM スイッチを使用して必要なサーバに配線します。このハードウェアの準備にはある程度の労力が必要ですが、ローカルインストールには、リモートインストールに比べて 2 つの重要な利点があります。

- ローカルインストールでは Installation Manager のガイドモードを使用でき、これによりターゲットハードウェアが自動的に検出され、インストール処理の間はこの情報が使用されます。このモードは、デプロイメントブレードをエラーなくインストールする最も安全な方法です。



- インストールプロセスはすべてローカルで実行されるので、セキュリティの問題はありません。

リモートインストールには上述したハードウェアの準備は必要ありませんが、リモートインストールを実行可能なデプロイメントサーバをインストールする必要があります。このデプロイメントサーバには、デスクトップ PC またはノート PC を使用できます。

リモートインストールは次の 2 つのステップで行います。最初に Installation Manager を準備モードで実行し、デプロイメントサーバに構成ファイルを生成します。次のステップで、この PXE サービスから以前生成した構成ファイルを使用して、デプロイメントブレードが Installation Manager を無人モードでブートして実行できるように、デプロイメントサーバ上で PXE サービス/FTP サービスを準備します。

最後に、ターゲットサーバで PXE ブートを起動する必要があります。

次の 2 つのデメリットがあります。

- 準備モードは、ターゲットハードウェア上でローカルに実行されないため、ハードウェア構成を検出できません。
- リモートインストールでは DHCP サービスと PXE サービスを使用します。

デプロイメントブレードの LAN セグメントに 1 つの DHCP と 1 つの PXE しかない場合、ターゲットサーバはこれらのサービスのみにアクセスするので、セキュアな構成と見なされます。

インストールサーバにインストールされている PXE サービス以外に別の PXE サービスがある場合は、以下の点を確認してください。

- これらの PXE サービスがパッシブであるか。つまり、設定された MAC アドレスからの要求にのみ反応するか。
- PXE サービスが信頼できるか。つまり、それらが管理対象/スキャン対象の MAC アドレスがデプロイメントサーバの PXE サービスの MAC アドレスと競合しないか。

これらの条件が満たされない場合、目的とするソフトウェア以外のソフトウェアでターゲットサーバがインストールされる危険があります。

#### Recommendation 15

最も安全な方法はローカルインストールで、さらにハードウェア構成を自動的に検出するというガイドモードの利点もあります。リモートインストールを使用する場合は、以下の点を確認してください。

- デプロイメントサーバにインストールされている PXE サービス以外に LAN セグメントに別の PXE サービスがあるか。
- ある場合は、この PXE サービスがパッシブか。つまり、設定された MAC アドレスからの要求にのみ応答するか。また、この PXE サービスが信頼できるか。つまり、管理対象/スキャン対象の MAC アドレスがデプロイメントサーバの PXE サービスの MAC アドレスと競合しないか。
- PXE サービスが 2 つある場合、DHCP サービスが存在するマシンには PXE サービスをインストールしてはなりません。

そうしないと、その PXE サービスしかクライアントから見えなくなります。



## 5. ユーザ管理

ServerView Operations Manager V5.00 以降では、包括的なユーザ管理が導入されています。このユーザ管理は常にディレクトリサービスに基づきます。ServerView 製品をインストールするときに、ユーザは目的に合った既存のディレクトリサービスを使用するか、ServerView の組み込みディレクトリサービスを使用するかを選択します。ディレクトリサービスを使用すると以下のようなさまざまな利点があります。

- 実ユーザの個人識別情報 - 明確でないローカルアカウントの代わりに個人識別情報を使用できます。
- 中央でのユーザの権限の管理 - ユーザの権限を一元的に定義します。
- ユーザとサーバ管理を分離 - サーバ管理者は、ディレクトリサービスデータを変更する権限がなければ、ユーザの権限を変更できません。

ServerView 製品では、ユーザの認証と許可の両方のためにディレクトリサービスを使用します。

- 認証ではユーザの識別情報を定義します：「ユーザが誰であるか」
- 許可ではユーザの権限を定義します：「ユーザに何が許可されるか」

### 5.1. 中央認証サービスとシングルサインオン

各種 ServerView 製品には固有の Web サーバまたはアプリケーションサーバが含まれ、そのすべては管理者権限を許可する前に個々にユーザの識別情報を定義する必要があります。そのため、ある製品の Web ページから別の製品の Web ページへ移動するたびに、ユーザは自分の資格情報を繰り返し発行する必要があります。このような動作が望ましくないため、ServerView Operations Manager V5.00 以上にはいわゆるシングルサインオン（SSO）機能が導入されました。SSO では、ユーザは一度認証を受けるだけでどの Web ベースの ServerView インターフェースへもアクセスでき、その他の操作は不要です。ServerView では、中央認証サービス（CAS）を使用して SSO メカニズムを実装し、ユーザからは完全に見えない形で、シングルサインオン手順を処理します。CAS はユーザの識別情報をブラウザのセキュアな Cookie に保存します。Cookie は、ユーザが明示的にログアウトするか、ブラウザを閉じると削除されます。これは、無人ブラウザセッションによって重大なセキュリティギャップが生まれることを意味します。

#### Recommendation 16

PC の前を離れる場合は、必ずログアウトしてブラウザを閉じてください。

### 5.2. 統合ロールベースのアクセス制御（URBAC）

ServerView Suite のユーザ管理は統合ロールベースのアクセス制御（URBAC）に基づいているため、ユーザのセキュリティコンセプトとユーザの組織構造を連携させることができます。

#### 5.2.1. ユーザ、ユーザ役割、権限

RBAC では、ユーザに対応する権限を直接割り当てる代わりに、ユーザ役割を使用してユーザへの権限の割り当てを制御します。

- 一連の権限が各ユーザ役割に割り当てられます。各権限セットでは、ServerView Suite のアクティビティにタスク指向の権限プロファイルを定義します。
- 1 つまたは複数の役割が各ユーザに割り当てられます。

ユーザ役割の概念には、以下のような重要な利点があります。

- 各々のユーザまたはユーザグループに、個別に許可を割り当てる必要がない。その代わりに、許可はユーザロールに従って割り当てられる。
- 許可の構造が変更された場合のみ、ユーザ役割の許可を調整する必要がある。

### 5.2.2. ユーザ役割の割り当て

使用するディレクトリサービスによって、複数の役割を各ユーザに割り当てることができます。この場合、このユーザへの権限は、割り当てられたすべての役割のすべての権限を組み合わせで定義されます。事前に定義された、Monitor、Operator、Administrator という名前の 3 つのユーザ役割があります。個々のユーザ役割によって付与される許可の範囲は、低い方から Monitor（最低許可レベル）、Operator、Administrator（最高許可レベル）です。Operations Manager にアクセスするときの役割ベースの許可については、『ServerView でのユーザ管理』マニュアルの操作と対応する必要な役割の表で、ユーザへの適切な役割の割り当てについて参照してください。

#### Recommendation 17

『ServerView でのユーザ管理』マニュアルの操作と対応する必要な役割の表「Operations Manager へのアクセスに関する役割ベースの許可」で、ユーザへの適切な役割の割り当てについて参照してください。

#### Recommendation 18

必要な操作を許可する最小限の権限を持つ役割を割り当ててください。

## 6. 管理対象サーバ上の ServerView Agents と CIM Provider

本章では、ServerView 管理用サーバからエージェントノードまたは管理対象サーバへの複数の通信パスにおけるセキュリティの問題について説明します。ServerView 管理用サーバは、次の管理対象ノードで実行中の複数のコンポーネントに接続することができます。

- PRIMERGY サーバ、PRIMERGY サーバブレード、または仮想サーバ（ホストマシンおよびゲストマシン）のターゲット OS 上で実行する SNMP エージェント。リモートマネジメントコントローラ（iRMC）またはブレードサーバのリモートマネジメントボードで実行する SNMP エージェントについては、9 章「SNMP Agents for out-of-band management」を参照してください。
- CIM XML または WS-MAN プロトコルスタックを使用する CIM Provider
- SOAP ベースの ServerView コネクタサービス

ServerView を使用してシステムを管理するには、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て、それらを SNMP 経由でこの情報の要求元である Operations Manager や Event Manager へ送信します。

SNMP サービスを、管理対象サーバとマネージャ（Operations Manager や Event Manager など）の側にインストールする必要があります。本章では、管理対象サーバにのみ着目します。

ESXi サーバの管理については、ServerView CIM Provider を ESXi にインストールする必要があります。

### 6.1. SNMP サービス

SNMP は幅広く利用され、一般に受け入れられている管理プロトコルです。SNMP v1 と SNMP v2c はセキュアではなく、暗号化機能がありません。代わりに SNMP v3 を使用することを検討してください。しかしながら、SNMP サービスを適切に設定すると、基本的なセキュリティ機能を実現できます。デフォルト設定の使用は避けてください。

管理対象ノードでデフォルト設定を変更するときに、マネージャサイトの設定も変更することを忘れないでください。

#### Recommendation 19

SNMP サービスのデフォルト設定を変更します。詳細は、以下を参照してください。

SNMP サービスのパラメータは、OS の実装によって異なる可能性があります。OS 別のインストールと設定の詳細については、『ServerView – Installation under Windows』および『ServerView – Installation under Linux』マニュアルに記載されています。使用可能な場合、以下のパラメータを次の規則に従って設定してください。

SNMP 要求を受け付けるためのコミュニティ文字列: コミュニティ文字列は、マネージャからエージェントへ送信される各 SNMP 要求の一部です。SNMP の唯一の認証メカニズムで、暗号化されません。暗号化されることが問題になることもありますが、デフォルトのコミュニティ文字列「public」は、多数の SNMP デバイスで使用されます。そのため、パスワードに適用される規則に従って変更してください。エージェントサイトでデフォルトのコミュニティ文字列を変更する場合、マネージャサイトのコミュニティ文字列のデフォルト設定も変更する必要があります。原則的に、各サーバまたはサーバグループに個々のコミュニティを使用できます。

コミュニティ文字列は、読み取り専用、読み書きなどの権限に関連付けられます。ServerView の機能をすべて使用する場合、「読み書き」権限を使用する必要がありますが、エージェントの機能を「読み取り専用」の操作に制限することもできます。

注意: Operations Manager は、SNMP 要求に対して 1 つのコミュニティしかサポートしません。そのため、読み取り専用「public」、読み書きに「secret」のように 2 つのコミュニティを設定しないでください。

選択したサーバ/任意のサーバからの SNMP パケットを受け付ける: ここでは、管理アプリケーションと、使用する場合はデプロイメントサーバの IP アドレスを明示的に定義します。これにより、エージェントが、マネージャがインストールされているサーバ以外のサーバから SNMP 要求を受け取らないようにします。

注意: この場合、管理アプリケーションの IP アドレスは、DHCP 経由では届きません。

トラップ送信先: ここでは、トラップを受信する管理アプリケーションが常駐するシステムの IP アドレスを明示的に指定します。

注意: 管理アプリケーションの IP アドレスは、DHCP 経由では届きません。

トラップを送信するためのコミュニティ文字列: ここでは、SNMP トラップの一部として管理アプリケーションへ送信するコミュニティ文字列を指定します。このコミュニティ文字列を使用してトラップを受け入れるように管理アプリケーション側の SNMP サービスを設定します。

SET 要求の有効化/無効化: SNMP サービスの実装の中には、SNMP SET 要求の実行を有効または無効にできるものがあります。ここで再び、ServerView 機能をすべて使用する場合は無効にしてください。この場合、「SNMP SET 操作に関する ServerView のセキュリティコンセプト」も適用します。一般的にセキュリティ上の理由から SNMP SET 操作を無効にする場合、これに応じて SNMP サービスを設定できます。

### 6.1.1. SNMP v3

SNMPv3 プロトコルはセキュリティモデルをサポートし、古いコミュニティベースの疑似認証に代わって、暗号化によって通信プライバシーを提供する新しいコンセプトを定義します。

AES および DES のような Privacy Crypto アルゴリズムでは、Kerberos v5 のような RSA-MD5 および des3-cbc-SHA1 ハッシュアルゴリズムを使用する認証は、SNMPv3 でユーザープライバシーとユーザー認証アクセスコントロールを保証するためのオプションです。USM (User Security Model) の属性があり、iRMC の Net-SNMP パッケージで使用できます。

### 6.1.2. MMB と CPU ブレード間の通信

ブレードサーバが管理対象システムの場合、1 つの SNMP エージェントがマネジメントブレード (MMB) で実行され、もう 1 つの SNMP エージェントがサーバブレードで実行されます。ServerView マネージャは、両方のタイプの SNMP エージェントと通信します。原則的に、MMB エージェントと個々のサーバブレードエージェントに異なる SNMP コミュニティを設定できます。それに応じてマネージャを設定すると、マネージャとエージェント間の通信は問題なく行われます。

別々のサーバブレードを別々のクライアントへ割り当てる場合、あるクライアントが別のクライアントのサーバブレードの情報を取得しないように、各クライアントのサーバブレードには異なるコミュニティを使用する必要があることがあります。この場合、MMB を使用する別のクライアントのサーバブレードの情報を、クライアントが取得しないようにする必要もあります。

## 6.2. ServerView Agents

SNMP v1/SNMP v2c の唯一の認証メカニズムはコミュニティ文字列です。SNMP v1 は暗号化をサポートしていないので、クリアテキストとして転送されます。そのため、SNMP SET 操作は危険とみなされることがあります。しかし、ServerView では SNMP サービスの設定に加え、「SNMP SET 操作に関する ServerView のセキュリティコンセプト」を提供します。このコンセプトは、SNMP SET 操作の 3 つのオプションで構成されます。

- 特定の SET 操作を禁止する
- すべての SET 操作を禁止する
- ユーザ認証を使用して SET 操作を保護する

オプションは、『ServerView – Installation under Windows』および『ServerView – Installation under Linux』マニュアルの説明に従って設定できます。

これらのオプションによる SET 操作の禁止は、ServerView エージェントへのみ適用されます。他の SNMP エージェントの SET 操作には影響がありません。

「Protecting SET operations with a user authentication」オプションは、以下のように機能します。ServerView エージェントをインストールするときに、ユーザグループ（ローカルまたはドメイン）を指定します。ServerView Manager は SNMP SET 操作を管理対象ノードに送信する前に、管理者にアカウント（名前とパスワード）の入力を求めます。ServerView Manager は SNMP 経由でエージェントに、エージェントのインストールで指定されたアカウントを求めます。この情報は、SNMP 転送時に弱く暗号化されます。Server Manager は、エージェントから受信したアカウントが管理者が入力したアカウントと一致した場合のみ、SNMP SET 要求を送信します。

このユーザ認証は、ServerView マネージャでのみ使用できます。他の SNMP ツールでは使用できません。

### Recommendation 20

エージェントのインストール時に、認証用に Operations Manager で使用するユーザグループを指定してから、エージェントへ SNMP SET 要求を送信します。

Operations Manager V5.00 以降では、ほとんどの SET 操作が除外され、該当する機能は Server Configuration Manager に移されています。Server Configuration Manager には完全な RBAC 保護があります（ServerView Remote Connector Service による、SSL 暗号化された通信）。残りの SET 操作は RBAC 権限によって保護されます（SET 要求は、認証されたユーザに適切な権限が付与されている場合のみ送信されます）。

## 6.3. IPSec を使用した SNMP メッセージのセキュリティ保護

上述したように、SNMP v1 は暗号化を使用しません。これによるセキュリティ欠如は、すべての SNMP エージェントとマネージャに IPSec ポリシーを設定することにより回避されます。これにより、悪意のあるユーザやサイバー攻撃者が SNMP メッセージを受信できなくします。

ただし IPSec は SNMP トラフィックを自動的に暗号化しません。SNMP マネージャとエージェント間のトラフィック用の適切なフィルタリストに、フィルタ仕様を作成する必要があります（表「通信パス」も参照）。

### Recommendation 21

SNMP v1 の暗号化の欠如を回避する必要がある場合は、IPSec を使用して SNMP メッセージのセキュリティを確保します。

## 6.4. ServerView CIM Provider

### 6.4.1. ServerView ESXi CIM Provider

VMware ESXi にはコンソール OS がなく、SNMP もサポートされません。そのため、ServerView Agents for Linux を使用できません。

VMware ESXi システムの監視は、Management Task Force (DMTF) によって定義された共通情報モデル (Common Information Model : CIM) に従ってのみ可能です。CIM-XML は、管理対象サーバと管理用サーバ間のデータ交換に使用されます。

ServerView ESXi CIM Provider は、FTS から ESXi Installable および ESXi Embedded イメージで提供されます。オフラインバンドル (VIB ファイル (vSphere Installation Bundle ファイル) を含むオフラインバンドル) も、FTS のインターネットポータルサイトのサポートページからダウンロードできます。

VMware ESXi を ESXi Installable および ESXi Embedded イメージとともにインストールした後に、ServerView ESXi CIM Provider を

インストールして使用できます。さらに、オフラインバンドルを FTS のインターネットポータルサイトのサポートページからダウンロードした後、次のコマンドを使用して、すでにインストールされている VMware ESXi システムをアップデートすることができます。

`esxupdate` (ローカル)

`vihostupdate` (リモート)

どちらのコマンドについても、VMware のマニュアルで詳しく説明しています。

ServerView ESXi RAID Core プロバイダは、FTS から ESXi Embedded イメージとしても提供されます。上記で説明したオフラインバンドルによるインストールおよびアップデートも可能です。

ESXi システムから SV Operations Manager の監視情報を取得するには、「ESXi host」オブジェクトに対して「Administrator」役割を持つ任意のユーザを ESXi システムで作成してください。

VMware のマニュアル『ESXi Configuration Guide』 (<https://docs.vmware.com/en/VMware-vSphere/6.5/vsphere-esxi-vcenter-server-65-installation-setup-guide.pdf>) からダウンロード可能) の「Security」の章に、その他の役に立つ情報が記載されています。

### 6.4.2. Windows 用 ServerView CIM Provider

ServerView CIM Provider は、「ServerView Agent & CIM Providers for Windows (x64)」パッケージの一部として提供されます。Microsoft の WMI を使用可能な CIM クラスへのローカルアクセスには、Microsoft WSMAN を通じてリアルタイムモジュールとアクセスできます。

CIM Provider にアクセスするクライアントは管理者になるか、ServerView Agents のインストール時に作成されたユーザグループに属する必要があります。

### 6.4.3. Linux 用 ServerView CIM Provider

CIM Provider を実行するには、CIMOM (CIM Object Manager) サービスを使用できます。サポートされる CIMOM は、SFCB および OpenPegasus です。CIM Provider には、サーバで「ルート」ユーザとしてのみアクセスできます。



## 6.5. ServerView Connector Service

略称 SCS です。ServerView Remote Connector Service と呼ばれます。

これは、SSL および非 SSL 呼び出しに 1 つのポート番号 (3172) を使用する TCP/IP Web サービスで、複数のエージェントプロバイダライブラリを処理できます。これは、FUJITSU LIMITED が所有する特許に基づく汎用サービスです。

インターフェースは SOAP (および診断呼び出しの場合は CGI に類似する呼び出し) および REST です。SCS にはさまざまなセキュリティピックが集約されます。呼び出されたエージェントプロバイダライブラリでは、どの操作にどのセキュリティを使用するかを指定できます。

以下を使用できます。

- セキュリティなし - 汎用ユーザで読み取りおよび作業可能
- 簡単な認証 (ユーザ ID/パスワード/..) (認証データの内部暗号化)
- HTTP 認証、HTTP ダイジェスト認証 (該当する暗号化を使用)
- SSL 標準の使用 (標準 SSL 暗号化)
- WS-Security の部分および使用している WS-Security インターセプタ技術でトークン (RBAC/SSO など) を検証 (SSL 暗号化を組み合わせた RBAC の場合)
- 呼び出し側の SSL 証明書送信による、証明書ベースのアクセス制御検証、およびチェック。

最後の 2 つの点については、CA 証明書と、SCS のトラストストアにある信頼される管理用サーバの該当する設定ファイル (pki ディレクトリ内のこれらのファイルのコピー) が必要です。

これを行うには、『ServerView でのユーザ管理』マニュアルの「RBAC およびクライアント認証用の管理対象ノードの準備」の項を参照してください。

管理対象ノードの管理者は、この管理対象ノードが信頼する対象を指定します。

## 6.6. ServerView System Monitor

ServerView System Monitor は、HTML5 ベースの Web アプリケーションです。このアプリケーションは、HTTPS と管理対象ノードにインストールされている ServerView Remote Connector との接続を確立します。

Remote Connector クライアントアクセスは、管理者ユーザのみ、またはエージェントの設定または ServerView Agents のインストール時に指定されるユーザグループメンバーに制限される可能性があります。



## 7. 管理 (Operations Manager)

### 7.1. SNMP サービス

管理対象ノードでの SNMP サービスの設定と同様に、中央管理用サーバには 2 つの設定が必要です。

- Operations Manager、Event Manager、Win32 ベースの ServerView サーバを中央管理用サーバにインストールする前に、SNMP サービスをインストールして、エージェントから SNMP トラップを受信するように設定する必要があります。この設定は、管理対象ノードの SNMP サービスの設定と一致する必要があります (Recommendation 19: 「トラップ送信先」および「トラップを送信するためのコミュニティ文字列」を参照)。
- 中央管理用サーバへのインストール後、各管理対象サーバまたは管理対象サーバグループに SNMP サービスを設定する必要があります。つまり、中央管理用サーバが SNMP 要求を管理対象サーバのエージェントへ送信するときに使用するコミュニティ文字列です。これは、Recommendation 19 のアクション「SNMP 要求を受け付けるためのコミュニティ文字列」に対応して行う必要があります。

ServerView Agents と中央管理用サーバは、SNMP 経由で通信します。SNMP は暗号化もセキュアな認証も提供しないので、ServerView マネージャと ServerView Agents をファイアウォールの内側にインストールすることを推奨します。SNMP がファイアウォールを越えないように設置してください。

#### Recommendation 22

中央管理用サーバと ServerView Agents の両方を、SNMP 通信を保護するファイアウォールの内側にある管理対象サーバにインストールしてください。

### 7.2. Operations Manager 環境への Web サーバのインストール

Operations Manager の大きな利点は、イントラネットのファイアウォールの内側で実行できるにもかかわらず、どこからでも、インターネットアクセス可能な任意の Web ブラウザで管理ツールにアクセスできる点です。

ただし、セキュリティ上の見地から、アプリケーションサーバをインストールすることで、既存の構成にセキュリティホールが生じる可能性があります。次の 3 つの理由があります。

- アプリケーションサーバ自体に、検出されていないセキュリティ欠陥が含まれている可能性がある。
- Web サーバで実行中のアプリケーションソフトウェアにセキュリティホールがある可能性がある。
- アプリケーションサーバをインストールするディレクトリが書き込みアクセスに対して十分にセキュリティ保護されていない場合、CMS の非管理者ユーザが、アプリケーションサーバまたはアプリケーションの有害な動作を発生させる可能性がある。

お客様としてのユーザは、開発および品質保証プロセスをくぐり抜けたこのようなエラーには当然対処できません。ただし、所定のルールに従えば、このようなエラーの影響を最小限に抑えることができます。

まず、CMS 上の Web サーバとそのアプリケーションソフトウェアへのアクセス権をできる限り制限します。このためには、アプリケーションサーバ (TomEE) を実行するための最小限のアクセス権を持つユーザアカウントを作成することを推奨します。

このアカウントは、Operations Manager のインストール中に、アプリケーションサーバを実行させるためのアカウントを求められたときに指定します。この目的で、非管理者アカウントを作成し、他のアカウントがそのデータにアクセスできないようにすることを強く推奨します。

## Recommendation 23

ServerView Operations Manager と共にインストールされているアプリケーションサーバ専用の非管理者アカウントを作成します。アカウントのこのセキュリティ設定により、すべての非管理者ユーザがアプリケーションサーバのアカウントのディレクトリおよびファイルの読み取りまたは書き込みをできないようにします。

### 7.3. Operations Manager の SSL 証明書の交換

SSL 証明書の交換については、『ServerView でのユーザ管理』マニュアルの 4.2.4 項の「中央管理用サーバ（CMS）での証明書の交換」を参照してください。このマニュアルは、[Manuals Download Page](#) からダウンロードできます。

### 7.4. Operations Manager 向け TLS/SSL 暗号スイートの制限

暗号スイートは、認証、暗号化、メッセージ認証コード（MAC）アルゴリズムの名前付き組み合わせで、Transport Layer Security（TLS）または Secure Sockets Layer（SSL）ネットワークプロトコルを使用して、ネットワーク接続のセキュリティ設定のネゴシエートに使用されます。暗号スイートのコンセプトの構造と使用方法は、プロトコルを定義する文書（TLS バージョン 1.2 の [RFC 5246](#) 規格）で規定されています。指定された暗号スイートへの参照は、[RFC 2434](#) の TLS 暗号スイートレジストリで規定されています。

TLS 接続が確立されると、TLS ハンドシェイクプロトコルと呼ばれる \_\_\_\_\_ が実行されます。このハンドシェイク中に、ClientHello と ServerHello メッセージが交信されます。（[RFC 5246](#)、p. 37）まず、クライアントが暗号スイートリストを送信します。これは、クライアントがサポートする暗号スイートを、優先する順序で並べたリストです。次にサーバが、クライアントの暗号スイートリストから選択した暗号スイートを返信します。（[RFC 5246](#)、p. 40）サーバがサポートする TLS 暗号をテストするために、SSL/TLS スキャナを使用できます。」（引用：『フリー百科事典 ウィキペディア日本語版』より。）

暗号化アルゴリズムには強弱があるため、暗号スイートの強度もさまざまです。したがって、Web サーバが提供する TLS/SSL 暗号スイートの強度を確認することは、いわゆる「脆弱性スキャナ」の行うタスクの一部となっています。脆弱性スキャナは、コンピュータ、コンピュータシステム、ネットワーク、またはアプリケーションの弱点にアクセスするために使用されるツールです。通常、ソフトウェアベンダはセキュリティ面について自社製品の強度を可能な限り高めて、脆弱性スキャンによってどの製品にもエラーが発生しないよう常に努めています。しかし、TLS/SSL 暗号スイートを適用されると、クライアントは脆弱性スキャナによって弱いと判断された暗号スイートのみを提供するため、安全な接続を確立できなくなります。このため、一部の ServerView 製品では暗号スイートの使用を制限しませんが、適用についてはユーザの判断に任せています。

当然ながら、最も優れた SSL は、最新の SSL プロトコルバージョン（TLSv1.2）のみ許可し、暗号スイートを現在の規格に従って安全であると見なされる暗号スイートに制限する構成です。ただし、SSL プロトコルバージョン TLSv1.2 も、直前の TLSv1.1 も、Operations Manager に接続可能なシステムのすべてに対して前提とすることはできません。そのため、現在のすべての OM バージョンにおける SSL デフォルト構成では、追加の TLSv1.0 を許可します。ただし、このプロトコルは、「CBC」（Cipher Block Chaining）モードの暗号スイートと共に使用する場合、「BEAST」攻撃に対して脆弱になります。残念ながら、Java 7 でサポートされるすべての暗号スイートは、CBC モードタイプであるか、RC4 タイプの暗号スイートのように他の理由で安全でないと見なされるため、Java 7 ベースの OM バージョンには代替がありません。

その結果、Operations Manager を TLSv1.0 を使用して構成する場合は、絶対安全な SSL 構成は不可能になります。ただし、BEAST 攻撃はセッションクッキーの取得を許可するだけで、データ交換全体の複合化を許可しないうえ、中間者攻撃および特別に変更されたクライアントプログラムを構成するには多大な労力を要します。そのため、Fujitsu では、このタイ

プの攻撃のリスクは、従来の暗号化攻撃よりもはるかにリスクが少ないと判断しています。このアプローチに従う「比較的」安全な構成について、次に説明します。これは、Operations Manager バージョン 6.10 以降で有効です。それらのバージョンでは、以下のように構成を変更することで、暗号スイートを制限できます。

#### (A) Operations Manager バージョン 7.10 以前：

- (1) テキストエディタを使用して次のファイルを開きます。

<ServerView Suite>\jboss\standalone\configuration\standalone.xml.orig on Windows, resp. /opt/fujitsu/ServerViewSuite/jboss/standalone/configuration/standalone.xml.sav on Linux  
XML セクション <subsystem xmlns="urn:jboss:domain:web:1.1" ...> を探して、属性 cipher-suite を XML タグ <ssl ...> に追加します。以下に例を示します。

```
<subsystem xmlns="urn:jboss:domain:web:1.1" default-virtual-server="default-host" native="false">
  <connector name="http" protocol="HTTP/1.1" scheme="http" socket-binding="http"/>
  <connector name="https" protocol="HTTP/1.1" scheme="https" socket-binding="https" secure="true">
    <ssl name="https" password="changeit" certificate-key-file="../../standalone/svconf/pki/keystore" cipher-suite="TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_EMPTY_RENEGOTIATION_INFO_SCSV" protocol="SSLv2" verify-client="false"/>
  </connector>
  <virtual-server name="default-host" enable-welcome-root="false"/>
</subsystem>
```

protocol=SSLv2 では、実際には SSL バージョン 2 ではなく、TLSv1.0 + TLSv1.1 + TLSv1.2 の組み合わせが指定されます。

効率的に TLSv1.1 + TLSv1.2 の組み合わせのみ有効にする protocol=TLSv1 を試してみるのも得策です。この構成で接続に関する問題が発生しない場合は、BEAST 攻撃に対しても絶対に安全なため、この構成を維持してください。

- (2) テキストエディタを使用して、Windows では <ServerView Suite>\opends\config\schema\02-config.ldif、Linux では /opt/fujitsu/ServerViewSuite/opends/config/schema/02-config.ldif を開きます。

objectclasses 宣言を ds-cfg-administration-connector に変更して、MAY 行を以下のようにします。

```
MAY ( ds-cfg-listen-address $ ds-cfg-ssl-cipher-suite $ ds-cfg-ssl-protocol )
```

- (3) Operations Manager バージョン 7.10 以前の場合は、ServerView ディレクトリサービス (OpenDJ) の構成も変更する必要があります。

テキストエディタを使用して、Windows では <ServerView Suite>\opends\config\config.ldif、Linux では /opt/fujitsu/ServerViewSuite/opends/config/config.ldif を開きます。

使用するすべての暗号スイートに対して、属性 ds-cfg-ssl-cipher-suite と ds-cfg-ssl-protocol をエントリ cn=LDAPS Connection Handler, cn=Connection Handlers, cn=config に追加します。以下に例を示します。

```
dn: cn=LDAPS Connection Handler,cn=Connection Handlers,cn=config
objectClass: ds-cfg-ldap-connection-handler
...
ds-cfg-use-ssl: true
ds-cfg-ssl-cipher-suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA
ds-cfg-ssl-cipher-suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
ds-cfg-ssl-cipher-suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
ds-cfg-ssl-cipher-suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
ds-cfg-ssl-cipher-suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
ds-cfg-ssl-cipher-suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
```

```
ds-cfg-ssl-cipher-suite: TLS_EMPTY_RENEGOTIATION_INFO_SCSV
ds-cfg-ssl-protocol: TLSv1
ds-cfg-use-tcp-keep-alive: true
```

同じ設定ファイルで、エントリ

dn: cn=Administration Connector,cn=config の属性 ds-cfg-listen-address を 0.0.0.0 から 127.0.0.1 に変更します。

```
dn: cn=Administration Connector,cn=config
objectClass: ds-cfg-administration-connector
objectClass: top
ds-cfg-listen-address: 127.0.0.1
ds-cfg-listen-port: 4444
cn: Administration Connector
ds-cfg-key-manager-provider: cn=Administration,cn=Key Manager Providers,cn=config
ds-cfg-ssl-cert-nickname: svcs_cms
ds-cfg-trust-manager-provider: cn=Administration,cn=Trust Manager Providers,cn=config
```

Operations Manager バージョン 7.10 の場合は、ServerView ディレクトリサービスは ApacheDS に変更されています。残念ながら、このディレクトリサービスの SSL 構成を構成で変更することはできません。

- (4) Windows で、サービス「ServerView JBoss Application Server 7」を、コントロールパネルから、または以下のコマンドラインから再起動します。

```
%WINDIR%\system32\net.exe stop "SVJBASSVC"
%WINDIR%\system32\net.exe start "SVJBASSVC"
```

Linux で、以下のコマンドラインで ServerView JBoss デーモンを再起動します。

```
/etc/init.d/sv_jboss restart
```

## (B) Operations Manager バージョン 7.10 より後：

- (1) テキストエディタを使用して、Windows では <ServerView Suite>\tomee\conf\server.xml、Linux では /opt/fujitsu/ServerViewSuite/tomee/conf/server.xml を開きます。  
XML セクション <Connector port="3170" ...> を探して、属性 ciphers を追加します。以下に例を示します。

```
<Connector port="3170" protocol="org.apache.coyote.http11.Http11NioProtocol"
  maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
  clientAuth="false"
  sslEnabledProtocols="SSLv2Hello,TLSv1,TLSv1.1,TLSv1.2"
  ciphers="TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_
  SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_
  CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_
  CBC_SHA256,TLS_EMPTY_RENEGOTIATION_INFO_SCSV"
  keystoreFile="svconf/pki/keystore" keystorePass="changeit"
  truststoreFile="svconf/pki/cacerts" />
```

TLSv1.1 + TLSv1.2 の組み合わせのみ有効にする、

sslEnabledProtocols="SSLv2Hello,TLSv1.1,TLSv1.2" を試してみるのも得策です。この構成で接続に関する問題が発生しない場合は、BEAST 攻撃に対しても絶対に安全なため、この構成を維持してください。

- (2) Operations Manager バージョン 7.11 の場合は、ServerView ディレクトリサービスは ApacheDS に変更されています。残念ながら、このディレクトリサービスの SSL 構成を構成で変更することはできません。

Operations Manager バージョン 7.20 以降の場合、ServerView ディレクトリサービスは自動的に TomEE の構成を採用します。

- (3) Windows の場合、サービス「ServerView ApplicationService」を、コントロールパネルから、または以下のコマンドラインから再起動します。

```
%WINDIR%\system32\net.exe stop "SVTomEE"  
%WINDIR%\system32\net.exe start "SVTomEE"
```

Linux の場合、以下のコマンドラインで ServerView ApplicationService デーモンを再起動します。

```
/etc/init.d/sv_jboss restart
```

#### 7.4.1. BEAST 攻撃に対抗する暗号スイート設定

前述したように、SSL プロトコルバージョン TLSv1.0 と共に使用する場合、BEAST 攻撃に対して安全である Java 7 で使用可能な、安全な暗号スイートが現在ありません。（暗号スイート SSL\_RSA\_WITH\_RC4\_128\_MD5 and SSL\_RSA\_WITH\_RC4\_128\_SHA のみ BEAST に対して安全とされていますが、これらは RC4 ベースのため、最近では安全でないと思われています）Java 7 によって提供される「優れた」暗号スイートはすべて CBC モードタイプのため、少なくともプロトコルバージョン TLSv1.1 を構成し、その構成から TLSv1.0 を実行する必要があります。

#### 7.4.2. Operations Manager バージョン 8.00 以降のセキュリティ設定

バージョン 8.00 以降の Operations Manager は、前のバージョンと異なるテクノロジーを使用して、クライアントサーバにユーザインターフェースを提供します。新しいフロントエンドは、WebStart（Web ブラウザを使用せずに Java アプレットを実行する Oracle のテクノロジー）アプリケーションの形式なので、Web ブラウザは、Webstart アプリケーションへの開始点である .jnlp ファイルのダウンロードにのみ使用されます。新しいテクノロジーが導入された結果、Java 8 はそれらの Operations Manager バージョンでのみサポートされます。

Java 8 はより多くの暗号セットのサポートを提供するため、設定をシンプルに維持するために、セキュリティレベル選択ダイアログが Operations Manager インストール中に提供されます。このダイアログを使用すると、管理者は 3 つの事前定義されたレベルのいずれかを選択して、セキュリティ設定を自分のニーズに合わせて簡単に調整できます。「Modern」レベルでは、出荷時のまま最高の保護を提供する一方、他の 2 つのレベルはレガシーアプリケーションとの互換性を提供するように設計されており、特定のビジネスケースによって、最新のセキュリティ標準をサポートしない Server View Suite の一部の旧式コンポーネントをやむを得ず使用しなければならない場合のみ使用します。

「Modern」レベルが十分にセキュアでないまれなケースにおいては、TLSv1.2 以外のプロトコルのサポートを手動で無効にすることができます。このような場合は、付属のソフトウェア（SV Agents など）も導入して TLSv1.2 を使用する必要があります。Windows の Microsoft ODBC ドライバの一部のバージョンに関する既知の問題があり、システム管理者が処理する必要があることも注意してください。（このような場合は最新バージョンへのアップデートが必要です。または、解決策としては、FIPS 互換性モードをオンにします。詳細については、次のリンクを参照してください：

<https://dba.stackexchange.com/questions/93127/sql-server-service-won-t-start-after-disabling-tls-1-0-and-ssl-3-0>)

純粋な TLSv1.2 構成を実行するには、次の手順に従います。

1. インストール時に「Modern」セキュリティ設定を選択します。
2. インストール後に、テキストエディタを使用してファイル <install\_dir>/tomee/conf/server.xml を変更します。
  - 2.1. 「<Connector port="3170"」で始まる行を探します。
  - 2.2. 属性 sslEnabledProtocols= で、TLSv1.2 以外のすべてを削除します。
  - 2.3. 変更内容を保存します。



### 3. テキストエディタを使用してファイルを変更します：

```
<install_dir>/apacheds/instances/default/conf/ou=config/ads-  
directoryserviceid=default/ou=servers/ads-serverid=ldapserver/ou=transport/ads-  
transportid=ldaps.ldif:
```

3.1. TLSv1.2 以外のプロトコルに関しては、ads-enabledProtocols: で始まるすべての行を削除します。

3.2. 変更内容を保存します。

### 4. Operations Manager サービス（または可能であればサービス全体）を再起動します。これ以降、Operations Manager 全体で通信には TLSv1.2 のみ使用してください。

## Recommendation 24

可能な限り、Operations Manager のインストール/アップグレード時には「**Modern**」セキュリティを選択します。やむを得ない場合を除き、上記の手動での変更は使用しないでください。

### 7.4.3. Operations Manager バージョン 9.00 以降のセキュリティ設定

バージョン 9.00 以降の Operations Manager は、前のバージョンと異なるテクノロジーを使用して、クライアントサーバにユーザインターフェースを提供します。新しいインターフェースは、ネイティブ HTML5 Web アプリケーションの形式です。アプリケーションサーバは、Operations Manager パッケージに含まれる AdoptOpenJDK で提供される Java 8 LTS バイナリで実行します。

Operations Manager のバージョン 8 以降では、セキュリティと暗号の設定は、インストール/アップグレード手順の間に管理されます。次の 3 つのセキュリティレベルがあります。

- Modern (TLSv1.2)
- Intermediate (TLSv1.2, TLSv1.1, TLSv1.0)
- Old (TLSv1.2, TLSv1.1, TLSv1.0, SSLv3)

インストール後にセキュリティ設定を変更するには、（Windows の「プログラムと機能」ユーティリティで）FUJITSU Software ServerView アプリケーションサーバの変更インストールを実行するか、Linux で

```
<install_dir>/svom/ServerView/Tools/ChangeComputerDetails.sh スクリプトを実行して、適切なセキュリティ設定を選択します。
```

## 7.5. ユーザ認証を使用する 設定操作

ユーザ認証を使用して設定操作を保護するために、管理対象サーバへのエージェントのインストール時にパスワード認証を有効にしていた場合（Recommendation 23）、ユーザ名とパスワードの入力を求めるプロンプトが表示されることがあります。この場合、指定した ServerView ユーザグループまたは管理者グループに属するユーザアカウントのアカウントデータを入力する必要があります（エージェントの設定によって異なります）。

## 7.6. Event Manager とアンチウイルスプログラム

電子メールで管理者にイベントを報告するように、Event Manager を設定できます。アンチウイルスプログラムを Alarm Service がインストールされている中央管理用サーバで実行する場合、このアンチウイルスプログラムによってアラームサービスの電子メール送信が妨害されることがあります。アラームサービスが電子メールを送信できるようにするには、このアンチウイルスプログラムの設定によって、以下のプロセスで電子メールを送信できるようにする必要があります。

- Windows: blat.exe (SVOM 7.11 以前)、mail.exe (SVOM 7.11 およびそれ以降)
- Linux、Solaris : smtpm

## 7.7. 変更可能な SNMP ポート

デフォルトポート 161 および 162 を使用しないようにするには、以下の変更を行います。

管理対象ノード上の ServerView Agent Linux

CMS 上の ServerView Operations Manager Linux

SuSE (SLES) の場合も Red Hat (RHEL) の場合も、以下の変更を行う必要があります。

1. /etc/services ファイルで、以下のエントリを変更します。

- snmp の場合                      161 から <new port 1> (tcp と udp の両プロトコル)
- snmptrap の場合                162 から <new port 2> (存在する場合、tcp と udp の両プロトコル)

2. /etc/snmp/snmpd.conf ファイルでの作業

- プロトコル udp に対して snmp が使用する新しいポート <new port 1> を指定します。  
IPv6 を使用する場合は、プロトコル udp6 に対する新しいポートも指定します。

```
agentAddress udp:<new port 1> [,udp6:<new port 1>]
```

3. /etc/snmp/snmpd.conf ファイルでの追加作業

- ポート番号をアドレスに追加して、トラップ先に別のポートを指定します。  
trapsink            machine:<new port 2>            <community>

4. /etc/snmp/snmptrapd.conf ファイルでの作業

- プロトコル udp に対して snmptrap が使用する新しいポート <new port 2> を指定します。  
snmpTrapdAddr udp:<new port 2>

5. /var/net-snmp/snmp.conf ファイルでの作業

- snmp が使用するデフォルトポートを指定します。  
defaultPort <new port 1>



6. サービスを再起動します（または OS をリブートします）。

- [/sbin/] service snmpd restart
- [/usr/bin/] sv\_services restart
- [/usr/sbin/] srvmagt restart

これらのいずれかのファイルが存在しない場合は、権限 0644 のユーザー「root」として作成してください。

ディレクトリ /var/net-snmp に権限 0755 が付与されていることを確認します（一部の OS では、「group」および「other」の権限がなく、この場合は機能しません）。

その他の類似のディレクトリ（/var/lib/net-snmp など）やファイル名（snmp.conf/snmpd.conf など）と間違えないようにしてください。

## 管理対象ノード上の ServerView Agent Windows

1. <WINDOWSDIR>\System32\drivers\etc\services ファイルで、以下のようにエントリを変更します。

- snmp の場合                      161 から <new port 1>                      (udp プロトコル)
- snmptrap の場合                  162 から <new port 2>                      (udp プロトコル)

2. Agents と SNMP のサービスを再起動します。

- 以下の手順で、ServerView Agents を Agents Tool の「Restart Agents」で再起動します。  
「スタート」->「すべてのプログラム」->「Fujitsu」->「ServerView Suite」->「Agents」->  
「Diagnostic Tools」->「Restart Agents」

## CMS 上の ServerView Operations Manager Windows

1. 以下の変更を行う前に、以下の順序でサービスを停止します。

- ServerView ダウンロードサービス
- ServerView サービス
- SNMP サービス

2. <WINDOWSDIR>\system32\drivers\etc\services ファイルで、以下のようにエントリを変更します。

- snmp の場合                      161 から <new port 1> (udp プロトコル)
- snmptrap の場合                  162 から <new port 2> (udp プロトコル)

3. C:\usr\snmp\persist\snmp.0.conf ファイル（存在しない場合は、作成してください）で、以下の行を追加します。

- defaultPort <NewPort-1>

4. 以下の順序でサービスを再起動します。

- SNMP サービス
- ServerView サービス
- ServerView ダウンロードサービス

## 8. メンテナンス

メンテナンス用として、管理者の作業を軽減するためのアップデート管理および PrimeUp などの強力なツールが提供されています。

### 8.1. アップデート管理

PRIMERGY ServerView Suite のアップデート管理では、管理者は、サーバコンポーネントのファームウェアやソフトウェアをアップデートするための便利なオプションを使用できます。このタスクには、以下のツールを使用できます。

- Update Manager (Operations Manager に統合)

Update Manager は、グラフィカルユーザインターフェース (GUI) やコマンドラインインターフェース (CLI) により、BIOS、ファームウェア、ドライバ、および一部のサーバ管理製品について、ネットワーク経由でのアップデートを可能にします。中央管理用サーバを使用したスケジュールおよび制御により、複数のサーバを同時に自動的にアップデートできます。Update Manager は、中央管理用サーバに置かれる、アップデートリポジトリを利用します。このディレクトリは、最初に以下のいずれかの方法によって作成できます。

- 最新の ServerView Update DVD からインポート
  - 統合されているツール「Download Manager」を使用してインターネット経由で取得
- どちらの場合も、後で Download Manager を使用してリポジトリを最新の状態に維持できます。

- Update Manager Express および ASP (Autonomous Support パッケージ)

これらの製品は、各種サーバコンポーネントの BIOS とファームウェアをローカルでインストールおよびアップデートするために開発されています。

ASP は署名ファイルで提供され、整合性が確保されます。

- System Monitor の Update Function

System Monitor の Update Function では、System Monitor の GUI (Graphical User Interface) を使用して BIOS、ファームウェア、ドライバを確実にアップデートすることもできます。

System Monitor は、Operation Manager のドメインに統合する必要なく、サーバで自立的に動作します。

アップデートパッケージは次のいくつかの方法で入手できます。

- ServerView Update DVD
- Web で FTS サポートサイトからダウンロード
- カスタマネットワークにインストールされているリポジトリサーバーからダウンロード

System Monitor は、SV\_Agent パッケージに含まれています。

- PrimeUp および PSP (PRIMERGY Support Package)

PrimeUp では、PSP に基づいて、管理対象サーバでローカルにドライバソフトウェアと ServerView Agents を自動的にアップデートできます。

#### ■ iRMC S4/S5 のアップデート機能

iRMC S4/S5 の eLCM パッケージには、Online Update および Offline Update の機能が統合されています。これらの機能は、iRMC WebUI または REST スクリプティング API を使用して設定および起動することができます。eLCM パッケージを使用するには、サーバメインボードの SD カード、および有効な eLCM ライセンスもインストールする必要があります。

Online Update には、BIOS、ファームウェア、ドライバを確実にアップデート可能にするすべての機能が含まれています。SVAS（エージェントレスパッケージ）をサーバにインストールするだけで、サーバで SV\_Agent を実行する必要はありません。

アップデートパッケージは次のいくつかの方法で入手できます。

- Web で FTS サポートサイトからダウンロード
- カスタマネットワークにインストールされているリポジトリサーバからダウンロード

Offline Update には、BIOS および ファームウェアを確実にアップデート可能にするすべての機能が含まれています。サーバで SV\_Agent または SVAS（エージェントレスパッケージ）を実行する必要はありません。そのため、ESXI のインストールに最適です。

アップデートパッケージは次のいくつかの方法で入手できます。

- Web で FTS サポートサイトからダウンロード
- カスタマネットワークにインストールされているリポジトリサーバからダウンロード

不正アップデートはサーバに重大なダメージを及ぼす可能性があるため、ファームウェア、BIOS、ドライバのアップデートの操作は保護する必要があります。また、ほとんどの場合、システムはアップデートが正常終了した後再起動されるので、予期しないシステムのダウンタイムが発生することがあります。

Update Manager Express および PrimeUp などのローカルアップデートメカニズムが管理者権限を暗黙的に要求する一方で、中央集中型のアップデートサービス(Update Manager)は、ユーザの利便性を低下させることなく、この要件についてより注意を払う必要があります。

そのため、Update Manager では認証に対してさまざまなセキュリティメカニズムを提供します。V5.00 未満の従来のバージョンでは、ユーザ/パスワードベースのメカニズムを使用していましたが、V5.00 以降、「シングルサインオン」アクセスに証明書ベースの認証を使用する方法が推奨されています。

#### Recommendation 25

Update エージェントの初回インストール時に、あらかじめ管理対象サーバでユーザグループとユーザを作成してください。Update エージェントのインストール時に「セキュリティ設定」画面で「アカウントチェック」を選択し、作成しておいたグループを「アップデート用ユーザグループ」として使用します。インストール後に、関連する Update Manager の機能またはその他の方法で、CMS 固有の証明書を配布します。

これにより、関連する LDAP 設定の一部である GUI ユーザのみ管理者アクセス権限を付与されることが保証されます。何らかの理由で証明書プロセスが失敗した場合、エージェントはユーザ/パスワードモードへ自動的に切り替わります。これにより、管理対象ノードは管理可能な状態に維持され、保護されたモードのままとなります。

上述したように、Download Manager の目的は、管理用サーバのリポジトリを最新状態に維持することです。適切に設定した場合、Download Manager は新しいアップデートパッケージがないか Fujitsu Web サーバを定期的にチェックし、新しいパッケージを中央管理用サーバ（CMS）のアップデートリポジトリにダウンロードします。

指定された Web サイトからダウンロードされるファイルには、技術的な理由から署名されていないものがあります。バージョン 5.0 以降、ダウンロード中にこれらのファイルが改ざんされないように、セキュアな HTTPS プロトコルがサポートされています。

#### Recommendation 26

Download Manager 機能に対して、可能であれば HTTPS プロトコルを選択してください。

#### Recommendation 27

オペレーティングシステム VMWare ESXi、MMB、コネクションブレードを使用するシステムの BIOS/iRMC をアップデートする場合は、Configuration Manager で Plink を設定してください。これに関連して、Plink には主に次の 2 つの用途があります。

1. 管理対象ノードがメンテナンスモードであることを確認する
2. コネクションブレード FW を更新する

## 8.2. PrimeCollect

PrimeCollect は、インベントリ情報、OS の情報、センサデータ（温度の値など）、さまざまなログ（システムイベントログなど）、その他のサポートする関連データを収集するツールです。収集されるデータの種類と量は、システム構成によって異なります。すべての情報は、サービスエンジニアに送信できるように、自動的に .zip または .tar ファイルに追加されます。これによって、PrimeCollect を使用してサポートエンジニアは顧客の問題を分析し、解決策や回避策を練るのに必要な時間を短縮できます。

セキュリティ上の理由から、ユーザはこのアーカイブでサービスエンジニアに送信された情報を知ることができます。

『PrimeCollect』マニュアルには、アーカイブに含まれるファイルとその内容をまとめた表があります。ユーザのセキュリティポリシーによって異なりますが、アーカイブ内の特定ファイルを削除してからアーカイブを提供したり、アーカイブをまったく提供しないように対処することができます。

#### Recommendation 28

PrimeCollect で収集された情報を含む .zip アーカイブを提供する前に、このアーカイブをチェックして、セキュリティポリシーに要求される場合はその情報を削除することが可能です。『PrimeCollect』マニュアルには、この情報をまとめた表があります。

#### Recommendation 29

CA 証明書と関連する設定ファイルを処理する方法については、6.5 項の「ServerView Connector Service」を参照してください。

### 8.3. リポジトリサーバ

リポジトリサーバでは、分散方式でファームウェアコンポーネントのリポジトリを維持できます。リポジトリサーバソフトウェア製品を使用してインストールされる（仮想）マシンは、インターネットに接続されていない管理対象ノードを監視するブロキシサーバとして使用できます。リポジトリサーバを使用するダウンロードプロセスは、管理対象ノードのアップデートから完全に独立しています。管理者は、ダウンロードプロセスとエラー状況に関して電子メールメッセージを受け取ります。

リポジトリサーバに接続される管理対象ノードは、ファームウェアコンポーネントに必要なアップデートを受け取ります。リポジトリサーバを使用して、eLCM、System Monitor、Update Manager などの FTS アップデート管理ツールにリポジトリを作成することもできます。

## 9. Out-of-band 管理用 SNMP エージェント

6 章「ServerView Agents and CIM providers on managed servers」では、管理対象サーバの SNMP エージェントにおけるセキュリティの問題について説明しています。In-band 管理は、管理情報へアクセスするためにターゲットサーバハードウェアおよびターゲット OS が必要であることを意味します。また、SNMP エージェントなどの 1 つのソフトウェアをターゲット OS の上位にインストールする必要があります。

Out-of-band 管理では、管理対象サーバの管理情報にアクセスするために、実行しているターゲット OS を必要としません。次の 2 つのケースが可能です。

- 管理対象のサーバハードウェアが特別な診断 OS を実行している。
- 管理対象サーバの管理情報にアクセスするために、完全に独立したハードウェアコンポーネントが使用されている（ブレードサーバのマネジメントブレードなど）。

本章では、このような特別な管理デバイスにおける SNMP エージェントのセキュリティの問題について説明します。

SNMP は、特別な管理デバイスとリモート管理フロントエンドの両側で使用可能である必要があります。本章では、特別な管理デバイスにのみ着目します。

### 9.1. iRMC

iRMC（リモートマネジメントコントローラ）は SNMP Protocol および SNMP トラップの送信をサポートします。

一般の SNMP のように、権限に関連付けられている SNMP コミュニティを設定でき、トラップ送信先を設定できます。iRMC で設定される SNMP コミュニティは、ServerView Operations Manager のサーバのプロパティでも設定する必要があります。iRMC には、独自のイベント管理があります。SNMP エージェントは SNMP トラップを送信することにより SNMP マネージャに通知しますが、iRMC のアラームハンドラを設定して、ポケットベル、電子メール、または SNMP トラップを使用して管理者に通知することができます。SNMP トラップは失われる可能性があるので信頼できないと考えられているのに対して、その他の保証される配布方法は十分に信頼できると考えられています。

#### Recommendation 30

特定のイベントに関する通知が失われるのを回避するために、iRMC またはマネジメントブレードのアラームハンドラを適切に設定することを推奨します（SNMP 経由以外でも通知設定を行う）。

### 9.2. マネジメントブレード

マネジメントブレードは、デフォルトではコミュニティ文字列の設定は無く、「読み取り専用」です。

マネジメントブレードの以下のポートを通信に使用します。

http:	80	MMB へのインバウンド（設定可能）
https:	443	MMB へのインバウンド（設定可能）
SSH:	22	MMB へのインバウンド（設定可能）
Telnet:	3172(/23)	MMB へのインバウンド（設定可能）
SMTP:	25	MMB からのアウトバウンド（設定可能）
SNMP:	161	MMB へのインバウンド（固定）
SNMP トラップ:	162	MMB からのアウトバウンド（固定）
LDAP:	636	MMB からのアウトバウンド（固定）

CAS: 実装されていない  
RMCP: 623 MMB へのインバウンド（固定）  
WS-Man: 8889 MMB へのインバウンド（固定）  
他のポートが開いている場合は、何らかの問題が発生しています。

マネジメントブレードで SNMP を使用する場合、SNMP V3 が使用されます。このモードは ServerView Suite のすべての製品でサポートされていないことを認識しておく必要があります。

以前のマネジメントブレードの SNMP サービスではすべての操作（SNMP GET および SET 操作の両方）に対してこのコミュニティ文字列を使用します。新しいマネジメントブレードでは、別のコミュニティ許可を提供します。

マネジメントブレードは SNMP アドレスフィルタリングもサポートします。指定した IP アドレスのみマネジメントブレードが SNMP 要求元として受け付ける設定 とすることができます。3.1 項の「Communication Paths」の表に従って、このフィルタを設定することを推奨します。



## 10. 特別な設定

### 10.1. DMZ (Demilitarized Zone) のサーバを管理するためのオプション

DMZ (Demilitarized Zone) は、組織の内部ネットワークと外部のネットワーク（通常はインターネット）との間にあるネットワーク領域です。DMZ は通常、通信フローを制限するファイアウォールによってその両方から隔離されています。DMZ のセキュリティポリシーは、高レベルのセキュリティ要件によって構築されています。このような領域でサーバを管理するためには 2 つの方法があり、以下のように考えられます。

最初のオプションは、ファイアウォールが管理プロトコル（特に SNMP）に対して閉じられていることを前提とします。つまり、DMZ でのサーバのアクティブな管理は不可能であることを意味します。それでも、一部の管理情報はこのような環境からファイアウォール経由で管理対象サーバから取得することができます。

- 障害情報  
SNMP トラップがファイアウォールによってブロックされると、イベント情報は次の方法のいずれかでファイアウォールを通過できます。Event Manager を SNMP エージェントと共に DMZ へインストールする場合、特定のイベントが発生したときに電子メールを送信するように Event Manager を設定できます。同様に、iRMC やマネジメントブレードなどの管理デバイスを、SNMP トラップの代わりに電子メールを送信するように設定できます。もう 1 つの方法として、ServerView がログファイルにエントリを作成するので、中央管理用サーバにログファイルを送信することもできます。
- アセット情報  
ServerView Agents と Operations Manager が DMZ のサーバにインストールされている場合、HTTPS 経由でレポートファイルまたはアーカイブファイルに定期的に情報を書き込むように Operations Manager を設定できます。この場合、SNMP エージェントによって通知された情報が管理対象ノードのファイルへ書き込まれます。つまり、SNMP 通信は回線またはファイアウォール経由で行われず、データはローカルで収集されます。これらのファイルは、後でファイアウォール経由で中央管理用サーバへ転送することができます。

2 つ目のオプションは、分離した管理ネットワークを DMZ のサーバに使用できることを前提とします。この場合、管理トラフィックはこのネットワーク上を通り、一方で、本番ネットワークのセキュリティポリシーによって必要なセキュリティレベルが保証されます。DMZ 内のサーバは、専用のネットワークインターフェースカードまたは iRMC やマネジメントブレードなどの管理デバイスを使用して、分離した管理ネットワークへ接続されます。ゲートウェイシステムを使用して、イントラネットの中央管理用サーバから、DMZ のサーバの分離された管理ネットワークに VPN でアクセスできます。

## 11. まとめ

セキュリティは自動的に入手できるものではありません。すべての PRIMERGY サーバ管理コンポーネントをデフォルト値を使用してインストールしただけでは、すべての機能が動作しますが、この場合のセキュリティレベルは最も低くなります。すべてのコンポーネントを個別に設定すると、非常に優れたセキュリティを達成できますが、すべてのコンポーネントを一貫して設定しないとすべてが正しく動作することはありません。つまり、設定する前に、全体の設定を慎重に計画する必要があります。これらの詳細な計画は、設定および継続的な保守のベースとなります。

PRIMERGY サーバ管理は、以下の 3 つの異なる管理レベルがあります。

- 管理レベル「ターゲットオペレーティングシステムアップ」：ターゲットオペレーティングシステムを管理対象サーバでブートする必要があります。エージェントをこのオペレーティングシステムにインストールする必要があります。管理情報は運用可能な通信と同じパス上を流れます。
- 管理レベル「診断アップ」：ターゲットオペレーティングシステムは起動していませんが、システムボードは正しく動作しています。診断オペレーティングシステムまたは Pre-OS エージェントをブートできます。
- 管理レベル「セカンダリ管理チャネル」：この種類の通信は、ターゲットオペレーティングシステムともシステムボードとも完全に独立しています。iRMC やマネジメントブレード（ブレードサーバの場合）など、この種類の管理には特別な設備を使用します。この種類の管理は「セカンダリ管理チャネル」としても知られています。

次の表に、これまで説明したすべての推奨事項をまとめて示し、その目的（全体的なセキュリティの維持、セキュアな管理操作の実現、管理レベル）について分類します。

全体的なセキュリティの維持

## セキュアな管理操作の実現

イベント： 推奨	管理レベル		
	ターゲット OS アップ	診断 OS アップ	セカンダリ 管理チャンネル
<b>PRIMERGY サーバ管理のインストール:</b> ファイアウォールの内側にツール/コンポーネントと管理対象サーバを配置します。			
<b>一般事項:</b> 各システムで開くポートの数を最小限にします。			
<b>管理 VLAN の分離:</b> 運用トラフィックから管理トラフィックを分離します。			
<b>JBoss 用の非管理者アカウント:</b> ServerView Operations Manager と共にインストールされている JBoss アプリケーションサーバ専用の非管理者アカウントを作成します。アカウントのこのセキュリティ設定により、すべての非管理者ユーザが JBoss のアカウントのディレクトリおよびファイルの読み取りをできないようにします。			
<b>役割の割り当て</b> 必要な操作を許可する最小限の権限を持つ役割を割り当ててください。			
<b>管理デバイスの分離された管理 LAN:</b> iRMC などのネットワークインターフェースを分離された管理 LAN へ接続します。			
<b>Installation Manager を使用するリモートインストール:</b> Installation Manager のコンテンツのネットワーク共有をパスワードで保護します。 読み取り専用アクセス権限での OS 共有への TFTP アクセスが危険と見なされる場合は、Installation Manager をローカルモードでのみ使用することを推奨します。			
<b>SNMP エージェントのインストール:</b> SNMP サービスのデフォルト設定を変更します。大部分の設定に MS システムポリシーエディタを使用できます。			
<b>SNMP エージェントのインストール:</b> SET 操作のために ServerView 認証/許可メカニズム用のユーザグループを指定します。			
<b>SNMP エージェントのインストール:</b> IPSec を使用して SNMPv1 を保護します（Microsoft の指示に従います）。			
<b>中央管理用サーバ（CMS）および SNMP エージェント:</b> ファイアウォールの内側の管理対象サーバに CMS とエージェントをインストールします。			

イベント： 推奨	管理レベル		
	ターゲット OS アップ	診断 OS アップ	セカンダリ 管理チャネル
<b>Operations Manager への Web サーバのインストール:</b> SSL によりブラウザへの接続をセキュリティ保護します。			
<b>アップデートファイルの入手:</b> インターネット経由でのダウンロードが非常に危険であると見なされる場合は ServerView Update DVD を使用します。			
<b>Update Manager の設定:</b> Update Manager の認証/承認機能用のユーザグループを作成し、それに応じて Update エージェントの認証設定をします。			
<b>ドライバ、エージェント、BIOS、ファームウェアのアップデート:</b> ローカルツールを選択する場合、Update エージェントおよび Update Manager Express のローカルコマンドラインインターフェースを使用できま す。			
<b>iRMC での SNMP インターフェースの設定:</b> 読み取り専用でコミュニティを設定します。			
<b>iRMC またはマネジメントブレードでのアラームハンドラの設定:</b> 信頼できる通知のために、SNMP トラップに加えて設定します。			
<b>BMC の設定:</b> IP アドレスとパスワードを設定します。			
<b>iRMC/マネジメントブレードのアカウント:</b> デフォルトのアカウントを新しいアカウントに変更するか、少なくともパスワ ードを変更します。			
<b>iRMC/マネジメントブレードのポート:</b> HTTP 用のポート 80 を無効にし、HTTPS 用のポート 443 経由での SSL でセキュリティ確保された接続のみ使用します。			

## 12. ログファイル

Installation Manager	インストールが完了したら、現在のリモートインストールプロセスに対して作成したデプロイメントサーバの状態ディレクトリへ、インストールログファイルを保存し直します。そこで、Installation Manager インターフェースを使用して表示できます。
Asset Manager	GUI を使用したログファイルの検査
RAID Manager	デフォルトでは、ファイルのイベントは ServerView RAID ログファイルへ書き込まれます。デフォルトでは、すべてのイベントはオペレーティングシステムのログ機能に表示されます。Windows ベースのシステムの場合、エントリは「スタート」->「設定」->「コントロールパネル」->「管理ツール」->「イベントビューア」（アプリケーション）、Linux システムの場合、/var/log/messages に保存されます。
Download Manager	ログファイルは GUI を使用して表示できます。
Update Manager	ログファイルは GUI を使用して表示できます。
Virtual-IO Manager	Virtual-IO Manager は常にログファイルをディレクトリ <ServerView_Suite>\plugins\viom\Manager\logs に作成します。Windows ベースの管理用サーバでは、<ServerView_Suite> は通常以下のディレクトリです。 C:\Program Files\Fujitsu\ServerView Suite Linux ベースの管理用サーバでは、<ServerView Suite> は通常以下のディレクトリです。 /opt/Fujitsu/ServerViewSuite また、Virtual-IO Manager は、すべての設定変更とエラーを含むログエントリを、システムイベントログ（Windows）または syslog（Linux）に常に書き込みます。
iRMC	エラーメッセージは指定したログファイルに書き込まれます。ログファイルが指定されていない場合、出力は flbmc.log ファイルに転送されます。

## 13. ServerView のデフォルトの証明書

ここでは、各種 ServerView 製品によってデフォルトでインストールされている証明書を取り扱います。すべての証明書は、SHA1withRSA という同じ証明書の署名アルゴリズムと同じ SSL バージョン（バージョン 3）を使用します。

### 13.1. マネジメントコントローラ/マネジメントブレード

#### 13.1.1. ルート CA

所有者： EMAILADDRESS=ServerView@ts.fujitsu.com, CN=ServerView Root CA,  
O=Fujitsu Technology Solutions GmbH, L=Munich, ST=Bavaria, C=DE  
発行者： EMAILADDRESS=ServerView@ts.fujitsu.com, CN=ServerView Root CA,  
O=Fujitsu Technology Solutions GmbH, L=Munich, ST=Bavaria, C=DE  
シリアル番号： 0  
発行日： Wed Apr 22 16:37:44 CEST 2009  
有効期限： Sat Apr 20 16:37:44 CEST 2019  
フィンガープリント： MD5: 8E:B5:8D:B8:DE:7D:4C:2E:6A:5C:E2:A5:A6:12:19:E2  
SHA1: FD:9B:B0:3E:23:60:73:2E:85:B5:F6:25:38:7F:CF:99:EB:BF:37:CC

#### 13.1.2. iRMC のデフォルトの証明書

iRMC の初回ブート時に生成される、自動生成される自己署名証明書。

サブジェクト： C=DE, ST=Bavaria, O=Fujitsu Technology Solutions GmbH,  
CN=iRMC/emailAddress=primergy-pm@ts.fujitsu.com  
発行者： C=DE, ST=Bavaria, O=Fujitsu Technology Solutions GmbH,  
CN=iRMC/emailAddress=primergy-pm@ts.fujitsu.com  
シリアル番号： Auto-generated  
発行日： Auto-generated  
有効期限： Valid for 1825 days (5 years) since Issued On  
フィンガープリント： Auto-generated

#### 13.1.3. MMB のデフォルトの証明書

所有者： O=Fujitsu Technology Solutions, EMAILADDRESS=ServerView@ts.fujitsu.com,  
C=DE, ST=Bavaria, CN=PRIMERGY MMB 1024bit default RSA SSL Cert  
発行者： EMAILADDRESS=ServerView@ts.fujitsu.com, CN=ServerView Root CA,  
O=Fujitsu Technology Solutions GmbH, L=Munich, ST=Bavaria, C=DE  
シリアル番号： 54 (decimal)  
発行日： Mon Jun 15 16:50:10 CEST 2009  
有効期限： Sat Jun 14 16:50:10 CEST 2014  
フィンガープリント： MD5: 40:78:F6:08:8D:3E:62:38:10:39:74:30:5F:06:7A:62  
SHA1: 6D:E0:A2:35:F0:EA:17:75:32:1B:D8:89:3C:DA:6F:B5:EF:E4:26:1B

## 13.2. ServerView Connector Service (SCS)

### 13.2.1. ルート CA

所有者 : CN=Fujitsu Technology Solutions, OU=IP SW SV, O=Fujitsu Technology Solutions, L=Munich, ST=Bavaria, C=DE

発行者 : CN=Fujitsu Technology Solutions, OU=IP SW SV, O=Fujitsu Technology Solutions, L=Munich, ST=Bavaria, C=DE

シリアル番号 : 0

発行日 : Thu Feb 26 14:17:15 CET 2009

有効期限 : Sat Nov 05 14:17:15 CET 2022

フィンガープリント : MD5: B4:BC:CA:41:16:23:4D:9F:08:10:34:64:D6:57:A1:84  
SHA1: 22:DE:20:A1:BE:2B:6D:D2:4B:BA:C9:18:BB:C0:C8:97:D2:87:0A:99

### 13.2.2. SCS のデフォルトの証明書

所有者 : CN=RemoteConnector, OU=IP SW SV, O=Fujitsu Technology Solutions, L=Munich, ST=Bavaria, C=DE

発行者 : CN=Fujitsu Technology Solutions, OU=IP SW SV, O=Fujitsu Technology Solutions, L=Munich, ST=Bavaria, C=DE

シリアル番号 : 2

発行日 : Thu Feb 26 14:18:52 CET 2009

有効期限 : Sat Nov 05 14:18:52 CET 2022

フィンガープリント : MD5: CC:8A:B2:C7:8D:01:32:98:5F:DC:C9:97:5C:66:03:D7  
SHA1: 09:25:E8:C6:6E:6C:44:B5:3C:78:F5:FF:32:91:21:D0:EF:55:93:63



## 14.エンタープライズセキュリティに関する詳細情報

Fujitsu は、セキュアなシステム開発の最前線にいます。Fujitsu は高可用性サーバを基盤として、大手エンタープライズセキュリティパートナーと協力して、エンタープライズセキュリティのあらゆる分野に対応する洗練された実証済みの技術をお客様に提供します。このトピックの詳細については、以下を参照してください。

[http://ts.fujitsu.com/solutions/it\\_infrastructure\\_solutions/security/index.html](http://ts.fujitsu.com/solutions/it_infrastructure_solutions/security/index.html)

## 15.付録: iRMC S4 の概要/暗号技術のサポート

### 15.1. IPMI

#### 15.1.1. RMCP

アルゴリズム	対称/非対称、長さ
MD5	対称 - 128 bit

#### 15.1.2. RMCP+

アルゴリズム	対称/非対称、長さ
HMAC-SHA1	対称 - 160 bit
HMAC-SHA1-96	対称 - 96 bit
HMAC-SHA256	対称 - 256 bit
HMAC-MD5-128	対称 - 128 bit
MD5-228	対称 - 128 bit
AES-CBC	対称 - 128 bit

#### 15.1.3. IPMI でサポート暗号スイートのリスト

ID	認証アルゴリズム	完全性アルゴリズム	機密性アルゴリズム
1	RAKP-HMAC-SHA1	NONE	NONE
2	RAKP-HMAC-SHA1	HMAC-SHA1-96	NONE
3	RAKP-HMAC-SHA1	HMAC-SHA1-96	AES-CBC-128
6	RAKP-HMAC-MD5	NONE	NONE
7	RAKP-HMAC-MD5	HMAC-MD5-128	NONE
8	RAKP-HMAC-MD5	HMAC-MD5-128	AES-CBC-128
11	RAKP-HMAC-MD5	MD5-128	NONE
12	RAKP-HMAC-MD5	MD5-128	AES-CBC-128
15	RAKP_HMAC_SHA256	NONE	NONE
16	RAKP_HMAC_SHA256	HMAC-SHA256-128	NONE
17	RAKP_HMAC_SHA256	HMAC-SHA256-128	AES-CBC-128

## 15.2. OpenSSH

	Relaxed	Intermediate	Restricted
鍵交換	diffie-hellman-group-exchange-sha1 diffie-hellman-group-exchange-sha256 diffie-hellman-group1-sha1 diffie-hellman-group14-sha1 ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521  *iRMC S4 9.60F、iRMC S5 2.60P 以降に追加:  diffie-hellman-group14-sha256 diffie-hellman-group16-sha512	diffie-hellman-group-exchange-sha1 diffie-hellman-group-exchange-sha256 diffie-hellman-group1-sha1 diffie-hellman-group14-sha1 ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521  *iRMC S4 9.60F、iRMC S5 2.60P 以降に追加:  diffie-hellman-group14-sha256 diffie-hellman-group16-sha512	diffie-hellman-group-exchange-sha256 ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521  *iRMC S4 9.60F、iRMC S5 2.60P 以降に追加:  diffie-hellman-group14-sha256 diffie-hellman-group16-sha512
サーバホストキー	*iRMC S4 9.20F および iRMC S5 2.50P まで使用:  rsa-sha2-256 rsa-sha2-512 ssh-rsa  *iRMC S4 9.60F、iRMC S5 2.60P 以降:  ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 ecdsa-sha2-	*iRMC S4 9.20F および iRMC S5 2.50P まで使用:  rsa-sha2-256 rsa-sha2-512 ssh-rsa  *iRMC S4 9.60F、iRMC S5 2.60P 以降:  ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 ecdsa-sha2-nistp512	*iRMC S4 9.20F および iRMC S5 2.50P まで使用:  rsa-sha2-256 rsa-sha2-512 ssh-rsa  *iRMC S4 9.60F、iRMC S5 2.60P 以降:  ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 ecdsa-sha2-nistp512

	nistp512		
暗号化	3des-cbc aes128-cbc aes128-ctr aes192-cbc aes192-ctr aes256-cbc aes256-ctr blowfish-cbc cast128-cbc <a href="mailto:rijndael-cbc@lysator.liu.se">rijndael-cbc@lysator.liu.se</a>	aes128-ctr aes192-ctr aes256-ctr	aes128-ctr aes192-ctr aes256-ctr
MAC	hmac-sha1 hmac-sha2-256 hmac-sha2-512 <a href="mailto:umac-64@openssh.com">umac-64@openssh.com</a>  *iRMC S4 9.20F および iRMC S5 2.50P まで使用:  hmac-ripemd160 <a href="mailto:hmac-ripemd160@openssh.com">hmac-ripemd160@openssh.com</a>	hmac-sha1 hmac-sha2-256 hmac-sha2-512 <a href="mailto:umac-64@openssh.com">umac-64@openssh.com</a>  *iRMC S4 9.20F および iRMC S5 2.50P まで使用:  hmac-ripemd160 <a href="mailto:hmac-ripemd160@openssh.com">hmac-ripemd160@openssh.com</a>	hmac-sha2-256 hmac-sha2-512  *iRMC S4 9.20F および iRMC S5 2.50P まで使用:  hmac-ripemd160 <a href="mailto:hmac-ripemd160@openssh.com">hmac-ripemd160@openssh.com</a>
圧縮	なし <a href="mailto:zlib@openssh.com">zlib@openssh.com</a>	なし <a href="mailto:zlib@openssh.com">zlib@openssh.com</a>	なし <a href="mailto:zlib@openssh.com">zlib@openssh.com</a>

### 15.3. SNMPv3

アルゴリズム	対称/非対称、長さ
SHA	対称 - 160
MD5	対称 - 128
AES	対称 - 128, 192, 256 bit
DES	対称 - 56 bit

## 15.4. Web、KVM、VMEDIA、Redfish (iRMC S5 のみ)

これらのサービスでは、iRMC ファームウェアに含まれる OpenSSL ライブラリを使用します。ファームウェアバージョンに依存して、OpenSSL バージョン 0.9.8 や 1.0.1 や 1.0.2 を使用します。詳細は、使用する iRMC リリースに提供される iRMC マニュアルを参照してください。

### 15.4.1. SSLv3 の暗号リスト

暗号	鍵交換	認証	暗号化	MAC
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DH	RSA	AES (256)	SHA1
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DH	RSA	AES (128)	SHA1
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	DH	RSA	Camellia (256)	SHA1
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	DH	RSA	Camellia (128)	SHA1
TLS_RSA_WITH_AES_256_CBC_SHA	RSA	RSA	AES (256)	SHA1
TLS_RSA_WITH_AES_128_CBC_SHA	RSA	RSA	AES (128)	SHA1
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	RSA	RSA	Camellia (256)	SHA1
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	RSA	RSA	Camellia (128)	SHA1

## 15.4.2. TLSv1.2 の暗号リスト

暗号	鍵交換	認証	暗号化	MAC
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH	RSA	AESGCM (256)	AEAD
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	DH	RSA	AES (256)	SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DH	RSA	AES (256)	SHA1
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	DH	RSA	Camellia (256)	SHA1
TLS_RSA_WITH_AES_256_GCM_SHA384	RSA	RSA	AESGCM (256)	AEAD
TLS_RSA_WITH_AES_256_CBC_SHA256	RSA	RSA	AES (256)	SHA256
TLS_RSA_WITH_AES_256_CBC_SHA	RSA	RSA	AES (256)	SHA1
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	RSA	RSA	Camellia (256)	SHA1
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	DH	RSA	AESGCM (128)	AEAD
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	DH	RSA	AES (128)	SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DH	RSA	AES (128)	SHA1
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	DH	RSA	Camellia (128)	SHA1
TLS_RSA_WITH_AES_128_GCM_SHA256	RSA	RSA	AESGCM (128)	AEAD
TLS_RSA_WITH_AES_128_CBC_SHA256	RSA	RSA	AES (128)	SHA256
TLS_RSA_WITH_AES_128_CBC_SHA	RSA	RSA	AES (128)	SHA1
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	RSA	RSA	Camellia (128)	SHA1

## 15.5. CIM/SMASH (iRMC S4 のみ)

TLSv1.1 の暗号リスト

暗号	鍵交換	認証	暗号化	MAC
TLS_RSA_WITH_AES_256_CBC_SHA	RSA	RSA	AES (256)	SHA1
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	RSA	RSA	Camellia (256)	SHA1
TLS_RSA_WITH_AES_128_CBC_SHA	RSA	RSA	AES (128)	SHA1
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	RSA	RSA	Camellia (128)	SHA1

## 15.6.

### Linuxカーネル暗号

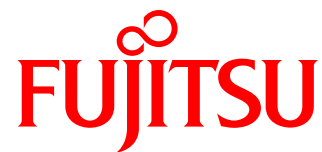
次のアルゴリズムをカーネルで使用でき、各種 FW バージョンでのカーネル設定に基づいて異なります。

アルゴリズム	対称/非対称、長さ
DES	対称 - 56
3DES	対称 - 56, 112, 168
MD5	対称 - 128
SHA1	対称 - 160



## 16.用語集

AVR	ビデオリダイレクション (AVR)
証明書	サブジェクトの公開鍵とそのサブジェクトに関する識別情報を含む電子文書。証明書は、鍵とサブジェクト ID を結び付けるために、CA (認証局) によって署名されます。
CA	認証局 (Certification Authority) は、デジタル署名および公開鍵と秘密鍵のペアを作成するために使用されるデジタル証明書を発行する、信頼されるサードパーティ組織または企業です。このプロセスでの CA の役割は、一意の証明書が与えられた個人が、CA が示す個人であることを保証することです。
CGI	Common Gateway Interface
DHCP	Dynamic Host Configuration Protocol
DMZ	DMZ (Demilitarized Zone) は、組織の内部ネットワークと外部のネットワーク (通常はインターネット) との間にあるネットワーク領域です。
HTML	ハイパーテキストマークアップ言語
IANA	Internet Assigned Numbers Authority
IIS	Internet Information Server (Microsoft)
JBoss	JBoss アプリケーションサーバの同義語 ( <a href="http://www.jboss.org/jbossas/">http://www.jboss.org/jbossas/</a> )
KVM	キーボード/ビデオ/マウス
OS	オペレーティングシステム
POST	Power On Self Test
PXE	Pre-boot Execution Environment
iRMC	リモートマネジメントコントローラ (ボードの RSB 機能)
LDAP	Lightweight Directory Access Protocol は、IP (インターネットプロトコル) ネットワークに実装されたディレクトリサービスのデータをキューに格納したり変更したりするためのアプリケーションプロトコルです。
RSB	RemoteView サービスボード
RTDS	Remote Test and Diagnosis System
セキュリティ メカニズム	システムによって、またはシステム内に提供されるセキュリティサービスを実装するために、システムで使用可能なプロセス (またはこのようなプロセスが組み込まれたプロセス)。例: 認証交換、チェックサム、デジタル署名、暗号化など。
セキュリティ ポリシー	機密扱いの重要なシステムリソースを保護するために、システムや組織がセキュリティサービスを提供する方法を指定または規制するための、一連の規則および慣例。
自己署名証明書	サブジェクトと CA が同一の、それ自身の認証局 (CA) となっている証明書。
SNMP	Simple Network Management Protocol (簡易ネットワーク管理プロトコル)
SSL	Secure Socket Layer - TCP/IP の上位にあるプロトコル
SSDP	Simple Service Discovery Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
WBEM	Web-Based Enterprise Management - イニシアチブ



---

知的財産権を含むすべての権利を留保します。技術仕様は変わる場合があります。また、納品期日は在庫状況によって異なります。データおよび図の完全性、実際性、正確性について、一切責任は負いません。

このマニュアルには各メーカーの商標名および著作物が指定されている可能性があり、第三者が独自の目的のために使用する場合、その商標所有者の権利を侵害する可能性があります。

詳細は、[ts.fujitsu.com/terms\\_of\\_use.html](https://ts.fujitsu.com/terms_of_use.html) を参照してください。