Dell Technologies Secure Remote Serviceのご案内

デル・テクノロジーズ株式会社

2021/2/10　第30版

Agenda

導入メリットと基本的な動作

Secure Remote Service機能概要

Policy Manager機能概要

導入要件

オンラインアカウントのご準備

構築後の注意点/FAQ

導入メリットと基本的な動作

Secure Remote Services のメリット

メリット：

- 自動ヘルスチェックで最適なパフォーマンスを確保
- 通知機能で健全性と高可用性を実現
- プロアクティブなケース作成と、リモート接続による迅速な問題解決
- Policy Manager で、アクセスと権限を完全に制御

エキスパート

- SRS 接続を通じたリモートトラブルシューティング
- ログ、コード、およびファイル共有のための、安全で双方向のパイプライン

インサイト

- プロアクティブな監視により、問題発生を防止
- リモート問題分析および診断
- オンラインサポートと MyService360 に、価値の高い最新データを供給

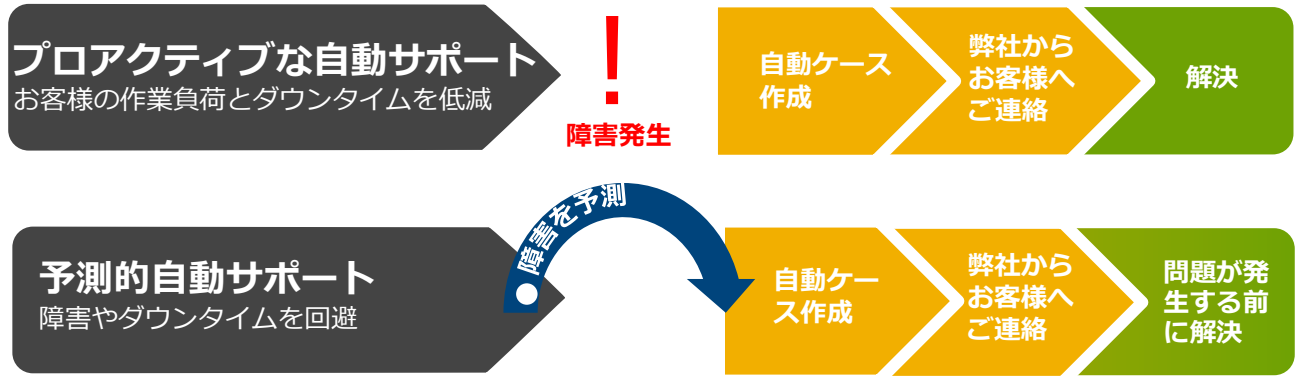
使いやすさ

- カスタマによるインストールが可能
- 仮想エディションに対して、追加のハードウェアまたは OS ライセンスは不要
- Linux ベースのシステムの場合、Docker エディションによるセキュリティ強化

問題解決時間が最大 73% 短縮1

従来のサポート

接続サポート



- システムの可用性が平均: **15%向上**
- EMCが最初のアクセスで問題を解決できる可能性が **3倍増**

[1] *2017 年 7 月の 分析結果に基づきます。実際の結果とは異なる場合があります。*

Secure Remote Service/Policy Managerで提供する４つの機能

自動化
- 24時間365日のプロアクティブなリモート監視
- IP接続による迅速な解決

認証
- AES 256ビット暗号化
- RSAデジタル証明書

承認
- Policy Manager (オプション)によるRemoteセッションの許可
- 権限を割り当て、ポリシー・フィルタを適用

監査
- Policy Managerによる各リモート・セッションの監査ログ
- 法令遵守の実現

Secure Remote Servicesのセキュリティの特徴

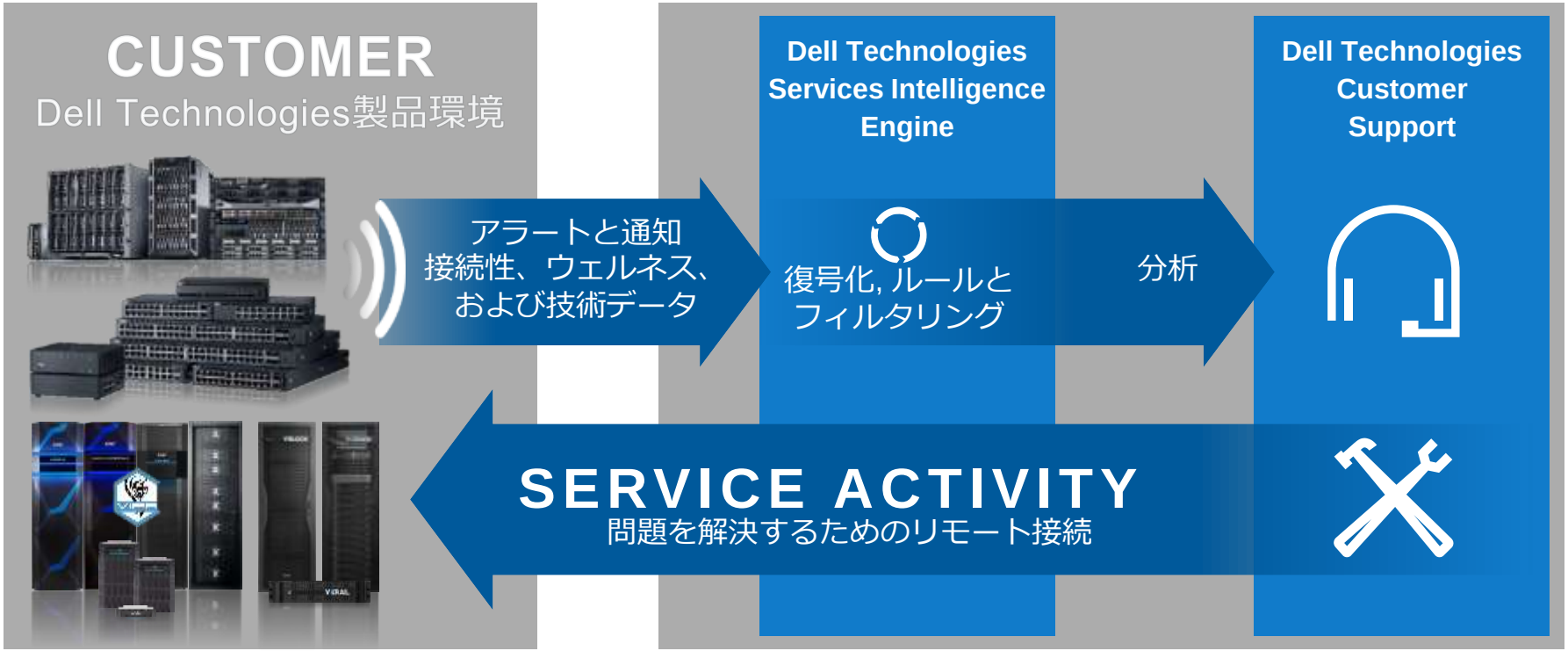
安全で強固なセキュリティ

- ✓IPベースで、TLS VPN を使用
- ✓AES-256アルゴリズムによる保護
- ✓RSAデジタル証明書キー交換を使用したクライアント/サーバ認証
- ✓リモート・アクセスは認証および承認されたDell Technologies担当者に制限され、お客様はリモート・サポート・セッションの拒否が可能
- ✓お客様サイトのERSゲートウェイ・ソフトウェアではFIPS 140-2確認済みの暗号を使用
- ✓Dell Technologiesとお客様のDell Technologiesシステムとの間の接続は、すべてSRSアプリケーションから開始および管理

Secure Remote Service機能概要

基本的な機能

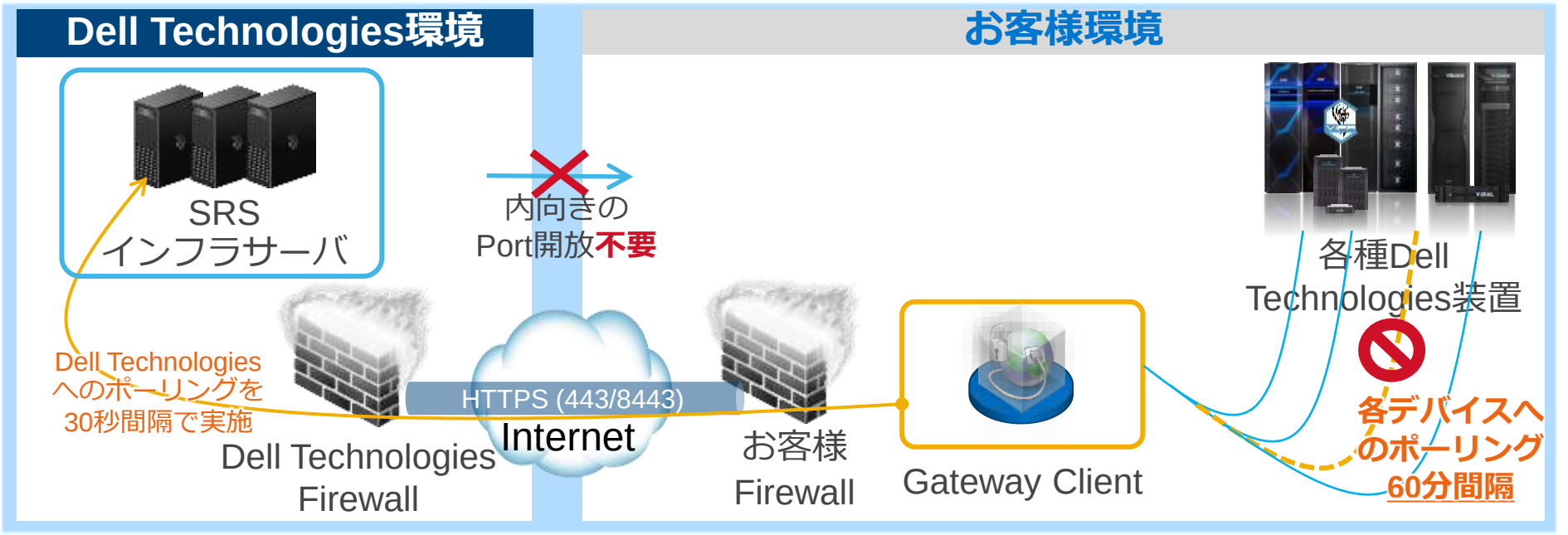
Dell Technologies 製品とDell Technologies 間のセキュアな双方向接続を実現



Secure Remote Servicesの動作

お客様各装置–お客様Gateway Client 間動作概要

- Gateway Clientとプロダクトデバイス間の通信ポートは、各プロダクト毎に異なります
- Gateway Clientからデバイスに対する60分間隔のポーリングに失敗すると、オフラインステータスとなります
  ※Gateway Clientと各種デバイス間への接続ステータスは Gateway Client GUI にて確認可能

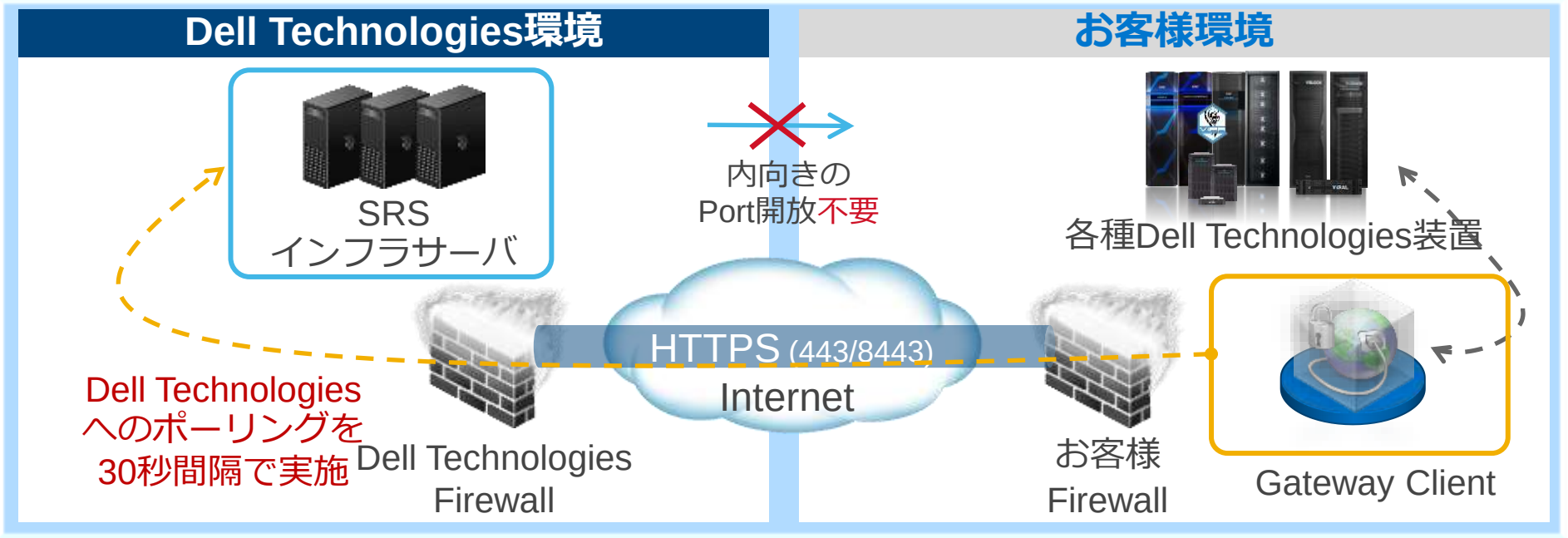


Secure Remote Servicesの動作

お客様Gateway Client – Dell Technologies間 動作概要

- Gateway Clientから外部方向に TCP Port 443 及び 8443をOpen（outboundのみ）
- 30秒毎のHeartbeat Pollingによる接続確認 (24時間365日)
- ポーリングは必ずGateway Clientからのみ開始され、Gateway Clientから15分間以上Polling疎通が無いとSRSインフラサーバ上でオフラインステータスとなる

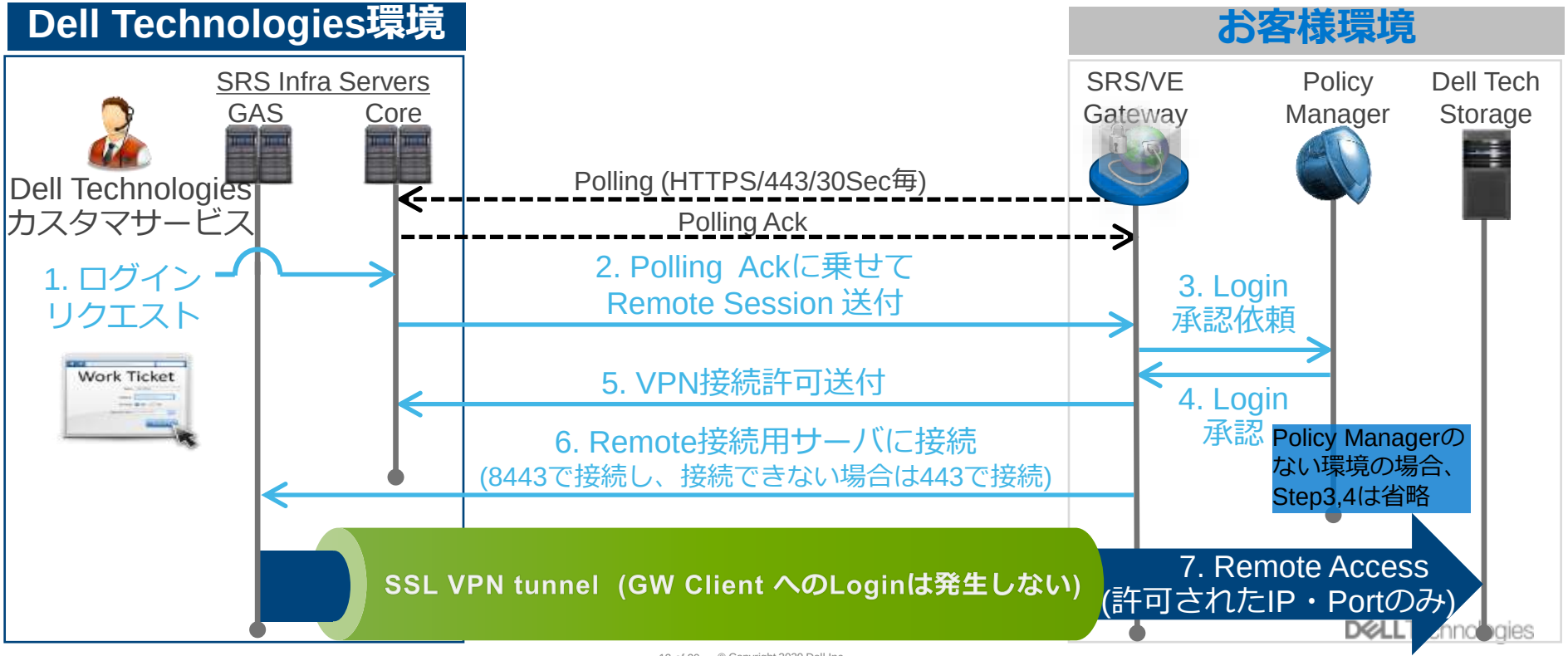
※SRSインフラサーバ上でGWオフライン状態が長時間継続した場合、お客様Emailアドレスへメール通知が可能です。
なお、本動作はお客様でのSRS GW稼働監視に代わるものではなく、あくまで補助的な位置付けとなります。



Secure Remote Servicesの動作

リモート接続ステップ

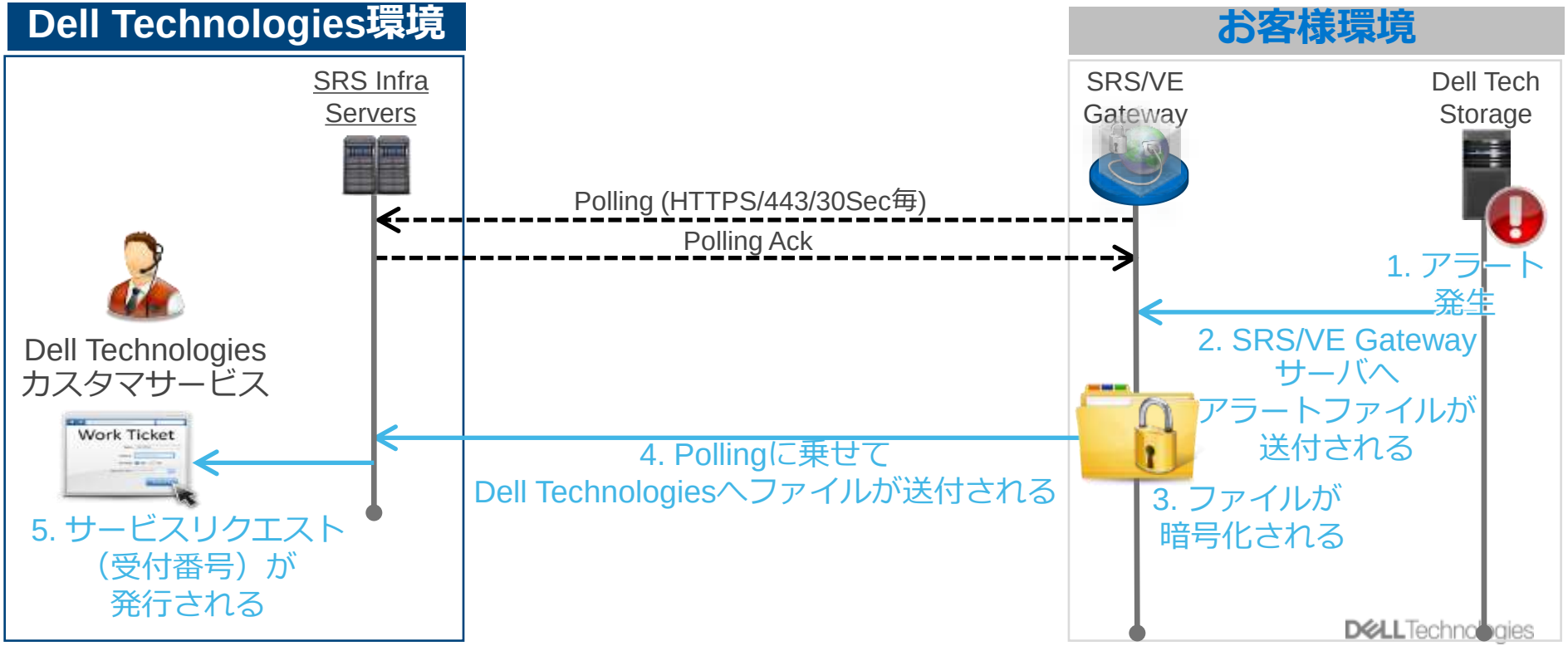
Loginセッションは、Gateway ClientのPollingから実施されます
リモート・アクセス時はDell Technologiesとお客様のデバイス(機器)間でのみ接続され、
Gateway Clientサーバへのログインは発生しません



Secure Remote Servicesの動作

エラー通知時

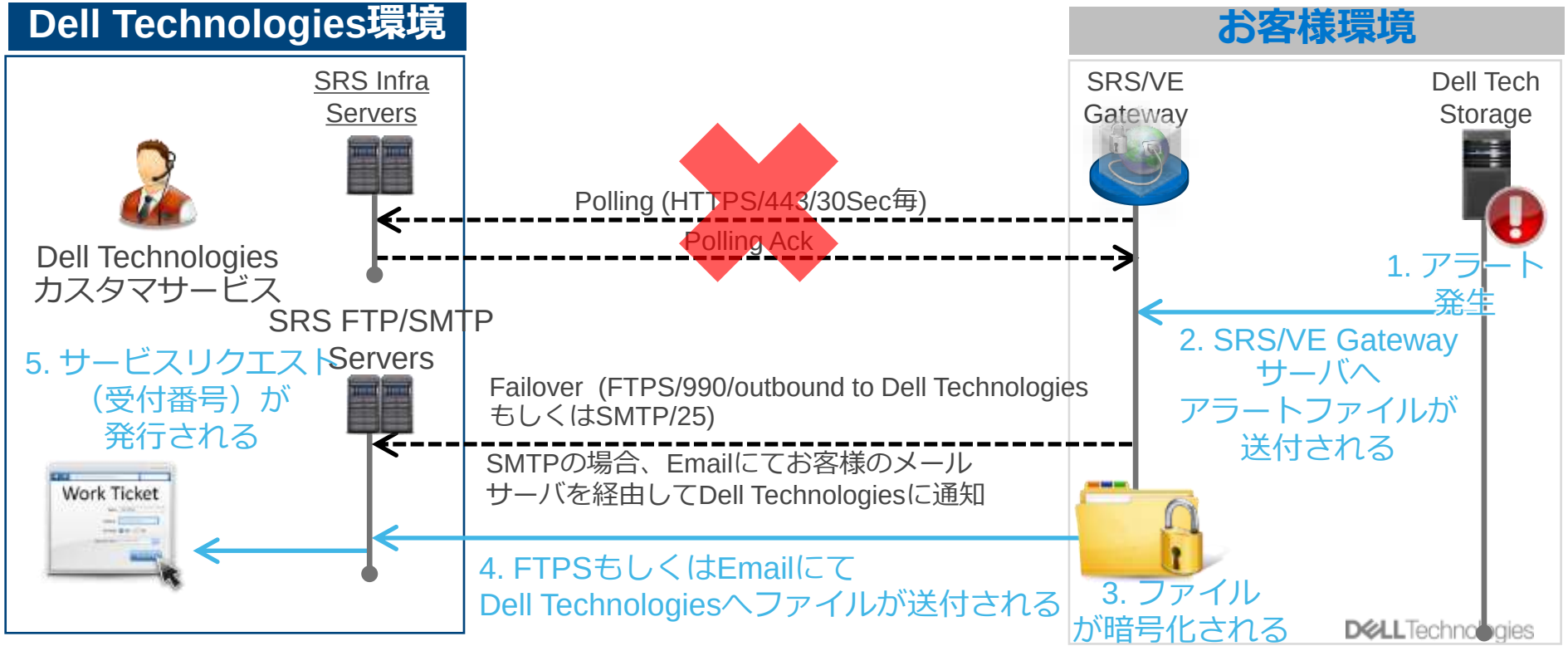
アラート発生時、Gateway Clientを経由して、Dell Technologiesへ通知されます
アラートファイルは、暗号化され通知されます



Secure Remote Servicesの動作

エラー通知代替機能

Gateway Clientから通常使用する8443/443での接続ができない場合に備え、代替エラー送信のFailOver機能設定を強く推奨しております。
Gateway ClientよりFTPS(990)若しくはSMTP(25)により、Dell Technologiesへエラー通知が実行されます。（オプション機能）
なおアラートファイルは、暗号化され通知されます。



Policy Manager機能概要

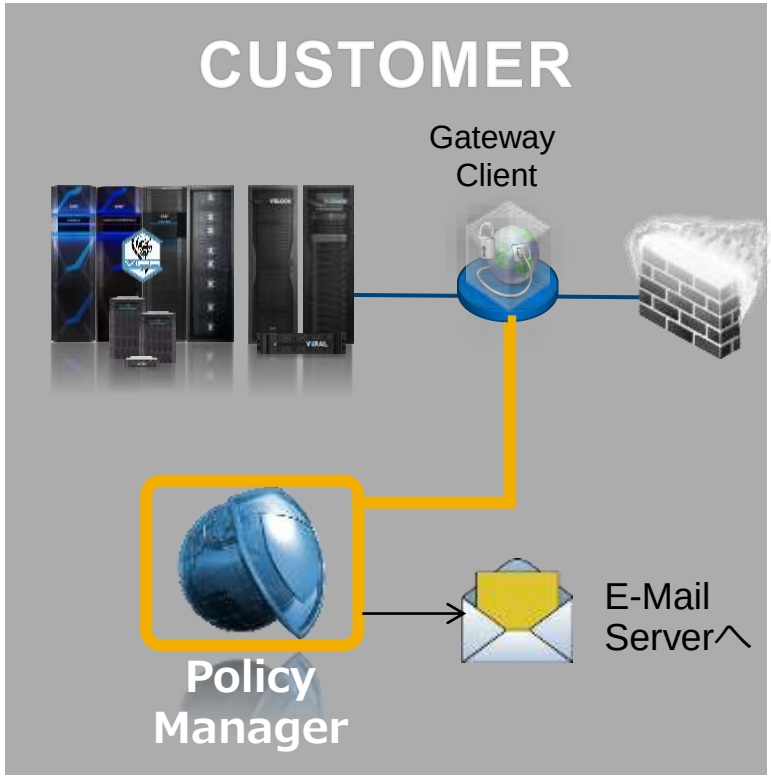
Policy Manager

アクセス監査ログの取得管理とアクセス制御

各デバイスに対するアクセス要求の制御、
履歴の保存が可能となります。

- **リモートアクセスポリシーの設定変更、確認**
- **リモートアクセス要求に対する承認、確認**
- **監査ログの確認**
- **リモートセッションの確認**
- **ユーザの作成**
- **ユーザ管理（閲覧。編集権限の変更）**

ユーザ作成を実施しない場合でも、
Dell Technologies標準のAdminアカウントにて
運用可能です。

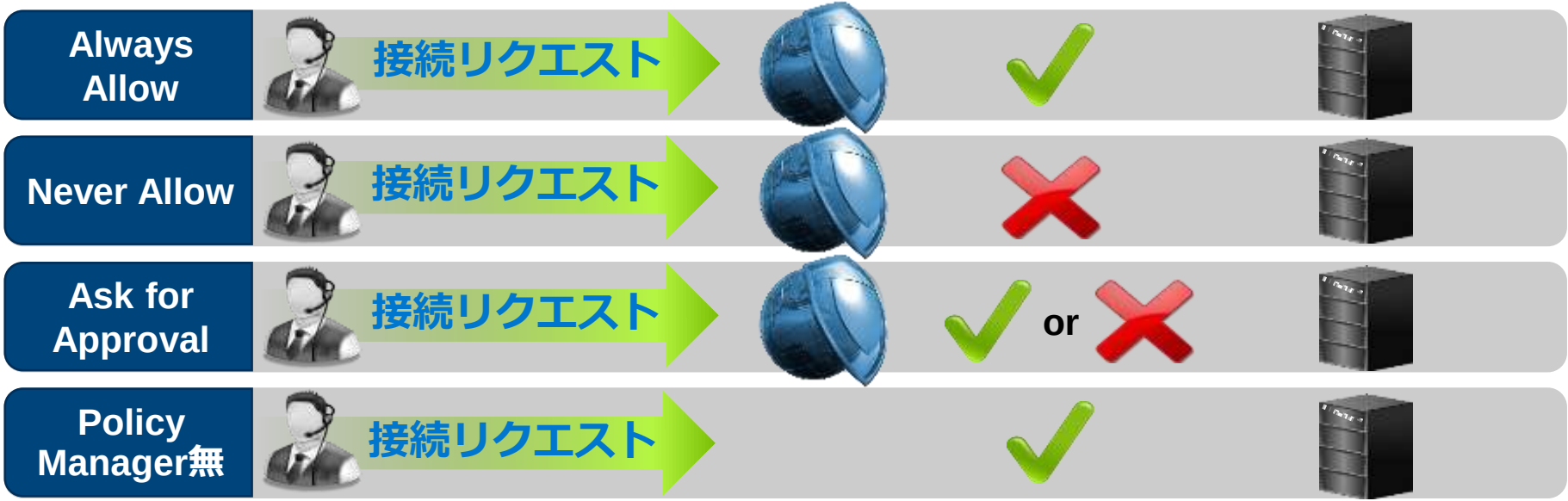


Policy Managerによるアクセス制御

Always Allow:
Dell Technologiesからデバイス(機器)へのリモートアクセスを許可 <<デフォルト設定>>

Never Allow:
Dell Technologiesからデバイス(機器)へのリモートアクセスを拒否

Ask for Approval:
Dell Technologiesからデバイス(機器)へのリモートアクセスに、お客様の承認操作が必要



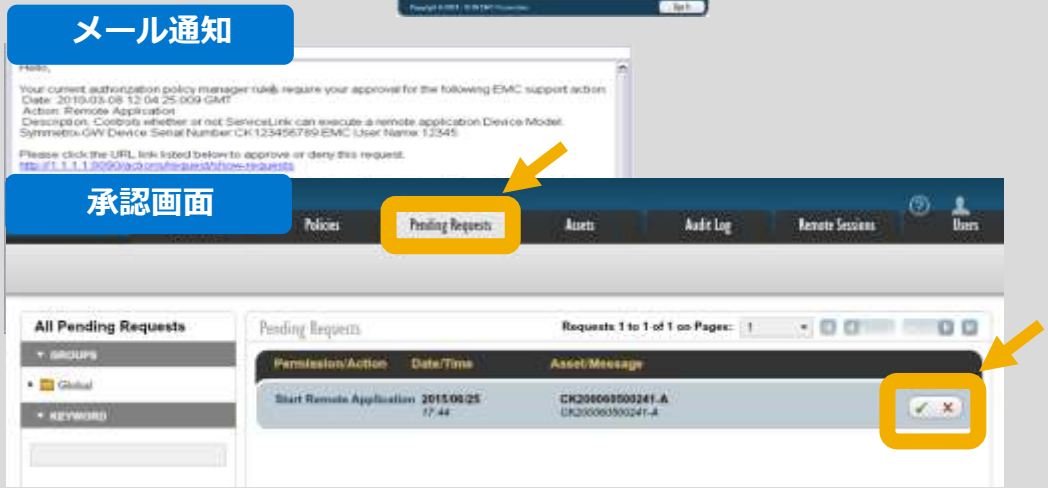
Policy Manager – Ask for Approval時の承認プロセス

① リモートアクセス要求に伴い、設定したEメールアドレスへ承認メールが通知される

② Eメール内のLinkをクリックすると、Policy Managerが起動

③ Policy ManagerにLogin

④ Accept✓またはDeny✗を選択(*)



Ask for Approvalポリシー設定時の補足

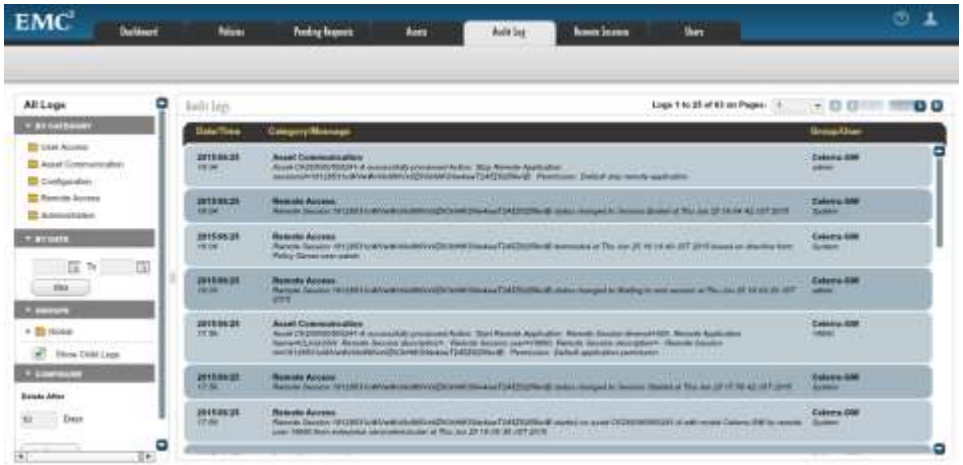
- お客様がAcceptを選択しない限り、リモートセッションは確立されません。
- Dell Technologiesによるシステム上の定期的な自動リモート接続およびConnect Homeテストは、例外的にAlways Allowに設定されています(本スクリプトのPolicy変更は非推奨)

(*) 設定時間以内(デフォルト60分/変更可)の間に、承認されない場合、承認プロセスは最初からやり直しとなります

Policy Manager – 監査ログ

Policy managerの監査ログファイルには以下情報が含まれます

- ✓ アクセス日時
- ✓ アクセスしたデバイス(機器シリアル)
- ✓ アクセスに使用したアプリケーション
- ✓ リクエスト応答結果
- ✓ サービスリクエスト番号、コメント(任意)
- ✓ Dell Technologiesユーザ識別番号
- ✓ 適応されたポリシー



GUIの表示：表示期間を設定（左記以外はLogファイルを確認）

Audit LogはPolicy Managerサーバに保持（世代管理による上書きなし）

保存場所：`<Install Directory>:¥EMC¥SRS¥PolicyManager¥audit¥APM_Audit_<yyyy>_<mm>_<dd>.txt`

Policy Manager – 多彩なユーザ

閲覧権限のみ、編集権限を持たせた等の多彩なユーザー権限の作成が可能

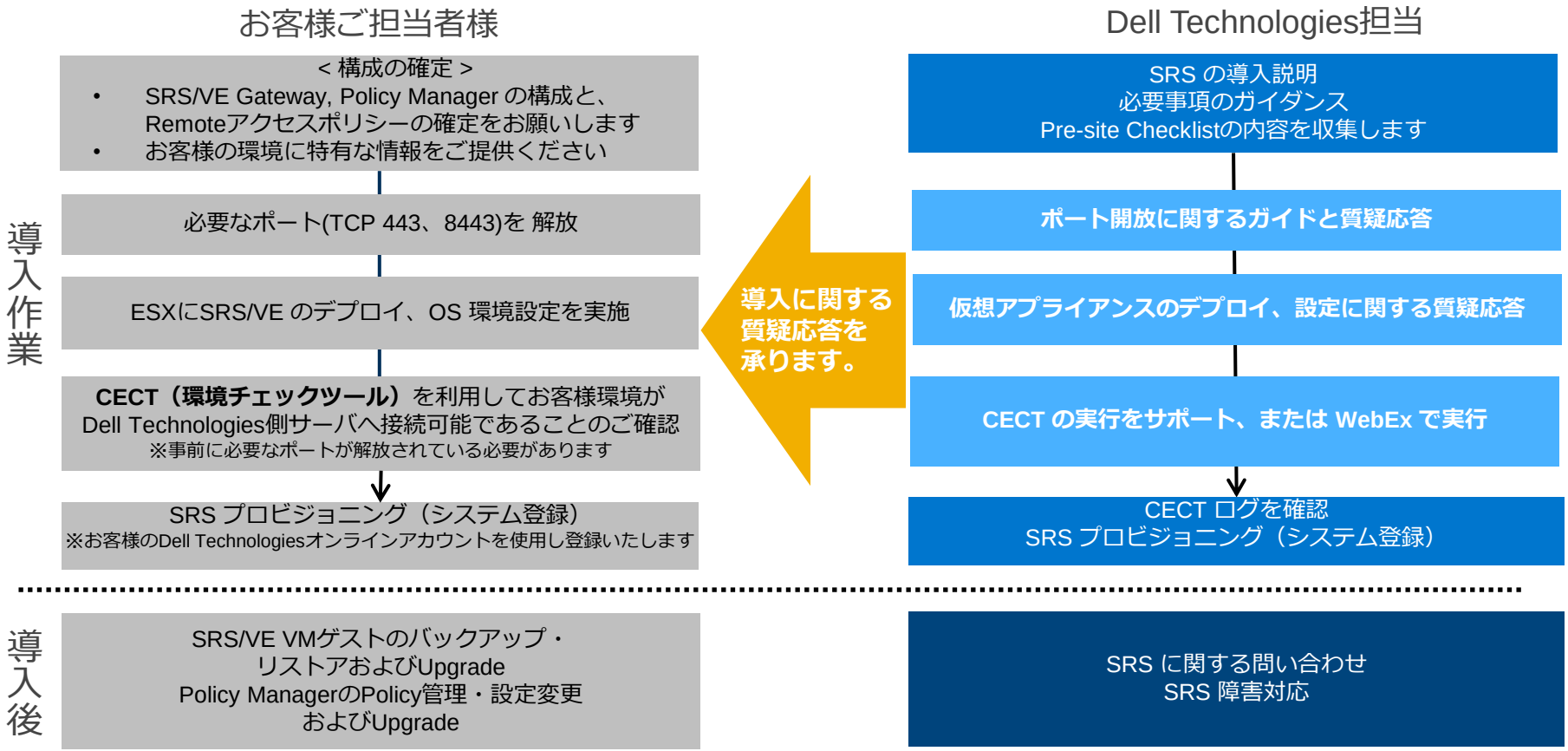
Policy Filtersによる詳細なポリシー（Ask for Approvalの時間帯設定など）が可能

外部SyslogサーバへのLoggingに対応

Audit Logタブから、Sessionの開始、停止時間の確認が可能

導入要件

SRS導入に向け、お客様に実施頂く内容



＊プロビジョニング作業のみ（システム登録のみ）を依頼される場合は記入済みのPre-site Checklist、CECTログを添えて Dell Technologies 担当者へお問い合わせください。

SRS Gateway サーバー要件

サーバハードウェア要件
VMWare ESX server 5.x以上
Windows Hyper-V environment
Linux Host (Docker Engine インストール済み https://docs.docker.com/engine/installation/)
CPU :1CPU 以上　2.2 GHz以上　 SSE2サポート
メモリ: 4 GB以上
DISK容量: 64GB以上
ネットワーク: GbE アダプタ推奨

Hypervisor Type ESX v5.x 以上　もしくは Hyper-V	**Docker Edition** Docker supported Linux distribution (x64 bit)
vCPU：vCPU数: x1 以上2.0 GHz以上　 64ビット メモリ ：4 GB以上 RAM ディスク空き容量: 64GB以上　 （vDISK の容量）	vCPU：vCPU数: x1 以上　2.0 GHz以上　 64ビット メモリ ：4 GB 以上 ディスク空き容量：64GB以上の領域 ポート： FTP 21 / HTTPS 443 / SMTP 25 / Provision, WebUI & REST 9443

*アプリケーション設定はOperations Guideをご参照ください

Policy Manager 7.0 サーバ要件

必要スペック

CPU 要件: 2.1 GHz以上

メモリ 要件： 4 GB RAM 以上

ディスク空き容量　推奨値: 80GB (最小値: 2GB)

Microsoft .NET Framework 2.0 SP1~3.5 (4.0は未対応)

お客様 SMTP サーバー

Remote SessionなどのEmail通知を実施する場合、お客様SMTPサーバ情報が必要

- OS （US英語版のみ）
  - RedHat 7/8 64bit
  - CentOS 7/8 64bit
  - SuSE11 64bit
  - Windows8 64bit、Windows2012R2、Windows2016、Windows2019
- Webブラウザ
  - Microsoft Internet Explorer 10+
  - Google Chrome
  - Mozilla Firefox
- Java Runtime Environment
  - Java 1.8.x
  - Amazon Corretto1.8.x
  - Oracle Java, OpenJDK

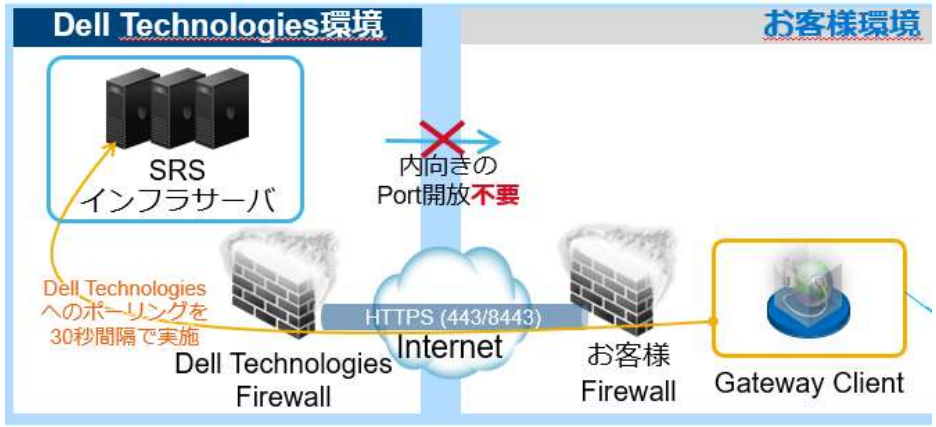
SRS Gateway外部ネットワーク接続に際して

From: SRS Gateway Client ⇒ To: 外部ネットワーク(インターネット)

- SRSインフラサーバのアドレスに対して、TCP Port 443及び8443を使用したOutbound通信が許可されていること
- SRS インフラサーバのアドレス・リストは下記 Knowledge Baseを参照お願いします

  494729: SRS: What IP addresses are used by the EMC Secure Remote Support IP Solution?

  https://support.emc.com/kb/494729
- Proxy環境の場合、Proxyサーバからの Outbound 通信にて上記要件を満たす必要がございます
- SRSインフラサーバが名前解決（DNS推奨）されることが必要です
- SSLチェックやSSLインスペクション、SSL復号化等はコネクションの切断の原因となります



SRS Gateway貴社内部ネットワーク接続に際して

From: SRS Gateway Client ⇒ To: 各導入済Dell Technologiesデバイス

- SRS Gateway Client ⇔ Dell Technologiesデバイス間の内部Port要件は、各通信ソフトウェアにより異なります。


EMC²

EMC® Secure Remote Services
Release 3.16

Port Requirements

REV 01

September 12, 2016

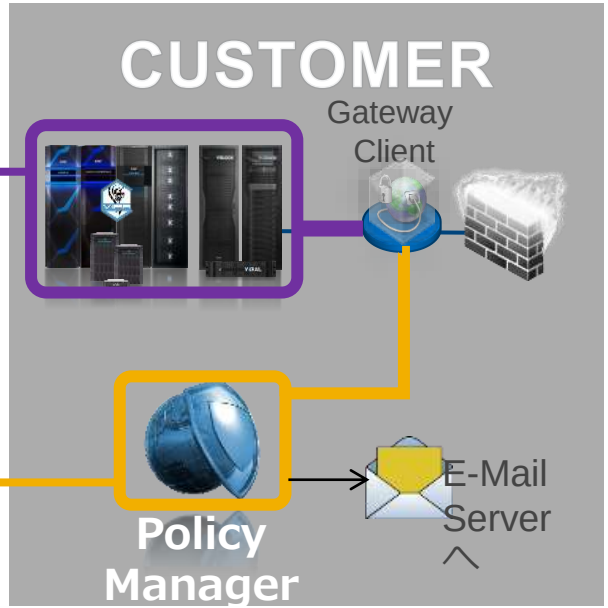
This document contains supplemental information about the EMC Secure Remote Services (ESRS), Release 3.16. ESRS 3.16 is the virtual edition of ESRS. This document includes the following topics:

- Communication between ESRS and EMC 2
- Communication between ESRS and Policy Manager 2
- Communication between ESRS and devices 2
- Port requirements for ESRS and Policy Manager (VM) servers 4
- Port requirements for devices 7

各デバイスの通信ポート要件については、
Port Requirementsドキュメントの各デバイス部分を参照

Policy Managerの通信ポート要件についても、Port Requirementsドキュメントを参照

EMC product	TCP port or Protocol	Notes for port settings	Direction open	Source -or- Destination	Application name	Communication (network traffic) type	Performed by authorized EMC Global Services personnel: Support objective (frequency)
Policy Manager	HTTP (configurable) Default = 8090		Inbound	from ESRS IP Clients (and customer browser)	Policy Manager service	Policy query (and policy management by customer)	N/A
	HTTPS 8443						
	SMTP 25		Outbound	to Customer email server		Action request	



https://dl.dell.com/content/docu99514_Secure_Remote_Services_3.46_Port_Requirements.pdf?language=en_US /

（参考）DNSにご登録いただくアドレスの一覧

文書番号: 494729　　印刷　Eメール

(E)SRS: What IP addresses are used by the Dell EMC Secure Remote Services solution?

概要: Information on what IP addresses and ports are used outbound to Dell/EMC

ESRS UI, port 443:
Prod: esrs3.emc.com 128.221.236.245
DR: esrs3-dr.emc.com 168.159.224.235

ESRS Core (for GW Pings) port 443:
Prod: esrs3-core.emc.com 128.221.236.246
DR: esrs3-coredr.emc.com 168.159.224.236

Global Access Servers (GAS) ports 443 and 8443:

esr3gduprd01.emc.com 128.221.204.207
esr3gduprd02.emc.com 128.221.204.208
esr3gduprd03.emc.com 128.221.204.209
esr3gduprd04.emc.com 128.221.204.212
esr3gduprd05.emc.com 128.221.204.214
esr3gduprd06.emc.com 128.221.204.215

esr3ghoprd01.emc.com 168.159.209.91
esr3ghoprd02.emc.com 168.159.209.92
esr3ghoprd03.emc.com 168.159.209.93
esr3ghoprd04.emc.com 168.159.209.94
esr3ghoprd05.emc.com 168.159.209.95
esr3ghoprd06.emc.com 168.159.209.96

esr3gscprd01.emc.com 137.69.120.227
esr3gscprd02.emc.com 137.69.120.222
esr3gscprd03.emc.com 137.69.120.223
esr3gscprd04.emc.com 137.69.120.224
esr3gscprd05.emc.com 137.69.120.225
esr3gscprd06.emc.com 137.69.120.226

esr3gckprd01.emc.com 152.62.177.21
esr3gckprd02.emc.com 152.62.177.22
esr3gckprd03.emc.com 152.62.177.23
esr3gckprd04.emc.com 152.62.177.24
esr3gckprd05.emc.com 152.62.177.25
esr3gckprd06.emc.com 152.62.177.26
esr3gckprd07.emc.com 152.62.177.27
esr3gckprd08.emc.com 152.62.177.28
esr3gckprd09.emc.com 152.62.177.29
esr3gckprd10.emc.com 152.62.177.30
esr3gckprd11.emc.com 152.62.177.31
esr3gckprd12.emc.com 152.62.177.32

esr3gsprd01.emc.com 152.62.45.21
esr3gsprd02.emc.com 152.62.45.22
esr3gsprd03.emc.com 152.62.45.23
esr3gsprd04.emc.com 152.62.45.24
esr3gsprd05.emc.com 152.62.45.25
esr3gsprd06.emc.com 152.62.45.26

2020年9月現在情報：
最新の情報をサポートまで必ずお問い合わせください
https://support.emc.com/kb/494729

Traffic must be permitted on ports 443 and 8443 for https traffic for the GAS (Global Access Servers) Servers. Failure to open port 8443 for the GAS servers will result in significant performance impact (30 - 45 %) and may result a delay in resolving issue with the end device.
NO SSL checking, Certificate verification, or Certificate Proxying is permitted.

In addition, SRS V3 (VE/DE) requires access to the below hosts for alternate connectivity method FTPS:
corpusfep4.emc.com = 168.159.209.45
corpusfep3.emc.com = 128.221.234.66
*The port for both hosts is 990

All GAS servers must be usable to allow for traffic efficiency and full redundancy.

The latest **Customer Environment Check Tool (CECT)** is available for download from Dell/EMC Online Support.

For ESRS Device Clients that are user installable, you must also permit traffic to EMC Online Support (support.emc.com). Users MUST have a registered account that is for the site at which the device / ESRS Device client is located.

Note:
We are unable to supply a specific IP address or range of addresses as the IP address is dependent on the location (Geo) of the DNS server resolving the EMC Online Support host to use. If the user MUST supply an IP address, they should use nslookup locally and use that IP address. It may be found that there is more than one IP address as DNSs may be doing a " Round Robin". If this is found, the user should configure this IP address in their firewall to permit failover. If using the hosts file on the ESRS IP Client (Gateway for Device), you can only use one IP address for EMC Online Support. This does create a minor exposure if the specific host referenced in the hosts file authentication to EMC Online Support may fail.

Search Dell Technologies for the most recent "Secure Remote Services Port Requirements" Guide

オンラインアカウントのご準備

事前準備

フルアクセス権限を持つオンラインアカウントの登録

1. Dell Technologies オンラインアカウントの登録（フルアクセス権限）
2. Loginを行い、対象のサイトIDを確認
3. サイト ID の配下にSRS接続を行う機器が入っていることを確認
4. SRS構成作業開始へ

https://www.delltechnologies.com/ja-jp/index.htm

アカウントの登録手順 (1/2)

1. Dell Technologies サイト（**https://www.delltechnologies.com/ja-jp/index.htm**）に移動し、ログインをクリックします。

2. サインインページの「Dell Technologiesを初めて使用しますか？」の必須入力フィールドを入力してください。
※電子メールフィールドには、会社のメール アドレスを入力してください。導入サイトとメールアドレスが紐づかない場合、その後の登録が完了しない場合がございます。

3. 「アカウントを作成」をクリックします。

4. 次のページへ移動すると、記入いただいたメールアドレスに、認証コード記載されたメールが届きます。

アカウントの登録手順 (2/2)

5. 認証コードを入力して「ビジネス アカウントの登録」の入力を行います。

6. 「Dell Technologiesとお客様との関係を選択してください」で「Dell Technologies の製品またはサービスの所有者」を選択します。

7. 「組織の情報を送信してください」に会社・組織名と住所を入力して「送信」してください。

8. 登録が終わると、登録完了とアクセスに関する情報が記載されたメールが届きます。

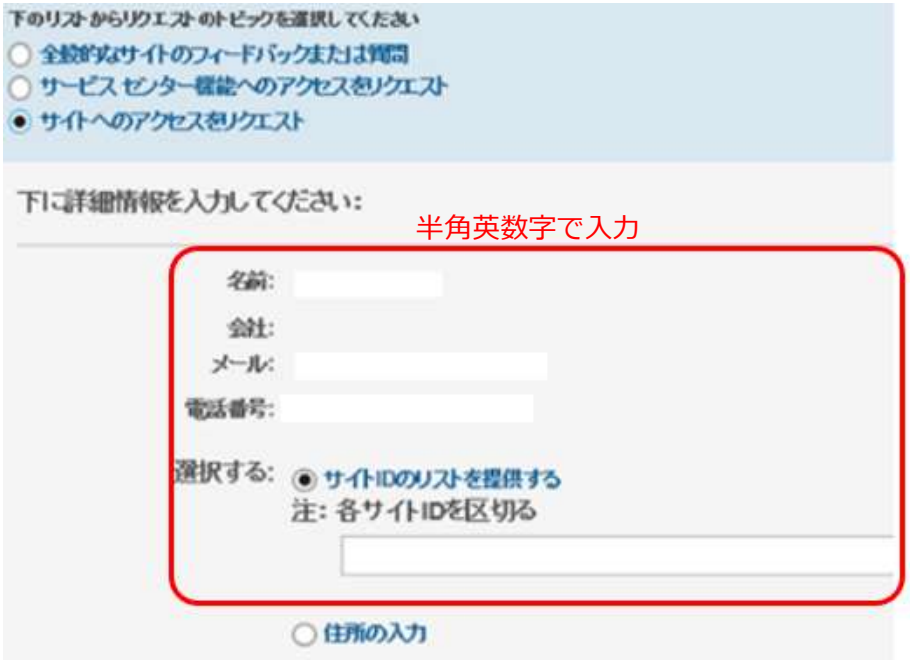
フルアクセス権限について

- Secure Remote Services を構成するためには、Dell Technologies オンライン サポート サイトのフル アクセス権限でのアカウントが必要です。
- 初期登録時の情報にて紐づくサイト情報が確認できない場合、制限のかかったアカウント登録となります。
- ご本人様確認のため、お客様自身からの申請（対象サイトID）を契機に承認が進められます。
  （すでにサイトに対して、管理者アカウントが設定されている場合、そのお客様に対して承認依頼が送付されます）

フルアクセス権限のリクエスト方法

1. https://support.emc.com/feedback にアクセスします。
2. [サイトへのアクセスをリクエスト] を選択します。
3. 表示された詳細情報を入力して、送信します。

注意：
このアカウントは管理者(※)としてのお客様に対してのみ有効であり、導入するパートナー様へ付与することはできません。
※エンドユーザー様のドメインを持つメールアドレスでの登録が必要となります。



構築後の注意点/FAQ

サポート構成に関する注意点

- SRS Gatewayは、冗長構成を取ることが推奨されております。（２台以上の配置）
- SRS Gateway１台（もしくはHA単位）あたり、**250デバイス**まで管理可能となります。
  （Policy Managerは、１台あたり、**750デバイス**まで管理可能）
- SRS/VE Gateway サーバはESXもしくはHyper-V環境のゲストVMとしてのみ動作します。
  SRS Gatewayサーバへのアプリケーション導入は、**非サポート構成**となります。
- Docker Editionの場合、SRSのみが動くLinuxをご用意ください。
- SRS/VE HA Gatewayの場合、異なる物理サーバ上のESXサーバもしくはHyper-Vに配置してください。
- SRSネットワーク要件を満たせば、SRS/VE Gateway の配置に関する制限はございません。
  （DMZ内外の配置、NIC冗長構成などの制限はございません。）
- SRS/VE Gateway 冗長構成の場合でも、1つのGlobal IPで問題ありません
- SRS Gateway へのPolicy Manager導入(co-locate)は不可となります。
- 外部接続時のProxy Serverにて認証が求められる場合、ADを使用した認証 (NTLM)は不可 となります。
- Policy Managerが動作するOSはPort 8090/8443を使用するため、それらを使う他のアプリケーション、Tomcat web server、VMware vCenter Server等との共存は不可となります
- Domain ControllerとなっているWindows ServerにPolicy ManagerをInstallすることは不可となります

構築後の注意点

SRSでは、サーバパラメータを変更した場合、再インストールが必要となるケースがございます

- SRS/VE Gateway　Reinstall **不要**

GW, IP Client に対する変更点	補足
Global IP　変更	設定変更不要
Internal IP 変更	FTP, SMTP, 筐体のConnect Home設定の変更が必要
Proxy IP 変更	Configuration Tool上でIP変更が必要

- SRS/VE Gateway　Reinstall **必要**

GW, IP Client に対する変更点	補足
Domainを構築時から変更(Join, Unjoin)	RSA LockBox Technologyの影響
Hostname変更	RSA LockBox Technologyの影響
MAC address 変更	RSA LockBox Technologyの影響
ESX server Upgradeを実施	Guest OSのMAC Addressが変更されない場合は、Reinstall 不要

構築後の注意点

- Policy Manager でサーバパラメータを変更しても、基本的には、再インストールは不要
  （障害対応等で必要と判断された場合は除く）
- Policy Managerの設定変更・Policy変更はお客様にて実施お願い致します。

Policy Managerに対する変更点	補足
Internal IP 変更	SRS Web UIのPolicy Manager IP設定変更が必要
Hostname 変更	Policy Managerの設定ファイルの変更
MACアドレス変更	設定変更不要
ESX Upgrade	設定変更不要
vMotionによるサーバ移動	設定変更不要
承認メール宛先変更	Policy Manager GUI上で設定変更
SMTPサーバ IP変更	Policy Manager の設定ファイル変更必要
Domainを構築時から変更(Join, Unjoin)	設定変更(Gateway側でReinstall) Domain ControllerをPolicy ManagerがInstallされているサーバに設定することは不可

そのほかFAQ

Question	Answer
ネットワーク環境での必要な設定は何か？	Dell TechnologiesのSRSインフラサーバのアドレスに対して、TCP Port 443及び8443を使用したOutbound 通信が許可されていることと、SRSインフラサーバが名前解決（DNS推奨）されることが必要です。 より詳細な情報につきましては、Port requirement guide や Knowledge Base (494729) をご参照ください。
外部からの脅威に対して大丈夫と言えるのですか？	業界標準の認証、証明書、暗号化技術を採用しており、充分なセキュリティを実現しています。通信で利用されるポートはTCP Port 443及び8443を使用したOutbound 通信のみです。Inbound の通信を許可する必要はありません。 また、お客様のDell Technologies機器とDell Technologies間の接続はすべてSRSアプリケーションから開始および管理が行われます。
Dell Technologiesのサポートエンジニアはどんなデータにアクセスするのか？	基本的にDell Technologiesのエンジニアがユーザデータにアクセスすることはございません。Policy Managerを利用することで、Dell Technologiesからデバイス(機器) へのリモートアクセスを拒否したり、アクセスの承認を要求することができます。履歴の保存も可能です。
すべての障害に対して、24時間365日の運用監視を保証してくれますか？	SRSのリモート監視機能は、お客様の高度な運用監視に代わってシステムの監視を保証するものではございません。インターネットを経由した機能となりますことから、特にミッションクリティカルなシステムでは、SRSに加えてお客様でも監視を実施いただくことをお勧めさせていただきます。

そのほかFAQ

Question	Answer
SRSは常時Pollingをしていますが、ネットワーク帯域に影響を与えますか？	30秒に一度、数kBのデータが送付されますが、NWに影響を与えることはございません。また、Log収集などの際のパケット転送量は、お客様NW帯域に依存した転送量となります。
SRS/VE Gateway とPolicy Managerは同一サーバに構成可能でしょうか？	構成できません。
SRSを冗長構成にする場合、Global IPは2つ以上必要でしょうか？	1つでも問題ございません。（IPマスカレードを使用可能です）
バックアップはどのように取得すればよいですか？	SRS GatewayPolicy Manager共にイメージバックアップが推奨となります。
Policy ManagerのRemote Access承認は何分以内に実施すれば宜しいでしょうか？	設定に依存いたしますが、30分以内が推奨値です。
Policy Manager 障害は、Dell Technologiesで検知されるのでしょうか？	いいえ、検知されません。

付録

SRS に関する最新情報については、EMC Online Support Siteの資料をご参照ください

SUPPORT BY PRODUCT > EMC Secure Remote Services Virtual Edition > Documentation >

現在Port Requirement guide / site Planning Guide / Installation Guideについて日本語ドキュメントを準備しており、Online Support Siteより入手可能となります。

< SRS Gateway Virtual Edition >

EMC Secure Remote Services Virtual Edition

- EMC Secure Remote Services Release 3.xx Release Notes
- EMC Secure Remote Services Release 3.xx Technical Description
- EMC Secure Remote Services Release 3.xx Port Requirements
- EMC Secure Remote Services Release 3.xx Site Planning Guide
- EMC Secure Remote Services Release 3.xx Operations Guide

Policy Manager

- EMC Secure Remote Services Policy Manager 6.8 Operations Guide
- EMC Secure Remote Services Policy Manager 6.8 Installation Guide


DELL Technologies

SRSクライアントの種類

Gateway Client
SRS/VE(Virtual Edition)

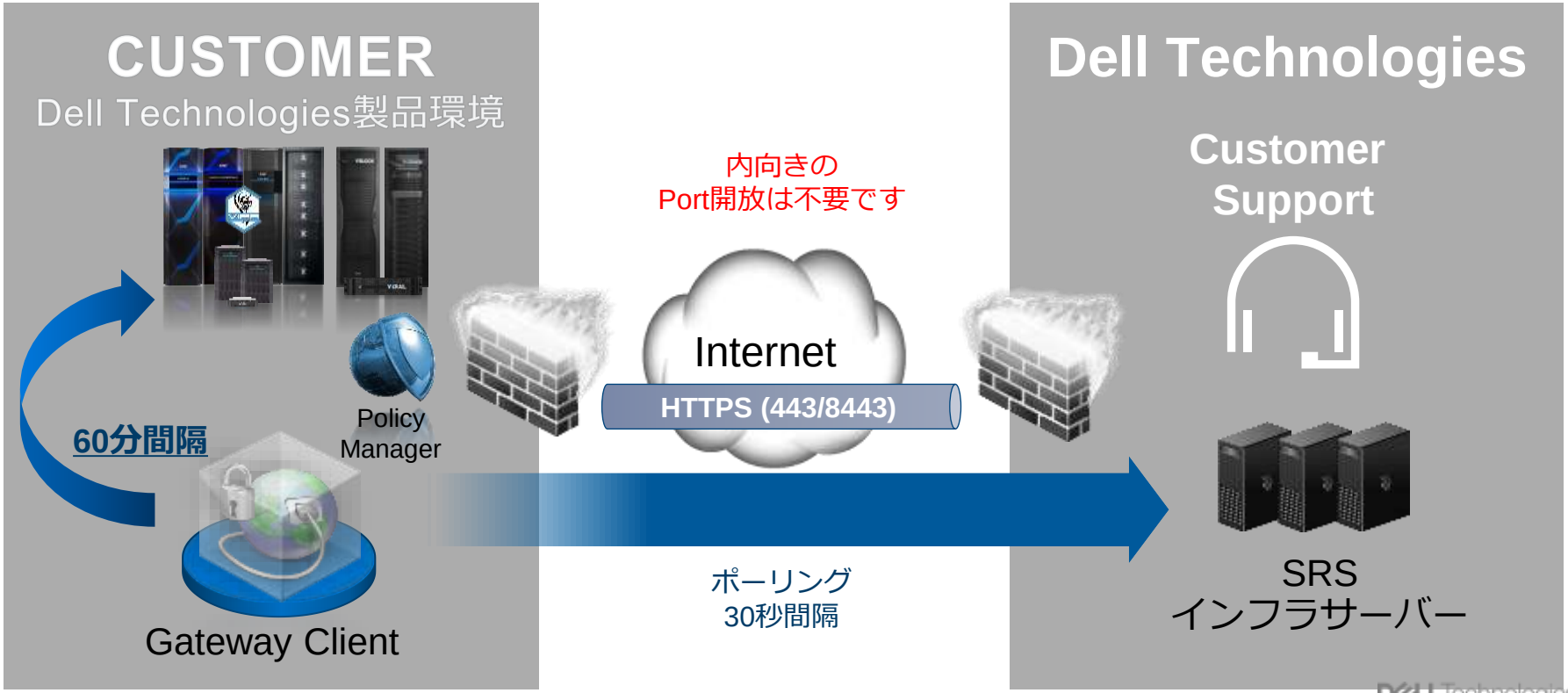
- 仮想アプライアンスや Docker コンテナとして提供
- 複数機器の情報をまとめてEMCのインフラサーバへ送信
- Gatewayとして機能
- HA (冗長)構成が可能

Device Client
統合型（Integrated)

- 製品に組み込まれた機能
  Unity、XtremIO、VxRail、
  VNX、VNXe
- 別途インストール不要
- 該当製品単体のみを監視
- 製品からEMCのインフラサーバへ直接通信

Gateway Client / マルチデバイス集約用SRS

Gateway Client 経由でのセキュアな接続



Device Client / 統合型SRS

製品に統合されたSRS機能を使用して直接接続