Hitachi Solutions Create

HITACHI

特権ID管理ソリューション SMART Gatewayのご紹介

株式会社日立ソリューションズ・クリエイト

目次

HITACHI

1. 内部不正による脅威

1. 内部不正による脅威

HITACHI

『情報セキュリティ10大脅威2025』では、組織向けの脅威として「内部不正による情報漏えい等」が4位に順位付けされています。

※2022年は5位、2023年は4位、2024年は3位、そして2025年は4位と高い順位で推移しています。

内部不正は、社会的信用の失墜、損害賠償により多大な損害を与えます。

1位	ランサム攻撃による被害	6位	リモートワーク等の環境や仕組みを狙った攻撃
2位	サプライチェーンや委託先を狙った攻撃	7位	地政学的リスクに起因するサイバー攻撃
3位	システムの脆弱性を突いた攻撃	8位	分散型サービス妨害攻撃（DDos攻撃）
4位	内部不正による情報漏えい等	9位	ビジネスメール詐欺
5位	機密情報等を狙った標的型攻撃	10位	不注意による情報漏えい等

出典：独立行政法人情報処理推進機構（IPA）発行「情報セキュリティ10大脅威 2025」より

事例（2023年10月社外発表）

コールセンタシステムの運用保守業務従事者が、**システム管理者アカウントを悪用**し、**お客さまデータが保管されている**
サーバーに不正にアクセスして、業務で使用していた端末等から、複数のクライアントのお客さま情報を持ち出していた。
不正に持ち出されたお客さま情報の件数：59組織、約900万件

2. 特権ID管理に求められる要件とは？

2. 特権ID管理に求められる要件とは？

HITACHI

「特権ID管理」に求められる要件(※)は、以下の4点です。

#	シーン	求められる要件	SMART Gateway	
			機能	実現方法
1	利用前	特権IDを利用できる人は **誰か？**	特権ID管理機能	SMART GatewayのユーザーIDと各システムの特権IDをひもづけて管理 グループに分けた管理も可能
2		特権IDの利用を **責任者が認めているか？**	ワークフロー機能 [オプション]	ワークフローによる特権IDの申請が可能
3	利用後	特権IDを使用した **作業の記録は残っているか？**	操作ログ管理機能	セッションログ、コマンドログ、ファイル 転送ログ、Webアクセスログ、SQLログの 取得が可能。また、動画も記録可能
4		特権IDを使用した**作業の** **妥当性を確認しているか？**		「誰が、いつ」を基本として、「どこへ接続したか」「何を転送したか」「何を実行したか」など、作業の妥当性を確認可能

SMART Gatewayで対応可能！

※ IT全般統制、J-SOX監査、PCI DSSなどのガイドラインにおいてうたわれている要件

3. SMART Gatewayの特長

3. SMART Gatewayの特長①　ゲートウェイ型で設置がしやすい

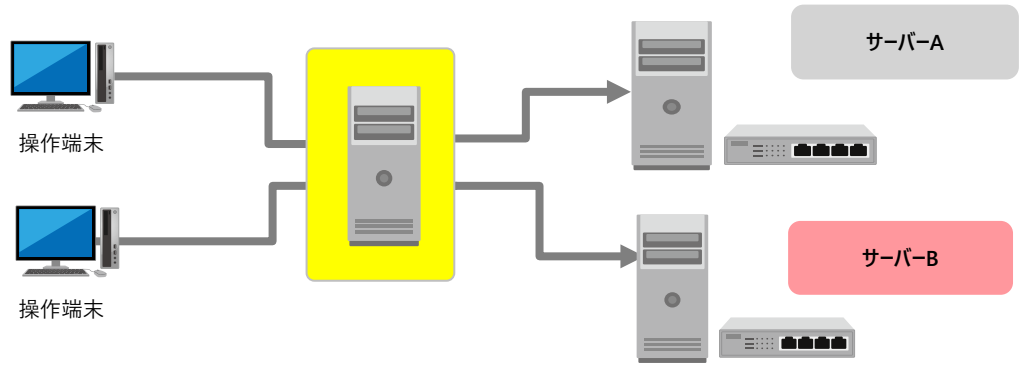
HITACHI

特権IDの管理方式の説明

【凡例】　・特権IDシステムへのアクセス（管理、制御、ログ取得など）
・操作端末から管理対象機器へのアクセス
・ID/パスワードの貸出

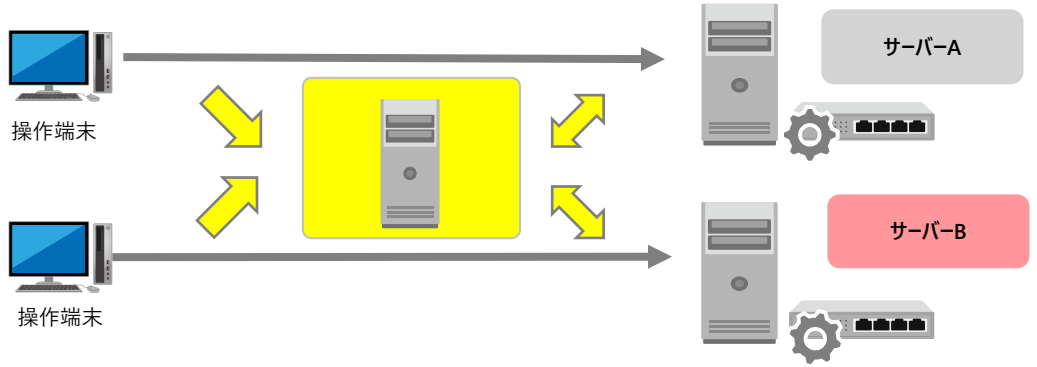
ゲートウェイ型 (エージェントレス)

■操作端末と管理対象機器の**間に**ゲートウェイサーバーを配置



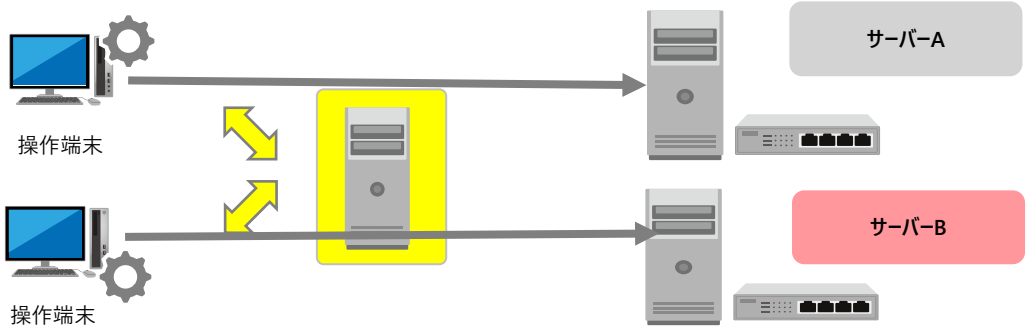
サーバー・エージェント型

■管理対象機器**全てに**エージェントをインストール



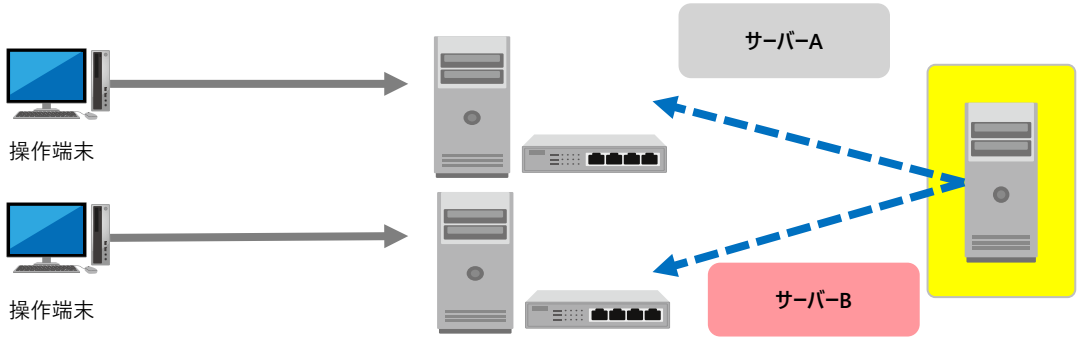
クライアント・エージェント型

■操作端末**全てに**エージェントをインストール



ID/パスワード貸出型

■ID/パスワード貸出用のサーバーを設置



3. SMART Gatewayの特長①　ゲートウェイ型で設置がしやすい

HITACHI

特権IDの管理方式の比較

管理対象が多く、
既存システムへの影響を
最小限にしたい場合

	ゲートウェイ型	クライアント・エージェント型 接続端末が特定されている場合	サーバー・エージェント型 管理対象で詳細なログを取得したい場合	ID/パスワード貸出型 特権IDが少ない場合、統合認証基盤と併用する場合
システム導入	ゲートウェイサーバーのみ、エージェント不要のため導入が容易	操作端末の事前検証、インストール工数が必要	管理対象の事前検証、インストール工数が必要	事前にID/パスワードの棚卸しが必要
導入後の拡張性、保守運用	管理対象による接続設定のみで利用可能	クライアントへの影響確認が必要、インストール分の費用増額	管理対象への影響確認が必要、インストール分の費用増額	定期的にID/パスワードの棚卸しが必要
アクセス制御	細かな制御が可能(グループ単位、アクセス先の制限)	使わせる/使わせないの二択での制御(管理対象にはシングルサインオン)	ローカルログインを含めたきめ細やかな制御が可能	使わせる/使わせないの二択での制御
ログ取得	ゲートウェイを通過する操作のログを取得(エージェント型より取得できるログは少ない)動画の記録が可能	操作端末での操作ログを取得	ローカルログインを含めたきめ細やかなログ取得が可能	貸出、利用のログのみ

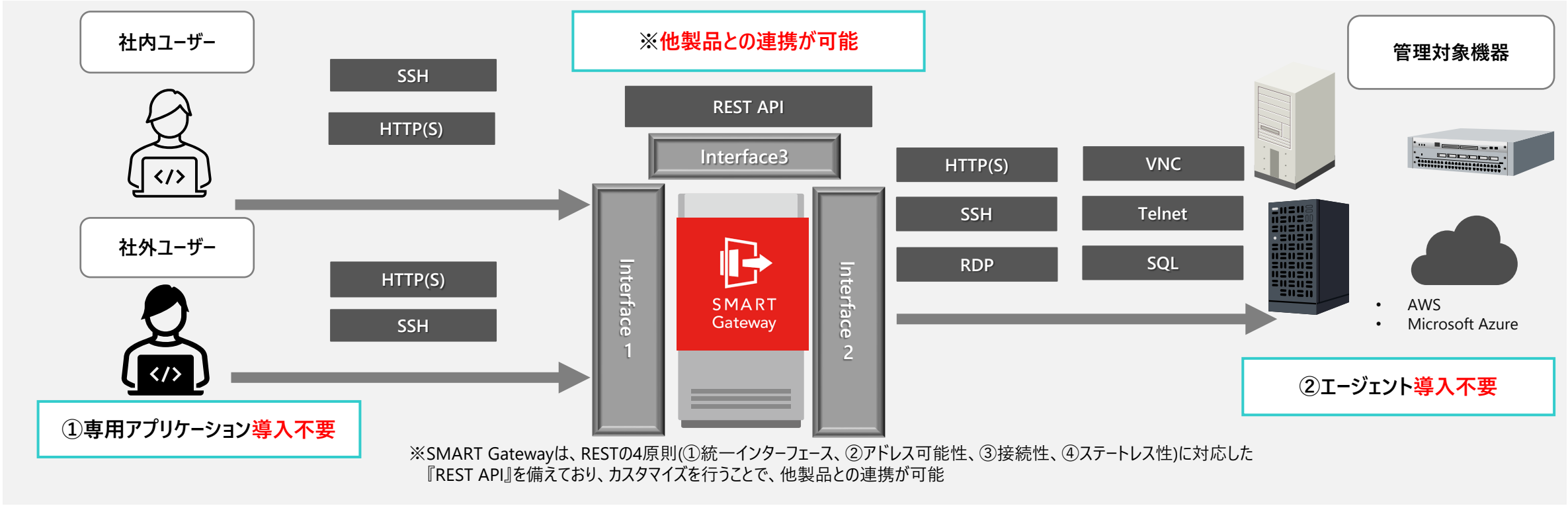
3. SMART Gatewayの特長①　ゲートウェイ型で設置がしやすい

HITACHI

ゲートウェイ型の利点

ユーザー側、管理対象機器側にソフトウェアのインストールが不要

①ユーザー側に専用アプリケーションが不要 [Interface1]
　→Webブラウザーもしくは、SSHクライアントでアクセス
②管理対象機器側にエージェント導入不要 [Interface2]
　→HTTP(S), SSH, RDPなどの基本的なプロトコルで接続



※SMART Gatewayは、RESTの4原則(①統一インターフェース、②アドレス可能性、③接続性、④ステートレス性)に対応した
『REST API』を備えており、カスタマイズを行うことで、他製品との連携が可能

3. SMART Gatewayの特長②　操作がしやすい

HITACHI

Webブラウザーからワンクリックで対象機器へアクセス

SMART Gatewayにログインすると、接続権限がある接続先の一覧が表示され、
ユーザーは、接続先を選択してクリックするだけで、対象機器にアクセス可能

Web UIからの接続例

Webブラウザーが端末エミュレーターとなり、
LinuxのCLIやWindowsのGUIを表示

※接続可能な機器は管理者が設定するため、
　ユーザーは、接続先のID/パスワードを知らなくても対象機器にアクセス可能

3. SMART Gatewayの特長③　取得できるログの種類が豊富

HITACHI

特権IDを使用した作業の記録を基に作業の妥当性を確認可能

取得ログ

セッションログ

- 誰が、いつ、どこへ接続
- ユーザー
- 接続先
- 接続元
- プロトコル
- 接続開始時間
- 接続終了時間

コマンドログ

- 誰が、いつ、どこへ接続
- ユーザー
- 接続先
- 接続元
- プロトコル
- 接続開始時間
- 利用コマンド

ファイル転送ログ

- 誰が、いつ、どこへ接続
- ユーザー
- 接続先
- 接続元
- プロトコル
- 方向
- MD5値

Webアクセスログ

- 誰が、いつ、どこへ接続
- ユーザー
- 接続先
- 接続元
- プロトコル
- 接続開始時間
- 接続終了時間

SQLログ

- 誰が、いつ、どこへ接続
- ユーザー
- 接続先
- 接続元
- プロトコル
- 接続開始時間
- 利用コマンド

動画ログ

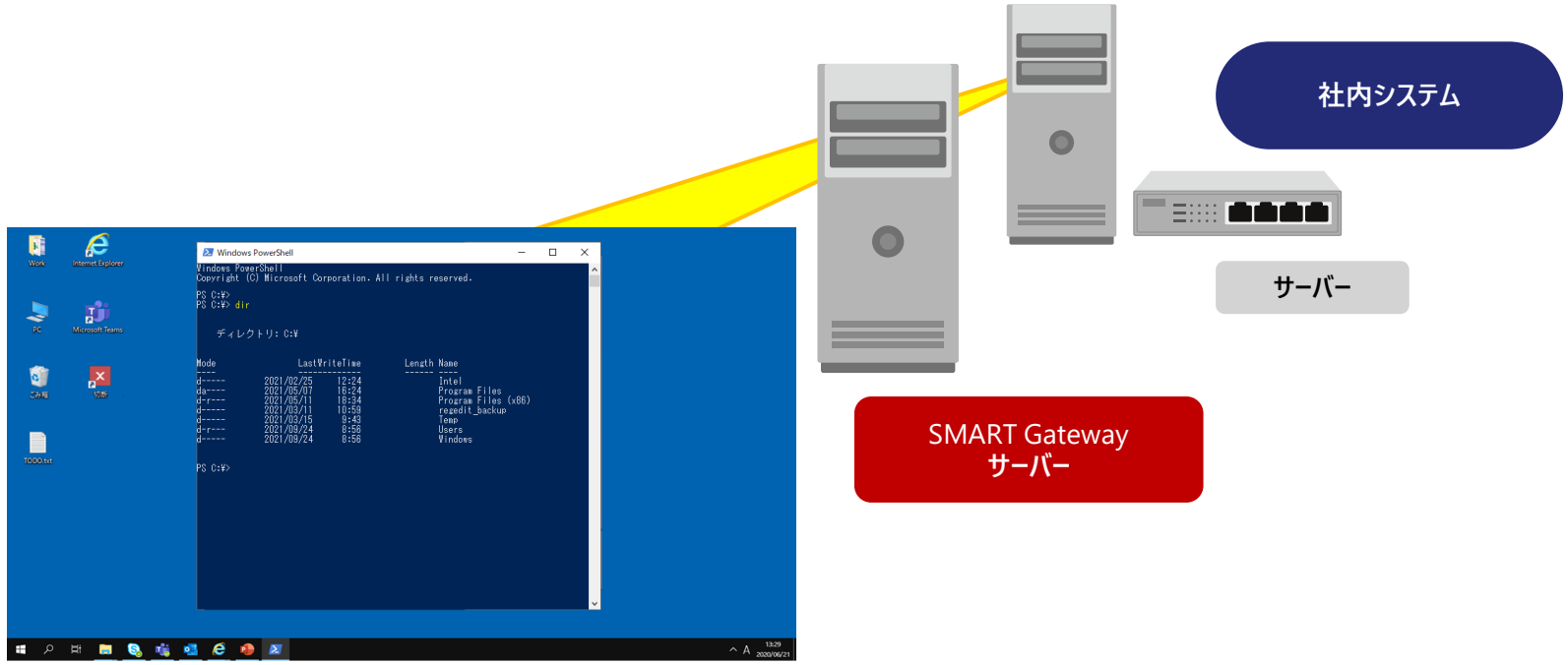
- 全てのプロトコルで対応
- ユーザー

3. SMART Gatewayの特長④　特権IDを使用する業務を支援

HITACHI

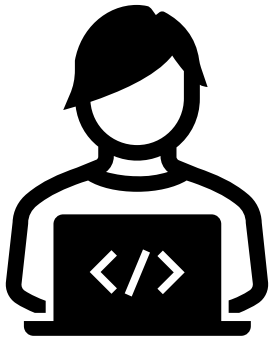
リモートコントロールで作業

■サーバールームに入室せずに作業可能
■作業途中やチェックポイントで、
　複数人でチェックが可能



「作業の効率化」を支援

■マルチモニター機能
　→複数の管理対象に同時に接続
■ファイル転送機能
　→作業対象サーバーにファイルを転送



「作業品質の確保」を支援

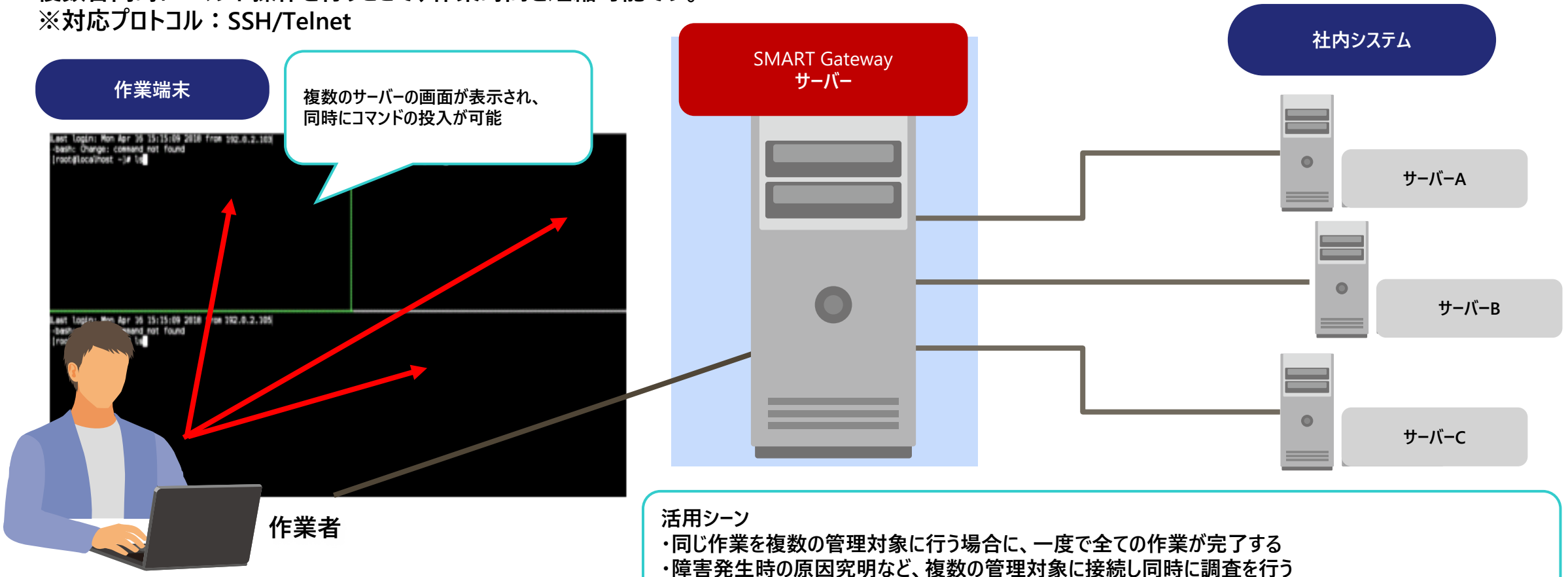
■アクション(自動実行)機能
　→同じ作業を複数のサーバーに実施
■アクセス制御機能
　→誤った機器への接続を防止
■特権コマンド制御機能
　→許可しないコマンドをブロック

3. SMART Gatewayの特長⑤　[ご参考]各機能の詳細

HITACHI

マルチモニター機能　⇒「作業の効率化」を支援

複数の管理対象に対し同時に接続し、作業を行えます。
複数台同時にコマンド操作を行うことで、作業時間を短縮可能です。
※対応プロトコル：SSH/Telnet



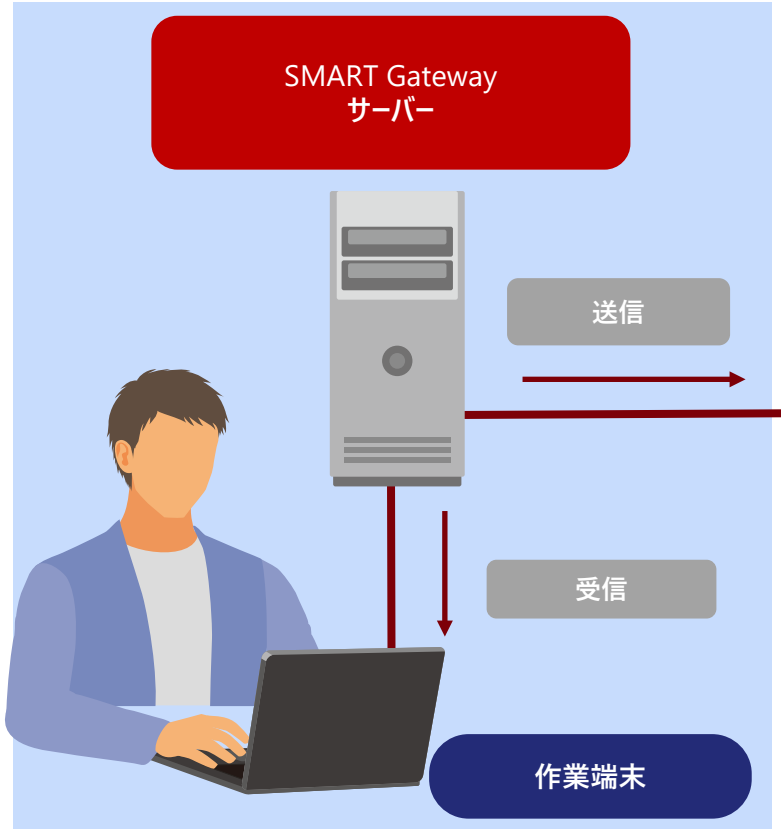
活用シーン
・同じ作業を複数の管理対象に行う場合に、一度で全ての作業が完了する
・障害発生時の原因究明など、複数の管理対象に接続し同時に調査を行う

3. SMART Gatewayの特長⑤　[ご参考]各機能の詳細

HITACHI

ファイル転送機能　⇒「作業の効率化」を支援

Webブラウザー経由で管理対象に手を加えずにファイルの送受信が可能です。
ファイルの送受信結果は操作ログとして記録されます。
※対応プロトコル：SSH/RDP/HTTP



※RDP 接続にてWindows にログイン

3. SMART Gatewayの特長⑤　[ご参考]各機能の詳細

HITACHI

アクション(自動実行)機能　⇒「作業品質の確保」を支援

定例的に行う処理をアクションとして登録し、実行できます。
定例処理をボタンひとつで実行可能にすることで、人的ミスの軽減および作業効率を向上させます。

アクション作成 → **実行** → **ログ確認**

実行コマンドを記述した
アクションを作成し、事前に登録

ユーザーが実行ボタンを
押すだけで、自動で処理を実行

実行結果はテキストログで
すぐに確認可能

3. SMART Gatewayの特長⑤　[ご参考]各機能の詳細

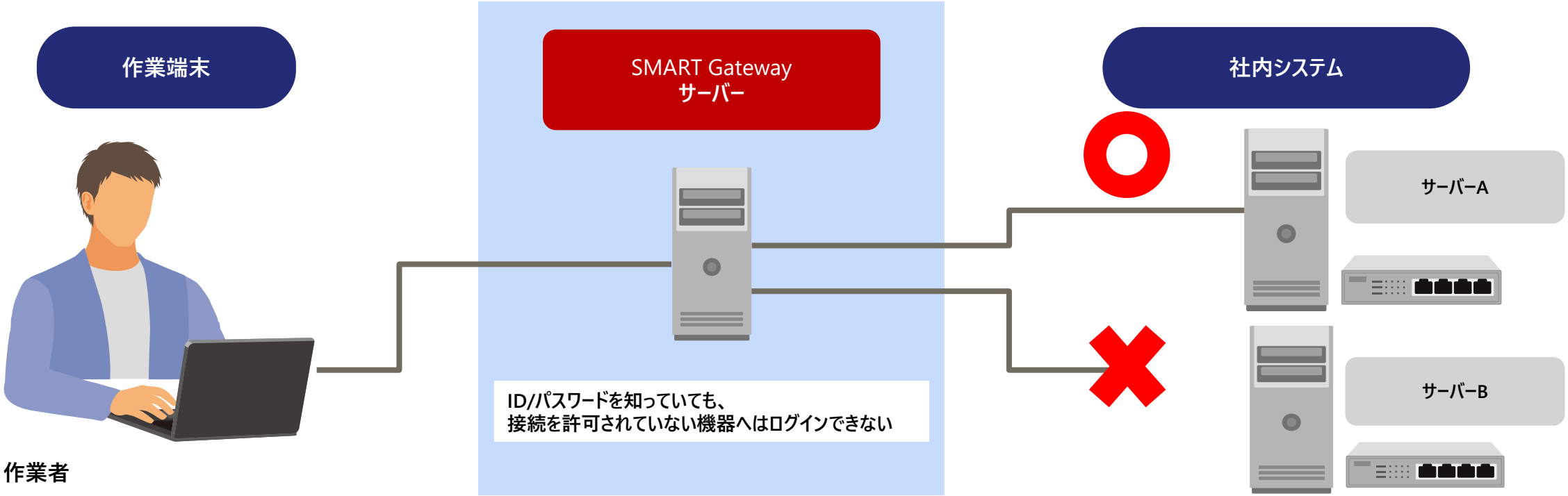
HITACHI

アクセス制御機能　⇒「作業品質の確保」を支援

SMART Gatewayで利用者ごとに接続可能な管理対象機器を設定することで、
間違った対象への接続を防止できます。

例）サーバーAの接続のみを許可するよう設定した場合
　　サーバーAへの接続：接続可能
　　サーバーBへの接続：接続不可

アクセス制御機能により、
ゲートウェイ型の特長である、
細かなアクセス制御を実現



3. SMART Gatewayの特長⑤　[ご参考]各機能の詳細

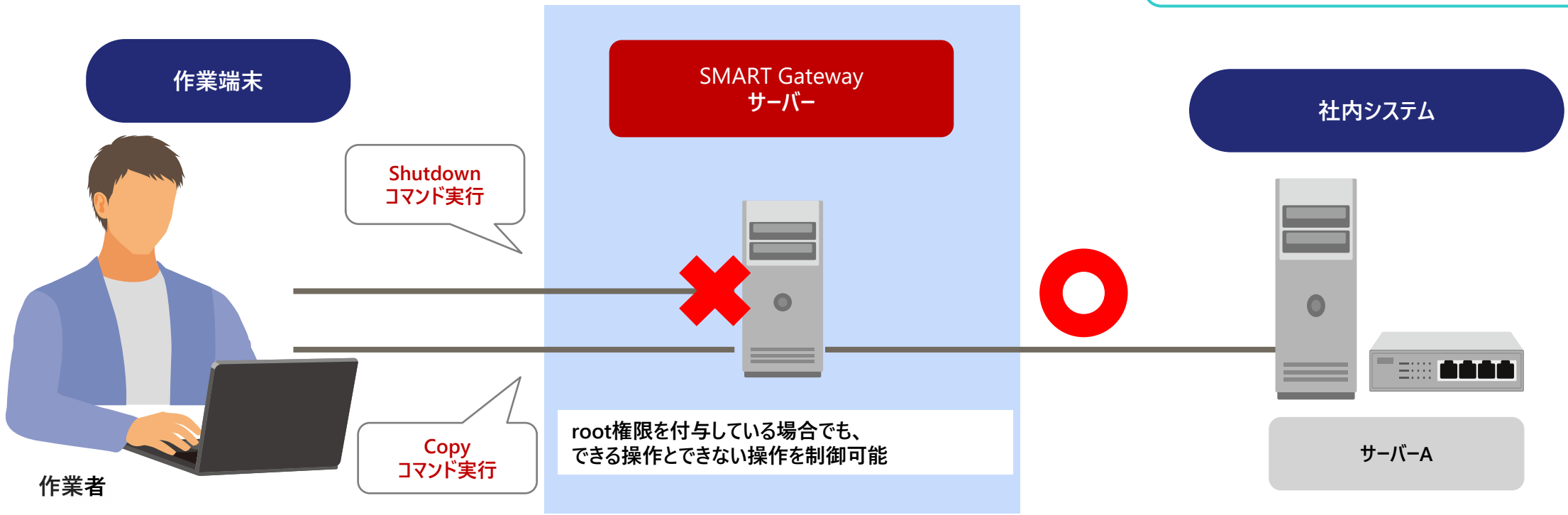
HITACHI

特権コマンド制御機能　⇒「作業品質の確保」を支援

利用者や管理対象機器に対して、コマンドレベルでのルールの作成が可能です。
許可していないコマンドをブロックすることで、操作ミスや不正操作によるシステム変更を防止します。

例）Shutdownコマンドを実行できないように設定した場合
　　Shutdownコマンド　：実行拒否
　　上記以外のコマンド：実行許可

特権コマンド制御機能により
ゲートウェイ型の特長である、
細かなアクセス制御を実現

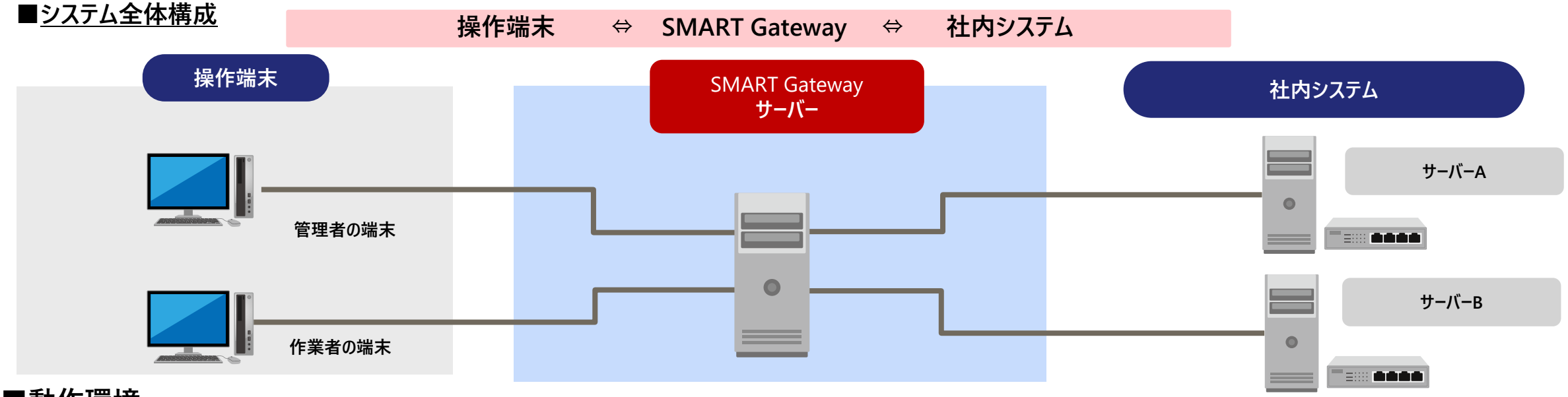


4. SMART Gatewayの構成

HITACHI

SMART Gatewayの構成

■システム全体構成



■動作環境

操作端末	HTML5対応のWebブラウザー(Google Chrome、Firefox、Microsoft Edge)からGUIへのアクセス、 またはSSHからCUIへのアクセス
SMART Gatewayサーバー	Linux (CentOS Stream 8 / Red Hat Enterprise Linux 8 / AlmaLinux 8 / Rocky Linux 8 / Oracle Linux 8 / CentOS Stream 9 / Red Hat Enterprise Linux 9 / AlmaLinux 9 / Rocky Linux 9 / Oracle Linux 9 / Ubuntu20 / Ubuntu22)系のサーバー（オンプレミス・クラウドいずれも構築可能）
社内システム	RDP、SSH、Telnet、HTTP(S)でアクセス可能なアプリケーション全般

HITACHI

SMART Gatewayサーバーについて

■ハードウェア要件

導入規模	CPU/Memory	Disk容量	同時接続数	備考
小規模	2コア / 8GB 以上	40GB 以上	20	セッション録画なし、接続の割合としてCLI 利用:8 割、Web UI 利用:2 割を想定したシステムの場合。 録画を実施する場合は初期設定（640x480、2Mbps）で毎時900MByte 程度のDisk 容量が追加で必要。
中規模	8コア / 24GB 以上	60GB 以上	250	
大規模	40コア / 248GB 以上	100GB 以上	5,000	

■ソフトウェア要件

ソフトウェア	バージョン
OS	CentOS Stream 8 / Red Hat Enterprise Linux 8 / AlmaLinux 8 / Rocky Linux 8 / Oracle Linux 8 / CentOS Stream 9 / Red Hat Enterprise Linux 9 / AlmaLinux 9 / Rocky Linux 9 / Oracle Linux 9 / Ubuntu20 / Ubuntu22

HITACHI

SMART Gatewayサブスクリプション・ライセンス体系(通常)

ライセンス	管理対象	標準価格（円/年） （税抜）
スタンダード	管理対象数　：1 ～ 20 接続*1 セッション数：1 ～ 20 セッション*2	970,200 円
エンタープライズ	管理対象数　：1 ～ 250 接続*1 セッション数：1 ～ 250 セッション*2	4,851,000円
キャリア	管理対象数　：1 ～ 5000接続*1 セッション数：1 ～ 5000セッション*2	14,850,000円

*1: 管理対象への接続タイプ(プロトコル)登録数。
　同一管理対象ホストに対して、HTTP接続とSSH接続を行う場合には 2 接続とカウントします。
*2: SMART Gatewayを介して作業をしているセッション数（アクティブセッション数）。

例）管理対象数270台で、HTTP接続とSSH接続を行う環境(合計540接続)へ導入する場合
　エンタープライズのライセンス 2 本とスタンダード 2 本の購入が必要です。

HITACHI

SMART Gatewayプラグイン体系　◆サブスクリプション（年間契約）

プラグイン	機能説明	標準価格（円/年）（税抜）		
		スタンダード	エンタープライズ	キャリア
ファイル転送	接続先とグラフィカル、直感的かつ円滑なファイル転送を実現する機能を提供します。FTP、SFTP、SCP、TFTPなどさまざまなプロトコルに対応しています。	96,000円	236,000円	360,000円
CSVインポート・エクスポート	CSVによる一斉データ登録や一斉データ更新など情報を一斉インポートする機能を提供します。	80,000円	196,000円	300,000円
承認フロー	接続先の利用承認を管理し、接続許可のワークフロー化をSMART Gateway上で実現できる機能を提供します。	192,000円	472.000円	720,000円
SSHワンタイムパスワード	SSH接続で、ワンタイムパスワードを利用した SMART Gatewayへのログインを実現する機能を提供します。	297,000円	735,000円	1,080,000円
マネジメントログ	SMART Gateway本体の管理ログを集積して表示します。SMART Gatewayそのものへの管理操作の監査遂行において強力な機能を提供します。	80,000円	196,000円	300,000円
アナウンスメント	SMART Gateway利用ユーザーに対して、各種情報のアナウンスメントを行う機能を提供します。	80,000円	196,000円	300,000円
監査ログ自動削除	収集したデータを一定期間で削除する機能を提供します。	80,000円	196,000円	300,000円

お問い合わせ先

HITACHI

■お問い合わせ先

株式会社 日立ソリューションズ・クリエイト

- **Webでのお問い合わせ**
  www.hitachi-solutions-create.co.jp/contact/solution.html

  お問い合わせページより、商品・サービスをお選びください。
- **メールでのお問い合わせ**
  hsc-contact@mlc.hitachi-solutions.com

■お問い合わせ情報について

ご相談、ご依頼いただいた内容は回答などのため、当社の関連会社（日立ソリューションズグループ会社）および株式会社日立製作所に提供（共同利用含む）することがあります。
取り扱いには充分注意し、お客さまの許可なく他の目的に使用することはありません。

表示に関する注意事項

HITACHI

■他社商品名、商標などの引用に関する表示

- SMART Gatewayは、株式会社ボスコ・テクノロジーズの日本における登録商標です。
- AWSは、Amazon.com, Inc. またはその関連会社の商標です。
- Linuxは、Linus Torvaldsの登録商標です。
- Google Chrome は、Google LLC の登録商標です。
- Firefox は、Mozilla Foundation の登録商標です。
- Microsoft Azure、Microsoft Edge、Windows は、Microsoft Corporation の登録商標です。
- CentOSは、Red Hat, Inc. の商標です。
- Red Hat Enterprise Linuxは、米国およびその他の国におけるRed Hat, Inc.の登録商標です。
- AlmaLinuxは、AlmaLinux OS Foundation の商標です。
- Rocky Linuxは、Rocky Enterprise Software Foundationの商標です。
- Oracleは、Oracle Corporation の登録商標です。
- Ubuntuは、Canonical Ltd. の商標または登録商標です。

表示に関する注意事項

HITACHI

■サービス・製品の仕様に対する表示

本資料に記載しているサービス・製品の仕様は、2025年8月現在のものです。

サービス・製品の改良などにより予告なく記載されている仕様が変更になることがあります。


HITACHI