

統合システム運用管理

セキュリティ管理

JP1/秘文 のご紹介

～情報漏えいを未然に防ぎ会社の大切な情報を守る～



株式会社 日立製作所

Contents

- JP1/秘文 の概要
- できること
- システム構成例
- 安心してお使いいただくためのサポート

「出さない」「見せない」2つのシンプルな対策で 会社の大切な情報を漏えいのリスクから守ります

JP1/秘文は、情報の不正な持ち出しや、人的ミスによる情報漏えいを未然に防ぎ、
安全な方法で情報を利用するためのセキュリティ対策製品です

出さない



漏えいしてはいけない情報を
社外に「出さない」

見せない



機密データの
中身を「見せない」

できること

- JP1/秘文 でできること
- 漏えいしてはいけない情報を、社外に「出さない」
- 機密データの中身を「見せない」

会社の大切な情報資産を守る

JP1/秘文 Device Control、JP1/秘文 Data Encryption

出さない

- デバイスの利用を制限
- 接続先ネットワークを制御
- ネットワーク識別による
スクリーンロック
- ログの取得・管理



見せない

- 社内利用のデータを自動的に暗号化
- 社外に持ち出すデータは
パスワードで保護
- マルウェアによるアクセスから
機密ファイルを保護



「出さない」 × 「見せない」 で
管理者主導のセキュリティ対策を実現



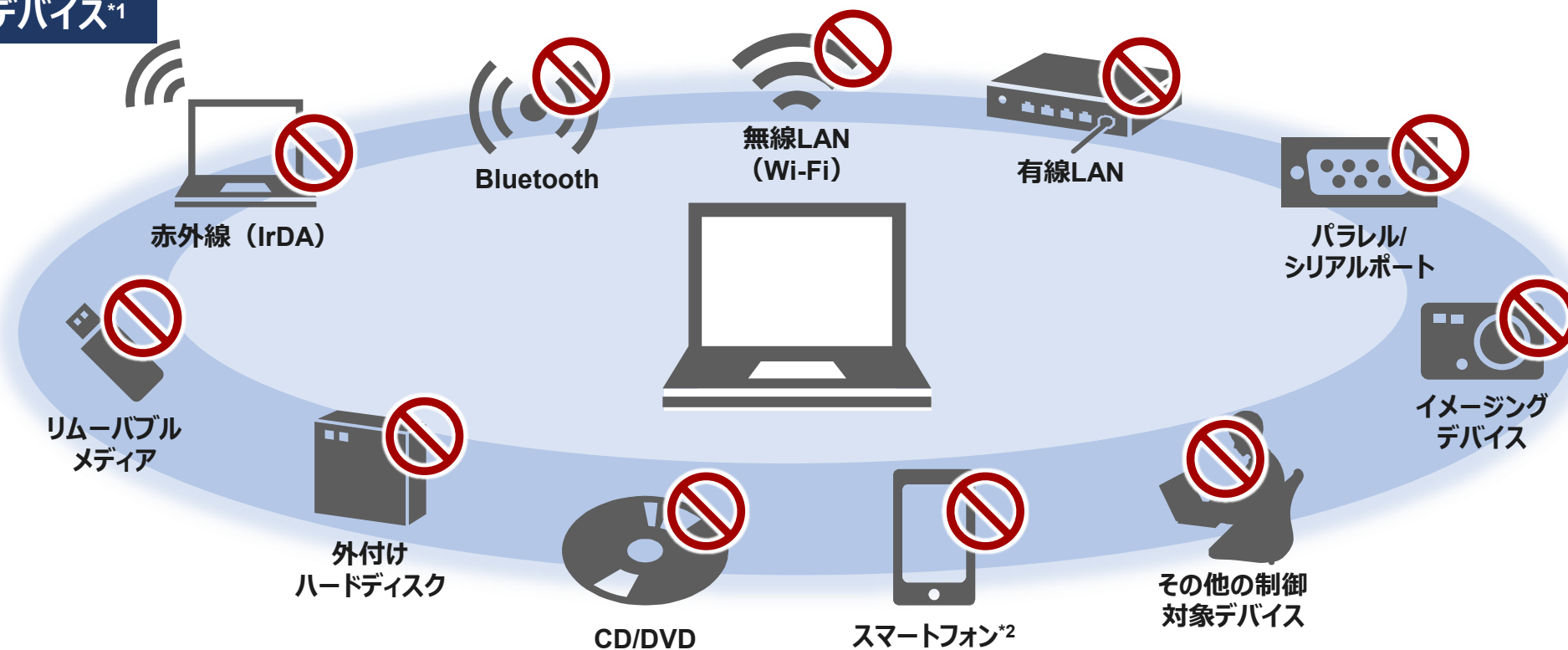
漏えいしてはいけない情報を、社外に「出さない」 デバイスの利用を制限

出さない

HITACHI
Inspire the Next

さまざまなデバイスの利用やネットワーク接続を制限することで、不正なデータの持ち出しによる情報漏えいを防ぎます。特定の機種のみ利用を許可することや、部署や利用者ごとに許可・禁止を設定できるため、お客さまの状況にあわせた柔軟な運用が可能です。

制限できるデバイス*1



IrDA: Infrared Data Association

*1 キーボード、マウスなどのヒューマンインタフェースデバイスは対象外です。

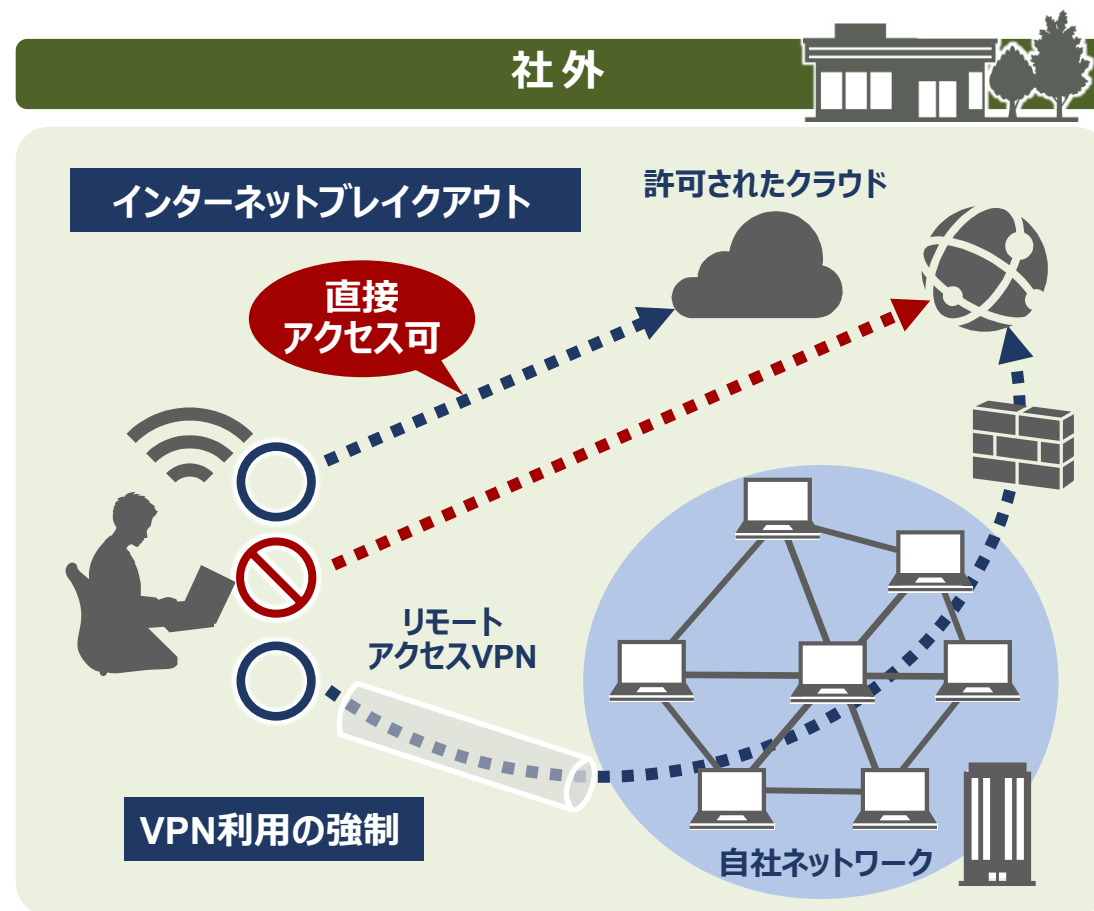
*2 スマートフォンは、OS、製造メーカー、接続方法などの違いによって、さまざまなデバイスとして認識されます。JP1/秘文はこれらのすべてのデバイスを利用禁止にすることで、スマートフォンへのデータコピーを防止します。

漏えいしてはいけない情報を、社外に「出さない」 接続先ネットワークを制御

出さない

HITACHI
Inspire the Next

社内ではWi-Fi制御により、管理者が許可したアクセスポイントのみを表示し、それ以外のアクセスポイント利用を禁止できます。社外では、インターネット接続時に社内VPNへの接続を強制することで、安全性を確保します。許可されたクラウドサービスへの接続時は、インターネットブレイクアウトを利用して直接アクセスできるようにすることで、クラウドサービスの快適な利用を実現します。

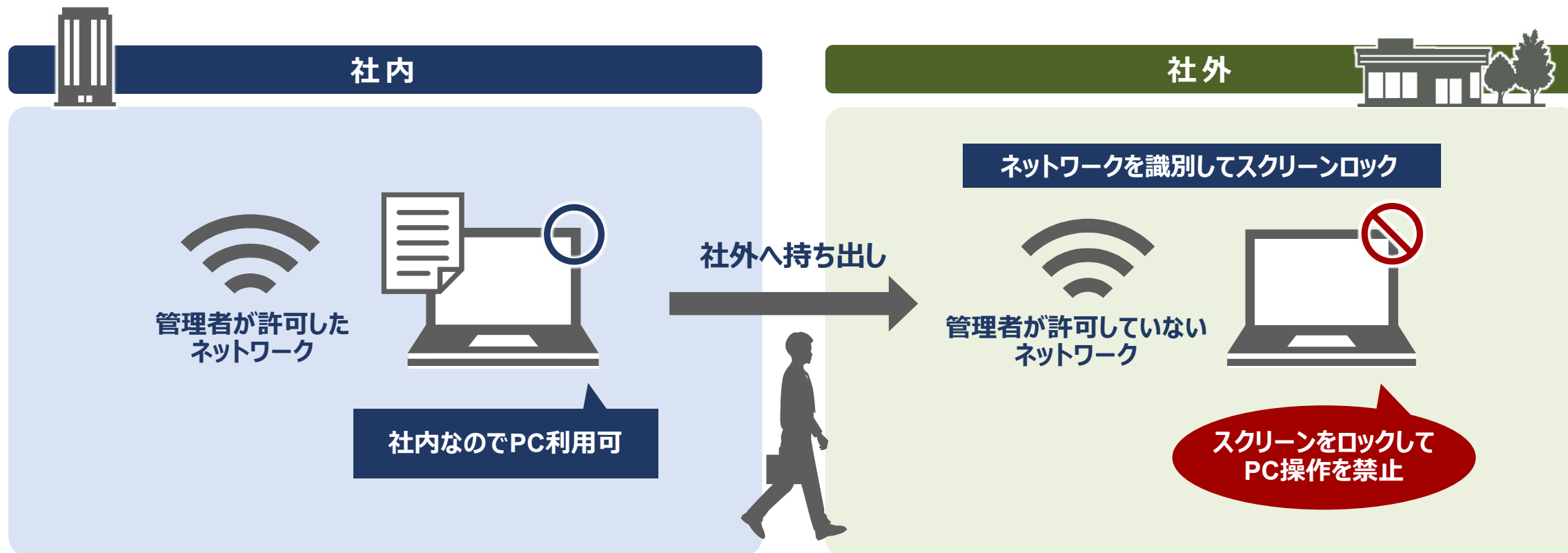


漏えいしてはいけない情報を、社外に「出さない」 ネットワーク識別によるスクリーンロック

出さない

HITACHI
Inspire the Next

管理者が許可したネットワークに接続していない場合、スクリーンロックによりPC操作を禁止します。ノートPCなどを社外に持ち出しても、スクリーンロックにより不正なデータ利用が防止できます。

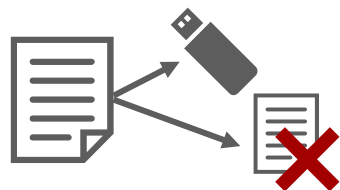


PC上のさまざまなユーザー操作ログが取得できます。USBメモリへのデータコピーといったファイル操作ログを確認することで、不正なデータ持ち出しなど違反の検出が可能。また、ログ管理を周知することで不正行為の抑止効果も期待できます。

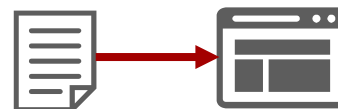
取得できる主なログ*



ファイル操作ログ



ブラウザー操作ログ



クリップボード操作ログ



アプリケーション操作ログ



リモートデスクトップ
接続ログ



Windowsサインイン・
サインアウトログ



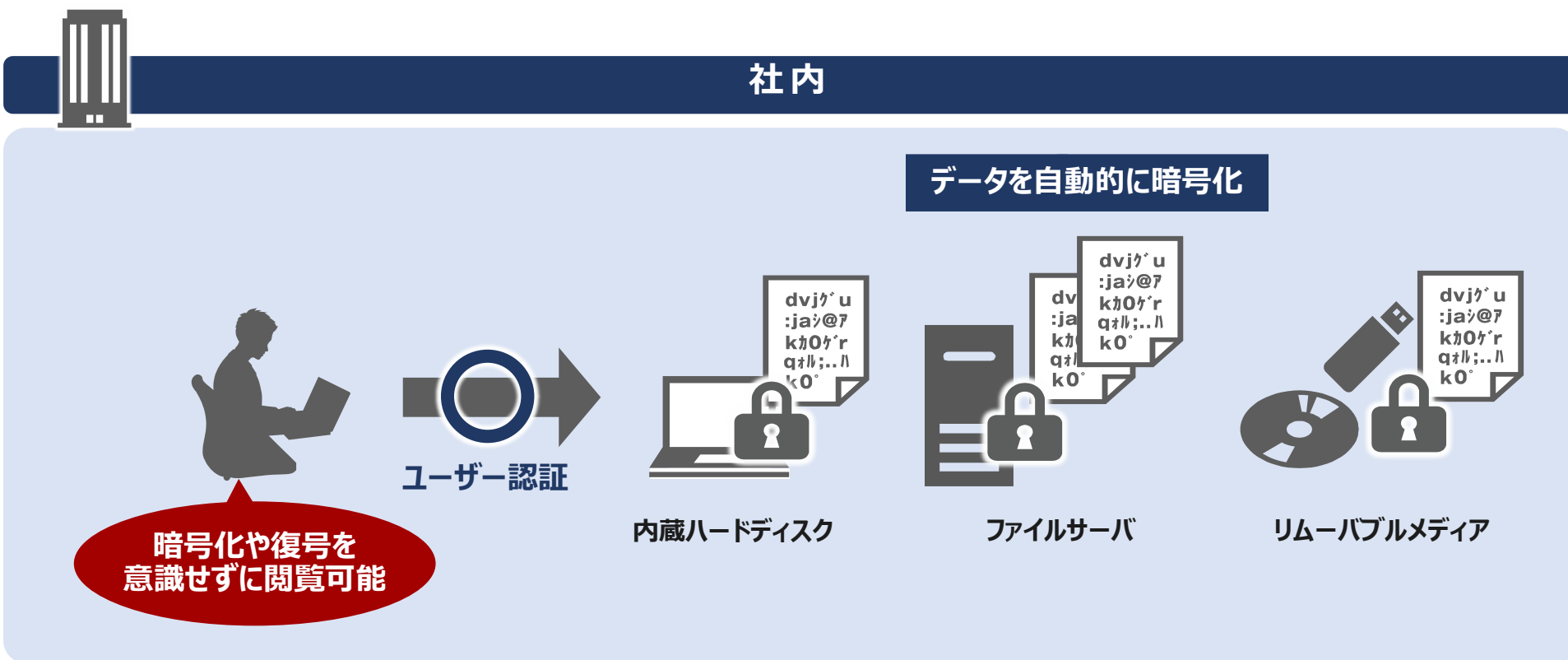
*取得可能な操作ログの詳細についてはお問い合わせください。

機密データの中身を「見せない」 社内利用のデータを自動的に暗号化

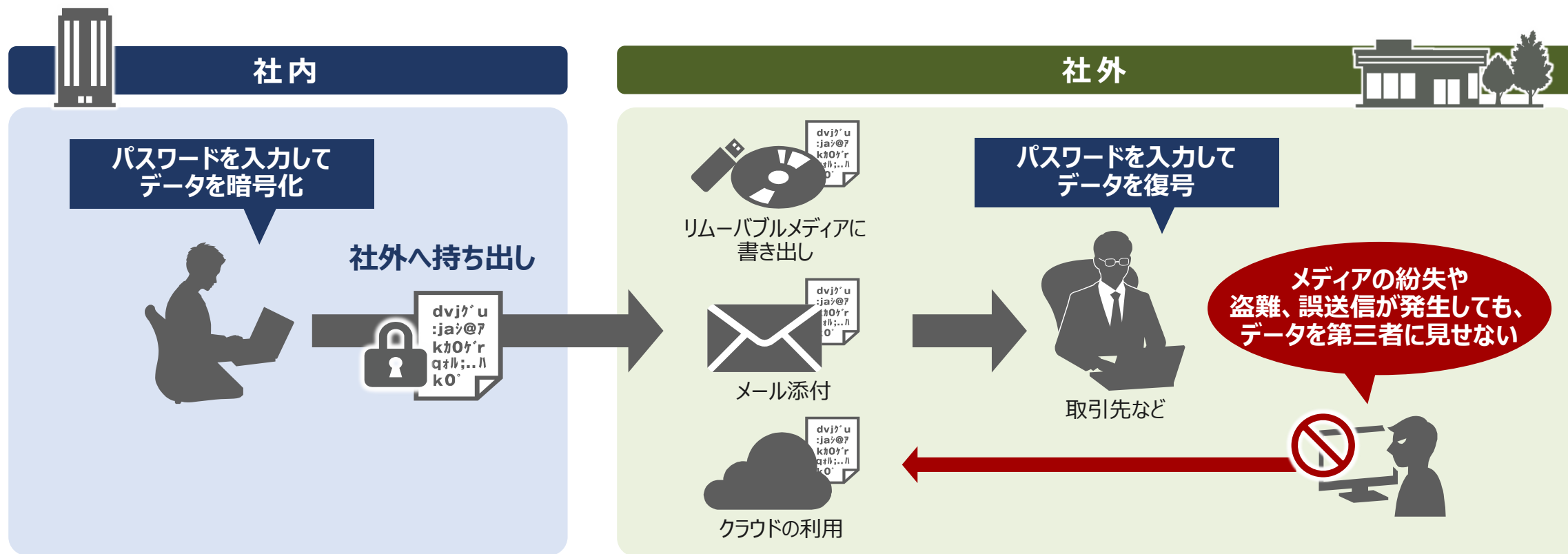
見せない

HITACHI
Inspire the Next

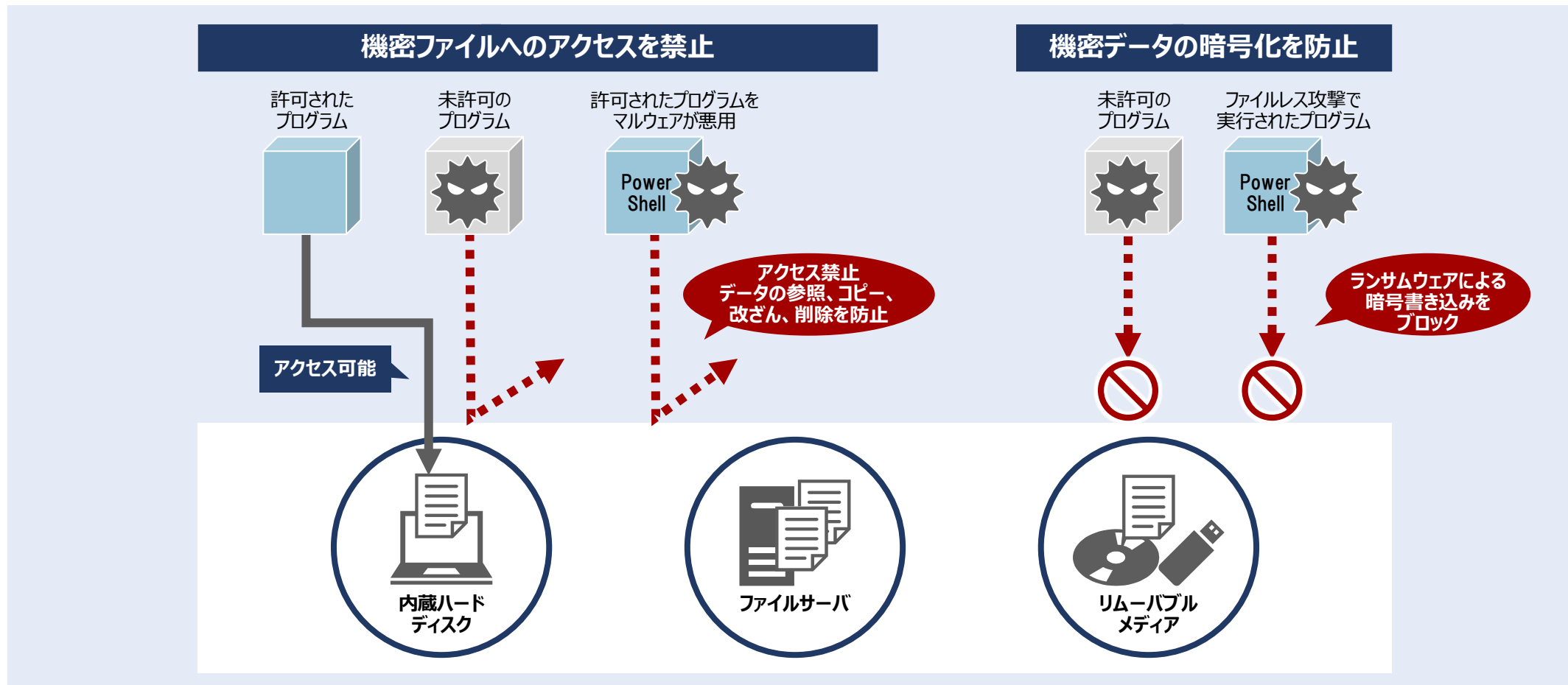
社内PCの内蔵ハードディスクをドライブごと暗号化し、PCの盗難や置き忘れなどによる情報漏えいを防止します。PCに保存されたデータは強制的・自動的に暗号化されるため、利用者が暗号化や復号を意識する必要はありません。また、リムーバブルメディアや外付けハードディスク、CD/DVD、ファイルサーバの共有フォルダも暗号化するので、社内でのデータのやりとりを安全に効率よく行えます。



リムーバブルメディアへの書き出しやメール添付、クラウドサービスの利用などで社外にデータを持ち出す場合は、パスワード入力により復号可能な形式でデータを暗号化できます。万一、紛失や盗難、誤送信が起きた場合でも、パスワードを知らない第三者による解読を防ぎます。



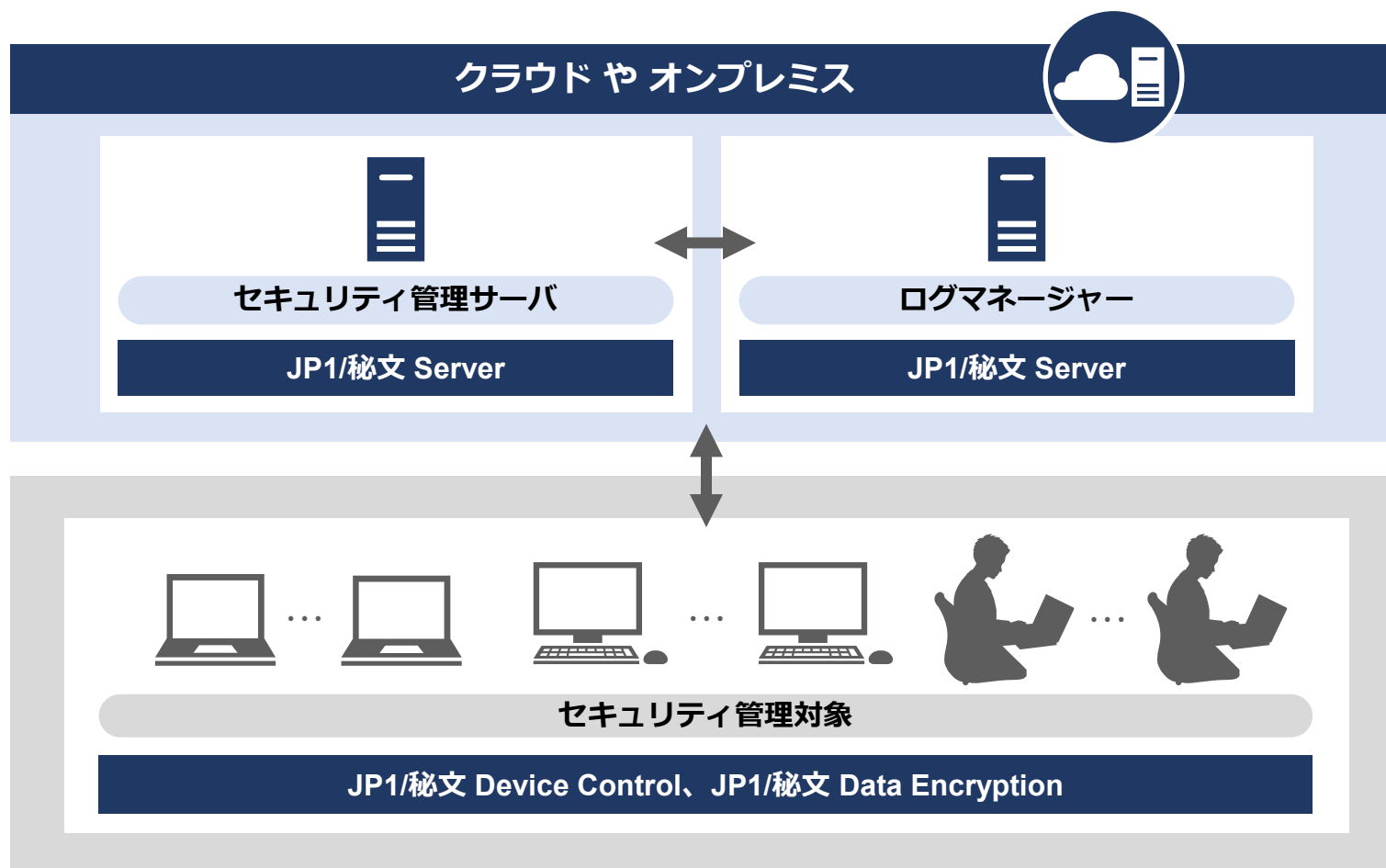
電子署名のあるプログラムや個別に許可されたプログラムなど、安全性が確認できるプログラムのみアクセスを許可し、安全性が確認できないプログラムのアクセスを禁止します。また、ランサムウェアによる機密データの暗号化を防止します。万一、PCがマルウェアに感染しても、機密ファイルを保護できます。



システム構成例

■ システム構成例

JP1/秘文を導入し、管理対象へのデバイス利用制限、ネットワーク制御により情報漏えいを防止し、操作ログを一元管理するための構成は、次のようになります。



安心してお使いいただくためのサポート

- JP1のプロフェッショナルがお客さまを支援
- ワンストップで問題を早期解決
- 長期利用も安心・下位バージョンとの互換性も保証
- 確かな品質をお客さまへ

お客さまにとって最適なシステム運用を実現できます。

JP1のプロフェッショナルが、お客さまの要件やシステムの規模・環境に適したシステムの運用方法を導き出し、実現を支援します。

お客さまにとって最適なシステム運用の実現プロセス



* JP1の機能やJP1の運用方法など、技術的なお問い合わせ

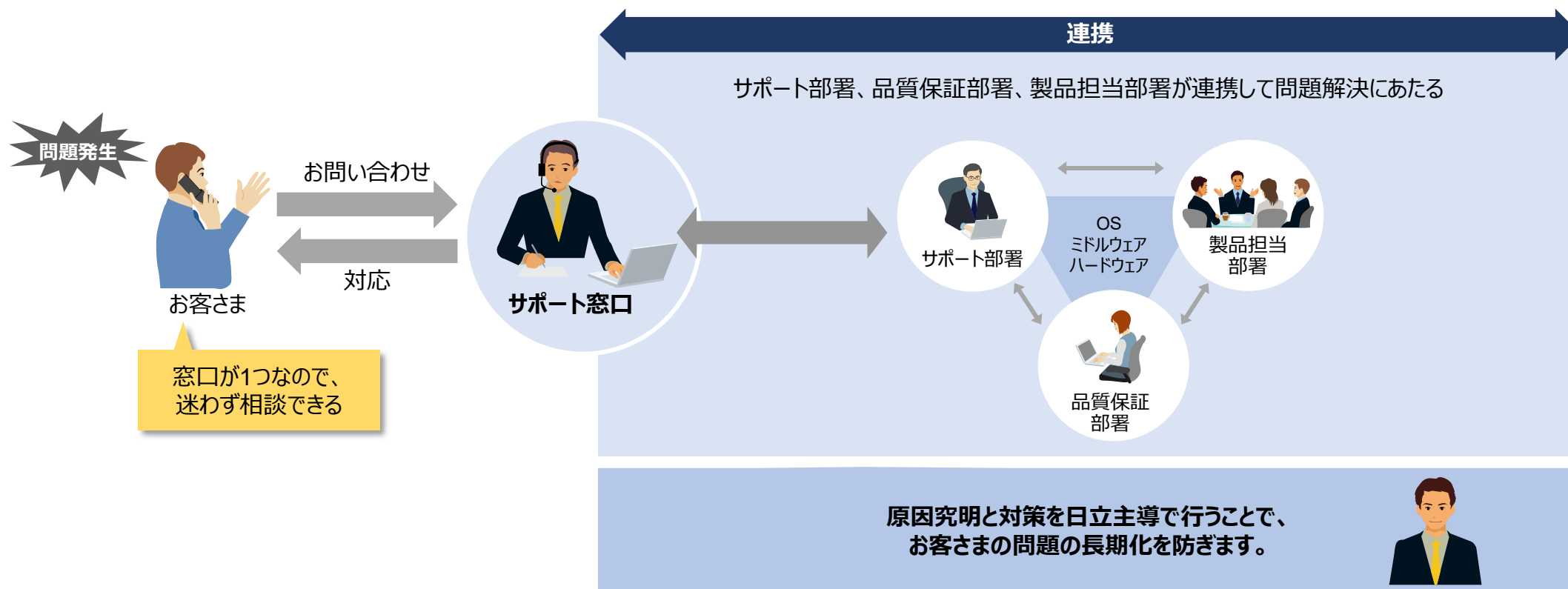
JP1のプロフェッショナルが関わることで、システム運用要件の明確化、検討・実装期間の短縮、運用部署へのスムーズな引き継ぎが可能です。

※ JP1のプロフェッショナルは、JP1技術者資格認定制度に基づいて認定された、JP1の一定以上のスキルを有する技術者です。

ワンストップサポートで問題を早期解決。問題発生時のお客さまの負担を軽減できます。

OSやミドルウェアなど複数の要素が複雑に関連する問題の早期解決を支援します。

ワンストップサポートで問題を早期解決・再発防止、お客さまシステムの安定稼働を支援



長期利用、業務システムの拡張にも安心してご利用いただけます。

お客さまシステムのライフサイクルが長期にわたる場合にも継続してサポート。
JP1はバージョン間の互換性を確保しているため、段階的なシステム拡張が可能です。

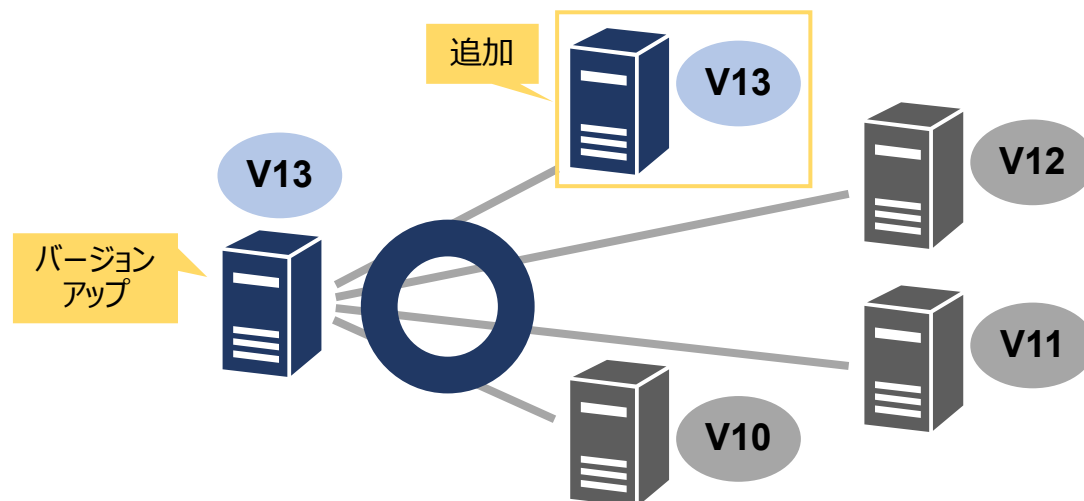
お客さまシステムのライフサイクルを見据えた長期サポート



同一バージョンで

最低**10**年間のサポートを保証

業務システムの拡張に柔軟に対応

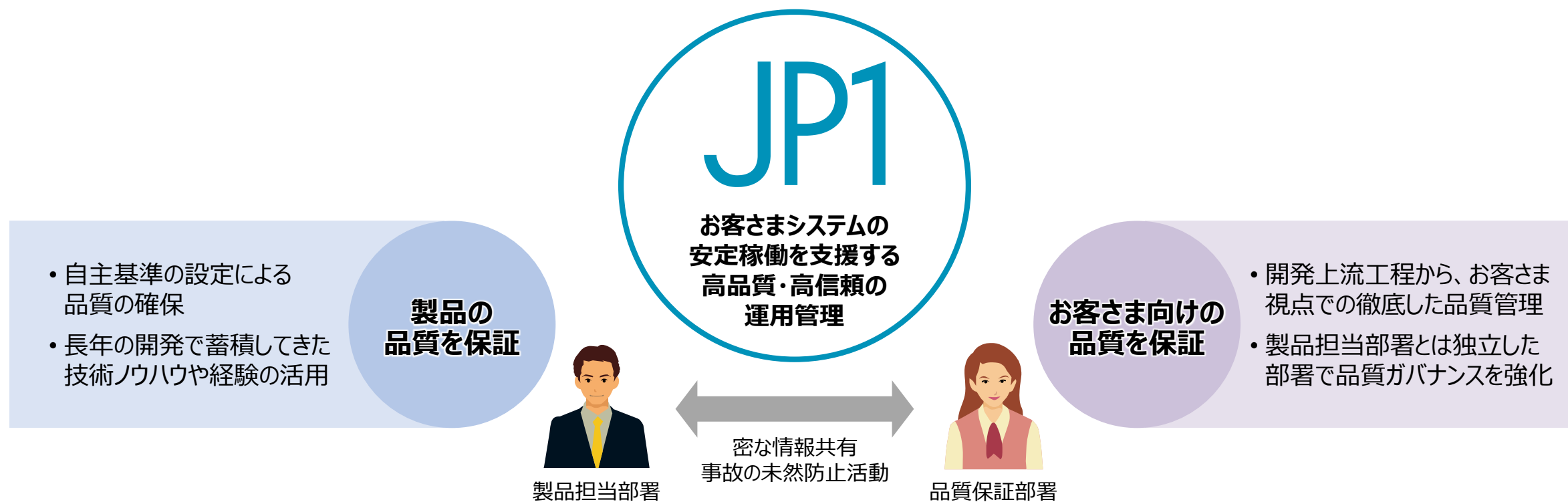


下位3メジャーバージョン間での互換性を保証。
JP1のバージョンが混在してもシステムを運用できます。

※ JP1をバージョンアップしても、インタフェースの互換性が維持されるため、
連携する製品・サービスやユーザプログラムなどを改修せずに利用できます。

ミッションクリティカルなシステムの安定稼働を実現できます。

お客さまに安心してご利用いただくために、高品質・高信頼を維持する体制を整えて取り組んでいます。



- Bluetooth® ワードマークおよびロゴは登録商標であり、Bluetooth SIG, Inc. が所有権を有します。
- Windows は、マイクロソフト グループの企業の商標です。
- その他記載の会社名、商品名は、それぞれの会社の商標または登録商標です。

- 本カタログで紹介するJP1/秘文は、日本でのみ販売している製品です。
- 記載の仕様は、改良などのため予告なく変更することがあります。
- 輸出される場合には、外国為替および外国貿易法の規制ならびに米国の輸出管理規則など外国の輸出関連法規をご確認のうえ、必要な手続きをお取りください。
なお、ご不明な場合は、当社担当営業にお問い合わせください。
- 動作環境や対応状況については、JP1 Webサイトで最新情報をご確認ください。

END

統合システム運用管理

セキュリティ管理

JP1/秘文 のご紹介

～情報漏えいを未然に防ぎ会社の大切な情報を守る～

株式会社 日立製作所