Hitachi Solutions Create

HITACHI

～柔軟な働き方を実現するリモートアクセスシステム～

DoMobile 紹介資料

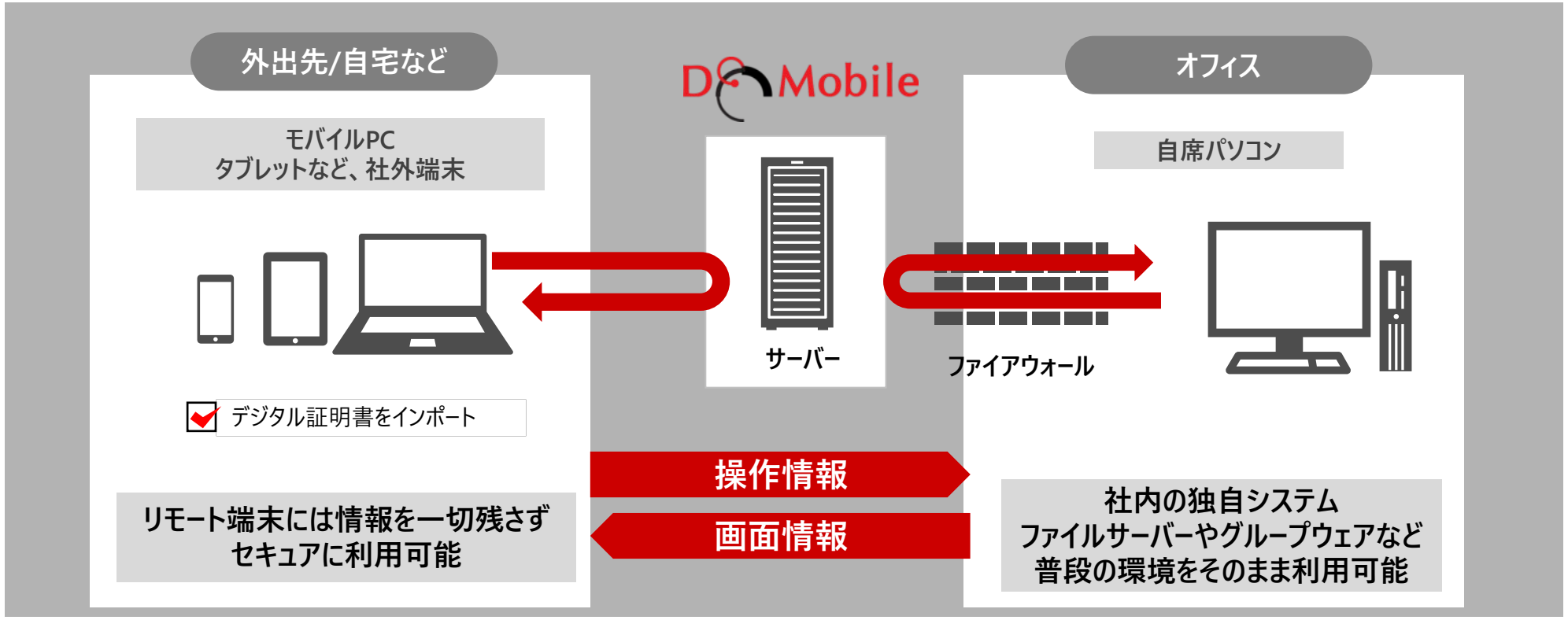
株式会社 日立ソリューションズ・クリエイト

DoMobileの概要

HITACHI

「DoMobile」は画面転送方式でリモートアクセスを行います

リモート端末の操作情報と自席パソコンの画面情報を論理的にひも付け、既存のネットワーク環境を変更せず
自席パソコンをセキュアに操作可能です。



HITACHI

「DoMobile」ならば短納期・低コストで『即効性のあるセキュアなテレワーク環境』を構築！

構築方法	セキュリティ	利用デバイス	構築期間	労務管理	コスト
DoMobile ASP （自席パソコンを遠隔操作）	◎ 耐量子暗号 データ持出し不可	○ PC／タブレット	○ 3営業日	◎ 管理者にて設定 （利用可能日時を設定可能）	○ 安価
パソコン持参 （HDD暗号化）	× ユーザーに依存	△ PCのみ	○ 数日程度	× ユーザーに依存	○ 安価
アプライアンス製品を導入 （例：VPN装置）	△ 通信プロトコルに依存	○ PC／タブレット VPN装置に依存)	△ 1カ月以上	○ 管理者にて設定 （選定機器により管理不可）	× 高価
自席パソコンを仮想化 （VDI）	△ 通信プロトコルに依存	○ PC／タブレット	△ 1カ月以上	× ユーザーに依存	× 高価

HITACHI

快適なテレワーク環境を実現するための機能を実装し、ユーザー部門・管理部門が抱える課題解決を支援します！

ユーザー部門	在宅勤務者	**セキュアに利用** ●特別なITスキルは不要
	テレワーカー	**マルチデバイス対応** ●iOS/Android/Windowsをサポート
管理部門	労務管理者	**適切な労務管理** ●アカウントごとに設定可能
	システム管理者	**簡単設定** ●ユーザー自身でインストール可能
	経営層	**安価に導入** ●ASPサービスで安価に利用可能

HITACHI

快適なテレワーク環境を実現するための機能を実装しユーザー部門・管理部門が抱える課題解決を支援します！

テレワークの利便性は理解している。

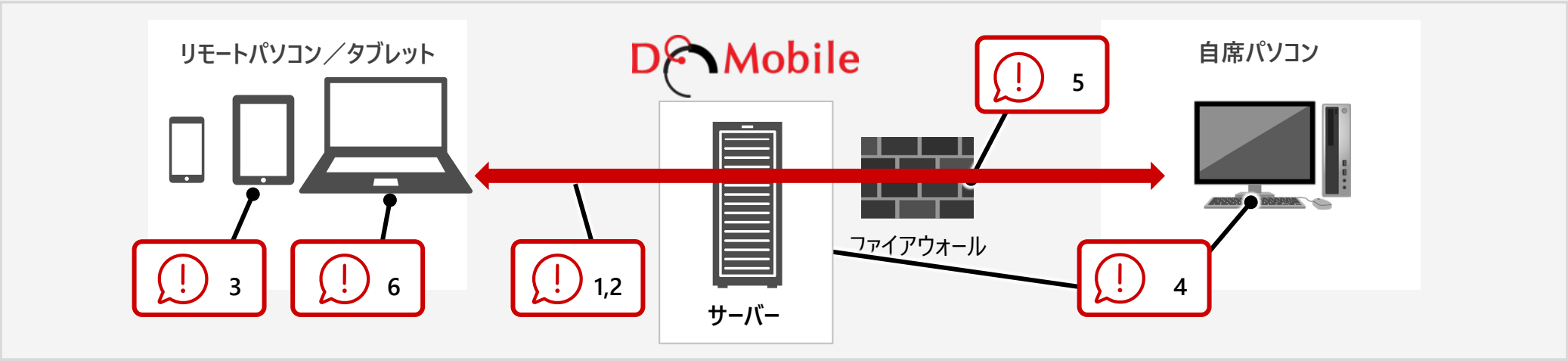
しかし、
ユーザー部門が利用する場合に運用上の課題があるのでは…？
とお考えの管理者さまへ

課題❶	課題❷	課題❸	課題❹	課題❺
				
セキュリティ	デバイス	労務管理	設定作業	コスト

2.1 テレワーク環境の課題 – ① セキュリティの課題

HITACHI

「DoMobile」はどのようにセキュアなリモートアクセス環境を実現している？

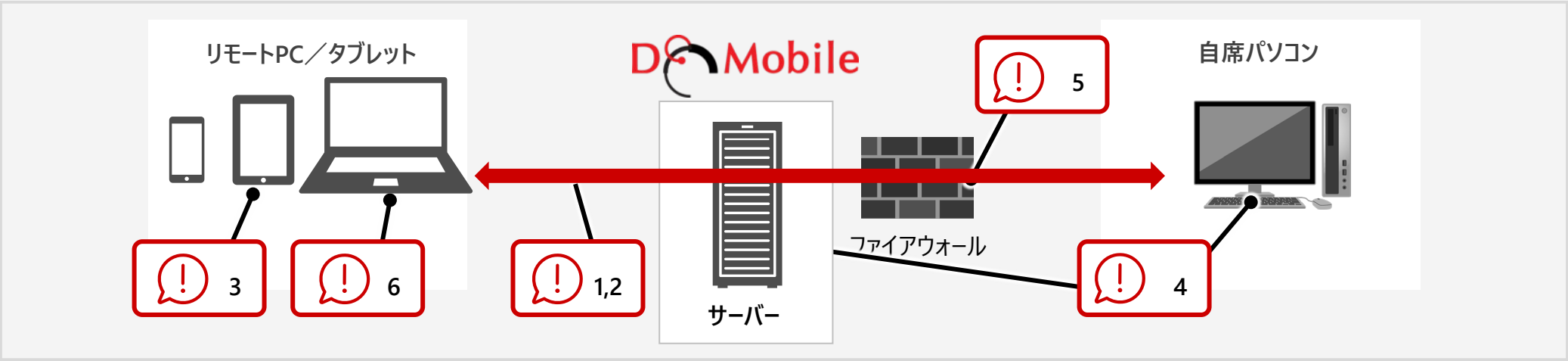


リスク例	「DoMobile」による対策
1. 将来の漏えいリスクに対する備え	暗号通信に使用する鍵交換に、耐量子計算機暗号（PQC）が利用できます。 ※　鍵交換の部分にFIPS 203の標準として採用されたCRYSTALS-Kyber（ML-KEM）を使用 RSAに代表される公開鍵暗号方式は、将来的に量子コンピュータで複号が可能になると考えられています。 その結果、公開鍵暗号方式で暗号化された共通鍵が解読され、後続の「共通鍵を用いた暗号化通信」も危険にさらされます。 このリスクを防ぐため、耐量子計算機暗号を導入し、量子コンピュータによる攻撃を抑止します。
2. 第三者による通信の盗聴	自席パソコンとリモート端末間をend to endで暗号化された通信で接続。 リモートアクセス中の盗聴対策を実現しています。

2.1 テレワーク環境の課題 – ① セキュリティの課題

HITACHI

「DoMobile」はどのようにセキュアなリモートアクセス環境を実現している？



リスク例	「DoMobile」による対策
3.なりすまし	認証には、パスワード＋デジタル証明書を利用。 管理者が定めたリモート端末のみ、自席パソコンへの接続を許可します。
4.中継サーバーへの攻撃	ASPサーバー、自席パソコンで分散して認証情報を保持。 サーバー／自席パソコンから認証情報が漏えいしても、第三者から自席パソコンへのリモート接続を防ぎます。
5.F/Wのポート開放	セキュアな既存環境を変更することなくリモートアクセスを実現します。
6.リモート端末へのデータ持ち出し	ワンタイムのリモートコントロールビューアを利用し、自席パソコンの画面情報をリモート端末へ転送することで、 実データの持ち出しを制御します。

2.1 テレワーク環境の課題 – ① セキュリティの課題

HITACHI

お客さまが懸念されるセキュリティリスクについて、「DoMobile」を利用することで解決可能です！

Q　リモート端末がウイルスに感染していた場合、自席パソコンに感染するのでは？

A　画面情報のみを転送することで、ウイルス感染リスクを排除します。

Q　画面キャプチャを取得されることでリモート端末に情報が残るのでは？

A　独自のリモートコントロールビューの機能により、画面キャプチャの取得※を抑止します。
※リモート端末がPCの場合のみ。

Q　リモート端末を紛失した場合に第三者からの利用されてしまうのでは？

A　管理者から、特定のアカウントを停止可能です。ユーザーごとに利用日時を制限し時間外労働を抑止します。

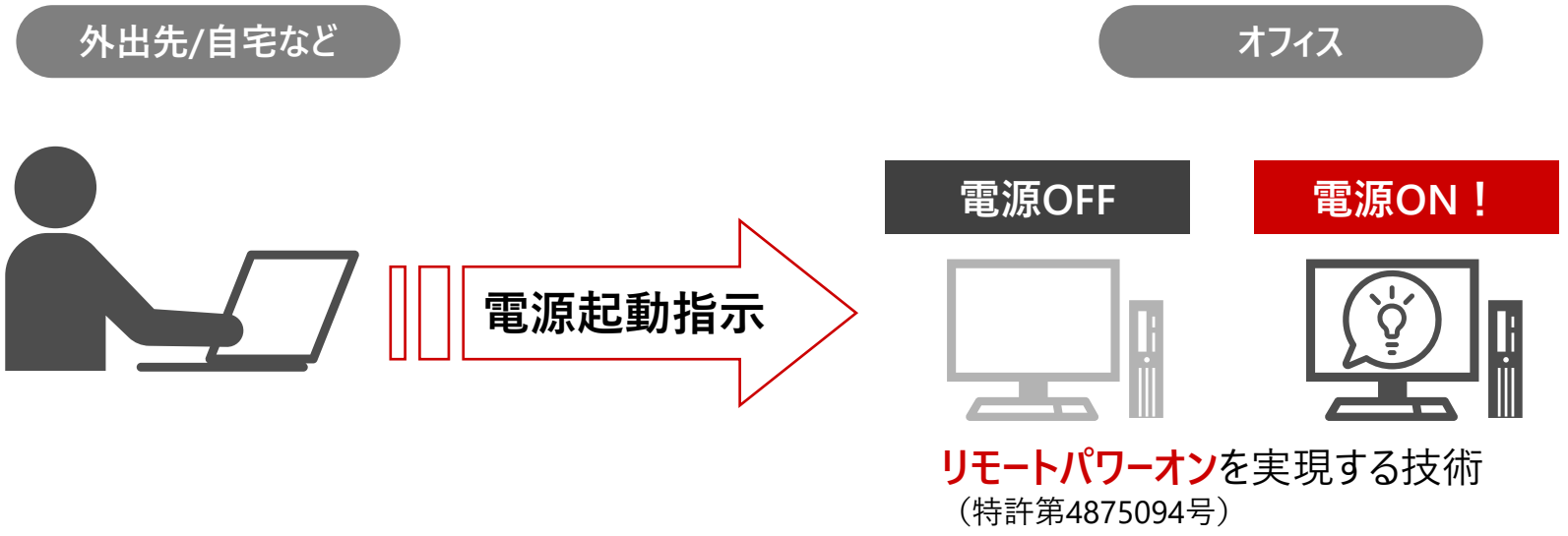
高度なセキュリティレベルが求められる公共機関・医療機関・金融業への導入実績もあります。

2.1 テレワーク環境の課題 – ② デバイスの課題

HITACHI

Q リモートアクセスを行うためには自席パソコンを24時間立ち上げおかないといけないのでは？

A Wake On LAN（WOL）機能を利用し、社外から遠隔で自席パソコンの電源起動が可能なため、常時自席パソコンを起動しておく必要はありません。
使用電力の節約や柔軟な働き方の実現に貢献します。



リモートパワーオンを実現する技術
（特許第4875094号）

※WOLをご利用いただく際には、当社Webサイトに掲載されている最新の前提条件を満たしている必要があります。

2.1 テレワーク環境の課題 – ② デバイスの課題

HITACHI

Q タブレットを利用したいが、Windows環境の業務には適用できないのでは？

A タブレット利用時には、Windows配列のオリジナルキーボードを表示。
iPadでは通常サポートしていない「ファンクションキー」も利用可能。

社内の専用業務システムを利用するための半角入力やファンクションキーが必要な操作も、快適にご利用いただけます。

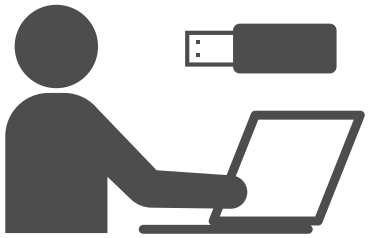
2.1 テレワーク環境の課題 – ② デバイスの課題

HITACHI

Q リモート端末の紛失対策をより強固に実現したい。何かいい方法はないか？

A シンクライアントPC※をリモート端末として利用可能です。
専用USBトークンと連携することで、物理キーとの二要素認証を実現
複雑なパスワードの暗記が不要、といったメリットがあります。

オフィス



① シンクライアントPCへ
USBトークンを挿入

② PINコードを一度入力し、
OKを押下

③ 自動的に認証を行い
リモートアクセス開始！

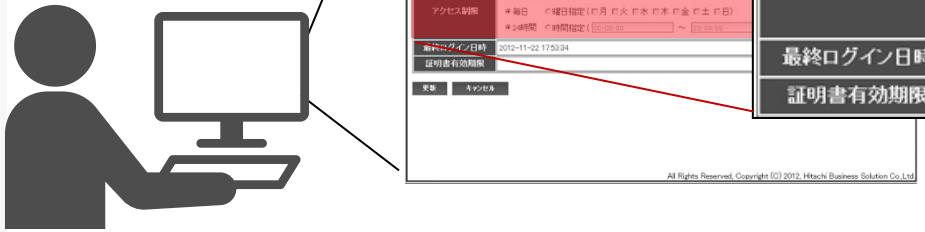
2.1 テレワーク環境の課題 – ③労務管理の課題

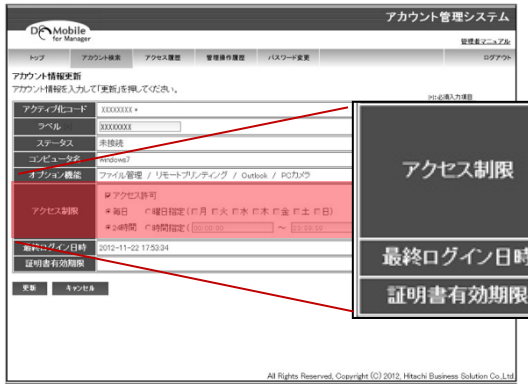
HITACHI

Q テレワークを行うと、適切な労務管理を現することが難しいのでは？

A 適切な労務管理を実現するために、ユーザーごとに利用日時の制限や特定のアカウントのアクセス制限が可能です。
利用統計を一括取得し、テレワークの効果測定にも活用いただけます。

管理者





アクセス管理画面

・利用可能な曜日、時間帯設定　・アクセス可否設定

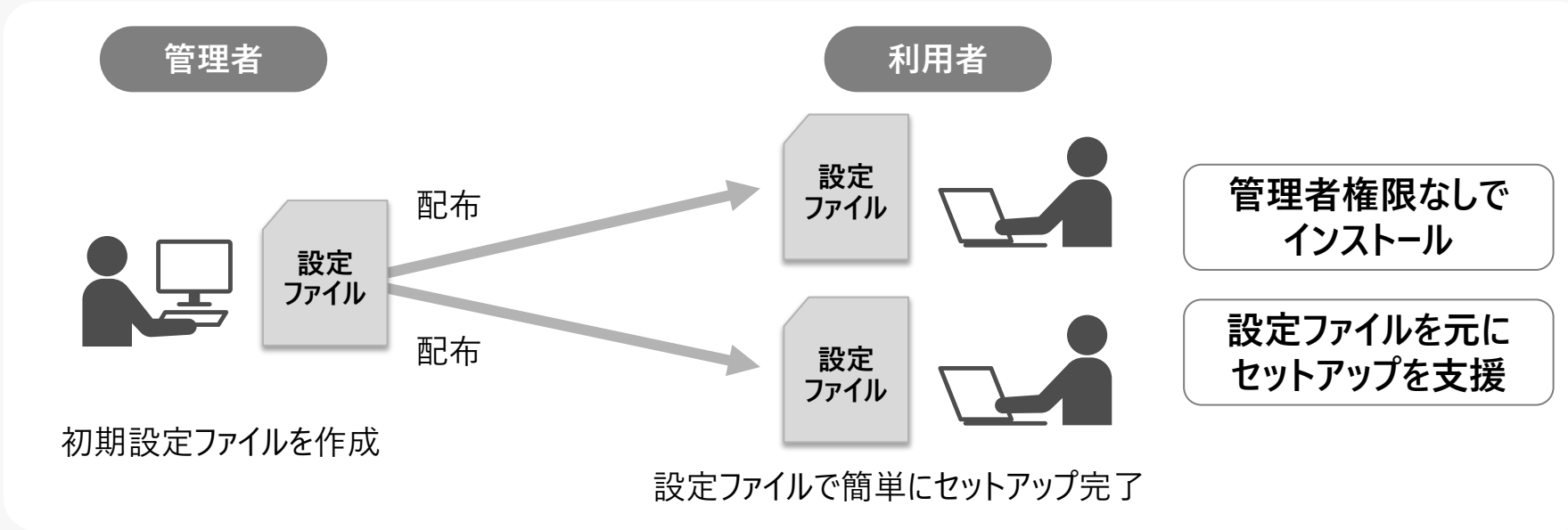
アクセス履歴確認　・1年間の利用履歴　・指定ユーザー検索　・利用履歴の出力 → CSV出力

2.1 テレワーク環境の課題 – ④設定作業の課題

HITACHI

Q 初期設定について、ユーザー部門で対応してほしいがWindowsの管理者権限は開示したくない。何かいい方法はないか？

A インストール支援ツール※により、Windowsパソコンの管理者権限を開示することなく初期セットアップやアップデートを実現します。



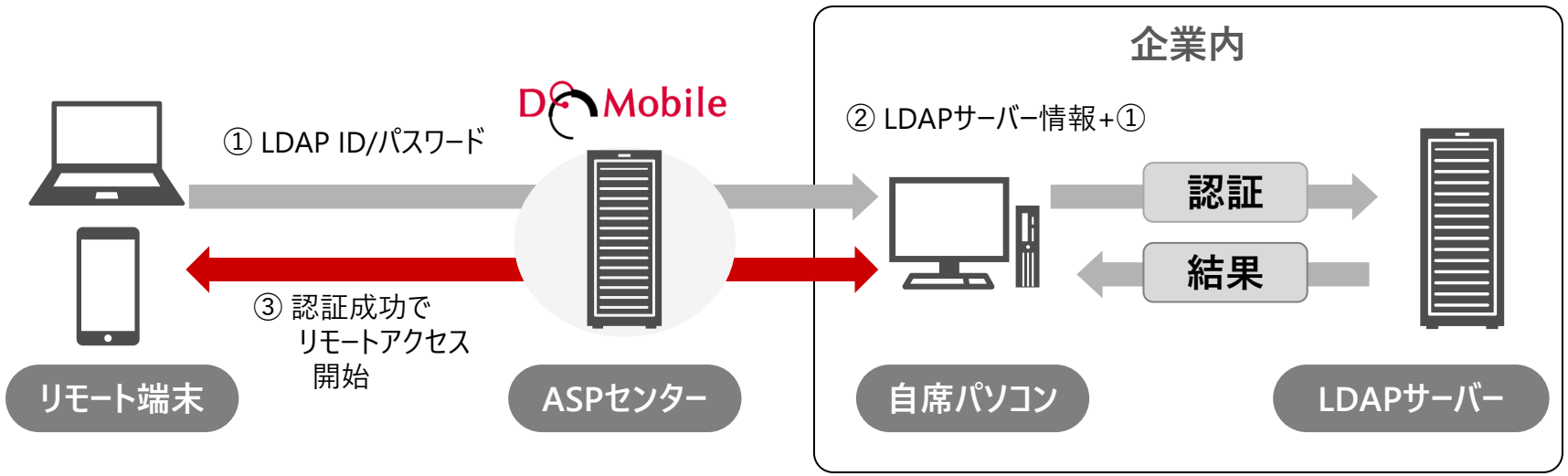
※導入企業の管理者が企業のネットワーク情報などを事前に設定することで、セットアップ時の利用者の操作を大幅に削減し、ユーザー/管理者の負荷を軽減します。

2.1 テレワーク環境の課題 – ④設定作業の課題

HITACHI

Q リモートアクセスの認証情報について、パスワードの更新時期など現在の運用ポリシーと合わせたいが対応可能か？

A リモートアクセス認証時のLDAP認証をサポートし企業内の認証情報およびセキュリティポリシーに柔軟に対応可能です。



※一般的にはRADIUS⇔LDAPと連携し認証を行いますが、「DoMobile」は自席パソコンを介して連携します
※「DoMobile」サーバーと企業のLDAPサーバー間の通信路の確保は不要です

2.1 テレワーク環境の課題 – ⑤コスト面の課題

HITACHI

Q テレワーク導入には、新たなハードウェアの導入や大規模なシステム構築作業、安定した運用を行うためにサポートを行う人員が必要なのでは？

A 「DoMobile ASPサービス」ならば、最小限のIT投資で運用を含めたテレワーク環境を構築可能です。

初期費用（利用デバイス導入）

「DoMobile」であれば、
既存のIT資産を自席パソコン／リモート端末としてそのまま流用可能！

運用コスト（サーバー管理）

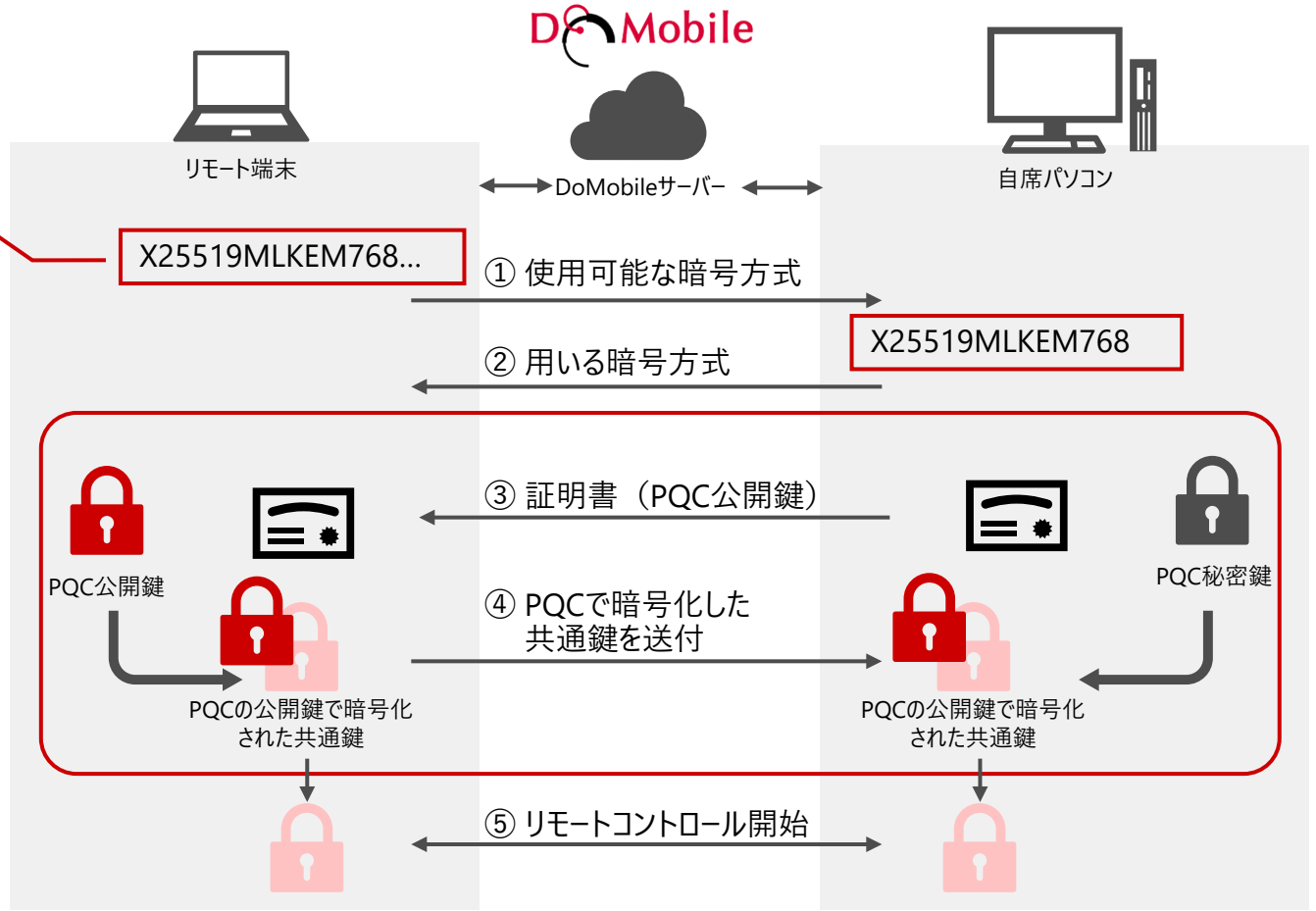
ASPサービスを利用すれば、
サーバー管理の運用コストは利用料に含まれるため、考慮不要！

3. DoMobile Ver.5 特長

公開鍵暗号方式にPQCを追加することで、量子コンピューターによるHNDL攻撃※など、
新たなセキュリティ脅威にも対応し、安心して利用できます。

サーバー/リモート端末/自席パソコンがリモートコントロール時に使用する暗号通信にPQCを追加。
鍵交換をより安全に行えるよう改良。

※　PQCのON/OFFは自席パソコンで切替可能
※　Microsoft EdgeやGoogle Chromeなど、PQCをサポートするリモート端末の場合はサーバーとの通信にも適用
※　自席パソコンとサーバー間の通信についても適用



※HNDL攻撃：今は暗号化されたデータを収集し、将来量子コンピューターが発展した時点で一気に解読する攻撃手法

4. 動作環境

■自席パソコン、起動用サーバー／パソコン

OS	Microsoft Windows 11 Pro / 11 Enterprise Microsoft Windows Server 2016 Standard Microsoft Windows Server 2019 Standard Microsoft Windows Server 2022 Standard Microsoft Windows Server 2025 Standard
CPU	上記OSの推奨環境相当以上
HDD	OSがインストールされているドライブに100MB以上の空き容量 自席パソコン（DoMobile PC）用DoMobileプログラムをインストールするドライブに30MB以上の空き容量が必要。
接続回線	DoMobileサーバーに接続可能なネットワーク環境
その他	リモートパワーオン機能の前提条件： 自席パソコンがWake On LANに対応していることが必要。 自席パソコンが休止またはスタンバイモードのリモートパワーオンはサポートしておりません。 リモートパワーオンされる自席パソコンの他に、同一セグメント内に少なくとも 1 台の起動している自席パソコンが必要。 （少なくとも2アカウントの契約が必要）

※動作環境の最新情報については、当社ホームページをご覧ください。
https://www.hitachi-solutions-create.co.jp/solution/domobile_asp/require/index.html

4. 動作環境

■リモート端末

パソコン ※お使いのOSにより サポートブラウザーが 異なります	サポートOS：自席パソコン（DoMobile PC）の動作環境に準じます。 【ブラウザー】 Microsoft Edge Google Chrome Mozilla Firefox
タブレット	サポートOS：iPadOS 17.0以降 / 26.0以降
	サポートOS：Android™ 7.0
スマートフォン	サポートOS：iOS 17.0以降 / 26.0以降
	サポートOS：Android™ 13

※動作環境の最新情報については、当社Webサイトをご覧ください。
https://www.hitachi-solutions-create.co.jp/solution/domobile_asp/require/index.html

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**
  https://www.hitachi-solutions-create.co.jp/contact/solution.html
- **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

- Apple、iPad、iPad mini、iPad Air、iPhoneは、米国および他の国々で登録されたApple Inc.の商標です。
- Androidは、Google Inc.の商標または登録商標です。
- Intel、Pentiumは、アメリカ合衆国およびその他の国におけるIntel Corporation の商標です。
- Microsoft、Internet Explore、Windows、Windows Server、Microsoft Teamsは、米国Microsoft Corporationの、米国およびその他の国における登録商標または商標です。
- Zoomは、Zoom Video Communications, Inc.の米国およびその他の国における登録商標または商標です。
- Google ChromeはGoogle LLC の商標です。
- Microsoft Edgeは、米国、その他の国における米国Microsoft Corp.の登録商標です。
- Firefoxは、Mozilla Foundationの米国およびその他の国における登録商標です。

■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・価格は、2026年1月時点のものです。
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