



今お使いのPCを セキュアなデータレ ス

VDIレベルの
クライアントに
セキュアな業務環境を、
低コストで実現



※本資料の記載の内容・仕様は、予告なく変更となる可能性があります。あらかじめご了承ください。
※本資料に記載の製品名・サービス名は、各社の商標または登録商標です。

ソリトンシステムズは、設立以来IT・エレクトロニクス業界にあって、常に新しい技術トレンドを見据え、いくつもの「日本で初めて」を実現してきました。近年は、認証を中心としたITセキュリティからサイバー対策製品まで、また、携帯電話回線4G、5GやWi-Fiを利用したハイビジョン・レベルの映像伝送システム、リモートドライブなどに取り組んでいます。国産メーカーとして、オリジナルの「もの創り」、「独創」にこだわった製品とサービスを提供しています。

本 社 所 在 地 東京都新宿区新宿 2-4-3

設 立 1979年3月1日

売 上 186億円 (2024年12月期連結)、プライム市場

資 本 金 13 億2,650万円

代表取締役社長 鎌田 理

従 業 員 数 678人(ソリトングループ連結)

国 内 事 業 所 札幌営業所、東北営業所、名古屋営業所、大阪営業所、
福岡営業所、山形総合開発センター、長野開発分室
開発分室（東京）、ロジスティックセンター（東京）

海 外 拠 点 Soliton US、Soliton China、Soliton Europe



DX・クラウドシフトが
進み、社内外の境界が
薄れる

いつでも、どこでも、安全に業務を行える環境の需要が増加

業務データや端末が、組織ネットワークの外に出ていくようになった現在。
働く場所を問わず、オンプレミスやクラウドのデータへアクセスし仕事ができる『利便性』と、
そのような環境においても情報漏えいを起こさない『安全性』の両立が、
高いレベルで求められるようになっていきます。



クラウドシフト



組織を超えたデータ共有

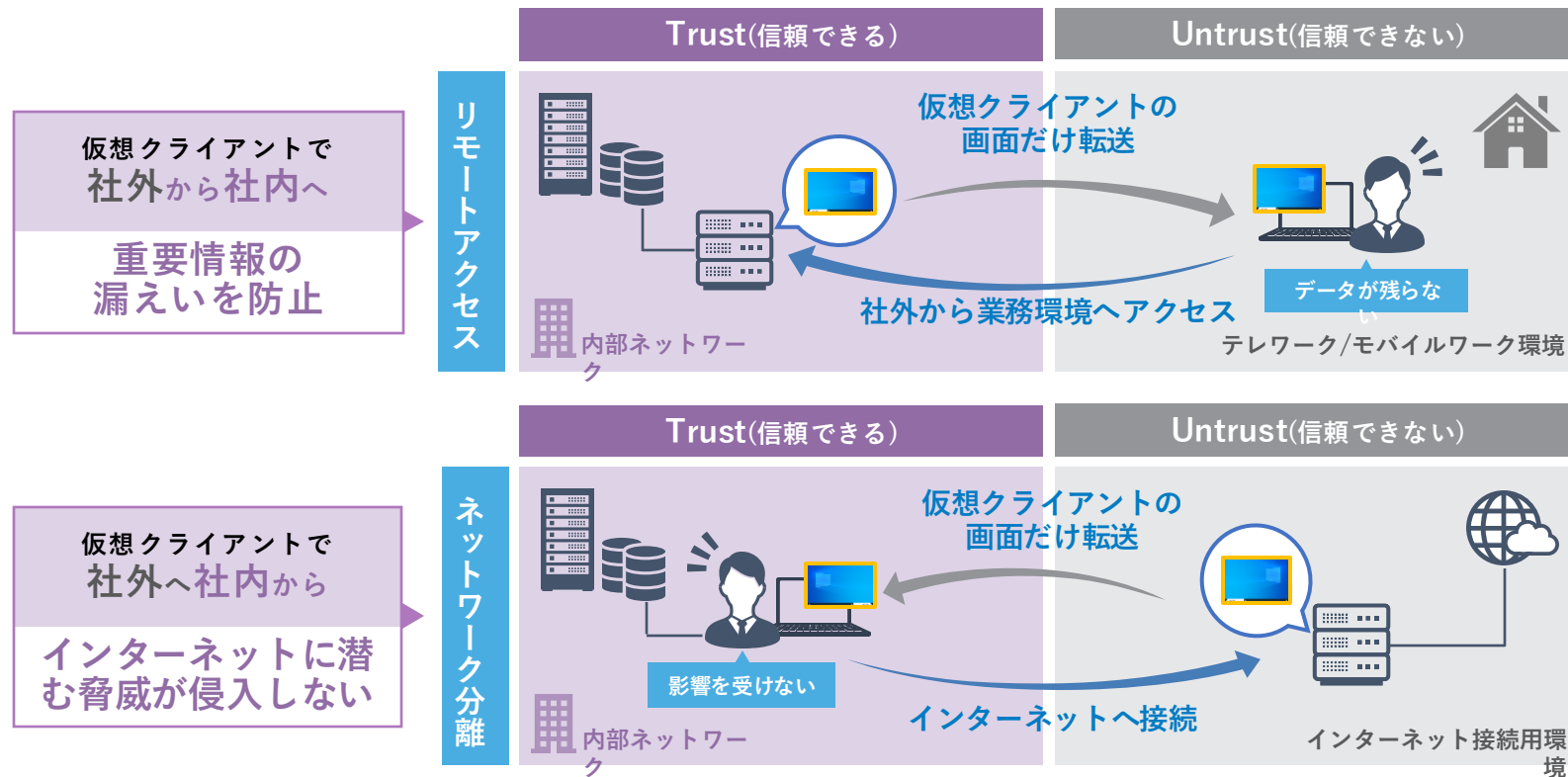


ハイブリッドワーク

VDI※1やSBC※2
など・・・

● 業務端末を“データレス化”する仕組みがより有効に

「クラウド活用」や「テレワーク」、また組織内の重要情報をインターネット脅威から隔離する「インターネット分離」など。
あらゆるシーンで利便性と安全性を両立する手法として、端末にデータを残さずに業務する仕組み(=データレスクライアントソリューション)の有用性が高まっています。



※1 Virtual Desktop Infrastructure：仮想デスクトップ基盤
※2 Server Based Computing：サーバーベースコンピューティング

従来ソリューションの 活用と課題

● 利便性と安全性に加え、コストバランスも考慮

最も知られたデータレスの仕組みといえば、VDIをはじめとする『クライアント仮想化ソリューション』。

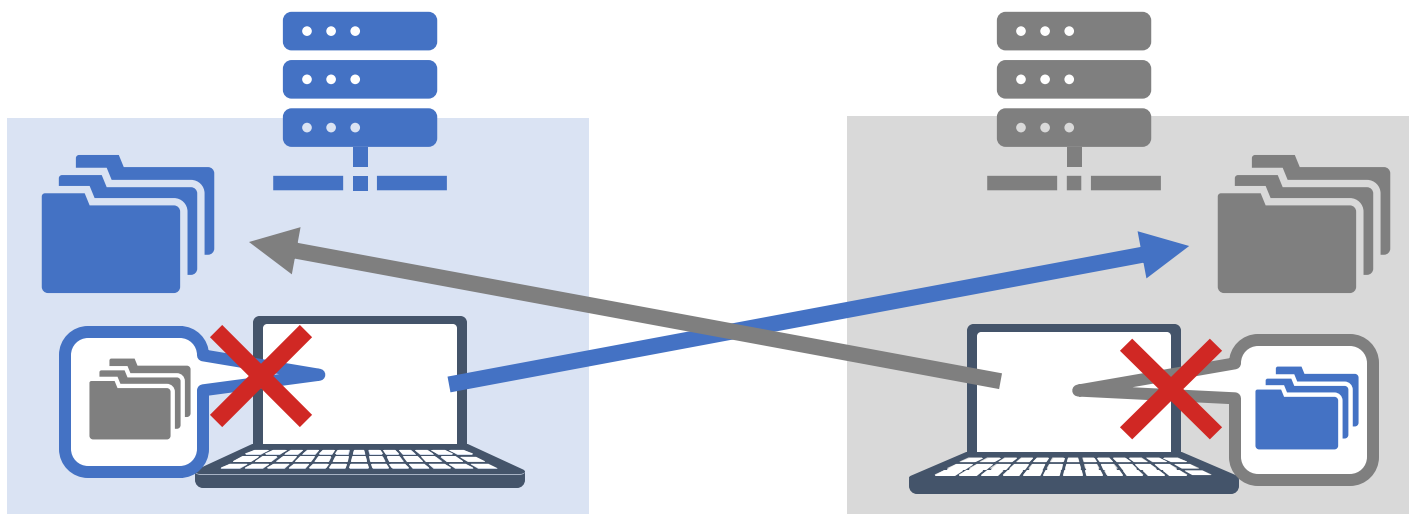
これを用いれば、端末に一切データを残さず、業務を完結させることが可能です。一方で、サーバーやライセンスの導入、保守・運用における高額なコストが課題になるケースも見られます。VDIを活用していきたいものの、諦めかけているお客様も少なくありません。



『VDI導入』は
目的でなく手段

● コストを抑えて『やりたかったこと』を実現する

VDIが検討される大きな理由は、どこでも業務できる『利便性』とデータを残さない『安全性』が、現在のビジネスシーンにマッチしているためです。これは『異なるネットワークに安全にアクセスし、端末にデータを残さず、データの閲覧や編集ができる』ということであり、同じことが実現できるのであれば、必ずしもVDIにこだわる必要はありません。より低コストで、運用しやすいソリューションを選択肢に入れることができます。



実現したいことは

「異なるネットワーク上」にある情報やファイルを「端末にデータを残さず」「閲覧したり編集したり」

することであり、『VDI導入』ではない

さまざまな データレスクライアン ト ソリューション

● 自組織の環境に沿った選択を

今では、古くからあるVDIやSBC、リモートデスクトップといった方式に加え、多様なデータレスクライアントソリューションが存在します。中でもコストを抑える選択肢として、大掛かりなシステム投資が不要で、業務端末1台で完結することができる『端末内仮想化方式』が注目されています。『やりたいこと』とコストのバランスを考慮し、最適な選択を行うとよいでしょう。

	ソリューション	説明	導入コスト
 画面転送	仮想デスクトップ (VDI) 方式	仮想化基盤に集約された端末をリモートから操作	高
	アプリケーション仮想化 (SBC) / RBI方式 (Remote Browser Isolation)	サーバー側で実行されるアプリやブラウザをリモートから操作	高
	リモートデスクトップ方式	別ネットワークの端末をリモートから操作	中
 端末内仮想化	セキュアコンテナ方式 	ローカル端末に隔離環境を作り アプリケーションを稼働	中
	セキュアブラウザ方式 Soliton SecureBrowser	ローカル端末に隔離環境を作り ブラウザを稼働	低



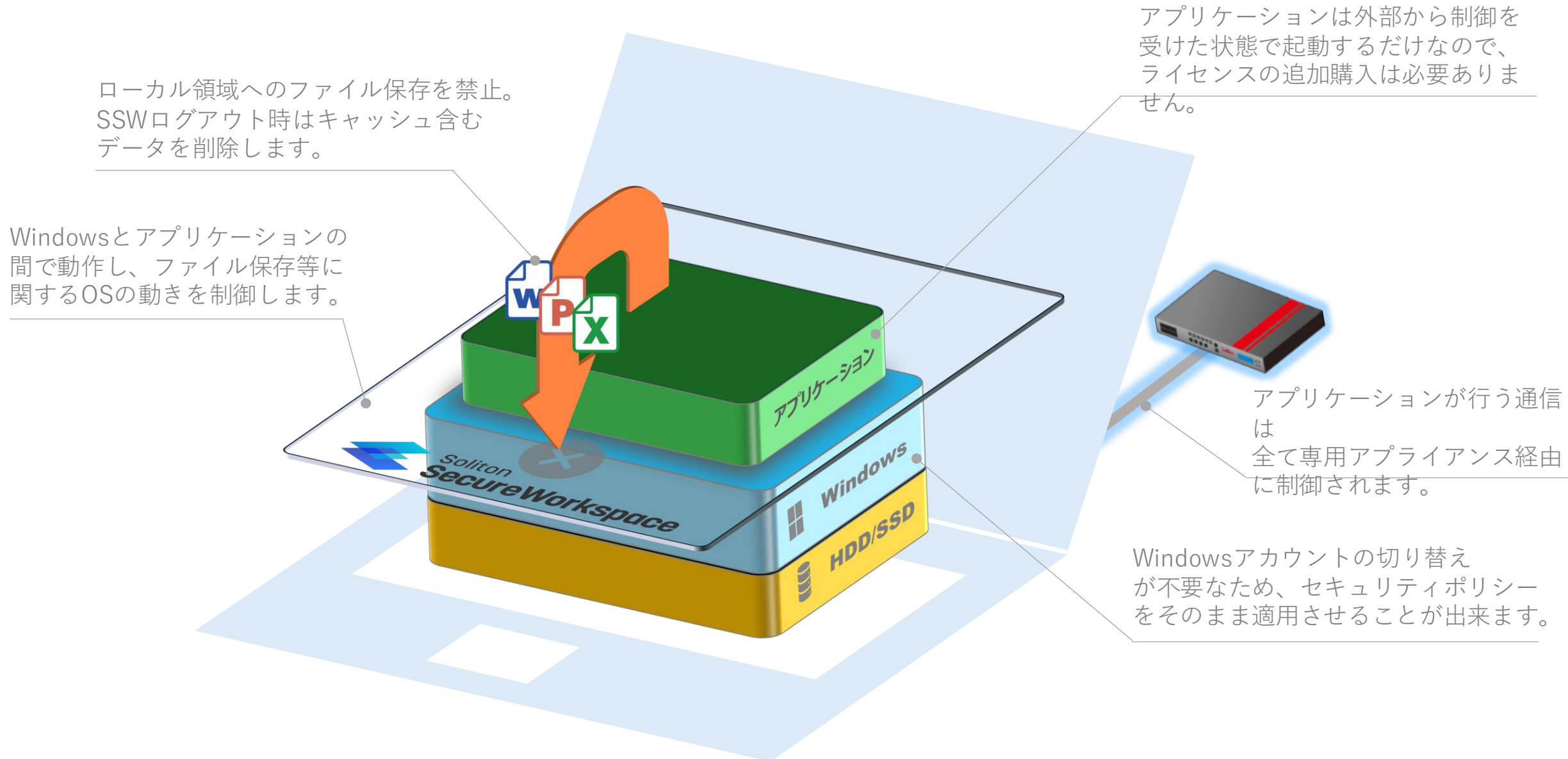
Soliton
SecureWorkspace

製品のご紹介

業務アプリのファイル保存やWebアクセスを制御し、安全な業務環境を実現します

- ◆ ブラウザ、Officeアプリ、Web会議などが**普段通りの操作感**で利用可能です。
- ◆ 制御下にあるアプリケーションは**ローカル領域へのファイル保存ができません**。
- ◆ イン트라サイトへは**制御下のアプリからのみ**、といったアクセス制限が専用ゲートウェイによって可能。
- ◆ 通信を行うのは起動時や、ファイルを開く/保存の時のみ。低帯域回線、瞬断にも対応。





簡便な操作性

専用ソフトウェアの起動とアプライアンスへの認証のみで、アプリケーションの隔離環境を容易に構築できます

柔軟な環境切替

セキュリティ要件の高い特定のネットワーク領域にアクセスする際にのみ、隔離された安全な環境に切り替えることが可能です

データ保護

ローカル環境にデータを保存しないため、端末の紛失や故障時のデータ損失、情報漏えいリスクを大幅に低減します

通常のWebアクセス



ローカル領域



アプリケーションによるローカル領域へのファイル保存禁止



アプリケーション

隔離環境からローカル領域へのデータ持ち出し禁止



ローカル領域から隔離環境へのデータ持ち込みは可能



隔離環境からは専用アプライアンス経由のみ通信を許可



端末のIPアドレスは接続拒否
(アプライアンスのみ許可)

Soliton SecureWorkspaceのみ
アクセスを許可するネットワーク (例)

ファイルサーバー

社内ポータル

業務用クラウド

特定業務システム

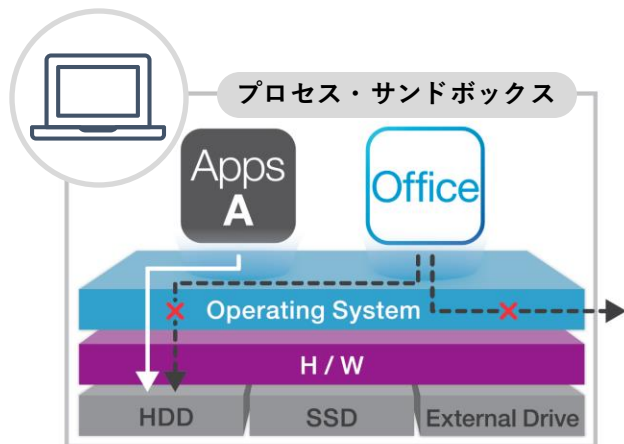
ネットワーク分離
における指定領域

関係会社の
社内システム

フランチャイズ
本部のシステム

顧客の社内システム

カーネルレベルのプロセス監視



隔離環境内で動作しているアプリケーションの
 出入り口を『カーネルレベル』で監視し、情
 報漏えいにつながるプロセスの動作を制御しま
 す。

ファイル保存 / クリップボードコピー / レジストリ編
 集 /
 プリント / ネットワーク接続 / COMアプリ呼び出し

データの自動消去



作成・編集したファイルは隔離領域に。
 ログオフすると、読み書きしたデータは自動で
 消去します。

特許技術の高度なセキュリティ



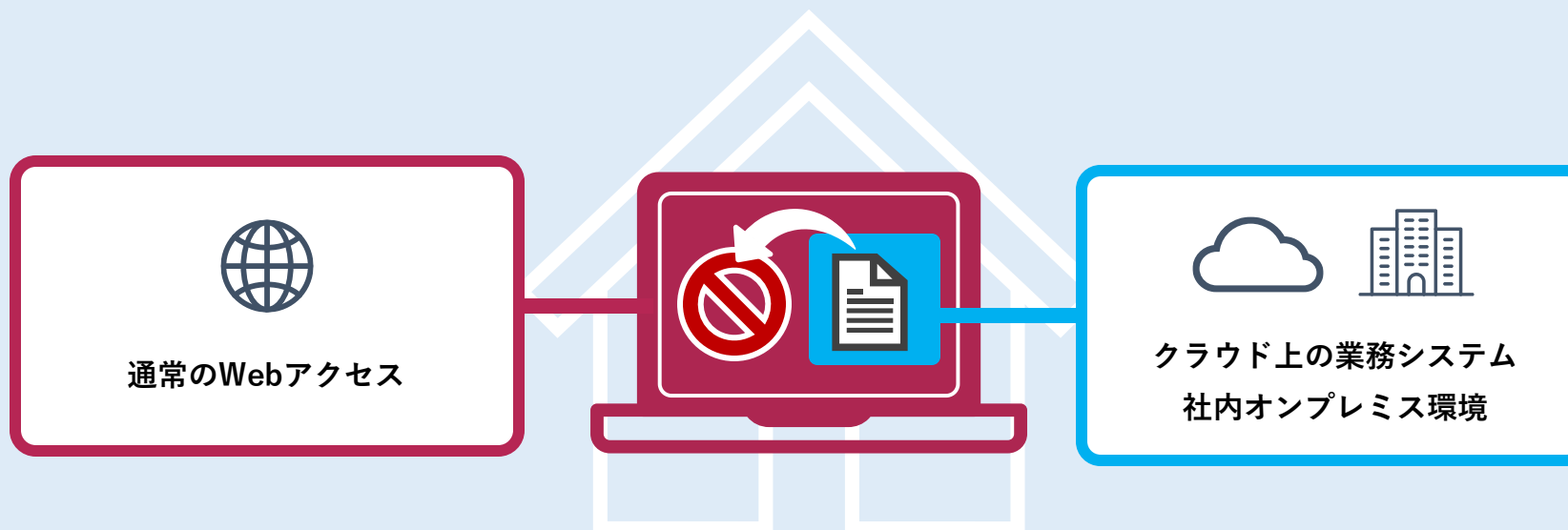
対応が困難とされるCOM*経由で行われる他ア
 プリケーション機能の呼び出しも制御。
 情報漏えいを防止します。

特許第6104447号

1.低コストでテレワーク環境を構築

- セキュアコンテナ方式によるテレワーク環境の構築
- VDI/SBCと比較して圧倒的なコスト削減が可能
 - ※VDIと比較して約1/10程度
- 常時通信を必要とせず、ネットワーク帯域を削減可能

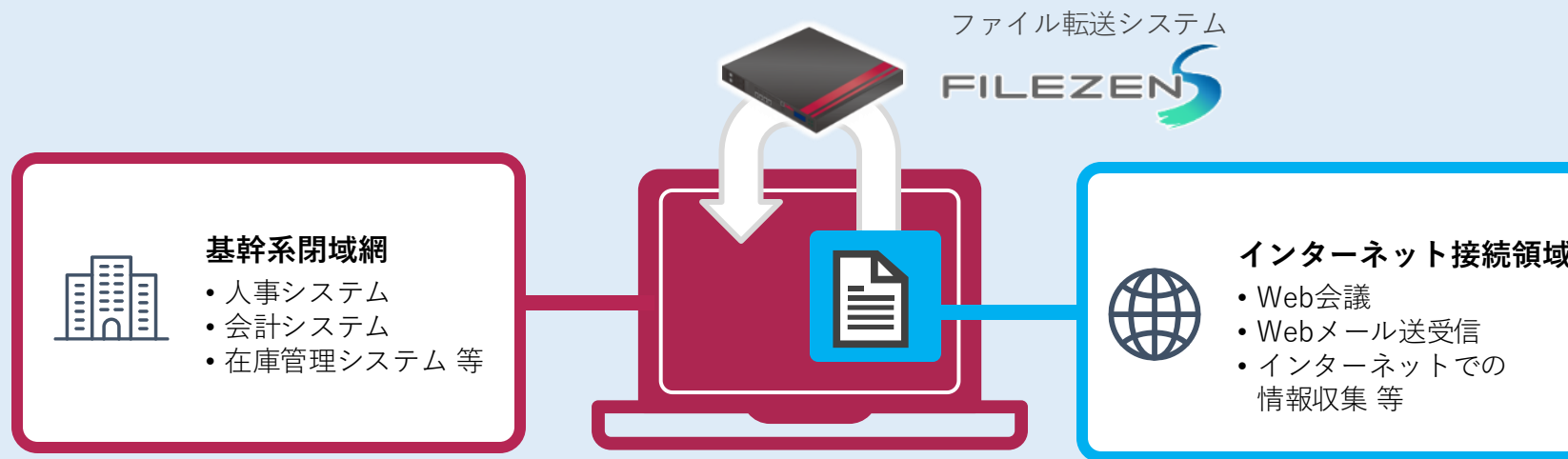
- VPN不要のため、管理コストを圧縮
 - ※端末とゲートウェイ間の通信は独自プロトコルで暗号化
- 隔離領域からのファイル移動制限で情報漏えい防止



2.分離ネットワーク環境への対応

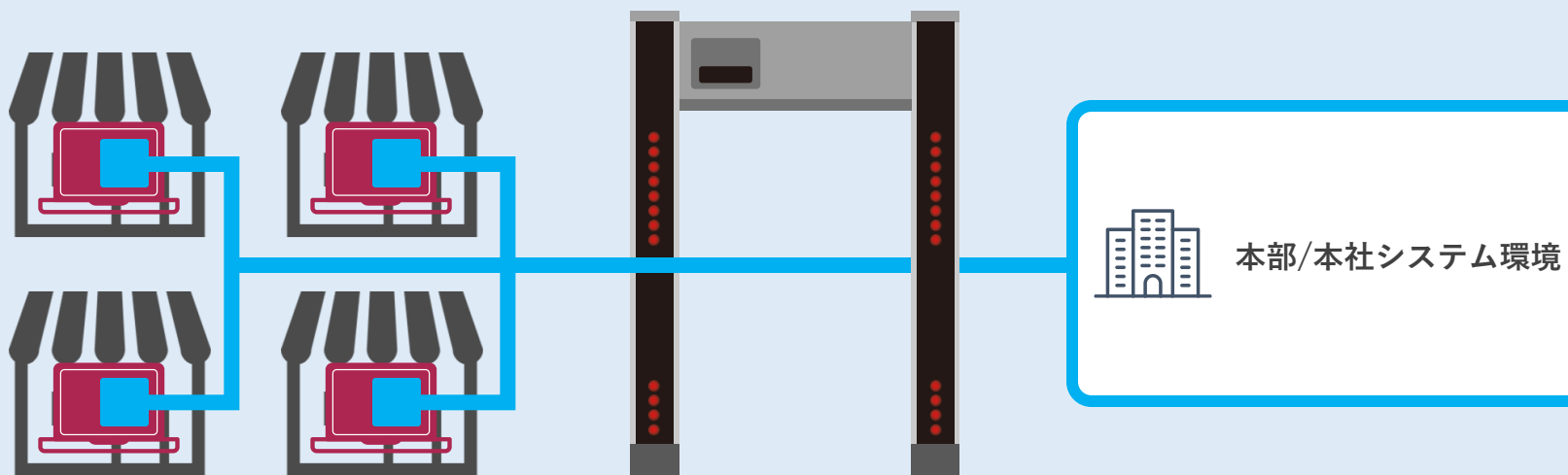
- 自治体等におけるネットワーク分離（論理的分離）環境での業務対応を1台のPCで実現可能
- 無害化製品※と連携したファイル転送システムにより、ネットワーク間でファイルを安全に受け渡し
- VDIと比較した場合、約1/10の運用費（当社調べ）

※OPSWATと連携



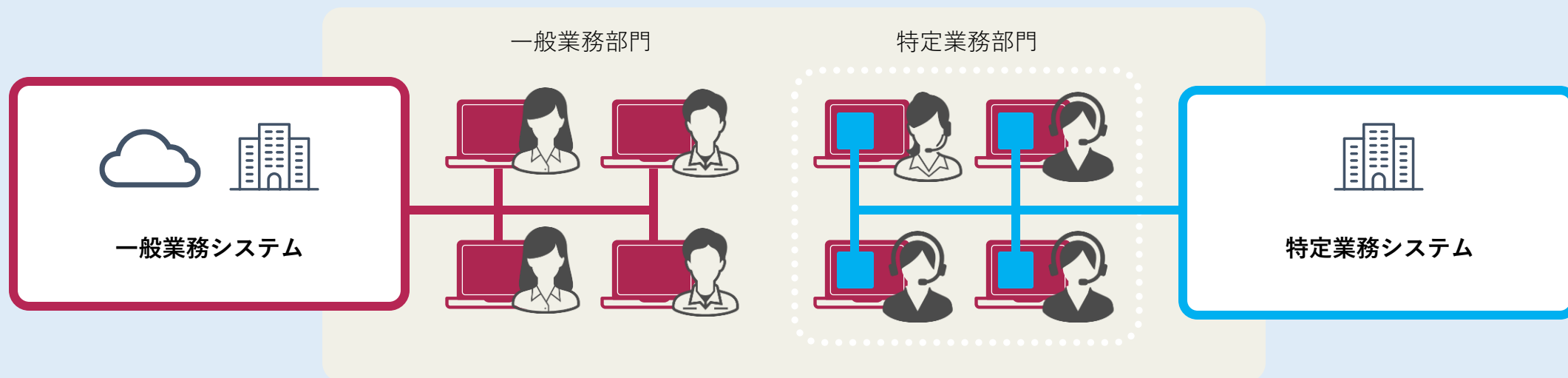
3.多店舗型環境でのコスト削減とセキュリティ

- 個人情報等の重要情報を各拠点で取り扱う多店舗型企業は情報の管理・統制が重要課題
- 専用線、VPN接続はコストや運用負荷の面で課題多
- 各拠点1台のPCと専用ゲートウェイサーバーのみで重要情報を扱う業務が可能に



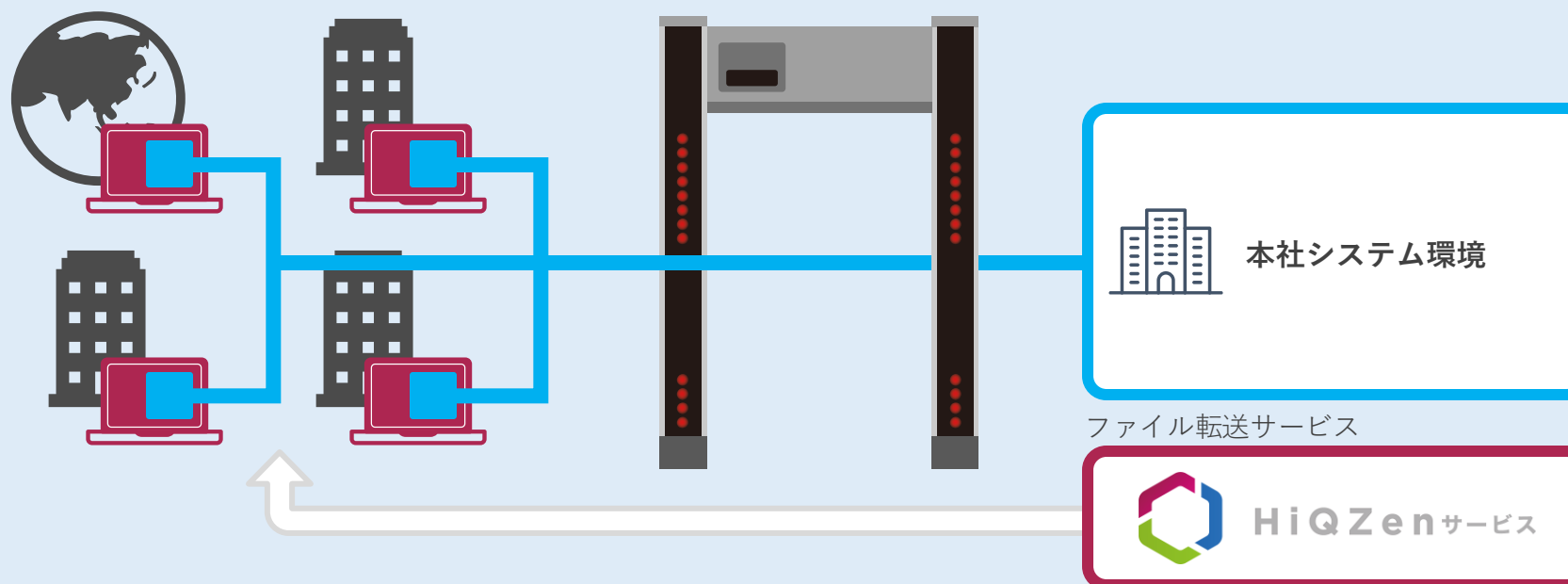
4. 特定業務端末のみ一部導入

- 個人情報に頻繁に触れるコールセンター等、特定業務専用端末のセキュリティを特に強化
- 特定業務用アプリケーションがWebアプリの場合、Soliton SecureBrowserでの対応も可能



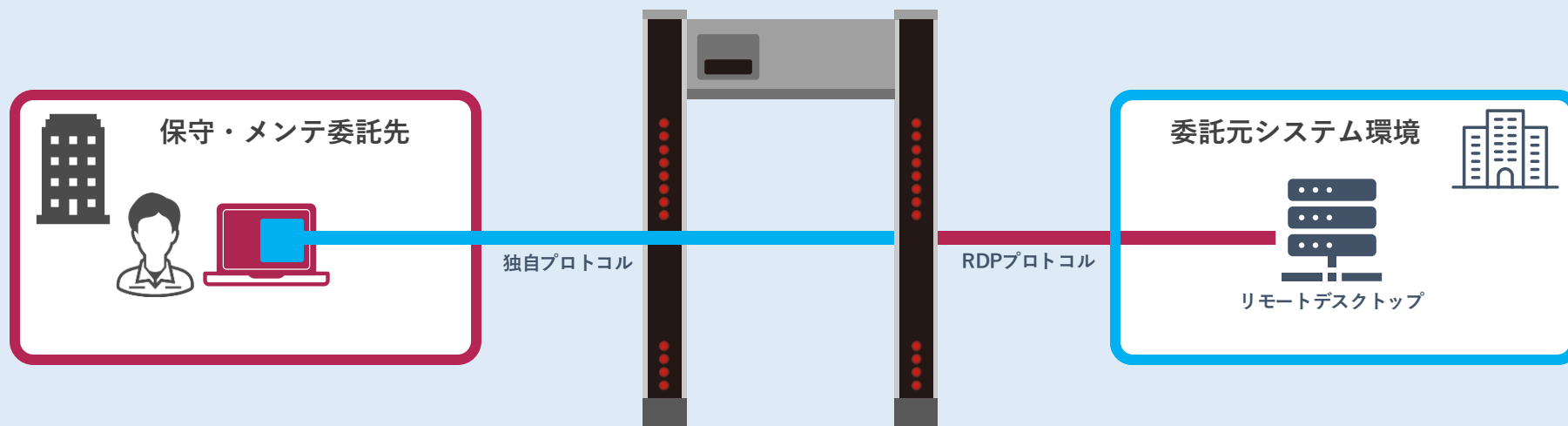
5. サプライチェーンリスク管理

- セキュリティレベルの異なる関連企業や取引先、海外拠点から本社システムへのアクセス時に利用
- 端末にデータを残さない形でシステムを利用させることで重要データの管理を徹底
- ファイルの受け渡しが必要な場合はファイル転送サービスで申請制にし履歴を管理



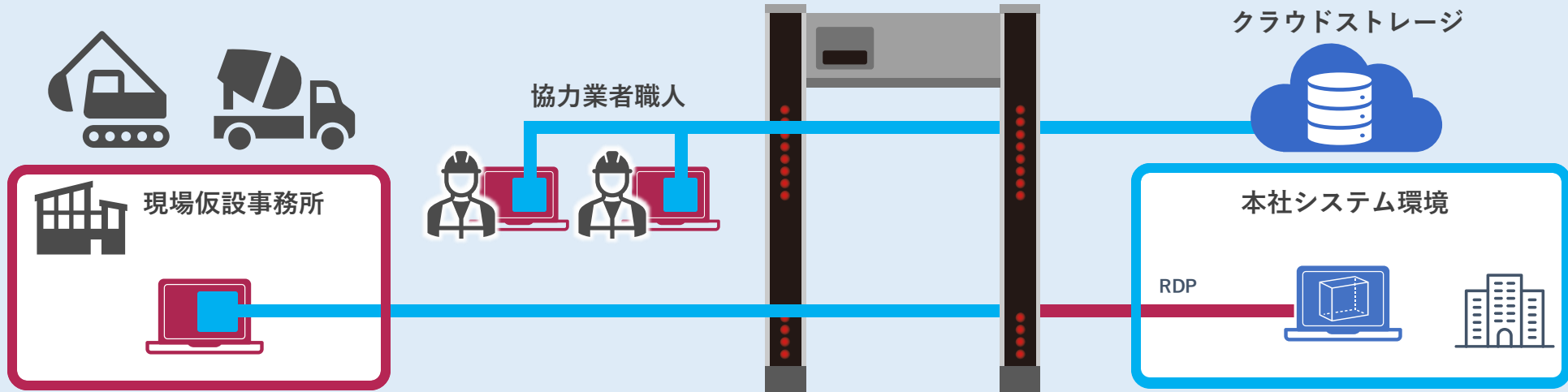
6.保守・メンテナンス委託先の情報管理

- Windows標準のリモートデスクトップ接続を隔離領域内で安全に利用
- 端末にデータを残さない形でシステムを利用させることで重要データの管理を徹底
- 保守業者の過失による情報漏洩を防止 削除証明書の提出要求など、不要・不毛な業務を省略



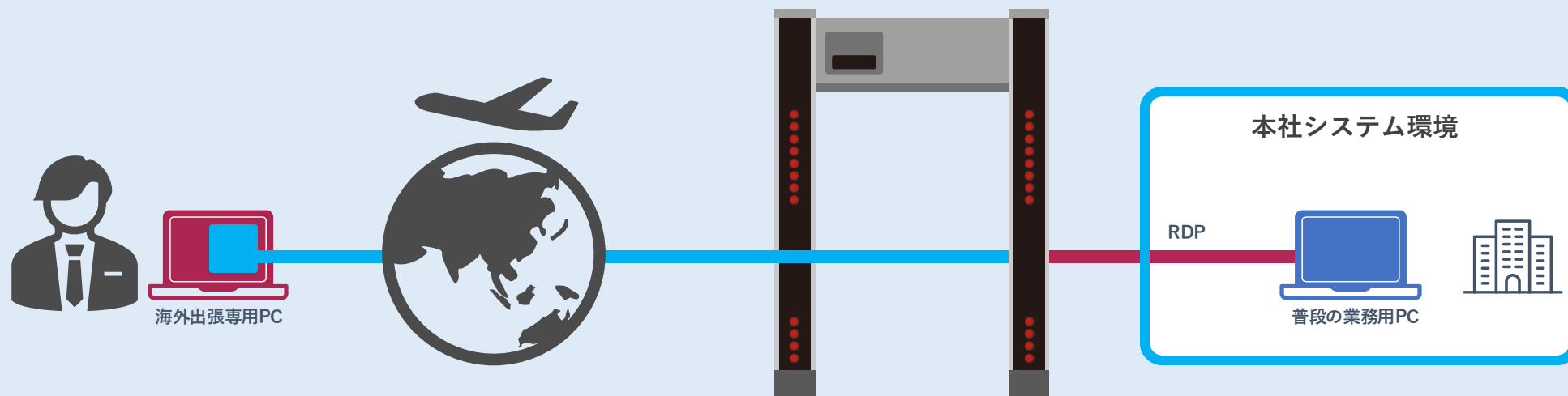
7.建設現場のセキュアなリモートアクセス環境構築

- 建設現場のセキュリティ環境をVPNを用いず安価・短納期で構築
- RDP接続で本社のCADソフトをリモートで操作
- 協力業者のPCで図面を確認させつつ、外部へのデータ持ち出しを制限



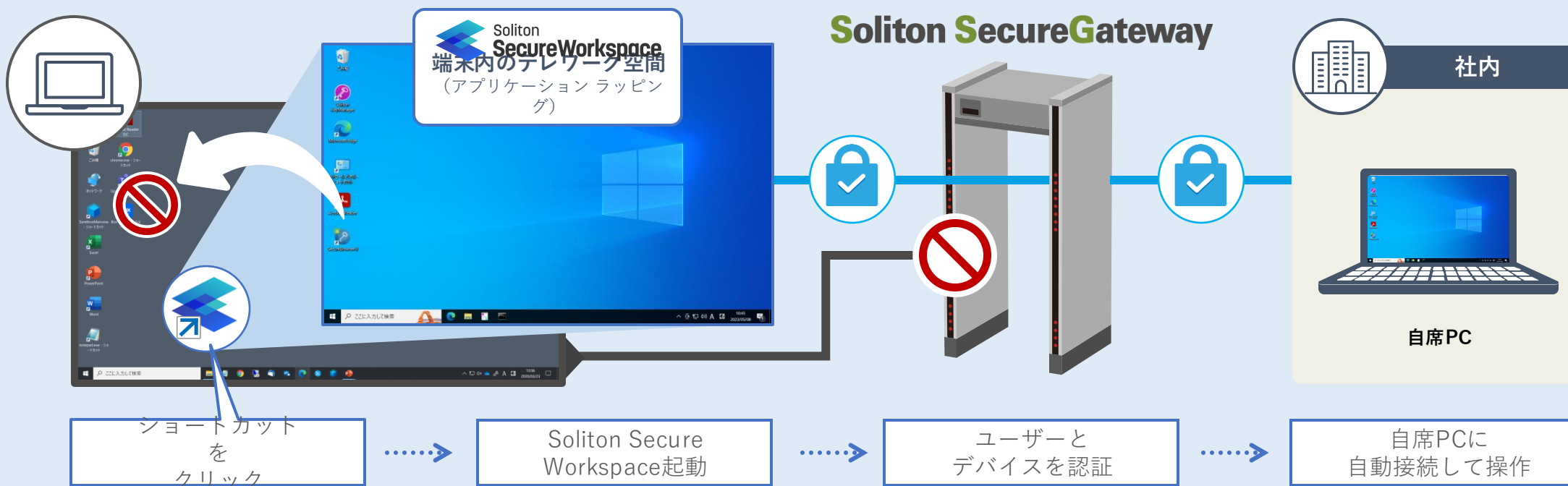
8. 海外出張専用端末の安全・低コストな運用に

- 盗難リスクの高い海外出張時の専用貸し出し端末に導入し出張先から普段のPCにRDP接続
- 接続時の多要素認証でなりすましを防止 安全に業務システムを利用
- 盗難事故や海外当局の不当捜査による重要・機密情報の漏えいを防止



リモートデスクトップも安全・快適に

- ◆Soliton SecureWorkspaceをRDPのクライアントとして動作させることも可能です。
- ◆Windows標準の **リモートデスクトップ接続を隔離領域内で安全に利用** することができます。
- ◆独自のショートカット機能から、**ワンタッチで会社PCのリモート操作**を開始。
- ◆会社端末から**手元の端末へのデータのコピー・ペースト等を制御**。情報漏えいを防ぎます。



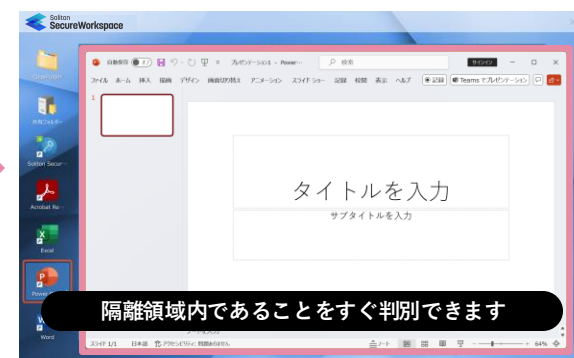
普段お使いのWindows環境、アプリケーションをそのまま利用

隔離領域用のWindowsアカウントを作成する必要はありません
SSWアプリケーションを起動するだけで隔離領域が展開します。

隔離領域内でのMS Office等のアプリケーションは普段お使いのライセンスを利用しますので、追加購入は必要ありません。

隔離領域内で起動中の業務アプリケーションはフレームカラー（色指定可能）で囲われるため、どの領域で作業をしているか、視覚的に判別が容易です

SSWログアウト時はファイルやキャッシュデータを自動的に削除するため、端末にデータが残ることによる情報漏洩の心配はありません



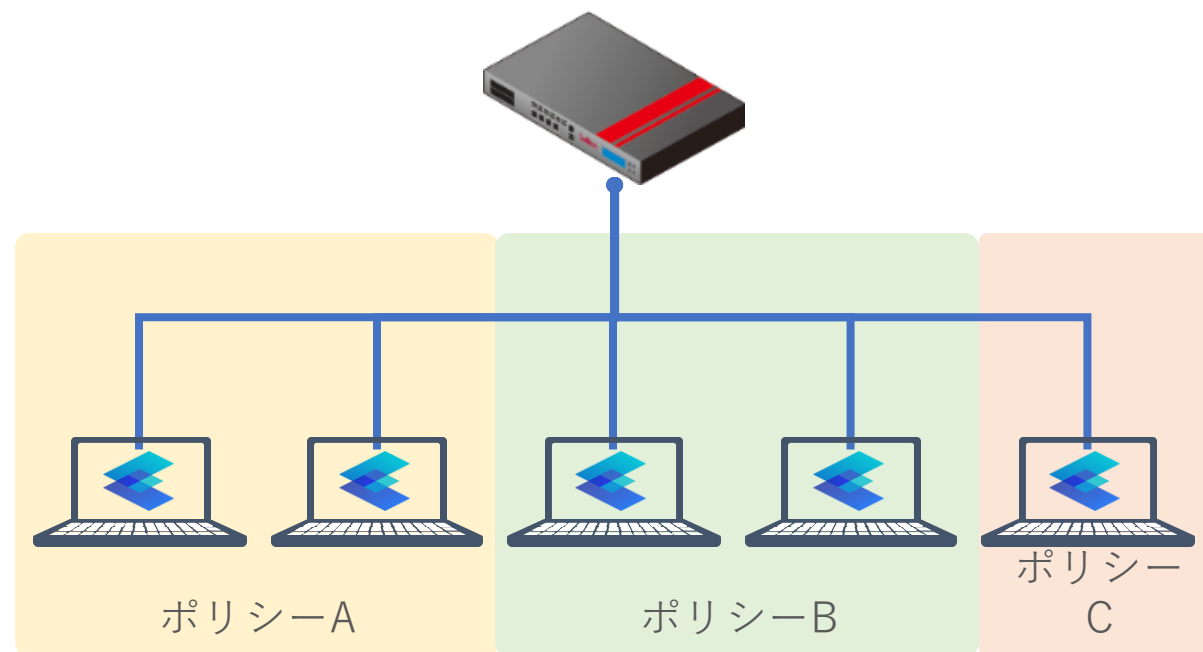
専用のゲートウェイアプライアンス

Soliton SecureGatewayで認証とプロファイル配布が可能

アプライアンスはプロキシとして動作します。
隔離領域からのみ共有フォルダやクラウドストレージへのアクセスを許可
といった制限をIPアドレスで行うことが可能です。

アカウント/グループ/組織ごとのポリシー設定が可能です。

- ・ユーザー領域へファイル保存禁止/許可
- ・テキストのコピー&ペースト禁止/許可 等

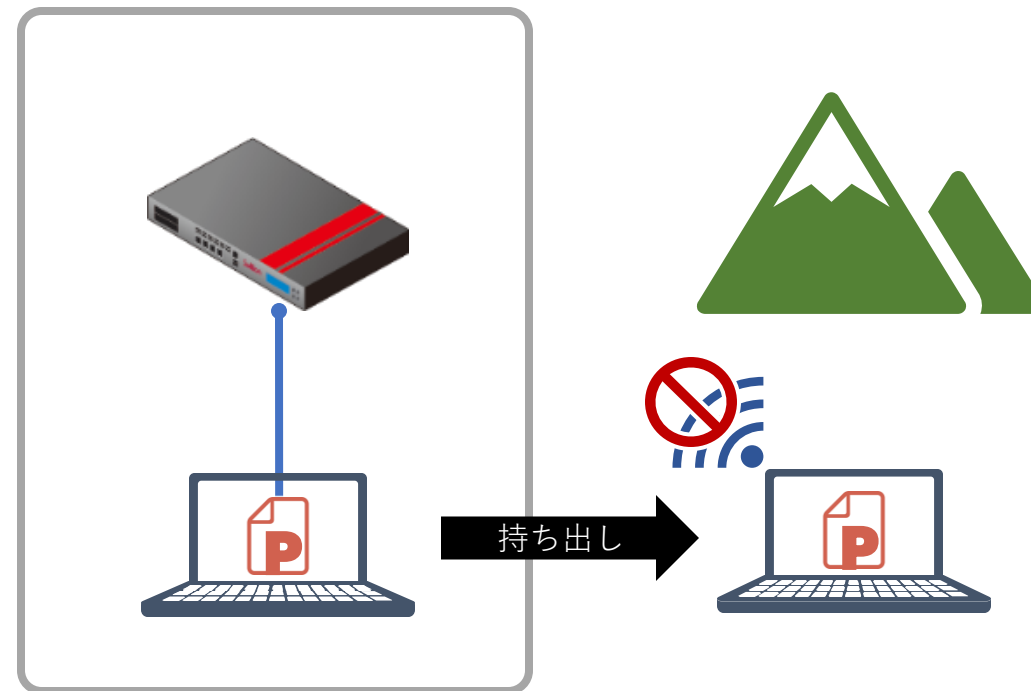


- ・SSWインストールクライアントとは独自の暗号化通信で接続（VPN不要）
- ・Soliton OneGate/ LDAP(S)/Active Directory/RADIUSと連携
- ・冗長化対応
- ・HTTP Keep-Alive対応

利用中のオフライン対応

画面転送方式ではないため、ファイル閲覧中の通信途絶や、PCをスリープ状態にした場合も、作業状態は維持することが可能です。

山間部や、高層階/地下など電波の届きにくいエリアに移動後もファイル閲覧が可能です。



- ・ ファイル編集後、共有フォルダに保存する際は通信が必要になります

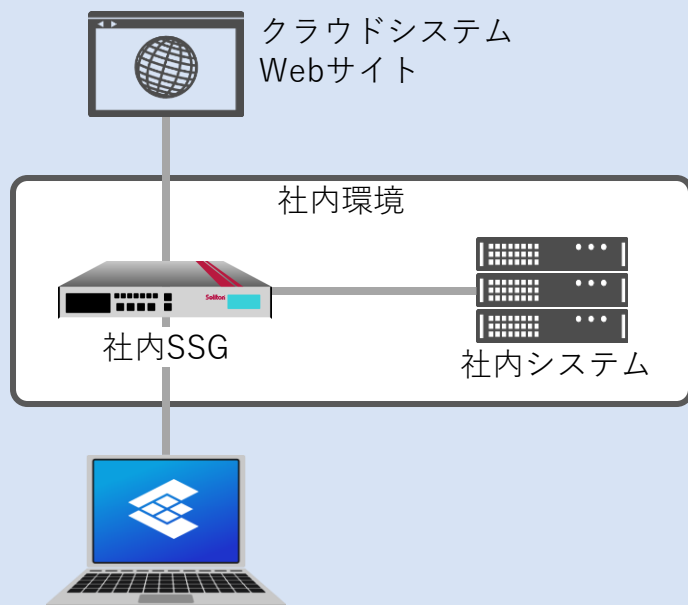


Soliton
SecureWorkspace

仕様・ラインナップ

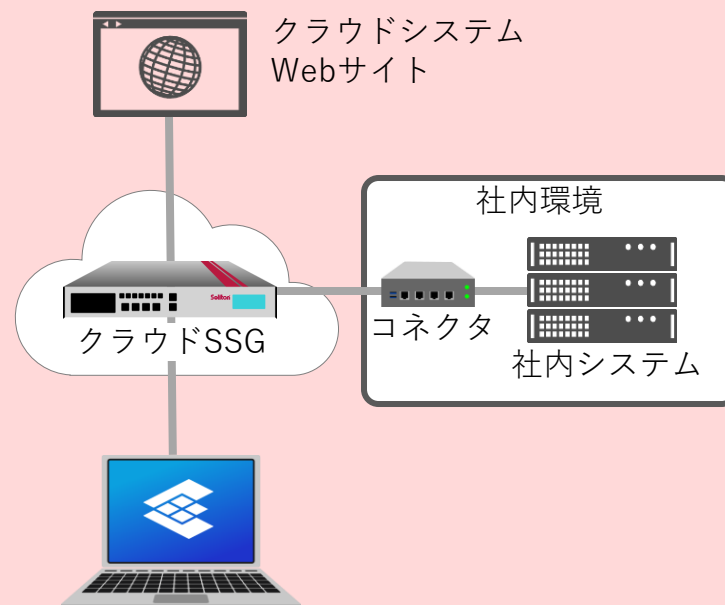
ご利用用途・環境に合わせてオンプレミス版・サービス版をお選びいただけます

オンプレミス版



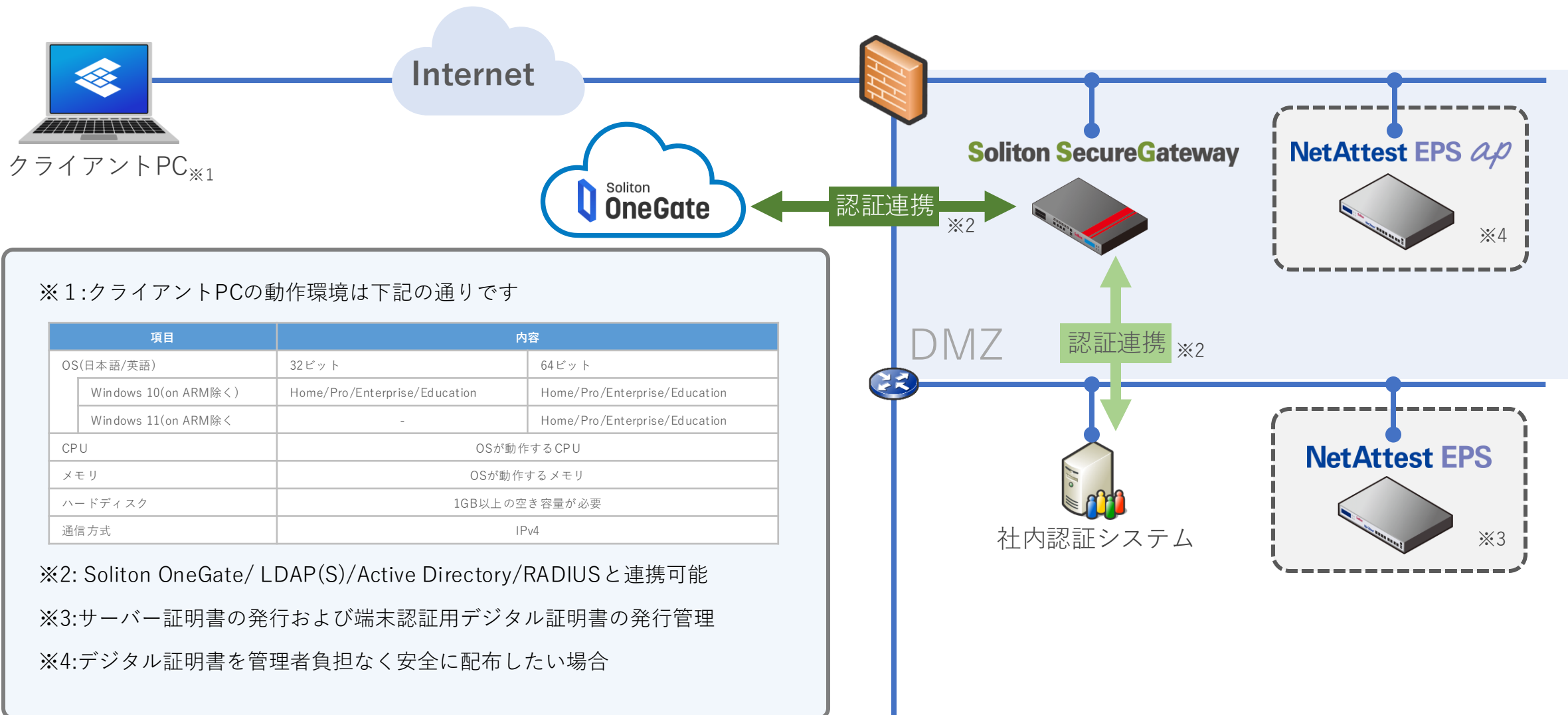
- ・専用ゲートウェイであるSoliton SecureGateway(SSG)を社内設置
- ・SSGはアプライアンスサーバーとしてご提供（物理 or VA）
- ・RDP接続で社内PCへ接続することも可能

サービス版



- ・クラウド上のシステムやWebアクセスのみ利用の場合は基本プランでOK
- ・社内イントラへアクセスする際は社内にレンタルコネクタを設置
- ・RDP接続機能はご利用頂けません

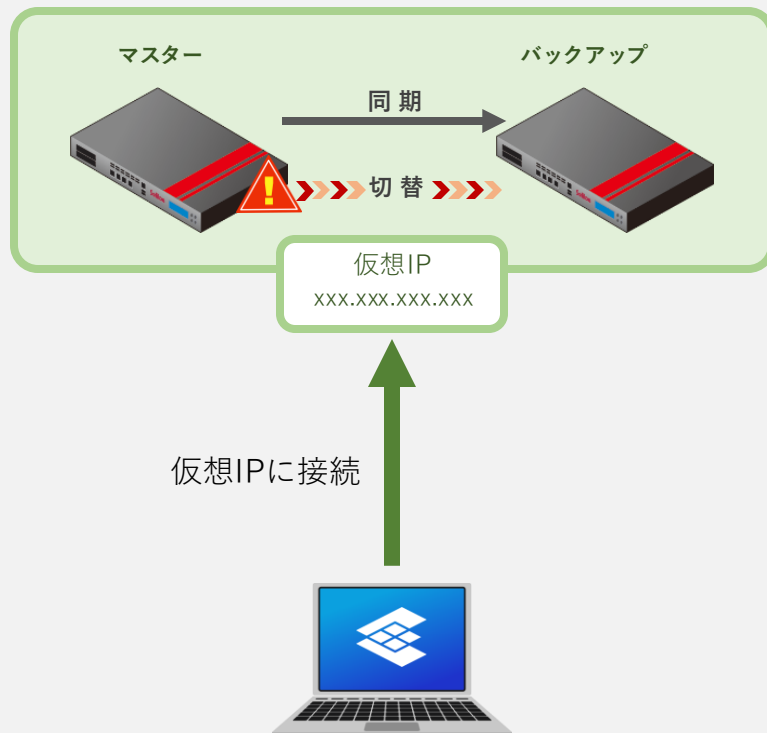
オンプレミス版



オンプレミス版

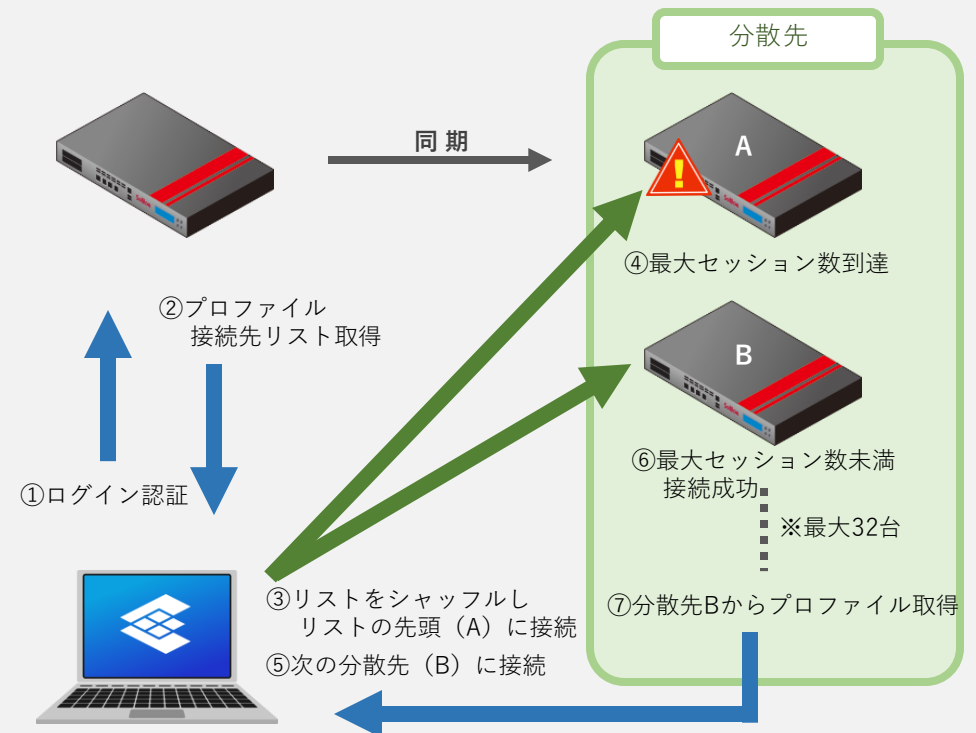
冗長化構成

マスターとスタンバイのSecureGatewayを2台ご用意いただくことで、アクティブスタンバイ構成を構築できます。※ホットスタンバイ
この2台に同一の仮想IPアドレスを設定し、SecureWorkspaceの接続先として指定します。
マスター機でサービス停止等の障害が発生した場合、速やかにバックアップ機がアクティブに切り替わるためサービスの継続利用が可能になります。



負荷分散構成

複数台のSecureGatewayを導入している環境では、負荷分散機能によってSecureWorkspaceからのアクセスを分散させることが可能です。高負荷・大規模なネットワークでも安定したサービスを提供できます。なお、接続先の選択は自動的に行われるため、ユーザーが意識することはありません。



オンプレミス版

必須

SecureWorkspace ユーザーライセンス

- SecureWorkspaceを利用するためのサブスクリプションライセンス
- 13,200円/年/1ライセンスあたり
- 最小購入数10lic / 購入単位 10lic

必須

SecureGateway サーバー価格

- SecureWorkspaceを利用するための専用アプライアンス
- 物理アプライアンス：¥1,200,000-
- 仮想アプライアンス：¥900,000-
- サイジング目安：サーバー 1 台あたり 5 0 0 ユーザーまで

必須

SecureGateway サーバー保守価格

- 物理アプライアンス
 - センドバック：¥223,000/年/台
 - 平日オンサイト：¥328,000/年/台
- 仮想アプライアンス：¥173,000/年/台
- 先き出しSENDバック：¥273,000/年/台
- 24×365 オンサイト：¥410,000/年/台

任意

NetAttest EPS / EPS-ap / Soliton OneGate

- サーバー証明書の発行および端末認証用デジタル証明書の発行管理を行う場合(NetAttest EPS)
- デジタル証明書を管理者負担なく安全に配布したい場合(NetAttest EPS-ap)
- 価格/詳細は別途お問い合わせください

サービス版

サービス版は社内イントラへのアクセス有無および証明書配布の方式によって
4つの契約パターンがあります

社内イントラへのアクセス有無

クラウドプラン（基本プラン）

- ・クラウドへのアクセスのみ
- ・システム管理者が証明書配布

Plusクラウドプラン

- ・クラウドへのアクセスのみ
- ・ユーザー申請による証明書自動配布

クラウド・イントラプラン

- ・クラウドと社内イントラにアクセス可能
- ・システム管理者が証明書配布

Plusクラウド・イントラプラン

- ・クラウドと社内イントラにアクセス可能
- ・ユーザー申請による証明書自動配布

証明書配布方式

サービス版

基本月額費用で10ユーザーまでご利用頂けます。

ライセンス追加は10ユーザー単位で月額10,000円(全プラン共通)

社内イントラへのアクセス有無

証明書配布方式

クラウドプラン（基本プラン）

- ・ 初期費用 : ¥100,000
- ・ 基本月額費用 : ¥10,000 (10usr分込み)
- ・ 追加月額費用 : ¥10,000 (10usr分)

Plusクラウドプラン

- ・ 初期費用 : ¥200,000
- ・ 基本月額費用 : ¥20,000 (10usr分込み)
- ・ 追加月額費用 : ¥10,000 (10usr分)

クラウド・イントラプラン

- ・ 初期費用 : ¥300,000
- ・ 基本月額費用 : ¥30,000 (10usr分込み)
- ・ 追加月額費用 : ¥10,000 (10usr分)

Plusクラウド・イントラプラン

- ・ 初期費用 : ¥400,000
- ・ 基本月額費用 : ¥40,000 (10usr分込み)
- ・ 追加月額費用 : ¥10,000 (10usr分)

【参考】VDIとの比較

	必要 コンポーネント	オフライン対応	アプリケーション の動作検証	操作性	ライセンス費用
	環境の構築に必要な ソフトウェア/ハードウェアの 構成要素	作業中の通信途絶、 瞬断の影響	導入前検証の 要否・検証のしやすさ	動画再生・オンライン会議	
	- クライアントソフトウェア - 専用ゲートウェイ プライアンスのみ	ログインやファイル保 存時のみ通信を行うた め、通信が途絶しても 作業状態を維持、通信 帯域も抑制できます。	必要 専用アプライアンスと クライアントソフトの みで事前の動作検証が 可能	テレワークに必要なオ ンライン会議もストレ スなく利用可能 ※ブラウザ版推奨	ゲートウェイアプライア ンス ¥1,200,000/台 +ユーザーサブスクリプ ション ~¥13,200/年 VDIと比べ 10分の1程度 ※当社比
VDI	- 中央管理サーバー - ハイパーバイザー - エージェントソフトウェ ア - クライアントソフトウェ ア - 追加PC - etc,etc,etc...	画面転送方式のため、 常にオンラインである 必要があります	必要 動作検証を行うには本 番と同じ環境を構築す る必要あり	画面転送方式のため、 動画再生やオンライン 会議に不向き	- 高額なライセン ス費用 - 為替影響 - 価格改定・・・

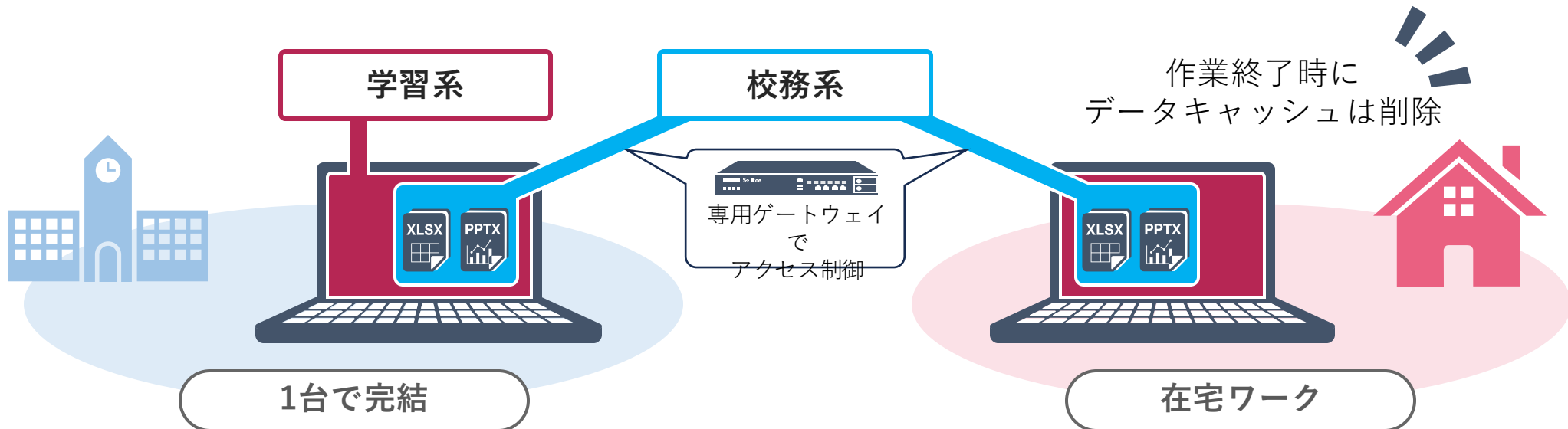
特定業務、および在宅ワーク用ツールとして活用

従前の課題

- 生徒も使う学習系と、機微な情報を扱う校務系とで、ネットワークおよび端末が分かれている
- 業務によって端末を使い分ける機会が多く、教職員に負担が掛かっている
- 自宅から、リモートで校内業務ができる環境も整えたい

導入効果

- 都度使い分けていた端末が1台に集約され、教職員の生産性が向上
- 自宅からでも安全に校内業務が行えるようになったことで、働き方が柔軟に



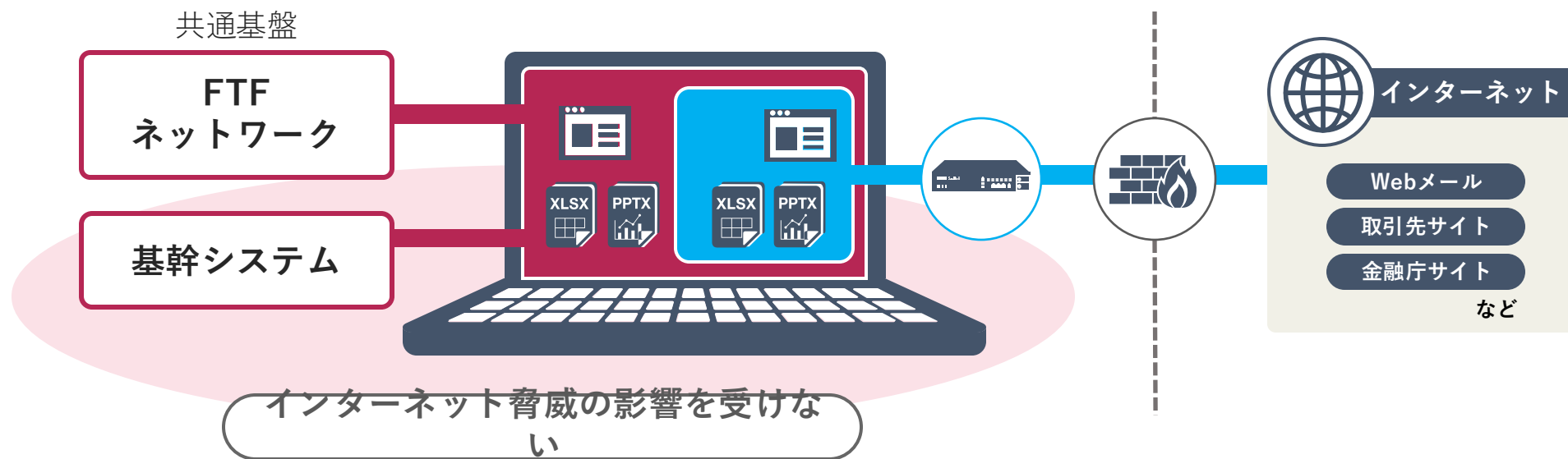
インターネット業務専用ツールとして活用

従前の課題

- 関連組織からの指導があり、基幹業務環境とインターネット接続環境の分離を検討
- 対応期限が迫っており、短期間で実現する必要があった
- メールで受け取ったファイルを編集して送り返す作業が頻繁にあり、分離後の生産性低下が懸念される

導入効果

- 大掛かりなシステムが不要な端末内仮想化方式で、早期にインターネット分離を実現
- 隔離領域内でWebメール、ファイル編集、再送が完結でき、利便性を担保



三層分離環境の業務を手元の端末に集約

従前の課題

- 総務省ガイドラインの改定により、番号利用事務系への他のセグメントからの接続について、要件が緩和。
- これまでは物理分離だったため、専用業務端末までの移動や順番待ちが発生し、業務効率が低下。
- VDIを検討するも、対象端末数が少なく、コスト効果が極めて悪い

導入効果

- 低コストで画面転送による専用端末への接続が実現
- 接続時の要件になっていた多要素認証を同一メーカー製品で実現。サポート面も安心。
- インターネット接続系で利用していたセキュアブラウザは同梱されている同一製品に置き換え、手元端末への業務集約が実現



普段と変わらない操作感の
安全なワークスペースを提供するソフトウェア



(ソリトンセキュアワークスペース)

エンドユーザー様向け、販売会社様向けに
評価環境のお貸出しが可能です。



Soliton[®]

株式会社 ソリトンシステムズ

〒160-0022 東京都新宿区新宿 2-4-3
TEL 03-5360-3811 netsales@soliton.co.jp

大阪営業所 06-7167-8881

札幌営業所 011-242-6111

福岡営業所 092-263-0400

名古屋営業所 052-217-9091

東北営業所 022-716-0766