データレスクライアントの概要と導入事例

業務システムの変遷からひも解く
経営層のための次世代エンドポイントアーキテクチャ

ビップシステムズ株式会社
AI推進室長
馬島　宗平

本セミナの目次

本セミナは、皆様の組織における業務用端末の導入戦略立案に役立つ情報を
当社の導入事例をもとに持ち帰っていただくことを目的としています。

--- 目次 ---

1. ビップシステムズ（株）紹介（インフラ構築やシステム開発をSESや派遣で実施）
2. 課題1　在宅勤務をどのように実現するか
   - ✓ 在宅勤務実現方式（M方式・U方式・W方式・A方式）
   - ✓ BYODの限界と全社員端末配布をする場合のVDIコスト比較
3. 課題2　業務システムのクラウド化（SaaS化、AI対応）にどう対応するか
   - ✓ ネットワーク境界では守れない(端末・IDで、都度アプリ認証が必要)
4. データレスクライアントとPCサブスクを組み合わせたSPCSSの紹介
   - ✓ SPCSSは、どのような要件に適し、また、適さないか

1．ビップシステムズ株式会社の概要

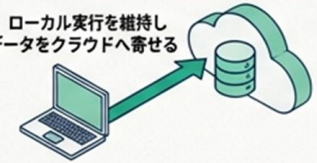
2026年4月現在

社名	ビップシステムズ株式会社　　https://www.bip.co.jp
本社所在地	東京都渋谷区桜丘町9-1　ビアンクォード 電話：(03)3463-1061 (代表)
設立	1976年11月
資本金	2000万円　（自己資本：17億円）
売上高	44.8億円　（2025年8月期）
従業員数	グループ全体 309名（内ビップシステムズ株式会社　270名） （2026年4月1日現在）
事業内容	コンピュータに関する基礎技術及びソフトウェア受託開発
関連子会社	BIP SYSTEMS Vietnam Co., Ltd.　http://www.bip.com.vn

2. 在宅勤務をどのように実現するか

単純な「ライセンス単価の安さ」で選ぶと失敗する。方式の実体は「どこで計算処理とデータ保持を行うか」というアーキテクチャの違いであり、自社の優先事項に基づく選択が不可欠。

U方式（データレスクライアント）



総額最適・UX重視

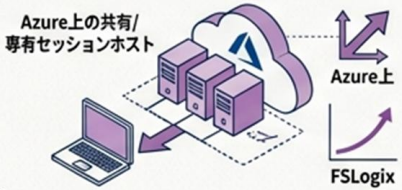
ローカル実行を維持しデータをクラウドへ寄せる。
VDIを作らないためコストが最小化（約1,500万円/年）し、
Web会議の体験も最も自然。

W方式（SaaS型クラウドPC）

完全標準化・運用予見性

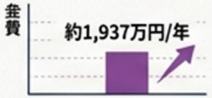
ユーザー専有のクラウドPC。最も導入・標準化が容易だが、インフラ費がライセンスに内包されるため総額は最も高い（約3,480万円/年）。

A方式（可変費型 VDI）

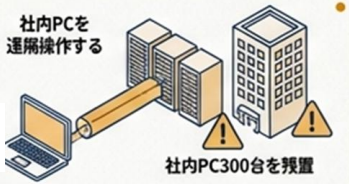


Azure運用力・スケーラビリティ

Azure上の共有/専有セッションホスト。
オートスケールでW方式より大幅に安価（約1,937万円/年）になるが、FSLogix等の運用責任が伴う。



M方式（リモートアクセス）

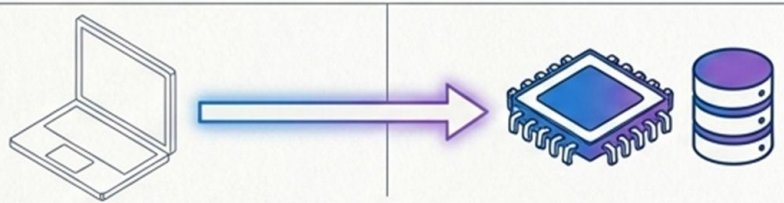
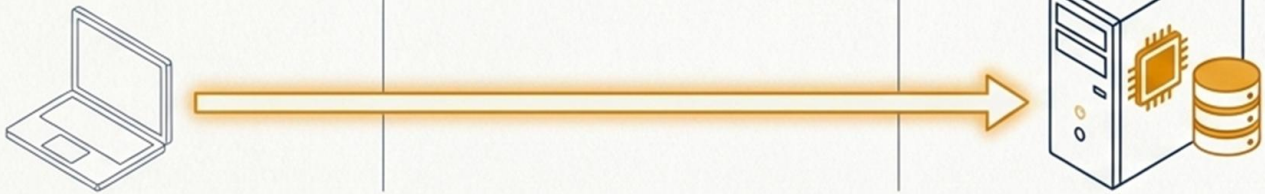


既存資産活用・短期つなぎ

既存の社内PCを遠隔操作

社内PCを遠隔操作する。ライセンスは安価だが「社内PC300台を残置」する特異な構造により、隠れた運用費・BCPリスクが重くのしかかる。

アーキテクチャの根本的差異：計算処理（Compute）とデータはどこにあるか？

	手元端末	クラウド	オフィス
U方式			
	処理は手元、データはクラウド。VDI構築不要。		
W/A方式			
	処理もデータもクラウド。ユーザーは画面転送のみ。		
M方式			
	処理もデータも「オフィス残置PC」。手元端末とは別に、社内に接続先ハードウェアを維持し続ける必要がある。		

コロナ禍の緊急対応では、手元端末はBYOD（個人所有PC）、社内PCは既存PCを活用できるM方式が最適だった

緊急避難から戦略的負債へ：2020年モデルの限界

2020年の緊急避難

「コストとスピードの最適化」

- BYODの緊急解禁
- 社内PCの電源つけっぱなし運用
- 簡易VDIによるアクセス

端末調達費の大幅削減（例：300台×15万円＝4,500万円の抑制）

現在露呈している負債

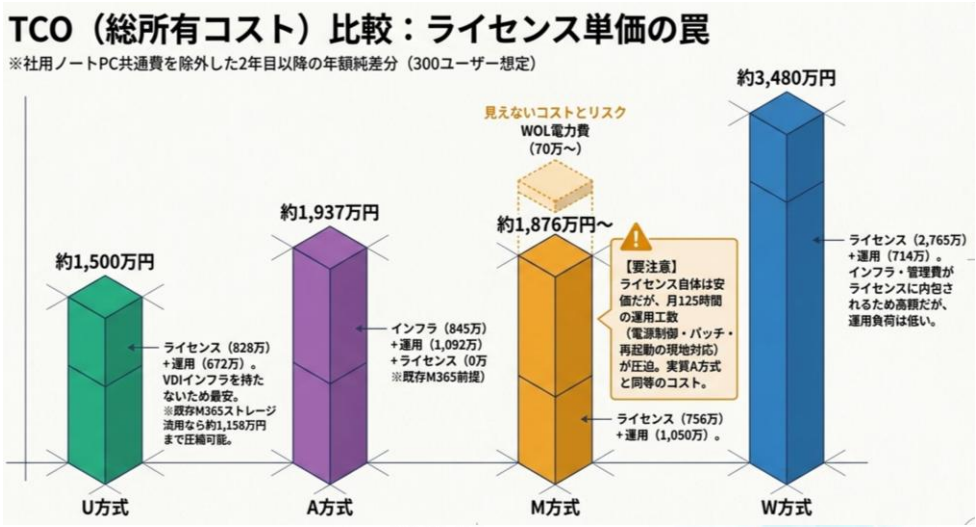
「運用限界とセキュリティリスク」

- **BYOD限界:** 個人資産のため会社のセキュリティ対策（MDM等）が強制できず、シャドーIT化。
- **オフィス依存:** 停電や再起動のたびに出社が必要。無駄な電力消費。
- **コミュニケーション不全:** 個人スマホでのチャット制約により、リモートワーク時の連携が低下。

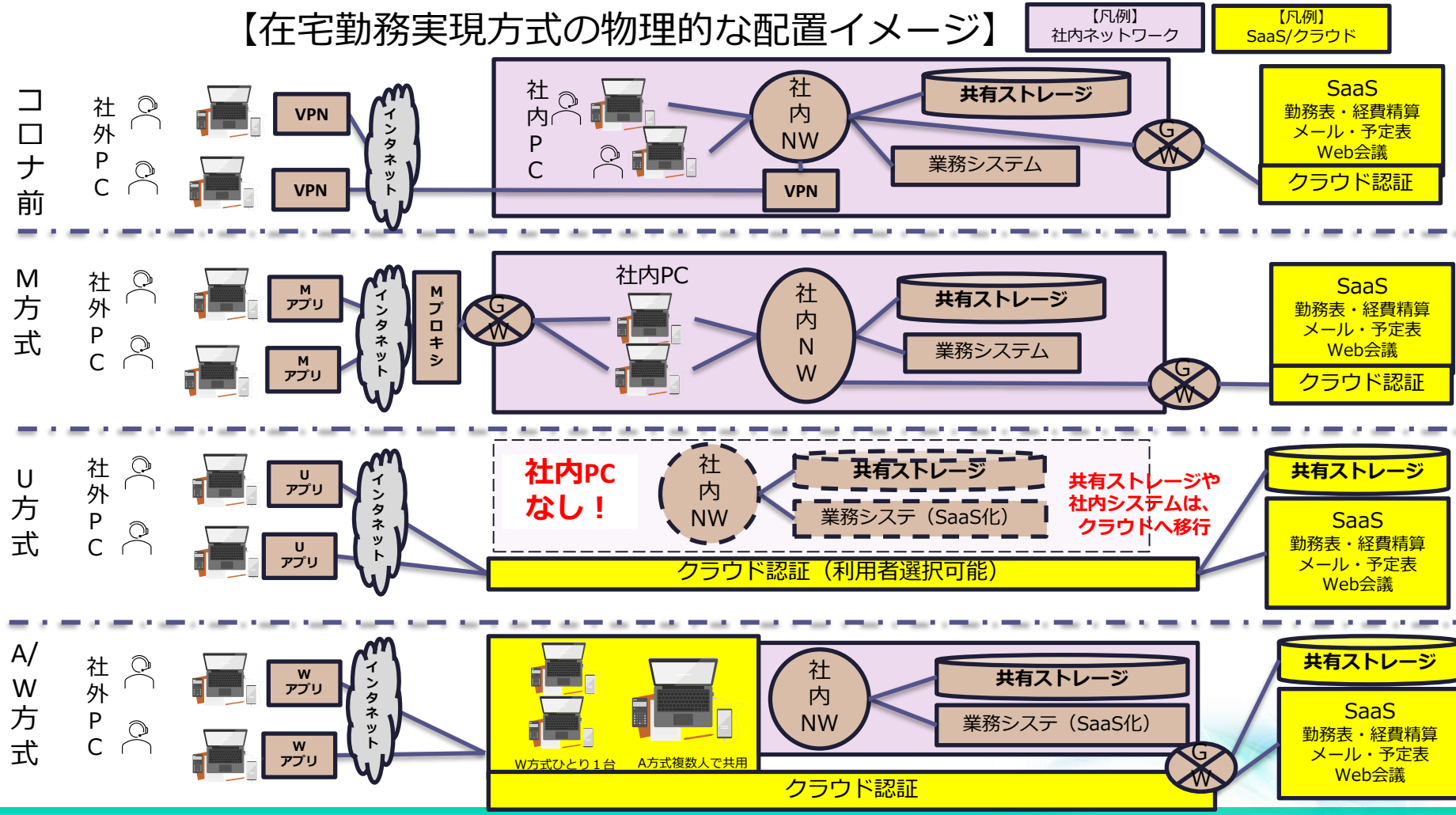
全社員端末配布をする場合のコスト比較

コロナ禍対応の緊急対策（特にPCのBYOD利用）は、課題が多かったので、当社では、全社員（ここでは仮に300名とする）に業務用にノートPCを配布することとした。
ただし、当社の社員はSESが多く、顧客から顧客業務用PCを貸与されているケースが多いため利用用途は社内業務、社内チャットが主体でありコストは極力抑える必要があった。

※右表の棒グラフの価格は、300名に新規導入した場合の手元PC以外のTCOをカタログ値で比較した



【在宅勤務実現方式の物理的な配置イメージ】



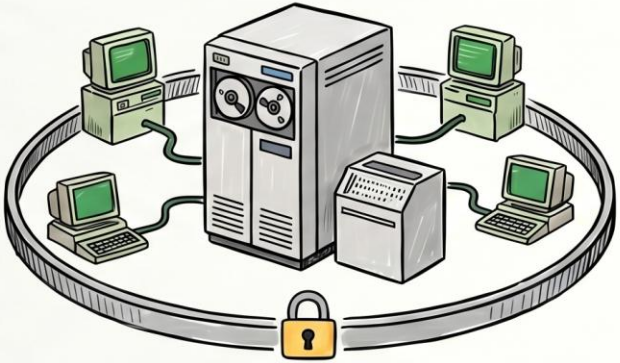
3. 業務システムのクラウド化（SaaS化、AI対応）にどう対応するか

1970年代から現代まで、システム基盤と守るべき境界が物理的な「場所」から個別の「端末・ID」へシフトした過程を追う

第1世代：1970〜80年代 (社内閉域・専用端末)

中央集中型のメインフレーム・オフコン時代

システムは社内データセンターに設置され、すべての処理が中央で行われる「中央集中型」の構成



物理的な「閉域網」による防御

専用回線と閉域網を使用し、外部からのインターネット接続は存在しないため、社内設備そのものが強靭な境界でした

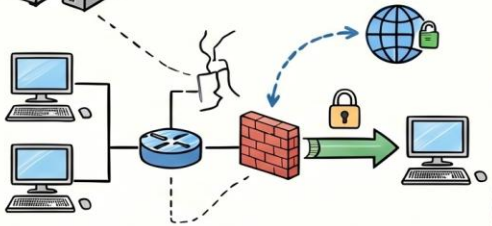
セキュリティ境界 = 社内設備 + 専用線

専用端末は社内設置が原則であり、物理的な場所を信頼の機軸としていました

第2世代：1990〜2000年代 (オープン系・社内PC)

オープン系サーバとクライアント/サーバ構成

自社DCやサーバ室にオープン系サーバを配置し、業務端末として社内PCが普及した時代です

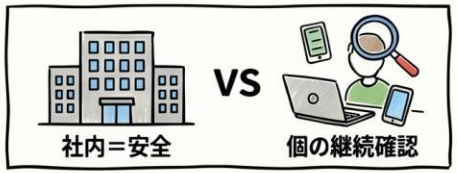


ネットワーク制御（VPN）の導入

社内LANを基本としつつ、社外拠点からはVPNや専用船を用いて接続する境界型防御が中心となりました

セキュリティ境界 = ネットワーク + VPN

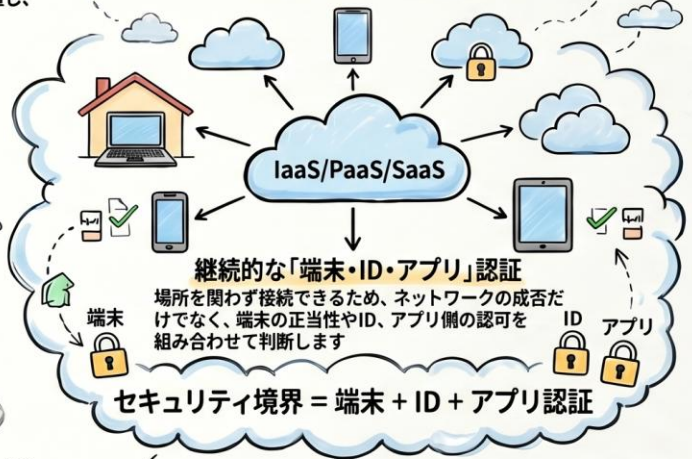
PCが業務処理の一部を担うようになり、ネットワークの入り口を管理することがセキュリティの基本でした



第3世代：2010年代後半〜現在 (クラウド・在宅対応)

パブリッククラウドとSaaSの全面活用

システム基盤はIaaS/PaaS/SaaSへ移行し、インターネット経由でのアクセスが前提となります



継続的な「端末・ID・アプリ」認証

場所を関わず接続できるため、ネットワークの成否だけでなく、端末の正当性やID、アプリ側の認可を組み合わせて判断します

セキュリティ境界 = 端末 + ID + アプリ認証

「場所」に依存せず、ゼロトラストの考え方に基づき、アクセスごとに信頼を確認する形態へと進化しました

まとめ：セキュリティ設計の焦点の変化

以前は「社内＝安全」という場所の信頼に依存していましたが、現代では「誰がどの端末で何に」アクセスするかを継続的に確認することが不可欠です

多角的な運用評価マトリクス（UX・BCP・セキュリティ）

Web会議などリッチなUXならローカル実行の「U方式」。ゼロトラストとBCPを極めるなら「W方式」。M方式はオフィス環境への依存が最大の脆弱性となる。

	U方式	W方式	A方式	M方式
UX / レスポンス (Web会議・Office)	4.5/5 ■■■■◧ ローカル実行で最も自然。動画も遅延なし	4.0/5 ■■■■□ 一般業務には十分	4.0/5 ■■■■□ Teams最適化設定が必須	3.5/5 ■■■◧□ **社内回線に依存**
BCP / 災害耐性	4.0/5 ■■■■□	4.5/5 ■■■■◧ 完全なクラウド依存で堅牢	4.0/5 ■■■■□	2.5/5 ■■◧□□ オフィスの停電・ネットワーク障害で全社停止のリスク
運用標準化 / ログ管理	4.0/5 ■■■■□ MFA/条件付きアクセスの設計要確認	4.5/5 ■■■■◧ Intune一元管理・復元容易	4.5/5 ■■■■◧ Azure Monitorでの深い分析可	4.0/5 ■■■■□ 管理機能は厚いが、ハードウェア障害対応が残る

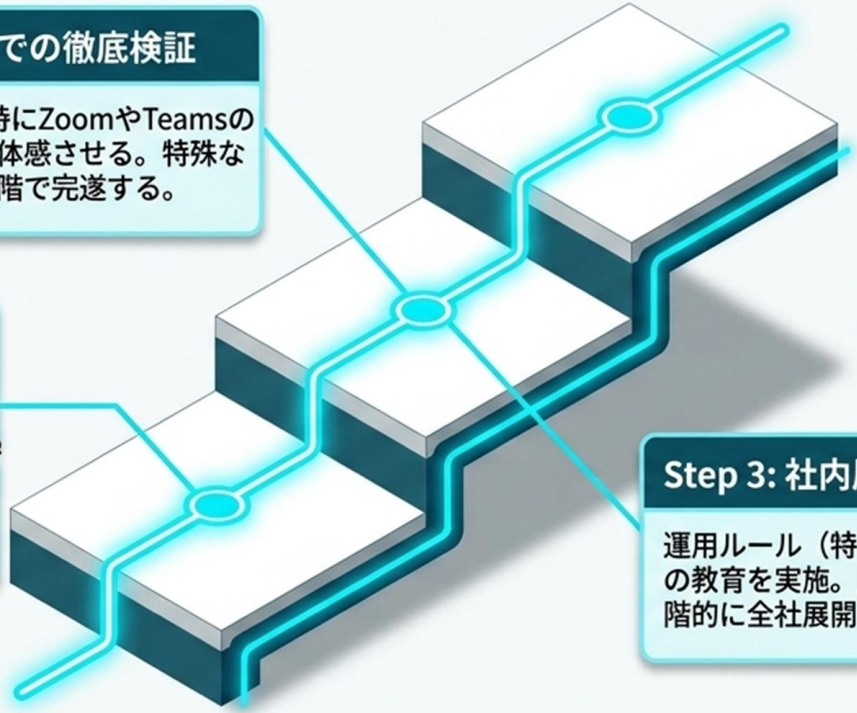
導入ノウハウ：自社に最適化するためのステップ（PoC～展開）

Step 2: PoC（概念実証）での徹底検証

VDIとのパフォーマンス比較、特にZoomやTeamsの圧倒的な軽さをユーザーに直接体感させる。特殊な社内アプリの動作検証もこの段階で完遂する。

Step 1: スモールスタートと対象切り分け

全社一斉展開は避け、まずは「Web会議頻度が高い部門」や「機密情報を扱うバックオフィス」からパイロット版として選定する。



Step 3: 社内展開とルール浸透

運用ルール（特にオフライン時の対応フロー）の教育を実施。成功体験を社内広報しつつ、段階的に全社展開へと拡大していく。

自社に最適な方式は？ 要件に基づく推奨シナリオとPoCへの道筋

Decision Panel

コスト最適化と自然なUXを両立したい	**【U方式】を第一候補に。** VDIを作らないため最安。Web会議もローカルPC感覚。
Azure運用チームがあり、費用対効果と拡張性を最大化したい	**【A方式】を選択。** マルチセッションと自動スケールを活用。
予算よりも「全社員・社外委託先への均一な環境配布」を最優先する	**【W方式】を選択。** 最も高額だが、Intuneによる完全な標準化が可能。
既存のレガシー業務アプリをそのまま短期で在宅化したい	**【M方式】を「部門限定の短期つなぎ」として併用。** 全社の中長期基盤としてはBCPリスクが高いため、段階的な移行を推奨。

Action Panel

PoC（概念実証）の推奨手順

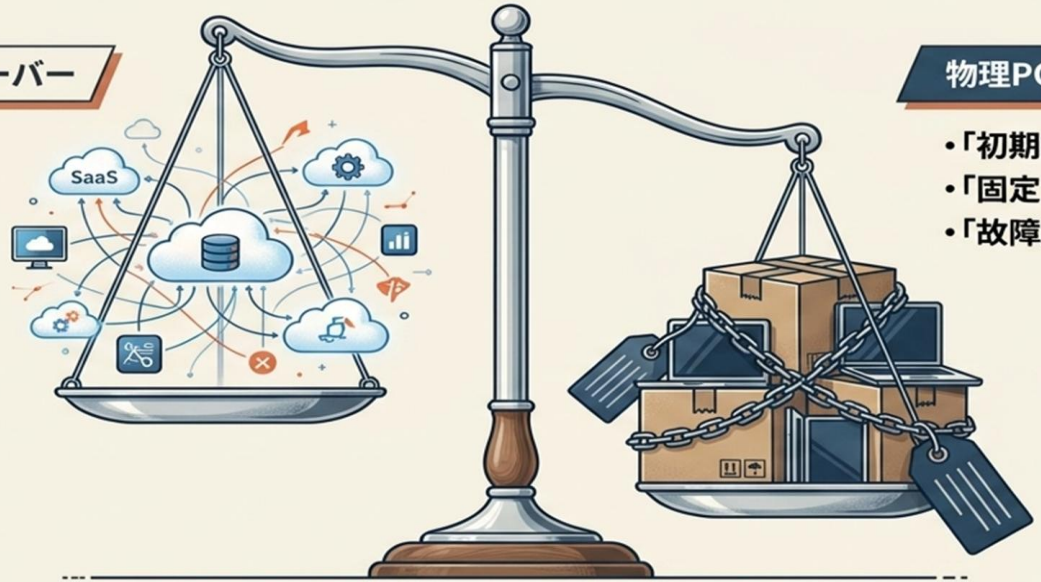
1. **本命の並走:** まず「U方式」と「A方式」のPoCを30〜50名規模で並走させる。
2. **検証ポイント:** U方式は「アプリとの相性・例外設定」、A方式は「FSLogix性能・Teams最適化・ログ監視」を重点確認することで、正式見積りの精度が飛躍的に向上する。

4.セキュアPCサブスクサービス（SPCSS）の紹介

DXにおける「ミッシングリンク」：ハードウェアの硬直性

ソフトウェアやサーバー

- 「使った分だけ」
- 「柔軟に増減」
- 「運用レス」



物理PC（ハードウェア）

- 「初期投資の重圧」
- 「固定資産管理」
- 「故障対応・キッティングの負担」

ソフトウェアやサーバーがクラウド化し柔軟性を手に入れた一方で、手元の物理PCの調達・運用は旧態依然としている。クラウドの柔軟性を「物理エンドポイント」にも適用する必要がある。

クラウドの柔軟性を物理PCへ：「SPCSS」の全体像

データレスクライアント技術（U方式）

データはクラウドへ、
アプリはローカルで稼働。

＋

PCサブスクリプションサービス

端末調達、キッティング、故障交換、
問い合わせ対応をパッケージ化。

＝

SPCSS（Secure PC Subscription Service）

※OSライセンスは含むが、MS365等のクラウドサービス・ストレージ（OneDrive, Google Drive等）は顧客の既存資産をそのまま活用可能。

SPCSSの価値 ①：妥協のないセキュリティと業務継続性

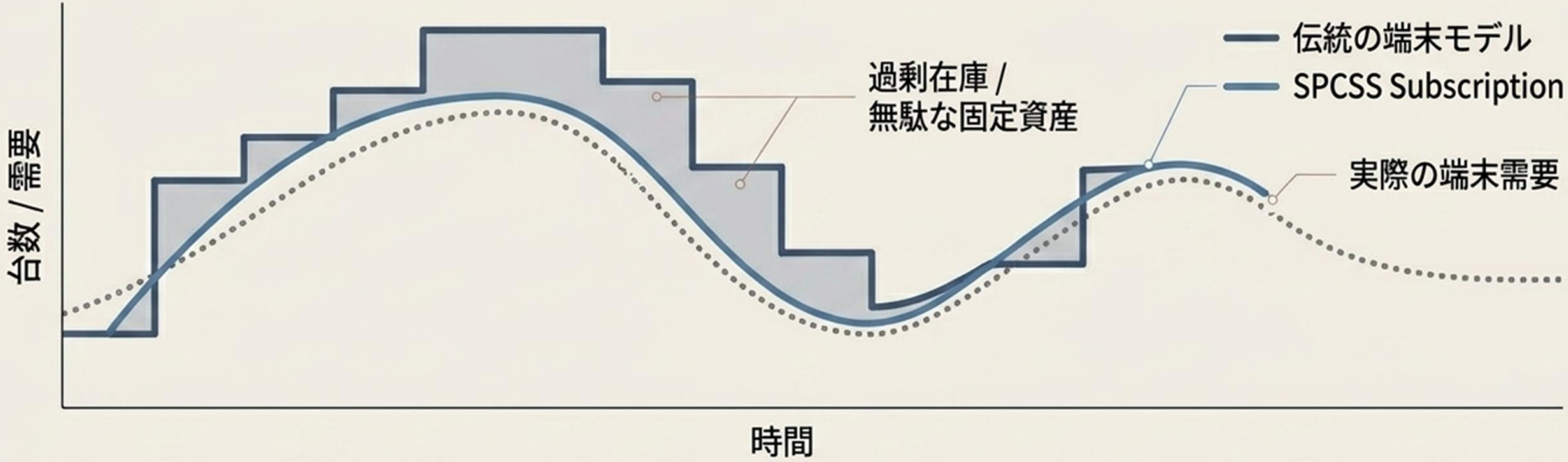
オフライン作業の快適性

キャッシュ技術により、移動中やネットワーク不安定な環境でもExcel等の作業がシームレスに継続。通信回復時に自動同期。

紛失・ランサムウェア対策

- ローカルにユーザデータを残さない。
- 盗難時はセンターからクラウドストレージと端末を即時切り離し。
- ランサムウェア感染時も、多世代バックアップにより新しいPCで感染前のデータへ即復元可能（※オプション）。

SPCSSの価値②：需要にアジャストするクラウド型調達



初期投資ゼロ

PC調達を資産購入から月額のサービス利用料（Opex）へ転換。

柔軟な増減

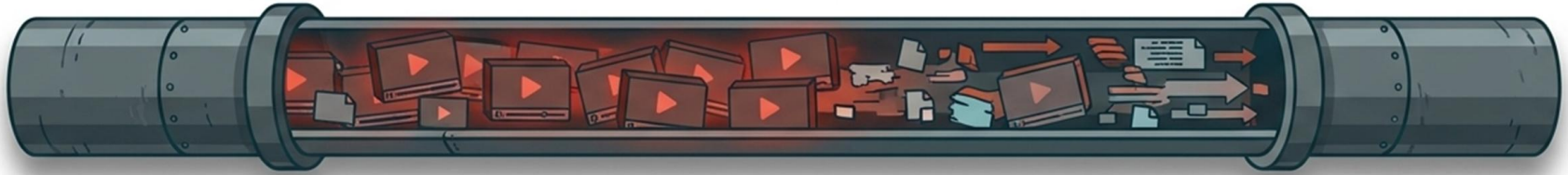
端末需要が見通せない場合でも、半年後などのスパンで必要数にアジャスト可能。過剰在庫のリスクを排除。

運用のアウトソース

どうしても発生する端末の故障、紛失、盗難時の交換対応ももサブスクリプション内に包含。

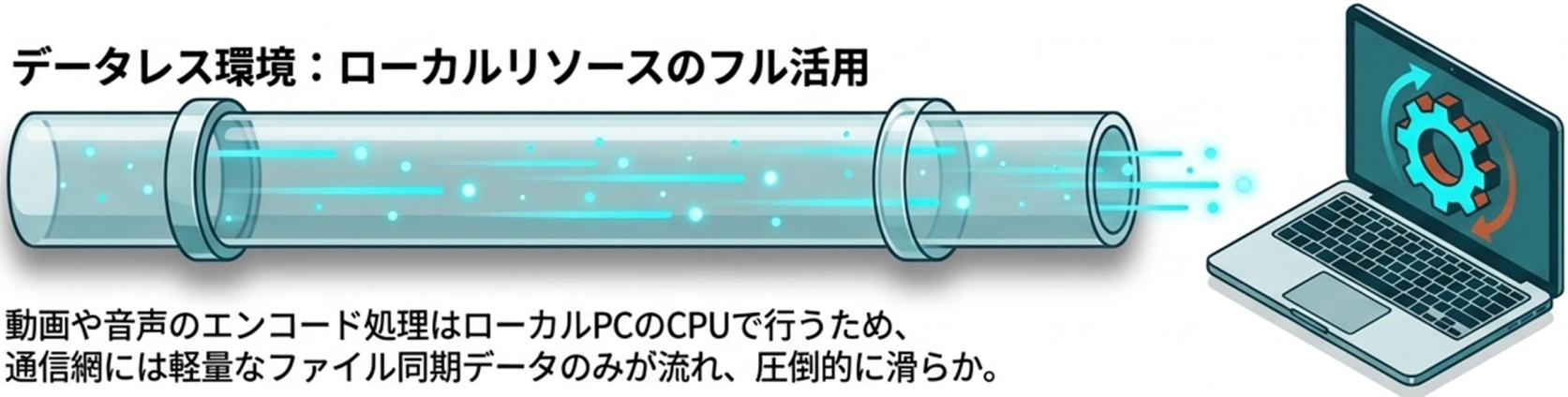
SPCSSは、U方式を利用
最大の選定理由：Web会議とアプリケーションの圧倒的なスムーズさ

VDI環境：画面転送による帯域逼迫



重い映像データのレンダリング通信がネットワークを塞ぎ、ZoomやTeamsが頻繁に遅延・フリーズする。

データレス環境：ローカルリソースのフル活用



動画や音声のエンコード処理はローカルPCのCPUで行うため、
通信網には軽量なファイル同期データのみが流れ、圧倒的に滑らか。

SPCSSは、U方式を利用

運用面の隠れたメリット：いざという時の「アジリティ（機敏性）」

通常時：ユーザーの自律性重視

ガチガチの設定制限による利便性の阻害を行わず、日々の業務スピードを最大化。

有事の際：ピンポイント介入

即時切断

端末紛失やインシデント疑い時には、申告ベースで即座にクラウドとのアクセスを強制切断。

詳細ログ

トラブルシューティング要請に応じて、ピンポイントで詳細な動作ログを取得。

運用効果：一律の強権的な制限によるサポート負荷の増大を防ぎつつ、きめ細かで迅速な故障・インシデント対応を実現。

物理的な「場所」の管理から解放されるDX組織へ

Architecture

境界防御からゼロトラスト（継続的なID/端末認証）への完全移行。

Strategy

「2020年の緊急避難」による負債を清算し、戦略的な社用PC+データレス環境を構築。

Agility

ソフトウェアのクラウド化に合わせ、ハードウェア調達もSPCSSによって「サブスク化（サービス化）」する。

組織の柔軟性とセキュリティを両立する次世代エンドポイント戦略について、
ぜひブースで詳細なデモをご体験ください。

技術で情報社会を追求する企業です。

デジタル革命の真っ只中にある日本。
ビップシステムズは豊富な実績、ノウハウと先進的な技術で
お客様を強力にサポートします。

ビップ システムズ