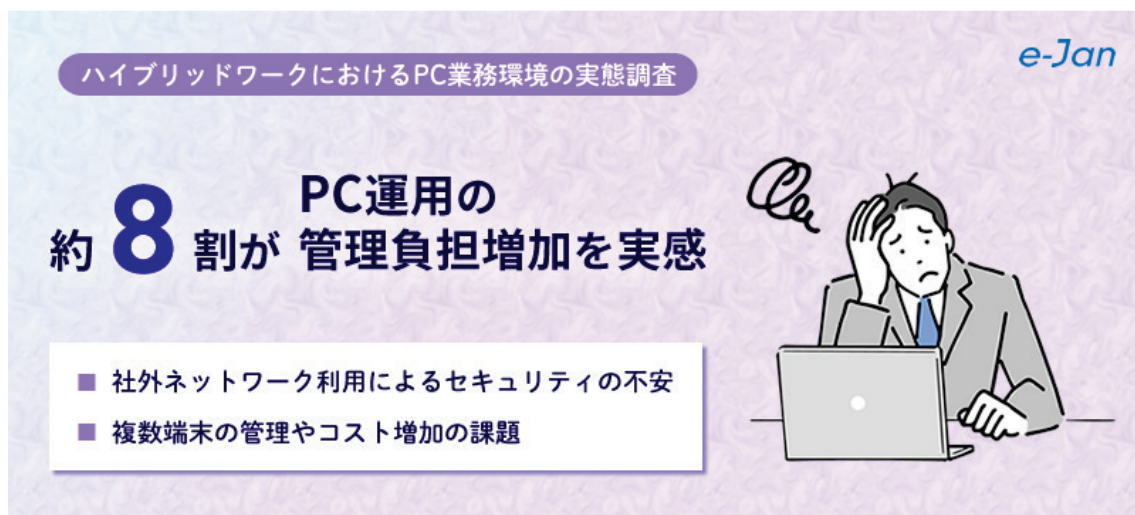


「ハイブリッドワークにおける PC 業務環境の利用や課題」に関する調査を実施、 ハイブリッドワーク下の PC 運用に約 8 割が管理負担増を実感

～情報システム部門に集中するセキュリティと運用管理の課題が明らかに～

e-Jan ネットワークス株式会社（本社所在地：東京都千代田区、代表取締役：坂本 史郎）は、ハイブリッドワーク環境における PC 業務環境の実態と課題を把握することを目的として、中堅～大企業の情報システム担当者・責任者 1,014 名を対象に「ハイブリッドワークにおける PC 業務環境の利用や課題」に関する調査を実施しました。調査の結果、リモート接続手段の普及が進む一方で、セキュリティ運用や PC 管理に関する負担が情報システム部門に集中している実態が明らかになりました。



■ 調査の背景

近年、オフィス勤務とリモートワークを組み合わせたハイブリッドワークは、多くの企業において定着しつつあります。柔軟な働き方を実現できる一方で、業務環境が社内外に分散することにより、PC 運用やセキュリティ管理の複雑化が進んでいます。

特に情報システム部門では、リモート接続手段の選定、端末管理、セキュリティ対策、トラブル対応など、従来以上に多岐にわたる業務を担う状況となっています。

こうした背景を踏まえ、ハイブリッドワーク環境における PC 業務環境の利用実態と課題を明らかにするため、本調査を実施しました。

■ 調査結果サマリー

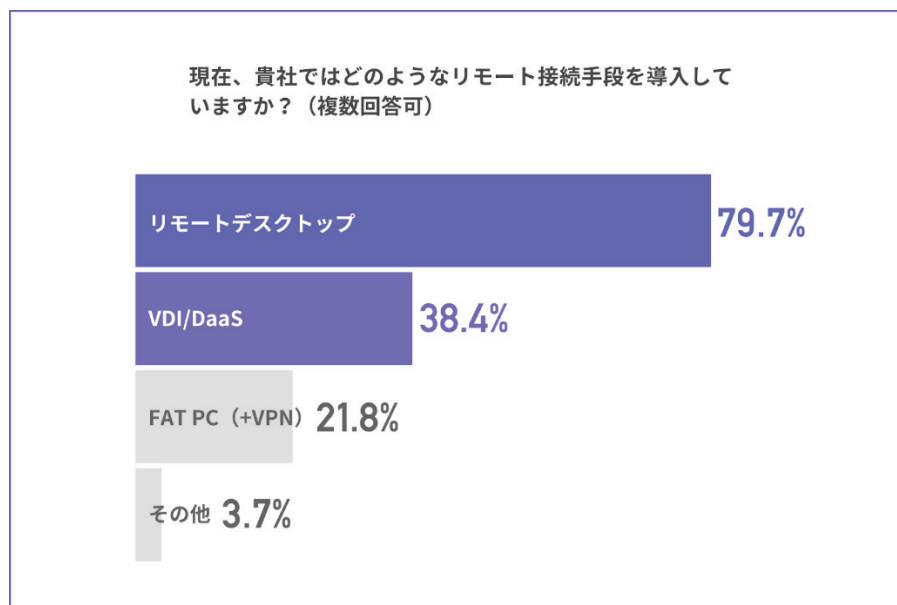
1. 約 8 割が「リモートデスクトップ」を導入
2. リモート接続手段を問わず、セキュリティ運用やコスト、管理工数が課題
3. リモート接続手段導入後、約 8 割が PC 運用・管理負荷の増加を実感
4. 社外ネットワーク利用や端末紛失など、セキュリティリスクの不安が顕在化
5. 理想の PC 業務環境は「1 人 1 台」「端末にデータを残さない仕組み」

■ 調査の結果

・ 現在導入しているリモート接続手段

導入しているリモート接続手段について尋ねたところ、「リモートデスクトップ（79.7%）」が最多となり、「VDI/DaaS（38.4%）」「FAT PC（+VPN）（21.8%）」と続きました。「リモートデスクトップ」が最も多く利用されている結果となった一方で、「VDI/DaaS」や「FAT PC（+VPN）」などを用途や部門ごとに併用している企業も一定数存在しています。このことから、リモートデスクトップ利用が主流である一方、複数の接続手段が併存することで、運用管理の複雑化につながる可能性が示唆されます。（図表 1）

【図表 1：リモート接続手段の導入状況】

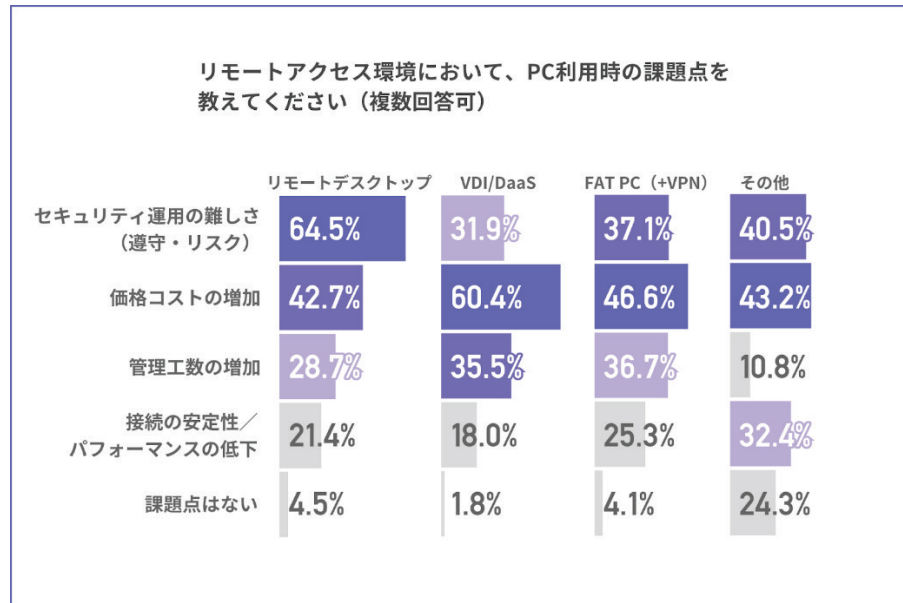


・ リモートアクセス環境における PC 利用時の課題（接続手段別）

リモートアクセス環境での PC 利用時の課題についてリモート接続手段別に見ると、リモートデスクトップでは「セキュリティ運用の難しさ（遵守・リスク）（64.5%）」が最も多く、「価格コストの増加（42.7%）」「管理工数の増加（28.7%）」と続きました。VDI/DaaS では「価格コストの増加（60.4%）」が最多で、「管理工数の増加（35.5%）」「セキュリティ運用の難しさ（遵守・リスク）（31.9%）」が挙げられています。FAT PC（+VPN）でも「価格コストの増加（46.6%）」「セキュリティ運用の難しさ（遵守・リスク）（37.1%）」「管理工数の増加（36.7%）」と、FAT PC（+VPN）でも「価格コストの増加」「セキュリティ運用の難しさ（遵守・リスク）」「管理工数の増加」が上位を占めました。

リモート接続手段を問わず、コスト負担に加えて、セキュリティ運用や管理工数といった運用面の課題が上位に挙げられていることが分かりました。（図表 2）

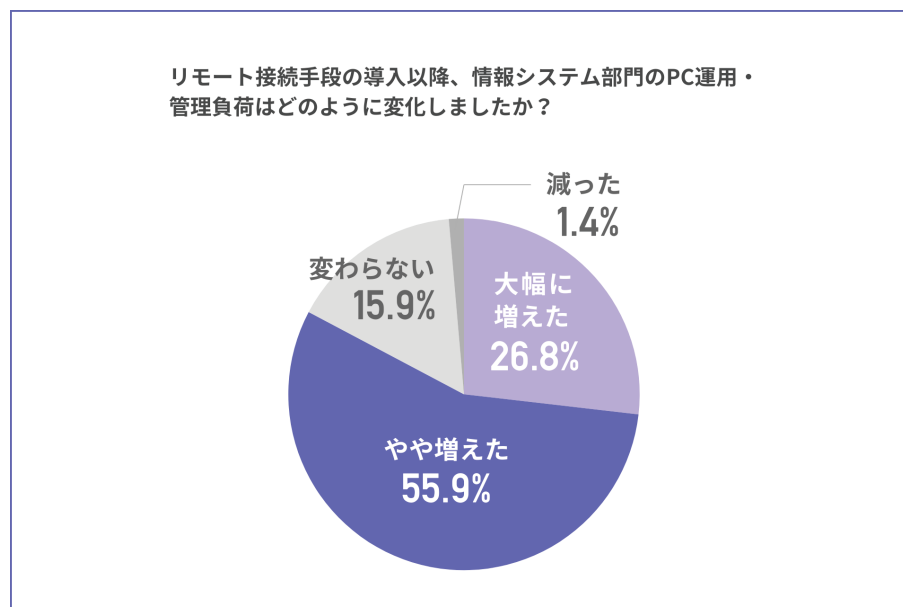
【図表 2：リモートアクセス環境による PC 利用時の課題】



・ リモート接続手段導入後の PC 運用・管理負荷

リモート接続手段導入以降の、情報システム部門の PC 運用・管理負荷について尋ねたところ、「大幅に増えた（26.8%）」「やや増えた（55.9%）」を合わせ、約 8 割が負荷増加を実感していました。ハイブリッドワークの定着が、情報システム部門の業務量増加につながっていることが示されていました。（図表 3）

【図表 3：リモート接続手段導入以降の情報システム部門の PC 運用・管理負荷】



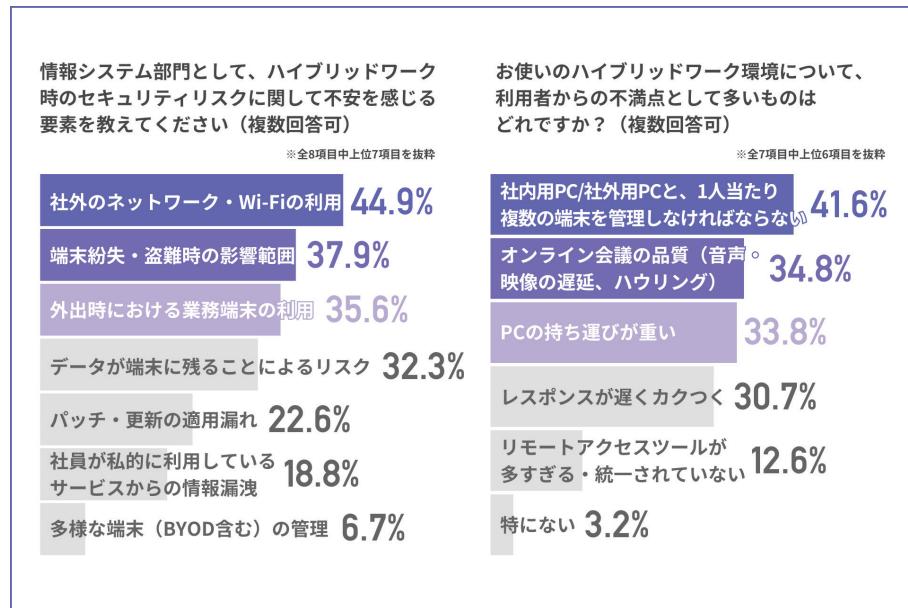
・ ハイブリッドワーク時のセキュリティリスクへの不安

ハイブリッドワーク時のセキュリティリスクに関して不安を感じる要素としては、「社外のネットワーク・Wi-Fi の利用（44.9%）」「端末紛失・盗難時の影響範囲（37.9%）」「外出時における業務端末の利用（35.6%）」が上位に挙がりました。社外利用を前提とした業務環境において、管理外環境への懸念が強まっていることがうかがえます。（図表 4）

- ・ **利用者から多く寄せられる不満点**

ハイブリッドワーク環境についての利用者からの不満点では、「社内用 PC/社外用 PC と、1 人あたり複数の端末を管理しなければならない（41.6%）」「オンライン会議の品質（音声・映像の遅延、ハウリング）（34.8%）」「PC の持ち運びが重い（33.8%）」が多く挙げられました。運用上の都合が、利用者の業務効率や満足度に影響している様子がうかがえます。（図表 4）

【図表 4：情報システム部門としてハイブリッドワーク時のセキュリティリスクに関する不安と
ハイブリッドワーク環境について利用者からの不満点】



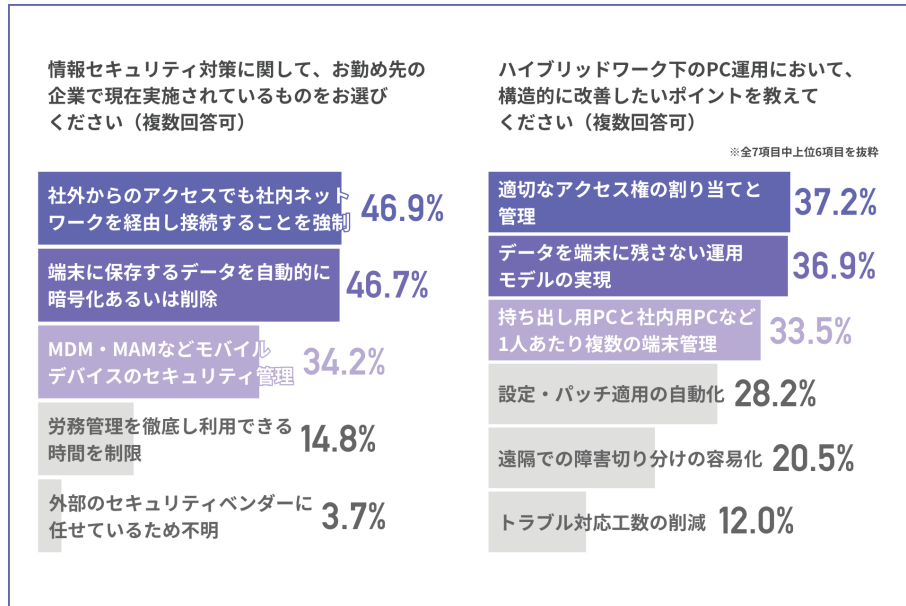
- ・ **実施している情報セキュリティ対策**

現在実施している情報セキュリティ対策としては、「社外からのアクセスでも社内ネットワークを経由し接続することを強制（46.9%）」「端末に保存するデータを自動的に暗号化あるいは削除（46.7%）」「MDM・MAM などモバイルデバイスのセキュリティ管理（34.2%）」が上位となりました。一定の対策は進んでいるものの、運用負荷との両立が課題となっている可能性があります。（図表 5）

- ・ **構造的に改善したい PC 運用のポイント**

ハイブリッドワーク下の PC 運用において改善したいポイントとしては、「適切なアクセス権の割り当てと管理（37.2%）」「データを端末に残さない運用モデルの実現（36.9%）」「持ち出し用 PC と社内用 PC など 1 人あたり複数の端末管理（33.5%）」が挙げられました。部分的な対応ではなく、運用構造そのものの見直しを求める声が多い結果となりました。（図表 5）

【図表 5：お勤め先で現在実施している情報セキュリティ対策と
ハイブリッドワーク下の PC 運用で構造的に改善したいポイント】



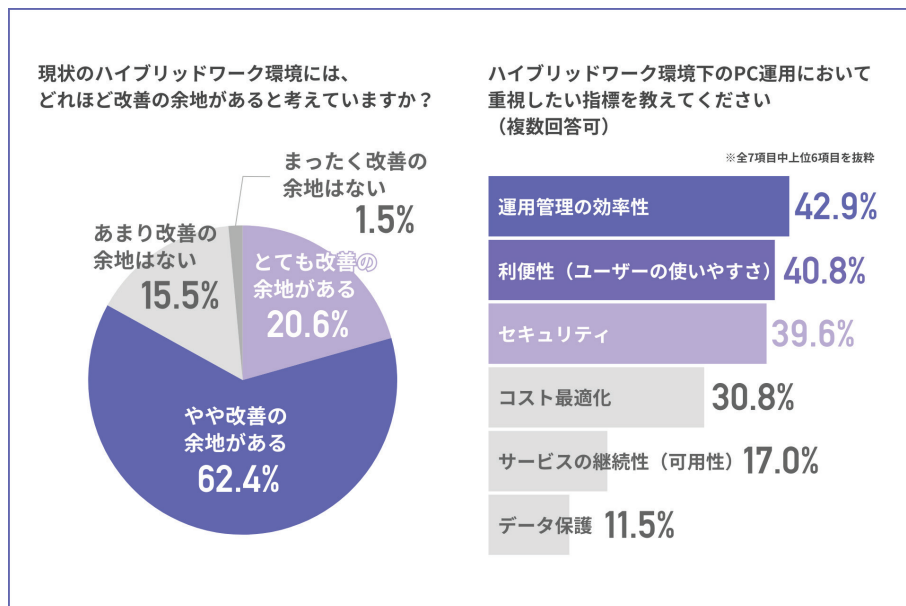
・ 現状のハイブリッドワーク環境に対する改善余地

現状のハイブリッドワーク環境については、「とても改善の余地がある（20.6%）」「やや改善の余地がある（62.4%）」と、8割以上が改善の必要性を感じていると回答しました。（図表 6）

・ PC 運用において重視したい指標

ハイブリッドワーク環境下の PC 運用において重視したい指標では、「運用管理の効率性（42.9%）」「利便性（ユーザーの使いやすさ）（40.8%）」「セキュリティ（39.6%）」が上位に並びました。効率性・利便性・安全性を同時に満たす PC 運用が求められています。（図表 6）

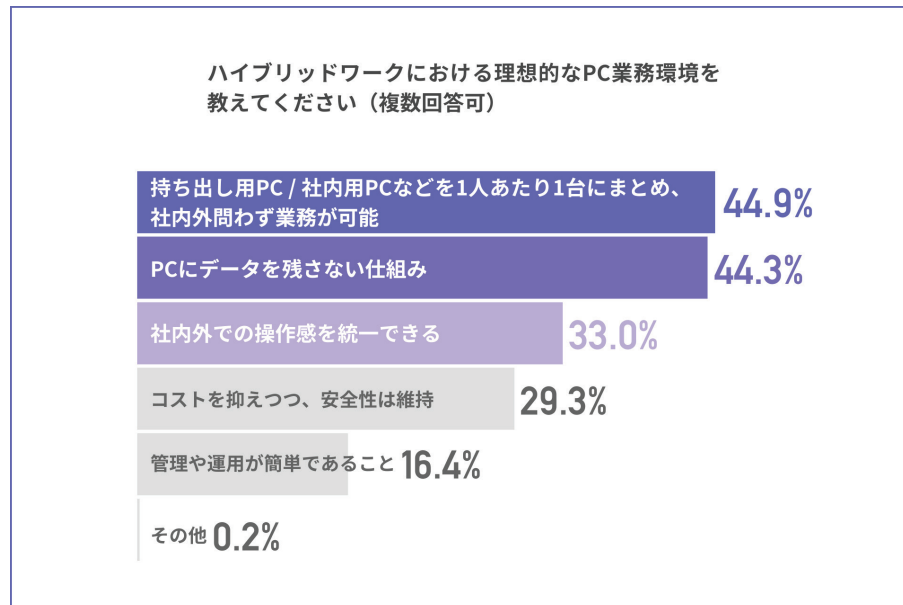
【図表 6：現状のハイブリッドワーク環境への改善の余地と PC 運用において重視したい指標】



・ 理想的な PC 業務環境

ハイブリッドワークにおける理想的な PC 業務環境としては、「持ち出し用 PC/社内用 PC などを 1 人あたり 1 台にまとめ、社内外問わず業務が可能（44.9%）」「PC にデータを残さない仕組み（44.3%）」「社内外での操作感を統一できる（33.0%）」といった回答が多く見られました。利用環境や端末の違いを意識せずに業務を行えることに加え、情報漏洩リスクを抑えつつ運用を簡素化できる、構造的に整理された PC 業務環境が求められていることがうかがえます。（図表 7）

【図表 7：ハイブリッドワークにおける理想的な PC 業務環境】



■ 総論：安全性と管理性の両立が求められる、ハイブリッドワーク時代の PC 運用環境

今回の調査結果から、ハイブリッドワークの普及により PC 業務環境は柔軟性を増す一方で、情報システム部門における運用・管理負荷やセキュリティリスクへの対応が大きな課題となっている実態が明らかになりました。

部分的な対策にとどまらず、PC 運用やリモート接続の在り方を構造的に見直すことが、今後のハイブリッドワーク環境の安定運用において重要になると考えられます。

なお、本調査の詳細をまとめたレポートは、弊社製品サイトよりダウンロードいただけます。

調査レポートダウンロード：https://engage.cachatto.jp/wp12_cachatto

調査名： 「ハイブリッドワークにおける PC 業務環境の利用や課題」に関する調査
実施期間： 2025 年 12 月 18 日（木）～12 月 19 日（金）
調査方法： PRIZMA によるインターネット調査
対象： 中堅～大企業の情報システム担当者・責任者
回答数： 1,014 件
調査主体： e-Jan ネットワークス株式会社
モニター提供元： PRIZMA リサーチ

■業務データを端末に残さない「セキュアコンテナ AD」

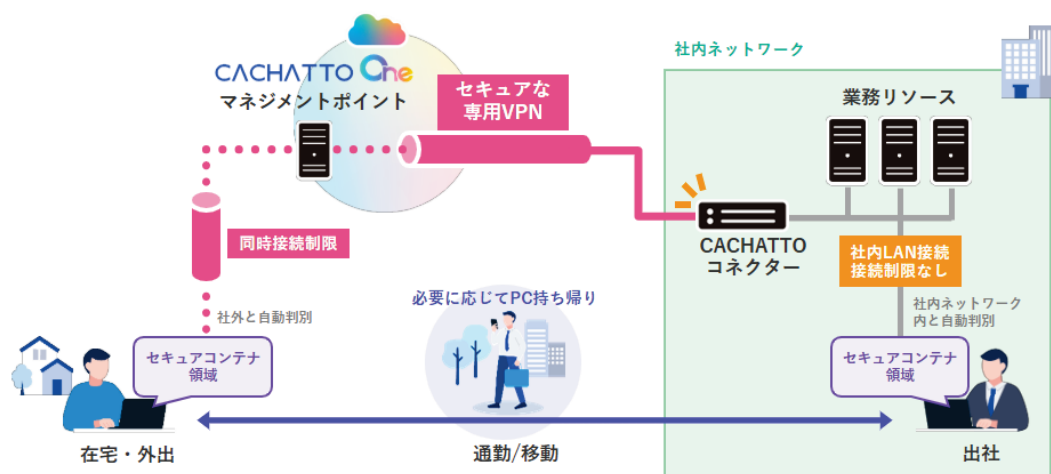
今回の調査を行った e-Jan ネットワークス株式会社が提供する「セキュアコンテナ AD」は、業務データを端末に残さず、安全な PC 業務環境を実現するデータレスクライアントです。ハイブリッドワークの普及により、「端末紛失・盗難時の情報漏洩リスク」や「社内外で PC を利用することによる管理・運用負荷」は、多くの企業に共通する課題となっています。

セキュアコンテナ AD では、PC 起動時にセキュアコンテナ領域が自動的に起動し、ユーザーはセキュアコンテナ専用の PC 環境で業務を開始します。業務データやアプリケーションはすべてセキュアコンテナ領域内で管理され、業務終了時には領域内のデータが削除されるため、端末に情報が残りません。

また、Active Directory のドメインアカウントを利用し、既存のグループポリシーをそのまま適用できるため、従来の社内 PC と同様の管理・運用を維持したまま導入が可能です。

さらに、セキュアコンテナ領域からのみ利用可能な専用のセキュアな VPN 接続を通じて、クラウドサービスやオンプレミス環境へ安全にアクセスでき、社内外を問わず同一の PC 業務環境を提供します。これにより、情報システム部門は高いセキュリティ水準を保ちながら、運用負荷を抑えたハイブリッドワーク環境の構築が可能となり、利便性と安全性の両立を実現します。

【システム構成イメージ】



製品サイト： <https://www.cachatto.jp/cscad/>

■CACHATTO について

「端末にデータを残さない」という特長により、テレワークにおけるセキュリティリスクを最小限に抑えられることが決め手となり、金融業界や自治体・官公庁など様々な業種で採用されている法人向けリモートアクセスサービスです。「スマートデバイス用リモートアクセスツール」市場および「セキュア・ゲートウェイ／ブラウザ」市場において 12 年連続トップシェアを占めています。[累計販売実績：国内 1,800 社 85 万ユーザー超（2025 年 11 月現在）]

製品サイト： <https://www.cachatto.jp/>

■e-Jan ネットワークス株式会社について

e-Jan ネットワークス株式会社は、2000 年 3 月に設立以来、「いつでも、どこでも、安全に」を理念に掲げ、ハイブリッドワークプラットフォーム「CACHATTO One」および関連製品の企画・開発・販売・運営を中心として事業を展開しています。

リモートアクセスおよび端末セキュリティ分野における長年の知見を活かし、企業の安全で柔軟な働き方を支援しています。

代表者名： 代表取締役 坂本史郎

従業員数： 111 名（2025 年 4 月 1 日現在、パートタイム従業員含む）

URL： <https://www.e-jan.co.jp/>

※ CACHATTO は、e-Jan ネットワークス株式会社の登録商標です。

※ 本リリースに記載されている会社名および製品名は、各社の商標または登録商標です。