



# 分散した IT リソースの効率的運用とは？

## セキュアでコスト削減にも効く究極のリモート管理

## 概要

企業にとって、支店やリモートオフィスの増加は成長を示す良い兆候ですが、IT 部門にとっては難しい課題となりがちです。データセンタの管理に加え、ルーター、スイッチ、ファイアウォール、WAN オプティマイザ、およびサーバといった支店の IT 資産の管理や保守も重圧となります。リモートオフィスで働く一般の従業員は、そのほとんどが問題を解決するほどの IT スキルを有していません。こうした課題を克服するため、多くの IT 部門はリモートアクセスソフトウェアを使用して支店で生じた問題を診断し、対応しています。しかしこれらのツールは、OS やネットワークが機能している時しか役に立ちません。ネットワークや OS がダウンしていると、現場の従業員をサーバの前に行かせ、問題に対処させることもあります。それでも解決しない場合は、出張、修理時間、ビジネスの停止に伴う追加費用が発生します。

このホワイトペーパーは、支店向けのアウトオブバンド（帯域外）アクセスツールや制御ツールの付加価値について、アップタイムやセキュリティの観点から明らかにします。

## 支店の課題

調査会社のインターネットリサーチグループによると、本社との直接のコミュニケーション機能を有する支店は、米国だけでも 150 万箇所があると推定されています。この数には、キオスクや ATM などセルフサービス型の施設は含まれていません。

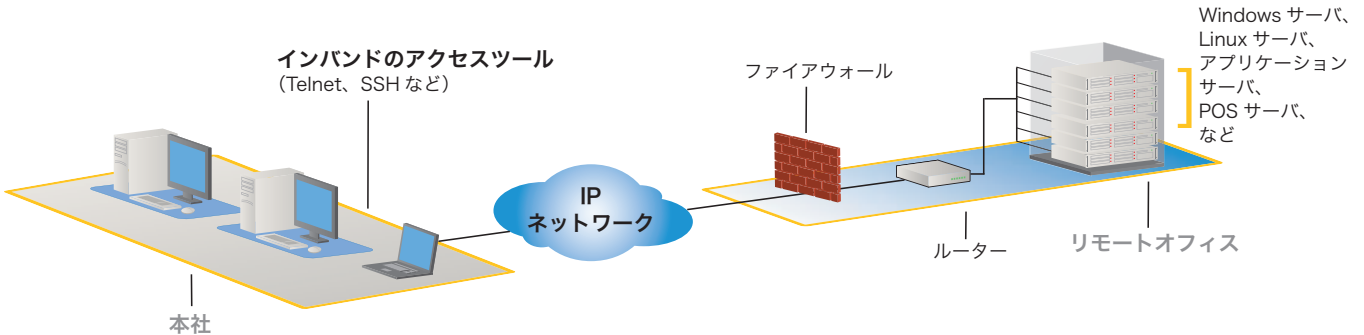
支店を展開することでビジネスの勢力範囲は広がりますが、一方で、さまざまな場所での IT 設備の設置、監視、保守を担当する IT 管理者の負担も大きくなっています。これらの設備には、ルーター、スイッチ、WAN オプティマイザ、ファイアウォールといったネットワーク機器や、トランザクション、電子メール用の分散アプリケーションやストレージサーバが含まれることもあります。

リモートオフィスの管理に伴う課題は、下記のカテゴリに分類できます。

**管理と複雑性：**支店ネットワークは、デバイスの種類やメーカーにより多種多様なコンポーネントが混在しています。このようにネットワークが複雑になればなるほど、不具合や修理方法についての懸念も増大します。また、数え切れないほどの IT 資産が世界中に分散する中で、これらのデバイスを管理するための集中型ダッシュボードの確保が重要な課題となっています。

**セキュリティ：**多くの支店、特に小売店舗や銀行の場合、機密性の高い顧客情報やクレジットカードのデータなどを抱えており、適切な予防対策を施さなければ攻撃に対して脆弱になります。また支店における Wi-Fi の普及も、こうしたセキュリティ上の懸念を一層強める要因となっています。

**限られた予算やリソース：**通常、支店は IT 専門のスタッフを擁していません。このような状況では、本社の IT 管理者がネットワークやサーバの問題を診断し、修正しなければなりません。時には現場まで出張して問題解決を図ることもあり、これに伴う出張コストが増えるだけでなく、平均修復時間（MTTR）も増大します。もう 1 つの選択肢として、現場にサービスプロバイダを派遣する方法もありますが、これも費用がかかります。しかし、問題が深刻で直ちに修正する必要がある場合は、このような出張は選択肢とならないでしょう。支店やリモートオフィスの IT システムにログインし、問題を解決するリモートアクセスツールこそが、理想的な方法となります。ほとんどのリモートアクセスソリューションは、インバンド（帯域内）とアウトオブバンド（帯域外）という 2 つのカテゴリに分けられます。



## インバンドのアクセスオプション

**リモート管理ソフトウェア：**このタイプのソリューションを使用すると、IT 管理者は対象サーバ上で実行されているデスクトップやアプリケーションにアクセスできます。リモート管理ソフトウェアの大きな欠点は、対象 OS が利用可能である必要があるという点です。OS がフリーズしていたりクラッシュしていたりすると、サーバにアクセスできません。さらに、これらのソフトウェアソリューションは、対象サーバのネットワークインタフェースカードへの接続に依存しています。したがってネットワークが利用不可である場合、これもまた問題解決を困難にする要因となります。

表 1 は、リモートアクセスソフトウェアと、KVM-over-IP といったアウトオブバンドオプションとの間の違いを示しています。

|                          | インバンド          | アウトオブバンド    |
|--------------------------|----------------|-------------|
|                          | リモートアクセスソフトウェア | KVM-over-IP |
| サーバへのリモートアクセス            | ✓              | ✓           |
| BIOS レベルのアクセス            | ✗              | ✓           |
| ネットワークが利用不可である場合のモデムアクセス | ✗              | ✓           |
| ユーザプロファイル、ポートレベルのアクセス許可  | ✗              | ✓           |
| 複数ユーザ、同時セッションへの対応        | ✗              | ✓           |
| ウォームリブート                 | ✓              | ✓           |
| コールドリブート                 | ✗              | ✓*          |
| ログ                       | ✗              | ✓           |

\* リモート電源管理ツールと併用する場合

表 1

**端末エミュレーションプロトコル：**ルーター、スイッチ、ファイアウォール、インテリジェント電源タップ PDU、およびサーバといったシリアルポート付きのデバイスへのアクセスとその構成には、Telnet や、その暗号化バージョンである SSH が使用されます。リモート管理ソフトウェアと同様、このアクセス方法はネットワーク接続が可能なおきのみ有効です。従って、WAN に問題がある場合、IT プロフェッショナルが現場に出向き、修理を要する場合があります。加えて、これらのメンテナンス用インタフェースにより、支店がネットワーク攻撃に対してより脆弱になる恐れもあります。なぜならハッカーがこれらと同じインタフェースを使用して、データを盗んだりウィルスで攻撃したりする場合がありますからです。

表 2 は、セキュアコンソールサーバのようなアウトオブバンドのアクセスが持つセキュリティ上の優位性を示します。

|                     | インバンド  |     | アウトオブバンド     |
|---------------------|--------|-----|--------------|
|                     | Telnet | SSH | セキュアコンソールサーバ |
| セキュアアプライアンス         | ✗      | ✗   | ✓            |
| ネットワーク利用不可時のモデムアクセス | ✗      | ✗   | ✓            |
| 暗号化                 | ✗      | ✓   | ✓            |
| TCP ポートのカスタマイズ      | ✗      | ✗   | ✓            |
| 強力なパスワード            | ✗      | ✗   | ✓            |
| パスワードリトライロックアウト     | ✗      | ✗   | ✓            |
| Syslog              | ✓      | ✓   | ✓            |
| キーストロークログ           | ✗      | ✗   | ✓            |
| セキュリティログインバナー       | ✗      | ✗   | ✓            |

表 2

## アウトオブバンドのアクセスオプション

**シリアルコンソールサーバ：**ほとんどの支店の IT 配備に共通する特徴はネットワーク接続で、通常、ルーター、スイッチ、ファイアウォールを必要とします。リモートオフィスでこれらのコンポーネントが故障すると、業務運営に支障が出ます。ほとんどのネットワーク機器はシリアルインタフェースを持ち、前述のとおり、SSH や Telnet といったインバンドツールが、遠隔から機器にアクセスし保守する手法として一般的に用いられています。しかし、ネットワークに問題が発生すると、これらのアクセスツールは役に立たなくなる可能性があります。一方、シリアルコンソールサーバ（SCS）は、SSH/Telnet または Web ブラウザを介して、シリアル運用される複数のサーバやシリアルデバイスへのリモートアクセスを提供します。SCS の利点の 1 つは、シリアル運用される複数のサーバ、WAN 機器、ネットワーク機器、電力制御装置に一箇所からアクセスし、制御できる点です。その他の利点としては、WAN が利用不可であるときにモデムアクセスが可能であることが挙げられます。これにより、現場に出向く必要はなくなり、修理時間が短縮されます。

コンソールサーバを選択する時は、下記を考慮する必要があります。

▶ 権限と認証

- ▷ ローカルアカウント
- ▷ ポートレベルのアクセス
- ▷ 強力なパスワード
- ▷ Active Directory、LDAP、RADIUS、TACACS+ への対応

▶ コンソールの機能

- ▷ ログ
- ▷ SNMP トラップ
- ▷ Solaris キートラップ
- ▷ アクセスの共有（または）アクセスのシェア

▶ 管理機能

- ▷ 電子メールアラート
- ▷ SNMP 対応

▶ アクセス手法

- ▷ SSH
- ▷ Telnet
- ▷ Web インタフェース
- ▷ ダイアルインオプション

▶ 設備管理

- ▷ デュアル配電
- ▷ 電源管理
- ▷ CAT5 ケーブル

---

「以前、私たちはある失敗をしたため、ファイアウォールがロックアップして、ネットワークを通じた接続ができなくなったことがありました。結局その時は現場に人を派遣して、サーバを操作し、再起動させました。あの時にDominion<sup>®</sup> SXを使えたなら、問題は5分もあれば解決したはずです。あの出来事がきっかけで、当社はラリタンのセキュアシリアルコンソールサーバをITインフラ管理に導入することを決心したのです。」

ケビン・バーン

チャーター・コミュニケーションズ社  
ネットワーク・オペレーションズ・エンジニア

---

**KVM-over-IP:**KVM スイッチを使用すると、キーボード、ビデオ、マウスインタフェースを持つサーバにアクセスし、制御できます。KVM スイッチは、データセンタ内でサーバに直接アクセスしているかのような使用感をもたらします。

KVM-over-IP スイッチにもそうした使用感がありますが、セキュア IP 接続を介するという点が異なります。どこからでもサーバにアクセスできることが KVM-over-IP の最大のメリットであり、リモートオフィスサーバへのアクセスと制御の手段として理想的です。IT 管理者が本社にしようと、吹雪の午前 2 時に自宅にしようと、支店の IT 設備にアクセスできるのです。

さらに、KVM-over-IP スイッチは、インバンドとアウトオブバンドのアクセスの両方を提供します。すなわち、IT スタッフは OS/ アプリケーションレベルまたは、OS が反応しない場合は BIOS レベルでサーバにアクセスし、制御できます。さらに、KVM-over-IP スイッチにはモデムが統合されており、ネットワークの故障の際にはさらに別のアクセス手法を選択できることも安心につながります。

また仮想メディアといった付加価値機能により、デスクトップ、CD-ROM、USB スティックから世界中のサーバにファイルを伝送できます。これは、多数のリモートロケーションにアップグレードやパッチプログラムをインストールする必要がある場合に理想的なツールです。

『KVM-over-IP 購入者ガイド』は、スイッチを選択する際の検討事項として下記を挙げています。

▶ **いつでもどこからでもリソースにアクセス可能**

- ▷ マルチプラットフォームへの対応
- ▷ ブラウザまたはデスクトップとの互換性
- ▷ IP とモデムの両方でアクセス
- ▷ 費用のかからない、ダウンロード可能なクライアント
- ▷ ローカルポートを介したノンブロックアクセス
- ▷ リモート電源制御
- ▷ 仮想メディアによるアクセス

▶ **セキュリティとパフォーマンスのレベル**

- ▷ 脆弱性の最小化
- ▷ 外部および内部のアクセス制御
- ▷ Syslog への対応
- ▷ データの暗号化
- ▷ 強力なパスワードへの対応

▶ **アプライアンスペースのソリューション**

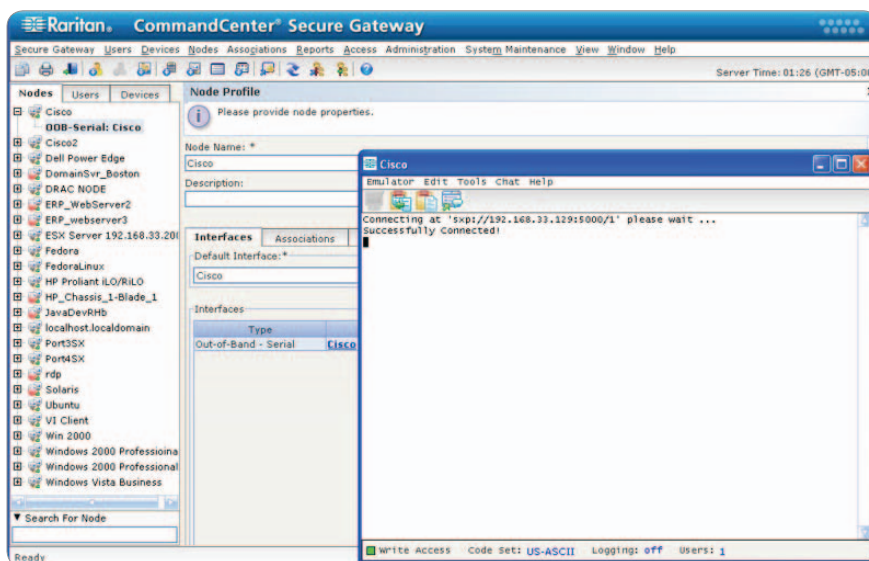
- ▷ 導入のしやすさ
- ▷ サイズとポート密度
- ▷ 信頼性とアップタイム

**インテリジェント電源タップ (PDU)：**問題解決の最後の手段として、コールドリブートが必要になる場合があります。スイッチ型の PDU は通常、リモート電源サイクルに関連付けられますが、電力モニタリングといったインテリジェントな機能を持つ PDU もあります。支店において、IT 機器が小部屋にまとめられている場合、環境的な要素や電力の使用率がユーザ定義のしきい値を越えたときにその旨を知らせる機能があることが重要です。例えば、小さなオフィス内の電気室は換気と冷却が悪くなりがちで、たった 1 つの電気回路でも他の機器と共有していることがあります。室内の温度と IT 機器の電気の流れを監視すれば、ネットワークの停止や機器の損傷を防止できます。

リモート電力監視ソリューションを選択する時は、下記の機能を考慮に入れる必要があります。

- ▶ コンセントレベルスイッチへの、リモートからのシリアルおよび TCP/IP アクセス
- ▶ ユーザによる設定が可能な、コンセントレベルでの電源シーケンスの遅延設定機能
- ▶ ユニットレベルおよびコンセントレベルでの電力監視と使用状況についての情報
- ▶ ユーザ定義のしきい値
- ▶ しきい値を越えた場合に機能する、SNMP、電子メール、および Syslog を介したアラート
- ▶ 最大 256 ビットの AES 暗号化およびストロングパスワードへの対応
- ▶ コンセントレベルの権限、LDAP/S、RADIUS および Active Directory® を含む、高度な認証オプションや認可オプション
- ▶ HTTP、HTTPS、IPMI、SMASH-CLP、SSH、Telnet、SNMP への対応

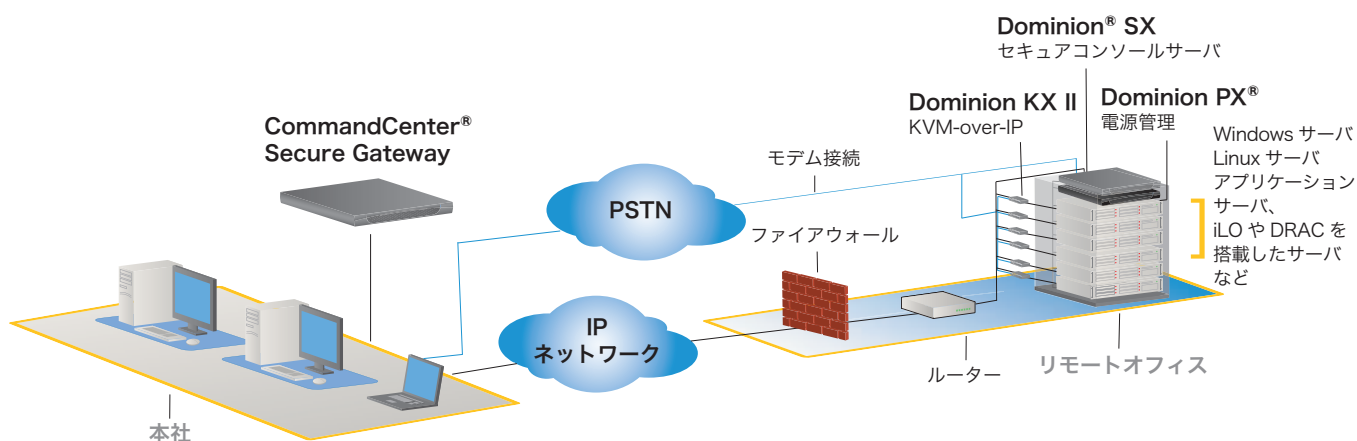
**集中管理：**何十、何百、何千以上といった多くの拠点を管理することは、煩雑な仕事です。KVM-over-IP、シリアルコンソールサーバ、組込み型サービスプロセッサ (iLO、DRAC、RSA)、インテリジェント PDU を用いて遠隔からの問題解決に対応するにしても、これらの多様な設備のすべてを統合された画面で追跡することが不可欠です。つまり、広範な種類のデバイスと、高度なセキュリティ機能や認証機能に対応できる集中型管理ソリューションの導入を検討する必要があります。



IT デバイスへの集中アクセスと管理を可能にする CommandCenter® Secure Gateway のサンプル画面

## 結論

物事を円滑に進めるためには、各支店に IT プロフェッショナルを常駐させることが一番良い方法ですが、このような贅沢ができる企業はわずかです。次に良い方法は、本社にいる IT スタッフがリモートオフィスの機器を操作できるような、適切なツールを用意することです。現在、無料またはわずかな費用で利用可能なツールもいくつかありますが、実際には可用性やセキュリティに払う犠牲という意味で、コストがかかります。結果として予期せぬ出張費用やダウンタイムが生じてしまいますが、こうした費用を回避しようというのがリモートアクセスソリューションの目的です。インバンドのアクセスツールでは対応できない部分を、アウトオブバンドのソリューションがカバーしてくれます。リモートオフィスネットワークの管理と維持に役立つラリタンのソリューションの詳細については、[raritan.co.jp/remote-office-management](http://raritan.co.jp/remote-office-management) を参照してください。



## ラリタンについて

ラリタンは、あらゆる規模のデータセンタに適した電源管理、インフラ管理、KVM、シリアルソリューションで豊富な実績を誇るリーディングサプライヤーです。インテリジェントラック PDU、電力管理ソフトウェア、DCIM ソフトウェアソリューションなど、ラリタンのハードウェアおよびソフトウェア製品は世界 5 万箇所以上の施設で使われており、データセンタの容量管理、アセット管理、および変更管理の効率化に貢献しています。ラリタンは、IT 管理者や施設管理者に向けて、KVM-over-IP および Serial-over-IP アクセス製品など、電力管理の効率性向上、データセンタの生産性強化、遠隔拠点の IT 運用の改善に必要なソリューションを提供しています。米ニュージャージー州サマセットに本社を置くラリタンは、世界各地にオフィスを有し、76 カ国に製品を供給しています。詳しくは、[raritan.co.jp](http://raritan.co.jp) をご覧ください。