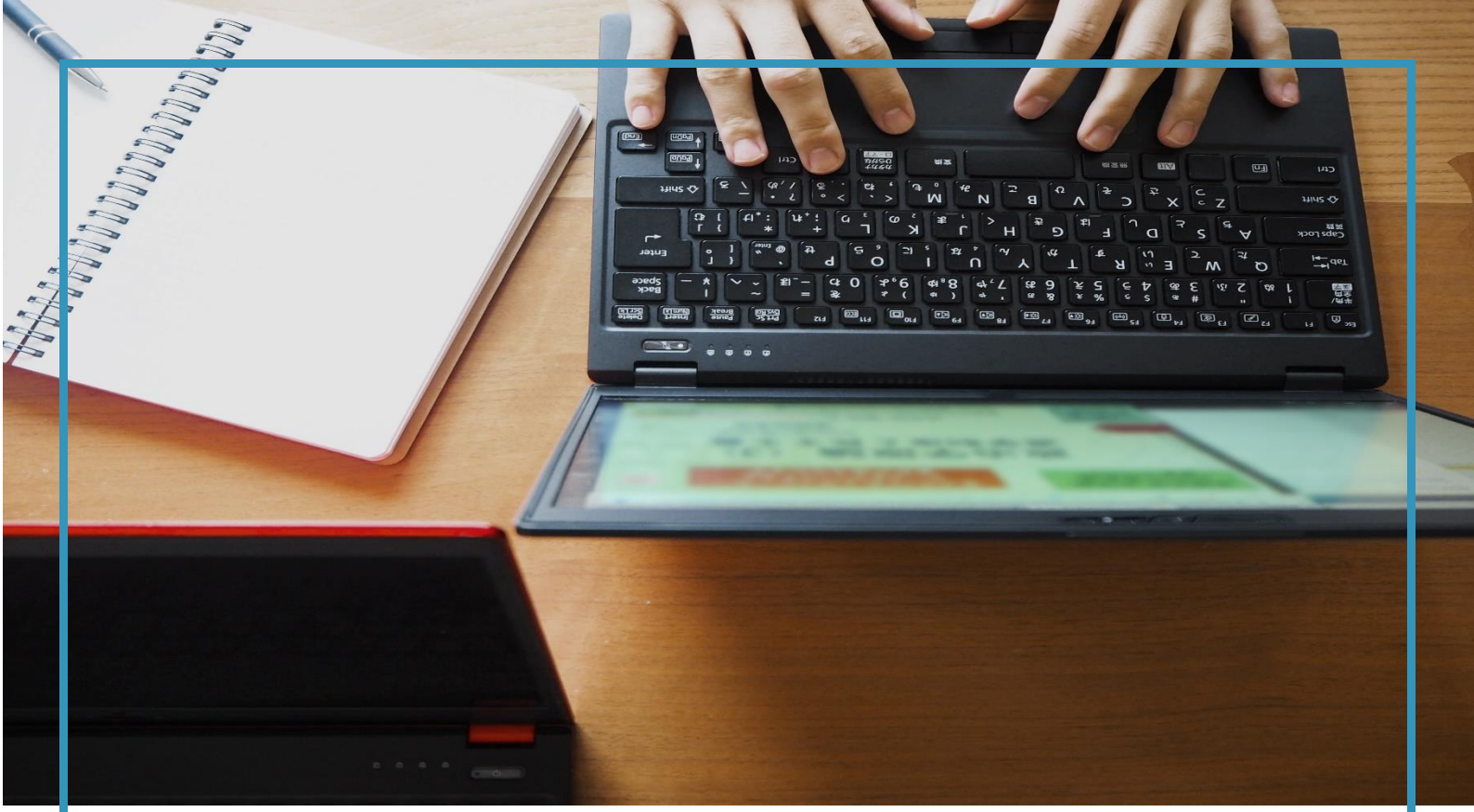


テレワーク環境下での
効率的なセキュリティパッチ管理

tdi 情報技術開発株式会社

IT 技術を駆使し、場所や時間に捕らわれない柔軟な働き方が求められる、ニューノーマル（新しい生活様式）時代となりました。決まった場所で仕事をするワークスタイルからテレワークに移行し、場所を選ばず仕事ができる環境が増えています。例えば、自宅で仕事をする在宅勤務、移動中に仕事をするモバイル勤務、企業のサテライトオフィスや一般的なコワーキングスペースです。

個人が仕事をする場所を選択できるというワークスタイルの変化に対応するため、企業は環境を整備することが求められています。

tdi では、様々なお客様のセキュリティ対策をご支援しています。様々なワークスタイルに対してより柔軟に対応するため、ニューノーマル時代にも適応したパッチ管理や IT 資産管理のご提案を行っています。これから先の時代を見据えて、今何を考え、何をすれば良いのか、一つの選択肢として、運用管理者の方々のご参考となれば幸いです。

目次

1. IT 資産管理ツールによるセキュリティパッチの運用管理

セキュリティパッチの運用管理方法は企業によって様々です。セキュリティパッチ公開後、PC の利用者に任せて適用を実施している企業もあれば、運用管理者が管理、統制している企業もあります。運用管理者が管理する場合、IT 資産管理ツールを利用して、各 PC にセキュリティパッチの配布・適用を行います。 IT 資産管理ツールはインベントリ収集による IT 資産の把握機能だけでなく、統合的なセキュリティ管理ツールとしての機能も実装していることが一般的です。

運用管理者がセキュリティパッチの適用を管理するメリットは、運用管理者によって検証された安全なセキュリティパッチが適用できることや、PC がセキュリティポリシーに準拠しているかを把握できることなどが挙げられます。

セキュリティパッチの適用が業務アプリケーションなどに影響を及ぼさないことを運用管理者が事前に確認した上で、保有している PC に最新のセキュリティパッチを適用します。

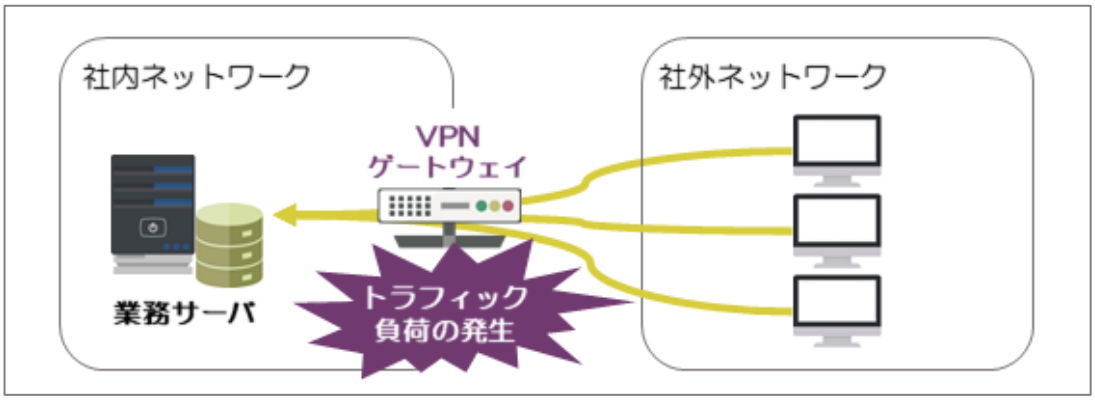
2. テレワークの現状と普及による課題

厚生労働省の調査結果[1]では、テレワーク（在宅勤務）は企業規模の大きさに比例して導入率が高くなっています。従業員数が 1,000 人以上の企業では 70%以上がテレワークを実施しているという結果となっており、今後も新型コロナウイルス流行時よりも利用を拡大したい、または新型コロナウイルス流行時と同程度に維持したいと全体の 60%以上が示しています。テレワークは、私たちの新しい働き方の選択肢の一つとして定着しつつあります。

しかし、テレワーク環境下においても同様に実施しなければいけない、セキュリティパッチ管理の運用において、いくつかの課題が浮き彫りになってきました。ネットワークなどの環境に起因する問題、製品機能に起因する問題、IT リテラシーなどのユーザに起因する問題などです。特に環境に起因する課題の中で、「ネットワークトラフィックの逼迫にどのように対処すべきか悩んでいる」との声をよく耳にします。テレワークの導入により社外で利用する PC が急激に増加しました。社外の PC に対して従来通りの設定で大容量のセキュリティパッチを配信すると、社内ネットワークと社外を隔てるゲートウェイ機器に対してアクセスが集中します。結果として、ネットワークトラフィックが逼迫し、業務ネットワークに著しい影響を及ぼしかねません。

---

[1] 第４回「これからのテレワークでの働き方に関する検討会」資料
https://www.mhlw.go.jp/stf/newpage_14849.html



3. テレワーク環境下でのネットワーク負荷への対応

テレワークによるネットワーク負荷の課題を回避するため、セキュリティパッチの適用スケジュールを変更している企業も見られます。例えば、今まで PC100 台に一斉にパッチを適用していた運用を、25 台ずつ 4 回に分けてパッチを適用するようスケジュール変更することでネットワーク負荷を分散させます。他にもインターネットの使用頻度が低い PC は社内に戻ったタイミングでパッチを適用するなど様々な工夫をしています。

運用管理者はネットワークトラフィックの逼迫により業務が滞らないように、また何より PC がセキュリティリスクに晒されないために、適切なセキュリティパッチ管理の運用が求められます。これまで運用管理者の頭を悩ませていたセキュリティパッチ管理の運用が、テレワークにより細分化が必要となり、従来の運用を見直す必要が出てくるなど、運用管理者への負担がさらに増加しています。

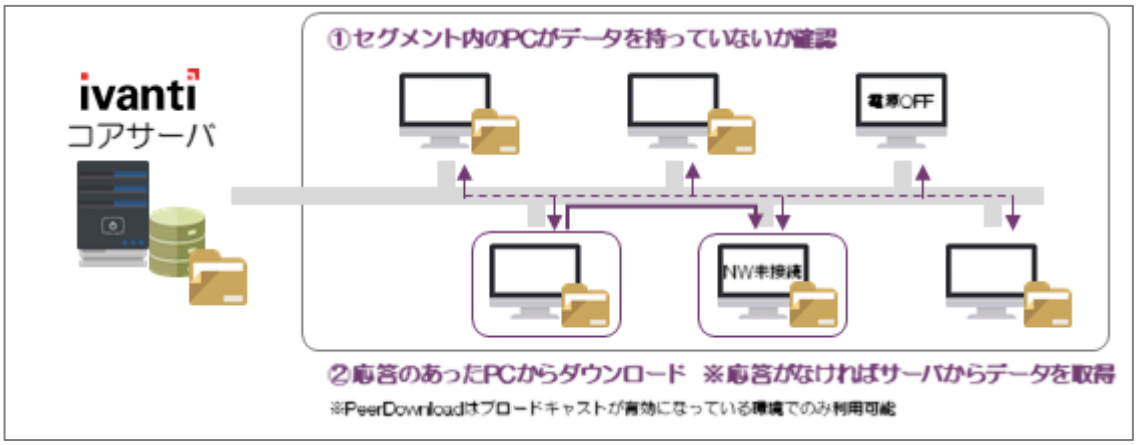
4. Ivanti でのセキュリティパッチ管理

IT 資産管理ツール「Ivanti」では、PC の台数やネットワーク環境などにあわせ、効率的にセキュリティパッチの管理・運用ができます。

Ivanti では、運用管理者からそれぞれの PC にセキュリティパッチを配信するだけではなく、PC に「ポリシー」（適用ルール）を持たせてセキュリティパッチを PC から取得させることもできます。各 PC は登録されている「ポリシー」に準拠するタイミングで、セキュリティパッチの配信を管理する Ivanti コアサーバへ問合せを行います。適用するセキュリティパッチが存在する場合は、コアサーバからセキュリティパッチ取得先の指示を受け、その取得先からダウンロードを行い、パッチを適用します。

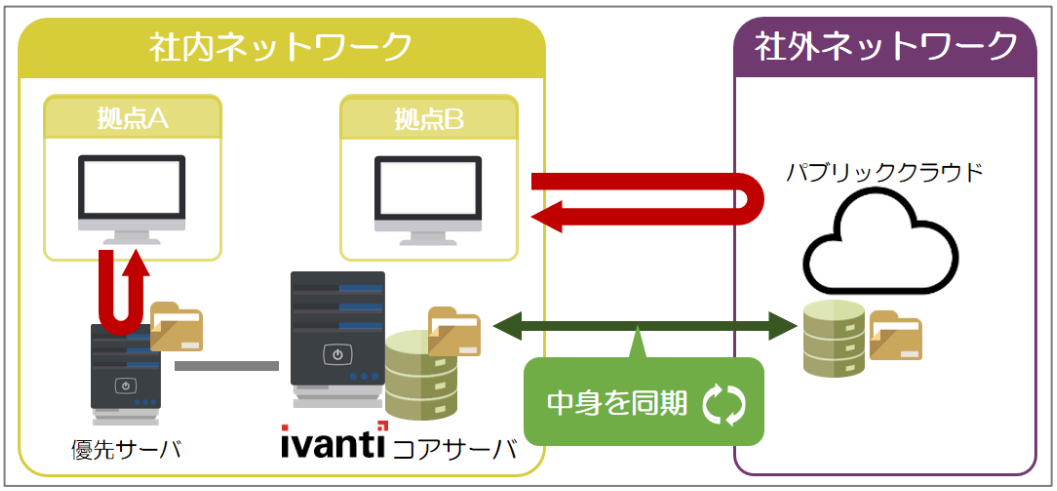
IT 資産管理ツールを利用する企業の多くは多数の PC を保有しており、ネットワーク負荷の影響を考慮した運用設計が必要になります。tdi でも数千、数万台を超える大規模な PC 運用環境下で、ネットワーク負荷の課題を抱えたお客様からご相談を受け、解決した事例が数多くあります。

Ivanti には、Ivanti コアサーバから直接ファイルを取得するのではなく、クライアント PC 同士がファイルを直接転送しあう「ピアダウンロード」という優れた配信テクノロジーが搭載されています。ピアダウンロードは、同一セグメントにセキュリティパッチのデータを持っている PC が存在すれば、その PC からセキュリティパッチをダウンロードできる技術です。そのため、拠点間を結ぶ WAN に負荷をかけずネットワーク帯域に配慮した配信ができます。



その他にもそれぞれの PC が持つ「ポリシー」ごとに、優先的にセキュリティパッチ取得先を指定できる「優先サーバ」という機能があります。PC の保有台数が多い企業では、拠点やネットワークのセグメントごとに複数のセキュリティパッチ取得先を用意することで、ネットワークの負荷分散ができます。

セキュリティパッチ取得先は、社内にあるサーバを参照することが一般的ですが、Ivanti であれば社外ネットワークサーバ（パブリッククラウド）上にも取得先を設定できます。社外ネットワークにセキュリティパッチの取得先を分散させることで、社内のネットワークトラフィックを最小限にできます。

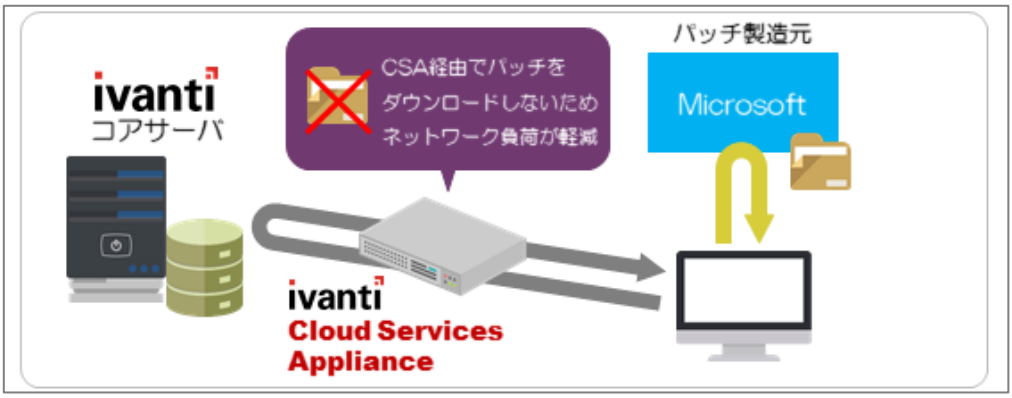


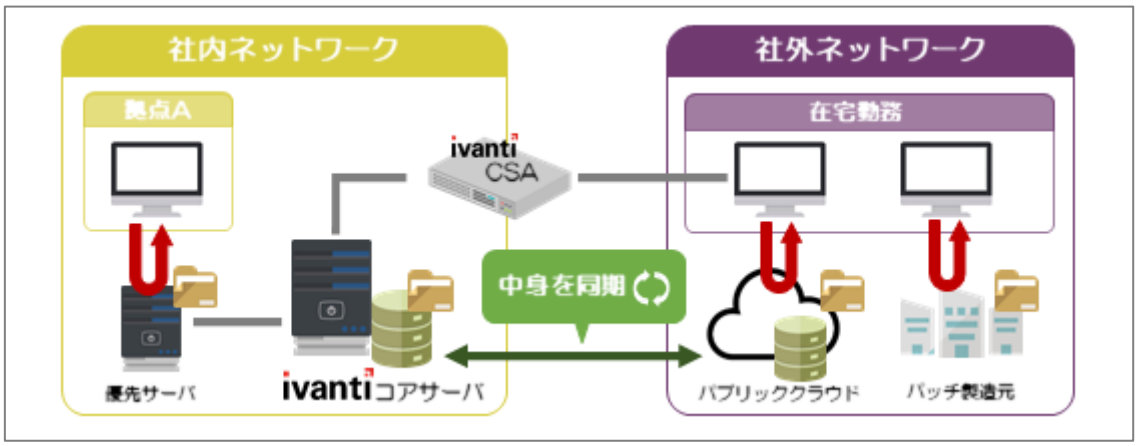
5. Ivanti でのセキュリティパッチの円滑な適用方法

Ivanti Cloud Services Appliance(以下、CSA)は、VPN を使用せず、インターネット経由で社内ネットワークにあるコアサーバへのアクセスを実現できる製品です。CSA を利用することで、従来のセキュリティパッチ管理の運用をそのままテレワークにより社外で利用している PC に適用することができ、運用管理者の負荷を軽減できます。

CSA では従来の運用どおり、セキュリティパッチの取得先を社内ネットワーク上のサーバに指定することができます。社内のネットワーク負荷を最小限に抑えるために、優先サーバの機能を利用し、ネットワークセグメントを分けた社外サーバを指定することもできます。

加えて、CSA での構成の最大の利点として、製造元から直接セキュリティパッチをダウンロードするように指定することもできます。例えば、Windows のセキュリティパッチであれば、Microsoft 社で公開されているダウンロードサイトを取得先に指定し、セキュリティパッチをダウンロードするように指示できます。VPN を経由せずにセキュリティパッチのダウンロードができるため、パッチ取得スケジュールを分散させる必要がありません。





他にも、社外にある PC に対して、従来通りのセキュリティパッチ適用タイミングを維持しながらセキュリティ対策を行う方法はいくつかあります。例えば、SD-WAN の仕組みなどを用いてローカルブレークアウトを行い、セキュリティパッチを取得する経路を分散させる方法。また、VPN 経由で接続しているケースでは、VPN ゲートウェイ本体のスケールアップを行い、大容量のネットワークトラフィックに対処する方法も考えられます。

これらの方法と Ivanti の負荷分散テクノロジーを組み合わせ、効率的なネットワーク設計を行い、運用されている事例もあります。それぞれの企業のネットワーク環境やセキュリティポリシーにあった運用方針を検討し、選択することが肝要です。

6. 終わりに

tdi グループでは、お客様の IT 環境における様々な課題を解決する支援を数多くさせて頂いております。Ivanti においては 15 年にわたり計 30 万ライセンスの利用実績もございます。既に多くの企業で導入している IT 資産管理ツールと Ivanti で可能な運用方法を比較していただくことで、お客様の一つの選択肢として気づきになりましたら幸いです。

お困りのご担当者の方は、どうぞお気軽にお問合せください。

【tdi HP 資産管理ツール「Ivanti」】https://www.tdi.co.jp/ivanti/

【Ivanti 製品紹介資料、How to】https://www.tdi.co.jp/ivanti/material/

【お問い合わせ】https://tdi.smktg.jp/public/application/add/35

情報技術開発株式会社 **営業本部**

東京: 〒163-1332 東京都新宿区西新宿六丁目 5 番 1 号 新宿アイランドタワー32 階
TEL.03-5325-4826 (直通) FAX.03-5325-4812

中部:〒451-6027 愛知県名古屋市西区牛島町 6 番 1 号 名古屋ルーセントタワー27 階
TEL.052-571-6871(代表) FAX.052-571-3856

関西:〒530-0005 大阪府大阪市北区中之島二丁目 2 番 7 号 中之島セントラルタワー20 階
TEL.06-6201-7739(代表) FAX.06-6201-7740

九州:〒812-0013 福岡県福岡市博多区博多駅東二丁目 10 番 1 号 福岡ビル S 館 7 階
TEL.092-451-8218(代表) FAX.092-474-7379