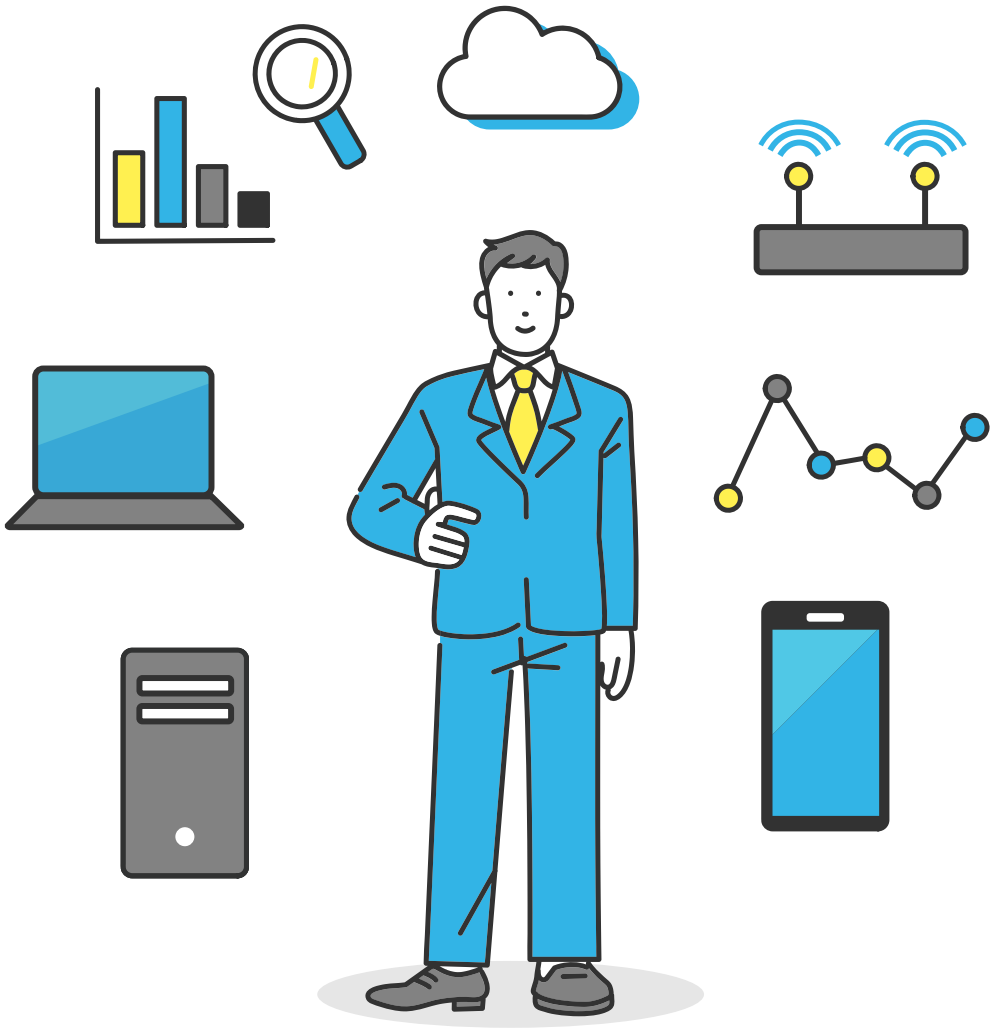
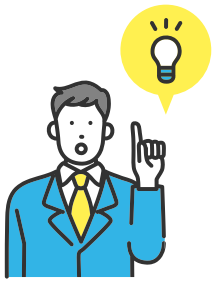
テレワーク時代の新しい運用様式

ネットワーク構築運用SIer編



ゾーホージャパン株式会社　ManageEngine

Contents



1 はじめに

COVID-19 に罹患された方々及び関係者の方々に謹んでお見舞い申し上げますとともに、一日も早いご快復を心よりお祈り致します。
日本では 5 月 25 日に緊急事態宣言が解除され、段階を経て社会活動が再開されています。しかし今回、全世界規模で COVID-19 の影響が波及したことで、パンデミックは事業継続性を脅かす重大なリスクであることを社会全体が痛感したのではないでしょうか。

地震や津波といった自然災害に対する備えと同様に、昨今ではパンデミック対策の重要性がクローズアップされてきています。そんな中注目を集めているのが**テレワーク**です。
企業におけるテレワークの導入は今後も加速していくと考えられます。

当 eBook では、テレワークの運用で情報システム部門に求められることを考えていきます。また、情報システム部門はシステムインテグレーター（SIer）とも密接に連携してテレワークを運用していくことになります。本稿ではこの SIer の視点で、テレワーク時代に求められるネットワーク運用を整理していきます。情報システム部の皆様や SIer の皆様のお役に立てましたら幸いです。

2 テレワークの状況とSIerへの影響

この章のポイント

- COVID-19 後は中小企業のテレワーク対応が加速
- これを受けて中小企業向け提案機会が増加
- 中小企業向けのテレワーク運用のガイドラインが必要

SIer は顧客である情シス担当者と連携して、テレワーク環境の導入、運用、保守を行っていくことになりますが、顧客企業のテレワーク導入状況によって、求められることが違ってきます。
まずは、企業規模によるテレワーク導入状況について見ていきましょう。

企業規模によるテレワーク導入状況について

企業規模によって、テレワークの導入状況に格差がみられます。中小企業庁のデータによると、国内の企業で働く従業員の総数4,013 万人の内、約 1,229 万人が大企業に勤めており、約 2,784 万人が中小企業に勤めております。*
また、総務省が平成 30 年に調査した結果によると、資本金

* 出典：https://www.chusho.meti.go.jp/koukai/chousa/chushoKigyouZentai9wari.pdf

5000 万円～ 1 億円未満の中小企業の、テレワーク導入率は 15.9% となっております。
一方、大企業と言われる資本金 1 億円～ 5 億円未満の企業のテレワーク導入率は 26.9% となっており、資本金 50 億以上の企業に至ってはテレワーク導入率は 53.9% となっております。*
2 つの調査結果を元に、資本金 1 億円以上を大企業と定義して試算した場合、大企業の約 480 万人、中小企業の約 360 万人がテレワーク対象となりますので、人数でも格差がみられます。
推計ですが、労働人口の約 20%にテレワークが普及していることになります。

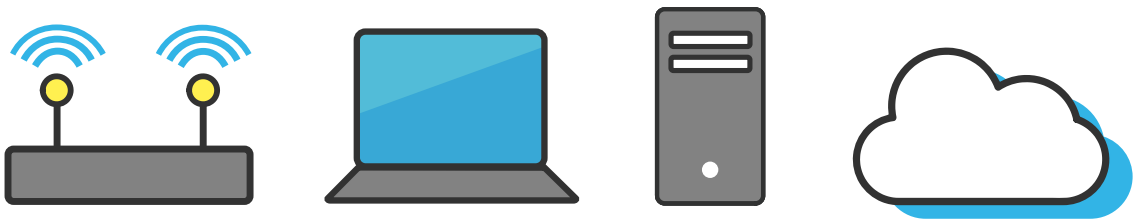
筆者の経験に基づく見解を交えて、大企業の実例をご紹介します。一部上場企業の中でも、TOPIX CORE30 のある企業では、スケールメリットを生かして、グループ企業全体でキャリアと一括契約しコストを抑え、自前の閉域網を始めとする IT インフラを構築しておりました。国内外に多数の拠点を構え、また、社会的に事業継続性を求められることも背景にあり、2015 年頃から、テレワーク環境が整備されておりました。
今般の COVID-19 の影響で、テレワーク対象者の拡大など社内規定の見直しは行われるかもしれませんが、テレワーク関連設備はすでに確立している状況です。同様に、他の大企業でも、テレワークへの設備投資のフェーズは終了していると考えられます。SIer に求められる保守運用体制は既に確立しており、大きく変わることはないでしょう。

それでは、中小企業の場合を考えてみましょう。前述の調査結果の通り、大企業に比べてテレワーク導入が進んでいませんが、COVID-19 の影響を受けて導入が加速すると推測されます。また、マーケットとしても、大企業向けより、中小企業向けのテレワーク市場が大きいといえますので、SIer 視点でいえば、今後、中小企業向けの導入提案の機会が増えると考えられます。

* 出典：https://www.soumu.go.jp/johotsusintokei/statistics/data/190531_1.pdf

もちろん、製造系や飲食サービス系などの、設備や場所に制約がある企業は、完全にテレワークに移行できない為、業種や職種によって普及率に差が出ます。
一方、オフィスワークで業務が完結する業種、職種のテレワーク化は、先の緊急事態宣言を受けて、半ば強制的に始まってしまいました。情シス担当者が、様々なクラウドサービスをパッチワークのように組み合わせて、テレワーク環境を突貫で構築して凌いでいる状況です。COVID-19 終息後は、暫定的に利用している様々なクラウドサービスが、そのまま正式採用されるケースもありますが、部署や部門によってバラバラなので、一本化のための整理、シャドー IT の把握と正式化などの導入検討が行われる事になります。

SIer としては、運用保守やセキュリティ面から、テレワーク環境のあるべき姿の提案が求められます。この先懸念される、COVID-19 の再流行に備えて、遅くとも 2020 年内には、サービス選定と導入検討を終わらせるべきだと考えます。したがって SIer は、早急に**中小企業の情シス担当者向けに、テレワーク導入と運用のガイドラインをまとめ、提案する必要がある**でしょう。



3 テレワークを導入する 3 ステップ

この章のポイント

- IT インフラのテレワーク化には「導入開始」「混在」「導入完了」の 3 ステップがある
- VPN・クラウドインフラ・クラウドサービスの活用が鍵

前節では、大企業と、中小企業のテレワーク導入状況について述べました。大企業のテレワークの保守運用体制は確立していますので、ここからは、中小企業向けのテレワーク導入と運用について考えていきたいと思います。

IT インフラのテレワーク対応は、ステップを踏んで進んでいきます。業種業態によって、完全にテレワークには移行できない業務もあるので、一概には言えないですが、おおむね、「**導入開始**」「**混在**」「**導入完了**」の 3 つのステップがあると考えられます。
SIer と情シス担当者は、連携してステップ毎に導入と運用計画を立てる必要があります。
本節では、オンプレミスのサーバーと PC で構成されている、一般的な中小企業の情報システムを想定し、各ステップの内容と留意点を見ていきましょう。

ステップ１：導入開始

社内リソースへ外部からのアクセスを導入するステップです。具体的なソリューションとしては、社内 LAN への VPN 接続が挙げられます。

ソリューション　：インターネットVPN（SSL-VPN）
コスト　：低
既存業務影響　：小
保守のポイント　：ユーザーやトラフィックの可視化
留意点　：情報漏洩のリスク対策、運用ルールの制定

ステップ１の状態で大半のオフィスワークができるようになったとしても、セキュリティの観点からあくまでも暫定的な構成とすべきです。なぜなら、全社員に社内 LAN へのアクセス権を付与することで、確率的に情報漏洩や不正アクセスのリスクが高まるからです。したがって、VPN ユーザーアカウント管理と、トラフィックの監視は重要なので、SSL-VPN 機能を持っているファイアウォールを導入することをお勧めします。
また、PC 紛失の際は、ハードディスクからの情報漏洩に加えて、悪意のある拾得者から社内 LAN に不正侵入される危険性があります。そのため、PC 紛失時のエスカレーション先や迅速なアカウントロックなどの運用ルールや運用体制の検討も重要です。また、保守の観点でいえば、VPN 装置が単一障害点とならないように冗長化を行いたいですが、設備投資の予算とリスクはトレードオフの関係にあるので、経営層を交えて検討する必要があるでしょう。
SIer は、顧客企業の予算に合わせて SLA を選択できる複数の保守プランを用意しておくとよいでしょう。

ステップ２：混在

オンプレミス環境とクラウド環境の混在するステップです。
社員が利用するPCをVDI化し、シンクライアントで提供することで、セキュリティを強化することができます。

ソリューション	**：クラウドプラットフォーム、VDI**
コスト	**：中**
既存業務影響	**：中**
保守のポイント	**：オンプレミスとクラウドのシームレスな監視**
留意点	**：オンプレミスとクラウドのすみ分け**

情報漏洩のリスクを解決する為には、クラウド上の仮想デスクトップインフラ（VDI）環境が効果的です。シンクライアントならば、万が一PCを紛失した場合も、データが流出することはありません。今後、中小企業でも、VDIの導入が広がっていくでしょう。
しかし、クラウドプラットフォーム上のVDIから、オンプレミスのサーバーを利用する構成は、外部から社内へのアクセスが発生する為、セキュリティ上好ましくありません。技術的にレガシーで仮想化できないサーバーや、物理的な制約があるサーバーでなければ、VDIとサーバーは同一のネットワーク上に移行する事が望ましいでしょう。
このステップで、情報システムを棚卸して、オンプレミス、クラウドのすみ分けを検討します。業務フローの変更でクラウド化できるケースもあるので、バックオフィス部門の有識者を交えて検討会を開催し、次のステップへの可否を判断する事になります。

ステップ３：導入完了

社内システム全体のクラウド化になります。オンプレミスサーバーをクラウドプラットフォームに移行します。オンプレミスの制約がなくなり、テレワーク環境が完成するステップです。

ソリューション	**：P2Vマイグレーション、クラウドプラットフォーム、VDI**
コスト	**：高**
既存業務影響	**：中～高**
保守のポイント	**：オンプレミスとクラウドのシームレスな監視**
留意点	**：オンプレミスとクラウドのすみ分け**

このステップでは、SIer、情シス部門、事業部門、経営層をメンバーにしたプロジェクト化が必須になります。クラウドプラットフォームのランニングコスト、SLA を比較検討し、経営計画とすり合わせながら導入スケジュールを立てます。
単純なファイルサーバーであれば、マイグレーションに手間をかけるよりも、オンラインストレージへの切替を検討してもよいかもしれません。その場合、既存の業務フローを変更する必要があるので、SIer と情シス担当者は、業務改善のコンサルティングも念頭にしたシステム提案が必要です。
保守の観点で言えば、オンプレミスのサーバーをクラウド上の仮想環境にマイグレーションすると可用性が向上するメリットがあります。しかし、混在から導入完了までは、情報システムが分散し、システム構成が複雑になるので、障害が発生した際に切り分けに時間がかかることが懸念されます。したがって、オンプレミスとクラウドをシームレスに監視できるシステムを導入し、障害発生箇所を特定した上でオンラインで対応するか現場に行くか判断する必要があります。

テレワーク導入後のネットワーク運用のポイント

前章までで、中小企業がテレワークを導入する3つのステップを考えてみました。まとめると、テレワーク導入を進めていくとオンプレミス環境とクラウド環境が混在し、保守が煩雑になることが分かりました。
COVID-19対策のために急遽テレワーク体制を用意せざるを得ない企業においては、新しい技術などの導入や運用体制の変更など、業務プロセスを変更を迫られ、手探り状態となることも少なくないでしょう。そのような慌ただしい状況にある中で、煩雑な保守業務を新たに開始すべきではありません。
テレワークのために新たに増えたVPNやクラウドサービスなどの監視業務は、**これまでの監視業務と合わせて同じ監視プロセスの中で行われるべき**です。

SIerや情シスの業務を増やすことなく効率化するためには、**保守体制の再検討**を行ったり、**クラウドもオンプレミスもシームレスに監視できる仕組みの導入**が必要になるといえるでしょう。 また、新たな技術を導入した企業においては、その監視ノウハウがない場合が多いといえます。**適切な監視をするためには経験豊富なSIerからの助言**が望まれます。

次の章からは、テレワークを導入した企業の監視業務や運用業務の具体的な手法について紹介していきたいと思います。

5 テレワーク時代のネットワークを効率良く管理する方法

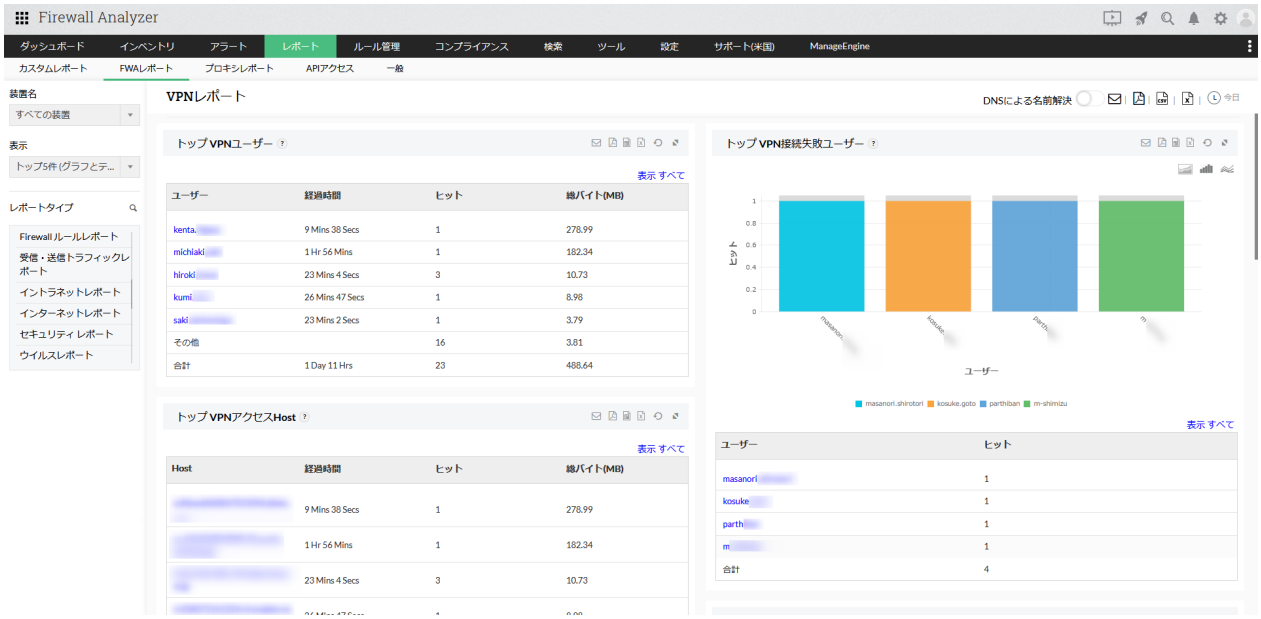
これまでご紹介してきたとおり、テレワークの導入によりネットワークの構成と運用が複雑に変化した環境を管理するためには、運用管理する状況にある管理者が効率良くネットワークを管理し、状況を把握できるようにする必要があります。

ネットワークを手軽に可視化するためのツールとして、今回はManageEngineが提供するネットワーク監視ツールをご紹介します。ManageEngineを使用すると、テレワーク導入後のネットワーク管理を複雑化させず、効率的に管理することが可能になります。

VPN利用状況の可視化

VPNを導入した場合、社内ネットワークへの接続帯域の利用状況を把握して帯域が適切かどうかを確認することと、不要な通信や危険な通信がVPN経由で社内に流れていないかを確認することが重要です。
一般的に、VPN通信を監視するにはファイアウォールの通信ログの収集と解析が必要になります。しかし、ファイアウォールログは量が多くなりやすいため、解析の経験が豊富な社員がいる場合はスムーズに監視ができますが、そのような社員がいない企業は解析に多くの時間と工数が必要になります。

VPN 通信のログ解析を効率化する手段としては、ManageEngine が提供するファイアウォールログ解析ソフトウェアである「**Firewall Analyzer**」があります。Firewall Analyzer を使用すると、これまでテキストで一つ一つ確認していた**ログをレポート形式で可視化**し、誰が見ても状況がすぐに分かるようにすることが可能です。
また、VPN 接続で問題のある動作を検知した場合に、管理者に直ちにお知らせすることが可能です。これにより、**調査の効率化とリスク検知の迅速化の両面を実現**することができます。



Firewall Analyzer の VPN レポート画面。各ユーザーの VPN 接続状況やアクセスホストなどをわかりやすく表示している。Firewall Analyzer はマルチベンダーのファイアウォールのログ解析に対応するほか、プロキシログにも対応している。

Firewall Analyzer 概要資料

Firewall Analyzer 評価版

Firewall Analyzer 体験サイト

クラウド・オンプレ環境の統合監視

クライアントPCをパブリッククラウド上のVDI環境に移行した場合や社内サーバーをクラウドなどに移行した場合、ネットワーク管理者は、既存のオンプレミス環境に加えてクラウド環境も監視対象に追加する必要があります。
既にある監視ツールがプライベートクラウド・パブリッククラウド環境の監視に対応している場合は問題ありませんが、クラウド環境の監視に対応していない監視ツールを使用している場合はツールを再検討する必要があります。
この場合、クラウド監視専用のツールをこれまでのツールとは別に導入することは避けるべきです。管理者はオンプレミス環境の監視ツールのコンソールとクラウド環境の監視ツールのコンソールを行ったり来たりしてネットワークの状況を確認しなければなりません。

テレワーク需要によりネットワーク構成や運用の変化が生じている場合、現場では混乱が発生しやすい状況にあります。監視ツールをクラウド環境とオンプレミス環境で使い分けている場合、重大な障害の見逃しや、調査や状況把握に余計な時間が掛かってしまうおそれがあります。
このため、監視ツールはクラウド環境・オンプレミス環境の両方に対応できるものを選ぶ必要があります。

ManageEngineのネットワーク統合監視ツールである「**OpManager**」は、クラウド環境・オンプレミス環境両方の監視に対応したソフトウェアです。OpManagerを使用すると、オンプレミス環境にあるサーバーやネットワーク機器のみならず、**クラウドに移行したサーバーのパフォーマンスを同時に監**

視することが可能です。

マップ機能を使用して可視化することで、クラウド・オンプレのどこでどのような問題が発生しているかを一目で突き止めることができるようになります。この可視化機能を用いることで、運用しているネットワークの障害調査の時間を短縮することが可能です。

社内ネットワークにあるオンプレミスサーバーとネットワーク機器と、パブリッククラウド AWS 上にある EC2 サーバー 3 台を同時に監視した画面。OpManager をパブリッククラウド上に配置し、社内ネットワークと接続することで実現。

トラフィックの可視化

クラウドへの移行やクラウドアプリケーションの導入が進んだ場合、ネットワークの帯域を占めるアプリケーションへの通信が増加することが予想されます。社内 LAN を経由するオンライン会議は、ネットワーク利用状況によって帯域が逼迫する場合もあります。
「テレワークに移行してからネットワークが遅くなった」と社員から言われた場合に適切に対処するには、社内ネットワークの帯域設定を変更するべきなのか、インターネット回線を増強すべきなのか、または社内外ネットワークが原因ではなく社員個人の端末の問題なのかを切り分ける必要があります。この切り分けを素早く行うため、トラフィックを監視しておくとよいでしょう。

ManageEngine が提供するトラフィック解析ソフトウェアである「**NetFlow Analyzer**」を使用すると、これまでにご紹介した Firewall Analyzer・OpManager のネットワーク機器の監視とファイアウォールの可視化と同時に、トラフィックの内訳監視まで実現可能です。

NetFlow Analyzer はフローコレクターと呼ばれるフロー解析ツールです。NetFlow や sFlow などに対応したネットワーク機器を利用した環境の場合、ネットワークの中で**誰が・どんな種類の通信を・どれくらい行っているかを一目で把握**できる状態まで可視化することが可能です。
ネットワークの輻輳が発生した場合の原因調査や不要な通信の発見など、ネットワーク調査およびセキュリティ向上のために役立つソフトウェアです。

フローを用いてトラフィックの内訳を可視化した画面。SNMP 等のネットワーク監視プロトコルでは総量までしかわからないトラフィック調査もフローコレクターを使用すると内訳を特定することが可能。上記スクリーンショットの場合は大部分を占めるのが https であることがわかる。

ここまでで紹介したファイアウォール監視・ネットワーク監視・トラフィック可視化ツールは、**1 つのツール上からすべての機能を操作することが可能**です。管理ツールを統合することで、複数のツールを使い分けて管理が煩雑になってしまうことを防ぎ、1 つの画面を見ればすべて把握できる環境を実現することが可能です。

NetFlow Analyzer 概要資料

NetFlow Analyzer 評価版

NetFlow Analyzer 体験サイト

6 まとめ

当 eBook では、テレワークの運用で SIer や情報システム部門に求められることと、実践すべきポイントを提案してきました。テレワークは、感染防止の観点だけでなく社員が柔軟に働きやすくする環境を作るためにも重要な仕組みです。テレワーク導入の動きは一過性のものとならず、今後も継続していくことが予想されます。

テレワーク導入が進んだ現場の管理や運用に対応し、問題を解決するための手段として、当 eBook が少しでもお役に立てましたら幸いです。
ネットワーク運用管理の可視化や効率化のためのツールをお探しの場合は、是非 ManageEngine 製品をご検討ください。

ManageEngine のネットワーク運用 eBook

テレワークのセキュリティ対策 ベストプラクティス集

あなたの会社のセキュリティ対策は、テレワークに対応できていますか？

急増するテレワークに対応するためのセキュリティ対策のポイントと、テレワークで働く社員自身が気をつけるべきポイントを簡潔にまとめました。
テレワークが急に始まってどう対応したものかとお悩みの方は是非ご覧ください。

URL：https://www.manageengine.jp/download/products/FWA/fwa-ebook-telework-security.pdf

クラウド移行のための 5 ステップ

オンプレミスはメンテナンスが大変！クラウドサービスに移行したい…でも何から手を付けて良いのかわからない！
クラウド移行を検討しているネットワーク管理者がまず見るべきこと、実施すべきことをまとめました。
クラウドを初めて利用する方や実際の移行プロセスをどうすべきかお悩みの方は是非ご一読ください。

URL：https://www.manageengine.jp/download/products/OPM/opm-ebook-cloud-migration.pdf

ひとり情シスでもできる！クラウド化を乗り切るためのネットワーク管理術とは？

情シスのみなさまは、物理環境とクラウド環境が入り乱れる昨今のネットワーク環境をどのように管理されていますか？物理環境とクラウド環境を別々のツールで管理することで、ツールの＂行ったり来たり＂を強いられていませんか？

当 eBook では、ハイブリッドクラウド環境を効率的に管理するためのコツをご紹介しています。

URL：https://www.manageengine.jp/download/products/OPM/opm-ebook-cloud-monitoring.pdf

テレワーク時代の新しい運用様式
ネットワーク構築運用 SIer 編

2020 年 6 月発行

お問い合わせ先
ゾーホージャパン株式会社
〒220-0012
神奈川県横浜市西区みなとみらい 3 丁目 6 番 1 号
みなとみらいセンタービル 13 階
Web : https://www.manageengine.jp/
E-mail : jp-mesales@zohocorp.com（弊社営業宛）