ランサムウェア攻撃やコロナ禍の在宅勤務などを踏まえて、エンドポイント中心の対策をサーバ/ネットワークやアプリケーションまで拡充するために必要な施策は何か？を1300社の調査結果を元に分析/提言

2021年版 中堅・中小企業のセキュリティ・運用管理・バックアップに関する今後のニーズとベンダ別導入意向レポート案内

本ドキュメントは「調査対象」「設問項目」および「試読版」を掲載した調査レポートご紹介資料です。

[調査レポートで得られるメリット]

1. **年商/業種/従業員数/地域といった様々な観点で市場動向を把握することができます。**
2. **収録されているデータをカタログや販促資料などに引用/転載いただくことができます。**

調査対象ユーザ企業属性

本レポートでは以下のような属性に合致する1300件（有効件数）の中堅・中小企業を対象とした調査を行っている。

有効サンプル数:　1300社（1社1レコード）

A1.年商区分:　5億円未満 / 5億円以上～10億円未満 / 10億円以上～ 20億円未満 / 20億円以上～50億円未満 / 50億円以上～100億円未満 / 100億円以上～ 300億円未満 / 300億円以上～ 500億円未満

A2.職責区分:　以下のいずれかの職責を持つ社員
- 情報システムの導入や運用/管理の作業を担当している
- 情報システムに関する製品/サービスの選定または決裁の権限を有している

A3.従業員数区分:　10人未満 / 10人以上～20人未満 / 20人以上～50人未満 / 50人以上～100人未満 / 100人以上～300人未満 / 300人以上～500人未満 / 500人以上～1000人未満 / 1000人以上～3000人未満 /3000人以上～5000人未満 / 5000人以上

A4.業種区分:　組立製造業 / 加工製造業 / 建設業 / 卸売業 / 小売業 /流通業（運輸業） / IT関連サービス業 / 一般サービス業 / その他

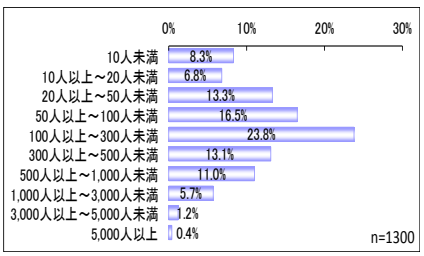
A5.地域区分:　北海道地方 / 東北地方 / 関東地方 / 北陸地方 / 中部地方 / 近畿地方 / 中国地方 / 四国地方 / 九州・沖縄地方

調査実施時期: 2021年6月～7月

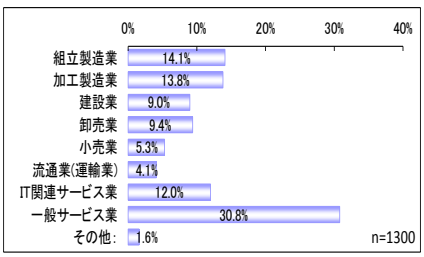
上記に加えて、**「A6.IT管理/運用の人員規模」**（IT管理/運用を担う人材は専任/兼任のいずれか？人数は1名/2～5名/6～9名/10名以上のどれに当てはまるか？）および**「A7.ビジネス拠点の状況」**（オフィス、営業所、工場などの数は1ヶ所/2～5ヶ所/6ヶ所以上のいずれか？ITインフラ管理は個別/統一管理のどちらか？）といった属性についても尋ねており、A1～A7を軸として以降に述べる全ての設問を集計したデータが含まれる。

以下の3つのグラフは1300社の有効サンプルの「従業員数」「業種」「所在地」分布を表したものである。『従業員数1000人以上の大企業が中心で、中小企業のサンプルはわずかしかない』などといったサンプル件数不足や『IT関連サービス業が大半を占めてしまっており、純粋な意味でのユーザ企業が少ない』といったサンプルの偏りがないことが確認できる。

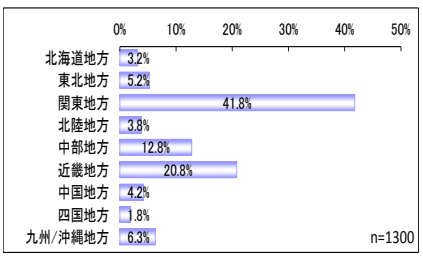
従業員数分布



業種分布



所在地分布



本調査レポートの位置付けと基本構成

旧来、中堅・中小企業におけるセキュリティ、運用管理、バックアップといった「守りのIT対策」はPCなどのエンドポイントを対象としたマルウェア対策が中心であり、サーバ/ネットワークやアプリケーションも含めた包括的な取り組みには至っていなかった。

だが、コロナ禍に起因する在宅勤務の増加によって、「従業員の自宅から社内の業務システムを安全に利用する」ための手段に注目が集まり、中堅・中小企業の「守りのIT対策」に対する視野を大きく広げる結果となった。

一方で、「守りのIT対策」に関する製品/サービスを提供するベンダ側も「ゼロトラスト」を始めとしたキーワードを通じて、ユーザ企業の啓蒙に取り組んでいる。

本調査レポートではこうした背景を踏まえて、1300社のユーザ企業を対象とした調査結果を元に中堅・中小企業における「守りのIT対策」の取り組みを拡大し、製品/サービスを幅広く訴求するためには何が必要か？に関する分析と提言を行っている。

本調査レポートでは以下の3つの観点から調査データの集計/分析を行っている。

A.守りのIT対策に関する今後の方針/ニーズ

エンドポイント、サーバ/ネットワーク、アプリケーション利用の3分野について集計/分析

B.守りのIT対策に関するベンダ別導入意向

セキュリティパッケージ主体、運用管理パッケージ主体、バックアップパッケージ主体、大手のITベンダ/SIerなど、計32社に渡るベンダが対象

C.守りのITに対して拠出可能な年額合計費用

セキュリティ/運用管理/バックアップを担うソフトウェア製品/サービスを利用する際に許容できる年額の合計費用

以下に本調査レポートの章構成および各章で主な分析対象となる設問番号を記載する。2～4章が上記におけるA、5章がB、6章がCに対応している。

第1章.本調査レポートの背景と構成

調査レポートの概要について説明している。

第2章.エンドポイントに関する守りのIT対策の方針/ニーズ

守りのIT対策のうち、エンドポイントに着目した分析と提言を述べている。設問R1が主な集計対象となる。

第3章.サーバ/ネットワークに関する守りのIT対策の方針/ニーズ

守りのIT対策のうち、サーバ/ネットワークに着目した分析と提言を述べている。設問R2が主な集計対象となる。

第4章.アプリケーション利用に関する守りのIT対策の方針/ニーズ

守りのIT対策のうち、アプリケーション利用に着目した分析と提言を述べている。設問R3が主な集計対象となる。

第5章.ベンダ別に見た時の守りのIT対策に関する導入意向

計32社に渡るベンダの導入状況を俯瞰した後、それらと守りのIT対策の方針/ニーズとの関連を述べている。設問R4が主な集計/分析対象となる。

第6章.守りのITに対して許容できる年額の合計費用

ユーザ企業が守りのIT対策に供出可能な年額費用を年商別や業種別に俯瞰した後、拠出可能額と守りのIT対策の方針/ニーズとの関連を述べている。設問R5が主な集計/分析対象となる。

設問項目(1/7)

本調査レポートの設問項目は大きく分けて、以下の3つのグループから構成されている。

A. 守りのIT対策に関する今後の方針/ニーズ(設問R1、R2、R3)
B. 守りのIT対策に関するベンダ別導入意向(設問R4-1～R4-33)
C. 守りのITに対して拠出可能な年額合計費用(設問R5)

以下では、上記のグループ毎に設問項目の詳細を記載する。

[A.守りのIT対策に関する今後の方針/ニーズ(設問R1、R2、R3)]

R1.エンドポイントに関する守りのIT対策の方針/ニーズ(複数回答可)

設問R1ではエンドポイントの守りのIT対策の方針/ニーズについて尋ねている。「エンドポイント」とはPCやスマートデバイス(スマートフォン/タブレット)といったユーザが利用する端末機器および機器上で稼動するOS/ファームウェアを指す。

エンドポイントに関する守りのIT対策には以下のようなものがある。

PC/スマートデバイスのセキュリティ対策:
　　不正なプログラムやアクセス手法を用いたPC/スマートデバイスへの攻撃を防ぐ
PC/スマートデバイスのバックアップ対策:
　　PC/スマートデバイスのプログラム、データ、設定情報などを複製して保管する
PC/スマートデバイスの資産管理:
　　PC/スマートデバイスへのプログラム導入状況を把握し、起動や使用を制御する
PC/スマートデバイスの操作管理:
　　PC/スマートデバイス上の操作(印刷やUSBメモリの使用など)を監視/制御する

上記を踏まえて、設問R1では以下の選択肢を提示している。選択肢は2つのグループに分かれており、「方針に関する項目」はエンドポイントに関する守りのIT対策に取り組む際の考え方や重視する事項に当てはまる選択肢、「ニーズに関する項目」は有償でも利用したいと考える製品/サービス内容として当てはまる選択肢を列挙している。

<<方針に関する項目>>

・製品/サービスを特定のベンダに集約していく
　　例) PCのセキュリティとバックアップについては、同じベンダの製品/サービスで統一する
・複数ベンダの製品/サービスを適宜使い分ける
　　例) マルウェア対策とWebフィルタリングは各分野でシェア首位の製品/サービスを利用する
・新型コロナ感染症対策に伴い刷新/更新する
　　例) 継続的な在宅勤務を前提として、PCのセキュリティ/バックアップ対策を大幅に見直す
・Windows 10への移行に伴い刷新/更新する
　　例) 年2回のOS機能更新に対応できるように、PCの運用管理体制を見直す
・働き方改革への対応に伴い刷新/更新する
　　例) 外出中も社外から業務を行えるようにPCのデータ管理/保護を見直す
・親会社や取引会社からの要請で刷新/更新する
　　例) 親会社のPCセキュリティ指針に従って、使用するツールを変更する
・BCP(事業継続計画)の策定に伴い刷新/更新する
　　例) 災害発生時のデータ保護のため、PCバックアップ対策を刷新する
・社内サーバが不要なクラウドサービスへ移行する
　　例) PCバックアップデータの保存先を社内からクラウドへと移行する
・守りのIT対策を推進する社内人材を育成する
　　例) IT管理/担当の若手社員にセキュリティ対策の講習を受けてもらう
・守りのIT対策を推進する社外人材を利用する
　　例) ITコーディネータに経営層向けのセキュリティ対策講演を依頼する

(次頁へ続く)

設問項目（2/7）

（前頁からの続き）

<<ニーズに関する項目>>

・社内のPCを個人宅でも問題なく利用できる仕組み
　例） 社外に持ち出すと社外秘のファイルが自動的に見えなくなるツールを利用する
・在宅勤務をする従業員のPCを管理できる仕組み
　例） 自宅用PCにUSBメモリを指すと、社内PCの環境が再現できるツールを利用する
・社外で使用するPC内にデータを残さない仕組み
　例） 紛失時にモバイル回線を通じてデータを遠隔削除できる機能を持つPCを利用する
・様々なクラウドサービスを統合管理する仕組み
　例） 様々なクラウドサービスのアクセス権をまとめて管理/設定できるツールを利用する
・クラウドサービスの設定を確認/改善する仕組み
　例） 外部に公開されているなど、不適切な設定項目を通知してくれるサービスを利用する
・リモートで顧客と安全/円滑に対話できる仕組み
　例） Webブラウザを用いて、顧客との商談を手軽に行えるサービスを利用する
・Windows10の更新プログラムを制御する仕組み
　例） 更新プログラムの配布/展開を支援するコンサルティングを利用する
・スマートデバイスとPCを統合管理できる仕組み
　例） PCとスマートデバイスの双方に対応した資産管理ツールを利用する
・トラブル発生後の対策を自動化する仕組み
　例） トラブルが発生したPCを遠隔で診断し、復旧させるサービスを利用する
・不正アクセス発生後の被害拡大を防ぐ対策
　例） 不正アクセスを受けたPCをネットワークから遮断する仕組みを利用する
・顔や指紋などの生体認証技術への対応
　例） ノートPCが備えるカメラを活用して、顔認証によるログインを導入する
・災害時に業務を継続するための仕組み
　例） データをクラウドに保存し、災害発生時に社外からも利用可能にする
・従業員を狙った標的型攻撃への対策
　例） 関係者を装った攻撃メールを疑似的に送信する訓練サービスを利用する

R2.サーバ/ネットワークに関する守りのIT対策の方針/ニーズ（複数回答可）

設問R2では業務システムが稼動するサーバ機器、様々なIT機器を接続するネットワーク機器、およびそれらの機器のOSやファームウェアにおける守りのIT対策について尋ねている。

サーバ/ネットワークに関する守りのIT対策には以下のようなものがある。

サーバのセキュリティ対策：
　不正なプログラムやアクセス手法を用いたサーバへの攻撃を防ぐ
サーバのバックアップ対策：
　サーバのプログラム、データ、設定情報などを複製して保管する
サーバの稼動監視：
　サーバ機器やOSが正常に稼働し、障害/遅延がないかを監視する
ネットワークのセキュリティ対策：
　不正なPCのLANへの接続やスイッチ/ルータへの攻撃などを防ぐ
ネットワークの稼動監視：
　スイッチ/ルータが正常に稼働し、障害/遅延がないかを監視する
外部からの侵入の検知/防止：
　外部と繋がるネットワーク機器を標的とした侵入/攻撃の防御

（次頁へ続く）

設問項目（3/7）

（前頁からの続き）

前頁の記載内容を踏まえて、設問R2では以下の選択肢を提示している。選択肢は2つのグループに分かれており、「方針に関する項目」はサーバおよびネットワークに関する守りのIT対策に取り組む際の考え方や重視する事項に該当する選択肢、「ニーズに関する項目」は有償でも利用したいと考える製品/サービス内容として当てはまる選択肢を列挙している。

<<方針に関する項目>>

・製品/サービスを特定のベンダに集約していく
　例） サーバのセキュリティとバックアップについては、同じベンダの製品/サービスで統一する
・複数ベンダの製品/サービスを適宜使い分ける
　例） ファイアーウォールとスパムメール対策は各分野でシェア首位の製品/サービスを利用する
・新型コロナ感染症対策に伴い刷新/更新する
　例） 継続的な在宅勤務を前提として、社外からのリモートアクセスを大幅に見直す
・サーバOSの入れ替えに伴い刷新/更新する
　例） サーバOSのサポート終了に伴って業務システムもバージョンアップする
・海外でデータ管理/保存を行う業者は避ける
　例） データセンタが海外に置かれたクラウドサービスは利用しないようにする
・働き方改革への対応に伴い刷新/更新する
　例） 外出中も社外から業務を行えるように業務システムをクラウドへ移行する
・親会社や取引会社からの要請で刷新/更新する
　例） 親会社の業務システム指針に従って、販売管理をクラウドへ移行する
・BCP(事業継続計画)の策定に伴い刷新/更新する
　例） 災害発生時のデータ保護のため、サーバのバックアップ対策を刷新する
・「ゼロトラスト」の考え方に沿って刷新/更新する
　例） LAN内も安全とは考えず、不正な通信を検知/遮断する仕組みを導入する

<<ニーズに関する項目>>

・個人宅と社内を安全/手軽に接続できる仕組み
　例） オフィス側の機器設置のみで利用できるリモートVPNサービスを導入する
・社内のサーバを個人宅から管理できる仕組み
　例） IT管理担当者がブラウザで操作できるサーバ管理ツールを利用する
・社内とクラウドの双方を統合管理する仕組み
　例） 社内とクラウド上の双方のサーバを統合管理できるツールを利用する
・VPNに代わる安全/手軽なアクセスサービス
　例） クラウド経由で社内外のシステムをWebで利用できるサービスを利用する
・Webフォーム画面の乗っ取りを防ぐ仕組み
　例） Webフォームの動作に異常がないかをチェックできるツールを利用する
・大手キャリアが提供する5G回線網での防御
　例） 通信モジュール（SIMカード）の不正な交換を検知するツールを利用する
・特定業者が提供するローカル5Gでの防御
　例） ローカル5Gでの不正なデバイス接続を監視/遮断するツールを利用する
・IoT機器を対象としたセキュリティ対策
　例） IoT機器向けのマルウェア対策ツールを利用する
・システムの脆弱性を診断するサービス
　例） ECサイトに疑似的に不正アクセスして診断するサービスを利用する
・不正アクセスの防護壁となるサービス
　例） WAF（Web Application Firewall）のクラウドサービスを利用する
・データ保護における非IT機器とIT機器の連携
　例） 製造装置のデータをインターネットを介して安全に共有する

（次頁へ続く）

設問項目（4/7）

（前頁からの続き）

・トラブル発生後の対策を自動化する仕組み
　　例） サーバの故障個所をWeb経由で通知するサービスを利用する
・不正アクセス発生後の被害拡大を防ぐ対策
　　例） 社内から社外への疑わしい通信を遮断する仕組みを利用する
・災害時に業務を継続するための仕組み
　　例） 遠隔地に待機用のサーバ環境を構築できるサービスを利用する

R3.アプリケーション利用に関する守りのIT対策の方針/ニーズ（複数回答可）

企業では業務システム、Webサイト、メールなど多種様々なアプリケーションを利用しており、それらを保護/保全する必要がある。また、アプリケーションを利用する従業員に対する啓蒙や教育も重要となる。設問R3ではこうしたアプリケーションを利用する際に必要となる守りのIT対策について尋ねている。

アプリケーション利用に関する守りのIT対策には以下のようなものがある。

業務システムソフトウェアの稼動監視：
　業務システムソフトウェアに障害/遅延がないかを監視する
業務システムソフトウェアの構成管理：
　業務システムソフトウェアの設定情報や変更履歴を管理する
スパムメール/不正メールの排除：
　スパムメールや不正メールを検知し、社内への配布を防止する
メール誤送信/漏えいの防止：
　メールの宛先や内容をチェックし、誤送信や情報漏えいを防ぐ
WebサイトやeコマースサイトのWeb保護：
　社外に公開しているサイトに対する不正侵入や攻撃を防ぐ
不正Webサイトへのアクセス防止：
　URLフィルタリングなどで従業員のWeb閲覧を管理/制御する
従業員に対する標的型攻撃対策：
　知人を装ったメールなどによる個人を標的とした攻撃の防御
従業員向けのヘルプデスク：
　従業員からのIT関連の質問に対応できる窓口の設置/運営

上記を踏まえて、設問R3では以下の選択肢を提示している。選択肢は2つのグループに分かれており、「方針に関する項目」はアプリケーション利用に関連する守りのIT対策に取り組む際の考え方や重視する事項に該当する選択肢、「ニーズに関する項目」は有償でも利用したいと考える製品/サービス内容として当てはまる選択肢を列挙している。

<<方針に関する項目>>

・製品/サービスを特定のベンダに集約していく
　　例） アプリの資産管理とバックアップのツールを同じベンダで統一する
・複数ベンダの製品/サービスを適宜使い分ける
　　例） オンプレミスとクラウドでアプリのバックアップツールを使い分ける
・新型コロナ感染症対策に伴い刷新/更新する
　　例） 在宅勤務に適したブラウザで操作可能なアプリへと移行する
・Windows 10への移行に伴い刷新/更新する
　　例） Windows 10への移行に合わせて業務システムを刷新する
・サーバOSの入れ替えに伴い刷新/更新する
　　例） サーバOSのサポート終了に伴って業務システムも刷新する
・働き方改革への取り組みに伴い刷新/更新する
　　例） 社外で利用できるスマートデバイス対応のアプリを優先する

（次頁へ続く）

設問項目(5/7)

(前頁からの続き)

・親会社や取引会社からの要請で刷新/更新する
　　例) 親会社のERP刷新に伴い、自社の基幹系システムも変更する
・BCP(事業継続計画)の策定に伴い刷新/更新する
　　例) 日頃利用しているアプリが社外からも利用できるかを検証する
・社内サーバが不要なクラウドサービスへ移行する
　　例) クラウドサービスへ移行可能なアプリの確認と選定を行う

<<ニーズに関する項目>>

・アプリケーションをブラウザで利用可能にする仕組み
　　例) クライアント/サーバ形態の画面をブラウザ用に変換するサービスを利用する
・利用可能なアプリケーションを制限/管理する仕組み
　　例) PCに標準で備わっている管理用ツールを禁止できる仕組みを利用する
・様々なクラウドサービスの安全性を評価するサービス
　　例) 民間企業が提供するクラウドセキュリティ評価サービスなどを利用する
・セキュリティ全般に関する従業員向け教育サービス
　　例) 標的型攻撃の手法と対策を解説したeラーニングを受講する
・プライバシーマークなどの公的な認定の取得支援
　　例) プライバシーマーク認定を支援するコンサルティングを利用する
・複数のID/アカウントを統合管理する仕組み
　　例) 複数のクラウドサービスのID/アカウントを統合するサービスを利用する
・ID/アカウントをクラウド上で管理する仕組み
　　例) ID/アカウントの管理基盤を社内サーバからクラウドサービスに移行する
・データをクラウド上にバックアップする仕組み
　　例) ファイルサーバの文書を自動でクラウドに複製するサービスを利用する
・データを社内にバックアップする仕組み
　　例) 業務システムのデータを保管するバックアップ専用機器を導入する
・トラブル発生後の対策を自動化する仕組み
　　例) OS更新で動かなくなったアプリ環境を手軽に元に戻すツールを利用する
・不正アクセス発生後の被害拡大を防ぐ対策
　　例) アプリのログを解析し、情報漏えいの有無を確認できるツールを導入する
・災害時に業務を継続するための仕組み
　　例) 災害発生時に社員の所在を確認できるサービスを導入する

[B. 守りのIT対策に関するベンダ別導入意向(設問R4-1～R4-33)]

セキュリティ、運用管理、バックアップといった守りのIT対策を担うソフトウェア製品/サービスを開発/販売するベンダも多数存在する。設問R4-1～R4-33ではこうしたベンダを列挙し、以下の選択肢を設けて各ベンダの導入意向を尋ねている。

導入済み＆継続:
　　該当するベンダの製品/サービスを既に導入しており、今後も利用を継続する
導入済み＆変更:
　　該当するベンダの製品/サービスを既に導入しているが、今後は他社に変更する予定である
導入予定:
　　現時点では導入していないが、該当するベンダの製品/サービスを導入する予定である
予定なし:
　　現時点では導入しておらず、今後も該当するベンダの製品/サービスを導入する予定はない
認知なし:
　　該当するベンダを知らない

(次頁へ続く)

設問項目（6/7）

（前頁からの続き）

導入意向を尋ねる対象となるベンダは以下の通りである。上記の選択肢によって各ベンダ（計32社+その他）の導入意向を尋ねた結果がR4-1～R4-33の設問に対応している。「」内は各ベンダにおける代表的な製品/サービス名称である。
（必ずしも最新の製品/サービスではなく、中堅・中小企業が該当するベンダを最も確実に想起できるものを記載している）

<<セキュリティパッケージ主体>>

R4-1. トレンドマイクロ（「ウイルスバスター」など）
R4-2. シマンテック（ブロードコム）（「Symantec Endpoint Protection」など）
R4-3. マカフィー（「McAfee Endpoint Protection」など）
R4-4. キヤノンITソリューションズ（「GUARDIANWALL」「ESET」など）
R4-5. カスペルスキー（「カスペルスキー」など）
R4-6. ソースネクスト（「ZEROシリーズ」など）
R4-7. エフ・セキュア（「F-Secure」など）
R4-8. FFRIセキュリティ（「FFRI yarai」など）

<<運用管理パッケージ主体>>

R4-9. Sky（「SKYSEA Client View」など）
R4-10. クオリティソフト（「QND」など）
R4-11. エムオーテックス（「LanScope」など）
R4-12. Ivanti（LANDESK）（「Ivanti(LANDESK)」など）
R4-13. ハンモック（「AssetView」など）

<<バックアップパッケージ主体>>

R4-14. ベリタステクノロジーズ（「Backup Exec」など）
R4-15. Arcserve（「Arcserve」など）
R4-16. クエストソフトウェア（「NetVault」など）
R4-17. ストレージクラフト（「ShadowProtect」など）
R4-18. アクティファイ（ネットジャパン）（「ActiveImage Protector」など）
R4-19. アクロニス（「Acronis」など）

<<その他のパッケージ主体>>

R4-20. アルプスシステムインテグレーション（「InterSafe」など）
R4-21. デジタルアーツ（「i-FILTER」など）
E4-22. ソリトンシステムズ（「InfoTrace」など）

<<大手のITベンダ/SIer>>

R4-23. 日立製作所（「JP1」など）
R4-24. 富士通（「Systemwalker」など）
R4-25. NEC（「WebSAM」など）
R4-26. 日本ヒューレット・パッカード(HPE)（「Ice Wall」など）
R4-27. デル・テクノロジーズ（「RSA SecureID」など）
R4-28. シスコシステムズ（「CiscoWorks」など）
R4-29. 日本マイクロソフト（「Microsoft System Center」など）
R4-30. 日本IBM（「Tivoli」など）
R4-31. NTTデータ（「Hinemos」など）
R4-32. 野村総合研究所（「Senju」など）

<<その他>>

R4-33.その他
※「その他」の4番目の選択肢は「認知なし」の代わりに「未回答」となっており、その他の回答がなかった場合が当てはまる

さらにR4-1～R4-33の結果をカテゴリ毎にまとめた以下の派生設問が設けられている。

R4S-1.セキュリティパッケージ主体（複数回答可）

セキュリティパッケージ主体のベンダ（R4-1～R4-8）に関する回答結果を以下の選択肢でまとめた派生設問である。

・導入済み＆継続	R4-1～R4-8の少なくとも1つで「導入済み＆継続」と回答している場合
・導入済み＆変更	R4-1～R4-8の少なくとも1つで「導入済み＆変更」と回答している場合
・導入予定	R4-1～R4-8の少なくとも1つで「導入予定」と回答している場合
・予定なし/認知なし	上記3つの選択肢のいずれにも当てはまらない場合

（次頁へ続く）

設問項目（7/7）

（前頁からの続き）

R4S-2.運用管理パッケージ主体（複数回答可）

運用管理パッケージ主体のベンダ（R4-9～R4-13）に関する回答結果を以下の選択肢でまとめた派生設問である。

- ・導入済み＆継続　　R4-9～R4-13の少なくとも1つで「導入済み＆継続」と回答している場合
- ・導入済み＆変更　　R4-9～R4-13の少なくとも1つで「導入済み＆変更」と回答している場合
- ・導入予定　　R4-9～R4-13の少なくとも1つで「導入予定」と回答している場合
- ・予定なし/認知なし　　上記3つの選択肢のいずれにも当てはまらない場合

R4S-3.バックアップパッケージ主体（複数回答可）

バックアップパッケージ主体のベンダ（R4-14～R4-19）に関する回答結果を以下の選択肢でまとめた派生設問である。

- ・導入済み＆継続　　R4-14～R4-19の少なくとも1つで「導入済み＆継続」と回答している場合
- ・導入済み＆変更　　R4-14～R4-19の少なくとも1つで「導入済み＆変更」と回答している場合
- ・導入予定　　R4-14～R4-19の少なくとも1つで「導入予定」と回答している場合
- ・予定なし/認知なし　　上記3つの選択肢のいずれにも当てはまらない場合

R4S-4.その他のパッケージ主体（複数回答可）

その他のパッケージ主体のベンダ（R4-20～R4-22）に関する回答結果を以下の選択肢でまとめた派生設問である。

- ・導入済み＆継続　　R4-20～R4-22の少なくとも1つで「導入済み＆継続」と回答している場合
- ・導入済み＆変更　　R4-20～R4-22の少なくとも1つで「導入済み＆変更」と回答している場合
- ・導入予定　　R4-20～R4-22の少なくとも1つで「導入予定」と回答している場合
- ・予定なし/認知なし　　上記3つの選択肢のいずれにも当てはまらない場合

R4S-5.大手のベンダ/SIer（複数回答可）

大手のベンダ/SIer（R4-23～R4-32）に関する回答結果を以下の選択肢でまとめた派生設問である。

- ・導入済み＆継続　　R4-23～R4-32の少なくとも1つで「導入済み＆継続」と回答している場合
- ・導入済み＆変更　　R4-23～R4-32の少なくとも1つで「導入済み＆変更」と回答している場合
- ・導入予定　　R4-23～R4-32の少なくとも1つで「導入予定」と回答している場合
- ・予定なし/認知なし　　上記3つの選択肢のいずれにも当てはまらない場合

[C. 守りのITに対して拠出可能な年額合計費用（設問R5）]

設問R5では守りのITに対して拠出可能な年額合計費用（万円）を数値記入形式で尋ねている。ハードウェアとOS/ファームウェアに関する費用は除外し、セキュリティ/運用管理/バックアップを担うソフトウェアの製品/サービスを利用する上で許容できる年額の合計費用を記入する形式となっている。集計データでは回答結果の平均値を算出しており、他のR系列設問とは異なる集計データファイル【R5】(【A1～A7】表側).xlsxに結果が収録されている。

レポート試読版1（「分析サマリ」その1）

本調査レポートの分析サマリでは50ページ超に渡って、中堅・中小企業におけるセキュリティ、運用管理、バックアップといった守りのIT対策の実態、32社に及ぶベンダの導入意向、およびベンダや販社/SIerに向けた提言などを述べている。以下のレポート試読版では、「第3章.サーバ/ネットワークに関する守りのIT対策の方針/ニーズ」に関する分析サマリの一部を紹介している。（第2章でエンドポイント、第4章でアプリケーション利用に関して同様の分析を行っている）

3. サーバ/ネットワークに関する守りの IT 対策の方針/ニーズ

本章では業務システムが稼動するサーバ機器、様々な IT 機器を接続するネットワーク機器、ならびにそれらの機器の OS やファームウェアにおける守りの IT 対策について尋ねている。サーバ/ネットワークに関する守りの IT 対策には以下のようなものがある。

**********中略**********

コロナ禍に伴う在宅勤務においては従業員の自宅から社内の業務システムを安全に利用できる仕組みが必要とある。そのため、昨今では前章のエンドポイントに加えて、サーバ/ネットワークの守りの IT 対策にも注目が集まっている。そうした背景を踏まえて、本調査レポートでは以下の選択肢を列挙した設問「R2.サーバ/ネットワークに関する守りの IT 対策の方針/ニーズ」でサーバ/ネットワークの守りの IT 対策に関する方針やニーズを尋ねている。

<<方針に関する項目>>

・製品/サービスを特定のベンダに集約していく

例） サーバのセキュリティとバックアップについては、同じベンダの製品/サービスで統一する

・複数ベンダの製品/サービスを適宜使い分ける

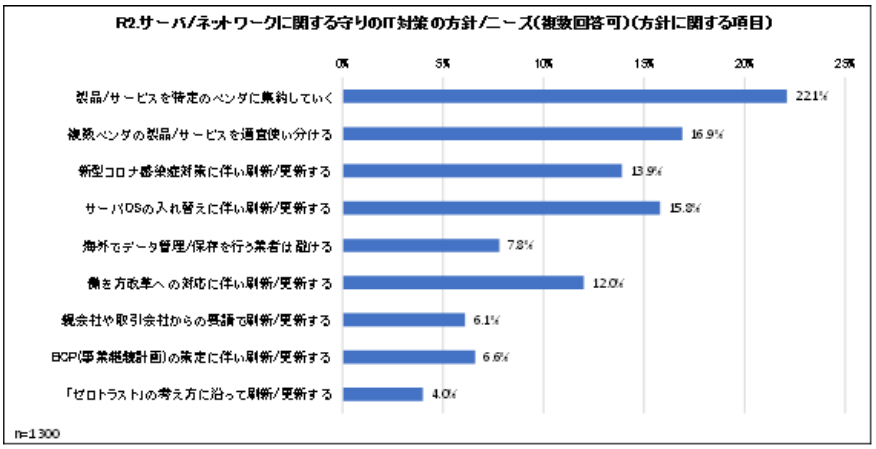
例） ファイアーウォールとスパムメール対策は各分野でシェア首位の製品/サービスを利用する

・新型コロナ感染症対策に伴い刷新/更新する

例） 継続的な在宅勤務を前提として、社外からのリモートアクセスを大幅に見直す

**********中略**********

以下のグラフは設問 R2 の「方針に関する項目」を中堅・中小企業全体で集計したものだ。（集計データ￥単純集計データ￥【R 系列】単純集計.xlsx から、方針に関する項目を抜粋）



サンプルのため、実際のグラフよりも大きさを縮小して掲載している

上記のグラフが示すように、「サーバ OS の入れ替え」といった更新需要が依然として最も多く、「新型コロナ感染症対策」と「働き方改革」を上回っていることが確認できる。ただし、これら 3 項目の差異は大きくないため、販社/SIer としては更新需要に留まらない訴求に取り組んでいくことが重要となってくる。

**********以下、省略**********

レポート試読版2(「分析サマリ」その2)

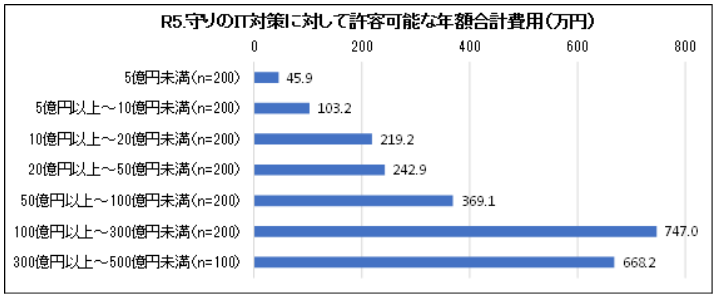
さらに分析サマリでは中堅・中小企業がセキュリティ、運用管理、バックアップといった守りのIT対策に対して拠出可能な年額合計費用についても分析を行っている。以下のレポート試読版ではその点を述べた「第6章.守りのITに対して許容できる年額の合計費用」の一部を抜粋して掲載している。

6.守りの IT に対して許容できる年額の合計費用

ベンダや販社/SIer が守りの IT 対策を訴求する際にはユーザ企業が全体として拠出できる費用を把握しておくことも大切だ。そこで、本調査レポートでは守りの IT に対して拠出可能な年額合計費用(万円)を数値記入形式で尋ねている。

**********中略**********

以下のグラフは設問 R5 の結果を年商別に集計したものだ。(集計データ¥主要分析軸集計データ¥【R5】(【A1～A7】表側).xlsx)



サンプルのため、実際のグラフよりも大きさを縮小して掲載している

ユーザ企業の年商規模が大きくなるにつれて、拠出可能な年額合計費用も概ね高くなる傾向が確認できる。ただし、年商 300～500 億円未満の中堅上位企業層では年商 100～300 億円の中堅中位企業層と比べて数値が下がっている点に注意が必要だ。中堅上位企業層の IT 活用傾向は年商 500 億円以上の大企業に近く、既に様々な守りの IT 対策を構築済みであるケースも多い。その結果、中堅中位企業層と比べて拠出可能な年額費用がやや低くなっていると考えられる。

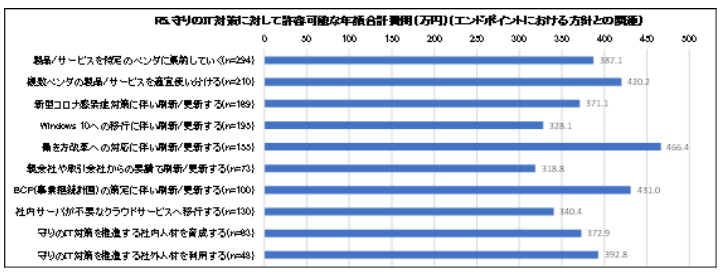
以下のグラフは設問 R5 の結果を業種別に集計したものだ。(集計データ¥主要分析軸集計データ¥【R5】(【A1～A7】表側).xlsx)

**********中略**********

続いて、第 2 章で述べた「エンドポイントの守りの IT 対策における方針/ニーズ」と「拠出可能な年額合計費用」の関連を見ていくことにする。

以下のグラフはエンドポイントの守りの IT 対策における「方針」を軸として拠出可能な年額合計費用の関連を集計した結果である。(集計データ¥質問間クロス集計データ¥【R5】(【R1～R3】表側).xlsx [R1 表側]シートから方針に関する項目を抜粋)

**********中略**********



サンプルのため、実際のグラフよりも大きさを縮小して掲載している

**********以下、省略**********

レポート試読版3(「主要分析軸集計データ」)

「設問項目」に掲載した設問結果を年商、業種、従業員数、所在地などの基本属性を軸として集計したものが、「主要分析軸集計データ」であり、Microsoft Excel形式で調査レポート内に同梱されている。以下の試読版に掲載したものは「A6. IT管理/運用の人員体制」を集計軸として「R系列」(本調査レポートの全設問)を集計した結果の一部である。

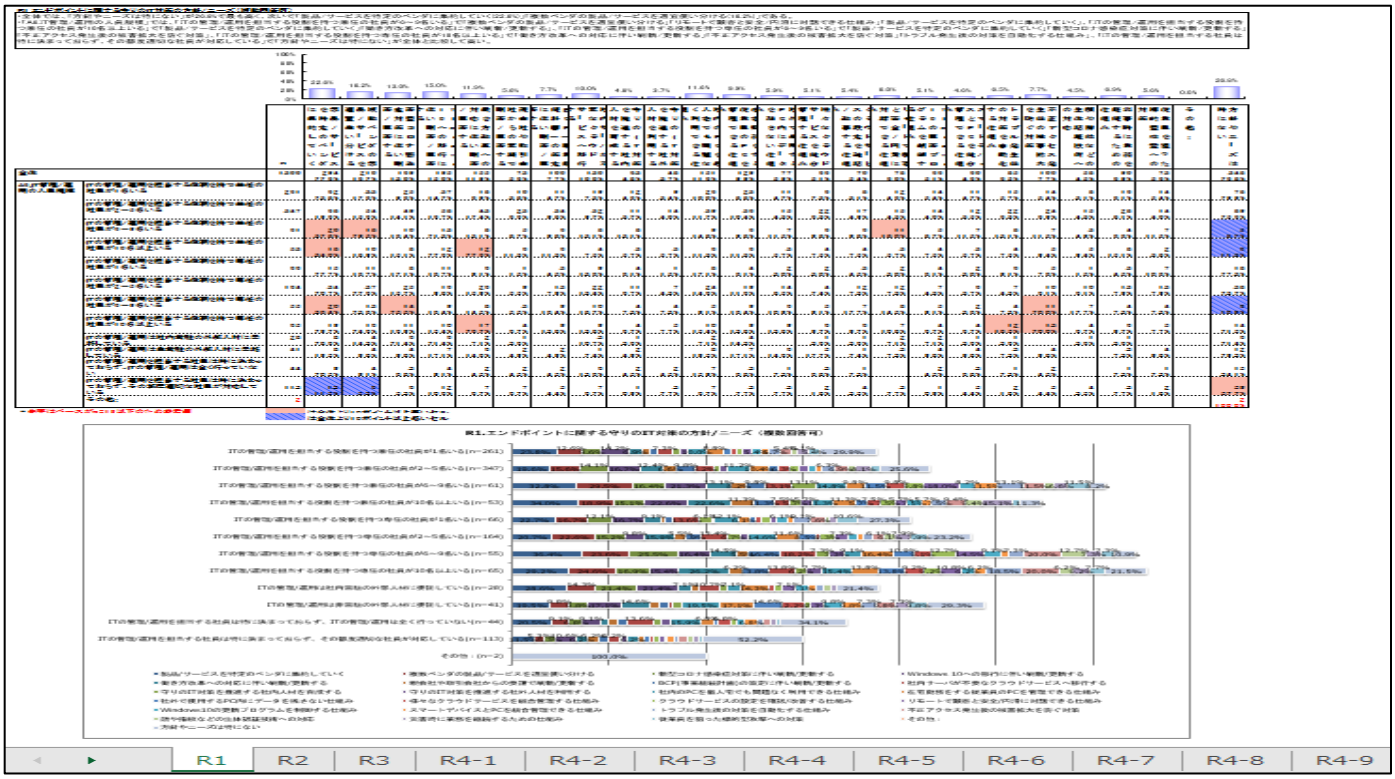
以下のMicrosoft Excelファイル名は『【R系列】(【A6】表側).xlsx』となっている。【R系列】とは、本調査レポートのR1系列～R5系列を含む全設問を指している。また、【A6】とはIT管理/運用の人員体制を示す企業属性であり、以下に列挙された選択肢から構成されている。

- ・ITの管理/運用を担当する役割を持つ兼任の社員が1名いる
- ・ITの管理/運用を担当する役割を持つ兼任の社員が2～5名いる
- ・ITの管理/運用を担当する役割を持つ兼任の社員が6～9名いる
- ・ITの管理/運用を担当する役割を持つ兼任の社員が10名以上いる
- ・ITの管理/運用を担当する役割を持つ専任の社員が1名いる
- ・ITの管理/運用を担当する役割を持つ専任の社員が2～5名いる
- ・ITの管理/運用を担当する役割を持つ専任の社員が6～9名いる
- ・ITの管理/運用を担当する役割を持つ専任の社員が10名以上いる
- ・ITの管理/運用は社内常駐の外部人材に委託している
- ・ITの管理/運用は非常駐の外部人材に委託している
- ・ITの管理/運用を担当する社員は特に決まっておらず、ITの管理/運用は全く行っていない
- ・ITの管理/運用を担当する社員は特に決まっておらず、その都度適切な社員が対応している

したがって、『【R系列】(【A6】表側).xlsx』の結果を見ることによって、IT管理/運用を担う人材が1名のみの場合(ひとり情シス)と2～5名、6～9名、10名以上のそれぞれの場合で、「守りのIT」への取り組み状況にどのような違いがあるか？を確認することができる。同じように、年商別の傾向については『【R系列】(【A1】表側).xlsx』(A1が年商区分を表す)、業種別の傾向については『【R系列】(【A4】表側).xlsx』(A4が業種区分を表す)といった集計データが用意されている。このように、ファイル名を見ることで「どの設問を対象として何を軸として集計したものか？」がわかるようになっている。

本調査レポートの設問数はR1系列(1設問)、R2系列(1設問)、R3系列(1設問)、R4系列(38設問)、R5系列(1設問)の計42設問となっており、集計の軸となる属性は「A1.年商」「A2.職責」「A3.従業員数」「A4.業種」「A5.IT管理/運用の人員規模」「A6.ビジネス拠点の状況」「A7.所在地」の7項目存在する。そのため本調査レポートにおける「主要分析軸データ」の合計シート数は42設問×7属性＝294シートに達する。(ただし「年商30億円以上～50億円未満かつ組立製造業」といったように2つ以上の属性を掛け合わせたものを軸とした集計結果については本レポートの標準には含まれない)

個々のシートは画面上部に軸を設定しない状態の縦帯グラフ、画面中央には年商や業種といった属性軸を設定して集計した結果の数表データ、画面下部にはその数表データを横帯グラフで表したものが掲載されるという書式になっている。



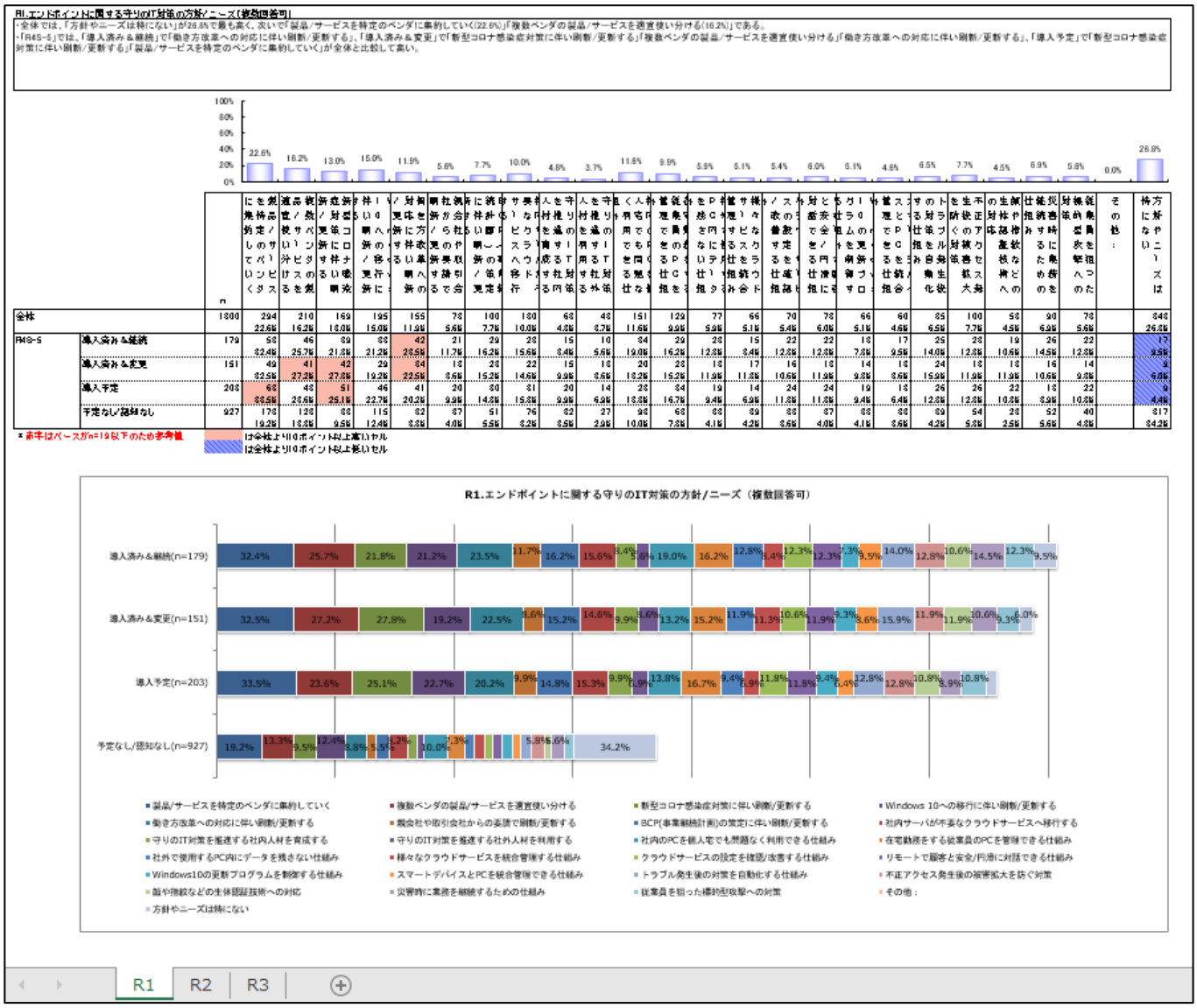
レポート試読版4(「質問間クロス集計データ」)

「設問項目」に掲載した設問結果を他の設問結果を軸として集計したものが、「質問間クロス集計データ」であり、「主要分析軸集計データ」と同様にMicrosoft Excel形式で同梱されている。

以下の試読版に掲載したものは「エンドポイント(R1)、サーバ/ネットワーク(R2)、アプリケーション利用(R3)の守りのIT対策における方針/ニーズ」を尋ねた結果を「大手のベンダ/SIerの導入状況(R4S-5)」を軸として集計した結果である。
この結果を見ることで、大手ベンダが開発/販売する統合運用管理システムの導入意向(導入済みの製品/サービスを継続する、他の製品/サービスに変更する、新規に導入を予定している、など)に影響を与える事象(コロナ禍や働き方改革など)や機能ニーズは何か?を知ることができる。

以下のMicrosoft Excelファイル名は『【R1～R3】(【R4S-5】表側).xlsx』となっている。「【R1～R3】表側」の部分は設問R1、R2、R3の各設問が集計対象の設問であることを示しており、「【 R4S-5 】の部分は設問R4S-5が集計軸(表側)となっていることを示している。このようにファイル名を見ることによって「どの設問を軸としてどの設問の結果を集計したものか?」がわかるようになっている。

個々のシートには画面上部に軸を設定しない状態の縦帯グラフ、画面中央には特定の設問を軸として設定した集計結果の数表データ、画面下部にはその数表データを横帯グラフで表したものが掲載されるといった書式になっている。



本レポートの価格とご購入のご案内

『2021年版 中堅・中小企業のセキュリティ・運用管理・バックアップに関する今後のニーズとベンダ別導入意向レポート』

【価格】180,000円(税別)　【発刊日】2022年2月28日
【媒体】CD-ROM (分析サマリ: PDF形式、集計データ: Microsoft Excel形式)
【サンプル/ダイジェスト】 以下より、本レポートのサンプル/ダイジェストをご覧いただけます。

中堅・中小企業のセキュリティ対策ニーズをエンドポイントからサーバ/ネットワークに広げる施策
https://www.norkresearch.co.jp/pdf/2021Sec_usr_rel1.pdf

中堅・中小企業におけるバックアップ対策とランサムウェア攻撃やサーバインフラ更新の関係
https://www.norkresearch.co.jp/pdf/2021Sec_usr_rel2.pdf

【お申込み方法】 弊社ホームページからの申し込みまたはinform@norkresearch.co.jp宛にご連絡ください

その他のレポート最新刊のご案内(各180,000円税別)

2021年版中堅・中小向け5G/ネットワーク関連サービスの展望レポート

ローカル5G、ゼロトラスト、エッジコンピューティングなどの新たなネットワーク活用を普及させるためには何が必要か？
【レポートの概要と案内】 https://www.norkresearch.co.jp/pdf/2021NW_user_rep.pdf
【リリース(ダイジェスト)】 中堅・中小市場における5G/ネットワーク関連サービスの訴求ポイント
https://www.norkresearch.co.jp/pdf/2021NW_user_rel1.pdf
ゼロトラストに向けた中堅・中小ネットワーク環境の実態と今後
https://www.norkresearch.co.jp/pdf/2021NW_user_rel2.pdf
ローカル5G活用を成功させるための業種別シナリオ
https://www.norkresearch.co.jp/pdf/2021NW_user_rel3.pdf

2021年版 中堅・中小企業の業務システム購入先のサービス/サポート評価レポート

プライム率、導入効果、商材ポートフォリオなどの指標とユーザ評価を照合し、DX時代を担う販社/SIer像を明らかにする
【レポートの概要と案内】 https://www.norkresearch.co.jp/pdf/2021SP_usr_rep.pdf
【リリース(ダイジェスト)】 中堅・中小市場で販社/SIerが注力すべきDX評価指標
https://www.norkresearch.co.jp/pdf/2021SP_usr_rel1.pdf
DX商材のチャネル開拓/拡大に向けてIT企業が着目すべきポイント
https://www.norkresearch.co.jp/pdf/2021SP_usr_rel2.pdf
中堅・中小企業がDX時代に重視する保守/サポートの在り方
https://www.norkresearch.co.jp/pdf/2021SP_usr_rel3.pdf

2021年版 中堅・中小企業におけるRPAおよびノーコード/ローコード開発ツールの活用実態レポート

コロナ禍で停滞したRPA導入提案などを再び加速させるために必要な施策とは？
【レポートの概要と案内】 https://www.norkresearch.co.jp/pdf/2021RPA_user_rep.pdf
【リリース(ダイジェスト)】 RPA導入提案における「有効な用途」と「解決すべき課題」
https://www.norkresearch.co.jp/pdf/2021RPA_user_rel1.pdf
RPAツールの導入社数シェアおよびワークフローとの役割分担に関する展望
https://www.norkresearch.co.jp/pdf/2021RPA_user_rel2.pdf
ノーコード/ローコード開発ツールの活用実態とRPAとの関係
https://www.norkresearch.co.jp/pdf/2021RPA_user_rel3.pdf

本ドキュメントに関するお問い合わせ

NORK RESEARCH
株式会社 ノークリサーチ　担当：岩上 由高
〒160-0022 東京都新宿区新宿2-13-10　武蔵野ビル5階23号室
TEL 03-5361-7880 FAX 03-5361-7881
Mail: inform@norkresearch.co.jp
Web: www.norkresearch.co.jp