PRESS RELEASE（報道関係者各位）

2022年12月13日

2022年 中堅・中小企業におけるエンドポイント環境のセキュリティ対策と今後の方針

調査設計/分析/執筆：岩上由高
ノークリサーチ（本社〒160-0022東京都新宿区新宿2-13-10武蔵野ビル5階23号室　代表：伊嶋謙ニ TEL：03-5361-7880
URL：http//www.norkresearch.co.jp）は中堅・中小企業におけるエンドポイント環境のセキュリティ対策と守りのIT対策全般における今後の方針に関する調査を行った結果を発表した。本リリースは「2022年版 中堅・中小企業のセキュリティ/運用管理/バックアップ利用実態と展望レポート」のサンプル/ダイジェストである。

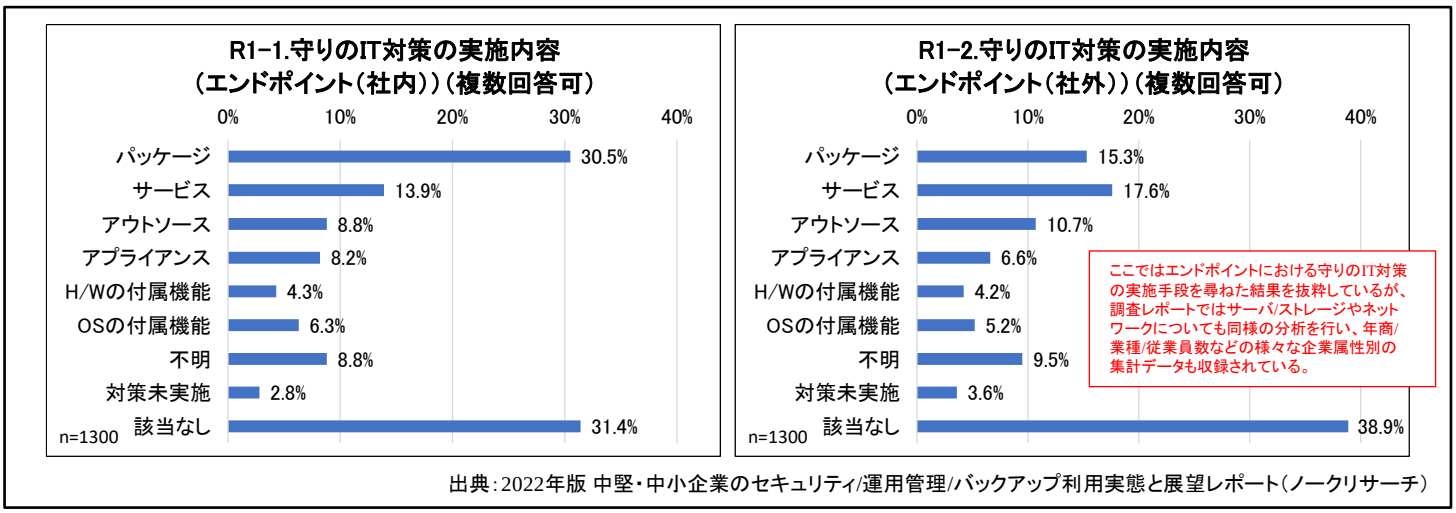
＜サービス化に向けた提案/啓蒙を進めながら、社内と社外の双方をカバーした対策を強化すべき＞
■エンドポイントの守りの対策が社内と社外で不一致、一貫したソリューションの提供が必要
■社外エンドポイントと社内の安全な通信手段では「サービス」が「アプライアンス」を上回る
■クラウド型デスクトップ仮想化への移行も有効な対策、Device as a Serviceは啓蒙が必要

対象企業：　年商500億円未満の中堅・中小企業1300社（日本全国、全業種）（有効回答件数）
対象職責：　情報システムの導入や運用/管理または製品/サービスの選定/決済の権限を有する職責
※調査対象の詳しい情報については右記のレポート案内を参照　https://www.norkresearch.co.jp/pdf/2022Sec_user_rep.pdf

エンドポイントの守りの対策が社内と社外で不一致、一貫したソリューションの提供が必要

本リリースの元となる調査レポート「2022年版 中堅・中小企業のセキュリティ/運用管理/バックアップ利用実態と展望レポート」では、年商500億円未満の中堅・中小企業（有効回答件数1300社）を対象に、エンドポイント（PC、スマートデバイス）、サーバ/ストレージ、ネットワークの守りのIT対策（セキュリティ、運用管理、バックアップなど）の現状、課題、今後の方針を尋ねた結果を分析している。

以下のグラフはエンドポイントの守りのIT対策をどのような手段で実施しているか？の回答結果を社内のエンドポイント（左側）と社外のエンドポイント（右側）で比較したものだ。



出典：2022年版 中堅・中小企業のセキュリティ/運用管理/バックアップ利用実態と展望レポート（ノークリサーチ）

社内のエンドポイント（オフィス内で利用しているPCなど）ではパッケージ（マルウェア対策ソフトウェアを各PCにインストールするなど）が30.5%と最も高い値を示している。一方で、社外のエンドポイント（外出先や自宅で利用するPCやスマートデバイスなど）ではパッケージとサービス（端末側のエージェントを介してマルウェア対策やバックアップを提供するSaaSなど）が15～17%程度で拮抗している。

つまり、多くの中堅・中小企業はエンドポイントの守りのIT対策において、社内と社外で異なる実施手段を講じていることになる。昨今ではコロナ禍を通じて働く場所が多様化し、DXの取り組みを通じてオフィス外の様々な場面（工場、店舗、作業現場など）でのデータ活用が進みつつある。さらに、巧妙化する攻撃手法を防ぐためには社内/社外に関係なく、一貫したセキュリティ対策を展開するゼロトラストの発想も不可欠だ。エンドポイントにおける守りのIT対策を提供するベンダや販社/SIerには社内/社外の双方をカバーできる一貫したソリューションの提案が求められてくる。次頁では更なる分析結果について紹介している。

社外エンドポイントと社内の安全な通信手段では「サービス」が「アプライアンス」を上回る

本リリースの元となる調査レポートでは、以下のような項目を列挙して、守りのIT対策の「実施個所」毎にどのような「実施手段」を講じているか？を尋ねた結果を集計/分析している。

守りのIT対策の「実施個所」

エンドポイント（社内）：（※1）
社内で利用するPC、スマートフォン、タブレットなどの端末機器

エンドポイント（社外）：（※2）
在宅勤務中や外出中に利用するPC、スマートフォン、タブレットなどの端末機器

サーバ/ストレージ（社内）：
社内に設置されたサーバ/ストレージ機器

サーバ/ストレージ（社外）：
データセンタに設置されたサーバ/ストレージ機器、およびIaaS/ホスティング

社外エンドポイントと社内の通信：（※3）
在宅勤務中や外出中のPCから社内業務システムを利用する際のネットワーク環境

クラウドサービスと社内の通信：
SaaSなどのクラウドサービスと社内業務システムを連携させる際のネットワーク環境

前頁に掲載したグラフは（※1）と（※2）の「実施手段」を年商500億円未満の中堅・中小企業全体で集計した結果である。

守りのIT対策の「実施手段」

パッケージ：
ソフトウェアのパッケージを購入/導入している場合
例） PCにマルウェア対策のパッケージ製品をインストールしている

サービス：
クラウドなどのサービスを利用している場合
例） 不正アクセスを監視/防止するサービスをECサイトに適用している

アウトソース：
管理/運用の作業を外部に委託している場合
例） 業務システムが稼動するサーバの遠隔監視を業者に委託している

アプライアンス：
専用の機器を購入/設置している場合
例） 迷惑メールを検知/除去できるファイアーウォールを設置している

H/Wの付属機能：
ハードウェア（H/W）が持つ機能を利用している場合
例） PCが備えるデータ紛失時の遠隔データ削除機能を有効にしている

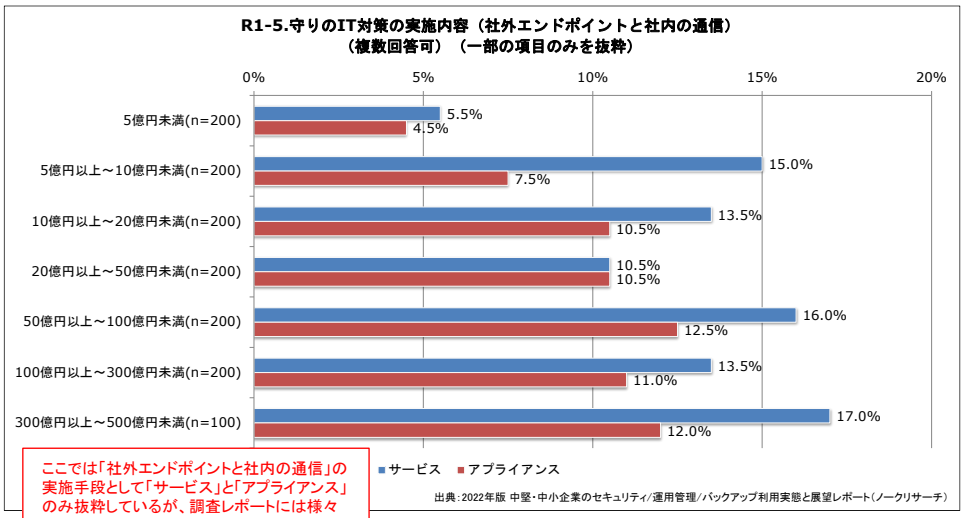
OSの付属機能：
OSに備わっている機能を利用している場合
例） Windows OSの「Windows Defender Antivirus」を利用している

不明：
対策を実施しているかどうか？の現状を把握していない場合

対策未実施：
対策を全く実施していない場合

該当なし：
上記のいずれにも該当しない場合（他の対策を講じているなど）

コロナ禍では在宅勤務中に社内へのVPN接続が切断/遅延するなどの事象も発生し、SASEを始めとする新たな接続手段にも注目が集まっている。そこで、「社外エンドポイントと社内の通信」（※3）の実施手段として「サービス」および「アプライアンス」と回答した割合を年商別に集計したものが以下のグラフだ。



ここでは「社外エンドポイントと社内の通信」の実施手段として「サービス」と「アプライアンス」のみ抜粋しているが、調査レポートには様々な守りのIT対策の実施手段を集計した結果が収録されている。

左記のグラフを見ると、多くの年商帯において「サービス」が「アプライアンス」を既に上回っていることがわかる。

実際に中堅・中小企業向けのセキュアなVPNサービスも多数存在している。

前頁で述べたように、今後は社内/社外を問わず一貫したエンドポイントの守りのIT対策が重要となる。その際は「どのようなエンドポイント形態を選ぶか？」の基本方針も深く関係してくる。次頁ではその点に関する分析結果の一部を紹介している。

クラウド型デスクトップ仮想化への移行も有効な対策、Device as a Serviceは啓蒙が必要

本リリースの元となる調査レポートでは以下のような選択肢を列挙して、守りのIT対策における今後の方針についても詳しい集計/分析を行っている。

<<自社の体制/人員に関する項目>>

・IT機器の管理/運用を遠隔支援するサービスを利用する

例） NEC「MAST」、大塚商会「たよれーる らくらくオフィスシリーズ」

・情シス部門の役割を外部委託できるサービスを利用する

例） Gizumo「クラウドSE」、デジタルハック「情シス君」、エイネット「情シス業務代行サービス」

・「CISO」として遠隔で助言してくれるサービスを利用する

例） セキュアベース「サイバーセキュリティ参謀」、株式会社CISO「経営者のためのセキュリティ参謀サービス」
「CISO」（Chief Information Security Officer）とは経営とITの双方の視点から企業における守りのIT対策をリードする職責を指す

・守りのIT対策に関する従業員向けの教育/訓練を行う

例） ラック「標的型攻撃メール訓練 T3 with セキュリティ教育」

<<エンドポイントに関する項目>>

・クラウド型のデスクトップ仮想化に移行していく

例） 日本マイクロソフト「Windows 365」「Azure Virtual Desktop」

・「Device as a Service」の利用を増やしていく

例） 日本HP「HP Device as a Service」、横河レンタ・リース「Cotoka for PC」、デル・テクノロジーズ「ゼロタッチPC for SMB」
「Device as a Service」とは端末を購入せずにサブスク形式で月額利用できるサービスを指す

・エンドポイントOSの標準機能を積極的に活用する

例） マルウェア対策ソフトウェアは導入せずに、Windows 11が備える「Windows Defender Antivirus」を利用する

・未知の攻撃でも防御できる製品/サービスを選ぶ

例） Blue Planet-works「AppGuard」（プログラムの動作を監視し、許可された正常な動作のみを認めることで未知の攻撃を防ぐ）

・従業員のIT活用を監視/制御できるサービスを利用する

例） Skyhigh Security（旧McAfee）「Skyhigh CASB（旧：MVISION Cloud）」（従業員のクラウド利用を監視/制御するCASB（Cloud Access Security Broker）に該当）

・端末が標準で備えている機能を積極的に活用する

例） 日本HP「HP Secure Erase」（PCの盗難/紛失が発生した際に、当該PCのデータを遠隔で削除する）

・アカウントやデータを集約管理できるサービスを利用する

例） Why「BUNDLE」（複数のクラウドサービスを利用する際のアカウントやファイル共有状況を把握し、アカウントやデータの一元管理を支援する）

<<サーバ/ストレージに関する項目>>

・守りのIT対策の手段としてサーバをクラウドに移行する

・災害や攻撃に強いデータバックアップ手法を利用する

例） デル・テクノロジーズ「PowerProtect」（バックアップデータをネットワークから隔離することで社内にランサムウェアが侵入した場合もデータを保全できるアプライアンス）

・オンラインストレージサービスを用いたデータ授受を行う

例） HENNGE「HENNGE Secure Download」（SaaS認証基盤「HENNGE One」の一機能）（パスワード付ZIPファイル添付の代わりに、メールに添付されたファイルをオンラインストレージサービスを介して相手と共有する）

次頁へ続く

前頁からの続き

<<**ネットワークに関する項目**>>

・「ボックス型ワーキングスペース」を積極的に活用する

例） 富士フイルムビジネスイノベーション「CocoDesk」
「ボックス型ワーキングスペース」とは駅構内などに設置された電話ボックス型設備で、時間貸しでインターネット接続可能な作業環境を利用できるサービスを指す

・社内外を安全/手軽に繋ぐクラウドサービスを利用する

例） ソニックウォール・ジャパン「SonicWall Edge Secure Access」（社内の様々な機器を仲介役となるクラウドサービスを介して接続することによって、社内にアクセスポイントのための機器などを設置しなくても社外から社内へのリモートアクセスなどを実現するサービス、SASE（Secure Access Service Edge）やZTNA（Zero Trust Network Access）と呼ばれることもある）

・国内企業が管理/運用する国内のデータセンタを選ぶ

海外の委託事業者が国内の個人情報を閲覧していた事案などを踏まえて、データセンタの設置場所だけでなく、管理/運用を担う業者が国内企業か？という点も考慮されるようになってきている

・「ゼロトラスト」を前提としたネットワーク対策を講じる

「ゼロトラスト」とは社内ネットワークもインターネットなどの社外と同じ危険度であると見なし、業務システムを利用する度にIT機器の認証を常に行うなど、社内と社外を包括的にカバーしたネットワーク対策を指す

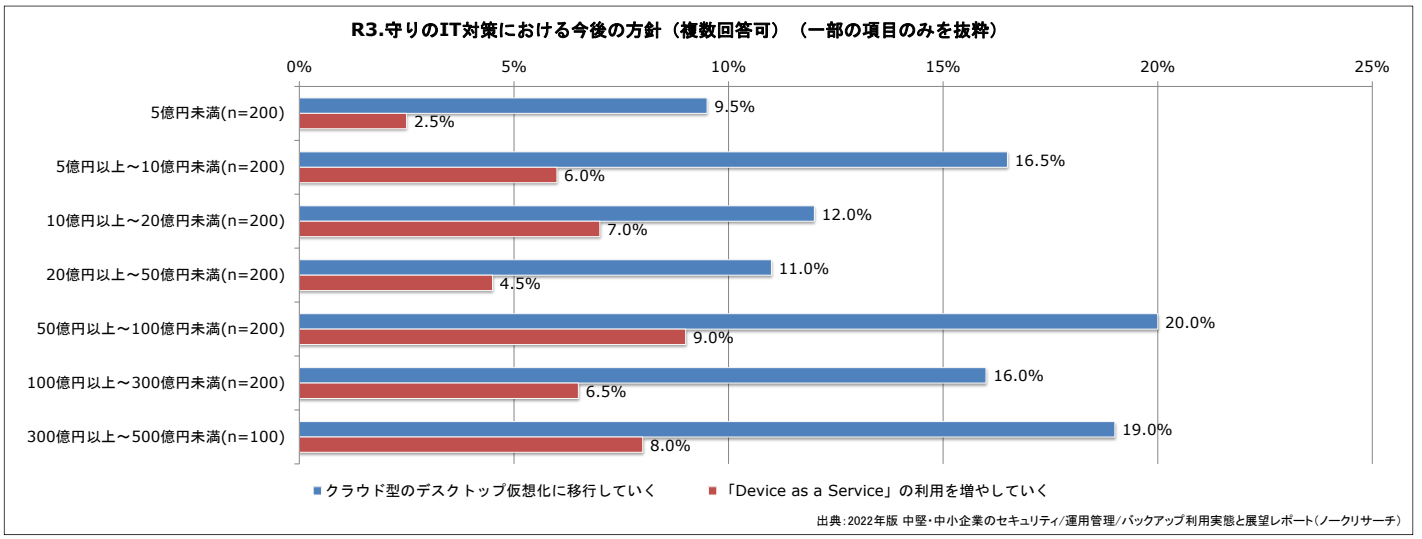
<<**その他**>>

・セキュリティ認証を受けている製品/サービスを選ぶ

クラウドサービスについてもクラウドサービスを対象としたセキュリティ認証「ISO27017」を取得するケースが増えている

・その他

以下のグラフは上記に列挙した守りのIT対策における今後の方針の中から、『クラウド型のデスクトップ仮想化に移行していく』と『「Device as a Service」の利用を増やしていく』の回答結果を年商別に集計したものだ。



デスクトップ仮想化（VDI）は既存のPC環境からの変化も大きく、事前の検証なども必要となるため、中堅・中小企業における導入割合はまだ低い。しかし、上記のグラフが示すように守りのIT対策という観点では有望な選択肢の一つと捉えられていることがわかる。一方、エンドポイント端末の調達から運用までを担う「Device as a Service」は社内/社外を問わず一貫したエンドポイント管理を実現する上でも有効な手段だ。だが、上記のグラフが示すように回答割合はデスクトップ仮想化と比べて低い。「Device as a Service」の考え方やサービス内容がまだ十分に認知されていないことが主な要因と考えられる。ベンダや販社/SIerがエンドポイントの守りのIT対策を訴求する際には、従来の社内設置型と比較して導入障壁の低い「クラウド型のデスクトップ仮想化」や「Device as a Service」といった新たなエンドポイント形態の啓蒙も並行して進めていくことが大切となってくる。

本リリースの元となる調査レポート

『2022年版 中堅・中小企業のセキュリティ/運用管理/バックアップ利用実態と展望レポート』

ランサムウェアの脅威、散在するアカウント、OSのアップデート管理、クラウドサービスに分散したデータ、ゼロトラストを前提としたネットワーク環境構築など、様々な課題を抱えた中堅・中小企業における守りのIT対策の実態と今後を詳説

【本調査レポートの背景】

セキュリティ/運用管理/バックアップといった守りのIT対策はユーザ企業がIT活用を安全かつ円滑に進める上で不可欠な取り組みだ。だが、その範囲は幅広く、ベンダや販社/SIerとしても「守りのIT対策の提案をどこから始めれば良いか？」の判断が難しくなっている。そこで、本調査レポートでは社内/社外のエンドポイントやサーバ/ストレージ、さらにはネットワークといったITインフラ全般の守りのIT対策の実施手段（パッケージ、サービス、アウトソース、アプライアンスなど）の実態を明らかにした上で、守りのIT対策においてユーザ企業が抱える課題や今後の方針を元に、ベンダや販社/SIerが今後注力すべき守りのIT活用の領域はどこか？を提言している。さらに、今後の守りのIT対策の主な担い手となるのは製品/サービスを提供するベンダなのか？それらをインテグレーションする販社/SIerか？、あるいはクラウド事業者か？についても分析を行っている。

【対象企業属性】（有効回答件数：1300社）

年商：　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

従業員数：　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～1,000人未満 / 1,000人以上～3,000人未満 / 3,000人以上～5,000人未満 / 5,000人以上

業種：　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(公共/自治体など)

地域：　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

その他の属性：「IT管理/運用の人員規模」（12区分）、「ビジネス拠点の状況」（5区分）

【分析サマリ（調査結果の重要ポイントを述べたPDFドキュメント）の章構成】

第1章.守りのIT対策の実施状況

6項目の実施個所（エンドポイント、サーバ/ストレージ、ネットワークなど）と8項目の実施手段（パッケージ、サービス、アウトソース、アプライアンスなど）の選択肢を設けて、ユーザ企業における守りのIT対策がどのように実施されているか？の実態を明らかにしている

第2章.守りのIT対策における課題

24項目に渡る選択肢を列挙し、ユーザ企業が守りのIT対策において直面している課題は何か？を分析している

第3章.守りのIT対策における基本方針

19項目に渡る選択肢を列挙し、ユーザ企業が守りのIT対策に取り組む際の基本方針を尋ねた結果を分析している

第4章.今後の導入を増やす/減らすIT企業

11区分の種別（セキュリティ主体のベンダ、運用管理主体のベンダ、バックアップ主体のベンダ、複合機系の販社/SIer、地場の販社/SIer、OSベンダ、クラウド事業者など）を列挙し、守りのIT対策の導入を増やす/減らすIT企業はどれか？を尋ねた結果を分析している

第5章.許容可能な年額合計費用

守りのIT対策に対して許容できる年額合計費用を尋ねた結果を俯瞰し、現状で抱える課題や今後の基本方針との関連を分析している

【発刊日】2023年1月16日　**【価格】** 180,000円(税別)

さらに詳細なレポート案内は右記を参照 https://www.norkresearch.co.jp/pdf/2022Sec_user_rep.pdf

DX関連、ITインフラ関連、販社/SIerのシェアと評価など、ご好評いただいているその他の調査レポートについては次頁を参照

ご好評いただいている2022年の新刊調査レポート　各冊180,000円（税別）

『2022年版 中堅・中小企業のDXソリューション導入実態と展望レポート』

DXを一部の先進企業から、中堅・中小の幅広い裾野に広げるために必要な施策を徹底解説

【レポートの概要と案内】https://www.norkresearch.co.jp/pdf/2022IT_user_rep.pdf

【リリース(ダイジェスト)】

ユーザ企業(利用側)とIT企業(提案側)が抱えるDXソリューション導入の共通課題
https://www.norkresearch.co.jp/pdf/2022IT_user_rel1.pdf

業種別に見た「中堅・中小企業の導入が今後増えるDXソリューション」とは？
https://www.norkresearch.co.jp/pdf/2022IT_user_rel2.pdf

中堅・中小企業におけるIT投資市場規模とITソリューション支出額
https://www.norkresearch.co.jp/pdf/2022IT_user_rel3.pdf

伴走型SI/サービスは中堅・中小企業とIT企業の新しい関係性となるか？
https://www.norkresearch.co.jp/pdf/2022IT_user_rel4.pdf

メタバースやブロックチェーンなどの最新技術に対する企業の受容性動向
https://www.norkresearch.co.jp/pdf/2022IT_user_rel5.pdf

『2022年版 サーバ＆エンドポイントにおけるITインフラ導入/運用の実態と展望レポート』

サーバ＆エンドポイント、クラウド＆オンプレミスといった多角的な視点からITインフラ導入の提案ポイントを解説

【レポートの概要と案内】https://www.norkresearch.co.jp/pdf/2022SrvPC_user_rep.pdf

【リリース(ダイジェスト)】

サーバ管理における課題＆ニーズとユーザ企業が求めるクラウド移行パターン
https://www.norkresearch.co.jp/pdf/2022SrvPC_user_rel1.pdf

サーバ導入の注目トピック（オフコン移行/CentOS 8代替/クラウド社数シェア）の動向
https://www.norkresearch.co.jp/pdf/2022SrvPC_user_rel2.pdf

企業規模別に見たサーバインスタンス数とストレージ形態の傾向
https://www.norkresearch.co.jp/pdf/2022SrvPC_user_rel3.pdf

エンドポイント端末(PC/スマートデバイス)の導入実態が示す有望な販売施策
https://www.norkresearch.co.jp/pdf/2022SrvPC_user_rel4.pdf

PC/スマートデバイスのシェア動向とITインフラ全体に影響する課題
https://www.norkresearch.co.jp/pdf/2022SrvPC_user_rel5.pdf

『2022年版 中堅・中小企業のIT支出と業務システム購入先の実態レポート』

中堅・中小企業は”どの販社/SIer”から”何のIT商材やソリューション”を”幾らの金額”で導入/購入しているか？を徹底分析

【レポートの概要と案内】https://www.norkresearch.co.jp/pdf/2022SP_usr_rep.pdf

【リリース(ダイジェスト)】

中堅・中小企業が選ぶIT商材/ソリューションの購入先/委託先
https://www.norkresearch.co.jp/pdf/2022SP_usr_rel1.pdf

年商別と販社/SIer別に見た25項目に渡るDX、業務アプリ、ハードウェア、クラウド、アウトソースの導入割合
https://www.norkresearch.co.jp/pdf/2022SP_usr_rel2.pdf

中堅・中小企業から見たベンダや販社/SIerの評価点および不満点
https://www.norkresearch.co.jp/pdf/2022SP_usr_rel3.pdf

中堅・中小企業におけるIT商材/ソリューション別の年間IT支出額と市場規模
https://www.norkresearch.co.jp/pdf/2022SP_usr_rel4.pdf

当調査データ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