PRESS RELEASE（報道関係者各位）

2022年2月24日

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

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：伊嶋謙二 TEL：03-5361-7880
URL：http//www.norkresearch.co.jp）は中堅・中小企業のバックアップ対策がセキュリティ（例. ランサムウェア攻撃からの防御）や運用管理（例. OSサポート終了に伴うサーバインフラ更新）とどう関連しているか？の調査結果を発表した。本リリースは「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」のサンプルならびにダイジェストである。

＜セキュリティや運用管理の動向も踏まえながら、バックアップの必要性を啓蒙することが大切＞
■バックアップ製品/サービスの導入割合はセキュリティと比べて低く、今後の改善が不可欠
■業務データ量が少ない企業においてもバックアップ対策ニーズを活性化させることが急務
■「ランサムウェア攻撃対策」や「HCI導入」はバックアップの必要性を訴求できる重要な場面

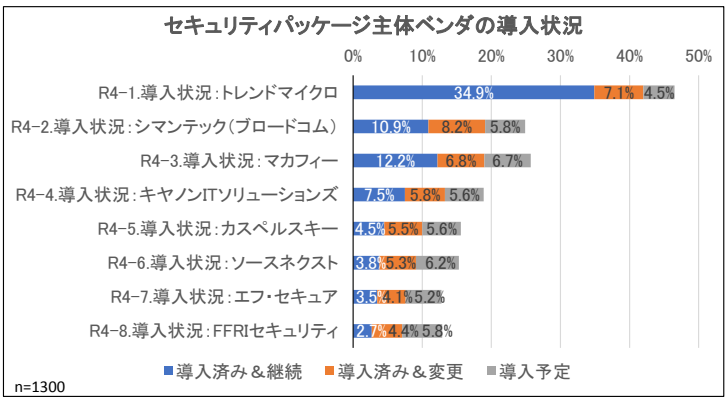
対象企業：　年商500億円未満の中堅・中小企業1300社（日本全国、全業種）（有効回答件数）
対象職責：　情報システムの導入や運用/管理または製品/サービスの選定/決済の権限を有する職責
調査期間：　2021年6月～7月
※調査対象の詳しい情報については本リリースの末尾を参照

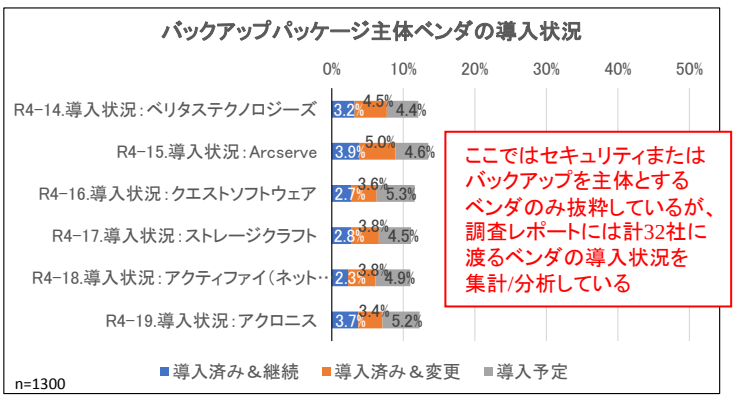
バックアップ製品/サービスの導入割合はセキュリティと比べて低く、今後の改善が不可欠

本リリースの元となる調査レポートでは「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」、「その他のパッケージ（Webフィルタリングや操作ログ分析など）主体」、「大手のITベンダ/SIer」の5グループ、計32社に渡るベンダを列挙し、以下のような選択肢を設けて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

以下のグラフは上記の中からセキュリティパッケージおよびバックアップパッケージを主体とするベンダの導入状況を中堅・中小企業全体で集計したものだ。（調査対象となっているベンダの一覧は本リリースの4頁を参照）





出典：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（ノークリサーチ）

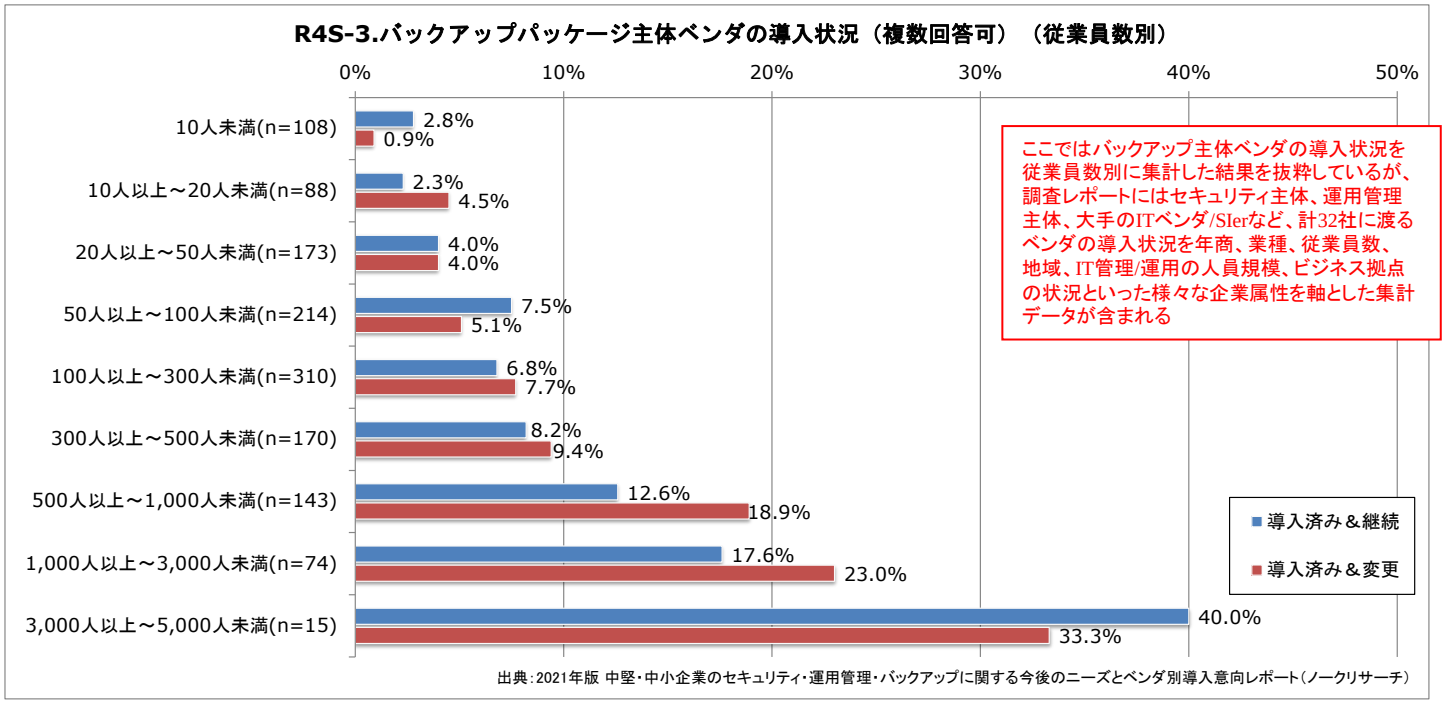
セキュリティパッケージ主体のベンダと比べると、バックアップベンダ主体のベンダは「導入済み」の回答割合が低くなっている。だが、中堅・中小企業を取り巻くビジネス環境の変化（業務に用いるデータの増加など）やシステム環境の変化（クラウドの普及など）を踏まえると、単なるファイルコピーに留まらないバックアップ対策の取り組みが不可欠となってくる。本リリースの元となる調査レポートではセキュリティや運用管理といった他の守りのIT対策との関連性を分析しながら、中堅・中小企業向けにバックアップ製品/サービスを訴求するための施策を提言している。次頁以降ではその一部をサンプル/ダイジェストとして紹介する。

業務データ量が少ない企業においてもバックアップ対策ニーズを活性化させることが急務

前頁のグラフ「パッケージ主体ベンダの導入状況」を見ると、「導入済み（継続と変更の合計）」の割合はトレンドマイクロが4割超で最も高く、シマンテック（ブロードコム）とマカフィーが2割弱で続いており、これらが3強と言える状況となっている。だが、「導入予定」の割合はいずれのベンダも5%前後に留まっている一方、上位3社のベンダは4位以下と比べて「導入済み＆変更」の割合が若干高くなっている。そのため、今後は上位3社と4位以下のシェア差が少しずつ縮まっていく可能性がある。

本リリースの元となる調査レポートには前頁の結果を年商、業種、従業員数、地域、IT管理/運用の人員規模、ビジネス拠点の状況といった様々な企業属性を軸とした集計データが含まれる。以下のグラフはその中からバックアップパッケージ主体ベンダの導入状況（「導入済み＆継続」および「導入済み＆変更」）を従業員数別に集計した結果を以下の選択肢によって一つの複数回答設問にまとめたものである。

・導入済み＆継続　　少なくとも1つのバックアップパッケージ主体ベンダについて、「導入済み＆継続」と回答している場合
・導入済み＆変更　　少なくとも1つのバックアップパッケージ主体ベンダについて、「導入済み＆変更」と回答している場合
・導入予定　　少なくとも1つのバックアップパッケージ主体ベンダについて、「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



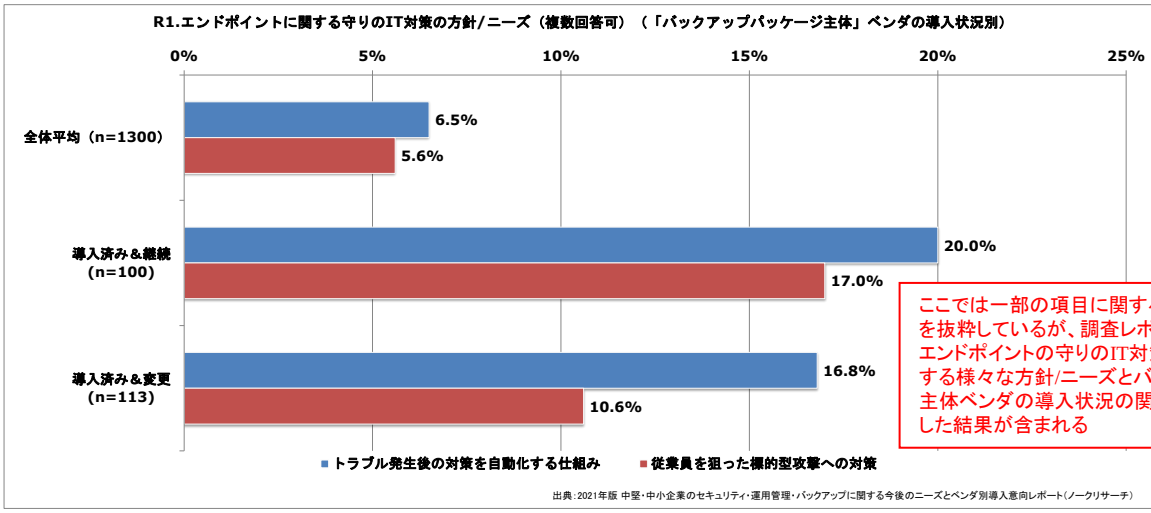
バックアップ主体ベンダの導入割合は従業員数規模によって大きく異なることが確認できる。従業員数が多くなれば企業規模も大きくなり、企業規模が大きくなれば業務データ量も増加する。業務データ量が多ければ、バックアップ対策ニーズも高まるため結果的に従業員数規模がバックアップ主体ベンダの導入状況に大きく影響することになる。

だが、業務データ量が少なかったとしても、その重要度が高ければ適切かつ十分なバックアップ対策が必要となる。今後はDXに向けた取り組みによって中堅・中小企業の業務データ量も増加していくことが予想される。しかし、その増加スピードを上回る勢いで企業の業務データを狙った攻撃のリスクも高まっている。

そのためバックアップ製品/サービスを開発/販売するベンダや販社/SIerとしては「業務データ量の増加」だけでなく、セキュリティ対策に伴うバックアップの必要性を早期に啓蒙し、ニーズを活性化させることが急務となってくる。次頁ではそうした観点からの分析結果の一部を調査レポートから抜粋して紹介している。

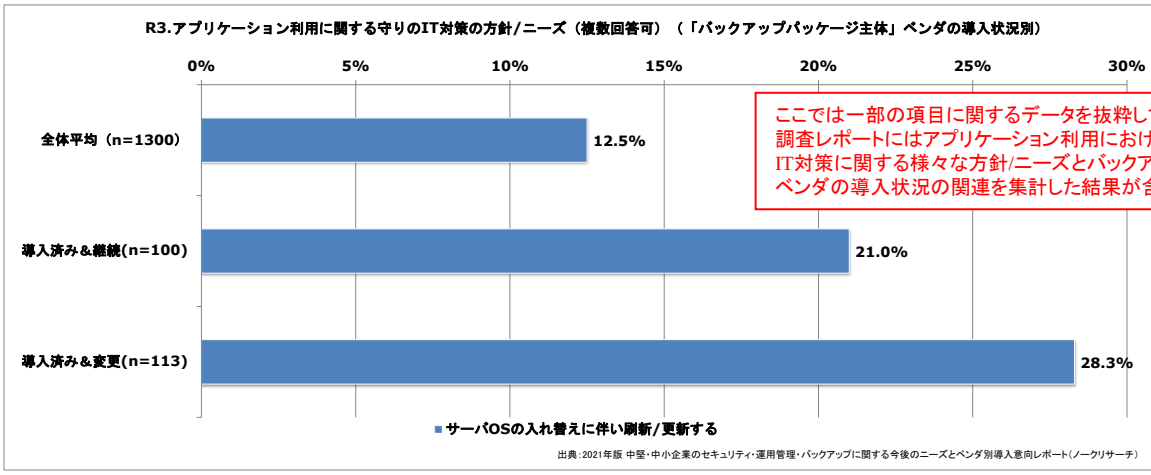
「ランサムウェア攻撃対策」や「HCI導入」はバックアップの必要性を訴求できる重要な場面

本リリースの元となる調査レポートでは、エンドポイントやアプリケーション利用における守りのIT対策に関する方針/ニーズを本リリース5頁に記載した様々な選択肢によって尋ねている。以下のグラフは「バックアップ主体ベンダの導入状況」と「エンドポイントの守りのIT対策の方針/ニーズ」の関連性を集計した結果のうち、特に留意すべき項目を抜粋したものだ。



PCなどのエンドポイントを対象とした守りのITにおける方針/ニーズのうち、「トラブル発生後の対策を自動化する仕組み」や「従業員を狙った標的型攻撃への対策」は全体平均と比べてバックアップ主体ベンダを「導入済み＆継続」または「導入済み＆変更」の場合に高い回答割合を示している。つまり、標的型攻撃対策やトラブル発生後の対処（例. ランサムウェア攻撃を受けた場合の速やかなデータ復旧など）を重視するユーザ企業はバックアップ対策も進んでいることがわかる。したがって、バックアップ製品/サービスを訴求するベンダや販社/SIerにとっては、世界的にも増加傾向にあるランサムウェア攻撃対策の一貫としてバックアップの重要性を訴えていくことも重要となってくる。

また、以下のグラフは「バックアップ主体ベンダの導入状況」と「アプリケーション利用における守りのIT対策の方針/ニーズ」の関連性を集計した結果のうち、特に留意すべき項目を抜粋したものだ。



アプリケーション利用における方針/ニーズのうち、「サーバOSの入れ替えに伴い刷新/更新する」の回答割合は全体平均と比べて「導入済み＆変更」において大幅に高くなっている。サーバOSのサポート終了を契機とした更新時には、HCIのような分散型のサーバ構成も新たなバックアップ需要を生み出す契機となりうる。上記の結果にはこうした「サーバ構成の変化」と「バックアップ対策ニーズ」の関連性も影響していると考えられる。バックアップ製品/サービスを訴求する際にはこうした側面にも着目することが大切だ。本リリースの元となる調査レポートではこうした分析を通じて、バックアップ対策ニーズを活性化させる施策に関する提言を述べている。

補記1:導入状況の調査対象となっているベンダー一覧

本リリースの元となる調査レポートでは「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」、「その他のパッケージ(Webフィルタリングや操作ログ分析など)主体」、「大手のITベンダ/SIer」の5グループ、計32社に渡るベンダを列挙し、以下のような選択肢を設けて導入状況を尋ねている。

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

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調査レポートにおけるR4-1～R4-33の設問に対応している。「」内は各ベンダの代表的な製品/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

補記2：守りのIT対策における方針/ニーズに関する選択肢一覧

本リリースの元となる調査レポートでは、エンドポイントやアプリケーション利用における守りのIT対策に関する方針/ニーズを以下の様々な選択肢で尋ねている。（調査レポートにはエンドポイントとアプリケーション利用に加えて、サーバ/ネットワークの守りのIT対策についても方針/ニーズの集計/分析を行っている、詳細は本リリース末尾にURLを記載した「レポート案内」参照）

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。

<<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
・複数ベンダの製品/サービスを適宜使い分ける
・新型コロナ感染症対策に伴い刷新/更新する
・Windows 10への移行に伴い刷新/更新する
・働き方改革への対応に伴い刷新/更新する
・親会社や取引会社からの要請で刷新/更新する
・BCP(事業継続計画)の策定に伴い刷新/更新する
・社内サーバが不要なクラウドサービスへ移行する
・守りのIT対策を推進する社内人材を育成する
・守りのIT対策を推進する社外人材を利用する

<<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
・在宅勤務をする従業員のPCを管理できる仕組み
・社外で使用するPC内にデータを残さない仕組み
・様々なクラウドサービスを統合管理する仕組み
・クラウドサービスの設定を確認/改善する仕組み
・リモートで顧客と安全/円滑に対話できる仕組み
・Windows10の更新プログラムを制御する仕組み
・スマートデバイスとPCを統合管理できる仕組み
・トラブル発生後の対策を自動化する仕組み
・不正アクセス発生後の被害拡大を防ぐ対策
・顔や指紋などの生体認証技術への対応
・災害時に業務を継続するための仕組み
・従業員を狙った標的型攻撃への対策

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。

<<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
・複数ベンダの製品/サービスを適宜使い分ける
・新型コロナ感染症対策に伴い刷新/更新する
・Windows 10への移行に伴い刷新/更新する
・サーバOSの入れ替えに伴い刷新/更新する
・働き方改革への取り組みに伴い刷新/更新する
・親会社や取引会社からの要請で刷新/更新する
・BCP(事業継続計画)の策定に伴い刷新/更新する
・社内サーバが不要なクラウドサービスへ移行する

<<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
・利用可能なアプリケーションを制限/管理する仕組み
・様々なクラウドサービスの安全性を評価するサービス
・セキュリティ全般に関する従業員向け教育サービス
・プライバシーマークなどの公的な認定の取得支援
・複数のID/アカウントを統合管理する仕組み
・ID/アカウントをクラウド上で管理する仕組み
・データをクラウド上にバックアップする仕組み
・データを社内にバックアップする仕組み
・トラブル発生後の対策を自動化する仕組み
・不正アクセス発生後の被害拡大を防ぐ対策
・災害時に業務を継続するための仕組み

本リリースの元となる調査レポート

『2021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』

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

【レポート案内】サンプル属性、設問項目、試読版などの詳細

https://www.norkresearch.co.jp/pdf/2021Sec_usr_rep.pdf

【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)

【分析サマリの概要】集計データにおける重要ポイントを解説し、ベンダや販社/SIerが今後注力すべきポイントを提言

第1章:本調査レポートの背景と構成
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
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
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
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
第6章:守りのITに対して許容できる年額の合計費用

【価格】 180,000円(税別)　　**【発刊日】** 2022年2月28日

ご好評いただいているその他の調査レポート

「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NW活用を普及させるためには何が必要か？
レポート案内: https://www.norkresearch.co.jp/pdf/2021NW_user_rep.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とユーザ評価を照合分析し、DX時代の販社/SIer像を明らかにする
レポート案内: https://www.norkresearch.co.jp/pdf/2021SP_usr_rep.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