ランサムウェアの危険性を訴えるだけでなく、今後のIT活用方針とマッチした「ポジティブな守りのIT対策提案」が求められている

2023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

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/所在地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. **収録されている集計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

本調査レポートでは以下のような属性に合致する1300件(有効回答件数)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(有効回答件数)

A1.年商区分:　5億円未満(200社) / 5億円以上～10億円未満(200社) / 10億円以上～20億円未満(200社) / 20億円以上～ 50億円未満(200社) / 50億円以上～ 100億円未満(200社) / 100億円以上～ 300億円未満(200社) / 300億円以上～ 500億円未満(100社)

A2.職責区分:　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

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

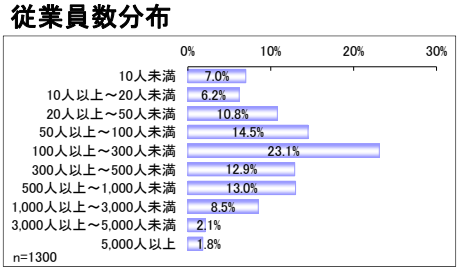
A5.所在地区分:　北海道地方 / 東北地方 / 関東地方 / 北陸地方 / 中部地方 / 近畿地方 / 中国地方 / 四国地方 / 九州・沖縄地方

調査実施時期:　2023年7月～8月

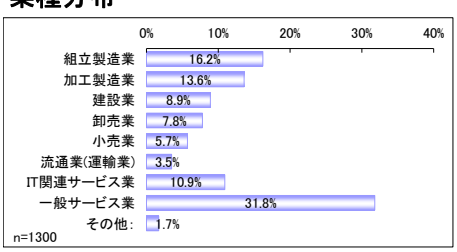
上記に加えて、**「A6.IT管理/運用の人員規模」**(IT管理/運用を担う人材は専任/兼任のいずれか？人数は1名/2～5名/6～9名/10名以上のどれに当てはまるか？)および**「A7.ビジネス拠点の状況」**(オフィス、営業所、工場などの数は1ヶ所/2～5ヶ所/6ヶ所以上のいずれか？ITインフラ管理は個別/統一管理のどちらか？)といった属性についても尋ねており、A1～A7を軸として以降に述べる全ての設問を集計したデータが含まれる。

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。

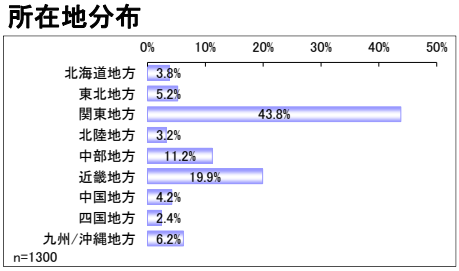
従業員数分布



業種分布



所在地分布



価格:　￥180,000円(税別)
発刊日:　2024年1月22日
お申込み方法:　弊社ホームページから、またはinform@norkresearch.co.jp宛にご連絡ください

本調査レポートの背景

近年では大企業のみならず、中堅・中小企業にとってもランサムウェアに代表される情報セキュリティ面の脅威が重要な経営課題の一つとなっている。攻撃手法も日々巧妙化しているため、IT企業としては最新の「守りのIT対策」を訴求・啓蒙していく必要がある。しかし、最新のセキュリティ対策への更新・刷新を促進するためには悪意のある攻撃という「脅威」を訴えるだけでなく、業績改善に寄与する「攻めのIT活用」との兼ね合いも考慮した「守りのIT対策」の提案を進めていくことが大切だ。
本調査レポートではセキュリティ/運用管理/バックアップといった「守りのIT対策」の実施状況、現状の課題、今後のニーズに加えて、業務アプリケーションの活用方針といった「攻めのIT活用」と「守りのIT対策」との関連性についても集計/分析を行い、IT企業が「守りのIT対策」の提案において一歩差をつけるために取り組むべき事柄は何か？を提言している。

分析サマリの章構成

本調査レポートは調査結果の要点と提言を記載した「分析サマリ」（PDF形式）と多数の集計データ（Microsoft Excel形式）で構成されている。集計データには3ページ以降に列挙した各設問を様々な観点で集計した結果が収録されている。それらの詳細は8ページの「本調査レポートの集計データ」で述べる。一方、分析サマリは以下の6つの章から構成されている。

第1章：守りの IT 対策を実施している箇所と内容

守りのIT対策を実施する箇所として、エンドポイント（社内 or 社外）、サーバ/ストレージ（社内 or 社外）、社外エンドポイントと社内の通信、クラウドサービスと社内の通信の計6項目を提示し、対策の実施内容（＝手段）としてパッケージ、サービス、アウトソース、アプライアンス、H/Wの付属機能、OSの付属機能のどれを講じているか？を尋ねた結果を集計/分析。

第2章：守りのIT対策の最も主要な導入元と評価点/満足点

守りのIT対策の最も主要な導入元として、IT商材の購入/導入における「最も主要な委託先/購入先（プライムの販社/SIer）」、「主要ではない委託先/購入先」、「製品/サービス毎に開発元から購入」の3通りの中のどれが最も近いか？を尋ねた上で、そこから導入している守りのIT対策に関して評価/満足している機能や特徴（計23項目）を尋ねた結果（※1）を集計/分析。
「最も主要な委託先/購入先」のうち、以下に列挙した12社の販社/SIerについては、販社/SIer毎に（※1）の項目を集計した結果も掲載。

※1の集計対象となっている販社/SIer：大塚商会、NTTデータ（系列企業を含む）、オービック、NTTコミュニケーションズ（系列企業を含む）、富士通Japan（富士通マーケティング、富士通エフ・アイ・ピー）、リコー（系列企業も含む）、富士ソフト、富士通（関連会社や子会社を除く）、富士フイルムビジネスイノベーション（富士ゼロックス）、NECソリューションイノベータ、キヤノンマーケティングジャパン（系列企業を含む）、NECネクサソリューションズ

第3章：守りのIT対策において現状で抱えている課題

計23項目に渡る選択肢を列挙し、守りのIT対策においてどのような課題を抱えているか？を集計/分析。

第4章：守りのIT対策の製品/サービスが今後持つべき機能や特徴

計23項目に渡る選択肢を列挙し、守りのIT対策を担う製品/サービスに対するニーズ（機能や特徴）は何か？を集計/分析。
さらに、API連携などの機能面、法制度対応、生成AIなど、計22項目に渡る業務アプリケーションの導入/更新に関する方針と守りのIT対策における今後のニーズとの関連についても分析。

第5章：守りのIT対策の開発元

セキュリティを主体としたベンダ、運用管理/資産管理を主体としたベンダ、バックアップ/リストアを主体としたベンダ、その他のベンダ（SSO、WAF、Webフィルタリングなど）、ネットワーク関連が主体のベンダ、総合ベンダの計6カテゴリ、合計51社に渡る守りのIT対策のベンダを列挙し、既に導入済みの製品/サービスの開発元はどれか？を尋ねた結果を集計/分析。
（集計対象となっているベンダの一覧は7ページを参照）

第6章：守りのIT対策における費用

守りのIT対策に対して許容可能な年額合計費用を尋ねた結果を集計/分析。
ここでの年額合計費用とはハードウェアと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製品/サービス（ソフトウェア、アプライアンス、クラウドサービス）を導入/利用する上で必要となる年額の合計費用を指す。

本調査レポートの設問項目（1/5）

本調査レポートの設問はR1～R7の計7項目で構成されており、R1はさらにR1-1～R1-6の計6つの枝番設問に細分化されている。以下ではこれらの設問の構成や内容について列挙していく。R7以外の設問はいずれも与えられた選択肢から回答を選ぶ「選択肢設問」、R7は守りのIT対策に対して許容可能な年額合計費用を数値で記入する「数値記入設問」となっている。

R1. 守りのIT対策を実施している箇所と内容（複数回答可）

セキュリティ/運用管理/バックアップといった守りのIT対策の現状を「実施箇所」（何処に対策を講じているか？）と「実施内容」（どのような手段で対策を講じているか？）の2つの観点から尋ねた設問である。各々の観点における項目内容は以下の通りである。

実施箇所：

エンドポイント（社内）：	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）：	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：	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

実施内容：

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）

設問R1は6つの枝番設問で構成されており、上記に列挙した6つの実施箇所がR1-1～R1-6の枝番設問に対応する。各々の枝番設問では上記に列挙した9項目の実施内容が選択肢として設定されている。実施内容では複数の選択肢を選ぶことができるが、「不明」「対策未実施」「該当なし」のいずれかを選んだ場合には他の選択肢を選ぶことはできない（排他選択肢）。

R1-1.守りのIT対策の実施内容（エンドポイント（社内））（複数回答可）

選択肢「パッケージ」「サービス」「アウトソース」「アプライアンス」「H/Wの付属機能」「OSの付属機能」「不明」「対策未実施」「該当なし」

R1-2.守りのIT対策の実施内容（エンドポイント（社外））（複数回答可）

選択肢「パッケージ」「サービス」「アウトソース」「アプライアンス」「H/Wの付属機能」「OSの付属機能」「不明」「対策未実施」「該当なし」

R1-3.守りのIT対策の実施内容（サーバ/ストレージ（社内））（複数回答可）

選択肢「パッケージ」「サービス」「アウトソース」「アプライアンス」「H/Wの付属機能」「OSの付属機能」「不明」「対策未実施」「該当なし」

次頁へ続く

本調査レポートの設問項目(2/5)

前頁からの続き

R1-4.守りのIT対策の実施内容(サーバ/ストレージ(社外))(複数回答可)

選択肢「パッケージ」「サービス」「アウトソース」「アプライアンス」「H/Wの付属機能」「OSの付属機能」「不明」「対策未実施」「該当なし」

R1-5.守りのIT対策の実施内容(社外エンドポイントと社内の通信)(複数回答可)

選択肢「パッケージ」「サービス」「アウトソース」「アプライアンス」「H/Wの付属機能」「OSの付属機能」「不明」「対策未実施」「該当なし」

R1-6.守りのIT対策の実施内容(クラウドサービスと社内の通信)(複数回答可)

選択肢「パッケージ」「サービス」「アウトソース」「アプライアンス」「H/Wの付属機能」「OSの付属機能」「不明」「対策未実施」「該当なし」

R2. 守りのIT対策の最も主要な導入元

セキュリティ/運用管理/バックアップといった守りのIT対策に関連する製品/サービスを最も多く導入しているIT企業を尋ねた設問である。多くの場合、こうしたIT企業はIT商材全般を最も多く導入している委託先/購入先(プライムの販社/SIer)と一致することが多いため、本設問の選択肢としては以下の3通りを設けている。(「守りのIT対策に関連する製品/サービス」とはハードウェアやOS/ファームウェアといったシステム基盤を除いたセキュリティ/運用管理/バックアップを担うソフトウェア、アプライアンス、クラウドサービスを指す)

・最も主要な委託先/購入先(プライムの販社/SIer)
・主要ではない委託先/購入先
・製品/サービス毎に開発元から購入

R3. 守りの IT 対策に関して評価/満足している機能や特徴(複数回答可)

設問R2で回答した最も主要な導入元から導入した守りのIT対策に関して評価/満足している機能や特徴を以下の選択肢(計23項目)で尋ねた設問である。

<<セキュリティ全般>>
・具体策を例示しながら、「ゼロトラスト」を提案してくれる
・社内外で端末を安全/最新な状態に保つことができる
・権限を制限/分割して不正アクセス被害を局所化できる
・メールによる秘匿情報の漏えいや誤送信を防止できる

<<マルウェア対策>>
・標的型攻撃を想定した実地訓練サービスを利用できる
・異常な振る舞いを元に未知のマルウェアも検知できる
・侵入したマルウェアを封じ込めて隔離し、無力化する
・サーバや高性能な端末が不要なクラウド形態である
・運用/保守のアクセス回線にもマルウェア対策が施せる
・PCに加えてスマートデバイスも一括で管理/保護できる

<<アカウント管理>>
・特権/管理アカウントは運用条件を厳しく設定できる
・未使用の放置アカウントを自動的に検出/停止できる
・複数システムのアカウントを集約して一括管理できる
・生体認証または多要素/二段階認証に対応している

<<バックアップ/リストア>>
・バックアップだけでなく、復元の検証も行ってくれる
・ネットワークから隔離してバックアップを保管できる
・クラウド上にシステムとデータを複製して保管できる
・検索/参照が容易な状態で大量データを保管できる

<<運用管理/資産管理>>
・端末の操作ログを記録して、不正や攻撃を防止できる
・OS更新の状況を可視化して、更新を自動で制御できる
・脆弱性やサポート期限への対処方法を提示してくれる
・無駄なライセンスがないかを自動で検索/一覧できる

<<その他>>
・個人情報保護に関する認証取得の支援も付属している
・その他:
・評価/満足している機能や特徴は全くない(排他)

次頁へ続く

本調査レポートの設問項目（3/5）

前頁からの続き

本調査レポートの分析サマリでは「設問R2.守りのIT対策の最も主要な導入元」で「最も主要な委託先/購入先」を選択した場合について、以下に列挙された具体的な販社/SIer毎に「設問R3.守りの IT 対策に関して評価/満足している機能や特徴」の集計/分析も行っている。

設問R3の結果を企業毎に集計している「最も主要な委託先/購入先」の一覧（計12社）

・大塚商会
・NTTデータ（系列企業を含む）
・オービック
・NTTコミュニケーションズ（系列企業を含む）、
・富士通Japan（富士通マーケティング、富士通エフ・アイ・ピー）
・リコー(系列企業も含む)
・富士ソフト
・富士通（関連会社や子会社を除く）
・富士フイルムビジネスイノベーション（富士ゼロックス）
・NECソリューションイノベータ
・キヤノンマーケティングジャパン(系列企業を含む)
・NECネクサソリューションズ

上記の販社/SIerは姉妹編となる調査レポート「2023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」でIT商材全般における「最も主要な委託先/購入先」を尋ねた結果のうち、設問R2の「最も主要な委託先/購入先」の回答件数が多かった上位12社を抽出したものだ。つまり、本調査レポートの分析サマリではIT商材全般における主要な委託先/購入先であり、かつ守りのIT対策においても主要な委託先/購入先となっている12社について、中堅・中小企業から見た評価点/満足点（設問R3の結果）を集計/分析している。

R4. 守りのIT対策において現状で抱えている課題（複数回答可）

セキュリティ/運用管理/バックアップといった守りのIT対策において現時点で抱えている課題は何か？を以下の選択肢（計23項目）で尋ねた設問である。

<<セキュリティ全般>>
・「ゼロトラスト」を提唱しているが、具体策が分からない
・社内外で対策が異なり、安全/最新の状態が保てない
・管理権限が強いため、乗っ取られた時の被害が大きい
・メールによる情報漏えい/誤送信の対策を講じていない

<<マルウェア対策>>
・標的型攻撃の被害や危険性が十分に周知されていない
・未知のマルウェアに対処できる仕組みが備わっていない
・マルウェアに侵入された時、隔離/無力化する手段がない
・サーバ導入が必須、もしくは端末側の処理が重い/遅い
・運用/保守のアクセス回線はマルウェア対策が不十分
・スマートデバイスの対策が不十分、またはPCと異なる

<<アカウント管理>>
・特権/管理アカウントの悪用を防ぐ施策を講じていない
・未使用のアカウントが削除されずに放置されている
・システム毎に複数のアカウントが散在/乱立している
・生体認証や多要素/二段階認証に対応できていない

<<バックアップ/リストア>>
・バックアップを復元できるかの検証を実施していない
・LANなどを介してバックアップが消される恐れがある
・システムやデータを安全なクラウド上に保管できない
・保管した大量データを容易に検索/参照できない

<<運用管理/資産管理>>
・端末の不正操作や故意の情報漏えいを防止できない
・OS更新の現状が把握できず、管理/制御もできない
・脆弱性やサポート期限への対策を講じられていない
・ライセンスの利用状況を把握しておらず、無駄が多い

<<その他>>
・個人情報保護に関する認証取得の方法が分からない
・その他：
・課題は全くない（排他）

次頁へ続く

本調査レポートの設問項目（4/5）

R5. 守りのIT対策の製品/サービスが今後持つべきと考える機能や特徴（複数回答可）

セキュリティ/運用管理/バックアップといった守りのIT対策を担う製品/サービスが今後どのような機能や特徴を持つべきか？（今後のニーズ）を以下の選択肢（計23項目）で尋ねた設問である。（排他選択肢を除き、選択肢は設問R3と共通）

<<セキュリティ全般>>
- 具体策を例示しながら、「ゼロトラスト」を提案してくれる
- 社内外で端末を安全/最新な状態に保つことができる
- 権限を制限/分割して不正アクセス被害を局所化できる
- メールによる秘匿情報の漏えいや誤送信を防止できる

<<マルウェア対策>>
- 標的型攻撃を想定した実地訓練サービスを利用できる
- 異常な振る舞いを元に未知のマルウェアも検知できる
- 侵入したマルウェアを封じ込めて隔離し、無力化する
- サーバや高性能な端末が不要なクラウド形態である
- 運用/保守のアクセス回線にもマルウェア対策が施せる
- PCに加えてスマートデバイスも一括で管理/保護できる

<<アカウント管理>>
- 特権/管理アカウントは運用条件を厳しく設定できる
- 未使用の放置アカウントを自動的に検出/停止できる
- 複数システムのアカウントを集約して一括管理できる
- 生体認証または多要素/二段階認証に対応している

<<バックアップ/リストア>>
- バックアップだけでなく、復元の検証も行ってくれる
- ネットワークから隔離してバックアップを保管できる
- クラウド上にシステムとデータを複製して保管できる
- 検索/参照が容易な状態で大量データを保管できる

<<運用管理/資産管理>>
- 端末の操作ログを記録して、不正や攻撃を防止できる
- OS更新の状況を可視化して、更新を自動で制御できる
- 脆弱性やサポート期限への対処方法を提示してくれる
- 無駄なライセンスがないかを自動で検索/一覧できる

<<その他>>
- 個人情報保護に関する認証取得の支援も付属している
- その他：
- 欲しいと考える機能や特徴は全くない（排他）

本調査レポートの分析サマリでは、姉妹編となる調査レポート「2023年版 中堅・中小企業のITアプリケーション利用実態と評価レポート」（※）における以下の設問「P0.業務アプリケーションの導入/更新に関する全体的な方針」の選択肢毎に設問R5を集計した結果も分析している。（設問P0を年商/業種などで集計した結果は本調査レポートには含まれず、※に収録されている）

P0.業務アプリケーションの導入/更新に関する全体的な方針（複数回答可）

<<機能に関連する項目>>
- APIを用いた他社との連携/協業が活発か？を重視する
- 自動化によって業務効率を改善できるか？を重視する
- 個別カスタマイズが不要なアプリケーションを優先する
- データ分析による高度な判断が行えるか？を重視する
- 顧客や取引先と遠隔で対話できるか？を重視する
- 従業員の働きやすさに貢献できるか？を重視する
- 必要な情報を対話的に検索できるか？を重視する
- ペーパレス化を推進できるアプリケーションを選ぶ
- 在宅勤務の対応が容易なアプリケーションを選ぶ
- ブラウザのみで利用できるアプリケーションを選ぶ

<<法制度に関連する項目>>
- 残業割増率の変更に伴って、業務効率改善に取り組む
- サードパーティCookie規制に伴って販促施策を変更する
- 外国人労働者の活用を見据えた機能の強化を重視する
- 省エネ対策の実現や認定取得にも役立つかを重視する
- 経済安全保障に伴う環境変化への対応力を重視する

<<生成AI（ジェネレーティブAI）に関連する項目>>
- 生成AIは業務アプリケーションに組み込んで利用する
- 生成AIは業務アプリケーションと切り離して利用する
- 関連する法整備が整うまで生成AIの利用は控える
- AIが自社の知見やデータを学習することは拒否する

<<価格に関連する項目>>
- 購入ではなく、サブスクリプション型の費用体系を選ぶ
- データ量や人数に応じた従量制の課金体系を選ぶ
- 売上などの成果報酬に基づく課金体系を選ぶ

<<その他>>
- その他：
- 特に方針はない（排他）

設問P0の選択肢毎に設問R5を集計した結果を見ることによって、「自動化による業務効率改善に取り組もうとするユーザ企業が重視する守りのIT対策は何か？」や「生成AIの取り組み状況の違い（業務アプリケーションに組み込むか or 切り離して利用するか？）によって、守りのIT対策に関する今後のニーズがどう変わるか?」などを知ることができる。このように本調査レポートでは業績改善に寄与する「攻めのIT活用」との兼ね合いも考慮して「守りのIT対策」のニーズを分析している。

次頁へ続く

本調査レポートの設問項目(5/5)

R6. 既に導入している守りのIT対策の開発元(複数回答可)

現時点で導入済みのIT対策を担う製品/サービスを開発しているベンダを尋ねた設問である。(製品/サービスを購入した販社/SIerではない点に注意)選択肢は計6カテゴリ、合計51社に及ぶ。以下では社名と共に代表的な製品/サービスも例示している。

<<セキュリティを主体としたベンダ>>

- トレンドマイクロ 例) ウイルスバスター
- ブロードコム(シマンテック) 例) Symantec Endpoint Security
- マカフィー 例) McAfee
- イーセットジャパン 例) ESET PROTECT
- クラウドストライク 例) CrowdStrike
- サイバーリーズン 例) Cybereason
- ディープインスティンクト 例) Deep Instinct
- カスペルスキー 例) Kaspersky
- ソースネクスト 例) ZERO ウイルスセキュリティ
- エフ・セキュア 例) F-Secure
- ソフォス 例) Sophos
- FFRIセキュリティ 例) FFRI yarai
- AppGuard Marketing 例) AppGuard
- セキュリティを主体としたその他のベンダ:

<<運用管理/資産管理を主体としたベンダ>>

- Sky 例) SKYSEA Client View
- クオリティソフト 例) ISM / QND
- エムオーテックス 例) LANSCOPE
- Ivanti(LANDESK) 例) Ivanti(LANDESK)
- ハンモック 例) AssetView
- ラネクシー 例) MylogStar
- ソリトンシステムズ 例) InfoTrace
- 運用管理/資産管理を主体としたその他のベンダ:

<<バックアップ/リストアを主体としたベンダ>>

- ベリタステクノロジーズ 例) Backup Exec
- Arcserve 例) Arcserve
- クエストソフトウェア 例) NetVault
- アクティファイ(ネットジャパン) 例) ActiveImage Protector
- アクロニス 例) Acronis
- ヴィーム・ソフトウェア 例) Veeam
- バックアップ/リストアを主体としたその他のベンダ:

<<その他のベンダ(SSO、WAF、Webフィルタリングなど)>>

- HENNGE(へんげ) 例) HENNGE One
- NTTコミュニケーションズ 例) ID Federation
- アイピーキューブ 例) CloudLink
- サイオステクノロジー 例) Gluegent Gate
- クラウドブリック 例) Cloudbric
- モニタラップ 例) AIONCLOUD
- アルプスシステムインテグレーション 例) InterSafe
- デジタルアーツ 例) i-FILTER
- その他のベンダ(SSO、WAF、Webフィルタリングなど):

<<ネットワーク関連が主体のベンダ>>

- エフファイブ・ネットワークス・ジャパン 例) F5 Distributed Cloud Services
- ソニックウォール・ジャパン 例) Edge Secure Access
- フォーティネットジャパン 例) FortiGuard
- チェック・ポイント・ソフトウェア・テクノロジーズ 例) Harmony
- パロアルトネットワークス 例) Cortex
- バラクーダネットワークスジャパン 例) CloudGen
- ネットスコープ 例) Netskope
- ゼットスケーラー 例) Zscaler
- Cloudflare 例) Cloudflare
- ネットワーク関連が主体のその他のベンダ:

<<総合ベンダ>>

- NEC 例) WebSAM
- 富士通 例) Systemwalker
- 日立製作所 例) JP1
- HPE/日本HP 例) ICE Wall
- デル・テクノロジーズ 例) Power Protect
- 日本IBM 例) Tivoli
- 日本マイクロソフト 例) System Center / Intune
- ヴイエムウェア 例) Carbon Black
- その他の総合ベンダ:

<<その他>>

- 導入している製品/サービスはない(排他)

R7. 守りのIT対策に対して許容可能な年額合計費用(万円)

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製品/サービス(ソフトウェア、アプライアンス、クラウドサービス)を導入/利用する上で必要となる年額の合計費用として許容できる金額を数値(万円)で回答する設問である。

本調査レポートの集計データ(1/3)

本調査レポートで用いられている用語の説明やファイルの命名規則は以下の通りである。

【用語の説明】

「表頭」　実際の集計対象となる設問を指す。集計表では列表記に相当し、グラフでは凡例に相当する。

「表側」　表頭となるデータを区切って集計する際の区分に相当する設問を指す。集計表においては行表記に相当し、グラフにおいてはそれぞれの帯に相当する。

【ファイルの命名規則】

本調査レポートの集計データはMicrosoft Excel形式となっており、以下の命名規則に沿って作成されている。

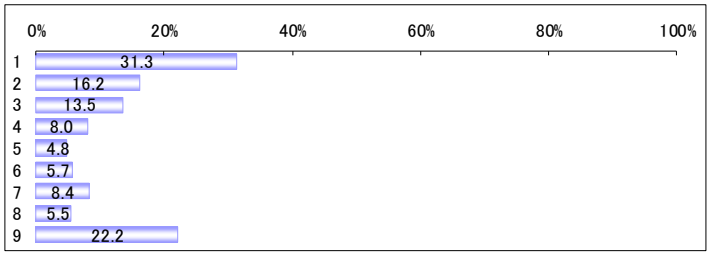
表側を伴わない集計データ: 単純集計データ
命名規則: 【表頭名】単純集計.xlsx

表側を設定しない集計結果は「単純集計データ」と呼ばれ、設問の回答結果を棒グラフでプロットする形式となる。ファイル名は集計対象(表頭)となる設問名の後に「単純集計」というキーワードを付加された書式となる。例えば、本調査レポートの設問には全てRの接頭辞が付加されており、全設問の単純集計データを収録したファイル名は「【R系列】単純集計.xlsx」となる。

単純集計データの例

R1-1.守りのIT対策の実施内容(エンドポイント(社内))(複数回答可)

		n	%
	全体	1300	100.0
1	パッケージ	407	31.3
2	サービス	211	16.2
3	アウトソース	175	13.5
4	アプライアンス	104	8.0
5	H/Wの付属機能	62	4.8
6	OSの付属機能	74	5.7
7	不明	109	8.4
8	対策未実施	72	5.5
9	該当なし	288	22.2



表側を伴う集計データ: 主要分析軸集計　および　質問間クロス集計データ
命名規則: 【表頭名】(【表側名】表側).xlsx

表側が設置された集計結果は「主要分析軸集計データ」または「質問間クロス集計データ」と呼ばれる。

「主要分析軸集計データ」とは、A1～A7までのサンプル属性区分を表側として集計したデータを指す。例えば、本調査レポートにおける数値回答設問を除いた全ての設問(与えられた選択肢から選ぶ形式の設問)を表頭とし、「A1.年商」を表側として集計した「主要分析軸集計データ」のファイル名は「【R系列】(【A1】表側).xlsx」となる。

一方で、「質問間クロス集計データ」とは、サンプル属性区分以外の何らかの設問を表側として集計したデータを指す。ファイル名は集計対象(表頭)である設問名に表側となっている設問名が続き、「表側」というキーワードが付加された書式となる。例えば、本調査レポートにおける数値回答設問を除く全ての設問を表頭とし、設問「R2.守りのIT対策の最も主要な導入元」を表側として集計した「質問間クロス集計データ」のファイル名は「【R系列】(【R2】表側).xlsx」となる。

表側を伴う集計データは1設問につき1シートの形式となっており、表頭となっている設問名が各シートのタブ名に記載されている。ただし、選択肢の数が多い場合は複数シートにデータが分割される。その際はタブ名に[設問名-1]、[設問名-2]といった枝番が付加され、シート内のグラフタイトルには「***(1/2)」、「***(2/2)」といったように分割されたシートの一部であることを示す接尾辞が付加される。

次頁へ続く

本調査レポートの集計データ(2/3)

前頁からの続き

表側を伴う集計データの各シートは以下の4つの要素から構成される。

A [自動生成コメント]

集計データの概要が端的なコメントとして記載されている。ただし、このコメントは自動生成された参考コメントとしての位置付けであるため、設問選択肢の詳しい意味合いなどは加味されていない点に注意する必要がある。

B [設問結果の単純集計結果グラフ]

選択肢の数に応じて縦棒グラフまたは横帯グラフのいずれかによって表側が設定されていない状態の集計結果を端的に示している。

C [表側を伴う設問結果の数表]

表側を設定した状態での集計結果を数表として表示している。数表内には選択肢毎の回答件数と回答割合(パーセント)が記載されている。

D [表側を伴う設問結果のグラフ]

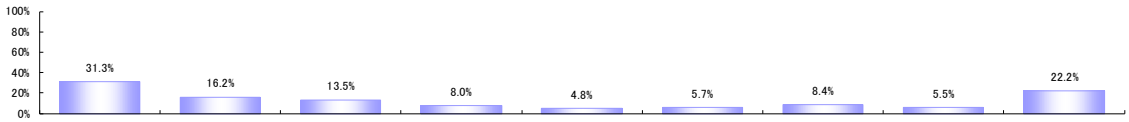
表側を設定した状態での集計結果を積み上げ横棒グラフとして表示している。可視性を考慮して、5%未満の数値についてはグラフ中の数字表記を非表示としている。表頭となる設問が単一回答設問である場合は目盛に値の付いた横軸が表示される。複数回答設問の場合には複数の選択肢を合計した数値には重複が含まれるため、誤った数値の読み取りを避ける目的で横軸の目盛り値を非表示としている。

表側を伴う集計データの例

R1-1.守りのIT対策の実施内容(エンドポイント(社内))(複数回答可)

A
・全体では、「パッケージ」が31.3%で最も高く、次いで「該当なし(22.2%)」「サービス(16.2%)」である。
・「A1.年商」では、「5億円未満」で「該当なし」が全体と比較して高い。

B



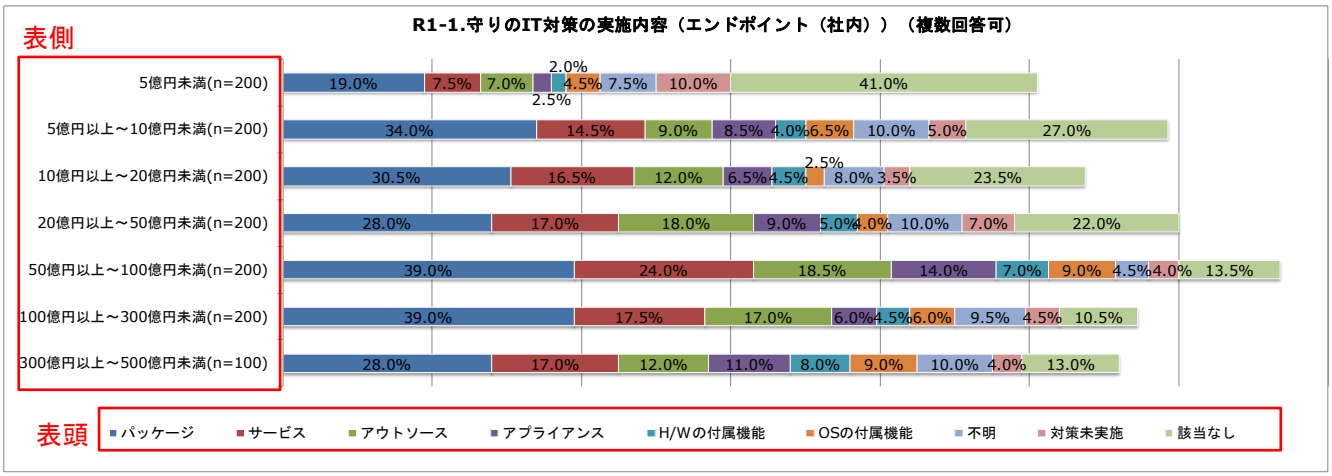
表側 / 表頭

C

		n	パッケージ	サービス	アウトソース	アプライアンス	H/Wの付属機能	OSの付属機能	不明	対策未実施	該当なし
全体		1300	407 31.3%	211 16.2%	175 13.5%	104 8.0%	62 4.8%	74 5.7%	109 8.4%	72 5.5%	288 22.2%
A1.年商	5億円未満	200	38 19.0%	15 7.5%	14 7.0%	5 2.5%	4 2.0%	9 4.5%	15 7.5%	20 10.0%	82 41.0%
	5億円以上～10億円未満	200	68 34.0%	29 14.5%	18 9.0%	17 8.5%	8 4.0%	13 6.5%	20 10.0%	10 5.0%	54 27.0%
	10億円以上～20億円未満	200	61 30.5%	33 16.5%	24 12.0%	13 6.5%	9 4.5%	5 2.5%	16 8.0%	7 3.5%	47 23.5%
	20億円以上～50億円未満	200	56 28.0%	34 17.0%	36 18.0%	18 9.0%	10 5.0%	8 4.0%	20 10.0%	14 7.0%	44 22.0%
	50億円以上～100億円未満	200	78 39.0%	48 24.0%	37 18.5%	28 14.0%	14 7.0%	18 9.0%	9 4.5%	8 4.0%	27 13.5%
	100億円以上～300億円未満	200	78 39.0%	35 17.5%	34 17.0%	12 6.0%	9 4.5%	12 6.0%	19 9.5%	9 4.5%	21 10.5%
	300億円以上～500億円未満	100	28 28.0%	17 17.0%	12 12.0%	11 11.0%	8 8.0%	9 9.0%	10 10.0%	4 4.0%	13 13.0%

D

表側



本調査レポートの集計データ(3/3)

本調査レポートに収録されている集計データは以下の通りである。

単純集計データ:

【R系列】単純集計.xlsx	表側を設定せずに本調査レポートの全ての設問を集計したデータ

主要分析軸集計データ:

【R系列】(【A1】表側).xlsx	年商(A1)を表側として、数値回答設問(設問R7)を除く選択肢設問を集計したデータ
【R系列】(【A2】表側).xlsx	職責(A2)を表側として、数値回答設問(設問R7)を除く選択肢設問を集計したデータ
【R系列】(【A3】表側).xlsx	従業員数(A3)を表側として、数値回答設問(設問R7)を除く選択肢設問を集計したデータ
【R系列】(【A4】表側).xlsx	業種(A4)を表側として、数値回答設問(設問R7)を除く選択肢設問を集計したデータ
【R系列】(【A5】表側).xlsx	所在地(A5)を表側として、数値回答設問(設問R7)を除く選択肢設問を集計したデータ
【R系列】(【A6】表側).xlsx	IT管理/運用の人員規模(A6)を表側として、数値回答設問(設問R7)を除く選択肢設問を集計したデータ
【R系列】(【A7】表側).xlsx	ビジネス拠点の状況(A7)を表側として、数値回答設問(設問R7)を除く選択肢設問を集計したデータ
【R系列数値】(【A1】表側).xlsx	年商(A1)を表側として、数値回答設問(設問R7)を集計したデータ
【R系列数値】(【A2】表側).xlsx	職責(A2)を表側として、数値回答設問(設問R7)を集計したデータ
【R系列数値】(【A3】表側).xlsx	従業員数(A3)を表側として、数値回答設問(設問R7)を集計したデータ
【R系列数値】(【A4】表側).xlsx	業種(A4)を表側として、数値回答設問(設問R7)を集計したデータ
【R系列数値】(【A5】表側).xlsx	所在地(A5)を表側として、数値回答設問(設問R7)を集計したデータ
【R系列数値】(【A6】表側).xlsx	IT管理/運用の人員規模(A6)を表側として、数値回答設問(設問R7)を集計したデータ
【R系列数値】(【A7】表側).xlsx	ビジネス拠点の状況(A7)を表側として、数値回答設問(設問R7)を集計したデータ

質問間クロス集計データ:

【R系列】(【R2】表側).xlsx	設問R2(守りのIT対策の最も主要な導入元)を表側として、数値回答設問(設問R7)を除く選択肢設問を集計したデータ
【R5】(【R4】表側).xlsx	設問R4(守りのIT対策において現時点で抱えている課題)を表側として、設問R5(守りのIT対策の製品/サービスが今後持つべきと考える機能や特徴)を集計したデータ
【R系列数値】(【R4】表側).xlsx	設問R4(守りのIT対策において現時点で抱えている課題)を表側として、数値回答設問(設問R7)を集計したデータ
【R系列数値】(【R5】表側).xlsx	設問R5(守りのIT対策の製品/サービスが今後持つべきと考える機能や特徴)を表側として、数値回答設問(設問R7)を集計したデータ

分析サマリ掲載データ:

分析サマリ掲載データ.xlsx	本調査レポートの要点と提言を記載した「分析サマリ」(PDF形式)内に掲載されたデータ(本調査レポートには含まれない姉妹編調査レポート内のデータとのクロス集計結果も含む)

レポート試読版1(「分析サマリ」)

本調査レポートの重要ポイントや今後に向けた提言をまとめたものが「分析サマリ」(PDF形式)である。この分析サマリを通読することで、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対策に関する市場動向を把握することができる。(分析サマリの章構成については本ドキュメントの2ページを参照) 以下の試読版では分析サマリの「第1章.守りの IT 対策を実施している箇所と内容」の冒頭部分を抜粋して掲載している。

第 1 章. 守りの IT 対策を実施している箇所と内容

本章では中堅・中小企業における守りの IT 対策(セキュリティ、運用管理、バックアップ)の現状を実施箇所と実施内容の 2 つの観点から俯瞰していく。

設問「R1.守りの IT 対策を実施している箇所と内容」では、守りの IT 対策の現状を以下のように

「実施箇所」 どこに対策を講じているか?(対象)

「実施内容」 どのような対策を講じているか?(手段)

との 2 つの観点から尋ねている。

実施箇所:

エンドポイント(社内): 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): 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

**********中略**********

実施内容:

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

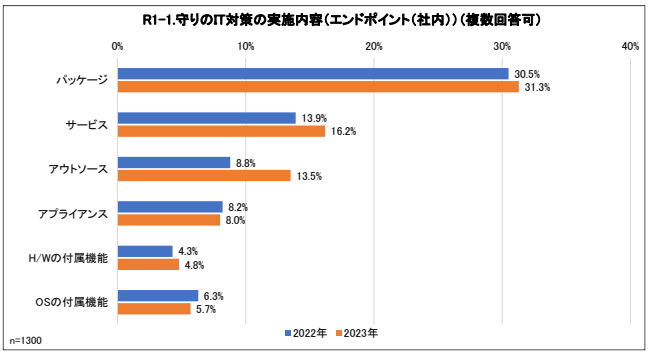
例)PC にマルウェア対策のパッケージ製品をインストールしている

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

**********中略**********

以下のグラフは設問「R1-1.守りの IT 対策の実施内容(エンドポイント(社内))」の結果を 2022 年と 2023 年で比較したものだ。(集計データ¥分析サマリ掲載データ.xlsx 「第 1 章-1」シート)



サンプルのため、ここでは
グラフのサイズを小さくして
掲載している

2022 年から 2023 年にかけて「サービス」や「アウトソース」が増加している。近年では社内のエンドポイントにおける守りの IT 対策においても、管理サーバを社内に設置する必要のないクラウド形態のセキュリティ/運用管理/バックアップのアプリケーションや端末の調達/廃棄といったライフサイクル管理も含めた管理/運用を委託できるソリューションも登場してきている。上記の結果はこうした動きを反映したものと捉えることができる。ただし、全体としては「パッケージ」が依然として

**********以下、省略**********

レポート試読版2(「主要分析軸集計データ」)

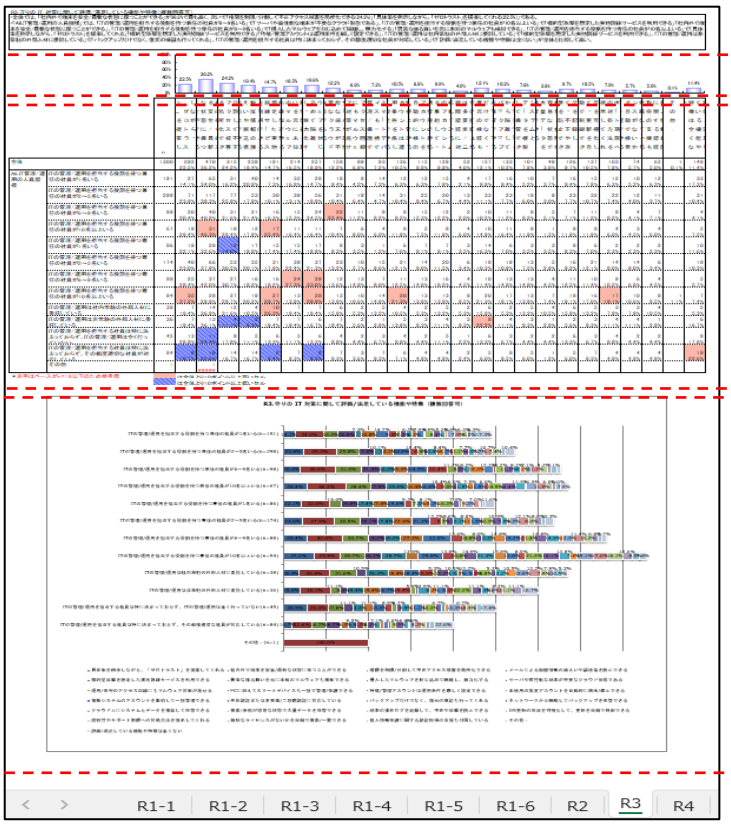
「設問項目」に掲載した設問結果を年商、業種、従業員数、所在地などの基本属性を軸として集計したものが、「主要分析軸集計データ」であり、Microsoft Excel形式で調査レポート内に同梱されている。以下の試読版に掲載したものは「A6. IT管理/運用の人員体制」を集計軸として本調査レポートの各設問の結果を集計した結果の一部である。

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、本調査レポートにおいて数値回答を除いた選択肢設問(与えられた選択肢から選んで回答する形式の設問群)を指す。また、【A6】とは本ドキュメントの1ページに記載されたIT管理/運用の人員体制を示す企業属性であり、以下のような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』の結果を見ることで、IT管理/運用を担う人材が1名のみの場合(ひとり情シス)、2～5名、6～9名、10名以上の場合や専任/兼任の違いによって、守りのIT対策における現状の課題や今後の方針がどのように異なるか？などを確認できる。
同様に年商別の傾向は『【R系列】(【A1】表側).xlsx』(A1が年商区分を表す)、業種別の傾向は『【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、ファイル名を見れば「どの設問を対象として、何を軸として集計したものか？」が把握できる。

主要分析軸集計データにおける設問数は(R1-1～R1-6、R2、R3、R4、R5、R6、R7)の計12設問あり、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所在地」「A6.IT管理/運用の人員規模」「A7.ビジネス拠点の状況」の7項目あるため、「主要分析軸データ」の集計データ数は12設問×7属性＝84となる。
(ただし「年商20億円以上～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)



※1
※2
※3

個々のシートは左記のようなレイアウトになっている。

画面上部:※1
軸を設定していない状態の縦帯グラフもしくは横帯グラフ

画面中央:※2
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:※3
画面中央の数表データを横帯グラフで視覚化したもの

集計データの種類や命名規則などの詳細は本ドキュメントの8～10ページを参照

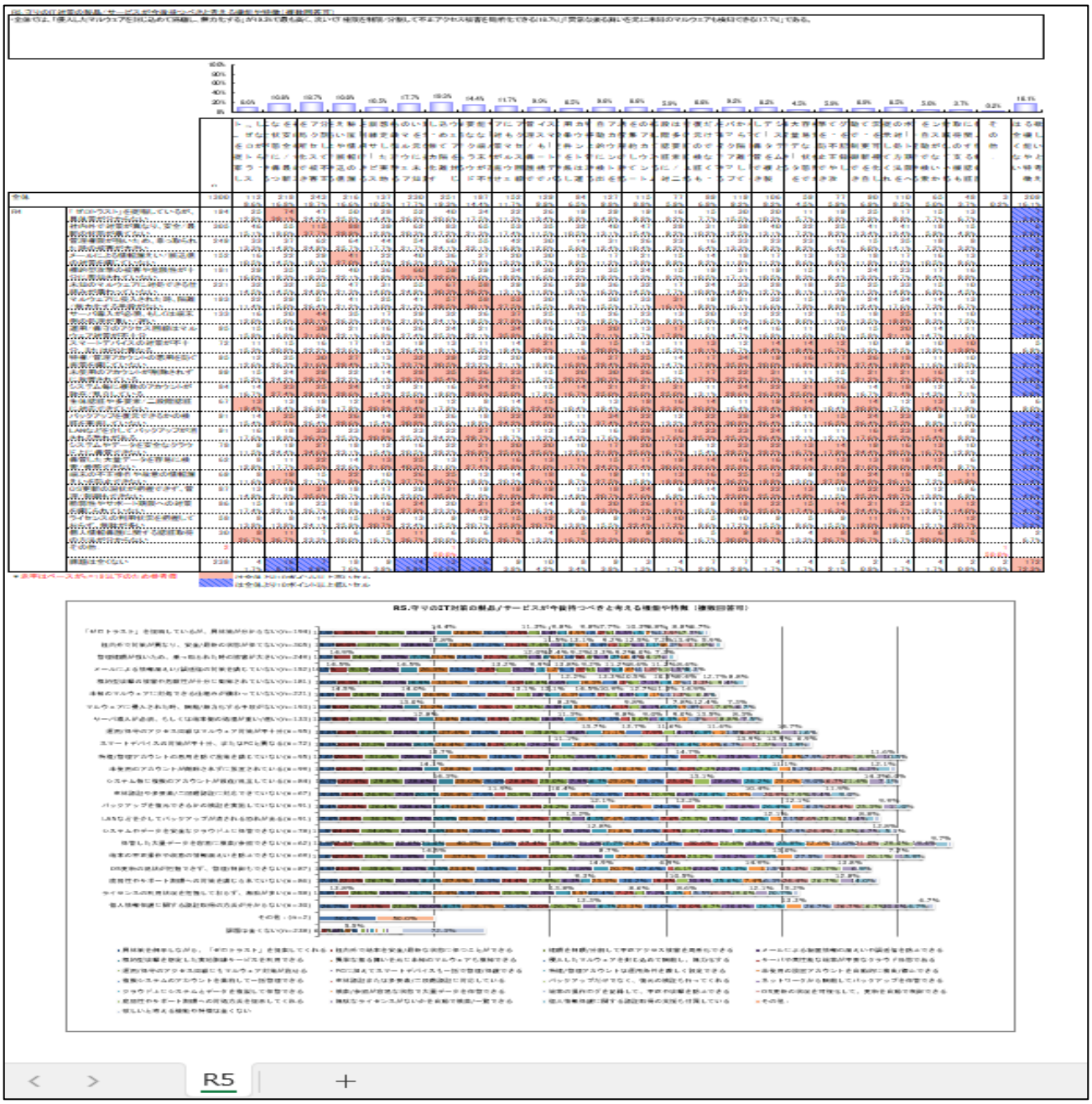
レポート試読版3(「質問間クロス集計データ」)

「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設問「R5.守りのIT対策の製品/サービスが今後持つべきと考える機能や特徴」を設問「R4.守りのIT対策において現時点で抱えている課題」を軸として集計した結果である。これを見ることによって、守りのIT対策においてユーザ企業が抱えている課題が今後のニーズにどう影響するか？を知ることができる。

以下のMicrosoft Excelファイル名は『【R5】(【R4】表側).xlsx 』となっている。「【R4】表側」の部分は設問「R4」が集計の軸(表側)となっていることを示している。ファイル名の先頭にある【R5】の部分は設問「R5」が集計対象(表頭)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？」を把握できる。

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もしくは横帯グラフ、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レイアウト(前頁の主要分析軸集計データと同様)となっている。



ご好評いただいているその他の調査レポート （各冊：180,000円税別）

『2023年版 中堅・中小企業のDXおよびITソリューション選定の実態レポート』

50項目に渡る具体的なDX/ITソリューションの導入状況、ユーザ企業が抱える課題とニーズ、選ぶべき訴求手段を網羅した一冊

【レポートの概要と案内】 https://www.norkresearch.co.jp/pdf/2023IT_user_rep.pdf

【リリース(ダイジェスト)】 中堅・中小市場で選ぶべき顧客接点とは？(Webサイト/SNS/メール/電話/Web会議など)
https://www.norkresearch.co.jp/pdf/2023IT_user_rel1.pdf

中堅・中小企業のIT支出を左右する経常利益の増減見通しとその要因分析
https://www.norkresearch.co.jp/pdf/2023IT_user_rel2.pdf

12分野、50項目に渡るDX/ITソリューションの活用実態における変化
https://www.norkresearch.co.jp/pdf/2023IT_user_rel3.pdf

中堅・中小市場で留意すべきユーザ企業とIT企業の「すれ違い」ポイント
https://www.norkresearch.co.jp/pdf/2023IT_user_rel4.pdf

年商別/業種別のIT支出増減予測およびIT支出を増やす商材と減らす商材
https://www.norkresearch.co.jp/pdf/2023IT_user_rel5.pdf

『2023年版 中堅・中小企業におけるネットワーク環境の実態と展望レポート』

今後不可欠となるネットワーク環境とセキュリティ対策を同時に考慮したITインフラ整備の提案ポイントを分析/提言

【レポートの概要と案内】 https://www.norkresearch.co.jp/pdf/2023NW_user_rep.pdf

【リリース(ダイジェスト)】 セキュリティ対策を起点とした中堅・中小向けネットワーク製品/サービスの訴求
https://www.norkresearch.co.jp/pdf/2023NW_user_rel1.pdf

IT企業が見落としやすい中堅・中小ネットワーク環境の意外な課題/ニーズ
https://www.norkresearch.co.jp/pdf/2023NW_user_rel2.pdf

中堅・中小企業におけるネットワーク製品/サービスの市場規模と導入時の基本方針
https://www.norkresearch.co.jp/pdf/2023NW_user_rel3.pdf

『2023年版 中堅・中小企業のITアプリケーション利用実態と評価レポート』

10分野の導入済み/導入予定の社数シェアとユーザ評価に加えて、法制度対応やデータ分析/生成AIの動向を網羅

【レポートの概要と案内】 https://www.norkresearch.co.jp/pdf/2023itapp_rep.pdf

【リリース(ダイジェスト)】

データ分析や生成AI	https://www.norkresearch.co.jp/pdf/2023itapp_ex2_rel.pdf
インボイス/電帳法	https://www.norkresearch.co.jp/pdf/2023itapp_ex1_rel.pdf
ERP	https://www.norkresearch.co.jp/pdf/2023itapp_erp_rel.pdf
生産管理	https://www.norkresearch.co.jp/pdf/2023itapp_ppc_rel.pdf
会計管理	https://www.norkresearch.co.jp/pdf/2023itapp_acc_rel.pdf
販売・仕入・在庫管理	https://www.norkresearch.co.jp/pdf/2023itapp_sbc_rel.pdf
給与・人事・勤怠・就業管理	https://www.norkresearch.co.jp/pdf/2023itapp_hrw_rel.pdf
ワークフロー・ビジネスプロセス管理	https://www.norkresearch.co.jp/pdf/2023itapp_wf_rel.pdf
コラボレーション(グループウェア/ビジネスチャット/Web会議)	https://www.norkresearch.co.jp/pdf/2023itapp_gw_rel.pdf
CRM	https://www.norkresearch.co.jp/pdf/2023itapp_crm_rel.pdf
BI	https://www.norkresearch.co.jp/pdf/2023itapp_bi_rel.pdf
文書管理・オンラインストレージサービス	https://www.norkresearch.co.jp/pdf/2023itapp_dm_rel.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