ランサムウェア対策や経済安全保障の取り組みが急務となる中、2024～2025年の経年変化に基づいて中堅・中小企業のセキュリティ/運用管理/バックアップの導入社数シェア、実施状況、課題、ニーズを明らかにした必携レポート

2025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。**

価格: ￥225,000円(税別)　**発刊日:** 2025年11月7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

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/決裁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

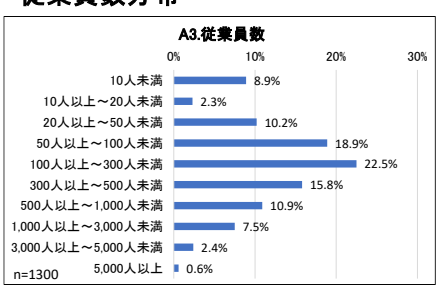
A4.業種区分: 組立製造業 / 加工製造業 / 建設業 / 卸売業 / 小売業 / 流通業(運輸業) / IT関連サービス業 / 一般サービス業 / その他

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

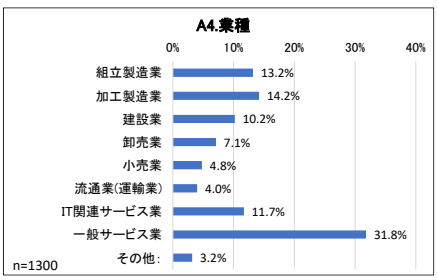
調査実施時期: 2025年7月～8月

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つのグラフは調査対象1300社の「従業員数」「業種」「所在地」分布である。中堅・中小市場の幅広い企業が対象となっていることが確認できる。

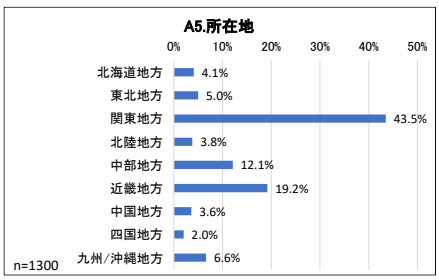
従業員数分布



業種分布



所在地分布



本調査レポートの背景

ランサムウェア被害件数は減少する兆候が見られず、大企業だけでなくサプライチェーンを構成する中小規模の企業も標的となるリスクが高まっている。一方、自民と維新が連立した高市政権では経済安全保障を重視しており、規模/業種を問わずサイバー攻撃に対する防御や機密情報の管理に関する意識向上が求められてくる。

上記の背景を受けて、今後は中堅・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対策の重要性も一層高まっていくと予想される。こうした状況の中で、ベンダや販社/SIerが守りのIT対策を担う製品/サービスを拡販していくためには、「近年で対策が進んだ箇所は何処か？逆に遅れている取り組みは何か？」といった変化を捉えることが大切だ。

そこで、本調査レポートでは2024年～2025年の経年変化を中心とした集計/分析を行い、中堅・中小企業の守りのIT対策において更なる改善が求められる点や対策が遅れている点などを明らかにし、IT企業がどのような提案/啓蒙を進めるべきかを提言している。

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3～6ページ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7～10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 対策の実施状況における変化

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？を尋ねた結果の2024～2025年の経年変化を集計/分析。また、守りのIT対策をどのようなIT企業から導入したか？（販社/SIer経由か？ベンダ直接か？）についても2024～2025年の経年変化を集計/分析している。

第2章：守りのIT対策における評価/満足の変化と最新動向

「侵入したマルウェアを封じ込めて隔離し、無力化する」、「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」など、導入済みの守りのIT対策について評価/満足している事柄を計15項目に渡る経年変化（2024～2025年）と最新動向を踏まえた8項目に渡る新たな選択肢（「セキュリティ責任者の代わりとなる相談サービスがある」、「なりすましのメールや電話への対策も提示してくれる」など）で尋ねた結果を集計/分析。

第3章：守りのIT対策における課題の変化と最新動向

「管理権限が強いため、乗っ取られた時の被害が大きい」、「未使用のアカウントが削除されずに放置されている」など、導入済みの守りのIT対策における課題を計15項目に渡る経年変化（2024～2025年）および最新動向を踏まえた8項目に渡る新たな選択肢（「自社が攻撃を受けると、取引先も巻き込む恐れがある」、「クラウドサービスのアクセス権設定は見直しが不十分」など）で尋ねた結果を集計/分析。

第4章：守りのIT対策におけるニーズの変化と最新動向

第2章と共通する選択肢を設けて、計15項目に渡る経年変化（2024～2025年）と最新動向を踏まえた計8項目で守りのIT対策を担う製品/サービスに対するニーズ（機能や特徴）を集計/分析。

第5章：守りのIT対策の開発元（ベンダ）の導入社数シェア変化

「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6カテゴリ、計56項目に渡る守りのIT対策の開発元（ベンダ）を列挙し、導入社数シェアの経年変化（2024～2025年）を集計/分析。

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の経年変化（2024～2025年）を集計/分析。

本調査レポートの設問項目（1/4）

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対策の実施内容（枝番設問毎に複数回答可）

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「箇所」（何処に対策を講じているか？）と「手段」（どのような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。

実施している箇所：

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

実施している手段：

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）

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「実施している箇所」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「実施している手段」が選択肢として設定されている。「実施している手段」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」は排他選択肢となっており、選んだ場合には他の選択肢は選べない。

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（2/4）

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。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。そうした背景を踏まえて本設問の選択肢には以下の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、「その他」や排他選択肢は除く）で尋ねた設問である。<<その他>>以外の選択肢のうち、下線のついた項目は最新動向を踏まえて2025年に追加された選択肢、下線のない項目は前回調査と共通の選択肢であり、2024～2025年の経年変化を集計/分析している。

<<セキュリティ全般>>
・セキュリティ対策を担う人材を育成できるサービスがある
・セキュリティ責任者の代わりとなる相談サービスがある
・取引先への影響も含めた対策の重要性を啓蒙してくれる
・情報漏えい発生時の対策マニュアルを提示してくれる
・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
・外出中やテレワーク時のセキュリティ対策を講じてくれる

<<マルウェア対策>>
・なりすましのメールや電話への対策も提示してくれる
・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

<<アカウント管理>>
・クラウドサービスのアクセス権設定も改善してくれる
・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

<<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

<<運用管理/資産管理>>
・OSアップデートを安全/確実に行う支援をしてくれる
・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>>
・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（3/4）

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。<<その他>>以外の選択肢のうち、下線のついた項目は最新動向を踏まえて2025年に追加された選択肢、下線のない項目は前回調査と共通の選択肢であり、2024～2025年の経年変化を集計/分析している。

<<セキュリティ全般>>
- セキュリティ対策を担う人材を採用/育成できていない
- セキュリティ責任者（CIO）を社内に置く余裕は全くない
- 自社が攻撃を受けると、取引先も巻き込む恐れがある
- 情報漏えいが発生した時などの対策マニュアルがない
- 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
- 外出中やテレワーク時のセキュリティ対策が不十分

<<マルウェア対策>>
- なりすましのメールや電話は不正を見抜くのが難しい
- 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

<<アカウント管理>>
- クラウドサービスのアクセス権設定は見直しが不十分
- 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

<<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

<<運用管理/資産管理>>
- OSアップデート適用が原因の障害で業務が停止する
- 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>>
- その他：
- 課題は全くない（排他）

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。最後の選択肢を除き、選択肢は設問R3と共通である。<<その他>>以外の選択肢のうち、下線のついた項目は最新動向を踏まえて2025年に追加された選択肢、下線のない項目は前回調査と共通の選択肢であり、2024～2025年の経年変化を集計/分析している。

<<セキュリティ全般>>
- セキュリティ対策を担う人材を育成できるサービスがある
- セキュリティ責任者の代わりとなる相談サービスがある
- 取引先への影響も含めた対策の重要性を啓蒙してくれる
- 情報漏えい発生時の対策マニュアルを提示してくれる
- 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
- 外出中やテレワーク時のセキュリティ対策を講じてくれる

<<マルウェア対策>>
- なりすましのメールや電話への対策も提示してくれる
- 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

<<アカウント管理>>
- クラウドサービスのアクセス権設定も改善してくれる
- 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

<<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

<<運用管理/資産管理>>
- OSアップデートを安全/確実に行う支援をしてくれる
- 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>>
- その他：
- 欲しいと考え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（4/4）

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守りの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56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。全ての選択肢について、2024～2025年の経年変化を集計したデータも収録されている。

<<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） Falcon
- 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ドコモビジネス（ NTTコミュニケーションズ）　例） docomo business RINK IDaaS
- アイピーキューブ　例） CloudLink
- サイオステクノロジー　例） Gluegent Gate
- ペンタセキュリティ（Cloudbric）　例） クラウドブリック
- 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） TZ Series
- 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） IceWall
- 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
- 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。2024～2025年の経年変化を集計したデータも収録されている。

次頁へ続く

本調査レポートの集計データ(1/4)

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。

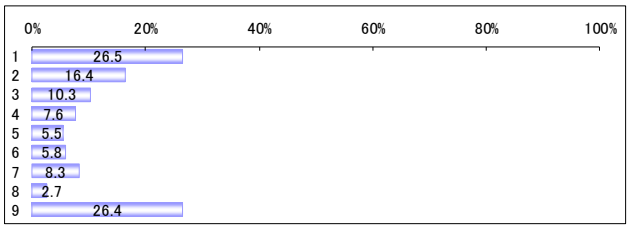
表側を伴わない集計データ: 単純集計データ
命名規則: 【表頭名】単純集計.xlsx

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	344	26.5
2	サービス	213	16.4
3	アウトソース	134	10.3
4	アプライアンス	99	7.6
5	H/Wの付属機能	72	5.5
6	OSの付属機能	75	5.8
7	不明	108	8.3
8	対策未実施	35	2.7
9	該当なし	343	26.4



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(2/4)

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]

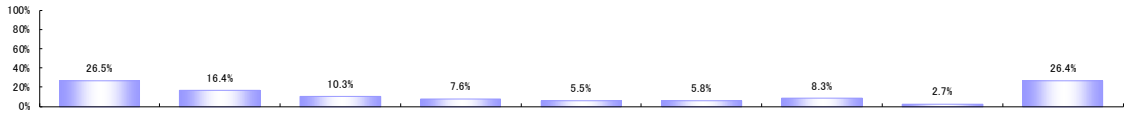
表側を設定した状態での集計結果を積み上げ横棒グラフとして表示している。可視性を考慮して、5%未満の数値についてはグラフ中の数字表記を非表示としている。表頭となる設問が単一回答設問である場合は目盛に値の付いた横軸が表示される。複数回答設問の場合には複数の選択肢を合計した数値には重複が含まれるため、誤った数値の読み取りを避ける目的で横軸の目盛り値を非表示としている。

表側を伴う集計データの例

A

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)
・全体では、「パッケージ」が26.5%で最も高く、次いで「該当なし(26.4%)」「サービス(16.4%)」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

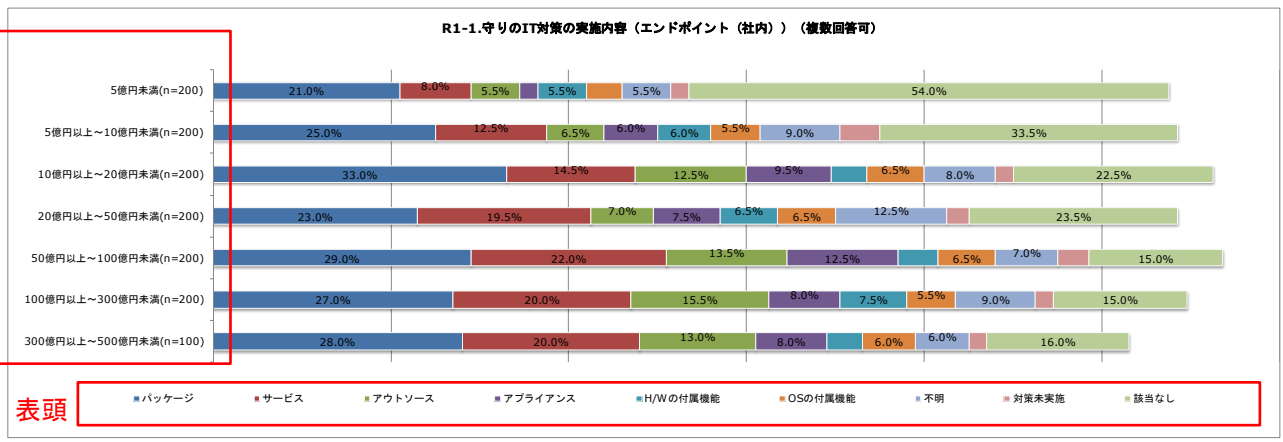
C

		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	344 26.5%	213 16.4%	134 10.3%	99 7.6%	72 5.5%	75 5.8%	108 8.3%	35 2.7%	343 26.4%
A1.年商	5億円未満	200	42 21.0%	16 8.0%	11 5.5%	4 2.0%	11 5.5%	8 4.0%	11 5.5%	4 2.0%	108 54.0%
	5億円以上～10億円未満	200	50 25.0%	25 12.5%	13 6.5%	12 6.0%	12 6.0%	11 5.5%	18 9.0%	9 4.5%	67 33.5%
	10億円以上～20億円未満	200	66 33.0%	29 14.5%	25 12.5%	19 9.5%	8 4.0%	13 6.5%	16 8.0%	4 2.0%	45 22.5%
	20億円以上～50億円未満	200	46 23.0%	39 19.5%	14 7.0%	15 7.5%	13 6.5%	13 6.5%	25 12.5%	5 2.5%	47 23.5%
	50億円以上～100億円未満	200	58 29.0%	44 22.0%	27 13.5%	25 12.5%	9 4.5%	13 6.5%	14 7.0%	7 3.5%	30 15.0%
	100億円以上～300億円未満	200	54 27.0%	40 20.0%	31 15.5%	16 8.0%	15 7.5%	11 5.5%	18 9.0%	4 2.0%	30 15.0%
	300億円以上～500億円未満	100	28 28.0%	20 20.0%	13 13.0%	8 8.0%	4 4.0%	6 6.0%	6 6.0%	2 2.0%	16 16.0%

＊赤字はベースがn=19以下のため参考値　　は全体より10ポイント以上高いセル　　は全体より10ポイント以上低いセル

表側

D



表側

表頭

本調査レポートの集計データ(3/4)

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 (※1) 【R系列数値】(【R2】表側).xlsx(※2)	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(※1)と数値回答設問(※2)を集計したデータ
【R系列】(【R3】表側).xlsx (※1) 【R系列数値】(【R3】表側).xlsx (※2)	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)を表側として、数値回答設問(設問R7)を除く選択肢設問(※1)と数値回答設問(※2)を集計したデータ
【R系列】(【R4】表側).xlsx (※1) 【R系列数値】(【R4】表側).xlsx (※2)	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)を除く選択肢設問(※1)と数値回答設問(※2)を集計したデータ
【R系列】(【R5】表側).xlsx (※1) 【R系列数値】(【R5】表側).xlsx (※2)	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)を除く選択肢設問(※1)と数値回答設問(※2)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(詳細については次頁に記載)

本調査レポートの集計データ(4/4)

分析サマリ掲載データ.xlsxには、本調査レポートの全設問(R1～R7)の経年変化(2024～2025年)を集計したデータが収録されている。

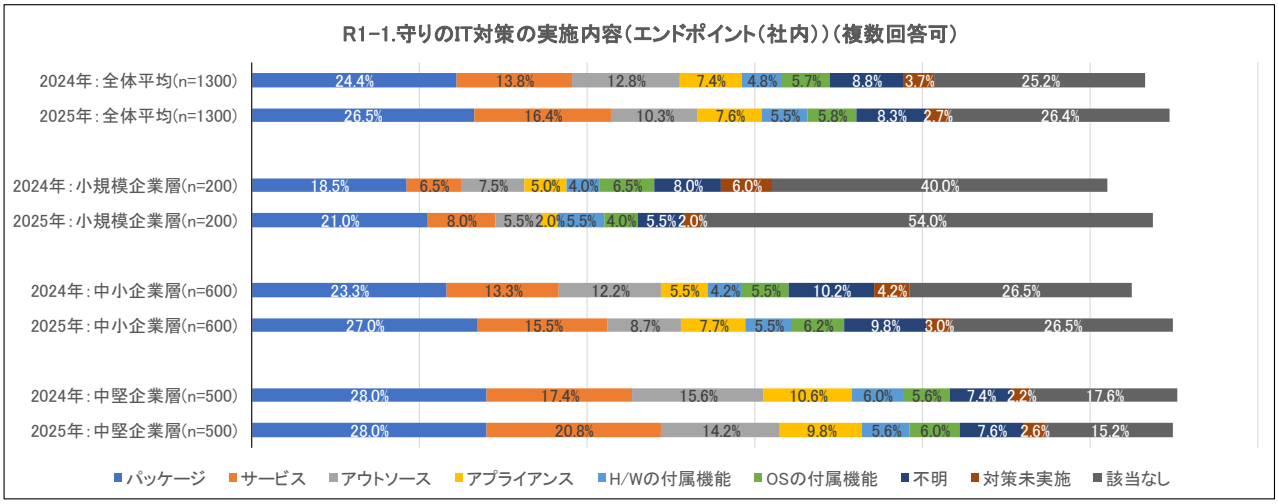
経年変化の集計では中堅・中小企業全体に加えて、以下の3つの年商区分毎にも集計を行っている。
・小規模企業層　年商5億円未満
・中小企業層　年商5億円以上～50億円未満
・中堅企業層　年商50億円以上～500億円未満

以下は「分析サマリ掲載データ.xlsx」の「R1-1経年変化」シートに掲載された設問「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)」の経年変化データである。

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)

	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
2024年:全体平均(n=1300)	24.4%	13.8%	12.8%	7.4%	4.8%	5.7%	8.8%	3.7%	25.2%
2025年:全体平均(n=1300)	26.5%	16.4%	10.3%	7.6%	5.5%	5.8%	8.3%	2.7%	26.4%
2025年-2024年のポイント差	2.1	2.6	-2.5	0.2	0.7	0.1	-0.5	-1.0	1.2
2024年:小規模企業層(n=200)	18.5%	6.5%	7.5%	5.0%	4.0%	6.5%	8.0%	6.0%	40.0%
2025年:小規模企業層(n=200)	21.0%	8.0%	5.5%	2.0%	5.5%	4.0%	5.5%	2.0%	54.0%
2025年-2024年のポイント差	2.5	1.5	-2.0	-3.0	1.5	-2.5	-2.5	-4.0	14.0
2024年:中小企業層(n=600)	23.3%	13.3%	12.2%	5.5%	4.2%	5.5%	10.2%	4.2%	26.5%
2025年:中小企業層(n=600)	27.0%	15.5%	8.7%	7.7%	5.5%	6.2%	9.8%	3.0%	26.5%
2025年-2024年のポイント差	3.7	2.2	-3.5	2.2	1.3	0.7	-0.4	-1.2	0.0
2024年:中堅企業層(n=500)	28.0%	17.4%	15.6%	10.6%	6.0%	5.6%	7.4%	2.2%	17.6%
2025年:中堅企業層(n=500)	28.0%	20.8%	14.2%	9.8%	5.6%	6.0%	7.6%	2.6%	15.2%
2025年-2024年のポイント差	0.0	3.4	-1.4	-0.8	-0.4	0.4	0.2	0.4	-2.4

赤字はポイント差の絶対値が3超の項目



上段の数表では単に数値を列挙するだけでなく、2024～2025年の経年変化で比較的大きかったポイント増減を赤字でマークすることで、変化が生じた箇所を把握しやすくしている。

また下段のグラフを俯瞰することで、2024年と2025年における各項目の増減比較や年商規模による傾向差を視覚的に把握できるようになっている。

レポート試読版1:「分析サマリ」

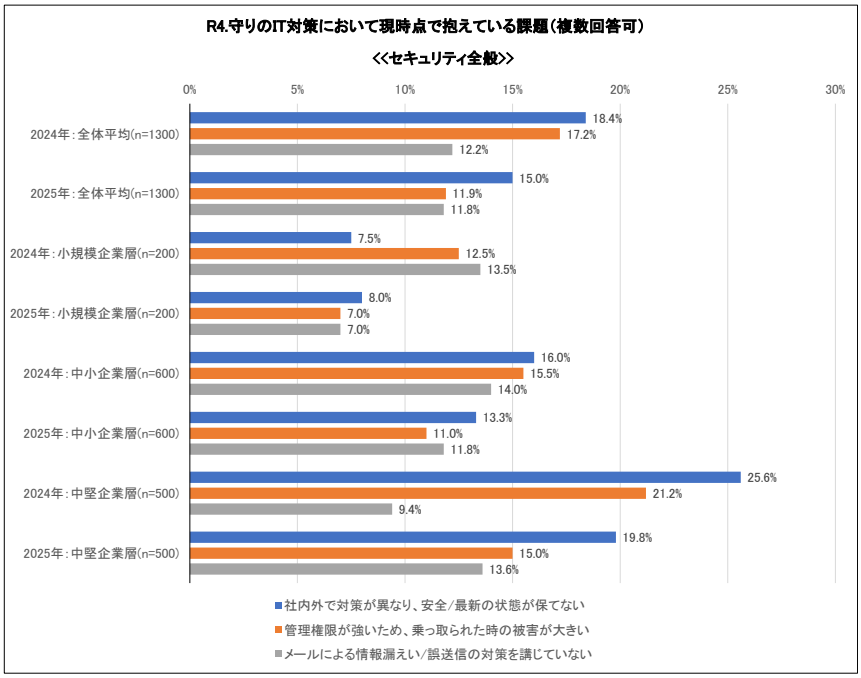
本調査レポートの重要ポイントや今後に向けた提言をまとめたものが「分析サマリ」(PDF形式)である。この分析サマリを通読することで、中堅・中小企業におけるセキュリティ/運用管理/バックアップといった守りのIT対策に関する市場動向を把握することができる。(分析サマリの章構成については本ドキュメントの2ページを参照) 以下の試読版では分析サマリの「第3章: 守りのIT対策における課題の変化と最新動向」の一部を抜粋して掲載している。

第3章: 守りのIT対策における課題の変化と最新動向

本章では、導入済みの守りのIT対策における課題を計15項目に渡る経年変化(2024～2025年)および最新動向を踏まえた8項目に渡る新たな選択肢で尋ねた結果を集計/分析している。

**********中略**********

以下のグラフは<<セキュリティ全般>>における課題項目の経年変化を年商別に集計した結果である。(集計データ￥分析サマリ掲載データ.xlsx「R4経年変化」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

2024年と比べた場合の2025年のポイント増減幅が5超となっている項目を整理すると、次頁のようになる。(右端の数字はポイント差)

全体平均:
「管理権限が強いため、乗っ取られた時の被害が大きい」 -5.3

小規模企業層:
「管理権限が強いため、乗っ取られた時の被害が大きい」 -5.5
「メールによる情報漏えい/誤送信の対策を講じていない」 -6.5

**********中略**********

したがって、2024～2025年にかけてはユーザ企業における<<セキュリティ全般>>の課題意識が低下したことになる。特に「管理権限が強いため、乗っ取られた時の被害が大きい」は中小企業層のポイント増減幅も-4.5に達していることを加味すると、中堅・中小企業の幅広い範囲で減少幅が比較的大きいことになる。そのため、IT企業には管理権限が奪取された場合のリスクとその管理の必要性を啓蒙していく取り組みが求められてくる。

**********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9～10ページを参照

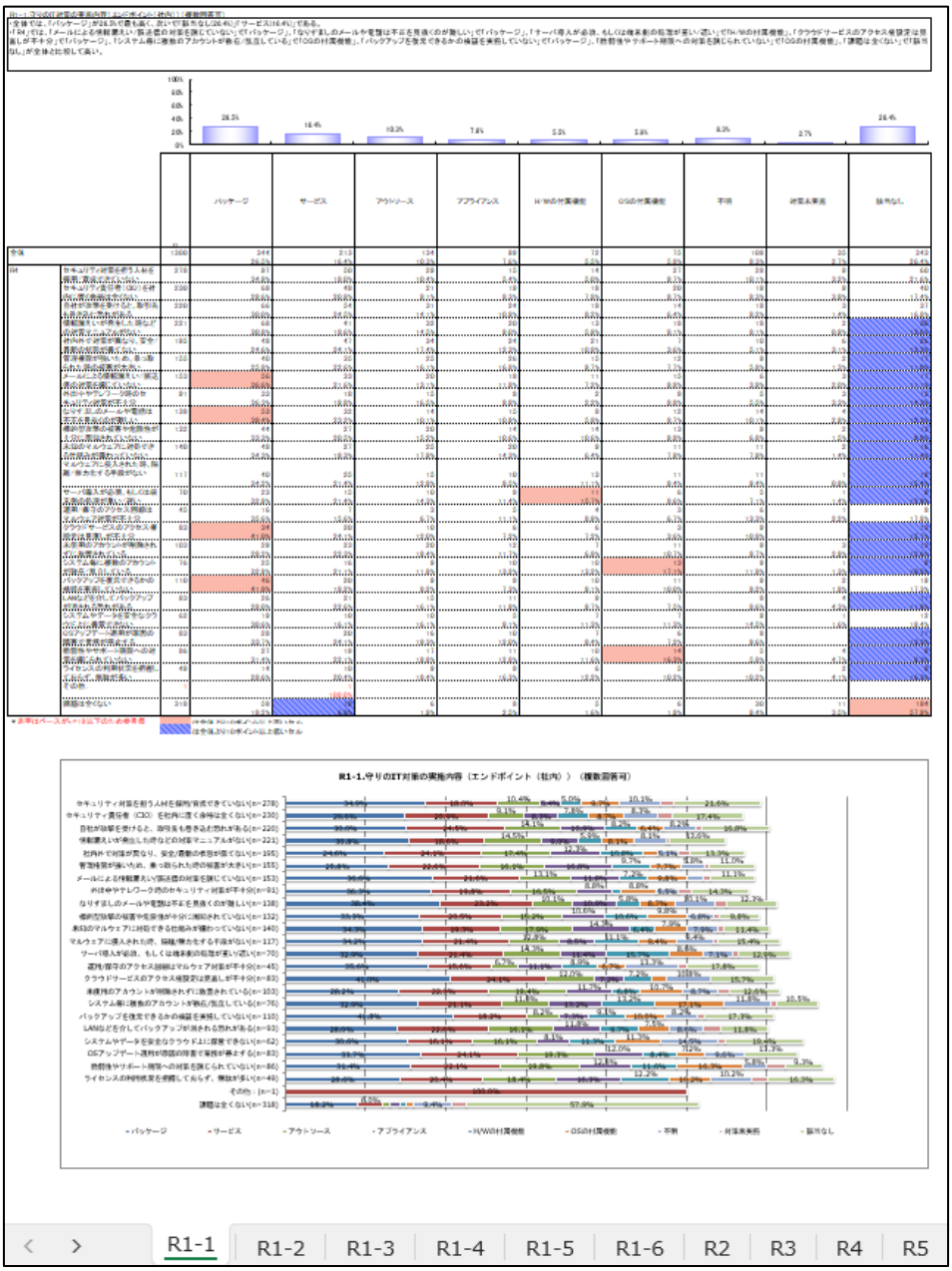
レポート試読版3:「質問間クロス集計データ」

「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質問間クロス集計データファイル【R系列】(【R4】表側).xlsxの「R1-1」シートである。同ファイルは設問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)を除く選択肢設問を集計した結果を収録している。その中の「R1-1」シートには設問「R1-1.守りのIT対策の実施内容(エンドポイント(社内))」を表頭としたデータが収録されている。このシート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に応じて、社内のエンドポイント(PC端末など)における守りのIT対策の実施状況がどう変わってくるか?を知ることができる。

同ファイルの名称『【R系列】(【R4】表側).xlsx 』のうち、【R系列】の部分は数値回答設問を除く選択肢設問が表頭となっていることを表している。また「【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。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既存の調査レポート

2025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

ERP、会計、販売、人事給与、グループウェア、CRM、BIなど、計10分野に渡る業務アプリケーションの導入済み/導入予定の社数シェア、導入年、運用形態（オンプレミス/クラウド）、 課題、ニーズを年商別や業種別などの多角的な視点から集計/分析

【レポート案内】 https://www.norkresearch.co.jp/pdf/2025itapp_rep.pdf

2025年版 DX＆AIソリューションの導入パターン類型化と訴求策の提言レポート増補版

ユーザ企業における人材不足の深刻化を受けて、ご好評いただいている調査レポートにIT管理/運用の人員体制に着目した集計/分析および今後に向けた提言を加えた増補版レポート

【レポートの概要とダイジェスト】 https://www.norkresearch.co.jp/pdf/2025DXAI_user_repex.pdf

2025年版 Windows10から11への移行状況とAI PC活用意向に関する速報レポート

セキュリティ対策のためのOS刷新だけでなく、AI PCのメリットを活かしたポジティブなPC環境を提案するための施策を提言

【レポートの概要とダイジェスト】

Windows 11導入に利点を感じないユーザ企業にも、AI PCの良さは伝えられる

https://www.norkresearch.co.jp/pdf/2025PCflash_rel.pdf

2025年版 中堅・中小ERP市場の経年変化に基づく施策立案レポート（セミカスタムレポート）

生成AIの回答からは得ることが難しい、一貫性のある5年間の経年変化データが導き出す今後の最善策

【レポートの概要とダイジェスト】

顧客層(年商/業種)とベンチマーク対象となるERP製品/サービスを指定した分析例

https://www.norkresearch.co.jp/pdf/2025ERPcustom_rel1.pdf

2025年版 AIエージェント開発における業務シナリオ策定の実践レポート（セミカスタムレポート）

IT企業毎の現状に合わせて、AIエージェントの具体的なタスクフロー(業務シナリオ)を策定する分析/提言を個別に実施

【レポートの概要とダイジェスト】

AIエージェント開発で先駆者となるための業務シナリオ策定

https://www.norkresearch.co.jp/pdf/2025AIAcustom_rel1.pdf

2025年版 中堅・中小向けノーコード/ローコード拡販の実践レポート（セミカスタムレポート）

購入したベンダや販社/SIerの現状を踏まえてツール拡販の施策を個別に分析/提言

【レポートの概要とダイジェスト】

現状を適切に分析すれば、顧客層やツール用途の拡大は十分可能

https://www.norkresearch.co.jp/pdf/2025NLDcustom_rel1.pdf

2025年版 中堅・中小セキュリティ対策のタイプ別クロスセル提案レポート（セミカスタムレポート）

IT企業が提示するターゲット層に合致する分析モデルを選定し、課題/ニーズを元に最適なクロスセル商材を提言

【レポートの概要とダイジェスト】

中堅・中小向けセキュリティ対策提案を「点」から「面」に広げる

https://www.norkresearch.co.jp/pdf/2025Seccustom_rel1.pdf

2025年版 販社/SIerの顧客層タイプ別分析レポート（セミカスタムレポート）

レポートを購入したIT企業毎に顧客層タイプを分析し、タイプに応じた最善策を提言するカスタムメイドの調査レポート

【レポートの概要とダイジェスト】

顧客層タイプを把握すれば、自社の強み/弱み/今後の施策が見えてくる

https://www.norkresearch.co.jp/pdf/2025SPcustom_rel1.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