守りのIT対策における課題＆ニーズ、ベンダ社数シェア、支出額に加えて、守りのIT対策を提案する販社/Slerに対する評価や業務アプリケーション導入/更新における方針との関連性についても分析

2024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

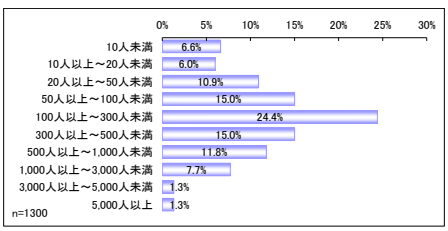
A5.所在地区分:　北海道地方 / 東北地方 / 関東地方 / 北陸地方 / 中部地方 / 近畿地方 / 中国地方 / 四国地方 / 九州・沖縄地方

調査実施時期:　2024年7月～8月

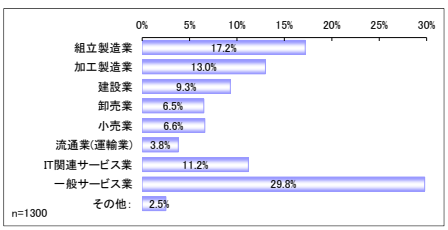
上記に加えて、**「A6.IT管理/運用の人員規模」**（IT管理/運用を担う人材は専任/兼任のいずれか？人数は1名/2～5名/6～9名/10名以上のどれに当てはまるか？）および**「A7.ビジネス拠点の状況」**（オフィス、営業所、工場などの数は1ヶ所/2～5ヶ所/6ヶ所以上のいずれか？ITインフラ管理は個別/統一管理のどちらか？）といった属性についても尋ねており、A1～A7を軸として以降に述べる全ての設問を集計したデータが含まれる。

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。

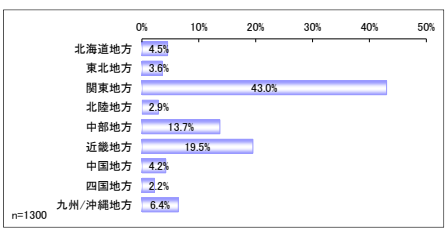
従業員数分布



業種分布



所在地分布



価格:　￥225,000円（税別）
発刊日:　2025年1月20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

ランサムウェアの脅威が高まるにつれて、中堅・中小企業においても従来のパターンファイルでは対策が難しいゼロデイ攻撃やマルウェア侵入後の被害拡大を最小限に抑える出口対策の必要性が高まっている。本調査レポートでは中堅・中小企業に対して守りのIT対策（セキュリティ/運用管理/バックアップ）の実施状況や課題/ニーズを尋ねた結果を分析し、NGAVやXDRを訴求する際のポイントを提言している。さらに、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）の導入社数シェアや守りのIT対策の年額合計費用についても集計/分析を行っている。また、守りのIT対策の委託先/購入先となった販社/SIerのプラス評価/マイナス評価と守りのIT対策における満足点＆課題との関連、業務アプリケーション導入/更新における方針と守りのIT対策における今後のニーズとの関連といったように、更に視点を広げた分析に基づいた提言も述べている。

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9～11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8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対策に関して評価/満足している機能や特徴

「異常な振る舞いを元に未知のマルウェアも検知できる」、「特権/管理アカウントは運用条件を厳しく設定できる」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23項目に渡って尋ねた結果を集計/分析。

第3章：守りのIT対策において現状で抱えている課題

「標的型攻撃の被害や危険性が十分に周知されていない」、「バックアップを復元できるかの検証を実施していない」など、導入済みの守りのIT対策における課題を計23項目に渡って尋ねた結果を集計/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

第2章と同様の計23項目を列挙し、守りのIT対策を担う製品/サービスに対する今後のニーズ（機能や特徴）は何か？を集計/分析。

第5章：守りのIT対策を担う販社/SIerの評価との関連性

導入済みの守りのIT対策の委託先/購入先となった販社/SIerのプラス評価/マイナス評価と守りのIT対策における満足点＆課題との関連性を分析。（例.「DX提案に積極的な販社/SIerはゼロトラストの導入提案においても評価が高いのか？」）

第6章：業務アプリケーション導入/更新における方針との関連性

「ペーパレース化の推進」「自動化による業務効率改善」「生成AIの利用」など、業務アプリケーション導入/更新における様々な方針と守りのIT対策における今後のニーズとの関連性を分析。

第7章：守りのIT対策の開発元（ベンダ）の導入社数シェア

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）を列挙して導入社数シェアを集計/分析。

第8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。

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（2/4）

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。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、「その他」や排他選択肢は除く）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
・複数のネットワーク機器を統合的に管理/保護できる

<<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。

<<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
・複数のネットワーク機器を適切に管理/保護できない

<<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。（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
・複数のネットワーク機器を統合的に管理/保護できる

<<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。

<<セキュリティを主体としたベンダ>>

- トレンドマイクロ　例） Apex（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
- 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） 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） 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。

次頁へ続く

本調査レポートでクロス集計を行っている姉妹編レポートの設問項目（1/2）

本調査レポートでは前頁までに掲載した設問R1～R7に加えて、姉妹編となる2冊の調査レポートに収録された一部の設問とのクロス集計による分析も行っている。集計/分析の対象となっている姉妹編調査レポートの設問は以下の通りである。

1冊目： 2024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

レポート案内： https://www.norkresearch.co.jp/pdf/2024SP_user_rep.pdf

本調査レポートの分析サマリ第5章において、以下に掲載した 守りのIT対策を担う販社/SIerの評価を尋ねた以下の2設問とのクロス集計分析を行っている。

S7. 最も主要な委託先/購入先に関する利点または満足点（複数回答可）

最も主要なベンダや販社/SIerに関して利点と感じている点や評価している点を全て選ぶ設問である。
選択肢は以下の通り。

<<**DX関連の提案や支援に関する項目**>>
- ・DXとは何か？を具体的に示し、業績改善につながる提案を行ってくれる
- ・DXを適切に推進していくための新しいIT商材を積極的に提案してくれる
- ・自社の業務を理解し、DXに必要な社内の改革を一緒に推進してくれる
- ・DXを推進するための自社の人材育成にも積極的に協力してくれる

<<**課金体系や費用面の支援に関する項目**>>
- ・データ量や処理量に応じた従量課金の体系を提案してくれる
- ・講読型/サブスクリプション型の課金体系を提案してくれる
- ・金融機関と連携して、IT活用の資金調達も支援してくれる
- ・IT活用に適用できる補助金制度の利用を支援してくれる

<<**システム構築力や最新技術への対応力に関する項目**>>
- ・ノーコード/ローコードの仕組みなどを用いて、カスタマイズを抑制できる
- ・オンプレミスとクラウドの使い分けが適切であり、両者が連携できている
- ・RPAを用いた業務の自動化など、人材不足への対策も考慮されている
- ・IoTや5Gなど、IT以外のエンジニアリングに近い領域もカバーできている

<<**保守/サポートに関する項目**>>
- ・複合機やLED照明など、IT以外のオフィス全体を保守/サポートしてくれる
- ・装置/機器などのエンジニアリング領域も保守/サポートしてくれる
- ・複数メーカの製品/サービスを一括で保守/サポートしてくれる
- ・状況に応じて保守/サポートの費用を定期的に見直してくれる
- ・セキュリティ対策やトラブル復旧の対応も一括して対応してくれる
- ・サポート期限切れとなったシステムの延命策も提供してくれる

<<**その他**>>
- ・その他：

S8. 最も主要な委託先/購入先に関する課題または不満点（複数回答可）

最も主要な委託先/購入先に関して課題と感じている点や不満を抱いている点を全て選ぶ設問である。
選択肢は以下の通り。

<<**DX関連の提案や支援に関する項目**>>
- ・DXとは何か？の説明が抽象的で、業績改善につながる提案になっていない
- ・DXの推進を謳っているが、提案されるIT商材は従来のものと何ら変わらない
- ・自社の業務を理解しておらず、DXに必要な社内の改革には非協力的である
- ・DXを推進するための自社の人材育成には無関心であり、非協力的である

<<**課金体系や費用面の支援に関する項目**>>
- ・データ量や処理量に応じた従量課金の体系に対応できていない
- ・講読型/サブスクリプション型の課金体系に対応できていない
- ・IT活用に必要な資金の調達については支援してくれない
- ・IT活用に適用できる補助金制度の利用は支援してくれない

<<**システム構築力や最新技術への対応力に関する項目**>>
- ・ノーコード/ローコードなどの新技術に疎く、カスタマイズに頼りがちである
- ・オンプレミスとクラウドの一方に偏りがちで、両者の連携もできていない
- ・RPAを用いた業務の自動化など、人材不足への対策を考慮していない
- ・IoTや5Gなど、IT以外のエンジニアリングに近い領域はカバーできない

<<**保守/サポートに関する項目**>>
- ・複合機やLED照明など、IT以外のオフィス全体は保守/サポートしない
- ・装置/機器などのエンジニアリング領域は保守/サポートしない
- ・保守/サポートが特定メーカの製品/サービスに限定される
- ・保守/サポートの費用は常に固定額であり、割高になっている
- ・セキュリティ対策やトラブル復旧の対応は自社で行う必要がある
- ・サポート期限切れとなったシステムの延命策は提供してくれない

<<**その他**>>
- ・その他：

次頁へ続く

本調査レポートでクロス集計を行っている姉妹編レポートの設問項目（2/2）

前頁からの続き

2冊目： 2024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

レポート案内： https://www.norkresearch.co.jp/pdf/2024itapp_rep.pdf

本調査レポートの分析サマリ第6章において、業務アプリケーション導入/更新における方針を尋ねた以下の設問とのクロス集計を行っている。

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）：

業務アプリケーションの分野に依存しない全体的な方針を尋ねた設問である。
選択肢は以下の通り。

<<**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	例） パートナSIerを認定/支援する制度が充実している
・自動化によって業務効率を改善できるか？を重視する	例） 様々なRPAシステムを連携オプションで選択できる
・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	例） 独自の画面や項目を標準機能の枠内で作成できる
・データ分析による高度な判断が行えるか？を重視する	例） 工場や店舗の稼働データを元にシフトを最適化する
・顧客や取引先と遠隔で対話できるか？を重視する	例） Web会議を用いたセミナーや商談を開催できる
・従業員の働きやすさに貢献できるか？を重視する	例） 従業員同士が交流できる社内SNSを開設できる
・必要な情報を対話的に検索できるか？を重視する	例） チャットを用いて在庫の照会を対話的に行える
・ペーパレス化を推進できるアプリケーションを選ぶ	例） AI-OCRによる紙面読み取りの機能が充実している
・在宅勤務の対応が容易なアプリケーションを選ぶ	例） ビデオ会議が包含されており、いつでも対話できる
・ブラウザのみで利用できるアプリケーションを選ぶ	例） 個々のPCに専用モジュールを導入する必要がない

<<**社会環境や国際情勢の変化に関連する項目**>>

・賃上げを実現/継続するための利益率の向上を重視する	例） データ分析を活用したアップセル/クロスセルの販売施策を進める
・人材不足に対処するための省力化や効率化を重視する	例） ヘッドセットを通じて熟練者が若手を遠隔で支援できるようにする
・外国人労働者の活用を見据えた機能の強化を重視する	例） 業務マニュアルを自動で各国語に翻訳できる仕組みを導入する
・省エネ対策の実現や認定取得にも役立つかを重視する	例） Scope3まで含めたCO2排出量の算出を行える体制を整えておく
・経済安全保障に伴う環境変化への対応力を重視する	例） 国際紛争に備えて、調達先を迅速に切り替えられるようにしておく

<<**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	例） 販売管理システム上でチャットで指示を出して見積書を自動生成する
・生成AIは業務アプリケーションと切り離して利用する	例） キャッチコピーやロゴデザインを自動作成してくれるサービスを利用する
・関連する法整備が整うまで生成AIの利用は控える	例） 著作権侵害の恐れがあるため、業務での生成AIの利用は不安がある
・AIが自社の知見やデータを学習することは拒否する	例） 知らない間に自社が入力したデータも学習に利用されるのは避けたい

<<**導入/運用や費用に関連する項目**>>

・テスト環境上で一定期間無償利用できるかを重視する	例） 試用版をインストールして実際のデータを登録して試用する
・購入ではなく、サブスクリプション型の費用体系を選ぶ	例） 会計パッケージを月額支払いのサブスク形式で利用する
・データ量や人数に応じた従量制の課金体系を選ぶ	例） データ容量で課金されるオンラインストレージを利用する
・売上などの成果報酬に基づく課金体系を選ぶ	例） 販売管理システムの費用を売上の増分に応じて支払う

<<**その他**>>

・その他：
・特に方針はない（排他）

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。

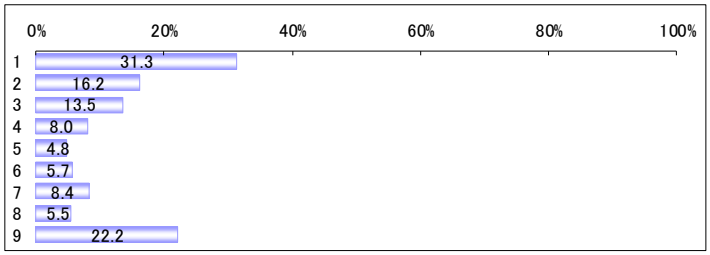
表側を伴わない集計データ: 単純集計データ
命名規則: 【表頭名】単純集計.xlsx

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]

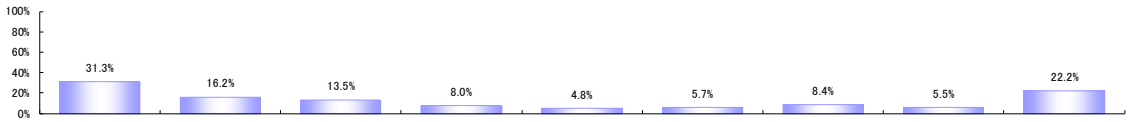
表側を設定した状態での集計結果を積み上げ横棒グラフとして表示している。可視性を考慮して、5%未満の数値についてはグラフ中の数字表記を非表示としている。表頭となる設問が単一回答設問である場合は目盛に値の付いた横軸が表示される。複数回答設問の場合には複数の選択肢を合計した数値には重複が含まれるため、誤った数値の読み取りを避ける目的で横軸の目盛り値を非表示としている。

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



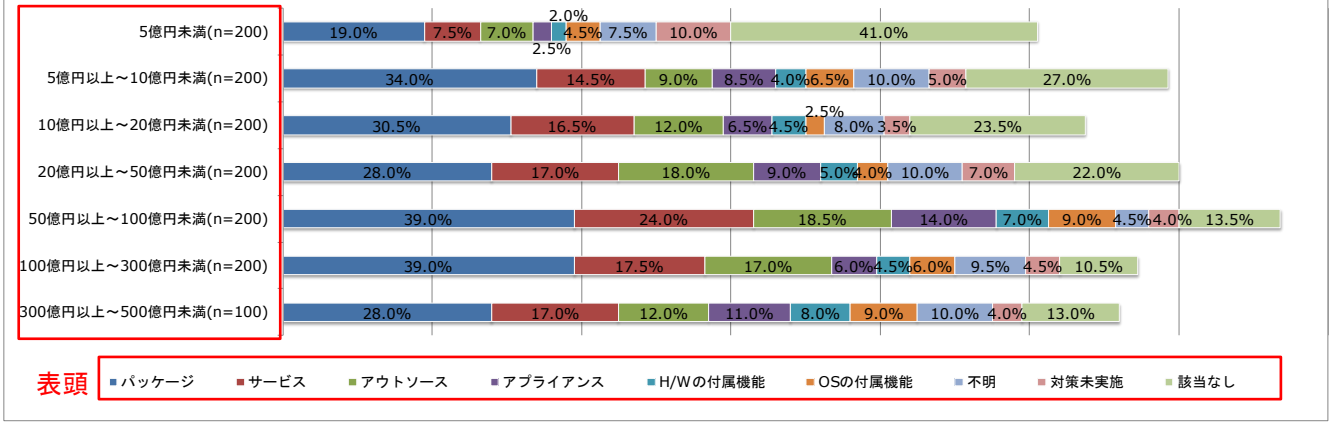
表側 / 表頭

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 (※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)	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(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)

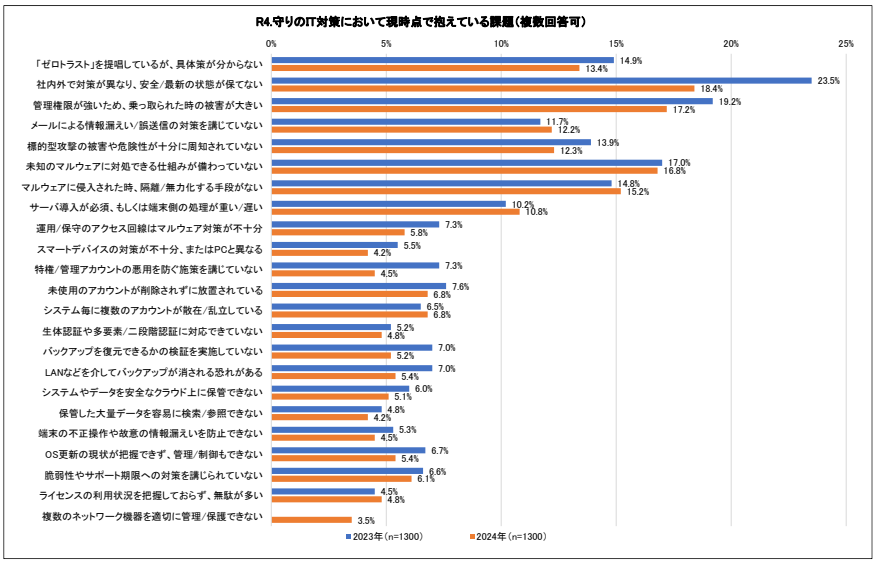
レポート試読版1:「分析サマリ」その1

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対策において現状で抱えている課題」の一部を抜粋して掲載している。

第3章. 守りのIT対策において現状で抱えている課題

本章では計23項目に渡る選択肢を列挙し、中堅・中小のユーザ企業が守りのIT対策においてどのような課題を抱えているか?を集計/分析している。

以下のグラフは設問「R4.守りのIT対策において現時点で抱えている課題」の結果を中堅・中小企業全体で集計したものだ。(集計データ¥分析サマリ掲載データ.xlsx「第2～4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

- 2023年と2024年の双方において回答割合が1割超となっているのは以下の8項目である。
- 「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

**********中略**********

「社内外で対策が異なり、安全/最新の状態が保てない」は2023年と比較した場合の2024年の増減幅が-5.1ポイントと最も大きく減少しているものの、2024年においても18.4%と最も高い値を示している。したがって、IT企業としてはオンプレミスとクラウドの双方で一貫した守りのIT対策を進めていくことが最も重要となってくる。

同様に「管理権限が強いため、乗っ取られた時の被害が大きい」も2023年と比較した2024年の値は-2.0ポイントと減少幅が比較的大きいが、2024年における値は17.2%と2番目に高い。今後は中堅・中小企業に対しても特権アクセス管理(Privileged Access Management)の考え方を採用して、特権IDや特権アカウントに管理において、多要素認証を導入する、特権利用時には承認のプロセスを挟むと共に操作を記録する、パスワードを定期的に変更する仕組みを設ける、付与する権限は必要最小限に留めるなどの対処を講じることが大切だ。

**********以下、省略**********

レポート試読版2:「分析サマリ」その2

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6章.業務アプリケーション導入/更新における方針との関連性」の一部を抜粋して掲載している。

第6章. 業務アプリケーション導入/更新における方針との関連性

本章では姉妹編となる調査レポート「2024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」に収録されている設問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」の違いにより、本調査レポートの設問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」の回答割合がどう変わるか?を確認していく。これにより、「ペーパレース化の推進」「自動化による業務効率改善」「生成AIの利用」など、業務アプリケーション導入/更新の方針と守りのIT対策における今後のニーズの関連性を知ることができる。

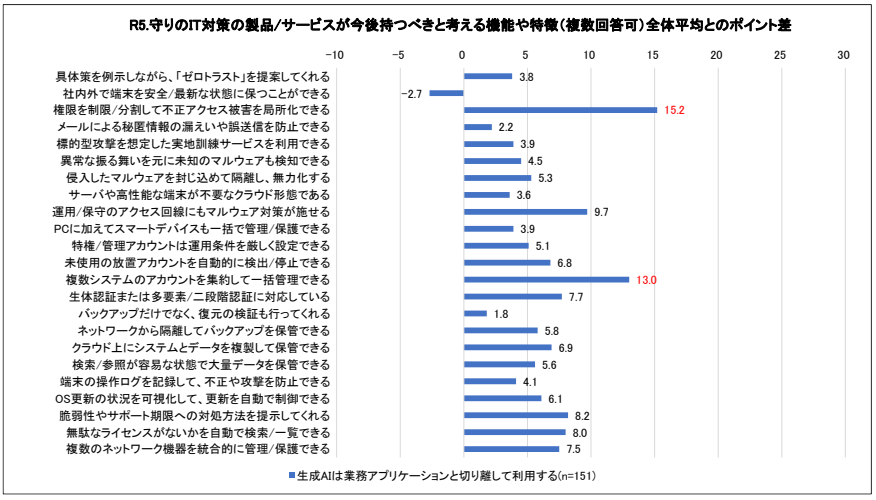
設問P0「業務アプリケーションの導入/更新に関する全体的な方針」の選択肢は以下の通り。

<<**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

**********中略**********

以下のグラフは設問P0において「生成AIは業務アプリケーションと切り離して利用する」と回答したユーザ企業の設問R5の回答状況(全体平均とのポイント差)を示したものだ。(集計データ¥分析サマリ掲載データ.xlsx「第6章」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

**********中略**********

「生成AIは業務アプリケーションと切り離して利用する」というユーザ企業では全体平均と比べて
・権限を制限/分割して不正アクセス被害を局所化できる
・複数システムのアカウントを集約して一括管理できる
といったニーズが相対的に高いことが確認できる。
つまり、つまり、業務アプリケーションと分離して生成AIを活用しようとするユーザ企業に対しては「アクセス権限の精緻化による被害の局所化」といった安全性の強化と「アカウントの集約による一括管理」といった利便性の強化の双方を並行して進める取り組みが有効となる。

**********以下、省略**********

レポート試読版3:「主要分析軸集計データ」

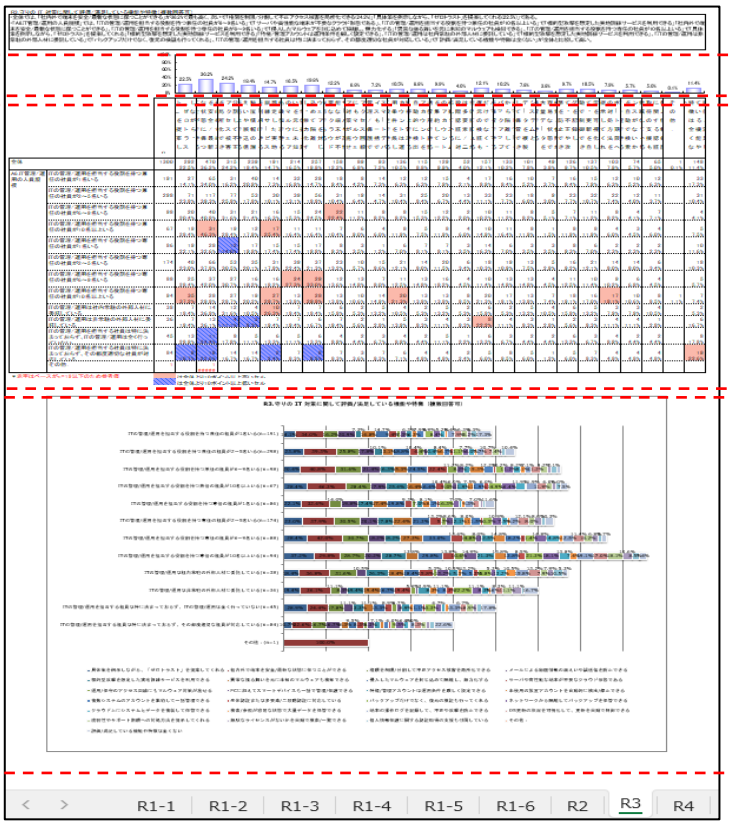
「設問項目」に掲載した設問結果を年商、業種、従業員数、所在地などの基本属性を軸として集計したものが、「主要分析軸集計データ」であり、Microsoft Excel形式で調査レポート内に同梱されている。以下の試読版に掲載したものは「A6. IT管理/運用の人員体制」を集計軸として本調査レポートの各設問の結果を集計した結果の一部である。

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)



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9～11ページを参照

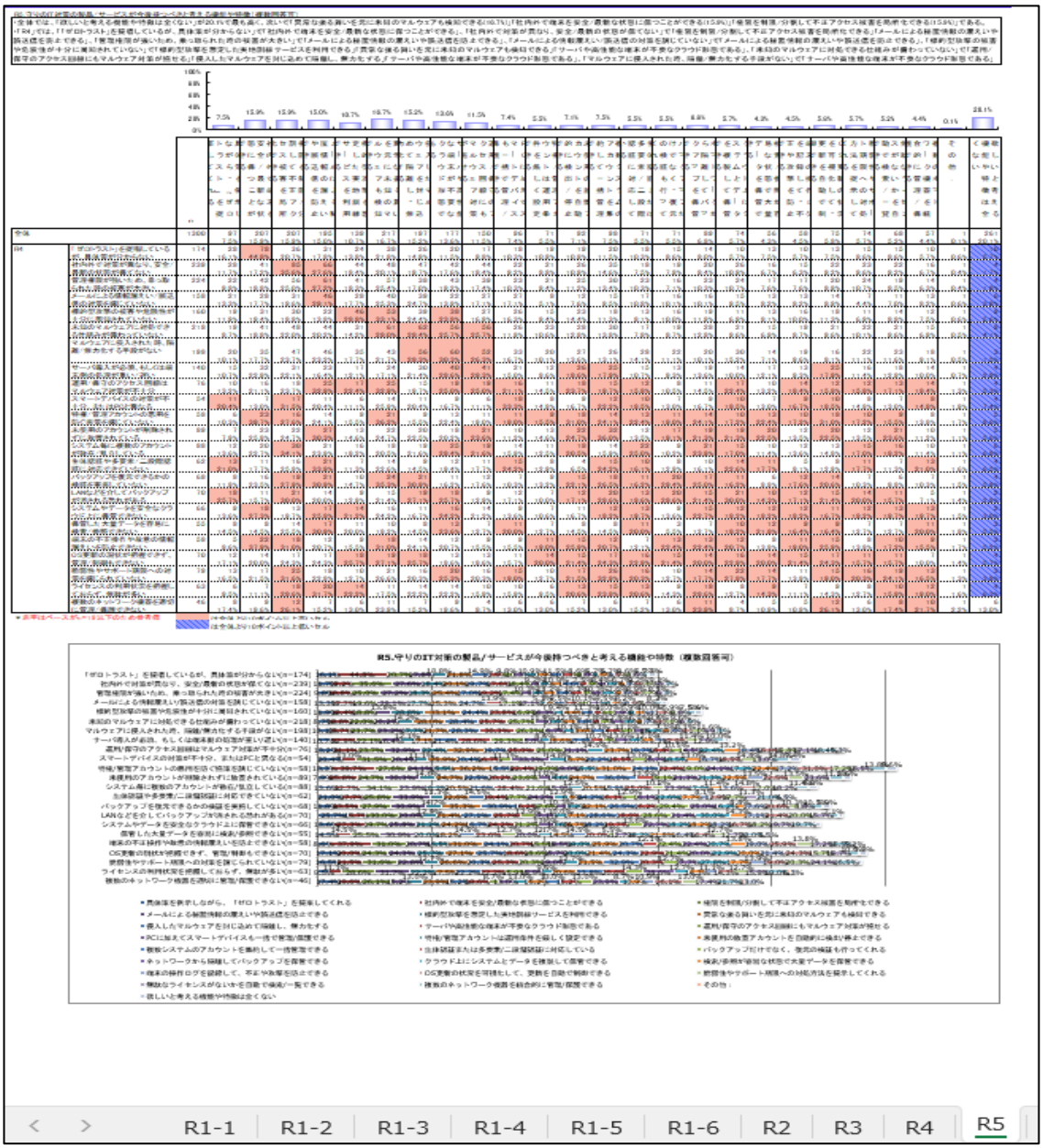
レポート試読版4:「質問間クロス集計データ」

「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質問間クロス集計データファイル【R系列】(【R4】表側).xlsxの「R5」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「R5」シートには設問「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、今後のニーズ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。



レポート試読版5:「公開リリース(サンプル/ダイジェスト)」

前頁までに掲載した紹介資料に加えて、ノークリサーチのホームページ上では各種調査レポートのサンプル/ダイジェストをリリースとして公開している。本調査レポートに関連するリリースは以下の通りである。

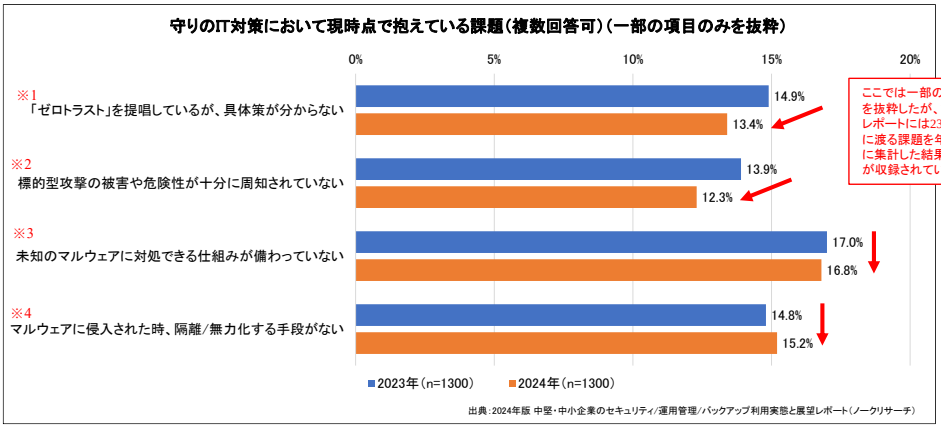
中堅・中小企業のセキュリティ課題＆ゼロトラスト導入とDX推進および生成AI活用の関係性

https://www.norkresearch.co.jp/pdf/2024Sec_user_rel1.pdf

＜販社/SIerのDX提案状況や業務アプリ導入/更新のユーザ方針を考慮すると、守りのIT提案の精度も上がる＞
■中堅・中小向けにもゼロデイ攻撃を前提とした「NGAV」と出口対策を含む「XDR」が不可欠
■DX推進に取り組む販社/SIerはマルウェア対策においてもユーザ評価が高い傾向にある
■業務アプリと切り離した生成AI活用を考えるユーザはアクセス権の局所化ニーズが高い

セキュリティ、運用管理/資産管理、バックアップといった守りのIT対策はユーザ企業の業績に関係なく、ITを活用する上では欠かすことのできない取り組みだ。とは言え、中堅・中小企業はIT支出も限られるため、ベンダや販社/SIerとしては最大限の効果を得られる守りのIT対策を提示する必要がある。本リリースの元となる調査レポートでは有効回答件数1300社の中堅・中小企業を対象として、守りのIT対策の課題やニーズなどに関する様々な集計/分析を行っている。

以下のグラフは「守りのIT対策において現時点で抱えている課題」を尋ねた結果の一部を2023年と2024年で比較したものだ。(調査レポートでは計23項目に渡って守りのIT対策の課題を尋ねており、課題項目の一覧は次頁に掲載している)

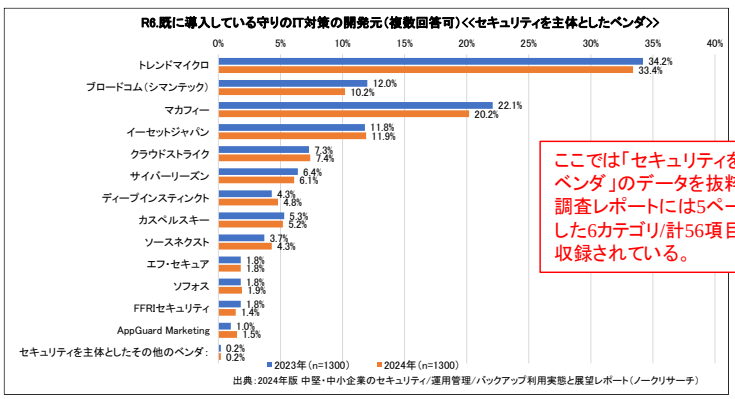


中堅・中小企業におけるセキュリティ対策の実施手段、ベンダ選択、支出額の変化

https://www.norkresearch.co.jp/pdf/2024Sec_user_rel2.pdf

＜従来の分野や区分に固執せずに、柔軟な視点で市場を捉えることが大切＞
■「社内エンドポイント」の守りのIT対策を実施する手段としては「パッケージ」が大幅に減少
■「クラウドサービス＋軽量エージェントによるNGAV/XDR」を分かりやすく伝える必要がある
■ベンダのシェア動向ではセキュリティと運用管理/資産管理の双方に跨る動きにも要注目
■H/Wの機能を活かしたエンドポイント保護に取り組むユーザ企業は守りのIT支出額が高い

本リリースの5ページに列挙したように、調査レポートでは6カテゴリ/計56項目の選択肢を提示して、中堅・中小企業に対して導入済みの守りのIT対策を担う製品/サービスの開発元(ベンダ)を尋ねている。以下のグラフはその中から「セキュリティを主体としたベンダ」のカテゴリにおける結果を2023年と2024年で比較したものだ。



ご好評いただいているその他の調査レポート （各冊：225,000円税別）

『2024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』

従来の社数シェアやユーザ評価に加えて、各アプリ分野の重要トピックに関する新たな分析/提言まで網羅した進化版レポート

【レポートの概要と案内】 https://www.norkresearch.co.jp/pdf/2024itapp_rep.pdf

【リリース(ダイジェスト)】

グループウェアやWeb会議を起点とした生成AIの普及の第一歩
https://www.norkresearch.co.jp/pdf/2024itapp_gw_rel.pdf

「コンポーザブルERP」は中堅・中小向けERP市場にも広まるか？
https://www.norkresearch.co.jp/pdf/2024itapp_erp_rel.pdf

中堅・中小向け会計管理パッケージと経費精算サービスの役割分担
https://www.norkresearch.co.jp/pdf/2024itapp_acc_rel.pdf

ワークフロー拡販に必要な視点は年商＆運用形態+ERP導入状況
https://www.norkresearch.co.jp/pdf/2024itapp_wf_rel.pdf

SaaSが中堅・中小向け生産管理システムにもたらす変化
https://www.norkresearch.co.jp/pdf/2024itapp_ppc_rel.pdf

販売・仕入・在庫管理はシェア差が縮小、CRM更新が新たな商機
https://www.norkresearch.co.jp/pdf/2024itapp_sbc_rel.pdf

勤怠管理を起点とした中堅・中小向け人事給与システムの進化
https://www.norkresearch.co.jp/pdf/2024itapp_hrw_rel.pdf

中堅・中小向けBI導入提案に不足している視点
https://www.norkresearch.co.jp/pdf/2024itapp_bi_rel.pdf

法整備や経済安全保障が中堅・中小生成AI活用に与える影響
https://www.norkresearch.co.jp/pdf/2024itapp_p0_rel.pdf

セールスフォース一強状態のCRM市場に変化は起きるか？
https://www.norkresearch.co.jp/pdf/2024itapp_crm_rel.pdf

文書管理・オンラインストレージサービス市場の新たな成長段階
https://www.norkresearch.co.jp/pdf/2024itapp_dm_rel.pdf

『2024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』

80社超に及ぶIT企業の社数シェア、商材ポートフォリオ、プラス評価/マイナス評価に加えてIT導入で得られる17種類の成功体験に基づいた今後有望なITソリューション提案を提言、さらには年間IT支出の市場規模（年商別/業種別/地域別）も網羅

【レポートの概要と案内】 https://www.norkresearch.co.jp/pdf/2024SP_user_rep.pdf

【リリース(ダイジェスト)】 17種類に渡る「ユーザ企業における成功体験」から導かれるIT導入提案のキーポイント
https://www.norkresearch.co.jp/pdf/2024SP_user_rel1.pdf

中堅・中小企業における企業属性別(年商/業種/地域)＆商材別のIT支出市場規模
https://www.norkresearch.co.jp/pdf/2024SP_user_rel2.pdf

今後伸びるDX分野およびIT企業における成功体験スコアとDX比率の関係
https://www.norkresearch.co.jp/pdf/2024SP_user_rel3.pdf

『2024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』

サーバはクラウドファーストの加速とオンプレ回帰のどちらに進むのか？PCでWindows 11移行を加速させるための施策とは？

【レポートの概要と案内】 https://www.norkresearch.co.jp/pdf/2024SrvPC_user_rep.pdf

【リリース(ダイジェスト)】

中堅・中小ハイブリッドクラウドの適用状況と解決すべき課題
https://www.norkresearch.co.jp/pdf/2024SrvPC_user_rel1.pdf

中堅・中小サーバ環境におけるクラウド移行とオンプレ回帰の実態
https://www.norkresearch.co.jp/pdf/2024SrvPC_user_rel2.pdf

HCI(ハイパーコンバージドインフラ)の導入状況、社数シェア、導入障壁
https://www.norkresearch.co.jp/pdf/2024SrvPC_user_rel3.pdf

中堅・中小サーバ市場(オンプレミス＆クラウド)のシェア動向
https://www.norkresearch.co.jp/pdf/2024SrvPC_user_rel4.pdf

Windows 11への移行を阻害している要因とその打開策
https://www.norkresearch.co.jp/pdf/2024SrvPC_user_rel5.pdf

中堅・中小エンドポイント環境のOSと端末/サービスのシェア動向
https://www.norkresearch.co.jp/pdf/2024SrvPC_user_rel6.pdf

中堅・中小ストレージ環境の形態選択と活用課題の動向
https://www.norkresearch.co.jp/pdf/2024SrvPC_user_rel7.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