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した一冊

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

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

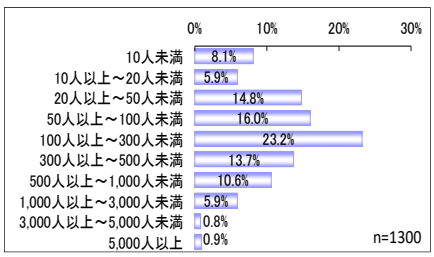
A5.所在地区分:　北海道地方 / 東北地方 / 関東地方 / 北陸地方 / 中部地方 / 近畿地方 / 中国地方 / 四国地方 / 九州・沖縄地方

調査実施時期:　2022年7月～8月

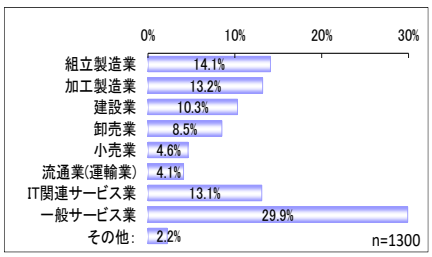
上記に加えて、**「A6.IT管理/運用の人員規模」**(IT管理/運用を担う人材は専任/兼任のいずれか？人数は1名/2～5名/6～9名/10名以上のどれに当てはまるか？)および**「A7.ビジネス拠点の状況」**(オフィス、営業所、工場などの数は1ヶ所/2～5ヶ所/6ヶ所以上のいずれか？ITインフラ管理は個別/統一管理のどちらか？)といった属性についても尋ねており、A1～A7を軸として以降に述べる全ての設問を集計したデータが含まれる。

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。

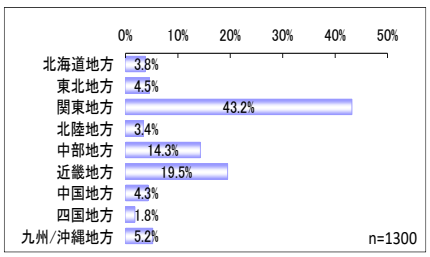
従業員数分布



業種分布



所在地分布



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。

分析サマリの構成

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4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。それらの詳細については、以下の「用語説明とファイル命名規則」で述べる。分析サマリは以下の5つの章から構成されており、前半の3つの章では守りのIT対策の実施状況、課題、基本方針といったユーザ企業における実態に焦点を当て、後半の2つの章では守りのIT対策を提供する側であるIT企業に関連する動向ならびにユーザ企業が守りのIT対策に対して許容可能な年額合計費用について述べている。

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

用語説明とファイル命名規則

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。

次頁へ続く

用語説明とファイル命名規則（前頁からの続き）

【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

表側が設定されていない集計結果は「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っている。ファイル名は集計対象となる設問名に「単純集計」というキーワードを付加した書式となる。例えば、本調査レポートの設問番号は全てRの接頭辞が付いており、全設問の単純集計データファイル名は「【R系列】単純集計.xlsx」となる。

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、選択肢から回答を選ぶ形式の設問を表頭として、「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系列選択肢】(【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、設問「R2.守りのIT対策における現状の課題」を表頭とし、設問「R4.守りの IT 対策に関する導入を増やすIT企業」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「【R2】(【R4】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。

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。

[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。

[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。

[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。

[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の値を非表示としている。

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～R6の計6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。R6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」、R6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

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「実施手段」（どのように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。それぞれ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）

守りのIT対策の実施内容は上記に列挙した「実施箇所」と「実施手段」の組み合わせで表すことができる。そこで、設問R1では6項目に渡る「実施箇所」をR1-1～R1-6の枝番設問とし、8項目（「該当なし」を除く）の「実施手段」を各枝番設問の選択肢とすることで「実施箇所」と「実施手段」の組み合わせを網羅した設問構成としている。したがって枝番設問R1-1～R1-6の設問文と選択肢は以下の通りとなる。「実施手段」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」

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

R1-3.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」

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対策における現状の課題（複数回答可）

24項目に渡る以下の選択肢を列挙し、セキュリティ/運用管理/バックアップといった守りのIT対策において直面している課題を尋ねた設問である。

<<**自社の体制/人員に関する項目**>>
- 守りのIT対策を担う社内人材が不足している
- 従業員の守りのIT対策に対する意識が低い
- ランサムウェア被害に遭う危険性がある
- 「シャドーIT」を把握/制御できない

<<**エンドポイントに関する項目**>>
- 社外に持ち出した端末の管理/保護が不十分である
- 個人が所有する端末の管理/保護が不十分である
- URLフィルタリングでは管理/制御が不十分である
- Windows 10/11の機能更新管理が負担である
- パスワード付ZIPファイル添付の代替策がない
- USBメモリによるデータ授受の代替策がない
- アカウントの管理が煩雑になっている

<<**サーバ/ストレージに関する項目**>>
- バックアップデータをサーバに復元できる確証がない
- アクセス/処理が増加した時の対策が不十分である
- 障害や故障に備えた監視/予防が不十分である
- データ容量の増加に対処できる良い方法がない
- クラウドでは従来と同じサーバ管理が行えない

<<**ネットワークに関する項目**>>
- VPNでは安全性や十分な通信帯域を確保できない
- 外出時でも安全にモバイル接続できる手段がない
- 社内とクラウドサービスの接続を管理/把握できない

<<**その他**>>
- データが様々なクラウドサービスに分散して管理できない
- 利用するクラウドサービスが多く、逆に管理負担が増える
- 災害時の事業継続/バックアップ対策が不十分である
- IT以外の設備における守りのIT対策が不足している
- サプライチェーンでの守りのIT対策が不足している
- その他：

R3.守りのIT対策における今後の方針（複数回答可）

19項目に渡る以下の選択肢を列挙し、セキュリティ/運用管理/バックアップといった守りのIT対策における基本的な方針（製品/サービスの選定において、重視する事柄など）を尋ねた設問である。

<<**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」

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

・「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）

<<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で、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）

次頁へ続く

本調査レポートの設問項目（4/5）

前頁からの続き

・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

R4.守りのIT対策に関する導入を増やすIT企業（複数回答可）

11区分に渡る以下のIT企業の種別を列挙して、セキュリティ/運用管理/バックアップといった守りのIT対策に関する製品/サービスを新たに導入する予定がある、もしくは導入を今後増やす予定であるIT企業を尋ねた設問である。

・セキュリティ主体のベンダ	例）トレンドマイクロ、シマンテック（ブロードコム）、キヤノンITソリューションズ
・運用管理主体のベンダ	例）Sky、クオリティソフト、エムオーテックス、ハンモック
・バックアップ主体のベンダ	例）ベリタステクノロジーズ、Arcserve、クエスト・ソフトウェア、ストレージクラフト
・国内の大手H/Wベンダ	例）NEC、富士通、日立製作所
・外資系の大手H/Wベンダ	例）HPE、デル・テクノロジーズ、レノボ・ジャパン、シスコシステムズ
・大手の独立系販社/SIer	例）大塚商会、オービック、TISインテックグループ
・複合機系の販社/SIer	例）リコー、富士フイルムビジネスイノベーション、キヤノンマーケティングジャパン
・キャリア系販社/SIer	例）NTTコミュニケーションズ、KDDIまとめてオフィス、SBテクノロジー
・地場の販社/SIer	例）地域に密着した近隣の販社/SIer
・OSベンダ	例）日本マイクロソフト、レッドハット
・クラウド事業者	例）グーグル、アマゾンウェブサービスジャパン
・その他：	

R5.守りのIT対策に関する導入を減らすIT企業（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対策に関する製品/サービスを既に導入しているが、今後は導入をやめる、もしくは減らす予定のIT企業を尋ねた設問である。選択肢は設問R4と同様。

設問「R4」と設問「R5」を比較することで、今後の導入が伸びる/縮小するIT企業の種別はどれか？を知ることができる。
さらに、本調査レポートには設問「R4」「R5」を表側として、設問「R2.守りのIT対策における現状の課題」ならびに設問「R3. 守りのIT対策における今後の方針」を集計した以下の質問間クロス集計データも収録されている。

【R2】(【R4】表側).xlsx
【R2】(【R5】表側).xlsx
【R3】(【R4】表側).xlsx
【R3】(【R5】表側).xlsx

これらを参照することで、守りのIT対策を提供するIT企業の種別によってユーザ企業が抱える課題や今後の方針がどのように変わってくるか？も把握することができる。

次頁へ続く

本調査レポートの設問項目（5/5）

R6.守りのIT対策に対して許容可能な年額合計費用（万円）

守りのIT対策に対して許容可能な年額合計費用（万円）を数値記入形式で尋ねた設問である。ここでの年額合計費用とは、ハードウェアとOS/ファームウェアといったインフラは除外し、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。本設問の集計データは平均値となる。例えば、単純集計データでは中堅・中小企業全体の平均値、年商を表側とした主要分析軸集計データにおいては年商区分毎の平均値となる。

設問「R6」の集計結果を収録したファイル名は「【R系列数値】(【表側名】表側).xlsx」となっている。例えば、許容可能な年額合計費用の平均値を年商別に集計した主要分析軸集計データのファイル名は「【R系列数値】(【A1】表側).xlsx」、設問「R2.守りのIT対策における現状の課題」別に許容可能な年額合計費用の平均値を集計した質問間クロス集計データのファイル名は「【R系列数値】(【R2】表側).xlsx」となっている。

次頁へ続く

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。(章構成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対策の実施状況」の冒頭部分を抜粋して掲載している。

第 1 章.守りの IT 対策の実施状況

本章では 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のか？の実態を明らかにしている。

設問「R1. 守りの IT 対策の実施内容」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 対策の現状を「実施箇所」（何処に対策を講じているか？）と「実施手段」（どのように対策を講じているか？）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

：

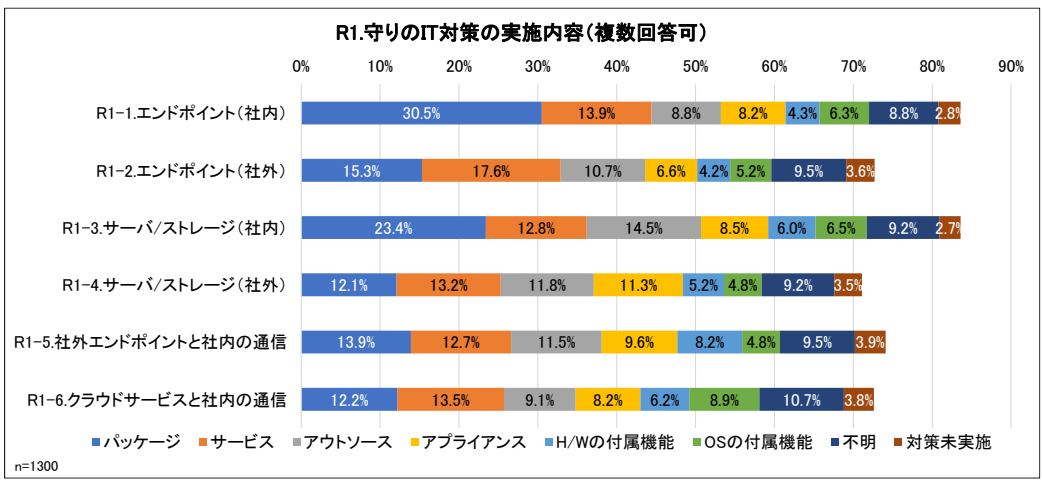
実施手段：　**********中略**********

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

：

**********中略**********

以下は設問 R1（6 つの実施箇所に対応する R1-1～R1-6 の枝番設問で構成される）の結果を中堅・中小企業全体で集計して、1 つのグラフにまとめたものだ。（集計データ￥単純集計データ￥【R 系列】単純集計.xlsx）



以下では 6 つのグラフを「エンドポイント」(R1-1 と R1-2)、「サーバ/ストレージ（R1-3 と R1-4)、「ネットワーク」(R1-5、R1-6）の 3 つの観点で詳しく見ていくことにする。

**********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系列選択肢】(【A6】表側).xlsx』となっている。【R系列選択肢】とは、本調査レポートの設問項目のうちで、与えられた選択肢から選んで回答する形式の設問群(数値記入形式である設問「R6」を除いた全設問)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系列選択肢】(【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、さらに専任/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などがどのような異なるか？を確認できる。
同様に年商別の傾向は『【R系列選択肢】(【A1】表側).xlsx』(A1が年商区分を表す)、業種別の傾向は『【R系列選択肢】(【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。

本ドキュメントの4～8ページに記載されているように、主要分析軸集計データにおける設問数は計11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.IT管理/運用の人員規模」「A6.ビジネス拠点の状況」「A7.所在地」の7項目あるため、本調査レポートにおける「主要分析軸データ」の集計データ数は11設問×7属性＝77に達する。
(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2ページを参照

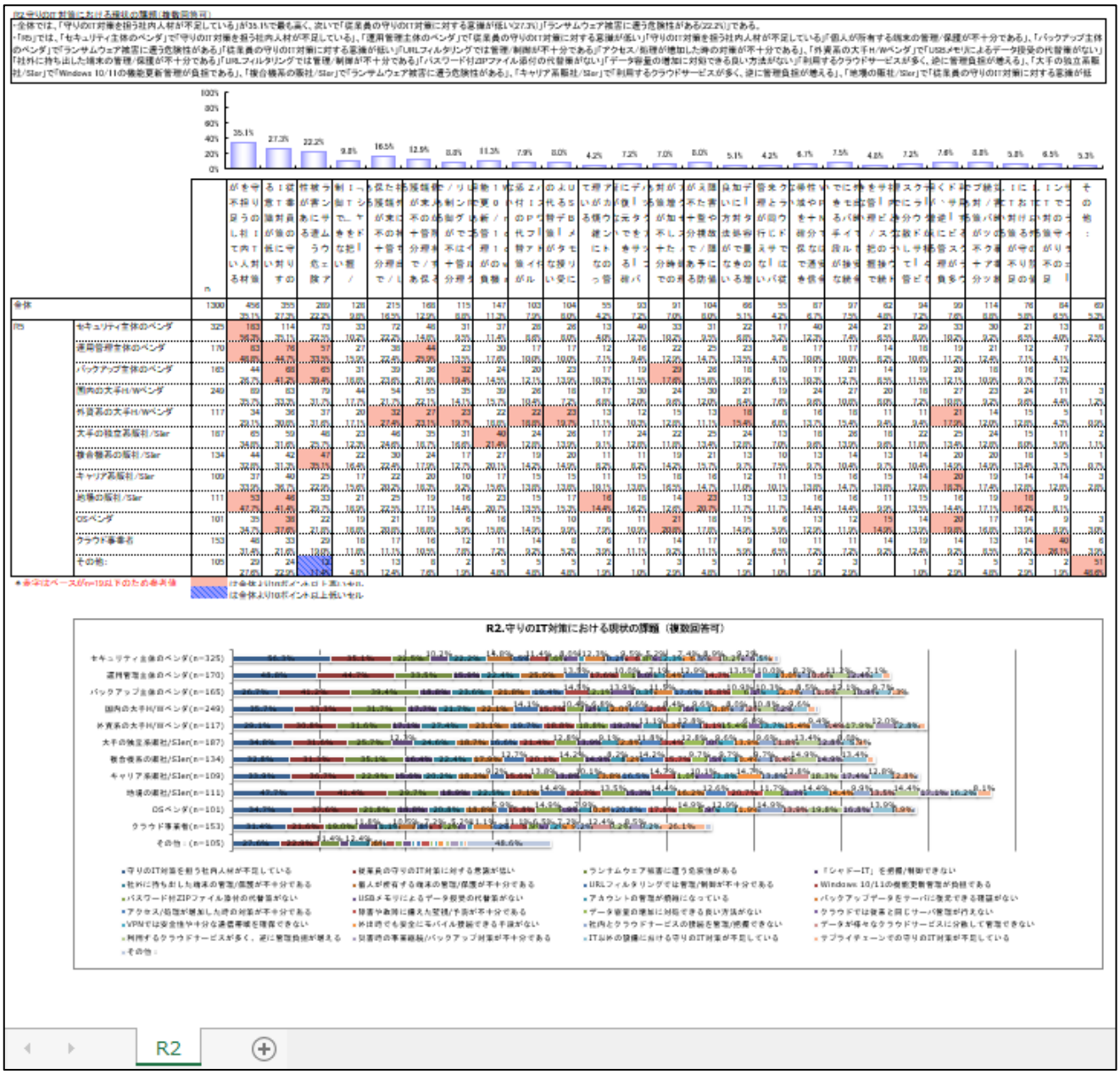
レポート試読版3(「質問間クロス集計データ」)

「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「R2.守りのIT対策における現状の課題」を設問「R5.守りのIT対策に関する導入を減らすIT企業」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対策の導入が減るIT企業においてはユーザ企業がどのような課題を抱えているケースが多いのか？を知ることができる。IT企業側としては、この課題を解消することができれば守りのIT対策の導入減少を回避することが期待できる。

以下のMicrosoft Excelファイル名は『【R2】(【R5】表側).xlsx 』となっている。「【R5】表側」の部分は設問「R5」が集計の軸(表側)となっていることを示している。【R2】の部分は設問「R2」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。



本調査レポートの価格とご購入のご案内

『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』

【価格】180,000円(税別) 【発刊日】2023年1月16日

【媒体】CD-ROMまたはダウンロード (分析サマリ: PDF形式、集計データ: Microsoft Excel形式)

【リリース(ダイジェスト)】

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
https://www.norkresearch.co.jp/pdf/2022Sec_user_rel1.pdf

中堅・中小企業におけるセキュリティ/運用管理/バックアップの課題と支出額/購入先選定の関連
https://www.norkresearch.co.jp/pdf/2022Sec_user_rel2.pdf

【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

ご好評いただいているその他の調査レポート(1/2)(各冊:180,000円税別)

『2022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』

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

【リリース(ダイジェスト)】

ERP:

基幹系統合とクラウド併用で再編が進みつつあるERP市場
https://www.norkresearch.co.jp/pdf/2022itapp_erp_rel.pdf

生産管理:

運用形態や課題が変化しつつある中堅・中小向け生産管理システム
https://www.norkresearch.co.jp/pdf/2022itapp_ppc_rel.pdf

会計管理:

中小企業の会計管理でもニーズが高まるAIを活用した経営分析や監査支援
https://www.norkresearch.co.jp/pdf/2022itapp_acc_rel.pdf

販売・仕入・在庫管理:

販売管理の重点課題は売上分析から在庫管理へと移行
https://www.norkresearch.co.jp/pdf/2022itapp_sbc_rel.pdf

給与・人事・勤怠・就業管理:

人事給与システムでは「法改正」と「ジョブ型」に伴う変化への対応が今後のカギ
https://www.norkresearch.co.jp/pdf/2022itapp_hrw_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):

グループウェアは「グローバルなクラウド+独自の差別化要素」が新たな標準形
https://www.norkresearch.co.jp/pdf/2022itapp_gw_rel.pdf

ワークフロー:

今後のワークフローに求められるノンカスタマイズの業務フロー対応力
https://www.norkresearch.co.jp/pdf/2022itapp_wf_rel.pdf

CRM:

今後のCRMに求められるのは「PaaS+Web会議サービスとの差別化」
https://www.norkresearch.co.jp/pdf/2022itapp_crm_rel.pdf

BI:

BIは初級ユーザと中～上級ユーザで訴求すべき機能が変わる
https://www.norkresearch.co.jp/pdf/2022itapp_bi_rel.pdf

文書管理・オンラインストレージサービス:

文書管理・クラウドストレージはオンプレ/クラウドの競合から連携の段階へ
https://www.norkresearch.co.jp/pdf/2022itapp_dm_rel.pdf

業務アプリケーション導入/更新の全体的な方針:

中堅・中小企業は何を基準に業務アプリケーションを選定するか?
https://www.norkresearch.co.jp/pdf/2022itapp_P0_rel.pdf

次頁へ続く

ご好評いただいているその他の調査レポート（2/2）（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

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