エンドポイント、サーバ/ネットワーク、アプリケーションの3分野における守りのIT対策(セキュリティ、運用管理、バックアップ)の訴求ポイントと合計32社に渡るベンダの導入意向を分析し、今後取るべき施策を提言

2020年版 中堅・中小企業のセキュリティ・運用管理・バックアップに関する今後のニーズとベンダ別導入意向レポート案内

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/地域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

本レポートでは以下のような属性に合致する1300件(有効件数)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(1社1レコード)

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

A2.職責区分:　以下のいずれかの職責を持つ社員
- 情報システムの導入や運用/管理の作業を担当している
- 情報システムに関する製品/サービスの選定または決裁の権限を有している

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 / 流通業 / 建設業 / 卸売業 / 小売業 / IT関連サービス業 / 一般サービス業 / その他

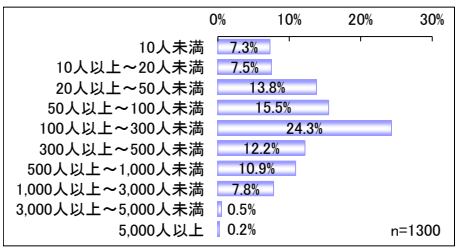
A5.地域区分:　北海道地方 / 東北地方 / 関東地方 / 北陸地方 / 中部地方 / 近畿地方 / 中国地方 / 四国地方 / 九州・沖縄地方

調査実施時期: 2020年7月～8月

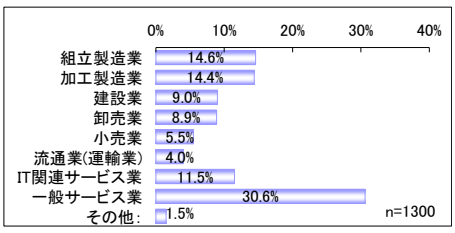
上記に加えて、**「A6.IT管理/運用の人員規模」**(IT管理/運用を担う人材は専任/兼任のいずれか？人数は1名/2～5名/6～9名/10名以上のどれに当てはまるか？)および**「A7.ビジネス拠点の状況」**(オフィス、営業所、工場などの数は1ヶ所/2～5ヶ所/6ヶ所以上のいずれか？ITインフラ管理は個別/統一管理のどちらか？)といった属性についても尋ねており、A1～A7を軸として以降に述べる全ての設問を集計したデータが含まれる。

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。

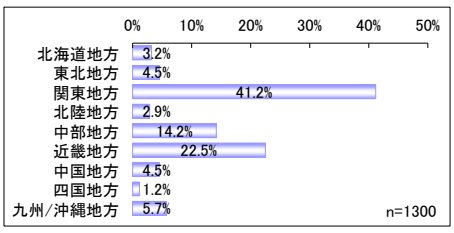
従業員数分布



業種分布



所在地分布



本調査レポートの位置付けと基本構成

本調査レポートは2020年7～8月に実施された年商500億円未満の中堅・中小企業を対象とする守りのIT対策（セキュリティ、運用管理、バックアップ）に関する今後のニーズと守りのITに関連するベンダ別の導入意向に関する調査結果をまとめたものである。

近年、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」は
・クラウドの普及によるシステム形態の多様化
・スマートフォン/タブレットなどの新たな端末
・標的型攻撃に代表される新たな脅威
などによって、対象範囲が大きく広がりつつある。さらに2020年には新型コロナウイルスの影響により、在宅勤務における守りのIT対策も大きな課題となってきた。こうした状況を踏まえて、本調査レポートでは以下の3つの観点から守りのIT対策に関する集計/分析を行い、ベンダや販社/SIerに向けた提言を述べている。

A.守りのIT対策に関する今後の方針/ニーズ
（エンドポイント、サーバ/ネットワーク、アプリケーション利用）

B.守りのIT対策に関するベンダ別導入意向
（セキュリティパッケージ主体、運用管理パッケージ主体、バックアップパッケージ主体、大手のITベンダ/SIer、その他の計32社に渡るベンダが対象）

C.守りのITに対して拠出可能な年額合計費用
（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製品/サービスを利用する際に許容できる年額の合計費用）

以下に本調査レポートの章構成および各章で主な分析対象となる設問番号を記載する。（設問構成については次頁以降で詳述） 2～4章が上記におけるA、5章がB、6章がCに対応している。

第1章.本調査レポートの背景と構成
調査レポートの概要を記載している。

第2章.エンドポイントに関する守りのIT対策の方針/ニーズ
設問R1が主な集計/分析対象となる。

第3章.サーバ/ネットワークに関する守りのIT対策の方針/ニーズ
設問R2が主な集計/分析対象となる。

第4章.アプリケーション利用に関する守りのIT対策の方針/ニーズ
設問R3が主な集計/分析対象となる。

第5章.ベンダ別に見た時の守りのIT対策に関する導入意向
設問R4が主な集計/分析対象となる。

第6章.守りのITに対して許容できる年額の合計費用
設問R5が主な集計/分析対象となる。

次頁へ続く

設問項目(1/5)

本調査レポートの設問項目は大きく分けて、以下の3つのグループから構成されている。

1. 守りのIT対策に関する今後の方針/ニーズ(設問R1、R2、R3)
2. 守りのIT対策に関するベンダ別導入意向(設問R4-1～R4-33)
3. 守りのITに対して拠出可能な年額合計費用(設問R5)

以下では、上記のグループ毎に設問項目の詳細を記載する。

[1.守りのIT対策に関する今後の方針/ニーズ(設問R1、R2、R3)]

R1.エンドポイントに関する守りのIT対策の方針/ニーズ(複数回答可)

設問R1ではエンドポイントの守りのIT対策の方針/ニーズについて尋ねている。「エンドポイント」とはPCやスマートデバイス(スマートフォン/タブレット)といったユーザが利用する端末機器および機器上で稼動するOS/ファームウェアを指す。

エンドポイントに関する守りのIT対策には以下のようなものがある。

PC/スマートデバイスのセキュリティ対策:
　　不正なプログラムやアクセス手法を用いたPC/スマートデバイスへの攻撃を防ぐ
PC/スマートデバイスのバックアップ対策:
　　PC/スマートデバイスのプログラム、データ、設定情報などを複製して保管する
PC/スマートデバイスの資産管理:
　　PC/スマートデバイスへのプログラム導入状況を把握し、起動や使用を制御する
PC/スマートデバイスの操作管理:
　　PC/スマートデバイス上の操作(印刷やUSBメモリの使用など)を監視/制御する

上記を踏まえて、設問R1では以下の選択肢を提示している。選択肢は2つのグループに分かれており、「方針に関する項目」はエンドポイントに関する守りのIT対策に取り組む際の考え方や重視する事項に当てはまる選択肢、「ニーズに関する項目」は有償でも利用したいと考える製品/サービス内容として当てはまる選択肢を列挙している。

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

<<**ニーズに関する項目**>>
- 社内のPCを個人宅でも問題なく利用できる仕組み
- 在宅勤務をする従業員のPCを管理できる仕組み
- 社外で使用するPC内にデータを残さない仕組み
- リモートで顧客と安全/円滑に対話できる仕組み
- Windows10の更新プログラムを制御する仕組み
- スマートデバイスとPCを統合管理できる仕組み
- PCの操作内容や着席状態を把握できる仕組み
- トラブル発生後の対策を自動化する仕組み
- 不正アクセス発生後の被害拡大を防ぐ対策
- 顔や指紋などの生体認証技術への対応
- 改正個人情報保護法やGDPRへの対応
- 災害時に業務を継続するための仕組み
- 従業員を狙った標的型攻撃への対策

次頁へ続く

設問項目(2/5)

R2.サーバ/ネットワークに関する守りのIT対策の方針/ニーズ(複数回答可)

設問R2では業務システムが稼動するサーバ機器、様々なIT機器を接続するネットワーク機器、およびそれらの機器のOSやファームウェアにおける守りのIT対策について尋ねている。

サーバ/ネットワークに関する守りのIT対策には以下のようなものがある。

サーバのセキュリティ対策:
　　不正なプログラムやアクセス手法を用いたサーバへの攻撃を防ぐ
サーバのバックアップ対策:
　　サーバのプログラム、データ、設定情報などを複製して保管する
サーバの稼動監視:
　　サーバ機器やOSが正常に稼働し、障害/遅延がないかを監視する
ネットワークのセキュリティ対策:
　　不正なPCのLANへの接続やスイッチ/ルータへの攻撃などを防ぐ
ネットワークの稼動監視:
　　スイッチ/ルータが正常に稼働し、障害/遅延がないかを監視する
外部からの侵入の検知/防止:
　　外部と繋がるネットワーク機器を標的とした侵入/攻撃の防御

上記を踏まえて、設問R2では以下の選択肢を提示している。選択肢は2つのグループに分かれており、「方針に関する項目」はサーバおよびネットワークに関する守りのIT対策に取り組む際の考え方や重視する事項に該当する選択肢、「ニーズに関する項目」は有償でも利用したいと考える製品/サービス内容として当てはまる選択肢を列挙している。

<<**方針に関する項目**>>
・製品/サービスを特定のベンダに集約していく
・複数ベンダの製品/サービスを適宜使い分ける
・新型コロナ感染症対策に伴い刷新/更新する
・サーバOSの入れ替えに伴い刷新/更新する
・ISDNサービス終了に備えて刷新/更新する
・働き方改革への対応に伴い刷新/更新する
・親会社や取引会社からの要請で刷新/更新する
・BCP(事業継続計画)の策定に伴い刷新/更新する
・社内サーバを減らしてクラウドサービスへ移行する

<<**ニーズに関する項目**>>
・個人宅と社内を安全/手軽に接続できる仕組み
・社内のサーバを個人宅から管理できる仕組み
・社内とクラウドの双方を統合管理する仕組み
・大手キャリアが提供する5G回線網の活用
・特定業者が提供するローカル5Gの活用
・ IoT活用に伴うネットワーク環境の整備
・システムの脆弱性を診断するサービス
・不正アクセスの防護壁となるサービス
・製造装置など非IT機器のデータ保護
・複数のID/アカウントを統合管理する仕組み
・トラブル発生後の対策を自動化する仕組み
・不正アクセス発生後の被害拡大を防ぐ対策
・改正個人情報保護法やGDPRへの対応
・災害時に業務を継続するための仕組み

次頁へ続く

設問項目(3/5)

R3.アプリケーション利用に関する守りのIT対策の方針/ニーズ(複数回答可)

企業では業務システム、Webサイト、メールなど多種様々なアプリケーションを利用しており、それらを保護/保全する必要がある。また、アプリケーションを利用する従業員に対する啓蒙や教育も重要となる。設問R3ではこうしたアプリケーションを利用する際に必要となる守りのIT対策について尋ねている。

アプリケーション利用に関する守りのIT対策には以下のようなものがある。

業務システムソフトウェアの稼動監視:
　　業務システムソフトウェアに障害/遅延がないかを監視する
業務システムソフトウェアの構成管理:
　　業務システムソフトウェアの設定情報や変更履歴を管理する
スパムメール/不正メールの排除:
　　スパムメールや不正メールを検知し、社内への配布を防止する
メール誤送信/漏えいの防止:
　　メールの宛先や内容をチェックし、誤送信や情報漏えいを防ぐ
Webサイトやeコマースサイトの保護:
　　社外に公開しているサイトに対する不正侵入や攻撃を防ぐ
不正Webサイトへのアクセス防止:
　　URLフィルタリングなどで従業員のWeb閲覧を管理/制御する
従業員に対する標的型攻撃対策:
　　知人を装ったメールなどによる個人を標的とした攻撃の防御
従業員向けのヘルプデスク:
　　従業員からのIT関連の質問に対応できる窓口の設置/運営

上記を踏まえて、設問R3では以下の選択肢を提示している。選択肢は2つのグループに分かれており、「方針に関する項目」はアプリケーション利用に関連する守りのIT対策に取り組む際の考え方や重視する事項に該当する選択肢、「ニーズに関する項目」は有償でも利用したいと考える製品/サービス内容として当てはまる選択肢を列挙している。

<<**方針に関する項目**>>
- 製品/サービスを特定のベンダに集約していく
- 複数ベンダの製品/サービスを適宜使い分ける
- 新型コロナ感染症対策に伴い刷新/更新する
- Windows 10への移行に伴い刷新/更新する
- サーバOSの入れ替えに伴い刷新/更新する
- 働き方改革への取り組みに伴い刷新/更新する
- 親会社や取引会社からの要請で刷新/更新する
- BCP(事業継続計画)の策定に伴い刷新/更新する
- 社内サーバが不要なクラウドサービスへ移行する
- 在宅勤務に適したアプリケーションへ移行する

<<**ニーズに関する項目**>>
- アプリケーションをブラウザで利用可能にする仕組み
- 利用可能なアプリケーションを制限/管理する仕組み
- 操作画面をスマートデバイス向けに変換する仕組み
- 様々なクラウドサービスの安全性を評価するサービス
- セキュリティ全般に関する従業員向け教育サービス
- プライバシーマークなどの公的な認定の取得支援
- データをクラウド上にバックアップする仕組み
- データを社内にバックアップする仕組み
- トラブル発生後の対策を自動化する仕組み
- 不正アクセス発生後の被害拡大を防ぐ対策
- 改正個人情報保護法やGDPRへの対応
- 災害時に業務を継続するための仕組み

次頁へ続く

設問項目(4/5)

[2. 守りのIT対策に関するベンダ別導入意向(設問R4-1～R4-33)]

セキュリティ、運用管理、バックアップといった守りのIT対策を担うソフトウェア製品/サービスを開発/販売するベンダも多数存在する。設問R4-1～R4-33ではこうしたベンダを列挙し、以下の選択肢を設けて各ベンダの導入意向を尋ねている。

導入済み＆継続:
　該当するベンダの製品/サービスを既に導入しており、今後も利用を継続する
導入済み＆変更:
　該当するベンダの製品/サービスを既に導入しているが、今後は他社に変更する予定である
導入予定:
　現時点では導入していないが、該当するベンダの製品/サービスを導入する予定である
予定なし:
　現時点では導入しておらず、今後も該当するベンダの製品/サービスを導入する予定はない
認知なし:
　該当するベンダを知らない

導入意向を尋ねる対象となるベンダは以下の通りである。上記の選択肢によって各ベンダ(計32社+その他)の導入意向を尋ねた結果がR4-1～R4-33の設問に対応している。「」内は各ベンダにおける代表的な製品/サービス名称である。
(必ずしも最新の製品/サービスではなく、中堅・中小企業が該当するベンダを最も確実に想起できるものを記載している)

<<セキュリティパッケージ主体>>

R4-1. トレンドマイクロ(「ウイルスバスター」など)
R4-2. シマンテック(「Symantec Endpoint Protection」など)
R4-3. マカフィー(「McAfee Endpoint Protection」など)
R4-4. キヤノンITソリューションズ(「GUARDIANWALL」「ESET」など)
R4-5. カスペルスキー(「カスペルスキー」など)
R4-6. ソースネクスト(「ZEROシリーズ」など)
R4-7. エフ・セキュア(「F-Secure」など)
R4-8. FFRI(「FFRI yarai」など)

<<運用管理パッケージ主体>>

R4-9. Sky(「SKYSEA Client View」など)
R4-10. クオリティソフト(「QND」など)
R4-11. エムオーテックス(「LanScope」など)
R4-12. Ivanti(LANDESK)(「Ivanti(LANDESK)」など)
R4-13. ハンモック(「AssetView」など)

<<バックアップパッケージ主体>>

R4-14. ベリタステクノロジーズ(「Backup Exec」など)
R4-15. Arcserve(「Arcserve」など)
R4-16. クエストソフトウェア(「NetVault」など)
R4-17. ストレージクラフト(「ShadowProtect」など)
R4-18. ネットジャパン(「ActiveImage Protector」など)
R4-19. アクロニス(「Acronis」など)

<<その他のパッケージ主体>>

R4-20. アルプスシステムインテグレーション(「InterSafe」など)
R4-21. デジタルアーツ(「i-FILTER」など)
E4-22. ソリトンシステムズ(「InfoTrace」など)

<<大手のITベンダ/SIer>>

R4-23. 日立製作所(「JP1」など)
R4-24. 富士通(「Systemwalker」など)
R4-25. NEC(「WebSAM」など)
R4-26. 日本ヒューレット・パッカード(HPE)(「Ice Wall」など)
R4-27. デル/EMCジャパン(「RSA SecureID」など)
R4-28. シスコシステムズ(「CiscoWorks」など)
R4-29. 日本マイクロソフト(「Microsoft System Center」など)
R4-30. 日本IBM(「Tivoli」など)
R4-31. NTTデータ(「Hinemos」など)
R4-32. 野村総合研究所(「Senju」など)

<<その他>>

R4-33.その他

次頁へ続く

設問項目（5/5）

[3. 守りのITに対して拠出可能な年額合計費用（設問R5）]

設問R5では守りのITに対して拠出可能な年額合計費用（万円）を数値記入形式で尋ねている。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ソフトウェアの製品/サービスを利用する上で許容できる年額の合計費用を記入する形式となっている。集計データでは回答結果の平均値を算出している。

レポート試読版1（「分析サマリ」その1）

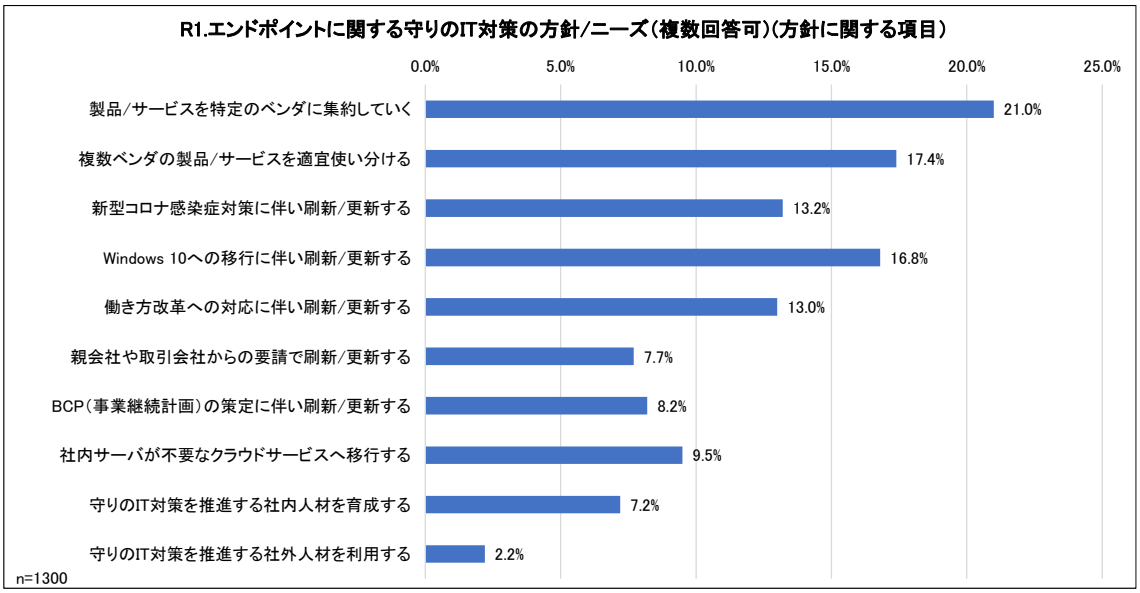
本調査レポートには50ページ超に渡って、中堅・中小企業におけるセキュリティ、運用管理、バックアップといった守りのIT対策の実態とベンダ導入意向に関する重要ポイントとベンダや販社/SIerに向けた提言を述べた「分析サマリ」が含まれる。以下のレポート試読版では「第2章.エンドポイントに関する守りのIT対策の方針/ニーズ」に関する分析サマリの一部を紹介している。（第3章でサーバ/ネットワーク、第4章でアプリケーション利用に関する同様の分析を行っている）

2. エンドポイントに関する守りの IT 対策の方針/ニーズ

本章ではエンドポイントの守りの IT 対策の方針/ニーズについて尋ねている。「エンドポイント」とは PC やスマートデバイス（スマートフォン/タブレット）といったユーザが利用する端末機器および機器上で稼動する OS/ファームウェアを指す。エンドポイントに関する守りの IT 対策には以下のようなものがある。

**********中略**********

以下のグラフは設問 R1 の「方針に関する項目」を中堅・中小企業全体で集計したものだ。（集計データ￥単純集計データ￥【R 系列】単純集計.xlsx）



**********中略**********

したがって、中長期的な方針という観点ではコロナ禍や法改正の影響よりも、ベンダの集約/使い分けや Widows 10 で新たに導入された WaaS（Windows as a Service）への対応を重視する中堅・中小企業が多いと考えられる。ベンダの集約と使い分けについてはどちらか一方の回答割合が突出して高い状況ではないため、IT 企業側としてはユーザ企業の実態や意向を踏まえた提案を行う必要がある。（年商別に見た場合の傾向差については後述する） WaaS については年 2 回の機能更新プログラムを利点よりも負担を捉えるユーザ企業が多くなると予想されるため、IT 企業側はユーザ企業の負担を最小限に抑える WaaS 対応策を検討する必要があると考えられる。

**********中略**********

一方で、エンドポイントの守りの IT 対策においてどのような製品/サービスを導入しようとしているか？の「ニーズ」を尋ねた結果は「方針」とは異なる傾向を示す。

以下のグラフは設問 R1 の「ニーズに関する項目」を中堅・中小企業全体で集計したものだ。（集計データ￥単純集計データ￥【R 系列】単純集計.xlsx）

レポート試読版2(「分析サマリ」その2)

さらに分析サマリの第6章ではエンドポイント、サーバ/ネットワーク、アプリケーション利用に関する守りのIT対策の方針/ニーズと守りのITに対して許容できる年額の合計費用との関連についても分析している。単なるクロス集計だけではなく、ベイジアンネットワークを用いて、守りのIT対策の支出額を増やすために有効な方針/ニーズの訴求ポイントは何か？についても分析を行っている。以下のレポート試読版では第6章の一部を抜粋して掲載している。

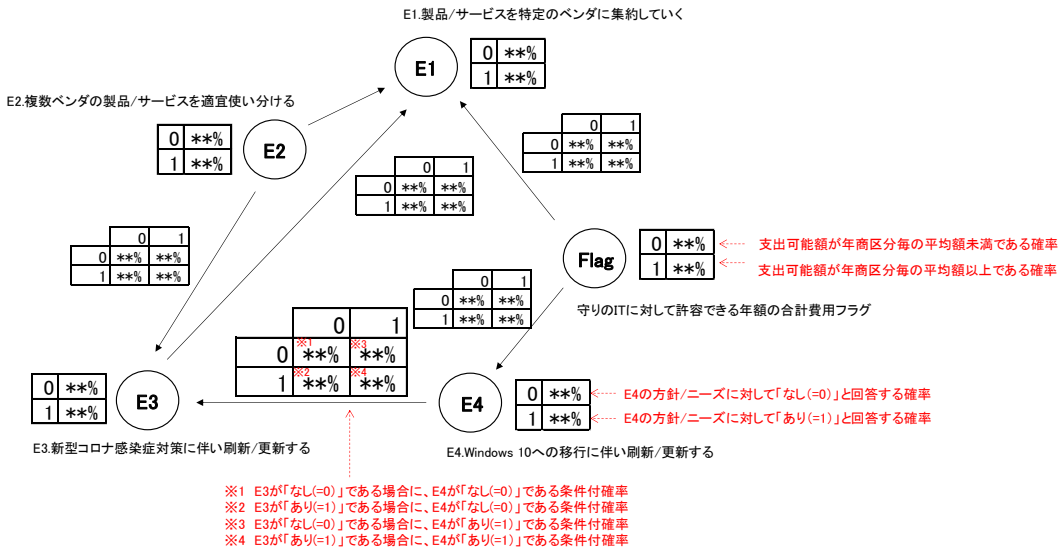
6.守りの IT に対して許容できる年額の合計費用

ベンダや販社/SIer が守りの IT 対策を訴求する際にはユーザ企業が想定する費用感を把握しておくことも大切だ。そこで、本調査レポートでは守りの IT に対して拠出可能な年額合計費用(万円)を数値記入形式で尋ねている。**********中略**********

守りの IT に対して許容できる年額の合計費用と多岐に渡る方針/ニーズ項目の関連性を明らかにしようとする場合、2 つの項目間の相関を測ることは現実的ではない。エンドポイント、サーバ/ネットワーク、アプリケーション利用における方針/ニーズの項目数はそれぞれ 20 超に渡るため、2 つの項目間の組み合わせは膨大な数となる。したがって、20 超の項目数の関連をまとめて俯瞰できる何らかの方法が必要となる。それを実現する手法がベイジアンネットワーク分析である。

**********中略**********

例えば、以下の図はエンドポイントに関する守りの IT 対策における方針/ニーズ項目と「フラグ」に対してベイジアンネットワーク分析を適用した結果を略図として示したものだ。「フラグ」に対応する「Flag」ノードには支出可能額が平均以上か？平均未満か？に応じた確率値が割り当てられる。また、ノード間に割り当てられた条件付確率の説明として、E3 と D4 の場合が例示されている。



**********中略**********

他のノードへと伝播していき、各ノードの確率値が変化していく。これによって、「もし、支出可能額が平均未満であった場合と比較して、平均以上であった場合に回答割合が高い方針/ニーズは何か？」を計算すれば、逆に「守りの IT 対策の支出額を増やすためにはどのような方針/ニーズを訴求すれば良いか？」を知ることができる。このようにベイジアンネットワークにエビデンスを設定することによって、今後取り組むべき施策を探索するのが「確率推論」である。

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「R系列」(本調査レポートの全設問)を集計した結果の一部である。

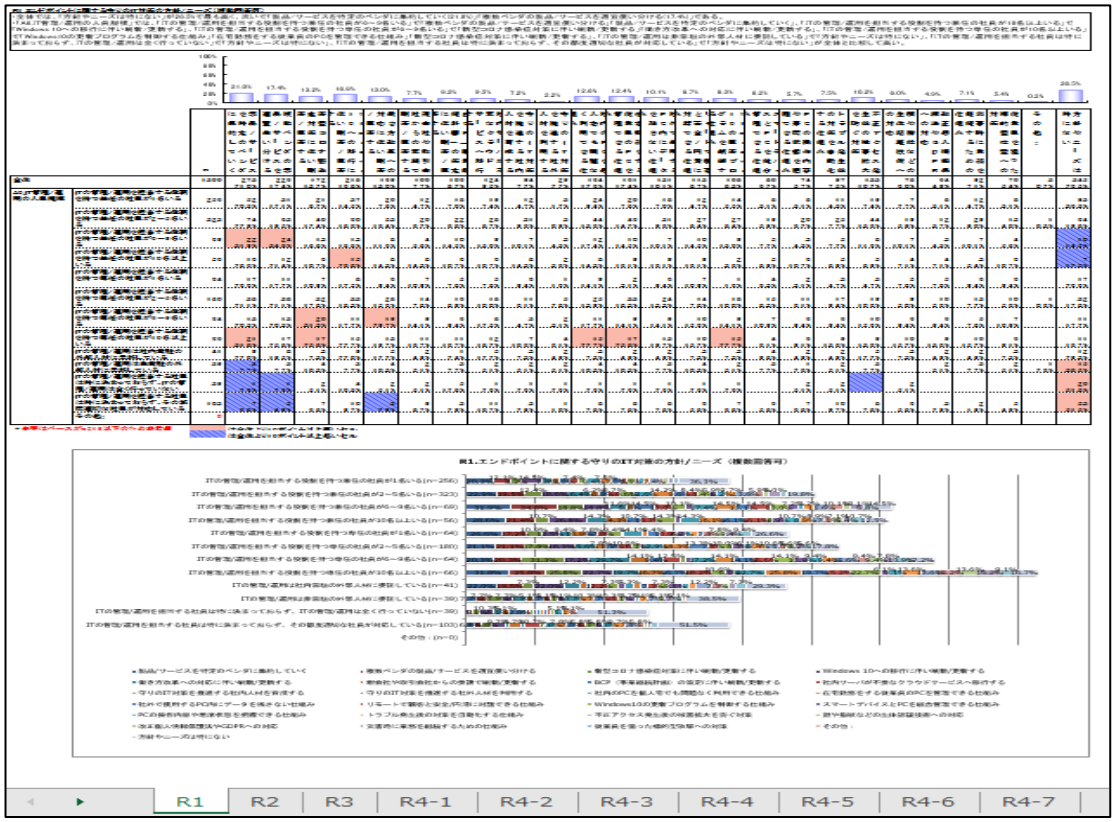
以下のMicrosoft Excelファイル名は『【R系列】(【A6】表側).xlsx』となっている。【R系列】とは、本調査レポートのR1系列～R5系列を含む全設問を指している。また、【A6】とはIT管理/運用の人員体制を示す企業属性であり、以下に列挙された選択肢から構成されている。

・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』の結果を見ることによって、IT管理/運用を担う人材が1名のみの場合(ひとり情シス)と2～5名、6～9名、10名以上のそれぞれの場合で、「守りのIT」への取り組み状況にどのような違いがあるか？を確認することができる。同じように、年商別の傾向については『【R系列】(【A1】表側).xlsx』(A1が年商区分を表す)、業種別の傾向については『【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、ファイル名を見ることで「どの設問を対象として何を軸として集計したものか？」がわかるようになっている。

本調査レポートの設問数はR1系列(1設問)、R2系列(1設問)、R3系列(1設問)、R4系列(33設問)、R5系列(1設問)の計37設問となっており、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項目存在する。そのため本調査レポートにおける「主要分析軸データ」の合計シート数は37設問×7属性＝259シートに達する。(ただし「年商30億円以上～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)

個々のシートは画面上部に軸を設定しない状態の縦帯グラフ、画面中央には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う書式になっている。



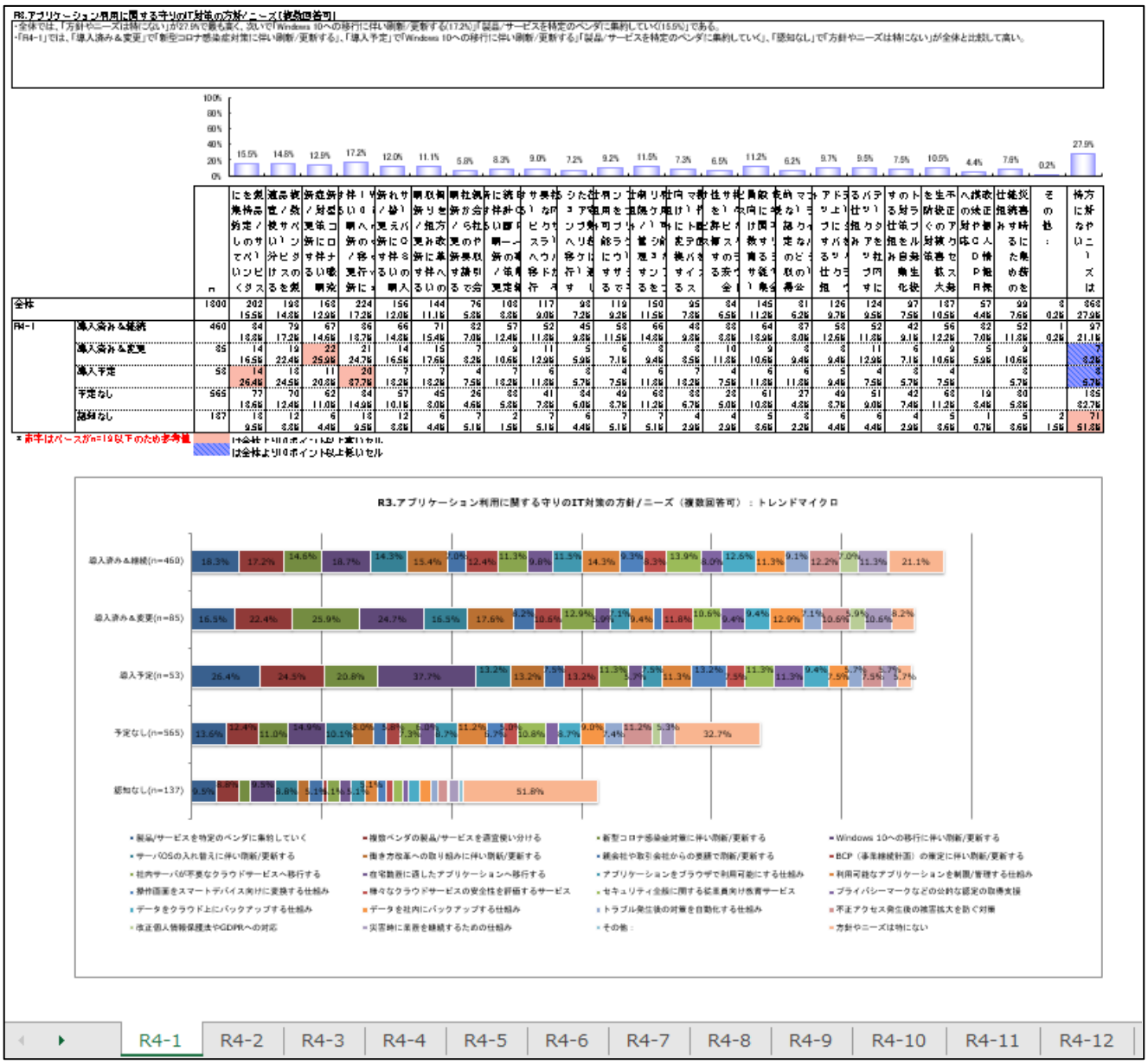
レポート試読版4(「質問間クロス集計データ」)

「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「R3.アプリケーション利用に関する守りのIT対策の方針/ニーズ」の結果をR4系列の各設問を軸として集計した結果である。R4系列は本ドキュメントの6ページに記載されているように計32社に渡るベンダの導入意向を尋ねた設問となっている。したがって以下の質問間クロス集計データを見ることによって、「あるベンダA社を導入する予定のユーザ企業がアプリケーション利用の守りのIT対策ではどのような方針を採ろうとしているか？」などを知ることができる。

以下のMicrosoft Excelファイル名は『【R3】(【R4系列】表側).xlsx』となっている。「【R4系列】表側」の部分は設問「R4-1」～「R4-32」のR4系列設問が集計軸(表側)となっていることを示しており、「【R3】」の部分は設問「R3.アプリケーション利用に関する守りのIT対策の方針/ニーズ」が集計の対象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？」がわかるようになっている。

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、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書式になっている。



本レポートの価格とご購入のご案内

『2020年版 中堅・中小企業のセキュリティ・運用管理・バックアップに関する今後のニーズとベンダ別導入意向レポート』

【価格】180,000円(税別)　【発刊日】2021年3月22日
【媒体】CD-ROM (分析サマリ: PDF形式、集計データ: Microsoft Excel形式)
【サンプル/ダイジェスト】 以下より、本レポートのサンプル/ダイジェストをご覧いただけます。

2020年 コロナ禍が中堅・中小企業のセキュリティ/運用管理/バックアップ対策に与える影響
https://www.norkresearch.co.jp/pdf/2020Sec_usr_rel1.pdf

2020年 中堅・中小企業におけるセキュリティ/運用管理/バックアップのニーズ状況とベンダ動向
https://www.norkresearch.co.jp/pdf/2020Sec_usr_rel2.pdf

【お申込み方法】 弊社ホームページからの申し込みまたはinform@norkresearch.co.jp宛にご連絡ください

その他のレポート最新刊のご案内(各180,000円税別)

2020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/ 生産/ 販売/ 人給/ ワークフロー/ コラボレーション/ CRM/ BIなど10分野の導入済み＆新規予定のシェアとユーザによる評価を網羅

【リリース(ダイジェスト)】

シェア順位も変動、ERPの課題/ニーズに起きている変化
https://www.norkresearch.co.jp/pdf/2020itapp_erp_rel.pdf

IoTなどを見据えた新たな中堅・中小向け生産管理システムへの道筋
https://www.norkresearch.co.jp/pdf/2020itapp_ppc_rel.pdf

CRMが担うべきオンライン/リモートの商談を伴った顧客管理
https://www.norkresearch.co.jp/pdf/2020itapp_crm_rel.pdf

中堅・中小企業におけるBI活用の裾野を広げるために必要な施策
https://www.norkresearch.co.jp/pdf/2020itapp_bi_rel.pdf

【レポート案内(サンプル属性、設問項目、試読版など)】 https://www.norkresearch.co.jp/pdf/2020itapp_rep.pdf

2020年版 中堅・中小企業におけるRPAおよびノーコード/ローコード開発ツールの活用実態レポート

RPA市場の最新動向をノーコード/ローコード開発ツールの視点も交えて俯瞰する

【リリース(ダイジェスト)】

ノーコード/ローコード開発ツールの導入率と課題
https://www.norkresearch.co.jp/pdf/2020RPA_user_rel1.pdf

RPA活用の普及に向けて注力すべき用途と課題
https://www.norkresearch.co.jp/pdf/2020RPA_user_rel2.pdf

RPA市場のシェア動向およびERPなどの既存業務システムとの関連
https://www.norkresearch.co.jp/pdf/2020RPA_user_rel3.pdf

【レポート案内(サンプル属性、設問項目、試読版など)】 https://www.norkresearch.co.jp/pdf/2020RPA_user_rep.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