PRESS RELEASE（報道関係者各位）

2025年10月27日

2025年 中堅・中小企業におけるセキュリティ対策の経年変化と今後の展望

調査設計/分析/執筆：岩上由高
ノークリサーチ（本社〒160-0022東京都新宿区新宿2-13-10武蔵野ビル5階23号室　代表：伊嶋謙二 TEL：03-5361-7880
URL：www.norkresearch.co.jp）は中堅・中小企業におけるセキュリティ対策の経年変化と今後の展望に関する調査結果を発表した。本リリースは「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」のサンプル/ダイジェストである。

＜新政権の方針を受けて、中堅・中小企業におけるセキュリティ対策が再び注目を集める＞
■経済安全保障の取り組みに伴い、中堅・中小企業のセキュリティ対策強化の機運も高まる
■VPN/ZTNAのニーズは中堅企業ではピークを過ぎたが、中小企業や小規模企業では健在
■セキュリティ上位4社、およびNGAVで注目が高まる3社のシェア増減は年商によって異なる

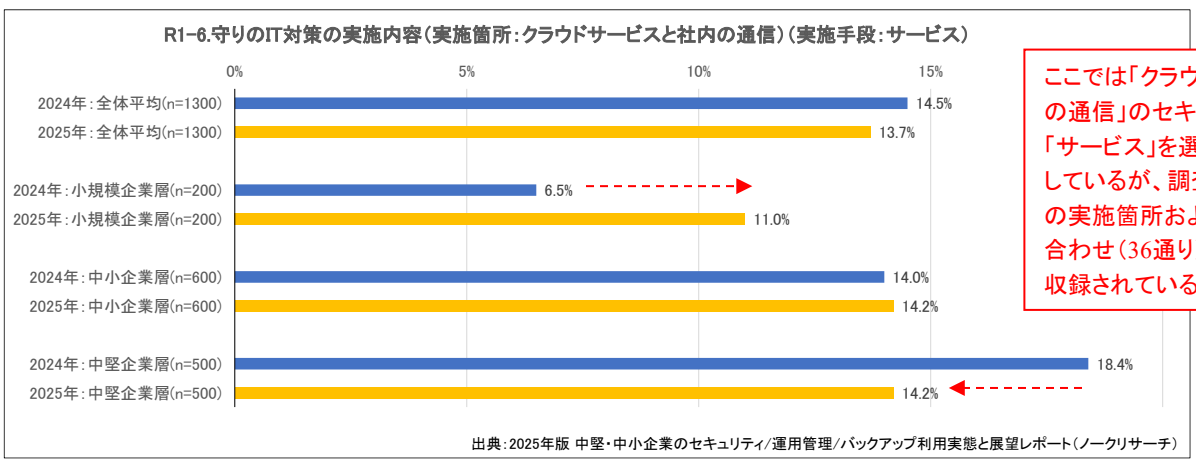
調査時期：　2025年7月～8月
対象企業：　日本全国、全業種の年商500億円未満の中堅・中小企業1300社（有効回答件数、1社1レコード）
対象職責：　情報システムの導入や運用/管理または製品/サービスの選定/決裁の権限を有する職責
詳細については右記の調査レポート案内を参照：　https://www.norkresearch.co.jp/pdf/2025Sec_user_rep.pdf

経済安全保障の取り組みに伴い、中堅・中小企業のセキュリティ対策強化の機運も高まる

近年ではランサムウェアによるサイバー攻撃が日本各地で発生しており、産業/医療/教育などに大きな被害を与えている。こうした状況を受けて、政府も2025年7月に従来のNISC（内閣サイバーセキュリティセンター、National center of Incident readiness and Strategy for Cybersecurity）をNCO（国家サイバー統括室、National Cybersecurity Office）へと組織改定し、指揮命令系統や体制を強化した。さらに、2025年10月に発足した高市政権では経済安全保障を重視しており、今後は企業におけるサプライチェーンの多元化/強靭化に向けた取り組みが進むと予想される。その過程では日本における産業の裾野を支える中堅・中小企業のセキュリティ基盤強化が不可欠だ。

こうした背景を受けて、「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」では中堅・中小企業におけるセキュリティ対策の実施状況が2024～2025年にどう変化したか？に着目し、そうした経年変化を踏まえてベンダや販社/SIerがどのようなセキュリティ製品/サービスを訴求すべきか？を分析/提言している。

中堅・中小企業においても、セキュリティ対策を実施すべき箇所は「社内で利用する端末」、「社外で利用する端末」、「社内のサーバ/ストレージ」、「社外（クラウド等）のサーバ/ストレージ」などと多岐に渡る。さらに、各々の箇所でパッケージ、サービスアウトソース、アプライアンス、H/Wの付属機能などの様々な手段の中から何が選ばれているのか？ の実態も把握する必要がある。本リリースの元となる調査レポートでは、そうした「実施箇所」と「実施手段」の全ての組み合わせの経年変化を集計/分析している。以下のグラフはその中から、「クラウドサービスと社内の通信」（実施箇所）において「サービス（実施手段）」を選択している割合の経年変化を年商別に集計したものだ。次頁では以下のグラフが何を意味しているか？を述べていく。



ここでは「クラウドサービスと社内の通信」のセキュリティ対策として「サービス」を選んだケースを抜粋しているが、調査レポートには全ての実施箇所および実施手段の組み合わせ（36通り）を集計したデータが収録されている

VPN/ZTNAのニーズは中堅企業ではピークを過ぎたが、中小企業や小規模企業では健在

前頁で述べた「クラウドサービスと社内の通信」（実施箇所）において「サービス」（実施手段）」を選択しているケースとは、社内とIaaS/ホスティングの通信をVPNやZTNAの各種サービスによってセキュアに保つ取り組みを指す。前頁の経年変化グラフを確認すると、全体平均では目立った変化は見られない（微減）。だが、年商別に見た場合は小規模企業層（年商5億円未満）は4ポイント超の増加、中小企業層（年商5～50億円）は横ばい、中堅企業層（年商50～500億円）は4ポイント程度の減少といったように傾向が大きく異なる。つまり、社内とクラウド間の通信をセキュアに保つ取り組みは中堅企業層では既にピークが過ぎているが、中小企業層ではまだ継続しており、小規模企業層ではニーズが増加傾向にあると捉えることができる。本リリースの元となる調査レポートでは、以下の選択肢を列挙して「実施箇所」と「実施手段」の様々な組み合わせ（6×6=36通り）の経変変化を年商別に集計/分析している。（各項目の詳細な説明は右記の調査レポート案内を参照 https://www.norkresearch.co.jp/pdf/2025Sec_user_rep.pdf ）

R1. 守りのIT対策の実施内容

実施している箇所（6通り）

- ・エンドポイント（社内）
- ・エンドポイント（社外）
- ・サーバ/ストレージ（社内）
- ・サーバ/ストレージ（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

実施している手段（※を除いて6通り）

- ・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（※）

上記によって、「社外で利用する端末（PCやスマートデバイス）のセキュリティ対策はパッケージとサービスのどちらが伸びているのか？年商規模による違いはあるか？」などを把握することができる。さらに調査レポートではセキュリティ/運用管理/バックアップの対策においてユーザ企業が抱える課題やニーズについても詳細な集計/分析を行っている。以下には課題を尋ねた選択肢を列挙している。（<<その他>>以外の選択肢のうちで、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）

R4. 守りのIT対策において現状で抱えている課題

<<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

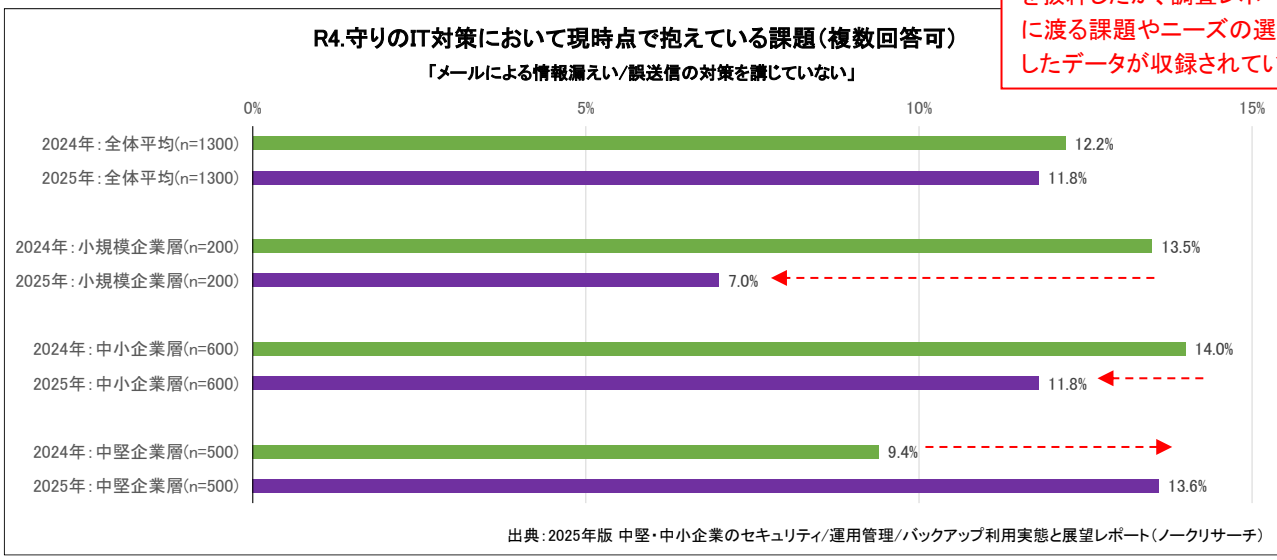
<<その他>>
- ・その他：
- ・課題は全くない（排他）

上記に列挙された課題項目が示すように、ランサムウェアの脅威に対抗するためにはマルウェア対策だけでなく、侵入後の被害拡大を防ぐための適切なアカウント管理やデータの搾取/悪用を防止するバックアップ/リストアといった多角的な視点が必要となる。次頁では、上記に列挙した課題項目に関する集計/分析の一例を紹介している。

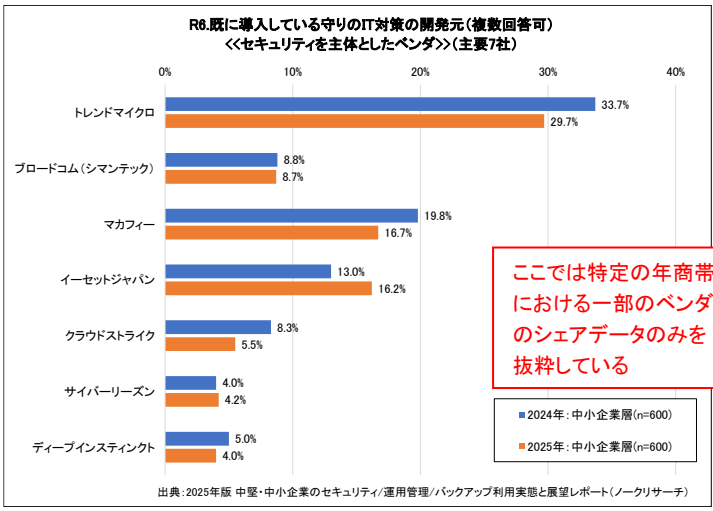
セキュリティ上位4社、およびNGAVで注目が高まる3社のシェア増減は年商によって異なる

以下のグラフは前頁に列挙した課題項目の中から、「メールによる情報漏えい/誤送信の対策を講じていない」の回答割合の経年変化を年商別に集計したものだ。中堅企業層（年商50～500億円）では4ポイント程度増加しており、メール経由でのデータ流出への危機感が高まっている状況が確認できる。

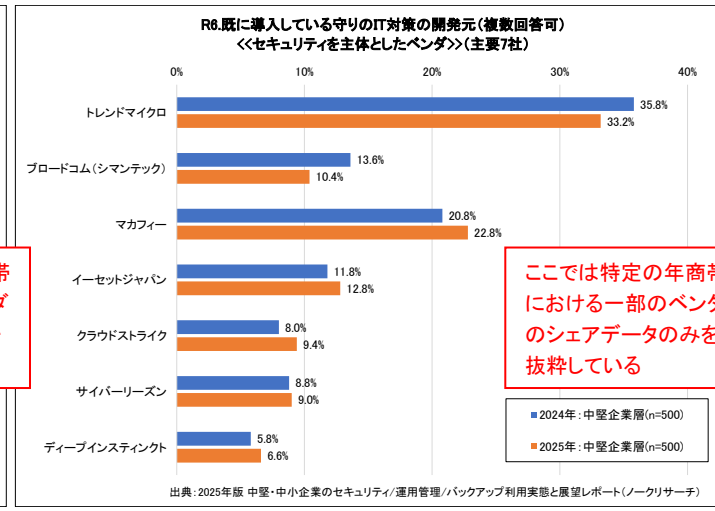
ここでは一部の課題項目の集計結果を抜粋したが、調査レポートには20超に渡る課題やニーズの選択肢を集計したデータが収録されている



一方で、小規模企業層（年商5億円未満）では5ポイント超の大幅な減少、中小企業層（年商5～50億円）では3ポイント程度の減少となっている。この場合、「対策が講じられた結果、課題が解消している」または「ユーザ企業の課題意識が薄れている」のどちらなのか？の判断が重要だ。それにより、IT企業が訴求すべきセキュリティ対策の製品/サービスも大きく変わってくる。調査レポートではそうした観点からの集計/分析を行い、IT企業が採るべき施策を提言している。さらに調査レポートでは次頁に列挙したセキュリティ/運用管理/バックアップの製品/サービスを開発/販売するベンダ（計56社）の導入社数シェアを集計し、経年変化を年商別に分析している。以下のグラフはその中からセキュリティ分野におけるシェア上位ベンダ（トレンドマイクロ、ブロードコム（シマンテック）、マカフィー、イーセットジャパン）とNGAV（次世代アンチウイルス、Next Generation Anti-Virus）という用語と共に近年注目を集めるベンダ（クラウドストライク、サイバーリーズン、ディープインスティンクト）の導入社数シェアを抜粋したものだ。左グラフ（中小企業層）ではマカフィーが減少、イーセットジャパンが増加、NGAV関連3社は横ばいor 微減とである一方で、右側グラフ（中堅企業層）ではマカフィーが増加、イーセットジャパンが微増、NGAV関連3社も横ばいor 微増といったように 年商規模によってシェア増減の傾向が異なっていることがわかる。販社/SIerが複数のセキュリティ製品/サービスを販売する際はこうした実態を踏まえた商材ポートフォリオ（どの年商帯にどの製品/サービスを訴求するか？）が重要となる。



ここでは特定の年商帯における一部のベンダのシェアデータのみを抜粋している



ここでは特定の年商帯における一部のベンダのシェアデータのみを抜粋している

次頁では、調査レポートにおいて導入社数シェアの集計対象となっている計56社のベンダー覧を掲載している。

補記：社数シェア集計/分析の対象となっているベンダー一覧

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）

次頁では、本リリースの元となる調査レポートの詳細（価格、収録内容など）について記載している。

本リリースの元となる調査レポート

『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』

【調査時期】 2025年7月～8月 **【発刊日】**2025年11月7日 **【価格】** 225,000円(税別)

【対象企業属性】(有効回答件数:1300社、1社1レコード)

年商: 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

従業員数: 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～1,000人未満 / 1,000人以上～3,000人未満 / 3,000人以上～5,000人未満 / 5,000人以上

業種: 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:

地域: 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

その他の属性: 「IT管理/運用の人員規模」(12区分)、「ビジネス拠点の状況」(5区分)、「職責」(2区分)

【調査レポートの収録内容】(有効回答件数:1300社、1社1レコード)

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。分析サマリの章構成は以下の通りであり、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)に関する実態を網羅した内容となっている

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。

更に詳細な調査レポート案内(サンプル属性、設問項目一覧、集計データ例、試読版など)**を以下にてご覧いただけます**
調査レポート案内: https://www.norkresearch.co.jp/pdf/2025Sec_user_rep.pdf

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

当調査データに関するお問い合わせ

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

NORK RESEARCH