PRESS RELEASE（報道関係者各位）

2025年11月4日

2025年 中堅・中小企業のランサムウェア対策と守りのITに拠出可能な年額費用

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・中小企業におけるランサムウェア対策の現状および守りのITに拠出可能な年額合計費用に関する調査を行い、その結果を発表した。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。

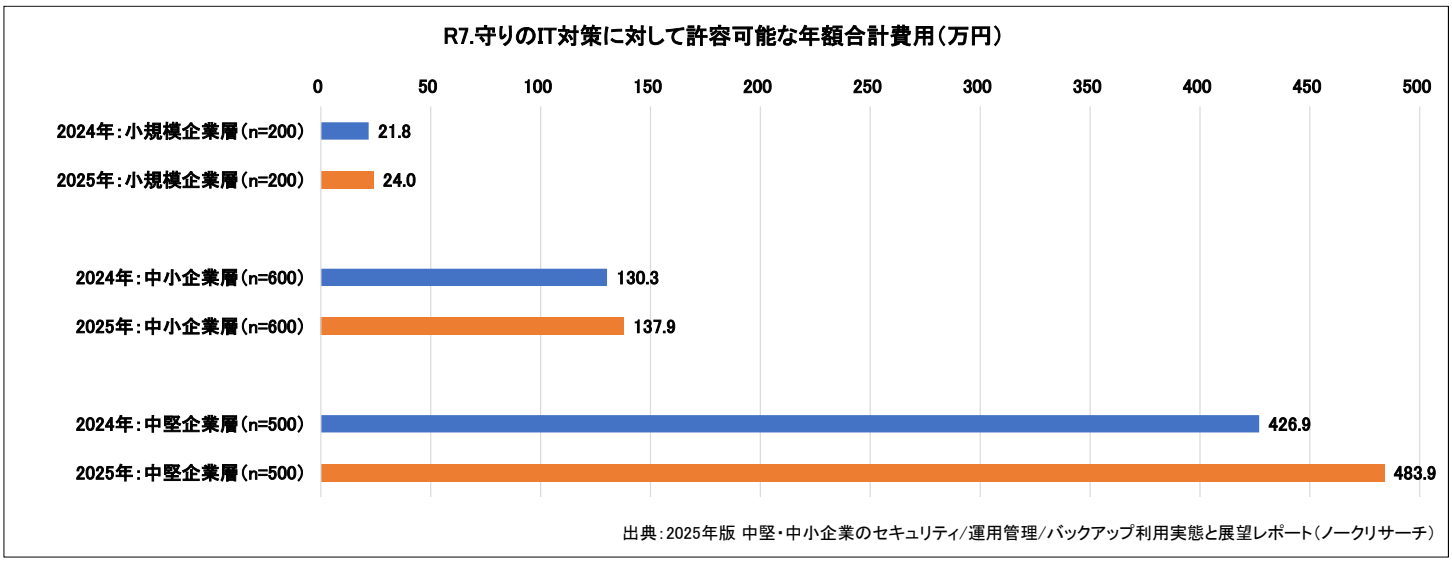
＜ランサムウェア対策を前提とした新たなニーズに応えるための製品/サービス強化が求められる＞
■セキュリティやバックアップに拠出可能な年額合計費用はいずれの年商帯においても増加
■ランサムウェアの被害を受けて「ネットワークから隔離したバックアップ」のニーズが高まる
■中堅企業層に対しては「取引先（大企業）への影響も考慮した対策」を支援することが重要

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

セキュリティやバックアップに拠出可能な年額合計費用はいずれの年商帯においても増加

昨今猛威を振るうランサムウェア攻撃では、大企業のみならずサプライチェーンを構成する中堅・中小企業が標的となるケースも今後増えていく可能性がある。こうした状況を踏まえて、本リリースの元となる「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、有効回答件数1300社のユーザ企業を対象とした調査データを元にIT企業が中堅・中小企業に提示すべきランサムウェア対策は何か？を分析/提言している。

以下のグラフは調査レポートの中から、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対策に対して拠出可能な年額合計費用の経年変化（2024～2025年）を示したものだ。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を指す。



年商規模によって金額に大きな差があるが、いずれの年商帯においても2024～2025年にかけて拠出可能な年額合計費用が増加していることが確認できる。つまり、昨今のランサムウェア被害の報道などを目にして、中堅・中小のユーザ企業も守りのIT対策の強化を図ろうとしている。次頁以降では上記の詳細について補足した上で、ユーザ企業が求めるニーズ項目を元にランサムウェア対策の現状と今後の重要ポイントを分析した結果の一部を調査レポートのダイジェストとして紹介していく。

ランサムウェアの被害を受けて「ネットワークから隔離したバックアップ」のニーズが高まる

前頁の「守りのIT対策に対して拠出可能な年額合計費用」では、年商帯の大分類（小規模企業層、中小企業層、中堅企業層）で集計した結果を掲載した。だが、中小企業層や中堅企業層は年商の幅が広いため、更に詳細な傾向を把握する必要がある。実際に中小企業層と中堅企業層は全体としては年額合計費用が増加しているが、詳細な区分を見ると増加幅が大きい/小さいまたは減少しているといった違いが見られる。調査レポートではそうした傾向差も踏まえた上で、IT企業が特に注力すべき年商区分はどこか？などを提言している。

年商区分の定義

小規模企業層： 年商5億円未満

中小企業層： 年商5～50億円 →
- 年商5～ 10億円
- 年商10～20億円
- 年商20～50億円

中堅企業層： 年商50～500億円 →
- 中堅下位企業層： 年商50 ～100億円
- 中堅中位企業層： 年商100 ～300億円
- 中堅上位企業層： 年商300 ～500億円

さらに、調査レポートでは以下の選択肢を列挙して、ユーザ企業が守りのIT対策を担う製品/サービスに求めるニーズは何か？も集計/分析している。（下線の項目は2025年に新規追加した選択肢、下線のない項目は2024年からの経年変化を分析している選択肢）

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

<<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

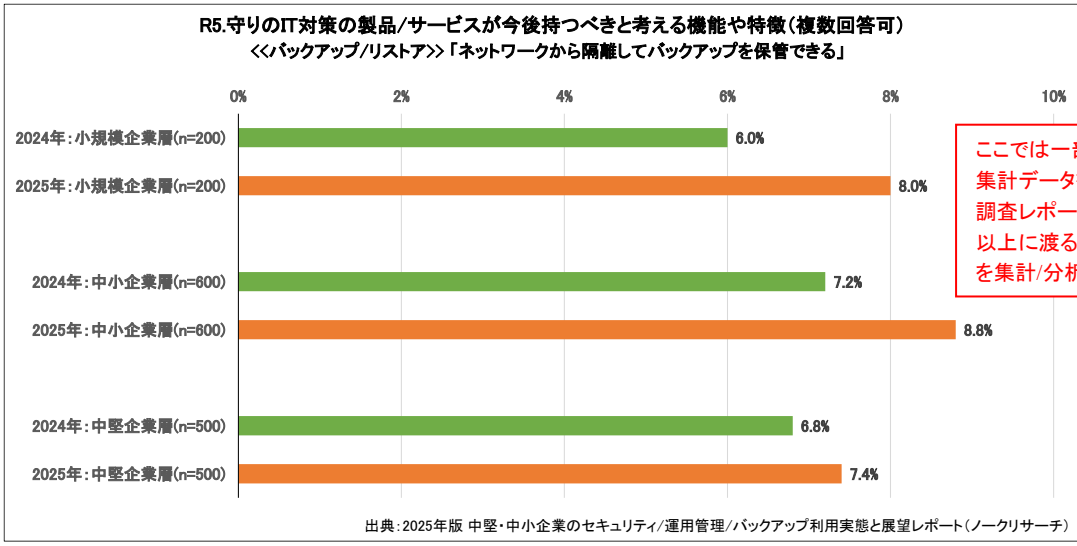
<<その他>>
- その他：
- 欲しいと考える機能や特徴は全くない（排他）

上記に列挙した項目はいずれもランサムウェア攻撃を回避する上で重要な取り組みと言える。調査レポートの中では、上記と対になる課題を尋ねた設問「R4. 守りのIT対策において現状で抱えている課題」との比較なども行いながら、中堅・中小のユーザ企業におけるランサムウェア対策がどこまで進んでおり、どこを改善していくべきなのか？を明らかにしている。

ランサムウェア攻撃において被害が甚大化/長期化しやすい事象の1つが「LANに侵入したマルウェアがバックアップを削除/改変する」というものだ。そうした現状を受けて、上記に赤字で示した「ネットワークから隔離してバックアップを保管できる」というニーズ割合はいずれの年商帯においても増加している。次頁では、その点に関する詳細を述べていく。

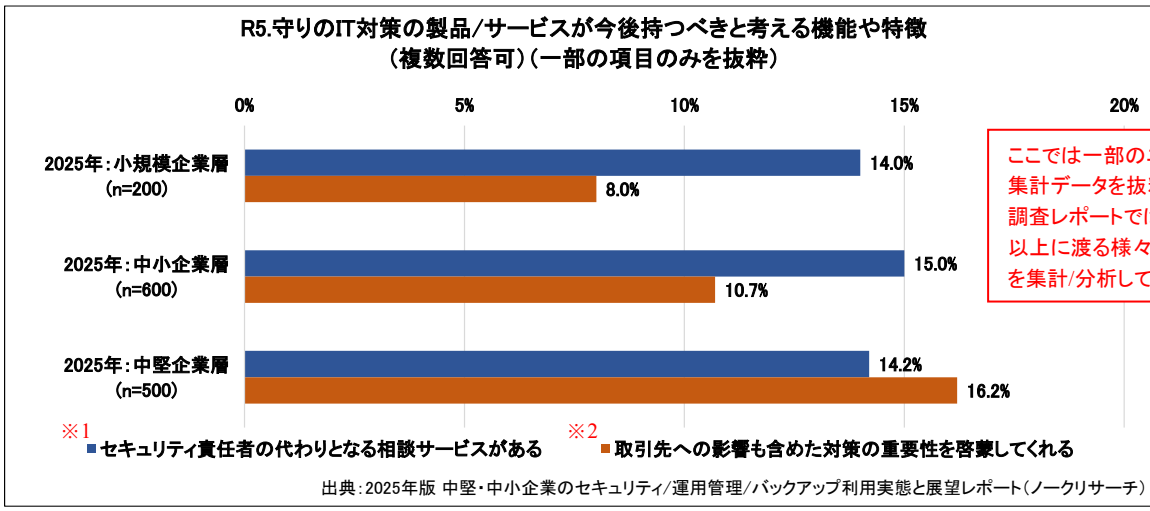
中堅企業層に対しては「取引先（大企業）への影響も考慮した対策」を支援することが重要

以下のグラフは前頁に赤字で記載した「ネットワークから隔離してバックアップを保管できる」のニーズ項目の経年変化を年商別に集計したものだ。いずれの年商帯においても値が増加しており、年商規模が小さい企業層の方が増加幅が大きいことがわかる。したがって、バックアップ/リストアの製品/サービスを開発/販売するベンダとしては「LANから隔離可能なデータ保管」の仕組みを中堅・中小企業の広い裾野に提供できれば、今後の大きな差別化ポイントとなってくる。とは言え、小規模企業層や中小企業層にとって本格的な「エアギャップ」を構築することは容易ではない。ストレージ筐体内に隔離された領域を設けるなど、規模の小さなユーザ企業でも導入/運用しやすい仕組みが求められてくる。



ここでは一部のニーズの集計データを抜粋したが調査レポートでは20項目以上に渡る様々なニーズを集計/分析している

さらにランサムウェア対策においては、日頃の備えや有事の対応に向けた人員体制の整備も欠かせない。だが、IT管理/運用を担う人材が限られる中堅・中小企業では、この点が弱点となりやすい。そうした実情がニーズを尋ねた結果にも表れている。以下のグラフは前頁に青字で記載した「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」（※1）と「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」（※2）の2つのニーズ項目の回答割合を年商別に集計したものだ。



ここでは一部のニーズの集計データを抜粋したが調査レポートでは20項目以上に渡る様々なニーズを集計/分析している

中堅企業層は大企業直下の下請けとなることも少なくないため、上記のグラフの※2が示すようにランサムウェア被害に遭った時の取引先に与える影響への危機感が中小企業層や小規模企業層と比べて高いことが確認できる。一方、※1は年商規模に依らないため、CIOに該当する役割を肩代わりする支援策は幅広い企業層に対してニーズが見込めることがわかる。ここではごく一部のニーズ項目について触れたが、調査レポートではその他の課題/ニーズについても詳細な集計/分析を行い、IT企業が提供すべき支援は何か？を提言している。

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