

SCS評価制度(サプライチェーン強化に向けたセキュリティ対策)を見据えてIT企業が準備すべきこと

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)は経産省/IPAが主導するSCS評価制度(サプライチェーン強化に向けたセキュリティ対策評価制度)を見据えて、中堅・中小企業を顧客とするIT企業が準備すべきことは何か?を分析し、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増補版」のサンプル/ダイジェストである。

<中堅・中小企業におけるセキュリティ対策意識の高まりを的確に捉えることが重要>

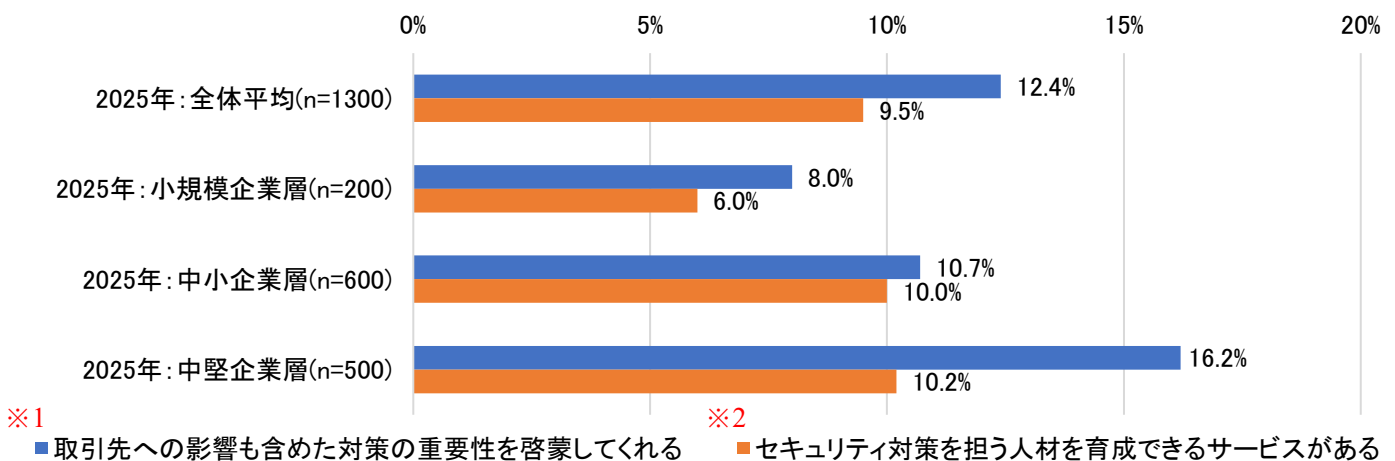
- セキュリティ対策の重視事項では全ての年商区分で「取引先への影響」≧「人材育成」
- 中堅・中小企業から見た「SECURITY ACTION」と「SCS評価制度」の違いを理解しておく
- 製造業・建設業では従業員の啓蒙/訓練や運用管理/資産管理も含めた広い視点が必要
- 今後は中小企業層でもマルウェア侵入後の対策(権限の制限/分割など)の重要性が増す

セキュリティ対策の重視事項では全ての年商区分で「取引先への影響」≧「人材育成」

近年、日本国内の有名企業を標的としたランサムウェア攻撃が大きく報道されるようになってきた。その中には取引先である中堅・中小企業が攻撃の入り口/踏み台となったケースも少なくない。その結果、中堅・中小企業においても「自社だけでなく、取引先への影響も踏まえたセキュリティ対策」への意識が高まってきている。さらに、2026年度末(2027年1~3月頃)からは経産省やIPAが主導する『サプライチェーン強化に向けたセキュリティ対策評価制度(SCS評価制度)』の申請受付開始も予定されている。こうした背景を受けて、ノークリサーチでは「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」にSCS評価制度に関連する集計/分析を追加した増補版を発刊することとなった。本リリースはそのサンプル/ダイジェストを紹介したものである。

以下のグラフは中堅・中小企業に対して、セキュリティ/運用管理/バックアップ対策のニーズを尋ねた結果の中から、「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」(※1)および「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」(※2)の回答割合を年商別に集計したものだ。

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)



出典: 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増補版(ノークリサーチ)

セキュリティ対策を担う人材の育成は中堅・中小企業にとって喫緊の経営課題の1つだ。だが、それと同等もしくは上回る形でサプライチェーンを意識したセキュリティ対策の啓蒙が求められていることがわかる。IT企業にとっては、SCS評価制度に伴うユーザ企業の意識の高まりを実際の製品/サービス導入に結びつけられるか?が重要となってくる。次頁以降では、増補版の調査レポートの中から、上記に述べた観点での分析/提言の一部をサンプル/ダイジェストとして紹介している。

中堅・中小企業から見た「SECURITY ACTION」と「SCS評価制度」の違いを理解しておく

企業間のサプライチェーンを狙ったランサムウェア攻撃が増加する中、発注側と受注側は互いのセキュリティ対策状況を適切に把握しておく必要がある。だが、そのための判断基準を個々の企業が策定することは難しい。そこで、経産省とIPAが策定を進めているのが「サプライチェーン強化に向けたセキュリティ対策評価制度(SCS評価制度)」(※)である。

※ <https://www.ipa.go.jp/security/scs/index.html>

SCS評価制度はサプライチェーンを構成する企業が実施すべきセキュリティ対策を3つのレベルに体系化し、第三者による評価を通じて、取引先が安心して受発注を行える環境整備を推進する取り組みだ。受注側は自社の対策レベルを客観的に示すことで安全/信頼をアピールすることができる。また、発注側は取引先選定やリスク管理の判断材料として同制度を活用できる。

一方、IPAが従来から推進している「SECURITY ACTION」は主に中小企業がセキュリティ対策に自主的に取り組むことを宣言する制度であり、「1つ星」と「2つ星」の2段階で取り組み状況を示す仕組みとなっている。「SECURITY ACTION」は自己宣言によるものなので、サプライチェーンにおいて取引先がセキュリティ対策状況を客観的に確認する手段としては必ずしも十分とは言えなかった。

これに対して、SCS評価制度は定められた基準を満たしていることを第三者が評価する形式となっており、対応レベルによって「3つ星」「4つ星」「5つ星」の3段階が設けられている。つまり、SECURITY ACTIONが「セキュリティ対策の第一歩」を啓蒙する制度であるのに対して、SCS評価制度は「取引先から信頼されるセキュリティ水準を証明する制度」と位置付けることができる。SCS評価制度は2027年3月末までに「3つ星」と「4つ星」の申請開始が予定されており、「5つ星」については実施内容の検討が進んでいる。(2026年7月現在) SECURITY ACTIONおよびSCS評価制度をレベルに沿って整理すると以下ようになる。

「SECURITY ACTION」(※1)および「SCS評価制度」(※2)の概要

	レベル	内容	実施方法	制度の実施状況
※1	1つ星	セキュリティ対策の取り組み意思を宣言する	第三者評価は不要(宣言のみ)	既に実施中
	2つ星	自己診断を行い、対策方針を宣言/公開する	第三者評価は不要(宣言のみ)	既に実施中
※2	3つ星	サプライチェーンに含まれる企業が実施すべき最低限のセキュリティ対策	専門家の確認を伴う自己評価	2027年3月末までに開始予定
	4つ星	サプライチェーンに含まれる企業が実施すべき標準的なセキュリティ対策	第三者機関による評価	2027年3月末までに開始予定
	5つ星	サプライチェーンに含まれる企業が目指すべき高度なセキュリティ対策	第三者機関による評価	内容を現在検討中

出典: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増補版(ノークリサーチ)

制度の開始前ということもあり、現段階ではSCS評価制度が中堅・中小企業に広く認知されている状況には至っていない。だが、中堅・中小企業にとって、自社のセキュリティ対策状況を客観的に示す取り組みは今後更に重要になっていく。IT企業としてはユーザ企業におけるSCS制度の星取得を支援するだけでなく、取引先への影響を考慮したセキュリティ対策に直結する製品/サービスを的確に提案する役割が求められる。

そこで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増補版」では、セキュリティ/運用管理/バックアップ対策のニーズを尋ねた設問の中で「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」という選択肢を選んだユーザ企業(=取引先への影響を考慮したセキュリティ対策への意識が高いユーザ企業)がどのような課題やニーズを抱えているのか?を分析し、SCS評価制度に伴う製品/サービス提案を「点」から「面」に広げていくために何をすべきか?を提言している。次頁以降では、そうした分析/提言の一部を紹介している。

製造業・建設業では従業員の啓蒙/訓練や運用管理/資産管理も含めた広い視点が必要

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「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？」を尋ねている。

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

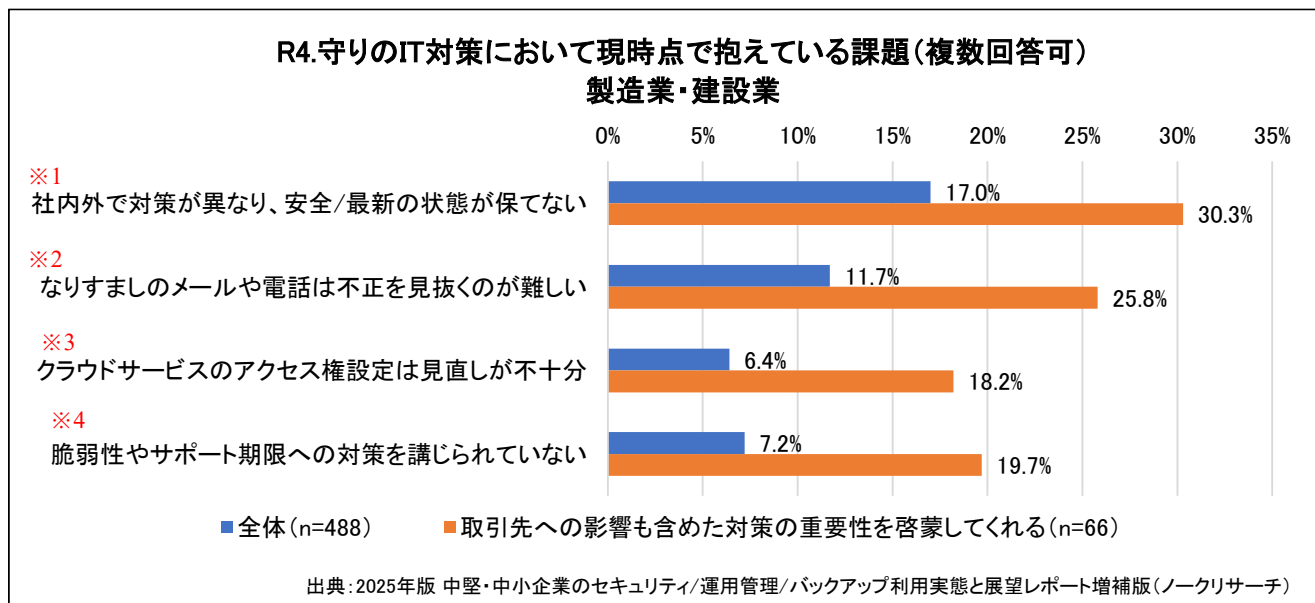
<<運用管理/資産管理>>

- ・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)

調査レポートでは、年商3区分と業種3区分の計6区分について「取引先への影響を考慮したセキュリティ対策への意識が高いユーザ企業」が全体平均と比較して、どのような課題を多く挙げているか？を集計/分析している。以下のグラフはそこから、製造業・建設業における課題項目の集計結果の一部を抜粋したものだ。



全体平均と比べて「社内外での対策の違い」(※1)、「なりすましへの対処」(※2)、「クラウドサービスのアクセス権設定」(※3)、「脆弱性やサポート期限への対策」(※4)の回答割合が高くなっている。そのため、サプライチェーンを考慮したセキュリティ対策の意識が高い製造業・建設業に対してはマルウェア対策ツールの導入提案だけでなく、従業員の啓蒙/訓練(※2)や運用管理/資産管理(※3、※4)、社内外を網羅したインフラ管理(※1)といった幅広い視点に立ったセキュリティ対策を提示していくことが重要となってくる。ここでは製造業・建設業における課題の一部を抜粋したが、調査レポートでは年商3区分および業種3区分の計6区分について同様の集計/分析を行っている。次頁ではニーズの観点から見た分析/提言の一部を紹介していく。

今後は中小企業層でもマルウェア侵入後の対策(権限の制限/分割など)の重要性が増す

さらに、本リリースの元となる調査レポートでは、以下の選択肢を列举して「セキュリティ/運用管理/バックアップといった守りのIT対策における今後のニーズ」についても尋ねている。

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

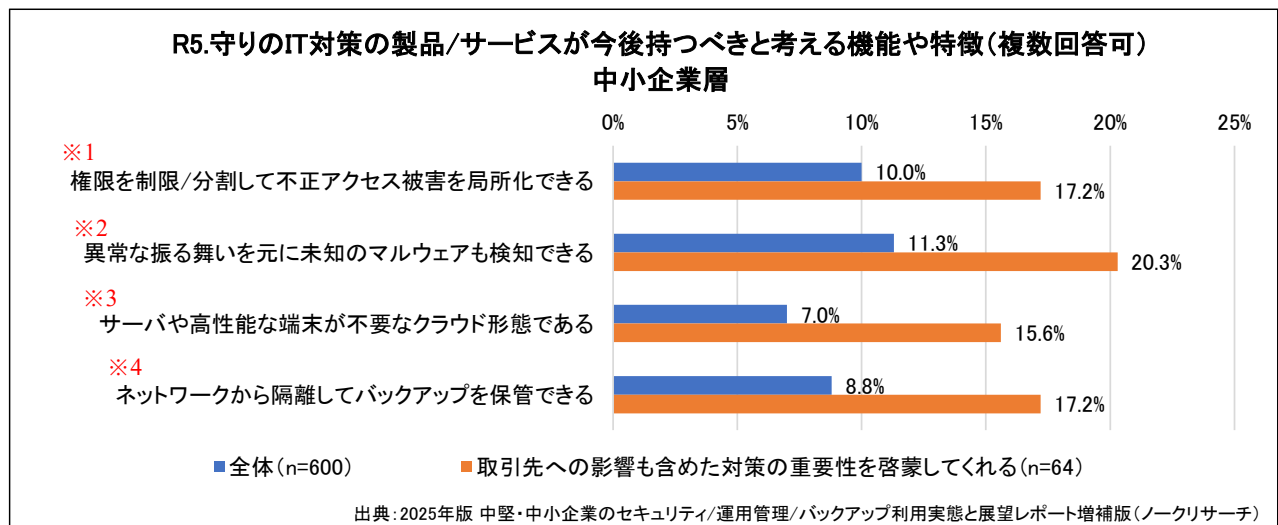
<<運用管理/資産管理>>

- ・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)

調査レポートでは、年商3区分と業種3区分の計6区分について「取引先への影響を考慮したセキュリティ対策への意識が高いユーザ企業」が全体平均と比べて、どのようなニーズ項目を多く挙げているか?を集計/分析している。以下のグラフはその中から、中小企業層(年商5億円以上～50億円未満)におけるニーズの集計結果の一部を抜粋したものだ。



全体平均と比べると、「未知のマルウェア検知」(※2)や「クラウド形態の対策」(※3)に加えて、「権限の制限/分割」(※1)、「N/Wから隔離されたバックアップ」(※4)といったニーズも多く挙げられている。つまり、中小企業層においても、サプライチェーンへの影響を踏まえたセキュリティ対策意識の高い企業ではマルウェアの防御だけでなく、侵入された場合を想定した対策(※1、※4)も重視している状況がうかがえる。SCS評価制度の認知が高まるにつれて、こうした傾向が中小企業層全体に広がる可能性も十分考えられる。IT企業としては、そうした展開を見越した製品/サービス展開を進めていくことが大切だ。ここでは中小企業層(年商5億円以上～50億円未満)におけるニーズの一部を抜粋したが、調査レポートでは年商3区分および業種3区分の計6区分について同様の集計/分析を行っている。(次頁では、調査レポートの詳細を掲載)

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増補版』

本調査レポートは本ページ下段に記載した通常版の調査レポートに以下の集計/分析を加えた内容となっています。

年商3区分および業種3区分の計6区分について、以下の2つの設問の回答内容を「取引先への影響を考慮したセキュリティ対策への意識が高いユーザ企業」が全体平均で比較した結果を集計/分析

・R4.守りのIT対策において現時点で抱えている課題(複数回答可)

⇒ 製造業・建設業における集計/分析の抜粋を本リリースの3ページに掲載

・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)

⇒ 中小企業層における集計/分析の抜粋を本リリースの4ページに掲載

年商区分:

小規模企業: 年商5億円未満

中小企業: 年商5億円以上～50億円未満

中堅企業: 年商50億円以上～500億円未満

業種区分:

製造業・建設業: 組立製造、加工製造(プロセス製造)、建築、土木、設備など

卸売業・小売業: 商品の卸売(商社、仲介など)、小売(スーパー、専門店など)

運輸業・サービス業: 運輸(トラック運送、倉庫など)および各種のサービス業

価格: 270,000円(税別) 通常版をご購入済みの場合は45,000円(税別)で増補版収録分を追加購入可

発刊日: 2026年7月31日

通常版『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】

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

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

第3章: 守りのIT対策における課題の変化と最新動向

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

第6章: 守りのIT対策における費用

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刊の調査レポート(1/2):

2026年版 中堅・中小企業におけるERPのリプレイス/新規導入を促進する要因と市場規模予測レポート

年商別(小規模企業/中小企業/中堅企業)と業種別(製造業・建設業、卸売業・小売業、運輸業・サービス業)にERPのリプレイスや新規導入につながるユーザ企業の重視事項、課題、ニーズは何か?を分析&提言。

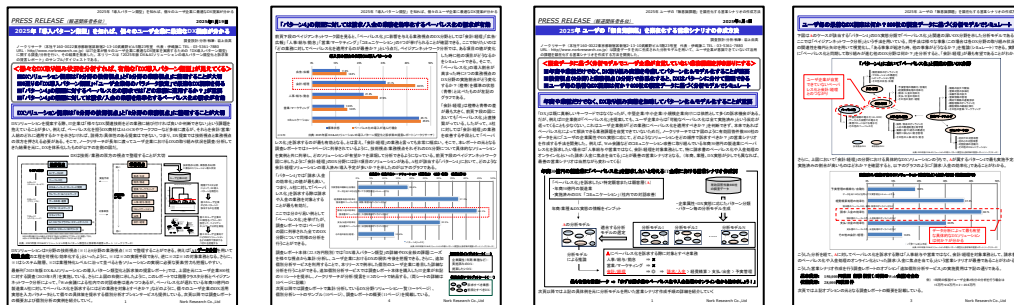
【レポート案内】 https://www.norkresearch.co.jp/pdf/2026ERPBN_rell.pdf



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

DXソリューションを技術視点(9分野/48項目)&業務視点(8分野/38項目)に基づく導入パターン類型に整理し、個別分析サービス(オプション)による個々のユーザ企業向けDX提案の施策/提言までカバーした次世代型の調査レポート。生成AIのサービスシェア、適用場面、ユーザ企業の課題/ニーズ、導入費用も網羅。

【レポート案内】 https://www.norkresearch.co.jp/pdf/2025DXAI_user_rep.pdf



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

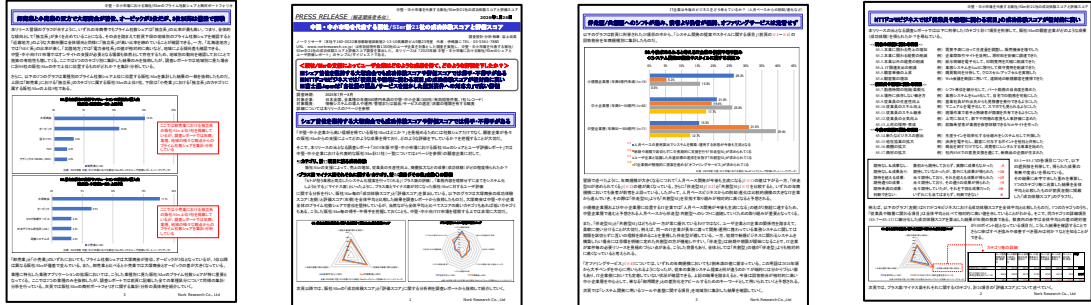


ご好評いただいている既刊の調査レポート(2/2):

2025年版 中堅・中小市場における販社/SIerのシェアとユーザ評価レポート

中堅・中小市場で注目すべき販社/SIerの導入社数シェア(年商別/業種別/地域別)、商材ポートフォリオ、顧客企業が得た成功体験、顧客企業から見たプラス/マイナス評価を集計/分析、さらにAI活用、ユーザ内製、伴走型SI/共創型SIへのシフトなどに関するIT企業側の実態と考え方も網羅。

【レポート案内】 https://www.norkresearch.co.jp/pdf/2025SIer_user_rep.pdf



2025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「どんなIT商材/ソリューションをどのIT企業から導入するのか?」「それで得られた成功体験(売上増、従業員の生産性向上など)は何か?」「委託先/購入先のIT企業に関する満足点や不満点は何か?」を集計/分析し、今後有望なIT商材/ソリューションやユーザ企業セグメント(年商や業種)を提言

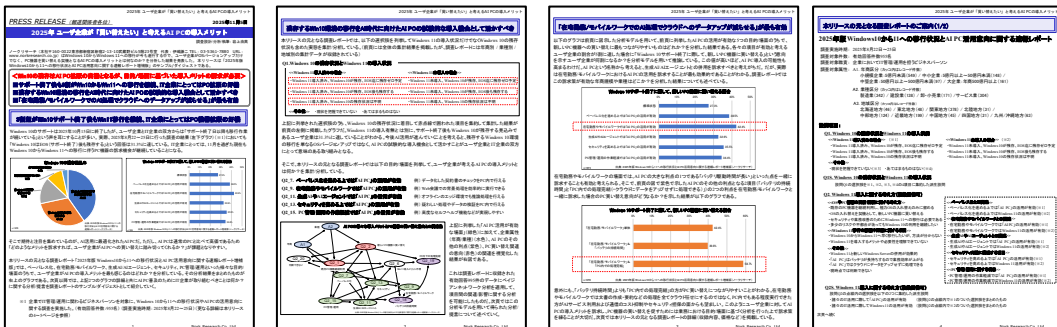
【レポート案内】 https://www.norkresearch.co.jp/pdf/2025SP_user_rep.pdf



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増補版

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

【レポート案内】 https://www.norkresearch.co.jp/pdf/2025PCflash_relex.pdf

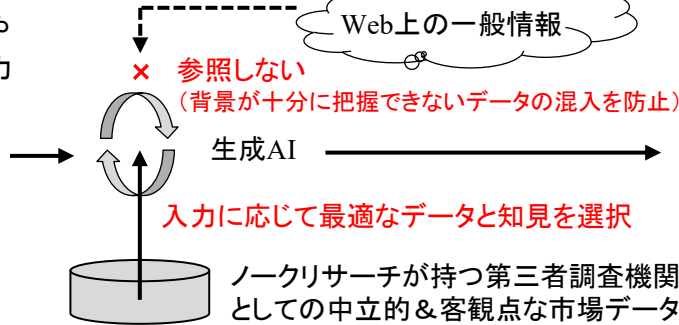


各種の関連サービス

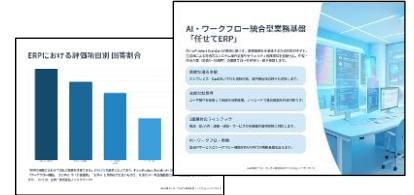
入力された企画案や販促アピールを元に、ノークリサーチの市場調査データや知見が盛り込まれたPPTX資料を自動生成

AI×市場データ:プレゼン資料生成サービス

製品/サービスの企画案や
アピールをブラウザで入力



市場調査のデータや知見を元に
製品/サービスが注力すべき点や
効果的なアピールをPPTX / PDF
形式のプレゼン資料として提示



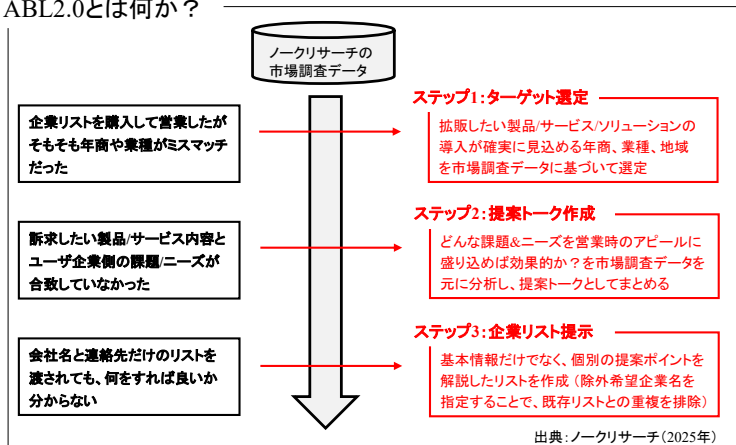
詳しいご案内については、右記をご参照ください
サービスの活用例紹介:

https://www.norkresearch.co.jp/pdf/pmc_service.pdf

https://www.norkresearch.co.jp/pdf/2026pmc_rel3.pdf

市場調査データを元にターゲット選定/提案トーク作成/企業リスト提示を行う『ABL2.0』

ABL2.0とは何か?



サービス案内と実施の具体例を以下でご覧いただけます。

https://www.norkresearch.co.jp/pdf/2025ABL20_rel.pdf

ターゲットに沿った提案トークを含む企業リストの具体例

企業名	株式会社DEスタイル
設立年	1964年
資本金	5億円
売上高	45億円(2025年1月期)
決算月	1月
従業員数	436名(2025年2月現在)
上場有無	未上場
所在地	大阪府大阪市**区**町 1-1-1
ホームページ	https://www.destyle.**.**
メールアドレス	info@destyle.**.**
Webフォーム	https://www.destyle.**.**/contact.html
電話番号	06-****-****
業態と特徴	衣料素材の卸問屋として創業し、近年ではアパレルの企画/開発/生産/販売を一気通貫で担うビジネスを展開。試作品段階では3Dモデリングを積極的に活用するなど、DXやSDGsに対する意識が高い。 参照ページ: https://www.destyle.**.**/profile.html
提案時のポイント	「AI需要予測を用いた在庫管理ソリューション」の提案トーク解決が有効な課題: C.1: 仕入先の倒産リスク C.2: 勤や経験による管理関連性の高いニーズ: D.3: センサによる入庫記録 DXへの取り組みが進んでいるため、C.2の課題は既にクリアされており、D.3についても既に着手済みの可能性が高い。素材の調達先には海外企業も多いため、地政学的情報も含めてC.1を分析できるソリューションを提示することが有効。

本リリースの無断引用・転載を禁じます。引用・転載をご希望の場合は下記をご参照の上、担当窓口にお問い合わせください。

引用・転載のポリシー: <https://www.norkresearch.co.jp/policy/index.html>

本リリース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