PRESS RELEASE（報道関係者各位）

2024年5月27日

2024年 ゼロトラスト提案の満足度から導かれる「最初に訴求すべきセキュリティ対策」

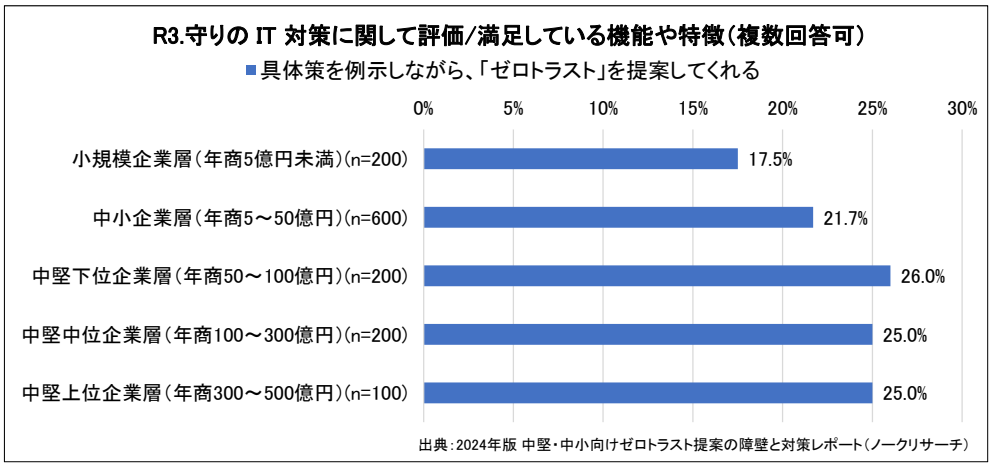
調査設計/分析/執筆：岩上由高

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：http//www.norkresearch.co.jp）はゼロトラスト提案において最初に訴求すべきセキュリティ対策は何か？の分析結果を発表した。本リリースは「2024年版 中堅・中小向けゼロトラスト提案の障壁と対策レポート」のサンプル/ダイジェストである。

＜重点を置くべき具体的なセキュリティ対策は何か？の判断がゼロトラスト提案の成否を分ける＞

■ゼロトラスト提案の満足度は改善/向上し、中小企業層で20%強、中堅企業層では25%以上
■年商規模はゼロトラスト提案の評価/満足にも影響、最初に訴求すべき項目は全部で5つ
■年商50～100億円には「標的型攻撃訓練」と「バックアップ復元検証」を最初に訴求すべき
■評価/満足の状況に加えて「現状の課題」「今後のニーズ」に関する分析も行うことが重要

ゼロトラスト提案の満足度は改善/向上し、中小企業層で20%強、中堅企業層では25%以上



ゼロトラストは中堅・中小企業においても今後最も重要なセキュリティ対策となっている。

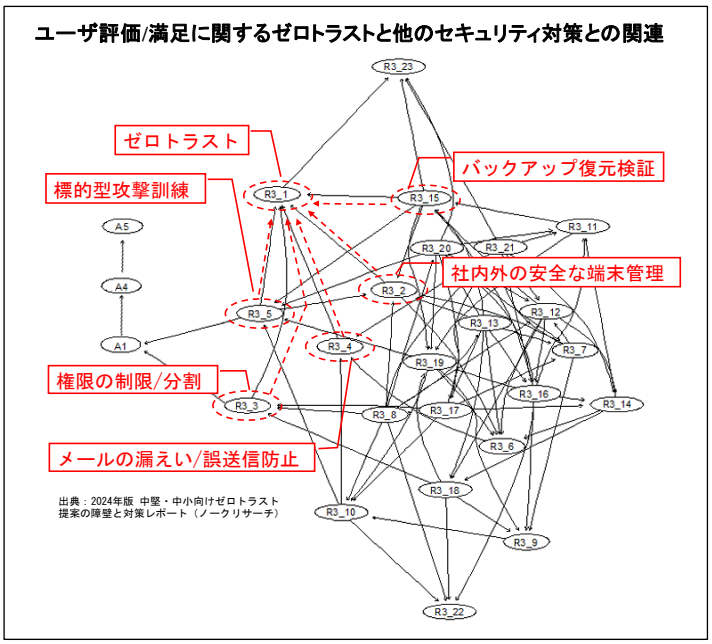
左記のグラフは有効回答件数1300社の中堅・中小企業に対し、ゼロトラスト提案の満足度を尋ねた結果を年商別に集計したものだ。

「具体策を例示しながら、ゼロトラストを提案してくれる」と回答した企業の割合は小規模企業層では2割未満であるが、中小企業層では20%強、中堅企業層（上記のグラフでは3つの企業層に細分化されている）では25%以上に達している。「ゼロトラスト」というキーワードが広く知られるようになってから数年が経過し、IT企業側の提案も徐々に洗練されてきている状況が垣間見える。だが、ゼロトラストに関しては依然として

・ファイアーウォールを用いないことがゼロトラストである
・クラウド経由でのリモート接続がゼロトラストである
・ID管理を強化/改善することがゼロトラストである

などのように、特定の製品/サービスに大きく偏った理解/認知も見受けられる。とは言え、ゼロトラストの考え方を抽象的に説明するだけではIT企業側/ユーザ企業側のいずれも最初の一歩を踏み出すことができない。

そこで、本リリースの元となる「2024年版 中堅・中小向けゼロトラスト提案の障壁と対策レポート」では有効回答件数1300社のユーザ企業における様々なセキュリティ対策の評価/満足度を調査し、ゼロトラスト提案に最もつながりやすいのはどれか？を分析している。右図はその結果を図示したものだ。次頁では右図が示す意味合いと分析結果の一部を調査レポートのサンプル/ダイジェストとして掲載している。



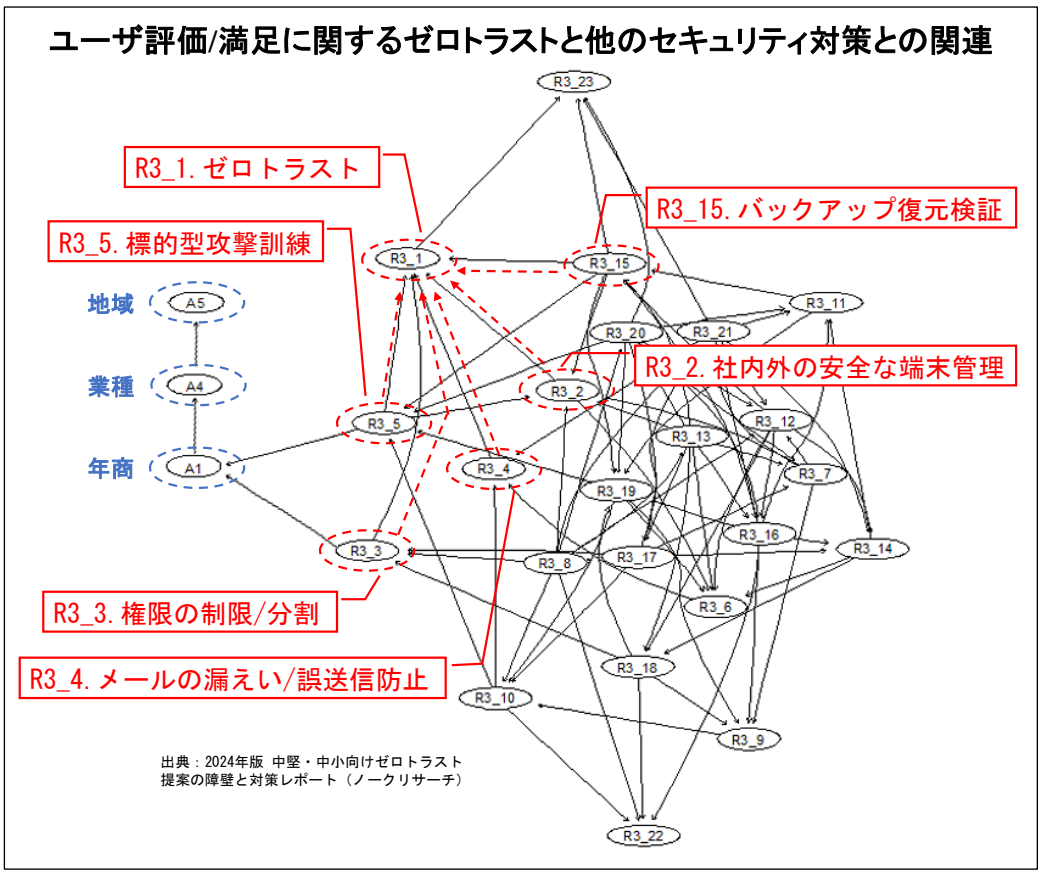
年商規模はゼロトラスト提案の評価/満足にも影響、最初に訴求すべき項目は全部で5つ

本リリースの元となる調査レポートでは、以下の項目を列挙して「守りのIT対策に関して評価/満足している機能や特徴」は何かを尋ねた結果を分析している。これによって、セキュリティ関連を中心とした守りのIT対策の製品/サービスに関してユーザ企業が評価/満足しているポイントを様々な観点から把握できる。

R3.守りの IT 対策に関して評価/満足している機能や特徴（複数回答可）

- R3_1.具体策を例示しながら、「ゼロトラスト」を提案してくれる
- R3_2.社内外で端末を安全/最新な状態に保つことができる
- R3_3.権限を制限/分割して不正アクセス被害を局所化できる
- R3_4.メールによる秘匿情報の漏えいや誤送信を防止できる
- R3_5.標的型攻撃を想定した実地訓練サービスを利用できる
- R3_6.異常な振る舞いを元に未知のマルウェアも検知できる
- R3_7.侵入したマルウェアを封じ込めて隔離し、無力化する
- R3_8.サーバや高性能な端末が不要なクラウド形態である
- R3_9.運用/保守のアクセス回線にもマルウェア対策が施せる
- R3_10.PCに加えてスマートデバイスも一括で管理/保護できる
- R3_11.特権/管理アカウントは運用条件を厳しく設定できる
- R3_12.未使用の放置アカウントを自動的に検出/停止できる
- R3_13.複数システムのアカウントを集約して一括管理できる
- R3_14.生体認証または多要素/二段階認証に対応している
- R3_15.バックアップだけでなく、復元の検証も行ってくれる
- R3_16.ネットワークから隔離してバックアップを保管できる
- R3_17.クラウド上にシステムとデータを複製して保管できる
- R3_18.検索/参照が容易な状態で大量データを保管できる
- R3_19.端末の操作ログを記録して、不正や攻撃を防止できる
- R3_20.OS更新の状況を可視化して、更新を自動で制御できる
- R3_21.脆弱性やサポート期限への対処方法を提示してくれる
- R3_22.無駄なライセンスがないかを自動で検索/一覧できる
- R3_23.個人情報保護に関する認証取得の支援も付属している

下図は1300社の中堅・中小企業に対し、上記に列挙した項目を尋ねたデータにベイジアンネットワーク分析を適用したものだ。守りのIT対策の評価/満足に関する様々な項目のうち、関連性の高いもの同士は互いに近接したノード（楕円）として表現され、エッジ（矢印）が項目間の影響状況を反映している。最初に着目すべきなのは「A1.年商」「A4.業種」「A5.地域」といった主要な企業属性については「A1.年商」を介して他の項目と接続している点である。つまり、守りのIT対策の評価/満足については業種や地域よりも年商規模の違いが最も重要な企業属性であることがわかる。



その上で、「R3_1.ゼロトラスト」の評価/満足に強く影響を与えている(矢印が直接つながっている）項目を確認すると、以下の5つの項目であることが確認できる。

R3_2.社内外の安全な端末管理
R3_3.権限の制限/分割
R3_4.メールの漏えい/誤送信防止
R3_5.標的型攻撃訓練
R3_15.バックアップ復元検証

したがって、ゼロトラスト提案で高い評価/満足を得るためには、まずは上記5つの項目を具体的な最初の一歩としてアプローチしていくことが有効と考えられる。

次頁ではこれら5つの項目の中で最も注力すべきもの（優先度を上げるべき項目）はどれなのか？について見ていくことにする。

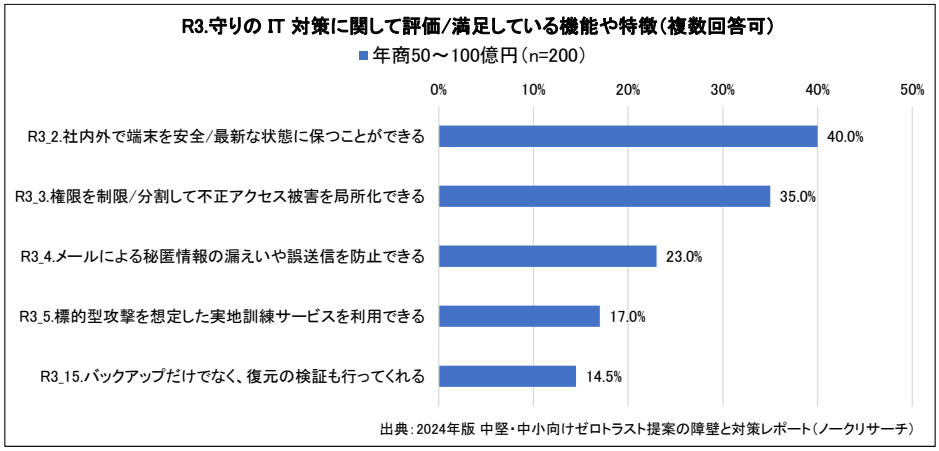
年商50～100億円には「標的型攻撃訓練」と「バックアップ復元検証」を最初に訴求すべき

前頁までの分析が示すように、ゼロトラスト提案の評価/満足を高めるためには最初の一歩となる守りのIT対策として

R3_2.社内外の安全な端末管理
R3_3.権限の制限/分割
R3_4.メールの漏えい/誤送信防止
R3_5.標的型攻撃訓練
R3_15.バックアップ復元検証

の5つの項目を訴求することが有効だ。
だが、これら全てを実施することは容易ではないため、最も優先度の高い項目は何かについても確認しておく必要がある。

前頁で述べたように、守りのIT対策における評価/満足は年商規模の違いも深く関係する。そこで、以降では本リリース冒頭のグラフでゼロトラスト提案の評価/満足が最も高かった年商50～100億円の中堅下位企業層を具体例とした分析結果を述べる。（年商規模が異なれば、以下で述べる内容も変わってくる点に注意）

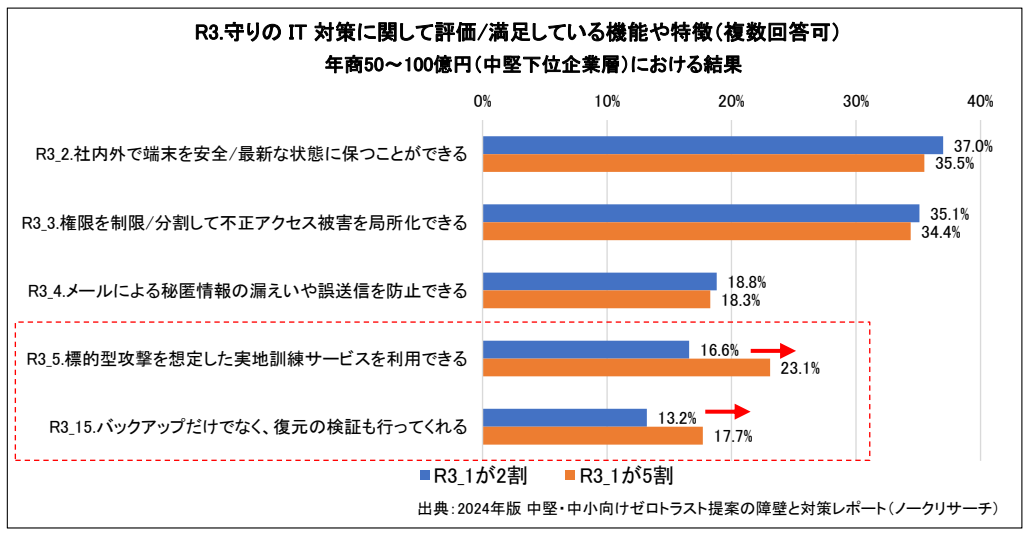


まず、左記のグラフは中堅下位企業層におけるR3_2～R3_5およびR3_15の5項目の回答割合を集計したものだ。

回答割合の高さという点では
R3_2.社内外の安全な端末管理
R3_3.権限の制限/分割
が3割超で比較的有望ということになる。

ただし、これらは各項目単体での回答割合であり、ゼロトラスト提案の評価/満足との関連を加味した結果ではない。

一方、ベイジアンネットワーク分析では「ある項目の回答割合が***に達したとした場合、その他の項目の値はどうなるか？」を推論（シミュレーション）できる。そこで、「R3_1.ゼロトラスト」の値が2割程度から5割程度に高まった時、上記の5項目の値がどう変化するか？を示したものが以下のグラフである。



青帯（ゼロトラスト提案の評価/満足が2割程度だった場合）と比較して、橙帯（5割程度に高まった場合）の増加幅が大きな項目がゼロトラスト提案の評価/満足にプラスの効果をもたらすものということになる。

グラフ内でそれに該当するのが

R3_5.標的型攻撃訓練
R3_15.バックアップ復元検証

の2項目である。中堅・中小企業においても、特定の企業を標的としたランサムウェア攻撃の脅威が近年高まっていることを踏まえると、これら2項目の訴求は堅実な取り組みとも言える。したがって、IT企業が中堅下位企業層向けのゼロトラスト提案に取り組む際は、まず標的型攻撃を想定した実地訓練サービス（※1）とバックアップの復元検証サービス（※2）を組み合わせ、ランサムウェア攻撃の事前（※1）と事後（※2）の対策を講じた上で、その他のゼロトラスト提案（ID管理やSASEなど）へと展開することが有効だ。ここでは中堅下位企業層における分析結果を紹介したが、本リリースの元となる調査レポートではその他の年商帯についても同様の分析を行っている。さらに次頁ではゼロトラスト提案の評価/満足の観点に加えて、現状の課題や今後のニーズに関連したポイントについても述べている。

評価/満足の状況に加えて「現状の課題」「今後のニーズ」に関する分析も行うことが重要

本リリースの元となる調査レポートでは、前頁までに述べた「評価/満足している項目」だけでなく、以下に列挙したように「現状の課題」や「今後のニーズ」の観点での分析も行っている。

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） ← 現状の課題

- R4_1.「ゼロトラスト」を提唱しているが、具体策が分からない
- R4_2.社内外で対策が異なり、安全/最新の状態が保てない
- R4_3.管理権限が強いため、乗っ取られた時の被害が大きい
- R4_4.メールによる情報漏えい/誤送信の対策を講じていない
- R4_5.標的型攻撃の被害や危険性が十分に周知されていない
- R4_6.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
- R4_7.マルウェアに侵入された時、隔離/無力化する手段がない
- R4_8.サーバ導入が必須、もしくは端末側の処理が重い/遅い
- R4_9.運用/保守のアクセス回線はマルウェア対策が不十分
- R4_10.スマートデバイスの対策が不十分、またはPCと異なる
- R4_11.特権/管理アカウントの悪用を防ぐ施策を講じていない
- R4_12.未使用のアカウントが削除されずに放置されている
- R4_13.システム毎に複数のアカウントが散在/乱立している
- R4_14.生体認証や多要素/二段階認証に対応できていない
- R4_15.バックアップを復元できるかの検証を実施していない
- R4_16.LANなどを介してバックアップが消される恐れがある
- R4_17.システムやデータを安全なクラウド上に保管できない
- R4_18.保管した大量データを容易に検索/参照できない
- R4_19.端末の不正操作や故意の情報漏えいを防止できない
- R4_20.OS更新の現状が把握できず、管理/制御もできない
- R4_21.脆弱性やサポート期限への対策を講じられていない
- R4_22.ライセンスの利用状況を把握しておらず、無駄が多い
- R4_23.個人情報保護に関する認証取得の方法が分からない

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） ← 今後のニーズ

- R5_1.具体策を例示しながら、「ゼロトラスト」を提案してくれる
- R5_2.社内外で端末を安全/最新な状態に保つことができる
- R5_3.権限を制限/分割して不正アクセス被害を局所化できる
- R5_4.メールによる秘匿情報の漏えいや誤送信を防止できる
- R5_5.標的型攻撃を想定した実地訓練サービスを利用できる
- R5_6.異常な振る舞いを元に未知のマルウェアも検知できる
- R5_7.侵入したマルウェアを封じ込めて隔離し、無力化する
- R5_8.サーバや高性能な端末が不要なクラウド形態である
- R5_9.運用/保守のアクセス回線にもマルウェア対策が施せる
- R5_10.PCに加えてスマートデバイスも一括で管理/保護できる
- R5_11.特権/管理アカウントは運用条件を厳しく設定できる
- R5_12.未使用の放置アカウントを自動的に検出/停止できる
- R5_13.複数システムのアカウントを集約して一括管理できる
- R5_14.生体認証または多要素/二段階認証に対応している
- R5_15.バックアップだけでなく、復元の検証も行ってくれる
- R5_16.ネットワークから隔離してバックアップを保管できる
- R5_17.クラウド上にシステムとデータを複製して保管できる
- R5_18.検索/参照が容易な状態で大量データを保管できる
- R5_19.端末の操作ログを記録して、不正や攻撃を防止できる
- R5_20.OS更新の状況を可視化して、更新を自動で制御できる
- R5_21.脆弱性やサポート期限への対処方法を提示してくれる
- R5_22.無駄なライセンスがないかを自動で検索/一覧できる
- R5_23.個人情報保護に関する認証取得の支援も付属している

例えば、**「既にゼロトラスト提案を進めているが、顧客企業がセキュリティ上で様々な課題を抱えており、どれを優先的に解決すれば良いか分からない」**という場合は上記の「現状の課題」を尋ねた結果について本リリースと同様の分析を行い、『R4_1.「ゼロトラスト」を提唱しているが、具体策が分からない』という課題が減少した時に同時に回答割合が減少する項目は何か？を探れば良いことになる。そこで、減少幅が最も大きな課題が既に進めているゼロトラスト提案を成功させる上で、まず最初に解決すべき課題となる。

あるいは**「今後ゼロトラスト提案を進めるに際して、特権/管理アカウントの制限、放置アカウントの検出/停止、アカウント集約といったアカウント関連のソリューションを突破口にしたいと考えているが、どれに注力すべきか？が判断できない」**という場合は「今後のニーズ」を尋ねた結果について本リリースと同様の分析を行い、R5_11（特権/管理アカウントの制限）、R5_12（放置アカウントの検出/停止）、R5_13（アカウント集約）の3つの項目の中で『R5_1.具体策を例示しながら、「ゼロトラスト」を提案してくれる』というニーズが高まった時に回答割合が最も増加するものを選べば良いことになる。

次頁では、本リリースの元となる調査レポートの提供内容や価格などを記載している。

本リリースの元となる調査レポートのご紹介

2024年版 中堅・中小向けゼロトラスト提案の障壁と対策レポート（セミカスタムレポート）

個別の事前ヒアリング結果を元に、ゼロトラスト提案で重点を置くべきセキュリティ対策は何か？をIT企業毎に分析/提言するカスタムメイドの調査レポート

調査対象属性

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）

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

調査レポートの提供内容

本調査レポートは指定/選択された条件によって成果物が変わる「セミカスタムレポート」の形式を採用している。

ステップ1： 事前ヒアリング

調査レポートを購入いただいたIT企業様におけるゼロトラスト提案の現状や課題/ニーズをヒアリング（Web会議）。

例） ゼロトラスト提案における顧客満足度を高めたいと考えているが、自社が提供する様々なセキュリティ対策が多岐に渡っており、どれを重点的に改善すべきか？が分からない

例） 既にゼロトラスト提案を進めているが、顧客企業がセキュリティ上で様々な課題を抱えており、どれを優先的に解決すれば良いか分からない

例） 今後ゼロトラスト提案を進めるに際して、特権/管理アカウントの制限、放置アカウントの検出/停止、アカウント集約などのアカウント関連のソリューションを突破口にしたいと考えているが、どれに注力すべきか？が判断できない

※訴求対象となる企業属性（年商、業種、所在地）が明確である場合はそれらもステップ2の分析に反映

ステップ2： 分析と提言

ステップ1で得た課題/ニーズを踏まえて、本リリースに記載した流れに沿った分析を行う。その結果を提言事項としてMicrosoft Powerpoint形式の報告書（5～10スライド）にまとめ、90分のWeb会議にて説明および質疑応答を実施する。

価格/納期など

納品物： 調査報告書（Microsoft Powerpoint形式、5～10スライド）、左記報告書に掲載したデータ（Microsoft Excel形式）

納期： ご発注日から10営業日（2週間）（発注とほぼ同時にステップ1を実施した場合の想定日数）

価格： 48万円（税別）

次頁では、既にご好評いただいている各種の発刊済み調査レポートを紹介している。

ご好評いただいている既存の調査レポートなど

2023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

IT支出が活発な企業層や支出額の内訳は変わってきている、有効回答件数1300社のユーザ調査を集計/分析し、ベンダや販社/SIerが今後注力すべき顧客セグメントやIT商材は何か？を明らかにする必携レポート

調査レポート案内： https://www.norkresearch.co.jp/pdf/2023SP_user_rep.pdf

---

2023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

今後はレイトマジョリティへの訴求が焦点。課題/ニーズの変化を捉え、市場拡大を阻む障壁を打開するためには何をすべきか？

調査レポート案内： https://www.norkresearch.co.jp/pdf/2023RPA_user_rep.pdf

---

2023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、人給、生産、ワークフロー、Web会議、CRM、BI、クラウドストレージといった10分野のシェアと評価に加えて、法制度対応やデータ分析/生成AIの動向を網羅

調査レポート案内： https://www.norkresearch.co.jp/pdf/2023itapp_rep.pdf

---

2024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

サーバはクラウドファーストの加速とオンプレ回帰のどちらに進むのか？PCでWindows 11移行を加速させるための施策とは？

調査レポート案内： https://www.norkresearch.co.jp/pdf/2024SrvPC_user_rep.pdf

---

2023年版 中堅・中小企業のDXおよびITソリューション選定の実態レポート

50項目に渡る具体的なDX/ITソリューションの導入状況、ユーザ企業が抱える課題とニーズ、選ぶべき訴求手段を網羅した一冊

調査レポート案内： https://www.norkresearch.co.jp/pdf/2023IT_user_rep.pdf

---

2023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

ランサムウェアの危険性を訴えるだけでなく、今後のIT活用方針とマッチした「ポジティブな守りのIT対策提案」が求められている

調査レポート案内： https://www.norkresearch.co.jp/pdf/2023Sec_user_rep.pdf

---

2023年版 中堅・中小企業におけるネットワーク環境の実態と展望レポート

今後不可欠となるネットワーク環境とセキュリティ対策を同時に考慮したITインフラ整備の提案ポイントを分析/提言

調査レポート案内： https://www.norkresearch.co.jp/pdf/2023NW_user_rep.pdf

---

『カスタムリサーチ』のご案内

カスタムリサーチとは、個別ニーズに応じてWebアンケートやグループインタビューといった様々な調査を設計&実施し、調査レポートよりも数段深い分析と提言を行うものです。調査レポートで市場動向を一通り理解した後、製品/サービスの開発や拡販、パートナ活性化、ユーザの理解など、各々の目的に応じたカスタムリサーチに進む流れが一般的です。
カスタムリサーチの詳細は右記をご参照ください。 https://www.norkresearch.co.jp/pdf/norkresearch.pdf

---

当調査データ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