PRESS RELEASE（報道関係者各位）

2025年7月14日

2025年 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

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：伊嶋謙ニ TEL：03-5361-7880 URL：http//www.norkresearch.co.jp）は中堅・中小企業向けのセキュリティ対策提案を「点」から「面」へと広げるための施策を提言する調査結果を発表した。本リリースは「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）」のサンプル/ダイジェストである。（調査レポートの詳細は本リリース7ページを参照）

＜中堅・中小向けのセキュリティ商材提案では、「的確なクロスセル施策」の有無が勝負を分ける＞

■インシデント対応策を一過性に終わらせず、セキュリティ商材のクロスセルにつなげていく

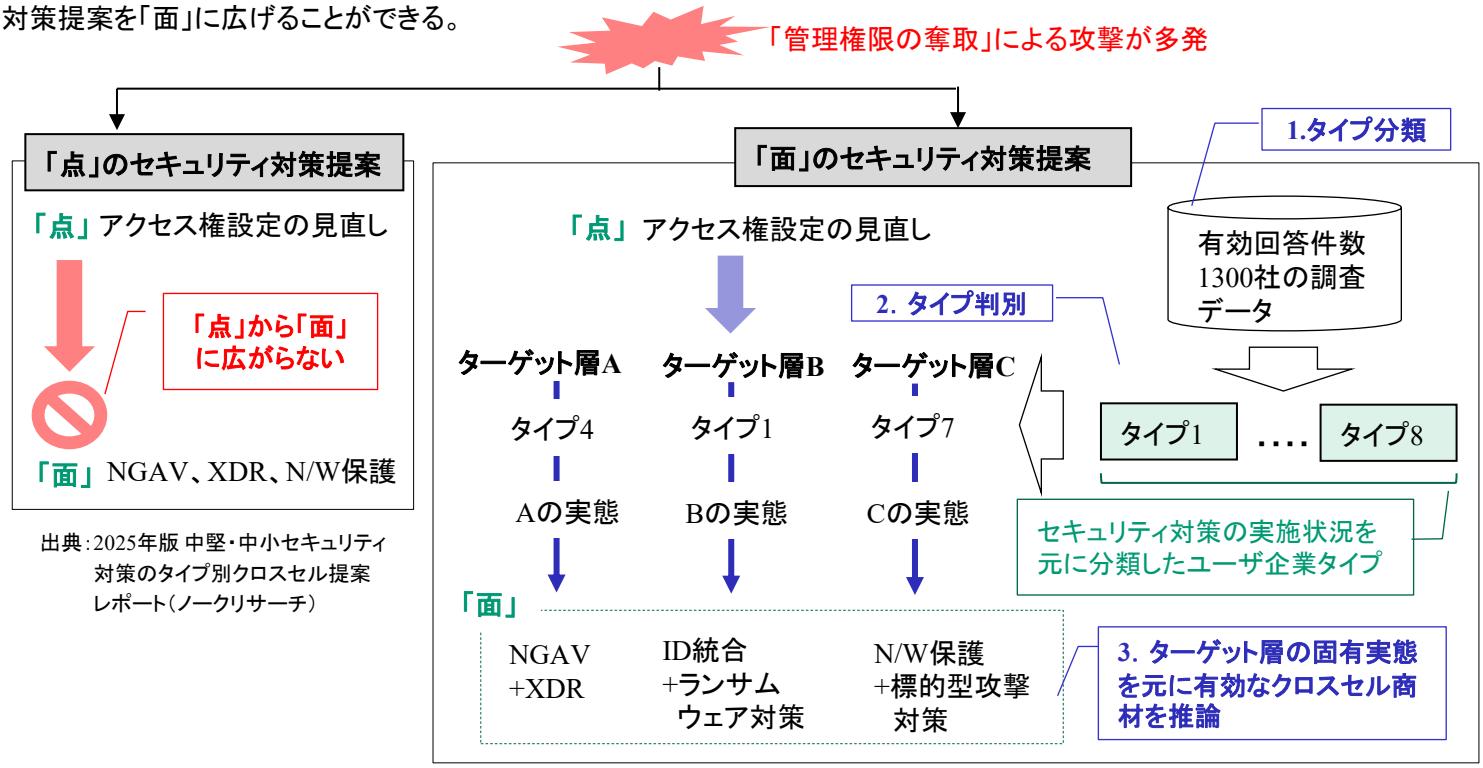
■「管理権限の奪取」への危機感が高まっても、「出口対策」は後回しになりやすい点に注意

■「特権ID管理ツール」の有効なクロスセル商材は「XDRツール」と「アクセス回線の強化策」

インシデント対応策を一過性に終わらせず、セキュリティ商材のクロスセルにつなげていく

今後AIを活用した業務の自動化が進んでいけば、企業間のデータ連携も緊密になっていくと予想される。不正アクセスによるサプライチェーン/デマンドチェーン全体の障害を防ぐためにも、大企業のみならず中堅・中小企業におけるセキュリティ対策の強化が不可欠となってくる。例えば、中堅・中小企業に対する「管理権限の奪取」の攻撃が増えたとする。当然、下図の左側が示すようにアクセス権設定の見直しなどの対策が意識されることになるが、IT管理/運用の人員が限られる中堅・中小企業では「未知のマルウェアへの対処」（NGAV）、「出口対策」（XDR）、「ネットワーク保護」といった関連する他の対策を認知/検討するだけの余裕がない。また、IT企業側も多岐に渡るセキュリティ商材の中から何をクロスセルすべきか？の判断が難しい。

そこで有効となるのが、下図の右側が示すように「1. セキュリティ対策の実施状況を元にユーザ企業全体をタイプ分類する」、「2. IT企業が考えるターゲット層が該当するタイプを判別する」、「3. ターゲット層に固有の実態をタイプ毎の分析モデルにパラメータとして指定し、最適なクロスセル商材を推論する」といった手法だ。こうして従来は「点」だった中堅・中小向けセキュリティ対策提案を「面」に広げることができる。



出典：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（ノークリサーチ）

次頁以降では、最新の調査レポートを活用することで実現できる上図のような「点」から「面」に広がるセキュリティ対策提案を具体例と共に解説/紹介していく。

本リリースの元となる「2025年版 中堅・中小セキュリティ対策のタイプ別シナリオ提案レポート」ではレポートを購入したIT企業毎に個別の分析/提言を提供するセミカスタムレポート形式を採用している。以降では、とあるセキュリティベンダD社における同レポートの活用を具体例として、前頁で示した「点」から「面」へのセキュリティ対策提案の実践例を紹介する。

【具体例の背景】

大手セキュリティベンダD社では「管理権限の奪取」による中堅・中小企業への攻撃が増加するという見通しを踏まえて、中堅・中小向け特権ID管理ツールの販売を開始した。だが、そこから他の商材へのクロスセルが進まないという課題を抱えていた。

【ステップ1:ターゲット層のインプット】

まず、D社はノークリサーチから提供される以下の「インプットシート」に●を付ける形で、クロスセルの主要な訴求対象としたい企業層を指定する。ここでは年商や業種だけでなく、セキュリティ対策の実施内容も確認する。(以下の例が示すように不明な属性は未チェックのままでも構わない)

D社の場合はセキュリティ商材を訴求したいターゲット層を複数抱えていたが、まずは「管理権限の奪取」の事案が目立つ以下の企業層を分析対象として選択した。(「従業員数」や「ビジネス拠点の状況」も指定すれば、更にタイプ判定の精度が上がる)

年商: 100億円以上～300億円未満　　**業種**: 小売業　　**所在地**: 近畿地方

またインプットシートではセキュリティ対策の実施状況を6つの視点で尋ねている。例えば、「エンドポイント(社内)」は社内で利用するエンドポイント環境(PCなど)のセキュリティ対策の実施内容(手段)を指す。パッケージのマルウェア対策ツールを導入している場合は「パッケージ」を選ぶ。これらの項目は把握している範囲で指定すれば十分だが、D社はターゲット層の状況を比較的把握できていたため、以下のように指定した。

エンドポイント(社内):	パッケージ	**エンドポイント(社外)**:	サービス
サーバ/ストレージ(社内):	パッケージ	**サーバ/ストレージ(社外)**:	サービス
社外エンドポイントと社内の通信:	対策未実施	**クラウドサービスと社内の通信**:	対策未実施

インプットシート.xlsx

A1.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

A3.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

A4.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:

A5.所在地
○ 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

A6.IT管理/運用の人員規模
○ 兼任1名
○ 兼任2～5名
○ 兼任6～9名
○ 兼任10名以上
○ 専任1名
○ 専任2～5名
○ 専任6～9名
○ 専任10名以上
○ 社内常駐の外部人材に委託
○ 非常駐の外部人材に委託
○ ITの管理/運用は全く行っていない
○ その都度適切な社員が対応している
○ その他:

A7.ビジネス拠点の状況
○ 拠点は1ヶ所のみ
○ 2～5ヶ所の拠点があり、インフラは全拠点で統一的に管理
○ 2～5ヶ所の拠点があり、インフラは各拠点で個別に管理
○ 6ヶ所以上の拠点があり、インフラは全拠点で統一的に管理
○ 6ヶ所以上の拠点があり、インフラは各拠点で個別に管理
○ その他:

R1-1.守りのIT対策の実施内容(エンドポイント(社内))(複数回答可)
■ 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

R1-2.守りのIT対策の実施内容(エンドポイント(社外))(複数回答可)
□ 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

R1-3.守りのIT対策の実施内容(サーバ/ストレージ(社内))(複数回答可)
■ 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

R1-4.守りのIT対策の実施内容(サーバ/ストレージ(社外))(複数回答可)
□ 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

R1-5.守りのIT対策の実施内容(社外エンドポイントと社内の通信)(複数回答可)
□ 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

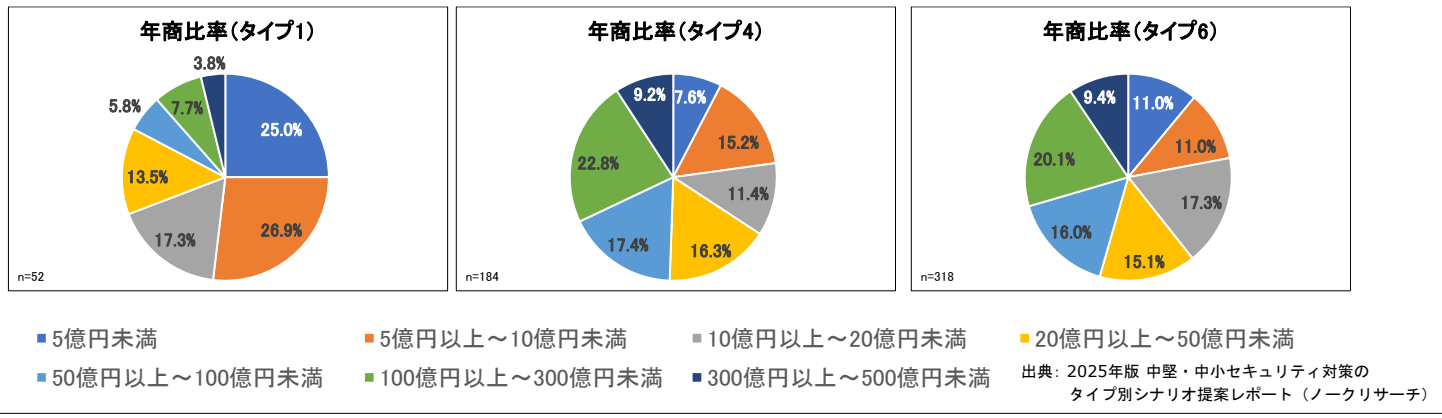
R1-6.守りのIT対策の実施内容(クラウドサービスと社内の通信)(複数回答可)
□ パッケージ
□ サービス
□ アウトソース
□ アプライアンス
□ H/Wの付属機能
□ OSの付属機能
□ 不明
■ 対策未実施
□ 該当なし

前頁で図示したように、調査レポートでは有効回答件数1300社に尋ねたセキュリティ対策の実施状況に関する調査データを元にユーザ企業全体をタイプ1～タイプ8の合計8つのタイプに分類している。次頁では上記のインプットシートを元にD社が指定したターゲット層がどのタイプに該当するか？について述べる。

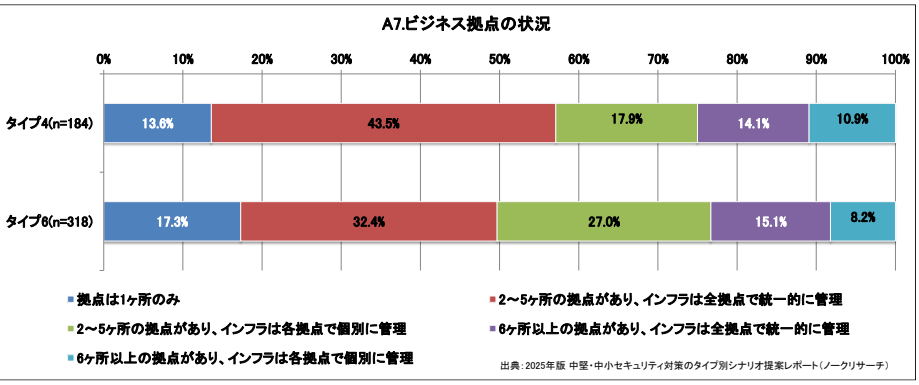
【ステップ2：ターゲット層タイプの判別】

インプットシートを元に、D社が提示したターゲット層がタイプ1～タイプ8のどれに最も近いか？を判別する。D社のターゲット層は「タイプ4」に該当する。以下のグラフはタイプ1、4、6に属するユーザ企業の年商構成比率を示したものだ。D社の訴求年商は100～300億円（緑部分）だが、該当するタイプ4はタイプ1と比べて同年商帯の比率が高いことが確認できる。

タイプ別の年商構成比率



出典：2025年版 中堅・中小セキュリティ対策のタイプ別シナリオ提案レポート（ノークリサーチ）



さらに左記のグラフはタイプ4と6のビジネス拠点の状況を比べたものだ。上記の円グラフが示すように年商構成比率では両者に大きな差異は見られない。だが、タイプ4はタイプ6と比べて、2～5箇所の拠点数においてインフラを統合管理している割合が高い。詳細は後述するが、この点がクロスセルの施策においても重要な留意点となってくる。

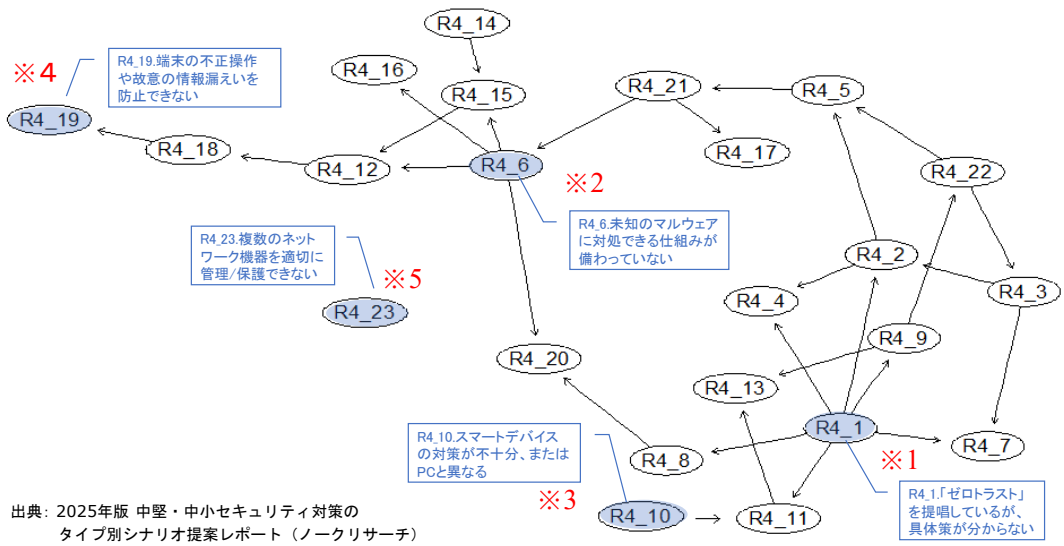
【ステップ3：分析モデルによる推論】

調査レポートでは8つのタイプ毎にベイジアンネットワーク分析を用いた分析モデルが用意されている。同分析モデルによってセキュリティ対策における様々な課題やニーズの関連性を視覚化し、ある課題/ニーズが顕著になった時、他の課題/ニーズがどう変化するか？を推論（予測）できる。右図はタイプ4の企業層がセキュリティ対策において抱く課題項目の関連性を示す分析モデルである。

ゼロトラスト（※1）や未知のマルウェア（※2）に関する課題は他の課題項目とも関連が深いことが右図から読み取れる。一方、スマートデバイス（※3）、端末の不正操作（※4）、ネットワーク管理（※5）は他の課題との関連が薄いため、手薄になりがちな領域であることも分かる。

次頁では右図の分析モデルを

タイプ4のセキュリティ対策における課題（タイプ4）



出典：2025年版 中堅・中小セキュリティ対策のタイプ別シナリオ提案レポート（ノークリサーチ）

を用いて、「管理権限の奪取」に関する課題が顕在化した時に何が起きるか？を明らかにしていく。

「管理権限の奪取」への危機感が高まっても、「出口対策」は後回しになりやすい点に注意

前頁の分析モデルで示されたセキュリティ対策における課題項目の一覧は以下の通りである。

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>>
- 「ゼロトラスト」を提唱しているが、具体策が分からない
- 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 ※1**
- **メールによる情報漏えい/誤送信の対策を講じていない ※2**

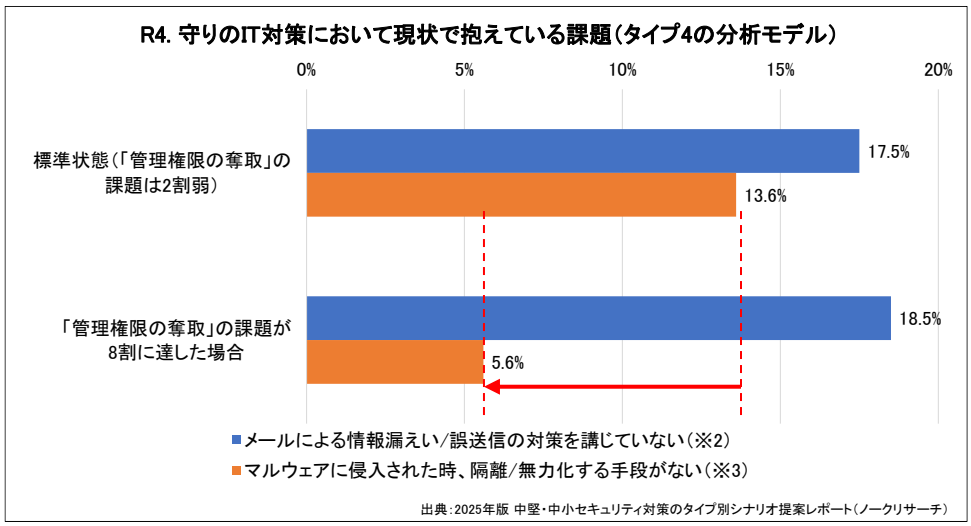
<<マルウェア対策>>
- 標的型攻撃の被害や危険性が十分に周知されていない
- 未知のマルウェアに対処できる仕組みが備わっていない
- **マルウェアに侵入された時、隔離/無力化する手段がない ※3**
- サーバ導入が必須、もしくは端末側の処理が重い/遅い
- 運用/保守のアクセス回線はマルウェア対策が不十分
- スマートデバイスの対策が不十分、またはPCと異なる

<<アカウント管理>>
- 特権/管理アカウントの悪用を防ぐ施策を講じていない
- 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
- 生体認証や多要素/二段階認証に対応できていない

<<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
- 保管した大量データを容易に検索/参照できない

<<運用管理/資産管理>>
- 端末の不正操作や故意の情報漏えいを防止できない
- OS更新の現状が把握できず、管理/制御もできない
- 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
- 複数のネットワーク機器を適切に管理/保護できない

以下のグラフは前頁の分析モデルにおいて、上記の「**管理権限が強いため、乗っ取られた時の被害が大きい**」(※1)の課題を挙げる割合が標準状態の2割弱から8割に高まった時、「**メールによる情報漏えい/誤送信の対策を講じていない**」(※2)および「**マルウェアに侵入された時、隔離/無力化する手段がない**」(※3)を課題と考える割合がどう変化するか？を示したものだ。



つまり、「管理権限の奪取」による攻撃が増加するなどして、※1に対する課題意識が高まると、タイプ4ではメール対策（※2）や出口対策（※3）に関連する課題意識も同時に高まるのか？を知ることができる。

左記のグラフを見ると、※1の課題が深刻になったとしても、※2に大きな変化はなく※3は逆に減少していることがわかる。

中堅・中小企業はIT管理/運用の人員も限られるため、特定のセキュリティ課題が発生した場合、その対応のみに集中してしまいやすい。上記の場合も多くのユーザ企業が既に実施しているメール対策は継続するものの、比較的新しい考え方である出口対策については後回しになっている。だが、入口対策と出口対策は双方を同時に進める必要があることは言うまでもない。

D社としては、まず自社のターゲット層に対して「管理権限の奪取」を防止するための入り口対策だけでなく、侵入したマルウェアを隔離/無力化する出口対策の必要性を啓蒙することが最初の取り組み事項となる。その上で、販売中の「中堅・中小向け特権ID管理ツール」とクロスセルすべき商材は何か？を探っていくことになる。次頁では、セキュリティ対策におけるニーズに関する分析によって上記の点を明らかにしていく。

「特権ID管理ツール」の有効なクロスセル商材は「XDRツール」と「アクセス回線の強化策」

前頁で述べた課題項目と対になる形で、調査レポートでは以下に列挙したセキュリティ対策におけるニーズ項目に基づく分析/提言も行っている。

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

<<セキュリティ全般>>
- ・具体策を例示しながら、「ゼロトラスト」を提案してくれる
- ・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 ※1**
- **・メールによる秘匿情報の漏えいや誤送信を防止できる ※3**

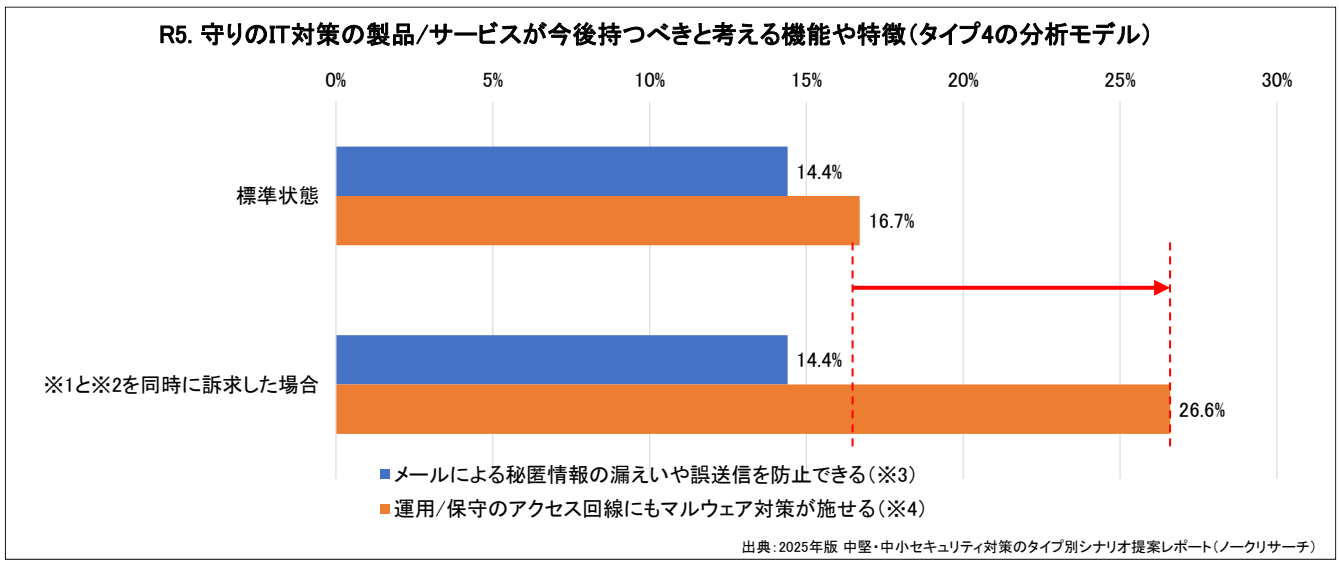
<<マルウェア対策>>
- ・標的型攻撃を想定した実地訓練サービスを利用できる
- ・異常な振る舞いを元に未知のマルウェアも検知できる
- **・侵入したマルウェアを封じ込めて隔離し、無力化する ※2**
- ・サーバや高性能な端末が不要なクラウド形態である
- **・運用/保守のアクセス回線にもマルウェア対策が施せる ※4**
- ・PCに加えてスマートデバイスも一括で管理/保護できる

<<アカウント管理>>
- ・特権/管理アカウントは運用条件を厳しく設定できる
- ・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
- ・生体認証または多要素/二段階認証に対応している

<<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
- ・検索/参照が容易な状態で大量データを保管できる

<<運用管理/資産管理>>
- ・端末の操作ログを記録して、不正や攻撃を防止できる
- ・OS更新の状況を可視化して、更新を自動で制御できる
- ・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
- ・複数のネットワーク機器を統合的に管理/保護できる

前頁の分析結果を踏まえて、D社は上記の※1と同時に※2の必要性も訴求することにした。その場合、※3と※4のニーズ項目にどのような変化が生じるか？を示した結果が以下のグラフである。



「中堅・中小向け特権ID管理ツール」（※1）と同時に出口対策を担う「XDRツール」（※2）も訴求すると、メール対策（※3）に変化は見られないが、「運用/保守のアクセス回線における対策」（※4）のニーズが高まることが確認できる。3ページで述べたようにタイプ4はタイプ6と比較して、2～5箇所の拠点数においてインフラを統合管理している割合が高い。したがって、アクセス回線の対策についても意識が高まりやすいと考えられる。このようにターゲット層のタイプを判別し、分析モデルを用いた課題とニーズの推論を行うことによって、D社の場合には**『中堅・中小向け特権ID管理ツールと共にXDRツールとアクセス回線の強化策を提供する』**という有効なクロスセル戦略を立案することができた。

次頁では本リリースの元となる調査レポートについて紹介している。

本リリースの元となる調査レポートのご案内

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）

本調査レポートは購入いただいたIT企業様毎に個別の分析/提言を提供するセミカスタムレポート形式を採用しています。

集計/分析には既に多くのご好評をいただいている以下の市販調査レポートのデータを用いています。

「2024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」（※）

https://www.norkresearch.co.jp/pdf/2024Sec_user_rep.pdf

・本調査レポートの購入に際して、（※）の市販調査レポートを事前に購入いただく必要はございません

・本リリースで紹介している分析/提言は（※）の市販調査レポートには含まれませんのでご注意ください

調査レポートの提供内容

ステップ1： 事前ヒアリングとターゲット層のインプット

調査レポートを購入いただいたIT企業様とのWeb会議を開催し、ノークリサーチから現状の課題/ニーズをヒアリングしながら、IT企業様にて本リリースの【ステップ1】（2ページ）で例示したターゲット層に関する「インプットシート」を記入いただく。

ステップ2： ターゲット層タイプの判別

ノークリサーチにて、本リリースの【ステップ2】（3ページ）で例示した分析を実施し、IT企業様のターゲット層がタイプ1～タイプ8のいずれに該当するかを判別する。同時に該当するタイプの概況（年商構成比率など）についても後述の調査報告書に記載する。

ステップ3： 分析モデルによる推論

IT企業様のターゲット層が該当するタイプの分析モデルを用いて、セキュリティ商材のクロスセル施策を分析/提言する。具体例は本リリースの【ステップ3】（3～5ページ）の通りである。

調査報告会：

調査報告書の内容を解説し、Q&Aに応じるWeb会議（60分、1回）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） 上記に列挙したステップ1～3の分析と提言を記載したもの
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） （納期は調査報告書の納品日を指し、調査報告会は納品後に日程調整の上で実施します）
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。

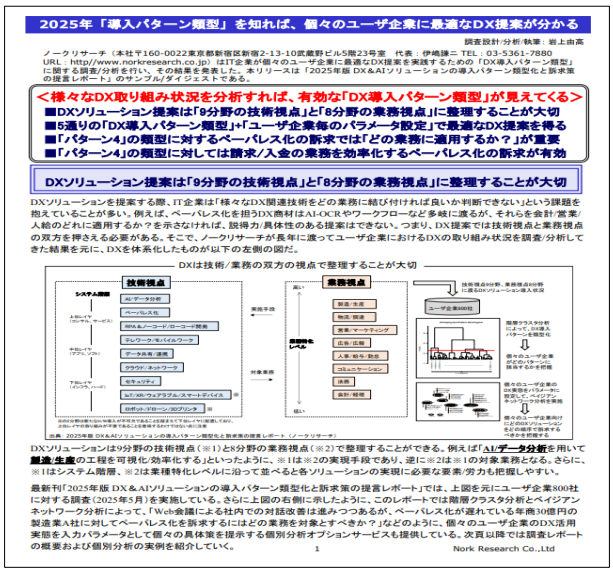
ご好評いただいている既存の調査レポート(1/2) 各冊225,000円(税別)

『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』

【レポートの概要と案内】 https://www.norkresearch.co.jp/pdf/2025DXAI_user_rep.pdf
【リリース(ダイジェスト)】

業種別の導入実態と課題に基づく「失敗しないDX提案」
https://www.norkresearch.co.jp/pdf/2025DXAI_user_rel5.pdf
IoTやロボットを活用したDXは「無理のない足元からの取り組み」が有効
https://www.norkresearch.co.jp/pdf/2025DXAI_user_rel3.pdf
ユーザ企業の生成AI活用状況と生成AIサービスの導入社数シェア
https://www.norkresearch.co.jp/pdf/2025DXAI_user_rel2.pdf

企業における生成AIサービス活用の市場規模と有望な適用場面
https://www.norkresearch.co.jp/pdf/2025DXAI_user_rel4.pdf
生成AIサービスが解決すべき課題と重要度の高いニーズ傾向
https://www.norkresearch.co.jp/pdf/2025DXAI_user_rel6.pdf
導入パターン類型が示すユーザ企業毎の最適なDX提案
https://www.norkresearch.co.jp/pdf/2025DXAI_user_rel1.pdf
ユーザの「無自覚課題」を顕在化する営業シナリオの作成方法
https://www.norkresearch.co.jp/pdf/2025DXAI_user_rel7.pdf



『2024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』

【レポートの概要と案内】 https://www.norkresearch.co.jp/pdf/2024itapp_rep.pdf
【リリース(ダイジェスト)】

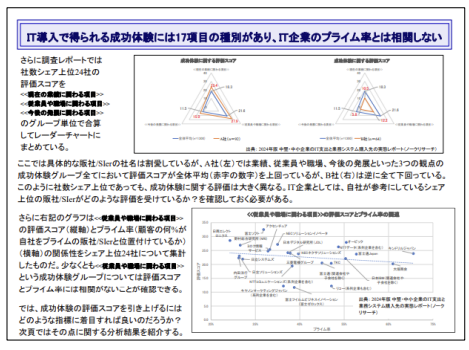
グループウェアやWeb会議を起点とした生成AIの普及の第一歩
https://www.norkresearch.co.jp/pdf/2024itapp_gw_rel.pdf
「コンポーザブルERP」は中堅・中小向けERP市場にも広まるか？
https://www.norkresearch.co.jp/pdf/2024itapp_erp_rel.pdf
中堅・中小向け会計管理パッケージと経費精算サービスの役割分担
https://www.norkresearch.co.jp/pdf/2024itapp_acc_rel.pdf
ワークフロー拡販に必要な視点は年商＆運用形態+ERP導入状況
https://www.norkresearch.co.jp/pdf/2024itapp_wf_rel.pdf
SaaSが中堅・中小向け生産管理システムにもたらす変化
https://www.norkresearch.co.jp/pdf/2024itapp_ppc_rel.pdf

販売・仕入・在庫管理はシェア差が縮小、CRM更新が新たな商機
https://www.norkresearch.co.jp/pdf/2024itapp_sbc_rel.pdf
勤怠管理を起点とした中堅・中小向け人事給与システムの進化
https://www.norkresearch.co.jp/pdf/2024itapp_hrw_rel.pdf
中堅・中小向けBI導入提案に不足している視点
https://www.norkresearch.co.jp/pdf/2024itapp_bi_rel.pdf
法整備や経済安全保障が中堅・中小生成AI活用に与える影響
https://www.norkresearch.co.jp/pdf/2024itapp_p0_rel.pdf
セールスフォース一強状態のCRM市場に変化は起きるか？
https://www.norkresearch.co.jp/pdf/2024itapp_crm_rel.pdf
文書管理・オンラインストレージサービス市場の新たな成長段階
https://www.norkresearch.co.jp/pdf/2024itapp_dm_rel.pdf

『2024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』

【レポートの概要と案内】 https://www.norkresearch.co.jp/pdf/2024SP_user_rep.pdf
【リリース(ダイジェスト)】

17種類に渡る「ユーザ企業における成功体験」から導かれるIT導入提案のキーポイント
https://www.norkresearch.co.jp/pdf/2024SP_user_rel1.pdf
中堅・中小企業における企業属性別(年商/業種/地域)＆商材別のIT支出市場規模
https://www.norkresearch.co.jp/pdf/2024SP_user_rel2.pdf
今後伸びるDX分野およびIT企業における成功体験スコアとDX比率の関係
https://www.norkresearch.co.jp/pdf/2024SP_user_rel3.pdf



ご好評いただいている既存の調査レポート(2/2)　各冊225,000円(税別)

『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』

【レポートの概要と案内】 https://www.norkresearch.co.jp/pdf/2024SrvPC_user_rep.pdf

【リリース(ダイジェスト)】

中堅・中小ハイブリッドクラウドの適用状況と解決すべき課題
https://www.norkresearch.co.jp/pdf/2024SrvPC_user_rel1.pdf

中堅・中小サーバ環境におけるクラウド移行とオンプレ回帰の実態
https://www.norkresearch.co.jp/pdf/2024SrvPC_user_rel2.pdf

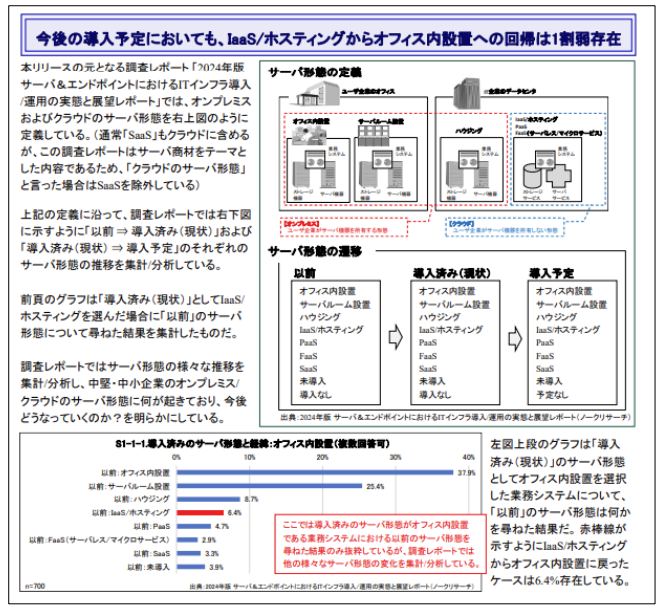
HCI(ハイパーコンバージドインフラ)の導入状況、社数シェア、導入障壁
https://www.norkresearch.co.jp/pdf/2024SrvPC_user_rel3.pdf

中堅・中小サーバ市場(オンプレミス＆クラウド)のシェア動向
https://www.norkresearch.co.jp/pdf/2024SrvPC_user_rel4.pdf

Windows 11への移行を阻害している要因とその打開策
https://www.norkresearch.co.jp/pdf/2024SrvPC_user_rel5.pdf

中堅・中小エンドポイント環境のOSと端末/サービスのシェア動向
https://www.norkresearch.co.jp/pdf/2024SrvPC_user_rel6.pdf

中堅・中小ストレージ環境の形態選択と活用課題の動向
https://www.norkresearch.co.jp/pdf/2024SrvPC_user_rel7.pdf



『2024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』

【レポートの概要と案内】 https://www.norkresearch.co.jp/pdf/2024RPA_user_rep.pdf

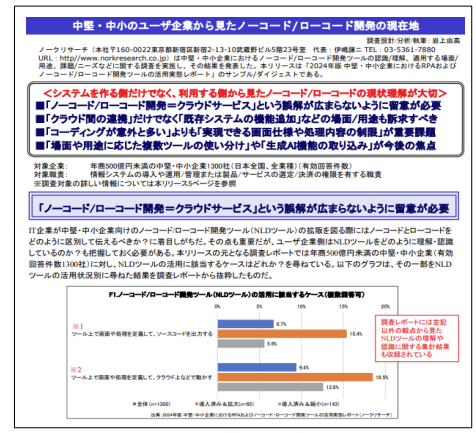
【リリース(ダイジェスト)】

ハイパーオートメーションを目指す取り組みがRPA市場の再活性化につながる
https://www.norkresearch.co.jp/pdf/2024RPA_user_rel1.pdf

RPAツールを適用する場面/用途と導入シェアが指し示す今後の要注力ポイント
https://www.norkresearch.co.jp/pdf/2024RPA_user_rel2.pdf

中堅・中小のユーザ企業から見たノーコード/ローコード開発の現在地
https://www.norkresearch.co.jp/pdf/2024RPA_user_rel3.pdf

ノーコード/ローコード開発ツールの活用状況、社数シェア、導入費用
https://www.norkresearch.co.jp/pdf/2024RPA_user_rel4.pdf



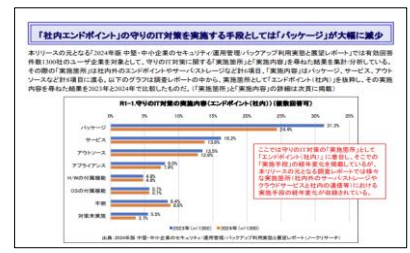
『2024年版 中堅・中小企業のセキュリティ/運用管理/バックアップ利用実態と展望レポート』

【レポートの概要と案内】 https://www.norkresearch.co.jp/pdf/2024Sec_user_rep.pdf

【リリース(ダイジェスト)】

中堅・中小企業のセキュリティ課題＆ゼロトラスト導入とDX推進および生成AI活用の関係性
https://www.norkresearch.co.jp/pdf/2024Sec_user_rel1.pdf

中堅・中小企業におけるセキュリティ対策の実施手段、ベンダ選択、支出額の変化
https://www.norkresearch.co.jp/pdf/2024Sec_user_rel2.pdf



本データの無断引用・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: http://www.norkresearch.co.jp/policy/index.html

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
Nork Research Co.,Ltd