PRESS RELEASE（報道関係者各位）

2022年2月21日

中堅・中小企業のセキュリティ対策ニーズをエンドポイントからサーバ/ネットワークに広げる施策

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：伊嶋謙ニ TEL：03-5361-7880
URL：http//www.norkresearch.co.jp）はランサムウェア攻撃やコロナ禍に伴う在宅勤務などの影響を踏まえた上で、エンドポイントが中心だった中堅・中小企業のセキュリティ対策をサーバ/ネットワークまで拡大していくためには何が必要か？に関する調査を行い、その分析結果を発表した。本リリースは「2021年版 中堅・中小企業のセキュリティ・運用管理・バックアップに関する今後のニーズとベンダ別導入意向レポート」のサンプルならびにダイジェストである。

＜「効果的な事由/背景」と「有望なユーザ企業像」を知ることがセキュリティ商材拡大の最短経路＞

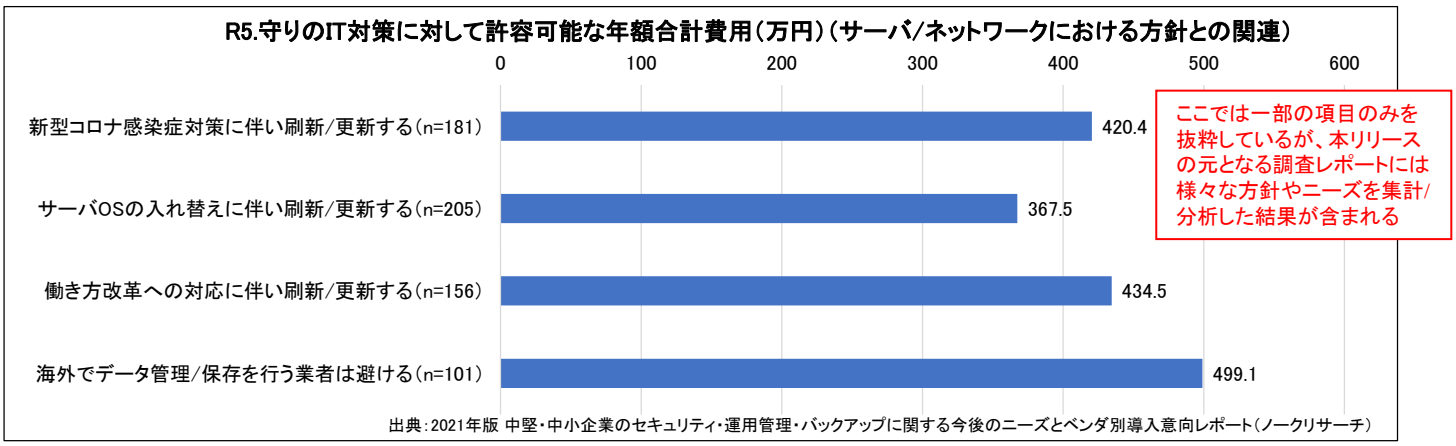
■海外でのデータ管理/保存を避けるユーザ企業では守りのIT対策における支出額が高い
■ZTNAに代表されるVPNの代替手段は中小企業層においても今後のニーズが期待できる
■DXを見据えたセキュリティ対策提案では「BCP策定」よりも「ゼロトラスト」を起点とすべき

対象企業：　年商500億円未満の中堅・中小企業1300社（日本全国、全業種）（有効回答件数）
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/決済の権限を有する職責
調査期間：　2021年6月～7月
※調査対象の詳しい情報については本リリースの末尾を参照

海外でのデータ管理/保存を避けるユーザ企業では守りのIT対策における支出額が高い

中堅・中小企業におけるセキュリティ対策は依然としてPCなどのエンドポイントが主体となっている。しかし、昨今増加している企業を狙ったランサムウェア攻撃への対処や依然として続くコロナ禍に起因する在宅勤務においてはサーバやネットワークを含めた包括的なセキュリティ対策が不可欠となる。ベンダや販社/SIerがセキュリティ対策の提案をエンドポイントからサーバ/ネットワークへと拡大していくためには、まず最初に「効果的な事由/背景」や「有望なユーザ企業像」を見出す必要がある。

以下のグラフは年商500億円未満の中堅・中小企業に対し、セキュリティ/運用管理/バックアップといった守りのIT対策を担う製品/サービスに拠出可能な年額合計費用を尋ね、その結果をサーバ/ネットワークの守りのIT対策に取り組む事由や背景を軸として集計したものだ。サーバOSの入れ替えといった更新需要よりも働き方改革や新型コロナ対策を事由/背景とした提案の方が多くの支出額を見込めることがわかる。また、データの置き場所を意識するユーザ企業ではさらに高い支出額が期待できる。したがって、ベンダや販社/SIerがサーバ/ネットワークも含めたセキュリティ対策の拡充を図る際には更新需要だけに頼らず、データの置き場所を意識するユーザ企業に優先的にアプローチする取り組みが有効と考えられる。



本リリースの元となる調査レポートでは中堅・中小企業におけるセキュリティ対策をエンドポイントからサーバ/ネットワークへと拡大するためには何が必要か？を分析し、ベンダや販社/SIerが取り組むべき今後の施策を提言している。次頁以降ではその一部をサンプル/ダイジェストとして紹介している。

ZTNAに代表されるVPNの代替手段は中小企業層においても今後のニーズが期待できる

本リリースの元となる調査レポートでは以下のような項目を列挙して、サーバ/ネットワークのセキュリティ対策に関する方針やニーズを尋ねている。

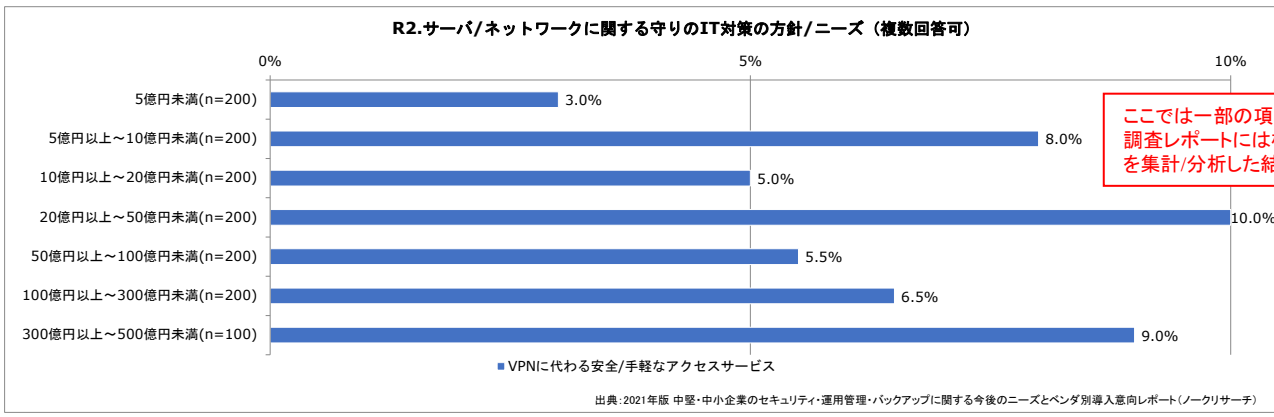
<<方針に関する項目>>

・製品/サービスを特定のベンダに集約していく	例） サーバのセキュリティとバックアップについては、同じベンダの製品/サービスで統一する
・複数ベンダの製品/サービスを適宜使い分ける	例） ファイアーウォールとスパムメール対策は各分野でシェア首位の製品/サービスを利用する
・新型コロナ感染症対策に伴い刷新/更新する	例） 継続的な在宅勤務を前提として、社外からのリモートアクセスを大幅に見直す
・サーバOSの入れ替えに伴い刷新/更新する	例） サーバOSのサポート終了に伴って業務システムもバージョンアップする
・海外でデータ管理/保存を行う業者は避ける	例） データセンタが海外に置かれたクラウドサービスは利用しないようにする
・働き方改革への対応に伴い刷新/更新する	例） 外出中も社外から業務を行えるように業務システムをクラウドへ移行する
・親会社や取引会社からの要請で刷新/更新する	例） 親会社の業務システム指針に従って、販売管理をクラウドへ移行する
・BCP(事業継続計画)の策定に伴い刷新/更新する	例） 災害発生時のデータ保護のため、サーバのバックアップ対策を刷新する
・「ゼロトラスト」の考え方に沿って刷新/更新する	例） LAN内も安全とは考えず、不正な通信を検知/遮断する仕組みを導入する

<<ニーズに関する項目>>

・個人宅と社内を安全/手軽に接続できる仕組み	例） オフィス側の機器設置のみで利用できるリモートVPNサービスを導入する
・社内のサーバを個人宅から管理できる仕組み	例） IT管理担当者がブラウザで操作できるサーバ管理ツールを利用する
・社内とクラウドの双方を統合管理する仕組み	例） 社内とクラウド上の双方のサーバを統合管理できるツールを利用する
・VPNに代わる安全/手軽なアクセスサービス	例） クラウド経由で社内外のシステムをWebで利用できるサービスを利用する
・Webフォーム画面の乗っ取りを防ぐ仕組み	例） Webフォームの動作に異常がないかをチェックできるツールを利用する
・大手キャリアが提供する5G回線網での防御	例） 通信モジュール（SIMカード）の不正な交換を検知するツールを利用する
・特定業者が提供するローカル5Gでの防御	例） ローカル5Gでの不正なデバイス接続を監視/遮断するツールを利用する
・IoT機器を対象としたセキュリティ対策	例） IoT機器向けのマルウェア対策ツールを利用する
・システムの脆弱性を診断するサービス	例） ECサイトに疑似的に不正アクセスして診断するサービスを利用する
・不正アクセスの防護壁となるサービス	例） WAF（Web Application Firewall）のクラウドサービスを利用する
・データ保護における非IT機器とIT機器の連携	例） 製造装置のデータをインターネットを介して安全に共有する
・トラブル発生後の対策を自動化する仕組み	例） サーバの故障個所をWeb経由で通知するサービスを利用する
・不正アクセス発生後の被害拡大を防ぐ対策	例） 社内から社外への疑わしい通信を遮断する仕組みを利用する
・災害時に業務を継続するための仕組み	例） 遠隔地に待機用のサーバ環境を構築できるサービスを利用する

調査レポートには上記に列挙した方針/ニーズを年商、業種、従業員数、地域、IT管理/運用の人員規模、ビジネス拠点の状況といった様々な属性別に集計したデータが含まれる。例えば、以下のグラフは「VPNに代わる安全/手軽なアクセスサービス」のニーズを尋ねた結果を年商別に集計したものだ。



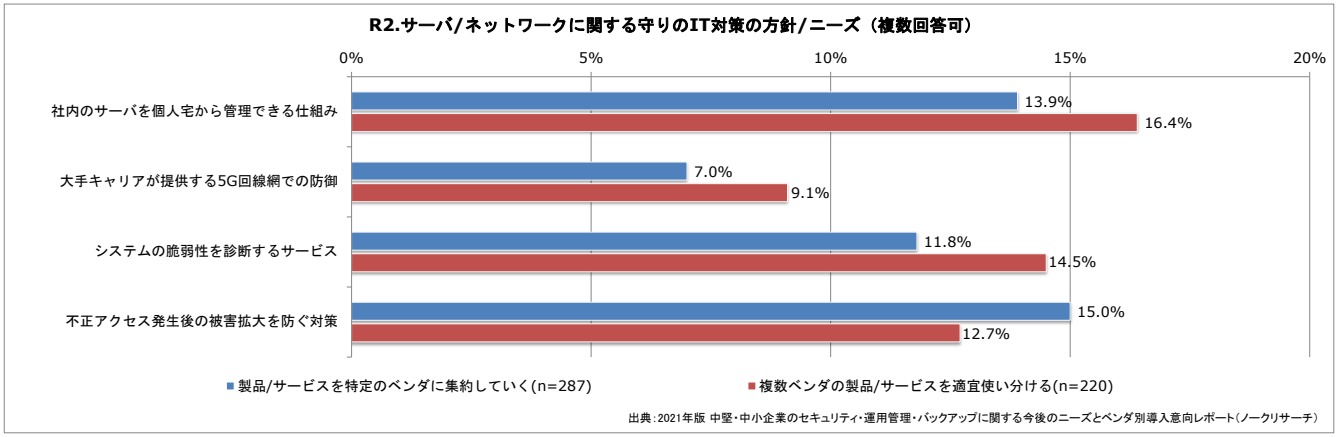
ここでは一部の項目を抜粋しているが、調査レポートには様々な方針やニーズを集計/分析した結果が含まれる

グラフが示すように現時点の回答割合はまだ低いものの、ZTNA（Zero Trust Network Access）に代表されるVPNの代替手段は年商50～500億円の中堅企業層だけでなく、年商5～50億円の中小企業層に対しても今後のニーズが期待できる。（次頁へ続く）

DXを見据えたセキュリティ対策提案では「BCP策定」よりも「ゼロトラスト」を起点とすべき

さらに、本リリースの元となる調査レポートではサーバ/ネットワークのセキュリティ対策における方針とニーズの関係性も分析している。以下のグラフは前頁に列挙した選択肢のうち、以下の4項目をベンダ選定の方針別に集計した結果である。

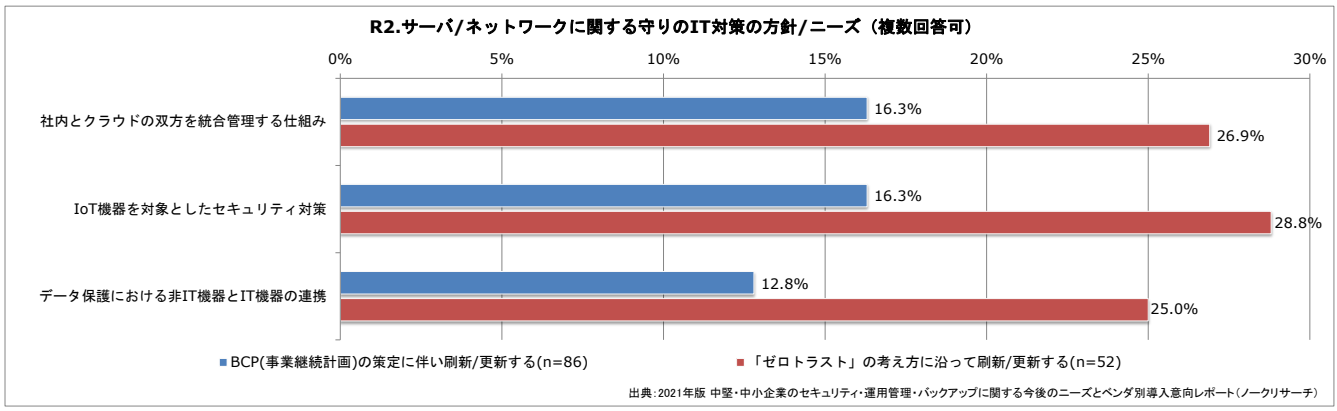
- ・社内のサーバを個人宅から管理できる仕組み（※1）　例） IT管理担当者がブラウザで操作できるサーバ管理ツールを利用する
- ・大手キャリアが提供する5G回線網での防御（※2）　例） 通信モジュール（SIMカード）の不正な交換を検知するツールを利用する
- ・システムの脆弱性を診断するサービス（※3）　例） ECサイトに疑似的に不正アクセスして診断するサービスを利用する
- ・不正アクセス発生後の被害拡大を防ぐ対策 （※4）　例） 社内から社外への疑わしい通信を遮断する仕組みを利用する



グラフが示すように、ベンダを使い分ける方針のユーザ企業は集約する場合と比べてネットワーク関連のセキュリティ意識が高く（※1、※2）、予防措置にも前向き（※3）であることがわかる。一方、ベンダを集約する方針のユーザ企業は不正アクセスの事後対策への関心が高い（※4）。こうした方針の違いによるニーズ傾向を把握しておくことも大切だ。

また、中堅・中小企業に対してセキュリティ対策の拡充を促そうとする場合、パンデミック対策を含めた「BCP策定」に軸足を置くか？それともランサムウェア攻撃などを踏まえて「ゼロトラスト」を強調するか？も重要な選択だ。以下のグラフは前頁に列挙した選択肢から以下の3項目を抜粋して、BCP策定とゼロトラストのそれぞれを守りのIT対策の事由/背景とする場合に分けて集計したものだ。

- ・社内とクラウドの双方を統合管理する仕組み（※5）　例） 社内とクラウド上の双方のサーバを統合管理できるツールを利用する
- ・IoT機器を対象としたセキュリティ対策（※6）　例） IoT機器向けのマルウェア対策ツールを利用する
- ・データ保護における非IT機器とIT機器の連携（※7）　例） 製造装置のデータをインターネットを介して安全に共有する



※5、※6、※7はクラウドやIoTなど、DX時代に向けて今後の活性化が期待される領域に関する項目だ。いずれもBCP策定と比べてゼロトラストを事由/背景とする場合の方が高い値を示していることがわかる。そのため、ベンダや販社/SIerがDX時代を見据えたサーバ/ネットワークのセキュリティ対策を訴求する際には、BCP策定よりもゼロトラストを起点とした提案が有効と考えられる。

本リリースの元となる調査レポート

『2021版 中堅・中小企業のセキュリティ・運用管理・バックアップに関する今後のニーズとベンダ別導入意向レポート』

ランサムウェア攻撃やコロナ禍の在宅勤務などを踏まえて、エンドポイント中心の対策をサーバ/ネットワークやアプリケーションまで拡充するために必要な施策は何か？を1300社の調査結果を元に分析/提言

【レポート案内】サンプル属性、設問項目、試読版などの詳細

https://www.norkresearch.co.jp/pdf/2021Sec_usr_rep.pdf

【対象企業属性】(有効回答件数:1300社)

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(公共/自治体など)

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)

【分析サマリの概要】集計データにおける重要ポイントを解説し、ベンダや販社/SIerが今後注力すべきポイントを提言

第1章:本調査レポートの背景と構成
第2章:エンドポイントに関する守りのIT対策の方針/ニーズ
第3章:サーバ/ネットワークに関する守りのIT対策の方針/ニーズ
第4章:アプリケーション利用に関する守りのIT対策の方針/ニーズ
第5章:ベンダ別に見た時の守りのIT対策に関する導入意向
第6章:守りのITに対して許容できる年額の合計費用

【価格】 180,000円(税別)　　**【発刊日】** 2022年2月28日

ご好評いただいているその他の調査レポート

「2021年版中堅・中小向け5G/ネットワーク関連サービスの展望レポート」

ローカル5G、ゼロトラスト、エッジコンピューティングなどの新たなNW活用を普及させるためには何が必要か？
レポート案内: https://www.norkresearch.co.jp/pdf/2021NW_user_rep.pdf

「2021年版 中堅・中小企業の業務システム購入先のサービス/サポート評価レポート」

プライム率、導入効果、商材ポートフォリオとユーザ評価を照合分析し、DX時代の販社/SIer像を明らかにする
レポート案内: https://www.norkresearch.co.jp/pdf/2021SP_usr_rep.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