PRESS RELEASE（報道関係者各位）

2019年11月25日

2019年 中堅・中小サーバ/ネットワーク関連の守りのIT対策におけるニーズと支出

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・中小企業がサーバ/ネットワークの守りのIT対策に取り組む際のニーズと支出に関する調査を実施し、その結果を発表した。本リリースは「2019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」のサンプルおよびダイジェストである。

＜サーバ/ネットワークにおける守りのIT活用提案の機会はOSサポート終了だけではない＞

■今後のベンダ選定方針は「適宜使い分ける」よりも「集約する」と考えるユーザ企業が多い
■中堅・中小企業においても、「不正アクセスにおける事後対策の重要性」が広まりつつある
■5G、IoT、テレワーク/モバイルワークと関連付けた訴求が守りのIT対策の支出額を高める

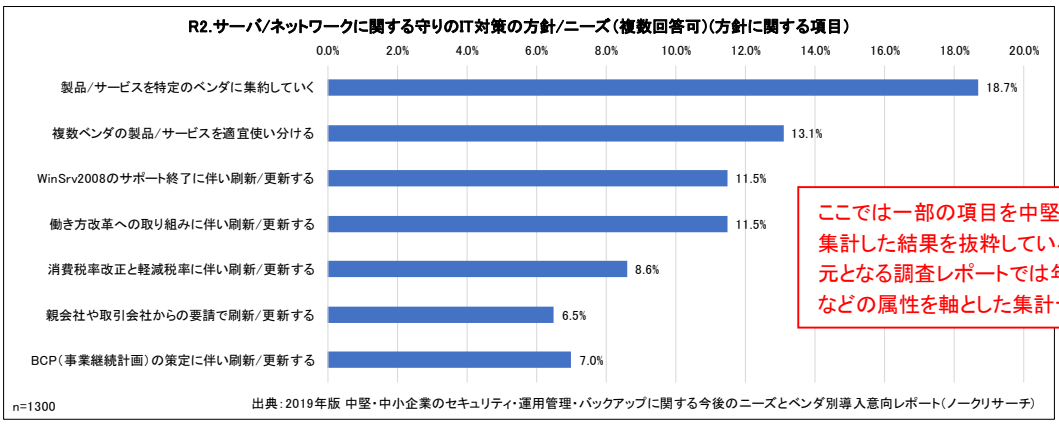
対象企業：　年商500億円未満の中堅・中小企業1300社（日本全国、全業種）（有効回答件数）
対象職責：　情報システムの導入や運用/管理または製品/サービスの選定/決済の権限を有する職責
※調査対象の詳しい情報については左記のレポート案内を参照　http://www.norkresearch.co.jp/pdf/2019Sec_usr_rep.pdf

今後のベンダ選定方針は「適宜使い分ける」よりも「集約する」と考えるユーザ企業が多い

本リリースの元となる調査レポート「2019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」では、エンドポイント（※）だけでなく、以下のようなサーバ/ネットワークに関する「守りのIT対策」についても詳しい集計/分析を行っている。（※　http://www.norkresearch.co.jp/pdf/2019Sec_usr_rel1.pdf　）

サーバのセキュリティ対策：	不正なプログラムやアクセス手法を用いたサーバへの攻撃を防ぐ
サーバのバックアップ対策：	サーバのプログラム、データ、設定情報などを複製して保管する
サーバの稼動監視：	サーバ機器やOSが正常に稼働し、障害/遅延がないかを監視する
ネットワークのセキュリティ対策：	不正なPCのLANへの接続やスイッチ/ルータへの攻撃などを防ぐ
ネットワークの稼動監視：	スイッチ/ルータが正常に稼働し、障害/遅延がないかを監視する
外部からの侵入の検知/防止：	外部と繋がるネットワーク機器を標的とした侵入/攻撃の防御

以下のグラフはサーバ/ネットワークの守りのIT対策に関する今後の方針を尋ねた結果の一部を年商500億円未満の中堅・中小企業全体で集計したものだ。（調査レポートには年商、従業員数、業種などの企業属性別に集計した結果が含まれる）



ここでは一部の項目を中堅・中小企業全体で集計した結果を抜粋しているが、本リリースの元となる調査レポートでは年商/従業員数/業種などの属性を軸とした集計データが含まれる

「製品/サービスを特定のベンダに集約していく」の回答割合が「複数ベンダの製品/サービスを適宜使い分ける」を上回っていることから、ベンダや販社/SIerとしては集約時に自社が選択されるようにサーバ/ネットワークの守りのIT対策における守備範囲を広げておくことが重要となってくる。また、同じ法制度に関する項目でも、働き方改革と消費税率改正/軽減税率では傾向に若干の差がある点に注意が必要だ。さらに親会社/取引会社の意向やBCP策定よりもOSサポート終了の方がサーバ/ネットワークの守りのIT対策に強く影響していることも確認できる。調査レポートではこうしたサーバ/ネットワークの守りのIT対策に関する傾向を様々な視点から分析している。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する。

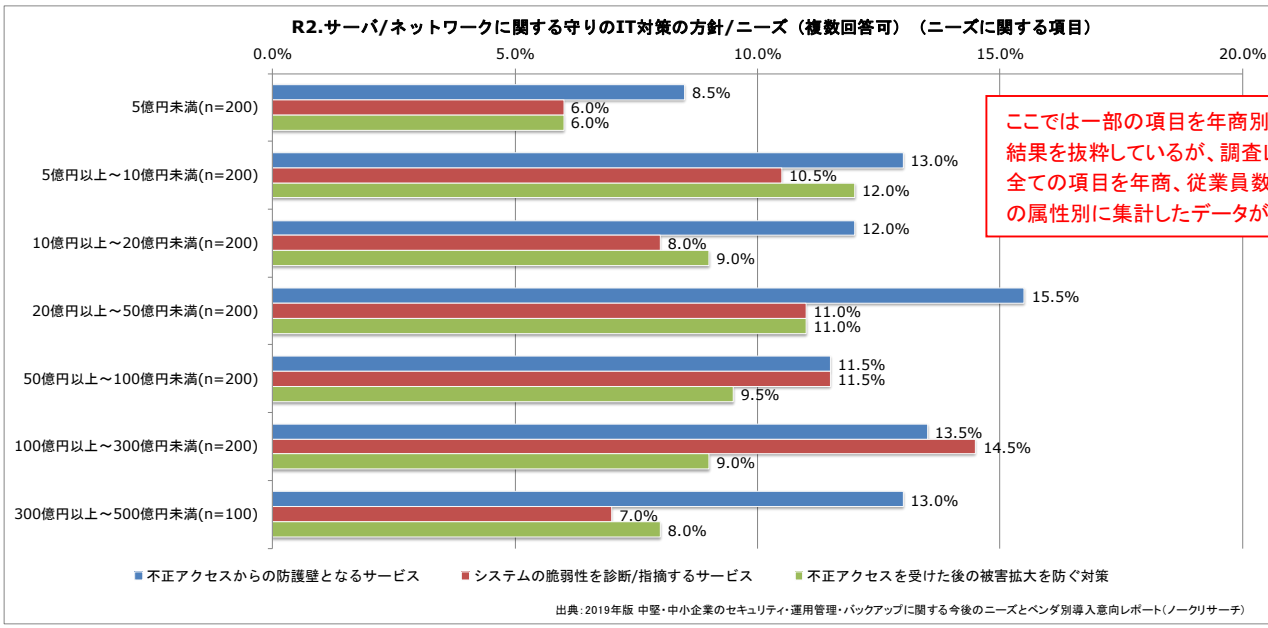
中堅・中小企業においても、「不正アクセスにおける事後対策の重要性」が広まりつつある

本リリースの元となる調査レポートでは以下に列挙した様々な選択肢を設けてサーバ/ネットワークの守りのIT対策に関する今後の方針やニーズを集計/分析している。

<<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
- 複数ベンダの製品/サービスを適宜使い分ける
- WinSrv2008のサポート終了に伴い刷新/更新する
- 働き方改革への取り組みに伴い刷新/更新する
- 消費税率改正と軽減税率に伴い刷新/更新する
- 親会社や取引会社からの要請で刷新/更新する
- BCP(事業継続計画)の策定に伴い刷新/更新する
- サーバ/ネットワーク機器の付属機能でカバーする
- 業務アプリケーションの付属機能でカバーする
- OS/ファームウェアの付属機能でカバーする
- 機器に負荷を与えないツールに入れ替える

<<ニーズに関する項目>>
- 5Gネットワーク対応に伴う守りのIT対策の更新/刷新
- IoTへの取り組みに伴う守りのIT対策の更新/刷新
- システムの脆弱性を診断/指摘するサービス（※）
- 不正アクセスからの防護壁となるサービス（※）
- 製造装置などIT以外の機器におけるデータ保護
- テレワーク/モバイルワークに向けたデータ保護
- 不正アクセスを受けた後の被害拡大を防ぐ対策（※）
- 実体ファイルが存在しない攻撃手法への対応
- 複数のIDやアカウントを統合管理できる仕組み
- 社内とクラウドの双方を統合管理できる仕組み
- 改正個人情報保護法やGDPRへの対応
- 災害時に業務を継続するための仕組み

前頁に掲載したグラフは上記の「方針に関する項目」の結果を中堅・中小企業全体で集計したものだ。さらに以下のグラフは「ニーズに関する項目」の中で（※）の付いたものを年商別に集計した結果である。



年商5億円未満の小規模企業ではいずれの項目も回答割合が1割未満に留まっている。小規模企業では「自社のような小さな企業が不正アクセスの標的になることはない」と考える経営層も少なくない。だが、実際は小規模企業のオンラインバンキングを標的とした不正送金などの被害も発生している。ベンダや販社/SIerとしては「小規模企業でも不正アクセスの標的となりうる」ことを地道に啓蒙していく取り組みも重要となってくる。

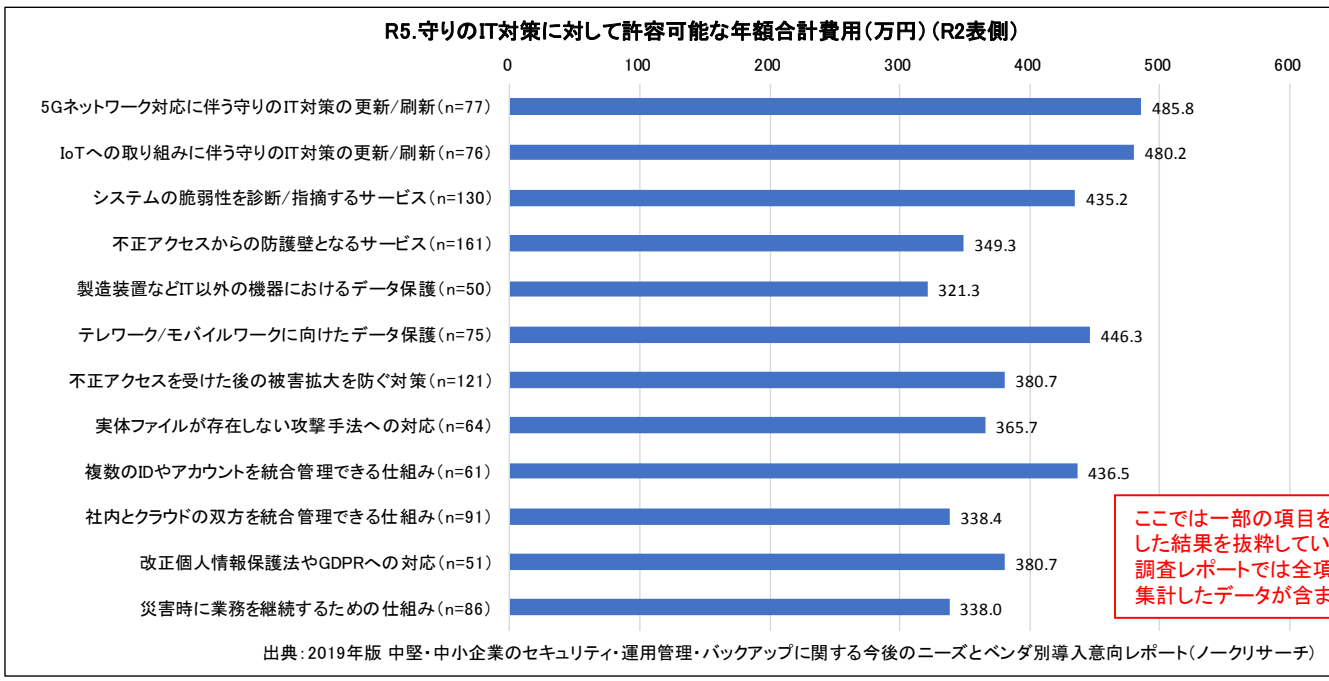
さらに年商5～500億円では年商規模が小さくなるにつれて、「不正アクセスを受けた後の被害拡大を防ぐ対策」の回答割合が徐々に高くなっている点にも注意する必要がある。不正アクセスにおける事後対策の重要性は標的型攻撃の認知などと共に中堅・中小企業にも認識されるようになってきた。そのため、年商規模の小さな企業層では不正アクセスの事後対策がまだ十分でないと考える企業が多い。ベンダや販社/SIerとしては中堅・中小企業でも無理なく導入できる不正アクセスの事後対策（例. 社外から社内のインバウンドだけでなく、社内から社外のアウトバウンドの制御/保護も手軽に行うことができるファイアーウォールなど）を提供することが重要となってくる。

5G、IoT、テレワーク/モバイルワークと関連付けた訴求が守りのIT対策の支出額を高める

ベンダや販社/SIerが守りのIT対策を訴求する際にはユーザ企業が想定する費用感を把握しておくことも大切となる。そこで、本調査レポートでは守りのITに対して拠出可能な年額合計費用（万円）を数値記入形式で尋ねている。（ハードウェアとOS/ファームウェア関連の費用は除外し、セキュリティ/運用管理/バックアップを担うソフトウェアの製品/サービスを利用する上で許容できる年額の合計費用を記入する形式となっている）

ここでは詳細は割愛するが、調査レポートでは年商別、従業員数別、業種別に集計した「拠出可能な年額合計費用」の分析を行っている。さらにベンダや販社/SIerにとっては「守りのIT対策に対して許容可能な年額合計費用が高めのユーザ企業はどのような方針/ニーズを抱いているのか？」を把握することも重要だ。

そこで、前頁に列挙した「サーバ/ネットワークに関する守りのIT対策のニーズ項目」毎に「守りのIT対策に対して許容可能な年額合計費用（万円）」を集計した結果が以下のグラフである。以下のグラフに示された数値は個々の選択肢の導入/利用に要する年額合計費用とは異なる点に注意が必要だ。だが、数値の高い項目があった場合、その選択肢を選んだユーザ企業をサーバ/ネットワークにおける守りのIT対策の訴求対象とすれば、高めの支出を期待することができる。



守りのIT対策に対して許容できる年額合計費用が400万円以上となっているユーザ企業が取り組み意向を示しているサーバ/ネットワーク管理の守りのIT対策は以下の通りである。

「5Gネットワーク対応に伴う守りのIT対策の更新/刷新」
「IoTへの取り組みに伴う守りのIT対策の更新/刷新」
「システムの脆弱性を診断/指摘するサービス」
「テレワーク/モバイルワークに向けたデータ保護」
「複数のIDやアカウントを統合管理できる仕組み」

上記の結果を見ると、5G、IoT、テレワーク/モバイルワークといったように比較的新しいIT活用に関連した選択肢が目立つ。いずれも新規のIT支出となることで守りのIT対策の金額も高くなると考えられるが、実際にはこれらの守りの項目に対する取り組み意向の割合も合わせて考慮する必要がある。本リリースの元となる調査レポートではそうした観点も含めて、OSのサポート終了対策だけに依存しないサーバ/ネットワークの守りのIT対策の訴求/提案に関する提言を述べている。

本リリースの元となる調査レポート

『2019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』

エンドポイント、サーバ/ネットワーク、アプリケーションの3つの分野における守りのIT対策の方針/ニーズを網羅すると共に、合計32社に渡るベンダの導入意向との関連を分析し、中堅・中小向けのセキュリティ、運用管理、バックアップの訴求ポイントを解説

【レポート案内】 http://www.norkresearch.co.jp/pdf/2019Sec_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などを提言。

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】** 2019年12月2日

ご好評いただいているその他の調査レポート

「2019年版 中堅・中小IT活用シーン別クラウド導入の実態/予測レポート」

働き方改革、IoT、AR/VR、ウェアラブルなどのIT活用基盤として、クラウドはどこまで浸透するのか？
レポート案内: http://www.norkresearch.co.jp/pdf/2019Cloud_user_rep.pdf

「2019年版 中堅・中小向け通信/ネットワーク関連サービスのニーズ予測レポート」

5G、LPWA、リモートアクセス、音声/データ統合などのネットワーク導入とDX時代のITソリューションとの関連を分析
レポート案内: http://www.norkresearch.co.jp/pdf/2019NW_user_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

NORK RESEARCH