

2019年 エンドポイントのセキュリティ/運用管理/バックアップ対策のニーズ展望

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）は中堅・中小企業におけるエンドポイントのセキュリティ/運用管理/バックアップ対策の
ニーズ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。

<中堅・中小企業のエンドポイントにおける守りのIT対策は2020年以降に変化する>

- エンドポイントの守りのIT対策では「WaaS対応」や「不正アクセスの事後対策」が優先課題
- 有償の製品/サービス導入を伴ったエンドポイント対策意向は従業員数50～100人で高い
- バックアップではベンダの集約に要注意、セキュリティや運用管理では働き方改革も有効

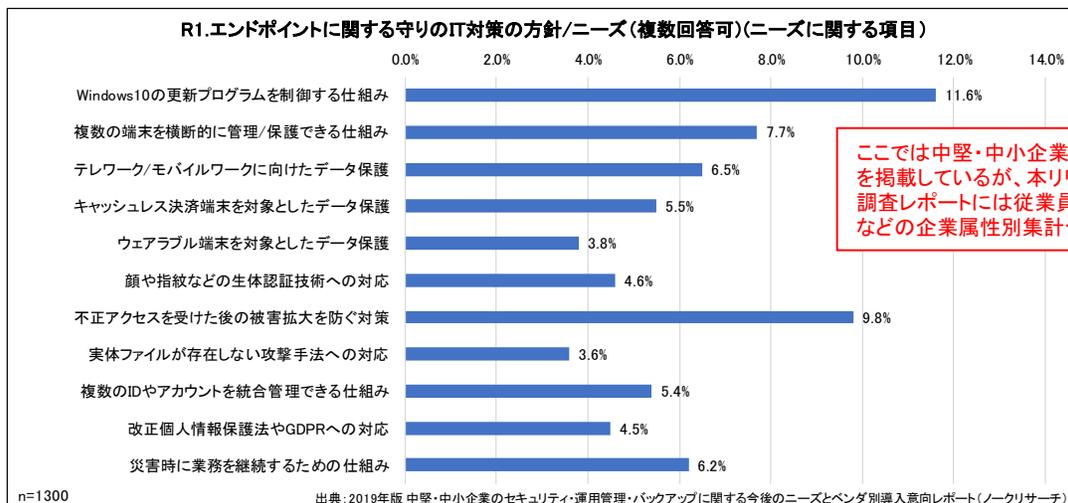
対象企業： 年商500億円未満の中堅・中小企業1300社（日本全国、全業種）（有効回答件数）

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

エンドポイントの守りのIT対策では「WaaS対応」や「不正アクセスの事後対策」が優先課題

大企業だけでなく、中堅・中小企業においてもセキュリティ、運用管理、バックアップといった守りのIT対策は不可欠の取り組みとなっている。だが、ユーザ企業が「守りのIT対策をできるだけ手軽/簡潔に行いたい」と考える一方、セキュリティ、運用管理、バックアップの製品/サービスが個別に提供されているケースも依然として多い。ベンダや販社/SIerとしては一歩高い視点から中堅・中小企業が必要とする守りのIT対策とは何か？を理解することが大切だ。2020年にはWindows 7 のサポートが終了し、Windows 10移行に伴うエンドポイント管理に注目が集まると予想される。そこで、年商500億円未満の中堅・中小企業に対してエンドポイント(PCやスマートデバイス)の守りのIT対策において「有償でも利用したいと考える製品/サービス」を尋ねた結果が以下のグラフである。（本リリースの元となる調査レポートでは、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つの領域における守りのIT対策ニーズを従業員数、年商、業種などの企業属性別に集計したデータが含まれる）



中堅・中小企業における守りのIT対策では「外部からの攻撃をツールで防ぐ」という考え方が比較的多い。だが、標的型攻撃に代表されるように、昨今では単にツールを導入するだけでは対処が難しくなっている。そうした状況を反映し、上記のグラフが示すように「不正アクセスを受けた後の被害拡大を防ぐ対策」といった事後対処にも着目するユーザ企業が出てきている。また、「Windows10の更新プログラムを制御する仕組み」が最も高い回答割合を示していることからわかるように、今後は中堅・中小企業においてもWaaS(Windows as a Service)への対応が重要となり、エンドポイント管理全体に大きな影響を及ぼす可能性も十分予想される。次頁以降ではこうした分析結果の一部をサンプル/ダイジェストとして紹介している。

有償の製品/サービス導入を伴ったエンドポイント対策意向は従業員数50～100人で高い

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、以下に列挙した様々な選択肢を設けてエンドポイントの守りのIT対策に関する動向を集計/分析している。

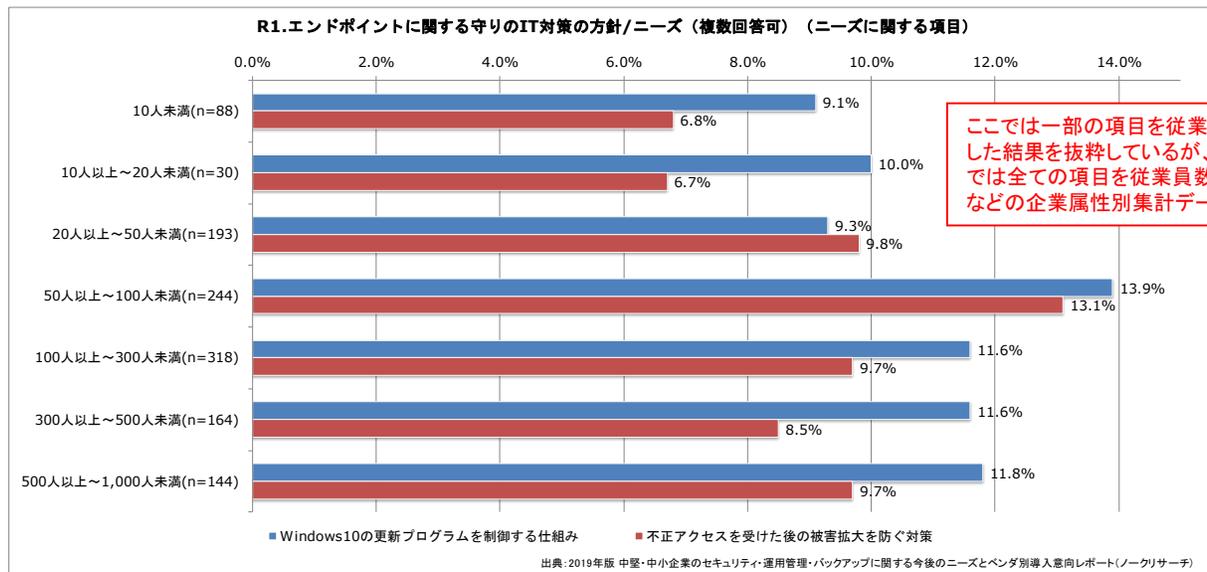
<<方針に関する項目>>

- ・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
- ・Windows 7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
- ・PCやスマートデバイス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
- ・端末内にデータを保存しない形態へ移行する
- ・端末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>>

- ・Windows10の更新プログラムを制御する仕組み
- ・複数の端末を横断的に管理/保護できる仕組み
- ・テレワーク/モバイルワークに向けたデータ保護
- ・キャッシュレス決済端末を対象としたデータ保護
- ・ウェアラブル端末を対象としたデータ保護
- ・顔や指紋などの生体認証技術への対応
- ・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
- ・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「ニーズに関する項目」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冒頭のグラフで回答割合の高かった2つの項目を従業員数別に集計した結果である。(ここでは従業員数1000人未満の7区分の結果のみを抜粋している)



いずれの従業員数区分においても、「Windows10の更新プログラムを制御する仕組み」の回答割合が「不正アクセスを受けた後の被害拡大を防ぐ対策」を上回っており、WaaS対応が中堅・中小企業にとって優先度の高い取り組み事項となっていることが確認できる。

また、エンドポイントにおける守りのIT対策ニーズは従業員数が多くなるにつれて高くなるのが一般的だ。だが、上記のグラフを見ると、「Windows10の更新プログラムを制御する仕組み」と「不正アクセスを受けた後の被害拡大を防ぐ対策」のいずれにおいても回答割合が最も高いのは従業員数50～100人の企業層である。従業員数が多い企業では守りのIT対策を担う人員や予算も多いため、既に対策を実施しているケースも多い。一方、従業員数が少ない企業ではPC台数も少ないため手作業での対応する場合もある。その結果、従業員数では中間的な位置付けとなる従業員数50～100人においてWaaS対応や不正アクセスの事後対策における製品/サービスの導入ニーズが高くなっていると考えられる。

バックアップではベンダの集約に要注意、セキュリティや運用管理では働き方改革も有効

さらに本リリースの元となる調査レポートでは合計32社に渡る守りのITに関連するソフトウェア製品/サービスを自社で開発しているベンダやSIerを列挙し、それらの導入意向を尋ねている。

セキュリティパッケージ主体: トレンドマイクロ、シマンテック、マカフィー、キヤノンITソリューションズ、カスペルスキー、ソースネクスト、エフ・セキュア、FFRI

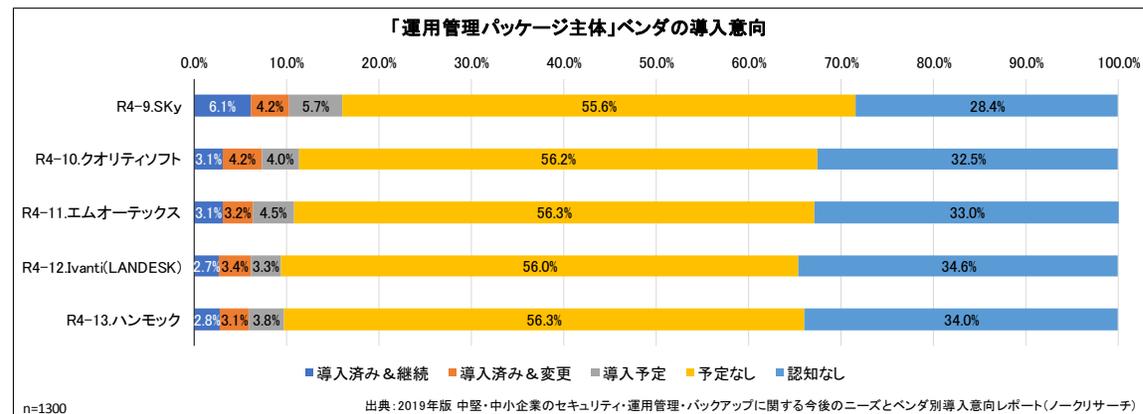
運用管理パッケージ主体: Sky、クオリティソフト、エムオーテックス、Ivanti (LANDESK)、ハンモック

バックアップパッケージ主体: ベリタステクノロジーズ、Arcserve、クエストソフトウェア、ストレージクラフト、ネットジャパン、アクロニス

その他のパッケージ主体: アルプスシステムインテグレーション、デジタルアーツ、ソリトンシステムズ

大手のITベンダ/SIer: 日立製作所、富士通、NEC、日本ヒューレット・パカード(HPE)、デル/EMCジャパン、シスコシステムズ、日本マイクロソフト、日本IBM、NTTデータ、野村総合研究所

以下のグラフは「運用管理パッケージ主体」ベンダの導入意向を尋ねた結果を中堅・中小企業全体で集計したものだ。(本リリースの元となる調査レポートには全ベンダの導入状況を従業員数別、年商別、業種別などで集計した結果が含まれる)



導入済み&継続:
既に導入しており、今後も利用を継続する

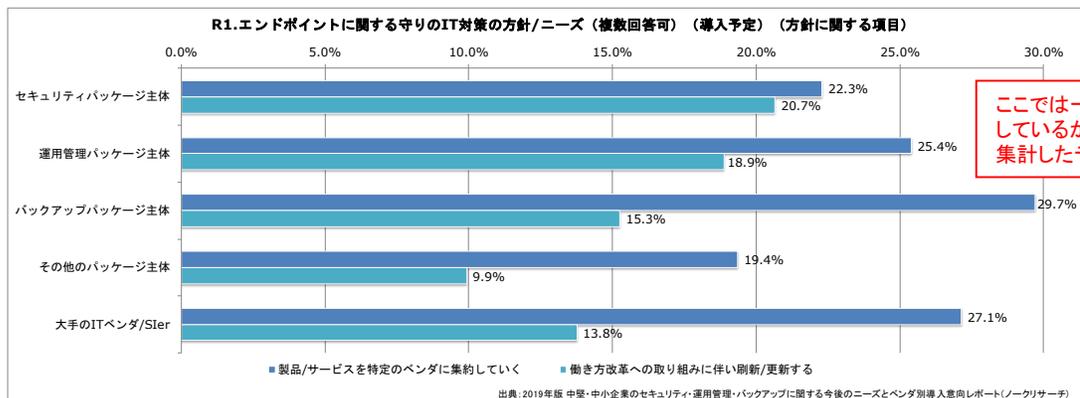
導入済み&変更:
既に導入しているが、今後は他社に変更する予定である

導入予定:
現時点では導入していないが、導入する予定である

予定なし:
現時点では導入しておらず、今後も導入する予定はない

認知なし:
該当するベンダを知らない

前頁で述べたWaaS対応に対するニーズの高まりは運用管理パッケージを主体とするベンダにとって市場拡大の大きな機会となる。だが、上記のグラフが示すように大企業と比べて中堅・中小企業における理解や認知はまだ高くない。まずは運用管理製品/サービスの啓蒙を進めることが重要な取り組みとなってくる。さらに、以下のグラフは上記に列挙した5つのベンダ区分毎に「導入予定」と回答した企業に対してエンドポイントの守りのIT対策における方針を尋ねた結果の中から、「ベンダの集約」と「働き方改革」に関連する結果を抜粋したものだ。(調査レポートには全ての項目をベンダ別に集計した結果が含まれる)



ここでは一部の項目を集計した結果を抜粋しているが、調査レポートでは全ての項目を集計したデータが含まれる

上記のグラフを見ると、「バックアップについてはベンダを集約しようとする志向が強い」ため、バックアップ主体のベンダとしては「統合パッケージなどに顧客を奪われないように注意する必要がある」や「セキュリティや運用管理では働き方改革と関連付けた訴求策が有効」などといった留意事項を読み取ることができる。本リリースの元となる調査レポートではこうした観点での集計と分析を行い、守りのIT対策を訴求する際に留意すべきポイントを述べている。

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/ 生産/ 販売/ 人給/ ワークフロー/ コラボレーション/ CRM/ BI・帳票など10分野のシェアとユーザによる評価を網羅
レポート案内: http://www.norkresearch.co.jp/pdf/2019itapp_rep.pdf

『2019年版 DX時代に向けた中堅・中小ITソリューション投資動向レポート』

IoT、VR/AR、ロボット、ドローン、HRTech、ウェアラブル、働き方改革、シェアリング、サブスクリプションの最新動向を網羅
レポート案内: http://www.norkresearch.co.jp/pdf/2019IT_user_rep.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