中堅・中小企業におけるセキュリティ・運用管理・バックアップ対策に起きつつある変化とは何か？

2017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利用実態と展望レポート案内

本ドキュメントは「調査対象」「設問項目」および「試読版」を掲載した調査レポートご紹介資料です。

[調査レポートで得られるメリット]

1. **年商/業種/従業員数/地域といった様々な観点で市場動向を把握することができます。**
2. **収録されているデータをカタログや販促資料などに引用/転載いただくことができます。**

調査対象ユーザ企業属性

本レポートでは以下のような属性に合致する1300件（有効件数）のサンプルを抽出した調査を行っています。
情報システムの決済/選定ないしは運用/管理といった適切な職責を持った社員を調査の対象としています。

有効サンプル数：　1300社（1社1レコード）

A1.年商区分：　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

A2.職責区分：　以下のいずれかの職責を持つ社員
- 情報システムの導入や運用/管理の作業を担当している
- 情報システムに関する製品/サービスの選定または決裁の権限を有している

A3.従業員数区分：　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～1000人未満 / 1000人以上～3000人未満 /3000人以上～5000人未満 / 5000人以上

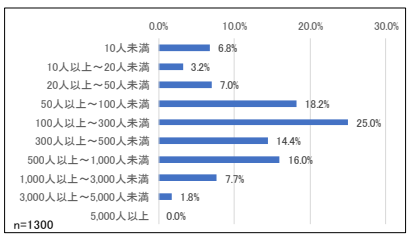
A4.業種区分：　組立製造業 / 加工製造業 / 流通業 / 建設業 / 卸売業 / 小売業 / IT関連サービス業 / 一般サービス業 / その他

A5.地域区分：　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

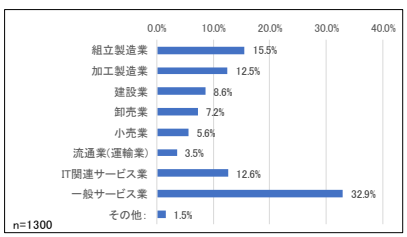
調査実施時期： 2017年7月～8月

上記のA1～A5に加えて、**「A6.IT管理/運用の人員規模」**（IT管理/運用を担う人材は専任/兼任のいずれか？人数は1名/2～5名/6～9名/10名以上のどれに当てはまるか？）および**「A7.ビジネス拠点の状況」**（オフィス、営業所、工場などの数は1ヶ所/2～5ヶ所/6ヶ所以上のいずれか？ITインフラ管理は個別/統一管理のどちらか？）といった属性についても尋ねており、A1～A7を軸として以降に述べる全ての設問を集計したデータが含まれます。
以下の3つのグラフは1300件の有効サンプルの「従業員数」「業種」「所在地」による分布を表したものです。
『従業員数1000人以上の大企業が中心で、中小企業のサンプルはわずかしかない』といったサンプル件数不足や『実はIT関連サービス業が大半を占めてしまっており、実態の業種分布と乖離している』といったサンプルの偏りがないことが確認できます。

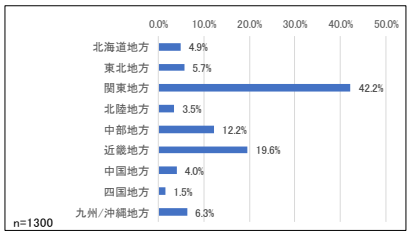
従業員数分布



業種分布



所在地分布



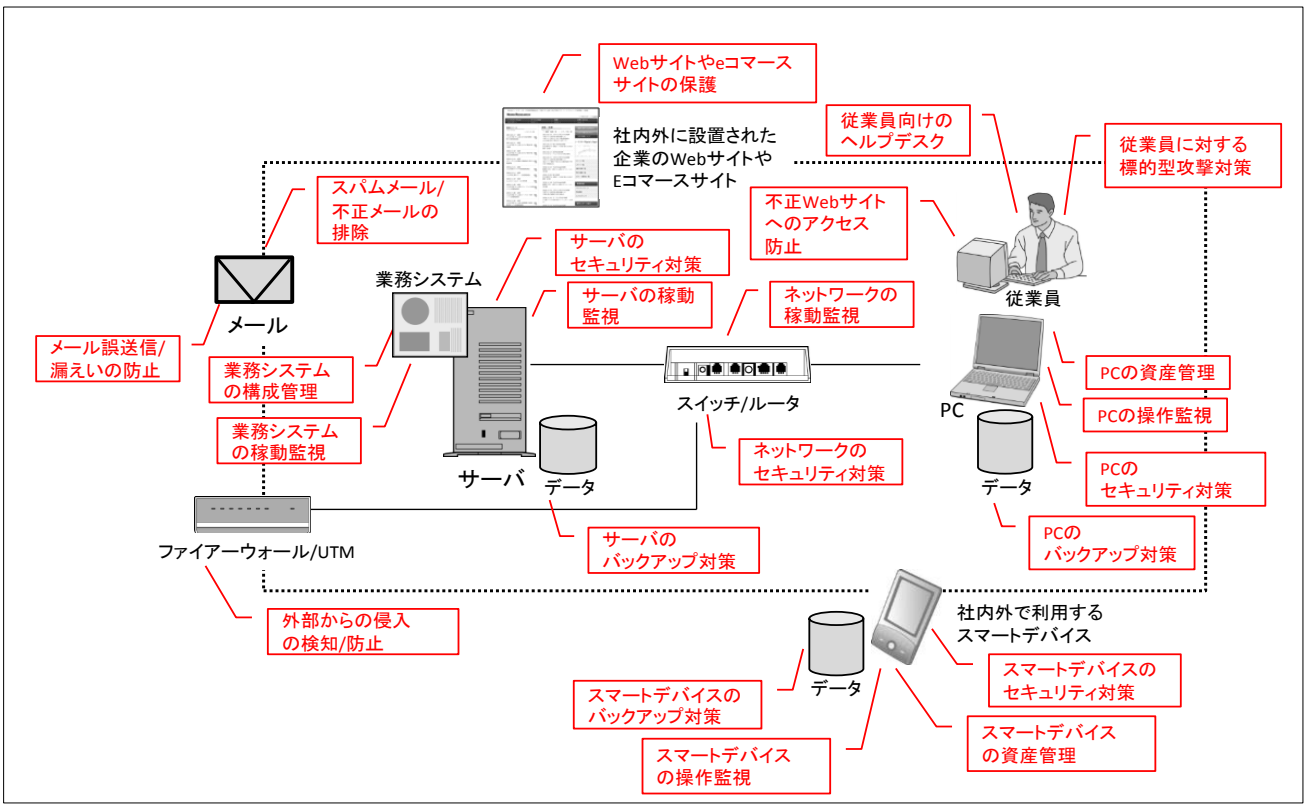
設問項目(1/5)

R1系列設問:

[R1-*]という番号を持つ設問群では「PCを対象としたソフトウェアによるマルウェア対策」だけでなく、「アプライアンスによるサーバの稼働監視」「サービスによる標的型攻撃対策」「アウトソーシングによるWebサイトやeコマースサイトの保護」などといったように多種多様な「管理対象」と「実施手段」を網羅的に尋ねています。

旧来、中堅・中小企業におけるセキュリティ・運用管理・バックアップに関連した取り組みはPCを対象としたものが主体でした。ですが、スマートフォン/タブレットなどのスマートデバイスやインターネットを介して業務システムを利用するクラウドサービスが普及するにつれて、中堅・中小企業が対策を講じるべき「管理対象」も広がってきています。

こうした背景を受け、本調査レポートではPC、サーバ、メール、Webサイト、標的型攻撃など、中堅・中小企業がセキュリティ・運用管理・バックアップに関連した対策を講じるべき「管理対象」を下図のように整理しています。



上図に示した「管理対象」を整理すると、後述のように全部で22項目となります。それぞれの「管理対象」について、R1系列設問では「現時点でどのような対策を講じているか？」(「実現手段」)を以下の選択肢(複数回答可)で尋ねています。

「アプライアンス」: 専用の機器(ハードウェア)を導入する
例)「外部からの侵入の検知/防止」のためにファイアーウォール機器を導入する

「パッケージソフト」: ソフトウェアのパッケージを購入し、PCやサーバにインストールする
例)「PCのセキュリティ対策」のために、マルウェア対策ソフトを導入する

「クラウドサービス」: 月額/年額で利用するクラウドサービスを利用する
例)「Webサイトやeコマースサイトの保護」のために、アクセスを仲介するサービスを利用する

「アウトソーシング」: 必要な作業や役務を社外の業者に委託する
例)「従業員向けのヘルプデスク」のために、Q&A応対の業務を社外の業者に委託する

「機器付属ツール」: PC、サーバ、ネットワーク機器に付属するツールを利用する
例)「ネットワークの稼動監視」のために、スイッチ/ルータ機器に付属のツールを使用する

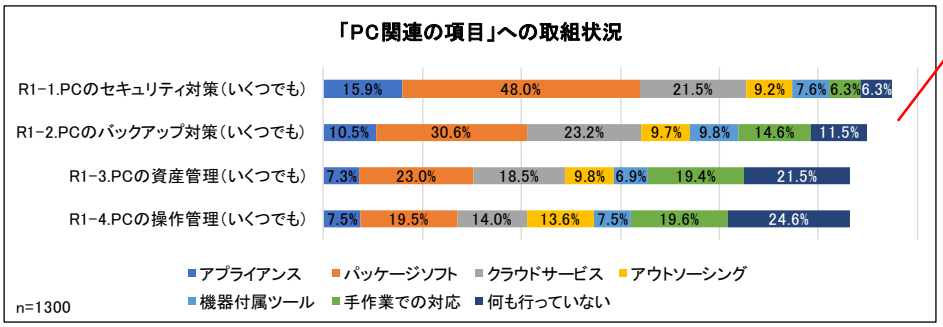
「手作業での対応(排他選択肢)」: ツールやサービスは利用せず、従業員が手作業で対応する
例)「スパムメール/不正メールの排除」は従業員が個々に内容を判断して削除している

「何も行っていない(排他選択肢)」: ツールやサービスは利用せず、手作業による対応も行っていない

次頁へ続く

設問項目(2/5)

前頁で図示した「管理対象」は以下のように8グループ、全22項目となります。この22項目がR1系列の22個の設問[R1-1]～[R1-22]に対応しており、設問ごとに前頁下段に記載した「実施手段」を尋ねています。例えば、以下のグラフは<<1.PC関連の項目>>グループの4つの設問([R1-1]～[R1-4])の結果を示したものです。ここでは設問結果を単純集計した結果を掲載していますが、調査レポートには以下のデータを年商/業種/従業員数/所在地など(1ページ目のサンプル属性)を軸として集計したデータも含まれます。



ここでは年商500億円未満全体の集計結果のみを掲載しているが調査レポートには年商別、業種別、従業員数別、所在地別などの様々な属性別に集計したデータが含まれる。

<<1.PC関連の項目>>

R1-1.PC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PCへの攻撃を防ぐ
R1-2.PCのバックアップ対策:	PCのプログラム、データ、設定情報などを複製して保管する
R1-3.PCの資産管理:	PCへのプログラム導入状況を把握し、起動や使用を制御する
R1-4.PCの操作管理:	特定の操作(印刷やUSBメモリの使用など)を監視/制御する

<<2.スマートデバイス関連の項目>>

R1-5.スマートデバイスのセキュリティ対策:	不正なプログラムやアクセス手法によるスマートデバイス攻撃を防ぐ
R1-6.スマートデバイスのバックアップ対策:	スマートデバイスのプログラム/データ/設定などを複製して保管する
R1-7.スマートデバイスの資産管理:	スマートデバイスのプログラム導入状況を把握し、起動/使用を制御する
R1-8.スマートデバイスの操作管理:	特定の操作(通信/通話や無線によるデータ授受など)を監視/制御する

<<3.サーバ関連の項目>>

R1-9.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
R1-10.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
R1-11.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

<<4.業務システム関連の項目>>

R1-12.業務システムの稼動監視:	アプリケーションやミドルウェアに障害/遅延がないかを監視する
R1-13.業務システムの構成管理:	アプリケーションやミドルウェアの設定情報や変更履歴を管理する

<<5.メール関連の項目>>

R1-14.スパムメール/不正メールの排除:	スパムメールや不正メールを検知し、社内への配布を防止する
R1-15.メール誤送信/漏えいの防止:	メールの宛先や内容をチェックし、誤送信や情報漏えいを防ぐ

<<6.Webサイト関連の項目>>

R1-16.WebサイトやeコマースサイトのWeb保護:	社外に公開しているサイトに対する不正侵入や攻撃を防ぐ
R1-17.不正Webサイトへのアクセス防止:	URLフィルタリングなどで従業員のWeb閲覧を管理/制御する

<<7.ネットワーク関連の項目>>

R1-18.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
R1-19.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
R1-20.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

<<8.その他の項目>>

R1-21.従業員に対する標的型攻撃対策:	知人を装ったメールなどによる個人を標的とした攻撃の防御
R1-22.従業員向けのヘルプデスク:	従業員からのIT関連の質問に対応できる窓口の設置/運営

次頁へ続く

設問項目(3/5)

R2系列設問:

[R2-*]という番号を持つ設問群では中堅・中小企業が対策を講じるべきセキュリティ、運用管理、バックアップに関する項目において、どのベンダの製品/サービスを導入しているのか?を尋ねています。

R2-1.PC関連の項目において導入済みの製品/サービスのベンダ(いくつでも):

R1系列設問の選択肢に見られるように中堅・中小企業がセキュリティ・運用管理・バックアップ対策の「管理対象」とすべき範囲は広がってきています。ですが、「PC関連」は依然として最も重要度の高い領域でもあります。そこで、設問[R2-1]では以下の選択肢を列挙し、PC関連のセキュリティ・運用管理・バックアップ対策に関して導入済みの製品/サービスのベンダ名を尋ねています。(カッコ内は各社の代表的な製品/サービス)(以下ではセキュリティ・運用管理・バックアップに関する自社製の製品/サービスを開発/販売しているIT企業を対象としている)

<<セキュリティパッケージ主体>>
- トレンドマイクロ(「ウイルスバスター」など)
- シマンテック(「Symantec Endpoint Protection」など)
- マカフィー(「McAfee Endpoint Protection」など)
- キヤノンITソリューションズ(「GUARDIANWALL」「ESET」など)
- カスペルスキー(「カスペルスキー」など)
- ソースネクスト(「ZEROシリーズ」など)
- エフ・セキュア(「F-Secure」など)
- FFRI(「FFRI yarai」など)
- Cylance(「Cylance PROTECT」など)

<<運用管理パッケージ主体>>
- Sky(「SKYSEA Client View」など)
- クオリティソフト(「QND」など)
- エムオーテックス(「LanScope」など)
- LANDESK Software(「LANDESK」など)
- ハンモック(「AssetView」など)

<<バックアップパッケージ主体>>
- ベリタステクノロジーズ(「Backup Exec」など)
- Arcserve(「Arcserve」など)
- クエストソフトウェア(「NetVault」など)
- ストレージクラフト(「ShadowProtect」など)
- ネットジャパン(「ActiveImage」など)
- アクロニス(「Acronis」など)

<<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(「InterSafe」など)
- デジタルアーツ(「i-FILTER」など)
- ソリトンシステムズ(「InfoTrace」など)

<<アプライアンス主体>>
- チェック・ポイント・ソフトウェア・テクノロジーズ(「Check Point」など)
- ウォッチガード・テクノロジー・ジャパン(「Firebox」など)
- ジュニパーネットワークス(「SRXシリーズ」など)
- パロアルトネットワークス(「PAシリーズ」など)
- ブルーコートシステムズ(「Blue Coat」など)
- フォーティネットジャパン(「Fortigate」など)
- アライドテレシス(「ARシリーズ」など)
- ソニックウォール(「NSAシリーズ」など)
- サクサ(「SS3000 II 」など)
- Clavister AB(キヤノンITソリューションズ)(「Clavister」など)
- ファイア・アイ(「FireEye」など)
- ソフォス(「XG Firewall」など)
- バラクーダネットワークス(「Barracuda」など)
- 日本プルーフポイント(「Proofpoint」など)

<<大手のITベンダ/SIer>>
- 日立製作所(「JP1」など)
- 富士通(「Systemwalker」など)
- NEC(「WebSAM」など)
- 日本ヒューレット・パッカード(「Ice Wall」など)
- デル/EMCジャパン(「RSA Secure ID」など)
- シスコシステムズ(「CiscoWorks」など)
- 日本マイクロソフト(「Microsoft System Center」など)
- 日本IBM(「Tivoli」など)
- NTTデータ(「Hinemos」など)
- 野村総合研究所(「Senju」など)

<<その他>>
- その他のベンダ:
- 対策を検討しているが、製品/サービスは導入していない(排他選択肢)
- 対策そのものを実施していない(排他選択肢)

R2-2. PC以外に重要と考えるセキュリティ/運用管理/バックアップの対象分野

設問[R2-2]では「PC関連」以外の取り組み分野を列挙し、そこから最も重要と考えられるもの(1つのみ)を尋ねています。選択肢(全8項目)は以下の通りです。(R系列設問における「監理対象」のグループと概ね一致しています)

- スマートデバイス関連
- サーバ関連
- 業務システム関連
- メール関連
- Webサイト関連
- ネットワーク関連
- 標的型攻撃関連
- ヘルプデスク関連
- その他:

次頁へ続く

設問項目(4/5)

R2-3. PC以外に重要と考える対象分野で導入済みの製品/サービスのベンダ(いくつでも)

設問[P2-3]では、設問[P2-2]で回答した「PC関連」以外の最も重要な取り組み分野において、どのベンダの製品/サービスを導入しているか?を尋ねています。選択肢は設問[R2-1]と同様です。

R3系列設問:

[R3-*]という番号を持つ設問群ではセキュリティ・運用管理・バックアップのそれぞれにおいて、製品/サービスが今後どのような機能や特徴を備えるべきか?を尋ねています。つまり、ユーザ企業の今後のニーズを尋ねた設問群となります。

R3-1.セキュリティ関連の製品/サービスが今後備えるべきと考える機能や特徴(いくつでも)

セキュリティ関連の製品/サービスが今後備えるべきと考える機能や特徴(今後のニーズ)を尋ねた設問です。(選択肢は以下の通り)

・標的型攻撃を防ぐための従業員向け教育やトレーニング
・セキュリティ対策を立案/遂行できる社内人材の育成支援
・必要なセキュリティ対策が網羅され、取捨選択の必要がない
・複数の変化や兆候を総合的に判断し、被害を未然に防げる
・セキュリティの警告だけでなく、対処まで自動で行ってくれる
・社内ネットワークに負荷をかけずにセキュリティ対策を行える
・サーバなどのIT機器を導入せずにセキュリティ対策が行える
・1台の専用機器を導入すれば、セキュリティ対策を網羅できる
・IoT活用に必要なセキュリティ対策を網羅した製品/サービス
・指紋、顔、静脈などの生体認証技術を利用することができる
・その他:
・特にニーズはない(排他選択肢)

R3-2.運用管理関連の製品/サービスが今後備えるべきと考える機能や特徴(いくつでも)

運用管理関連の製品/サービスが今後備えるべきと考える機能や特徴(今後のニーズ)を尋ねた設問です。(選択肢は以下の通り)

・従業員の質問に答えてPC操作を支援するサービスを利用できる
・ライセンスの過不足を把握し、最適な購入プランを提示してくれる
・社外で利用するスマートデバイスも社内PCと一緒に管理できる
・社内環境とクラウド環境を同一の製品/サービスで管理できる
・場所や端末に依存せず、常に同じ業務システムを利用できる
・システムの開発と運用を融合した体制(DevOps)が実現できる
・社内ネットワークに負荷をかけずにPC操作を制御/管理できる
・店舗や営業所のネットワーク機器を遠隔から設定/管理できる
・店舗や営業所のサーバやPCを遠隔から設定/管理できる
・その他:
・特にニーズはない

次頁へ続く

設問項目(5/5)

R3-3.バックアップ関連の製品/サービスが今後備えるべきと考える機能や特徴(いくつでも)

バックアップ関連の製品/サービスが今後備えるべきと考える機能や特徴(今後のニーズ)を尋ねた設問です。(選択肢は以下の通り)

・社内ネットワークに負荷をかけずにPC内のデータを保存できる
・普段利用しないデータを自動で判断し、クラウドに保存できる
・過去の利用状況を元にデータの上書きミスを警告してくれる
・バックアップ元とは異なる機器にシステム全体を復元できる
・保存データが確実に復元できるかを自動的にチェックできる
・利用中のアプリケーションを停止せずにデータを保存できる
・データだけでなくシステム全体を手軽にバックアップできる
・圧縮や重複排除によって保存データの容量を抑えられる
・データやシステム全体を遠隔地に複製して復元できる
・その他:
・特にニーズはない

レポート試読版1(「分析サマリ」その1)

本レポートには40ページに渡って、中堅・中小企業におけるセキュリティ・運用管理・バックアップ対策の実態と今後の展望に関する重要ポイントとIT企業に向けた提言をまとめた「分析サマリ」が含まれます。以下のレポート試読版では分析サマリの一部を紹介しています。

2017 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
に関する利用実態と展望レポート

分析サマリ

本ドキュメントでは「2017 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利用実態と展望レポート」における重要ポイントと今後に向けた提言を記載している。分析や提言は本調査レポートの作成に際してノークリサーチが独自に実施したユーザ企業を対象としたアンケート調査に基づいている。アンケート調査のサンプル属性や設問項目を把握しておくことが重要であるため、本サマリの前に「本レポートの概要(はじめにお読みください).pdf」に目を通すことをお勧めする。

1.セキュリティ・運用管理・バックアップに関する取り組み状況

従来、中堅・中小企業におけるセキュリティ・運用管理・バックアップに関連する取り組みは**「PC を対象としたソフトウェアによる対策」**が主体だった。

だが、昨今では

・スマートフォンやタブレットの普及によって、企業が管理すべき端末の種類が増えてきた。
・クラウドや e コマースへの取り組みによってインターネットと接続する場面が増え、それに伴うネットワーク管理の必要性が高まってきた。
・標的型攻撃に代表される新たな攻撃手法の登場によって、単にツールを導入するだけでは対処が難しくなってきた。

などといった状況の変化が見られる。

こうした変化によって、中堅・中小企業においても**「PC に限定されない幅広い管理対象に対して、ソフトウェアだけではない様々な実施手段を用いた対策」**が求められるようになってきている。

そこで、本調査レポートでは中堅・中小企業におけるセキュリティ・運用管理・バックアップに関連する取り組みを

「PC 関連」「スマートデバイス関連」「サーバ関連」「メール関連」「Web サイト関連」「ネットワーク関連」「その他の項目」の 8 つのグループ、合計 22 項目の**『管理対象』**

と

「アプライアンス」「パッケージソフト」「クラウドサービス」「アウトソーシング」「機器付属ツール」といった合計 7 項目の**『実施手段』**

に整理し、それぞれの『管理対象』において、どのような『実施手段』が講じられているか?の集計/分析を行っている。

**********以下、省略**********

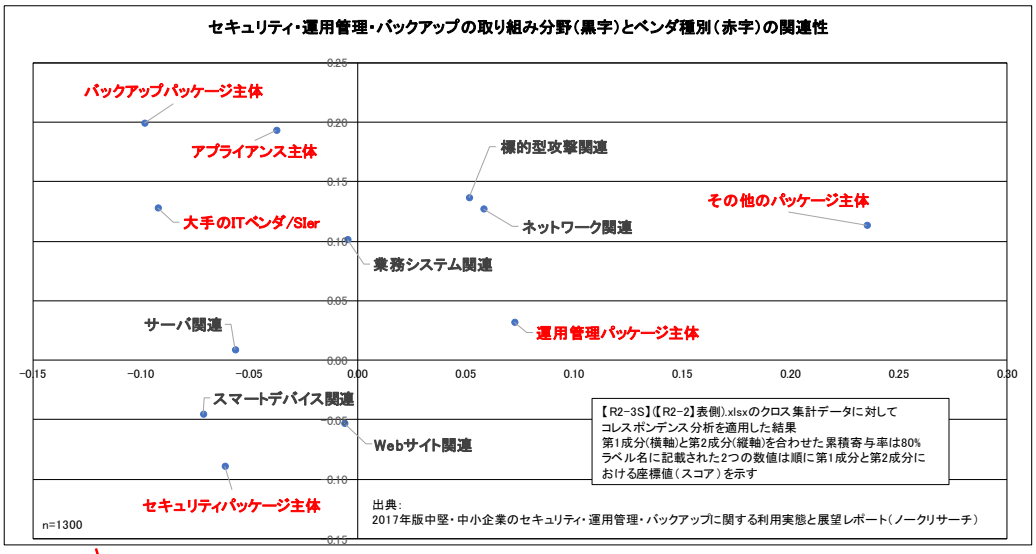
レポート試読版2(「分析サマリ」その2)

本レポートでは本ドキュメントの2ページから6ページに掲載された設問項目を年商/職責/従業員数/業種/所在地/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観点を軸とした集計データに加えて、コレスポンデンス分析の手法を用いて「各ベンダが顧客に対して次に訴求すべき取り組み分野は何か？」の提言も行っています。以下は分析サマリにおいて上記に記載した内容を掲載している箇所の一部を抜粋したものです。

このように、セキュリティ・運用管理・バックアップ対策における 8 つの取り組み分野(前述のグラフにおける表側)と「対策を検討しているが、製品/サービスは導入していない」および「対策そのものを実施していない」を含む 9 つのベンダ種別(前述のグラフにおける表頭)の関連を整理すると、「各ベンダが顧客に対して次に訴求すべき取り組み分野は何か？」を知ることができる。

こうした場面で有効な手法が「コレスポンデンス分析」である。前述のグラフの元となるクロス集計データから、表側と表頭に記載された項目間の対応関係を数量的に導き出す手法である。以下はその結果を図示したものだ。

一般的にコレスポンデンス分析では対応関係を数量的に表す軸(成分)が複数存在する。(表側と表頭のどちらか小さい値から 1 を引いた数となるので、この場合は 8-1=7)となる。ただし、以下のケースでは各成分がどれだけデータの状況を反映しているか？の指標(寄与度)を見た場合には第 1 成分と第 2 成分で全体の 8 割超となる。そのため、第 1 成分を横軸、第 2 成分を縦軸とした以下の図が項目間の対応関係を的確に説明した結果と捉えることができる。



試読版のため、一部のデータ項目を割愛した状態で掲載している

上図においてセキュリティ・運用管理・バックアップの取り組み分野(黒字)とベンダ種別(青字)が近接している場合は、ユーザ企業が該当する取り組み分野の製品/サービスを導入する際に近接するベンダが選ばれやすいことを示す。つまり、この図を見ることによって、「PC 関連以外の分野として次に何を訴求するのが有効か？」をベンダ種別ごとに把握することができる。その点を整理すると以下のようになる。(有望度の高い取り組み分野を順に等号/不等号で並べて表記する)

**********以下、省略**********

レポート試読版3(「主要分析軸集計データ」)

「設問項目」に掲載した設問結果を年商、業種、従業員数、所在地などの基本属性を軸として集計したものが、「主要分析軸集計データ」です。Microsoft Excel形式で調査レポート内に同梱されています。

以下の試読版に掲載したものは「業種」を集計軸とし、「R1系列」の各設問項目を集計したものです。

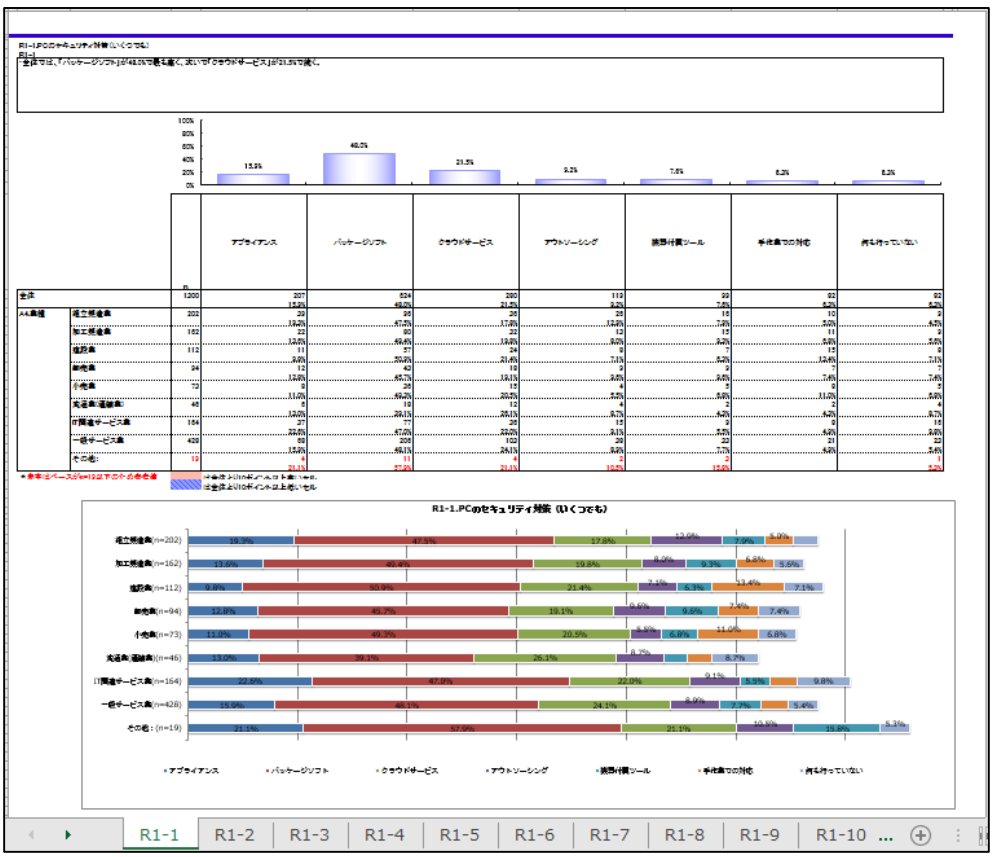
以下のMicrosoft Excelファイル名は『【R1系列】(【A4】表側).xlsx』となっています。[R1系列]とは本ドキュメントの2ページに記載されているように、全22項目に渡るセキュリティ・運用管理・バックアップ対策の「管理対象」における取り組み状況を尋ねた設問であることがわかります。[A4]とは本ドキュメントの1ページに記載されているように、基本属性の4番目である「A4.業種」を表します。このようにファイル名を見れば、どの設問について何を軸として集計したものか？が把握できるようになっています。

画面の最下部からは多数のシートがあることがわかります。この1シートが1つの設問結果データに相当します。R1系列は全部で22設問あり、集計の軸となる属性は「A1.年商」「A2.職責」「A3.従業員数」「A4.業種」「A5.所在地」「A6.IT管理/運用の人員規模」「A7.ビジネス拠点の状況」の7項目ですので、R1系列における「主要分析軸データ」のシート数は22×7 =154 となります。R2系列やR3系列も含めると、本レポート全体では以下のような主要分析軸データの数は合計で(22+3+3)×7 = 196シートとなります。

個々のシートには画面上部に軸を設定しない状態の縦帯グラフ、画面中央には年商や業種といった属性軸を設定して集計した結果の数表データ、画面下部にはその数表データを横帯グラフで表したものが掲載されるという書式になっています。

こうした「主要分析軸集計データ」を見れば、
「従業員数によってセキュリティ・運用管理・バックアップの対策実施状況がどう変化するのか？」
「セキュリティ・運用管理・バックアップにおける今後のニーズが業種によってどう違ってくるか？」
「PC以外に重要と考えるセキュリティ・運用管理・バックアップの管理対象に地域差はあるか？」
といったことを客観的な見地から数量的に確認することができます。

ただし、「年商5億円以上～50億円未満かつ組立製造業」といったように2つ以上の属性を掛け合わせたものを軸とした集計結果については本レポートの標準には含まれません。



レポート試読版4(「質問間クロス集計データ」)

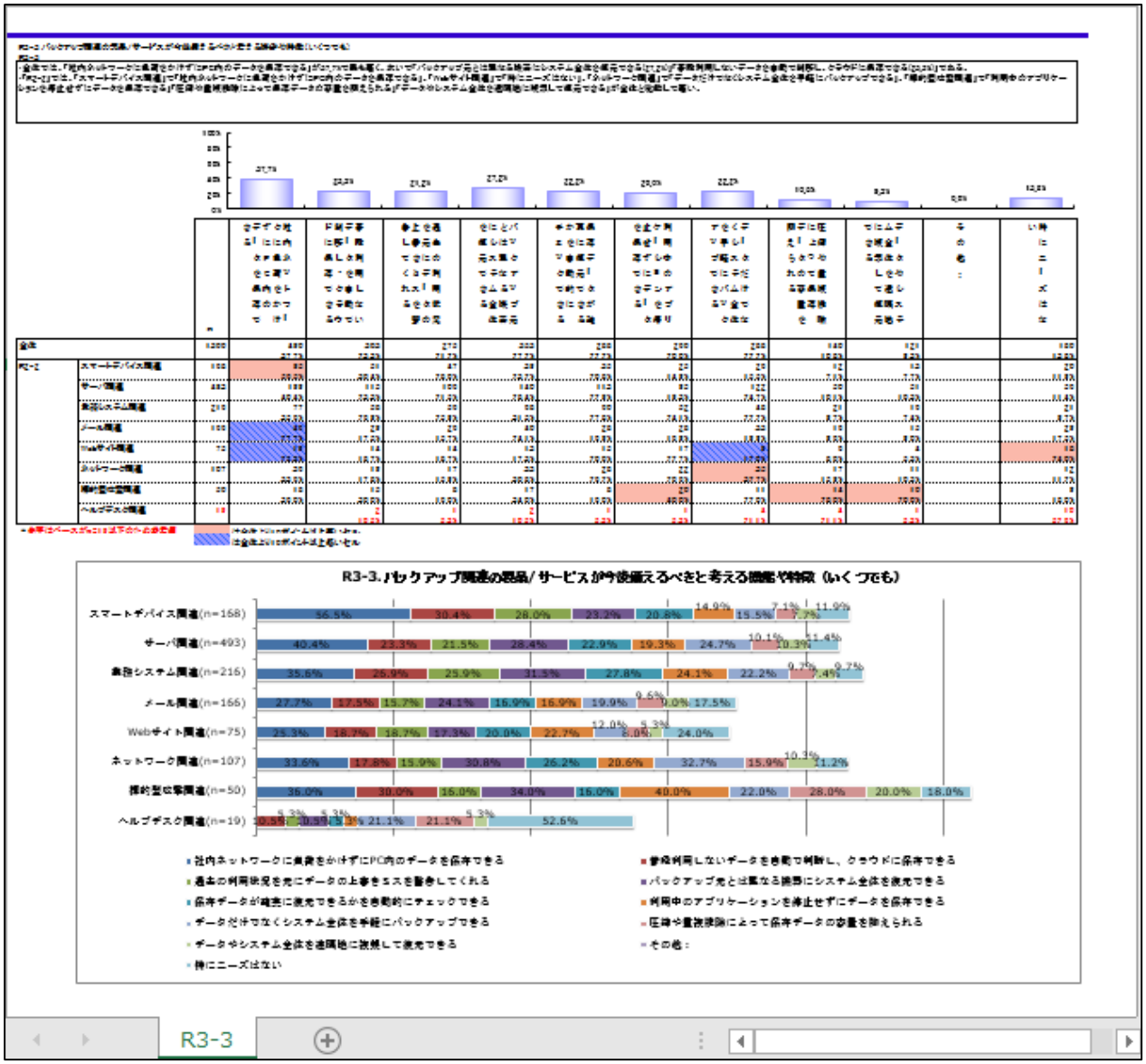
「設問項目」に掲載した設問結果を他の設問結果を軸として集計したものが、「質問間クロス集計データ」です。「主要分析軸集計データ」と同様にMicrosoft Excel形式で同梱されています。

以下の試読版に掲載したものは「バックアップ関連の製品/サービスが今後備えるべきと考える機能や特徴」を「PC以外に重要と考えるセキュリティ/運用管理/バックアップの対象分野」を軸として集計したものです。

以下のMicrosoft Excelファイル名は『【R3-3】(【R2-2】表側).xlsx』となっています。[R3-3]とは本ドキュメントの6ページに記載されているように「R3-3.バックアップ関連の製品/サービスが今後備えるべきと考える機能や特徴」に関する設問項目であることがわかります。同様に[R2-2] とは本ドキュメントの4ページに記載されているように「R2-2. PC以外に重要と考えるセキュリティ/運用管理/バックアップの対象分野」であることがわかります。この[R2-2]が集計の軸となる設問を表します。

つまり、以下のデータは「PC以外に重要と考えているセキュリティ・運用管理・バックアップの対象分野によって、バックアップ関連の製品/サービスに求める機能や特徴がどのように変わってくるか？を表しています。スマートデバイス管理を重視するユーザ企業とサーバ管理を重視するユーザ企業ではバックアップ製品/サービスに求める機能や特徴も変わってくる可能性があります。以下の諮問間クロス集計データを見ることによってそうした違いを把握することができます。

個々のシートには画面上部に軸を設定しない状態の縦帯グラフ、画面中央には特定の設問を軸として設定した集計結果の数表データ、画面下部にはその数表データを横帯グラフで表したものが掲載されるといった書式になっています。



本レポートの価格とご購入のご案内

【価格】180,000円(税別)
【媒体】CD-ROM (分析サマリ: PDF形式、集計データ: Microsoft Excel形式)
【発刊日】2017年10月23日
【サンプル/ダイジェスト】 以下より、本レポートのサンプル/ダイジェストをご覧いただけます。

http://www.norkresearch.co.jp/pdf/2017Sec_usr_rel1.pdf
http://www.norkresearch.co.jp/pdf/2017Sec_usr_rel2.pdf
http://www.norkresearch.co.jp/pdf/2017Sec_usr_rel3.pdf
http://www.norkresearch.co.jp/pdf/2017Sec_usr_rel4.pdf

【備考】「セキュリティ関連設問のみ」といった一部データのみの分割販売は行っておりません。
【お申込み方法】 弊社ホームページからの申し込みまたはinform@norkresearch.co.jp宛にご連絡ください

その他のレポート最新刊のご案内

「ノークリサーチQuarterly Report 2017年夏版 ～中堅・中小企業がIT企業各社に抱く印象やイメージ～」
ベンダからSIerまで国内外の主要なIT企業33社を対象に1300社のユーザ企業による評価を多角的に分析
・レポート案内とダイジェスト: http://www.norkresearch.co.jp/pdf/2017QRsum_rel.pdf

「2017年版中堅・中小企業におけるIT投資の実態と展望レポート」
「ワークスタイル改革」「IoT」「RPA」「人工知能」「音声操作」「ドローン」など24分野の投資動向と市場規模を網羅
・レポート案内: http://www.norkresearch.co.jp/pdf/2017IT_usr_rep.pdf
・ダイジェスト(サンプル): http://www.norkresearch.co.jp/pdf/2017IT_usr_rel1.pdf
http://www.norkresearch.co.jp/pdf/2017IT_usr_rel2.pdf

「2017年版中堅・中小企業におけるクラウドインフラ活用の実態と展望レポート」
クラウド(IaaS/ホスティング)は既にITインフラの主要な選択肢の一つ、今後は差別化要因の探索が焦点となる
・レポート案内: http://www.norkresearch.co.jp/pdf/2017IaaS_usr_rep.pdf
・ダイジェスト(サンプル): http://www.norkresearch.co.jp/pdf/2017IaaS_usr_rel.pdf

「2017年版中堅・中小企業におけるサーバ導入の実態と展望レポート」
HCIを始めとする新たなニーズを捉えれば、クラウド時代にもオンプレミスのサーバ販売を伸ばすことは可能
・レポート案内: http://www.norkresearch.co.jp/pdf/2017Server_usr_rep.pdf
・ダイジェスト(サンプル): http://www.norkresearch.co.jp/pdf/2017Server_usr_rel1.pdf
http://www.norkresearch.co.jp/pdf/2017Server_usr_rel2.pdf
http://www.norkresearch.co.jp/pdf/2017Server_usr_rel3.pdf

「2017年版中堅・中小企業におけるストレージ導入の実態と展望レポート」
「オールフラッシュ」や「SDS」など、新たな形態はどこまで浸透しつつあるのか？」
・レポート案内: http://www.norkresearch.co.jp/pdf/2017Storage_usr_rep.pdf
・ダイジェスト(サンプル): http://www.norkresearch.co.jp/pdf/2017Storage_usr_rel1.pdf
http://www.norkresearch.co.jp/pdf/2017Storage_usr_rel2.pdf

「2017年版中堅・中小向けサーバ/ストレージ販売のチャネル実態レポート」
サーバ/ストレージ販売のチャネルパートナはベンダやクラウド事業者をどう評価しているのか
・レポート案内: http://www.norkresearch.co.jp/pdf/2017SrvChannel_rep.pdf
・ダイジェスト(サンプル): http://www.norkresearch.co.jp/pdf/2017SrvChannel_rel1.pdf
http://www.norkresearch.co.jp/pdf/2017SrvChannel_rel2.pdf

本ドキュメント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
〒120-0034 東京都足立区千住1-4-1東京芸術センター1705
TEL 03-5244-6691 FAX 03-5244-6692
inform@norkresearch.co.jp
www.norkresearch.co.jp