資料２

中小企業のセキュリティ対策とクラウド活用

内閣サイバーセキュリティセンター 情報セキュリティ指導専門官
八剱　洋一郎

サイバーセキュリティにかかる中小企業の現状

中小企業がセキュリティ対策を推進できない理由 4つ

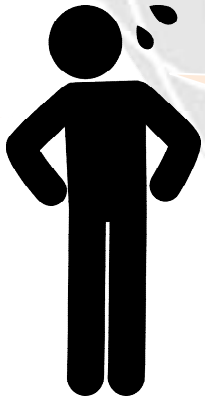
① 対応すべき基準が不明
② 費用対効果が見えない
③ 対策コストがかかる
④ 業務負担を増やしたくない

※ 警視庁の調査より

特に“対応すべき基準が不明”ということが大きな要因であると考えています。

いくらお金をかけたら安全なの？

人が足りないくらい忙しいのに、
何かやらないといけないの？

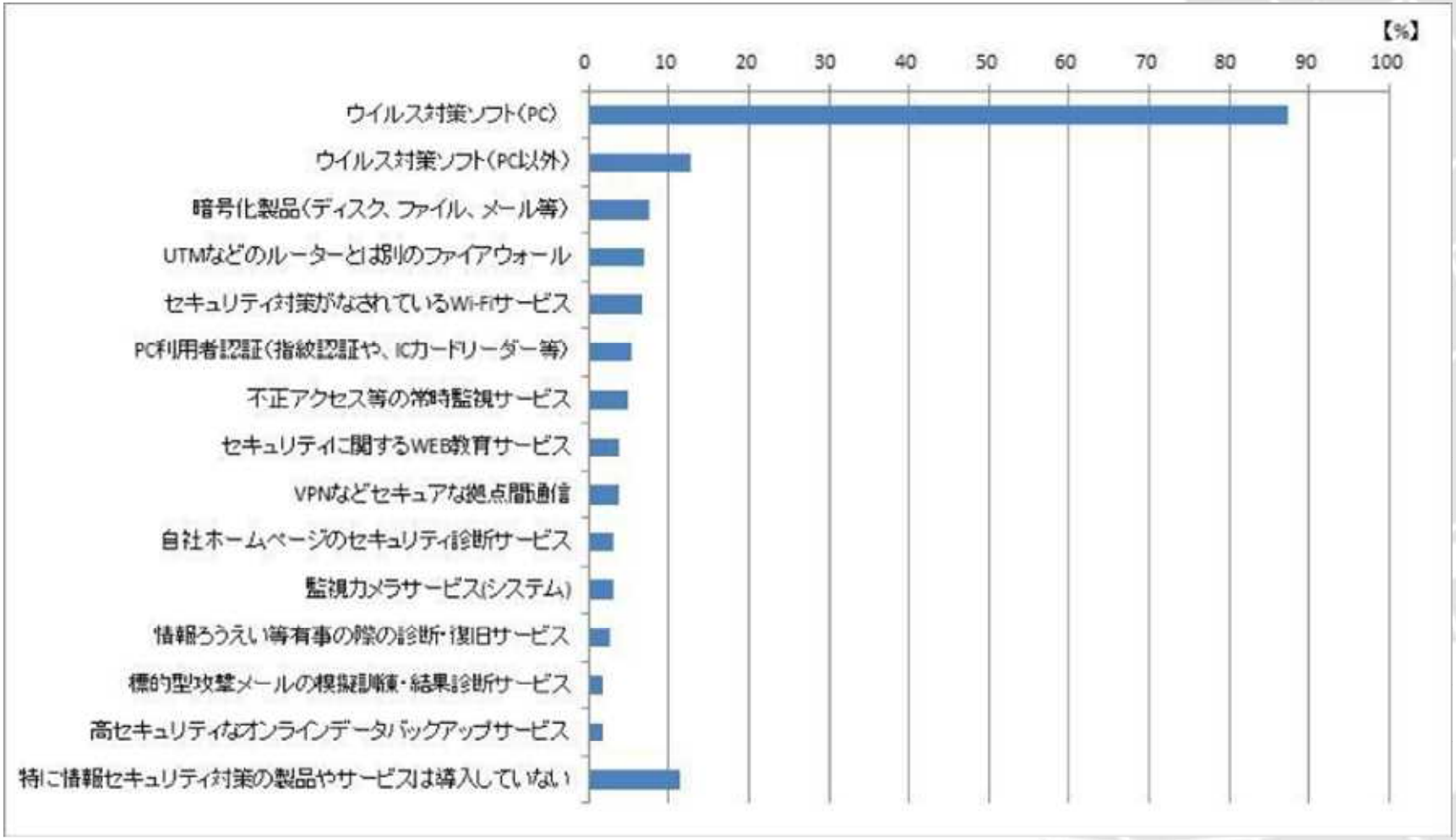


何をすればいいかわからない！

何かメリットがあるの？

参考：中小企業におけるセキュリティ対策状況

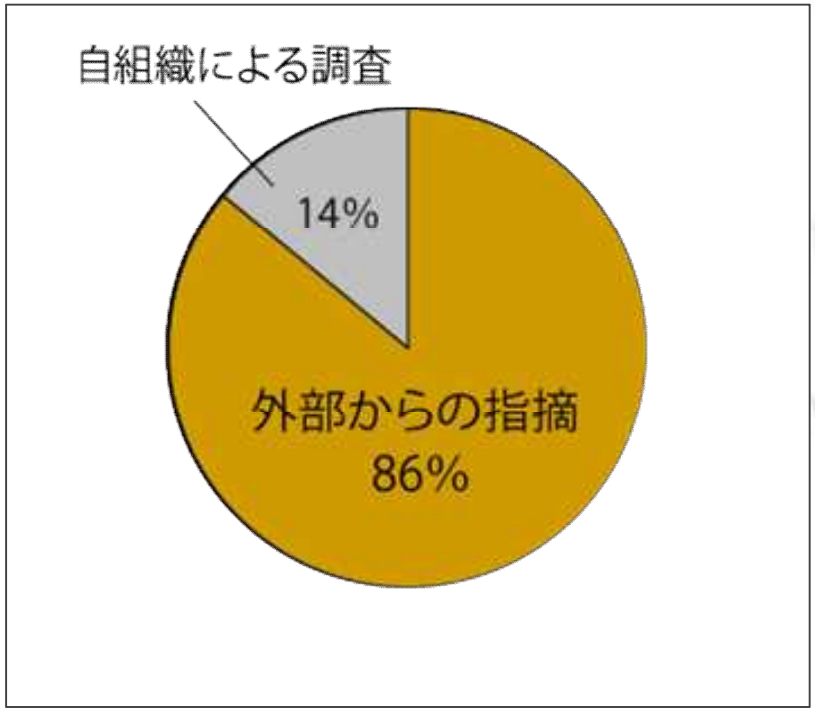
中小企業におけるセキュリティ対策状況



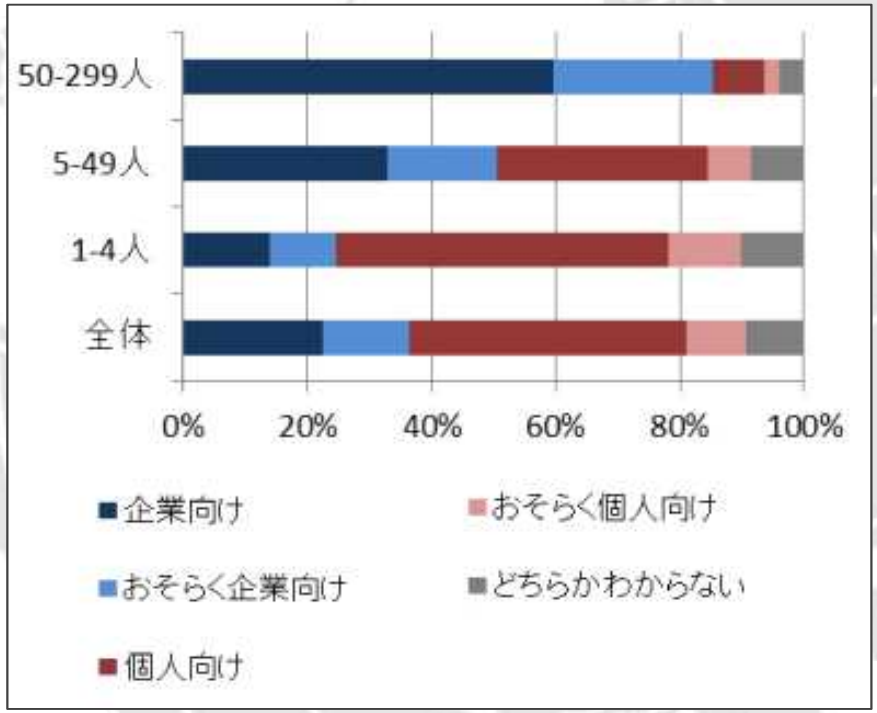
出典:NTT東日本 Web調査より(N=1,200企業、2016年12月)

参考：中小企業におけるセキュリティ対策状況

中堅・中小企業がサイバー攻撃による
被害を把握したきっかけ



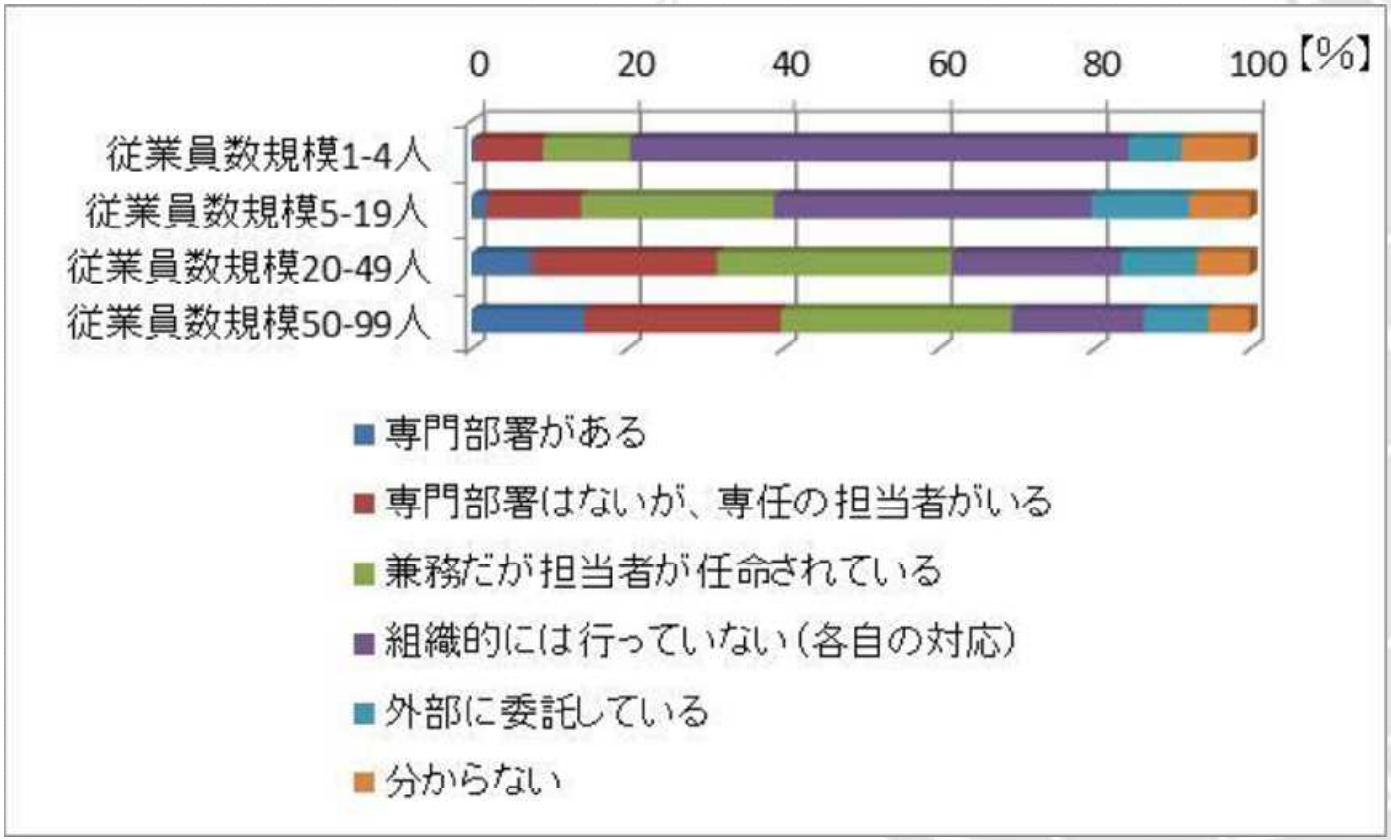
中堅・中小企業における
個人向けウイルス対策ソフトの利用状況



出典: (左)トレンドマイクロ株式会社
トレンドマイクロ社のサポートセンタに申告があった事例の集計結果より(2015 年 1~7 月)
(右)NTT東日本 Web調査より(N=1,200企業、2016年3月)

参考：中小企業におけるセキュリティ対策体制

中小企業におけるセキュリティ対策体制



出典:NTT東日本 Web調査より(N=1,200企業、2016年12月)

クラウド利用形態とセキュリティ対策

1. オンプレミスでのサーバー運用の場合には100%ユーザー責任

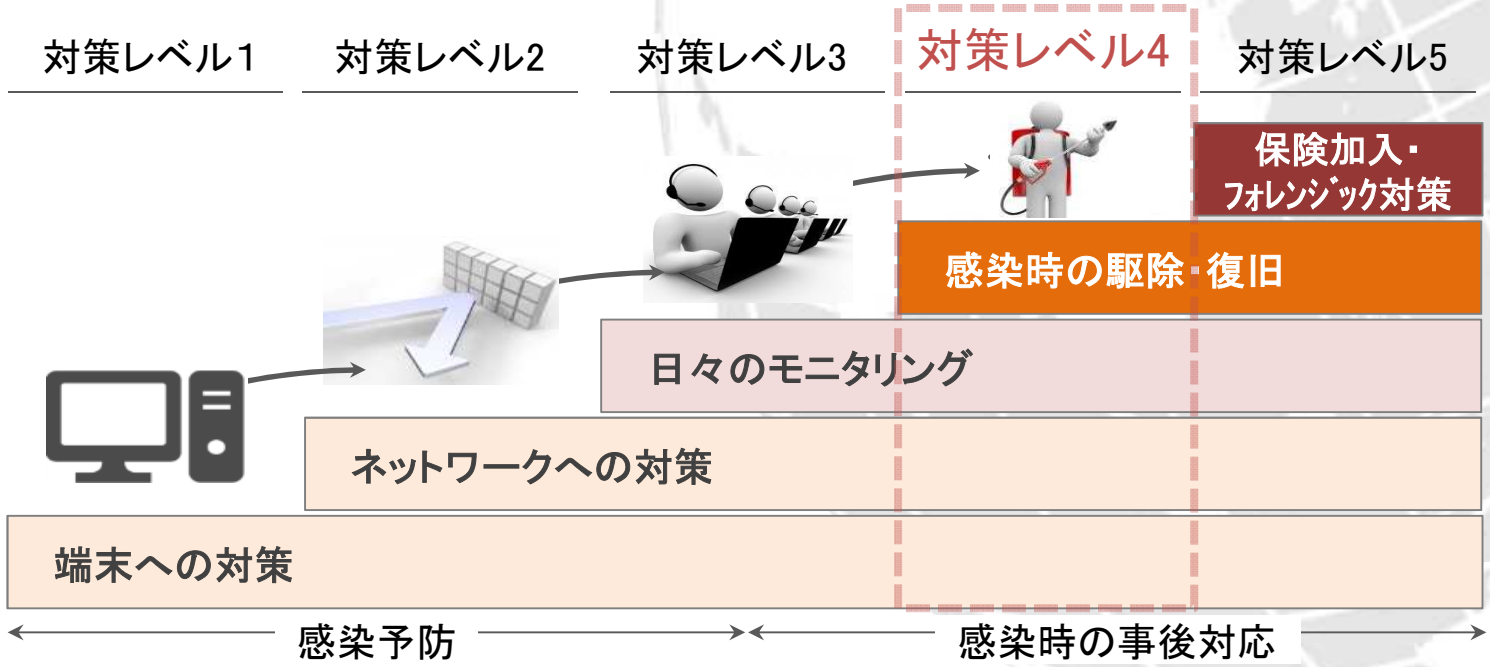
2. クラウドを基盤としてのみ使用する場合（IAAS形態）でも基本セキュリティーはクラウド事業者が提供。セキュリティー基準もクリアーしていることが多い。FIPSに注目

3. クラウド基盤を利用し、かつアプリケーションもパッケージ系であれば、パッケージベンダーのセキュリティーも加わる。ユーザー毎に環境を設営するシングルテナント方式、更に複数ユーザーを同一環境にて運用するマルチテナント方式になるとセキュリティーは極めて厳重となる。

考えられる中小企業のセキュリティ対策レベル

中小企業が対応すべき基準

手口が巧妙化・複雑化するサイバー攻撃すべてを防ぐことは困難なため、近年では事故が起きたとしても、その被害を最小限に食い止めるような対応が重要視されているため、「対応すべき基準」としては、少なくとも下記レベル4まで対策することが推奨されます。



端末やネットワークへの対策以外にも、日々のモニタリングで**感染後の対策が重要**です。

中小企業のセキュリティ問題の解決策

中小企業における基幹系アプリケーション

サーバー層

ERP基幹系システムをクラウド化を推奨し、
アプリケーションベンダーにより防御。

ネットワーク層

ネットワークキャリアにより中小企業向けの
ネットワークや機器をデザインし、防御。

クライアント層

某大企業によりクライアントセキュリティ強化。
中小企業向けのPCレンタル事業をデザイン。

取引先企業との連携に関するアプリケーション

サーバー層

取引先との相互認証型システムで
取引先等により防御

ネットワーク層

ネットワークキャリアにより防御し、
取引先等により認証

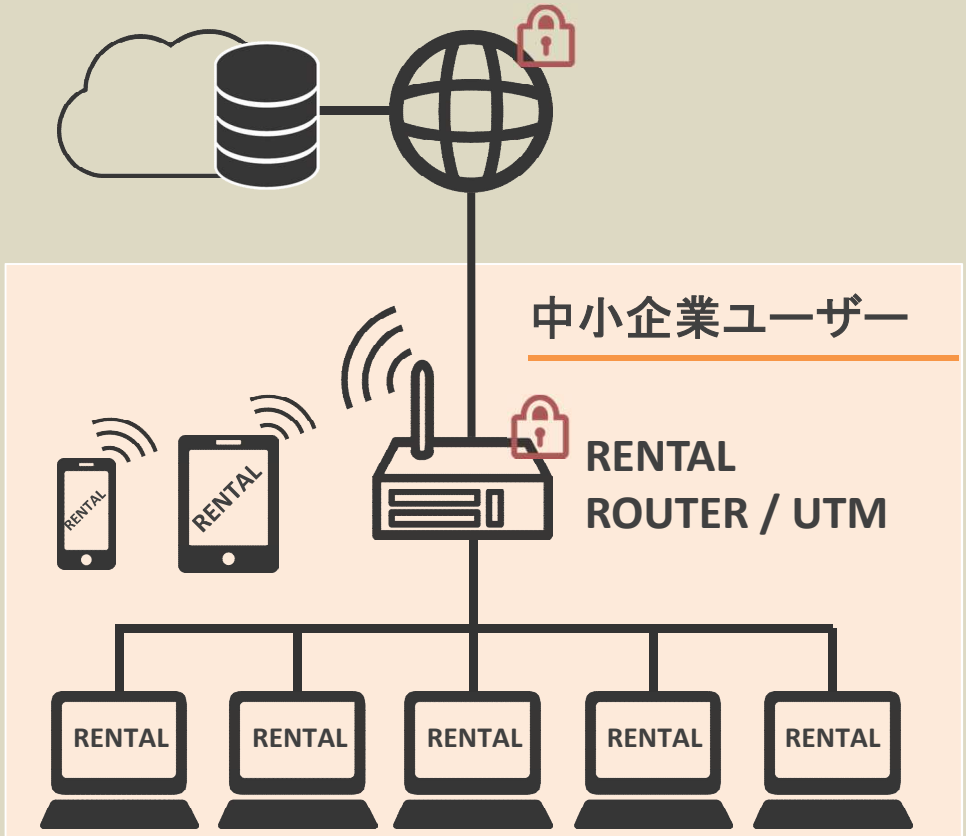
取引条件

中小企業と取引する際には、
公的認証されたシステムを使
用している会社と行う事を推奨

中小企業を守るのは1社ずつのセキュリティーでは限界があるため、
セキュリティ全般のレベルを公的機関に認証させる仕組みを作る。
金融機関の融資等の評価項目としても考慮する。

ネットワーク層（ネットワーク・機器レンタル事業）

通信事業者よりクラウドまでのネットワークをセキュアにサポート。



中小企業におけるIT系ハードウェア全般のレンタル事業

ネットワーク層のセキュリティを担当する企業はモバイル系サポートも行う。
モバイルで使うスマートフォン、タブレット、PCもすべてレンタル化し、OSやミドルウェアも一元管理。
セキュリティについては専用ソフトウェアを投入し、異常を常時監視する。
アプリケーションは専用ダウンロードサイトからのみ行う。

有事の際に対策として・・・

・サイバーリスク保険
・事後対策コンサルティング

クライアント層（PCレンタル事業領域）

レンタル事業者よりキッティング済パソコンの内容例

モニターする領域

・ハードウェア
・OS / ミドルウェア
・メール対策（クラウド化）
・アプリケーション(勘定奉行等)
・インターネットブラウザ
・セキュリティ

追加ソフトウェアの管理

ソフトウェア・アプリケーションダウンロード用の専用サイトよりインストール作業を行う。

特別なソフトウェアを追加でインストールする場合には、セキュリティ事業者を含めた認証が必要。

セキュリティアドバイザー

グローバルオペレータの協力を得る
→Symantec、Trend Micro等

・EDR等の次世代セキュリティ
→常に最新の状態を維持。

・ブラウザやOS等、常に最新環境へアップデートされる。

・Administrator権限を事業者側で管理し、重要な設定変更や個別のソフトウェアインストールをする際は事業者側で認証を行う。

全ユーザーの適用を条件にしたい場合には、データだけをクラウドに保存する
データレスPCのような仕組みも有効。

FIPSについて

FIPS 140 (Federal Information Processing Standardization 140)

暗号モジュールに関するセキュリティ要件の仕様を規定する
米国連邦標準規格である。

FIPS 140-2

連邦情報処理規格（Federal Information Processing Standards/FIPS）出版物140-2 は、機密情報を保護する暗号モジュールのセキュリティ要件を規定する米国政府のセキュリティ基準です。FIPS 140-2 への準拠を必要とするお客様をサポートするために、AWS GovCloud (米国) 内の Amazon Virtual Private Cloud VPN エンドポイントおよび SSL 終端は、FIPS 140-2 検証済み暗号化モジュールを使用して運用されています。AWS では、AWS GovCloud (米国) 環境をご利用いただくときのコンプライアンス管理に役立つ情報を AWS GovCloud (米国) のお客様に提供します。