セキュリティの現状、製品のポイント

株式会社アンラボ
パートナーセールス

はじめに　～皆様と皆様の顧客企業の経営者様、ご担当者様に知っていただきたいこと　AhnLab

近年狙われるのは中小企業

- ウイルス攻撃の標的は政府・自治体や重要インフラ、**大企業** だけではない
- 最近では大企業は **防御が** 厳重なため、 **防御の** 甘い取引先の中小企業がターゲット
- 中小企業を狙いそこから **大企業のシステム内部へ侵入** するケースが増加

ウイルス攻撃を受けて企業が被る不利益

金銭 の喪失	・顧客の個人情報や、取引先の機密情報漏えいによる多大な損害賠償 ・インターネットバンキングの不正送金被害などによる直接的な損失
顧客 の喪失	・攻撃を受けたことで管理責任を問われ、社会的評価は低下し顧客離れ ・風評被害が消えず、イメージ回復が見込めずに事業の存続危機
業務 の喪失	・攻撃被害の拡大を防止するため、システムを一時停止する措置が必要 ・その間はメールすら使えなくなり、営業機会の喪失と、社内業務の停滞
従業員 の喪失	・内部不正が容易に行える職場環境で、従業員のモラル低下、退職 ・従業員の個人情報が適切に保護されず、従業員から訴訟を起こされる可能性

企業におけるセキュリティの脅威（種類）

AhnLab

情報セキュリティ10大脅威 2023 脅威ランキング

2023年3月 独立行政法人情報処理推進機構 (IPA)発表

順位	「組織」向け脅威
1	ランサムウェアによる被害
2	サプライチェーンの弱点を悪用した攻撃
3	標的型攻撃による機密情報の窃取
4	内部不正による情報漏えい
5	テレワーク等の ニューノーマルな働き方を狙った攻撃
6	修正プログラムの公開前を狙う攻撃 （ゼロデイ攻撃）
7	ビジネスメール詐欺による金銭被害
8	脆弱性対策情報の公開に伴う悪用増加
9	不注意による情報漏えい等の被害
10	犯罪のビジネス化 （アンダーグラウンドサービス）

特に中小企業で注目

- PC等保存ファイルを暗号化され使用不可
- 復旧と引き換えに金銭を要求
- 情報を窃取しそれを公開する、攻撃を受けている事をビジネスパートナー等に公表する、と脅迫

- 標的の取引先や業務を委託している外部組織を踏み台とするウイルス感染攻撃
- 標的組織の取引先や委託先を攻撃し、そこが保有する標的の機密情報を狙う

- メール等を利用し特定組織のPCをウイルスに感染させる
- 組織内部に潜入し長期にわたり侵害範囲を徐々に広げる
- 組織の機密情報窃取やシステムの破壊を行う

- 取引先や社外の権威ある第三者等へのなりすましメールで偽サイト等へ誘導して感染させる
- メールやシステムアカウント情報、顧客・取引先情報、社外秘情報等を窃取し悪用（なりすまし、脅迫、金銭盗取）

- サイバー犯罪に使用するサービスやツール等の売買取引
- 専門知識不要で不正に個人情報、機密情報の搾取環境増加
- 詐取した情報はダークウェブ上での公開や犯罪組織へ販売

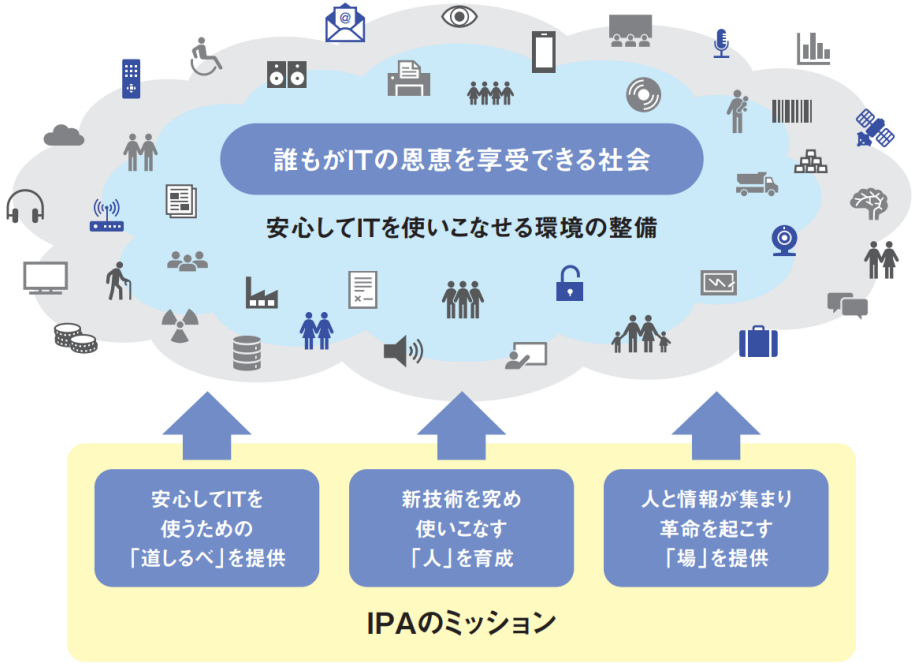
・本ランキングは前年に発生したセキュリティ事故や 攻撃の状況等からIPAが脅威候補を選出
・セキュリティ専門家や企業のシステム担当等による投票でTOP10入りしたもの

中小企業のセキュリティ事情の実態

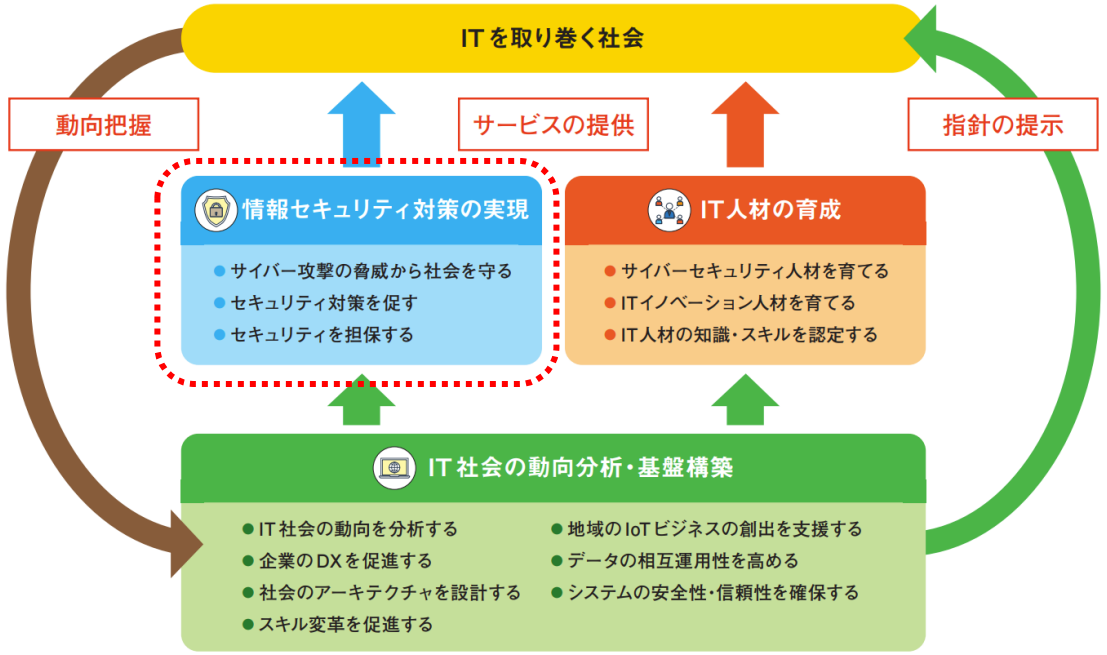
AhnLab

独立行政法人情報処理推進機構 (IPA) の企業セキュリティ調査データに基づき実態を紹介します

IPAビジョン



IPAの役割・事業領域



セキュリティに関するおもな活動

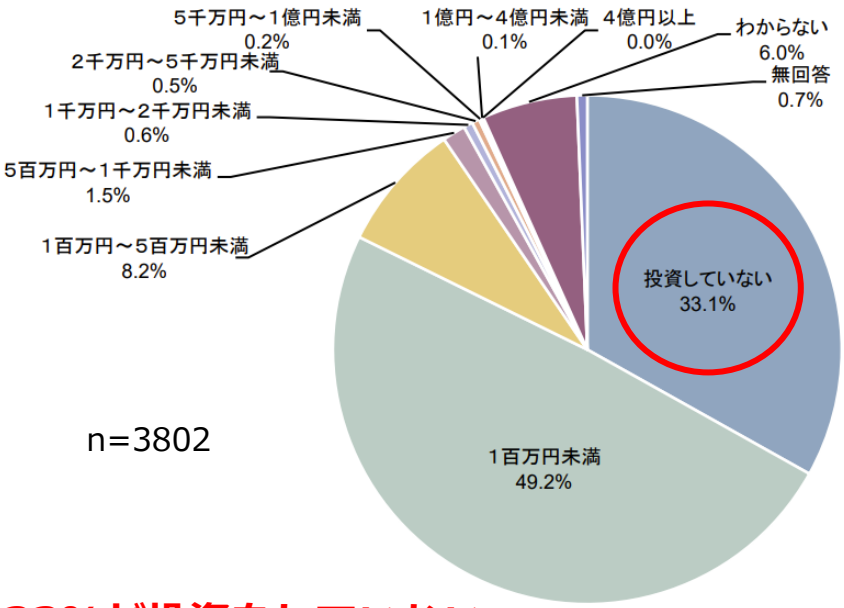
- 独立行政法人等のセキュリティ監査・監視事業
- 脆弱性対策促進事業
- セキュリティ対策の普及啓発事業
- セキュリティ対策の普及啓発事業（中小企業向け）
- 脅威動向やDX、新たな技術に関する調査・分析
- セキュリティ対策の普及啓発事業（IT利用者向け）

中小企業のセキュリティ事情の実態

AhnLab

直近過去３期の情報セキュリティ対策投資額

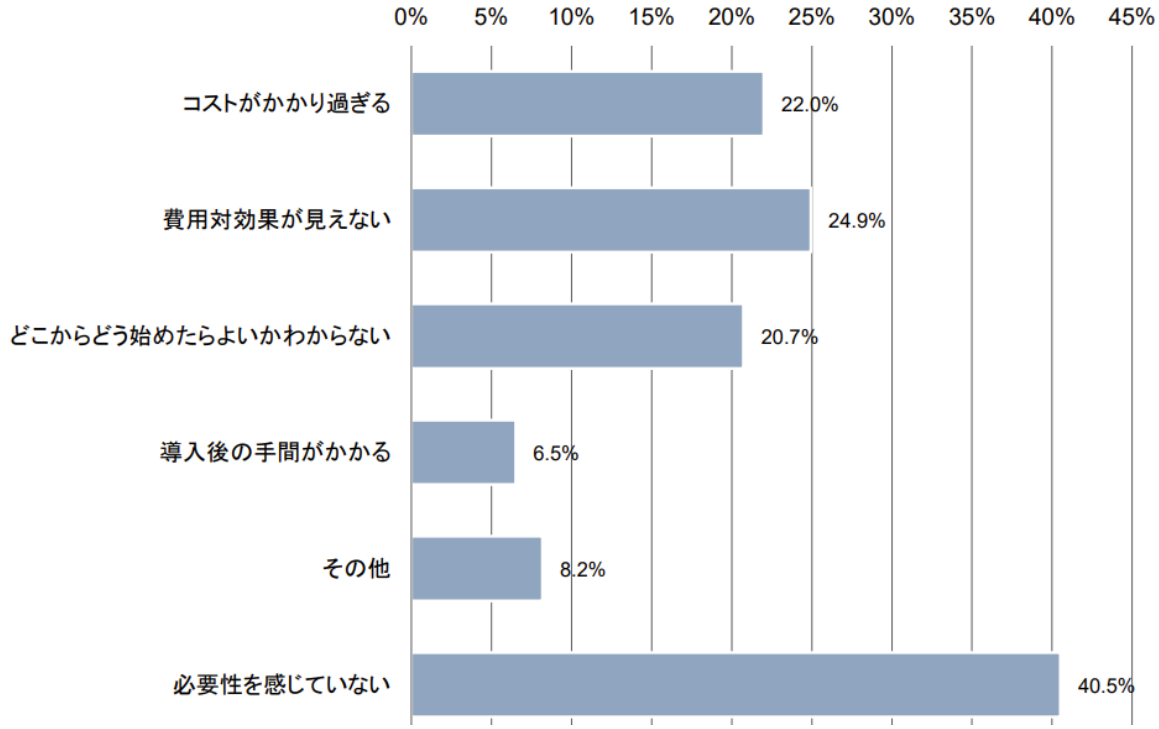
「投資していない」は何%？



n=3802

33%が投資をしていない
（＝対策が甘い、していない）

情報セキュリティ対策投資を行わなかった理由



n=1259

・コストがかかり過ぎる（一番上）
・必要性を感じていない（一番下）

コストの抵抗と意識が低い中小企業は一定数あり

2022年3月 独立行政法人情報処理推進機構 (IPA)発表

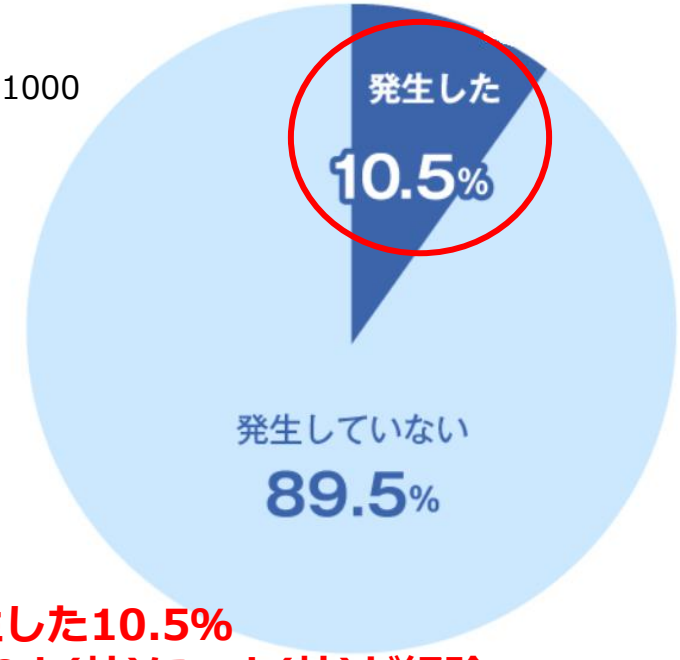
中小企業のセキュリティ事情の実態

AhnLab

中小企業でのセキュリティ事故・トラブル

過去3年間（2018 年 10 月～ 2021 年 9 月）の間、セキュリティ上の事故やトラブルを経験した中小企業従業員は何%？

n=1000



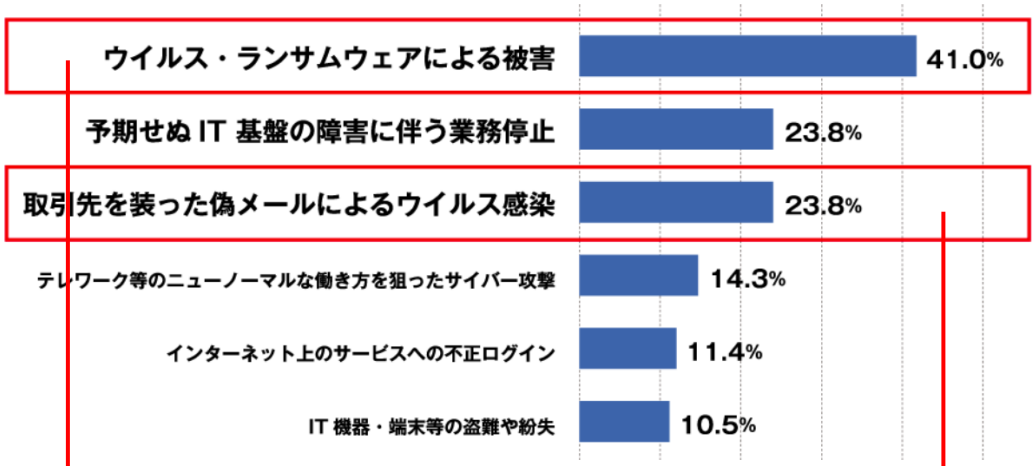
発生した10.5%
約10人(社)に一人(社)が経験

【参考】日本の中小企業数：約360万社

中小企業でも起こっている

2022年3月 独立行政法人情報処理推進機構 (IPA)発表

おもなセキュリティ事故・トラブルの内容



ウイルス関連が上位

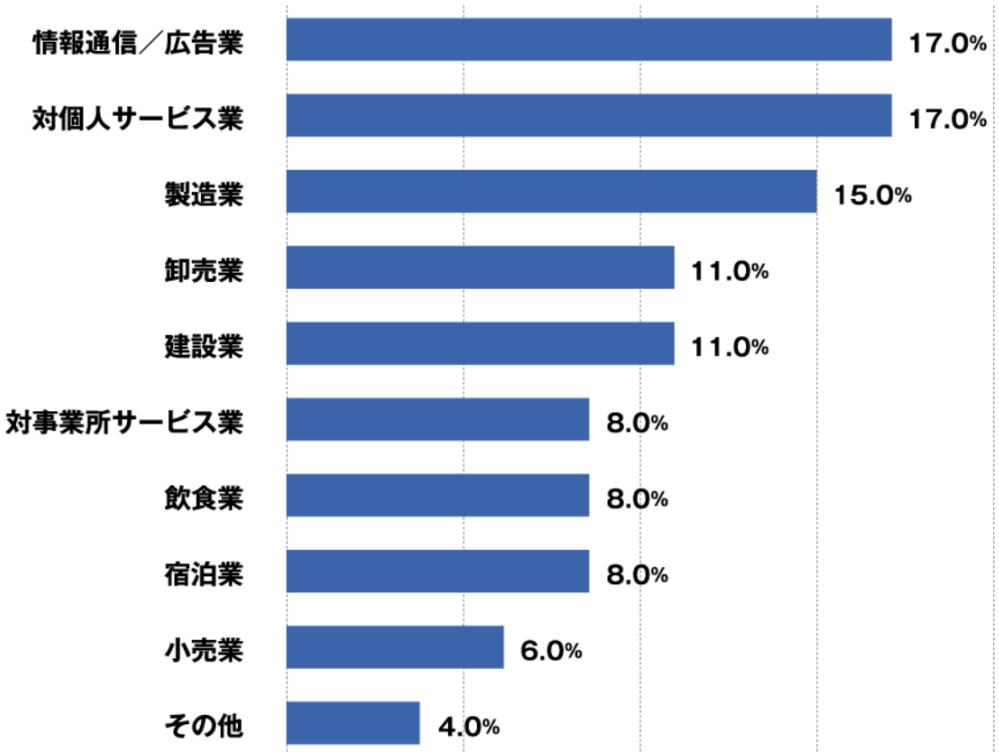
デバイスを利用できない(暗号化等)状態とされ、解除と引き換えに金銭や、機密情報等を要求

システムへ侵入され各種情報の詐取行為等の被害
- 顧客、取引先情報（流出）
- システムアカウント情報（乗っ取り）
- 従業員情報（流出、なりすまし）
- 技術、IR、業務情報（流出、恐喝）

中小企業のセキュリティ事情の実態

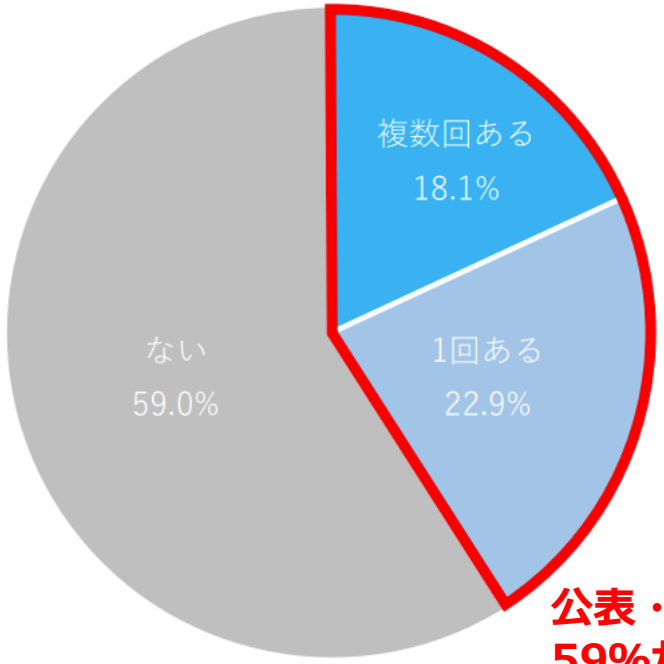
AhnLab

過去3年業種別、事故・トラブル発生率



中小企業での事故やトラブルの公表・公開

社外への公表・公開等（プレスリリース や、HP等への掲載等で）を行ったと答えた中小企業は何%？



公表・公開した41%
59%が公表・公開せず

状況、内容にもよるが、事故事実の公表はビジネスリスクや信用問題につながるため、公表せずに済ませたいとの考えが一般的

2022年3月 独立行政法人情報処理推進機構 (IPA)発表

中小企業のセキュリティ事情の実態

AhnLab

報告事例は氷山の一角。
事故発生時、公表・公開の機会が少なく経営者、担当者が身近に感じられない状況

テレ朝news
FOLLOW US
テレ朝newsを検索
トップ | ウクライナ | 速報 | 社会 | 政治 | 経済 | 国際
トップ ＞ 経済 ＞ 記事
コクヨ　エーザイ　“サイバー攻撃”被害相次ぐ　身代金要求型
[2023/06/08 11:29]

NHK
NEWS WEB


サイバー攻撃被害 データ復旧に高額請求トラブル相次ぐ 注意を
2022年12月16日 21時25分

ニュース
エーザイがランサムウエア被害を公表、複数サーバーが暗号化
渥美 友里　日経クロステック／日経コンピュータ
2023.06.06

主要 | 国内 | 国際 | 経済 | エンタメ | スポーツ | IT | 科学 | ライフ | 地域
トヨタでさえ起きる「顧客情報漏洩事故」…“情報漏洩”や“サイバー攻撃”に備えて入るべき「保険」とその「4つの補償」
5/13(土) 11:01 配信
幻冬舎 GOLD ONLINE

インシデント・事故
JBグループのシーアイエスにランサムウェア攻撃、個人・企業情報含む一部データが外部流出
JBグループで企業の基幹システム開発やクラウドサービスの提供を行う株式会社シーアイエスは6月29日、同社サーバへの不正アクセスについて発表した。
CIS

NHK
NEWS WEB
FUJITSU
サイバー攻撃で通信内容流出 富士通に行政指導 総務省
2023年6月30日 19時05分

インシデント・事故
新潟大学のメールサーバに不正アクセス、151万件の迷惑メール送信の踏み台に
国立大学法人新潟大学は6月22日、不正アクセスによる迷惑メールの送信について発表した。
新潟大学

SaaS Select with ITreview
マイナンバー漏えいの可能性明かす企業も　社労士向けシステムへのランサムウェア攻撃、ユーザーへの影響広がる
2023年06月19日 12時40分 公開
[吉川大貴，ITmedia]

主要 | 国内 | 国際 | 経済 | エンタメ | スポーツ | IT | 科学 | ライフ | 地域
貨幣処理機大手「グローリー」、不正アクセスで情報漏えい…種類や件数は「調査中」
7/5(水) 23:51 配信
讀賣新聞 オンライン

ランサムウェアに感染、個人情報流出の可能性 - IDOM
中古車販売のガリバーを運営するIDOMは、同社サーバがランサムウェアに感染し、保有する個人情報が外部に流出した可能性があることを明らかにした。

セキュリティ対策意識が低い事例

AhnLab

①中小企業は狙われない。狙われるのは大手企業

- 規模の小さい中小企業も攻撃の対象に十分なり得る
- 対策が甘い中小企業を狙い、そこを踏み台として大企業を襲う攻撃方法が近年増加
- 取引先の事故発端となる可能性があり、その場合取引先等に対し多額の賠償請求や調査請求が発生

②個人情報を扱っていないからあまり気にならない

- 企業が持つ重要な情報は個人情報だけではない
- 人事、取引先、IR、技術、セキュリティ(防犯)、契約等、企業が守る情報は多岐に渡る
- セキュリティ対策は個人情報の取扱い有無のみで考え決めるものではない

③業務用PC・スマホで怪しいサイトにアクセスしないから大丈夫

- メイン銀行のネットバンクやECサイト、オフィス用品購入サイトを装った悪質サイト詐欺被害が急増
- 正規サイトとまったく同様の画面で作りこまれた偽サイトに気づかず使用したことで
  会社のID、パスが抜き取られ多額の金銭被害あり
- 偽サイトは見た目では気づけないほど近年では巧妙化。システム的防御が必要

④中小企業でセキュリティ事故を起こしたところを見たことがない

- 状況や内容にもよるが、セキュリティ事故の発生を公表する企業はそう多くない
- 情報漏洩やセキュリティの脆弱さから事故を起こし、多額の支払い発生は周囲には伝えずらい
- 事故事実の公表はビジネスリスクや信用問題につながるため、隠したいとの考えが一般的。
  とはいえ、起こした事象に関連する各所への報告は必須

アンラボ製品でのセキュリティ対策

AhnLab

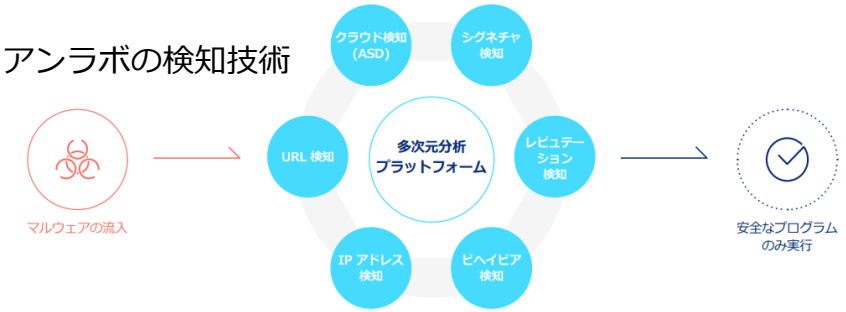
①『マルウェア』対策

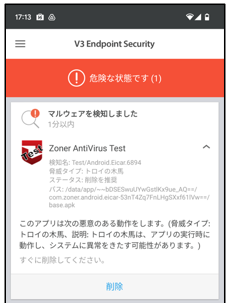
Windows　mac OS　android

マルウェアとは？　パソコンやスマホに**様々な種類、手法**で不利益をもたらす悪意あるソフトウェア

総称	種類（代表例）	特徴	おもな被害	おもな感染経路
マルウェア	ウイルス	意図的に被害を及ぼすプログラム。 ファイルやプログラム(宿主)に感染 しそれが実行されることで活動、増殖	急増 ・PCの使用不可、破壊、 ・社内情報の改ざん、消去 ・金銭、情報の要求 ・重要情報の略奪、盗聴 ・乗っ取りによる遠隔操作、なりすまし ・取引先等の第三者への攻撃	・メール等メッセージツール内URLアクセス、添付ファイル開封 ・ウェブ閲覧 ・ファイルインストール ・不正アプリ ・外部媒体 ・社内ネットワーク
	ランサムウェア	暗号化され使用が不可に。 解除と引き換えに金銭を要求される		
	ワーム	ウイルスと似ているが、ファイルや プログラム(宿主)がなくても活動、増殖		
	トロイの木馬	無害の画像ファイルや文書ファイル、 スマートフォンのアプリなどに偽装し、 内部へ密かに侵入し攻撃		
	スパイウェア	情報の収集、詐取を目的として、 気づかれないように侵入する		

アンラボの検知技術





6種の技術でスピーディーかつ正確に分析・検知を実行

アンラボ製品でのセキュリティ対策

AhnLab

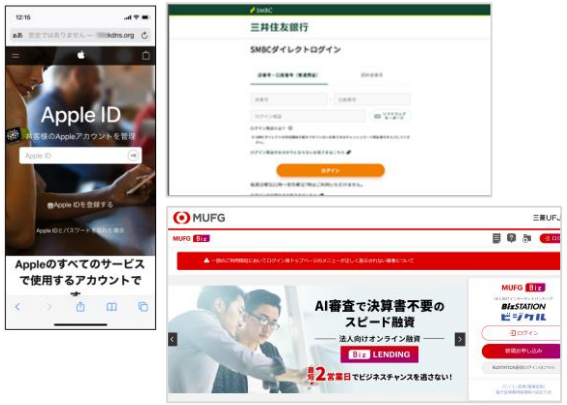
②Web遮断管理（フィルタリング）

Windows　mac OS　android　iOS

不正、不要なサイトを遮断し外部からの悪意ある攻撃や流入、フィッシングサイト等から守る

悪意のあるプログラムの侵入を狙った偽警告

巧妙につくり込まれた偽サイト

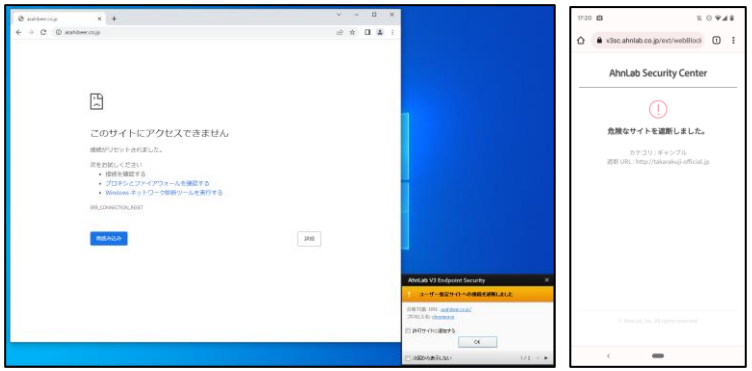


業務用スマホでの不要なアクセス、データ通信

- アダルト
- 動画
- ギャンブル
- 違法
- ゲーム

URLから瞬時に悪性を判断して遮断を実行

- 危険を瞬時に判断
- 部署単位の設定可能
- スマホ遮断履歴確認
- 簡単ON/OFF設定



- 「許可」「遮断」のサイトを個別に設定可能
- スマホはカテゴリごとに遮断選択可能
- アプリ内にある危険URLも検知
- スマホのプランデータ超過対策にも有効

アンラボ製品でのセキュリティ対策

AhnLab

③紛失・盗難時対策

android　iOS

「位置情報」の機能を活用して紛失時、盗難時に必要な対策が取れる

Android		iOS	
・位置情報の取得 ・端末初期化 ・画面ロック ・電話発信 ・アラーム発動とメッセージ送信	※スマホでロック設定時 ※管理画面から発信可	・位置情報の取得 ・端末初期化 ・画面ロック ・電話発信	※MDM加入時 ※MDM加入、スマホでロック設定時

GoogleMapにて位置とおおむねの住所が表示

検索履歴確認が可能

※画像はAndroidでの検索時

アンラボ製品でのセキュリティ対策

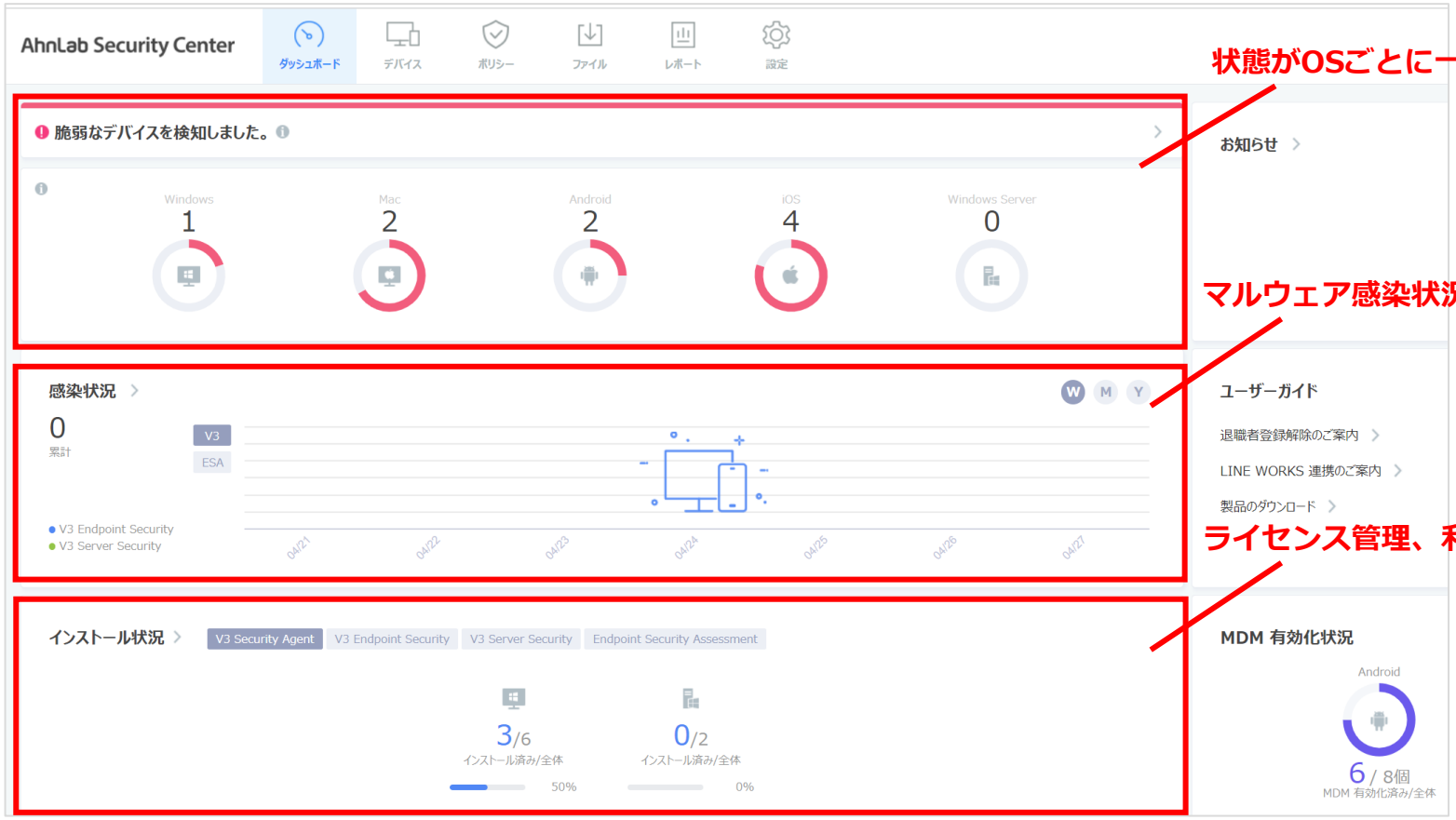
AhnLab

④管理画面からの一元管理

Windows　mac OS　android　iOS

管理者用の管理画面よりすべてのOS、デバイスの運用、設定状況を一元管理できる

ログイン後のトップ画面はダッシュボードが表示



状態がOSごとに一目でわかる

マルウェア感染状況も即時に確認ができ対応

ライセンス管理、利用状況確認も手間がかからない

ダッシュボードはとにかく
シンプル。
直感的に操作が可能

アンラボ製品でのセキュリティ対策

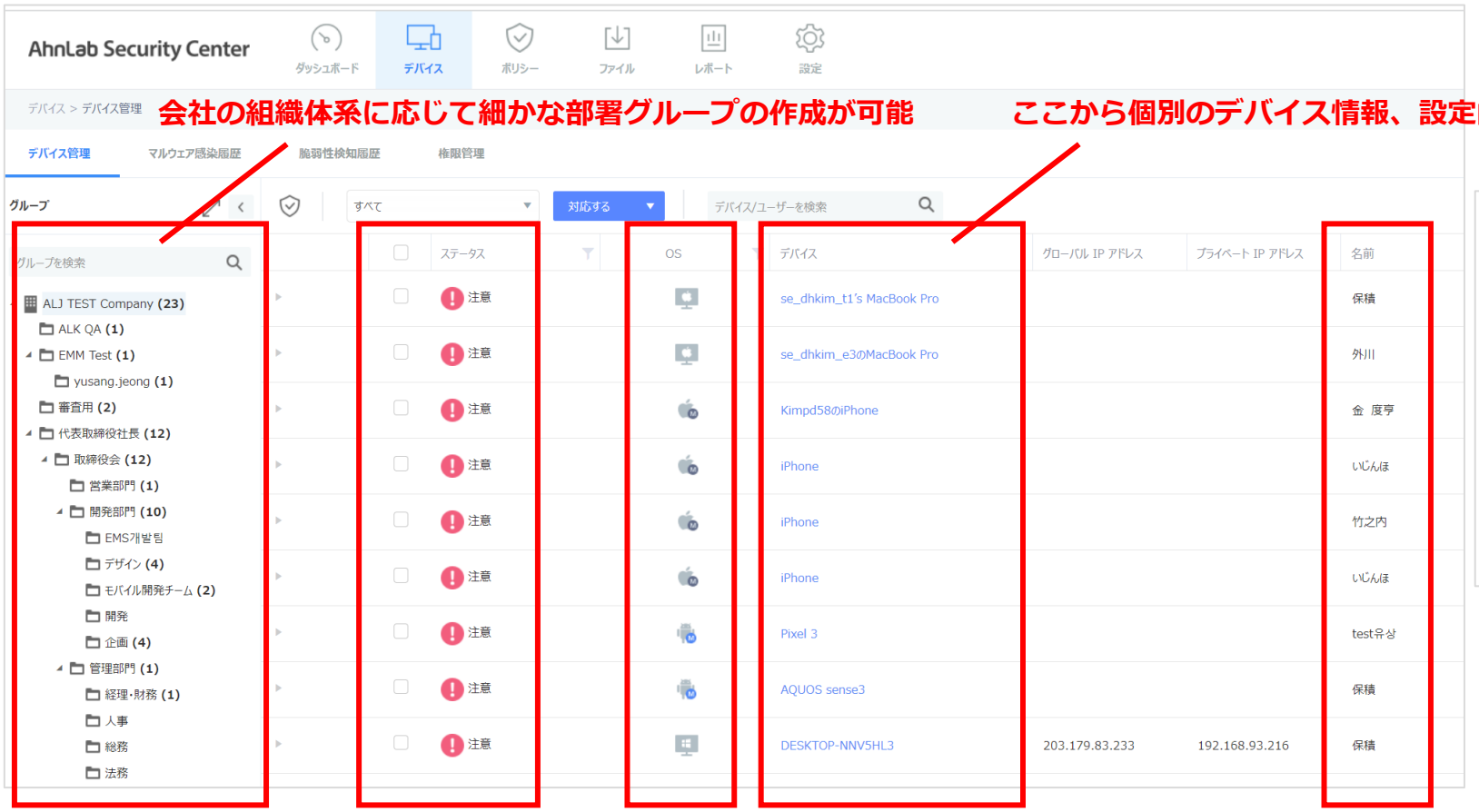
AhnLab

④管理画面からの一元管理

Windows　mac OS　android　iOS

管理者用の管理画面よりすべてのOS、デバイスの運用、設定状況を一元管理できる

登録デバイス一覧画面



会社の組織体系に応じて細かな部署グループの作成が可能

ここから個別のデバイス情報、設定内容が個別に確認できる

【個別情報画面】

部署、チームごとにデバイス一覧を表示。
これも見やすくわかりやすい

一目で状況が確認

OSをわかりやすく表現

ユーザー情報編集も簡単

アンラボ製品の強み

AhnLab

①シンプルを追究した中小企業に向けた製品で軽い

複雑さを排除し、「とにかくシンプル、誰にでもわかりやすく」をコンセプトとしている。
過剰機能はなく、中小企業に必要な機能をすべて網羅。他メーカーと比べて速度低下なしで軽い

②マルウェア検知、収集力

マルウェア、サイバー攻撃の標的、発祥地は中国、韓国、日本が世界でも上位。
すべてに法人拠点があることで収集と検知対策のスピード感が早い

③マルウェア対策とフィルタリング対策が1製品で同時に取れる

マルウェア対策とフィルタリングを同時に開発、実装している製品は他メーカーにはない。
（URLからマルウェアを検知やi-Filter社と連携したフィルタリング展開は他社あり）

④プラン、オプションも多岐に渡らずシンプルなワンプラン

ワンプランで中小企業に必要な機能を実装。複雑で複数のプラン・オプションなし

⑤MDMも自社開発で一元管理が可能

現在MDMは機能拡充、利便性向上に向けて開発対応中　※次ページ参照

アンラボ製品の強み　セキュリティとMDMの一元管理機能の提供開始　2022年～　AhnLab

管理画面が統合された効率的一元管理が可能

- 社内のセキュリティとMDMの管理がひとつの管理者用画面内で行える
- 管理画面が統合されることで、効率的に一元管理、運用が可能！
- 画面がシンプル、操作が簡単で誰でも容易な製品設計

会社全体の運用効率化、経費削減につながる

- 社内導入ツール自体の管理・運用も効率化！
- 今までセキュリティとMDM、それぞれ別に利用料支払していたものが一本化され契約管理、更新対応が効率化、かつ安価のため経費が削減できる
- 従業員のデバイス登録、入社・退職・人事異動処理等での発生業務が一元化され管理運用人件費削減にもつなげることが可能に！

他社にはない

セキュリティの脅威対策と業務用モバイルの管理を
ワンストップ簡単運用

安全なセキュリティ環境を簡単構築！

中小法人向け
セキュリティマネジメント

＋ **一体型製品**

業務用スマートデバイスを効率的に管理！

MobileDeviceManagement
(MDM)

ガチガチの“管理”、“制御”はしたくない、できない、する必要ない、といった中小法人向け

「使わない過剰な機能は不要」といった多くの中小法人向けに必要な機能のみを簡単、わかりやすく

おもな機能

- 紛失、盗難時対応（遠隔ロック、遠隔初期化）
- 位置情報取得
- パスコードロックポリシー作成
- 複数ポリシーグループ作成
- アプリー括配信、削除(Android)
- ブラックリスト/ホワイトリスト(Android)
- 機能制限（カメラやスクリーンショット、端末ロック等）
- 会社所有端末と個人所有端末のすみ分け管理（BYOD利用時）
  他

現在、パートナー要望等から機能の拡充に向け順次対応中

※OSにより機能が異なる場合がございます

ターゲット（＝中小企業の担当者によくあるケース）

AhnLab

このような経営者、担当者の気を引いて商談化を狙う

コスト	セキュリティ製品は支払っているコストが適正なのか、相場感はいくらなのか、見直しの余地、必要があるのか、を気にしていない。コスト削減に貪欲
機能・性能	導入している製品の使い方が実はわからない、使いずらいけどどれもそんなものかなと思っている、機能が多すぎて逆に困っている
中小法人最適化	自社の規模に最適な製品なのかわからない、規模の大きい企業と同じ製品を導入しているのが不安、大手ほどの対策レベルではなく自社の規模にあった対策をしたい
サポート	何かあったときに今の製品メーカの対応が不安、会社規模からか問い合わせ対応が雑な気がする、営業は売ったら売りっぱなし
無関心	現在導入がない、現在導入してる製品の価格、機能、効果等気にしていない、とりあえず導入はしているが放置状態で良い悪いもわからない、スマホでも対策が必要であることの認識なし

商談化のケース事例に関して

AhnLab

	課題	ケース	事例
コスト	**契約更新間近による見直し**	更新間近による製品見直しの検討	現行より安価な提案を行えた
	コストの見直し、削減	コスト削減は通年の課題で現行と比較したい	現行より安価な提案を行えた
	現在かけているコストが適正か不明、または正確な金額を知らない、無関心	この機会に一度現行コストを把握して見直しを検討したい	現行より安価な提案を行えた
	既存のセキュリティソフトがマルチデバイスに対応していない（iOSが対応の法人ソフトがない）	スマホ、PC、タブレットすべて一元管理をしたい。支払いを一本化したい	マルチデバイスに対応しており、PCもモバイルも一元管理で脅威から守る運用が可能
機能・性能	**使い勝手に不満**	既存セキュリティソフトが複雑でわかりずらく使い勝手が悪い	大手製品の場合、インターフェースや設定、操作が複雑なものもあり、使いやすさを重視で乗換
	業務に負担をかけずに運用したい	社内のIT関連業務を複数掛け持ちしているため、セキュリティ管理、運用の業務負荷を軽減させたい	専門部署構築や人材確保せず、ライセンスの購入だけで容易にセキュリティ環境を構築できる。また、直感的に操作可能なわかりやすい管理者用サイトで簡単運用
	会社が小規模のため個人用のセキュリティソフトを使っている（購入代金は会社で負担）	従業員各自が個人向けのソフトを購入しそれぞれがバラバラに使用している（経費で従業員個人に任せている）	個人用ソフトの利用では管理、統制が取れず、更新もバラバラになるケースが多いことから法人用製品にて商談化
	現在マルウェア対策とフィルタリングは別々のサービスを利用している	統合された製品を知らない	統合させた製品導入により効率化とコスト削減が可能な提案

商談化のケース事例に関して

AhnLab

	課題	ケース	事例
中小法人最適化	**不要な機能が多く自社にマッチしない（スペシャルな機能は不要）**	不要な機能が多く、使い切れていないため自社に合う必要な機能のみ搭載の製品を要望	中小法人に必要な機能はすべて搭載。中小企業には不要な細かすぎる設定等なく使いやすい
	自社が中小規模法人のため、自社の規模に適した製品を検討したい	エンタープライズ向けの製品として大手企業の導入実績が多くあるものは中小規模である自社に適しているのか不安	中小規模法人向けに使いやすいよう研究、設計で他社と差別化
	商品選定、検討にかかる負担が大きい	複数の複雑なプランやオプションが多くあり、社内検討作業が煩雑で負担が大きい	アンラボは他社と同一の機能が搭載されてワンプランのため検討もスムーズ
	セキュリティソフトを未導入	セキュリティソフトの必要性を感じていない。実際の脅威に直面したことがないため、さまざまな脅威があることの認識不足	未導入による自社で持つ技術、取引情報、従業員情報、社内運用情報等の窃取や破壊、改ざんリスク。導入による各種リスクの回避や、取引先への信用、従業員の安心を得られる提案
	スマホ対策が必要であることを未認識	スマホは現在対策をしていない。（必要だと思っていなかった）	業務用スマホも外部攻撃の脅威や、不正、不要サイトへのアクセスによるリスク、不都合が存在することを理解いただいた
サポート	**既存サポート体制への不満**	既存セキュリティソフトのサポート体制がよくない 例：メールのみの対応、レスポンスが遅い、電話窓口がつながりずらい、オペレーターや担当営業の態度、受付時間、等	アンラボでは貴社に対して含め、営業担当、技術担当が状況に応じて柔軟に対応をいたします