法人向け統合型セキュリティソリューション「V3 Security for Business」のご紹介

AhnLab

Agenda

01 株式会社アンラボ概要

02 ご提案の背景

03 V3 Security for Businessの製品紹介

AhnLab

株式会社アンラボ概要

AhnLab

株式会社アンラボ

AhnLab

韓国本社概要

- 1995年 総合セキュリティ・ソリューション・プロバイダとして創業
- 韓国のサイバーセキュリティ市場にてシェア60%以上 (2024)のトップベンダー
- 韓国の銀行では８割以上がセキュリティ対策でアンラボ製品を導入
- Global企業を含めた契約社数：25,000社～
- 韓国内の金融向モバイルアプリ (V3 Mobile Plus) 利用者は約3,000万人～

日本オフィス

- 商号　　：株式会社アンラボ
- 所在地　　：東京都港区芝4-13-2　田町フロントビル３F
- 資本金　　：1億円
- 設立　　：2002年2月
- 事業内容　：個人及び法人向けサイバーセキュリティソリューションの提供

Global Employee

AhnLab

計 1,278 名

全体の 70%以上が R&D に集中

2024年7月基準

企業コアコンピタンス – 統合セキュリティプラットホーム

AhnLab

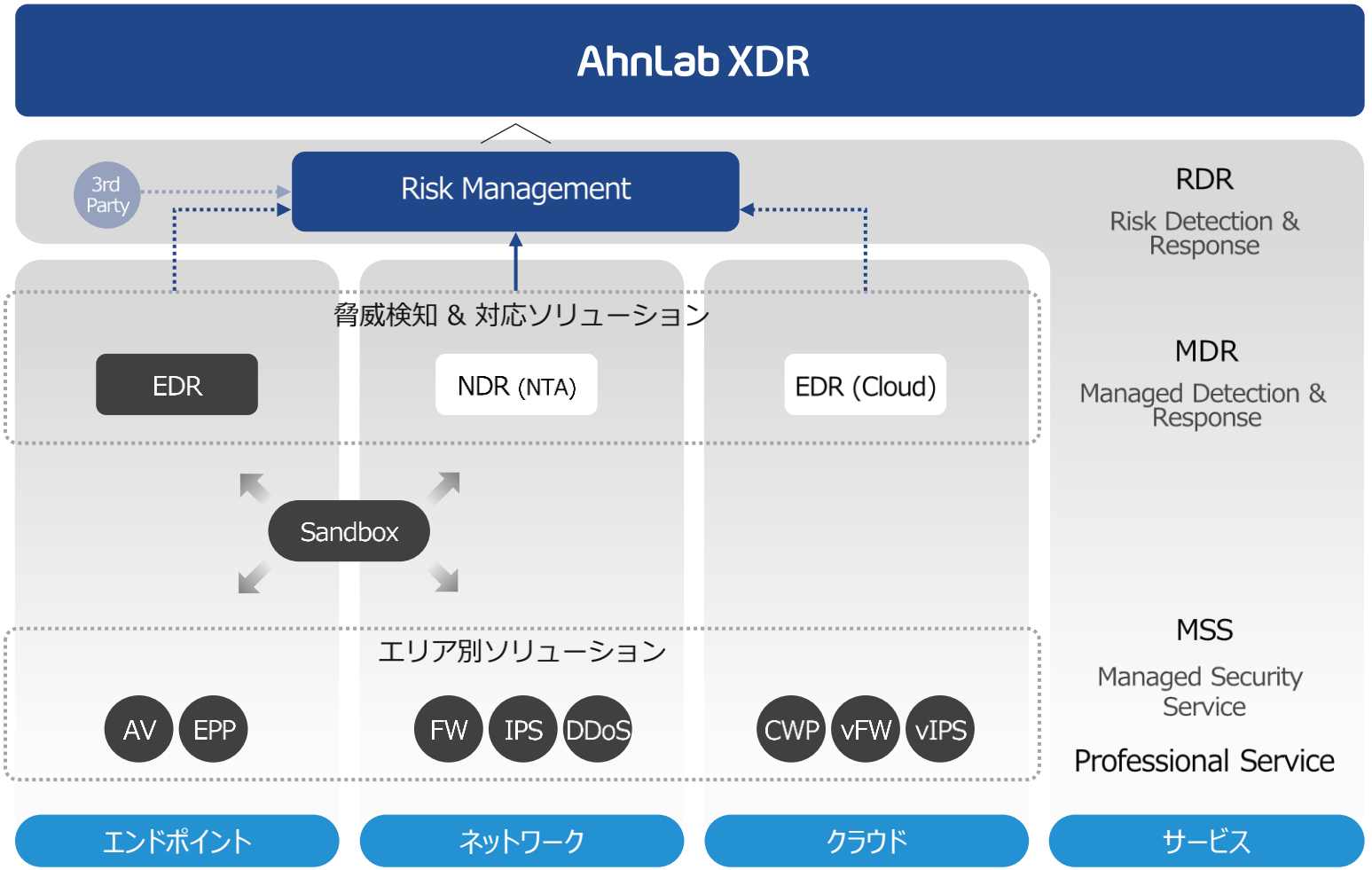
保護対象はエンドポイント、ネットワーク、クラウド

ビジネス全体を守れるプラットフォーム

03 予測および推奨

02 分析および追跡

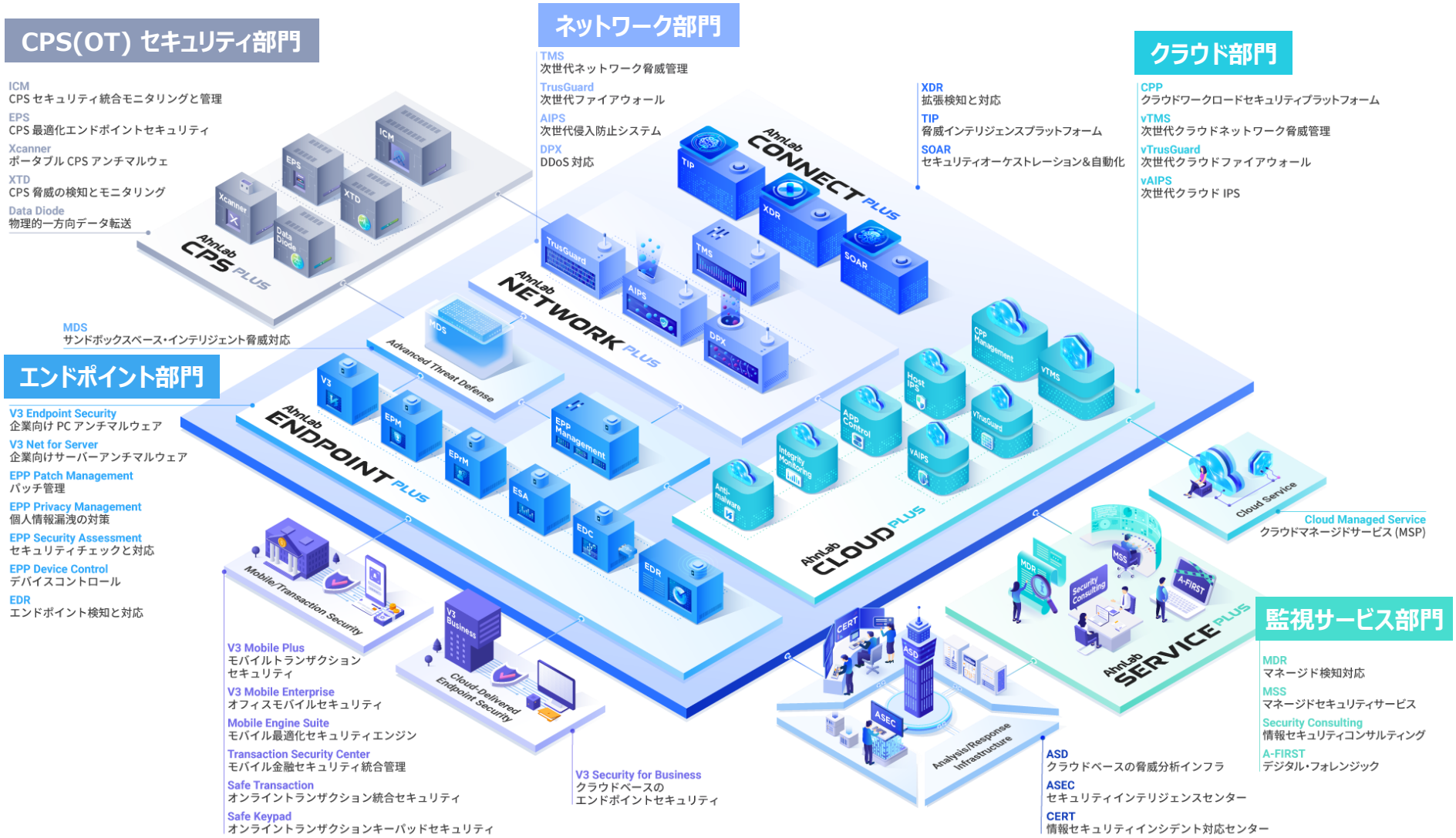
01 遮断および制御



AhnLab　セキュリティマップ

AhnLab

総合セキュリティ・ソリューション・プロバイダとして約40のソリューションを提供



国内事業展開

AhnLab

国内の金融機関でも利用されている製品

AhnLab

■金融機関へのサイバーセキュリティサービスの提供

日本の80社以上の金融機関へ
サイバーセキュリティサービスを提供しています。

MIZUHO みずほ銀行

埼玉りそな銀行

りそな銀行

NEOBANK 住信SBIネット銀行

JCB 世界にひとつ。あなたにひとつ。

TOKYO STAR BANK 東京スター銀行

MUFG 三菱UFJニコス

常陽銀行

and more…

日本国内の金融機関
80社以上

SaT Netizen
ネットバンク専用セキュリティ対策ソフト

AhnLab ソリューションのご紹介　BtoC

AhnLab

■個人のお客様へ　サイバーセキュリティ対策ソフトの提供

量販店、EC、コンテンツプロバイダ、MVNO事業者(ODM)などを通じ
個人向けセキュリティソフトを提供しています。

脅威を検知

負担の軽さ

万が一の紛失対策

プライバシー保護

Best Advanced Protection
2023 Award

※イオンモバイル様

AhnLab ソリューションのご紹介　BtoB(SMB)

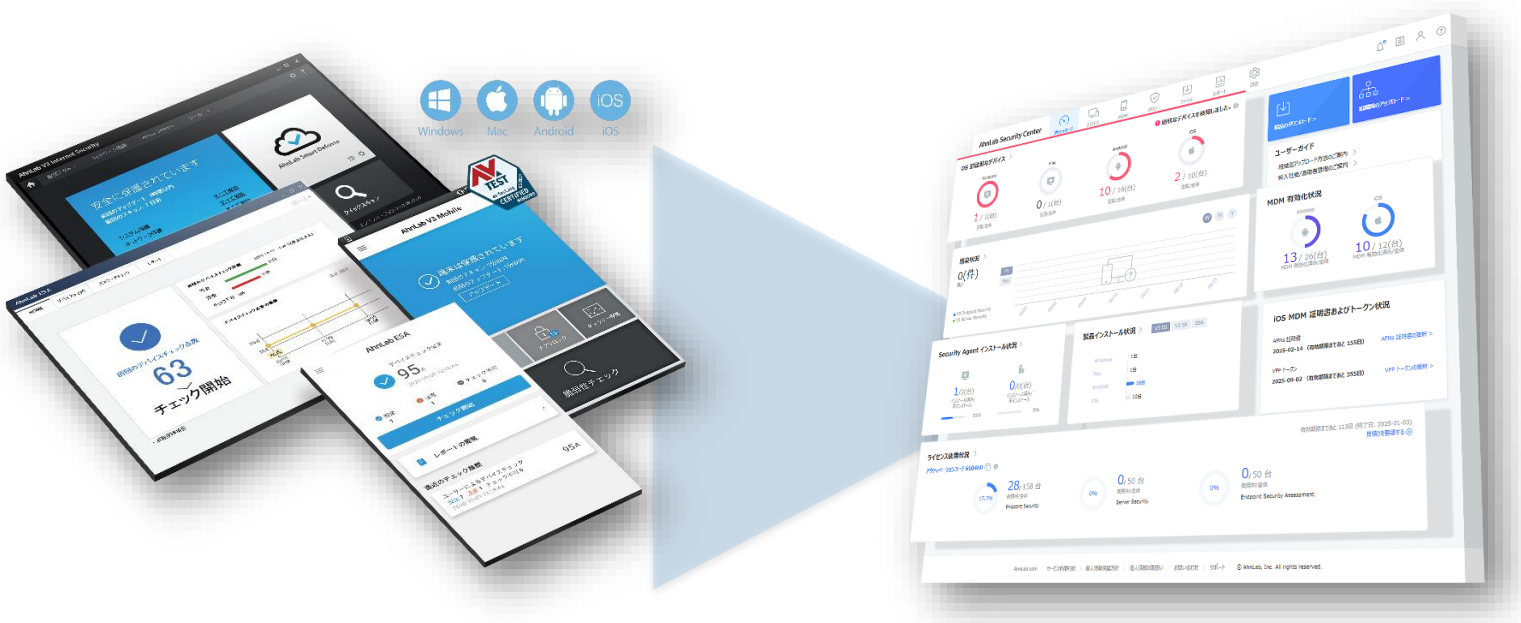
AhnLab

■法人のお客様へ　統合型セキュリティ対策ソリューションの提供

ディストリビュータ、携帯販売代理店、SIerなどを通じ
法人向け統合型セキュリティソリューションを提供しています。

① ウイルス対策
② WEBフィルタリング
③ MDM(モバイルデバイスマネジメント)

統合 → AhnLab V3 Security for Business



AV-TEST av-test.org 2023 AWARD BEST ADVANCED PROTECTION AhnLab V3 Endpoint Security

Best Advanced Protection 2023 Award

AhnLab ソリューションのご紹介　BtoB(CPS)

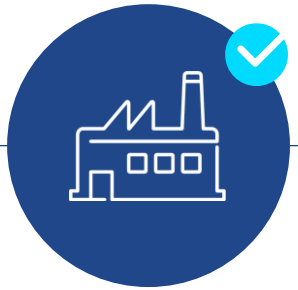
AhnLab

■ICS(特殊制御システム)、インフラ、IoT機器に対する セキュリティソリューションの提供

ディストリビュータ、デバイス商社、SIerなどを通じ
CPS領域に対するセキュリティソリューションを提供しています。

金融

ATM
決済システム (POS)



デジタル生産設備

半導体
ディスプレイ
家電
自動車生産自動化設備

医療

病院処方システム
各種医療機器

公共インフラ

電力、水道、ガス、
などの設備制御システム、
無人の各種証明書発行機、
信号制御システム

その他

KIOSK、
交通情報を表す電子掲示板など

ご提案の背景

AhnLab

求められる企業内サイバーセキュリティ対策

AhnLab

すべての法人(業務利用)で利用されるPC、スマートフォン、タブレット等デバイスが対象で
サイバー攻撃が年々増加傾向、手口も巧妙化し業務停止や金銭の詐取も発生

【参考】情報セキュリティ10大脅威2025（組織）　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	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサム攻撃による被害	2016年	10年連続10回目
2	サプライチェーンや委託先を狙った攻撃	2019年	7年連続7回目
3	システムの脆弱性を突いた攻撃	2016年	5年連続8回目
4	内部不正による情報漏えい等	2016年	10年連続10回目
5	機密情報等を狙った標的型攻撃	2016年	10年連続10回目
6	リモートワーク等の環境や仕組みを狙った攻撃	2021年	5年連続5回目
7	地政学的リスクに起因するサイバー攻撃	2025年	初選出
8	分散型サービス妨害攻撃（DDoS攻撃）	2016年	5年ぶり6回目
9	ビジネスメール詐欺	2018年	8年連続8回目
10	不注意による情報漏えい等	2016年	7年連続8回目

特に中小企業で増加

- ランサム攻撃による被害：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や情報を要求し脅迫
- サプライチェーンや委託先を狙った攻撃：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。自社ではなく取引先等の関係各所が脅威に晒される
- 機密情報等を狙った標的型攻撃：メール等を利用し特定組織のPCをウイルス感染させ長期にわたり侵害範囲を徐々に広げ組織の機密情報窃取やシステムの破壊を行う
- ビジネスメール詐欺：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

セキュリティリスクは年々高まる一方。巧妙化する攻撃に対し、
大手企業のみならず中小規模の企業も万全のウイルス対策が必要不可欠

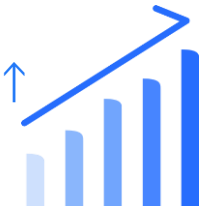
サイバー攻撃の対象は大企業のみならず、中小企業も対象に

AhnLab

ランサムウェア被害が37%増加

中小企業におけるランサムウェア被害は約37%増加
被害の長期化・高額化も進む

約37%↑



※警察庁調査参照

国内中小企業におけるサイバー攻撃の経験

中小企業の内、サイバー攻撃を受けた経験があると
回答したのは約20%

約20%

※帝国データバンク調査参照

世界的傾向：中小企業への標的シフト

世界的な数値では、中小企業でサイバー攻撃を受け
た経験があると回答したのは約44%

約44%

※Dell調査参照

中小企業を踏み台にするサプライチェーン攻撃

大企業のサイバーインシデントの内、サプライ
チェーン攻撃とされるものは約48%

約48%

※KPMG調査参照

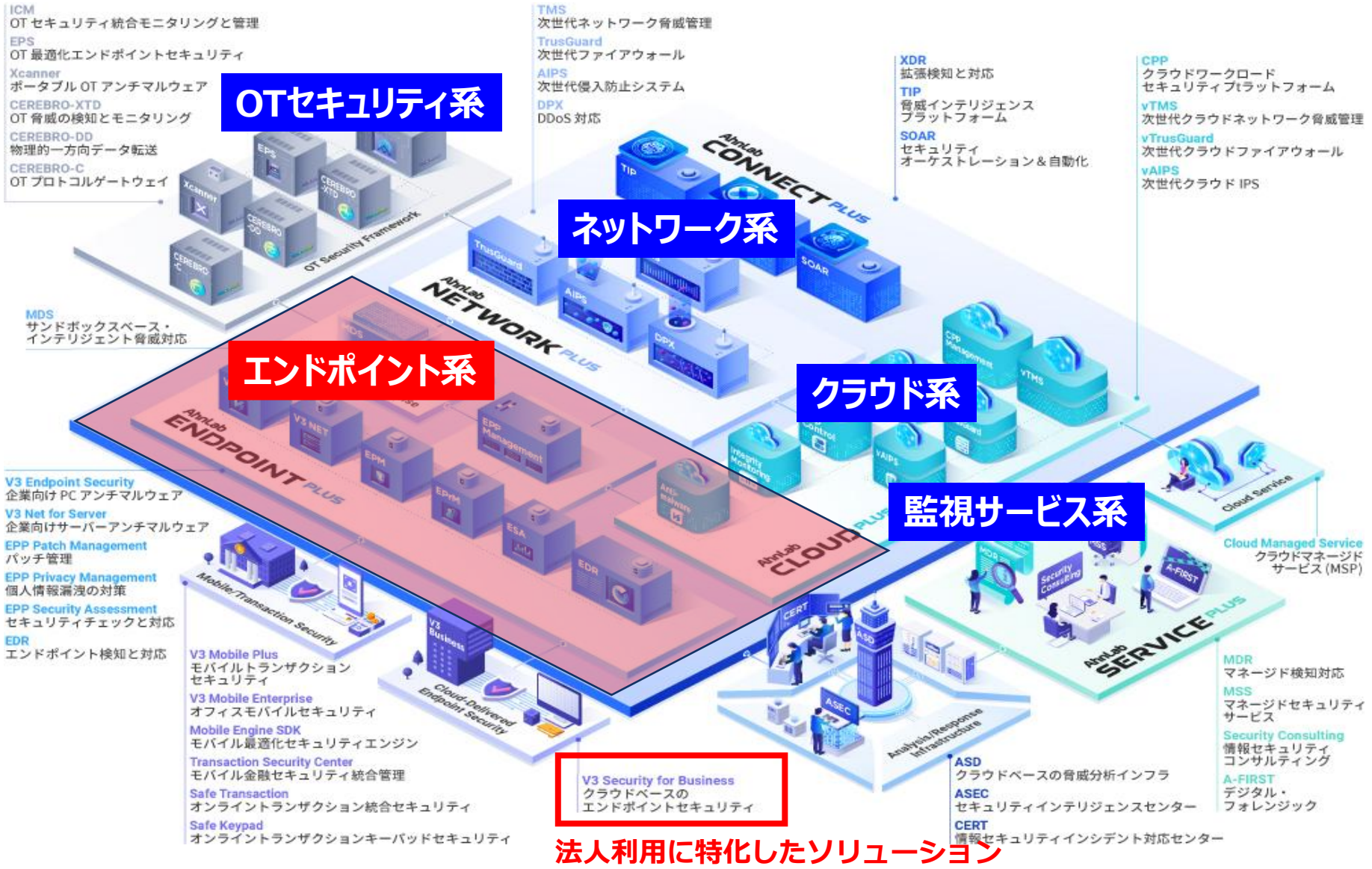
AhnLab V3 Security for Business
製品紹介

AhnLab

AhnLabのサービス展開(グローバル)

AhnLab

日本国内では一部のソリューションのみ提供しております



法人利用に特化したソリューション

アンラボ法人向け統合型セキュリティのご紹介

AhnLab

法人向けのセキュリティマネジメントにモバイルデバイス管理(MDM)をプラス

AhnLab V3 Security for Business

法人向けセキュリティマネジメントとして開発された製品。

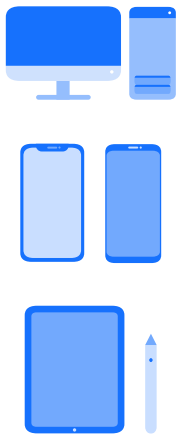
エンドポイントセキュリティ＋モバイルデバイス管理(MDM)で
管理担当者の業務負荷を軽減

法人向け

ビジネス利用通信デバイスの管理・運用・対策　【課題】

AhnLab

現在多くの法人様でのPC、モバイル関連ソリューション導入状況



管理、運用、対策項目	導入ソリューション / 製品	
マルウェア、ウイルス対策	「●●セキュリティー」	A社製
Webフィルタリング	「●●フィルター」	B社製
MDM（モバイルデバイスマネジメント）	「●●マネージャー」	C社製
IT資産管理	「●●クラウド」、Excel管理	D社製

各種管理、運用、対策にそれぞれのソリューションを契約して導入、利用

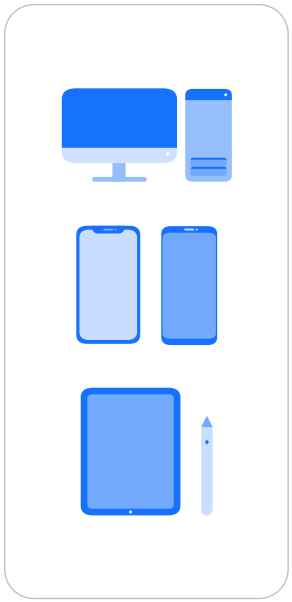
発生していること

- 複数のシステム、ツール契約、導入、利用状況管理
- 複数の利用料金支払い処理
- 入社、異動、退職、部署新設、部署統合等に関わる複数のユーザー情報更新作業
- 複数の利用マニュアル管理や製品問い合わせ時の複数の問い合わせ先窓口管理
- 管理担当者変更時の複数システム、ツールの引継ぎ対応

ビジネス利用通信デバイスの管理・運用・対策　【解決】

AhnLab

管理・運用・対策に必要な機能が統合され業務の効率化、コストの削減が見込める製品



管理、運用、対策項目

- マルウェア、ウイルス対策
- Webフィルタリング
- MDM（モバイルデバイスマネジメント）
- IT資産管理

統合

導入ソリューション　/　製品

マルチな機能が実装されワンストップ

AhnLab V3 Security for Business

中規模くらいまでの法人様向けに開発

必要なソリューションが統合された製品

解決すること

- システム、ツール契約、導入、利用状況の管理負担減
- 利用料金支払い処理も複数から1箇所(1社)へまとまる
- 入社、異動、退職、部署新設、部署統合等に関わる複数のユーザー情報更新作業も1回のみ
- 利用マニュアル、製品問い合わせ窓口も一つで完結
- 管理担当者変更時の複数システム、ツールの引継ぎも一つで完結

アンラボ法人向け統合型セキュリティでの管理・対策

AhnLab

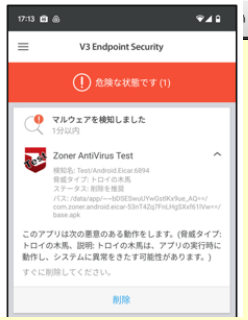
- セキュリティとMDMが一体化され同一の管理画面で一元管理
- マルウェア・ウイルス対策からアプリの制御・一斉配信、紛失時対策等ワンストップ簡単運用
- セキュリティ対策にはフィルタリング機能も含まれておりデバイスを徹底コントロール

AhnLab V3 Security for Business（クラウド型） ※下記は一部機能

セキュリティ管理・対策

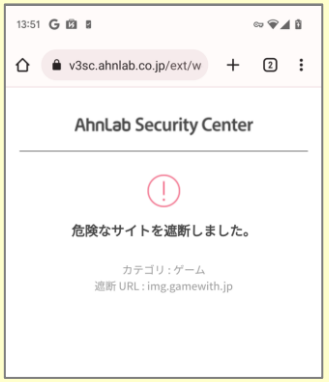
マルウェア・ウイルス対策

インターネットやアプリを介するさまざまなマルウェアをスキャン、駆除



フィルタリング(Web遮断管理)

悪意のあるサイトへのアクセスや業務に不要なサイトへのアクセスを防止

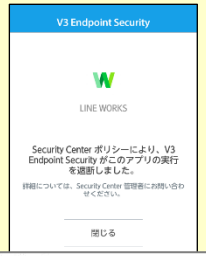


PC、スマホ、タブレット、サーバー

Windows
Android
iOS
Mac
iOS

MDM(モバイル管理)

アプリ制御、配信、紛失対策、デバイス機能制御等、法人デバイスをコントロール



スマホ、タブレット

Android
iOS
iOS

※OS、デバイスによって対応する機能や操作方法は異なります

本製品で可能な主な対策(1)『マルウェア対策』

AhnLab

業務利用のデバイス（スマホ・タブレット・PC）をマルウェア（ウイルス）から守る

マルウェア・・・悪意を持って作られたプログラム　⇒　おもにメールやインターネットを介して侵入

感染時の代表的な被害例

- ✓ **デバイス起動不可**
  復旧には高いリテラシーを持った人もしくは専門業者への依頼が必要
- ✓ **ファイルの消失・破壊**
  失ったファイルを取り戻すには手間とコストがかかる可能性大。
  確実に取り戻せる保証がない
- ✓ **社内ファイル・データへの侵入**
  社内ファイル・データへ侵入され書き換え、改ざん・消去をされる。
  そのことに気づけないケースも多い
- ✓ **情報の流出・搾取**
  人事データ、取引先データ、財務データ、技術データ、
  セキュリティ(防犯)データ、契約データなど抜き取られる
- ✓ **取引先、業務委託先を標的**
  自社ではなく取引先や業務委託先を攻撃するために侵入、攻撃。
  他社のセキュリティ事故の発端、原因とされてしまう。
- ✓ **企業データの不正暗号化**
  企業のデータを不正暗号化した上で、復旧と引き換えに
  金銭等の要求事項で脅迫

おもな目的

- 愉快犯
- 業務妨害

- 要求(金銭等)
- 情報横流し
- 企業信用低下

増加

マルウェアを駆除

マルウェア感染履歴も確認できる

V3 Security for Businessの多層防御

AhnLab

従来のシグネチャベースの検知に加え、NGAVの要素も加わった ハイブリッド方式のエンドポイントセキュリティ

多次元分析プラットフォームの最新検知技術を通じてスピーディーかつ正確に分析でき、未知の新種・亜種のマルウェアまで検知することができます。

URL / IP アドレス検知

·不正な URL および IP アドレスを事前に遮断し、インターネットを介して流入するマルウェアによる被害を予防します。

クラウド検知

·クラウドベースの ASD (AhnLab Smart Defense) 技術および ASD ネットワークを介してリアルタイムで脅威情報を共有し、多様な新種の脅威に迅速かつ正確に対応することができます。

シグネチャ検知

·ASD DB に蓄積されている 7億個の不正なファイル情報を通じて、より迅速で効果的な診断ができます。

レピュテーションおよびビヘイビア検知

·レピュテーションおよびビヘイビア検知技術により、未知のファイルやプログラムの潜在的な脅威を事前に遮断します。新種/亜種のマルウェアや検知を回避するマルウェアを検知し対応します。

マルウェア対策　グローバル認証の取得

AhnLab

アンラボ製品はセキュリティ製品のグローバル第三者評価機関等より毎回高得点の評価を得ています

AV-TEST The Independent IT-Security Institute Magdeburg Germany

ドイツのセキュリティ製品性能評価最大手機関

Windows(個人向け、企業向け)、Androidともに最新マルウェアの検知率評価では
常に高得点を獲得し毎回認証を取得、2023年度最優秀保護部門賞獲得。

---

virus BULLETIN Covering the global threat landscape

イギリスのアンチウイルス製品評価専門誌

AhnLab

Virus Bulletin が実施した 「VB100 認証付与テスト」 で検知率100%を記録。
さらに「多様性テスト」 において99.9%の検知率を記録

他社マルウェア対策製品との比較(AV-TEST)

AhnLab

AV-TEST The Independent IT-Security Institute Magdeburg Germany

2024年６月
最新認証テスト**満点**獲得！（参加メーカー16社）
(各項目6点満点、総合18点)

2023年度
WW年間最優秀製品賞
受賞

		Protection	Performance	Useability
AhnLab	V3 Endpoint Security 9.0	6	6	6
CHECK POINT	Endpoint Security 86.60	6	6	6
eset Digital Security Progress. Protected.	PROTECT Advanced 11.0	6	6	6
TREND	Apex One 14.0	6	6	6

大手ベンダーでも満点取れていないケースも

Symantec. A Division of Broadcom	Endpoint Security Complete 14.3	6	5.5	6
Microsoft	Defender Antivirus (Enterprise) 4.18	5.5	6	6
cybereason	NGAV 23.2	4	6	6
Trellix	Endpoint Security 10.7	6	6	5.5

本製品で可能な主な対策(2) 『Webフィルタリング』

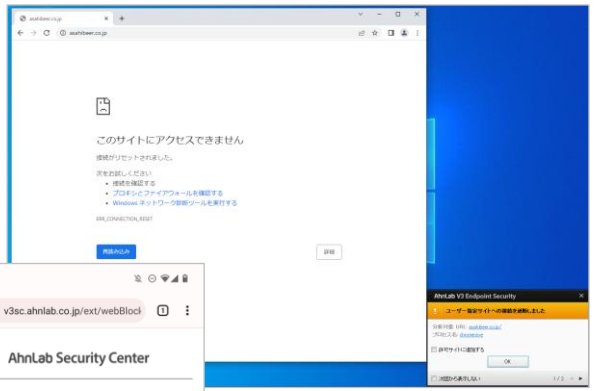
AhnLab

業務に不要なURL(サイト)や従業員に不適切なURL(サイト)へのアクセスを防止

✓ フィッシングサイトへのアクセス防止

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。
偽サイトも巧妙化(偽物だと気づけない)しておりウイルス感染や情報搾取
されてしまう企業被害が拡大

瞬時にURLから判断して遮断を実行



プログラムの侵入を狙った偽警告(例)

巧妙につくり込まれた偽サイト(例)

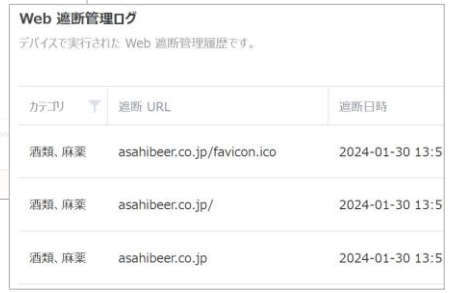
✓ 業務用での不適切なサイトへのアクセス防止（カテゴリごとに設定可能）

業務に不適切なサイトアクセスによる詐欺被害、ウイルス感染のリスクや
無駄なデータ通信を防ぐ

モバイル端末はカテゴリごとに遮断/許可の設定が可能です。
左記カテゴリは一部の例となります

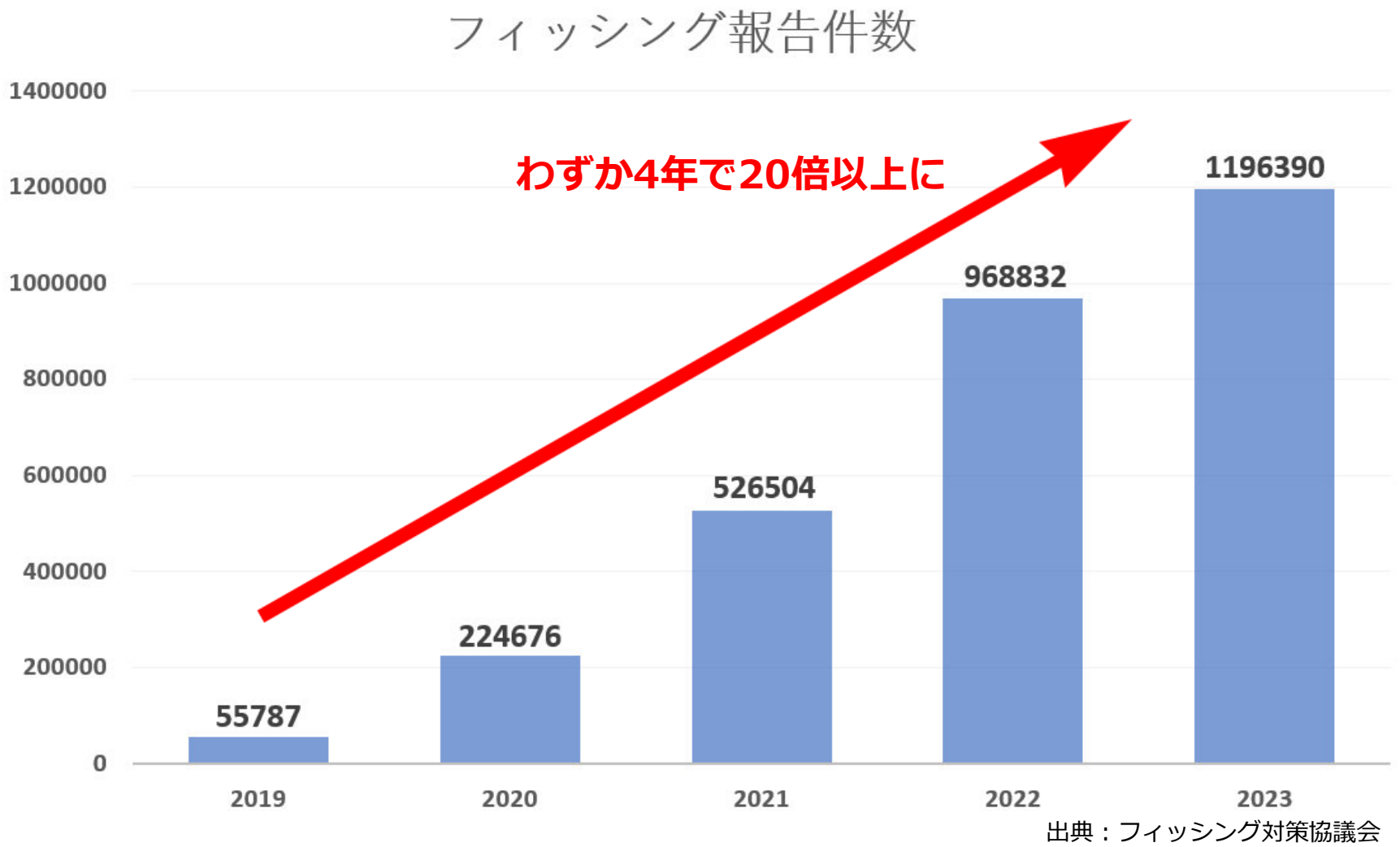
アダルト	動画	ゲーム	ダウンロード
ギャンブル	出会い系	暴力	酒、麻薬

遮断ログ確認機能



急速に増加しているフィッシング報告件数

AhnLab



出典：フィッシング対策協議会

フィッシングの認知が広まった為、報告件数が増加している事もあるが
巧妙化するフィッシングに対する対策も求められているのが実情

本製品で可能な主な対策(3) 『MDM』

AhnLab

セキュリティ対策と同時にモバイル管理（MDM）

Android			iOS	
アプリインストール制御	インストールアプリ閲覧	アプリ利用許可/遮断設定	画面ロックパス設定強制	アプリインストール制御
画面ロックパス設定強制	アカウント設定制御	データローミング許可/遮断	アプリ配信(一斉配信可)	インストールアプリ閲覧
Wi-Fi接続制限	オーディオ機能許可/遮断	Bluetooth機能制御	アプリ利用許可/遮断設定	アカウント設定制御
アプリ配信(一斉配信可)	端末初期化制御	カメラ利用の許可/遮断	App内課金不可	Safari利用制御
テザリング利用制御	SDカード利用制御	スクショ機能許可/遮断	Appストア利用制御	MDM自動インストール
Wi-Fi接続制御	USB接続データ転送制御	Playストア利用制御	カメラ利用の許可/遮断	Bluetooth機能制御
IMEI、回線番号情報取得	初期化制御		スクショ機能許可/遮断	Wi-Fi接続制御
			IMEI、回線番号情報取得	初期化制御

※上記は一部機能例となります。OSによって対応している機能は異なります。

盗難、紛失対策

Android	
・位置情報の取得 ・位置情報の軌跡取得 ・端末初期化 ・画面ロック ・電話発信 ・アラーム発動	※スマホでロック設定時 ※管理画面から発信可
iOS	
・位置情報の取得 ・位置情報の軌跡取得 ・端末初期化 ・画面ロック ・電話発信 ・メッセージ送信 ・画面ロックパス削除	※スマホでロック設定時 ※管理画面から発信可

「複雑かつ使わない過剰で細かすぎる機能は不要」といった多くの中規模までの法人向けに、必要な機能のみを提供

管理者の管理・運用業務負担増や、利用者の利便性低下を懸念する等で、極端な管理までは不要とお考えの企業様に最適です

ご利用用途に合わせたご提供形態 Android

AhnLab

デバイスの利用想定に合わせて必要な機能のみお申込みいただけます

android

No.	お申込み形態	主な機能			
1	セキュリティのみ	ウイルス対策	フィルタリング	位置情報取得	Root化チェック
		インストール済みアプリの制御　※１	ポップアップメッセージ送信	アラーム鳴動	リモートロック　※２
2	セキュリティ＋MDM (仕事用プロファイル) **※端末初期化不要**	上記１すべて	アプリ配信	Playストアからのアプリ制御　※３	画面ロック設定の強制
		Wi-Fi接続制限	Googleアカウント利用制限	野良アプリインストール制御	仕事用プロファイルリモート初期化
3	セキュリティ＋MDM (完全管理デバイス) **※端末初期化必要**	上記２すべて	インストールアプリ情報取得	VPN設定制御	データローミング制御
		Bluetooth利用制限	NFC利用制限	デバイスの初期化制限	リモート初期化

※１　Playストアの制御も可能です

※２　端末ロックパスコード設定時

※３　アプリの許可もしくは遮断設定(ホワイトリスト/ブラックリスト)

例えば・・・
ウイルス対策、フィッシング対策、位置情報の取得を検討なら『No.1』を
初期化は行いたくないが、アプリ制御等MDMの機能を利用したい場合は『No.2』を
機種変更の際など、全方面で管理・運用を行いたい場合は『No.3』と、お選び頂けます！

ご利用用途に合わせたご提供形態 iOS

AhnLab

デバイスの利用想定に合わせて必要な機能のみお申込みいただけます

iOS

No.	お申込み形態	主な機能			
1	セキュリティのみ	フィルタリング	Root化チェック	位置情報取得	ポップアップメッセージ送信
2	セキュリティ＋MDM (プロファイルモード) **※端末初期化不要**	上記１すべて	カメラの使用制限	iCloudバックアップ制限	Touch ID、Face ID利用制御
		信頼できないHTTPS証明書によるアクセス	App内課金制御	ロック画面でのControl Center表示制限	リモート初期化
3	セキュリティ＋MDM (監視モード※１) **※端末初期化必要**	上記２すべて	VPPアプリ配信	アプリ制御※２	画面ロック設定の強制
		インストールアプリ情報取得	Wi-Fi接続制限	Bluetooth利用制限	デバイス初期化制限

※１　ABMの登録と端末のDEP化が必要です

※２　アプリの許可もしくは遮断設定(ホワイトリスト/ブラックリスト)

例えば・・・
フィッシング対策や不要なWEBアクセス防止、位置情報の取得を検討なら『No.1』を
初期化は行いたくないが、簡易MDM・リモート初期化まで利用したい場合は『No.2』を
機種変更の際など、全方面で管理・運用を行いたい場合は『No.3』と、お選び頂けます！

アンラボ統合型セキュリティの管理者メリット

AhnLab

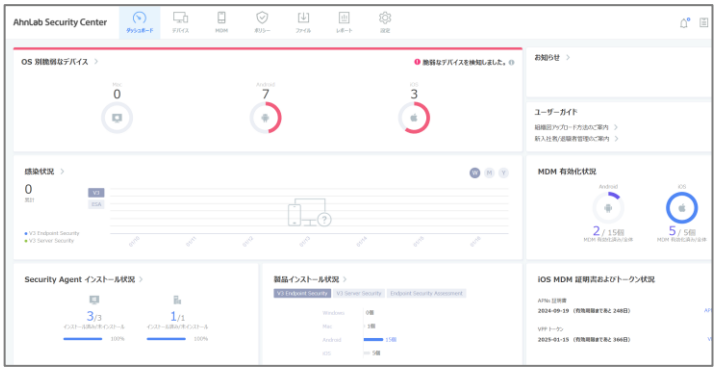
いつでもどこでもアクセス可能な管理者用Webサイトをご提供いたします

シンプルインターフェースで
容易な管理・運用

PC、モバイルセキュリティ
紛失、盗難時のリモート対応
MDM管理、制御

一目でわかる直感的なダッシュボードや
各種設定画面

直感的に状況を確認、把握



いつでもどこでも便利に
セキュリティ、MDM管理

管理者用Web マネジメント
ユーザー一括登録、一元管理

直感的でわかりやすい管理者用Webサイトで
ユーザー情報をExcelでかんたんに一括登録することが可能

Microsoft Excel
ワークシート

アンラボ統合型セキュリティの管理者画面(ダッシュボード)

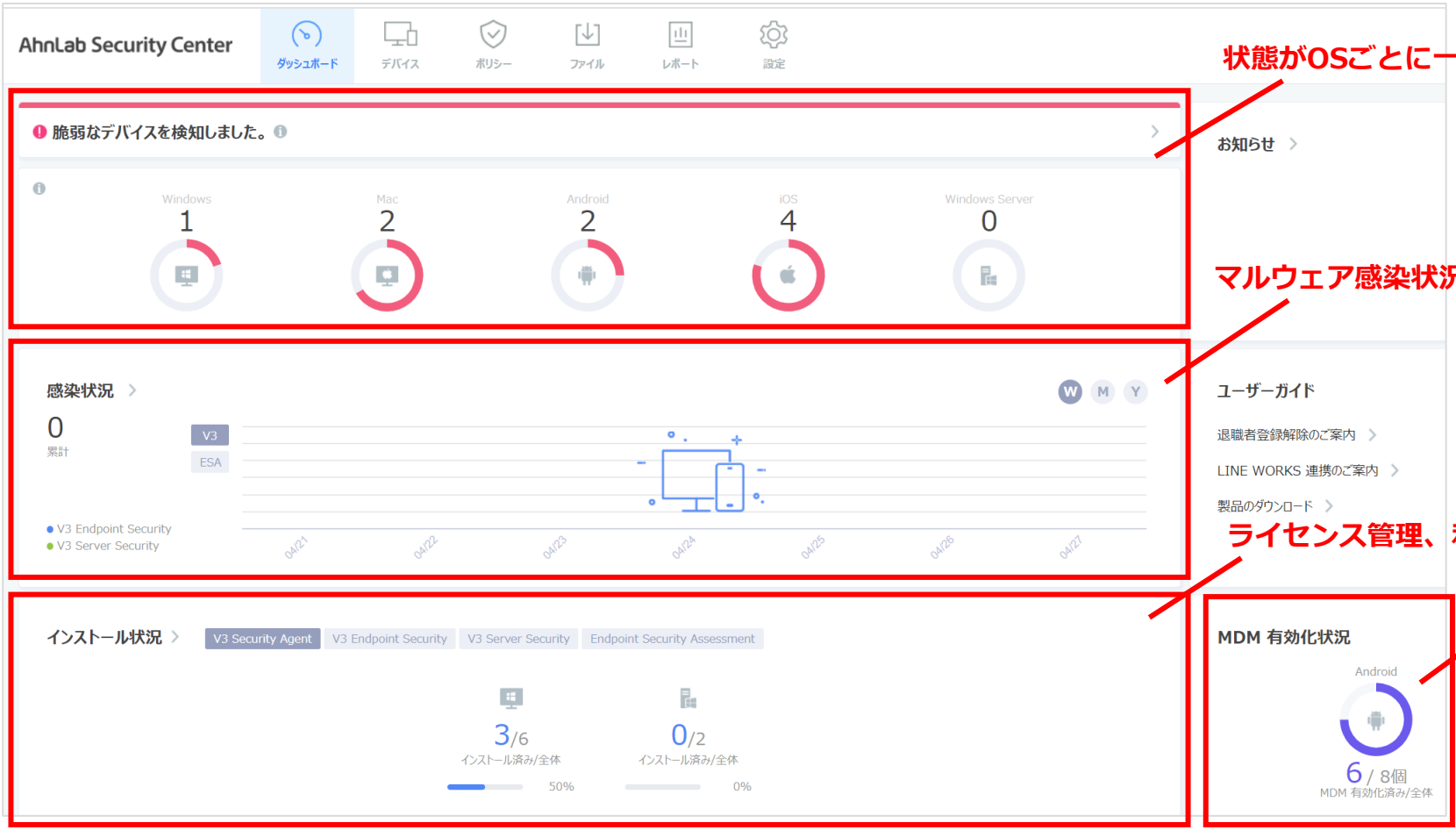
AhnLab

管理画面でのデバイス状態管理

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

MDM有効化の状態が確認でがきデバイスへの適用を漏れなく確認

アンラボ統合型セキュリティの管理者画面(デバイス一覧)

AhnLab

管理画面での組織・ユーザー一元管理

Windows　mac OS　android　iOS

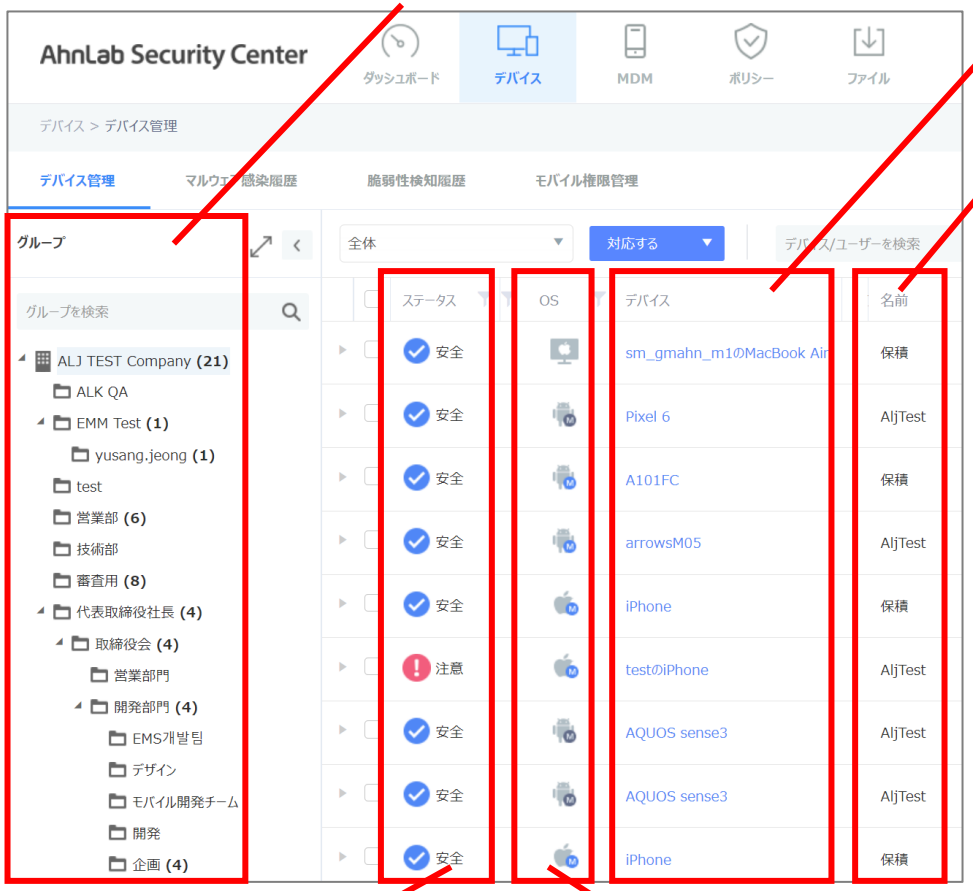
管理者用の管理画面より組織ごと、ユーザーごとにデバイス情報や状況確認、管理ができる

【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

ここからデバイス情報、設定内容が個別に確認できる

ユーザー情報編集も簡単



一目で状況を確認

管理OSをわかりやすく表現

【個別情報画面】

製品比較　法人向けエンドポイントセキュリティ

AhnLab

競合他社製品と比較し、特筆して可/不可な機能は御座いません

機能		AhnLab V3 Security for Business	Trend Micro VBBSS	ESET PROTECT Essential クラウド	ESET PROTECT Entry クラウド	WithSecure Elements Endpoint Protection	Webroot Business Endpoint Protection
対応OS	Windows	○	○	○	○	○	○
	macOS	○	○	○	○	○	○
	Android	○	○	○	○	○	×
	iOS	○	○	×	×	○	×
	Windows Server	○	○	○	○	○	×
	Linux	○	○	○	○	○	×
セキュリティ	総合ウイルス対策	○	○	○	○	○	○
	スパイウエア対策	○	○	○	○	○	○
	フィッシング対策	○	○	○	○	○	○
	迷惑メール対策	×	○	×	○	×	×
	有害サイト遮断機能	○	○	×	○	○	○
	ネットワーク侵入遮断機能	○	○	×	○	○	○
	URLフィルタリング	○	○	×	○	○	×
	USBデバイス対策	○	○	○	○	○	○
	OS起動時事前診断機能	○	○	○	○	×	○
	大規模感染防止(端末隔離)機能	×	×	○	○	○	×
	モバイルデバイス管理(MDM)	○	○	○	○	×	×
初期導入	管理者アカウント自動発行	○	○	×	×	×	×
	ライセンス自動活性化	○	○	×	×	×	×
	インストールファイル一括配布	○	○	×	×	○	×
デバイスコントロール(PC)	クライアント一括管理	○	○	○	○	○	○
	リモートスキャン	○	○	○	○	○	○
	リモートアップデート	○	○	○	○	○	○
	メール・メッセージ送信	○	○	○	○	○	○
	システム状況確認	○	○	○	○	○	○
	ポリシー管理	○	○	○	○	○	○
	インストールファイルの配布	○	○	○	○	○	○
レポート	期間別レポート出力	○	○	○	○	○	○
	グループ別出力	○	○	○	○	○	×
	予約出力	○	×	○	○	○	×
	宛先指定出力	○	○	○	○	○	○
サポート	電話サポート	365日 9-20	平日 9-18	平日 9-17	平日 9-17	平日 9:30-17:30	平日 10-18
	メールサポート	○	○	○	○	○	○

製品比較　MDM

AhnLab

サービス名		V3 Security for Business		MobiConnect	Optimal Biz	CLOMO MDM	SPPM3.0	LANSCOPE EP マネージャー	ビジネス・コンシェル デバイスマネジメント
開発元		アンラボ		インヴェンティット	オプティム	アイキューブド システムズ	AXSEED	エムオーテック	ソフトバンク
対応OS		Android	iOS	iOS Android	iOS Android	iOS Android	iOS Android	iOS Android	iOS Android
主なMDM機能 (主要抜粋)	Jailbreak/root化(不正改造)検知	○	○	○	○	○	○	○	○
	リモートロック	○	○	○	○	○	○	○	○
	リモートワイプ	○	○	○	○	○	○	○	○
	パスワード初期化	×	○	○	○	○	○	○	○
	端末のパスコード強制	○	○	○	○	○	○	○	○
	カメラ利用制限	○	○	○	○	○	○	○	○
	Bluetooth利用制限	○	○	×	○	○	○	○	○
	WiFi接続制限	○	○	○	○	○	○	○	○
	VPN制限	○	×	○	○	○	○	×	○
	デザリング利用制限	○	×	×	Androidのみ○	Androidのみ○	○	×	○
	USBポート利用制限	○	○	×	Androidのみ○	Androidのみ○	○	○	○
	URLフィルタリング	○	○	有償オプション/外部製品	有償オプション/外部製品	有償オプション/外部製品	有償オプション/外部製品	有償オプション	有償オプション/外部製品
	許可サイト指定	○	○	有償オプション/外部製品	有償オプション/外部製品	有償オプション/外部製品	有償オプション/外部製品	×	有償オプション/外部製品
	遮断サイト指定	○	○	有償オプション/外部製品	有償オプション/外部製品	有償オプション/外部製品	有償オプション/外部製品	×	有償オプション/外部製品
	カテゴリ指定遮断	○	○	有償オプション/外部製品	有償オプション/外部製品	有償オプション/外部製品	有償オプション/外部製品	有償オプション	有償オプション/外部製品
	遮断履歴確認	○	○	有償オプション/外部製品	有償オプション/外部製品	有償オプション/外部製品	有償オプション/外部製品	×	有償オプション/外部製品
	ブラックリスト	○	○	○	○	Androidのみ○	Androidのみ○	Androidのみ○	Androidのみ○
	ホワイトリスト	○	○	○	○	Androidのみ○	Androidのみ○	Androidのみ○	Androidのみ○
	アプリー括配信	○	○	○	○	○	○	○	○
	アプリストアー無効化	○	○	○	○	○	○	○	○
	アプリインストール無効化	○	○	Androidのみ○	○	○	○	○	Androidのみ○
	アプリ制御履歴確認	○	○	○	○	○	○	○	○
	インストールアプリ情報	○	○	○	○	○	○	○	○
	スクリーンキャプチャ禁止	○	○	×	○	○	○	×	○
	位置情報取得	○	○	○	○	○	○	○	○
	マルウェア対策	○	-	×	有償オプション/外部製品 Androidのみ	有償オプション/外部製品 Androidのみ	有償オプション/外部製品 Androidのみ	有償別サービス Androidのみ	外部製品利用 Androidのみ
	Apple Business Manager	-	○	○	○	○	○	○	○
	Android Enterprise	○	-	○	○	○	○	○	○
	プロファイル削除防止	×	○	iOSのみ○	iOSのみ○	×	×	×	iOSのみ○
	プロファイル削除検知	○	○	○	○	○	○	○	○

・本資料は公表されている他社情報をもとに独自で調査したものとなり、必ずしも資料内記載のとおりであることを保証するものではございません
・製品機能説明の表現、定義が各社異なるため、実際の操作によっては一部適用とならない機能がある場合がございます
・価格、利益に関する表記は想定のものとなり、実際のものとは異なる場合がございます
・各社の機能、価格等サービス全般に関して弊社では詳細をお答えすることはできません
・各社の機能、価格は予告なく変更となる可能性がございますので、詳細は貴社のご責任の範囲にて開発元にお問い合わせください

アンラボ法人向け統合型セキュリティのポイント

AhnLab

ポイント① 情報システム担当者不在の企業様でもご利用頂ける安心の操作性

- ✓ 複雑さがなくとにかくシンプル！知識に多少不安な方でも操作いただける
- ✓ 極端に高い制限レベルを求めた製品設計ではないため、機能が細か過ぎない
- ✓ 複数のプランやオプション等なく、ワンプランで必要なセキュリティ機能を実装

ポイント② 経費削減と業務効率化

- ✓ セキュリティ対策とMDM、それぞれ別導入するよりもコスト安（初回登録料や新規事務手数料等の初期費用なし）
- ✓ セキュリティとMDMの一体化で製品契約管理、請求管理、各種機能問い合わせ等の業務が効率化
- ✓ 入退社、異動、デバイスリプレイス等に伴うユーザー情報更新も一度にできて業務負荷軽減

ポイント③ PCやモバイルデバイスのサイバーセキュリティ対策をワンストップで提供

- ✓ 法人向けサイバーインシデント対策に最適な機能のみを選定して実装！不要な管理、手間が省ける
- ✓ デバイス機能の管理、制御を過剰なものとせず業務用デバイスの役割を最大限生かせる
- ✓ デバイス配布者の利便性維持と管理運用業務を最小限に留めたいと考える法人に最適

「**他社製品を利用中、多機能過ぎて不明な機能も多く複雑**」
「**ITリテラシーが無いため導入/運用に不安**」
「**必要最低限の導入しやすいセキュリティを求めている**」

多くの利用者様の声を反映し、複雑な機能は搭載せず、必要な機能のみを簡単、わかりやすく

導入前、導入後のサポートに関して

AhnLab

導入前

トライアルの提供

トライアル要望をお受けしております。
希望数量、期間のご連絡をお願い致します。（ご提供にはトライアル申込書が事前に必要となります）

トライアル申込連絡先
メール：jp.sales@ahnlab.com
お電話：03-6453-8315

導入後

電話対応窓口

・電話番号：03-6453-8320（法人のお客様専用窓口）
・受付時間：365日/9時～20時

お問い合せメールフォーム

・https://www.ahnlab.com/jp/overseas/support/qna
・受付時間：365日/24時間　※ご返信は365日/9時～20時

個別対応

お困りのことがございましたらお気軽に営業担当までご連絡ください。
状況や内容により技術担当のものがご対応をさせていただく場合がございます。