AhnLab

V3 Security for Business

スマートオフィス環境のためのセキュリティマネジメントソリューション

個別デバイスの保護からポリシーの中央管理まで
サーバーや特別な投資の要らない効率的なセキュリティ管理ソリューション

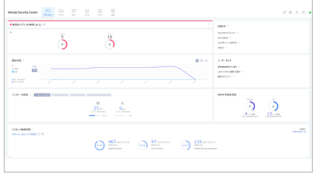
製品紹介

AhnLab V3 Security for Business は、ASD Cloud Threat Intelligence により、ランサムウェアやゼロデイ攻撃をリアルタイムで検知し、未知のセキュリティ脅威を遮断して中小企業の IT 環境を保護します。 クラウドベースのマネジメントでセキュリティ運用の利便性を向上し、セキュリティ環境構築のコストを削減することができます。AhnLab V3 Security for Business により、管理サーバーと個々のデバイスを簡単に一元管理・保護できます。

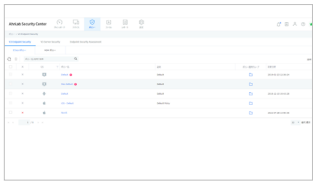
- 多次元分析プラットフォーム基盤の **優れた検知率による事前防御**
- クラウドベースの分析技術により **新種・亜種マルウェアに対応**
- サーバーや特別な投資が要らず、 **低コスト**
- Web 上の管理者用ページで **セキュリティ状況をモニタリングおよび管理**
- 一つのライセンスで **マルチ OS・マルチデバイスを統合管理**
- 独自開発エンジンとスマートスキャン技術による **超高速スキャン**

特長

AhnLab V3 Security for Business は、いつ・どこでも一目でセキュリティ状況を確認および管理できる Web ベースのマネジメントを提供します。シンプルな情報構成、簡単なポリシー適用、総合コマンド送信などを通じて柔軟かつ効率的にセキュリティ環境を運用・管理することができます。



直観的な UI

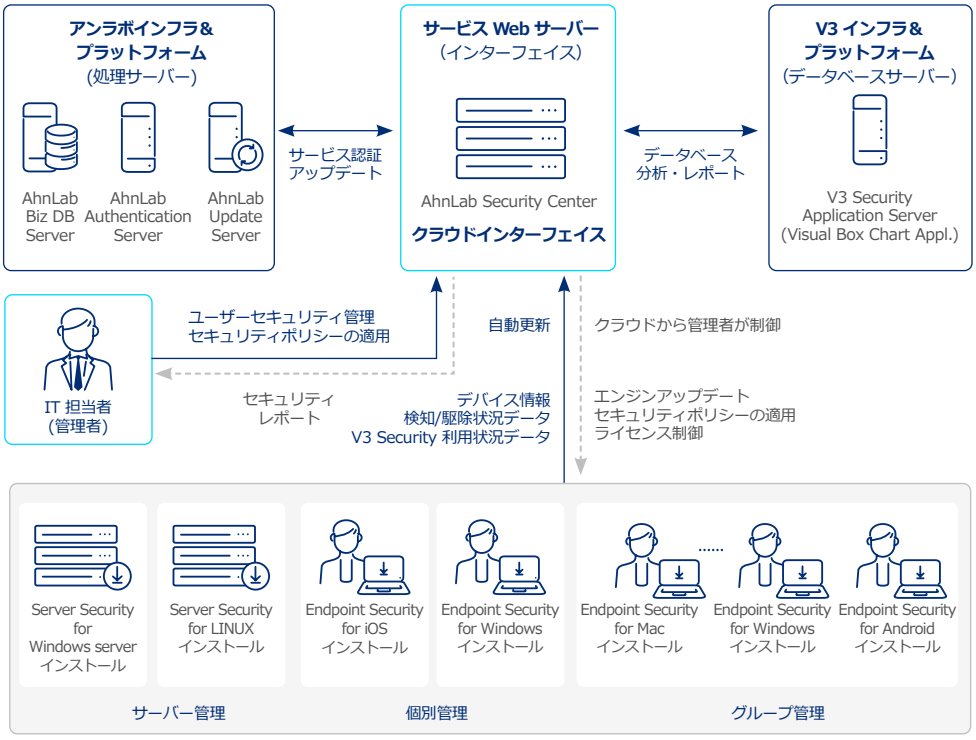


簡単なポリシー適用

利便性の高いセキュリティ管理

構成図

AhnLab V3 Security for Business は PC/Mobile 専用の V3 Endpoint Security、サーバー専用の V3 Server Security、デバイスの脆弱性チェックおよび対応ソリューションである Endpoint Security Assessment、そして 総合 Web マネジメントの AhnLab Security Center で構成されています。別途のサーバーを構築せずに社内デバイスのセキュリティ状況や使用状況をモニタリングすることができます。



導入効果

AhnLab V3 Security for Business は、スマートオフィス環境に最適化されたセキュリティ管理ソリューションです。

セキュリティインフラ構築コストの削減効果

·セキュリティ専門家を採用しなくても、ライセンス購入のみで簡単にセキュリティ環境を構築可能
·AhnLab V3 Security for Business 購入時に提供される「AhnLab Security Center」により、セキュリティシステム構築・運用管理コストの悩みを解決
·単一企業のオールインワン (All-in-one) サービスの導入により、多重契約管理の煩わしさを最小化

利便性に優れた脅威管理および対応プラットフォーム

·クラウド環境により、インターネットに接続するだけでいつでもどこでもマネジメントアクセスが可能
·直観的なユーザーインターフェース(User Interface)により、管理パフォーマンスの向上およびセキュリティ強化
·一つの画面で脅威モニタリング、迅速な対応およびセキュリティポリシー適用が可能
·設定に応じて定期的にメールで届くセキュリティレポートにより、セキュリティ状況およびライセンスの使用状況を確認

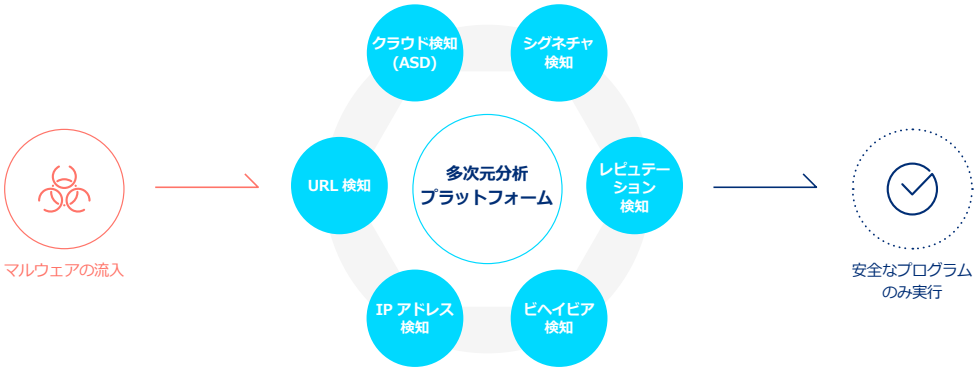
効率的な企業資産のセキュリティ管理

·SaaS ベースの統合マネジメント (AhnLab Security Center) による一元化されたセキュリティ運用および管理環境の整備
·マルチ OS、マルチデバイスのセキュリティチェックおよび様々な管理機能により、運用の利便性向上

主要機能

PC

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。

Windows

マルウェア検知

·クラウドベースの ASD DB を通してリアルタイムでマルウェア検知・対応
·プロセス/メモリ領域における脅威検知および ASMI 診断
·マシンラーニングベースの亜種マルウェアの検知

Active Defense

·疑わしいプロセス/プログラムの動作などレピュテーションおよびビヘイビア情報の提供
·プロセスおよびファイルの詳細レポートにより、セキュリティの可視化

レピュテーションおよびビヘイビア検知

·プログラムの評価情報をもとに、安全性が検証されていないプログラムの実行を遮断
·モニタリングを通して異常なパケットの有無を判断

PC 最適化

·ユーザーが手軽に運用できるようにメイン画面を構成
·セキュリティのチェック結果が「注意」 の場合、ワンクリックで対応可能

ネットワークセキュリティ

·URL / IP など 7億個の DB 情報を活用してアクセスした Web サイトの情報を提供
·ビヘイビア侵入遮断、ネットワーク侵入遮断、有害サイト遮断
·ファイアウォール設定

ランサムウェア対応

·ランサムウェアの疑いがあるプロセスに対する隔離スキャン
·デコイ(Decoy) 診断技術の適用
·ランサムウェアの疑いがあるプロセスへのアクセス遮断
·フォルダー保護機能を通して重要ファイルの暗号化防止

mac OS

マルウェア検知

·クラウドベースの ASD DB を通してリアルタイムでマルウェア検知・対応
·不要なプログラム (PUP)、評価が低いプログラム検知

Web セキュリティ

·不要な Web サイト遮断
·不要なプログラム (PUP) 遮断
·ユーザー指定サイトの許可/遮断管理

ネットワークセキュリティ

·ファイアウォール設定機能
·IP アドレス、ポートおよびプロトコル(TCP、UDP、ICMP) の接続許可/遮断制御

プログラム規則

·インストールされたプログラムのネットワーク接続の許可/遮断制御
·TrueFind (隠ぺい型マルウェア検知)を通して侵入遮断

主要機能

Mobile

お客様のニーズに適したセキュリティ技術で脅威からデバイスを守ります。バッテリーの消耗を最小限に抑えることでデバイスに負担をかけず、セキュリティ脅威に触れることなく安全なスマートフォン環境を構築することができます。

android

マルウェアに対する強力な防御力

· AV-TEST、AV-Comparatives などのグローバル認証機関のテストにて 1位を獲得した強力なアンチウイルスエンジンを搭載
· 2013年から連続で AV-TEST 認証を取得中 / モバイルマルウェアの検知率 (Protection) 100%を記録

デバイスに負担をかけない設計

·バッテリーの消耗を最小限に抑えた設計および業界最低水準の CPU 使用率

スピーディーで正確なスキャン

· リアルタイムスキャン：アプリインストール時に悪性の有無をスキャン
· クイックスキャン：スマートフォンにインストールされているアプリをスキャン
· 指定スキャン：ファイルへのアクセスが許可されたすべてのファイルおよび不要なアプリ (PUA) をスキャン
· URL スキャン：アクセス先 URL の安全性を判定

脆弱性およびアプリ権限チェック

· エンジンを最新バージョンにアップデートした後、スキャンを実行
· デバイス root 化の有無 / 提供元不明アプリのインストール許可の有無 / 画面ロック設定の有無などをチェック
· デバイス管理アプリ / 録音機能 / アプリ内課金 / 位置情報へのアクセス / 連絡先へのアクセスなど、アプリの権限使用状況を15 項目に分けて表示

リモートコントロール (盗難紛失対策)

·デバイス位置情報の追跡 / 画面ロック / アラーム発動 / 電話発信 / メッセージ送信 / データ初期化など、リモートによるコントロールを実行

iOS

Jail-Break（脱獄）の検知

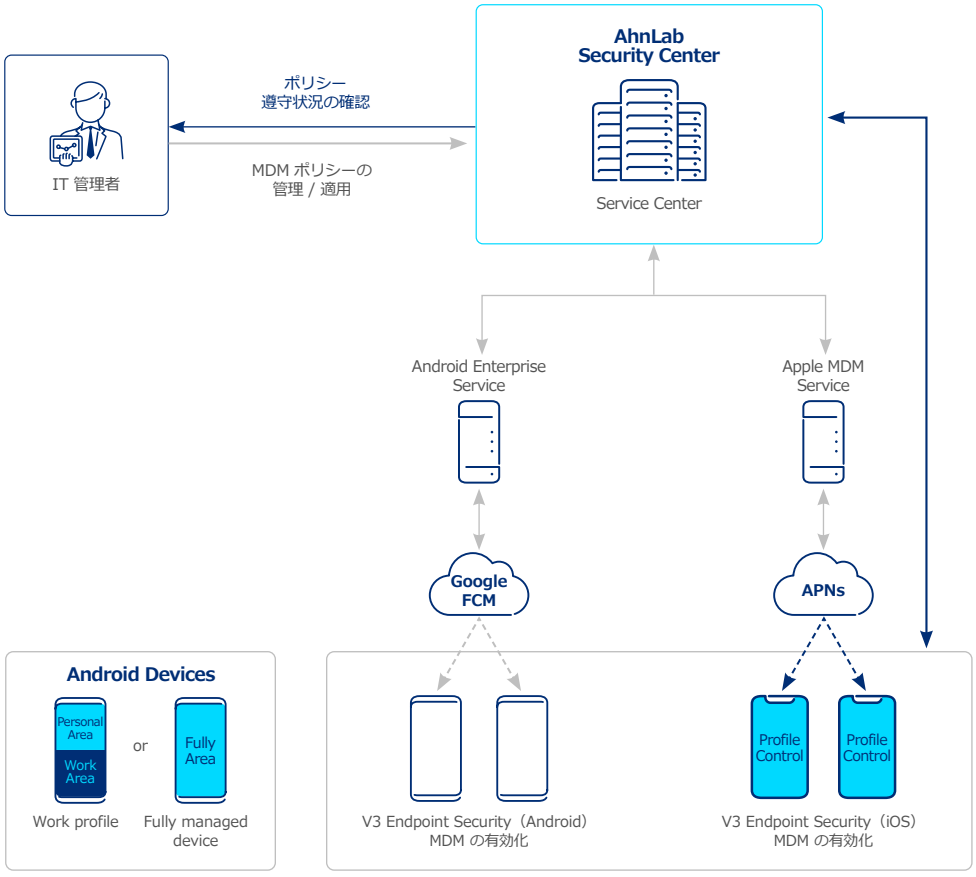
· OS 改ざんの有無を検知

URL スキャン / リモートコントロール

· アクセスする URL の安全性を判定
· デバイス位置情報の追跡 / 電話発信 / メッセージ送信など、リモートコントロールを実行

MDM 機能

MDM (Mobile Device Management) 機能を利用して、企業で管理するモバイルデバイスを一元管理することができます。MDM 管理対象デバイス専用のポリシーを作成して適用することで、企業環境やセキュリティポリシーに適した細かいデバイス管理が可能になります。



·仕事用プロファイル（Work profile）：
個人所有デバイス（BYOD）に対応
·完全管理対象デバイス（Fully managed device）：
企業所有デバイスに対応

Google Firebase Cloud Messaging(Google FCM)
Apple Push Notification service(APNs)

android

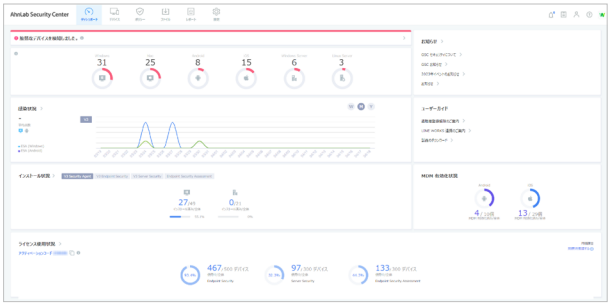
- MDM 機能により、企業で管理するモバイルデバイスを一元管理可能
- 画面ロックパスワード機能により、セキュリティ強度、パスワード有効期限などを設定可能
- 企業 Wi-Fi ネットワーク設定および仕事用アプリ管理制御機能により、仕事用アプリの有効化の有無、自動アップデート設定可能
- 個人用プロファイル/仕事用プロファイル（領域）を分離して制御管理
- 完全管理対象デバイスで企業デバイスの制御管理可能
- リモートコマンド機能により、画面ロック、デバイス再起動可能

iOS

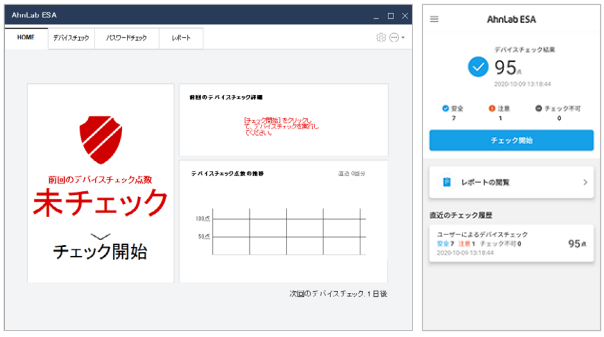
- MDM ポリシー設定により、モバイルデバイス機能の制御可能
- カメラの使用、スクリーンショットの撮影、Touch ID/Face ID、App 内課金などの使用有無を設定可能
- 信頼できない HTTPS 証明書によるアクセスの可否設定
- リモートコマンド機能により、画面ロックおよび画面ロックパスワードの削除、デバイスの初期化可能

ESA

AhnLab Endpoint Security Assessment (Windows/Android) は、中小企業向けのセキュリティマネジメントソリューションです。セキュリティ運用・脅威管理プラットフォームの Security Center と連動して利用することができます。



[Security Center]



[Endpoint Security Assessment]

Windows

49個のチェック項目の中から実行する項目の指定可能

- デバイスチェック時に企業の環境および内部ポリシーに応じて、チェックする項目を指定して実行可能
- チェック項目は、基本項目 (13個) と拡張項目 (36個) で構成
- Windows 自動実行プログラムおよびスタートアッププログラムリストの収集可能

高いセキュリティ運用の利便性

- 管理者がデバイスチェックの周期を設定可能
- 設定した脆弱判断基準点数未満のデバイスへの対応が容易

脆弱性への積極的な対応

- 脆弱判断基準点数未満の場合、デバイスチェック状況を常時通知
- 具体的な対応方法の提示

OS およびソフトウェアの最新バージョンチェック

- OS、MS Office などが最新バージョンであるかをチェック

android

ユーザーによるデバイスチェック

- 製品からユーザーが直接デバイスチェックを実行

管理者設定デバイスチェック

- 管理者が Security Center で設定した内容に基づいてバックグラウンドでデバイスチェックを実行
- 管理者設定デバイスチェック完了後に通知を表示

リモートデバイスチェック

- Security Center からリモートデバイスチェックコマンドを受信した際に実行
- スキャン中である旨の通知を表示

デバイスチェック実行の誘導

- デバイスチェックを誘導するための脆弱判断基準点数の設定
- デバイスチェック点数が脆弱判断基準点数未満であった場合は、デバイスチェックの実行を誘導する通知を表示

使用環境

AhnLab Security Center(Web Management)

区分	仕様
Web ブラウザ	Microsoft Edge (Chromium) 109.x 以後
	Chrome 109.x 以後
	Safari 16.x 以後
対応言語	日本語、英語、韓国語

AhnLab V3 Security Agent/V3 Endpoint Security/Endpoint Security Assessment(Windows)

区分	仕様
OS	Windows 7 SP1 (KB4490628、KB4474419 パッチ管理) / Windows8(8.1) / 10 /11
CPU	Intel Core i3 以上
メモリ	4GB 以上
ストレージ	1GB 以上の空き容量
対応言語	日本語、英語、韓国語

AhnLab V3 Endpoint Security(macOS)

区分	仕様
OS	macOS 10.15 (Catalina) 以後
CPU	CPU Intel / M1, M2
メモリ	4GB 以上
ストレージ	5GB 以上の空き容量
配布方式	.dmg ファイル
対応言語	日本語、英語、韓国語

AhnLab V3 Endpoint Security/Endpoint Security Assessment(Android)

区分	仕様
OS	Android 8.x 以後
CPU	Android ベースのスマートデバイス
メモリ	540 x 960 以上
ストレージ	Play Store
対応言語	日本語、英語、韓国語

使用環境

AhnLab V3 Endpoint Security(iOS)

区分	仕様
OS	iOS 13 以後
デバイス	iPhone 5 / iPad 2 / iPad mini 以上
スクリーン	
配布方式	APP Store
対応言語	日本語、英語、韓国語

AhnLab V3 Server Security(Windows)

区分		仕様
Windows Server 2008、2012(R2 含む) / 2016 / 2019 / 2022	CPU	2GHz 以上
	メモリ	4GB 以上
共通	ストレージ	1GB 以上の空き容量
	対応言語	日本語、英語、韓国語

AhnLab V3 Server Security(Linux)

区分		仕様
OS		CentOS 5.0 ~ 8.0 / Debian 9.5 ~ 10.4 / Fedora 16 ~ 32 / openSUSE 12.1 ~ 15.2 Oracle Linux 5.5 ~ 8.2 / RedHat Enterprise Linux 5.0 ~ 8.2 / SuSE Enterprise Linux 11.0 ~ 15.1 / Ubuntu 11.10 ~ 20
CPU		2GHz 以上
メモリ		1GB 以上の空き容量
共通	ストレージ	2GB 以上の空き容量
	対応言語	日本語、英語、韓国語

東京都港区芝4丁目13-2 田町フロントビル3階 〒108-0014
ホームページ: www.jp.ahnlab.com
TEL: 03-6453-8315 FAX: 03-6453-8316

AhnLab