More security,
More freedom

2024. 03.19

AhnLab

V3 Security for Business

導入ガイド

[目次]

5. AhnLab Security Center での V3 Security Agent インストール

1. 製品紹介

1) AhnLab V3 Security for Business 製品定義と構成の概要

a) V3 Security for Business のコンセプト

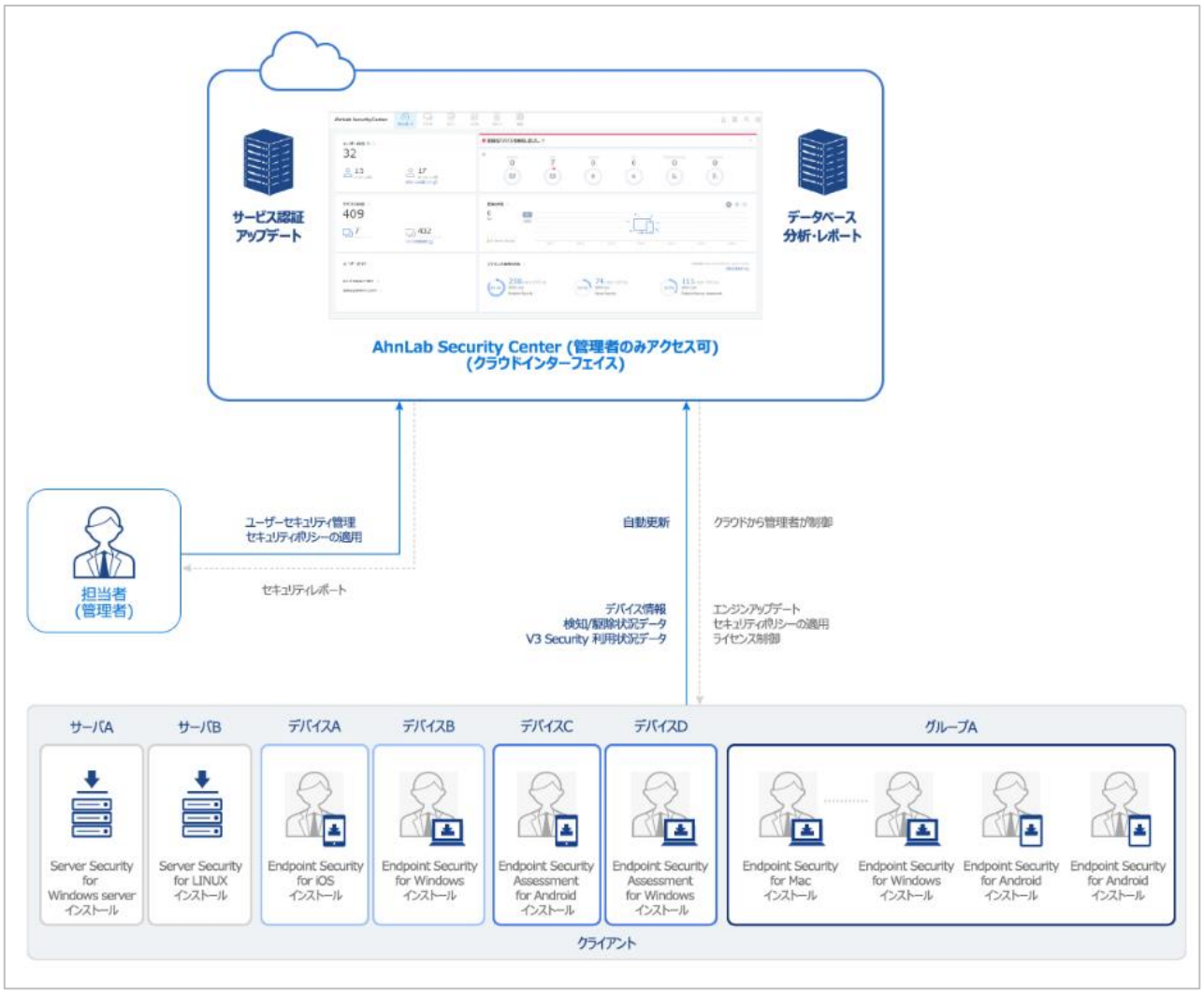
スマートオフィス環境のセキュリティに最適化されたセキュリティマネジメントソリューション

中小企業の業務環境は、Mobility Workflow 時代に伴い、あらゆる危険にさらされています。
近年ではランサムウェアによる攻撃の42%、標的型攻撃の65%が中小企業を対象としたものであり、企業側での対策が求められるなかで、IT リソースの不足や、セキュリティ戦略にかかる費用面での負担といった悩みを抱える中小企業は少なくありません。

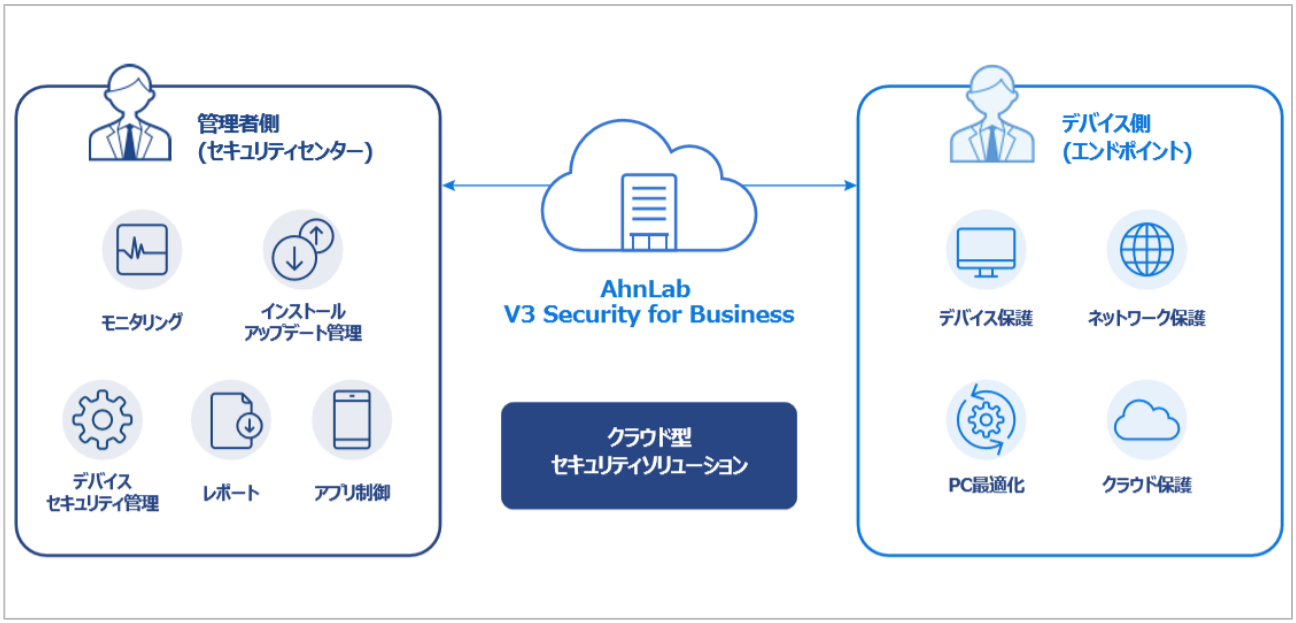
- １つのコンソール・最小限のリソースで、企業の IT 環境を保護
- マルチOS対応で多様なデバイスに対するセキュリティ管理
- 迅速な環境構築 ・ 容易な全社管理

「V3 Security for Business」は、ランサムウェアおよび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する ASD Cloud Threat Intelligence を基盤に中小企業の業務環境を保護します。

AhnLab V3 Security for Business をご利用いただくことで、社員が使用するすべてのデバイスの業務環境および管理サーバーを短時間で保護することができます。



2) 主要機能の紹介



a) V3 Endpoint Security (for Windows)の主要機能

機能分類	主要機能
アンチウイルス	ASD (AhnLab Smart Defense) クラウドネットワークの使用
	スマートスキャン (Smart Scan) 技術の適用
	ビヘイビアスキャン、レピュテーションスキャン (クラウドビヘイビアスキャン、クラウドレピュテーションスキャンを含む)
	Active Defense の適用
	DNA スキャンに対応
	リアルタイムスキャン、手動 (指定) スキャン、スケジュールスキャン
	スタートアッププログラムの監視、実行中のプロセススキャン、メモリスキャン
	製品プロテクト (自動再起動、プロテクト対象の設定)
	重要システムファイルの保護、ブートタイム製品保護
	不要なプログラム (PUP) スキャン、有害プログラムスキャン
	圧縮ファイルスキャン、USBドライブスキャン、共有フォルダーの共有オプションを解除してスキャン
	ランサムウェア対策 (保護フォルダーの設定)
	セキュリティ状態の設定 / 解決
ネットワーク保護	ネットワーク侵入遮断 / ビヘイビア侵入遮断 (HIPS) / IP アドレスの許可・遮断
	有害サイトの遮断 (不要なサイト(PUS)/フィッシングサイト)
	ユーザー指定サイトの管理
	ファイアウォール
その他設定	ログ / バックアップセンター
	最適化 / ファイル完全削除
	ログ、イベント、バックアップセンターでの保存期間の設定
	環境設定のロック
	通知設定 / アップデート設定 / サーバー設定
対応言語	日本語、英語、韓国語 (メイン UI、ユーザーガイド)

b) V3 Server Security (Windows)の主要機能

機能分類	主要機能
アンチウイルス	ASD (AhnLab Smart Defense) クラウドネットワークの使用
	スマートスキャン (Smart Scan) 技術の適用
	ビヘイビアスキャン、レピュテーションスキャン (クラウドビヘイビアスキャン、クラウドレピュテーションスキャンを含む)
	Active Defense の適用
	DNA スキャンに対応
	リアルタイムスキャン、手動 (指定) スキャン、スケジュールスキャン
	スタートアッププログラムの監視、実行中のプロセススキャン、メモリスキャン
	製品プロテクト (自動再起動、プロテクト対象の設定)
	重要システムファイルの保護、ブートタイム製品保護
	不要なプログラム (PUP) スキャン、有害プログラムスキャン
	圧縮ファイルスキャン、USB ドライブスキャン、共有フォルダーの共有オプションを解除してスキャン
	ランサムウェア対策 (保護フォルダーの設定)
	セキュリティ状態の設定 / 解決
ネットワーク保護	署名基盤のネットワーク侵入遮断 (許可・遮断 IP アドレスの使用、攻撃者 IP アドレスの一時遮断)
	ポート遮断 (ポート遮断方式/除外ポートの設定、ポート遮断規則の管理)
	マルウェア拡散時のネットワーク緊急遮断
	許可・遮断 IP アドレスの登録
	有害サイトの遮断 (不要なサイト(PUS)/フィッシングサイト)
	ユーザー指定サイトの管理
その他設定	ログ / バックアップセンター
	ログ、イベント、バックアップセンターでの保存期間の設定
	環境設定のロック
	通知設定 / アップデート設定 / サーバー設定
対応言語	日本語、英語、韓国語 (メイン UI、ユーザーガイド)

c) V3 Endpoint Security (for Mac)の主要機能

機能分類	主要機能
アンチウイルス	リアルタイムスキャン (すべてのファイル)
	クイックスキャン (重要フォルダー)
	手動スキャン (フォルダー/ファイル) - 選択スキャン / 圧縮ファイルの設定 / 駆除方法の設定
	スケジュールスキャン
	スキャン除外設定
	製品プロテクト (自動再起動)
	クラウド検知 / クラウド自動分析
ネットワーク保護	IP アドレスの許可・遮断
	ポートの許可・遮断
ファイアウォール	インバウンド通信の遮断 (プログラムの選択)
	署名済みソフトウェアのインバウンド通信の許可
	TrueFind (隠ぺい型マルウェア検知) 機能のアクティブ化
有害サイトの遮断	不要なサイト (PUS) の遮断
	ユーザー指定サイトの管理
その他設定	ログ / バックアップセンター
	バックアップセンターでの保存期間の設定
	環境設定のロック (macOS がサポートするデフォルト機能)
	通知設定 (設定した状況で、通知ウィンドウを表示/タスクバーに V3 アイコンを表示)、アップデート設定 (自動アップデート/スケジュールアップデート)
対応言語	日本語、英語、韓国語 (メイン UI、ユーザーガイド)

d) V3 Endpoint Security (for Android)の主要機能

区分	機能	V3 Endpoint Security (for Android)
動作方式	起動 / 終了	Stand Alone / Security Center による動作
使用エンジン	モバイルエンジン	Mobile Engine SDK
必要な権限の設定	権限の設定 / ガイド	製品利用時に必要な権限ガイドおよび設定の誘導
セキュリティチェック	脆弱性チェック	初回実行時にデフォルト実行、その後「脆弱性チェック」ボタンで実行
		端末起動完了時 / メイン画面へのアクセス時 / 該当項目を on に設定時
		- エンジンアップデート
		- アンチマルウェア設定基準に沿った端末スキャン
		- 端末 root 化の有無チェック (デフォルト: on) (off 設定可能)
		- 提供元不明アプリのインストール許可の有無チェック (デフォルト: on) (off 設定可能) [制約条件 : Android 7.0以下に対応]
		- 開発者モード有効の有無チェック (デフォルト: on) (off 設定可能)
		- 画面ロック設定 (PIN/Pattern/Password/Face unlock) の有無チェック (デフォルト: on) (off 設定可能)
アンチウイルス	端末スキャン	手動およびリモートコマンドによるクイックスキャン (デフォルト : インストール済みアプリ) / PUA スキャン (任意) / 指定スキャン (フォルダーファイルを含む)
	リアルタイムスキャン	常時 ON / セキュリティレベル設定の制御可能 / apk ダウンロード時の対象ファイルスキャン (デフォルト: on) (off 設定可能)
		端末起動時のクイックスキャン
	初回実行時のスキャン	初回実行時にアクセス権限の設定 > スキャンを誘導
	スケジュールスキャン	管理者設定によるリモートスキャン / ユーザーによるスケジュールスキャン
	ダウンロードフォルダースキャン	該当フォルダー内の apk ファイル (ダウンロード後) 生成時のファイルスキャン
	エンジンアップデート	管理者設定によるリモートアップデート
		初回実行時にネットワークに繋がっている場合はエンジンを最新バージョンにアップデート
		その後、自動アップデートの設定に従って動作 (モバイルネットワーク/Wi-Fi の選択はなし)
		自動アップデートの適用 (デフォルト: on) / 自動アップデートが off の場合は手動アップデートのみ動作
アプリ削除防止	管理者権限の設定	アプリ削除防止のための管理者権限設定
		環境設定内で設定可能 (デフォルト : off) (on に設定する場合は、設定権限ガイドおよび削除時の案内ガイドが必要)

端末root 化のチェック	端末root 化の有無チェック	Mobile Root Checker SDK
ログ管理	検知ログ、イベントログ	マルウェアスキャンおよびイベント (スキャン/アップデート状況) の結果ログの確認
アプリ権限の管理	アプリ権限チェック	アクセス権限チェック / ユーザーが設定した権限項目に該当するアプリがインストールされた場合に通知
紛失端末の制御 (Security Center と連動)	位置情報の確認	マップ上で、端末の位置情報を確認
	盗難紛失対策関連機能の設定	位置の転送 / アラーム機能のアクティブ化などに関する設定情報
	端末情報の確認	端末情報の表示 (OS、モデルなど)
	アラート発動およびメッセージ送信	リモートでアラームを発動させた場合、紛失端末の画面にメッセージが表示され、アラームが発動
	電話発信	紛失端末への電話発信 (1分間/VoIP 使用)
	画面ロック	紛失端末の画面ロック (画面ロックが設定されていない場合は、企業ライセンスの下4桁でロック)
	端末初期化	画面ロックと同時に端末を初期化
URL スキャン (Security Center と非連動)	URL スキャン	アクセス先 URL を機能画面上で直接入力して安全性を判別
		URL をコピー (クリップボード) して安全性を判別
バージョン管理	製品パッチのお知らせ	製品実行時、パッチのお知らせ > インストールを誘導 強制 / 一般パッチの管理 (Admin)

e) V3 Endpoint Security (for iOS)の主要機能

区分	機能	V3 Endpoint Security (for iOS)
動作方式	起動 / 終了	Stand Alone / Security Center による動作
必要な権限の設定	権限の設定 / ガイド	製品利用時に必要な権限ガイドおよび設定の誘導
セキュリティチェック	脆弱性チェック	製品実行時の Jail-Break (脱獄) 有無の自動チェック (デフォルト: on) (off 設定可能) / 初回実行時は設定に関わらず実行
		ユーザーが直接 [スキャン] ボタンをタップして実行
		Jail-Break (脱獄) 有無の自動チェック (デフォルト: on) (off 設定可能)
紛失端末の制御 (Security Center と連動) [VoIP Push/Call 使用]	位置情報の確認	マップ上で、端末の位置情報を確認
	盗難紛失対策関連機能の設定	位置の転送のアクティブ化などに関する設定情報
	端末情報の確認	端末情報の表示 (OS、モデルなど)
	メッセージ送信	紛失端末の画面にメッセージが表示され、アラームが発動
	電話発信	紛失端末への電話発信 (1分間/VoIP 使用)
URL スキャン (Security Center と非連動)	URL スキャン	アクセス先 URL を機能画面上で直接入力して安全性を判別
ログ管理	検知ログ、イベントログ	セキュリティチェックの結果ログ
バージョン管理	製品パッチのお知らせ	製品実行時、パッチのお知らせ > インストールを誘導 強制 / 一般パッチの管理 (Admin)

f) V3 Server Security (Linux)の主要機能

機能分類	主要機能
アンチウイルス	リアルタイムスキャン (On/Off 設定、スキャン終了後の自動再開)
	手動 (指定) スキャン (スキャン対象の設定)
	スケジュールスキャン (スキャンの追加/変更/削除)
	圧縮ファイルスキャン
アップデート / パッチ	自動アップデート使用有無の選択およびアップデート周期 (1~24時間) の設定
	スマートアップデートを利用した自動アップデートおよびパッチの提供
	指定した時間に実行されるスケジュールスキャン (アップデート周期の設定)
	アップデートサーバーの設定 (インターネットを通じたアップデート/ユーザー定義サーバーを通じたアップデート/ローカルディレクトリを通じたアップデート)
	その他設定 (アップデート時の製品パッチ/アップデート情報の確認/整合性スキャン)
	署名済みソフトウェアのインバウンド通信の許可
	Stable エンジンに対応
有害サイトの遮断	許可 IP アドレスの設定
	サーバー管理ポートの設定 (サーバー接続時に使用される TCP ポートの設定) ・ホスト名の設定、管理者情報 (ID/PW)
スキャン設定	駆除方法の設定 ・駆除する / 駆除せずにそのまま残す ・自動駆除 ・駆除/削除する前にバックアップセンターに保存する
	スキャン対象の設定 ・すべてのファイル、感染しやすいファイル (実行ファイル/マクロファイル/スクリプトファイル) ・圧縮ファイル
ログ管理 / バックアップセンター	検知ログ、イベントログ
	バックアップセンターリストの確認、ファイル復元
統計	月別/期間別のマルウェア統計
中央管理	Web Management 統合管理ソリューションとの連動
Agent Web UI	Linux 環境に適合した Web UI の Agent

g) AhnLab Endpoint Security Assessment (for Windows)の主要機能

機能	AhnLab Endpoint Security Assessment (for Windows)
自動対応	チェック結果に対してバックグラウンドで自動対応
	ユーザーによる別途対応や管理者の介入は必要なし（完全自動対応）
	内部セキュリティポリシーに応じて自動対応の有無および内容をユーザーに提供
	自動対応で業務用 PC のセキュリティを常に「安全」な状態に維持
ワンクリック対応	内部セキュリティポリシーによる手動対応が可能
	脆弱な項目に対してチェック画面でワンクリック対応
	詳細な対応ガイドを提供 - 管理者がガイド内容を追加可能
ユーザー PC 環境の設定	脆弱な項目への対応完了時までユーザー PC 画面に AhnLab ESA を強制的に表示可能
	管理者ポリシーによってユーザー PC 画面にウィジェット（Widget）を常に表示
	ユーザー画面（UI）の多言語対応：日本語、英語、韓国語に対応

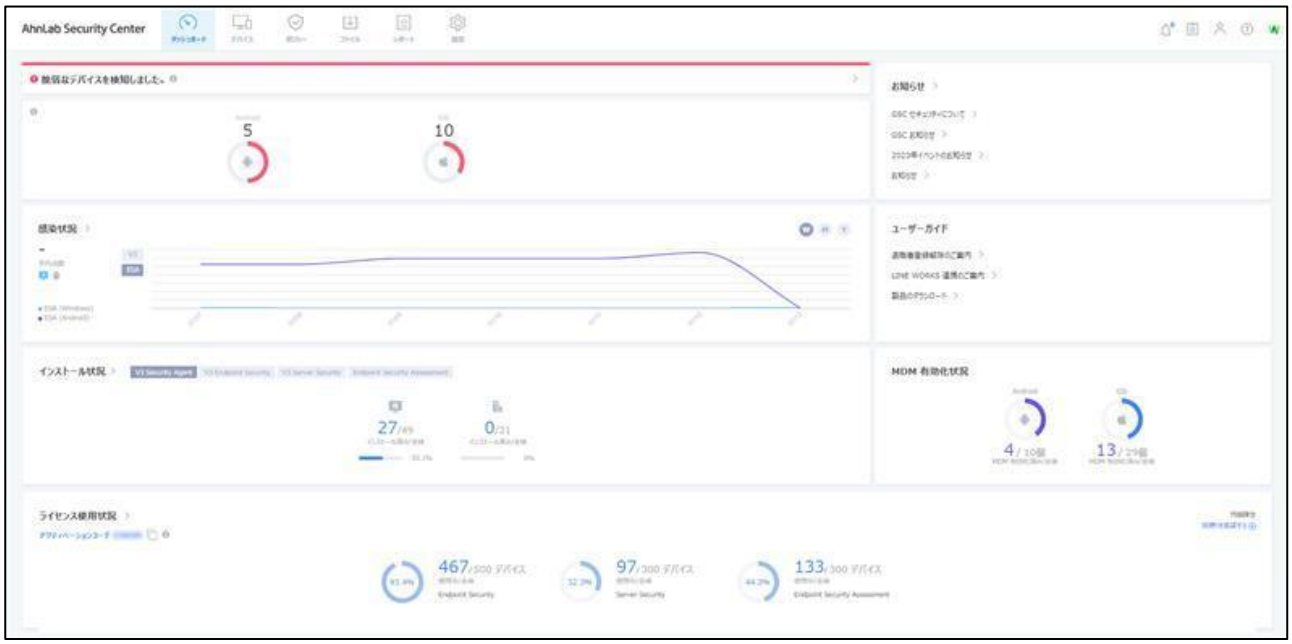
h) AhnLab Endpoint Security Assessment （for Android)の主要機能

機能	AhnLab Endpoint Security Assessment (for 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 AhnLab 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	AhnLab 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

i) AhnLab V3 Security Agent (for Windows/Server)の主要機能

機能	AhnLab V3 Security Agent (for Windows/Server)
Security Center との連携	V3 Security Agent がインストールされたシステムの情報およびエージェントログを Security Center に送信可能
キュリティ製品のインストール/アンインストール管理	インストール/アンインストールコマンドから、セキュリティ製品のインストール/アンインストール可能
セキュリティ製品の実行	V3 Security Agent と共にインストールされたセキュリティ製品を V3 Security Agent のトレイメニューから実行可能
ユーザー情報の確認	Security Center と連携中の V3 Security Agent のユーザー情報を確認

j) AhnLab Security Center の主要機能



AhnLab Security Center (管理コンソール)	ダッシュボード
	ライセンス管理
	グループ別 PC 管理
	セキュリティポリシー管理
	インストール管理
	週間 / 月間レポート (E-mail)
	エンジンアップデート / パッチ管理

3) 動作環境

a) V3 Endpoint Security (for Windows)の動作環境

区分	推奨仕様
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
配布方式	.exe ファイル

b) V3 Server Security (Windows)の動作環境

Windows Server	区分	推奨仕様
Windows Server 2008、2012 (R2を含む) / 2016 / 2019 / 2022	CPU	2GHz 以上
	メモリ	4GB 以上
共通事項	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

c) V3 Endpoint Security (for Mac)の動作環境

区分	推奨仕様
OS	macOS 10.15 (Catalina) 以降
CPU	Intel Core 2 Duo 2.53GHz 以上, M1
メモリ	4GB 以上
ストレージ	5GB 以上の空き容量
対応言語	日本語、英語、韓国語
配布方式	.dmg ファイル

d) V3 Endpoint Security (for Android)の動作環境

区分	推奨仕様
OS	Android 8.x 以降
デバイス	Android ベースのスマートデバイス
スクリーン	540 x 960 以上
対応言語	日本語、英語、韓国語
配布国	韓国 / グローバル (日本など)
配布方式	インストールファイル (.apk) の配布、Google Play ストア

e) V3 Endpoint Security (for iOS)の動作環境

区分	推奨仕様
OS	iOS 13 以降
デバイス	iPhone 5 / iPad 2 / iPad mini 以上
スクリーン	
対応言語	日本語、英語、韓国語
配布国	韓国 / グローバル (日本など)
配布方式	App Store

f) V3 Server Security (Linux)の動作環境

区分	推奨仕様
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
メモリ	1GB 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

※ 上記 OS バージョンへの対応の有無は一般的事項であり、今後リリースされるすべての OS バージョンへの対応を保証するものではありません。

※ 下位バージョンを含む対応 OS については、別途お問い合わせください。

※ pSeries および Itanium には対応しません。

g) AhnLab Endpoint Security Assessment(for Windows)の動作環境

区分	推奨仕様
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
配布方式	.exe ファイル

h) AhnLab Endpoint Security Assessment(for Android)の動作環境

区分	推奨仕様
OS	Android 8.X 以上
デバイス	Android ベースのスマートデバイス
スクリーン	540 x 960 以上
対応言語	日本語、英語、韓国語
配布方式	インストールファイル (.apk)

i) AhnLab V3 Security Agentの動作環境

区分	推奨仕様	
	Windows	Server
CPU	Intel core i3 以上	2GHz 以上
メモリ	4GB 以上	4GB 以上
HDD	1GB 以上の空き領域	4GB 以上
対応言語	日本語、英語、韓国語	

j) AhnLab Security Centerの動作環境

区分	推奨仕様
対応ブラウザ	Microsoft Edge (Chromium) 109.x 以後 / Chrome 109.x 以後 / Safari 16.x 以後
解像度	1280 X 1024 以上 (PC バージョン基準)
ネットワーク環境	HTTPS SSL プロトコール TLSv1.0, TLSv1.1, TLSv1.2 サポート

2. 製品導入までの流れ

V3 Security for Business（以下、本製品）は企業のお客様向けの製品です。

製品契約の申請処理が完了しますと、申請書の「④お客様の管理者情報」欄にご入力いただいたメールアドレス宛に初回ログイン用の仮パスワードなどが記載された「アカウント情報メール」が送信されます。

アカウント情報メール

タイトル：AhnLab Security Center のパスワードを発行しました

送信元アドレス：v3sb-noreply@ahnlab.com

メールが受信されたことを確認出来たら、以下の手順で初回ログインと設定を行ってください。

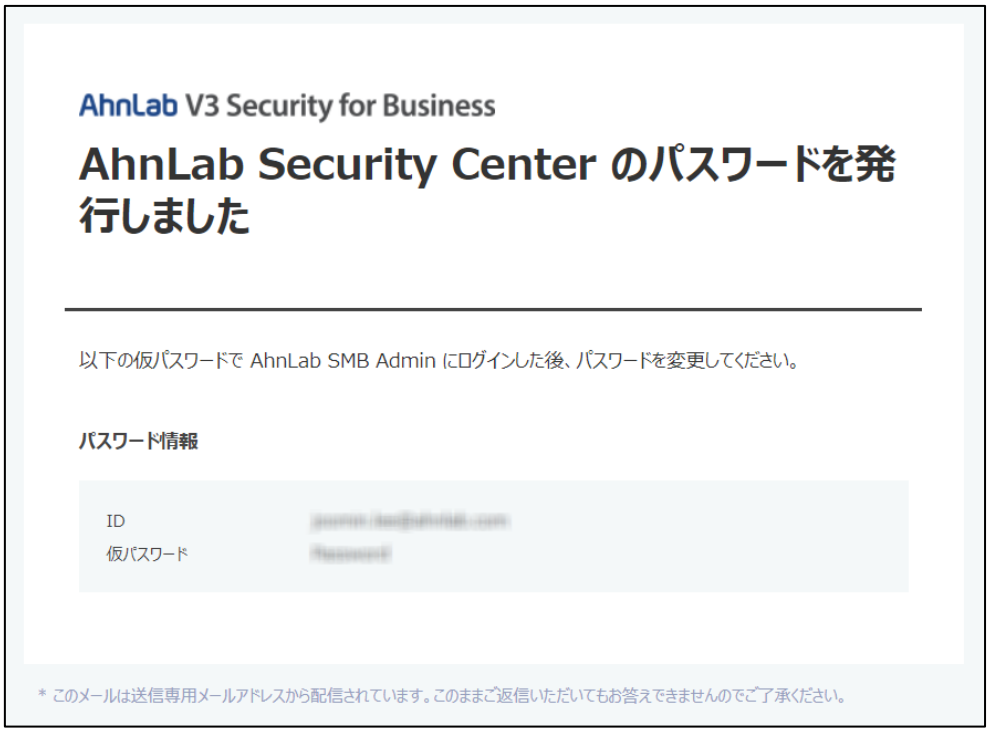
2-1) AhnLab Security Center 管理者がログインするまで

製品ご購入後に、管理者(最高管理者)が製品にログインするまでの流れは以下の通りです。

① 本製品を購入します。

＊ 製品のご購入につきましては、別途お問い合わせください。

② 購入プロセスが完了したら、購入者にアカウント情報メールが送信されます。


AhnLab V3 Security for Business

AhnLab Security Center のパスワードを発行しました

以下の仮パスワードで AhnLab SMB Admin にログインした後、パスワードを変更してください。

パスワード情報

ID [redacted]
仮パスワード [redacted]

* このメールは送信専用メールアドレスから配信されています。このままご返信いただいてもお答えできませんのでご了承ください。

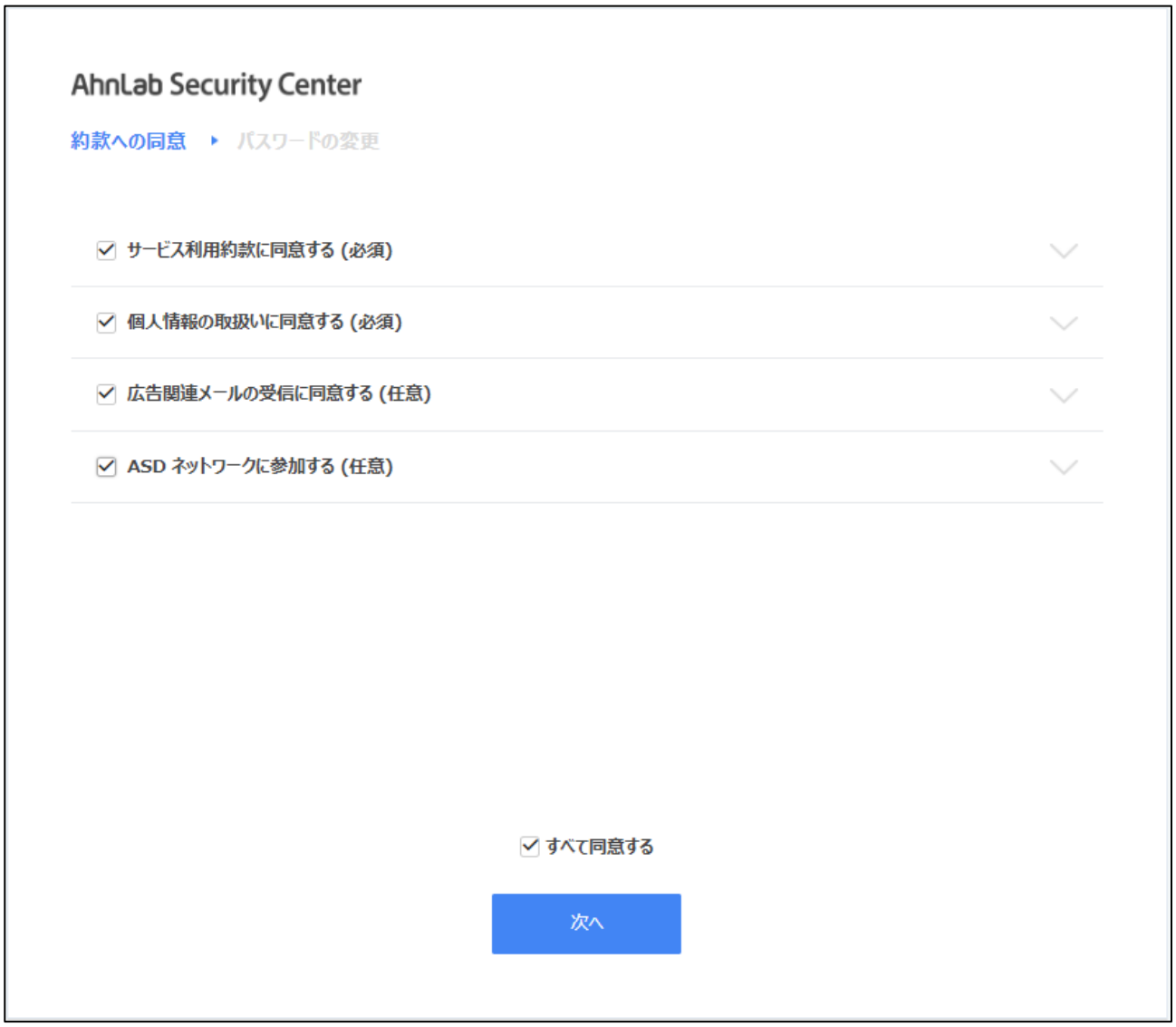
<管理者へのアカウント情報メール>

③ 仮発行されたパスワードで Security Center にログインします。

AhnLab Security Centerにログインします。(URL: https://v3sc.ahnlab.co.jp)

<ログイン画面>

④ 本製品を使用するために必要な約款に同意します。



<約款への同意画面>

注意

「必須」項目はチェックしないと次のステップに進めません。

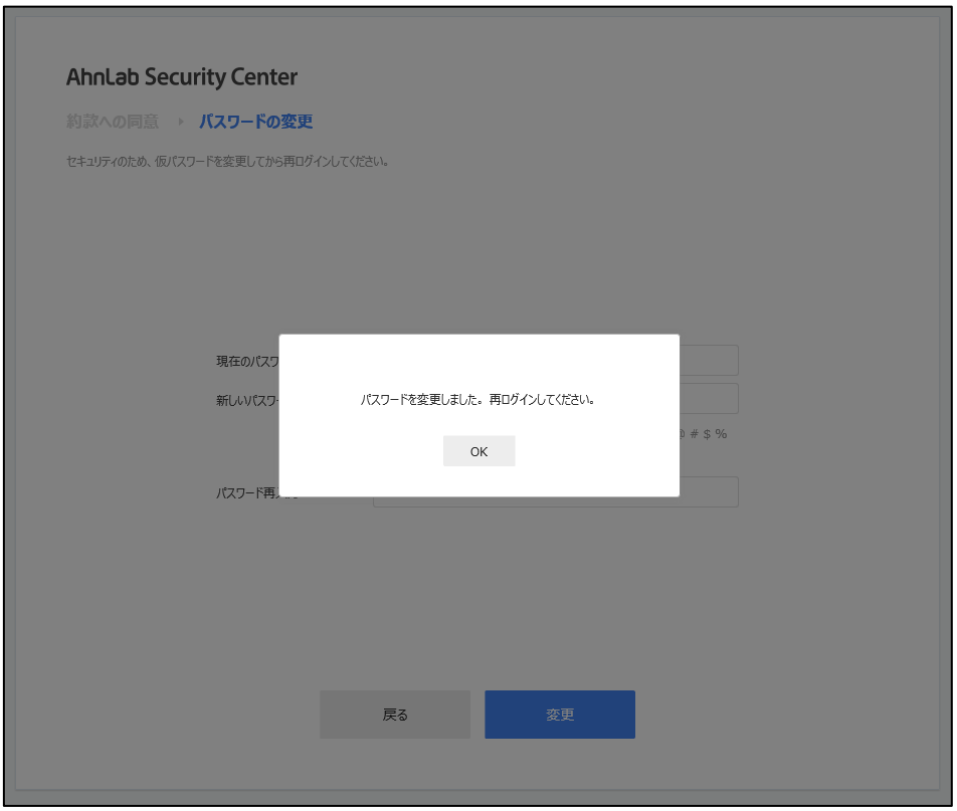
⑤ 仮発行されたパスワードを変更します。

<仮パスワードの変更画面>

注意

仮パスワードはログインプロセスで必ず変更してください。パスワードは、英数字 (大文字小文字を区別) と特殊文字 (! @ # $ % ^ & *) を組み合わせて 8~16桁以内で入力してください。

⑥ 変更したパスワードで再ログインします。



<パスワードの変更画面>

注意

3回以上ログインに失敗するとアカウントがロックされます。アカウントがロックされた場合は、「パスワードの再発行」をクリックしてパスワードを再発行するか、「再実行」をクリックして５分経過後に再実行してください。

2-2) AhnLab Security Center 初期設定の流れ

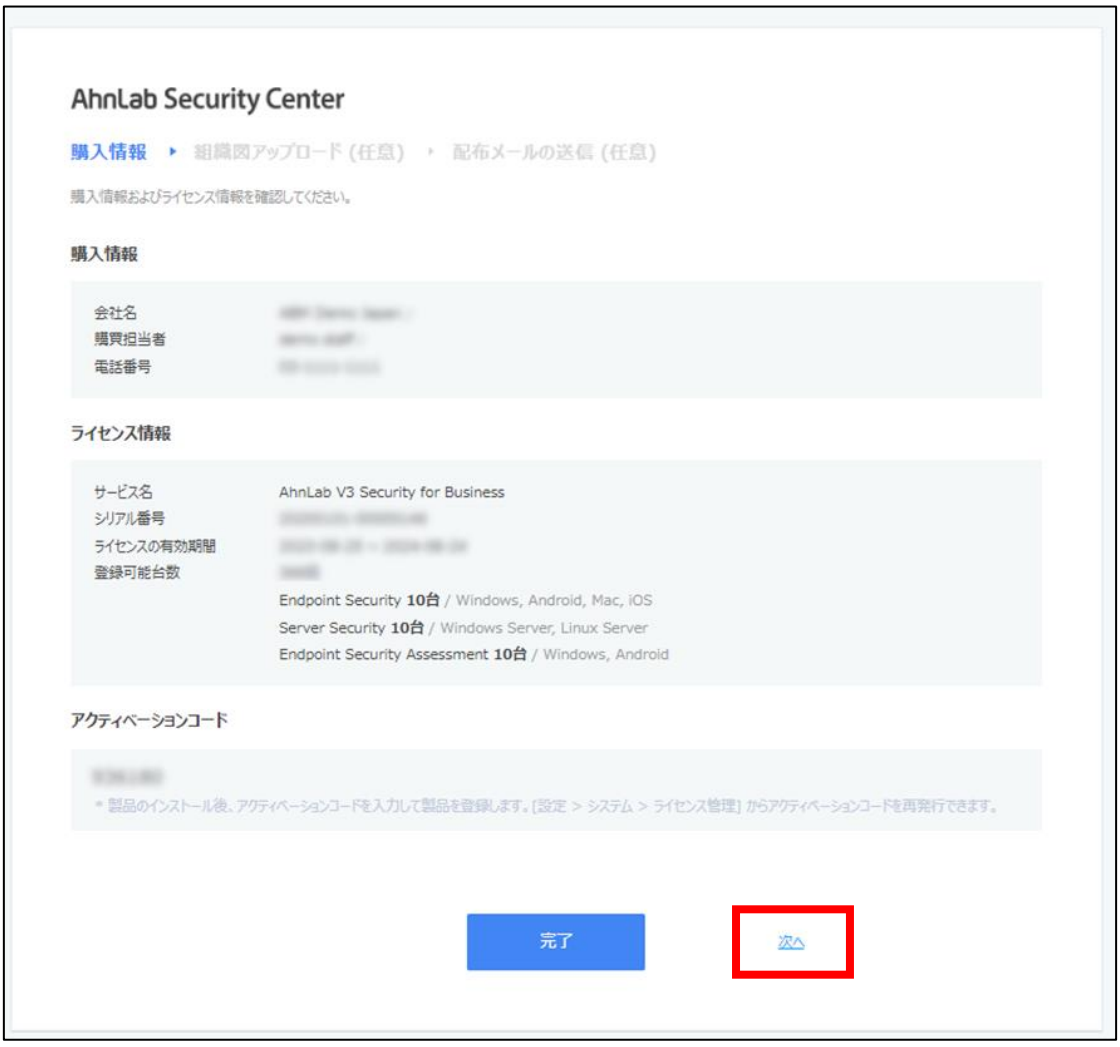
最高管理者が製品にログインした後、初期設定の流れは以下の通りです。

① 再ログイン後、購入情報およびライセンス情報を確認します。

設定を完了する場合は「完了」、組織図をアップロードする場合は「次へ」を選択します。「次へ」を選択した場合は、②に進みます。

以下の情報が表示されます。

項目	表示情報
購入情報	会社名、購入担当者、電話番号、購入先
ライセンス情報	サービス名、ライセンス番号、ライセンスの有効期間、ライセンス情報
アクティベーションコード	現在発行されたアクティベーションコード

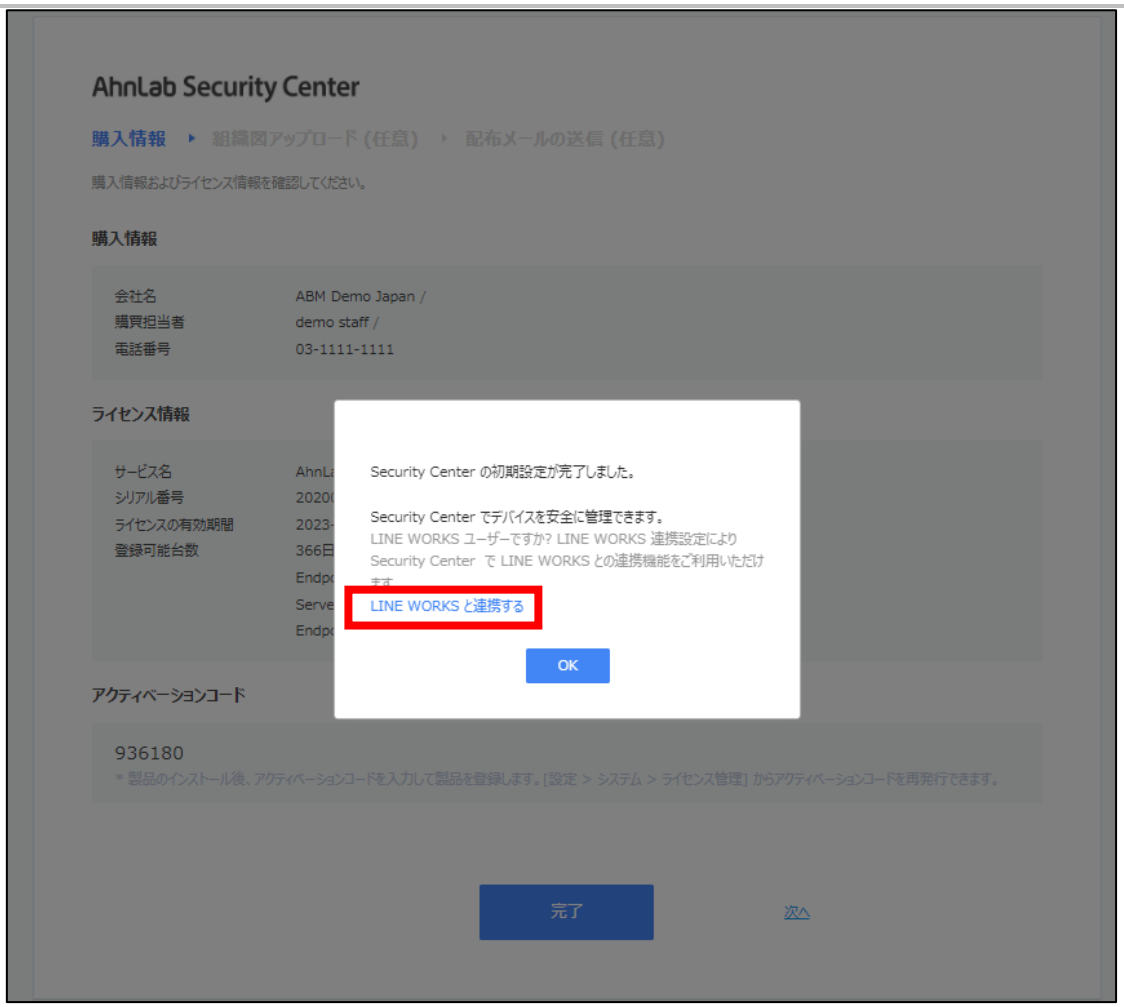


<購入情報画面>

参考

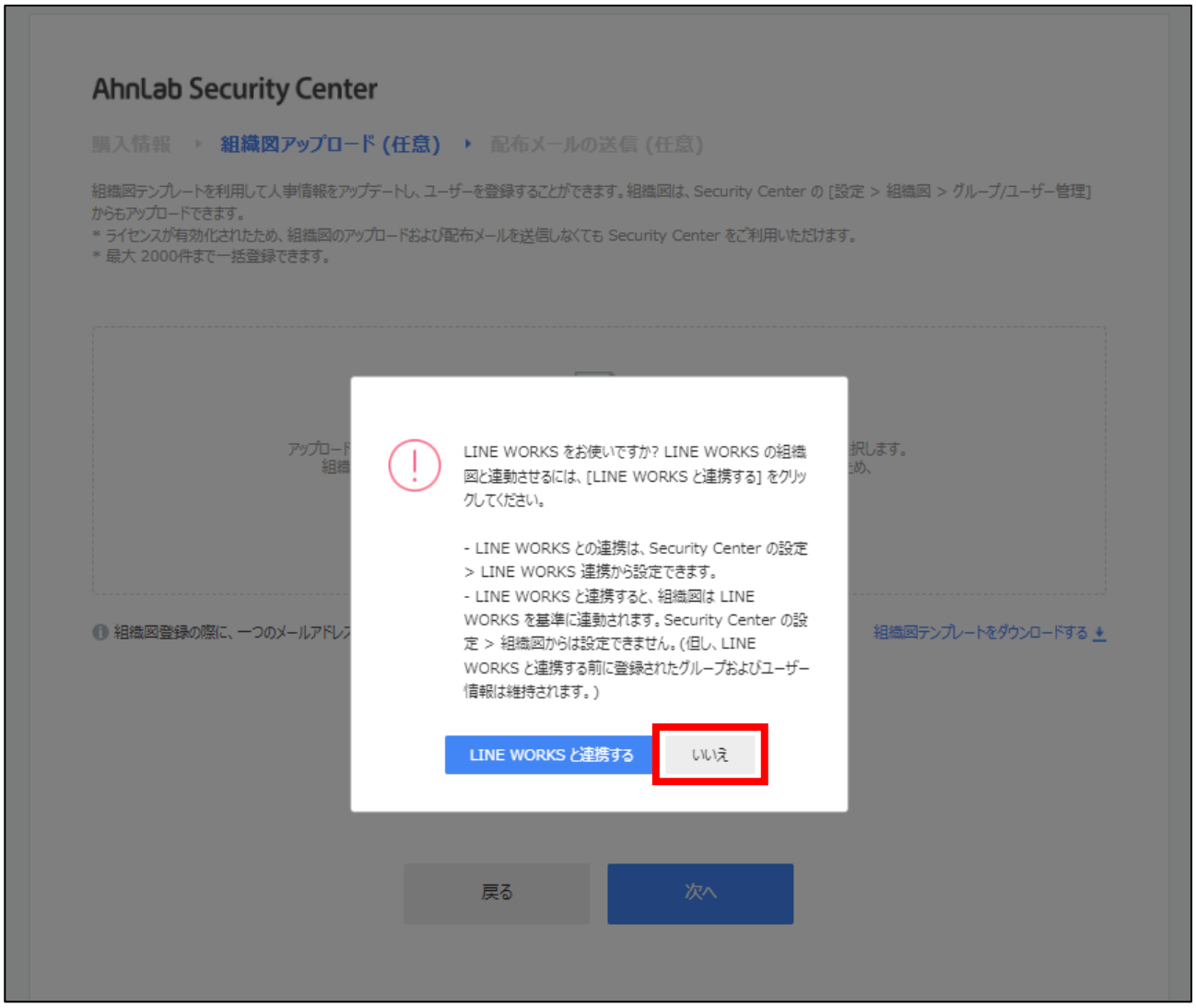
「完了」を選択すると、以下の画面が表示されます。 LINE WORKS を使用中で、AhnLab Security Center と LINE WORKS を連携する場合は、「LINE WORKS と連携する」を選択してください。

「LINE WORKS と連携する」を選択せず「OK」を選択すると、設定が終了します。



<設定完了画面>

② LINE WORKSと連携しない場合は「いいえ」を選択して③に進みます。



<LINE WORKS との連携確認画面>

参考
LINE WORKS を使用中で、LINE WORKS の組織図を連携する場合は「LINE WORKS と連携する」を選択します。

③管理する社内組織図をアップロードします。

まず組織図テンプレートをダウンロードします。

テンプレート（ 組織図テンプレート.xlsx ）に沿って必要な情報を入力しアップロードしてください。

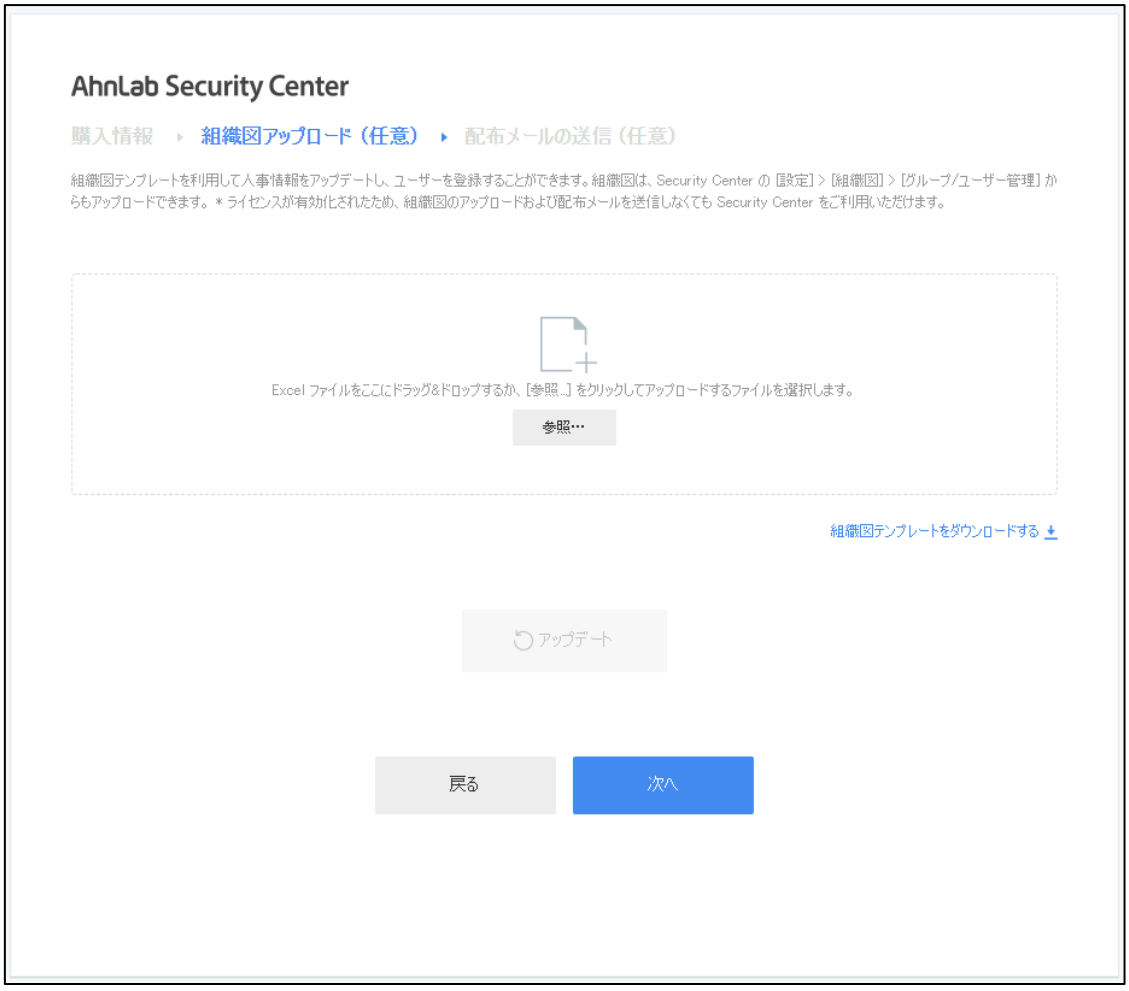
組織図は、初期設定で行わなくとも製品の設定> 組織図> グループ/ユーザー管理> グループリストのインポート( )にて組織図テンプレートのダウンロード、組織図のアップロードを行うことができます。

1. 対象の登録は一度に 2,000個までアップロードできます。
2. 管理者権限/管理対象は、大文字小文字を区別せずに、入力した英字が一致した場合のみ登録できます。
3. 管理者として登録する場合、対象者にアカウント情報をメールで送信します。
4. 既存の管理者の場合は、テンプレートで情報を変更しても適用されません。

管理者権限: Policy (ポリシー管理者) / Monitor (モニタリング管理者)
管理者対象: Total (すべての管理者) / Group (所属グループの管理者)

グループ名	*名前	*ふりがな	*メールアドレス	電話番号	内線番号	社員番号
CEO | OO事業部 | OO部門 | OOチーム	山田太郎	やまだたろう	ooo@ooo.com	031-722-0000	1234	1234

<組織図テンプレート.xlsx>



<組織図アップロード画面>

テンプレートには以下の情報を入力してください。

項目	表示情報
グループ名	ユーザーが所属する部門を入力します。 組織図に階層を設ける際には、「|」(半角のパイプ)で区切ることで階層を設けることができます。
*名前 (必須)	ユーザー名(漢字) を入力します。
*ふりがな (必須)	ユーザー名の読み方(仮名) を入力します。
*メールアドレス (必須)	ユーザーのメールアドレスを入力します。
電話番号	ユーザーの電話番号や携帯電話を入力します。
内線番号	ユーザーの社内の内線番号を入力します。
社員番号	ユーザーの社内の社員番号を入力します。

注意

組織図は Excel ファイル形式のみアップロードできます。

一つのメールアドレスで**複数の名前**を登録することはできませんので、ご注意ください。

※以下は実際の入力例と組織図をアップロードした際の反映画面です。

**** 組織図テンプレートガイド (このガイドは削除しないでください。)**
1. 対象の登録は一度に 2,000個までアップロードできます。
2. 管理者権限/管理対象は、大文字小文字を区別せずに、入力した英字が一致した場合のみ登録できます。
3. 管理者として登録する場合、対象者にアカウント情報をメールで送信します。
4. 既存の管理者の場合は、テンプレートで情報を変更しても適用されません。
管理者権限: Policy (ポリシー管理者) / Monitor (モニタリング管理者)
管理者対象: Total (すべての管理者) / Group (所属グループの管理者)

グループ名	*名前	*ふりがな	*メールアドレス	電話番号	内線番号	社員番号	説明	管理者権限	管理対象
Default	あんらぼ管理者0(		alj.customer03@gmail.com	123-123-4321	123-123-4321				
東京支店|営業部	営業	えいぎょう	sales@ahnlab.com						
東京支店|技術部	技術	ぎじゅつ	technical@ahnlab.com					Policy	Total
埼玉支店|企画部	企画	きかく	plan@ahnlab.com					Monitor	Group
埼玉支店|企画部|デザインチーム	デザイン	でざいん	design@ahnlab.com						
神奈川支店|環境部	環境	かんきょう	environment@ahnlab.com						
神奈川支店|経理部	経理	けいり	accounting@ahnlab.com					Monitor	Total

<組織図の入力例>

<組織図アップロード後の反映画面>

参考

③は任意のステップですので、組織図をアップロードしない場合、そのまま④にお進みください。組織図は、製品メニューの設定 > 組織図 > グループ/ユーザー管理から再設定できます。

④ アップロードした組織図をベースに製品の配布メールを送信します。(任意)

④で組織図をアップロードした場合、登録された組織図からユーザーを選択して製品のインストールご案内メールを送信することができます。

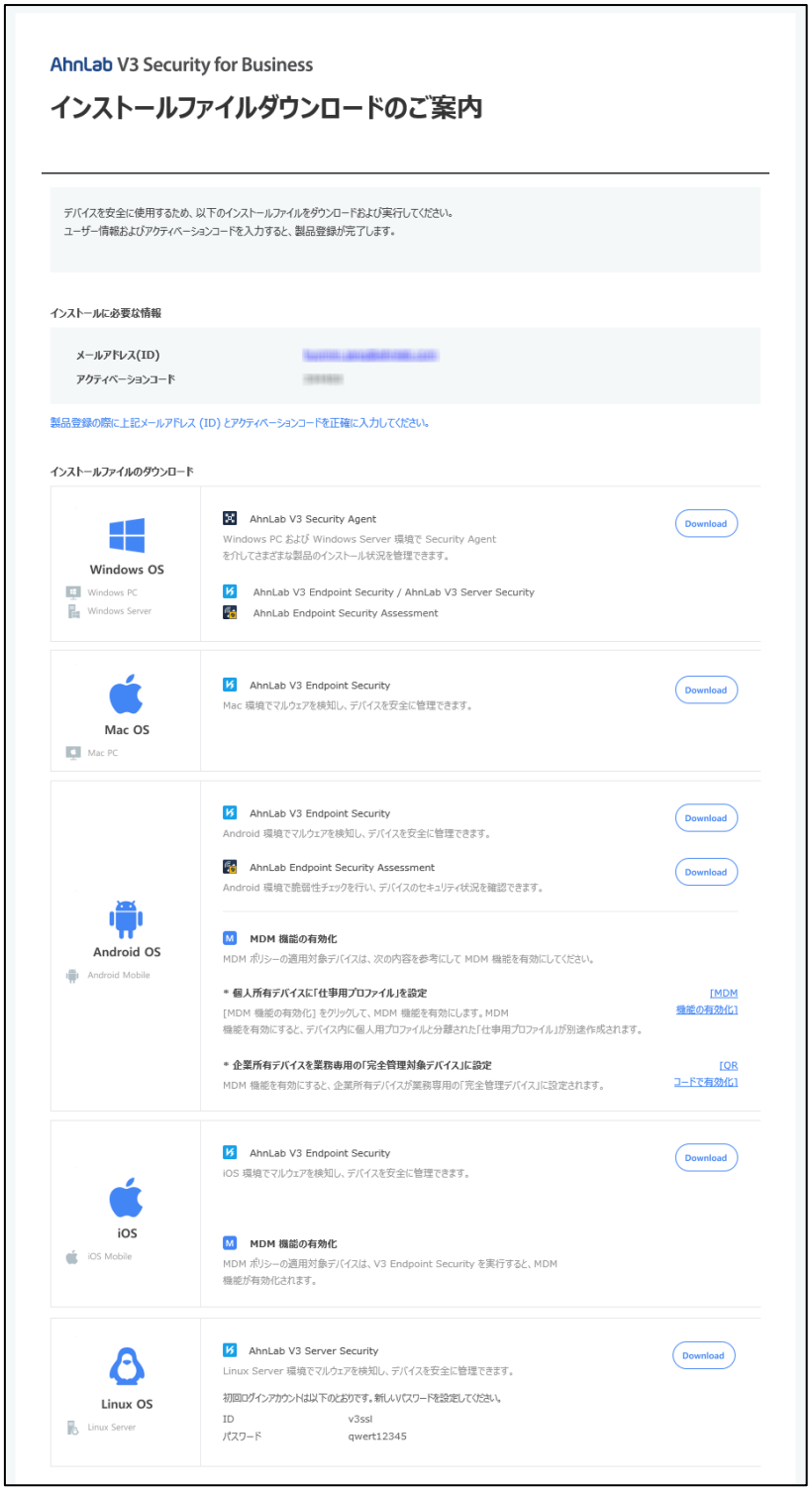
参考

④は任意のステップですので、製品の配布メールを送信しない場合は、そのまま⑥にお進みください。配布メールは、製品メニューのファイル > 配布メールの送信 からいつでも送信することができます。

2-3) AhnLab Security Center ユーザー側の製品使用までの流れ

管理者が配布したメールをユーザーが受信し、製品を使用するまでの流れは以下の通りです。

① 管理者が送信した配布メールを確認します。



AhnLab V3 Security for Business

インストールファイルダウンロードのご案内

デバイスを安全に使用するため、以下のインストールファイルをダウンロードおよび実行してください。
ユーザー情報およびアクティベーションコードを入力すると、製品登録が完了します。

インストールに必要な情報

メールアドレス(ID)
アクティベーションコード

製品登録の際に上記メールアドレス (ID) とアクティベーションコードを正確に入力してください。

インストールファイルのダウンロード

Windows OS
Windows PC
Windows Server

AhnLab V3 Security Agent
Windows PC および Windows Server 環境で Security Agent を介してさまざまな製品のインストール状況を管理できます。
Download

AhnLab V3 Endpoint Security / AhnLab V3 Server Security
AhnLab Endpoint Security Assessment

Mac OS
Mac PC

AhnLab V3 Endpoint Security
Mac 環境でマルウェアを検知し、デバイスを安全に管理できます。
Download

Android OS
Android Mobile

AhnLab V3 Endpoint Security
Android 環境でマルウェアを検知し、デバイスを安全に管理できます。
Download

AhnLab Endpoint Security Assessment
Android 環境で脆弱性チェックを行い、デバイスのセキュリティ状況を確認できます。
Download

MDM 機能の有効化
MDM ポリシーの適用対象デバイスは、次の内容を参考にして MDM 機能を有効にしてください。

* 個人所有デバイスに「仕事用プロファイル」を設定
[MDM 機能の有効化] をクリックして、MDM 機能を有効にします。MDM 機能を有効にすると、デバイス内に個人用プロファイルと分離された「仕事用プロファイル」が別途作成されます。
[MDM 機能の有効化]

* 企業所有デバイスを業務専用の「完全管理対象デバイス」に設定
MDM 機能を有効にすると、企業所有デバイスが業務専用の「完全管理デバイス」に設定されます。
[QR コードで有効化]

iOS
iOS Mobile

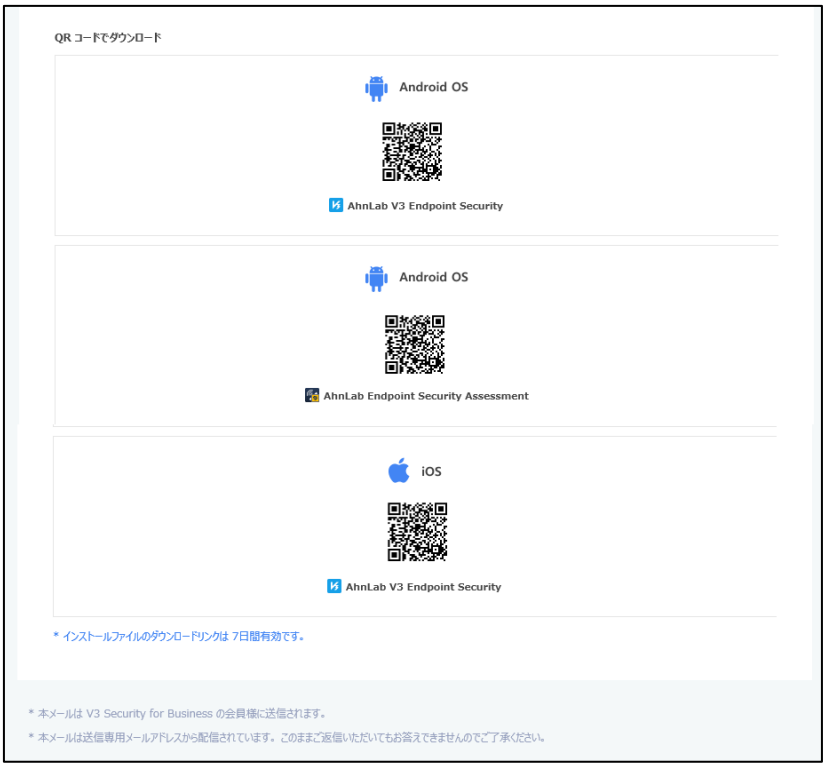
AhnLab V3 Endpoint Security
iOS 環境でマルウェアを検知し、デバイスを安全に管理できます。
Download

MDM 機能の有効化
MDM ポリシーの適用対象デバイスは、V3 Endpoint Security を実行すると、MDM 機能が有効化されます。

Linux OS
Linux Server

AhnLab V3 Server Security
Linux Server 環境でマルウェアを検知し、デバイスを安全に管理できます。
Download

初回ログインアカウントは以下のとおりです。新しいパスワードを設定してください。
ID v3ssl
パスワード qwert12345



<インストールファイルの配布メール>

参考

Security Center > ファイル > ファイルの配布の**配布メール送信**から「**V3 Endpoint Security (Android/iOS) MDM を有効化するためのリンクおよびガイドを表示する**」オプションを選択すると、インストールファイルダウンロードのご案内メールに MDM 有効化に関する内容が表示されます。

※MDM有効化のためのリンクおよびガイドはMDMオプションを契約した場合のみ表示されます。

② ユーザーが使用する OS タイプのインストールファイルをダウンロードします。

OS タイプは以下の種類に対応します。

- AhnLab V3 Endpoint Security
  - Windows PC
  - Mac PC
  - Android Mobile
  - iOS Mobile
- AhnLab V3 Server Security
  - Windows server
  - Linux Server
- AhnLab Endpoint Security Assessment
  - Windows PC
  - Android Mobile
- AhnLab V3 Security Agent
  - Windows PC
  - Windows server

参考
AhnLab V3 Endpoint Security(Android/iOS)、AhnLab Endpoint Security Assessment(Android) は、メールにある **[QR コードでダウンロード]** の QR コードからインストールすることができます。

参考
OSタイプ別のセットアッププロセスは「第3章 V3 Security for Business クライアントのインストール」をご参考ください。

③ インストールファイルを実行して、製品をセットアップします。

④ アクティベーションコードを入力して、製品認証を完了します。

2-4) AhnLab Security Center メニューの説明

製品ログイン後、管理者がアクセスする初期画面のメニューは次の通りです。

< AhnLab Security Center メインメニュー「SVMなし」「MDMあり」共通 >

< AhnLab Security Center メインメニュー「SVMあり」>

※「MDM」メニューはiOS Supervised Mode を契約した場合のみ表示されます。

- ダッシュボード：セキュリティ、デバイス、ライセンスなど様々な情報が表示されます。情報によっては数字や詳細表示へのリンクをクリックすると、詳細情報ページに移動します。
- デバイス：登録されたデバイス状況やセキュリティ情報、インストール状況が表示されます。
- ポリシー：V3 Endpoint Security、V3 Server Securityなどデバイスに適用するポリシーに関する設定ができます。
- MDM ： iOS Supervised Mode 設定にて Security Center に登録されているiOSデバイスを管理できます。
- ファイル：指定ユーザーにインストールファイルの配布およびお知らせメールを送信する設定ができます。
- レポート：管理者が設定した表示項目で構成されたレポートに関する情報確認や設定ができます。
- 設定：本製品の環境設定メニューです。

メインメニュー	詳細メニュー	説明
ダッシュボード	OS別脆弱なデバイス	感染デバイス数、古いエンジン使用中のユーザー数、リアルタイムスキャンが無効のデバイス数をOS別に表示します。
	製品インストール状況	本製品に登録されているデバイスへの製品インストール数を製品別に表示します。
	ユーザーガイド	新入社者/退職者登録解除のご案内、組織図アップデートのご案内を表示します。クリックすると詳細情報を確認できます。
	感染状況	製品のマルウェア感染状況を期間別（週・月・年）にグラフで表示します。

	MDM有効化状況	本製品に登録されたAndroid / iOS デバイスのMDM有効化状況を表示します。	
	Security Agent インストール状況	本製品に登録されているデバイスへの Security Agentインストール状況を表示します。	
	iOS MDM 証明書およびトークンの状況	APNs証明書およびVPPトークンの登録状況および有効期限を表示します。	
	ライセンス使用状況	ライセンスの有効期限とインストール状況を表示します。	
デバイス	デバイス管理	デバイスの接続状況、OS情報、脆弱性情報(感染デバイス数、古いエンジン、リアルタイムスキャン無効)のサマリーとデバイスリストを表示します。	
	マルウェア感染状況	デバイスのOS別マルウェア感染状況とエンジンアップデート状況、感染デバイス(直近５件)、検知マルウェア(直近５件)を表示します。	
	脆弱性検知状況	指定した期間中に検知された脆弱なデバイスおよび脆弱性の詳細情報を表示します。	
	モバイル権限管理	V3 Endpoint Security の機能動作に必要な権限設定が行われているかを確認することができます。	
MDM (iOS)	ABM登録済みデバイス	Apple Bussiness Manager に登録されているデバイスの Supervised Mode 有効化の状況を確認することができます。	
	ABM未登録デバイス	Configurator 環境設定で登録したデバイスを確認することができます。	
	VPPアプリ	購入したVPPアプリを確認してデバイスとの接続/接続解除を行ったり、接続されているアプリをデバイスにインストール要請を送ることができます。	
ポリシー	セキュリティ製品ポリシー	V3 Endpoint Security	登録済みのデバイスに適用する V3 Endpoint Security デフォルトポリシーの追加・変更・削除することができます。
		V3 Server Security	登録済みのデバイスに適用する V3 Server Security ポリシーの追加・変更・削除することができます。
		Endpoint Security Assessment	登録済みのデバイスに適用する Endpoint Security Assessment ポリシーの追加・変更・削除することができます。
		共通ポリシー	登録済みの Windows/Mac/Windows Serverに適用する共通ポリシーの追加・変更・削除することができます。

	MDMポリシー	MDM管理対象デバイスに適用する V3 Endpoint Security MDM ポリシーを追加・変更・削除することができます。
ファイル	ファイルの配布	指定ユーザーにインストールファイルの配布およびお知らせメールを送信する設定ができます。
	ファイルのダウンロード	製品のインストールに必要なアクティベーションコードを確認や、インストールファイルをダウンロードすることができます。
レポート	レポート作成履歴	管理者が作成したレポートや予約設定によって自動的に作成・送信されたレポート履歴を確認することができます。
	レポート作成	組織図から対象を選択し、送付するレポートの表示項目を設定して新規作成できます。(*基本レポートは表示項目の設定を変更できません。)
	レポート予約	作成したレポートの送付時間を予約できます。(*基本レポートは表示項目の設定を変更できません。)
設定	システム設定	ログイン設定、ファイル配布のデフォルト設定、休止モードのデバイスに関して設定できます。
	エンジンアップデート	最新エンジンへのアップデート有無を設定できます。(*iOSは設定対象ではありません。)
	ライセンス管理	使用中のデバイス状況とライセンスの詳細情報を確認できます。使用可能なライセンスを超えた場合や有効期限が切れた場合、見積を要請できます。
	LINE WORKS API 設定	Security Center で、LINE WORKS 連携機能を使用するには LINE WORKS API の設定が必要です。LINE WORKS Developer Console から発行された IP 情報を入力してください。 LINE WORKS Developer Console で LINE WORKS API 認証情報を発行する方法は、Developer Console - API 設定ガイドをご参照ください。(*AhnLab V3 Security Center_Line works 連携ガイド別添)
	LINE WORKS SSO 設定	Security Center で、LINE WORKS 連携機能を使用するには LINE WORKS SSO 設定が必要です。LINE WORKS Developer Console で SP (Service Provider) 詳細情報を登録する方法は、Developer Console - SSO 設定ガイドをご参照ください。(*AhnLab V3 Security Center_Line works 連携ガイド別添)
	Supervised Mode	Apple iOS デバイスの Supervised Mode を利用するための環境設定をすることができます。
	管理者アカウント	最高管理者はポリシー管理者とモニタリング管理者を指定することができます。(*最高管理者は変更のみ可能です。追加・削除することは

		できません。)
	グループ/ユーザー管理	組織図を登録/管理できます。(*組織図は最大５段階まで構成できます。グループ情報のないユーザーは自動で 未指定グループに指定されます。)
	通知設定	様々な状況におけるお知らせ通知の宛先を設定できます。(*お知らせ通知の宛先は管理者のみとなります。)

参考

AhnLab Security Center の機能詳細は製品の機能ガイドをご参考ください。

2-5) AhnLab Security Center 初期設定後に組織図を登録する場合の流れ

※以下の手順は初期設定で組織図を行わなかった場合の手順です。初期設定で組織図の登録を完了している場合は製品のインストールへと進んでください。

① AhnLab Security Center にアクセスする

② AhnLab Security Center 画面上部のメニューから「設定」をクリックする

③ 画面左部のメニューから「グループ/ユーザー管理」をクリックする

④ 「グループリストのインポート」をクリックする

⑤ 「組織図のテンプレートをダウンロードする」をクリックする

テンプレート（ 組織図テンプレート.xlsx ）に沿って、必要な情報を入力してください。

※詳細については本ガイド 2-2)③を参照してください。

⑥ 「参照…」をクリックし、組織図を入力したファイルを選択する

⑦ 「アップデート」をクリックする

3. V3 Security for Business クライアントのインストール

管理者が配布したメールをユーザーが受信し、メールのガイドに従ってデバイスに製品をインストールすると、Security Centerから管理者がユーザーの端末をモニタリング/管理できるようになります。使用するデバイスのOSタイプに合わせてインストールファイルをダウンロードしてセットアッププロセスを進行してください。

V3 Security Agent インストールファイルダウンロード		
	Windows PC V3 Security Agent	
	Windows Server V3 Security Agent	
Endpoint Security インストールファイルダウンロード		
	Windows PC V3 Endpoint Security	
	Mac PC V3 Endpoint Security	
	Android Mobile V3 Endpoint Security	
	iOS Mobile V3 Endpoint Security	
Server Security インストールファイルダウンロード		
	Windows Server V3 Server Security for Windows	
	Linux Server V3 Server Security for Linux	
Endpoint Security Assessment インストールファイルダウンロード		
	Windows PC Endpoint Security Assessment	
	Android Mobile Endpoint Security Assessment	

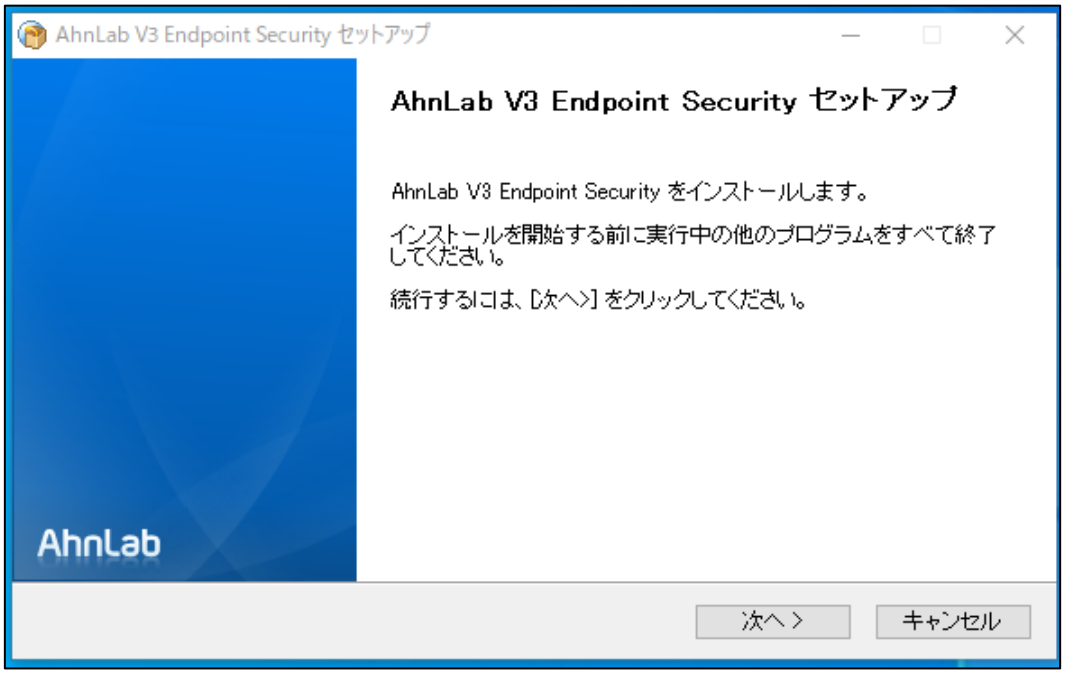
<OSタイプに対応するインストールファイル>

3-1) V3 Endpoint Security (for Windows) クライアントのインストール

Windows PC製品のセットアッププロセスの流れは以下の通りです。

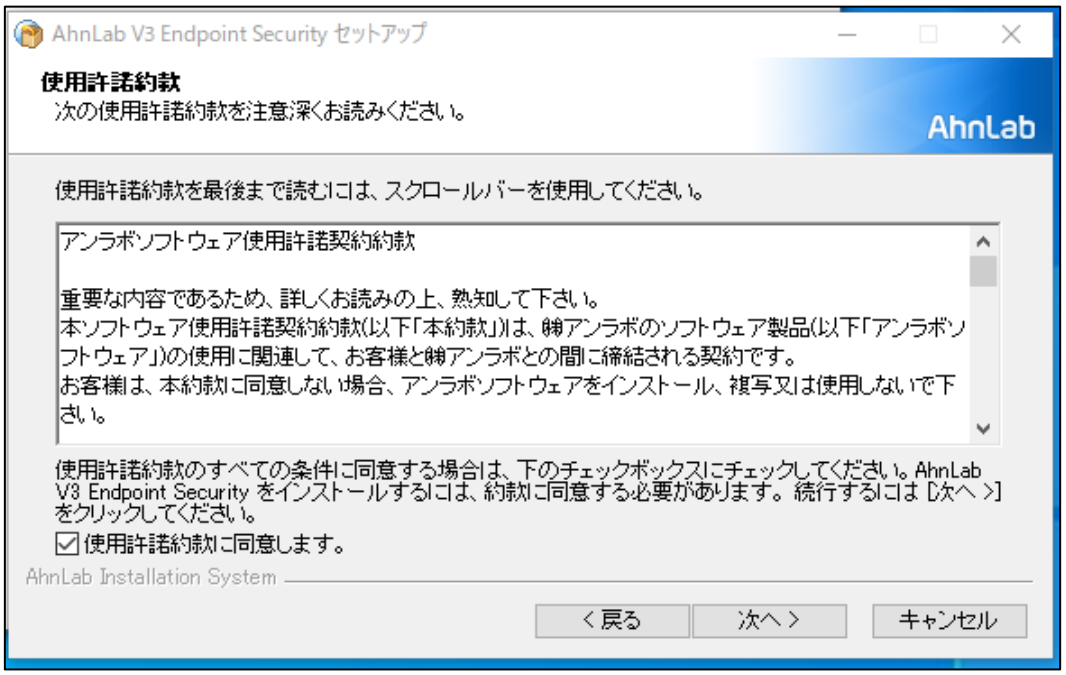
① ダウンロードしたインストールファイルを実行します。

② V3 Endpoint Securityセットアップ画面が表示されたら「次へ」ボタンをクリックします。



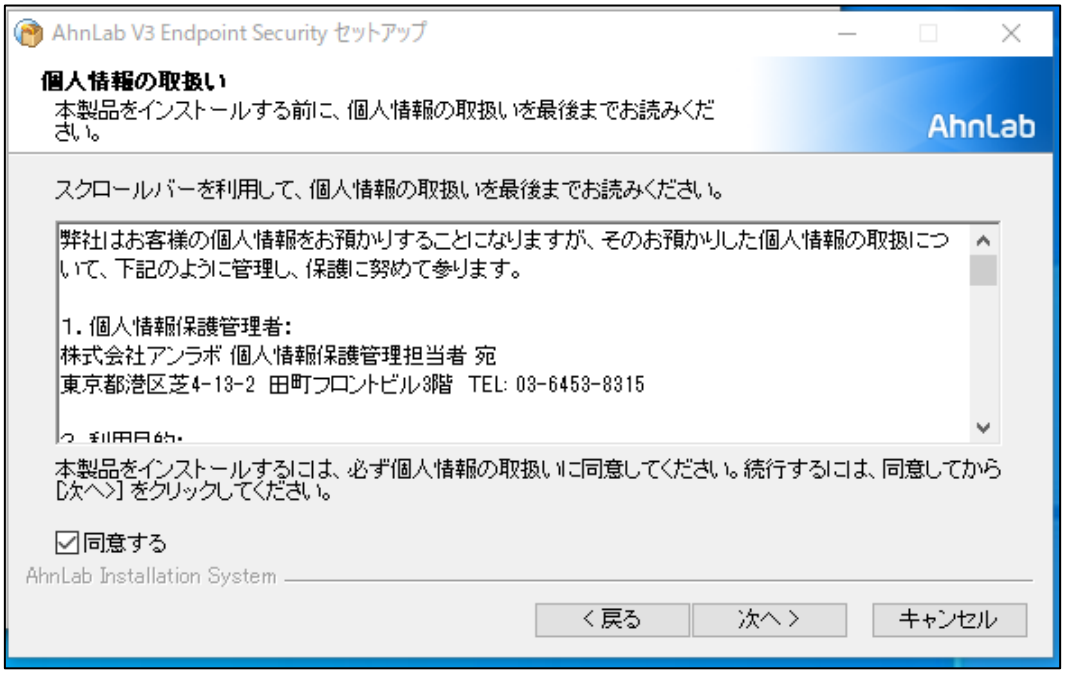
<セットアップ画面>

③ V3 Endpoint Securityの使用許諾約款に同意し、「次へ」ボタンをクリックします。



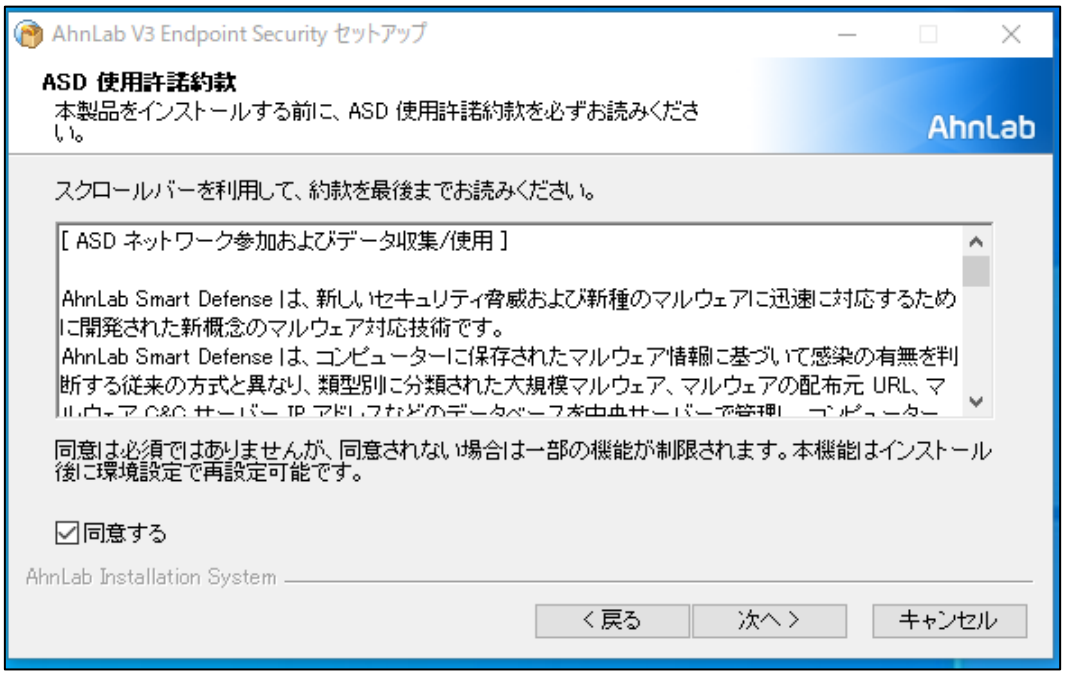
<使用許諾約款画面>

④ V3 Endpoint Securityの個人情報の取扱いに同意し、「次へ」ボタンをクリックします。



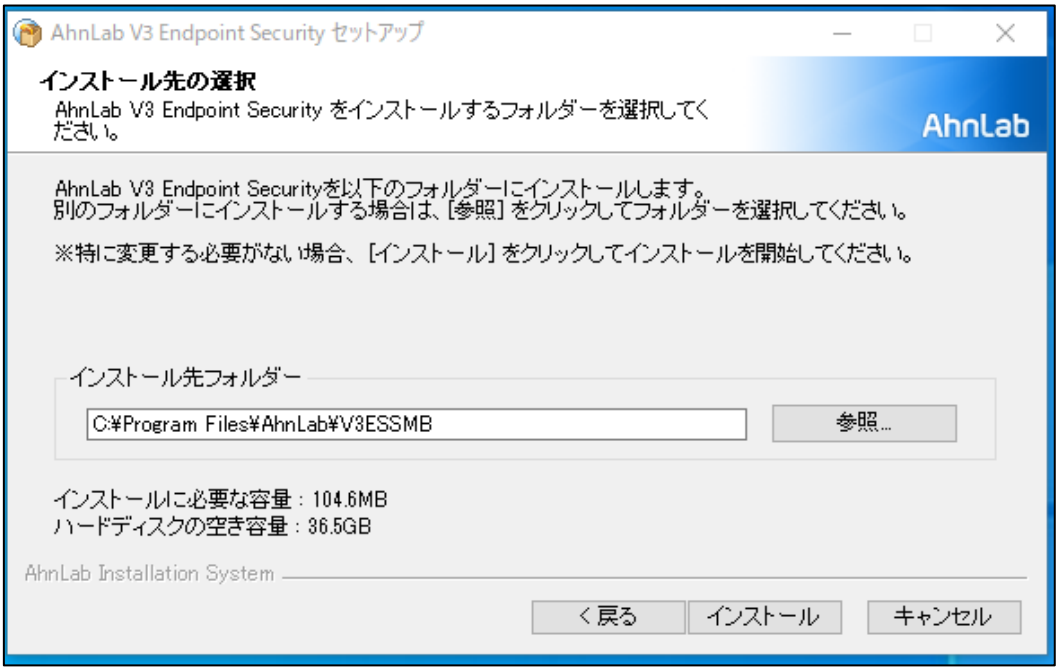
<個人情報の取扱い画面>

⑤ V3 Endpoint SecurityのASD使用許諾約款に同意し、「次へ」ボタンをクリックします。



<ASD 使用許諾約款画面>

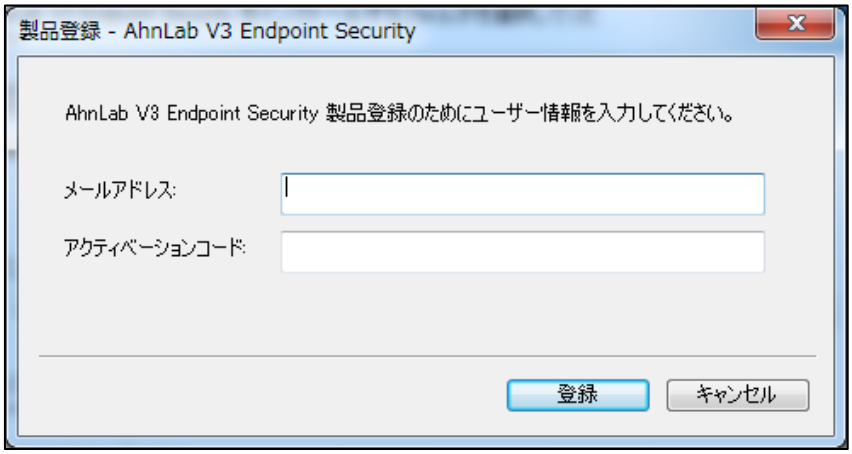
⑥ V3 Endpoint Security製品のインストール先フォルダーを指定します。



<インストール先の選択画面>

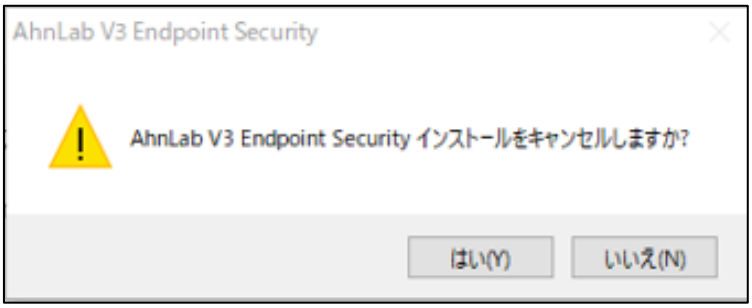
⑦ 製品登録のために必要な情報を入力して「登録」ボタンをクリックします。

メールアドレス、アクティベーションコードを入力してください。(* アクティベーションコードは、配布メールに記載されています。)



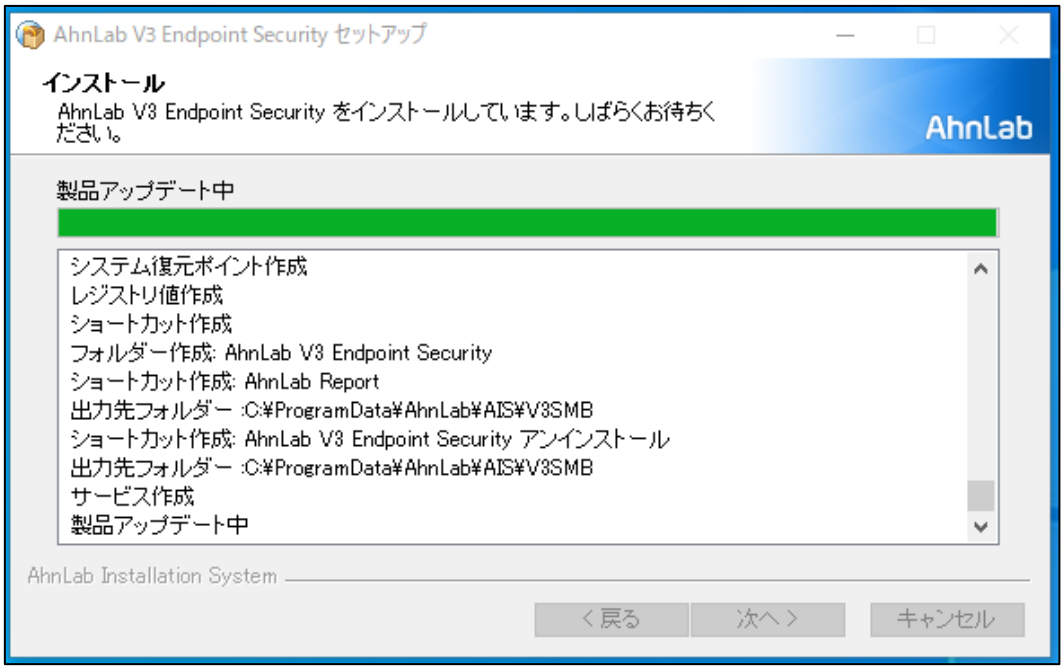
<製品登録画面>

ユーザー情報やアクティベーションコードを入力しないとインストールを完了できません。



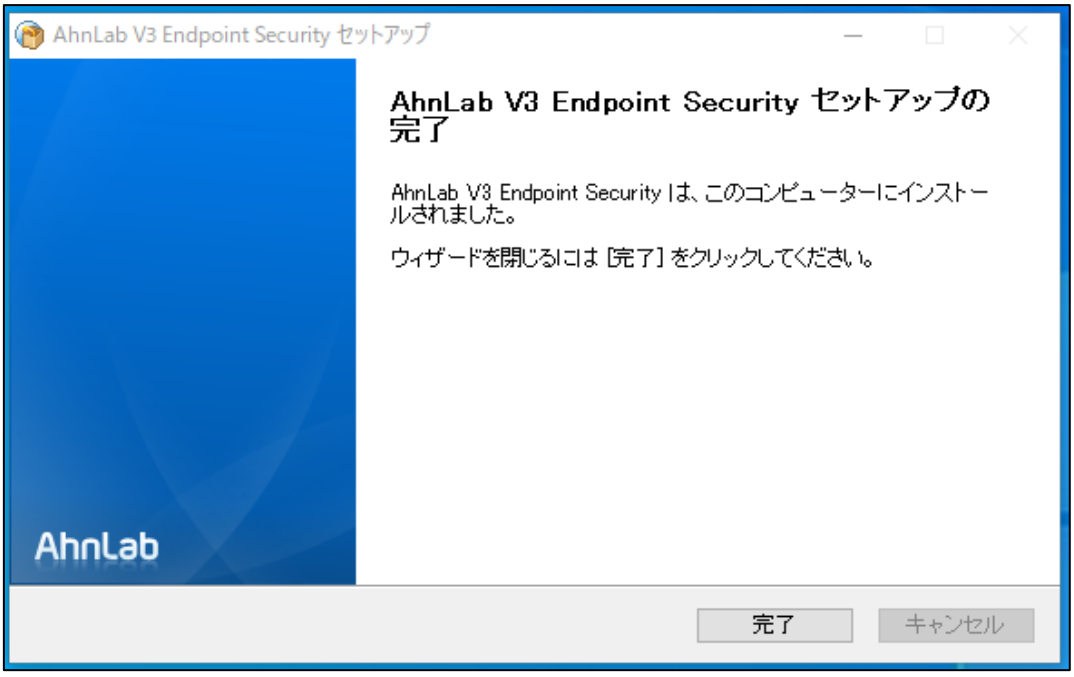
<キャンセルの選択肢画面>

⑧ インストールが進行されます。



<インストール進行画面>

⑨ **セットアップ完了画面が表示されたら「完了」ボタンをクリックします。**



<セットアップ完了画面>

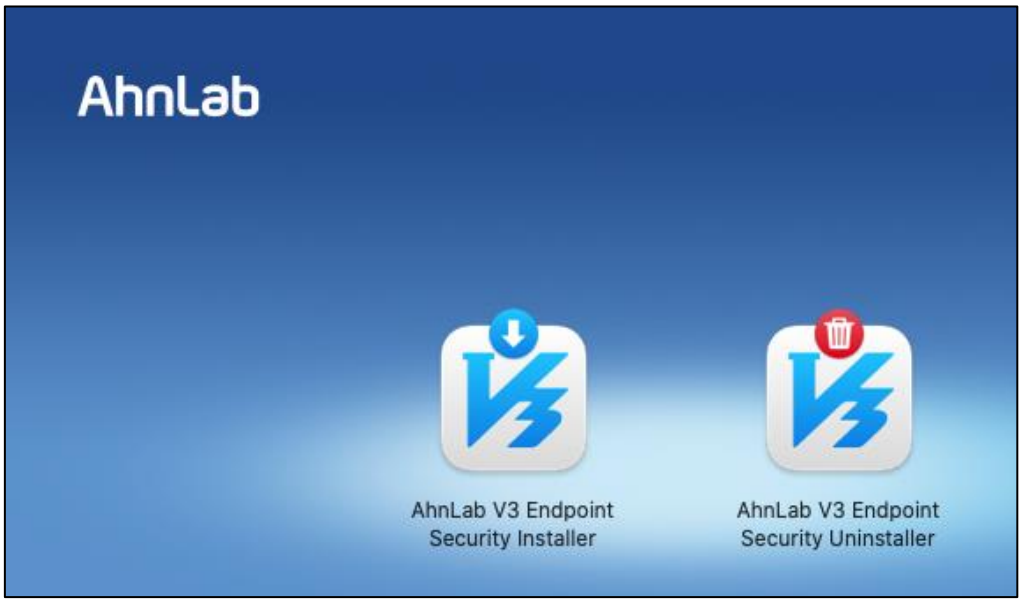
セットアップが完了すると AhnLab Security Center > デバイス タブで確認できるようになります。

3-2) V3 Endpoint Security (for Mac) クライアントのインストール

1) Mac PC製品のセットアッププロセスの流れは以下の通りです。

① ダウンロードしたインストールファイルを実行します。

② AhnLab V3 Endpoint Security Installer ファイルを実行します。



<製品のインストーラーファイル>

③ システムの警告メッセージが表示されたら「開く」ボタンをクリックします。

<システムメッセージ画面>

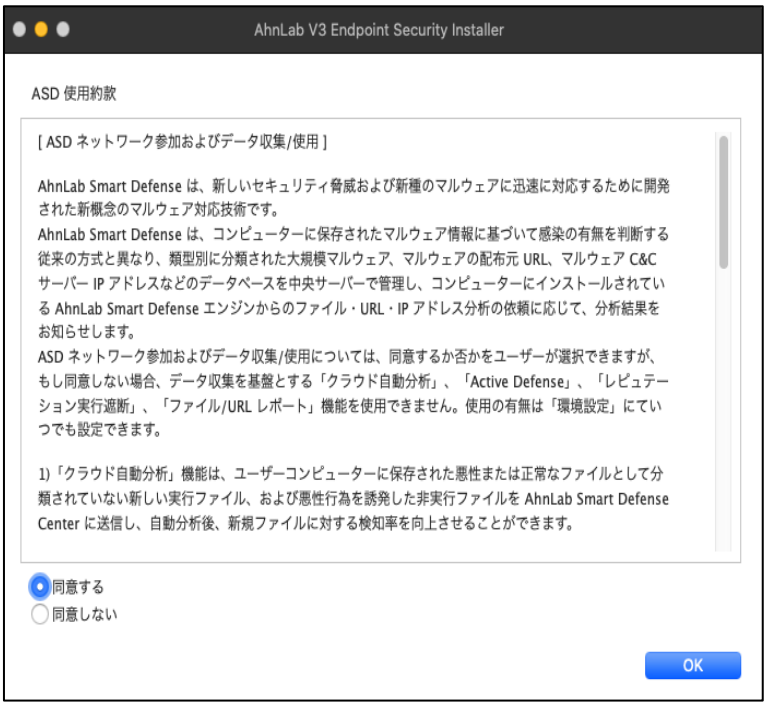
④ ソフトウェア使用約款画面が表示されたら「同意する」ボタンをクリックします。

<ソフトウェア使用約款画面>

⑤ 個人情報の取扱い画面が表示されたら「同意する」ボタンをクリックします。

<個人情報の取扱い画面>

⑥ ASD 使用許諾約款が表示されたら「同意する」にチェックし、「OK」ボタンをクリックします。



<ASD 使用約款画面>

⑦ ユーザー情報の登録画面で必要な情報を入力し、「登録」ボタンをクリックします。

メールアドレス、アクティベーションコードを入力してください。(* アクティベーションコードは、配布メールに記載されています。)

<ユーザー情報の登録画面>

⑧ 製品登録が完了するとインストールを進行します。

⑨ 完了メッセージが表示されます。

インストールが完了すると AhnLab Security Center > デバイス タブで確認できるようになります。

3-3) V3 Endpoint Security (for Android) クライアントのインストール

Android 製品のインストールプロセスの流れは以下の通りです。

① ダウンロードしたインストールファイルを実行します。

② ソフトウェア使用約款と個人情報の取扱いに同意し、「次へ」ボタンをタップします。

<約款への同意画面>

③ 製品登録のために必要な情報を入力して「登録」ボタンをタップします。

メールアドレス、アクティベーションコードを入力してください。(* アクティベーションコードは、配布メールに記載されています。)

<製品登録画面>

④ 製品登録メッセージが表示されたら、「OK」ボタンをタップします。

<登録完了画面>

製品登録が完了すると AhnLab Security Center > デバイス タブで確認できるようになります。

⑤ V3 Endpoint Securityを使用するために必要なアクセス権限を許可します。

<アクセス権限の設定画面>

⑥ インストール完了後、初回脆弱性チェックを実行します。

<初回デバイスの脆弱性チェック画面>

参考

Android13以降では[ユーザー補助]を使用するために、「権限付き設定]の許可が必要です。[権限付き設定]の許可方法は以下の通りです。

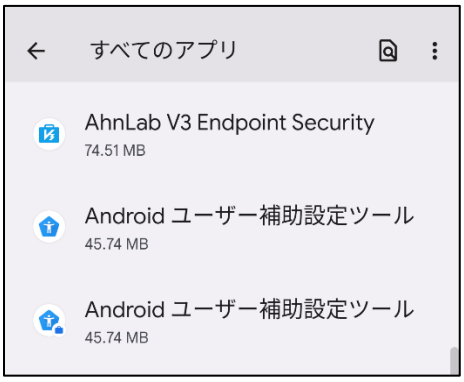
1）アクセス権限の設定画面にて、[ユーザー補助]ボタンをタップします。

<アクセス権限の設定画面>

2）設定「ユーザー補助」で [AhnLab V3 Endpoint Security]をタップすると[権限付き設定]のポップアップが表示されるので、[OK]をタップします。

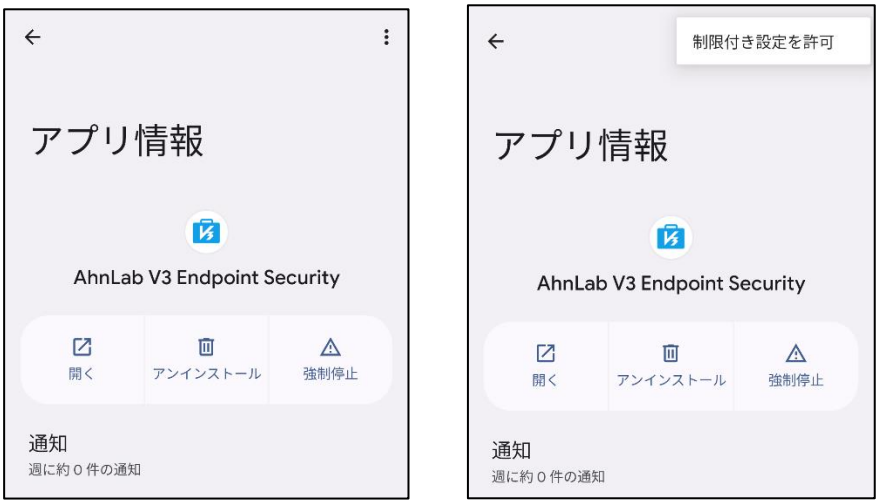
<デバイス設定「ユーザー補助」画面>

3）デバイスの設定「アプリ」を開き、[AhnLab V3 Endpoint Security]をタップします。



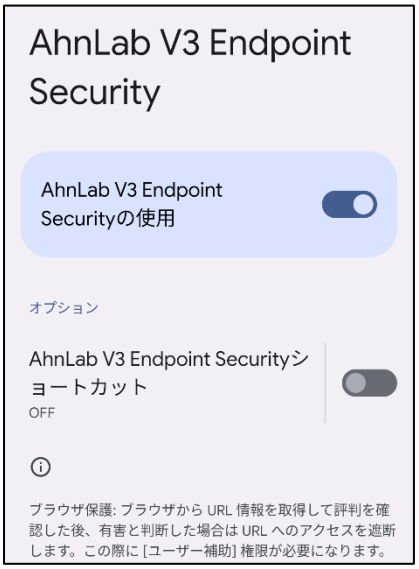
<デバイス設定「アプリ」画面>

4）画面右上の[⋮]をタップして表示された[権限付き設定を許可]をタップして、デバイスに設定している画面ロックのPINコードまたはパスワードを入力します。



<デバイス設定「アプリ」画面>

5）再度「ユーザー補助」から[AhnLab V3 Endpoint Security]を開き、[AhnLab V3 Endpoint Securityの使用]のトグルをONにして、ユーザー補助の設定が完了です。



<デバイス設定「ユーザー補助」画面>

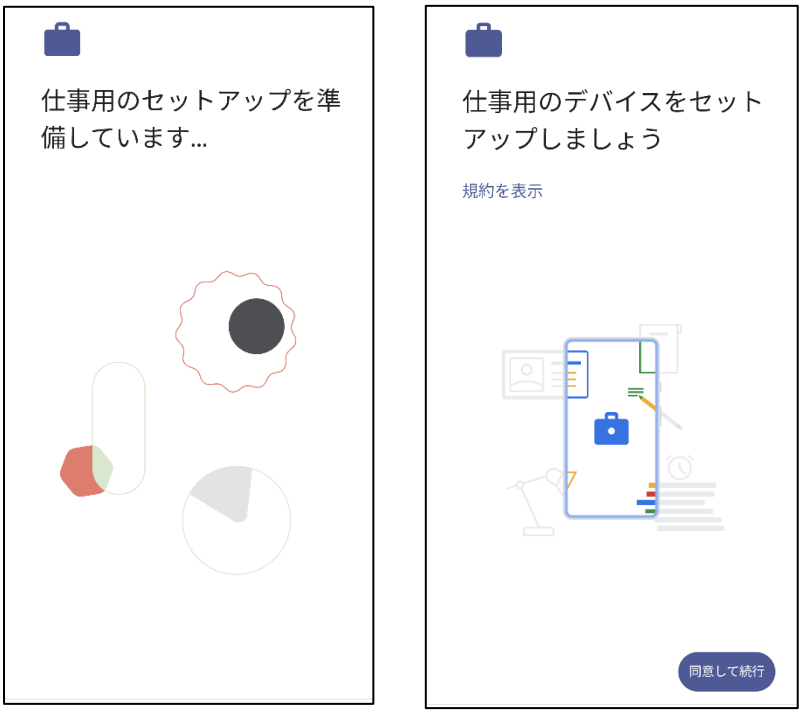
a) MDM 機能の有効化 - 個人所有デバイスに「仕事用プロファイル」を設定

個人所有のデバイス内に個人用プロファイルとは分離された「仕事用プロファイル」を設定することができます。「仕事用プロファイル」に設定する方法は次の通りです。

① 管理者が送信したインストールファイルダウンロードのメールから [MDM 機能の有効化] をクリックします。

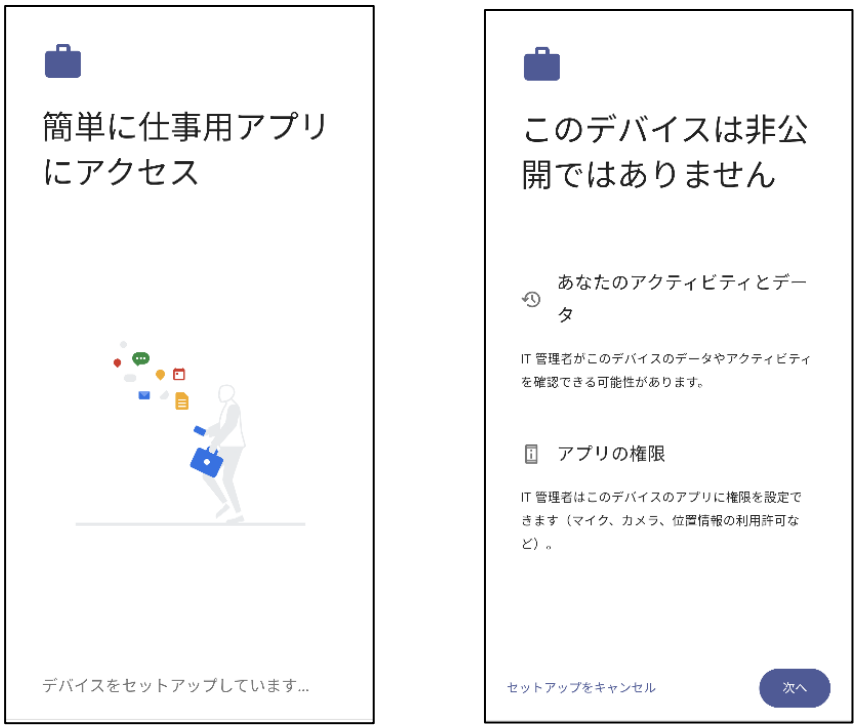
<インストールファイルダウンロードのご案内メール>

② [同意して続行]をタップして個人所有デバイスに「仕事用プロファイル」を設定します。



<仕事用プロファイルの設定画面>

④ 仕事用アプリにアクセスおよび必要な権限を確認し、「次へ」をタップして続行します。



<アクセスおよび権限設定画面>

⑤ デバイス登録を完了します。

<デバイス登録完了画面>

⑥ 仕事用アプリのインストールおよび V3 Endpoint Security の登録設定を行います。

<仕事用アプリのインストール完了画面>

参考

Security Center 管理者が送信した MDM ポリシーコマンドによって、画面ロックの設定が追加されます。

⑦ V3 Endpoint Security のソフトウェア使用約款および個人情報の取扱いに同意して、「次へ」ボタンをタップします。

<V3 Endpoint Security インストール画面>

⑧ メールアドレスおよびアクティベーションコードを入力します。

<V3 Endpoint Security 登録画面>

⑨ V3 Endpoint Security の登録を完了します。

<V3 Endpoint Security 登録完了画面>

製品登録が完了すると AhnLab Security Center > デバイス タブで確認できるようになります。

⑩ 仕事用アプリのアップデート後、すべての設定が完了されます。

<V3 Endpoint Security 登録画面>

参考
ユーザーが使用するデバイスによって、「仕事用プロファイル」に設定する手順や画面表示が多少異なります。

b) MDM 機能の有効化 – 会社所有デバイスを業務専用の「完全管理対象デバイス」に設定

会社所有デバイスを業務専用の「完全管理対象デバイス」に設定するには、端末の初期化が必要です。 初期化後、端末に対してMDM 機能を有効化し、「完全管理対象デバイス」に設定する方法は以下の通りです。

① 管理者が送信したインストールファイルダウンロードのメールから [QR コードで有効化] をクリックします。

② 端末にて「ようこそ」を6回タップしQRコードスキャナを起動して、①にて表示した QR コードをスキャンします。

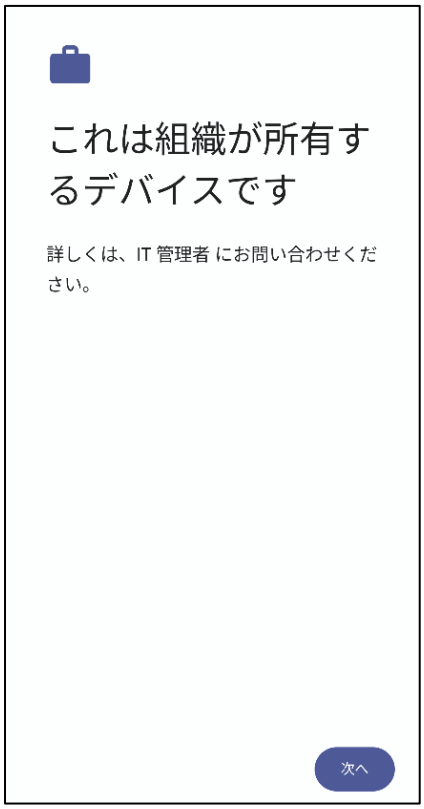
参考

QR コードをスキャンするには、 端末の初期化が必要です。端末を初期化し、端末の初期画面から QR コードのセットアップを開始してください。

※端末のカメラアプリからQRコードを読み込んでもMDMのセットアップは開始されません。

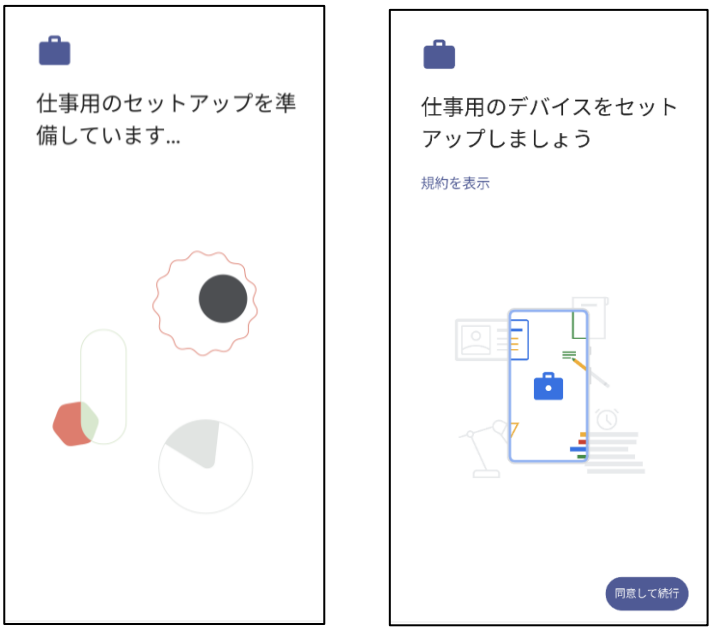
③ 接続する Wi-Fi を選択します。

④ 組織所有デバイスを業務専用の「完全管理対象デバイス」に設定します。「次へ」をタップして続行します。



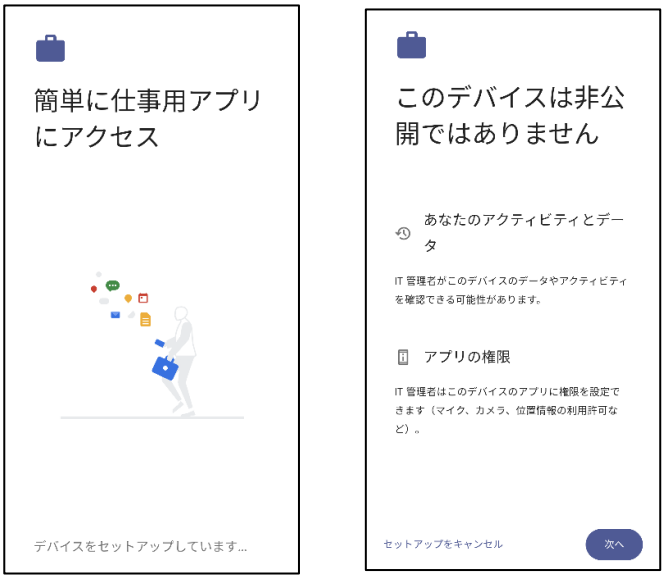
<「完全管理対象デバイス」の設定開始画面>

⑤　仕事用のデバイスをセットアップします。「同意して続行」をタップして続行します。



<完全管理対象デバイスの設定画面>

⑥ 仕事用アプリにアクセスおよび必要な権限を確認し、「次へ」をタップして続行します。



<アクセスおよび権限設定画面>

⑦ デバイス登録を完了します。

<デバイス登録完了画面>

⑧ 仕事用アプリのインストールおよび V3 Endpoint Security の登録設定を行います。

<仕事用アプリのインストール完了画面>

⑨ V3 Endpoint Security のソフトウェア使用約款および個人情報の取扱いに同意して、「次へ」ボタンをタップします。

<V3 Endpoint Security インストール画面>

⑩ メールアドレスおよびアクティベーションコードを入力します。

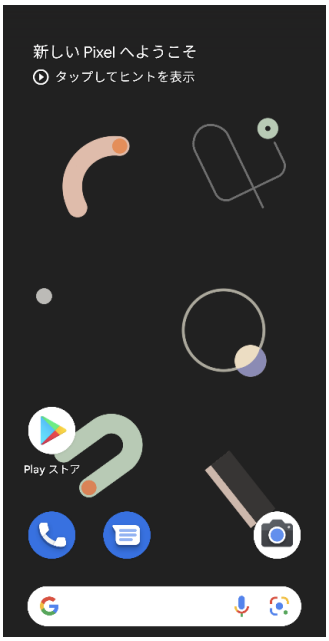
<V3 Endpoint Security 登録画面>

⑪ V3 Endpoint Security の登録を完了します。

<V3 Endpoint Security 登録完了画面>

製品登録が完了すると AhnLab Security Center > デバイス タブで確認できるようになります。

⑫ 仕事用アプリのアップデート後、すべての設定が完了されます。



<「完全管理対象デバイス」の設定完了画面>

参考
ユーザーが使用するデバイスによって、「完全管理対象デバイス」に設定する手順や画面表示が多少異なります。

3-4) V3 Endpoint Security (for iOS) クライアントのインストール

iOS 製品のインストールプロセスの流れは以下の通りです。

① ダウンロードしたインストールファイルを実行します。

② ソフトウェア使用約款と個人情報の取扱いにチェックし、「同意する」ボタンをタップします。

<約款への同意画面>

③ 製品登録のために必要な情報を入力して「登録」ボタンをタップします。

メールアドレス、アクティベーションコードを入力してください。(* アクティベーションコードは、配布メールに記載されています。)

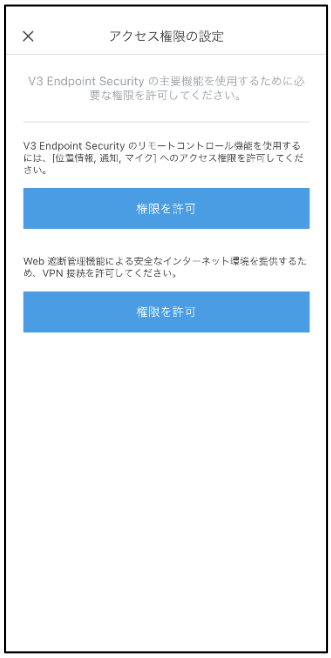
<製品登録画面>

④ 製品登録完了メッセージが表示されたら、「OK」ボタンをタップします。

<登録完了画面>

製品登録が完了すると AhnLab Security Center > デバイス タブで確認できるようになります。

⑤ V3 Endpoint Securityを使用するために必要なアクセス権限、VPN 接続権限の設定を有効にします。

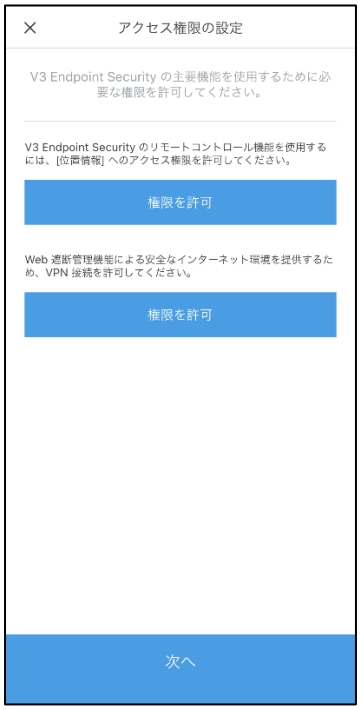


<アクセス権限の設定画面>

⑥ リモートコントロール機能を使用するための[権限を許可]をタップして、位置情報・通知・マイクの設定を行います。

<アクセス権限の設定画面>

⑦すべての権限を許可するとアクセス権限の設定画面に戻ります。再度「権限を許可」をタップします。



<アクセス権限の設定画面>

⑧　アプリの設定画面が表示されます。「位置情報」を「常に」に変更します。

<アプリの設定画面>

⑨ VPN接続の[権限を許可]をタップして、ポップアップ画面で[OK]をタップします。

<VPN 有効化の確認画面>

⑩ VPN構成の追加確認のポップアップ画面で[許可]をタップ後、iPhoneのパスコードを入力してVPN設定が完了します。

<VPN構成の追加画面>

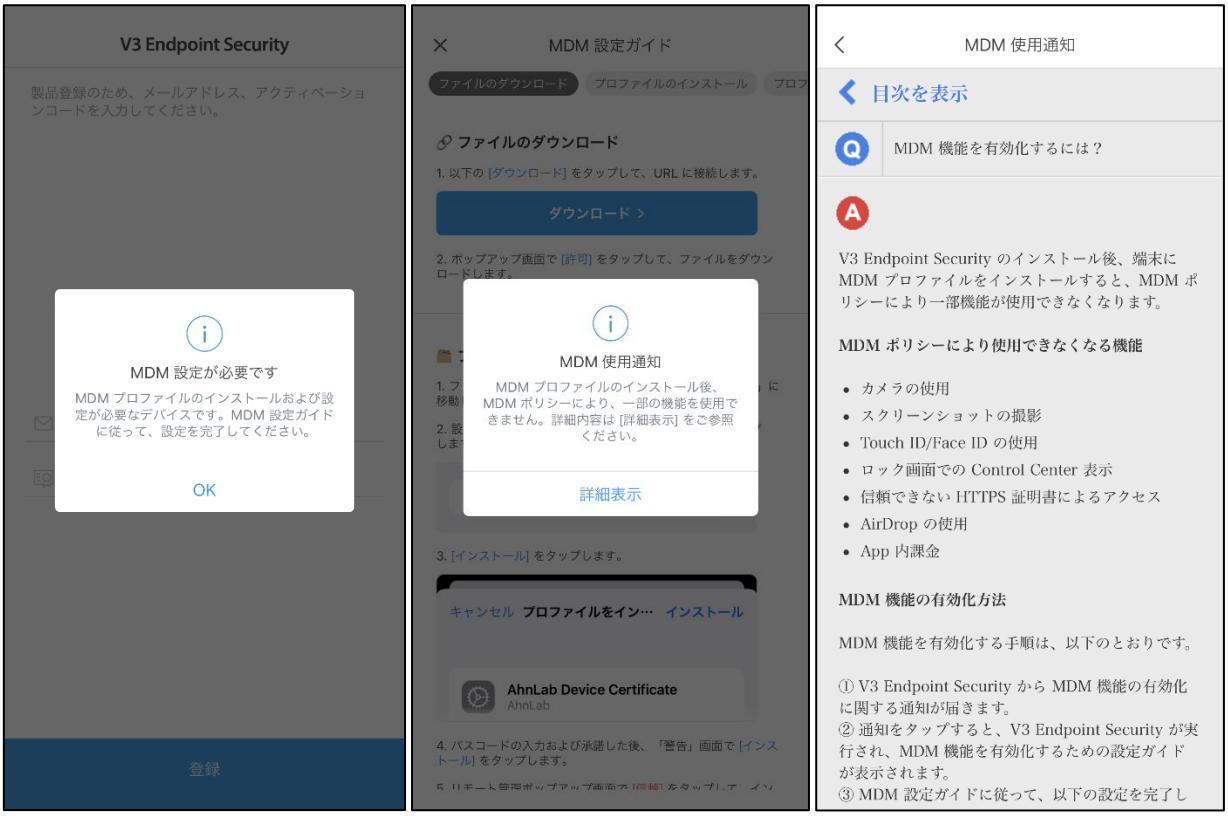
⑪ インストール完了後、初回脆弱性チェックを実行します。

<初回デバイスの脆弱性チェック画面>

a) MDM 機能の有効化

MDM ポリシーの適用対象デバイスは、V3 Endpoint Security を実行すると、MDM 機能が有効化されます。有効化する方法は以下の通りです。(* V3 Endpoint Security インストール必須)

① V3 Endpoint Security 登録完了後、 MDM 設定画面が表示されます。[OK]> [詳細表示]をタップしてMDM機能についての内容を確認します。

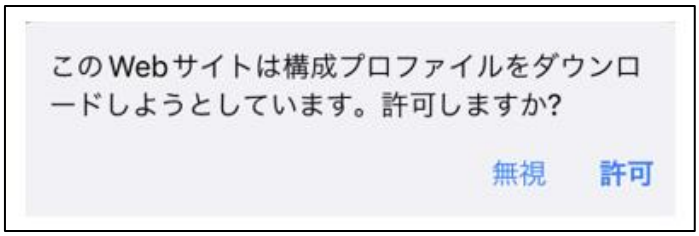


<MDM 機能詳細画面>

② MDM設定ガイド画面に戻り、[ダウンロード]をタップしてURLに接続します。

<MDM 設定ガイド画面>

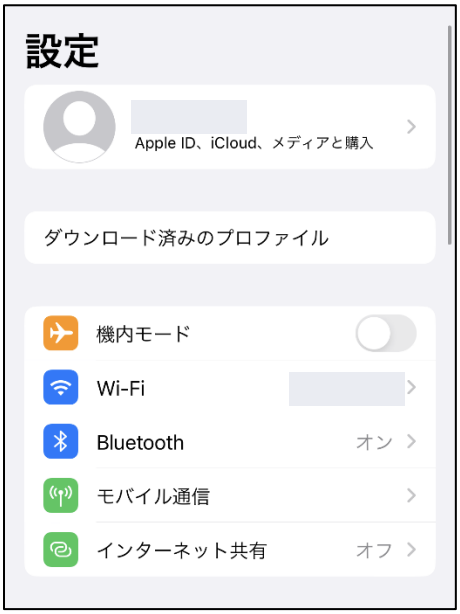
③ ポップアップ画面で、「許可」をタップして、ファイルをダウンロードします。



<ファイルダウンロード許可の確認画面>

④ ファイルのダウンロードが完了したら、デバイスの「設定」に移動します。

⑤ 設定画面から「ダウンロード済みのプロファイル」をタップします。



<設定画面>

⑥ 画面上部にある「インストール」をタップして、プロファイルをインストールします。

<プロファイルのインストール画面>

⑦ リモート管理ポップアップ画面で、「次へ」をタップしてインストールを完了します。

<リモート管理画面>

⑧ 「インストール」をタップします。

<ルート証明書･モバイルデバイス管理確認画面>

⑨ インストールが完了したら、インストール完了画面が表示されます。

<インストール完了画面>

3-5) V3 Server Security(Windows) クライアントのインストール

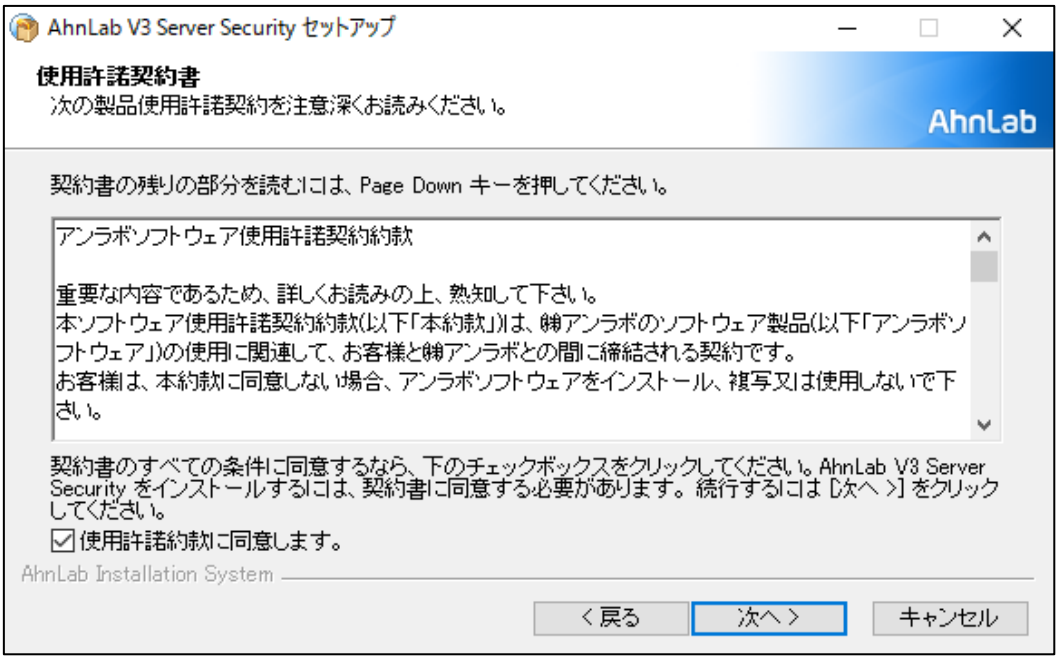
Windows Server製品のセットアッププロセスの流れは以下の通りです。

① ダウンロードしたインストールファイルを実行します。

② V3 Server Securityセットアップ画面が表示されたら「次へ」ボタンをクリックします。

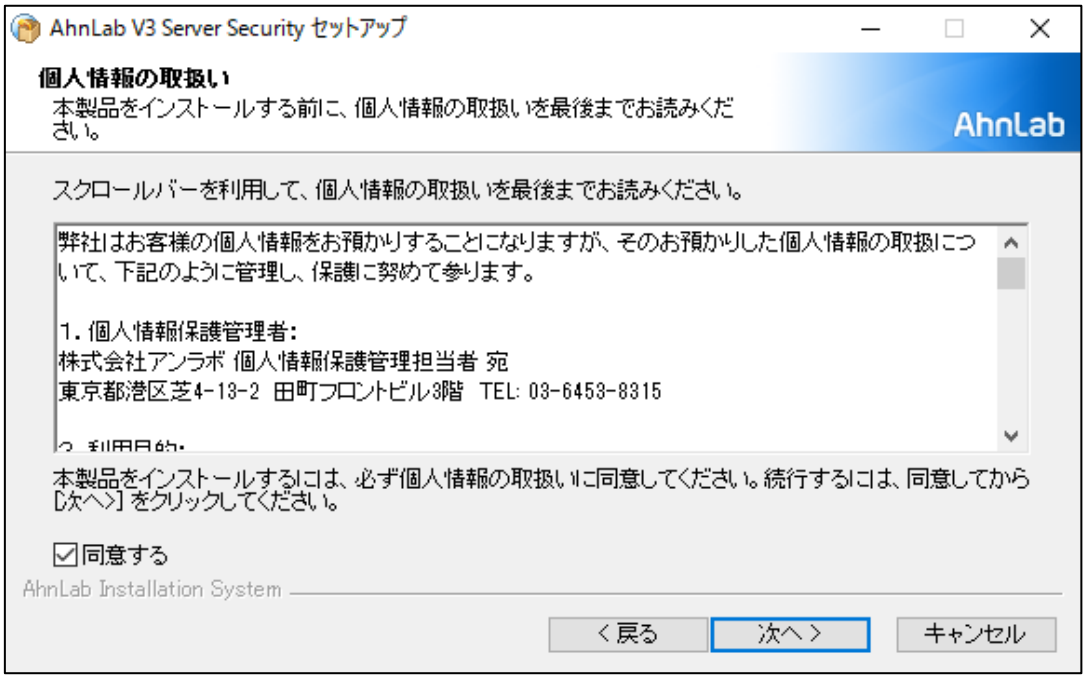
<セットアップ画面>

③ V3 Server Securityの使用許諾約款に同意し、「次へ」ボタンをクリックします。



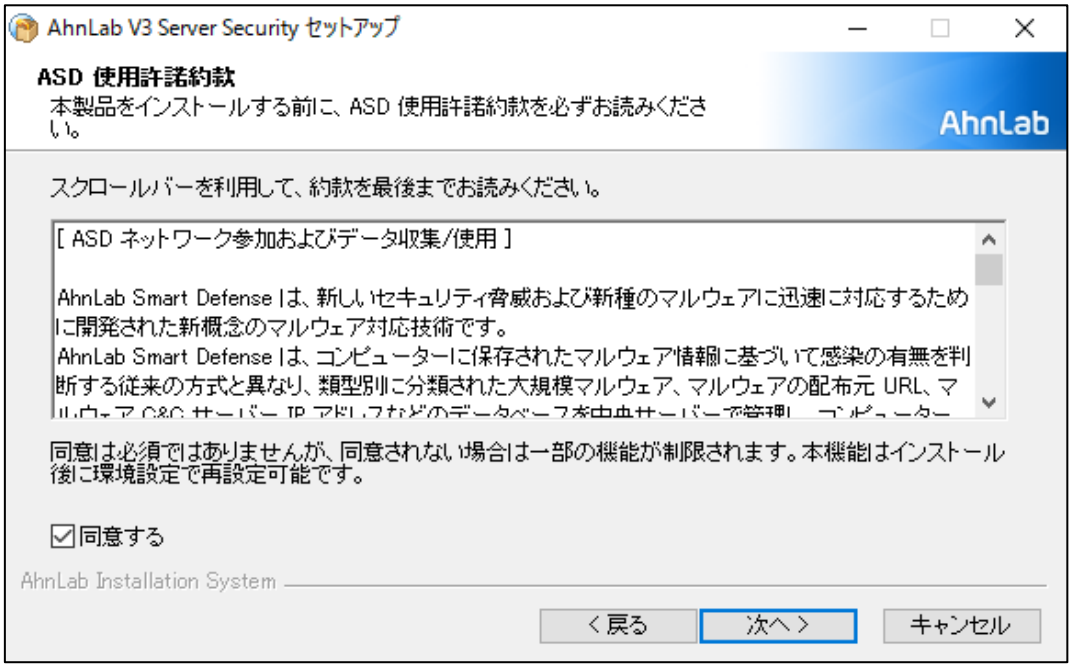
<使用許諾約款画面>

④ V3 Server Securityの個人情報の取扱いに同意し、「次へ」ボタンをクリックします。



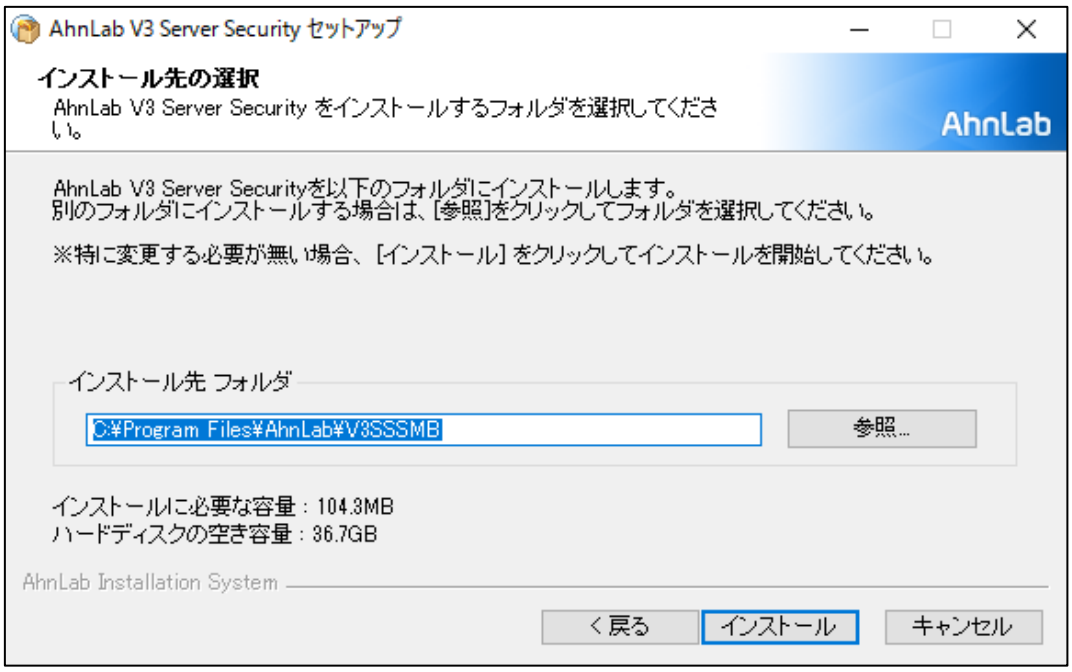
<個人情報の取扱い画面>

⑤ V3 Server SecurityのASD使用許諾約款に同意し、「次へ」ボタンをクリックします。



<ASD 使用許諾約款画面>

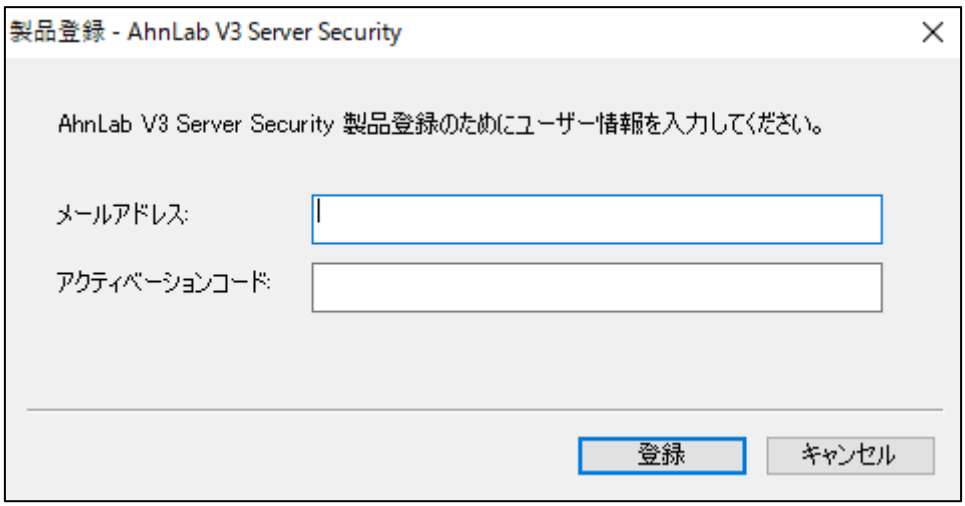
⑥ V3 Server Security製品のインストール先フォルダーを指定します。



<インストール先の選択画面>

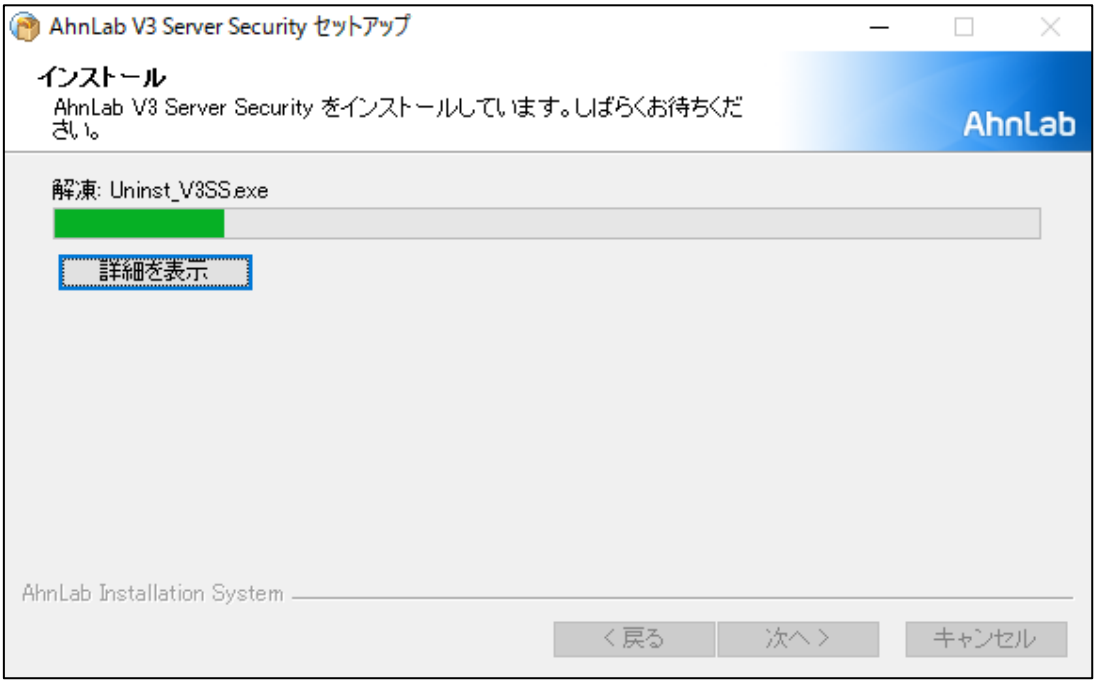
⑦ 製品登録のために必要な情報を入力して「登録」ボタンをクリックします。

メールアドレス、アクティベーションコードを入力してください。(* アクティベーションコードは、配布メールに記載されています。)



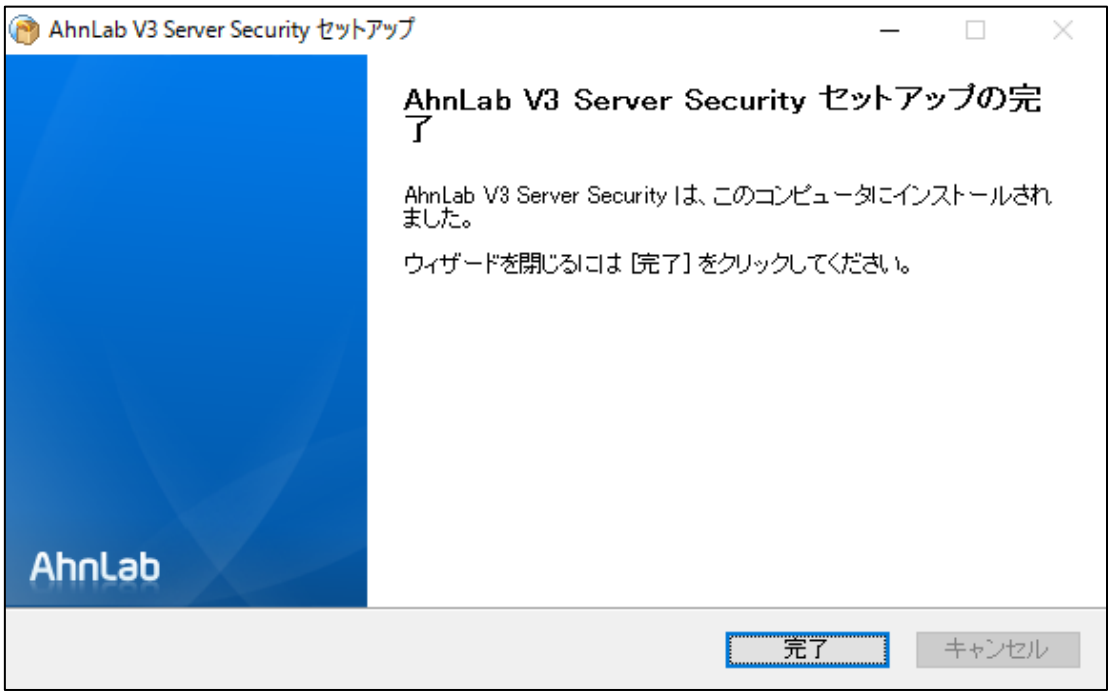
<製品登録画面>

⑧ インストールが進行されます。



<インストール進行画面>

⑨ セットアップ完了画面が表示されたら「完了」ボタンをクリックします。



<セットアップ完了画面>

セットアップ が完了すると AhnLab Security Center > デバイス タブで確認できるようになります。

3-6) V3 Server Security (Linux) クライアントのインストール

Linux Server製品のインストールプロセスの流れは以下の通りです。

① ダウンロードしたインストールファイルの圧縮を解除して、実行します。

```
[root@Server: /tmp ]# tar zxvf v3ss-X.X.X.X.X.tar.Z
```

② インストールファイルのディレクトリに移動します。

```
[root@Server: /tmp ]# cd v3ss
```

③ インストールスクリプト install.sh を実行します。

```
[root@Server: /tmp/v3ss ]# ./install.sh
```

④ パッケージインストールのメッセージが表示されます。

※インストールするシステムに COMMNAD、LIBRARY パッケージがない場合のみ表示されます。 同意「y」を入力して、Enter キーを押します。

(COMMAND)

```
'command name' : Command is not installed.
Note that the package name may differ depending on the distribution you use.
```

(LIBRARY)

```
'library name' : Library is not installed.
Note that the package name may differ depending on the distribution you use.
```

```
Do you want to install 'package name' package? (y/n) :
```

⑤ ソフトウェア使用許諾契約書(EULA)の同意メッセージが表示されます。

同意「y」を入力して、Enter キーを押します。

```
AhnLab Software License Agreement

IMPORTANT - READ CAREFULLY BEFORE USING AHNLAB SOFTWARE.
This Software License Agreement (this "Agreement") is a legal agreement by and between you and AhnLab, Inc. ("AhnLab") with regard
...(省略)...
```

```
Do you accept the terms of the EULA?(y/n):
```

⑥ 個人情報の取扱いの同意メッセージが表示されます。

同意「y」を入力して、Enter キーを押します。

```
AhnLab Japan, Inc. ( AhnLab ) will store your personal information and make efforts to manage and protect your personal information as set forth below:

1.  Manager in Charge of Protection of Personal Information
...(省略)...
```

```
Do you accept the privacy policy of the AhnLab?(y/n):
```

⑦ メールアドレス入力のメッセージが表示されます。

メールアドレスを入力して、 Enter キーを押します。

```
E-mail address:
```

⑧ アクティベーションコード確認のメッセージが表示されます。

アクティベーションコードを入力して、 Enter キーを押します。

```
Activation code:
```


⑨ 製品のインストールディレクトリを確認するメッセージが表示されます。

デフォルトのディレクトリ「/opt/AhnLab/v3serversecurity」にインストールする場合は、 Enter キーを押します。別のディレクトリにインストールする場合は、インストールディレクトリを入力して Enter キーを押します。

```
Installation Path(default: /opt/AhnLab/v3serversecurity):
```

⑩ Web 保護機能の使用有無を確認するメッセージが表示されます。

Web 保護機能を使用する場合は、Enter キーを押します。

```
Use Web Security?(y/n) (default: Yes):
```

⑪ Web 画面にアクセスするためのポートを確認するメッセージが表示されます。

デフォルトポートを使用する場合は、 Enter キーを押します。別のポートを使用する場合は、使用するポートを入力して Enter キーを押します。

```
//Web 保護を有効にする場合
HTTP Port (default: 443):

//Web 保護を無効にする場合
HTTP Port (default: 80):
```

⑫ 製品の表示言語を確認するメッセージが表示されます。

```
Select Language (1:Japanese, 2:Korean, 3:English):
```

⑬ 入力内容の確認およびインストール進行状況を選択するメッセージが表示されます。


```
[ Configured Information ]
------------------------------------------------------------------------
Installation Path: /opt/AhnLab/v3serversecurity
Use Web Security: Yes
HTTP Port: 443
Language : Korean
------------------------------------------------------------------------

Do you want to continue to install?(y/n):
```

⑭ 製品のインストールが完了したら、次のメッセージが表示されます。

```
Installation completed.

Starting the process...
```

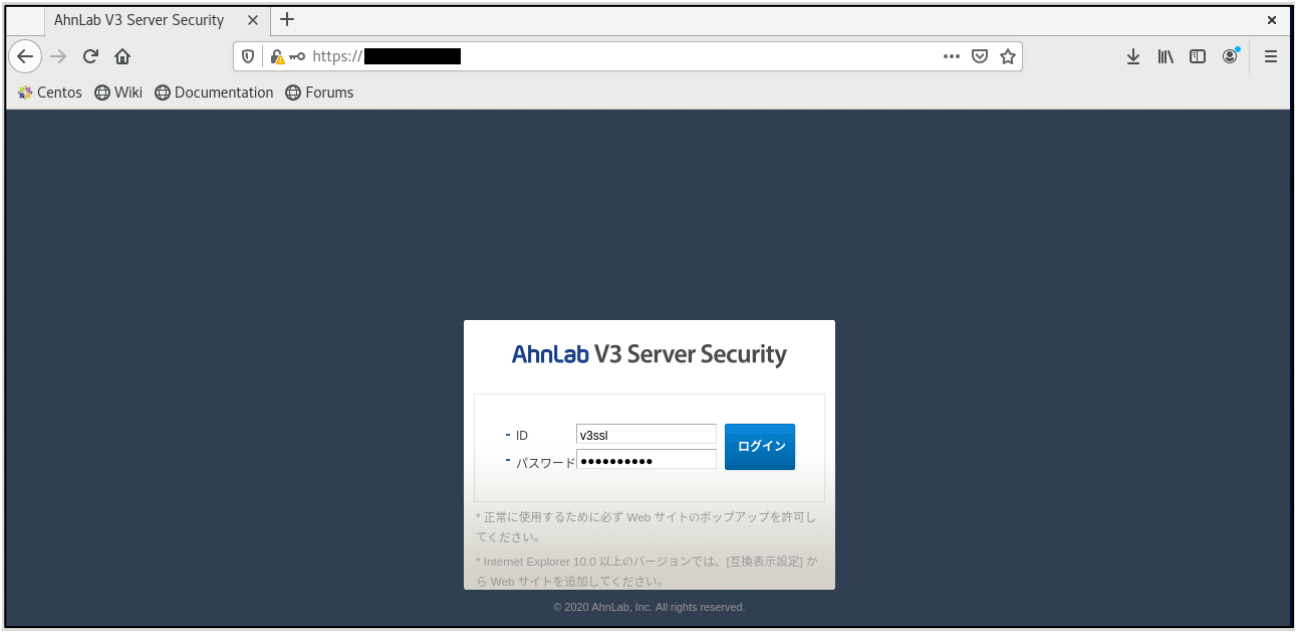
⑮ 製品をインストールしたディレクトリに移動して、製品の実行状況を確認します。

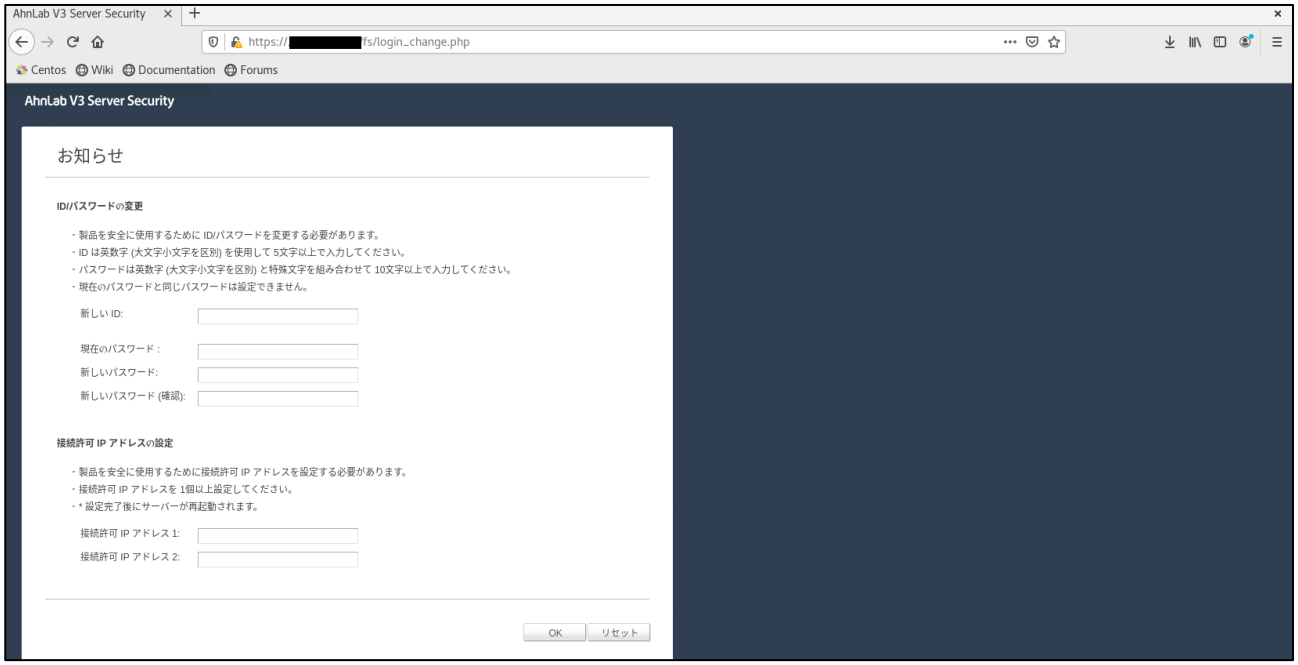
```
[root@Server: /opt/AhnLab/v3serversecurity]# ./v3ss.sh status

 ----------------------------------------
   V3 Server Security for Linux status
 ----------------------------------------
 v3ssd                  - running (15691)
 v3ssd watchdog         - running (15823)
 v3ss-agentd            - running (15702)
 v3ss-agentd watchdog   - running (15831)
 lighttpd               - running (15697)
 v3fbmond               - running (15819)
 v3fbmond watchdog      - running (15842)
 ----------------------------------------
```

⑯ ブラウザで製品をインストールしたIPアドレスに接続して、デフォルトに設定されているIDとPWを変更します。

接続許可IPは、製品をインストールしたIPアドレスを入力します。





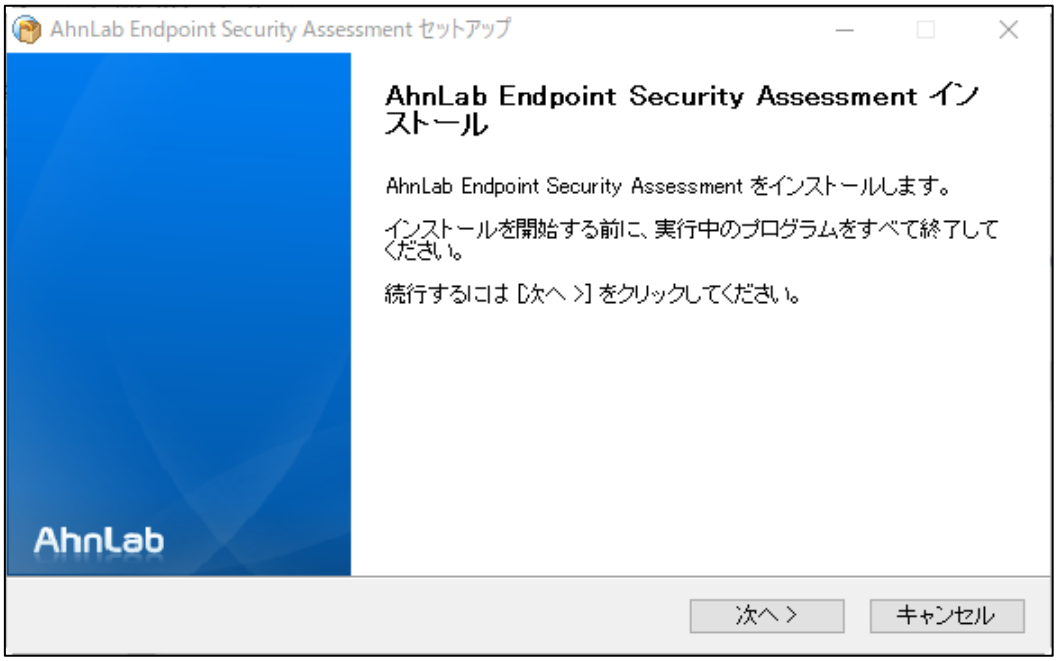
セットアップ が完了すると AhnLab Security Center > デバイス タブで確認できるようになります。

3-7) AhnLab Endpoint Security Assessment (Windows) クライアントのインストール

AhnLab Endpoint Security Assessment 製品のセットアッププロセスの流れは以下の通りです。

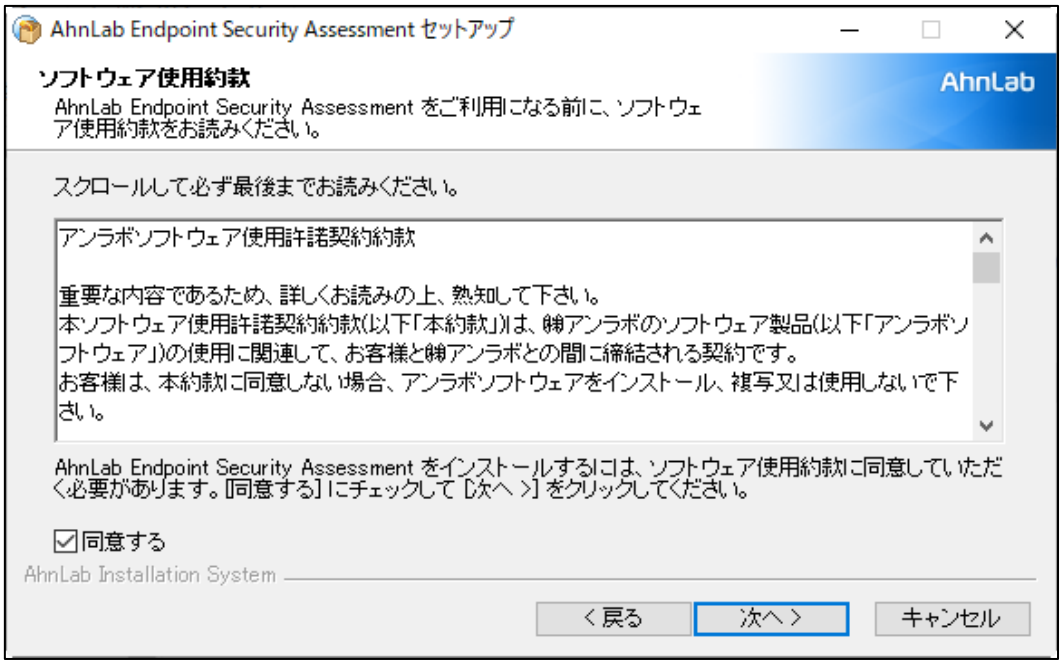
① ダウンロードしたセットアップファイルを実行します。

② AhnLab Endpoint Security Assessment インストール画面が表示されたら「次へ」ボタンをクリックします。



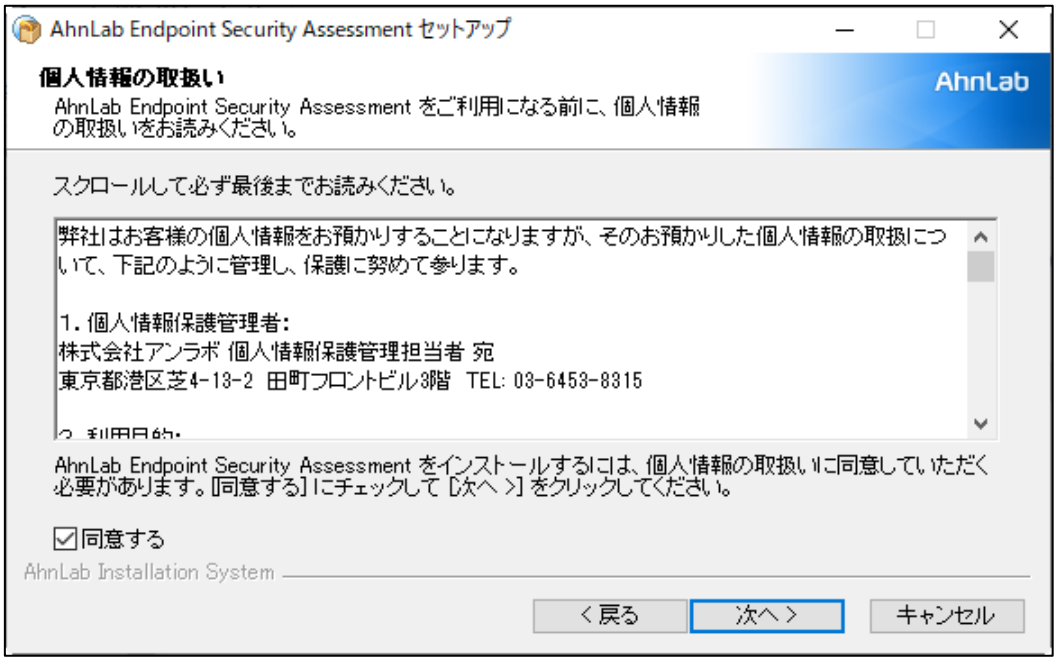
<インストール画面>

③ AhnLab Endpoint Security Assessmentのソフトウェア使用約款に同意し、「次へ」ボタンをクリックします。



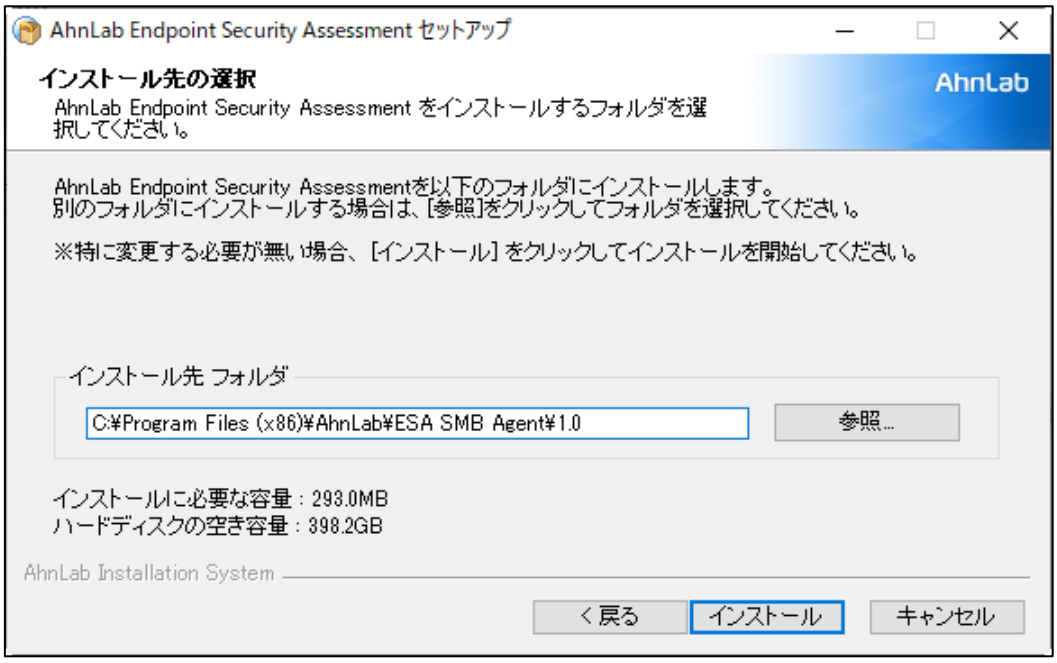
<ソフトウェア使用約款画面>

④ AhnLab Endpoint Security Assessmentの個人情報の取扱いに同意し、「次へ」ボタンをクリックします。



<個人情報の取扱い画面>

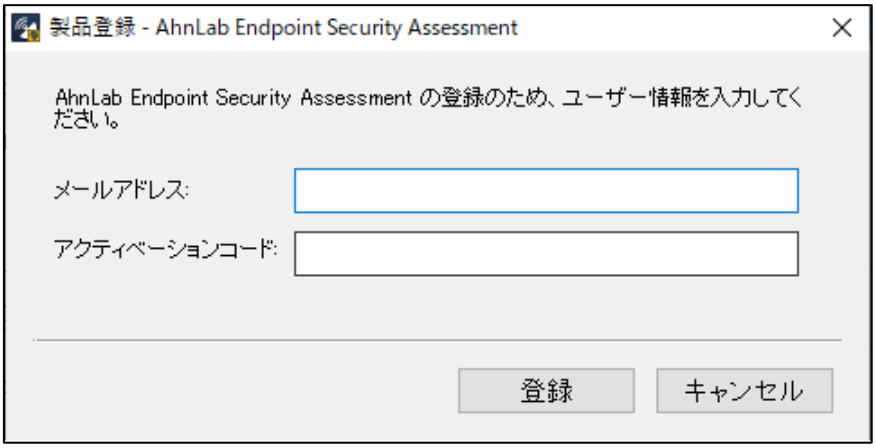
⑤ AhnLab Endpoint Security Assessment製品のインストール先フォルダーを指定します。



<インストール先の選択画面>

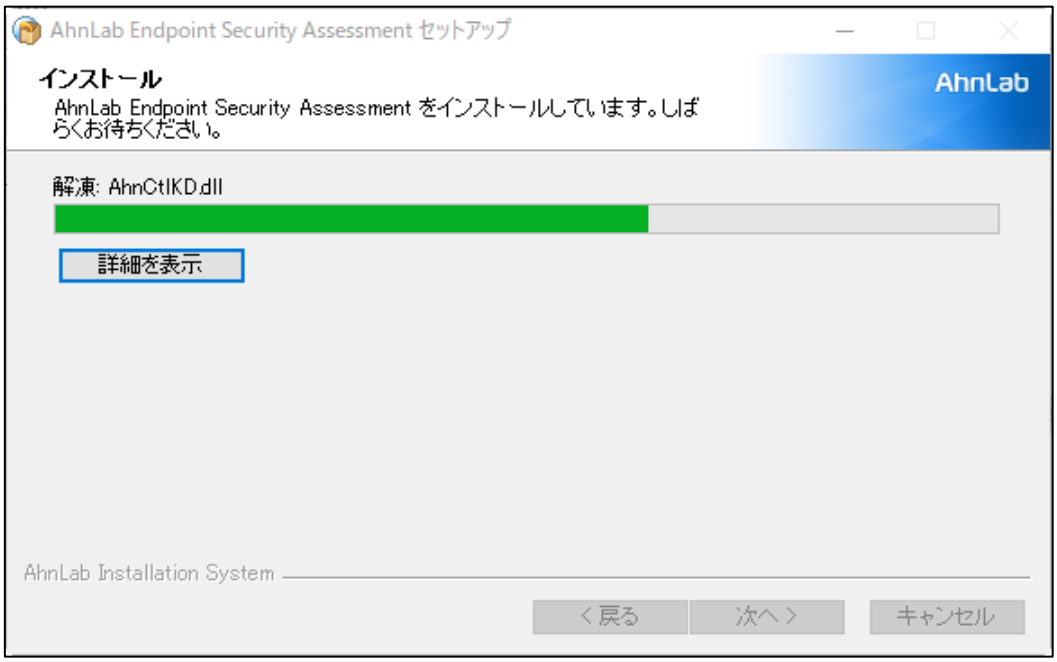
⑥ 製品登録のために必要な情報を入力して「登録」ボタンをクリックします。

ユーザー名、メールアドレス、アクティベーションコードを入力してください。(* アクティベーションコードは、配布メールに記載されています。)



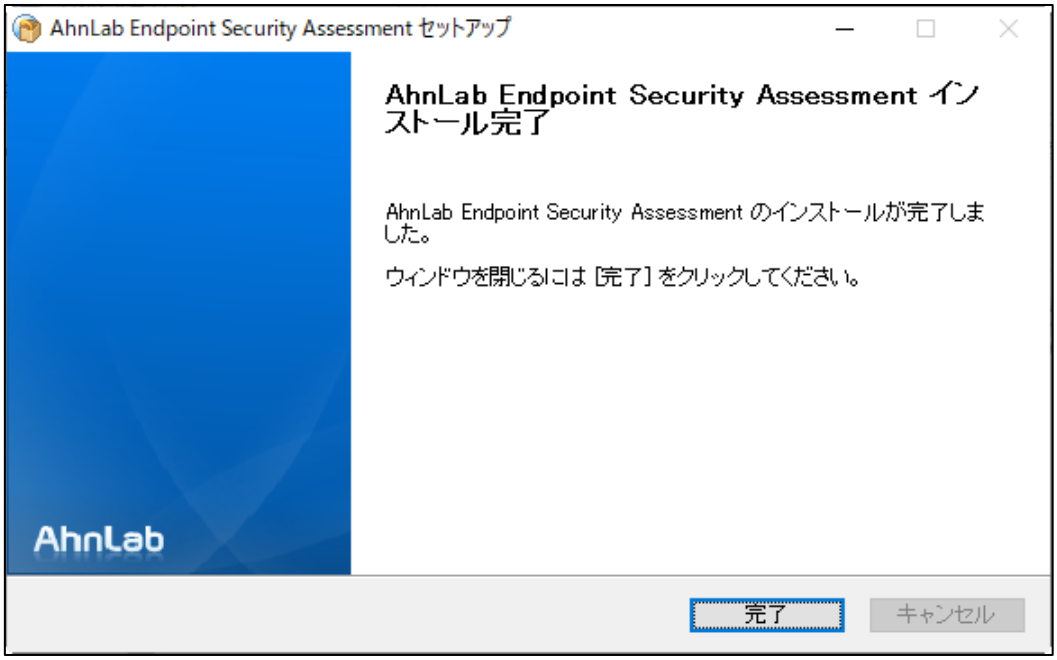
<製品登録画面>

⑦ インストールが進行されます。



<インストール進行画面>

⑧ セットアップ完了画面が表示されたら「完了」ボタンをクリックします。



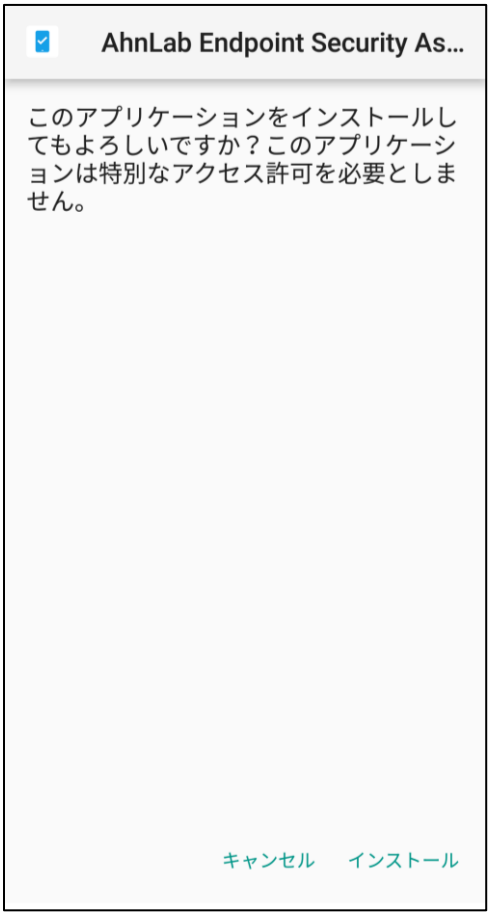
<セットアップ完了画面>

セットアップ が完了すると AhnLab Security Center > デバイス タブで確認できるようになります。

3-8) Endpoint Security Assessment (For Android) クライアントのインストール

Android 製品のインストールプロセスの流れは以下の通りです。

① ダウンロードしたインストールファイルを実行して、インストールを開始します。



<製品のインストール画面>

② ソフトウェア使用約款と個人情報の取扱いに同意し、「OK」ボタンをタップします。

<約款への同意画面>

③ 製品登録のために必要な情報を入力して「登録」ボタンをタップします。

メールアドレス、アクティベーションコードを入力してください。(* アクティベーションコードは、配布メールに記載されています。)

<製品登録画面>

④ 製品登録完了メッセージが表示されたら、「OK」ボタンをタップします。

<登録完了画面>

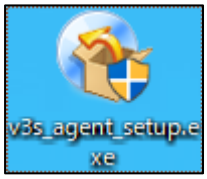
⑤ インストール完了後、初回脆弱性チェックを実行します。

<初回デバイスの脆弱性チェック画面>

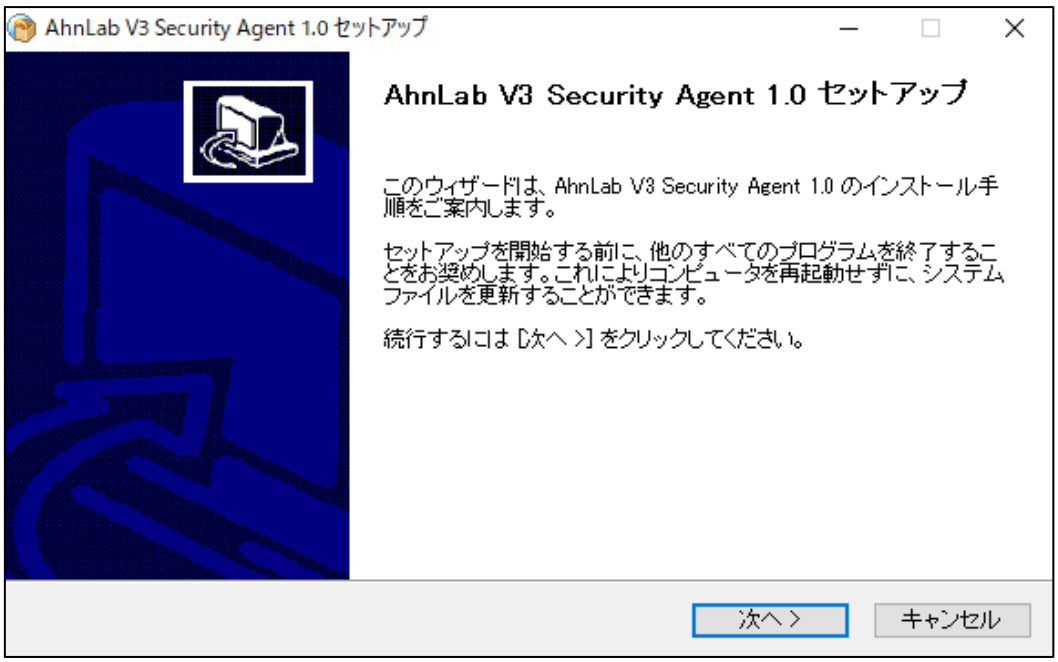
3-9) AhnLab V3 Security Agent (for Windows/Server) クライアントのインストール

Windows PC/Server 製品の V3 Security Agent インストールプロセスの流れは以下の通りです。

① ダウンロードしたインストールファイルを実行します。

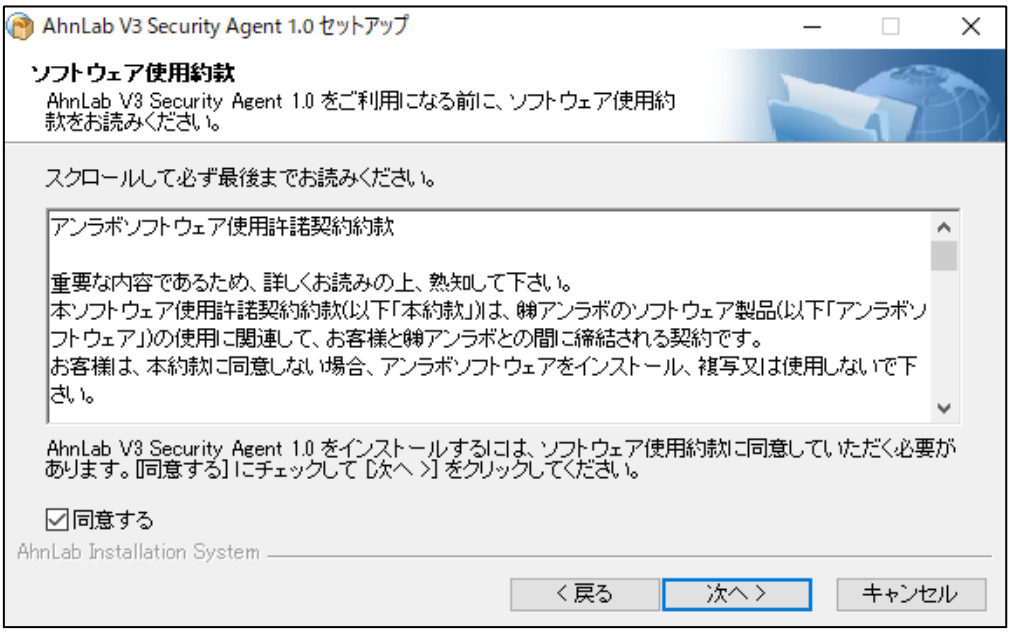


② <V3 Security Agent インストール>画面が表示されたら、[次へ] をクリックします。



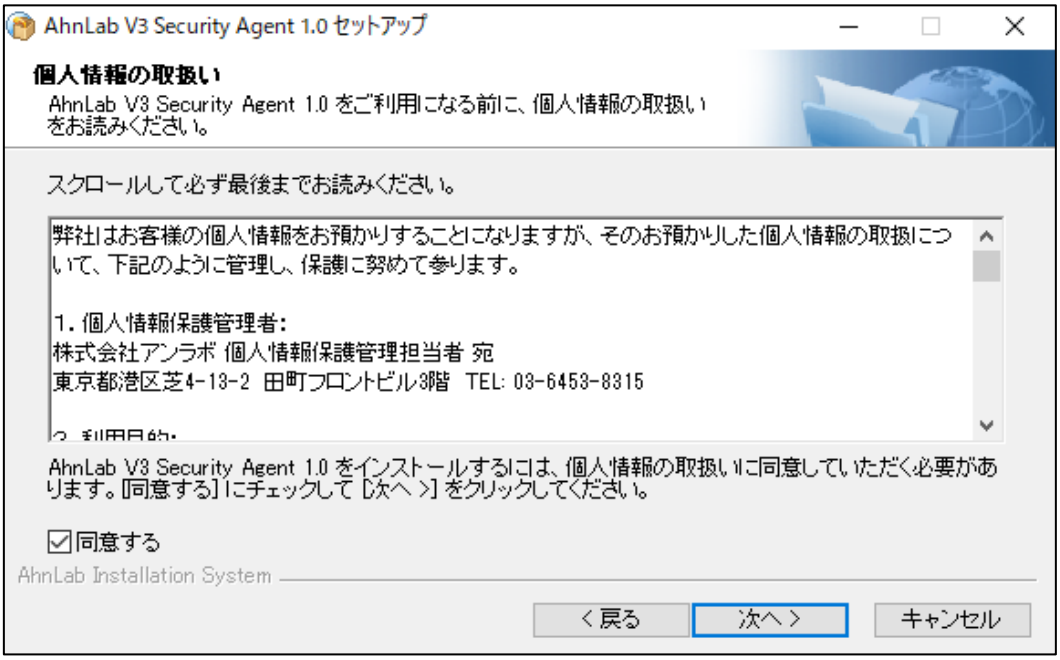
<インストール開始の画面>

③ <ソフトウェア使用約款>画面から、[同意する] にチェックして、[次へ] をクリックします。



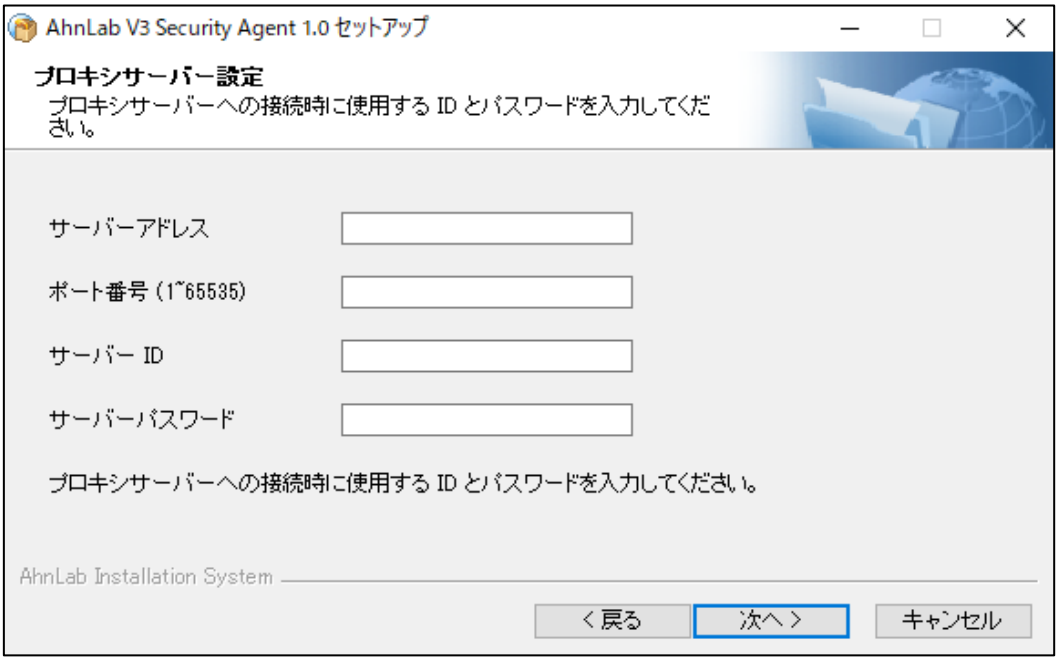
<ソフトウェア使用約款の画面>

④ <個人情報の取扱い>画面から、[同意する] にチェックして、[次へ] をクリックします。



< 個人情報の取扱いの画面>

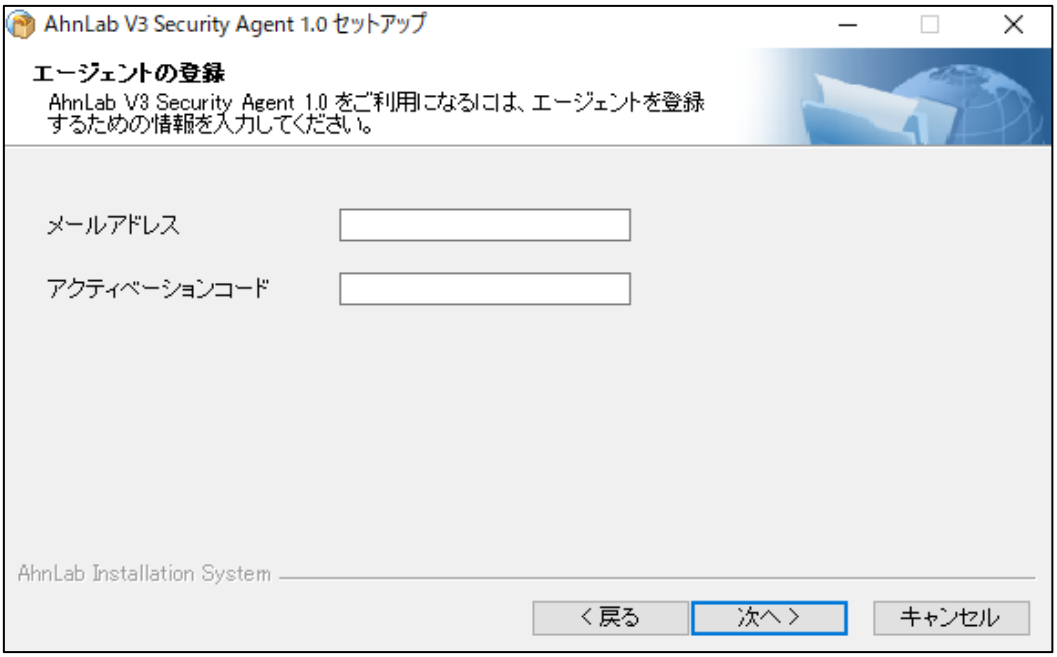
⑤ <プロキシサーバー設定>画面から、プロキシサーバー情報およびプロキシサーバーへの接続時に使用する ID とパスワードを入力して、[次へ] をクリックします。
(※プロキシサーバー設定を行わなくても次のステップに進めます。)



<プロキシサーバー設定の画面>

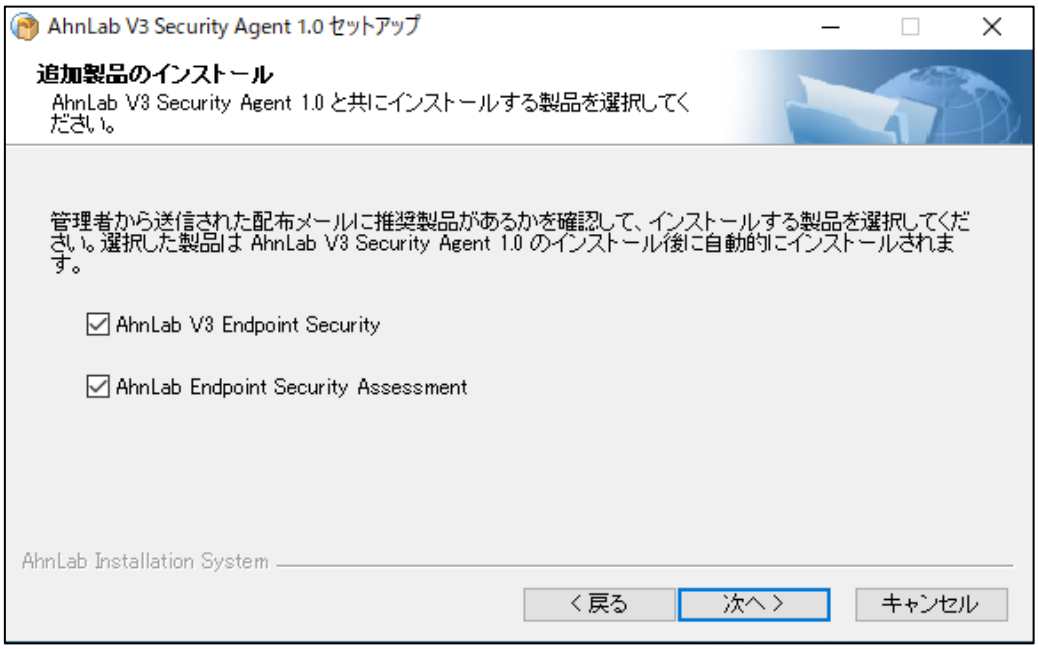
⑥ <エージェントの登録>画面から、メールアドレスとアクティベーションコードを入力して、[次へ] をクリックします。

* メールアドレスとアクティベーションコードはエージェントの登録およびユーザー情報の認証に必要な必須情報です。
Security Center の管理者から送信されたインストールファイルダウンロードの案内メールからメールアドレスとアクティベーションコードを確認してください。 または、 Security Center のファイル > ファイルのダウンロード画面や、設定 > システム > ライセンス管理画面からも確認できます。



<エージェントの登録画面>

⑦ <追加製品のインストール>画面から、エージェントと共にインストールする製品を選択して、[次へ] をクリックします。



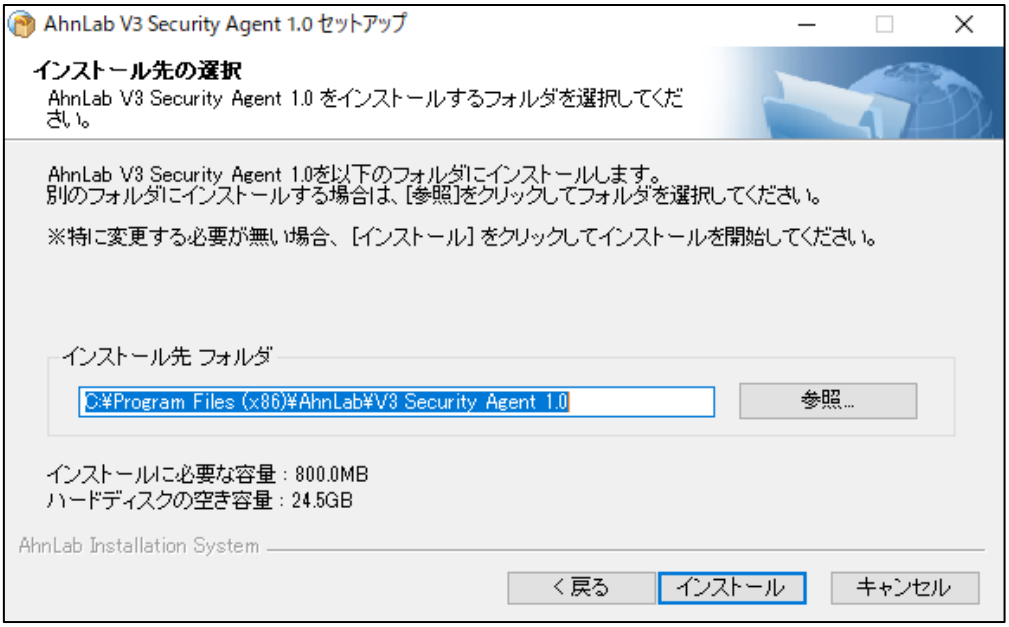
<追加製品のインストール画面>

参考

購入済のライセンスがある場合 、V3 Security Agent のインストール進行中に Desktop / Server 環境の有無によって、インストール可能な製品が表示されます。選択した製品は V3 Security Agent のインストール後に自動的にインストールされます。

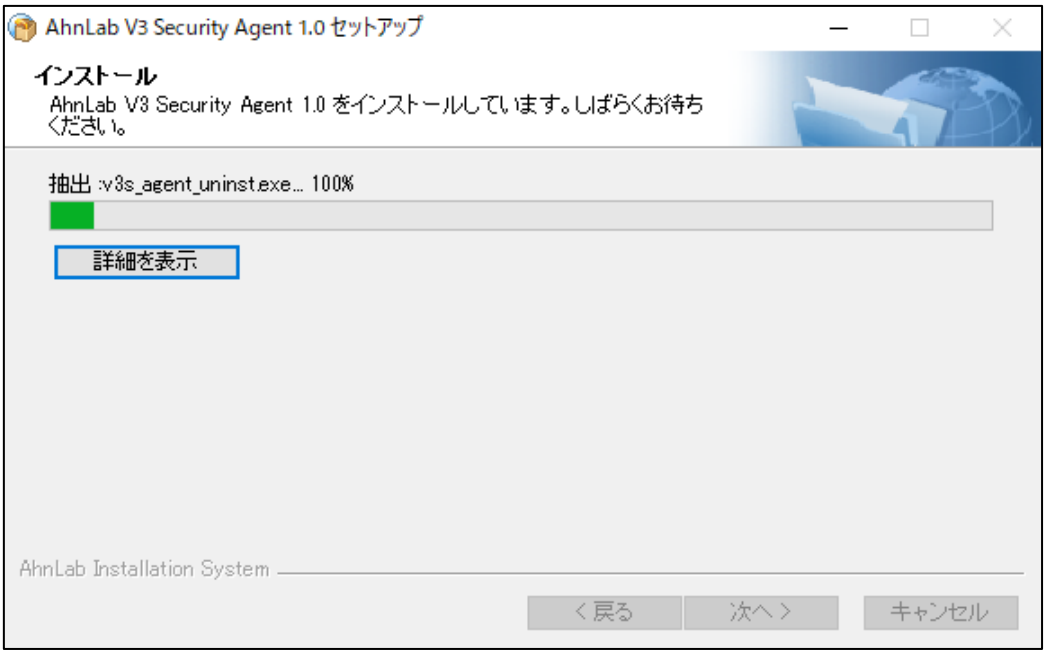
⑧ <インストールフォルダの選択>画面から、インストールするフォルダを選択して、[次へ] をクリックします。

インストール先フォルダはデフォルトフォルダに設定することを推奨します。



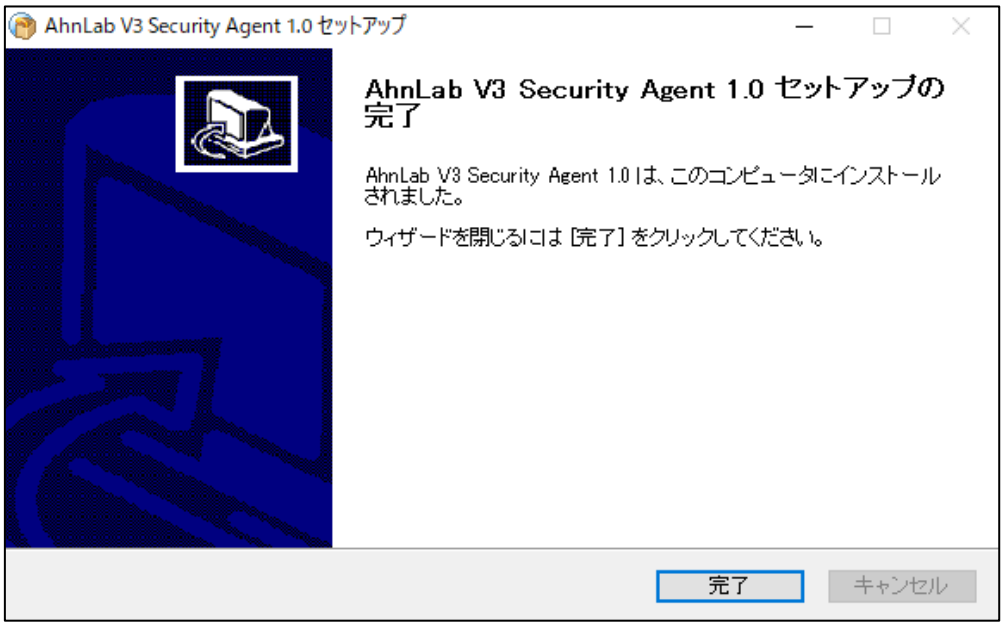
<インストール先の選択画面>

⑨ V3 Security Agent のインストールが開始されます。



<インストールの進行画面>

⑩ 製品のインストールが完了したら、[完了] をクリックします。



<インストール完了画面>

セットアップ が完了すると AhnLab Security Center > デバイス タブで確認できるようになります。

4. V3 Security for Business クライアントのアンインストール

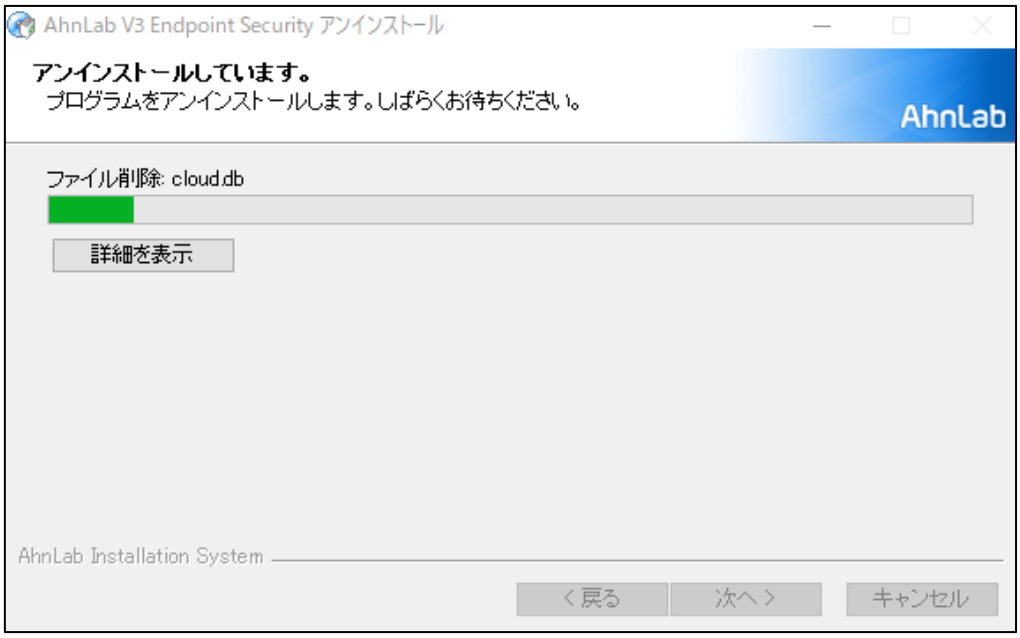
Security Center のデバイスリストから管理者がデバイスの登録を解除すると、ユーザー側のデバイスで製品が使用できなくなります。ただし、ユーザーデバイスにインストールされた製品のアンインストールは、デバイス上で直接行う必要があります。

<Security Center デバイスの登録解除画面>

4-1) V3 Endpoint Security (for Windows) クライアントのアンインストール

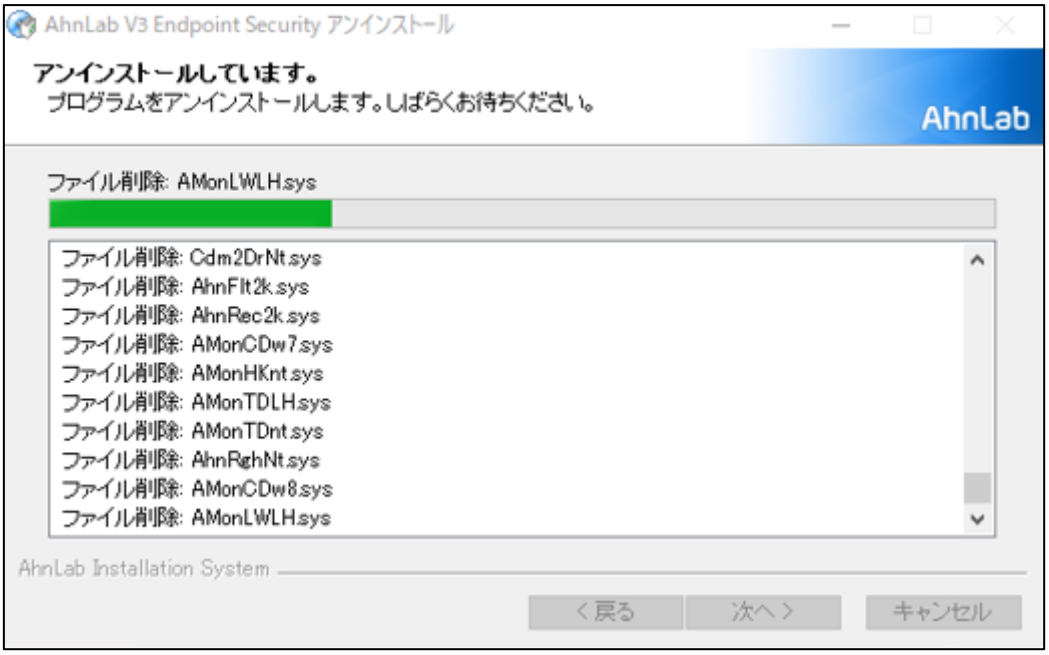
Windows PC製品のアンインストールプロセスの流れは以下の通りです。(ここでは Windows 10を基準に説明します。)

① デスクトップ画面から検索 > コントロールパネル > プログラムのアンインストールまたは変更 > AhnLab V3 Endpoint Security > アンインストールを選択します。



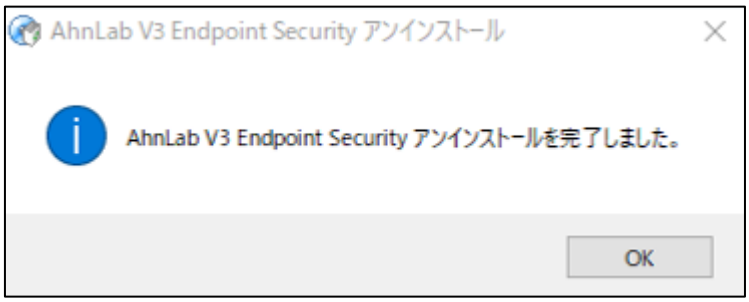
<製品のアンインストール進行画面>

② アンインストールプロセスを進行します。



<アンインストール進行画面>

③ アンインストール完了のメッセージが表示されます。



<アンインストール完了画面>

4-2) V3 Endpoint Security (for Mac) クライアントのアンインストール

Mac PC製品のアンインストールプロセスの流れは以下の通りです。

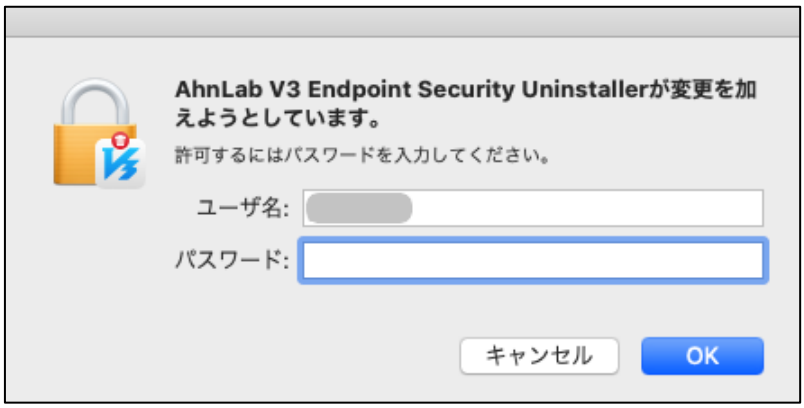
① AhnLab V3 Endpoint Security Uninstaller ファイルを実行します。

<製品のアンインストーラーファイル>

② システムの警告メッセージが表示されたら「開く」ボタンをクリックします。

<システムメッセージ画面>

③ 続行するにはシステムパスワードを入力します。



<システムパスワード入力画面>

④ アンインストール進行状況が表示された後、完了画面が表示されます。

<アンインストール完了画面>

4-3) V3 Endpoint Security (for Android) クライアントのアンインストール

Android 製品のアンインストールプロセスの流れは以下の通りです。

① Security Centerからデバイス登録を解除すると、製品を使用できなくなります。

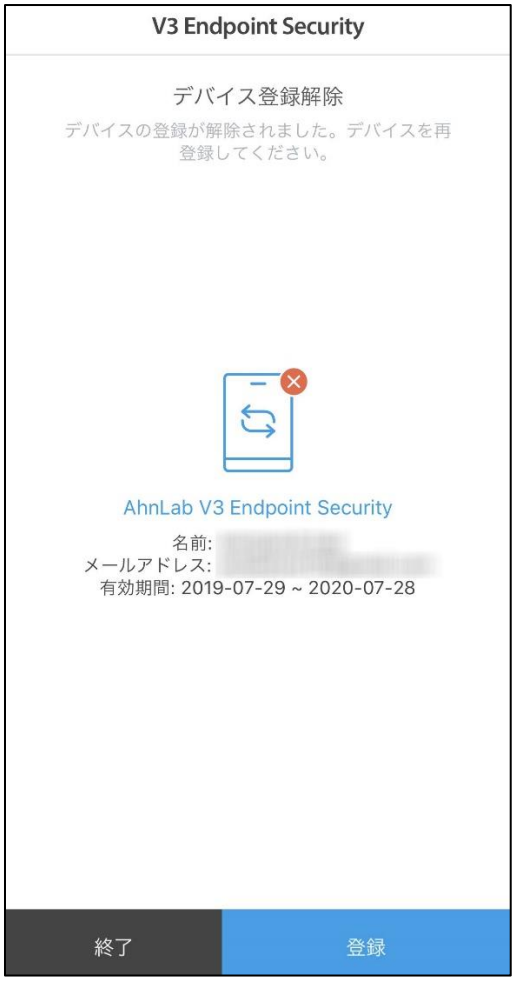
<デバイス登録解除のお知らせ画面>

② デバイスのシステム設定からアプリをアンインストールするか、アクティベーションコードを登録します。

4-4) V3 Endpoint Security (for iOS) クライアントのアンインストール

iOS 製品のアンインストールプロセスの流れは以下の通りです。

① Security Centerからデバイス登録を解除すると、製品を使用できなくなります。



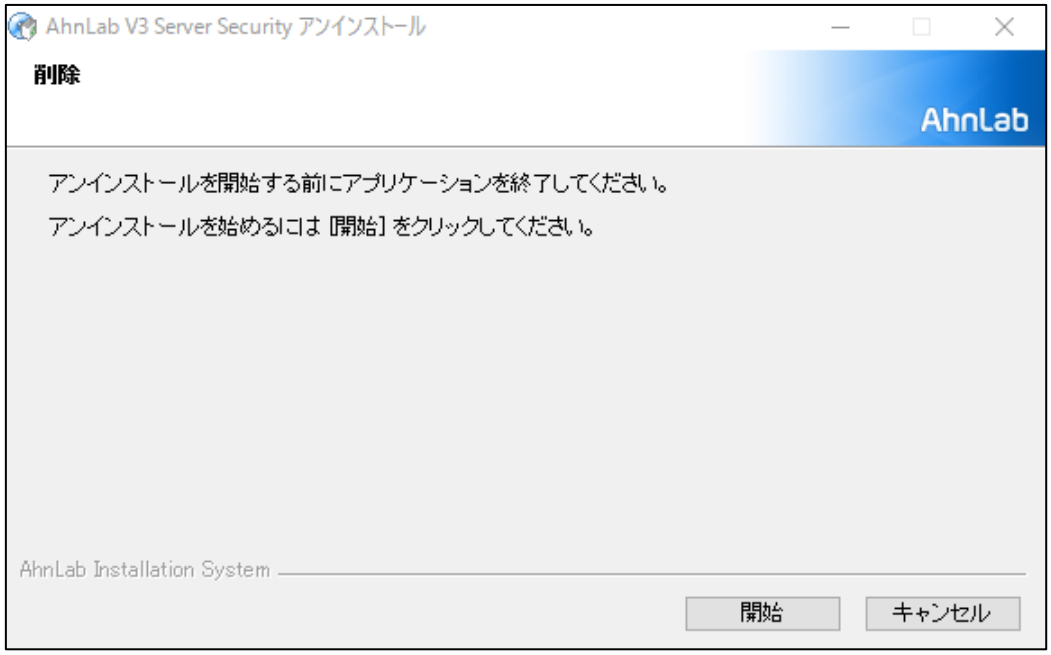
<デバイス登録解除のお知らせ画面>

② デバイスからアプリを削除するか、アクティベーションコードを登録します。

4-5) V3 Server Security(Windows) クライアントのアンインストール

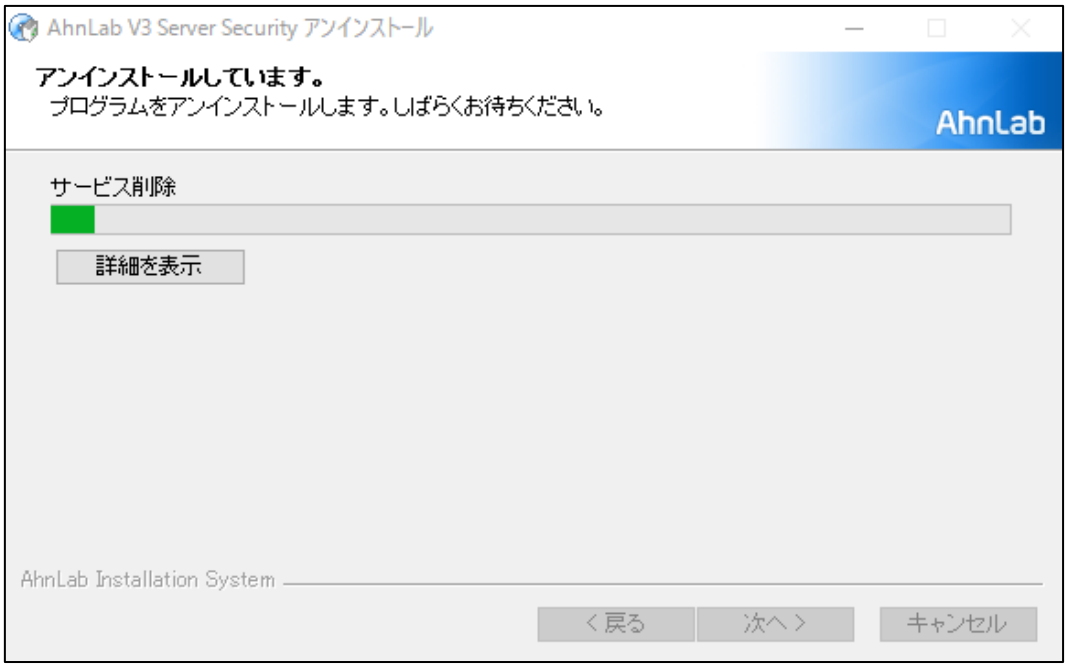
Windows Server製品のアンインストールプロセスの流れは以下の通りです。(ここでは Windows 10を基準に説明します。)

① デスクトップ画面から検索 > コントロールパネル > プログラムのアンインストールまたは変更 > AhnLab V3 Server Security > アンインストールを選択します。



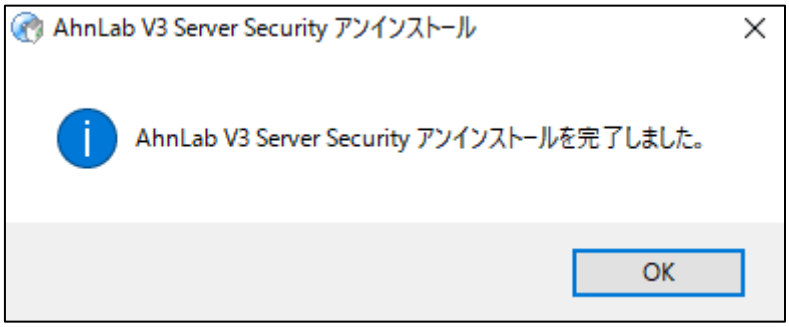
<製品のアンインストール進行画面>

② 「開始」ボタンをクリックして、アンインストールプロセスを進行します。



<アンインストール進行画面>

③ アンインストール完了のメッセージが表示されます。



<アンインストール完了画面>

4-6) V3 Server Security (Linux) クライアントのアンインストール

Linux Server製品のアンインストールプロセスの流れは以下の通りです。

① 製品インストールディレクトリの uninstall.sh を実行します。

```
[root@Server: /tmp ]# /opt/AhnLab/v3serversecurity/uninstall.sh
```

② アンインストールを確認するメッセージが表示されます。

同意「y」を入力して、Enter キーを押します。

```
Do you want to delete V3 Server Security for Linux (X.X.X.X (Build XXX))? (y/n):
```

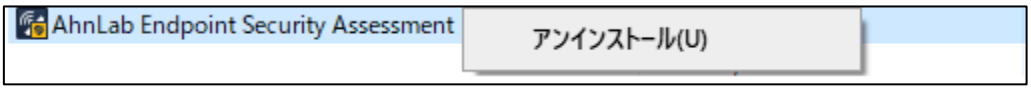
③ アンインストールが完了すると、次のメッセージが表示されます。

```
Uninstallation completed.
```


4-7) AhnLab Endpoint Security Assessment (Windows) クライアントのアンインストール

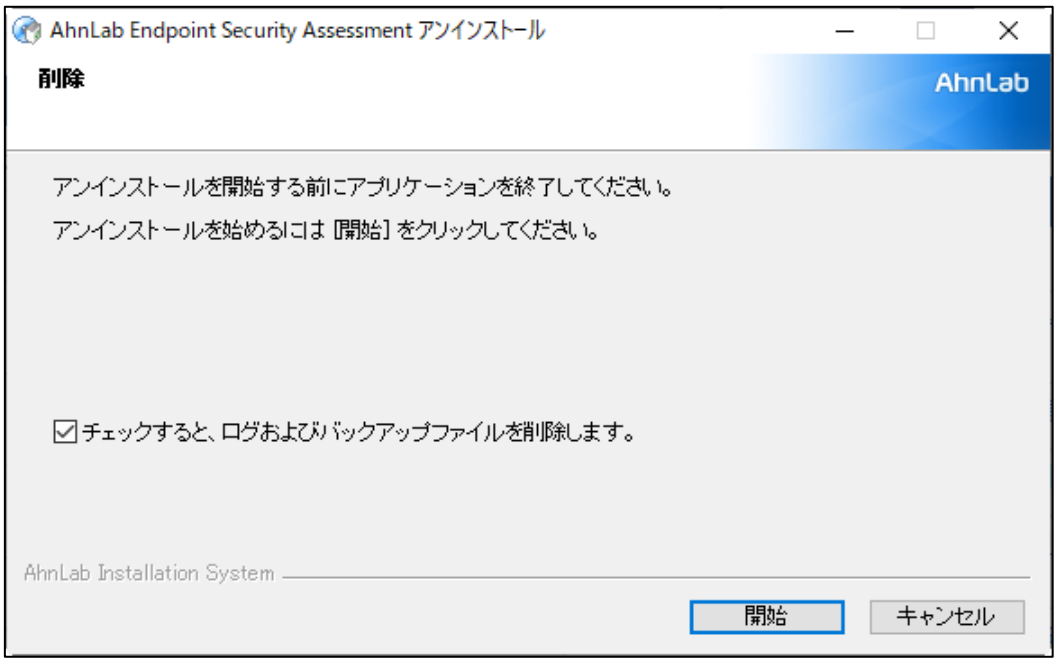
AhnLab Endpoint Security Assessment 製品のアンインストールプロセスの流れは以下の通りです。

① デスクトップ画面から検索 > コントロールパネル > プログラムのアンインストールまたは変更 > AhnLab Endpoint Security Assessment > アンインストールを選択します。



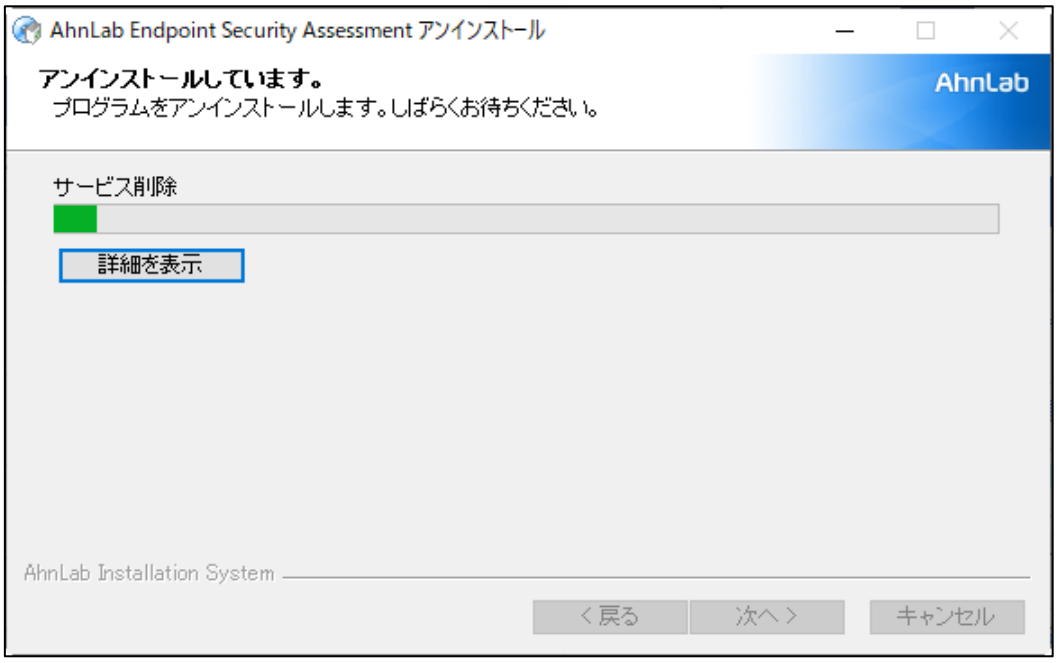
<製品のアンインストール画面>

② 「開始」ボタンをクリックして、アンインストールを開始します。



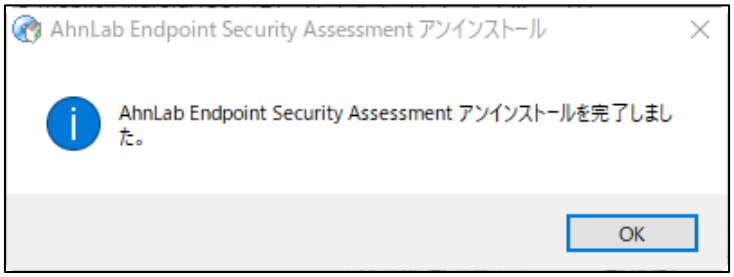
<製品のアンインストール開始画面>

③ アンインストールプロセスを進行します。



<アンインストール進行画面>

④ アンインストール完了のメッセージが表示されます。



<アンインストール完了画面>

4-8) Endpoint Security Assessment (For Android) クライアントのアンインストール

Android 製品のアンインストールプロセスの流れは以下の通りです。

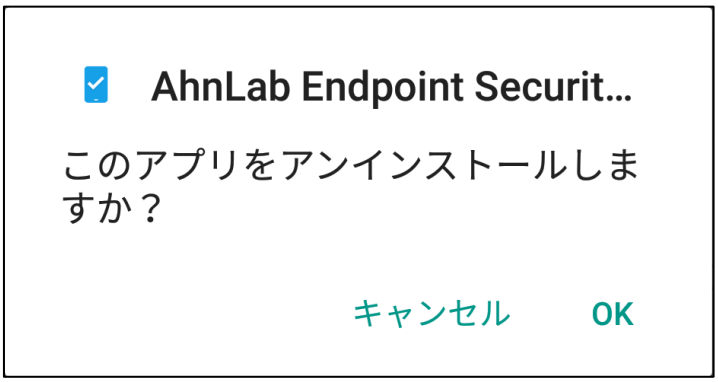
① Endpoint Security Assessmentアプリを長押しするとアプリ情報が表示されます。

<製品のプリ情報画面>

② アプリ情報からアンインストールを選択します。

<アプリ情報のアンインストール画面>

③ Endpoint Security Assessmentアプリがアンインストールされます。

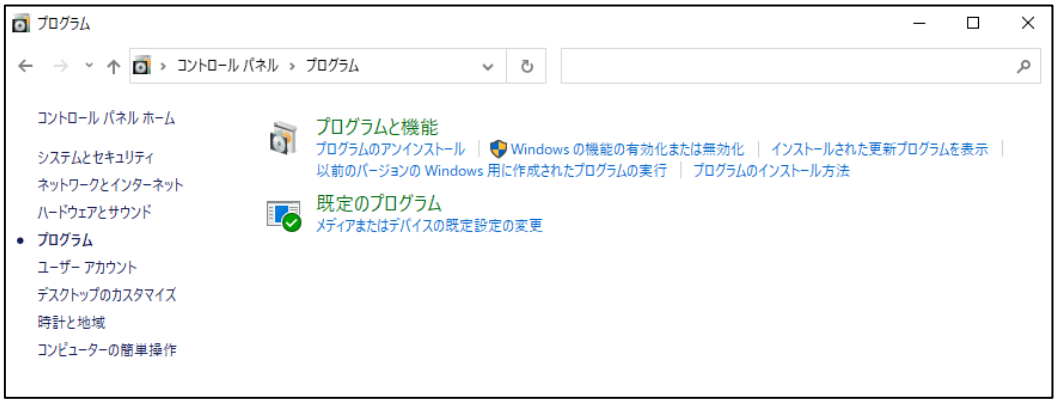


<アンインストールのお知らせ画面>

4-9) AhnLab V3 Security Agent (for Windows/Server) クライアントのインストール

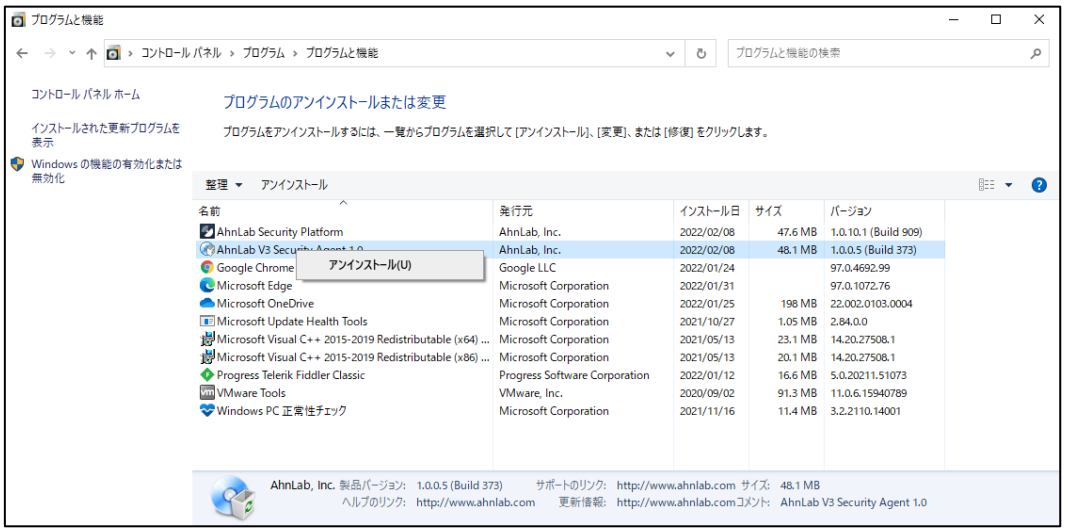
AhnLab V3 Security Agent 製品のアンインストールプロセスの流れは以下の通りです。

① デスクトップ画面から検索 > コントロールパネル > プログラム > プログラムと機能を選択します。



<コントロールパネルの画面>

② <プログラムのアンインストールまたは変更>が表示されます。AhnLab V3 Security Agent をマウス右クリックして、[アンインストール]をクリックします。



<プログラムのアンインストールまたは変更の画面>

③ <AhnLab V3 Security Agent アンインストール>ウィンドウが表示されます。アンインストールを開始するには、[アンインストール] をクリックします。

④ アンインストールが開始されます。 製品のアンインストールの完了メッセージが表示されたら [終了] をクリックします。

5. AhnLab Security Center での V3 Security Agent インストール

V3 Security Agent とは

デバイスにダウンロードすることで、Security Center から送られるインストールファイルの配布メール、またはインストール/アンインストールコマンドを V3 Security Agent が受信し、ユーザーの操作なしでデバイス上に任意のセキュリティ製品をインストール/アンインストールさせることができます。

Security Center で V3 Security Agent をインストールする方法は以下の通りです。

5-1) 配布メールの送信機能を通して V3 Security Agent インストール

① Security Center に接続し、ID とパスワードを入力して [ログイン] をクリックします。

<AhnLab Security Center ログイン画面>

② Security Center 画面上部のメインメニューからファイル > ファイルの配布をクリックします。

<AhnLab Security Center メインメニュー>

③ ユーザーリストから配布メールを送信するユーザーを選択します。(複数選択可能)

<メール送信ユーザー選択画面>

④ リストの上にある [配布メールの送信] をクリックします。

<配布メールの送信ボタン>

⑤ <配布メールの送信>画面から、宛先、件名、内容を入力した後、[送信] をクリックします。

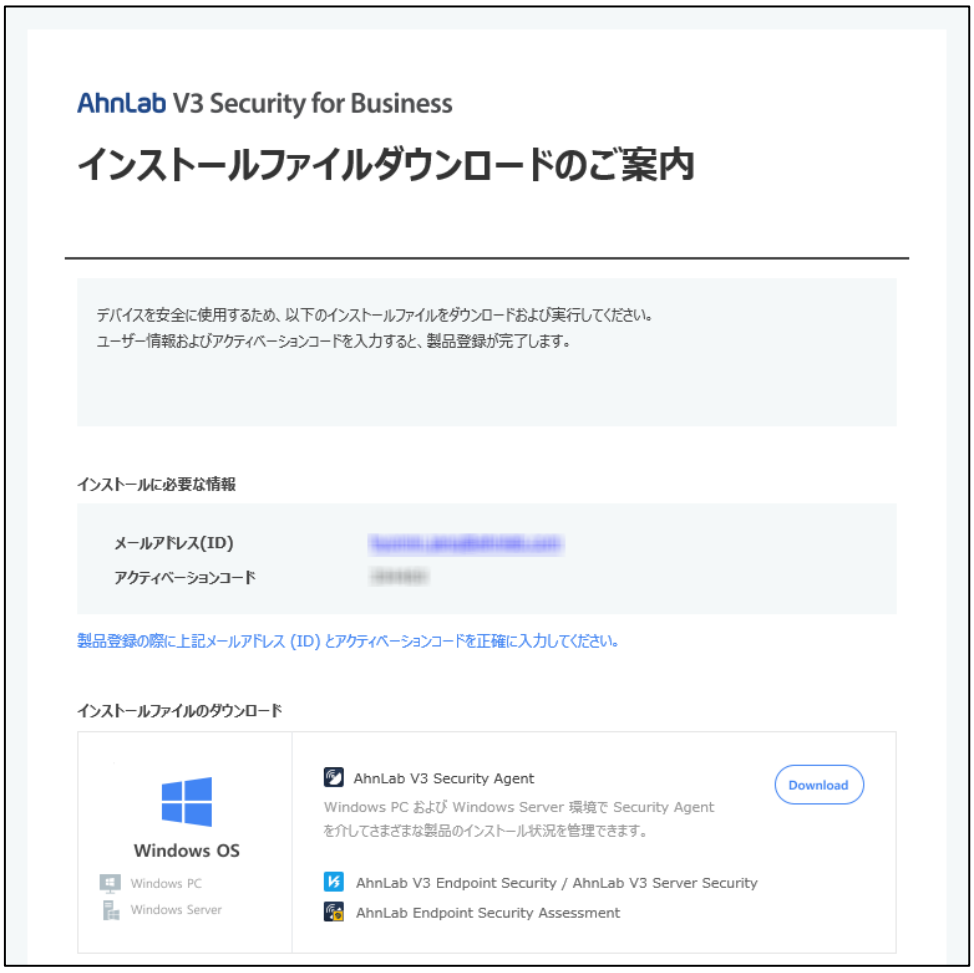
<配布メールの送信画面>

⑥ 選択したユーザーに［インストールファイルダウンロードのご案内］件名のメールが送信されます。

＊ 製品のダウンロードリンクおよびメールアドレス（ID）、アクティベーションコードを提供する以下のメールが送信されます。

<受信メールの画面>

⑦ 受信したメールから V3 Security Agent インストールファイルをダウンロードします。



<V3 Security Agent ダウンロードファイル>

⑧ V3 Security Agent 製品のインストールを行います。

5-2) インストールコマンドの送信機能を通して V3 Security Agent インストール

以下のインストール方法は、既に V3 Endpoint Security および AhnLab Endpoint Security Assessment がインストールされている状況、または過去にインストールした履歴がある場合のみ実行できます。

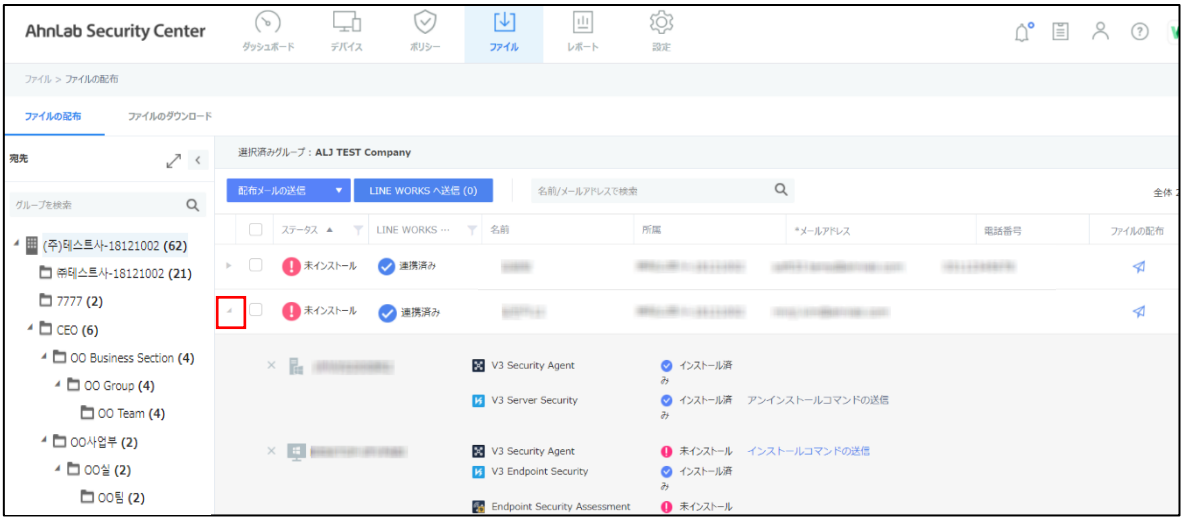
① Security Center に接続し、ID とパスワードを入力して [ログイン] をクリックします。

<AhnLab Security Center ログイン画面>

② Security Center 画面上部のメインメニューからファイル > ファイルの配布をクリックします。

<AhnLab Security Center メインメニュー>

③ ユーザーリストからインストールコマンドを送信するユーザーを選択し、左側の アイコンをクリックします。V3 Security Agent およびセキュリティ製品のインストール状況を確認できます。

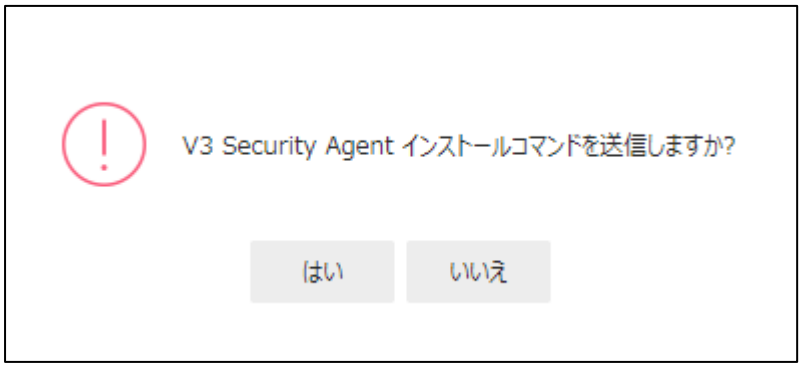


<メール送信ユーザー選択画面>

④ 製品のインストール状況が未インストールの場合、[インストールコマンドの送信] をクリックして、Security Agent をインストールします。

<インストールコマンドの送信画面>

⑤ インストールコマンドの送信を確認するメッセージが表示されます。[はい] をクリックします。



<インストールコマンドの送信メッセージ>

⑥ バックグラウンドで V3 Security Agent 製品のインストールが行われます。

More security,
More freedom

アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。

1995 年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できる IT 環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。

アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

〒108-0014 東京都港区芝4丁目13- 2 田町フロントビル3階 | TEL: 03-6453-8315 (代)

AhnLab