WithSecure™ Atlant 製品紹介資料

2023年4月

ウィズセキュア株式会社

はじめに

本資料は「WithSecure™ Atlant」の紹介資料となります。
AtlantはICAPや他のAPI等で他製品と連携し、連携先へマルウェアスキャン機能を提供するセキュリティソフトウェア製品となります。

例として、Atlantをi-FILTERやSquid等、ICAPクライアント機能を持つHTTPプロキシ製品と連携させることで、HTTP通信のネットワークスキャンを行うことが可能です。

これまで弊社ではネットワークスキャン製品としてLinuxゲートウェイ（別称：IGK、Internet Gatekeeperなど）という製品を販売しておりましたが、当該製品は2024年12月末をもって製品サポート終了を予定しているため、今後ネットワークスキャンをご検討のお客様への候補として「WithSecure™ Atlant」をご紹介いたします。

WithSecure™ Atlant 機能紹介

Atlant 動作環境

◆サポートOS

- Alma Linux8,9
- Rocky Linux 8/9(2023年5月から対応予定)
- Amazon Linux2
- CentOS7, 8
- CentOS Stream8
- RHEL7, 8, 9
- Oracle Linux7, 8
- Debian10, 11
- Ubuntu16.04, 18.04, 20.04, 22.04
- SUSE Linux Enterprise Server12(Service Pack1以降)
- SUSE Linux Enterprise Server15(Service Pack1以降)

◆ハードウェアリソース(最小要件)

- Processor: X86-64 互換 CPU
- Memory: 2GB RAM以上
- Disk space: 少なくとも 3 GB 以上を推奨

✓ 十分なスワップメモリ領域をご用意いただくことを強くお勧め致します。

✓ マルウェア解析で一時的に保存されるコンテンツのために十分な空きディスク容量が必要となります。

✓ Atlantのハードウェア要件はユースケースによって異なります。上記はAtlantをインストールする上での必要最低限のハードウェアリソースとなります。

※インストールに必要なパッケージ等の詳細については下記URLをご参照ください。
https://help.f-secure.com/product.html#business/atlant/latest/en/concept_FE8EDD82C8954CD2AF8A0546131B6E86-latest-en

WITH secure

Atlantの主な機能

- ファイル検査
  ウィズセキュアのオンラインファイルレピュテーションサーバによる評価や、パターンファイルによる検査を行い、マルウェアかどうかの判定を行います。
- URL検査
  ウィズセキュアのオンラインURLレピュテーションサーバへの問い合わせを行い、危険なサイトかどうかの判定を行います。
- セキュリティクラウド
  未知のファイルに対する評価を、オンラインファイルレピュテーションサーバのデータベースを利用して行う機能（ORSP）
- 自動更新
  ウイルス定義ファイルやマスターエージェントも自動で最新のものに更新
- ICAPプロトコルをサポート。（ICAPサーバーとして動作）
- ファイルスキャン及び製品設定を管理するためのREST APIを提供。

※ICAPはInternet Content Adaptation Protocolの略で、RFC3507で標準化されているプロトコルです。その名前の通り、インターネットのコンテンツを変更して適切な内容に変えることを目的としたプロトコルです。主にコンテンツ（ダウンロードファイル）の検査、URLフィルタリングの用途として広く使われています。

スキャンに関する仕様及び制限事項

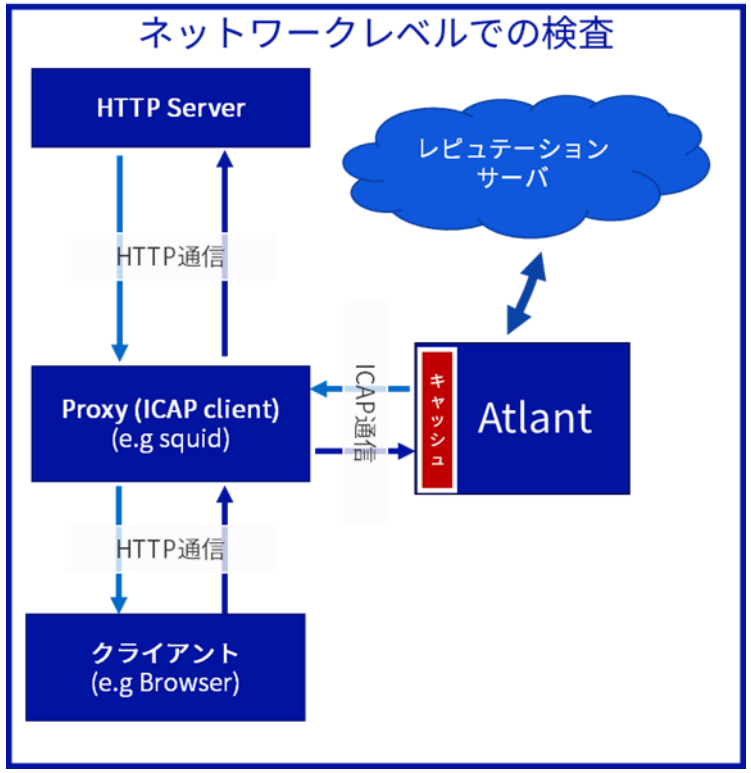
- スキャンできるファイルタイプ（拡張子等）に制限はありません。
- スキャンできるファイルサイズに制限はありません。
- パスワード付きファイル（圧縮ファイル含む）についてはスキャンが行えません。
- スキャン除外機能についてはございません。※1
- マルウェアの隔離機能についてはございません。※1
- マルウェアを検知したファイルの制御を行うことはできません。（削除やリネーム等）※1
- 最大で500のスキャン要求を処理できます。※2
- 最大同時スキャン数はCPUコア数に依存します。

※1：お客様側アプリケーションにて制御いただく必要がございます。

※2：500以上のスキャン要求を同時に受け付けた場合Linuxカーネルが接続をバッファします。弊社開発部でのテストでは、4,000程度の同時接続スキャンにて問題ないことを確認していますがスキャンコンテンツや環境設定によっては結果が異なる場合がございます。

HTTP/HTTPS通信の検査

- Atlantを既存のHTTPプロキシ製品（Squid等）に統合することで、既存のネットワークを大幅に変更することなくウィルス検査とコンテンツレピュテーションを提供することが可能です。



構成メリット
ゲートウェイ製品を多段接続した場合に比べ、ネットワークの信頼性を確保できます。
（外部の製品がダウンしても最低限の通信を確保できます。）

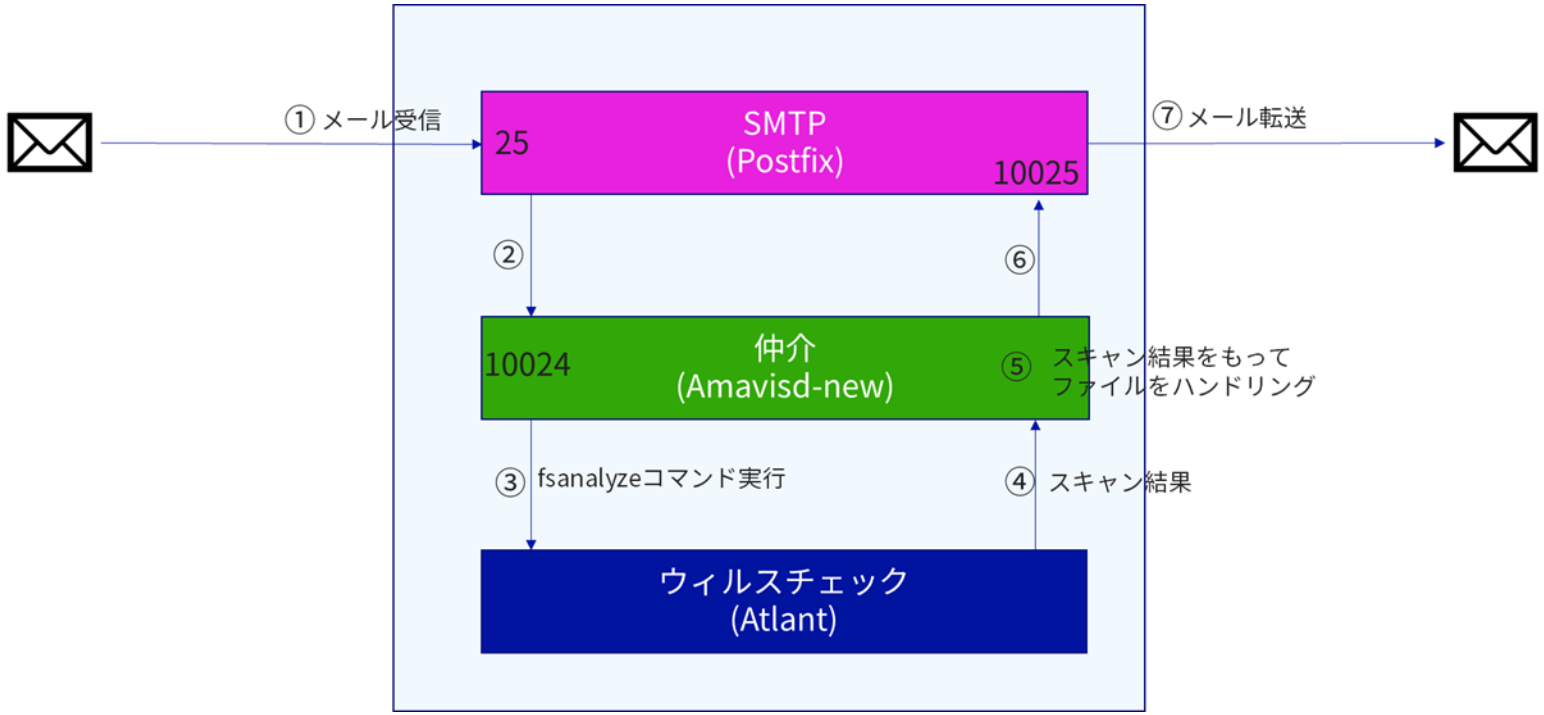
- ICAPクライアントはネットワーク経由でソケットを介してスキャンサービス（Atlant）にファイルを渡します。クライアントアプリケーションがスキャンサービスと通信し、スキャンするファイルを渡し、スキャンサービスがクライアントにスキャン結果を返します。
- HTTP Proxy（Squid側）でSSLをデクリプションして処理をAtlantに渡すことでHTTPSサイトについてもスキャンが可能になります。（SSL Bump設定）

※Atantはファイルのマルウェア検査のみで検知時の当該ファイルの隔離保存や通知アクションは行いません。
※弊社のサポート範囲はAtlantのみで、squidの設定・運用は範囲外となります。

W / T H
secure

メールの検査

- オープンソースのAmavisd-new・Postfixを利用することで、MTAで受信したメールをAtlantでスキャンすることが可能です。
- 本構成ではAtlantのマニュアルスキャン機能（fsanalyzeコマンド）を使ってメールのスキャンを行います。



※Amavisd-newとAtalantは同一サーバ上である必要があります。
※Atantはファイルのマルウェア検査のみで検知時の当該ファイルの隔離保存や通知アクションは行いません。
※Atalantはメールアイテムのファイルのマルウェア検知のみで、検知後のアクションはAmavid-new側の設定が必要となります。
※弊社のサポート範囲はAtlantのみで、Postfix/Amavisd-newの設定・運用は範囲外です

W / T H
secure

関連資料・各種お問い合わせ先

- Atlant オンラインマニュアル
  https://help.f-secure.com/product.html#business/atlant/latest/ja

- 営業窓口（価格・見積等もこちらへお申し付け下さい）
  japan@WithSecure™.com

LinuxゲートウェイからAtlantへの移行について

WITH secure

LinuxゲートウェイからAtlantへの移行について

LinuxゲートウェイからAtlantへの移行にあたっては、製品のアンインストール/インストールにて入れ替えを行ってください。
（移行ツールのようなものはございません。製品のアンインストール/インストール手順については、下記URLをご参照下さい）

- Linuxゲートウェイのアンインストール
  https://help.f-secure.com/product.html#business/igk/5.50/ja/concept_ED2013B642DE49FF812D417C4E72351E-5.50-ja

- Atlantのインストール
  https://help.f-secure.com/product.html#business/atlant/latest/ja/concept_94067ECBA705473F9BC72F4282C2338D-latest-ja

WITH secure

ATLANTとLINUXゲートウェイとの比較

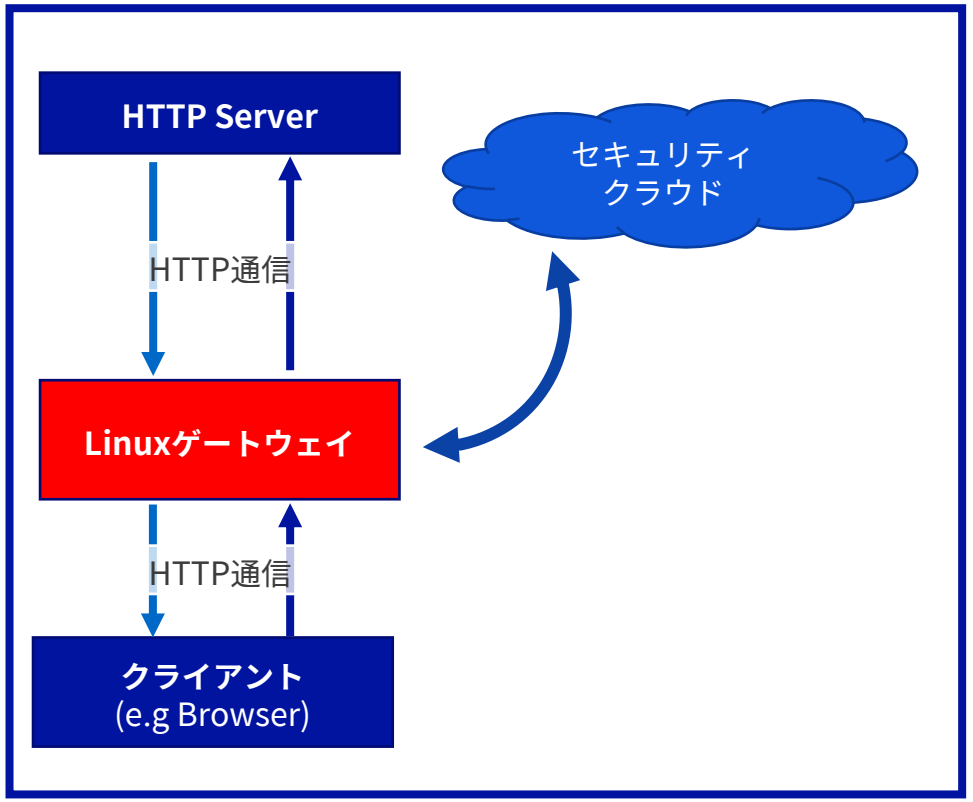
	Atlant	Linuxゲートウェイ
製品コンセプト	ICAP、REST APIで他製品と連携し、 連携先へマルウェアスキャン機能を提供する	プロキシ機能を持ち、 ネットワーク上のマルウェアスキャンが可能
プロキシ機能	なし	HTTP,SMTP,POP,FTP対応
ICAP連携（ICAPサーバー）	○	○
クラウドベーススキャン（ORSP）	○	○
Webコンテンツ制御機能	○（信頼済みサイト」「拒否したサイト」の設定はありません。）	○
管理UI	コマンドライン	GUI
マルウェア検知時の管理者通知	×（連携先の製品にて設定が必要）	○
マルウェア隔離	×（連携先の製品にて設定が必要）	○
スキャン除外機能	×（連携先の製品にて設定が必要）	○
スキャンできるファイルサイズの上限	なし	あり(上限は2GB)
パターンファイル自動更新	○	○
製品自体の自動アップデート	○	×
SPAMメール対策	△（不可能ではないが非常に困難）	○

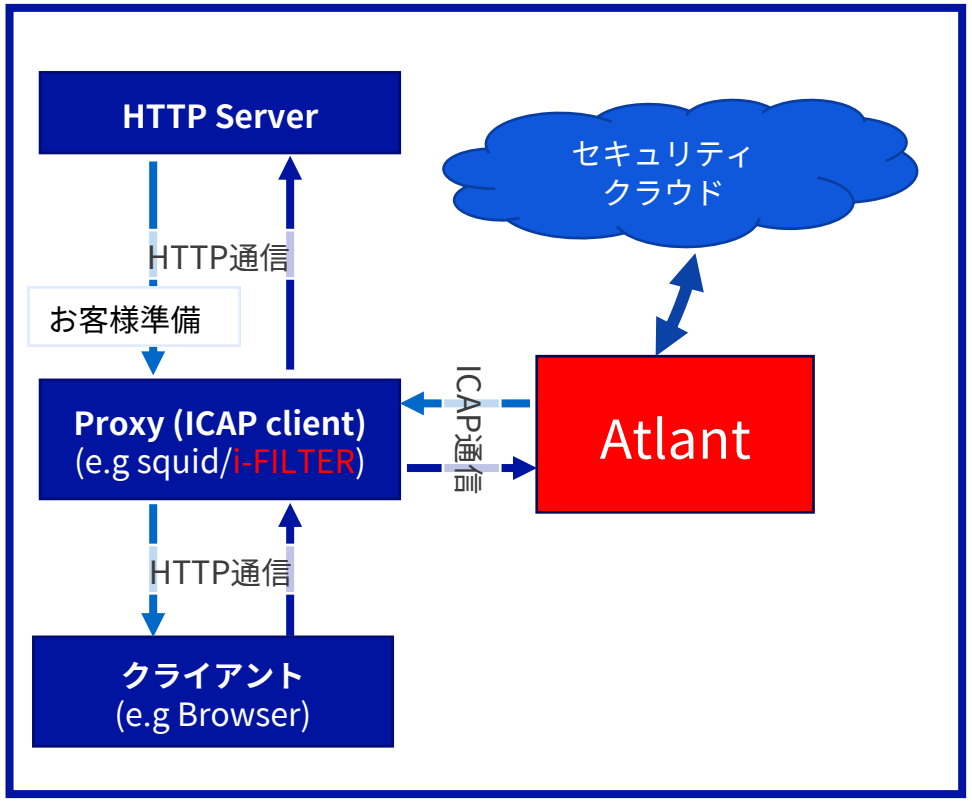
LINUXゲートウェイとの違い: HTTPスキャンの例

■Linuxゲートウェイ
・Linuxゲートウェイ自体がプロキシとして機能します。

■Atlant
・SquidなどICAPクライアント機能をもつHTTPプロキシ製品との連携が必要

※弊社が動作保証するのは弊社製品のAtlantの動作部分（ウイルスチェック部分）のみです。
システム全体の動作やICAP ClientやAmavisd-newなどの弊社製品ではない部分については
保証できかねます。事前に十分な動作検証を実施のうえ運用いただくことを推奨いたします。



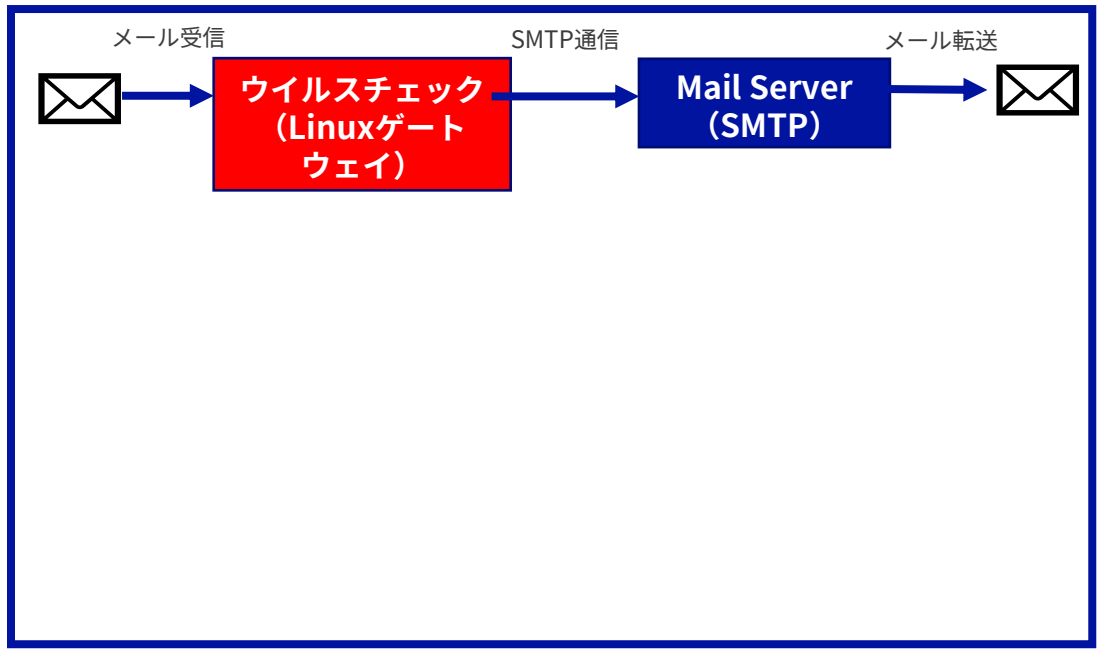


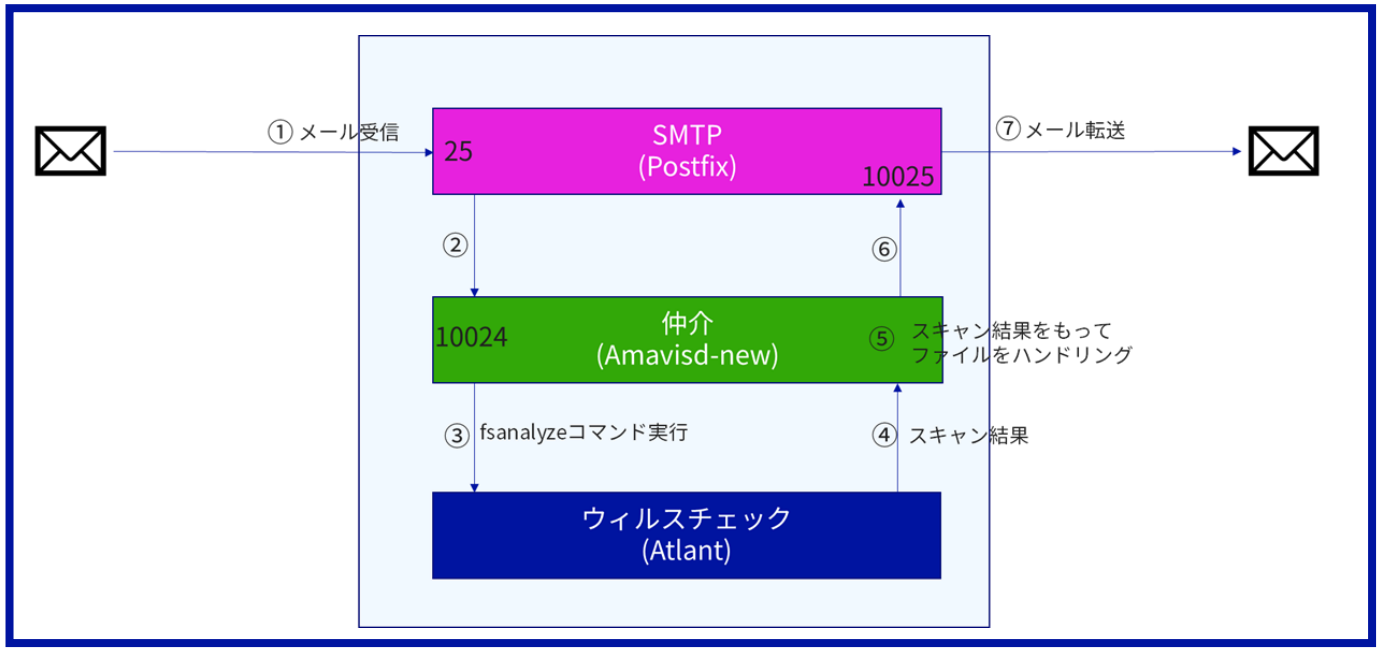
LINUXゲートウェイとの違い：メールスキャン

■Linuxゲートウェイ
・Linuxゲートウェイ自体がプロキシとして機能します。

■Atlant
・SquidなどICAPクライアント機能をもつHTTPプロキシ製品との連携が必要

※弊社が動作保証するのは弊社製品のAtlantの動作部分（ウイルスチェック部分）のみです。
システム全体の動作やICAP ClientやAmavisd-newなどの弊社製品ではない部分については
保証できかねます。事前に十分な動作検証を実施のうえ運用いただくことを推奨いたします。





LINUXゲートウェイのサポート終了

- サポート期限は2024年12月31日でサポート終了の影響は以下となります。
  - ✓ パターンファイルの提供保証が無くなり、予告なく提供を停止する可能性があります。
  - ✓ 不具合や動作等の相談についてサポートセンターにてのリクエスト受付を終了します。
  - ✓ サポート期限終了後直ちに製品の動作が止まる訳ではありませんが、お早目にAtlantへの製品変更をご検討下さい。
- ライセンス
  - ✓ LinuxゲートウェイとAtlantのライセンスは違うものになりますので、Linuxゲートウェイのライセンスをそのまま使うことはできません。
  - ✓ Atlantへ製品変更される場合には別途Atlantのライセンスの購入が必要となり、価格体系も変更となります。
- 連絡先
  - ✓ Atlantへ製品変更にあたり、詳細技術資料の提供・説明会の実施・費用見積等をいたしますので、弊社営業担当者または以下の弊社営業窓口までお気軽にご連絡下さい。

japan@withsecure.com

WITH secure


WITH
secure