AlaxalA

The Guaranteed Network
いちばん近くで、もっと先へ。

AX シリーズ

ホワイトリスト機能 活用ガイド
《導入編》

第 2 版

資料 No. NTS-16-R-001

アラクサラネットワークス株式会社

はじめに

本資料は、アラクサラのホワイトリスト機能のシステム導入に役立てるものとして 概要、システム構築例など 導入する際に考慮すべき内容について記載しています。

関連資料

- AX シリーズ製品マニュアル
  （http://www.alaxala.com/jp/techinfo/manual/index.html）
  AX2500S シリーズ
  《ソフトウェアマニュアル》
  ・コンフィグレーションガイド Vol.2
  ・コンフィグレーションコマンドレファレンス
  ・運用コマンドレファレンス
  《ライセンス設定ガイド》
  AX260A シリーズ
  《ソフトウェアマニュアル》
  ・コンフィグレーションガイド Vol.2
  ・コンフィグレーションコマンドレファレンス
  ・運用コマンドレファレンス
  《ライセンス設定ガイド》

本資料使用上の注意事項

本資料に記載の内容は、弊社が特定の環境において基本動作を確認したものであり、機能・性能・信頼性についてあらゆる環境条件すべてにおいて保証するものではありません。また製品マニュアルの補助資料としてご利用いただけますようお願いいたします。

なお本資料作成時の OS ソフトウェアバージョンは特記の無い限り以下となっております。

AX2500S	Ver. 4.4
AX260A	Ver. 4.4

本資料の内容は、改良のため予告なく変更する場合があります。

輸出時の注意

本製品を輸出される場合には、外国為替及び外国貿易法の規制並びに米国輸出管理規制など外国の輸出関連法規をご確認の上、必要な手続きをおとりください。

なお、不明な場合は、弊社担当営業にお問い合わせ下さい。

商標一覧

- アラクサラの名称およびロゴマークは、アラクサラネットワークス株式会社の商標および登録商標です。
- Ethernet は、富士ゼロックス株式会社の登録商標です。
- イーサネットは、富士ゼロックス株式会社の登録商標です。
- そのほかの記載の会社名、製品名は、それぞれの会社の商標もしくは登録商標です。

改訂履歴

版数	Rev.	日付	変更内容	変更箇所
初版	-	2016.07.01	初版発行	-
第 2 版	-	2016.07.29	･第 2 版作成時の OS ソフトウェアバージョンを Ver.4.4 に変更 ･AX260A シリーズを追加	はじめに
			･製品ラインアップに AX260A シリーズを追加	2.3
			･Ver.4.4 の追加機能を追加	3.1
			･trust モード 4 を追加	3.1.2
			･エントリ数に AX260A シリーズを追加	3.3
			･パケットリストで運用する機能の説明を追加	4

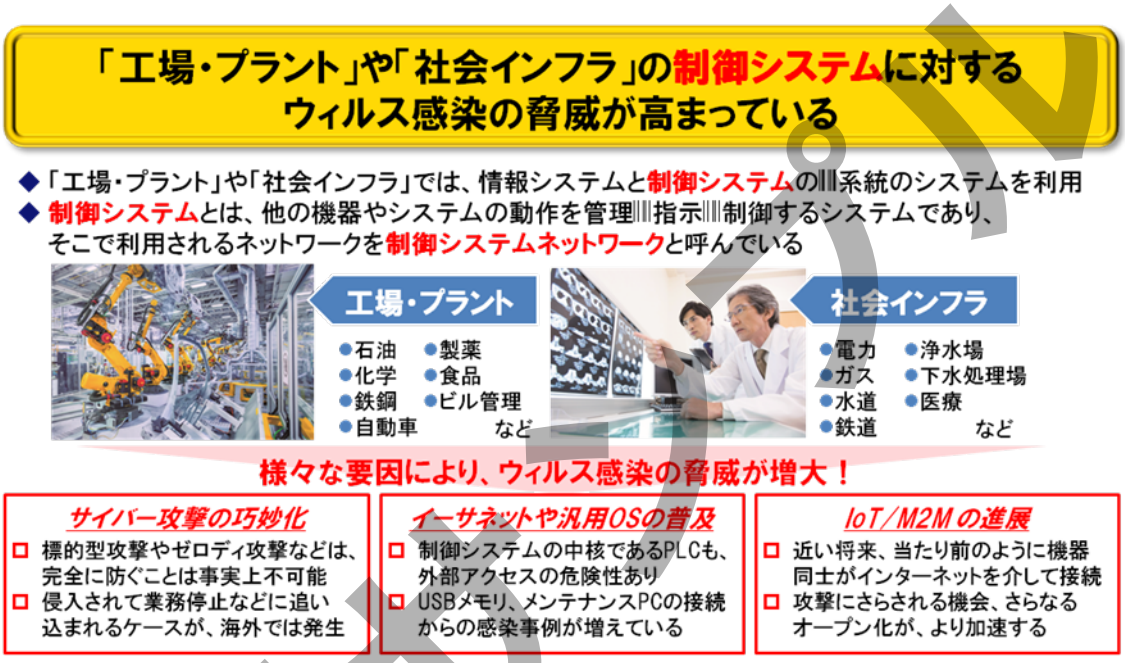
目次

1. ホワイトリストとは

1.1 制御システムの抱える課題

昨今、情報システムだけでなく、制御システムなど、さまざまなネットワークがインターネットなどの外部ネットワークとつながるようになりつつあります。また、モノのインターネットと言われる IoT（Internet of Things）や、機器同士が通信する M2M（Machine to Machine）など新技術が登場し、こうした動きはますます加速しています。

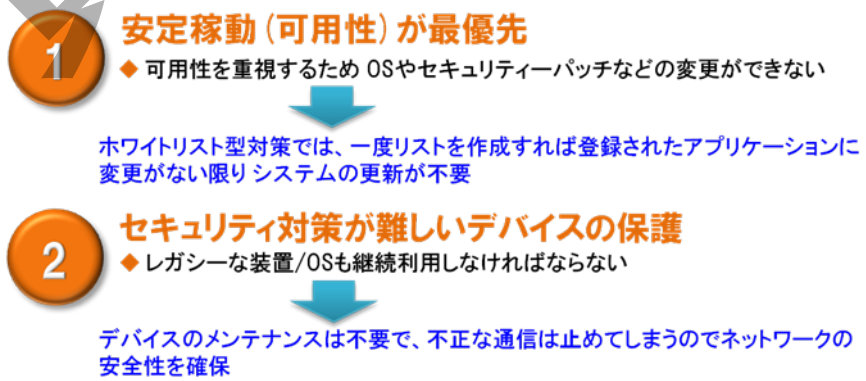
制御システム内などには、一般的なパーソナルコンピュータとは異なり、セキュリティ対策が十分にできないデバイスが存在します。セキュリティ対策が不十分なデバイスが外部ネットワークと接続することで、サイバー攻撃の脅威に晒されています。



1.2 ホワイトリスト型のセキュリティー対策

オフィスや家庭でも使用されている通常のウイルス対策ソフトとして知られるアンチウイルスソフトは、ブラックリスト型と呼ばれる方法をベースとしています。ブラックリスト型の対策は、日々世の中で発生するマルウェア情報を集めた「**悪いもの（ブラック）リスト**」（定義ファイル）を用いて、マルウェアを検知する方法です。これに対しホワイトリスト型の対策は、この正反対のアプローチでマルウェアを防ぎます。動作して良いと判断した「**良いもの（ホワイト）リスト**」を作り、これ以外のサービスやアプリケーションを起動しないように制限をかけるものです。

ホワイトリスト型の対策は、制御システムのセキュリティー対策の課題を解決することができることで注目されています。



2. ホワイトリスト機能の概要

2.1 ホワイトリストスイッチ

ホワイトリストスイッチは、ホワイトリストを生成しそのリストに基づいて通信をおこなう機能をもったイーサネットスイッチです。ホワイトリスト機能は、受信したフレーム，IPv4 パケット，ARP パケットをもとに許可リストを自動生成し、信頼されていない端末からのアクセスを制限する機能です。

ホワイトリスト機能を有効にした際、「学習状態」と「運用状態」の 2 つの状態を持ちます。学習状態の期間にホワイトリストスイッチで受信したすべてのパケットを 設定内容に応じた通信許可リストを自動で生成します。学習完了後に 運用状態に切り替えると 自動生成したホワイトリストに基づき、未学習パケットの廃棄やログの通知およびパケットのミラーが可能となります。

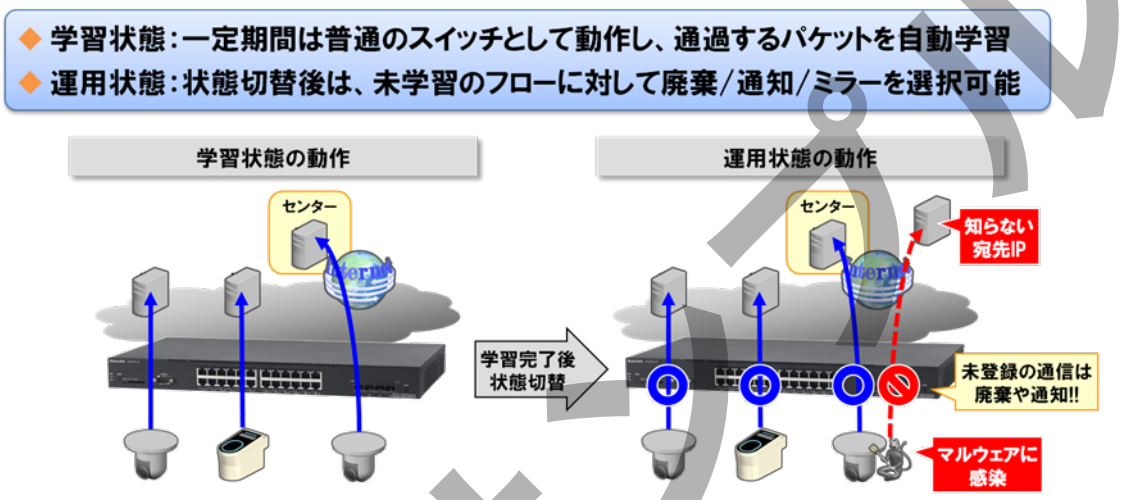


図 2-1 ホワイトリスト機能の概要

2.2 ホワイトリスト機能の特徴

アラクサラのホワイトリスト機能は、トラフィックから自動で通信許可リストを生成するアラクサラ独自の機能を実装しており、以下のような特徴があります。

【特徴 1】 ホワイトリストは自動で生成・登録

アラクサラのホワイトリスト機能は、リストを自動で生成・登録します。人手による登録作業は必要なく、サーバ、ネットワーク管理者に余計な負担をかけません。またネットワークスイッチのコンフィグ設定などの知識も不要で、担当者のスキルに依存することなく、誰でも簡単に運用することができます。

【特徴 2】 最低限のメインテナンスで OK

アラクサラのホワイトリスト機能なら、リストを一度作成してしまえば、ネットワーク構成に変更がない限り、メンテナンスをする必要がありません。

【特徴 3】 さまざまな攻撃に対応

アラクサラのホワイトリスト機能は、「MAC アドレス」「IP アドレス」「TCP/UDP ポート番号」など複数のパラメータから不正な通信フローを特定します。そのため、持ち込み PC から内部のネットワークに侵入してきたウイルスや、送信元を詐称した不正な通信など、さまざまなタイプの攻撃を防ぐことができます。

【特徴 4】 設置が簡単

既存のスイッチを、ホワイトリスト機能を搭載したスイッチに置き換えるだけで導入できるため、設置に面倒がありません。最小限のコストで ネットワーク全体のセキュリティーを高めることができます。

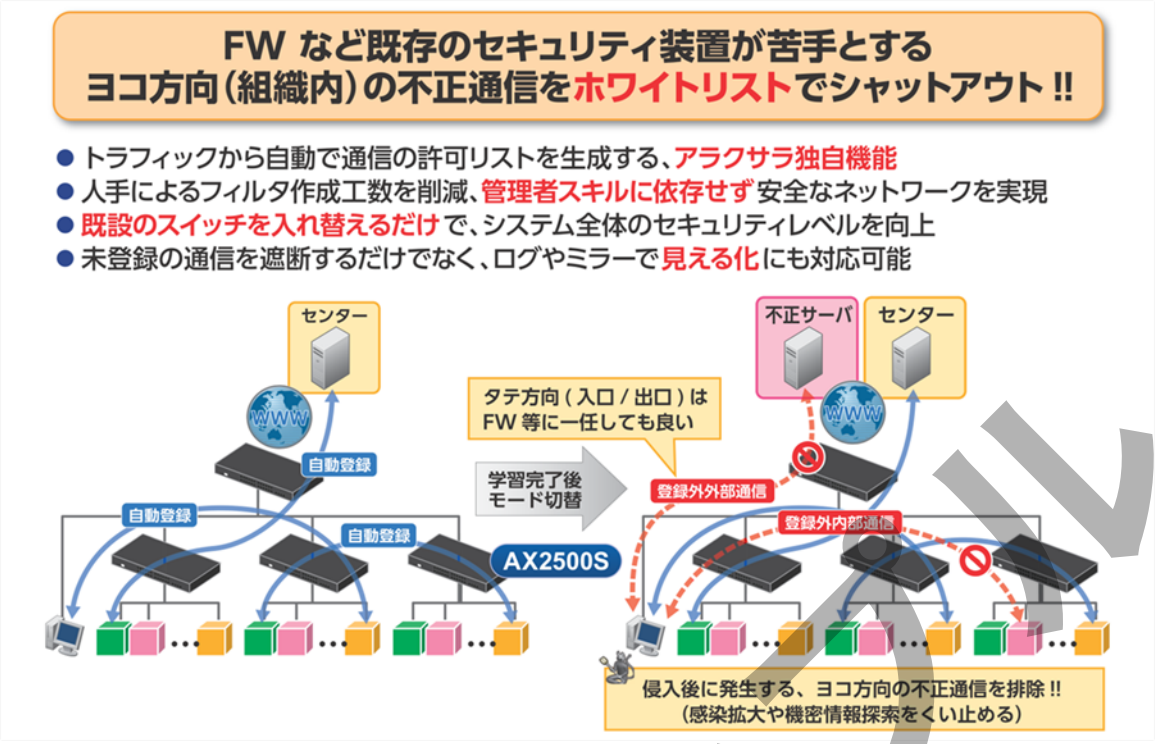


図 2-2　ホワイトリスト機能の特徴

2.3　製品ラインアップ

ホワイトリスト機能をサポートする製品ラインアップは 以下のとおりです。

(a)　AX2500S シリーズ

ホワイトリスト機能は Ver.4.2 以降でサポートしています。別途 アドバンストソフトウェアアップグレードライセンス(OS-L2A) が必要となります。

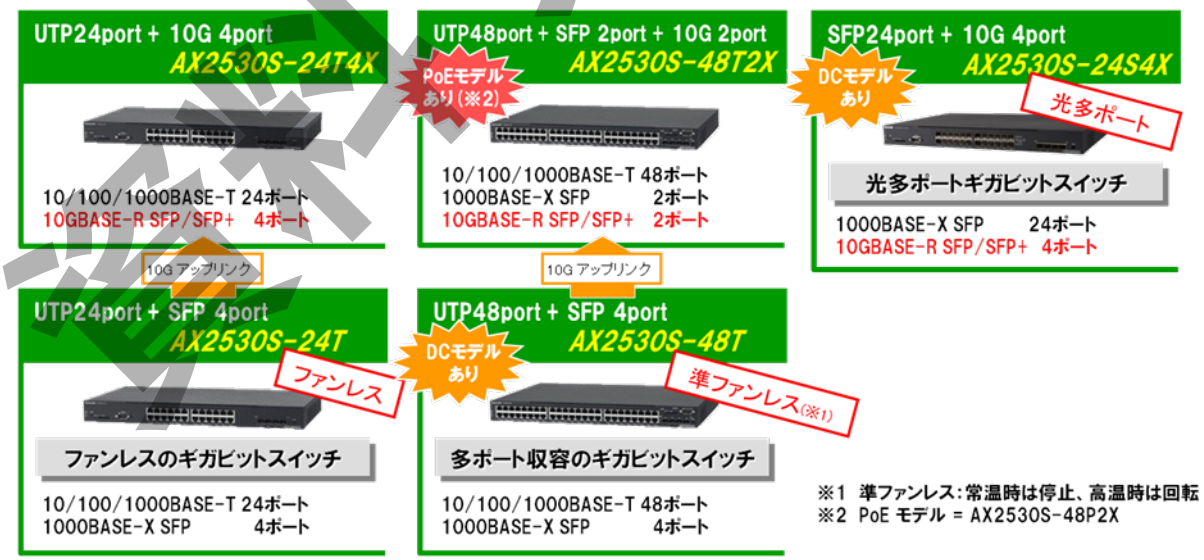


図 2-3　AX2500S シリーズ

(b) AX260A シリーズ

AX260A シリーズは Ver.4.4 以降でのサポートとなります。AX260A シリーズはエントリモデル(AX260A-08T)とハイエンドモデル(AX260A-08TF)の 2 つのモデルがあります。

エントリモデルは、オプションライセンス不要で ホワイトリスト機能を使用可能です。またエントリ数は、AX2500S と同じです。

ハイエンドモデルは、オプションライセンスのホワイトリスト基本ライセンス(OP-WL)を登録することでホワイトリスト機能を使用可能です。またホワイトリスト拡張ライセンス(OP-WLE)を追加登録することで、最大 32,000 エントリまで拡張可能です。

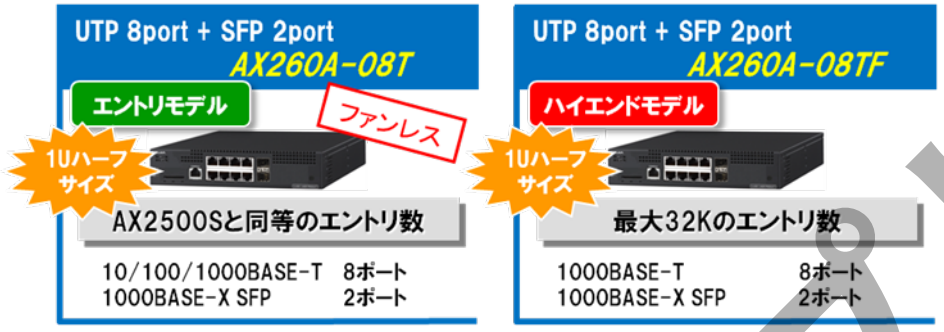
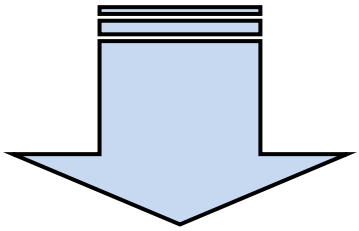


図 2-4 AX260A シリーズ

気になる続きは…



・アラクサラ　インテグレータ会員

または

・ビジネスパートナー様会員

にご登録いただければ、全てをご覧いただけます！

アラクサラ インテグレータ会員またはビジネスパートナー様会員へ登録することで、アラクサラ製品のご利用にあたり役立つ各種資料(システム構築ガイドなど)を全て閲覧することができます。ぜひこの機会にご登録下さい。

アラクサラネットワークス株式会社

〒212-0058
川崎市幸区鹿島田一丁目１番２号 新川崎三井ビル西棟
http://www.alaxala.com/