

AX シリーズ

ホワイトリスト機能 活用ガイド 《導入編》

第 3 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. 4.10
AX260A	Ver. 4.10

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	はじめに
			・AX260A シリーズを追加	
			・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
第 3 版	-	2018.05.25	・パケットリストで運用する機能の説明を追加	4
			・第 3 版作成時の OS ソフトウェアバージョンを Ver.4.10 に変更	はじめに
			・製品ラインアップの AX2500S シリーズを更新	2.3
			・ホワイトパケットリスト動作モードの追加にともない 内容を更新	3.1
			・表 3 5 他機能との併用不可機能 を更新	3.2

目次

1. ホワイトリストとは	5
1.1 制御システムの抱える課題	5
1.2 ホワイトリスト型のセキュリティー対策	5
2. ホワイトリスト機能の概要	6
2.1 ホワイトリストスイッチ	6
2.2 ホワイトリスト機能の特徴	6
2.3 製品ラインアップ	7
3. ホワイトリスト機能の仕様	9
3.1 ホワイトリスト機能	9
3.1.1 ホワイトアドレスリスト機能	10
3.1.2 ホワイトパケットリスト機能	10
3.2 他機能との併用	13
3.3 ホワイトリスト機能のエントリ数	14
4. ホワイトリスト機能の導入	15
4.1 ホワイトリスト機能の導入例	15
4.2 システム構成図	16
4.3 ホワイトリスト機能の導入手順	17
5. 留意事項	25
付録 1. コンフィグレーションファイル	26
付録 2. Windows 端末の送信パケットについて	27

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。

「工場・プラント」や「社会インフラ」の制御システムに対する ウィルス感染の脅威が高まっている

- ◆「工場・プラント」や「社会インフラ」では、情報システムと**制御システム**の両方のシステムを利用
- ◆ **制御システム**とは、他の機器やシステムの動作を管理指示制御するシステムであり、そこで利用されるネットワークを**制御システムネットワーク**と呼んでいる



工場・プラント

- 石油 ●製薬
- 化学 ●食品
- 鉄鋼 ●ビル管理
- 自動車 など



社会インフラ

- 電力 ●浄水場
- ガス ●下水処理場
- 水道 ●医療
- 鉄道 など

様々な要因により、ウィルス感染の脅威が増大！

サイバー攻撃の巧妙化

- 標的型攻撃やゼロデイ攻撃などは、完全に防ぐことは事実上不可能
- 侵入されて業務停止などに追い込まれるケースが、海外では発生

イーサネットや汎用OSの普及

- 制御システムの中核であるPLCも、外部アクセスの危険性あり
- USBメモリ、メンテナンスPCの接続からの感染事例が増えている

IoT/M2Mの進展

- 近い将来、当たり前のように機器同士がインターネットを介して接続
- 攻撃にさらされる機会、さらなるオープン化が、より加速する

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。

1

安定稼動(可用性)が最優先

- ◆ 可用性を重視するため OSやセキュリティーパッチなどの変更ができない

ホワイトリスト型対策では、一度リストを作成すれば登録されたアプリケーションに変更がない限りシステムの更新が不要

2

セキュリティー対策が難しいデバイスの保護

- ◆ レガシーな装置/OSも継続利用しなければならない

デバイスのメンテナンスは不要で、不正な通信は止めてしまうのでネットワークの安全性を確保

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。

- ◆ 学習状態：一定期間は普通のスイッチとして動作し、通過するパケットを自動学習
- ◆ 運用状態：状態切替後は、未学習のフローに対して廃棄/通知/ミラーを選択可能

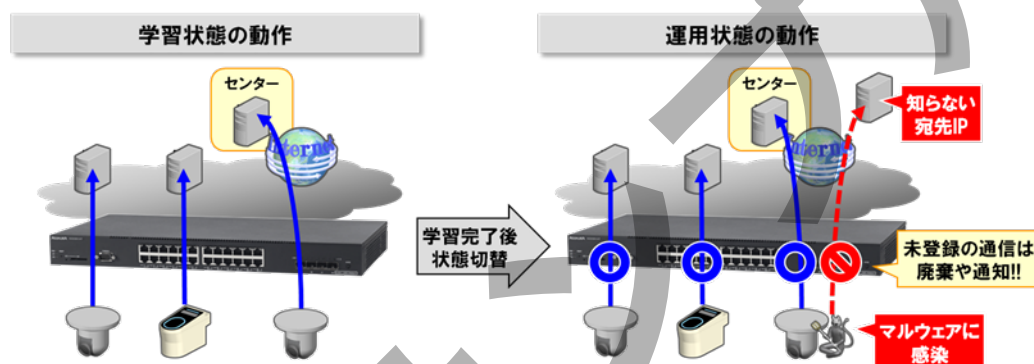


図 2-1 ホワイトリスト機能の概要

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。

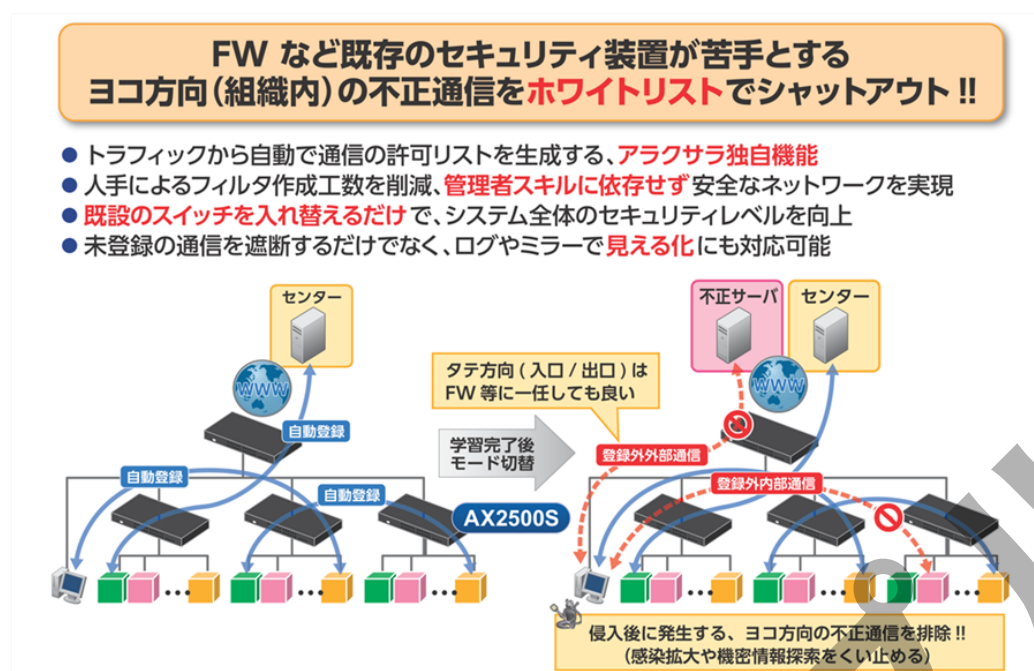


図 2-2 ホワイトリスト機能の特徴

2.3 製品ラインアップ

(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 アドバンスド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。

UTP24port + 10G 4port AX2530S-24T4X 10/100/1000BASE-T 24ポート 10GBASE-R SFP/SFP+ 4ポート 10G アップリンク	UTP48port + SFP 2port + 10G 2port AX2530S-48T2X PoEモデルあり(※2) 10/100/1000BASE-T 48ポート 1000BASE-X SFP 2ポート 10GBASE-R SFP/SFP+ 2ポート 10G アップリンク	SFP24port + 10G 4port AX2530S-24S4X DCモデルあり 光多ポート 光多ポートギガビットスイッチ 1000BASE-X SFP 24ポート 10GBASE-R SFP/SFP+ 4ポート
UTP24port + SFP 4port AX2530S-24T DCモデルあり ファンレス ファンレスのギガビットスイッチ 10/100/1000BASE-T 24ポート 1000BASE-X SFP 4ポート	UTP48port + SFP 4port AX2530S-48T DCモデルあり 準ファンレス(※1) 多ポート収容のギガビットスイッチ 10/100/1000BASE-T 48ポート 1000BASE-X SFP 4ポート	
UTP8port + SFP 2port AX2530S-08P DCモデルあり 8ポートPoE 雷サージ対策 耐環境スイッチ 10/100/1000BASE-T 8ポート 1000BASE-X SFP 2ポート	UTP8port + SFP 2port AX2530S-08TC1 ファンレス DINレールマウント型モデル 10/100/1000BASE-T 8ポート 1000BASE-X SFP 2ポート	

※1 準ファンレス: 常温時は停止、高温時は回転
※2 PoE モデル = AX2530S-48P2X

図 2-3 AX2500S シリーズ

(b) AX260A シリーズ

AX260A シリーズはエントリーモデル(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。

エントリーモデルは、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。またエントリー数は、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 エントリーまで拡張可能です。

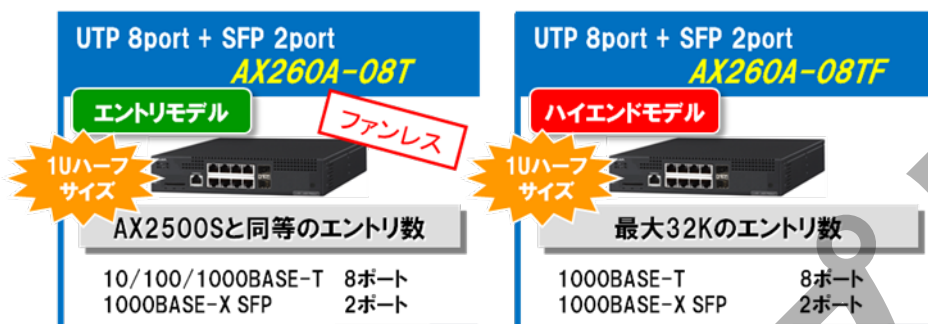
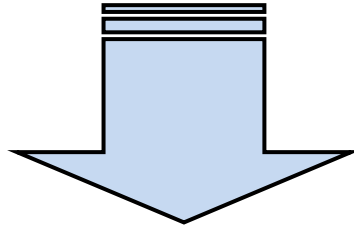


図 2-4 AX260A シリーズ

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/>