

端末トレーサビリティソリューション 活用ガイド

初版

資料 No. NTS-18-R-004

アラクサラネットワークス株式会社

はじめに

アラクサラネットワークスの「端末トレーサビリティソリューション」は、ネットワークにつながる多数の端末情報を自動的に収集して、対象となる端末の特定と接続場所の把握をリアルタイムに行えるようにするソリューションです。本ガイドは、端末トレーサビリティソリューションの活用例を紹介し、一助となることを目的としています。

関連資料

- アラクサラ AX シリーズ製品マニュアル
(<http://www.alaxala.com/jp/techinfo/manual/index.html>)
- アラクサラ AX-Security-Controller ユーザーズガイド
(<http://www.alaxala.com/jp/techinfo/manual/index.html#AX-SC>)

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、ユーザーズガイド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。

- アラクサラ スイッチ

AX3660S	Ver. 12.1.E
AX2530S	Ver. 4.11
- アラクサラ セキュリティコントローラ

AX-Security-Controller	Ver. 1.6
------------------------	----------
- 他社製 スイッチ

Cisco 社 Catalyst 2960S	
HP 社 ProCurve Switch 2510G	

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。

目次

1. 端末トレーサビリティソリューションとは	5
1.1 端末管理の課題	5
1.2 端末トレーサビリティソリューションの概要	5
1.3 端末トレーサビリティソリューションの特徴	6
2. 端末トレーサビリティソリューションの要件	7
2.1 システム要件	7
2.2 AX-Security-Controller	7
2.3 AX-SC のライセンス	8
3. システム構築例	9
3.1 ネットワーク構成例	9
3.1.1 システム構成図	10
3.1.2 システム構築について	11
3.2 管理対象装置の設定	12
3.2.1 コンフィグレーションの設定例	12
3.3 AX-SC の起動	15
3.3.1 AX-SC(Manager)の起動方法	15
3.3.2 AX-SC(Tracker)の起動方法	16
3.4 AX-SC へのアクセス	17
3.4.1 AX-SC(Manager)へのアクセス	17
3.4.2 AX-SC(Tracker)へのアクセス	17
3.5 AX-SC の初期設定	18
3.5.1 ライセンスの設定	18
3.5.2 管理対象装置の登録	20
3.5.3 接続情報の設定	25
3.5.4 エイリアスとポートエイリアスの設定	28
3.5.5 マップの設定	30
3.6 AX-SC での端末一覧とマップの表示例	33
3.6.1 端末一覧の表示例	33
3.6.2 マップの表示例	34
4. ソリューション活用例	36
4.1 リアルタイムの端末接続情報を可視化する	36
4.2 セキュリティインシデント発生時に被疑端末を調査する	37
4.3 その他の活用例	38

4.3.1	外部 SOC のインシデント検知における対処に活用.....	38
4.3.2	端末誤接続のチェックに活用	38
4.3.1	情報資産管理に活用	39
5.	注意事項.....	40
付録 1.	動作環境	41

資料サンプル

1. 端末トレーサビリティソリューションとは

1.1 端末管理の課題

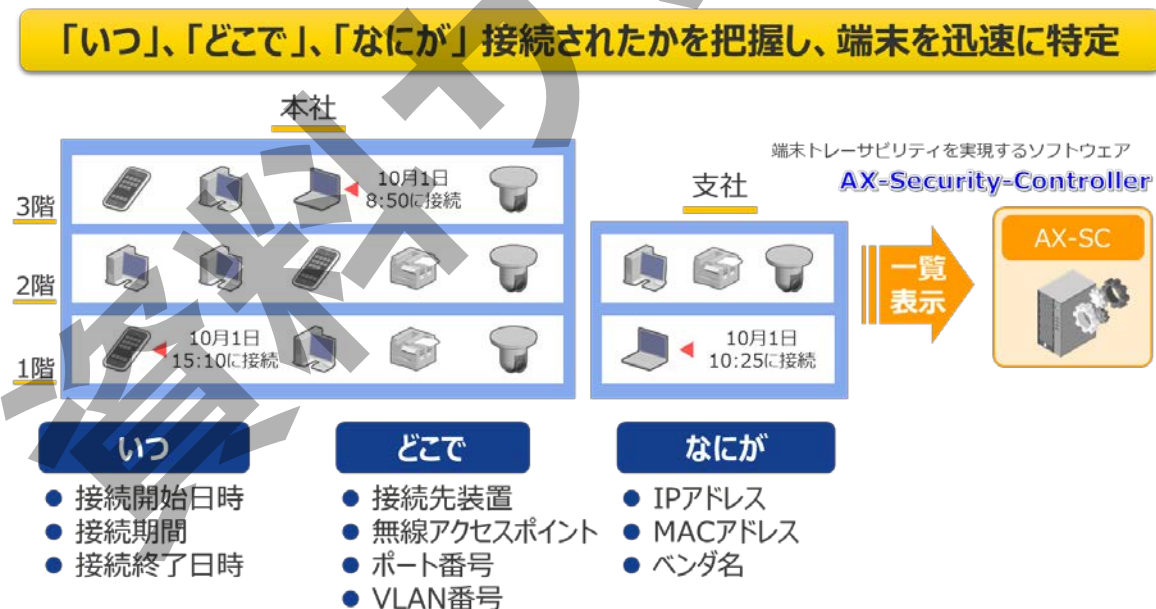
企業だけでなく、医療機関や教育機関でもスマートフォンやタブレット端末の活用が進み、ネットワークにアクセスする端末の運用管理は大きく様変わりしています。

ノート PC、スマートフォン、タブレット端末などモバイル利用を主体とする端末がネットワークに多数アクセスするようになり、セキュリティインシデントへの対応や不正な端末からのアクセス遮断など、端末の特定と接続場所の把握が必要な状況も日常的になっています。

これまで端末の情報として取得できるのは IP アドレスだけという場合が多く、問題のある端末を特定するには、いろいろな機器のログ情報を集めて解析するなど多大な時間と工数を要することが課題でした。利用場所がほぼ固定されるデスクトップ PC 主体だったときと異なり、端末（ユーザ）が随時移動するため、実際にどの端末が、どのネットワーク機器にアクセスしているかは流動的です。セキュリティインシデントや何らかの問題が確認されてから時間が経てば、それだけ端末の特定は困難になり、ログ解析などに要する時間と工数も膨大になっていきます。また対象となる端末やネットワークが遠隔地などにあり、物理的に遠い場合には、現地に担当者を派遣するなど人的リソースの負担も高まります。どこからでも端末の情報とアクセスしている場所を速やかに把握、特定でき、効率的な運用管理を実現することも重要です。

1.2 端末トレーサビリティソリューションの概要

端末の特定、トレースを行うソリューションを導入する際、ネットワークの再設計や再構築が必要になることがあります。また、すべての端末にソフトウェア（エージェントなど）を追加する場合もあります。いずれも導入にあたっての検討や実装、コストなどいろいろな面で負担が増えますし、エージェント型のソリューションでは未導入の端末を不正なものとして検知はできても、その動向を逐次追いかけることはできません。



アラクサラの「端末トレーサビリティソリューション」は、既存のネットワークにセキュリティコントローラ(AX-Security-Controller)を設置するだけで利用でき、端末へのエージェント導入も不要です。設置済みのネットワーク機器から情報を自動的に収集して、各端末が接続されている装置、ポート、VLAN などの状況をリアルタイムに確認できるほか、トポロジマップや実際のフロア見取り図の上で端末の位置を具体的に可視化することもできます。

また関連する情報は、すべてダッシュボード画面に集約されるので、知りたいことを素早く捉えられるだけでなく、遠隔地の端末やネットワークの状況も一括して見る事が可能です。

1.3 端末トレーサビリティソリューションの特徴

＜特長1＞必要な情報を自動収集してリアルタイムに端末を特定・可視化

端末がアクセスしている装置やネットワークなどの情報は、ネットワークスイッチから自動的に収集、蓄積するので運用の負荷が少なくて済みます。

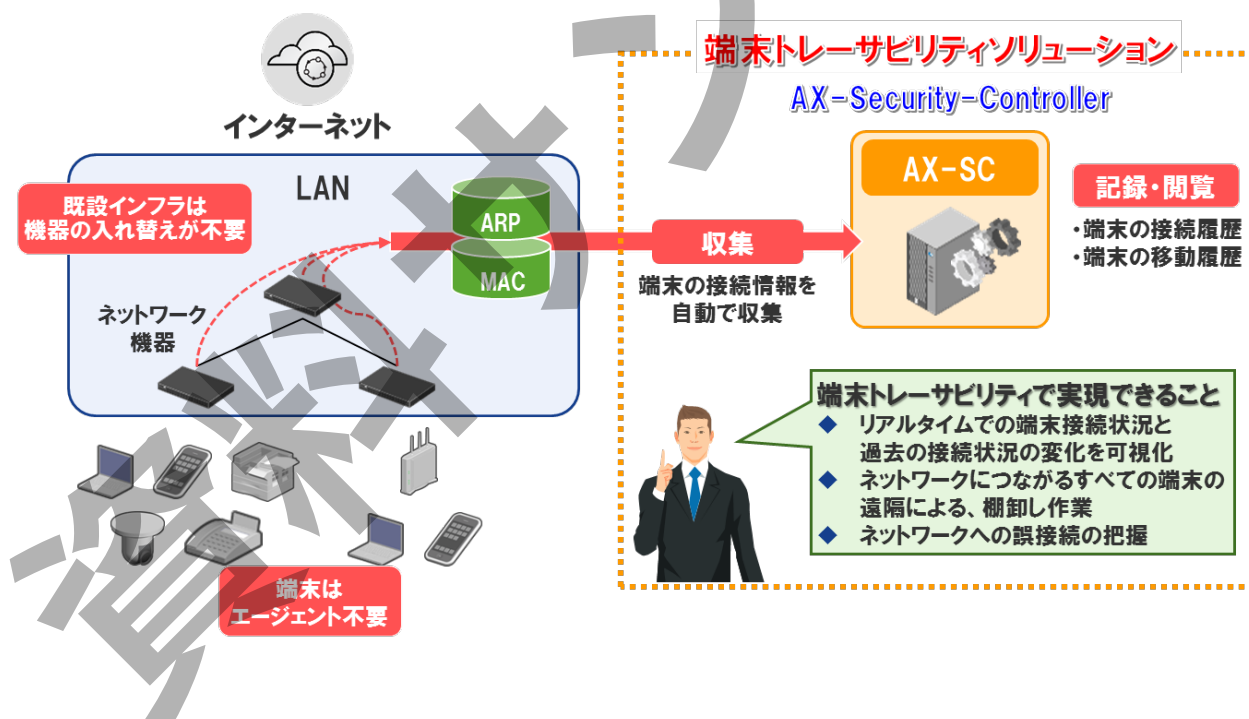
端末に利用者や部署名といったエイリアス（ラベル）を設定したり、ネットワークスイッチやアクセスポイントの設置場所を装置名として設定したりすることで一覧表示の見やすさを高め、より直感的でわかりやすい可視化を行えます。

＜特長2＞過去の端末情報（履歴）も可視化

自動収集した過去の履歴を保持しており、問題発生時に遡って端末の利用状況を容易にトレースできます。事象の把握と影響範囲の絞り込みをアシストします。DHCP のアドレス変更や端末の移動など、時間の経過に伴う変化にも自動追従します。

＜特長3＞既設ネットワークへ迅速に導入・適用

アラクサラのセキュリティコントローラ「AX-Security-Controller」を既存のネットワークに追加するだけで、端末の特定や接続位置の可視化を実現します。他社製品のスイッチなどを利用している場合にも導入できます。端末へのエージェントの導入も不要です。



2. 端末トレーサビリティソリューションの要件

2.1 システム要件

AX-Security-Controller は、汎用サーバ上で動作する Python ソフトウェアです。本ソリューションのシステム要件を以下に示します。ハードウェア構成やソフトウェア構成および管理対象装置の詳細な内容については「付録 1. 動作環境」を参照ください。

- AX-Security-Controller を動作させる汎用サーバと Python ソフトウェア
- AX-Security-Controller
- 管理対象装置
- AX-Security-Controller に Web アクセスするための端末とブラウザ

2.2 AX-Security-Controller

端末トレーサビリティソリューションでは、AX-Security-Controller(以下 AX-SC)を利用し端末情報を収集します。本ソリューションでは、端末位置情報やトポロジ管理をおこなう AX-Security-Controller(Manager) と 過去の端末情報を参照する AX-Security-Controller(Tracker)を活用します。

(1) AX-Security-Controller (Manager)

ネットワーク上の端末位置情報を表形式やトポロジ図形式で管理するトポロジ管理をおこないます。セキュリティ装置と連携した場合は、インシデント情報やインシデント対策指示から、トポロジ管理やトポロジに応じたポリシーに基づいてインシデント対策を行うことにより、マルウェア感染端末を収容する装置で同端末をネットワークから遮断することができます。また、ネットワーク管理者が Web インタフェースを通して AX-SC を管理することができます。



図 2-1 AX-Security-Controller(Manager)のイメージ

(2) AX-Security-Controller (Tracker)

AX-Security-Controller(Manager)が管理しているトポロジから、端末が接続している装置およびポートを定期的に収集し、最大 3650 日(※)の履歴を保持することで、端末の移動履歴を算出します。また、ネットワーク管理者がこの算出結果を Web インタフェースを通して参照することができます。

※ 履歴保持期間は、1～3650 日でカスタマイズ可能です。初期値は 365 日です。

履歴検索結果

CSV形式で保存

表示カラム切替 25 件表示

検索:

接続開始日時	接続終了日時	接続期間	MACアドレス	ベンダ	IPアドレス	エリアス	接続先装置	ポート番号	ポートエリアス	VLAN
2017/12/06 18:34:24 JST	2017/12/06 18:44:24 JST	0d0h10m0s	000c.e6	Meru Networks Inc	192.168.1.127	None	A線エッジスイッチ1	0/5	Fortinet AP2	1
2017/12/06 18:34:24 JST	2017/12/06 18:54:24 JST	0d0h20m0s	000c.e6	Meru Networks Inc	192.168.1.127	None	A線エッジスイッチ1	1/0/26	Fortinet AP1	1
2017/12/06 18:49:24 JST	2017/12/06 18:54:24 JST	0d0h5m0s	000c.e6	Meru Networks Inc	192.168.1.127	None	A線エッジスイッチ1	0/5	Fortinet AP2	1
2017/12/07 09:09:37 JST	2017/12/07 10:29:38 JST	0d1h20m1s	7831.c1	Apple, Inc.	192.168.1.127	None	A線エッジスイッチ1	0/2	D-Link AP1	1
2017/12/07 09:09:37 JST	2017/12/07 09:29:37 JST	0d0h20m0s	7831.c1	Apple, Inc.	192.168.1.127	None	A線エッジスイッチ1	1/0/11		1
2017/12/07 11:14:38 JST	2017/12/07 11:29:39 JST	0d0h15m1s	7831.c1	Apple, Inc.	192.168.1.127	None	A線エッジスイッチ1	0/2	D-Link AP1	1
2017/12/07 11:54:39 JST	2017/12/07 12:04:39 JST	0d0h10m0s	7831.c1	Apple, Inc.	192.168.1.127	None	A線エッジスイッチ1	0/10	D-Link AP2	1
2017/12/07 14:29:41 JST	2017/12/07 14:54:41 JST	0d0h25m0s	7831.c1	Apple, Inc.	192.168.1.127	None	A線エッジスイッチ1	0/6	Aruba AP2	1
2017/12/07 14:54:41 JST	2017/12/07 15:09:41 JST	0d0h15m0s	7831.c1	Apple, Inc.	192.168.1.127	None	A線エッジスイッチ1	0/4	Aruba AP1	1
2017/12/07 15:09:41 JST	2017/12/07 15:14:41 JST	0d0h5m0s	7831.c1	Apple, Inc.	192.168.1.127	None	A線エッジスイッチ1	0/2	D-Link AP1	1
2017/12/07 15:14:41 JST	2017/12/07 15:19:41 JST	0d0h5m0s	7831.c1	Apple, Inc.	192.168.1.127	None	A線エッジスイッチ1	0/6	Aruba AP2	1
2017/12/07 15:19:41 JST	2017/12/07 15:24:41 JST	0d0h5m0s	7831.c1	Apple, Inc.	192.168.1.127	None	A線エッジスイッチ1	0/4	Aruba AP1	1
2017/12/07 15:24:41 JST	2017/12/07 15:29:41 JST	0d0h5m0s	7831.c1	Apple, Inc.	192.168.1.127	None	A線エッジスイッチ1	0/2	D-Link AP1	1
2017/12/07 15:29:41 JST	2017/12/07 15:34:41 JST	0d0h5m0s	7831.c1	Apple, Inc.	192.168.1.127	None	A線エッジスイッチ1	0/4	Aruba AP1	1
2017/12/07 15:34:41 JST	2017/12/07 15:39:41 JST	0d0h5m0s	7831.c1	Apple, Inc.	192.168.1.127	None	A線エッジスイッチ1	0/2	D-Link AP1	1
2017/12/07 15:49:42 JST	2017/12/07 16:04:42 JST	0d0h15m0s	7831.c1	Apple, Inc.	192.168.1.127	None	A線エッジスイッチ1	0/6	Aruba AP2	1
2017/12/07 17:39:43 JST	2017/12/07 17:54:43 JST	0d0h15m0s	7831.c1	Apple, Inc.	192.168.1.127	None	A線エッジスイッチ1	0/2	D-Link AP1	1
2017/12/08 09:19:58 JST	接続中	299d8h37m28s	7831.c1	Apple, Inc.	192.168.1.127	None	A線エッジスイッチ1	0/10	D-Link AP2	1

18 件中 1 から 18 まで表示

前のページ 1 次のページ

図 2-2 AX-Security-Controller(Tracker)のイメージ

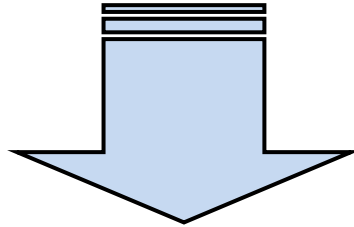
2.3 AX-SC のライセンス

AX-SC はサブスクリプション方式のソフトウェアです。端末トレーサビリティ機能に関するライセンスは、下記 2 種類のライセンスです。

表 2-1 AX-SC のライセンス

項目	説明
基本ライセンス	AX-SC を使用するためのライセンスで必須となります。 管理対象スイッチは、10 台まで登録することができます。
AX-SC	基本ライセンス(管理対象スイッチ 10 台まで)
管理対象スイッチ拡張ライセンス	管理対象スイッチ数を拡張するためのライセンスでオプションとなります。管理対象スイッチを 10 台より増やしたい場合に必要となります。
OP-20	管理対象スイッチ拡張ライセンス +20 台
OP-50	管理対象スイッチ拡張ライセンス +50 台
OP-100	管理対象スイッチ拡張ライセンス +100 台

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/>