

LanScope Cat6

技術情報 Vol.19

～不正検知オプション導入時の注意事項～

2008年11月10日

第9版

エムオーテックス株式会社

VLAN使用環境での注意点

VLANについて

VLANとはスイッチの内部で複数のネットワークに分割する技術のこと。ネットワークを任意に分割することで、ブロードキャストパケットが届く範囲を区切ることができる。

LanScopeCatの不正PC検知機能は検知エージェント(DA)がノードの発行するARPを検知する仕組みのため、**ARPが届く範囲を正しく理解しておく必要がある。**
本資料は代表的なVLANの技術を紹介し、構成に応じたDAの配置を解説している。

VLAN技術の種類について

①ポートVLAN

スイッチの**ポート毎**に「どのVLANに所属するか」を設定する。現在のVLANの主流方式。

②タグVLAN

複数のスイッチを使用して、「それぞれのネットワークでVLANを設定し、かつ離れた場所にある別々のVLANを1つのVLANとしてまとめる」ことができる。
LANフレームにどのVLANから送られたかという情報を格納した**タグ**を付加する。

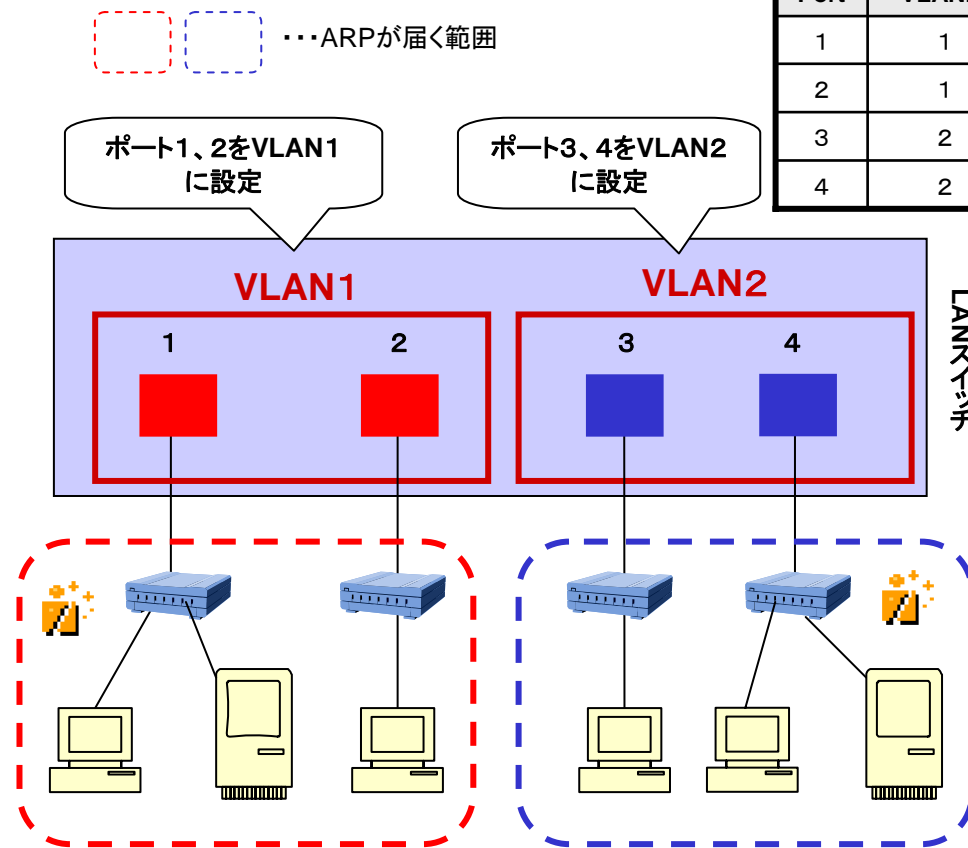
③マルチプルVLAN

VLANが設定された各ポートにクライアントとアップリンクを設定し、**クライアントとアップリンク間の通信**を許可することで、セキュリティを保ちながら設定の柔軟性を向上させることができる。
※アップリンク…どのVLANからでもアクセス可能な領域

①ポートVLAN環境での構成例

ポートとVLANの対応表

Port	VLANID
1	1
2	1
3	2
4	2



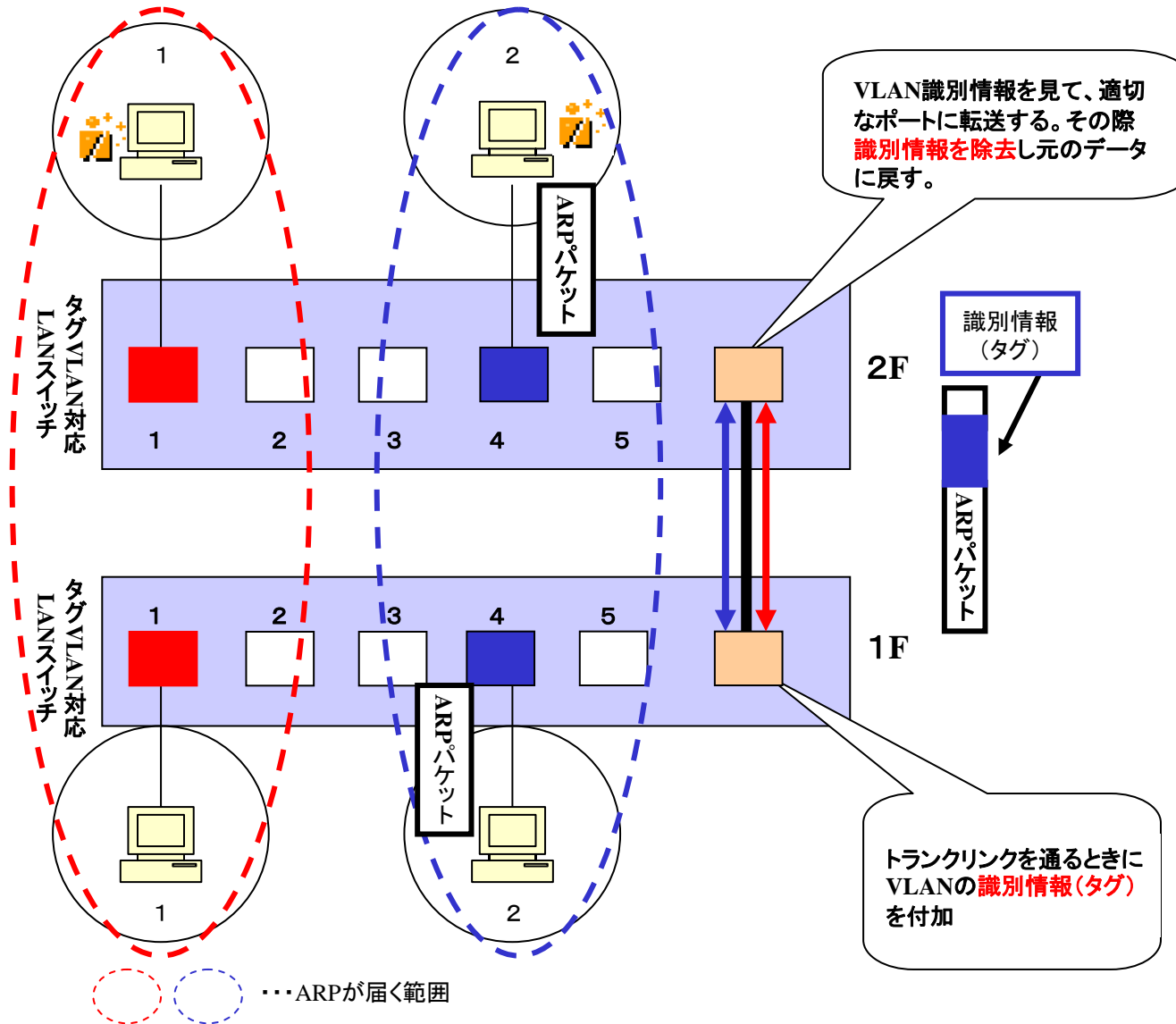
注意事項

ポートVLANの環境では、DAはVLANIDごとに1つ必要。

Point

ポートVLANの環境では、DAはVLANIDごとに1つ必要。
上記構成では**VLANが2つ**あるので**DAは2ライセンス**必要になる。

② タグVLAN環境での構成例



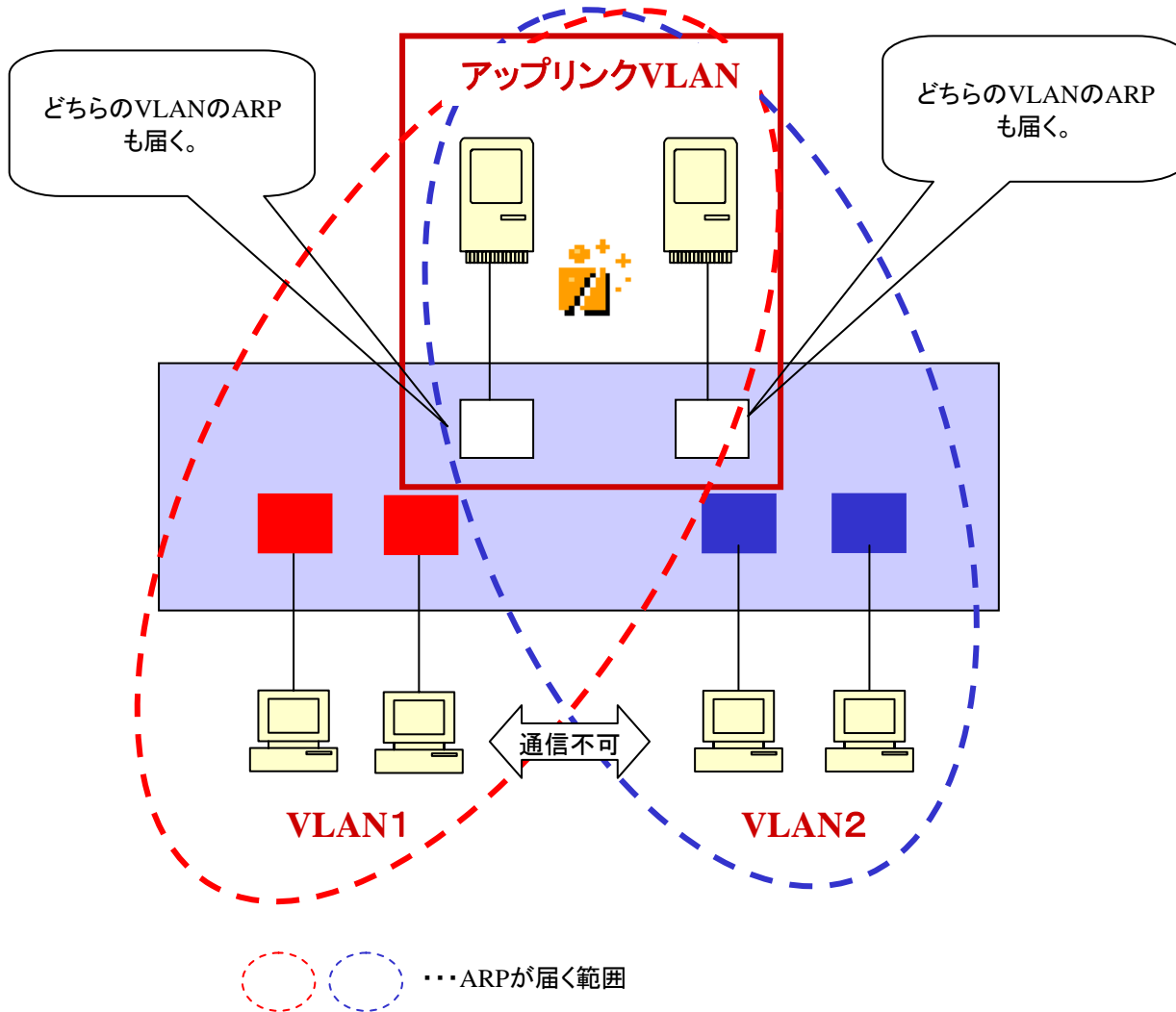
解説

タグVLANの環境では、DAはVLANごとに1つ必要。

Point

左図ではVLANが2つあるのでDAは2ライセンス必要になる。

③マルチプルVLAN環境での構成例



解説

マルチプルVLANではアップリンクVLANにすべてのVLANからのARPが届く。

そのため、アップリンクVLAN内にDAを設置することですべてのVLANの検知が可能。

※ただし、1DAで管理できるノード数の上限は1000ノードまで。マルチプルVLAN環境に1000ノード以上所属する場合はVLAN毎にDAを設置する。

Point

左図ではVLANが2つあるが、DAのライセンスは1ライセンスでよい。

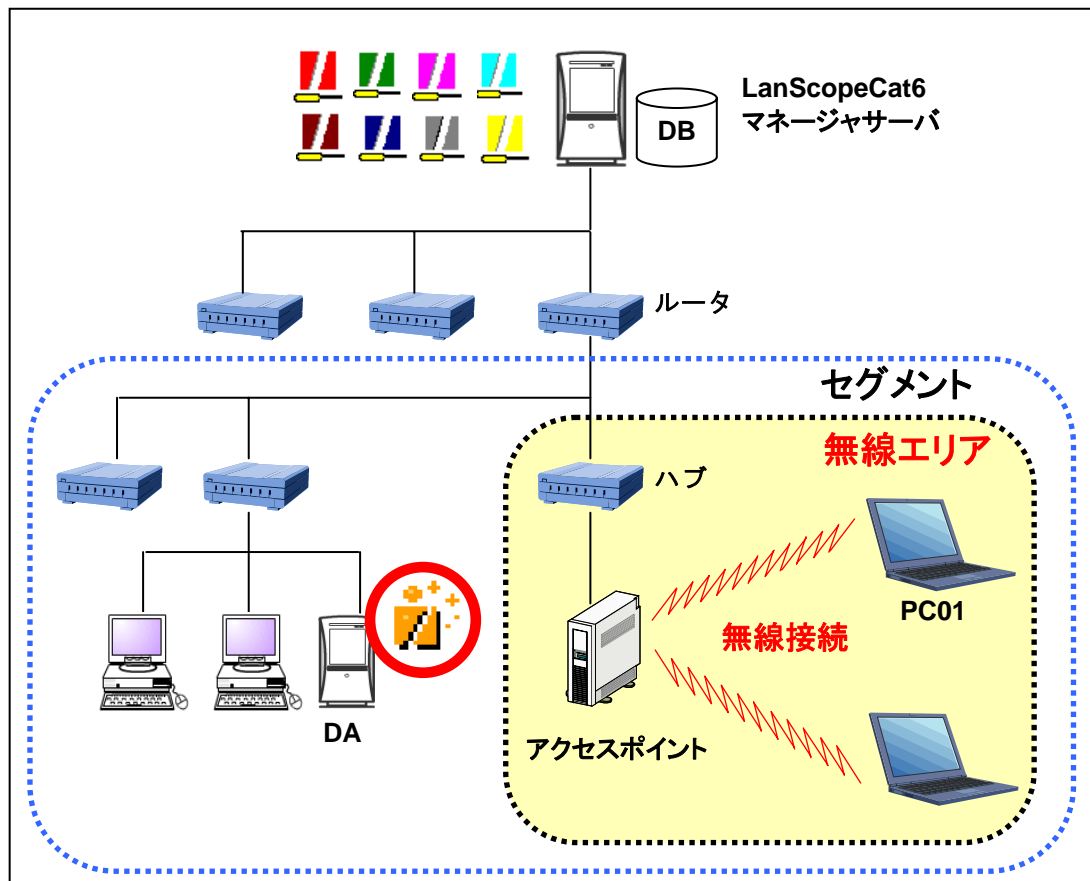
※ただし、1000ノードまでの制限あり。

無線LAN使用環境での注意点

■無線LAN環境での注意事項について

無線LAN環境であってもLanScope Cat6の不正PC検知機能は正常に使用できます。但し、アクセスポイントの設定によってDAのライセンス数と設置場所が異なります。

①アクセスポイントがブリッジ設定の場合



アクセスポイントがブリッジ設定の場合、PC01を検知・遮断するためのDA設置と注意事項について記載します。

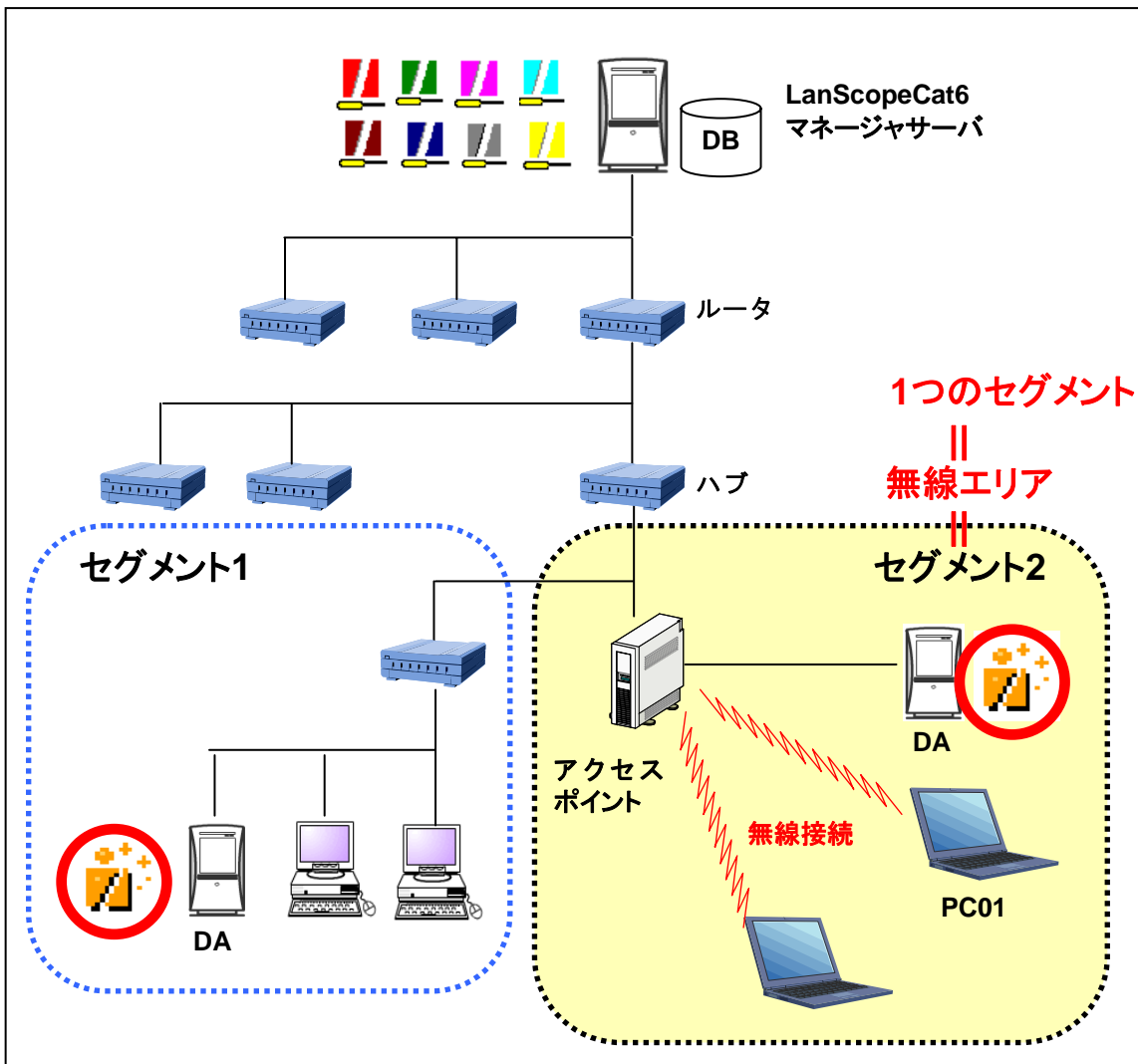
Point

- 左図構成では1セグメントのためDAは1つ必要。
無線エリアにDAは必要ありません。
アクセスポイントを設置しても無線エリアは同一セグメントと見なされます。
- 既存のネットワークに無線環境を追加する場合は、ブリッジ設定であればDAを追加する必要はありません。

注意事項

有線LAN、無線LANに関わらず、クライアントPCの禁止は可能。アクセスポイントを禁止しても、無線接続しているクライアントPCは接続可能となります。禁止する場合は、クライアントPC自身を禁止にしてください。

②アクセスポイントがルーター設定の場合



アクセスポイントがルーター設定の場合、PC01を検知・遮断するためのDA設置と注意事項について記載します。

Point

- 左図構成では2セグメントのためDAは2つ必要。
無線エリアにDAが必要となります。
アクセスポイントを介して無線エリアが別ネットワークと認識され、セグメントも異なります。

注意事項

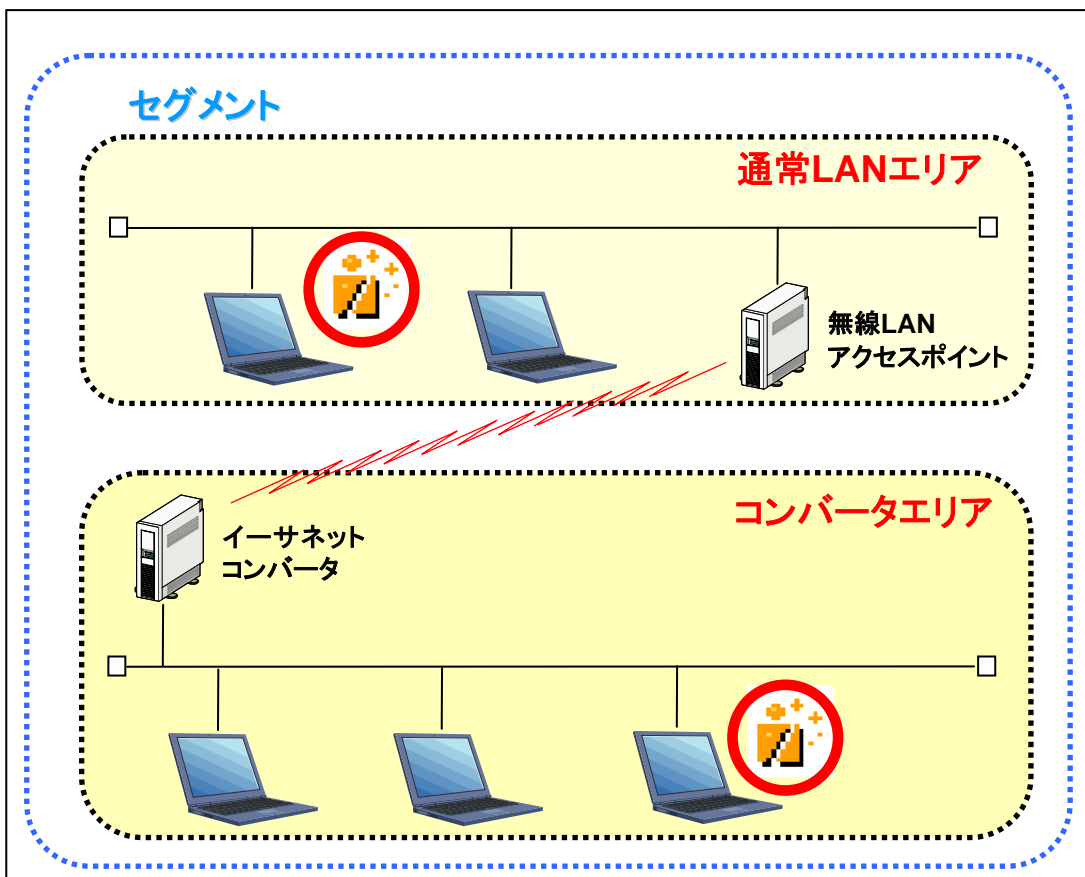
- 無線エリアでクライアントを検知・遮断する条件は以下2つであります。
1. 無線エリア内にDAを設置してください。
 2. DAを設置する場合はアクセスポイントのLANポートに有線接続してください。
- ※無線エリア内のアクセスポイントとDA端末が無線接続ではPC01を遮断できません。

コンバータ使用環境での注意点

■イーサネットコンバータを使用している環境での注意事項について

イーサネットコンバータ環境であってもLanScope Cat6の不正PC検知機能は使用できます。但し、DAの設置箇所やコンバータの設定によっては、許可端末が禁止になる、または不正端末が禁止されない場合があります。

イーサネットコンバータとは、LANポートが搭載されているPCやネットワーク対応家電製品(テレビなど)を無線LANルーターに通信させたい時に使われます。



イーサネットコンバータを使用している環境において、正しく検知/遮断する為の、設定について記載します。

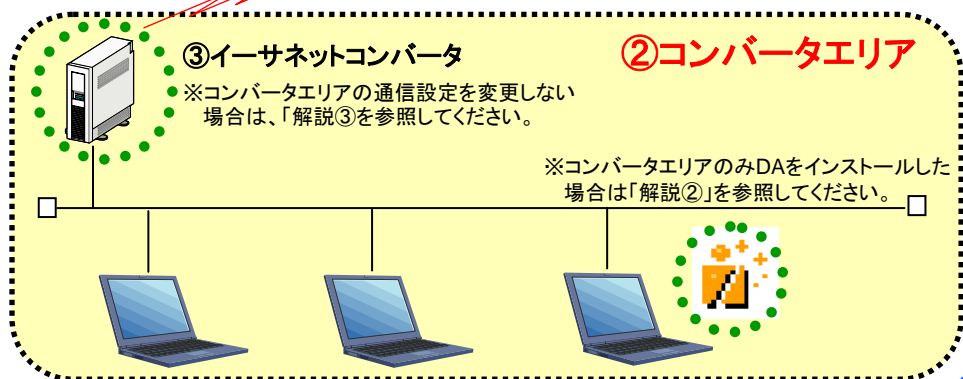
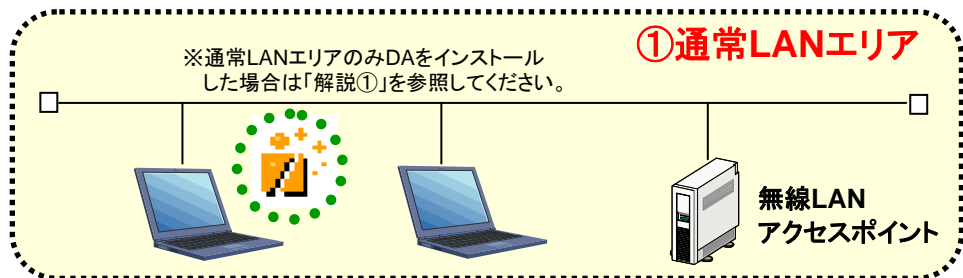
Point

1. 通常LANエリアとコンバータエリアの一方のエリアにしかDAがなければ、端末を検知したり、接続検知の俊敏性に欠ける為、左図構成ではセグメント数は1つですが、通常LANエリアとコンバータエリアのそれぞれにDAは必要です。
2. イーサネットコンバータ側の通信設定を、イーサネットコンバータ自身のMACアドレスを使用する設定に変更してください。
3. イーサネットコンバータを使用している環境でも、クライアントPCの禁止は可能です。ただし、イーサネットコンバータを禁止にすると、コンバータに接続されている端末も全て禁止になる為、任意MACアドレス許可設定でコンバータのMACアドレスをあらかじめ登録しておいてください。

イーサネットコンバータについて

このページでは、**P-11の設定を行わなかった場合の説明を記載します。**

セグメント



解説①

通常LANエリアのみDAをインストールした場合は、イーサネットコンバータは検知できますが、**コンバータエリア内の端末を検知することはできません。**

解説②

コンバータエリアのみDAをインストールした場合は、コンバータ内の端末及び通常LANエリアの端末の両方を検知することが可能ですが、**DAが検知できるARPの量が通常より減ってしまう為、接続を検知するまでに時間がかかります。**

解説③

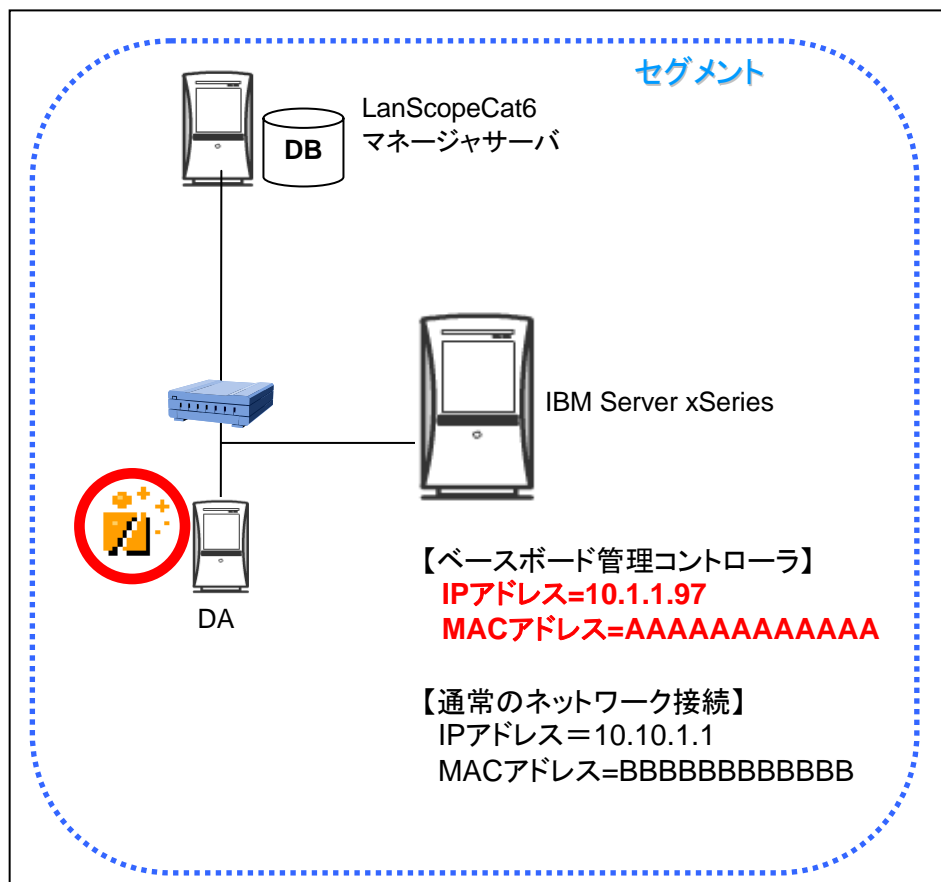
イーサネットコンバータ側の通信設定を、**イーサネットコンバータ自身のMACアドレスを使用する設定ではない場合は、コンバータ内に接続されている端末のMACアドレスを、コンバータが自分のMACアドレスとして通信を行います。**

この場合、コンバータエリア内に禁止端末が接続された場合は、**コンバータ自身も禁止され、コンバータエリア内の全ての端末が禁止されます。また、禁止端末が許可されてしまう場合もあります。**

その他の環境で確認できている 注意点

■ IBM Server xSeries 236, 336, 346, 366を使用している環境での注意事項について

上記IBM製サーバを使用している場合、必要な設定について記載します。



Point

- IBM Server xSeries236,336,346,366には、ベースボード管理コントローラ(BMC)というシステム管理プロセッサを持っています。ベースボード管理コントローラには通常のネットワーク接続とは別のIPアドレス、MACアドレスが設定される場合があります。

この場合、ベースボード管理コントローラは本体のIBM Serverとは別のノードとして認識されますので、個別許可設定、任意MACアドレス許可、任意IPアドレス許可のいずれかを設定する必要があります。

注意事項

IBM製サーバ起動時に、以下の順番でARPが飛ぶ場合があります。

1. ベースボード管理コントローラ
2. 通常のネットワーク接続用

この場合、通常のネットワーク接続用のMACアドレスのみ任意MACアドレス許可設定を行っている場合、サーバ起動時にIBM Serverが禁止される場合がありますので、必ず両方のMACアドレスを任意MACアドレス許可設定に登録してください。

ベースボード管理コントローラのIPアドレス、MACアドレス確認方法は下記の日本IBM株式会社のWebより、ご確認ください。

【ベースボード管理コントローラの設定方法に関して】

<http://www-1.ibm.com/support/docview.wss?uid=pcd1syj0-0070ffc>

■HP製の端末（HP-DX2000MTとd530）使用している環境での注意事項について

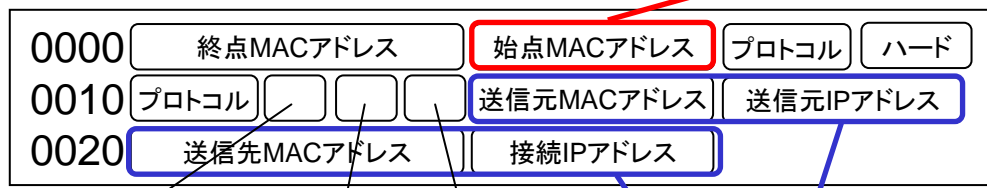
上記HP製の端末を使用している場合、必要な設定について記載します。

【ARPの概要】

イーサネット環境において、IPアドレスからMACアドレスを得るために用いるプロトコルです。TCP/IPにおいて、IPパケットを送受信するためには、下位のデータリンク層のアドレスを取得する必要があり、送信先のMACアドレスを解決する為に、ARPが用いられます。

ARPパケットの中身

デフォルトの設定では、禁止用の偽ARPパケットにはDAのインストール端末のMACアドレスを格納します（通常的环境では、設定を変更する必要はありません）



MACアドレス長, IPアドレス長, 操作コード, ARPテーブルに登録される情報

Point

●不正PC検知は、左図のようなARPパケットを使用して端末の検知/遮断を行っています。

注意事項

上記のHP製端末を禁止設定した場合、検知エージェントのデフォルトの動作では禁止されないことが、確認できています。管理上は**禁止端末扱い**（禁止アイコンや禁止ログが通知される）となりますが、実際の端末では、ARPテーブルには擬似のMACアドレスが登録されていてもネットワークに接続できてしまいます。

【対策】
「**DAFilter.ini**」を作成し、始点MACアドレスの設定を、「DA端末のMACアドレス」から「**禁止用擬似MACアドレス(000000000001)**」に変更すれば、禁止することが可能です。



- 【DAFilter.iniの作成方法】
- ①DAのインストールフォルダに「**DAFilter.ini**」を作成。
(C:\Program Files\MOTEX\LanScope Cat DA)
 - ②左の図のように、「**[FSTARTMAC]**」を作成し、「**true**」と入力する。
 - ③LSPSERVICE_DAを再起動で設定が完了。

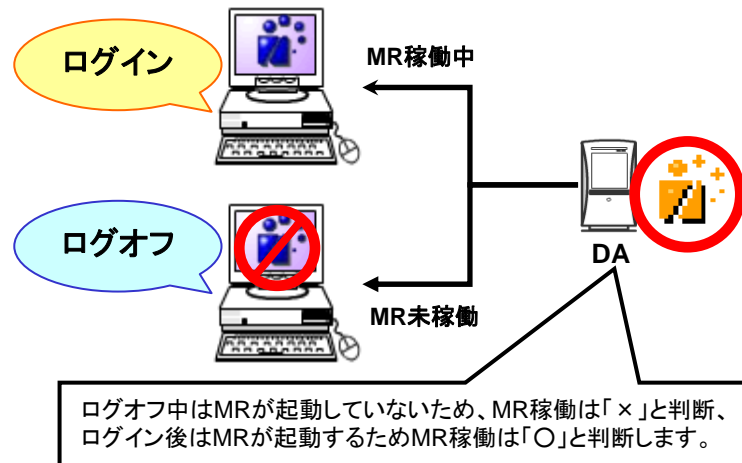
その他の制限事項

■その他の制限事項1

Windows98のエージェント端末は、ユーザがログインした後にMRが起動する仕様のため、ログイン前に検知エージェントがMR稼働チェックを行った場合MR稼働が×として判断されます。

【影響】

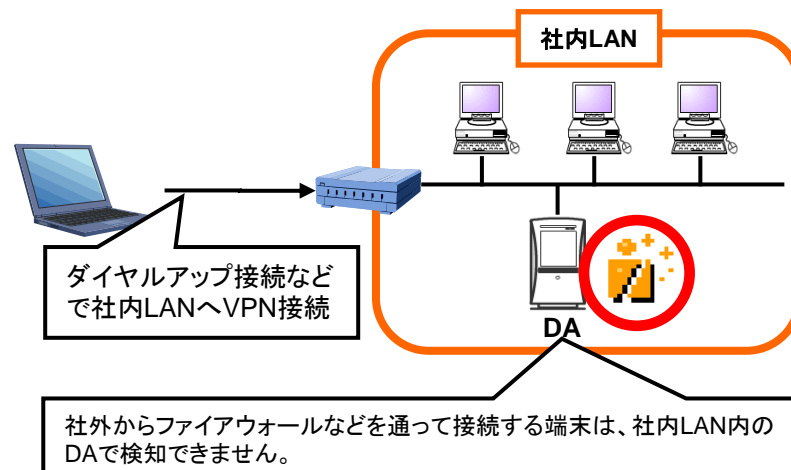
管理者がアラーム通知メールを受信し、その後で統合コンソールからノード管理一覧画面を確認すると正常にMRが稼働していたという状況が発生する場合があります。



社外からVPNなどを使用して社内LANに接続した場合、その端末は不正PC検知機能で検知することができません。

【影響】

社外からダイヤルアップや専用線、VPNソフトなどを使用して社内LANへ接続した場合、ARP通信が発生しないため、その端末を検知することができません。



■その他の制限事項2

No	制限事項	内容	発生対象の製品バージョン	対策
1	禁止設定をしている端末にpingが通ってしまう場合がある。	禁止になっている端末に対してpingが通ってしまいます。(一時的にpingは通るがファイルコピーなどの他の通信はできません)	—	pingが通ってしまうのは仕様。(プリンターなどではPingが通ることを確認できている)pingは通るが通信は遮断されている為、問題ありません。
2	プリンタを禁止できない。	プリンタに対して、禁止設定をしても、禁止がされず印刷ができてしまいます。	—	現状、対策はありません。
3	IBM Server xSeries (236,336,346,366)を使用している環境での注意事項。	IBMサーバの中にはMACアドレスを2種類もっているサーバの存在が確認できます。両方のMACアドレスを設定しない場合、一方のMACアドレスが禁止になってしまい、IBMサーバ自体が禁止になります。	—	通常のネットワークアダプタのMACアドレスと、BIOSのMACアドレスの2種類を例外許可設定に登録することで、IBM Serverが禁止されることを回避できます。
4	MRインストール済みのPCがMR未稼働になる場合がある。	Windows98などMRがサービス稼働されないOSの場合、ログオフ状態にて、DAよりMR稼働チェックが行われ、20分程度ログオフ状態が続くと、90回のリトライが終了し、MRがインストールされていないと判断し、MRが未稼働扱いになります。	～ Ver5.6.2.2	Windows98のOSについては、ログインするまでMRが動作しないために制限事項となります。回避方法として、該当端末には許可IPアドレス/許可MACアドレスを入力することで許可端末にできます。
5	1セグメントに複数のDAを同時に稼働させると、ログが複数上がる。	1セグメントにDAを複数稼働させていると、接続ログがDAの稼働台数分上がります。	～ Ver5.6.2.2	10分以内に同一ログが上がった場合は、フィルタ処理を行い、重複したログが表示されないようにします。
6	DA端末がスタンバイ/休止状態になると正常に端末を検知できない場合がある。	DAのインストール端末がスタンバイや休止状態になってしまった場合、次回復帰後、ON通信を行うまでの時間(約1分)正常に動作しません。	～ Ver5.6.2.2	回避方法として、DAをインストールしている端末では、スタンバイやスリープ、休止状態にしない設定にします。Ver5.7.0.0にて対策を行い、復帰後から動作が可能です。
7	HP製の一部の端末(HP-DX200MT、d530)に対して、禁止ができない。	原因は不明だが、デフォルトの設定で端末を禁止設定にしても、統合コンソール画面では禁止扱いになっているが、実際の端末では禁止になっていません。(禁止アイコンになっており、禁止ログが上がっている)	～ Ver5.7.2.0	Ver5.7.3.0にて対策。DAFilter.iniを編集し、始点MACアドレスを禁止用MACアドレスに編集すれば端末の禁止が可能。(デフォルトではDAのMACアドレスを使用する設定になっています)
8	ホスト名を取得できない場合や機器がある。	Ver5.6.0.0よりホスト名の取得が可能となっています。(DA端末のhostsファイル⇒DNSサーバ⇒NetBIOS通信)の順番でノードのホスト名を取得します。	Ver5.6.0.0～	ホスト名が取得できない場合は以下の3点の方法を実施してください。 1.Windowsファイアウォールの設定を無効にします。 2.ホスト名取得で使用するポート番号(UDP137)を設定にします。 3.初期の例外リストにある「ファイルとプリンタの共有」にチェックをします。
9	自社MR許可設定をする際に、対応バージョン未満のエージェントが入っている場合は禁止される。	Ver5.7.0.0より自社MRの許可設定が可能となりました。DAとMRIに「MR確認キー」を持たせ、ARPを検知する度にそれぞれのキーを確認して合致する場合は、自社のMRと認識し許可されます。(MR確認キー……自社の統合マネージャサーバのMACアドレス) MRのバージョンがVer5.7.0.0未満の場合、自社MR許可設定をした場合、確認キーを持っていない為、全てのノード(Ver5.7.0.0未満のMR端末)が禁止されます。	Ver5.7.0.0～	Ver5.7.0.0未満のMRが存在する場合は、自社MR許可設定を使用しないでください。使用する場合は以下の手順で対応してください。 1.MRのバージョンを5.7.0.0以上にします。 2.MRのバージョンが上がったことを確認してから、自社MR許可設定を使用します。
10	初回検知のみセグメント内のノードを検知するのに時間がかかる。	マネージャと通信が行える全ノードに対してMRの稼働チェックを行ってから、統合コンソールにノードアイコンを表示させます。(約1分間×ノード数)	Ver5.7.0.0～	初回構築時のみの制限事項となります。
11	禁止セグメントに新規ノード(MRインストールの可否に関わらず)が接続された場合、一時的に禁止になる。	DAは禁止設定のセグメントに新規で接続されたノードに対して、MR稼働チェックが有効になるまで禁止にします。MR稼働チェックが完了し、MRの稼働の確認ができれば接続が可能です。	Ver5.7.0.0～	新規ノードの端末に対して、許可MACアドレスもしくは許可IPアドレスの設定をすることで回避することは可能です。

■ その他の制限事項3

No	制限事項	内容	発生対象の製品バージョン	対策
12	無線LAN環境でのライセンスについて。	環境によって、DAの設置箇所やライセンスが異なります。	Ver5.7.0.0未満では導入する検知エージェント数のライセンスが必要 Ver5.7.0.0以上では管理するセグメント数分のライセンスが必要	【ブリッジ設定の場合】 同セグメントであれば、DAの設置箇所は気にする必要はありません。 【ルーター設定の場合】 別セグメントとなる為に、DAはそれぞれに設置が必要です。 【コンバータ使用の場合】 通常のセグメントとコンバータエリアにDAの設置が必要です。
13	VLAN環境でのライセンスについて。	環境によって、DAの設置箇所やライセンスが異なります。	Ver5.7.0.0未満では導入する検知エージェント数のライセンスが必要 Ver5.7.0.0以上では管理するセグメント数分のライセンスが必要	【ポートVLAN】 VLANIDごとに1つDAが必要です。 【マルチプルVLAN】 アップリンクVLANにDAを設置する場合、DAは1つで運用が可能です。 ただし、1000ノードまでの制限があります。 アップリンクに設置しない場合は、VLANIDごとにDAが必要です。
14	Teaming環境でBroadcom Advanced Control Suiteドライバを使用している場合	DA端末のドライバ(Broadcom Advanced Control Suite)のバージョンが古いとDA導入後、そのDA端末では一切、通信が行えなくなります。	Broadcom Advanced Control Suite2(8.2.4)にて現象確認	ドライバのバージョンを最新にアップデートしてください。 ※Broadcom Advanced Control Suite3(11.60.1)で正常動作を確認しています。