# 5章　管理設計

　　後々の運用を楽にするため、以下を設計する。

　１．ホスト名

　２．オブジェクト名

　３．ラベル定義

　４．パスワード

　５．運用管理ネットワーク

　６．設定情報

## １．ホスト名

　ホスト名は位置や機器、役割などの識別子を定義して、分かりやすいものにしていくべき。

(http://news.headline.example.jp ホスト名：news.headline、ドメイン：example、FQDN:news.headline.example.jp)

重要なポイントは、「文字数」と「呼び名(呼称)」。

「文字数」

　AnsibleやTera Termマクロなどを使用して、作業を自動化する際に、ホスト名の文字数を

合わせておくとコードが書きやすくなり文字列操作の手間が省ける。

「呼び名(呼称)」

　会議やドキュメント内で使用する呼び名。ホスト名は色々な識別子が入っていて、定義を理解していないと混乱する。

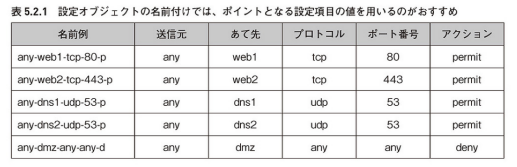
## ２．オブジェクト名

　ファイアウォールポリシー、アドレスグループ、VLANからリングアグリゲーションの論理ポート

など、各種設定オブジェクトの命名規則も重要な設計要素。

オブジェクト毎に命名規則を設け、わかりやすい名前を付けておくと運用管理の自動化が楽になる＆

引き継ぎもしやすくなる。



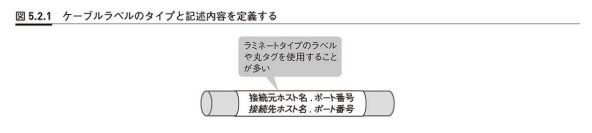
## ３．ラベル定義

　いざトラブルが発生したとき、どこに対象となる機器があるかを物理的に即座に把握するために必要。

・ケーブルラベル

　LANケーブル、電源ケーブルやSANで使用するファイバケーブルなど、サーバサイト内にある全てのケーブルを表す。どういう種類のラベルで、どのような内容を記述するかを定義する。

ラミネートタイプのラベルや丸タグに接続元・接続先の機器のホスト名とポート番号を記述することが多い。(既存のものがあればそれに準ずる)

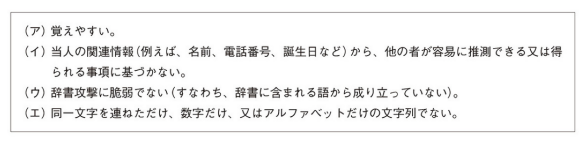


・本体ラベル

　サーバやネットワーク機器本体に貼るラベルも同じように定義する。どこにどんな内容のラベルを貼るかを定義する。

## ４．パスワード

　機器に設定するパスワードも管理設計で定義しておく。どんなに厳重なデータセンターに設置していても、パスワードが「password」だったら意味がない。



## ５．運用管理ネットワーク

　ネットワーク機器の運用管理形態は、ネットワークの配置により「アウトオブバンド(OOB,Out-Of-Band)管理」と「インバンド(Inband)管理」に大別することができる。

・アウトオブバンド管理

　サービスを提供するネットワークとは別に、運用管理をするためだけのTrustedネットワーク(以下、運用管理ネットワーク)を用意する形態。大規模ネットワークでよく採用されている。

最近のネットワーク機器は、サービスを提供するポートとは別に、運用管理を行うための管理ポートを持っている。このポートに運用管理ネットワークのIPアドレスを割り当て、このポート経由でNTPやSNMP、Syslog、GUIアクセス、CLIアクセスなどなど、運用管理に関するトラフィックをやり取りする。

信頼されたネットワークで運用管理するため、運用管理トラフィックに関するセキュリティを考慮する必要がない。その分、信頼できる運用管理ネットワークを別で用意しなくてはいけない。

・インバンド管理

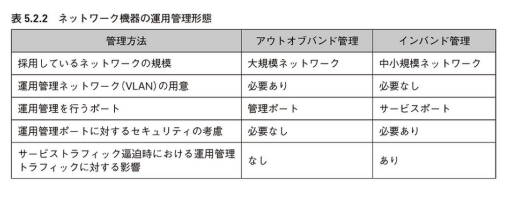
　サービスを提供するネットワークを、運用管理ネットワークとしても使用する形態。

中小規模ネットワークでよく採用されている。

管理ポートを使用せず、サービスを提供するポートを使用して運用管理を行う。

運用管理ネットワークを別に用意する必要がないが、一方でサービストラフィックの逼迫という異常事態が起きるデメリットがある。

また、運用管理トラフィックのためのセキュリティを考慮する必要がある。



## ６．設定情報

　ネットワーク機器の設定情報をどのようにバックアップし、どのようにリストアするかも管理設計の一つ。サーバのバックアップ・リストアには注意を払うのに、ネットワーク機器のバックアップ・リストアにはそこまで注意を払わないことが多いのが現状。

ネットワーク機器の設定情報は、そのシステムの根幹を担うもので、サーバのそれと同じくらい重要。

いつ、どこに、どのように、どうやってバックアップ・リストアしていくか定義する。

・タイミング

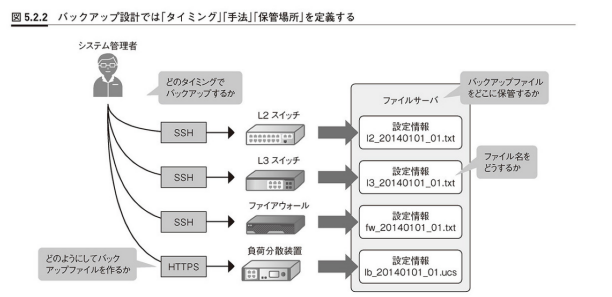
　ネットワーク機器のバックアップは、定期的に取得することは少ない。たいていの場合は、設定変更する前のタイミングで取得する。

・手法

　使用する機器によって異なるが、機器によってはバックアップファイルを作成するためのメニューが用意されている。それぞれの機器において、「どんな情報を取得すべきか」「どのプロトコルでバックアップを取得すべきか」を確認して定義すること。

・保管場所

　バックアップファイルの保管場所も定義しておく。ファイル名称のフォーマットにも注意を払うこと。



リストア

　それぞれの機器でどのような手法でリストアすべきか、また、リストアにはどれくらいの時間がかかるかを確認して定義しておくこと。

機器や設定の量によっては、リストアするより最初から設定しなおしたほうが早いこともある。

そのような機器の場合は例外として定義しておいたほうが良い。

