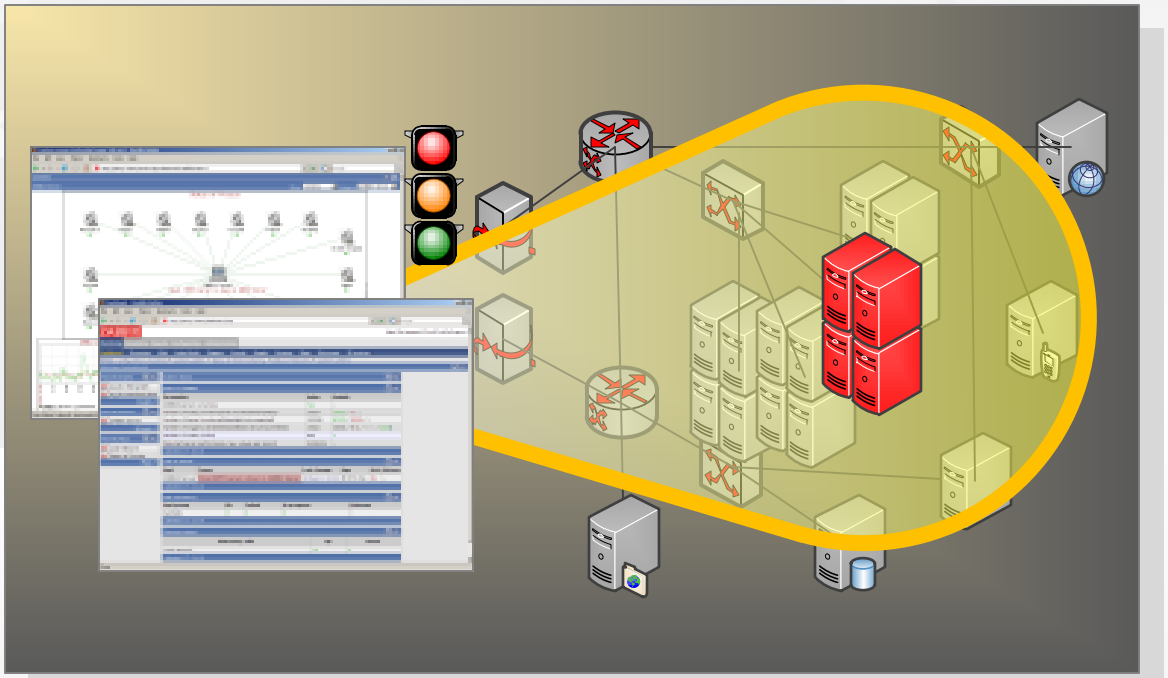
ZABBIX 監視ソフトウェア

~ 『ZABBIX』とは、今、注目されているオープンソース、フリーライセンス(*1)のソフトウェア ~

『商用ソフトとオープンソースソフト』

この違いは多々あります。
ただ、それは不変のものではなく、かつてサポートのなかったオープンソースの世界で、サポート浸透してきたように今後も、この違いはなくなっていくでしょう。



『監視ソフトウェアで重要なことは』

監視ソフトウェアは、その機能、安定性も重要ですが、いまだ標準化しきれない多機種、多OSの中で如何に柔軟に対応し、あるべき監視へ導けるかが、最重要と考えます。
「どのように監視するのか」ではなく、
「今、この状況を把握できているのか」
が重要なのです。
だからこそ、カスタマイズ性の高いソフトウェアが求められます。

注意：本ドキュメントは非公認です。記載内容に対し保障するものではありません。
本ドキュメントは使用者の責任を以って使用して下さい。

(*1) GPLライセンス(GNU GENERAL PUBLIC LICENSE)準拠製品

ZABBIX 監視構成

～『ZABBIX』の監視機能における構成について ～

『監視マスタの構成』

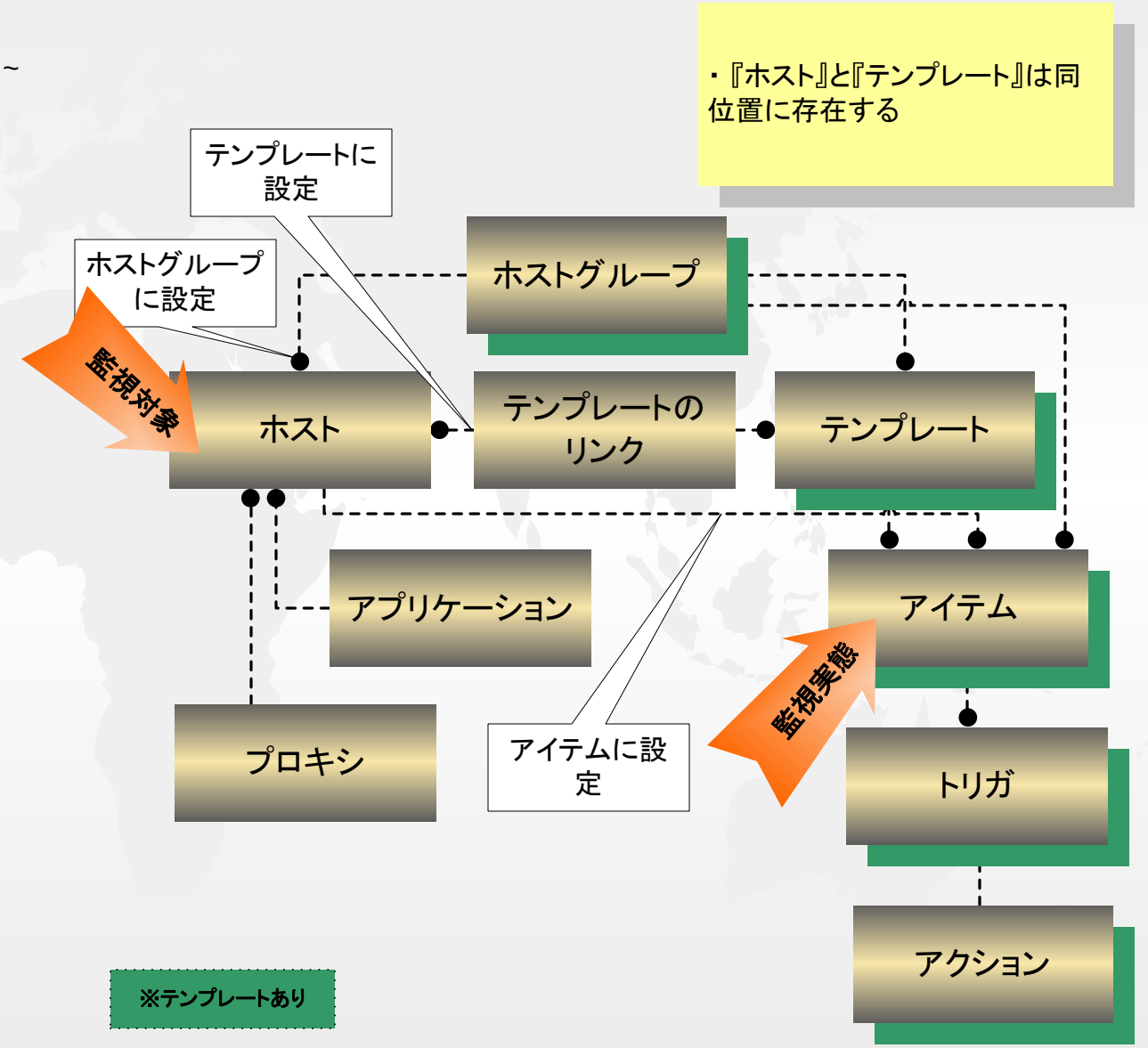
右記は、監視に関わるマスタ構成図です。
これはシステムからみた構成で、実運用上では、これをベースに拠点やサービス体系に合わせて構成します。

監視するには『ホスト』(監視対象)と『アイテム』(監視実態)が、最低限必要になります。
連携には下記のようにいくつか方法があります。

① ホストとアイテムを直接する連携する方法
② ホストとテンプレートを連携する方法
③ ホストグループに所属させる方法

他のマスタは任意(またはデフォルト)に設定します。

また、『トリガ』、『アクション』は通知機能で使用するマスタで、『アイテム』の実行結果から呼び出されます。これには『ユーザ』や、『メディア』というマスタを連携させる必要があり、後述します。



ZABBIX 監視構成

～『ZABBIX』の監視機能における構成について ～

下表に各マスタの概要を記載します。

マスタ	関連付け	複製・テンプレート	内容
ホスト	ホストグループ	あり ・ ―	監視対象のサーバ、ネットワーク機器を設定する
テンプレート	ホストグループ	あり ・ あり	アイテムを機種毎に分類したホストのテンプレート
プロキシ	ホスト	あり ・ ―	ホストを管理する監視サーバ（複数サーバ使用時）
ホストグループ	ホスト	あり ・ あり	ホストの分類分け
テンプレートのリンク	ホスト	― ・ ―	ホストとテンプレートの紐付
アプリケーション	ホスト	― ・ ―	
アイテム	ホストグループ、ホスト	あり ・ あり	監視方法（ping、リソース、接続監視）を設定する
トリガ	ホスト、アイテム	あり ・ あり	検知条件を設定する
アクション	（全てのトリガ）	― ・ ―	通知方法を設定する

【補足】

・『関連付け』 ・・・ 親マスタとして自身が所属する分類を設定します

・『複製』 ・・・ 自分自身を複製する機能があるか、否かを記載しています

・『テンプレート』 ・・・事前にテンプレートとして用意されているか否かを記載しています

ZABBIX 構築概要

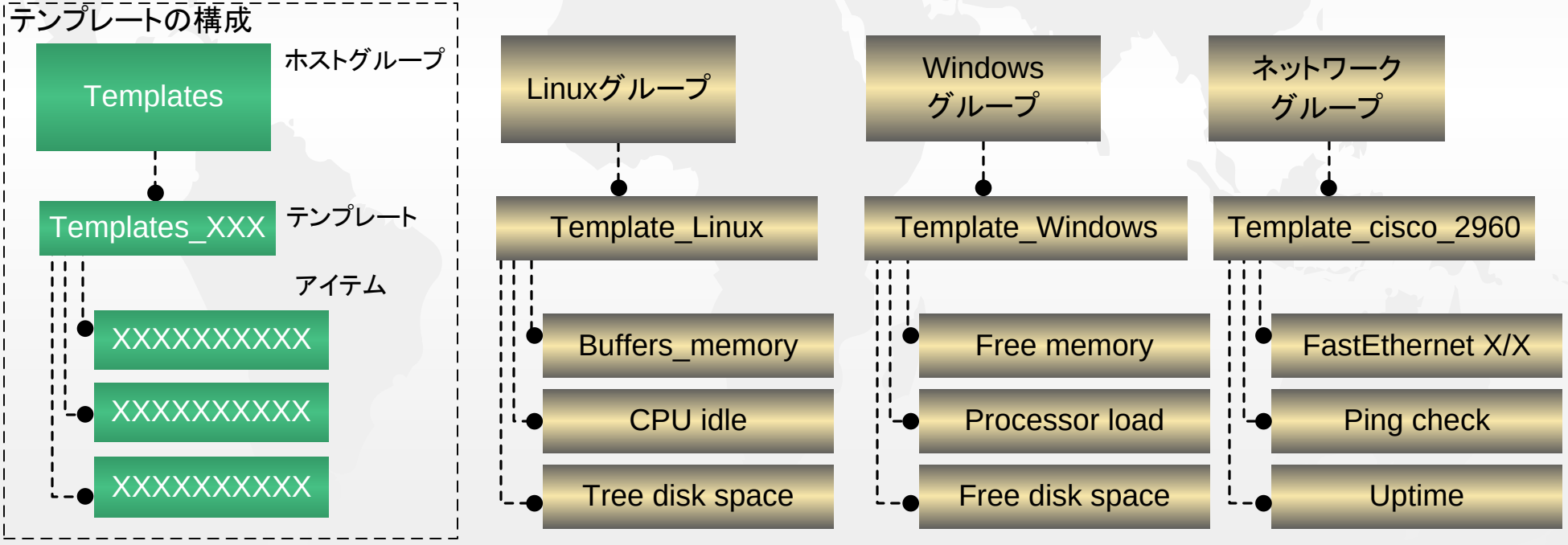
～『ZABBIX』の構築において最初に考えること ～

・機種毎に分類するのか、拠点で分類するのか、サービス毎に分類するのか。

・何で分類するのかが重要

『ZABBIX構成と運用構成』

テンプレートの構成を考慮すると、下記のように機種毎の構成になります。
ご覧のとおり、全ての機器が頭の中に入る規模であれば、構築には一番早い方法です。
ただし、障害を検知した場合にその機器の名前から重要性や、設置、構成上の位置を把握している必要があります。

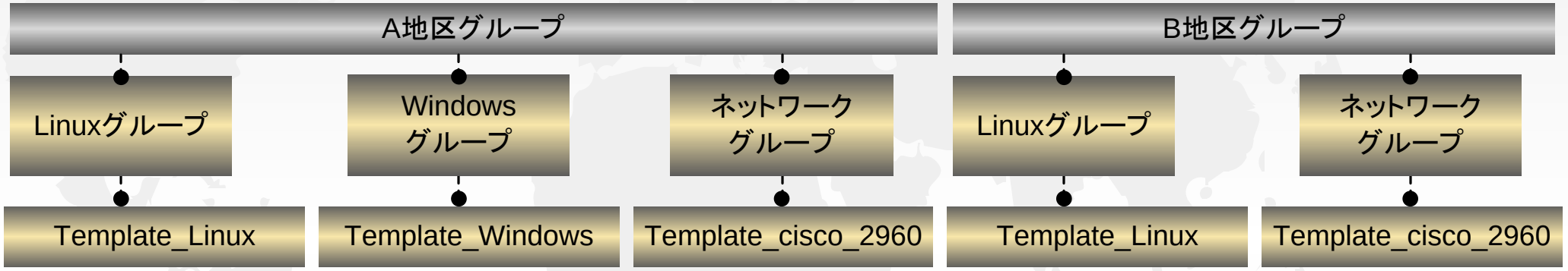


ZABBIX 構築概要

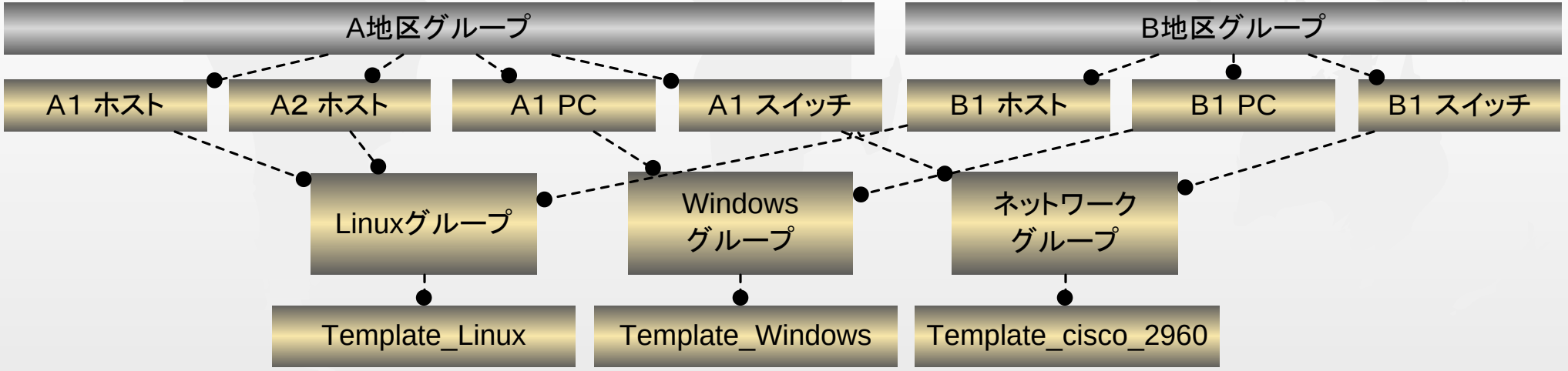
～『ZABBIX』の構築において最初に考えること ～

・どのように構成するか
・重複設定をどこまで許すのか

実際は下記のように機種以外に分けるなど、管理面を考慮した構成が必要です。



地区のみをグループ管理するのであれば、下記のようにホスト（サーバ、NW機器）とグループにします。



ZABBIX 構築概要

～『ZABBIX』の構築において最初に考えること ～

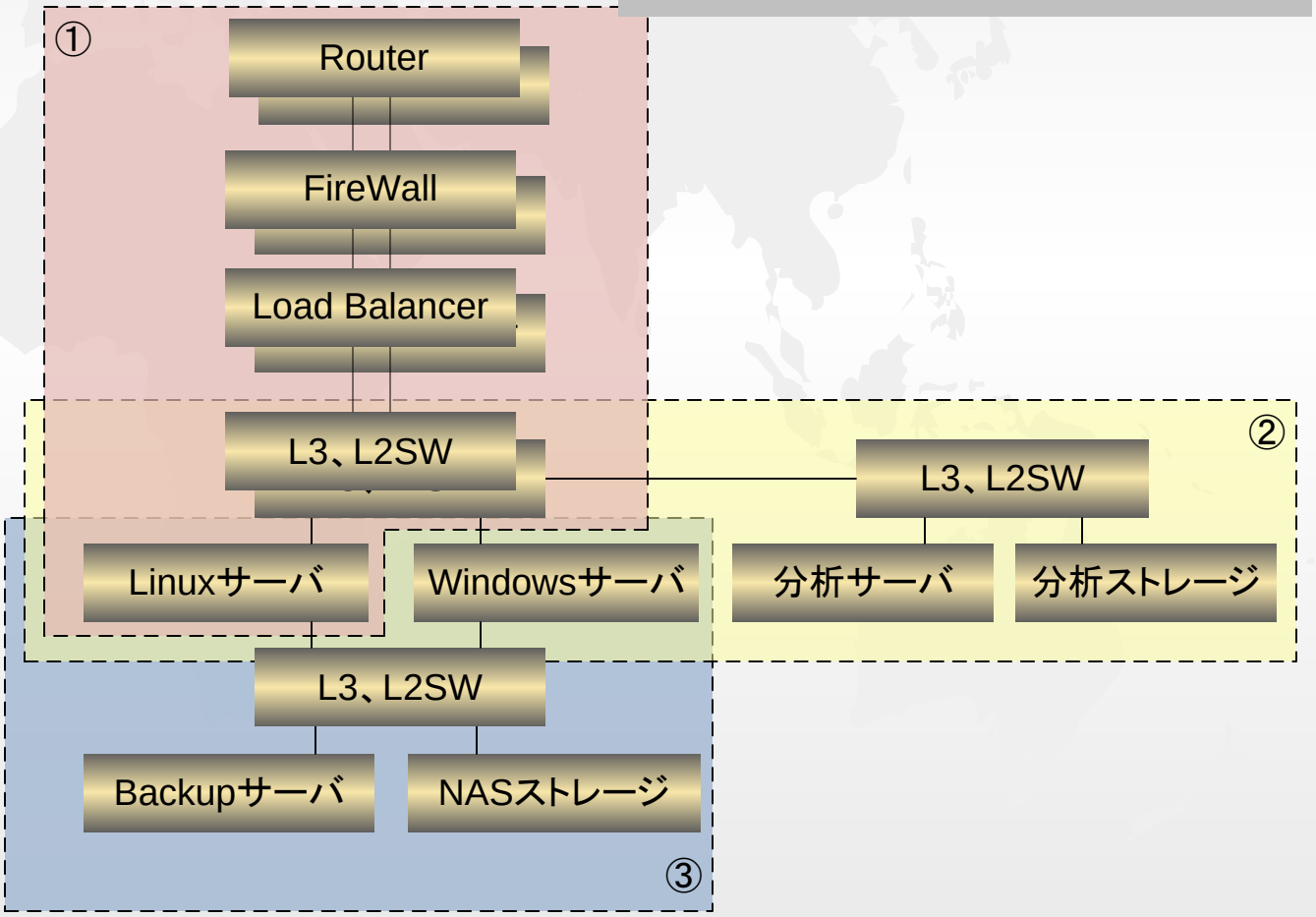
・設計では、『ホストグループ』が重要
・ホストグループからホストを容易に確認できる
・ホストからホストグループは容易に確認できない
※ホストグループへの不用意なホストの重複設定は避ける
・機器の重要度、緊急度を把握する

中規模システムでは、機器連携を管理する局面があります。
一覧機能は一つのホストグループに関連するアイテム状況を確認する事ができます。

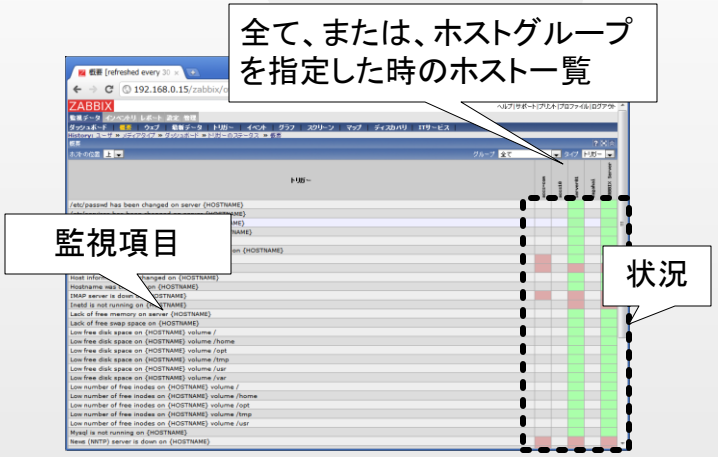
この機能を利用すると、右記のようにシステムグループに分けて管理する事ができます。

① WEBサービスグループ
② 分析システムグループ
③ バックアップグループ

※グループへのホストの重複設定は可能。



下記は、ZABBIXの『監視データ』『概要』画面。
ホストグループ毎に全監視項目の状況を確認します。



ZABBIX 監視設計

～ 監視項目の選定と実装方針 ～

・システム構成を踏まえた重要性、緊急性を把握する事が重要
・重要性、緊急性が通知機能に備わっているか重要

『監視とは』

テンプレートは機器に対し提供できうる監視項目が記載されています。
テンプレートに記載している全ての監視項目を採用する事は容易ですが、重要性、緊急性に関しては構築者が決めなくてなりません。

重要性は、下記のように定義する事ができます。

重要性	定義
大	サービスに影響がでている状態
中	現在は大丈夫だが、放置するとサービスに影響がでてくる状態
小	半年後、1年後の状況予測の材料として必要な項目

緊急性は、下記のように定義する事ができます。

緊急性	定義
大	問題に対し即時に対応する必要がある状態
中	回避されているが、再発の可能性が残る状態
小	単発発生で、対応の必要性はないが警戒しておく必要がある状態

結局のところ、どれも重要であることは変わらず、システム担当がどのペースで対応しなくてはならないかの指標になります。
重要性、緊急性はシステムの冗長性、人員体制、保守契約内容など監視以外の要素が絡んできます。
監視システムは、上記を踏まえシステム担当に如何に正確に伝えるかがカギになります。
重要性、緊急性が『大』のものと、『小』のものを同じように伝えると、判断を誤る可能性があります。

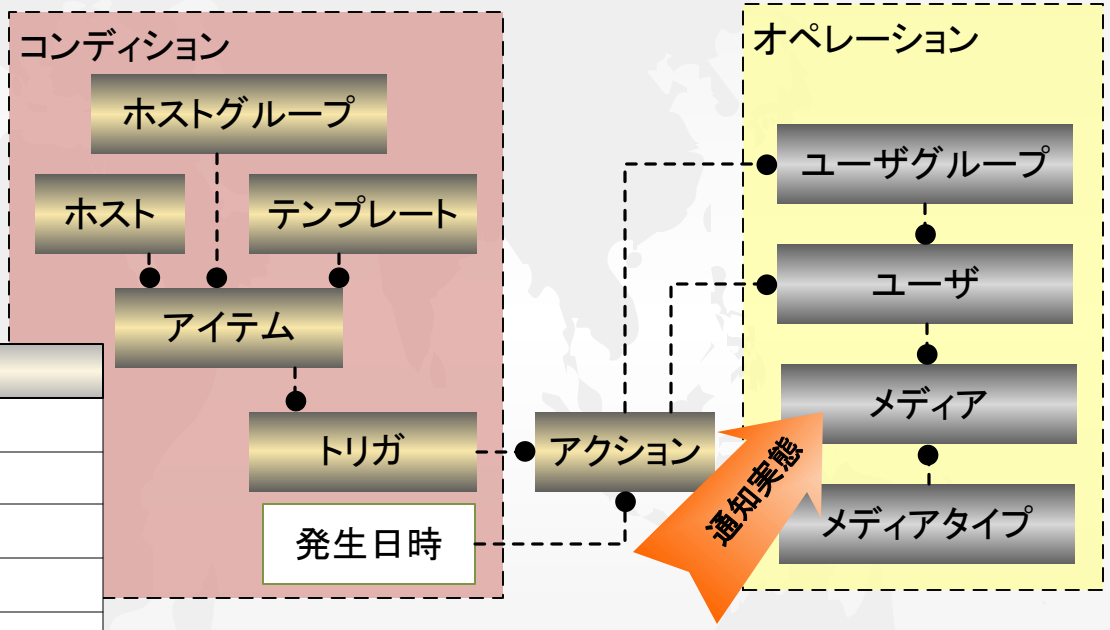
ZABBIX 監視設計

～ 監視項目の選定と実装方針 ～

・通知処理をいくつ用意するか
・トリガの深刻度だけでは状況を正確に伝えられない

『通知処理（アクション）』

ZABBIXの通知機能はアクション設定を行う。
アクションの設定は、下記に分かれる。
・『アクション』 ・・・ メッセージのフォーマットを定義する
・『コンディション』 ・・・ 実行時の状況を定義する
・『オペレーション』 ・・・ 通知方法など処理内容を定義する



『コンディション』、『オペレーション』の設定項目を以下に記載します。

コンディション	条件
ホストグループ	ホストグループを条件にする。
ホストテンプレート	テンプレートを条件にする。
ホスト	ホストを条件にする。
トリガー	トリガーを条件にする。
トリガーの名前	トリガーの名前を条件にする。
トリガーの深刻度	トリガーに設定した深刻度を条件にする。
トリガーの値	トリガーに設定した値(アイテム実行結果)を条件にする。
期間	対象、除外期間を指定する。

オペレーション	処理内容
メッセージの送信	メール、トラップ通知を行う。
リモートコマンド	ZABBIXに対するコマンドを実行する。

ZABBIX 監視設計

～ 監視項目の選定と実装方針 ～

・ホストグループの構成を考慮する事でシステム担当者は正しい重要度、緊急度で対応する。

『監視分類と監視項目について』

仕組み以上に設計において、考慮しなくてはならない事は何を監視するかです。

分類	重要度	緊急度	内容
異常監視	大	中	ハード、ミドル、アプリケーションと何れの場合でも、その異常通知が最も重要である。自らが異常を検知しているのに監視できていないのは危険である。 トラップ監視や、ログ監視が該当する。
予防監視	中	小	増え続けるデータ、トラフィック、CPU使用率など1ヶ月後、半年後に起きる事態に事前に対応する事が重要である。 リソース監視が該当する。 ※ 突発的なリソースの枯渇（ディスクフル、CPU 100%など)は、ミドルやアプリケーションの暴走が考えられ、異常監視で検知すべきである。
正常性監視	小	大	システムを使用していれば、正常か異常かは気づく内容である。利用者より前に気づく必要がある項目で、他の項目からすると重要度は低くても、緊急度は高い。 問題箇所の特定である視覚性が重要になる。 また、メンテナンス作業からサービス開始する際のチェック項目としても重要である。 死活監視、接続監視、トラップ監視（復帰）、ログ監視（復帰）が該当する。

※ 監視ソフトウェアでの異常監視は不得意分野と言えます。異常は検知できても、正常復帰するには機器や、ミドル、アプリケーション側のトラップ、ログ出力機能に委ねられています。
　現状では復帰操作をシステム担当がマニュアル操作で行う。また、その操作を考慮した設定内容が必要になり、構築コストが増えます。

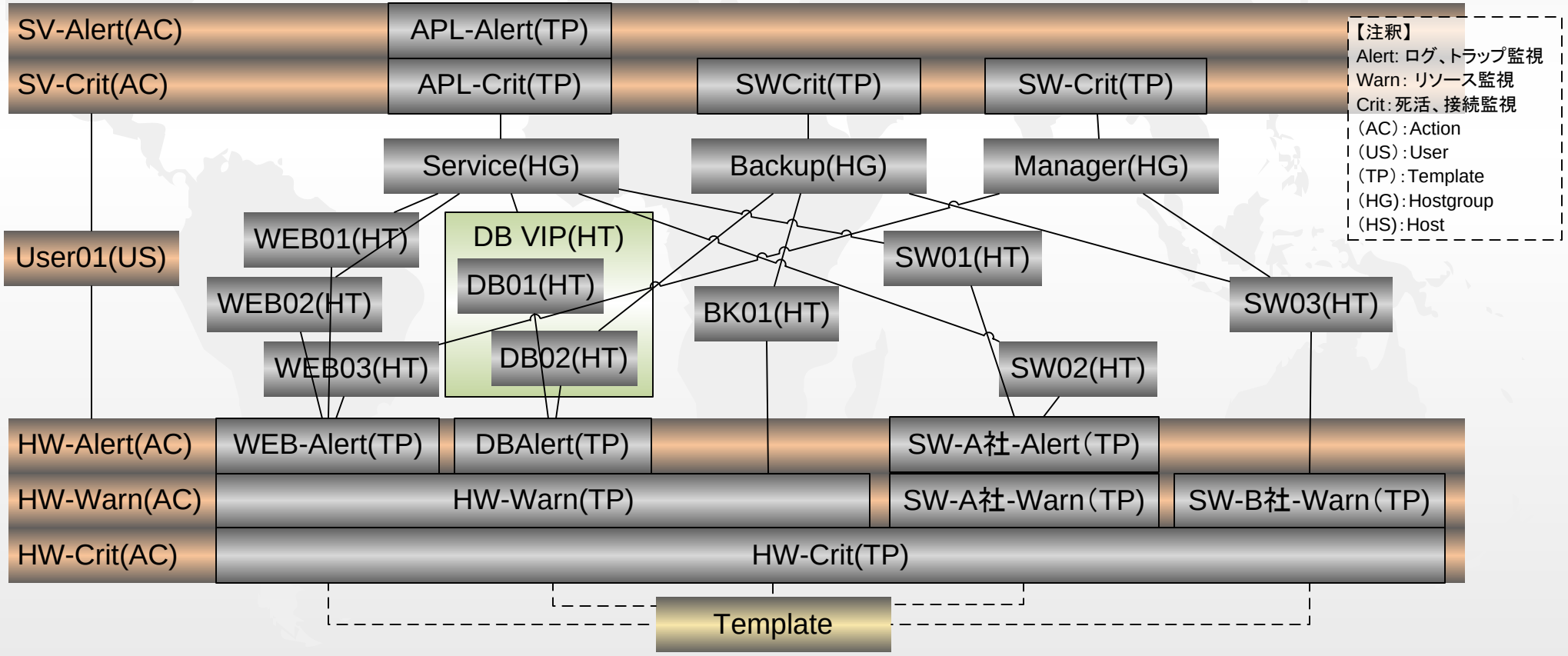
ZABBIX 監視設計

～ 監視項目の選定と実装方針 ～

・Templateを参考に重要度、緊急度、機器に合わせたテンプレートを作成する。
・重要度、緊急度に合った通知処理(Action)を設定する。
・冗長構成の有無で、重要度(SV-Alert or HW-Alert)が決まる。

『監視分類と監視項目について』

監視分類(重要度、緊急度)を考慮した場合の各マスタの構成例です。
『SV-Alert』を検知した場合、『Service(HG)』の監視概要から、関連ホストの全監視項目(Item)を確認します。



ZABBIX 最後に

～ 監視概要と詳細設計、構築 ～

『監視概要』

ZABBIXは操作性を重視している為、各マスタの連携が画面からは分かりづらいものになっています。
本書は、マスタ関連を明確にし、実運用に合わせた構成を記載しました。
監視構成は、システム規模、運用担当者の人数、役割分担により、変わってきます。例えば、HW監視は監視担当者が行い、サービス監視は各システムの担当者が行うなどで、通知やユーザ管理の方法が変わってきます。
今回は小、中規模のシステムをターゲットに記載しています。

『詳細設計、構築』

ZABBIXの詳細ドキュメントは公開されていますので、本書では触れていません。
各監視項目（アイテム）は、ハードウェアに依存しているのも監視システムとして悩ましい課題です。
ログ監視とログファイルのローテート機能といったOSとの連携の課題や、NW機器のSNMP監視において標準MIBが使えないという課題があります。ZABBIXでは多くのテンプレートを提供する事で、改善しようとしています。

現状ではまだ、正しい状況を把握するにはメーカーサポートとの間で時間を要する状況があります。これらはZABBIXに関わらず全ての監視ソフトウェア VS 機器メーカーの課題です。

監視の構築には、サーバ、ネットワーク、ミドルウェア、アプリケーション、そして運用経験と仕組み以上に多岐に渡ったスキルが必要です。
非生産分野の監視システムは安価を求められますが、正常運用に持っていくには、どうしてもコストと時間がかかります。
監視されていなかった（あるいは、通知を見逃した）というのが一番致命的であり、運用担当や企業における損失は計り知れません。
次回は、必要最低限の監視項目に関して執筆しますが、監視項目数が増えると見逃す可能性が高くなります。まずは概要設計として絞り込み、それから見逃してはいけない監視項目を増やす事が大切です。

最後にコストの厳しい昨今ではありますが、あらゆる企業様において、安定したサービス提供の一助になりましたら幸いです。