

株式会社エクストランス

X-MON3

入門リファレンス


## まえがき

本書は X-MON3 系列を用いて監視を実施する入門リファレンスとなっております。

そのため、基本的な OS や GUI の一般的な操作、用語などについては知識をご理解の上でお読みください。

また、X-MON の操作画面はお使いの OS やブラウザによって異なる場合がございます。

本書については章立てで下記のようになっています。

- 
- 1章 ～ 7章 監視・X-MONの基礎解説
  - 8章 ～ 9章 サンプルを使用した監視設定解説
  - 10章～11章 管理画面の解説

監視の基礎、X-MON についての解説をご覧になる方は 1 章から、監視の基礎を理解している方は 8 章のサンプルを使用した監視設定解説からご覧頂ければ幸いです。

・ 本書における解説環境

X-MON ver 3.10.0

本書以外のマニュアルについては X-MON サポートページにログインしてご確認ください。

<https://x-mon.jp/support/>

改訂履歴	
2012 年 10 月	初版
2020 年 01 月	第五版

Copyright © 2004 X-TRANS, Inc. All Rights Reserved.

## 内容

---

まえがき .....	1
1 はじめに ～X-MON と Nagios について～ .....	4
1.1 Nagios とは？ .....	4
2 監視概念.....	5
2.1 Core.....	5
2.2 プラグイン.....	5
2.3 アドオン.....	5
2.4 ホストとサービス .....	5
3 監視とは？ .....	6
3.1 死活・稼働監視.....	7
3.2 リソース監視.....	7
3.3 性能監視.....	8
3.4 セキュリティ監視 .....	9
4 監視の機能.....	10
4.1 しきい値.....	10
4.2 アクティブチェック .....	11
4.3 オンデマンドホストチェック.....	11
4.4 パッシブチェック .....	12
4.5 パフォーマンスデータ .....	13
5 監視ステータス .....	14
5.1 soft 状態と hard 状態 .....	14
5.2 ホストのステータス .....	16
5.3 サービスのステータス .....	16
6 通知機能.....	17
6.1 通知の文章.....	19
7 その他の設定項目 .....	21
7.1 分散監視.....	21
7.2 警告灯管理.....	21
7.3 Syslog 管理.....	21

7.4	構成管理.....	22
8	サンプルネットワークを使った監視.....	23
8.1	監視対象を決める.....	24
8.2	監視内容を決める.....	24
8.3	ホストの監視設定をする.....	25
8.4	サービスの監視設定をする.....	31
8.5	時刻の設定.....	38
9	通知設定.....	40
10	X-MON の画面とそのほかの機能について.....	41
10.1	ダッシュボード画面.....	41
10.2	監視概要画面.....	44
10.3	未処理の障害画面.....	45
10.3.1	認知済みとは.....	45
10.3.2	ダウンタイムとは.....	46
10.4	ダウンタイム画面.....	48
10.4.1	ダウンタイムの定期設定.....	50
10.5	グラフ画面.....	52
10.6	稼働率画面.....	53
10.7	ホストの一括登録.....	54
11	X-MON のデフォルトの監視項目.....	57
12	さいごに.....	60

## 1 はじめに ～X-MON と Nagios について～

---

X-MON は総合監視ソフトですがオープンソースソフトウェアである Nagios をベースに開発されました。そのため、X-MON では Nagios の概念や仕様、用語を使用している部分が多くあります。

本リファレンスでは機能部分を中心に、サンプルネットワークを使用して監視サンプルを作成し、X-MON で使用されている Nagios 部分について解説していきます。

### 1.1 Nagios とは？

Nagios は Ethan Galstad 氏により 1998 年ごろから NetSaint という名称で開発が始められた、サーバやネットワークの総合監視ツールです。

オープンソースソフトウェアで開発が進められ、現在も 100 人を超すエンジニアが開発に携わっています。

また、アドオンやプラグインもエンジニアにより開発、公開され世界中で幅広く使用されています。

Nagios の詳細については Nagios の Web サイトをご参照ください。

<https://www.nagios.org/>

## 2 監視概念

---

Nagios での監視概念を X-MON でも実装しています。

### 2.1 Core

監視の中核部分にあたります。

監視のスケジューリングや監視の結果を処理する本体部分です。

2019 年 9 月時点での最新バージョンである X-MON3.9.0 では Nagios Core 4.2.4 が採用されています。

### 2.2 プラグイン

Core 自身は監視を実施する機能は備わっておりません。

監視スケジュールに従って Core がプラグインを呼び出し、プラグインがチェック（監視の実施）を行います。監視設定されているしきい値やオプションに従い、異常であるか正常であるかを判断し、Core へ結果を送ります。

X-MON では Nagios 独自のプラグインを Web インタフェース上で簡単に設定できるように実装しています。

### 2.3 アドオン

アドオンとは Nagios にはない機能を実装するためのプログラムです。

X-MON ではサーバのリソース監視で使用する NRPE やグラフを作成するための RRDTool、SNMP TRAP を受け取るための snmpttなどをアドオンとして実装しています。

### 2.4 ホストとサービス

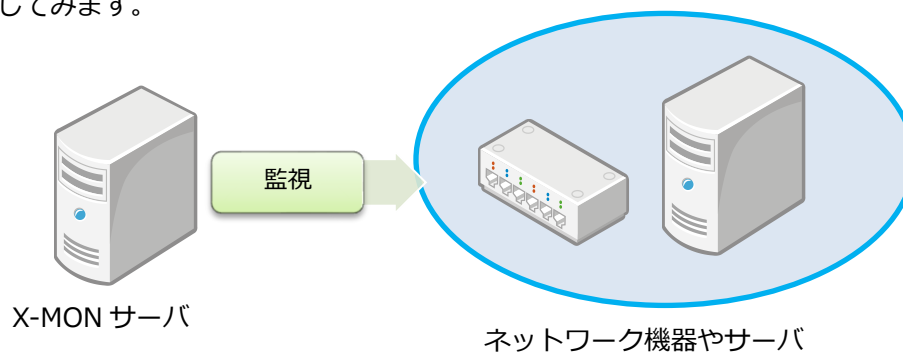
Nagios で使用している用語を X-MON でも多く使用していますが、まず「監視をされる機器」の事を「ホスト」といいます。ネットワーク機器やサーバに限らず、監視に設定されている機器を指します。そのホストで稼働している Web アプリケーションやデータベースなど、サービスを提供しているものを「サービス」といいます。

その他の用語については章ごとに説明を加えていきます。

### 3 監視とは？

X-MON は「監視」をするためのソフトです。

「監視」とは携わる人によって印象は様々ですが、本リファレンスでは、監視とは  
「サーバやネットワークにおいて障害が発生しないように、システムも含めて正常に稼働している事を確認する」  
という定義をしてみます。



すると、監視する対象の機器やシステムの内容によりさまざまなタイプが出てきます。  
それぞれの対応に分けて監視のタイプを整理してみます。

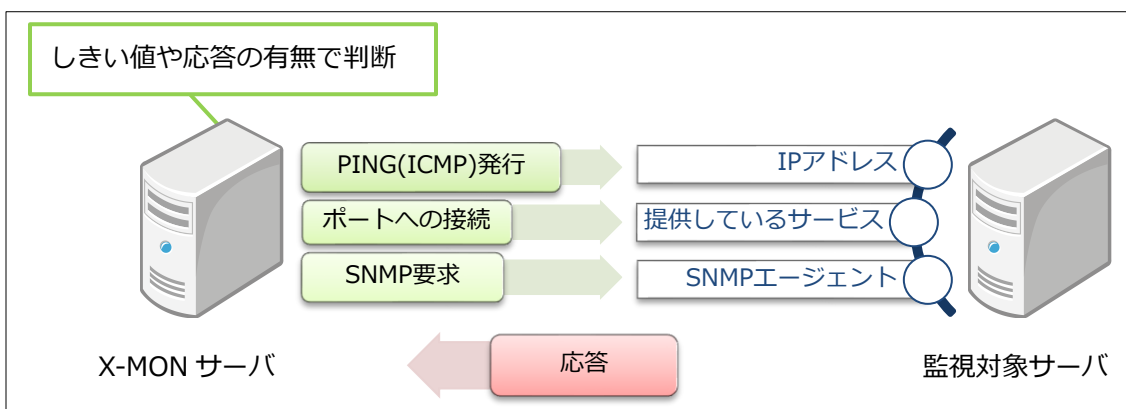
死活・稼働監視	ネットワーク、サービスの応答があるかの監視
リソース監視	ディスク、CPU、メモリ、ネットワーク帯域などのハードウェア上のリソースの稼働状況、利用状況の監視やハードウェアそのもののエラーやシステムエラーの監視
性能監視	ネットワークのパフォーマンス、サービスの応答時間の監視
セキュリティ監視	ネットワークやサービスのセキュリティに関する検知をする監視

### 3.1 死活・稼働監視

一般的に死活・稼働監視は機器が正常に稼働しているかどうかを、ping コマンドにて応答があるかを判断する、もしくは特定のサービスを提供しているポートへの応答があるかどうかを判断する事により実現します。

また、SNMP エージェントを使用し、異常が発生した場合は SNMP TRAP を X-MON へ通知し、判断する事も出来ます。

図 死活・稼働監視



### 3.2 リソース監視

サーバ機器の場合、サーバへログインして内部でリソースを確認するコマンドを発行し確認する事が出来ます。

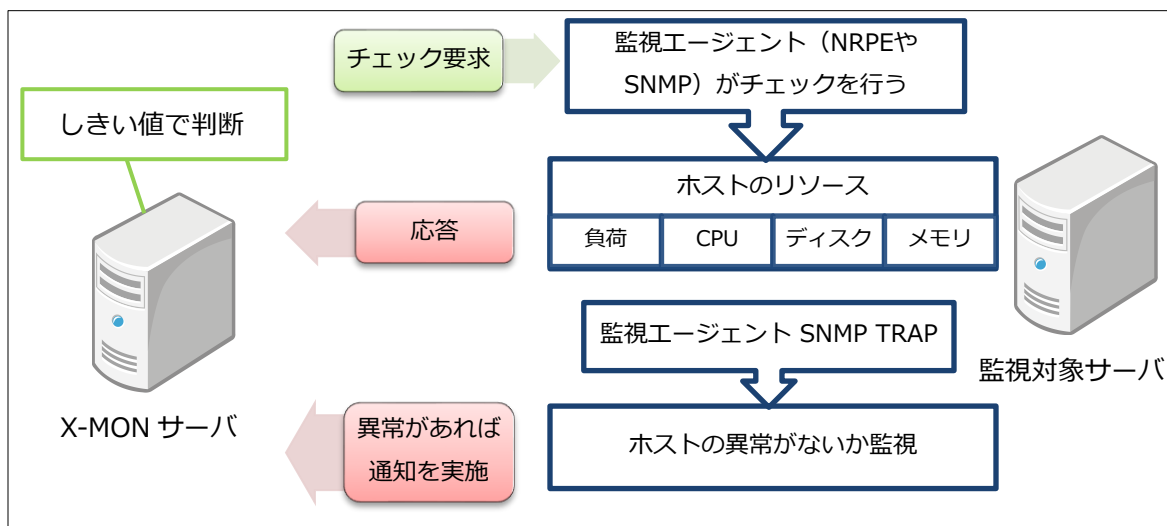
X-MON では監視エージェントである NRPE もしくは SNMP を使用する事により監視エージェントからリソース確認の結果を受け取り、判断する事が出来ます。

異常が発生した際に通知を実施する SNMP エージェントもネットワーク機器やシステムエラーの通知を行うので判断材料となります。

また Windows サーバの場合は WMI 機能や NSClient++ エージェントにて判断する事が出来ます。



図 リソース監視

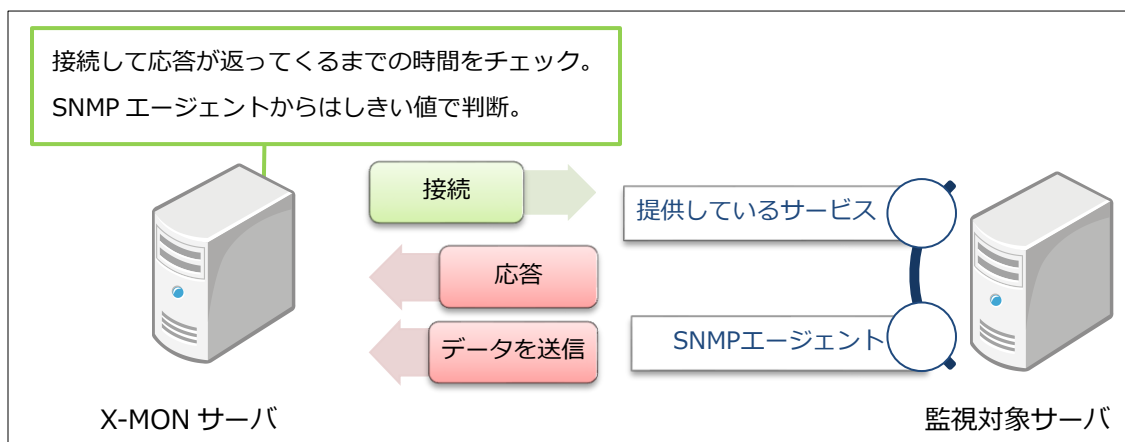


### 3.3 性能監視

性能監視とリソース監視の違いは、性能監視はサービスの提供に対する応答時間（レスポンスタイム）が一番の判断材料となります。提供しているサービスが Web サービスの場合は、Web サービスに接続し、リクエストを送った結果が返ってくるまでの時間となります。

また、データベースへの接続する応答時間やネットワークの帯域の使用率も性能監視となります。

図 性能監視

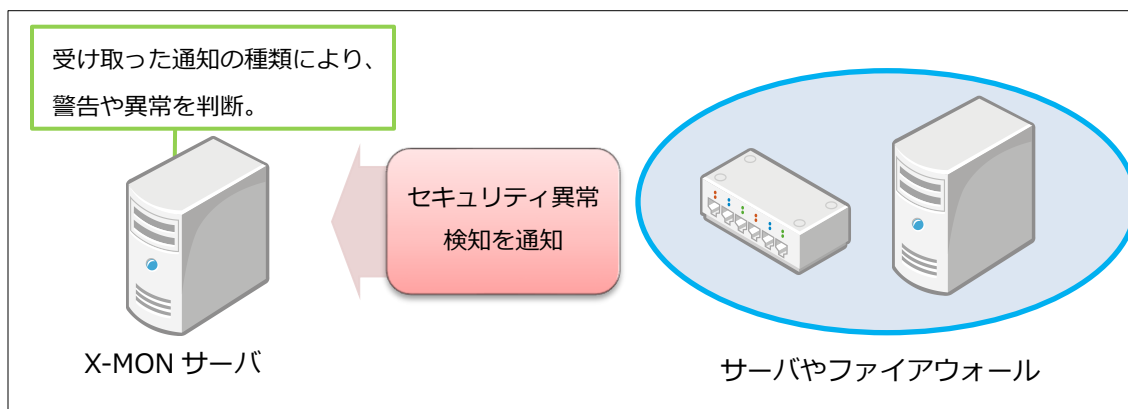


### 3.4 セキュリティ監視

ファイアウォール機器などにてセキュリティの異常が発生した場合、SNMP TRAP の機能により X-MON へ通知を行い、判断する事が出来ます。

その他サーバ機器ではログ監視を実施し、特定のイベントや文字列がログに発生した場合を異常とする設定にしておけば X-MON にて検知し、セキュリティ異常を早急に対応する事が出来ます。

図 セキュリティ監視



文頭でも述べましたが X-MON は「監視」ソフトウェアですが「総合監視」というのが正しいでしょうか。

上記のような監視もできれば、監視の結果をグラフで表示したり、レポートに出力したり、性能の分析や異常の前兆についても分析する事が出来ます。

本リファレンスでは「入門」という事ですので、「監視入門」として次章より解説を行います。

## 4 監視の機能

概念をご理解いただいたうえで、監視の機能に関する解説を行います。

### 4.1 しきい値

しきい値とは、サービスが正常に稼働しているかの判断に用いる値です。

あらかじめ設定しておき、監視チェックの結果と比較、正常・警告・異常を判断します。

Nagios の概念を引き継いでいる X-MON では以下の様に表記されます。

図 警告 WARNING (黄色)

ホストID (ホスト名称)	サービスID	監視ステータス	最終チェック時刻	経過時間	試行回数	ステータス情報
server1 (server1)	HTTP	WARNING	2019-09-19 13:26:22	0日と00時間00分02秒	1/3	HTTP WARNING: HTTP/1.1 403 Forbidden - 5237 bytes in 0.010 second response time

図 異常 CRITICAL (赤色)

ホストID (ホスト名称)	サービスID	監視ステータス	最終チェック時刻	経過時間	試行回数	ステータス情報
server1 (server1)	HTTP	CRITICAL	2019-09-19 13:27:46	0日と00時間00分12秒	2/3	接続を拒否されました

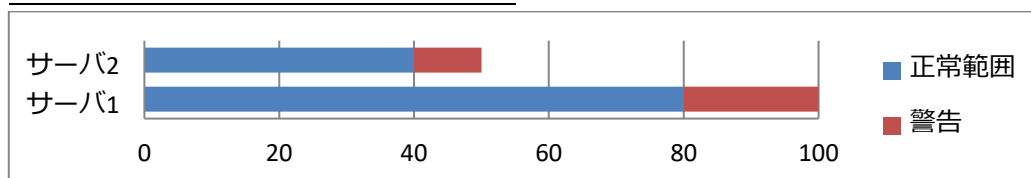
例としては Web サーバの監視にて、「HTTP のレスポンスが 5 秒以上かかっているなら異常である」や、リソース監視にて「ディスクの使用率が 80%を超えると警告、90%で異常」という形があります。

また、しきい値は監視条件やサーバ条件によって適切に設定する必要があります。

例えば、ディスク容量が 50G のサーバと 100G のサーバとでは、「使用率が 80%で警告」と同じ設定をしても残りの容量が異なります。

図 サーバ 2 は 50G の容量、サーバ 1 は 100G の容量。しきい値はともに 80%。

警告が発生する残り容量に差が出てくる。



## 4.2 アクティブチェック

アクティブチェックとは、X-MON が監視のスケジュールに従って監視プラグインを呼び出し、監視を実施して結果を処理します。

「通常の監視方法」と認識して頂ければと思います。

## 4.3 オンデマンドホストチェック

X-MON ではホストの監視と、HTTP や FTP などサービス監視の 2 種類があります。ホストの監視では主に ping コマンドを使用したホストの死活監視を実施します。

サービスの監視では HTTP のレスポンス監視や SMTP のポートが開いているかなどサービスが提供されているかの監視を行います。

これは Nagios からの監視の概念になるのですが、

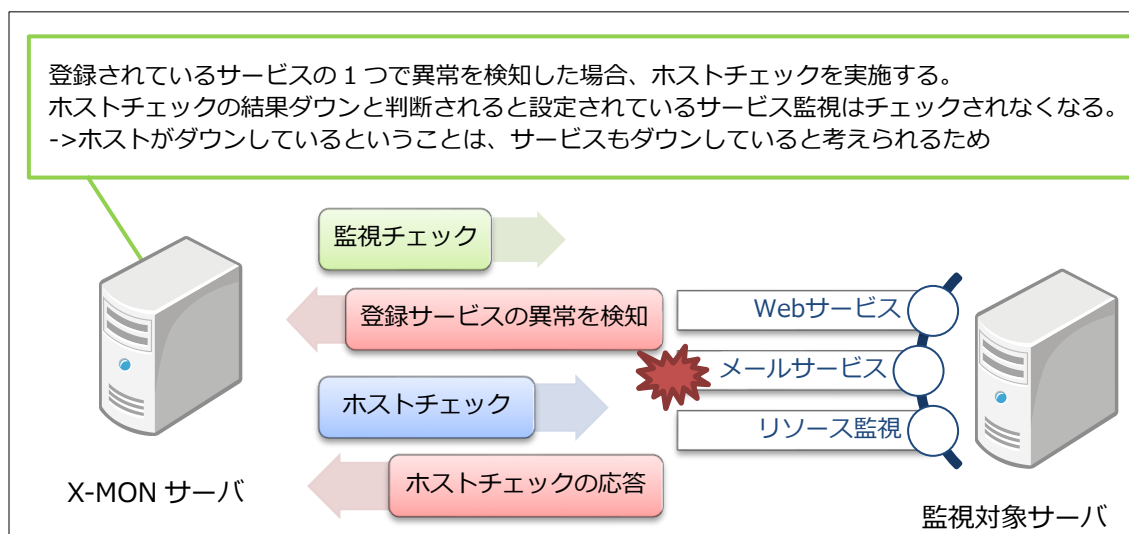
「サービスが正常に稼働しているホストはダウンしている状態とは通常考えにくい」というのがあるため、ホストの死活監視はそのホストに登録されているサービス監視の 1 つが異常

(CRITICAL) を検知した場合にのみ実施するという機能があります。

これをオンデマンドホストチェックといいます。

X-MON においては、デフォルトがオンデマンドホストチェックとなっております。

図 オンデマンドホストチェック



#### 4.4 パッシブチェック

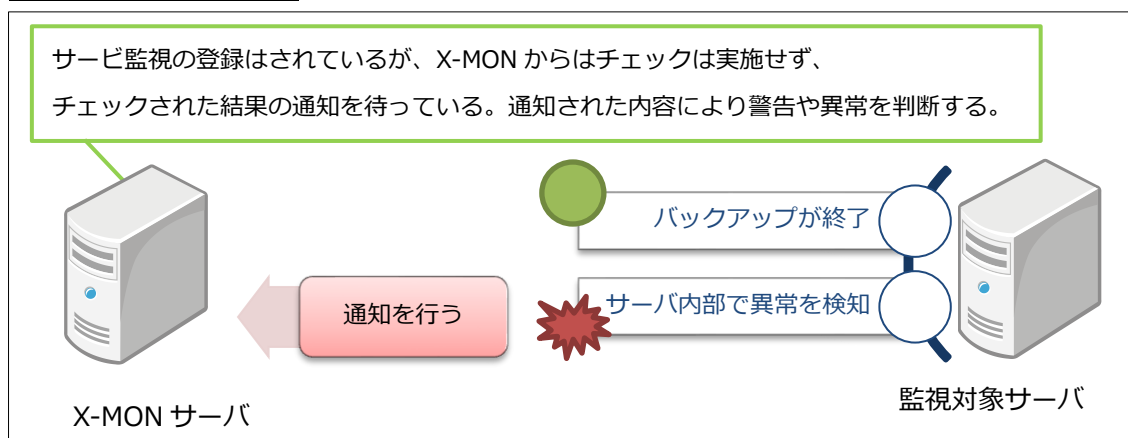
パッシブチェックはアクティブチェックとは逆に、X-MON 以外のソフトウェアやハードウェアが監視タイミングを制御し、結果を X-MON へ送る方法です。言い換えるとパッシブチェックは、監視結果の通知を待っている、という状態です。

Nagios では、Cron ジョブで登録されたジョブの実行結果を送ったりするのに使用されています。

X-MON では、例えばバックアップソフトが一日一回のバックアップ終了時に結果を SNMP TRAP で X-MON へ通知するよう設定をすれば、通知された SNMP TRAP の種類により正常である、異常であると結果を判断する事が出来ます。

その他ではファイアウォール機器にて異常を検知し、同じく SNMP TRAP を X-MON へ通知する、という監視も可能です。

図 パッシブチェック 1

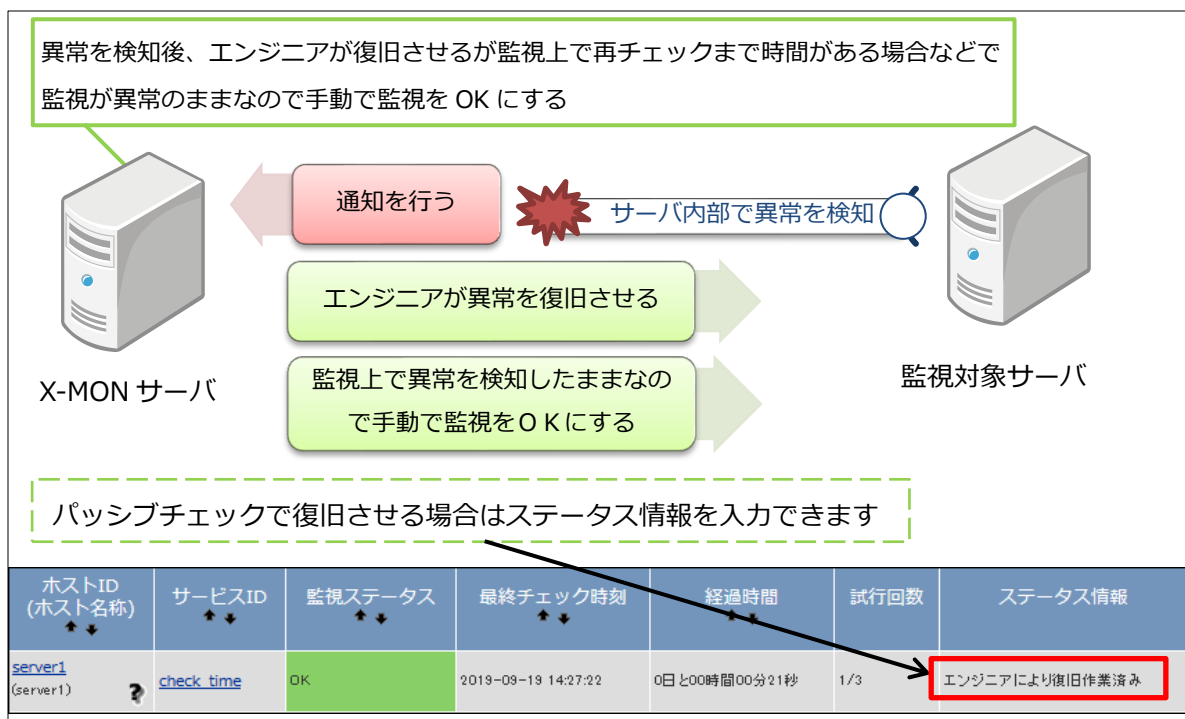


もう一つの機能として手動で監視状態を変更する事が可能です。

例としては、サーバの時刻監視を 1 時間に 1 度実施し、時刻のズレが発生しているため異常を検知しエンジニアがサーバの時刻を修正したとします。

この場合、次の監視チェックが動くまで監視画面上では異常の表示のままになってしまいます。そういった場合に手動でパッシブチェックを送信し、結果（ステータス状態）を変更する事が可能です。監視結果に関しては正常も異常も送信する事が可能です。

図 パッシブチェック 2



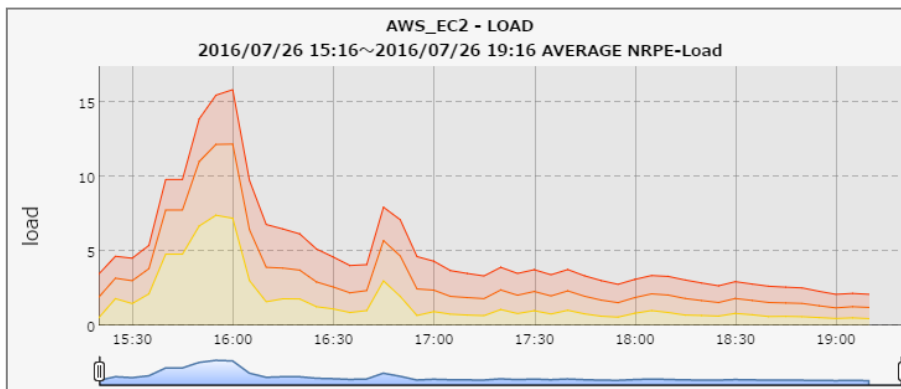
## 4.5 パフォーマンスデータ

パフォーマンスデータとは監視の結果をデータとして別の処理に使用する事です。

例えばディスクの使用率の結果や、インタフェースの帯域の使用率などです。

X-MON では標準でグラフ化のアドオンが搭載されており、多くのパフォーマンスデータをグラフ化する事が可能です。

図 パフォーマンスグラフ



## 5 監視ステータス

監視概念について解説してきましたが、次は監視を実施し、どのような結果（ステータス）になったのかについて解説していきます。

### 5.1 soft 状態と hard 状態

この状態変化についても Nagios から引き継いで X-MON でも採用されているものの一つです。

「監視を行った結果が一時的なエラーや誤認識によるエラーの可能性がある」という概念に基づいています。

監視結果で警告・異常を検知した場合は、まず soft 状態となります。

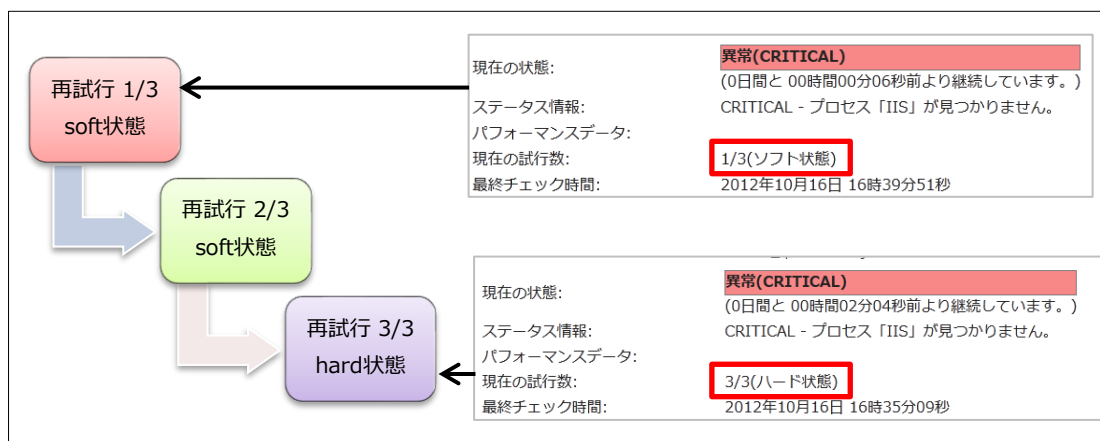
この状態では、通知機能を使用している場合はまだ通知もされず、「本当に障害が発生しているかを確認している状態」と認識して頂ければと思います。

確認している状態の時は、監視設定で再試行回数というのが設定されていますのでその回数分、監視が実施され、結果それでも警告・異常の場合はエラーとなり、hard 状態となります。

hard 状態になると通知も実施されます。

逆に、何度も soft 状態での検知を繰り返すサービスなどがあれば、不安定な状態であるとも言えますので、障害が発生する前に予防保守を実施するよう考慮する必要も出てくる事でしょう。

図 soft 状態と hard 状態の遷移



### 監視間隔と再試行間隔・回数について

ステータスの変化の上で、監視間隔と再試行回数の関係について理解する必要があります。

監視間隔はアクティブチェックの監視間隔となります。アクティブチェックで異常を検知した場合、設定している再試行回数分の監視が、再試行間隔を空けて実施されます。

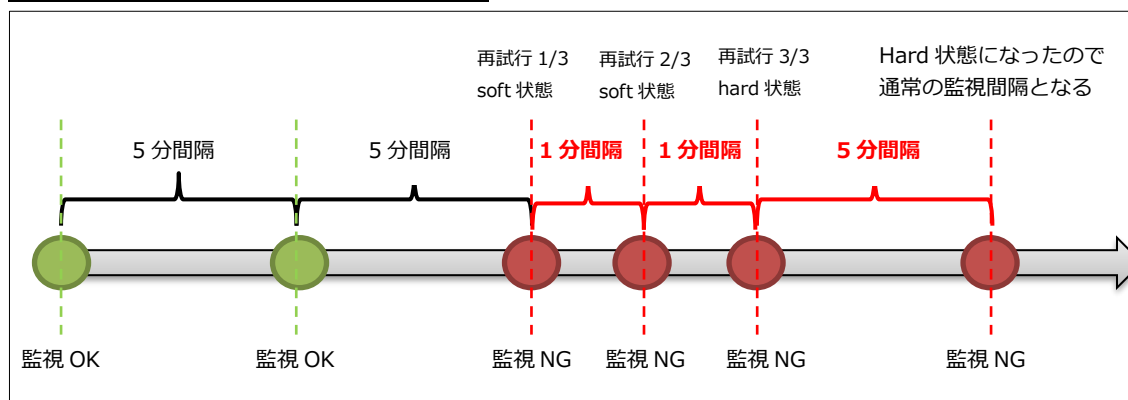
例として、監視間隔が 5 分、再試行回数が 3 回、再試行間隔が 1 分のサービス監視があるとし  
ます。

その場合、異常を検知し soft 状態になった時点で再試行回数の 1 回 (1/3) が実施された事にな  
ります。

その後 1 分間隔で残りの 2 回のチェックが実施され、3/3 になった時点でも異常の場合は hard  
状態となります。

hard 状態になった後は、通常の監視間隔である 5 分毎にチェックが実施されます。

図 監視間隔と再試行間隔・回数の関係





## 5.2 ホストのステータス

ホストのステータスには 4 種類にわかれます。

UP	ホストが起動している状態です。
DOWN	ホストが監視結果で異常であると判断された場合の状態です。 主に ping の結果となります。
UNREACHABLE	3.2 で解説したオンデマンドチェックの機能の一つです。日本語では「到達不可」という意味です。 ホスト設定で親ホストを設定している場合、「親ホストがダウンしているなら、子ホストには到達は出来ない」という概念により、親ホストがダウンした場合に子ホストは UNREACHABLE 状態となります。
PENDING	日本語で「保留」という意味です。ホストが登録されてからサービス監視が実施されていない状態です。

## 5.3 サービスのステータス

サービスのステータスは 5 種類あります。

OK	正常な状態です。監視結果が正常値であることを示しています。
WARNING	警告の状態でしきい値の WARNING で設定された値を超えたことを示しています。
CRITICAL	異常の状態でしきい値の CRITICAL で設定された値を超えたことを示しています。
UNKNOWN	不明な状態です。監視結果から判断出来ない設定ミスなどが考えられます。
PENDING	サービスが登録されてからまだ監視が実施されていない状態です。

## 6 通知機能

通知とは、ホストやサービスの状態に変化が起こった場合に外部へ通知する機能です。

一般的には電子メールでの通知となり、これも Nagios の機能を引き継いでいます。

そのため X-MON ではユーザの連絡先に PC 向けのアドレスと携帯向けの 2 つが登録出来ます。

- ・ E-MAIL アドレス
- ・ 携帯モバイル用 E-MAIL アドレス

X-MON ではホストグループやサービスグループといった監視のまとまりごとに通知先を設定したり、単一のホスト・サービスへ通知先が設定出来たりと柔軟な設定が行えます。

そのため、同じホストでも、HTTP サービスに異常が起こった際の連絡先と、Mail サービスに異常が起こった際の連絡先を分けることも可能です。

通知を実施するタイミングも X-MON では管理画面から容易に設定できるようになっています。

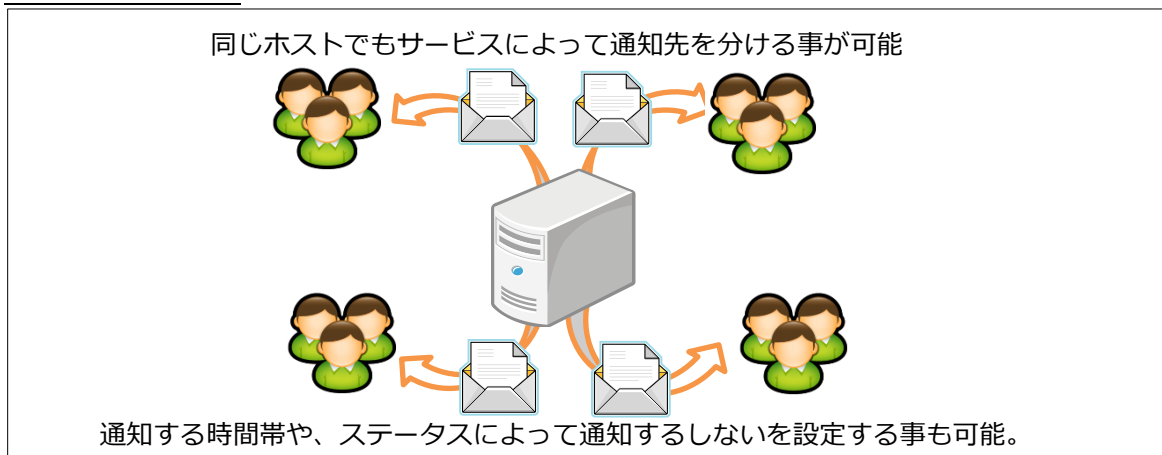
基本的には 24 時間 365 日の通知ですが、時間帯を指定する事により、

例えば深夜のみであったり、月曜日から金曜日の平日のみであったりと週のスケジュールによって通知をする時間帯を設定できます。

通知する状態の変化のタイミングも選択が可能です。

警告である WARNING の状態では通知は実施せず、CRITICAL の際にのみ通知を行うことも可能です。

図 通知について 1



メールでの通知になるため、大量のメールが一度に送られると ISP によってはスパムメールと認識される可能性があります。

そのため、基本概念として、発生を検知したら通知されるタイミングはその一度だけです。通知がされても、その後の監視のチェックは実施されますが、通知は再通知という設定で行われていますのでチェックの度にメールが送信されるという事ではありません。次に状態が変わった（復旧し監視が OK になった等）か、再通知で指定した時間が経てば通知が実施されます。

図 通知に関して 2

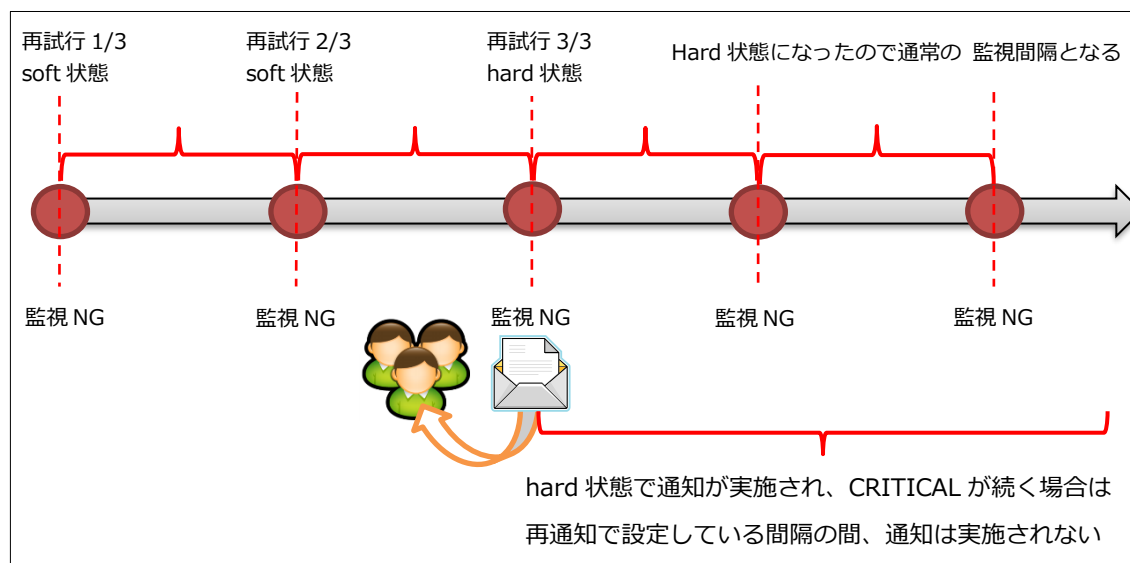
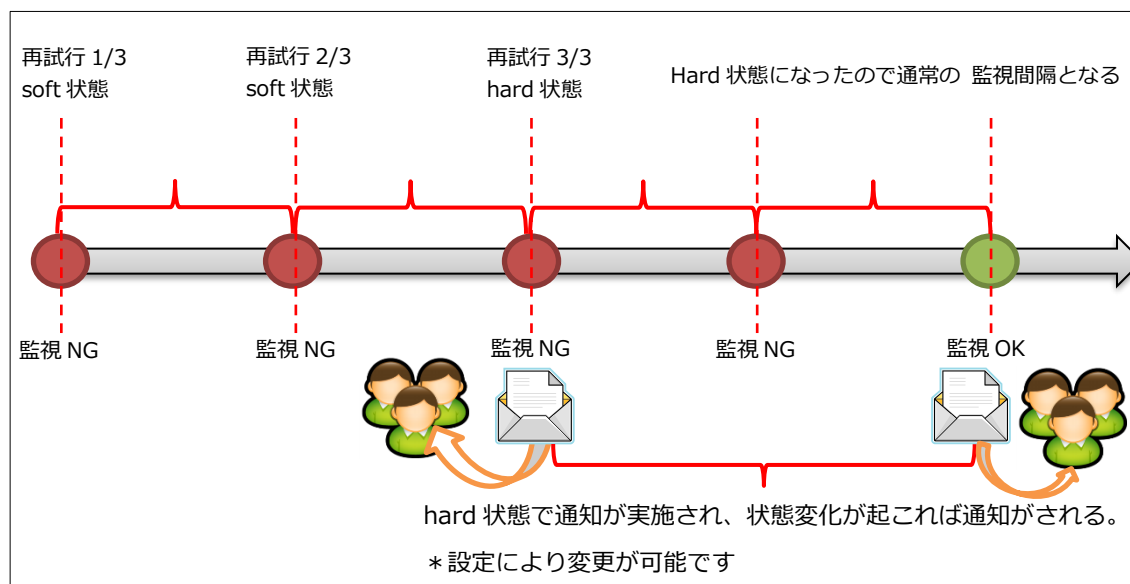
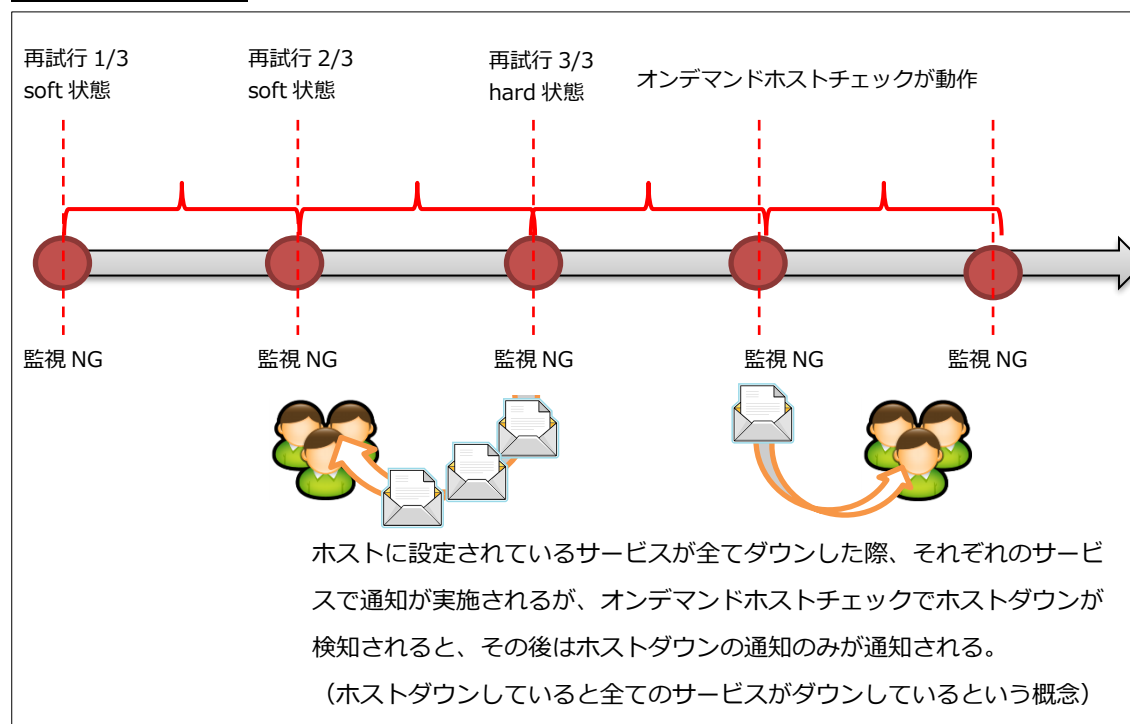


図 通知に関して 3



オンデマンドホストチェックと同じく、ホストがダウンしているならすべてのサービスがダウンしている、という概念があるため  
ホストダウンを検知した場合は他のサービスの通知は実施されなくなる制御も行われます。

図 通知に関して 4



## 6.1 通知の文章

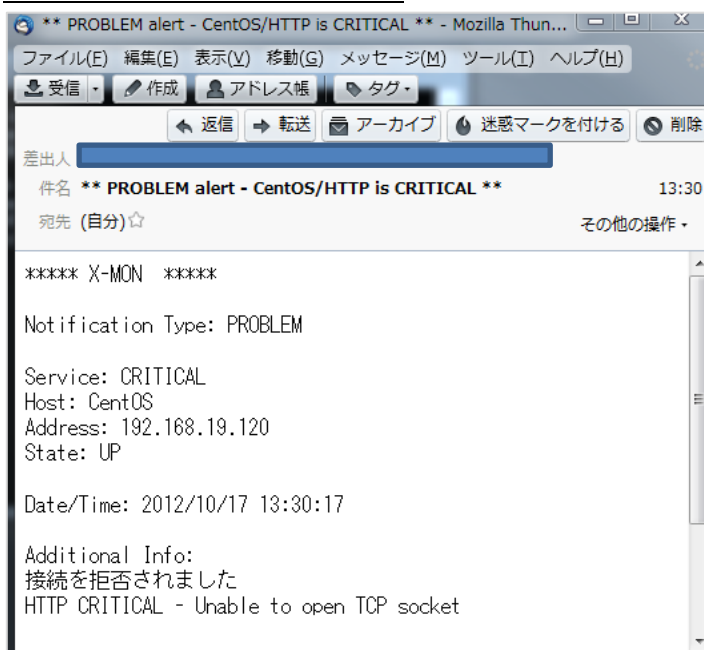
X-MON では通知のメールの内容を設定する事が可能です。

デフォルトの設定では Nagios の機能を引き継いでいますので必要最低限の情報しか記載がありませんが、メールの件名や内容に日本語を含ませる、またホストの情報をさらに記載させる事も可能です。

注意としては、通知ユーザにつきメールの内容は 1 つしか設定が出来ません。

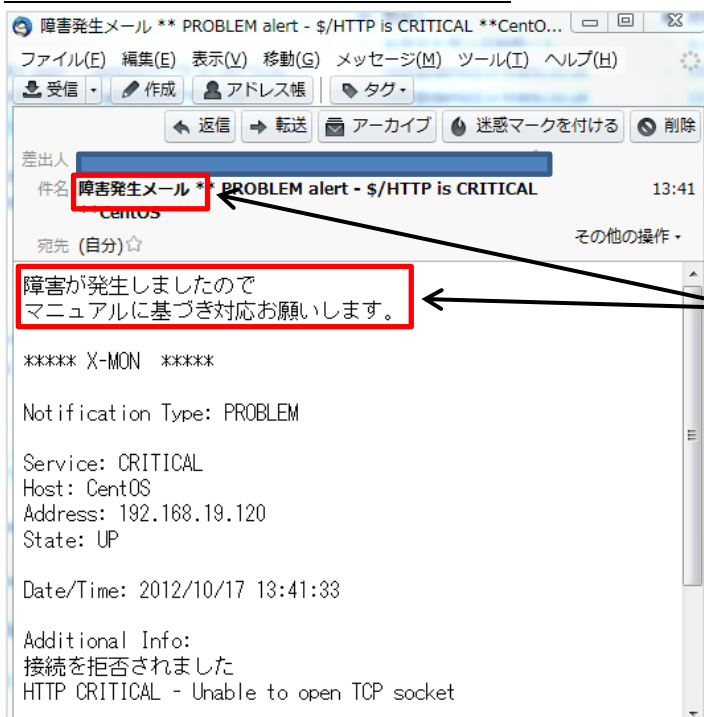
また、CRITICAL を検知やホストが復旧した際もメールの内容を分ける事は出来ません。

図 デフォルトの通知メールの例



デフォルトは最低限の情報  
のみ。

図 文章の内容を編集した通知メールの例



任意の内容を記載出来る

## 7 その他の設定項目

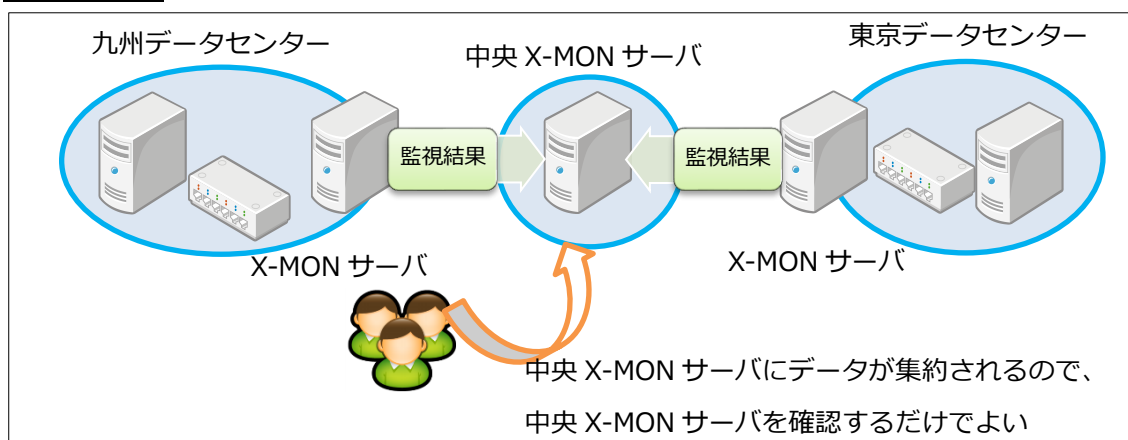
本リファレンスでは扱いませんが、X-MON に搭載されている設定項目をご紹介します。

### 7.1 分散監視

分散監視とは X-MON を二台以上使用し、直接監視する X-MON から一台の中央監視をする X-MON ヘデータを送り管理画面ですべての監視を確認出来る機能です。

詳細は別途マニュアル「分散監視リファレンス」をご参照ください。

図 分散監視



### 7.2 警告灯管理

通知機能の一つとして警告灯を光らせたり音を出したりして通知する事が可能です。

X-MON にてサポートしている警告灯の種類については X-MON サポートサイトをご参照ください。

### 7.3 Syslog 管理

X-MON を Syslog サーバとして動作させ、ホストからのログを受け取り、設定した文字列を検知すると障害として検知させる事が出来ます。

詳細は別途マニュアル「X-MON 高度リファレンス」をご参照ください。

## 7.4 構成管理

構成管理とは登録しているホストのハードウェアの情報や設置している場所の情報、ラックの場所などを登録できます。障害が発生し、どの場所に設置されている、保守期限がまだあるのかなども確認が出来ます。

詳細は別途マニュアル「構成情報管理リファレンス」をご参照ください。

図 構成管理情報

障害対応ガイド	ホスト詳細	ドキュメント	リンク	構成情報	イベントログ	通知履歴	外部コマンド履歴	コメント
概要								
ハードウェア								
<u>WinServer2019_001</u>								
ハードウェア保守情報								
ハードウェア名		WinServer2019_001						
メーカーシリアル番号		Dell-001						
保守期限		2020年03月31日						
保守情報		未設定						
場所情報								
設置場所		<u>大阪データセンター</u>						
対象ラック		<u>ラック1</u>						
電源情報								
電源A		1600 W		30%				
データセンター設置ラック								
<u>ラック1</u>								

## 8 サンプルネットワークを使った監視

監視概要についてはご理解頂けたでしょうか。

ここからは、実際にサンプルネットワークを用いて監視の設定をしていきます。

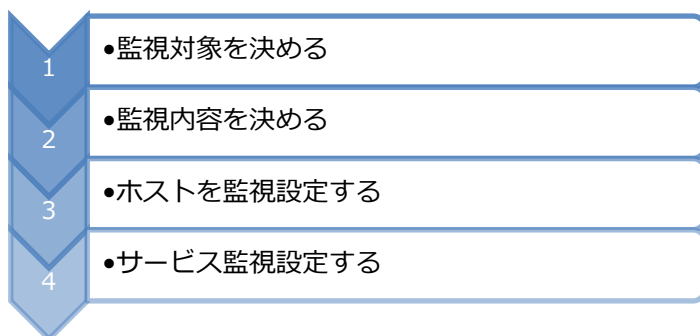
X-MON では主に 2 通りの監視登録方法があります。

- ① IP アドレスのみを入力し、X-MON が検出したサービスから監視を行いたいサービスを選択し、登録する
- ② 手動でホストやサービスを登録する

①の方法は「かんたん監視登録」という機能を使用します。8.2 章までを確認の上、別途マニュアル「かんたん監視登録マニュアル」をご確認ください。

8.3 章からは②の手動でホスト・サービスを登録する方法を解説します。

監視をしている順序としては下記ようになります。

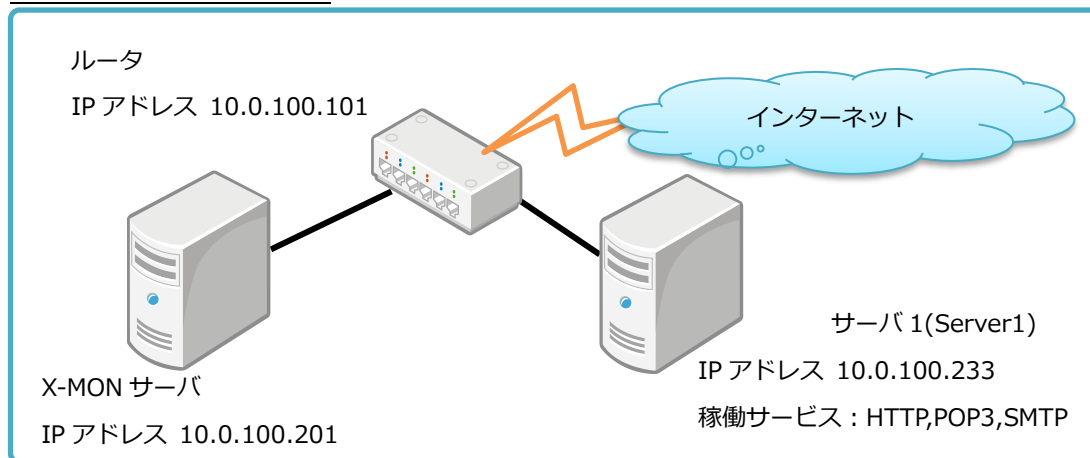


サンプルネットワークに基づいて、監視対象を決めるところから始めていきましょう。



## 8.1 監視対象を決める

図 サンプルネットワーク



まずは同一のサブネットネットワーク内に X-MON と監視対象のルータ、サーバがある状況で考えていきましょう。

このサンプルでは、サーバ 1 はルータの配下にあります。そのためルータが停止してしまうとサーバ 1 はいくら稼働していてもインターネットにはアクセス出来ない事になります。そのため監視対象としてはルータとサーバ 1 という事になります。

## 8.2 監視内容を決める

監視対象が決まったら、次は監視内容を考えます。

サーバ 1 ではまず Web サービス（HTTP）が稼働しているので監視対象のサービスとなります。またメールサーバ機能もあるので監視対象サービスとなります。メールサーバ機能はメールを受信する POP3 とメールを配送する SMTP の 2 つが稼働していますので、2 つとも監視するようにしましょう。

次にルータの監視内容を考えてみましょう。

ルータはルータ自身の死活監視が第一です。X-MON ではオンデマンドホストチェックがありますので死活監視は全サービスが異常となった際にチェックが動きますが、何もサービスが登録されない場合は PENDING(保留)ステータスのままになってしまいます。そのため、サービスとして PING 監視を追加する事にします。

監視の内容を表にまとめてみましょう。

ホスト ID	名称	監視サービス名	監視ポート番号	内容
Server1	www-server	HTTP	80	Web サービス
		POP3	110	メール受信
		SMTP	25	メール配送
Router	gw-router	PING	N/A	死活

かんたん監視登録機能を使用する場合は「かんたん監視登録マニュアル」をご確認ください。

### 8.3 ホストの監視設定をする

それでは、実際にホストを X-MON に登録してみましょう。

X-MON の画面にアクセスします。アクセスはブラウザで X-MON がインストールされている IP アドレスにアクセスします。ログイン ID とパスワードは初期値です。

Login ID : admin

Password: x-mon

ダッシュボード画面からメニューを開き、「管理者メニュー」の「ホスト・サービス管理」を選択してください。

図 管理者メニュー



ホスト一覧の画面になります。一番初めは X-MON 自身のみが登録されています。

左上の「新規作成」をクリックしてください。

## 図 ホスト一覧

ホスト一覧

ホスト・サービス管理 | [ホストグループ管理](#) | [サービスグループ管理](#) | [アイコン管理](#) | [構成管理](#) | [ドキュメント管理](#)

検索

**新規作成** | [かんたん監視登録](#) | [ネットワークからホストを検出する](#) | [削除](#) | [削除と承認](#)

ID	名称	IPアドレス/FQDN	エスカレーション	監視エージェント状況
<input type="checkbox"/> X-MON	X-MON	127.0.0.1	有効 1 無効 0	NRPE OK SNMP OK WMI -

[詳細表示](#) | [サービス設定](#) | [ホストエスカレーション設定](#)

新規のホストの登録画面になりますので、ルータの情報を次のように入力してみます。

ホスト ID(英数字)	Router
ホスト名称	gw-router
機器種別	ルータ
IP アドレス	10.0.100.101
MAC アドレス	N/A(入力なし)

## 図 ホスト登録

ホストの作成

[キャンセル](#) | [すべて開く](#)

基本設定

ホストID(英数字)  
Router

ホスト名称  
gw-router

種別  
ルータ/L3スイッチ

IPアドレス/FQDN  
10.0.100.101

MACアドレス

☒ 監視を行う ☐ 監視は行わない

リンク

SNMP認証設定

WMI認証設定

AWS設定

[キャンセル](#) | [作成](#) | **作成と承認** | [詳細な設定へ進む](#)

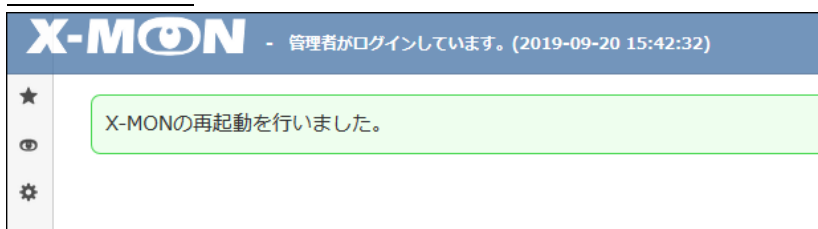
その他の項目はそのまま「作成と承認」ボタンを押してください。

「設定を追加し、反映しました」と画面になりますので、X-MON を再起動させてホストの登録は完了です。

図 ホスト登録完了



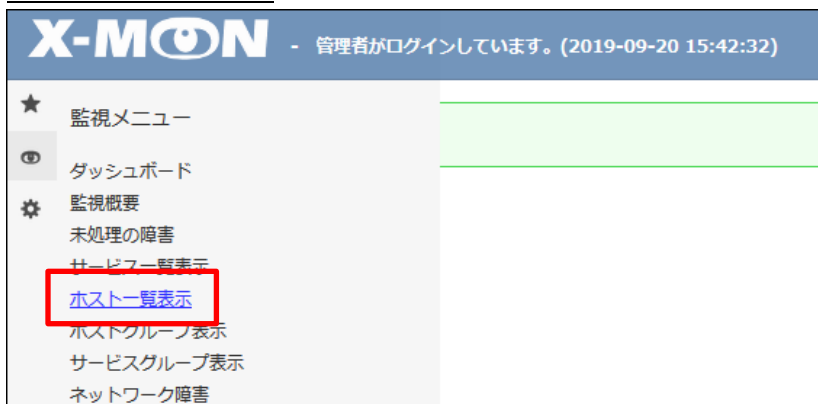
図 再起動完了



登録されているか確認してみましょう。

「監視メニュー」から「ホスト一覧表示」を開きます。

図 ホスト一覧を選択



ルータが登録されています。

この段階ではまだサービスの登録がされていないためステータス情報では「このホストはチェックするようにスケジュールされていません。」と表示されますが正常です。

図 ホスト登録直後

ホストID ↑ ↓	ホスト名称	監視ステータス ↑ ↓	最終チェック時刻 ↑ ↓	経過時間 ↑ ↓	ステータス情報
Router ?	gw-router	PENDING	N/A	N/A	このホストはチェックするにはスケジュールされていません。

それでは同じようにサーバ1についてもホストを登録してみましょう。

入力する情報は下記となります。

ホスト ID(英数字)	Server1
ホスト名称	www-server
機器種別	物理サーバ
IP アドレス	10.0.100.233
MAC アドレス	N/A(入力なし)

図 ホスト登録

ホストの作成

キャンセル

すべて開く

基本設定

ホストID(英数字)

Server1

ホスト名称

www-server

種別

物理サーバ

IPアドレス/FQDN

10.0.100.233

MACアドレス

監視を行う

監視は行わない

リンク

SNMP認証設定

WMI認証設定

AWS設定

キャンセル

作成

作成と承認

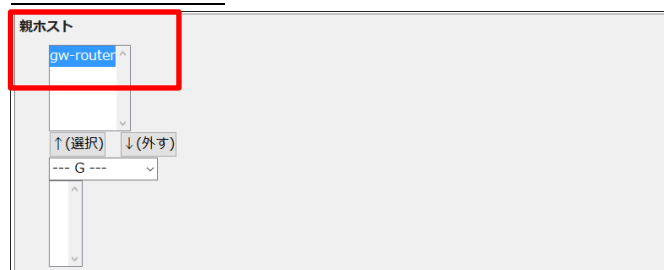
詳細な設定へ進む

ルータと同じように登録しますが、画面下にて「詳細な設定へ進む」を選択してください。

詳細なホスト設定の画面に移ります。その中で「親ホスト」という項目があるのでホスト「gw-router」を選択し、「↑(選択)」ボタンを押してください。

これで、ルータの下にサーバが配置されているというネットワークの親子関係が設定できます。

図 親ホスト設定



ルータを親ホストに設定出来たら「作成と承認」ボタンを押し、X-MON を再起動してください。X-MON を再起動後、「ホスト一覧表示」で登録出来ているか確認してみましょう。

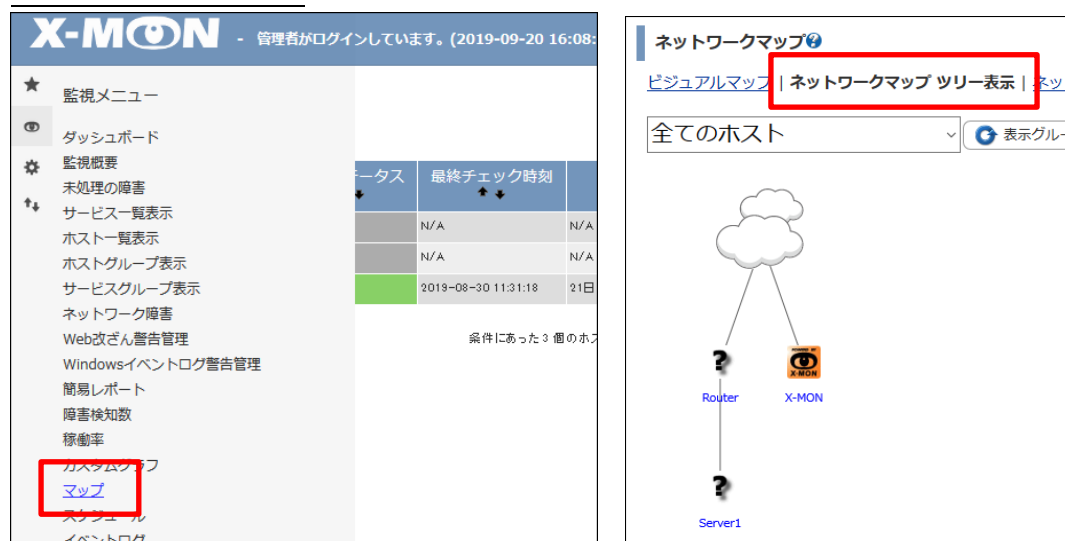
図 ホスト一覧表示

ホストID	ホスト名称	監視ステータス	最終チェック時刻	経過時間	ステータス情報
Router	gw-router	PENDING	N/A	N/A	このホストはチェックするようにはスケジュールされていません。
Server1	www-server	PENDING	N/A	N/A	このホストはチェックするようにはスケジュールされていません。

設定した親子関係についても確認します。

「監視メニュー」の「マップ」を選択し「ネットワークマップツリー表示」をクリックすると、Router の下に Server1 があるので親子関係が設定されている事がわかります。

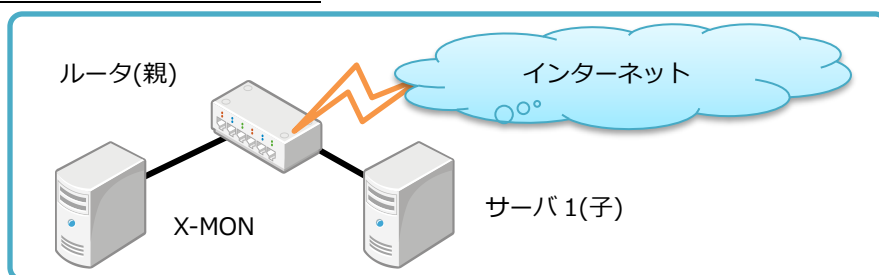
図 ネットワークマップ



### 親子関係について

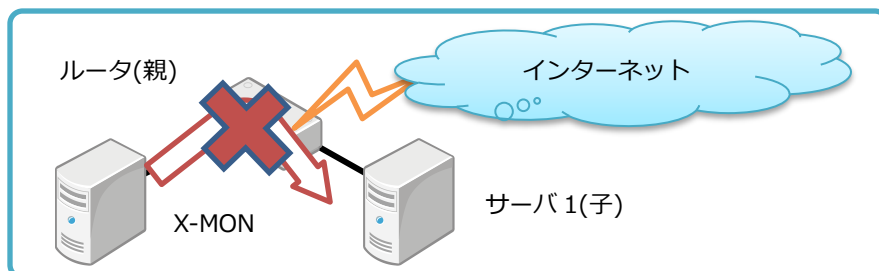
X-MON で用いている親子関係も Nagios の概念に基づいています。  
親子関係をしっかり設定する事で、余計な通知や警告を出さなくなります。  
サンプルネットワークの場合、ルータが親、サーバ 1 が子という関係です。

図 サンプルネットワーク



例えばルータに障害が発生したとします。その場合、X-MON から見るとサーバ 1 へはルータを経由しないと到達できないと認識されます。

図 サンプルネットワーク



その際ホストステータスは、ルータはダウン状態、サーバ 1 は未到達（Unreachable）状態となります。そして、ルータを始点とした「ネットワーク障害」と認識されます。

もし、この親子関係を設定していない場合、ルータに障害が発生しダウンとなってもネットワーク障害と認識されず、X-MON はサーバ 1 もダウンしていると認識してしまいます。  
そのため管理画面上からでは根本原因となる対象が特定し辛く、障害の切り分けに時間がかかってしまいます。  
せっかく監視をしているのに、これだと逆効果です。そのため、親子関係はしっかり設定するようにしましょう。

## 8.4 サービスの監視設定をする

ホストが登録できたのでサービスを登録して監視設定をしましょう。

各ホストへ登録するサービスは以下です。

ホスト ID	名称	監視サービス名	監視ポート番号	内容
Server1	www-server	HTTP	80	Web サービス
		POP3	110	メール受信
		SMTP	25	メール配送
Router	gw-router	PING	N/A	死活

ルータの PING サービスから登録します。「管理者メニュー」の「ホスト・サービス管理」を開きます。

ホスト一覧が表示されますので、ホスト「Router」の「サービス設定」を開きます。

図 ホスト一覧

ID	名称	IPアドレス/FQDN	エスカレーション		監視エージェント状況		
<input type="checkbox"/> Router	? gw-router	10.0.100.101	有効 0	無効 0	NRPE -	SNMP -	WMI -
<div> <a href="#">→ 詳細表示</a> <a href="#">🔧 サービス設定</a> <a href="#">→ ホストエスカレーション設定</a> </div>							

何もサービスが登録されていない場合は X-MON で用意されている「監視パッケージ」で多数の監視設定を一括で登録する事が出来ます。今回は監視パッケージの中から「死活監視パッケージ」を選択してみましょう。選択が出来たら「選択した監視パッケージで登録と承認」を押してください。

図 監視設定

gw-router - サービス一覧

監視パッケージメニュー

死活監視パッケージ

▼

表示できるサービス情報はありません。



PING のサービスが追加されました。右上の再起動ボタンで X-MON を再起動させて設定を反映させてください。

図 監視設定 2

gw-router - サービス一覧

設定を追加し反映しました。

検索

戻る 新規作成 SNMPサービス一括作成 snmpwalk実行 削除 削除と承認

監視パッケージメニュー

-- 選択して下さい -- 選択した監視パッケージで登録と承認 監視パッケージの新規作成

サービスID	エスカレーション	操作
<input type="checkbox"/> PING	有効 0 無効 0	詳細表示 サービスエスカレーション設定

再起動を実施したら、サービスが登録されているか確認してみましょう。

「監視メニュー」の「サービス一覧表示」を開いてください。

図 監視メニュー

X-MON - 管理者がログインしています。(2019-09-24)

- ★ 監視メニュー
- 📊 ダッシュボード
- ⚙️ 監視概要
- 未処理の障害
- サービス一覧表示**
- ホスト一覧表示
- ホストグループ表示
- サービスグループ表示

ルータに PING サービスが登録されています。登録された直後はまだ監視チェックが動いていないためステータス情報では次回のチェック予定日時が表示されます。

図 監視登録直後

ホストID (ホスト名称)	サービスID	監視ステータス	最終チェック時刻	経過時間	試行回数	ステータス情報
Router (gw-router)	PING	PENDING	N/A	N/A	1/3	次回 チェック予定日時は、2019年09月24日 08時59分50秒です。

サービス一覧の画面はブラウザで自動更新されますので、チェック予定日時が過ぎて更新されますと、下のように監視の結果が表示されます。

図 正常に監視されている状態

ホストID (ホスト名称)	サービスID	監視ステータス	最終チェック時刻	経過時間	試行回数	ステータス情報
Router (gw-router)	PING	OK	2019-09-24 09:45:58	0日と00時間02分15秒	1/3	PING OK - Packet loss = 0%, RTA = 10.92 ms

それでは、サーバ1のサービスも監視追加していきます。

再度「管理者メニュー」の「ホスト・サービス管理」を開いてサーバ1の「サービス設定」を開いてください。先ほどのルータを同じく、何も監視設定がされていないため監視パッケージを登録する事が出来ますが、今度は手動で監視を追加していきましょう。

左上の「新規作成」を開いてください。

図 監視設定



サービスの新規作成画面に遷移します。

X-MON では基本的な監視設定は選択するだけで設定が出来ます。

まずは Web サービスの HTTP を監視設定しますので以下の入力を行ってください。

サービス ID(英数字)	HTTP
サービス監視用コマンド	Web サービス監視 - HTTP 監視

詳細な監視設定も可能ですが、ここではデフォルトのままにします。

詳細な項目設定についてはオンラインマニュアルをご参照ください。

図 サービスの作成

The screenshot shows the '基本設定' (Basic Settings) section of the service creation form. A red box highlights the 'サービスID(英数字)' (Service ID) field containing 'HTTP' and the 'サービス監視用コマンド' (Service Monitoring Command) dropdown menu, which has 'Webサービス監視' (Web Service Monitoring) and 'HTTP監視' (HTTP Monitoring) selected. The 'ホストID(英数字)' (Host ID) field above contains 'Server1'.

入力が出来たら画面の下の「作成と承認」ボタンを押し、設定を追加後右上の再起動ボタンで X-MON を再起動させてください。

再起動が出来たら、「サービス一覧」から追加出来ているか確認してみましょう。

図 監視設定直後

ホストID (ホスト名称)	サービスID	監視ステータス	最終チェック時刻	経過時間	試行回数	ステータス情報
Router (gw-router)	PING	OK	2019-09-24 10:05:58	0日と00時間21分52秒	1/3	PING OK - Packet loss = 0%, RTA = 10.64 ms
Server1 (www-server)	HTTP	PENDING	N/A	N/A	1/3	次回チェック予定日時は、2019年09月24日 10時08分37秒です。

HTTP サービス監視が追加されています。チェックが実行されると下記画像のようになります。

図 正常に監視されている状態

Server1 (www-server)	HTTP	OK	2019-09-24 10:45:37	0日と00時間38分36秒	1/3	HTTP OK: HTTP/1.1 200 OK - 5241 bytes in 0.051 second response time
-------------------------	------	----	---------------------	---------------	-----	---

これで HTTP のサービス監視の追加は完了しましたので、POP3 と SMTP も同じように監視を追加してみましょう。

POP3 では下記のように設定してみましょう。

サービス ID(英数字)	POP3
サービス監視用コマンド	メールサービス監視 - POP3 監視

その他の設定はデフォルトのままです。

図 POP3 サービス作成

基本設定

ホストID(英数字)

Server1

サービスID(英数字)

POP3

サービス監視用コマンド

メールサービス監視

POP3監視

ポート番号

110

タイムアウト(秒)

10

WARNINGしきい値(秒)

3

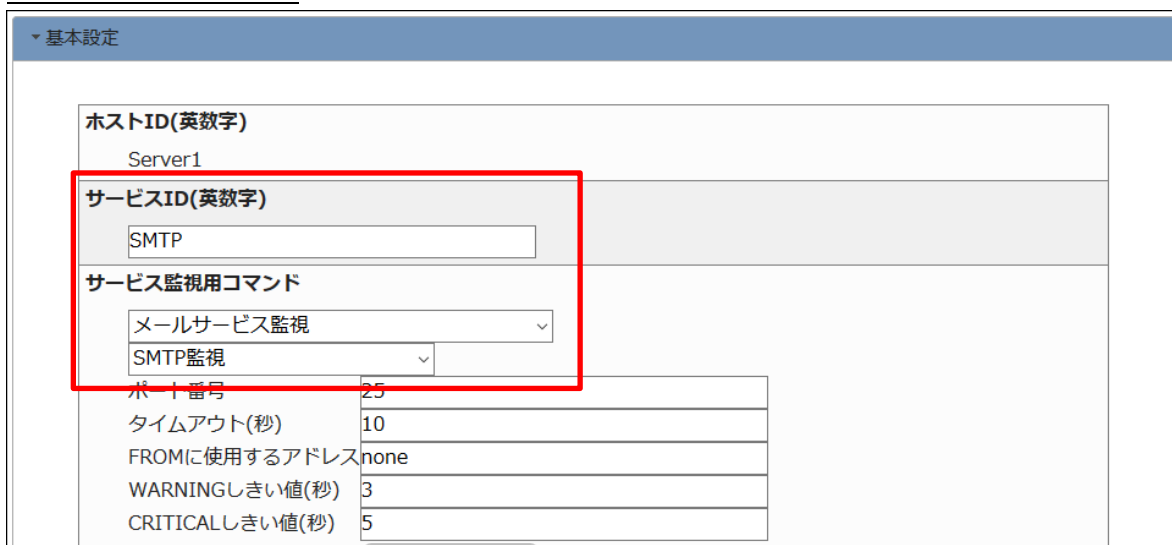
CRITICALしきい値(秒)

5

SMTP は下記のように設定してみましょう。

サービス ID(英数字)	SMTP
サービス監視用コマンド	メールサービス監視 - SMTP 監視

図 SMTP サービス作成



入力が出来たら「作成と承認」を押して X-MON の再起動ボタンから再起動させてください。

サービス一覧から正常に監視が出来ているか確認してみましょう。

図 正常に監視されている状態

Server1 (www-server)	HTTP	OK	2019-09-24 11:09:31	0日と01時間03分56秒	1/3	<a href="#">HTTP OK: HTTP/1.1 200 OK - 5241 bytes in 0.059 second response time</a>
	POP3	OK	2019-09-24 11:13:33	0日と00時間01分00秒	1/3	POP OK - 0.042 second response time on port 110 [+OKDovecot ready]
	SMTP	OK	2019-09-24 11:14:24	0日と00時間00分09秒	1/3	SMTP OK - 0.006 sec. response time

これで監視サービスの監視設定は完了です。

## ⚠ ホスト情報の画面遷移について

さて、監視も追加が完了しました。

これまではサービス一覧から確認していましたが、ホストが多くなるとサービスの数も多くなるので大変です。そのため、ホストごとに情報を表示できる機能があります。

「ホスト一覧」または「サービス一覧」画面でホスト ID のリンクを選択します。

図 サービス一覧表示

ホストID (ホスト名称)	サービスID	監視ステータス	最終チェック時刻	経過時間	試行回数	ステータス情報
<a href="#">Router (gw-router)</a>	<a href="#">PING</a>	OK	2019-09-24 10:55:58	0日と01時間14分38秒	1/3	<a href="#">PING OK - Packet loss = 0%, RTA = 8.74 ms</a>
<a href="#">Server1 (www-server)</a>	<a href="#">HTTP</a>	OK	2019-09-24 10:59:31	0日と00時間49分52秒	1/3	<a href="#">HTTP OK: HTTP/1.1 200 OK - 5241 bytes in 0.055 second response time</a>

サーバ1のホスト情報の画面になります。ここでは、ホストの詳細の情報や関連付けられたドキュメントや構成情報、通知の履歴などが確認できます。

図 ホスト情報

?

Server1(www-server)

IPアドレス/FQDN:10.0.100.233

ホストグループ: 所属なし

最終チェック時刻: 2019年09月24日 11時01分39秒

次回チェック予定: 2019年09月24日 11時01分50秒

🔄

🔄

🔄

🔄

🔄

-- その他コマンド --

戻る

障害対応ガイド

ホスト詳細

ドキュメント

リンク

構成情報

イベントログ

通知履歴

外部コマンド履歴

コメント

現在のステータスは、UP

0日間と 00時間53分15秒前より継続しています。

FPING OK - 10.0.100.233 (loss=0%, rta=0.040000 ms)

関連付けられたドキュメント

ホストドキュメント

場所・ラックドキュメント

「障害対応ガイド」もしくは「ホスト詳細」タブの一番下にメニューがあります。

このメニューからホストの情報を表示できます。

🖥️ このホストの監視結果一覧を表示

全サービス

未処理の障害

⚙️ 設定確認・変更

ホスト

ホストの全サービス

ホストエスカレーション

■ このホストの監視結果一覧を表示 - 全サービス -

これはホストに設定されているサービスの状態の一覧を表示できます。

「サービス一覧」では全ホストのサービスが表示されますが、ここではホストに登録されているサービスのみが表示されます。

■ このホストの監視結果一覧を表示 - 未処理の障害 -

これは上記で説明したホストに登録されているサービスの中で、障害状態(OK や PENDING 以外のステータス)かつダウンタイムや認知済みの処理が行われていないものを表示します。

なおホストが障害状態(DOWN や UNREACHABLE)の場合は表示されません。

■ 設定確認・変更 - ホスト -

「管理者メニュー」の「ホスト・サービス管理」で該当ホストの「詳細表示」画面に遷移します。

■ 設定確認・変更 - ホストの全サービス -

「管理者メニュー」の「ホスト・サービス管理」で該当ホストの「サービス設定」に遷移します。

■ 設定確認・変更 - ホストのエスカレーション -

「管理者メニュー」の「ホスト・サービス管理」で該当ホストの「ホストエスカレーション設定」に遷移します。

登録方法の詳細は別途マニュアル「エスカレーション設定クイックリファレンス」をご参照ください。

このように、ホスト情報の画面からも各種設定画面へ遷移する事が可能ですので、

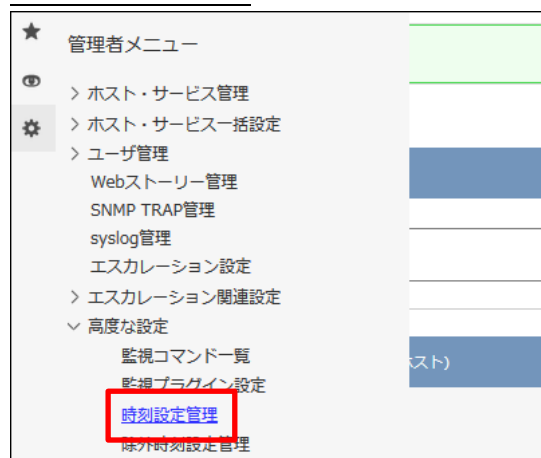
「この情報が見たい、設定したい」という時はホスト情報を開くとスムーズに出来る事です。

## 8.5 時刻の設定

時刻の設定とは、例えば監視は 24 時間 365 日で行うが、メールなどでの通知は営業時間内だけ実施するなど時間を設定できる機能です。

「管理者メニュー」から「高度な設定」を選び「時刻設定管理」を開きます。

図 管理者メニュー



時刻一覧が表示されます。デフォルトでは 24 時間 365 日通知する設定があります。

この設定は X-MON での標準となっていますので、削除は行わないでください。

図 時刻設定一覧



例として営業日(月～金の 9 時～18 時)を対象とする時刻設定を追加します。

「新規作成」ボタンを押し、設定追加画面に遷移します。

下記のように設定してみましょう。名称は任意のもので問題ありません。

時刻設定 ID	Weekdays
月曜日～金曜日	09:00-18:00
土曜日、日曜日	00:00-00:00

図 時刻設定

時刻ID(英数字)	
<input type="text" value="Weekdays"/>	
時刻名称	
<input type="text" value="営業日"/>	
日曜日の監視時間帯	
00:00-00:00	
<input type="range"/>	
月曜日の監視時間帯	
09:00-18:00	
<input type="range"/>	
火曜日の監視時間帯	
09:00-18:00	
<input type="range"/>	
水曜日の監視時間帯	
09:00-18:00	
<input type="range"/>	
木曜日の監視時間帯	
09:00-18:00	
<input type="range"/>	
金曜日の監視時間帯	
09:00-18:00	
<input type="range"/>	
土曜日の監視時間帯	
00:00-00:00	

設定できましたら「作成と承認」ボタンを押し、X-MON を再起動します。

時刻設定画面で表示されましたら、登録は完了です。

時刻設定一覧

← 一覧へ

+ 新規作成

✖ 削除

🔄 削除と承認

ID	名称	操作	
<input type="checkbox"/> 24x7	24時間365日	→ 詳細表示	🔍 使用状況の確認
<input type="checkbox"/> Weekdays	営業日	→ 詳細表示	🔍 使用状況の確認

登録した時刻設定はホストやサービスの設定、ユーザ設定、エスカレーション設定の「監視時間帯」や「通知時間帯」で指定できます。



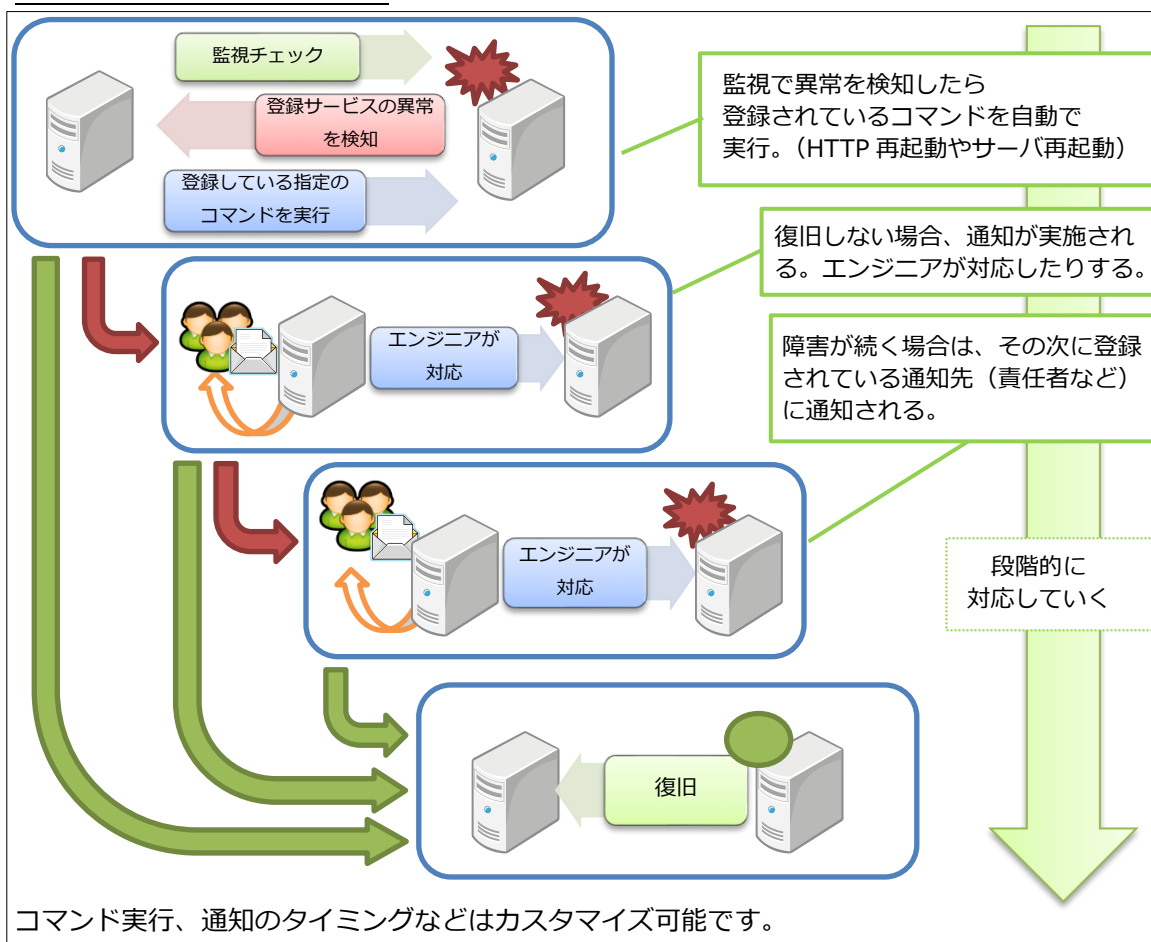
## 9 通知設定

前章で登録したホストの設定やサービスの設定に、障害が発生した場合のメール通知設定を行うために「エスカレーション設定」を登録します。

エスカレーション設定とは、障害が発生した際に行う通知を、障害ステータス別や経過時間などで設定できる機能です。

設定されたエスカレーションは障害発生と同時に動き始め、障害が復旧するまで行われます。

図 エスカレーション機能の例



登録方法はマニュアル「エスカレーション設定クイックリファレンス」をご確認ください。

## 10 X-MON の画面とそのほかの機能について

X-MON の概要、監視設定についてはご理解頂けたでしょうか。

それを踏まえて、基本的な X-MON の画面と機能について説明します。

### 10.1 ダッシュボード画面

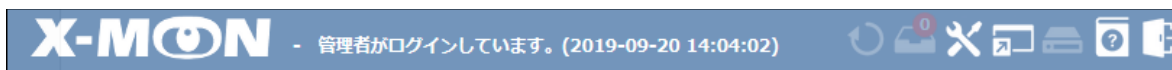
X-MON にログインした際、一番初めに表示される画面です。



この画面では、X-MON が監視しているステータス情報やパフォーマンスグラフの確認を行う事が出来ます。各情報は 60 秒で自動更新されます。

ダッシュボードの設定に関しては別途マニュアル「ダッシュボード操作マニュアル」をご覧ください。

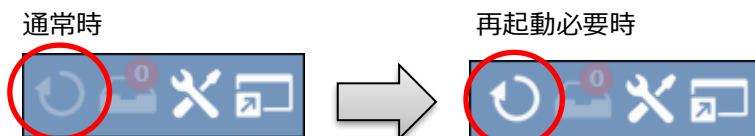
X-MON の画面で右上に表示されるアイコンを説明します。



#### ■ 再起動アイコン

X-MON で設定の変更が行われた後、設定を反映させるために再起動が必要な場合に、このボタンが点滅します。

#### 図 再起動ボタン



また、X-MON の再起動は「管理者メニュー」の「X-MON 再起動」からでも可能です。

## ■ 承認アイコン

X-MON で変更がされた際、承認権限のないユーザが変更を実施した場合や権限があっても承認をしなかった場合、承認が実施されないと実際に変更や追加は実施されません。

そのため、承認する申請があるのをお知らせするボタンとなっています。

図 承認ボタン

通常時



承認申請がある時



また、承認一覧の画面は「管理者メニュー」の「設定変更の承認」でも同じ画面に遷移します。

## ■ プロセス情報アイコン



「監視メニュー」の「プロセス情報」で無効となっているものがある場合、このアイコンが表示されます。マウスをアイコンの上に乗せると無効となっているものが表示されます。また、アイコンを押すことで「プロセス情報」画面へ遷移します。

## ■ ショートカットアイコン



現在表示されている画面をショートカット登録し、メニューから遷移できるようにします。

## ■ バックアップアイコン

「管理者メニュー」の「バックアップ管理」でバックアップが作成中の場合アイコンが変化します。バックアップ作成中に X-MON の監視設定などを変更すると、正しい情報が保存できなくなる恐れがあります。

通常時



バックアップ作成中



## ■ オンラインマニュアルアイコン



オンラインマニュアルをクリックすると、オンラインマニュアルの画面が表示されます。  
監視プラグインの説明や、機能について解説されていますので是非ご活用ください。

## 図 オンラインマニュアル

ヘルプ - ダッシュボード - ダッシュボード

オペレーションメニュー

- 監視設定
- 監視設定 (上級者向け)
- 権限
- TRAP設定
- syslog監視設定
- アイコン設定
- システム情報
- 任意のパフォーマンスグラフ
- プロセス情報
- 構成情報
- ネットワークマップ
- 通知設定
- ダウンタイム
- コメント

ページ内ジャンプ

[ 概要 | 権限 | 表示項目 | 操作 ]

概要

X-MONのトップ画面です。  
各機能への遷移や、現在のホスト・サービスのステータス情報の確認、パフォーマンスグラフの作成などを行うことができます。  
各表示項目は60秒ごとに自動で更新されます。  
グラフに関しては読み込みは60秒ごとに行われますが、グラフ自体の更新については5分ごととなっています。

権限

	システム管理者	運用責任者	オペレータ	閲覧者	通知ユーザ
閲覧	○	○	○	△	×

※閲覧者に関しては、権限を与えられているホストグループに所属するホスト情報のみ表示を行います。

表示項目

チェックコマンドメニュー

AWS EC2

AWS ELB

## ■ ログアウトアイコン



X-MON からログアウトします。X-MON では一度ログインするとログインした状態になりますので、適切にログアウトするようにしてください。

## ■ ログイン情報

X-MON

管理者がログインしています。(2019-09-20 14:04:02)

リフレッシュ

通知

設定

ヘルプ

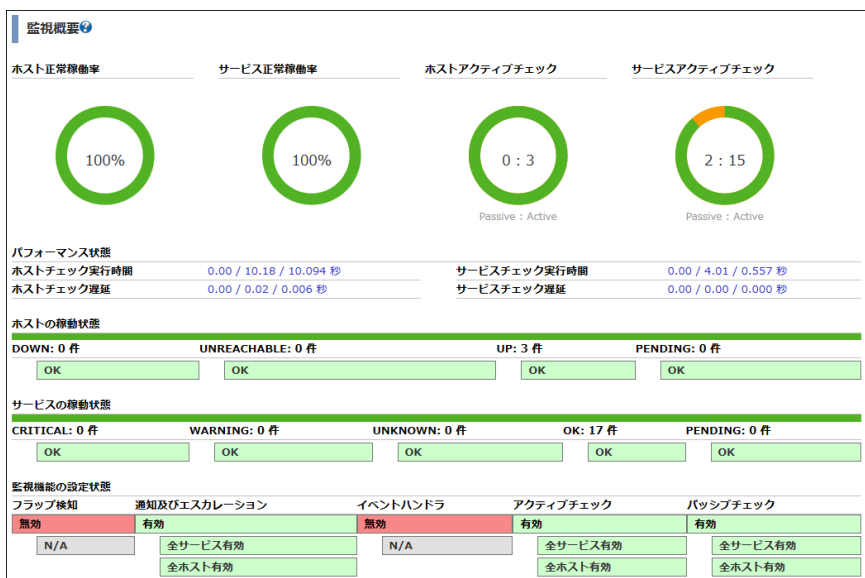
ログアウト

中央には、現在ブラウザでログインしているユーザの名称と X-MON サーバの現在時刻が表示されます。

## 10.2 監視概要画面

「監視メニュー」の「監視概要」で開く画面です。

この画面では、X-MON で監視しているホスト・サービスの全体的な情報を表示できます。



### ■ パフォーマンス状態

パフォーマンス状態には、ホスト・サービスのチェック実行時間、チェック遅延時間が表示されます。左から順に最小値、最大値、平均値となっています。

実行時間に表示されるのは、チェックを行った際にホスト・サービスからの反応が返ってくるまでに、どの程度の時間がかかったかです。

遅延に表示されるのは、チェックを行う際にスケジュールされた日時から、どの程度の誤差があったかです。

### ■ ホストの稼働状態・サービスの稼働状態

「ホストの稼働状態」「サービスの稼働状態」には、監視対象となるステータスをまとめて表示します。

### ■ 監視機能の設定状態

監視機能の設定状態には、X-MON の監視で得た全体の情報を簡潔にまとめて表示します。

フラップ検知、エスカレーション、イベントハンドラの詳細はオンラインマニュアルをご参考ください。

### 10.3 未処理の障害画面

「監視メニュー」の「未処理の障害」で開く画面です。

障害状態(OK や PENDING 以外のステータス)かつダウンタイムや認知済みの処理が行われていないサービスを表示します。

なおホストが障害状態(DOWN や UNREACHABLE)の場合は表示されません。

#### 10.3.1 認知済みとは

X-MON で監視を行っているホスト・サービスで障害が発生した際、エンジニアなどが障害の対応を開始した際に「この障害を認知して、対応を行っている」と示す事を認知済といいます。

認知済みとすることで、X-MON からの障害通知メールなどを停止させることが出来ます。

認知済にするには、該当のサービス、もしくはホストの 情報画面 から設定します。

図 サービス詳細



この赤丸で囲っているアイコンをクリックすると認知済に設定出来ます。

### 10.3.2 ダウンタイムとは

ダウンタイムは、あらかじめホストやサービスがダウンする事がわかっている場合に、通知を抑制する目的で設定します。たとえば、システムのメンテナンスやアップデート作業に伴う再起動で、サーバが一時的にダウンする場合などに使用します。そうすることで、ダウンを検知した場合に通知を抑制することが出来ます。

ダウンタイムをスケジュールするには、該当のサービスもしくはホストの詳細画面のメニューから設定します。

図 サービス詳細

**サービス情報**

**Server1 (www-server)**  
 サービスID: HTTP  
 IPアドレス/FQDN: 10.0.100.233

ホストグループ: 所属なし  
 サービスグループ: 所属なし  
 最終チェック時刻: 2020年01月07日 13時27分24秒  
 次回チェック予定: 2020年01月07日 13時32分24秒

-- その他コマンド --

← 戻る

障害対応ガイド サービス詳細 ドキュメント リンク 構成情報 イベントログ 通知履歴 外部コマンド履歴 コメント

現在のステータスは、 **OK**  
 0日間と 00時間01分04秒前より継続しています。

HTTP OK: HTTP/1.1 200 OK - 5233 bytes in 0.055 second response time

今回はサーバ1のHTTPサービスをダウンタイムの設定をします。  
 赤い丸で囲っているアイコンをクリックします。

ダウンタイムの設定画面となりますので設定を入力します。

対象	自動的に対象のサービスIDが選択されています。
コメント	自由に入力出来ます。
種類	デフォルトの「固定」とします。
ダウンタイム期間	ダウンタイムの期間を入力します。 デフォルトで現在時刻から2時間が指定されています。

対象の「関連するホストにもダウンタイムを設定する」を押すことでホストであるサーバ 1 にも一括でダウンタイムが設定できます。

今回はコメントに「メンテナンス」と入力し、「発行」ボタンを押します。

図 コメント入力

ダウンタイムの新規作成

対象 (入力必須)

サービス: Server1:HTTP x

ホストID ▼ ホストの検索

☐ 関連するホストにもダウンタイムを設定する

コメント

メンテナンス

種類

☒ 固定 ☐ フレキシブル

ダウンタイム期間

☒ 日付 ☐ 期間

2020/01/07 13:30-15:30

発行 閉じる

サービス一覧画面で確認してみましょう。

Server1 (www-server)	HTTP	OK	2020-01-07 13:47:24	0日と00時間22分58秒	1/3	<a href="#">HTTP OK: HTTP/1.1 200 OK - 5233 bytes in 0.041 second response time</a>
-------------------------	------	----	---------------------	---------------	-----	---

ダウンタイム前では、変化はありませんがダウンタイムに入ると

Server1 (www-server)	HTTP	D OK	2020-01-07 13:32:24	0日と00時間08分45秒	1/3	<a href="#">HTTP OK: HTTP/1.1 200 OK - 5233 bytes in 0.054 second response time</a>
-------------------------	------	------	---------------------	---------------	-----	---

HTTP の横に「D」が表示されます。

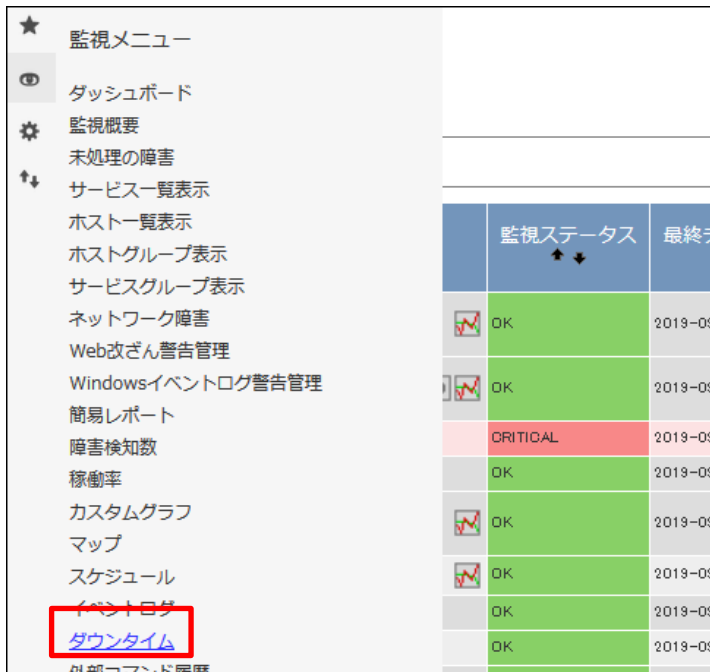
これでダウンタイム設定が完了しました。

次章で設定したダウンタイムを確認します。



## 10.4 ダウンタイム画面

「監視メニュー」の「ダウンタイム」を開いてみましょう。



現在、ダウンタイムがスケジュールされている一覧が表示されます。

図 ダウンタイム一覧



ダウンタイムが解除されるトリガーは以下となります。

- 設定しているダウンタイム期間が過ぎる
- 手動で解除する

手動で解除するには、削除したいダウタイム設定の横の×アイコンを押す、またはチェックボックスにチェックを入れ、「削除」ボタンを押します。

## 図 ダウンタイム解除

ダウタイム

ダウタイム | 定期設定

Q 絞り込み条件設定

ホスト / サービス

ダウタイム設定

種類

対象の絞り込み

☒ ホスト設定

☒ 設定済み

☒ 固定

全て

☒ サービス設定

☒ 設定予約

☒ フレキシブル

Q 検索

リセット

+ 新規作成

<input type="checkbox"/>	ダウタイムID / 定期設定名称	ホストID	サービスID	開始時間	終了時間	期間	種類	コメント	トリガーID	登録者	操作
<input type="checkbox"/>	設定済み 8	Server1	HTTP	2020/01/07 13:30:00	2020/01/07 15:30:00	2 時間 0 分	固定	メンテナンス	N/A	admin	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>

問題が無ければ「発行」ボタンを押します。

ダウタイムの削除

対象ダウタイム

ダウタイムID / 定期設定名称	ホストID	サービスID	開始時間	終了時間
<div>設定済み</div> S	Server1	HTTP	2020/01/07 13:30:00	2020/01/07 15:30:00

発行

閉じる

これでダウンタイム設定が解除されました。

### 10.4.1 ダウンタイムの定期設定

毎週・毎月など定期的なサーバのメンテナンスに合わせ、自動でダウンタイムの設定が行えます。ダウンタイム画面より「定期設定」のリンクを押し、表示された画面で「新規作成」ボタンを押します。

定期ダウンタイムの設定画面となりますので設定を入力します。

名称	定期設定の名称を入力します。
対象	ダウンタイムを設定するホストやサービス、グループを指定します。
コメント	自由に入力できます。
間隔	毎週または毎月を選択し、ダウンタイムとする時間帯を指定します。

例として毎月第2水曜日の午前2時~3時の間、ネットワークのセキュリティアップデートを対象とした設定を登録します。

設定が登録されました。

ダowntime

ダowntime | 定期設定

Q 絞り込み条件設定

パターン

☒ 毎週
☒ 毎月

対象の絞り込み

全て

Q 検索

リセット

+ 新規作成

	名称	対象	関連対象	パターン	開始時間	終了時間	期間	コメント	登録者	操作
<input type="checkbox"/>	セキュリティアップデート	ホスト: Osaka-FW, Osaka-Switch, Osaka-Switch2		毎月: 第2水曜日	02:00:00	03:00:00	1 時間 0 分	大阪拠点 NW	admin	<div></div> <div></div>

ダowntime一覧へ移動し確認すると、定期設定からダowntimeの予約が表示されていることが分かります。

ダowntime

ダowntime | 定期設定

Q 絞り込み条件設定

+ 新規作成

	ダowntimeID / 定期設定名称	ホストID	サービスID	開始時間	終了時間	期間	種類	コメント	トリガーID	登録者	操作
<input type="checkbox"/>	設定予約 セキュリティアップデート	Osaka-FW		2020/01/08 02:00:00	2020/01/08 03:00:00	1 時間 0 分	固定	[定期設定]大阪拠点 NW	N/A	admin	<div></div> <div></div>
<input type="checkbox"/>	設定予約 セキュリティアップデート	Osaka-Switch		2020/01/08 02:00:00	2020/01/08 03:00:00	1 時間 0 分	固定	[定期設定]大阪拠点 NW	N/A	admin	<div></div> <div></div>
<input type="checkbox"/>	設定予約 セキュリティアップデート	Osaka-Switch2		2020/01/08 02:00:00	2020/01/08 03:00:00	1 時間 0 分	固定	[定期設定]大阪拠点 NW	N/A	admin	<div></div> <div></div>

これでダowntimeの定期設定が完了しました。

ダowntimeの開始時間の 5 分前に「設定予約」のダowntimeが「設定済み」のダowntimeとなり、次の「設定予約」が作成されます。

## ? 間隔の指定について

### 第 n ○曜日

その月の一番初めに指定した曜日が現れた日を第一とします。

例) 2020 年 01 月の第一月曜日 → 2020 年 01 月 06 日

### 月によって存在しない日(31 日等)

存在しない月はダowntimeが予定されません。

例) 2020 年 2 月時点で 30 日を指定 → 2020 年 03 月 30 日

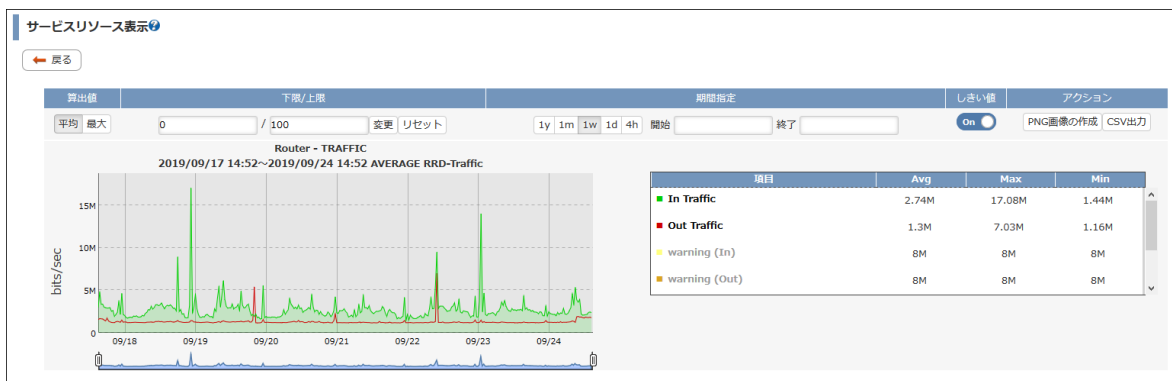
## 10.5 グラフ画面

X-MON にはパフォーマンスデータをもとにグラフ描画する機能があります。

グラフが作成できるサービスには「サービス一覧」でグラフアイコンが表示されます。

Router (gw-router)	PING		2019-09-24 14:55:58	0日と06時間11分30秒	1/3	PING OK - Packet loss = 0%, RTA = 2.38 ms
	TRAFFIC		2019-09-24 14:56:39	0日と00時間00分42秒	1/3	OK - 受信 2.09Mbits 送信 1.76Mbits

グラフアイコンを押すことで該当のサービスのパフォーマンスグラフを確認することが出来ます。



グラフの操作に関してはオンラインヘルプの「付録」の「グラフ操作方法」をご確認ください。

## 10.6 稼働率画面

「監視メニュー」の「稼働率」で開く画面です。

ホストやサービスの稼働率を表示・ダウンロードすることが出来ます。稼働率の算出式に関してはオンラインヘルプをご確認ください。

稼働率を求めたいホストと算出期間を選択し「算出」ボタンをクリックすると稼働率を算出し、結果が出力されます。

「EXCEL ダウンロード」ボタンをクリックすると、算出結果を EXCEL ファイル形式でダウンロードできます。

**Server1(www-server)**

ホスト稼働率

UP	DOWN	UNREACHABLE
100.000 %	0.000 %	0.000 %

サービス稼働率

サービスID	OK	WARNING	CRITICAL	UNKNOWN
HTTP	0.000 %	0.000 %	100.000 %	0.000 %
POP3	89.054 %	0.000 %	10.946 %	0.000 %
SMTP	89.821 %	0.000 %	10.179 %	0.000 %

## 10.7 ホストの一括登録

本リファレンスでのホストの登録方法は手動で行いましたが、実際監視を実施しているとホストの数は数十台から数百台まで多い場合があると思います。

X-MON では独自機能として、ネットワークからホストを検出し登録する事が可能です。

「管理者メニュー」の「ホスト・サービス管理」を開き、「ネットワークからホストを検出する」ボタンを押します。

図 ホスト一覧

ID	名称	IPアドレス/FQDN	エスカレーション		監視エージェント状況		
<input type="checkbox"/> Router	? gw-router	10.0.100.101	有効 0	無効 0	NRPE -	SNMP -	WMI -

ホストの検出画面になります。ここでネットワークの範囲を指定しその検出されたホストを登録する事が出来ます

図 ホストの検出

第3オクテット  
連続していれば範囲指定可能

第4オクテット  
連続していれば範囲指定可能

第1オクテット

第2オクテット

ここでは例として、10.0.100.200～10.0.100.255 までを範囲としてみます。

入力が出来たら「新しいホストをネットワークから検出する」を押します。

図 ホストの検出

ホストの検出

← ホスト一覧へ

検出するIPアドレス範囲

10 . 0 . 100 - 100 . 200 - 255

← ホスト一覧へ → 新しいホストをネットワークから検出する

検出が出来ると下記のような画面となります。

図 ホストの検出完了

ホストの検出

← ホスト一覧へ

検出するIPアドレス範囲

10 . 0 . 100 - 100 . 200 - 255

検出結果

	ホストID	IPアドレス	MACアドレス
<input checked="" type="checkbox"/>	IP_10.0.100.200 種別: 物理サーバ 監視設定: ホスト監視を行う	10.0.100.200	
<input checked="" type="checkbox"/>	IP_10.0.100.203 種別: 物理サーバ 監視設定: ホスト監視を行う	10.0.100.203	
<input checked="" type="checkbox"/>	IP_10.0.100.204 種別: 物理サーバ 監視設定: ホスト監視を行う	10.0.100.204	
<input checked="" type="checkbox"/>	IP_10.0.100.208 種別: 物理サーバ 監視設定: ホスト監視を行う	10.0.100.208	

## ■ チェックボックス

チェックしたホストの登録を行います。

検出したホストが既に登録されている場合、「登録済み IP」と表示され、登録することができません。



- ホスト ID

任意のホスト ID を入力します。

新規作成時のみ設定が可能であり、変更はできません。

- 種別

ホストの種別を選択します。

- 監視設定

監視パッケージ管理 - 監視パッケージ一覧を指定します。

監視パッケージを使用する場合、選択された監視パッケージに登録されたサービスが一括登録されます。監視パッケージを使用せず、ホストの登録のみの場合、「監視設定は行わない」を選択します。

- SNMP バージョン

- SNMP ポート番号

- コミュニティ名

SNMP の情報を入力します。

全てのホストに対して同じ値が設定されますので注意してください。

- WMI アカウント

- WMI パスワード

Windows の監視を行う際に、WMI の設定を入力します。

全てのホストに対して同じ値が設定されますので注意してください。

登録するホストの情報が入力出来たら画面一番下の「選択したホストを登録する」を押してください。

X-MON の再起動ボタンを押して再起動を実施すれば設定は完了です。

## 11 X-MON のデフォルトの監視項目

X-MON3.0.8 以降の X-MON では X-MON サーバ自身のプロセスの監視がございます。

ホストID (ホスト名称)	サービスID	監視ステータス	最終チェック時刻	経過時間	試行回数	ステータス情報
X-MON (X-MON)	PING	OK	2019-09-13 11:19:01	20日と22時間05分18秒	1/3	PING OK - Packet loss = 0%, RTA = 0.05 ms
	XMON_CHECK_DISK	OK	2019-09-13 11:19:01	20日と22時間04分51秒	1/1	DISK OK - free space: / 5055 MB (61.81% in use=99%)
	XMON_CHECK_cron	OK	2019-09-13 11:18:58	20日と22時間04分24秒	1/1	PROCS OK: 1 process with command name 'crond'
	XMON_CHECK_nscd	OK	2019-09-13 11:19:03	20日と22時間03分56秒	1/1	PROCS OK: 1 process with command name 'nscd'
	XMON_CHECK_postfix	OK	2019-09-13 11:19:05	20日と22時間03分29秒	1/1	PROCS OK: 8 processes with command name 'postres'
	XMON_CHECK_postfix	OK	2019-09-13 11:18:57	20日と22時間03分02秒	1/1	PROCS OK: 1 process with command name 'master'
	XMON_CHECK_redis	OK	2019-09-13 11:18:57	8日と16時間37分27秒	1/1	PROCS OK: 1 process with command name 'redis-server'
	XMON_CHECK_rrdcached	OK	2019-09-13 13:23:45	20日と22時間02分35秒	1/1	PROCS OK: 1 process with command name 'rrdcached'
	XMON_CHECK_rsyslog	OK	2019-09-13 11:18:59	20日と22時間02分07秒	1/1	PROCS OK: 1 process with command name 'rsyslogd'
	XMON_CHECK_snmp	OK	2019-09-13 11:18:56	20日と22時間01分40秒	1/1	PROCS OK: 1 process with command name 'snmpd'
	XMON_CHECK_snmptrap	OK	2019-09-13 11:18:58	20日と22時間01分13秒	1/1	PROCS OK: 1 process with command name 'snmptrapd'
	XMON_CHECK_snmpd	OK	2019-09-13 13:23:41	20日と22時間00分45秒	1/1	PROCS OK: 2 processes with command name 'snmpd'
	XMON_CHECK_supervisord	OK	2019-09-13 11:19:05	8日と16時間37分27秒	1/1	PROCS OK: 1 process with command name 'supervisord'

プロセスが停止すると CRITICAL を検知しますので、その場合は以下をご参考に対応をお願いします。

サービス ID	XMON_CHECK_DISK
説明	DISK の容量を監視します
復旧方法	# df -Th コマンドなどで容量を確認し、不要ファイルを削除してください。

サービス ID	XMON_CHECK_cron
説明	cron を監視します
復旧方法	(RHEL6)# /etc/init.d/crond restart (RHEL7)# systemctl restart crond.service

サービス ID	XMON_CHECK_nscd
説明	nscd プロセスを監視します。
復旧方法	(RHEL6)# /etc/init.d/nscd restart (RHEL7)# systemctl restart nscd.service

サービス ID	XMON_CHECK_pgsql
説明	postgresql プロセスを監視します。
復旧方法	(RHEL6)# /etc/init.d/postgresql restart (RHEL7)# systemctl restart postgresql.service

サービス ID	XMON_CHECK_postfix
説明	postfix プロセスを監視します。
復旧方法	(RHEL6)# /etc/init.d/postfix restart (RHEL7)# systemctl restart postfix.service

サービス ID	XMON_CHECK_redis
説明	redis プロセスを監視します。
復旧方法	(RHEL6)# /etc/init.d/redis restart (RHEL7)# systemctl restart redis.service

サービス ID	XMON_CHECK_rrdcached
説明	X-MON-rrdcached プロセスを監視します
復旧方法	(RHEL6)# /etc/init.d/X-MON-rrdcached restart (RHEL7)# systemctl restart X-MON-rrdcached.service

サービス ID	XMON_CHECK_rsyslog
説明	rsyslog プロセスを監視します。
復旧方法	(RHEL6)# /etc/init.d/rsyslog restart (RHEL7)# systemctl restart rsyslog.service

サービス ID	XMON_CHECK_snmp
説明	snmp プロセスを監視します。
復旧方法	(RHEL6)# /etc/init.d/snmpd restart (RHEL7)# systemctl restart snmpd.service

サービス ID	XMON_CHECK_snmptrap
説明	snmptrap プロセスを監視します。
復旧方法	(RHEL6)# /etc/init.d/snmptrapd restart (RHEL7)# systemctl restart snmptrapd.service

サービス ID	XMON_CHECK_snmpptt
説明	snmpptt プロセスを監視します。
復旧方法	(RHEL6)# /etc/init.d/snmpptt restart (RHEL7)# systemctl restart snmpptt.service

サービス ID	XMON_CHECK_supervisord
説明	supervisord プロセスを監視します。
復旧方法	(RHEL6)# /etc/init.d/supervisord restart (RHEL7)# systemctl restart supervisord.service

再起動を実施しても改善しないや、DISK の不要なファイルがわからないなどございましたら X-MON テクニカルサポートにご連絡をお願いします。

## 12 さいごに

---

X-MON の基本的な設定方法、監視の概念や基本について解説してきました。

X-MON には多種多様な現代のシステムを監視できるような機能、プラグインやレポート機能や構成管理など ITIL に準ずる機能も備わっております。

X-MON の基本を本リファレンスにて理解して頂き、一つでも多くの監視が速やかに実施出来、対応できるような運用の参考になればと思います。

高度な設定については、それぞれのマニュアルやオンラインマニュアルをご参考ください。