

株式会社エクストランス

X-MON3

X-MON 監視リファレンス

2018/9 版

まえがき

本書はX-MON3系列を用いてLinuxサーバを監視する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。

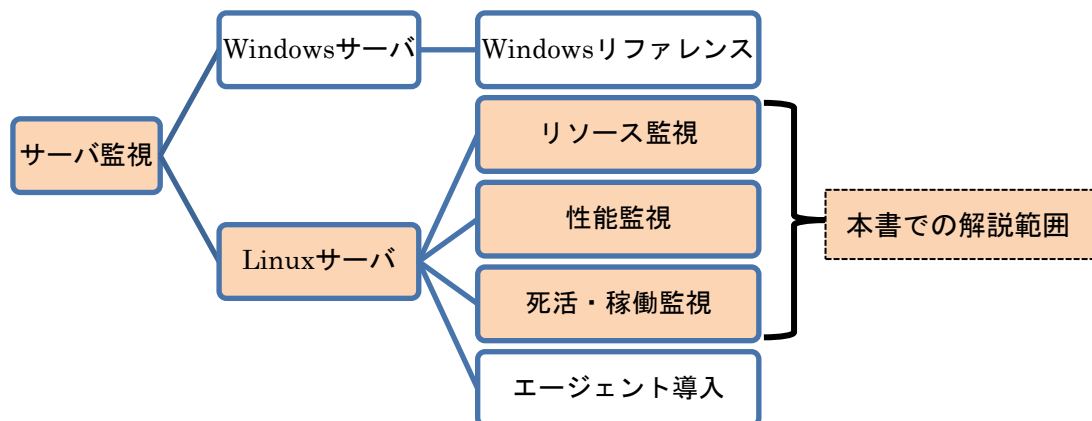
また、X-MONの操作画面はお使いのOSやブラウザによって異なる場合がございます。

- ・ 本書における解説環境

X-MON ver 3.7 以降

X-MONの入門リファレンスや監視エージェント導入、Windowsサーバの監視方法など本書以外のマニュアルをご参照ください。

詳細はX-MONサポートページにログインしてご確認ください。



X-MON サポートサイト

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

2013 年 1 月

改定履歴	
2013 年 1 月	初版
2016 年 7 月	第二版
2018 年 9 月	第三版

Copyright © 2004-2018 X-TRANS, Inc. All Rights Reserved.

目次

1	はじめに 本書で使用する監視について	6
1.1	監視パッケージとは.....	6
1.2	監視パッケージ一覧.....	6
1.2.1	Linux 標準監視一覧	7
1.2.2	Linux Web サーバ監視一覧	7
1.2.3	Linux メールサーバ監視一覧.....	7
1.2.4	Linux MySQL サーバ監視一覧.....	8
1.2.5	Linux PostgreSQL サーバ監視一覧	9
1.3	サンプルネットワーク	9
1.4	監視の設定方法について	10
1.4.1	監視パッケージの場合.....	10
1.4.2	新規にサービス追加する場合.....	11
1.5	監視設定の編集時の注意点.....	12
2	Linux 標準監視 (共通監視)	13
2.1	PING 監視	13
2.1.1	監視設定例.....	13
2.1.2	設定項目一覧	14
2.2	NRPE 経由での SWAP 監視	14
2.2.1	監視設定例.....	14
2.2.2	設定項目一覧	15
2.3	NRPE 経由でのディスク監視	15
2.3.1	監視設定例.....	16
2.3.2	設定項目一覧	17
2.4	NRPE 経由でのロードアベレージ監視.....	17
2.4.1	監視設定例.....	18
2.4.2	監視パッケージ登録時のタイムアウト値について.....	18
2.4.3	設定項目一覧	18
2.5	CPU 監視	19
2.5.1	X-MON における CPU 使用率の算出仕様.....	19
2.5.2	サーバのコア数による最大値について	20
2.5.3	監視設定例.....	20
2.5.4	設定項目一覧	21
2.6	TRAFFIC 監視.....	22
2.6.1	X-MON におけるトラフィック量の算出仕様.....	22

2.6.2	監視設定例	22
2.6.3	しきい値について	23
2.6.4	設定項目一覧	24
2.7	メモリ監視(Cache/buffer 除外)	25
2.7.1	監視設定例	25
2.7.2	設定項目一覧	26
2.8	SSH 監視	26
2.8.1	監視設定例	27
2.8.2	設定項目一覧	27
2.9	NRPE 経由での NTP サーバ OS 時刻監視	27
2.9.1	監視設定例	27
2.9.2	他のチェックコマンドとの違い	28
2.9.3	設定項目一覧	29
3	Linux Web サーバ監視	30
3.1	FTP 監視	30
3.1.1	監視設定例	30
3.1.2	設定項目一覧	30
3.2	HTTP 監視	30
3.2.1	監視設定例	31
3.2.2	設定項目一覧	37
3.3	HTTPS 監視	38
3.3.1	監視設定例	38
3.3.2	設定項目一覧	39
3.4	SSL の証明書有効期限監視	40
3.4.1	監視設定例	40
3.4.2	設定項目一覧	41
3.5	SSL の証明書有効期限間監視(SNI)	42
3.5.1	監視設定例	42
3.5.2	設定項目一覧	42
3.6	Web コンテンツ改ざん監視	43
3.6.1	監視設定例	43
3.6.2	監視の復旧方法について	44
3.7	Web コンテンツ改ざん監視 (一括監視)	46
3.7.1	設定項目一覧	47
3.8	その他の Web サービス監視のチェックコマンド	47
3.8.1	HTTP IP ベースバーチャルホストの監視,HTTPS IP ベースバーチャルホスト	

の監視	48
3.8.2 HTTP ネームベースバーチャルホストの監視、HTTPS ネームベースバーチャルホストの監視	48
3.8.3 NRPE 経由での HTTP 監視、NRPE 経由での HTTPS 監視	48
4 Linux メールサーバ監視	49
4.1 POP3 監視	49
4.1.1 監視設定例	49
4.1.2 設定項目一覧	50
4.2 POPS 監視	50
4.2.1 監視設定例	50
4.2.2 設定項目一覧	51
4.3 SMTP 監視	51
4.3.1 監視設定例	51
4.3.2 サブミッションポートの監視	52
4.3.3 設定項目一覧	53
4.4 SMTPS 監視	53
4.4.1 監視設定例	53
4.4.2 設定項目一覧	54
4.5 IMAP4 監視	54
4.5.1 監視設定例	54
4.5.2 設定項目一覧	55
4.6 IMAPS 監視	55
4.6.1 監視設定例	56
4.6.2 設定項目一覧	56
4.7 NRPE 経由でのメールキュー監視	57
4.7.1 監視設定例	57
4.7.2 設定項目一覧	58
4.8 その他のメールサービス監視のチェックコマンド	59
4.8.1 NRPE 経由での IMAP4 監視,NRPE 経由での IMAPS 監視	59
4.8.2 NRPE 経由での POP3 監視,NRPE 経由での POPS 監視	59
4.8.3 NRPE 経由での SMTP 監視,NRPE 経由での SMTPS 監視	59
4.8.4 メールキュー監視	59
5 Linux MySQL サーバ監視	61
5.1 MySQL 監視	61
5.1.1 監視設定例	61
5.1.2 設定項目一覧	62

5.2	NRPE 経由での MySQL 監視	62
5.2.1	監視設定例	62
5.2.2	設定項目一覧	63
6	Linux PostgreSQL サーバ監視	64
6.1	PostgreSQL 監視	64
6.1.1	監視設定例	64
6.1.2	設定項目一覧	65
6.2	NRPE 経由での PostgreSQL 監視	65
6.2.1	監視設定例	66
6.2.2	設定項目一覧	67

1 はじめに 本書で使用する監視について

本書は Linux サーバへの監視登録について基本的な技術解説を行います。
監視登録するプラグインについては、監視パッケージに含まれるプラグインです。
それぞれに共通するプラグインと、目的別（監視パッケージ毎）に解説を行いますので、読み方として始めから読み進める、目次を参考に目的の監視プラグインのみを参考に頂く方法でも対応できるようにしております。

また監視ホスト自体の X-MON への登録、監視ホストが提供するサービス、アプリケーション、エージェントについては監視ホストにインストール・設定が実施されている事を前提としておりますのでご了承ください。

監視プラグインについてはオンラインマニュアルにも詳細な仕様や情報が記載されておりますので併せてご参照頂ければと思います。

X-MON の入門リファレンスや監視エージェント導入、Windows サーバの監視方法など本書以外のマニュアルをご参照ください。

1.1 監視パッケージとは

監視パッケージとは X-MON で監視登録する際に複数のサービスを一括で定義する事が出来ます。Windows 用、Linux 用などがあり、ホストで監視するサービスが決まっている時など纏めて登録する事が出来ます。

1.2 監視パッケージ一覧

Linux で使用できる監視パッケージは5個あります。名前に目的が書かれていますが、サーバの提供するサービスの目的に合わせて選定されております。

Linux 標準監視
Linux Web サーバ監視
Linux メールサーバ監視
Linux MySQL 監視
Linux PostgreSQL 監視

この中で「Linux 標準監視」は他の Linux 用監視パッケージにも含まれている標準の死活監視、リソース監視設定です。そのため、本書では共通している監視については標準部分で解説し、その他監視パッケージ毎の目的別に解説を行います。

次の章より、一覧を記載します。黄色で色づけしている部分は Linux 標準監視（各パッケージの共通部分）になります。また、そのプラグインのサービス登録名、どの監視エージェントを使用するかも記載しておりますので、予めサーバに必要なかどうか確認にもご利用頂けます。

1.2.1 Linux 標準監視一覧

テンプレート名	登録サービス ID	使用エージェント
PING 監視	PING	使用なし (ICMP 監視)
NRPE 経由での SWAP 監視	SWAPMEMORY	NRPE
NRPE 経由でのディスク監視	DISK	NRPE
NRPE 経由でのロードアベレージ監視	LOAD	NRPE
CPU 監視	CPU	SNMP
TRAFFIC 監視	TRAFFIC-LAN	SNMP
	TRAFFIC-WAN	SNMP
メモリ監視(Cache/buffer 除外)	MEMORY	SNMP
SSH 監視	SSH	使用なし (ポート番号監視)
NRPE 経由での NTP サーバ OS 時刻監視	CheckTime	NRPE

1.2.2 Linux Web サーバ監視一覧

テンプレート名	登録サービス ID	使用エージェント
PING 監視	PING	使用なし (ICMP 監視)
NRPE 経由での SWAP 監視	SWAPMEMORY	NRPE
NRPE 経由でのディスク監視	DISK	NRPE
NRPE 経由でのロードアベレージ監視	LOAD	NRPE
CPU 監視	CPU	SNMP
TRAFFIC 監視	TRAFFIC-LAN	SNMP
	TRAFFIC-WAN	SNMP
メモリ監視(Cache/buffer 除外)	MEMORY	SNMP
SSH 監視	SSH	使用なし (ポート番号監視)
NRPE 経由での NTP サーバ OS 時刻監視	CheckTime	NRPE
FTP 監視	FTP	使用なし (ポート番号監視)
HTTP 監視	HTTP	使用なし (ポート番号監視)
HTTPS 監視	HTTPS	使用なし (ポート番号監視)
SSL の証明書有効期限監視	SSL-CERT	使用なし
Web コンテンツ改ざん監視	HTTP-INCIDENT	使用なし

1.2.3 Linux メールサーバ監視一覧

テンプレート名	登録サービス ID	使用エージェント
PING 監視	PING	使用なし (ICMP 監視)

NRPE 経由での SWAP 監視	SWAPMEMORY	NRPE
NRPE 経由でのディスク監視	DISK	NRPE
NRPE 経由でのロードアベレージ監視	LOAD	NRPE
CPU 監視	CPU	SNMP
TRAFFIC 監視	TRAFFIC-LAN	SNMP
	TRAFFIC-WAN	SNMP
メモリ監視(Cache/buffer 除外)	MEMORY	SNMP
SSH 監視	SSH	使用なし (ポート番号監視)
NRPE 経由での NTP サーバ OS 時刻監視	CheckTime	NRPE
POP3 監視	POP3	使用なし (ポート番号監視)
POPS 監視	POP3S	使用なし (ポート番号監視)
SMTP 監視	SMTP	使用なし (ポート番号監視)
	SMTP-Submission	使用なし (ポート番号監視)
SMTPTS 監視	SMTPTS	使用なし (ポート番号監視)
IMAP4 監視	IMAP	使用なし (ポート番号監視)
IMAPS	IMAPS	使用なし (ポート番号監視)
NRPE 経由でのメールキュー監視	MAILQ	NRPE

1.2.4 Linux MySQL サーバ監視一覧

テンプレート名	登録サービス ID	使用エージェント
PING 監視	PING	使用なし (ICMP 監視)
NRPE 経由での SWAP 監視	SWAPMEMORY	NRPE
NRPE 経由でのディスク監視	DISK	NRPE
NRPE 経由でのロードアベレージ監視	LOAD	NRPE
CPU 監視	CPU	SNMP
TRAFFIC 監視	TRAFFIC-LAN	SNMP
	TRAFFIC-WAN	SNMP
メモリ監視(Cache/buffer 除外)	MEMORY	SNMP
SSH 監視	SSH	使用なし (ポート番号監視)
NRPE 経由での NTP サーバ OS 時刻監視	CheckTime	NRPE
MySQL 監視	MySQL	使用なし (ポート番号監視)
NRPE 経由での MySQL 監視	MySQL-NRPE	NRPE

1.2.5 Linux PostgreSQL サーバ監視一覧

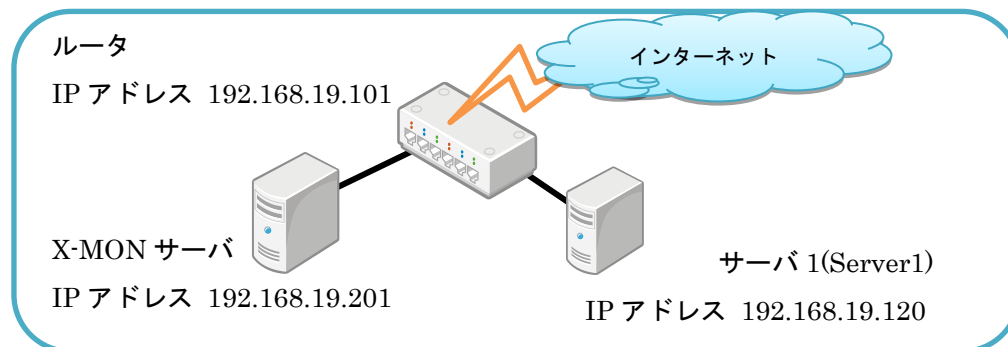
テンプレート名	登録サービス名 ID	使用エージェント
PING 監視	PING	使用なし (ICMP 監視)
NRPE 経由での SWAP 監視	SWAPMEMORY	NRPE
NRPE 経由でのディスク監視	DISK	NRPE
NRPE 経由でのロードアベレージ監視	LOAD	NRPE
CPU 監視	CPU	SNMP
TRAFFIC 監視	TRAFFIC-LAN	SNMP
	TRAFFIC-WAN	SNMP
メモリ監視(Cache/buffer 除外)	MEMORY	SNMP
SSH 監視	SSH	使用なし (ポート番号監視)
NRPE 経由での NTP サーバ OS 時刻監視	CheckTime	NRPE
PostgreSQL 監視	PGSQL	使用なし (ポート番号監視)
NRPE 経由での PostgreSQL 監視	PGSQL-NRPE	NRPE

1.3 サンプルネットワーク

本リファレンス内で使用する設定例のネットワークです。

図の「サーバ 1」に対して監視設定をするように解説を行います。

図 サンプルネットワーク



サーバ 1 のホスト登録時の情報

ホスト ID		Server1
ホスト名称		サーバ 1
IP アドレス		192.168.19.120
SNMP 認証設定	バージョン	v2c
	コミュニティ名	xtrans

1.4 監視の設定方法について

監視の設定方法について簡単に説明します。

1.4.1 監視パッケージの場合

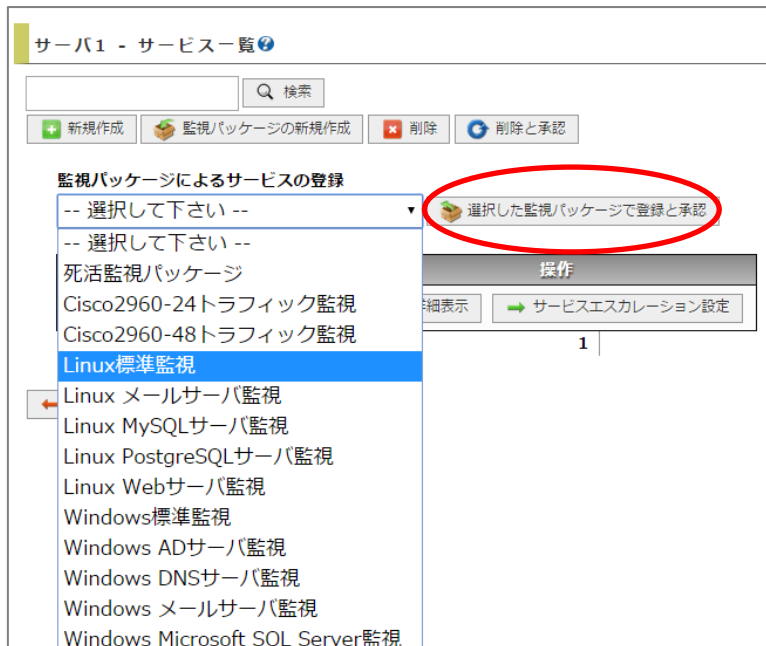
監視パッケージで監視設定する場合はホストを登録後、X-MON の[管理者メニュー] の[ホスト・サービス管理] にて該当ホストの[サービス設定]を開きます。

図 サービス設定



監視パッケージが選択出来ますので、任意のパッケージを選択し、[選択した監視パッケージで登録と承認] をしてください。

図 監視パッケージ



監視パッケージに登録されているサービス監視が設定されます。

このまま X-MON を再起動して反映する事も出来ますし、[詳細表示] を開くと[編集] メニューもありますので、この場で設定を変更する事も可能です。また、必要ないサービスがある場合は、チェックボックスにチェックを入れて削除する事も可能です。

図 監視パッケージ設定

サーバ1 - サービス一覧

設定を追加し反映しました。

検索

新規作成 監視パッケージの新規作成 削除 削除と承認

監視パッケージによるサービスの登録

-- 選択して下さい -- 選択した監視パッケージで登録と承認

サービスID	エスケーション設定数	操作	
<input type="checkbox"/> CheckTime	有効: 0, 無効: 0	→ 詳細表示	→ サービスエスケーション設定
<input type="checkbox"/> CPU	有効: 0, 無効: 0	→ 詳細表示	→ サービスエスケーション設定
<input type="checkbox"/> DISK	有効: 0, 無効: 0	→ 詳細表示	→ サービスエスケーション設定
<input type="checkbox"/> LOAD	有効: 0, 無効: 0	→ 詳細表示	→ サービスエスケーション設定
<input type="checkbox"/> MEMORY	有効: 0, 無効: 0	→ 詳細表示	→ サービスエスケーション設定
<input type="checkbox"/> PING	有効: 0, 無効: 0	→ 詳細表示	→ サービスエスケーション設定
<input type="checkbox"/> SSH	有効: 0, 無効: 0	→ 詳細表示	→ サービスエスケーション設定

1.4.2 新規にサービス追加する場合

監視パッケージを使用せず、1つずつも監視追加は可能です。

監視パッケージで監視設定する場合はホストを登録後、X-MON の[管理者メニュー] の[ホスト・サービス管理] にて該当ホストの[サービス設定]を開きます。

図 サービス設定

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	エスケーション設定数
<input type="checkbox"/> Server1	サーバ1	127.0.0.1	有効: 0, 無効: 0

→ 詳細表示 → サービス設定 → ホストエスケーション設定

左上の[新規作成] を開くと新規にサービスの追加が可能です。

図 新規作成

サーバ1 - サービス一覧

検索

新規作成 削除 削除と承認

監視パッケージによるサービスの登録

-- 選択して下さい -- 選択した監視パッケージで登録と承認

図 サービスの作成

1.5 監視設定の編集時の注意点

設定した監視設定を編集する際ですが、[サービス監視用コマンド] の選択 BOX が [DHCP サービス監視] が表示されます。

図 注意点

これは X-MON の仕様によるもので、監視テンプレート（チェックコマンド）を絞り込むためのグループなので、その下の選択 BOX で監視テンプレートが選択されていれば問題はなく、直接監視には影響はありません。

設定時に気になるユーザ様はグループを選択し直して頂いて設定も出来ますが、その際にオプションで入力していた値がクリアされます。

そのため、グループの選択はそのまま [DHCP サービス監視] のままで編集を実施してください。本件については、弊社内にて改善計画中です。

図 注意点

2 Linux 標準監視（共通監視）

Linux 標準監視では、サーバを監視する基本的な監視を含めています。

また、他の監視パッケージにも標準監視は全て含まれています。

監視には NRPE、SNMP を使用する物もありますので予め監視ホストへインストールしてください。

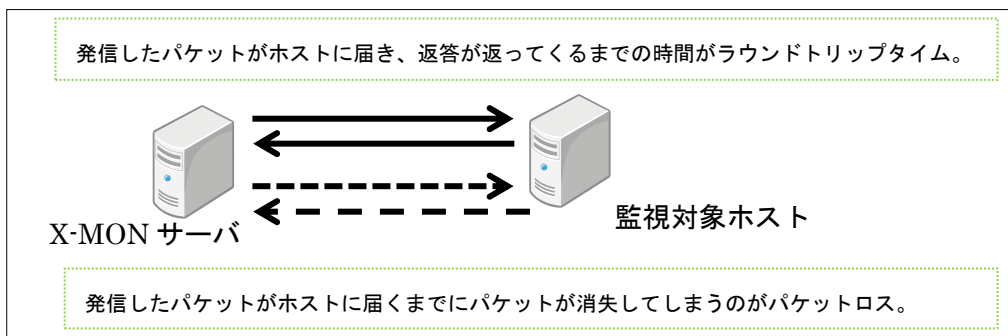
2.1 PING 監視

監視グループ	チェックコマンド
死活監視	PING 監視

PING による監視対象ホストの死活監視を行います。

ラウンドトリップタイム（RTT）またはパケットロス率がしきい値を超える場合は、監視ステータスを WARNING または CRITICAL にします。

図 PING 監視



2.1.1 監視設定例

標準的な死活監視においては、設定はデフォルトで充分ですが、シビアに監視する際はタイムアウトの秒数（デフォルト 10 秒）を短くしたり応答時間であるラウンドトリップタイムのしきい値を変更したり調整してください。

図 設定例

サービス監視用コマンド	
死活監視	
PING監視	
ラウンドトリップタイムWARNINGしきい値(平均ms)	300
パケットロス率WARNINGしきい値(%)	30
ラウンドトリップタイムCRITICALしきい値(平均ms)	500
パケットロス率CRITICALしきい値(%)	50
PING送信回数(回)	5
タイムアウト(秒)	10

2.1.2 設定項目一覧

ラウンドトリップタイム WARNING しきい値(平均 ms)	ラウンドトリップタイムがこの値を超えた場合、監視ステータスを WARNING にします。
パケットロス率 WARNING しきい値(%)	パケットロス率がこの値を超えた場合、監視ステータスを WARNING にします。
ラウンドトリップタイム CRITICAL しきい値(平均 ms)	ラウンドトリップタイムがこの値を超えた場合、監視ステータスを CRITICAL にします。
パケットロス率 CRITICAL しきい値(%)	パケットロス率がこの値を超えた場合、監視ステータスを CRITICAL にします。
PING 送信回数(回)	1 回の監視につき実行する PING の回数を指定します。
タイムアウト(秒)	監視対象ホストから指定した秒数以上応答がない場合、チェックを終了し、監視ステータスを CRITICAL にします。

2.2 NRPE 経由での SWAP 監視

監視グループ	チェックコマンド
Linux/Unix 系リソース監視(NRPE)	NRPE 経由での SWAP 監視

NRPE を利用して、監視対象ホストのスワップメモリの空き容量の監視を行います。スワップメモリの空き容量がしきい値を下回る場合は、監視ステータスを WARNING または CRITICAL にします。

スワップメモリはサーバの用途により、使用量が異なりますのでサーバの状況をよく確認してからしきい値を決定してください。またしきい値は空き容量をパーセントで計算されます。

2.2.1 監視設定例

Server1 ではスワップメモリは 1G 割り当てられているとします。

残りのスワップメモリが 80%以下で WARNING,60%以下で CRITICAL とする場合は下記のように設定します。

図 SWAP 監視

サービス監視用コマンド

Linux/Unix系リソース監視(NRPE)
NRPE経由でのSWAP監視
WARNINGしきい値(%) 80
CRITICALしきい値(%) 60
タイムアウト(秒) 15

2.2.2 設定項目一覧

WARNING しきい値(%)	監視対象ホストのスワップメモリの空き容量がこの値を下回った場合、監視ステータスを WARNING にします。
CRITICAL しきい値(%)	監視対象ホストのスワップメモリの空き容量がこの値を下回った場合、監視ステータスを CRITICAL にします。
タイムアウト(秒)	監視対象ホストから指定した秒数以上応答がない場合、チェックを終了し、監視ステータスを CRITICAL にします。

2.3 NRPE 経由でのディスク監視

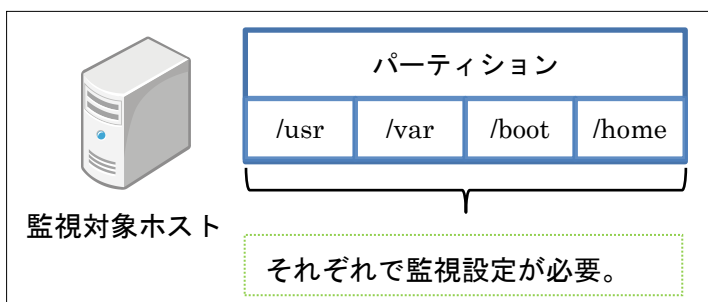
監視グループ	チェックコマンド
Linux/Unix 系リソース監視(NRPE)	NRPE 経由での DISK 監視

NRPE を利用して、監視対象ホストのディスク空き容量の監視を行います。

ディスク空き容量がしきい値を下回る場合は、監視ステータスを WARNING または CRITICAL にします。

1 つの監視設定で設定できるパーティション（マウントポイント）は 1 つとなります。そのため、複数のパーティションを監視するには複数の監視設定が必要となります。

図 ディスク監視



また、しきい値は空き容量をパーセントで計算します。そのため、同じしきい値で違うパーティションの監視設定をする際は注意してください。

例：/usr には 50G,/var には 100G 割り当てられている。

WARNING のしきい値を 20%,CRITICAL のしきい値を 10%とした場合、

/usr は残り 10G で WARNING,残り 5G で CRITICAL を検知

/var は残り 20G で WARNING,残り 10G で CRITICAL を検知

となります。

2.3.1 監視設定例

入力するパーティションの入力欄は「対象ディレクトリパス」となっています。

図 監視設定

サービス監視用コマンド

Linux/Unix系リソース監視(NRPE) ▼

NRPE経由でのディスク監視 ▼

対象ディレクトリパス

空き容量WARNINGしきい値(%) 20

空き容量CRITICALしきい値(%) 10

タイムアウト(秒) 15

通常のパーティションを監視するようでしたら、/var や/usr をそのまま入力します。

図 パーティション指定

対象ディレクトリパス

パーティションになっていない、/ 以下にマウントされている場合は入力してもマウントポイントの容量が表示されます。

- ・例 1 : /tmp はパーティションになっておらず、/ 以下にマウントされている。
この場合、/tmp を入力しても/ の容量が返ってきます。

```
# df -Th
Filesystem      Type サイズ  使用  残り  使用% マウント位置
/dev/sda3      ext3   7.7G  1.9G  5.4G  26% /
/dev/sda1      ext3    99M   12M   82M  13% /boot
```

- ・例 2 : /dev/sdb を/var/www としてマウントしている場合は/var/www を指定する事で/var/www の容量の監視が可能です。

```
# df -Th
Filesystem      Type サイズ  使用  残り  使用% マウント位置
/dev/sda3      ext3   7.7G  1.9G  5.4G  26% /
/dev/sda1      ext3    99M   12M   82M  13% /boot
/dev/sdb       ext3   9.9G  151M   9.2G   2% /var/www
```

デバイス名でも指定は可能です。

- ・例 3:/dev/sda1 と/boot としてマウントしている場合、/dev/sda1 を指定する事で/boot の容量の監視が可能。

図 デバイス名で指定

対象ディレクトリパス	<div style="border: 2px solid red; padding: 2px;">/dev/sda1</div>
------------	---

```
# df -Th
Filesystem      Type サイズ  使用  残り  使用% マウント位置
/dev/sda1      ext4   485M   30M  430M    7% /boot
```

監視結果はマウントポイントの名前で表示されます。

図 監視結果

現在の状態:	正常(OK) (0日間と 00時間02分18秒前より継続しています。)
ステータス情報:	DISK OK - free space: /boot 429 MB (93% inode=99%):
パフォーマンスデータ:	/boot=29MB;387;435;0;484

それぞれ環境に合わせて設定ください。

2.3.2 設定項目一覧

対象ディレクトリパス	監視するパーティションをデバイスのフルパスあるいはマウントポイントへのフルパスで指定します。
空き容量 WARNING しきい値(%)	監視対象ホストの空き容量がこの値を下回った場合、監視ステータスを WARNING にします。
空き容量 CRITICAL しきい値(%)	監視対象ホストの空き容量がこの値を下回った場合、監視ステータスを CRITICAL にします。
タイムアウト(秒)	監視対象ホストから指定した秒数以上応答がない場合、チェックを終了し、監視ステータスを CRITICAL にします。

2.4 NRPE 経由でのロードアベレージ監視

監視グループ	チェックコマンド
Linux/Unix 系リソース監視(NRPE)	NRPE 経由でのロードアベレージ監視

NRPE を利用して、監視対象ホストのロードアベレージの監視を行います。

監視ホスト上では w コマンド、uptime コマンドで確認できます。

ロードアベレージがしきい値を超える場合は、監視ステータスを WARNING または CRITICAL にします。サーバ環境にあわせてしきい値を調整してください。

2.4.1 監視設定例

しきい値はカンマ区切りでの入力となります。

入力欄にも記載がありますが、1 分,5 分,15 分 の順で入力します。

図 しきい値入力

WARNINGしきい値(1分,5分,15分)	12,10,8
CRITICALしきい値(1分,5分,15分)	15,15,15

2.4.2 監視パッケージ登録時のタイムアウト値について

X-MON3.0.5 をご使用で監視パッケージにてロードアベレージ監視を追加した際、タイムアウト値が「24,20,16」と自動入力されています。

図 タイムアウト値バグ

タイムアウト(秒)	24,20,16
-----------	----------

これは X-MON3.0.5 上でのバグになります。今後のアップデートで改善予定ですので大変恐れ入りますが、「10」など任意の秒数へ修正をお願いします。

図 タイムアウト値修正後

タイムアウト(秒)	10
-----------	----

2.4.3 設定項目一覧

WARNING しきい値(1 分,5 分,15 分)	カンマ区切りで 1 分間の平均のしきい値、5 分間の平均のしきい値、15 分間の平均のしきい値を指定します。監視対象ホストのロードアベレージがこの値を超えた場合、監視ステータスを WARNING にします。
CRITICAL しきい値(1 分,5 分,15 分)	カンマ区切りで 1 分間の平均のしきい値、5 分間の平均のしきい値、15 分間の平均のしきい値を指定します。監視対象ホストのロードアベレージがこの値を超えた場合、監視ステータスを CRITICAL にします。
タイムアウト(秒)	監視対象ホストから指定した秒数以上応答がない場合、チェックを終了し、監視ステータスを CRITICAL にします。

2.5 CPU 監視

監視グループ	チェックコマンド
Linux/Unix 系リソース監視(SNMPv1,v2 対応)	CPU 監視

SNMP(バージョン 1 または 2c)を利用して、監視対象ホストの CPU 使用率(ユーザプロセス、nice プロセス、システムプロセス合計の CPU 使用率)の監視を行います。CPU の使用率がしきい値を超える場合は、監視ステータスを WARNING または CRITICAL にします。X-MON から SNMP での情報取得ができない場合は、監視ステータスを UNKNOWN にします。

2.5.1 X-MON における CPU 使用率の算出仕様

監視ホスト上では top コマンドの部分で確認出来ます。

```
top - 16:31:00 up 24 days, 17 min, 3 users, load average: 1.37, 0.53, 0.22
Tasks: 103 total, 2 running, 101 sleeping, 0 stopped, 0 zombie
Cpu(s): 0.3%us, 8.0%sy, 0.0%ni, 0.0%id, 89.4%wa, 1.0%hi, 1.3%si, 0.0%st
Mem: 1026080k total, 1017472k used, 8608k free, 2220k buffers
Swap: 1072248k total, 4388k used, 1047860k free, 702576k cached
```

ユーザ CPU

システム CPU

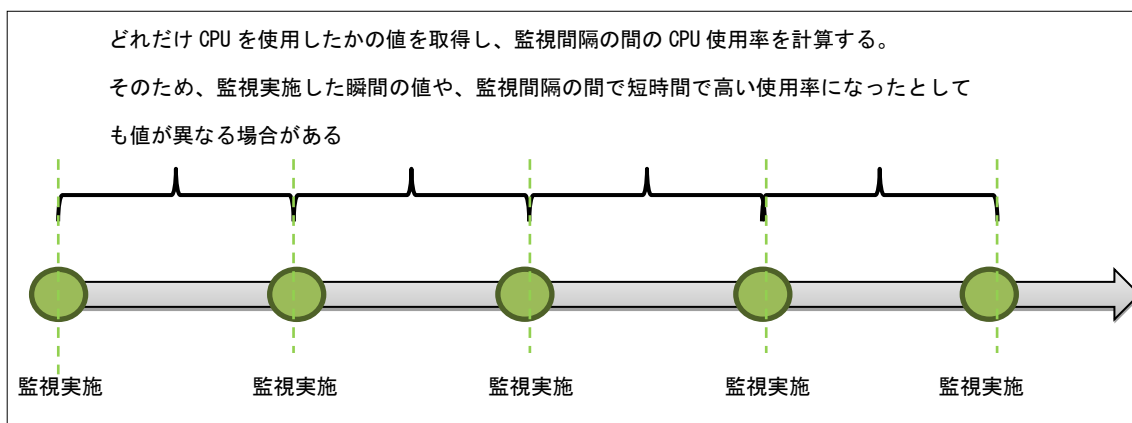
niceCPU

アイドル CPU

監視ホスト上でコマンドで確認出来る使用率は「その瞬間の使用率」となっており、X-MON から SNMP を使用して CPU 使用率を監視する場合は「監視間隔の間に CPU を使った時間から平均使用率を算出」しています。

そのため、短時間で CPU 使用率が 100%など高い数値を出した場合において監視間隔が長いと、X-MON 上では CPU 使用率が低くなる場合があります。

図 CPU 使用率の算出



2.5.2 サーバのコア数による最大値について

CPU のコア数によって最大値が変わります。

最大値は「コア数×100%」です。

そのため、4core 搭載のサーバでしたら最大値は 400%となります。

監視ホスト上では下記コマンドで確認出来ます。

* 4 コアの例

```
$ cat /proc/cpuinfo | grep processor
processor : 0
processor : 1
processor : 2
processor : 3
```

また、top コマンドからでも確認出来ます。top コマンドでサーバ情報を表示中に「1」を押すと CPU がコアごとに表示されます。

```
top - 18:05:32 up 37 min, 1 user, load average: 0.00, 0.00, 0.00
Tasks: 118 total, 1 running, 117 sleeping, 0 stopped, 0 zombie
Cpu0  :  0.0%us,  0.0%sy,  0.0%ni, 100.0%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu1  :  0.0%us,  0.0%sy,  0.0%ni, 95.2%id,  0.0%wa,  0.0%hi,  4.8%si,  0.0%st
Cpu2  :  0.0%us,  0.8%sy,  0.0%ni, 95.2%id,  0.0%wa,  0.0%hi,  4.0%si,  0.0%st
Cpu3  :  0.0%us,  0.0%sy,  0.0%ni, 96.7%id,  0.0%wa,  0.0%hi,  3.3%si,  0.0%st
Mem:   2057640k total, 270300k used, 1787340k free, 16320k buffers
Swap:  2096472k total,  0k used, 2096472k free, 145068k cached
```

最大値を 100%で指定したい場合は

監視グループ	チェックコマンド
Linux/Unix 系リソース監視(SNMPv1,v2 対応)	CPU 監視(コア数分割)

をご使用ください。

2.5.3 監視設定例

サンプルネットワークで Server1 に対して監視設定する場合は下記のようになります。ホスト登録時に SNMP 情報を指定している場合は自動的に入力されます。指定していない場合は入力してください。

- ・ ユーザ CPU タイム OID
- ・ nice CPU タイム OID
- ・ システム CPU OID
- ・ アイドル CPU OID

通常の Linux/Unix にて net-snmp を使用する際はデフォルトで結構です。

図 設定例

サービス監視用コマンド	
Linux/Unix系リソース監視(SNMPv1,v2対応) ▾	
CPU監視 ▾	
SNMPバージョン	2c ▾
SNMPコミュニティ名	xtrans
ユーザCPUタイムOID	.1.3.6.1.4.1.2021.11.50.0
nice CPUタイムOID	.1.3.6.1.4.1.2021.11.51.0
システムCPUタイムOID	.1.3.6.1.4.1.2021.11.52.0
アイドルCPUタイムOID	.1.3.6.1.4.1.2021.11.53.0
WARNINGしきい値(%)	80
CRITICALしきい値(%)	90
タイムアウト(秒)	10

2.5.4 設定項目一覧

SNMP バージョン	監視対象ホストの SNMP バージョンを指定します
SNMP コミュニティ名	監視対象ホストの SNMP コミュニティ名を指定します。
ユーザ CPU タイム OID	監視対象ホストのユーザプロセスのCPU 占有時間を取得するカウンタ型の OID を指定します。初期値では一般的な Linux サーバのユーザプロセスのCPU 占有時間を取得する「ssCpuRawUser」のOIDが指定されています。
nice CPU タイム OID	監視対象ホストの実行優先度 (nice)を変更したユーザプロセスの CPU 占有時間を取得するカウンタ型の OID を指定します。初期値では一般的な Linux サーバの実行優先度 (nice)を変更したユーザプロセスの CPU 占有時間を取得する「ssCpuRawNice」のOIDが指定されています。
システム CPU タイム OID	監視対象ホストのシステムプロセスのCPU 占有時間を取得するカウンタ型の OID を指定します。初期値では一般的な Linux サーバのシステムプロセスのCPU 占有時間を取得する「ssCpuRawSystem」のOIDが指定されています。
アイドル CPU タイム OID	監視対象ホストのCPUの空き状態の時間を取得するカウンタ型の OID を指定します。初期値では一般的な Linux サーバの CPU の空き状態の時間を取得する「ssCpuRawIdle」のOIDが指定されています。
WARNING しきい値(%)	監視対象ホストの CPU 使用率がこの値を超えた場合、監視ステータスを WARNING にします。CPU 使用率の最大値は「コア数×100%」となります。

CRITICAL しきい値(%)	監視対象ホストの CPU 使用率がこの値を超えた場合、監視ステータスを CRITICAL にします。CPU 使用率の最大値は「コア数×100%」となります。
タイムアウト(秒)	監視対象ホストから指定した秒数以上応答がない場合、チェックを終了し、監視ステータスを UNKNOWN にします。

2.6 TRAFFIC 監視

監視グループ	チェックコマンド
Linux/Unix 系リソース監視(SNMPv1,v2 対応)	TRAFFIC 監視

SNMP(バージョン 1 または 2c)を利用して、監視対象ホストのネットワークインタフェースのトラフィックの監視を行います。

トラフィックがしきい値を超える場合は、監視ステータスを WARNING または CRITICAL にします。X-MON から SNMP での情報取得ができない場合は、監視ステータスを UNKNOWN にします。

監視パッケージ一覧では「TRAFFIC-LAN」と「TRAFFIC-WAN」の2つが追加されます。「TRAFFIC-LAN」はサーバの eth1 を、「TRAFFIC-WAN」は eth0 を監視します。NIC の確認方法は [2.6.2 監視設定例](#) をご参照ください。

2.6.1 X-MON におけるトラフィック量の算出仕様

CPU 監視と同じですが、監視のタイミングの「瞬間値」ではなく「監視間隔の間のトラフィック量から監視間隔の時間で平均的に算出」します。そのため監視間隔の間に短時間で多くのトラフィックが流れたとしても X-MON 上ではトラフィック量が少なくなる場合があります。

例として監視間隔が 5 分の間に合計 30Mbps のトラフィックが流れたとします。そうすると 1 分平均 6Mbps になりますので X-MON 上では 6Mbps のトラフィックが流れた、と認識されます。この 6Mbps が監視設定で指定するしきい値と比較されます。そのためトラフィック監視は監視間隔を短くする事をおすすめします。

2.6.2 監視設定例

トラフィックの値を取得するには、どの OID が監視対象の NIC に対応しているかを調べる必要があります。

X-MON3.2.0 以降では、管理画面から SNMPWALK 実行機能がございます。その他コマンドで調べるには X-MON サーバからコマンドで確認します。

■構文

```
# snmpwalk -v 2c -c <コミュニティ名> <IP アドレス> ifDesc
```

サンプルネットワークに当てはめると

- ・ コミュニティ名 : xtrans
- ・ IP アドレス : 192.168.19.120

となりますので、その場合は

```
# snmpwalk -v 2c -c xtrans 192.168.19.120 ifDesc
```

を発行します。

■発行例

```
# snmpwalk -v 2c -c xtrans 192.168.19.120 ifDescr
```

```
IF-MIB::ifDescr.1 = STRING: lo
```

```
IF-MIB::ifDescr.2 = STRING: eth0
```

```
IF-MIB::ifDescr.3 = STRING: eth1
```

この場合、「eth0 は ifDescr.2 に対応」し、「eth1 は ifDescr.3 に対応」となります。

監視設定を見てみましょう。画像は新規作成時の画像となります。

図 新規作成時

サービス監視用コマンド	
Linux/Unix系リソース監視(SNMPv1,v2対応) ▾	
TRAFFIC監視 ▾	
SNMPバージョン	2c ▾
SNMPコミュニティ名	xtrans
受信トラフィックOID	.1.3.6.1.2.1.2.2.1.10.2
送信トラフィックOID	.1.3.6.1.2.1.2.2.1.16.2

初期値で

受信トラフィック OID 「.1.3.6.1.2.1.2.2.1.10.2」

送信トラフィック OID 「.1.3.6.1.2.1.2.2.1.16.2」

となっています。OID の最後の数字が先ほど調べた「ifDescr.○」の数字となります。そうすると、初期値で監視をすると最後の数字が2ですので eth0 を監視するとなります。eth1 を監視したい場合は「ifDescr.3」ですので最後の数字を3にします。

eth1 の受信トラフィック OID は「.1.3.6.1.2.1.2.2.1.10.3」

eth1 の送信トラフィック OID は「.1.3.6.1.2.1.2.2.1.16.3」

複数の NIC がある場合はこのようにして OID を指定してください。

2.6.3 しきい値について

WARNING と CRITICAL のしきい値を入力しますが単位が「bit」での指定となります。そのため、桁数が大きくなりますので気を付けてください。

byte で確認するには8で割る必要があります。

・新規作成時の初期値

WARNING しきい値(bit) 8000000bit -> 1000000 バイト -> 約 1M バイト

CRITICAL しきい値(bit)10000000bit -> 1250000 バイト -> 約 1.25M バイト

図 しきい値

受信トラフィックWARNINGしきい値(bit)	8000000
送信トラフィックWARNINGしきい値(bit)	8000000
受信トラフィックCRITICALしきい値(bit)	10000000
送信トラフィックCRITICALしきい値(bit)	10000000

NIC の転送量により、しきい値を設定してください。

2.6.4 設定項目一覧

SNMP バージョン	監視対象ホストの SNMP バージョンを指定します
SNMP コミュニティ名	監視対象ホストの SNMP コミュニティ名を指定します。
受信トラフィック OID	監視対象の NIC の受信トラフィックを取得するカウンタ型の OID を指定します。初期値では一般的な Linux サーバの NIC 「eth0」 の受信トラフィックを取得する 「ifInOctets」 の OID が指定されています。
送信トラフィック OID	監視対象の NIC の送信トラフィックを取得するカウンタ型の OID を指定します。初期値では一般的な Linux サーバの NIC 「eth0」 の送信トラフィックを取得する 「ifOutOctets」 の OID が指定されています。
受信トラフィック WARNING しきい値(bit)	監視対象 NIC の受信トラフィック量がこの値を超えた場合、監視ステータスを WARNING にします。
送信トラフィック WARNING しきい値(bit)	監視対象 NIC の送信トラフィック量がこの値を超えた場合、監視ステータスを WARNING にします。
受信トラフィック CRITICAL しきい値(bit)	監視対象 NIC の受信トラフィック量がこの値を超えた場合、監視ステータスを CRITICAL にします。
送信トラフィック CRITICAL しきい値(bit)	監視対象 NIC の送信トラフィック量がこの値を超えた場合、監視ステータスを CRITICAL にします。
タイムアウト(秒)	監視対象ホストから指定した秒数以上応答がない場合、チェックを終了し、監視ステータスを UNKNOWN にします。

2.7 メモリ監視(Cache/buffer 除外)

監視グループ	チェックコマンド
Linux/Unix 系リソース監視(SNMPv1,v2 対応)	メモリ監視(Cache/buffer 除外)

SNMP(バージョン 1 または 2c)を利用して、監視対象ホストの実メモリ使用率とスワップメモリ使用率の監視を行います。この監視における物理メモリ使用量とは、総メモリ量から未使用のメモリ(キャッシュされていないメモリ, free)量とキャッシュメモリ(キャッシュされているメモリ, buffer と cached)量を引いたメモリ量を指します。

スワップメモリの使用率や実メモリ使用率がしきい値を超える場合は、監視ステータスを WARNING または CRITICAL にします。X-MON から SNMP での情報取得ができない場合は、監視ステータスを UNKNOWN にします。

■監視ホストでの確認

free -m

	total	used	free	shared	buffers	cached
Mem:	499	184	314	0	16	136
-/+ buffers/cache:		32	466			
Swap:	1023	0	1023			

通常のメモリ監視ではこの値を監視する。
500M の中で 184M 使用なので 36.8% の使用率となる。

Cache/buffer 除外メモリ監視ではこの値を監視する。
500M の中で 32M 使用なので 6% の使用率となる。

2.7.1 監視設定例

通常、監視ホストでメモリ使用量を確認する際は GByte や MByte 単位で確認していると思いますが、監視では「使用率」となるためしきい値はパーセントで設定します。また、監視設定ではスワップメモリの使用率と実メモリの使用率を指定出来ます。監視の検知はどちらかのしきい値を超えた段階で検知します。

図 監視設定例

サービス監視用コマンド

Linux/Unix系リソース監視(SNMPv1,v2対応) ▾

メモリ監視(Cache/Buffer除外) ▾

SNMPバージョン 2c ▾

SNMPコミュニティ名 xtrans

スワップメモリWARNINGしきい値(%) 10

実メモリWARNINGしきい値(%) 90

スワップメモリCRITICALしきい値(%) 20

実メモリCRITICALしきい値(%) 95

タイムアウト(秒) 10

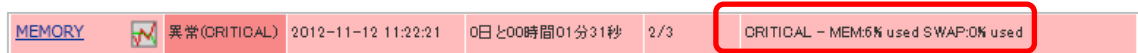
監視が正常に行われている場合は、画像のように実メモリは MEM、スワップは SWAP として使用率が表示されます。

図 メモリ監視



注意点としては監視を検知した場合に実メモリのしきい値を超えたのかスワップのしきい値を超えて検知したのか表示はされませんので監視ホストを直接確認して下さい。

図 検知時



2.7.2 設定項目一覧

SNMP バージョン	監視対象ホストの SNMP バージョンを指定します
SNMP コミュニティ名	監視対象ホストの SNMP コミュニティ名を指定します。
スワップメモリ WARNING しきい値(%)	監視対象ホストのスワップメモリ使用率がこの値を超えた場合、監視ステータスを WARNING にします。
実メモリ WARNING しきい値(%)	監視対象ホストの実メモリ使用率がこの値を超えた場合、監視ステータスを WARNING にします。
スワップメモリ CRITICAL しきい値(%)	監視対象ホストのスワップメモリ使用率がこの値を超えた場合、監視ステータスを CRITICAL にします。
実メモリ CRITICAL しきい値(%)	監視対象ホストの実メモリ使用率がこの値を超えた場合、監視ステータスを CRITICAL にします。
タイムアウト(秒)	監視対象ホストから指定した秒数以上応答がない場合、チェックを終了し、監視ステータスを UNKNOWN にします。

2.8 SSH 監視

監視グループ	チェックコマンド
SSH サービス監視	SSH 監視

監視対象ホストの SSH サービスの監視を行います。

監視対象ホストで SSH サービスが起動していない場合、監視ステータスを CRITICAL にします。

X-MON サーバから SSH 接続できるように監視ホストに予め設定をお願いします。

2.8.1 監視設定例

通常、SSH はポート番 22 番を使用します。デフォルトの設定でも 22 番が指定されますので、監視ホストの設定で違うポート番号を指定している場合はその番号を指定してください。

図 監視設定例

サービス監視用コマンド	
SSHサービス監視	
SSH監視	
ポート番号	22
タイムアウト(秒)	10

2.8.2 設定項目一覧

ポート番号	監視対象となる SSH サービスのポート番号を指定します。
タイムアウト(秒)	監視対象ホストから指定した秒数以上応答がない場合、チェックを終了し、監視ステータスを CRITICAL にします。

2.9 NRPE 経由での NTP サーバ OS 時刻監視

監視グループ	チェックコマンド
時刻監視	NRPE 経由での NTP サーバ OS 時刻監視

NRPE を利用して、監視ホストのシステム時刻のずれの監視を行います。

誤差（秒数）がしきい値を超える場合は、監視ステータスを WARNING または CRITICAL にします。比較対象の NTP サーバから時刻が取得できない場合は、監視ステータスを UNKNOWN にします。

監視パッケージ一覧で設定した場合は比較する NTP サーバとして「ntp.jst.mfeed.ad.jp」が指定されています。

図 監視パッケージでの設定

NTPサーバホスト名またはIPアドレス	ntp.jst.mfeed.ad.jp
---------------------	---------------------

2.9.1 監視設定例

監視設定において[NTP サーバホスト名または IP アドレス] と[ポート番号] と[タイムアウト] を指定します。この 2 つは監視ホストと比較する NTP サーバの情報を指定します。

一般的な NTP サーバ（公開されている public なもの）はポート番号は 123 番を使用しますが、自社内用などでポート番号を変更している場合はそこで使用されているポート番号を指定してください。

図 監視設定例

サービス監視用コマンド	
時刻監視	
NRPE経由でのNTPサーバOS時刻監視	
NTPサーバホスト名またはIPアドレス	ntp.jst.mfeed.ad.jp
ポート番号	123
タイムアウト(秒)	10
WARNINGしきい値(秒)	1
CRITICALしきい値(秒)	2
NRPEタイムアウト(秒)	15

時刻のズレを検知した場合はステータス情報には「Offset <ズレている秒数>」が表示されます。

図 検知時

CheckTime	異常 (CRITICAL)	2012-11-12 12:01:24	4日と20時間21分 39秒	3/3	NTP CRITICAL: Offset -32.20409432 secs
-----------	------------------	---------------------	-------------------	-----	---

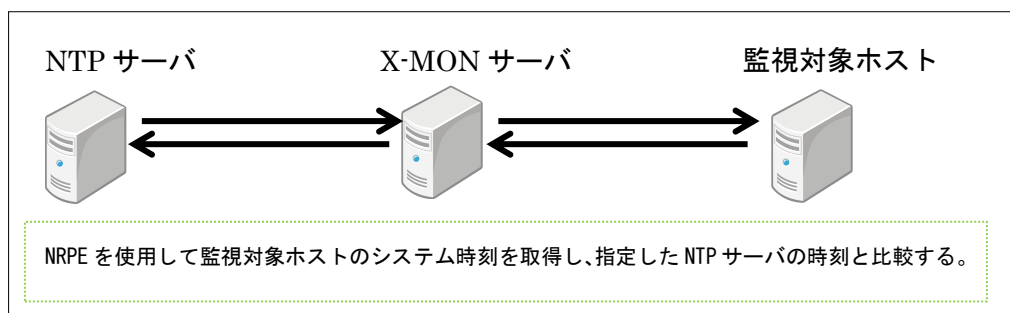
2.9.2 他のチェックコマンドとの違い

時刻監視は他にもチェックコマンドがありますので解説します。

2.9.2.1 NRPE 経由での NTP サーバ OS 時刻監視

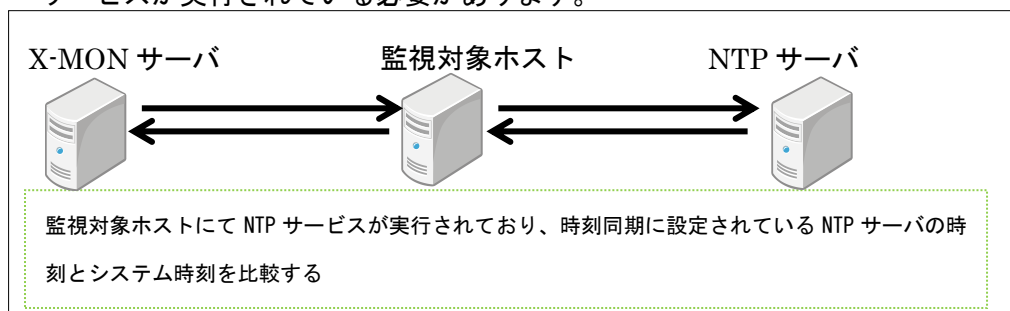
本章で説明している項目となります。

NRPE を利用して、監視ホストのシステム時刻を指定した NTP サーバと比較します。



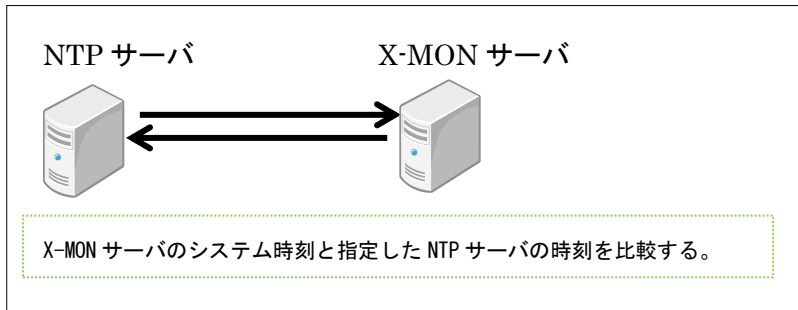
2.9.2.2 NRPE 経由での NTP サーバ動作監視

NRPE を利用して、監視対象ホストの NTP サービスにて設定されている時刻同期するための NTP サーバとシステム時刻のズレの監視を行います。監視対象ホストにて NTP サービスが実行されている必要があります。



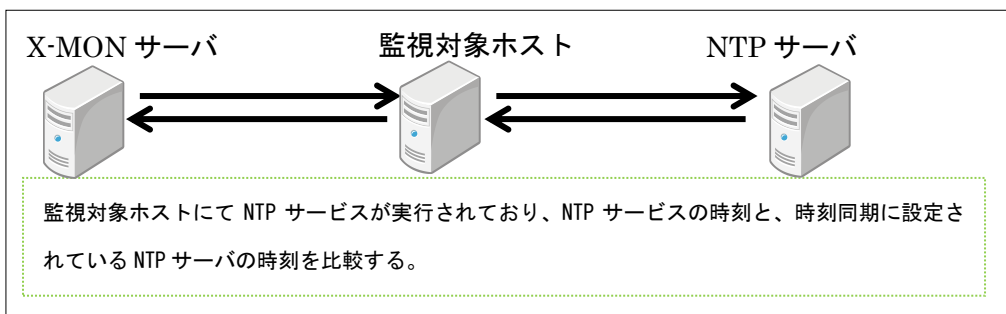
2.9.2.3 NTP サーバ OS 時刻監視

この監視は X-MON サーバと指定した NTP サーバとの時刻のズレを監視します。そのため X-MON サーバに使用してください。



2.9.2.4 NTP サーバ動作監視

監視対象ホストが提供している NTP サービスの時刻が、NTP サービスにて設定されている時刻同期するための NTP サーバと時刻のズレの監視を行います。監視対象ホストにて NTP サービスが実行されている必要があります。



2.9.3 設定項目一覧

NTP サーバホスト名または IP アドレス	監視対象ホストの時刻と比較する NTP サーバのホスト名または IP アドレスを指定します。
ポート番号	時刻を比較する NTP サーバのポート番号を指定します。
タイムアウト(秒)	監視対象ホストから指定した秒数以上応答がない場合、チェックを終了し、監視ステータスを CRITICAL にします。
WARNING しきい値(秒)	監視対象ホストと NTP サーバとの時刻の誤差がこの値を超えた場合、監視ステータスを WARNING にします。
CRITICAL しきい値(秒)	監視対象ホストと NTP サーバとの時刻の誤差がこの値を超えた場合、監視ステータスを CRITICAL にします。
NRPE タイムアウト(秒)	監視対象ホストから指定した秒数以上応答がない場合、チェックを終了し、監視ステータスを CRITICAL にします。

3 Linux Web サーバ監視

Linux Web サーバ監視では Web サービスを提供しているホストに対する監視パッケージです。

内容は Linux 標準監視と Web サービスに特化した監視項目です。

項目一覧は [1.2.2 Linux Web サーバ監視一覧](#)をご参照ください。

3.1 FTP 監視

監視グループ	チェックコマンド
FTP サービス監視	FTP 監視

監視対象ホストの FTP サービスの監視を行います。

接続できない場合、監視ステータスを CRITICAL にします。

3.1.1 監視設定例

通常、FTP はポート番号 21 番を使用します。デフォルトの設定でも 21 番が指定されますので、監視ホストの設定で違うポート番号を指定している場合はその番号を指定してください。

図 監視設定例

3.1.2 設定項目一覧

ポート番号	監視対象である FTP サービスのポート番号を指定します。
タイムアウト(秒)	監視対象ホストからの応答時間がこの値を超えた場合、監視ステータスを CRITICAL にします。

3.2 HTTP 監視

監視グループ	チェックコマンド
Web サービス監視	HTTP 監視

Web ページの監視を行います。

HTTP ステータスコードを指定しないとき、接続が可能(HTTP ステータスコードが 200 番台または 300 番台)な場合、監視ステータスを OK にします。クライアント側のエラー(HTTP ステータスコードが 400 番台)の場合、監視ステータスを WARNING に

します。サーバ側のエラー(HTTP ステータスコードが 500 番台または 100 未満)やタイムアウトの場合、監視ステータスを CRITICAL にします。

X-MON サーバからは IP アドレスでアクセスします。

3.2.1 監視設定例

3.2.1.1 基本的な設定例

サンプルネットワークでの構成の場合、IP アドレスは 192.168.19.120 のため、X-MON サーバからは

http://192.168.19.120

のアドレスでアクセスする形となります。オプションで設定を入れる事が可能です。

新規作成の際のデフォルトの設定は下記となります。

図 デフォルトの設定

The screenshot shows a configuration window titled "サービス監視用コマンド" (Service Monitoring Command). It contains the following fields and values:

Field	Value
Webサービス監視 (dropdown)	Webサービス監視
HTTP監視 (dropdown)	HTTP監視
URLパス	/
ポート番号	80
BASIC認証ユーザ名	none
BASIC認証パスワード	●●●●
タイムアウト(秒)	10
応答時間WARNINGしきい値(秒)	4
応答時間CRITICALしきい値(秒)	8
HTTPステータスコードの指定 (dropdown)	無効
HTTPステータスコード	
検出文字列	

URL パスは、IP アドレスの最後にパスを追加が出来ます。

デフォルトは「/」です。例えば、

http://192.168.19.120/x-mon/

を監視する URL パスとする場合は

/x-mon/

と指定します。

図 URL パス

The screenshot shows a configuration field for "URLパス" (URL Path). The value entered is "/x-mon/", which is highlighted with a red rectangular box.

厳密にファイル名まで指定する事も可能です。

使用用途としては、「index.html はページビューをカウントしているため、kanshi.html という監視するためだけのページを配置させ、X-MON からのアクセスを別ファイルにする」などです。

図 http://192.168.19.120/kanshi.html にアクセスする場合

URLパス	/kanshi.html
-------	--------------

3.2.1.2 ポート番号

ポート番号を指定できます。アプリケーションでポート番号を指定して web 管理画面を使用している場合に指定します。

http://192.168.19.120:8080/

を監視したい場合はポート番号に 8080 を指定します。

図 ポート番号指定

URLパス	/
ポート番号	8080

3.2.1.3 Basic 認証を使用する場合

監視するページに Basic 認証がかかっている場合はユーザ名とパスワードを入力出来ます。

デフォルトではユーザ名は none パスワードも none になっています。

監視するページに Basic 認証が設定されていない場合、入力された情報は使用されません。

図 Basic 認証

BASIC認証ユーザ名	none
BASIC認証パスワード	● ● ● ●

3.2.1.4 HTTP ステータスコードの指定

HTTP はアクセスした際にステータスコードを返答します。

この章の初めにも記載しておりますがデフォルトは下記です。

HTTP ステータスコードが 400 番台 : WARNING

HTTP ステータスコードが 500 番台または 100 未満:CRITICAL

しかし、運用上で指定のステータスコードについては既知の問題や仕様で障害としない場合も出てきますのでその場合はこのオプションを使用してください。

また、カンマ「,」を使用する事で複数のステータスコードを指定出来ます。

HTTP ステータスコードの指定を有効にするには、設定を有効にしてください。

図 ステータスコードの有効

HTTPステータスコードの指定	無効 ▾	⇒	HTTPステータスコードの指定	有効 ▾
-----------------	------	---	-----------------	------

例) Basic 認証のユーザ名、パスワードが不明な場合

監視する URL に Basic 認証が設定されているが、情報がわからずアクセスした場合は認証が出来ないためステータスコードは 401 が返答されます。

「HTTP サービス自身は正常に稼働しているためこれは障害と見なさない」とする場合は HTTP ステータスコードの指定を有効にし、HTTP ステータスコードに 401 を指定します。

図 ステータスコード指定

HTTPステータスコードの指定	有効 ▾
HTTPステータスコード	401

例) X-MON サーバからアクセス許可がされていない場合

特定の IP アドレスからのみ HTTP に接続が出来る場合等、アクセス権がない場合はステータスコード 403 が返答されます。

「HTTP サービス自身は正常に稼働しているためこれは障害と見なさない」とする場合は HTTP ステータスコードの指定を有効にし、HTTP ステータスコードに 403 を指定します。

図 ステータスコード指定

HTTPステータスコードの指定	有効 ▾
HTTPステータスコード	403



ステータスコードを有効にする場合の注意点

ステータスコードを有効にした場合、そのステータスコード以外は CRITICAL を検知します。

例えば、URL パスをデフォルトの設定で正常にアクセスできる環境とします。

その場合に HTTP ステータスの設定を 500 に設定し監視を行います。

図 ステータスコード指定

URLパス	/
ポート番号	80
BASIC認証ユーザ名	none
BASIC認証パスワード	●●●●
タイムアウト(秒)	10
応答時間WARNINGしきい値(秒)	4
応答時間CRITICALしきい値(秒)	8
HTTPステータスコードの指定	有効 ▾
HTTPステータスコード	500

正常に監視出来ているのでステータスコードは 200 番が返答されますが、ステータスコード 500 番を指定しているので、アクセスは出来るにもかかわらず監視上では CRITICAL となります。

図 ステータスコードの注意点

正常にアクセスが出来ていてステータスコードの指定がない場合

現在のステータスは、**正常(OK)**
0日間と 23時間23分52秒前より継続しています。

HTTP OK: HTTP/1.1 200 OK - 268 bytes in 0.001 second response time



ステータスコードが監視検知される。

現在のステータスは、**異常(CRITICAL)**
0日間と 00時間01分16秒前より継続しています。

HTTP CRITICAL Invalid HTTP response received from host: HTTP/1.1 200 OK

正常なステータスコードの返答が来てもステータスコードの指定があるので CRITICAL を検知する。

デフォルトでは WARNING 検知となる 400 番台を検知しても同様に指定ステータスコード以外になりますので CRITICAL となります。

3.2.1.5 検出文字列

監視するページで表示される文字列（ページのソース内）で監視が出来ます。

バーティカルバー(|)で区切ると複数の文字列を指定が出来、正規表現を使用する事も可能です。文字列に使用できるのは英数字と平仮名、カタカナ、漢字です。

例) データベースとの接続が true の場合に OK、false の場合に NG を表示する HTML を準備し、それにアクセスして文字列監視をします。

しきい値としては OK の文字列があれば正常、それ以外は CRITICAL となります。

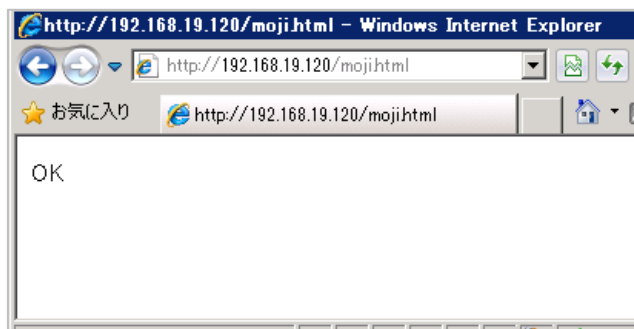
監視する HTML が moji.html とする場合は下記のように設定します。

図 検出文字列設定

URLパス	/moji.html
ポート番号	80
BASIC認証ユーザ名	none
BASIC認証パスワード	●●●●
タイムアウト(秒)	10
応答時間WARNINGしきい値(秒)	4
応答時間CRITICALしきい値(秒)	8
HTTPステータスコードの指定	無効 ▾
HTTPステータスコード	
検出文字列	OK

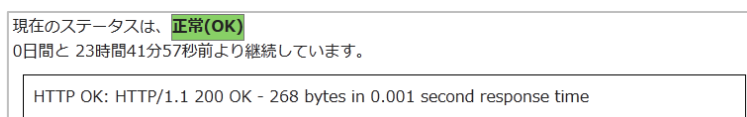
実際ブラウザでアクセスした際の例は下記です。

図 ブラウザでアクセス



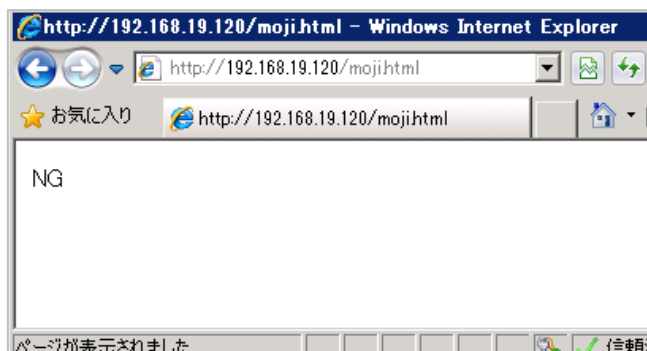
正常に監視が出来ている場合は HTTP 監視と同じステータス情報が表示されます。

図 正常時ステータス情報



CRITICAL にするために、表示の文字列が NG になるようにしてみます。

図 ブラウザでアクセス



OK 以外の文字列が表示されているので CRITICAL を検知します。

HTTP のステータスコードは 200 番なので正常ですが、「pattern not found」と文字列検知にて CRITICAL になっています。

図 CRITICAL 時ステータス情報



正規表現も使用可能です。

例として、下記条件のような HTML である success.html を作成するとします。

プログラムが正常な動作をしていれば「success<処理にかかった秒数>sec」を表示する
 プログラムが異常な動作をしていれば「nonsuccess<処理にかかった秒数>sec」を表示する

例えば処理にかかった時間が 30 秒でしたら「success30sec」と表示されます。

90 秒処理して異常な動作の場合は「nonsuccess90sec」と表示されます。

検知する文字列を「success」に設定だけだと両パターンでも監視は OK になってしまうため、「文字列の先頭であり、success の後は 1 文字以上の文字とする」とします。

指定すべき文字列は「^success*」となります。

図 監視設定

URLパス	/success.html
ポート番号	80
BASIC認証ユーザ名	none
BASIC認証パスワード	●●●●
タイムアウト(秒)	10
応答時間WARNINGしきい値(秒)	4
応答時間CRITICALしきい値(秒)	8
HTTPステータスコードの指定	無効 ▼
HTTPステータスコード	
検出文字列	^success*

ブラウザで確認では正常に動作している表示となっているため、監視でも正常が検知されます。

図 ブラウザでアクセス

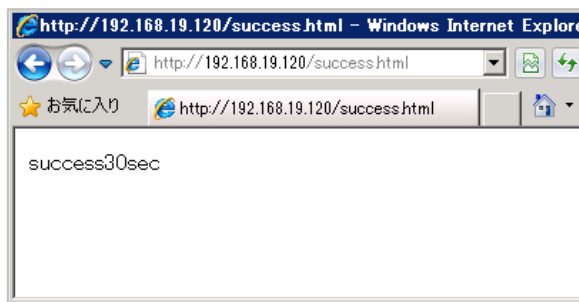


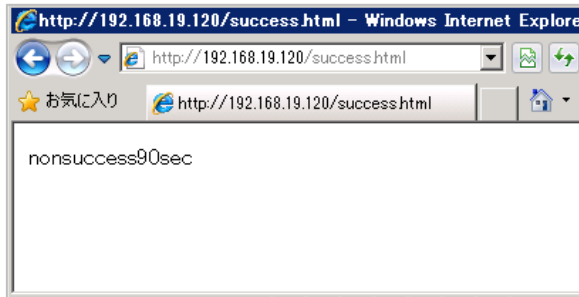
図 正常時ステータス情報

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

HTTP OK: HTTP/1.1 200 OK - 279 bytes in 0.001 second response time

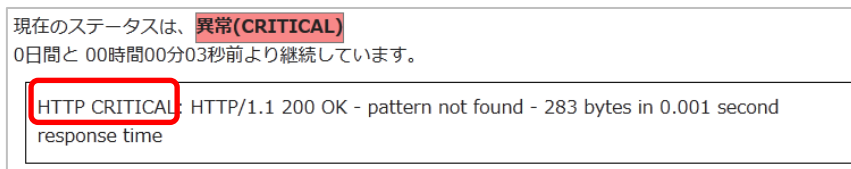
CRITICAL にするために、表示の文字列が NG になるようにしてみます。

図 ブラウザでアクセス



検知文字列が「success」だけですと CRITICAL にはならないため、正規表現にて CRITICAL を検知します。

図 CRITICAL 時ステータス情報



3.2.2 設定項目一覧

URL パス	監視対象ページを指定します。
ポート番号	監視対象のポート番号を指定します。
BASIC 認証ユーザ名	監視対象ページに BASIC 認証の制限をかけている場合、ユーザ名を入力します。
BASIC 認証パスワード	監視対象ページに BASIC 認証の制限をかけている場合、パスワードを入力します。
タイムアウト(秒)	監視対象ページから指定した秒数以上応答がない場合、チェックを終了し、監視ステータスを CRITICAL にします。
応答時間 WARNING しきい値(秒)	監視対象ページの応答時間がこの値を超えた場合、監視ステータスを WARNING にします。
応答時間 CRITICAL しきい値(秒)	監視対象ページの応答時間がこの値を超えた場合、監視ステータスを CRITICAL にします。
HTTP ステータスコードの指定	HTTP ステータスコードを指定して監視するかどうか指定します。HTTP ステータスコードの監視を行う場合は「有効」を選択します。
HTTP ステータスコード	監視ステータス OK とする HTTP ステータスコードを指定します。カンマ(,)で区切ることで複数の HTTP ステータスを指定できます。

	タスコードを指定することができます。この項目を指定する場合、前項で「有効」を選択する必要があります。監視対象ページの HTTP ステータスコードがこの値以外の場合、監視ステータスを CRITICAL にします
検出文字列	監視対象ページ内で監視する文字列を指定します。この項目では正規表現を使用することができます。また、バーティカルバー()で区切ることで複数の文字列を指定することができます。 監視対象ページ内に指定した文字列がひとつも含まれていない場合、監視ステータスを CRITICAL にします。

3.3 HTTPS 監視

監視グループ	チェックコマンド
Web サービス監視	HTTPS 監視

SSL に対応した Web ページの監視を行います。

HTTP ステータスコードを指定しないとき、接続が可能(HTTP ステータスコードが 200 番台または 300 番台)な場合、監視ステータスを OK にします。クライアント側のエラー(HTTP ステータスコードが 400 番台)の場合、監視ステータスを WARNING にします。サーバ側のエラー(HTTP ステータスコードが 500 番台または 100 未満)やタイムアウトの場合、監視ステータスを CRITICAL にします。

X-MON サーバからは IP アドレスでアクセスします。

3.3.1 監視設定例

サンプルネットワークでの構成の場合、IP アドレスは 192.168.19.120 のため、X-MON サーバからは

https://192.168.19.120

のアドレスでアクセスする形となります。オプションで設定を入れる事が可能です。

その他の設定項目は [3.2 HTTP 監視](#) と共通ですので、そちらを参照ください。

新規作成の際のデフォルトの設定は下記となります。

図 デフォルトの設定

サービス監視用コマンド	
Webサービス監視	▼
HTTPS監視	▼
URLパス	/
ポート番号	443
BASIC認証ユーザ名	none
BASIC認証パスワード	●●●●
応答時間WARNINGしきい値(秒)	4
応答時間CRITICALしきい値(秒)	8
タイムアウト(秒)	10
HTTPステータスコードの指定	無効 ▼
HTTPステータスコード	
検出文字列	
SSLバージョン	自動 ▼

3.3.2 設定項目一覧

URL パス	監視対象ページを指定します。
ポート番号	監視対象のポート番号を指定します。
BASIC 認証ユーザ名	監視対象ページに BASIC 認証の制限をかけている場合、ユーザ名を入力します。
BASIC 認証パスワード	監視対象ページに BASIC 認証の制限をかけている場合、パスワードを入力します。
タイムアウト(秒)	監視対象ページから指定した秒数以上応答がない場合、チェックを終了し、監視ステータスを CRITICAL にします。
応答時間 WARNING しきい値(秒)	監視対象ページの応答時間がこの値を超えた場合、監視ステータスを WARNING にします。
応答時間 CRITICAL しきい値(秒)	監視対象ページの応答時間がこの値を超えた場合、監視ステータスを CRITICAL にします。
HTTP ステータスコード の指定	HTTP ステータスコードを指定して監視するかどうか指定します。HTTP ステータスコードの監視を行う場合は「有効」を選択します。
HTTP ステータスコード	監視ステータス OK とする HTTP ステータスコードを指定します。カンマ(,)で区切ることで複数の HTTP ステータスコードを指定することができます。この項目を指定する場合、前項で「有効」を選択する必要があります。

	監視対象ページの HTTP ステータスコードがこの値以外の場合、監視ステータスを CRITICAL にします
検出文字列	監視対象ページ内で監視する文字列を指定します。この項目では正規表現を使用することができます。また、バーティカルバー()で区切ることで複数の文字列を指定することができます。 監視対象ページ内に指定した文字列がひとつも含まれていない場合、監視ステータスを CRITICAL にします。
SSL バージョン	SSL のバージョンを自動、SSLv2、SSLv3、TLSv1、TLSv1.1、TLSv1.2 から指定できます。

3.4 SSL の証明書有効期限監視

監視グループ	チェックコマンド
Web サービス監視	SSL の証明書有効期限監視

監視対象ホストの SSL 証明書の有効期限の監視を行います。

SSL 証明書の有効期限がしきい値を超える場合は、監視ステータスを WARNING にします。有効期限が切れた場合は、監視ステータスを CRITICAL にします。

X-MON サーバからは IP アドレスでアクセスします。

3.4.1 監視設定例

サンプルネットワークでの構成の場合、IP アドレスは 192.168.19.120 のため、X-MON サーバからは

https://192.168.19.120

のアドレスでアクセスした際に設定されている証明書のための監視となります。

X-MON では 1 つの監視ホストに複数の IP バージョンホストが監視されている場合は、IP バージョンホスト監視を使用する事により監視ホストを増やすことなく監視が可能です。同じく一つのサーバでの有効期限を監視したい場合は「SSL の証明書有効期限監視(SNI)」プラグインを使用し、コモンネームを指定してください。

監視設定では証明書が切れる日にちまでの日数を指定します。

デフォルトではしきい値は 30 日で設定されます。

図 デフォルトの設定

サービス監視用コマンド

Webサービス監視
SSLの証明書有効期限監視

WARNINGしきい値(日) 30

正常に監視が行われている場合は下記画像となります。証明書の有効期限日も表示されます。

図 正常時

現在のステータスは、**正常(OK)**
0日間と 00時間00分03秒前より継続しています。

OK - Certificate will expire on 11/12/2013 07:20

しきい値の 30 日を切り、WARNING を検知した場合は残り日数と有効期限日が表示されます。

図 WARNING 時

現在のステータスは、**警告(WARNING)**
0日間と 00時間01分14秒前より継続しています。

WARNING - Certificate expires in 29 day(s) (12/14/2012 07:07).

有効期限日の前日はその日で切れるため、today と表示されます。

図 WARNING 時

現在のステータスは、**警告(WARNING)**
0日間と 00時間16分30秒前より継続しています。

WARNING - Certificate expires today (11/15/2012 07:24).

有効期限が切れた場合は CRITICAL を検知、失効日が表示されます。

図 CRITICAL 時

現在のステータスは、**異常(CRITICAL)**
0日間と 01時間17分53秒前より継続しています。

CRITICAL - Certificate expired on 11/15/2012 07:24.

3.4.2 設定項目一覧

WARNING しきい値(日)	監視対象ホストの SSL 証明書の残り有効期限がこの値を下回った場合、監視ステータスを WARNING にします。有効期限が切れた場合は CRITICAL とします。
-----------------	---

3.5 SSL の証明書有効期限間監視(SNI)

監視グループ	チェックコマンド
Web サービス監視	SSL の証明書有効期限監視(SNI)

監視対象ホストの SSL 証明書の有効期限の監視を行います。

1 つの IP アドレスで複数の証明書を使う SNI 設定がされているサーバで利用できます。SSL 証明書の有効期限がしきい値を超える場合は、監視ステータスを WARNING にします。有効期限が切れた場合は、監視ステータスを CRITICAL にします。

3.5.1 監視設定例

監視を行いたいサーバの URL が「www.example.com」の場合、設定項目のコモンネームに「www.example.com」と入力してください。

その他の設定項目は [3.4 SSL の証明書有効期限監視](#) と共通ですので、そちらを参照ください。

新規作成の際のデフォルトの設定は下記となります。

図 デフォルトの設定

サービス監視用コマンド	
Webサービス監視	▼
SSLの証明書有効期限監視(SNI)	▼
コモンネーム	<input type="text"/>
WARNINGしきい値(日)	30

3.5.2 設定項目一覧


コモンネーム	監視対象の SSL 証明書のコモンネームを指定します。
WARNING しきい値(日)	監視対象ホストの SSL 証明書の残り有効期限がこの値を下回った場合、監視ステータスを WARNING にします。有効期限が切れた場合は CRITICAL とします。

3.6 Web コンテンツ改ざん監視

監視グループ	チェックコマンド
Web サービス監視	Web コンテンツ改ざん監視

Web ページの改ざんの監視を行います。前回チェック時の Web ページ（ページファイルのチェックサム）と比較し、一致するか監視します。

Web ページの改ざんがある場合、監視ステータスを CRITICAL にします。

 **ファイルのソースのリンク先のファイル名は同じままで画像ファイルが差し替えられたりしても検知はしません。**

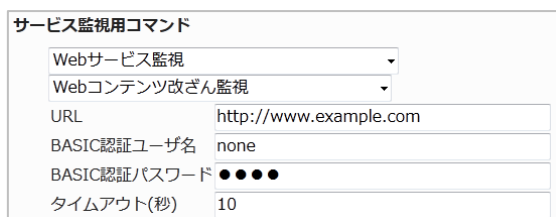
3.6.1 監視設定例

URL にアドレスを指定します。デフォルトでは `http://www.example.com` です。

比較するファイルはアクセスした際のトップページとなります。Web サーバの設定によりませんが、トップページの設定が `index.html` の場合は

`http://www.example.com/index.html` となります。

図 デフォルトの設定



サービス監視用コマンド

Webサービス監視 (選択)

Webコンテンツ改ざん監視 (選択)

URL: `http://www.example.com`

BASIC認証ユーザ名: none

BASIC認証パスワード: ●●●●

タイムアウト(秒): 10

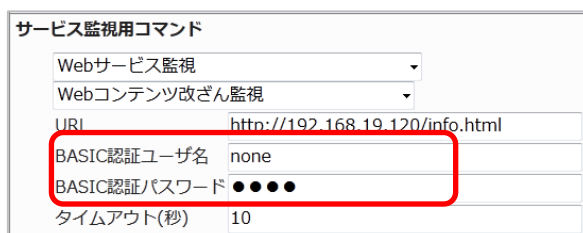
特定のページを指定する場合は、フルパスで記載をしてください。

1 つの監視で監視できるページは 1 ページですので、複数のページを監視する際は各々監視作成が必要です。もしくは、「Web コンテンツ改ざん監視（一括監視）」プラグインをご使用ください。

`http://192.168.19.120/info.html` を監視対象としてみましょう。

URL の部分に `http`～からのフルパスを記載します。BASIC 認証は使用していませんので削除するかもしれませんが記載しても Basic 認証の設定が入っていないと無効となります。（HTTP 監視での Basic 認証欄と同様です）

図 設定例



サービス監視用コマンド

Webサービス監視 (選択)

Webコンテンツ改ざん監視 (選択)

URI: `http://192.168.19.120/info.html`

BASIC認証ユーザ名: none

BASIC認証パスワード: ●●●●

タイムアウト(秒): 10

正常に監視が出来ている場合は下記のような画像となります。

図 正常時

現在のステータスは、**正常(OK)**

0日間と 00時間00分04秒前より継続しています。

OK - 「http://192.168.19.120/info.html」 は、前回の確認から変更はありません。

info.html が改ざんされ CRITICAL を検知した場合はこのような画像となります。

図 CRITICAL 時

現在のステータスは、**異常(CRITICAL)**

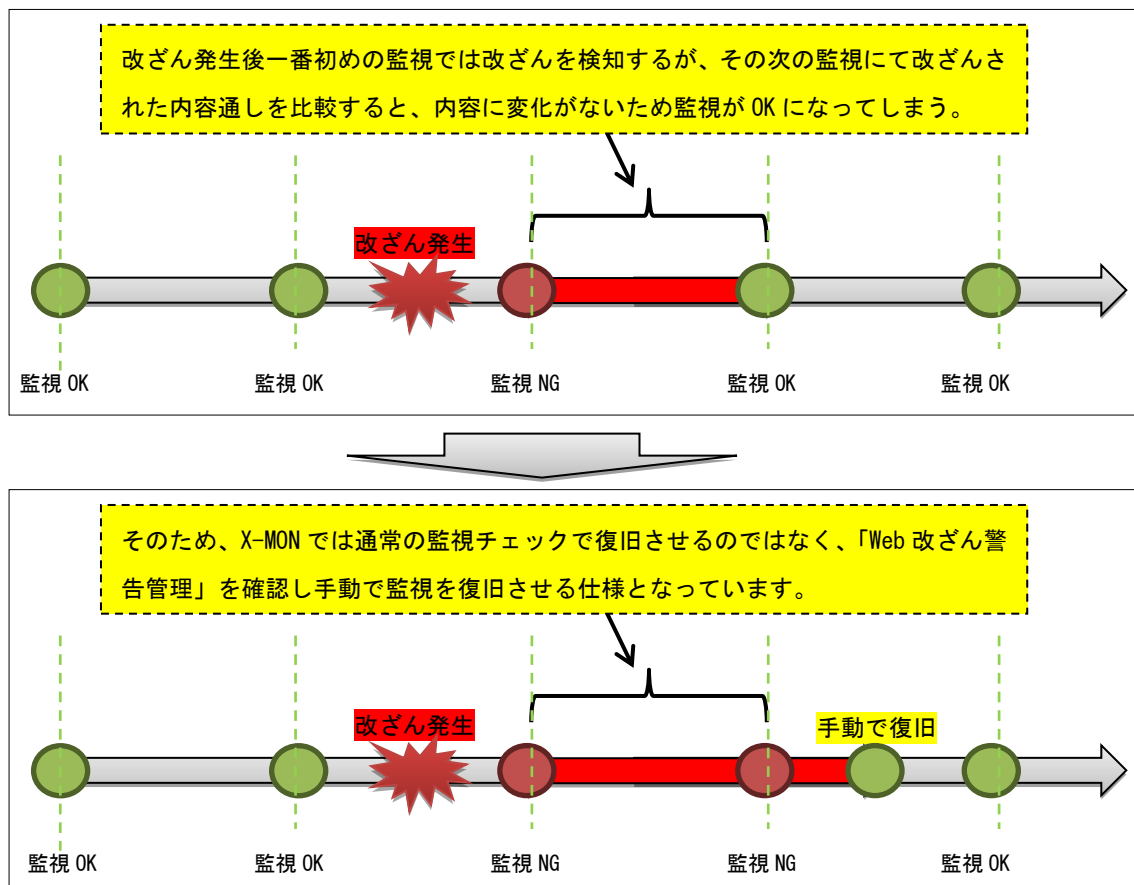
0日間と 00時間00分07秒前より継続しています。

CRITICAL - 「http://192.168.19.120/info.html」 の変更が検出されました。

3.6.2 監視の復旧方法について

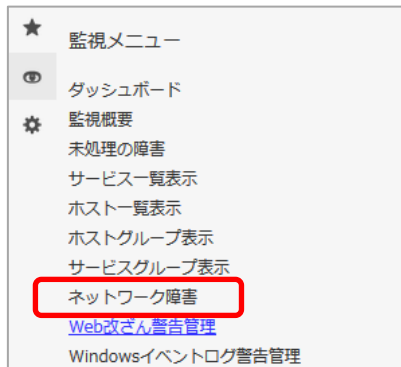
Web コンテンツ改ざん監視は変更が加わったページと、そのあとのページを比較すると「変更がない」となってしまうため復旧させる（監視を OK にする）には監視メニュー「Web 改ざん警告管理」を確認します。

図 復旧仕様



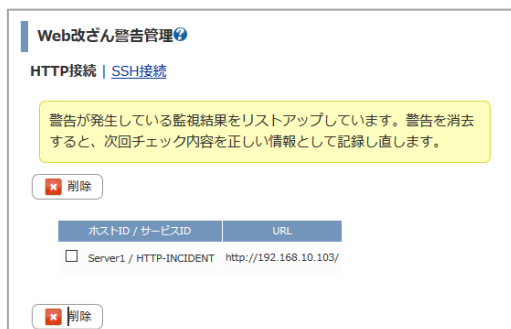
[Web 改ざん警告管理]は[監視メニュー] の中にあります。

図 MENU



Web 改ざんを検知している場合は画像のように検知したホスト、サービス ID が表示されます。URL の欄は監視対象 URL が表示されます。

図 Web 改ざん警告管理



復旧させるには、チェックボックスにチェックを入れて[削除] を実行します。

図 監視復旧



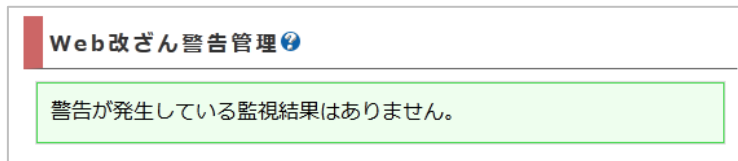
削除の確認の画面が表示されますので、問題なければ[OK]を押してください。

図 監視復旧確認



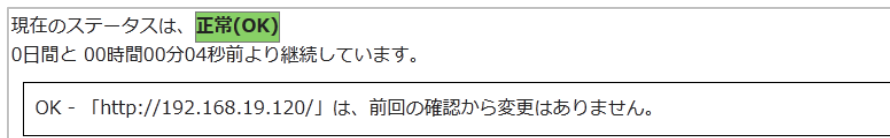
削除が完了します。

図 削除後



削除完了後、監視が復旧するか確認してください。

図 正常ステータス



⚠ 改ざん監視、並びに改ざん警告管理は改ざんが検知された事を表示します。比較したページのどの部分が改ざんされたかのか詳細は表示されませんので、お客様にてページをご確認ください。

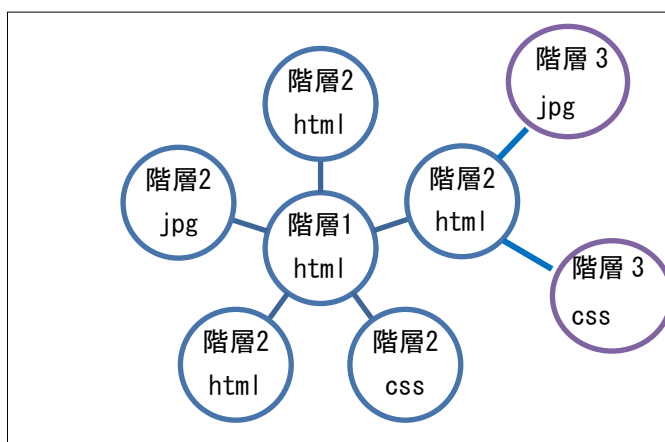
3.7 Web コンテンツ改ざん監視（一括監視）

監視グループ	チェックコマンド
Web サービス監視	Web コンテンツ改ざん監視（一括監視）

Web コンテンツ改ざん監視（一括監視）をご利用頂くと、リンク数と除外ファイルの設定が可能です。リンクする画像ファイルも名前が同じでも差し替えられた場合は検知する事が出来ます。

リンク先を辿る階層は指定するページが階層 1 となります。そこから階層 1 からリンクが張られて移動できるページが階層 2 となり、同じように階層 2 からリンクが張られて移動できるページが階層 3 となります。

図 階層



設定の詳細はオンラインマニュアルをご参照ください。

リンクを辿る回数	<p>前項で指定した監視対象ページ URL からリンクするページのうち、監視対象に含めるページの深さを指定します。</p> <p>例えば「3」と指定すると、前項で指定した URL 内にあるリンクから移動できるページと、そのページ内にあるリンクから移動できるページまでが監視対象となります。</p>
除外するファイル (後方一致)	<p>監視対象から除外するファイルのファイル名後方から一致する文字列を指定します。また、カンマ(,)で区切ることで複数の文字列を指定することができます。</p> <p>例えば、Web ページ内の画像の変更については改ざんとして検出しないよう「.jpg,.png,.gif」等と指定すると、ファイル拡張子が.jpg, .png, .gif のいずれかに該当するファイルの変更については、改ざんとして検出しません</p>

3.7.1 設定項目一覧

URL	監視対象ページを指定します。
ポート番号	監視対象のポート番号を指定します。
BASIC 認証ユーザ名	監視対象ページに BASIC 認証の制限をかけている場合、ユーザ名を入力します。
BASIC 認証パスワード	監視対象ページに BASIC 認証の制限をかけている場合、パスワードを入力します。
タイムアウト(秒)	監視対象ページから指定した秒数以上応答がない場合、チェックを終了し、監視ステータスを CRITICAL にします。

3.8 その他の Web サービス監視のチェックコマンド

監視パッケージに含まれていませんが、Web サービス監視のチェックコマンドを簡単に説明します。詳細はオンラインマニュアルをご参照ください。

3.8.1 HTTP IP ベースバーチャルホストの監視,HTTPS IP ベースバーチャルホストの監視

1 つのホストにて、割り当てられている IP アドレス以外の IP アドレスを設定し、IP ベースのバーチャルホスト設定を行っている Web ページの監視を行います。

HTTP ステータスコードを指定しないとき、接続が可能(HTTP ステータスコードが 200 番台または 300 番台)な場合、監視ステータスを OK にします。クライアント側のエラー(HTTP ステータスコードが 400 番台)の場合、監視ステータスを WARNING にします。サーバ側のエラー(HTTP ステータスコードが 500 番台または 100 未満)やタイムアウトの場合、監視ステータスを CRITICAL にします。

3.8.2 HTTP ネームベースバーチャルホストの監視、HTTPS ネームベースバーチャルホストの監視

1 つのホストにて、複数のドメインを割り当ててネームベースのバーチャルホストを設定している Web ページの監視を行います。

HTTP ステータスコードを指定しないとき、接続が可能(HTTP ステータスコードが 200 番台または 300 番台)な場合、監視ステータスを OK にします。クライアント側のエラー(HTTP ステータスコードが 400 番台)の場合、監視ステータスを WARNING にします。サーバ側のエラー(HTTP ステータスコードが 500 番台または 100 未満)やタイムアウトの場合、監視ステータスを CRITICAL にします。

監視を行う際には、この監視サービスを設定するホストから監視対象ページを閲覧した状態を監視します。

3.8.3 NRPE 経由での HTTP 監視、NRPE 経由での HTTPS 監視

X-MON から直接監視できないホストを監視する際に、監視対象ホストを経由して Web ページの監視を行います。

HTTP ステータスコードを指定しないとき、接続が可能(HTTP ステータスコードが 200 番台または 300 番台)な場合、監視ステータスを OK にします。クライアント側のエラー(HTTP ステータスコードが 400 番台)の場合、監視ステータスを WARNING にします。サーバ側のエラー(HTTP ステータスコードが 500 番台または 100 未満)やタイムアウトの場合、監視ステータスを CRITICAL にします。

4 Linux メールサーバ監視

Linux メールサーバ監視ではメールサービスを提供しているホストに対する監視パッケージです。内容は Linux 標準監視とメールサービスに特化した監視項目です。

項目一覧は [1.2.3 Linux メールサーバ監視一覧](#) をご参照ください。

4.1 POP3 監視

監視グループ	チェックコマンド
メールサービス監視	POP3 監視

監視対象サーバの POP サービスの死活監視を行います。

応答時間がしきい値を超える場合は、監視ステータスを WARNING または CRITICAL にします。接続できない場合は、監視ステータスを CRITICAL にします。

ポート番号へのサービス稼働監視ですので、実際にメールの受信は行いません。

4.1.1 監視設定例

通常、POP3 はポート番号 110 番を使用します。デフォルトの設定でも 110 番が指定されますので、監視ホストの設定で違うポート番号を指定している場合はその番号を指定してください。

図 POP3 設定

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

正常に監視出来たら下記のようなステータス情報となります。

(設定例サーバでは dovecot を使用)

図 正常時

現在のステータスは、 **正常(OK)**

0日間と 00時間12分03秒前より継続しています。

POP OK - 0.011 second response time on port 110 [+OK Dovecot ready.]

4.1.2 設定項目一覧

ポート番号	監視対象となる POP サービスのポート番号を指定します。
タイムアウト(秒)	監視対象ポートから指定した秒数以上応答がない場合、チェックを終了し、監視ステータスを CRITICAL にします。
WARNING しきい値(秒)	応答時間がこの値を超えた場合、監視ステータスを WARNING にします。
CRITICAL しきい値(秒)	応答時間がこの値を超えた場合、監視ステータスを CRITICAL にします。

4.2 POPS 監視

監視グループ	チェックコマンド
メールサービス監視	POPS 監視

監視対象サーバの POPS サービスの死活監視を行います。Over SSL(STARTTLS ではありません)での接続を行って監視します。

応答時間がしきい値を超える場合は、監視ステータスを WARNING または CRITICAL にします。接続できない場合は、監視ステータスを CRITICAL にします。

ポート番号へのサービス稼働監視ですので、実際にメールの受信は行いません。

4.2.1 監視設定例

通常、POP3 はポート番号 995 番を使用します。デフォルトの設定でも 995 番が指定されますので、監視ホストの設定で違うポート番号を指定している場合はその番号を指定してください。

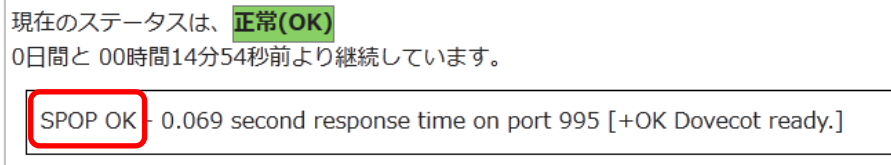
図 POPS 設定

正常に監視出来たら下記のようなステータス情報となります。

ステータス情報では SPOP-OK となりますが、これは監視で使用している nagios プラグインの仕様となります。SPOP でも正常に POPS 監視出来ています。

(設定例サーバでは dovecot を使用)

図 正常時



4.2.2 設定項目一覧

ポート番号	監視対象となる POSP サービスのポート番号を指定します。
タイムアウト(秒)	監視対象ポートから指定した秒数以上応答がない場合、チェックを終了し、監視ステータスを CRITICAL にします。
WARNING しきい値(秒)	応答時間がこの値を超えた場合、監視ステータスを WARNING にします。
CRITICAL しきい値(秒)	応答時間がこの値を超えた場合、監視ステータスを CRITICAL にします。

4.3 SMTP 監視

監視グループ	チェックコマンド
メールサービス監視	SMTP 監視

監視対象サーバの SMTP サービスの死活監視を行います。

応答時間がしきい値を超える場合は、監視ステータスを WARNING または CRITICAL にします。接続できない場合は、監視ステータスを CRITICAL にします。

ポート番号へのサービス稼働監視ですので、実際にメールの送信は行いません。

4.3.1 監視設定例

通常、SMTP はポート番号 25 番を使用します。デフォルトの設定でも 25 番が指定されますので、監視ホストの設定で違うポート番号を指定している場合はその番号を指定してください。

また、SMTP サービスにおいて送信元メールアドレスを限定している場合もありますのでメール送信元のアドレスを指定する事が出来ます。デフォルトでは none です。指定しない場合は空白、もしくは none を指定してください。

図 SMTP 設定

サービス監視用コマンド	
メールサービス監視	
SMTP監視	
ポート番号	25
タイムアウト(秒)	10
FROMに使用するアドレス	none
WARNINGしきい値(秒)	3
CRITICALしきい値(秒)	5

正常に監視出来たら下記のようなステータス情報となります。

図 正常時

現在のステータスは、 正常(OK)
1日間と 00時間31分23秒前より継続しています。
SMTP OK - 0.033 sec. response time

4.3.2 サブミッションポートの監視

監視パッケージから監視登録した際、サブミッションポートを使用した「SMTP-Submission」も追加されます。

設定としては通常の SMTP とかわりません。ポート番号がサブミッションポートで使用する 587 番を指定します。

図 サブミッションポート設定

サービス監視用コマンド	
メールサービス監視	
SMTP監視	
ポート番号	587
タイムアウト(秒)	10
FROMに使用するアドレス	none
WARNINGしきい値(秒)	3
CRITICALしきい値(秒)	5

正常に監視出来たら下記のようなステータス情報となります。

図 正常時

現在のステータスは、 正常(OK)
1日間と 00時間31分07秒前より継続しています。
SMTP OK - 0.039 sec. response time

4.3.3 設定項目一覧

ポート番号	監視対象となる SMTP サービスのポート番号を指定します。
タイムアウト(秒)	監視対象ポートから指定した秒数以上応答がない場合、チェックを終了し、監視ステータスを CRITICAL にします。
FROM に使用するアドレス	監視の際に実行する mail コマンドの送信元メールアドレスを指定します。実際にメールが送信されることはありません。
WARNING しきい値(秒)	応答時間がこの値を超えた場合、監視ステータスを WARNING にします。
CRITICAL しきい値(秒)	応答時間がこの値を超えた場合、監視ステータスを CRITICAL にします。

4.4 SMTPS 監視

監視グループ	チェックコマンド
メールサービス監視	SMTPS 監視

監視対象サーバの SMTPS サービスの死活監視を行います。Over SSL(STARTTLS ではありません)での接続を行って監視します。

応答時間がしきい値を超える場合は、監視ステータスを WARNING または CRITICAL にします。接続できない場合は、監視ステータスを CRITICAL にします。

ポート番号へのサービス稼働監視ですので、実際にメールの送信は行いません。

4.4.1 監視設定例

通常、SMTPS はポート番号は 465 番を使用します。デフォルトの設定でも 465 番が指定されますので、監視ホストの設定で違うポート番号を指定している場合はその番号を指定してください。

図 SMTPS 設定

サービス監視用コマンド

メールサービス監視
SMTPS監視

ポート番号
465

タイムアウト(秒)
10

WARNINGしきい値(秒)
3

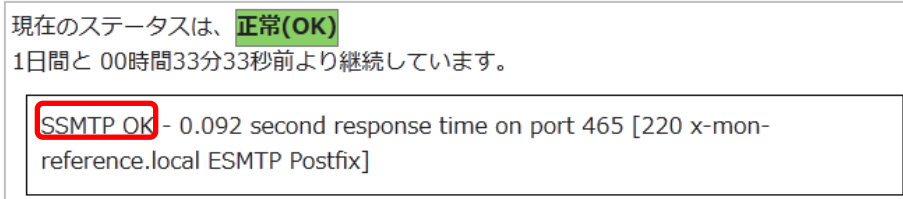
CRITICALしきい値(秒)
5

正常に監視出来たら下記のようなステータス情報となります。

ステータス情報では SSMTP-OK となりますが、これは監視で使用している nagios プラグインの仕様となります。SSMTP でも正常に SMTPS 監視出来ています。

(設定例サーバでは Postfix を使用)

図 正常時



4.4.2 設定項目一覧

ポート番号	監視対象となる SMTPS サービスのポート番号を指定します。
タイムアウト(秒)	監視対象ポートから指定した秒数以上応答がない場合、チェックを終了し、監視ステータスを CRITICAL にします。
WARNING しきい値(秒)	応答時間がこの値を超えた場合、監視ステータスを WARNING にします。
CRITICAL しきい値(秒)	応答時間がこの値を超えた場合、監視ステータスを CRITICAL にします。

4.5 IMAP4 監視

監視グループ	チェックコマンド
メールサービス監視	IMAP4 監視

監視対象サーバの IMAP サービスの死活監視を行います。

応答時間がしきい値を超える場合は、監視ステータスを WARNING または CRITICAL にします。接続できない場合は、監視ステータスを CRITICAL にします。

ポート番号へのサービス稼働監視ですので、実際にメールの受信は行いません。

4.5.1 監視設定例

通常、IMAP4 はポート番号 143 番を使用します。デフォルトの設定でも 143 番が指定されますので、監視ホストの設定で違うポート番号を指定している場合はその番号を指定してください。

図 IMAP 設定

サービス監視用コマンド	
メールサービス監視	
IMAP4監視	
ポート番号	143
タイムアウト(秒)	10
WARNINGしきい値(秒)	3
CRITICALしきい値(秒)	5

正常に監視出来たら下記のようなステータス情報となります。

(設定例サーバでは dovecot を使用、設定によりレスポンスメッセージの部分は変わります。)

図 正常時

現在のステータスは、 正常(OK) 0日間と 00時間19分50秒前より継続しています。
<pre>IMAP OK - 0.006 second response time on port 143 [* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE STARTTLS LOGINDISABLED] Dovecot ready.]</pre>

4.5.2 設定項目一覧

ポート番号	監視対象となる IMAP サービスのポート番号を指定します。
タイムアウト(秒)	監視対象ポートから指定した秒数以上応答がない場合、チェックを終了し、監視ステータスを CRITICAL にします。
WARNING しきい値(秒)	応答時間がこの値を超えた場合、監視ステータスを WARNING にします。
CRITICAL しきい値(秒)	応答時間がこの値を超えた場合、監視ステータスを CRITICAL にします。

4.6 IMAPS 監視

監視グループ	チェックコマンド
メールサービス監視	IMAPS 監視

監視対象サーバの IMAPS サービスの死活監視を行います。Over SSL(STARTTLS ではありません)での接続を行って監視します。

応答時間がしきい値を超える場合は、監視ステータスを WARNING または CRITICAL にします。接続できない場合は、監視ステータスを CRITICAL にします。

ポート番号へのサービス稼働監視ですので、実際にメールの受信は行いません。

4.6.1 監視設定例

通常、IMAPS はポート番号 993 番を使用します。デフォルトの設定でも 993 番が指定されますので、監視ホストの設定で違うポート番号を指定している場合はその番号を指定してください。

図 IMAPS 設定

サービス監視用コマンド	
メールサービス監視	▼
IMAPS監視	▼
ポート番号	993
タイムアウト(秒)	10
WARNINGしきい値(秒)	3
CRITICALしきい値(秒)	5

正常に監視出来たら下記のようなステータス情報となります。

ステータス情報では SIMAP-OK となりますが、これは監視で使用している nagios プラグインの仕様となります。SIMAP でも正常に IMAPS 監視出来ています。

(設定例サーバでは dovecot を使用)

図 正常時

現在のステータスは、	正常(OK)
0日間と 00時間19分36秒前より継続しています。	
<div style="border: 1px solid black; padding: 5px;"> SIMAP OK - 0.075 second response time on port 993 [* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN] Dovecot ready.] </div>	

4.6.2 設定項目一覧

ポート番号	監視対象となる IMAP サービスのポート番号を指定します。
タイムアウト(秒)	監視対象ポートから指定した秒数以上応答がない場合、チェックを終了し、監視ステータスを CRITICAL にします。
WARNING しきい値(秒)	応答時間がこの値を超えた場合、監視ステータスを WARNING にします。
CRITICAL しきい値(秒)	応答時間がこの値を超えた場合、監視ステータスを

	CRITICAL にします。
--	----------------

4.7 NRPE 経由でのメールキュー監視

監視グループ	チェックコマンド
メールサービス監視	NRPE 経由でのメールキュー監視

NRPE を利用して、監視ホストのメールサーバのメールキュー数の監視を行います。

メールキュー数がしきい値を超える場合は、監視ステータスを WARNING または CRITICAL にします。監視対象のサービスが起動していない場合は、監視ステータスを UNKNOWN にします。

sendmail,qmail,postfix,exim が対応している MTA となります。

4.7.1 監視設定例

新規作成でのメールキュー監視のデフォルトの MTA は「sendmail」が選択されています。監視パッケージで設定した場合は「postfix」がデフォルトで選択されます。

環境に合わせて MTA を指定してください。設定例では postfix を指定します。

しきい値はメールキューの数を数値で入力します。

図 メールキュー設定

サービス監視用コマンド

メールサービス監視

メールキュー監視

MTAの種類

WARNINGしきい値
(キュー数)

CRITICALしきい値
(キュー数)

タイムアウト(秒)

postfix

5

10

15

正常に監視出来ている場合は下記画像のようになります。(メールキューがない状態)

図 正常時

現在のステータスは、**正常(OK)**

0日間と 00時間00分31秒前より継続しています。

OK: mailq reports queue is empty

メールキューがある場合でしきい値より低い場合は、その数也表示します。

図 メールキューがある正常時

現在のステータスは、**正常(OK)**
0日間と 00時間08分18秒前より継続しています。

OK: mailq (3) is below threshold (5/10)

障害を検知した場合は下記画像のようになります。メールキューの数と CRITICAL のしきい値が表示されます。

図 障害時

現在のステータスは、**異常(CRITICAL)**
1日間と 00時間11分06秒前より継続しています。

CRITICAL: mailq is 12 (threshold c = 10)

mailq は通常のサーバで mailq コマンド (qmail では qmail-qstat) コマンドを発行した際のメールキューの数を監視します。

■監視ホストでの mailq コマンド発行例

```
# mailq
-Queue ID- --Size-- ----Arrival Time---- -Sender/Recipient-----
1FDE71C7C      449 Thu Nov 15 17:15:12 root@x-mon-reference.local
                                     (deferred transport)
                                     test@localhost.localdomain

~中略~
A34E11C82      449 Thu Nov 15 17:15:14 root@x-mon-reference.local
                                     (deferred transport)
                                     test@localhost.localdomain

- 8 Kbytes in 12 Requests.
```

メールキューの数の監視になりますので、実際にどのようなメールキューがたまっているか内容は監視ホスト内にて確認してください。

4.7.2 設定項目一覧

MTA の種類	監視対象メールサーバの MTA を指定します。
WARNING しきい値(キュー数)	メールキュー内のメール数がこの値を超えた場合、監視ステータスを WARNING にします。
CRITICAL しきい値(キュー数)	メールキュー内のメール数がこの値を超えた場合、監視ステータスを WARNING にします。
タイムアウト(秒)	監視対象サービスから指定した秒数以上応答がない場合、チェックを終了し、監視ステータスを CRITICAL に

	します。
NRPE タイムアウト(秒)	指定した秒数以上 NRPE プラグインからの応答がない場合、チェックを終了し、CRITICAL を検出します。

4.8 その他のメールサービス監視のチェックコマンド

監視パッケージに含まれていませんが、メールサービス監視のチェックコマンドを簡単に説明します。詳細はオンラインマニュアルをご参照ください。

4.8.1 NRPE 経由での IMAP4 監視,NRPE 経由での IMAPS 監視

NRPE を利用して、監視対象サーバの IMAP サービス,IMAPS サービスの死活監視を行います。

応答時間がしきい値を超える場合は、監視ステータスを WARNING または CRITICAL にします。接続できない場合は、監視ステータスを CRITICAL にします。

NRPE は X-MON から直接監視できないホストを監視する際に利用します。

4.8.2 NRPE 経由での POP3 監視,NRPE 経由での POPS 監視

NRPE を利用して、監視対象サーバの POP サービス,POPS サービスの死活監視を行います。

応答時間がしきい値を超える場合は、監視ステータスを WARNING または CRITICAL にします。接続できない場合は、監視ステータスを CRITICAL にします。

NRPE は X-MON から直接監視できないホストを監視する際に利用します。

4.8.3 NRPE 経由での SMTP 監視,NRPE 経由での SMTPS 監視

NRPE を利用して、監視対象サーバの SMTP サービス,SMTPS サービスの死活監視を行います。

応答時間がしきい値を超える場合は、監視ステータスを WARNING または CRITICAL にします。接続できない場合は、監視ステータスを CRITICAL にします。

NRPE は X-MON から直接監視できないホストを監視する際に利用します

4.8.4 メールキュー監視

X-MON サーバ内のメールサーバのメールキュー数の監視を行います。

メールキュー数がしきい値を超える場合は、監視ステータスを WARNING または

CRITICAL にします。監視対象のサービスが起動していない場合は、監視ステータスを UNKNOWN にします。

5 Linux MySQL サーバ監視

Linux MySQLサーバ監視ではMySQLデータベースサービスを提供しているホストに対する監視パッケージです。

内容は Linux 標準監視と MySQL データベースサービスに特化した監視項目です。

項目一覧は 1.2.4 Linux MySQL サーバ監視一覧をご参照ください。

5.1 MySQL 監視

監視グループ	チェックコマンド
データベース監視	MySQL 監視

監視対象ホストの MySQL への接続の監視を行います。

データベースへの接続に問題がある場合は、監視ステータスを WARNING にします。

データベースへ接続できない場合は、監視ステータスを CRITICAL にします。

この監視では、監視実行時に ps のプロセスリストに表示されます。また、接続する際にデータベース名、ユーザ名、パスワードを入力します。そのため監視の接続には権限を最小限に抑えた監視専用のデータベースとアカウントを使用することをお勧めします。

5.1.1 監視設定例

通常、MySQL はポート番号 3306 番を使用します。デフォルトの設定でも 3306 番が指定されますので、監視ホストの設定で違うポート番号を指定している場合はその番号を指定してください。

接続するデータベース、ユーザ名とパスワードを入力します。

設定例では監視用データベースの「kanshi_db」に対して監視用ユーザ「kanshi_user」で接続しています。

図 MySQL 監視

サービス監視用コマンド

データベース監視

MySQL監視

ポート番号

3306

データベース名

kanshi_db

ユーザ名

kanshi_user

パスワード

●●●●●●

正常に監視出来たら下記のようなステータス情報となります。

(メッセージの詳細は環境により異なります)

図 正常時

現在のステータスは、 正常(OK) 2日間と 15時間44分19秒前より継続しています。
Uptime: 229829 Threads: 1 Questions: 1565 Slow queries: 0 Opens: 15 Flush tables: 1 Open tables: 8 Queries per second avg: 0.6

5.1.2 設定項目一覧

ポート番号	MySQL への接続ポート番号を指定します。
データベース名	監視対象のデータベース名を指定します。
ユーザ名	MySQL 接続時のユーザ名を指定します。
パスワード	MySQL 接続時のユーザ名に対応するパスワードを指定します。

5.2 NRPE 経由での MySQL 監視

監視グループ	チェックコマンド
データベース監視	NRPE 経由での MySQL 監視

NRPE を利用して、監視対象ホストの MySQL への接続の監視を行います。

使用用途はデータベースを外部から接続許可がない時や、データベースサーバに X-MON が直接アクセスできない場合等となります。

データベースへの接続に問題がある場合は、監視ステータスを WARNING にします。
データベースへ接続できない場合は、監視ステータスを CRITICAL にします。

この監視では、監視実行時に ps のプロセスリストに表示されます。また、接続する際にデータベース名、ユーザ名、パスワードを入力します。そのため監視の接続には権限を最小限に抑えた監視専用のデータベースとアカウントを使用することをお勧めします。

5.2.1 監視設定例

対象ホスト名または IP アドレスを入力します。

監視対象ホスト自身の場合は、ローカルホストである 127.0.0.1 を入力します。

監視対象ホストから別ホストへ接続する場合はそのホストの IP アドレスを入力してください。

通常、MySQL はポート番号 3306 番を使用します。デフォルトの設定でも 3306 番が指定されますので、監視ホストの設定で違うポート番号を指定している場合はその番号を指定してください。

接続するデータベース、ユーザ名とパスワードを入力します。

設定例では監視用データベースの「kanshi_db」に対して監視用ユーザ「kanshi_user」で接続しています。

図 MySQL 監視

サービス監視用コマンド

データベース監視

NRPE経由でのMySQL監視

対象ホスト名またはIPアドレス 127.0.0.1

データベース名 kanshi_db

ポート番号 3306

ユーザ名 kanshi_user

パスワード ●●●●●●

NRPEタイムアウト(秒) 15

正常に監視出来たら下記のようなステータス情報となります。

(メッセージの詳細は環境により異なります)

図 正常時

現在のステータスは、**正常(OK)**

0日間と 00時間00分15秒前より継続しています。

Uptime: 230698 Threads: 1 Questions: 1571 Slow queries: 0 Opens: 15 Flush tables: 1 Open tables: 8 Queries per second avg: 0.6

5.2.2 設定項目一覧

対象ホスト名またはIP アドレス	監視対象のホスト名、もしくは IP アドレスを指定します。
データベース名	監視対象のデータベース名を指定します。
ポート番号	MySQL への接続ポート番号を指定します。
ユーザ名	MySQL 接続時のユーザ名を指定します。
パスワード	MySQL 接続時のユーザ名に対応するパスワードを指定します。
NRPE タイムアウト(秒)	NRPE 経由ホストから指定した秒数以上応答がない場合、チェックを終了し、監視ステータスを CRITICAL にします。

6 Linux PostgreSQL サーバ監視

Linux PostgreSQL サーバ監視では PostgreSQL データベースサービスを提供しているホストに対する監視パッケージです。

内容は Linux 標準監視と PostgreSQL データベースサービスに特化した監視項目です。項目一覧は 1.2.4 Linux PostgreSQL サーバ監視一覧をご参照ください。

6.1 PostgreSQL 監視

監視グループ	チェックコマンド
データベース監視	PostgreSQL 監視

監視対象ホストの PostgreSQL への接続の監視を行います。

接続の応答時間がしきい値を超える場合は、監視ステータスを WARNING または CRITICAL にします。データベースへ接続できない場合は、監視ステータスを CRITICAL にします。

この監視では、監視実行時に ps のプロセスリストに表示されます。また、接続する際にデータベース名、ユーザ名、パスワードを入力します。そのため監視の接続には権限を最小限に抑えた監視専用のデータベースとアカウントを使用することをお勧めします。

6.1.1 監視設定例

通常、PostgreSQL はポート番号 5432 番を使用します。デフォルトの設定でも 5432 番が指定されますので、監視ホストの設定で違うポート番号を指定している場合はその番号を指定してください。

接続するデータベース、ユーザ名とパスワードを入力します。

設定例では監視用データベースの「kanshi_db」に対して監視用ユーザ「kanshi_user」で接続しています。

図 PostgreSQL 監視

サービス監視用コマンド	
データベース監視	
PostgreSQL 監視	
タイムアウト(秒)	30
ポート番号	5432
データベース名	kanshi_db
接続ユーザ名	kanshi_user
接続パスワード	●●●●●●
接続応答時間WARNINGしきい値(秒)	2
接続応答時間CRITICALしきい値(秒)	8

正常に監視出来たら下記のようなステータス情報となります。

図 正常時

現在のステータスは、 **正常(OK)**
0日間と 00時間00分03秒前より継続しています。

OK - database kanshi_db (0 sec.)

6.1.2 設定項目一覧

タイムアウト(秒)	監視対象データベースがこの値を超えた場合、監視ステータスを CRITICAL にします。
ポート番号	PostgreSQL への接続ポート番号を指定します。
データベース名	監視対象のデータベース名を指定します。
接続ユーザ名	PostgreSQL 接続時のユーザ名を指定します。
接続パスワード	PostgreSQL 接続時のユーザ名に対応するパスワードを指定します。
接続応答時間 WARNING しきい値(秒)	PostgreSQL への接続に要した時間がこの値を超えた場合、監視ステータスを WARNING にします。
接続応答時間 CRITICAL しきい値(秒)	PostgreSQL への接続に要した時間がこの値を超えた場合、監視ステータスを CRITICAL にします。

6.2 NRPE 経由での PostgreSQL 監視

監視グループ	チェックコマンド
データベース監視	NRPE 経由での PostgreSQL 監視

NRPE を利用して、監視対象ホストの PostgreSQL への接続の監視を行います。
使用用途はデータベースを外部から接続許可がない時や、データベースサーバに X-MON が直接アクセスできない場合等となります。

データベースへの接続に問題がある場合は、監視ステータスを WARNING にします。
データベースへ接続できない場合は、監視ステータスを CRITICAL にします。

この監視では監視設定でデータベース名、ユーザ名、パスワードを入力しますが、監視実行時に監視対象ホストのプロセスリスト (ps コマンド) にそれら接続情報が表示されます。そのため監視の接続には権限を最小限に抑えた監視専用のデータベースとアカウントを使用することをお勧めします。

6.2.1 監視設定例

対象ホスト名または IP アドレスを入力します。

監視対象ホスト自身の場合は、ローカルホストである 127.0.0.1 を入力します。

監視対象ホストから別ホストへ接続する場合はそのホストの IP アドレスを入力してください。

通常、PostgreSQL はポート番号 5432 番を使用します。デフォルトの設定でも 5432 番が指定されますので、監視ホストの設定で違うポート番号を指定している場合はその番号を指定してください。

接続するデータベース、ユーザ名とパスワードを入力します。

設定例では監視用データベースの「kanshi_db」に対して監視用ユーザ「kanshi_user」で接続しています。

図 PostgreSQL 監視

サービス監視用コマンド

データベース監視

NRPE経由でのPostgreSQL監視

対象ホスト名またはIPアドレス 127.0.0.1

タイムアウト(秒) 30

ポート番号 5432

データベース名 kanshi_db

接続ユーザ名 kanshi_user

接続パスワード ●●●●●●

接続応答時間WARNING しきい値(秒) 7

接続応答時間CRITICAL しきい値(秒) 8

NRPEタイムアウト(秒) 15

正常に監視出来たら下記のようなステータス情報となります。

図 正常時

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

OK - database kanshi_db (0 sec.)

6.2.2 設定項目一覧

対象ホスト名またはIPアドレス	監視対象のホスト名、もしくは IP アドレスを指定します。
タイムアウト(秒)	監視対象データベースがこの値を超えた場合、監視ステータスを CRITICAL にします。
ポート番号	PostgreSQL への接続ポート番号を指定します。
データベース名	監視対象のデータベース名を指定します。
接続ユーザ名	PostgreSQL 接続時のユーザ名を指定します。
接続パスワード	PostgreSQL 接続時のユーザ名に対応するパスワードを指定します。
接続応答時間 WARNING しきい値(秒)	PostgreSQL への接続に要した時間がこの値を超えた場合、監視ステータスを WARNING にします
接続応答時間 CRITICAL しきい値(秒)	PostgreSQL への接続に要した時間がこの値を超えた場合、監視ステータスを CRITICAL にします。
NRPE タイムアウト(秒)	NRPE 経由ホストから指定した秒数以上応答がない場合、チェックを終了し、監視ステータスを CRITICAL にします。