株式会社エクストランス

X-MON3

Web コンテンツ改ざん監視(SSH)

まえがき

本書は X-MON3.4.0 より追加された Web コンテンツ改ざん監視（SSH）を実施するためのマニュアルとなっております。

本書における解説環境
X-MON ver3.4.0(一部 3.9.0)

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/

2016 年 10 月

改訂履歴
2016 年 10 月　　初版
2019 年 09 月　第二版

内容

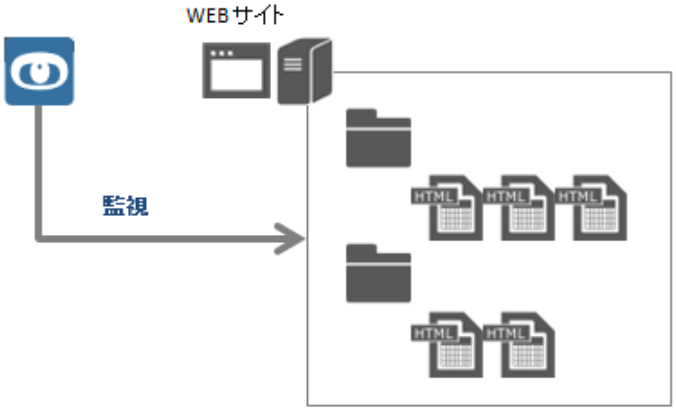
1　概要

1.1 Web コンテンツ改ざん監視(SSH)とは

X-MON3.4.0 より新機能として追加されました。

既存の「Web コンテンツ改ざん監視」とは監視方法が大きく異なり、SSH 経由でコンテンツファイルの監視を行います。

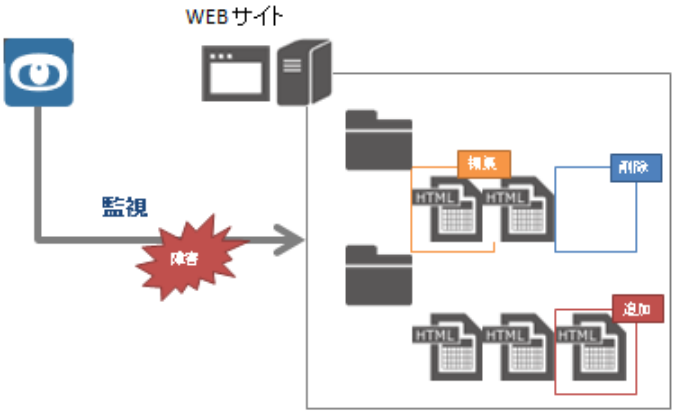
SSH 経由で接続を行う為、監視対象サーバとの事前接続設定、コマンドの準備等必要となります。(「下の 2.1 監視対象サーバでの事前準備」に準備内容を記載しております)



指定した監視するディレクトリ内のファイルハッシュを取得、記録し、次回監視時に照らし合わせファイルが追加、編集、削除されていないか監視を行います。

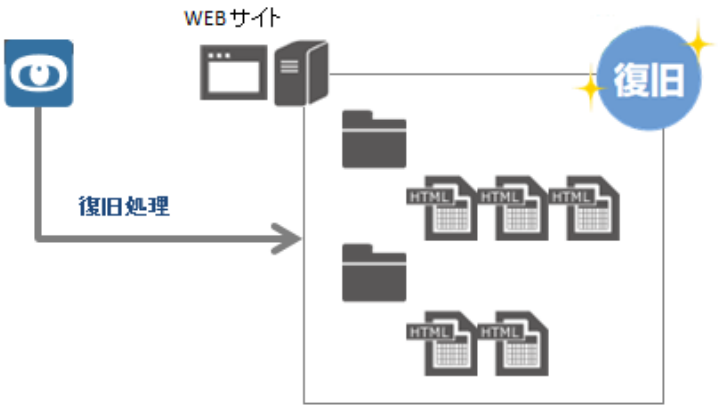
後述「2.2 サービスの登録」でサービス登録時にどのディレクトリを監視するか指定します。(ドキュメントルート直下より監視を行いたい場合「/var/www/html/」指定)

勿論、「/var/www/html/」以下のみを監視するわけではなく、「/var/www/html/」以下にあるディレクトリ内のファイルも監視対象とします。



SSH 接続にて内部ファイルの監視を行うのではなく、HTTP 接続にて WEB コンテンツの改ざん監視を行う場合は「Web コンテンツ改ざん監視」または「Web コンテンツ改ざん監視（一括監視）」をご利用ください。
「Web コンテンツ改ざん監視」「Web コンテンツ改ざん監視（一括監視）」の場合、公開鍵の登録や sudo の設定等は必要としません。監視用途等に合わせ、HTTP 接続か SSH 接続をご選択ください。

また、事前にバックアップを取得しておけば、改ざん前の正常な状態に復旧させることも可能です。
復旧処理は管理画面での手動実行と、エスカレーションコマンドによる自動実行、どちらでも行えます。



1.2 Web コンテンツ改ざん監視(SSH)でできること

SSH 経由で対象サーバへアクセスし、指定したディレクトリ内のファイルに追加・編集・削除処理があったか監視を行い、変更を検知した場合障害を発生させる。
事前に対象サーバ内にバックアップ用ディレクトリ（以降マスターディレクトリ）を用意すると、自動、または手動で変更内容を元に戻す復旧処理が行える。

1.3 監視可能なファイル数の上限について

Web コンテンツ改ざん監視(SSH)では、監視の実行時に監視対象ディレクトリ以下のファイル一覧を取得します。
ファイル数が多い場合、監視コマンドの実行時間が 60 秒を超えタイムアウトとなり、正常に監視が行えません。

弊社では以下の環境で監視が行えることを確認しております。

監視対象サーバ：Red Hat Enterprise Linux Server release 7.2
ネットワーク：同一セグメント内からのアクセス
監視対象ディレクトリ以下のファイル数：20,000 件
監視対象ディレクトリ以下のディレクトリ数：1,206 件
監視対象ディレクトリ以下のファイルサイズ：398MB

また、上記の環境で 10,000 件のファイル削除を行い、自動復旧エスカレーションにより監視が復旧することを確認しております。

処理時間は監視対象サーバの性能や、通信速度といった環境に依存いたしますので、タイムアウトが頻発するような場合、監視対象ファイル数を減らす対応が必要です。

2　サービス利用の流れ

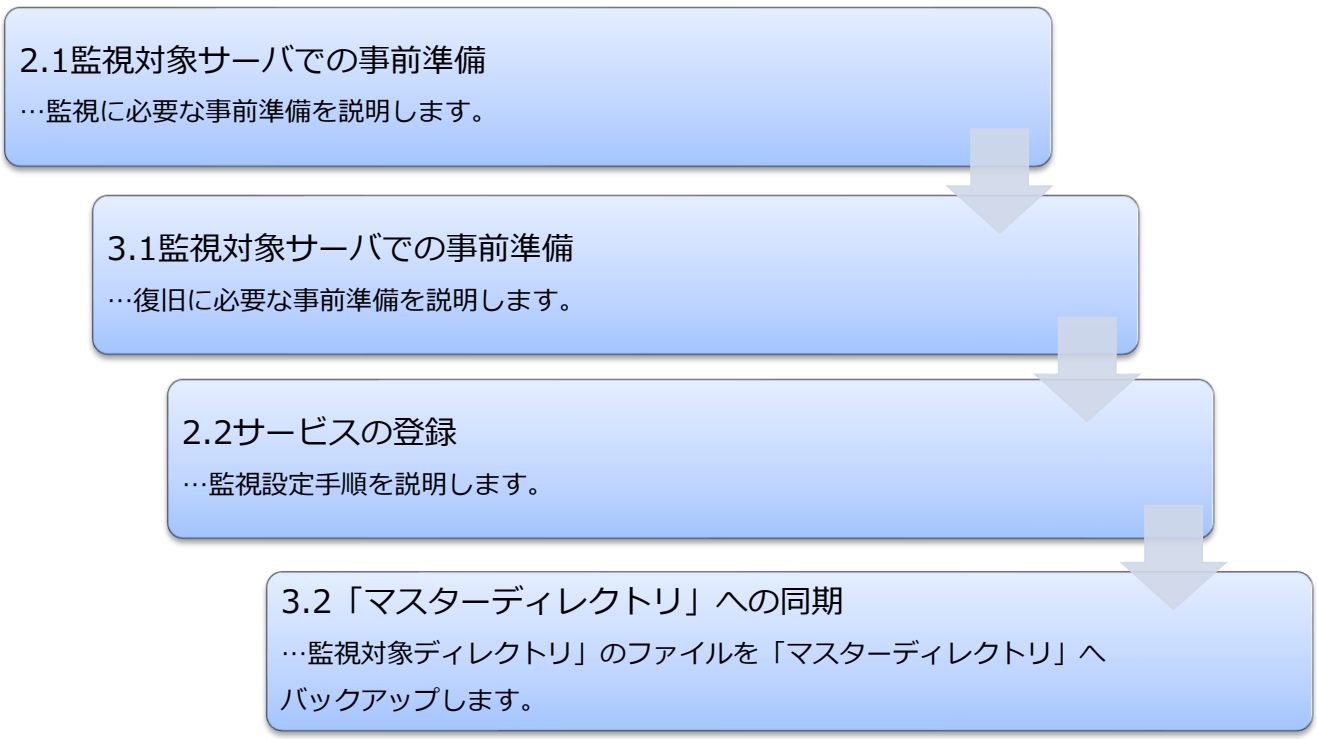
2.1 監視対象サーバでの事前準備

監視対象サーバへ接続するにあたり、以下 2 つの事前準備を行う必要があります。

1. X-MON SSH 公開鍵の登録
2. SSH ログインユーザへ sudo 権限の割り当て

復旧処理設定まで行う場合、上記事前設定とは別に追加で事前準備設定を行う必要がございます。

本マニュアルを以下のような流れで読み進めると、X-MON 操作画面と監視対象サーバを極力行き来せずに監視準備を進めることができます。
正し、以下の順に進めなければ「復旧処理設定が後々設定できなくなる」といったことはございません。
「まずはしっかり監視設定を行ってから、次に復旧処理設定を」とお考えの方は本マニュアルを順にお読みいただければ、監視→復旧設定といった流れになっております。



2.1.1　X-MON SSH 公開鍵の登録

Web ブラウザより X-MON へログインし、管理者メニュー「システム情報」より SSH 公開鍵をダウンロードし、監視対象サーバで登録を行います。

詳しい情報は、X-MON へログイン後、以下、ヘルプ画面にてご確認ください。詳しい説明を載せております。

・ヘルプ
　・チェックコマンドメニュー
　　・Web サービス監視
　　　・Web コンテンツ改ざん監視（SSH）
　　　　・事前準備

2.1.2　SSH ログインユーザへ sudo の割り当て

監視を行うにあたり、監視対象となるファイルの権限次第では監視できるもの、できないものが出てきてしまいます。そのため、本監視では sudo は必須としております。

2.2 サービスの登録

本監視を利用する場合、サービス登録時に以下の「サービス監視用コマンド」を選択します。

- グループ … Web サービス監視
- サービス監視コマンド名 … Web コンテンツ改ざん監視（SSH）

「Web コンテンツ改ざん監視（SSH)」を選択すると以下の設定項目が表示されます。それぞれ監視を行う内容に合わせ、設定を行ってください。

「マスターディレクトリパス」「除外設定」の 2 項目につきましては必須項目ではありません。

項目名		説明	入力例
SSH ポート	**必須**	SSH 接続時に利用するポート番号を指定します。 デフォルト「22」が指定されています。	22
SSH ユーザ名	**必須**	SSH 接続先で利用するログインユーザ名を指定します。 デフォルト「none」が指定されています。使用するログインユーザ名への変更をお願いします。	Root
監視ディレクトリパス	**必須**	監視対象先のディレクトリを指定します。 末尾には/(スラッシュ)を付けるようにします。	/var/www/html/
マスターディレクトリパス	任意	復旧処理を行う場合、監視対象ディレクトリのバックアップ対象となるディレクトリを指定します。 末尾には/(スラッシュ)を付けるようにします。	/tmp/backup/
除外設定	任意	監視対象先ディレクトリで監視から除外するものを監視対象ディレクトリからの相対パスで指定します。 一度監視を行ってから調整を行うこともできます。 除外指定方法は正規表現ではありませんが *(ワイルドカード)の指定は行えます。 例) *.png で拡張子 png ファイルの除外 *(ワイルドカード)の使用不使用に関係なく、全階層の除外を行うわけではありません。（image.png と除外設定すると /var/www/html/image.png は除外され、別階層にある /var/www/html/image/image.png は除外されません。）ディレクトリ毎に設定する必要があります。 複数件の除外設定が行えます。 複数件の除外設定を行う場合、|(パイプ)区切りで指定を行ってください。	監視対象ディレクトリ ・/var/www/html/ ---------- 除外したいファイル ・/var/www/html/image/001.png 設定内容 「image/001.png」 ---------- 複数件の除外したいファイル ・/var/www/html/image/001.png ・/var/www/html/.htaccess 設定内容 「image/001.png|.htaccess」

サービス新規登録時、「監視間隔（分）」は「5（分）」、「試行回数」は「3」とデフォルトで指定されています。
「監視間隔（分）」→「30」、「試行回数」→「1」等、設定内容に合わせ調整をお願いいたします。

「テスト実行」ボタンについて

必須項目の入力内容に誤りがあるかどうか確認できます。
「SSH ポート」「SSH ユーザ名」「監視ディレクトリパス」の指定に誤りがある場合（監視ディレクトリパスが存在しない、SSH ユーザ名が存在しない等）、以下のように UNKNOWN ステータスが返ります。設定内容に誤りがないかご確認ください。

正しく設定されている場合、OK ステータスを返しますが、「初回監視では比較用のデータが存在しないため、次回より監視を行います」と表示され、ここではどのファイルが監視対象だったのかまで確認は行えません。
監視対象ファイルの確認を行う場合は「4.1 除外するディレクトリ、ファイルの指定を調整する場合」をご確認ください。

サービス登録を行った後は、管理者メニュー「X-MON 再起動」で設定内容を反映させるようにしてください。

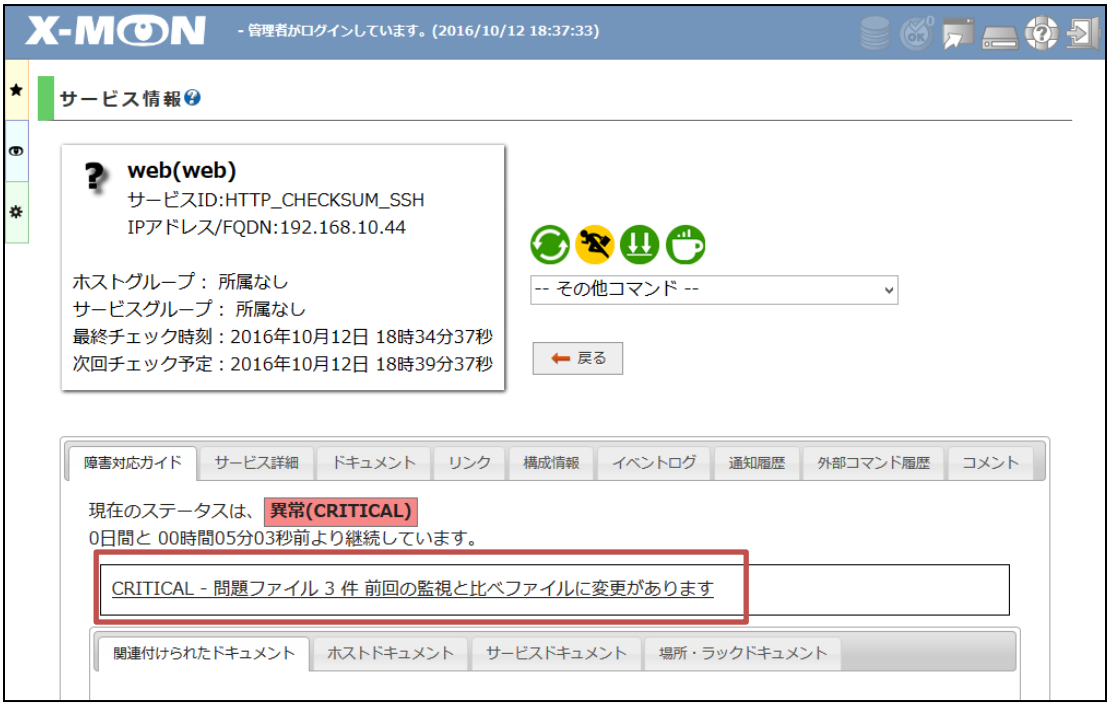
2.3 監視内容の確認

「2.1 監視対象サーバでの事前準備」と「2.2 サービスの登録」の設定情報が正しく行えている場合、正常に監視を行えます。
UNKNOWN ステータス等を返す場合、設定情報の再確認をお願いいたします。

正常に監視が行えている場合も、初回監視のみ次回監視より比較に利用するファイルハッシュ一覧を取得する必要があるため「OK – 初回監視では比較用のデータが存在しないため、次回より監視を行います」と表示されます。

ファイルを比較し、追加・編集・削除ファイルの有無を検知できるようになると「OK – 問題ファイル 0 件 前回の監視と比べファイルに変更はありませんでした」と表示されるようになります。

監視対象ディレクトリ下でファイルに対し追加、編集、削除操作を検知した場合「CRITICAL – 問題ファイル〇件 前回の監視と比べファイルに変更があります」と表示されます。



上記赤枠、「ステータス情報」部分をクリックすると監視詳細画面へ遷移します。

以下のページから監視詳細画面へ遷移できます。

「サービス情報」画面　「ステータス情報」部分

「サービス一覧表示」画面　「ステータス情報」部分

「Web 改ざん警告管理」画面　「SSH 接続」→ 対象サービス「詳細情報」ボタン

上から順に最新の履歴から表示されています。

最大 10 件まで履歴が表示され、監視が正常だった場合と異常だった場合で表示項目が異なります。

	正常	異常
フォーマット	{監視時刻} 正常 監視対象ファイル {数}件	{監視時刻} 異常 監視対象ファイル {数}件 追加、編集、削除件数 {数}件 追加されたファイル {ファイル名} 編集されたファイル {ファイル名} 削除されたファイル {ファイル名}

例	2016-10-07 22:45:05 正常 監視対象ファイル 8 件	2016-10-07 22:46:16 異常 監視対象ファイル 9 件 追加、編集、削除件数 3 件 追加されたファイル /var/www/html/redirect.php 編集されたファイル /var/www/html/index.html /var/www/html/.htaccess 削除されたファイル なし

また、以下の条件の場合、履歴が追加されます。

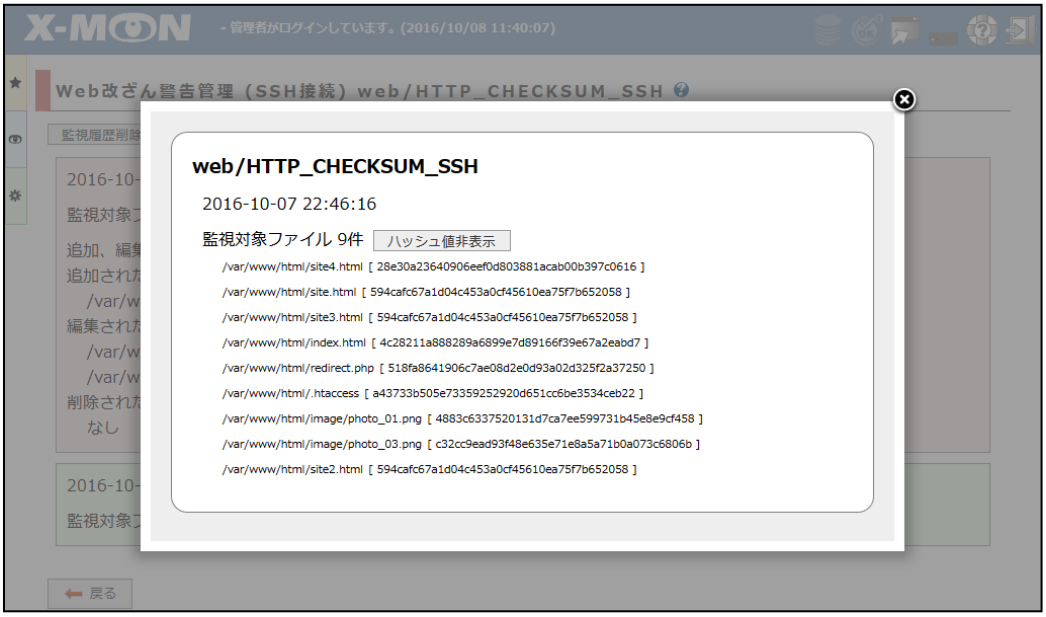
・監視比較を行い、最初の結果の場合

・前回の追加・編集・削除ファイルと、比較しファイル数に変更がある場合

（ハッシュ値までの比較は行いません。）

・前回の履歴が異常、次の監視結果が正常だった場合

「ファイル詳細」ボタンをクリックすると対象監視時刻に監視対象となったファイル名の一覧と sha1sum のハッシュ値を表示します。



監視履歴情報は X-MON のバックアップには含まれません。

3　復旧処理利用の流れ

3.1 監視対象サーバでの事前準備

1.　「監視対象サーバでの事前準備」の実施

復旧処理を行う場合も同様に「X-MON SSH 公開鍵の登録」「SSH ログインユーザへ sudo の割り当て」作業は必要になります。作業を終えていない方は再度事前準備項目をご確認いただき設定の程よろしくお願いいたします。

サービス監視時に本作業を終えている方は 2 度行う必要はございませんので、以下の準備より作業をお願いいたします。

2.　rsync コマンドのインストール

復旧処理、または同期処理を行う場合、事前に rsync コマンドをインストールしておく必要がございます。

3.　「マスターディレクトリ(バックアップ)」の準備

本監視では監視対象サーバとは別に rsync サーバを用意し、rsync サーバから復旧用ファイルを同期するといったことは行えません。

監視対象サーバ内にバックアップ用のディレクトリを用意していただくことになります。

監視対象サーバへ SSH 接続する。

バックアップを取得したい箇所にディレクトリを生成する。

3.2 「マスターディレクトリ」への同期

「マスターディレクトリ」への同期を行う場合、「2.2 サービスの登録」が済んでいる必要があります。

「OK – 問題ファイル 0 件 前回の監視と比べファイルに変更はありませんでした」と正常に監視をし始めた段階で、「監視対象ディレクトリ」に以下のファイルを置いてください。

- __renew.txt (アンダーバーを先頭に 2 つ付けます)

「監視対象ディレクトリ」以下に存在するファイルを rsync コマンドを利用し、「マスターディレクトリ」へバックアップします。

同期処理を実行すると、「OK – ディレクトリの同期を行いました」と表示されます。

これで復旧処理を行う準備は整いました。

復旧処理は次章以降に以下の自動・手動復旧手順を記載しております。自分に合った方をご利用ください。

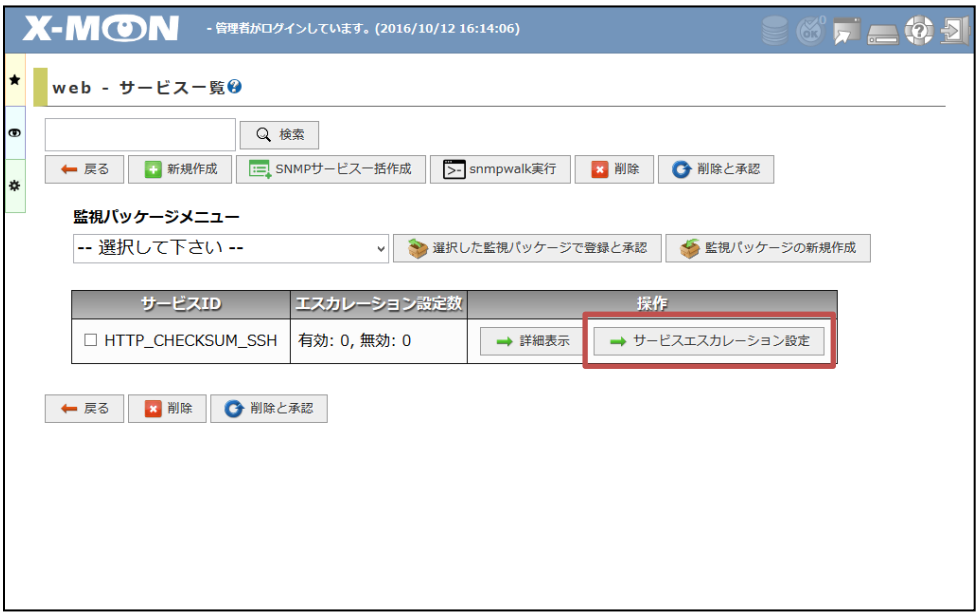
	自動復旧の場合	手動復旧の場合
方法	エスカレーション設定	Web 改ざん警告管理の復旧ボタン
メリット	自動で差し戻るため、改ざんされた場合すぐにコンテンツの復旧が行える	どのファイルが追加、編集、削除されたのか確認が可能
デメリット	どのファイルが追加、編集、削除されたのか確認しないまま、差し戻し処理が実行される	急ぎ修正を必要とする場合、ボタンを押すまで復旧処理が走らない。

3.3 自動復旧

3.3.1　エスカレーション設定(3.8.0 以前のバージョン)

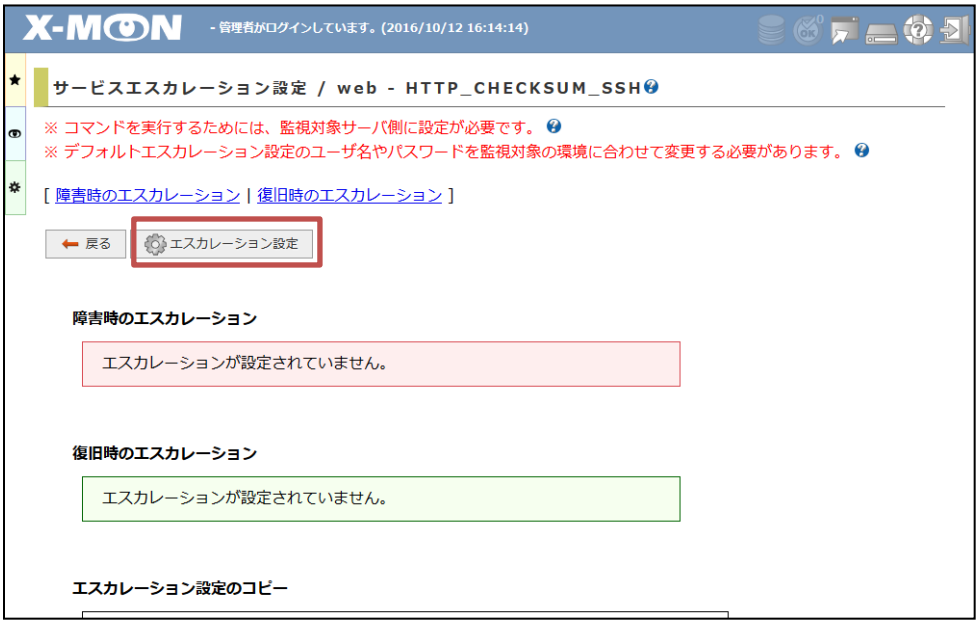
障害発生直後に自動復旧を行う場合、エスカレーション設定を利用します。

「サービス管理」画面より「サービスエスカレーション設定」ボタンをクリックし「エスカレーション設定」画面へ遷移します。



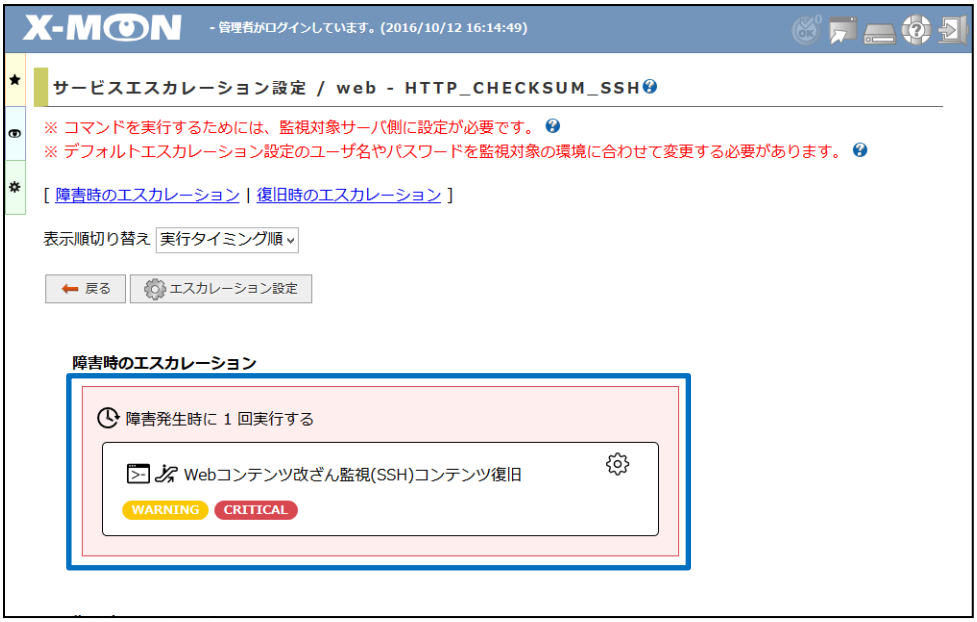
エスカレーション設定を行うには「エスカレーション設定」ボタンをクリックします。

ポップアップ画面が表示されます。



エスカレーション設定画面では「追加」ボタンをクリックすると設定パネルが表示されます。
X-MON3.4.0 よりエスカレーションコマンド設定に「Web コンテンツ改ざん監視（SSH）コンテンツ復旧」が追加されました。こちらを選択し「設定と承認」をクリックします。

設定されると、以下青枠のように設定内容が表示されます。
正しく設定されている場合、管理者メニュー「X-MON 再起動」をクリックし設定内容を反映させてください。



3.3.2　エスカレーション設定(3.9.0 以降のバージョン)

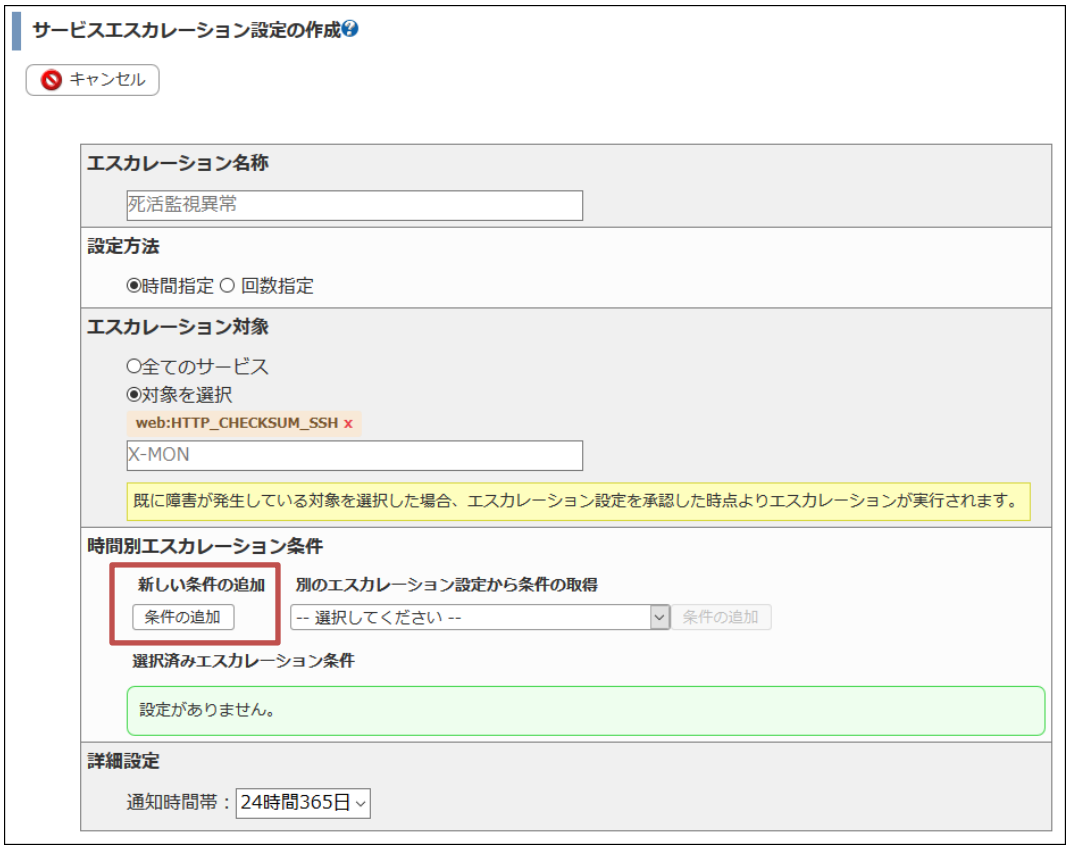
障害発生直後に自動復旧を行う場合、エスカレーション設定を利用します。

「サービス管理」画面より「サービスエスカレーション設定」ボタンをクリックし「エスカレーション設定」画面へ遷移します。

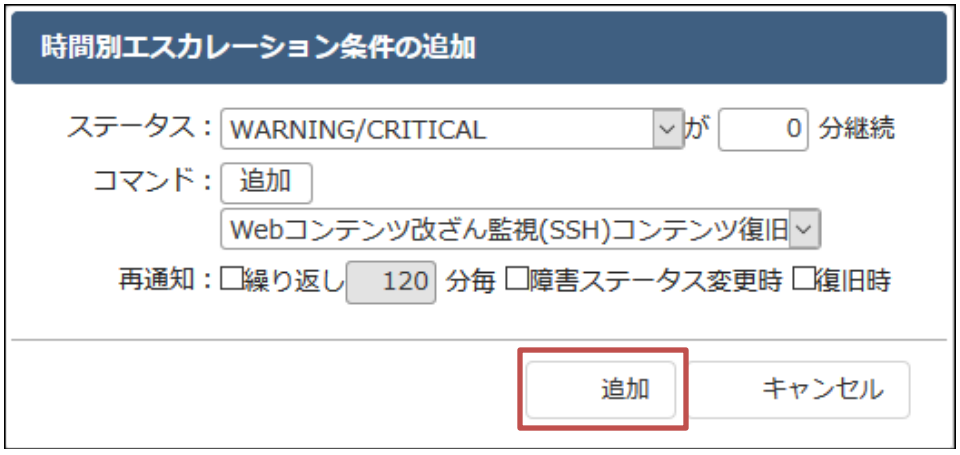
サービスエスカレーション設定画面が表示されますので、「新規作成」ボタンをクリックします。

設定画面が表示されますので、エスカレーション名称に任意な名称を入力し、新しい条件の追加からエスカレーション条件を入力します。

※エスカレーション対象はデフォルトで遷移元のサービスが選択されているため、操作は不要です。



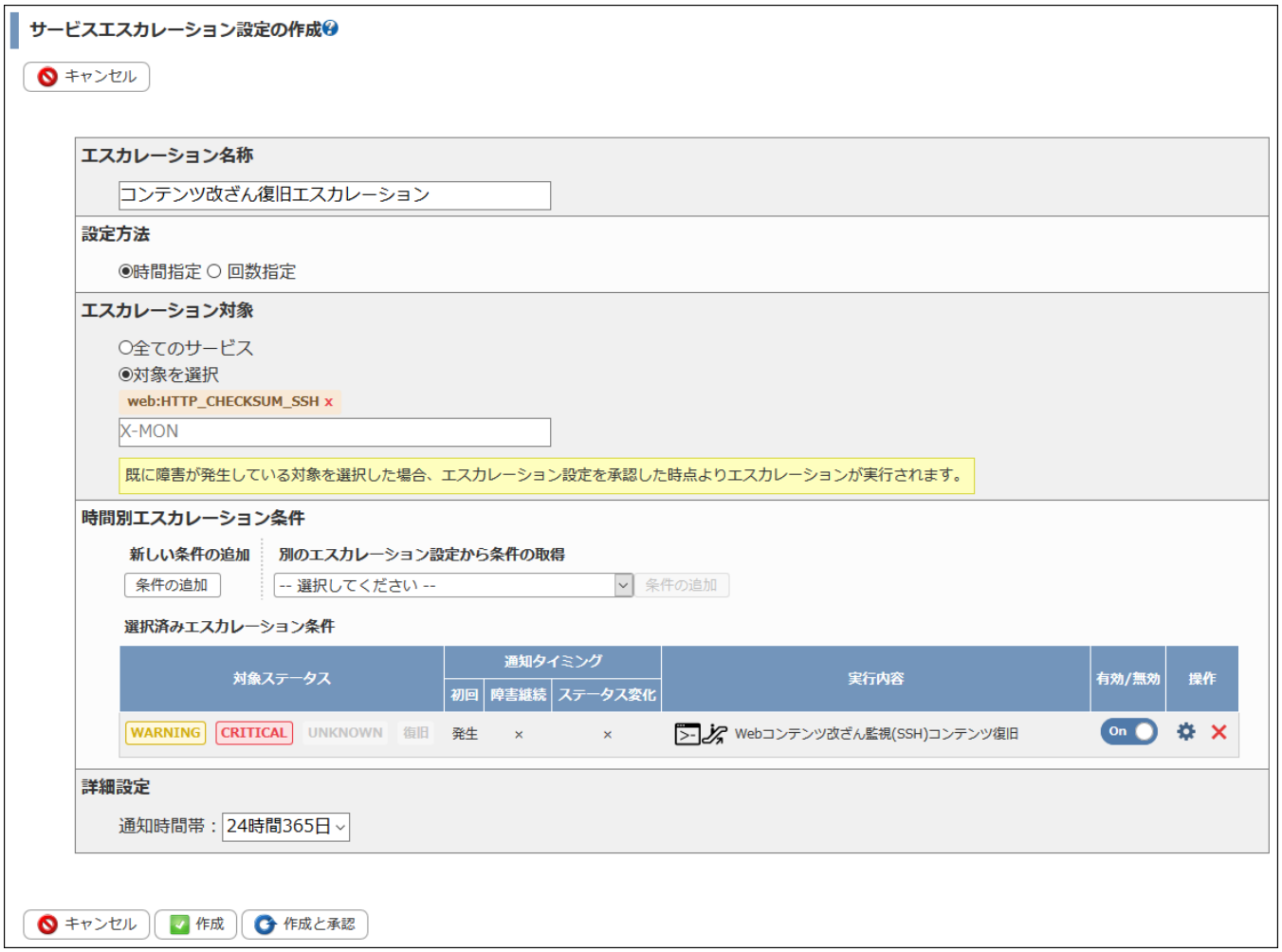
表示された画面でエスカレーション条件を入力し、「追加」ボタンを押します。



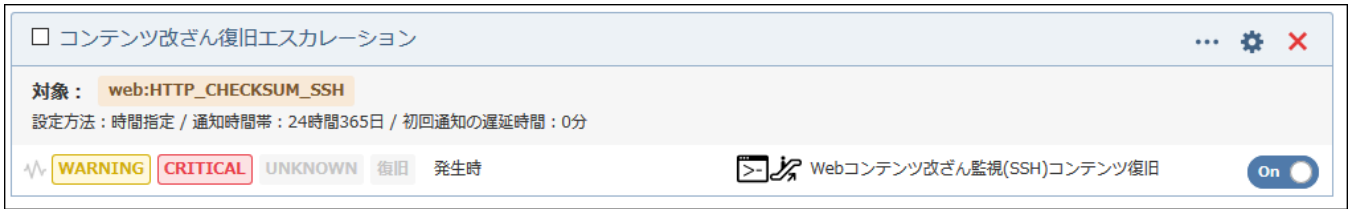
上記の例は、改ざんが起こった際に 1 度だけ復旧コマンドを実行する設定です。

コマンドは「コマンド実行」より「Web コンテンツ改ざん監視（SSH）コンテンツ復旧」を選択します。

エスカレーション条件を追加した状態です。



「作成と承認」ボタンをクリックするとエスカレーション設定が登録されます。



以上で、エスカレーション登録は完了です。

3.4 手動復旧

どのファイルが追加、変更、削除があったのか確認を行ってから復旧を行う場合、管理画面「Web 改ざん警告管理」を利用します。

対象ファイル名や、ファイル sha1sum ハッシュ値の確認は行えます。しかし、対象ファイルの内容（どこの行がどういったように修正が加わったのか）までは X-MON の画面では確認は行えません。

障害発生後、以下のページから監視詳細画面へ遷移します。

「サービス情報」画面 「ステータス情報」部分

「サービス一覧表示」画面 「ステータス情報」部分

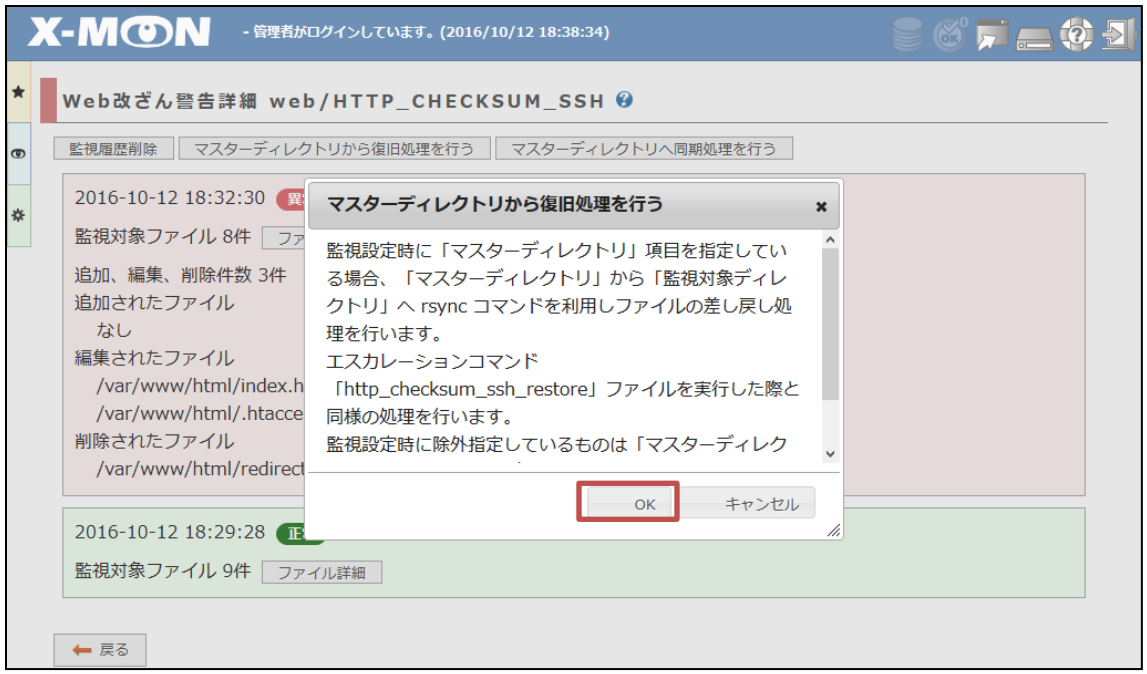
「Web 改ざん警告管理」画面 「SSH 接続」→ 対象サービス「詳細情報」ボタン

上記赤枠、「マスターディレクトリから復旧処理を行う」ボタンをクリックします。

ボタンをクリックした瞬間に処理が実行されるわけではございません。確認画面を挟みます。

確認画面に表示されている注意事項をよく読み、「OK」ボタンをクリックします。

これでマスターディレクトリから監視対象ディレクトリへファイルの差し戻し処理を行います。



無事処理を終えると、以下青枠部分に案内が表示されます。

4　場面ごとの対処方法

4.1 除外するディレクトリ、ファイルの指定を調整する場合

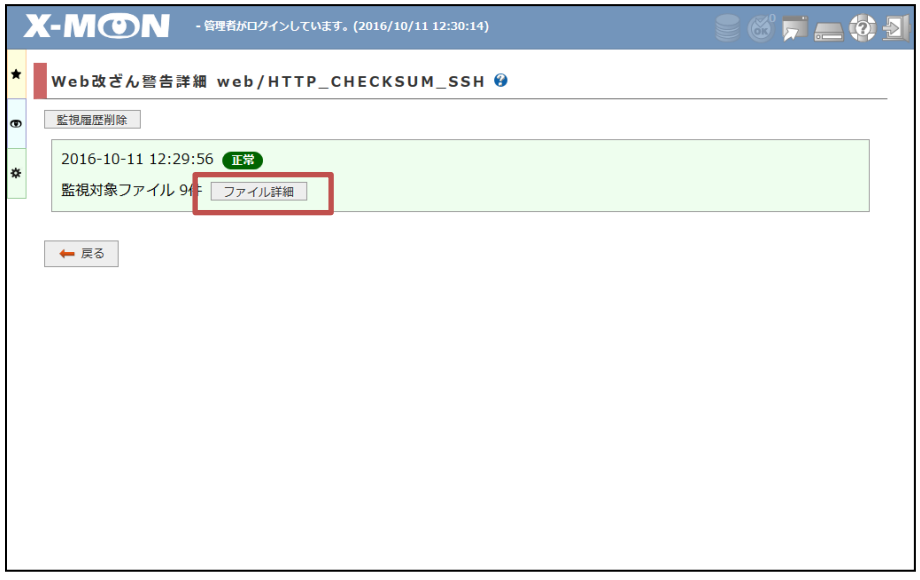
「2.2 サービスの登録」時点で初めから除外指定を的確に行うことは難しいものがあります。

以下のサイクルを活用し、除外指定の調整を行ってください。

1.　監視しているファイルの一覧を確認する。

正常に監視が行われた後、「Web 改ざん警告管理（SSH 接続）」画面へ遷移します。

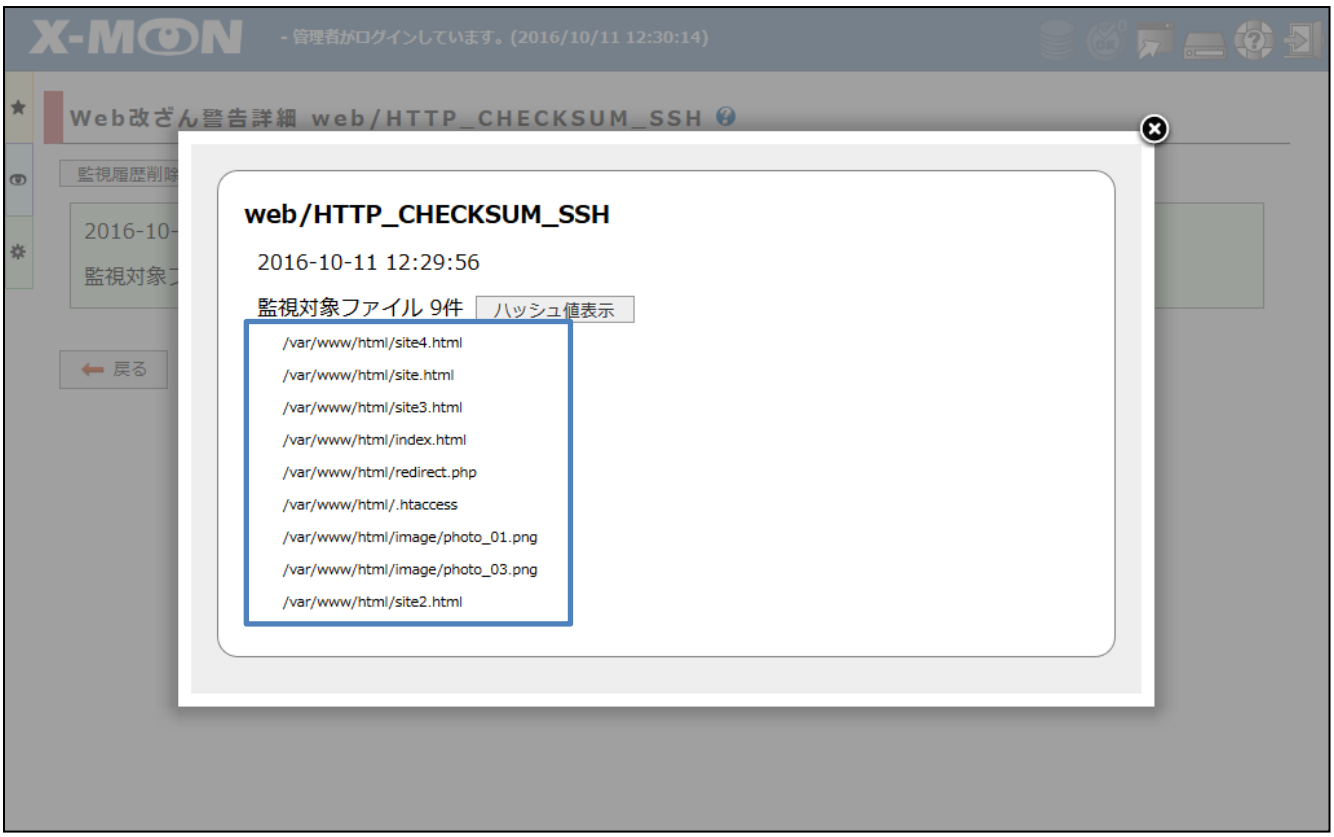
最新の監視結果横に表示されている「ファイル詳細」ボタンをクリックします。



ポップアップウィンドウが表示され、以下青枠部分に表示されているファイル一覧が監視対象としてファイルハッシュを取得した一覧になります。

除外したファイルは、以下の青枠部分にも表示されません。

除外したいファイルが表示されている場合、サービスの編集より除外設定を再度行い、管理者メニュー「X-MON 再起動」で設定内容を再反映させます。



2.　「監視履歴削除」ボタンで最新のハッシュと履歴を削除し、監視を初期化する。

以下、赤枠内「監視履歴削除」ボタンをクリックします。

「監視履歴削除」ボタンを利用すると、最新のハッシュ情報（前回の記録）と履歴情報を削除し、監視を初期化します。

履歴情報というのは、以下、青枠内の情報のことを指しています。

「監視履歴削除」ボタンを利用し、履歴の削除が実行されても、全ての Web 改ざん監視（SSH）の履歴が削除されるわけではございません。対象サービスの履歴のみ削除を行います。

4.2 運用開始後、ファイルの更新や削除を行う場合

監視対象サーバでファイルを自分で更新する際に「改ざん」として検知されてしまうと、意図した更新であっても復旧処理で差し戻る恐れがあります。

以下の手順を踏むことで「改ざん」として検知されないようにファイルの差し替えを行うことが可能です。

1.　「監視対象ディレクトリ」直下に「__stop.txt」ファイルを設置

「__stop.txt」は空ファイルで結構です。

本ファイルを設置すると、一時的に監視処理をスキップさせることができます。

監視対象サーバ

```
[root@localhost ~]# cd /var/www/html/
[root@localhost html]# touch __stop.txt
```

「__stop.txt」を設置している間は、監視自体は実行され続けますが、ファイルハッシュの取得、比較と言った監視処理は行いません。ステータス情報には「OK – コンテンツの更新中です」と表示され続けます。

2. コンテンツの更新

FTP クライアントでファイルの差し替え、SSH クライアントで直接ファイルの操作を行ってください。

3. 「監視対象ディレクトリ」直下に「__renew.txt」ファイルを設置

こちらも空ファイルで結構です。「__renew.txt」を設置しても「__stop.txt」が存在する限り監視処理が実行されることはありません。

監視対象サーバ

```
[root@localhost ~]# cd /var/www/html/
[root@localhost html]# touch __renew.txt
```

4. 「__stop.txt」ファイルの削除

「__renew.txt」ファイルは削除しなくて結構です。「マスターディレクトリ」を指定している場合、マスターディレクトリと、前回のハッシュ値を更新後、「__renew.txt」ファイルを削除します。「マスターディレクトリ」を指定していない場合、前回のハッシュ値を更新後、自動で「__renew.txt」ファイルを削除します。

正しく同期処理を行うと「OK – ディレクトリの同期を行いました」と表示されます。

4.3 障害として検知した内容が正しい反映だった場合

前述「4.2 運用開始後、ファイルの更新や削除を行う場合」を行わず、正しい変更だったにも関わらず障害として検知してしまった場合、マスターディレクトリへ同期し、前回のハッシュ結果を現在の状態に移行することができます。

「Web 改ざん警告詳細」画面で障害が発生している際に表示される 「マスターディレクトリへ同期処理を行う」ボタンをクリックします。

表示内容をしっかり確認し、問題がなければ「OK」ボタンをクリックしてください。
「OK」ボタンをクリックすると、「マスターディレクトリ」へ同期後、前回のハッシュ結果記録を現状の結果に更新します。

4.4 「マスターディレクトリ」を変更する場合

既にある「マスターディレクトリ」から、別のマスターディレクトリへ変更する場合、旧マスターディレクトリから新マスターディレクトリへ移行する機能はございません。
以下の手順で変更作業を行えます。
一部、監視対象サーバへ SSH クライアント等でログインし操作する必要がございます。

以下、手順途中では間を空けず作業を行ってください。
マスターディレクトリが空ディレクトリ（__renew.txt による同期処理）を行わないまま障害が発生すると正しく復旧処理が行えません。

1. 監視対象サーバ側で新たなバックアップ用ディレクトリを作成する
2. X-MON 管理者メニュー「サービスの編集」画面で対象サービス（Web コンテンツ改ざん監視（SSH）を行っているサービス）で新たに作成したディレクトリを指定する
3. X-MON 管理者メニュー「X-MON 再起動」で設定内容を反映する
4. 「3.2「マスターディレクトリ」への同期」を参考に__renew.txt ファイルを監視ディレクトリへ設置し、新たなマスターディレクトリへ監視ディレクトリのファイルを同期する
5. X-MON ステータス情報に「OK – ディレクトリの同期を行いました」と表示されるのを確認する
6. 監視対象サーバ側で旧マスターディレクトリを削除する