REDMINE
flexible project management

セキュリティ担当者必見！
オープンソースではじめる

CSIRT インシデント管理

Computer Security Incident Response Team

オープンソースのタスク管理ツール「Redmine」で、
インシデント管理をはじめよう！

**組織内のセキュリティインシデントの管理方法のひとつに、オープンソースのRedmineを活用する例があります。
本紙では、企業等のCSIRT（コンピュータ セキュリティ インシデント レスポンス チーム）におけるインシデントハンドリングをRedmineで行うための設定例をご紹介します。**

本記事はウェブサイトでもご覧頂けます　blog.redmine.jp/articles/redmine-for-csirt/（短縮URL：goo.gl/UmSs4c）

CSIRTとインシデントハンドリング

組織のセキュリティ対策のトライとして **CSIRT（コンピュータ セキュリティ インシデント レスポンス チーム）** が注目されています。 CSIRTの中心となる活動の一つが **インシデントハンドリング** です。

インシデントハンドリングとは

インシデント発生から解決までの処理全般の活動を指します。インシデントの発生から解決までには事象の発見から情報収集・判断・対応・内外への報告など多くの活動が伴います。

活動の状況を関係者で共有すること、過去に取り組んだ対応を見直すなど、活動の運用をシステム化するメリットは大きいです。

発生したインシデントの管理をオープンソースのタスク管理ツール Redmine を使って行う事例が増えてきています。強力な課題管理機能を備える **Redmine** はインシデントハンドリングにも適しています。

Redmineによるインシデント管理画面の例

インシデント管理に活用できるRedmineとは

REDMINE
flexible project management

Redmineとは、webベースでタスク管理・情報の集約管理が行えるオープンソースのソフトウェアです。誰でもダウンロードして利用できます。使用方法などの情報をインターネット上で容易に入手でき、市販の解説書も充実していることから、タスク管理の定番のソフトウェアとなっています。

Redmineでこんな課題を解決！

- 表計算ソフトでの管理に限界を感じている → チケット管理で進捗が明確化！
- インシデント発生を検知したらすぐ管理対象にしたい → メールトリガーでチケット登録
- 処理の流れを細かく管理したい → ワークフローできめ細かく設定可能

Redmineによるインシデント管理

インシデントの管理では記入する内容はエビデンスとして情報の改ざんから守る必要があります。Redmineではログインユーザ毎に権限を細かく設定できるため、登録された情報の誤削除や改ざんなどを防ぐことができます。

またチケット操作について操作者や操作時刻、変更差分が自動的に記録されますので安心して利用することができます。

そして、対応の経過をいくらでも履歴として追記することができるため、表計算ソフトなど帳票で管理する場合と比べ、柔軟に運用することが可能です。

子チケット

その他インシデントに関連し行わなければいけない活動を **子チケット** として管理することで、

子チケット

~~タスク #18816~~: サーバセグメントSWの手配
~~タスク #18817~~: SW交換作業

関連するチケット

関連している ~~インシデント報告 #18848~~: 2018-01-15 System Alert on mail.example.com

インシデント発生から解決まで一連の活動を関係づけることができます。類似のインシデントや関係する事象などは **関連するチケット** として関係づけておくことにより他のインシデントの対応などと連携づけることもできます。

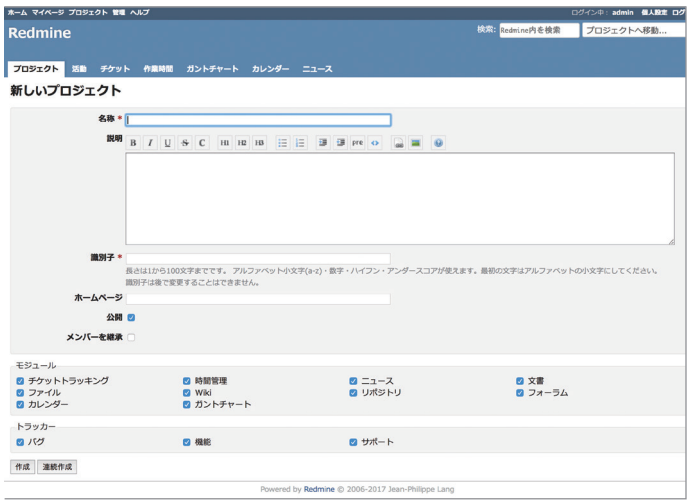
インシデント管理用の設定

インシデント管理専用にRedmineを使用する事もできますが、既に利用しているRedmineに組み込むこともできます。どちらの場合でもRedmineのデフォルトの項目とは管理する内容が異なるためインシデント管理用に個別の設定をすることにします。以下、その設定について説明します。

プロジェクトの設定

1.プロジェクト

Redmineでは プロジェクト という単位で個別の設定をすることができます。
[管理]→[プロジェクト]→[新しいプロジェクト]



プロジェクトごとに個別に以下の設定が行えます。
メンバーと権限／処理の流れ／個別項目／項目の表示設定

2.トラッカー

インシデント管理の様な特別なプロジェクトに対し専用の項目や処理の流れを組み込む場合、専用のトラッカーを作成し適用します。
※トラッカーが増えすぎると管理が大変です。トラッカーは必要最小限で作成しましょう。

トラッカーの作成画面で
・何のプロジェクトで使用するか
・デフォルト項目のうち使用するものはどれか
を指定します。

またチケットのデフォルト状態を指定できます。
一般的なタスクであれば 新規 の状態からチケットを起票しますが、実際にインシデントが発生した際は、起票より対応が優先すると考えられます。

起票するタイミングでは既にインシデントやインシデントへの対応は進んでいる事が想像できますので、進行中 をデフォルトのステータスとして設定します。

トラッカーの詳細な使い方については下記のページをご参照ください。

【参考ウェブサイト】
Redmineワンポイントチェック(5): トラッカーを正しく使おう
blog.redmine.jp/articles/opc/tracker/

フィールドの追加

インシデントの管理では事象の性質や影響、情報源など管理すべき項目(＝フィールド)が多岐に渡ります。事象の共有や事後の分析のためにも必要となるフィールドを増やす必要があります。

Redmineでは標準のフィールドの他に カスタムフィールド で追加することができます。
[管理]→[カスタムフィールド]→[新しいカスタムフィールド]

カスタマイズのサンプルとして今回は次のフィールドを追加します。

項目	内容	フィールドの種類	選択肢など
情報源	インシデントの発見・検出元	リスト（複数選択可）	システムからの通知 社外からの連絡 社内からの連絡 その他
インシデント重要度	重要度の指標を選択	リスト（複数選択可）	個人情報を含む 社外への影響がある 法令違反（の可能性がある） 再発インシデント
インシデント種別	インシデントの種別	リスト（複数選択可）	マルウェア関係 情報紛失・流出 システムトラブル その他
役員への報告	インシデントの経過が経営層に伝わっているか	リスト（複数選択可）	要 済
事象経過	インシデントに関する発生の経過	長いテキスト	
一次対応内容	一時的にインシデントを抑えるために行った内容	長いテキスト	

リスト型としては リスト と、キー・バリューリスト の2種類ありますが、リスト型を選択しました。

キー・バリューリストは値にリスト選択肢文字が割り当てられるため、選択肢文字の設定を変更すると既に登録済みのチケットの内容も変更されます。

とても便利な機能ですが、インシデント管理ではそれぞれのチケットは内容を変更せず、記録として残すべき対象と考えられます。

今回はあえてリスト型を採用しています。

設定例：情報源

設定例：事象経過

カスタムフィールド作成画面で対象となるトラッカーとプロジェクトにチェックを入れることで利用可能になります。

表示フィールドのカスタマイズ

画面上に不必要なものが表示されていると操作者は混乱してしまいます。これらを整理します。

まずトラッカーとワークフローで不必要なフィールドを消しましょう。

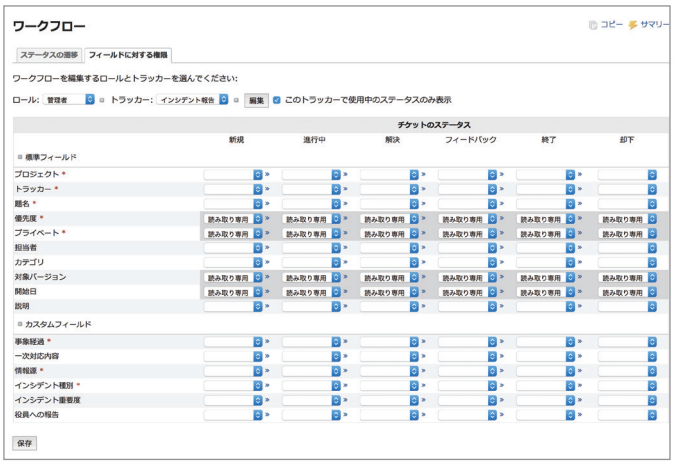
1.トラッカー

使用するトラッカーにて標準フィールドの項目から使用しないフィールドのチェックを外します。指定したトラッカーではチェックを外したフィールドは使用しないことになります。
[管理]→[トラッカー]

2.ワークフロー

フィールドに対する権限 のタブにてフィールドの表示を消すことができます。

使用しないフィールドを 読み取り専用 とすることでそのフィールドが表示されなくなります（システム管理権限を持っているアカウントでは表示されます）。
[管理]→[ワークフロー]



【参考ウェブサイト】
Redmine 2.1新機能紹介: トラッカー/ロール/ステータスごとにチケットの項目を必須・読み取り専用に設定可能
blog.redmine.jp/articles/new-feature-2_1/configurable-require-fields/

3.プロジェクト

画面上部で選択出来るRedmineの機能で使用しないものも消してしまいましょう。プロジェクトの設定からモジュールタブを選び不必要な機能のチェックを外します。
[プロジェクト]→[プロジェクト名]→[設定]→[モジュール]

変更前

変更後

チェックを外して更新すると、使用しない機能がメニュー上に表示されなくなりました。

続いて、ガイダンス文章を画面内に表示する方法について説明します。

ガイダンス表示

インシデント報告は多くの状況から対応を管理する必要があるため、できるだけ詳細に事象を把握している当事者が起票した方が望ましいです。

しかしながら滅多に使用しないシステムの画面を操作するのは難しいですし、インシデントの報告となると起票する行為自体気が重い作業です。

できるだけ難しさを省くためにもガイドとなる文章を表示しておくといくらかは楽になると思います。

Redmineには画面を装飾する機能はありませんが、View-Customizeプラグインを使用するとCSSやJavas-criptを挿入することができます。

【参考ウェブサイト】
GitHub - onozaty/redmine-view-customize: View customize plugin for Redmine
github.com/onozaty/redmine-view-customize

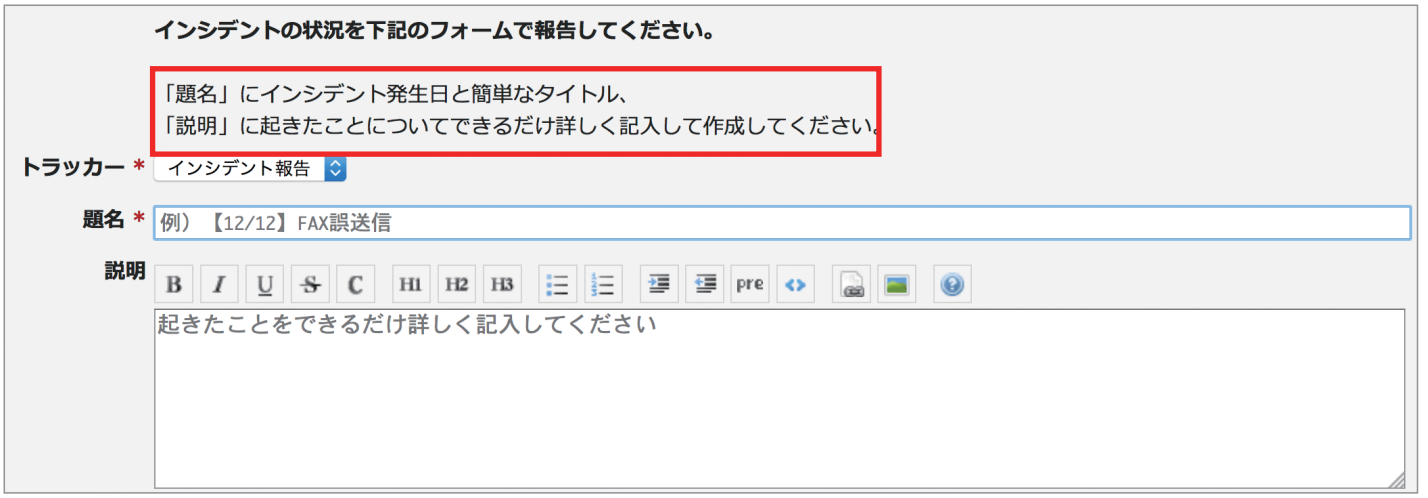
README.mdの通りインストールすると管理画面に設定項目が表示されます。

起票ガイドの例を示します。

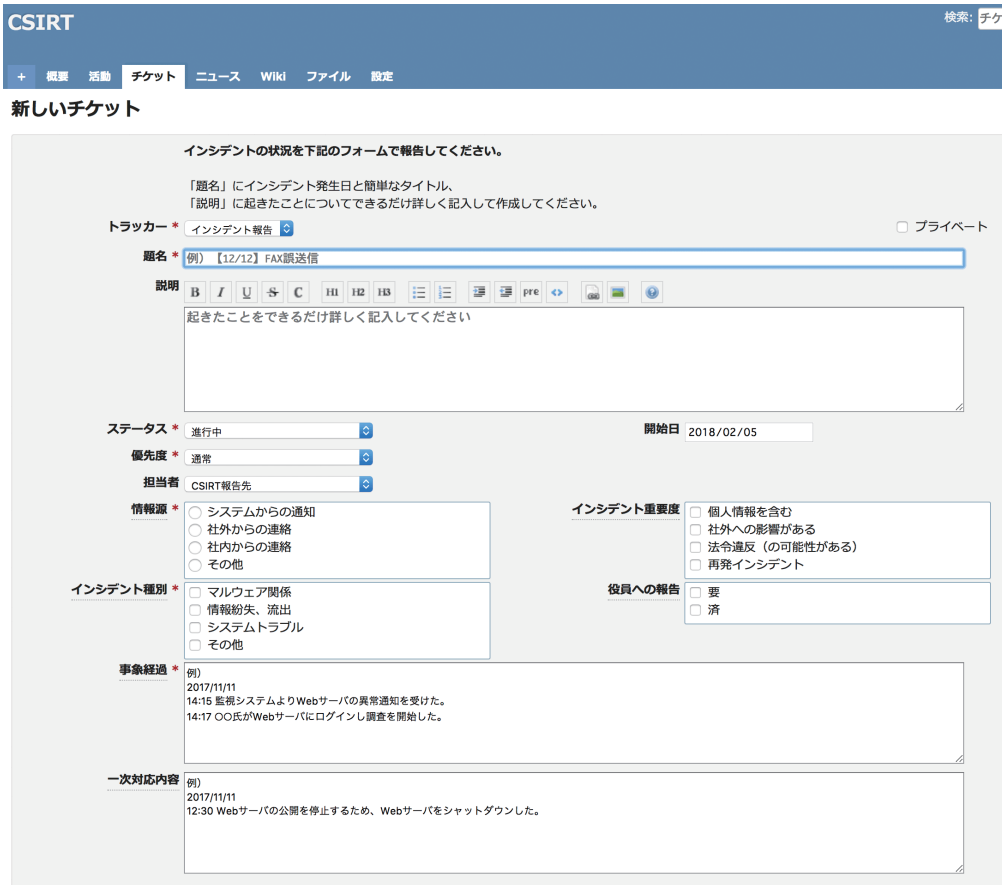
上の図では下の表の内容を設定しています。

Path Pattern	/projects/csirt/issues/new
Type	Javascript
Code	$(function() { $('select#issue_assigned_to_id').val('13'); var guideText = ' インシデントの状況を下記のフォームで報告してください。 「題名」にインシデント発生日と簡単なタイトル、 「説明」に起きたことについてできるだけ詳しく記入して作成してください。 '; $('div#all_attributes').prepend(guideText); var sampleSubject = '例）【12/12】FAX誤送信'; $('input[name = "issue[subject]"]').attr('placeholder', sampleSubject); var sampleDescription = "起きたことをできるだけ詳しく記入してください"; $('textarea[name = "issue[description]"]').attr('placeholder', sampleDescription); $('textarea[name = "issue[description]"]').attr('rows', "6"); })();

これにより、Path PatternにURLがマッチしたページで、このJavascriptが動作し、以下のような表記を画面上部に挿入します。



これらの設定で次ページのような起票画面を作る事ができました。



インシデント報告用のチケット例

最後に

まずは簡単なところからはじめよう

今回はRedmineでインシデントを登録する簡単なサンプルを紹介しました。 このほかにもいろいろなアイデアでそれぞれの組織に合ったインシデントハンドリングのツールを作ることができます。

インシデント管理の方法が既に確立されているところはそれを具体化できれば良いですが、まだ試行錯誤されている組織ではしっかりとしたものを作り上げるより、まずは簡単なところから使い始めて記録を残していき、チームなりの良い形を探っていくのが良いでしょう。

Redmineのクラウドサービス 無料でお試しできます！

発行・お問い合わせ先

FAR END Technologies
ファーエンドテクノロジー株式会社
〒690-0003 島根県松江市朝日町498番地 松江センタービル
お問い合わせ www.farend.co.jp/go/support/

SaaS提供に関わる企画、開発及び運用において
ISO 27001 認証取得
（情報セキュリティマネジメントシステム）

10th anniversary
ファーエンドテクノロジー10周年特設サイト公開中
www.farend.co.jp/10th/