



第 17 章 ケース管理

この章の具体的な内容は次のとおりです。

- ・ ケース管理の概要
- ・ ケース バーの表示/非表示
- ・ 新しいケースの作成
- ・ 現在のケースの編集および変更
- ・ ケースへのデータの追加
- ・ ケース レポートの生成および電子メールでの送信

ケース管理の概要

ケース管理機能を使用すると、ユーザが選択した MARS データをケースという専用レポートに取り込んで、結合、保護できます。ケースに追加できるデータは、次のとおりです。

- ・ テキスト注釈
- ・ Incident ID ページ
- ・ インシデント デバイス情報 (送信元 IP アドレス、宛先 IP アドレス、レポート デバイス)
- ・ Session Information ページ
- ・ Query Results ページ
- ・ Build Report ページ
- ・ Report Results ページ
- ・ View Case ページ (現在のケースから別のケースを参照できる)

すべてのユーザが、すべてのケースを作成または変更できます。同じマシン上の MARS ユーザにケースを割り当てたり、ケースのステータスを assigned (割り当て済み)、resolved (解決済み)、closed (終了済み) に変更できます。ケースの内容は単一の GUI (グラフィカル ユーザ インターフェイス) ページ (View Case) にカテゴリ別に表示され、自動的にアセンブルされて、単一の HTML ケース ドキュメントが生成されます。ケースに割り当てられた MARS ユーザにケース ドキュメントを電子メールで送信できます。



注 ケースが終了済みの場合は、テキスト注釈のみを追加できます。

インシデント、セッション、クエリー、レポート、および軽減ログで収集されたケース情報は、次の項目に関する法的根拠となります。

- ・ 監査 (適合規格監査など)
- ・ Access Control List (ACL; アクセス制御リスト) やポリシー変更の正当化
- ・ MARS フォールス ポジティブの調整に関する注意事項
- ・ 許可および禁止する動作例

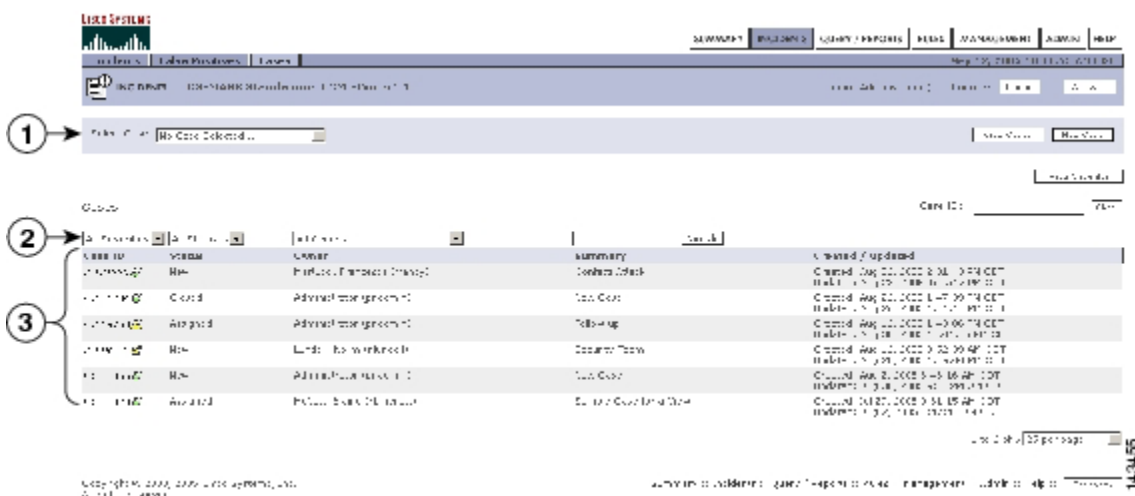
ケースは選択されたデータをケースに追加された時点の状態で保護し、表示します。あとで行われた MARS の状態の変更は関係しません。たとえば、MARS データを消去したり、自動検出または脆弱性スキャンングによってトポロジーが変更されたり、規則またはレポートの編集時に設定全体を変更したりしても、ケースで報告されたデータは取り込まれた時点と同じ状態のまま維持されます。



注 MARS ソフトウェア バージョン 4.1.1 では、ケース管理機能がインシデント エスカレーション機能の代わりに採用されました。

ケース管理のホームページは、Incidents タブの Cases サブタブです (図 17-1 を参照)。

図 17-1 Case Management タブ — Local Controller



1	ケース バー	2	ドロップダウン表示フィルタ
3	個別のケース		

新しいケース、割り当て済みケース、解決済みケース、終了済みケースにはすべて、Cases サブタブからアクセスできます。

ケースの内容を表示するには、ケースのケース ID 番号をクリックします。View Case ページが表示されます (図 17-2 を参照)。

電子メールで送信可能な、**View Case** ページの内容を示す HTML ドキュメントを生成するには、**View Case** ページの下部にある **View Case Document** をクリックします。レポートに基づいて描画された図やチャートも、Case Document に取り込まれます。

図 17-2 View Case ページ — Local Controller

1 → Case ID: 709227 (Case ID: 709227)

2 → View Case: 709227

Case ID	Status	Owner	Summary	Created / Updated
709227	Resolved	Local Administrator (johndoe@cs.com)	Malware Detected	Created: Aug 15, 2007 07:22:00 PDT Updated: Aug 15, 2007 07:22:00 PDT

Select/Unselect Case

3 → Last History

User	Action	Comment	Time
Local Administrator (johndoe@cs.com)	Case Closed		Aug 15, 2007 07:22:00 PDT
Local Administrator (johndoe@cs.com)	Case Opened		Aug 15, 2007 07:22:00 PDT
Local Administrator (johndoe@cs.com)	Summary Changed	Initial Summary/Action Note	Aug 15, 2007 07:22:00 PDT
Local Administrator (johndoe@cs.com)	Case ID Changed	Case ID Changed	Aug 15, 2007 07:22:00 PDT
Local Administrator (johndoe@cs.com)	Case ID Changed	Initial Case ID	Aug 15, 2007 07:22:00 PDT
Local Administrator (johndoe@cs.com)	Summary Changed	Case ID to ID	Aug 15, 2007 07:22:00 PDT
Local Administrator (johndoe@cs.com)	Case ID Changed	Case ID to ID	Aug 15, 2007 07:22:00 PDT
Local Administrator (johndoe@cs.com)	Summary Added	Summary Added	Aug 15, 2007 07:22:00 PDT
Local Administrator (johndoe@cs.com)	Case ID Changed	Case ID to ID	Aug 15, 2007 07:22:00 PDT
Local Administrator (johndoe@cs.com)	Case ID Changed	Case ID to ID	Aug 15, 2007 07:22:00 PDT
Local Administrator (johndoe@cs.com)	Case ID Changed	Case ID to ID	Aug 15, 2007 07:22:00 PDT
Local Administrator (johndoe@cs.com)	Case ID Changed	Case ID to ID	Aug 15, 2007 07:22:00 PDT
Local Administrator (johndoe@cs.com)	Case ID Changed	Case ID to ID	Aug 15, 2007 07:22:00 PDT
Local Administrator (johndoe@cs.com)	Case ID Changed	Case ID to ID	Aug 15, 2007 07:22:00 PDT
Local Administrator (johndoe@cs.com)	Case ID Changed	Case ID to ID	Aug 15, 2007 07:22:00 PDT
Local Administrator (johndoe@cs.com)	Case ID Changed	Case ID to ID	Aug 15, 2007 07:22:00 PDT

4 → Relevant

Display Name	Event	Source IP	Destination IP	Port	Protocol	Direction	Display Name	Policy Name	Action
192.168.1.100	HTTP GET	192.168.1.100	192.168.1.100	80	HTTP	Out	192.168.1.100	HTTP GET	Deny
192.168.1.100	HTTP GET	192.168.1.100	192.168.1.100	80	HTTP	Out	192.168.1.100	HTTP GET	Deny
192.168.1.100	HTTP GET	192.168.1.100	192.168.1.100	80	HTTP	Out	192.168.1.100	HTTP GET	Deny
192.168.1.100	HTTP GET	192.168.1.100	192.168.1.100	80	HTTP	Out	192.168.1.100	HTTP GET	Deny

1	ケース バー — 現在のケースを識別します。	2	ケース ID の表示 — ケースの属性を表示します。
3	ケース履歴 — ケースに対するすべての変更を記録します。	4	ケースに追加されたデータのサマリー

Global Controller のケース管理における考慮事項

Global Controller のケース管理は、Local Controller で実行する場合と、次の点で異なります。

- Global Controller ではケースは作成されません。ケースを表示したり、変更することはできません。
- Global Controller ではケース バーが表示されません。すべてのケースを選択するには、Incident -> Cases ページから実行します。
- Cases ページには、ローカル コントローラごとにケースを表示するための追加のドロップダウン フィルタも用意されています。

ケース バーの表示/非表示

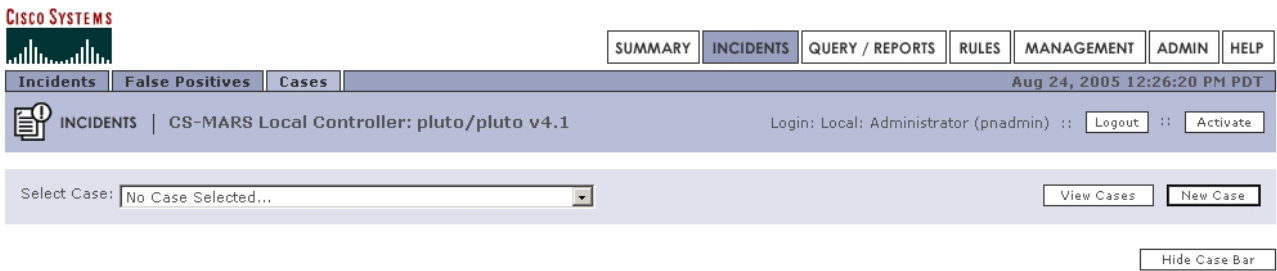
ケース バーはデフォルトで表示されます。表示位置は、各ページの一番上です。ケースを作成または変更する場合は、ケース バーを表示する必要があります。

ケース バーの非表示

ケース バーを非表示にする手順は、次のとおりです。

ステップ 1 Cases サブタブ (Incidents > Cases) にナビゲートします (図 17-3 を参照)。

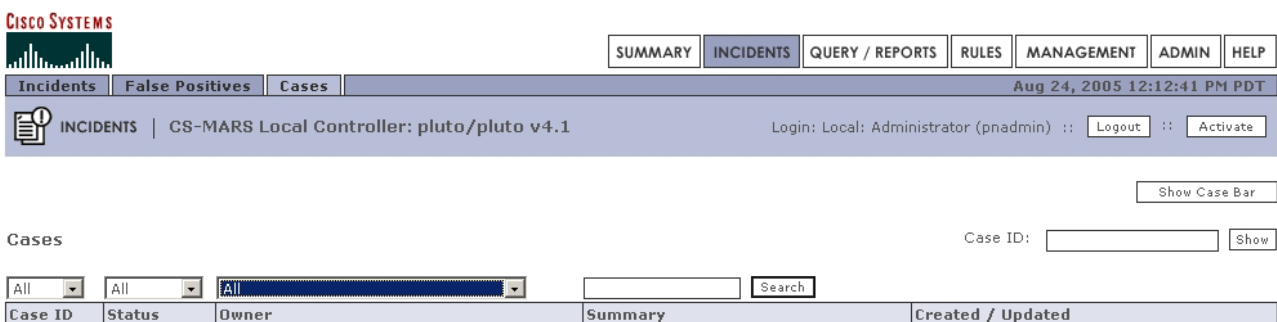
図 17-3 Incidents ページに表示されたケース バー



143451

ステップ 2 Hide Case Bar をクリックします。
すべてのタブにケース バーが表示されなくなります(図 17-4 を参照)。

図 17-4 ケース バーが非表示の場合のページの外觀



141309

ケース バーの表示

ケース バーを表示する手順は、次のとおりです。

ステップ 1 Cases サブタブ(Incidents > Cases)にナビゲートします(図 17-4 を参照)。

ステップ 2 Show Case Bar をクリックします。
ケース バー(図 17-3)がすべてのページに表示されます。

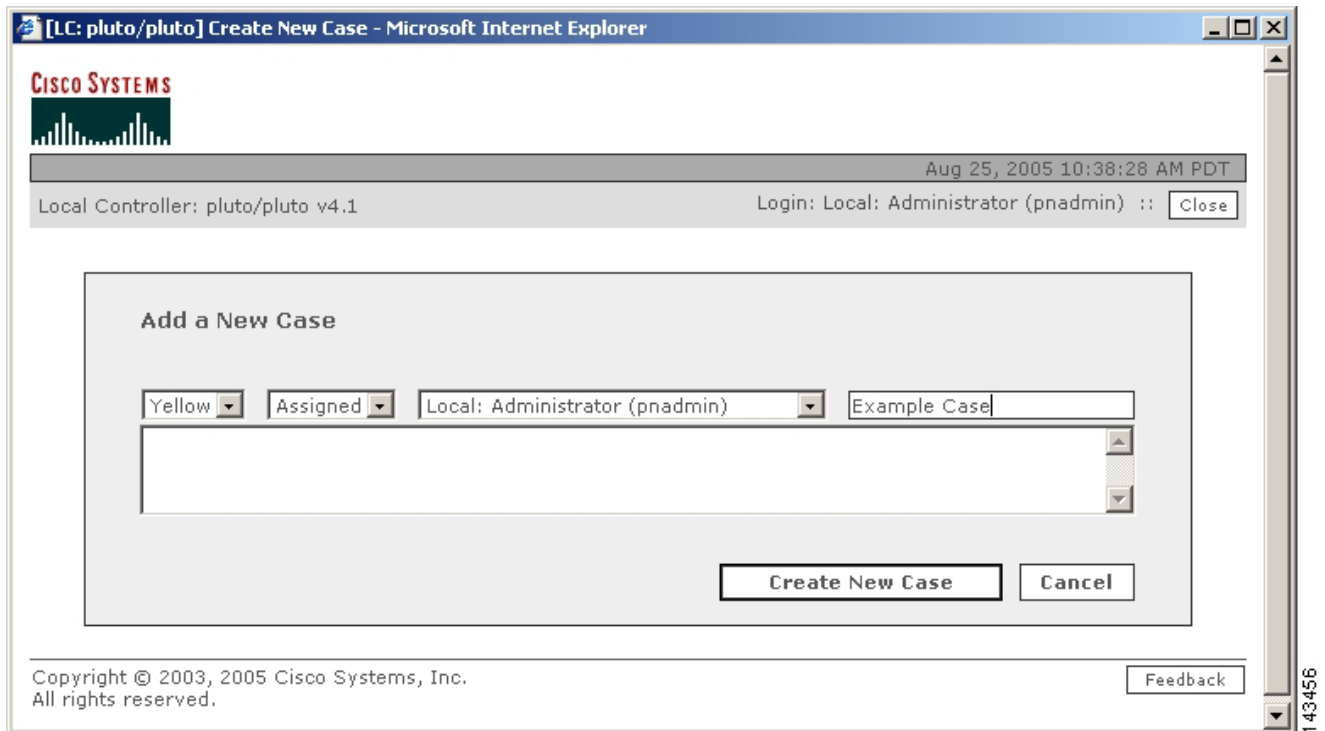
新しいケースの作成

新しいケースを作成する手順は、次のとおりです。

ステップ 1 「ケース バーの表示/非表示」の説明に従って、ケース バーを表示します。

ステップ 2 New Case をクリックします。
Add a New Case ダイアログボックスが表示されます(図 17-5 を参照)。

図 17-5 Add a New Case ダイアログボックス



ステップ 3 重大度を示すカラーを選択します。必要に応じてステータスを new から assigned に変更します。所有者を選択して、デフォルトのサマリー名 (New Case) を置き換えます。

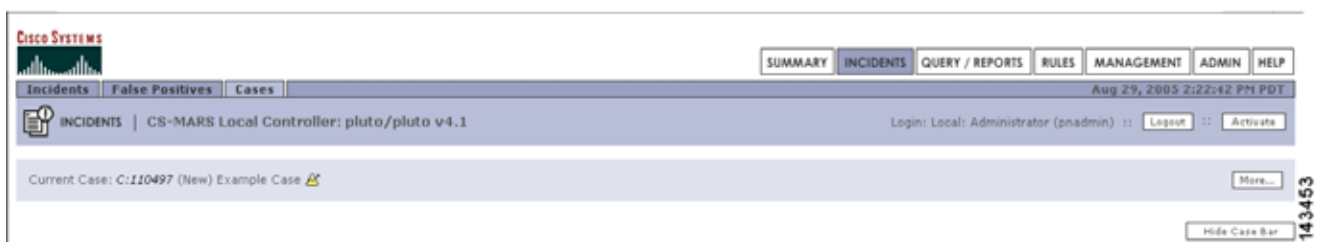
図 17-5 に、管理者に割り当てられた、プライオリティ カラーがイエローの (デフォルトはグリーン)、Example_Case というケース サマリーのケースを示します。

ステップ 4 テキスト スペースに注釈を入力するか、または貼り付けます。

ステップ 5 **Create New Case** をクリックします。

新規に作成されたケースに番号が設定され、ケース バーに現在のケースとして表示されます (図 17-6 を参照)。

図 17-6 現在のケースとしてケース バーに表示された新規作成ケース



「ケースへのデータの追加」に進んで、1 つのケースに複数のデータを統合する手順を参照してください。

現在のケースの編集および変更

現在ケースの編集

現在のケースを編集する手順は、次のとおりです。

ステップ 1 ケース バーを表示して、**More** をクリックします。

ケース バーが展開され、編集オプションが表示されます (図 17-7 を参照)。

ケース バーを表示する手順については、「ケース バーの表示/非表示」を参照してください。

図 17-7 ケース バーの展開



ステップ 2 ケースの重大度、ステータス、所有者、またはサマリーを必要に応じて変更します。

ステップ 3 必要に応じて、テキストボックスに注釈を追加します。

ステップ 4 **Submit** をクリックします。

現在のケースの選択解除

現在のケースを別のものと置き換える手順は、次のとおりです。

ステップ 1 上記の説明に従って、ケースバーを展開します。

ステップ 2 **Deselect** をクリックします。

ケースバーのドロップダウンリストに **No Case Selected..** と表示されます (図 17-4 を参照)。

ステップ 3 現在のケースとして別のものを選択するには、ケースバーのドロップダウンリストでケースを選択します。

ケースへのデータの追加

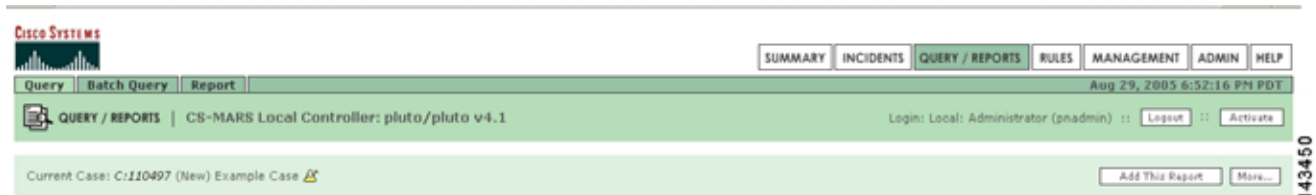
ケースにデータを追加する手順は、次のとおりです。

ステップ 1 現在のケースを選択します。現在のケースを選択する手順については、「現在のケースの編集および変更」を参照してください。

ステップ 2 ケースに取り込むページにナビゲートします。この例では、Query ページが選択されます。

ステップ 3 ケースバーで **Add this..** をクリックします。

図 17-8 ケースバーの Add ボタン



ステップ 4 選択したデータがケースに追加されたことを確認するには、ケースバー内のケース ID 番号をクリックして、View Case ページを表示します。

図 17-8 の例では、選択したレポートが View Case ページの Reports セクションに表示されます。図 17-2 に、View Case ページの一部を示しています。

ケース レポートの生成および電子メールでの送信

ケース データのケース レポートを生成して、ログイン先の MARS アカウントに電子メールで送信できます。電子メール イベントは View Case ページに表示されたケース履歴に記録されます。



注 ケース レポートを電子メールで送信できるのは、セッションにログインしているユーザのアドレスのみです。ケース所有者には送信できません。

ケース レポートを生成して電子メールで送信する手順は、次のとおりです。

ステップ 1 Cases ページまたはケース バーのドロップダウン リストでケースを選択します。

ステップ 2 ケース ID 番号をクリックして、**View Case** ページにナビゲートします。

ステップ 3 **View Case** ページの下部にある **View Case Document** をクリックします。
MARS によってケース レポートが生成され、表示されます。

ステップ 4 レポート ページの下部にある **Email Case** をクリックします。
電子メールが送信されてケース履歴が更新され、ケース履歴の最新項目として電子メール イベントが表示されます。
