[全国共同利用情報基盤センター研究開発論文集 No.28]より

インシデント情報管理システムの運用性の向上に関する報告

新妻　聡† 今野　将‡ 水木敬明‡ 曽根秀昭‡
†東北大学情報部情報基盤課ネットワーク係
‡東北大学情報シナジーセンターネットワーク研究部

1 はじめに

東北大学では，一昨年より，キャンパスネットワーク TAINS/G においてウェブブラウザを用いて部局のサブネット情報やインシデント情報について一元管理が可能な「TAINS/G におけるサブネット/インシデント情報管理システム」（以下，インシデント情報管理システムと略す）の構築を行い，その運用を開始した。インシデント情報管理システムにより TAINS/G 運用担当者がデータベースに蓄積された情報を閲覧・検索することが容易になった。しかし，部局でインシデントが発生した疑いの連絡が届くたびに TAINS/G 運用担当者が手作業で，１．部局管理者を検索，２．インシデントに関する対応依頼のメールを転送，３．転送したインシデント情報をデータベースへ登録，という作業が必要なため，同時期に複数の部局でインシデントが発生した疑いの連絡が届いた場合，TAINS/G 運用担当者にかかる負担が増大してしまうという問題点があった。

そこで，TAINS/G 運用担当者にかかる負担を軽減するために，手作業で行われている上記の作業の半自動化を可能にするシステムを開発することによって運用性の向上を図ることにした。具体的には，情報管理サーバへインシデント情報のメールを転送することにより「部局管理者の検索」と「対応依頼メールの作成」を自動で行い，TAINS/G 運用担当者がウェブブラウザを用いて情報管理サーバへアクセスし，簡単な内容確認を行うのみで部局管理者にインシデントに関する対応依頼のメールを送信できるというものである。

本稿では,インシデント情報管理システムに関する作業の半自動化について述べる。

2 システムの概要

2.1 インシデント情報管理システムの概要

東北大学では，各部局で TAINS/G ネットワークに接続する時や部局管理者が変更になった時などに，部局管理者が TAINS/G 管理部門にサブネット申請書とルータ申請書（以下，サブネット申請書とルータ申請書をサブネット情報と略す）を提出す

ることになっている。提出されたサブネット情報は，TAINS/G 管理部門のメーリングリストにより TAINS/G 運用担当者に配信される。TAINS/G 運用担当者は，提出されたサブネット情報をインシデント情報管理システムに追加登録または情報の変更を行う。

また，部局でインシデントが発生した疑いがあり，学内通報者や外部ネットワークから TAINS/G 管理部門に連絡が届いた場合，部局のインシデント情報としてインシデント情報管理システムのデータベースに登録し管理を行っている。

インシデント情報管理システムは，TAINS/G 運用担当者のみが操作できるようにしなくてはならない。そのため，情報管理サーバを TAINS/G 管理部門のプライベートネットワークに設置し，管理部門外からのアクセスの制限を行った。また，「.htaccess」ファイルによる端末のアクセス制限を併用することにより，よりいっそうの安全性の確保に努めている。

2.2　新規に追加した機能の詳細

TAINS/G 運用担当者が情報管理サーバへインシデント情報のメールを転送し，データベースの仮領域への登録に成功すると，TAINS/G 運用担当者はウェブブラウザを用いて転送したメールの一覧を表示することができる。図 1 に転送メール一覧画面を示す。

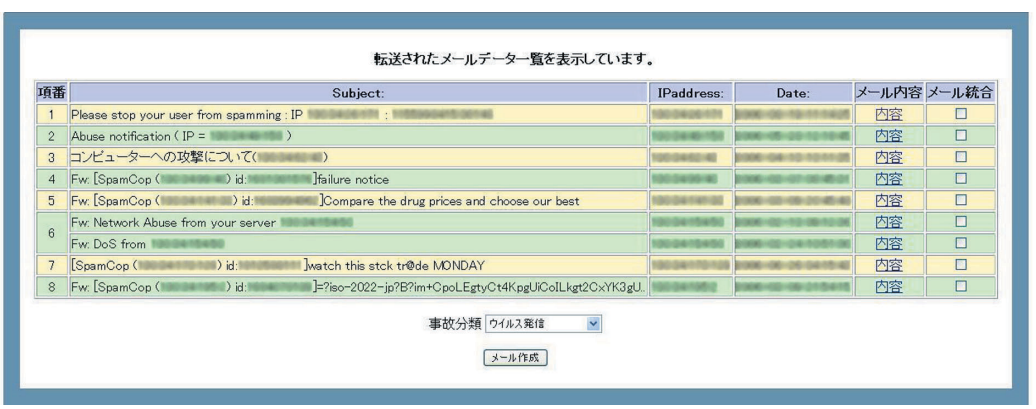

図 1　転送メール一覧画面

転送メール一覧画面では，同じ IP アドレスで発生したインシデント情報に関するメールを同じ色でまとめ，わかりやすいように IP アドレスが変わるたびに色を交互に変更している。「内容」のアンカーをクリックすると，そのインシデント情報の発信元のサブネット情報を管理する部局管理者の連絡先やインシデント情報

に関するメールの内容を表示することができる。図 2 に転送メール詳細画面を示す。また，転送メール一覧画面では，同じ IP アドレスで発生したインシデント情報のメールについて，メール統合のチェックボックスにチェックを入れて「メール作成」ボタンをクリックすると，それらのメールを統合してウェブブラウザ上でメールを作成することができる。図 1 の転送メール一覧画面で表示されている事故分類で「spam 発信」を選択して，メール統合のチェックボックスにチェックを入れ，「メール作成」ボタンをクリックした時に表示できる事故情報メール統合登録画面を図 3 に示す。

事故情報メール統合登録画面ではインシデント情報の対応依頼文を編集できる。事故情報メール統合登録画面で事故発生年月日を入力し，「登録」ボタンをクリックすると，インシデント情報の対応依頼文とメールの内容を統合して，実際に送るメールの内容を確認できる事故情報メール統合登録確認画面が表示される。事故情報メール統合登録確認画面で「メール送信/登録」ボタンをクリックすると，事故情報メール統合登録完了画面が表示され，作成したメールを部局管理者と TAINS/G 管理部門に送信できる。また同時に送信したメールの内容が該当する部局の事故情報としてインシデント情報管理システムのデータベースに追加登録することができ，事故統計情報にも内容が反映されるようになっている。

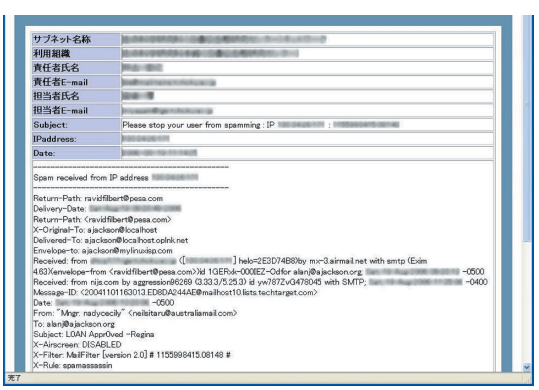

図 2　転送メール詳細画面

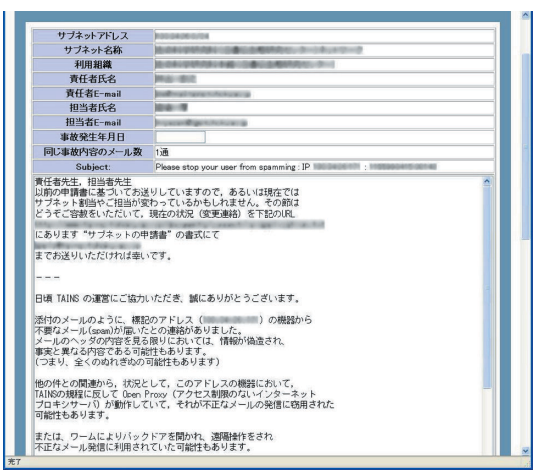

図 3　事故情報メール統合登録画面

2.3　システムの機能追加前の TAINS/G 運用担当者の作業の流れ

システムの機能追加前に部局でインシデント発生した疑いの連絡が届いた時の TAINS/G 運用担当者の作業の流れを図 4 に示す。

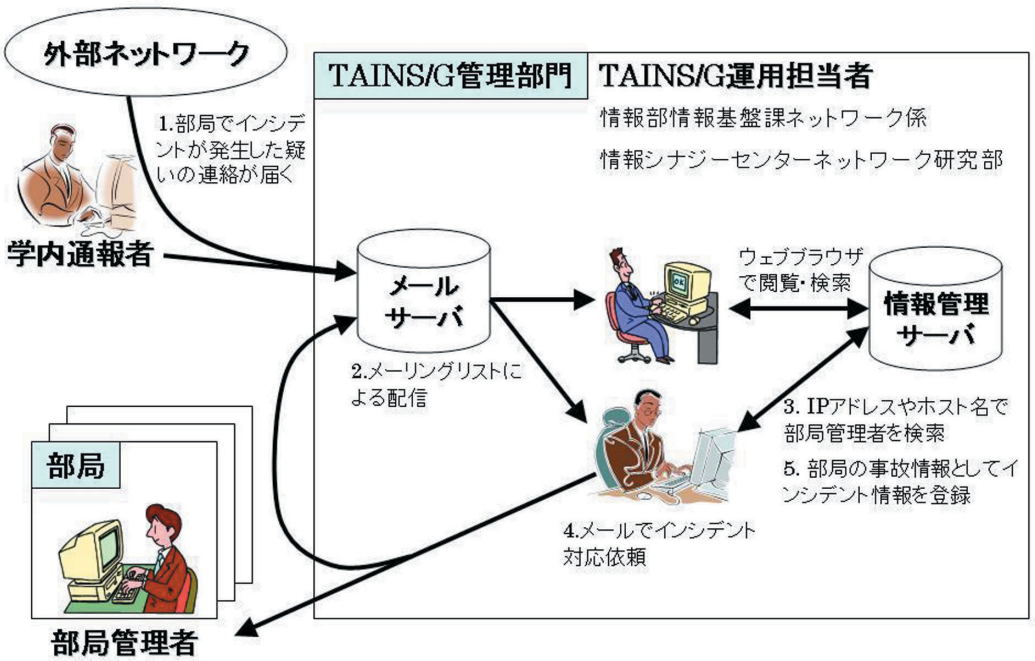

図 4　システムの機能追加前の TAINS/G 運用担当者の作業の流れ

1. 学内通報者や外部ネットワークから部局でインシデントが発生した疑いの連絡が TAINS/G 管理部門に届く。
2. TAINS/G 管理部門のメールサーバのメーリングリストで TAINS/G 運用担当者に配信する。
3. 届いたインシデント情報に記述されている IP アドレスやホスト名から部局のサブネット情報を検索し，検索結果に表示されるサブネット情報から部局管理者の連絡先を抽出する。
4. 抽出した部局管理者宛にメールでインシデントの対応依頼を行う。また同時に TAINS/G 管理部門にもメールを転送する。
5. 部局の事故情報として部局管理者宛に転送したインシデント情報をデータベースに登録する。

2.4　システムの機能追加後の TAINS/G 運用担当者の作業の流れ

システムの機能追加後に部局でインシデント発生の疑いの連絡が届いた時の TAINS/G 運用担当者の作業の流れを図 5 に示す。

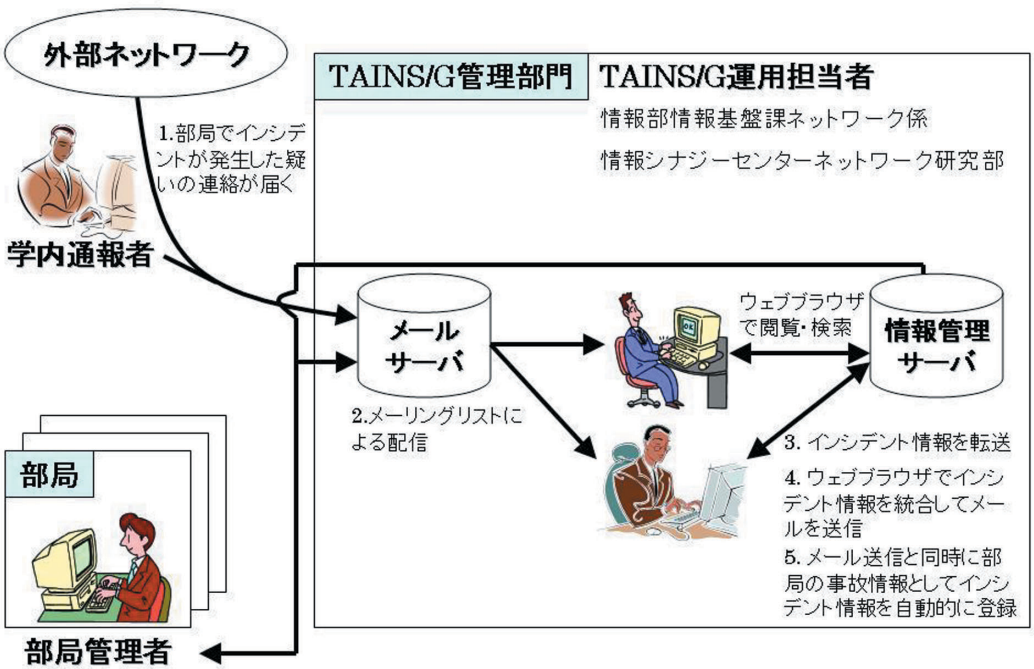

図 5　システムの機能追加後の TAINS/G 運用担当者の作業の流れ

1. 学内通報者や外部ネットワークから部局でインシデントが発生した疑いの連絡が TAINS/G 管理部門に届く。
2. TAINS/G 管理部門のメールサーバのメーリングリストで TAINS/G 運用担当者に配信する。
3. 届いたインシデント情報を情報管理サーバへ転送する。情報管理サーバへ転送されると同時に自動的にプログラムによりデータベースの仮領域に情報を登録する。プログラムの動作後，転送したインシデント情報の登録結果を TAINS/G 運用担当者にメールで返信する。
4. ウェブブラウザで情報管理サーバへアクセスして，データベースの仮領域に転送されたインシデント情報の一覧と詳細情報を参照し，必要であれば幾つかのインシデント情報を統合して部局管理者と TAINS/G 管理部門にメールを送信する。
5. メール送信と同時に部局の事故情報としてインシデント情報を自動的にデータベースに追加登録する。

3　まとめ

インシデント情報管理システムへ新しい機能を追加したことにより，追加前に手作業で行われていた作業である「部局管理者を検索」と「インシデントに関する対応依頼のメールを転送」と「転送したインシデント情報をデータベースへ登録」を半自動化することに成功し，同時期に複数の部局でインシデントが発生しても TAINS/G 運用担当者にかかる負担を軽減することができた。

現在のインシデント情報管理の問題点として，部局管理者に対応依頼メールが届かないという問題点がある。これは，部局で部局管理者が変更されているにも関わらず部局から新しいサブネット情報が提出されないためであり，部局によっては旧部局管理者が新部局管理者に転送する場合もあるが，不達で終わることも多く，実際のインシデントの対応が遅くなる場合がある。そのため，定期的に部局管理者に対して，部局担当者の交代も含めた部局のサブネット情報が正しいかどうか確認するメールを送信し情報を更新する機能を追加したい。

また実現には困難（認証問題や他のセキュリティ問題）が予想されるが，トラブルチケット制を導入し，部局管理者が過去のインシデントの履歴や現在の進捗状況などを段階ごとに確認することが可能なシステムの実現を検討していきたい。

参考文献

[1]新妻聡，森倫子，水木敬明： TAINS/G におけるサブネットおよびインシデント情報管理システムの構築，全国共同利用情報基盤センター研究開発論文集 No.27, 2005.10