3E-3

Web メール・ソーシャルメディアフィルタリングシステムの実装

浦川　順平†　　鈴木　健二†
電気通信大学大学院†

1. はじめに

近年，Web メールおよび BBS，Blog，SNS 等のソーシャルメディアのように Web を利用した情報発信型アプリケーションが広く普及している．企業においても利便性，有用性の観点から多くの従業員に利用されている反面，情報漏洩原因の一つとして懸念されている．特に Web メールは利用頻度が高く情報漏洩の危険性があり．また，ソーシャルメディアは一度情報漏洩すると多数のユーザに閲覧される可能性があるため，十分な対処が必要である．

筆者等は先に Web メールおよびソーシャルメディアによる情報発信を規制するフィルタリング手法を提案し，プロトタイプ実験で有効性を示した[1][2]．本稿では，企業等の多数ユーザが存在する環境で利用される汎用的な Web メール・ソーシャルメディア（以下 WS）フィルタリングシステムの実装手法を報告する．

2. WS フィルタリング手法の概要

Web メール・ソーシャルメディアはその有用性から，アクセスを全面的に規制するのではなく，発信情報の中で情報漏洩の原因となりうるものだけを規制することが理想的である．しかし，在来の技術ではコンテンツを正確に識別することは困難であるため，我々は情報漏洩防止における一つのアプローチとして，Web メール・ソーシャルメディアの閲覧は許可し，情報発信は全面的に規制する WS フィルタリング手法を開発した．本手法の概要を図 1 に示す（図 1）．

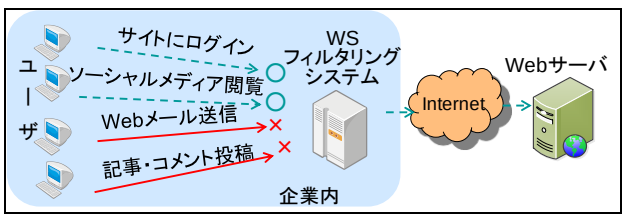


図 1 WS フィルタリング手法の概要

Implementation of the Web-based Email and Social Media Filtering System
†Jumpei Urakawa and Kenji Suzuki
The University of Electro-Communications

3. WS フィルタリングシステムの要件

企業等での広い活用を想定し，WS フィルタリングシステムでは以下の要件が必要である．

(1) Web メール・ソーシャルメディアの特徴およびブラックリスト/ホワイトリストによるデータ判定を行い，ユーザが外部に情報発信するタイミングで規制を実施する．
(2) 規制の事実を管理者ならびに規制対象ユーザ自身へ通知する．
(3) HTTP および HTTPS 通信の両方に対応する．
(4) 規制の有無にかかわらず，クライアント・サーバ間の送受信データをすべて記録する．
(5) 管理者がブラックリスト/ホワイトリスト，規制対象キーワードを登録できる．
(6) 管理者がユーザ利用状況を閲覧できる
(7) ユーザと管理者との対話をサポートする．

これらの要件を満たし，ユーザに利用可能とする形態としては，専用ハードウェアもしくはソフトウェアの 2 種類が想定される．前者は通信回線に挿入する形態でそのまま使用でき，後者は，システムおよび関連ライブラリのインストーラが必要となる．

4. WS フィルタリングシステムの実装

NIC を 1 枚使用した場合の基本構成図を図 2 に示す．ここでは，システムと回線との整合をとる通信制御，情報漏洩を判断するフィルタリング，さらにはフィルタリング結果に基づき管理者やクライアントに規制発生を通知する管理という 3 種類のモジュールと，各種データを保管するストレージ群，メールサーバからなる．

(1) 通信制御モジュール

本システムは企業内ネットワークに設置する．NIC を 1 枚使用する場合，本システムを LAN 内の 1 ホストと同等に配置する．Web（80 番ポート）アクセスするすべてのノードは，必ず本システムを経由して通信させ，その他のポートアクセスは直接 GW と通信させる．一方，NIC を 2 枚使用する場合は GW とタンデム（透過型）に挿入し，すべての通信が本システムを経由する．このため，80 番ポートが関与する通信を選別し，本システムに取り込む必要がある．

Copyright ©2011 Information Processing Society of Japan.
All Rights Reserved.

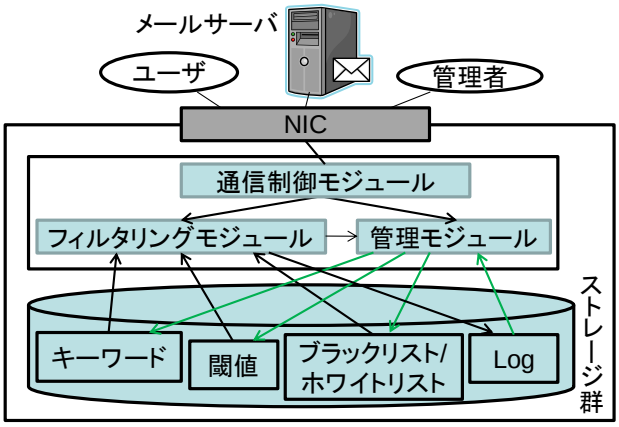


図 2　システムの構成図

(2) フィルタリングモジュール

①　HTTPS 解析機能

サーバにはクライアント，クライアントにはサーバとして SSL ハンドシェイクし，データの暗号化/復号化に必要な共通鍵を取得し解析する．

②　WS フィルタリング機能

サーバおよびクライアントから送信されるデータの特定箇所に存在するキーワード数を数え，あらかじめ指定した閾値と比較して，情報漏洩につながる情報発信か否かを判定する．

③　Log 記録機能

リクエスト+レスポンスを 1 データとしてフィルタリング適用後，図 3 に示す SQL 文により Log テーブルに格納する．

```
INSERT INTO Log VALUES (Log_No , Time , Client , Server , Request , Response , Detection_Type , Keywords)
```

図 3 Log 記録用 SQL

④　管理モジュールへの規制情報通知機能

Log 情報をストレージに格納したことを確認後，規制したデータの Log_No を管理モジュールに通知する．

(3) 管理モジュール

①　管理者と規制対象ユーザへの規制通知機能

管理者へはメール送信，規制対象ユーザへは HTML 文書で規制発生通知を実現する．メールに添付するデータは，Log_No を基に Log テーブルから取得する．一方，HTML 文書には規制した事実，該当するデータ，管理者への連絡方法が通知される．

②　各種データの投入機能

HTML 文書でインタフェースを提供することによりブラウザから，ブラックリスト/ホワイトリスト登録，キーワード，閾値登録を可能とする．また，ブラックリスト/ホワイトリストの作成時には，互いに重複しないことを確認する．

③　Log 閲覧機能

Log テーブルから日時，クライアント IP 等のパラメータで検索，表示する．また，視認性向上のため 1 つの HTML 文書取得時に付随して自動的にクライアントから送信される画像，CSS，JavaScript に対するリクエストを非表示にするオプションも実装した．

(4) ストレージ群

Log テーブル，ブラックリスト/ホワイトリストならびにキーワード，閾値テーブルはストレージ内に格納され，そのテーブルフォーマットを表 1，2，3，4 に示す．この際，キーワードテーブルでは，件名，タイトル等，同種の言葉が複数個現れた場合に，一つのカテゴリとしてカウントすることにより，不必要に合計値をあげて誤判定することを防いだ．

表 1 Log テーブル

Log_No	Date_Time	Client	Server	Request	Response	Detection	Keywords
識別子	日時	クライアント IP	サーバの URL	リクエストデータ	レスポンスデータ	規制の有無 (0:検出なし, 1:検出あり)	検出したキーワード

表 2 ブラックリスト/ホワイトリストテーブル

List_No	Type	URL	Time	Group	Comment
識別子	0:ブラックリスト, 1:ホワイトリスト	接続先 URL	登録日	対象グループ	備考

表 3 キーワードテーブル

Keyword	Value	Category
キーワード	重み付け値	カテゴリ

表 4 閾値テーブル

Target	Threshold
規制対象 (0:Webメール, 1:ソーシャルメディア)	閾値

(5) メールサーバ

管理モジュールから管理者への規制報告，ユーザからの質問・苦情処理，ならびにユーザと管理者との連絡に使用する．

5. おわりに

現在，本システムの実装が終了した段階で，Web メールおよびソーシャルメディアを利用した情報発信を適切に規制後，クライアントへの警告や管理者への報告等，基本動作を確認している．引き続き実用化を進める予定である．

参考文献

[1] 浦川順平，鈴木健二：Web メールフィルタリングシステムの機能拡張および性能評価，情報処理学会全国大会第 72 回全国大会，No.2G-2，pp-3-583-3-584(2010)

[2]浦川順平，鈴木健二：ソーシャルメディアにおける情報漏洩防止手法の提案，情報処理学会研究報告，コンピュータセキュリティ研究会報告，Vol.2010-CSEC-51 No.9(2010)

Copyright ©2011 Information Processing Society of Japan.
All Rights Reserved.