Vol.2010-CSEC-51 No.9
2010/12/10

ソーシャルメディアにおける情報漏洩防止手法の提案

浦川順平[†]　　鈴木健二[†]

近年，企業内部からの情報漏洩が増加している．その漏洩媒体の一つとしてBBS，Blog，SNS等のソーシャルメディアを利用したものがある．ソーシャルメディアはWebメールやIM同様，従業員の利用頻度が高いが，不特定多数が閲覧可能な場での情報発信を前提にしているため，情報漏洩した際の被害が甚大である．企業ではソーシャルメディアによる情報漏洩を防ぐため，既存Webフィルタリングの活用を試みるが，未知サイトを規制できない，誤規制率が高い等の問題がある．本論文では，調査分析により確認したソーシャルメディア特有のデータ構造を判定基準にし，加えて情報漏洩防止に適切なタイミングで規制実施する手法を提案した．また，評価尺度として，ソーシャルメディアアクセスの規制率，誤規制率を測定評価することにより，情報漏洩防止の一ステップとなるサイトアクセス規制に有効であることを示した．

Proposal for Preventing Information Leakage on Social Media

Jumpei Urakawa[†]　and　Kenji Suzuki[†]

In recent years, information leakage from companies has been increasing. In the information leakage medium, there are social media such as BBS, Blog, SNS and so on. While social media, as well as web-based email and IM, are frequently being used by company employees, the damages for companies will continue to grow as the users disclose information to the social media, which the general public can browse once the information is leaked. Companies are attempting to prevent information leakage through social media by applying existing web-filtering systems; however, they include some problems. For example, they cannot regulate new and unknown websites or they regard non social media, as social media. In this paper, we propose a social media filtering system that possesses decision-making criteria that consider the data construct of social media and can enforce regulations at the right time for preventing information leaks. Moreover, we measure the regulation rate of social media and the false regulation rate of other web sites to show the overall effectiveness of the proposal method.

1. はじめに

近年，BBS，Blog，SNS等ソーシャルメディアが広く普及している．その利用は一般家庭だけにとどまらず，企業の従業員にも及ぶ．企業におけるソーシャルメディアの利用は様々な情報を簡便に収集できるという利点がある一方で，外部に漏らしてはいけない情報を漏洩させる危険性も含む．実際，2009年の情報セキュリティインシデントに関する調査報告書[1]によると，特にサービス，情報通信，製造，卸売・小売業等においてインターネットによる情報漏洩インシデントの比率が高い．一方，各企業におけるインターネット活用の実態調査では，メール利用に次いで，ソーシャルメディア利用の比率が高い．特定ユーザを宛先とする電子メールに比して，不特定多数への情報提供・提示を狙ったソーシャルメディアは，電子メール以上に情報漏洩の潜在的危険性が大きいとも考えられる．筆者等は先に，インターネットにおける情報漏洩原因の一つであるWebメールの利用規制のためにWebメールフィルタリングシステムを開発した[2][3]が，ソーシャルメディアによる情報漏洩に対処することも緊急の課題となっている．

これまでも，ソーシャルメディアの危険性については指摘されていたが，現在，専用の情報漏洩対策はなく，大多数の企業ではWebフィルタリングシステムの活用で対処している．Webフィルタリングシステムは，ポルノ，暴力，麻薬などに関連した特定Webサイトへのアクセスを規制し，また，クライアントからの不必要な情報発信を規制するシステムである．既存のWebフィルタリングシステムの多くはブラックリスト方式，キーワード方式等に依存しているが，ブラックリスト方式では，未知のサイトを規制できない問題点がある．その問題点を解決するために，”記事”，”タイトル”，”投稿”等のようなWebコンテンツの種類を特定しうるキーワードの出現頻度判定により規制する方式も採用される．サーバ・クライアント間で送受されるデータに特定キーワードが含まれているか否かを判断する場合，サーバから送信されるデータに対して適用する場合とクライアントから送信されるデータに対して適用する場合がある．サーバからのデータを解析する方法は，キーワードと共に設定する各キーワードの重み付け値および判断基準となる閾値の設定次第で，規制対象のものを許可する（False Negative），また，許可対象のものを規制する（False Positive）問題が生じる．逆にクライアントからのデータを解析する方法には，解析対象データ量が少量なため，高い規制率を実現できない，ならびに誤規制率が高くなるという問題点がある．このため，筆者等は，上記問題点を克服するソーシャルメディアによる情報漏洩防止手法を検討したので，報告する．

本論文ではまず2章でソーシャルメディアの特徴および既存Webフィルタリングシ

[†] 電気通信大学
The University of Electro-Communications

ステムの問題点を示し，3 章でソーシャルメディア情報漏洩防止の考え方および核となるフィルタリング方式を提案する．4 章ではソーシャルメディアへのアクセス規制率，誤規制率を示す．5 章では本方式の考察を加え，最後に 6 章で結論を述べる．

2. ソーシャルメディア

2.1 ソーシャルメディアと情報漏洩

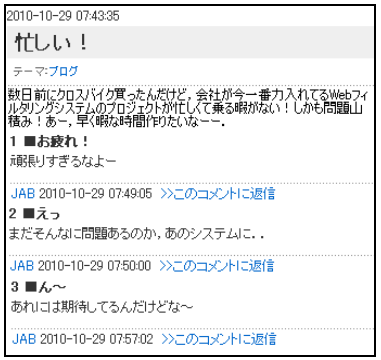


図 1 ソーシャルメディア(Blog)の例
Fig.1 Example of Social Media (Blog)

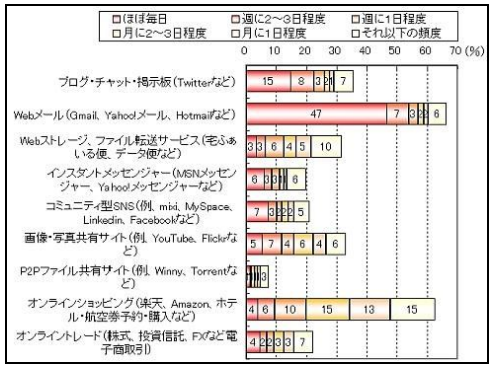


図 2 職場での従業員の Web 使用頻度
Fig.2 Web usage by employees in the industry

ソーシャルメディアの定義はネットワーク上にいくつか散在しているが，総じて，「ソーシャルメディアは，Web 技術を駆使し，人々が情報を発信・受信しながら，お互いに情報を共有し，活用させることができる手段と場を提供するメディア」と要約されると考える．複数のユーザから発信された情報によりコンテンツが成長していくメディアで（図 1）BBS，Blog，SNS 等が代表的な例である．また，一般ユーザから幅広い情報を取得できる利点から企業内でも広く利用されている．CLEAR SWIFT の調査[4]によると従業員の 31%は「ブログ・チャット・掲示板の利用はビジネス面で効果がある」，24%は「コミュニティ型 SNS 利用はビジネス面で効果がある」と答えている．実際，図 2 のように，調査した 515 人の従業員の内，36%がブログ・チャット・掲示板，また，21%がコミュニティ型 SNS を利用しており，かなりの普及率を示す．

このようにソーシャルメディアは企業にとって有用なツールである反面，気軽に情報発信できることから機密情報流出の危険性が高いメディアとも言える．また，図 2 に示すように，Web を利用した情報漏洩の原因となるツールに Web メールがあるが，Web メールが特定宛先に情報を発信するのに対し，ソーシャルメディアでは不特定多数に情報発信するため，情報漏洩した際の被害は甚大となる．

2.2 ソーシャルメディアの特長

国内外で広く普及している BBS，Blog，SNS において．新規記事を作成，ないしは既存記事へコメントする際のサーバから送信される HTML 文書ならびに，実際に記事およびコメントを投稿する際に,クライアントから送信されるデータの構造を比較検討した．図 3 に，BBS における新規記事およびコメント投稿時にサーバから送信される HTML 文書例を示す．HTML 文書内には POST メソッドが指定された form タグが存在しており，その form タグ内にソーシャルメディア特有のキーワードが含まれている．この構造は Blog，SNS でも同様である．しかし，調査した SNS に JavaScript を利用してクライアント側で HTML 文書を動的に生成しているため，転送データ中にこのような構造上の特徴を含まないものも 1 例存在した．調査した国内外 22 件のソーシャルメディアと form タグ内に存在するキーワードの対応を表 1 に示す．ここで得られたキーワードは，記事作成者についての情報（名前，メールアドレス），フォームについての説明（記事，投稿，質問等），記事内容を示す情報（タイトル，本文，カテゴリ，

表 1 ソーシャルメディア特有のキーワード
Table 1 Specific keywords of social media

種類	名前	キーワード(記事投稿)	キーワード(コメント投稿)	備考
BBS	Yahoo!掲示板	タイトル，メッセージ，投稿， 投稿前に確認(ボタン)*1	タイトル，メッセージ，投稿， 投稿前に確認(ボタン)	
	2ch	タイトル，名前，内容，新規スレッドの作成	名前，E-mail，書き込む(ボタン)	
	教えて!goo	質問，内容，投稿	質問，内容，投稿	
	gaia online	Subject, Tags, Message, Submit(ボタン)	Post a Reply, Message, Submit(ボタン)	
	4chan	Name, E-mail, Subject, Comment, Verification, File, Password, Submit(ボタン)	Name, E-mail, Subject, Comment, Verification, File, Password, Submit(ボタン)	
	d2jsp	Topic Title, Topic Description, Post Message, Post New Topic(ボタン)	Reply, Add Reply(ボタン)	
SNS	myspace	投稿日，投稿時間，タイトル，カテゴリー，本文， プレビューして投稿	コメント，ブログ，投稿	
	facebook	(該当なし)*2	(該当なし)	*3
	mixi	タイトル，本文，写真，日記公開範囲，投稿	コメントを書く，投稿	
	Yahoo!モバゲーTOWN	タイトル，本文，投稿，掲載する	コメント，投稿，コメントする(ボタン)	
	Gree	タイトル，投稿，フォト	コメントを書く	
	Otaba	タイトル，本文，タグ，日記，公開範囲，写真	コメントを書く，次ページ　書き込む	
	電気通信大学	タイトル，本文，写真，カテゴリ，日記，公開範囲	書き込む，本文，写真	
	@games	日記内容，タイトル，カテゴリー，本文， 公開範囲，タグの追加，写真，投稿する(ボタン)	コメントを書く，本文，コメントする(ボタン)	
Blog	Ameba	タイトル，テーマ，コメント，公開	タイトル，コメント，名前，URL，投稿する	
	ココログ	タイトル，カテゴリー，本文，記事，コメント	名前，メールアドレス，URL，内容	
	DTI Blog	記事のタイトル，記事のカテゴリ，スレッドテーマ， 記事を保存・投稿	TITLE，NAME，Eメール，URL，コメント， パスワード	
	FC2 BLOG	タイトル，カテゴリ，投稿，記事を保存	Name，Title，Mail，URL，Comment，Pass	
	blogger	タイトル，ラベル，投稿を公開(ボタン)	コメント，コメントの投稿(ボタン)	
	ウェブリブログ	タイトル，本文，URL，デザインテンプレート， テーマ設定，公開	ニックネーム，本文，コメント(ボタン)	*4
	LiVEJOURNAL	From, Subject, Message, Post Comment(ボタン)	From, Subject, Message, Post Comment(ボタン)	
	TypePad	Title, Body, Comments, Tag, Publish	comment, URLs, Post(ボタン)	

*1…ブラウザ上にボタンとして表示されている，*2…POSTが指定されたformが存在しない，*3…JavaScript，*4…HTTPS

写真等)，クライアントの動作を促す情報（投稿，公開等）に大別される．この際，クライアントの動作を促す情報はそれ以外の情報とは異なり，input タグの value フィールドおよび img タグの alt フィールドに出現する傾向が強い．また，コメント投稿時のキーワードは新規記事投稿時に比べ，その種類が少ないことが分かる．これは，コメントではタイトルやカテゴリ等を設定することが少なく，入力フォームについての説明も必要とされないからと考えられる．

```
<form action="bbs.cgi?id=jift" method="POST">名前<input type="text" name="name">
メール<input type="text" name="email">URL<input type="text" name="url">
件 名 <input type="text" name="subject"><textarea name="comment" cols="70"
rows="10"></textarea><input type="submit" value="投稿する"></form>
```

図 3　サーバから送信される HTML 文書(BBS の例)(抜粋)
Fig.3　HTML document sent by the server (example of BBS)

記事およびコメントをサーバへ送信する際に，クライアントから送信される POST データにも，ソーシャルメディア特有のキーワードが同様に含まれている（図 4）．これらのキーワードはクライアントが入力したものではなく，サーバ管理者が設定したキーワードを返送したものであるため，Content-Type 固有の文字列（図 4 の場合，&, =）と組になって出現している．多くの場合，クライアントから送信される POST データはサーバから送信される HTML 文書内のキーワードを英語化したもの（名前→name）のみを含んでいるが，一部ソーシャルメディアでは POST データ内のみに特定のキーワードが含まれている例（図 3，図 4 の場合 comment）も存在する．

```
name=Jum&email=Jum%40m.inf.com&url=http%3A%2F%2Fwww.inf.com&subject=
hello&comment=I%27m+busy+now& pass=14&id=jze&mode=write&time_stamp=126
```

図 4　クライアントから送信される POST データ(BBS の場合)(抜粋)
Fig.4　POST data sent by the client (example of BBS)

ソーシャルメディアの記事投稿時には HTTP, HTTPS 通信が利用される．本調査では，1 種類の Blog が HTTPS 通信を利用していたが，これは新規記事投稿時のなりすましや，ユーザ情報の盗難を防止するためだと考えられる．ソーシャルメディアに対するセキュリティへの関心が高まるにつれ，HTTPS 通信利用率も向上するものと考えられる．ソーシャルメディアにおけるコメント投稿は既存記事に対するものであるため，その入力フォームは，新規記事投稿時と同様に独立のページに存在しているものだけでなく，既存記事と同じページ内に設置されている場合がある．

2.3　企業におけるソーシャルメディア情報漏洩対策と Web フィルタリングシステム

企業におけるソーシャルメディアはビジネスに役立つ反面，従業員に無制限の利用を許可すると，情報漏洩につながる危険があり，管理者を悩ませている．このため，いくつかの企業は，i-FILTER[5]，InterSafe WebFilter[6]等の Web フィルタリングシステムを利用し，対策を施している．これらのシステムでは規制の手法として，ブラックリスト方式，あらかじめ指定したキーワードの出現頻度により規制判定を行うキーワード方式，さらには，Web アプリケーションでよく使用される POST メソッドの利用を判断基準にする POST メソッド規制方式を備えるが，各々一長一短ある．以下に，既存の Web フィルタリングシステムで採用されている各方式とこれらをソーシャルメディア利用規制のために適用した場合の問題点を示す．

・URL ブロック方式
Web サイトの URL をあらかじめブラックリストに登録しておき，ユーザがリクエストした URL がそのリストに含まれているか否かでサイト閲覧を規制/許可する方式である．ブラックリストを用いることは，危険きわまりないサイトへのアクセスが阻止できる反面，事前に調査されていない未知のサイトを規制できない欠点がある．現在，Web の普及によりソーシャルメディアは日々増加しているが，全てのソーシャルメディアを包含したブラックリストを生成し，最新状態に維持することは容易ではない．

・キーワード/フレーズ方式
クライアントおよびサーバから送信されるデータ内で特定キーワード/フレーズを検出し，データの受信・送信を規制する方式である．本方式の多くは，各キーワードに重み付け値を設定し，その値の合計が閾値に達した場合に規制する．しかし，一般に，クライアント側が発信する POST データの情報量は少なく，それだけで特徴を検出するのは難しい．それに比べ，サーバから送信されるデータはキーワードが多く出現する可能性があるが，重み付け値や閾値の設定により，False Positive，False Negative になり，最適値を導出することが困難である．

・POST メソッド規制方式
事前に指定したバイト数よりも大きなサイズの body を持つ POST リクエストの利用を規制する方式である．本方式は body サイズが比較的大きなファイルアップロード，ならびに，ファイルを添付した Web メール送信等の規制を目的としている．しかし，適切，不適切かを body サイズのみで判断するのは困難であり，POST メソッドを使った特定サイトへのログイン，ユーザ登録などまでをも規制してしまう恐れがある．

・PICS (Platform for Internet Content Selection) 方式
Web サイト作成者（セルフレイティング）もしくは第三者機関（サードパーティーレイティング）が Web サイトを評価し，ラベル付けを行い，クライアントはそのラベルを参考に規制/許可を判断する方式である．現状，本方式で利用されるラベルはアダルト・暴力・麻薬等の有害情報に関するものだけであり，それらの有害情報を持っていないソーシャルメディアを規制することはできない．また，ソーシャルメディアに関するラベルが増えたとしても，全てのサイトがラベリングされているものではなく，また，そのラベルの信頼性はクライアントの要望どおりであるかは不明である．

情報漏洩対策のため，上記各方式を採用した Web フィルタリングシステムを導入する企業側の問題点として，十分な規制率が得られていない現状とともに，見落とされがちではあるが誤規制率の高さがある．即ち，規制する必要があるものを規制できない（False Negative）ならびに，規制する必要がないのに規制してしまう（False Positive）問題である．実際，ネットスター株式会社の調査[7]によると業務に必要なサイトを誤規制された経験がある従業員は全体の 38%にものぼり，そのうち 35%は BBS，SNS，Blog が使用されていた．情報漏洩を防ぐという目的においては規制率が高いことが重要視されるが，従業員の業務効率を低下させないためにも，誤規制率をできるだけ低く抑えることもフィルタリングシステムにおいて重要な要件となる．
以上の点から，ソーシャルメディアのみを適切に規制するためには，ソーシャルメディアが持つ技術的特徴に基づいた新たなフィルタリング手法が必要であると考えられる．

3. ソーシャルメディア情報漏洩防止手法の提案

3.1 我々の狙いとアプローチ

企業にとってのソーシャルメディアは，閲覧によりユーザから様々な情報を取得できる利点とともに，情報発信することにより，企業宣伝，ユーザとのつながり拡大による更なる情報取得を期待する向きもある．例えば，質問投稿サイトの活用，Blog 公開等による広報活動などにより，多数ユーザの意見聴衆を行う等である．一方，企業や組織が，独自の目的や商行為のために，自らの持つ知的財産を外部に発信することなく保持したがるのも極めて当然である．従って，相容れないこれら二つの要求を満たしながら情報漏洩防止を考えるのが，我々のスタートポイントになる．
このため，我々が考えるソーシャルメディア情報漏洩防止手法は，ソーシャルメディアを利用した全情報発信を規制することでなく，企業にとって外部流失を防ぎたい情報発信のみを規制することである．これには，判断を下すシステムが，ユーザの入力した情報を正確に把握できる必要がある．しかし現状では，このような判断を自動的に行うことは困難である．そこで我々は情報漏洩防止手法実現に向けた一つのアプローチとして，まず，ユーザによるソーシャルメディア閲覧は許可し，情報発信は全面的に規制するソーシャルメディアフィルタリングを考える．この概要を図 5 に示し，我々が現在実現すべき考慮点を以下に列挙する．

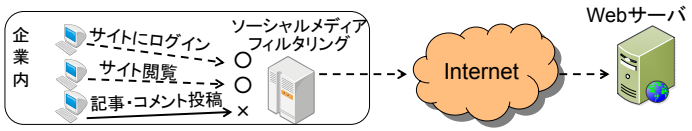


図 5 ソーシャルメディアフィルタリングの概要
Fig.5 Concept of social media filtering

(1) ユーザによるソーシャルメディアの閲覧や情報取得作業は許可し，情報漏洩の原因となるクライアントからの記事，コメント投稿のみを規制する．
(2) 既存システムのようなブラックリスト方式に依存したものではなく，クライアント・サーバ間で送受信されるデータを常にチェックし，特定のルールに基づいてフィルタリングすることにより未知のサイトに対応する．
(3) コメント投稿用ページにおけるキーワードの種類は記事投稿ページに比べ少ない傾向があるため，サーバにより設定される情報だけでなく，クライアントによる入力情報も加味して解析し，判定する．
(4) キーワードに応じた重み付け値，閾値の設定を可能とする．
(5) ソーシャルメディア利用の規制率・誤規制率において有効な手法を提案する．
(6) HTTP だけでなく，HTTPS 通信を利用したソーシャルメディアにも対応する．

筆者等は先に Web メールフィルタリングシステムを開発したが，Web メールはソーシャルメディアと同様に，POST メソッドを利用，HTML 文書内の POST が指定された form タグ内に特有のキーワードが出現，POST データ内に Content-Type 固有の文字列と組になって特有のキーワードが出現している等の共通点がある．そこで Web メールフィルタリングシステムを土台として，ソーシャルメディアフィルタリングシステムを構成するのが適切だと考えられる．

3.2 ソーシャルメディアフィルタリングシステムの提案

図 6 にソーシャルメディアフィルタリングシステムの機能構成を示す．本システムは，サーバとクライアントの間に介在し，送受信されるデータを解析し，サーバから送信される Web ページを判定 1 で，次いでクライアントから送信される POST データ

を判定 2 で解析する．規制はクライアントからの POST リクエスト受信時および判定 2 による解析後に実施する．以下に判定方式および規制実施についての詳細を示す．尚，図 6 では HTTPS 通信の場合の例を示したが，その通信解析は Web メールフィルタリングシステム[3]と同様の手順であるため省略する．

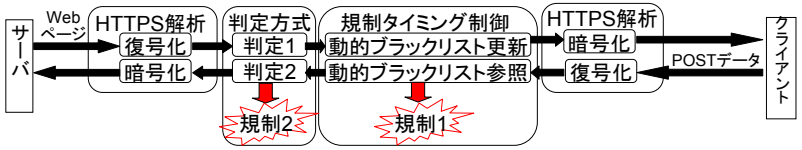


図 6　ソーシャルメディアフィルタリングシステムの機能構成
Fig.6　Functional modules in social media filtering system

(1)　判定 1 のメカニズム

サーバからクライアントに送信される記事，コメント作成ページの特徴から，HTML 文書内の POST メソッドが指定された form タグ内にソーシャルメディア特有のキーワードが含まれている場合，ソーシャルメディアであると判断する．本判定では既存の Web フィルタリングシステムで利用されているキーワード方式とは異なり， input タグの value フィールドおよび img タグの alt フィールドも解析対象とする．textarea, script 等のタグフィールド値およびそれらタグで囲まれた部分は誤規制抑制のため解析対象外とした．また，キーワードにはあらかじめ重み付け値を付与し，検出キーワードの合計値が閾値を超えた場合，ソーシャルメディアであると判定する．

(2)　判定 2 のメカニズム

記事，コメント投稿時にクライアントから送信される POST リクエスト内にソーシャルメディア特有のキーワードが含まれているかを解析する．ここで対象とするキーワードはクライアントが入力したものではなく，サーバからクライアントにあらかじめ送信されたキーワードである．これを判別するために，キーワードが Content-Type 固有の文字列と組で出現していた場合のみキーワードが出現したとみなす．判定 1 と同様に重み付け値と閾値の関係を利用する．

調査結果でも示したように，ソーシャルメディアのコメント投稿フォームでは，サーバから送信される HTML 文書およびクライアントから送信される POST データ内のキーワードが Web メールに比べ少ない事例がある．そのため，判定 2 では，name, title, message 等サーバにより設定されたキーワードでなく，“社外秘”，“氏名”，“住所”等ユーザが入力した情報が POST データにおける変数の値部分（図 7 下線部）に出現しているかを解析する．

name=Jum&email=Jum%40m.inf.com&url=http%3A%2F%2Fwww.inf.com&subject=for+internal+use+only&comment=name+Jumpei%0D%0Anumber+090-1234-5678%0D%0Aaddress+chofu-shi%2CTokyo

図 7　クライアントから送信される POST データ(抜粋)
Fig.7　POST data sent by the client

(3)　重み付け値および閾値の設定

ソーシャルメディアは BBS，Blog，SNS 等様々な入力形態を持つため，Web メールに比して，判定対象となるキーワードの種類も多く，多様な重み付け値を設定しなければならない．また，重み付けの方針は，ソーシャルメディアのみで現れる可能性の高いキーワード（ボタン形式の“投稿”，“書き込む”等）の値を大きくし，規制対象外である特定サイトへのログイン，ならびに，新規ユーザ登録でも利用されるキーワード（名前，アドレス等）の値は小さくすることも必要となる．閾値は重み付け値およびキーワードの数に依存するが，少なくとも 2 つ以上のキーワードが含まれない限り規制しない等の工夫が必要である．

理想的には，規制率が高く，誤規制率が低くなるように重み付け値および閾値を設定する必要があるが，最適な組み合わせを見つけるためには実際の Web サイトに対して適用実験を繰り返す必要性がある．

(4)　規制実施

本手法における規制実施のタイミングは図 6 に示すように以下の 2 つである．

規制 1：判定 1 の結果によって随時 URL が追加される動的ブラックリストを導入し，その後クライアントからの POST リクエスト受理時に，その POST リクエスト先 URL と動的ブラックリストの URL が一致した時

規制 2：判定 2 でソーシャルメディアと判断した時

一般にソーシャルメディアのコメント入力フォームは特定記事の直後に設置されていることが多いため，フォーム解析時に規制実施してしまうと，記事情報自体がクライアントに伝わらなくなる．本来，情報漏洩はクライアントがサーバへフォーム情報を発信することにより発生するため，規制実施のタイミングを遅らせ，クライアントからの情報発信を見て規制することが極めて重要となる．

4.　ソーシャルメディアフィルタリング評価実験

提案するソーシャルメディアフィルタリングシステムの評価実験を実施した．本実験では，既存のソーシャルメディア 41 件と，Google で「タイトル，メッセージ」と

検索して得られた 65 件のソーシャルメディア以外の Web サイトに対して，従来のキーワード方式と提案するキーワード方式の両方を適用し，ソーシャルメディア規制率と誤規制率を比較した．

従来方式は，POST メソッドが指定された form タグ内のみを解析対象とする我々の提案手法とは異なり，HTML 文書内の各種タグを除く全領域を解析対象とする．また本実験では，重み付け値に対する規制率，誤規制率の影響を測定するため，複数の重みづけ値の組を用意し，これらのキーワードと重み付けは表 2(a)，(b)に示す．ここでは，A が最も判定が易しく（False Negative の可能性が高い），E が最も厳しく（False Positive の可能性が高い）なっており，閾値はいずれの実験でも 5 と設定した．従来方式と提案方式による規制率，誤規制率をそれぞれ図 8(a)，(b)に示す．

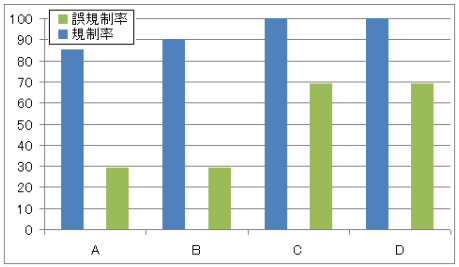
表 2　キーワードと重み付け
Table 2　Keywords and their weighted value

(a) 判定 1
(a) decision 1

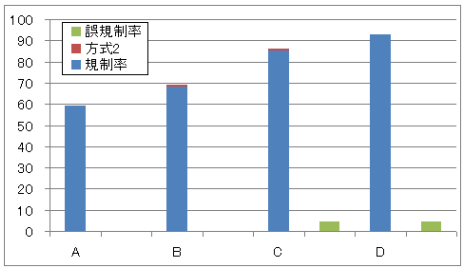
キーワード＼組	A	B	C	D
名前	1	1	1	1
メール，アドレス，URL	1	1	1	1
日記，ブログ，質問	1	1	1	1
投稿	1	1	1	2
タイトル，件名，題名	1	1	2	2
本文，メッセージ，コメント，内容	1	1	2	2
削除キー	1	2	2	3
（ボタン）投稿・書き込む	1	2	2	3

(b) 判定 2
(b) decision 2

キーワード＼組	A	B	C	D
Name	1	1	1	1
Mail，Address，URL	1	1	1	1
Submit，Post	1	1	1	1
Diary，Blog，Question	1	1	1	2
Title，Subject	1	1	2	2
Body，Message Comment，Content	1	1	2	2
delete	1	2	2	3



(a) 従来方式
(a) Conventional method



(b) 提案手法
(b) Proposed method

図 8　規制率・誤規制率
Fig.8　Correct and false regulation rate

(1) ソーシャルメディア規制率

図 8(b)に示すように，提案方式の規制率は表 2 に示すキーワードの組 D の場合に 93%であり，高い値となっている．これは，POST メソッドが指定されたフォーム内にソーシャルメディア特有のキーワードが含まれている可能性が極めて高いことを示している．従来方式の規制率が高いのは，入力フォーム以外の領域のみにキーワードが出現していたためである．本実験では，クライアントからの送信データを解析する判定 2 の効果が少ないが，これはクライアントから送信されるデータ中のキーワードが，サーバから送信されるものと同一の場合が多かったためである．しかし，入力フォームが JavaScript 等によりクライアント側で動的に生成されるものに対しては，判定 2 が有効であるため，今後評価実験対象を拡大するにつれ重要性が高まると考えられる．

(2) 誤規制率

図 8(a)，(b) を比較すると，提案方式は誤規制率を大幅に改善している．これは，判定 1 が解析対象を POST メソッドが指定された form タグ内に限定しているためである．Web サイトの中には GET メソッドを利用するページ遷移ボタン，検索フォーム等がページ内に設置されている例は多いが，POST メソッド使用のための form は設置されていることが少ない．POST が指定された form を持たないページはいくらキーワードが多く出現していたとしても，解析対象として扱わないため，誤規制を減らすことが可能となっている．

(3) 重み付け値の設定

図 8(a)を見ると，キーワードの重み付けの値を大きくするほど規制率は向上しているが，それに伴い誤規制率も向上している．つまり，情報漏洩を防げる可能性をあげたいと考える企業の場合はキーワードの組 D のように重み付け値に大きい値を設定するが，誤規制率が 69%と非常に大きいため，業務効率の大幅な低下は免れない．逆に，組 A を選択した場合は，誤規制による業務効率の低下は少ないが，情報漏洩の可能性が極めて高くなる．このように，従来方式は最適な重み付けの値の導出が困難である．それに対し，図 8(b)の提案方式を見ると，重み付け値を大きくするにつれ，誤規制率を低く抑えながら規制率を向上させている．従って多様なソーシャルメディアが出現する状況では，キーワードを増加させる必要があるが，重み付け値を変化させた試行実験を行うことで，高い規制率を実現できるキーワードの組を見つけ出すことができる．

5. 考察

(1) 企業内でソーシャルメディアを利用し情報を取得する必要はあるが，情報漏洩は防がなければならない．この要件を満たす方式は，クライアントから送信されるデータのみを解析するキーワード方式，POST メソッド規制方式があるが，現状において，十分な規制率を得られない，規制対象 POST データのサイズ設定が困難であるなどの理由からこれらのフィルタリングを利用せず，URL ブロッキングによりアクセス自体を禁止する方法を採用している．提案方式は，サーバおよびクライアント双方から送信されるデータを解析することで 93%という高い規制率を維持しつつ，解析対象を POST メソッドが指定された form タグ内に限定することで誤規制率も極めて低く抑えることができる，また，クライアントからの記事コメント投稿を待って，最適なタイミングで情報漏洩を防止するフィルタリングシステムである．

(2) 提案方式の判定手法に若干の修正を行うことにより，規制率の増大が期待される，図 9(a)，(b)に示すようなサーバとクライアント間のデータ通信例がある．提案方式の判定基準では，表 2 の重み付け値の組 D を用いた場合，サーバから送信されるデータの重み付け値の合計が 3，クライアントからが 3 となり，当該サイトをソーシャルメディアであると判断しない．しかし，これらキーワードの組み合わせはソーシャルメディア利用と判断するのに十分であるため，判定 2 を適用する際に，判定 1 の結果と加算して合計値で判断することで対応できる（図の場合には合計値 6 で規制可能とする）．また別の事例として，記事投稿のための入力フォーム内におけるキーワード出現頻度が低いために規制できなかったものがあったが，ソーシャルメディア，特にコメント投稿ページは，コメント入力目的でない異なるフォーム内に特定情報（既存記事の日付，タイトル，名前等）を含んでいることが多く，これら情報の多少を判定基準の一つとして利用することも有効であると考えられる．

<form method="POST" action="write.html"><textarea name="content" class="area"></textarea><img src="cl.gif" class="Irpy" id="com_id27" alt="投稿"></form

(a) サーバからのデータ

crumb=qWn&s=art_cmt&fid=759&pid=277&category_id=5511&update=1&emoticon=01.gif&nickname=jumpei&content=this+is+comment

(b) クライアントからのデータ

(a) Data by the server (b) Data by the client

図 9 サーバ・クライアント間の送受信データ(抜粋)

Fig.9 Transmitted and received data by the server and the client

(3) 本研究のゴールは，ソーシャルメディアの利用により，従業員が企業における重要情報を外部へ漏洩するのを規制することである．しかし，現状のフィルタリングシステムでは，記事内容などコンテンツに対するキーワードマッチング機能は備えるものの，キーワードマッチングの対象には，コンテンツを省いている．このため今後は，ユーザが入力した情報に対して，キーワードの出現頻度，共起等を利用し，フィルタリングシステムが正確にこれら情報を把握する機構を開発し，クライアントからの記事，コメント投稿の内容自体での規制も可能にしたいと考えている．

6. 結論

本論文では，企業におけるソーシャルメディア利用による情報漏洩を規制するために，まず，ソーシャルメディアの技術的特徴を調査した．その結果，サーバおよびクライアント双方から送信データの構造に Web メールとの類似点があることを確認した．この結果，企業従業員によるソーシャルメディアアクセス規制には筆者達が開発した Web メールフィルタリングシステムが活用できる展望を得た．このため，従業員が企業活動として情報発信しながら，企業の知的財産情報などの情報漏洩のみを防止する考え方を示し，情報漏洩防止に必要となるソーシャルメディアフィルタリングシステムを提案した．本システムでは，ソーシャルメディアの多様性に合わせてキーワードを多数設定する必要性，ならびにキーワードの組み合わせと閾値の設定を示した．また，評価実験を通じ，ソーシャルメディア規制率，誤規制率などで，提案方式の有効性を示した．今後は，クライアントによって入力されたコンテンツの中身を正確に把握し，情報漏洩防止手法の確立に役立てていく予定である．

参考文献

1) NPO 日本ネットワークセキュリティ協会 JNSA：2009 年情報セキュリティインシデントに関する調査報告書，http://www.jnsa.org/result/incident/data/2009incident_survey_v1.1.pdf(2010)
2) 浦川順平，鈴木健二： Web メールの手順解析に基づくフィルタリング手法の 拡充提案，DICOMO2009 シンポジウム，7C-2，pp.1465-1472(2009)
3) 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)
4) CLEAR SWIFT：従業員の Web と電子メール利用実態調査報告書 2010，http://www.clearswift.com/jp/promotions/web-usage-survey(2010)
5) DigitalArts：i-FILTER，http://www.daj.jp/bs/if7/
6) ALSI：InterSafe WebFilter，http://www.alsi.co.jp/security/is/index.html
7) ネットスター株式会社：第五回職場でのインターネット利用実態調書 http://www.netstar-inc.com/press/press080805.html(2010)