2004－DSM－34　(1)
2004／7／30

負荷分散を考慮した不正コンテンツフィルタの提案

月城 史行† 泉 裕†† 齋藤 彰一‡ 塚田 晃司‡
上原 哲太郎‡‡ 國枝 義敏§

†和歌山大学大学院システム工学研究科 ††和歌山大学システム情報学センター
‡和歌山大学システム工学部 ‡‡京都大学 §立命館大学

内容梗概インターネット上に氾濫する不正コンテンツによる様々な問題が増加し, 不正コンテンツ対策の必要が高まっている. 大学などの教育機関は不正コンテンツ配布の温床となっているとの批判もあり, 早急に不正コンテンツ対策をとる必要がある. 不正コンテンツ対策としては不正コンテンツフィルタの導入が進んでいるが, 近年問題となっている不正コンテンツの流出には対応しておらず, 偽装ファイルなどにも対応していない. そこで, 複数の不正コンテンツフィルタを組み合せ, 不正コンテンツの流出入や偽装ファイルに対応し, 負荷分散を実現した不正コンテンツ対策支援システムについて述べる.

キーワード：コンテンツ管理，コンテンツフィルタ

A Proposal of Distributed Contents Filtering System

Fumiyuki TSUKISHIRO † Yutaka IZUMI †† Shoichi SAITO ‡ Kouji TSUKADA ‡
Tetsutaro UEHARA ‡‡ Yoshitoshi KUNIEDA §

†:Wakayama University Graduate School of System Engineering
††:Center for Infomation Science Wakayama University
‡:Faculty of System Engineering Wakayama University
‡‡:Kyoto University §:Ritsumeikan University

Contents Management has been attached to pretty importance in Network Management. That Contents which are out WWW or Mail have worked so many peoples' communication and business succeeded through the Internet. However, many Network Managers are suffering from undesirable contents, such as illegal contents. It is very difficult to detect and filter out illegal contents, sometimes camouflaged, from bidirectional traffic between intranet and extranet.

In this paper, we address some problems in present filtering system, then propose a filtering system detect and filter out illegal contents, even though the file camouflaged with malicious modification and bidirectional traffic. This system runs by cooperation of host-based contents checker, gateway-based and network-based one. These components work in discovering contents doubtful as malicious, detecting one on certain condition and blocking it.

Keywords：Contents Management, Contents Filter

1　はじめに

企業や研究機関，および学校教育機関におけるネットワークの私的利用に関する問題が急増している．特に著作権違反や公序良俗に反する等の不正コンテンツは，私的利用を前提としたインターネット接続サービスでも問題視されている．不正コンテンツが流入出する経路には，大きく分類して二種類あると考える．一つはWorld Wide Web（以下WWW）サービスによって提供・取得できる場合であり，もう一つは特定のファイル共有ソフトによって不正コンテンツを交換する場合である．

特定のファイル共有ソフトによる不正コンテンツの交換には，古くはGnutellaやNapster，昨今ではKaZaAやWinMXおよびwinnyがある．多くはP2P型としてクライアント間のファイル共有が指摘されているが，クライアント同士を仲介する特定サーバの存在や特定ポートの利用を前提としていたため，個別に対応策が施されている．これら特定できる情報を必要としないwinnyについても，One Point Wall[1]などによって対応が可能であると考える．しかし，上記の各ソフトや今後出現する同種のソフトごとに対応することは現時点で不可能であるため，本研究の対象からは除外する．

WWWサービスの場合，コンテンツへのアクセスはWWWサーバ側に記録されるため，取得者をインターネットに接続させている管理側では一般に不正コンテンツ流入の検出が困難である．加えて，WWWサーバの運用管理側でも，公開しているコンテンツが不正であるかどうか，および不正コンテンツ流出の検証が困難である．したがって，不正コンテンツに係る検証と，検知してアクセスを停止させる機能およびこれらを支援するシステムを実現しなければならない．

WWWサービスにおけるコンテンツへのアクセス手法は一般的に限定されるため，原理的にアクセス監視が可能である．しかし，コンテンツが不正であるかどうかを直接的に判断，あるいは検知する機能がシステム化されていないため，人的労力による管理負荷によって運用のスケーラビリティが得られない．この機能を間接的に実現しているのが，URLフィルタ等に代表されるフィルタリング・システムである．

上記のプロダクトでは，ウィルスチェッカと同様に，不正コンテンツであることを間接的に示すURL（Uniform Resource Location）データベースが定期的に更新される．このURLによって，特定のWWWサイト全体あるいは個別ファイルの所在に基づきコンテンツの取得を制限する．しかし，インターネット上には膨大な数の不正コンテンツが存在しているために，個々の不正コンテンツをデータベースに登録するのではなく，サイト全体を登録するケースが多い．不正コンテンツを直接的に指定しないために，所在の分散・変更やコンテンツの偽装による二次配布，および頻繁にコンテンツがアップロードされるサイトへの対応が困難である．

本研究では，不正コンテンツの疑いがあるコンテンツの発見を支援し，URL以外に不正コンテンツを直接指定する手法で同コンテンツを検知・制御するシステムについて設計する．本システムは不正コンテンツの発見・検知および停止においてフィルタリング機能を有するが，各機能に適した個別のフィルタを構築し，これらを連携させる．各フィルタには，ネットワーク型不正コンテンツフィルタ，ゲートウェイ型不正コンテンツフィルタおよびホスト型不正コンテンツフィルタがある．

本紙では，不正コンテンツの発見・検知および停止について既存の問題点を考察し，上記システムに必要な機能およびシステム設計を提案する．

2　問題点

現状の不正コンテンツと不正コンテンツ対策の問題点をあげる．

2.1　不正コンテンツ

不正コンテンツとは，法律に反するコンテンツや公序良俗に反するコンテンツを指す．下記に具体的な例をあげる．

偽装形式	拡張子	ファイルヘッダ
璃樹無	.rez	REZ
あかね	.moe	Ver.
C&C	.cac	C&C
magician	.mgc	mgc\x00\x00\x00\x00

表 1: 偽装ファイルの拡張子とヘッダ

・著作権を侵害したコンテンツ
・ポルノ, 暴力, 差別などの他人に不快感を与えるコンテンツ
・犯罪を助長するコンテンツ

不正コンテンツ対策から逃れるために不正コンテンツを偽装・分割して配布することが多い. 偽装とはファイルヘッダや拡張子を変更する方法であり，分割とは巨大なコンテンツを分割し配布しやすくする方法である．偽装・分割ファイルは拡張子やファイルによって判別できる．代表的な偽装・分割ファイルの拡張子やファイルヘッダを表 1 で示す.

2.2 不正コンテンツフィルタ

一般的な不正コンテンツ対策ツールとして，不正コンテンツへのアクセスを制限する不正コンテンツフィルタがある．不正コンテンツフィルタのフィルタリング方式を以下に示す.

・データベース方式
・キーワード検索方式
・セルフレーティング方式

データベース方式とは，予めサイトを登録しておく方式である．本方式にはアクセスを拒否するサイトを登録しておくブラックリスト形式とアクセスを許可するサイトを登録しておくホワイトリスト形式がある．キーワード検索方式は，コンテンツに特定のキーワードが含んでいる場合，コンテンツ閲覧者にアクセス制限する方式である．セルフレーティング方式は，サイトの製作者が自分のページを格付けを行い，コンテンツ閲覧者側の不正コンテンツフィルタでこの格付けに応じてアクセス制限を行う方式である.

市販の不正コンテンツフィルタには，i-フィルター [2]，SmartFilter[3]，SurfControl[4]，WebSENSE[5]，InterScan WebManager[6] などがあげられる．さらに，フリーの不正コンテンツフィルタとして squidGuard[7] があげられる.

不正コンテンツフィルタは学校や企業などに加え，プロバイダへの導入も進んでいる．学校などの教育機関では教育上の配慮から不正コンテンツフィルタを導入している．企業ではウイルス感染や情報漏洩, 業務の効率の低下を防ぐために不正コンテンツフィルタを導入している.

市販の不正コンテンツフィルタの多くは，不正コンテンツを含んだサイトの IP アドレスやドメイン，URL などを登録したデータベースを使用してフィルタリングするデータベース方式を採用している．データベースには膨大な量の不正コンテンツが登録されており，URL ごとのアクセス制限が可能となっている.

しかし，既存の不正コンテンツフィルタには下記の問題点があげられる.

・双方向のトラフィックに対応していない
・画像, 動画, 音声ファイルなどのバイナリファイルに対応していない
・偽装した不正コンテンツに対応してない

市販の不正コンテンツフィルタは不正コンテンツの流入の監視を目的としており，不正コンテンツの流出は考慮していないために，不正コンテンツの流出を監視するのは不可能である．さらに，データベースに登録されている URL でアクセスを制限するため，データベースの精度によって性能が左右される．すなわち，不正コンテンツを配布しているサイトが頻繁に移転し，別のサイトで公開されると，データベース方式ではアクセスを制限するのが困難である.

3 システムの構築

ここでは，本研究で提案するシステムについて述べる.

3.1 本システムのモデル

不正コンテンツの発見を支援し，アクセス制限を自動化した「不正コンテンツ対策支援システム」を提案する．本システムは，ネットワーク型不正コンテンツフィルタ (以下, ネットワーク型), ゲートウェイ型不正コンテンツフィルタ (以下, ゲートウェイ型)，ホスト型不正コンテンツフィルタ (以下, ホスト型) を互いに連携させ，様々な組織間の差異を吸収できるだけでなく，負荷分散を実現できる設計している．導入時のネットワーク構成をできるだけ変更させない場合，ネットワーク型とホスト型の組み合わせが適している．確実に不正コンテンツへのアクセス制限を行う場合にはゲートウェイ型とホスト型の組み合わせ，あるいはネットワーク型も加えた組み合わせが適している．

3.2 各不正コンテンツフィルタの機能

本説では各不正コンテンツフィルタの機能について説明する．なお，不正コンテンツと疑わしいコンテンツを見つけ出すのを検出と定義し，アクセス制限のために，不正コンテンツを見つけ出すのを検知と定義する．

ホスト型

ホスト型は直接コンテンツを読み取ることによって，不正コンテンツと疑わしいコンテンツを検出する．調査の際に使用するのは，ファイルサイズやファイルヘッダ，ファイル名である．2 章で説明したように，偽装ファイルは特有のファイルヘッダや拡張子を持つために，コンテンツを読み取ることによって偽装ファイルであるか判断できる．ホスト型が検出した不正コンテンツと疑わしいコンテンツはファイル名やファイルサイズ，チェックサムを疑わしいコンテンツのデータベースに登録する

ホスト型を外部公開用サーバなどに導入し，公開されているコンテンツを調査することでネットワーク型やゲートウェイ型の負荷を分散できる．NFS でディスクをマウントすれば直接サーバにホスト型をインストールする必要がなくなる．

さらに，プロキシサーバに導入し，キャッシュされているコンテンツをチェックできるようにすると，内部向けのトラフィックに含まれるコンテンツも監視できるようになる．

ネットワーク型

ネットワーク型は，トラフィックを監視して不正コンテンツと疑わしいコンテンツを検出するために，ネットワークのトラフィックを監視できる場所に設置する必要がある．そして，URL やファイル名に特定のキーワードが含まれていたり，極端に大きいファイルサイズのコンテンツを検出する．検出した不正コンテンツと疑わしいコンテンツはファイル名や URL を疑わしいコンテンツのデータベースに登録する．

ネットワークを監視し，不正コンテンツデータベースに登録されている不正コンテンツの URL もしくはチェックサムと一致するコンテンツを検知すると，クライアント側とサーバ側に RST パケット送信し，コネクションを強制的に切断させる事によりアクセス制限を行う．

ゲートウェイ型

ゲートウェイ型は，ネットワーク型と同じようにネットワークのトラフィックを監視できる場所に設置し．トラフィックを中継する．中継する段階で，URL やファイル名に特定のキーワードが含まれていたり，極端に大きいファイルサイズのコンテンツを検出する．検出した不正コンテンツと疑わしいコンテンツはファイル名や URL を疑わしいコンテンツのデータベースに登録する．

トラフィックを中継する段階で，不正コンテンツデータベースに登録されている不正コンテンツの URL もしくはチェックサムと一致するコンテンツを検知すると，中継を中断し，アクセス制限を行う．

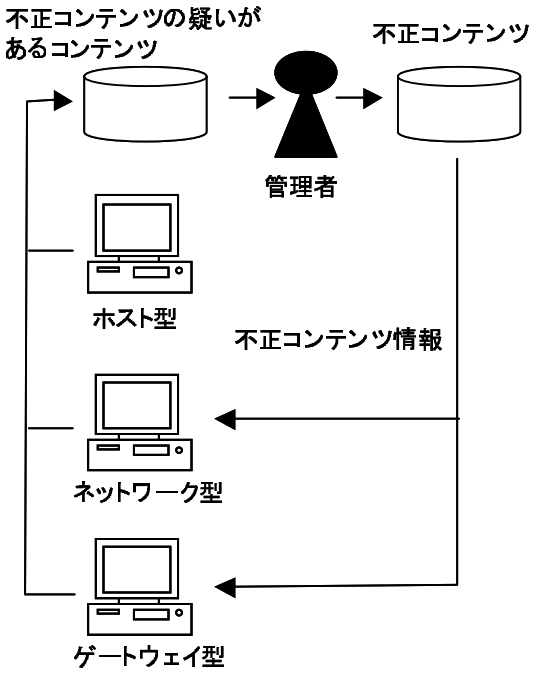

図 1: 発見からアクセス制限まで流れ

3.2.1 動作

一連の動作を図 1 に示す．管理者は不正コンテンツと疑わしいコンテンツのデータベースに登録されているコンテンツを調査し，不正コンテンツであるのならば不正コンテンツデータベースに登録する．不正コンテンツをデータベースに登録の際，URL やチェックサムが重複しないようにする．不正コンテンツデータベースには不正コンテンツの URL もしくはチェックサムを登録がされており，それを利用してネットワーク型もしくはゲートウェイ型が不正コンテンツを検知する．

本システムは，チェックサムを利用しているので，特定のコンテンツへのアクセスを確実に制限できる．特に，画像や動画，音楽などのコンテンツは一度配布されると加工されることなく何度も配布されることが多いので，チェックサムによるアクセス制限は有効であると考えられる．

	既存製品	本システム
不正コンテンツ流入	○	○
不正コンテンツ流出	×	○
画像・動画・音楽	×	○
偽装ファイル	×	○
発見支援	△	○
導入コスト	○	×

表 2: 既存製品と本システムの比較

4 考察

本システムと既存の不正コンテンツフィルタとの比較を表 2 に示す．

本研究で提案したシステムの問題点を以下に述べる．

・アクセス制限の有効性・パフォーマンス
・データベースのパフォーマンス
・不正コンテンツの誤検知
・導入・運用コスト

ネットワーク型は RST パケット送信によってアクセス制限を行っているため，ネットワークの負荷が高い状態では効果的にアクセス制限を行えない可能性がある．この場合ゲートウェイ型を導入すれば，確実にアクセス制限を行えるようになるが，ネットワークのスループットは低下する．ネットワーク型かゲートウェイ型のどちらかを選択するのは組織の運用ポリシに応じて決定すべきである．

本システムでは不正コンテンツの疑いがあるコンテンツと不正コンテンツをデータベースに格納している．データベースにアクセスが集中し性能が低下しないように，インデックス化して高速化したり，不正コンテンツフィルタ側でデータをキャッシュさせるなどの対策をとる必要がある．

さらに，古くなった不正コンテンツのデータを定期的に削除する必要もある．

不正コンテンツフィルタが誤検知によって，通常のコンテンツを不正コンテンツの疑いがあると判断することが考えられる．大量に誤検知が発生した場合には，管理者の処理が追い付かな

いため，重み付けなどにより優先度を設定するなどの対策が必要である．不正コンテンツデータベースに URL で登録されている不正コンテンツでは誤検知によるアクセス制限が発生する．誤検知を減らすためには健全なコンテンツを登録したホワイトリストの適用を検討すべきである．しかし，ホワイトリストの全般的な適用はスケーラビリティ著しく損なうために，ホワイトリストのサイズや適用範囲，ブラックリストとの参照順序等，実運用で検証すべき事項は多いと考える．

本システムは，複数の不正コンテンツフィルタが連携して動作し，組織に応じて構成を選択するために，市販の不正コンテンツフィルタよりも柔軟性がある．管理者が不正コンテンツを判断する必要があるため，人的運用コストは高い．運用コストを下げるためには，疑わしいと検出する絞り込みの多様化や，フリーで公開されている不正コンテンツのリストを使うなどの必要があると考えられる．

5 おわりに

不正コンテンツを取り巻く状況は目まぐるしく変わっているが，今後も WWW サービスは不正コンテンツ流出入の経路であると予測できる．よって，HTTP を対象にしたフィルタリングソフトの需要もなくならないと考えられる．本システムは不正コンテンツの流出や偽装ファイルに対応し，負荷分散を実現するために複数の不正コンテンツフィルタが連携して動作する不正コンテンツ対策支援システムである．今後は本システムの実装，評価を行う所存である．

参考文献

[1] One Point Wall
http://www.netagent.co.jp/onepoint

[2] i-フィルター
http://www.daj.co.jp/

[3] SmartFilter
http://www.securecomputing.com/index.cfm?skey=85

[4] SurfControl
http://www.surfcontrol.com/

[5] WebSENSE
http://www.websense.com/

[6] InterScan WebManager
http://www.trendmicro.com/jp/products/gateway/iswm/evaluate/overview.htm

[7] squidGuard
http://www.squidguard.org/