

Web サーバリモート監視におけるホームページ改竄判定

竹森 敬祐 三宅 優 中尾 康二

KDDI 研究所 〒356-8502 埼玉県上福岡市大原 2-1-15

E-mail: {takemori, miyake, nakao}@kddilabs.jp

あらまし コンテンツの変更を検知してアラームを通知する Web サーバリモート監視システムにおいて、正規の更新によって通知されるアラームの中に、注意すべき改竄アラームが埋もれてしまいかねないという問題が明らかになった。そこで本稿では、監視中のコンテンツに変更を検知した場合、そのコンテンツの特徴や変更前後の変化の様子を解析することで、改竄を的確に検出する改竄判定手法を提案する。提案手法は、改竄にみられる特徴のうち1つでも該当する項目があれば改竄とみなす手法であり、その判定結果は、正規の更新と改竄を区別して出力する。実際の改竄のデータを用いて提案手法の改竄判定率を評価した結果、小さな誤判定率で全ての改竄を検出できることを確認した。これにより、サイト管理者は改竄アラームに集中できるようになり、検出された改竄の特徴を知られることで、コンテンツの改竄状況の把握と改竄時の対策を迅速に実施できるようになる。

キーワード リモート監視, ホームページ, 改竄, 検知

Detection Algorithms of Unauthorized Manipulation for Web Remote Patrol Systems

Keisuke TAKEMORI Yutaka MIYAKE and Koji NAKAO

KDDI R&D Laboratories 2-1-15 Ohara, Kamifukuoka-shi, Saitama, 356-8502 Japan

E-mail: {takemori, miyake, nakao}@kddilabs.jp

Abstract We have developed a remote patrol system for web servers which detects the change of contents. However, it could not distinguish between regular update and unauthorized manipulation. The administrator of web servers may receive many alarms from this system if the contents are updated, frequently. In this paper, we propose detection algorithm of unauthorized manipulation by concentrating on the characteristics on HTML contents as well as the correlation between before and after changes. We could abstract six characteristics, which are so-called signatures to detect manipulations based on the several sample data. We also evaluate our algorithm using many sample data, and as the results our algorithm is quite feasible to detect any types of contents with little miss-detection of faults positive. In conclusion, administrators of the web servers detect and manage the unauthorized detection efficiently among their routine works.

Keyword Remote Patrol, Homepage, Unauthorized Manipulation, Detection

1. はじめに

近年、ホームページの改竄事件が大きな社会問題となっている。Web サイトを構成する機器には、日々セキュリティホールが報告されており、その全てに対して迅速かつ適切なセキュリティ対策[1]を図ることは難しく、悪意の侵入者やインターネットワーム[2][3]からの攻撃を完全に防ぐことは困難である。サイトによっては、改竄された場合の被害を最小限に抑えることを目的として、ホストベースの変更検知システム[4][5]を適用しているところもあるが、その運用・管理の煩雑さから、一般への導入は思うように進んでいない。

そこで我々は、ホストに監視用モジュールをインス

トールする必要なく、かつ容易な操作で監視を行えるシステムとして、リモートからホームページを定期的にダウンロードして変更を検知する Web サーバリモート監視システムを開発し、評価を行ってきた[6][7]。その結果、導入時の煩雑さは軽減されたが、改竄の検出方法として監視コンテンツの日付やサイズ、コンテンツ部のハッシュ値を用いているため、コンテンツの内容が更新された場合、それが正規の更新であるのか侵入者による改竄なのかを区別できなかった。これにより、改竄ではない正規の更新の際にもアラームが通知されてしまい、改竄を知らせるアラームが埋もれてしまいかねないという問題が明らかになった。

そこで本稿では、Web サーバリモート監視システム

においてコンテンツの変更を検知した場合、そのコンテンツの特徴と、変更前の変化の様子を解析することによって、正規の更新と改竄を的確に判定する手法を提案する。提案手法は、改竄にみられ特徴のうち1つでも該当する項目があれば改竄とみなす手法であり、その判定結果は、正規の更新と改竄を区別して出力する。改竄の実例を基に提案手法を評価した結果、正判定率ならびに誤判定率の両面で、十分なレベルを達成していることを示す。

以下2章において Web サーバリモート監視システムについて述べ、3章で典型的な改竄事例を取りあげてその特徴について整理を行い、各種改竄を検出するために注目する特徴について提案する。4章で今回収集した70件程の改竄事例を基に提案手法の評価を行い、最後に5章でまとめる。

2. Web サーバリモート監視システム

我々は、外部利用者の視点から Web サーバのコンテンツ状態を監視する Web サーバリモート監視システムを開発、評価を行ってきた[6][7]。本節では、このシステムの概要と問題点、および、問題点を解決するために求められる要件について述べる。

2.1. リモート監視手法

図1に、Web サーバリモート監視システムによる、コンテンツ変更検知の様子を示す。

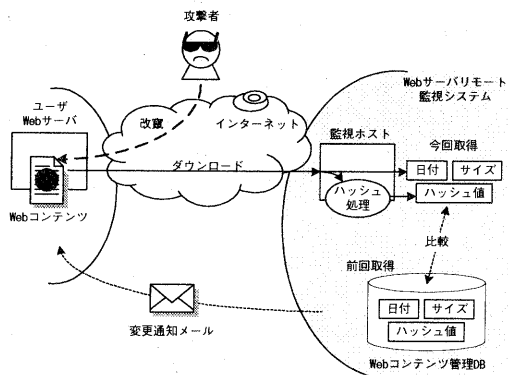


図1. Web サーバリモート監視システムによるコンテンツ変更検知

本システムは、インターネット越しに Web サーバ上のコンテンツを定期的にダウンロードして、そのヘッダ情報である日付やサイズ、さらには、コンテンツ部のハッシュ値を、前回取得した値と比較することで、変更を検知している。もし変更を検知した場合には、新たに取得した日付やサイズ、ハッシュ値を Web コン

テンツ管理 DB に保存して次回の検査に利用するとともに、ユーザに対して変更を検知した旨をメールで通知する。

2.2. 変更検知における問題点

Web サイトの中には、コンテンツ作成者と管理者が異なるケースがあり、この場合、往々にしてコンテンツのアップデートが管理者に通知されることなく行われている。日付やサイズ、ハッシュ値を用いてファイルの変更を検知する機能では、作成者による正規の更新と改竄を区別なく変更と判定してしまうため、通知を受けた管理者がコンテンツの状態を再確認する必要がある。頻繁に更新される Web サイトの場合、管理者が変更を知らせるアラームに慣れてしまい、改竄を知らせるアラームを見落としてしまう問題がある。

2.3. 変更検知に求められる要件

コンテンツの変更を検知した場合、それが正規の更新なのか、それとも改竄なのかを、的確に判定する必要がある。また、改竄を知らせるアラームには、どのような改竄が検知されたのかを説明する必要がある。

3. 改竄の分類と判定手法の提案

ここでは、典型的な改竄事例に注目し、これらについてタイプ分けを行う。分類されたタイプごとに、改竄を検出するための特徴について提案する。

3.1. 改竄事例の解説

いくつかの改竄事例を調査した中から、典型的な改竄事例を図2から図5で示し、その特徴について述べる。ただし、図2と図3については、実際の様子を試作コンテンツで再現したものとなっている。各図はネットスケープナビゲータ (Copyright © 2000-2002 Netscape Communications Corporation.[8])を用いて表示した様子である。

図2は、HTML 文書の終わりを表す</HTML>タグのさらに後ろにスクリプトを挿入された改竄事例である。また図3は、正規コンテンツ中にメッセージを埋め込んだ改竄事例である。この二つの事例の中には、"<!-- ~-->"によるコメント文やスクリプトを埋め込まれたものもあり、このような場合、ブラウザには改竄イメージなどは表示されないため、気付くのが遅れがちとなる。ちなみに Nimda [3]の場合は、</HTML>タグの後ろにスクリプト

"<html><script language="JavaScript"> window.open("readme.eml"...)"が挿入される (図2)。これらの事例の特徴は、元の HTML 文書がそのまま利用されていることであり、改竄前後のコンテンツを比較しても変更

点が少ない。ただ、改竄者からのメッセージが挿入される場合には、何処かの団体を批判することもあるが、多くは、自らのスキルをアピールするために改竄の成功を知らしめるキーワードが使われている。

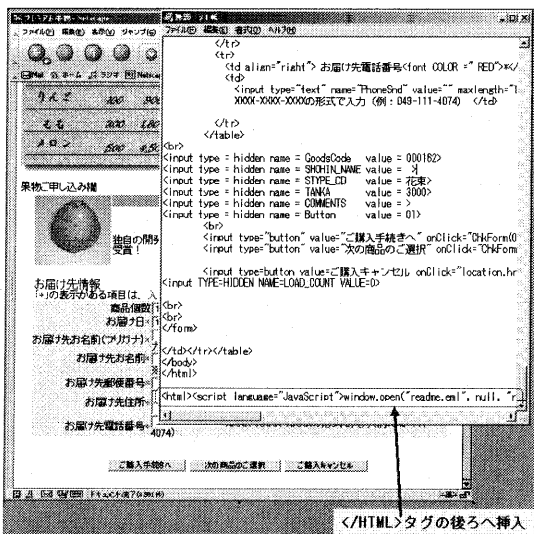


図 2. 正規 HTML 文書の後部への挿入改竄

テンツに上書きする改竄事例である。この場合、元のコンテンツと多くの点で特徴が異なってくる。例えば、ブラウザ[8]の左上に表示されるページのタイトルや、改竄らしく見せるための背景色や文字色などに特徴が現れる。また、このタイプの多くは、国籍に関係なく行われるため、言語エンコードがターゲットサイトと異なっている場合が多い。

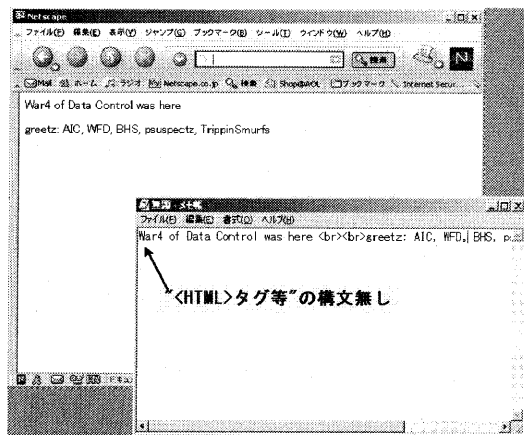


図 4. 簡易テキストによる上書き改竄

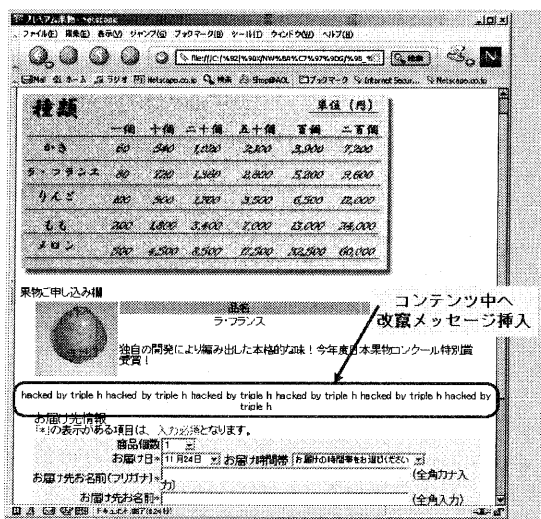


図 3. 正規 HTML 文書中への挿入改竄

図 4 は、正規コンテンツを簡易なテキストで上書きする改竄事例である。このような改竄の場合、HTML 文書としての構文すら持っていないものが多くみられる。

図 5 は、一目で改竄と分かるコンテンツを正規コン

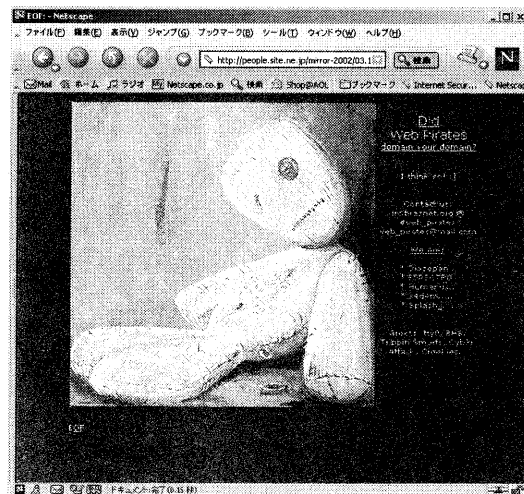


図 5. 明らかな改竄用コンテンツによる上書き改竄

3.2. 改竄タイプごとの判定手法の提案

改竄は、図 2、図 3 に代表される正規コンテンツの一部を改変する部分改竄タイプと、図 4、図 5 に代表される正規コンテンツを改竄用コンテンツに入れ替えてしまう上書き改竄タイプに大きく分けられる。前者は、挿入手法や挿入文字列の特徴に注目し、後者は、

挿入手法や挿入文字列の特徴に加え、変更前後のコンテンツを比較することで、改竄を判定する。

本稿では、改竄コンテンツのみを解析して判定する手法を単独判定、変更前後のコンテンツを比較する手法を比較判定と呼ぶこととする。この2つの判定手法において、それぞれ3つずつ、合計6つの特徴を改竄判定の基準として利用することを提案する。この様子を図6に整理する。最終的に改竄と判定する条件は、図6に示される6つの特徴のうち、1つでも該当する項目が検出された場合とする。

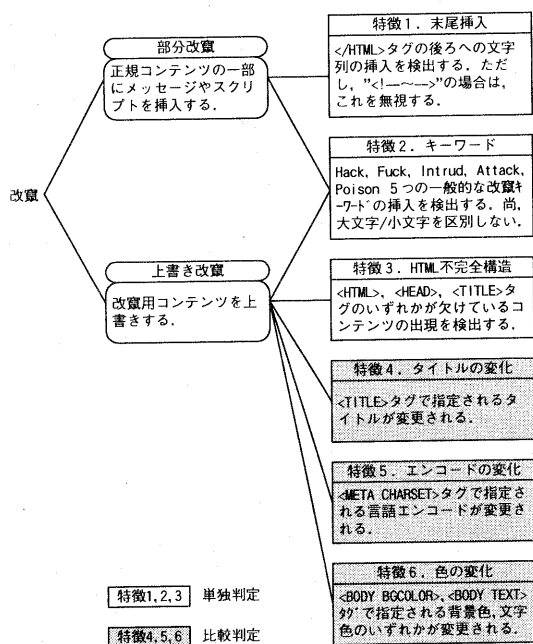


図6 改竄タイプと改竄判定のための注目すべき特徴

以下に、図6で示される各特徴について説明する。

【特徴1】末尾挿入

HTML文書の終わりを表す</HTML>タグの後ろに、文字列が挿入されたことを検出する。ただし、"<!-->"で指定されるコメントの場合は、これを無視する。尚、本特徴はHTML文書として好ましくない構文の存在を改竄と判定しているものである。

【特徴2】キーワード

Hack, Fuck, Intrud, Attack, Poisonの5つの改竄を主張する一般的なキーワードが挿入されたことを検出する。ここでは、大文字と小文字を区別しない。

【特徴3】HTML不完全構造

<HTML>, <HEAD>, <TITLE>タグのいずれかが欠けていることを検出する。尚、本特徴はHTML文書と

して好ましくない構文を持つコンテンツの出現を改竄と判定するものである。

【特徴4】タイトルの変化

変更前後のコンテンツにおいて<TITLE>タグが指定されている場合、タイトルの変化を検出する。

【特徴5】エンコードの変化

変更前後のコンテンツにおいて<META CHARSET>タグが指定されている場合、言語エンコードの変化を検出する。

【特徴6】色の変化

変更前後のコンテンツにおいて<BODY BGCOLOR>タグもしくは<BODY TEXT>タグが指定されている場合、背景色もしくは文字色の変化を検出する。

尚、本稿で対象にする改竄は、外部の閲覧者の立場から改竄と識別できるものを対象としており、Webサイト管理者のみが識別できるような改竄を考慮しない。例えば、メッセージの主旨を改竄する場合や、Eコマースサイトにおける価格の改竄などは対象としない。

3.3. 判定結果の通知

検出された特徴については、検出された箇所を示す説明とともに、Webサイト管理者へ通知する。これにより、改竄の様子を迅速に把握することが可能になる。

4. 評価

前章で提案した判定手法を評価するために、正規コンテンツと改竄コンテンツの各特徴、ならびに、正規更新時と改竄時の変化の特徴について、改竄された実例を基に調査する。

4.1. 評価サンプルの収集

正規更新時のサンプルとして、産官学のトップページのうち、2002年5月中に、更新を確認した16件のサイトの更新前後のコンテンツを用いる。

また、改竄時のサンプルとして、改竄コンテンツを数多く収集・管理している[9]から、2002年1月から2002年4月に発生した改竄事件のうち、2002年5月に、改竄コンテンツならびに正規コンテンツの両方を取得できた57件を用いる。さらに、バラエティに富んだサンプルにすることを目的として、インターネット上に公開されている様々な改竄事件のうち、2002年5月に、改竄コンテンツならびに正規コンテンツの両方取得できた16件を加える。ここでの正規コンテンツとは、改竄されてしまったサイトの2002年5月に公開中のトップページであり、改竄コンテンツと比較するために用いる改竄前のコンテンツとみなす。

まとめると、

- 正規コンテンツ=89件 (57件+16件+更新前コンテンツ16件)
- 改竄コンテンツ=73件 (57件+16件)
- 正規更新時の変更=16件
- 改竄時の変更=73件

を評価サンプルとする。

尚、改竄コンテンツと比較するために収集した正規コンテンツについては、改竄発生時点から収集時点までの経過時間が長くなるにつれて修正が多く加えられていくと予想されるため、改竄前の正規コンテンツとみなし難くなるが、サンプル数を確保するために本調査では全てを改竄前の正規コンテンツとみなす。

ちなみに、73件の改竄サンプルのうち、日本語による改竄は1件のみである。また、部分改竄が5件、上書き改竄が68件となっている。

4.2. 評価結果

収集したサンプルについて、部分改竄と上書き改竄を区別することなく、特徴1～6について統計調査を行った。

特徴1～3を検出する単独判定の統計結果を表1に、特徴4～6を検出する比較判定の統計結果を表2に示す。

表1. 特徴1～3による単独判定

単独判定		正規コンテンツ 89件		改竄コンテンツ 73件	
		件数	率 (%)	件数	率 (%)
特徴1	</HTML>後へ挿入	0	0.0	4	5.5
	!Hack*	0	0.0	24	32.9
	!Fuck*	0	0.0	8	11.0
	!Attack*	0	0.0	12	16.4
	!Intrud*	0	0.0	7	9.6
特徴2	!Poison*	0	0.0	1	1.4
	計 一つ以上該当	0	0.0	41	56.2
	特徴3	<HTML>欠落	1	1.1	12
<HEAD>欠落		0	0.0	20	27.4
<TITLE>欠落		0	0.0	16	21.9
計 一つ以上該当		1	1.1	28	38.3
特徴1～3の一つ以上該当		誤り1件	誤り率 1.1%	正解 54件	正解率 74.0%

表2. 特徴4～6による比較判定

比較判定		正規更新 16件		改竄変更 73件	
		変化数	変化率 (%)	変化数	変化率 (%)
特徴4	タイトル変更	0	0.0	55	75.3
特徴5	エンコード変更	0	0.0	17	23.2
特徴6	背景色変更	0	0.0	25	34.2
	文字色変更	0	0.0	10	13.7
	計：一つ以上該当	0	0.0	29	39.7
特徴4～6の一つ以上該当		誤り0件	誤り率 0.0%	正解 57件	正解率 78.1%

改竄については、特徴1～3を用いた単独判定、ならびに、特徴4～6を用いた比較判定の両手法とも、それぞれ7割以上を判定できた。調査したサンプルの多くが上書き改竄タイプであったため、結果としては変更前後のコンテンツを比べる比較判定の方が正判定率ならびに誤判定率ともに良かった。

統計調査を行う中で、改竄者が用いるキーワードには、"pombooooooooooooo"や"HoHoHo"などの造語や、

綴りを誤ったキーワードが多く見られたが、特徴2に示した5つのキーワードに注目すると、5割以上の改竄を検出できた。この他にも、"root"や"admin"というキーワードも多くみられたが、これについてはいくつかの正規コンテンツにも用いられていたため、今回は特徴から除外した。

特徴4のタイトルの変更で検出される割合が高いが、これで検出されない改竄は、特徴3の<TITLE>タグの欠落に引っ掛かっている場合が殆どであった。実際に、68件の上書き改竄の全てが、この二つの特徴で検出されていた。

特徴1～6を総合したときの、改竄の正判定率と誤判定率を表3に示す。また、全改竄サンプルの該当特徴数の分布を表4に示す。

表3. 特徴1～6による総合判定

特徴1～6の一つ以上該当	正規 89件※		改竄 73件	
総合判定	件数	率 (%)	件数	率 (%)
正規更新と判定	88	98.9	0	0.0
改竄変更と判定	1	1.1	73	100.0

※89件中の73件については、特徴1～6を一切持たないコンテンツから、今回収集した正規コンテンツへ変更されたものとみなしている。

表4. 改竄サンプルの該当特徴分布

該当特徴数	0点	1点	2点	3点	4点	5点	6点	計
件数	0	17	26	20	9	0	0	73
率 (%)	0.0	23.3	35.6	27.4	12.3	0.0	0.0	100.0

表3の総合判定の結果は、正判定率100%、誤判定率1.1%となっており、小さな誤判定率で全ての改竄を検知することができており、改竄を見逃さないフォルスポジティブの立場からは、十分な結果が得られたものと言える。誤判定した1件は、正規コンテンツに<HTML>タグが欠けているためであり、コンテンツ作成者に内容を通知して正規コンテンツの改修を依頼することで、誤検知を防ぐことができる。表4から、今回のサンプルについては、多くの改竄が複数の特徴を持っていることがわかるが、2割程度の改竄については1つの特徴しか該当していないため、今後収集を進めていくサンプルの中には、検出できない改竄が現れる可能性がある。

4.3. 改竄の傾向

過去の改竄事例の調査を行った際に、提案した6つの特徴以外にも、正規コンテンツと改竄コンテンツと見分ける特徴を発見したため、ここに報告する。

【参考特徴1】<A>タグ数

変更前のコンテンツに含まれるリンクを表す<A>タグ数が、変更後に大きく減少する場合や、全く無くな

ってしまう場合を検出する。これは、一般的な正規コンテンツには他ページへ遷移するためのリンクが多く含まれているのに対して、改竄コンテンツにはリンク先のページが限られていたり、リンクの必要すら無いものが多い点に注目している。

【参考特徴2】コンテンツサイズ

変更前のコンテンツサイズに比べて、変更後のコンテンツサイズが大きく減少してしまう場合を検出する。これは、正規コンテンツでは主張すべき内容が豊富なものに対して、改竄コンテンツは、改竄の成功を主張するのみであり、内容に乏しい点に注目している。

【参考特徴3】黒色の背景

<BODY BGCOLOR>で指定される背景色が黒いコンテンツの出現を検出する。これは、改竄の成功をビジュアル的に主張しやすい色が使われていることに注目している。

これらの特徴についても今回のサンプルに対して統計調査を行った(表5)。

殆どの正規コンテンツは、<A>タグを持っているのに対して、<A>タグを1つも持たない改竄コンテンツは7割以上あった。また、正規コンテンツの<A>タグ数は平均27.1個なのに対して、改竄コンテンツは1.7個であり、数や変化率で改竄を判定できうることを示している。コンテンツサイズについては、正規コンテンツが平均12.4Kbyteなのに対して、改竄コンテンツは平均2.0Kbyteとなっており、変更前後のファイルサイズの変化率で改竄を判定できうることを示している。黒色の背景については、正規コンテンツが3件しかないのに対して、改竄コンテンツの約5割が黒色であった。

表5. 正規コンテンツと改竄コンテンツの傾向

	正規コンテンツ 89件	改竄コンテンツ 73件
リンク: <A>タグ無し	2件 2.2%	57件 78.1%
リンク: <A>タグ数	平均 27.1個	平均 1.7個
コンテンツサイズ	平均 12.4KByte	平均 2.0KByte
背景: BGCOLOR黒	3件 3.4%	37件 50.7%

5. おわりに

本稿では、Web サーバリモート監視システムにおいて、コンテンツに変更を検知した場合、コンテンツ自体の特徴、ならびに、変更前後の変化の特徴に注目することで、その変更が正規の更新によるものか、それとも改竄によるものかを、判定する手法を提案した。実際の改竄サンプルを用いて、改竄判定率を評価した結果、100%の正判定率と、1.1%の誤判定率を達成していた。これにより、正規の更新による多数の変更アラームに悩まされていたサイト管理者は、改竄アラーム

に集中することができるようになり、また、改竄箇所とその特徴を知らされることで、コンテンツの改竄状況を迅速に確認することができるようになる。

今回評価に用いたサンプルの多くが、海外から日本のWebサイトをターゲットにしたものであり、日本人による部分改竄型のサンプルについては、評価に至っていない。今後は、改竄サンプルや正規更新サンプルの数や種類を増やししながら、提案手法の妥当性について検討を進める。今後の調査の中で、検知できない改竄があった場合には、<A>タグやコンテンツサイズなどの特徴にも注目した新たな判定則について提案する。また、検知できない改竄が増えたときに、判定則をより広げることによって誤検知率が高まることが懸念されるが、このときには、検出された各特徴間の相関や重み付けを用いた改竄危険度を、率やレベルで推定する手法について提案する予定である。

文 献

- [1] “Web 改竄の防止を目的として行う価値のある対策”，情報処理振興事業協会，
<http://www.ipa.go.jp/security/ciadr/webjack.htm>.
- [2] ワーム sadmind/IIIS による Web 改竄インシデントの対策について，情報処理振興事業協会，
<http://www.ipa.go.jp/security/ciadr/200105sadmindii.s.html>.
- [3] “新種ウィルス「W32/Nimda」に関する情報”，情報処理振興事業協会(IPA)，
<http://www.ipa.go.jp/security/topics/newvirus/nimda.html>.
- [4] 伊原秀明，“TRIPWIRE for LINUX”，トリップワイヤ・ジャパン監修，オライリー・ジャパン発行，初版 2001 年 4 月。
- [5] 可部孝二，曾我正和，西垣正勝，田窪昭夫，“ホームページ改竄パトロール方式”，情処技法，コンピュータセキュリティ研究会（CSEC），pp.173-178，2000 年 3 月。
- [6] 大東俊博，増田進介，三宅崇之，白石善明，森井昌克，“インターネットを介した Web ページ改竄監視システムの開発とその運用実験”，信学技法，オフィスシステム研究会（OFS），pp.24-30，2001 年 11 月。
- [7] 竹森敬祐，田中俊昭，中尾康二，大東俊博，三宅崇之，白石善明，森井昌克，“Web サーバリモート監視システムの実装および評価”，2002 年暗号と情報セキュリティシンポジウム（SCIS2002），pp.651-656，2002 年 1 月。
- [8] Netscape
<http://wp.netscape.com/ja/index.html>
- [9] EVERYDAY PEOPLE，
<http://people.site.ne.jp/2002/>.
- [10] Net Security
<https://www.netsecurity.ne.jp/>.
- [11] アンク，“HTML タグ辞典 - 第 4 版 -”，翔泳社発行，初版 2001 年 1 月。