新版

Web改ざん検知システム『WebS@T』※のご説明資料

～Interop 2007 Best of Show Award～
WebS@T
情報セキュリティ製品部門　グランプリ受賞

開発：KDDI株式会社
研究：株式会社KDDI研究所、神戸大学森井教授
発売元：株式会社ネットワールド

(V.2.1.4)

NETWORLD
株式会社ネットワールド

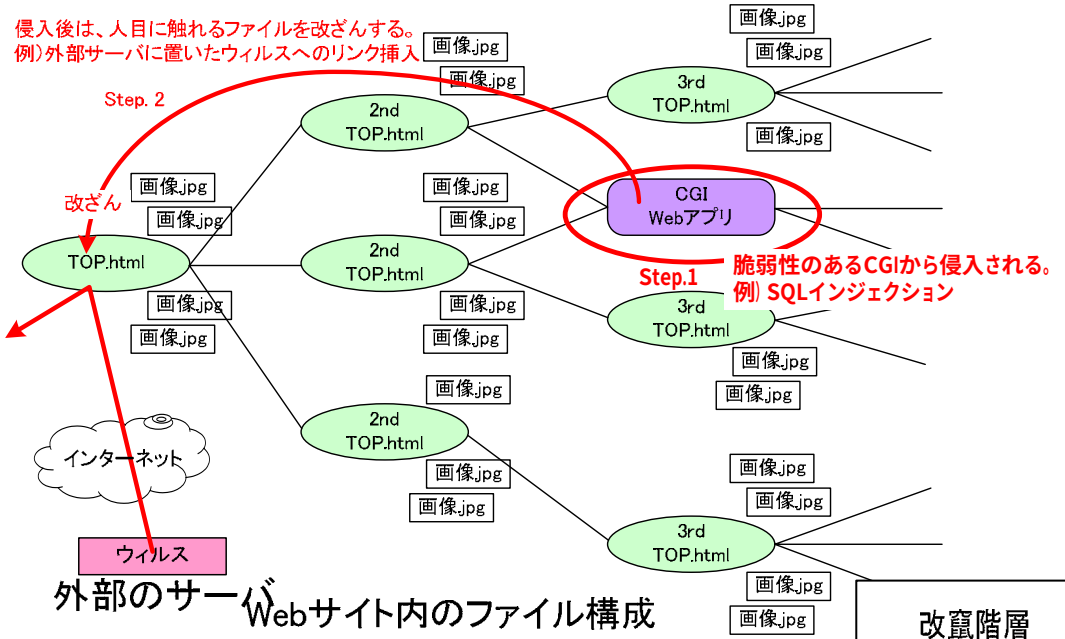
※『WebS@T』：通称ウェブサット

目次

NETWORLD
株式会社ネットワールド

最近の改ざん事情　1

- 侵入に利用されるWebページ
  - ログイン機能などを提供するWebアプリケーションに対して、セキュリティ侵害を引き起こすコマンドを混入して、ログイン認証をすり抜けるSQLインジェクション攻撃がある。
- 改ざんされるWebページ
  - 侵入後は、改ざん画像の設置やウイルスをダウンロードさせるためのリンクを貼る。



Webサイト内のファイル構成

狙われやすい上位のWebページ

2006年8月調査

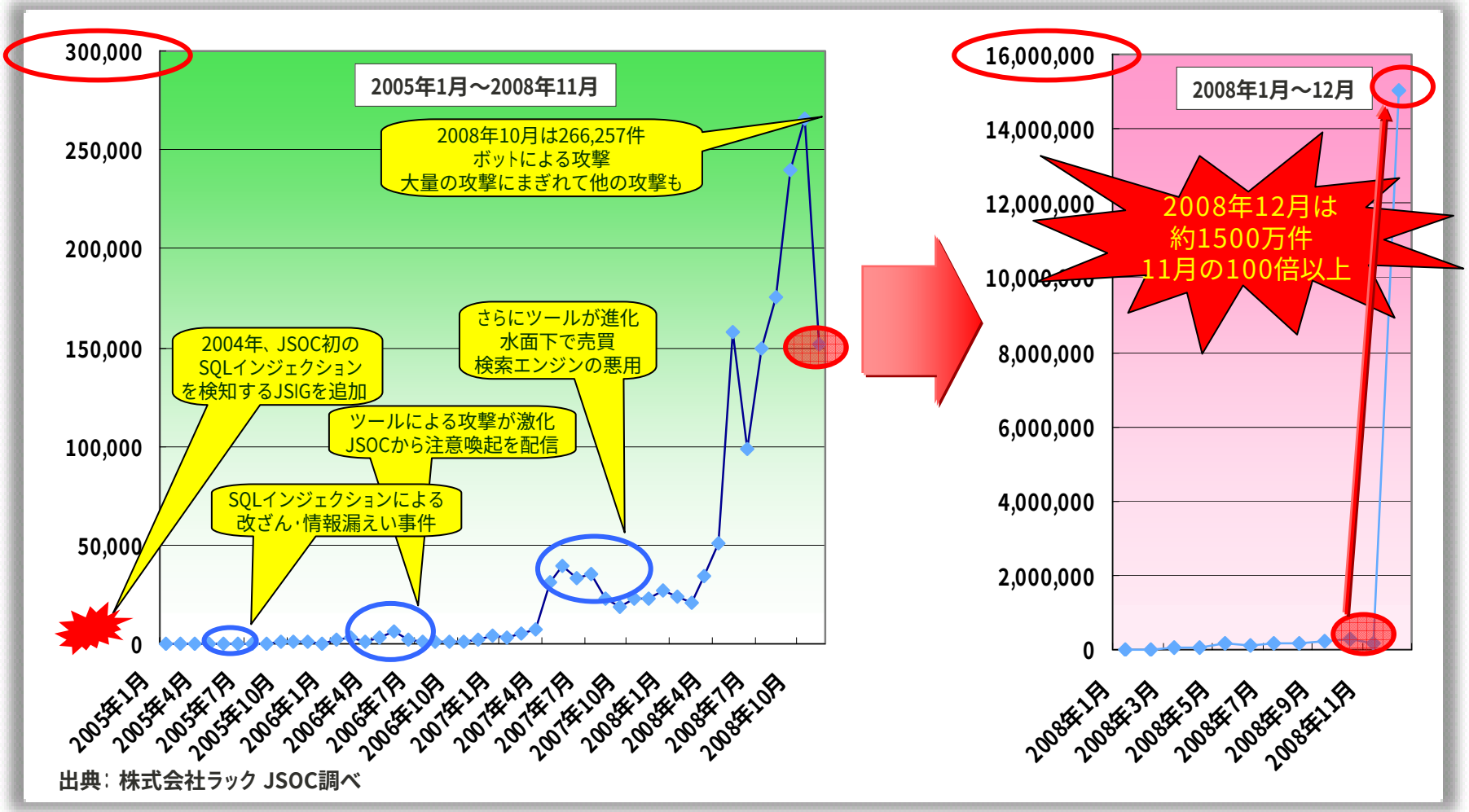
http://www.fearoot.com/

改ざんされるのは、ﾄｯﾌﾟﾍﾟｰｼﾞから第3層までで90%以上となる。

改竄階層	第1層 TOPﾍﾟｰｼﾞ	第2層	第3層	第4層	第5層 以下
該当数 率	18/24(種) =75.0%	3/24(種) =13%	1/24(種) =4%	0/24(種) =0%	2/24(種) =8%

最近の改ざん事情　2

驚異的に増加するWebアプリケーションへの攻撃は、2008年12月には**前月の100倍以上に急増**しました。



出典：株式会社ラック JSOC調べ

最近の改ざん事情 3

iframeを利用したウイルスの急増

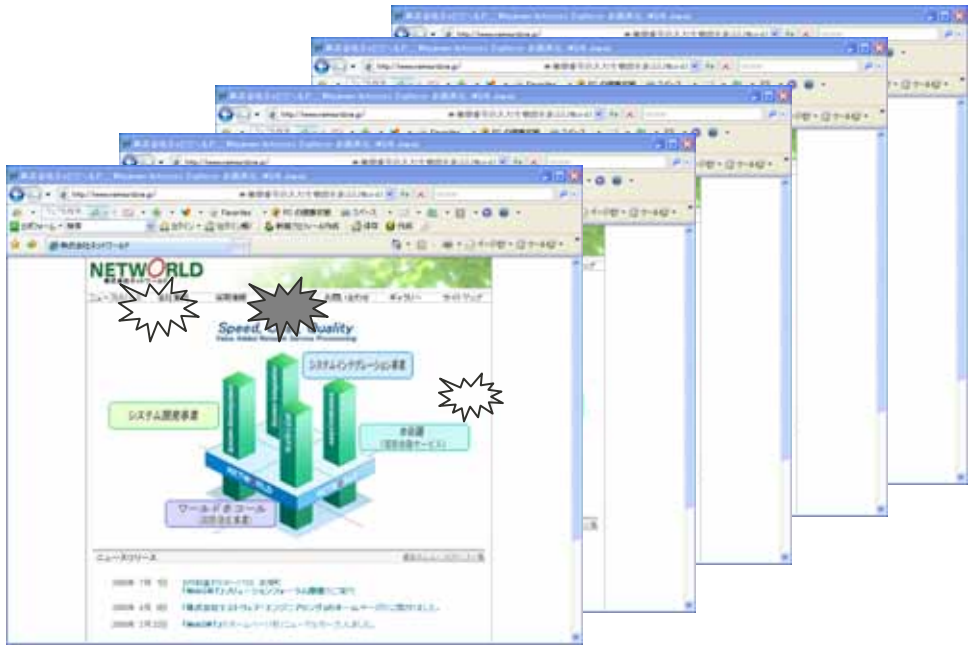
- iframeとは「インラインフレーム」のことで、HTMLテキストの中にフレームを埋め込むタブ
- 最近、iframeの機能を悪用して、外部から任意のコードを実行させるといった手法でよく使用されるため、現在では「iframa=Malware」というような認識が増えている。
- iframeはWebサイトの脆弱性をついてサイト内に埋め込まれる。
- Malwareとは、遠隔地のコンピュータに侵入したり、攻撃したりするソフトウェアやコンピュータウイルスのようにコンピュータに侵入して他のコンピュータへの感染活動や破壊活動を行ったり、情報を外部に漏洩させたりする有害なソフトウェアのことを言う。

遠隔操作

フィッシング詐欺

最近の改ざん事情　3

九州地方H市のWebページ改ざん多発



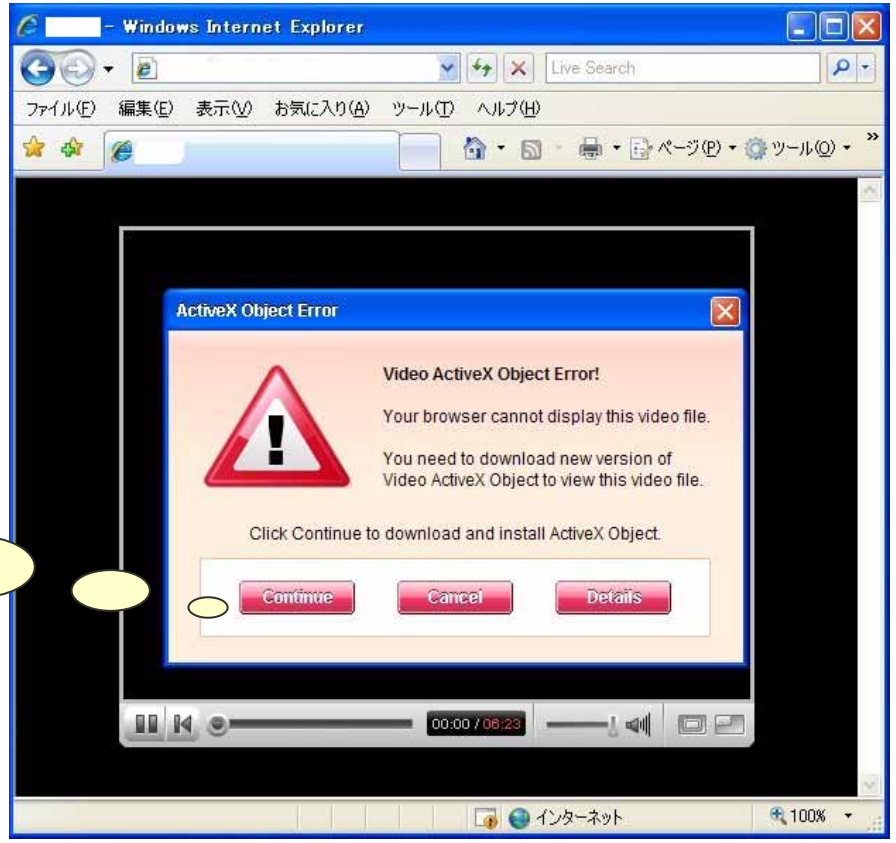
その後、ホームページで謝罪を！

最近の改ざん事情　4

大規模な改ざん

セキュリティ企業各社はWebサイトを改ざんする大規模な攻撃が再び確認されたと注意を呼びかけている。

改ざんサイトから誘導されるメッセージが表示される。



改ざんの目的

Webサイト改ざんの目的は……

◆政治的なデモンストレーション、イデオロギー表現
・政府系や公共系の攻撃は、多くは政治的・宗教的なﾃﾞﾓﾝｽﾄﾚｰｼｮﾝ行為で、閲覧数の多いWebサイトも狙われる。

◆自己顕示欲を誇示、興味本位（愉快犯）
・ハッカーが自分のスキルを誇示したい、興味本位で騒動を起こすため。

◆産業スパイ、利害関係による怨恨
・機密・秘密情報を取得する、過去の怨恨を晴らす、損害を与えるため。

◆直接・間接的に個人情報を搾取
・Webサイトやデータベースから直接的に、フィッシング詐欺のように間接的に個人情報を取得するため。

◆サイバーテロ
・社会や特定の組織・企業を混乱させるため。

Webサイト改ざんの影響

Webサイトが改ざんされると……

取引先や顧客からの**信用が失墜**し、**ブランド価値も低下**し、ましてフィッシング詐欺を含む個人情報の搾取等に悪用された場合、被害者からの**損害賠償**にまでに発展する可能性がある!!

WebS@T開発の背景

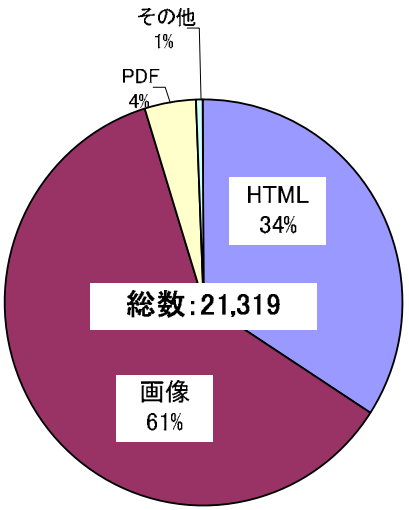
- 企業Webサイトの状況
  - 企業のWebサイトは、数百～数万個のホームページファイルを管理している。
  - 1ヶ月あたり延べ数百回の頻度でホームページファイルが更新されている。
  - さまざまな種類のファイルから構成されている。

ファイル数と更新頻度

企業	URL	URL数	更新頻度（回/月）
A社	http://www.***.com/	25,144	259
B社	http://www.***.com/	21,319	153
C社	http://www.***.ne.jp/	20,944	180
D社	http://www.***.co.jp/	10,046	–
E社	http://www.***.jp/	614	–
F社	http://www.***.com/	356	–
G社	http://www.***.com/	140	–

困難
全てのファイルのセキュリティ監査

ファイル種別と更新ミスの頻度



種別	取得成功	取得失敗 Not Found?
JPG	12,992	5
HTML	7,096	210
PDF	879	3
XLS	75	0
DOC	12	0
ASX	12	0
XML	8	0
RAM	8	0
CGI	5	0
EXE	4	0
WAV	2	0
JavaScript	0	8
計	21,093	226

困難
各種ファイルのセキュリティ監査

NETWORLD
株式会社ネットワールド

参考

改ざん事例の課題と従来の対策方法

◆課題

- 運営者は改ざんされたことに気付かない。または、気付くまで時間が掛かってしまう。
- 利用しているユーザ、もしくは顧客が気付く場合が多く見られ、また利用しているユーザにも被害が及んでる。
- 改ざんが発生してから気付くまでの時間が長いほど被害が大きくなる。

従来のソリューションでは・・・

改ざんされた事をいち早く気付くことが重要

＋サイトを監視する専門の人員を確保

サイトの規模によっては人海戦術による監視では、コストの壁によるリソース・物理的限界が発生してしまう・・・・

＋監視ソフトウェアを導入

動作検証、及び導入のためにサービスを停止させることが必要なため、時間とコストが掛かってしまう・・・・・

NETWORLD 株式会社ネットワールド

検知の要件

◆監視作業の自動化

- システム的に監視することができ、しかも更新･改ざんを識別して通知してくれるため、**監視要員をミニマイズ**。

◆システム導入が簡単

- ネットワーク環境やOSに依存しないので、既存のシステムを変更する必要がなく、通常は**短時間で導入**。

◆システム運用が容易

- 監視対象のサイトURLを指定するだけで、自動（もしくは手動）で監視対象コンテンツを登録･監視し、以降24H/365D、ほぼ**メンテナンス･フリーで運用**。

Web改ざん検知システムの開発

◆改ざん検知システムの開発

- ハッカーが改ざんを行った際にあらわれるコンテンツ特徴を検知するアルゴリズムを、２００1年からKDDI研究所ネットワークセキュリティグループ竹森Ph.D及び神戸大学森井教授が長年研究してシステムを開発

KDDI研究所のリリースからの一節

WEB P@TROLLER(WebS@T呼称に変更)は、監視中のホームページファイルに変更を検知すると世界で初めて開発した”改ざん判定パターン”との照合を行い、正規の更新と悪意の改ざんを見分けてアラームを発信します。この照合は、高い精度で更新と改ざんを判定できており、改ざん時の緊急対応に寄与します。

2007 年6 月11 日から15 日に千葉県幕張メッセで開催されたInterop Tokyo 2007 へ出展し、Best of Show Award プロダクトアワード部門 情報セキュリティ製品にて、グランプリを獲得しました。これは、独創性と利便性を高く評価して頂いた結果であり、ホームページに対する攻撃監視製品として期待されています。

http://www.kddilabs.jp/news/img/3_1.pdf

WebS@Tの基本機能

◆情報収集

- 監視対象サイトのリンク先から監視対象の「コンテンツ」を収集します。

◆検知

- 継続的に監視対象の「コンテンツ」を監視し、不審な「コンテンツ」を検知します。

◆サイト構造の解析

- クローラが監視対象サイトのリンク構造、反応速度を分析します。

◆報告

- 改ざんされた「コンテンツ」を記録し、管理者に即座に知らせます。
- 監視対象サイトのリンク構造、反応速度を分析します。

機能例-1：監視対象コンテンツの自動登録

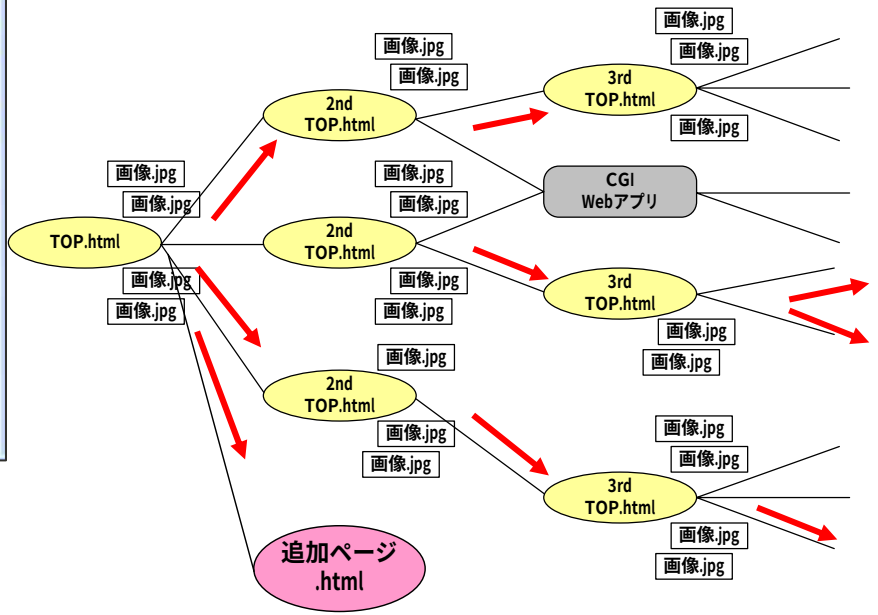
監視ファイルの自動設定

◆ Webサイトのトップページ のURL（例：http://www.kddilabs.jp/）を指定するだけで、ホームページのリンク構造を解析して、監視ファイル（10～1,000ファイル）を自動的に選択する。

利点⇒ 簡単な監視設定を実現。

監視ページの設定画面

★ リンクの自動探索による監視ファイルの選択



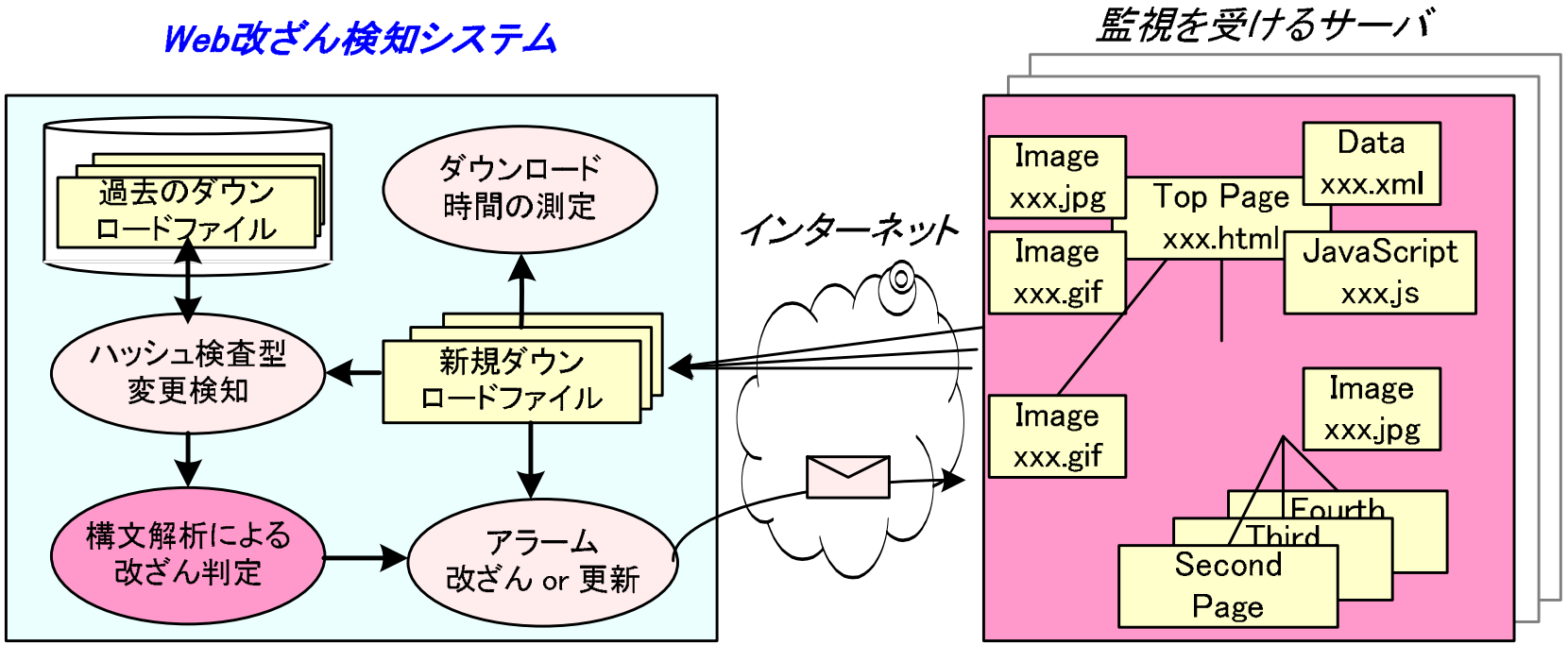
Webサイトの更新に対する自動追従

◆ 追加や削除されるホームページに対して、監視すべきページを日々自動的に追従する。

利点⇒ 完全な自動運用を実現。

機能例-2：改ざんコンテンツの発見

- リモート監視と構文解析による改ざん検知
  - 定期的に監視対象のWebファイルをダウンロードして、構文解析を行い、正規の「更新」と悪意の「改ざん」を見分けてアラームを発信する。
  - ダウンロードの遅延やファイルを取得できない場合には「障害」アラームを発信する。



【世界初】更新と改ざんを見分けるための改ざんパターンDBを世界で初めて開発した。

機能例-3：SQLインジェクション攻撃（結果の痕跡：ホームページ改ざん）の監視（動的ページの監視）

動的ページの監視

- SQL-DBと連携して、アクセスする度に変化する動的なホームページ（CGI）がある。
- こうしたサイトの多くは、Webアプリケーションで作成されており、攻撃対象になりやすい。

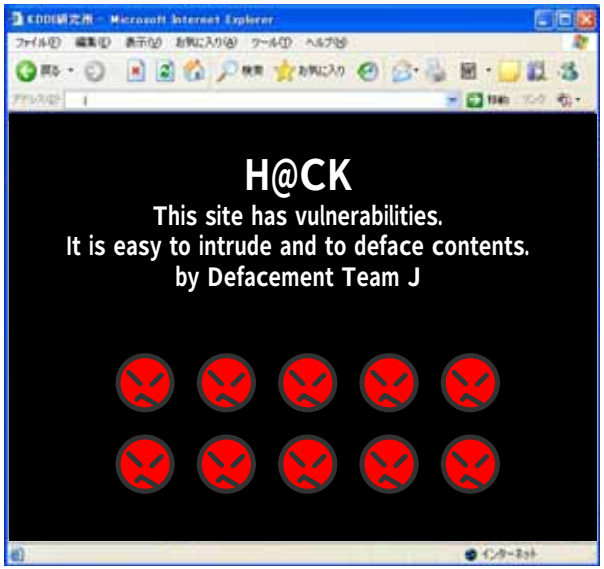
SQLインジェクション攻撃の監視

- 定型的な変化を、更新と判定しない。
- 定型箇所以外の変化に注目した構文解析を適用することで改ざん判定を行う。

利点⇒ 動的ページの監視を実現

auオークションにおける動的Webページ

機能例-4：検知率の評価

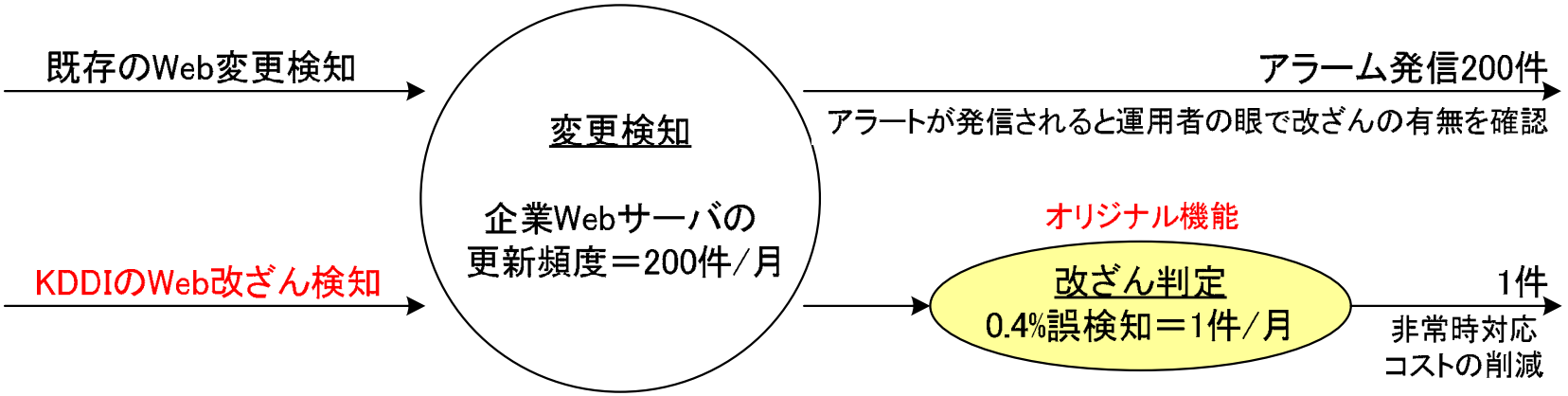


判定精度の評価

- 公開されている59個のWebサイトを1週間監視して、「更新」と「改ざん」の判定精度を評価した。

改ざん判定アルゴリズムのフィールド評価 (2007年5月実施)

判定結果	商用サイトの変更477件	改ざんファイル158件
更新	475件（99.6%）	0件（0.0%） 誤検知
改ざん	2件（0.4%） 誤検知	158件（100.0%）



機能例-5：サイト構築の解析

■監視対象のサイトURLリンク解析

- 監視対象のWebサイトにて管理されているファイル種類、リンク切れページ、平均ダウンロード時間速度の分析ができます。
- 詳細な分析情報としてリンクエラーページの特定やレスポンス遅延ページが特定できます。

機能例-6：改ざんコンテンツ・ダウンロード速度遅延

障害検知

- コンテンツが正常に取得できない場合（回線障害・遅延・リンク切れ）は障害として検知します。

緊急アラーム

- WebS@Tは、改ざんコンテンツの“検知”または“障害“を識別した場合、直ちに緊急メールが発信されます。

月次レポート

- 更新・改ざん・障害の履歴が、毎月一回レポートとして配信されます。

WebS@T導入のメリット (1)

管理者向けメリット

⇒ コンテンツの内容に着目し改ざんを発見

- SQLインジェクションによるコンテンツ改ざんなど、これまで検出できなかった事象に対して検知がおこなえます。

⇒ 監視対象サーバは変更する必要なし

- 監視対象ホストOS・Webアプリの変更を一切必要としないソリューション。
- 監視対象に対してネットワーク構成の変更は必要なし。
- LANに接続し、監視URLを登録するだけで導入可能。

⇒ 監視のメンテナンス作業は不要

- 監視対象のURLを設定するだけで自動的にシステムがリンク検索を行い、監視対象のコンテンツ登録・削除。

何よりも、管理者に導入の負担を掛けません！

NETWORLD 株式会社ネットワールド

WebS@T導入のメリット (2)

経営者向けメリット

⇒ 低導入コスト

- 既存のシステムに対して変更が必要ないため、検証作業が発生しません。

⇒ Webサイトのモニタリング体制を確立

- ECサイトなど金銭取引が発生するシステムに対しても、短時間で導入できることから、すばやく監視体制を確立することができます。

⇒ 監視品質の確保

- システム的に監視を行うため、監視品質が一定に保つことができます。今後の内部統制対策にも有効となります。

企業・組織の信頼性向上に寄与します！

【WebS@T】の導入モデル

同一機能を持っていますが、お客様の環境に合わせて
3つのモデルを用意しています。

◆ＡＳＰアカウントサービス　⇒即導入を希望される小規模のお客様へ
サーバは弊社側で用意･運用。
1ＵＲＬごとの毎月の費用のみで、即、改ざん監視が可能。

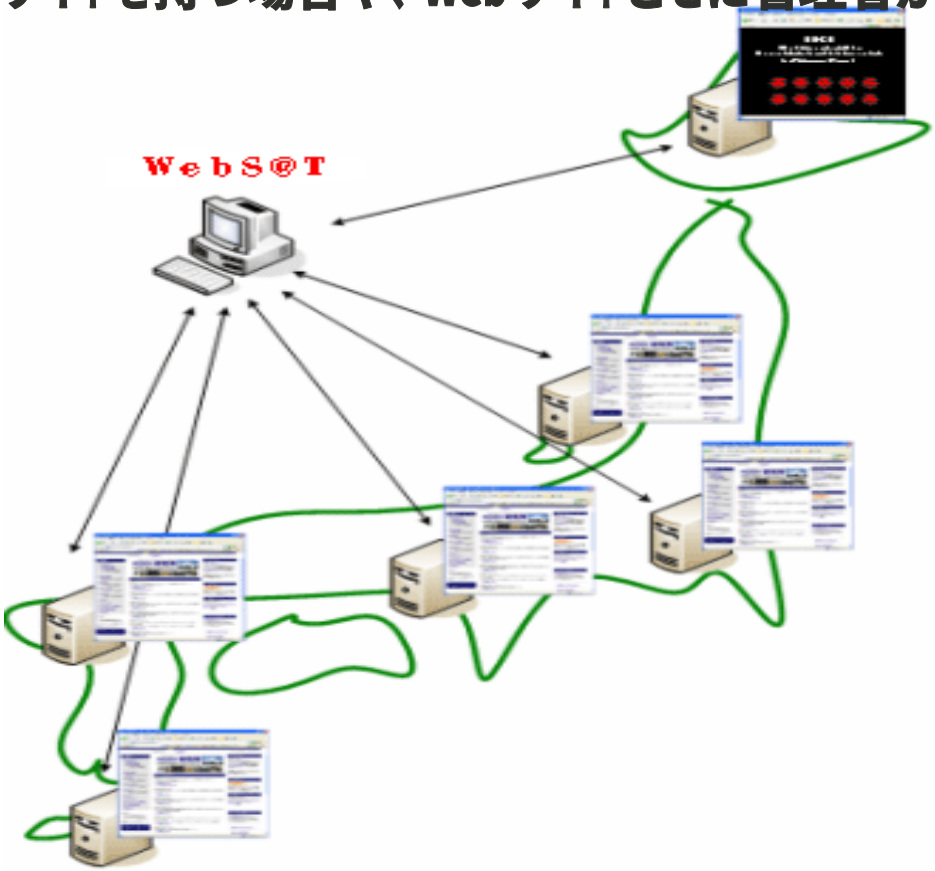
◆ＡＳＰモデル　⇒第三者様へのサービス展開をお考えのお客様へ
サーバは御社環境に設置。稼働環境費用が必要となる。
１ＵＲＬあたりに低価格な毎月の費用を設定。

◆アプライアンスモデル　⇒クローズ運用を必要とする、または多数のHPをお持ちのグループ企業さまや大規模のお客様へ
サーバは御社環境に設置。初期費用に5～１００ＵＲＬ監視のライセンスを含む。4モデルあり、モデルごとにurl数を制限。

NETWORLD
株式会社ネットワールド

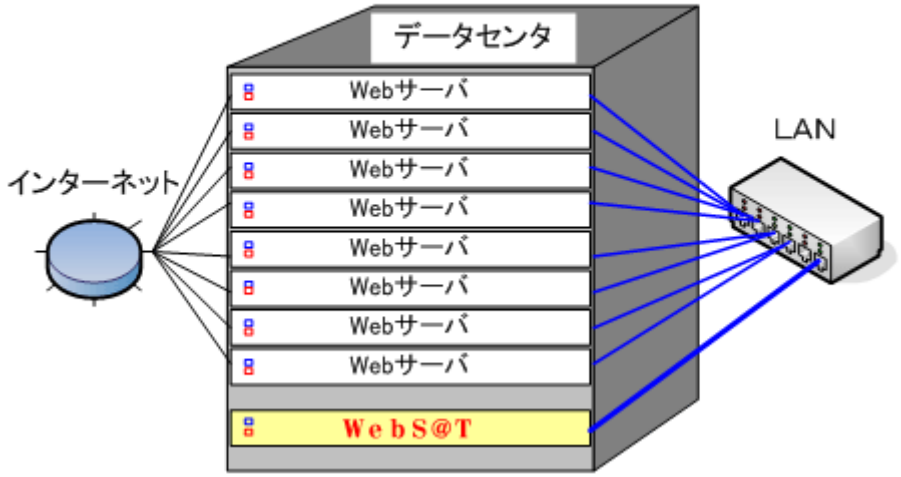
導入事例その1　(アプライアンス販売)

■全国にWebサイトを持つ場合や、Webサイトごとに管理者が違う法人向け。



導入事例その2　(監視サービス販売)

■ お客様のWebサーバを管理する事業者。



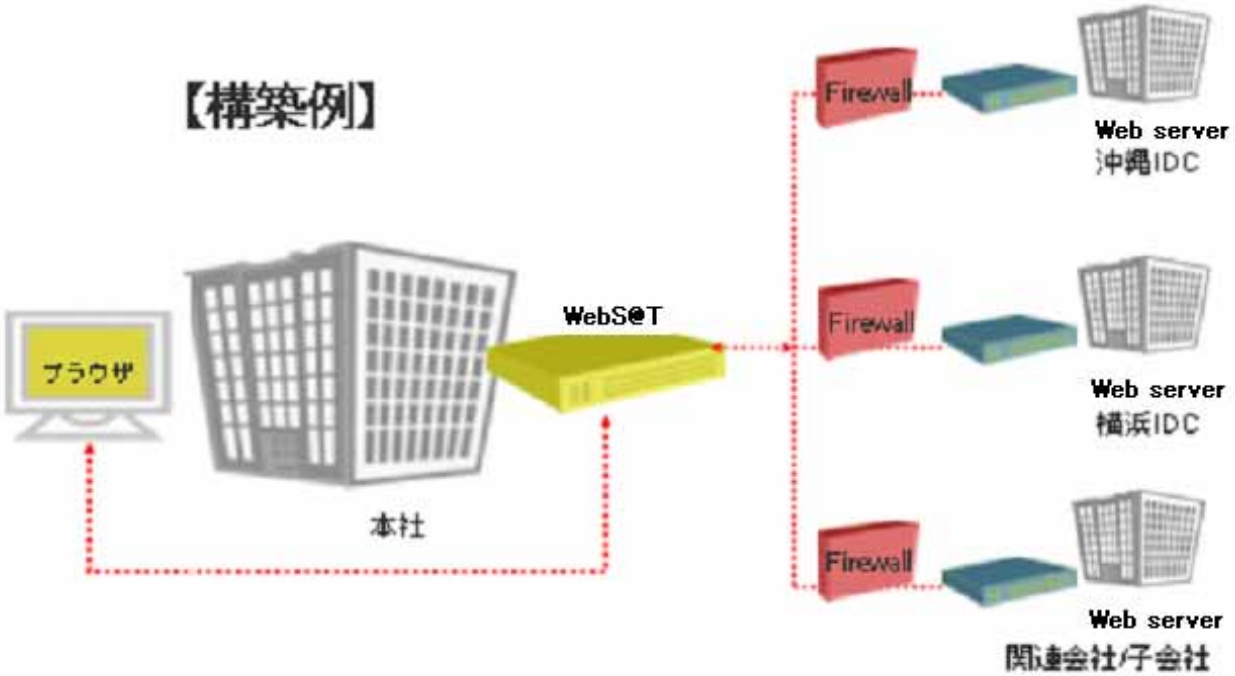
■ 処理能力

◆ 1台のWebS@Tで、一括監視できる。

導入事例その3　(導入と運用)

導入と運用

WebS@TのLANポートに接続し、登録IPアドレス及びメールサーバの設定を行います。
WEBブラウザから機器や監視の設定、また監視対象サイトのステータス確認を行うことができます。
各サイトの管理者毎にアカウントを発行することが可能です。



WebS@Tお問合せ先

株式会社ネットワールド
営業本部　ソリューション営業グループ
WebS@Tカスタマーセンター
http://www.networld.ne.jp/websat/　(http://www.kaizankenchi.jp/　近日サービス)
TEL：03-5542-3289　　E-mail：websat@networld.ne.jp

会社概要

商号	株式会社ネットワールド
本社	〒104-0033　東京都中央区新川1-5-13　伊成ビル5F
設立	１９９７年７月７日
代表	高野　清

システム開発事業インターネットやインターネットへつながる各種システム（モバイル、PDA、PC等）、及びオープンソフトウェア類を活用した情報通信システムに関わる調査、企画、設計、製造、構築、試験、運用を行っております。

システムインテグレーション事業企業、SOHO向けのネットワークや各種サーバの構築、運用管理、保守サポートを行い、また、必要に応じてセキュリティに関するコンサルタントをいたします。eビジネス／各種業務システムの導入、VoIP製品、CTI製品の導入および構築を行っております。

国際通信事業20年以上携わってきた国際通信のベテランがお届けする高品質･格安の国際電話サービス事業（プリペイドカードコール、デポジットコール、ポストペイドコール）の提供および付随するOEMカードの企画･製作･運用などの代行業務サービスの提供をメインに行っております。また、携帯電話（au、TU-KA、Vodafone）やNTT、NTT-com、KDDIなどのネットワーク販売代理業務、レンタル携帯事業も行っております

電話会議サービス
http://www.e-conf.jp
WEBブラウザによる会議のオンライン予約、キャンセルが簡単な操作で行えます。参加者の呼び出し、切断、ミュート、会議延長などの制御も自在。接続状況や残り時間をモニタで確認できるので、安心してご利用いただけます。海外との発着信利用も可能です。携帯電話やPHSの接続もサポートしています。登録料 は一切かかりません。IDが届いたその日から、ご利用形態に合わせて自由な電話会議がはじめられます。利用料は1回線20円/分。他社と比較しても約3割 お得です

NETWORLD 株式会社ネットワールド