

「我が社のウェブサイトが、知らぬ間にウィルス配布サイトになっていた。」

被害多発中の改ざん攻撃に終止符を！

ウェブサイト改ざん瞬間検知・瞬間復旧ソリューション WebARGUS（ウェブアルゴス）をリリース

デジタル・インフォメーション・テクノロジー株式会社（本社：東京都中央区八丁堀 4-5-4 ダヴィンチ桜橋ビル3階、代表取締役社長：市川 憲和 <http://www.ditgroup.jp>）は、2014年7月1日、企業のウェブサイトやサイト訪問者をサイバー攻撃の脅威から守るセキュリティソフトウェア新製品、『改ざん瞬間検知・瞬間復旧ソリューション WebARGUS（ウェブアルゴス）』をリリース・販売開始いたしました。

◆WebARGUS（ウェブアルゴス）の特徴◆

1. ウェブサイトの改ざん状態を極力ゼロにする、瞬間検知・瞬間復旧。 悪質な未知のサイバー攻撃から、サイト運営企業やサイト閲覧者を保護します。

監視対象のファイル・ディレクトリが改ざんされたときに発生する“OSのイベント”を直接監視しているため、イベント発生と同時に検知・自動復旧処理が作動します。これにより、改ざん発生からわずか1秒以内※1で正常な状態に自動復旧することができるため、一般的な“定期監視タイプ”の改ざん検知製品などで生じる、改ざんに気づいてから復旧までのタイムラグがほとんどありません。

※1：動作環境、及び復旧対象データのサイズにより異なる場合がございます。

2. 正規ユーザーになりすました改ざんや内部犯行、防御が困難な新手の手口にも対応。

監視対象に設定したファイル・ディレクトリへの変更・追加・削除・権限変更自体を監視するため、正規ユーザーになりすました不正アクセスや内部犯行による改ざん、攻撃のパターンマッチによるセキュリティ製品では防ぐのが困難な、新たな手口の攻撃（ゼロデイ攻撃）による改ざんも検知・復旧が可能です。

3. 1ビットの改ざんも見逃さない、『電子署名』技術を駆使した高精度の改ざん検知。

大手金融機関を中心に長年ご愛用頂いている、メール改ざん防止製品『APMG（2005年リリースの自社製品）』のコアエンジン技術を駆使し、1ビットの改ざんも見逃さない高精度な改ざん検知機能を実現しています。また、

製品本体や復旧元データにも電子署名を付与しているため、製品本体への改ざんも見逃しません。

4. 通常監視時にウェブサーバにかかる CPU 負荷（使用率）は 1%未満。

OS のイベントを監視する検知方式のもう一つのメリットとして、通常監視時（改ざんのイベントが発生していない状態）には処理が発生しない特徴があります。これにより、既存環境へソフトウェアをインストールし、稼働させることによって生じるウェブサーバへの CPU 負荷（使用率）を 1%未満※2に抑えることができています。

※2：監視対象範囲等により異なる場合がございます。

5. アプリケーションや設定ファイルを狙った高度な改ざん攻撃にも対応。

本製品は「サーバ内部監視型」。対象のウェブサーバに監視用のソフトウェアをインストールして作動させるため、ウェブサーバ内のほぼすべてのファイル・ディレクトリへの変更・追加・削除・権限変更を検知し、自動復旧することができます。（監視することで OS の稼働に影響が出るディレクトリを除きます。）

6. その他、安心・便利にご利用いただける各種機能を搭載。

主な
便利
機能

【GUI 管理画面】

ウェブブラウザ経由でアクセスできる管理画面で、各種設定作業がスムーズに行えます。

【証拠保全機能】

自動復旧前に、改ざん状態のファイルをコピーして退避。

改ざんの中身を証拠として残します。

【簡単監視設定】

ウェブサーバのディレクトリ構成を、視覚的に確認しながら、簡単に監視設定が行えます。

【アラートメール通知機能】

改ざんや復旧、Agent の動作異常検知時に、指定したメールアドレスにアラートメールを送信します。

※詳しくはウェブサイトでご紹介しています。

◆背景◆

近年の、日本国内企業のウェブサイトへの改ざん攻撃が急増しております。その攻撃は、一般的に認知されている、特定企業や団体への嫌がらせや破壊活動などではなく、金銭目的と見受けられる攻撃が多発しているのが実態です。

その手口の多くは、サイト管理者やウェブセキュリティ製品でさえも気が付きにくい方法によって、通常的一般企業のウェブサイトマルウェア配布サイトに改ざんするもので、サイトを閲覧したユーザーのパソコンが知らぬ間にウィルスに感染してしまう危険があります。具体的な被害としては、

- ・機密情報やクレジットカード情報を搾取される
- ・偽のインターネットバンキングサイトを表示し不正送金をさせられる

- ・ PC を遠隔操作される

などが挙げられ、改ざん攻撃にあった企業だけでなく、ウェブサイトを開覧しているだけの不特定多数の個人までもが脅威にさらされています。

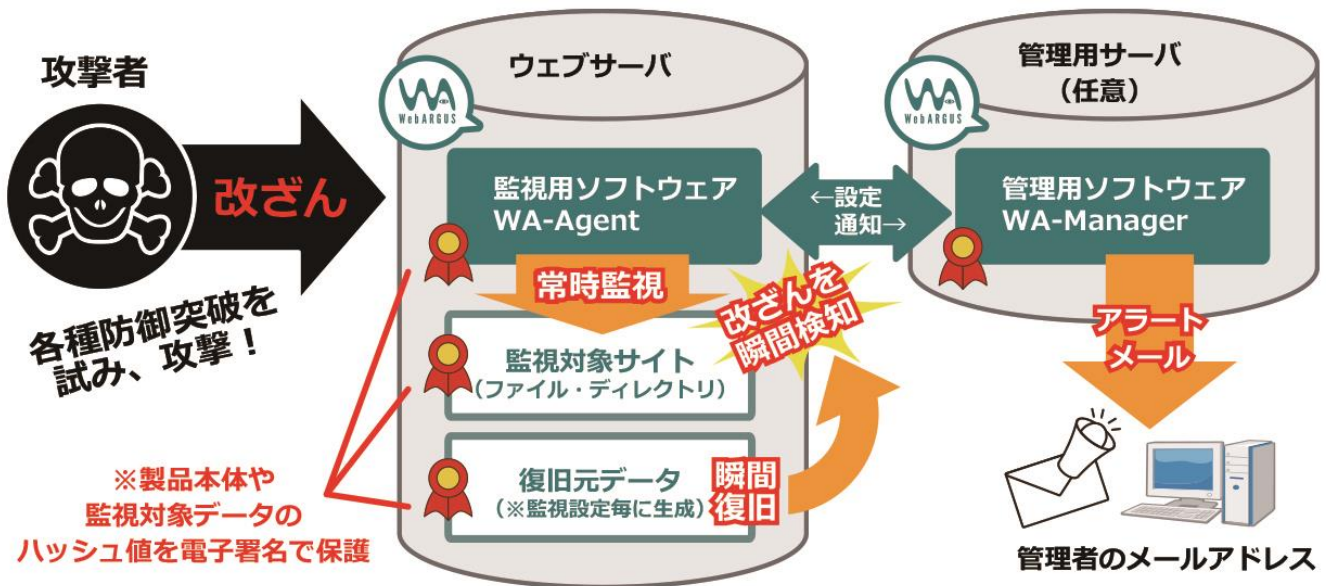
こうした深刻な背景を受け、日本国内の企業や不特定多数の個人を標的としたウェブサイト改ざんの被害軽減に貢献すべく、ウェブサイト改ざん対策製品を新たに自社開発いたしました。

そのコア技術には、2005年に発売を開始し、現在も多くの金融機関でご愛用いただいている自社開発のセキュリティ製品が保有する電子署名の技術が生かされています。

ウェブサイトを狙ったサイバー攻撃に対する防御強化の1つとして本製品を多くの企業様にご利用いただくことで、日本国内のセキュリティ強化の一助になればとの所存です。

◆システム構成◆

ウェブサイトを監視・復旧するためのソフトウェア「WA-Agent」と、WA-Agentの管理や各種設定、WA-Agent自体の稼働監視を行うための「WA-Manager」の2システム構成になります。



※「WA-Agent」を監視対象のウェブサーバに、「WA-Manager」を監視対象とは別のサーバに配置してご利用いただけます。

【補足】 WA-Manager と WA-Agent 間の通信は TLS 通信+TLS クライアント認証により保護されたセキュアな通信方式を使用しています。

◆動作環境◆

<稼働要件>

- ☆JAVA : Java Runtime Environment (JRE) 1.7.0_25 以降
- ☆CPU : Intel(R) Xeon(R) CPU E5-2650 0 @ 2.00GHz (1 core) 相当以上
- ☆MEM : 1.7GB 以上
- ☆HDD : 100MB(インストール用の空容量として)

<サポートプラットフォーム>

LinuxOS 搭載サーバに対応。各種クラウド環境でもご利用いただけます。

※詳しくはウェブサイトでご紹介しています。

◆料金体系◆

<ソフトウェア年間ライセンス>

- ・WA-Manager（管理用ソフトウェア）：48万円／年 ※複数 Agent の一元管理可能
- ・WA-Agent（監視・復旧ソフトウェア）：24万円／年 ※1ホストあたり
(ボリュームディスクカウントは別途ご相談ください。)

<サポート> ※年間ライセンスに含まれます。

- ・一般的な問い合わせに対する対応。(サポートサイト経由)
- ・障害発生時の、原因調査と調査結果の報告。
- ・バグ対応：バグ対応後、修正モジュールを提供。
- ・マイナーバージョンアップ対応：マイナーバージョンアップ時のモジュールを提供。
- ・セキュリティホール対応：対応モジュールを提供。
(ただし、JDK 及び、オープンソースソフトウェア部分は除く)

<初回設定・導入サポート等>

- ・別途ご相談内容に応じてご提案いたします。

デジタル・インフォメーション・テクノロジー株式会社について

デジタル・インフォメーション・テクノロジーは、業務系システム開発や組込み系システム開発、システム運用を得意とする独立系 SIer として 1982 年に創業。近年では、顧客起点をモットーとした IT サービスの商品化を進め、10 年前からはセキュリティ分野での自社製品開発・自社販売に参入。東京都中央区八丁堀に本社を構えるほか、西日本の窓口である大阪、愛媛、仙台、アメリカ合衆国に拠点を構え、IT サービス全般を広くご支援しています。

会社概要

【代表者】 代表取締役社長 市川 憲和 (イチカワ ノリカズ)

【資本金】 212 百万円

【住所】 東京都中央区八丁堀 4-5-4 ダヴィンチ桜橋ビル 3F

【TEL/FAX】 TEL 03-6311-6520 (代表) / FAX 03-6311-6521

【ウェブアルゴス 製品特設サイト URL】 <https://webargus-jp.ditproducts.com/>

【本社 URL】 <http://www.ditgroup.jp/>

<本件に関するお問い合わせ>

デジタル・インフォメーション・テクノロジー 商品開発部

飯嶋 範崇 (イイジマ ノリタカ) security-sol@ditgroup.jp

TEL 03-6311-6600 / FAX 03-6311-6521