トレンド

ネクスト・イット

書き換えられてはならない情報を「書き変えさせない」コンテンツ監視&自動復旧システム「WebALARM」

～通常のWebコンテンツの更新はWebALARMの監視を止めずに実行可能～

「Web改ざんを発見すると同時に、自動的に修復してほしい」、「改ざん発生時には、管理者に直ぐに通知してほしい」、「正規のWeb更新作業中に影響を受けたくない」といった要望に対応した『WebALARM』は、国内で官公庁を中心に300サイト以上の導入実績がある、コンテンツモニタリング＆不正改ざん自動リカバリシステムである。意図しないコンテンツの追加・変更・削除を検知すると直ぐに、そのバックアップデータから変更を修正し、メールまたはアラートで管理者等にその改ざんを連絡するなど、全ての静的なファイルを監視することができるセキュリティ製品である。

Webコンテンツを厳重に監視してサイトの即時回復を実行

Webサイトを守るために、既にファイアウォールやシステム監視を整備している企業は多いが、それでも、クッラカーはそれらの脆弱性をつき、攻撃を行ってくる。そして、何よりもその目的が、愉快犯から利益を求めた悪質な攻撃に変わっていくことが大きな脅威が生まれる時である。愉快犯のように、わざと痕跡を残すのではなく、利用者に気が付かれないように悪質なウイルスがWebサイトに仕込まれてしまったり、Webサイトが踏み台にされてしまうことで「被害者だったはずが加害者になっていた」ということもある。このような悩みに対応したのが、国内で官公庁を中心に300サイト以上の導入実績を持つコンテンツモニタリング＆不正改ざん自動リカバリシステム「WebALARM」である。

図1は、お客様からの要望に対して、WebALARMができることをまとめたものである。また、主な対象領域とメリットは次のとおりだ。

◆整合性と正確性：1日24時間365日の監視と自動回復により、データが常に正確で、知らない間に変更されていないことを保証。

◆ビジネスの継続性：インテリジェントなバックアップおよび即時データ回復により、データの欠落や改ざんによるダウンタイムを最小限に抑え、ビジネスの継続性を保証。

お客様のご要望

◆Web改ざんを『発見』するだけでは困る。
発見したからには自動的に修復してほしい。
◆改ざん発生時には管理者にはすぐに通知してほしい。
◆正規のWeb更新作業中に影響を受けたくない。
◆インストールや設定が簡単で、
後は全自動で動くシステムがいい。
◆Windows版、UNIX版の両方に対応してほしい。

WebALARMができること

◆Web改ざんをリアルタイムで発見し、自動的に修復。
修復はバックアップからの復旧や、「工事中」などの
代替ファイルで置き換える方法。
◆Web改ざん時にはメール、アラーム音などで即時通知。
◆Ver. 3.0からはUMAの導入により、『正規のWeb更新』
と『不正な改ざん』との区別がつけられるようになった。
◆WebALARMは、設定のほとんどが2クリックで可能。
◆WebALARMにはWindows版、UNIX版の両方がある。

図1　WebALARMができること

◆会社の信用：Webサイトが書き換えられて企業のイメージや信用が損なわれる心配が不要に。

◆法的な問題：Webサイトへの侵入によって引き起こされるWebコンテンツの書き換え、政治的な声明文、および商品価格の改ざんに起因する不要な法的争いを回避することが可能に。

◆安心感：連日夜遅くまでWebの書き換えやデータ破壊の対応に追われることから解消。信頼性が高く手間のかからない監視と回復が自信と安心感をもたらす。

◆低い運用コスト：自動的な監視と回復により、手動での検出リソースと回復プロセスが削減され、運用コストが低減される。

また、WebALARMは、情報セキュリティに対する具体的な実装を要求しているPCI DSS（Payment Card Industry Data Security Standard）にも準拠している。PCI DSSの準拠要件の一部として、整合性を保証し、規則違反を検出するために、ITシステムの重要なファイルを連続的に監視することが要求されている。WebALARMは、通常のファイル、ログファイル、およびシステムレジストリの監視に関する要件や、データ整合性の結果の報告に関する要件への準拠にも対応している。例えばWebALARMには、重要な業務システムが円滑に実行されるように、変更されたファイルや壊れたファイルを自動的に修復する追加機能が用意されている。

違反検出後は即時にアラートを発行

図2は、WebALARMの動作の仕組みを表したものである。また、各コンポーネントの概要は次のとおりである。

WebALARMエージェント（WAA）：Webサーバ上にインストールするコンポーネント。管理者のコンソールからのコントロールにより、改ざんの検知、管理者への通知、ログの生成、改ざんファイルの保存を行う。

WebALARM コンソール（WAC）：ファイアウォール内の管理者の端末にインストールするコンポーネント。コンソールからエージェントの各種設定を行う。

更新管理エージェント（UMA）：公開Webサーバのミラーサーバなど、通常ファイアウォール内に設置するコンテンツが収容されているサーバにインストールするコンポーネント。UMAが改ざんの監視を止めることなく、公開サーバへのPUTを行う。

更新管理コンソール（UMC）：上記UMAを管理するための管理者用モジュール。

以上のコンポーネントを目的に応じて活用することで、次のような機能が提供される。

【データ整合性の監視】

WebALARMはファイルとフォルダーを1日24時間連続的に監視し、監視対象データに対する変更を検出することができる。各ファイルをスキャンして、ファイルの存在、整合性、およびアクセス許可をチェックすることで、次のような規則違反を検出する。

- 監視対象ファイル／フォルダーが削除された
- 新しいファイル／フォルダーが監視対象フォルダーに追加された
- 監視対象ファイルの内容が変更された
- 監視対象ファイル／フォルダーのアクセス許可が変更された

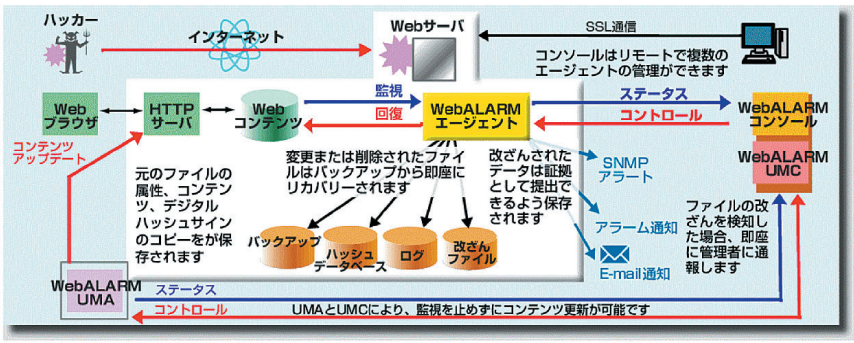

図2　WebALARMの動作の仕組み

トレンド

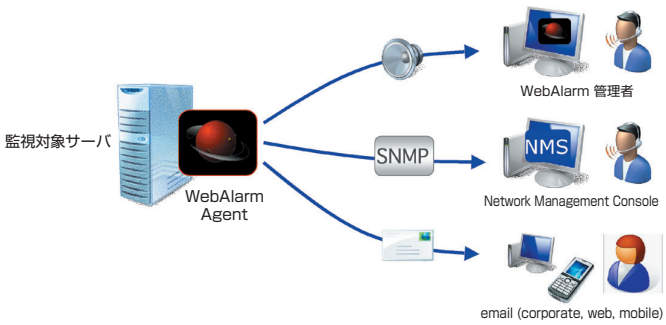

図３　WebALARMのアラート機能

図４　WebALARMのリカバリ機能

【データ違反アラート】

WebALARMは、データ整合性違反を検出するとアラートを発行する。発行されるアラートには、次のような種類がある（図３参照）。

・WebALARMコンソールアラート
・ネットワーク管理コンソールアラート（SNMP経由）
・電子メールアラート

【自動回復】

WebALARMは、データ整合性違反イベントを検出すると、自動的に即時対応する。WebALARMのこの組込み機能は、管理者による追加のスクリプトを必要としない。自動回復に関しては、次のオプションが用意されている。

・バックアップからのファイルコンテンツ全体の自動回復
・標準テンプレートファイルとの置き換えによる自動回復
・サードパーティプログラムまたはカスタムプログラム（専用の回復プログラムやウイルス対策プログラムなど）の自動起動

【監査ログと証拠保全】

WebALARMは、監視対象データの範囲内で発生したすべてのデータ違反イベントおよび更新イベントについて、完全な監査ログを記録する。ログに記録される情報として、次のような情報がある。また、改ざんされたデータを任意のディレクトリを指定し、保存することができる。

・イベントの日付と時刻
・イベントの種類
・違反ファイルの完全パス名

さらに、フォレンジック調査または分析に備えて、変更されたファイルコンテンツを隔離することもできる。

【データ更新管理】

WebALARMでは、一部のデータが更新されている最中も、運用を中断することなく連続的な監視が可能だ。WebALARMには、コンテンツ所有者が誤った警告を発生させずに監視対象データを更新できるように、２つの柔軟な方法が用意されている。

【更新時間枠の使用】

WebALARMコンソールを使用して、指定した一定時間の間WebALARMを“更新モード”に設定することができる。WebALARMは、この許可された期間中の新たな変更を学習する。“更新モード”への切り替えは、必要になった時点で随時行うことも、あらかじめスケジュールを設定しておくこともできる。

【更新管理エージェントの使用】

ステージングサーバやコンテンツ管理システムが稼働している展開環境では、WebALARMの更新管理エージェント（UMA）を使用した更新方法が最適だ。UMAをステージングサーバ上に配置し、許可された新たな変更をステージングサーバ上で検出したら、安全な方法でライブサーバのWebALARMエージェントに更新情報を配信する。ライブサーバは、UMAから配信される認証済みの更新のみを受け入れるので、時間枠を使用する場合のようなリスクがない。

●お問い合せ先●
ネクスト・イット㈱
TEL：03-5783-0702
URL：http://NextIT.jp/