CCS 株式会社 シーイーシーカスタマサービス

*Web*改ざん検知ソリューション

TRIPWIRE®
ENTERPRISE

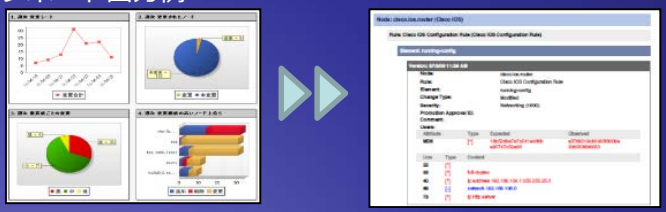
止められないWeb改ざん
不正な攻撃を即座に発見！

Tripwire Enterprise は
リアルタイム検知により、
不正な改ざんを発見、通知します！

変更検知例

不正な変更を即座に検知、メールで通知

レポート出力例



確認したいレポートを選択して、ドリルダウン

別途ステージングサーバ等を使用する事により、正規の変更か不正な変更かを判断させることが可能となります。
検知した内容は、メール、SNMPトラップ、コマンド発行等で通知することが可能です。
また、変更状況やポリシー対応状況を定期的にレポート出力する事も可能です。

*Web*改ざん検知を実現する*Tripwire Enterprise*

Web改ざん発生時の対応	Tripwire Enterpriseがサポートする内容
迅速な検知	
Web改ざんを迅速に検知し、対外的影響を最小限に抑える	リアルタイム検知、Hash関数による改ざん検知が可能です。
正しい状態のコンテンツと比較し、改ざんを発見 次第対処	ファイルの属性監視、改ざんの自動判別も可能です。
被害拡大を防ぐため、ネットワーク切断	コマンドの発行が可能です。 (ネットワーク切断のコマンド発行など)
詳細な被害状況の把握	
改ざんされたファイルを特定し、すべての変更点を発見する	ファイル単位で追加/削除/変更されたファイルを特定できます。
Webコンテンツ/Webサービスプログラム/設定 ファイル/OSファイルも含めた改ざん監視	ファイルの属性監視、改ざんの自動判別も可能です。
リカバリーするべきファイルリストの作成	属性/コンテンツの変更点を表示することが可能です。
悪意をもって追加/削除されたファイルの検知	正規の変更か否かを判別する事が可能です。 ※判別方法によっては、別途ステージングサーバが必要となる場合があります。
原因究明	
悪意のあるプログラムの設置の有無、改ざん実行犯などWeb改ざんの原因を究明すると同時に、証拠を自動収集し、証拠保全を行う	コマンド発行により、証拠収集を実現します。
侵入の形跡の収集	監査情報の取得を行います。
ファイル改ざん者の特定	いつ、誰が、何を改ざんしたのかをレポート出力することが可能です。 Web関連以外のファイルも改ざんも検知可能です。
対策	
セキュリティパッチの適用や、セキュリティ設定の修正などの対策 (最新のセキュリティパッチの確実な適用)	対応済みサーバと比較することで、確実なパッチ適用やセキュリティ設定が施されていることを証明します。
復旧	
追加された不正なファイルを削除、バックアップからリストアすることでWebサーバを正常な状態に復旧	追加されたファイルを特定します。
追加されたファイル、フォルダの発見、削除	追加、削除されたファイル一覧を表示します。
変更がかかったファイルのみリストア	外部リストアソフトウェアと連携することで自動リカバリを実現します。
バックアップデータの完全性の証明	バックアップ作業と同期してシステムの改ざん検知を行う事により、バックアップデータの完全性を証明します。
改ざん以前の状態に復旧されたことの証明	侵入前の状態をシステムレベルで比較することにより、確実な復旧を証明します。

監視対象のシステム要件に関しては、弊社までご連絡ください。

CCS 株式会社 シーイーシーカスタマサービス
営業部
〒150-0022 東京都渋谷区恵比寿南 1-5-5 JR恵比寿ビル 8F
TEL：03-5789-2443 FAX：03-5789-2575
URL：https://ceccs.site E-mail：ESECinfo@cec-ltd.co.jp