Webサイトの改ざんをいち早く お客様へお知らせするサービス

TSecured

Web サイト 改ざん検知

■セキュリティ

Webサイト セキュリティの課題

攻撃手法の高度化、巧妙化

- 新手の攻撃が次々登場し、対策が追い付かない
- WAFのみでは、WEBサイトの攻撃を100%防ぐことが困難

各社の対策レベルの不一致

- グループ会社や取引先で講じている対策のレベルが異なり、セキュリティ強度が保てない

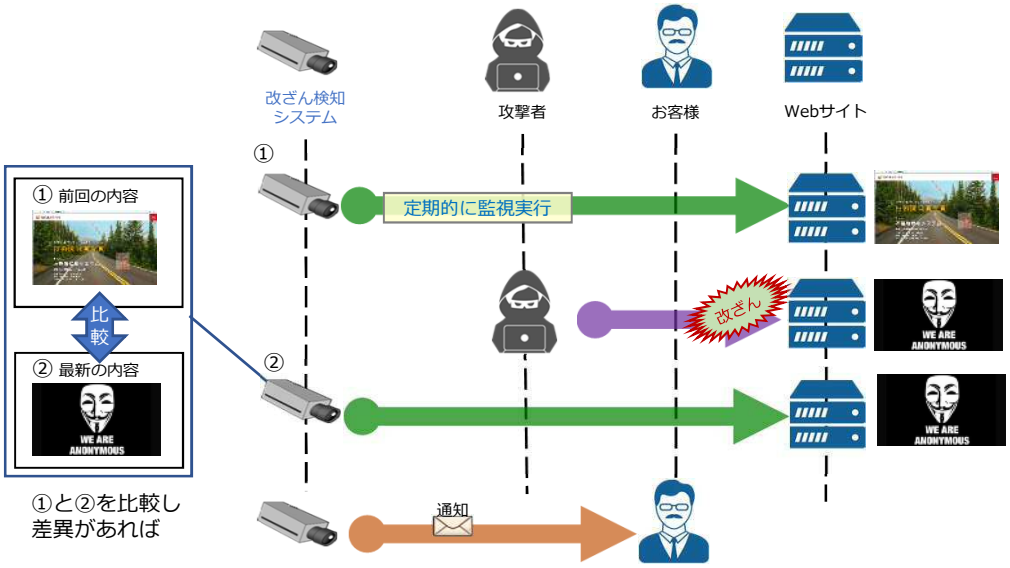
導入・運用の負担増加

- 自社で対象サイトの改ざんを見分けるのは困難
- 夜間などの監視体制を組むことが難しい

対応できる人材の不足

- セキュリティの専門知識を持つ人材がいない

Webサイト 改ざん検知サービスが解決します



導入が容易なクラウド型サービス 社外のWebサービスにも適用可能

エージェントレスで導入可能。Microsoft Azure やAmazon Web Services（AWS）などにも対応

オールトヨタセキュリティレベル準拠 各社の対策レベルを統一

「公開Webサイトの４施策」のトヨタグループ推奨対策サービス

TOYOTA SYSTEMS

導入までの流れ（標準スケジュール例）

提供サービス

標準	
改ざん監視	●改ざんを監視し、改ざん検知時にメールを送付します。（下段にサンプルを記載）
履歴管理	●過去の改ざん履歴などをログとして管理します。
ライセンス数管理	●Webサイトの更新などにより、監視ファイル数が契約ファイル数に到達した場合、お知らせいたします。必要に応じ、監視ファイル数の追加をご提案いたします。
運用オプション	
一次切り分け代行	●改ざん通知について、アナリストにて切り分けを行い、改ざんの可能性が高いと思われる内容のみ通知いたします。
WAF連携によるアクセス遮断	●一次切り分けの結果、改ざんと判定された場合はお客様のご申告に基づき、Webページへのアクセスを、弊社にて遮断いたします。（監視対象のWebサイトが弊社D.e-WAFⅡサービスをご利用している場合のみ対象）
設定変更＆チューニング	●お客様のご依頼に基づき設定値の変更や追加を実施いたします。過検知と判断されるアラートを抑制するための検知動作設定をご提案いたします。
月次レポート	●WebS@Tの監視状況を月次レポートとしてまとめ提供いたします。レポートは12営業日までに、テナント管理者様へメールにて提出いたします。

通知メールサンプル

株式会社XXXXXXXXXX 御中
以下の通り、改ざんと判定されたURLについてご報告申し上げます。

検知日時：2019/01/01 xx:xx:xx
マスタURL名：サンプルサイト
マスタURL：www.example.co.jp
対象URL：www.example.co.jp/test.html
判定理由：ブラックリストURLの検知
検知ブラックリストURL：ttp://www.blacklist.com

上記内容により、改ざんと判定いたしました。
内容について確認いただければと存じます。

月次レポートサンプル

■月別グラフ イメージ

検知仕様

改ざんとして判定されるケース(※)

- ●プロパガンダ的なコンテンツに差し替えられた場合
- ●サイトの構成・デザインが大幅に変えられた場合
- ●ハッカー集団のページに置き換えられた場合
- ●暴力的、反社会的な表現に変更された場合
- ●恣意的に外部サイトからマルウェアを仕向けるコンテンツに変更された場合

更新として判定されるケース

- ●コンテンツの内容変更およびコンテンツに含まれる文章内容の一部を変更した場合
- ●画像、バイナリ形式（例：フラッシュファイル、PDF、ドキュメントなど、）のファイルの内容が変更された場合

※何れもテキストのみが対象となります。
※すべての検知を保証するものではありません。

TOYOTA SYSTEMS

株式会社トヨタシステムズ　営業本部
TEL：050-3142-7889　Mail：helpdesk01@tns.toyotasystems.com
URL：https://www.toyotasystems.com

2019年第1版