GMO CLOUD

SiteLock 操作マニュアル

～エントリープラン向け～

XSS 脆弱性診断

SQL インジェクション脆弱性診断

アプリ診断

GMO クラウド株式会社

GMO CLOUD

目次

1. XSS（クロスサイトスクリプティング）とは？ 2

2. XSS 脆弱性診断（XSS SCAN）とは？ 2

3. SQL インジェクション（SQL INJECTION）とは？ 3

4. SQL インジェクション脆弱性診断（SQL INJECTION SCAN）とは？ 3

5. アプリ診断とは？ 3

5.1 アプリ診断とは？ 3

5.2 診断対象 4

5.3 診断対象 4

5.4 診断方法 4

6. 各種診断の脆弱性利用回数と事前準備 4

7. 各種診断の設定 5

8. 各種診断の再実施 6

GMO CLOUD

1. XSS（クロスサイトスクリプティング）とは？

XSS（クロスサイトスクリプティング）とは、脆弱性のあるWebサイトを踏み台（中継地）として、悪意のあるプログラムをそのサイトの訪問者に送り込む攻撃（ハッキング）手法です。

参考：独立行政法人 情報処理推進機構「クロスサイトスクリプティング」
https://www.ipa.go.jp/security/vuln/vuln_contents/xss.html

2. XSS 脆弱性診断（XSS SCAN）とは？

SiteLockはお客さまのWebサイトを対象に定期的な診断を実施し、セキュリティの脅威となるXSS脆弱性の有無を判定いたします。エントリープランでは、契約期間中に1回のみ利用できます。より多くの回数の診断を実施するには、上位プランへのアップグレードを推奨いたします。

脆弱性が検知されたプログラム／ソフトウエア等の調査・改修は、サービス／サポート対象範囲外です。プログラム／ソフトウエア開発者、提供元またはシステム会社等に改修をご依頼ください。インターネット上で無償配布されているプログラム／ソフトウエアをご利用の場合、最新バージョンにアップデートすることで問題解決できる場合もあります。配布元サイトをご確認ください。

診断対象	XSS脆弱性の有無について診断します。
診断範囲	診断対象のWebサイトを診断します。 ご契約プランにより、ページ数に上限があります。上限数に達した場合、それ以上の診断は行われません。
診断方法	SiteLockの診断サーバーが、インターネット経由で診断対象のWebサイトにアクセスします。そして、外部からXSSの手法で侵入をします。この手法では、サイト内の入力フィールド（例：お問い合わせフォームの氏名の入力欄）に向けてテスト送信を実施するものです。なお、当診断を実施する時に、お客さまのWebサイトには影響を与えないため、ご安心ください。
診断結果	診断結果は、URL単位で「脆弱性あり」と「脆弱性なし」のどちらかで判定されます。なお、診断結果は、コントロールパネル上で確認できます。 脆弱性が検知された場合、脆弱性のあるURLならびに入力フィールドに割り当てられたパラメータを診断結果として記録します。この情報は、プログラム改修時に役立ちます。
通知	脆弱性が検知された場合、お客さま宛てにメールにて通知します。また、コントロールパネル上のお知らせインボックスにも通知します。脆弱性なしと診断された場合、コントロールパネル上のお知らせインボックスに通知します。

3. SQL インジェクション（SQL INJECTION）とは？

SQL インジェクションとは、アプリの脆弱性を意図的に利用し、アプリが想定しない SQL 文を実行させることにより、データベースシステムを不正に操作する攻撃（ハッキング）方法を指します。

参考：独立行政法人 情報処理推進機構「SQL インジェクション」
https://www.ipa.go.jp/security/vuln/vuln_contents/sql.html

4. SQL インジェクション脆弱性診断（SQL INJECTION SCAN）とは？

SiteLock はお客さまの Web サイトを対象に定期的な診断を実施し、セキュリティの脅威となる SQL インジェクション脆弱性の有無を判定いたします。エントリープランでは、契約期間中に 1 回のみ利用できます。より多くの回数の診断を実施するには、上位プランへのアップグレードを推奨いたします。

脆弱性が検知されたプログラム／ソフトウエア等の調査・改修は、サービス／サポート対象範囲外です。プログラム／ソフトウエア開発者、提供元またはシステム会社等に改修をご依頼ください。インターネット上で無償配布されているプログラム／ソフトウエアをご利用の場合、最新バージョンにアップデートすることで問題解決できる場合もあります。配布元サイトをご確認ください。

診断対象	SQL インジェクション脆弱性の有無について診断します。
診断範囲	SQL インジェクション脆弱性診断は ANSI SQL に基づいて行われますので、すべての SQL データベースに適用されます。
診断方法	SiteLock の診断サーバーが、インターネット経由で診断対象の Web サイトにアクセスします。そして、外部から SQL インジェクションの手法で侵入をします。この手法では、サイト内の入力フィールド（例：お問い合わせフォームの氏名の入力欄）に向けてテスト送信を実施するものです。なお、当診断を実施する時に、お客さまのデータベースには影響を与えないため、ご安心ください。
診断結果	診断結果は、URL 単位で「脆弱性あり」と「脆弱性なし」のどちらかで判定されます。なお、診断結果は、コントロールパネル上で確認できます。
通知	脆弱性が検知された場合、お客さま宛てにメールにて通知します。また、コントロールパネル上のお知らせインボックスにも通知します。脆弱性なしと診断された場合、コントロールパネル上のお知らせインボックスに通知します。

5. アプリ診断とは？

5.1 アプリ診断とは？

WordPress 診断、アプリ＆ホームページ診断は、SiteLock のアプリ診断機能を用いて行います。アプリ診断では、お客さまの Web サイト内にあるアプリケーションを対象に定期的な診断を実施し、セキュリティの脅威となる脆弱性の有無を判定

いたします。エントリープランでは、契約期間中に１回のみ利用できます。より多くの回数の診断を実施するには、上位プランへのアップグレードを推奨いたします。

脆弱性が検知されたプログラム／ソフトウエア等の調査・改修は、サービス／サポート対象範囲外です。プログラム／ソフトウエア開発者、提供元またはシステム会社等に改修をご依頼ください。インターネット上で無償配布されているプログラム／ソフトウエアをご利用の場合、最新バージョンにアップデートすることで問題解決できる場合もあります。配布元サイトをご確認ください。

5.2 診断対象

アプリケーションに外部から侵入し、サーバーのセキュリティポリシーやプロトコル、PHP や Apache など現在実施中のサービスのバージョンに関する脆弱性の有無を確認します。

5.3 診断対象

診断対象の Web サイト内にある、OS、Web サーバー、データベース、プログラミング言語よりも上位のアプリケーションを診断します。自作を含め、以下のアプリケーションにも対応しています。

- WordPress
- Movable Type
- Drupal
- Joomla!
- PHP Nuke
- DotNet Nuke
- PHP BB
- vBulletin

5.4 診断方法

SiteLock の診断サーバーは、インターネット経由で診断対象の Web サイトにアクセスします。そして、自動クロールで Web サイトの情報収集を行います。SiteLock は、約 35,000 件（2016 年９月時点／随時更新中）の脆弱性データを格納する自社データベースと照合し、脆弱性の確認を行います。

6. 各種診断の脆弱性利用回数と事前準備

エントリープランでは、**契約期間中**、下記の診断を**１回だけ**利用できます。また、同時に実施する手配を行います。

① XSS 脆弱性診断

② SQL インジェクション脆弱性診断

③ アプリ診断（WordPress 脆弱性診断、ホームページ脆弱性診断）

※ 以降、上記３種の診断を「各種診断」と記述します。

各種診断を受ける環境を整えてから、診断を実施してください。

STEP1　事前準備のチェックリストをご確認ください。

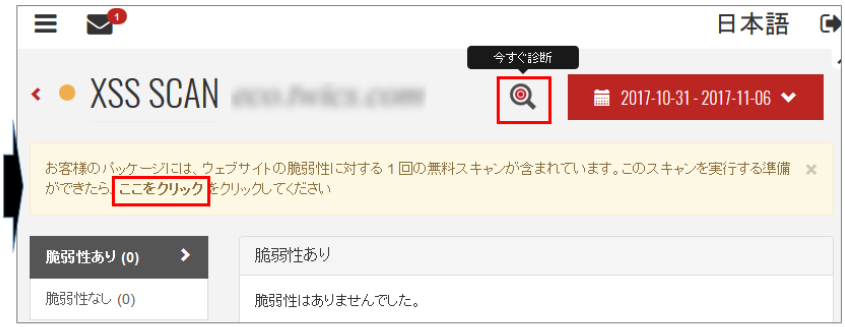
1	特定の国または日本国外からのアクセスを制限していない →　制限している場合、SiteLock 操作マニュアルの「事前準備」を参照してアクセス制限を一部解除します
2 3	脆弱性診断を受ける Web サイトは公開されている →　未公開であれば、診断前に Web サイトの公開を行います
4	SiteLock の**ドメイン認証**は終わっている →　SiteLock 操作マニュアルの「ドメイン認証の設定」を参照して、ドメイン認証を行います →　アプリ診断を実施する場合、ドメイン認証が必要です

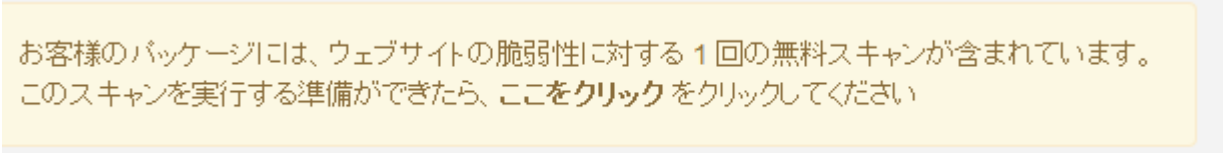
7. 各種診断の設定

各種診断のスキャンは、１回のみ行うことができます。

ダッシュボードの各スキャンにカーソルを合わせると、[今すぐ診断]のアイコンが表示されますので虫眼鏡マークをクリックします。

または、ダッシュボード上のアイコンをクリックし、診断画面右上にある虫眼鏡マークまたは[ここをクリック]をクリックしてもスキャンを行えます。





8. 各種診断の再実施

各種診断の結果、プログラムに脆弱性が見つかることがあります。脆弱性のあるプログラムに適切な修正を施した場合、再診断によって安全性の確認を行うことを推奨します。一度の修正ですべて解決できない場合、何度か修正を施す必要があります。修正の都度、再診断を必要とするケースもまれではありません。

エントリープランでは、契約期間中、各種診断を利用できるのは１回のみです。診断を再び実施するには、上位プランへのアップグレードを推奨いたします。上位プランでは、実施回数の制限はありません。各プランが定める実施頻度に応じて、定期的な診断を繰り返し実施できます。