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

プラットフォーム診断

GMO グローバルサイン・ホールディングス株式会社

GMO CLOUD

目次

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. プラットフォーム診断とは？

5.1 プラットフォーム診断とは？

※WordPress または Platform Scan (プラットフォーム診断)は WordPress と Joomla をご利用のサイトのみ対象のサービスです。（利用されていない場合、PLATFORM SCAN のタブは表示されません）

診断対象	アプリケーションに外部から侵入し、お客さまのサーバーで稼動する WordPress と Joomla を対象に定期的な脆弱性診断を行います。(現在は WordPress と Joomla のみ対応しています。)
診断範囲	WordPress と Joomla の本体、検出されたプラグイン、テーマとすべて含まれます。
診断方法	スパイダリング手法(※1)で外側から内側へ対象の Web サイトの情報収集を行い、SiteLock が認識している約 35,000 件（※2）の脆弱性データが格納されている専有データベースと比較し、脆弱性チェックを行います。
診断結果	「低」「中」「高」「重大」「緊急」に分類されます。 各脆弱性の詳細は診断日部分をクリックして確認できます。 重要度：「低」「中」「高」「重大」「緊急」 カテゴリー：検知した脆弱性のカテゴリー Summary：検知した脆弱性のサマリー 詳細：検知した脆弱性の説明 ※脆弱性は共通脆弱性評価システム CVSS （Common Vulnerability Scoring System)を基に評価・分類しされています。 ■参考情報： 英語：https://www.first.org/cvss/specification-document https://www.first.org/cvss/v3.1/specification-document 日本語：https://www.ipa.go.jp/security/vuln/CVSS.html 各レベルの脆弱性の詳細は「低」「中」「高」「重大」「緊急」に分類されています（※3）。 ※Platform SCAN (プラットフォーム診断)の脆弱性の詳細は英語のみとなりますこと、ご了承ください。 「高」「重大」「緊急」の脆弱性を検知した場合、ダッシュボートの VULNERABILITY SCAN が赤（X）になります。

※1 スパイダリング手法：SiteLock が管理している bot からお客さまのサイトに入って診断する手法

※2 2016 年 9 月 28 日現在の数値となり、SiteLock の脆弱性データベースは随時更新されます。

※3 Platform Scan (プラットフォーム診断)の診断結果例

GMO CLOUD

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　※以降、上記２種の診断を「各種診断」と記述します。

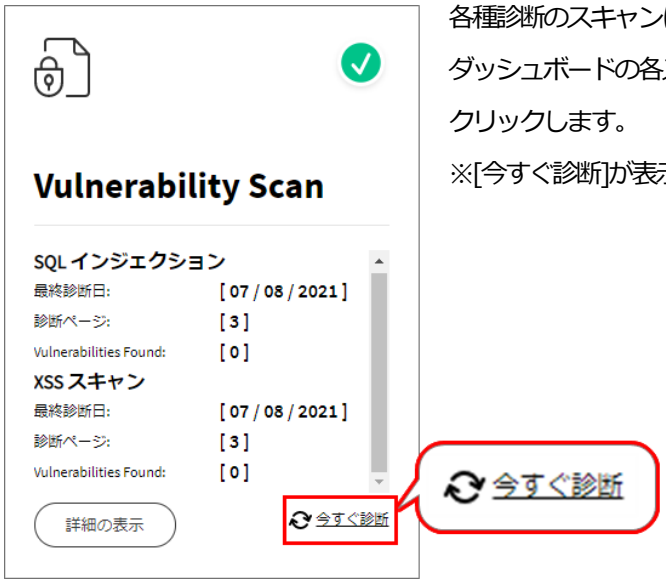
③ プラットフォーム診断　(Wordpress と Joomla をご利用のサイトのみ対象,診断頻度：毎日)

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　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

7. 各種診断の設定

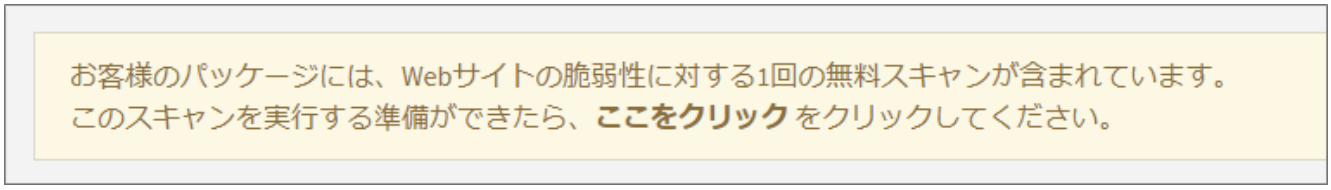


各種診断のスキャンは、１回のみ行うことができます。

ダッシュボードの各スキャン項目に [今すぐ診断]のアイコンが表示されますので、クリックします。

※[今すぐ診断]が表示されていない場合は設定を完了してください。

または、[詳細の表示]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。