GMO CLOUD

SiteLock 操作マニュアル

～ SQL インジェクション脆弱性診断 ～

GMO クラウド株式会社

GMO CLOUD

目次

1. SQL インジェクションとは？

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

2. 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。ご契約プランによって、選べる診断頻度は異なります。

脆弱性が検知されたプログラム／ソフトウェア等の調査・改修は、サービス／サポート対象範囲外です。プログラム／ソフトウェア開発者、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／ソフトウェアをご利用の場合、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。

3. SQL インジェクション脆弱性診断の事前準備

SQL インジェクション脆弱性診断を受ける上で正しい診断結果を得るため、事前に環境を整えてください。

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 → インターネット経由でアクセスできるよう、Web サイトの公開を行います

4. SQL インジェクション脆弱性診断の開始日

SiteLock をご契約後、お客さま専用のアカウントが発行されます。初回の SQL インジェクション脆弱性診断は、アカウント発行後から最大 24 時間以内に自動で実施されます（エントリープランを除く）。

5. SQL インジェクション脆弱性診断の実行頻度を設定

SiteLock のコントロールパネルにログインして、SQL インジェクション脆弱性診断の診断頻度を設定できます。

STEP1　図 1 のメニュー「設定」をクリックします。

図 1

STEP2　「スキャン設定」をクリックすると、図2が表示されます。

図2

STEP3　SQLインジェクション脆弱性診断の実行頻度を設定するには、[XSS Scan / SQL Injection Scan]の右にあるプルダウンから、お望みの実行頻度を選びます。なお、XSS脆弱性診断とSQLインジェクション脆弱性診断は、同じ実行頻度しか設定できません。

図3

選択可能な実行頻度は、ご契約プランによって異なります。また、診断の実行日時を指定することはできません。

四半期ごと	3カ月ごとに1回、診断します。
毎月	月に1回、診断します。
毎週	週に1回、診断します。
毎日	日に1回、診断します。

STEP4　選択後、[送信]ボタンをクリックします。これにて、設定終了です。

6. SQL インジェクション脆弱性診断の停止

SQL インジェクション脆弱性診断は、停止できません。ただし、実行頻度を「四半期」に設定することで、
契約期間中の診断回数を減らすことはできます。