

SiteLock 操作マニュアル

GMO デジロック株式会社

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. XSS 脆弱性診断の事前準備	3
4. XSS 脆弱性診断の開始日	3
5. XSS 脆弱性診断の実行頻度を設定	3
5. XSS 脆弱性診断の停止	4

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はお客様の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。ご契約プランによって、選択できる診断の実行頻度は異なります。

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	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、お客様の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並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、お客様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. XSS 脆弱性診断の事前準備

XSS 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
→ 未公開であれば、診断前に Web サイトの公開を行います |

4. XSS 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 XSS 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. XSS 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、XSS 脆弱性診断の診断頻度を設定できます。

STEP1 ダッシュボードから「設定」をクリックします。

The screenshot shows the SiteLock dashboard interface. On the left, there's a sidebar with several menu items: 'ダッシュボード' (Dashboard), 'ユーザー' (User), '設定' (Settings) which is highlighted with a red box, 'メッセージ' (Message), 'サポート' (Support), and 'ログアウト' (Logout). The main content area is titled 'ダッシュボード' and 'アカウントダッシュボードビュー'. Below the title, it says 'サイトセキュリティ'.

STEP2 「スキャン設定」をクリックすると、下図が表示されます。

The screenshot shows the 'Scan Settings' configuration page. On the left, there's a sidebar with '言語設定', '通知', 'スキャン設定' (Scan Settings) which is highlighted with a red box, 'ダウンロード設定', and 'SMART 設定'. The main content area is titled 'スキャン設定'. It contains a descriptive text about setting the execution frequency for vulnerability scans and two dropdown menus: one for 'Vulnerability Scan (XSS Scan, SQL Injection Scan, Malware Scan)' set to '毎月' (Monthly), and another for 'SMART' set to '毎日' (Daily). A blue '保存' (Save) button is at the bottom right.

STEP3 XSS 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、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。

スキャン設定

脆弱性診断の実行頻度を設定できます。Webサイトをテストして、ハッカーに悪用される可能性のある弱点を見つけます。SiteLockの重要な機能であるため、定期的に実行する必要があります。ただし、ご利用のホストが帯域幅や訪問数に制限を設けている場合は、実行頻度を下げることをお勧めします。

Vulnerability Scan (XSS Scan, SQL Injection Scan, Malware Scan)

SMART

毎月

四半期ごと

毎月

毎週

送信

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。

5. XSS 脆弱性診断の停止

XSS 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。