GMO CLOUD

SiteLock 操作マニュアル

～ XSS 脆弱性診断の読み方 ～

GMO クラウド株式会社

GMO CLOUD

目次

1. XSS 脆弱性診断のステータス確認

XSS 脆弱性診断（XSS SCAN）のステータスを確認するには、SiteLock のコントロールパネルにログインします。ログイン後に表示されるダッシュボード（図 1）のアイコンで、以下を確認できます。

- XSS 脆弱性診断が実施される前、または実施された後であるか
- XSS 脆弱性診断が実施された場合
  - 診断を合格したかどうか
  - XSS 脆弱性診断の最終合格日
  - XSS 脆弱性診断の最終診断日

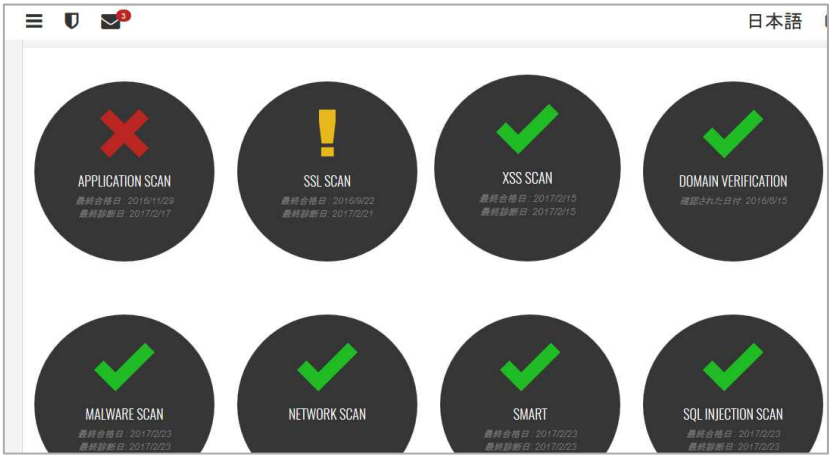

図 1

表示されるアイコンや情報には、それぞれ意味があります。

アイコン一覧		
		
● XSS 脆弱性診断は実施済み ● 最終合格日は、最後に診断を実施し、安全を確認できた日 ● 最終診断日は、最後に診断を実施した日 ● 安全を脅かす問題なし	● XSS 脆弱性診断の開始を待っている（エントリープランのみ） ● 安全を脅かす問題があるかどうかは、診断実行前なので不明（エントリープランのみ）	● XSS 脆弱性診断は実施済み ● 最終合格日は、最後に診断を実施し、安全を確認できた日 ● 最終診断日は、最後に診断を実施した日 ● **安全を脅かす問題あり**

2. XSS 脆弱性診断の診断結果

2.1 診断結果の閲覧

SiteLock のコントロールパネル上で、詳細な診断結果を閲覧できます。

STEP1 ダッシュボードの「XSS SCAN」のアイコン（図 2）をクリックします。表示されるアイコンは、アプリ診断のステータスに応じて異なります。

図 2

STEP2 アイコンをクリックすると、XSS 脆弱性診断の結果が表示されます。図 3 は、2017 年 2 月 16 日時点の診断結果を表示しています。診断結果は、XSS 脆弱性はなく、診断対象となった 550URL において安全が確認されたことを指しています。

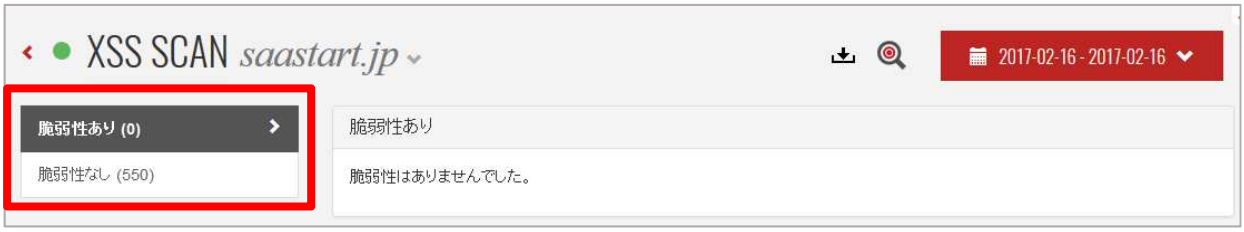

図 3

STEP3 ページ右上の日付表示されている箇所をクリックすると、図 4 のように任意の日または期間を指定して診断結果を表示できます。これにより、最大 90 日間まで遡って診断結果を確認できます。

図 4

STEP4 左メニューの「脆弱性なし」をクリックすると、下図のように診断を実施して「脆弱性なし」と確認できたURL一覧を表示できます。

図5

図6は、XSS脆弱性が検知された診断結果の事例です。診断結果です。脆弱性のあるURLとパラメータがそれぞれ表示されます。

図6

2.2 診断結果のエクスポート

診断結果をエクスポートするには、図7のようにコントロールパネルの右上にある  アイコンをクリックします。これにより、CSV形式のファイルとしてエクスポートできます。

図7

エクスポートの方法ですが、図8のように①Microsoft EXCELなど指定のプログラムで開く、または②お客さまのパソコン上にダウンロードしてファイルを保存するなど、2種類の方法から選べます。

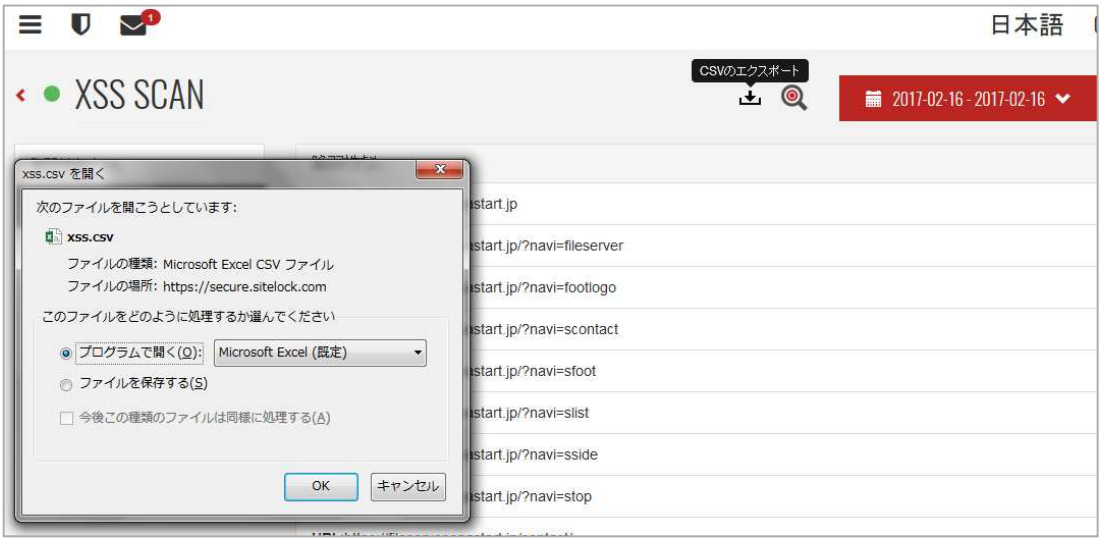

図8

3. 診断結果の通知

XSS 脆弱性を検知した場合、お客さま宛てにメールで通知します。また、図 9 のように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。脆弱性が見つからなかった、または「中・低」の脆弱性を検知した場合、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。

図9

4. 診断結果が不合格になる要因

XSS 脆弱性診断の結果、診断対象のドメイン配下に XSS 脆弱性が検知されると不合格になります。

5. XSS 脆弱性診断が保留中または未設定と表示される要因

XSS 脆弱性診断が保留中、または診断未設定と表示される主な要因は、以下のとおりです。

1. XSS 脆弱性診断を実施する設定を行っていない（エントリープランのみ）
2. XSS 脆弱性診断の初回診断が行われるのを待っている状態である
3. その他、XSS 脆弱性診断が開始されない問題が生じている