GMO CLOUD

SiteLock 操作マニュアル

～ アプリ診断の読み方 ～

GMO クラウド株式会社

GMO CLOUD

目次

1. アプリ診断のステータス確認

アプリ診断（APPLICATION 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。

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

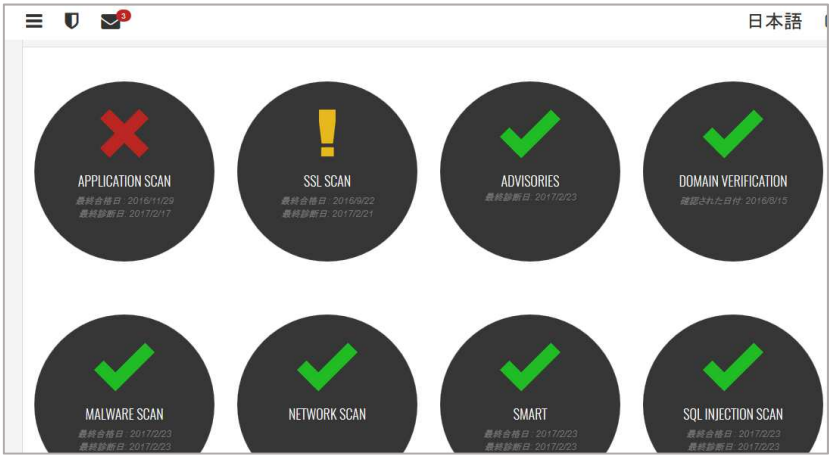
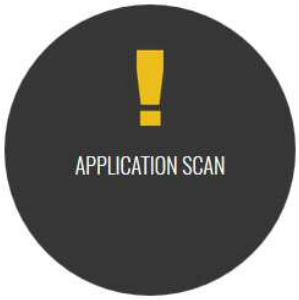


図 1

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		
		
● アプリ診断は実施済み ● 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、最後にアプリ診断を実施した日 ● 安全を脅かす問題なし	● ドメイン認証前のため、アプリ診断は未実施 ● ドメイン認証完了後、診断開始を待っている ● 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	● アプリ診断は実施済み ● 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、最後にアプリ診断を実施した日 ● **安全を脅かす問題あり**

2. アプリ診断の診断結果

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「APPLICATION 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。

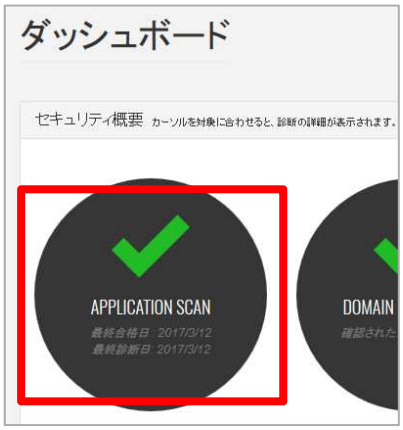


図２

STEP2 アイコンをクリックすると、図３のように直近に実施されたアプリ診断の履歴が表示されます。

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、過去に遡って診断結果を確認できます。

図４

STEP4　図５にある診断日をクリックします。または、１以上の検知個数を直接クリックして、優先度の高い脆弱性から閲覧できます。なお、検知個数が「0」の場合、脆弱性がなかったことを意味します。

図５

STEP5　診断日をクリックすると、見つかった脆弱性が一覧表示されます。脆弱性の評価に応じて分類されていますので、それぞれをクリックして詳細を確認できます。図６は、ブラインド SQL インジェクション脆弱性を見つけた事例です。

図６

2.2 脆弱性の分類

検知された**脆弱性の評価は、「高」「中」「低」に分類**されます。

複数の脆弱性が検知された場合、「高」に分類される脆弱性から順次にご確認、ご対応ください。

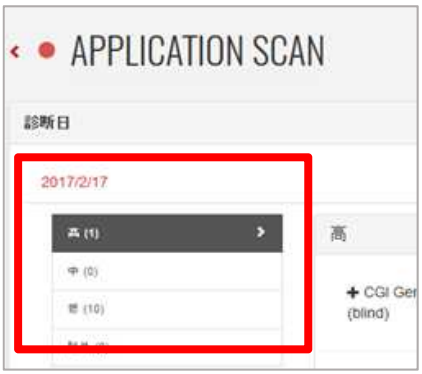


図７

「低」に分類された診断結果（図8）は、すべて脆弱性とは限りません。診断対象となったアプリケーションに関する注意喚起、情報共有に留まる場合もあります。情報共有の場合は、解決策に「n/a」（解決策なし）と表示されます（図9）。

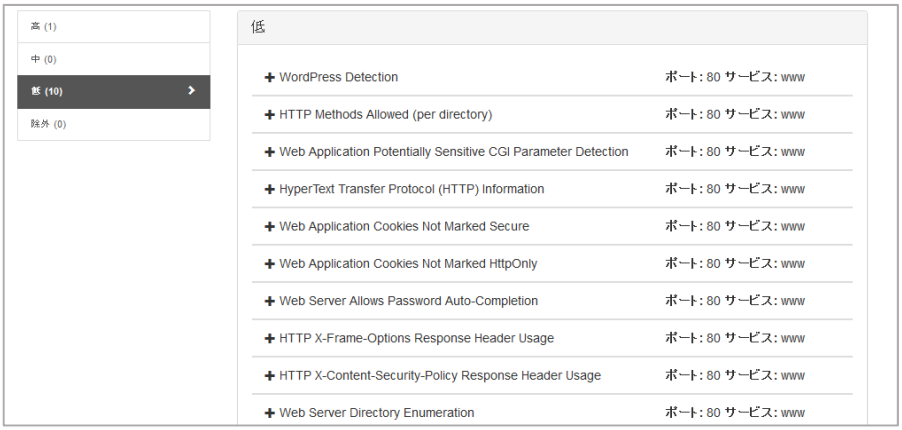


図8

図9では、診断対象のドメイン配下にバージョン4.7.2のWordPressが検知されたことを情報共有しています。情報共有なので、解決策は「n/a」とあります。これは、診断日（2017年2月17日）の時点で対策を行う必要がないことを示しています。将来的にバージョン4.7.2に脆弱性が見つかり、対策が必要だと判断されれば、アプリ診断の「高」または「中」など上位の評価として検知されることになります。

図9

2.3 診断結果の読み方

診断結果では、脆弱性とその影響を確認できます。脆弱性の詳細は、以下の4項目に分類されて表示されます。

概要・・・・・・検知した脆弱性

説明・・・・・・検知した脆弱性の詳細

解決策・・・・・検知した脆弱性の解決方法

技術的な詳細・・検知した脆弱性の技術的な説明

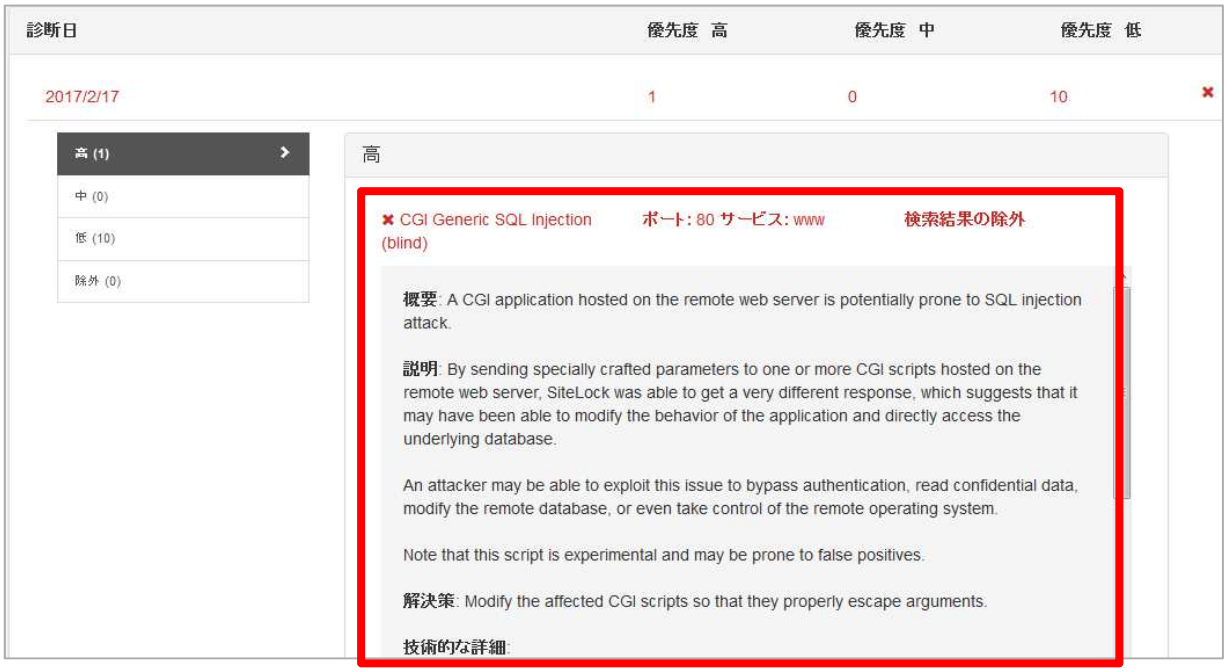


図 10

図 10 は、評価「高」に分類された脆弱性の詳細です。読み方ですが、「概要」では診断対象のドメイン配下の CGI プログラムにブラインド SQL インジェクション脆弱性が検知されたことを示しています。「説明」では、脆弱性の脅威を説明しています。「解決策」では、脆弱性の脅威を解決する方法を説明しています。

```
Using the GET HTTP method, SiteLock found that :

+ The following resources may be vulnerable to blind SQL injection :

+ The 'action' parameter of the /wp-login.php CGI :

/wp-login.php?redirect_to=http%3a%2f%2fchobimeg.me%2fwp-admin%2f&wp-subm
it=%e3%83%ad%e3%82%b0%e3%82%a4%e3%83%b3&testcookie=1&rememberme=forever&
log=&pwd=&reauth=1&action=lostpasswordzzhttp%3a%2f%2fchobimeg.me%2fwp-ad
min%2f&wp-submit=%e3%83%ad%e3%82%b0%e3%82%a4%e3%83%b3&testcookie=1&remem
berme=forever&log=&pwd=&reauth=1&action=lostpasswordyy

-------- output --------

        hamasitelocktest &lsaquo; ......................
```

図 11

また、図 11 は、「技術的な詳細」で表示される情報の一部です。問題のある箇所を指摘しています。プログラムを修正する際にお役立てください。

3. 診断結果の通知

「高」の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 12 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 12

4. 診断結果が不合格になる要因

アプリ診断の結果、不合格になる主な要因として考えられるのは、以下のとおりです。

1. 診断対象のドメイン配下に脆弱性が検知された
2. SiteLock がアプリ診断を実施しようと試みたが、何らかの原因で診断を正常に実施できなかった。そのため、安全性を確認できず、「合格」するまでには至っていない。よくある原因の幾つかは、下記のとおりです。詳細は、コントロールパネル上に表示されるエラーメッセージをご確認ください。
    - ① お客さまの Web サイトの Firewall が、SiteLock の診断サーバーをブロック
    - ② お客さま、または SiteLock 側のネットワーク遅延／障害など問題が生じていた
    - ③ お客さまの Web サーバーに障害など問題が生じていた
    - ④ SiteLock 側の診断サーバーに障害など問題が生じていた
    - ⑤ その他、診断を最後まで実施できない問題が生じていた

5. アプリ診断が保留中または未設定と表示される要因

アプリ診断が保留中、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. ドメイン認証が終わっていない
2. アプリ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、アプリ診断が開始されない問題が生じている