GMO CLOUD

SiteLock 操作マニュアル

GMO クラウド株式会社

GMO CLOUD

目次

1. コントロールパネルのアクセス方法と概要

1.1 ログイン

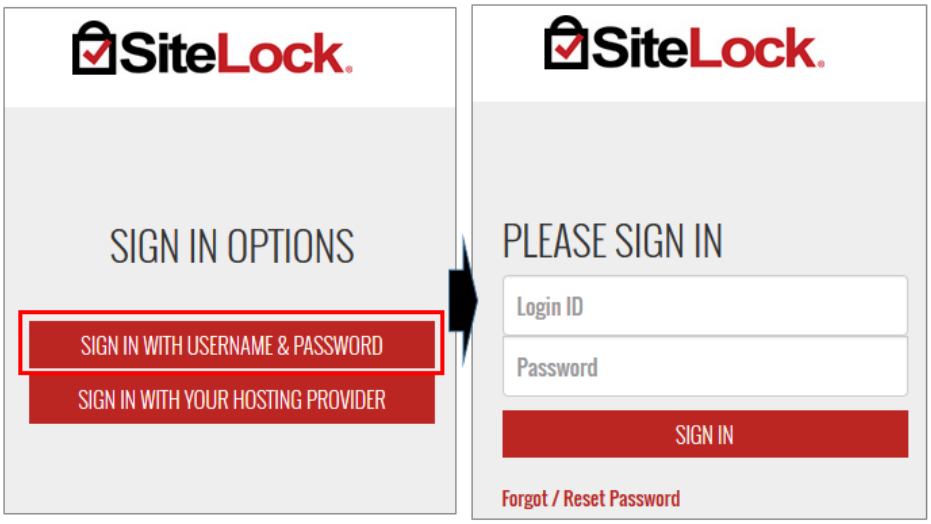
SiteLock のコントロールパネルにログインするためのログイン ID およびパスワードは、SiteLock サービスのお申し込み手続き完了後にご登録のメールアドレス宛にお送りする、設定完了のお知らせのメール内に記載されております。

メール件名は以下の通りです。

メール件名:　【GMO クラウド】SiteLock 設定完了のお知らせ

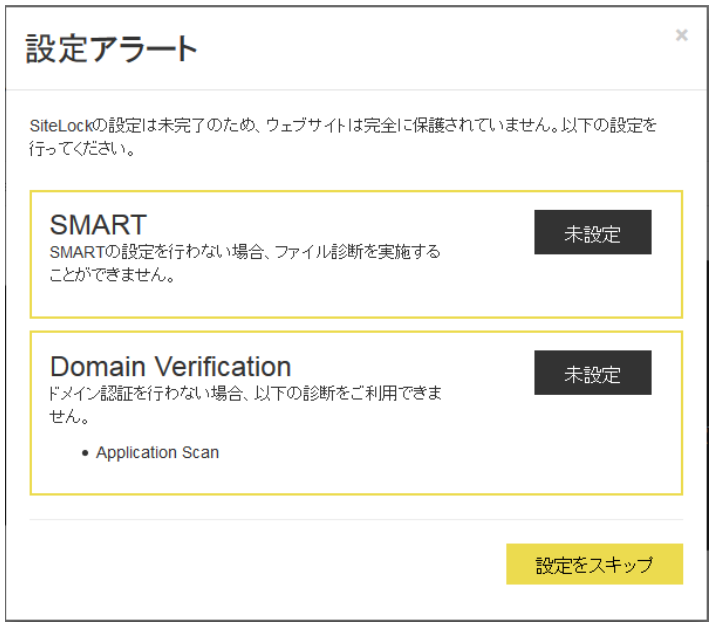
ログイン URL: https://secure.sitelock.com/login

[SIGN IN WITH USERNAME & PASSWORD]をクリックし、ログイン ID とパスワードを入力し[SIGN IN]をクリックします。



※ドメイン認証と SMART 設定が完了していない場合、ログイン後に下記の画面が表示されます。

すぐに設定される場合にはそれぞれの **[未設定]** ボタンをクリックすると、2.1 SMART WIZARD (SMART 設定) および 3. ドメイン認証の設定の設定画面に進みます。



1.2. コントロールパネルの概要

SiteLock のコントロールパネルの各セクションのご案内は、以下の通りです。

1	**SiteLock のロゴ**	トップページに戻ることができます。
2	**メニューの切り替え**	左側のメニューを表示/非表示することができます。
3	**警告**	「SMART WIZARD」と「ドメイン認証」の設定が未完了の場合に表示されます。 ※設定完了後にも表示が消えるまでお時間がかかる場合がございます。
4	**安全シール**	安全シールの設定画面に進みます。
5	**メールボックス**	SiteLock のメールボックスにて、各種診断の結果を確認できます。
6	**言語選択**	コントロールパネルとアラートの言語を変更することができます。 ※日本語以外はサポート対象外となります。
7	**ログアウト**	コントロールパネルからログアウトできます。

1	**ダッシュボード**	トップページに戻ることができます。
2	**ユーザー**	アクセスできるユーザーを登録できます。最大限２０ユーザーまでに追加できます。
3	**設定**	診断設定、ダウンロード設定、SMART 設定の画面に進みます。
4	**サポートへのお問い合わせ**	お問い合わせフォームが表示されます。

セキュリティの状況は、項目ごとにマウスをアイコンの上に置くと各診断の詳細が現れます。

緑	問題がありません。
黄	保留中あるいは未設定の状態です。
赤	診断に関するエラーが発生、またはマルウェア、脆弱性などを検知した状態です。

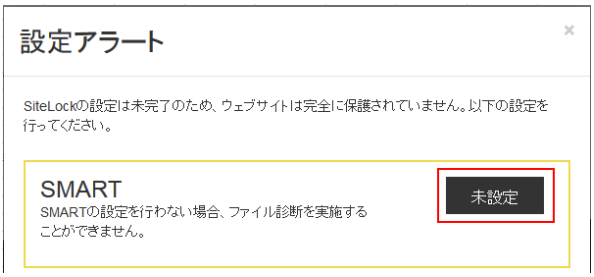
2. 設定メニュー

SiteLock の各設定についてご案内します。

2.1 SMART WIZARD (SMART 設定)

SMART（SMART 診断）を利用するための設定です。登録サイトの診断をする際に利用する FTP 接続設定をします。

STEP1　警告文章の SMART 欄の[未設定]ボタン、または[！]アイコンをクリックし、[ここ]の文字部分をクリックします。



※設定後に変更する場合は、[設定]から[SMART 設定]画面に進み、[ウィザード]をクリックすると画面が表示されます。

STEP2　対象ドメイン名の FTP アカウントを入力して[テスト接続]ボタンをクリックします。

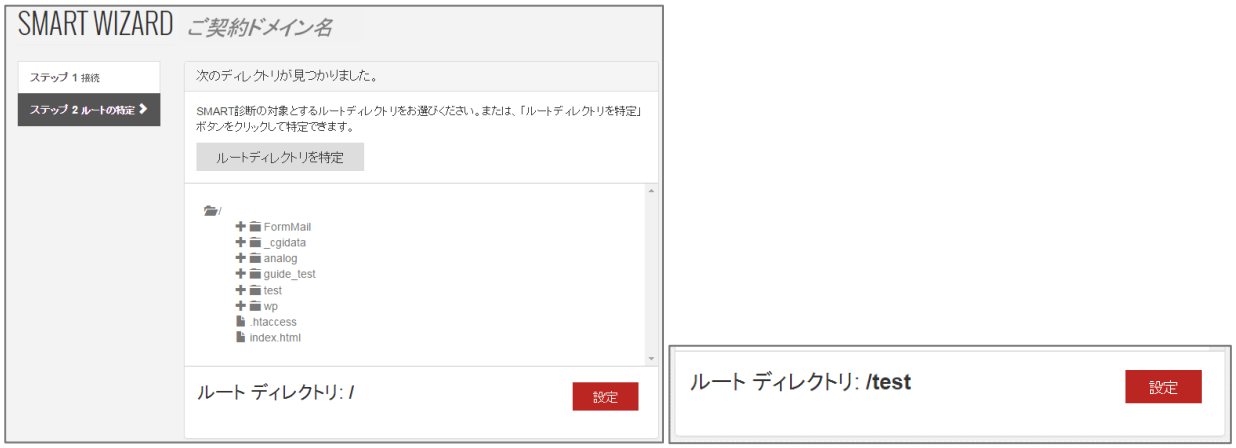
ファイル転送方法	FTP、SFTP、FTPS　から選択します。
FTP ホストアドレス	FTP 接続のための、FTP サーバー名または FTP サーバーの IP アドレスを入力します。
(S)FTP ポート番号	ファイル転送設定で選択した転送方法のポート番号を入力します。
ユーザー名	FTP アカウントを入力します。
パスワード	FTP アカウントのパスワードを入力します。

STEP3　接続が完了すると、ディレクトリーの指定に進みます。

診断するディレクトリーを指定して、[設定]ボタンをクリックします。

※サーバー側で接続元 IP アドレスによるアクセス制限を設けているお客さまは、公式サイトの「よくある質問」をご確認ください。SiteLock からの接続を許可いただく必要があります。

※ディレクトリーを指定した場合は、次のページにある右側の図のように表示されます。



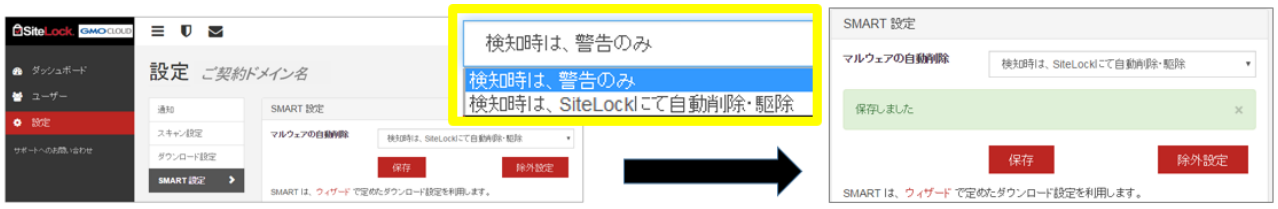
続いて SMART の設定画面に進みます。

STEP1　[SMART 設定]ボタンをクリックします。

STEP2　マルウェアを検知した際の動作をプルダウンから選択して、[保存]ボタンをクリックします。

※検知された場合でも削除されたくないファイルがある場合には、「検知時は、警告のみ」をご選択ください。

保存が完了すると、右図の画面が表示されます。



■スキャンの対象から外したいディレクトリーやファイルがある場合

STEP1　除外したいディレクトリーやファイル(拡張子)がある場合には、[除外の管理]ボタンをクリックして設定します。

STEP2　除外したいディレクトリーをクリックし[更新]ボタンをクリックすると、[保存された除外]欄に表示されます。

※対象ディレクトリーを間違えてクリックした場合、再度クリックすると対象から外すことができます。

※除外していたディレクトリーをスキャン対象に戻す場合、[保存された除外]の対象ディレクトリーをクリックし、[更新]ボタンをクリックします。

[種類とサイズでファイルを除外]の欄では、ファイルの種類やファイルサイズで除外を選択することができます。

対象の拡張子、またはファイルサイズを選択して[Update]ボタンをクリックします。

2.2 通知設定

SiteLock からのセキュリティに関する通知メールの受信設定の変更が行えます。（初期設定では、登録時に設定した管理者のメールアドレスが登録されています。）

セキュリティアラートの受信（ON/OFF）	アラートメールを受信する（ON）、受信しない（OFF）を選択できます。
メール	アラートメールを受信するメールアドレスを変更できます。

情報を変更後、[保存]ボタンをクリックして完了です。

2.3 スキャン設定

診断の頻度を設定し、[送信]ボタンをクリックします。

※ご利用プランにより、実行頻度の選択肢は異なります。

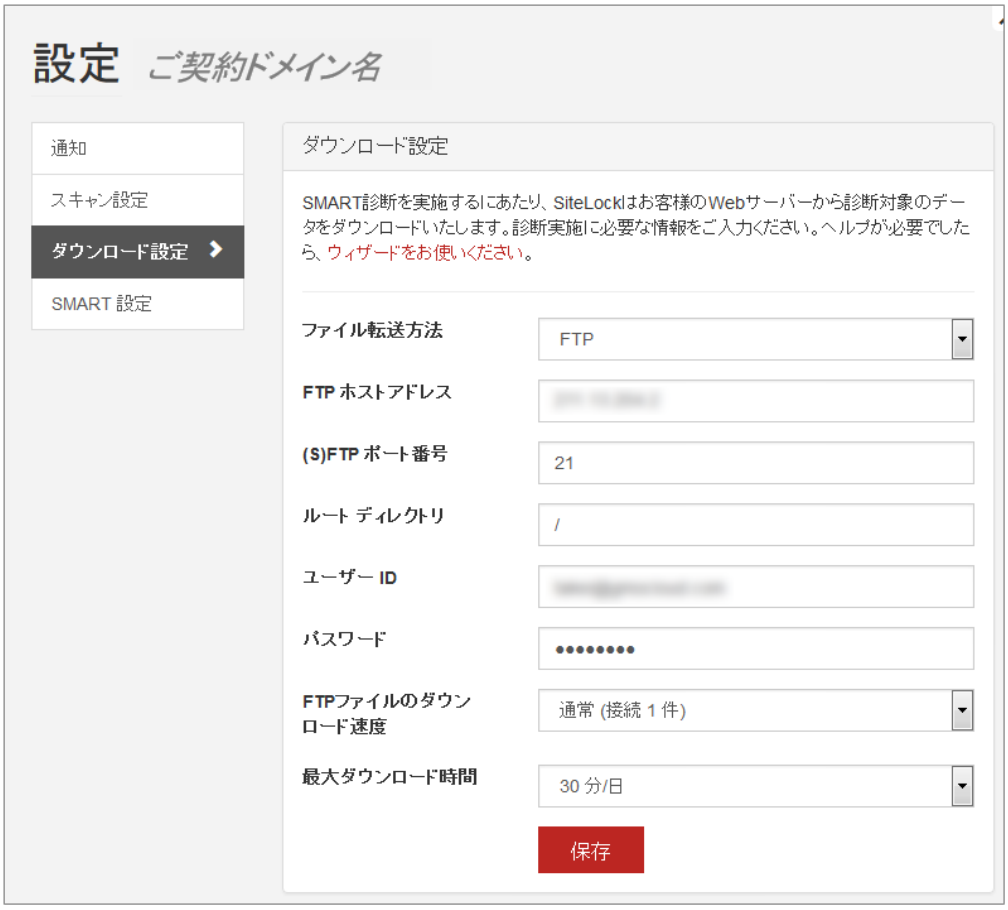
※3. ドメイン認証の設定が完了していない場合、下記の表示となっているため、先にドメイン認証を行ってください。

※ドメイン認証の設定が完了してからも、表示が消えるまで、緒時間がかかる場合がございます。

2.4 ダウンロード設定

2.1 SMART WIZARD で設定したFTP接続設定の変更を行います。

設定変更後、[保存]ボタンをクリックすると変更内容が反映されます。



ファイル転送方法	FTP、SFTP、FTPS　から選択します。
FTPホストアドレス	FTP接続のための、FTPサーバー名またはFTPサーバーのIPアドレスを入力します。
(S)FTPポート番号	ファイル転送設定で選択した転送方法のポート番号を入力します。
ルートディレクトリ	診断を行う最上位のディレクトリを指定します。
ユーザー名	FTPアカウントを入力します。
パスワード	FTPアカウントのパスワードを入力します。
FTPファイルダウンロードの速度を選択してください。	通常（接続1件）、より高速（2件同時接続）、最速（3件同時接続）から選択できます。 ※ご利用サーバーのFTP接続の同時接続数によりご変更ください。
最大ダウンロード時間	30分、60分、90分、120分・/日　が選択できますが、初期値　**30分/日**　を推奨します。

GMO CLOUD

3. ドメイン認証の設定

APPLICATION SCAN（アプリ診断）を利用するには、DOMAIN VERIFICATION（ドメイン認証）を行う必要があります。

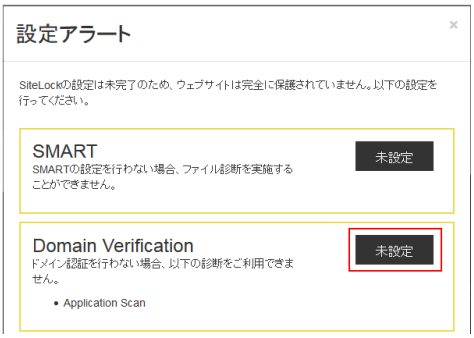
※　アプリ診断以外の診断を利用する場合は、ドメイン認証は必要ではありません。

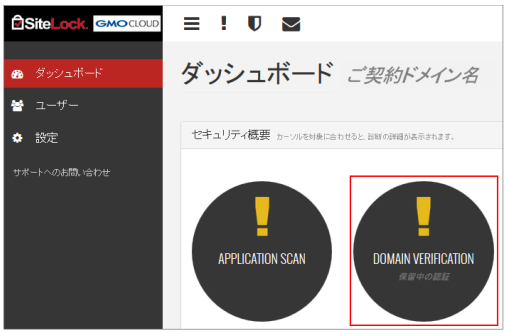
なお、ドメイン認証の設定手順はドメイン認証１またはドメイン認証２の**いずれかの手順**で設定を行ってください。

認証方法１	SiteLock 指定の認証用 META タグをお客さまサイトの中に埋め込み設定を行います。
認証方法２	SiteLock 指定の html ファイルをダウンロードし、診断対象とする登録ドメインのルートディレクトリ配下にアップロードします。

3.1 認証方法１

STEP1　設定アラートの Domain Verification 欄の[未設定]ボタン、またはダッシュボードの [DOMAIN VERIFICATION] アイコンをクリックします。





STEP2　META タグをコピーして、診断対象となる登録サイト内の<head>と</head>の中に挿入します。

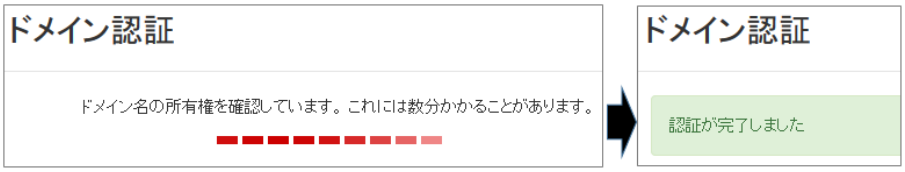
※下記の画像はサイト内の記述の一例です。

```
1 <head>↓
2 ↓
3 </head>↓
4 <body bgcolor="#FFE4E1">↓
5 ***** SiteLockテスト用indexページです。*****<br>
6 <img alt="Image" src="./photo.jpg" /><br>↓
7 ↓
8 </body>↓
```

<head>の下から</head>の上の間に META タグを貼り付けます。

STEP3　サイト内への埋め込みが完了したら、[確認]ボタンをクリックします。

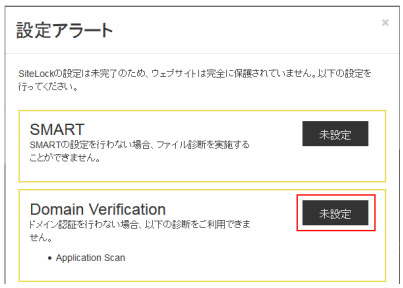
STEP4　ドメインの確認完了まで数分かかる場合があります。[認証が完了しました。] と表示されたら完了です。

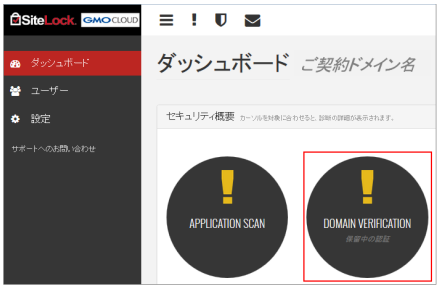


ダッシュボードの [DOMAIN VERIFICATION] のアイコンが緑色の表示になります。

3.2　認証方法２

STEP1　設定アラートの Domain Verification 欄の[未設定]ボタン、またはダッシュボードの [DOMAIN VERIFICATION] アイコンをクリックします。

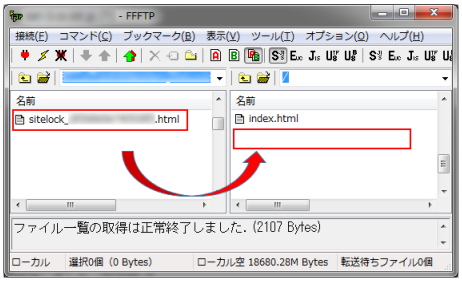




STEP2　[認証方法 2]をクリックし、説明文内の[ここをクリック]の赤文字部分、または[ダウンロード]ボタンをクリックして、対象ファイル（.html のファイル）をいったんお手元の PC に保存します。

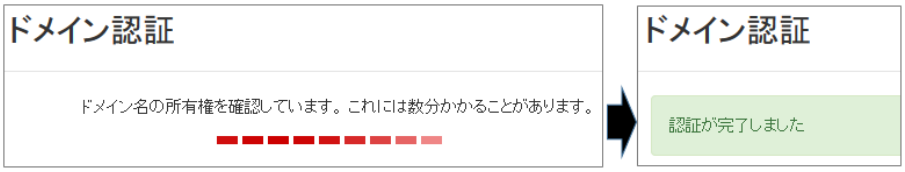
STEP3　FTP ソフトを用いてダウンロードしたファイルを、診断対象となる登録ドメインのルートディレクトリ配下にアップロードします。

※FTP ソフトの設定につきましては、ご利用サーバーのマニュアル等にてご確認ください。



STEP4　アップロードが完了したら、STEP2 の画面に戻って[確認]ボタンをクリックします。

STEP5　ドメインの確認完了まで数分かかる場合があります。[認証が完了しました。] と表示されたら完了です。



ダッシュボードの [DOMAIN VERIFICATION] のアイコンが緑色の表示になります。

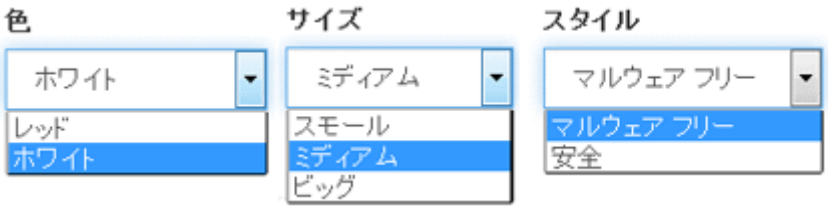
4. 安全シールの設定

一定時間ごとに SiteLock による診断を実施し、Web サイト内の脆弱性あるいはマルウェア感染の危険性がないことを確認できた時のみ、安全シールが表示されます。安全シールには各種診断の最終診断日が表示されます。
安全シールをクリックすると、対象となる Web サイトの情報および最新の診断結果ページが表示されます。

なお、マルウェアあるいは脆弱性を検知した時は、サイト管理者にリアルタイムで通知を行います。
対象のウェブサイトでマルウェアあるいは脆弱性に発見された場合、72 時間以内に対象のウェブサイトで問題を解決できないと安全シールは自動的に表示されなくなります。安全シールが表示されない場合、その他の画像は透けて表示されます。リンク切れの画像は表示されません。
Web サイトの復旧が完了し、再度安全性が確認されたら、安全シールは再び表示されるようになります。

STEP1　左上のダッシュボードに盾のアイコンをクリックし、シールに表示する言語を選択して[次へ]をクリックします。

STEP2　シールの色、サイズ、スタイルを選択するとプレビューに選択したものが表示されますので、確認して[次へ]をクリックします。



STEP3　安全シールを表示させる場所を選択し、②で表示されたコード部分をコピーして対象のサイトに貼り付けます。

※安全シールの位置によって埋め込むタグの場所が異なるため、ご注意ください。

表示エリア	安全シールの表示場所	コードを埋め込む場所
手動	ご希望場所	ご希望場所部分
左下部	サイトの左側の下部	</body>タグの上
中央下部	サイトの中央の下部	
右下部	サイトの右側の下部	

サイト内への追記が完了してから、[構成設定を保存]をクリックします。

STEP4　安全シールを設定したサイトに表示されているかをご確認ください。

※[構成設定を保存]ボタンをクリック後、反映されるまでお時間を要する場合もございます。

　安全シールが表示されない場合には、少しお時間を置いてから再度お試しください。

参考：**右下部に設定した場合**、下の画像のような位置に配置されます。


テストサイト
SiteLockテストサイト
GMO CLOUD
VERI-4.CS.IDD.JP
SiteLock.
安全
合格
2016-09-06

5. スキャン機能性について

5.1 診断のルールについて

SMART 診断以外の、リモートによる各種診断は、SiteLock のご契約時に登録されたドメイン（例：example.com）のサイト自体、またサイトからリンクされているサブドメイン（例：contact.example.com）を対象として診断を実施します。ただし、診断を実施する範囲は、ご契約プランの定めるページ数（ユニークの URL 数）の上限までとなります。
たとえば、example.com を登録している場合、以下のページに診断を行います。

・登録ドメイン（example.com）からリンクされている同一ドメイン（example.com）内のページ
・登録ドメイン（example.com）からリンクされているサブドメイン（sub.example.com）内のページ

登録ドメインから外部ドメイン（例：another-example.com）へリンクが設けられている際は、アクセス時にセキュリティの脅威があるか、ないか判別するのみとなります。この際、１ページ（URL）とはカウントされません。

[初回診断時]
初回診断時は、起点となる最初のページの構文解析を行い、次のリンク先のページに診断対象を移します。登録ドメイン、そのディレクトリ配下のページを優先し、次にリンクされたサブドメインの順となります。

[2 回目以降]
診断対象となるページは、登録ドメインのサイトにある内部リンクに下記のアルゴリズムを適用することによって決定されます。

[優先順位]
1. 直近の診断で問題が検出されたページ
2. ページからリンクされているページ
3. 過去の診断で診断頻度の高いページ
4. 引数がすべて消去されたページ（訪問回数）
   例）引数なしのページを優先 引数付き
   http://www.example.com/index.html?id=top ※引数は「?id=top」
   引数なし（こちらが優先されます）
   http://www.example.com/index.html
5. 上位階層の「/」の少ないページ
   例）上位階層のページを優先
   下層ページ（「/」は４個）　http://www.example.com/sales/product/price/index.html
   上位階層のページ（「/」は２個）を優先　http://www.example.com/sales/index.html

5.2 APPLICATION SCAN (アプリ診断)

診断対象	アプリケーションに外部から侵入し、サーバーのセキュリティポリシーやプロトコル、現在実行中のサービスのバージョン（PHP、Apache など）の脆弱性の有無について確認します。
診断範囲	OS、Web サーバー、データベース、プログラミング言語よりも上位のアプリケーションを診断します。 アプリケーションには以下のようなものが含まれます。 ・WordPress ・Drupal ・Joomla! ・PHP Nuke ・DotNet Nuke ・PHP BB ・vBulletin
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	「高・中・低」優先度の脆弱性に分類します。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。 各レベルの脆弱性の詳細は「概要・説明・解決策・技術的な詳細」に分類されています（※3）。 概要：検知した要点 説明：検知した要点の詳細 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 ※「低　優先度」の結果はすべて脆弱性ではなく、アプリケーションに関する情報共有もあります。 例）HTTP configuration (HTTP 設定) なお、情報共有の場合、「解決策: n/a 」(解決策なし)という結果になります。 ※APPLICATION SCAN（アプリ診断）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」の脆弱性を検知した場合、お客さま宛にメールにて通知し、管理画面上のお知らせインボックスにも通知します。 「中・低」の脆弱性を検知した場合、スキャンの結果を管理画面上のお知らせインボックスに通知します。

※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 APPLICATION SCAN (アプリ診断)の診断結果例

5.3 XSS SCAN（XSS 脆弱性診断）

診断対象	クロスサイトスクリプティング脆弱性の有無について確認します。
診断範囲	全ページ（設定したルートディレクトリ配下）を診断します。 ※ご契約プランにより、ページ数に上限がある場合もございます。
診断方法	サイトに外部からクロスサイトスクリプティングの手法(※1)で侵入します。 なお、クロスサイトスクリプティングの手法を実施する時に、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	診断の結果を、「**脆弱性あり**」と「**脆弱性なし**」URL に分類します。 「脆弱性あり」の URL を検知した場合、お客さま宛にメールにて通知し、管理画面上のお知らせインボックスにも通知します。 ※ XSS SCAN（XSS 脆弱性診断）は、脆弱性の解決策の提供は行いません。 「脆弱性なし」の場合には、スキャンの結果を管理画面上のお知らせインボックスに通知します。

※1 クロスサイトスクリプティング手法：サイト内の入力フィールドに向けてテスト送信を実施します

5.4 SQL INJECTION（SQL インジェクション脆弱性診断）

診断対象	SQL インジェクション脆弱性の有無について確認します。
診断範囲	SQL インジェクション脆弱性診断は ANSI SQL に基づいて行いますので、すべての SQL データベースに適用されます。
診断方法	サイトに外部から SQL INJECTION の手法(※1)で侵入します。SQL インジェクション脆弱性を検知する場合、対象のデータベースにレコードが残ります(※2)。 対象のレコードの値は繰り返すため、容易に認識できます。 ※ SQL インジェクションの手法を実施する時に、お客さまのデータベースに影響を与えないため、ご安心ください。

診断結果	診断の結果を、「**脆弱性あり**」と「**脆弱性なし**」URL に分類します。 「脆弱性あり」の URL を検知した場合、お客さま宛にメールにて通知し、管理画面上のお知らせインボックスにも通知します。 ※ SQL INJECTION（SQL 脆弱性診断）は、脆弱性の解決策の提供は行いません。 「脆弱性なし」の場合には、スキャンの結果を管理画面上のお知らせインボックスに通知します。

※1 SQL INJECTION 手法：サイト内の入力フィールドに向けてテスト送信を実施します

※2 診断の際に、1111 や 2222 などの単純な数字の羅列のレコードが残ります。

5.5 ADVISORIES（アドバイザリー）

診断対象	サイト上の疑わしいコードとファイルを確認し、パスワード入力ページへの SSL 暗号化の適用や第三者製のアプリケーションのアップグレードなど、使用上の注意事項やアドバイスを提供します。 疑わしいコード/ファイルは難読化（暗号化）が実施されるコード/ファイルです。 このスキャンは暗号化を解除し、マルウェアファイルが頻繁に採用するパターンについて検知します。 例：外部リソースに接続し、ファイルシステムやオペレーティングシステムなどとやり取りするかどうかをチェックします。
診断範囲	全ページ（設定したルートディレクトリ配下）を診断します。 ※ご契約プランにより、ページ数に上限がある場合もございます。
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 が認識している疑わしいコードとファイル種類が格納されている専有データベースと比較し、チェックを行います。
診断結果	優先度により、「高・中・低」に分類します。 各レベルのアドバイスの詳細は「ページの URL・概要・説明・アクション」に分類されています。 「ページの URL」は対象のウェブサイトページの URL です。 概要：検知した要点 説明：検知した要点の詳細 アクション：検知した要点の対策の提供 **「高」**を検知した場合、お客さま宛にメールにて通知し、管理画面上のお知らせインボックスにも通知します。 **「中・低」**を検知した場合、スキャンの結果を管理画面上のお知らせインボックスに通知します。 リスクスコアは、脆弱性とマルウェアの発見に関係なく、全体的なセキュリティ問題が発生する可能性を評価します。 SiteLock は、約 200（内部）の項目に基づきのウェブサイトのリスクスコアを評価します。 評価する項目は以下の通りです。 ・人気度：Facebook の「いいね」数/Twitter のフォロワー数など

	・ウェブサイト ビルダー：WordPress plugin 数など ・複雑度 ：ページのスピード、動的 vs 静的なコンテンツなど ※計算方法の一例： ①Twitter のフォロワー数が多いほどセキュリティ問題が発生する場合、影響が高くなるため、人気度のパーセンテージが高くなり、全体のリスクスコアも高めます。 ②WordPress plugin 数が多ければ、管理が困難になるため、ウェブサイト ビルダーのパーセンテージが高くなり、全体のリスクスコアが高まります。 ⇒各項目の評価に応じて全体のリスクスコアが異なります。 リスクスコアの種類：高/中/低

※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

5.6 SSL SCAN（SSL 診断）

診断対象	SSL 証明書をモニターし、下記を監視・検証します。 1．SSL 証明書の有効期限が切れていないかチェック 2．名前/ドメインが正しい情報で登録されているかチェック
診断範囲	お客さまのサーバー上にインストールされた SSL 証明書
診断方法	SiteLock から契約の Web サイトの SSL 証明書有効期限がきれていないかを**毎日１回**チェックします。
診断結果	SSL 証明書の有効期限が切れる前に、カレンダーに合わせて１ヶ月間の事前告知をお客さまのメール宛に通知します。また SSL 証明書の有効期限が切れた場合、お客さま宛にメールにて通知し、管理画面のお知らせインボックスに通知します。

5.7 MALWARE SCAN（マルウェア診断）

診断対象	お客さまの Web サイトを診断して、下記を検証いたします。 1．既知のマルウェアサイトへのリンクの有無 2．悪意のある Java Script
診断範囲	全ページ（設定したルートディレクトリー配下）を診断します。 ※ご契約プランにより、ページ数に上限がある場合もございます。
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、Web サイトのページやサイト上のリンクが、Google/Yandex/PhishTank/Anti-Virus Blacklist のプロバイダーによって管理されているブラッ

	クリストに掲載されていないか確認（ブラックリスト監視）します。また、SiteLock によって管理されている既知のマルウェアサイト情報が格納された内部データベースにも照会して確認を徹底しています。
診断結果	以下の項目について検証します。 ・診断日：診断を行った日 ・診断されたページ：検証したページ数 ・確認済みのリンク：検証したリンク数 ・マルウェア検知：悪意のある Java Script のファイル数 ・マルウェアリンク：ブラックリスト登録がされたサイトへのリンク数 ・ステータス：安全性のステータス（緑：安全、赤：警告） マルウェアを検知した場合、お客さま宛にメールにて通知し、管理画面のお知らせインボックスに通知します。

※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

5.8 SMART（SMART 診断）

診断対象	お客さまの Web サイトを診断して、下記を検証いたします。 1．ファイル変更の有無 2．既知のマルウェアサイトへのリンクの有無 3．悪意のある Java Script 4．疑わしいコードの有無
診断範囲	全ページ（設定したルートディレクトリ配下）を診断します。 ※ご契約プランにより、ページ数に上限がある場合もございます。
診断方法	SiteLock のサーバーにお客さまのディレクトリーをダウンロードし、徹底的な検知を行い、悪意のあるコードを検知した場合、そのコードをお客さまの希望に応じて自動的に削除して(※1)、除法したファイルを感染したファイルと切り替え、お客さまのサーバーにアップロードします。また SMART によりお客さまはサイトに加えられた予期せぬ/承認されていない変更(書き換え)を特定することができます。
診断結果	SMART は以下の項目について検証します。 日時：診断を行った日 診断済み：検証したファイル数 追加済み：前回の診断から追加したファイル 削除済み：前回の診断から削除したファイル マルウェア検知：診断における検知したマルウェア 除去されたマルウェア：SiteLock より削除したマルウェア(※1)

	また特定な診断日をクリックすると、以下の詳細が現れます。 悪意のあるファイル：診断における検知した悪意のあるファイル 不審なファイル：診断によりソースファイルに存在する疑わしいコードを指摘します。 確認中のファイル：即時診断ができない不明なファイルがある場合、SiteLock のエクスパートチームより個別に検討するファイル。診断が完了するまで数日を要します。 マルウェアまたは不審なファイルを検知した場合、お客さま宛にメールにて通知し、管理画面のお知らせインボックスに通知します。
診断のルール	SMART 診断を利用するには、コントロールパネルにて登録ドメインの FTP/SFTP 情報を登録いただく必要があります。1 アカウントのみ登録可能です。 SiteLock では、登録アカウントを利用して取得（ダウンロード）できるデータを対象に診断を行います。取得したデータに登録ドメインのサイト自体、そしてサブドメイン（例：contact.example.com）が含まれていれば、両方に対して診断を実施できます（※）。なお、診断を実施する範囲は、ご契約プランの定めるページ数（ユニークの URL 数）の上限までとなります。 ※ SMART 診断では、特定のコンテンツに対する除外設定を行えます。 ※ 登録ドメインと異なるドメイン（例：another-example.com）のサイトは、対象外となります。 ※ 登録ドメインとサブドメインのサイトを別々の FTP/SFTP アカウントで管理されている場合、別アカウントで管理されているサブドメインのサイトは診断対象外となります。

※1 2.1 SMART WIZARD の設定にて「検知時は、SiteLock にて自動削除、駆除」を選択した場合のみ削除されます。

5.9 SPAM SCAN（スパム診断）

診断対象	お客さまのドメイン名がスパム発信元として主だったブラックリストに掲載されていないか監視します。
診断範囲	SiteLock に登録しているドメイン名
診断方法	スパマーを登録した代表的なブラックリスト(Spamhouse など)を照会し、ご利用のドメインが登録されていないことを確認します。**毎日１回**チェックします。
診断結果	スパムを検知した場合、お客さま宛にメールにて通知します。また、管理画面のお知らせインボックスにも通知します。

6. その他の機能

6.1 ユーザー情報の変更・追加

ご契約時にご案内しているログイン情報の変更やユーザーの追加が行えます。

6.1.1 管理ユーザーの情報変更

STEP1　左メニューの[ユーザー]をクリックし、右側の[ツール]部分のペンマークをクリックします。

STEP2　変更したい情報を入力し、[送信]ボタンをクリックします。

※名前、ID とも日本語入力ができないため、半角英数字を使用してください。

※名前の登録名称は、SiteLock をご利用のすべてのユーザーと共通となります。そのため、重複している場合には、登録できません。

STEP3　設定変更が完了すると下記の画面が表示され、STEP1 の画面に戻ります。

6.1.2 ユーザーの追加

管理者以外に、ダッシュボードにアクセスできるユーザーの登録が行えます。

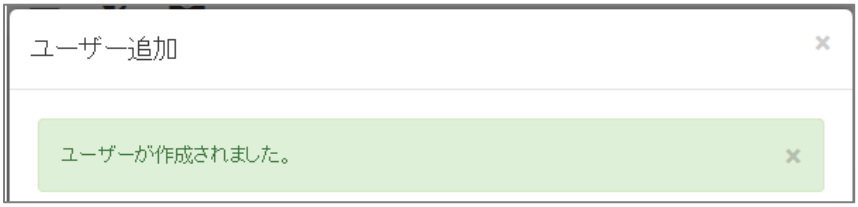
STEP1　左メニューの[ユーザー]をクリックし、[ユーザーの追加]ボタンをクリックします。

STEP2　情報を入力し、[送信]ボタンをクリックします。

※名前、ID とも日本語入力ができないため、半角英数字を使用してください。

※名前の登録名称は、SiteLock をご利用のすべてのユーザーと共通となります。そのため、重複している場合には、登録できません。

STEP3　設定変更が完了すると下記の画面が表示され、STEP1 の画面に戻ります。



STEP4　STEP2 で設定したメールアドレス宛にパスワードを設定するメールが届きますので、URL 部分をコピーしてブラウザでアクセスします。

STEP5　パスワードの設定画面が表示されますので、パスワードを設定後、保存ボタンをクリックします。

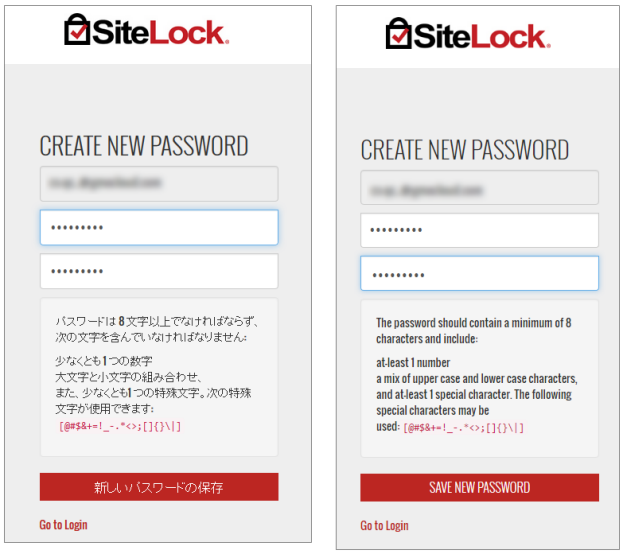
※パスワード設定ポリシーは、以下の通りです。

・少なくとも一つの大文字

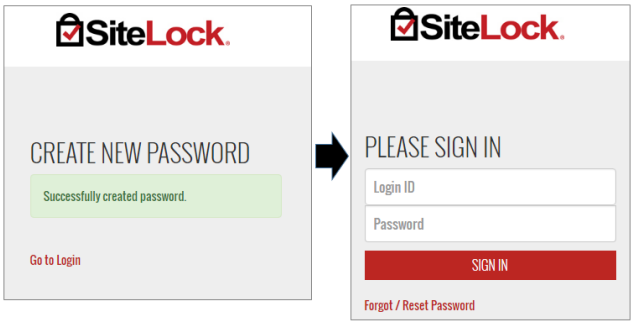
・少なくとも一つの小文字

・少なくとも一つの数値

・特殊文字（@#$&+=!_-.*<>;[]{}\|）



STEP6　設定間表の表示のあとに、再度ログイン画面が表示されますので、ID と設定したパスワードでログインします。



STEP7　ダッシュボードのおよびユーザーメニューのみの画面にアクセスができます。

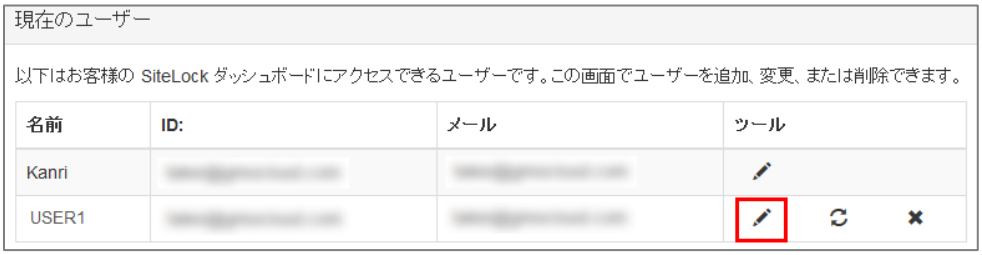
※追加ユーザーが利用できるユーザーメニューはログインしているユーザーの情報変更のみとなります。

6.1.3 追加ユーザーの各種情報変更

管理者のアカウントから、追加ユーザーの情報の変更、パスワードのリセット、削除が行えます。

■追加ユーザーの情報変更

STEP1　対象のユーザーの[編集]のアイコンをクリックします。



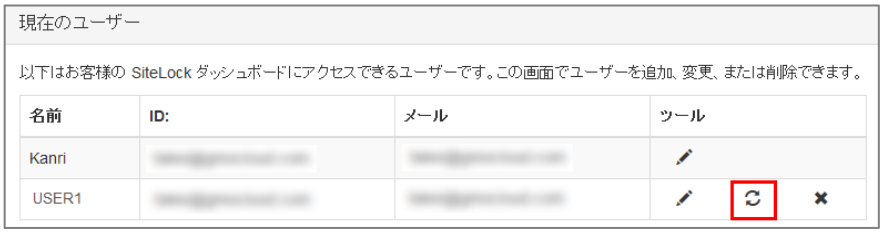
STEP2　管理者が変更できる項目は、名前、ID、メールアドレスです。編集後、[送信]ボタンをクリックし完了です。

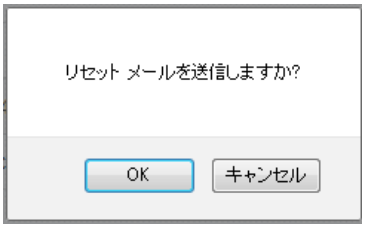
■追加ユーザーのパスワードリセット

追加ユーザーのパスワードが不明になった場合、新たにパスワードを設定することができます。

STEP1　[パスワードのリセット]のアイコンをクリックすると、確認画面が表示されます。

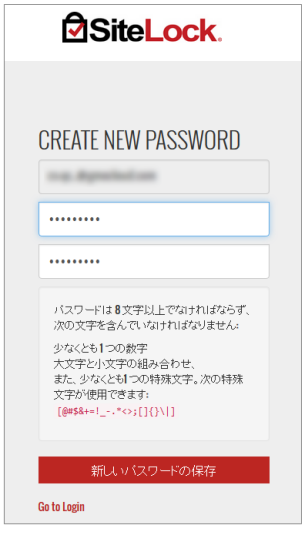
[OK]をクリックすると、追加ユーザーのメールアドレス宛にパスワード再設定のメールが届きます。

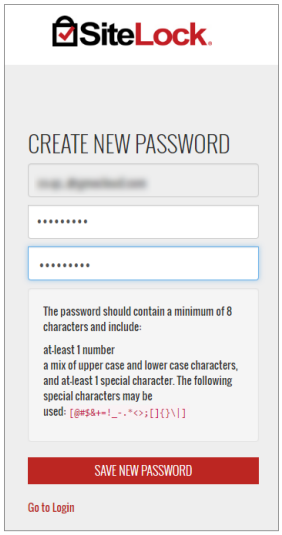




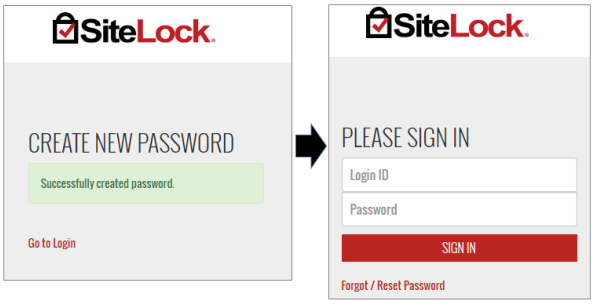
STEP2　届いたメール本文内の URL 部分をコピーしてブラウザに貼り付けてアクセスします。

STEP3　パスワードの設定画面が表示されますので、パスワードを設定後、保存ボタンをクリックします。





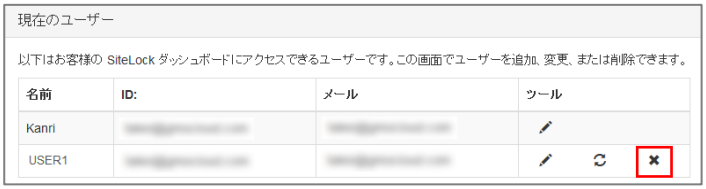
STEP4　設定完了の表示のあとに、再度ログイン画面が表示されますので、ID と設定したパスワードでログインします。

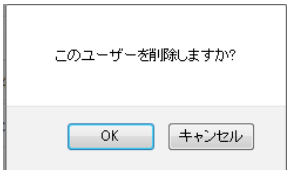


■追加ユーザーの削除

追加したユーザーを削除する場合、[ユーザーの削除]のアイコンをクリックすると、確認画面が表示されます。

[OK]をクリックして、削除完了です。





6.2 お知らせインボックス（メール通知）

コントロールパネルのメールのアイコンをクリックすると、各種情報の確認が行えます。

未読のメッセージがある場合、メール部分に未読数が表示され、クリックすると内容の一部が表示されます。

文章部分をクリックすると全文の確認が行えます。

未読がない場合には、メール部分をクリックし、[さらに表示]をクリックすると詳細の確認が行えます。