SiteLock 操作マニュアル

1.コントロールパネルのアクセス方法と概要	2
1.1 ログイン	2
1.2. コントロールパネルの概要	4
2.設定メニュー	5
2.1 SMART 診断	5
2.2 通知設定	9
2.3 スキャン設定	9
2.4 ダウンロード設定	10
3. ドメイン認証の設定	11
3.1 認証方法 1 - HTML Meta Tag	11
3.2 認証方法 2 - Upload HTML File	13
3.3 認証方法 3- DNS Record	15
4. 安全シールの設定	17
5. スキャン機能性について	19
5.1 診断のルールについて	19
5.2 VULNERABILITY SCAN (プラットフォーム診断)	20
5.3 VULNERABILITY SCAN(XSS 脆弱性診断)	21
5.4 VULNERABILITY SCAN(SQL インジェクション脆弱性診断)	21
5.5 RISK SCORE (リスクスコア)	21
5.6 SSL SCAN(SSL診断)	22
5.7 MALWARE SCAN(マルウェア診断)	23
5.8 SMART(SMART診断)	23
5.9 SPAM SCAN(スパム診断)	24
6. その他の機能	26
6.1 ユーザー情報の変更・追加	26
6.1.1 管理ユーザーの情報変更	26
6.1.2 ユーザーの追加	27
6.1.3 追加ユーザーの各種情報変更	30
6.2 お知らせインボックス(メール通知)	33

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へのログインは、各サービスのコントロールパネルより行っていただくことが可能です。

■レンタルサーバー RS

コントロールパネル URL: https://cp.onamae.ne.jp/login

^{FA128599 お名前.comomo}	レンタルサーバーコントロールバ	パネル	
★ ホーム			
● ドメイン		主要な設定	
☑ メール			
ホームページ設定			
□ 基本設定			
⊘ セキュリティ	国 SSL証明書		
① ファイル管理	🖹 WAF	? NEW	
目 データベース	○ アクセス制限		
≅う Web表示高速化	⊚ ads.txt	ファイル高速化	
🕞 高度な設定	SiteLock	マネージャー 🛛	
ー サーバー		お知らせ 1	
E SSL証明書	世日 WAF	ads.txt	
Sitel ock		2	
ホームページに仕込まれた悪意の	Dあるコードやマルウェアを自動で検知&駆	図除するサービスです。	
		管理画面	
🌐 選択中のドメイン			
詳細情報			
契約中のプラン		■ 解約	
ステータス	稼働中		

■共用サーバー SD

コントロールパネル URL: https://cp.rentalserver.jp/Login.aspx

コントロールパネル	μ			
サービス設定 service > 管 > 独 > フ > サ > サ > W > S	T理者アカウント 全自ドメイン設定 ディスク利用容量 トーバー情報 /ebフォント iteLock			
♪ 芬 コントロールパネル	ध上事項、制限事項	★-ム ■ <u>ガイド</u> ② FAQ	○ 当問い合わせ ■ ログアウト	
 SiteLock一覧 SiteLockは1契約につき、1UR SiteLockの追加、プラン変更に SiteLockオンラインマニュアリ V SiteLockプラン SiteLock エコノミー 	L利用可能です。 <u>はお名前.com Navi</u> ぴからお申込みください。 ₂ ぴ ▼SiteLock URL	<mark>▼ステータス</mark> 稼働中	▼SiteLockへログイン	
		☆ ±-4		

※SMART設定が完了していない場合、ログイン後に右記の

画面が表示されます。

すぐに設定される場合には**[未設定]** ボタンをクリックすると、

2.1 SMART WIZARD (SMART 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									
日 ^{ダッシュボー}	2 ⁵	ダッシュオ	、 ード							最大リスクスコア ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・
路 ユーザー	③	///////////////////////////////////////								低
口 設定	4									Z
🛂 メッセージ	5									
▶ ログアウト	6									
		サイトセ	キュリラ	ァ イ						^
		ドメイン ↑↓	Malware 🖴	Spam 🖴	Vulnerability 🛝	SSL 🖴	App 🛧	Risk Score 🖘	SMART $\uparrow \downarrow$	WAF Plan 🔨
		example.com	Good	Good	Good	未設定	未設定	低	未設定	保留中
		1件中1から1まで	表示							前 1 次

1	SiteLockのロゴ	トップページ(ダッシュボード)に戻ることができます。
2	ダッシュボード	ダッシュボードではドメインの保護状態の概要を表示します。
3	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ユーザーまで追加できます。
4	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。
5	メッセージ	SiteLockからのメッセージから、各種診断の結果を確認できます。
6	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。
7	最大リスクスコア	低・中・高のスコアリングが表示されます。クリックして詳細を確認できます。

セキュリティの状況は、各診断の概要が表示され、[詳細の表示]をクリックすると、設定や診断詳細を確認できます。

ドメイン統計							
example.com	•						
6	€ 失敗	0	<mark>.)</mark> 未設定	6	Ø	6	۲
SSL Scan		SMART		Domain Ve	rification	Malware	Scan
最終秒延日: [] ステータス: []		最終診断日: [] 思惑のあるファイ [] ル: 確認中のファイル [] 不喜なファイル [] ステータス: []				最純彩吹日: 診断ページ: マルウェア検知: 確認済みのリンク: Spam Links:	[06/30/2021] [1] [0] [1] [0]
詳細の表示		詳細の表示		詳細の表示		詳細の表示	

	問題がありません。
•	保留中あるいは未設定の状態です。
$\textcircled{\begin{tabular}{c} \hline \hline$	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 診断

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 設定アラートのSMART欄の[未設定]ボタンアイコンをクリックします。



※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。

ダッシュボー ド	設定 信 example.com	T	
	一 环和,		
	吉诺段正	SMART 設定	
🕒 メッセージ	通知		
▶ ログアウト	スキャン設定	マルウェアの自動削除	検知時は、警告のみ ▼
	ダウンロード設定		
	SMART 設定	SMART は、 <u>ウィザード</u> で	⁹⁶⁷ で定めたダウンロード設定を利用します。

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。

< Smart Wizard		
example.com	•	
ステップ1接続		
ステップ2ルートの特定 >	FTP ログイン情報	
	手順	
	ファイル転送方法	FTP
	FTP ホストアドレス	
	(S)FTP ポート番号	
	ユーザー ID	
	パスワード	
		テスト接続
		テスト接続

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ID	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。

MART診 Jを特定	断の対象とするルートディレクトリをお選びください。または、「ルートディレクト 」ボタンをクリックして特定できます。
JL-	ディレクトリを特定
b .	
	+ merror_docs
	Bhttpdocs
	➡ logs
レー	トディレクトリ:

※ 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「<u>よくある質問</u>」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。

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。

SMART ウィザード	×
ルートディレクトリを検証しまし た。リダイレクト中	
SMART 設定	

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。

ØSiteLock				
日 ^{ダッシュボー} ド 器 ユーザー	設定 后 example.com		•	
□ □ 設定	言語設定	>	SMART 設定	
🖻 メッセージ	通知	>		検知時は、音古のみ 検知時は、SiteLockにて自動削除・駆除
Ե ログアウト	スキャン設定	>	マルウェアの自動削除	検知時は 警告のみ
	ダウンロード設定	>		
	SMART 設定	>	CMADT (는 스, 너희 N 고등	
			SMARTIAL <u>DADEN</u> CA	.0) ビダウノロー Figue 化利用します。

保存が完了すると、右図の画面が表示されます。

マルウェアの自動削除	検知時は、SiteLockにて自動削除・駆除	•
保存しました		×
	保存	除外設定
SMART は、 <u>ウィザード</u> で定る	めたダウンロード設定を利用します。	

■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、[除外設定]ボタンをクリックして設定します。

SiteLock.		
日 ダッシュボー ド 路 ユーザー	設定 Ē example.com	•
昂 設定	言語設定	SMART 設定
🛂 メッセージ	通知	
	スキャン設定 >	マルウェアの自動削除 検加時(+ 数先の3)
	ダウンロード設定 >	
	SMART 設定 >	

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。

SMART診断で診断対象外とするフォ	ルダ・ファイル等を設定します。	SMART診断で診断対象外とするフォ	ルダ・ファイル等を設定します。
ファイルとフォルダを選択	種類とサイズを選択	ファイルとフォルダを選択	種類とサイズを選択
 ► merror_docs ► httpdocs + test index.html + mercor_docs 	へ 保存された除外 Select items to remove from Exclusions List 項目なし	 t merror_docs t httpdocs t test index.html t modes 	▲ 保存された除外 Select items to remove from Exclusions List ■ logs
更新		更新	

※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。

SMART診断で診断対象外とするフォル	レダ・ファイル等を設定します。	SMART診断で診断対象外とするフォ	ルダ・ファイル等を設定します。
ファイルとフォルダを選択	種類とサイズを選択	ファイルとフォルダを選択	種類とサイズを選択
 + merror_docs - bhtpdocs + test index.html + mlogs 	▲ 保存された除外 Select tems to remove from Exclusions ■ logs	 terror_docs thtpdocs test index.html tess 	へ 保存された除外 Select items to remove from Exclusions List 項目なし
更新		更新	

[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。

詠外するファイルの	0種類		選択したサイズより大きなファイルを除外
拡張子	サイズ (MB)	除外中	▲ ● 制限なし ● 5 MB
tif	0		○ 10 MB
docx	0		 15 MB 20 MB
rar	0		
pdf	0		
mov	0		
zip	0	✓	•

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。)

SiteLock	<		通知
田 ダッシュボー ド 路 ユーザー	設定 Ē example.com		SiteLockからのセキュリティ アラート メールの受信を開始するには、以下のチェックボック スをオンにしてください。SiteLockからのメールを受信するメールアドレスを変更できます。
□ □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	言語設定	>	セキュリティ アラートの受 オン
🛂 メッセージ	通知	>	(E)
🗗 ログアウト	スキャン設定	>	メール example@example.com
	ダウンロード設定	>	保存
	SMART 設定	>	

セキュリティアラートの受信 (オン/オフ)	アラートメールを受信する(オン)、受信しない(オフ)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。

SiteLock		スキャン設定
 	設定 example.com	施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。
□ ハッこ ソ	通知 > スキャン設定 > グウンロード設定 > SMART設定 >	SQL Injection Scan, Malware Scan) SMART 毎日 送信

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。

設定			
example.com		\checkmark	
言語設定通知	>	ダウンロード設定	
スキャン設定 ダウンロード設定	> >	SMART診断を実施するにあたり、SiteLockはお客様のWebサーバーから診断対象のデータをダウンロ ードいたします。診断実施に必要な情報をご入力ください。ヘルプが必要でしたら、 <u>ウィザードを</u> <u>お使いください</u> 。	
SMART 設定	>	ファイル転送方法	
		FTP ホストアドレス	
		(S)FTP ポート番号 21	
		ルートディレクトリ	
		ユーザーロ	
		パスワード	
		FTPファイルのダウンロード 速度 ・ 通常(接続1件) ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	
		最大ダウンロード時間 90分/日 ▼	
		保存	

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ーを指定します。
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	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。
速度を選択してください。	※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。

3. ドメイン認証の設定

DOMAIN VERIFICATION (ドメイン認証)を行います。

ドメイン認証の設定手順はドメイン認証1、ドメイン認証2、ドメイン認証3のいずれかの手順で設定を行ってください。

認証方法 1-HTML Meta Tag			
ドメインの確認	STELOOK 指定の認識L用 META タクをお各さまサイトの中にご里の込み設定を行います。		
認証方法 2 - Upload HTML File	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		
認証ファイルをアップロード	トリー配下にアップロードします。		
認証方法 3-DNS Record			
TXT レコードによるドメイン認証			

3.1 認証方法 1 - HTML Meta Tag

STEP1 ダッシュボードの [DOMAIN VERIFICATION] から[詳細の表示]をクリックします。

	→ 未設定	
Domain Verification	SMART	SSL Scan
	最終診断日: [] 悪意のあるファイ [] ル: 確認中のファイル: [] 不喜なファイル: [] ステータス: []	最終診断日: [] ステータス: []
詳細の表示	詳細の表示	(詳細の表示)

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。

Comain Name Verification		
example.com	T	
認証方法 1 - HTML Meta Tag 💙		
認証方法 2 - Upload HTML File 🔰	ドメインの確認	
認証方法 3 - DNS Record 🔰	表示されたメタタグを診断対象のWebサイトのトップページに挿入します。挿入後、[確認]をクリックすればドメイン認証が始まります。	
	<meta name=" />	
	確認	

※下記の画像はサイト内の記述の一例です。

1 <head>↓ 2 ↓</head>	
3 ↓ 4 <body bgcolor="″#FFE4E1″">↓ 5 ****** Sitel ockテスト用indexページです。****** br></body>	く「昭和シの下がらく」「昭和シの王の前に「西日本シンを用う行います。
6 ↓ 7 ↓ 8 ↓	

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。

Comain Name Verification		
example.com	Ť	
認証方法 1 - HTML Meta Tag 💙		
認証方法 2 - Upload HTML File 🔰	ドメインの確認	
認証方法 3 - DNS Record >	表示されたメタタグを診断対象のWebサイトのトップページに挿入しま す。挿入後、[確認]をクリックすればドメイン認証が始まります。	
	<meta name=" />	
	在1200	

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。

Domain Verification	
ドメイン名の所有権を確認しています。 これには数分かかることがあります。	
 0	

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- Upload HTML File

STEP1 ダッシュボードの [DOMAIN VERIFICATION] から[詳細の表示]をクリックします。

	6	 0	● 未設定
Domain Verification	SMART	SSL Scan	
	 最終診断日: [] 悪意のあるファイ [] ル: 確認中のファイル: [] 不審なファイル: [] ステータス: [] 	最終診断日: [ステータス: [1
詳細の表示	詳細の表示	詳細の表示	

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。

< - Domain Name	Verification
example.com	v
認証方法 1 - HTML Meta Tag 》 認証方法 2 - Upload HTML File 》 認証方法 3 - DNS Record 》	ルートディレクトリに認証ファイルをアップロード <u>ここをクリック</u> して、認証ファイルをダウンロードしてください。診断 対象とするWebサイトのルートディレクトリ(Public_html、www、 root、wwwなど)にアップロードしてください。詳細については、右の [手順をクリックしてください。ファイルをアップロード後、[確認]ボタ ンをクリックすればドメイン認証が始まります。 <u>ダウンロード</u> 確認

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ー配下に

アップロードします。



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。

Domain Verification	×
ドメイン名の所有権を確認しています。 これには数分かかることがあります。	
0	

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。



3.3 認証方法 3- DNS Record

STEP1 ダッシュボードの [DOMAIN VERIFICATION] から[詳細の表示]をクリックします。

	 未設定 	
Domain Verification	SMART	SSL Scan
	 最終診断日: 【】 悪意のあるファイ 】 確認中のファイル: 【】 不審なファイル: 【】 ステータス: 	最終診断日: [] ステータス: []
詳細の表示	詳細の表示	詳細の表示

STEP2 枠内のレコード内容をコピーして、ご利用サーバーの DNS レコードに TXT レコードを追加します。

※DNSレコードの記述方法は、お客さまご利用のDNSサーバーによって異なるため、管理会社さまにご確認ください。

Comain Name Verification		
example.com	•	
認証方法 1 - HTML Meta Tag		
認証方法 2 - Upload HTML File	TXTレコードによるドメイン認証	
認証方法 3 - DNS Record	SiteLock診断対象ドメインのゾーン情報を編集し、以下記述をTXTレコード ● FIE の値としてご入力ください。 手順の詳細については、右の[手順]をクリックしてください。TXTレコード を設定後、[確認]ボタンをクリックすればドメイン認証が始まります。 ドメインのゾーン情報の設定方法はご利用のネームサーバー提供元へお問い合わせください。	
	sitelock-domain-validation=	

STEP3 DNS レコード浸透後、[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。



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サイトの復日が完了し、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 ダッシュボード「ドメイン統計」の右上に表示される盾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。

SiteLock.		
ダッシュボー 田	ダッシュボード	最大リスクスコア
► ≌	アカウントダッシュボードビュー	15
日 設定		1広, 果大リスクスコア
🗐 メッセージ		
~~~~~~~	サイトセキュリティ	·····
	ドメイン統計	
	example.com	$\bigcirc$
SITELOCI	<b>K</b> の安全シール 、	
ステップ1言語の選択 ステップ2色、サイズ、 の選択	スタイル >           ステップ 1 言語の選択            日本語	プレビュー
<b>ステップ 3</b> 安全シールの ール	Druzh > Deutsch English Español Français Italiano	SiteLock. マルクエアフリー・ 合格
	Język Polski Nederlands Português Português Brasileiro	次へ 保存
	中义 日本語 ελληνικά	

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。

<ul> <li>✓ SITELOCKの安全</li> </ul>	シール
example.com	T
ステップ1言語の選択 >	
<b>ステップ 2</b> 色、サイズ、スタイル <b>〉</b> の選択	ステップ2色、サイズ、スタイルの選択       色     サイズ     スタイル     プレビュー
<b>ステップ 3</b> 安全シールのインスト <b>〉</b> ール	レッド マ ミディアム マ マルウェアフリーマ Stelock
	色 サイズ スタイル
	レッド
	レッド スモール マルウェアフリー

ミディアム ビッグ 安全

STEP3 安全シールを表示させるためのコード部分をコピーして対象のサイトに貼り付けます。

※安全シールの位置は任意でご設定ください。

サイト内への追記が完了してから、[保存]をクリックします。

ホワイト

<b> </b>	シール	
example.com	T	
ステップ1言語の選択		
ステップ2色、サイズ、スタイル <b>〉</b>	<b>ステップ3</b> 安全シールのインストール	
の選択	Use the code below to install your Trust Seal	
<b>ステップ 3</b> 安全シールのインスト <b>〉</b> ール	<a href="#" onclick="window.open('https://www.sitelock.com/verify.php?&lt;br&gt;site=example.com';SiteLock';width=600,height=600,left=160,top=170');"><img <br="" class="img-responsive"/>alt="SiteLock" title="SiteLock" src="//shield.sitelock.com/shield/example.com" /&gt;</a>	<i>h</i> .
	- SiteLock セキュリティ バッジをインストールするためのステップ バイステップ ガイド	
	前へ 前へ	保存

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。

※[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。

### 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。 例えば、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

また、リモートによる各種診断は、トップページを起点にページ内リンクをたどって下層へのスキャンを実施しますのでリ ンクが貼られていないページ、ディレクトリーはスキャンが行えません。 スキャン対象とする場合は、一時的なリンク設置またはサイト非公開リンクの設置などのご対応が必要となります。

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、そのディレクトリー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 VULNERABILITY SCAN (プラットフォーム診断)

※WordPress または Platform Scan (プラットフォーム診断)は WordPress と Joomla をご利用のサイトのみ対象のサービスです。(利用されていない場合、PLATFORM SCAN のタブは表示されません)

診断対象	アプリケーションに外部から侵入し、お客さまのサーバーで稼動する WordPress と Joomla を対象に定期的な
	脆弱性診断を行います。(現在は WordPress と Joomla のみ対応しています。)
診断範囲	WordPress と Joomla の本体、検出されたプラグイン、テーマとすべて含まれます。
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	「低」「中」「高」「重大」「緊急」に分類されます。
	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。
	重要度:「低」「中」「高」「重大」「緊急」
	カテゴリー:検知した脆弱性のカテゴリー
	Summary:検知した脆弱性のサマリー
	詳細:検知した脆弱性の説明
	※脆弱性は共通脆弱性評価システム CVSS (Common Vulnerability Scoring System)を基に評価・分類しされて
	います。
	参考情報:
	英語:
	https://www.first.org/cvss/specification-document
	https://www.first.org/cvss/v3.1/specification-document
	日本語:
	https://www.ipa.go.jp/security/vuln/CVSS.html
	各レベルの脆弱性の詳細は「低」「中」「高」「重大」「緊急」に分類されています(※3)。
	※Platform SCAN (プラットフォーム診断)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」「重大」「緊急」の脆弱性を検知した場合、ダッシュボートの VULNERABILITY SCAN が赤(X)になり
	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御時更新されます。

※3 Platform Scan (プラットフォーム診断)の診断結果例

### 5.3 VULNERABILITY 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(設定したレ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	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。
診断線	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、お客さま宛て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 VULNERABILITY SCAN (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、お客さま宛て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 SQLINJECTION 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 RISK SCORE (リスクスコア)

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/ファイルは撲聴化(暗号化)が実施されるコード/ファイルです。

このスキヤンは喧亏化を開味し、イルノエアノアイルの頻繁に採用するハ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。
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。
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。
Webサイトのリスクスコアを決定するには、以下の3つの評価要素が用いられます。
(1) COMPLEXITY (複雑さ)
Web サイトに掲載されたメールアドレス、iframe、フォームやソフトウエアの使用、その数やペー
ジ数といった指標から、Webサイト全体の複雑さを評価します。
(2) COMPOSITION (構造)
WordPress、Joomla! といった Web サイトを構築する上で使用するソフトウエアの利用状況など、
Web サイト全体の構造を評価します。
(3) POPULARITY (人気度)
サイト訪問者数や SNS の反響を指標とし、Web サイトの人気度を評価します。 SNS のフォロワー
数、いいねの数など、SNS における影響力などを考慮します。
前述の3つの評価要素を鑑み、SiteLockは「リスクスコア(RISK SCORE)」を管理画面上に表
示します。 リスクスコアは、 「高」 「中」 「低」 の3 つのいずれかになります。 それぞれの評価
要素が、リスクスコアに決定する上で寄与した割合も表示されます。 Web サイトの潜在的なリ
スクがどこにあるか、絞り込むことができます。
※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 plug In 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。
2 例 J   刍 ※   / 吳   >   >   >   >   >   >   >   >   >

※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)

診跡対象	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証明書有効期限が切れていないかを毎日1回チェックします。
診断線	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カ月間の事前告知をお客さまのメール宛てに通
	知します。また SSL 証明書の有効期限が切れた場合、お客さま宛て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。
診脈課	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
診断課	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
診断課	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
診断結果	以下の項目について検証します。 ・診断を1: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
診断結果	以下の項目について検証します。 ・診断を1: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)
診断結果	以下の項目について検証します。 ・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、お客さま宛て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

※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(設定したリレ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	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。
診脈課	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のエキ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、お客さま宛て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	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
ルール	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。			
診断課	スパムを検知した場合、お客さま宛て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 | 静変更

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。

ダッシュボー ド	ユーザー	の詳細		(ユーザー追加)
路 ユーザー	最大20ユーザー	ーを追加		
口 設定	羽在のつ	++*`		
🛂 メッセージ	以下はお客様のSite	- ン Lockダッシュボードにアクセスで	きるユーザーです。この画面でユーザーを追加、変更、または削除で	್ ಕೆಸ್,
▶ ログアウト	名前	ID	メール	ツール
		0000000	example@example.com	

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、<u>SiteLock をご利用のすべてのユーザーと共通</u>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。

ユーザーの編集 ×		※パスワードは以下を含む8文字以上でご設定ください。
		● 少なくとも1つの数字
名前		● 大文字と小文字の組み合わせ
ID	0000000	● 少なくとも1つの特殊文字
メール	example@example.com	@#\$&+=!*<>;[]{}¥
現在のパスワード		
新しいパスワード		
パスワードの確認		
	パスワードは8文字以上でなければなら ず、次の文字を含んでいなければなりま せん: ・ 少なくとも1つの数字 ・ 大文字と小文字の組み合わせ ・ 少なくとも1つの特殊文字: @#\$&+=!*<>;[]{}\] プライバシーポリシー	
	キャンセル 送信	

1ーザーの編集	×
Successfully updated	×

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。
-------	---------------------	-----------------------

SiteLock.			•	
日 ^{ダッシュボー} ド	ユーザーの詳細	田		(ユーザー追加)
ಜಿ ユーザー	最大20ユーザーを追加			
<b>昂</b> 設定	羽在のフーザー			
🛂 メッセージ	以下はお客様の SiteLock ダッシュボ・	ードにアクセスできるユーザーで	す。この画面でユーザーを追加、変更、または削除できまで	σ.
▶ ログアウト	名前	ID	メール	ツール
	user-name1	0000000	example@example.com	1

#### STEP2 情報を入力し、[送信]ボタンをクリックします。

ユーザー追加 ×		※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
<i>2</i> #		てください。
名則	user-name	※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
ID	loginID	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。
メール	user@example.com	
	プライバシーボリシー	
	キャンセル 送信	

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。

ユーザー追加	×
ユーザーが作成されました。	×

#### STEP4 STEP2 で設定したメールアドレス宛て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。

※パスワードは以下を含む8文字以上でご設定ください。

CREATE NEW PASSWORD
Login ID
パスワードは8文字以上でなければなら ず、次の文字を含んでいなければなりま せん:
少なくとも1つの数字 大文字と小文字の組み合わせ、 また、少なくとも1つの特殊文字。次の特 殊文字が使用できます: @#\$&+=!・*<>;[]{}\]
新しいパスワードの保存
<u>Go to Login</u>

● 少なくとも1つの数字

- 大文字と小文字の組み合わせ
- 少なくとも1つの特殊文字

@#\$&+=!_-.*<>;[]{}¥|

STEP6 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。



**STEP7** ダッシュボード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。



SiteLock.	<			
ダッシュボー ド	ユーザー	の詳細		
路 ユーザー	最大20ユーザー	を追加		
口。 設定	現在のつい	+f`		
🛂 メッセージ	レ 大 「 上 し ノ 上 し ノ 上 し ノ ー 上 し 、 い も お 客様の SiteLo	ン ckダッシュボードにアクセ	2スできるユーザーです。この画面でユー!	ザーを追加、変更、または削除できます。
▶ ログアウト	名前	ID	メール	ツール
	user-name	testuser	user@example.com	ø

※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。

ユーザーの約	扁集    ×
名前	user-name
ID	(1111111
メール	user@example.com
	プライバシーポリシー
	キャンセル 送信

#### ■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てにパスワード再設定のメールが届きます。

SiteLock.				
ダッシュボー ド	ユーザーの	詳細		(ユーザー追加)
路 ユーザー	最大20ユーザーを	追加		
<b>同</b> 設定	現在のユー	ザー		
🛂 メッセージ	ット 以下はお客様の SiteLock ダ	ー 'ッシュボードにアクセスで	きるユーザーです。この画面でユーザーを追加、	変更、または削除できます。
➡ ログアウト	名前	ID	メール	ツール
	user-name1	0000000	example@example.com	ð
	user-name	1111111	user@example.com	<i>∎</i> €×

Confirm?	×
リセット メールを送信しますか?	
	キャンセル

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。

ダッシュボー ド	ユーザーの	詳細		(ユーザー追加)
路 ユーザー	最大20ユーザーをì	自加		
<b>口</b> 設定	現在のフー-	<b>⊢#`</b>		
🛂 メッセージ	いた はお客様の SiteLock ダ	ッシュボードにアクセスで	きるユーザーです。この画面でユーザーを追加、	変更、または削除できます。
┣ ログアウト	名前	ID	メール	ツール
	user-name1	0000000	example@example.com	1
	user-name	1111111	user@example.com	1 2 ×

[OK]をクリックして、削除完了です。

Confirm?	×
このユーザーを削除しますか?	
	++>211 OK

### 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。

SiteLock	
日 ダッシュボー ド	<お知らせ ■ example com
い ユーザー	
は認定	SiteLockからのお知らせです。
🖻 メッセージ	
➡ ログアウト	すべての設定 <u> </u>
	14時間前     日付:8月前       タイプ: Security/重要度: Critical     月社のウェブサイトexample
	□ <b>8月前 〉</b> <i>sAJ: Verification</i> /重要度: <i>Notice</i> お客様のウェブサイトのドメ