Webサイトの安全確認を３ステップで

SiteLock（サイトロック）のご紹介資料

「SiteLock」とは？

お客さまのWebサイト内に
潜むリスクを診断します。

SiteLockは、お客さまのWebサイトを監視・診断・復旧できるクラウドセキュリティサービスです。
Webサイトの安全性を日々監視し、セキュリティ事故発生時は速やかに復旧に向けた処置を進められるようになります。

「SiteLock」が選ばれる3つの理由

SiteLock

セキュリティ診断の選択基準を
高い次元で満たしています。

世界が認めた技術力＆知名度

米国Gartner社の
「Magic Quadrant for Application Security Testing」
レポートで2年連続でマジック・クアドラント選出

世界800万件の導入実績

クラウド、ホスティング事業者を通じて囲い込んだ
世界800万以上のWebサイトを日常的に診断、
膨大なセキュリティ・データベースに情報を集約・分析

圧倒的な低料金

①定評あるサービスを月あたり350円からと、
セキュリティ業界の常識を覆すコストパフォーマンス
②都度診断ではなく、継続的な監視と診断をオファー

セキュリティ診断の分野で際立つ存在感

SiteLock

Garner社
Magic Quadrant 2年連続で選出

競争の激しいセキュリティ市場における企業のビジョンと遂行能力を評価する米国Gartner社発表（2017年2月）の「Magic Quadrant for Application Security Testing」レポートにおいて、

2年連続でニッチ・プレイヤーのクアドラントに選出
主要なベンダーの一つとして高い評価を受ける

“Magic Quadrant”は特定の市場におけるリサーチの集大成であり、
市場内で競合するベンダーの相対的な位置付けを広い視野から提示するものです。

出典：Gartner, Feb 2017
https://www.gartner.com/doc/reprints?id=1-3UKD88S&ct=170301&st=sb
https://www.gartner.co.jp/research/methodologies/research_mq.php

SiteLockのミッション

Webサイトの「安全・安心」を守る

見つける

- WordPressの脆弱性
- アプリの脆弱性
- ホームページ内の脆弱性
- XSS脆弱性
- SQL インジェクション脆弱性
- マルウェア
- 不正なリンク、コード
- 不正改ざんの痕跡
- Webセキュリティの問題

解決する

- マルウェアを駆除
- 不正なリンク、コードを除去
- 改ざん復旧
- 問題解決の方法を提案

守る

- 定期診断で監視
- SSLサーバー証明書を監視
- ブラックリスト監視
- セキュリティレポート提出
- 安全シールで情報開示
- カスタマーサポート

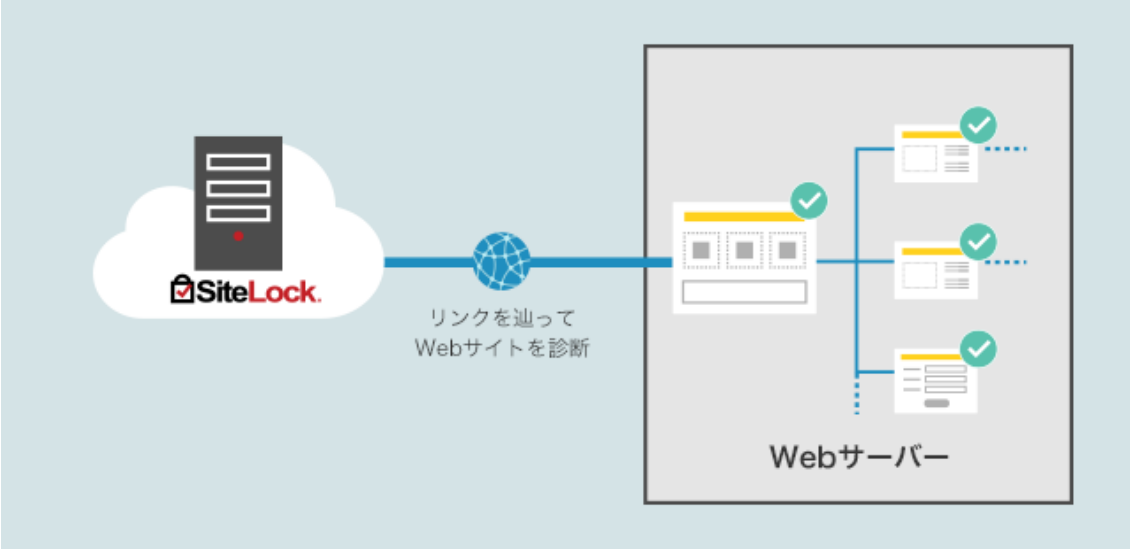
SiteLockの診断方法

2種類の診断を組み合わせて、お客さまのWebサイトを診断します。

診断方法	①リモート診断	②SMART診断
診断内容	インターネット経由で ページ内のリンクを辿る方式で 定期的な診断を実施いたします。	FTP経由でデータを取得後 SiteLockの診断サーバー上で 診断を実施します。
通信方法	http/https	FTP/SFTP/FTPS
診断単位	ページ／リンク	ディレクトリ／ファイル／ファイルタイプ
診断上限	契約プラン数	無制限
診断項目	●WordPress脆弱性診断 ●アプリケーション脆弱性診断 ●XSS脆弱性診断 ●SQLインジェクション脆弱性診断 ●マルウェア診断 ●SSL診断 ●スパム・ブラックリスト監視 ●ブラックリスト監視	●マルウェア検知・駆除 ●Webサイト改ざん検知
診断効果	脆弱性診断 マルウェア検知	改ざん検知 マルウェア検知・駆除

SiteLockの診断タイプ①

インターネット経由のリモート診断



■ページの診断方法

SiteLockのスキャナーはまず、サイトのホームページを読み込み、
ページコンテンツを検証してページ上のリンクをすべて検出します。

それらのリンクは同じサイトへの内部リンクと、
別のサイトへの外部リンクに分類されます。
尚、サイト上のフォームはすべて内部リンクとして保存され、
それぞれのページは拡張子(.html/.css/cgi/php)に基づいて分類します。

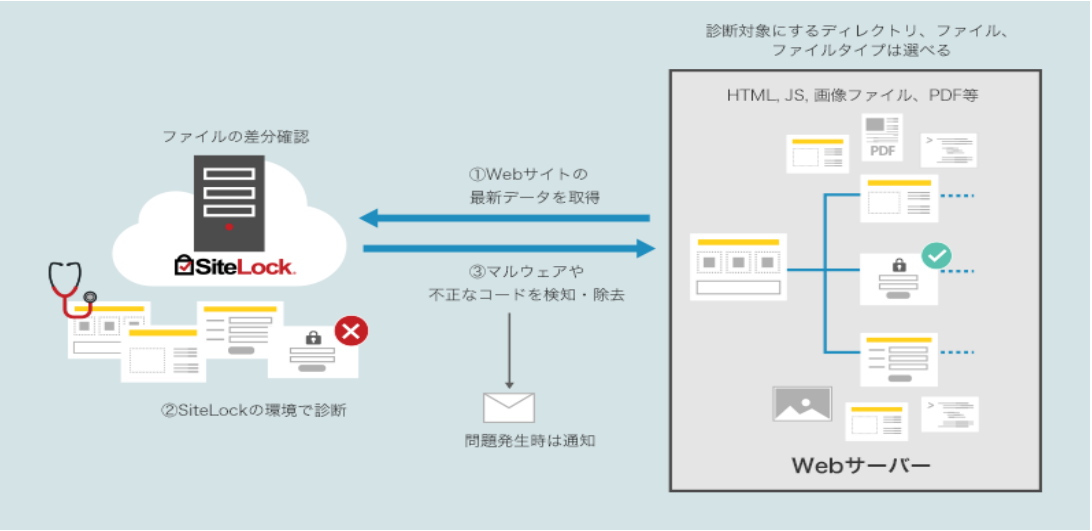
スキャナーは最初のページの構文解析を終えたら次のページに移動し、
まず訪問したことのない全ての内部リンクに対して診断を開始します。

■ページの診断順序ルール

1.前回の診断時に問題が検出されたページ。
2.サイトツリーに従い、段階的にページを診断。
3.パラメーターを省略したページで、SiteLockの訪問回数が多い順で診断します。但し、実際の診断では任意のパラメータを複数回、指定して診断します。例えば、www.shoppingcart.com/catalog.php?product=1 という構造のURLの場合、商品番号（product=1）を任意に”n”個を設定して診断します。
SiteLock契約ページ数内で可能な限り、”n”個を設定して診断します。
4.パラメータが設定されたページで、
SiteLockが訪問した回数の多い順で診断します。
5.URL内の " / " の数が最も少ないページ（＝上位階層のページ）

SiteLockの診断タイプ②

FTP経由でデータ取得後、診断サーバーで実施（SMART診断）



リモート診断とは異なり、
診断可能なファイル数に
上限はありません。

■SMART診断とは

SMART（セキュアマルウェア自動削除ツール）は、既知のマルウェアを検出して駆除まで実施するSiteLockの主要機能の１つです。

FTP経由で対象Webサイトの物理的なファイルに直接アクセスし、Webサイトに関連するすべてのファイルを診断します。

SMARTは既知のマルウェアスクリプト、アルゴリズム、バックドアファイル、および悪意のあるコードをFTP経由で物理ファイルレベルで診断します。また第三者によるWebファイルへの不正アクセスや改ざんをユーザーに通知し、変更内容を正確に示します。

■SMART診断の自動削除について

SMART診断の自動削除では悪質なコード、ファイル、またはリンクを特定し、それらを自動的に削除することが可能です。
但し、Webサイトに影響を及ぼすと判断した場合、対象コードを残してその結果を警告するに留まります。

SMART設定では、マルウェア検知時の処理を
以下から選択することができます。

①検知時は、警告のみ。
②検知時は、SiteLockにて自動削除・駆除。

WordPress脆弱性診断

SiteLock

改ざんの標的となりやすいWordPressの安全性をチェック

脆弱性を狙った攻撃が多発するWordPress

普及率の高いWordPressの脆弱性診断

アプリ診断 <APPLICATION SCAN>
診断頻度: 週 / 月 / 四半期

全世界の1/4のWebサイトで採用されているWordPressは、悪意のある第三者による攻撃対象として常に狙われています。SiteLockは、リモートによるアプリ診断を実施して、WordPressの脆弱性を洗い出します。診断対象には、WordPress本体、プラグインとすべて含まれます。大切なWebサイトを守る取り組みとして、定期的な診断をお勧めいたします。

期待できる導入効果

- WordPressの安全性を確認
- 脆弱性のない健全なブログとしての監視履歴を保管
- 緊急性の高い脆弱性検知時は、状況を把握して、迅速な対応へ
- 改ざん攻撃による影響を低減

アプリ診断

SiteLock

情報漏えい、不正改ざん等の要因となるアプリの脆弱性を診断

既知の脆弱性のある古いバージョンを
使っていませんか？

信頼度の高いアプリ脆弱性診断

アプリ診断<APPLICATION SCAN>
診断頻度: 週 / 月 / 四半期

Webサイトを対象として、リモートによるアプリ脆弱性診断を行います。自作アプリ、Movable Typeなど、幅広い種類のアプリを対象とした診断を実施できます。情報漏えい、不正改ざんなど重大なセキュリティ事故の要因となりえる脆弱性の有無を判別いたします。定期的な診断を実施することで、緊急度の高い脆弱性に対する監視体制を築けます。お問い合わせフォームやショッピングカートなど、Webサイト上で個人情報を取り扱うお客さまには、特に導入をお勧めいたします。

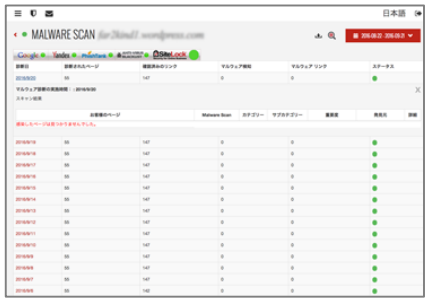
期待できる導入効果

- Webサイト内のアプリの安全性を確認
- 脆弱性のない健全なWebサイトとしての監視履歴を保管
- 脆弱性検知時は、迅速に状況を把握・アクションへ繋げる危機管理体制を構築

脅威を検知！マルウェア診断

SiteLock

Webサイトに潜む不正なマルウェアやコード等を洗い出します



随時更新されるシグネチャベースのデータベースに照合し、Webサイトに埋め込まれた不正なマルウェアをピンポイントで検知

Webサイトを常時監視

マルウェア診断 <MALWARE SCAN>
診断頻度: 毎日

悪意のある第三者によって改ざんされ、不正なマルウェア等を埋め込まれると、正規サイトはサイト訪問者へ害を及ぼす危険な有害サイトへ変わります。そのため、問題発生時の早期発見が重要です。SiteLockは、毎日リモートによるマルウェア診断を行います。お客さまのWebサイトにマルウェアが検知された場合は、問題のあるURLをいち早く通知いたします。

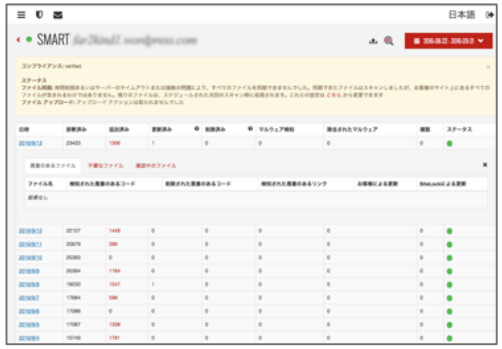
診断で見つけられるマルウェア

- 有害サイトへの誘導リンク
- サイト訪問者に不利益をもたらす不正なソフトウェア
- その他、セキュリティ脅威となる情報

不正なマルウェア駆除・削除

SiteLock

マルウェア検知時は、Webサイトの脅威を駆除・削除



危険な作業は、SiteLockにお任せ

手作業による駆除・削除は危険

SMART診断 <SMART>
診断頻度: 日 / 週 / 月 / 四半期

リモートによるマルウェア診断に加え、定期的なSMART診断を併用することでマルウェア駆除・除去も可能になります。マルウェア検知時は、SiteLockがお客さまに代わって自動でマルウェアを駆除・削除いたします。お客さまが診断結果を確認した上で、コントロールパネルを操作して同様の作業を行うこともできます。アクセスすると閲覧者の端末に危害を加える恐れのあるマルウェアや何百ページにわたって埋め込まれた危険なコード等の除去など、危険かつ面倒な作業はSiteLockにお任せください。

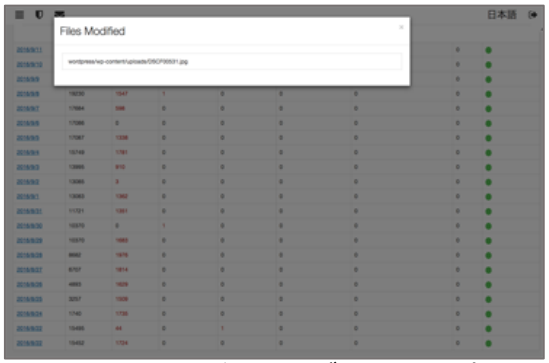
期待できる導入効果

- 危険なマルウェア対応は、お任せ
- マルウェアの二次感染をガード
- 自社による迅速な問題解決
- 情報セキュリティ対策の確立

SMART診断

SiteLock

SiteLockのサーバー上で、お客さまのWebサイトを多角的に診断



Webサイトの影響を及ぼさない環境で
本格的な診断を実施

深層まで診断を徹底

SMART診断 <SMART>
診断頻度: 日 / 週 / 月 / 四半期

お客さまのWebサイトのデータを取得し、SiteLockのサーバー上で高度な診断を定期的に実施いたします。不正改ざんされた痕跡、脅威となりえるマルウェアの存在を洗い出し、お客さまに診断結果をお伝えいたします。問題が検知された場合、問題発生前の状態にWebサイトを復旧して安全性を維持できる診断サービスです。

期待できる導入効果

- 改ざんを見据えた監視体制を構築
- 改ざん及び改ざん箇所の素早い特定
- 改ざん時に埋め込まれた不正コンテンツの復旧フローを確立
- 定期的な診断実施による安全確認効果

SQL INJECTION脆弱性診断

SiteLock

SQL INJECTION（インジェクション）脆弱性の有無を判定

機密情報を格納するデータベースは
狙われやすい

脆弱性の有無を調べる

SQLインジェクション脆弱性診断 <SQL INJECTION SCAN>
診断頻度: ワンタイム / 日 / 週 / 月 / 四半期

アプリに対する代表的な攻撃手法であるSQL インジェクション。データベース（DB）を不正に操作し、情報漏えいといった深刻な事故を引き起こします。脆弱性のない状態で維持し続けることは困難であることから、脆弱性の有無を定期的に診断しましょう。WordPressやMovable Typeといった主要CMSを利用したWebサイト、お問い合わせフォームや資料請求フォームのある企業サイト、ショッピングサイト等は、導入をお勧めいたします。

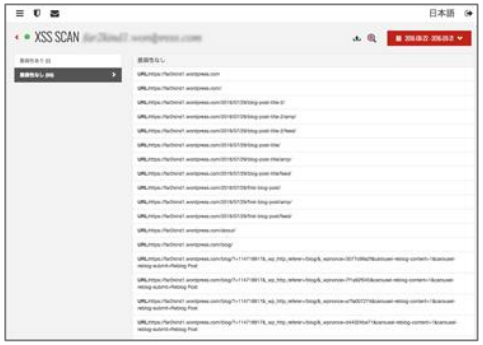
脆弱性が引き起こす被害例

- WordPressで運営するブログの改ざん
- ショップの会員データ、クレジットカード情報の漏えい
- 懸賞サイトの応募者情報漏えい
- Webサイトにマルウェアを埋められ、サイト被害者が感染、二次被害拡大へ

XSS脆弱性診断

SiteLock

XSS（クロスサイトスクリプティング）脆弱性の有無を判定



脆弱性のない
安全なWebサイトであることを監視

脆弱性の有無を調べる

XSS脆弱性診断 <XSS SCAN>
診断頻度: ワンタイム / 日 / 週 / 月 / 四半期

アプリに対する代表的な攻撃手法であるXSS。悪意のある第三者によってXSS脆弱性を攻撃されると、サイト訪問者に不利益をもたらす結果を招きます。被害を未然に防ぐためにも、XSS脆弱性のない安全なサイト管理にSiteLockをお役立てください。

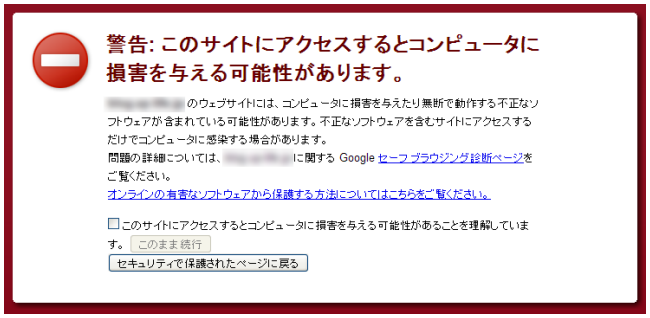
XSS脆弱性が引き起こす被害例

- お問い合わせフォームで入力された個人情報の不正搾取
- サイト訪問者を危険なフィッシングサイトへ誘導
- サイト訪問者のcookieを抜き取り、第三者による不正ログイン
  （例：オンラインバンキングやショッピングサイト等）

Webサイトのブラックリスト監視

SiteLock

有害サイトを集めたブラックリストへ登録されるリスクを警戒しよう



主要検索エンジンから
アクセスしないよう警告されるリスク

ペナルティによるアクセス遮断を防ぐ

マルウェア診断 <MALWARE SCAN>
診断頻度: 毎日

不正なマルウェア等を埋め込まれると、サイト訪問者に害を及ぼす危険な有害サイトとしてブラックリストに登録されるリスクがあります。一旦、登録されると検索エンジンからのアクセスを遮断されるなど悪影響を及ぼします。SiteLockは、Googleや主要セキュリティ会社が利用する主要なブラックリストを監視。登録された時は、いち早く通知いたします。

[ブラックリスト一覧] Google/Yandex/PhishTank/ANTI-VIRUS BLACKLIST/SiteLock

期待できる導入効果

- 主要検索エンジンや第三者に指摘を受ける前に自社で状態把握、素早く対処
- アクセス減による受注、お問い合わせの減少など、機会損失を抑制

メールのブラックリスト監視

SiteLock

スパムのブラックリストへ登録されるリスクを警戒しよう

取引先にメールを送信できない
リスクを警戒しよう

ペナルティによるメール遮断を防ぐ

スパム診断 <SPAM SCAN>
診断頻度: 毎日

メールの大量配信など迷惑メールの送信行為だと認定されると、悪質なスパム配信元としてお客さまのドメインがブラックリストに登録されるリスクがあります。一旦、登録されると該当ドメインからメールを送信できないなど悪影響が出ます。SiteLockは、主要なスパム配信元を集めたブラックリストを監視。登録された時は、いち早く通知いたします。

ブラックリスト登録が引き起こす被害例

- メールの配信到達率が大幅に低下
- メールを使えず、一般業務や営業活動の鈍化
- ペナルティ解除に必要な人、時間、手間といったリソース浪費

SSLサーバー証明書の監視

SiteLock

SSLによる暗号化通信を途切れなく継続しよう

有効期限切れを告げる警告メッセージが表示されます

SSL診断で証明書の期限切れを監視

SSL診断 <SSL SCAN>
診断頻度: 毎日

お客さまのWebサイトが、SSLによる暗号化通信によって保護されているか毎日診断します。また、更新月の前月（例：2/14更新なら1/14に通知）には、更新が迫っていることをお伝えするメールを送ります。安全な通信の有効性、SSLサーバー証明書を監視することで、更新忘れによる有効期限切れや設定ミスによるトラブルをいち早く把握し、対処できます。

期待できる業務改善＆導入効果

- 「人」や「記憶」に頼らないSSL監視体制を実現
- SSLサーバー証明書の更新前にリマインダー。有効期限が切れたら、いち早く通知
- 主要ブラウザや第三者による指摘を受ける前に自社で状態を把握、対処へ
- 有効期限切れで、Webサイトからの受注、お問い合わせ減少など機会損失を抑制

タイムリーなセキュリティ勧告

SiteLock

Webサイトに係るセキュリティ勧告を情報配信

注意喚起から緊急度の高い勧告まで
幅広く情報収集

タイムリーにセキュリティ情報を入手

アドバイザリー<ADVISORIES>
診断頻度: 毎日

SiteLockは、診断対象となるWebサイトの安全性に影響を及ぼす可能性のあるセキュリティ勧告を高・中・低の緊急度に振り分け、情報配信いたします。既知の脆弱性のあるプログラムやアプリケーションに対するバージョンアップ勧告など、管理者が独自に収集し、把握するには手間のかかるセキュリティ情報をSiteLock経由で集めることができます。

期待できる導入効果

- Webサイトに係る様々な緊急度のセキュリティ勧告を手間なく自動収集
- 使用中のプログラム、アプリのバージョン情報も楽々収集
- Webサイトを安全に管理する上で役立つ情報も入手可

安全性を可視化する安全シール

SiteLock

貴社の取り組みをサイト訪問者に伝えよう

掲載ページにタグを埋め込むだけ！

サイトに掲載できる安全シール

安全シール

お客さまのWebサイトの訪問者に対して、サイトの「安全・安心」を視覚的に伝える安全シールをご用意しています。日本語をはじめとする11ヶ国の言語から、自由に選択できます。また、シールの色、サイズもカスタマイズ可能です。

期待できる掲載効果

- サイトの安全性をわかりやすくアピール
- 企業のセキュリティの取り組みを可視化
- サイト訪問者の信頼獲得
- サイト離脱率、滞在時間の改善
- お問い合わせ・見積請求数の向上
- オンライン取引額の向上
- コンバージョン率（成約率）の向上

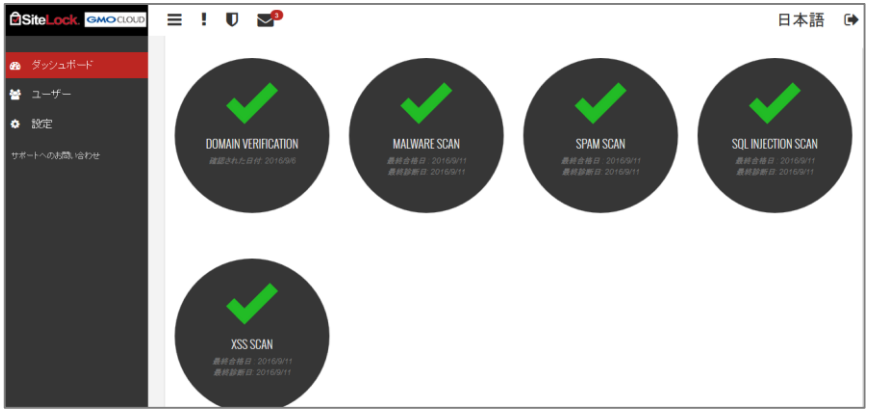
操作性に優れたコントロールパネル

SiteLockの設定から診断の履歴、結果閲覧まで一元管理

SiteLockを使いこなす便利ツール

コントロールパネル

インターネット経由でアクセス可能なコントロールパネルで、SiteLockの設定から診断履歴や結果の閲覧まですべて管理できます。PCはもちろん、スマホやタブレットなどモバイル端末にも対応。万が一の事故発生時には、いつでも迅速にアクセスして状況を把握できます。



インターネット経由でいつでもアクセス可能

シンプルな手順にそって簡単設定

プラン一覧 1/2

SiteLock

対象ページ、診断内容や頻度に応じて選べる4プラン

	エントリー	レギュラー	ビジネス	エンタープライズ
診断対象ページ	50ページ	200ページ	600ページ	2,000ページ
WordPress診断 （アプリ診断）	ワンタイム	週／月／四半期に1回		
アプリ＆ ホームページ診断	ワンタイム	週／月／四半期に1回		
XSS脆弱性診断	ワンタイム	週／月／四半期に1回	日／週／月／四半期に1回	
SQL インジェクション 脆弱性診断	ワンタイム	週／月／四半期に1回	日／週／月／四半期に1回	
マルウェア診断	毎日1回			

※ エントリープランを除き、お客さまで診断頻度を設定できます。ワンタイムと表示されている診断は、ご契約期間中、1回だけ診断可能です。
※ SMART診断のみ、当社指定のIPに対してFTP/SFTPポートを開く必要があります。

プラン一覧 2/2

SiteLock

対象ページ、診断内容や頻度に応じて選べる4プラン

	エントリー	レギュラー	ビジネス	エンタープライズ
マルウェア駆除	なし	日／週／月／四半期に1回		
SMART診断	なし	日／週／月／四半期に1回		
ブラックリスト監視	毎日1回			
スパム・ブラックリスト監視	毎日1回			
SSL診断	毎日1回			
アドバイザリー	なし	有		
安全シール	なし	有		

※ エントリープランを除き、お客さまで診断頻度を設定できます。

料金

SiteLock

月額350円から、手軽にWebセキュリティ対策をスタート

	エントリー	レギュラー	ビジネス	エンタープライズ
初期費用	無料			
月額換算	350円	1,200円	3,359円	8,300円
年額費用	4,200円	14,400円	40,311円	99,600円

※税抜表示

お支払い方法

1. 銀行振込
2. クレジットカード

VISA MasterCard JCB AMERICAN EXPRESS Diners Club International

契約期間

12ヵ月契約のみ

プラン変更

上位プランへ変更可能

診断対象

ご契約の1プランにつき、お客さまが管理されている独自ドメインまたはサブドメインを診断対象として登録できます。

お申し込み①

かんたん３ステップで、即日診断スタート

SiteLock関連URLのご案内

- お申し込み　https://order.saastart.jp/websecurity/
- お申し込みの流れ　https://saastart.jp/service/websecurity/
- ご契約前のよくあるご質問　https://support.saastart.jp/service/websecurity/faq/

お申し込み②<作業内容>

作業 ステップ	お客さまの 作業項目	お客さまの 作業内容	ご利用可能な機能
STEP1	お申し込み	診断ドメインのご入力	XSS脆弱性診断 SQLインジェクション脆弱性診断 マルウェア診断 ブラックリスト監視 スパム・ブラックリスト監視 SSL診断
STEP2	ドメイン認証	[方法①] 認証用METAタグのサイト埋め込み https://support.saastart.jp/service/websecurity/document/pdf/sitelock_domain_verification1_manual.pdf [方法②] 指定のhtmlファイルを登録ドメインの ルートディレクトリ配下にアップロー ド https://support.saastart.jp/service/websecurity/document/pdf/sitelock_domain_verification2_manual.pdf	WordPress診断 アプリ＆ホームページ診断
STEP3	FTPアカウント のご準備	FTPの接続設定 ※以下、P4-P9に記載 https://support.saastart.jp/service/websecurity/document/pdf/sitelock_control_manual.pdf	SMART診断 ※悪意のあるマルウェアを検知した場合、削除することが可能になります。

運用スタイルに応じて選べる３つの診断メニュー

SiteLock

人気 No.1

即日スタート！低料金で定期診断＆監視体制をらくらく実現

SiteLock

月あたり**350**円～

- 低料金、自社で始めるWebセキュリティ対策
- 簡単設定、定期診断＆監視を即日スタート
- 診断結果は、いつでも管理画面で確認可

詳細を見る

定期診断から報告書作成まで
24時間365日すべておまかせ運用

SiteLock

おまかせ定期診断

月**20,000**円～

- 定期的な診断＆監視は、おまかせ
- 24時間365日サポート体制で安心
- 毎月の診断結果報告書で安全確認

ワンショットでさくっと診断
診断結果は報告書で把握

SiteLock

ワンショット診断

1回**10,000**円～

- 1回だけ、さくっと診断
- 診断は、GMOクラウドにおまかせ
- 診断結果報告書で現状把握

よくある質問①

Q1	WordPressの診断対象範囲を教えてください。.htaccessファイルも対象になりますでしょうか？
A1	はい。WordPress本体のバージョンや脆弱性診断、加えてプラグインのコードレベルでの脆弱性診断も実施します。 htaccessファイルも対象になります。
Q2	SiteLockがページとカウントする条件は何でしょうか。
A2	Webページ数がカウントされます。 Webページに掲載されているリンクは契約ページ数としてカウントされませんが、リンク先が同一サイト内のWebページにリンクされている場合は契約ページ数としてカウントされます。 リンク先が外部サイトにリンクされている場合には、アクセス時にセキュリティの脅威があるかないかのチェック対象としてリストされますが、契約ページ数としてはカウントされません。
Q3	SMART診断につきましては登録ドメインに対し、ソースをみてリンクをすべて診断するような形でしょうか もしくはディレクトリー配下を徐々に診断してくような仕組みでしょうか。
A3	後者です。SMART診断はFTP接続により指定ディレクトリに移動し、Webサイトに関連する指定ディレクトリ配下のファイルすべてをスキャンします。また初回診断時以降は差分のみを対象とします。

よくある質問②

Q4	外部リンクの診断は行われるのでしょうか？
A4	外部リンクの診断も行います。 サイトからリンクされている外部リンクのマルウェア診断を行うことで、 リンク先の安全性を確認します。 なお、外部リンク先のページ数は契約数にカウントしません。
Q5	Windows Server 2008 r2でも診断できる認識でよろしかったでしょうか。
A5	FTP接続が出来れば診断可能ですので、プラットフォームに依存しません。
Q6	マルウェアスキャンの仕組みを教えてください。
A6	マルウェアスキャンは外部からウェブサイトをクロールし、ソースコード内のマルウェアシグネチャ、リンク、JavaScriptをチェックします。SiteLockは対象ソースコードと照合するため、既知のハッキング、脅威、シグネチャの大規模なデータベースを保持しています。マルウェアのスキャン自体は問題を解決するものではありませんが発見したページやページを警告します。 一方、XSSスキャンは、SQLインジェクションと同様、クロスサイトスクリプティング技術を使用して外部からサイトに侵入できるか試みます。サイトに侵入することができれば、その問題に関するダッシュボードに警告と助言を通知します。

よくある質問③

Q7	FTP接続についてIPによる接続制限を行っている場合がございます。（FWや.ftpaccess等） その場合に「SiteLock」からの接続については固定のIPからの接続となるのでしょうか？
A7	SMART診断の際のFTP/SFTPアクセスにつきましては、ご認識の通り固定IPアドレスからのアクセスとなります。 ただ、複数の診断サーバーがございますので、それぞれ許可追加が必要でございます。
Q8	スキャンサーバーによるサイトへの負荷は発生しますか？
A8	アプリ診断（APPLICATION SCAN）利用時は、SiteLockにて診断対象に対して擬似的な攻撃を行います。 この際、アクセスが一時的に増えるため、システム負荷が上がる可能性がございます。そのため、実施頻度を毎日、週1回から選べるようにしています。ただし、過去にアプリ診断によって、Webサイトやサーバーが不安定になるといった事象は報告されておりませんので、ご安心頂ければと存じます。
Q9	改ざん検知だけ（ファイル削除機能なし）の場合でも、外部からのFTPアクセスが必須でしょうか？
A9	はい。必須となります。 ハッシュ、サイズ、タイムスタンプを利用して、 追加・更新ファイルを検知しますので、 お客さまのファイル情報を取得する上で、FTPアクセスが必須となります。 FTPアクセスを必要としない、マルウェアスキャン、アプリケーションスキャンは悪意のあるマルウェアや脆弱性を診断・検知しますが、ファイルの差分情報を取得しておりませんので、改ざん検知を目的とした機能ではございません。

お問い合わせ

SiteLock

- SiteLock公式サイト（サイトロック）

SiteLock　GMO　検索

URL： https://www.saastart.jp/service/websecurity/

- お問い合わせ先

導入前のご相談、サービス仕様に関するご質問は、公式サイトの専用窓口よりお問い合わせください。

URL： https://www.saastart.jp/form/websecurity/contact/

記載されている内容は、2017年5月現在のものです。
最新の情報は、公式サイトをご確認ください。

GMOクラウドについて

GMOクラウド株式会社概要

代表者
青山 満
アオヤマ ミツル

社員**833**名 平成28年12月31日現在

本社　東京都**渋谷**区桜丘町26-1
セルリアンタワー

1993年 設立

クラウド・ホスティングサービスおよび**セキュリティサービス**を中核とした各種**インターネットソリューション**の開発・運用

東証一部
証券コード3788

情報セキュリティ国際規格
ISMS取得
2006年11月
より継続

24年にわたり13万社を超えるITインフラ導入実績

設立
1993

ホスティング
1996

クラウド本格参入
2011

インターネット黎明期 → 現在

24 年にわたるITインフラ運用・販売実績

国内最大級

13 万社を超えるお客さまの
ITインフラを支えています

レンタルサーバーからクラウドまで幅広いラインナップ

共用サーバー

専用サーバー

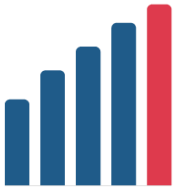
VPS

パブリック
クラウド

プライベート
クラウド

ハウジング

業務改善
Webマーケティング
ソリューション



ファイルサーバー

セキュリティ

導入コンサルから
初期構築・運用代行

SaaStart by GMO

クラウドにやさしさを、もっと

GMOクラウド

お客さまからいただく声が私たちの仕事の原動力です。
ひとりひとりがお客さまへの想いを寄せて、
クラウド・ホスティングサービスを提供しています。

サーバーというと無機質なサービスに思われるかもしれません。
ですが、スペック表だけでは比較できない、 人に寄り添ったサービスをお届けしたい。
みなさまのビジネスの支えになりたいと願っています。

GMOクラウドのサービス品質向上に対する取り組みやスタッフインタビューをご紹介しています

URL : https://brand.gmocloud.com/