GRED Webセキュリティ診断Cloud

完全自動化されたクラウドベースの継続的な脆弱性診断サービス

（ホワイトペーパー 2021年3月版）

SecureBrain

はじめに

脆弱性を悪用して企業から重要情報を窃取するサイバー攻撃があとを絶たない。その対策として、事前に脆弱性を診断し、攻撃を未然に防ぐ脆弱性診断が主流ではあるが、従来の脆弱性診断にはコストや工数の面で課題がある。そこで期待されているのが、脆弱性診断を定期的かつ自動で行う継続的な脆弱性診断サービスだ。本稿ではその代表的なサービスである「GRED Web セキュリティ診断 Cloud」を紹介する。

クラウド時代に狙われやすくなった Web サイトの脆弱性

脆弱性を悪用して企業から重要情報を窃取するサイバー攻撃があとを絶たない。IPA（情報処理推進機構）が公開している「情報セキュリティ 10 大脅威 2020（組織編）」によると、1 位から 10 位までの脅威のうち、脆弱性が一因となって引き起こされる脅威は、実に半数を超える。

具体的には「標的型攻撃による機密情報の窃取」「サプライチェーンの弱点を悪用した攻撃」「ランサムウェアによる被害」「インターネット上のサービスからの個人情報の窃取」「IoT 機器の不正利用」などだ。

脆弱性とは、製品やサービスにおけるセキュリティ上の弱点のことだ。今日の製品やサービスはさまざまなハードウェアやソフトウェアを組み合わせて構成されるため、脆弱性が潜むリスクは増加し続けている。

特に近年は、クラウドサービスの普及やコロナ禍による EC サイトの利用増などを受けて、Web サイト（Web アプリケーション）に潜む脆弱性が企業にとっての大きなリスクになってきた。Web サイトの脆弱性を突く攻撃は 1990 年代から存在するが、近年は攻撃がより高度化・巧妙化し、従来の脆弱性診断の手法やセキュリティ対策では対応しきれなくなっている。

実際「情報セキュリティ白書 2020」によると、脆弱性の報告件数は年々増加傾向にあり、2017 年以降は年間 1 万 4,000 件を超える規模で推移している。Web 関連の脆弱性も多く、1 日当たりの発生件数は 8 件を超えるほどだ。

そうした中で重要なのが Web サイトに潜む脆弱性を診断する「脆弱性診断」である。脆弱性診断はこれまで、製品やサービスの開発工程など限られたタイミングでしか行われてこなかった。しかし、Web サイトに対する脅威が大きなリスクとなる中、継続的に脆弱性診断を実施する必要性が高まっている。

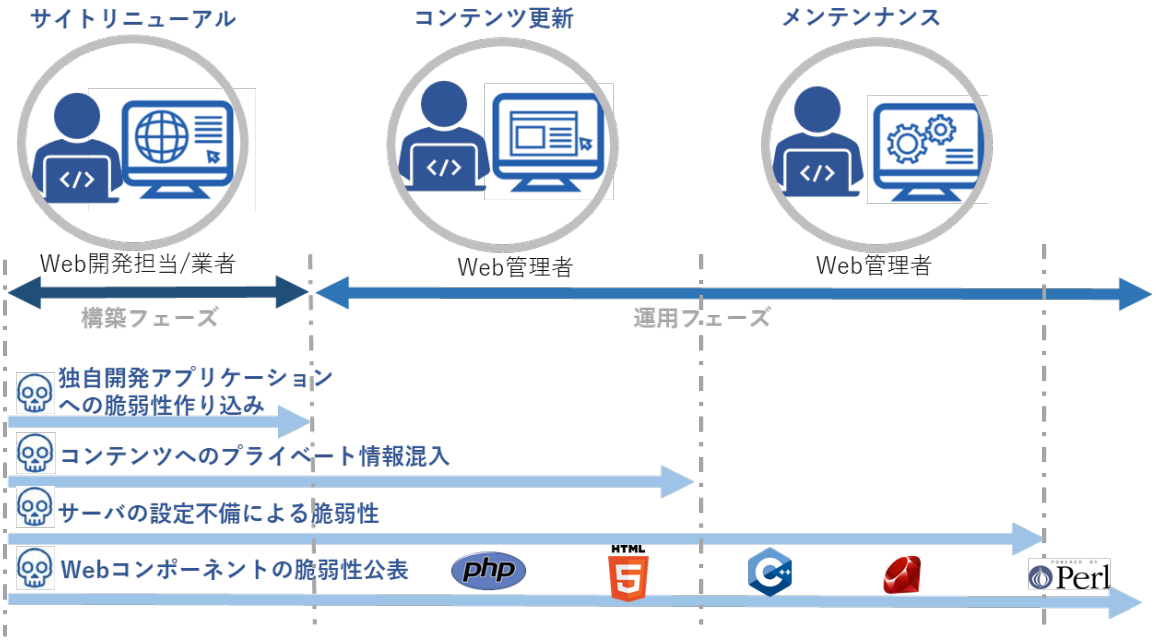
継続的に脆弱性診断を行うことで、製品やサービスを運用している期間も定期的に診断を行うことが可能になる。近年は完全自動で診断を行い、最新の脅威に対してもリアルタイムに対処できるサービスも登場している。Web サイトがビジネスにおいて不可欠になった今日、継続的な脆弱性診断サービスは、企業を脅威から守るために欠かせないサービスの 1 つともいえる。

従来の脆弱性診断がかかえる「コスト」と「工数」の問題

もともと Web アプリケーションに対する脅威は、Web サイトの登場以来、常に存在し続けてきたものだ。ただ、こうした脅威に対する従来の脆弱性診断は、「予防的」「事後的」な傾向が強かった。

予防的とは、Web サイトを作成する段階でどのような脆弱性があるかを調査し、必要に応じて解決策を講じるというものだ。しかしこの場合、Web サイトが公開されたあとにページが増えていくと、脆弱性の診断結果が無意味になってしまいやすい。

Web サイトのセキュリティリスク



また事後的というのは、実際に攻撃を受けたあとに、被害の影響や攻撃の要因を探るために行う脆弱性診断のことだ。診断結果を次の攻撃への対策に生かすことはできるものの、当然のことながら、すでに受けてしまった被害への対策にはならない。

一方で、WAF（Web アプリケーションファイアウォール）を使った Web サイトの保護も行われてきた。WAF は、XSS（クロスサイトスクリプティング）や SQL インジェクションなど、さまざまな Web 上の脅威に対抗できる。しかし WAF は、サイバー攻撃に対する対症療法的なセキュリティ対策でもある。WAF による防御だけでは、脅威の全体像を把握しにくい場合が多く、最新の高度なサイバー攻撃に対しては、十分に対抗できない場合もある。また、設定や運用の見直しにセキュリティ専門家の手が必要なことも課題になりやすい。

さらに、従来の脆弱性診断は、実施するために工数がかかることも課題となる。診断のためには、ベンダーのセキュリティ専門家による調査や確認、設定などが必要になるため、実施費用が高くなる。また、実施プロセスも複雑で期間も長期化しやすい。脆弱性診断を行う場合、一般的には「事前打ち合わせや調査」「診断」「分析とリスク評価」「レポート作成」というステップで進められるが、それぞれにおいて 1 カ月程度の時間とコストがかかる。最終的に脆弱性に対応できるのは半年から 1 年後というケースも少なくないのだ。

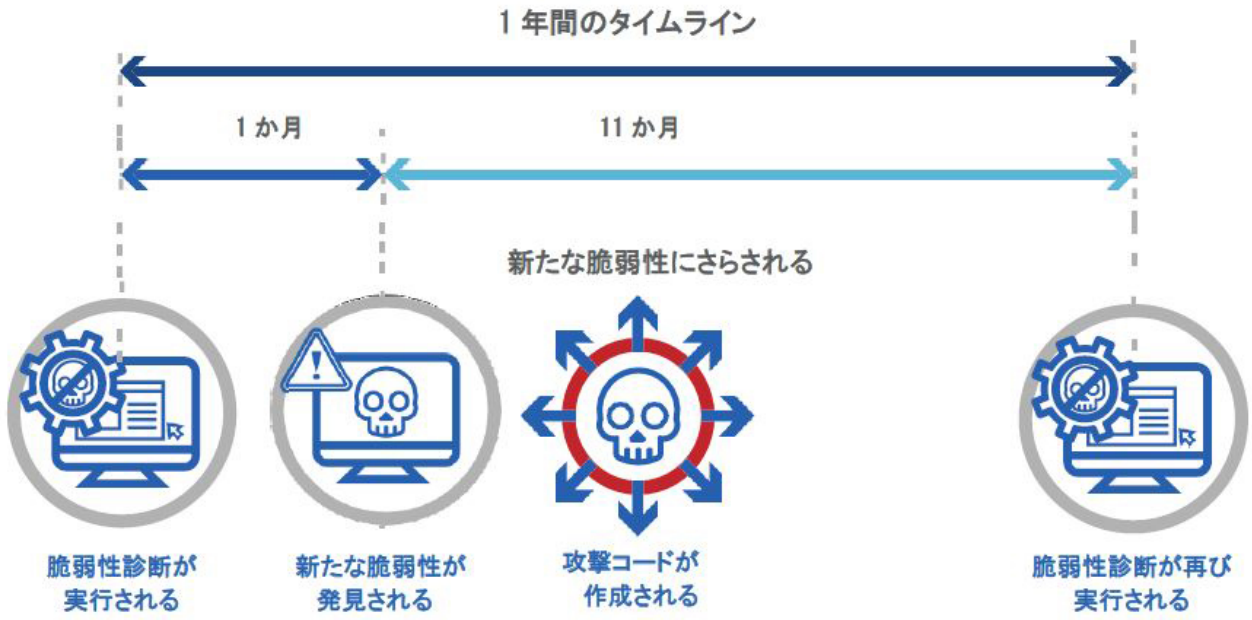
もちろん、従来の脆弱性診断にも多くのメリットがある。最大のメリットは、網羅的で徹底していることだ。セキュリティ専門家が調査や診断を行う場合、Web アプリケーションやプロセスの問題点を明確にできるため、その診断結果を活用することで、的確なセキュリティ対策を整備していくことにつながる。将来の攻撃に備えるプロアクティブ（事前対策的）なセキュリティ対策としては最適だろう。

なぜ継続的な脆弱性診断サービスが必要とされるのか

現在のサイバー攻撃は、こうした従来型の脆弱性診断だけでは、十分に対応できないケースが増えてきている。その理由の 1 つが、脆弱性の発見から攻撃までのタイムラインが短期化していることだ。脆弱性が発見されると攻撃コード（エクスプロイトコード）が作成されるが、その多くで、脆弱性の公表から 1 週間以内にインターネット上で攻撃通信が観測されている。これは、脆弱性情報が公表されて 1 週間後に攻撃が始まっているという意味であり、言い換えると、もし Web サイトに脆弱性が見つかった場合、すばやく対応しなければ攻撃を受ける可能性が高まるということだ。

また、脆弱性診断の実施数がそもそも少ないことも大きな課題だ。従来の脆弱性診断は、サービス開発時に 1 回、サービス開始後は年 1 回といった頻度でしか実施されていない。実施するためにコストや手間がかかるため、実施したくても実施できないという事情がある。しかし、新たな脆弱性が発見後、約 1 週間後には攻撃コードが作成されることをふまえると、1 年に 1 回の脆弱性診断では不十分である。

脆弱性発見から攻撃までのタイムライン



そこで有効な対策となるのが、継続的な脆弱性診断だ。脆弱性診断を月 1 回、週に 1 回といった頻度で実施することで、攻撃までのタイムラインの短期化や、診断実施数の不十分さを解決できる。

もっとも、継続的な脆弱性診断を行うためには、セキュリティ専門家による詳細な調査や、脆弱性に対する網羅的な診断が欠かせない。実施数をこなすために診断が簡潔になり、脆弱性を見つけることすらできなくなるのでは本末転倒だ。そのため、継続的な脆弱性診断には、セキュリティ専門家が行うような網羅的な診断ができること、人手をかけずに自動的に診断できること、月 1 回・週 1 回・毎日といった頻度で定期的に診断できることが必須といえる。また機能面でも、Web サイトの構成が変化しても診断できることや、最新の脅威に対応していること、脅威の全体像を把握できることなどが求められる。継続的な脆弱性診断は、従来の脆弱性診断を補完するものであり、双方をうまく使い分けることが重要になる。

NIST CSF や OWASP TOP 10 を活用し、運用上のリスクにも対応

脆弱性診断サービスを評価するうえで目安になるのが、対応しているセキュリティフレームワークやセキュリティ基準、診断項目などだ。

セキュリティフレームワークについては、業界で標準的に用いられているものに NIST（国立標準技術研究所）が定めるサイバーセキュリティフレームワーク（CSF）がある。「特定」「防御」「検知」「対応」「復旧」といった攻撃のフェーズごとに対策を講じるもので、現状のセキュリティ課題を明確化し、目標とする姿に向かって改善していくための方法論やアプローチが示されている。このほかにも、脆弱性管理のグローバル標準となっている CVE（共通脆弱性識別子）/CVSS（共通脆弱性評価システム）や PCI DSS などの規格などがある。

Web アプリケーションの脆弱性を診断する指標としては、セキュリティ民間団体 OWASP（Open Web Application Security Project Foundation）が公表している「OWASP TOP 10」がある。これは、悪用されやすいセキュリティリスクのランキングであり、最新版では「インジェクション」「認証の不備」「機密データの露出」「XML 外部エンティティ参照（XXE）」「アクセス制御の不備」「不適切なセキュリティ設定」「クロスサイトスクリプティング（XSS）」「安全でないデシリアライゼーション」「 既知の脆弱性のあるコンポーネントの使用」「不十分なロギングとモニタリング」を挙げている。

また、IPA でも「安全なウェブサイトの運用管理に向けての 20 カ条」として、Web アプリケーションのセキュリティ対策を挙げている。具体的には、「公開すべきでないファイルを公開していないか」「Web アプリケーションを構成しているソフトウェアの脆弱性対策を定期的にしているか」「Web アプリケーションのログを保管し、定期的に確認しているか」「インターネットを介して送受信する通信内容の暗号化はできているか」などだ。

脆弱性診断サービスを選定する際には、こうしたフレームワークや基準、ガイドラインにどのように準拠しており、サービスの中でどう活用できるかをチェックしておくことがポイントだ。

セキュアブレインが提供する「GRED Web セキュリティ診断 Cloud」

こうした要件を備え、おすすめしたい継続的な脆弱性診断サービスとして、セキュアブレインが提供しているクラウドサービス「GRED Web セキュリティ診断 Cloud」が挙げられる。「GRED Web セキュリティ診断 Cloud」の特長は、大きく 3 つある。

1 つめは、シンプルさと使いやすさだ。クラウド上に構築されたサービスが脆弱性診断を毎日定期的に実行し、その結果を簡潔でわかりやすいレポートとして自動的にまとめてくれる。レポートには、自社組織に対する多種多様な攻撃から Web サイトを保護するための対策まで記載されているため、ガイドにしたがって有効な防御手段を講じることが可能だ。

2 つめは、リードタイムの短さだ。多くの脆弱性診断サービスは、診断を実施しレポートを作成するまでに数カ月程度の期間を要する。これに対し、「GRED Web セキュリティ診断 Cloud」は対象の Web サイトの URL を登録するだけで、自動的にサイトの構造を解析し、適切な診断を実施してくれる。

3 つめは、費用対効果の高さだ。従来の脆弱性診断は、診断のために多くのコストがかかっていた。たとえば、診断のために事前に Web サイト内の構成やプログラムを調査したり、Web サイト内に特定のプログラムをインストールしたりする人手が必要となる。「GRED Web セキュリティ診断 Cloud」は、そうした調査や作

業が不要で、ほとんどの作業を自動化し、投資効果を高めることができるのだ。
また、「OWASP TOP 10」や IPA の「安全なウェブサイトの運用管理に向けての 20 カ条」が提示する重要な脆弱性を基準とした診断項目を 7 つに分類。Web サイトのリリース時のみならず運用上発生しうる脆弱性の検出に対応している。また、CVE/CVSS 情報を参照しながら、攻撃フェーズに応じた素早い診断が可能だ。

SaaS 型脆弱性診断サービスの特長比較

	刻目	GRED	製品A	製品B
1	対象者	Web管理者	NW/インフラ管理者	Web開発者
2	スケジューリング	有り	有り	無し
3	診断範囲/項目	△：Webアプリ ○：CMS ○：サーバー △：OS ×：NW	△：Webアプリ ×：CMS ○：サーバー ○：OS ○：NW	○：Webアプリ △：CMS ×：サーバー ×：OS ×：NW
4	対応規格	OWASP-10 CVE/CVSS	PCI-DSS CVE/CVSS	OWASP-10(一部)
5	特徴	定期的な診断に対応し、CMS等のWebコンポーネントとその脆弱性を診断可能	定期的な診断に対応し、複数NW機器に対する診断等、範囲や対象ともに広範囲	独自Webアプリのリリース前の診断を主対象としており、手動診断の簡易版

Web サイトの安全確保はビジネスを成長させるための投資

「GRED Web セキュリティ診断 Cloud」を導入し、日々運用するまでの流れは、以下の通り大きく 5 つのステップに分けられる。

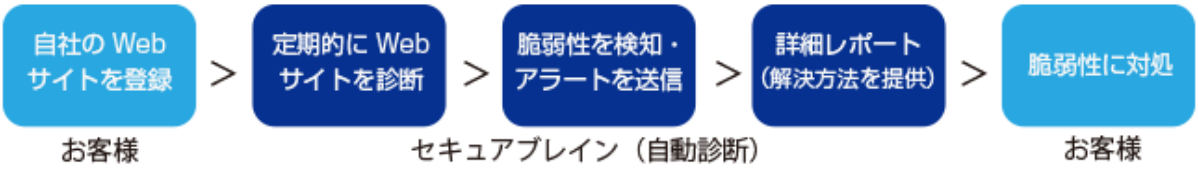
ステップ 1：URL の登録
「GRED Web セキュリティ 診断 Cloud」の Web ポータル上で、診断を行いたい自社の Web サイトのトップページの URL を登録すると、リンクから診断対象ページの URL （200 ページ）を自動的に収集する。

ステップ 2：日々の診断の実施
登録された Web サイトの情報を定期的にスキャンし、Web サイトに何か異常がないか、適切に保護されているかを確認し、すべてのリスクに迅速に対処する。

ステップ 3：アラートメールによる通知
Web サイトに対する脅威を検知した場合、Web サイトの所有者やシステム管理者に特定された脆弱性の詳細を示すアラートメールを送信する。

ステップ 4:診断レポートの作成
アラートメールに加えて、診断によって特定したリスクに関する詳細情報を提供する。このレポートには、検知した脆弱性への解決法も記載されている。

ステップ 5:脆弱性への対応
Web サイトの管理者は、脆弱性対策の推奨事項に従って、脅威に迅速に対応できるようになる。Web サイトの保護と攻撃によるビジネスへの影響を最小限に抑えることが可能だ。



診断方式は、システムが自動でスケジューリングし定期的に診断する「スマートスキャン」、月 5 回まで必要に応じて診断を行う「オンデマンドスキャン」の 2 種類で、提供価格は月 12 万 8,000 円から（年間 128 万円から）と、利用しやすい価格帯となっている。

継続的な脆弱性診断を高度なレベルで実現する「GRED Web セキュリティ診断 Cloud」は、Web サイトの安全を確保することで、結果的に組織のビジネス成長を大きく支援してくれることだろう。

セキュアブレインについて

約20年に及ぶ経験を積み重ねてきたセキュアブレインは、日本の大手セキュリティソフトウェアプロバイダとして認知されるようになりました。東京に本拠を置く当社は、国内外を問わずあらゆる種類の企業に多様なセキュリティ対策の選択肢を提供することを目指しています。

セキュアブレインは、Webサイトのマルウェア検知と保護において最先端の技術を提供するために、独自の研究センターを運営しています。当社の研究者チームは、オンラインWebサイトの新たなセキュリティリスクの特定と、現在と将来の脅威に対するソリューションの開発に専念しています。

株式会社セキュアブレイン
〒102-0094 東京都千代田区紀尾井町 3-12 紀尾井町ビル 7F
電話:03-3234-3001、FAX:03-3234-3002
e-mail: sales@securebrain.co.jp
https://www.securebrain.co.jp/

付録:
Web ポータルのスクリーンショット

■ダッシュボート TOP 画面

検知結果詳細

結果詳細

診断対象 TOP URL: http://

診断カテゴリ: 全カテゴリ

診断日: 2020/07/30

診断種別: スマートスキャン

リスクが検知された診断項目	検知件数		
	High	Medium	Low
パスワードの脆弱性	2	2	0
Webコンポーネントの脆弱性	7	31	0
サービスの脆弱性	0	2	0
不正な証明書	0	0	2
私的情報の公開	0	0	1
不要なサービスの起動	0	0	13

診断項目	パスワードの脆弱性
リスク	High
内容	脆弱なユーザ名やパスワードが設定されています。
影響	ユーザ名やパスワードが推測可能である場合、容易に本人になりすまして機微な情報にアクセスすることができます。
解決方法	adminやrootといった特定されやすいユーザ名を使用しないでください。また、パスワードは推測不可能なものを設定してください。10文字以上の長さ、英大文字小文字、数字が使われていることが望ましいです。
詳細	[URL] http:// username : user1 password : admin ---------- [URL] http:// username : root password : abc123

PDFレポートダウンロード　診断対象URL一覧ダウンロード

戻る


サイト設定
サイト設定
脆弱性診断の設定を行ってください。
診断対象 TOP URL
http://
オンデマンドスキャン破壊型診断
OFF
スマートスキャン
OFF
OFF
ログインフォームのあるURL(必須)
http://www.example.com/
Usernameに該当するパラメータ名(必須)
Username(必須)
ログイン認証
Passwordに該当するパラメータ名(必須)
Password(必須)
レスポンスに含まれるログイン済を示す文字列(必須※1)
レスポンスに含まれる未ログインを示す文字列(必須※1)
(※1)はどちらか一方を入力してください。
詳細設定...
ログイン認証設定の確認
保存

SecureBrain