

ツールと疑似攻撃で弱点をあぶり出す 項目を絞った廉価版も登場

「外部からの攻撃」に対して、自社のシステムはどれほど安全なのか。あるいは、どれほど無防備なのか。これをチェックしてくれるのが専門業者が提供する「セキュリティ診断サービス」だ。

編集部

SQLインジェクションによるデータベース改ざん、クロスサイトスクリプティングによる情報漏洩、セッション管理の不備によるなりすまし。企業のWebサイトが直面する脅威は増え続けている。もちろん多くの企業はすでに何らかの対策を講じているが、その堅牢度のレベルは客観的に判断しにくい。そこで検討したいのが、最新のセキュリティ動向に通じた外部の専門家の助けを借りることだ。

ベンダー各社は、Webアプリケー

ションにおける脆弱性の有無を検査・分析し、緊急度や対策法をアドバイスするサービスを展開している。その多くは、ツールを使ったソースコード解析と、技術者がWebサイトに疑似攻撃する手動診断を併用している。

一方、ツール診断に絞ったサービスもある。こちらは、大量のWebアプリケーションを短期間にチェックしたい企業に向くとと言える。

これらサービスの価格は数十万からと、決して安くはない。しかも、Webサ

イトの安全対策は費用対効果が見えにくいため、投資しづらいと感じている企業は少なくない。そうした企業に向けて、診断項目や対象を限定することにより価格を抑えたサービスも出てきている（表6-2）。SaaS型で診断サービスを提供するベンダーも登場した。比較的気軽に試せるこれらのサービスを利用して自社のWebサイトの現状をある程度つかんでから、より詳細な診断サービスを検討するといった使い方をするのもよいだろう。

表6-1 主なWebサイト脆弱性診断サービス

	サービス名/ベンダー	診断から報告までの期間	料金、その他
ツールと手動による診断	Webアプリケーションアドバンスド診断/アルファネット	1週間～	3URLまで25万円（税別）から。1URL追加ごとに5万円
	EINS/SVA+ / インテック	個別見積もり	1画面22万5000円から。認証などの手動診断は別途料金
	ウェブアプリケーションセキュリティ診断/インフォセック	1週間～	個別見積もり
	WebSiteScan Pro / インフォリスクマネージ	10日以内 (速報は3日以内)	1URL95万円～
	Webアプリケーション診断/ NRI セキュアテクノロジーズ	3営業日以内	5画面で164万円（税別）～
	NEC ActSecure セキュリティ診断サービス/ NEC	2週間程度	1サイト125万円～
	ちえっくME インスペクション (Webコンテンツ検査) / NTT-ME	約2週間	入力フォーム5ページ (50項目) で50万円から
	Webアプリケーション診断サービス/ NTTデータ・セキュリティ	10営業日～	個別見積 (サイトの規模などによる)。PCISSC ^{※1} の認定を受けている

	サービス名/ベンダー	診断から報告までの期間	料金、その他
ツールと手動による診断	Web脆弱性診断サービス Standard Plan / 京セラコミュニケーションシステム	20ページを診断した場合、2週間	1サイト147万円から。「Economy Plan」、「Advanced Plan」などもある
	Webアプリケーション脆弱性診断 by LAC / KDDI	約2週間	個別見積(サイトの規模などによる)。利用企業の要望に応じて、経営層向けの報告書も作成する
	ProactiveDefense Standard / 神戸デジタルラボ	1週間~	基本料金60万円のほか、1画面ごとに10万円。診断したWebサイトで半年以内に外部からの攻撃による漏洩などが起きた場合、診断費用を全額返金
	Webアプリケーション脆弱性検査(手動検査) / さくら情報システム	12営業日(25リクエスト ^{*2} の場合)	基本料金50万円のほか、1リクエストごとに12万円。ツール診断に絞った「スタンダード検査」もある
	Webアプリケーション診断 / JMCリスクソリューションズ	10画面で3日程度	基本料金40万円のほか、1画面あたり7万5000円
	セキュリティ脆弱性検査サービス / シマンテック	静的画面100ページの場合、約3週間	左記の条件の場合で500万円~。個別に脆弱性診断ツールを作成する。作成したツールは診断終了後に顧客に提供する
	Webアプリケーション検査 アドバンスド / 住商情報システム	2日~	1サイト150万円~。ツール診断を中心とした「スタンダード」もある
	Webアプリケーション診断サービス(ハイブリッド診断) / セコムトラストシステムズ	約5~8営業日	1サイト20画面の場合で95万円~。すべて技術者の手動による診断メニューも提供する
	脆弱性診断ライトプラン / ソフトバンク・テクノロジー	1週間~	5ページまでで40万円(サーバーやネットワークの脆弱性診断も含む)。診断対象のページ数が無制限の「スタンダードプラン」もある
	脆弱性検査サービス / ディアイティ	1週間以内(緊急報告は3営業日以内)	7ページで30万円~
	セキュリティ診断サービス 拡張診断Lv3 / 日立システムアンドサービス	標準で約2週間	IPアドレス5つ分で147万円(サーバーやネットワークの脆弱性診断も含む)
	SHIELDセキュリティ診断サービスWebアプリ診断スタンダード / 日立情報システムズ	3週間~	100画面まで84万円から。複数の診断ツールによる診断や侵入テストを含む「エンハンスト」、ツール診断に絞った「クイック」もある
	Webアプリケーションセキュリティ診断サービス / 富士通	2日間~	個別見積もり
	ウェブアプリケーション診断 / ベリサイン	1週間程度~	1画面5万円~、基本料金は個別見積もり
Webアプリケーション脆弱性検査 アドバンスド検査 / 三井物産セキュアディレクション	5日(10リクエスト ^{*2} の場合)	基本料金50万円のほか、1リクエストごとに12万円。ツール診断に絞ったスタンダード検査もある	
Webアプリケーション診断 / ラック	1週間	10画面で約130万円。より多くの項目を診断する「アドバンスド」、項目を絞った「ライト」がある	
主にツールを利用する診断	Webアプリケーション脆弱性検査サービス / NECネクサソリューションズ	50ファイルで約1.5か月	50ファイルで150万円~
	アプリケーションソースコード診断サービス / 三菱総研 DCS	6日間~	1言語50万行以内で120万円~

*1 PCISSC: PCI Security Standards Council (PCIDSSの推進協議団体) *2 リクエスト: ページ遷移の際にWebブラウザからサーバーへ送信されるhttpリクエスト

表6-2 検査項目や対象領域を限定し、価格を抑えたサービスが出てきた。SaaS型の診断サービスも登場

サービス名/ベンダー	サービス内容	料金
Webアプリケーション診断サービス / アルファネット	SQLインジェクションとクロスサイトスクリプティングに対する脆弱性の有無を診断する	3URLまで17万円(税別)。1URL追加ごとに3万円
WebSiteScan / インフォリスクマネージ	SQLインジェクションとクロスサイトスクリプティング、強制ブラウジングなどよく知られた脆弱性5項目をツールにより診断する	1URL19万8000円~
Web健康診断 / 京セラコミュニケーションシステム	SQLインジェクションやクロスサイトスクリプティング、クロスサイトリクエストフォージェリなど12項目について診断する。1サイト約10ページ程度の抜き取り診断	18万円(サーバーの脆弱性診断を含む)
Webセキュリティ診断・初診コース / ラック	SQLインジェクションとクロスサイトスクリプティングに特化して診断する	1ドメイン10URLまでで6万3000円。Amazonでも販売している
WebChecker / シーイーシー	SQLインジェクション、クロスサイトスクリプティング、OSコマンドインジェクションの危険性を診断するSaaS型サービス	1か月に1回の定期検査を実施する「定期Webアプリケーション検査」は年間24万円、単発の検査は1回につき8万円
gredセキュリティサービス / セキュアブレイン	SQLインジェクションなどによるWebサイトの改ざんの有無を、1日4~24回確認するSaaS型サービス。社内ネットワーク上で発見された不審ファイルを解析する機能も提供する	1か月3万円~