

高性能なツールでは不十分？ 身近になった脆弱性診断ツールがセキュリティ担当者を救う

April 2020

目次

▶ はじめに	3
専門家のサービスや高性能なツールだけではセキュリティを担保できない 疲弊するセキュリティ担当者 「小回りの効く」診断ツール VAddy どこで使える？ VAddy の活用例	
▶ Web アプリケーション脆弱性診断の種類と方法	8
動的解析（DAST）と静的解析（SAST） 動的解析ツール市場における VAddy の位置付け	
▶ クラウド型 Web 脆弱性診断ツール VAddy の解説	11
▶ 個別相談会のご案内	22

はじめに

近年増加している Web アプリケーションの脆弱性を突いた攻撃を未然に防ぐために、有効なセキュリティ対策として多くの企業が脆弱性診断の実施を意識するようになりました。しかし、現実にはセキュリティの専門家がいなかったり、セキュリティ対策予算が限られている企業がほとんどです。では、限られた条件の中でどう対処すればよいのか、これからの『脆弱性診断』の在り方について説明します。

従来の脆弱性診断サービスやツールの泣き所

Web アプリケーションの脆弱性診断を行う場合「**専門の診断会社（診断部門）による手動診断**」または「**専門家向けの診断ツールの利用**」が一般的です。

診断会社の手動脆弱性診断では事前のヒアリングで診断を実施する画面や機能を決定し、その後数日かけて専門家が手動で（一部ツールを使って）診断を行います。専門のセキュリティエンジニアが診断を実施するため、高い精度で脆弱性を検出できる反面、まとまった**規模の予算とスケジュールの確保**が必要です。

診断ツールを用いて社内で診断を実施する場合、高い専門性と経験を持ったセキュリティ担当者が在籍する限りにおいては高い精度で脆弱性を検出できますが、そうでない組織では**専任の担当者を新たに育成する必要があります**。また、ツール自体も高額であるため限定された数のライセンスを使い回すことになり、繁忙期で案件が重なる場合など、**ツール利用の順番待ち**が発生することもあります。

その結果、下記のようなプロジェクトの多くで脆弱性診断が実施されないままリリースされています。

過去に開発された古い Web サイト／Web サービス

→個人情報扱っているものの、利用者が減少しており**脆弱性診断費用の確保が難しい**

期間限定のキャンペーンサイト

→短期間のキャンペーンサイトは**脆弱性診断のスケジュールを確保できない**

小規模な制作会社が手掛ける小規模な Web サイト

→予算が少なく、**脆弱性診断費用は見込まれていない**。クリエイティブ系の制作会社では診断ツールを使える人材がいない

これまでの脆弱性診断ツールやサービスは幅広いアプリケーションや多くの診断項目に対応するため取り回しが悪く、結果として多くの Web サイト／Web アプリケーションにおいて最低限の診断すら実施できないというジレンマに陥っています。

しかしながら、顧客のセキュリティ意識がかつてなく高まっている昨今、こうしたプロジェクトにおいても脆弱性診断を要求されるケースが急増しており、**これまでのやり方とは異なる小回りの効く診断方法が求められています。**

はじめに 疲弊するセキュリティ担当者

セキュリティ担当者の業務範囲の 広がり

社内のセキュリティ担当部門の業務は Web サイト / Web アプリケーションのセキュリティ対策だけではなく、社内システム全体のセキュリティ対策はもちろんのこと、全社的なセキュリティポリシーの策定にも関わります。

昨今のセキュリティ意識の高まりや「働き方改革」を始めとする業務改革の機運のもと、**セキュリティ担当部門の業務範囲はかつて無いほど広くなり、かつスピードを求められるようになってきています。**それに加えて前頁のように今まで見過ごされていたプロジェクトでも Web アプリケーションの脆弱性診断を要求されるケースが急増し、**知識と経験を持つセキュリティ部門担当者が大量の診断依頼に翻弄される**ということが起きています。

非専任セキュリティ担当者の増加

本稿読者の方であれば御存知の通りセキュリティ人材不足も深刻になっており、それまで**セキュリティを担当してこなかった社内システム担当者が情報セキュリティ担当も兼ねる**というケースも多く耳にするようになってきました。しかしながら社内システムのセキュリティ対策全般を担当する中で、**高機能な脆弱性診断ツールを新たに習得するのは並大抵のことではありません。**

また、近年では「脆弱性診断の内製化」という言葉のもと、情報システム部門を中心に社内で脆弱性診断を実施するという動きが広まっています。メガベンチャーと呼ばれる企業の中には、**診断業務の一部を情報システム部門やセキュリティ部門から開発部門に移管しようと、開発チーム向けの脆弱性診断ツールのトレーニングを開催する**という動きもあります。

しかし、開発業務で多忙なアプリケーションエンジニアが診断ツールの習得に時間をかけるのは難しく、プロジェクトは難航していると聞きます。

このように、**情報セキュリティ対策に責任を持っている担当者達は業務範囲の広がりや案件数の急増に翻弄されるいっぽう、周辺部門の協力を得られず、疲弊し始めています。**

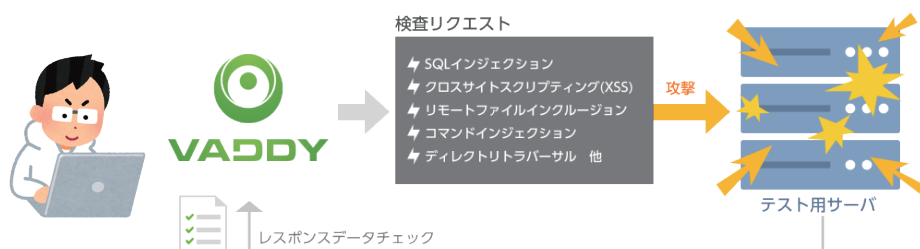
はじめに 小回りがきく脆弱性診断ツール VAddy

クラウド型 Web アプリケーション脆弱性診断ツール「VAddy」は**セキュリティ知識がない人でも手軽に毎日でも診断を実施できる**ことを目的として開発された純国産ツールです。

クラウド型ツールなのでソフトウェアを PC にインストールする必要がなく、Web ブラウザの操作ができる程度の IT リテラシーがある方であれば、サインアップ（アカウント作成）から最短 10 分程度で初回の診断を開始することができます。もちろん専門のトレーニングを受けていただく必要はありません。

突然の診断要請でも、セキュリティの専門家がいない現場でも、予算が限られたプロジェクトでも、VAddy なら今日から診断を開始できます。

VAddy はセキュリティ担当者の負荷を大幅に削減します。



はじめに どこで使える？ VAddy の活用例

開発中からプログラマー自身で診断

Web アプリケーションの開発を担当しているプログラマーが、自身が開発を担当した機能を自身で診断。アプリケーションの仕様を熟知したプログラマーだからこそ、漏れなく効率的な診断が可能になります。

QA（品質保証）担当者が診断

脆弱性もバグの一種という考え方のもと、QA 担当者がセキュリティテストを担当する事例が増えています。VAddy を使えばセキュリティテストの知見を持たない QA 担当者でも、通常の動作テストと同じ手順で脆弱性診断を実施できます。

制作会社の納品前診断

VAddy アカウント一つで同時に 3 つのプロジェクトを登録可能。例えば同時に 3 案件が並行して稼働している制作現場ではアカウント一つで全ての案件の納品前診断を実施できます。

CI ツールと連携して診断を自動化

VAddy では Command Line Tool を提供しているので、CircleCI や Jenkins などの CI ツールとの連携も簡単。単体テストから脆弱性診断までの一連の流れを自動化することができます。

受け入れ検査時に脆弱性診断

外部の協力会社／制作会社から納品物の受入検査時に脆弱性診断を実行。VAddy を使えばブラウザでの動作確認テストと同時に脆弱性診断を実行できます。担当者にセキュリティテストの専門知識は不要です。

手動脆弱性診断の補完として

定期的に手動脆弱性診断を実施している企業でも、対象の Web アプリケーションの全ての画面／機能を診断することはまれです。手動脆弱性診断でカバーできなかった画面／機能を VAddy で検査することで診断のカバレッジを大幅に向上させることができます。

Web アプリケーション脆弱性診断の種類と方法

Web アプリケーション脆弱性診断の種類と方法

動的解析（DAST）と静的解析（SAST）

Web アプリケーションの脆弱性診断手法は大きく以下の 2 つに分類されます。

動的解析（DAST）：動いている Web アプリケーションを外部から診断する手法

静的解析（SAST）：ソースコードなど Web アプリケーションの内部を診断する手法

※他に利用している OSS の脆弱性を解析するコンポジション解析（SCA）と呼ばれる方法もあります。

※手動脆弱性診断は動的解析の手法を取ることが大半です。

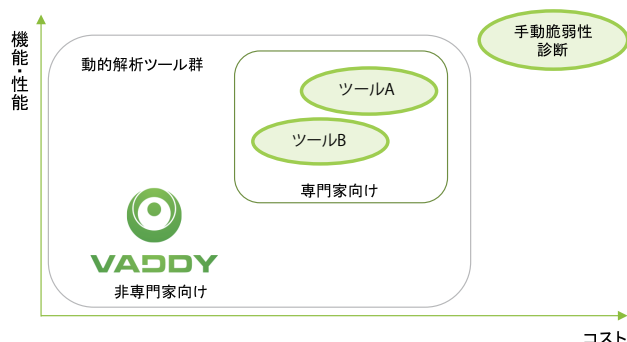
	メリット	デメリット	代表的なツール
動的解析	・実際に動いているアプリケーションに攻撃者視点で検査するため、検査精度が高い ・ソースコード非開示で検査でき、どの開発言語・フレームワークであっても検査可能 ・テスターは対象のアプリケーションで利用されている技術を理解している必要は無い	・ Web アプリケーションが動作していることが必要 ・脆弱性が検出された場合、原因となる箇所を特定することが難しい場合も	・  VADDY ・ VEX ・ AppScan ・ Burp Suite
静的解析	・アプリケーションが動作する前から診断できるため、開発の初期段階から実施が可能	・誤検知が多い ・検出された脆弱性が現実の脅威となりうるかの検証が必要 ・ツールによっては開発言語の制約がある	・ Fortify SCA ・ Coverity

いずれの診断手法にもメリット / デメリットがあり、組み合わせて使うとより効果が高くなります。

VAddy は動的解析型のクラウド型 Web アプリケーション脆弱性診断ツールです。

Web アプリケーション脆弱性診断の種類と方法

動的解析ツール市場における VAddy の位置付け



日本国内で提供されている主要な脆弱性診断ツール（動的解析ツール）は、主にセキュリティエンジニア向けに開発されています。

トレーニングを受けた専門家が利用することで、幅広い脆弱性を高い精度で発見することができます。

いっぽう **VAddy** はそうした専門家「以外」の方の利用を想定して開発されています。

	トレーニング	検査項目	想定利用者	提供形態	コスト
 VADDY	不要	少	開発エンジニア、QA 担当、情報システム部門、ディレクター、デザイナー	クラウド	年間 20 万円程度 / 150 ユーザー
ツールA	必要	多	セキュリティエンジニア	インストール	年間 200～300 万円 / ユーザー
ツールB	必要	多	セキュリティエンジニア	インストール（一部クラウド）	年間 200～300 万円 / ユーザー
手動脆弱性診断	-	-	-	-	数十万円～数千万円 / 回

クラウド型 Web 脆弱性診断ツール VAddy の解説

クラウド型 Web 脆弱性診断ツール VAddy の解説 特長

導入が容易

クラウド型サービスだから専用の端末を用意する必要はありません。Web ブラウザさえ入っていればどんな PC 環境からも診断が可能です。

また、専用のトレーニングも不要なので、Web サイトからサインアップして最短 10 分で初回の検査を実行することができます。

国内売上 10 年連続 No.1 WAF のノウハウ

クラウド型 WAF 国内売上 10 年連続 No.1 の「Scutum（スキュータム）」で観測されている実際の攻撃傾向を元に、検査項目と検査手法を設計。現実的な脅威に即した効率的な診断を確立しました。

それにより一回の平均検査時間 12 分という驚異的な検査時間を実現しています。

複数人でテレワークでも使える

VAddy にはチーム機能／組織管理機能といったコラボレーション機能を備えています。例えば Professional プランの場合は一つのアカウントを 150 人程度で利用することができます。

それぞれの参加者が在宅勤務であっても、別会社であっても、遠隔地に勤務していても全く問題ありません。

完全固定料金

VAddy は初期費用無料で、最低利用期間一ヶ月から使える完全固定料金制です。

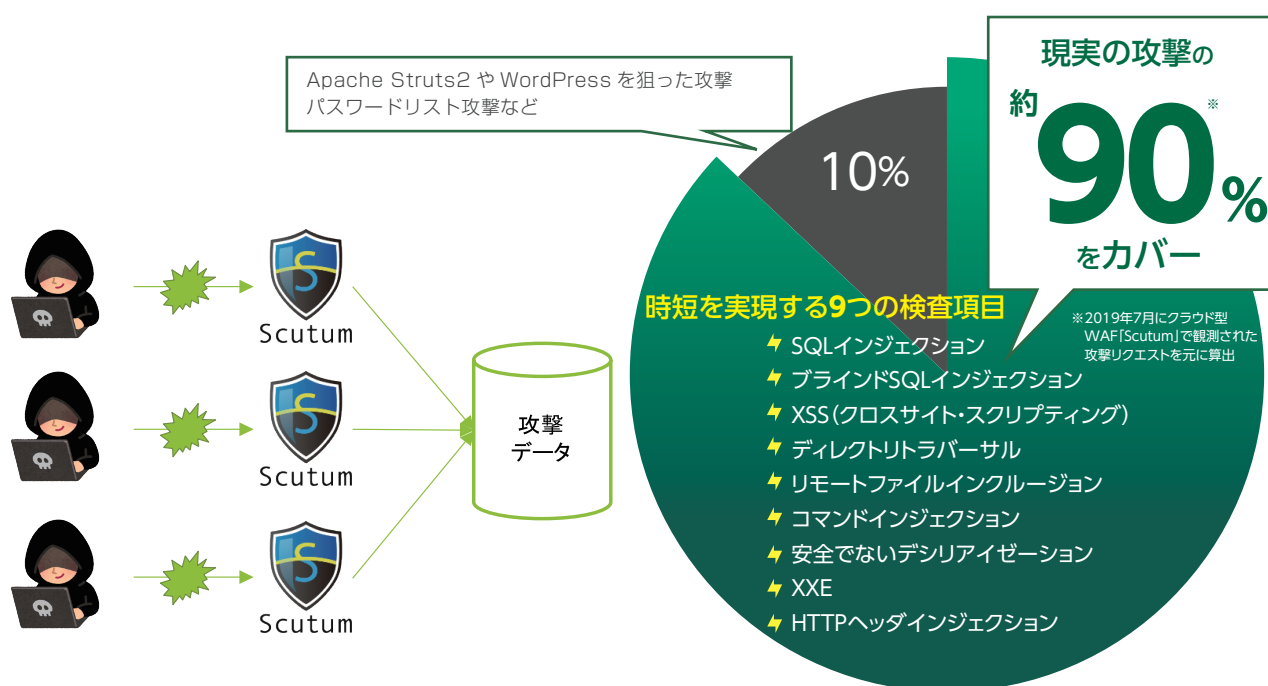
予算を気にすることなく、何度でも脆弱性診断を実施できます。

クラウド型 Web 脆弱性診断ツール VAddy の解説

9つの検査項目

クラウド型WAF国内売上10年連続 No.1*「Scutum」で

観測された攻撃データを元に検査項目を決定



「Scutum」は2009年のサービス開始より

金融機関、公的機関、教育機関などを含む多数のWebサイトで幅広く導入いただいております。

10年連続で国内クラウド型WAF市場シェアNo.1*を獲得しています。

*2010年度から2019年度のクラウド型WAF市場（ミック経済研究所 ほか）



Scutum

* 株式会社ビットフォレストが開発／運用を行っているクラウド型WAFサービス「Scutum」で
2017年1月に観測された攻撃リクエストを元にVAddyの検査項目は作成。

<https://www.scutum.jp/>

クラウド型 Web 脆弱性診断ツール VAddy の解説

検査内容

検査内容

VAddy ではお客様が事前に登録したクロールデータ（URL、パラメータ等）を元に検査を実行します。
パラメーターや URL パスなどに検査リクエストを送信し、Web アプリケーションからのレスポンスの内容を元に脆弱性の有無を判定する「動的解析」を行います。

診断項目	診断方法
SQL インジェクション	SQL 文として特別な意味を持つ文字を検査対象のパラメータに送信して Web アプリケーションの挙動を解析します。
ブラインド SQL インジェクション	外部から SQL インジェクションの有無が判定しにくいアプリケーションでも、特定の SQL 関数を検査対象のパラメータに送信して解析します。
コマンドインジェクション	特定のコマンドを検査対象のパラメータに送信して Web アプリケーションの挙動を解析します。
HTTP ヘッダインジェクション	改行コードを含めた文字を検査対象のパラメータに送信して、HTTP レスポンスヘッダの中で不要な改行が発生していないか解析します。
クロスサイトスクリプティング (XSS)	検査用の JavaScript コードを検査対象のパラメータに送信して HTTP レスポンスの内容を解析します。
リモートファイルインクルード (RFI)	リモートコード呼び出しのコードを検査対象のパラメータに送信して、外部サーバのコードが呼び出されていないか挙動を解析します。
ディレクトリトラバーサル	任意のファイルパスを検査対象のパラメータに送信して、非公開のファイルが読み込まれないか解析します。
安全でないデシリアライゼーション	シリアライズされたデータを処理するアプリケーションに、検査用のシリアライズデータを送信して任意のコードが実行されないか挙動を解析します。
XML 外部実体攻撃 (XXE)	XML を受付けるアプリケーションに検査用の XML データを送信して任意のコードが実行されないか挙動を解析します。

クラウド型 Web 脆弱性診断ツール VAddy の解説

ほぼ全ての Web アプリケーションを複数ユーザーで検査

検査可能な Web アプリケーション

検査対象のアプリケーションに制限はありません。ほぼ全ての Web アプリケーションが検査対象です。

動的解析型の診断ツールなので、対象のアプリケーションで使われている言語／フレームワーク／ミドルウェアの制限はありません。

検査可能な Web アプリケーション
フォーム認証
SSO 認証
REST API サーバー
CSRF 対策トークンを含むアプリ
VIEW_STATE を利用したアプリ
複数の FQDN をまたぐアプリケーション
ローカル環境／イントラネット上のアプリケーション

対応していない Web アプリケーション
第三者がホストする認証基盤を利用したアプリケーション
第三者がホストする Web サービス
二要素認証を利用するアプリケーション

コラボレーション機能

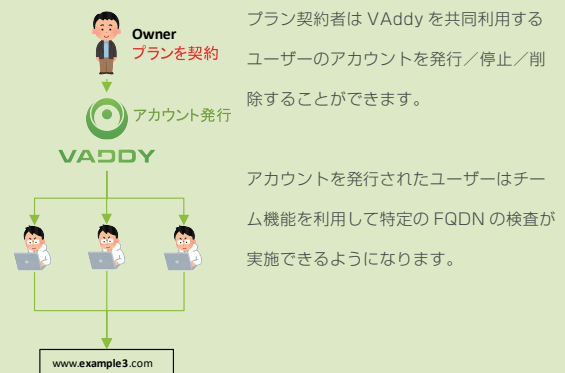
VAddy ではチーム機能／組織管理機能と呼ばれるコラボレーション機能を提供しています。

1 契約あたり検査対象のサーバーを 3FQDN まで同時登録可能。登録されたサーバーには **5 人以上**の共同作業者を登録できます。

チーム機能 利用例（Professional プラン）



組織管理機能 利用例（Enterprise プラン）



クラウド型 Web 脆弱性診断ツール VAddy の解説

その他機能とセキュリティ対策

その他の機能

プライベートネット機能

Professional プラン以上で無償提供している VAddy for PrivateNet CLI tool を使えば、イントラネット内やローカル PC 内の Web アプリケーションも検査が可能です。

Web API とコマンドラインツール (CLI)

全てのプランで VAddy の Web API とコマンドラインツールをご利用いただけます。WebAPI から検査の実行や確認ができますので、例えば cron でコマンドラインツールを実行すれば毎日の定期診断が手軽に実現できます。

CI 連携

Jenkins、CircleCI、TravisCI などの CI とも手軽に連携可能です。Jenkins の場合は VAddy プラグインを Jenkins にインストールすることで、それ以外の CI の場合は VAddy コマンドラインツールを実行するだけで自動診断環境を構築できます。

レポートダウンロード

Professional プラン以上をご利用のお客様は PDF ダウンロード機能をご利用いただけます。

セキュリティ対策

Web Application Firewall で保護

VAddy サーバーは自社のクラウド型 WAF「Scutum」で保護されています。

管理画面へのログインには 2 要素認証

VAddy 管理画面へのログイン時に 2 要素認証を設定することが可能です。

常に最新版の OS / ライブラリを利用

VAddy で使われている OS / ライブラリ / フレームワークなどは全て最新版が使用されています。使用しているツールにセキュリティパッチが提供された場合は、即時適用しています。

お客様情報にアクセスするスタッフの制限

お客様の個人情報および利用状況データにアクセスできるスタッフは制限されており、スタッフの操作ログは常時取得しています。

クラウド型 Web 脆弱性診断ツール VAddy の解説

サポート体制

サポート体制

脆弱性診断ツールを初めて使う方のために、複数のサポート窓口を用意しています。
ご質問の内容や緊急度に合わせてお選びください。

チャット



操作中に困ったときは！
平均 1 分 40 秒で対応

サポート



営業時間内のご質問は
当日回答 100%

個別相談会



操作デモもご覧になれます。
在宅勤務の方や遠方の方はオンラインでも OK

クラウド型 Web 脆弱性診断ツール VAddy の解説

料金体系（基本プラン）

料金体系(基本プラン)

		手軽に脆弱性検査をはじめてみるなら	VAddyの基本機能が全て使える	組織管理機能追加と 検査内容を大幅強化
		Starter 月額 ¥6,000	Professional 月額 ¥19,800	Enterprise 月額 ¥59,800
検査項目 チーム機能	SQLインジェクション	○	○	○
	ブラインドSQLインジェクション			○
	XSS	○	○	○
	RFI		○	○
	コマンドインジェクション		○	○
	ディレクトリトラバーサル		○	○
	安全でないデシリアイゼーション			○
	XXE			○
	HTTPヘッダインジェクション			○
チーム機能	チームメンバー	5ユーザー／FQDN	50ユーザー／FQDN	無制限／FQDN
組織管理	組織メンバー			30ユーザー
機能	スキャン回数	無制限	無制限	無制限
	スキャン上限時間	30分／回	2時間／回	5時間／回
料金	スキャン履歴	過去1年分	過去2年分	過去2年分
	ローカル環境への検査		○	○
	レポートダウンロード		○	○
	検査対象FQDN	3	3	3
	基本利用料	月額 ¥6,000	月額 ¥19,800 年額 ¥198,000 年額だと2ヶ月分お得	月額 ¥59,800 年額 ¥598,000 年額だと2ヶ月分お得
	FQDN追加	月額 ¥2,000／FQDN	月額 ¥6,000／FQDN 年額 ¥60,000／FQDN 年額だと2ヶ月分お得	月額 ¥10,000／FQDN 年額 ¥100,000／FQDN 年額だと2ヶ月分お得
	組織メンバー追加			月額 ¥15,000／10ユーザー 年額 ¥150,000／10ユーザー 年額だと2ヶ月分お得
お支払い方法		クレジットカードのみ	クレジットカード 銀行振込(請求書発行)	銀行振込(請求書発行)

※価格は税別です。

クラウド型 Web 脆弱性診断ツール VAddy の解説

料金体系（脆弱性診断会社サポート付きプラン）

		Professional + 年額 ¥598,000	Enterprise + 年額 ¥998,000
VAddy 年間ライセンス		Professional	Enterprise
診断チケット		20 チケット	20 チケット
料金	基本料金	年額 ¥598,000	年額 ¥998,000
	追加診断チケット	150,000 円 / 10 チケット	150,000 円 / 10 チケット
お支払い方法		銀行振込	銀行振込

※価格は税別です。

VAddy の基本プラン（年間ライセンス）に、セキュリティ対策のエキスパート「**SHIFT SECURITY**」によるサポートが付いたプランです。

Professional + / Enterprise + プランに付属する診断チケットは、

OWASP TOP10* に準拠した手動脆弱性診断の他、プラットフォーム診断、脆弱性対応サポートなど幅広い用途でご利用いただけます。

*OWASP TOP10

米国の NPO 団体、OWASP (Open Web Application Security Project) が四年に一度発表している「最も重大なウェブアプリケーションリスクトップ 10」

脆弱性診断・検査といえは



OWASP TOP 10 2017
A1: インジェクション
A2: 認証の不備
A3: 機微な情報の露出
A4: XML 外部エンティティ参照
A5: アクセス制御の不備
A6: 不適切なセキュリティ設定
A7: クロスサイトスクリプティング
A8: 安全でないデシリアライゼーション
A9: 既知の脆弱性のあるコンポーネントの使用
A10: 不十分なロギングとモニタリング

クラウド型 Web 脆弱性診断ツール VAddy の解説

導入企業（一部）の紹介と実際にご利用いただいた方からの声

導入企業（一部）



実際にご利用いただいた方からの声

開発エンジニアでなくても使える

弊社ではツールでの診断を QA チームで実施することが大前提でしたので、VAddy に関しては **開発エンジニアでなくても使える**という点が最大のポイントでした。

属人的な対策から仕組みの対策へ

現在弊社では **VAddy を使った脆弱性検査**を全ての**案件の納品前に実施**するようにしています。これまで個々のエンジニアのスキルに依存する側面があったソースレビューの後に VAddy の検査を入れることで、**属人的な対策から仕組みとしての対策に移行できている**と考えています。

開発チームの負担にならないツール

客観性がありなおかつ開発メンバーの負担が少ないやり方を模索する中で VAddy に出会いました。VAddy のように**開発のスピードを損なわず**、開発チームの負担にならないツールはあまり無かったと思います。特に**クラウド型の診断ツールは他には見つけられませんでした**。

セキュリティ対策は「何層にも継続的に」

今までもセキュリティ対策はやっていましたが、必ずしも十分ではありませんでした。きちんとした枠組みを作り「**何層にもそして継続的に**」これが非常に大切だと考えており、そうした体制を作っています。

クラウド型 Web 脆弱性診断ツール VAddy の解説

販売パートナー募集

販売パートナー

VAddy では継続して販売パートナープログラムへの参加を募集しております。

販売代理店、取次代理店にご興味がある方は info@vaddy.net までご連絡ください。



有限会社アリウープ

販売代理店 取次代理店



ALH株式会社

販売代理店



株式会社セキュリティア

販売代理店 取次代理店



株式会社フラッグシステム

取次代理店



株式会社セキュアスカイ・テクノロジー

販売代理店



株式会社ビヨンド

販売代理店 取次代理店



株式会社ネットフォレスト

取次代理店



株式会社SHIFT SECURITY

手動診断パートナー

個別相談会のご案内

個別相談会のご案内

VAddy の利用をご検討されている方向けに個別相談会を開催しています。
本稿で紹介できなかった他社の導入事例などもお話しします。

「お客様から脆弱性診断についてのお問い合わせが増えてきたけど、何から始めていいかわからない」
「もともと脆弱性診断は行っていたけれど予算の見直しを検討中」
「実際に他社はどのような脆弱性診断を行っているのか教えてほしい」 など
お客様のご要望に合わせた内容で開催します。

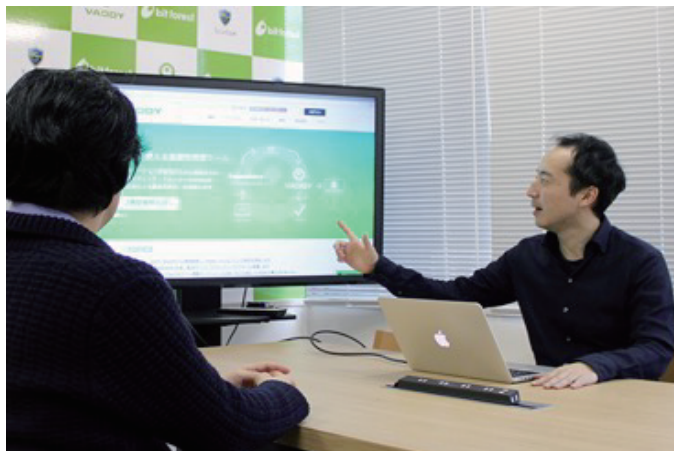
コンテンツ例

VAddy の基本的な機能や操作方法のご説明
他の診断ツールとの比較
手動脆弱性診断との比較
効果的な利用方法
診断サービス／ツールの組み合わせ例
導入事例

開催場所

ビットフォレスト東京オフィス
ビットフォレスト福岡オフィス
オンライン（Skype、Zoom など）

お申し込みは [Web サイト](#)から



クラウド型 Web アプリケーション脆弱性診断ツール VAddy

VAddy お問い合わせ先／会社概要



VAddyに関するお問い合わせ

☎ **03-5577-2032**

受付時間 平日 10:00～18:00

✉ info@vaddy.net [@vaddynet](https://twitter.com/vaddynet)

株式会社ビットフォレスト

VAddy事業部 (担当: 西野・市川)

VAddyブログ

<https://blog-ja.vaddy.net/>

VAddyサイト

<https://vaddy.net/ja/>



株式会社ビットフォレスト

東京本社

東京都千代田区神田錦町 1-17-5 神田橋 PR-EX 8F

TEL : 03-5577-2032 FAX : 03-5577-2034

福岡オフィス

福岡県福岡市中央区天神 2-14-35

野村不動産天神ビル 4F



Scutum



VADDY

株式会社ビットフォレスト

「Web アプリケーションセキュリティサービスの開発・販売」

<https://www.bitforest.jp/>

業務内容

国内売上 10 年連続 No.1 クラウド型 WAF「Scutum」の開発・運用
クラウド型 Web 脆弱性検査サービス「VAddy」の開発・運用・販売

沿革

2002 年 2 月 有限会社ビットフォレストとして設立

2007 年 1 月 株式会社ビットフォレストに商号変更

2009 年 6 月 Scutum 販売開始

2015 年 9 月 VAddy 販売開始