

クラウド型Webアプリケーション脆弱性診断ツール

VAddy - バディ -

Webアプリケーション脆弱性診断をすべての人へ



運営会社紹介／沿革／業務内容

運営会社紹介

株式会社ビットフォレスト

所在地	[東京本社] 東京都千代田区神田錦町1-17-5 Daiwa神田橋ビル 8F
	[福岡オフィス] 福岡県福岡市中央区天神4-6-28 天神ファーストビル 6F
代表者	代表取締役 高尾 都季一

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
2024年10月	Loggol販売開始

業務内容

リアルタイムに防御する

- クラウド型Webアプリケーションファイアウォール
「**Scutum**」の開発・運用
<https://www.scutum.jp/>



事前に防御する

- クラウド型Web脆弱性診断ツール
「**VAddy**」の開発・運用・販売
<https://vaddy.net/ja/>



現状を正しく把握する

- Web攻撃ログ分析ツール
「**Loggol**」の開発・運用・販売
<https://www.loggol.jp/>



VAddyとは？

2015年に製品化された、もっとも手軽で高速な
ブラックボックス型Web脆弱性診断ツールです。



レスポンスデータチェック

診断リクエスト

- SQLインジェクション
- クロスサイトスクリプティング (XSS)
- リモートファイルインクルージョン
- コマンドインジェクション
- ディレクトリトラバーサル 他



攻撃



テスト用サーバ

こんな方々にご利用いただいています

開発部門

品質管理部門

インフラ部門

情報システム部門

こんな場面にご利用いただいています

開発途中で診断

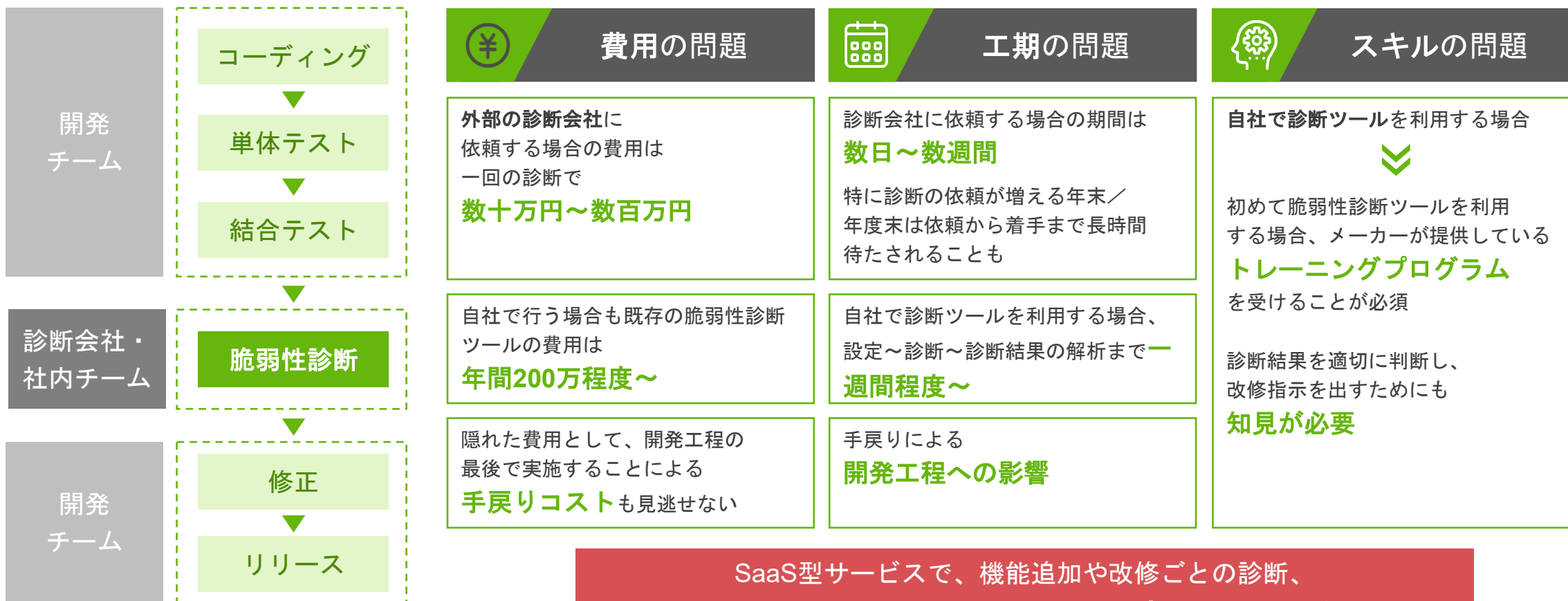
受け入れテスト時に診断

納品／リリース前に診断

毎日の定期診断

これまでのWebアプリケーション脆弱性診断の課題

通常、脆弱性診断は全ての開発工程が終了した後に、
外部の診断会社や社内のセキュリティ部門（品質管理部門）で実施されます。

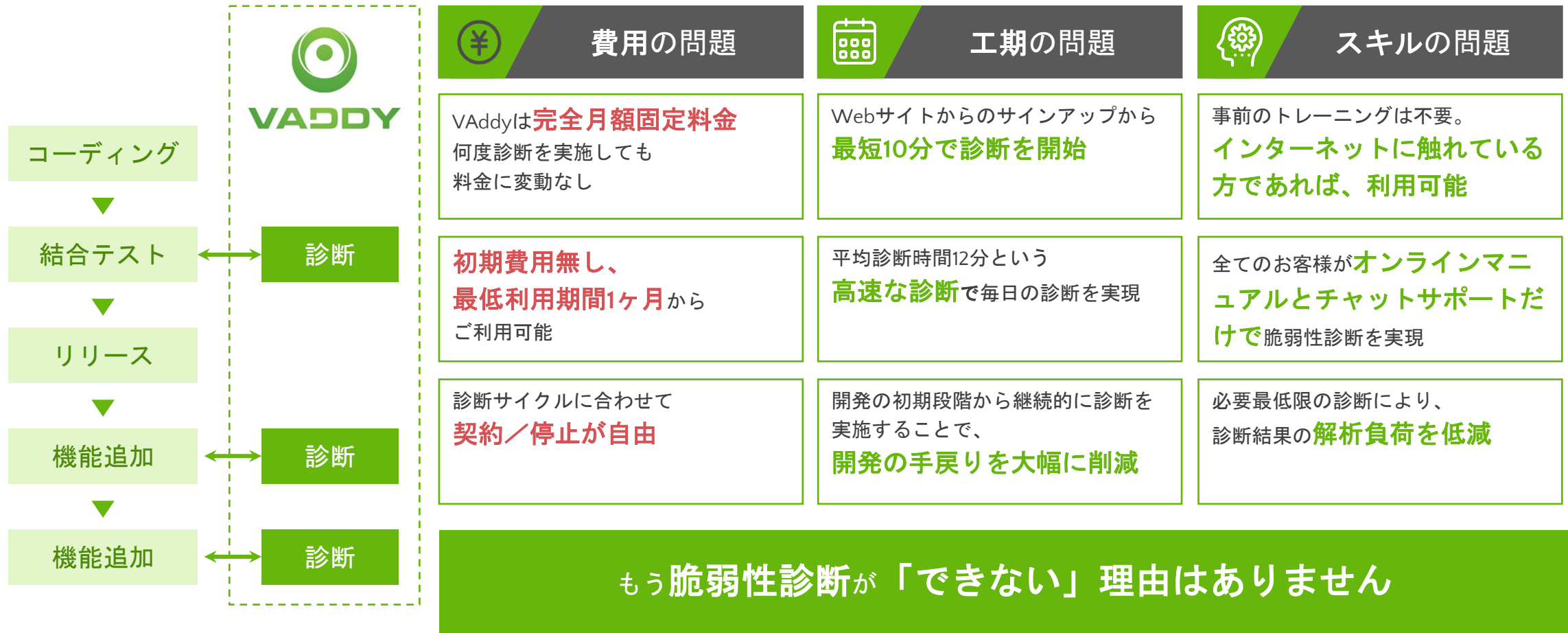


SaaS型サービスで、機能追加や改修ごとの診断、
小規模プロジェクトでの脆弱性診断は**事実上不可能**

Webアプリケーション脆弱性診断を全ての人へ

開発の初期段階から**何度でも**。

費用やスケジュールを気にすること無く脆弱性診断を実施できます。



最低限の工数でIPA基準+αの脆弱性を診断

Webアプリケーション

フレームワーク

ミドルウェア

OS

サーバー

ネットワーク

VAddy Advancedプランの診断項目(18個)

情報処理推進機構 (IPA)

安全なウェブサイトの作り方チェックリスト

- SQLインジェクション
- ブラインドSQLインジェクション
- クロスサイト・スクリプティング
- コマンドインジェクション
- ディレクトリトラバーサル
- HTTPヘッダインジェクション
- CSRF
- メールヘッダインジェクション
- クリックジャッキング
- バッファオーバーフロー
- セッション管理の不備
- アクセス・認可制御の不備

実際に観測される攻撃の上位から選定された基準

- リモートファイルインクルージョン
- 安全でないデシリアイゼーション
- XXE
- SSRF脆弱性
- 非公開ファイル検査
- evalインジェクション

+

IPAのチェックリストに実際の攻撃データから選定された診断項目を追加

市場における手動脆弱性診断と診断ツールの位置づけ

診断内容

自動診断ツール製品群

開発／情シス／QA向け



年間20万円～／ライセンス

セキュリティエンジニア向け

他社A

他社B

年間200～300万円／ライセンス

手動脆弱性診断

100万円～／回

費用

診断できる環境、組織管理機能

診断できる環境、アプリケーション

- ・ フォーム認証（ログイン画面）を含むアプリケーション
- ・ SSO（Single Sign On）を利用するアプリケーション
- ・ 複数のFQDNをまたぐアプリケーション
- ・ REST APIサーバ
- ・ SPA
- ・ URLパスに含まれるパラメータ
- ・ CSRF対策トークンを含むアプリケーション
- ・ イン트라ネット内や開発PC上のアプリケーション (1FQDN のみ)

診断例

例えば、診断したいURLが下記の場合

<http://example.com/search.php?keyword1=foo&keyword2=bar>

keyword1のデータ foo を検査用のデータに差し替えて検査対象サーバに送ります。そのレスポンスの状況を確認して、脆弱性の有無を判定します。

<http://example.com/search.php?keyword1=foo&keyword2=ba>

<http://example.com/search.php?keyword1=foo<script>vaddy</script>&keyword2=bar...>

keyword1の検査が完了した後に、同じようにkeyword2に対しても検査を実行します。

組織管理機能

共同利用する**ユーザーを一元管理**することができます。
自社社員の「誰がどのように」VAddyアカウントを利用しているかをひと目で把握できます。

Advanced / Enterpriseプラン

組織メンバー

ご利用メンバー数 10, 上限人数 20

組織権限	ログインID	名前	メール	部署	電話番号	言語	ステータス	2段階認証	API利用	作成日	操作
Member	user1	ユーザー太郎	user1@vaddy.net			日本語	利用中	OFF	OFF	2018/03/26	編集
Owner	user2	市川	user2@vaddy.net			日本語	利用中	OFF	ON	2019/05/11	
Member	user3	市山	user3@vaddy.net			日本語	利用中	ON	OFF	2019/08/27	編集
Member	user4	市原	user4@vaddy.net			日本語	利用中	OFF	OFF	2019/08/27	編集
Co-Owner	user5	市谷	user5@vaddy.net			日本語	利用中	OFF	OFF	2019/08/27	編集
Member ProjectAdmin	user6	西野	user6@vaddy.net			日本語	利用中	OFF	OFF	2019/08/29	編集
Member	user7	東野				日本語	利用中			2019/08/29	編集
Member	user8	名前	メール			日本語	利用中			2019/08/30	編集
Co-Owner	user9	ユーザー太郎	user1@vaddy.net		11112222	日本語	利用中			2019/08/30	編集
Co-Owner	user10	市川	user2@vaddy.net			日本語	利用中			2019/08/30	編集
		市山	user3@vaddy.net			日本語	利用中			2019/08/30	編集
		市原	user4@vaddy.net			日本語	利用中			2019/08/30	編集
		市谷	user5@vaddy.net			日本語	利用中			2019/08/30	編集

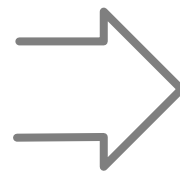
新規メンバー追加 メンバー

VAddyの診断の流れ

VAddyはお客様が作成したテストシナリオに沿って診断を実施します。



1. お客様のアプリケーションの操作（画面遷移）をテストシナリオとしてVAddyに記録します。



2. 作成されたテストシナリオに沿って診断を実施します。

- アプリケーションを理解しているお客様自身でテストシナリオを作成することで網羅的に診断が可能
- 機能ごとにシナリオを作成して小さいサイクルでの診断を実施

レポート

Result Details

脆弱性検査の結果、問題を発見しました。下記の詳細を確認ください。

脆弱性種別	URL	脆弱性があるパラメータ名	検査データ
ディレクトリトラバーサル	/xvwa/vulnerabilities/fi/?file=readme.txt	file	Request Response
Remote File Inclusion	/xvwa/vulnerabilities/fi/?file=readme.txt	file	Request Response
SQLインジェクション	/xvwa/vulnerabilities/sqli/	search	Request Response

発見した脆弱性一覧

脆弱性があったURL、パラメータ名、脆弱性の種別が表示されます。

脆弱性が検知された際にVADdyスキャンサーバから送ったHTTPリクエストデータ

Vulnerability	URI	Vulnerable
クロスサイトスクリプティング	?name=aaa&name2=bbb	name

```
GET /?name=aaa%3Cscript+src%3Dhttp%3A%2F%2Fwww.example.jp%2Fvaddy1.js%3E%3C%2Fscript%3E&name
Host: vaddytest.ichikaway.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:57.0) Gecko/20100101 Firefox/57.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Referer: http://vaddytest.ichikaway.com/
Authorization: Basic eWFZdTpzaGk=
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

リクエストデータ

脆弱性を発見した際に送信した検査リクエストのデータが参照できます。お手元で問題の再現をする際に便利です。

```
<br/>
<br/>
hello :
38
aaa<script src=http://www.example.jp/vaddy1.js></script>
12
<br/>
hello2 :
```

レスポンスデータ

脆弱性を発見した際に受信したレスポンスデータが参照できます。どのようなエラーだったのか、XSSの場合はhtmlのどの箇所がエスケープされていなかったのか確認できます。

箇所には、×2のようにハン印と脆弱性件数が表示されます。
を×の上に乗せると、脆弱性があるパラメータ名が表示されます。

URL	SQL Injection	XSS	RFI	Command Injection	Directory Traversal
/xvwa/vulnerabilities/sqli/	○	○	○	○	○
/xvwa/vulnerabilities/sqli/	× 1	○	○	○	○
/xvwa/vulnerabilities/fi/	○	○	○	○	○
/xvwa/vulnerabilities/fi/?file=readme.txt	○	○	× 1	○	× 1
/xvwa/	○	○	○	○	○

全体の診断レポート

脆弱性の発見の有無に関わらず、どのURLを検査したのか、問題があったURLはどこかをレポートで一覧表示します。全体の把握や、上長への報告などにご利用に便利です。

VAddyご利用プラン

お客様のご利用シーンに合わせたプランをご用意しています。

診断 **18** 項目
全ての機能が使える

Advanced

IPA「安全なウェブサイトの作り方(チェックリスト)」全項目と合わせて診断ができるプラン

月額 **99,800**円

診断 **11** 項目
必要最低限の診断を

Enterprise

組織管理機能と幅広い診断項目を備えたプラン。
アカウント管理が必要な大規模組織向けプラン

月額 **59,800**円

診断 **5** 項目
手軽にお試し

Professional

攻撃の発生頻度が高い5つの脆弱性を効率的に診断。
組織の規模や業種を問わずご利用いただける **ミニマムプラン**

月額 **19,800**円

Vaddyの年間ライセンスに、SHIFT SECURITYの自動脆弱性診断を+（プラス）！



Advanced
+ 自動脆弱性診断

Advanced +

年額 **1,398,000**円

Enterprise
+ 自動脆弱性診断

Enterprise +

年額 **998,000**円

Professional
+ 自動脆弱性診断

Professional +

年額 **598,000**円

金額は税別です。

VAddy基本プラン料金

		Advanced	Enterprise	Professional
診断項目数		18 (IPA対応)	11	5
チーム機能	チームメンバー	無制限/FQDN	無制限/FQDN	50ユーザー/FQDN
組織管理	組織メンバー	30ユーザー	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	8時間/回	5時間/回	2時間/回
	スキャン一括実行	✓	-	-
	スキャン同時実行	3	3	1
	ローカル環境への診断	✓	✓	✓
	診断可能サイト数 (FQDN)	3	3	3
料金	基本利用料(税別)	月額 99,800円 年額 998,000円	月額 59,800円 年額 598,000円	月額 19,800円 年額 198,000円



手動脆弱性診断付きプラン

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。

各プランに付属する診断チケットは、OWASP TOP10（※1）に準拠したWEBアプリケーション手動脆弱性診断でご利用いただけます。（※2）

※1 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」

OWASP TOP 10	
A1	アクセス制御の不備
A2	暗号化の失敗
A3	インジェクション
A4	安全が確認されない不安な設計
A5	セキュリティの設定ミス
A6	脆弱で古くなったコンポーネント
A7	識別と認証の失敗
A8	ソフトウェアとデータの整合性の不具合
A9	セキュリティログとモニタリングの失敗
A10	サーバーサイドリクエストフォージェリ (SSRF)

		Advanced + 手動脆弱性診断	Enterprise + 手動脆弱性診断	Professional + 手動脆弱性診断
		Advanced +	Enterprise +	Professional +
VAddy	診断チケット	Advanced 年間契約	Enterprise 年間契約	Professional 年間契約
	料金	20チケット		
料金	基本料金 (年額)	1,398,000円	998,000円	598,000円
	追加診断 チケット	150,000円/10チケット		

金額は税別です。

※2 WEBアプリケーション手動脆弱性診断（チケット20枚以上）を必須とし、クラウド診断、プラットフォーム診断、脆弱性対応サポート等は10枚単位の追加チケットでの対応となります。



プラットフォーム診断オプション

VAddyの基本プラン（月間・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」によるプラットフォーム診断が追加できます。

VAddy年間契約だけでなく、VAddy月間契約にもオプション形式でプラットフォーム診断サービスを追加できます。

こんなお客様に最適です

- ・ 監査目的で年1回Webアプリとプラットフォームを診断して報告書を出したい
- ・ リリース前にインフラ環境を含めて広く診断したい

VAddy標準プラン月額料金に追加いただいた料金例

ご参考例	Advanced	Enterprise	Professional
利用料金(税別)	¥299,800	¥259,800	¥219,800
料金内訳	Advanced ¥99,800 + オプション ¥200,000	Enterprise ¥59,800 + オプション ¥200,000	Professional ¥19,800 + オプション ¥200,000

- ・ リモートでの実施を基本とし、3IPまで10チケットでご利用可能です。
- ・ 10チケット単位での追加購入も可能。4IP以上の診断やオンサイトでの実施、環境構築費が発生する場合は追加チケットを購入いただきます。

※価格は税別です。

所有者確認方式（DNS）追加オプション【NEW】

認証用ファイルを設置できないお客様向けの、DNSレコードを利用した所有者確認方式です。
すべての検査対象サーバーにHTMLファイルを設置する必要がなくなり、DNSレコードを登録するだけで所有者確認が可能になります。

<ご利用例>

- ・ 同一ドメイン内に検査対象サーバーが多く、HTMLファイルの設置作業が煩雑な場合
 - ・ VAddyの認証ファイルを設置するためにリポジトリへコミットし、デプロイフローに組み込む必要があるが、それを避けたい場合
 - ・ HTMLファイルの設置方法が不明、または担当者・権限の都合でファイルを配置できない場合
- ・・・など

オプション料金・・・¥50,000/1回（複数ドメイン利用可）

- ・ 本機能をご利用いただくには、オプション機能の購入が必要です。
一度購入いただくと複数のドメインで利用でき、以後は追加料金なしで継続してお使いいただけます。
- ・ 本機能は現在VAddy PrivateNet版では提供していません。

※価格は税別です。

本資料についてのお問い合わせ

株式会社ビットフォレスト
VAddy事業部

info@vaddy.net



VAddy
<http://vaddy.net/ja/>



VAddy技術ブログ
<http://blog-ja.vaddy.net/>

