アドリフト株式会社

Company Introduction

会社紹介資料

2026/08/05

Contents

Chapter

Ⅰ

会社概要

Chapter

Ⅱ

代表者の
紹介

Chapter

Ⅲ

サービスの
紹介

01

会社概要

Company Information

会社概要

会社名	アドリフト株式会社
オフィス	東京都渋谷区道玄坂1丁目10番8号渋谷道玄坂東急ビル2F−C
資本金	100万円
代表取締役	廣田　光冴
事業内容	サイバーセキュリティ
WEBページ	https://www.adriftjb.com/
創立	2023年2月
法人設立	2026年5月

02

代表者の紹介

Entrepreneur Introduction

代表者の紹介

廣田　光冴
Mitsuki Hirota

北海学園大学経済学部経済学科卒
University of Massachusetts Lowell
MBA 在学中

情報処理安全確保支援士
登録番号　023127

元警視庁警察官
警視庁退官後、倉庫やスーパーでの日雇いや派遣社員を経験

インド系IT企業インターソフト(株)にてインドに駐在し、テスト工程を担当
米国系不動産企業CBRE(株)にて業務自動化や建築プロジェクトのファイナンスを担当
CBRE(株)在職時に、情報処理安全確保士を取得し、セキュリティのITフリーランスとして独立

セキュリティエンジニアとしてEDRの導入やSIEMの運用を経験
フリーランス時代、日系製造業IT子会社にて**脆弱性診断**のサービス立ち上げ責任者を担当し、2年で売上額を3倍以上(**500万円→1800万円**)に伸ばす。

2026年、ITフリーランスと同時並行してサイバーセキュリティの法人設立
顧客の獲得と売上の拡大を目指す。

03

サービスの紹介

Services Introduction

サービス

WEB脆弱性診断

WEBサイトに対して毎月脆弱性診断を実施します。
脆弱性診断は主に自動ツールを使います。
自動ツールに併せて、ハッカーが実際に使うパスワードリストを使用してログイン周りの脆弱性も調査します。

OSINT

インターネット上に存在する、自社に対する攻撃のヒントになる可能性のある情報を調査します。
調査の結果、意外な攻撃の糸口が見つかるかも知れません。

サービス

WEB脆弱性診断

特徴

自動ツールの利用

業界内で広く使われる診断ツールを使用して診断をします。
この診断ツールによって約100以上もの診断項目に対するテストが実施されます。
自動ツールを使うことにより脆弱性見落としのリスクが減ります。

信頼あるパスワードリスト

当社が信頼できると判断するパスワードリストを使用します。
WEBサイトで標的になりやすい箇所は第一に管理者のログイン機能です。
ハッカーが実際に使用するパスワードリストを使って管理者のログイン機能をテストします。

毎月実施

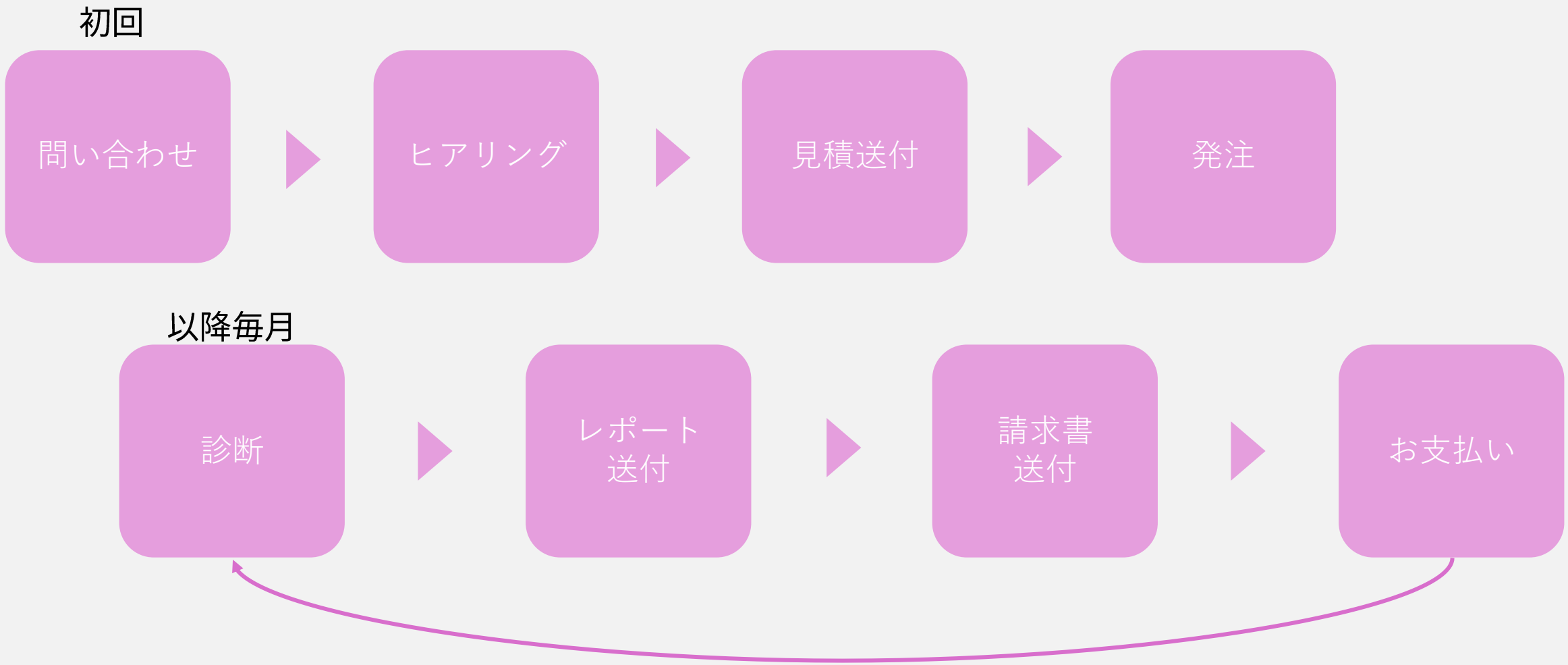
脆弱性診断を毎月1回実施します。
脆弱性診断でよくあるのが、毎年1回実施するパターン。脆弱性情報は日々更新されます。
毎月実施することにより、最新の脆弱性情報を反映した診断になります。

*1回のみの診断はできません。6か月以上の契約が必要です。

サービス

WEB脆弱性診断

サービス提供の流れ



サービス

WEB脆弱性診断

価格

1つのWEBサイトにつき**月額10万円**(消費税別)

※

- 大規模なWEBサイト及びビジネスロジックの診断に対しては、別途見積を実施します。
- 半年以上の診断継続をお願い致します。半年以降契約解除可能。
- 診断のためのログイン用のアカウントのご提供をお願いします。

サービス

OSINT

種類

OSINTとはOpen-Source Intelligenceの略です。
公開されているソース(主にインターネット)からハッカーの立場に立った自社の情報の調査を行います。

攻撃対象領域調査

インターネット上に公開されている自社のドメイン、サブドメイン、及びオープンポートを調査し、どこから攻撃される可能性があるかを把握します。

１ドメイン
月額10万円

パスワード等漏洩調査

メールアドレスを元に、過去どのような情報(パスワード等)が漏洩した記録があるかを調査します。

≦100メールアドレス
月額5万円
≦ 1,000メールアドレス
月額30万円

脆弱性情報収集

ソフトウェア/ハードウェア及びバージョンに基づいて、公開されている脆弱性情報を調査します。

１資産
月額1万円

ドキュメント漏洩調査

インターネット上でに漏洩している機密情報が含まれている可能性があるファイルを調査します。

１ドメイン
月額10万円

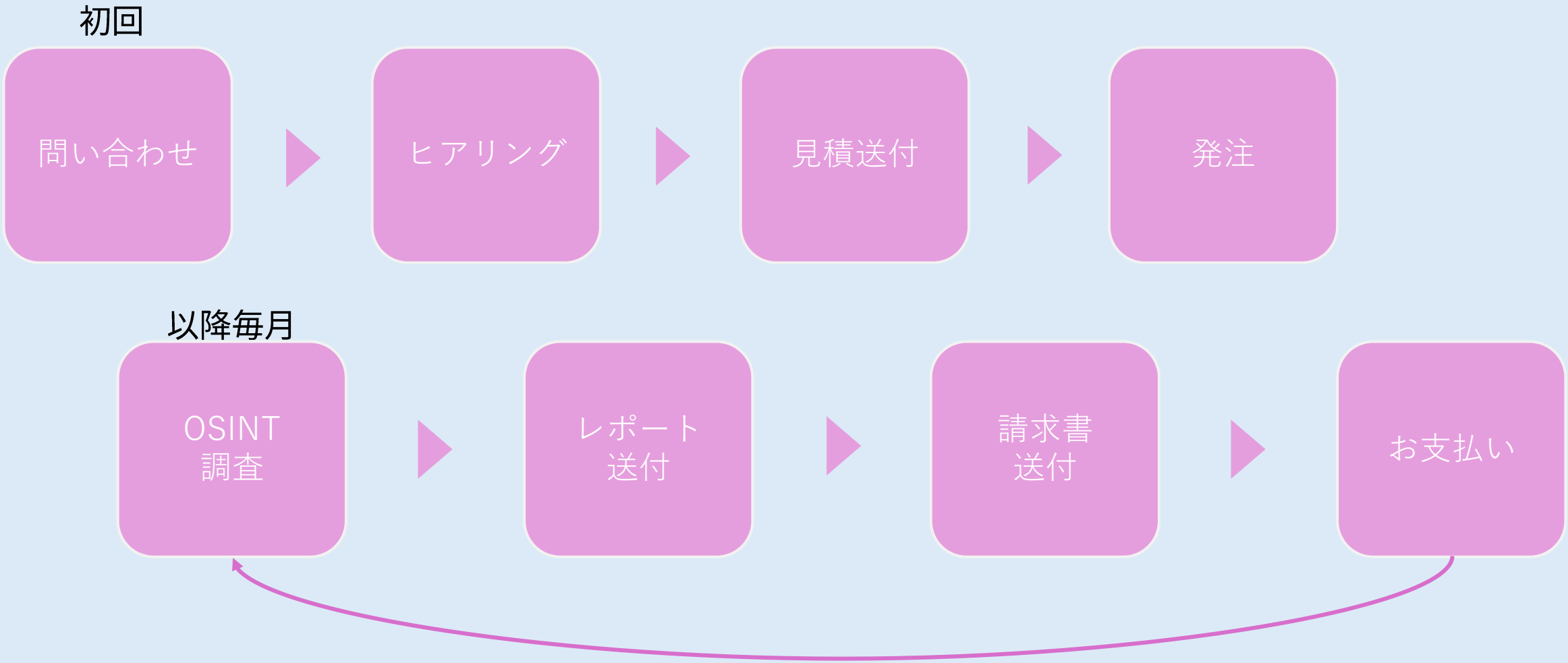
タイポスクアッティング調査

インターネット上にある自社のドメイン(例:google.com→goggle.com)に類似したドメインを調査します。

１ドメイン
月額5万円

*価格は全て消費税別です。

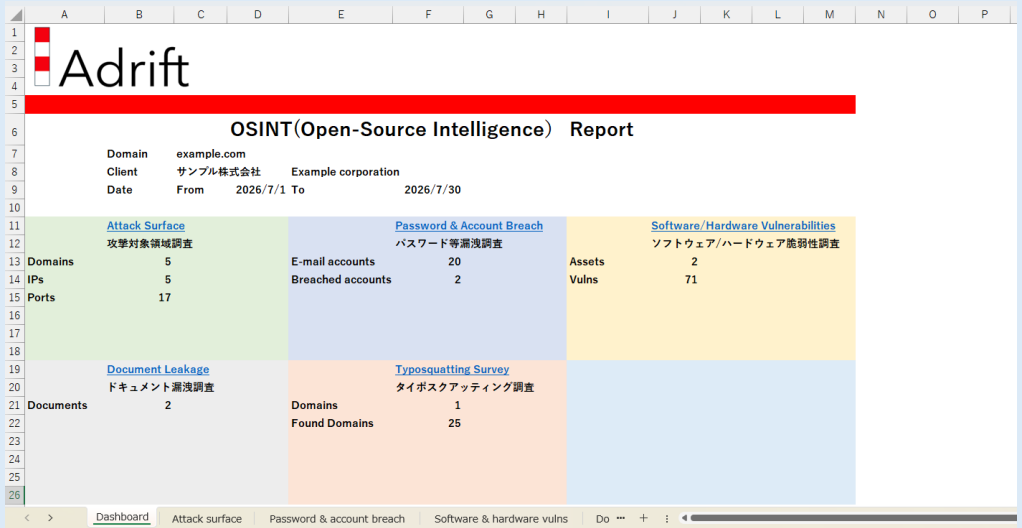
サービス提供の流れ



サービス

OSINT

OSINTレポートのサンプル



Adrift

OSINT(Open-Source Intelligence) Report

Domain	example.com
Client	サンプル株式会社 Example corporation
Date	From 2026/7/1 To 2026/7/30

Attack Surface 攻撃対象領域調査

Domains	5
IPs	5
Ports	17

Password & Account Breach パスワード等漏洩調査

E-mail accounts	20
Breached accounts	2

Software/Hardware Vulnerabilities ソフトウェア/ハードウェア脆弱性調査

Assets	2
Vulns	71

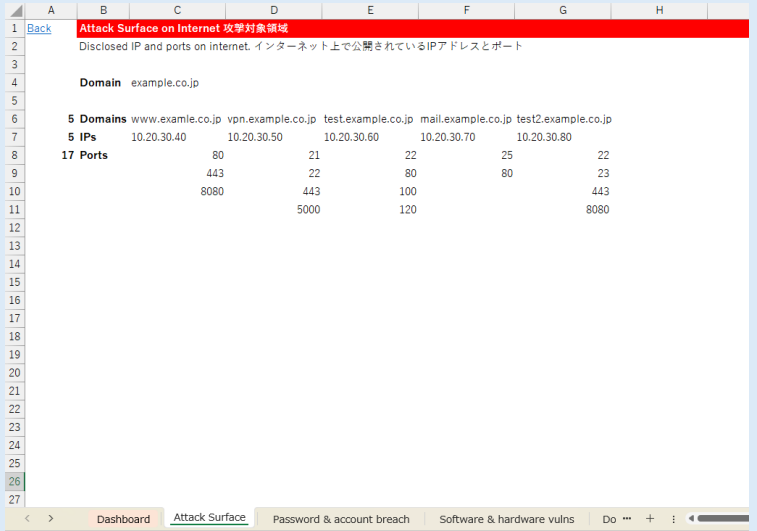
Document Leakage ドキュメント漏洩調査

Documents	2

Typosquatting Survey タイポスクアッティング調査

Domains	1
Found Domains	25

Dashboard | Attack surface | Password & account breach | Software & hardware vulns | Do



Back

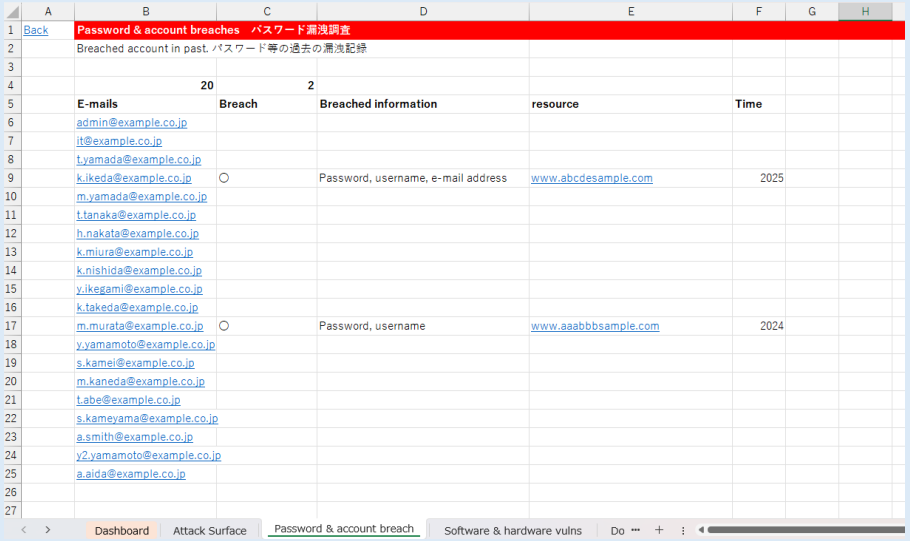
Attack Surface on Internet 攻撃対象領域

Disclosed IP and ports on internet. インターネット上で公開されているIPアドレスとポート

Domain example.co.jp

5	Domains	www.exaмle.co.jp	vpn.example.co.jp	test.example.co.jp	mail.example.co.jp	test2.example.co.jp
5	IPs	10.20.30.40	10.20.30.50	10.20.30.60	10.20.30.70	10.20.30.80
17	Ports	80	21	22	25	22
		443	22	80	80	23
		8080	443	100		443
			5000	120		8080

Dashboard | Attack Surface | Password & account breach | Software & hardware vulns | Do



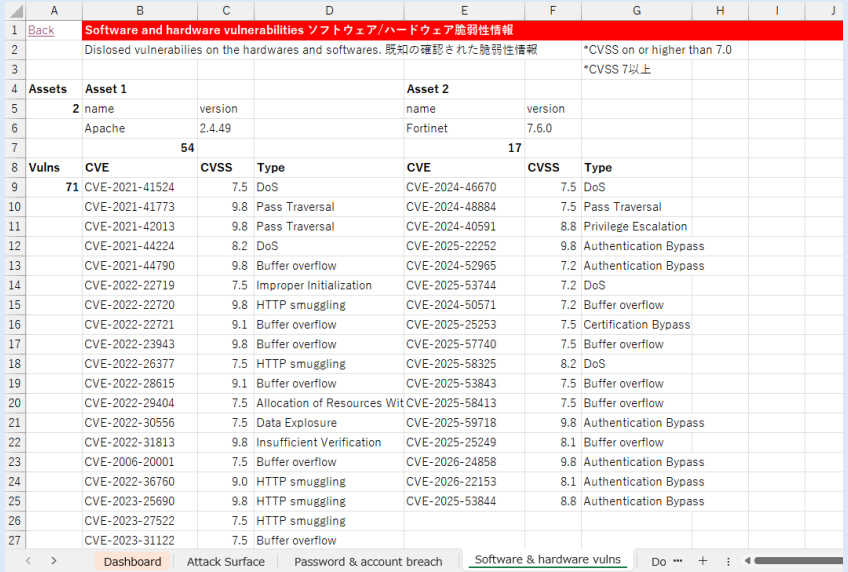
Back

Password & account breaches パスワード漏洩調査

Breached account in past. パスワード等の過去の漏洩記録

	20	2			
E-mails	Breach	Breached information	resource	Time	
admin@example.co.jp					
it@example.co.jp					
t.yamada@example.co.jp					
k.ikeda@example.co.jp	○	Password, username, e-mail address	www.abcdesample.com	2025	
m.yamada@example.co.jp					
t.tanaka@example.co.jp					
h.nakata@example.co.jp					
k.miura@example.co.jp					
k.nishida@example.co.jp					
y.ikegami@example.co.jp					
k.takeda@example.co.jp					
m.murata@example.co.jp	○	Password, username	www.aaabbbsample.com	2024	
y.yamamoto@example.co.jp					
s.kamei@example.co.jp					
m.kaneda@example.co.jp					
t.abe@example.co.jp					
s.kameyama@example.co.jp					
a.smith@example.co.jp					
y2.yamamoto@example.co.jp					
a.aida@example.co.jp					

Dashboard | Attack Surface | Password & account breach | Software & hardware vulns | Do



Back

Software and hardware vulnerabilities ソフトウェア/ハードウェア脆弱性情報

Dislosed vulnerabilies on the hardwares and softwares. 既知の確認された脆弱性情報 *CVSS on or higher than 7.0

*CVSS 7以上

Assets	Asset 1			Asset 2		
2	name	version		name	version	
	Apache	2.4.49		Fortinet	7.6.0	
	54			17		
Vulns	CVE	CVSS	Type	CVE	CVSS	Type
71	CVE-2021-41524	7.5	DoS	CVE-2024-46670	7.5	DoS
	CVE-2021-41773	9.8	Pass Traversal	CVE-2024-48884	7.5	Pass Traversal
	CVE-2021-42013	9.8	Pass Traversal	CVE-2024-40591	8.8	Privilege Escalation
	CVE-2021-44224	8.2	DoS	CVE-2025-22252	9.8	Authentication Bypass
	CVE-2021-44790	9.8	Buffer overflow	CVE-2024-52965	7.2	Authentication Bypass
	CVE-2022-22719	7.5	Improper Initialization	CVE-2025-53744	7.2	DoS
	CVE-2022-22720	9.8	HTTP smuggling	CVE-2024-50571	7.2	Buffer overflow
	CVE-2022-22721	9.1	Buffer overflow	CVE-2025-25253	7.5	Certification Bypass
	CVE-2022-23943	9.8	Buffer overflow	CVE-2025-57740	7.5	Buffer overflow
	CVE-2022-26377	7.5	HTTP smuggling	CVE-2025-58325	8.2	DoS
	CVE-2022-28615	9.1	Buffer overflow	CVE-2025-53843	7.5	Buffer overflow
	CVE-2022-29404	7.5	Allocation of Resources Wit	CVE-2025-58413	7.5	Buffer overflow
	CVE-2022-30556	7.5	Data Explosure	CVE-2025-59718	9.8	Authentication Bypass
	CVE-2022-31813	9.8	Insufficient Verification	CVE-2025-25249	8.1	Buffer overflow
	CVE-2006-20001	7.5	Buffer overflow	CVE-2026-24858	9.8	Authentication Bypass
	CVE-2022-36760	9.0	HTTP smuggling	CVE-2026-22153	8.1	Authentication Bypass
	CVE-2023-25690	9.8	HTTP smuggling	CVE-2025-53844	8.8	Authentication Bypass
	CVE-2023-27522	7.5	HTTP smuggling			
	CVE-2023-31122	7.5	Buffer overflow			

Dashboard | Attack Surface | Password & account breach | Software & hardware vulns | Do

問い合わせ先

メールでの問い合わせ
sales@adrift-jp.com

HPからの問い合わせ
https://www.adriftjb.com/
*トップページ>Service>OSINTもしくはWEB脆弱性診断より

概ね、3営業日以内に返信します。

Thank you !