大企業の不正アクセス、アカウント乗っ取りの闘い: 最新対策策略

株式会社プロシド／Human社のご紹介

株式会社プロシド

アジェンダ

会社紹介

事例1：アカウント乗っ取り

事例2：不正アクセスやJSの改ざんによる情報漏えい

Human Securityの紹介

現状・課題

Human Security Platform

株式会社プロシド

細江　由二 (ホソエ　ユウジ)
米国カリフォルニア州、サンディエゴ出身。2000年慶応義塾大学商学部卒業。大手外資系コンサルティング会社に入社。日本、シンガポール、アメリカ、タイオフィスへ在籍、15年間グローバルプロジェクトを担当。退社後、株式会社プロシドへ代表取締役として就任。

会社概要

社名　株式会社プロシド	設立　2019年3月8日
代表者　代表取締役　細江 由二	オフィス　東京都港区

事業概要

グローバルスタンダードの優れたITサービスを日本国内で販売。販売だけでなく、導入/運用のサポートまで確実に実行。

世界のサイバー攻撃：現状

- 2021年の22.4%が金融業界に向けたサイバー攻撃
- BCGの調べでは、金融業界は他業界よりも300倍ものサイバー攻撃被害の可能性がある。

金融機関への攻撃は利益が大きい
個人情報が多く集まる

金融期間におけるサーバー犯罪は他業界に比べコストが**40%**増

事例１：アカウント乗っ取り

QRコード決済サービスへの不正ログイン
2019年7月、QRコード決済サービスで一部のアカウントに対する不正アクセス

不正アクセスによる被害は、不正チャージおよび不正利用で、2019年7月31日時点の**計808人、被害額は約3,860万円**。また、ブランド、イメージに傷がつき、最終的に、2019年9月30日をもって**3ヶ月でサービスは廃止**。

66% のユーザーが同じパスワードをサイト間で再利用

240億件のユーザー名とパスワードのペアがダークウェブで売買されている。

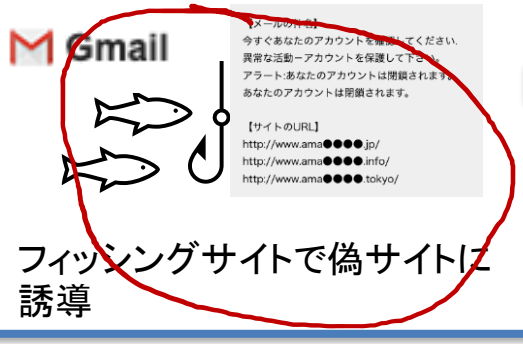
知らない内に自社のウェブサイトが不正の手口に加担しているかも知れません。

60%の消費者が過去1年サイバー攻撃を受けた会社のサービスの利用を控えると回答

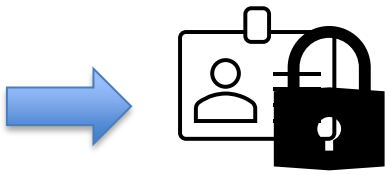
2020年、金融サービス業のみで34億件の不正アクセスアタックを記録（前年比45%増）*

*Akamaiより

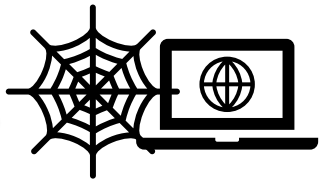
攻撃例



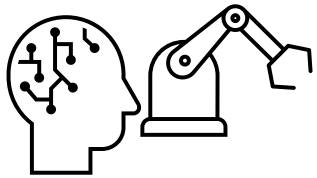
フィッシングサイトで偽サイトに誘導



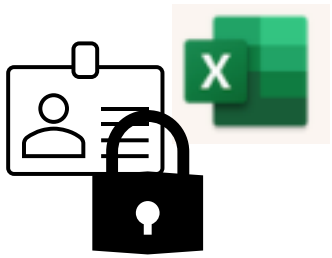
IDとパスワードを取得



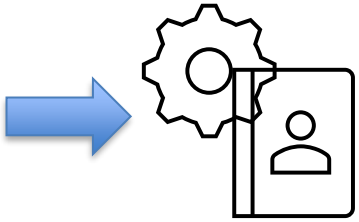
ダークウェブ等でデータの売買



IDとパスワードを利用した、BOTを作成する

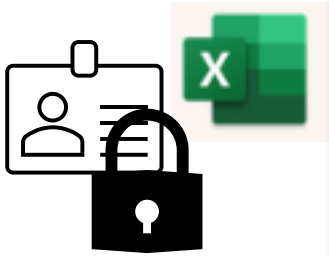


IDとPasswordの組み合わせでBOTを実行



住所、口座情報等の個人情報取得

アカウントの乗っ取り



有効なアカウント、個人情報をさらに売買、またはその他のサイトでIDとPWを利用してアタック

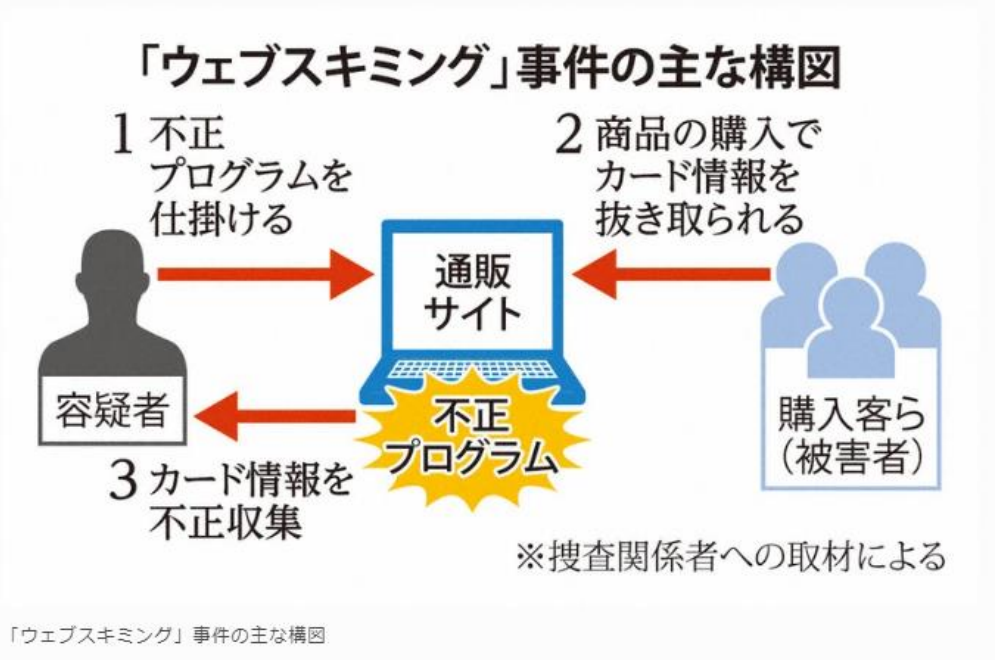
＊IDとパスワードをサイト間で使いまわしているユーザーは多く、一度情報が漏れると、影響範囲が広い

事例２：不正アクセスや加盟店のJSの改ざんによる情報漏えい

カード情報流出

2023年2月に第三者による不正アクセスを受け、ユーザーの**個人情報12万982件**、**クレジットカード情報11万2,132件**が**漏洩した可能性**を受け、カード決済サービスを停止。一部ユーザーのクレジットカードが不正利用された可能性があることを確認

サイトのシステムの一部の貧弱性を利用した**ペイメントアプリケーションの改ざん**が行われた。



「ウェブスキミング」事件の主な構図

加盟店は不正なJSによりいつのまに不正者にカードや個人情報を抜き取られている。今後はJSに関してもPCIDSSによって責任を負うことが求められる

毎日新聞11月15日2023年より

PCI DSS4 6.4.3

PCI Security Standards Council

要件とテスト手順		ガイダンス
定義されたアプローチの要件	**定義されたアプローチのテスト手順**	**目的**
6.4.3 消費者のブラウザに読み込まれ実行されるすべての決済ページスクリプトは、以下のように管理される。 • 各スクリプトが認可されていることを確認するための方法が実装されている。 • 各スクリプトの整合性を保証するための方法が実装されている。 • すべてのスクリプトのインベントリが、それぞれのスクリプトが必要な理由を説明した文書とともに維持される。	**6.4.3.a** ポリシーと手順を調査し、消費者のブラウザに読み込まれて実行されるすべての支払ページスクリプトを管理するためのプロセスが、この要件で指定されたすべての要素に従って定義されていることを確認する。 **6.4.3.b** 担当者にインタビューを行い、インベントリ記録およびシステム構成を調査し、消費者のブラウザに読み込まれ実行されるすべての支払ページスクリプトが、この要件で指定されているすべての要素に従って管理されていることを確認する。	決済ページでロードされ実行されるスクリプトは、事業体が知らないうちにその機能が変更されることがあり、また追加の外部スクリプト（例えば広告やトラッキング、タグ管理システムなど）をロードする機能を持つこともあります。 このような一見無害なスクリプトは、潜在的な攻撃者が消費者ブラウザからカード会員データを読み取り、流出させる悪意のあるスクリプトをアップロードするために使用される可能性があります。 そのようなスクリプトのすべての機能が支払ページの操作に必要であると理解されるようにすることで、改ざんされる可能性のあるスクリプトの数を最小限に抑えることができます。 スクリプトが明示的に許可されていることを確認することで、適切な管理承認なしに不要なスクリプトがペイメントページに追加される可能性を減らすことができます。 スクリプトの改ざんを防止する技術を使用すると、スクリプトが修正されて、決済ページからカード会員データをスキミングするなどの不正な動作が実行される確率を最小にできます。 *(次ページに続く)*
カスタマイズアプローチの目的		
消費者のブラウザでレンダリングされる決済ページには、未許可のコードは存在できない。		
適用に関する注意事項		
この要件は、事業体の環境からロードされるすべてのスクリプトと、サードパーティおよび第 4 のパーティからロードされるスクリプトに適用される。 この要件は、2025 年 3 月 31 日まではベストプラクティスであり、それ以降は必須となるため、PCI DSS 評価時に十分に検討する必要がある。		

PCI DSS4 11.6.1

PCI Security Standards Council

要件とテスト手順		ガイダンス
11.6 決済ページの不正な変更が検知され、対応されている。		
定義されたアプローチの要件 **11.6.1** 変更・改ざん検知のメカニズムは、以下のように展開されている。 • 消費者ブラウザが受信した HTTP ヘッダーと決済ページのコンテンツに対する不正な変更 (侵害の指標、変更、追加、および削除を含む) を担当者に警告すること。 • メカニズムは、受信した HTTP ヘッダーと決済ページを評価するように構成される。 • メカニズムの機能は、以下のように実行される。 – 少なくとも 7 日に 1 回 **または** – 定期的に（要件 12.3.1 に規定されたすべての要素に従って実施される事業体のターゲットリスク分析で定義された頻度で）	**定義されたアプローチのテスト手順** **11.6.1.a** システム設定、監視された決済ページ、および監視活動の結果を調査し、変更および改ざん検知メカニズムが使用されていることを確認する。 **11.6.1.b** 構成設定を調べて、この要件で指定されたすべての要素に従ってメカニズムが構成されていることを確認する。 **11.6.1.c** メカニズム機能が事業体定義の頻度で実行される場合、頻度を決定するための事業体のターゲットリスク分析を調べ、リスク分析が要件 12.3.1 に規定するすべての要素に従って実行されたことを確認する。 **11.6.1.d** コンフィギュレーション設定を調べ'担当者にインタビューを行い、メカニズムの機能では次のどちらかが実行されているかを確認する。 • 少なくとも 7 日に 1 回 **または** • この要件のために実施された事業体のターゲットリスク分析で定義された頻度で。	**目的** 多くのウェブページは、現在、アクティブコンテンツ（主に JavaScript）を含むオブジェクトを、インターネットの複数の場所から組み立てることに依存しています。さらに、多くのウェブページのコンテンツは、コンテンツ管理システムやタグ管理システムを使って定義されており、従来の変更検出メカニズムでは監視できない場合があります。 したがって、悪意のある活動による変更や指標を検出する唯一の場所は、ページが構築され、すべての JavaScript が解釈される消費者ブラウザの中です。 消費者ブラウザが受信した HTTP ヘッダーの最新バージョンと決済ページのアクティブコンテンツを、以前のバージョンまたは既知のバージョンと比較することにより、スキミング攻撃を示唆する不正な変更を検出することが可能です。 さらに、既知の侵害の指標や、スキマーに典型的なスクリプト要素や動作を探すことで、疑わしいアラートを発することができます。 *(次ページに続く)*
カスタマイズアプローチの目的 電子商取引のスキミングコードやテクニックは、消費者ブラウザが受信した決済ページに、適時警告を発生させることなく追加することはできません。迅速な警告が生成されない限り、スキミング防止策を決済ページから削除することはできない。		

PCCI DSS4の準備はできていますか？

タイムリミットは2025年3月

Human Security について

会社概要

社名	Human Security (旧社名：White ops)
本社	New York州　米国
売上	非公開
設立	2012年
拠点	米国
URL	www.humansecurity.com

・ゴールドマンサックスポートフォリオカンパニー
・ホワイトハッカーメンバーが多数在籍
・グーグル社が広告不正対策に採用するツール

ISO27001認定

外部機関からの評価（一例）

HUMAN was named a Distinguished Vendor for 2021 by TAG Cyber

FAST COMPANY

CEO Tamer Hassan was named the #1 Most Creative Person in Business by Fast Company

Human社　実績

導入顧客（一例）

Advertising

Google
Microsoft
FACEBOOK
Adobe
theTradeDesk
Yahoo
verizon media
PubMatic
RISE
xandr
OneView by Roku
triplelift
FREEWHEEL A COMCAST COMPANY
Magnite
MediaMath

Retail eCommerce

build.com
carter's
HIBBETT SPORTS
INDOCHINO MADE TO MEASURE
L'ORÉAL
Lbrands
SKECHERS
SALLY BEAUTY
wayfair

Travel & Hospitality

Alaska
SeatGeek
سيرا SEERA

Media and Gaming

anzu
APPLOVIN
dailymotion
FANDUEL
pandora
SOUNDCLOUD
VIDAZOO

Marketplaces

GRUBHUB
realtor.com
LAYBUY

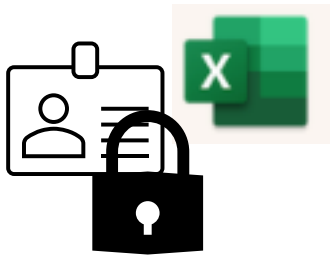
Financial Services

Goldman Sachs
Amica AUTO HOME LIFE
bill.com
MassMutual
kiva

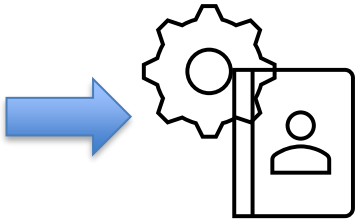
SAAS

crunchbase
wave
WiX.com

現状：攻撃に対する対策

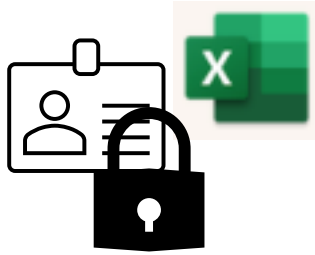


購入した、IDとPasswordの組み合わせでBOTを実行

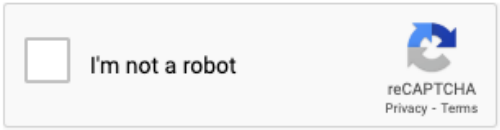


住所、口座情報等の個人情報取得

アカウントの乗っ取り



有効なアカウント、個人情報をさらに売買、またはその他のサイトでIDとPWを利用してアタック



- ユーザーからは“迷惑”だと不評
- 回避するAPI等が多々存在
- アカウントが乗っ取られたら止めるのが困難

大企業がもとめる攻撃に対する理想対策

- 個人情報は第三社に渡したくない
- 不正リスクを数値化して、アカウント乗っ取りを止めたい
- リアルタイムでモニターし、アカウント乗っ取りと判断した場合、自社のルールを適応したい
- ボットの良し悪しをコントロールしたい
- ユーザー体験を損なわずに、不正を止めたい。
- 不正ソフトが人をボットとして誤検知した場合、ユーザーにはあまり負荷がかからない回避方法がほしい

人がBOTか否かを判断するのではなく、不正対策ソフトにBOTか
人間かの判断をして欲しい

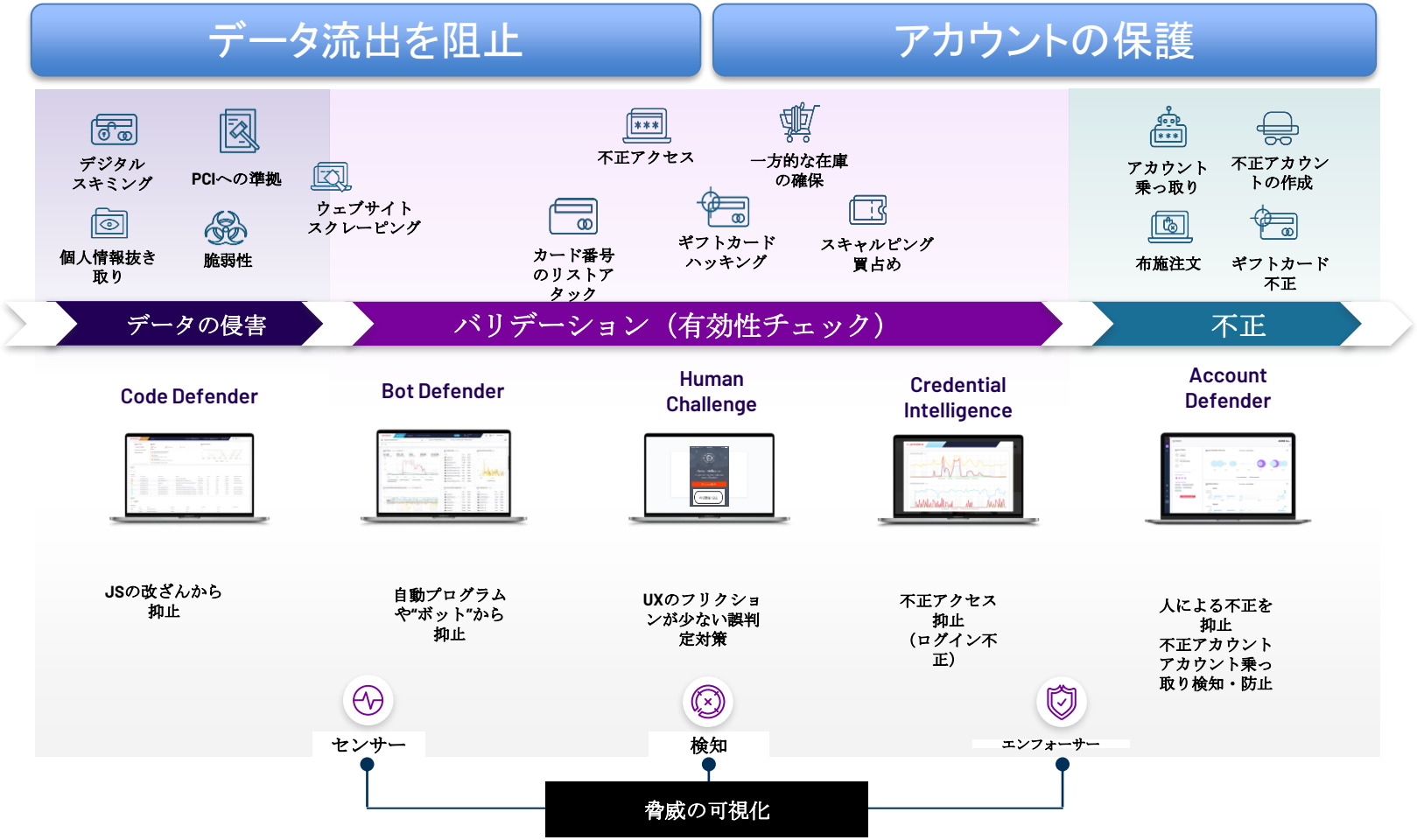
PCI DSS4準拠の課題

- ほとんどの企業が対応をしていない
- PCI DSS4の要件は理解したが、どこから手をつけてよいかわからない
- 7日に1回の改善・検知メカニズムをどう実現してよいかわからない
- 理想はリアルタイムでデータの流れを可視化し、コントロールしたい
- 3rdパーティのjavascriptのデータの受け渡しを把握したい

リアルタイムでデータの流れを把握し、不正があった場合、すぐに検知、アクションを打てるようにしたい

不正対策プラットホーム　“Human Security Platform（HSP)”

～総合的なアカウントのプロテクション～



人や自動プログラムによる不正アクセス・リストアタックを守る総合的なサービス

HSPの特徴

■現状不正対策

・多くの不正対策システムはユーザの不正行為を行った後を
中心にリスク判定

例
・会員登録後
・ログイン後
・決済後

・多くは取得した属性情報や個人情報に依存しており、エンドユーザのプライバシーが損なわれる傾向がある

■次世代型の不正対策

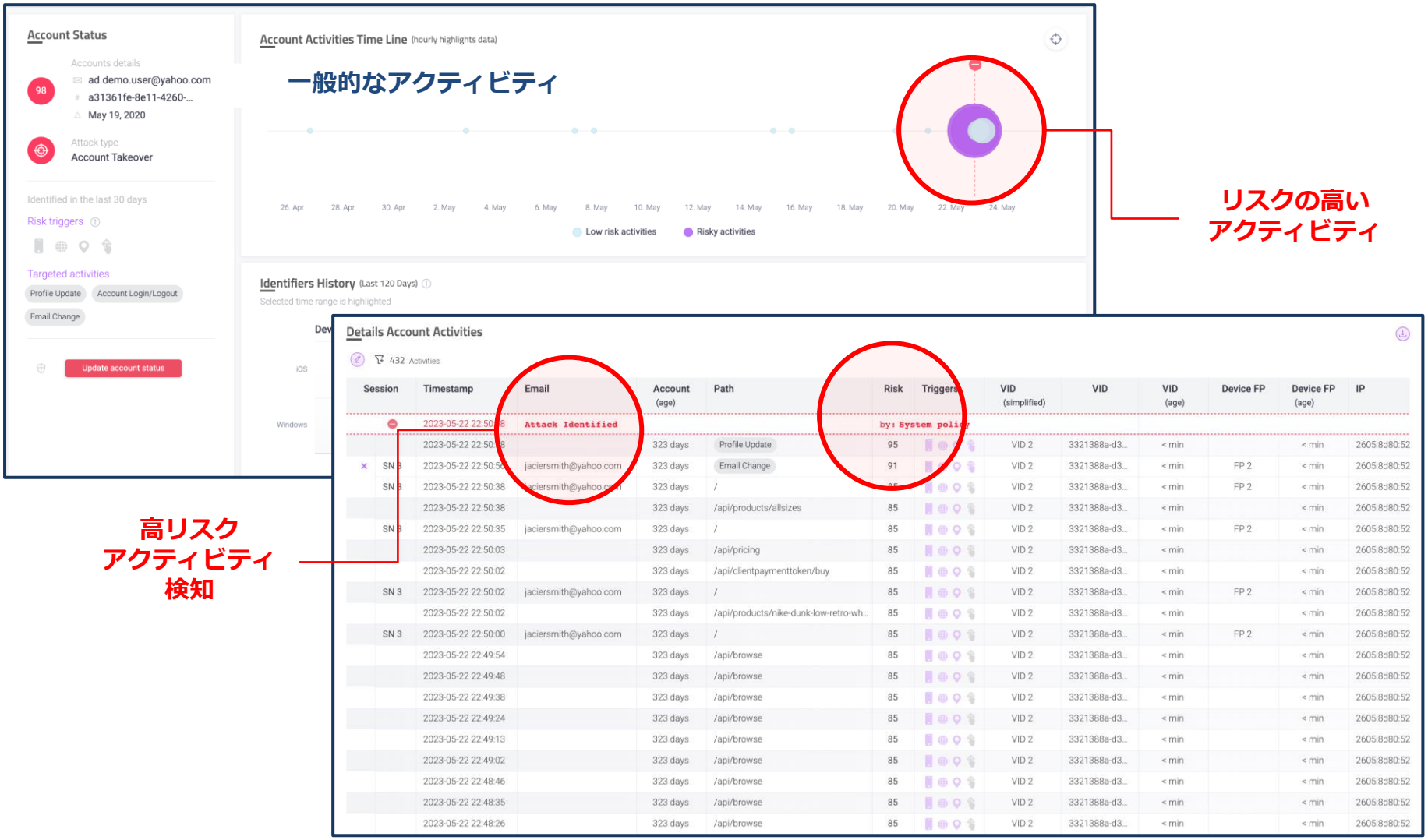
・不正行動が行われる前に抑止をすることに注力
→会員登録時に会員を作成させない
→不正ログインをそもそもさせない
☆結果的に大量のアカウントを作成させない、不正ログインをさせないことにより不正決済絶対数を減らす

・自動化を検知したり、エンドユーザのサイト内でのビヘビアを見て不正ユーザを検知

・データを漏洩させない為のプラットホームモニタリングを別途提供

・個人情報に依存しないまたは比較的個人を特定することがしにくいデータのみで対策をとることができるサービス

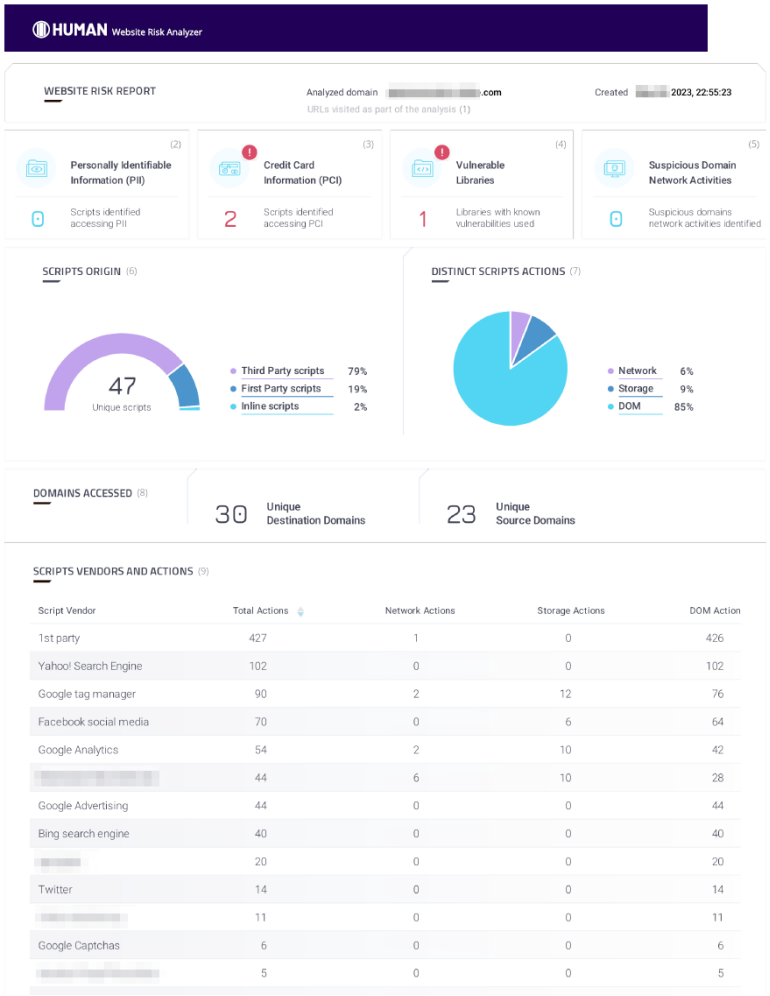
管理画面サンプル（高リスクアクティビティ）



Session	Timestamp	Email	Account (age)	Path	Risk	Triggers	VID (simplified)	VID	VID (age)	Device FP	Device FP (age)	IP
	2023-05-22 22:50:38	Attack Identified			by: System policy							
	2023-05-22 22:50:38		323 days	Profile Update	95		VID 2	3321388a-d3...	< min		< min	2605:8d80:52
SN 3	2023-05-22 22:50:5[illegible]	jaciersmith@yahoo.com	323 days	Email Change	91		VID 2	3321388a-d3...	< min	FP 2	< min	2605:8d80:52
SN 3	2023-05-22 22:50:38	jaciersmith@yahoo.com	323 days	/	85		VID 2	3321388a-d3...	< min	FP 2	< min	2605:8d80:52
	2023-05-22 22:50:38		323 days	/api/products/allsizes	85		VID 2	3321388a-d3...	< min		< min	2605:8d80:52
SN 3	2023-05-22 22:50:35	jaciersmith@yahoo.com	323 days	/	85		VID 2	3321388a-d3...	< min	FP 2	< min	2605:8d80:52
	2023-05-22 22:50:03		323 days	/api/pricing	85		VID 2	3321388a-d3...	< min		< min	2605:8d80:52
	2023-05-22 22:50:02		323 days	/api/clientpaymenttoken/buy	85		VID 2	3321388a-d3...	< min		< min	2605:8d80:52
SN 3	2023-05-22 22:50:02	jaciersmith@yahoo.com	323 days	/	85		VID 2	3321388a-d3...	< min	FP 2	< min	2605:8d80:52
	2023-05-22 22:50:02		323 days	/api/products/nike-dunk-low-retro-wh...	85		VID 2	3321388a-d3...	< min		< min	2605:8d80:52
SN 3	2023-05-22 22:50:00	jaciersmith@yahoo.com	323 days	/	85		VID 2	3321388a-d3...	< min	FP 2	< min	2605:8d80:52
	2023-05-22 22:49:54		323 days	/api/browse	85		VID 2	3321388a-d3...	< min		< min	2605:8d80:52
	2023-05-22 22:49:48		323 days	/api/browse	85		VID 2	3321388a-d3...	< min		< min	2605:8d80:52
	2023-05-22 22:49:38		323 days	/api/browse	85		VID 2	3321388a-d3...	< min		< min	2605:8d80:52
	2023-05-22 22:49:24		323 days	/api/browse	85		VID 2	3321388a-d3...	< min		< min	2605:8d80:52
	2023-05-22 22:49:13		323 days	/api/browse	85		VID 2	3321388a-d3...	< min		< min	2605:8d80:52
	2023-05-22 22:49:02		323 days	/api/browse	85		VID 2	3321388a-d3...	< min		< min	2605:8d80:52
	2023-05-22 22:48:46		323 days	/api/browse	85		VID 2	3321388a-d3...	< min		< min	2605:8d80:52
	2023-05-22 22:48:35		323 days	/api/browse	85		VID 2	3321388a-d3...	< min		< min	2605:8d80:52
	2023-05-22 22:48:26		323 days	/api/browse	85		VID 2	3321388a-d3...	< min		< min	2605:8d80:52

JSのモニタリング簡易分析ツール（サンプル）

HSPの簡易分析アナライザーをウェブサイトで実施、現在の状態を確認。どのようなリスクがあるか、確認。HSPでは、このチェックをリアルタイムで常にモニタリングすることが可能。より詳細な情報をモニターすることが可能。また、データの受け渡しをコントロールすることも可能



- 個人情報は第三社に渡したくない
- 不正リスクを数値化して、アカウント乗っ取りを止めたい
- リアルタイムでモニターし、アカウント乗っ取りと判断した場合、自社のルールを適応したい
- ボットの良し悪しをコントロールしたい
- ユーザー体験を損なわずに、不正を止めたい。
- 不正ソフトが人をボットとして誤検知した場合、ユーザーにはあまり負荷がかからない回避方法がほしい

- ほとんどの企業が対応をしていない
- PCI DSS4の要件は理解したが、どこから手をつけてよいかわからない
- 7日に1回の改善・検知メカニズムをどう実現してよいかわからない
- 理想はリアルタイムでデータの流れを可視化し、コントロールしたい
- 3rdパーティのjavascriptのデータの受け渡しを把握したい

企業の理想を実現、懸念事項を対処

HSPは**ユーザーの体験を損なわず**にウェブサイト、アカウントの安全性を
リアルタイムで守ります

Human Security Platformの詳細につきましては
株式会社プロシドまで問い合わせお願い致します。

Info@prosido.com