AeyeScan

セキュリティに、確かな答えを。

20240917

AeyeScan 導入事例集

? なぜ、あの企業は

脆弱性診断の内製化にあたり AeyeScanを選んだのか？

── さらなるセキュリティ強化とコスト・業務軽減を目指して ──

AeyeSecurityLab

脆弱性診断に課題があるお客様へ

Webサイトへのサイバー攻撃が増加傾向にある中、
セキュリティ強化のために
脆弱性診断を見直している企業も多いのではないでしょうか。

本資料では、
人手やコストなどのリソース不足が
課題となりやすい脆弱性診断を、
AeyeScanを活用することで
課題解消とセキュリティ強化を実現した
企業の成功事例をご紹介します。
ぜひ参考になさってください。

AeyeScanなら解決できます！

クラウド型Webアプリケーション脆弱性診断ツール

AeyeScanとは？

専門知識・トレーニングも不要

最短10分で利用できる！

1

最短10分で診断開始

SaaS環境なので
24時間放置しておけます。

2

画面遷移図を自動作成

専門知識は不要！
AeyeScanがサイトを自動巡回、診断すべき画面を抽出して画面遷移図を生成します！

3

診断結果レポートも自動生成

開発担当にすぐ渡せるレポートが簡単に出力できます。

AeyeScan（エーアイスキャン）により
セキュリティ対策にかかる コストを削減！

クラウド型Webアプリケーション
脆弱性検査ツール

国内市場シェア
No.1

有償契約
100社以上

富士キメラ総研調べ「2023ネットワークセキュリティビジネス調査総覧 市場編」(Webアプリケーション脆弱性検査ツール（クラウド）2022年度実績)
ITR調べ「ITR Market View：サイバー・セキュリティ対策市場2024」SaaS型Webアプリケーション脆弱性管理市場：ベンダー別売上金額シェア（2022年度実績）

ユーザー企業

製造
AISIN / KOSÉ / SAKI / TIGER / Mizuno / ユーグレナ

インフラ
HIS / HOSTALINK / ぱかサイグループ / Suzuyo / NTT東日本 / Looop

金融
アイフル / JOBPAY / SOMPOひまわり生命 / DMM FinTech / Tokyo Century

出版メディア
集英社 / 中日新聞 / NIKKEI

エンタメ
e+ イープラス / CAPCOM / とらラボ!

SaaS
estie / エムティーアイ / OZ INTERNATIONAL / COACH A Co.,Ltd. / cybozu / JINSOKEN / Schoo / Speee / ZENKIGEN / Direct Sourcing / TAL / TEMONA / NAVITIME / KNOCK ON THE DOOR / BATONZ / VALUE HR / hokan / Money Forward / RUN.EDGE / RVSTA

SI・IT企業

Rworks / アクモス株式会社 / AVANT GROUP / CTC / Insight Edge / Infcurion / SB Technology / SBWorks / NTTデータ先端技術株式会社 / NTTビジネスソリューションズ / Globalway / circlace / さくら情報システム / CEC / tdi情報技術開発株式会社 / Simplex Inc. / 777WORKS / SOFT CREATE / SOLTEC / 電通総研 / TOPPAN / JOPS / NHC / Human Interactive Technology inc. / FUJISOFT / FUJITSU / YONA / リピスト

セキュリティ企業

NEC NECセキュリティ / cybertrust / LAC

社名五十音順（導入いただいた企業様の一部です）会社名及びロゴは各社の商標または登録商標です

（2024年9月時点）

AeyeScan 導入事例集INDEX

あなたにおすすめの成功事例は？

START

すでに**診断内製化**に取り組んでいますか？

NO

脆弱性診断ツールの
導入経験はありますか？

NO

脆弱性診断は
開発部門が実施しますか？
セキュリティ部門が実施しますか？

開発部門

アイフル → P05

セキュリティ部門

Simplex Inc. → P09

毎日を、給料日にする。JOBPAY → P13

YES

TIGER → P17

AVANT GROUP → P21

YES

脆弱性診断は
開発部門が実施しますか？
セキュリティ部門が実施しますか？

開発部門

貴社は**事業会社**ですか？
SI・IT 企業ですか？

事業会社

Money Forward → P25

SI・IT 企業

HIS → P29

FUJISOFT → P33

Human Interactive Technology inc. → P37

セキュリティ部門

LAC → P41

CASE 01 アイフル株式会社 様

アジャイル開発との相性の良さを実感、セキュリティの担保とスピーディな開発を両立

課題

外部に手動の脆弱性診断を依頼するとコストがかさむ上に、調整に想像以上の手間がかかり、アイフルの開発スタイルにそぐわなかった。

導入

画面やレポートがわかりやすい上に、ガイドや問診票、Q&A集など導入のハードルを下げるドキュメント類が充実しているAeyeScanを採用。

効果

コストはもちろん調整の手間も減り、開発チームの好きなタイミングでいつでも脆弱性診断を実施した上でセキュアなプロダクトを提供。

01 背景と課題

IT金融グループとしての成長を目指すアイフルは、経営環境の最適化の一環としてこの数年でクラウド化を進め、同時に、外部に委託してきたWebサイトやスマホアプリ開発の内製化に取り組んでいる。

「自分たちの思いが届くように、自分たちの手でサービスを作り、自分たちのお客様に届けることに取り組んでいます」（アイフル株式会社　デジタル推進1部1課課長　柿迫雅量氏）

また顧客向けだけでなく、業務効率化を目指した社内向けシステムも、同様に内製している。

「お客様からの問合せをオンライン完結できるシステムや、サービス申込から成約にかかわる業務を一元管理できるシステムを構築するなど、よりよい顧客体験を実現するとともに、社員がより気持ちよく仕事でき、業務を効率化できるシステムの開発に取り組んでいます」（アイフル株式会社　デジタル推進1部2課　姉川壮太氏）

こうしたシステムは顧客情報を扱うこともあり、高いセキュリティが求められる。開発者たちもセキュリティを自分ごとと捉え、当たり前のように必要な要素として取り組んでいる。

「顧客サービスへの入り口としての重要性もあり、自分たちの作ったプロダクトについては、セキュリティも含め、自分たちで責任を持つのが当然だという意識で取り組んでいます」（柿迫氏）

ただ、Webやアプリの開発に関してはエンジニアがそろっていても、セキュリティの知識となると深いところまでは手が回らず、診断のやり方もわからない状態だった。そこで、京都拠点で最初に内製したプロダクトについては外部の専門業者に手動での脆弱性診断を依頼することで、セキュリティを担保した。

しかし、外部の手動診断ではシステム全体で数百万単位のコストがかかる上に、日程調整や現場とのやり取りのために想像以上の手間がかかった。また、いったん日程が決まれば融通がきかず、アイフルの開発スタイルとは相性がいいとは言えなかった。

「やはり自分たちの開発スタイルにあった診断ができるものが必要だと考え、2022年末からツールを探し始めました」（柿迫氏）

02 ソリューションの選定

アイフルでは、オープンソースのツールのほか、複数の商用脆弱性診断ツールを比較検討した。実際に触って試したところ、他のサービスでは脆弱性診断のシナリオ作成時にオペレーションミスがあると抜け・漏れが生じる可能性があったり、オンプレミス環境に管理サーバを構築する必要があって維持コストがかかったりと、アイフルの環境に合った運用が難しいと感じた。

コスト面ではオープンソースのツールが優位ではあったが、「セキュリティという重要な情報を守る最後の砦を、オープンソースのツールにどこまで寄りかかってもいいものかと考えました。また、サポート体制でも選びにくいと判断しました」（柿迫氏）

検討の末、使い勝手、脆弱性診断の項目・精度、コストなど、総合的に見て選択したのがAeyeScanだ。

特に評価したポイントは、使い勝手やレポートの見やすさだった。アイフルでは、Webアプリケーションを開発するエンジニアが、リリース前に自らツールを用いて脆弱性診断を行う運用を考えていたが、もし診断ツールの使い方に迷ったり　、思い通りの設定ができなかったりするようでは困ってしまう。

「1チームあたり3〜4人でプロダクトを開発し、中には複数のプロダクトを掛け持ちしているエンジニアもいます。

各チームにセキュリティ専門家を配置することは難しいため、エンジニアにとってもわかりやすく、使いやすいことを重視しました」（柿迫氏）

　また、単に脆弱性を指摘するだけでなく、その問題をどのように修正すべきかの提案までもレポートに記載されていることも安心感につながった。

「スキャンの精度がしっかりしていることに加え、画面遷移図を自動的に生成してくれるのがありがたいと感じました。また、『問診票』が用意されていて事前の準備が容易な上に、依頼への返信が当日中に返ってくるほどサポートがしっかりしている点に非常にいい印象を受けました。診断途中で遷移に詰まるなどの困りごとが出てきた時でも、安心できると考えました」（姉川氏）

03 導入効果

　アイフルではシステム内製化の方針に沿って、数多くのプロダクトを次々に開発、リリースしていく計画だった。一連のプロダクトのセキュリティを自分たちの手で担保できる体制を整えるべく、迅速にAeyeScanの導入を進め、2023年4月から運用を開始した。

「AeyeScanが用意しているスタートガイドを参照することで、予想よりもスムーズに導入できました」（姉川氏）

　また、Web上に用意されているQ&A集が充実しており、わからないことがあればすぐ検索できた上、充実したサポート体制にも助けられたという。

「あるWebアプリケーションを診断する際、画面遷移で一ヶ所、どうしても詰まってしまうところがありました。サポートに問い合わせをしたところ、バグと認識され、後日『もう修正を完了したので、安心してお使いいただけます』と連絡をいただきました。こんなにスピーディに更新していただけて助かるなと思ったことが、非常に印象に残っています」（姉川氏）

　現在アイフルでは、複数のチームの手で20〜30種類のプロダクトが並行して開発されているが、各チームがスケジュールに合わせながらAeyeScanを活用している。コスト削減もさることながら、調整に関する工数を大幅に削減できた効果も感じているという。

「手動診断を依頼した際には、診断会社との事前調整だけで一ヶ月もの時間がかかってしまいました。開発など他のタスクを進める合間に、早かったり、遅かったりとタイミングもまちまちな相手からのレスポンスに対応する必要があり、ストレスもありましたが、そういった手間が一気になくなり、精神的にも楽になりました」（姉川氏）

　さらに、開発チーム側の都合に合わせていつでも脆弱性診断が行える点も、非常に大きなメリットと捉えている。

「外部に依頼すると非常に手間がかかりますが、ツールを使って診断を内製化すれば、自分の好きなタイミングで何回でも診断が行えます。コンスタントに、スムーズに、しかも柔軟なシステム開発が行えると思っています」（姉川氏）

　もちろん、クライアントやユーザー部門に対しても「きちんと脆弱性検査を行ったプロダクトであり、問題なくリリースできます」と根拠を持って示し、安心材料を提供できるようになった。

04 今後の展開

　アイフルではエンジニア一人一人がセキュリティを非常に重要な要素と捉え、セキュアな開発に取り組んでいる。

「セキュリティの専門家との知見の差を埋めるためにも、こういった診断ツールが有用だと感じます」と柿迫氏は述べ、スピードや開発生産性とのバランスもとりながら、セキュリティについても過不足がない状態を維持していきたいとした。

姉川氏も「外部診断の経験と比べ、AeyeScanは非常にスピーディで、信頼できるレポートも修正内容も含めて作成されるため、エンジニア目線でも非常にいい選択肢だったと考えています」と述べる。

　実は姉川氏は、エンジニアとして働き始めてまだ数年の若手だが、それでもAeyeScanのレポートの内容を理解しながら、プロダクト開発を進めることができている。今後、さらに多くのエンジニアがセキュリティを理解し、改善していく体制を整える上でも、AeyeScanの導入は非常に有益だと判断している。

　アイフルでは引き続き、セキュリティをしっかり考えた上でスピーディに開発が行えるエンジニアを育成し、便利で安心して使えるプロダクトを増やしていく方針だ。「ツールを活用しつつ、エンジニアのセキュリティに関する知見をしっかり培いながら、プロジェクトを推進していければと考えています」（柿迫氏）

　柿迫氏は「開発の速度を上げた結果、品質や安全性を下げるという選択肢はあり得ません。」と断言する。開発と運用、セキュリティを一体で進めるDevSecOpsも見据えており、そのためにもさらなる精度向上と自動化の推進に期待しつつ、AeyeScanを活用していく。

Company profile

アイフル株式会社

事業内容　消費者金融事業、事業者金融事業、信用保証事業

従業員数　単体 1,229名（2024年3月31日現在）　連結 2,470名（2024年3月31日現在）

ローン事業やクレジットカード・保証事業などを通じて、顧客の健全な消費活動や事業活動を支援し、経済活動に貢献。環境変化に応じた組織・制度の変革とデジタル技術の活用により、多角的な金融事業を国内外で展開している。

2024年4月時点

CASE 02 シンプレクス株式会社 様

アジリティとの両立が求められる金融システムに対し、持続可能な診断を内部で実施

課題

機能追加や画面の改修といったエンハンスのたびに外部に診断を依頼していたが、コストや調整面でハードルが高くなっていた。

導入

サポートの手厚さに加え、専門知識がなくともプロジェクト側でセルフサービス的に診断が実施できることからAeyeScanを選定。

効果

ナレッジを貯めつつ社内で持続可能な診断プロセスを構築し、ビジネスのアジリティを損なわずにセキュリティを確保。

01 背景と課題

シンプレクスは、長年にわたって手がけてきた金融関連のシステム・サービス構築はもちろん、そのナレッジを活かして他の領域にも事業を拡大している。

近年、金融をはじめ、あらゆるビジネスを取り巻く環境がこれまでにないスピードで激変している。「ある会社が一般投資家向けの金融取引サービスにおいて、 従来よりも低い手数料を発表したら、翌日にはそれをさらに下回る手数料を発表するといった具合に、情報更新のスピード感が求められています。その時に、ITがビジネスのアジリティを損ねないようにしなくてはなりません」（シンプレクス株式会社　クロス・フロンティアディビジョン　角田貴寛氏）

そこでシンプレクスでは、クロス・フロンティアディビジョンの各部門が連携しながら、クラウド基盤やマイクロサービス、DevOps、IaCといった「ビジネスのアジリティを損ねないためのIT技術」を積極的に活用し、機能や品質を担保した上で、開発者の負担を減らしつつアジリティを実現する取り組みを進めてきた。

だが、セキュリティに関しては問題が残っていた。「金融業界はもちろん、それ以外の分野でもセキュリティ対策は非常に重視されつつあります。我々もその重要性を認識し、サービスの立ち上げ時には外部の専門ベンダーに依頼して脆弱性診断を実施し、その後も追加開発や画面の改修といったエンハンスのたびに診断を行っていましたが、徐々にハードルが高くなっていました」（シンプレクス株式会社　岸野秀昭氏）

外部に診断を依頼するとコストがかかるのはもちろん、事前の調整も不可欠になる。一方で、開発プロジェクトには不確定要素がつきもので、必ずしもスケジュール通りに進むとは限らない。「診断員のリソースを確保するために二ヶ月くらい前から調整し、発注をかけていく必要があるのですが、いざ期日が近づくと、進捗が遅れているため期日を延ばしてほしいといった調整が発生することがあり、対応する手間が増えていました」（岸野氏）

コストや調整の手間といった課題をクリアして「持続可能な脆弱性診断」を実現するために、シンプレクスではツールを導入して診断を内製する方針に決定した。

02 ソリューションの選定

ツールの選定に当たってまず重視したのは、「開発に当たるプロジェクトチーム側でセルフサービス的に診断できること」だった。

加えて、診断を正確に実施するには、その前段でサイトを巡回するシナリオを作成する必要がある。診断すべきページを漏れなく網羅できているかを最も適切に判断できるのは開発者自身であり、その意味からも開発者自ら診断する方が望ましいと判断した。「中には、特殊な条件でしか発注できない商品を扱う金融取引もあります。 そこまで含めてセキュリティチームが把握するのは難しく、プロジェクト側が行う方が望ましいと考えました」（岸野氏）

その観点で、オープンソースのものも含め複数のツールを比較。必ずしもセキュリティ専門ではないエンジニアでも利用できることからAeyeScanが浮上した。

AeyeScanの特徴の一つは、AIを活用して巡回シナリオを作成できることだ。シンプレクスでもAI活用に取り組み始めていることもあり、抵抗なく、むしろ開発エンジニア

が事前に多くのスキルや知識を持たなくても良いことにメリットを感じた。

加えて、国産ツールならではのメリットとして充実したサポート体制が整っており、セキュリティベンダーのラックがパートナーとなって支援を得られることも安心感につながった。「実際にトライアルを行ってみても、使って感じた課題に対するエンハンスを迅速に取り込んでいただくなどフットワークの軽さを感じ、この先何か問題があっても柔軟に対応してくれそうだと感じました」（岸野氏）

さらに、多数のサービスに診断を行っても一定のライセンス費用で診断が行えることも後押しとなり、採用を決定した。

シンプレクスでは、時期によって変動はあるものの、常に数十から100近くの開発プロジェクトが稼働している。一方でセキュリティチームのリソースには限りがあり、全てのリリースに対して診断を行うやり方ではスケールしづらい。「プロジェクトチーム側で診断作業を行ってもらい、サポートが必要になれば我々を頼ってもらう形が現実的だと考えました」（岸野氏）

03 導入効果

シンプレクスは2024年1月から、サービスのエンハンス時にAeyeScanによる診断を「必須」とする運用を開始した。そこから約2ヶ月の間に、AeyeScanによる診断を経てのリリース数は早くも約30件に上っている。

セルフサービス的な診断を実現する際には、自分たちが関わるリリースに対してだけ診断が行えるよう、プロジェクトメンバーに対するアクセス制御が必須となる。シンプレクスはその仕組みをAeyeScanのAPIを活用して実現した。「APIを提供してもらうことで、アカウントの払い出しや権限の付与を柔軟に行える仕組みをツール化し、自動化できたのは良かったポイントです」（岸野氏）

ただ、どうしても自動巡回ができない部分が出てきたり、診断に時間がかかる場面も生じてしまう。シンプレクスはその都度エーアイセキュリティラボのサポート窓口に問い合わせ、回答や対応履歴を記録することで社内のQA集を充実させていき、ナレッジを蓄積していった。この結果、「便りがないのは良い便りではありませんが、大量のクレームが来ることもなくうまく回っています」（岸野氏）

運用がスムーズにいった要因として、ただツールを採用して終わるのではなく、組織的な取り組みを進めたことが挙げられる。

シンプレクスでは今回の施策を、脆弱性診断の必須化というトップダウンの指示の元、全社的な取り組みとして進めてきた。加えて、AeyeScanの本格運用を始める半年ほど前からしっかり時間をかけて繰り返しリマインドを行い、必須化するまでには少なくとも一回はAeyeScanによる診断を経験し、操作に慣れてもらうようにしたという。

さらに「私たちが常にTeamsのオンラインミーティングに控え、プロジェクト側でスキャンを行って何かトラブルがあったらすぐに入っていく『強化サポート期間』を定期的に設け、社内のエンジニアが安心して使える体制を用意しました」（岸野氏）

また、現場の中心となって各プロジェクトを取りまとめるシニアプロジェクトマネージャーに声をかけ、協力を得たこともポイントだ。意思決定権者を巻き込む工夫をしたことで、AeyeScanによる診断必須化を混乱なく、うまく進めることができた。

ポイント

- エンハンス時の診断を必須化し、セキュアに開発するカルチャーをいっそう醸成
- プロジェクト側で診断を実施し、ビジネスのアジリティを損なわずにセキュリティを担保
- サポートへの問い合わせや対応履歴といったナレッジを蓄積し、スムーズな運用を実現

04 今後の展望

AeyeScanの導入によって、持続可能な診断体制を実現したシンプレクス。セキュリティ水準がどれだけ向上したかを数値で示すのは難しいが、「AeyeScanというツールなくしては、社内で手軽に脆弱性診断ができる仕組みを整え、セキュアに開発するカルチャーをいっそう醸成することはできなかったと捉えています」（岸野氏）という。

診断は自動化が難しいと考えていた角田氏も、「専門知識がなくても短納期で、何よりビジネスのアジリティを損ねずに診断を実施できるのは本当にすごいことだと感じています」と述べている。

シンプレクスは今回の診断必須化だけでなく、SBOMの必須化、クラウド環境のアカウント管理や監査の仕組みの構築、全社規模でのセキュリティ訓練の実施など、さまざまな側面からセキュリティレベルの向上に努めている。

AeyeScanも、ビジネスの足を引っ張ることなくセキュリティを高めていく技術の一つとして、引き続き活用していく。

Company profile

シンプレクス株式会社

事業内容　コンサルティングサービス、システム開発、運用保守

従業員数　連結従業員数1,554名（2024年4月1日現在）

シンプレクスは1997年の創業以来、メガバンクや大手総合証券を筆頭に、日本を代表する金融機関のテクノロジーパートナーとしてビジネスを展開してきました。現在では、金融領域で培った豊富なノウハウを活用し、金融以外の領域でもソリューションを展開しています。2019年3月にはAI企業のDeep Percept株式会社、2021年4月には総合コンサルティングファームのXspear Consulting株式会社がグループに加わり、創業時より付加価値の創造に取り組んできたシンプレクスとワンチームとなって、公的機関や金融機関、各業界をリードする企業のデジタルトランスフォーメーション（DX）の推進を支援しています。

2024年5月時点

CASE 03 株式会社JOBPAY 様

エンジニアの手をほぼ動かすことなく診断を実施、高レベルのセキュリティを実現

課題

人や予算が限られる中、少ない工数でより高頻度の脆弱性診断をいかに実現するかを模索

導入

エンジニアの作業工数がかからず、問い合わせへの対応も迅速なことからAeyeScanを選定

効果

自動化機能も駆使し、工数をかけることなく、資金移動業者としてのセキュリティを確保

01 背景と課題

JOBPAYでは、ATMで直接受取りまたは口座振込を選択できるコンテンツの利用により、給与日前に給与相当額を受取れるサービスを提供。警備や飲食、訪問介護など給与前払いが歓迎される業界を中心に、すでに登録会員が12万人を超える。

金融サービスは内閣サイバーセキュリティセンター（NISC）が定義する「重要インフラ」の一つとして社会基盤を支える存在であり、万一システムに支障が生じた場合には社会に大きな影響を与える恐れがありセキュリティ体制は事業の要だ。

「資金移動を伴うサービスを提供している以上、障害が起きたり、脆弱性を突かれてサービスが止まるといった事態が起きないよう、24時間365日安定して動くことを重視し、緊張感を持ってサービスを提供しています」（株式会社JOBPAY　サービス開発部　開発グループ　サブマネージャー　長峰大輝氏）

こうした立場からJOBPAYは、セキュリティに関しても一層厳しく取り組む必要があると考え、さまざまな対策に取り組んできた。その一つがWebサービスの脆弱性診断だ。同社は中核となる支払いシステムだけでなく、周辺サービスとして会員向けサイトの他、勤怠情報を入力するための打刻サイトなど、複数のサービスを開発・展開している。これらについても脆弱性診断を実施してきた。

「ただ、診断サイクルは年に一回程度にとどまっていました。重要インフラ事業者としてその頻度では少なすぎると判断し、より短いサイクルで診断を回したいと考えましたが、エンジニアのリソースに限りがある以上、診断だけに人やコストを割くわけにもいかないという課題がありました」（長峰氏）

02 ソリューションの選定

周辺サービスは基幹の支払いシステムとは異なり、アジャイル的な手法を用いて比較的短いサイクルで、時には週に数回のペースでリリースを繰り返している。これらの脆弱性診断を行うに当たって、同社は三つの選択肢を検討した。

一つ目は、診断サービスを提供する外部の企業に定期的に依頼する方法だ。だが、「実際にスキャンを始めるまでにさまざまな資料を用意しなければならず、そこに多くの工数を取られることを懸念しました」（長峰氏）。診断を一回実施するたびに費用がかさむことも、向いていないと判断する理由となった。

二つ目は、診断対象のシナリオ作成、いわゆるクローリング作業を人が手で行い、その後のスキャンは自動的に実施する半自動ツールを用いて診断を内製する方法だった。コスト的には最も有利な選択肢だったが、「画面をぽちぽち触りながら登録していく作業に多くの工数が取られることがネックでした」（長峰氏）

そして三つ目がAeyeScanだった。「ツール本体のコストとエンジニアのコストを合わせて比較してみると、半自動ツールとほぼ変わらない結果になりました。ならば、エンジニアの作業工数がかからない方がエンジニアが他のところにリソースを割くことができる上、慣れていけばさらにエンジニアのコストを減らせると判断しました」（長峰氏）

JOBPAYはさらにAeyeScanのPoCを行い、実際の使

用感を確認した。JOBPAYの周辺サービスは、前払い支援というサービスの特性もあり、メールアドレスなどのIDとパスワードだけでログインできる一般的なサイトとは異なり、カード番号も加えた三つのフォームに入力する必要があるなど、特殊な作りのページも含まれる。「当初は自動巡回だとうまくログインできない場面もありましたが、その旨をエーアイセキュリティラボに伝えるとすぐに修正してもらえました」（長峰氏）

その対応に安心感を抱いたことと、当初の目的通り、診断サイクルをどんどん短くしていける手応えがつかめたことから導入を決定した。

03 導入効果

JOBPAYは2022年からAeyeScanを導入し、各サービスに対して四半期に一回のペースで診断を行う体制で運用している。当初はうまく巡回できない場所があるといった課題もあったが、その都度、AeyeScanのサポートからアドバイスを得ることで解決できた。「何か問題が起きても聞けるところがあるのは、非常に大きな安心感になっています」（長峰氏）

レポート結果は管理画面を介して開発エンジニアと共有している。「診断が終われば自動的にレポートが出力されます。英語で書かれた他のツールですとどうしてもハードルが高くなりますが、AeyeScanはきちんと日本語で出力されておりエンジニアにも伝えやすいですし、エンジニア以外の方が見てもわかりやすい内容だと思います」（長峰氏）

これまでのところ、迅速な対処が求められる深刻な問題は検出されていない。比較的優先度の低い問題を、開発スケジュールをにらみながら「今年中に修正するスケジュールで行きましょう」といった具合に相談しながら対応している。

AIによる自動巡回機能によって、診断の工数は大きく削減できた。同社の舟山侑希氏（サービス開発部　開発グループシステムエンジニア）は「以前の工数を100とすれば、今は10以下、ひょっとするとゼロかもしれません」と述べる。また長峰氏も「人数も決して多いわけではないため、脆弱性診断だけに人を一人張りつけるのは難しい状況であり、とても助かっています」と評価する。

JOBPAYでは、AeyeScanのスケジュール機能を用い、診断を定期的に実施するよう自動設定した上に、APIを用い、レポートが出力されたらSlackに自動通知する仕組みを実装。エンジニアがほぼ手を動かさなくても診断サイクルを回せる仕組みまで整えた。「スタートさせておいて、あとは他の作業をしていればよく、終わったらSlackの通知を見てレポートを共有するだけなので非常に楽になりました。スケジュールを設定することで、今や診断のスタートボタンすら押す必要がなくなっています」（長峰氏）

脆弱性診断の結果は、万一問題が発生した際の「証跡」としても活用できると考えている。そうした事態が起きないのが一番だが、仮にセキュリティインシデントが発生したときに「何をやっていたのか」と責められても、「このようにきちんと診断を実施し、セキュリティを担保してきました」と、責任を果たしてきたことを示すツールとしても役立つと考えている。

ポイント

- AIで工数を大幅に削減しつつ、資金移動業者に求められるセキュリティ水準を実現
- APIを活用してSlackと連携し、レポート出力通知を自動化
- サポートの手助けを得ることで、やや複雑なログイン画面でも巡回を自動化

04 今後の展望

「資金移動業者としてセキュリティ面は絶対に落とすことはできませんが、工数もそれほどかけられません。この二つの問題を一気に解決できるのがAeyeScanだと感じています」（舟山氏）

JOBPAYは今後も、AeyeScanを活用した診断の自動化を拡大していく計画だ。現時点では、診断が終了した旨の通知に留まっているSlackとの連携をさらに広げ、AWS Lambdaなどを活用してレポートそのものをSlackに送付し、コンソールにログインしなくても結果を確認できるようにして、開発者の生産性をさらに高めたいと考えている。

ゆくゆくはCI/CDサイクルにAeyeScanを組み込むことも検討している。「プログラムを改修してリリースした際に、同時にAeyeScanによる診断を回すことが目標です。そうすれば、工数削減と同時に診断サイクルをさらに短縮でき、セキュリティを担保して、顧客メリットも大きくなると考えています」（長峰氏）

おりしも同社ではVisual Studioで構築されていた基幹システムをリニューアルし、Webアプリケーションに置き換える一大プロジェクトも進行中だ。「これが置き換わった際には、AeyeScanをさらに広範囲で活用し、セキュリティを診断を自動的に、定期的に実行することになるかと思っています」（長峰氏）

Company profile

毎日を、給料日にする。 JOBPAY

株式会社JOBPAY

事業内容　給与前払いサービス、および求人コンテンツサービス

給与前払いサービス及び求人コンテンツサービスを展開。給料日を待たずに、ATMから引き出せる給与現金随時払いサービス「JOBPAY（ジョブペイ）」を提供している。

2024年6月時点

CASE 04 タイガー魔法瓶株式会社 様

コストを抑えて、時短、簡単、高精度な診断が実現できた

課題

公開サイトの診断を外部委託していたが、数百万円単位の診断コストがかかるだけでなくスケジュール調整等の負荷も高く、内製化を検討していた。

導入

自動巡回の精度や脆弱性の検知率、誤検知の少なさ等を定量的に比較検討した結果、AeyeScanが一番だと判断して導入を決定。

効果

2022年9月から公開サイトを対象に年1回の定期診断を順次展開中。「自動巡回機能」により作業のほとんどを自動化でき、担当者の負荷も軽減できた。

01 背景と課題

タイガー魔法瓶は「世界中に幸せな団らんを広める。」というビジョンを掲げ、「真空断熱技術」と「熱コントロール技術」を生かした魔法瓶や炊飯器といった調理家電を提供し続けてきた。2023年2月3日に創立100周年を迎え、記念商品なども販売している。

この100年で変化したことの1つがデジタル化だろう。タイガー魔法瓶もメーカーとして、スマホアプリと連携して家事DXを実現するIoT炊飯器を開発・販売するほか、販路としてもインターネットを活用し、ECサイト「タイガーオンラインストア」を展開。ほかにもコーポレートサイトを通して取り組みを伝え、顧客との接点を強化してきた。

ただ、こうした公開サイトのセキュリティをどのように担保するかが課題となっていた。「コーポレートサイトをはじめ公開サイトについては、新規立ち上げ時や、リニューアルのタイミングで必ず脆弱性診断を実施するルールになっていました。しかし、その診断を外注せざるを得ない状況がありました」（タイガー魔法瓶株式会社　経営企画グループ　情報システムチーム　主事　安川明伸氏）

タイガー魔法瓶では基本的に、Webサイトの構築・開発は外部の事業者に委託してきた。しかし、セキュリティの担保はやはり自社の責任だ。ただ、脆弱性診断には専門的なスキルやノウハウが必要となる。セキュリティ人材不足がうたわれる中、社内でそうした人材を確保するのは難しく、ここも外注せざるを得ない。この結果、1つのサイトを診断するのに数百万円単位のコストがかかる上に、診断実施に至るまでの調整コストも膨らんでいた。

また、日程調整も大きな課題であった。「リニューアル時などはスケジュールがギリギリになってしまい、脆弱性診断を実施するのも日程的に厳しい状況になってしまうことがありました。また、いざ実施するとなっても外部の診断業者とのスケジュール調整を、非常にタイトな日程の中でやらなければいけないこともありました」（安川氏）

02 ソリューションの選定

おそらく多くの企業が同様の課題を抱えているだろう、こうした背景からタイガー魔法瓶では脆弱性診断の「内製化」を目指し、そのための診断ツールを探し始めた。

まず情報収集を進め、その中から国内でも実績のある脆弱性診断ツール3種類に絞り込んでいった。「自分たちでも使いこなせるか、運用できるか」という点を重視しながら、社内のいくつかのサイトを対象にPoCを実施した結果、選択したのがAeyeScanだった。

特に評価したポイントの1つが「自動巡回機能」だ。「他のツールも自動巡回機能や自動診断機能を備えていましたが、実際に試してみると止まって進まないことがあり、結局人が手を動かさなければならないこともありました」（安川氏）。AeyeScanはそれらに比べ自動巡回の精度が高く、仮に行き詰まる箇所があっても充実したサポートによって解決できたという。

2つ目のポイントは診断精度だ。他の製品では、過検知も含め非常に大量のアラートが検出され、「本当にそれが正しい指摘なのか」を見極める作業が必要となる上、自分たちだけで判断を下すのは難しいと感じた。これに対しAeyeScanでは信頼性のある結果が得られた。

「自動巡回の精度、そして検知率や誤検知の少なさといった精度を定量的に比較検討した結果、AeyeScanが一番だと判断しました」（同情報システムチーム、松田晋篤氏）。これまで外注していた診断費用に比べて、コストを大幅に削減できることもポイントだった。

率直に言えば、AeyeScanは立ち上がって数年という比較的新しいサービスであり、歴史や実績の面で不安がなかったわけではない。しかし、情報処理推進機構（IPA）の「2021年度セキュリティ製品の有効性検証における対象製品」に選定されたことも後押しとなった。

03 導入効果

タイガー魔法瓶は2022年9月からAeyeScanの導入を開始し、まず安川氏、松田氏の2人で診断の内製化に取り組み始めた。手始めに、ちょうどリニューアルのタイミングを迎えていたコーポレートサイトのリリースに合わせて診断を実施したのを皮切りに、年に1回の定期診断という位置づけで公開Webサイトを対象とした診断を順次展開している。

PoC段階から評価していた「自動巡回機能」を活用することによって、作業のほとんどを自動化することができ、担当者の負荷軽減につながっている。加えて、開発側が気付いていなかった細かな脆弱性が指摘される場面もあり、セキュリティレベルの担保にもおおいに役立っていると感じている。

さらに、使い始めてみて実感したのが、GUIの使いやすさだ。「GUIが直感的に作られているため、使いやすいだけでなく、CSIRTの他のメンバーにAeyeScanの使い方を教育しやすいと感じています」（松田氏）。この先、内製化を進めるにあたって人員の育成は不可欠だが、脆弱性診断の方法を教える側、教えられる側の双方にとって理解しやすい点がポイントだと語った。

クラウドサービスならではの、こまめな機能改善にも好印象を抱いている。たとえば、何らかの理由で巡回しきれなかったページがあった場合に最初から診断し直すのではなく、中断した時点から先だけを再検査できる機能が、バージョンアップで新たに加わった。「ちょっとした手間を省ける機能、かゆいところに手が届く機能がどんどんAeyeScanに追加されていくので、とても便利だと感じています」（松田氏）

ポイント

- 自動巡回の精度が高く、行き詰まる箇所があっても充実したサポートによって解決できた
- 過検知・誤検知が少なく、信頼性のある結果が得られる
- 外注していた診断費用と比較して、コストを大幅に削減できる

04 今後の展開

タイガー魔法瓶ではAeyeScanを活用し、定期的に脆弱性診断を実施しつつ、診断の頻度を高めることで、公開Webサイトのリスクを下げていきたいと考えている。

また今後は、IoT製品とWebサイトやアプリのやりとりを担うAPIについても、現時点では脆弱性診断を外注しているが、ゆくゆくはAeyeScanを用いて内製化できればと期待している。

「安く早く脆弱性の診断ができるという話を聞いて、当初は『そんなうまい話があるのかな』と疑心暗鬼でした。しかし、しっかり社内で検証を行った結果、機能面でもコスト面でもバランスの取れた製品であることがわかり導入しました。いい判断だったと思いますし、本当に安く早く診断ができる環境を実現できて驚いています。また、Webサイトの構築業者や診断業者にお任せではなく、我々自身が

診断し、セキュリティ強化に向けたアプローチをしていける点でも非常に有効な手段であり、今後もフルに活用していきたいです。」（同情報システムチーム　マネージャー　竹原健太氏）

Company profile

タイガー魔法瓶株式会社

事業内容　生活用品総合メーカー

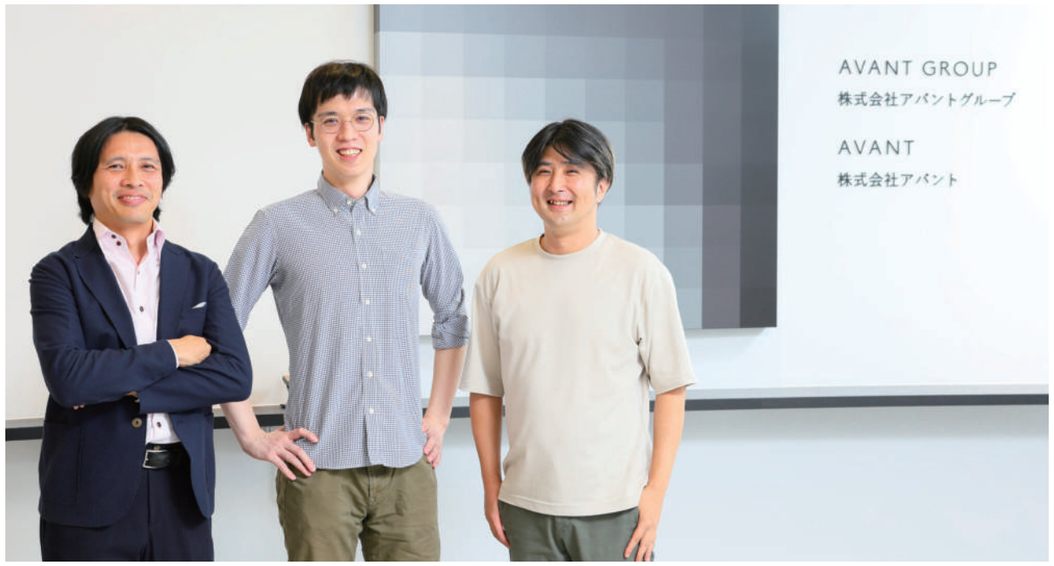
従業員数　769名（2023年6月時点）

「世界中に幸せな団らんを広める。」というビジョンのもと、真空断熱ボトルや卓上用ポットに代表される「真空断熱技術」と電子ジャーをはじめとする炊飯器などの「熱コントロール技術」を用いた製品づくりで、食卓からアウトドアまで、さまざまな暮らしのシーンに快適さと便利さを提供している。

2023年5月時点

CASE 05 株式会社アバントグループ 様

開発の中にセキュリティを浸透させる取り組みをAeyeScanが加速



課題

アプリケーション開発のセキュリティ強化を開発者が日常的に意識し、対応できる環境が整っておらず、散発的な対応となっていた。

導入

開発者にわかりやすいレポートが提供され、OWASP Top 10をはじめとする業界標準に沿ってリスクが示されることを評価し、AeyeScanを採用。

効果

リスクを定性的かつ定量的に把握し、共通の土台を作ることで、セキュリティエンジニアと開発者のよりよいコラボレーションを加速。

01 背景と課題

アバントグループは、連結会計ソフトウエア開発をはじめとして、決算業務アウトソーシング、グループ経営支援、DX・データ活用支援など幅広く事業を展開し、さまざまなサービスの提供を通じてお客様の経営のDXを総合的に支援している。

「市場環境が変化し経営者の責任範囲も拡大する中、求められる情報の質と量は過去とは圧倒的に異なっています。我々は、ノウハウを形にしたソフトウェアのパワーでお客様をご支援し、企業価値を高めるお手伝いをしています」（株式会社アバントグループ　マテリアリティ実現室 ディレクター 兼 株式会社ディーバ プロダクト開発本部、三宅良和氏）

27年にわたる歴史の中でIT環境は大きく変化し、アバントグループの中核会社であるディーバ自身もクライアント・サーバ型のパッケージソフトウェアから、クラウドを前提にしたサブスクリプションモデルへとビジネスのあり方をシフトしている。一連の変化に伴って浮上した課題の1つが、セキュリティだった。

「お客様に製品ではなく利用価値を届ける形にシフトし、責任分界点が変わっていくにつれ、社内のセキュリティ体制に危機感を覚えるようになりました。そこでクラウド展開を準備するタイミングでグループクラウドセキュリティ推進室を手探りで立ち上げ、仲間を集めながら整備に取り組んでいます」（三宅氏）

そんな仲間の一人としてディーバに加わった山本裕介氏（株式会社アバントグループ　グループクラウドセキュリティ推進室 シニアマネージャー 兼 株式会社ディーバ プロダクト開発本部 プロダクト開発統括部 SRE部長(当時)）によると、アバントグループは、他のソフトウェア会社とも共通する悩みに直面していた。

「検討を始めた当初は、まずお客様のニーズに応え、リリースしていくことが第一となりがちで、非機能要件であるセキュリティ対策は相対的に優先度が低くなる傾向がありました」（山本氏）

今は社内でセキュリティを率いる立場にある宮部大志氏（株式会社ディーバ プロダクト開発本部 セキュリティガバナンス部）も、入社当初はアプリケーションエンジニアとして製品開発に携わっていた。「以前は、開発チーム内ではセキュリティ要件よりも機能要件に関するものが優先的に議論される傾向がありました」と同氏は振り返る。

しかし今や、顧客情報の漏洩でも発生すれば、事業そのものに大きなインパクトが及ぶ時代だ。エンジニアチームでも徐々にセキュリティを担保したプロダクト開発の気運が高まってきたが、問題は具体的な手段とそれを担う人材だった。「チーム体制を見直していく必要がありました」（宮部氏）

02 ソリューションの選定

将来的にグループ全体への適用も視野に入れて、子会社のディーバで先行検証（PoC）を進めることにしてソリューションの検討を開始した。当初検討したのが、オープンソースソフトウェアとして無償で公開されている「OWASP ZAP」だ。しかし「出力されたレポートを見ると、セキュリティエンジニアにはわかっても、開発者がすぐに理解しやすい状態かというと疑問が残りました」（宮部氏）

そこで、開発者にも問題や対処方針がきちんと伝わるレポートが出力されることを条件に他のツールを探し始めた。「この先、セキュリティエンジニアだけでなく開発者もセキュリティを理解し、修正していく文化を根付かせるには、開発者が出力されたレポートを理解できることが重要であり、それが製品の品質の底上げにつながると考えていました」（山本氏）

他に、結果がベンダー独自の解釈に頼るのではなく、OWASP Top 10をはじめとする標準的な指標とひも付け

され、網羅的に確認できること、オンプレミス環境ではなくSaaS形式で利用できること、検査を実施するチームだけでなく結果を参照する関係者らの権限管理が適切に行えることなど、脆弱性検査という基本機能以外の要件も加味して検討した結果、AeyeScanが浮上した。

もう一つ見落とせないポイントはコストだ。サイト数に基づく課金体系では、グループ企業が展開するサイト・サービスに対象を拡大していくと価格が跳ね上がってしまい、導入しにくい。

「AeyeScanは、どれだけスキャンを回しても年間定額で利用できるため、コストパフォーマンスに優れると判断しました」（山本氏）

03 導入効果

導入検討に際して、まずはディーバにてPoCを実施した。「過検知・誤検知も含めて自力でひもといていく必要のあるOWASP ZAPに比べ、AeyeScanのレポートは非常に読みやすいと感じました」（宮部氏）

単に検出された脆弱性を羅列するのではなく、CVSSをはじめとする一般的な評価基準に基づいてリスクが示され、「どのパラメータで脆弱性が検出されたか」「どんなレスポンスが返ってきたため脆弱性と判断したのか」といったエビデンスが、スクリーンショットとともにレポートされるため、追跡や検証が容易なことも評価につながった。「非常に理解しやすく、見やすいという印象を持ちました」（宮部氏）

さらにレポートの末尾には、OWASP Top 10など各種標準との対応表が付加されている。「これも今後、セキュリティ部門として、各種標準に基づいて評価していく上で有効に活用できるのではないかと考えました」（宮部氏）

設定が容易に行えることも印象に残った。英文のサイトを検索し、「果たしてこれで正しいのだろうか」と試行錯誤しながら設定していたOWASP ZAPとは異なり、AeyeScanにはわかりやすいユーザーインターフェイスが用意されている。

「将来的に、セキュリティガバナンス部だけでなく開発チームがスキャンを回していく場面も増えていくと考えています。そんなときに、品質高く、標準化して回していきやすいと感じました」（宮部氏）

ディーバのPoCの結果を受けて、アバントグループではAeyeScanを採用することに決定し、2023年春から導入していった。SaaS形式の利点が生き、導入は非常にスムーズに進んだ。

ディーバが提供する製品については、サーバやクライアントアプリケーションに改修を加えたタイミングでセキュリティガバナンス部がAeyeScanで診断を実施し、結果を開発者に共有している。さらに、アバントグループが外部に公開しているWebサイトやサービスに対しても、三ヶ月に一回の頻度で定期的に診断を回し始めている。

実のところ、AeyeScanの導入後、クリティカルに分類される深刻な脆弱性は発見されていない。安全に開発できていることが再確認できた形だ。そして当初の狙い通り、開発者にもわかりやすいレポートが得られている。

「グループ会社それぞれに所属する開発者にAeyeScanのレポートを見せると、やはり、わかりやすいとレスポンスがありました」（山本氏）

「技術者はもちろん、その上長や関係者にも共有しやすくなると期待しています。ただ危ないと言うのではなく、どこがどう危ないのかが具体的になるためアクションにつなげやすくなる効果も一部出ており、これをグループ全体に浸透していきたいと考えています」（三宅氏）

最近ではAeyeScanのレポートが、セキュリティエンジニアと開発者の共通の土台になりつつある。個人の知識に基づいてバラバラに会話をするのではなく、共通の認識を元に「リスクをどう判断し、どう対処していくか」「どの問題を優先すべきか」といった計画を立てられるようになり、組織としてプラスになっている。

「セキュリティはホラーストーリーで始まり、声の大きい人の意見に流されがちです。しかし、AeyeScanというツールを通すことによって、個々人の感覚ではなく、定量的かつ定性的にリスクをとらえることが可能になりつつあります」（山本氏）

ディーバではまた、宮部氏が主体となって、クロスサイトスクリプティングをはじめとする基本的な脆弱性に関するハンズオンデモを実施し、脅威について認識してもらう取り組みも展開している。開発者側も積極的に参加し、セキュリティガバナンス部に気軽に話しかけ、しっかりしたコミュニケーションが取れるようになった。

「セキュリティに関して、セキュリティエンジニアと開発者がよりよいコラボレーションができるようになりました。AeyeScanの導入はそれを加速している一因になっています」（山本氏）

04 今後の展開

顧客のセキュリティ要求水準は高まるばかりだ。「クラウドサービスはお客様の情報をお預かりする形になります。お客様が外部のサービスに情報を保管することに対して弊社が安全性を担保できないと安心してご利用いただくことができません。万一でも漏洩などの事象が発生すれば、お客様の事業にも影響を与える事態になりかねません」（山本氏）

アバントグループはそんな緊張感を持ちながら、グループクラウドセキュリティ推進室、各社のセキュリティ部門と開発者が一体となって、引き続きセキュリティ向上に取り組んでいく。たとえば、現在は三ヶ月に一回という頻度で実施しているグループ各社のサイト診断の頻度を高め、一ヶ月に一回、さらには一週間に一回といった具合に、よりリアルタイムに近づけていきたいと考えている。

また、開発時の規定やプロセスの整備、教育などを通したセキュリティ文化の浸透も引き続き推進し、DevSecOpsの確立に努めていく。「ある程度の段階まで来たら、開発者が自分たちでスキャンを実施し、自分たちで脆弱性を見つけて対処し、セキュリティ部門にはそのエビデンスを上げるだけという状態にしていければと考えています」（山本氏）

グループクラウドセキュリティ推進室も、開発者を突き放すのではなく、理解を促し、寄り添う姿勢で伴走していく。その際の共通言語としてAeyeScanを今後も活用し、「これまで以上に安全な状態で製品をお客様に出荷できるようになると思います」（山本氏）

Company profile

AVANT GROUP

株式会社アバントグループ

事業内容：グループ経営管理・連結会計・事業管理に係るソフトウエア開発、コンサルティング、システム企画・構築、導入支援、運用・保守

従業員数：連結1,389名（2023年6月時点）

財務情報・非財務情報を問わず様々な情報に基づき、お客様が適時・適切な経営判断を行い、経営改革を推進するためのソフトウエア開発・販売・保守や、ソフトウエアベースのコンサルティング・BPOサービスを提供し、「経営のDX」に貢献している。

2023年12月時点

CASE 06 株式会社マネーフォワード様

金融プロダクトすべてに、定期的な脆弱性診断の運用を実現

課題

プロダクトが増えるにつれ、網羅的・定期的な脆弱性診断ができているかの懸念が生じていた

導入

ライセンス体系、対応言語、診断精度に加え、継続的に活用できる使いやすさを重視しAeyeScanを選定

効果

全プロダクトで定期診断を開始し、自動巡回によって生成される画面遷移図も活用

01 背景と課題

マネーフォワードは「お金を前へ。人生をもっと前へ」というミッションを掲げ、すべての人のお金の課題解決を目指し、お金の見える化サービス『マネーフォワード　ME』やバックオフィスSaaS『マネーフォワード　クラウド』など50を超える多様なサービスを提供している。

「お金」という資産そのものに関する情報を扱う以上、同社のサービスには一定以上のセキュリティレベルが求められる。ただ、何が何でもセキュリティ第一ではなく、デベロッパーに寄り添いながら、現実的な解決策を模索してきた。

「開発者と非常に密接に働いており、コストなども考慮し、あるセキュリティ要件が満たせなければ代替手段がないかといった建設的な提案を行うことを大切にしてきました」（株式会社マネーフォワード　CISO室プロダクトセキュリティ部　セキュリティエンジニア　中川 浩輔氏）

その一環として、外部のセキュリティベンダーに依頼し、プロダクトの脆弱性診断も実施してきた。だが、事業が拡大し、プロダクトの数も増えるにつれ、脆弱性診断の間隔が空いてしまうことが懸念材料になっていたと言う。「サービスの立ち上げ時はもちろん、その後も新機能の追加や大規模な改修の際には脆弱性診断を行うことにしていましたが、それ以外はプロダクト側の判断に委ねていました」（中川氏）

そこでCISO室が起点となって、すべてのプロダクトを対象に、定期的に脆弱性のアセスメントを行いたいと考えるようになった。これは、複数の顧客から提出を求められる「セキュリティチェックシート」でも求められる事柄でもあった。

02 ソリューションの選定

外部の診断サービスでは、専門知識を持った診断員の目で深くチェックが行われる。マネーフォワードはその利点を認めながらも、内部での定期的な診断を併用する方法を模索し始めた。

「ベンダーに診断を外注する場合、その結果を社内でナレッジとして蓄積することはできません。また、基本的にエンドポイント数（画面数）に応じた料金体系となるため、コストパフォーマンス的な観点から網羅的な診断を受けづらい状況もありました」（中川氏）。外部との「契約」という形式に基づく以上、開発が予定よりも遅れた場合の調整が困難という課題もあった。

「ボタンを一つ追加するといった、それほど大きくもない改修のたびに外部に診断を依頼するのではなく、内部での診断で迅速に済ませるといった具合に、使い分ける選択肢を社内に持たせる方がベターではないかと考えました」（中川氏）

そこで、「外国籍エンジニアも多く在籍するマネーフォワードでの利用を想定し、日本語だけでなく英語にも対応していること」「自社だけでなく、グループ会社のプロダクトも診断できるライセンス体系になっていること」などを条件に、診断ツールの選定を進めていった。技術的にはOWASP Top 10やASVSで挙げられている主要な脆弱性を確実に検出でき、API診断も可能なこと、Slackをはじめとする外部サービスとの連携性も要件だった。

特に気にしていたのは使いやすさだった。マネーフォワードでは、過去に一度自動脆弱性診断ツールを導入し、内部での診断に取り組んだものの継続できなかった経験があった。「診断経験者以外にとってハードルが高くて継続できない、ということにならないよう、使いやすいツールを導入したいと考えていました」（株式会社マネーフォワード　CISO室プロダクトセキュリティ部　万 萌遠氏）

複数のツールの比較検討を進め、実際にいくつかのプロダクトを対象に検証を実施した末に選定したのがAeyeScanだ。特に印象に残ったのは、自動巡回機能のカバー率だった。「AeyeScanの自動巡回機能は、文句なしの二重丸でした。しかも、巡回した画面をURLのリストではなく、キャプチャ付きでビジュアルに示してくれるため、きちんと検査対象を巡回できたかどうかの確認が容易なことを評価しました」（中川氏）

03 導入効果

検証の結果も踏まえ、マネーフォワードではAeyeScanを導入し、2024年2月から内部での脆弱性診断を開始した。

導入初年度は約60のプロダクトを対象にAeyeScanによる定期脆弱性診断を実施することとし、5月末までに約20プロダクトの診断を完了している。その後も、AeyeScanによる診断を最低でも一年に一回は実施していく計画だ。

本格運用を開始してみると、検証時にも印象に残ったクローリング機能と画面遷移図のメリットにあらためて気づいたという。

マネーフォワードが展開するプロダクトは多数に上っている。一つや二つならばともかく、すべてのプロダクトについてどのような画面があり、どんな挙動が適切なのかといった事柄を、CISO室がすべて把握するのは困難な状況となっていた。

「定期脆弱性診断を開始したことで、各画面で行われるHTTPのリクエストやレスポンスも含め、どのような画面遷移があるかがAeyeScan側に保存されるようになりました。各プロダクトを理解した上で、開発者からの問い合わせに対応できるようになりました」（中川氏）

懸念していた使い勝手についても、「ドキュメント類が充実している上に、ユーザーインターフェイスが自明で、画面をクリックしていけば診断できます」（万氏）という。中川氏らが主導する形で、誰が実施しても同レベルで診断を行えるように社内での診断手順を標準化し、マネーフォワード推奨の診断設定をまとめた上で運用している。

診断結果は、AeyeScanが生成するレポートに加え、特に留意が必要な指摘項目についてはCISO室がコメントも加えてスプレッドシートにまとめ、開発チームと共有している。

同社の開発チームでは、自主的にSASTツールを導入、運用済みだ。そのため指摘される脆弱性も軽微なものばかりだという。「CookieにSecure属性が付いていないといった、LowやInfoレベルの脆弱性が指摘されています。そのためかどうかはわかりませんが、開発者からは、Cookie属性を意識した問い合わせが来ることもあり、脆弱性診断を経て開発者のセキュリティ意識が高まっているのかもしれません」（万氏）

現在は、外部ベンダーによる脆弱性診断の結果とAeyeScanの診断結果を個別に管理しているが、エーアイセキュリティラボの「診断マネジメント」を活用することで、一つのダッシュボードで統合的に管理していくことも検討している。

04 今後の展望

「当社はほぼすべてのサービスを内製で開発しており、当社のセキュリティスペシャリストのこの活動をAeyeScanがサポートしてくれています」と、マネーフォワード グループ執行役員 CISOの松久 正幸氏は評価している。

当面はCISO室プロダクトセキュリティ部のエンジニアがAeyeScanによる診断を実施しているが、標準化した手順をベースに、診断ツールを使いこなすメンバーを広げていく方針だ。マネーフォワードには別途、プロダクトのテストを実施するQAチームが存在しており、そちらでも簡易的に脆弱性診断を実施していたが、「AeyeScanの方が使い勝手がいいと感じているため、QAチームにも使ってもらい始めています」（中川氏）

同時に、グループ企業とも定期的にミーティングを持ち、互いの状況を把握した上で、グループ統一のセキュリティスタンダードを適用し、全体での底上げを図っていく。ここでもAeyeScanを活用できればと考えている。

その意味で、「AeyeScanの機能がさらに向上し、ロジックバグを指摘したり、自動クローリングのカバー率がさらに向上して人間に劣らないような品質で診断ができるようになり、DASTとしてのデファクトスタンダードになるとうれしいと期待しています」（万氏）

今後もマネーフォワードでは、「現場や開発者に寄り添う」という原則を貫きながら、さまざまな施策を実施していく。会社の成長と共にCISO室の体制も強化しており、AeyeScanの導入に加え、クラウド環境のセキュリティ統制などさまざまなセキュリティ対策を進めている。今後はそうした取り組みの一部をテックブログなどで公開し、活動の透明度を高めていきたいという。

Company profile

株式会社マネーフォワード

事業内容	PFMサービスおよびクラウドサービスの開発・提供
従業員数	2,400名（2024年5月末日現在）

「お金を前へ。人生をもっと前へ。」というミッションを掲げ、すべてのお金の課題解決を目指すSaaS/Fintech企業。個人向けお金の見える化サービス『マネーフォワード ME』や事業者向けバックオフィスSaaS『マネーフォワード クラウド』など、50を超える多様なサービスを提供している。

2024年7月時点

CASE 07 株式会社エイチ・アイ・エス様

増え続ける社内からの診断依頼に効率よく応じるため、AeyeScanで大部分を自動化

課題

セキュリティの内製化が困難である一方で、外部に診断を委託するコストも削減したかった。

導入

情報処理推進機構（IPA）の検証でも高評価を得ていたAeyeScanのPoCを実施し、「7割以上は自動化が可能」という点が決め手となり導入を決定した。

効果

5日かかっていた診断作業を約3日に短縮できた。ツール習得コストも低いため、今後は診断要員の育成スピードを上げて内製化比率を高めていく。

01 背景と課題

国内だけでなく海外にも多くの拠点を展開し、国内外のツアー企画販売やホテル事業など、旅行を中心としたさまざまなサービスを提供している株式会社エイチ・アイ・エス（以下、HIS）は、コロナ禍を経て再び人の移動が活発化する中、新たな挑戦に取り組んでいる。

こうした状況で顧客と企業を結ぶ重要なチャネルとなっているのがオンラインだ。HISでは大小合わせると、のべ150種類以上のWebサービスやアプリケーションを開発しており、その数は今も増え続けている。

そんなHISにとって、セキュリティ対策は重要な柱の一つだ。Webサイトに示した「情報セキュリティ基本方針」にもある通り、顧客から預かった個人情報や情報システムなどの「情報資産」を脅威から保護するため、 さまざまな施策に取り組んできた。

そうした対策の一つが、Webアプリケーションの脆弱性診断だ。数年前は、リリース前に行う脆弱性診断の重要性がなかなか認知されない部分もあったが、粘り強く社内での啓蒙・啓発に取り組んできた。また、ニュースなどでWebアプリケーションの脆弱性を狙った不正アクセスがたびたび報じられることもあり、徐々にアプリケーションの開発者にも、またその開発を依頼する事業部側にも、脆弱性診断の必要性が浸透してきた。

問題は、それを実施する体制だ。HISが開発するWebアプリケーションは 、社内の内製部隊が開発するもの、外部のパートナーに依頼するものも含めると3桁のオーダーに上る。それらすべてに診断を実施しようとすると、現体制では対応できなくなってきた。対応しきれない部分は外部の専門サービスに依頼することもあったが、そのコストも無視できない額に膨らんできた。

02 ソリューションの選定

それまでHISでは手動で診断を実施していた。かつては、「なぜこんな面倒なプロセスが必要なのか」といった反発もあった というが、少しずつ理解を得られるようになり、内製での脆弱性診断が軌道に乗り始めた。だが、コロナの影響でオンラインへのシフトが進み、どう頑張ってもさばききれない量の診断依頼が押し寄せることになった。

しかも、Webアプリケーション診断は一度実施すれば終わりではない。顧客の利便性向上のため支払い方法を追加するなどの大規模な改修や、プラットフォームの変更が行われるたびに診断依頼が寄せられる。

こうした状況を解決するには、脆弱性診断の自動化を進める必要がある。HISはそう判断し、2022年7月から脆弱性診断ツールの情報収集を開始した。その中で浮上したのがAeyeScan（エーアイスキャン）だ。

選択の決め手は、情報処理推進機構（IPA）の「2021年度セキュリティ製品の有効性検証の試行」において選定されたことだ。「自動化できても、性能が落ちてしまっては意味がありません。その意味でIPAのお墨付きがあり、高評価を得ていることが重要だととらえました」（石谷氏）

早速エーアイセキュリティラボに連絡を取り、既存のテストケースを示してHISが抱えている課題について相談しながらPoCを実施した。その中で「7割以上は自動化が可能」という回答が得られたことも決め手の後押しとなった。最も多くの利用者がある旅行商品購入サイトなどに加え、社内で利用しているイントラネットのシステムを対象にPoCを実施し「これならいけそうだ」という手応えを得て、同年9月、正式に導入を決定した。

03 導入効果

HISでは現在、開発部門とセキュリティ部門が連携しながら脆弱性診断を実施し、セキュアなアプリケーションの提供に努めている。

具体的には、以下のような3ステップで診断を進めており、一部は手動で作業する部分もあるものの、診断に要する時間は以前に比べ確実に削減できた。

「以前はフルに5営業日かかってしまい、他の業務にまでなかなか手が回りませんでした。しかしAeyeScan導入後は、1日フルに使わず6時間程度の作業時間と短縮しつつも、約3営業日で診断を終えています」（岩崎氏）。あらかじめ仕掛けておけば、かなりの部分を自動で診断できる点が工数削減に役立っている。

また、レポート機能も重宝している。「以前はレポート作成作業だけで丸1日割いていました。多少の手直しは必要ですが、AeyeScanはレポートの大枠を作ってくれるため非常に助けられています」（石谷氏）。HISでは、もしCriticalやHighに該当する脆弱性が発見された場合、修正が完了しない限りリリースしないルールとなっているが、「その場合は全体の結果を待たずに速報を開発側にお伝えし、早めに対応方法を検討してもらうようにしています」（岩崎氏）

この結果「深刻な脆弱性が発覚してしまったが、修正しているとリリース期日に間に合わない」という悩みで板挟みになることもなく、深刻な脆弱性を潰した状態でWebアプリケーションをリリースできるようになっている。また、以前から進めてきた取り組みの成果もあり、「開発を依頼する事業部側も、事件・事故を起こしてしまったらそれまでの苦労が水の泡になってしまうことを理解し、きちんと診断の期間や予算を取るようになりました。開発側もしっかりと事前対策を施し、ほとんど脆弱性を検知しない状態で診断フェーズに持ってくるようになっています」（石谷氏）という。

時間短縮を可能にした3ステップ

1. 開発部門からセキュリティ部門に大まかな機能テスト完了予定日を伝え、診断予定日の調整を行う
2. AeyeScanからアクセスできるよう、予定日までに通信元IPアドレスを許可し、アクティベーションファイルを診断対象サイトに設置する
3. 診断開始日にAeyeScanを実行して、AeyeScanから生成した診断結果レポートを開発部門に提供する

04 今後の展開

AeyeScanの導入にあたり、もう1つ期待していた効果が「それまで外部の診断サービスに支払っていたコストの削減」だった。AeyeScanの導入によってそれを削減できると考えていたが、当初の想定以上に多くの診断依頼が寄せられ続けたため、全体として内製比率はそれほど変わっていない。

このような診断ニーズの高まりを踏まえ、HISでは「今後はAeyeScanをさらに活用し、脆弱性診断ができるエンジニアを増員したいと考えています」（石谷氏）という。

しかもそれは困難なことではないと考えている。「AeyeScanは、設定のところさえ理解できれば、それまで診断業務を経験したことのない新たなメンバーでも7割以上は診断項目をカバーできます。診断業務を新たなスタッフに伝えていくスピードが上がることも、導入して良かったポイントだと考えています」（石谷氏）

今後も開発および脆弱性診断の内製化の比率を高め、DevSecOpsに向けた取り組みにもつなげられたらと期待しているが、まずはAeyeScanを用いて自動化できる範囲をできるだけ増やしていく計画だ。そして、脆弱性診断に携わる人員を増やし、チームとして更なるセキュリティの向上に取り組んでいきたいという。

Company profile

株式会社エイチ・アイ・エス

事業内容　総合旅行会社

従業員数　10,849名（2023年6月時点）

“「心躍る」を解き放つ”をHIS Group Purpose（存在意義）とし、旅行事業および旅行関連事業の深化を図るとともに、非旅行事業の探索により事業の多角化を図っている。

2023年3月時点

CASE 08 富士ソフト株式会社様

簡易かつ低コストなAeyeScanを活用し、社内におけるセキュア開発のルール化を推進

課題

セキュア開発のルールと運用を円滑にするためには、簡易かつ低コストで診断できる何らかの方法が必要だった。

導入

幅広い言語や開発環境に対応している「AeyeScan」を導入し、開発プロジェクトの好きなタイミングで検査できるようにした。

効果

セキュア開発ルール整備との両輪でAeyeScanを活用することで、ほぼ手放しでの運用が可能になった。

01 背景

約1万人の技術者を抱える富士ソフトは、独立系としては国内最大規模を誇るシステムインテグレータだ。流通や金融、サービス、製造、教育や公共機関に至るまで、幅広い分野の顧客向けにシステムの受託開発を手がけるほか、独自パッケージの提供にも力を入れており、最近では「AI／IoT／セキュリティ／クラウド／ロボット／モバイル・オートモーティブ」の頭文字を取ったAIS-CRM（アイスクリーム）に注力している。

同社は創業以来、「ひのき」（品質・納期・機密保持）という理念を掲げ、セキュリティも含めた品質管理体制に注力しながらソフトウェア開発を進めてきた。

しかも、年々サイバー攻撃が増加し、巧妙化する中、システムやソフトウェアに脆弱性が含まれていた場合のインパクトは甚大なものになっている。そこで「社長自らが『この先、セキュリティの重要性は高まり、やって当たり前という世界になっていくだろう』というビジョンを持ち、全社的な取り組みを徹底するようトップダウンで号令がありました」（富士ソフト株式会社　技術管理統括部セキュリティマネジメント部長／エグゼクティブフェロー 渡辺 露文氏）

このビジョンを実践する部隊がセキュリティマネジメント部だ。同社が提供するソフトウェアのセキュリティを高めるための「セキュア開発・運用」と、「社内セキュリティ対策」の両面から事業部門の支援を行っている。

特にセキュア開発・運用に関しては「ルール策定に加え、各事業部門に一人は情報処理安全確保支援士を育てることを目標に人材育成に取り組んでいます」（渡辺氏）

より事業部門に近いところで支援を行う「セキュリティ対策支援室」と両輪で、専門的な知識・知見が求められるセキュリティ対策の支援を行っている。

02 課題

トップの強い意識もありセキュア開発・運用の取り組みを加速させた富士ソフトだが、「どうしても開発者の興味は、新機能やよりよいユーザーエクスペリエンス（UX）といった領域に向きがちで、セキュリティも含めた非機能要件の優先順位は後回しになりがちでした」（渡辺氏）という側面は否めなかった。そこでセキュリティマネジメント部では、いわゆる単体テストや結合テストに加え、セキュリティテストを開発プロセスの中流に組み入れるための環境やツールの整備を開始した。

第一歩として、同社がニアショア開発やテストを主な業務として沖縄県に設置した「沖縄開発センター」の機能を約4年前に強化し、脆弱性検査を行える体制を整えた。Webアプリケーションの脆弱性検査ツールを導入し、センターに検査体制を集約することで、外注する場合に比べ低コストで脆弱性検査を行えるようになり、一部の事業部で採用が始まった。

だがそれでも、すべてのプロジェクトをカバーするには至らなかった。これまでセキュリティ検査をやっていなかった部署からすると、いくら外注より安価になるといってもコストがゼロではない以上、躊躇するのも無理はない。「今まで何もしていなかった部分を底上げすることを目的に、脆弱性診断を実施する習慣を付ける仕組みができないかと考えました」（富士ソフト株式会社 技術管理統括部セキュリティマネジメント部セキュリティ技術推進室エキスパート、水戸部一貴氏）

中には逆に、セキュリティに興味を持った一部のメンバー

が自力で学び、OWASP ZAPなどのツールを用いて独自にセキュリティ検査に取り組む部署もあった。歓迎すべきことだが、プロジェクトに関わるすべてのエンジニアが同じようにツールを使いこなせるとは限らない。

「開発者にセキュリティ検査のやり方を教え、自ら検査を回してもらおうとすると、やはり教育コストがかかる上に、検査ツールのライセンスコストもかさんできます」（渡辺氏）。この結果、プロジェクトのコストが高まり、開発競争力が下がっては元も子もない。

そもそも富士ソフトでは、このようにプロジェクトごと、担当者ごとにばらつきのあったセキュア開発のベースラインを定めることが大切だと考え、セキュア開発に関するルールの策定を進めていた。OWASP Proactive Controlsをベースに、これまでの開発経験を踏まえて独自の項目を追加した「セキュア開発・運用チェックリスト」を作成し、各プロジェクトに遵守を求める形だ。

ただ、「ルール化すれば、プロジェクトに何らかのコストがかかってくるのは避けられません。ルール化する以上は、もっと簡易かつ低コストで診断できる何らかの方法を提供しなければいけないと考えました」（水戸部氏）

03 ソリューションの選定

こうした悩みを抱えていた2020年秋に日本セキュリティオペレーション事業者協議会（ISOG-J）のワーキンググループで耳にしたのが、「AeyeScan」だった。文字通りAIを使って簡易な操作で、必要十分な脆弱性検査が行える点に魅力を感じたという。「コンタクトをとって実際に画面操作も見せてもらい、『これならセキュリティ検査に関するスキルを持たない人でも、検査ができるだろう』と感じました」（渡辺氏）

実は富士ソフトでは静的ソースコード解析（SAST）という選択肢も検討し、一部導入もしていたが、開発プロセスになかなかなじまないと感じていたという。「ソースコード解析はどうしても問題を過剰に見つけてしまうところがあります。実際に現場に持って行ったところ、『このアラートを全部つぶしていくなんて無理』という反応でした」（渡辺氏）

また、幅広い言語や開発環境に対応していることも必須の条件だった。富士ソフトの開発プロジェクトでは、C/C++とC#、Javaがメインだが、他にもPHPやPythonといったさまざまな言語が活用されている。しかもIT環境の変化に伴い、言語自体がどんどんバージョンアップしていく中では、特定のIDEしか使えなかったり、最新のバージョンはサポートされないといった状態では採用が難しいが、幅広い環境で検査が行えることも好印象だった。

ちなみに多数の開発案件を抱える富士ソフトでは、同じメンバーが長年にわたって同一のプロジェクトに携わり、同じプログラムを作り続けるケースはあまりない。コーディング規約を充実させることである程度セキュア開発が実践できるのでは、というアイデアもあったが、多様な顧客を相手に次々と開発プロジェクトが進むことを考えると非現実的だった。「『コーディング規約は作らないのですか』と言われたこともありましたが、富士ソフトではゆうに10以上の言語を扱い、しかもお客様ごとに異なるコーディング規約を持っていることもあります。となると、社内でルールを作り更新し続けるのは合理的ではありません」（渡辺氏）

こうした条件に合致し、行き当たりばったりに対応するのではなく一定のセキュリティベースラインを設けたいという狙いに、AeyeScanはぴったりはまる選択肢だった。「開発者任せにしているとその開発者が知っている問題にしか対策できませんが、スキャンをかければ何かしら問題が指摘され、自分が知らない問題、できていない問題を認識してもらえるようになります。こうして、AeyeScanを活用して、何もしていない状態から脱却しようと考えました」（水戸部氏）

04 導入効果

富士ソフトでは2021年4月からAeyeScanの導入作業を具体化させ、6月には、セキュア運用のルールと表裏一体の形で運用を開始した。

「それまでも自分たちで検査してもいいし、沖縄開発センターに委託してもいいし、あるいは外注してもいい。手段は問わないので何らかの形で脆弱性診断をしてください、というルールを定めていましたが、コストやスケジュールの問題で難しい場合がありました。ここにAeyeScanが加わることで、『依頼があればアカウントを払い出すので、好きなタイミングで検査をしてください』という形が整いました」（水戸部氏）

運用開始後、セキュア開発ルールとAeyeScanの周知のため社内セミナーと動画で情報共有を図ったところ、半年で10件程度の申し込みがあった。月に1〜2件はAeyeScanを使ってのスキャン申し込みがある形だ。

「事前にテストシナリオを作成する手間もなく、URLを入力してボタンを押すだけでテストが実行できます。ヘルプもよくできていて使い方もわかりやすいので、アカウントを発行した後はほとんど問い合わせもありません。われわれとしてもほぼ手放しでの運用ができています」と水戸部氏は言う。

社員に対するアンケートからも「使い方が簡単だ」「外部に委託する場合と異なり、自分たちの好きなタイミングで検査ができる」と高く評価されているという。

そして、開発に携わるエンジニアのセキュア開発に関する知識と意識の高まりも感じている。「セキュリティマネジメント部への問い合わせ内容が高度化してきているように思います。何をどうすればいいかという丸投げ的な質問の代わりに、顧客の要件とセキュリティのバランスをどのようにとるべきかといった、具体的で高度な問い合わせが増えてきました」（渡辺氏）

ルール整備との両輪でAeyeScanを導入した結果、納品前の脆弱性検査を行っていないプロジェクトが見受けられる状態から脱却しつつある富士ソフト。ルール作りと支援体制、そしてツールが相まって、「まいた種が一度に芽を出し始めているように思います」と水戸部氏は述べている。

ただ富士ソフトは、ここで歩みを止めるつもりはない。経営トップからは、開発段階のさらに手前である見積もりの段階からセキュリティを考慮し、「どのようなセキュリティリスクがあるか」「それにどのように対処していくか」を顧客とともに議論しながら提案することで、セキュリティの体系化、メニュー化を図りたいという声もあるという。

「ここまではベースラインを上げるところに注力してやってきましたが、さらにもう一段高みを目指していきたいと考えています。ただ特定のソリューションを入れるのではなく、セキュア開発によって業界を、それもセキュリティ業界ではなくシステム開発業界をリードし、セキュア開発の世界に持っていきたいと考えています」（渡辺氏）

Company profile

富士ソフト株式会社

事業内容 システム開発

従業員数 8,991名（2023年6月時点）

富士ソフト株式会社は、ソフトウェアの作り手としてトップレベルの開発力を生かし、「お客様にとってのベストは何か」を徹底的に追求して、コンサルティング、開発、システム構築からサポートまで充実した体制でトータルソリューションをご提供します。

2023年2月時点

CASE 09 株式会社ヒューマンインタラクティブ テクノロジー様

「AIでここまでセキュリティ診断が簡単に」AeyeScanを生かしセキュリティをシステム開発における強みの一つに

課題

第三者による脆弱性診断の実施が求められていたが、外部サービスは診断までにさまざまな準備や調整が必要で、労力やコストがかかることが課題だった。

導入

将来的にセキュリティ診断を内製化していく上でも有効であると判断し、「AeyeScan」を活用した「Quick WATCH」の導入を決定した。

効果

テスト作成の自動化により、期間の限られたプロジェクトでも手間をかけずに診断を実施。わかりやすいレポートを参考に、診断と修正のサイクルをスピーディに実現。

01 背景と課題

HITはITプロフェッショナル集団として、システム開発やインフラ構築コンサルティングサービスを通して顧客の課題解決を支援してきた。近年は、Microsoft AzureやMicrosoft 365など、マイクロソフトのクラウド導入の支援も展開している。

かつてのシステム開発では、機能要件と納期、コストといった事柄が重視されてきた。しかし、サイバー攻撃が増加し、情報漏洩事件が多発する近年では、それらの要素と並んでセキュリティという非機能要件も求められるようになっている。このためHITでは社内のセキュリティレベルを高めるだけでなく、顧客向けに構築するシステムにおいても必要十分なセキュリティ対策を実施してきた。

具体的には、システムに脆弱性を作り込まないよう各エンジニアがセキュアコーディングについて学び、開発プロセスの速い段階からセキュリティを意識して安全なシステムを構築するよう努めている。さらに、オープンソースの脆弱性診断ツールを用いてスキャンを実施し、プラットフォーム側の既知の脆弱性はもちろん、Webアプリケーションにも SQLインジェクションやクロスサイトスクリプティングといったよく知られた脆弱性が存在しないことを確認した上で納品する、という流れを整備しつつある。

ただ、いくら「自社できちんとセキュリティをチェックしています」と言っても、それは主観的な主張に過ぎない、と言われれば反論できない。事実、ソリューションサービス事業部 サービスグループ グループリーダー 木暮氏が携わったあるプロジェクトでは、顧客から「HIT自身の診断に加え、第三者による診断を行った上でシステムをリリースしたい」という要望が寄せられたという。

「お客様が扱う情報の重要度が高いプロジェクトであることに加え、近年、不正アクセスが頻発しています。もし脆弱性を攻撃されて個人情報の漏洩につながれば、直接的な被害はもちろん、お客様の信用やブランドそのものも傷つくことになりかねません。こうした情勢を踏まえ、客観的な立場からの脆弱性診断を要望されるようになりました」（木暮氏）。HITから顧客の担当者への説明はもちろん、顧客側担当者から上層部へ説明責任を果たす上でも、第三者的な観点での評価が求められていた。

02 ソリューションの選定

HITがまず考えたのは、外部のセキュリティ診断サービスの活用だった。ただ、診断までにさまざまな準備や調整が必要で、労力やコストがかかることが課題となった。

しかもこうしたサービスは、必要な時にそのつど単発で診断を実施する「スポット契約」がほとんどだ。だが、目の前のプロジェクトだけでなく、他の案件でも診断を実施し、「HITのシステムはセキュリティがしっかりしている」と付加価値を高めていくことを考えると、セキュリティ診断サービスという形態はそぐわないと考えた。それもできれば一度きりでなく、クラウド基盤をベースに改修・修正を加えるたびに継続的に診断を行い、セキュリティを担保し続けることを考えると不十分だった。

そんな悩みを抱いていたときにラックから提案されたのが、エーアイセキュリティラボのAeyeScanを活用し、ラックの専門家の支援を受けながら自社で繰り返し脆弱性診断を行える、Quick WATCHというラックのセキュリティ診断サービスだった。

ポイントの1つは、Quick WATCHでAeyeScanを活用

すれば、従来型の手法に劣らない水準の診断を、より少ない期間と労力で実現できることだった。「細かな部分となると別ですが、人が行う診断結果とほぼ変わらないレベルの結果が出るという説明を受けて手放しで喜びました。『ツールだけでそこまでできるんだ』と、いい意味で驚きました」（木暮氏）

03 導入効果

HITではPoCを実施し、目の前にあるプロジェクトだけでなく、将来的にセキュリティ診断を内製化していく上でも有効であると判断し、Quick WATCHの導入を決定した。導入にあたってはラックの専門家とともに、どの水準を満たせば顧客の要望に応えられるかを検討し、ベースラインを形作っていった。

実際に診断を回し始めて出てきたのは、「おぉ、Quick WATCHでAeyeScanを利用するとここまで診断が簡単になるのか」というエンジニアからの驚きの声だった。

一般にWebアプリケーションの脆弱性診断を実施する際には、どの画面でログインし、どのように画面遷移が行われ、どんな順番でサイトを巡回していくかというシナリオを人間の手で作成し、ツールに教える必要がある。だが、AeyeScanではAIを用いてその部分を自動化している。人手による作業の手間がかからず、十二分に目的を達成できることがわかったからこその、喜びの声だった。「ちゃんと巡回してチェックしているのを見て、周囲のエンジニアにも『ねえねえ、ほら見てよ』とわくわくしながら声をかけました」（木暮氏）

もちろん、認証の部分などでつまずきがなかったわけではない。しかし、事前のPoCを通してAeyeScanの癖を知り、巡回に詰まってしまう部分を洗い出し、どのように対処すればいいかをラックの専門家にアドバイスしてもらいながら進めていたため、ほとんど問題とはならなかった。

プロジェクトチームは年度末までに脆弱性診断を実施し、適切に修正を加えてリリースしなければならないというプレッシャーにさらされていた。当初現場には、「診断をするのはいいが、何が出てくるかわからない。もし対策が間に合わなければどうするんだ」という緊張感が漂っていたという。

しかし、AeyeScanを活用し、ラックの専門家による支援を得ることで、スピーディに診断と修正のサイクルを回すことができた。検出された脆弱性に対しては顧客に対策の方向性を説明した上で一通り対策を実施し、再度AeyeScanによるスキャンを実施して問題が修正されていることを確認した上で、無事にリリースにこぎ着けることができた。スキャンレポートも生成されるため、効果も説明しやすかったという。

04 今後の展開

コストや時間を無限にかければ究極のセキュアなシステムが実現できるかもしれないが、それは非現実的な話だ。HITではこのプロジェクトを皮切りに、「どこまでがNGで、どこからはOKか」というセキュリティ基準を形作り、AeyeScanというツールの特性と開発するシステムの特性の双方を踏まえながら、ライフサイクルの中でどうセキュリティスキャンの網羅性を維持し、セキュリティ品質を保っていくかという課題に取り組んでいく。

「我々自身の手で何回も脆弱性診断を実行できることには、それだけで高い価値があると考えています。我々がこの先リリースしていくシステムやサービスのセキュリティを自分たちの手で担保していけるのは、非常に心強いことだと考えています」（木暮氏）

そして、システムインテグレーションサービスやマネージドサービスの付加価値を高める武器として、AeyeScanおよびQuick WATCHを活用し、お客様との信頼関係を作り上げていきたいという。「単に技術を提供したりシステムを提供するだけではなく、『HITなら安心』という安心材料を付加価値として感じてもらえる存在になることを目指しています」（木暮氏）

さらに「AeyeScanについてはセキュリティの文脈だけでなく、AIを用いた画面遷移や情報収集といった部分にも着目し、システム開発の効率化やテストの自動化といった方向にも展開できるのではないかと期待しています」（木暮氏）。AeyeScanが得意とするCI/CDツールとのインテグレーションといった部分も視野に入れながら、よりよいシステム開発の在り方を広げていく。

Company profile

Human Interactive Technology inc.

株式会社ヒューマンインタラクティブ テクノロジー

事業内容　インフラ / セキュリティ、システム開発、Microsoftクラウド購入、エンジニア業務委託

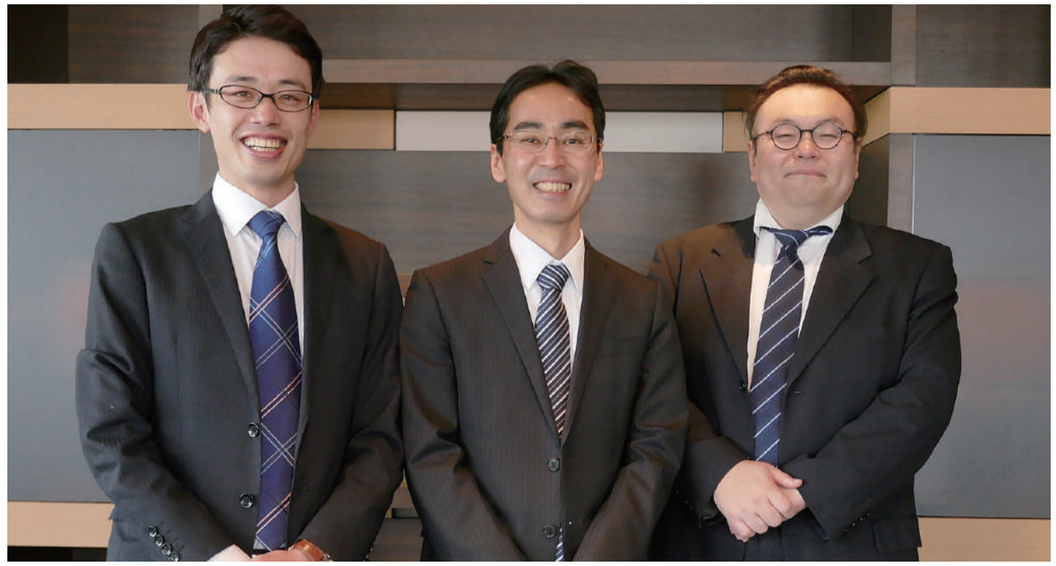
従業員数　40名（2020年3月末現在）

私たちヒューマンインタラクティブテクノロジー（HIT）のサービスは、社名のとおり、一人ひとりのエンジニアが、お客様とインタラクティブに対話を重ねながら、本当の課題や目的を共有することから始まります。その上で、培ってきた技術力やサービス力を最大限に発揮。具体的な目標到達への道のりを共に走り続けていきます。

2023年2月時点

CASE 10 株式会社ラック様

ツールとスペシャリストによる診断を目的に応じて使い分け、診断内製化の波を後押し



課題

スペシャリストが人の手で深く丁寧に見ていく診断サービスの性質上、「すべてのページを網羅的にチェックしてほしい」という要望に対応しきれなかった。

導入

「AeyeScan」はセキュリティ診断を内製化したい企業でも使えると評価、2021年11月にAeyeScanを活用した「Quick WATCH」サービスの提供を開始。

効果

これまでコストや時間、リソースの問題でやむを得ず対象外としてきたページの診断が可能になるだけでなく、半日かけていた見積もり時間が10分と大幅に短縮できた。

01 背景

ラックは、システムインテグレーションとサイバーセキュリティの両面で事業を展開し、国内におけるセキュリティサービスの草分け的存在となってきた。2000年から開始したセキュリティ監視センター「JSOC」によるセキュリティ運用監視サービスをはじめ、セキュリティインシデント発生時の緊急対応サービスやセキュリティ教育など、幅広いセキュリティソリューションを展開している。

ITシステムやWebアプリケーションに外部から悪用可能な脆弱性や設定不備がないかをチェックする「セキュリティ診断サービス」も、主要なセキュリティサービスの1つだ。ラックが長年開発・改良を続けてきた独自の検査ツールと専門家の手によって、SQLインジェクションやクロスサイトスクリプティングといった、悪用されると深刻な事態につながる脆弱性を見つけ出し、報告することで、個人情報の漏洩や金銭的な被害を未然に防ぐ手助けを行っている。

「ツールによる診断に加え、専門知識を持った診断員の手作業によって、かゆいところに手が届く診断を提供してきました」と、デジタルイノベーション事業部 セキュリティアセスメント部　副部長　柳澤伸幸氏は語る。ただ問題点を見つけるだけでなく、アプリケーションの性質や使われ方を踏まえてどこをどのように診断すべきかを検討する診断前のコンサルティングや発見された脆弱性への対応指針といった部分まで含め、全体的に支援できることも特徴だ。

ラックがセキュリティ診断サービスを展開し始めてから二十年以上が経った。その間、Webアプリケーションがカバーする領域は広がる一方で、個人が利用する多様なサービスはもちろん、企業システムや公的機関でも重要な役割を担っている。開発手法も変化し、仕様を決めてコーディングを行い、最後にテストや脆弱性診断を行うまでを数ヶ月単位で行うウォーターフォール方式から、1〜2週間といったサイクルでこまめに開発とテスト、リリースを繰り返すアジャイル開発が広がってきた。

これに伴い、「頻繁にバージョンアップするため、改修を加えるたびに外部に診断を依頼しているとうまく運用できないし、コストもかかるため、自分たちの手でセキュリティ診断を行えるようにしたい」という声も高まってきている。ラックではこうしたニーズに応え、セキュリティ診断の内製化を支援するコンサルティングサービスも提供し始め、開発と運用、セキュリティを一体化したサイクルを回すDevSecOpsの推進にも取り組み始めている。

02 課題

安全なWebアプリケーション開発に関するノウハウが徐々に蓄積され、ツールや開発フレームワークの改善も進み、深刻な脆弱性が検出される割合は減少しつつある。とはいえ、人間の作るものである以上、脆弱性はなくなることはなく、実際に攻撃ターゲットになってしまう事件も起こってきた。その上前述の通り、Webアプリケーションが果たす役割が高まり、重要なデータを扱う場面も増えたことから、セキュリティ診断サービスに対するニーズは高まる一方で、年度末などには依頼が集中し、応えきれなくなる事態も増えてきた。

ラックも例外ではなく、教育を通して要員を増やしているものの、「すぐに見てほしい」といったニーズの高まりになかなか応えきれない状況が続いてきた。デジタルイノベーション事業部 セキュリティアセスメント部長の西村篤志氏は、「スケジュールやコストの面で、お客様のご要望にすべて応えることができないケースがありました」と振り返る。

03 ソリューションの選定

そうした時に耳に入ったのが「AeyeScan」の存在だった。常々Webアプリケーションのセキュリティに関心を持ち、情報交換を行っているエンジニアのつながりを通して技術評価の依頼があり、早速検証してみることにした。

検証に当たったデジタルイノベーション事業部　セキュリティアセスメント部 第二グループ GLの久原和起氏は、「たとえば海外製の脆弱性スキャナだと、英語のマニュアルを読み解きながら苦労して使う必要がありましたが、AeyeScanには、日本人が作ったツールならではのきめ細かな配慮があり、使いやすいな、というのが最初の感想でした」と振り返った。

それでいて、OWASP Top 10に含まれる主な脆弱性を取りこぼすことなく検出できることも確認できた。「それほど手間をかけない割に、非常に高品質な結果が出てくるところも印象的でした」（久原氏）

さらに、「これまでWeb診断を行うには、パラメータをはじめ細かな設定が必要で、Webサイトの構造や脆弱性の仕組みに詳しい必要がありました。AeyeScanであれば、SaaSサービスでFQDNを登録するだけでサイトを巡回し、脆弱性を見つけてくれるため、調査コストが大幅に削減できると判断しました」（久原氏）

特に、これだけ手軽に使えるのであれば、ラック自身のセキュリティ診断サービスでの活用はもちろん、セキュリティ診断を内製化し、設計や開発の初期段階からセキュリティを組み込むシフトレフトに取り組みたいと考える企業でも使いこなせると判断した。

04 導入効果

こうした検証を経てラックはエーアイセキュリティラボと業務提携を結び、2021年11月に「Quick WATCH」サービスの提供を開始した。

Quick WATCHは、従来のセキュリティ診断サービスを置き換えるものではない。これまで、コストや時間、リソースの問題でやむを得ず検査対象外としてきたより多くのページについても、AIとRPAを組み合わせて診断を実施できることが特徴の1つだ。

また、ツールによる検査と、ラックのスペシャリストによる事前準備や検出された脆弱性への修正方針策定といった専門的なサービスを組み合わせることで、網羅性と手厚い支援の両方が得られることになる。また、セキュリティ人材が足りず、診断の内製化になかなか踏み込めなかった企業でも、ハードルを下げることができる。

「AeyeScanを活用して網羅的な検査を提供すると同時に、大事なところは深掘りして見てほしいというご要望に対しては、われわれのスペシャリストの手でしっかり見ていきます。診断の目的に合わせて使い分けていければと考えています」（西村氏）

すでにQuick WATCHに対して、「とにかくスピード優先で、急ぎで診断を行いたい」「脆弱性修正後の再検査もセットで実施してほしい」と考える企業からの問い合わせが入っている。

「これまでも、一度検査して見つかった脆弱性を直した後に再診断してほしいというニーズはありましたが、改修が予定通りに進むかどうかは事前にわからないため、スケジュール調整が難しい部分がありました。AeyeScanを活用すれば、そうしたニーズにも応えることができます」（柳澤氏）

診断の現場では、診断前の見積もりに要する工数を大幅に簡略化できるメリットも得られた。「診断をお引き受けする前には、お客様のサイトにどのくらいの画面が含まれるかを確認する見積もり工程が必要です。大事な作業ですが、これまでその工程に半日から一日くらいの時間を要していました。それがAeyeScanを活用すれば5分、10分といった時間で可能で、われわれの手間が減るだけでなく、お客様にもメリットになります」（柳澤氏）

05 今後の展開

ラックではAeyeScanを採用することで、より多くの顧客に対し、網羅的な検査が提供できると期待している。「これまで、お声がけいただいたり、せっかく頼ってもらったにもかかわらず、タイミングの問題でお応えできなかったお客様もありました。そこに対してもう一歩、二歩、幅広いレンジでご支援できるのは大きいことだととらえています」（西村氏）

また、機械的な作業をツールに委ねることで、スペシャリストの能力を、人間ならではの専門性が求められるより深い問題、本質的な問題の指摘といった分野で発揮できるようになるとも考えている。「診断自体はツールでかなりの程度カバーできるようになるでしょう。一方、お客様のポリシーや業態、守るべきものと照らし合わせながら、検出された脆弱性のリスク評価を行うといった作業は、人手でやらなければいけない部分です。そういった部分で、ラックとしての付加価値を出していければと考えています」（久原氏）

デジタルトランスフォーメーション時代を控え、Webアプリケーションが果たす役割はさらに高まっていくはずだ。ラックではAeyeScanを活用しながらDevSecOpsの実現を支援し、安全なアプリケーションをよりスピーディに開発していける世界を作り出そうとしている。

Company profile

株式会社ラック

事業内容　トータルITソリューションベンダー

従業員数　連結2,192名（2024年3月31日時点）

株式会社ラックは、先進のセキュリティ対策技術を核としたITトータルソリューションで、お客様のビジネス発展に貢献し、安心・安全な情報化社会の実現を目指します。

2023年2月時点

AeyeScanの多彩な機能

専門知識・トレーニングも不要

最短10分で利用できる

自動巡回

AI・RPAを活用することで、高いカバー率で自動巡回が可能。
（手動巡回機能もあります）

脆弱性診断

検出した脆弱性が攻撃に悪用される可能性を分析・評価。

画面遷移図生成

巡回時に自動で画面遷移図を生成。リンク切れも容易に把握。

定期スキャン実行

あらかじめ設定しておくことで、定期的にスキャンを実行。

ダッシュボード

ダッシュボードから進捗状況や結果に容易にアクセス可能。

各種ガイドライン対応

業界標準の各種ガイドラインに沿った診断項目を網羅。

CI ツール連携

CIツールと連携することでセキュリティテストを自動化。

Teams・Slack 連携

コミュニケーションツールにより情報の一元管理が可能。

グループ管理

ユーザーの属性に合わせた詳細なグループ設定・管理が可能。

権限管理

あらかじめユーザーに設定した役割ごとの権限設定が可能。

画面遷移図生成

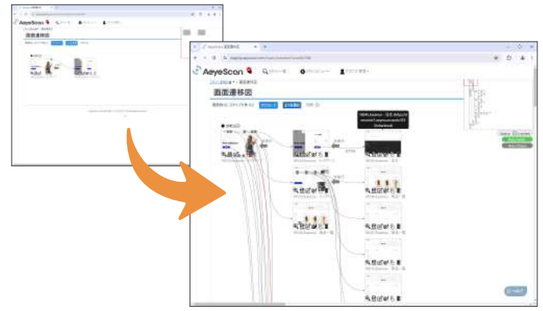
巡回時に、自動で画面遷移図を生成

診断範囲が可視化され分かりやすい

課題 遷移が正しくできていないと、どこからリンクされている画面か分からなかった

↓

存在しないページなどの 404 エラーもすぐに発見できる



PICK UP マネーフォワード様

「定期脆弱性診断を開始したことで、各画面で行われる HTTP のリクエストやレスポンスも含め、どのような画面遷移があるかがAeyeScan側に保存されるようになりました。各プロダクトを理解した上で、開発者からの問い合わせに対応できるようになりました」（中川氏）

各種ガイドライン対応

業界標準の幅広い脆弱性に対応

各種セキュリティガイドラインの自動化可能な項目に対応

OWASP TOP10

OWASP アプリケーション
セキュリティ検証標準

IPA 安全なウェブサイトの
作り方

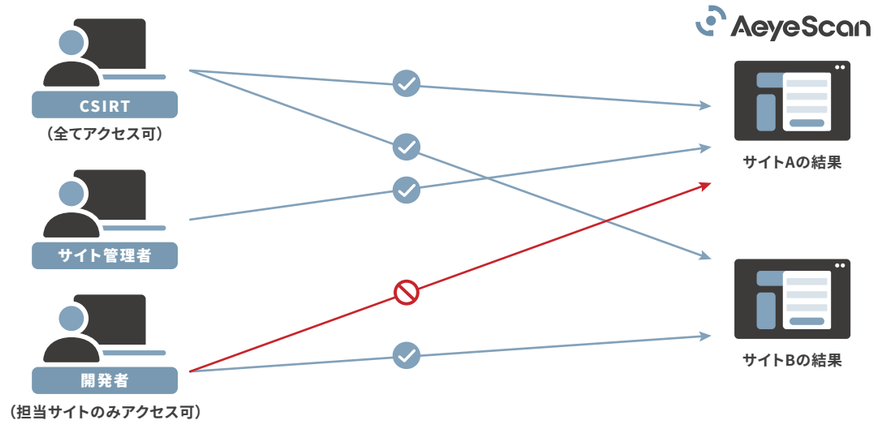
PICK UP アバントグループ様

さらにレポートの末尾には、OWASP Top 10など各種標準との対応表が付加されている。「これも今後、セキュリティ部門として、各種標準に基づいて評価していく上で有効に活用できるのではないかと考えました」（宮部氏）

グループ管理　権限管理

グループ設定と役割設定により、**一元管理された結果と詳細な権限設定**ができます。

グループ設定によるサイト毎のアクセス権限設定が可能



役割に応じた実行権限設定が可能

	CSIRT セキュリティ担当者	サイト 管理者・開発者	パートナー
管理権限	●	○	○
実行権限	○	●	○
閲覧権限	○	○	●

PICK UP　シンプレクス様

「API を提供してもらうことで、アカウントの払い出しや権限の付与を柔軟に行える仕組みをツール化し、自動化できたのは良かったポイントです」（岸野氏）

CIツール連携　Teams・Slack連携

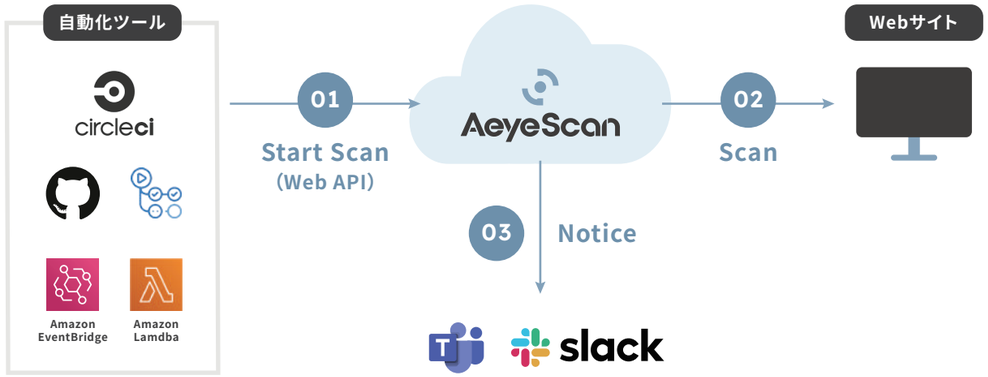
CIツールを使った自動化にも対応

CIツール・AWS Lambda・Googleスプレッドシートなどを活用し
セキュリティテストの自動化が可能です。

01 Start Scan：CIツールなどがAeyeScanのAPIからスキャン開始

02 Scan：AeyeScanがWebサイトの脆弱性をスキャン

03 Notice：スキャンの開始、終了をSlackやメールでお知らせ



PICK UP　JOBPAY 様

JOBPAYでは、AeyeScanのスケジュール機能を用い、診断を定期的に実施するよう自動設定した上に、APIを用い、レポートが出力されたらSlackに自動通知する仕組みを実装。エンジニアがほぼ手を動かさなくても診断サイクルを回せる仕組みまで整えた。「スタートさせておいて、あとは他の作業をしていればよく、終わったらSlackの通知を見てレポートを共有するだけなので非常に楽になりました。スケジュールを設定することで、今や診断のスタートボタンすら押す必要がなくなっています」（長峰氏）

AeyeScanの導入を
検討してみませんか？

操作性の確認、
実際に利用してみたい方へ 無料トライアル

トライアルにかかる費用は不要。実際の操作性はどうなの？
またどのように脆弱性が発見されるのか？
などの疑問は無料トライアルで解消しましょう。

申し込み

無料トライアルのお申し込み

お見積りの希望・
導入を検討している方へ お問い合わせ

お見積りの希望・導入をご検討してくださっている方は
お問い合わせフォームよりご連絡ください。
当日もしくは遅くとも翌営業日にはご連絡を差し上げます。

お問い合わせ

お問い合わせフォーム

無料セミナーも
随時開催中！

オンライン開催で、全国どこからでもご参加いただけます。デモ動画もございますので、ぜひ案内ページをご覧ください。

セミナー案内

メールマガジン登録

メールマガジンでは、セキュリティ対策や脆弱性診断に役立つ、様々な情報をお届けします。

- 脆弱性対策に関する最新情報
- AeyeScanの導入事例
- イベント／セミナーのご案内

メルマガ登録

会社概要

商号	株式会社 エーアイセキュリティラボ		
役員	代表取締役社長	青木 歩	
	取締役副社長	安西 真人	
	取締役	杉山 俊春	角田 茜
	執行役員 CTO	浅井 健	
	執行役員	関根 鉄平	田中 大介
事業内容	情報セキュリティ関連事業（調査・コンサルティング） セキュリティ診断クラウドサービス「AeyeScan」提供		
設立	2019年4月		
拠点	東京都千代田区神田錦町2-2-1 KANDA SQUARE 11F WeWork内		
資本金	1億円		
Webサイト	https://www.aeyesec.jp/		
取得認証	情報セキュリティマネジメントシステム（ISMS） ISMSクラウドセキュリティ認証（ISO27017） 情報セキュリティサービス基準適合サービスリスト		

AeyeSecurityLab

**セキュリティに
「あらたな答え」を提供し続ける
プロ集団**

IS 752963 / ISO 27001

CLOUD 790050 / ISO 27017

023-0026-20