セキュリティ競技コース事例

スカイマーク株式会社 様

セキュリティ技術への関心喚起に加え、チーム力強化にCTFを活用

定時就航率や顧客満足度指数で国内トップの評価を得ているスカイマーク株式会社（以下、スカイマーク）。日々、膨大な乗客と貨物を輸送する業務を支えているのは、システム開発部だ。システムインフラから予約システムまでを内製開発する技術者集団は、頻発するサイバー攻撃に対してどのような準備をしているのか、キーマンである清宮氏と白川氏に話を聞いた。

DX 本部 システム開発部
部長
清宮 英揮氏

DX 本部 システム開発部
システム業務推進課
IT 統制グループ グループ長
白川 晃司氏

システム内製化に取り組むスカイマーク

スカイマークは、国土交通省航空局が発表した「特定本邦航空運送事業者に係る情報」において、2018 年より 6 年連続で定時就航率の国内トップを記録している。また、公益財団法人日本生産性本部 サービス産業生産性協議会が調査した、2023 年度の日本版顧客満足度指数で 2 年連続の一位を獲得するなど、サービス品質において日本トップクラスの評価を得ている。

好調な輸送事業を支える情報システム部門は、航空券予約システムといった業務システムから、人事管理システムといった社内システムまでを内製開発している。スカイマークでは、IT を経営の重要なツールと位置づけている。先に上げた航空券予約システムに関しても、内製化は開発リードタイムの圧縮やコストの見える化を通じて、膨大なユーザーに満足してもらうための取り組みだ。何よりスカイマークが実現したいシステムを自ら追求できる点も大きい。

エンジニアのセキュリティ技術への関心を高めたい

スカイマークの IT を統括するシステム開発部は今、情報セキュリティ対策に注目している。航空事業者として最も重視するのが運航の安全性だ。人の命に係わる事業であることから、社員全員が運航の安全を期するための、あらゆる教育を受けている。しかし、情報セキュリティ対策については、リテラシー教育や具体的なセキュリティ対策の浸透など、やるべきことは残されている。

情報セキュリティ対策を進捗させるには、情報システムを統括するシステム開発部のメンバーの育成が重要だ。これまで、セキュリティインシデントに対する事故対応の机上訓練は行ってきたが、有事対応に特化した訓練であり、期間も短く技術的な要素は少ない。そこで、技術者が数週間程度セキュリティ関連技術に触れる機会を設けるため、セキュリティ競技コースの導入を検討した。

セキュリティ競技コースは、CTF（Capture The Flag の略）として知られるセキュリティの知識や技術を試す競技を、社員教育に活用したものだ。セキュリティに関する問題を解くことで得点を得て、同時に参加しているエンジニアとポイント勝負をする。

清宮氏は、CTF を部門内で開催する狙いを「セキュリティに関しての知識は座学でも得られます。しかし、知識としてわかっていても自分事にしなければ身に付かないので、参加型の教育プログラムが必要だと考えていました。」と語る。CTF により、ゲーム感覚で楽しみながら自発的に技術に触れ、セキュリティ技術への関心を高められる効果に期待し、本コースの導入に向けて準備を行った。

CTFをチーム戦としたことで得られたもの

スカイマークのシステム開発部で実施した CTF は、３週間にわたって開催された。競技に参加したメンバーが、ラックから提供される様々な課題を解きながら獲得スコアを競うものだ。この CTF でユニークな取り組みとなったのがチーム制を採用したことだ。

スカイマークのシステム開発部には、IT 統制、インフラ、アプリケーション、デザイナー、データ分析、運用といった職種のエンジニアが所属するが、同じ職種でまとまらないようチーム分けをした。

この発案について白川氏は「ネットワークや Web 開発など、自分がこれまで経験してきた分野には抵抗が無いと思いますが、苦手な分野の問題に挑戦することでモチベーションを下げることになるのは本意ではありません。個人によっては、解決できないことをつらいと感じる人もいます。そこで、苦手な分野は仲間に任せるなどチームワークで乗り越えることで、これまでに触れてこなかった分野にも安心して挑戦してもらいたいと思いました。」と振り返る。

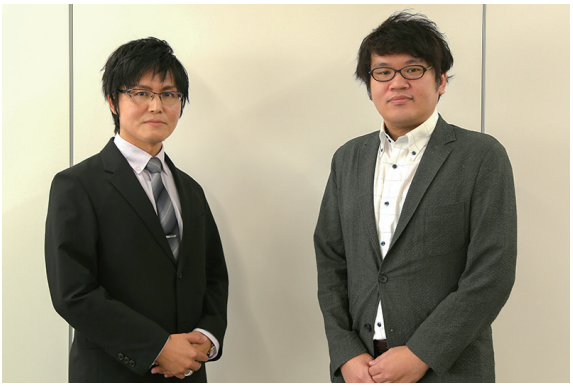
清宮氏は、実際に CTF を開始して驚いたことがあったという。「当初は、それぞれ得意な領域を解きあうと思っていましたが、アプリケーション開発者がフォレンジックの問題を解いていたり、Web デザイナーが Python のコードを書いて問題を解いていたりと、それぞれのエンジニアの違う側面が見えてきました。」と、エンジニアの才能の発見につながったようだ。

体験参加型トレーニングとしてのCTF

セキュリティ対策は非機能要件ということもあり、意識しなければ技術に触れる機会は少ない。しかし、ゲーム感覚で体験できる参加型のトレーニングは、攻撃者の視点で技術に触れることでセキュリティ対策の重要性が感覚的に理解できる点が優れているという。実際、CTF が始まると、多くのエンジニアが初日から時間をかけて取り組んでおり、モチベーションの高さを感じたようだ。

白川氏は「チームの成績が常に把握できるようになっているので、競争心をあおることでチームの団結が促進されました。結果、先輩後輩のコミュニケーションが活発になり、CTF を終えた後のチームビルディングに良い影響がありました。」と語る。

CTF 後に行われた課題の解説会においては、チャレンジする楽しさを語る声があった反面、課題が解けないことへのストレスもあったようだ。白川氏も「業務内容や経験が異なる参加者に対して、どの程度の難易度の問題が適切か判断することが最も難しかった。」と語るように、CTF の事前説明会で３問ほどデモンストレーションを行い、CTF の特徴や解き方のイメージを事前に掴んでもらうことで、取り組みとして成功させた。



セキュリティ技術の競技を、セキュリティ教育とチーム力強化に活用したスカイマーク。サイバーセキュリティのインシデント発生に向け、仕組み作りとエンジニアの育成に取り組みながら、IT のビジネス活用を強力に推進していく。

［お問い合わせ］
株式会社ラック
サービス紹介ページ https://www.lac.co.jp/education/course/security_competition.html

● ラックおよびLACは株式会社ラックの登録商標です。 ● 記載されている会社名、サービス名、製品名は、一般に各社の登録商標または商標です。

© 2024 LAC Co., Ltd.