Google Cloud

Submission API でフィッシング サイト検知から セーフ ブラウジング リスト登録までの作業を効率化

通信事業者としてのセキュリティ対策で培われた知見を活かして、さまざまなセキュリティ ソリューションを提供している KDDIデジタルセキュリティ株式会社（以下、KDDIデジタルセキュリティ）。フィッシング サイトの検知・対策サービスを提供する同社では、検知されたフィッシング サイトの早期閉鎖に向けて、Google のサービスである Google Safe Browsing（セーフ ブラウジング）のリストへの登録申告に Web Risk Submission API を導入しました。導入の背景や導入効果などについて話を伺いました。

利用しているサービス

Web Risk Submission API, Web Risk Lookup API

Digital Security
KDDI × LAC

KDDIデジタルセキュリティ株式会社

https://www.kddi-dsec.com/
〒102-0074
東京都千代田区九段南 3-3-6　麹町ビル 5F

KDDI株式会社と株式会社ラックの合弁により 2018 年 2 月 19 日に設立。通信事業者として常にサイバー攻撃に対応してきた実績のある KDDI と、サイバーセキュリティ分野の専門家として豊富な経験を持つラック。この 2 社の知見とノウハウを活かし、顧客の企業活動をサイバー セキュリティ面でサポートするさまざまな製品やソリューションを提供しています。

インタビュイー（写真右から）

- CROSS本部 副本部長 兼 企画統括部長　富山 修吾 氏
- セキュリティビジネス開発本部 セキュリティ開発部長　浦川 順平 氏
- セキュリティビジネス開発本部 副本部長 兼 サービス企画開発部長　小川 泰生 氏

フィッシング被害を防ぐためにはセーフ ブラウジング リストへの早期登録が鍵

近年、主に金融機関や EC 系の企業を装ったウェブサイトを用いて、アカウント情報やクレジット カード番号といった情報を詐取するフィッシング サイトの報告が後を絶ちません。これらのフィッシング サイトは、個人のユーザーに直接的な被害をもたらすだけでなく、名前を利用された企業の信用を傷つけ、安全なサービス提供の阻害要因にもなります。インターネットの利用をさらに普及させる上でも、フィッシング サイト対策はますます重要になってきました。

KDDIデジタルセキュリティはフィッシング サイトの検知・対策サービスを提供。顧客の企業名やサービス名などを不正に使用するフィッシング サイトが出現した際に、それを検知して注意喚起を促し、さらに検知したサイトの閉鎖に向けた手続きを顧客に代わって実施しています。

CROSS本部 副本部長 兼 企画統括部長の富山 修吾氏は、フィッシング サイトによる被害を未然に防ぐために有効な方法を、このように説明します。

「1 つ目はサイトのドメインを管理するレジストラやホスティング事業者などに働きかけて、サイトやドメイン自体を閉鎖してもらう方法です。しかし、この方法は閉鎖完了までに時間がかかるという問題があります。また、事業者によっては対応が遅く、閉鎖される前に被害が拡大してしまうリスクも抱えています。私たちが重視してきたのは、より迅速に効果が出る 2 つ目の方法、対象のフィッシング サイトをウェブブラウザ向けのブロックリストに登録するやり方です。リストに登録されれば、ユーザーがそのサイトに到達するのは困難になり、被害を未然に防ぐことができるからです。私たちはブロックリストの中でも、国内外で最もシェアが大きい Google セーフ ブラウジングのリストへの登録が特に効果的だと考えています。」

以前、KDDIデジタルセキュリティでは、Google セーフ ブラウジングのリストへの登録申告をすべて手作業で行っていました。フィッシング サイトが検知されると管理コンソールにアラートが表示されるので、オペレータはそれを見ながらウェブサイトの報告フォームに入力して報告していました。しかし、この方法では 1 件あたりの報告を終えるまでの作業時間が長くかかるため、短時間で大量のフィッシングサイトが出現した場合などは迅速な対応が難しく、さらにはオペレーション コストが瞬間的に非常に高くなるという課題がありました。

セキュリティビジネス開発本部 セキュリティ開発部長の浦川 順平氏は、以前の方式について次のように語ります。

「弊社のフィッシング サイト検知システムは長年のノウハウによって構築されたもので、性能については自信を持っています。しかし検知だけが早くても、セーフ ブラウジングリストへの登録が遅ければあまり効果は得られません。申告のオペレーションコストを減らして、いかに素早く申告できるようにするかは大きな課題でした。昨今のフィッシング サイト数の増加や、弊社のお客さまの拡大を見据え、フィッシングサイトが大量に発生した際の申告作業を簡略化する必要にも迫られていました。」

その解決策として同社が導入したのが Google Cloud の Web Risk Submission API です。この API を使えば、フィッシング サイトの URL を機械的に Google セーフブラウジングのリストに送信し、登録申告を行うことが可能になります。

「Submission API を利用すれば、短期間かつ集中的にフィッシング サイトが出現した場合でも、素早く確実に申告を行えるようになります。API 経由での申告は、手動での申告に比べてより安定した速度で Google セーフ ブラウジングのリストに登録されるということでしたので、申告から登録までの時間短縮の効果も期待して採用を決めました。」（浦川氏）

Submission API の導入により、申告にかかる時間を 1/10 以下に短縮

浦川氏は Submission API の導入にあたって、申告のための無駄なオペレーションの発生を極力排除しつつ、操作ミスが起こりにくいようにウェブ UI を設計したと説明します。

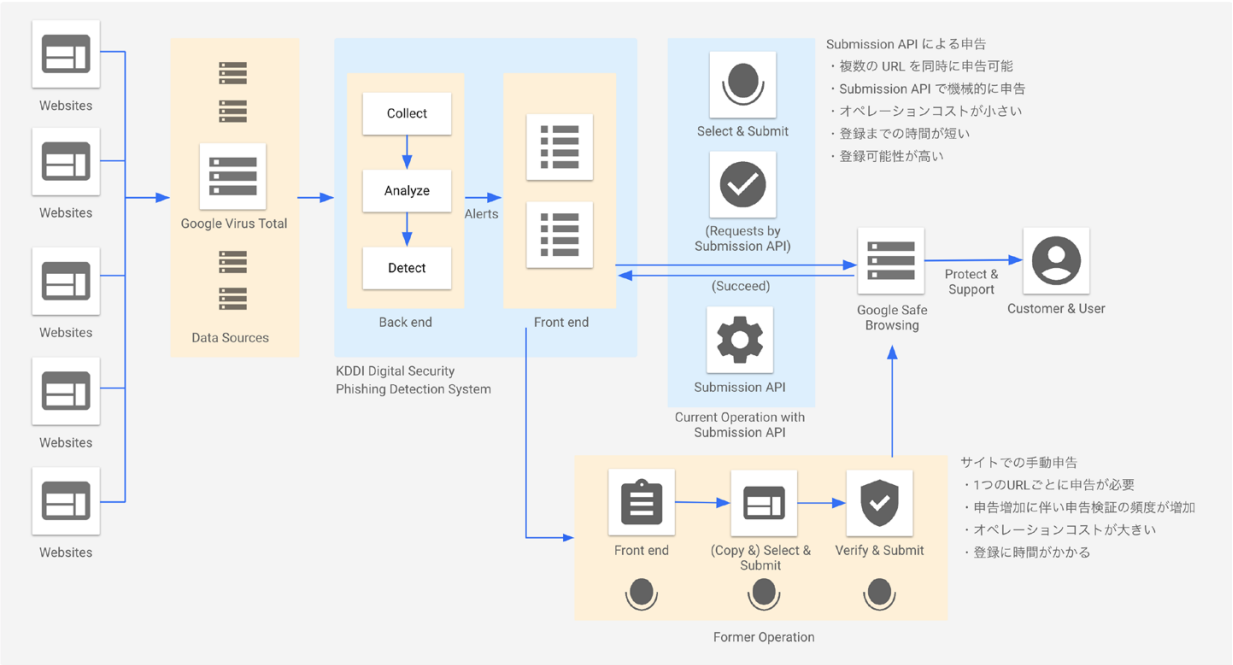
「オペレーション コストを下げることが API 導入の第一目的だったので、ウェブ UI はクリックなどの操作回数をできるだけ少なくする工夫をしています。例えばアラートが出た場合もクリックせずに画像まで確認できるようになっており、そこから選択・申告までをスムーズに行えるようにしました。Submission API で申告できるのは 1 リクエストあたり 1 件だけですが、UI 上は最大 300 サイトまで一括で申告できるようにして、大量アラートの発生にも対応しています。」

浦川氏によれば、この方法はオペレーション コストを削減する上で大きな効果をもたらしました。

「Submission API 導入で、従来は 1 件あたり 10〜30 秒かかっていた申告を、1 秒程度に抑えられるようになりました。弊社のお客さまを狙ったサイトの報告は 1 年間で 20 万件以上あったので、単純計算で年間約 555〜1,665 時間もかかっていた作業を 55 時間にまで短縮できることになります。」

新たな方法では、申告から実際の登録までの速度についても顕著な効果が現れました。Google セーフ ブラウジングのリストに登録されている URL は、Web Risk Lookup API を使用することでアプリケーションから確認できます。KDDIデジタルセキュリティのフィッシング サイト検知システムでは、この API を活用して申告したウェブサイトの登録状況を確認しています。その結果、従来の手作業による申告方法に比べて実際に登録される確率が高く、登録されるまでの時間も短いことがわかったため、「お客さまの安全を守るという本来の目的達成につながった実感がある」と浦川氏は言います。

システム構成



アラートに関する統計情報の可視化など、よりユーザーにわかりやすい形での情報提供を

Submission API の活用はセーフ ブラウジング リストへの迅速な登録を可能にしました。浦川氏は、より使いやすいサービスにするため、継続的な機能アップデートにさらに挑戦していくことを目指しています。

「現在は、個々のアラートを受けて申告を行った時刻は記録できていますが、ウェブサイト全体の何パーセントが実際に登録されたのか、登録までにどのぐらい時間がかかったのかといった統計情報は確認できるようになっていません。今後はそういったマクロな情報も可視化して、よりわかりやすい形でお客さまにデータを提供したいと考えています。」

その過程では、Google Cloud のサポートで得られた情報も積極的に活用されていくことになります。

「Google Cloud チームには、弊社が Submission API のベータ版で検証を進めていた頃から、仕様やメリットの説明や実装サンプルの提供など、さまざまな支援を受けてきました。最近も、追加情報を送信してセーフ ブラウジング リストへの登録申告をより速くする方法や、登録状況のさらに正確な確認の仕方などを説明いただいたので非常に助かっています。こういう知見も、将来的なアップデートに活かしていく予定です。」(浦川氏)

セキュリティビジネス開発本部 副本部長 兼 サービス企画開発部長の小川 泰生氏は、中小企業にも使いやすいセキュリティ ソリューションを積極的に開発し、セキュリティをなるべく意識せずに本来の事業に集中できる環境を提供していきたいと、今後の展望を語りました。

「サイバー攻撃は、以前はサプライ チェーンなどの大手企業が主な標的とされていましたが、近年ではバイヤーやコンシューマーなどの中小企業にも矛先が移ってきています。このため、従来はあまりセキュリティを意識されていなかった企業も対策に追われています。一般的にセキュリティ商材は、導入までに必要なステップが多くなりがちです。しかし中小企業のお客さまにもご使用いただくためには、説明がなくても簡単に導入できるようなサービスにしなければなりません。Google Cloud が提供しているゼロトラスト ソリューションの BeyondCorp も、これに近い発想に基づくものだと思いますが、手に届きやすいサービスや方法を、Google Cloud とも一緒に検討していければと考えています。」

Google Cloud を活用することで、ビジネスの将来に注力できるようになります。インフラストラクチャの管理やサーバーのプロビジョニング、ネットワークの構成などに起因する負担を軽減することができます。つまり、イノベーターもプログラマーも、自分の本来の仕事に集中することができます。

お問い合わせはこちらから
https://goo.gl/CCZL78

Google Cloud

Google Cloud の詳細については、右記 URL もしくは QR コードからアクセスしていただくか、同ページ「お問い合わせ」よりお問い合わせください。