導入事例

Secureworks

# インシデント管理リテーナーを活用し 国際標準に基づくアセスメントを実施 安心・安全を武器にB2Bビジネスを加速

**お客様名：** ポケトーク株式会社

**設 立：** 2022年2月

**所在地：** 東京都港区東新橋
1-5-2汐留シティセンター33階

**URL：** www.pocketalk.co.jp

**ソリューション**
インシデント管理リテーナー

**プロジェクトのゴール**

1. 顧客向けサービスを支えるインフラの安全性を担保すること
2. 情報セキュリティに関わる社内規程やルールを整備すること
3. インシデント発生時に速やかに対応できる体制を確立すること

**プロジェクト実施時期**
2023年6月

## 「言葉の壁をなくす」ための製品・サービスをグローバルに展開

グローバル化が一段と進む現代社会。ビジネスにおいてもプライベートにおいても、海外の人々と交流する機会が珍しくなくなっている。こうした中でネックとなるのが、コミュニケーションの問題だ。学生時代に苦労して英語を学習したにも関わらず、思うように話せない、聞き取れないと感じている人は多いことだろう。これは何も日本に限った話でなく、世界中の人々が同様の悩みを抱えている。

このような社会課題の解決に敢然と挑戦しているのが、「言葉の壁をなくす」を使命として掲げるポケトークだ。大手ソフトウェア企業であるソースネクスト株式会社から会社分割により設立された同社では、累計100万台を超えるAI通訳機「ポケトーク」やスマートフォン向け通訳アプリ「ポケトーク」などの製品を展開。仕事や旅行、語学学習など、様々なシーンで人々に貢献している。

さらに近年では、B2B向けのサービスも意欲的に推進。ポケトーク　デベロップメントディビジョン ディレクター 三木 静思 氏は「その一環として、先頃発表したソリューションが、『ポケトーク for BUSINESS』です。ここでは、英語をはじめとする10の言語を73言語の音声と字幕で通訳する『ポケトーク for BUSINESS 同時通訳』や、多言語での会議をAI技術で通訳する『ポケトーク for BUSINESS カンファレンス』、動画ファイルの翻訳を行う『ポケトーク for BUSINESS ムービー翻訳』などのサービスを展開。日本企業はもとより、グローバルに事業を行う世界中の企業をご支援していきたいと考えています」と語る。

## セキュリティの現状把握と体制整備が今後に向けた課題に

もっとも、B2Bビジネスをグローバルに拡げていく上では、解決すべき課題もあった。それはセキュリティ体制のさらなる強化だ。ポケトーク ITディビジョン ITチーム ディレクター

恒遠 玄崇 氏は「企業内で翻訳/通訳サービスを利用される場合、業務に関わる重要情報が取り扱われるケースも想定されます。このため、法人ユーザーのお客様からは、セキュリティチェックシートへの回答を求められるケースも少なくありません。特に海外企業のお客様は、セキュリティやデータ保護に対する感度が高いため、チェックシートの質問項目も非常に細かく具体性が要求されます」と明かす。

もちろん、同社でも、サービスの安全性確保には日頃から細心の注意を払っている。とはいえ、その取り組み内容を手作業でチェックシートに落とし込んでいくとなると、相当な時間と工数が掛かってしまう。またユーザー企業から求められる以上、迅速に対応する必要がある。

「その都度個別に対応していたのでは、こうした負荷が高まるばかりです。正確な回答を素早くお伝えする上でも、一度全社的なリスクアセスメントを行って、現状を把握する必要があると感じていました」と三木氏は語る。

加えて、もう一つの課題が、情報セキュリティ関わる社内規程やルールの整備だ。恒遠氏は「親会社から独立したことを機会にグローバルにサービス展開しているポケトークにより適した仕組みをここでしっかりと作り上げれば、お客様にとって安心・安全なサービスであることを自信をもって伝えられる材料ともなります」と語る。

## インシデント管理リテーナーで網羅的なセキュリティ対策を実施

このような課題を解決すべく導入されたのが、セキュアワークスの「インシデント管理リテーナー」(以下、IMR)である。ここでは、緊急時のインシデント対応に加えて、インシデント対応アドバイザリーサービス、ワークショップ/演習、診断/アセスメントなどのコンサルティングサービスも包括的に提供される。

三木氏はIMRを選んだ理由を「リスクアセスメントを実施したいというのが最初のきっかけではありますが、我々のようなスタートアップにとっては、インシデント対応も大きな課題です。人員がそれほど多いわけではありませんので、脅威に対応している間は肝心の開発業務が止まってしまう場合もあります。その点、セキュアワークスのIMRはカバレッジが非常に広く、平時の診断、体制構築支援から有事対応まで、まとめてサポートしてもらえます」と語る。

また、恒遠氏も「加えて、もう一つのポイントが、NIST(米国立標準技術研究所)の『サイバーセキュリティフレームワーク(CSF)』やCIS(インターネットセキュリティセンター)の『クリティカルセキュリティコントロール(CSC)』などのグローバル標準に基づくアセスメントが受けられる点です。いくら安全ですと訴えても、その評価軸が何なのか分からなければ、お客様としても判断が難しい。その点、NIST CSFやCIC CSCで評価したということであれば、グローバルに事業を展開するお取引先にも大丈夫だとご納得いただけます」と続ける。

## 脆弱性診断でリスクを可視化<br>迅速なインシデント対応も実現

今回の取り組みの手始めに、同社は、顧客向けの端末管理サービスや社内決済システムの脆弱性診断を実施した。「前者にはお客様の翻訳データが集まりますし、後者についても情報漏えいなどが発生すると大変なことになります。このように、重要性の高いシステム／サービスから優先して脆弱性診断を行いました。また、このほかに、当社ネットワークへの侵入検査なども行っています」と三木氏は説明する。

脆弱性診断の内容には、非常に満足したとのこと。「5営業日程度の期間でスピーディに診断してもらえた上に、日程調整に柔軟に対応してもらえました。レポートの診断結果が大変詳しく分かりやすかったですね」と三木氏。また、恒遠氏も「診断結果に対して、あえて細かい突っ込みを入れてみたのですが、すべてきちんと回答してくれたのは素晴らしかった。たとえば、ある項目のリスクが『Low』評価である理由を尋ねたところ、『場合によっては危険につながるおそれがあるが、貴社 の場合は別の部分で制御できているので大丈夫と判断した』とのこと。単純に〇×を付けるだけの診断では、こうした回答は決して返ってきません。きちんと環境を分析した上で、裏付けのある評価を行っているのだなと感心しました」と続ける。

この結果、現状のシステムや脆弱性管理プロセスに、大きな問題がないことを確認。三木氏は「これまでの取り組みが間違っていないことが分かったのは大変良かった。頂いた評価結果を元に、さらなる改善を進めていきます」と語る。セキュアワークスの脆弱性管理サービス「Taegis VDR™」の活用も検討していきたいとのことだ。

また、社内規程やルール整備の取り組みにおいても、IMRに大きな期待が掛けられている。恒遠氏は「現在当社では、ISO 27001/27017認証取得に向けた取り組みを進めている最中です。ここでも様々な検討が必要になりますので、セキュアワークスの知見をぜひ活用させてもらえれば」と語る。こうした取り組みが進んでいけば、前述のセキュリティチェックシートへの回答なども容易に行えるようになる。

もちろん、万一のインシデント対応でも、IMRが大きな威力を発揮。緊急インシデント対応サービスのサービスレベル・オブジェクティブ(SLO[1])では、4時間以内にスコーピングコール、24時間以内にリモートであれば調査が行われるため、迅速な対応が可能になる。

「グローバルビジネスにおいて、セキュリティは攻めの武器となります。それだけにIMRを導入した活動は、いわば世界で戦う挑戦権を手にするためだと考えています」と恒遠氏。三木氏も「言葉の壁が無くなった時に、世界がどう変わるのかが非常に楽しみです。我々としても、その実現に向けて今後も力を尽くしていきたい」と抱負を述べた。

ポケトーク株式会社
ITディビジョン
ITチーム
ディレクター
恒遠 玄崇 氏

ポケトーク株式会社
デベロップメントディビジョン
ディレクター
三木 静思 氏

- 取材 2023年9月
- 記載内容は、2023年9月21日時点のものです。
- 本文書に記載されている仕様は2023年9月時点のものであり、予告なく変更する場合があります。最新の仕様については、弊社ホームページにてご確認ください。

[1] 緊急インシデント対応のSLOは、日本国内拠点が対象です。

**セキュアワークス株式会社**
Secureworks(セキュアワークス、NASDAQ: SCWX)は、Secureworks® Taegis™を通じてお客様のビジネス進捗を保護するサイバーセキュリティのグローバルリーダーです。Taegisはクラウドネイティブなセキュリティ分析プラットフォームであり、20年以上にわたる実業務を通して蓄積された脅威インテリジェンスとリサーチに基づき構築されています。お客様は、高度な脅威を効果的に検知し、合理的な調査と関係チーム間のコラボレーションを行い、そして適切な対応アクションを自動化することが可能となります。

詳細は当社のセキュリティ専門家までご相談ください。

**03-4400-9373**
secureworks.jp