WASEDA University

Smart SE

IoT/AIコース　修了制作

Chatbotを用いたセキュリティリスクアドバイザリーシステム

学籍番号　sse07-20　　名前　萩野貴政　　メールアドレス　takamasa.hagino@vnss.jp

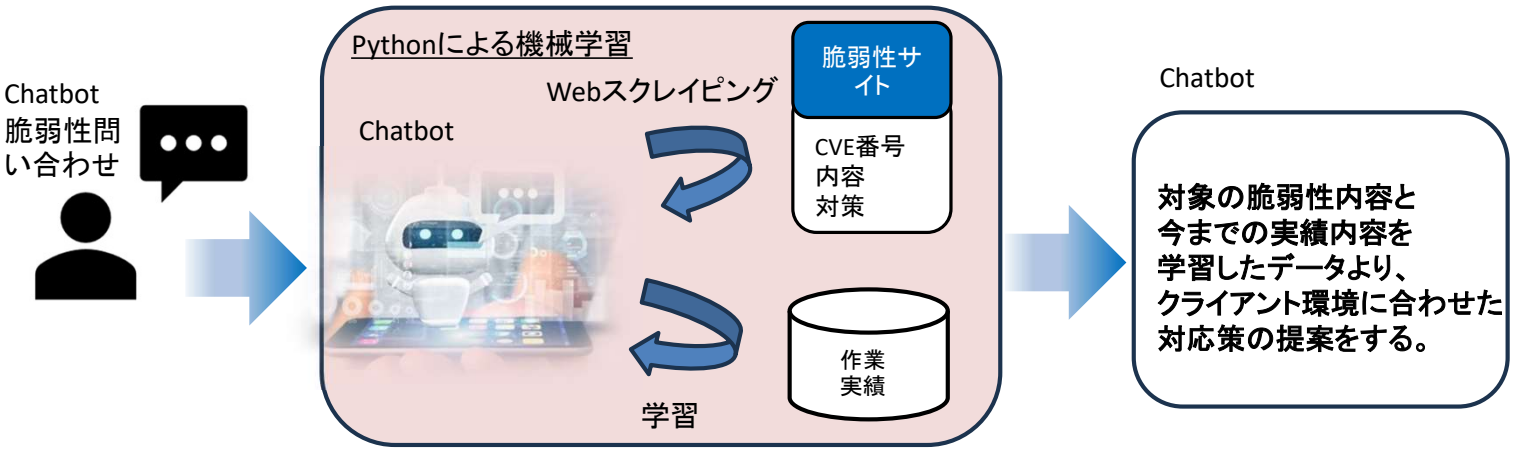
開発における問題点

現状、脆弱性の調査として、内容を把握し、対応策として何があるか、過去に対応した実績がないか、などを完全にマニュアルで調査をし、方針を立てている。
実際に対応したものを再度調査をし直しすこともあり、非常に非効率的である。

手法・ツールの適用による解決

GSNを活用したGQM＋Strategiesによる戦略
ストラテジー：サイバーセキュリティ対策の自動化戦略としてPythonによる機械学習
ソリューション：サイトにアクセスしWebスクレイピングをして実績のデータベースから対策の提案をChatbotで行う。

ポスターの構成



本終了制作の成果

問題の整理とGQM+Strategiesによる戦略
Goal: 情報の自動抽出と対応の可否と対応策の提案を自動で効率的に行う。
Solution：インターフェースとしてChatbotを利用しインタラクティブでリアルタイムでのやり取りを可能とする。Pythonによる情報抽出と機械学習による過去実績のデータの学習行う。
システム開発
Pythonを使用して脆弱性の取りまとめサイトにアクセス、Webスクレイピングを実施し、必要な情報を抽出する。

今後に向けて

本修了制作では実装できなかった下記を導入をする。
１．Chatbotをインターフェースとして導入す
【技術】自然言語処理（NLP）：対話型のインタフェース
２．過去の対応実績データを用いて機械学習のモデルをトレーニングをする。
【技術】ディープラーニング：脆弱性評価モデルの構築

※最終的には対象を拡大しITインフラ全体をカバーする汎用的な脆弱性管理システムを目指す。

.