

ティッカー表示による組織に即した脅威情報の閲覧

後藤 圭太† 毛利 公美† 白石 善明‡

†岐阜大学工学部電気電子・情報工学科 ‡神戸大学大学院工学研究科／ATR

1. はじめに

サイバーレジリエントな組織に貢献するサイバーセキュリティチームにおいては、最新の脅威情報のモニタリングが不可欠であり、速報性のある Web や SNS に投稿される短文のメッセージの活用が注目されつつある。

他方で、工場での現場活動の促進[1]や機械の安定稼働のための適切なメンテナンス[2]など諸分野で IoT によるデータの活用が模索されている。これらは、“データ提供者”、“データ蓄積者”、“データ利用者”の三者から構成される形を基本としている(図1)。このモデルと同様の脅威情報を閲覧するシステムを本稿では検討する。

2. 擬似プッシュ型脅威情報閲覧

セキュリティレポートや SNS、組織で所有している資産であるハードウェア・ソフトウェアの公式サイトの閲覧により脅威情報を入手できる。セキュリティレポートや SNS では通知機能により閲覧までの手順が一部簡略化できるが、データ利用者がデータ提供者にアクセスして入手する二者によるプル型モデルが基本である。

Web を含めた脅威情報を二者モデルで受動的に得ることは難しいため、図1に示すデータ蓄積者が介在した三者モデルにより以下の要件を満たす擬似的なプッシュ型で組織に即した脅威情報を閲覧できるシステムを本研究では構築する。

要件1: 条件に合う脅威情報の収集ができる

組織により保有する資産は異なる。資産と関連が弱い情報を省き、関連が強い情報を閲覧できることが求められる。

要件2: テキストを抽出・加工ができる

配信される情報を利用者が閲覧する際に、原文が長い場合には短縮するなどの加工ができるようにテキストデータを抽出できることが求められる。

要件3: テキストのティッカー表示ができる

利用者が何らかのアクションをとることなく情報を見れることが求められる。



図1 脅威情報閲覧システムのモデル

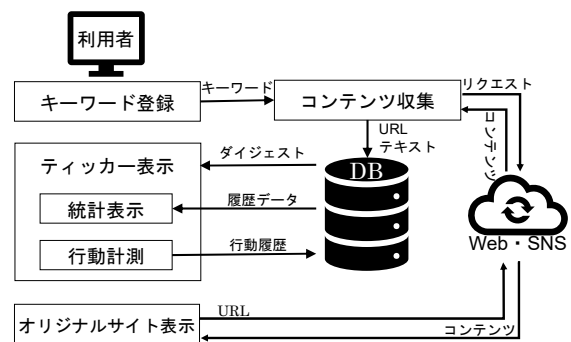


図2 擬似プッシュ型脅威情報閲覧システムの構成

要件4: オリジナルサイトの閲覧ができる

ティッカー表示を閲覧した上で詳細情報が必要とされる場合に速やかにオリジナルサイトを見られることが求められる。

要件5: 行動履歴の取得・保存ができる

既読情報をティッカー表示の候補から除外するなどの表示上の工夫をするために行動履歴の取得が求められる。行動履歴を保存することで自身への提示内容の最適化や他者への推薦が可能となる。

3. 擬似プッシュ型脅威情報閲覧システム

提案システムの構成を図2に示す。システムの主な機能は“キーワード登録機能”、“コンテンツ収集機能”、“テキスト抽出・加工機能”、“ティッカー表示機能”、“オリジナルサイト表示機能”、“行動計測機能”、“統計表示機能”である。システムの動作は次のようになる。

キーワード登録: 利用者は収集したい情報に関するキーワードを登録する。【キーワード登録機能による: 要件1に対応】

コンテンツ収集: システムは登録されているキーワードをもとにインターネットで検索して脅威情報を収集する。【コンテンツ収集機能による: 要件1に対応】

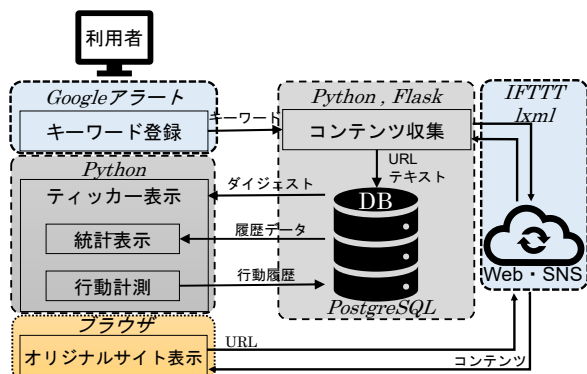


図3 実装環境

テキスト抽出・加工：長さが異なるコンテンツを適当な分量に揃えるなど、ティッカー表示のためにテキストデータを抽出しDBに保存する．利用者に配信するときに表示環境に応じてテキストを加工する．【テキスト抽出・加工機能による：要件2に対応】

ティッカー表示：システムは利用者のビューにダイジェストを配信してティッカー表示により組織に関連する脅威情報を配信する．閲覧時の状況を計測し，システムはDBに行動データを保存する．システムは利用者に配信する際に履歴データによりティッカー表示を適応的に変更する．【ティッカー表示機能，行動計測機能および統計表示機能による：要件3および要件5に対応】

オリジナルサイト表示：ティッカーの表示内容から利用者が詳細情報を取得したい場合はリンクをクリックしてオリジナルサイトにアクセスしブラウザ等で閲覧する．【オリジナルサイト表示機能による：要件4に対応】

4. 実装

サーバサイドはPythonのFlaskフレームワークで記述する．図3は，利用者の指定するキーワードをGoogleアラートへ登録し，IFTTTで受信したRSSフィードによりlxmlで当該サイトにアクセスしてそのURLとテキストデータを抽出してPostgreSQLデータベースに格納する実装例である．配信されてきたダイジェスト情報と行動履歴の統計データを表示するPythonクライアントの実行画面が図4である．下部のURLをクリックするとブラウザによりオリジナルサイトにアクセスする．

5. まとめ

組織に即した脅威情報を特段のアクションを要さずに閲覧できれば，脅威トレンドに敏感であることが期待されるサイバーセキュリティチームに有用であると期待される．本研究では速

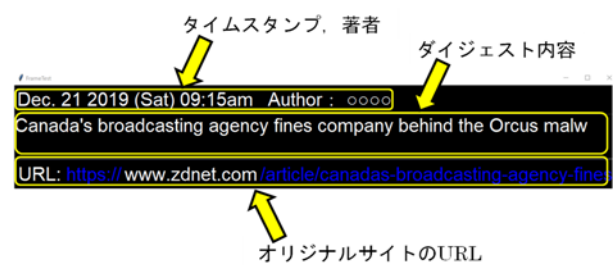


図4 利用者端末でのティッカー表示

表1 RSSリーダーとの比較

	本提案	RSSリーダー
要件1	○	○
要件2	○	—
要件3	○	—
要件4	○	○
要件5	○	—

報性のある脅威情報の収集にRSSを利用することでWeb・SNSから最新コンテンツを収集し，ティッカー表示することで利用者が能動的に情報にアクセスせずに閲覧することを可能にした．

表1にRSSリーダーとの違いをまとめる．提案システムは，ダイジェスト表示などの工夫ができるようにテキストを加工できる点（要件2），行動履歴を取得し利用することで利用者ごとに表示内容をカスタマイズできる点（要件5），そして，疑似プッシュ型で構築することで利用者が何らアクションを起こさずにティッカー表示できる点（要件3）がRSSリーダーと異なる．

多様な情報源から集約した脅威情報を検索可能にするEXIST[3]やオープンソースインテリジェンス(OSINT)ツールとの連携を検討することが今後の課題である．

謝辞 本研究の一部は国立研究開発法人情報通信研究機構の委託研究「機械学習に基づくサイバー攻撃情報分析基盤技術の研究開発」およびJSPS科研費19K11963, 18K04133の支援のもとに行われた．

参考文献

- [1] 知崎一紘，地主岳史：IoT活用による工場の生産活動最適化，デジタルプラクティス，vol.8, no.3, pp.203-209 (2017)．
- [2] 濱町好也，柳本裕章，久保田一輝：建設機械の遠隔監視とトータルソリューション提案の実現（ConSite）—情報収集・インテリジェンスフィルタ機能・情報配信の全自動化—，デジタルプラクティス，vol.8, no.3, pp.224-229 (2017)．
- [3] サイバー脅威情報集約システム EXIST, <https://blog.nictcr.jp/2019/03/exist/>．