情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

修士論文審査

SOC業務支援のためのオープンソースインテリジェンスシステムの提案と評価

2023年2月18日

情報セキュリティ大学院大学
後藤研究室　博士前期課程2年
大村篤生

研究概要

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

SOC業務の課題

・スキルを持った人材の確保が困難
・現場運用のウェイトが重く、脅威動向を追えていない

SOC業務支援のためのOSINTシステム提案

・セキュリティに関する最新の脅威動向を自動的に収集する
・緊急性の高い脅威や脆弱性についてはその他の情報と区別して収集する
・要約された収集情報をチェックすることでSOCの通常業務への負担を少なくして**攻撃**の高度化を追う

OSINTシステムの実装・評価

既存のOSINTシステムに新規要件を付加

要件①収集情報の保存
要件②情報収集の脅威排除
要件③収集情報の翻訳
要件④収集情報の要約

SOC業務従事者にアンケートを実施

・既存OSINT機能より、新規OSINT機能の方が評価が高い
・要件①、要件③の評価が高い

結論

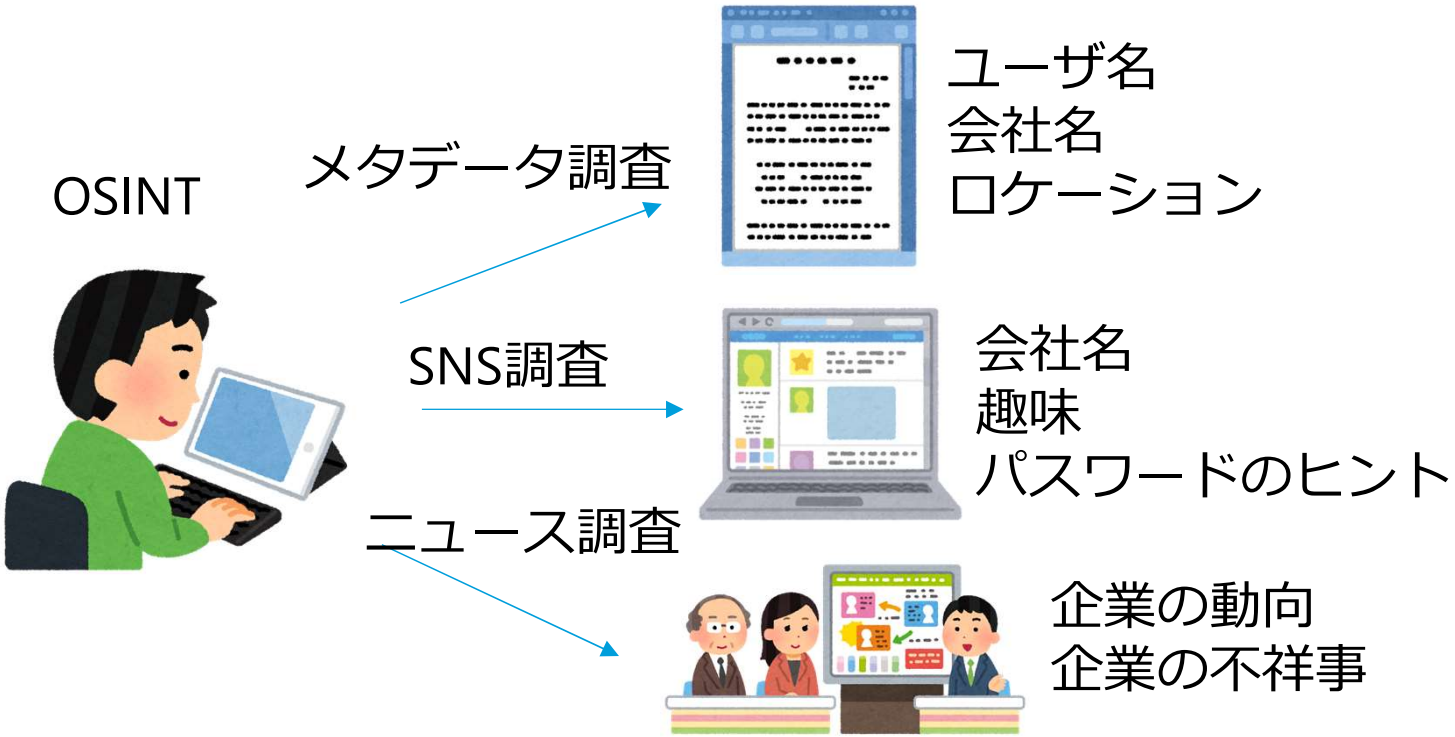
提案するOSINTシステムの実装と評価により、SOC業務における脅威動向収集に実用的な価値を示した

OSINTとは

◆OSINT(open source intelligence)

・「合法的に入手できる資料」を「調べて突き合わせる」手法。「合法的に入手できる資料」とは、報道・ネット記事・新聞記事・書籍・科学誌・企業が公表しているニュースなど

・ネット上で収集できる情報は膨大な量となっており、情報の収集においては自動化が必要不可欠となっている。



出典：SQL Master データベースエンジニアとセキュリティエンジニアとLinuxエンジニアのための情報 –諜報活動はOSINT、SIGINT、HUMINTの3種類が基本(閲覧日：2021年5月19日)
http://www.sql-master.net/articles/SQL1639.html

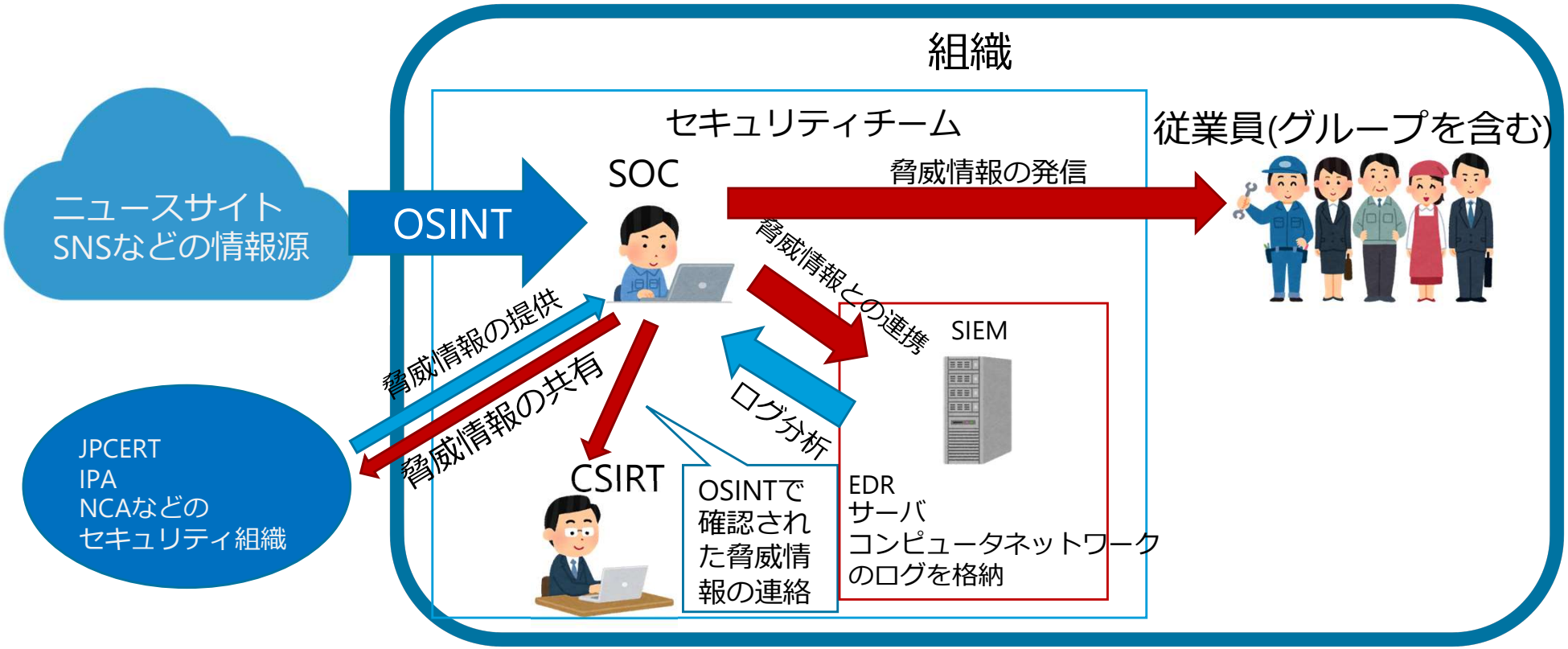
SOC業務へのOSINTの活用

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■OSINTの活用による効果

・ニュースサイトやSNSからサイバーセキュリティに関連する情報を収集し、セキュリティチーム内および社内従業員へ通知する。(脅威の最新動向の共有・活用)
・OSINTで収集される情報をSIEMへ連携させることでシステムで発生していることの緊急性を判断する。(SOCのログ分析の支援)

・セキュリティチームによる従業員への「情報セキュリティ啓発」を最新動向の情報で実施できる
・発見される脆弱性を素早くセキュリティチーム内で共有できる



提案手法について

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■本研究の焦点、OSINTに求めること

本研究では、「自組織へのセキュリティ脅威に対する予防と、セキュリティチームの知見・関心の向上を目的とする脅威・脆弱性情報の早期認識のため、公開情報(主にインターネットのニュースサイトやSNS)から情報収集を行いその情報を有効に活用すること」をOSINTの定義とし、考察を行っていく。

また、本研究においてOSINTの要件として以下を提示し、SOCの情報収集やインシデント判断を支援することを目的として機能を実装し、評価を行う。

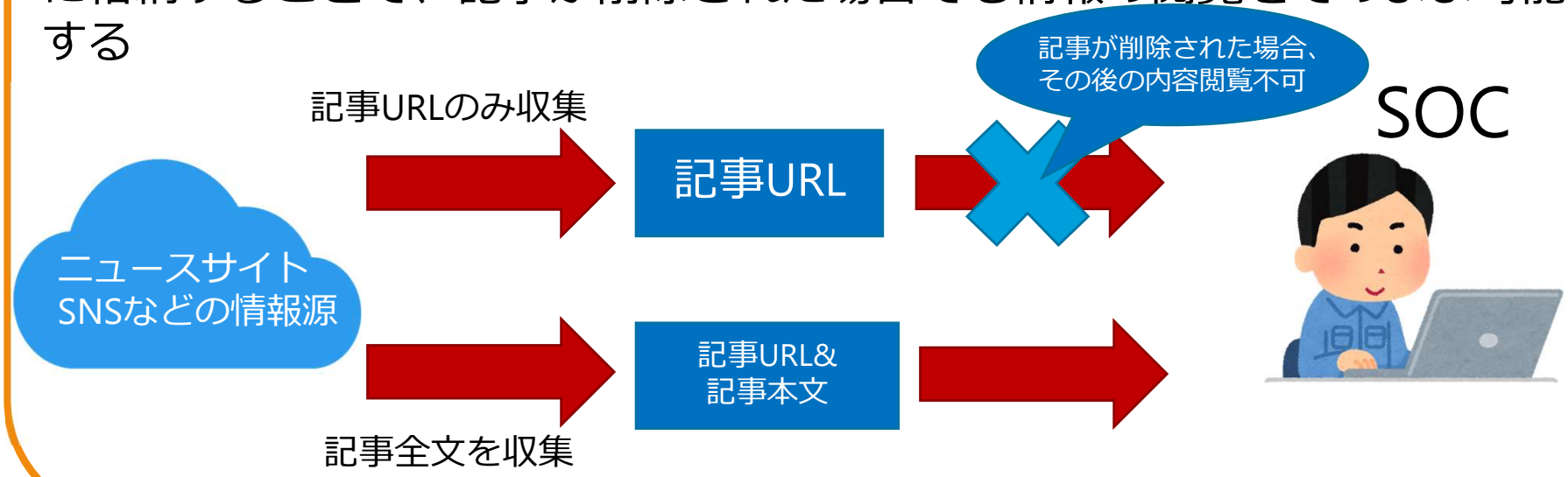
1．情報収集後は、元記事が削除された場合でも情報の閲覧が可能である
2．情報収集の自動化にセキュリティ脅威がない
3．収集された情報を分かりやすくするため、収集情報の日本語翻訳が自動的に行われる
4．収集された情報を分かりやすくするため、収集情報の要約が自動的に行われる

要件毎の効果と仕組み

1.情報収集後は、元記事が削除された場合でも情報の閲覧が可能である

●効果
・過去の脅威・脆弱性を振り返れる状態にすることで現在の脅威・脆弱性への進化の過程や傾向をつかむことができ、以降の脅威への対応やセキュリティ関連の知見向上に繋がる

●考案する仕組み
・情報収集の際に記事URLだけでなく、本文内容も併せて収集しデータベースに格納することで、記事が削除された場合でも情報の閲覧をそのまま可能にする



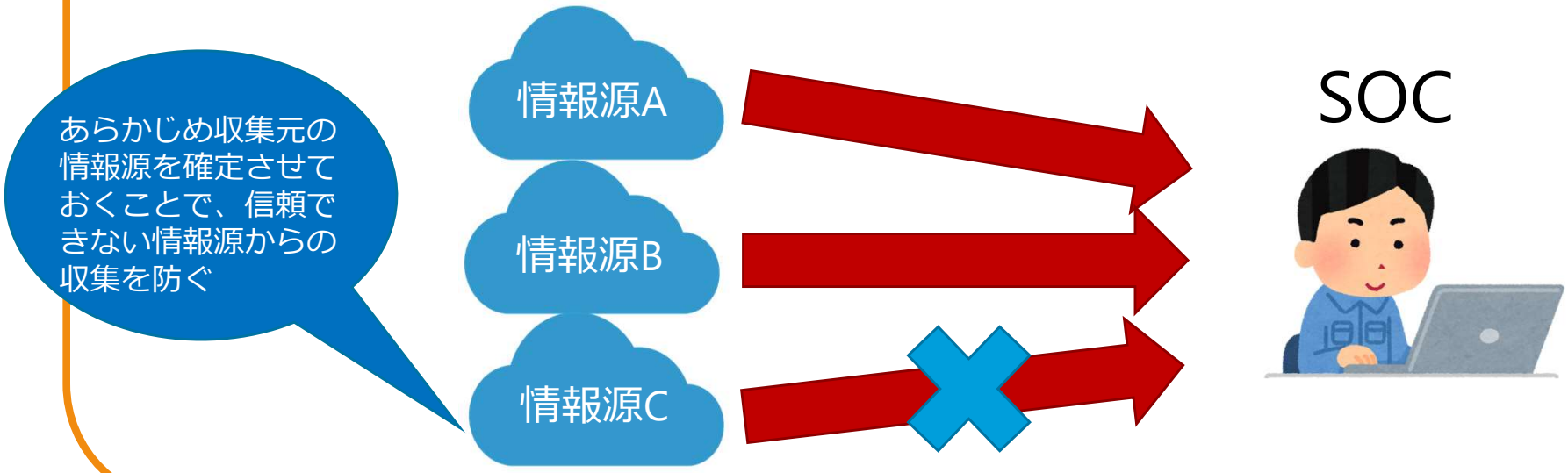
要件毎の効果と仕組み

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

2.情報収集の自動化にセキュリティ脅威がない

●効果
・収集元の設定を行わずに情報収集を行うと、意図せずマルウェアや個人情報などを収集してしまう可能性がある
⇒自動収集に脅威を無くすことで安全に情報収集をすることができる

●考案する仕組み
・事前に信頼できる収集元の固定化を行うことで意図しないものの収集を防止する



要件毎の効果と仕組み

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

3.収集された情報を分かりやすくするため、収集情報の日本語翻訳が自動的に行われる

●効果
・情報源が日本語以外表記の情報だと、内容の把握に時間がかかる・正確に内容の把握ができない等の可能性がある
⇒収集情報の内容の把握が円滑かつ正確になる

●考案する仕組み
・Google Translate APIもしくはDeepL APIの技術を活用して収集する情報の日本語翻訳を行う

要件毎の効果と仕組み

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

4.収集された情報を分かりやすくするため、収集情報の要約が自動的に行われる

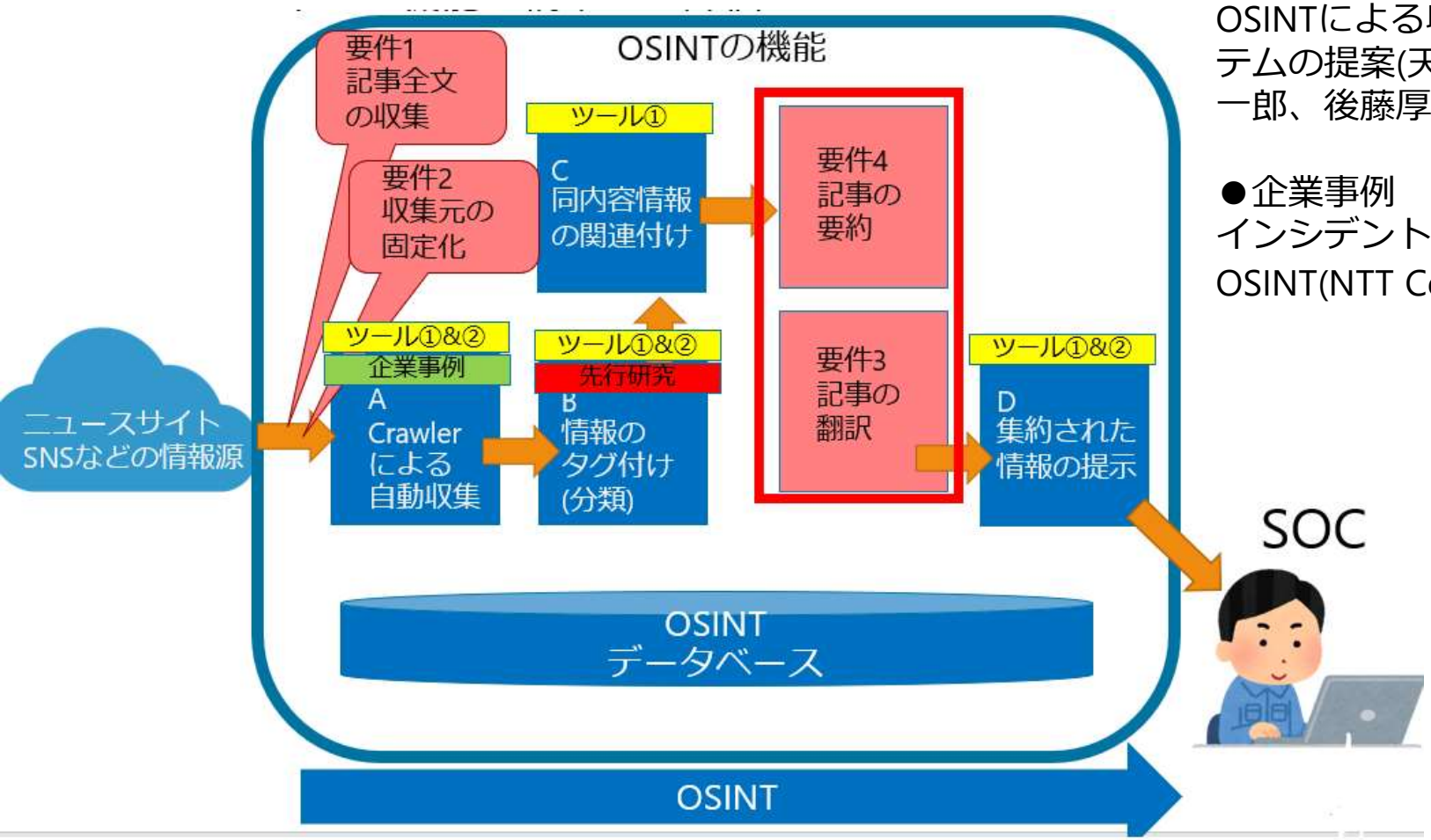
●効果
・情報源が要約されていない状態だと、内容の把握に時間がかかる・正確に内容の把握ができない等の可能性がある
⇒収集情報の内容の把握が円滑かつ正確になる

●考案する仕組み
・長文要約生成API(朝日新聞社)の技術を活用して収集する情報の要約化を行う
●機能
・指定した長さごとに生成型要約
・文の長さを揃える
・文の圧縮
・重要な文の抽出

OSINTの従来機能と新規機能

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

図に既存のOSINTツールや先行研究等で確認されているOSINTの従来機能(青)と本研究で新規に追加する機能(赤)を示す
→本研究では下図の機能の構築し、評価を行う



●ツール
ツール①：MISP&EXIST
ツール②：Inoreader

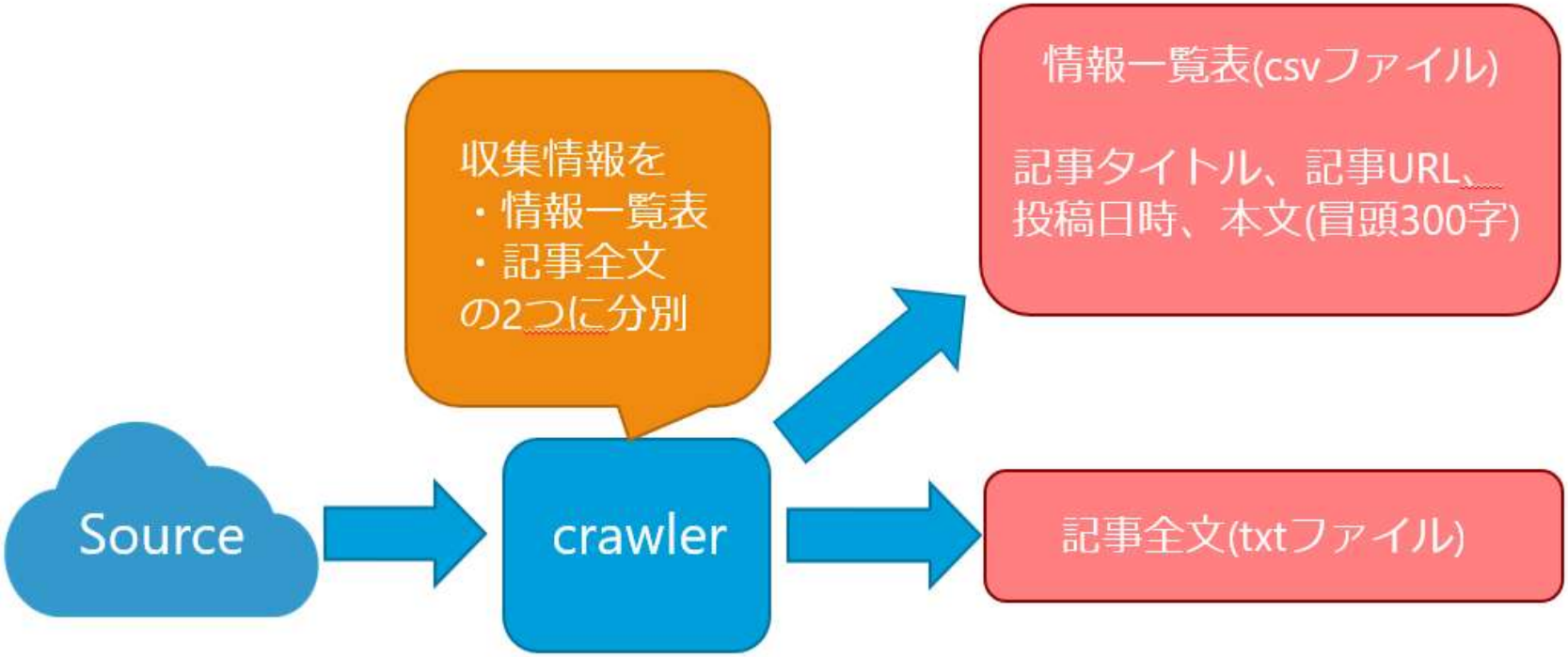
●先行研究
OSINTによる収集と自動タグ生成システムの提案(天野純一郎、森滋男、水越一郎、後藤厚宏)

●企業事例
インシデントレスポンスを支えるOSINT(NTT Communications)

要件1の実装

1.情報収集後は、元記事が削除された場合でも情報の閲覧が可能である

要件1では従来のクローラより収集する情報量を増やすため、
1記事あたり記事タイトル、記事URL、記事投稿日時、記事全文を収集する。
収集した情報は情報一覧表(csvファイル)と記事全文(txtファイル)に分類し、各ファイルに必要な情報を分別する。



要件1の実装

1.情報収集後は、元記事が削除された場合でも情報の閲覧が可能である

情報一覧表(例)

title	URL	投稿日時	キーワード	本文
Google、「Chrome 109」をリリ	https://ww	2023/1/12	セキュリティ/対策/脆弱	Googleは、WindowsやmacOS、Linux向けにブラウザの最新版「Chrome 109」をリリースした。複数の脆弱性を修正
教委認定講習の論文が所在不明に	https://ww	2023/1/11	セキュリティ/対策	大阪府は、大阪府教育委員会免許法認定講習の受講者が作成した論文が所在不明になったことを明らかにした。同府に
アンケートフォームで設定ミス、	https://ww	2023/1/11	セキュリティ/対策/個人	大阪府守口市は、イベント参加者向けのアンケートフォームにおいて、他回答者に関する個人情報が閲覧できる状態と
Synology製ルータのOSやVPNサ	https://ww	2023/1/11	セキュリティ/対策/脆弱	Synology製ルータのOSやアドオンパッケージのVPN機能に深刻な脆弱性が明らかとなった。アップデートが提供され
米政府、「OWASSRF」など悪用	https://ww	2023/1/11	セキュリティ/対策/脆弱	2022年11月に明らかとなった「Microsoft Exchange Server」の脆弱性や、年明け2023年1月の月例パッチで修正された
「Adobe Acrobat/Reader」に深	https://ww	2023/1/11	セキュリティ/対策/脆弱	Adobeは、PDFファイルの生成や編集機能を提供する「Adobe Acrobat」や閲覧機能を提供する「Adobe Reader」向け
「PHP」にセキュリティアップ	https://ww	2023/1/11	セキュリティ/対策/脆弱	PHPの開発チームは、最新版となる「PHP 8.2.1」「同8.1.14」「同8.0.27」をリリースした。今回のアップデートでは
MS、2023年1月の月例セキュリ	https://ww	2023/1/11	セキュリティ/対策/脆弱	マイクロソフトは、2023年最初となる月例セキュリティ更新プログラムを公開した。98件の脆弱性に対処しており、す
トレンドマイクロが新ロゴ - 「T	https://ww	2023/1/10	セキュリティ/対策	トレンドマイクロは、1月10日よりあらたなコーポレートロゴを使用すると発表した。従来と同様に円形の赤を主体と
解約元帳やローン借入申込書など	https://ww	2023/1/10	セキュリティ/対策/個人	ザ信用金庫の宜野湾支店において、顧客情報が記載された書類の所在がわからなくなっている。廃棄業者に誤って引き
健保組合向け管理システムでダウ	https://ww	2023/1/10	セキュリティ/対策	健康保険組合向けに人間ドック受診管理システムを提供しているイーウェルは、健保加入事業者へダウンロード権限を
「Apache Kylin」にアップデート	https://ww	2023/1/10	セキュリティ/対策/脆弱	10月にオープンソースの分散分析エンジン「Apache Kylin」のアップデートにて脆弱性が修正されたが、対策をバイパ
「Zoom Rooms」のクライアント	https://ww	2023/1/10	セキュリティ/対策/脆弱	ビデオ会議サービスを展開するZoomは、WindowsやmacOS向けの「Zoom Rooms」においてアップデートを通じて脆
2022年12月のフィッシングURL、	https://ww	2023/1/10	セキュリティ/対策/フィ	フィッシング対策協議会は、2022年12月に報告を受けたフィッシング攻撃の状況について取りまとめた。報告数全体の
宅食サービス会社がランサム被害	https://ww	2023/1/6	セキュリティ/対策/ラン	食事宅配サービス「ナッシュ」を展開するナッシュは、パソコンが不正アクセスを受けてランサムウェアに感染し、デ
医療従事者向け求人サイトにサイ	https://ww	2023/1/6	セキュリティ/対策/サイ	医療機関向けのコンサルティングサービスや、医療従事者向けの求人検索サイトを運営するメディウェルは、「病院事
胃がん検診票が所在不明、郵便局	https://ww	2023/1/6	セキュリティ/対策	神奈川県相模原市は、個人情報含む胃がん検診票が所在不明になっていることを明らかにした。同市によれば、検診を
EC事業者の6割弱がサイバー攻撃	https://ww	2023/1/6	セキュリティ/対策/サイ	eコマース事業者の6割弱がサイバー攻撃による被害を経験していることがわかった。また3割強が不正注文による被害
セブンイレブンのマルチコピー機	https://ww	2023/1/6	セキュリティ/対策	セブン・イレブン・ジャパンの店舗に設置されているマルチコピー機において一時障害が発生し、一部行政サービスを

要件1の実装

1.情報収集後は、元記事が削除された場合でも情報の閲覧が可能である

記事全文(例)

Google、「Chrome 109」をリリース - 複数の脆弱性を修正.txt - メモ帳

ファイル(F)　編集(E)　書式(O)　表示(V)　ヘルプ(H)

Googleは、WindowsやmacOS、Linux向けにブラウザの最新版「Chrome 109」をリリースした。複数の脆弱性を修正している。

Windows向けに「同109.0.5414.74」「同109.0.5414.75」、macOS向けに「同109.0.5414.87」、Linux向けに「同109.0.5414.74」をリリースしたもの。セキュリティに関する17件の修正を行った。

CVEベースで脆弱性14件に対処したことを明らかにしている。重要度が4段階中もっとも高い「クリティカル（Critical）」とされる脆弱性は含まれていない。

2番目に高い「高（High）」とされる脆弱性は2件。解放後のメモリを使用するいわゆる「Use After Free」の脆弱性「CVE-2023-0128」や、ヒープバッファオーバーフローの脆弱性「CVE-2023-0129」などを修正した。

あわせて重要度が1段階低い「中（Medium）」とされる脆弱性8件や、もっとも低い「低（Low）」とされる脆弱性4件を解消している。同社は数日から数週間をかけてアップデートを展開していく予定。今回修正された脆弱性は以下のとおり。

CVE-2023-0128
CVE-2023-0129
CVE-2023-0130
CVE-2023-0131
CVE-2023-0132
CVE-2023-0133
CVE-2023-0134
CVE-2023-0135
CVE-2023-0136
CVE-2023-0137
CVE-2023-0138
CVE-2023-0139
CVE-2023-0140
CVE-2023-0141

（Security NEXT - 2023/01/12 ）|

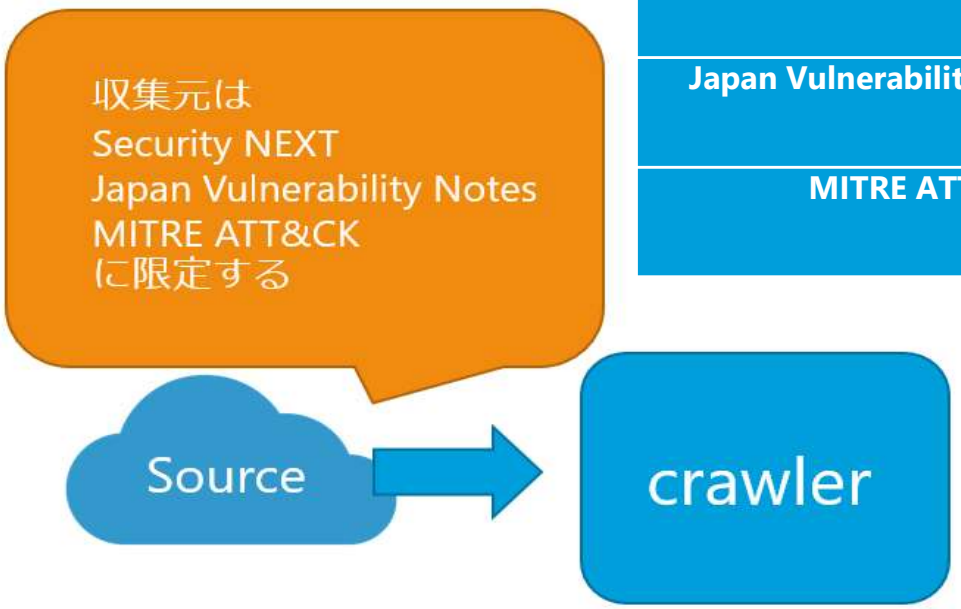
要件2の実装

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

2.情報収集の自動化にセキュリティ脅威がない

本研究は対象が企業等組織となるため、セキュリティ脅威は最大限削減する必要がある。そのため、OSINTシステムによって収集される情報の収集元を限定させ、マルウェアや収集を想定していない情報の誤収集を防ぐ。
本研究では収集元をSecurity NEXT、Japan Vulnerability Notes(JVN)、MITRE ATT&CKに限定し、セキュリティニュースを収集する。

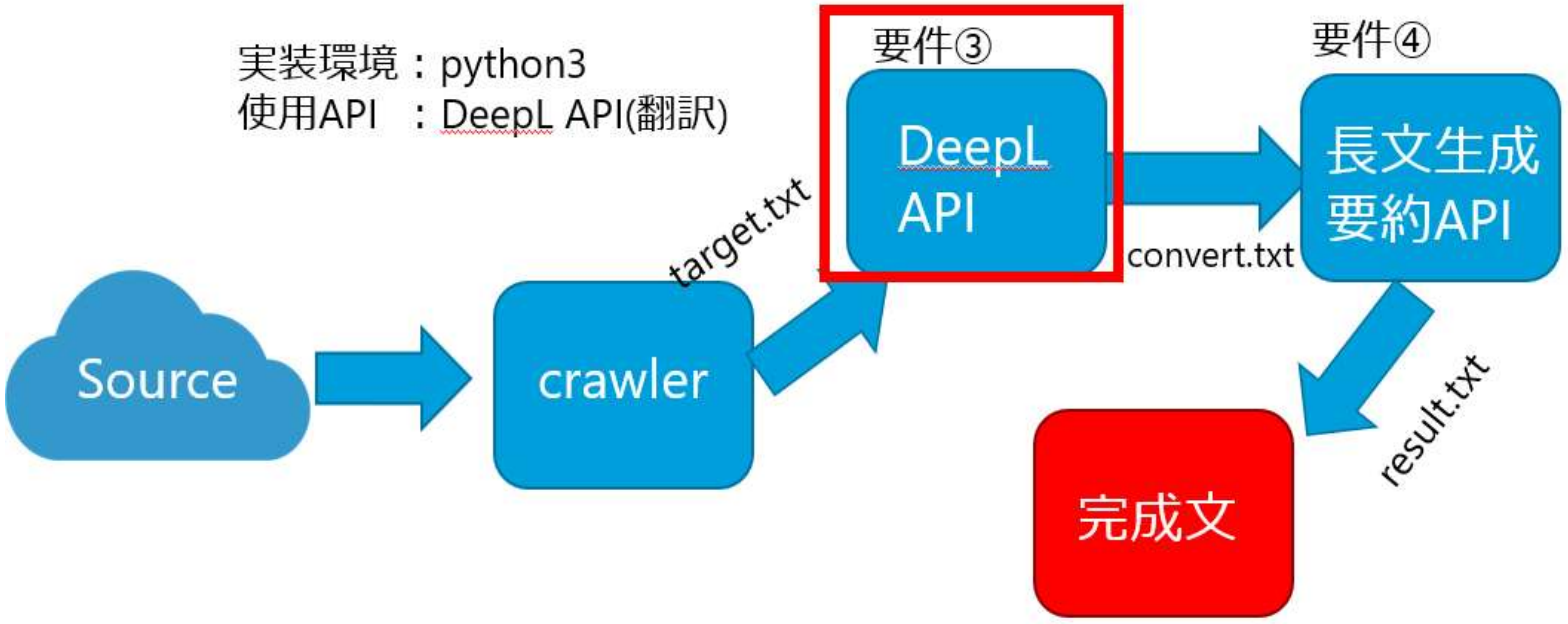
収集元	言語	収集内容
Security NEXT	日本語	日本国内の脅威情報、脆弱性情報を中心としたセキュリティ情報全般
Japan Vulnerability Notes(JVN)	日本語	日本国内のものを中心とした、全世界の脆弱性情報
MITRE ATT&CK	英語	日本国外の脅威情報、脆弱性情報を中心としたセキュリティ情報全般



要件3の実装

3.収集された情報を分かりやすくするため、収集情報の日本語翻訳が
自動的に行われる

クローラによって収集された本文(target.txt)をDeepL APIによって自動翻訳を行い、次の長文要約のフローへ流している(convert.txt)



要件3の実装

3.収集された情報を分かりやすくするため、収集情報の日本語翻訳が自動的に行われる

翻訳前の記事文(target.txt)

target.txt - メモ帳

ファイル(F) 編集(E) 書式(O) 表示(V) ヘルプ(H)

BEIJING -- The Chinese government on Thursday called on Washington to repeal its technology export curbs after California-based chip designer Nvidia said a new product might be delayed and some work might be moved out of China.

The latest controls add to mounting U.S.-Chinese tension over technology and security. American officials say they need to limit the spread of technology that can be used to make weapons.

Nvidia said it was told last week it needs a U.S. government license to export any product with performance equal to its A100 graphics processing chips or better to China, Hong Kong or Russia. It said buyers of the A100, and development of the newer H100, might be affected.

But in an amended disclosure Thursday to U.S. securities regulators, the company said the U.S. government was offering some reprieve by authorizing certain chip exports that will enable Nvidia to keep supplying them to American customers through March.

The high-end chips are designed to help power data centers and run artificial intelligence applications. The restrictions don't affect Nvidia's better-known products used in video games and automotive technology.

要件③(DeepL APIの利用)

翻訳後の記事文(convert.txt)

*convert.txt - メモ帳

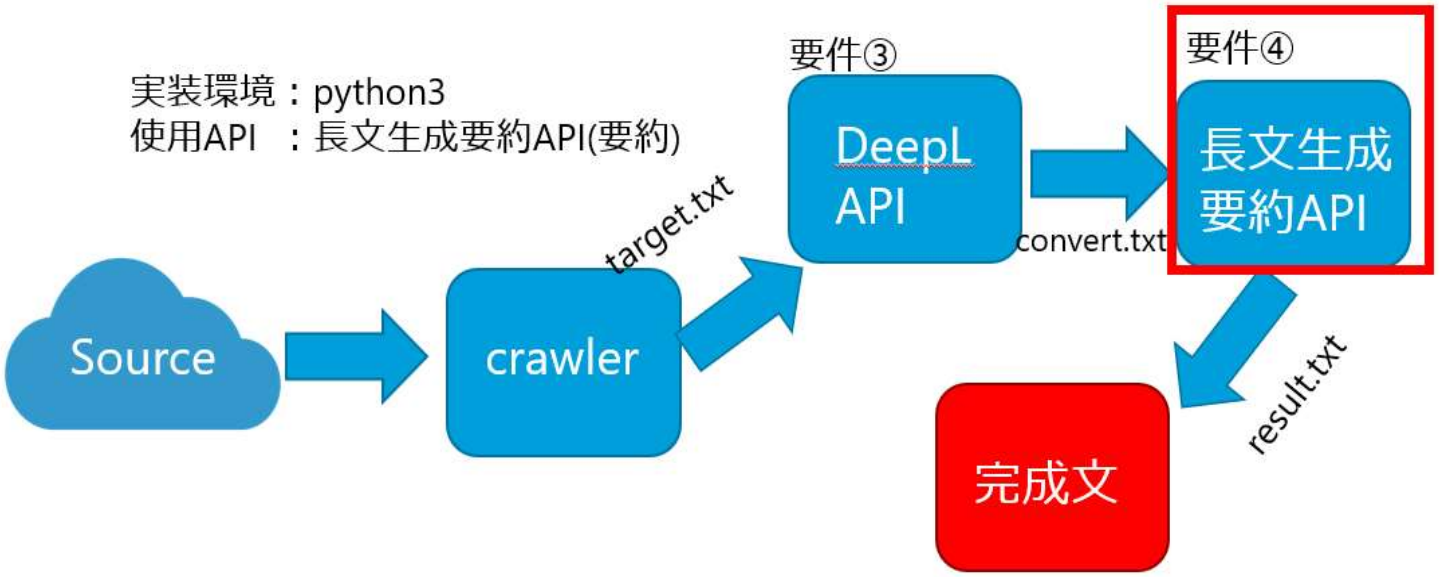
ファイル(F) 編集(E) 書式(O) 表示(V) ヘルプ(H)

北京発--カリフォルニア州に本拠を置くチップ設計会社Nvidiaが、新製品を延期し、一部の作業を中国から移すかもしれないと述べたことを受け、中国政府は24日、ワシントンに対し技術輸出規制を撤廃するよう要請した。　今回の規制は、技術と安全保障をめぐる米中間の緊張を高めるものだ。米政府関係者は、兵器の製造に使用できる技術の普及を制限する必要があると述べている。　Nvidiaは先週、同社のA100グラフィック処理チップと同等以上の性能を持つ製品を中国、香港、ロシアに輸出するには、米国政府のライセンスが必要だと告げられたという。A100の購入者や、より新しいH100の開発に影響を与える可能性があるという。　しかし、木曜日に米証券規制当局に提出した修正開示資料の中で、同社は、米政府が一部のチップ輸出を許可することによって、Nvidiaが3月まで米国の顧客に供給を続けることができるよう、一定の猶予を与えていることを明らかにした。　ハイエンドチップは、データセンターの電力供給や人工知能アプリケーションの実行に役立つよう設計されている。この規制は、ビデオゲームや自動車技術に使用される、よりよく知られたNvidiaの製品には影響を与えない。

要件4の実装

4.収集された情報を分かりやすくするため、収集情報の要約が自動的に行われる

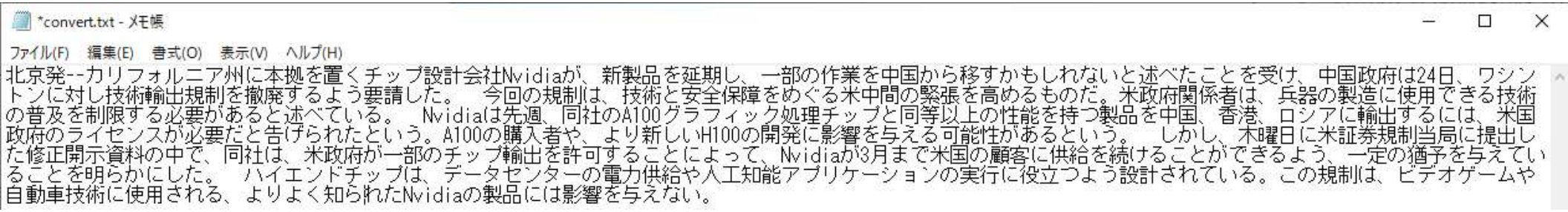
DeepL APIによって翻訳された記事文章(convert.txt)を長文生成要約APIにかけ、完成文(result.txt)に流している。



要件4の実装

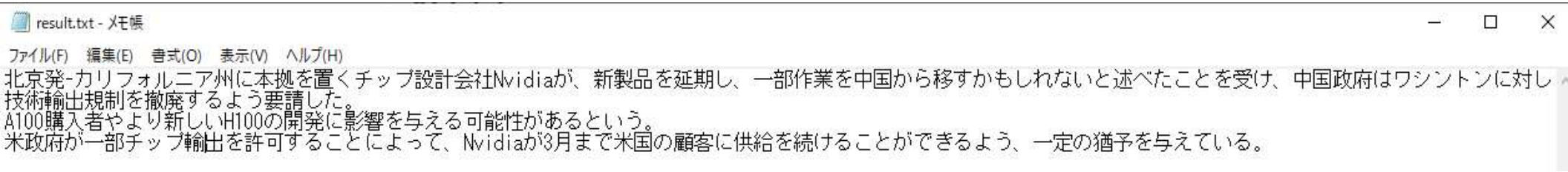
4.収集された情報を分かりやすくするため、収集情報の要約が自動的に行われる

要約前の記事文(convert.txt)



要件④(長文生成要約APIの利用)

要約後の記事文(result.txt)



利用者評価

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

利用者評価では、筆者が所属する企業のセキュリティ担当4名に対して以下の流れで実験を行い、実験後のアンケートをもとに評価を行う

①事前アンケート
②研究内容・OSINT機能の説明
③既存OSINT機能利用(要件機能追加前)
④新規OSINT機能利用(要件機能追加後)
⑤事後アンケート

事前アンケート

セキュリティ業務歴(年)/保有しているIT・セキュリティ関連資格/OSINT(クローリング)機能の利用経験有無

事後アンケート

研究内容・説明の分かりやすさ/1回目OSINT機能の評価(使いやすさ)/2回目OSINT機能の評価(使いやすさ)/要件1～4の評価(有効度)

利用者評価

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

事前アンケート結果

氏名	セキュリティ業務歴(年)	保有しているIT・セキュリティ関連資格	OSINT(クローリング)機能の利用有無
A	13	基本情報技術者、CND、CEH	有り
B	3	基本情報技術者、ITパスポート、CCNA	無し
C	3	ITパスポート、応用情報技術者	無し
D	2	ITパスポート、セキスペ	無し

事後アンケート結果：1(分かりにくい・無効)～5(分かりやすい・有効)

氏名	研究内容・説明の分かりやすさ	既存OSINT機能の評価	新規OSINT機能の評価	内容の取り込み機能(要件1)	情報収集の脅威排除機能(要件2)	情報の翻訳機能(要件3)	情報の要約機能(要件4)
A	4	3	4	5	1	5	3
B	5	4	5	4	3	5	4
C	5	3	5	5	2	5	5
D	4	4	5	5	3	5	4
Avg.	4.5	3.5	4.75	4.75	2.25	5	4

利用者評価

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

事後アンケート結果：1(分かりにくい・無効)～5(分かりやすい・有効)

氏名	研究内容・説明の分かりやすさ	既存OSINT機能の評価	新規OSINT機能の評価	内容の取り込み機能(要件1)	情報収集の脅威排除機能(要件2)	情報の翻訳機能(要件3)	情報の要約機能(要件4)
A	4	3	4	5	1	5	3
B	5	4	5	4	3	5	4
C	5	3	5	5	2	5	5
D	4	4	5	5	3	5	4
Avg.	4.5	3.5	4.75	4.75	2.25	5	4

氏名	コメント
A	1つ目のシステムと2つ目のシステムでは、2つ目のシステムの方が使いやすかった。特に要件1の一覧と全文が分かれている部分については、詳細に調べたい記事をすぐにみることができるようになっていたのでよかった。要件2は、普段閲覧しているサイトが使えなかったため使いにくさを感じた。要件4は、使用する状況によっては助かる機能かもしれない。
B	説明が分かりやすく、使用したシステムも使いやすかった。翻訳は手動で翻訳機にかける手間が省けたのでとても良いと感じた。
C	2回目のシステムの方が比較して利用しやすい。要件2はもっと複数のサイトから記事を集められると良いと感じた。
D	

まとめ

情報セキュリティ大学院大学

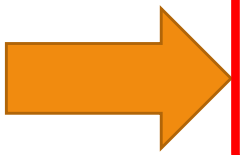
SOC業務の課題
・スキルを持った人材の確保が困難
・現場運用のウェイトが重く、脅威動向を追えていない

SOC業務支援のためのOSINTシステム提案
・セキュリティに関する最新の脅威動向を自動的に収集する
・要約された収集情報をチェックすることでSOCの通常業務への負担を少なくして**攻撃**の高度化を追う

OSINTシステムの実装・評価

既存のOSINTシステムに新規要件を付加

要件①収集情報の保存
要件②情報収集の脅威排除
要件③収集情報の翻訳
要件④収集情報の要約



SOC業務従事者にアンケートを実施

・既存OSINT機能より、新規OSINT機能の方が評価が高い
・要件①、要件③の評価が高い

結論

提案手法の実装を実装し、セキュリティ業務の従業員4名の評価を受けたところ、**要件付加前のOSINT機能より提案するOSINT機能の方が扱いやすく、SOC業務に必要な情報収集の面で支援されていることを示した。**残課題として、以下がある
(1)組織で定常的に利用する場合の環境・スペックの決定
(2)OSINT機能とSIEMの連携
(3)翻訳・要約機能の調整
(4)情報収集のセキュリティ脅威排除機能(要件2)の改善

論文構成

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

1.はじめに
1.1.研究背景
1.2.研究の目的
1.3.インテリジェンス活動の概要

2.SOC業務へのOSINTの活用
2.1.SOC業務の概要
2.2.一般的なSOC業務へのOSINT活用
2.3.本研究におけるSOC業務の課題とOSINT活用による解決
2.4.OSINT活用による効果

3.先行研究調査について
3.1.SOC業務におけるOSINTの自動化
3.2.OSINTの自動化に関する先行研究とツール

4.提案手法について
4.1.本研究の焦点、OSINTに求めること
4.2.OSINTで収集する情報の分類
4.3.本研究における組織の規模感
4.4.新規要件の効果と仕組み
4.4.1.要件①
4.4.2.要件②
4.4.3.要件③
4.4.4.要件④

5.本研究の実装と評価
5.1.本研究の実装
5.2.本研究の評価

6.今後の課題とまとめ
6.1.今後の課題
6.2.まとめ

7.参考文献

外部発表予定

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- ◆大会名称 ： 第22回情報科学技術フォーラム(FIT2023)
- ◆大会会期 ： 2023年9月6日（水）～9月8日（金）
- ◆会 場 ： 大阪公立大学 中百舌鳥キャンパス(大阪府堺市中区学園町1番1号)
- ◆発表テーマ： SOC業務支援のためのオープンソースインテリジェンスシステムの提案と評価

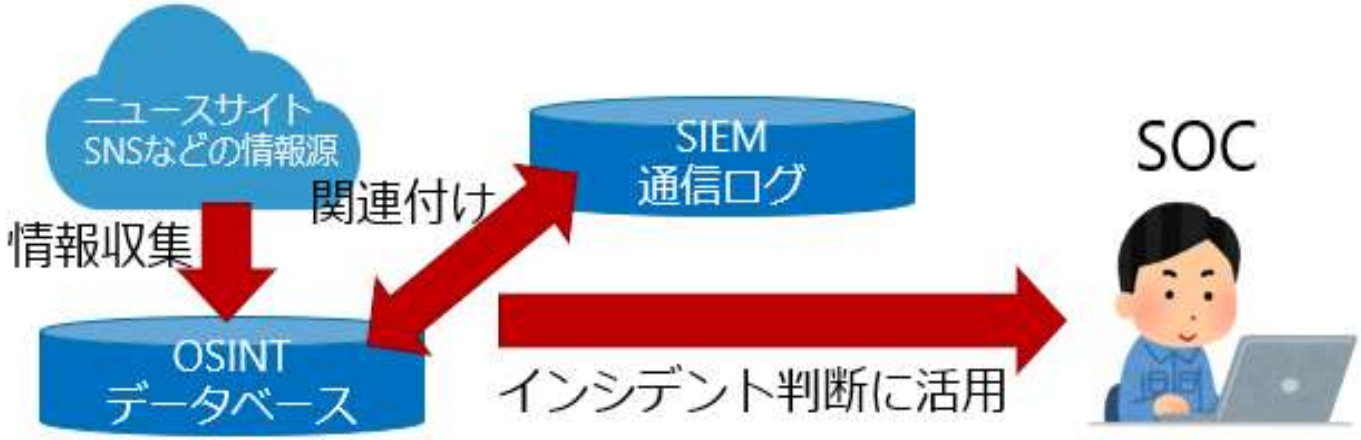
今後の課題

(1)組織で定常的に利用する場合の環境・スペックの決定

本研究では、OSINTの機能を試用的に活用しており、24時間のクローリングや膨大な収集記事を全て格納するスペックを求めていないため、本機能を組織が定常的に利用する場合に必要な環境やスペックが分かっていない。
今後の課題として、本研究内容を組織で本利用する場合に必要なスペックがどの程度なのかを調査・検討する必要がある。

(2) OSINT機能とSIEMの連携

SOC業務におけるインシデント判断は、通信ログのみでは困難であり、アラート内容の誤った判断に繋がる場合がある。本研究で提案するOSINT機能とSIEMで管理されているログを連携させることで、SOCのインシデント判断の正確化を図ることができると考える。



今後の課題

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

(3)翻訳・要約機能の調整

要件3「収集された情報を分かりやすくするため、収集情報の日本語翻訳が自動的に行われる」と要件4「収集された情報を分かりやすくするため、収集情報の要約が自動的に行われる」について、各種APIを選択して本研究に活用をしているが、API選択理由については先行研究におけるAPIの有効性や感覚的な有効性等となっており、理論的な選択ができていない。
そのため、今後SOC支援のためのOSINTシステムとして最も有効な翻訳システム、要約システムを提案する場合に、最有効できる証明が可能である必要があると考える。

(4)要件2の改善

要件2「情報収集の自動化にセキュリティの脅威がない」は、意図しないものを収集するための対策としては有効だが、利便性については評価が低いといった結果になった。
本研究では収集元を3つに絞り、信頼のある収集元のみの活用になったため、今後の課題としては同様に脅威対策を講じつつ幅広い収集元からの情報収集を実現することが必要だと考える。