様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２８ 年　 ６ 月 １１ 日現在

機関番号：８２６３６
研究種目：若手研究(B)
研究期間：2012～2015
課題番号：２４７０００８３

研究課題名（和文）サイバーセキュリティ情報交換のためのセマンティック情報検索手法に関する研究

研究課題名（英文）Studies on semantic information retrieval techniques for cybersecurity information

研究代表者

高橋　健志（Takahashi, Takeshi）

国立研究開発法人情報通信研究機構・ネットワークセキュリティ研究所セキュリティアーキテクチャ研究室・主任研究員

研究者番号：５０６００１６０

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：この4年間の研究では、組織の壁を超えた効率的なセキュリティ情報交換を促進すべく、ネットワーク上から必要かつ信頼できるセキュリティ情報を特定・発見する技術を構築することを目的として実施してきた。将来拡張性も担保するセマンティックデータ構造を構築し、それを用いた知識ベースを構築することで、必要な情報を必要なエンティティに届ける技術基盤を構築してきた。また、その技術の有効性を示すべく、最終年度には組織内のIT資産の脆弱性を自動的に検出する技術のプロトタイプを構築し、提案技術とそれを用いた知識ベースの有用性を示した。

研究成果の概要（英文）：In this four years of research, we have studied on the technique that identifies and discovers needed and trustful security information from the web in order to facilitate the efficient security information exchange beyond the borders of organizations. During this study, we proposed a semantic data structure that maintains future extensibility. With the data structure, we built a knowledge base, which delivers information to the entities that need it. To demonstrate the usability of the technique, I have introduced a system that automatically idenftifies vulnerability of IT asset within an Intranet. Based on these study, we conclude that the proposed technique and the knowledge base are viable and useful for the purpose of advancing cybersecurity information exchange and automation.

研究分野：サイバーセキュリティ

キーワード：ディスカバリ　サイバーセキュリティ　知識ベース　検索　データ表現

１．研究開始当初の背景

増え続けるサイバーセキュリティの脅威に対処すべく、組織の壁を越えたセキュリティ情報交換が求められている。しかし、現時点では効率的な情報交換がなされておらず、各国・各組織は独立してセキュリティ対策を講じているのが現状である。その結果、国境を越えて連携して襲ってくるサイバーセキュリティの脅威に対し、その対策は圧倒的に非効率かつ劣勢な状況にある。本状況に対処するには組織の壁を越えた情報交換が必要不可欠であるが、現時点では組織間での効率的な情報交換手法は確立しておらず、メール、電話、対面での打ち合わせなど、担当者レベルで属人的に、時間と人手を要して実施しているのが現状である。

２．研究の目的

本研究では、構造化されたサイバーセキュリティ情報をネットワーク上で特定・発見する技術を確立することを目指す。既に申請者が検討してきている技術フレームワークに基づき、実際にネットワーク上で情報交換を実現するのに必要な具体的な手法を確立することを目的とする、また、それに基づくプロトタイプ実装を構築する。

３．研究の方法

本研究を実施するにあたり、初年度にセマンティック情報検索手法を提案し、ネットワーク上の情報の中から関連性の高い情報を精緻かつ効率的に特定・発見する手法を確立する。次年度には、前年度の成果を用いて検索された情報を、信頼度に基づきランキングすることにより、ユーザにとっての検索結果の有効性を向上すると同時に、誤った情報に基づくセキュリティ増大リスクを抑制する。最終年度には、これまでの研究成果と既存技術を合わせてセキュリティ情報のセマンティック検索ツールを構築し、それに基づく評価、成果展開を実施する。また、最終年度の後 1 年の時間を用い、最終年度までの研究成果を用いたユースケース技術の開発にも着手し、提案技術の有効性及び有用性を示す。

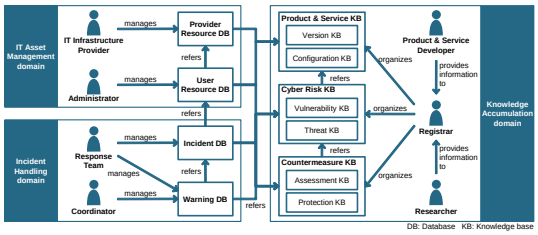
４．研究成果

この 4 年間の研究では、組織の壁を超えた効率的なセキュリティ情報交換を促進すべく、ネットワーク上から必要かつ信頼できるセキュリティ情報を特定・発見する技術を構築することを目的として実施してきた。将来拡張性も担保するセマンティックデータ構造を構築し、それを用いた知識ベースを構築することで、必要な情報を必要なエンティティに届ける技術基盤を構築してきた。また、その技術の有効性を示すべく、最終年度には組織内の IT 資産の脆弱性を自動的に検出する技術のプロトタイプを構築し、提案技術とそれを用いた知識ベースの有用性を示した。

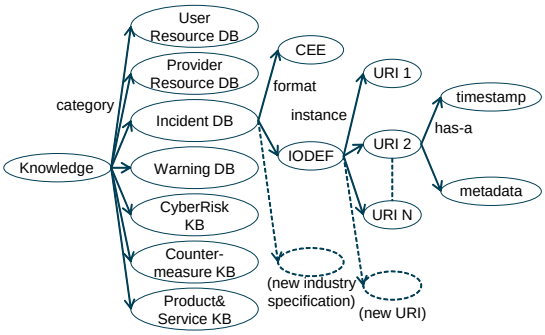
以下、本研究において特に強調したい成果について、個別に記載する。

(1) reference ontology の構築

本研究の核の一つに、拡張性の高いデータモデルの構築がある。下記の図が、そのモデルの概要を示している。



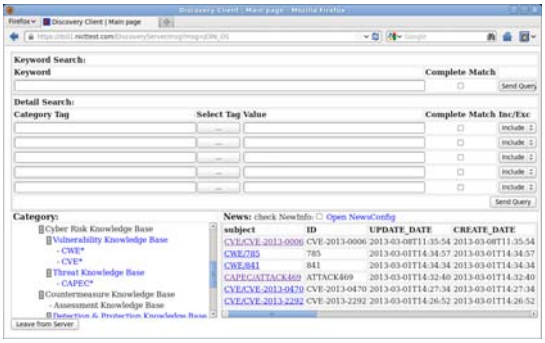
本モデルは、セキュリティオペレーションを実施する際に必要となる情報の種類を概念レベルで定義したものであり、これに基づき、蓄積する情報の構造を決定した。そして、具体的に下記の情報構造を確立するに至った。



本情報構造は、カテゴリとスキーマが分けて定義されているところが最大であり、将来的に新たなスキーマが登場した際には、一つのカテゴリとその新スキーマをリンクするのみで対応できるという、将来拡張性に優れるという特徴を持っている。本成果の詳細については、主な発表論文[1]を参照のこと。

(2) 知識ベースの構築

上述のデータ構造に基づき、インターネット上の各種セキュリティ関連情報をリンクし、横断検索を実現する知識ベースを構築した。データモデルを実装すると同時に、Restful なインターフェースを定義し、また検索のための SPARQL インターフェースを工夫することで、本技術を実現した。また、プロタイプを実装し、米国の National Vulnerability Database (NVD) と日本の Japan Vulnerability Notes (JVN)のデータをリアルタイムでリンク・監視できることを確認した。



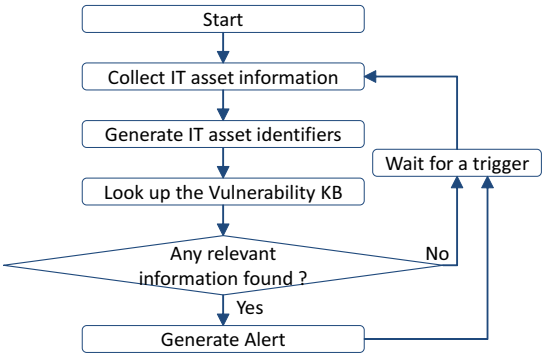
本成果の詳細については、主な発表論文[1]を参照のこと。

(3) 情報をネットワーク上で交換するためのツールとして、IODEF-SCI を構築

セキュリティ情報を収集し、その収集した情報を組織間で交換する際には、共通フォーマットが必要であり、そのための技術として、IODEF-SCI という技術を RFC 7203 として構築した。本技術は、各種の XML 情報や identifier を、その構造を壊さずにネットワーク上で伝送するための表現技術である。そして、その技術をツールとして実装し、その有効性を示した。本成果の詳細については、主な発表論文[2]を参照のこと。

(4) ユースケースとしての脆弱性自動管理技術の構築

知識ベースを構築し、各種セキュリティ情報を検索できる技術を構築したものの、それは何らかのユースケースに基づき活用されて初めて意味のある成果となる。そのため、一つのユースケースとして、Intranet 上に存在する各種 IT 資産に関する脆弱性情報を自動で収集し、警告を管理者で自動的に連絡する技術を構築した。下記に、本技術のプロセスフローを示す。



本技術により、下記の通りのアラートメッセージをシステム管理者に送ることができ、また、本メッセージはシステム管理者が知るべき情報のみ、知るべきタイミングにて送付されるようになっている。

本成果の詳細については、主な発表論文[3]を参照のこと。

５．主な発表論文等

〔雑誌論文〕
論文誌 1 件

1. T. Takahashi, Y. Kadobayashi, ″Reference Ontology for Cybersecurity Operational Information,″ The Computer Journal, 58, 2297 - 2312, Oxford, October, 2015（査読有）

〔学会発表〕（計 6 件）
国際学会 4 件
国内研究会 2 件

1. T. Takahashi, D. Miyamoto, ″Structured Cybersecurity Information Exchange for Streamlining Incident Response Operations,″ IEEE/IFIP Network Operations and Management Symposium, Istanbul(Turkey), IEEE, April 28, 2016
2. T. Takahashi, D. Miyamoto, K. Nakao, ″Toward Automated Vulnerability Monitoring using Open Information and Standardized Tool,″ IEEE International Conference on Pervasive Computing and Communications, Sydney(Australia), IEEE, March 16, 2016
3. T. Takahashi, Y. Kadobayashi, ″Mechanism for Linking and Discovering Structured Cybersecurity Information over Networks,″ IEEE International Conference on Semantic Computing, 279 - 284, Newport

Beach(USA), IEEE, June 16, 2014

4. T.Takahashi, Y.Kadobayashi, Y.Takano, ″Linking Cybersecurity Knowledge: Cybersecurity Information Discovery Mechanism,″ Annual Computer Security Applications Conference poster session, ACSAC, Orlando(USA), December 6, 2012
5. 高橋健志, 宮本大輔, パンタボーラ, 中尾康二, ”組織内のソフトウェア資産に対する脆弱性監視・警告自動化ツールの検討,” 九工大 百周年中村記念館(福岡県北九州市), 信学技報, 電子情報通信学会, 2015 年 6 月 12 日
6. 高橋健志, 門林雄基, 高野祐輝, ”インターネット上に存在するサイバーセキュリティ情報のディスカバリ技術に関する検討,” 北海道工業大学(北海道札幌市), 信学技報, 電子情報通信学会, 2012 年 7 月 19 日

〔図書〕(計０件)

〔産業財産権〕
特になし

〔その他〕
特になし

６．研究組織
(1)研究代表者
高橋健志（TAKAHASHI, Takeshi）
国立研究開発法人情報通信研究機構・サイバーセキュリティ研究所サイバーセキュリティ研究室・主任研究員
研究者番号：50600160

(2)研究分担者
なし

(3)連携研究者
なし