「革新的技術の国際法政治経済への影響の分析」研究経過報告

平成 30 年 3 月 28 日受付

岩 本 誠 吾*

要 旨

本稿では，特定課題研究「革新的技術の国際法政治経済への影響の分析」の中間報告を行う。なかでも，開発中のデータベースの一部である「サイバー攻撃情報自動分類システム」について解説する。本システムは，web 上に公開されているインターネットセキュリティ脆弱性データに対して，サイバー攻撃に特徴的なキーワードを用いて検索を行い，その結果に基づき，各脆弱性データを，想定される攻撃タイプ別に自動分類するシステムである。10 万件以上のデータを，6 つのパターンに自動的に分類することで明らかになる攻撃タイプの特徴の解明は，サイバーセキュリティに対する中長期的政策の立案において，有効な手段となることが期待される。

キーワード：サイバーセキュリティ，人工知能，国際法，国際政治，国際経済

1. はじめに

本研究は，「先端技術の開発・規制のための適切な国際ルールの提案」「先端技術に関する国際政治経済の実態把握」「先端技術情報データベース構築」を三本柱として，研究を遂行している。このうち，前二者については，本稿末に挙げた研究リストにおいて，その成果を示したので，本文では，第三のデータベースに関する中間成果報告を行う。

さまざまな先端技術のうち，本年度は，サイバー攻撃情報に関するデータベース構築に取り組んだ。これについては，2017 年 9 月 30 日に開催した定例研究会における客員研究員八槇博史らによる報告が，その基本的仕組みを最も簡潔に解説している。次節は，齋藤・八槇（2017）をもとに作成している。

2. サイバー攻撃情報自動分類システム

本研究で作成中のサイバー攻撃情報自動分類システム（以下では自動分類システム）とは，web 上で入手できる未分類の膨大なインターネット脆弱性データを，本研究で独自に定めた攻撃類型に基づいて，自動的に分類するシステムである。このシステムは，攻撃パターンの特徴を明らかにすること

* 京都産業大学法学部，グローバル公共財研究センター

で，サイバー攻撃への対策を純粋に技術的観点から容易にするのみならず，より包括的なサイバーセキュリティ政策立案全般にも役立てることを目的として構築されている。具体的な設計・仕様は，次の（1）から（3）のとおりである。

(1) 脆弱性情報データを分類するための検索単語群データベースの事前作成

周知のように，今日のコンピュータ・ネットワークにおいては，セキュリティ上の脆弱性は日々確認されるが，その脆弱性を利用したサイバー攻撃は，いくつかのパターンに分類できる。この特性に注目し，本研究の自動分類システムでは，web 上の膨大な脆弱性情報データ（記事）を，6 つの攻撃パターンごとに分類する。具体的な分類方法として，本自動分類システムでは，脆弱性データ（記事）のなかに，特定の攻撃パターンが実行される可能性を示唆する単語群が出現するか否かを基準とし，それによって分類を行うという方法を用いた，

上述の分類を実行する前提として，分類基準の単語群を集積した「単語群データベース」が別途事前に必要となるが，本研究では，この単語群データベース作成のためのデータとして，Exploit-DB を用いた。また，単語群選択アルゴリズムとしては単語 N-gram を使用した。実際の実装においては，単語 3-gram，出現頻度 6 回以上 10 回以下を用いた。

(2) Web 上の脆弱性データのローカル環境への移行

膨大な web 上のデータの分類作業を実行するために，データをいったんダウンロードしたローカル環境を構築する。ローカル環境の構築には，web アプリケーションの開発環境を比較的容易にする XAMPP を用いた。また，脆弱性データ本体は，RAPID7 社が公開している脆弱性情報データベースを対象とした。ここには，脆弱性情報・攻撃モジュール情報が約 10 万件登録されている。

(3) 単語群を用いた脆弱性情報の分類

（1）で作成した単語群を用いて，（2）でローカル環境に置いた脆弱性情報データを分析し，各データを攻撃パターンごとに分類する。具体的には，脆弱性情報 1 件ごとに，6 要素を持った配列を与え，初期値では，すべて 0 としておく。各配列は，先頭から順に「バッファオーバーフロー」「XSS」「ディレクトリトラバーサル」「SQL インジェクション」「ヒープスプレー」「CSRF」に対応させている。そして，各データごとに，（1）の単語群の検索をかけ，その単語群が出現した場合，それに対応する上記の配列を 1 にする（表 1 を参照）。

表 1　攻撃パターン分類の実行例

データ ID/ 攻撃手法	BOF	XSS	DirTra	SQLin	BSP	CSRF
1	0	1	0	0	0	0
2	1	1	0	0	0	0
3	1	1	0	0	0	0
4	0	1	1	0	0	0

齋藤・八槇（2017）を修正

表 1 では，ID2 と 3 が同じ類型を形成しており，これを同パターンとみなす。

(4) 課題

現在, 上記の実装のもと, 本格的にデータ分類を開始するとともに, さらに分類の精度の向上を図っている。本節の冒頭でも述べたように，本研究によって明らかにする攻撃パターンの特徴の解析結果を，サイバー攻撃の政策立案に生かすことが最終的な目標となる。

3. 本研究全体の今後の展望と課題

本研究では，2 で解説したような新技術に関するデータベースを，ドローン，ロボット兵器，仮想通貨など，サイバー技術以外のさまざまな新技術に対して構築し，政策立案に活用することを展望している。しかしながら, これまでの研究過程においては, 科学技術の進歩が著しいことから, サイバー攻撃に絞るだけでも，当初の予想以上に，たいへんな労力を，ますます必要するようになってきていることが明らかになってきている。次年度は，この課題に対応しつつ，可能な限り，サイバー攻撃以外の技術にも研究を発展させるように努める。

研究リスト

Hideaki Ashitate（2018）“Governance by Network and Its Applicability to National Aid Policies and Local Governance,” A. Farazmand ed., *Global Encyclopedia of Public Administration, Public Policy, and Governance*. https://doi.org/10.1007/978-3-319-31816-5_3505-1.（pp. 1–5.）

岩本誠吾（2018）「第 12 章　ロボット兵器と国際法」弥永真生・宍戸常寿編著『ロボット・AI と法』有斐閣 285-310 頁。

岩本誠吾（2018）「平和安全法制における自衛隊の法的地位－国際法と国内法との狭間で－」『産大法学』第 51 巻第 3/4 号，1（517）-28（544）頁。

岩本誠吾・吉田和男・八槇博史・坂口博紀・山本和也・藤本茂・岑智偉（2017）「グローバル公共財としての法規制と技術開発 : ドローンによる産業革命，課題と展望」『京都産業大学総合学術研究所所報』第 12 号, 149-154 頁。

Kazuhiro Yuki and Zhiwei Cen（2018）“Effects of the Size of a Country on Its Economic Performance” in M. Tadokoro, S. Egashira, and K. Yamamoto eds., *Emerging Risks in a World of Heterogeneity: Interactions Among*

Countries with Different Sizes, Polities and Societies. Singapore: Springer Nature, pp. 19–44.

ファン　タァン　クァン・八槇博史（2017）“感情解析に基づく誘導型サイバー攻撃検知の検討” コンピュータセキュリティシンポジウム 2017（CSS2017），2C1-3，山形市。

渋谷健太・久山真宏・松本隆・八槇博史・佐々木良一（2017）“標的型に対する知的ネットワークフォレンジックシステム LIFT の開発と機能拡張（その 4）－将来起こりうる攻撃方法の推定－” コンピュータセキュリティシンポジウム 2017（CSS2017），1D3-5，山形市。

齋藤皓介・八槇博史（2017）“サイバー攻撃情報における攻撃類型の自動分類”京都産業大学グローバル公共財研究センター定例研究会。

中山能之・宮本貴義・大石恵輔・岩東佑季・八槇博史（2017）“人工知能搭載型サイバーレンジによるシステム強靱性の検討”マルチメディア，分散，協調とモバイル（DICOMO2017）シンポジウム，pp. 1635-1639，札幌市。

大石恵輔・中山能之・岩東佑季・石川博也・宮本貴義・八槇博史（2017）“サイバー攻撃対策のための人工知能搭載型サイバーレンジの検討”マルチメディア，分散，協調とモバイル（DICOMO2017）シンポジウム，pp. 1635-1639，札幌市。

Kazuya Yamamoto（2018）“A Triad of Normative, Pragmatic, and Science-Oriented Approaches: The Development of International Relations Theory in Japan Revisited” *Korean Journal of International Studies* 16 (1): 22 pages, forthcoming.

Kaoru Ishiguro and Kazuya Yamamoto（2018）“Role of Third-Party Guarantors in Uncertainty of Preventive Civil War: Can Thucydides Trap Be Resolved?” in M. Tadokoro, S. Egashira, and K. Yamamoto eds., *Emerging Risks in a World of Heterogeneity: Interactions Among Countries with Different Sizes, Polities and Societies*. Singapore: Springer Nature, pp. 109–134.

Masayuki Tadokoro, Susumu Egashira, and Kazuya Yamamoto eds.（2018）*Emerging Risks in a World of Heterogeneity: Interactions Among Countries with Different Sizes, Polities and Societies*. Singapore: Springer Nature.

An Interim Report: Research about Effects of New Technologies on Law, Politics, and Economies from International Perspectives

Seigo IWAMOTO

Abstract

This paper presents interim research outcomes that have been produced under the auspices of a grant funded by Kyoto Sangyo University, entitled *Tokutei Kadai Kenkyu*. In particular, it explains a newly developed automated system that classifies data on network vulnerabilities. Based on keywords that are preset for identifying the characteristics of vulnerability, this system classifies each data into the six variants that are prone to certain types of cyberattack. Applying a data set that contains more than 100,000 cases of vulnerabilities to our system, the classified data is expected to be used to develop public policy from long-term perspectives as well as to resolve security problems on daily basis.

Keywords : Cyber Security, Artificial Intelligence, International Law, International Relations, International Economy