3-5　サイバーセキュリティ情報交換技術：情報オントロジの構築とCYBEX

3-5　Cybersecurity Information Exchange Techniques: Cybersecurity Information Ontology and CYBEX

高橋健志　　門林雄基
TAKAHASHI Takeshi and KADOBAYASHI Youki

要旨

グローバル規模でのサイバー社会が構築されつつある現在、サイバーセキュリティの重要性が強く認識されてきている。しかしながら、サイバーセキュリティの脅威は国境を越えてくるものの、その対応は各組織・機関毎に個別に実施されているケースが大半である。これは、サイバーセキュリティ情報交換のフォーマットやフレームワークが広く共有されていないことに一因がある。サイバーセキュリティ情報のフォーマットは複数提案され、そのいくつかは既に一部の地域、組織で使われ始めているものの、それらはグローバル標準ではなく乱立しており、各国・各組織が相互に連携する土台にはなりえていないのが現状である。そこで本稿では、サイバーセキュリティ情報交換フレームワークの土台を構築すべく、サイバーセキュリティオペレーションの情報オントロジを提案する。また、情報交換を促進するための国際標準X.1500/CYBEXの標準化活動とその有効性についても議論する。

Cyber threats cross country borders, but most organizations are currently coping with them individually without global collaboration mainly due to the lack of global standard for cybersecurity information exchange format and framework. Though some countries possess their local standards to solve this problem, these standards are not orchestrated in order for each organization to fully collaborate each other. To build the basis of cybersecurity information exchange framework, this paper proposes an ontology of cybersecurity operational information. It also discusses the standardization activity on cybersecurity information exchange, such as X.1500/CYBEX and its ensembles, and its effectiveness from the standpoint of advancing and expediting cybersecurity information exchange.

[キーワード]
サイバーセキュリティ，オントロジ，情報交換
Cybersecurity, Ontology, Information exchange

1　はじめに

インターネットが世界規模で普及したことにより、近年、サイバー社会が急速に発展してきている。しかしながら、サイバー社会におけるセキュリティ、すなわちサイバーセキュリティに関しては未だ発展途上の段階にある。サイバーセキュリティの脅威は国境を越えて襲ってくるものの、その対策は各国・各組織が個別に対応しているのが現状である。悪意のあるユーザは前もって準備したソフトウェアを走らせるだけで、世界中のコンピュータに対して攻撃可能であるものの、その対策は各国・各組織が独立して実施している。また、各国・各組織が協力するための前提となる情報交換・共有に関しても大変非効率であり、必要に応じてメール、電話、対面での打ち合わせなど、時間と人手を要しているのが現状である。

このような状況は、情報交換のフォーマットやフレームワークが各国・各組織を超えて統一されていないことに一因がある。各国・組織が協力し

てサイバーセキュリティ対策を実施するためには、情報交換のための共通のフレームワークとフォーマットがグローバルに共有される必要があり、それが実現すれば大きく2つのメリットを享受できる。1つ目は地球規模でのサイバーセキュリティ情報の地域格差解消である。これにより、サイバーセキュリティ構築の発展途上にあり、情報の蓄積が少ない国（以下、発展途上国）も情報獲得が容易になり、また、それらの国のコンピュータを利用した先進国への攻撃を激減させることも可能となる。2つ目は、サイバーセキュリティオペレーションの自動化の促進である。現在は手動で行っているオペレーションが自動化されていくことにより、これまで必要だったオペレーションの担当人員数を削減可能になり、また、人手依存体制に起因するミスを回避可能になる。さらには、自動化の推進により、上記の地球規模でのサイバーセキュリティ情報の地域格差解消がより一層推進される。

情報交換フォーマットに関する標準は各種存在するが、多数の地域標準が乱立している状況であり、全体としてのフレームワークが確立されるに至っていない。そのため、既存の標準によるサイバーセキュリティ情報の網羅性に関する議論もできず、非効率なサイバーセキュリティオペレーションの改善も困難なのが現状である。本問題に対処し、世界規模でサイバーセキュリティ情報を交換する土台を構築すべく、本稿ではサイバーセキュリティオペレーションのための情報オントロジを提案する。オントロジとは、世界の概念化モデルであり、これによりソフトウェア間での情報共有・再利用を促進することが期待される。本稿で提案されるオントロジは、日本、アメリカ合衆国、韓国において、実際にサイバーセキュリティオペレーションを実施している事業者各社との議論・検討の結果に基づくものである。各社のサイバーセキュリティオペレーションには差異が存在するものの、抽象化することにより共通のサイバーセキュリティオペレーションのための情報オントロジを構築することに我々は成功した。

以下、**2**にてサイバーセキュリティオントロジを、**3**でサイバーセキュリティ情報交換技術CYBEX（Cybersecurity Information Exchange Framework）の標準化活動を紹介し、**4**にてその有効性について議論し、**5**で結論および将来展望を述べていく。

2　サイバーセキュリティオントロジ

サイバーセキュリティ情報オントロジを構築するためのステップとして、オペレーションドメインを最初に定義し、そこに必要なロール、そして、それぞれのロールが扱う情報を定義する。

2.1　オペレーションドメイン

サイバー社会のセキュリティを担保するために必要なサイバーセキュリティオペレーションのドメインとして、我々はIncident Handling、IT Asset Management、そしてKnowledge Accumulationという、3つのドメインを定義する。

Incident Handlingドメイン：本ドメインは、インシデント、インシデントを構成するイベント、そしてインシデントによって生じる攻撃行為の3つを監視することにより、サイバー社会で生じる個々のインシデントを検知し、対処を行う。例えば、異常検知機器からの警告を通じて異常を検知し、各種ログを収集して証拠を構築する。また、ユーザ組織に対して、早期警戒、アドバイスを提供するのも本ドメインのオペレーションである。

IT Asset Managementドメイン：本ドメインは、各ユーザ組織内において、IT資産の設置、設定、管理と共に、それぞれに必要なサイバーセキュリティオペレーションを実施する。そして、各組織内でインシデントの予防と事後対策の両面のオペレーションを実施する。

Knowledge Accumulationドメイン：本ドメインは、サイバーセキュリティに関する情報の研究を実施し、その結果得られた知識を、別の機関で再利用できる形で蓄積する。その結果として、各組織間で広く共有すべき知をすべてここで集約することになる。

2.2　ロール

上記の各ドメインにおいてサイバーセキュリティオペレーションを実施するために必要なロールを定義する。Incident HandlingドメインにはResponse TeamとCoordinatorが、IT Asset ManagementドメインにはAdministratorとIT Infrastructure

Providerが、Knowledge Accumulationドメインには、Researcher、Product & Service Provider、Registrarが、それぞれロールとして存在する。なお、本ロール定義に当たり、我々は、果たすべき機能の観点から定義を実施した。従って、あるロールのインスタンスは、別のロールのインスタンスとなるケースも存在する点に留意されたい。

Administrator：本ロールは、各ユーザ組織のシステムを管理しており、組織内のIT資産に関する情報を所有している。各組織内でのIT管理者が本ロールの代表的インスタンスである。

IT Infrastructure Provider：本ロールは、各組織に対しITインフラを提供する。ITインフラとしては、ネットワーク接続性、データセンター、SaaSといったものが含まれる。インターネット接続サービス業者（Internet Service Provider, ISP）やアプリケーション・サービス・プロバイダ（Application Service Provider, ASP）が本役割を担っている。

Response Team：本ロールは、サイバー社会における不正アクセス、DDos攻撃やフィッシングといった各種インシデントを監視・分析し、インシデント情報として蓄積する。それらの情報に基づき、本ロールは、フィッシングサイトのアドレスをブラックリストに登録するなどの対策を実施する。セキュリティ管理サービスプロバイダ内のインシデント対策チームが、本ロールの代表的インスタンスである。

Coordinator：本ロールは、エンティティ間の調整を行い、既知のインシデントや犯罪情報に基づいた潜在的脅威に対処するコンピュータ緊急対応チーム／調整センター（CERT Coordination Center, CERT/CC）は本ロールの代表的インスタンスである。

Researcher：本ロールは、サイバーセキュリティ情報に関する研究を実施し、研究から得られた知識を抽出する。例えば、IBM社のX-forceやLAC社のサイバーリスク研究所（RRICS）など、MSSPにおけるサイバーセキュリティ研究チームは本ロールの代表的インスタンスである。

Product & Service Provider：本ロールは、識別子、バージョン、脆弱性、パッチとコンフィギュレーション情報などのソフトウェアやハードウェアなどの製品・サービスに関する情報を保持している。ソフトウェアハウス各社、個々のソフトウェア開発者などが本ロールの代表的インスタンスである。

Registrar：本ロールは、ResearcherとProduct & Service Providerによって提供されたサイバーセキュリティのナレッジを分類・整理し、別の組織が再利用できる形で提供する。アメリカ合衆国におけるNISTや日本におけるIPAなどが本ロールの代表的インスタンスである。

2.3 サイバーセキュリティ情報

上記のドメインとロールを元に、サイバーセキュリティオペレーションに求められる情報を定義する。図1に提案オントロジの概略図を示す。各ロールが提供する情報を考慮し、4つのデータベースと3つのナレッジベースを定義する。

Incidentデータベース：本データベースはインシデントに関する情報、すなわちイベント記録、攻撃記録、そしてインシデント記録を蓄積している。イベント記録はパケット、ファイルとそれらの処理に関するコンピュータイベント記録であり、通常はコンピュータログとして自動的に提供される。攻撃記録とは、実際のアタックシーケンスなどを記した攻撃情報であり、インシデントの解析が進むと共に、より詳細に記述されるべき記録である。インシデント記録とはコンピュータのステートや被害状況など、特定のインシデントに関する全般的な記録であり、複数のイベントレコードと推測・推定情報により生成され、また、攻撃情報も本記録に関連付けられる。この記録に基づき、管理者はインシデントの有害性ならびに対抗策の必要性を判断する。

Warningデータベース：本データベースはサイバーセキュリティにおける警告情報を蓄積しており、これはIncidentデータベースとCyber Riskナレッジベースに基づいて生成される。ユーザ組織は本情報に基づいて必要な対策を講じる。

User Resourceデータベース：本データベースは各ユーザ組織の資産管理に必要な情報を集積しており、ソフトウェア／ハードウェアリスト、その設定、リソースの使用状況、セキュリティポリシー、セキュリティレベル評価結果、そしてイントラネットトポロジといった情報を保持している。後述する加入しているクラウドサービスのリスト

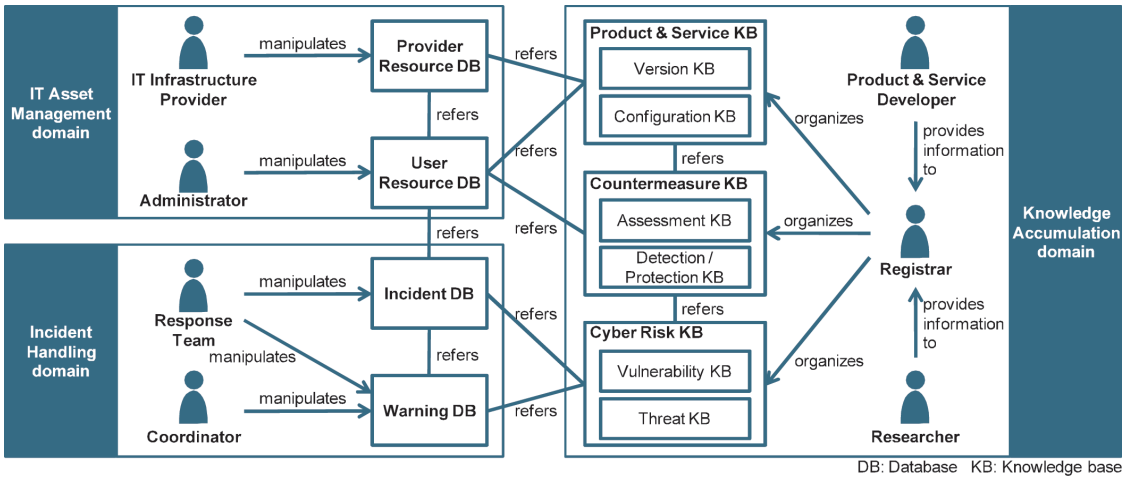

図 1 サイバーセキュリティオペレーション情報のオントロジ

やサービスの使用記録などの情報も含む。

Provider Resource データベース：本データベースは各組織が利用している組織外資産に関する情報を蓄積しており、外部ネットワーク情報と外部クラウドサービス情報がその主要な情報である。外部ネットワーク情報とは各組織が他の組織と接続されているネットワークに関する情報であり、組織間のネットワークトポロジ、経路情報、アクセス制御ポリシー、トラフィックステータスおよびセキュリティレベルといった情報が含まれる。外部クラウドサービス情報はクラウドサービス事業者自体、またその提供サービスに関する情報であり、サービス仕様、作業負荷情報、各サービスのセキュリティポリシー情報などを含む。

Cyber Risk ナレッジベース：本ナレッジベースはサイバーセキュリティリスクに関する情報を蓄積しており、Vulnerability ナレッジベースと Threat ナレッジベースを包含する。Vulnerability ナレッジベースは既知の脆弱性情報、すなわち脆弱性情報の命名法、分類そして目録を含むとともに設定ミスにより引き起こされた脆弱性などの情報を蓄積している。Threat ナレッジベースは既知のサイバーセキュリティ脅威に関する情報を蓄積しており、攻撃パターンや攻撃ツール、また傾向・統計情報などの攻撃情報と、ユーザの悪意の有無にかかわらず、不正な使い方により引き起こされる誤用の脅威に関する情報を蓄積している。

Countermeasure ナレッジベース：本ナレッジベースはサイバーセキュリティリスク対策に関する情報を蓄積しており、Assessment ナレッジベースおよび Detection/Protection ナレッジベースという 2 つのナレッジベースを持つ。前者は IT 資産に対するセキュリティレベル評価、すなわちルール情報、基準、またチェックリストなどが蓄積されており、後者はセキュリティ脅威の検知／保護に関する既知の知識、すなわち IDS/IPS シグネチャや、それに従った検知／保護ルールなどが蓄積されている。

Product & Service ナレッジベース：本ナレッジベースは商品とサービスに関するナレッジを蓄積しており、Version および Configuration という 2 つのナレッジベースを包含する。Version ナレッジベースは商品・サービスのバージョン毎の識別子の命名法やその目録を保持しており、特に商品に関しては、セキュリティパッチもここに含まれる。Configuration ナレッジベースは商品・サービスの設定情報を集める。設定情報には設定の命名法、分類、目録、そして利用時のガイドラインなどが含まれる。

尚、本オントロジの詳細は文献[1]を参考のこと。

3 サイバーセキュリティ情報交換の標準化活動

本オントロジにより、誰がどのような情報を持ち、また交換していくべきかということを議論す

る土台を構築した。この土台を構築するだけでは情報交換を促進することにはならず、この土台を用いて情報交換を実現するフレームワークを構築していく必要がある。その1つの取り組みとして、我々はITU-T勧告X.1500が定義するサイバーセキュリティ情報交換技術CYBEXの標準化活動にEditorとして従事している。以下、CYBEXの概要を紹介する。

CYBEXは、組織間での効率的な情報交換技術のITU-T勧告であり、具体的には、構造化した情報表現方法を規定し、その情報をセキュアに交換するためのフレームワークを規定している。これにより、サイバーセキュリティ情報の地域格差が解消され、また各組織にて実施されるサイバーセキュリティオペレーションの品質と効率が格段に向上することが期待される。

CYBEXは、情報表現ブロック、情報発見ブロック、情報クエリブロック、情報信頼性ブロック、そして情報伝送ブロックという、大きく5つの機能ブロックから構成され、それらの機能ブロックが連携することにより、組織間でのサイバーセキュリティ情報の交換を実現する（図2）。

情報表現ブロック：本ブロックでは、サイバーセキュリティ情報の表現・記述手法を規定している。既に、国際標準には至っていないものの、地域で利用されている有用な規格は多数存在する。表1は、その代表的なものであり、MITRE、FIRST、NIST、IETFなどが中心になって構築してきている。CYBEXでは、これらをはじめとする標準を取り入れるための枠組みを構築している。また、これらの規格の役割は、図3のように我々の提案オントロジでも、明確に示すことが可能である。

情報発見ブロック：本ブロックは上記の情報表現ブロックにて表現したサイバーセキュリティ情報について、その情報のありかを特定・発見する。そのための仕組みとして、集中管理する手法と分散管理する手法が存在し、CYBEXでは前者についてはOIDを、後者についてはRDFを用いた発見手法を定義している。尚、より具体的な内容は、X.1500ファミリー勧告の1つであるX.1570に記述されており、こちらも我々がEditorとして勧告制定に強くかかわっている。

情報クエリブロック：本ブロックではサイバーセキュリティ情報が構造化されて表現され、その情報を持つ組織を特定できた後、本ブロックにて、その組織に対し情報を要求、もしくは情報の追加・変更・削除を依頼するための本手法が定義されている。本手法は、SQLを拡張した手法で、SYIQLと呼ばれる方式であり、SQLによる操作と同様に、セキュアにクエリーをかけることができる。とはいえ、CYBEXは、SYIQLの利用を前提とはしていないため、この部分を他の方式で置き換えることも可能である。

情報信頼性ブロック：必要な情報をネットワーク上で伝送する前に、その情報、そして情報の発信元が信頼できるのかを確認するのが本ブロックであり、具体的には通信相手のアイデンティティを確認して信頼性を担保する。ある企業が、新たな企業と取引をする際、その新取引先の信頼性を担保するために、会社の謄本その他から、会社の身

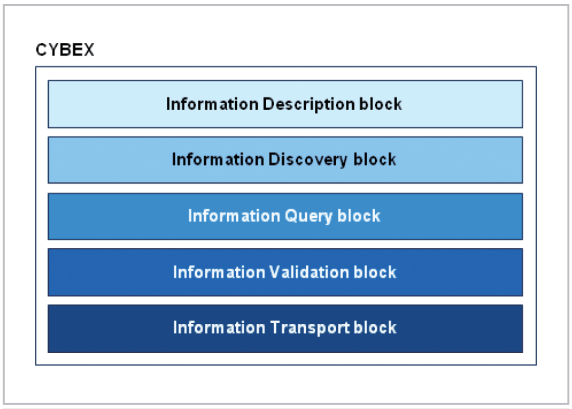

図2 CYBEXの機能ブロック

表1 サイバーセキュリティ情報の代表的な規格

規格名	内容
CVE	脆弱性情報の識別子の記述方法を規定
CAPEC	攻撃パターン情報の識別子の記述方法を規定
CCE	設定情報の表現方法を規定
CPE	ソフトウェアなどのIT資産の識別子の記述方法を規定
OVAL	機器の設定方法の記述方法を規定
CEE	コンピュータイベントの表現方法を規定
MAEC	マルウェアの表現方法を規定

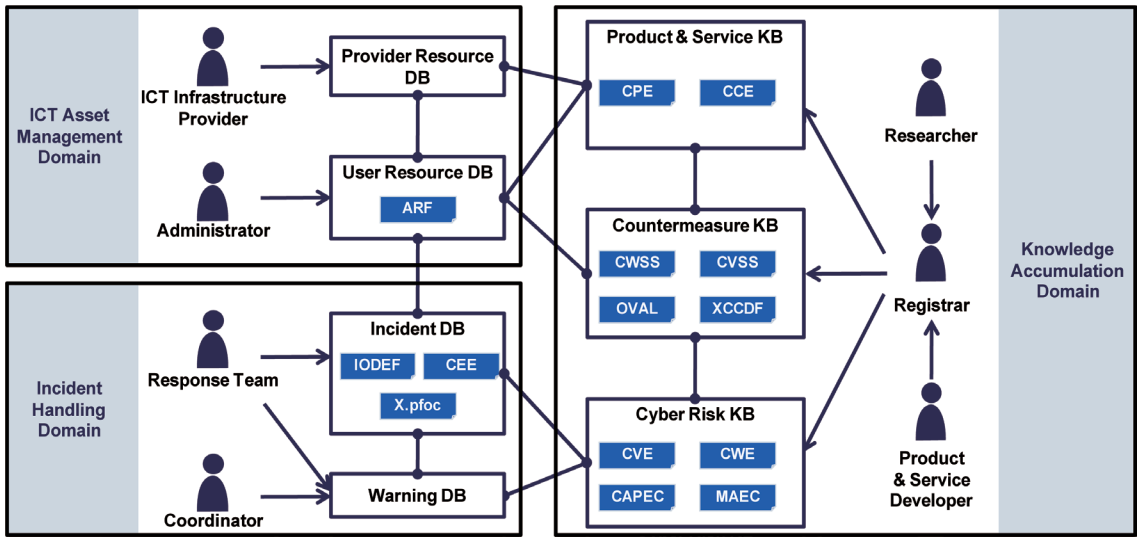

図3 サイバーセキュリティオントロジとCYBEXファミリー勧告

元情報を確認するのと同様に、サイバーセキュリティ情報を受け取る際に情報発信元の信頼性を確認するために、情報発信元の身元確認をするためのEVCERT技術などが利用される。

情報伝送ブロック：サイバーセキュリティ情報をネットワーク上で伝送するのが本ブロックであり、そのためのプロトコルに求められる機能を定義している。そのうちのBEEPを用いた伝送手法については、すでに我々が提案しており、概念実装も完了している[2]。

以上のように、CYBEXでは5つのブロックを連携することにより、情報を表現し、その情報を保持する組織を発見し、そこに対してクエリーを投げ、かつその組織の信頼性を担保した上で、情報交換を実現する。

尚、CYBEXの詳細については文献[3][4]を参考のこと。

4 有効性の評価および考察

ここでは、提案オントロジ、またそれに基づく標準化活動の有効性について議論する。

4.1 クラウド環境に対応するのに必要なサイバーセキュリティ情報

本オントロジがサイバーセキュリティ情報を議論するための土台として機能した例として、クラウド環境下にて求められるサイバーセキュリティ情報の洗い出し事例を紹介する。詳細な議論は文献[1]にあるが、結果として、表2のとおり、各データベースにて管理すべき情報を洗い出すことができる。その中にはクラウドになって新たに必要になったもの、またその重要性が一段と増加したものの双方が含まれている。そして、これに基づき、新たな情報表現フォーマットの規格の必要性も議論することができ、そのいくつかはCYBEXに将来的に組み入れることも検討している。

4.2 オペレーションの合理化

オントロジおよびCYBEXは、オペレーションの合理化を検討する土台にもなる。これらにより様々なサイバーセキュリティ情報が、機械可読な形で交換されるようになるため、実際にサイバーセキュリティオペレーションの現場を大きく合理化する可能性を持っている。以下に、合理化されるもののいくつかのユースケースを紹介する。

組織間での情報共有：従来は電話やEmail、また対面での会話、打ち合わせなどにより情報共有が行われており、悪意のあるユーザが世界中のコンピュータを相手に瞬時に攻撃をできるのに対し、大変非効率的であった。オントロジおよび

CYBEXによりサイバーセキュリティ情報が機械可読な形で交換されるようになると、ある情報を瞬時に世界中の無数のコンピュータへ共有することも理論的には可能となる。運用上の問題は存在するものの、組織間での情報共有の効率化を一歩進めることになると認識している。

情報の整理、蓄積の効率化：多くのサイバーセキュリティ情報が、機械可読な形で、また、分類やIDなどのメタ情報が付与された、整理された形で出てくるようになると、それらの情報を元に情報を整理することが可能となる。従来は、オペレータが自ら、人為的コミュニケーションにより獲得した情報を記録し、またそれにオペレータの判断でIDを付与し、分類をする必要があったが、これらの作業がすべて省略可能となるため、作業が効率的になるだけでなく、オペレータ間により生じるIDや分類の付与方法の違いなどの相違を考えるのも不要となる。

言語の壁を越えた情報共有：CYBEXで交換されるサイバーセキュリティ情報には、分類などのメタ情報が付与されるようになる。その分類方法自体もCWEなど、規格として確立していくことが期待されている。そして、その分類には番号やアルファベットなど、言語によらないIDが振られることになるため、自分に必要な情報を見つけ出す際には、その分類のみを理解していれば、たとえそれが外国語で記述されていたとしても、自分に必要なサイバーセキュリティ情報を絞り込んで探し出すことが可能となる。そして、その抽出された結果だけを翻訳することは可能であるし、また、その翻訳した情報を、別の機関に向けて再配信することも可能となる。従来のように、膨大な外国語のデータベースの中から、必要な情報を手探りで探すのは非現実的であったものの、絞り込んだ情報の翻訳であれば実現可能であるし、また、その翻訳をもし他の機関が既に実施しているのであれば、その翻訳済み情報を共有してもらうこともできるようになる。まだ、完全に言語の壁を越えたとは言えないものの、CYBEXにより、この問題を解決に向けて前進させていくことができると我々は考えている。

その他、組織間の情報共有を前提としたオペレーション設計、オペレーションの品質向上に費やす時間の増加、情報交換時の人為的なミスの減少、発展途上のオペレータの作業品質の向上、オペレータの意思決定を補助するシステムの可能性などについても我々の研究は貢献するが、詳細は文献[4]を参考にされたい。

4.3 発展途上国、世界、そして日本のサイバーセキュリティ

現在、発展途上国でのサイバーセキュリティの脅威が急上昇している。2010年4月に発行されたシマンテックのレポートによると、ブラジル、ポーランド、インド、ロシアなどの発展途上国での悪意のある活動が活発化しており、国別でトップ12にすべてランクインしている。特に、2009年には、ブラジルがドイツを抜いてトップ3にランクインし

表2 クラウド環境で重要になるサイバーセキュリティ情報群

KBs/DBs	必要なサイバーセキュリティ情報
User Resource DB	クラウドサービス加入情報、アイデンティティ情報、データアクセスコントロールポリシー、セキュリティレベル情報、リソース依存関係
Provider Resource DB	サービス利用者アイデンティティ、セキュリティ制御証明書、セキュリティレベル評価結果
Incident DB	データ来歴、データ配置履歴、データインシデント／イベント情報
Warning DB	データインシデントのサポート、危険にさらされているリソースの間接ユーザへの警告、適切な警告の表現フォーマット
Cyber Risk KB	脆弱性の影響範囲、設定の間違いにより生じる脆弱性、人的要因
Countermeasure KB	スコアリング手法、チェックリスト、ヒューリスティクス
Product & Service KB	サービス列挙とその分類、サービスの設定情報

ている。これらの国は、近年、急速にブロードバンドが普及してきているものの、セキュリティに対する意識や対策が後手に回っている国である。このような国が増えていくことにより、このような国のコンピュータがボットの温床になり、先進国のコンピュータに対する大きな脅威になりかねない。換言すれば、日本のサイバーセキュリティを担保するためには、世界のサイバーセキュリティを考える必要があり、そのためには発展途上国のサイバーセキュリティと向き合っていく必要があるというのが現在のサイバー社会である。

我々のオントロジやCYBEXが普及し、全世界的にも利用される様になれば、セキュリティについての情報が全く手に入らなかったこれらの発展途上国にも情報が共有されることになり、発展途上国で被害を受けるコンピュータの数を激減することが期待できる。逆にいえば、我々は、全世界規模でサイバーセキュリティ情報の格差を大幅に縮小し、セキュリティレベルの格差も大幅に縮小すべく、CYBEXを普及させていきたいと考えている。

5 まとめと将来展望

本稿では、組織の壁を越えたサイバーセキュリティ情報共有、協力を促進すべく、サイバーセキュリティ情報オントロジを提案し、また、CYBEXに関する国際標準化活動について紹介した。オントロジおよびCYBEXは情報共有を促進するためのツールであるが、このツールが活用されるためには、各国・各組織でサイバーセキュリティに対する意識が高まり、またCYBEXを活用してくれることが前提となる。如何にして、各国・各組織が我々のオントロジ、およびCYBEXを使うようになるのか、またそうするためにはどのようにするのかを我々は常に考えていく必要がある。

前述のとおり、CYBEXによりサイバーセキュリティオペレーションは変化することが予想される。それに先立ち、サイバーセキュリティオペレーションを見直し、新たなサイバーセキュリティオペレーションの絵姿を示すことが重要であり、それによりCYBEXを実装することのメリットを明示し、CYBEX導入への意欲を喚起したい。そうすることにより、CYBEXの普及を大幅に後押ししていきたいと考えている。

CYBEXは情報交換のみにフォーカスを絞っているものの、今後は、交換するための情報を如何に生成するか、また交換した情報を如何に有効利用するかについても検討していく必要がある。その一例として、サイバーセキュリティインシデントを追跡し、情報を収集するトレースバック技術[5]を検討してきているが、それ以外にも、情報の活用方法に関してもモデリング、標準化活動を通じて効率化を実現し、世界規模のサイバーセキュリティに貢献し、その結果としてついには日本のサイバーセキュリティに大きく貢献していきたいと考えている。

謝辞

常日頃から我々の研究活動をサポートいただいている北陸先端科学技術大学院大学の篠田陽一教授、株式会社ラックの武智洋氏、日本IBMの徳田敏文氏、情報通信研究機構の榎並和雅理事、高橋幸雄研究所長、松尾真一郎研究室長に深く感謝する。

参考文献

1 T. Takahashi, Y. Kadobayashi, and H. Fujiwara, “Onto-logical approach toward cybersecurity in cloud computing,” International Conference on Security of Information and Networks, ACM, Sep. 2010.

2 Cybex Information Exchange Tool (cybiet) — A Cybex Discovery and Cybex BEEP profile implementation, Sourceforge.net, http://cybiet.sourceforge.net/

3 A. Rutkowski, Y. Kadobayashi, I. Furey, D. Rajnovic, R. Martin, T. Takahashi, C. Schultz, G. Reid, G. Schudel, M. Hird, and S. Adegbite, “CYBEX — The Cybersecurity Information Exchange Framework (X.1500),” ACM SIG-COMM Computer Communication Review, ACM, Oct. 2010.

4 高橋健志，武智洋，門林雄基，“CYBEXで進化するセキュリティオペレーション，” アットマーク・アイティ，http://www.atmarkit.co.jp/fsecurity/index/index_cybex.html

5 T. Takahashi, H. Hazeyama, D. Miyamoto, and Y. Kadobayashi,“Taxonomical Approach to the Deployment of Traceback Mechanisms,”Baltic Conference on Future Internet Communications, IEEE, Feb. 2011.

（平成23年6月15日 採録）

高橋健志（たかはしたけし）
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研究員　博士（国際情報通信学）
サイバーセキュリティ

門林雄基（かどばやしゆうき）
ネットワークセキュリティ研究所
専攻研究員／
奈良先端科学技術大学院大学
情報科学研究科准教授　工学博士
IPトレースバック、サイバーセキュリティ