セキュリティ情報交換と標準化（CYBEX）

ー地球規模でのサイバーセキュリティ構築に向けてー

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

早稲田大学理工学研究科修了、2002 年 Tampere University of Technology にて研究員、2004 年同大学国際情報通信研究科にて研究員、2006 年（株）ローランド・ベルガー社にてコンサルタントを経て、2009 年より現職。情報通信プロトコル、サイバーセキュリティ、およびマルチメディア符号化に関する研究に従事。好きなことは新たな経験。経験の積み重ねこそが人生と信じ、現在はサイクリング、テニス、クッキング、そして中国語の学習に注力。博士（国際情報通信学）。

「組織・国境を越えた情報交換を促進することにより、サイバーセキュリティを向上させたい。その土台となる情報交換フレームワークについて、研究・標準化活動を展開しています。」

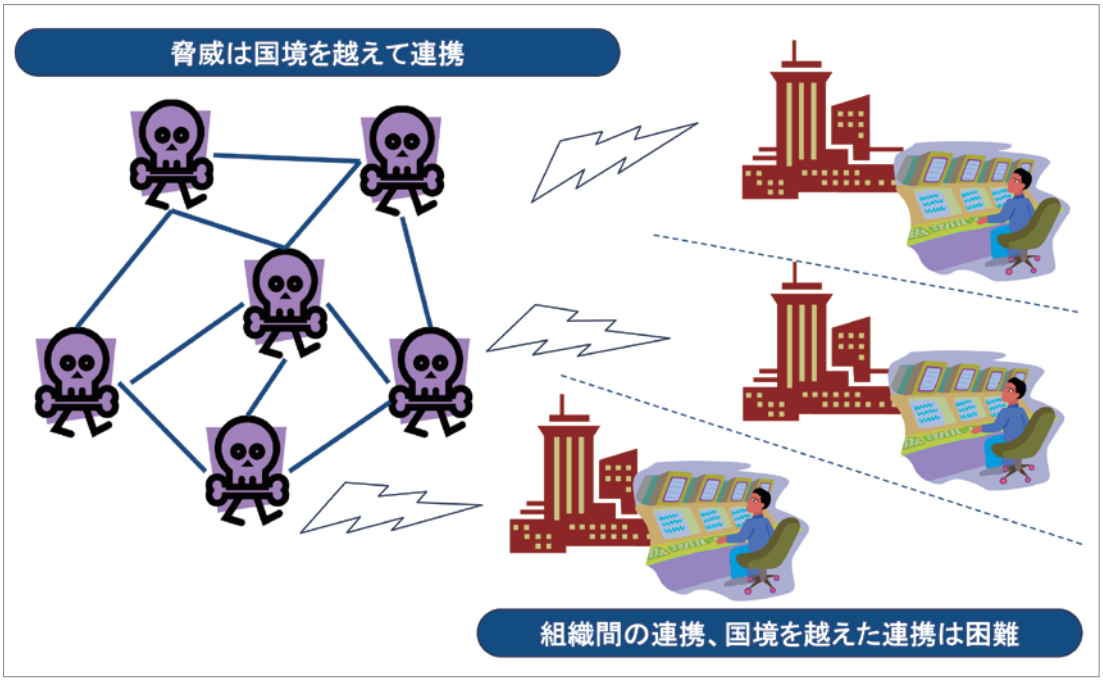

図1　脅威に劣後する対策

研究活動の背景

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ました。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ります。サイバー社会には国境はなく、脅威は国境を越えて襲ってきますが、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す(図 1)。すなわち、悪意のあるユーザーはリターンキーを押すだけで、互いに連携して世界中のコンピュータに対し攻撃が可能ですが、その対策は各国・各組織で独立して実施されています。各組織が連携するには、組織の壁を越えた情報交換が効率的に行われる必要がありますが、現時点では、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実施しているのが現状です。

このような状況が生じている主な要因の１つに、情報交換のフォーマットやフレームワークが各国・各組織で統一されていないことが挙げられます。各国・各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、サイバーセキュリティ情報の交換フォーマットやフレームワークがグローバルに共有される必要があります。

国際標準 CYBEX(X.1500)の構築

前述の情報共有フレームワークを構築すべく、我々は現在、国際標準化組織 ITU-T において CYBEX(Cybersecurity Information Exchange Techniques)という、組織間でのサイバーセキュリティ情報を交換するのに必要な技術群・フレームワークを定義しています。尚、CYBEX は組織間での情報交換に特化しているため、その情報の取得・活用については CYBEX の範囲外です(図 2)。

CYBEX では、この「サイバーセキュリティ情報の交換・共有」を実現するために、情報の表現手法、発見・交換手法、信頼性構築手法、

伝送手法のそれぞれを規定しています。特に、この情報の表現手法、発見・交換手法においては、後述する我々のオントロジの研究が大きく活かされています。CYBEX 自体は、ITU-T 勧告 X.1500 として勧告化されましたが、CYBEX を実現する具体的な技術については、今後も更なる発展が求められ、私も研究成果を積極的に ITU-T や IETF という国際標準化機関での活動に活かしています。

情報交換の基礎となるオントロジ

CYBEX に貢献する活動の 1 つとして、我々はサイバーセキュリティ情報のオントロジを構築しました（図 3）。オントロジとは、世界を概念レベルでモデリングしたものを指しますが、ここでは、サイバーセキュリティオペレーションのあるべき姿をモデル化したものを指し、サイバーセキュリティオペレーションの業務領域、そのそれぞれの領域の業務を実施するプレイヤー、および彼らが扱う情報群という、3 種類の情報を構造化して定義しています。すなわち、「どのオペレーションを」「誰が」「どの情報を利用して」実施するかをモデル化しています。本オントロジ構築に当たっては、日本だけでなく、米国、韓国のサイバーセキュリティ

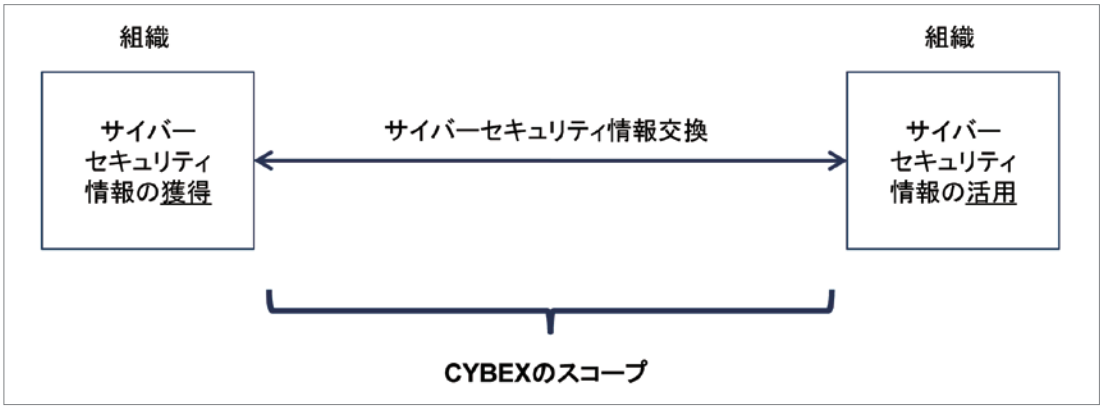

図2　CYBEXの範囲

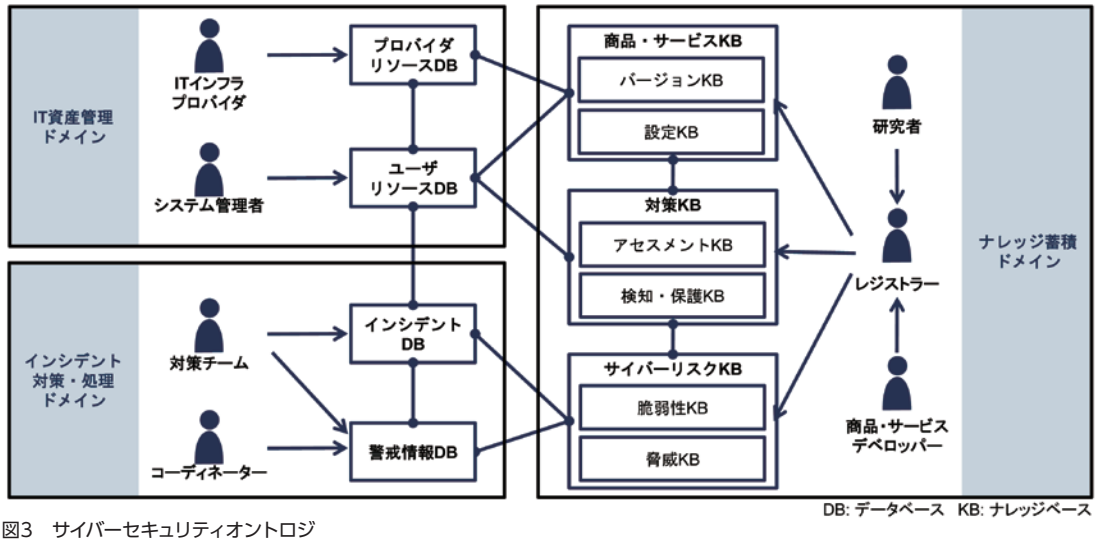

図3　サイバーセキュリティオントロジ

オペレーションの現状を鑑みており、サイバーセキュリティ先進国の知見が大いに活かされています。

本オントロジにより、サイバーセキュリティオペレーションの中でどのようなプレイヤーがどのような情報を必要とし、どのような情報交換がなされるべきかというものを体系立てて議論していくことが可能となり、CYBEX で交換されるべき情報を網羅的に議論するための土台となっています。これまでも様々な業界標準の動きはあったものの、部分最適な規格になる傾向がありました。CYBEX では、本オントロジに基づいて検討を進めることにより、サイバーセキュリティオペレーションを広く俯瞰しての規格制定を構築することを目指しています。

地球規模でのサイバーセキュリティ向上を目指して

このように、私はサイバーセキュリティ情報を「知」として共有するための手法・フレームワークを研究しております。ここにご紹介したもの以外にも、これらの世界中に存在するサイバーセキュリティ情報を、効果的に発見するための手法などの研究および開発も手掛けています。本オントロジに限らず、研究の成果を世の中に活きる形に昇華すべく、成果の国際標準化活動への展開、およびデモツールの構築・公開にも積極的に貢献しています。詳しくは、我々のホームページ(http://cybex.nict.go.jp/)をご参照ください。