ITU-T勧告X.1500：サイバーセキュリティ情報交換フレームワーク

独立行政法人 情報通信研究機構　ネットワークセキュリティ研究所　髙橋（たかはし）　健志（たけし）

あらまし

日増しに増大するサイバーセキュリティへの脅威に対処すべく、組織の壁を越えた情報交換が求められているが、そのような情報交換は現時点では大変非効率である。これは、サイバーセキュリティ情報交換の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。本問題に対処すべく、現在、ITU-TのStudy Group 17において、CYBEXというサイバーセキュリティ情報交換フレームワークを規定するITU勧告X.1500が制定された。本稿では、X.1500を中心としたサイバーセキュリティ情報交換技術の標準化活動の現状を紹介し、今後の方向性について議論する。

1．はじめに

サイバースペースの急速な発展に伴い、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。増大するサイバーセキュリティの脅威に対応するためには、組織間での効率的な情報共有が必要不可欠であるが、現在のそれは大変非効率であり、必要に応じてメール、電話、対面での打合せなど、時間と人手を要しているのが現状である。組織間での効率的なサイバーセキュリティ情報交換の重要性は既に様々な機関で認識されてきており、ETRI、FIRST、IETF、MITRE、NISTなど、各種標準化団体から様々な技術が各種規格として輩出され始めている。しかしながら、効率的に情報交換を実現するためには、これらの技術が一地域やコミュニティ規格の枠を超え、グローバルに使われる標準にならなければならない。そして、それらを組み合わせて効果的かつ効率的な情報交換を実現するフレームワークが求められている。

本問題に対処すべく制定されたのがITU-T勧告X.1500（2011年4月approval）[1]である。本勧告はサイバーセキュリティ情報交換技術のフレームワークCYBEX（Cybersecurity Information Exchange Frame-work）[2, 3]を定義しており、これにより、各種技術を組み合わせて情報交換を実現する。CYBEXでは、新たな技術を構築する代わりに、既存技術の中で既に現場にて利用されている、若しくは認知されているものを積極的に採用している。そうすることにより、CYBEXが実際のオペレーションの現場にて利用しやすい規格になるよう工夫している。いまだ規格・標準として構築されていない必要技術があった際には、単独若しくは他の機関と連携して新規勧告を構築する。そのため、X.1500は規格としての役割に加え、サイバーセキュリティ情報交換を実現するためのイニシアティブ的な役割も果たしている。筆者も本勧告にEditorとして関与してきたため、本勧告について、その背景、概要、期待される効果について、本稿にて共有したい。

以下、第2章にてX.1500で規定されるCYBEXを紹介し、第3章にてCYBEXがサイバーセキュリティにどのように貢献するかについて議論する。そして、第4章にて結論及び将来展望を述べていく。

2．CYBEXの概要

図1にCYBEXのスコープを示す。CYBEXは情報交換に焦点があり、情報の獲得、利用については、スコープ外である。CYBEXは情報を構造化し、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する。その交換を実現するには「情報表現」、「情報識別・発見・問い合わせ」、「アイデンティティ検証」、「交換」という四つの技術群が必要であるが、特に情報表現については、「弱点・脆弱性及び状態の記述」、「イベント・インシデント及びヒューリスティクスの記述」、そして「情報交換ポリシの記述」といった三つの技術群に分けられて定義されており、この詳細化された六つの技術群をそれぞれクラスタと呼んでいる。それらのクラスタ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。以下、各クラスタについて説明する。

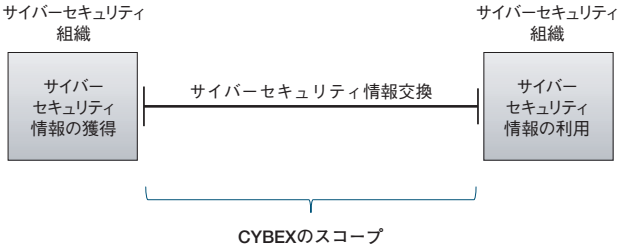

図1．CYBEXのスコープ

2.1　弱点、脆弱性及び状態の記述クラスタ

本クラスタを含む情報表現機能を提供する三つのクラスタは、サイバーセキュリティ情報をどのように記述するかを規定した技術群である。特に本クラスタは、サイバーセキュリティ情報のうち、弱点、脆弱性及び状態を記述する技術群である。具体的な個別技術についてはAppendix内にてリストアップされており、現時点では**表1**に示すものが存在する。

なお、X.1500自体はクラスタを定義するものの、各クラスタの各種個別技術については、上記のとおりAppendix内にてリストアップされ、リファレンスが提供される。その各種技術はX.1500外にて定義されている。こうすることにより、将来的に新たな技術が提供された際にはAppendixのみを更新することで、X.1500を常に最新の利用価値の高いものに維持することが可能となる。また、Appendix内にリストアップされている規格は、その有効性が認識され業界内で利用されている、もしくは利用されつつある規格であり、それら外部規格を直接参照するか、もしくは一度ITU-T勧告として取り込んだ後にその勧告を参照していることに留意されたい。

2.2　イベント、インシデント及びヒューリスティクスの記述クラスタ

本クラスタは、サイバーセキュリティ情報のうち、特にイベント、インシデント及びヒューリスティクスに関する情報を記述する技術群である。具体的な個別技術についてはAppendix内にてリストアップされており、現時点では**表2**に示すものが存在する。これらの情報は、攻撃に対する有効な対策を作るために利用される、若しくは、既存の弱点、脆弱性を削減するのに利用される。

2.3　情報交換ポリシの記述クラスタ

本クラスタは、交換されたサイバーセキュリティ情報の利活用のポリシ、条件について記述する技術群である。このポリシ・条件は、交換される特定の情報、若しくはある情報カテゴリ全般に適用されるものであり、これらの情報は関連するエンティティに単独で、若しくは情報と一緒に通知されることが望ましい。具体的な個別技術についてはAppendix内にてリストアップされるが、現時点では交換した情報の開示可能範囲を白、緑、黄、赤の4段階で定義するTLP（Traffic light protocol）のみが存在する。

2.4　識別、発見及び問い合わせクラスタ

本クラスタは、上記3つのクラスタにより構造化記述された情報をはじめ、各種サイバーセキュリティ情報をグローバルに一意に識別可能とし、問い合わせを行い、また識別子からサービス端点を発見可能とする技術群である。そのうちの一つとしてX.1570[4]が存在するが、これは、誰がどの情報を何のために使う、ということを情報カテゴリに焦点を当てて抽象化したモデル「サイバーセキュリティ情報オントロジ」（**図2**）[5]を定め、それに従って情報構造を定義し、情報を特定・発見する手法を規定している。その際には、識別方法

表１．弱点・脆弱性及び状態クラスタを構成する技術群

規格名	内容
CVE	脆弱性情報の識別子を規定
CVSS	脆弱性の深刻度をスコアリングする手法を規定
CWE	ソフトウェアの弱点タイプの識別子を規定
CWSS	ソフトウェアの弱点の深刻度をスコアリングする手法を規定
OVAL	機器の設定やステートなどの情報の記述言語を規定
XCCDF	セキュリティのチェックリストとその関連情報の記述言語を規定
CPE	ソフトウェアなどのIT資産の識別子の記述手法を規定
CCE	設定情報の表現手法を規定
ARF	IT資産のセキュリティレベルの評価結果の記述を構造化

表２．イベント、インシデント及びヒューリスティクスクラスタを構成する技術群

規格名	内容
CEE	コンピュータイベントの表現方法を規定
IODEF	CERT/CSIRT間でのコンピュータセキュリティ関連の事故情報を交換するための情報フォーマットを定義
CAPEC	攻撃パターン情報の識別子の記述方法を規定
MAEC	マルウェアの表現方法を規定

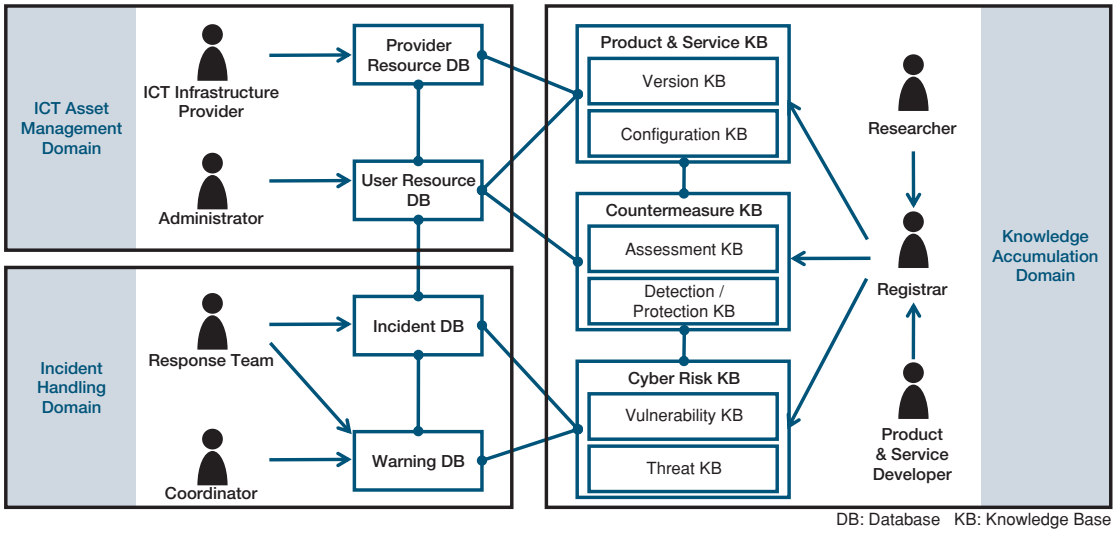

図2．サイバーセキュリティ情報オントロジ

としてOID及びRDFを利用した手法がそれぞれ規定されている。なお、本オントロジはサイバーセキュリティ情報交換を議論する土台としても重要なものであるという認識の下、X.1500のAppendixにも記載されている。

なお本クラスタの具体的な個別技術については、Appendix内にてリストアップされているが、上記のX.1570の他に、サイバーセキュリティ用のnamespace、そして関連するOIDの管理の要求条件について規定したX.1500.1も存在する。

2.5　アイデンティティ検証クラスタ

本クラスタは、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技術群である。具体的な個別技術はAppendix内にてリストアップされるが、電子商取引で用いられる電子証明書において、法人の登記情報などを検証可能にするEVCERTなど、現時点では**表3**に示すものが存在する。

2.6　伝送クラスタ

本クラスタは、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技術群であり、具体的な個別技術はAppendix内にてリストアップされるが、IODEF文書を組織間で交換する際のトランスポート層のメッセージ形式を定めたRIDや、コネクション志向で相互通信を実現するBEEPなど、現時点では**表4**に示すものが存在する。

3．CYBEXを用いたサイバーセキュリティ

CYBEXの利活用を促進することにより、サイバーセキュリティを大幅に向上できると筆者は考えている。そこで本章では、CYBEXの利活用促進に向けた取組、そして、それによりもたらされるサイバーセキュリティへの変化について議論する。

3.1　CYBEXの利活用促進に向けて

CYBEXはサイバーセキュリティ情報交換を実現・促進し、現場のサイバーセキュリティ業務を効率化することを目指し構築された技術である。CYBEX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おり、組織、言語の壁を越えた

表3．アイデンティティ検証クラスタを構成する技術群

規格名	内容
TPM	ハードウェアを利用し、強力なユーザ認証を実現する技術
TNC	ハードウェアを利用し、ネットワーク上での強力なアクセスコントロールを実現する技術
EAA	あるエンティティのアイデンティティとその関連情報の有効性管理のライフサイクルを規定する技術
EVCERT	電子書取引で用いられる電子証明書において、法人の登記情報などを検証可能にする
ETSI TS 102042	公開鍵証明書を発行する認証機関のオペレーションと管理に関するポリシの要求条件を定義

表４．伝送クラスタを構成する技術群

規格名	内容
RID	IODEF文書を組織間で交換するのに利用するメッセージを規定
Transport of RID messages	RIDメッセージを伝搬するトランスポート技術を規定
BEEP profile for CYBEX	コネクション志向、非同期、相互通信を実現するBEEPについて、そのCYBEXプロファイルを規定
SOAP for CYBEX	分散環境にて情報交換を実現するXMLベースのプロトコルSOAPについて、CYBEXへの活用方法を規定

情報共有、情報の整理・蓄積の効率化、マニュアルオペレーションが生じる人的作業ミス解消などを積極的に推進することが可能となる。

しかしながら、X.1500そのものが、サイバーセキュリティ情報交換の促進や現場業務の合理化に直結するわけではない。本勧告は広く利用されることにより、初めてその真価を発揮する。X.1500には様々な技術が取り入れられているため、実際にサイバーセキュリティ情報交換を実施する際には、X.1500にある技術を組み合わせて活用する必要があり、またそれを補助するツールが開発され、多くの人に積極的に利用してもらう必要がある。

既に、幾つかのツールが実在する。SCAP（Security Content Automation Protocol）は、XCCDF、OVAL、CPE、CCE、CVE、CVSSを組み合わせ、脆弱性情報管理の自動化を推進するものである。米国NIST（National Institute of Standard and Technology）が推進してきたものであり、NVD（National Vulnerability Database）では、本SCAPに基づく脆弱性情報提供を実施している。同様のものに日本のJVN（Japan Vulnerability Note）Security Content Automation Frameworkがあるが、これはIPA及びJPCERT/CCが推進しているものであり、米国のSCAPに準拠して脆弱性情報管理の自動化を推進する。なお、日本の製品情報、日本で発見された脆弱性情報なども含んでいる。上記二つのツールについては、X.1500内Appendixにも記載されている。これらの活動はX.1500制定に先行して行われているため、X.1500の実装・ツール例、という表現は不正確かもしれないが、そもそもX.1500自体が、サイバーセキュリティ情報交換を実現したいという現場の要望を背景に開始されたものであるため、幾つかの実用例が先行しているのは、当然とも言える。

CYBEXは今後更なる発展が望まれる技術群であるが、その発展には、実装・実運用をかんがみることが必須であり、そのような動きには、今後も期待したい。また、技術の問題と並行し、組織の壁を越えて情報を交換する際の法制面での準備、そして、組織が情報を交換するモチベーションを生じるメカニズムの構築など、非技術面でも課題が存在する。これらの問題を検討している団体の一つに、日本セキュリティオペレーション事業者協議会（ISOG-J）が存在するが、CYBEXが発展していく際には、このような活動とも同期していくことが必要不可欠である。

3.2　グローバルサイバーセキュリティに向けて

現在、サイバーセキュリティに十分な投資ができていない国々（以下、発展途上国。尚、本稿では、これと対をなす概念として先進国という言葉を利用）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、悪意のある活動が活発化している地域には、ブラジル、ポーランド、インド、ロシアなどの発展途上国があげられており、国別でトップ12に全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。

CYBEXが普及し、全世界的にも利用されるようになれば、サイバーセキュリティ情報が不足してい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。その結果、発展途上国のPC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。筆者は、全世界規模でサイバーセキュリティ情報、そしてセキュリティレベルの格差を縮小すべく、CYBEXを普及させていきたいと考えている。

現在、サイバーセキュリティ情報交換に関連する様々な技術が検討されているが、筆者もその技術発展に貢献したいと考えている。既に、X.1570で規定されるネットワーク上での情報特定・発見技術の機能深堀、発展、実装や、各種サイ

バーセキュリティ情報を組み合わせて伝送するための情報構造化技術[6]に着手している。また、CYBEXの先には、交換された情報を実際のサイバーセキュリティオペレーションに活かすことが考えられるが、それには様々なオペレーションにIDが付与される必要があり、そのための土台となるモデル構築技術[7]にも着手している。CYBEXを起点とし、サイバーセキュリティ情報が組織の壁を越えて共有される世界が到来するよう、今後も技術研究開発・標準化活動に注力したい。

4. まとめと将来展望

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CYBEXを規定するX.1500を中心に、組織の壁を越えたサイバーセキュリティ情報交換を促進する国際標準化活動について紹介した。CYBEXは情報共有を促進するためのツールであるが、それによりサイバーセキュリティオペレーションの合理化、及びグローバルサイバーセキュリティの飛躍的向上を実現する可能性を秘めている。しかしながら、CYBEXが真価を発揮するためには、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、CYBEXを活用してくれることが前提となる。筆者は今後、世界規模でCYBEXの利活用を促進すべく、様々なステークホルダとの対話を継続し、必要なアクションを積極的に講じていこうと考えている。

また、CYBEXはイニシアティブである。現在、CYBEXを契機に様々な場所でサイバーセキュリティ情報交換実現に向けた検討が進んできており、筆者はこの潮流を大切にしたい。筆者自身も研究者の立場から積極的に技術提案をし、またその国際標準化に尽力していきたい。サイバーセキュリティには国境はないため、より多くのステークホルダと対話をしつつ技術を構築できるITU-Tの国際標準化活動の場は非常に貴重なものであると思っている。

謝辞

サイバーセキュリティ情報交換に関する国際標準化活動、及び研究活動に多大なる御支援・御協力をいただいている奈良先端科学技術大学院大学の門林雄基准教授に心より感謝する。また、常日頃からこれらの活動を御支援いただいているKDDIの中尾康二氏、KDDI研究所の三宅優氏、日本IBMの徳田敏文氏、日立製作所の寺田真敏氏、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、永沼美保氏、情報通信研究機構の榎並和雅氏、高橋幸雄氏、松尾真一郎氏に深く感謝する。

参考文献

1. “Overview of cybersecurity information exchange”, Recommendation ITU-T X.1500, 2011年
2. 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 SIGCOMM Computer Communication Review, 2010年
3. 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
4. “Discovery mechanisms in the exchange of cybersecurity information”, Recommendation ITU-T X.1570, 2011年
5. T. Takahashi, Y. Kadobayashi, and H. Fujiwara, “Ontological approach toward cybersecurity in cloud computing”, International Conference on Security of Information and Networks, ACM, 2010年
6. T. Takahashi, K. Landfield, T. Millar, Y. Kadobayashi, “IODEF-extension to support structured cybersecurity information,” IETF Internet Draft, draft-ietf-mile-sci-01. txt, 2011年
7. T. Takahashi, Y. Kadobayashi, K. Nakao, “Toward Global Cybersecurity Collaboration: Cybersecurity Operation Activity Model,” ITU-T Kaleidoscope, 2011年