第 XI 部

サイバーセキュリティ情報交換技法

第 11 部
サイバーセキュリティ情報交換技法

第 1 章　はじめに

インターネットの普及によって情報通信機器が増え、また各種オンラインサービスが普及したことにより、サイバースペースが拡大を続けている。本報告では、情報通信機器と人間のインタラクションによって構成されるサイバースペースでのセキュリティ、つまりサイバーセキュリティを取り扱う。

サイバースペースは開放型の空間なので、価値観の対立や知識格差、経済格差など様々な問題を孕んだインタラクションがつねに発生しうる。したがってサイバースペースの拡大にともない、サイバーセキュリティ能力を拡大することが必要となる。そのような開放的なサイバースペースの在り方については批判もあろうが、いっぽうで知識格差、経済格差や価値観の対立を超えたコミュニケーション基盤は近年のグローバルな発展の原動力となっており、この新しい空間を安全に使いこなす能力は大きな競争力の源泉である。

サイバーセキュリティ能力を拡大する方法は、大きく分けて 2 つ考えられる。まず啓蒙による個人の能力向上や、サイバーセキュリティ教育によって専門家を養成する方法である。つぎにイノベーションによって能力向上をはかる方法が考えられる。

能力向上のための一つの取り組みとして、Traceback ワーキンググループでは 2000 年からトレース情報の交換プロトコルやスキーマ等に取り組んできた。CYBEX WG では、これをより一般化した取り組みとして、サイバーセキュリティ情報の交換プロトコルやスキーマ等に取り組んでおり、その成果の一部を ITU-T（国際電気通信連合電気通信標準化部門）での標準化活動に反映している。サイバーセキュリティの現場では、技術的な監視や分析もさることながら、関係機関や隣接業務との情報交換がかなり重要であり、これをグローバルかつ高信頼・迅速におこなうことがますます重要になるであろうという課題認識に基づいて技術開発と標準化に取り組んでいる。

本報告ではそのような高信頼かつ迅速なサイバーセキュリティ情報交換を実現する CYBEX（Cybersecurity Information Exchange Techniques）について、背景と標準化の取り組みを中心に述べる。

第 2 章　サイバーセキュリティの課題

サイバースペースは拡大を続けており、生来的にグローバルであり、タイムゾーンもない。そのような空間においてセキュリティを向上させるためには、まず、以下に挙げるような二種類の課題を解決する必要がある。

1. 情報爆発

   サイバースペースを構成する計算機、ネットワーク機器、ソフトウェア資産などは際限なく増えつつある。これらの機器やソフトウェアは導入された瞬間から劣化がはじまり、半年あるいは 1 年たった頃には相当数のバグや脆弱性が発見されることも多い。それらは脆弱性情報として提供される。また脆弱性を修正する方法や、当面の回避方法として脆弱性が発現しないように運用する方法なども情報として提供されることがある。これらの情報は当該ハードウェアあるいはソフトウェアがサイバースペースから消えてなくなるまで必要とされる。

   言い換えればサイバースペースの安全情報は生来的に情報爆発であるということである。

2. グローバル協調へむけての課題

   サイバースペースでは、機器同士はインターネットプロトコルによってグローバルかつ瞬時に通信がおこなわれるが、ひとたび問題が起きたとき、その両端にいる人間同士が共通の言語を持たず、会話がまったく成立しないこともある。また時差もあるため即時的対応が期待できないこともある。

   かりに言語の違いや時差の問題がなかったとしても、信頼できるコンタクト先をどのように見

つければよいのかという問題もある。

サイバーセキュリティ運用の現場では、これらの課題は認識されてはいるものの、個々の脅威への対処が優先される。このギャップを埋める技術開発と標準化が求められている。

第 3 章　サイバーセキュリティ運用における課題解決にむけて

サイバーセキュリティについて語るとき、ウイルス、ボットネット、フィッシングなど個別脅威のキーワードを挙げて問題認識を共有しようとする試みがすくなくない。また技術開発においても、ウィルス対策、フィッシング対策など個別脅威に対しての近視眼的な技術開発がおおい。標準化においてもおなじような構造がみられ、フィッシング対策勧告案、ボットネット対策勧告案など個別の脅威ごとに勧告案が持ち込まれることとなる。

実際のところ、急速に移り変わる個別の脅威に対して、対策技術を標準化することの実効性は疑わしい。標準化は少なくとも 1 年かかるのに対し、脅威は数ヶ月あるいは数週間の単位で遷移するためである。また対策方式が明文化された場合、それを迂回することはより容易なものとなってしまう。

CYBEX WG では、標準化の対象は個別の対策システムではなく、対策や運用の現場における情報交換であるべきだと考える。サイバーセキュリティ運用の現場では、おなじ言語であっても、会社やコミュニティが違えば同じ言葉が異なる意味で用いられている、といった状況がある。またセキュリティ機器はネットワーク機器とは異なり、相互接続性が低く、複数のセキュリティ機器を組み合わせて用いる際にオペレータが介在する必要がある、という問題もある。

このような問題意識をもとに、ITU-T スタディグループ 17 課題 4 を中心に CYBEX 審議グループを作成し、グローバルな国際協調のもとで議論をすすめた結果、サイバーセキュリティ情報の交換技法について体系的な知見が得られ、またそれを具現化する標準化体系を作り出すことができた。なお、このようなアプローチが可能となったのは課題 4 ラポータの Tony Rutkowski 氏の国際的かつ標準化団体をまたがる豊富な経験と人脈によるところが大きい。

体系化にあたっては、既存の標準を最大限に利用すること、および様々な標準化団体で独立して行われている活動を見つけ出し、リエゾン文書の交換などを通してつながりを作ることを念頭に活動をおこなった。具体的には、APWG（Anti-Phishing Working Group）、CCDB（Common Criteria Development Board）、ENISA（European Network and Information Security Agency）、ETSI TISPAN、FIRST（Forum of Incident Response and Security Teams）、IEEE ICSG（Industry Connections Security Group）、IETF（Internet Engineering Task Force）、ISO/IEC JTC1 SC7、ISO/IEC JTC1 SC27、ITU-D SG1 Q.22（ITU Development Sector Study Group 1 Question 22）、ITU-T SG13 Q.16、OMA（Open Mobile Alliance）、3GPP（3rd Generation Partnership Project）といった数多くの標準化団体およびサイバーセキュリティ関連団体にリエゾン文書を送り、CYBEX 勧告案についてコメントを求めると同時に、サイバーセキュリティ情報の交換技法に役立つ標準化活動について最新情報を求めた。CYBEX 審議グループでは、勧告案の編集およびレビューのため、隔週の電話会議に加え、年 2 回の公式会合のほか、18 ヶ月の間に計 4 回の中間会合を開催するなど、比較的速いペースで作業が行われた。

この結果、2010 年 12 月の ITU-T スタディグループ 17 会合において、ITU-T 勧告 X.1500（CYBEX）としてサイバーセキュリティ情報の交換技法をまとめることができた。

第 4 章　CYBEX

CYBEX では、サイバーセキュリティ情報の交換を表 4.1 のように 5 つの機能に分解し、それぞれの機能を提供する既存の標準を参照している。なお既存の標準がないものについては CYBEX 審議グループにおいて勧告案を作成し、ギャップを埋める作業をおこなっている。

CYBEX では、これらの 5 つの機能を実現する標準および勧告案を 6 つのクラスタに分けて参照している。クラスタの分類は便宜的なものである。異なる視点からの分類も可能であろうが、CYBEX 審議グ

表 4.1. サイバーセキュリティ情報交換を構成する 5 つの機能

機能	概要
サイバーセキュリティ情報の構造化	機械可読なかたちでサイバーセキュリティ情報を構造化し、関係機関や隣接業務に連絡しやすいようにする。
サイバーセキュリティ情報の識別と発見	ICT 資産や脆弱性、攻撃種別などのサイバーセキュリティ情報に識別子を付与する。また識別子からサービス・エンドポイントおよびサービス種別を発見できるようにする。
サイバーセキュリティ情報の共有条件の合意	情報共有が許される範囲を明示することで、情報共有における曖昧さを解消し、情報共有を促進する。
サイバーセキュリティ情報の要求と応答	識別子や指定した条件にもとづいてサイバーセキュリティ情報を検索する機能を提供する。
サイバーセキュリティ情報の検証	サイバーセキュリティ情報に誤りがないよう検証をおこない、情報の信頼性を向上させる。

ループにおける議論を経て現在の形に落ち着いている。クラスタの名称および概要は以下の通りである。

1. 弱点、脆弱性および状態
   このクラスタでは、弱点および脆弱性情報の交換、および、システムやアプリケーションの状態を評価する勧告案を参照している。それらは、CVE（Common Vulnerabilities and Exposures）、CVSS（Common Vulnerability Scoring System）、CWE（Common Weakness Enumeration）、CWSS（Common Weakness Scoring System）、OVAL（Open Vulnerability and Assessment Language）、XCCDF（eXtensible Configuration Checklist Description Format）、CPE（Common Platform Enumeration）、CCE（Common Configuration Enumeration）、ARF（Asset Reporting Format）である。例えば CVE はソフトウェアの脆弱性に番号を付与し管理するための勧告である。
2. イベント、インシデントおよびヒューリスティクス
   このクラスタでは、インシデント対策チーム間のイベント、インシデントおよびヒューリスティクスに関する情報交換をサポートする勧告案を参照している。それらは、CEE（Common Event Expression）、IODEF（Incident Object Description Exchange Format）、IODEF Phishing Extension、CAPEC（Common Attack Pattern Enumeration and Classification）、MAEC（Malware Attribute Enumeration and Characterization）である。例えば MAEC はマルウェアの行動や振る舞いを記述するためのスキーマを規定した勧告案である。
3. 情報交換ポリシ
   このクラスタでは、サイバーセキュリティ情報交換にまつわる諸条件を相手方に伝えるための勧告案を参照している。現時点では TLP（Traffic Light Protocol）のみが参照されている。TLP は Red、Amber、Green、White の 4 種の情報共有レベルで機密情報の取り扱い要件を明示するものである。
4. 識別、発見および問い合わせ
   このクラスタでは、サイバーセキュリティ関連組織、情報交換ポリシ、脆弱性情報などをグローバルに一意に識別可能とし、問い合わせをおこない、また識別子からサービス端点を発見可能とするための勧告案を参照している。それらは、Cybersecurity OID（Object Identifier）、Cybersecurity Information Query Language、CYBEX Discovery である。現在のところ、サイバーセキュリティ情報交換のための OID として joint-iso-itu-t(2) cybersecurity(48) を用いることが検討されている。
5. アイデンティティの検証
   このクラスタでは、アイデンティティの信頼度や、伝える情報の信頼度を検証するための勧告案を参照している。それらは、TPM（Trusted Platform Modules）、TNC（Trusted Network Connect）、EAA（Entity Authentication Assurance）、EVcert（Extended Validation Certificate framework）、ETSI TS102042（Policy requirements

for certification authorities issuing public key certificates）である。例えば EVcert（ITU-T X.1261）は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とする勧告である。

6. 交換プロトコル
   このクラスタでは、サイバーセキュリティ情報を交換するプロトコルを参照している。それらは Cybex BEEP（Blocks Extensible Exchange Protocol）プロファイル、SOAP（Simple Object Access Protocol）、RID（RFC 6046, Transport of Real-time Inter-network Defense Messages）である。

なお、これらのクラスタを構成する勧告は ITU-T 勧告 X.1500 シリーズの一部となることが決まっており、CVE は X.1520 として、また CVSS は X.1521 として ITU-T 勧告化された。これらも 2010 年 12 月の ITU-T スタディグループ 17 会合において確定したものである。今後も、速いペースで X.1500 シリーズの充実をはかっていく予定である。

第 5 章　CYBEX による運用効率化へむけて

CYBEX から参照しているそれぞれの標準や勧告案は、単体ではサイバーセキュリティ情報交換のすべての側面をカバーするものではない。前章でみてきたように、CYBEX は識別子、構造化、検証、交換などのそれぞれの機能を提供するモジュール性の高い標準と勧告案から構成されており、それらを組み合わせてサイバーセキュリティ情報交換を実現することが必要となる。

このため CYBEX の「実装例」として、既存の日米の取り組みを付録（Appendix）として紹介している。「実装例」と括弧書きにしたのは、これらの取り組みは CYBEX の標準化活動に先行して行われており、現時点では、6 つのクラスタの一部の実装例にとどまるためである。

1. **SCAP (Security Content Automation Protocol)**
   米国 NIST（National Institute of Standards and Technology）が推進する SCAP は、XCCDF、OVAL、CPE、CCE、CVE、CVSS からなる。XCCDF、OVAL はシステムの状態や脆弱性の有無を評価するための記述言語である。IT 資産およびその構成を記述するための語彙を CPE、CCE が与え、脆弱性の記述およびスコアリングをするための語彙や規準を CVE、CVSS が与えている [112]。
2. **JVN (Japan Vulnerability Notes) Security Content Automation Framework**
   日本の IPA および JPCERT/CC が推進する JVN は、米国の SCAP 相当の機能に加え、日本の製品情報、日本で発見された脆弱性情報などを含む [172]。

X.1500 勧告では、これらの参考情報をもとに、各国・各組織におけるサイバーセキュリティ運用が効率化されることを期待している。特にこれらの実装例は発展途上国における同様の取り組みを期待したものである。発展途上国におけるサイバーセキュリティ能力向上は ITU-T スタディグループ 17 における最重要課題のひとつであり、CYBEX は発展途上国におけるサイバーセキュリティ能力向上のための重要な技術標準となりうると我々は考えている。

これらの先行する実装例のほかに、CYBEX にもとづくより高機能な実装も考えられる。クラスタを構成する勧告をどのように組み合わせ、サイバーセキュリティ情報交換を行うのが良いのか、という点については今後も検討の余地がある。

第 6 章　グローバル協調へむけて

サイバーセキュリティ運用の現場では、言葉の壁、および、語彙が確立されていないという 2 つの問題により、組織を超えた協調が難しい。

言葉の壁については、我々は ITU-T が本来持つ機能をうまく使ってある程度の解決をはかれるのではないかと考えている。勧告というと英語だけで書かれていると思われがちだが、ITU-T の公式言語は 6 つあり、TAP（Traditional Approval Process）という承認プロセスを経て正式な勧告となったものについては、フランス語、スペイン語、アラビア語、ロシア語、中国語にも翻訳される。これにより中南米、

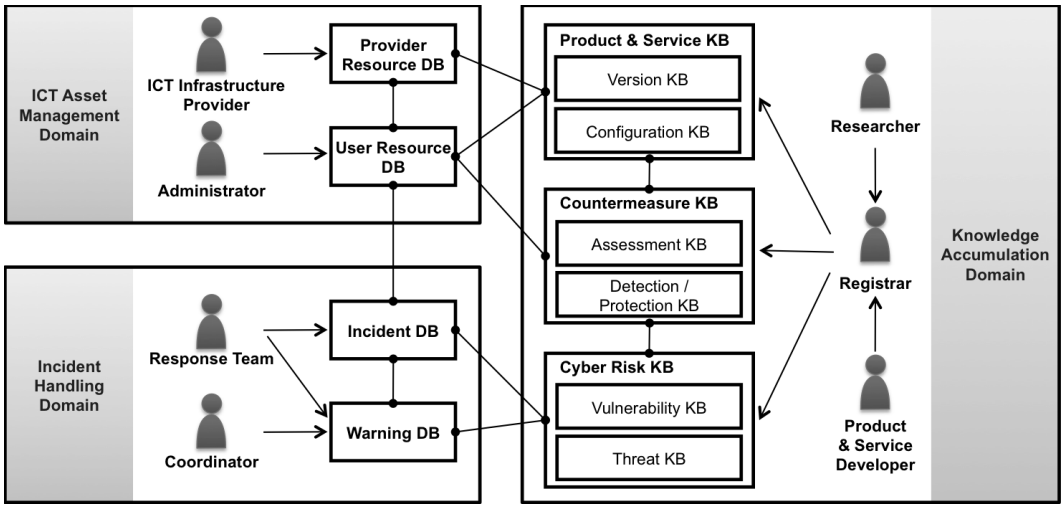

図 6.1. サイバーセキュリティ運用のオントロジ

アフリカ、東欧などに位置する発展途上国にも浸透しやすい勧告を作ることができる。

このほか、さきにのべた情報の構造化や識別番号の付与も、言葉の壁を超える助けとなる。情報を構造化することで、自然言語で事象を表現する必要を極力なくし、複雑な事象を正確に相手に伝えることができる。

語彙の確立については、「誰が」「何を」「どうする」という 3 種の語彙に分けて考えることができる。我々は、これらをそれぞれエンティティモデル、インフォメーションモデル、アクティビティモデルとしてモデル化することができると考えた。これらのモデリング作業は NICT（情報通信研究機構）において複数のセキュリティサービス事業者を対象として行った。その最初の結果として、ごく抽象的なエンティティモデルとインフォメーションモデルを抽出することができ、これを X.1500 付録に参考オントロジとして記した。抽象化の程度については様々な意見があり、実際には、より詳細なオントロジを求める声もある。しかし X.1500 勧告の確定段階でサイバーセキュリティ運用を包括的に扱ったオントロジは他になかったため、NICT オントロジのみが記されている。我々は複数の詳細なオントロジが乱立するより、ネットワーク業界における OSI 参照モデルにみられるように、標準の概念モデルをごく抽象的なレベルで決めたほうがよいと考えている。

図 6.1 にサイバーセキュリティ運用をモデル化した NICT オントロジを示す。図中の人形をしたものがセキュリティサービス事業者やセキュリティ対策組織などを表すエンティティであり、それらは大きく三つの業務ドメインに位置する。それらは、ICT 資産管理、インシデント対応、知識集約である。それぞれのエンティティは、図の中央に示すデータベースおよびナレッジベース群（ユーザ組織の有する ICT 資産に関するデータベース、インシデント対応のためのデータベース、対策のためのナレッジベースなど）にアクセスする。オントロジのより詳細な説明は紙面の都合上、X.1500 勧告または既出の論文 [168, 213] を参照されたい。なお、それぞれのサイバーセキュリティ・エンティティがどのような活動を行っているか、というアクティビティモデルについては本稿執筆時点において NICT を中心としてモデル化を行っているところである。

実際には、サイバーセキュリティ運用の現場では、オントロジで定義されるような抽象概念レベルの語彙だけではなく、個々の脆弱性や、脆弱性を発現させるパターンといった具体的な語彙が求められることになる。これらの語彙については CVE ID、CWE ID などの一意な識別子を付与し、各言語圏において説明文やアノテーションを付与することで意思疎通が容易になると考えられる。

第 7 章　おわりに

本報告では高信頼かつ迅速なサイバーセキュリティ情報交換を実現する CYBEX について、背景と標準

化の取り組みを中心に述べた。機器同士の通信がグローバルかつ瞬時におこなわれる今日において、ひとたび問題が起きたとき、その両端にいる人間同士が共通の言語を持たず、会話がまったく成立しないとしたら、どうして問題解決ができようか。CYBEX WG では、サイバーセキュリティの文脈において、人間のインターオペラビリティ能力向上のためのテクノロジに取り組んでいく予定である。