2014年度 CYBEX Working Group 活動報告

高橋 健志 (takeshi_takahashi@nict.go.jp)　宮本 大輔 (daisu-mi@nc.u-tokyo.ac.jp)
門林 雄基 (youki-k@is.aist-nara.ac.jp)　櫨山 寛章 (hiroa-ha@is.naist.jp)

2014年12月15日

目 次

1 CYBEX WG 2014年度の活動

サイバーセキュリティ対策には，組織の壁を越えた情報共有が求められるが，そのような情報共有は電話やEメール，打ち合わせなどの人手でのオペレーションによりなされているのが現状であり，大変非効率である．本問題に対応するため，IODEF (Incident Object Description Exchange Format) が提案されている．これは，インシデント情報を記述するXMLスキーマを定義し，それによりコンピュータ間にて情報交換を実現する．今年度，我々は，このIODEF技術を拡充し，組織間の情報連携を加速するための技術開発・標準化活動に従事してきた．

今年度の主な活動内容は以下の通りである．

- IODEF-SCIのRFC化
- Reference Ontology for Cybersecurity Operaitonal Informationの Journal化
- MILE Implementation Reportのドラフト執筆
- NECOMAtterシステムの試作

2 IODEF-SCIのRFC化

IODEFは情報構造を規定しているものの，詳細な情報を送る際には未だ自由記述形式のフィールドに頼らざるを得ないのが現状である．また，より詳細なデータ構造を定義しようにも，最適なスキーマはオペレーションの種類，時代によって異なるため，単一の詳細スキーマを定義することは非現実的である．本問題に対応すべく，我々はIODEFを拡張し，IODEF文書内に識別子やXMLなど，各種構造化情報を埋め込むIODEF-SCI技術を提案してきた．これにより，構造化されたセキュリティ情報のID，XML，もしくはURLをIODEFに埋め込んで情報交換することが可能となる．詳細は，参考文献を参考のこと．

尚，本活動は昨年度からの継続活動であり，RFCという形に仕上げたことが本年度の成果である．

詳細はwide-paper-cybex-rfc7203.txtを参照のこと．

3 Reference Ontology for Cybersecurity Operaitonal Information の Journal 化

我々は，情報交換を行う際には，誰が何のために度の情報を交換するかを定義することが重要と考え，セキュリティオペレーションの現場に登場する operation domain, role, information の 3 つの観点から抽象的モデル化を実施している．2009 年から検討を実施してきており，本検討は既に標準化が完了している ITU-T Recommendation X.1500 にも掲載されているが，今年度は，これまでの議論・検討を踏まえ，本モデルを Ontology として精緻化し，まとめ上げて Journal 化を実現した．今後，既に規格化が完了している X.1500 について，本 journal に合わせる形で修正依頼をかけていくことを考えている．

詳細は wide-paper-cybex-refontology.txt を参照のこと．

4 MILE Implementation Report

MILE Implementation Report とは，RFC 5070 にて標準化されている Incident Object Description Exchange Format (IODEF) に対応したソフトウェアのサーベイ及びソフトウェア開発の手引きを記載した文書であり，IETF の MILE WG において議論されている．2014 年 3 月より Kathleen Moriarty 氏から引き継ぐ形で，Chris Inacio 氏と WIDE CYBEX WG の宮本によって編集されている．

4.1 CIMS

NATO が開催した Cyber Coalition 2013 では，インシデント対応を協調して行う演習が行われた．この演習において，参加者らがサイバー脅威の状況を確認し，情報を共有する目的において CIMS (Collaborative Incident Management System) と呼ばれるシステムが利用された．

CIMS は多くの CSIRT/CERT 組織で利用されている RT [1] を基に開発されている．RT はインシデントをチケット単位で扱うよう設計されており，チケットが登録，変更または削除された際には電子メールを介して関係者に情報が伝搬される．CIMS はこの電子メールの内容を IODEF 形式にインポートし，電子メールに含めてメッセージを送信する機能を持つ．また，受け取ったメールに含まれる IODEF 形式のメッセージを RT にエクスポートする機能も併せ持つ．

これらの機能が実装された意図は，協調型のインシデント対応に関する IODEF の適合可能性を調査する趣旨である．CSIRT/CERT 組織は RT において従来通りのインシデント対応を行う中で，CIMS を用いた情報伝搬は，複数の組織においてインシデント対応状況や対応における知見の共有を可能とした．今回の演習では概念実証の段階に留められているが，IODEF を用いた協調型のインシデント対応の有効性は示されたと考えられる．

[1] Request Tracker: `https://www.bestpractical.com/rt/`

4.2 n6

n6 は CERT Polska が開発したインシデント対応に必要な情報を管理する枠組みである．従来型のオペレーションでは，ネットワークの異常状態を監視するためにはネットワーク機器にログインする，SNMP 情報を参照するなどの手法で確認し，IDS の状態を確認するためには IDS へのログインやクライアントの起動するなど，機器に応じて様々なアクセス方法により情報を取得していた．n6 では Representational State Transfer(REST) 型の API を提供し，様々なサイバー脅威に関する情報へのアクセスを一元化して提供するよう設計されている．この機能を通じ，様々な情報源の管理性，データ交換の有効性が向上することが狙いである．

n6 では主に JSON の形式によって情報の交換を行うが，互換性を維持するため IODEF 及び CSV 形式による出力をサポートしている．ただし互換性は完全ではなく，n6 の持ついくつかの機能は利用できない．例えば n6 では Country Code を記載できるが，厳密には IODEF においても Contact Class などで代用することは可能であるが，直接これに相当するフィールドはない．その要因には枚挙に暇がないが，攻撃の発信元の IP アドレスは個人を特定可能な情報であるため伝搬してはいけないのではないかとも分析されている．特に EU では IP アドレスを個人情報とする向き

が強く，インシデント対応のためであっても情報共有ができない場合がある，という解釈も有り得る．

なお，n6 システムを実装可能な SDK は，オープンソース・ソフトウェアとして GitHub において公開されている [2]．n6 は WIDE メンバーが中心となり研究を推進している NECOMA プロジェクト [3] においても情報伝播の枠組みで利用されている．

4.3 ソフトウェア開発の手引について

MILE Implementation Report では，ソフトウェア開発の際に得られた知見の共有も試みられている．IODEF は XML 構造によって表現されるため，IODEF に対応したソフトウェアを開発する場合，XML の各要素にアクセスを行う機能，XML 文書としての妥当性を検証する機能が求められる．

RFC 5070 には IODEF の XML Schema Document (XSD) が定義されており，コードジェネレータを用いることによって上記の機能を実装する際に有益なクラスライブラリを自動生成されると思われた．しかし，コードジェネレータに Perl 言語用の XML::Pastor, Ruby 言語用の RXSD，Python 言語用の PyXB，Java 言語用の JAXB，C++言語用の Codesynthesis XSD，C# 言語用の XSD.exe をそれぞれ用いてクラスライブラリの生成を行った所，XML::Pastor，RXSD，JAXB において，XSD 書式の複雑性に起因されると思われる問題が発生し，クラスライブラリを生成できないことがわかった．

この回避策として，XSD 形式の文書にデータを投入する一種のシリアライズを行うことによって XML 形式の文書に変換し，さらにこの変換された XML 形式の文書から XSD 文書を作成する，いわば二重変換を行うことによって文書の複雑性を回避できるのではないかと考えた．結果として，標準的な IODEF の XSD 文書では生成できなかった XML::Pastor，RXSD，JAXB においてもクラスライブラリの生成が行えることがわかった．

ただし，IODEF には属性や要素にハイフン記号を含む箇所がある．IODEF 文書であることを表す `IODEF-Document` 属性，VLAN の名前や番号の管理に用いられる `vlan-name` 及び `vlan-num` 要素，そして拡張様式を表す `ext-category` などの要素にハイフン記号が含まれている．近代的なプログラミング言語ではクラス名にハイフンをつけることが不可能となっており，PyXB 及び Codesynthesis C++ の場合はハイフン記号をアンダースコア記号に，JAXB 及び XSD.exe の場合はハイフンを取り除いたクラス名を作成する．これらのコードジェネレータでは名前空間を保持していると考えられ，プログラム内部の IODEF クラスから XML 文書を出力する際に，置換したり取り除いたりしたハイフンが復号される．しかし，XML::Pastor 及び RXSD の場合はハイフン記号がクラス名として残ってしまい，このため生成したクラスライブラリがプログラミング言語から呼び出せない問題があった．幸い，ハイフン記号を用いている箇所が多くないため，XSD 文書ファイル内におけるハイフン記号をアンダースコア記号で置換し，XML 文書を出力する際に再度ハイフン記号に再置換を行うことにより IODEF 文書が作成可能なライブラリを作成できることが分かった．

なお，上述の自動生成したクラスライブラリ，変換された XSD 文書は，GitHub において公開されている [4]．

5 NECOMAtter

近年のサイバー攻撃対策の分野では，インシデントに関連する情報を収集し，機械学習などのアルゴリズムで情報を解析するアプローチが採られる傾向にある．多発するサイバー攻撃に対応するには，攻撃対策の省力化，自動化が求められているため，このアプローチは合理的であるように思える．しかし，攻撃対策に人間の知能が活用できる場面はないのだろうか．機械が処理できる形式知だけで，高度化するサイバー攻撃への対策は可能なのか．サイバー空間を構成するコンポーネントのうち最も脆弱な箇所はシステムから人間に移りつつある現状を鑑みると，人類に求められる挑戦とは，人間のみが持ちえる知能をサイバーセキュリティに活用することではなかろうか．

NECOMAtter は，IODEF のような machine-to-machine のセキュリティ情報交換だけではなく，human-to-machine，human-to-human のセキュリティ情報交換も指向するシステムである．機械の知能を人

[2] `https://github.com/CERT-Polska`
[3] `http://www.necoma-project.jp/`
[4] `https://github.com/daisu-mi/IODEF-codegen`

間のオペレータらに届け，人間のオペレータの知能を機械に届ける橋渡しをするために設計されている．このような情報交換の課題は，多種多様な人間の知能を，如何に有機的に連携させるかという点にある．サイバー脅威の情報は膨大であり，その情報は様々なデータソースから得られた様々な形式・性質のデータであるため，一人の人間が全ての情報を解析することは難しい．そこで，NECOMAtter の利用者である様々な専門家に，彼らの得意とする部分だけを解析してもらい，その内容を結合することによる知識の発掘を目的とする．

このような専門家による解析には，アドホック性が求められる．これは，近年のサイバー攻撃は，予想もつかないほど即興で攻撃が行われるためである．このような攻撃に対抗するには，サイバー防御も即興で対応するしかない．

この問題を解決する糸口として我々が着目したのは，Twitter 及びそれを取り巻くキュレーションサービスである．Twitter においては，様々な利用者が様々な目的で様々な情報を Tweet している．一人の利用者が全ての Tweet を閲覧することは難しいが，Follow などの機能を用いて興味を持つ範囲の Tweet を読み，必要あれば自分も Tweet を返すことができる．このようなやりとりは，キュレーションサービスを使い，いわゆる「まとめサイト」として集約され，後から容易に読み返すことができる．

翻って，サイバーセキュリティ関連の情報を Tweet する Twitter があればどうか．ここでは，機械学習による解析アルゴリズムも人間のステークホルダーもサイバーセキュリティ情報を Tweet している．全てのサイバーセキュリティ情報を閲覧し解析することは難しいが，Follow によって興味を持つ範囲の Tweet を得ることができ，必要に応じて自分も Tweet を返すことができる．このメッセージ交換（Twitter で言うところの Mention 等）を受け，さらに機械による Tweet を促し，深度の高い解析を促すことも有り得る．

NECOMAtter の情報交換モデルを図 1 に示す．NECOMAtter BOT とは，様々な種類のデータを個々に解析し，その結果を NECOMAtter システムに Tweet するプログラムである．前述のとおり，サイバー脅威の情報は膨大であり，それらの形式・性質は様々であるが，NECOMAtter は Twitter のように外部ページにリンクを掲載することもでき，Tweet のように人間にとって読みやすいテキスト形式である．興味を持つ情報について，その内容に合わせて様々なステークホルダーが専門的知識を活用することができ，これらの Mention によってアドホックに協調したインシデント対応ができるものと考えられる．

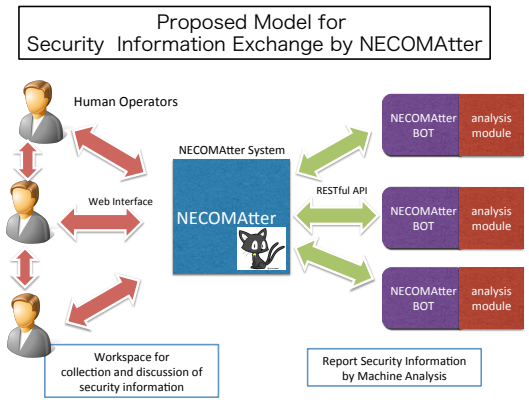

図 1: NECOMAtter における情報交換モデル

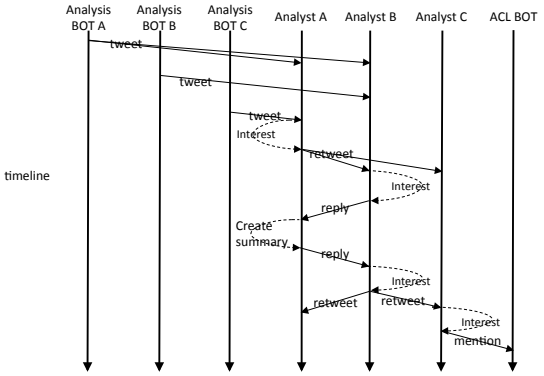

図 2: NECOMAtter における情報交換フロー

図 2 はこの情報交換フローの概念図である．例えば，NECOMAtter BOT が購読している Timeline 上に IP アドレスが出現すれば，DoS 解析を行う BOT，SPAM 解析を行う BOT，フィッシングサイト解析を行う BOT が当該 IP アドレスについての解析結果を個別に出力する．人間のオペレータらは必要に応じて自らの知見と加えたり，過去のインシデント情報と関連付けを行ったり，あるいは情報を他の BOT に伝搬させ，その断片化された情報から一連のセットであるサイバー脅威のキャンペーン情報を解析することができる．最終的に，BOT に ACL を設定させることも可能であろう．

なお，NECOMAtter はオープンソース・ソフトウェアとして GitHub 上で公開されている [5].

6　今後の予定

今年度は IODEF に注力した活動を展開しているが，IODEF は多数あるユースケースの一部に対応するものであり，すべてに対応できるわけではない．様々なユースケースを考慮し，より現場の現状に即した情報交換技術の研究開発を継続していきたい．また，規格や技術は作っただけでは，オペレーションの効率化を実現するには不十分であるため，ツールの構築などにも注力し，より技術が世の中に使われるように工夫していきたい．

[5] https://github.com/necoma/NECOMAtter