第８部

特集8 NECOMAプロジェクト：日欧協調による マルチレイヤ脅威分析およびサイバー防御の研究開発

田崎 創、岡田 和也、宮本 大輔、石原 知洋、飯村 卓司、長 健二郎、福田 健介、加藤 朗、関谷 勇司、門林 雄基

第１章　はじめに

NECOMA（Nippon-European Cyberdefense-Oriented Multilayer threat Analysis）プロジェクト[*1]は，日欧共同によるサイバーセキュリティ脅威分析とその防御に関する研究開発プロジェクトである．本プロジェクトは総務省と欧州委員会のFP7（Framework Program 7）による日欧共同研究開発プロジェクトである．欧州側からは，フランスのInstitut Mines-Télécomを中心としAtos Spain S.A.（スペイン），Foundation for Research Technology - Hellas（ギリシャ），Research and Academic Computer Network（ポーランド），6cure（フランス）という5つの大学・研究機関・民間企業がNECOMAプロジェクトに参画している．

日本側組織は，WIDEプロジェクトに参加している5組織（奈良先端科学技術大学院大学，IIJ-II，国立情報学研究所，慶應義塾大学，東京大学）の研究者が中心となり，総務省からの委託研究「日欧協調によるマルチレイヤ脅威分析およびサイバー防御の研究開発」（期間：2013年6月-2016年3月）として実施している．

本プロジェクトでは多種多様なサイバー脅威に対し異なるレイヤのデータを統合して分析し，その影響を軽減する手法やシステムの研究開発を行っている．昨今，インターネット上におけるサイバー脅威は規模もその手法も巧妙になっている．そのため迅速で効果的なサイバー脅威の検知と防御が求められている．特に大学や企業といった機密データを有する組織においては，自律的に自らのネットワーク，サーバ，利用者端末を防御し安全に運用することが求められている．

自律的なサイバー防御の実現には，自らで攻撃を検知し防御する手段を確立しなければならない．また，広域で発生する攻撃への対応には異なる組織間でのサイバー脅威情報の共有と連携が重要である．これまでにサイバー脅威データ収集，サイバー攻撃の検知，防御手法は，それぞれ独立した研究・開発が数多く行われてきた．NECOMAではこれらを互いに連携させることにより，迅速にサイバー脅威に対応可能な仕組を研究開発している．

WIDEプロジェクトは独自の広域インターネット網（WIDE Backbone）とクラウドサービス（WIDE Cloud）を持ち，その運用をWIDEに所属するメンバ自身が行っている．また，これらの基盤上で日々発生するサイバー攻撃に対するインシデントレスポンスを行っている．すなわちWIDEプロジェクトでは，自律的なサイバー防御手法を研究するには最適なインフラを有しており，NECOMAプロジェクトが目標とする技術を研究開発するにあたって十分な基盤と技術を有している．商用サービス・プロバイダでは，法律とプライバシ問題が深く関係するため，トラフィックデータ，各種ログの収集・解析を容易に実施できない．WIDEプロジェクトがこれらに先駆けて研究開発を行うことは，今後のインターネットにおけるサイバー防御機能向上に資することである．

本報告では，NECOMAプロジェクトで取り組んだ研究開発成果のうち，WIDEメンバーによる成果の一部を紹介する．

＊1　http://www.necoma-project.jp

第２章　活動記録

2013年6月
日本側コンソーシアムミーティング（以降，毎月開催）
2013年6月30日
NECOMA日本側コンソーシアム・キックオフミーティング（慶應義塾大学　日吉キャンパス）
2013年9月5日-6日
NECOMA日欧全体キックオフミーティング（フランス　パリ）
2013年11月6日
Gregg Schudel氏（Cisco）講演: LISP - A Next-Generation Networking Architecture
2013年11月30日
Deliverable D3.1: Policy Enforcement Point Surveyを公開
2014年3月31日
Deliverable D1.1: Multilayer threat data collection system design documentを提出
2014年3月31日
Deliverable D1.2: Infrastructure-layer Threat Datasetsを提出
2014年3月31日
Deliverable D1.3: Endpoint-Layer Threat Datasets を提出
2014年1月27日-28日
NECOMAコンソーシアム全体ミーティング（京都私学会館）
2014年5月22日-24日
NECOMA研究開発合宿（ラフォーレ修善寺）
2014年9月11日
The 3rd International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security（BADGERS2014[*2]）（ポーランド　ヴロツワフ）NECOMAプロジェクトが主催
2014年10月2日-3日
NECOMA研究開発合宿（慶應大阪シティキャンパス）
2014年11月30日
Deliverable D2.1: Threat Analysisを公開
2014年11月30日
Deliverable D2.2: Threat Analysis Platformを公開
2014年11月30日
Deliverable D3.2: Security Information Exchange - Designを提出
2014年11月30日
Deliverable D3.4: Countermeasure Application - Designを提出
2014年11月30日
Deliverable D5.2: Preliminary report on the use and dissemination of knowledge, and preliminary exploitation planを提出
2015年1月20日-22日
NECOMAコンソーシアム全体ミーティング（東京大学情報基盤センター）
2015年2月28日
Deliverable D4.1: Requirements and specifications of testing environmentsを公開
2015年3月31日
Deliverable D3.3: Security Information Exchange - Resultsを公開
2015年5月17日-19日
NECOMA研究開発合宿（ラフォーレ修善寺）
2015年7月29日-30日
NECOMAサマースクール（東京大学駒場キャンパス）
2015年11月2日-4日
The 18th International Symposium on Research in Attacks, Intrusions and Defenses（RAID2015[*3]）
NECOMAプロジェクトのメンバが中心となり，国際シンポジウムRAID2015を京都にて開催した.
2015年11月5日
The 4th International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security（BADGERS2015[*4]）（京都テルサ）NECOMAプロジェクトが主催

＊2　BADGERS2014: http://www.necoma-project.eu/badgers-2014/
＊3　RAID2015: http://www.raid2015.org/
＊4　BADGERS2015: http://www.necoma-project.eu/badgers-2015/

2015年11月30日

Deliverable D2.2: Threat Analysis Platformを公開

2015年11月30

Deliverable D3.5: Countermeasure Application - Resultsを公開

第３章　脅威データ収集・解析

NECOMAプロジェクトでは，プロジェクト発足初期から現在まで，コンソーシアム参画組織で収集した各種データ(トラフィック，DNS Queryログなど)を一元的に蓄積している．そして，蓄積されたデータからサイバー脅威を検知するための解析基盤をオープンソースソフトウェアを元に構築した．本節では，そのデータ収集解析基盤と解析内容の概要について述べる．

3.1　収集しているデーター覧と大規模データ収集解析基盤

NECOMAプロジェクトでは脅威分析・検知のために様々なデータを収集し，それらのデータを「クロスレイヤ分析」「マルチレイヤ分析」と呼ばれる手法で各種分析を行った．この分析では，「より多くの情報を分析すると，より多くの攻撃を検知できる」という仮定のもとシステム構築を行った．そのため，多種多様かつ多量な計測データを処理する必要があり，必然的に処理速度や多種類のデータ処理プログラムの複雑化といった課題に直面した．

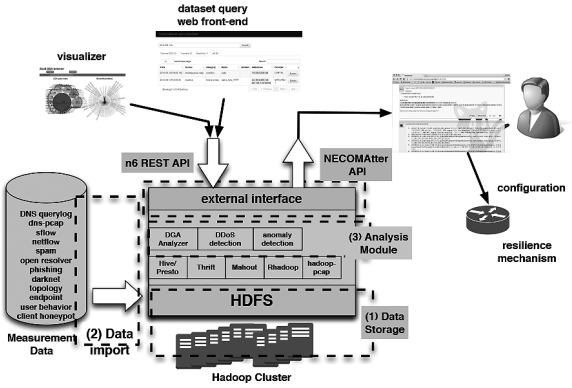

図3.1 MATATABIの内部構成

そこでNECOMAプロジェクトでは，独自の脅威分析基盤であるMATATABI [44]と呼ばれる解析基盤を設計・構築した．MATATABIはオープンソースを基盤としており，Apache Hadoop，Facebook presto-db等をベースに，ネットワークデータの蓄積や分析に適するプラグインの作成や改造などを加えることで実現した．このMATATABIによって，蓄積するデータ量やその多様性の問題と分析速度の問題を解決し，実用に耐えうるシステムを構築した．表3.1に収集データの抜粋とデータ量を示す．また，図3.1に示すシステムを，各参画組織が保有している合計11台のサーバにより構築・運用した．なお，本システムの簡素版をDockerイメージとして公開し[*5]，広く利用可能としている．

3.2　スパムメール分析

迷惑メール(スパム)は現在のインターネットにおける問題の一つである．スパムは単なる商品の宣伝のみではなく，悪意のあるプログラムや悪意のあるウェブページをダウンロードさせる等，ネットワークセキュリティ上でも大きな問題である．このようなスパムは，単一のホストから送られることは最近では少なくなり，その代わりにマルウェア等に感染した多数のホストがボットネットの一部となり，C&Cサーバより送られる指令に基づきスパムを送ることが多くなっている．本研究では，このようなボットネットの活動をスパムデータから抽出することを目的とした[45].

基本的なアイディアは，似たような文面を持つスパムは目的が同じであると仮定し，それらのスパムを送信したホスト群をクラスタとしてグループ化することにある．

表3.1　Hadoop hdfs上に蓄積している観測データと件数(2015/12月時点).

	#records	Duration
sFlow	1.9TB	2013/10 -
netFlow	0.8TB	2013/10 -
mawi	4.3TB	2013/10 -
DNS	4.2TB	2013/09 -
Spam	35.7MB	2012/06 -
Phishing	26.0GB	-

＊5　https://hub.docker.com/r/necoma/matatabi/

データセットには，本プロジェクトで収集された2011年～2013年に複数のアカウントに到着したスパムデータ（合計54万メール; 500メール/日）を使用する．

提案アルゴリズムは，特徴量抽出，ファジーハッシュ計算，ハッシュ値によるクラスタリングの3つの処理からなる．特徴量抽出では，各々のスパムメールより，送信時刻，タイトル，ヘッダ中のメールアドレス，メールID，メールソフトウエア，送信ホストIPを抽出する．とりわけ，送信時刻と送信ホストが重要となる．ファジーハッシュは，通常のハッシュと異なりハッシュ前の二つのデータの類似度を保存した結果を返す．つまり，入力となるメールの本文が似ている二つのスパムメールがあれば，それらは近いハッシュ値となる．本研究では，2つのメールの本文が85%似ているものをクラスタリングの対象とした．

提案アルゴリズムを54万件のスパムデータに適用したところ，12万個のクラスタを得ることができた．ほとんどのクラスタは1-2通のスパムからなる小さなクラスタであり，スパムキャンペーンには関係のないクラスタである．そのためサイズの大きなクラスタ（上位100個）のみに着目し，キャンペーンの継続期間や参加ホスト数等を解析した．

図3.2は，上位100キャンペーンの(a)スパム数，(b)ライフタイム，(c)ホスト数を示したものである．キャンペーンあたりのスパム数には大きな偏りがあること，キャンペーンあたりのホスト数はスパム数と強い正の相関があること，キャンペーンのライフタイムにも偏りがあるが，それらはスパム数とは必ずしも一致しないことが明らかとなった．また，詳細な解析により，スパムを送るためのテンプレート的なHTMLを使用するスパム送信者と用いない送信者の二種類が存在することが明らかとなった．これらの解析結果より得られた，ボットネットとそれに属するIPアドレスのリストは，他のデータセットで得られたボットネットデータとの比較のために有効なデータとなる．

3.3 異常トラフィック分類

インターネットトラフィックにおける異常トラフィックの検出には，各種の統計的な手法やルールベースの検出手法が用いられる．しかし，これらの検出手法の出力は単なる時刻であったりIPアドレスと時刻や，より詳細な情報（例えばポート番号）と各種さまざまである．とりわけ問題となるのは，異常検出器は異常なイベントを報告するが，それがどのような異常であるかについては言及しない．そのため，発見された異常イベントがどのようなイベントであるかの推定を後処理として行う必要がある．これは，異常イベントの重要度を評価するために必要不可欠な処理である．

本研究では，ルールベースのトラフィック分類木を構築することで上記課題を解決するアプローチを取る[46]．異常検出器の出力である異常イベントは，1つ以上のパケットから構成され，それぞれのパケットにはパケットヘッダ情報が付加されている．また，異常の発生時間・終了時間等の時間情報が付与されている．本アプローチでは，これらの特徴量に基づいたヒューリスティックなルールを用いて，異常イベントの種類を決定することを目標とした．

図3.3は，本研究で用いた分類木の構成図である．木構造

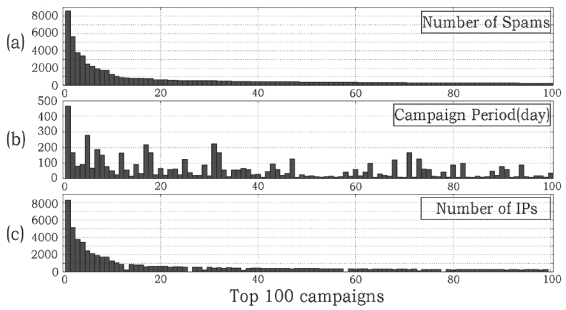

図3.2 スパムキャンペーンの特徴

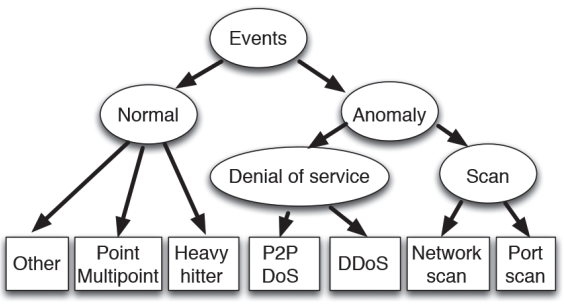

図3.3 ネットワーク異常分類木

のルートは全てのイベントを表し，各ノードが分類のクラスに対応する．たとえば最上位のイベントは，正常なイベントと異常なイベントに分離できる．さらに異常イベントには，スキャンやサービス不能攻撃といった各種の異常が含まれる．同様に正常イベントには，ヘビーユーザやサーバトラフィック等の一見異常と見えるが正常なイベントが含まれる．おのおののリーフには，対応する分類ルールが定義される．たとえばUDPネットワークスキャンは，(nb src addr < 5) && (nb packets/nb dst addr < 5)&& (nb udp packets/nb packets > 0.8) のように定義される．これは，送り元のIPアドレス数が5未満，かつ送り先への平均パケット数が5未満，かつUDPのパケットが全体の80%異常であるようなイベントである．我々は，過去14年間のパブリックに使用可能なトラフィックデータであるMAWI repositoryを用いて分類ルールを構築した．現在のバージョンでは独立した計84個のルールが定義されている．

図3.4は，既存手法であるヒューリスティックな手法による異常イベントのブレークダウン結果である．また，図3.5は提案手法によるブレークダウン結果を示したものである．既存手法では，分類不能なトラフィックが20%程度であったのに対して，提案手法では10%程度まで少なくすることができた．また，既存手法では単純なpingイベントと解釈されていたイベントが，ICMPパケットのデータ部を解析することで異なるイベントの集合であることを明らかにした．これらの結果は，マルチレイヤー解析を行う際に異なるレイヤー間でのイベントの対応付けに必要な情報であり，IPアドレス等の一次情報に追加的なイベントラベルとして使用されている．

3.4 DNSによるC&Cサーバ検知

DNSデータを用いた分析として，DGA型ボットネットのC&Cサーバ検知に取り組んだ[47]．本節では，その概要と結果について述べる．

近年，各種攻撃に用いられているボットネットでは，各種フィルタリング装置でのドメイン名からの通信検知を避けるため，ボットとC&Cサーバ間の通信時に擬似乱数などを用いたランダムなドメイン名(DGA:Domain Generation Algorithms)が利用されている．そこで本研究では，DGAの時間的局所性に着目したDGA型ボットネット検知システムlynxを開発した．本システムでは，DGAにより生成されたドメインに対する問い合わせは短期間のみ急増するという時間的局所性に対し，外れ値検知の手法を応用した．本システムを，学術ネットワーク内のDNSトラフィックを用いて評価したところ，従来手法に比べ大幅な精度の向上が確認された．

lynxは，検査対象のデータの時間的局所性に基づいてフィルタリングをおこなうDGA Extractionというモジュールと，フィルタによって検出されたデータをサポートベクターマシン(SVM)を利用しC&Cサーバの判別を行なうモジュールからなる．提案システムの比較対象には，ジョージア大学のAntonakakisらが開発したボットネット検知システムPleiades[*6]を使用した．Pleiadesは，隠れマルコフモデルを利用しDNS C&Cサーバを検知するシステムである．評価では，(1)Pleiades単独を適用した

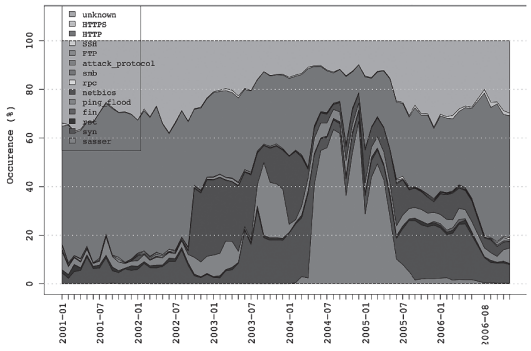

図3.4 従来のヒューリステック規則によるラベル結果

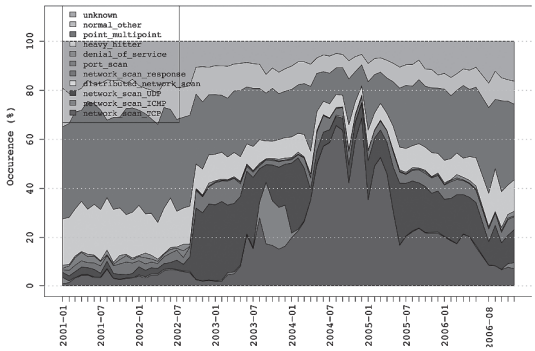

図3.5 提案分類木によるラベル結果

＊6　https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/antonakakis

場合，(2)検査対象のデータに対してDGA Extractionによるフィルタリングを実施してからPleaidesを適用した場合，(3)本方式を適用した場合(DGA Extraction + SVM)の3通りについて実施した．

図3.6，図3.7はそれぞれ，評価データに対して先行方式および本方式を適用した場合の検知率，誤検知率の比較である．両図より，提案システムは検知率を向上すると同時に，誤検知率の割合を抑えている事が明らかになった．この結果から，提案システムは先行方式に対してC&Cサーバの検出力が向上していることがわかる．また，先行方式に対してDGA Extractionを適用した場合において，検知率の割合が落ちていないことから，本来検出すべきデータについてDGA Extractionにより誤ってフィルタリングされていないことがわかる．さらに，SVMを利用した検知モジュールにより，既存の検出手法に比べてさらに高い検出精度を達成できることがわかった．

図3.6，図3.7はそれぞれ評価データに対して先行方式および本方式を適用した場合の検知率，見逃し率の割合の比較である．図3.6に示す通り，検知率の割合が向上しており，先行方式に対してC&Cサーバの検出性能が向上していることがわかる．また，先行方式に対してDGAExtractionを適用した場合において，検知率の割合が落ちていないことから，本来検出すべきデータについてDGA Extractionにより誤ってフィルタリングされていないことがわかる．図3.7に示す通り，見逃し率の割合は低下している．先行方式に対してDGA Extractionを適用したことにより見逃し率の低下が見られ，DGAExtractionにより効果的に検出対象を絞り込めていることがわかる．また，SVMを利用した検知モジュールにより，既存方式に比べてさらに高い検出精度を確保できた．

3.5　視線分析に基づくフィッシングサイト対策

NECOMAプロジェクトでは，フィッシングサイト対策を目的としたウェブサイト閲覧者の反応に関するデータ収集・解析を行った．

これまで，NECOMAの研究者はフィッシングサイトの判定精度を高める方法として，1)機械学習を用いる方法[48]，2)閲覧者の意思決定の結果を機械学習に取り入れる方法[49]，3)閲覧者の意思決定が，ウェブコンテンツ，アドレスバーに記載されたURL，ブラウザの表示するセキュリティ情報のいずれによって行われるかの調査とフィッシングサイト判定への相関分析[50]を行ってきた．NECOMAプロジェクト発足後は，閲覧者の視線移動を観測することで閲覧者に内在する精神状態を推測することができると考え，この手法の検証に着手した．

まず閲覧者の視線情報を収集するため，2013年11月から2014年2月までの期間内に東京大学の構内掲示板にて被験者を募集し，ウェブサイトを閲覧して真贋判定を行ってもらう実験を実施した．この実験参加者は25人であり，そのうち2名は実験シナリオに不備があり視線情報を正しく判別できていなかった．残りの23名についてそのうち20人が男性，3人が女性であった．また，22人が20代であり，残りの1人が30代であった．実験の際に用いたフィッシングサイトについては文献[51]を参照されたい．

図3.8は，被験者がアドレスバーを見た場合と見ない場合のフィッシングサイト判定精度を示している．延べ

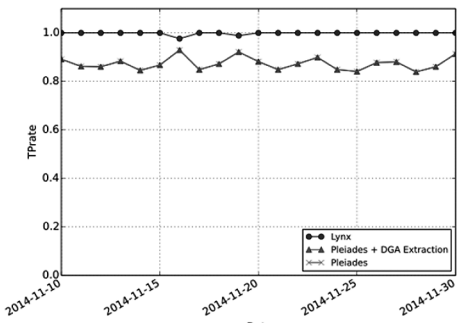

図3.6 先行方式に対するTrue Positiveの比較

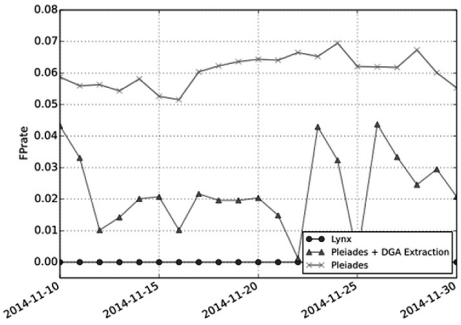

図3.7 先行方式に対するFalse Positiveの比較

331回のアドレスバーを目視した回数のうち，誤判定があったのは89回であった．フィッシングサイトに限定すると，200回のアドレスバーを目視した回数のうち61回が誤判定であり，残りの131回の正規サイトにおいてアドレスバーを目視した場合の誤判定は28回であった．従って，エラー率，見逃し率，誤判定率はそれぞれ26.9%，21.4%，30.5%となる．反対にアドレスバーを見ない場合は，41.1%（129回中53回），18.9%（53回中10回），56.6%（76回中43回）であった．見逃し率ではごくわずかにアドレスバーを見ない場合が低くなっているが，フィッシングサイトのコンテンツは正規サイトと見た目が区別しにくいため，アドレスバーを見ない限り誤検知率が高くなっている．以上より視線移動を観測することで，アドレスバーを見ることの優位性を検証できた．この調査を基に2014年度はアドレスバーを閲覧する習慣を閲覧者に身につけさせる研究，2015年度は閲覧者がどのような意図を持って閲覧しているのかを推測する研究を行った．

第４章　攻撃防御機構および脅威情報共有に関する研究開発

本節では，NECOMAプロジェクトにて研究開発を行った撃防御機構と脅威情報の共有機構について概要を記す．昨今のサイバー攻撃では多種多様な攻撃が発生しており，その対象もエンドポイント機器からインフラ機器といった幅広くなっている．そこで，本プロジェクトでは様々な攻撃を各要所で防御する機構を研究開発した．また，脅威情報共有は3章にて示した解析・検知結果を迅速に共有することを目的とした．

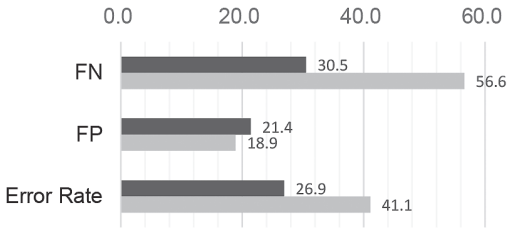

図3.8 アドレスバーを見た場合，見ない場合の判定精度

4.1　クラウド

NECOMAプロジェクトではクラウドにおける攻撃の分析と，その防御技術の研究開発を実施している．本節では，日本側研究者が中心となって行ったパブリッククラウドに関する成果について述べる．

パブリッククラウドは，多くのユーザがその資源を共有して利用する形態のクラウドである．本研究が対象とするパブリッククラウドは，主にIaaS（Infrastructureas a Service）形式のものとした．IaaSパブリッククラウド運用者の立場から脅威の検知と防御に関する手法について研究開発を行った．

パブリッククラウドの代表的な脅威には，**1）VM乗っ取りによる情報流出，2）クラウド内部におけるサービス妨害攻撃，3）クラウド外部から，もしくはクラウド外部へのサービス妨害攻撃**の3点が挙げられる．これらの脅威を検知するためには，各VMとVMが動作している共有資源の状態監視が必要である．IaaSパブリッククラウドでは利用者がVM上にて利用するゲストOSを選択できる場合がほとんどであり，VMは利用者の責任にて管理される．クラウド管理者は，VM内のゲストOSに状態を監視するソフトウェアを予め配備しておけば，VMの稼動状態を把握できる．しかし攻撃者がVMを乗っ取った場合には，このソフトウェアを利用不能にすることも可能である．そのため，クラウド管理者はVMの稼動状態をハイパーバイザ等の共有資源から監視する必要がある．

そこで，NECOMAプロジェクトでは図4.1に示す監視アーキテクチャを提案した．物理スイッチや論理スイッチで

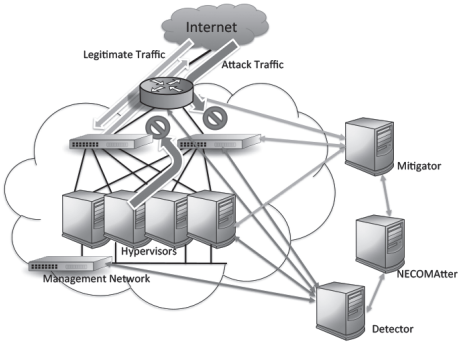

図4.1 パブリッククラウド脅威検知アーキテクチャ

は，sFlowやNetFlowを用いたトラフィックの監視を行い，ハイパーバイザでは，RFC7666 [52]の提案に基づくVM監視アーキテクチャを用いてVMの稼動状態を監視する．さらに，クラウドを構成する各機器からのsyslog情報を蓄積する．

sFlowやNetFlowによるトラフィック情報は，agurim[*7]と呼ばれるWIDE mawi WGにて開発されNECOMAプロジェクトの研究者によって改良された監視ソフトウェアを用い，リアルタイムでの異常トラフィック検知を行った．また，同じくNECOMAプロジェクトにて開発されたMATATABIというビッグデータ解析システムに蓄積された各機器のsyslogも脅威検知に利用した．この詳細はWIDE cloud WGの報告書に掲載されている．NECOMAプロジェクトが提唱したこの監視システムは，WIDE cloud WGが構築・運用しているIaaSパブリッククラウドであるWIDE Cloud上に構築し実運用を行った．

さらに我々は，解析基盤での検知結果に基づき攻撃防御を行うめのアーキテクチャ（図4.2）を設計した．このアーキテクチャでは，検知された脅威に基づき被疑対象となるトラフィックフローをOpenFlowにて別経路に誘導し，アプリケーションレベルにて防御を行うソフトウェアにて被疑トラフィックを浄化する．NECOMAプロジェクトでは，このアーキテクチャを、demand-and-opportunity based mitigation"と名付けた．図に示す通り，被疑トラフィックを検知すると物理スイッチならびに論理スイッチにてOpenFlowを利用して被疑トラフィックを別経路に誘導し，d4cと呼ばれる浄化ソフトウェアを用いて攻撃トラフィックのみフィルタリングする．このd4cは，NECOMAプロジェクトによって開発され，現在サンプル実装として，DNSの問い合わせクエリをQNAMEの条件に従ってフィルタリングする機能を有している．今後機能を拡充する予定である．この攻撃防御システムもWIDECloud上に構築し実運用を行った．

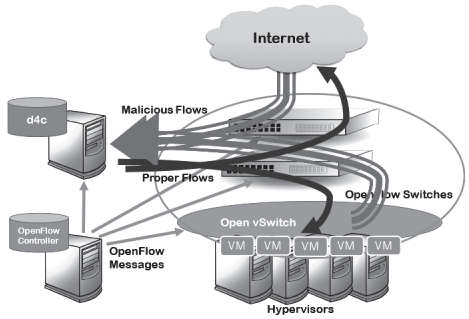

図4.2 d4cを用いた攻撃防御アーキテクチャ

4.2 SDN-IX

SDN IXは，Software Defined Networking（SDN）技術をIXの基盤に導入しIXの機能強化を目的としている．従来のIXではレイヤ2/3機器を用いて，AS同士の相互接続場所を提供していた．昨今では大規模な増幅型DDoS攻撃の増加に伴い，IXを含むドメイン間での攻撃対策が重要になってきている．しかし，従来のIXでは攻撃に対するフィルタリング等の対抗策を提供していない．そのため，攻撃を受けているAS側でフィルタ等を適応，もしくは攻撃トラフィックの流入元ASに連絡し対応してもらう必要がある．前者の場合は，フィルタにより攻撃先ホストの負荷を下げることはできるが，IXとAS間の帯域逼迫を解消できない．後者の場合は，流入元AS側への連絡後から対応までに時間を要する．また，ASによってはフィルタ等の対応を実施してもらえない場合がある．

そこで，SDN IXではIXにSDN技術を導入し，DDoS攻撃に対するフィルタリング機能といったセキュリティ機能の強化を目指している．SDN IXはAS間の相互接続をSDNに対応したスイッチを介して行い，独自に実装されたコントローラによりそれらのスイッチを制御する．現状ではSDN技術としてOpenFlowを採用し，オープンソースコントローラフレームワークRyuを用いてコントローラの実装を行っている．従来のIXでは，IX運用者のみがIXの機器（スイッチ／ルータ）設定をしていた．SDN IXではコントローラインターフェイス（Web GUI）を介して，IXに接続しているASの運用者自身による設定変更等が可能となる．これにより，迅速な攻撃防御が可能となる．本成果は，Interop Tokyo 2014/2015[*8]のShowNet内にて動態展示を行った．また，アジア太平洋地域にあるIX運用者の会合であるAPIX（2015年9月）にて発表を行った．

＊7　https://github.com/necoma/agurim/
＊8　プレスリリース：http://www.necoma-project.jp/ja/news/news-SDNIX-press

4.3 NECOMAtter

NECOMAtterは，個々のセキュリティ機器や解析モジュールからの検知情報，アナリストやオペレータからの情報を閲覧，ならびにそれらの情報を集約することを目的とした情報共有基盤ソフトウェアである．また，NECOMAtterを介して防御機構へのフィルタリング指示などの制御を簡便にすることも目的としている．

この共有基盤では，セキュリティ情報を収集し伝搬させるにあたり，Twitterのようなフォロー関係やRetweet等による情報伝搬の仕組みを導入した．図4.3は，NECOMAtterタイムラインの例である．NECOMATterにはセキュリティ技術者やネットワーク運用者といった人のみではなく，様々なセキュリティ情報を持つ機械も接続することで情報を提供し，また情報を受取る事も可能にした．他に，個々のTweetをまとめて一つのURLとすることによって分割された情報の一覧性を高める仕組みも導入している．これらの特性により，様々なセキュリティ情報源からの情報を収集・吟味することや，それらの情報をまとめて参照しやすくすること，個々のセキュリティ機器への司令を与えるなどといった運用が可能となる．

NECOMAtterでは人間のオペレータと監視を行っているBOTや機器を制御するBOTとが，同じNECOMAtter上のメッセージを通じて連携を行う．例えば，トラフィック監視を行っているBOTが異常を検知しその情報をNECOMAtterに書き込むと，人間のオペレータがその情報について詳しく知るために解析BOTへの解析指示や，関連情報の書き込みを行う．その書き込みを見た解析BOTや人間が，関連する情報を返信などの形式でNECOMAtterに書き込むことで情報が集まる．この情報のうち特に有用なものをNECOMAtomeとして纏めたり，それらの情報から問題となる異常を緩和するための指示をNECOMAtterに書き込んで，その指示を受けたネットワーク機器が異常の緩和を実行する．

このようにNECOMAtterは，NECOMAプロジェクトの情報共有基盤として構築され，オペレータ，分析結果，機器との間で情報交換を行う，パイプラインとしての役割を担っている．

第５章　おわりに

NECOMAプロジェクトは，2013年6月から2016年3月までの3年間のプロジェクトである．本プロジェクトの成果は，各課題毎に研究論文を発表するとともに，外部の産業組織，学術組織がその知見を活かせるようにソースコードや運用方法を報告書やブログ（http://www.necoma-project.co.jp），プロジェクト関係組織を交えた報告会を通じて公開している．

図4.3 NECOMAtterのタイムライン例