WannaCryを事例としたセキュリティレポートの分析

葛野 弘樹[1,]　稲垣 俊[2]　潤潟 謙一[2]

概要：セキュリティインシデントの発生に対して，各国の公的なセキュリティ対策機関や組織，民間企業ならびに個人研究者が解析結果や動向をレポートとして公開し対策を促している．その内容は，セキュリティインシデントの被害状況，検体の検出日時，利用された脆弱性や IP アドレスなど多岐にわたっている．我々はセキュリティインシデントの全体像の把握を容易にするため，複数のレポートの内容を分析しタイムラインとしてまとめる手法を提案する．提案手法は，レポートを相互に比較することで，セキュリティインシデントの網羅的な把握とサイバーセキュリティに関係する公的機関やそれに準じる組織，民間企業，個人研究者がいつの時期において兆候を捉えレポートを情報発信したのかを明らかにする．提案手法の適用例として，ランサムウェア WannaCry により発生したセキュリティインシデントへの取り組みが実際はどのように行われたのかを明らかにすることを試みた．分析対象としたレポート 19 本から作成した WannaCry に関するタイムラインにより，検体の検出日，脆弱性の公開などの重要なイベントに言及したレポートの関連性を網羅的に把握することが可能となった．

キーワード：セキュリティ脅威レポート分析，ランサムウェア，WannaCry

Evaluation of Multiple WannaCry Reports from Various Organizations

Hiroki Kuzuno[1,]　Shun Inagaki[2]　Kenichi Magata[2]

Abstract: Security incidents are major threat for information system management. Major attacks are caused by Malware, DDoS, Intrusion using vulnerability and so on. The attacking reports are one of the resources to identify the detail of attack trend uses what kind of technique to success the breaking of information system. Although many reports are published in huge security incident, we have to grasp the information from public sector, private company and researchers. In order to unveil the individual security incident, we propose the making method of time line that collects published security reports to focus a course of particular security incident. We apply our method WannaCry incident includes 19 reports cover essential events to evaluate the effects of our approach. In the result, it provides availability for user to catch the relation between important event and report released timing, then easy to handle the whole of security incident flow from the WannaCry time line.

Keywords: Open Source Intelligence, Ransomware, WannaCry

1. はじめに

計算機上のデータを暗号化し，身代金を要求するマルウェアであるランサムウェアによる被害が拡大している．特に，2017 年 05 月 12 日以降に発生した，ランサムウェア WannaCry （以下，WannaCry）は全世界で感染が確認され，被害をもたらした．このようなセキュリティインシデント（以下，インシデント）が起きた際，国や地域が設置するセキュリティ対策組織である ENISA（The European Union Agency for Network and Information Security），IPA（Information-technology Promotion Agency, Japan），公的な性質のある各国の CSIRT（Computer Security Incident Response Team）からセキュリティレポー

[1] セコム株式会社
SECOM Co., Ltd., Japan
[2] セコム株式会社 IS 研究所
Intelligent Systems Laboratory, SECOM Co., Ltd., Japan

ト（以下，レポート）が出される．さらに詳細な解析結果がセキュリティ対策企業からもレポートとして報告される．また近年では，コミュニティベースでマルウェアの観測を行った結果や感染，被害動向などが Twitter や Facebook などのソーシャルメディアやブログで個人の研究者により報告されている．

公的なセキュリティ対策組織，法執行機関，CSIRT から出されるレポート（公的レポート）には，主にインシデントの発生日時，マルウェアの概要，利用している脆弱性，感染経路，被害状況，そして対策が記載されている．一方，アンチウイルスソフト企業などセキュリティ対策を専門とする民間企業のレポート（ベンダレポート）には，企業においてのマルウェア検知日時，確認した感染状況，検体の解析結果として，亜種の有無，利用している IP アドレス，URL，アカウント情報，そして検体の開発背景や関連していると思われる組織について言及されている場合もある．コミュニティベースのレポート（コミュニティレポート）では，検体を検知した時期や VirusTotal といった外部サービスでの解析結果，追跡状況の継続的な更新など，クラウドソーシングとして情報が集積されている．

これら各種レポートを参考にすることで，インシデントを引き起こしたマルウェアや脆弱性を利用した攻撃がどのように発生しているかの確認や自組織への対策を行うことが可能である．しかし，レポートの種別や公開されたタイミングにより言及されている内容に差異があることから，複数のレポートを読み取り，整理することでインシデントの全体像を把握することが必要となっている．

我々は，大規模なインシデントに対して，より効率的かつ即座に全体像を把握し，網羅性を備えた有益な情報として整理し提供するために，複数レポートに対するインシデントのタイムラインを作成し，その内容を読み取る手順を一つのアプローチとして検討する．

複数のレポートを解析するにあたり，客観的な観点から内容を分析し，インシデント全体像のタイムラインを作成することが望まれる．本稿では，具体的な事例として WannaCry に着目した．WannaCry は使用された脆弱性ならびにバックドアへ未対策な環境が多数あったこと，ならびにワームとして感染活動を行うことから，世界的なインシデントとして捉えられ，セキュリティに関する主要な機関，組織，そして個人から多数のレポートが公開されたことが確認されている．WannaCry のレポートにおいて着目した点は，レポートの公開日，亜種を含む検体毎の検知日時や利用されている脆弱性の関連性とした．タイムラインの作成においては，WannaCry のレポート 19 本を調査分析し，得られた重要イベントとレポートを紐付けを行った．タイムラインで表されるレポート間の差異ならびにイベントとの関連性により，コミュニティレポートが早い段階で情報発信していること，公的レポートとベンダレポートによって言及されているイベントに差があることが容易に把握できた．

図 1 WannaCry Ver. 2.0 のスクリーンショット [1]．この検体では，支払い先として Bitcoin アドレスが用いられている．

本稿における，我々の研究による貢献ならびに得られた結果は以下の通りである：

- 特定のインシデントについて複数のレポートを対象とした分析手法の提案
- WannaCry ランサムウェアに関する各国組織・企業からのレポートについてのタイムライン

本稿では，以下，2 章にて WannaCry によるセキュリティインシデントの概要ついて，3 章で関連研究と分析手法を示す．4 章にて収集した複数のレポートの詳細とそれらを分析しタイムラインを作成する手順について述べる．5 章にて，収集したレポートの分析結果と WannaCry に関するタイムラインを示す．6 章にて分析収集したレポートならびにタイムラインを用いた考察を行い，今後の課題について述べる．最後に，7 章で全体のまとめについて述べる．

2. 背景知識

2.1 WannaCry の概要

WannaCry はランサムウェアとして，ユーザの端末に感染すると自動的にファイルを暗号化し，復号するために特定の暗号仮想通貨アドレスへの支払いを要求する（図 1 を参照）．我々が調査したレポートにおいては，検体の種別として Beta，Version 1.0（Ver. 1.0），Version 2.0（Ver. 2.0）の存在が確認されている [20]．2017 年 05 月 12 日に発生した世界的な感染は Ver. 2.0 により引き起こされている．感染するために使用された脆弱性は Server Message Block 1.0（SMBv1）に関する脆弱性（CVE-2017-0143 – CVE-2017-0148）[2] および，その一部を利用した EternalBlue と呼ばれるエクスプロイトである．また，EternalBlue への対策がされていた場合，情報機関の作成したバックドア

（DoublePulsar）を利用することが指摘されている [23]．公的レポート（ENISA）によると，WannaCry Ver. 2.0 は 150 国以上，230,000 以上の端末が感染による影響を受けたとされている [3], [4].

2.2 WannaCry の示した課題

WannaCry がこれほどまでに感染を拡大できた要因として，マイクロソフト社は SMB 脆弱性に対するパッチ MS17-010 を 2017 年 03 月 14 日にはサポート中 OS である Windows Vista/7/8.1/10 ならびに Windows Server 2008/2008 R2/2012/2012 R2/2016 には提供していたが，サポートの終了した Windows XP/XP Embedded/8 ならびに Windows Server 2003 には，WannaCry による被害発生後の 2017 年 05 月 13 日まで提供していなかったという点が大きい [2]．また，MS17-010 未適用の Windows 7 への感染も多数存在したことが確認されている [21]．さらに，DoublePulsar は，Ver. 2.0 の感染拡大の一ヶ月前に Shadow Brokers と呼ばれるハッカー集団からリーク [13] されており，既に DoublePulsar が端末に作成されていた場合も感染を許してしまうという点がある．一般に脆弱性を修正するパッチの公開と適用との間には，検証作業などにある程度の期間が必要であり，多くの組織で対応が取られる前に攻撃として利用された場合，パッチが適用されるまでのギャップをつくことで大規模インシデントにつながるものと考えられる．

WannaCry の事例では, 脆弱性の公開から二ヶ月後, バックドアのリークから一ヶ月後に攻撃として利用されている．組織によっては対策を行うタイミングより前に攻撃を受ける可能性も考えられる．そのため，それぞれの発生時期を時系列として網羅的に把握し，今後の対策に生かしていく必要があるといえる．

3. 関連研究

ワームの感染拡大によるインシデントとしては，2001 年 07 月 Code Red[35]，2001 年 09 月 Nimda[36]，2003 年 01 月 SQL Slammer[37], そして 2009 年 03 月に Conflicker[38] が発生している．いずれも，組織内ネットワークやインターネット経由で活動を行うことから多くの端末が被害にあった．これに対して，ワームの感染活動を攻撃として早期に検出し，未然に抑え込むことを目的としたネットワーク観測システムが提案され [24], [25]，インターネット定点観測としてトラフィックの監視を通じて攻撃傾向の分析と注意喚起が行われている [26], [27], [28].

デジタルフォレンジックスにおいては，タイムラインの作成と解析はインシデントに対応する際の主要な技術であり，調査する端末やネットワークにおいて端末上でのプログラムの動作履歴，機器間通信履歴を時系列上に並べ，インシデントの原因や影響の分析を行うために用いられている [29], [30].

災害対応では，事前にマニュアルとして整備された時系列順の防災行動計画がタイムラインと呼ばれている [31]．これは災害発生前から発生後に至るまでの連携や対処を順序立てて行う必要があるからであると考えられる [32]．また，公衆衛生においても，新型インフルエンザの感染に関するイベントの予測 [34]，世界的な鳥インフルエンザの感染状況の把握にタイムラインが用いられていることを確認できる [33].

4. 提案手法

大規模なインシデントが発生した場合，公的レポートが各国の対策組織や機関から，ベンダレポートが多数の企業から公開される．インシデントの内容によっては，コミュニティレポートが速報性の高いソーシャルメディアを利用してリアルタイムで公開，更新されている．

我々は，インシデントに対するタイムラインを作成するために，まずは，それら各種レポートを順次収集し，記載されている内容を分析することによって，時系列ごとにイベントを列挙する．その後，イベント内容の関係性を導き出し，レポートとの関連づけを行う．これにより，重要性の高いイベントや価値のあるレポートを洗い出し，最終的にタイムラインを参照することでインシデントに関する網羅性の高い有益な情報を読み取ることを可能とする．

4.1 タイムライン作成手順

インシデントに対するタイムラインの作成はいくつかの手順に分けて進めていくが，インシデントの発生および作成に用いるレポートが公開されるタイミングは把握できないことから，収集したレポートの内容を調査しながら行うこととなる．そのため，我々はインシデントの発生に対して以下の手順にて，各種レポートの取集，最終的にタイムラインを組み立てていく．

(1) インシデント発生の確認：ソーシャルメディアまたは速報的なレポートでのインシデントの把握
(2) インシデント詳細の確認：マルウェア検体や利用された脆弱性などインシデント原因の確認
(3) 公的レポートの確認：各国の対策組織，機関からのレポートにてインシデントと判断
(4) ベンダレポート，コミュニティレポートの収集：各種レポートの積極的な収集と段階的な調査の開始
(5) 重要イベントの抽出，タイムライン作成開始：収集したレポートを分析し，共通・重要イベント，イベント発生日時を調査，タイムラインを組み立てる
(6) 各種レポートとイベントの関連性調査：タイムライン上のイベントとレポートを紐付け，確認
(7) タイムライン作成完了：最終的なタイムラインとして整理，更新されたイベントがあれば適用

表 1 各種レポートに含まれる主要なコンテンツ．✓ は多くの場合に掲載されているコンテンツ，△ はレポートによっては掲載されるコンテンツとしている．

レポート名称	コンテンツ					
	公開日時	被害状況	インシデント内容	対応策	検体解析	背景
公的レポート	✓	✓	✓	✓		
ベンダレポート	✓	△	△	△	✓	△
コミュニティレポート	✓	△		△	✓	△

また，タイムラインの作成において収集し調査分析の対象とするレポートと分類は次のようにした：

- 公的レポート：国や地域の設置するセキュリティ対策組織，法執行機関，CSIRT などの公的な立場をもつ組織
- ベンダレポート：アンチウイルスソフト企業，セキュリティ対策ベンダなどの民間企業
- コミュニティレポート：ソーシャルメディアを利用した個人や有志グループによる情報発信

調査分析の対象となるレポートは，同じインシデントを扱っていたとしても，作成元によって含まれるコンテンツがそれぞれ異なる．これは，レポート作成元により注意喚起や情報提供といったインシデント対処への姿勢やレポートに含める対象範囲が違うためである．そこで，各種レポートの含むと考えられるコンテンツを表 1 にまとめた．これらのコンテンツはレポートの作成元によっては粒度も異なることからそれぞれの内容を加味してレポートの種別毎に着目すべき点を抜き出して，インシデントのタイムラインに加えていくこととしている．

4.2 タイムライン作成例

インシデントに対するタイムラインの作成例として，架空とするサンプルインシデントからタイムラインの作成を試みる．サンプルインシデントにおいては各種レポートにタイムラインの組み立てに必要な情報が含まれていることを想定した．

サンプルインシデント

サンプルインシデントとして，マルウェアによる情報漏洩を想定した．サンプルインシデントでは，2017 年 01 月 20 日，オフィスアプリケーションの脆弱性を利用するマルウェアを添付したメールが複数の企業に配布され，マルウェアに感染した環境から外部への情報漏洩が発生している内容とする．

サンプルインシデントに対して，我々は，2017 年 01 月 22 日，検体をマルウェア検査サイトにアップロードされていることを確認し，実際に検体が動作し通信先や被害が起きることを確認したとする．

各種サンプルレポート

我々が収集した各種レポートは以下の通りとする：

- 公的レポート：2017 年 01 月 22 日公開，インシデント概要，脆弱性情報
- ベンダレポート：2017 年 01 月 21 日公開，検出日時，脆弱性詳細
- コミュニティレポート：2017 年 01 月 20 日公開，検出日時

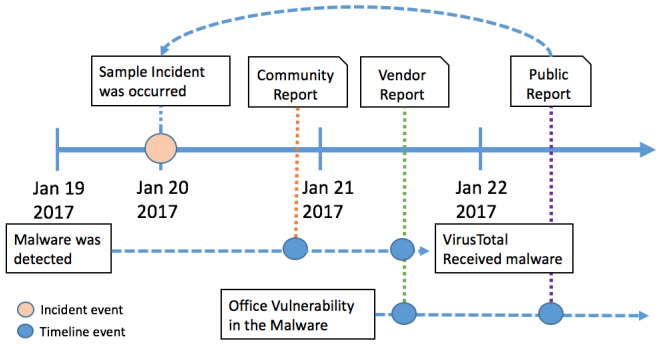

図 2 サンプルインシデントに関するタイムライン

サンプルタイムライン

タイムラインでは，時系列線を中心に，上部にインシデント（四角枠），レポート（一片の欠けた四角枠）と下部に重要イベント（四角枠）を配置している．そして，インシデント発生日（オレンジ丸），イベントへの言及（青丸）がレポートとの関連付けを表す．関連付けにおいて，コミュニティレポートにはオレンジ破線，ベンダレポートには緑破線，公的レポートには紫破線を用いる．

サンプルインシデントの各種レポートを収集し，調査分析して得られたイベントを元に作成したタイムラインを図 2 に示す．図 2 において，時系列として，サンプルインシデントの発生日である 2017 年 01 月 20 日後に各種レポートが公開されていることを表している．そのうち，コミュニティレポートではサンプルインシデント前日 01 月 19 日での検体検出に言及，ベンダレポートでは 01 月 19 日の検体検出と，オフィスアプリケーションの脆弱性について，そして，公的レポートではサンプルインシデントの概要と脆弱性情報について言及されていることを示している．

このように，タイムラインを作成することで，インシデントの全体像と重要イベントの流れ，また，各種レポートが重要イベントとどのように紐付いているかの確認を行うことができ，インシデントに対する必要な情報の網羅的な把握を可能とする．

5. 大規模インシデントにおけるタイムライン

提案手法の適用例として，我々は，WannaCry によるインシデントに着目した．WannaCry では，攻撃に使用された MS17-010 に関する脆弱性の公開，Shadow Brokers によるリーク，そして，感染が拡大したタイミングが密接に関係しているように考えられる．また，世界的に被害が発生したことから，大規模インシデントとして多数のレポートが公開されたことを確認している．インシデントの全体像を把握するためには，それらの内容を理解し，レポート間の差異を捉えつつ整理することが必要とされる．そこで，我々の提案するインシデントに対するタイムライン作成のアプローチが有効か評価するため，実際に WannaCry に関するタイムラインの作成を行う．

5.1 分析対象とした各種レポート

我々が WannaCry に関して収集したレポートと含まれるコンテンツを表 2 に示す．収集を行った期間は，2017 年 05 月 15 日から 06 月 19 日にかけてである．実際に収集し，タイムライン作成に使用したレポートは合計で 19 本とした．内訳は，公的レポート 5 本，ベンダレポート 9 本，コミュニティレポート 5 本である．その他に Twitter や Facebook での投稿などソーシャルメディアの断片的な情報やウイルス対策ソフト確認サイトの結果あるが，参考情報とした．また，収集したレポートの言語は英語，日本語だが，その他言語で書かれた参考情報も含まれる．

WannaCry では，非常に多数のレポートが公開されたため，その全ては収集かつ分析できていない．そのため，レポートの種別毎に主要な組織，団体，企業を列挙しタイムライン作成のための分析対象としている．コミュニティレポートについては，一次情報として投稿された情報を主な対象とすることとした．また，収集したレポートからの重要イベントの抽出，内容の分析を行う過程において，WannaCry の検体，検体検出日，使用された脆弱性などについてレポートに記載されている内容がそれぞれ異なることが明らかになった．その結果を表 2 としてまとめ，各レポートがどのようなコンテツを含むのか整理し，タイムラインの作成に用いた．

5.2 WannaCry に関するタイムライン

WannaCry により引き起こされたインシデントに対して，我々の提案するタイムライン作成手順に従い，最終的に組み立てられた WannaCry に関するタイムラインを図 3 に示す．図 3 では，表 2 のレポートを分析した結果，以下の重要イベントとそれぞれのイベント発生日時をタイムラインの基本的な流れとして配置した：

- Beta 検出日：2017 年 02 月 10 日
- SMB 脆弱性（MS17-010）公開日 [2]：2017 年 03 月 14 日
- Ver. 1.0 検出日：2017 年 03 月 26 日
- Shadow Brokers によるリーク日 [13]: 2017 年 04 月 14 日
- Ver. 2.0 検出日：2017 年 05 月 12 日
- Ver. 2.0 感染拡大日：2017 年 05 月 12 日
- キルスイッチの発見日：2017 年 05 月 12 日，14 日

続いて，タイムライン上へのイベントの配置後，各種レポートがいつの時点で公開され，それぞれのイベントに対して言及しているのかの紐づけを行いタイムラインの組み立てを行った．

表 2 により，我々の分析対象としたレポートにおいて各検体のイベントに関連するレポートは，Beta 検出に関して 2 本，Ver. 1.0 検出に関して 6 本，Ver. 2.0 検出に関して 17 本である．また，脆弱性のイベントに対し関連するレポートは，SMB 脆弱性公開日に関して 14 本，Shadow Brokers によるリークに関して 8 本，キルスイッチについて 3 本となった．図 3 のタイムライン上で注目すべき点として，大規模インシデントを引き起こした Ver. 2.0 感染拡大日以前のレポートとしては，コミュニティレポートが早く Beta，Ver. 1.0 いずれも 1 本ずつ報告されている．また，Ver. 2.0 感染拡大日以後も Shadow Brokers と Ver. 2.0 の関連性への言及はコミュニティレポートが最も早いことを確認できる．

パブリックレポートについては，WannaCry のインシデントについて Ver. 2.0 感染拡大後すぐに公開されており，被害状況や脆弱性についての言及されていた．パブリックレポートに続いてベンダレポートの多くが同日に公開されており，それらは Ver. 2.0 の解析を中心に SMB 脆弱性と Shadow Brokers との関連性に言及していることがタイムラインから読み取れる．また，一部のベンダレポートは Ver. 1.0 を Ver. 2.0 感染拡大日以前に検出していることを報告している．

6. タイムラインによる考察

我々は，複数のレポートからインシデントに関連する重要なイベントを抽出し，それぞれのレポートと関連付けることに提案手法により，インシデントの全体像の把握，重要イベントとレポートの関連性の有無を容易に読み取ることが可能と考えている．そして，その適用例として，WannaCry のインシデントに関するタイムライン上の重要イベントに対してどの組織，民間企業，コミュニティがどのタイミングで対応するレポートを公開したかを示した．WannaCry のタイムラインにおいては，脆弱性公開，各検体検出，実際のインシデント発生に至るまでの間隔，そして各種レポートがどの重要イベントに言及しているかを即座に見渡すことができる．そのため，多数のレポート間の

表 2 分析対象とした WannaCry に関するレポートに含まれるコンテンツ内容．✓ はレポート内で言及されているコンテンツ，△ は断片的に書かれているコンテンツとした．検体（Beta，Ver. 1.0，Ver. 2.0）については解析結果が掲載されていた場合 ✓ としている．

レポート名称	コンテンツ										
	公開日	被害状況	内容	対応策	Beta	Ver. 1.0	Ver. 2.0	SMB 脆弱性	Shadow Brokers	背景	Kill Switch
公的 01 US-CERT[3]	May 12, 2017	✓	✓	✓			✓	✓			
公的 02 ENISA[4]	May 15, 2017	✓	✓	✓			✓	✓	✓		
公的 03 CERT-EU[16]	May 12, 2017	△	✓	✓			✓	✓	✓		
公的 04 JPCERT/CC[5]	May 14, 2017		△	△			✓	△			
公的 05 IPA[6]	May 14, 2017		△	△			✓	△			
ベンダ 01 Kaspersky[21]	May 12, 2017	✓	✓				✓	✓			
ベンダ 02 Malwarebytes[22]	May 12, 2017	△					✓	✓	✓		✓
ベンダ 03 Trendmicro[18]	May 12, 2017	△				△	✓	✓	✓		✓
ベンダ 04 Fortinet[20]	May 15, 2017				✓	✓	✓				
ベンダ 05 Symantec[19]	May 12, 2017					△	✓	✓	✓	△	✓
ベンダ 06 ESET[17]	May 15, 2017						✓	✓			
ベンダ 07 Secdo[15]	May 17, 2017						✓	✓	✓	✓	
ベンダ 08 ENDGAME[12]	May 17, 2017		✓			✓	✓	✓		✓	
ベンダ 09 MBSD[11]	May 18, 2017		✓			✓	✓	✓			
コミュニティ 01 Github[14]	May 13, 2017	✓	✓				✓	✓	✓		
コミュニティ 02 Twitter[7]	Feb 10, 2017				✓						
コミュニティ 03 Twitter[8]	March 26, 2017					✓					
コミュニティ 04 Twitter[9]	May 12, 2017						✓				
コミュニティ 05 Twitter[10]	May 12, 2017						✓		✓		

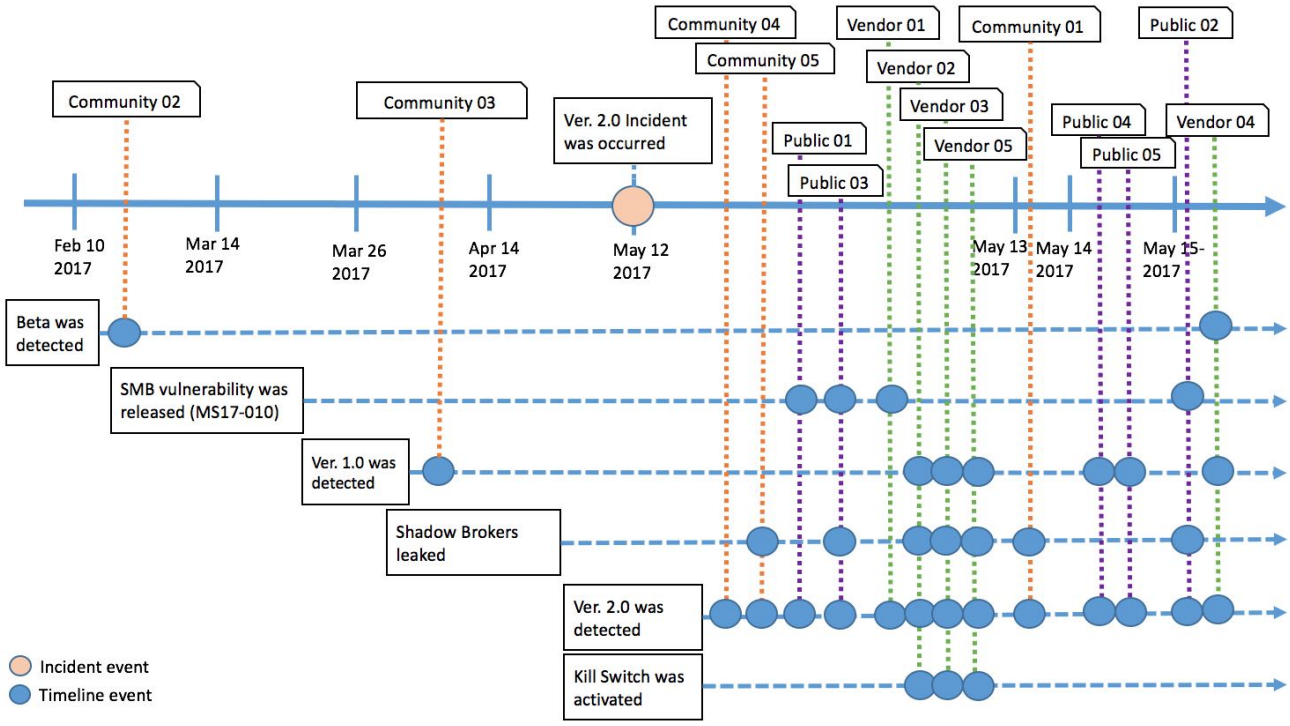

図 3 WannaCry インシデントに関するタイムライン

差異を見出したり，重視すべきレポートの絞り込みが可能であり，我々の提案手法により組み立てた大規模インシデントのタイムラインは網羅性の高い有益な情報と言える．

WannaCry のタイムラインより，コミュニティによるレポートが早期に Beta や Ver. 1.0 検体の検出について言及しており，SMB 脆弱性や Shadow Brokers リークと関連付けた内容についてもその他のレポートに先駆けて報告していることが分かる．これらのレポートは断片的な場合もあるが，一次情報源としてより注目して収集する必要があると考えている．

セキュリティ対策組織や CSIRT からのパブリックレポートについては，WannaCry による各国の被害内容や脆弱性の概要などインシデントへの対応の根拠となる情報を掲載している．しかし，国や地域によりレポートの公開日やコンテンツに差があり迅速な公開と継続的なコンテンツ追加が期待される．

民間企業によるベンダレポートは，Ver. 2.0 の解析による SMB 脆弱性の利用や Shadow Brokers リーク後の攻撃

に言及するなど，タイムライン上のイベントを網羅している．一部のレポートにおいては Beta や Ver. 1.0 をコミュニティレポートと同時期に検出していることが述べられているが，いずれも Ver. 2.0 感染拡大後の公開であり，インシデント発生前にそれらを知ることは難しい．

WannaCry やその他の攻撃によるインシデントの発生に対して，各種レポートは発行元の得た様々な情報に従い短期間で公開されている．コンテンツの内容によってはレポート間で矛盾が生じる可能性もあり，タイムラインの作成においては情報の確度の高さについて検討することが求められる．

7. おわりに

WannaCry はワーム型の感染活動と利用された脆弱性から多数の国で被害が発生した．このような大規模なインシデントに対しては，公的な機関・団体，企業，そしてコミュニティから多数のレポートが公開される．各種レポートには検体の検知日時，被害状況，亜種の有無，検体の解析結果などが含まれるが，公開日時や公開元により記載されている内容に差異があり，インシデントの全体像を把握するためには複数のレポートを分析することが必要となる．我々は，大規模なインシデントが起きた際，即座に網羅性を持った情報として各種レポートを整理し提供することを目的として，複数のレポートに対するインシデントのタイムラインを作成する手法を提案し，WannaCry の事例に関するタイムラインにおいて手法が有効かどうかの検証を行った．WannaCry のレポート 19 本の調査分析により作成したタイムラインより，各種レポートと重要イベントの関連性が明らかになり，網羅性の高い情報として整理し提供できることを示した．今後も規模や地域が異なるが大規模なインシデントは発生すると考えられる．そのため，継続的なレポートの分析ならびにタイムラインの作成を通じて提案手法の有効性を確認していく予定である．

参考文献

[1] Tech Media Network, “Huge Ransomware Attack Stopped by Accident: What to Do”, https://www.yahoo.com/tech/huge-ransomware-attack-spreads-across-120000879.html (2017.06.19).

[2] Microsoft Security Tech Center, “Microsoft Windows SMB サーバー用のセキュリティ更新プログラム (4013389)”, https://technet.microsoft.com/ja-jp/library/security/ms17-010.aspx (2017.06.19).

[3] US-CERT, “Indicators Associated With WannaCry Ransomware”, TA17-132A, https://www.us-cert.gov/ncas/alerts/TA17-132A (2017.06.19).

[4] ENISA, “WannaCry Ransomware Outburst”, https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst (2017.06.19).

[5] JPCERT/CC, “ランサムウエア ”WannaCrypt” に関する注意喚起”, JPCERT-AT-2017-0020, https://www.jpcert.or.jp/at/2017/at170020.html (2017.06.19).

[6] IPA, “世界中で感染が拡大中のランサムウェアに悪用されている Microsoft 製品の脆弱性対策について”, https://www.ipa.go.jp/security/ciadr/vul/20170514-ransomware.html (2017.06.19).

[7] S!Ri (@siri_urz), https://twitter.com/siri_urz/status/830008052954890242 (2017.06.19).

[8] Karsten Hahn (@struppigel), https://twitter.com/struppigel/status/846241982347427840 (2017.06.19).

[9] MalwareHunterTeam (@malwrhunterteam), https://twitter.com/malwrhunterteam/status/862946459376857088 (2017.06.19).

[10] Kafeine (@kafeine), https://twitter.com/kafeine/status/863049739583016960 (2017.06.19).

[11] MBSD, “WannaCry 2.0」の内部構造を紐解く”, http://www.mbsd.jp/blog/20170518.html (2017.06.19).

[12] ENDGAME, “WCry/WanaCry Ransomware Technical Analysis”, https://www.endgame.com/blog/technical-blog/wcrywanacry-ransomware-technical-analysis (2017.06.19).

[13] theshadowbrokers, “Lost in Translation”, https://steemit.com/shadowbrokers/@theshadowbrokers/lost-in-translation (2017.06.19).

[14] rain-1, “WannaCry—WannaDecrypt0r NSA-Cyberweapon-Powered Ransomware Worm”, https://gist.github.com/rain-1/989428fa5504f378b993ee6efbc0b168 (2017.06.19).

[15] SECDO, “Multiple Groups Have Been Exploiting ETERNALBLUE Weeks Before WannaCry”, http://blog.secdo.com/multiple-groups-exploiting-eternalblue-weeks-before-wannacry (2017.06.19).

[16] CERT-EU, “WannaCry Ransomware Campaign Exploiting SMB Vulnerability”, Security Advisory 2017-012.

[17] ESET, “Vulnerability CVE-2017-0144 in SMB exploited by WannaCryptor ransomware to spread over LAN”, http://support.eset.com/ca6443/?locale=en_US&viewlocale=en_US (2017.06.19).

[18] TrendMicro, “Massive WannaCry/Wcry Ransomware Attack Hits Various Countries”, http://blog.trendmicro.com/trendlabs-security-intelligence/massive-wannacrywcry-ransomware-attack-hits-various-countries (2017.06.19).

[19] Symantec, “Ransom.Wannacry”, https://www.symantec.com/security_response/writeup.jsp?docid=2017-051310-3522-99 (2017.06.19).

[20] Fortinet, “WannaCry: Evolving History from Beta to 2.0”, http://blog.fortinet.com/2017/05/15/wannacry-evolving-history-from-beta-to-2-0 (2017.06.19).

[21] SECURELIST, “WannaCry ransomware used in widespread attacks all over the world”, https://securelist.com/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/78351/ (2017.06.19).

[22] Malwarebytes, “WanaCrypt0r ransomware hits it big just before the weekend”, https://blog.malwarebytes.com/cybercrime/2017/05/wanacrypt0r-ransomware-hits-it-big-just-before-the-weekend/ (2017.06.19).

[23] Rapid7, “Microsoft CVE-2017-0143: Windows SMB Remote Code Execution Vulnerability”, https://www.rapid7.com/db/vulnerabilities/msft-cve-2017-0143 (2017.06.19).

[24] V Yegneswaran, P Barford, and J Ullrich, “Internet

intrusions: Global characteristics and prevalence", in ACM *SIGMETRICS*, 2003.
[25] CC Zou, L Gao, W Gong, and D Towsley, "Monitoring and early warning for internet worms", in ACM *CCS*, 2003.
[26] NICT, "NICTER WEB 2.0", `http://www.nicter.jp/` (2017.07.05).
[27] 警察庁 Police, "インターネット定点観測", `https://www.npa.go.jp/cyberpolice/detect/observation.html` (2017.07.05).
[28] JPCERT/CC, "TSUBAME(インターネット定点観測システム)", `https://www.jpcert.or.jp/tsubame/` (2017.07.05).
[29] F. Buchholz and C. Falk, "Design and Implementation of Zeitline: A Forensic Timeline Editor", in *DFRWS* 2005.
[30] J. Olsson and M. Boldt, "Computer forensic timeline visualization tool", in *DFRWS* 2009.
[31] 国土交通省水管理・国土保全局 タイムライン（防災行動計画）策定・活用指針 (初版), 2016.
[32] 平山修久, "災害時の安全な水の確保", 保健医療科学, Vol.64 No.2 p.94 ー 103, 2015.
[33] WHO, "H5N1 avian influenza: Timeline of major events 13 December 2011", 2011.
[34] P. McConnell, "Banks and Avian Flu: Planning for a Possible Pandemic", Risk Trading Technology, 2005.
[35] CERT/CC, "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL", CA-2001-19, 2001, `http://www.cert.org/historical/advisories/CA-2001-19.cfm` (2017.07.05).
[36] CERT/CC, "Nimda Worm", CA-2001-26, 2001, `http://www.cert.org/historical/advisories/CA-2001-26.cfm` (2017.07.05).
[37] CERT/CC, "MS-SQL Server Worm", CA-2003-04, 2003, `http://www.cert.org/historical/advisories/CA-2003-04.cfm` (2017.07.05).
[38] US-CERT, "Conficker Worm Targets Microsoft Windows Systems", TA09-088A, 2009, `https://www.us-cert.gov/ncas/alerts/TA09-088A` (2017.07.05).