Vol.2018-IOT-43 No.2
Vol.2018-SPT-30 No.2
2018/9/27

東工大CERTにおけるインシデント対応の分析とその自動化に関する考察

石井 将大[1,a)]　森 健人[1,b)]　松浦 知史[1,c)]　金 勇[1,d)]　北口 善明[1,e)]　友石 正彦[1,f)]

概要：本論文では，東工大 CERT におけるセキュリティインシデント対応のフローと，インシデントの重要度，対応に至るトリガー等の判断基準を示し，将来的なインシデント対応の自動化を見据えた，ログ・検知イベント分析基盤の構築と運用方法について述べる．
初めに，東工大 CERT が行ってきたインシデント対応のパターンを整理し，本学におけるインシデントの分類とそれらの性質を述べ，インシデント対応のフローやリスク判断について，JPCERT/CC や NIST 等が定める一般的な基準と比較した上で，インシデント対応の自動化に必要な点について明らかにする．
更に，高度標的型攻撃対策としての本学における Lastline の運用方法と，SOC 業務の省力化やインシデント対応の自動化を視野に入れた，Splunk を利用したログ分析基盤環境の構築について述べる．
最後に，これら自動化の柱をなす機械学習手法の適用について，一部試行的な取り組みを紹介し，考察を与える．

1. はじめに

近年の高度化された標的型メール攻撃やシステムの脆弱性を突いたサイバー攻撃等に対し，組織においてはリスクのより高いセキュリティインシデントが発生し，CSIRT (Computer Security Incident Response Team) によるインシデント対応に掛かるコストは増大の一途をたどっている．現在では CSIRT を持つ大学は珍しくないが，一般企業における CSIRT と比較すると，大学においてはその体制や人員構成，規定やポリシーに大きな差がある．従って，インシデント対応の手順・構成要素においても大きな違いが見られる．大学における CSIRT, 或いは実施するインシデント対応を成熟させるためには，他組織のノウハウを直接的に取り入れることは出来ず，自組織における対応の高度化等を図る必要がある．

本論文では東工大 CERT のインシデント対応フローの事例を基に紹介し，対応フローのパターンや基本要素を分析する．また，インシデント対応コストの削減，対応の自動化を見据えた，セキュリティ機器の運用方法や，ログ分析基盤の構築について述べる．

本論文の構成は以下の通りである．2 章において CSIRT におけるインシデント対応がどの様なものであるか概観し，3 章において東工大 CERT の組織体制と実際のインシデント対応事例を述べ，一般的な対応フローと比較する．4 章において高度標的型対策のサービスの一つである Lastline[*1] と，ログ解析基盤として Splunk[*2] を用いた対応事例について紹介し，運用方法における対応の際の有効的な点について述べる．5 章では，事例として取り扱うインシデント案件と対応内容を分析することにより，対応フローの基本構成要素を明らかにし，対応の自動化について考察を与える．最後に 6 章において本論文を纏める．

2. CSIRT におけるインシデント対応

本章では，インシデント対応の一般的な手順・プロセス，また，対応の際の分析対象や手法，インシデント分類といった，インシデント対応の構成要素について概観する．

2.1 インシデント対応フロー

初めに，組織における CSIRT を中心とした，一般的なインシデント対応フローを示し，各フェーズにおける基本事項を述べる．JPCERT/CC によるインシデント対応マニュアル [4] において，インシデント対応の際の典型的な

[1] 東京工業大学 Tokyo Institute of Technology, Meguro, Tokyo 152–8550, Japan
[a)] mishii@gsic.titech.ac.jp
[b)] mori@cert.titech.ac.jp
[c)] matsuura@gsic.titech.ac.jp
[d)] yongj@gsic.titech.ac.jp
[e)] kitaguchi@gsic.titech.ac.jp
[f)] tomoishi@noc.titech.ac.jp

[*1] https://www.lastline.com
[*2] https://www.splunk.com

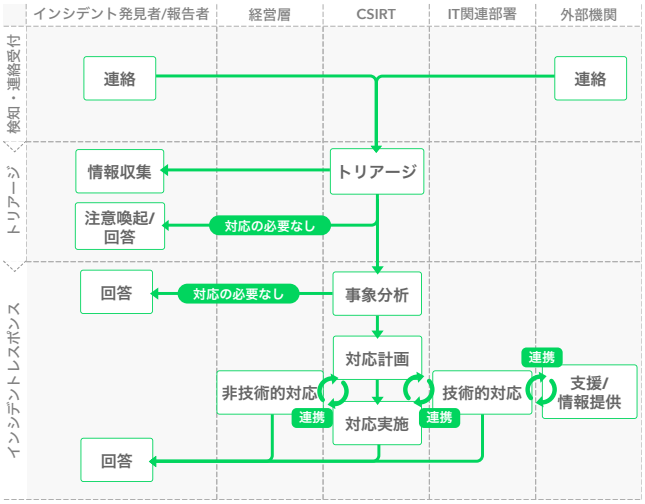

図 1 一般的なインシデント対応フロー

フローが示されている．図 1 は [4] のフロー図を簡略化したものである．

検知/連絡受付のフェーズにおいては，組織内のアラート検知や，組織内外からのインシデント報告により，インシデント事案として CSIRT にそれらの情報が伝達される．CSIRT は，外部機関として自組織外の CSIRT や専門的なセキュリティ組織・機関との対外連携を行い，外部機関の情報提供をトリガーとしたインシデント対応も行う．

トリアージのフェーズにおいては，CSIRT が受領した事案を分析し，インシデント案件としての対応の必要性，インシデントの重大度，対応の優先順位等を決定する．対応の必要がない場合は，発見者，或いは報告者に情報提供等を行う．

インシデントレスポンスのフェーズにおいては，まずインシデント案件に対し，事象分析を行い，攻撃による被害範囲の特定や発生原因等を調査する．事象によっては，即座にネットワークを遮断するといった初動対応を行う．インシデントの分析結果により，組織の体制やポリシーに従い，経営層等の上位層，IT 関連部門等との連携を含めた対応計画を作成し，それらをもとにインシデントの解決を行う．インシデントの内容に応じて，再発防止策を整理し，報告者等当該者に対して，情報提供・注意喚起も行う．案件の解決後は，対応内容の評価・フィードバックを行う．

2.2 インシデントの分類・トリアージ・分析

インシデント事案を分析し，対応すべき案件であるかを判断するコストは大きい．以下では，インシデント分析の際の基本的な事項を挙げる．

インシデント事案

自組織におけるセキュリティ機器やネットワークログの監視によって観測されるインシデントの候補と考えられる事案は膨大であり，関連するインシデントの兆候を正確に把握することは大変難しい．コンピュータセキュリティインシデント対応ガイド (SP800-61) [3] においては，インシデントの兆候として，IDPS・アンチウイルスソフトウェアのアラート，Web サービスの不具合，自組織内外のユーザからの報告，ネットワーク管理者による異常トラフィックの観測等を挙げている．

インシデントの分類

事象分析において，その事象がどのインシデントに分類可能であるかを判断することは，トリアージの際の重要な要素である．JPCERT/CC のインシデント報告対応レポート（2018） [5] においては，以下の通りにインシデントを分類している．

- フィッシングサイト，Web サイト改竄，
- マルウェアサイト，スキャン，
- DoS/DDoS, 制御システム関連，
- 標的型攻撃，
- その他（脆弱性等を突いたシステムへの不正侵入，マルウエア（ウイルス，ボット，ワーム等）の感染等）．

また，これらに加え，ネットワークやコンピュータリソースの利用規定違反が挙げられ，更に，不正侵入を行うためのマルウェア感染（バックドアの設置等）といった，複合要素を持つインシデント案件も考えられる．

トリアージ・分析

インシデントのトリアージ・分析の基本原則として以下が挙げられる [3].

インシデント事案はインシデントの候補であるが，事件ではないと確信を持って判断出来るまではインシデント扱いとするべきである．但し，全ての事案に対処することは現実的ではなく，実際には，一元化したログの利用等により，イベント相関処理を実施し，分析を行っていく．分析の際は，SOC オペレータ等の経験を最優先し，経験が少ないスタッフのためには診断マトリックスの作成が有効的である．

事象の性質によって，分析に必要な調査すべき情報は異なるが，どのシステム（プロセス），人が感染・影響を受けたか，感染源に何が起こったか，どの情報が不正に奪取されたか，ビジネスインパクト等を明らかにする必要がある．また，フォレンジック，法的な対応等，その他の調査手続きを取ることもある [2].

3. 東工大 CERT の組織体制とインシデント対応事例

本章では，初めに東工大 CERT の組織体制を簡単に述べ，インシデント対応業務におけるログ収集・分析，組織内のコミュニケーションツールや情報管理等を行うための基盤環境について紹介する．更に，東工大 CERT における典型的なインシデント対応事例を紹介し，2 章で述べた一般的なインシデント対応フローとの差異を示す．

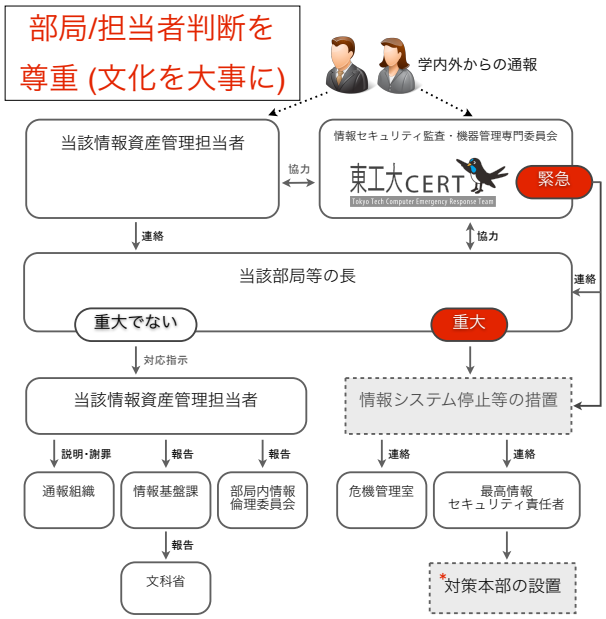

図 2 東工大 CERT の体制

3.1 体制

東工大 CERT の人員構成としては，教職員計 10 名程度と小規模であるが，教員，事務職員，技術職員，ネットワーク管理部門メンバー等連携を取り，全学をカバー出来る体制を取っている．

インシデントのトリアージ，或いは初動対応において，その事案の緊急性を判断することは東工大 CERT が持つ大きな役割のうちの一つである．緊急性の高い事案に関しては，ネットワーク遮断といった緊急対応をネットワーク管理部門と連携して実施し，インシデント発生源の除去や被害の最小化に努める．また，インシデントの重大度については，当該部局等の長が判断することとし，CERT はインシデント分析を通して意思決定のサポートを行う．この様な役割分担により，各部局内の意志や文化を尊重し，かつ，速やかにインシデント対応を進められる体制となっている．

図 2 において，東工大 CERT と関連組織によるインシデント対応の判断フローを示す．

3.2 仮想化基盤

東工大 CERT では内部向けサービスとして OSS のチャットツール，ファイル共有ツール等を仮想化基盤環境上で構築しており，これらのツールを効果的に導入・運用する方法については [6] にて紹介した．これらの内部向けサービスのアクセスログや認証ログを含め，本学で導入しているセキュリティ機器のログの全ては，Splunk に集約管理する体制を採用している．図 3 において仮想化基盤環境の概念図を示す．

Splunk に集約されたログは幾つかの用途において適宜整形・分析し，出力している．図 3 の Splunk の出力側上

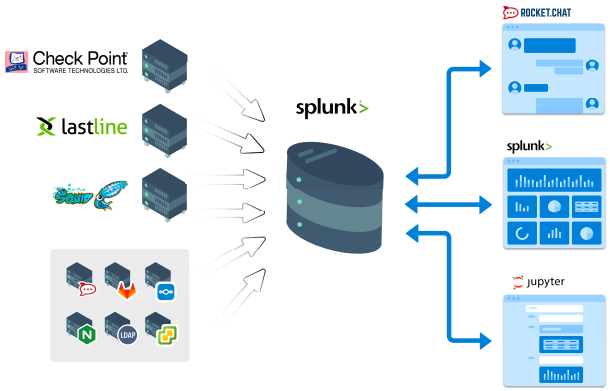

図 3 仮想化基盤環境

段は連携ツールとして利用しているチャットソフトウェアの RocketChat[*3] に対して，アラート等を通知し，CERT 内でインシデント対応を進める際に活用している．中段の Splunk のダッシュボードに関しては，様々な目的に応じてログのフィルタリング，分析をリアルタイム，或いは定期的に行い，その結果をインシデント対応に役立てている．下段は機械学習環境との接続であり，収集したログに対して機械学習の手法の適用により，トリアージにおけるログ解析や，通常時における異常通信の検知等を行える様に解析環境を構築している．

3.3 東工大 CERT におけるインシデント対応事例

3.1 において，東工大 CERT の体制とポリシーについて述べた．ここでは，具体的なインシデント事例をもとに，東工大 CERT のインシデント対応フローを示し，一般的な CSIRT による対応フローと比較する．事例として，サーバの脆弱な設定による不正侵入と，マルウェア感染の二例を挙げる．

サーバ不正侵入

各組織・研究室において，メールやプリンター，ネットワークストレージ等，様々な目的でサービスを公開している場合がある．特にグローバルドメインにおいてサービスを提供する場合は，認証等セキュリティに関する設定に注意する必要があるが，初期設定等，脆弱な状態によるインシデントが引き起こされるケースは少なくない．以下はその一例である．

事象：共同研究者が購入し，設置した NAS への不正侵入．
　　学内外に SSH 攻撃が行われた．
原因：グローバル IP アドレスを利用し，サービスを公開．
　　初期設定を納入業者に任せ，デフォルトパスワードを使用．
対応：ネットワーク管理者により異常通信を検知し，即座に遮断．検知から遮断まで短期間であり，確認の上，重篤な攻撃は無しと判断し，復旧作業，問題解決の確

*3 https://rocket.chat

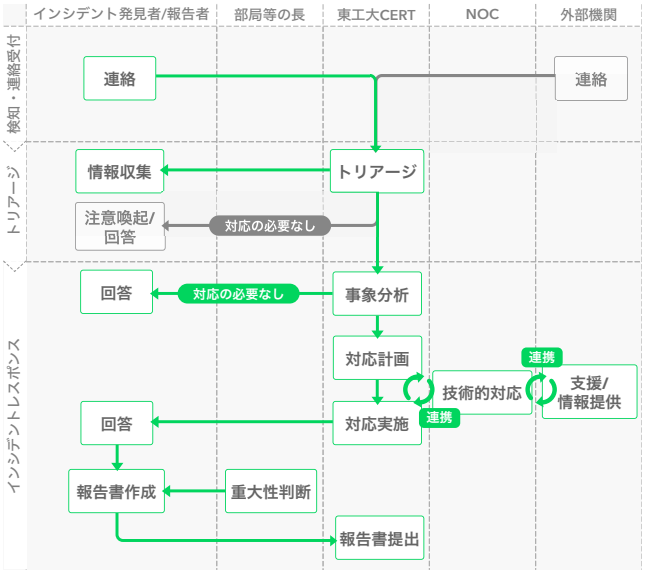

図 4 マルウェア感染案件の対応フロー

認，注意喚起を行った．

マルウェア感染

インシデント分類として，マルウェアのダウンロード・感染（未遂）を含む案件は代表的であり，特にばらまき型等の標的型メールがトリガーとなっていることが多い．以下はその一例である．

事象：当該支線のファイアウォールによりマルウェアのダウンロード通信を検知．当該端末においてアンチウィルスソフトウェアがマルウェアを検知し，削除．

原因：標的型メール内のリンクのクリック．

対応：当該ホストをネットワークから切り離し，ウィルススキャンの実施．関連通信の分析により，マルウェアの特性を把握した上で，二次感染等の被害状況，また，機密・個人情報保持の有無の確認．当該マルウェアとは別のシグネチャマッチしないマルウェア感染の可能性を考慮し，端末の交換，影響範囲内端末のウィルススキャンの実施．当該マルウェアはダウンロード検知後に速やかに削除されたこと，機密・個人情報を保持していないことから，当該部局において重大度は低いと判断した．

3.4 一般的な CSIRT におけるインシデント対応フローとの比較

図 4 において，3.3 で述べたマルウェア感染のインシデント事例について，対応フローを示す．

本案件では，3.1 において述べた様に，東工大 CERT によってインシデント事案の緊急性の判断が必要なため，インシデント報告者とやり取りを行い，トリアージの段階で初動対応と共にその判断を下している．また，事象分析を経て NOC 等のネットワーク管理部門と連携し，技術的な対応を実施し，インシデント報告者に回答する．この段階で，上層部等と連携した非技術的な対応は行われない．報告者が受け取った回答内容をもとに，当該部局等の長，或いは責任者はインシデントの重大度の判断を行い，必要に応じて CERT により更なる被害状況の調査・分析等を行う．更に，文部科学省への報告を目的とし，発生したインシデント案件に関して，指定された様式に従い，報告事項を纏めたインシデント報告書を作成する．本案件の様に，インシデント報告者が学内の構成員である場合，報告者がインシデント報告書を作成するが，報告書における各項目の必要情報の提供等，CERT がサポートする．

これらが，図 1 で示した，一般的なインシデント対応のフローと異なる点である．

東工大 CERT の現状において，セキュリティ機器のアラート等の膨大なインシデントの兆候に対して，次の行動に移行する判断基準・トリガーが乏しく，特にインシデント対応案件とする判断のコストが大きい．これは，大学が他の一般企業等の組織と異なり，様々なインシデントの兆候に対して，即座にネットワーク遮断といった行動に移れない，或いはその様なポリシーの策定が難しい点に起因する．従って，より正確に，かつコストを抑えたトリアージが必要である．

4 章において，特に確度の高い攻撃検知や，調査コストの低減のための，次世代型セキュリティ機器の一つである Lastline の運用体制とログ分析基盤 Splunk との連携について紹介する．

4. インシデント対応における Lastline の活用

本章では，東工大 CERT における Splunk を利用したログ分析基盤と連携させた Lastline の運用方法について，インシデント対応事例に基づいて紹介する．

4.1 Lastline の運用と Splunk による検知イベントの分析基盤

4.1.1 Lastline

Lastline は高度標的型攻撃対策に主眼を置いた，クウドベースでセンサー設置型のセキュリティサービスである．サンドボックス解析機能が強力であり，Lastline 自体は優れたダッシュボード機能を有しており，検知イベント・インシデントに対して，ドリルダウンを行い，通信やマルウェアの動的解析結果等，関連する詳細情報を得ることができる．

4.1.2 Splunk の構成

クラスタ構成

Lastline のログを集約する用途として，専用の Splunk クラスタ環境を構築している．図 5 により，その構成を示す．

構成としては，マスターノード 1 台，ピアノード 3 台，サーチヘッド 2 台から成り，ピアノード 3 台はインデクサクラスタとしてレプリケーションしており，ピアノード

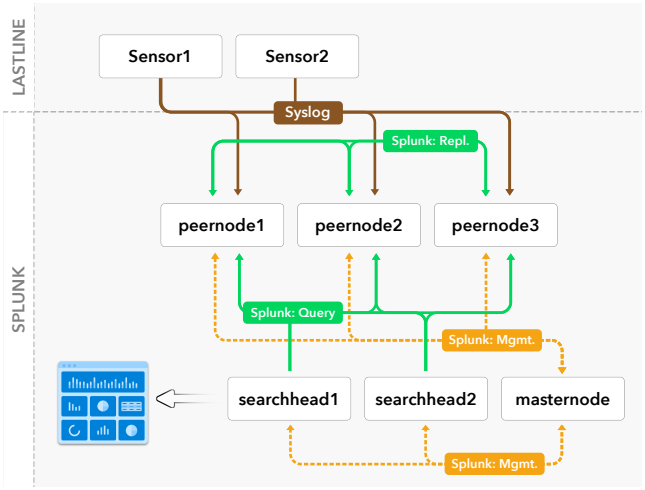

図 5 Splunk のクラスタ構成

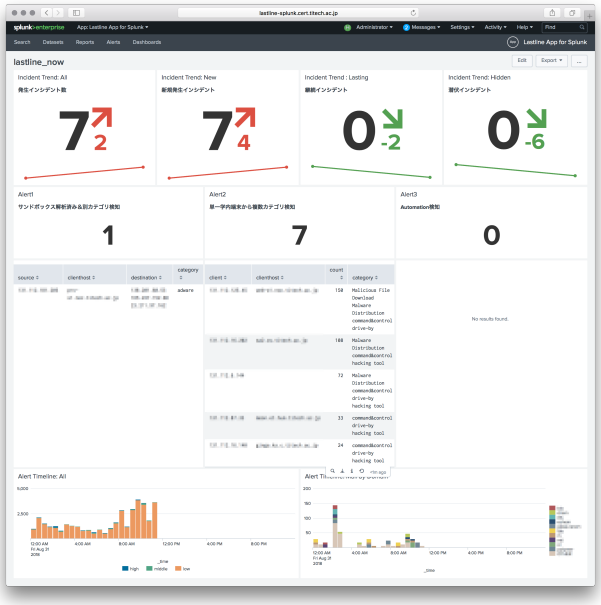

図 6 ダッシュボードによるサポート

はどれかが正常に稼働していれば，ログが欠落することはない．また，インデックス機能とサーチ機能を分離し，複数のインデクサに対する分散サーチを行っている．なお，サーチヘッドクラスタは構築していない．

ダッシュボード

ログ分析・調査等の SOC オペレータの作業コストの低減と，事務担当等，非技術系職員に対しても適切・有用な判断の支援を目的とし，Splunk のダッシュボード機能を利用している．図 6 に Lastline のログに対するダッシュボードの一例を示す．

図 6 の上段では，過去 24 時間のイベント件数の推移を表示し，中段では Lastline により検知された，注目すべきインシデント情報をリストアップしている．下段では，検知イベントのスコアと時間的な傾向，メール攻撃のスコア及び所属別の受信者数の時間的な傾向を表している．

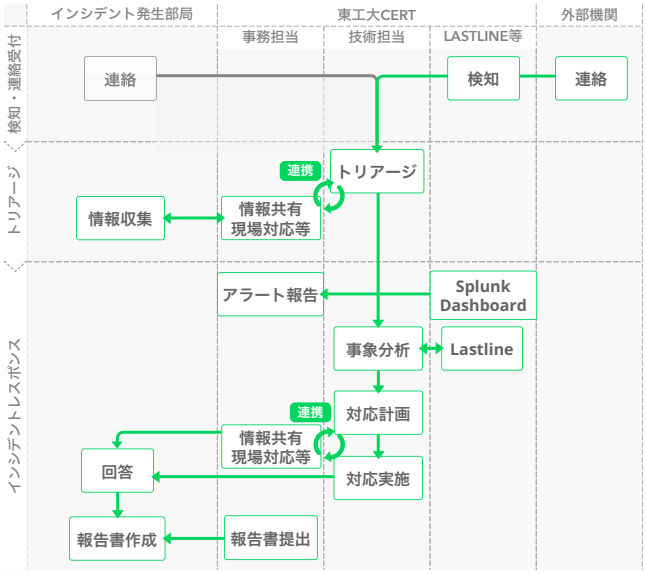

図 7 Lastline・Spkunk を利用したインシデント対応フロー

4.2 Lastline の運用を例にしたハンドリングフロー

本節では，4.1 節で述べた Lastline と Splunk によるインシデント分析基盤を利用し，どの様にインシデント対応を進めているか，一つの案件を題材にして説明する．下記のインシデント案件は，Lastline，また，Splunk にて作成したダッシュボードによるイベント検知を利用して対応が実施された．

事象：アドウェア判定されたバイナリのダウンロードを検知．バイナリの危険度が非常に高いわけでないが，数が比較的多い．初動対応後においても継続的な C2 サーバへの通信を確認し，これらは Splunk ダッシュボード上でも確認された．

原因：データ交換のために用いた USB メモリ経由，或いは，ダウンロードしたソフトウェアにウィルスが組み込まれていた可能性が高い．

対応：当該 PC のネットワーク接続を遮断すると同時にウィルススキャン・駆除．研究員個人の PC を使うことを禁止し，大学から新たに PC を用意した．不明なソフトウェアを無許可でインストールすることを禁止し，必要なソフトウェアのインストールはネットワーク管理者の監視下で行うこととした．

図 7 において，本案件の対応フローを，CERT 内のメンバ間の連携，更に Lastline, Splunk によるインシデント分析基盤の利用手順に焦点を当てて示す．

本案件のイベントは，Lastline の検知イベントとして Splunk ダッシュボードにおいても補足されていたものであり，外部機関からの報告もあったため，インシデント対応の優先度が高いものとして扱った．Lastline のイベント解析や，他の機器のログ分析は技術担当者が行い，その結果は非技術系職員である事務担当者に共有される．事務担当者は学内の当該者と連絡を取り，共有されたインシデン

ト事案の情報を用いて，場合によっては現地で初動対応を行う．本案件においては，当該ホストのネットワーク切り離し等の初動対応後，再び不正通信が観測されたが，それは Splunk ダッシュボードのアラート監視により**事務担当者**より報告が上がったものである．本対応は，初動対応と同様にして，技術担当者，事務担当者が連携を取り，報告書の作成までサポートを行う．

以上で示した CERT メンバ間の連携について，インシデント対応，或いは情報管理の一部として，Gitlab[*4], RocketChat を利用しており，3.2 節で紹介した OSS 基盤環境を活用したものである．インシデント対応中の情報を段階的に纏め，情報を共有するために試行的に Gitlab の issue 機能を利用しているが，非技術系職員である事務担当者の利用・操作コスト等，現状課題が多く見られる．これについては 5.2 節で少し議論する．

5. インシデント対応の分析と自動化

本章では，これまでに示したインシデント対応の例を基に，本学におけるインシデント対応の特徴を分析し，自動化に向けた議論を行う．ここで言うインシデント対応の自動化とは，対応の成熟された手順書，或いは様々なイベントに対する行動・判断のルール集といったものを活用し，対応フローを正規化して自動的・機械的に対応出来ることを目指すものである．このためには，自組織におけるインシデント対応の特性を把握し，対応フローの基本構成要素を整理する必要がある．

5.1 本学におけるインシデント対応の整理

本論文では，3.3,4.2 節にて，本学におけるサーバの不正侵入，マルウェア感染の対応案件の例を示した．これらの案件に対して，対応中の各イベント・行動に対して，何がトリガーに，或いは，判断基準になっていたか，また，その際に分析・収集すべき必要な情報はどの様なものであるかを整理する．

表 1 において，サーバ不正侵入の例について情報を整理した．事案の発生源はネットワーク機器のアラートであり，通信の性質からネットワークの即遮断に至っており，トリアージとしては最も優先度が高く処理されている．初動対応後は，表 1 にある情報を把握し，事案が再び発生しない様に安全策を取った上で復旧作業を行い，必要情報を集めて報告書を作成している．

同様に表 2 において，マルウェア感染の案件について纏めた．事案の発生源は，Lastline の検知イベントと共に，外部機関からの不正通信の報告もある．外部機関からの報告は，攻撃の確度と関連し，インシデント対応に移行するか否かの判断の際の重要な要素である．また，マルウェア感染の案件については，マルウェアのダウンロードが完遂されたか，そうであれば二次通信が発生しているかを確認し，内容に応じて初動対応を実施する．初動対応後は，サーバ不正侵入の案件と同様に，表 2 にある情報を収集し，被害状況，事案発生原因を把握し，復旧作業等の対応を行った後，報告書を纏める．

インシデント対応時に必要な情報のまとめ

更に，対応フローの各フェーズにおける収集・分析すべき必要情報についてより詳しく整理する．対応フローにおける行動がどの様な情報が入力として与えられた際に推移するか，即ち，トリガーと直結する必要情報に着目すると，各必要情報を繋いでいくことで全体のフローを捉えることが出来る．

図 8 において，対応の各フェーズに対して，分類された必要情報と，それぞれの分類のうちの詳細な必要情報を示す．

詳細な必要情報に関しては，インシデントの分類により大きく異なるが，ここでは中分類の必要情報毎に纏めている．また，この中分類の必要情報には図 8 の通り，依存関係があることが分かる．ここで示した中分類の必要情報を依存関係に従って収集することにより，ある程度の対応フローは定まり，大まかな対応タスクの役割分担等も可能になる．

5.2 インシデント対応の自動化に向けて

羽角ら [7] は，トリアージにおける業務プロセスを整理し，特に，被害端末を推定した上での関連ログの収集と，ログ分析によるインシデントの影響範囲の把握を目的としたトリアージ支援システムを提案している．この様な，インシデント対応の自動化，或いは対応コストの低減のためのシステムには，正規化されたインシデント対応マニュアル，対応情報等の管理システム，組織の構成に応じた通信・データの解析手法等が重要な構成要素となっている．

対応のマニュアル化

上で述べた様に，インシデント対応の際に収集すべき情報を整理することで，対応フローの構成の大枠が定まる．しかし，必要情報の “インシデント分類”, “当該インシデントの二次的な通信・イベントの有無” 等を分析・収集するためには，ネットワーク・セキュリティ機器やインシデント分類の別，或いはそれらの組み合わせに依って取るべき行動を決定すべきであり，更なる細分化したマニュアルが必要になる．

成熟した対応マニュアルはシスコシステムズの CSIRT では “プレイブック” と呼ばれている [1]．プレイブックはセキュリティ機器のアラートや不正な行動等あらゆるイベントに対し，対応手順や実施目的，対応手法の説明や，分析結果の解釈の仕方等が記述され，未熟なセキュリティエンジニアが同様のイベントに対応する際の助けとなる様に

[*4] https://gitlab.com

表 1 インシデント対応中の判断基準・必要情報（サーバ不正侵入）

フェーズ	イベント・行動	トリガー	判断基準	必要情報
検知/連絡受付	攻撃通信検知	アラート	—	—
トリアージ	ネットワーク遮断	攻撃通信検知	学外ホストへの攻撃	攻撃通信範囲・量
ハンドリング	被害状況・原因解明	初動対応	—	当該端末の情報・運用状況 攻撃通信観測期間 機密情報保持の有無
	復旧作業	被害状況・原因解明	十分な安全性	インシデント発生原因
	報告書作成	一次対応	—	部局重大度判断 再発防止策

表 2 インシデント対応中の判断基準・必要情報（マルウェア感染）

フェーズ	イベント・行動	トリガー	判断基準	必要情報
検知/連絡受付	不正サーバへのアクセス	アラート，外部機関報告	—	—
トリアージ	情報収集	不正通信検知	詳細情報の必要性	マルウェアのダウンロード， 二次通信の有無
	初動対応	情報収集	マルウェアのダウンロード 外部機関による報告	ログの詳細情報 —
ハンドリング	被害状況・原因解明	初動対応	—	当該端末の情報・運用状況 マルウェアダウンロードの経路 機密情報保持の有無， 情報漏えいの可能性 当該マルウェアの特性， 二次感染の可能性
	復旧作業	被害状況・原因解明	十分な安全性	インシデント発生原因
	報告書作成	一次対応	—	部局重大度判断 再発防止策

纏められたものである．組織の形に依り，プレイブックの内容は当然異なり，プレイブックが整備されて活用できるまでには，相当数のインシデント対応とそのフィードバック・解析を行う必要がある．

Lastline の検知イベントに対する，Splunk によるログ解析基盤を利用した案件においては，ダッシュボードの利用により，不完全ながらもシンプルなプレイブックの作成に繋がる点がある．ログ分析において，不正な振る舞いや異常通信等の実態を把握することは困難であり，複雑な検索を行う必要がある．ダッシュボードの作成は，その様な複雑さを隠蔽し，非技術系職員に対しても検索結果の意味・目的を共有することで，対応を実施出来る．

他の機器によるログも含めた解析基盤を構築し，プレイブックの運用を実施することは，対応手順のマニュアル化によるインシデント対応の自動化の達成により近づく．

インシデント対応自動化のための基盤構築について

近年ではインシデント対応管理システムとして，OSS, 商用ソフトウェアに限らず様々なものが利用されている．[1] のプレイブックの管理には Bugzilla[*5] が利用されており，他のバグ・課題トラッキングシステムである JIRA[*6] や Redmine[*7] を利用しているケースもある．

[*5] https://www.bugzilla.org
[*6] https://www.atlassian.com/software/jira
[*7] http://www.redmine.org

インシデントの対応手順を細分化し，それらの依存関係を適切に定義し，チーム内で連携を取って各タスクを実施するためには，上記の様なトラッキンシステムが必須となる．細分化された手順書は，プレイブックの様に，攻撃手法や自組織の環境の変化に応じて更新され，手順書やインシデント対応自体も対応後には都度評価され，手順書の充実化を図らなければならない．この様な要件を満たし，かつ，非技術系職員等も低コストで扱えるシステムの導入・運用が必要である．

機械学習手法の適用について

インシデント対応において，あるイベントに対する通信内容が悪性であるかの判断，攻撃であればその確度等を測るコストは膨大で省力化が必要である．また，新種のマルウェアによる通信の異常検知等，シグネチャマッチングでは対応出来ない場合も多い．機械学習手法の適用により，攻撃，或いは悪性通信・データ等を判定することで，上記の課題に対して部分的な解決策が与えられる．特に，確度が比較的高いと判定される攻撃に対しては，適切な機械学習モデルの適用により，判断のコストを下げ，機械的な対応手順を割り当てることにより，一部のインシデント対応の自動化が可能となる．

Splunk によるログ分析基盤では, Splunk Machine Learn-

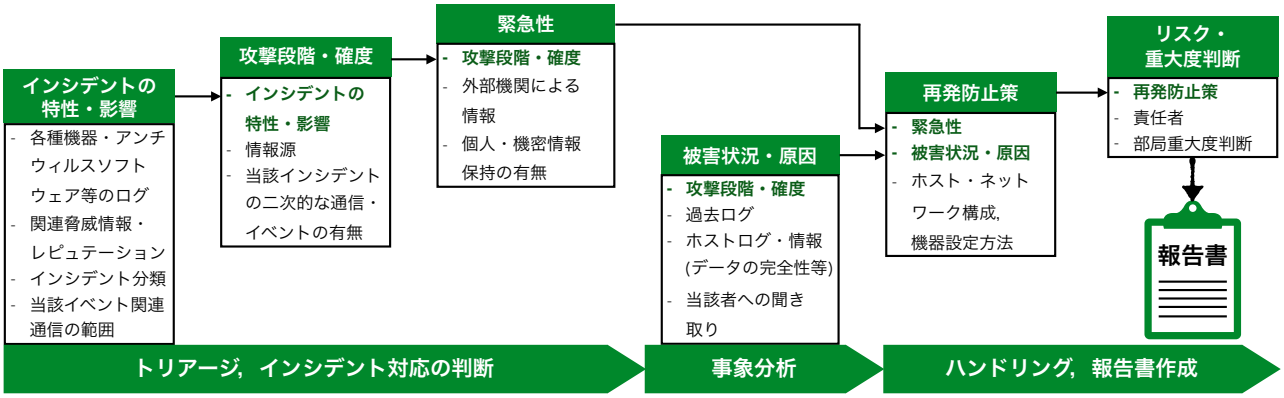

図 8 インシデント対応中の必要情報と依存関係

ing Toolkit[*8] を利用した解析環境を用意し，（複数のネットワーク・セキュリティ機器の）ログデータに単純な回帰分析やクラスタリング等を適用し，トリアージや事象分析の支援となる効果的な解析手法の試行的な開発・実験を行っている．

また，4.1.2 節で紹介したダッシュボード（図 6）において，“Alert3 Automation 検知” のエリアでは，簡単な相関分析や統計値の計算により，例えば C2 サーバへの定期通信等，不正な通信の疑いのあるものの件数をリアルタイムに計算し，表示している．

6. おわりに

本論文では，東工大 CERT におけるインシデント対応について，具体的な案件事例を紹介し，インシデント対応の基本要素である，対応中のイベント・行動のトリガー，判断基準，また，収集・分析すべき必要情報について整理し，対応フローがどの様に正規化出来るか示した．また，整理されたインシデント対応のパターン・基本要素について，対応のマニュアル化がインシデント対応の自動化に繋がることを示唆した．更に，高度標的型対策機器の一つである Lastline の運用と，Splunk を利用したログ分析基盤との連携について述べ，Splunk のダッシュボードを利用した対応フローが，効果的な対応手順書の作成に繋がる可能性を示した．

今後の課題として，インシデント対応の詳細な対応手順を作成するために，インシデント対応の評価の実施，対応の解析により，それぞれの事象の特性や依存関係を明らかにする．そのためには，インシデント対応管理システムが必要であり，課題トラッキングシステム等を導入し，5.1 節で示した，大まかに正規化された対応フローに従い，対応管理を行い，より詳細なフェーズの解析を実施する．また，その中で，CERT の省力化，対応の自動化に繋がる機械学習手法の適用方法について模索する．

[*8] https://splunkbase.splunk.com/app/2890/

謝辞 本研究の一部は，JST, CREST, JPMJCR1783, また，JSPS 科研費 JP15K00115 の支援を受けたものである．

参考文献

[1] Bollinger, J., Enright, B. and Valites, M.: *Crafting the InfoSec Playbook*, O'Reilly Media (2015), 飯島 卓也，小川 梢，柴田 亮，山田正浩（監訳），谷崎 朋子（訳）：実践 CSIRT プレイブック — セキュリティ監視とインシデント対応の基本計画, O'Reilly Japan, 2018.

[2] Brennan, T. and Jolo, J.: OWASP Top 10 Considerations For Incident Response (2015), https://www.owasp.org/images/9/92/Top10ConsiderationsForIncidentResponse.pdf, Accessed: 2018-09-05.

[3] Scarfone, K. A., Grance, T. and Masone, K.: SP 800-61 Rev. 1. Computer Security Incident Handling Guide, National Institute of Standards & Technology (2008).

[4] 一般社団法人 JPCERT コーディネーションセンター：インシデントハンドリングマニュアル (2015), https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0_20151126.pdf, Accessed: 2018-09-05.

[5] 一般社団法人 JPCERT コーディネーションセンター：インシデント報告対応レポート [2018 年 4 月 1 日 2018 年 6 月 30 日] (2018), https://www.jpcert.or.jp/pr/2018/IR_Report20180712.pdf, Accessed: 2018-09-05.

[6] 森 健人，松浦知史，金 勇，友石正彦：オンプレミスで実現する業務効率化のための OSS 基盤環境構築，情報処理学会研究報告 (2016).

[7] 羽角太地，島 成佳，高倉弘喜：効率的なインシデントハンドリングのためのトリアージ支援システムの提案，2017 年暗号と情報セキュリティシンポジウム (SCIS) (2017).