Vol.2019-IOT-47 No.4
Vol.2019-SPT-35 No.4
2019/9/19

セキュリティ維持活動の情報を活用する インシデント対応進捗管理システム

岩井亮太[1]　渡邉英伸[2]　相原玲二[2]　近堂徹[2]　西村浩二[2]

概要：情報セキュリティインシデント発生時には，その影響を最小限に留めるため迅速な対応が求められる．しかし，インシデント対応においては，状況の把握や調査など CSIRT 構成員と利用者とのやり取りが多く含まれるため，対応時間の増加の原因となっている．本研究では，ネットワーク運用のための端末管理情報の事前収集に加え，定期的に行なわれている教育や訓練などのセキュリティ維持活動で収集・蓄積される情報の活用と対応状況の可視化によって，対応時間の短縮と確実な進捗管理を支援するインシデント対応進捗管理システムを提案する．

キーワード：インシデント対応，CSIRT，進捗管理，セキュリティ維持活動，支援システム

An Incident Response Management System using Security Portfolio collected by Security Maintenance Activities

RYOTA IWAI[†1]　HIDENOBU WATANABE[†2]
REIJI AIBARA[†2] TOHRU KONDO[†2]
KOUJI NISHIMURA[†2]

Abstract: When an information security incident occurs, prompt response is required to minimize the impact. However, incident response involves a lot of communication among CSIRT members and users, such as understanding and investigation of the situation, which increase incident response delay. In this paper, we propose an incident response management system which supports the improvement of the delay and reliable progress management by using network management information of PCs and devices, security portfolio collected and accumulated by security maintenance activities such as periodical security education and incident response training. The system also supports visualization of the incident response status.

Keywords: Incident response,　CSIRT,　Progress management,　Security portfolio,　Support system

1. はじめに

現在セキュリティに関する事故が頻繁に起きている．特に組織内でのインシデント発生においては機密情報が漏洩する事例もいくつかある［1］．インシデント対策のためには事前対策も大切ではあるが，インシデントによる被害を100%防ぐということは不可能であるため，初動対応が重要である．インシデント対応にかける時間が長ければ長いほど被害の拡大につながることになる．迅速な対応のためには初動対応時の情報の収集が重要課題になる．

大学においては組織内ネットワークに接続される機器に関する情報の管理は個人に委ねられており，組織的な管理の徹底は難しい．個人が所有する端末を自由に大学内に持ち込むことができ，教育研究活動をはじめとする諸活動のためにネットワーク接続できる場合がほとんどである．認証により利用者の把握は可能なものの，端末状態や利用形態までを大学で管理することは現実的ではない．このような場合，組織の CSIRT はインシデントの初動対応として，該当端末の特定，該当端末利用者または管理部局等の担当者の連絡先の調査を行い，該当端末の調査依頼を行うため，対応に時間がかかってしまう．

広島大学では，日々のネットワーク運用で，ネットワークに接続された端末の利用者認証情報の把握，部局ネットワーク等の管理責任者や担当者情報の把握，ネットワーク運用で発生するログの蓄積等を行っている［2］．これらの情報は，インシデント発生時における通信発生の有無や利用者の把握，関係者への連絡に活用されている．さらに，広島大学では迅速な対応を行うためにインシデント対応訓練や新入生向けの初期講習会などのセキュリティ維持活動を定期的に行っている［3］．インシデント対応訓練ではインシデント発生の際に該当端末の情報を一般利用者が調査する訓練を行っている．インシデント対応訓練や初期講習会などで収集されている情報には，インシデントが発生した際に必要とされている情報が含まれているが，実際のインシデント対応時には活用されていない．これは，多くの組織が抱える共通の課題である．

ネットワーク運用のための端末管理情報の事前収集に加え，定期的に行なわれている教育や訓練などのセキュリティ維持活動において収集・蓄積されている情報を活用することで，インシデント対応時間の短縮が期待できる．そこで，本論文では，はじめにインシデント対応に必要な情

1 広島大学 大学院総合科学研究科
Graduate School of Integrated Arts and Sciences,　Hiroshima University.
2 広島大学 情報メディア教育研究センター
Information Media Center,　Hiroshima University

Vol.2019-IOT-47 No.4
Vol.2019-SPT-35 No.4
2019/9/19

報を調査し，収集のタイミングについて整理する．この結果とセキュリティ維持活動で収集可能な情報がどれだけインシデント対応に利用できるかについてまとめる．これらの考察をふまえ，収集する情報をフェーズごとに記録し，インシデント対応の進捗状況を可視化することで，対応時間の短縮と確実な進捗管理を支援するインシデント対応進捗管理システムを提案する．

提案システムは，平常時には主に一般利用者が所有する端末の情報管理のためのシステムとして利用する．情報の収集にはセキュリティ維持活動の情報も含めて蓄積する．これらの情報は大学内に存在する端末の資産管理にも活用できる．また，インシデント発生時には平常時から管理された情報をそのままインシデント発生時の端末特定や状態把握に利用することで，初動対応の迅速化を図ることができる．さらに，これらの情報を含めてインシデントハンドリングの進捗管理を行うことで，CSIRT と一般利用者，関連部署との間での迅速かつ円滑なインシデント対応を支援可能なシステムを構築することができる．

2. インシデント対応手順と関連研究

2.1 インシデント発生時の対応手順

インシデント対応時に行うべき内容について JPCERT コーディネーションセンター（以下「JPCERT/CC」）からは「CSRIT ガイド」[4] と「インシデントハンドリングマニュアル」[5]，独立行政法人情報処理推進機構（IPA）（以下「IPA」）からは「情報セキュリティセミナーインシデントマネジメント」[6] が一般公開されている．

「CSIRT ガイド」は自組織内に CSIRT を構築しようと考えている CIO（Chief Information Officer，最高情報責任者）などの経営層や CSIRT メンバーになる可能性のある方を対象に，CSIRT とはどのような組織でどのような活動をするのか，何が必要であるかについて解説してある．また，ここで述べられているものは「推奨」レベルのものであり，各組織は本資料を参考に自組織にとってふさわしい CSIRT を構築することが期待されている．

「インシデントハンドリングマニュアル」は，CSIRT が自組織で発生した情報セキュリティに関するインシデントに対して行うべき活動の内，発生時から解決までの一連の処理の対応マニュアルを作成する際に参考資料として使うことを目的とした資料である．図 1 にインシデント対応フローを示す．本マニュアルでは，この対応フローにおける各フェーズ（検知からトリアージ，インシデントレスポンス）での実施事項についてまとめられている．

「情報セキュリティセミナーインシデントマネジメント」は，効果的なインシデント対応を行うために平常時における事前準備として必要なことについてまとめている．

各資料には迅速なインシデント対応に必要とされる情報について列挙されており，これらの情報は組織におけるインシデントの初動対応で収集すべき情報と読み替えることができる．本論文では，これらの情報を平常時より収集しシステムで管理することを目的とする．それぞれの資料で列挙されている項目については 4.2 で述べる．

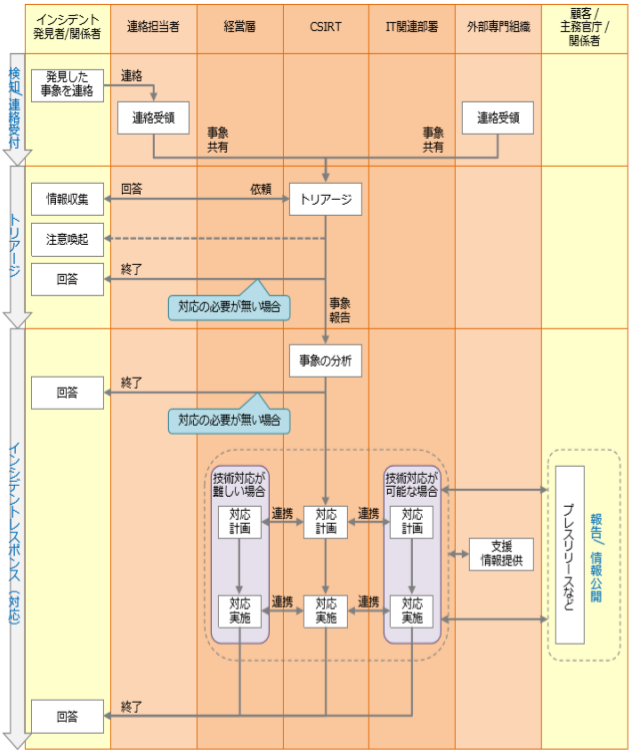

図 1　インシデントハンドリングマニュアルにおけるインシデント対応フロー［5］

2.2 先行研究

鳥取大学［7］ではインシデント対応に必要な情報として 49 項目を挙げている．これらの情報は，インシデント発生後に対応状況に応じた情報を収集し，システムに入力することになっており，CSIRT 間の情報共有や対応状況の記録もこのシステム上で管理している．

東工大［8］では将来多様なインシデントが発生したときに過去の対応の記録を参照することを目的に，インシデント対応時に情報を蓄積していくシステムの実装を行っている．このシステムはインシデント対応フローを 4 つのフェーズに分け，それぞれのフェーズで蓄積すべき情報を定義し，CSIRT の作業負荷及び心理的負荷を軽減しながらも情報の蓄積を可能としている．これらの先行研究はインシデント発生後の CSIRT の活動を効率化することが目的であり，一般利用者の平時の活動を含むインシデント対応の効率化は対象としていない．

3. 広島大学における取り組みと課題

3.1 インシデント対応手順

広島大学では図 1 の対応フローを参考にインシデント対応を行っている．以下に各フェーズでの実施内容について簡単に示す．

1. 検知/連絡受付
① 組織内調査もしくは NII-SOCS［9］等の外部通報先から通知による検知
② 該当端末の特定と通信制限を実施，情報の記録
③ 該当端末の所有者に対して端末情報と被害状況の調査を依頼，所有者は該当端末の調査と結果の報告

2. トリアージ
① 検知情報と該当端末の所有者からの調査結果よりトリアージを行う．事象の状況に応じて，3-1 のトラブル調査か 3-2 のインシデント調査に分かれる

3. インシデントレスポンス（対応）
3-1. トラブル調査
① 該当端末のキャッシュの初期化，デバイスの初期化を実施し通信制限を解除
② 該当端末の OS やウイルスパターンファイルを最新に更新
③ 報告書の作成

3-2. インシデント調査
① 該当端末の状態保全
② 該当端末の詳細調査
③ 報告書の作成

広島大学では学内ネットワーク機器の不正アクセスの予兆検出や，インシデント発生時の一般利用者の追跡などの目的で日々のネットワーク運用で発生するログの蓄積・参照ができるシステムを実装している．これらのネットワークログはインシデント発生時に事態の把握するうえで重要な情報が多く含まれる．蓄積ログには例えば接続開始時間，送信元 IP アドレス，宛先 IP アドレスなどがある．また，DHCP ログや L3 スイッチの MAC アドレステーブルからは端末の IP アドレスと MAC アドレスの対応関係，Web 認証ログからは端末の MAC アドレスと利用者 ID を対応づけることができる．

NII-SOCS などの外部組織からの通知を受けた後，CSIRT は該当端末や該当者の特定のためにネットワークログの分析を行う．その後，CSIRT が該当者に該当端末とその被害状況について調査を依頼する．通知を受けた該当者は依頼に対して端末の調査を行い，その調査結果を CSIRT に報告する．最終的に，CSIRT は検知情報や該当者からの報告書をもとにトリアージを行い，事象の状況に応じた対応を行う．対応後は，最終報告書を作成しクローズする．この間，CSIRT と該当者および該当部局のネットワーク管理者やセキュリティ担当者等との迅速かつ的確な意思疎通が求められる．

3.2 セキュリティ維持活動

セキュリティ維持活動とは組織内で平常時に行われているセキュリティ対策のための活動のことを指す．特に広島大学では年に一度行われる全構成員向けのインシデント対応訓練，新入生向けの必携パソコン初期講習会，2 年次以降の構成員向けの年度更新（自己点検），大学院生向けの PC 所有調査などがこれにあたる．インシデント対応訓練では実際にインシデントが発生した場合を想定し，一般利用者が取るべき対応について端末の調査と報告の手順に関する訓練を行っている．具体的には，一般利用者は訓練期間中に所有する端末に関する構成情報やセキュリティ状態を CSIRT に報告する．また必携パソコン初期講習会では，入学時に学生自身が保有するパソコンの初期設定やセキュリティ対策ソフトウェアのインストール作業を行い，講習会後の端末の状態を報告する．これらのセキュリティ維持活動は全学レベルで行われており，収集した情報の多くが組織的に蓄積されている． 自己点検では一年間を振り返り，必携 PC のセキュリティ状態を確認や情報リテラシーを再確認するものである．PC 所有調査は大学院生が持ち込む PC の情報を収集するためのものである．

インシデント対応訓練や必携パソコン初期講習会において，具体的に一般利用者に対して依頼している調査項目は以下のとおりである．なお，自己点検と PC 所有調査は初期講習会と調査項目が同様であるため本論文では省略する．

＜インシデント対応訓練での調査項目（全 17 項目）＞

- 該当するコンピュータについて
  - メーカー，型番，OS のエディションやバージョン，システムの種類，プロセッサ情報など
  - 該当するコンピュータの使用目的 について共同利用の有無や利用用途（研究利用，教育利用，事務利用等）など
- 該当するコンピュータに保存されている情報について
  - 個人情報などの重要情報の有無など
  - 該当するコンピュータの使用状況について OS の最終更新日，ウイルス対策ソフト名，パターンファイルの最終更新日，最終スキャン日など
  - 該当するコンピュータのファイルの異常について異常の有無，異常があった場合の具体的な状況など
- 指摘された原因について
  - 該当インシデントに対する思い当たる事象など
- ウイルススキャンの検知結果について
  - フルスキャン時の検知の有無，検知された場合のウイルス名や駆除状況など

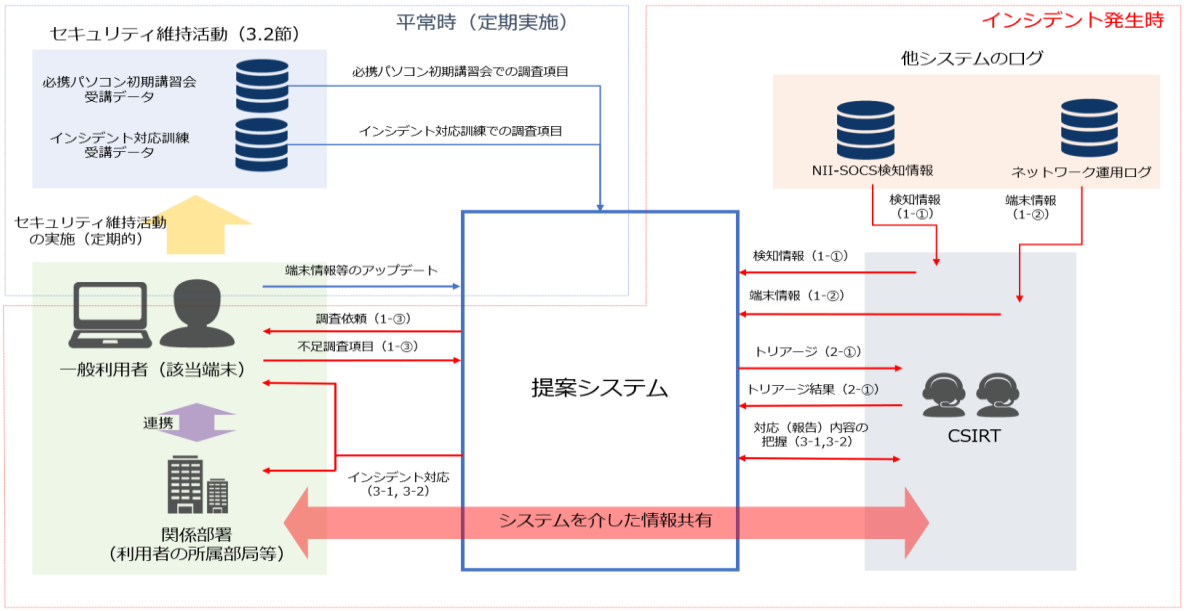

図 2　提案システムを用いた平常時からインシデント発生時における情報の流れ

＜必携パソコン初期講習会での調査項目（11 項目）＞

- OS の種類とバージョン
- OS の bit 数
- バッテリの駆動時間
- 学内ネットワークへの接続の可否
- OS の自動アップデート設定状態
- ウイルス対策ソフトのインストール状態
- ウイルス対策ソフトの自動アップデート機能の設定状態
- ウイルススキャンの実行結果
- Microsoft Office（Word，Excel，PowerPoint）のインストールの可否
- 学内プリンタへの出力可否

3.3 現状の課題

対応時間の短縮と確実な進捗管理を支援するために 2 つの課題を示す．

1 つ目の課題は，広島大学 CSIRT の活動の妥当性を客観的に確認可能にすることである．広島大学がインシデント対応時に集めている情報が一般性を持たず，必要十分でない場合，トリアージの的確な判断が不可能である．そのため，対応フローをベースにいつ・だれが・何の情報を収集すべきかといったポリシーを定義し，CSIRT メンバー全員が収集すべき情報の妥当性を確認できることが必要である．

2 つ目の課題は，平常時に行っているセキュリティ維持活動の情報をインシデント発生後に活用を可能にすることである．2 章の調査資料では平常時に CSIRT が行う業務として対策としてインシデントの未然防止策やインシデント検知後の対応手順の予行演習などが示されている．広島大学においてはその業務はセキュリティ維持活動としてすでに行っているものの，インシデント発生後にどの様に活用できるかは整理されていないため，一般利用者に再度調査をさせてしまっている現状がある．セキュリティ維持活動の情報がいつのタイミングで活用できるかについて明確にする必要がある．

4. インシデント対応進捗管理システム

4.1 課題に対する解決案

1 つ目の課題においては，本研究ではまず，2.1 で述べた調査資料をもとに，平常時から行っておくべきことについてとインシデント発生時に行うべきことについての整理を行った．整理の方法はフェーズごと（平常時，検知，トリアージ，対応）に分けて分類を行った．これは平常時からインシデント対策としてやっておくべきこと，平常時から収集が可能な情報についてと，インシデント発生時にいつ，どのような情報を収集すべきかを明確にするための整理である．次にこの結果をもとに広島大学での平常時からインシデント発生時における情報についても同様にフェーズごとに分類を行い，各フェーズでどの情報がどれだけ集められているかを整理した．

2 つ目の課題においては，セキュリティ維持活動であるインシデント対応訓練，初期講習会で収集されている情報がインシデント発生時にどのフェーズでどの情報が活用されるかが明確にした．

2 つの課題に対して行った解決案の結果を表 1 に示す．表 1 の左では JPCERT/CC や IPA が示している平常時とインシデント発生時に行うべき要件についてフェーズごとに分類した結果である．表 1 の右では広島大学の各フェーズ

図 3　CSIRT がログインした場合の提案システムの画面案

で取り扱っている情報の分類の結果である．この表では色分けによりだれがいつのタイミングで集める情報であるかを示した結果である．緑文字は CSIRT がそのフェーズで収集すべき情報である．青文字は CSIRT が収集済みの情報である．赤字と黒字については一般利用者が調査すべき情報であり，黒字は平常時やインシデント発生時にその都度情報を一般利用者集める情報である．赤字については平常時のセキュリティ維持活動で蓄積している情報が活用できる情報である．紫文字はインシデント発生時に一般利用者が収集済みの情報である．例えば表では平常時のフェーズでの予行演習を定期的に行う要件に足しては広島大学では対応訓練のセキュリティ活動で要件を満たしている．このように各要件に対して広島大学のセキュリティ維持活動やネットワーク運用のための端末管理情報などが要件を満たしていることで，広島大学で集めていた情報が一般性を持ち，集めるべき情報に漏れがなく必要十分であることが客観的に確認できる．また，セキュリティ維持活動で集めた情報がインシデント発生後のどのフェーズで活用されるかも確認できる．例えば，平時の初期講習会で収集している OS のバージョンやインシデント対応訓練で収集しているメーカーや型番などの情報はインシデント対応の検知フェーズの該当端末調査と同じ情報であり，さらに赤字で示すことによってその情報はインシデント発生後に収集不要であることが確認できる．日常的に行われている取り組みを活用することで，一般利用者にとっては該当端末の調査時に必要とされる作業が軽減され，調査報告にかかる時間の短縮に貢献する．CSIRT は，フェーズごとに収集すべき情報を確認しながら確実な対応を行うことができ，迅速な対応につながる．

4.2 システム構成

4.1 で述べた解決策について本研究では提案システムでインシデント対応に必要な情報を一元的に管理することで解決を図る．以下に提案システムの構成について述べる．

図 2 で提案システムを用いた平常時からインシデント発生時における情報の流れを示す．平常時に一般利用者がセキュリティ維持活動に参加することで，そこで蓄積された情報が提案システムに自動的に蓄積される．インシデント発生時には CSIRT は NII-SOCS の検知情報やネットワーク運用ログなど対応時に必要な情報をその都度提案システムに蓄積を行っていく．該当端末の所有者である一般利用者はセキュリティ維持活動への参加により端末情報の一部が既に提案システムに蓄積されている状態にある．そのため一般利用者は CSIRT の依頼に対して，すべての項目を調査する必要がなくなり，対応時間を短縮することができる．

図 3 で CSIRT がログインした場合の提案システムの画面案を示す．文字の色分けについては表 1 と同じである．表 1 の整理の結果より，収集済みの情報とこれから収集しないといけない情報が可視化されることにより進捗管理も容易となる．これから収集しないといけない情報については空白になっているため CSIRT はその情報を調査する．また一般利用者がインシデント発生時に調査する項目は黒字の部分の空白だけを埋めればよいことがわかる．ここで，赤字で示している項目は平常時にセキュリティ維持活動で収集できる項目を示している．一般利用者が定期的に行われるセキュリティ維持活動に参加しておくことでインシデント発生時に調査すべき項目のうち赤字の項目は蓄積された情報を活用でき，調査にかかる時間を短縮することができる．

5. 考察

本論文では，インシデント対応に必要な情報な情報の整理と平常時に行われるセキュリティ維持活動の活用法について調査を行った．そこで，インシデント対応時に必要とされる情報を一元的に管理する提案システムが導入されることで，広島大学のインシデント対応手順がどのように変化し，負荷が軽減するかを考察する．

検知 1-③（該当者への調査依頼と該当端末の調査）については 3.2 で述べたセキュリティ維持活動で収集した情報の活用により，一般利用者は表 1 の該当端末調査結果の 17 項目のうち最大 12 項目（表 1 の赤字の項目）は蓄積されている情報をそのまま活用でき，調査にかかる時間を短縮することができる．さらに，該当端末の所有者である一般利用者が迅速に調査の報告を行えば，CSIRT はインシデント対応の中で一般利用者とのやり取りにとられる時間を短縮につながり，次のフェーズへ速やかに移ることができ迅速な対応が可能となる．

インシデントレスポンス（対応）3-1-③，3-2-③（報告書の作成）についても効率化できる可能性がある．現状は事象の分析や一般利用者からの報告で収集された情報を再度別のシステムに情報の入力を行っているが，提案システムによって集まってきた情報をもとにシステムが自動的に報告書に必要な情報を抽出し作成することで CSIRT 手間を省くことができ，対応時間の短縮につなげることができる．

6. まとめと今後の課題

本論文ではインシデントに対する迅速な対応のためのシステムを提案した．このシステムは CSIRT のインシデント対応時間だけでなく，インシデントを引き起こした一般利用者にも目を向けた．一般利用者の所有する端末の調査にかかる時間を短縮することで迅速なインシデント対応につながると考えた．また，インシデント対応時に収集される情報を一元的に管理しておくことで情報共有がしやすくなり CSIRT 間や一般利用者との連絡にかかる時間の短縮と対応の進捗状況の把握がしやすくなると考えられる．

今後は，提案するシステムの実装に向けてまずは，インシデント対応に必要な情報の一元管理と進捗管理のための UI の開発，データ構造の作成を行っていく．また，平常時の情報収集のために他システムとの連携を取り自動的に必要な情報を収集・蓄積する機能についても作成を行う．

参考文献

[1] “大学被害事例”. https://xn--dckta5b5b2j4a3878bqnb245b20icpn0jz.com/tag/%E5%A4%A7%E5%AD%A6%E8%A2%AB%E5%AE%B3%E4%BA%8B%E4%BE%8B/ （参照 2019-7-29）

[2]近堂徹，田島浩一，岸場清悟，吉田朋彦，岩田則和，西村浩二，相 原玲二，全学ネットワークログの蓄積・参照システムの実装と評価，インターネットと運用技術シンポジウム 2016 論文集，pp. 11-17，2016.

[3]渡邉英伸，相原玲二，西村浩二，広島大学における情報セキュリティインシデント対応訓練，大学 ICT 推進協議会，2017 年度年次大会

[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/guide_ver1.0_20151126.pdf.

[5]一般社団法人 JPCERT コーディネーションセンター，CSIRT ガイド，2015， https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0_20151126.pdf

[6]独立行政法人情報処理推進機構，情報セキュリティセミナーインシデントマネジメント v. 1. 0， https://www.ipa.go.jp/files/000003121.pdf

[7]Motoyuki Ohmori, Masayuki Higashino, Toshiya Kawato, On a Finite State Machine and Input Fields for Incident Tracking System, IPSJ SIG Technical Report Vol. 2018-IOT-42 No. 6 2018/6/28.

[8]森健人，石井将大，松浦知史，金勇，北口喜明，友石正彦，セキュリティ事案における地検の蓄積・活用を可能とする対応フローの提案と実装，研究報告インターネットと運用技術（IOT），2019-IOT-46（2），pp. 1-8，2019.

[9]National Institute of Informatics: National Institute of Informatics, https://www.nii.ac.jp/

表 1　平常時とインシデント対応時に必要な取り組みの整理と広島大学で収集している情報の分類

フェーズ	JPCERT/CC と IPA が示す平常時とインシデント発生時に行うべき要件	広島大学がインシデント対応時に収集している情報
平常時	インシデントの未然防止策の実施すること	**初期講習会** （OS の種類とバージョン，OS の bit 数，バッテリの駆動時間，学内ネットワークへの接続の可否，OS の自動アップデート設定状態，ウイルス対策ソフトのインストール状態，ウイルス対策ソフトの自動アップデート機能の設定状態，ウイルススキャンの実行結果，Microsoft Office（Word，Excel，PowerPoint）のインストールの可否，学内プリンタへの出力可否）
	予行演習を定期的に行うこと	**インシデント対応訓練** （メーカー，型番，OS のエディション，OS のバージョン，システムの種類，プロセッサ情報，コンピュータの使用目的，個人情報などの重要情報の有無，OS の最終更新日，ウイルス対策ソフト名，パターンファイルの最終更新日，最終スキャン日，コンピュータのファイルの異常，異常があった場合の具体的な状況，インシデントに対する思い当たる事象，ウイルススキャンの検知の有無，検知された場合のウイルス名や駆除状況）
検知/連絡受付	インシデントの検知に必要なチェック項目をあらかじめ明確にしておくこと	**検知情報** （攻撃先ポート，フラグ，プロトコル，アクション，警報名，PA シグネチャ ID，カテゴリ，危険度レベル，方向，攻撃元国，攻撃先国，コンテンツタイプ，ダイジェストファイル，ユーザーエージェント，ファイルタイプ，X-転送，ペイロード有無，ペイロード情報） **特定情報** （攻撃先 IP アドレス，攻撃元 IP アドレス，通信の開始時間，通信の終了時間，ユーザ ID，ユーザ氏名，ユーザ身分，ユーザ E-mail，ホスト名，MAC アドレス，学内ゾーン ID） **該当端末調査結果** （メーカー，型番，OS のエディション，OS のバージョン，システムの種類，プロセッサ情報，コンピュータの使用目的，個人情報などの重要情報の有無，OS の最終更新日，ウイルス対策ソフト名，パターンファイルの最終更新日，最終スキャン日，コンピュータのファイルの異常，異常があった場合の具体的な状況，インシデントに対する思い当たる事象，ウイルススキャンの検知の有無，検知された場合のウイルス名や駆除状況）
トリアージ	取り扱っているインシデントに関して、「いつ」「どこで」「何が」「どのように」起こったのか、また当事者，関係者は「誰か」といった点を整理すること	**NII-SOCS からの検知情報** **ネットワークログの分析結果** **トリアージ結果** （トラブル種別警報 ID，セッション ID，関連 No，ユーザ特定不可要因，担当者，判断結果，判断日時） **該当端末の調査結果**
対応	インシデント対応の結果（顛末など）を、当該インシデントについて CSIRT に対応を要請した方や関係者（上位組織や監督官庁など）に報告すること	**広大トラブル報告書** （トラブル種別警報 ID，セッション ID，関連 No，対応完了日，解析者，警報名，部局等情報セキュリティ組織 No，部局等情報セキュリティ組織名称，ユーザ特定不可要因，ユーザ ID，ユーザ氏名，ユーザ身分，ユーザ E-mail，ホスト名，MAC アドレス，学内ゾーン，学内ゾーン，学内ゾーン ID，NII 検知日，NII 検知時刻，発生月， NII 通知日，NII 通知時刻，NII への返信日，NII への返信時刻，攻撃先 IP アドレス，攻撃元 IP アドレス，制限対象，制限実施日，制限実施時刻，部局通知日，部局通知時刻，切り離し日，切り離し時刻，制限解除依頼日，制限解除依頼時刻，制限解除日，制限解除時刻，報告書提出日，報告書提出時刻，保全期間終了日，備考，検知元，対応，ウイルススキャン検知の有無）

（注）緑文字は CSIRT がそのフェーズで収集すべき情報を示す．青文字は CSIRT が収集済みの情報を示す．黒文字は一般利用者がそのフェーズで収集すべき情報を示す．赤文字は平常時に一般利用者が収集済みの情報を示す．紫文字はインシデント発生時に一般利用者が収集済みの情報を示す．