2008－EIP－42 (1)
2008／11／29

情報セキュリティインシデント対応に関する法的課題

山川 智彦
㈱NTT データ

CSIRT（Computer Security Incident Management Team）の概念やCSIRTでのインシデントマネジメントの手法は、企業などの組織にも有益である。CSIRTのインシデントマネジメントの中心となるのは「D（発見）→T（トリアージ）→R（対応）」という業務プロセスであり、インシデント対応上の法的課題は、Rの中の「法的課題への対応」プロセスに位置づけることができる。今後、インシデントマネジメントプロセスの標準化、国際規格化のほか、サイバー演習などの手法との併用による組織マネジメントへの定着化などが期待されている。

Legal Issues on information security incident response

Tomohiko Yamakawa
NTT DATA Corp.,

It is quite effective and beneficial for organizations, such as business corporations, governments, and educational institute, to take advantage of the method of security incident management of Computer Security Incident Management Team, CSIRT. The core of the security incident management is “Detect (D) → Triage (T) → Response (R)” and all legal issues are listed in the sub-process of “Legal Response,” which is a part of Response process.

1. はじめに

CSIRT（Computer Security Incident Management Team）の概念、およびCSIRTでとりあげられているマネジメントの形態は、企業にとって情報セキュリティマネジメントに適用するのに有益であることは昨年の拙稿「CSIRTと情報セキュリティガバナンス」で明らかにしたところである。

本稿では、考察を一歩進め、一般的なCSIRTでの理解とされている「インシデントマネジメントの考え方」の核となるアイデアを、米国・CERT/CCのアプローチから抽出し、わが国企業にも適用可能な形で紹介する。その中で、わが国の実務上問題となりうる諸点を「法的課題として紹介する。

最後に、インシデントマネジメントのアイデアがわが国企業、政府機関などの組織で普及・展開していくにあたって、今後の課題となる諸点を述べる

情報セキュリティインシデントとそのマネジメント、取り扱い（ハンドリング）の定義や理解については、米国のCERT/CC、およびCERT/CCに関連深い団体であるCMU/SEIからくつかの文書が公表されている。これらの文

書はほとんどが英文のため、CSIRT の意義やマネジメントの枠組みがわが国に浸透し、情報セキュリティに性格に理解されているとは言いがたい。ただ、最近は JPCERT/CC からその内容を簡潔に紹介したものも公表され始めており、CSIRT の活動が一般に理解され、成功的取り組みとして普及していく素地ができつつある。

本稿では、以下、CERT/CC および CMU/SEI の文書に記載された内容をもとに、インシデント対応の詳細を紹介していく。

2. 情報セキュリティインシデント対応の一般的理解

企業や政府機関、研究機関をはじめとする「組織」には、自らの情報インフラに対するセキュリティインシデントを的確にマネジメントする機能が求められている。セキュリティインシデントとは、リソースの不正使用、サービス妨害行為、データの破壊、意図しない情報の開示など、コンピュータセキュリティに関係する人為的事象で、意図的および偶発的なものを含む、と一般に理解されている[1]。組織にとって、これらのインシデントに対応すること、言い換えれば、情報システムにおけるインシデントが発生した後のクライシスマネジメントを適切に行い、その被害の拡大を最小限にするための「事後」対応を的確にしなくては[2]、情報システム事故による業務の停滞、それにともなう損害を抑制することはできない。

この「インシデントマネジメント」機能をそなえるには、組織は、自らその機能を整備するほか、必要であれば、外部のリソースを活用する場合もある。逆に言えば、インシデントマネジメント機能は、CSIRT が提供するサービスのメニュー項目と対応しているといえる。

CSIRT が提供するサービスは、大きく分けて以下の 3 種類である。

（表 1）CSIRT が提供するサービスの内容

事後対応サービス	事前対応サービス	セキュリティ品質管理
·注意·警告·<u>インシデント取り扱い</u>（ハンドリング）＝インシデント解析/現場での対応/対応支援/対応コーディネーション·脆弱性取り扱い（ハンドリング）＝解析/対応/対応コーディネーション·アーティファクト取り扱い（ハンドリング）＝解析/対応/コーディネーション	·通知·技術動向調査·セキュリティ監査、評価·セキュリティツール、アプリケーション、基盤のコンフィグレーション、維持·セキュリティツールの開発·侵入検知サービス·セキュリティ関連情報の配布	·リスク分析·事業継続計画（BCP）、災害復旧計画（DRP）·セキュリティコンサルティング·認識構築·教育/訓練·製品評価・認証

参考文献：*Defining Incident Management Process for CSIRTs: A Work in Progress*（CMU-SEI 2004-TR-15）

上記のサービス分類は、CMU/SEI の文書 *Defining Incident Management Process for CSIRTs*[3] をもとに記述したものであるが、

[1] JPCERT/CC ウェブサイトより
http://www.jpcert.or.jp/faq.html#1a03

[2] 「インシデントマネジメント」の定義は JPCERT/CC ウェブサイトによる
http://www.jpcert.or.jp/ir/

[3] Alberts, Chiris; Dorofee, Audrey; Killcrece, Georgia; Ruefle, Robin; Zajicek, Mark. *Defining Incident Management Process for CSIRTs: A Work in Progress* (CMU/SEI-2004-TR-015). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, October 2004
http://www.sei.cmu.edu/pub/documents/04.reports/pdf/04tr015.pdf

CSIRT がここに列記したサービスをすべて提供しなくてはいけないわけではない。CSIRT が提供するサービスの内容は、サービス対象（コンスティチューエンシー）が期待する内容や、当該 CSIRT のミッションによって変わってくるのである。

ちなみに、JPCERT/CC の「インシデントハンドリングマニュアル」[4]でも、同様の理解を前提としている。

インシデントマネジメントは、これらのサービスの中では「インシデント取り扱い」（インシデントハンドリング）と対応しており、さらにいくつかのプロセスに細分化することができる。*Defining Incident Management Process for CSIRTs*」では、インシデントマネジメントプロセスを以下のとおり定義している[5]。

- Prepare (PC): Prepare/Sustain/Improve
  - 初期インシデントマネジメント、CSIRT ケイパビリティの計画と実施
  - ケイパビリティの維持
  - 教訓、評価、アセスメント活動を通じての既存ケイパビリティの改善
  - 必要時、インシデントマネジメント活動の事後見直しの実施
  - プロセス改善を次ステップ（PI）につなげる
- Protect (PI): Protect/Infrastructure
  - コンピュータ基盤を変更し、現在進行中のインシデントの停止・緩和、ハードウェア･ソフトウェア基盤の脆弱性の潜在的拡大を停止・緩和
  - 事後レビューなどのプロセス管理メカニズムに由来する基盤保護の改善の実施
  - 事前スキャニング、ネットワーク監視、セキュリティ・リスク評価によるコンピュータ基盤の評価
  - 進行中のインシデント、発見された脆弱性、評価過程で明らかになったセキュリティ関連イベントに関する情報を次ステップ（D）につなげる
- Detect (D)
  - イベントの通知、報告
  - イベントの報告を受け取る
  - ネットワーク監視、IDS、技術監視機能などの指標を事前に監視
  - 監視された指標の分析
  - 疑わしいイベント、顕著なイベントの情報を Triage プロセスに渡す
  - 可能であれば、イベントをインシデントマネジメント以外のエリアに割り当てる
  - Triage プロセスに引き継がないイベントのクローズ
- Triage (T)
  - イベントのカテゴライズと関連付け
  - イベントの優先順位付け
  - ハンドリング、対応へのイベント割り当て
  - 関連するデータ、情報を Response プロセスに引き継ぐ
  - 可能であれば、イベントをインシデントマネジメント以外のエリアに割り当てる
  - Response プロセスに引き継がないイベントのクローズ
- Response (R)

---

[4] 中間責任法人 JPCERT/CC「インシデントハンドリングマニュアル」（H20.6.24）
*以下のウェブサイトで閲覧可能
http://www.jpcert.or.jp/csirt_material/files/manual_ver1.0.pdf

[5] 前掲・注 3　CMU/SEI-2004-TR-015　P16-

- イベントの分析
- レスポンス戦略の計画
- 技術、管理、法制度上の対応のコーディネートと提供
- 部外者とのコミュニケーション
- 可能であれば、イベントをインシデントマネジメント以外のエリアに割り当てる
- 対応のクローズ
- 教訓・インシデントのデータをPCプロセスの事後レビュー使用のために提供

また、*Defining Incident Management Process for CSIRTs*では、これらのプロセスの流れを以下ように整理していると考えられる。

○ 全体として大きな3つのプロセスに分けることができる。すなわち、①Prepare、②Protect、③「D→T→R」という流れがある。

○ 「D→T→R」のプロセスはインシデントマネジメントの中に納まっているが、Prepare、Protectの両プロセスは、インシデントマネジメントの範疇を超えてセキュリティマネジメントの領域にも入っている。

日本でも、セキュリティマネジメントについては、ISMS、ITIL、さらにはJ-SOXへのコンプライアンスなどの手法が議論され、企業、政府機関などの組織ではどのような「ベストプラクティス」を実施すべきかが模索されている。しかしながら、インシデントマネジメントについては、JPCERT/CCなどのCSIRTに任せておくという風潮があるのではないか。組織としても、自らCSIRTとのPOC機能を整備し、公的なコーディネーション機関をより一層活用できるようにマネジメントプロセスを明確化、整備していくべきではないかと筆者は考える。

マネジメントプロセスの整理、明確化には様々な方法が考えられるが、CSIRTのマネジメント手法をセキュリティガバナンスに活用するという文脈で考えれば、企業のセキュリティマネジメントの中核となりうる「D→T→R」に注目すべきであろう。「D→T→R」のプロセスは、日本でも一部紹介されて入るもの、まだ組織のマネジメントに根付いているとは言いがたい。よって、本稿では「D→T→R」に焦点をおき、その内容を明確にしつつ、各プロセスの法的な論点を整理していきたい。

3. インシデント対応の骨格となる「D→T→R」

D、T、Rの各機能にどのようなサブプロセスが含まれるかは、前章で述べたとおりである。本章では、ひきつづき*Defining Incident Management Process for CSIRTs*に基づいて各機能の詳細を分析し、各機能間の関連を明確にする。

3-1. D=ディテクト。事故の発見。

「発見」のプロセスは、狭義ではネットワーク監視による侵入検知を意味する場合が多いが、インシデントマネジメント全般では、セキュリティ脅威やリスクに関するイベント全般がここに含まれると考えられる。具体的には、インシデント、脆弱性、その他のインシデントマネジメント関連の情報が収集される。

情報の収集は、受動的な収集と、能動的な収集の2通りがある。

受動的収集は、内部・外部のリソースから、レポート、通知などの形式で知らされることをいう。わが国の場合、JPCERT/CCやベンダ、グループ会社にCSIRTがある場合は当該機関からの脆弱性、インシデント情報の連絡がこれ

にあたる。

能動的収集は、インシデントの可能性をモニタリングから察知する、ネットワーク監視やIDSから脆弱性を検知するなどである。

「発見」プロセスで収集された情報は、次のプロセス＝トリアージに送られる

3-2. T=トリアージ。事例の優先割り当て。

「発見」プロセスで収集された情報は、「トリアージ」のプロセスで分析され、対策の立案につながっていく。状況の判断、さらに事実を相互に関連付け、対処の優先順位付け、方向性などを決めるのがこのプロセスである。

トリアージのプロセスは、さらに以下の3つのサブプロセスに分かれる。この3つのサブプロセスは、同時並行で起こることもある。

(1) 分類・関連付け。

収集した情報の有効性を検証し、どんな種類のイベント（たとえばWinnyによる情報漏えい、フィッシングサイトへの誘導など）が報告されているのか、その際、どんな行動をとるべきかを決定する。組織としては、対応すべきインシデントの種類と初期対応開始の判断基準を事前に明確にしておく必要がある。

(2) 優先順位付け

収集された情報が別のイベントのものであれば、そのいずれが優先されるべきかを決定する。このサブプロセスでは、組織は、事前にイベントの中での優先順位を明確にすることが要求される。

(3) イベントの割り当て

分類、優先順位付けなどに従い、各イベントに対してどのような対応をするかを割り当てる。この「対応」が、次のプロセス＝Responseになる。

3-3. R=レスポンス。対応の実施。

「トリアージ」を終えると、実際の「対応」にうつる。*Defining Incident Management Process for CSIRTs*の分類では、この「対応」は、「技術的課題への対応」「マネジメント課題への対応」「法制度上の課題への対応」に分かれる。

(1) 技術的課題への対応

「技術的課題」と表現しているが、「事前に取り決めのある対応の実施」ということができる。分析、トリアージの結果に基づいて、対策を立案、実施していく。

(2) マネジメント上の課題への対応

「技術的課題」とは対照的に、「事前に取り決めのない対応」であり、マネジメント層の判断が必要となるのがこの場合である。また、メディアへの対応など、事前に取り決めのあるマネジメント層の対応や、リスクマネジメント、財務管理と協働して、インシデントの影響やコストを決定するプロセスもここに含まれる。

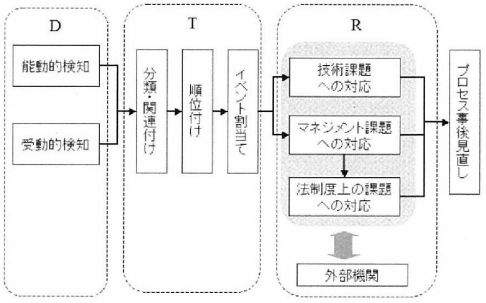
(3) 法制度上の課題への対応

マネジメント上の課題の中で、法律専門家によるアドバイスや支援が必要となる場合がこれに該当する。

いずれの対応も、最終的に「対応の事後見直し」のプロセスに移る。この「事後見直し」は、「PC」のプロセスの一部であり、「D→T→R」がPCおよびPIのプロセスと連携してくるポイントになる。セキュリティインシデント対応について、事後の見直しが重要だと主張される所以であり、PDCAのサイクルとの整合性のポイントになるともいえよう。

以上の関係を図に整理すれば、以下のとおりになると考えられる。

DTR各機能の関連



4. インシデントマネジメントプロセスでの法的課題と今後の展開

インシデントマネジメントの法的課題は、これまで見てきたように、「D→T→R」の中の「R」、とりわけ「法的課題への対応」に整理されているといえる。情報セキュリティマネジメントなど、視野を広げれば課題の設定も可能だが、本稿では、「具体的なプロセス遂行の際に考慮すべき課題」に絞りたい。

「法的課題」として、*Defining Incident Management Process for CSIRTs* では以下のような課題を具体的に列記している[6]。

- 適用可能な法や規制から、どのような対応のオプションが法的に許容されているかの助言の提供
- 組織のネットワークでおきている悪意ある行動の法的責任に関する法的専門家からの助言の提供
- 法制度上の課題、法的責任に関するプレスリリースや組織文書の確認
- レスポンス活動について外部関係者と協働する場合の秘密保持契約の締結
- 法執行機関への通知、巻き込み
- 法廷での法律で許容される証拠保全についてのコンピュータフォレンジックの実施。
- 現在進行中のレスポンス活動に関する法的文書、メモのレビュー

これらの対応を組織のどの部門が実行するかという課題はあるが、それは各組織の規則、文化により異なると考えられる。法務部門が実施する場合もあれば、インシデント対応組織のコアとなる部隊に法律専門家を配置する場合もある。また、法的なレビューは全部部外の組織にアウトソースするということもあるだろう。

どのような法律が問題になるかについては、*Defining Incident Management Process for CSIRTs* では未だ明確に記載されていない。考えられるのは、以下のような考えられるであろう。

(1) 個人情報保護に関する法

インシデントの状況を把握するには、様々な情報を収集する。その中には、個人に関する情報も含まれるが、必要以上に情報を収集した場合、個人情報保護に関する法規に抵触する場合がある。通信の秘密に関する法規がある場合には、それにも注意が必要である。

(2) サービスの提供、知的財産権に関する法

インシデント対応組織の立場で問題となるのは、被害発生時にサービスの切断をした場合、サービスの提供義務に関する法の規定と抵触しないか、という課題がある。また、他者の著作権を侵害しうるコンテンツがあるという通報をうけた事業者が一方的にコンテンツを削除しても、ほかの法規の規定と抵触しないかという課題も考えられる。

(3) サイバー犯罪に関する法

サイバー犯罪に関する法への対応という意味では、欧州評議会によるサイバー犯罪条約と、

[6]前掲・注 3　CMU/SEI-2004-TR-015　P152

関連する規定がある。最近では、2008年4月に公表された「サイバー犯罪に関する法執行機関とISPの協力に関するガイドライン」がある[7]。

(4) 証拠保全に関する法

証拠保全に関する法との関係では、「フォレンジック」という概念がある。わが国では「デジタル・フォレンジック研究会」での取り組みがあるが、CSIRTでいう実務的なフォレンジックとの差異など、今後研究すべき点も多い。

(5) 法執行機関との協働に関連する法

実務家の立場からすれば、法執行機関に何らかの対応を要請するのはどのような場合か、その場合、どのような手続きによるか、根拠となる法律は何か。

5. 今後期待される活動

ここまで明確にされてきたインシデントマネジメントの法制度上の諸課題をめぐって、今後、どのような展開が期待されるのか。大きく言えば、以下の3点であろう。

(1) インシデントマネジメントプロセスの標準化、国際規格化

発見→トリアージ→対応のプロセスは、組織のインシデントマネジメント対応プロセスとして幅広く普及・展開されるべきものと考えられるが、これらはあくまでCMU/SEIが文書で規定し、CSIRTコミュニティの中で普及をはかってきたものである。しかし、CSIRTコミュニティ以外での普及・展開を図るのであれば、ISOなど何らかの国際標準化のプロセスを経て規格化されてもいいのではないだろうか。その際、ISMSやその他のISOなど既存のマネジメント系諸規格との整合性や、「インシデントマネジメント」であって「セキュリティマネジメント」ではないことなどは、留意されてしかるべきであろう。

(2) 「D→T→R」プロセス検証のための手段の開発・展開

「D→T→R」のマネジメントプロセスが組織のインシデントマネジメントの規格として定着化するには、それを補完する手段が重要になってくる。たとえば、D、T、Rの各プロセスで重要となるケイパビリティや行動指標を定量化し、演習などの手段を実施することでチェック、更なる定着化を図ることができるのではないだろうか。

たとえば、米国では国土安全保障省が中心となって、HSEEP（Homeland Security Exercise and Evaluation Program）という名称の演習・評価プログラムを推進している[8]。米国のサイバー演習としてはサイバー・ストームなどが著名だが、HSEEPはサイバーインシデントだけではなく、バイオや災害復旧など、あらゆる領域への適用が可能であり、実際に運用されている事例もある。

具体的な手法、ノウハウについては、今後も検討を重ね、別途公表することとしたい。

(3) フォレンジックの取り組み

日本の「デジタル・フォレンジック研究会」では、デジタル・フォレンジックを以下のように規定している。

---

[7] Council of Europe. Guidelines for the cooperation between law enforcement and internet service providers against cybercrime (1-2 April 2008)

[8] 国土安全保障省のHSEEPウェブサイト https://hseep.dhs.gov/pages/1001_HSEEP7.aspx

「インシデント・レスポンスや法的紛争・訴訟に対し、電磁的記録の証拠保全及び調査・分析を行うとともに、電磁的記録の改ざん・毀損等についての分析・情報収集等を行う一連の科学的調査手法・技術を言う」[9]

これに対して、CSIRTコミュニティでも「フォレンジック」という概念が存在し、実際にフォレンジック業務に携わっているチームも存在している。

今後、前者のような学術的アプローチと、後者のような実務的アプローチの距離が縮まり、国際的にも通用するアプローチとなることを期待したい。

---

[9]特定非営利活動法人デジタル・フォレンジック研究会ウェブサイトより
http://www.digitalforensic.jp/