情報処理学会論文誌　Vol. 51　No. 4　1248–1256 (Apr. 2010)

推薦論文

社会・法政策の視点から見た情報セキュリティインシデント対応

山　川　智　彦[†1]

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．情報セキュリティインシデントが発生した場合，適切な事後対応と同時に重要となるのが，十分な即応体制（Preparedness）である．アメリカでは，国土安全保障政策の一環として，緊急事態への対応と即応体制が制度上明確に規定されており，準備体制整備のためのガイドラインやツールも整備されている．システム開発者のコミュニティであるCSIRTとしての連携自体は非常に有益であるが，「草の根」レベルでのインシデントマネジメントに関する情報共有をより効果的なものとするには，政府，企業などの「経営」レベルでインシデントマネジメントを活用するような仕組みを考える必要がある．

Information Security Incident Response, from the perspective of society, law and policy

Tomohiko Yamakawa[†1]

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, Triage, and Response” and all legal issues are listed in the sub-process of “Legal Response,” which is a part of Response process. To deal with major security events, such as terrorist attacks, natural disasters, and other emergencies, requires “national preparedness system” to all kinds of stakeholders. In the United States, Department of Homeland Security clearly requires preparedness and response systems to incidents by appropriate guidelines and effective tools. CSIRTS works well as a community of system developers. To make information sharing of incidents on grass roots more effective, it is necessary to set up an institute or organization which would activate an incident management system as management level.

1. はじめに

CSIRT（Computer Security Incident Management Team）の概念，およびCSIRTで取り上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2007年の拙稿「CSIRTと情報セキュリティガバナンス」[1)]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，米国で公表されている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いいがたい．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はじめており，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．

†1 日本電信電話株式会社
Nippon Telegraph and Telephone Corporation
本論文の内容は2008年11月の電子化知的財産・社会基盤研究会にて報告され，同研究会主査により情報処理学会論文誌ジャーナルへの掲載が推薦された論文である．

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[2]．組織にとって，これらのインシデントに対応すること，いい換えれば，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[3]，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，自らの一部門を「CSIRT」と位置づけて体制を整備するほか，必要であれば，外部のリソースを活用して対応する場合もある．CSIRT は，自らの組織内のリソースだけで構成しなくてはならないわけではなく，外部のリソースを活用して運営することも可能なのだ．

たとえば，JPCERT/CC のマテリアルでは，「インシデントマネジメント」と「インシデントハンドリング」を次のように定義づけている[4]．

- 「インシデントマネジメント」：情報セキュリティ上の危機管理体制．企業経営や事業活動，ブランドに重大な損失をもたらす，もしくは社会一般に重大な影響を及ぼす事態を「危機」と考え，万が一，危機が発生した場合に損失を極小化させるための活動．
- 「インシデントハンドリング」：緊急の対応．インシデントが発生した際に，通報を受け，状況をふまえ対処方針を決定し，問題解決を行い，インシデントを収束させる．

すなわち，企業や政府機関など，「組織」にとっての危機管理体制全般を「インシデントマネジメント」と位置づけ，その中の「緊急対応」の部分を「インシデントハンドリング」と定義している．

この「インシデントマネジメント」は，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
- Protect (PI): Protect/Infrastructure
  - Detect (D)
  - Triage (T)
  - Response (R)

また，同文書では，これらのプロセスの流れを以下のように整理している．

- 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，① Prepare，② Protect，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 に任せておくだけで，自らの経営課題としては整理できていない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いっそう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はいるものの，まだ組織のマネジメントに根づいているとはいいがたい．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．

「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．

3.2.1　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．

3.2.2　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．

3.2.3　イベントの割当て

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ゆえんであり，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．

4.　インシデントマネジメントプロセスの法的課題

インシデントマネジメントの法的課題は，*Defining Incident Management Process for CSIRTs* に規定されるプロセスのみに注目してみれば，「D→T→R」の中の「R」，とりわけ「法的課題への対応」に位置づけられているといえる．

4.1　Legal Response の意味するところ

最初に，*Defining Incident Management Process for CSIRTs* で「Legal Response」に関する記述を見る[5]．そこには次のような記述がなされている．

> Legal response includes actions with incident activity that relate to investigation; prosecution; liability; copyright and privacy issues; interpretation of legal rulings, laws, and regulations; non-disclosures; and other information disclosure agreements.

すなわち，インシデントに対する行動で，以下のとおり，課題，刑事，民事，知的財産，情報開示などあらゆる法的課題に関するものが Legal Response に含まれるとする．

- 捜査，訴追
- 責任
- 著作権およびプライバシ
- 法の支配の解釈
- 法律，規則
- 非開示および情報公開に関する協定

また，具体的に「Response」といえる活動の形式についても，以下のように記述されている[7]．助言の提供のほか，文書の作成・確認といった作業のほかに，法執行機関など外部との対応手順など，非常に多岐にわたっているといえる

- 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．このように実施主体が多様であるということを加味すれば，*Defining Incident Management Process for CSIRTs* に規定する「Legal Response」は，社会で企業や組織がインシデント対応をする際に考慮すべき法的課題をすべて網羅している，という一面があるといえる．

しかしながら，逆の見方をすれば，同文書で規定する課題は「インシデント対応プロセスで留意すべき法律上の課題の列挙」にすぎず，企業や組織が情報セキュリティインシデントを含むリスクに対応するには，ほかに考慮すべき課題があるのではないか，という視点もあると考えられる．以下，別の視点から，企業や組織の直面する危機管理の課題の中で，情報セキュリティインシデントがどうとらえているかを概観したい．

4.2　広義の「セキュリティ課題」の中での位置づけ

企業や組織の直面する「セキュリティリスク」，情報セキュリティに限らない，広義の「セキュリティリスク」については，数多くの論考でとりあげられている．なかには，コンサルティングなどビジネスのベースとして流布しているものもある．本稿では，近時の情報セキュリティ上の具体的な脅威に対応するための方策として，インシデントを企業が自ら検知し，組織全体で必要な対応をとることができる体制としての組織内 CSIRT の構築を推奨するマテリアルである「経営リスクと情報セキュリティ」[8] の記述をベースに，課題を整理する．

最初の JPCERT/CC での定義にあるように，インシデントマネジメントとは，組織にとっての「危機管理体制」そのものにほかならない．危機管理の課題と，その背景にある法制度としては，およそ以下のようなものがあると考えられる．

4.2.1　内部統制[9]

粉飾決算や食品偽装といった企業の「モラルハザード」は，わが国だけでなく，アメリカなど世界各国でもここ最近大きな問題となっている．その端緒ともいえるのが，アメリカのエンロン，ワールドコム事件であり，それをきっかけに制定されたサーベンス・オクスレー法（SOX 法）が企業の内部統制の重要性を法制化している．この動きは，わが国にも波及し，金融商品取引法が制定された．

4.2.2　事業継続[10]

欧米では 2001 年の米国同時多発テロ（9.11）を契機として，事業継続の視点が注目されている．事業継続管理（BCM）のガイドラインは，BS25999 などの形で国際標準化されつつある．

4.2.3　情報資産管理[11]

これはさらに 3 つの課題がある

情報漏洩

わが国では個人情報保護法の制定・施行ともあいまって，情報漏洩の問題が大きな課題になってきている．USB や PC の持ち出し，紛失といった従来型の不祥事もあれば，P2P ファイル交換システムの影響で情報流出が加速するような事例も出てきている

不正アクセスなど「新たな脅威」

新たな技術を駆使した不正アクセスだけでなく，コンピュータウィルスに感染した PC をネットワーク化（ボットネット）した一斉攻撃などの問題が発生している．また，昨今の国際情勢の関連から，グルジア，エストニアで「サイバー攻撃」の事例が顕在化し，2009 年には韓国や日本にもその影響が見えたともいえる例も発生している．

システム障害

金融機関，証券取引所といった社会インフラをさせる重要機関において，システム障害に起因するサービス停止が相次いだ．

このように，インシデントマネジメントを企業や組織に求めるセキュリティリスクは多数存在する．なかには「事業継続」など，「法的課題」とはいえないものもある．しかし，ここで留意すべきは，どのセキュリティリスクも，法や命令によって「インシデントマネジメントの整備を強制するものではない」ということである．まして，インシデントマネジメントに有益である「CSIRT」の設置を義務付ける法規制は存在しない．

「CSIRT」自体も，国家や企業のガバナンスがあって存在するものというよりは，情報セ

キュリティ，インシデントマネジメントのエキスパートたちの自発的フォーラムであり，強制的に組織として活動するものではないので，「草の根」的な活動として広まってはいるものの，いまだあまねく広く利用されるには至っていない．「信頼の輪」で組織を超えて連携しているCSIRTにとっては，企業のガバナンスや政策による「強制」は，活動の本質を損なうものであるというふうに映っているのかもしれない．

しかしながら，ITの脅威は今までのレベルを超えて高まってきており，情報システムやネットワークに依存している我々市民の生活にとって，新たな脅威や脆弱性に対抗するには，CSIRTで培われたノウハウや知見が必要なのではないだろうか．

5. アメリカの事例とわが国への示唆

では，法的に設置を強制されるとはいえないCSIRTを活用することで，企業や組織，さらにはそれらが構成する社会の安全・安心は適切に守られるのであろうか．1つのケースとして，アメリカでのセキュリティに関する対応の例を考える．アメリカは，インターネットにおける脅威・脆弱性に対して，CERT./CCを中心に「CSIRT」というアイデアを提唱，普及しているリーダであると同時に，国家として体系的な政策にインシデントマネジメントやCSIRTを位置付けようとしているのである．

5.1 アメリカにおける「インシデント対応」とセキュリティ政策

まず，セキュリティインシデント対応ということでいえば，政府レベルについては，連邦情報セキュリティ管理法（FISMA）の規定に従い整備される．FISMAは2002年「連邦電子政府法」の修正であり，連邦政府の情報セキュリティレベル向上のため，情報セキュリティ評価に対する結果責任まで詳細に規定している．具体的には，事件対応能力の確立のため，セキュリティ・インシデントの検出・報告・対応手順を含んだ「省内横断的セキュリティプログラム」を連邦各省庁に策定，文書化，実施させている（FISMA 3543条(a)(5)）．さらに，各省庁の取り組みに任せるだけではなく，OMBが「連邦情報セキュリティ・インシデントセンタ」を運営することも規定している（FISMA同条(a)(7)），3546条）．ちなみに，この「連邦情報セキュリティ・インシデントセンタ」の機能は，DHS設置後はUS-CERTに統合されたものと考えられる．

また，総合的な「セキュリティ」という視点から見れば，アメリカの国土安全保障政策は，「法制度」「科学技術」「情報共有のシステム」「国際協力」の4つの「基礎」の上に，「インテリジェンスと警告」「国境・交通手段のセキュリティ」「国内のテロ対応」「重要基盤・重要資産の保護」「大規模災害からの防衛」「緊急事態への即応体制・対応」といった6つの「重要ミッションエリア」に分類することができる[12]．ここで想定されている脅威は，サイバー世界の脅威だけではなく，生物，バイオ，自然災害など非常に幅広い領域にわたっている．この中で，サイバーセキュリティに関連する領域としては，「重要基盤・重要資産の保護」や，「緊急事態への即応体制・対応」が例として考えられる．

サイバースペースにおける緊急事態への即応体制・対応は，大統領令HSDP5[13]とHSPD8[14]で規定されている．この2つの大統領令により，あらゆる米国市民が脅威への即応体制（Preparedness）と対応（Response）のイニシアティブを確立する．このイニシアティブは，「国家インシデント管理システム（NIMS）」「国家対応計画（NRP）」「国家即応体制目標（National Preparedness Goal＝The Goal）」の3つである．「緊急事態への対応」にあたるResponse＝事後対応系のNIMSとNRPはHSPD5，「緊急事態への即応体制」になるPreparedness＝即応体制系のThe GoalはHSPD8でそれぞれ規定されている．重要インフラ保護政策は，2003年12月7日の「国土安全保障大統領令Hspd-7」[15]で，合衆国の重要インフラとその鍵となるリソースについて，連邦政府各省庁の役割分担を規定している．

5.2 「インシデント対応」の背景として推進される「演習」の取り組み

前節で見たように，米国では法律による明確な規定でインシデント対応を連邦各省庁に要求するだけでなく，包括的なリスク対応としての「国土安全保障政策」が存在し，その中には，インシデント対応をさらに一般化した形での「緊急事態への即応体制，対応」についても言及されている．さらに，米国のアプローチで特筆すべきは，このような「緊急事態への即応体制」をさせるノウハウ＝国土安全保障演習評価プログラム（Homeland Security Exercise and Evaluation Program＝HSEEP）[16]が，国土安全保障省により推進されているのである．

HSEEPは，連邦緊急事態管理庁（FEMA）の管理の下，演習の設計，開発，実施，評価，改善計画のための標準的な方法論と用語法を提供するフレームワークであり，サイバーテロのほか自然災害，バイオテロなどあらゆる種類の演習に活用されている．演習を通して各組織の強み，改善すべき領域の特定と是正がインシデント発生前に可能になることが特徴である．HSEEPで規定するアプローチは，どのような緊急事態がおこりうるかを15のシナリオに分けて想定し，想定した事態に至った場合，各主体がそれぞれ何をしなくてはいけないかを「タスク」とし，その「タスク」を実現するために必要となる能力を「ケイパビリティ」として，各主体はそれぞれに適した「ケイパビリティ」を計画的に高めることによって緊急事態への対応準備を進めよう，というものである．

HSEEP の「タスク」「ケイパビリティ」といった用語や演習のアプローチは，国家即応体制ガイドラインにも言及されており，HSEEP が NRP，NIMS のほか，HSDP-5，HSPD-8 に規定されたアプローチを実践するためのツールとしても有効であることが分かる．それを裏付けるものとして，国土安全保障省のウェブサイトでも以下のような記述がある[17]．

> HSEEP is compliant with and complements several historical and current Federal directives and initiatives. Some of these directives and policies include the following:

- National Strategy for Homeland Security
- HSPD-5, Management of Domestic Incidents
- HSPD-8, National Preparedness
- National Exercise Program (NEP)
- National Preparedness System
- NIMS

また，HSEEP が定義している文書・ノウハウについては，わが国にも情報が断片的にではあるが，入ってきている．インシデント対応を実践する専門家にはその存在が認知されているほか，コンサルティングビジネスの分野でも MSEL（マスタ・シナリオ・イベント・リスト）や AAR（アフター・アクション・レポート）によるレビュー手法を日本語で紹介する動きもある[18]．

（注）本稿執筆にあたって，米国だけでなくわが国でも普及しつつあるこれらサイバー演習の取り組みについて，日米の関係者に話を聞くことができたが，演習の実施にあたっては CSIRT で明確化しつつある「インシデントマネジメントプロセス」の考え方がベースになっているという印象であった．本来であれば，考察を一歩進めて，この点を学術的に明確に分析したいと考えたが，今の段階ではサイバー演習関連の情報は「関係者限りの秘密」とされることが多く，情報の入手がきわめて難しい．また，サイバー演習に関する理論的な分析もいまだ進んでいないことから，根拠となる客観的な記述による文献も限られているため，この点についての研究，分析は，今後の課題としたい．

5.3　日本のインシデント対応関連の法制度と米国の政策との比較

わが国の情報セキュリティ政策の基本となるのは，内閣官房情報セキュリティセンター（以下「NISC」）が 2006 年 2 月 2 日に公表した「第 1 次情報セキュリティ基本計画」[19] である．この基本計画は，2009 年月に「第 2 次情報セキュリティ基本計画」[20] として改定されているが，基本的なアプローチは第 1 次を踏襲していると考えられる．基本計画では，IT 社会を構成する主体の領域を，① 政府機関・地方公共団体，② 重要インフラ，③ 企業，④ 個人の 4 領域に分け，それぞれの特性に応じた対策のあり方を検討することが有効としている．基本計画を実行に移すための行動計画として策定されているのが，「セキュア・ジャパン」になる．

わが国各府省庁の情報セキュリティの確保については，各府省庁が自らの責任において対策を講じることを原則としつつ，「政府機関の情報セキュリティ対策の強化に関する基本方針」に基づき，政府機関が行うべき情報セキュリティ対策の統一的な枠組みを構築し，各府省庁の情報セキュリティ水準の斉一的な引き上げを図ることが必要と考えられている．

具体的には，政府機関の情報セキュリティ対策のための統一基準（第 2 版）[21] を見ていくことになるが，インシデント対応については「2.2.2 障害等の対応」の項目に記述されている．ここでは，(1) 障害等の発生に備えた事前準備，(2) 障害等の発生時における報告と応急措置，(3) 障害等の原因調査と再発防止策のそれぞれについて，基本遵守事項と強化遵守事項が記述されている．各府省庁で行政従事者から統括情報セキュリティ責任者への報告・連絡体制を整備することなどが規定されている．

このように，日本の政府レベルでのインシデント対応については，各府省庁の自発的な施策に委ねられており，米国のような法による命令的なものではないということができるだろう．

「重要インフラ」領域における取り組みは，「重要インフラの情報セキュリティ対策に係る行動計画」[22] に述べられている．すなわち，情報通信，金融，航空，鉄道，電力，ガス，政府・行政サービス（地方公共団体を含む），医療，水道，物流の各分野に属する事業を営む者のなかで，別途指定された「重要インフラ事業者等」に対し，(1) 重要インフラにおける情報セキュリティ確保に係る「安全基準等」の策定・見直し，(2) 情報共有体制の強化，(3) 相互依存性解析，(4) 分野横断的な演習の実施，などを期待するものである．これらも，わが国政府分野における取り組みと同様，基本的には重要インフラ事業者等の自発的な取り組みに期待する部分が多いといえよう．

インシデント対応については，この中の「情報共有体制の強化」に該当する．ここでは，以下の 3 つの施策が規定されているが，基本的に重要インフラ事業者の自主的対策に任されており，法的政策として CSIRT に言及したものはない．

- 官民の情報提供・連絡（「重要インフラ事業者等への情報提供」と「重要インフラ事業者等からの情報提供」）

- 情報共有・分析機能（CEPTOAR）
- 「重要インフラ連絡協議会（CEPTOAR-Council）」

このように，日本でも情報セキュリティインシデント対応をふまえたセキュリティ対策については，法制度で明確に規定している．基本的には政府の強制によるのではなく，企業の自主的施策や官民協力で目的を達成するというアプローチも基本的に同じである．実際，この情報セキュリティ基本計画が策定，実施されてから，日本でも情報セキュリティ対策についての意識は飛躍的に進んだといっていいだろう．

しかしながら，日米の法政策を比較した場合，やはり米国のほうに一日の長を認めざるをえないのではないかと考える．主に以下の点がその根拠であると筆者は考える．

- 米国には，政府分野において明確なインシデント対応関連の規定がある．1つの分野で制度による実施可能なモデルが提示されていれば，ほかの分野でも同様のモデルを構築するなど，推進のアイデアが生まれやすい．日本では，いずれの分野でも明確な規定がなく，既存の法制度との整合性など，インシデント対応や情報共有の実行段階で課題となっているものが多く残っている．実行面を見れば，CSIRT の普及という意味でも，日本は JPCERT/CC という組織はあるものの，一般の企業や組織で CSIRT の普及が立ち遅れており，「コーディネーションセンター」という機能を活用しきれる段階に至るにはまだ時間がかかりそうである．
- 米国には「HSEEP」という形で，緊急時対応，インシデントマネジメントといった体制への対応のプログラムが具体的に存在している．実態面では公開されていない部分は多いかもしれないが，連邦政府，州政府の双方が HSEEP に基づく「演習」を数多くの分野で推進している．基本的なノウハウを連邦政府がとりまとめ，ウェブで無償公開しているという点は，インシデント対応を文化的なものとして普及させるには大きなメリットがある．日本には HSEEP，もしくは類似の制度が存在せず，米国からは立ち遅れているといわざるをえないのではないだろうか．

6. 今後の展開への提言

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．インシデントマネジメントプロセスの自体の標準化，国際規格化だけでなく，「D→T→R」プロセス検証のための手段の開発・展開，さらにはフォレンジックの取り組みなどが考えられるが，何よりも期待されるのは，政府や企業のガバナンスに CSIRT というフレームワークをいかに効果的に組み込むことができるか，ということであろう．

政府としての取り組みとしては，日本政府が現在取り組んでいるような，CSIRT 相互間の連携を推進するということが1つ考えられる．もちろん，CSIRT 連携は非常に重要であり，CSIRT 連携を強化することで，新たな脆弱性や脅威への対応体制を迅速に整えることも可能である．しかしながら，「草の根」的に CSIRT の連携を広げるだけで，必要十分なのであろうか．政府，企業といった情報主体にとって，システム開発者を中心とした自発的な技術コミュニティである「CSIRT」のメリットをいっそう明確にし，組織の運営（政府の場合は政策，企業の場合は経営）に貢献するようなフレームワークを構想，実践していくことはできないだろうか．

もちろん，CSIRT で流通する情報を，法執行機関との連携，企業経営への活用など，各 CSIRT が情報収集した目的のほかに利用，さらには強制的に情報提供を共用するようなことは，厳に慎むべきである．しかし，情報流通ルールの本来の規則を守りながらも，ステイクホルダ間で協力，検討することで，CSIRT で収集した情報を「経営レベル」に利活用することは可能なのではないだろうか．

たとえば，組織のガバナンスとして，組織の責任者レベルで情報セキュリティに関する意思決定機関を設置し，CSIRT で収集した情報を活用するという仕組みはその例であろう．もちろん，CSIRT で収集した情報をそのまま「意思決定機関」にエスカレーションさせるのではなく，情報の匿名化，一般化など，CSIRT での情報流通ルールを損なわないような工夫をするプロセスが入ってしかるべきである．

このような「意思決定機関」を含んだ「社会の仕組み」としては，次のようなものが考えられるのではないだろうか．

6.1 企業の情報セキュリティ委員会（米国，日本）

積極的に情報セキュリティに取り組んでいる企業は，情報セキュリティ担当役員として，いわゆる CISO（Chief Information Security Officer）を任命するだけでなく，役員，事業本部など，情報セキュリティに関する責任者による「体制」を整備している．そして，「体制」とセットで，マネジメントのルール，インシデント発生時の報告ラインなど，必要な「規約，手続き」を定めることになる．

たとえばわが国で「情報セキュリティ報告書」を公表している企業は5社あるが，そのいずれもが社長，または CISO をトップとする情報セキュリティ管理体制を敷いていることを公表している[23]．

このように「体制」と「規約，手続き」をあわせて規定することで，情報の取扱いルール

が明確になり，一定の規律を持って組織の中で活用されるのである．

また，企業が役員レベルでの情報セキュリティ管理体制をしいているのは，日本だけではない．日本に先行して，アメリカでは “Governing for Enterprise Security” という概念を企業に幅広く普及させるべく，CERT/CC と関連の団体がセキュリティガバナンスの考え方をまとめたレポートや，実装のための手順書を公表していることは，拙稿「CSIRT と情報セキュリティガバナンス」で発表したとおりである[24]．

6.2　政府のトップダウンによるセキュリティ管理（米国）

前の章でアメリカの政府レベルにおけるサイバーセキュリティ対策が，ブッシュ政権下で整備されてきたことはすでに述べたとおりである．2009 年，オバマ政権成立後も，合衆国政府のサイバーセキュリティに関する関心は依然として高く，2009 年にはこれまでのサイバーセキュリティ政策の見直しを実施し，大統領にサイバーセキュリティに関する権限を集中させる，という議論もおきている．

はたして米国のサイバーセキュリティ政策が今後もこの方向で進むかどうかは今後の諸事情によると思われるが，以前よりサイバー攻撃が目につくようになった情勢を考えると，緊急時の対応にトップダウンアプローチを取り入れようという動きは，アメリカ以外でも起きてくるのかもしれない．

おそらく，具体的な仕組みを構築，運営するには，各組織の特性（人，物をはじめとして）を考慮しなくてはならないし，理想的なモデルは，組織によって異なってくることもあるだろう．個別に見れば「ベストプラクティス」なのかもしれないが，複数のモデルに見られる共通の法則，規則などを調べることで，汎用的にほかの組織にも適用可能なものがあるのではないだろうか．

参　考　文　献

1) 山川智彦：CSIRT と情報セキュリティガバナンス，*CSS2007*, p.471 (Oct. 2007).
2) JPCERT コーディネーションセンター：JPCERT/CC に関してよくある質問と答え（オンライン）．http://www.jpcert.or.jp/faq.html#1a03 (参照 2009-11-18).
3) JPCERT コーディネーションセンター：「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インシデント対応とは（オンライン）．http://www.jpcert.or.jp/ir/ (参照 2009-11-18).
4) JPCERT/CC：経営リスクと情報セキュリティ—CSIRT：緊急対応体制が必要な理由 (Dec. 2008).
JPCERT コーディネーションセンター：CSIRT マテリアル構想フェーズ（オンライン）．http://www.jpcert.or.jp/csirt_material/concept_phase.html (参照 2009-11-18).
5) Alberts, C., Dorofee, A., Killcrece, G., Ruefle, R. and Zajicek, M.: Defining Incident Management Process for CSIRTs: A Work in Progress (CMU/SEI-2004-TR-015). Pittsburgh, PA, Software Engineering Institute, Carnegie Mellon University (Oct. 2004) (online). http://www.sei.cmu.edu/pub/documents/04.reports/pdf/04tr015.pdf (参照 2009-11-18) p.16.
6) 前掲・文献 5), p.129 (Oct. 2004).
7) 前掲・文献 5), p.152 (Oct. 2004).
8) 前掲・文献 4) (Dec. 2008).
9) 前掲・文献 4), p.1 (Dec. 2008).
10) 前掲・文献 4), p.2 (Dec. 2008).
11) 前掲・文献 4), p.3 (Dec. 2008).
12) Department of Homeland Security: National Strategy for Homeland Security (July 2002) (online). http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf (参照 2009-11-18).
13) Department of Homeland Security, Homeland Security Presidential Directive/HSPD-5 (Feb. 28, 2003) (online). http://www.dhs.gov/xabout/laws/gc_1214592333605.shtm#1 (参照 2009-11-18).
14) Department of Homeland Security, Homeland Security Presidential Directive/HSPD-8 (Dec. 17, 2003) (online). http://www.dhs.gov/xabout/laws/gc_1215444247124.shtm (参照 2009-11-18).
15) Department of Homeland Security, Homeland Security Presidential Directive/Hspd-7 (Dec. 17, 2003) (online). http://csrc.nist.gov/drivers/documents/Directive-hspd-7.html (参照 2009-11-18).
16) HSEEP の概要は国土安全保障省のウェブサイトに詳しい (online). https://hseep.dhs.gov/pages/1001_HSEEP7.aspx (参照 2009-11-18).
17) About HSEEP (online). https://hseep.dhs.gov/pages/1001_About.aspx#HSEEPOverview (参照 2009-11-18).
18) 日本語での参考文献として以下が公開されている．
• 北村和生：本番で役立つ危機管理演習/訓練体系（2004 年 12 月 29 日），TRC EYE Vol.59（オンライン）．http://www.tokiorisk.co.jp/risk_info/up_file/200412292.pdf (参照 2009-11-18).
• 同：『After Action Review』という手法（2004 年 12 月 29 日），TRC EYE Vol.60（オンライン）．http://www.tokiorisk.co.jp/risk_info/up_file/200412294.pdf (参照 2009-11-18).
• 同：MSEL を使った演習指導計画書の作成要領の骨子（2005 年 12 月 28 日），TRC EYE Vol.82（オンライン）．http://www.tokiorisk.co.jp/risk_info/up_file/200512281.pdf (参照 2009-11-18).
19) 内閣官房情報セキュリティセンター：情報セキュリティ政策会議「第 1 次情報セキュ

リティ基本計画—『セキュア・ジャパン』の実現に向けて」（2006 年 2 月 2 日）（オンライン）．http://www.nisc.go.jp/active/kihon/pdf/bpc01_ts.pdf (参照 2009-11-18).
20) 内閣官房情報セキュリティセンター：情報セキュリティ政策会議「第 2 次情報セキュリティ基本計画— IT 時代の力強い「個」と「社会」の確立に向けて」（2009 年 2 月 3 日）（オンライン）．http://www.nisc.go.jp/active/kihon/pdf/bpc01_ts.pdf (参照 2009-11-18).
21) 内閣官房情報セキュリティセンター：情報セキュリティ政策会議「政府機関の情報セキュリティ対策のための統一基準（第 2 版）」（2007 年 6 月 14 日）（オンライン）．http://www.nisc.go.jp/active/general/pdf/k303-071.pdf (参照 2009-11-18).
22) 内閣官房情報セキュリティセンター：情報セキュリティ政策会議「重要インフラの情報セキュリティ対策に係る行動計画」（2005 年 12 月 13 日）（オンライン）．http://www.nisc.go.jp/active/infra/pdf/infra_rt.pdf (参照 2009-11-18).
23) 情報セキュリティ報告書について（経済産業省情報セキュリティ政策室）：内閣官房情報セキュリティセンタ情報セキュリティ報告書専門委員会資料（オンライン）．http://www.nisc.go.jp/conference/seisaku/sec_report/dai1/pdf/1siryou08.pdf （参照 2009-11-18).
24) Governing for Enterprise Security (online). http://www.cert.org/archive/pdf/05tn023.pdf (参照 2009-11-18). Governing for Enterprise Security Implementation Guide (online). http://www.cert.org/governance/ges.html (参照 2009-11-18).

(平成 21 年 8 月 11 日受付)
(平成 22 年 1 月 8 日採録)

推　薦　文

本論文の筆者は CSIRT（Computer Security Incident Management Team）の概念とそこで取り上げられるマネジメント形態が企業等の組織にも有益であるとの認識を前提として，一般的な CSIRT での理解とされる「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のアプローチから抽出し，日本企業にも適用可能な形でアレンジすることを目指し，研究を進めている．本論文では特にわが国での実務上問題となりうる諸点を法的課題として紹介し，インシデントマネジメントのアイデアがわが国企業，政府機関等の組織での普及・展開を図るうえでの今後の課題を指摘している．

9.11 テロの教訓によりアメリカでは「ホーム・ランドセキュリティ」が叫ばれるようになった．その日本版として提唱されたのが「ホーム・アイランドセキュリティ」であるが，CSIRT の法的問題や JPCERT/CC への一極依存への危惧に対する指摘等，具体的な内容の紹介や提言をした論考はほとんどない．これらの点に対し，本論文は米国のアプローチの研究をふまえて，日本にこれを応用する場合の検討を行ったものとして貴重である．特に今や基本インフラとなった情報インフラ分野においてセキュリティ演習を行うことは非常に重要である．災害時に医療現場で用いる「トリアージ」の手法をインシデントレスポンスに用いる提言は興味深い．

上記をふまえると，本論文の価値は，今後ライフログ，パーソナライズサービスなどで重要になる情報セキュリティインシデントマネージメントの課題を分析し，その重要性を示したうえ，さらにアメリカに比較して遅れている企業における情報セキュリティガバナンスの定着を訴えるなど現在の産業界にとっても非常に大きな意味を持つ点に認めることができる．以上から，本論文を研究会推薦論文として強く推薦するものである．

（電子化知的財産・社会基盤研究会主査　亀山　渉）

山川　智彦（正会員）

1965 年生まれ．1988 年東京大学法学部卒業，1995 年東京大学大学院法学政治学研究科修了（修士）．日本電信電話株式会社（NTT）研究企画部門プロデュース担当担当部長．1988 年 NTT 入社後，情報通信総合研究所，NTT データ勤務を経て，2009 年 4 月から現職．国際私法，通商法の観点から電子商取引に関する法制度問題，公共政策課題を研究，「貿易と関税」誌等に成果の一部を公表．サイバーセキュリティ，内部統制と IT マネジメント関連での調査・研究にも取り組んでいる．主な著書に『サイバーセキュリティの法と政策』（共著，NTT 出版），『デジタル ID 革命』（共著，日本経済新聞社）等がある．