連 載

組織とストーリーテリング　CSIRT における展開（2）

杉浦芳樹（すぎうら　よしき）
NTT-CERT
吉田尊彦（よしだ　たかひこ）
NTT-CERT
林　郁也（はやし　いくや）
NTT-CERT

1．はじめに

3回にわたって、組織における「ストーリーテリング（storytelling）」の研究を紹介する連載の2回目となる今回は、その実践フィールドであるCSIRT（シーサート、Computer Security Incident Response Team）の概要となぜこうした情報セキュリティの最先端の場において、ストーリーテリングが必要なのかを紹介する。

2．CSIRT とは

我々が所属するNTT-CERT（www.ntt-cert.org）はNTTグループのCSIRTである。この「CSIRT」が一般的にどのような組織であるかを最初に紹介する。

近年の情報システムの高度化と複雑化に伴い、情報システムなどをターゲットとした攻撃の手法も複雑かつ巧妙化してきている。そのため、ウイルス検知ソフトやファイアウォールの導入といった既存の情報セキュリティ対策では防ぎきれなくなってきている。そのような中、企業の情報セキュリティ担当者は同じような問題を抱えている。具体的には、以下のような点が挙げられる。

（1）同じようなウイルス感染や情報漏えいなどの事故がさまざまな部署で同じように繰り返されている。
（2）事故への対応がその場限りの付け焼刃であり、包括的な対策が取れない。
（3）情報セキュリティ対策の社内周知が徹底されない。

このような問題を解決するための社内全体を見渡した情報セキュリティ対応体制の中核をなす専門チームを一般的にCSIRTと呼ぶ。これは、「どんなに防御策を講じても、事故を完全に防ぐことはできない」という「事故前提」の考えに基づき、あらかじめ事故が発生した場合に備えて準備され、訓練された専門組織である。たとえて言えば、企業内に設置された「消防団」のような組織である。この専門組織であるCSIRTを中心に全社的な対応体制（対応プロセス、エスカレーションパス、権限委譲など）を整備しておくことが必要なのである。

これは、事故が起きてから慌てて対応体制を用意するのではなく、あらかじめ用意しておけば、対応が速やかに行われ、それゆえに2次被害を防ぎ、被害を最小限に抑えることが可能となるという「当たり前のこと」を実現するためのものとも言える。

このCSIRTは米国で生まれたものだが、既に日本でもいくつかの企業（または団体など）がCSIRTを設置している。日本国内のCSIRTのコミュニティである日本シーサート協議会（www.nca.gr.jp）には2011年4月現在、19チームが加盟している。

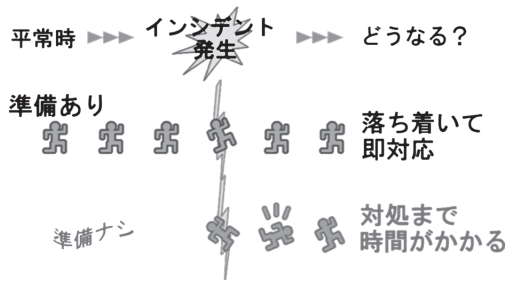

図1　いざ事故が起きたら

3. CSIRTの歴史

CSIRTが生まれる直接のきっかけとなったのは、1988年11月2日に発生し、インターネット上で感染を広めた「モリスワーム」と呼ばれる自己増殖型の悪性プログラムである。当時のインターネットに接続していたのは、一部の学術研究機関などに限られていたが、それでも世界中の約6,000台のコンピュータに感染し、当時のインターネットシステムの約10%を停止させたと言われている。しかし、当時はこのような事態をほとんど誰も想定していなかったため、対応する体制もなく、被害の実態がつかめないうえに、原因はおろか、「何が起こっているのか」すら、知ることができなかった。そのため被害は拡大する一方となったのである。

この事態を重く見た米国は、国防総省の資金援助の下、世界で最初のCSIRTとなるCERT/CC（CERT Coordination Center, www.cert.org）を同年11月17日（モリスワーム発生から約2週間後）に米国カーネギーメロン大学ソフトウェア工学研究所に設置した。CERT/CCは現在でも最も権威のあるCSIRTの1つである。

その後、さまざまな国や企業、組織にCSIRTが作られるようになった。そして1989年10月に発生した「ワンクワーム」をきっかけに、国境のないインターネット上で情報セキュリティ事故（以降、「インシデント」と呼ぶ）に対応するには国境を越えたCSIRT同士の情報交換が重要との考えから、1990年に当時の主だったCSIRTを中心にCSIRTの国際フォーラムFIRST（Forum of Incident Response and Security Teams, www.first.org）が設立された。2011年4月現在、FIRSTには世界中から200を超えるCSIRTが加盟している。加盟しているCSIRTは、いわゆる「IT関連企業」のCSIRTだけではない。大学をはじめ、銀行やカード会社、航空会社など、ITを利用する立場の企業や団体などのCSIRTも数多く加盟している。

一方、日本では、1992年にボランティアベースで日本最初のCSIRTであるJPCERTが活動を開始した。その後体制を整備し、1996年10月にJPCERT/CC（www.jpcert.or.jp）として本格的に活動を開始し、1998年8月に日本で最初にFISRTに加盟した。ちなみに、我々が所属するNTT-CERTは2003年7月1日に活動を開始し、2005年1月にFIRSTに加盟した。

4. CSIRTの実際

CSIRTと一言で言っても、その体制や活動内容は千差万別である。極端に言ってしまえば、2つとして同じCSIRTは存在しない。つまり「インシデントに対応する」という基本的な目的は同じでも、その「対応の仕方」がCSIRTによって大きく異なるのである。

JPCERT/CCの「CSIRTガイド」によれば、一般的にCSIRTは次の6つのタイプに分類される。

- 組織内CSIRT
- 国際連携CSIRT
- コーディネーションセンター
- 分析センター
- ベンダチーム
- インシデントレスポンスプロバイダ

この中で「組織内CSIRT」が、一般的に企業に設置される「企業内CSIRT」と呼ばれるもので、社内および顧客に関連したインシデントに対応する。「国際連携CSIRT」とは、前述の日本初のCSIRTであるJPCERT/CCのように、インシデントに関して海外と情報交換する際の国際的な「窓口」として機能するCSIRTである。「コーディネーションセンター」は、インシデントに関係している企業や部署、他のCSIRTなどとの情報連携、調整を行う。ここにはグループ企業間の連携が含まれる。「分析センター」はインシデントの傾向分析やウイルスなどの悪性プログラムの解析、攻撃の痕跡分析などを行い、必要に応じて注意喚起を行う。「ベンダチーム」は自社製品のセキュリティ上の欠陥（一般的に「脆弱性」と呼ぶ）に対応し、修正プログラムの作成や利用者への注意喚起などを行う。「インシデントレスポンスプロバイダ」は、組織内CSIRTの機能（の一部）を有償で請け負うサービスプロバイダであり、監視サービスなどを行っている「セキュリティベンダ」のことである。

多くのCSIRTはこれらの6つのタイプのうち複数の「機能」を有している。例えば、JPCERT/CCは「国際連携CSIRT」であるが、同時に国内外の関連企業や組織との情報連携や調整を行う「コー

ディネーションセンター」でもあり、さらに「分析センター」としての機能も有している。

また、我々NTT-CERTはNTTグループの「組織内CSIRT」であるが、同時にNTTグループ企業間の連携を行う「コーディネーションセンター」でもある。他にも「分析センター」としての機能も有している。

ここでNTT-CERTの、NTTグループの「コーディネーションセンター」としての業務を簡単に紹介する。

NTT-CERTはNTTグループが何らかの形で関わっているインシデントに対応する。そのために対外的な窓口を用意している。例えば、NTTグループのある企業のあるサイトが改ざんされ、ウイルスなどの悪性プログラムを配布するサイトにされていたとする。それを外部の第三者（主に他のCSIRT）が発見した場合、サイトの停止や復旧の依頼を当該サイトの管理者に直接連絡するのが難しいケースがある。特に発見者が海外の方の場合は、個別サイトの管理者（問い合わせ先）を見つけることはほとんど不可能に近い。しかしNTTグループのサイトであることさえわかっていれば、その情報をNTT-CERTに提供してくれるだけで、NTT-CERTで適切な問い合わせ先を見つけて連絡し、対応（サイトの停止や復旧など）を依頼することができるのである。

このような「窓口」および「調整」がNTT-CERTの「コーディネーションセンター」としての業務の中心となっている。

5. なぜ“ストーリーテリング”なのか

本研究は、NTT-CERTに限らず、一般的にCSIRTが抱えている業務上の課題を解決するにはどうすれば良いかという問題意識から始まっている。CSIRTの必要性を何とか経営層に理解させ、CSIRT設立にまで至っても、その活動を継続するにはさまざまな課題があるのだ。

CSIRTの活動はCSIRT（の属する企業）ごとに大きく異なるが、多くのCSIRTは「発生したインシデント」に対応する。そのため、想定されるインシデントを洗い出し、それぞれのインシデントに対する対応マニュアルや手順書を整備したり、それに基づき、他の社員に対して教育や演習を実施したりする。しかし現実にはこのような「抽象化」はきわめて難しい。それは、日々発生するインシデントが複雑多岐に亘っており、またCSIRTがサービスを提供する相手（Constituency＝社員、顧客など）が（特に大企業の場合）きわめて多様だからである。また手順書にこだわることで、手順書に依存し過ぎてしまい、イレギュラーな事態に対応できなかったり、「言われたからやる」という意識で実質的な対応ができなかったりする危険性もある。つまり、手順書などの「決まり」だけでは対応しきれないのがCSIRTの活動なのである。

事実、インシデントの発生（または予兆）の検知や被害規模の見込み（リスク予想）は、経験に基づく「想像力とそこからの連想」に依存する場合が多く、これは手順書やマニュアルには記載されない（できない）ものなのである。

このようにCSIRTの活動に求められる「抽象化できない部分」の補足や「暗黙知」の発見、更には「想像力とそこからの連想」には、「物語」「ナラティブ」を通して「価値観や“マインド”を共有」することが有効だと考えたのである。

6. CSIRT Modeling Architecture（CMA）

本研究は、我々が数年前から研究を進めている「CSIRT Modeling Architecture（CMA）」を支える2本の柱の1つとして実施されている。

CMAとは、(1)既に運用を始めているCSIRTが、その運用の過程で、攻撃の複雑化などの技術的な要因や、CSIRTの親組織内での位置づけといった組織的な要因など、さまざまな要因によりCSIRTの機能の追加、拡張、変更を実施する際に利用可能なモデル化の手法（モデリング）を検討分析し、(2)その検討分析結果に基づき、組織化の視点も考慮した上で、これら「モデリングのためのアーキテクチャ（モデリングアーキテクチャ）」の可能性の検討、提案を行うことを目的としている。

ここでモデリングアーキテクチャとは、CSIRTの機能の追加、拡張、変更を必要とさせる個々の要件、要因をモデリングし得るか否かを判定するための材料となる。またモデリング可能な場合は、それぞれのモデリングの関連、関係、相関、影響を考慮

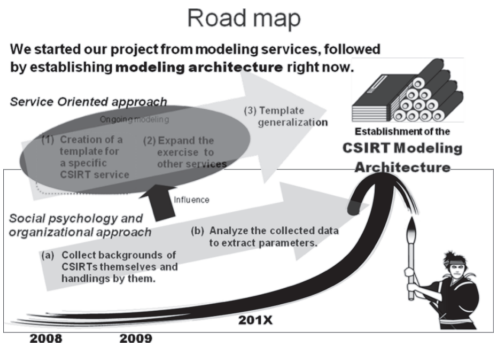

図 2　CSIRT Modeling Architecture の概要

した設計概念を提供するものである。

CMA の研究の 2 本の柱（アプローチ手法）は「モデリング」と「組織化」である。

「モデリング」については、CSIRT 構築に関する既存のさまざまな文献（CERT/CC の教育プログラムやヨーロッパの TF-CSIRT による TRANSITS など）を参考に、CSIRT の新規構築のためではなく、運用中の CSIRT のサービスの追加や見直し、評価などに利用できるサービステンプレートを作成するところから始めている。既にいくつかのサービスについてテンプレートを作成し、複数の CSIRT に適用することで完成度を高める段階に来ている。

一方、「組織化」については、特定の CSIRT（NTT-CERT）を対象にして、その CSIRT を特徴づけるファクターを抽出することから始めている。そのために、まず NTT-CERT がこれまでに経験したインシデント対応の事例を基にいくつかの「物語」を作成した。中には 1 つの事例を対象に、現場担当者の視点で作成した物語とマネージャ視点で作成した物語をそれぞれ別に作成したものもある。これらの「物語」は既存の手順書やマニュアルを補完し、「価値観や“マインド”を共有する」ための資料として有効に使えることが期待できる。また、研究の主目的ではないが、副次的な成果として、新人教育の教材としての利用も可能であることがわかっている。

7. おわりに

CMA の研究全体としては本来の目的に向けてまだまだ途上の段階であるが、研究を進める過程で、さまざまな成果が得られている。特に「組織化」のアプローチでは興味深い点がいくつか見出されている。そこで次回は、研究の中で見出された具体的な事例と知見について紹介する。

注

本稿は、2009 年に京都で開催された FIRST の年次会合「21st Annual FIRST Conference」で発表した『CSIRT Modeling Architecture（発表者：吉田尊彦など）』の内容を含んでいる。

参考文献

［1］JPCERT/CC『CSIRT ガイド』, 2008 年, 6 ページ. http://www.jpcert.or.jp/csirt_material/files/guide_ver1.0.pdf

［2］CERT/CC 教育プログラム, Creating a Computer Security Incident Response Team. http://www.sei.cmu.edu/training/P25.cfm

［3］Managing Computer Security Incident Response Teams.http://www.sei.cmu.edu/training/p28.cfm

［4］TF-CSIRT “TRANSITS (Training of Network Security Incident Teams Staff”. http://www.ist-transits.org/

略歴

杉浦　芳樹（すぎうら　よしき）

NTT-CERT リサーチスペシャリスト。平成 10 年よりセキュリティおよび CSIRT の活動に携わる。平成 16 年に NTT に入社、NTT-CERT の設立を行い、現在は NTT-CERT のインシデントハンドリングチームおよび CSIRT 構築 / 運用支援に携わっている。NCA 運営委員。

吉田　尊彦（よしだ　たかひこ）

NTT-CERT シニアメンバ。インシデントハンドリング運用の中核に携わり、NTT グループ内外を問わず CSIRT 啓発・運用支援活動を行う。

林　郁也（はやし　いくや）

NTT–CERT シニアメンバ。インシデントハンドリング運用に携わり、NTT グループ内外を問わず CSIRT 啓発・セキュリティ教育活動を行う。