特集　情報セキュリティ

サイバー攻撃の動向とセキュリティの対応体制

東京大学大学院情報学環
特任准教授　満永　拓邦

1．はじめに

近年、国内組織においてサイバー攻撃による情報漏えい等の被害が相次いでいます。以前は、予防的な対策によって被害の発生を防ぐことが情報セキュリティの主流的な考え方でありましたが、攻撃手法の巧妙化に伴い、予防対策では十分に対処しきれない事例も出てくるようになりました。そのため、事前の対策を十分に行うことと併せて、万が一のインシデント発生のリスクに備えたセキュリティ対応体制の構築が必要になってきています。

インシデント発生の抑止と被害の最小化にあたって重要な役割を果たすのが、CSIRT(Computer Security Incident Response Team)と呼ばれる組織のセキュリティインシデントを専門に扱うチームであります。本稿では、CSIRTの必要性、形態、サービスなどを解説するとともに、攻撃情報の共有による被害軽減について解説します。

2．CSIRTの必要性

インシデントの発生を想定していない組織では、対応手順やルール（例えば、各部門の担当者、役割、権限、報告方法など）が定まっていない、あるいは定まっていても形骸化していることが多く、初動対応に遅れが生じます。例えば、学生向けに教務情報を提供しているWebサーバが攻撃者に侵入され、他の組織への攻撃に踏み台として悪用されている場合を想定します。意図的ではないにせよ、攻撃に加担してしまっているため、速やかにサーバを停止するなどの対応が求められます。しかし、システム担当の判断だけで当該Webサーバを停止することは難しいです。サーバを停止する作業自体は容易であるが、システム担当はサーバを停止する権限を持たず、停止による業務影響（学生からの問い合わせ等）に対処できないためであります。責任者に事象を報告し判断を仰ぎ、関係部門と協議した上で、組織的な対応を取る必要があります。組織外に対しても、攻撃に加担してしまった状況を踏まえて広報部門と連携したプレスリリース発信や、被害組織に対する折衝を法務部門と連携して進めるなど組織横断的な対応が必要になります。そうした複雑な情報伝達と意思決定のプロセスを迅速に実施するために、インシデントの発生に備えて、予め対応手順やルールが明確に定められることが望まれます。

また、組織運営という観点からは、手順やルールに加えて、実質的なセキュリティ業務を行う担当者を確保する必要があります。インシデント発生時に明確な役割が与えられた要員がいないと、現実的な対応は困難です。そのため、組織内で発生したセキュリティインシデントに対して迅速に動ける体制(CSIRT)を平時から作っておくことは、インシデントの被害抑止のために非常に重要です。

3．CSIRTの形態

CSIRTを構成する形態は多種多様ですが、以下に代表的な形態を５つ紹介します。

（1）セキュリティチーム（次ページ図１参照）

専従担当者を設置せず、インシデントの発生に応じてIT部門の部員、システム管理者やネットワーク管理者などを招集し、対応チームを結成します。独立した部門の形態を取らないため、コストを低く抑えられるというメリットがあります。その反面、インシデント対応のみを目的とする仮想的なチームであるため、活動内容や提供するサービスは限定的となります。さらに外部の組織に対する窓口としては機能しにくいというデメリットがあります。

（2）分散型CSIRT（図２参照）

CSIRTの統括や調整を行う責任者の下、各部門の担当者をCSIRTのメンバーに指名します。メンバーは他の部門業務との兼務であり、インシデント発生時などにCSIRTの一員として対応にあたります。兼務であるため、CSIRT業務としてのリソースは限られているが、メンバーが所属している部門との連携が取りやすいというメリットがあります。

（3）集中型CSIRT（図３参照）

CSIRTとして正式に独立した部門として定義し、インシデント対応に責任を負います。メンバーはCSIRT専任であるため、CSIRTの業務に集中できるメリットがある反面、人件費がかかります。セキュリティ対応に全般的な責任を持つため、経営層への報告を義務付けられていることが多いです。

（4）統合（分散／集中）型CSIRT（図４参照）

分散型と集中型を組み合わせたCSIRTです。インシデント発生時には、各部門から指名されたCSIRTのメンバーが加わるため、現場に即した対応が可能です。また、専任メンバーを部門のリーダーとして配属させることで、独立した部門として責任を持って活動できます。

（5）調整型CSIRT（図５参照）

比較的規模の大きな組織で、企業の例では親会社がグループ会社を統括するために設置するCSIRTです。そのため、技術的な支援よりは、調整を担うことが多いです。

組織の構成や文化に適した形態のCSIRTの検討が必要です。それぞれの形態にメリットとデメリットがあり、最初は突発的に発生するインシデントに対応するために、まずは（1）のセキュリティチームから始めて、より計画的、組織的にインシデントに対応するために、分散型、集中型、統合（分散／集中）型のCSIRTへと発展させることが望ましいです。

4．CSIRTのサービス

CSIRTがインシデント対応のために活動する内容を「サービス」と呼びます。CSIRTを構築するためには、形態だけでなく、サービス内容や提供範囲を決めておくことが望ましいです。そのためにまずは、CSIRTが誰の(何の)ために活動するかを明確にする必要があります。大学のCSIRTでは、本部に所属する職員が業務上保有する情報資産をインシデントの被害から守る、あるいは大学のWebサイトを攻撃から守るなどが例として考えられます。それ以外にも、各学部・大学院に所属する教職員が保有する情報資産も対象とするか、学生に対するセキュリティ関連の相談対応を行うか、教職員向けのセキュリティ講習会を実施するかなど活動範囲について議論する必要があります。

次にCSIRTがサービス対象者に提供するサービス内容を明確にすると、活動範囲が定まります。活動範囲が明確になると必要なリソース（人や予

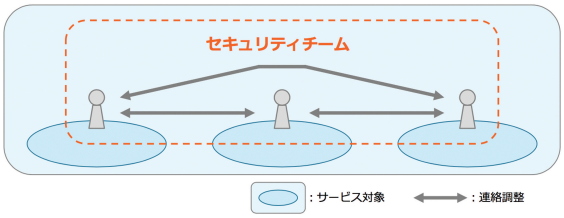

図１　セキュリティチーム
（出典　JPCERT/CC,「CSIRTマテリアル」）

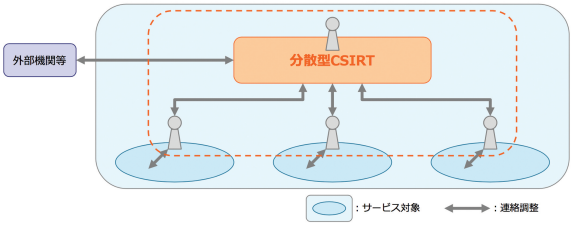

図２　分散型CSIRT
（出典　JPCERT/CC,「CSIRTマテリアル」）

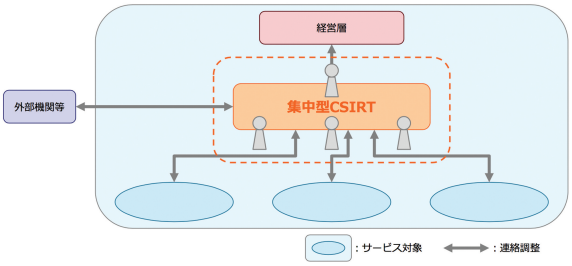

図３　集中型CSIRT
（出典　JPCERT/CC,「CSIRTマテリアル」）

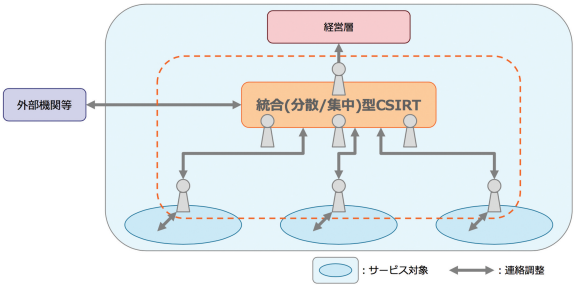

図４　統合（分散／集中）型CSIRT
（出典　JPCERT/CC,「CSIRTマテリアル」）

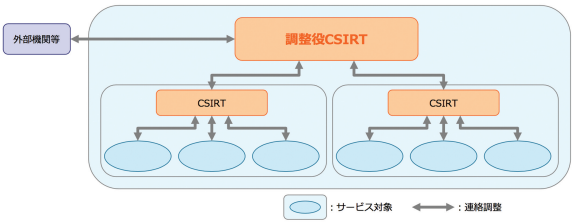

図５　調整型 CSIRT
（出典　JPCERT/CC,「CSIRTマテリアル」）

表１　サービスの分類の例（出典　JPCERT/CC,「CSIRTマテリアル」）

事後対応型サービス	事前対応型サービス	セキュリティ品質管理サービス
・アラートと警告 ・インシデントハンドリング - インシデント分析 - オンサイトでのインシデント対応 - インシデント対応支援 - インシデント対応調整 ・脆弱性ハンドリング - 脆弱性分析 - 脆弱性対応 - 脆弱性対応調整 ・アーティファクトハンドリング - アーティファクト分析 - アーティファクト対応 - アーティファクト対応調整	・告知 ・技術動向監視 ・セキュリティ監査または審査 ・セキュリティツール、 アプリケーション、インフラ、 およびサービスの設定と保守 ・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提供	・リスク分析 ・ビジネス継続性と障害回復計画 ・セキュリティコンサルティング ・意識向上 ・教育 / トレーニング ・製品の評価または認定

算など）やどのようなインシデントに注力すべきかが見えてくるはずです。以下に、CSIRTが提供するサービスの例について紹介します。（表１参照）

（１）事後対応型サービス（インシデント発生時に提供するサービス）

実際に発生しているインシデントに対応します。消防で例えるなら、火災発生時の消火活動と事後の原因分析などがこれに当たります。以下は、事後対応型サービスとして実施すべき事項の例です。

１）アラートと警告

セキュリティインシデントを示唆するアラートや予兆を捕捉し、対応が必要な部門へ通知を行い、対処に関する情報を提供します。また、ハブ機関（後述）から提供されるインディケータ情報を起点として、自組織の被害状況を確認します。具体的には、通信ログの確認や、適切な部門に対して確認を依頼します。インディケータに該当する情報が検出された場合は、インシデントハンドリングを実施します。

２）インシデントハンドリング

インシデント対応の現場に駆けつけて、直接対応を支援する「オンサイトでのインシデント支援」、電話会議やメールなどで遠隔から支援する「インシデント対応支援」、インシデントに関与する関係者同士の調整役となる「インシデント対応調整」などが含まれます。

３）脆弱性ハンドリング

脆弱性に関する情報を収集・分析し、自組織で使用しているハードウエアやソフトウエア、それらを利用するシステムへの影響を確認し、必要な対処（パッチの適用や回避策など）を実施するための情報を適切に通知します。

（２）事前対応型サービス（インシデントに対する準備として提供するサービス）

インシデントが発生する前に情報を収集し、インシデント発生の抑止や、発生時の被害を極小化するための対処を事前に実施します。消防でいうところの、装備や車両のメンテナンスや情報収集などです。以下は、事前対応型サービスとして実施すべき事項の例です。

１）告知やアナウンス

新たに発見された脆弱性に対する情報や流行している攻撃手法、技術的動向等をサービス対象者に通知します。

２）技術動向把握

新しい技術や攻撃活動に関する動向を収集する。収集対象の情報は、ニュースサイトやセキュリティベンダのサイトなどに加え、国内外の法令・法案、政治的脅威を含む社会的脅威も含まれます。収集した情報は、サービス対象者が理解しやすく、受け取りやすい形で通知します。

３）セキュリティ監査または審査

組織または該当する他の業界標準で定義された要件に基づき、組織のセキュリティ対策状況に対する監査または審査を実施します。

４）セキュリティツール、アプリケーション、インフラ、およびサービスの設定と保守

CSIRTやサービス対象者が使用するツール、アプリケーション、および一般的なコンピュータ設備を安全に設定・保守する方法に関する適切なガイダンスを提示します。

５）侵入検知サービス

セキュリティ機器（ファイアウォールやIDS、WAFなど）のログの分析、検知したイベントへの対応を行い、連絡ルートに基づいてイベントの発生を通知し、対処を促します。スムーズな対応を行うために、あらかじめ発動のためのしきい値（判断基準）や連絡ルート、手順を定義しておくことが望ましいです。

（３）セキュリティ品質管理サービス（組織のセキュリティレベルを高めるサービス）

リスク分析や教育等の活動を通じて自組織の状況を把握し、セキュリティレベルを向上するための活動を行います。消防でいうところの、地勢や家屋の状況把握、防災訓練などがこれにあたります。以下は、セキュリティ品質管理サービスとして実施すべき事項の例です。

1）リスク分析

自組織で保有している情報資産の価値や機密性（知的財産、個人情報など）を評価し、資産に対して攻撃を受ける脅威を評価します。具体的には、情報資産リストの作成や、インターネットから情報資産へのアクセス可否の把握などを行うことによって、今の組織に不足している設備や対策などが具体的に見えてくるでしょう。

2）事業継続と障害復旧計画

事業経営に深刻な影響をもたらすインシデントが発生する可能性を鑑み、リスク分析の結果を踏まえた上で、大規模インシデントが発生した際に事業を継続するための障害復旧計画を検討します。具体的には、発動基準の定義、報告経路や連絡体制の整備、復旧手順書の作成などがあげられます。

3）ポリシーやガイドラインの作成

組織のセキュリティに対する考え方（ポリシー）や、それを実現するためのガイドライン、具体的な手順書を提供します。このことにより、サービス対象者がインシデントをスムーズに報告、対応する能力の向上を図ります。

4）教育／トレーニング

セミナーや組織内広報活動を通じて、サービス対象者のセキュリティの知識やスキルを向上させます。例えば、全教職員、学生に対する標的型メール訓練や、関連部門を巻き込んだインシデント対応演習があげられます。他にもWeb学習などの自主コンテンツを積極的に活用している組織も存在します。

CSIRTを構築するにあたって、紹介した全てのサービスを備えている必要はなく、組織のセキュリティ能力向上に必要なサービスを選択します。JPCERT/CCの調査によると、多くのCSIRTではインシデントハンドリングサービスやトレーニングを提供している[1]。国内のCSIRTが提供しているサービスについては参考文献[1]を参考にして下さい。

またCSIRT活動を継続していれば、サービス対象者や経営層からの意見や要望を受けサービスの見直しを求められることもあります。これらの声に耳を傾けつつ、活動を定期的に評価し、見直す仕組みを設けることで、より実効的なCSIRTとなります。強調しておきたい点は、CSIRTはその存在自体を目的にするものではなく、インシデントによる被害の軽減を目的として、新たな脅威に対応すべく常に改善し続けるものです。

5．CSIRTに期待される役割

CSIRTに求められる役割は、発生したインシデントに対応するための技術的なスキルや要素だけではないです。効果的な情報連携を行うにあたって、組織内の他部門（システム管理部門、サービス提供部門、広報、経営など）や、外部組織（他社のCSIRT、JPCERT/CC、セキュリティベンダなど）との協力関係が必要とされます。

CSIRTは、組織内の連絡体制だけでなく、社外との連絡・調整を遂行する上でも重要な役割を果たしています。日常から、組織内の部門間の連携はもちろん、社外との情報交換・協力関係を構築しておく必要があります。そのためには、日常からセキュリティの動向を把握し、積極的に様々なセキュリティ関係のワーキンググループや情報共有の枠組みへの参加などを行い、他組織と信頼関係を構築しておくことが大切です。このことがCSIRTの活動はインシデント対応のみならず、平時の活動が重要と位置づけられている所以でもあります。

また、組織の現状を踏まえた上で、適切な状況判断を行うことが求められます。例えば、インシデント発生時の対応チームを構築する際には、組織における要件や利用できるリソースと照らし合わせて、慎重に検討を行った上で要員を配置することが求められます。

これらの役割を適切に遂行することで、CSIRTは一歩ずつ、組織内外から信頼される組織に成長していくことになります。それを支えているのは、前述の通り、地道な活動に他ならないです。

ここで、CSIRT同士の連携についても触れておく。CSIRTは有事だけではなく平時にも発生したインシデントの情報や、インシデントの予兆について交換し合うことがあります。場合によっては機微な情報を交換する可能性があるため、CSIRT同士の連携に際して事前に秘密保持契約を締結しておく方が安全です。また情報の取り扱いについては十分な注意を払う必要があります。ある組織で発生したインシデント情報が意図しない経路や範囲に伝わってしまうと、組織内外からの信用や期待を裏切ることに繋がってしまいます。

6．ハブ機関を通じた情報共有

CSIRTの役割の一つとして外部の組織との連携があり、日ごろからの情報共有が重要であることは前述の通りです。個別に他の組織と信頼できる関係を構築することに加えて、近年では複数の組織が、中核となるハブ組織を通じて情報連携等を推進する取り組みも増えています。ハブ組織は同業種で構成される業界団体や協会、あるいは公的な事業を行う組織（JPCERT/CCやIPA等）が担うことが多いです。私立大学であれば私立大学情報教育協会にて情報共有の検討が進んでいます。ハブ機関を通じて、脅威情報や脆弱性情報の送受信や情報共有の場に参加する機会を得ることが可能

となります。

ハブ機関を通じた情報共有を行うメリットとして、以下があげられます。

・信頼性が高い情報を幅広く入手することが可能になる：ハブ機関は国内外の広い範囲で情報を収集しているため、自組織や関連組織だけでは得ることができない幅広い情報を入手することが可能になります。また、ハブ機関で分析を行った上で有効と判断した情報を提供しているため、比較的信頼性が高い情報を入手することができます。

・インシデント情報などの機微情報を安全に共有できる：ハブ機関は、各組織と機密情報契約を締結しているケースが多いです。インシデント情報などを共有する際に、ハブ機関が組織固有の機微な情報などを削除した上で適切な範囲に共有するため、インシデントなどの機微な情報についても安全に共有することができます。

図６は、ハブ機関を通じた情報共有のイメージです。ここでは、ハブ機関の例として日本の国際連携CSIRTであるJPCERT/CCをあげています。

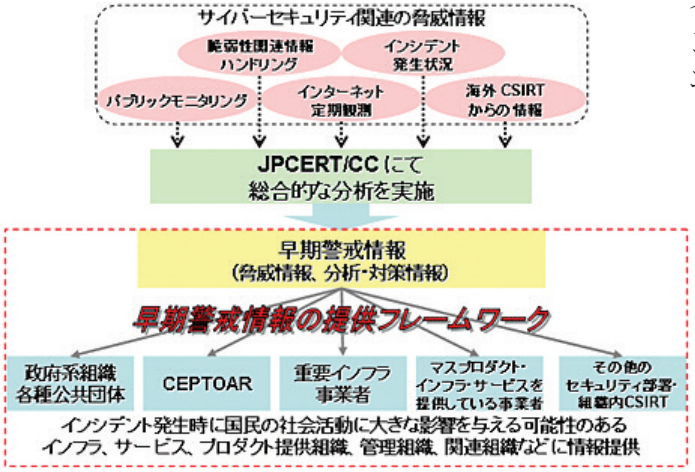

図６　早期警戒情報の流れと情報提供フレームワーク
（出典　JPCERT/CC,「早期警戒情報の提供について」）

ハブ機関が提供する情報の例としては、以下のようなものがあります。

・脆弱性情報：効果的なセキュリティ対策である脆弱性対応を通じて、インシデントを未然に防ぐために、脅威度の高い脆弱性の情報を提供します。

・インディケータ：インディケータとはサイバー攻撃を検知するために有効な情報のことを言います。具体的には標的型攻撃で使用されるIPアドレスやURLなどのマルウエアの通信先があります。

・個別組織に対する通知：被害を受けている可能性がある情報などについて、ハブ組織から該当組織に個別に通知を行うことがあります。例として、感染が疑われる端末に関する情報や、情報漏洩の可能性などについて、通知する場合などがあります。

これらの情報を受信したCSIRTは、これらの情報を分析して適切な部門に展開する必要があります。特にインディケータや個別に通知された情報については、インシデントの未然防止や被害抑止に直結する情報である可能性が高いため、迅速にハンドリングできる体制や仕組みを作っておくのが望ましいです。また、ハブ機関を通じた情報提供の活用にあたっては、業界全体のセキュリティを向上させるために、一方的に情報を受け取るだけではなく、可能な範囲で積極的に情報提供も行うことが期待されます。情報の流通が活発になることで、より深い分析を行うことが可能になり、結果的に有効な情報を追加的に提供することにつながるからです。

7. まとめ

攻撃手法の巧妙化により、予防対策のみでは対処できないケースが増えてきています。そのためにCSIRTの構築が求められているが、活動範囲はインシデント対応だけでなく、事前準備によるインシデントの抑止や被害の極小化、教育やトレーニングなど多岐に亘ります。

CSIRTは構築することが目的ではなく、適切なサービスの提供を通じて、インシデントの被害軽減を目的とします。そのためには、組織にとって適切な形態や権限を選択する必要があります。初めから完璧なCSIRT活動を目指さず、スモールスタートで活動を始めてみると良い。特にインシデントが外部からの連絡によって発覚する事例が多いことを踏まえて、インシデント報告の窓口を整備するところから初めて、定期的に見直しを行うことで、組織に必要とされるCSIRTに改善していくことが望まれます。

参考文献および関連URL

[1]JPCERT/CC,「2015年度 CSIRT構築および運用における実態調査」
https://www.jpcert.or.jp/research/2015_CSIRT-survey.html

[2]JPCERT/CC,「CSIRTマテリアル」
https://www.jpcert.or.jp/csirt_material/files/05_shape_of_csirt20151126.pdf

[3]JPCERT/CC,「早期警戒情報の提供について」
https://www.jpcert.or.jp/wwinfo/