2W-09

CSIRTにおける情報収集の方法について

宮坂　剛†　　後藤　厚宏†
情報セキュリティ大学院大学†

１．はじめに

IPA（独立行政法人情報処理推進機構）の「2014 年度 情報セキュリティ事象被害状況調査」によれば、従業員数３００人未満の中小企業でも 14% の企業がサイバー攻撃の遭遇経験有りと回答しており[1]、サイバー攻撃の脅威は大企業だけでなく、全ての企業が対象となり得る状況である。そんな中、サイバー攻撃に対応する手段として考え出された CSIRT に注目が集まっているが、日本の企業全体では、まだまだ CSIRT の構築が進んでいない状況である。CSIRT の構築が進んでいない原因はいくつか考えられるが、そのうちの１つとして、CSIRT の構築・運用をどのように行えば良いのかよく分からないと感じている企業が多いのではないかと筆者は推測している。実際に、筆者の所属する企業でも現状、コンサルティング会社に協力を仰ぎつつ、CSIRT の構築段階で試行錯誤している状況である。そこで本研究では、CSIRT の構築及び運営の一助となる事を目的とし、CSIRT の活動の中でも最も重要な活動である「情報収集」について、その実現方法を検討し、整理したいと考えている。なお、CSIRT の形態は、企業のビジネス形態及び規模に合わせて柔軟にカスタマイズされる性格のものであるため、企業によって異なる。そこで本研究では、標準的な事例として、情報セキュリティを専業とはしない、中規模以下の企業を対象に検討を行っている。

２．CSIRTにとって情報収集が重要な理由

CSIRT にとって収集すべき情報とは、主にサイバー攻撃に対抗するための情報であり、サイバー攻撃の攻撃手法や防御、対応方法、また、攻撃者に狙われる脆弱性の情報等がそれに当たる。CSIRT の活動の中で「情報収集」が最も重要な活動である理由は以下の２点である。

On information gathering method in CSIRT
Tsuyoshi Miyasaka, Atsuhiro Goto
†Institute of Information Security

① サイバー攻撃の複雑化、巧妙化に伴い、CSIRT が必要とする情報量が増加しており、１企業が単独で調査しただけでは、必要な情報を全て入手する事が不可能になっている。そのため、各 CSIRT は外部から効率的に必要な情報を収集する必要が有る。
② サイバー攻撃に対抗するための情報、特にサイバー攻撃の攻撃手法や防御、対応方法等は、インターネット等では公開されない情報である（理由は後述）。そのため、各 CSIRT は、然るべきルートを通じて外部から情報収集を行う必要が有る。情報が無ければ、自社のシステムを防御することは不可能であり、実際にサイバー攻撃を受けた場合、迅速に対応できない。

３．情報収集の方法

CSIRT の情報収集には以下の３つの方法が有る。本章では、①～③の各情報収集方法について、具体的に説明する。

①公開情報を利用した情報収集
②情報共有のためのコミュニティーを利用した情報収集
③他社の CSIRT からの情報収集

3-1 公開情報を利用した情報収集

公開情報とは、インターネットを経由して、誰しもが入手可能な情報を指す。代表的なものとしては、JPCERT/CC[2]がＨＰ上で公開している注意喚起情報、同じく JPCERT/CC が毎週発行する Weekly Report、また、JPCERT/CC と IPA が共同運営する JVN iPedia（脆弱性対策情報データベース）等が挙げられる。

公開情報から入手できるのは主として脆弱性情報であり、それ以外の情報を公開情報から入手するのは困難である。一般にサイバー攻撃に関する情報は公開されにくい傾向に有る。理由の一つは、サイバー攻撃の攻撃手法等を公開してしまうと模倣犯が現れる危険性が有ること。もう一つは、現在のサイバー攻撃は、被害者の防御責任も問われる傾向が有るため、攻撃手法

等の情報を被害者側からは公開しにくい点が挙げられる。そのため、CSIRT は、公開情報以外のルートで、サイバー攻撃に関する情報を収集する必要が有る。

3-2 情報共有のためのコミュニティーを利用した情報収集

公開情報では得られない情報を入手するために、情報共有（情報交換）を目的としたコミュニティーに参加し、コミュニティー内でのみ流通する情報を入手することは CSIRT にとって有用な活動である。コミュニティーには、業界に特化したコミュニティーと、特に業界を特定しないコミュニティーが有る。業界に特化したコミュニティーとしては、以下のコミュニティーが代表的である。

①ICT-ISAC … 情報通信技術に係る業界が対象
②金融 ISAC … 金融機関が対象
③J-SCIP … 重要インフラ機器製造業者、石油、電力、資源開発、ガス、自動車、化学の７業界が対象

また、業界を特定しないコミュニティーとしては、以下のコミュニティーが代表的である。

①日本シーサート協議会（脅威情報共有 WG）
②日本シーサート協議会（インシデント事例分析 WG）
③警察庁 サイバーインテリジェンス情報共有ネットワーク（CCI）

一般的には、業界に特化したコミュニティーの方が、その業界にとって重要な情報を選別した形で情報共有されるため、効率的な情報収集を行うことが可能と考えられる。

3-3 他社の CSIRT からの情報収集

もし各 CSIRT が保有している全てのサイバー攻撃関連情報が、コミュニティー内で共有されるのであれば、必要な情報は全てそこで入手する事が可能であるが、実際はそうではない。各 CSIRT が保有しているサイバー攻撃関連情報は以下の３つに分類される。

①外部には漏らさない機密情報
②コミュニティー内で公開する情報
③信頼関係に有り、強い協力関係を結んでおきたい特定の CSIRT（仲間の CSIRT）にのみ公開する情報

②③の切り分けは、各 CSIRT の裁量であり、自らの CSIRT 活動を優位に運ぶための戦略として②③の切り分けを利用することが可能である。そのため、参加するコミュニティーにもよるが、コミュニティー内で共有される情報だけでは情報が不足していると判断される場合、別途、③のルートを開拓し、他社の CSIRT からの情報収集を検討する必要が有る。

４．他社の CSIRT から情報収集を行う方法

業務的には必ずしも友好関係にはない他社 CSIRT から、自社 CSIRT にとって有効な情報を入手するためには、自社 CSIRT から他社 CSIRT に対しても有効な情報を提供する必要が有る。情報交換を通じて CSIRT 間の信頼関係を構築し、お互いに有意義な情報交換が行えていると認識できれば、さらに重要な情報の収集が可能になるのである。具体的には以下の方法が一般的と考えられる。

①日本シーサート協議会等のコミュニティーに参加することで、他社の CSIRT と交流する。
②情報収集のために協力関係を結びたい（仲間になりたい）CSIRT に対しては、こちらからも情報を提供することで、信頼関係を構築する。
③信頼関係に基づき、必要な情報を収集

まとめ

CSIRT がサイバー攻撃に対抗するための情報を収集するためには、最初に公開情報とコミュニティー内で共有される情報を当たり、情報が不足すると判断される場合は、他社の CSIRT からの情報収集を検討する必要が有る。また、他社の CSIRT と協力関係を結ぶためには、こちらからも情報を提供することによる信頼関係の構築が必要である。

参考文献

[1]IPA 2014 年度 情報セキュリティ事象被害状況調査 －報告書－（2015/1）
https://www.ipa.go.jp/files/000043418.pdf
（参照：2016/12/26）
[2] JPCERT/CC HP
https://www.jpcert.or.jp/
（参照：2016/12/29）