

インターネットトピック: 日本シーサート協議会

■日本シーサート協議会とその活動

日本シーサート協議会*1 は、日本国内におけるシーサート (Computer Security Incident Response Team: CSIRT) 組織の協調や情報交換を行うことで、会員組織の事案対応能力の向上を目指す団体として 2007年3月に発足しました。協議会発足時は6つのシーサートが会員でしたが、本稿執筆時点では17の組織が加盟しています*2。

一口にシーサートといってもその定義は様々ですが*3、ここでは、保護対象 (constituency) となる組織や集団を持ち、そこで発生したセキュリティ事件の解決そのものや、事案の早期検出、分析結果等を用いた注意喚起で保護対象のセキュリティ向上を目的とした活動を行っている組織と考えられています。また、これらの活動のために外部組織との連携窓口機能を持つことも特徴です。現在日本シーサート協議会に集まったチームは、セキュリティ専門企業から、IT系の事業者、IJJのようなISPまで多岐にわたっています。

この協議会では、会員が集って推進するWorking Groupを活動単位としています。その内容としては、実際の事案情報の共有、その対策技術の調査、情報交換方法の検討、現状のシーサートにかかわる課題の検討、外部組織との連携等、広範囲な活動を実施しています。例えば、実際の事案情報の共有については、その情報を会員内で交換するだけでなく、得られた情報をまとめて一般に対する注意喚起として公開しています*4。



執筆者:

齋藤 衛 (さいとう まもる)

IJJ サービス本部 セキュリティ情報統括室 室長

■国際連携ワークショップ

日本シーサート協議会では、外部連携の取り組みとして国内外の他の関連団体と連携を行っています。例えばシーサートの国際団体であるFIRST*5と共同で日本における会合*6を開催したり、昨年は独自に国際連携ワークショップ*7を開催しました。このワークショップでは、Shadowserver Foundation*8とHoneynet Project*9からそれぞれマルウェア対策やボットネット対策の専門家を招き、第一線で得られた観測情報や対処の方法等についてプレゼンテーションを受け、活発な意見交換を行いました。また、会場に構築された閉環境で、実際にマルウェアを捕獲する環境構築や、ボットネット操作者となる疑似体験を行うことで、通常では得られない知見を体得しました(図-1)。

■日本シーサート協議会への加盟について

本稿では日本シーサート協議会の活動について、その一端を紹介しました。現在この協議会に参加する組織はIT系の専門組織が多いのが実情ですが、同じ目的で活動する多くの組織の参加を募ることで、一つの事案に対して多様な知見を集約して早期の解決に役立つ相乗効果を得られることが期待されています。例えば、一般の企業の情報システム部門も、ある種のシーサートであると考えられますので、ここで紹介したような活動に興味がある組織は参加を検討してみたいかがでしょうか*10。



図-1 国際連携ワークショップの様子
講師のShadowserver FoundationのRichard Perlotto氏(右)とHoneynet ProjectのDavid Watson氏(左)

*1 日本シーサート協議会 Nippon CSIRT Association (<http://www.nca.gr.jp/>)。

*2 日本シーサート協議会 会員一覧 (<http://www.nca.gr.jp/member/index.html>)。IJJのシーサートであるIJJ-SECTは、この団体の発足時から加盟している。

*3 例えば米国の CERT/CC による CSIRT FAQ (http://www.cert.org/csirts/csirt_faq.html) や、EUのENISAによる What is CSIRT (<http://www.enisa.europa.eu/act/cert/support/guide2/introduction/what-is-csirt>) などを参照のこと。IJJのようなISPにおけるCSIRT活動については RFC3013 (BCP46) (<http://www.ietf.org/rfc/rfc3013.txt>) においても言及されている。

*4 たとえば、Gumblar対策 (<http://www.nca.gr.jp/2010/netanzen/index.html>)、PushDo (<http://www.nca.gr.jp/2010/pushdo-ssl-ddos/index.html>)、Stuxnet (<http://www.nca.gr.jp/2010/stuxnet/index.html>) 等。

*5 FIRSTについては本レポートVol.3「インターネットトピック: 21st Annual FIRST Conferenceについて」(http://www.ijj.ad.jp/development/iir/pdf/iir_vol03_topic.pdf) を参照のこと。

*6 Joint Workshop on Security 2008, Tokyo (<http://www.nca.gr.jp/jws2008/index.html>)。

*7 詳細はNCA2010イベント 国際連携ワークショップ参加レポート (<http://www.nca.gr.jp/2010/event/index.html>) を参照のこと。

*8 The Shadowserver Foundation (<http://www.shadowserver.org/wiki/>)。

*9 The Honeynet Project (<https://www.honeynet.org/>)。

*10 加盟資格や手続きに関する詳細は、日本シーサート協議会加盟について (<http://www.nca.gr.jp/admission/index.html>) を参照のこと。加盟には既存会員組織による推薦が必要。この推薦はIJJでも行っている。