小規模CSIRTにおける効率的な情報収集について

On efficient information gathering in small-scale CSIRT

宮坂剛・マネジメント分科会・情報セキュリティ大学院大学

Abstract :

CSIRT (Computer Security Incident Response Team), which was invented as a means for responding to cyber attacks, has attracted attention in the current situation where all companies can become the target of cyber attacks, but in many Japanese companies, it can be inferred that the establish of CSIRT is not advanced yet. As one of the reasons why CSIRT is not being developed, the author infers that many companies feel that it is not clear how to establish and manage CSIRT. The purpose of this study is to aid in establishment and management of CSIRT and examined how to realize "information gathering" which is the most important activity among CSIRT activities. The form of CSIRT differs depending on the company because it is a personality that is flexibly customized according to the business form and scale of the company.

There are three patterns of information gathering of CSIRT: information gathering using public information, information gathering using a community for information sharing, information gathering from another company's CSIRT, and for each pattern, in order for CSIRT to gather information efficiently, this study examined what specific measures should be taken. In addition, in order to evaluate whether information gathering can be actually handled with a small scale CSIRT, Perform man-hour estimation assuming three persons system was carried out and it was confirmed that it is possible. Finally, this study organized items to consider when newly formulating internal regulations on providing information to other company CSIRT, which is necessary for gathering information from other company's CSIRT.

"Guidelines for efficient information gathering in small-scale CSIRT" as the study results of the above study were prepared.

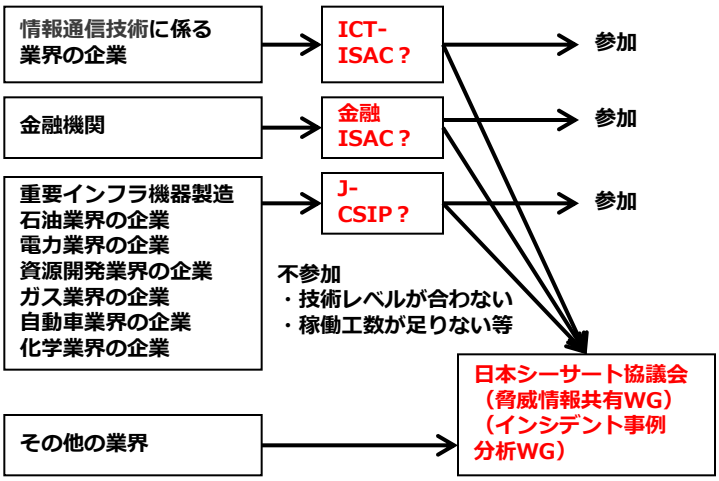
#1：公開情報を利用

JVN iPedia（脆弱性対策情報データベース）を利用

- JPCERT/CCとIPAが共同運営
- 毎月大量（2015年は248件～759件）の脆弱性情報！
- 自社システムに影響する脆弱性情報のみ自動抽出
  → 情報収集の効率化を図る必要有り

- SEfeed（アイティメディア株式会社）
  … 登録したソフトの脆弱性対策情報をメール配信！
- Vuls（フューチャーアーキテクト株式会社）
  … 脆弱性対策情報の検出を自動化するツール
  オープンソースとしてGitHubに公開、無償提供
  自社のソフト、サーバ情報を登録して自動検出！
- MyJVN API（公開API ）が提供されている
  → 自社用にカスタマイズしたＤＢ検索ツールを開発！

#2：情報共有のためのコミュニティーを利用



#3：他社のCSIRTから情報収集

他社のCSIRTが保有しているサイバー攻撃関連情報

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

・CSIRT活動を優位に運ぶための戦略として、他社は②③を切り分ける

→ ・自社にとって有力な他社CSIRTと仲間になることで③を入手！

小規模CSIRT（３名体制）で対応可能か？

作業項目	構築時	運用時	工数見積
CSIRTの運用体制の検討	●	□	
インシデント発生時の運用ルールの検討	●	■	48h/月
平常時の運用ルールの検討	●	□	
運用体制及び運用ルールの社内規程への反映	●	□	
情報収集	○	●	177h/月
ログ監視　※	○	–	
脆弱性対応　※	○	●	44h/月
教育、意識啓発　※	○	●	132h/月
管理工数	●	●	80h/月

凡例　●：作業有り　○：準備が必要
□：定期的に見直し要
■：随時見直し要
※：実務を既存部門に委託

計481h/月 ≒ ３人月
既存部門委託により可能！