D1-3 失敗から学ぶ、SOC/CSIRTのあり方

イントロダクション ～セキュリティ対応の今～

2016年11月29日

日本セキュリティオペレーション事業者協議会
セキュリティオペレーション連携WG(WG6)

講演者

- 武井　滋紀　です。
- JNSAのISOG-Jの方から来ました
- NTTソフトウェア株式会社
  - クラウド＆セキュリティ事業部　第一事業ユニット　勤務

ISOG-J 日本セキュリティオペレーション事業者協議会

ISOG-Jは11月1日現在、33社が加入しています。

各社が実際の現場で認識している課題や問題について活発に議論をしています。

今日はそこで得られた現在の課題や解決のコツを発表します。

- ホームページ：　http://isog-j.org
- facebook：/isogj
- twitter：@isog_j

去年もいましたよね？

- はい。去年は「150分でわかる！セキュリティ対応ができる組織になる10のコツ」と題しまして、SOC,CSIRTを含めたセキュリティのオペレーションを行う組織のポイントをお話ししました。

- 昨年のご意見から
  - 全体像としての方針が見えてよかった
  - もっと具体的にどうしたらいいか教えて欲しい

今年は事前アンケートを取りました！
みなさんご協力ありがとうございました！

（参考）去年はこうでした。

1. 防御から対応までのすべてをSOCに統合せよ
2. 規模と透明性/俊敏性のバランスを取れ
3. SOCに適切な権限を与えよ
4. できる事をやろう
5. メンバーは量より質を重視せよ
6. 買った技術は最大限利用せよ
7. データを集めて整理せよ
8. SOCの任務遂行を保護する
9. 脅威情報の賢い消費者であり供給者であれ
10. 冷静に・計算高く、プロらしく対応せよ

資料URL（約100ページ、4.74MB）
https://www.nic.ad.jp/ja/materials/iw/2015/proceedings/s13/

あれから1年……

- 「サイバー経営ガイドライン」出ました(2015.12)
  - http://www.meti.go.jp/press/2015/12/20151228002/20151228002.html
- 「産業横断サイバー人材育成検討会」の報告書が出ました(2016.8)
  - http://cyber-risk.or.jp/sansanren/index.html
- 「サイバーセキュリティ2016」出ました(2016.9)
  - http://www.nisc.go.jp/active/kihon/pdf/cs2016.pdf

- ランサムウェアが流行しました
- 某旅行会社の個人情報漏えいがありました

みなさん、対応できてますか？

セキュリティの対応をする組織の複雑さ

「ちゃんと」やろうとすると、範囲が広く業務が多い

「CSIRTでインシデント対応時の窓口」と思っていたら……

「監視」「インシデント時の分析」「広報」「社員教育」などなど！聞いてない！

セキュリティ事業者の視点から

- 丸投げされても、できないこともある
- マネージド・セキュリティ・サービス（MSS）のSOCで監視して報告しても、どうなったの？
- 見つけたインシデントに対応できてますか？

どうしてこうなった？？

ちゃんと

体制を構築して  体制？？

運用監視して  運用？？監視？？

インシデント対応して  対応？？

いれば問題ないですよね？

今日はなぜかうまくいかないセキュリティの対応の組織について、どこで失敗してしまうのか、どうあるべきなのかを紐解きながらあるべき組織像を考えます。

事前アンケートを取っています！

- 今年は事前の資料配布からアンケートを取っています
- パネルディスカッションでパネラーに質問できます！
- SOC,CSIRTの構築・運用・インシデント対応でのお悩みや質問があればどうぞ！
- 匿名でアンケートを取っています。このセッション以外には利用しません

- ご協力ありがとうございました！