150分でわかる セキュリティ対応できる組織にする 10のコツ

イントロダクション　～セキュリティ対応の今～

2015年11月19日

日本セキュリティオペレーション事業者協議会
あさまでSOC プロジェクト

© 2011-2015 ISOG-J

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　セキュリティ事業ユニット　勤務

NTTソフトウェア

先端技術を社会の力に！

30th ANNIVERSARY

みなさまに支えられて30周年！
～より愛される会社を目指して、先端技術を社会の力に～

© 2011-2015 ISOG-J

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、31社が加入しています。

各社が実際の現場で認識していることを活発に
情報交換をしています。

今日はそこから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

© 2011-2015 ISOG-J

最近起きている状況

- サイバー攻撃が巧妙かつ高度化し、対応するためには社内にCSIRTを組織しようとするが、人材が足りていない。
- 外部のコンサルに頼むか？社員を教育して育成をするか？

- アウトソースと言っても、何をどこまでどうやって頼んで良いのか？話が通じるのか？
  - 特に非IT系の企業では、IT系の営業トークでは難しいと感じる。

- 今日はそういった状況に効く10のコツを共有しつつ、あるべき組織や対応についてお話をしたい。

© 2011-2015 ISOG-J

今日のサマリ

- セキュリティの対応を組織的に、効率良くやるために10のコツを活用しましょう！
- SOCやCSIRTのような言葉の問題ではなく、やるべきことを明確にして、誰が何を分担するのか意識しましょう！

本セッションの言葉の定義に注意！

- 10のコツでの「SOC」はかなり広い意味での「SOC」です！
- 「セキュリティの対応」を全て行う組織をまとめてSOCと呼んでいます。
  - 広い意味でCSIRTと捉えている方もおられるかもしれません。

© 2011-2015 ISOG-J

飛び交う略語、横文字

CSIRT	Computer Security Incident Response Team
CIRT	Computer Incident Response Team
CIRC	Computer Incident Response Center
CSIRC	Computer Security Incident Response Center
SOC	Security Operations Center
CSOC	Cybersecurity Operation Center
CERT	Computer Emergency Response Team

みんなセキュリティの対応をする組織ですよねー
※CはCyberの場合もあります。

© 2011-2015 ISOG-J

困った時のIPA! みなさん参考にしてますか？

- 「高度標的型攻撃」対策　とは
- https://www.ipa.go.jp/files/000046236.pdf

攻撃の手口

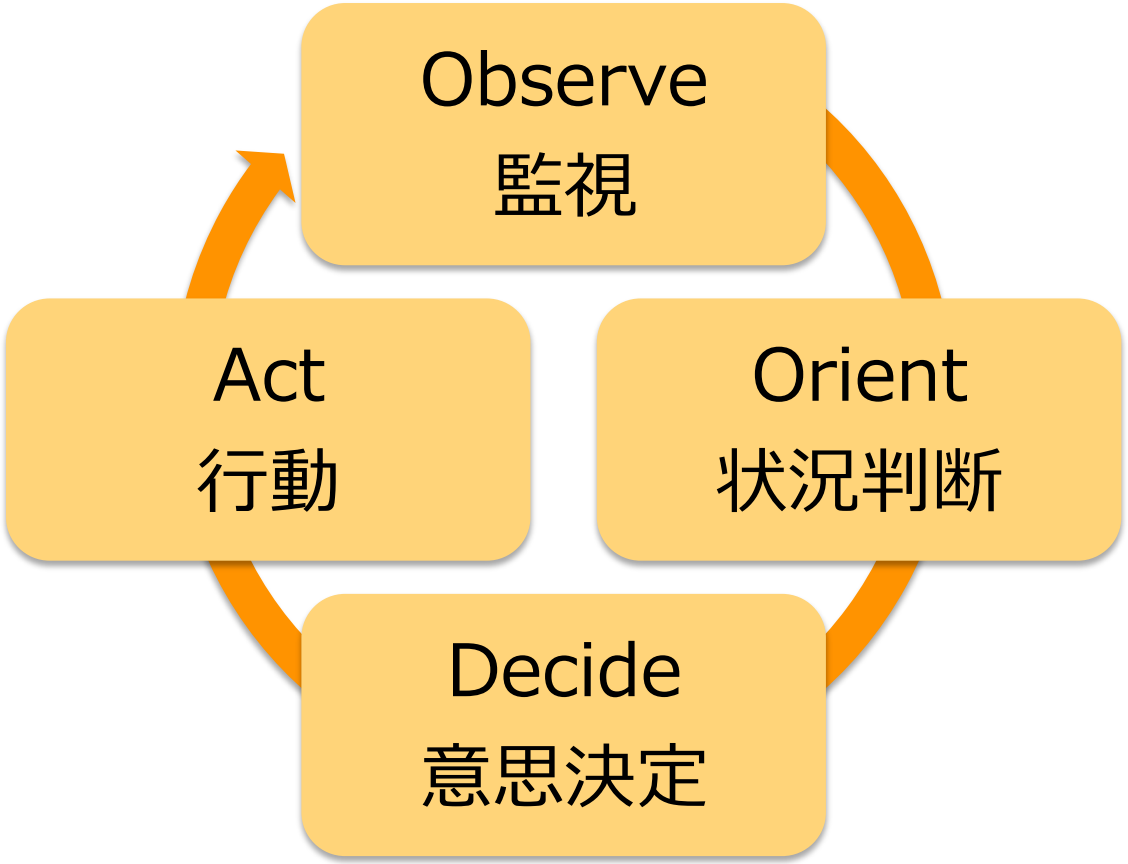
1.計画立案
2.攻撃準備
3.初期潜入
4.基盤構築
5.内部侵入・調査
6.目的遂行
7.再侵入

各段階で対策を打ち連鎖を断ち切る
サイバー・キル・チェーン
よく言われますね

© 2011-2015 ISOG-J

サイバー攻撃の対応ってなに？

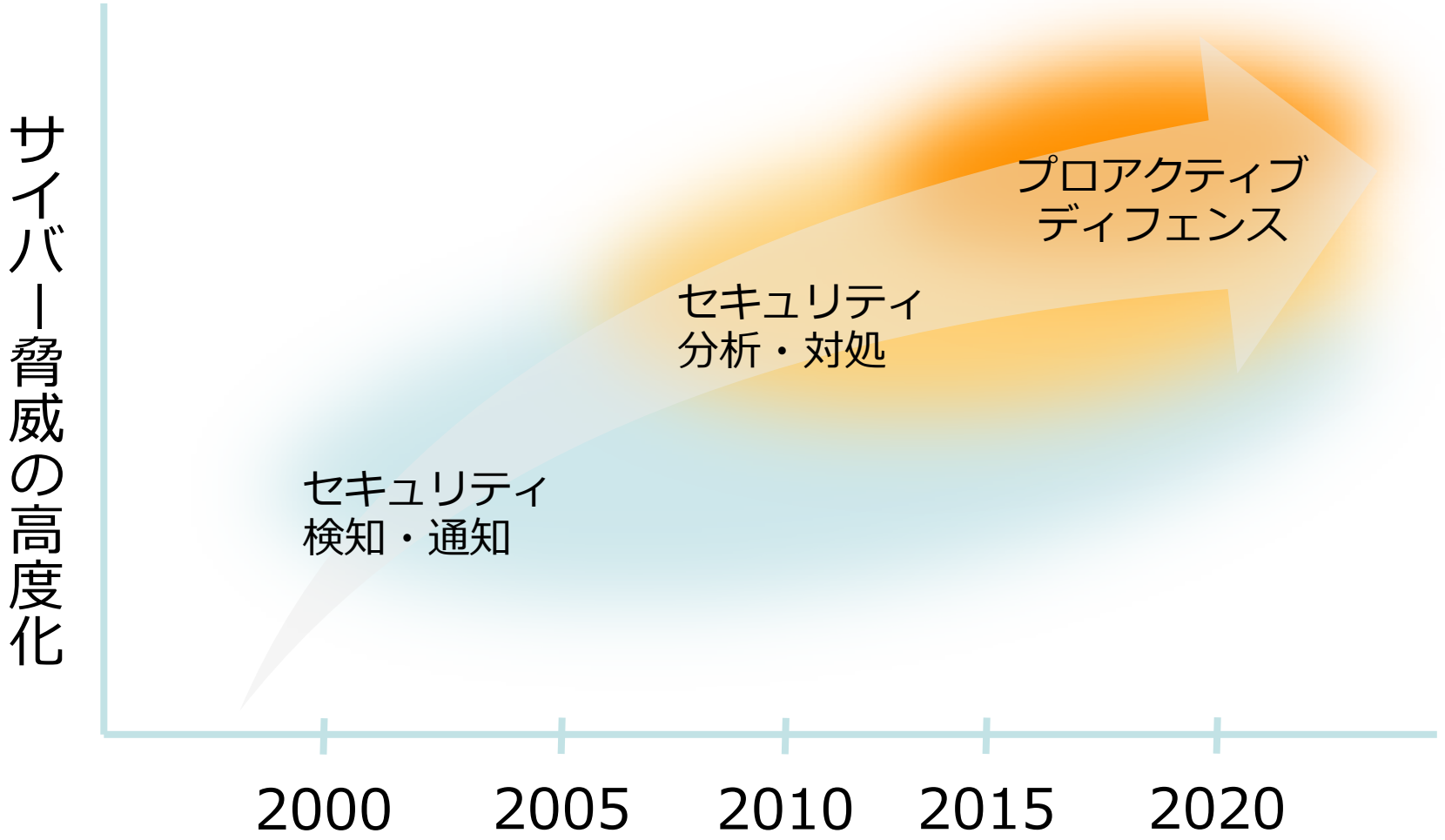
- よくある例：OODA Loop



© 2011-2015 ISOG-J

SOCのサービスの変化

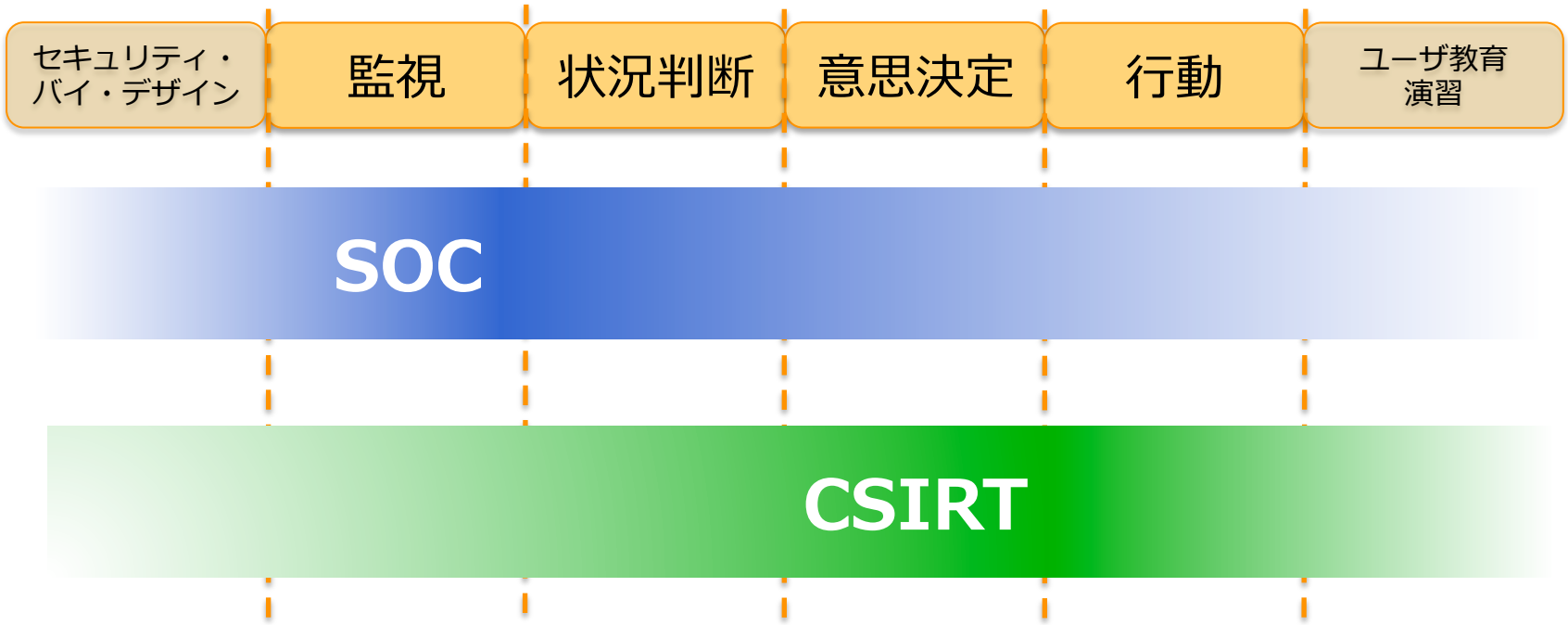
- サービス領域が拡大しています



© 2011-2015 ISOG-J

セキュリティの対応の変化

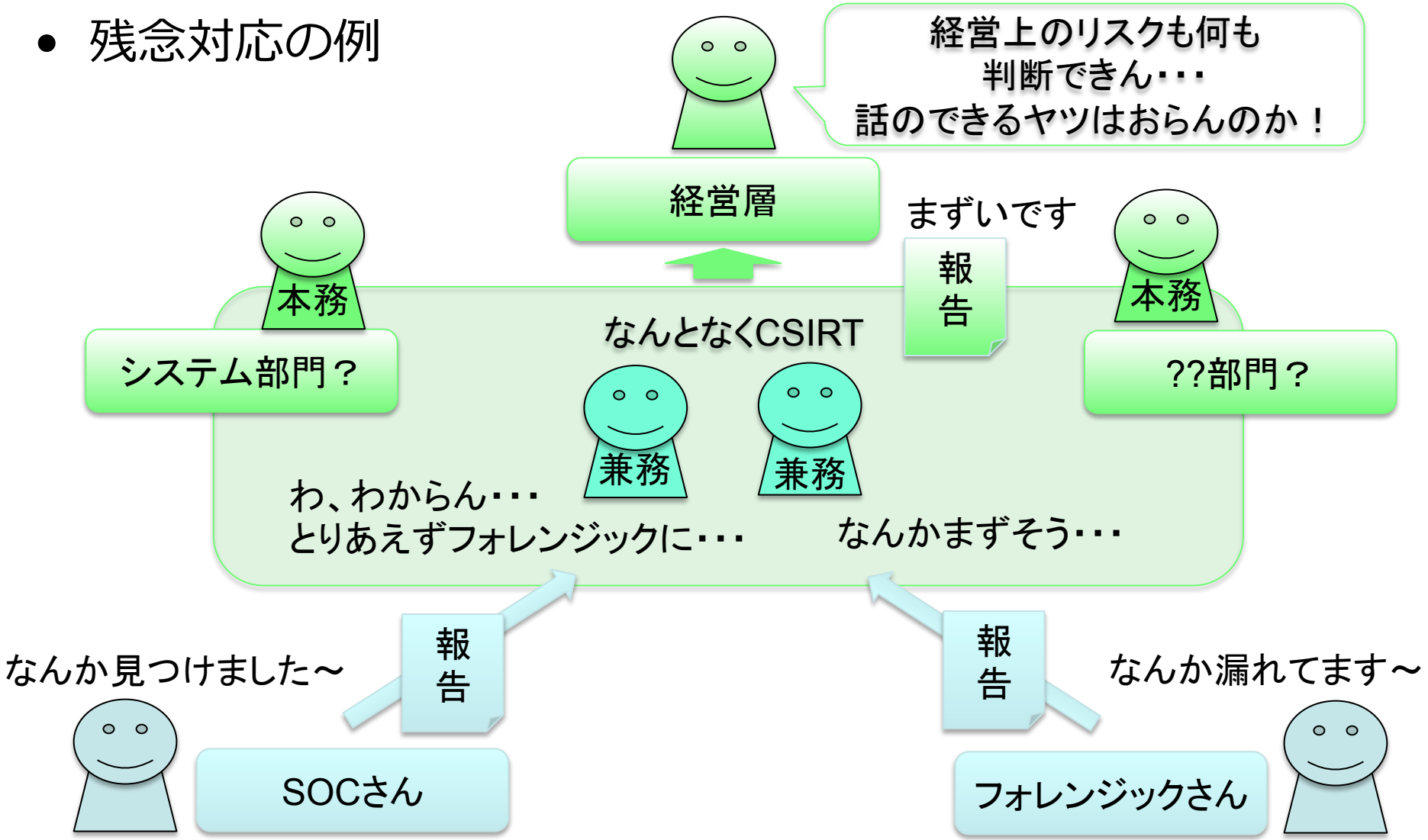
- 役割で例えると、カバーしている範囲が広がり、お互いに同じ領域をカバーし始めている



© 2011-2015 ISOG-J

あなたはある日会社からCSIRTに任命されました！

- 残念対応の例



© 2011-2015 ISOG-J

日々深刻化する状況

巧妙化する手口・止まらないインシデント

↓

CSIRT立ち上げの流行と不足する人材

↓

見えてきた新たな課題

© 2011-2015 ISOG-J

ISOG-J あさまでSOC プロジェクト での議論

- セキュリティの対応ができる組織について議論をしてきました

参考にした元ネタ
MITRE
Ten Strategies of a World-Class
Cybersecurity Operations Center

© 2011-2015 ISOG-J

今日のお題

- SOCやCSIRTといった名前でなんとなく範囲を決めて本来あるべき対応ができなくなっていませんか？

- 今日は見つけた10のコツを共有しながら、日本の組織としてどこまで有効なのか、それぞれの役割や最適解は何か、皆さんと議論をします。

© 2011-2015 ISOG-J