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

～セキュリティ対応できる組織にする10のコツ～

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

自己紹介

本田 秀行

- 日本セキュリティオペレーション事業者協議会(ISOG-J)　運営委員
- 富士通ソーシアルサイエンスラボラトリ　セキュリティソリューション本部所属
- CISA、CISM、CRISC、医療情報技師
- ITpro「SEのためのシステム監査入門」執筆

  http://itpro.nikkeibp.co.jp/article/COLUMN/20090716/333963/

自己紹介

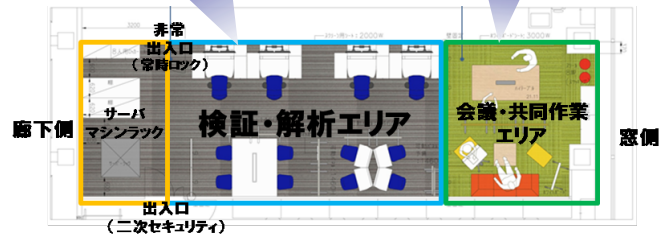
早川 敦史

- 日本セキュリティオペレーション事業者協議会(ISOG-J)　運営委員
- ＮＥＣソリューションイノベータ（株）　サイバーセキュリティグループ所属

２０１５年３月

セキュリティイノベーションセンター設立

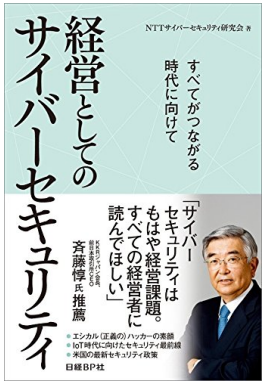
①	セキュリティ人材育成
②	サイバーセキュリティ事業連携
③	新規事業創出
④	関連組織／外部団体との連携

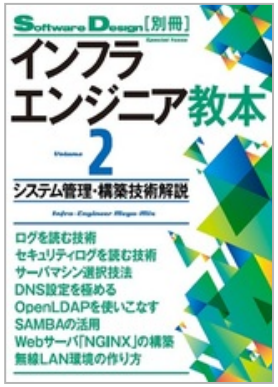


自己紹介

阿部 慎司

- 日本セキュリティオペレーション事業者協議会(ISOG-J)　運営委員
- NTTコムセキュリティ　SOC所属　高度分析チーム（L3）リーダー　/　シニアアナリスト





- NTT出版「.com Master★★ 公式テキスト」の執筆
- 技術評論社「Software Design」2015年7月号 の寄稿
- 技術評論社「インフラエンジニア教本2」の寄稿
- 日経BP社「経営としてのサイバーセキュリティ」に掲載

- Internet Week プログラム委員
- 「Internet Week 2014」での講演
  - CSIRT時代のSOCとのつき合い方: https://www.nic.ad.jp/iw2014/program/s13/
- 「Internet Week 2015」での講演
  - 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: https://internetweek.jp/program/s13/
  - CSIRT時代のSOCとのつき合い方 2015: https://internetweek.jp/program/s14/

自己紹介

井上 博文

- 日本セキュリティオペレーション事業者協議会(ISOG-J)　運営委員/WG4リーダー
- 日本アイ・ビー・エム株式会社 Tokyo SOC チーフ・セキュリティー・エンジニア

自己紹介

武井 滋紀

- 日本セキュリティオペレーション事業者協議会(ISOG-J)　運営委員
- 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

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～

断り書き(disclaimer)

・本ドキュメントはInternetWeek2015において情報提供を目的として、著作者が自らの経験および独自に調査した結果に基づき執筆したものであり、所属する組織・団体の意見を代表するものではありません。なお使用するデータおよび表現等の欠落・誤謬などについては著者はその責任をおいません。

・MITRE社発行「Ten Strategies of a World-Class Cybersecurity Operations Center 」のドキュメントに対し独自の評価を加えている部分があります。正確性の重要さは理解していますが時間的およびプレゼンテーションというコミュニケーションスタイルを考慮し、真実性の追求よりもわかりやすさを優先しています。このため表現・分類など参照元と異なる場合があることをご承知おきください。

本セッションの議論の元となったドキュメント

MITRE社
Ten Strategies of a World-Class
Cybersecurity Operations Center

https://www.mitre.org/publications/all/
ten-strategies-of-a-world-class-cybersecurity-operations-center

無償でPDFが公開されています
総ページ数が330ページ程度です

セキュリティ対応できる組織にする10のコツ

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

10のコツを解釈してまとめ、以下の順で発表をする。

- 2. 規模と透明性/俊敏性のバランスを取れ（発表者：本田）
- 3. SOCに適切な権限を与えよ（発表者：早川）
  - 5. メンバーは量より質を重視せよ
- 1. 防御から対応までのすべてをSOCに統合せよ（発表者：阿部）
  - 8. SOCの任務遂行を保護する
- 4. できる事をやろう（発表者：井上）
  - 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
- その他（発表者：武井）
  - 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

セキュリティ対応できる組織にする10のコツ

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

規模と透明性/俊敏性のバランスを取れ

本パートの内容

本パートの内容について：

・セキュリティオペレーションセンタを運営する上で、組織において最適なSOCの構築に必要な観点についてお話しいたします。

・SOCはコストセンタです。できるだけ費用をかけず、しかしながら十分な機能と早さを備えたSOCの運営を行うという二律背反した要素を満たすためにMITRE社発行「Ten Strategies of a World-Class Cybersecurity Operations Center 」に基づき、自治体様・企業様向けのベスト・プラクティスの一部をお話しいたします。

以下の3要素が規模と透明性/俊敏性のバランスがとれたSOC構築・運用においてのベストプラクティスとされています。

要素	ベストプラクティス		
SOC構築	組織の要件と監視対象のサイズによって最適な機能と構造を選ぶこと	小さな組織	伝統的なSOC
		大きな組織	セキュリティインテリジェンスも備えたSOC
		もっと大きな組織	階層構造を持ち、機能と役割を分割したSOC
素早さの確保	物理的な近さはコミュニケーションの効率を上げる		
	意思決定者との物理的な近さは、判断と決定の速度を早め、素早いインシデントへ対応が可能になる。		
SOCの運用	DRサイトにメインサイトの双子を作る必要はない		
	フォロー・ザ・サンはインシデント対応には不向き		
	階層化SOCの役割分担		

監視対象サイズに対応したSOCの例

SOCの分類	ユーザ数	インシデントへの対応	組織の例
仮想SOC	1000	親会社に従う	・小規模企業 ・単科大学 ・市町村
スモールSOC	10,000	予防・事後対策	・中規模企業 ・総合大学
ラージSOC	500,00	予防・事後対策	・フォーチュン500 ・都道府県
階層化SOC	500,000	下層SOCの指導も含めた予防・事後対策	・グローバル企業 ・省庁
ナショナルSOC	50,000,000	予防・事後対策なし アドバイスに特化	・国

メインのSOCは本社に近いところに設置すること

SOCは経営首脳陣と密に連携がとれるか？

コツ2. 規模と透明性/俊敏性のバランスを取れ

概要

- ビジネスの要求と経営者の要求に応え、必要な機能が実現されることが大事
- 自組織の規模や目的に応じて、身の丈にあったSOCを構築することが大事
- 監視対象および経営首脳陣と良好なコミュニケーションを取ることが迅速な対応に繋がる

外部活用出来ること

- 投資対効果の高いSOC機能の選定と運用設計

point

- 投資対効果を最大化するために、自分たちのニーズに対応した機能を備えたSOC構造を検討・実現していただくこと
- SOCの機能を最大化するために、監視対象および経営首脳陣と効果的なコミュニケーションが可能となる物理的なSOCのロケーションを検討していただくこと
- 災害対策用サイトでは最低でもログだけは直ちに利用できるようになっていること、また短時間で切り替えできるようになっていること
- フォロー・ザ・サンシナリオはTier1に限定すること

SOC導入においては必要な機能を見極め、構築においては現場・経営陣とコミュニケーションが容易な場所にSOCを構築することが重要です。これにより投資効果が高く、効果的で効率的なSOCを運用することが可能になります。

セキュリティ対応できる組織にする10のコツ

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

SOCはほとんどの場合、他の誰かが保持しているシステムやサービス、資産を守るために存在します。

- 守るべき対象は何であるか？
- どこまでやるべきなのか、やってよいのか？

（1）SOCに対して正しく権限を与える
（2）防御の実施に最適な組織配置を検討する

SOCに対して正しく権限を与える

ＳＯＣのCharterを作成する

- Charterとは？？
  組織内で合意をとるための基本文書。
  SOCのサービス対象や範囲を明確にする。

- Charterに書く基本的な内容とは？？
  SOCが何をすべきか。役割を記載する。
  - どのようにSOCのミッションを実施する(HOW)ではなく、何を実施するか（What）を記載する。
  - 今できることを書くだけではなく、今後できることも含めて記載する。

責任範囲について「誰が」「どこまで」を明確にする。

Charterを作成する場合の注意点

- SOCのサービス提供対象の決定では経営層の署名（承認）を得る。
- Charterは一度作っただけで終わりではなく、最適な内容に日々更新を行うことが重要である。
- Charter以外のセキュリティポリシー文書がある場合は、まずはその内容を念頭に置いた上でCharterを作成する。

コツ3. SOCに適切な権限を与えよ

概要

- SOCで対応するサービス範囲や対象、権限を明文化する
- 自組織にあったSOCの配置および権限の継承を実施する

外部活用出来ること

- SOC構築／運用におけるベストプラクティスなど、ノウハウ活用
- 組織、業務、ITなどのアセスメントの実施（コンサルティング）

point

- SOCが守るべきサービス範囲や対象は、事業の主体となる経営層などが決定する必要があります。また権限継承を行う上でも、範囲／役割／責任を明確にし、文章として明文化することが重要です。
- ベストプラクティスなど他組織を参考にしつつ、自組織にあった役割の定義と権限の与え方を検討しましょう。

セキュリティ対応できる組織にする10のコツ

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

コツ５．メンバーは量より質を重視せよ

本パートはSOCのメンバーアサインに関するお話。

SOCを立ち上げようとする際に経営者が抱える悩み。

（１）誰を雇うべきか？
（２）どのようなアナリストが必要か？
（３）どのようにSOCを維持するのか？

誰を雇うべきか？

- マインドセット
  「熱意」、「好奇心」、「知識欲」

どうしたら辞められないか？

- 仕事はよりスマートに、常に激しいのはダメ
- キャリアパスを示してあげて
- キャリアアップをサポートしてあげて
  - 社内での勉強会してみて
  - 研修受けに行かせて
  - 外部団体や活動に参加させて
    Blackhat、Defcon、RSA Conference etc.
- SOCメンバーの働きが事業の運営に役立っていることを定期的にフィードバックしてあげて
- 適切な人員配置を維持してね
- お金払ってね！！！

コツ５．メンバーは量より質を重視せよ

概要

- SOCで活躍する人材は非常に多様なスキルを保持している必要がある
- よい人材が集まるところによいSOCあり

外部活用出来ること

- 外部SOCサービスの利用（アウトソース）
- SOC人材の基本スキルセットの教育／演習

point

- SOCの業務を実施できる人材を集めるには、その組織での価値やキャリアパスを明確にする必要があります。
- 離職率が高い分野であり、自組織内で維持できない場合はアウトソースすることを検討するべきです。

セキュリティ対応できる組織にする10のコツ

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

このパートでは

セキュリティ対応を行う上で、

- **対応組織はどのような体制であるべきか**
- **その遂行を妨げないために考えるべきこと**

をお話しします。

セキュリティ対応できる組織にする10のコツ

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

セキュリティ対応組織保持すべき不可分な5要素

1. リアルタイム監視とトリアージ
2. インシデント分析、対応、およびそれに必要な調整
3. サイバー情報収集と分析
4. センサーのチューニングと管理、SOC基盤システム運用管理
5. SOCで使用するツールのエンジニアリング（開発・運用）と展開

理想的な組織体制

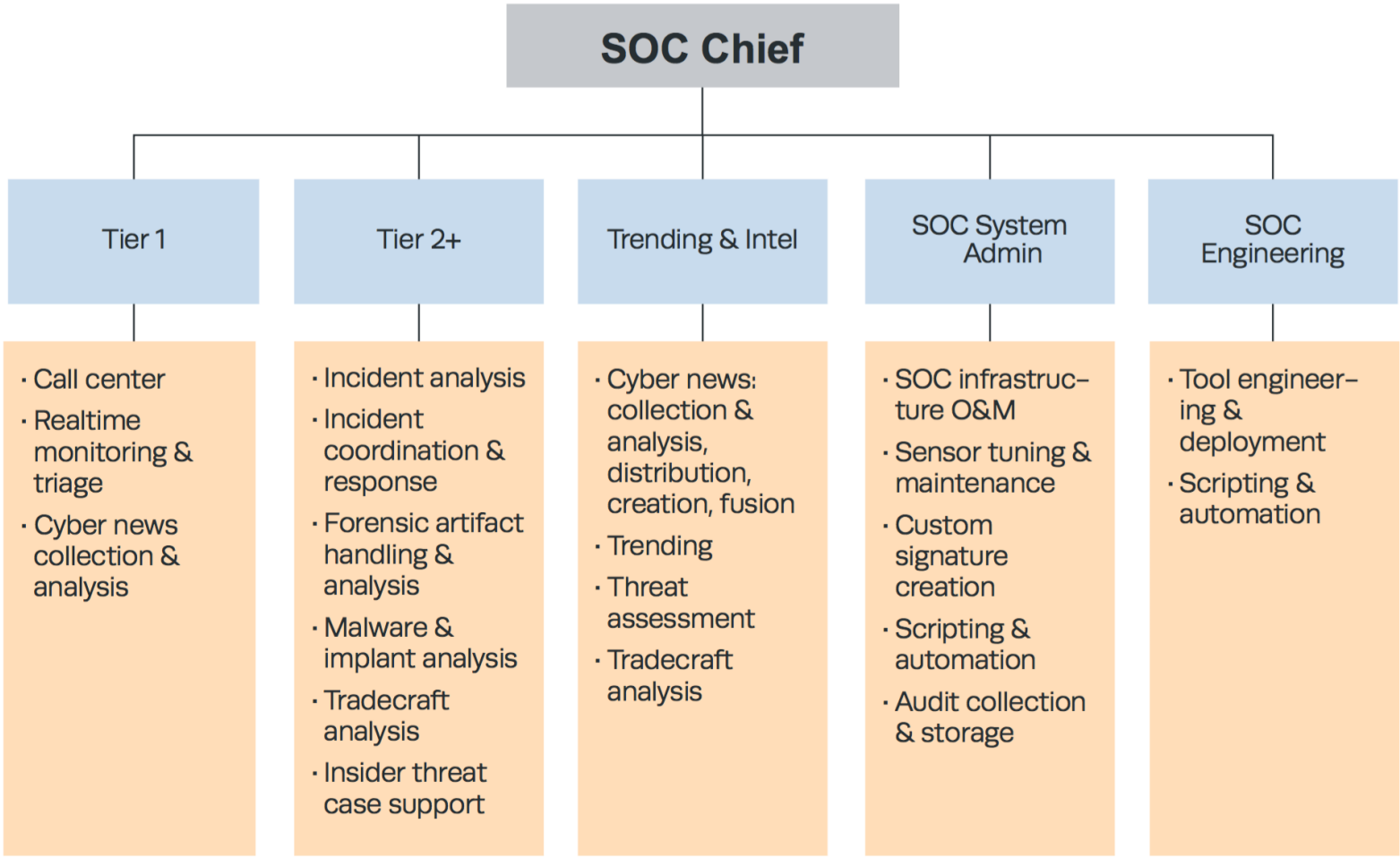


Figure 10. All Functions of CND in the SOC

コツ1. 防御から対応までのすべてをSOCに統合せよ

概要

- セキュリティ対応は１組織で統合的に実行されるべき
  - セキュリティ対応に求められる５要素は不可分

外部活用出来ること

- セキュリティ対応組織編成についてのコンサルティング

point

現実的に、統合を実現するのはとても大変です。まずは「１要素１組織」の形を目指しながら、それらの組織間の関係をいかに良好なものとするか検討していくのが良いでしょう。

セキュリティ対応できる組織にする10のコツ

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

8. SOCの任務遂行を保護する

完璧なSOCが目指すべき理想的な運営状態

- 指定のモニタリングポイントにおいて、パケットロスがほとんどない環境を実現する
- 攻撃者がIDSやIPSの様な監視・防御機能の存在を検出（回避）することを防ぐ
- 盗聴や改竄を試みようとする攻撃者から保護しながら、必要なときにエンドデバイスからSOC監視システムへのセキュリティイベント100%配送を保証する
- サービス対象の一部が侵害されていても、SOCミッションの活動を継続し、SOC資産への権限のないアクセスを防ぐ
- SOCに保持されている機密文書や記録の開示を防ぐ

現実には、米国最高のSOCにおいても隙がある状態。

理想を求めれば莫大な資金が必要。

できることを足元からしっかり実施する必要がある。

コツ8. SOCの任務遂行を保護する

概要

- セキュリティ対応に関するあらゆる情報は攻撃者から隠さなければならない
  - ネットワークセンサーの配置場所、方式をよく検討する
  - SOCの境界線が、安全に保たれるよう設計する
  - SOCの持つ情報、ノウハウは適切に統制する

外部活用出来ること

- 豊富な経験に基づくセキュリティ対応インフラの設計/構築

point

- 言うのは簡単ですが、実際には非常に高度な技術/ナレッジ/ノウハウが求められます
- 「完璧な状態」は目指してもきりがなく、際限なくコストもかかります
- 「意識高いだけ」にならないよう、まずはベースとなるセキュリティレベルを地道に高めることが大切です

セキュリティ対応できる組織にする10のコツ

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の任務遂行を保護せよ
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

セキュリティ対応できる組織にする10のコツ

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の任務遂行を保護せよ
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

規模に応じた提供機能例(一部抜粋)

Name	Virtual	Small	Large	Tiered	National
Real-Time Analysis					
Call Center	O	B	A	A	A
Real-Time Monitoring and Triage	O	B	A	A	O
Intel and Trending					
Cyber Intel Collection and Analysis	B	B	A	A	A
Cyber Intel Distribution	O	B	A	A	A
Cyber Intel Creation	-	O	B	A	A
Cyber Intel Fusion	O	B	A	A	A
Trending	O	O	A	A	A
Threat Assessment	-	O	B	B	A
Incident Analysis and Response					
Incident Analysis	B	B	A	A	O
Tradecraft Analysis	-	O	A	A	O
Incident Response Coordination	B	B	A	A	A
Countermeasure Implementation	O	O	O	O	O
On-site Incident Response	B	O	O	O	O
Remote Incident Response	B	B	A	A	O

B(Basic):
部分的もしくは基本的な能力を保持するエリア

A(Advanced):
十分な能力を保持すべきエリア

O(Optinal):
外部組織で代替可能ならば持たなくてもよいエリア

ー(Not Recommenned):
ミッションとの兼ね合いからサポートを推奨しないエリア

コツ4. できる事をやろう

概要

- 自組織の規模や目的に応じて、自SOCの「対応する範囲」を定義することが必要
- 5種類のSOCの規模を例に、それぞれで必要な機能を紹介

外部活用出来ること

- インシデントの監視・分析、マルウェア解析、フォレンジック解析、脅威情報の提供といった技術的な支援の提供

point

- 「内部組織でなければできない」統括や社内調整にかかわることに注力することが大事です
  - 例：エンドユーザーの窓口や関係部署、関係機関との調整機能、現地またはリモート環境からのインシデント対応
- 自SOCが対応する範囲は「狭い範囲だけでも質を高くする」が重要です。自組織ではカバーが難しい範囲は他部署やアウトソースを用いて補うことにより、全体の質を高めましょう

セキュリティ対応できる組織にする10のコツ

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の任務遂行を保護せよ
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

技術・ツールを最大限利用するために自組織に必要なこと

- 自組織にとって、何が最も脅威であるか、を把握する
- 持っている技術・ツールの機能、カバー範囲を整理し、重複を避ける
- 経営者と「技術・ツールの制約」を共有する
- 各ツールが、設計、監視、分析、および応答アーキテクチャに適合していることを確認する
- SOCのメンバーがツールを利用するための専門知識の有無を確認する
- 各ツールに対して、運用からのフィードバックを反映させ、専任担当者が継続的な改善を実行する

コツ6. 買った技術は最大限利用せよ

概要

- 購入した技術を最大限利用するためには、1)自組織にとって何が脅威なのかを常に把握、2)どの程度脅威をカバーしているのか、重複がないかを確認する、といったことが重要
- ツールは人を置き換えるものではない。人の成長も、ツールの効果を最大化するためには重要

外部活用出来ること

- セキュリティー技術の効率的な利用方法を製品、サービスなどで支援

point

購入した技術/ツールを最大限活用するには

- 前提となる脅威が変化することがあるため、脅威の継続的な把握や利用している技術・ツールの見直しが必要です
- 技術・ツールやツールを導入するだけではなく、それらを扱う人の維持・成長も重要な要素です
- また、導入した技術・対策のスコープを経営陣と共有することが必要です

セキュリティ対応できる組織にする10のコツ

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の任務遂行を保護せよ
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

コツ7. データを集めて整理せよ

- データを集めるとは？
  - すべて記録する？
  - アラートのみ見ていればよい？

インシデントの発見には、自組織に対する脅威(目的)に応じたデータの収集方法と 整理方法(手段)が必要

例えば、

目的:　　社外への許可していない通信の発見

データ収集方法：　Firewallログ、Proxyログ、IPS

整理方法:　1) FirewallとProxyのDenyログを調査

2) IPSのイベントログとFirewallやProxyのAcceptログの関係性の調査

コツ7. データを集めて整理せよ

概要

- データは目的(SOCの対応スコープ)にあわせて収集することが必要である
- データソースによって1)単体データで発見のトリガとなるもの、2)いくつかのデータを組み合わせることで発見のトリガとなるもの、3)事実を積み重ねてインシデントの確信を得るために必要なデータ、の3種類があり、これらの組み合わせが重要
- 機器毎にも、注目すべきデータがあり、それらを適切に取得する必要がある(例：Firewallのallowログ)

外部活用出来ること

- 収集すべきデータのアドバイスや、監視サービス等による具体的なデータ分析手法の技術支援

point

- やみくもにデータを取得しても、インシデントの発見はできません。自組織に対する脅威と分析方法に基づいた適切なデータソースの選択が重要です。
  - 脅威を明確に定義し、それらを保護するために必要なデータを持つシステムを洗い出しましょう
  - 保護対象のアップデートの把握と、変更に伴う監視システムのアップデートに必要な調整をしましょう
- データソースの種類、保持期間が適切であるかを、保護対象や脅威の変化にあわせて見直すことができる体制も必要です。

セキュリティ対応できる組織にする10のコツ

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の任務遂行を保護せよ
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

セキュリティ対応できる組織にする10のコツ

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の任務遂行を保護せよ
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

コツ9. 脅威情報の賢い消費者であり供給者であれ
（参考）日々収集し、参考にする情報

- 日本的には、IPAとJPCERTは基本
  - IPA：http://www.ipa.go.jp/
  - JPCERT：https://www.jpcert.or.jp/

- 参考として幾つかのサイトの情報を掲載しておく。
  - 英語中心のため、読みこなすには慣れも必要。
  - まずはIPAやJPCERTで情報を収集し、そこから情報源として英語の情報を辿るという考え方も。
  - RSSでチェックできるものはRSSでチェックし、twitterでも情報を収集する、という手もある。

- 注意！！解析系サイトに検体や情報をアップロードすることは、こちらの情報を外部に出していることにもなります。

コツ9. 脅威情報の賢い消費者であり供給者であれ
（参考）日々収集し、参考にする情報(1/3)

- **インターネットの状況**
  - ISC：http://www.isc.org
  - NetCraft：http://news.netcraft.com/
  - US-CERT：http://www.US-Cert.gov
- **一般的な技術とセキュリティの動向**
  - Schneier on Security Blog：http://www.schneier.com/
  - Krebs on Security：http://krebsonsecurity.com/
  - Security Dark Reading：http://www.darkreading.com/
  - Slashdot：http://slashdot.org
  - Engadget：http://www.engadget.net
  - Securosis：https://securosis.com/blog
- **脅威情報系**
  - Microsoft Security Intelligence Report：http://www.microsoft.com/security/sir/default.aspx
  - Team Cymru(要登録)： www.team-cymru.org
  - FBI Cybercrime information：http://www.fbi.gov/about-us/investigate/cyber/cyber

コツ9. 脅威情報の賢い消費者であり供給者であれ
（参考）日々収集し、参考にする情報(2/3)

- **マルウェアと脅威情報**
  - Threat Expert：http://threatexpert.com
  - Microsoft Malware Protection Center：http://www.microsoft.com/security/portal/default.aspx
  - SANS Internet Storm Center： http://Isc.sans.edu
  - Symantec Threat Explorer：http://www.symantec.com/business/theme. jsp?themeid=threatreport
  - McAfee Threat Center： http://www.mcafee.com/us/threat_center/
  - Metasploit Blog：https://community.rapid7.com/community/metasploit?view=blog
  - Security Focus：http://www.securityfocus.com/
  - Dshield：http://www.dshield.org/
  - Offensive Security’s Exploit Detabase：http://www.exploit-db.com/
  - Worldwide Observatory of Malicious Behaviors and Attack Threats (WOMBAT)：http://wombat-project.eu/
  - Symantec’s Worldwide Intelligence Network Environment(WINE)：http://www.symantec.com/about/profile/universityresearch/sharing.jsp
  - Mandiant M-Trends：https://www.mandiant.com/resources/mandiant-reports/
- **悪性のドメインやIPアドレスや関連する情報**
  - Malware Domain Blocklist：http://www.malwaredomains.com/
  - Unspam Technologies Project Honeypot：http://www.projecthoneypot.org/index.php
  - EXPOSURE (Exposing Malicious Domains)：http://exposure.iseclab.org/
  - Shadowserver Foundation：http://www.shadowserver.org/wiki/

コツ9. 脅威情報の賢い消費者であり供給者であれ
（参考）日々収集し、参考にする情報(3/3)

- **自動脅威分析**
  - Anubis(Analyzing Unknown Binaries) : http://anubis.iseclab.org/
  - Virustotal : http://www.virustotal.com/
  - Metascan online : http://www.metascan-online.com/
- **脅威と識別情報**
  - IBM ISS X-Force : http://xforce.iss.net
  - BotHunter Internet Distribution Page : http://www.bothunter.net/
  - Latest Snort publicly available Snort rules(要登録の箇所あり) : http://www.snort.org/snort-rules/
  - Emerging Threats signature list : http://www.emergingthreats.net/
  - Latest Tenable Nessus plugins(要登録) : http://www.nessus.org/ plugins/
- **パッチや脆弱性の情報**
  - MITRE's CVE : http://cve.mitre.org
  - NIST's National Vulnerability Database : http://nvd.nist.gov/
  - US-CERT Technical Cyber Security Alerts : http://www.us-cert.gov/cas/techalerts
  - Microsoft Security TechCenter : http://technet.microsoft.com/en-us/security/default.aspx

コツ9. 脅威情報の賢い消費者であり供給者であれ

概要

- セキュリティの対応をする組織には、サイバー脅威分析室(Cyber Threat Analysis Cell：CTAC)の活用を勧めている。
- 日々攻撃の情報を分析することで、執拗な攻撃や高度な攻撃に素早く対応できるように備えている。
- 情報を集めるだけではなく、コミュニティで発信することで情報を交換し、より良い対応ができるようにしている。

外部活用できること

- 継続的な日々の監視や分析から得られる、最新の脅威の情報の提供

point

- 提供される情報の理解を助けるための日々の情報収集や動向の把握、社内への情報発信をすることが必要です
- 外部から情報を買うのであれば、当初はアウトソースすることも可能です
- 収集した情報が自社に必要な情報か、影響のある情報で経営リスクとなるかを判断することは必要です

セキュリティ対応できる組織にする10のコツ

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の任務遂行を保護せよ
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

コツ10. 冷静に・計算高く、プロらしく対応せよ

- 決めた手順に従う
- パニックにならない
- 結論を急がない
- 属性情報には注意する（その情報の根拠に注意）
- 侵入に対して、もれなく分析評価する
- 「で、どうなんだ？」に答えるようにする
- 適切なタイミングでの証拠保全や報告作成のルールに従う
- 適度に適度な最新状況の報告をする（報告を待つ方も）
- 慎重に対策や応対の影響を評価する
- SOC全体が同じ目標に向かっていることを確認する
- 助けを求めることを恐れない

- 残り半分はインシデントレスポンスの効率化のためのフォーマットの利用やイベントのシステムでの管理についてのため、割愛。

- サンプルのインシデントレスポンスの記録の形式
  - CIO Magazine
    - http://www.cio.com/research/security/incident_response.pdf
  - NITC
    - http://www.nitc.state.ne.us/standards/
  - SANS
    - http://www.sans.org/incidentforms/
  - U.S. Secret Service
    - http://www.treas.gov/usss/forms/form_ssf4017.pdf
  - CERT/CC
    - http://www.cert.org/reporting/incident_form.txt

- **RTIR: RT for Incident Response**
  - https://bestpractical.com/release-notes/rtir/3.2.0

コツ10. 冷静に・計算高く、プロらしく対応せよ

概要

- 事案や事件が起きた場合、対応は冷静である必要がある。
- 情報を収集、精査してどのような対応をするか判断し、対応を進める必要がある。

外部活用出来ること

- 普段の監視で得た情報の分析による、現状の把握や分析。有事の際のフォレンジックの実施。

point

- 日々インシデントを想定し、対応の訓練をしておきましょう
- 自社の事案や事件の対応については、会社としての判断のために自社の要員で統括をする必要があります
- 対応に必要な業務やプロセスを分析し、外部に頼る部分は外部に頼りましょう

まとめ

- 「セキュリティ対応できる組織にする10のコツ」ということで、それぞれのコツを紹介しました。
- 実際に組織への適用については、既にできていることや、これからすぐにできそうなこと、これから時間をかけて取り組むべきことなど見つけていただければ幸いです。

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