D1-3 失敗から学ぶ、SOC/CSIRTのあり方

失敗から学ぶ、セキュリティ対応組織が担うべき役割～

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)

アジェンダ

- 自己紹介
- SOC/CSIRT構築の流れ（例）
- 失敗あるある傾向
- あるセキュリティチームの発足一年史
- 失敗あるある例　構築パート
- 失敗あるある例　運用パート
- 失敗あるある例　インシデントパート
- まとめ

講演者 自己紹介

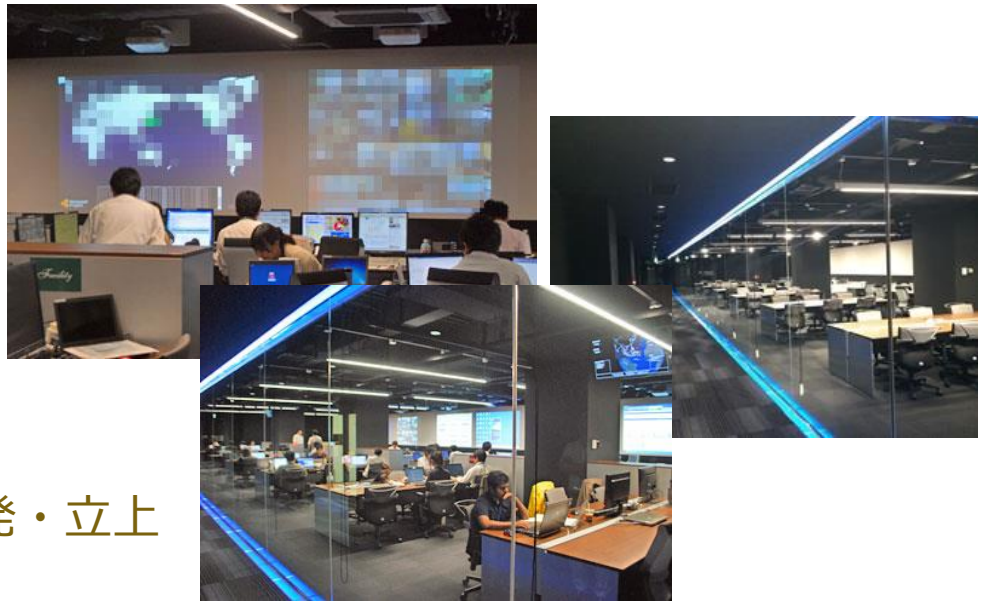
河島 君知

- 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データ先端技術（株）　セキュリティ事業部　所属

2003年　NTTデータ 先端技術
(旧：NTTデータセキュリティ)

セキュリティ監視業務
セキュリティインシデント対応
セキュリティ製品開発
セキュリティサービス企画・開発・立上

現在　SOC構築支援



Itmediaエグゼクティブ様取材記事より

講演者 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

２００２年～

統合ID管理、認証等基盤システム構築運用

実施

２０１４年～

インシデント対応体制構築等コンサルティング

セキュリティインシデント対応教育／演習

の実施

自社センター用
ジャケット着用


NEC \Orchestrating a brighter world wisdom

NEC自身もこのガイドラインの内容を受けて、あらためて「サイバーセキュリティ経営の重要10項目」に基づいて対策を見直し、社内のセキュリティ強化に取り組んでいる。CISO（最高情報セキュリティ責任者）の役割を明確化したのも、ガイドラインがこの役職の重要性に言及していることに対応したものだ。

ガイドラインでは、セキュリティ対策の「重要10項目」を定めているが、セキュリティサービスの前線で働く早川がとくに着目しているのは、「リスクの把握と計画」「サプライチェーン」「緊急対応チーム」といったキーワードだという。

NEC サイバーセキュリティ戦略本部 早川敦史

「自社のセキュリティリスクがどこにあるかをしっかりと把握すること、ビジネスのサプライチェーン全体を見たセキュリティ対策が求められること、サイバー攻撃などのセキュリティインシデントが発生した時、迅速に対応できるチームが必要であること――。それらが、とりわけ今後多くの企業が取り組まなければならない点であると考え

ロクロ回し記事

アジェンダ

- 自己紹介
- SOC/CSIRT構築の流れ（例）
- 失敗あるある傾向
- あるセキュリティチームの発足一年史
- 失敗あるある例　構築パート
- 失敗あるある例　運用パート
- 失敗あるある例　インシデントパート
- まとめ

SOC/CSIRT構築の流れ（例）

▼----SOC/CSIRT　構築フェーズ

① 経営層から理解を得る

② 組織内の現状把握
- 既存組織と役割
- 保有システム
- 実施セキュリティ対策

③ SOC/CSIRT構築活動のためのチーム結成と社内協力体制の構築

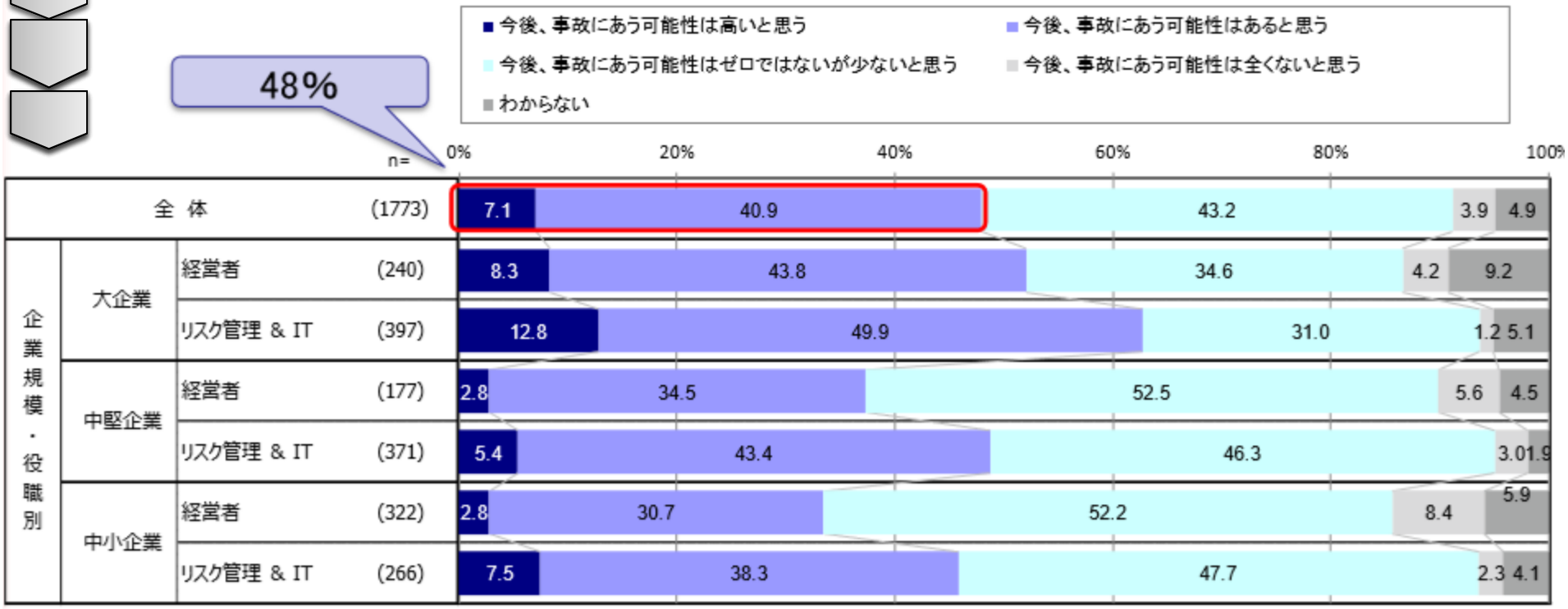
④ 設計と計画

⑤ 環境構築　必要な人・物・金
- 人　→　必要人財獲得、育成
- 物　→　場所(隔離環境)、監視システム、インシデント管理システム
- 金　→　みなさんご存じ

⑥ ルール作り
- 社内各組織体制
- セキュリティ組織
- 規則類・運用手順・チェックシートの整備

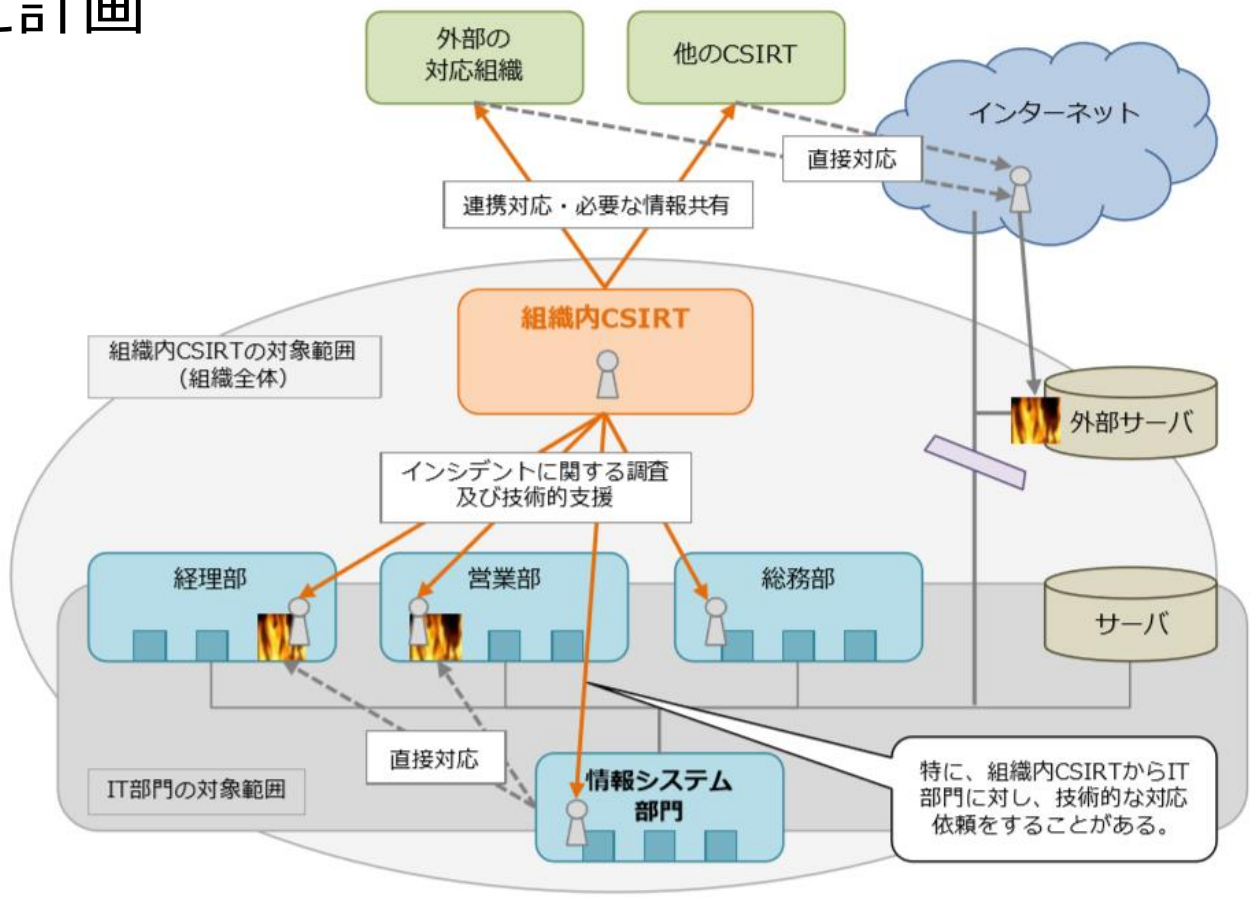
⑦ SOC/CSIRT の告知と活動開始
- 対象業務
- 連絡方法

① 経営層から理解を得る



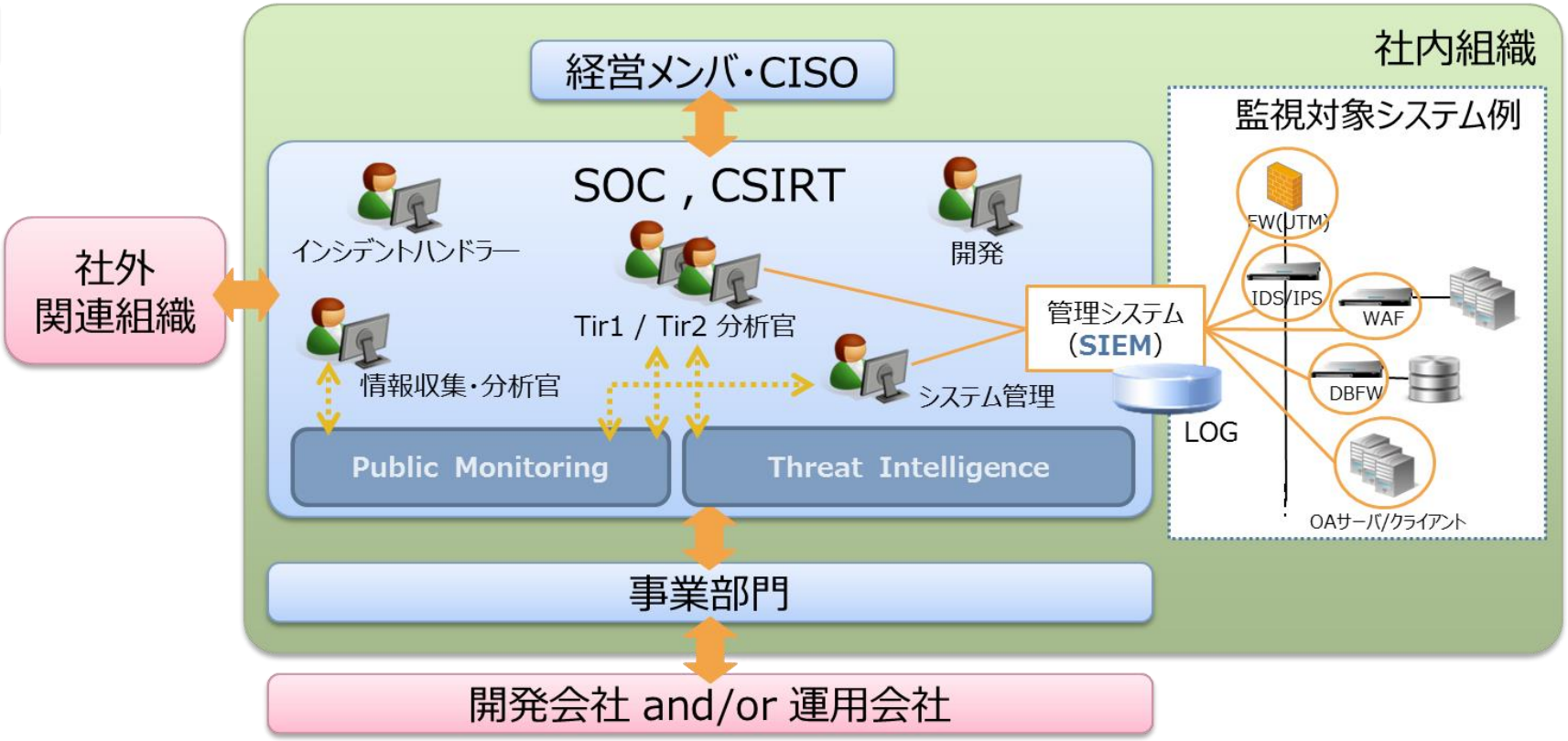
出典
IPA「企業におけるサイバーリスク管理の実態調査2015」
p48 自社で情報セキュリティ事故が発生すると認識している割合

② 組織内の現状把握
③ チーム結成と社内協力体制
④ 設計と計画



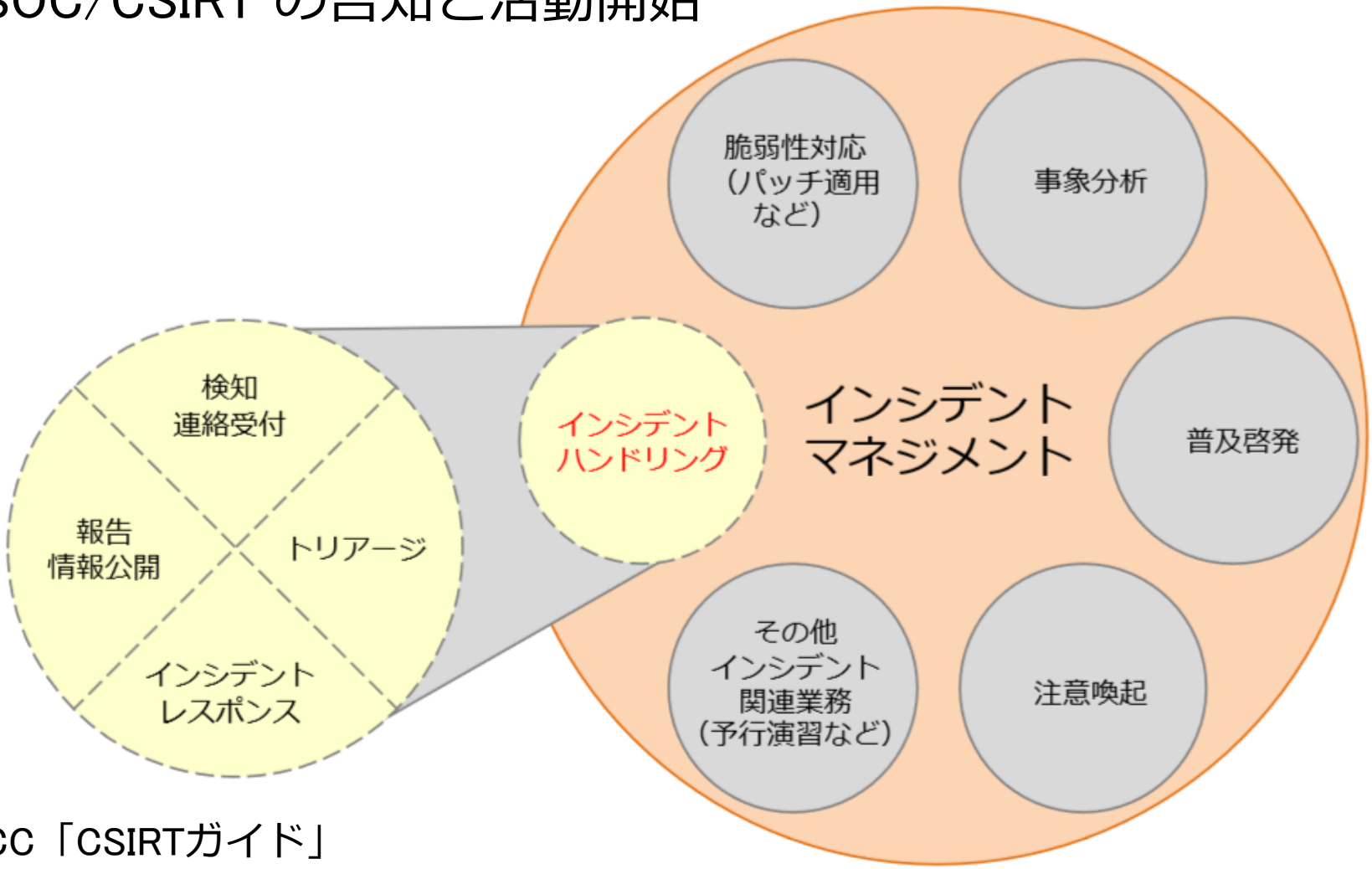
出典
JPCERT/CC「経営リスクと情報セキュリティ」
p38 CSIRTとIT部門の活動範囲の関係の例

⑤ 環境構築



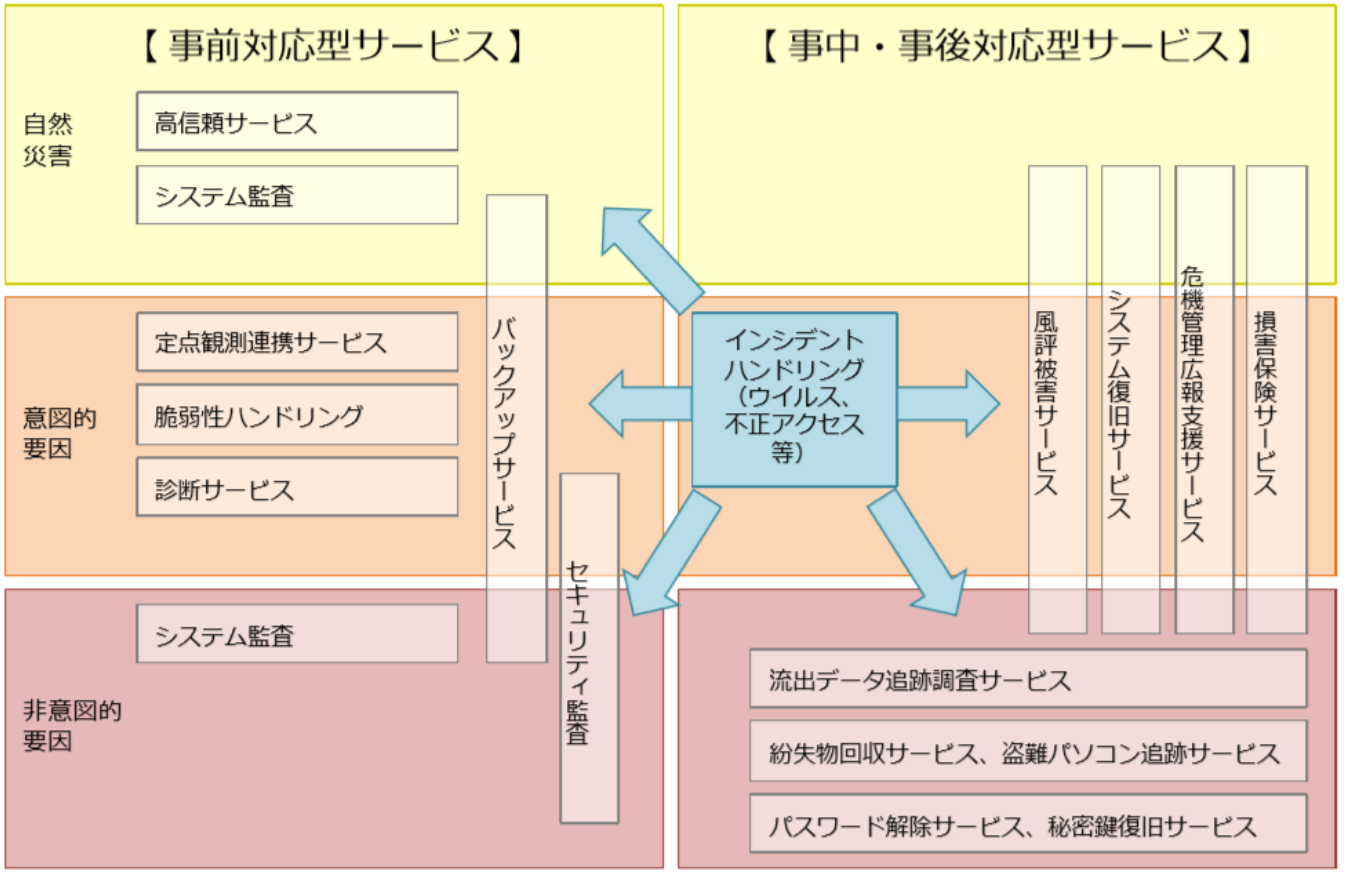
出典：ISOG-J作成

⑥ ルール作り
⑦ SOC/CSIRT の告知と活動開始



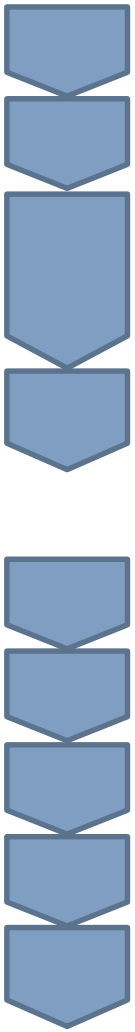
出典
JPCERT/CC「CSIRTガイド」
p27 インシデントマネジメント、ハンドリング、レスポンスの関係

⑥ ルール作り
⑦ SOC/CSIRT の告知と活動開始



出典
JPCERT/CC「経営リスクと情報セキュリティ」
p44 CISIRT関連サービス構成

SOC/CSIRT構築の流れ（例）



▼-----運用フェーズ

⑧ 施策の実行依頼　と　施策実行現場の教育(協力のお願い)

⑨ 実行レベル確認（監査）

⑩ スキルアップ

　　対策手法研究（新手法研究）

　　設備（性能維持・改善、脆弱性管理）

　　SOC/CSIRT人財スキル維持・改善

　　現場リテラシー維持・改善

⑪ SOC/CSIRTメンバ評価

▼-----インシデントフェーズ

⑫ インシデントハンドリング

⑬ 実害対策実施

⑭ フォレンジック

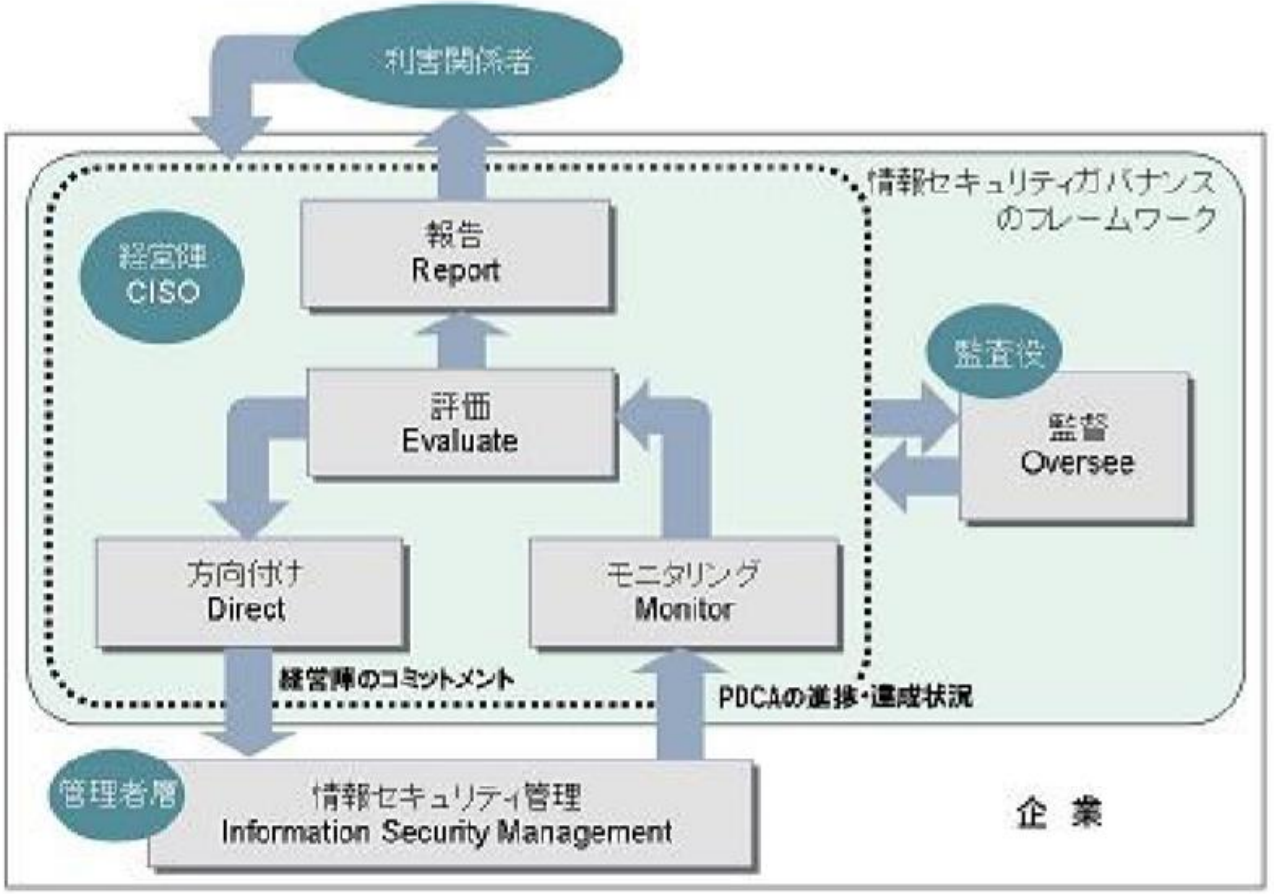
⑮ インシデント報告

　社外（サプライチェーン、警察、監督官庁、アナウンス）

　社内

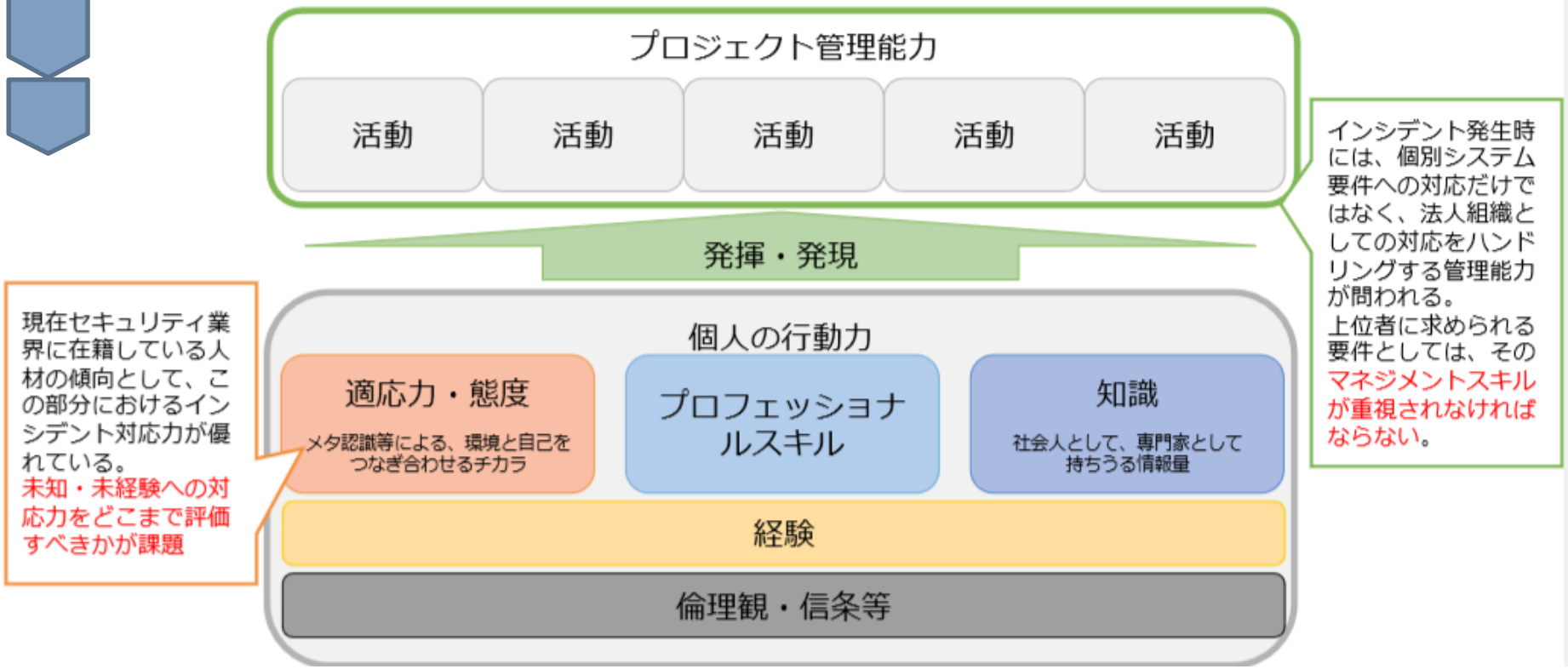
⑯ フィードバック　（と感謝！）

⑧ 施策の実行依頼　と　施策実行現場の教育(協力のお願い)
⑨ 実行レベル確認（監査）



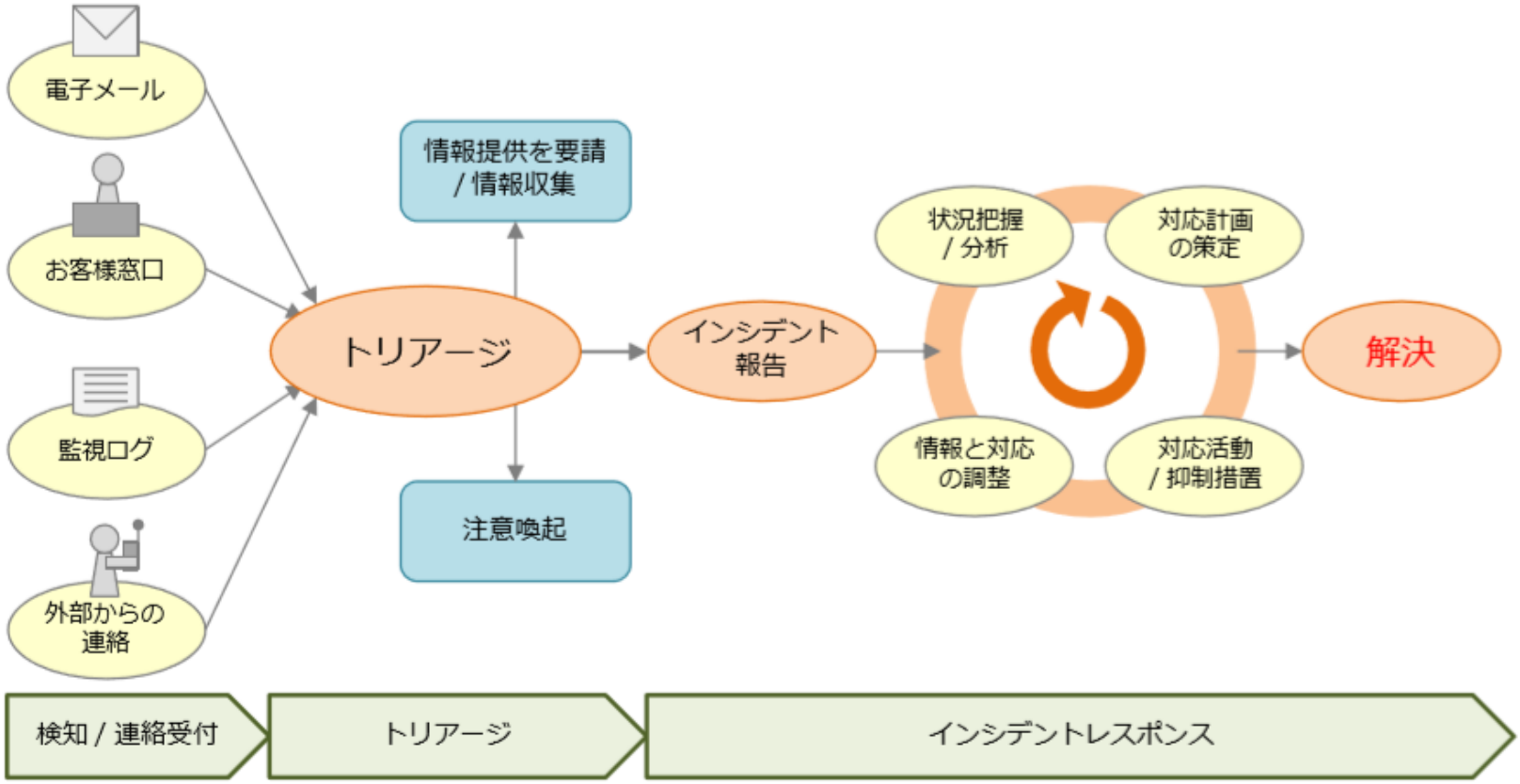
出典
経済産業省「情報セキュリティガバナンス導入ガイダンス」
p4 情報セキュリティガバナンスのフレームワーク

⑩ スキルアップ
⑪ SOC/CSIRTメンバ評価



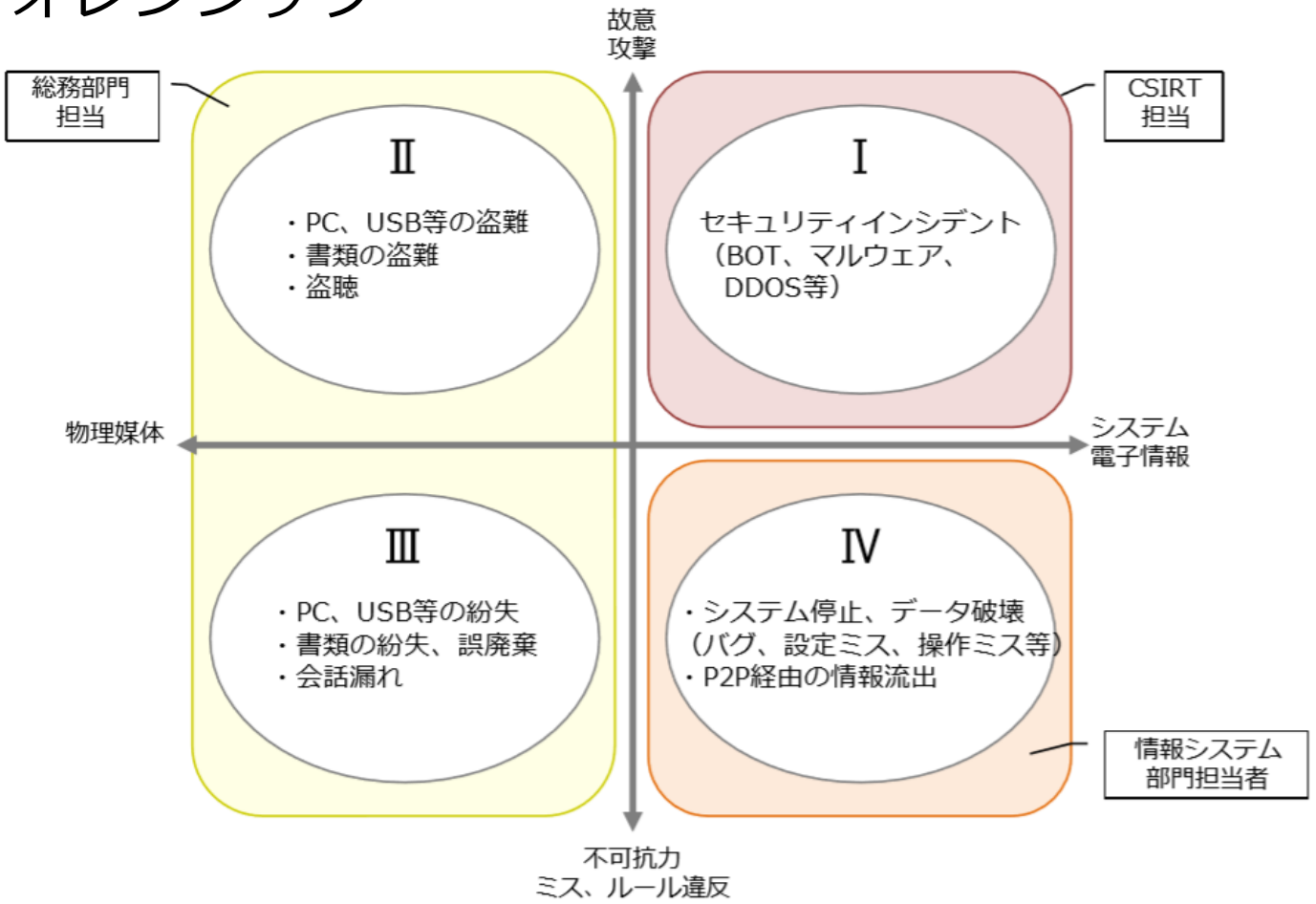
出典
産業横断サイバーセキュリティ人材育成検討会 第1.0版
p5 機能・役割を人的側面から検討する

⑫ インシデントハンドリング



出典
JPCERT/CC「CSIRTガイド」
p29代表的なインシデントハンドリングの流れ

⑬ 実害対策実施
⑭ フォレンジック



出典
JPCERT/CC「経営リスクと情報セキュリティ」
p39 情報資産に係る脅威の分類と対応担当

⑮ インシデント報告
⑯ フィードバック（と感謝！）

記載されている一次被害

サイバーセキュリティインシデント発生による一次被害の記載の中でも多いものを見ると以下表 3-5 のようになった。参考のために、平成 21 年度の記載企業数との差分を表した。

（表 3-5）

インシデント発生による一次的被害	平成25年度 記載企業数	平成21年度 記載企業数	差分
個人情報漏えい	113 (83%)	101	12
機密情報漏えい	105 (77%)	88	17
ITシステム障害	85 (63%)	62	23

	平成25年度 記載企業数(%)
	67 (49%)
情報セキュリティ方針、規定類の策定	29 (21%)
個人情報管理の体制整備／運用強化	21 (15%)
情報システムセキュリティ管理体制の強化	21 (15%)
情報システムセキュリティ対策の強化	58 (43%)

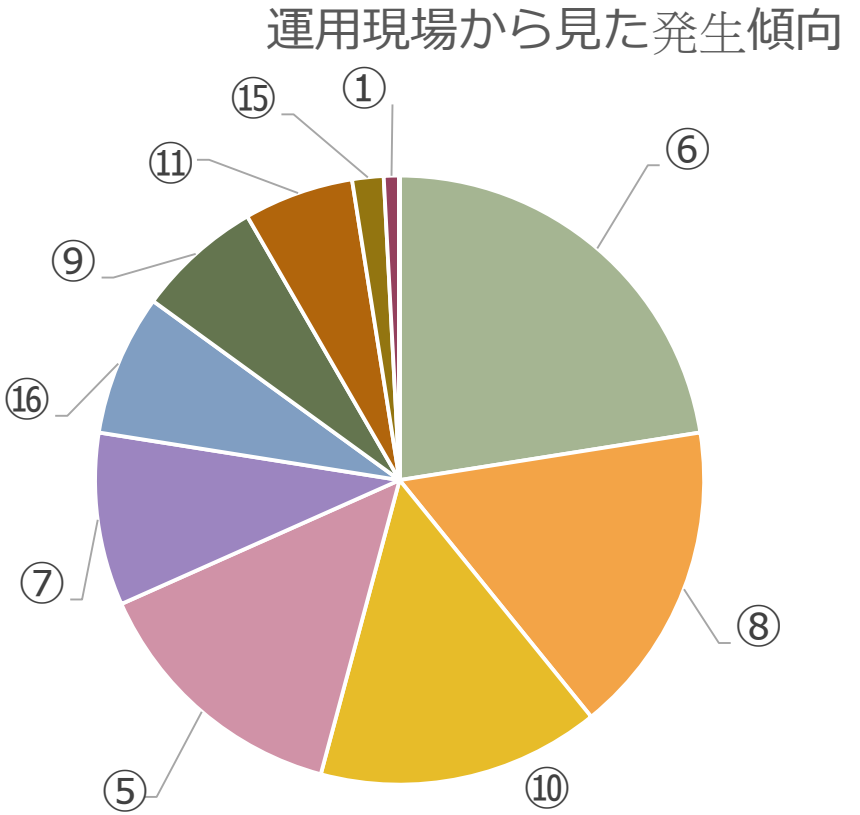
出典
内閣サイバーセキュリティセンター「企業の情報セキュリティリスク開示に関する調査」
p13 有価証券報告書のサイバーセキュリティリスク記載

アジェンダ

- 自己紹介
- SOC/CSIRT構築の流れ（例）
- 失敗あるある傾向
- あるセキュリティチームの発足一年史
- 失敗あるある例　構築パート
- 失敗あるある例　運用パート
- 失敗あるある例　インシデントパート
- まとめ

運用現場から見た失敗あるある傾向

▼----SOC/CSIRT　構築フェーズ
① 経営層から理解を得る
② 組織内の現状把握
③ SOC/CSIRT構築活動のためのチーム結成と社内協力体制の構築
④ 設計と計画
⑤ 環境構築　必要な人・物・金
⑥ ルール作り
▼----運用フェーズ
⑦ SOC/CSIRT の告知と活動開始
⑧施策の実行依頼　と　施策実行現場の教育
⑨実行レベル確認（監査）
⑩スキルアップ
⑪SOC/CSIRTメンバ評価
▼----インシデントフェーズ
⑫ インシデントハンドリング
⑬ 実害対策実施
⑭ フォレンジック
⑮ インシデント報告
⑯ フィードバック　（と感謝！）



アジェンダ

- 自己紹介）
- SOC/CSIRT構築の流れ（例）
- 失敗あるある傾向
- あるセキュリティチームの発足一年史
- 失敗あるある例　構築パート
- 失敗あるある例　運用パート
- 失敗あるある例　インシデントパート
- まとめ

©ブラックジャックによろしく 佐藤 秀峰 (漫画 on web http://mangaonweb.com/)

©ブラックジャックによろしく 佐藤 秀峰 (漫画 on web http://mangaonweb.com/)

©ブラックジャックによろしく 佐藤 秀峰 (漫画 on web http://mangaonweb.com/)

実録？？ドキュメンタリー

ブラックＳＯＣに

よろしく

©ブラックジャックによろしく 佐藤 秀峰 (漫画 on web http://mangaonweb.com/)

そして立ち上げ初日・・・・

©ブラックジャックによろしく 佐藤 秀峰 (漫画 on web http://mangaonweb.com/)

失敗あるある例：構築パート

©ブラックジャックによろしく 佐藤 秀峰 (漫画 on web http://mangaonweb.com/)

©ブラックジャックによろしく 佐藤 秀峰 (漫画 on web http://mangaonweb.com/)

失敗
あるある！

確かに技術力はすごいが、ＣＳＩＲＴとしての活動に役立っているのか？？
弊社の業務を理解していない。このインシデントに対する対応は正しいのであろうか・・・。
彼の言っていることがわからない。誰も彼を評価できない！！

何が問題だったのか・・・

©ブラックジャックによろしく 佐藤 秀峰 (漫画 on web http://mangaonweb.com/)

©ブラックジャックによろしく 佐藤 秀峰 (漫画 on web http://mangaonweb.com/)

失敗
あるある！

ＣＳＩＲＴ立ち上げ時にＣＳＩＲＴと言うものに対する理解が足りず、経営層、事業部門、実際に対応する運用部門などの全てから突き上げを食らってしまう。
これまでの運用体制との整合性をとらなかったため、運用部門との関係に亀裂が生じてしまった。
→結果、ＣＳＩＲＴが組織内で孤立化。

何が問題だったのか・・・

失敗あるある例：運用パート

そして導入後・・・

©ブラックジャックによろしく 佐藤 秀峰 (漫画 on web http://mangaonweb.com/)

失敗あるある！

運用が始まっているのに、製品から出るアラートに対して対応できる体制ができていない。
設定をチューニングしたいが、導入を丸投げしたため、対応できる人がいない。
ドライランなどの試験を実施していない・・・。

何が問題だったのか・・・

©ブラックジャックによろしく 佐藤 秀峰 (漫画 on web http://mangaonweb.com/)

©ブラックジャックによろしく 佐藤 秀峰 (漫画 on web http://mangaonweb.com/)

失敗
あるある！

ログを取る目的が決まっていないため全ての情報を取得し、キャパシティオーバー。アラートを拾いすぎて、監視システムがキャパシティオーバー。
→機器の性能を引き出せないまま運用することに。
アラートが出てるけど、危険度低だな！！安心安心。
→実は攻撃の予兆であり、導入したセキュリティ機器では検知できない攻撃でシステムを侵害される。
各機器で検知できる攻撃を理解していない。

何が問題だったのか・・・

失敗あるある例：インシデントパート

そして・・・

©ブラックジャックによろしく 佐藤 秀峰 (漫画 on web http://mangaonweb.com/)

©ブラックジャックによろしく 佐藤 秀峰 (漫画 on web http://mangaonweb.com/)

©ブラックジャックによろしく 佐藤 秀峰 (漫画 on web http://mangaonweb.com/)

©ブラックジャックによろしく 佐藤 秀峰 (漫画 on web http://mangaonweb.com/)

失敗
あるある！

インシデントの原因を特定し、対応を行うために必要となる人・物・金の準備ができていない。

- スキルがない。
- お金がない。
- 証拠がない。

原因が特定できないままただ時間だけが過ぎていく。。。

何が問題だったのか・・・

またまたインシデント発生・・・

©ブラックジャックによろしく 佐藤 秀峰 (漫画 on web http://mangaonweb.com/)


誰が止める手続きをするんだ？
役員会？この時間に役員は捕まらんよ
ただ勝手に止めた場合はきみの責任問題に発展するよ
止めると言っても実際どう止めるんです？
復旧の方法も教えてもらわないと、俺たち何もできないですよ。
インシデント対応マニュアル？
そんなもの見たこともないし、広報部門は関係ないから帰っていいですか？
©ブラックジャックによろしく 佐藤 秀峰 漫画 on web http://mangaonweb.com/

なんで時間があるときに

社内部門との関係作りや
インシデント対応訓練とかを
やっておかなかったんだろう・・・

©ブラックジャックによろしく 佐藤 秀峰 (漫画 on web http://mangaonweb.com/)

失敗
あるある！

インシデント対応における役割分担が明確でないため、実際の問題が発生したときに、責任の押し付け合いが発生。
調整先が多岐に渡り、インシデントの原因が判明しても対応までいかない。
インシデント対応訓練を実施しておらず、対応に習熟していないため、対応に遅れが発生してしまう。

何が問題だったのか・・・

まとめ

- 失敗あるあるはさまざまな観点で発生します。
  またその時の立場や役割、インシデントの内容などによって
  失敗の見え方も違ってきます。

次はより具体的な失敗あるあるネタを、
パネルディスカッションで議論します！