第6回
情報セキュリティマネージャー
ISACAカンファレンス in Tokyo

（配布用資料）

CSIRT現場からみるサイバーセキュリティと監査

佐藤元彦

Who am I ?

- 佐藤元彦
- 伊藤忠商事株式会社
  IT企画部 ITCCERT 上級サイバーセキュリティ分析官
- 国立大学法人　千葉大学
  運営基盤機構　情報環境部門
  准教授

- JPCERT/CC専門委員
- JASA特任研究員

My experience?

- それなりに長い間、この業界で働かせていただいています
  - 脆弱性検査(NW・Webアプリ)
  - 情報セキュリティ監査・システム監査
  - 政府の基準作り(情報セキュリティ管理基準等)
  - ISO SC27国内委員
  - セキュリティコンサルティング(方針策定・規程作り・体制整備・リスク分析)
  - インシデントレスポンス(複数の政府機関・民間事案をクローズ)
  - その他、情報セキュリティに関わる仕事(もちろん営業活動も)

今の仕事

・千葉大学と伊藤忠商事の二つのCSIRTを掛け持ち

・伊藤忠商事では、本体のサイバーセキュリティ施策の立案・遂行・運用が業務。また、グループ全体のサイバーセキュリティ施策の支援も実施。

・千葉大学は週に一回の勤務のため、制度作り・仕組み作り・実務支援・トリアージ支援・情報提供が主
・千葉大学では、バグバウンティ制度なども企画

簡単に仕事内容の紹介

- 伊藤忠商事株式会社のIT企画部に所属し、同社及びグループ会社のサイバーセキュリティの確保に努めています。

- 商社 / ユーザ企業のサイバーセキュリティ部隊のイメージ像？

- ISMSを下敷きにしたマネジメント
- 役割が回ってきたよくわかっていない担当者
- 現場が言うことを聞かないといつも愚痴ってる
- とりあえず(高い)製品ばっかり買っている
- でも運用は子会社か委託先に丸投げ
- 飲んでばかり？ <- 商社のイメージ

ITCCERT

- <投影のみ>

CSIRTの現場

CSIRT実務

- <投影のみ>

イベント・インシデント

・<投影のみ>

施策の具現化　(事業会社支援)

- 伊藤忠商事は、伊藤忠グループ会社をよりよくするために、有形・無形の責任を負っています。(グループ経営)

- そのため、これまでもメルマガ発行、連絡会を通じた情報提供、ワークショップ開催などを実施してきましたが。。。(間接支援)

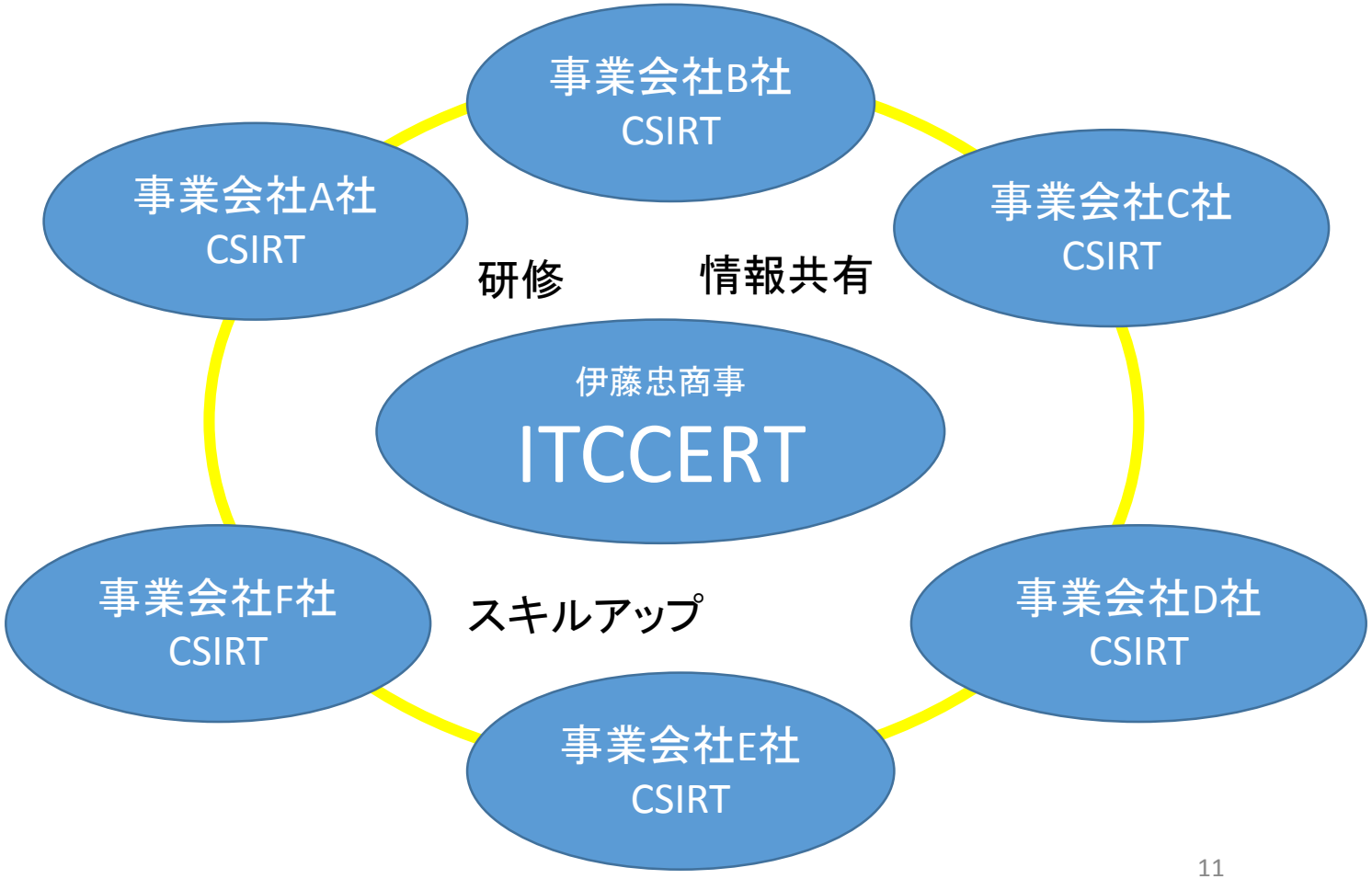
- 様々な事案が発生。適切なインシデントレスポンスで消火しているものの、これでよいのだろうか

- サイバー攻撃対応において、これらの間接支援を繰り返すことには限界がある。

グループ会社セキュリティ　理想

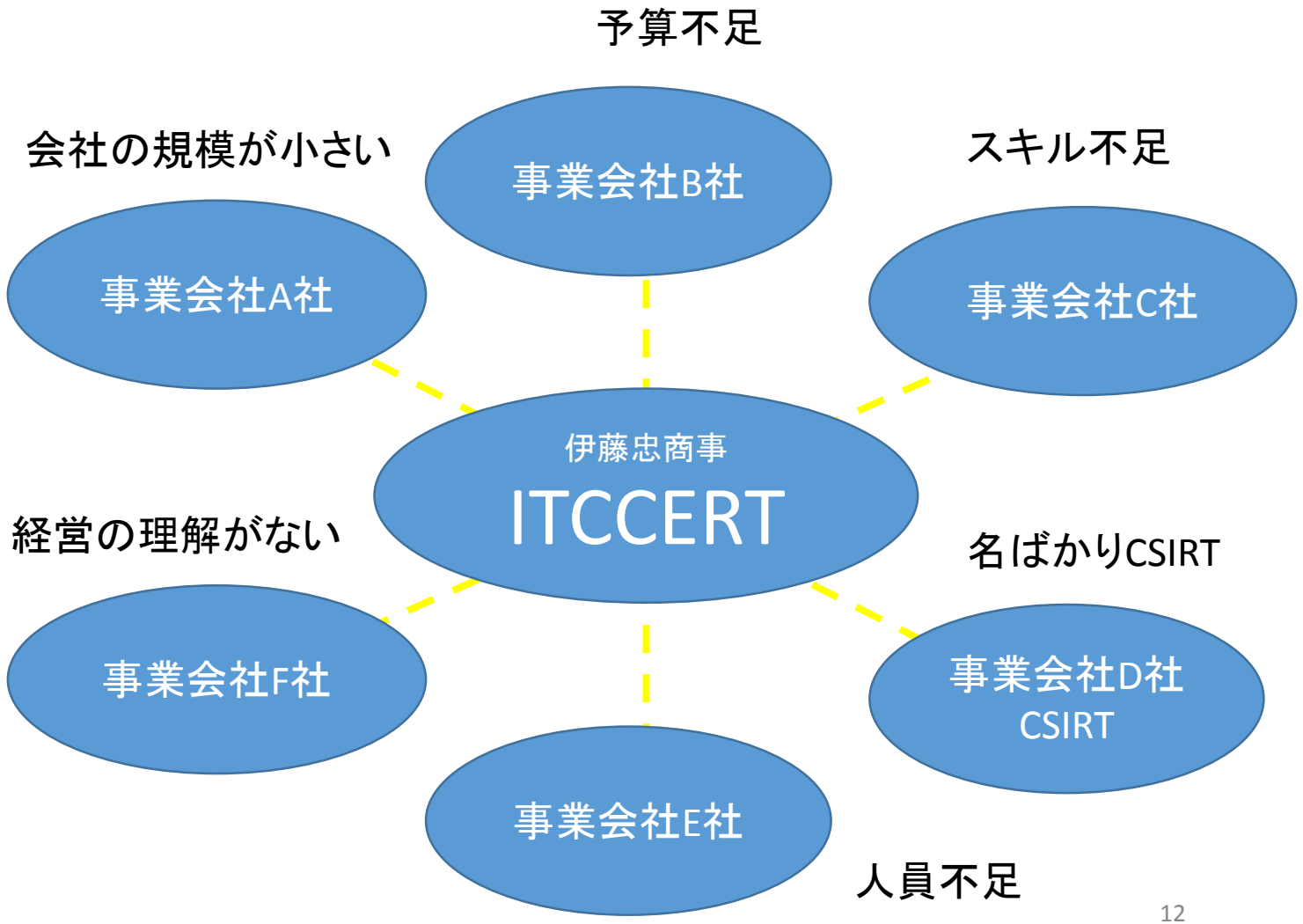
- 例えば、こういったコンサル的な絵を描きがち

- みんながCSIRTを作ってCSIRT連合で、グループ全体を底上げ!!



グループ会社セキュリティ　現実

- 現実は。。。
- 各社が自主自立で、高めあって相互連携することは夢物語
- ではどうするか？



現実解

我々がとれる現実的な策を考え抜いた

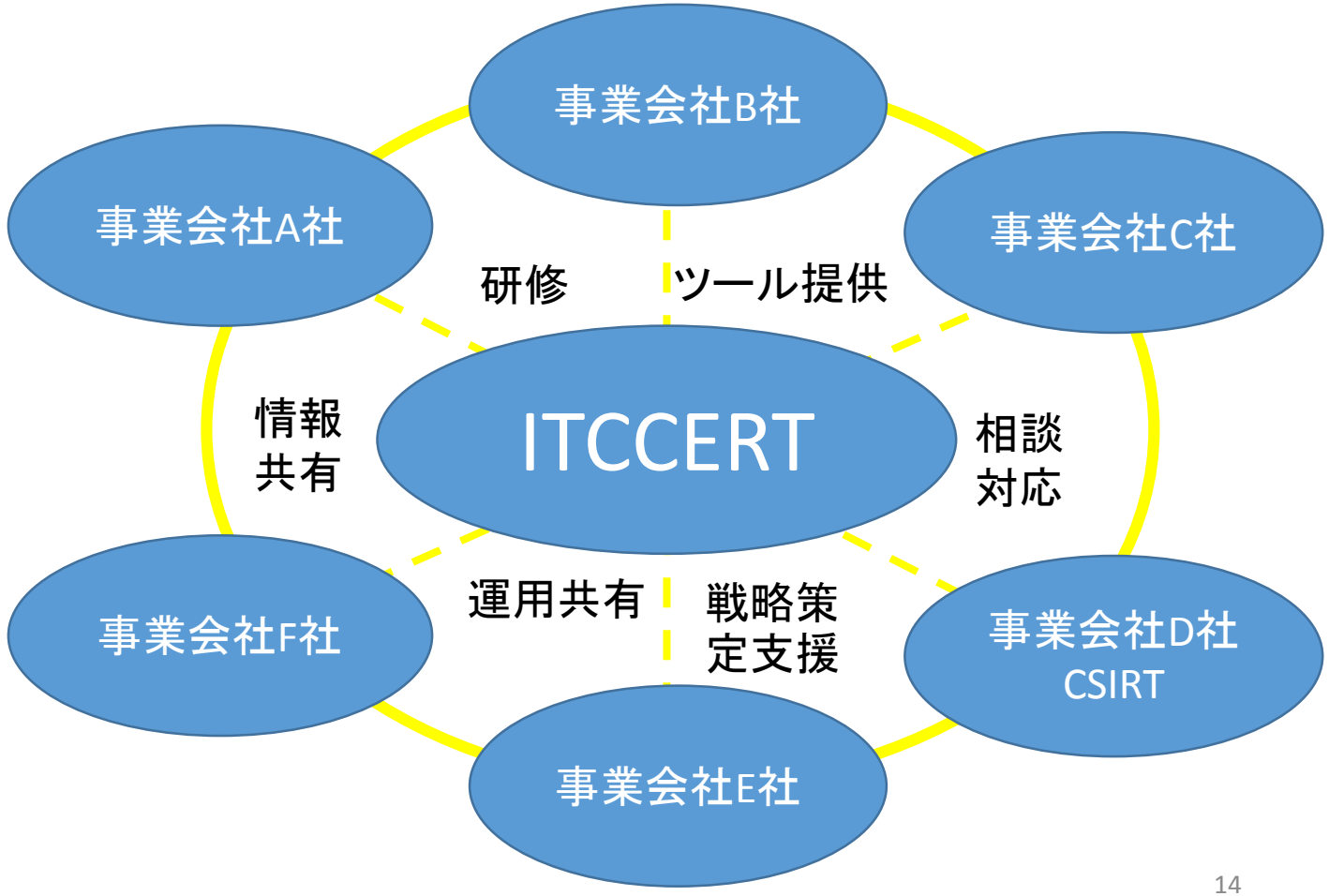
- サイバーセキュリティ対策の重要性は年々高まっており、グループ全体でのセキュリティレベル向上は必須
- しかし、個々の事業会社において、以下制約の一部において、もしくは全部において大きな限界がある

➢サイバーセキュリティ対策に投資できる“コスト”
➢サイバーセキュリティ対策を行える“人的リソース”
➢サイバーセキュリティ対策の為の“ナレッジ”

■ITCCERTが伊藤忠グループ全体に対し、さらに踏み込んでもっとダイレクトにサイバーセキュリティ対策支援を推進する。

グループ会社セキュリティ　施策

- サイバーセキュリティの部分に関し、ITCCERTがグループ会社を支援できるメニューを作成



自ら動くCSIRT

- 単なる技術者溜まりとしてのCSIRTでもなく、コンサルから賜った施策を外部に発注するCSIRTでもなく、もちろん名ばかりのCSIRTでもなく。。。
- 自分の手も動かす、頭も使う、足も運ぶ。戦略・戦術・実行部隊のエコシステムを繰り返しています。

- なので、現場を知らず「聞いた話と想像でとくとくと専門家っぽく語る(騙る)人」たちとは相容れないことが多く。。。
- とはいえ、それを許してしまうのは、ユーザ部門の怠慢かもしれません
- 今日は、自らのサイバーセキュリティ対応の仕組みを監査という視点で、見直すきっかけになれば、と思っています。

“I” シリーズの施策

- <投影のみ>

サイバーセキュリティと監査

監査人として

- 自分のキャリアの大きな部分を情報セキュリティ監査が占めています
- 管理策の成り立ちを聞いたり、どうしてこの管理策が求められるのかであったり、もっとよい管理策があるのではないかであったり、監査をベースに考えることが増えました。
- もちろん、実行性ではなく、有効性をメインに考えてきました。
- 助言型は、その実、コンサルティングと大差ないのですが、監査人倫理を持つ点、自分の判断に「責任」を有しているはず。

- ところが最近、監査人の中でも話があわないことが多い。。。
- 今時そんな対応では。。。という管理策を金科玉条として抱えている。

サイバー攻撃の事例

・<投影のみ>

これに対応するすべは？

・リスク分析していますか　[はい/いいえ]
では、”足りない!!”

・現場に必要なのは、実務として対応できる仕組みと運用

・でも、それを語れる人は少なく、さらに実現できる人は少ない

・結果。。。
・サンドボックスいかがっすかー
・次世代AVいかがっすかー
・CSIRT構築支援いかがっすかー

話を元に。。。

・このままいくと今のセキュリティ業界を監査してしまいそうなので。。。

昔の「セキュリティ」需要

リーダー

ISMS　スパム対策
ファイアウォール
ウイルス対策
USB管理・暗号化

ニッチャー

Webセキュリティ検査
脆弱性検査　VPN
DoS対策　改ざん検知
パケットアーカイブ

チャレンジャー

IDS　SOC　BCP / DR
PMS / 個人情報保護
フィッシング対策
ウェブフィルタリング

フォロワー

認証・ID管理
セキュリティ教育
検疫　監査
資産管理　パッチ管理

information security

今の「セキュリティ」需要

リーダー

CSIRT　RED TEAM

ログ分析 / SIEM

サンドボックス PROXY

DDoS対策 ゼロデイ対策

ニッチャー

インテリジェンス

セキュアプログラミング

DNSセキュリティ

PCI-DSS

チャレンジャー

内部不正検知 BEC対策

クラウドセキュリティ

セキュリティクラウド

次世代AV　可視化

フォロワー

旧来のセキュリティ

BYOD / シンクラ

SNSセキュリティ

cyber security

新旧セキュリティ

- 旧世代セキュリティ
  - 「学習」で身に付く智識
  - 顧客側に智識がない(担当になっちゃった人)
  - 規範策定と規範遵守を重要視
  - ウイルスと不正アクセスが技術用語
  - 金銭被害あるも小規模

- 新世代セキュリティ <- 今
  - 「実践」「経験」が必要な智識
  - 顧客側も学習。ユーザサイドにエキスパート
  - 監視・検知・対応を重要視
  - 標的型攻撃と内部不正(最近はBEC)
  - 風評被害も含め損害が大規模に

リスクが変化した

・持ち出しパソコンを台帳に記載しているか？

よりも、

・プロキシログを適切に分析し不審通信を特定できているか？
　※適切と不審の定義も重要

の方が、「サイバーセキュリティ」を重視しなければならない組織では重要であり、やらなければならないことになった

これに気づいていない？

リスクの変化に対応した監査を

- 今日は「監査人に聞いてもらいたい」質問を取り上げさせていただきます。

- もちろん、「これを聞け」ではなく、「現実」はこうなんだ、こういう「対策」をしているんだ、こういう「視点」で確認すればよいんだ、という部分を感じ取っていただければ。。。

※ここでいう「監査人」は実行性だけをチェックする、セキュリティを知らなくてもできるものは対照にしていません

監査項目

- <投影のみ>

ありがとうございました