2015年度
活動成果報告会 = J-fes!!

2015 年度
企業リスクマネジメント研究会活動報告

2016年4月21日

アジェンダ

1. 企業リスクマネジメント研究会の歴史と概要
2. 2015年度活動報告
   - 全体会
   - 分科会A（サイバーセキュリティ）
   - 分科会B（BCP）
   - 分科会C（セキュリティガバナンス）
3. まとめ

企業リスクマネジメント研究会の歴史と概要

ユーザーの要求が未来を切り拓く
ーイノベーションで企業を変える、日本が変わるー

JUAS活動

政策企画委員会

政策研究・調査
- IT経営協議会（CIO戦略フォーラム）
- IT経営調査
- IT融合フォーラム
- CIO育成カリキュラム
- 重要インフラの信頼性
- IT投資可視化

調査事業
- 企業IT動向調査
- ソフトウェアメトリックス

組織力強化普及・調査
ーUISSセンターー
- 情報システムユーザースキル標準
- IT人材モデルキャリア開発

セキュリティ・センター
- プライバシーマーク審査・認証

会員活動

フォーラム
- CIOフォーラム（３）
- 部門経営フォーラム（５）
- IT企業TOPフォーラム（３）
- ITグループ会社経営フォーラム（３）
- IT部門経営フォーラム関西
- IT企業TOPフォーラム関西
- ITグループ会社経営フォーラム関西
- 関西ミドルマネジメントフォーラム

研究会
テーマ型研究会
データマネジメント研究会
データサイエンス研究会 （New）
ITインフラ研究会
ITサービスマネジメント研究会

企業リスクマネジメント研究会
ビジネスプロセス研究会
ITポートフォリオ研究会 （New）
IT人材キャリア形成研究会
組織力強化研究会
IT戦略研究会 （旧ケース研究会）

ケース型研究会
ビジネスモデル研究会 etc.

アドバンスト研究会
情報共有研究会 etc.

研究プロジェクト
システム開発・保守QCD研究プロジェクト etc.

イノベーション経営カレッジ（IMCJ）

教育研修事業
- オープンセミナー
- 新人・配転者セミナー
- オーダーメイド研修
- 教材開発・出版
- 海外研修・調査

JUASラボ
JUASソリューションラボ
JUASトレンドラボ

公開事業
サマースクエア
JUASスクエア
JUAS FUTURE ASPECT

会員研修会
JUASアカデミー
関西アカデミー

企業リスクマネジメント研究会の経緯と現在

企業情報マネジメント研究会 （2006年～2007年）

日本版SOX法への対応を中心とした参加企業相互による情報交換

企業リスクマネジメント研究会

2008年度

- リスクマネジメントの研究
  - 情報管理
  - 法務
  - BCP

2009年度

- リスクマネジメントの研究

2010年度

2009年度、2010年度

- 情報管理
- 法務
- BCP

2011年度

- 震災後のリスクマネジメントの研究
  - 情報管理
  - BCP1
  - BCP2

情報セキュリティ研究会

2012年度

- サイバー関連
  - BCP（石橋）

企業リスクマネジメント研究会

2013年度

- 企業リスクマネジメントの研究

2013年度
- 情報セキュリティ
- 個人情報、スマホ
- BCP

2014年度

2014年度
- 情報セキュリティ1
- 情報セキュリティ2
- BCP

企業リスクマネジメント研究会の概要（2015年度募集案内）

【研究会概要】

健全な企業活動を阻害するリスクが多様化・高度化する中、その変化への対応が急務となっています。 本部会では多々ある**リスク対応**の中から以下のテーマについて、

個社での取組みに加え、企業の枠を超えた取組みの可能性について議論

を通じ情報交換します。

①サイバーセキュリティ	（サイバー攻撃、マルウェア感染、脆弱性対応基準、制御システム　等）
②BCP	（データセンター、有事の際の運用継続・コミュニケーション手段　等）
③個人情報保護	（内部犯行防止、従業者・委託先管理、各国法令の理解と対応　等）

研究会メンバー構成

51法人/54名の皆様にご参加いただきました。

ステータス	人　数
新規	32名
継続	17名
復帰	2名
途中交代	3名

参加状況

最終回の参加状況 ： 40/51（78.4%）

一年間の活動を無事終えることが出来ました

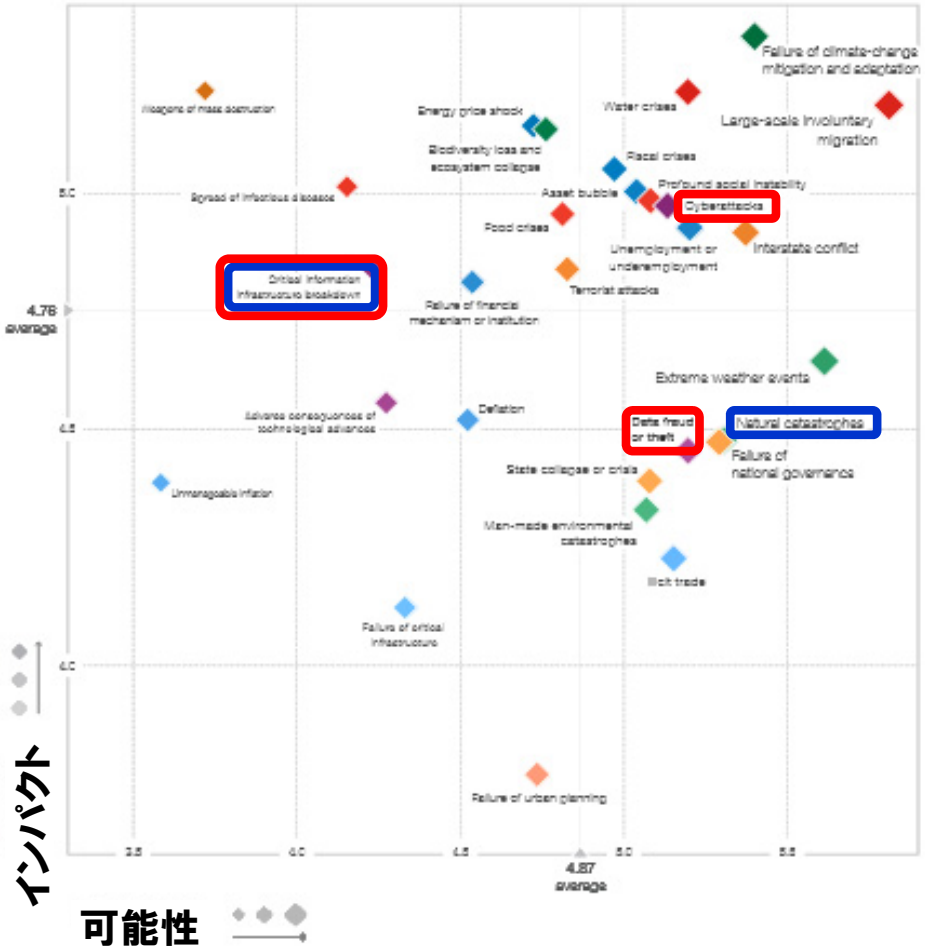
研究テーマの決定

サイバーセキュリティ		テーマ1
サイバー攻撃/マルウェア感染(技術対策)	28	
脆弱性対応基準	30	
インシデント/脆弱性情報の企業間連携	20	
事業継続計画(BCP)		テーマ2
BCP対策(データセンター/バックアップ)	13	
BCP対策(発動基準/体制)	12	
有事の際の運用継続・コミュニケーション手段	18	
企業(法人)間連携(自助/共助)	4	
セキュリティガバナンス/個人情報保護		テーマ3
グループ統制/グローバル統制	28	
委託先管理/監査	19	
ルール/体制	26	
個人情報保護対策(技術対策)	20	

【参考】The Global Risks Report 2016

～ 世界経済フォーラムの資料より ～

The Global Risks Landscape 2016



出典 ： http://www3.weforum.org/docs/GRR/WEF_GRR16.pdf

Global Risks of Highest Concern for Doing Business (Japan)

	Risk	Share
1.	Cyberattacks	51.6
2.	Natural catastrophes	46.2
3.	Fiscal crises	44.0
4.	Energy price shock	38.5
5.	Interstate conflict	30.8
6.	Failure of national governance	25.3
7.	Failure of financial mechanism or institution	22.0
8.	Critical information infrastructure breakdown	20.9
9.	Asset bubble	17.6
10.	Data fraud or theft	13.2
10.	Terrorist attacks	13.2
10.	Extreme weather events	13.2
10.	Food crises	13.2
14.	Failure of climate-change mitigation and adaptation	12.1
14.	Deflation	12.1

出典 ： http://reports.weforum.org/global-risks-2016/eos/#country/JPN

2015年度研究会活動形式

メンバーのコミュニケーションの距離・密度・質を上げるために、分科会形式で活動を行いました。

全体会
部会長　：（株）リコー
副部会長　：　東日本旅客鉄道（株）

- **サイバーセキュリティ**
  分科会長　：　ANAシステムズ（株）
  副分科会長　：（株）中電シーティーアイ
- **事業継続計画（BCP）**
  分科会長　：（株）NEC情報システムズ
  副分科会長　：　丸文（株）
- **セキュリティガバナンス／個人情報保護**
  分科会長　：　JFEシステムズ（株）
  副分科会長　：（株）JALインフォテック

事務局
（社）日本情報システム・ユーザー協会

2015年度　全体会
活動報告

2015年度全体会活動スケジュール

	日時	場所	テーマ（案）
第1回	2015年5月29日(金) 16:00 ～ 18:00	JUAS2階 2-2会議室	・顔合わせ ・活動方針説明/グループ分け ・研究テーマ検討
第2回 ＊合宿	2015年7月10日(金)～ 2015年7月11日(土)	静岡県沼津	・グループ活動 （285分） ・各グループからの事例発表 （30分/分科会） ・グループ活動年間計画発表 （15分/分科会）
第3回	2015年10月01日(木) 15:40 ～ 18:00	JUAS2階 2-2会議室	・情報処理推進機構様　ご講演 （15分） ・事例発表(ANAシステムズ様) （50分） ・SecureWorks Japan様　ご講演 （50分）
第4回	2015年11月25日(水) 15:45 ～ 18:00	JUAS2階 2-2会議室	・事例発表(某社様) （30分） ・事例発表(ｱｲ･ｱｲ･ｴﾑ様) （30分） ・ガートナージャパン様　ご講演 （45分）
第5回	2016年1月27日(水) 15:30 ～ 18:00	JUAS2階 2-2会議室	・事例発表(JFEｼｽﾃﾑｽﾞ様) （45分） ・総務省情報流通行政局情報流通振興課様 ご講演 （60分）
第6回	2016年3月09日(水) 15:00 ～ 18:00	JUAS2階 2-2会議室	・活動の振返り(良い点･改善点　など) （90分） ・活動結果発表 （20分/分科会）

全体会の概要

各分科会で議論されている内容の情報共有（事例発表）と、ゲストスピーカーによるプレゼンテーション

SecureWorks様　ご講演資料

ガートナージャパン様　ご講演資料

総務省様　ご講演資料

2015年度　分科会A
（サイバーセキュリティ）
活動報告

2015年度分科会A活動スケジュール

	日時	場所	実施内容
第1回	2015年05月29日(金)	JUAS会議室	・メンバ紹介 ・活動概要説明
第2回	2015年06月24日(水)	JUAS会議室	・年間スケジュール／個人情報漏洩事件に関する議論 ・【JUAS－SOC観測情報】ルールの確認
第3回 ＊合宿	2015年07月10日(金)～ 2015年07月11日(土)	沼津	・外部からの攻撃に対する対応について ・内部犯罪に対する対応について
第4回	2015年09月03日(木)	大田区内	・外部からの攻撃元、漏洩ルートの調べ方？ ・航空会社機体工場見学
第5回	2015年10月01日(木)	JUAS会議室	・膨大なproxyログの調査 ・SOCで観測された事象への対応について
第6回	2015年11月25日(水)	JUAS会議室	・CSIRTの作り方 ・CSIRT演習(First Season)
第7回	2015年12月17日(木)	JUAS会議室	・CSIRT演習(Second Season)
第8回	2016年01月27日(水)	JUAS会議室	・CSIRT演習(Third Season)
第9回	2016年03月09日(水)	JUAS会議室	・活動結果発表 ・日本シーサート協議会 人材育成の話

【JUAS－SOC観測情報】の共有

SOC観測情報って？
Security Operation Centerで観測されたセキュリティ脅威に関する情報

サイバーセキュリティ経営ガイドライン（経産省/IPA）

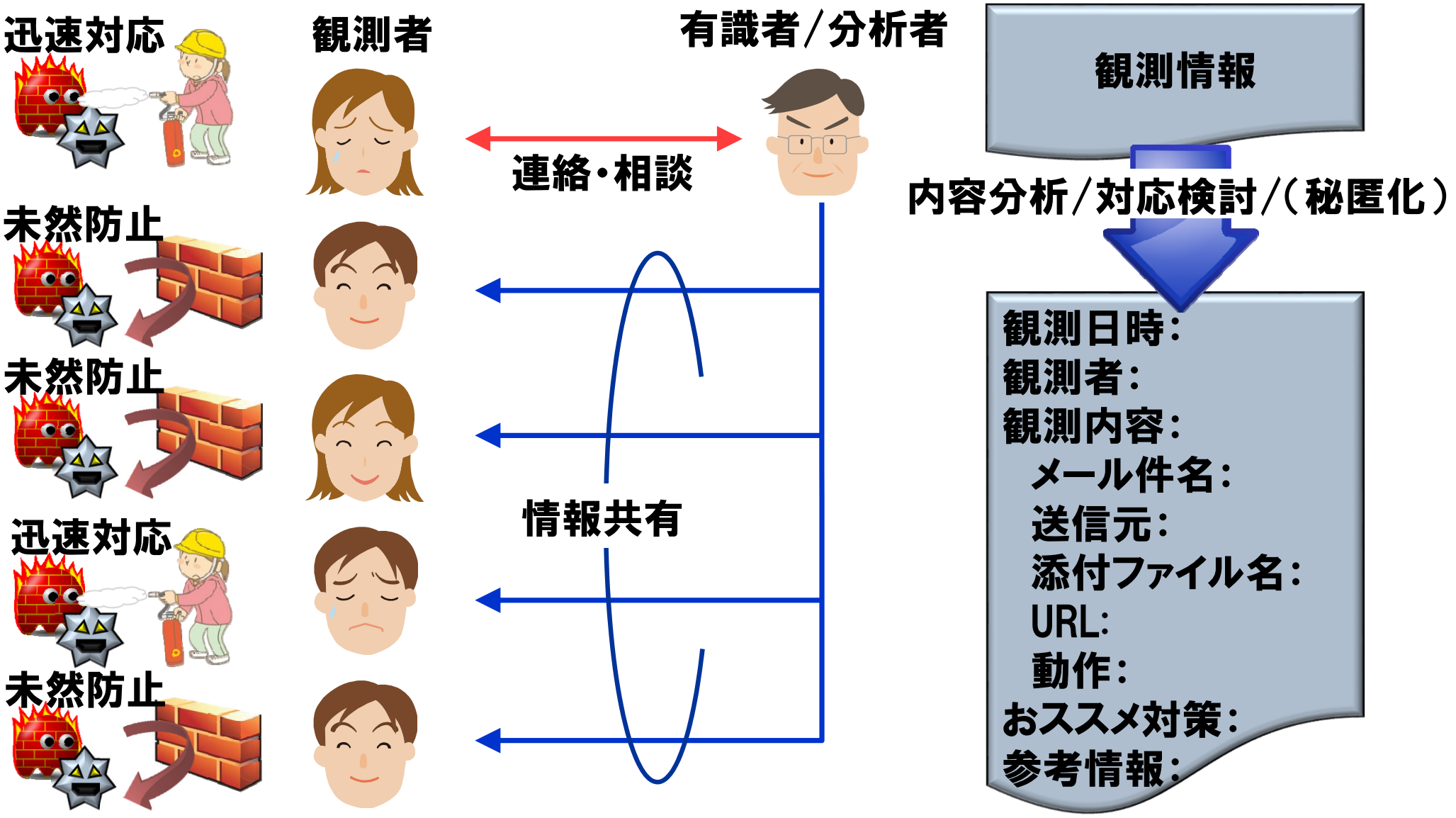
3. サイバーセキュリティ経営の重要10項目

1. リーダーシップの表明と体制の構築 （2項目）
2. サイバーセキュリティリスク管理の枠組み決定 （3項目）
3. リスクを踏まえた攻撃を防ぐための事前対策
   （6）サイバーセキュリティ対策のための資源（予算、人材等）確保
   （7）ITシステム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保
   （8）情報共有活動への参加を通じた攻撃情報の入手とその有効活用のための環境整備
4. サイバー攻撃を受けた場合に備えた準備 （2項目）

社会全体において最新のサイバー攻撃に対応した対策が可能となるよう、サイバー攻撃に関する情報共有活動への参加と、入手した情報を有効活用するための環境整備をさせていますか？

出典 ： http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf

【JUAS－SOC観測情報】の共有



【JUAS－SOC観測情報】の共有の結果（成果）

共有 27事案

有効

・情報の提供を受けた企業で同じ事象を発見！

嬉しい

・新種マルウェアのC&Cサイトとの通信！

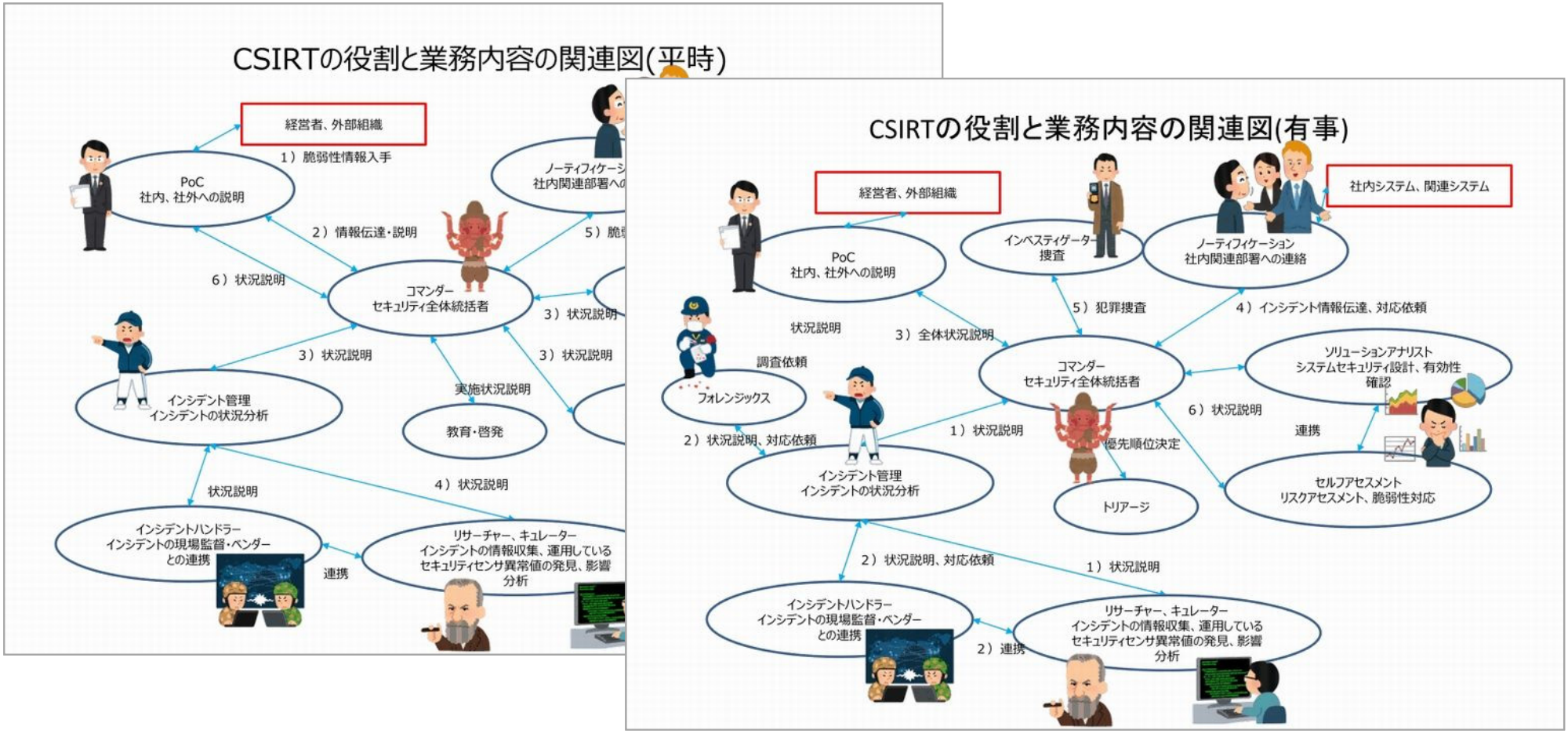
・複合機からの送信を語ったメール！

話題

皆さんも “企業リスクマネジメント研究会”に参加して、
情報共有しましょう！

CSIRTの作り方／演習

日本CSIRT協議会発行の “CSIRT 人材の定義と確保”（の補足資料）と想定事例に基づいて、演習を行った。



出典 ： http://www.nca.gr.jp/2016/pr-seminar/files/20160223recruit-hr-appendix.pdf

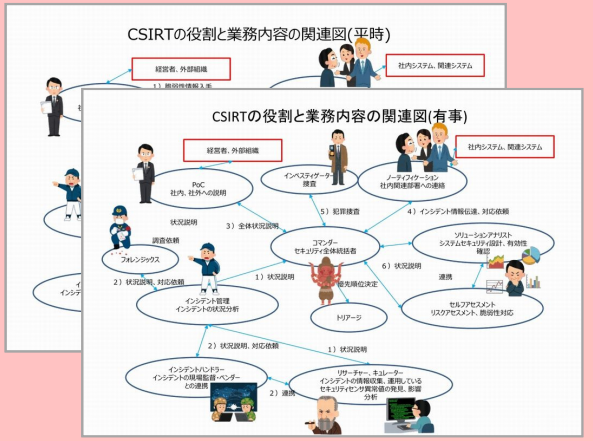
CSIRTの作り方／演習（想定事例）

第1話	脆弱性情報を入手した！
第2話	他社に着弾したランサム情報を入手した！
第3話	JUAS社内に不審な添付つきメールが送られてきたと、 社員から報告あり！
第4話	本当？JUAS社を名乗ったメールが取引先に届いた！ ウィルスが添付されているんだって！
第5話	ちょっとまって！ JUAS社内の端末がランサムにやられたかも！
第6話	ピンチ！JUAS社のホームページが改ざんされて ウィルスをまき散らしている模様。
第7話 （最終話）	謎。社内のSOCメンバから 不審な外部通信を見つけたとの報告あり！

CSIRTの作り方／演習の結果（成果）

＜特に勉強になった（んじゃないかと思っている）こと＞

- CSIRTを構成する各メンバーの役割
- 情報連携の重要性
- 対応の優先順位付けや深さは、状況の把握が大事



**皆さんも “企業リスクマネジメント研究会”に参加して、
有事の際の行動について勉強しましょう！**

2015年度　分科会B
（BCP）
活動報告

2015年度分科会B活動スケジュール

	日時	場所	実施内容
第1回	2015年05月29日(金)	JUAS会議室	・メンバ紹介 ・活動概要説明
第2回	2015年06月24日(水)	芝・大門	・年間スケジュール／合宿内容 ・事例紹介(共有) 1社
第3回 ＊合宿	2015年07月10日(金)～ 2015年07月11日(土)	沼津	・事例紹介(共有) 4社 ・事例に基づくディスカッション
臨　時	2015年09月03日(木)	大田区内	・航空会社機体工場見学
第4回	2015年09月11日(金)	福岡県	・セカンダリサイト見学 電力系DC(QIC様) ／ ベンダー系DC(NEC様)
第5回	2015年10月01日(木)	JUAS会議室	・事例紹介(共有) 2社 ・事例に基づくディスカッション
第6回	2015年11月25日(水)	JUAS会議室	・事例紹介(共有) 2社 ・事例に基づくディスカッション
第7回	2015年12月04日(金)	大阪府	・NEXCO西日本様　吹田道路管制センター見学
第8回	2016年01月27日(水)	JUAS会議室	・事例紹介(共有) 2社 ・事例に基づくディスカッション

現場視察（福岡・大阪）

“現場主義”！！　実際に “行って” “見て” “聞いて” “感じる” ことに意味がある
＃　非公開情報も聞けるかも “ここだけの話・・・”

日本電気株式会社　様

現場視察写真

株式会社キュウデンインフォコム　様

現場視察写真

西日本高速道路株式会社

現場視察写真

特別車両見学

管制室
イメージ

特別車両1

特別車両2

特別車両3

研究会を通じて学んだこと

- 要は人材！！
- 『伝承』が必要。
  専門性が高く、経験豊富な人材は直ぐには揃わない。
  人を育てる、伝承を何十年も実際にやっている…
- 『想定外なんて言っちゃいけません』
  想定外への対策を考えるのが、危機管理／リスク管理なのです。

2015年度　分科会C
（セキュリティガバナンス）
活動報告

2015年度分科会C活動スケジュール

	日時	場所	実施内容
第1回	2015年05月29日(金)	JUAS会議室	・メンバ紹介 ・活動概要説明
第2回	2015年06月17日(水)	JUAS会議室	・分科会テーマに関する議論 ・合宿テーマに関する議論
第3回 ＊合宿	2015年07月10日(金)～ 2015年07月11日(土)	沼津	・事例紹介(共有) 4社 ・事例/自由テーマに関するディスカッション
第4回	2015年08月28日(水)	日本橋	・事例紹介(共有) 2社 ・事例/自由テーマに関するディスカッション
臨時	2015年09月03日(木)	大田区内	・航空会社機体工場見学
第5回	2015年10月01日(木)	JUAS会議室	・事例紹介(共有) 2社 ・事例/自由テーマに関するディスカッション
第6回	2015年11月25日(水)	JUAS会議室	・事例紹介(共有) 1社 ・事例/自由テーマ/進め方に関するディスカッション
第7回	2015年12月11日(水)	JUAS会議室	・分科会メンバーを対象に行ったアンケート結果に基づいたフリーディスカッション
第8回	2016年01月27日(水)	JUAS会議室	・事例紹介(共有) 3社 ・事例/自由テーマに関するディスカッション
第9回	2016年03月09日(水)	JUAS会議室	・事例紹介(共有) 1社 ・事例/に関するディスカッション、活動の振り返り

分科会で取り扱った事例紹介テーマ（全11）

興味のあるテーマを抽出し、各社の “生” の取り組みを発表し、それをネタに意見交換を行った。

① マイナンバー制度
② 制御系システム
③ 子会社ガバナンス（国内編・海外編）
④ 委託先管理・監督（再委託、再々委託）
⑤ スマートデバイスアプリ開発・メンテナンス
→セキュリティ確保、ベンダーとの関係、責任の主体
⑥ 「あの件」のその後
→ 昨年度発生した顧客情報漏えい事故のその後
⑦ 従業者（役職員・委託先要員）教育（社内ルールの徹底）
⑧ インシデント対応、体制・訓練
⑨ 情報漏えい対策 → スマートデバイス、BYOD, シャドーIT
⑩ クラウド、ASPの扱い → ストレージサービスの許可、モニタリング
⑪ スマートデバイス等の業務スペース持ち込み

研究会ルール “その2”

研究会ルール “その1”

「マイナンバー制度」への取り組み

- 行政側のための制度で、企業側はメリットなし
- やり方はいろいろ
  - ① 人事給与をアウトソース → 委託先を管理・監査
  - ② パッケージを利用 → パッケージが対応
  - ③ 既存システムはそのままで個人番号管理を外付け
    - → 全体を作りなおしても、どうせそのうち制度も変わる
- システムはできても、その前後の取り扱いに注意
  - 紙の処分、使い終わったデータ → 要注意
  - 誤入力、社員が提供を拒否 → 行政側が言ってくるまで・・・
- 事故の風評が怖い → 社外に発見されないように

皆さんも “企業リスクマネジメント研究会”に参加して、“生”の情報交換を行いましょう！

まとめ

研究会参加による成果を上げる工夫

工夫1：分科会でコミュニケーションの距離を縮め、発言回数を増やす

- 参加者のモチベーションUPに貢献（しているはず）

工夫2：参加のハードルを下げる

- 各社の取り組み/悩みが研究材料です
- 宿題は出しません（自己学習、事例発表者は別ですが・・・）
- 欠席しても取り残されません（原則、一話完結）

工夫3：立派なドキュメントは作りません（研究の性格上・・・）

- サイバーセキュリティは変化が早い/BCP対策は各社まちまち
- 各社の対策に役立つ（と信じている）ノウハウは共有/検討します

2015年度活動の振り返り（反省点）

- 社内に持ち帰りフィードバック出来ない／アウトプット（企業秘密）が共有しにくい
  →行き辛い点もある。
- 新メンバーのために、最初に昨年度までの進め方・内容を話してもいいのでは
- もう少し短い時間の方が集まり易い
- 曜日がバラバラ（で、スケジュール確保が難しい）
- 自社の状況をもっと伝えたかった
- 各組織の、具体的な話をもっと深堀りしたかった
  例）担当者構成　悩み事　他社事例
- お酒を交えて交流したかった（遠方からの参加の方）
- 若手/女性の比率がぁぁぁ・・・
- 合宿会場がぁぁぁ・・・

2015年度活動の振り返り（良かった点）

- 勉強になった、知識を得た。
  - ➢業務に即していた。／初心者にも参考になった、視野が広がった
  - ➢各社実態・情報共有出来て良かった、参考になった
  - ➢各社同じような問題、悩みをもたれていて共有できたのはよかった
- 自社に成果を持ち帰ることができた。
  - ➢自社の業務への反映（還元）ができた。／自社CSIRTを構築した
- 「現場」を見に行く機会があり、他の業界の状況に触れて良かった
- 口外できないような話（情報）をして、心の中の叫びを共有しあえた
- 人間性豊かで多様な方々が集結。ざっくばらんに意見を言える雰囲気は良い
- 他分科会に自由に行けて良かった。
- 一話完結のテーマなので、仮に欠席したり、その会はついていくのは難しかった場合でも次回気持ちを切り替えて参加できる

2015年度企業リスクマネジメント研究会、無事完了

- 参加頂いた研究会メンバー皆さん
- 分科会をリードしていただいた幹事団の皆さん
- 無理な要望にも耐え、運営を支援いただいたJUASのスタッフの皆さん

１年間ありがとうございました！

それから・・・
私たちに研究会への参加の機会を与えていただきました
メンバー企業のマネージャの皆様、ありがとうございました

これからも当研究会をよろしくお願いします

ご清聴ありがとうございました