2016年度
企業リスクマネジメント研究会活動報告

2017年4月19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. 2016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

2010年度

- ● リスクマネジメントの研究

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
～
2016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～2016年
- ■ 情報セキュリティ1 （技術/体制）
- ■ 情報セキュリティ2 （ポリシー/ガバナンス）
- ■ BCP

企業リスクマネジメント研究会の概要（2016年度募集案内）

【研究会概要・方針】

本研究会では、健全な企業活動を阻害するリスクの中から研究対象を選び、その**リスクに対する**各企業の取組み状況や、**企業の枠を超えた取組みの可能性**について研究・情報交換します。

【研究内容案】

①サイバーセキュリティ　（新型攻撃対応、脆弱性情報収集、脆弱性監査、CSIRT、人材育成　等）

②事業継続　（自然災害、パンデミック、サイバー攻撃等の有事の際の運用継続・コミュニケーション手段、BCP策定・運用　等）

③セキュリティガバナンス　（セキュリティ・ポリシー、内部犯行防止、国内外グループ会社統制、改正個人情報保護対応、リスクアセスメント手法　等）

【参考】The Global Risks Report 2017

～ 世界経済フォーラムの資料より ～

The Global Risks Landscape 2017

出典 ： http://www3.weforum.org/docs/GRR17_Report_web.pdf

Global Risks of Highest Concern for Doing Business (Japan)

自然災害

サイバー攻撃

重要情報インフラの故障

データの不正利用/窃盗

	Risk	Share
1.	Natural catastrophes	65.5
2.	Cyberattacks	58.6
3.	Fiscal crises	57.8
4.	Interstate conflict	40.5
5.	Terrorist attacks	37.1
6.	Deflation	29.3
7.	Energy price shock	26.7
7.	Extreme weather events	26.7
7.	Critical information infrastructure breakdown	26.7
10.	Failure of financial mechanism or institution	25.0
11.	Failure of national governance	19.0
12.	Misuse of technologies	14.7
13.	Asset bubble	11.2
14.	Data fraud or theft	7.8
14.	Failure of climate-change mitigation and adaptation	7.8

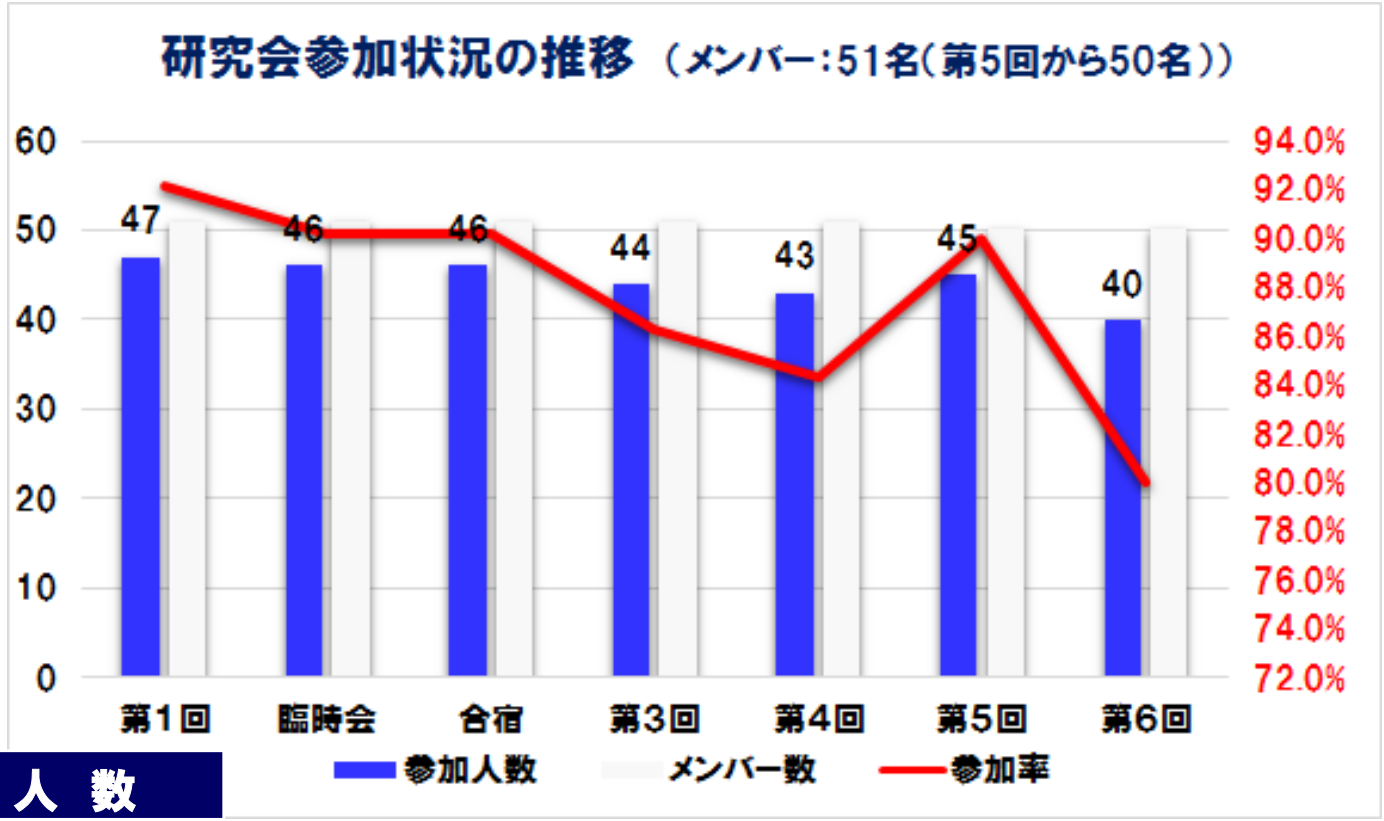
出典 ： http://reports.weforum.org/global-risks-2017/global-risks-of-highest-concern-for-doing-business-2017/#country/JPN

この数字は何でしょう？

87.6%

研究会(全体会)の参加率

メンバー皆様のご理解／ご協力のおかげで高参加率を維持することが出来ました。



ステータス	人　数
新規	29名
継続	20名
復帰	2名

メンバーが3つの分科会に分かれて活動

感謝

JUAS

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）
- 内職もOKです

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

2016年度　全体会
活動報告

2016年度研究会全体会スケジュール

	日時	場所	テーマ
第1回定例会 ＊交流会	2016年05月27日(金) 16:00 ～ 18:00 定例会 18:00 ～ 19:00 交流会	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回定例会 ＊合宿	2016年07月22日(金)～ 2016年07月23日(土)	静岡県沼津市	• グループ活動 (295分) • 各グループからの事例発表 (25分/分科会) • ゲスト講演 BPO/SI会社 (60分) • グループ活動年間計画発表 (10分/分科会)
第3回定例会	2016年09月02日(金) 16:00 ～ 18:00	JUAS2階 2-2会議室	• 事例発表(情報システム子会社) (30分) • ゲスト講演 日本サイバー犯罪対策センター (60分) • 活動状況報告 (6分/分科会)
第4回定例会	2016年11月11日(金) 16:00 ～ 18:00	JUAS2階 2-2会議室	• 事例発表(密封装置製造業) (30分) • ゲスト講演 セキュリティソリューション会社 (60分) • 活動状況報告 (6分/分科会)
第5回定例会	2017年01月13日(金) 16:00 ～ 18:00	JUAS2階 2-2会議室	• 事例発表(大手旅行業) (30分) • ゲスト講演 JPCERTコーディネーションセンター (60分) • 活動状況報告 (6分/分科会)
第6回定例会 ＊交流会	2017年03月03日(金) 16:00 ～ 18:00 定例会 18:00 ～ 19:00 交流会	JUAS2階 2-2会議室	• 活動の振返り(良い点・改善点 など) (40分) • 活動結果発表 (20分/分科会) • JUAS事務局からのご挨拶 • まとめ

2016年度　分科会A
（サイバーセキュリティ）
活動報告

2016年度研究会分科会Aスケジュール

	月日	場所	補足
1	6月13日	JUAS	合宿の発表内容、分科会活動内容確認
2	7月22日～ 7月23日	沼津	事例発表：「CDNは万能か？」 ディスカッション：運用体制（人的） CSIRT演習（ランサム対応）
3	8月18日	JUAS	事例発表：「サイバーセキュリティインシデント対応事例と課題」 ディスカッション：旅行業界のインシデントの読み解きと対応について
4	9月2日	JUAS	事例発表：「ISMSグローバル展開とGDPRについて」
5	10月20日	御成門	事例発表：「自社作成での標的型攻撃メール訓練」 ディスカッション：教育、トレーニング、エンドポイント製品について
6	11月11日	JUAS	ディスカッション：「内部犯行25のマトリクス」
7	12月16日	JUAS	ディスカッション：検証、予算確保
8	1月13日	JUAS	事例発表：「オリンピック準備について」 ディスカッション：セキュリティこれまでとこれから
9	3月3日	JUAS	まとめ

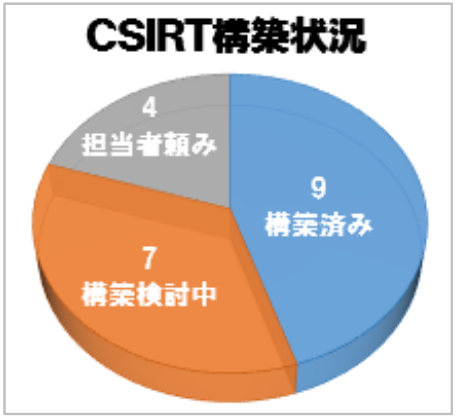
分科会Aの研究成果 ～ CSIRT運用体制・演習 ～

構築のきっかけは？

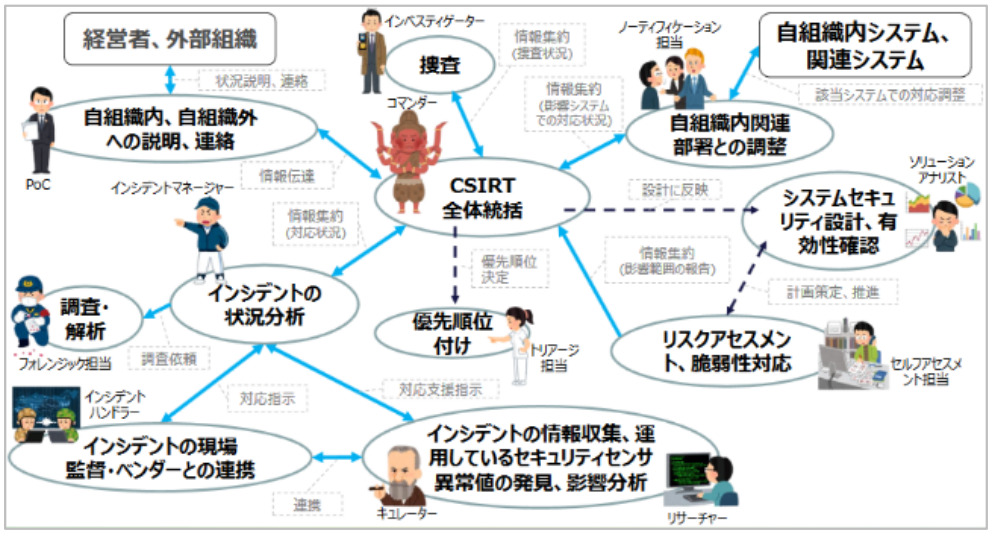
攻撃を受けての対策、
トップダウン　etc・・・

誰がサービス遮断を決断するか？

CISO、CSIRT、実担当、
ビジネスオーナー　etc ・・・



CSIRT機能（役割）図



出典：http://www.nca.gr.jp/activity/imgs/recruit-hr20170313.pdf

【シナリオ（基礎編）】

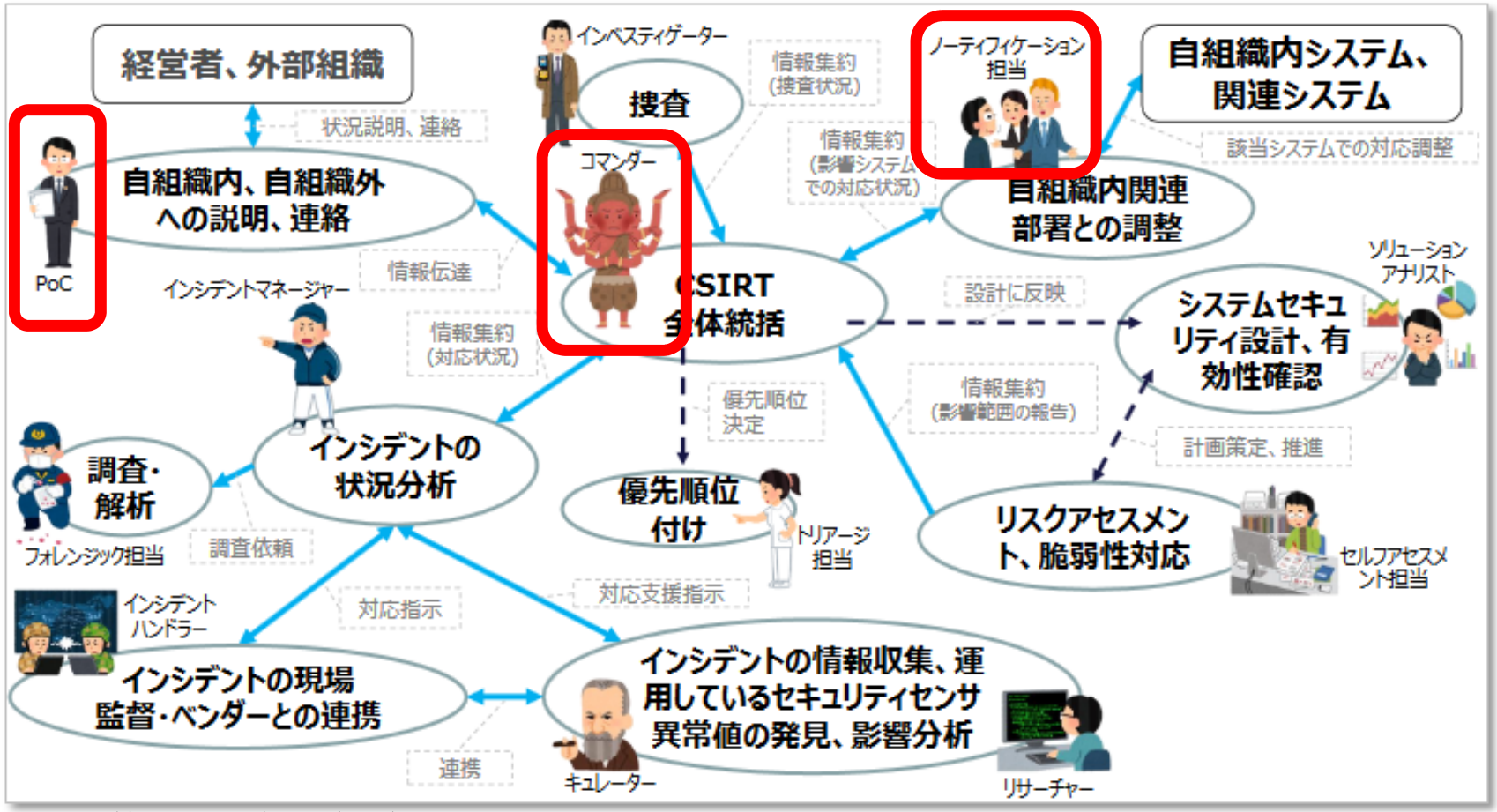
① 脆弱性情報を入手した場合
② DOS、DDOSのようなサービス妨害を受けた場合
③ 不正コマンド（SQLインジェクションなど）をインターネット側から受信した場合
④ 自組織内に不審な添付つきのメールが着信したとの情報を得た場合
⑤ 自組織外から自組織を名乗ったウィルスメールが着信したとの報告を受けた場合
⑥ 自組織の環境がランサムウェアの被害を受けたとの報告を受けた場合
⑦ 自組織の端末から不審なサイトへの通信を観測した場合
⑧ 自組織のWebページが改ざんされて、ウィルスが仕込まれていると報告を受けた場合

【シナリオ（応用編）】

⑨ 外部から顧客情報を入手したとの情報を受けた場合
⑩ お客様から知らない間にマイルが減算されているとの情報を受けた場合
⑪ 自組織の社員と思われる人物がSNSに内部情報を書き込んでいるとの通知を受けた場合
⑫ あるサーバで実行エラーが通知され、通常使われていない機器からの実行だった場合

分科会Aの研究成果 ～ CSIRT演習を通じた気付き ～

- 日頃のコミュニケーションが重要！（平常時の関係性が有事に及ぶ）
- PoC、ノーティフィケーション、コマンダーは自社要員で！（後は外部リソース活用も可）



出典：http://www.nca.gr.jp/activity/imgs/recruit-hr20170313.pdf

分科会Aの研究成果 ～ ディスカッション ～

	月日	場所	補足
1	6月13日	JUAS	合宿の発表内容、分科会活動内容確認
2	7月22日～ 7月23日	沼津	事例発表：「CDNは万能か？」 ディスカッション：運用体制（人的） CSIRT演習（ランサム対応）
3	8月18日	JUAS	事例発表：「サイバーセキュリティインシデント対応事例と課題」 ディスカッション：旅行業界のインシデントの読み解きと対応について
4	9月02日	JUAS	事例発表：「ISMSグローバル展開とGDPRについて」
5	10月20日	御成門	事例発表：「自社作成での標的型攻撃メール訓練」 ディスカッション：教育、トレーニング、エンドポイント製品について
6	11月11日	JUAS	ディスカッション：「内部犯行25のマトリクス」
7	12月16日	JUAS	ディスカッション：検証、予算確保
8	1月13日	JUAS	事例発表：「オリンピック準備について」 ディスカッション：セキュリティこれまでとこれから
9	3月3日	JUAS	まとめ

内部不正防止の基本原則

犯罪予防対策を5つに分類し、更に25の犯罪予防技術に細分化しています

犯行を難しくする（やりにくくする）	捕まるリスクを高める（やると見つかる）	犯行の見返りを減らす（割に合わない）	犯行の誘因を減らす（その気にさせない）	犯罪の弁明をさせない（言い訳させない）
対象の防御策を強化する	監視を強化する	標的を隠す（存在がわからない）	欲求不満やストレスを減らす	規則を決める
施設への出入りを制限する	自然監視を支援する	対象を排除する（存在をなくす）	対立（紛争）を避ける	指示を掲示する
出口で検査する	匿名性を減らす	所有物を特定する	感情の高ぶりを抑える	良心に警告する
犯罪者をそらす	現場管理者を利用する	市場を阻止する	仲間からの圧力を緩和する	コンプライアンスを支援する
情報機器やネットワークを制限する	監視体制を強化する	利益を得にくくする	模倣犯を阻止する	薬物・アルコールを規制する

出典 ： https://www.ipa.go.jp/files/000057060.pdf

対策の考え方

【その気にさせない／あきらめさせる】

A ＜ B+C

A ＝ 不正をすることによる犯罪者側の利益
B ＝ 不正をするための犯罪者側のコスト
C ＝ 不正が発覚した場合にうける犯罪者側のダメージ

【法人側の費用の考え方】

X ＞ Y+Z

X ＝ 実施しない場合に失うコスト
Y ＝ ソリューションや規約などの導入、実施コスト
Z ＝ 監視・業務運用コスト

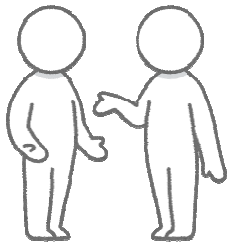
ディスカッション内容

- 何かあったときに実名公表するか？

  一部企業のみ公表、以外は公表しないで対処のみ

  実名公表は抑止力として効果はあると思うが、日本企業？はなかなか公表しない
- システムでの抑止はどこも行っているが、本当に“やる人”はかいくぐってやるのでシステムで止める事は難しい。
- 外資系は雇用契約で縛ってるので、あまりシステムでの抑止はしていない。

  ログ取得しているので何かあった時は調査して罰を受ける事になる
- RMSの導入を検討している
- 高権限者に関しては対策を取る必要がある



2016年度　分科会B
（事業継続）
活動報告

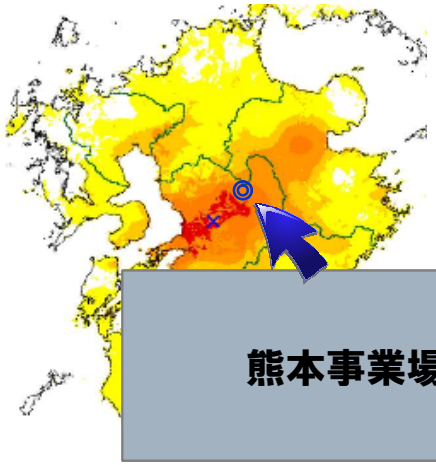
2016年度研究会分科会Bスケジュール

「現場」を見たり「生の声」聴くことで「身になる体験」を行うことが最も効果的と考える。

	月日	場所	補足
1	6月13日	JUAS	合宿の発表内容、分科会活動内容確認 事例発表： 1件
2	7月22日～ 7月23日	沼津	事例発表： 4件
3	9月2日	JUAS	事例発表： 1件
4	10月21日～ 10月22日	熊本	熊本事業場見学（製造）
5	11月11日	JUAS	事例発表： 1件
6	12月2日～ 12月3日	神戸	スーパーコンピューター「京」見学 データセンター見学（損保）
7	1月13日	JUAS	事例発表： 1件
8	2月10日	JUAS	事例発表： 1件
9	3月3日	JUAS	事例発表： 1件 まとめ

現場視察（熊本）

被災した工場を訪問し、震災に直面した現場の方々の生の声を拝聴し、知見を広げる。



熊本事業場

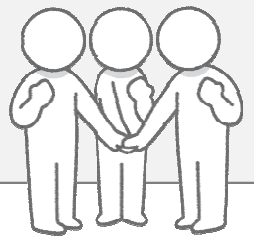
視察の様子

【スケジュール】

- 熊本地震の現場対応の説明
  - 地震の被害状況
  - 復旧対応／システム対応
- 工場見学
  - 復旧後の生産設備

【学んだこと】

- 大きな制約、限られたリソースの中で、“企業責任”を果たすために何をするべきか、現場が判断して動いた。
  - 本部の指示を無視したわけではなく、マニュアルに書けない所を柔軟に対応した
  - BCP対策として足りなかった部分を現場から意見を発信することにより迅速に解決した
  - 自社のリソース不足をグループ他社に補ってもらえるように動いた



現場視察（神戸）

セカンダリサイトの裏方見学と、特殊なセンター「京」のリスク対策を確認し、知見を広げる。

スーパーコンピュータ “京”

セカンダリサイト

【スケジュール】

- スパコン「京」の見学
  - 建物説明（免震構造etc）／サーバ見学
  - 事業内容説明（システム運用、活用方針）
  - 2020年次世代 ”京” 事業について
- セカンダリーサイトの見学
  - 建物説明（免震、発電室、プリント室 etc）

【学んだこと】

- 基本10人前後で、CPUの温度管理などの運用管理がしっかりしている（「京」）
  - ➢ 負荷分散は自動運転
  - ➢ サイバー攻撃は毎日受けている（これまで侵入を許したことはない）
- すごい少人数でのオペレーションを実現している。（有事の時この人数で完遂したらヒーローか！？）
  - ➢ エナージェンシーガスによる消火システム／72時間以上連続稼動可能な自家発電用燃料の確保

事例発表から学んだこと

- **各社のBCP対策状況**
  - BCP規程・基準・初動対策等の書類は完備
  - 安否確認に関しても導入済み（全体、個別）
  - 複数拠点を想定した準備も対応
  - 基本的なマニュアル、実施ガイドは作成済
  - 訓練も1回/年～複数回/年と実施している

- **バックアップセンターとの同期タイミングに関する考え方**
  - 1日のトランザクション量に応じて同期タイミングを決める　etc.
  - リカバリーポイントに関する考え方

- **全社的な啓蒙、教育について**
  - eラーニングでの教育はあるが、十分か？　（頻度、実地訓練の必要性）
- **災害時の参集ルールについて**
  - 誰がいつ出社するのか（～km県内の人、部長以上など）

2016年度　分科会C
（セキュリティガバナンス）
活動報告

2016年度分科会C活動スケジュール

14テーマについて事例紹介／ディスカッションすることが出来た。

	月日	場所	補足	
1	6月13日	JUAS	合宿の発表内容、分科会活動内容確認	
2	7月22日～ 7月23日	沼津	事例発表： 事例発表： 事例発表： 事例発表：	「当社グループにおけるウィルス感染事例を振り返って」 「CSIRTの取り組み」 「グループ会社のセキュリティ対策統制・ガバナンス」 「情報セキュリティ事象のその後」
3	9月2日	JUAS	事例発表： 事例発表：	「モニタリング」 「情報セキュリティ基準、規程、ルール、および体系」
4	10月14日	JUAS	事例発表：	「ASP／クラウド活用時のセキュリティ」
5	11月11日	JUAS	事例発表：	「社員教育」
6	12月9日	JUAS	事例発表： 事例発表：	「IT部門の人材育成について」 「情報セキュリティ検査（監査、システムの点検）」
7	1月13日	JUAS	事例発表： 事例発表：	「グループ統制－ 国内、海外のグループ会社の統制」 「当社における再発防止策の実施状況について」
8	2月3日	JUAS	ディスカッション：	メール （送受信ルール、フィルタリング、訓練　など）
9	3月3日	JUAS	ディスカッション： まとめ	スマートデバイス（利用ルール、紛失時対応　など）

社員教育（意識向上）のベストプラクティス？

1. 情報セキュリティ指導情報（月次）
   ポスター掲示は “トイレ” が効果的！！

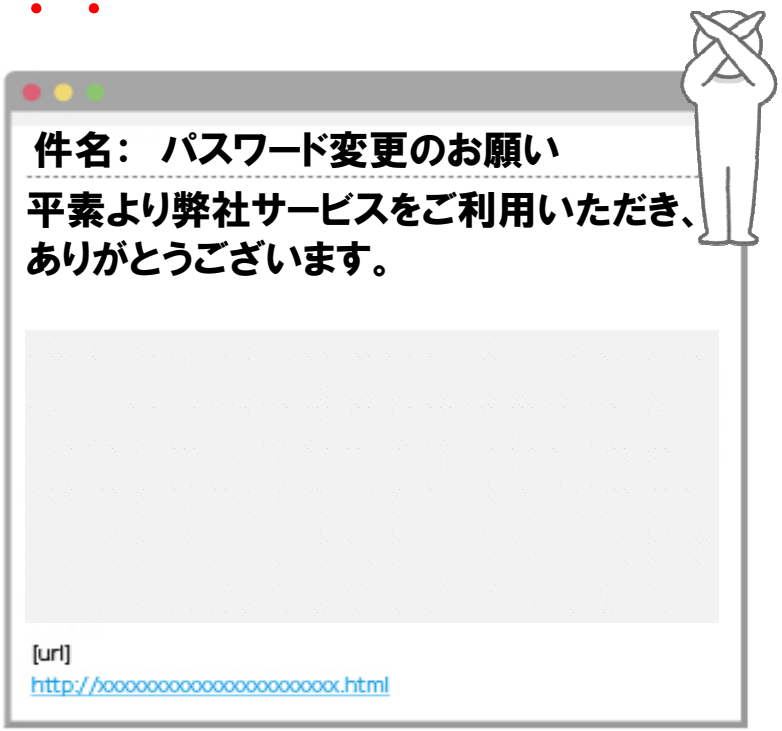
2. 標的型攻撃メール対応訓練（不定期）
   “パスワード”関連の模擬メールの利用価値“高”！！

3. 情報セキュリティ推進会議（年2回）

4. インターネット利用状況調査（適宜）

5. 若手システム社員交流会（入社10年目以内！）

6. 集合研修時の指導（階層や状況に応じて）



まとめ

2016年度活動の振り返り

- 他社事例をいろいろ聞けた、共有できた
  最新事例や悩みの共有、リアルな情報交換、異業種の方との意見交換

- 意見出しの雰囲気作りができた　（初心者でも判り易かった、参加しやすかった）
- 資料、演習が有用だった
  （CSIRT、セキュリティ温故知新、内部犯行、標的型分析結果等々）
- 外部講師聞けて良かった（JC3、JPCERT、etc…）
- 宿題がなかった（負担が少なくて良かった）
- 分科会間の交流があったほうがいい。 外に行きたい

- 金曜日開催に賛否両論(曜日を分散してもいいかも)
- Web会議も出来たらよい
- 自社へのフィードバック、目標管理できたのか

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