2017年度
企業リスクマネジメント研究会活動報告

2018年4月26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. 2017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マネジメント）
   - 分科会C（情報セキュリティ）
   - 分科会J（情報セキュリティ）
3. まとめ

企業リスクマネジメント研究会の歴史と概要

JUAS 一般社団法人 日本情報システム・ユーザー協会
Japan Users Association of Information Systems

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（2018年版より）

セキュリティ・センター
・プライバシーマーク審査・認証
・認定個人情報保護団体
・情報セキュリティ推進センター
（調査・研究・交流）

政策研究・調査

調査事業
・企業IT動向調査
・ソフトウェアメトリックス

JUASアカデミー
関西アカデミー

JUASコミュニティ
・ワークスタイル改革コミュニティ
・JUAS ITGC（女性技術者研究会）
・デジタル化戦略コミュニティ★

会員活動

フォーラム
CIOエグゼクティブフォーラム（１）
IT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）
グローバルフォーラム

関西支部
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

研究会
ビジネスデータ研究会
ITインフラ研究会
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投資ポートフォリオ研究会
組織人材育成研究会
組織力強化研究会
サービスデザイン実践研究会
AI研究会★
エコシステム研究会
デジタル化研究会
ダイバーシティ＆インクルージョン研究会
クラウド活用研究会★

アドバンスト研究会

研究プロジェクト

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
JUASラボ

グローバルクリエイティブフォーラム

公開事業
サマースクエア
JUASスクエア

JUAS

企業リスクマネジメント研究会の歴史

企業情報マネジメント研究会

企業リスクマネジメント研究会

2006年度
～
2010年度
2011年度

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

● リスクマネジメントの研究
- 情報管理
- 法務
- BCP

● 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）

無事、12年目を完了させることが出来ました

企業リスクマネジメント研究会

2013年度
～
2017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～2017年
- 情報セキュリティ1（サイバーセキュリティ）
- 情報セキュリティ2（CSIRT/ガバナンス）
- BCP

企業リスクマネジメント研究会の概要（募集要項）

【研究会概要・方針】

本研究会では、企業におけるリスクマネジメントについて有識者や参加企業の取り組みを基に、自社への適用や提言、企業の枠を超えた取組みの可能性について研究・情報交換をします

【研究内容案】

① サイバーセキュリティ（若干技術的話題多め）
② 事業継続計画（BCP・データセンターなど）
③ 情報セキュリティマネジメント（セキュリティに関して幅広く）

研究会活動を通じて・・・

①新しい情報・知識・考え方を持って帰りましょう！
②情報交換・意見交換できる仲間・コミュニティを一緒に作りましょう！

【参考】 世界の経営者が考えるビジネスリスク

～ 「Risk Barometer 2017」(Allianz社)より ～

順位		
1	事業中断	サプライチェーン、ディストリビューション
2	市場動向・価格変動	急上昇
3	サイバーインシデント	情報漏洩・DDoS攻撃
4	自然災害	台風・津波・地震
5	法律・規制の変更	改正個人情報保護法
6	マクロ経済動向	トランプ政権
7	ブランド価値の失墜	直接・間接の原因がある
8	火災	倉庫火災もありました
9	戦争・テロ	グローバルでのリスク
10	窃盗・詐欺・汚職	犯罪リスク

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

この数字は何でしょう？

90%

研究会(全体会)の参加率=90%

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。

	日付	人　数	参加率
第1回	5月25日	55名	98%
合宿	7月21日-22日	56名	100%
第3回	9月14日	49名	88%
第4回	11月17日	48名	86%
第5回	1月19日	44名	79%
第6回	3月9日	50名	89%
平均			90%

ステータス	人　数
新規	34名
継続	19名
復帰	3名

メンバーが4つの分科会に分かれて活動しました

感謝

研究会での成果を上げる工夫

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

- 議論しやすい雰囲気作り！

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
- 各自の目線で自由な意見交換（業種、職責に拘わらず）
- 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
- ノウハウ・アイデアを共有し、各社の対策に役立てる！

研究会のルール

“ Chatham House Rule ”ってご存知ですか？

"When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed".

王立国際問題研究所（イギリス）に源を発する、会議参加者の行為規範

当該会議で得られた情報を利用できるが、その情報の発言者やその他の参加者の身元および所属に関して秘匿する（明示的にも黙示的にも明かにしない）義務を負うというルール。（出典 ： Wikipedia）

と、言うわけで “成果ドキュメント” は有りません・・・

と，言う訳にはいかないので・・・

2017年度　活動報告

「全体会」の活動報告

2017年度研究会：6大講演会

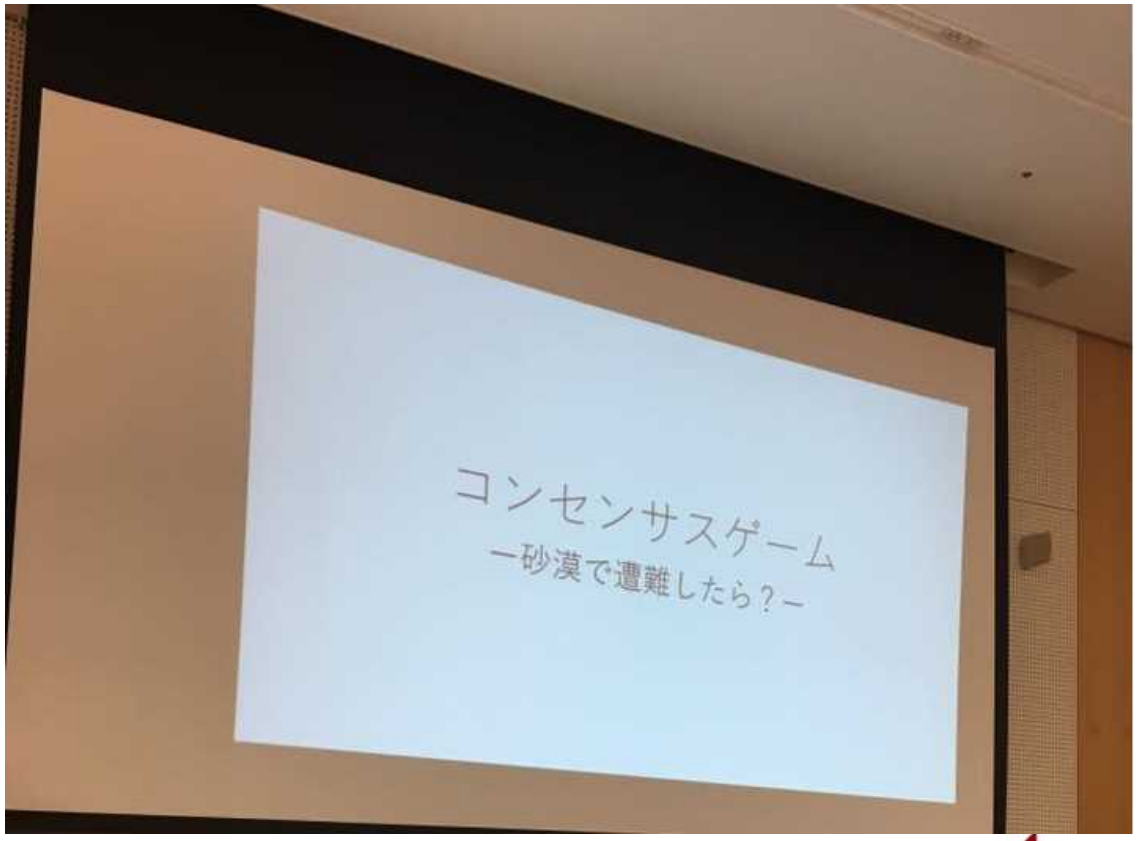
	日時	テーマ　（案）
第１回	5月25日（木）	• 情報交換会と宴会形式情報交換会
第２回 合宿	07月21日（金） ～7月22日（土）	• 大宣ｼｽﾃﾑｻｰﾋﾞｽ　石橋様 「ｴﾝﾄﾞﾎﾟｲﾝﾄ･ｲﾝﾃﾘｼﾞｪﾝｽ、IoTセキュリティ最前線」 • 中電ｼｰﾃｨｰｱｲ　永野様 「SOC立上げから見えた現状と課題」 • インテル　糀原様 「CISSP 受験体験記」
第３回	９月14日（木）	• ANAシステムズ　阿部様 「CSIRT構築後の次の一手」
第４回	11月17日（金）	• アクセンチュア　吉丸様 「震災から６年、改めて考えるエネルギーと事業継続」
第５回	１月19日（金）	• マカフィー　Mr. Scott Jarkoff 「Threat Intelligence 」※英語講演
第６回	3月09日（金）	• 情報交換会と宴会形式情報交換会

“コンセンサスゲーム”にチャレンジ（合宿）

アイスブレイク／チームビルディングにとても役立ちました！

砂漠に飛行機が不時着した!! 最も近くの町まで１１０Km 気温４３度
飛行機から持ちだせた荷物から、生き残るために最も重要な物は何か？
４名のチームで議論して選ぶゲームです。

＜飛行機から取り出せた物＞
・懐中電灯と乾電池
・2リットルのウォッカ
・化粧用の鏡
・本「食べられる砂漠の動物」
・落下傘の絹布
・銃弾入りの４５口径ピストル
などなど



2017年度　分科会A
（サイバーセキュリティ）
活動報告

2017年度分科会A 研究テーマ

①WannaCryマルウェア解析報告
②CASBについて（クラウドサービス利用時のセキュリティ）
③インシデント対応フローについて
④私物端末の業務利用におけるセキュリティ要件
⑤不審メールへの対応とクラウド利用について
⑥レピュテーションリスクとリスク調査方法について
⑦ログ保管期限に関するディスカッション
⑧自社のサイバー攻撃状況と対策
⑨標的型攻撃メール訓練
⑩グローバルでのセキュリティ統制

WannaCryマルウェア解析報告

マルウェアの解析環境、解析方法、外部の専門業者との連携方法など

【解析のトリガー】
・ニュースで報道されるようなウイルスの調査はどのレベルまで実施するか？
－検体を収集して、自社で解析
－セキュリティ専門会社から最新の情報を入手する
－JUASの仲間との情報交換により情報を入手する
－一般公開されている情報を収集する。

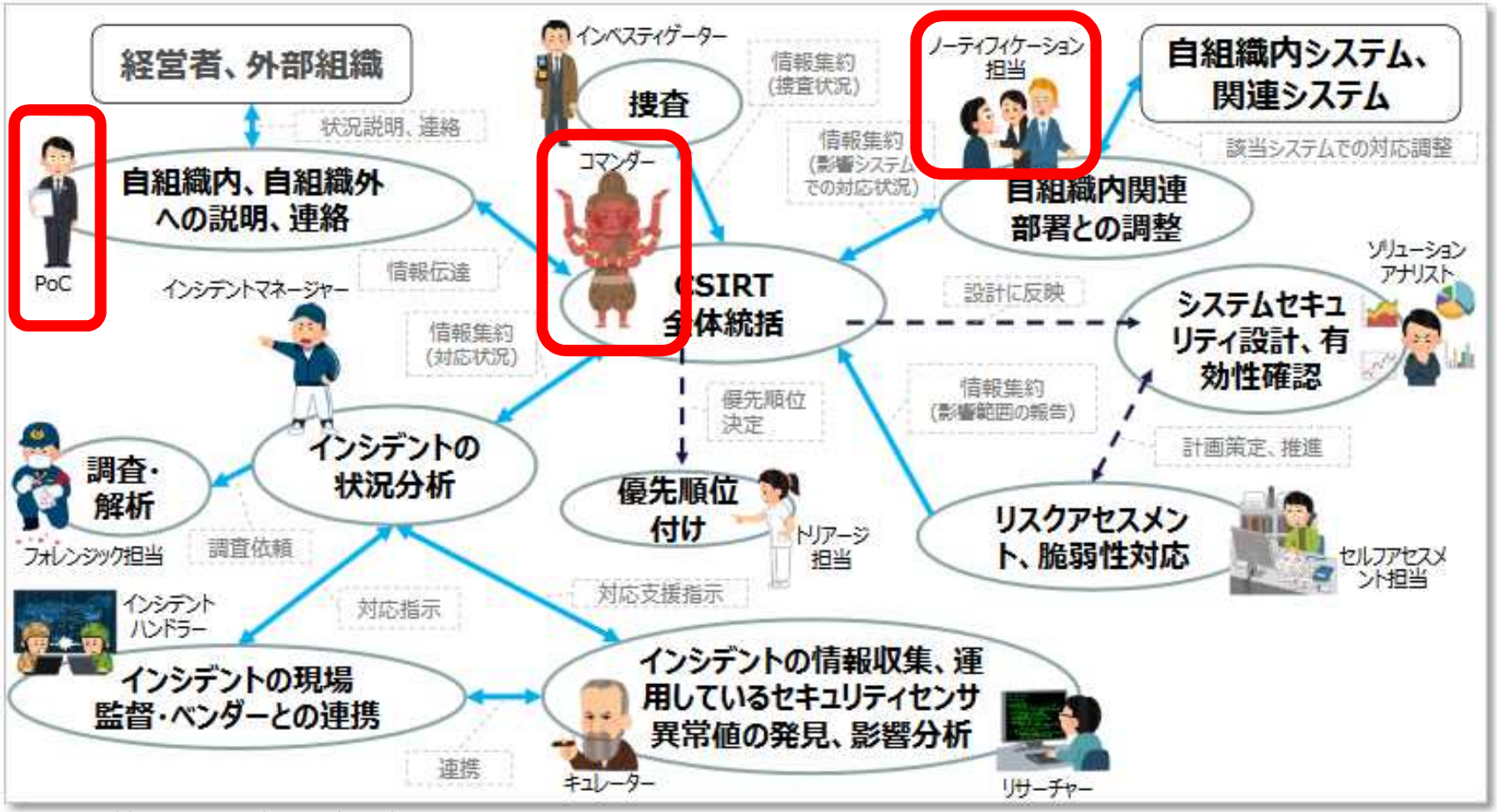
【解析環境】
・自社で解析環境を持つ会社による、解析環境と解析方法（実例）の紹介

【WannaCry対応時の課題への議論】
・OSのパッチ適用状況の確認方法

・土日にインシデントが発生し、月曜日にパソコン起動前に、情報を伝える手段

インシデント対応フロー ～ CSIRTメンバーの役割 ～

- 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

ログ保管期間

セキュリティに関連するログの保管期間について

【収集するログ】
・ネットワーク系ログ、サーバアクセスログ、ウイルス検知ログなど
【保管期間】法令等拠り所を決めて各社の判断で実施
・NISTのガイドライン（通常運用時）
１－２週間：低位影響レベルのシステム
１－３か月：中位影響レベルのシステム
３－１２か月：高位影響レベルのシステム
・IPAのログ保管実態調査
１か月：刑事訴訟法（通信履歴を30日保管）
３か月：サイバー犯罪に関する条約
１年間：PCI DSS方針/NISC方針
１８か月：EUデータ保護法
３年間：不正アクセス禁止法違反の時効
・分科会調査（上記より長期保管する場合を調査）
７年間：税務調査でデータ調査の可能性のある期間

標的型攻撃メール訓練

訓練方法、訓練の目的、訓練時の課題について

【実施方法】
- ツールを購入して、訓練実施を内部メンバーで対応
- 訓練メールの内容にリアリティを持たせる
- 新人や派遣社員の訓練機会を増やす

【効果測定】
- 開封率は目安。低いほうがよいが、ゼロにはならない
- 不審なメールを受信した際の通報制度
- 開封してしまった場合の報告率を計測
- 訓練後にアンケートを取るのも有効

【訓練ではなく、実際にウイルスをクリックした場合の対処】
- パソコンの隔離（有線LAN,無線LAN）
- OS起動時の実行プログラムの確認、ブラウザヒストリの確認
  レジストリの修正内容の確認など

2017年度　分科会B
（BCP）
活動報告

2017年度分科会B 研究テーマ

◆自社事例を紹介し、分科会全員でディスカッション

①事業継続計画／災害対策
②災害対策（データセンター／バックアップ）
③有事の際の運用、コミュニケーション手段
④企業（法人）間連携（自助／共助）

災害対策

東日本大震災1ヵ月後の現地視察状況（震災直後の写真を見て、当時を振り返る）

- 防災を考えるのか？減災を考えるのか？
  - 被害を出さないようにする「防災」の実現は難しい
  - 被害を最小限に抑える「減災」を考える
- 防波堤の扉を閉める人が亡くなった
  - 危険な仕事こそ人手ではなく自動化が必須
- 電力の優先供給契約はおまじないみたいなもの
  - 人命優先が実状
- 当時、輪番停電の対象となり、業務影響が出た
- 平穏な日常の中で忘れてしまうが、決して忘れてはいけないこと

有事の際のコミュニケーション手段

有事の際の運用、コミュニケーション手段について

- コミュニケーション手段は、現在も電話・メールか？
  - PC・NW利用可能を前提とし、外部から接続して業務を実施
  - NW利用不可を前提とし、衛星回線。しかし、有事の際は繋がり難い印象
    - MCA無線は繋がるが、ユーザーが増えたため使用時間帯が限られる
    - アマチュア無線は繋がるが業務利用はNG
  - 安否確認を実施するが社員のみ。システム稼動には協力会社メンバーも必要
  - マニュアルでは災害対策要員が集合して対応想定だが、支援メンバーは必要

災害対策訓練

定期的な災害対策訓練の実施について

- 災害対策訓練実施の目的
  - 実効性の担保
  - 理解を深めて役割明確化
  - 従業員間の連携・協力
- 各社で実施している訓練の例
  - 緊急連絡網
  - 安否確認
  - 代替システムへの切替、バックアップシステムからの復旧
  - システム部門外を含めた全体訓練
  - 人・物・金の動きの初期確認作業
  - 初動～1ヶ月後までのシュミレーション訓練（期間は半日）
  - マニュアルの作成でとどまり訓練は未実施

データセンター　現場から学ぶ

データセンター見学

- FRTデータセンター
  - ファーストライディングテクノロジー株式会社（沖縄電力子会社）が運営
  - 沖縄の優位性、沖縄国際情報通信ネットワーク
- 沖縄データセンター
  - 沖縄県による公設民営型のデータセンター
  - 沖縄データセンター株式会社（株主は地元企業16社）が運営
- 明治安田生命セカンダリサイト
  - 外部センターの活用

2017年度　分科会C
（情報セキュリティマネジメント）
活動報告

2017年度分科会C 研究テーマ

①CSIRT構築、セキュリティ体制構築、CISO設置
②CSIRT運営、外部セキュリティベンダ活用
③モバイル環境のセキュリティ、スマートデバイス活用ルール
④クラウド活用、SNS活用、評価ルール
⑤情報セキュリティ基準、規程、ルール、および体系
⑥内部不正対策、情報漏えい対策
⑦情報セキュリティ教育・訓練・演習（エンドユーザ向け）
⑧情報セキュリティ事故の対応事例
⑨海外法規（EUのGDPR;中国サイバーセキュリティ法等）対応
⑩ランサムウェア対策

モバイル環境に対応したセキュリティルール

モバイル環境・スマートデバイス利用ルールについて議論

◆社外から社内環境へのアクセスは限定的
VPNで社内ネットワークに接続して利用
利用できるサービス：
メール確認、勤務管理、経費/旅費申請、全社掲示板閲覧など
TV会議システムとスケジューラはクラウドサービス利用
→ 仮想デスクトップ環境で社内と同じ環境を許しているところも

◆在宅勤務を開始
子育て・介護支援目的で事前申請により許可

◆課題
いつでも、どこでも作業可能＝＞労務管理上の整理が必要
BYOD活用＝＞国内では、あまりメリットを感じない企業が多い
海外では自前で用意させる場合が多い

クラウド活用時のルール

クラウド環境の利用が増加し、様々な課題について議論

◆クラウドファースト
SaaS ＞ PaaS/IaaS ＞ 仮想サーバ ＞ オンプレミス

◆クラウド利用時のルール
利用する場合はIT部門へ申請
チェックツール（はい/いいえで答える52項目の質問）で確認

◆クラウドサービスのセキュリティ評価
セキュリティリスク調査に加えて、トラフィックが過大にならないか？も評価

◆課題
申告なしで使われても分からない、利用終了してもそのまま
→クラウド利用状況を可視化したい（CASB・・・）
取引先の要請で社内では利用不可としているサービスも使わざるを得ない

セキュリティ人材育成

セキュリティ人材の育成方法について議論

◆体制・役割は各社様々
メンバーは兼務がほとんど
一部を外部へ委託するのは一般的
→ いざという時動いてもらうチケット制の外部サービスを契約
ISMS運営体制にてインシデント対応
CSIRTの守備範囲（ちょっとした事象から取り扱う、重大事象に限定）

◆課題
24H・365日対応ができていない、レスポンスを早期化したい
見える化・常日頃からの情報発信が弱い
メンバーのモチベーション維持が必要
→ 外部セミナー参加、NCAの活動参画などで刺激を受ける
→ 情報処理安全確保支援士など資格はコストがかかる

内部不正対策

内部不正への対策について議論

◆内部不正対策は利用制限が主
外部からの脅威対策は技術的な対策を取る
内部不正に対しては厳しい利用制限で対応

◆内部不正を防ぐ点　＞　利便性
クラウドサービスは、原則利用禁止
（許可された場合も厳しい利用条件）
PCは机固定、社内での持ち運びも原則不可
会議資料は紙を利用し、使用後にシュレッダーで廃棄
特権ユーザもできることを厳しく制限・管理
※特権ユーザに必要以上の権限を与えやすくなる点への対応

2017年度　分科会 J
（情報セキュリティマネジメント）
活動報告

2017年度分科会J　研究テーマ

①標的型メール訓練について
②グループ会社統制・ガバナンス
③情報セキュリティ自己点検
④情報セキュリティ事故対応
⑤脆弱性診断・ペネトレーションテスト
⑥CSIRT構築・運営
⑦SIEM構築・運用/MSS利用事例
⑧情報セキュリティ規程・ルール
⑨セキュリティ保険
⑩情報セキュリティ脅威情報の収集

脆弱性診断

脆弱性診断(プラットフォーム診断とWebアプリ診断)について

◆実施時期
- システムの運用開始前に実施
- 毎年定期的実施

◆診断後の対応
- 診断結果のレベルによって対応の判断が必要

◆課題
- 対応後の再診断のコスト
- Webアプリの脆弱性診断はコスト・時間が必要

情報セキュリティ規程・ルール

情報セキュリティ規程・ルールについて

◆規程
- セキュリティポリシーの下に、規程、規則及び細則
  遵守状況に関する議論

- グループ会社や海外のグループ会社への展開について

◆情報資産管理
- 管理対象の選定
- 登録済機器と未登録の機器の識別方法
- 管理方法（インベントリ情報収集、現物確認の棚卸など）

セキュリティ保険

セキュリティ保険について

◆保険の補償内容
・毎年、補償内容の改訂がある。
補償内容（メインの補償とオプションの補償）の確認

◆活用判断
・自社のリスク・脅威を想定し、事故発生時の被害を想定
保険により補償できる範囲・金額を確認

・グループ会社や海外のグループ会社への展開について

◆課題
・判断には、一般的な保険の知識が必要

脅威情報の収集

情報セキュリティに関する脅威情報の収集について

◆公開情報
- セキュリティベンダーのサイト、ブログ
- IPA,JPCERT等
- 有識者のSNSなど
- 講習会、セミナーなど

各社の情報源を共有した

◆入手した情報の対処
- どの情報を、誰に、エスカレーションするか？
  分類、判断基準に検討が必要

◆情報共有の仕組み
- 業界ごとのISAC
- JUAS研究会のメーリス利用

まとめ

2017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。メーリスを有効活用できた。
  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）
- 現地視察（データセンター見学など）で、「見る」ことの重要性を実感した
- 外部講師の話が聞けて良かった
- 宿題がなかった（ノルマ・負担が少なくて良かった）
- 分科会間の交流を増やしたい
- もう1－2回開催しても良い。関西での開催希望

- 自社へのフィードバックが少なかった（深堀するテーマも選定したらどうか？）
- 合宿は沼津以外を希望
- Jフェス（当発表会）と次年度募集時期の日程を入れ替えて欲しい

2017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