2018年度
企業リスクマネジメント研究会活動報告

2019年4月18日

部会長　伊藤　吾朗（鹿島建設株式会社）

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. 2018年度活動報告
   - 全体会
   - 分科会A（情報セキュリティ：技術系）
   - 分科会C（企業リスク：BCP、セキュリティ）
   - 分科会J（情報セキュリティ：マネジメント系）
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（2019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）

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PARK（１）

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
システム開発・保守QCD研究会
ソーシャル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
U35・次世代ITとキャリアを考える研究会★

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

情報セキュリティ研究会
2012年度

企業リスクマネジメント研究会
2013年度
～
2018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

無事、13年目を完了させることが出来ました

●サイバー関連
- BCP（石橋）

●企業リスクマネジメントの研究

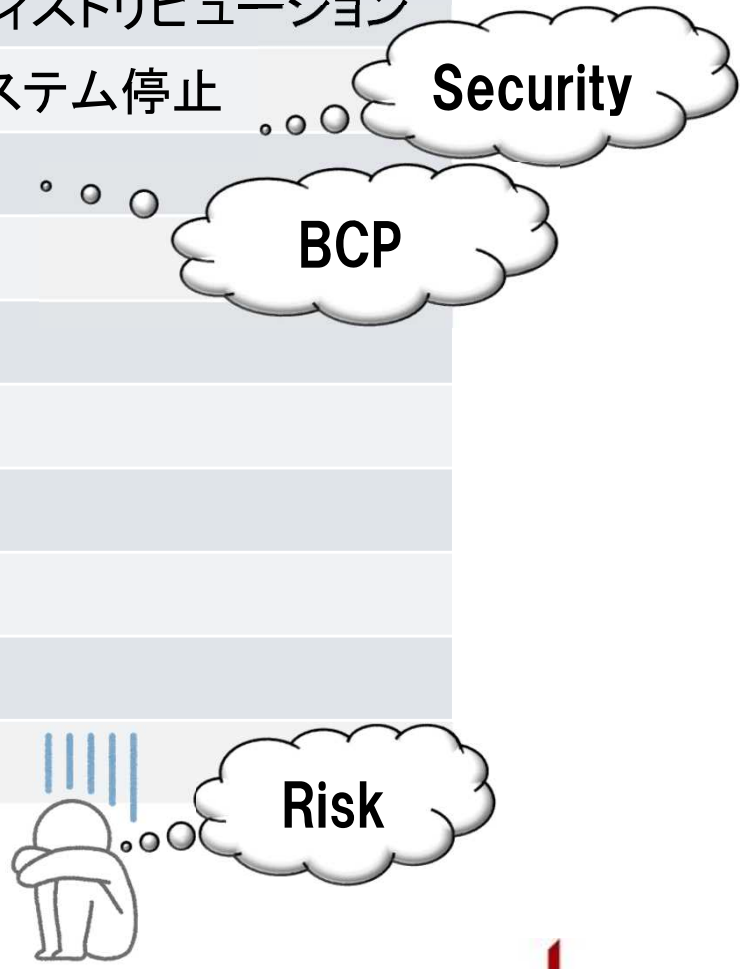
2013年度
- 情報セキュリティ
- 個人情報、スマホ
- BCP

2014年度～2018年
- 情報セキュリティ（サイバーセキュリティ）
- 情報セキュリティ（CSIRT/ガバナンス）
- BCP

【参考】 世界の経営者が考えるビジネスリスク

～「Risk Barometer 2018」(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	サイバーインシデント	情報漏洩、破壊、システム停止
3	自然災害	台風・津波・地震
4	市場変革	新規参入・企業買収
5	法律・規制の変更	GDPR
6	火災・爆発	工場・倉庫火災
7	新技術	AI, IoT
8	企業ブランド価値の損失	評判、SNSリスク
9	政治的リスクと暴力	戦争・テロ
10	気候変動	災害リスク



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

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。また、各分科会ではそれぞれの研究テーマについての研究・議論・情報交換をします。本研究会は、若手の方や女性の活躍を応援します。

【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 情報セキュリティマネジメント（事業継続リスク含めて幅広く）

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！

リスクマネジメントの研究方法＝＞発生したリスクへの対応

方法１：リアルなリスクの共有

- 実際に発生したリスク、実施した対策を共有する。

方法２：実施した対策に関する検証　＋　有識者による講演

- もっと良い対処方法はあるのだろうか？
- こんな対応はどうでしょうか？
- 予防方法はどうしたらよいか？
- 再発防止策はこれでよいのか？

方法３：現実に発生するその他事象の共有

- とは言っても予算が無いし・・・
- 対応する体制・人材もいないし・・・

情報共有のための「研究会の重要なルール」

“ 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）

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/災害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！

2018年度　活動報告

「全体会」の活動報告

2018年度研究会：5大講演会

	日時	テーマ
第１回	5月２３日（水）	• 情報交換会
第２回 合宿	07月20日（金） ～ 7月２１日（土）	• ＪＡＬインフォテック 坂様 「ビジネスメール詐欺への対策について」 • フィナンシャルシステムプラン株式会社 石橋様 「セキュリティ人材とテクノロジーの有り方」
第３回	９月14日（木）	• ANAシステムズ 阿部様 「インシデント対応の現場から」CSIRT小説「側線」
第４回	11月17日（金）	• クラウドネイティブ　齊藤様 「働き方改革とリモートワーク セキュリティアプローチの最低限とその先」
第５回	１月17日（木）	• 活動の振り返り
第６回	3月09日（金）	• テクマトリックス 佐山様 「AIはセキュリティ対策に有効か」 • 情報交換会

「分科会」の活動報告

分科会活動

グループに分かれてディスカッション

【グループ】
- 分科会A （情報セキュリティ：技術系）
- 分科会C （企業リスク：BCP、セキュリティ）
- 分科会J （情報セキュリティ：マネジメント系）

【ディスカッション方法】
- 毎月分科会を開催し、ディスカッション
  ※全体会開催月は、全体会の前に分科会実施。
- 担当者は、自己紹介と事例紹介
- 全員でディスカッション

2018年度　分科会A
（情報セキュリティ）
活動報告

2018年度分科会A 研究テーマ

①基本的なセキュリティ対策に関するディスカッション
②Box/Office365利用時のセキュリティ対策
③脆弱性情報の収集と社内システムへの反映
④管理対象外機器のセキュリティ対策
⑤スレットインテリジェンス活用事例
⑥業務パソコン持ち出し時のセキュリティ対策
⑦標的型攻撃メール訓練
⑧セキュリティアセスメントと資産管理
⑨国内グループ会社に対する情報セキュリティガバナンス
⑩セキュリティインシデント対応体制の構築

基本的なセキュリティ対策のディスカッション

テーマごとに利用ツールを中心としたディスカッション実施

【実施概要】
・基本的なセキュリティ対策について、各社で利用しているツールの紹介を中心に、メリット、デメリット、課題の共有を実施。

【テーマ】
・不正アクセス対策(FW/IDS/IPS/WAFなど)
・メールセキュリティ対策
・エンドポイントセキュリティ対策(ウイルス対策、EDRなど)
・サーバの資産管理、セキュリティ対策
・脆弱性診断
・他社との情報共有手段、海外拠点管理、GDPR対応などなど

※最初のテーマとして、自己紹介的に実施。自由に意見交換しました。

Box/Office365利用時のセキュリティ対策事例

クラウドサービスを自社のインフラとして利用する場合のセキュリティ対策事例

【概要】
・自社のインフラとして、BoxとOffice365を導入することになった。
利用状況を監視するために、専用のSIEMを構築した事例を共有。

【セキュリティ対策のポイント】
・クラウドサービスへのアクセス管理を実施
・セキュリティ要件にもとずき、取得すべきログを選定。
・専用SIEM環境の構築
・監視内容、監視方法について

【ディスカッション】
・クラウドサービスのアクセスログの違い・特徴
・クラウド環境の設定情報、アクセス権管理について
・CASBの利用について

脆弱性情報の収集と社内システムへの反映

社内システムの刷新にともない、脆弱性情報収集とシステムへの反映が課題となった

【実施体制と課題】
- 脆弱性情報収集担当の役割
  複数のリソースから脆弱性情報を収集し、システム担当者へ周知
- システム担当者の役割
  脆弱性情報を確認し、対応要否を判断
- 課題
  システム担当者側は、脆弱性情報の対応要否確認に時間がかかる

【セキュリティ対策のポイント】
- 社内システムの構成情報を管理するシステムを構築
- 登録されたシステム情報、バージョン情報を元に、対応すべき脆弱性情報を選定。
- 対処すべき脆弱性情報のみ通知される

【ディスカッション】
- 機能名などのマッチングについて
- 脆弱性情報のシステムへの連携について

管理対象外機器のセキュリティ対策

部署で個別に導入する機器へのセキュリティ対策について

【発生事象】
・不審な通信を検出。
調査した結果、デジタルサイネージのSTB(セットトップボックス)が
仮想通貨マイニングウイルスに感染していた。

【デジタルサイネージ(電子掲示板)の利用】
・部署毎に管理。社内システムへの接続が無い。
通信機能(STB)は、サービス業者側の設備
・導入にあたって、IT部門orセキュリティ担当部署への確認、報告はない。

【対処】
・デジタルサイネージ、WEBカメラ、スマートグラスなどなど、いわゆるパソコン
スマートデバイスと異なり、管理対象外機器導入時のガイドラインを周知
・管理外機器についても、新規導入の場合は、申請して許可を得ること。

リスクアセスメント事例

スレットインテリジェンスを活用したリスクアセスメントの実施事例の紹介

【実施事例】
・ドメインとキーワードを提示し、ダークウェブ等の脅威情報への漏洩度を評価

【実施効果】
・メールアドレスをもとに、アドレス、パスワードなどの漏洩状況
・企業や技術キーワードを元に、自社、業界に関する攻撃事例やリスク情報

【ディスカッション】
・リスクが判明しても、攻撃方法は不明なため、対策がたてにくい
・費用対効果について

2018年度　分科会C
（企業リスク／BCP：セキュリティ）
活動報告

2018年度分科会C 研究テーマ（その1）

①CSIRT構築、セキュリティ体制構築、CISO設置
②情報セキュリティポリシー、規程、ルール、および体系
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グループ会社、海外子会社ガバナンス
⑤情報セキュリティ教育・訓練・演習
⑥国内・海外法規（個人情報保護法、民法改正、EUのGDPR、
　中国サイバーセキュリティ法、等）への対応
⑦セキュリティ対策製品導入・活用事例（SIEM、CASB、EDR）
⑧ RPA、AIなど新技術(?)とセキュリティ

2018年度分科会C 研究テーマ（その2）

⑨BYOD、在宅勤務対応
⑩退職者の情報持出し、内部不正対策
⑪クラウド活用、SNS活用、評価ルール
⑫制御系セキュリティ
⑬BCP対策・事例
⑭災害対策（データセンター運用・予備系構築）

在宅勤務

各社の事例をもとにディスカッション

【実施形態】
- 育児・介護の目的に限定／申請すれば、誰でも可能
- シンクライアント、USB型シンクライアント、社給PC＋テザリング用iPhone

【ディスカッション】
- 規程
  - 勤務実績の把握、休日・深夜の作業制限など
  - 作業場所は自宅に限定など
- 作業環境
  - 社給機器利用か、個人所有機器か
  - 通信方法（社給、個人）
  - 印刷不可、データのダウンロード不可など
- ガイドライン
- 健康管理（歩かなくなると・・・）

※外資系企業：パソコンは必ず持ち帰る。自宅での会議参加はマスト。

BYOD

各社の事例をもとにディスカッション

【実施形態その１】
・夜間や休日のシステム障害への対応
自宅や外出先でもシステム障害状況を確認できる環境を整備
個人所有のスマートフォン上でセキュアブラウザーを利用して、社内システムの障害状況を保管したクラウドサービスを閲覧する。
オペレーションは、現地常駐スタッフへ電話で指示。

【実施形態その２】
・夜間や休日の震災発生時の安否確認
個人所有のスマートフォンを活用して、安否情報を収集する。

【課題】
・利用ツールや利用内容を規定する。通信料の負担、会社機器貸与、シャドーITの防止、SNSなどでの業務情報拡散の防止など
・ウイルス対策、紛失時の対応

退職者の情報持出し

内部不正対策をもとにディスカッション

【課題】
・退職者、退業社（派遣契約）の情報持出しへの対策

【対策内容】
・誓約書、規程
・監視していることの周知や罰則の明示（抑制効果）
・退職日から6か月前までのパソコン操作ログを保管（検証）

【課題】
・退職日までに操作ログを確認することが困難（莫大なログ）
メールは、退職前挨拶なども多くなる・・
・点検は「疑い」から始まるので、作業モチベーション維持が難しい
・メール、ファイル転送サービス、オンラインストレージ利用も確認が必要
・Bluetooth、DirectWiFiの通信監視
・「紙情報」は意外と・・・

クラウドサービス活用

クラウドサービス活用時のリスク対策をディスカッション

【実施事例】
- クラウドサービス利用時は申請書を提出

【審査内容】
- 利用目的、どのような情報が格納されるか？
- クラウドサービス側のサービスレベル確認、CASBでのレピュテーションなど
- 接続制限（IPアドレス制限、端末認証など）、認証の強化

【課題】
- 審査に時間がかかる
- 利用開始時のみ、その後の利用者拡大、利用機能拡大などに対応できない
- シャドウITを防げない
- サーバ設置場所（国内、米国、その他）による判断

制御系セキュリティ

工場のセキュリティ対策をもとにディスカッション

【課題】
・重要インフラ１４業種では、インフラへのサイバー攻撃対策として
制御系システムのセキュリティ対策が要請されている。

【工場などの制御系セキュリティ】
・基礎となる情報が不足している。
製造現場、工場における、ネットワーク、情報機器の構成図を作成

【課題】
・外部との接続箇所が明確になった。
接続箇所には、FW／IPSを設置
・機器の保守などで、外部の業者が制御系ネットワークへ機器を接続
・USBメモリなど外部メディアの接続の有無確認
・対策コストはどこの部署が負担するのか？

BCP関連リスク

各社の災害対策をもとにディスカッション

【各社事例】
- ISO 22301 事業継続マネジメントシステムの取得について
- 継続すべき事業の選定について
- 想定するリスクと被害規模算出について
- バックアップセンターについて
  被災時の切替訓練
- 震災想定の事業継続訓練

【課題】
- 災害の多様化：大雨、津波など
- 属人化の排除（手順書など）
  重要システムのパスワードは・・・
- 人の問題
  対応にあたって方の対応スキルに依存する・・・

2018年度　分科会J
（情報セキュリティマネジメント）
活動報告

2018年度分科会J 研究テーマ（その1）

①セキュリティインシデント対応／対応訓練

②社外公開WEBサイトのセキュリティ対策

③不審メール対策と従業員対応能力向上

④2020東京大会に向けてのセキュリティ対策

⑤脆弱性マネジメント

⑥サプライチェーン・外部委託先管理

2018年度分科会J 研究テーマ（その2）

⑦ベンダーサポート切れソフトの対応

⑧海外出張者/赴任者向けのセキュリティ対策とその課題

⑨紙媒体による情報漏えい対策

⑩情報セキュリティ基準、規程、ルール、および体系

⑪セキュリティ統制、ガバナンス（国内／国外）

⑫ISMS認証取得、および維持運営（ISO27001）

社外公開WEBサイトのセキュリティ対策

社外公開WEBサイト（運営サーバ）のセキュリティ対策について議論

◆社外公開WEBサイト設置時のガイドライン
構築方法、運営方法に関するガイドラインを公開
公開前の審査方法、部署独自運用の公開サーバの管理方法

◆情報管理
公開する情報の審査方法（広報や管理部のチェック）
公開サーバ上のファイルの情報管理区分・個人情報の有無など

◆運用後のセキュリティ診断
ペネトレーションテスト、定期保守（OSなどのアップデート）

標的型攻撃メール訓練

標的型攻撃メール訓練のノウハウや課題について議論

◆実施目的
開封率の低減
不審なメール受信時の報告率
開封した場合の対処
開封した通知を受けた場合の初動対応

◆対象者
経営層／新入社員／派遣契約社員／年齢別／問い合わせ受付部門など

◆実施頻度／事前周知の有無／事前教育・事例紹介の有無

◆訓練メールの文案の決め方
やりとり型メールでの訓練

◆スマートデバイスで受信した場合

外部委託先管理

サプライチェーン・外部委託先管理について議論

◆委託先審査

業務遂行能力、事業継続性、反社会的勢力との関連、情報セキュリティ対策
個人情報保護対策など
情報セキュリティ対策はチェックシート提出を依頼するケースも

◆課題

再委託先の管理
申請内容の妥当性確認・監査実施の依頼
情報セキュリティ対策などで、基準に満たない項目があった場合の対応
（猶予期限・チェックのみ・基準に満たない場合は委託しないなど）
委託先が、社内でパブリックなクラウドサービスを利用している場合の対応
メールアカウントがフリーメールの場合（個人経営の企業など）

セキュリティ監査

国内グループ会社・国外グループ会社へのガバナンスについて議論

◆実施状況

チェックシートによる点検、現地での監査

海外グループ会社の場合は、チェックシートやIT計画書の提出

ローテーション、他の監査と合わせて実施など

◆統制対象

出資比率

ネットワークの共用

異業種のグループ会社／会社規模（人数）によっては対象外など

◆課題

会社の規模によっては、本社と同一の対策がとれないケースも・・

自社にIT人材がいないため、改善対策に時間がかかる

他国の場合は、法制度、文化の違い

チェックシートの場合、チェック判断の妥当性・基準の同一性など

まとめ

2018年度活動の振り返り（メンバーの意見）

- 他社事例をいろいろ聞けた、共有できた。チャタムハウスルールのおかげ。
  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）
- もっと少人数での議論もよいかも
- １回１テーマもよいが深堀もしたい
- 他の分科会との交流もしたい。（最終回に急遽１回実施）
- 合宿は沼津以外を希望（あくまでも個人の感想です）
- 関西開催や遠征への出張費が課題

2018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のスタッフの皆さま！

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