2019年度
企業リスクマネジメント研究会活動報告

2020年4月16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. 2019年度活動報告
    - 全体会の活動
    - 分科会の活動
        - 議論したテーマ
        - 研究概要
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（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
～
2019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、14年目を完了させることが出来ました

●サイバー関連
- BCP

●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～2019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

～ 優先して着手が必要と思われるリスク（デロイトトーマツによる調査）より ～

順位		
1	自然災害	地震・風水害
2	法令順守違反	モラル
3	人材不足	情報セキュリティ人材
4	情報漏洩	不正アクセス・メール誤送信
5	製品・サービスの品質	
6	サイバー攻撃・ウイルス	脆弱性・標的型攻撃
7	過労死・長時間労働	
8	価格競争	
9	システムダウン	クラウドサービス・サイバー攻撃
10	法改正への対応	GDPR

出典 ： https://www2.deloitte.com/jp/ja/pages/about-deloitte/articles/news-releases/nr20180131.html

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】

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。

本研究会は、若手の方や女性の活躍を応援します。

【研究テーマ案】

サイバーセキュリティ、IoTセキュリティ、リスクマネジメント

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！

リスクメン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）

★研究会メンバーは、「チャタムハウスルール＝鉄の掟」を遵守して、円滑なコミュニケーションを実施しています。

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、即時に、各社の対策に役立てる！

2019年度　活動報告

「全体会」の活動報告

2019年度研究会：活動スケジュール

	日時	場所	活動内容
第1回定例会 ＊交流会	2019年05月23日(木) 16:00 ～ 18:00 全体会 18:00 ～ 19:00 交流会	JUAS2階 2B 会議室	・研究会方針 ・自己紹介 ・研究テーマ検討
第2回定例会 ＊合宿	2019年07月05日(金)～ 2019年7月06日(土)	静岡県沼津市	・ゲストによる講演①、② ・分科会活動 ・グループ事例発表・活動内容
第3回定例会	2019年09月12日(木) 16:00 ～ 18:00	JUAS 2B 会議室	・事例発表(研究会メンバー) ・ゲストによる講演③ ・活動状況報告
第4回定例会	2019年11月15日(金) 16:00 ～ 18:00	JUAS 2B 会議室	・事例発表(研究会メンバー) ・ゲストによる講演④ ・活動状況報告
第5回定例会	2020年01月16日(木) 16:00 ～ 18:00	JUAS 2B 会議室	・事例発表(研究会メンバー) ・シャッフル分科会 ・活動状況報告
第6回定例会 ＊交流会	2020年03月06日(金) ⇒ 4月8日(木)へ延期 ⇒ 中止	JUAS 2B 会議室	・活動の振返り(良い点・改善点 など) ・活動結果発表

2019年度研究会：4大講演会

	日時	テーマ
第1回 合宿	7月5日（金）	• ニュートンコンサルティング 石井様 「オリパラリスクとサイバーセキュリティ」
第2回 合宿	7月6日（土）	• フィナンシャルシステムプラン 石橋様 「セキュリティ担当が知っておきたいニッチなセキュリティ領域と予算管理」
第3回	9月12日（木）	• ANAシステムズ 阿部様 「事故を起こさないための活動とサプライチェーンの管理」
第4回	11月15日（金）	• クラウドネイティブ　齊藤様 「ID認証とデバイス認証および機密データアクセスへの信頼性検証について」

「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：技術系多め）
- 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：マネジメント系多め）

【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

2019年度　分科会
議論したテーマ

2019年度分科会A 主な研究テーマ

①セキュリティ情報収集について
②クラウドサービスのチェックについて
③AWS導入時のセキュリティ対策について
④メール訓練・ユーザ教育について
⑤セキュリティパッチ適用について
⑥脆弱性対応管理について
⑦WEBセキュリティについて
⑧オリンピック・パラリンピック対応
⑨制御系セキュリティについて
⑩シャドウIT対策について

2019年度分科会C 主な研究テーマ

①クラウド活用と評価・審査
②グループ会社、海外子会社ガバナンス
③サプライチェーン管理、海外子会社のガバナンス
④災害対策（データセンターの運用）
⑤BCP／事業継続
⑥情報セキュリティポリシー、ルール
⑦BYOD，在宅勤務、働き方改革
⑧情報セキュリティ教育・訓練・演習
⑨インシデント事例・インシデント対応
⑩モバイル環境、スマートフォンのセキュリティ対策

2019年度分科会J 主な研究テーマ

①会社経営幹部へのセキュリティの重要性の伝え方について
②情報セキュリティガバナンス強化の取り組み
③ビジネスメール詐欺の事例と対策
④情報セキュリティ教育、セキュリティ規程基準の構築、運用
⑤サプライチェーンマネジメント関連
⑥外部委託時のセキュリティ対策
⑦働き方改革に必要なセキュリティ
⑧ CSIRT／SOCの構築運営
⑨ユーザーID／パスワード管理
⑩クラウドサービス利用時のセキュリティ
⑪サポート切れOSへの対応。延命策

2019年度　分科会
研究概要

分科会 研究概要

各分科会で議論した内容の一部を掲載いたします。

概要掲載テーマ	
・リスク管理体制の構築	・脆弱性情報の収集と対応
・情報セキュリティのガバナンス強化	・サポート切れOSへの対応
・情報セキュリティ監査	・IoTセキュリティ
・サプライチェーンマネジメント	・制御系セキュリティ
・外部委託先管理	・退職者の情報持出しリスク対策
・クラウドサービス活用	・BCP（事業継続）
・在宅勤務	・オリパラリスクへの対応
・ビジネスメール詐欺への対策	

リスク管理体制の構築

会社経営幹部へのセキュリティの重要性の伝え方について

◆方法

取締役会、経営会議などでの定期報告（年1回/半期1回）
CISOへの定期報告（年1回/半期1回）

◆報告内容

セキュリティ対策やセキュリティインシデント発生状況を報告
技術的観点／管理的対策でのセキュリティ推進の実施状況
セキュリティ事象に関する主なリスクへの（脅威・事象）対策　など

◆報告時のポイント

KPI（Key Performance Indicators）やKRI（Key Risk Indicators）の活用
リスクの発生頻度や被害額を想定して報告

情報セキュリティのガバナンス強化

情報セキュリティガバナンス強化の取り組みについて

◆観点について

ルール・規程、体制,人材,仕組みの観点から対策を検討。
重点テーマ(イベント)をあげて、それぞれの観点を検討。

◆統制の単位

グローバル(地域単位) もしくは、会社単位

◆リスクの把握と対応計画の策定

セキュリティ機器のログを分析。複数機器のログの相関分析。
コンサルタントによるレビュー
チェックリストやヒアリングによる確認
顕在化した事象の分析

◆ガバナンスの強化

ベースラインの設定(パッチ適用率、パスワード規則など)
自己点検→ヒアリング→評価→対策。PDCAサイクルを回す
　改善が数値で表現できると、モチベーションアップにつながる

情報セキュリティ監査

国内グループ会社・海外グループ会社に対する監査について

◆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、他の事項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（この場合は必須）
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、文化の違いがある
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

サプライチェーンマネージメント

サプライチェーンマネジメント関連

◆サプライチェーンの形態

製造業など：部品の生産、組み立てなど、工程を通じて、多数の企業が
連携するケース
サービスの提供にあたり、協力会社と連携して対応する。
支店／本社、グループ会社との連携

◆課題

子会社であれば、
　情報セキュリティ遵守事項を共通化して、守らせることが可能。
契約関係であると、
　契約前に基準を提示して、遵守していることを契約条件とする。

サプライチェーン管理（グループ会社）

グループ会社／海外子会社のリスク管理について

◆実施内容

ISO38500（ITガバナンス）の活用
IT計画書による情報共有（年１回）
　同時に、「調査票」を添付して、追加のヒアリングや点検を実施
海外では、情報セキュリティ審査規定をグループ会社へ適用義務付ける

◆関連事項

クラウドサービスの利用については、本社への申請が必要
スマートデバイスについても、各社運用方法を本社側で詳細にチェック

◆課題

グローバル、もしくはグループ会社間でどこまでITインフラを共有するか？
小規模の会社への対応
GDPRなど各国の法制度への対応

外部委託先管理

外部委託先管理について

◆委託先審査項目

業務遂行能力、事業継続性、反社会的勢力との関連調査、
情報セキュリティ対策、個人情報保護対応など
情報セキュリティ対策や個人情報保護対応はチェックシート提出を依頼

◆課題

委託先の状況の確認方法：書類審査、インタビュー、訪問審査
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
委託先の情報セキュリティポリシーが、自社と異なる場合
　BYOD、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）
再委託先の管理について

クラウドサービス活用(1/2)

クラウドサービス活用時のリスク対策

◆審査方法

クラウドサービス利用時は申請書を提出

申請書をIT部門または情報セキュリティ管理部門/シーサートへ提出

◆審査内容

<利用者側への確認>

利用目的、どのような情報が格納されるか?(情報の秘匿性)

個人情報、特定個人情報の保存の有無

利用部署の管理体制(従来のサーバ管理と同等に扱う)

管理者アカウントの管理、利用者アカウントの管理方法の確認

<クラウドサービス提供側の確認>

係争裁判所、データセンターの所在地(日本以外の場合の確認)

第三者委託の有無

クラウドサービス側の運用レベル(外部認証取得:ISMSなど、第三者監査、ペネトレーションテスト実施状況など)

接続制限(IPアドレス制限、端末認証など)、認証の強化、暗号化について

クラウドサービス活用（2/2）

クラウドサービス活用時のリスク対策

◆課題

申請件数が多い（処理しきれない）、時間がかかる
申請をせずに利用できてしまう（ホワイトリスト運用していない）
　シャドウITを防げない。クラウドサービスと知らずに利用しているケースも
NISCが準備している政府の調達基準は、マネージメント要素が強い
　中小規模のサービス提供元では基準に満たない
申請後に、他サービスとの連携機能などが追加され、チェック漏れが発生
審査時に許可しても、その後の運用・管理が適切に実施できているか
　監査できていない
利用部門、利用者へのクラウドサービスに関する啓蒙・教育が必要

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
震災対策として導入
手段：シンクライアント、仮想デスクトップ、社給PC＋テザリング用iPhone

◆ディスカッション

・規程関連
勤務実績の把握方法、休日・深夜の作業制限など
作業場所：自宅に限定／外出先・サードプレイスを認める場合もあり。
在宅勤務を増やすと評価が課題となる

・作業環境関連
社給機器利用が多い。個人所有機器利用禁止が多い
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

ビジネスメール詐欺への対策

ビジネスメール詐欺への対策

◆事例

会社経営層を騙る発信元からの振込先変更指示（電話を利用するケースも）
取引先を騙る振込先変更指示メール

◆詐欺が成立しやすい要素

国際取引の場合、相手方へメール以外の手段で連絡が取りにくい。
国際取引の場合、利用する言語の課題（母国語でない）もある。
メールアカウントが乗っ取られている場合、不審な点が見つけにくい。

◆対策

振込先変更の対応プロセスはメール以外の手段も必須とする。
「緊急」であっても、一人で判断しない。上司や管理部門と連携する。
詐欺の事例を周知し、リスクの感度を高める
添付ファイルのパスワード通知方法をメール以外の手段とする
返信時に、初めて利用されたメールアドレスが存在している場合警告を表示

脆弱性情報の収集と対応

脆弱性情報収集と対応について

◆体制と役割

・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

社内システムで利用しているOS，ソフトウエア情報の収集方法
　変更時の連絡、バージョン情報の正確な収集など
対処すべき脆弱性情報のみ通知される
　システム運用側では、リスクが判断できず、適用の時期の判断ができない
脆弱性対応の完了報告を受けているか？

サポート切れOSへの対応

サポート切れOSへの対応。延命策

原則は、サポート切れの前に移行すべきだが、延命せざるを得ない場合の対策

◆リスク対策の判断基準

インターネットに直接つながるネットワーク環境の場合は継続利用禁止
インターネットに間接的につながるネットワーク環境の場合は
　業務上の理由を勘案し、延命を許可する場合あり。
インターネットにつながっていない環境の場合は、
　業務上の理由を勘案し、利用部門の要望に対応する。
　※スタンドアロン環境で無い場合は、延命時のリスク対策を検討

◆延命時のセキュリティ対策

延命を許可した場合でも、リスク低減策の適用を検討する

例）**Windows Server 2008**

- Azure環境へ移行して、パッチ提供を受ける
- マイクロソフト社の有償のパッチ提供サービスを契約する
- 仮想パッチを適用し、ネットワークからの攻撃を防ぐ
- ウイルス対策ソフトは、継続サポートしているので、確実に利用する。等

IoTセキュリティ

IoTセキュリティについてディスカッション

◆事例

IoTシステムの事例は、「センサー」「GW」「クラウドサービス」の3層構造が多い

◆各種リスクについて

・センサー機器

正しい場所に設置されているか？（いつの間にか移動しているケースあり）
正しい情報を送信しているか？の確認方法
プロジェクト終了時の回収が難

・GW（ゲートウェイ）

情報保存の有無、暗号化、盗難防止対策
ファームウェアのバージョンアップ方法
通信の暗号化、クラウドサービス側でのGW識別方法

・クラウドサービス

一般的なクラウドサービスのリスクと同様

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

◆現状

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の課題

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

◆ディスカッション

現状の整理を実施すると、外部との接続箇所が明確になる。
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？

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（及び検証）

◆課題

退職日に合わせて、操作ログを確認することが困難（莫大なログ）
　メールは、退職前挨拶などで多くなる・・
検証は「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の通信監視も必要・・・
「紙情報」対策は・・・

BCP（事業継続）

BCP／事業継続に関するディスカッション

◆各社事例

BCMS（事業継続マネジメントシステム）の導入事例
事業継続リスク（自然災害、製品不良、情報漏洩など）の検討
想定するリスクと被害規模算出について
震災想定の事業継続訓練
従業員が持ち歩く「災害時の心得カード」について

◆課題

災害の多様化：大雨、津波など
属人化の排除（手順書の整備など）
　BCP用のシステムのパスワードの管理とアナウンス・・・
人の問題が大きい
　対応にあたった方の対応スキルに依存することが多い

オリパラリスクへの対応

オリパラに向けたリスクと対応について

◆想定すべきオリパラリスク

交通リスク（電車の乗車率や道路渋滞）・・・物流リスクもあり
海外からの持ち込み感染症リスク
首都圏のホテル確保難（東京への出張が難）
人材不足（大会スタッフ確保優先）・・・サイバーセキュリティ関連も影響あり
20億件以上のサイバーインシデントが発生するリスク

◆対策

脅威情報の収集により、リスクを早期に把握する
詐欺サイトや不審メールに関する訓練や教育の実施
在宅勤務の環境準備
インシデント発生時の対応体制の検討

まとめ

2019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
- もっと分科会間の交流をふやしても良い
- 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

2019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

以上

ありがとうございました

以上