2023年度
企業リスクマネジメント研究会活動報告

2024年4月1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. 2023年度活動報告
    - 活動概要
    - 全体会の活動報告
    - 分科会の活動報告
        - 議論したテーマ
3. まとめ

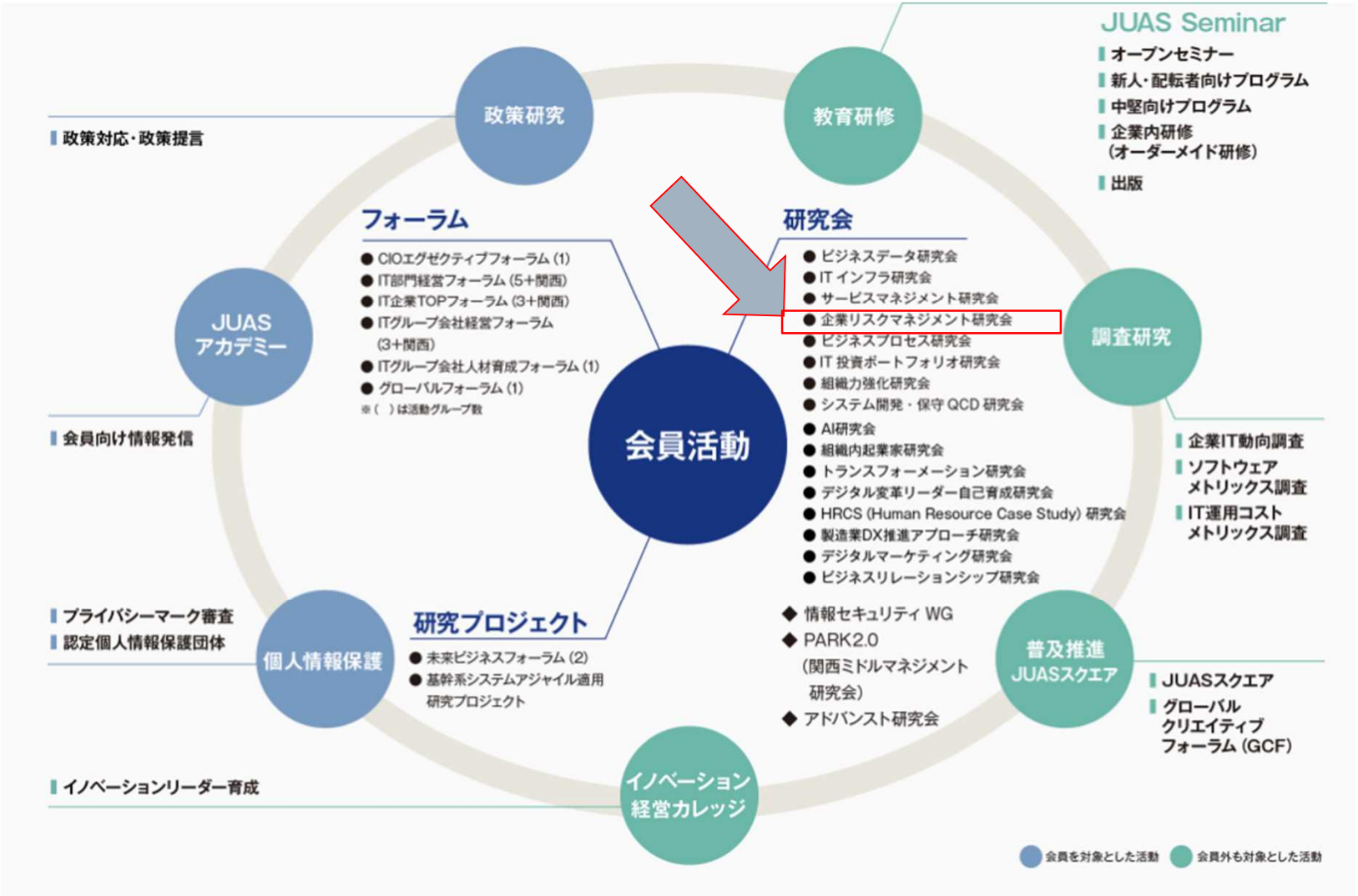
企業リスクマネジメント研究会の歴史と概要

1．企業リスクマネジメント研究会の歴史と概要

- 企業リスクマネジメント研究会とは

JUAS活動（2023年版より）

業種・業態の垣根を越えた会員活動



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
～
2023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

●サイバー関連
- BCP

コロナ禍を乗り越え、無事、18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～2023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

企業リスクマネジメント研究会の概要（募集要綱）

【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、情報セキュリティマネジメント

※BCP（震災対策・感染症対策）に関しても議論します

【対象者】

初心者・経験者・年齢・性別・職種を問わず

情報セキュリティ/リスクマネジメントについて関心が高い方

関連情報の収集や社外人脈を広げたいとお考えの方

リスクマメジメントの研究方法

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。
- 今直面している問題、検討している対処方法を共有する。

方法２：実施した対策に関する検証（分科会でのディスカッション）

- 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？
- このような対応をしたことがあります・・

方法３：有識者による講演と研究会全体のメンバー間での情報交換

- 有識者の知見の共有
- 様々な経験を持つメンバーの知見の共有

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」を遵守しています。

情報共有のための「研究会の重要なルール」

■ 当研究会では、「チャタムハウスルール＝鉄の掟」を遵守

★会議で得られた情報は利用できますが、
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は
秘匿します。

★「チャタムハウスルール＝鉄の掟」の遵守により、
リアルなリスクの共有・自由な意見の発信ができ、
円滑＆活発なディスカッションができます。

企業リスクマネジメント研究会とは

- **当研究会は、参加いただいたメンバーが、**
  今直面しているリアルなリスクについて、
  さまざまな視点でディスカッションしていきます。

  幅広い視点（業種、業務、世代など）で、
  自由に意見交換できるコミュニティです。

2023年度　活動報告

2023年度　活動報告

- **活動概要**
- 全体会の活動報告
- 分科会の活動報告
  - 議論したテーマ

2023年度　活動概要

活発な議論
復活!!

- **対面でのディスカッションによる活動**

コロナなど感染症対策を継続実施したうえで

対面会議のコミュニケーションを完全実施。

＝＞

オンライン会議のメリットもありますが、

対面のコミュニケーションにより

集中＆活発な議論、さまざまなメンバーの組み合わせ、

話題の発展など、研究会の満足度向上！

2023年度　活動概要：3つの取り組み

分科会：　10－15名でディスカッション（月１回開催）

- さまざまな業種・業務・役職・経験の融合。
- テーマを決めて、全員で議論、１回完結、宿題なし。
- テーマを事前に共有して、他の分科会への参加可能!!

全体会：　専門講師の講演＋各分科会の発表＋情報交換会

- 参加者の興味のあるテーマについての講演を開催
- 全体会開催日に分科会活動の概要共有や事例発表
- 情報交換会を開催して、メンバー間でのお悩み相談の場を提供

合宿・現地見学会・会社訪問：視覚・本物からの情報、メンバー間情報交換

- 合宿での集中した討議、見学会での新たな気づき

2023年度の参加企業

42社に参加していただきました。

企業名	企業名	企業名
株式会社ニッスイ	株式会社IHI	株式会社JALインフォテック
日本電気株式会社	株式会社読売新聞東京本社	コクヨ株式会社
JFEシステムズ株式会社	インテル株式会社	鹿島建設株式会社
NOK株式会社	不二サッシ株式会社	株式会社かんぽ生命保険
キリンビジネスシステム株式会社	SOMPOひまわり生命保険株式会社	イオン株式会社
第一三共株式会社	株式会社テプコシステムズ	日商エレクトロニクス株式会社
東日本旅客鉄道株式会社	日本プルーフポイント株式会社	株式会社LSIメディエンス
日揮ホールディングス株式会社	コニカミノルタ株式会社	かんぽシステムソリューションズ株式会社
前田建設工業株式会社	丸文株式会社	インフォテック株式会社
TDCソフト株式会社	アイエックス・ナレッジ株式会社	株式会社中電シーティーアイ
独立行政法人住宅金融支援機構	ヤマハ発動機株式会社	株式会社カジマアイシーティ
ファイルフォース株式会社	ニッセイ情報テクノロジー株式会社	日光ケミカルズ株式会社
ENEOS株式会社	第一生命情報システム株式会社	日本生活協同組合連合会
パーソルホールディングス株式会社	大王製紙株式会社	パーソルキャリア株式会社

ようこそ “企業リスクマネジメント研究会” へ

42名の皆様にご参加いただきました。

ステータス	人　数
新規	22名
継続・復帰	20名

幹事団の紹介

2023年度の幹事団です

【全体会】

- 部会長　伊藤　吾朗（鹿島建設株式会社）
- 副部会長　糀原　晃紀（インテル株式会社）
- 副部会長　長井　一広（不二サッシ株式会社）
- 副部会長　谷口　数実（日本電気株式会社）
- BAN　坂　靖史（株式会社JALインフォテック）

【分科会】

- 分科会N　分科会長　：　金子　様　（株式会社ニッスイ）
  副分科会長：　谷口　様　（日本電気株式会社）
- 分科会B　分科会長　：　奥村　様　（株式会社IHI）
  副分科会長：　新井　様　（株式会社読売新聞東京本社）
- 分科会J　分科会長　：　坂　様　（株式会社JALインフォテック）
  副分科会長：　松尾　様　（コクヨ株式会社）

2023年度　活動報告

- 活動概要
- **全体会の活動報告**
- 分科会の活動報告
  - 議論したテーマ

【参考】 世界の経営者が考えるビジネスリスク

～ 「Risk Barometer 2023」(Allianz社)より ～

順		
1	サイバーインシデント	システム停止、データ漏洩、データ破壊
2	事業中断	サプライチェーン、ディストリビューション
3	マクロ経済	世界的な景気後退リスク
4	電力危機	燃料費高騰、供給の混乱
5	法律・規制の変更	脱炭素化、持続可能性
6	自然災害	台風・津波・地震(損失額が巨大)
7	気候変動	災害リスク
8	熟練労働力不足	
9	火災・爆発	工場・倉庫火災
10	政治的リスク	紛争・暴力

Security

BCP

出典 ： https://www.allianz.com/en/press/news/studies/230117_Allianz-Risk-Barometer-2023.html

【参考】 情報セキュリティ10大脅威 2023

～ IPA 情報処理推進機構 より ～

順位	「組織」向け脅威	前年順位
1	ランサムウェアによる被害	1
2	サプライチェーンの弱点を悪用した攻撃	3
3	標的型攻撃による機密情報の窃取	2
4	内部不正による情報漏えい	5
5	テレワーク等のニューノーマルな働き方を狙った攻撃	4
6	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	7
7	ビジネスメール詐欺による金銭被害	8
8	脆弱性対策情報の公開に伴う悪用増加	6
9	不注意による情報漏えい等の被害	10
10	犯罪のビジネス化（アンダーグラウンドサービス）	圏外

【参考】 感染症対策リスク

～ 新型コロナウイルス(2019-NCOV)症例状況 ～

致死率　　0.08%
60歳以上　 2.5%

～ インフルエンザ感染者数(6月1週) ～

- 7,975人　　致死率 0.01%

～ エムポックス(サル痘ウイルス)(6月1週) ～

- 6人(国内175例) 致死率3-6%（現在:男性のみ）

出典 ： 厚生労働省

2023年度研究会：活動スケジュール

日程	研究会	場所	テーマ
6月14日（水）	**第1回研究会**	JUAS会議室	研究会方針・自己紹介
7月26日（水）	**第2回研究会**	JUAS会議室	・講演（IPA　安田様） ・フリーディスカッション
9月29日（金）- 9月30日（土）	**合宿 （第3回研究会）**	プラザヴェルデ沼津	・講演（サイバー研究所　石橋様） ・講演（ﾁｪﾝｼﾞﾎｰﾙﾃﾞｨﾝｸﾞｽ　吉丸様） ・分科会活動（3テーマ）
11月21日（火）	**第4回研究会**	JUAS会議室	・講演（ANAシステムズ　阿部様） ・分科会発表（ﾊﾟｰｿﾙｷｬﾘｱ　山崎様） ・分科会活動（2テーマ）
1月31日（水）	**第5回研究会**	JUAS会議室	・講演（日本ﾏｲｸﾛｿﾌﾄ　大谷様） ・分科会発表（NOK　河本様） ・分科会活動（2テーマ）
3月21日（木）	**第6回研究会**	JUAS会議室	・分科会発表（ｺﾆｶﾐﾉﾙﾀ　玉本様） ・活動のまとめ報告
4月10日（水）- 4月12日（金）	**Jフェス**		

テーマ決定

分科会

分科会

分科会

分科会

分科会

計7-8回の分科会

2023年度研究会：講演会5テーマ と 事例発表3件

	日時	テーマ
第2回	7月26日（水）	• （講演）情報処理推進機構（IPA）安田様 「内部不正防止体制に関する実態調査と サイバーセキュリティ経営ガイドライン」
第3回	9月29日（金）- 9月30日（土）	• （講演）サイバー研究所　石橋様 「サイバーインシデントでのレジリエンスリスクの重要性」 • （講演）チェンジホールディングス　吉丸様 「企業にとっての新たなリスク、気候変動・エネルギー、そしてその開示」
第4回	11月21日（火）	• （講演）ANAシステムズ　阿部様 「ANAグループにおけるセキュリティ活動」 • （事例発表）パーソルキャリア　山崎様 「生成AIにおけるプライバシー」
第5回	1月31日（水）	• （講演）日本マイクロソフト　大谷様 「MicrosoftのAIへの取組、Microsoftの責任あるAI」 • （事例発表）NOK　河本様 「CSIRT体制構築事例」
第6回	3月21日（木）	• （事例発表）コニカミノルタ　玉本様 「コニカミノルタのセキュリティの現状と今後の取り組み」

内部不正防止体制に関する実態調査とサイバーセキュリティ経営ガイドライン

IPA　安田様

◆最近のサイバー攻撃の動向
ランサムウェア攻撃、サプライチェーン攻撃、内部不正が多い

◆内部不正防止へのIPAの取り組み
「組織における内部不正防止ガイドライン」第5版改訂
テレワークの活用、雇用の流動化、DXの推進等の影響で内部不正リスクが増加

◆内部不正防止に関する実態調査
内部不正防止対策は遅れ気味（全社統制は50%程度）
中途退職者に課す秘密保持義務対策の強化が必要

◆サイバーセキュリティ経営ガイドラインの活用
経営への重要度や脅威の可能性を踏まえたサイバーセキュリティリスクの把握
サイバーセキュリティ管理体制の構築事例
必要なサイバーセキュリティ人材の定義と育成の事例

サイバーインシデントでのレジリエンスリスクの重要性

サイバー研究所　石橋様

◆レジリエンスとは？

IT-BCPの災害BCPとの違い
ITサービス継続ガイドライン（経産省）の活用
サイバーインシデントへの対応、CSIRTについて
初動行動の重要性（関連部署の招集など）と原因究明の難しさ

◆企業の取り組みの現状（アンケート実施）

CSIRTの構築状況、メンバー構成、SOCの状況など
IT-BCP対応状況（規程類の整備状況、訓練状況、復旧対応状況など）

◆トリアージと復元（復旧）

ランサムウェア被害発生時の復旧パターンについて
ディザスタリカバリーの基本形について

企業にとっての新たなリスク、気候変動・エネルギー、そしてその開示

チェンジホールディングス　吉丸様

◆地球は温暖化から沸騰化へ

世界リーダが気候変動を人類最大の危機と認識
気候変動（熱波・水害など）による企業の損失について
IPCC報告から考える（平均気温の上昇、降水量の増加の影響について）

◆気候変動が企業に与える影響

IFRS（財務報告の国際基準）適用：当研究会にて12社適用
IFRSでの報告と開示
　気象現象による物理的被害
　脱炭素政策への対応による業務の変革・移行
　温室効果ガス排出量のサプライチェーン管理
国際サステナビリティ開示の対応と準備

ANAグループにおけるセキュリティ活動

ANAシステムズ　阿部様

◆業務のレジリエンス

システム停止時の業務継続のシュミレーション
　実施すべき業務の優先順位付け
　お客様にとって大事なことの継続
　情報伝達の重要性（混乱させない、必要な情報の伝達など）
バックアップシステムの設計と「人」が実施する業務との連動

◆データのレジリエンスについて

ランサムウェア攻撃への耐性を評価する
システムの分離性の確認、バックアップデータの復旧時の考慮
クラウド運営ベンダーが攻撃されるリスクの考慮

◆これからのサイバーインシデント対応について

なりすまし対策、資産管理と脆弱性対策、クラウド環境の保護
社員のセキュリティリテラシー向上が重要

MicrosoftのAIへの取組、責任あるAI

日本マイクロソフト　大谷様

◆生成系AIの利用拡大

社会インフラとして圧倒的スピードでの普及拡大
AIの活用で作業量を減らす効果を狙う
　業務へのAI組込み（共存）の浸透
　調査、事例検索、サポート業務、要約作業など

◆安全に利用できる生成系AIプラットフォームの提供

Microsoftの取り組み
企業データの保護について
法的なリスクへの対応について

「分科会」の活動報告

分科会活動

分科会グループに分かれてディスカッション

【グループ】

どのような脅威への対策に興味があるか？
研究会で取り上げたいテーマは何か？などをアンケートで集計して
悩み・課題が似ているメンバーを同じ分科会へ

・分科会N　（情報セキュリティ：マネジメント系悩み多め）
・分科会B　（セキュリティ＆BCP：事業継続、ITガバナンス多め）
・分科会J　（情報セキュリティ：技術的悩み多め）

各分科会で、各自の悩み、課題を洗い出して、テーマ選定。

分科会活動

分科会グループに分かれてディスカッション

【ディスカッション方法】

- 全体会開催日及び、全体会の開催の無い月に分科会を開催
  （計7-8回）を開催
- 毎回１－２名がテーマ担当。
  担当者は、自己紹介と事例紹介、悩み・課題の相談。
- １時間で1テーマ完結。
  深堀りする場合は、別途開催。宿題は無し。
  万が一欠席した場合でも次回参加しやすくするため。
- 全員でディスカッション（誰かの発言を否定しない。自由な発言）
  チャタムハウスルールを守る
- 8、10、12、2月の分科会は、他の分科会へも参加可能!!

2023年度　分科会
議論したテーマ

分科会N

参加企業

・分科会N　14名

分科会リーダ：
　金子　様（株式会社ニッスイ）

分科会サブリーダ：
　谷口　様（日本電気株式会社）

分科会N
株式会社ニッスイ
日本電気株式会社
JFEシステムズ株式会社
NOK株式会社
キリンビジネスシステム株式会社
第一三共株式会社
東日本旅客鉄道株式会社
日揮ホールディングス株式会社
前田建設工業株式会社
TDCソフト株式会社
独立行政法人住宅金融支援機構
ファイルフォース株式会社
ENEOS株式会社
パーソルホールディングス株式会社

2023年度分科会N 主な研究テーマ

①DXの推進について
②生成系AIとセキュリティ対策
③セキュリティガバナンスについて
④CSIRT構築事例
⑤自社のセキュリティ対策状況について
⑥グループ会社のセキュリティガバナンス
⑦サプライチェーンのリスク評価
⑧ランサムウェア攻撃対策
⑨DDoS攻撃事例について
⑩攻撃メール訓練について
⑪セキュリティ人材育成について　　などなど

分科会B

参加企業

・分科会B　14名

分科会リーダ
　奥村　様（株式会社IHI）

分科会サブリーダ
　新井　様（株式会社読売新聞東京本社）

分科会B
株式会社IHI
株式会社読売新聞東京本社
インテル株式会社
不二サッシ株式会社
SOMPOひまわり生命保険株式会社
株式会社テプコシステムズ
日本プルーフポイント株式会社
コニカミノルタ株式会社
丸文株式会社
アイエックス・ナレッジ株式会社
ヤマハ発動機株式会社
ニッセイ情報テクノロジー株式会社
第一生命情報システム株式会社
大王製紙株式会社

2023年度分科会B 主な研究テーマ

①サイバーBCP対策について
②サイバーBCPにおける復旧プロセスについて
③ランサムウェア攻撃に対する会社としての対応について
④ネットワーク障害について
⑤BCP活動・訓練について
⑥生成AIの活用とリスクマネージメント
⑦クラウドサービス利用時のセキュリティリスク
⑧ゼロトラスト環境について
⑨ITモダナイゼーションについて　　などなど

分科会J

参加企業

・分科会J　１４名

分科会リーダ
坂　様　　（株式会社JALインフォテック）

分科会サブリーダ
松尾　様　（コクヨ株式会社）

分科会J
株式会社JALインフォテック
コクヨ株式会社
鹿島建設株式会社
株式会社かんぽ生命保険
イオン株式会社
日商エレクトロニクス株式会社
株式会社LSIメディエンス
かんぽシステムソリューションズ株式会社
インフォテック株式会社
株式会社中電シーティーアイ
株式会社カジマアイシーティ
日光ケミカルズ株式会社
日本生活協同組合連合会
パーソルキャリア株式会社

2023年度分科会J 主な研究テーマ

①CSIRT活動事例
②グループ会社で発生したサイバーインシデント対応事例
③脅威ベースの侵入テストの事例
④攻撃メール訓練について
⑤内部不正防止対策
⑥SEAM構築に関する製品の評価
⑦EDRの活用について
⑧脅威インテリジェンスの活用について
⑨CAIQによるクラウドサービスの評価について
⑩サポート詐欺の分析
⑪取引先からのセキュリティ対策状況調査について　などなど

2023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紹介いたします。

概要掲載テーマ
・CSIRT構築事例及び自社のセキュリティ対策について
・グループ会社へのセキュリティガバナンス
・サプライチェーンのリスク対策
・サイバーBCP対応について
・サイバーセキュリティ人材について
・防御・検知に関する訓練（脅威ベースの侵入訓練、攻撃メール訓練）
・内部不正対策
・生成AIの活用推進とリスク対策について
などなど

CSIRT構築事例及び自社のセキュリティ対策について

攻撃の高度化への対応と継続的な対策強化

◆CSIRT活動

インシデント対応

公開サービスへの不正アクセス

MS365への海外IPアドレスからのログイン試行

メールアカウントの乗っ取り

情報機器の紛失（PC/社給iPhoneなど）※貸与者が出社しなくなった・・

◆インシデント対応からの再発防止策・対策の改善

不正アクセスリスク低減には、監視と認証の両面の対応強化が必須

2要素認証も破られる・・・認証の重要性、リスクの啓蒙が必要

アカウントの乗っ取り対策

フィッシング対策や継続した啓蒙は必要、ポスターも効果あり

重要なシステムのパスワードの安全性強化（変更）、使いまわしの禁止

資産管理

野良クラウドサーバ、AppleWatchなどなど

グループ会社へのセキュリティガバナンス

セキュリティレベルの統一が重要、国外のグループ会社の統制も重要

◆グループ会社のセキュリティリスク評価・点検

各社のセキュリティ対策のレベルの統一が重要

チェックシート、ペネトレーションテスト結果、攻撃メール訓練結果など利用

- セキュリティ対策の成熟度評価（チェックシート）※回答精度の統一が難しい
- インターネット上からのチェック（外部からのリスク判断）
- アタックサーフェースマネジメント（脅威情報活用・非管理デバイス）

セキュリティフォローアップ（監査ではなく、意見交換を通してセキュリティ啓蒙）

◆インフラを共用するメリット

ネットワーク、パソコン、スマートデバイスの共通化

セキュリティ対策の共通化＋本社でのアラート監視（調達、サポートなども一元化）

小規模のグループ会社の場合、費用負担が課題になる場合がある

◆グローバル対応について

国外のグループ会社とのネットワークは分離している企業が多い

※国内・国外にかかわらず、侵入リスク低減の対策は重要

企業買収時のセキュリティチェックが重要!!

サプライチェーンのリスク対策

増加するリスクではあるが、効果的対策が難しい

◆事業継続への影響大

物・サービスの流れと情報の流れがある

サイバー攻撃による業務停止がビジネス運営に影響を与えている

◆リスク評価について

評価ツールを利用した調査

相手先の会社のリスクの特定（攻撃を受けるリスク）に有効

組織体制、情報管理ルールと教育など組織的・人的な確認も必要

「点検」と「課題の是正」

点検の精度（ヒアリング、検証結果要請）と是正の推進方法が課題

◆取引先からの調査票への回答について

詳細に回答すると情報漏洩＝セキュリティ対策の弱点が漏洩してしまう

◆情報に関するサプライチェーンリスク

委託先へ提供した情報（データ）がサイバー攻撃により漏洩・・・

提供・共有したデータの把握・管理が課題

契約完了時に提供したデータの廃棄を徹底

サイバーBCP対応について（ランサムウェア対応）

ランサムウェア攻撃の増加により、最大のリスクとなっている

◆ランサムウェア被害時の対応について

身代金要求への対応

「払わない」方針企業が多いが、対応方針未定の企業も多い

業務継続のために支払いを選択する可能性がある企業もある

◆情報漏洩リスク低減対応

不審な社外への通信を検知した場合

原因の特定ができていな状態で、ネットワーク停止判断が難しい

警察庁などからの指摘であれば、ネットワーク停止判断がとりやすい

◆システムの停止と復旧について

障害発生時のシステム停止と復旧については、訓練している企業が多い。

ランサムウェアを想定した、データのバックアップからの復旧訓練も増加

復旧のドキュメント整備と復旧の実機訓練は重要

※休日や夜間の対応も必要となる

※環境設定やアプリケーションのバックアップが課題

サイバーBCP対応について（組織的対応）

サイバー攻撃による業務停止のリスク

◆サイバー攻撃による業務停止リスクについて

経営層の理解

社長やCISOがリスクを理解している場合、組織的対策が進めやすい

事業部門への啓蒙

ITインフラやシステムの利用者は、サイバーセキュリティには詳しくないため
サイバー攻撃のリスクを分かりやすく啓蒙する必要がある。
※災害リスクと異なり、理解しにくい・・・

◆業務継続について

インフラ復旧までの日数

段階的復旧の検討、必要な日数を正確に算出して、課題を改善する

業務遂行の代替手段の準備

ITインフラの無い状況での業務遂行方法の検討

サイバーBCP対応について（技術的対策）

業務継続のためのシステムやデータの保護対策

◆インフラの被災リスク低減について

災害対策・障害対策との連動

DR対策、特にコールドスタンバイの仕組みは、IT-BCPにも有効

アクセス経路を冗長化するとセキュリティリスクになる場合がある

認証基盤被災時に、認証無しのデータアクセスを許容することは難しい

◆データの被災リスク低減について

バックアップ対策の基本（３－２－１ルール）

3か所で保管

2種類の媒体で保管

1つのバックアップを遠隔地で保管

※イミュータブルバックアップ（変更不可能システム）の活用

サイバーセキュリティ人材について

必要な人材の定義が重要

◆人材育成計画について

会社として必要な人材の定義が重要（必要なスキルと人数）
IT系企業と一般企業での格差拡大
キャリアパス、資格取得支援なども重要（特に予算：講習の受講費用）
　CSIRT/SOCのような専門人材
　部署長など情報セキュリテイに関して判断をする人材
　システムの利用者（一般の社員）へのセキュリティリテラシー教育

◆なぜ不足するのか？

セキュリティ業務の多様化（法令、DX、攻撃・リスク、インシデント、問い合わせ）

◆育成方法について

採用/社内公募＋自社業務に合わせた育成が重要
CSF（サイバーセキュリティフレームワーク）などから必要なスキルを定義
セキュリティ知識分野（SECBOK）やNCAのセキュリティ人材資料の活用
※IT関連企業以外の一般企業では、
　　セキュリティ専門教育の受講費用が予算上承認されにくい場合もある

防御・検知に関する訓練（脅威ベースの侵入訓練、攻撃メール訓練）

訓練の高度化と訓練の継続

◆脅威ベースのペネトレーション訓練

レッドチーム訓練の一種
　対応プロセスの検証が目的
　攻撃（レッド）と防御・運用（ブルー）と中立（ホワイト）の3チームで実施
　攻撃は、攻撃対象を分析の上、攻撃を準備する。
　攻撃は、事前予告無し。事業部門への連絡も無し。
　　※経営者の指示・許可が必須。

◆攻撃メール訓練

訓練の目的の明確が必要
　開封率を下げる、通報率を上げる、開封時の適切な対処など
目的に応じた準備
　事前学習資料、実施前の通知有無、メール内容など

内部不正対策

コンプライアンス強化はされているが減らない内部不正

◆事例からの原因分析

従来からの分析のとおり、動機＋機会＋正当化がそろわないようにする
退職・転職時だけでなく、テレワーク等により内部不正リスクは増加
　転職（人材の流動化）、派遣・請負の社外の方も頻繁に交替
メールだけでなく、クラウドサービスを利用したデータ持出も増加

◆発生防止への取り組み

「ログの監視」「ログ監視していることを周知」「教育」「誓約書」の活用
　ログからのアラート発信
　　印刷、送信先メールアドレス（企業メール以外）、USBメモリ利用など
クラウドサービスへのアップロード、メールの添付ファイル、チャットツールなど
監視対象の拡大や社給スマートフォンのアプリ利用制限も必要

◆新たなリスク：前職の情報持ち込みによる不正競争防止法違反

中途採用時のチェックも必要

生成AIの活用推進とリスク対策について

活用シーンの増加と利用者のリテラシー強化

◆生成AI活用時のルールの例

原則として、顧客から受領したデータ、個人情報、社内の秘匿性の高い情報は、入力禁止。
ソースコードを生成した場合は、社内限定で利用すること。
生成した情報を社外へ提供する場合は、「正確性」「著作権」などの問題がないことを確認してから提示すること。

◆社内での生成AI活用

DX推進、イノベーション推進の観点からも活用促進
活用に関する講演会・ウェビナーの提供
利用可能なサービスを明示
AzureOpenAIをカスタマイズして、社内向けに提供

守るべき情報の明確化について

情報管理区分の運用

◆情報管理区分について

「秘」「社外秘」などの情報管理区分の規程はあるが浸透していない。

区分のスリム化を図る

各区分の情報の具体例を明示して理解を助ける

◆考慮すべき点

法令順守：個人情報保護法、GDPRなど

顧客から受領した情報の情報管理区分に関するルールの整備・管理方法

保管場所（クラウドストレージ、ファイルサーバ）とフォルダ構成の管理とルール

アクセス権のグループ（部署単位、役職単位など）の管理とルール　など

EDRの運用について

SOCが重要

◆セキュリティ担当者による遠隔地パソコンへの対応

アラートが発生したパソコンに対して、遠隔地からネットワーク隔離や調査が可能
社外へ持ち出したパソコンやテレワーク環境にも対応可能

◆SOC運用（24／365）

大量に検知されるアラートへの遅滞ない一次切り分けが可能
　漏れない検知のためには、過検知は一定数発生する
夜間・休日に発生したアラートへも日中同様に対応可能
　夜間・休日に隔離した場合の利用者へ連絡方法の周知が必要
国内のベンダーの場合、追加サービスも豊富
　ホワイトリスト運用やポリシー管理の対応なども可能

◆EPP機能（従来のウィルス対策ソフト）の置き換えは可能なのか？

ウィルス対策ソフトによるウイルスの検知は一定数発生している
Webサイト閲覧やコールバックブロックなどウイルス対策以外の機能も利用

クラウドサービスのセキュリティ審査

リスクの啓蒙と点検へのシフト

◆セキュリティチェックの標準化

クラウドサービスの審査項目はほぼ標準化されてきた
業務の重要性、保存するデータの秘匿性がカギとなる
クラウドサービスの評価を代行するサービスもあり
CAIQの活用
（CAIQ：CSAが提供するグローバルで利用されているセキュリティチェック）

◆課題

IT担当がいない部署でのクラウドサービス契約の増加
クラウドサービス利用時のリスクの浸透度合いが不明
　管理者アカウントの保護、利用者アカウント管理
　アクセス制限（SAML連携、IPアドレス制限など）
　クラウド間のAPI連携　など
利用開始後の定期的なセキュリティ点検が重要（担当者変更も多い）
利用終了時のデータの取扱い

2023年度
現地視察

ユーザ企業訪問

分科会の開催時に実施

◆分科会は、参加企業の会議室を利用させていただいています。
各社のご協力ありがとうございます。

かんぽ生命保険様、ニッセイ情報テクノロジー様、日揮ホールディングス様などなど

◆合同分科会開催：ヤマハ発動機様

分科会開催時に
以下の見学対応ありがとうございます。

・製品（各種二輪車・自動車・エンジン）の見学

・製品の組立工場見学

スーパーコンピュータ富岳見学

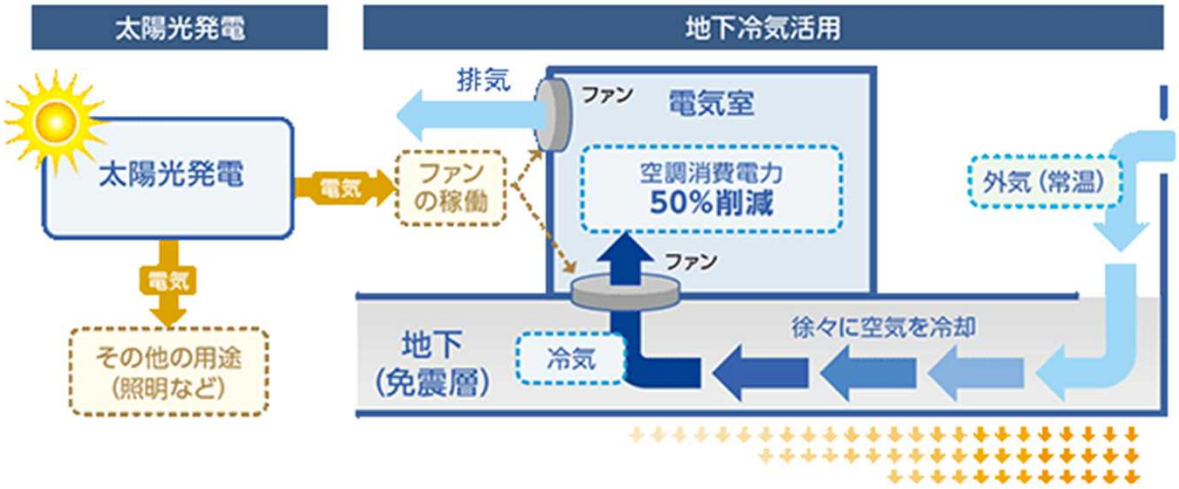
アプリケーション演算性能世界一

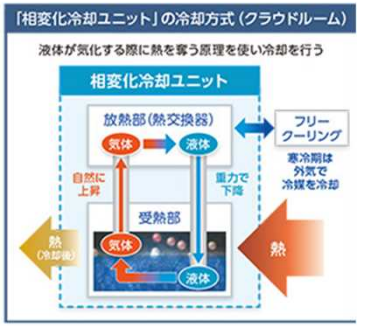
◆理化学研究所
富岳の説明、見学　ご対応ありがとうございます。

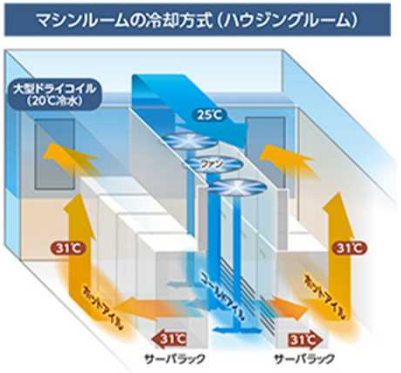
NEC神戸データセンター見学

自然エネルギーを活用したデータセンター

◆NEC神戸データセンター
データセンターの説明、見学　ご対応ありがとうございます。







まとめ

2023年度出席率

	出席者総数
第1回	39名
第2回	39名
第3回	37名
第4回	36名
第5回	36名
第6回	35名

◆出席率

平均　37名　（90%）

分科会は、複数参加の方も！

出席ありがとうございます！

2023年度活動の振り返り（メンバーの意見）

- 全体的に「満足/概ね満足」（100%：未回答除く）の評価をいただきました。
- 実際の事例、対策が共有できて効果的であった。想定以上の情報を得られた。
- 様々な業種、様々な年代の方との交流ができて良かった。
- 初参加でしたが、情報交換がスムーズにできた。
- 宿題がなかった（ノルマ・負担が少なくて良かった）
- 組立工場見学やスーパーコンピュータの見学は刺激がありよかった。
- ハイブリッド形式での開催があってもよいかと感じました。
- 合宿の会議室が手狭なため、他の分科会と声がまざり聞きとりにくい。
- チャット系ツールの導入により、よりコミュニケーションを活性化したい。
- 合宿が早めの時期に開催されれば、もっと議論が活性化したかと思う
- 他の分科会へもっと参加したかった。

2023年度活動の振り返り（運営サイド・幹事団）

・**合宿運営**

＝＞ 場所・日程は、調整は難しい面もありますが、

分科会の環境（他の分科会の会話も聞こえ、聞き取りにくい）は、改善します。

・**対面での交流**

＝＞ 対面での交流が効果的だった。

セキュリティインシデント対応のボードゲームの活用なども検討します。

ハイブリッド開催希望もありますので、実施について検討します。

・**コミュニケーションの強化**

＝＞ Box / メーリングリスト　の活用強化とセキュリティ対策の強化。

チャタムハウスルールを守った上で、資料・情報の共有も積極的に進めます

他社はどうしているか？について、アンケートを定例化してデータ共有します。

2023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
- 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
2024年もよろしくお願いします！

以上