2021年度
企業リスクマネジメント研究会活動報告

2022年4月13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. 2021年度活動報告
    - ニューノーマルな活動スタイル
    - 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

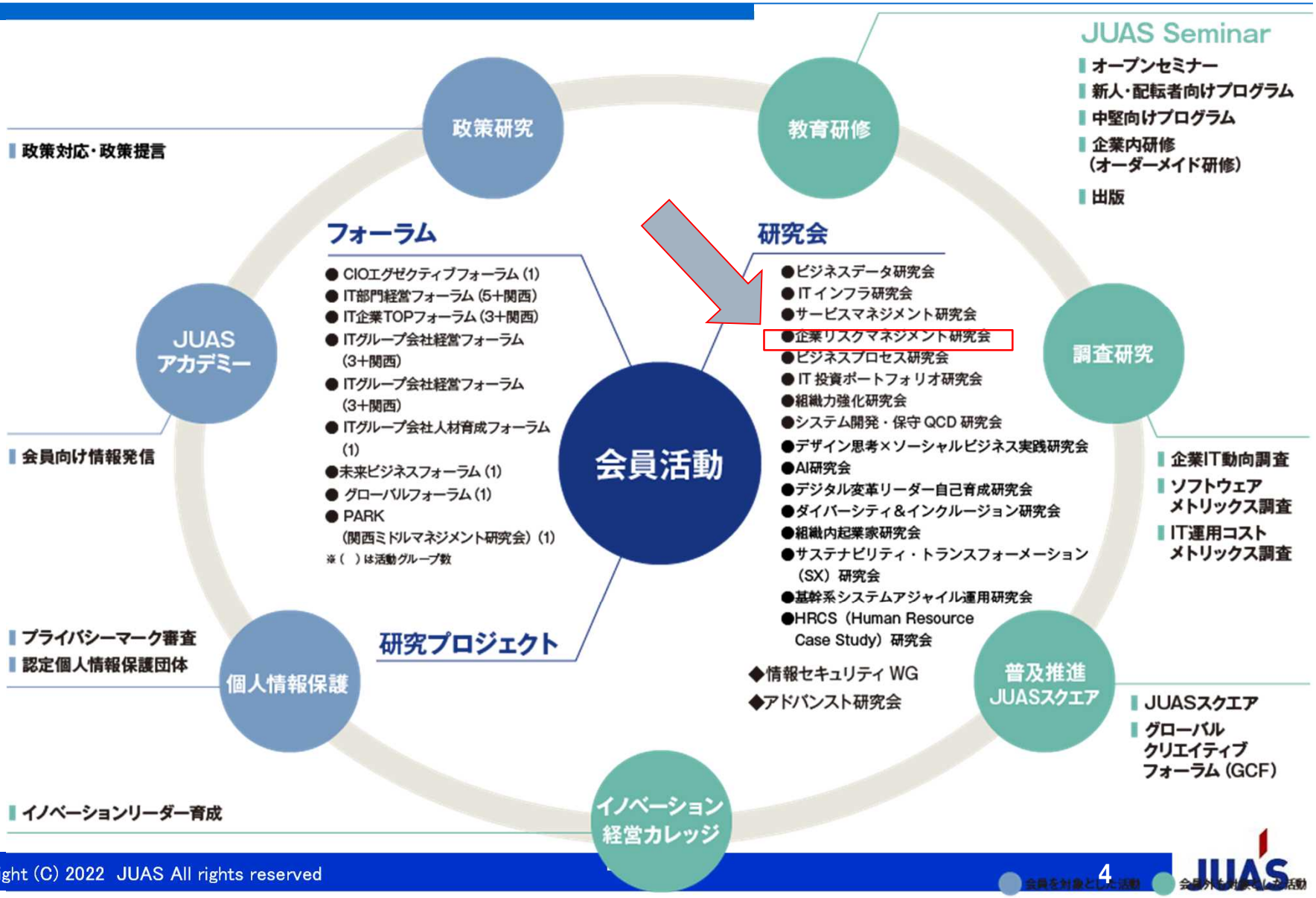
企業リスクマネジメント研究会の歴史と概要

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（2021年版より）

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



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
～
2021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（石橋）

コロナ禍を乗り越え、無事、16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～2021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（募集時）

【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。

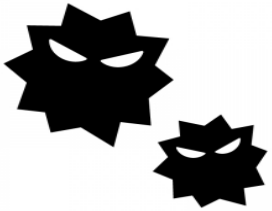
本研究会は、若手の方や女性の活躍を応援します。

【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

コロナの影響は継続・・・



オンライン開催2年目・・・

①オンライン開催・・・発言しやすい雰囲気作り・・・分科会人数検討

②合宿や懇親会が無い・・・コロナの状況に依存・・・

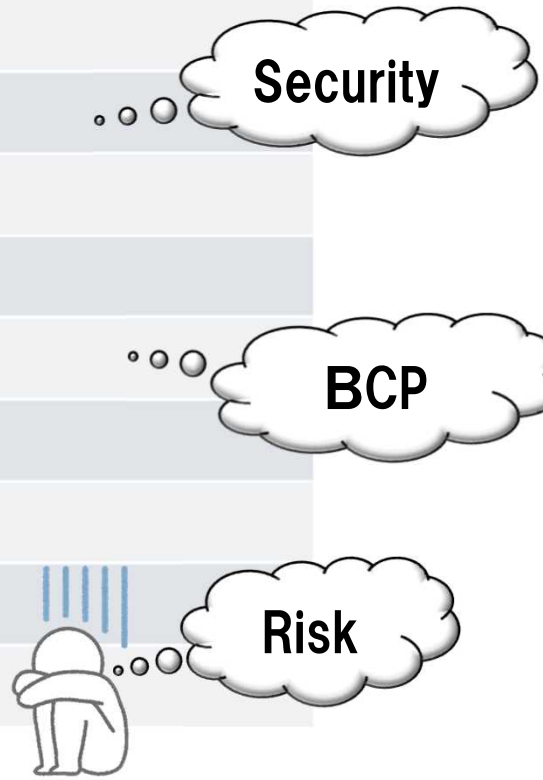
1．企業リスクマネジメント研究会の歴史と概要

- テーマとなる企業リスク

【参考】 世界の経営者が考えるビジネスリスク

～ 「Risk Barometer 2021」(Allianz社)より ～

順		
1	事業中断	サプライチェーン、ディストリビューション
1	コロナの世界的拡大	感染症リスク
1	サイバーインシデント	データ漏洩、データ破壊
4	市場変革	新規参入・企業買収
5	法律・規制の変更	米中摩擦、EU関連
6	自然災害	台風・津波・地震
7	火災・爆発	工場・倉庫火災
8	マクロ経済の動向	世界的な景気後退リスク
9	気候変動	災害リスク
10	政治的リスク	政情不安、テロ、暴動

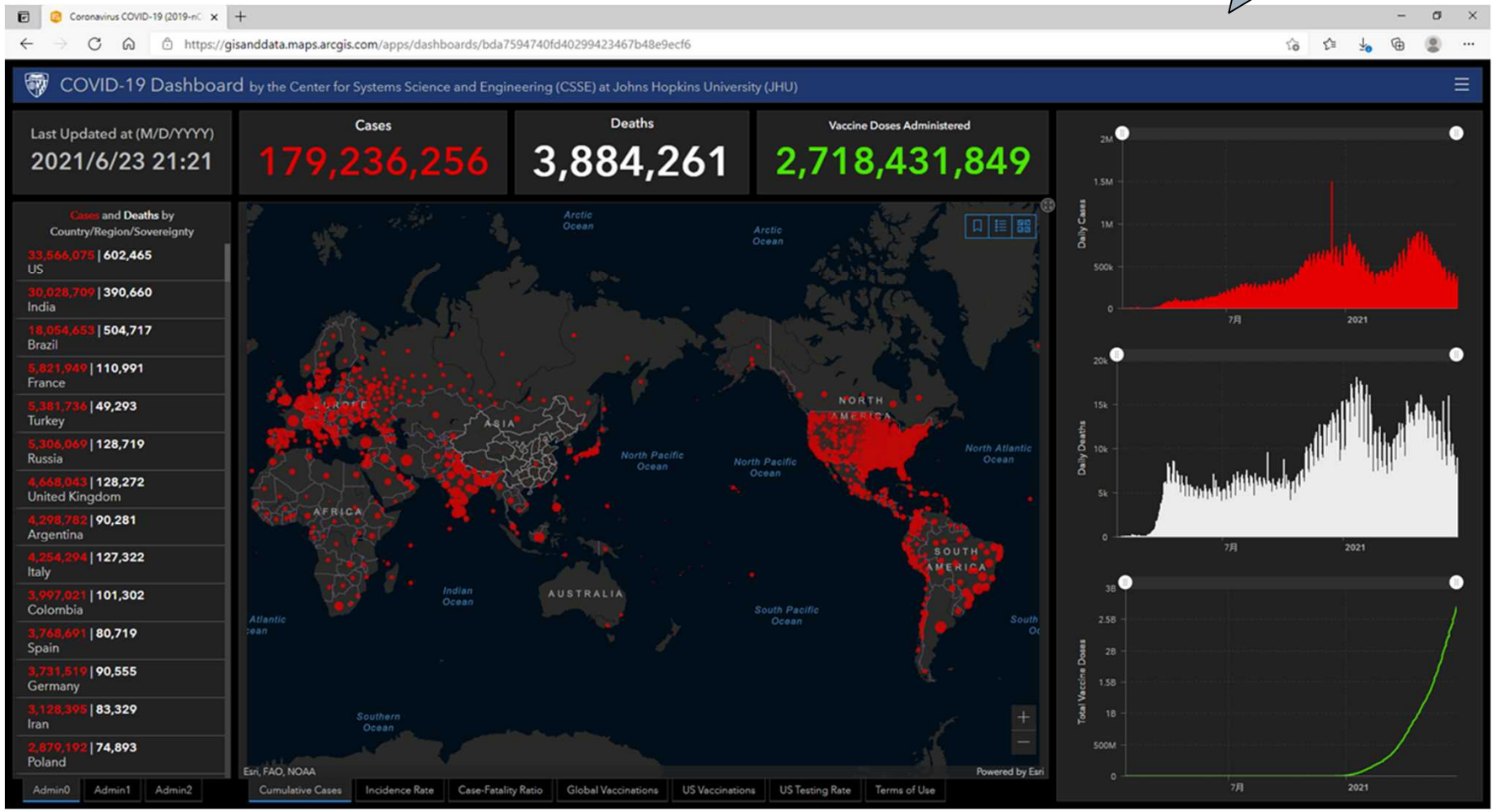


出典 ： https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2021-business-risks.html

研究会第１回実施日の頃の状況

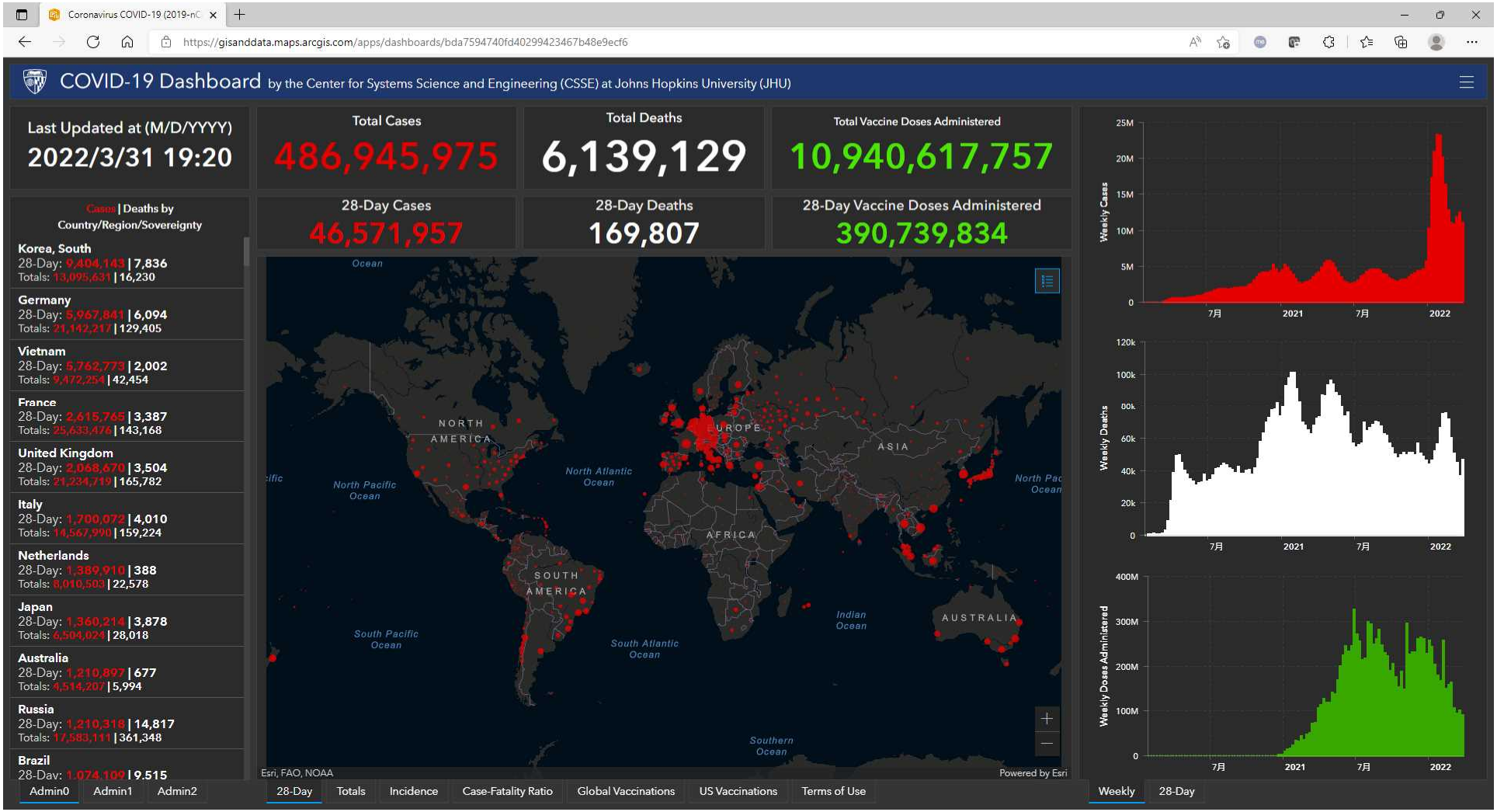
終息しそうな雰囲気
もありましたが・・

～ 新型コロナウイルス(2019-NCOV)症例状況 ～



出典 ： ジョンズ・ホプキンス大学システム科学工学センター

【参考】 感染症対策リスク



出典 ： ジョンズ・ホプキンス大学システム科学工学センター

【参考】 情報セキュリティ10大脅威 2021

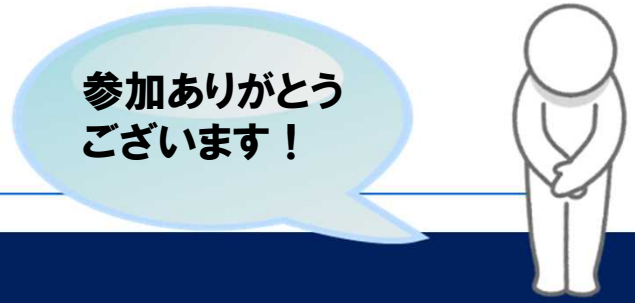
～ IPA 情報処理推進機構 より ～（2021：研究会開始時点）

昨年	個人		組織	昨年
1	スマホ決済の不正利用	1	ランサムウェアによる被害	5
2	フィッシング	2	標的型攻撃による機密情報漏洩	1
7	ネット上の誹謗・中傷・デマ	3	テレワークへの攻撃	N
5	メールやSMSを使った脅迫・詐欺	4	サプライチェーン攻撃	4
3	クレジットカード情報の不正利用	5	ビジネスメール詐欺	3
4	インターネットバンキングの不正	6	内部不正による情報漏えい	2
10	インターネット上での個人情報漏洩	7	IT基盤の障害に伴う業務停止	6
9	偽警告によるインターネット詐欺	8	サービスへの不正ログイン	16
6	不正アプリによるスマートフォンの被害	9	不注意による情報漏えい	7
8	サービスへの不正ログイン	10	脆弱性の公開に伴う悪用増加	14

1. 企業リスクマネジメント研究会の歴史と概要

- 2021年度の参加企業と運営体制

2021年度の参加企業



34社に参加していただきました。

企業名	企業名	企業名
IIMヒューマン・ソリューション株式会社	インテル株式会社	NECソリューションイノベータ株式会社
鹿島建設株式会社	コニカミノルタ株式会社	MS＆ADシステムズ株式会社
株式会社かんぽ生命保険	ＪＦＥシステムズ株式会社	コープ情報システム株式会社
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	ＪＸアイティソリューション株式会社
Ｔ＆Ｄ情報システム株式会社	積水化学工業株式会社	株式会社ＪＡＬインフォテック
東京ガスiネット株式会社	株式会社セブン＆アイ・ネットメディア	田辺三菱製薬株式会社
日商エレクトロニクス株式会社	第一生命情報システム株式会社	日揮ホールディングス株式会社
ファイルフォース株式会社	株式会社テプコシステムズ	日本水産株式会社
株式会社富士通エフサス	株式会社ミライト情報システム	パーソルホールディングス株式会社
富士フイルムシステムズ株式会社	株式会社LIXIL	パナソニック株式会社
丸文株式会社		東日本旅客鉄道株式会社
三菱総研DCS株式会社		株式会社ＩＨＩ

ようこそ “企業リスクマネジメント研究会” へ

34名の皆様にご参加いただきました。

ステータス	人　数
新規	16名
継続・復帰	18名

2021年度　活動報告

ひきつづき
ニューノーマルな活動スタイル

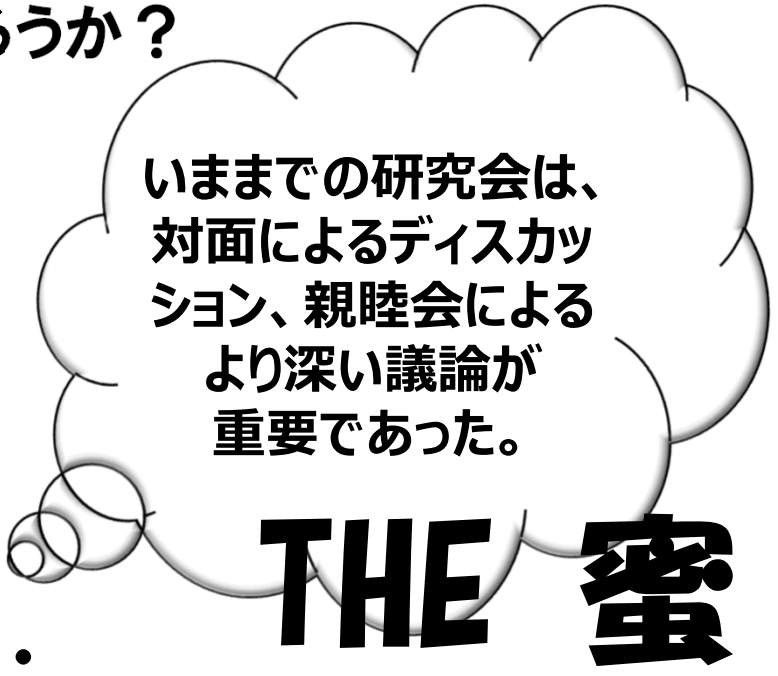
リスクマメジメントの研究方法

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。

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。

ニューノーマルなリスクマメジメント研究方法

全体会： 専門講師の講演＋各分科会の発表＋情報交換会（実施できず）

- 講演会は、オンラインで実施
- 全体会開催日に分科会も実施＋活動の共有

分科会： １０－１５名でディスカッション＋分科会情報交換会

- 分科会の人数は、１０数名（オンラインとしては若干多め）
  いろいろな事例・経験談を得るため。
- オンラインでもチャタムハウスルールを堅持
- 他の分科会への参加可能!!

合宿・現地見学会・会社訪問： 代案無し

- 新規参加の方からも希望あり。沼津合宿が懐かしい・・・

Chatham House Rule for Web会議

Web会議でもチャタムハウスルールを守ってください

- 会社では会議室にて参加お願いします
- 自宅でも、できるだけ個室での参加をお願いします
- カメラはオン（バーチャル背景は・・・）
- フルネームを表示しましょう（JUASルール）
- イヤホンマイクを利用してください（スピーカー厳禁）
- 録音・撮影・スクショも禁止です

★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する

「全体会」の活動報告

幹事団の紹介

2021年度の幹事団です

【全体会】

- CHO　　坂　様（株式会社JALインフォテック）
- 部会長　　伊藤　（鹿島建設株式会社）
- 副部会長　　糀原　様（インテル株式会社）
- 副部会長　　長井　様（株式会社LIXIL）

【分科会】

- 分科会A　分科会長　：　河原林　様（株式会社富士通エフサス）
  副分科会長：　佐々木　様（ファイルフォース株式会社）
- 分科会B　分科会長　：　寛座　様（株式会社ミライト情報システム）
  副分科会長：　坂上　様（第一生命情報システム株式会社）
- 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：　金子　様（日本水産株式会社）

2021年度研究会：活動スケジュール

研究会	日程		時間	場所	メインテーマ（予定）
第1回	6月25日	金	15:30～17:30	Zoom	研究会方針・自己紹介
第2回	7月16日	金	15:30～17:30	Zoom	・ゲスト講演（IPA　安田様） ・ディスカッション
第3回	9月3日	金	15:30～17:30	Zoom	・ゲスト講演（サイバー研究所　石橋様） ・分科会事例発表（A） ・分科会活動内容紹介（A/B/J）
第4回	11月10日	水	15:30～17:30	Zoom	・ゲスト講演（メンロセキュリティジャパン　寺田様） ・分科会事例発表（B） ・分科会活動内容紹介（A/B/J）
第5回	1月12日	水	15:30～17:30	Zoom	・シャッフル分科会 ・分科会事例発表（J） ・分科会活動内容紹介（A/B/J）
第6回	3月11日	金	15:30～17:30	Zoom	・活動の振返り ・分科会活動内容紹介（A/B/J）
Jフェス	4月13日～15日				研究会成果報告

テーマ決定

分科会

分科会

分科会

分科会

分科会

分科会

計8回の分科会

2021年度研究会：講演会3テーマ と 事例発表3件

	日時	テーマ
第2回	7月16日（金）	• IPA 安田様 「ビジネスリスクとしてのサイバーセキュリティ」
第3回	9月3日（金）	• サイバー研究所 石橋様 「コロナ2年目で情報システム部門が検討すべきリスク対策」 • （事例発表）丸文株式会社 塩様 「上手な標的型攻撃メール訓練」
第4回	11月10日（水）	• メンロセキュリティジャパン 寺田様 「検知に頼っていては脅威は止められない」 • （事例発表）株式会社 テプコシステムズ 江本様 「新型コロナウィルス・パンデミック対応」
第5回	1月12日（水）	• （事例発表）株式会社 ＪＡＬインフォテック 坂様 「セキュリティポリシーの作成・運用について」

ビジネスリスクとしてのサイバーセキュリティ

IPA　安田様

◆増大する脅威

Solarwinds社ツール、パイプラインシステムへのサイバー攻撃、
ランサムウェアと情報窃取（2重の脅迫）

◆サイバーセキュリティ経営ガイドライン

経営者が認識すべき3原則とCISOへ指示すべき重要10項目
- サイバーセキュリティ対策の人材の確保
- リスクの把握と対応が重要
- 実効性のあるCSIRTが重要
- サプライチェーン全体の対策が重要

◆実践のためのプラクティス集

サイバーセキュリティ対策への理解
「はじめの1歩」「悩み相談」へのガイド

コロナ２年目で情報システム部門が検討すべきリスク対策

サイバー研究所　石橋様

◆情報システム部門の共通認識は？

テレワークの基盤、Web会議システムの標準は？・・・
Teams利用企業が多い。
ネットワーク帯域への負荷・・・

◆コロナ2年目

テレワークでも従来と同等の成果を出せる
本番環境の操作を在宅で実施することへの許可

◆ファイルサーバはどうなるのか？

テレワークの日常化とランサムウェア攻撃の増加
テレワーク環境の構築は、緊急対応で実施したが、
コロナ2年目は、計画的なセキュリティ投資が必要
※VPN・仮想デスクトップ、SOC、クラウドサービス利用など

検知に頼っていては脅威は止められない

メンロセキュリティジャパン　寺田様

◆検知テクノロジー

ゼロディ脆弱性と新しい攻撃手法

検知による多層防御で守り切れない部分への対応は？

◆アイソレーションテクノロジー

業務の58%はブラウザーで実施している

アイソレーション＝攻撃をエンドポイントへ到達させない

※リソースファイルにも脅威を埋め込みことが可能

アイソレーション対策は、利便性を損なわない対応が重要

「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A （サイバーセキュリティ：技術系悩み多め）
・分科会B （セキュリティ＆BCP：事業継続、ガバナンス、オリパラなど）
・分科会J （情報セキュリティ：マネジメント系悩み多め）

【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（計８回）を開催
・毎回１－２名が担当。担当者は、自己紹介と事例紹介、悩み相談
・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）
・8,10,12,2月の分科会は、他の分科会へも参加可能!!

2021年度　分科会
議論したテーマ

2021年度分科会A 主な研究テーマ

①標的型攻撃メール訓練について
②IoT関連のインシデント事例について
③標準ブラウザの選定について
④PPAPについて
⑤FISC安全対策基準によるリスク評価について
⑥WEBサイトの脆弱性診断について
⑦SOCの構築と運用について
⑧ゼロトラストの考え方
⑨シンクライアントについて

2021年度分科会B 主な研究テーマ

①内部不正対策について
②テレワークと情報セキュリティ事故の変化
③新しい働き方について
④新型コロナウイルスへの対応
⑤情報セキュリティポリシー
⑥セキュリティのコンティンジェンシープラン
⑦情報セキュリティ教育・人材育成
⑧脅威に対するPCプロセッサー
⑨サイバーセキュリティ訓練
⑩CSIRT/SOCのグローバル展開
⑪セキュリティフレームワークの比較

2021年度分科会J 主な研究テーマ

①クラウドサービス利用時の審査ルールと判定基準
②ISMSの維持と推進について
③シャドーITの実態と対策
④DDoS攻撃への対応
⑤情報セキュリティ教育と標的型メール訓練
⑥パソコンの特権管理について
⑦在宅勤務のリスク（インターネットアクセス）
⑧グループ会社ガバナンス
⑨脆弱性対応とパッチ適用管理
⑩エンドポイントのセキュリティ対策
⑪自社のセキュリティ対策の充足度チェックについて

2021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
・新しい働き方について
・在宅勤務のリスク
・シャドーITの実態と対策
・内部不正対策
・パソコンの特権管理について
・Webサイトの脆弱性診断
・エンドポイントセキュリティ対策
・SOCの構築と運用
・サプライチェーンマネジメント

新しい働きかたについて

在宅勤務＋Web会議、オンラインコミュニケーション

◆在宅勤務について

在宅勤務が定常化。Web会議、スマートデバイス、ペーパーレスが加速

◆付随的な変化

通勤がなくなり、歩かなくなった（運動不足）
飲み会、歓送迎会がなく、対面での会話が減少
副業禁止規程がなくなった。昼休みと勤務の境界線があいまい。

◆あらたなリスク

フィッシングや詐欺行為に騙されやすくなる
社給PCで、VPNを経由せず、直接インターネット閲覧
Youtube閲覧・ウエビナー参加など通信量のさらなる増加
メール誤送信は減少したが、クラウドでのデータ共有ミスが発生
自宅で、機密情報を取扱う業務を実施しているリスク
管理されていない膨大な会議録画データ・・・

在宅勤務のリスク

在宅勤務＋Web会議、オンラインコミュニケーション

◆在宅勤務のリスク

社内への接続にVPNを利用している場合
　VPN切断時など社内ネットワークを経由しないインターネットアクセス
会社のPC持ち帰りの場合
　ローカル領域に保存しているデータの漏洩
　自宅のネットワークへの攻撃の波及

◆技術的な対策

クラウドプロキシーを利用したネットワーク
EDRツールなど、管理者側でPCの状態を監視できる仕組み
VDI環境の提供（社内データのダウンロードや印刷を制御）
外部接続機器への書き込み禁止制御

シャドーITの実態と対策

業務DX、クラウドサービスの普及とセキュリティリテラシーの普及

◆増加するシャドーIT

業務DX・働き方改革のもと、
許可なくアプリ、クラウドサービスを利用するケースが増加
利便性が優先され、セキュリティリスクについては、啓蒙が浸透していない

◆課題

アプリ・ソフトウェアの利用：IT部門の審査が無くても導入可能
導入したソフトのセキュリティパッチ適用やライセンス管理
Web会議、ビジネスチャット、個人用クラウドストレージ、翻訳、名刺管理等
会社で標準ツールを準備・全社員分のライセンスで難航
個人で利用しているクラウドサービスへ会社の業務データを保管
個人で利用しているメールアドレスへ業務メールを転送
社給PCの目的外利用
業務に関連のない動画の視聴
個人的なWeb会議（オンライン飲み会）

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
退職・転職時だけでなく、継続的な内部不正も発生している

◆再発防止への取り組み

直接コンシューマ対応する企業の場合
　現金授受を廃止する。例外を認めない。

全企業共通の対策
　行動規範の啓蒙・教育
　会社・組織風土の改善、具体的なあるべき姿の設定
　管理責任・監視の仕組み、モニタリング、アナウンス（注意喚起）

パソコンの特権管理

サイバー攻撃対策として重要性が高まっている

◆サイバー攻撃における特権・管理者アカウントの利用

権限奪取しやすい一般利用者のカウントの乗っ取り
ローカル管理者権限の奪取とネットワーク内の横展開
サーバアカウントやドメインアカウントを入手して権限昇格
ドメイン全体への攻撃（データ窃取、ランサムウェアなど）

◆多くの企業でのリスク

パソコン利用者へ管理者権限を付与している
　ソフトのインストールなどは利用者で実施している企業が多い

部署のサーバの管理は各部署にまかされている。
　管理者アカウトの管理状況に課題

ドメイン等の管理者アカウントの保護が十分でない
　操作ログは所得しているが操作との一致性の確認・・・

Webサイトの脆弱性点検

攻撃の起点となるため標準的に安全性の作りこみ、点検、監視が必要

◆侵入に利用される各種サーバ

Webサイト、公開サーバ、VPNサーバなどインターネット側からアクセス可能なサーバは、攻撃者からの侵入拠点となる。

◆課題

サーバ設置時、Webサービス開始時の対応
　環境構築・システム構築時にセキュリティ対策を実施

点検として、定期的な脆弱性診断の実施
　診断頻度の課題（セキュリティ部門として実施と部署管理者側での実施）
　診断コストは誰が負担するか？
　診断結果への対処時期の判断
　サーバやシステムへの優先度判断基準が必要

エンドポイントセキュリティ対策

攻撃の高度化への対応

◆攻撃の高度化

Emotetなど、実際のメールを利用した攻撃の復活
ダウンローダーにより、複数のウイルスの利用
正当なコマンドを利用した不正アクセス
テレワーク環境などの脆弱性を利用して攻撃

◆エンドポイントセキュリティ対策

結局は多層防御の考え方

- リスクあるWebサイト/攻撃者サイトへの通信ブロック
- 攻撃メールの排除、アイソレーション機能
- 外部デバイス接続
- ウイルス対策ツールの活用（監視業務の効率化）
- EDR「検知」ツールの活用
- 操作ログの収集
- データファイルの暗号化（暗号化方式と利便性）

SOCの構築と運用

インフラ稼働監視とは異なる監視体制

◆稼働監視との違い

監視対象：各PCからのアラート情報、ネットワークやシステムのログ
エンドポイント利用者への確認・対応依頼が必要となる。

◆SOC運用の課題

監視すべきアラート、イベントのボリューム
　監視体制、監視環境の構築に必要な前提条件となる
攻撃が変化・進化する
　機械的な判断でできる部分はあるが、
　問い合わせ対応のように1次受付で折り返せる事案は少ない
人材確保・育成
　心理的な負担も多く、要員の確保と育成は課題
勤務（休暇取得）
　年休取得を考慮すると要員は想定よりも増員が必要

サプライチェーンマネジメント

サイバー攻撃により、さらに強化が必要となった

◆サプライチェーンの拡大
グループ会社ガバナンス
海外グループ会社ガバナンス
協力会社へのガバナンス

◆セキュリティガバナンス（グループ会社・海外グループ会社）
アセスメントの範囲（会社レベル・システムレベル）
チェックリストが有効。未対応項目への対処。
　費用負担、人材の不足

◆企業買収時のセキュリティチェック
リスクアセスメントを実施してシステム統合の判断。改善の計画を設定。
メールアカウントの侵害有無やデバイスのウイルス感染有無チェックが必要

まとめ

2021年度出席率

第1回		32名	94%
第2回	分科会	33名	97%
	全体会	34名	100%
8月	分科会	38名	100%以上
第3回	分科会	28名	82%
	全体会	29名	85%
10月	分科会	38名	100%以上
第4回	分科会	31名	91%
	全体会	30名	88%
12月	分科会	32名	94%
第5回	分科会	27名	79%
	全体会	29名	85%
2月	分科会	29名	85%
第6回	分科会	31名	91%
	全体会	32名	94%

◆出席率
平均　32名　(94%)

分科会は、複数参加の方も

出席ありがとうございます！

2021年度活動の振り返り（メンバーの意見）

- 全体的に「満足」の評価をいただきました。
- 移動時間がない。遠方からの参加がしやすい。
- オンラインでも、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
- 各回完結である点がよい。発表によって自社のリスク対応の振り返りができた
- 宿題がなかった（ノルマ・負担が少なくて良かった）
- 発言が同時になったり、ゆずりあったり、沈黙があった・・・
- 全員の表情が見えないので、意思疎通が難しい
- 最初に決めたテーマ以外の話題につても話したかった
- チャットツールの活用ができれば、さらに効果アップできそう
- 対面での懇親会が無いのが残念

2021年度活動の振り返り（運営サイド・幹事団）

・**分科会運営**

＝＞ 他の分科会への参加が効果的だった。

次年度も分科会交流を増やす。

・**対面での交流**

＝＞ 希望者多数。対面とWeb会議のハイブリッドは会話の温度差がでるので

対面開催（人数の制限はでますが）を検討します

・**チャットツールの採用**

＝＞ 希望者多数。Web会議形式でのディスカッションに馴染んできたため、

人材交流の場として、研究会のチャットツールを採用を検討します

以前、研究会の前後や休憩時間に実施していたちょっとした相談・意見

交換をチャットツールで実施したいと考えます

2021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
- Zoom操作やオンライン運営の勘所を指導していただき、
  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

以上