2020年度
企業リスクマネジメント研究会活動報告

2021年4月14日

部会長　伊藤　吾朗（鹿島建設株式会社）

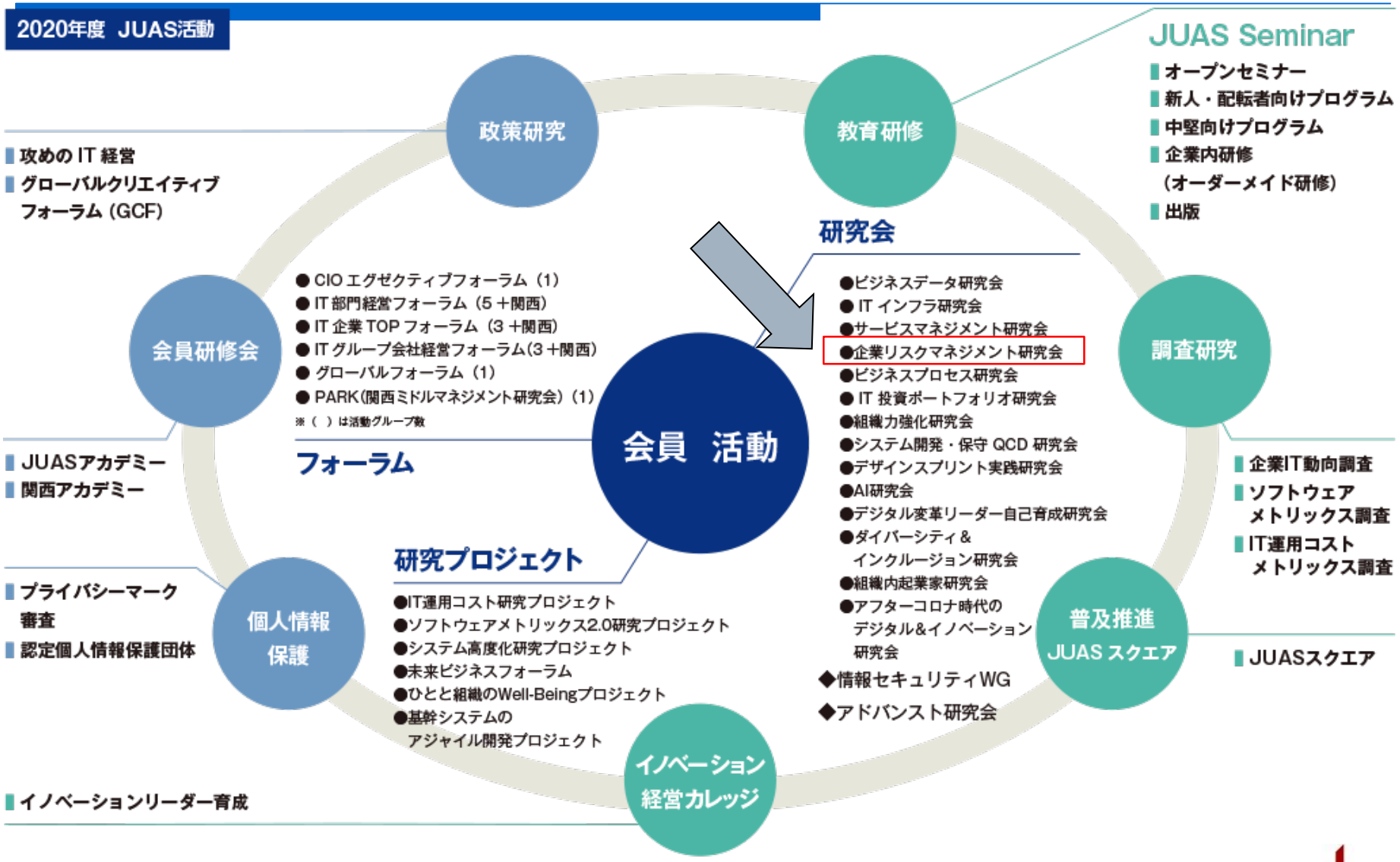
アジェンダ

1. 企業リスクマネジメント研究会の歴史と概要
2. 2020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

JUAS活動（2020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～2020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、15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～2020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 2020」(Allianz社)より ～　※1月14日公開

順位		
1	サイバーインシデント	情報漏洩、破壊、システム停止
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	法律・規制の変更	米中摩擦、EU関連
4	自然災害	台風・津波・地震
5	市場変革	新規参入・企業買収
6	火災・爆発	工場・倉庫火災
7	気候変動	災害リスク
8	企業ブランド価値の損失	評判、SNSリスク
9	新技術	AI, IoT
10	マクロ経済の動向	世界的な景気後退リスク

出典 ： https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2020-business-risks.html

【参考】 情報セキュリティ10大脅威 2020

～ IPA 情報処理推進機構 より ～

昨年	個人	順位	組織	昨年
NEW	スマホ決済の不正利用	1	標的型攻撃による機密情報の窃取	1
2	フィッシングによる個人情報の詐取	2	内部不正による情報漏えい	5
1	クレジットカード情報の不正利用	3	ビジネスメール詐欺による金銭被害	2
7	インターネットバンキングの不正利用	4	サプライチェーンの弱点を悪用した攻撃	4
4	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	5	ランサムウェアによる被害	3
3	不正アプリによるスマホ利用者への被害	6	予期せぬIT基盤の障害に伴う業務停止	16
5	ネット上の誹謗・中傷・デマ	7	不注意による情報漏えい（規則は遵守）	10
8	インターネット上のサービスへの不正ログイン	8	インターネット上のサービスからの個人情報の窃取	7
6	偽警告によるインターネット詐欺	9	IoT機器の不正利用	8
12	インターネット上のサービスからの個人情報の窃取	10	サービス妨害攻撃によるサービスの停止	6

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。

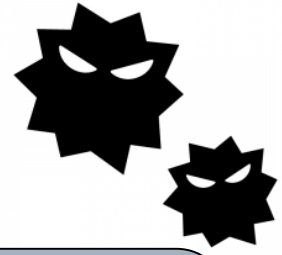
本研究会は、若手の方や女性の活躍を応援します。

【研究テーマ案】

サイバーセキュリティ、情報セキュリティマネジメント

※BCPに関しても議論します

コロナの影響で開始が7月に

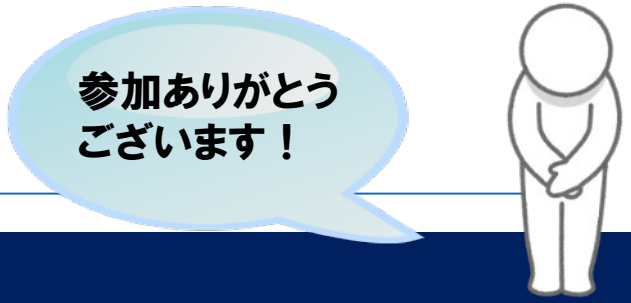


例年との違い・・・

①7月から開始・・・例年であれば、合宿で打ち解けている・・・

②オンライン開催？・・・先の見えない状況・・・

2020年度の参加企業



42社に参加していただきました。

正式名称	正式名称	正式名称
森永乳業株式会社	株式会社ミライト情報システム	株式会社JALインフォテック
株式会社J-POWERビジネスサービス	株式会社パソナグループ	ブレインズコンサルティング株式会社
大和ハウス工業株式会社	インテル株式会社	コニカミノルタ株式会社
コープ情報システム株式会社	株式会社LIXIL	ニッセイ情報テクノロジー株式会社
丸文株式会社	アクサダイレクト生命株式会社	株式会社富山富士通
日商エレクトロニクス株式会社	東海旅客鉄道株式会社	日本ハム株式会社
株式会社　中電シーティーアイ	第一生命情報システム株式会社	株式会社カジマアイシーティ
株式会社富士通エフサス	株式会社NTTデータ	旭化成株式会社
オリックス・システム株式会社	東日本旅客鉄道株式会社	三菱総研ＤＣＳ株式会社
IIMヒューマンソリューション	日立建機株式会社	株式会社JTB情報システム
株式会社読売新聞東京本社	ＪＦＥシステムズ株式会社	株式会社テプコシステムズ
メンロ・セキュリティ・ジャパン株式会社	ファイルフォース株式会社	帝人株式会社
日揮ホールディングス株式会社	日本水産株式会社	株式会社かんぽ生命保険
東芝インフォメーションシステムズ株式会社	鹿島建設株式会社	ＪＸアイティソリューション株式会社

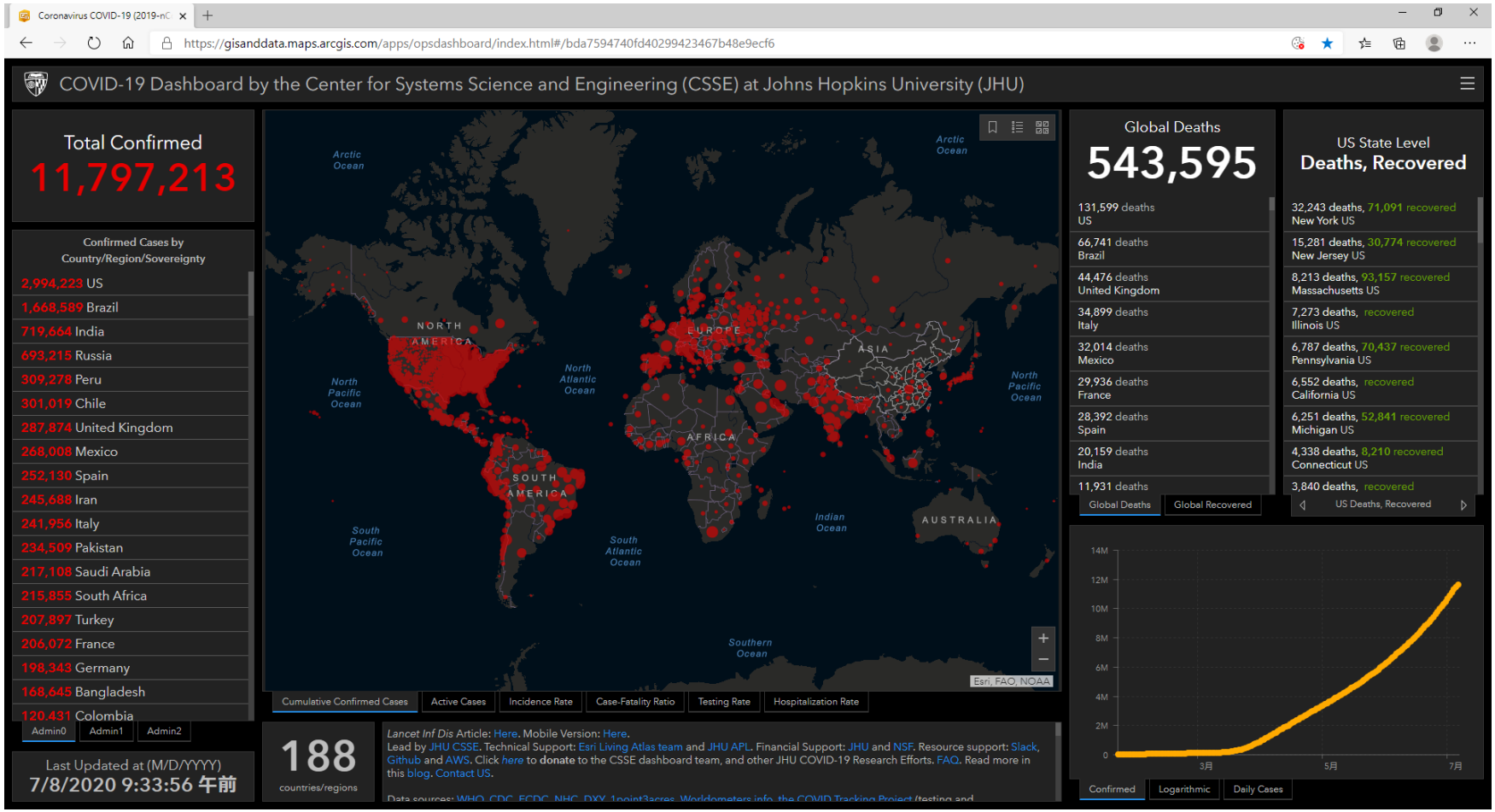
ようこそ “企業リスクマネジメント研究会” へ

42名の皆様にご参加いただきました。
よろしくお願いいたします。

ステータス	人　数
新規	26名
継続	13名
復帰	3名

【参考】 感染症リスク　7月8日

～ 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

2020年度　活動報告

ニューノーマルな活動スタイル

いままでのリスクメン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・・・

いままでの研究会は、対面によるディスカッション、親睦会によるより深い議論が重要であった。

THE 蜜

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。

あらたなスタイルのリスクメンジメント研究方法

全体会： 専門講師の講演＋各分科会の発表＋情報交換会

- 講演会は、オンラインで実施
- 情報交換会（宴会？）は、実施できず（一部Zoom懇親会実施）

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、あえて従来どおり。
  いろいろな事例・経験談を得るため。
- 分科会でも、情報交換会（宴会？）は実施できず
- オンラインでもチャタムハウスルールを維持・・・

合宿・現地見学会・会社訪問： 代案無し

- 開催当初は、秋にはハイブリッド形式も実施できると考えた・・・

ネット会議形式での分科会開催

ネット会議形式での分科会

- できる限りカメラオンでお願いします
- リーダもしくはサブリーダの司会にしたがってください
- 「挙手」機能も利用してください
- １回の発言は短めに！（これ大事！）
- ダメダシしない。
- 拍手機能使いましょう・・音鳴らないけど
- 全員発言しましょう！
- 結論を出すことが重要ではないので、自分が気になったことはなんでも発言して大丈夫です！（横道にそれてもOK!）

Chatham House Rule for ネット会議

ネット会議でもチャタムハウスルールを守ってください

- 会社では会議室で参加お願いします
- 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

2020年度の幹事団です（敬称略）

【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（株式会社LIXIL）
- COO　　坂　靖史（株式会社JALインフォテック）

【分科会】

- 分科会A　分科会長　：杉本 真一（森永乳業株式会社）
  - 副分科会長　：髙橋　奈央美（株式会社J-POWERビジネスサービス）
- 分科会C　分科会長　：寛座　勝巳（株式会社ミライト情報システム）
  - 副分科会長　：久冨 理佐子（株式会社パソナグループ）
- 分科会J　分科会長　：坂　靖史（株式会社JALインフォテック）
  - 副分科会長　：松谷　かのこ（ブレインズコンサルティング株式会社）

2020年度研究会：活動スケジュール

	日時	場所	テーマ （案）
第1回定例会	2020年7月9日（木） 15:00 ～ 17:30 定例会	ZOOM	• 顔合わせ／自己紹介 • 活動方針説明／グループ分け • 研究テーマ検討
第2回定例会	2020年8月6日（木） 13:30～15:30 分科会 15:30～18:00 全体会	ZOOM	• 分科会テーマ検討 • 分科会でのフリー討論 • 外部講師による講演
第3回定例会	2020年9月10日（木） 13:30～16:00 分科会 16:00～18:00 全体会	ZOOM	• 外部講師による講演 • 分科会実施 • シャッフル分科会
第4回定例会	2020年11月6日（金） 13:00～15:20 分科会 15:30～17:30 全体会	ZOOM	• 外部講師による講演 • 分科会実施 • シャッフル分科会
第5回定例会	2021年1月29日（木） 13:00～15:20 分科会 15:30～17:30 全体会	ZOOM	• 外部講師による講演 • 分科会実施 • シャッフル分科会
第6回定例会	2021年3月19日（金） 13:00～15:20 分科会 15:30～17:30 全体会	ZOOM	• 活動の振返り • 分科会活動結果発表

分科会

分科会

分科会

分科会

分科会

2020年度研究会：講演会

	日時	テーマ
第１回	８月６日（木）	• 丸紅ITソリューションズ　石橋様 「コロナ対策で情報システム部門が検討すべきリスク対策」
第２回	９月１０日（木）	• ミライト情報システム　寛座様 「当社のコロナ対応事例」 • 日商エレクトロニクス　荒尾様 「CISSP 取得体験談」
第３回	11月６日（金）	• コニカミノルタ　玉本様 「Security Management Office構想」 • クラウドネイティブ　齊藤様 「コロナ禍で話題なゼロトラストのリアル」
第４回	1月29日（金）	• 電気事業連合会　青木様 「電力データ活用と情報セキュリティ」

「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 （サイバーセキュリティ：技術系多め）
- 分科会B （セキュリティ＆BCP：マネジマント系）
- 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】

- 全体会開催日及び、10月、12月、2月に分科会を開催し、ディスカッション
- 担当者は、自己紹介と事例紹介
- 全員でディスカッション

2020年度　分科会
議論したテーマ

2020年度分科会A 主な研究テーマ

①セキュリティ人材の育成方法について
②SIEMの利用について
③ウイルス検知後の対応方法について
④テレワーク環境のセキュリティ対策について
⑤Webフィルタリング設定について
⑥クラウドサービスのセキュリティ対策について
⑦EDRについて
⑧脆弱性対応について
⑨脅威情報の活用について
⑩BEC詐欺対策について

2020年度分科会B 主な研究テーマ

①情報セキュリティポリシー、規程、ルール、および体系
②クラウド活用、SNS活用、評価ルール
③情報セキュリティ部門の役割と人材育成
④情報セキュリティ教育・訓練・演習
⑤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
⑥BYOD、シャドーIT対策、在宅勤務、働き方改革
⑦グループ会社、海外子会社ガバナンス、サプライチェーン
⑧BCP／事業継続
⑨新型コロナウィルス、パンデミック対応

2020年度分科会J 主な研究テーマ

①エンドポイントのセキュリティ対策
②情報セキュリティガバナンス強化の取り組み
③IT関連の中長期計画
④情報セキュリティ教育
⑤クラウドサービス利用時のセキュリティ
⑥グループ会社のセキュリティガバナンス
⑦メッセージングツールの業務利用
⑧IT投資と効果検証
⑨脆弱性診断
⑩セキュリティパッチの適用

2020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
・コロナ感染対策のためのテレワーク状況
・感染症(コロナ)対策
・BEC詐欺対策
・サプライチェーンマネジメント
・セキュリティ人材育成・教育
・クラウドサービス活用
・脆弱性情報の収集と対応
・エンドポイントセキュリティ対策
・PPAPへの対応

コロナ感染対策のためのテレワーク状況

各社のコロナ感染対策のためのテレワーク状況と課題

◆統計データ

コロナ以前から、テレワーク環境を用意していた企業（58%）
テレワークで利用したWeb会議サービス
　Teams（50%）、Zoom(25%)、WebEX
テレワーク環境　　VPN接続（58%）、VDI環境(34%)

◆トラブル事象

VPN通信が繋がらない、遅い
VPN環境を利用したが、外部デバイスへのデータコピーが増加
VPN環境だが、動画閲覧トラフィックが増加した・・・
自宅で業務情報を印刷している
テレワーク環境にセキュリティ対策が未実施。
テレワーク環境のパソコンの調査や対処を実施できる環境が必要
問い合わせ対応メンバーが在宅勤務なので、電話連絡ができない・・
派遣契約の方も在宅勤務のため、指示に時間がかかり効率が落ちた

コロナ感染対策のためのテレワーク状況

各社のコロナ感染対策のためのテレワーク状況と課題

◆制度的な課題

自宅の電気・通信代、通勤費などの補助に関する検討
ヘッドセット、大型ディスプレーなどの設備
作業用の椅子の要求
感染症対策（外出抑制）なのに、シェアオフィスの使用願いがある

◆その他

在宅勤務によりモラルは低下している・・・
　動画閲覧の増加、内部不正の発生、副業（布教活動、販売活動）の実施など
新入社員は、会社のルールの理解などのために、ある程度出社してもらうべき
会社オフィスが売却されている・・・（フロアが減っている）
作業の評価が難しい。

感染症(コロナ)対策

BCP観点でのコロナ対策

◆業務継続とのバランス

在宅では継続できない業務の洗い出し
在宅で実施した場合の作業効率の測定
出社抑制の基準の検討(会社側での指示、各自判断・・・)
代表電話、受付の対応

◆感染リスクレベルの定義

国・自治体の要請:緊急事態宣言など
関係者(委託先)から感染者発生の連絡を受けた場合の対応
自社で感染者が発生した場合の対応
(ビル閉鎖、フロア閉鎖など、複数人同時に感染した場合の対応)

◆事務所での感染防止対策

マスク着用、アクリル板の設置、ドア開放、消毒液の用意など
会議室の人数制限、出張の抑制、会食の禁止など

BEC詐欺対策

減らないBEC詐欺

◆BEC詐欺の発生状況

攻撃は減少していない。
新しい手口が使われる。
テレワークのためにメールサービスを社外から接続可能な状態としたため
アカウントを不正に利用されるリスクが高まった
２段階認証を突破するフィッシングにより、メールを悪用された

◆対策

「初めての送信元」からのメールを目立たせる、アラートを表示する
プロセスによる対策（複数人で対応、メールでの口座変更禁止など）
継続的なBEC詐欺の啓蒙教育
他社事例の社内周知

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管理方法

チェックリストによるセキュリティ対策の確認
NG（未実施）項目があっても、取引を停止するわけではない
NG（未実施）項目は、改善予定を申告してもらう
　対応期限を明示・基準に満たない場合は委託しない場合もあり

◆課題

子会社であれば、ガバナンスが効くが、委託先への指導が難しい
契約後のチェックでは効果が薄い、契約前に基準を提示すべき

◆企業買収時のセキュリティチェック

ISMS27001の取得を義務付ける
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。
メールの不正アクセス有無やデバイスのウイルス感染有無をチェック

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
申請をしなくても利用できてしまう(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
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
　アカウント管理、アクセス権管理の重要性が理解されていない

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？

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
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

◆EDRツールの導入と課題

「検知」機能なので、インシデントが減るわけではない。
「検知」後、遅滞無く対応できる体制の整備
外部SOCを活用しているが、「検知」後の報告に時間がかかる
リスクの低い検知への対応体制がない
予算の関係で、ツールは導入したが、監視は業務時間のみ
クラウドサービス側のサービス停止・遅延などのトラブルが発生

セキュリティ人材育成・教育

社員へのセキュリティリテラシーの普及

◆社員教育

「自分には関係ない」という意識を変えていただく
個人のミスから、情報漏洩が発生していることを周知
クラウドサービスの設定ミスから情報漏洩が発生していることを周知
ウイルス感染、フィッシングメールは、セキュリティ対策の不備という意識

◆課題

社内インフラ環境の具体的な利用方法を周知する必要がある
　社内ファイルサーバとパブリッククラウドのオンラインストレージの
　漏洩リスクの違い
　Web会議のレコーディングの確認、出席者の確認など
　クラウドサービス利用時のアクセス権管理（全員同一権限・・・）
　社給機器で利用するアプリは、セキュリティ的に問題ない？
　WiFiに違いがあるの？？

PPAPへの対応

内閣府による発表はあったが、問題点を明示されていない

◆PPAPについて

メール添付ファイルのZip暗号化利用の禁止に関する発表があったが、
厳密に問題点と代替方法が明示されていない。

◆対応状況

様子見。
売り込みが増加している

◆課題

URL方式に変更したが、メールの誤送信で結局は漏洩
Zip暗号化をやめても、相手先からZip暗号化ファイルが着信するので、
ウイルス対策にはならない・・・
原本のファイルにパスワード設定したが、パスワードを忘れて開けなくなった

まとめ

2020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
- 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）
- 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
- 会社から参加する場合は、会議室の確保が必要
- 会社からの業務割り込みが多い。
- 懇親会が無いのが残念

2020年度活動の振り返り（運営サイド・幹事団）

・オンライン開催でも、参加者の方にある程度「満足」の効果を
感じていただけた。

＝＞ ７月スタートとなり、活動期間が短かったが、参加者みなさんの協力で
有意義な情報交換・ディスカッションができた。

・分科会と全体会を同一日に実施しなくてもよい。

＝＞ オンラインなので、「移動」が無いので、１日に集約する必要がない。
オンラインなので、長時間拘束しないほうが効果的。

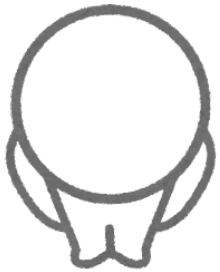
・分科会をより盛り上げるための改善

＝＞ 全員が発言する。ホワイトボード機能などで、キーワードを共有。など
反省点を改善して、議論を活発にできそう。

2020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

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

2021年も
よろしくお願いします！

以上