中国経済産業局委託業務

令和3年度中小企業サイバーセキュリティ対策促進事業
（中国地域におけるセキュリティコミュニティ形成事業）

事 業 報 告 書

令和4年3月

株式会社アシスト

令和3年度中小企業サイバーセキュリティ対策促進事業
（中国地域におけるセキュリティコミュニティ形成事業）

事業報告書

【 目 次 】

第1章　事業概要

1. 事業概要

1－1. 事業名　　令和3年度中小企業サイバーセキュリティ対策促進事業
（中国地域におけるセキュリティコミュニティ形成事業）

1－2. 発注者　　中国経済産業局

1－3. 受託者　　株式会社アシスト

1－4. 事業実施期間　　令和3年8月11日～令和4年3月31日

2. 事業目的

IoT、AI等の利活用は中小企業等のデジタル化や生産性向上に不可欠なものとなっている一方で、企業等が保有する顧客の個人情報や重要な技術情報等を狙うサイバー攻撃は増加傾向にあり、その手口は巧妙化している。また、新型コロナウイルス対応の一環でテレワーク等業務のデジタル化が急速に普及していることで、サイバー攻撃の脅威はより一層増大している。

こうした中、令和2年10月に中国経済産業局と中国総合通信局が共同事務局となり設立した「中国地域サイバーセキュリティ連絡会」（※1）や、中国経済連合会が事務局を務め中国地域の産学官で構成する「セキュリティ人材育成WG」（※2）等の活動により、中国地域においてセキュリティコミュニティの基盤が形成されつつあるものの、大都市圏と比較してサイバーセキュリティに精通した人材や人材育成のための学習の場等の不足が課題となっている。また、令和2年度実施した同事業（※3）においても、アンケートやヒアリング調査の結果、また、研修参加者の意見として、学習機会の充実を求める声が多数寄せられた。

そのため本事業は、中国地域において中小企業等のセキュリティ対策の中核を担える人材を育成する環境の充実を目指して、大学と連携した社会人向けの実務的なセキュリティ演習を実証的に実施するとともに、セキュリティ対策の促進に資するセミナーを開催することで、中国地域におけるコミュニティ全体のセキュリティレベルの底上げを図ることを目的とし実施した。

（参考）　※1 中国地域サイバーセキュリティ連絡会
https://www.soumu.go.jp/soutsu/chugoku/hodo_2020/01sotsu08_01001148.html
※2 セキュリティ人材育成WGの取組（中国地域産学官コラボレーション会議サイト内）
https://c-collabo.jp/
※3 令和2年度「中国地域におけるセキュリティコミュニティ形成事業」報告書
https://www.chugoku.meti.go.jp/research/seijyo/210421_2.html

3. 事業内容

3－1. 社会人セキュリティ人材育成講座

IoT・AI等のセキュアな活用を実践できる社会人セキュリティ人材の育成環境を充実するため、サイバーセキュリティに対する認識や対策の向上が求められる中小企業の技術者等を対象に、中国地域の経済界及び大学と連携したPBL演習（問題解決型学習）を実証的に実施した。

3－2. 中国地域サイバーセキュリティセミナー2022

中小企業のサイバーセキュリティに対する意識向上と対策強化を促すため、最新動向を踏まえたサイバーセキュリティセミナーをオンラインで開催した。

第2章　社会人セキュリティ人材育成講座

IoT・AI等のセキュアな活用を実践できる社会人セキュリティ人材の育成環境を充実するため、サイバーセキュリティに対する認識や対策の向上が求められる中小企業の技術者等を対象に、中国地域の経済界及び大学と連携したPBL演習（問題解決型学習）を実証的に実施した。

【講座における作業内容】

企画・準備	・連携機関との調整　・広報用チラシ（電子媒体）の作成及び広報 ・オンライン演習のための事前調整（配信手法の協議、各種手続き） ・各大学の演習講師謝金支払いの調整　・マニュアル／進行台本の作成
事務局対応	・申込み受付　・演習で使用する教材の受講者への発送作業 ・演習に関わる講義資料の配信、参加URL等の案内
事後業務	・アンケートのとりまとめ　・各種支払等手続

1. 開催内容

1－1. 講座名称等

名称：社会人セキュリティ人材育成講座
主催：経済産業省中国経済産業局、一般社団法人中国経済連合会
協力：国立大学法人岡山大学、広島市立大学
共催：総務省中国総合通信局、中国地域サイバーセキュリティ連絡会
運営：株式会社アシスト

1－2. 日時・場所・定員

開催方法	オンライン演習　※Cisco Webex にて
開催時期 演習概要 定　　員	**広島市立大学　サイバーセキュリティ入門演習** ①令和3年11月30日（火）13:00～15:00 ②令和3年12月 7日（火）13:00～15:00　　各回定員50名程度 ※1回目、2回目ともに同内容。 **岡山大学　マルウェア対策実践演習** ①令和3年12月2日（木）13:00～17:00 ／前編 ②令和3年12月9日（木）13:00～17:00 ／後編　定員20名程度 ※前編・後編セットでの受講

1−3. 広報

申　　込 ： 事前申込必要 （申込方法:メール）

費　　用 ： 無料

参加状況 ： 広島市立大学　サイバーセキュリティ入門演習

①令和3年11月30日(火)　事前参加申込者数　66名

②令和3年12月　7日(火)　事前参加申込者数　43名

岡山大学　マルウェア対策実践演習　　事前参加申込者数　23名

募集方法 ： 告知チラシ(A4サイズ、両面カラー、電子媒体にて)

主催者から、関係機関・団体等に対して、DMおよびメルマガ配信、

中国経済産業局HPへの掲載等にて募集告知を行った。

また、(株)アシストより、プレスリリース(計73件)、経済レポートへの

掲載依頼を行った。

▲講座告知チラシ

1−4. 実施運営担当者および講師

担当	氏名	所属
主催者	森脇　渉	中国経済産業局　地域経済部 製造・情報産業課
実施運営・司会	伊達　一徳	㈱アシスト　プロモーション事業部

	氏名	所属
講　師	稲村　勝樹　氏	広島市立大学　准教授
	石原　信也　氏	国立大学法人岡山大学　特任教授
	日下　卓也　氏	国立大学法人岡山大学　講師

2. 実施結果

2－1. 参加者数

広島市立大学　サイバーセキュリティ入門演習　※2回とも同内容にて実施

①令和3年11月30日(火)　62名　　②令和3年12月　7日(火)　36名

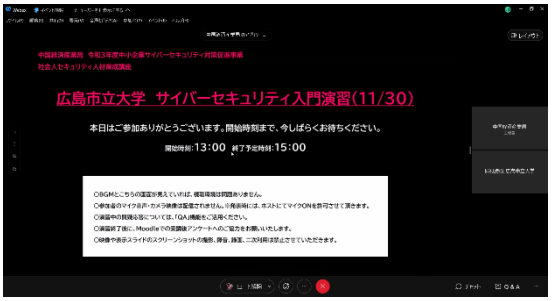
広島市立大学 稲村准教授により、近年のマルウェアの状況について講義形式で紹介するとともに、感染実例やその検証について講義いただいた。また、実際に各受講者に演習用のファイルをダウンロードしていただき、各自のデバイスにてマルウェア感染の挙動を体験してもらう作業なども行った。

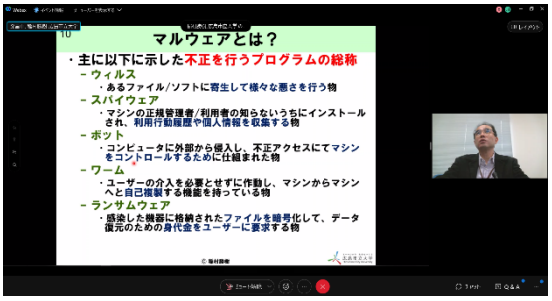
【実施詳細】

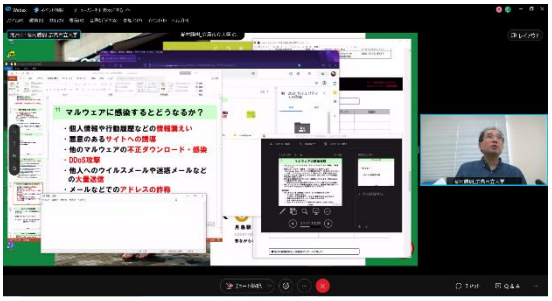
・当日演習に使用する配信ツール(Cisco Webex　Events)に関しては、中国経済産業局所有のアカウントを利用した。(11月29日(月)、13:15～稲村先生の接続チェック、テスト等実施。)

・受講者への配布資料等は、受講者へ事前登録頂いている岡山大学Moodle内へアップした。

・演習当日の配信会場は、(株)アシスト内会議室にて、有線インターネット回線にて実施。







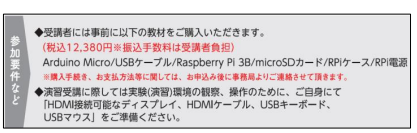
2. 実施結果

2－1. 参加者数

岡山大学　マルウェア対策実践演習　※前編・後編の2日間セットにて実施

①令和3年12月2日(木)　22名　　②令和3年12月9日(木)　21名

岡山大学 石原特任助教(前編ご担当)、日下講師(後編ご担当)により、受講者に事前に購入いただいた演習教材キット(BadUSBやRaspberry Piなど)を用いたマルウェア脅威の実体験と、パスワード入力によるセキュリティ対策の実装などを行った。前編・後編を通して、受講者は常に自身のデバイス環境にてオンライン講義を聴きながら作業を行い、質問対応や各受講者の進捗フォローなどは、岡山大学TA2名にてサポート・進行を行った。

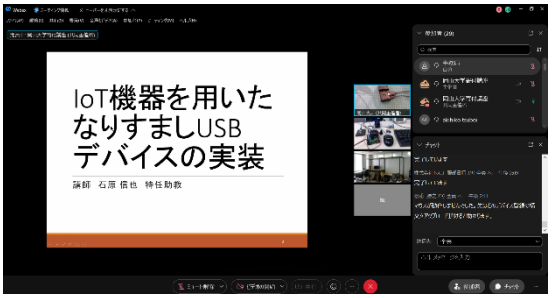


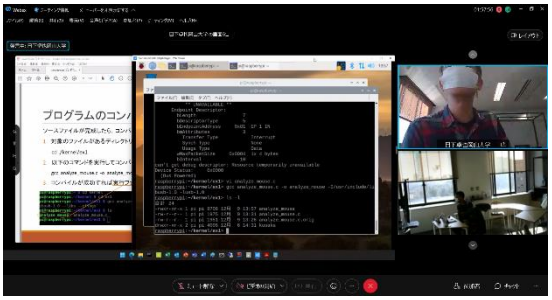
【実施詳細】

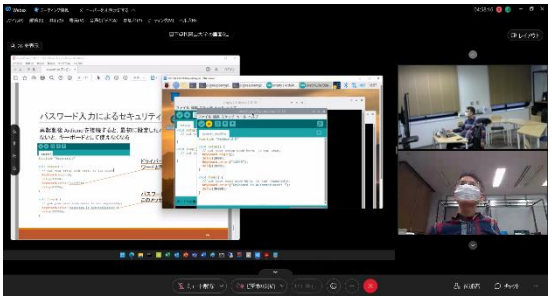
・当日演習に使用する配信ツール(Cisco Webex ミーティング)に関しては、岡山大学様にてご用意・運用した。

・受講者への配布資料等は、受講者へ事前登録頂いている岡山大学Moodle内へアップした。

・演習当日の配信会場は、岡山大学様学内にて、有線インターネット回線にて実施した。







2. 実施結果

2－2. 講座資料

国立大学法人岡山大学のeラーニングシステム（Moodle）を活用し、受講者へは
事前登録のうえ、各講座の講義資料等を閲覧いただける環境とした。
あわせて、オンライン演習に必要なアクセス方法などをまとめた資料をメール配布した。

【岡山大学Moodle内　資料内容】
・受講前アンケート　　・受講後アンケート
・広島市立大学　サイバーセキュリティ入門演習　講義資料（講座終了後に掲載）
・岡山大学　マルウェア対策実践演習　講義資料
・【ご紹介】おかやまIoT・AI・セキュリティ講座
※受講者への参考資料として、IoT・AI・セキュリティに関する20を超える専門的なVoD教材によるWEB講義と、実際にデバイスやプログラミングを用いたハンズオン・PBL演習を中心とした、岡山県内技術者のSociety5.0に向けたIoT・AIのセキュアな活用の底上げを狙う社会人人材の育成カリキュラムを公開。（岡山大学ご提供）

○岡山大学Moodle
「社会人セキュリティ人材育成講座2021」

○受講後アンケート

2－3. アンケート集計結果

両演習の受講者を対象に、岡山大学Moodleにて受講前・受講後アンケートを実施した。

受講前アンケート：回答者数　106名　／　受講後アンケート：回答者数　69名

2－3.(1)　受講前アンケート

1　本講座をどちらで知りましたでしょうか。

回答	平均	合計
中国経済連合会からのメール・WEB案内	53%	56
広島市立大学からのメール・WEB案内	2%	2
岡山大学からのメール・WEB案内	6%	6
その他（この後の自由記述にてお聞かせください）	43%	46
Total responses to question	100%	106/106

アンケート回答者の53%は、中国経済連合会からのメール・WEB案内での参加であった。その他内容に関しては、「中国経済産業局からのDM」「中国地域サイバーセキュリティ連絡会からの案内」など、関係機関・団体からの案内より参加にいたっている。

2　本講座の一部には実費（演習で必要となる機材の代金）を伴うものがございますが、受講エントリを検討される際の判断基準をお教えください。

回答	平均	合計
受講に必要となる機材は貸出・返却の手間があっても無料が良い	22%	23
返却の手間なども必要ない形で無料が良い	38%	40
実費1万円程度までなら有料でも良い	18%	19
有料・無料はさほど大きな判断材料ではない	19%	20
その他（この後の自由記述にてお聞かせください）	4%	4
Total responses to question	100%	106/106

無料を希望する方が60%を占めるなか、「有料でも良い」「有料・無料はさほど大きな判断材料ではない」が合わせて37%と、受講判断の際には得られるサイバーセキュリティ対策の知識・情報や、演習内容を重視する傾向がみられる。

2－3. アンケート集計結果

2ー3.(1)　受講前アンケート

3　本講座の一部には複数日に渡る演習があります。これは受講を検討する際の判断基準になりますでしょうか。

回答	平均	合計
1日だけで終わるものが良い	42%	45
内容によっては2日に渡るものでも良い	58%	61
その他（自由記述にてご意見をお聞かせください）	2%	2
Total responses to question	100%	106/106

「内容によっては2日に渡るものでも良い」が58%と高く、前述の受講の費用負担に関するアンケート結果と同様に、受講判断の際には得られるサイバーセキュリティ対策の知識・情報や、演習内容を重視する傾向がみられる。一方で、1日での実施を希望する方も、42%と一定数いることが見受けられる。

4　【自由記述】本講座を受講しようと思ったきっかけ・理由など、簡単にで結構ですのでお教えください。

（抜粋にて）

・今回の講習はラズベリーパイに興味があり、受講を決定しました。受講後、使用用途があるものであれば有料でも気になりません。
・ITシステムは日々複雑化しており、ウィルス関連の報道もよく目にするようになってきました。そういった状況において、セキュリティ対策は必須のものとなっており、少しでも知識習得に努めていきたいと考えています。
・OSCPという資格を取りたいと考えるくらいにサイバーセキュリティに興味があって少しでも学びたいと受講。
・サイバーセキュリティ対応の重要性は十分認識しており、受講料も無料であったので、今回の申込に至った。
・個人情報を取り扱うため知識を得たい。
・物理デバイスを使用する演習に興味をひかれた。
・ハンズオンで体験できるマルウェア対策講座はなかなかありません。座学だけでなく、ハンズオンやグループワーク中心のセキュリティセミナー（講座）を探しておりました。

2－3. アンケート集計結果

2－3.(2)　受講後アンケート

1　今回受講された演習すべてにチェックしてください。

回答	平均	合計
広島市立大学 サイバーセキュリティ入門演習	93%	64
岡山大学 マルウェア対策実践演習	23%	16
Total responses to question	100%	69/69

サイバーセキュリティ入門演習への参加者は、93%、マルウェア対策実践演習は23%（両演習受講含む）となっており、それぞれの特色に応じた受講結果となった。両演習とも、予定定員を超える参加となった。

2　貴社／貴団体の概要について、お教えください。

1）所在地について

回答	平均	合計
鳥取県	9%	6
島根県	6%	4
岡山県	41%	28
広島県	29%	20
山口県	10%	7
その他地域	6%	4
Total responses to question	100%	69/69

岡山県内の受講者が41%と一番多く、続きて広島県内の受講者が29%となっている。中国地域内の受講者が94%と大部分を占めるなか、中国地域外の受講も6%あった。（東京都、愛知県、奈良県、大阪府、福岡県、熊本県、計7名）

2－3. アンケート集計結果

2ー3.(2)　受講後アンケート

3　貴社／貴団体の概要について、お教えください。

2）従業員数について

回答	平均	合計
9人以下	4%	3
10～29人	7%	5
30～49人	7%	5
50～99人	13%	9
100人以上	68%	47
Total responses to question	100%	69/69

4　貴社／貴団体の概要について、お教えください。

3）業種について

回答	平均	合計
農林・水産	3%	2
建設業	1%	1
製造業	26%	18
電気・ガス	3%	2
運輸・通信業	7%	5
卸売・小売・飲食業	6%	4
金融・保険業	17%	12
不動産業	1%	1
サービス業	14%	10
その他	20%	14
Total responses to question	100%	69/69

製造業分野の受講者が26%と一番多い。金融･保険業やサービス業なども割合が高く、IoT、AI等の利活用やデジタル化の推進に取り組んでいる業種分野での受講者率が高い傾向がみられる。また、それ以外の業種もまんべんなく受講があり、幅広い業種でのサイバーセキュリティ対策に関する関心の高さがうかがえる。

2－3. アンケート集計結果

2ー3.(2)　受講後アンケート

5　本講座の満足度に関して、お聞かせください。

回答	平均	合計
満足	35%	24
やや満足	46%	32
普通	17%	12
やや不満	1%	1
Total responses to question	100%	69/69

「満足」「やや満足」を合計すると81%となり、おおむね受講者の満足度は高かった。

6　上記の質問（満足度）について、それを選んだ理由をお聞かせください。（記述式）

（抜粋にて）

・わかりやすい言葉で基本的な部分からの講座であり、とても理解がしやすかったと感じました。
・最近の動向であったり、実際に感染体験をしたり、感染事例について考えることで脅威に気付くことが出来ました。
また、弊社内のセキュリティやリテラシーの甘さを痛感させられました。
・事例自体はすでに聞いたことのあるものでしたが、なぜそれが問題なのか掘り下げた解説を聞けたことは
貴重でした。
・講義内容がケースに則った対応や防止策が説明されたので、分かり易く参考になりました。
・マルウェア対策など、実際に起こった事件をもとに考えさせられることが多かった。
・マルウェア対策などの知識が少なかったため、今回の入門講座で理解を深めることができました。初心者でも
分かりやすい表現で講義していただき、ありがたかったです。
・攻撃側を体験する機会はあまりないので、とても興味深かったです。
・実際のUSB経由のマルウェアの仕組みを知ることが出来たのは満足できた。
・ IT用語をそのまま使うだけではなく、用語の意味をわかりやすく丁寧に説明されていた。
・結構盛り沢山な内容だったので、実際の講義資料を手元に置きながらメモが取れると、より集中出来たと思う。
・基本的な内容でよい復習となった。マルウェア実例では、もう少し本物に近いものの挙動が見てみたかった。
・実践的でよかったです。キーロガーなどが体験できて面白かったです。
・広島市立大学と岡山大学（前編）はよかったが、岡山大学（後編）は、講師の進めるスピードが早く、
ついていけてない人が多かった印象がある。もっと小刻みに進捗を確認した方がよいのではないかと思った。
・講義内容について、やや難易度が高く、初学者にとっては分かりづらい部分が多々あり、講義についていけなく
なる場面があった。専門的な知識に対しての会話が多く、初歩的な受講者への配慮も必要だと感じた。
講義についていける基礎的なコマンドの方法などの資料の配布があれば、よりスムーズな受講につながったと思う。

おおむね演習内容について理解でき満足したコメントが多かったが、岡山大学のマルウェア対策実践演習に関しては、難易度が高く講義内容についていけなかったとの声もあった。受講者の基礎知識やスキルによる部分が大きいため、演習内容ごとに対象受講者のスキルや基礎知識を明確にする必要性を感じる。

2－3. アンケート集計結果

2－3.(2)　受講後アンケート

7　本講座の受講時間（ボリューム）に関して、お聞かせください。

回答	平均	合計
長い	1%	1
やや長い	12%	8
普通	80%	55
やや短い	4%	3
短い	3%	2
Total responses to question	100%	69/69

受講時間のボリュームに関しては、多くの受講者が適切と感じている。

8　本講座の難易度について、お聞かせください。

回答	平均	合計
難しい	1%	1
やや難しい	16%	11
普通	59%	41
やや易しい	20%	14
優しい	3%	2
Total responses to question	100%	69/69

難易度に関しては、「普通」が59%と一番多く、適切な難易度だったことが見受けられる。一方で、「やや難しい」が16%、「やや易しい」が20%と同程度の割合あり、受講者自身のスキルや基礎知識によってばらつきがある。

2－3. アンケート集計結果

2ー3.(2)　受講後アンケート

9　本講座を受講して、実務にどの程度活かせるとお考えでしょうか？

回答	平均	合計
十分活かせる	28%	19
ある程度活かせる	58%	40
どちらとも言えない	14%	10
Total responses to question	100%	69/69

「十分活かせる」「ある程度活かせる」を合わせると86%と高く、セキュリティ人材の育成やレベルの向上、サイバーセキュリティに対する機運醸成に寄与したと考えられる。

10　来年度より高いレベルの講座を開催した場合に受講したいですか？

回答	平均	合計
是非受講したい	26%	18
（タイミングがあえば）受講したい	59%	41
どちらとも言えない	13%	9
あまり受講したくない	1%	1
Total responses to question	100%	69/69

「是非受講したい」「(タイミングがあえば)受講したい」を合わせると85%と高く、サイバーセキュリティに関する情報収集や演習参加のニーズが高いことが分かる。

2－3. アンケート集計結果

2－3.(2)　受講後アンケート

11　開催手法について、ご要望をお聞かせください。

回答	平均	合計
会場でのリアル開催	4%	3
オンライン開催	58%	40
リアルとオンラインの同時開催	16%	11
とくに希望はない	22%	15
Total responses to question	100%	69/69

開催手法については、「オンライン開催」が58%と一番多く、受講者にとって距離的制約なく参加できるオンラインのニーズが高いことが見受けられる。今回のPBL演習（問題解決型学習）について、「会場でのリアル開催」希望は4%と低く、オンラインでの演習実施については、実施運営上の障害や受講しにくさなどはなかったと考えられる。

12　サイバーセキュリティに関して、関心の高い内容をお聞かせください。（複数回答可）

回答	平均	合計
最新動向について	72%	50
セキュリティ対策について	90%	62
被害事例について	54%	37
セキュリティ人材育成について	57%	39
DX関連	42%	29
支援制度について	10%	7
その他	1%	1
Total responses to question	100%	69/69

「セキュリティ対策について」が90%と一番多く、続いて「最新動向について」が72%と高い数値を示している。「被害事例について」「セキュリティ人材育成について」も50%を超える値となっており、サイバーセキュリティに対して、総じて高い関心が伺える。（その他1件：リモートワークやクラウド利用に伴う注意点）

2－3. アンケート集計結果

2ー3.(2)　受講後アンケート

14　そのほか、ご要望やご意見などありましたら、自由にご記入ください。　（抜粋にて）

非常に勉強になりました。一般で学ぶ事が出来ない内容でしたので貴重な経験となりました。
2日目は特に内容が難しく、ついていくのがやっとでした。恐らくプログラミングを知らない方も受講されていたではないかと思うので、講習のチラシにそういった旨の記載があればよかったかと思いました。

大変勉強になりました。ありがとうございました。

普段から常識として行っていたことが実は非常識であったことが分かったこともあり、大変参考になりました。

結構盛り沢山な内容だったので、実際の講義資料を手元に置きながら講義のメモが取りたかったです。

動向、事例からの対策、などのセミナーには今後も積極的に参加したいです。定期的に開催していただけると嬉しいです。

大変勉強になりました。業務に活かせるよう努めていきたいと思います。

貴重な講座を受講させていただきありがとうございました。

うまく動かなかった場合、取り残されてしまい。講師の先生が話している重要な事がまったく聞けず目の前の不具合対処に追われた。もう少し、お話を聞ける状況がよかった。終わってみて、「ただの作業を行った」というのが感想です。

被害を防ぐ方法を、もう少し具体的にあ事例を出していただきたかった。その内容を、自社に展開したいです。

セキュリティ業務に携わることになりましたが、経験と知識が少ないためこうした講義は大変参考になりました。
最新のセキュリティ脅威動向など情報収集のため、今後も講義があれば参加したいです。貴重なお時間ありがとうございました。

万が一マルウェアに感染してしまった際にどのような手順を踏むべきであるか、個人情報等が流出してしまったときの対応など、被害にあった後の具体的な解説があるとよりよいかなと思いました。

今回学んだことを出来るだけ、活かしていけるようより勉強したいと思います。

コンピュータやスマートフォン等は常に世界と繋がっていることを再認識することができました。また、マルウェアにはたくさんの不正方法があることが分かり、特にファイルを暗号化するランサムウェアに感染しない対策が重要であることが理解できました。

3. 考察と展望

3－1. 考察

社会人セキュリティ人材育成講座については、岡山大学、広島市立大学によるそれぞれ特色のある講座内容で、受講者の満足度は高かった。また、岡山大学のマルウェア対策実践演習に関しては、教材キットを実費購入する必要があったにもかかわらず予定の定員を上回る参加があった。これは、受講の際の判断基準に、「サイバーセキュリティ対策について得られる知識や情報量」や、「座学だけでなく、ハンズオンやグループワークなど、実践的かつ高度な演習」などを重視する傾向があると考えられる。

一方で、参加者の感想や要望をみると、おおむね演習内容について理解でき満足したコメントが多かったが、岡山大学のマルウェア対策実践演習に関しては、難易度が高く講義内容についていけなかったとの声もあった。受講者の基礎知識やスキルによる部分が大きいため、演習内容ごとに対象受講者のスキルや基礎知識を明確にする必要性を感じる。

開催手法に関しては、受講後のアンケート結果から「オンライン開催」が58%と一番多く、受講者にとって距離的制約なく参加できるオンラインのニーズが高いことが見受けられる。今回のPBL演習（問題解決型学習）について、「会場でのリアル開催」希望は4%と低く、オンラインでの演習実施について、実施運営上の障害や受講しにくさなどはなかったと考えられる。

3－2. 今後の展望

社会人セキュリティ人材育成講座については、ご協力いただいた岡山大学、広島市立大学のご尽力もあり、概ね受講者から評価を受け、受講者のサイバーセキュリティに対する関心や受講意欲も高いため、今後も継続して実施されることが期待される。また、サイバーセキュリティ対策やセキュリティ人材育成に向けた学習機会の充実を求める声があるなか、受講希望者の知識やスキルはそれぞれ異なるため、実施する演習内容とのミスマッチが懸念される。今後の検討・課題として以下の内容が考えられる。

○継続した社会人セキュリティ人材育成講座の実施について

・演習内容企画段階から、引き続き中国地域の経済界や大学と密な連携

・セキュリティ対策の中核を担える人材育成に向けた、受講対象者の詳細なニーズ把握

・演習実施に向けた各関係機関の明確な役割分担と体系化

例）広報・受講募集に関する分野（中国地域サイバーセキュリティ連絡会、経済界の各団体や機関など）

講座運営事務局対応分野（オンライン講義も含めた研修運営ノウハウのある事業者など）

演習カリキュラム構築・講義分野（岡山大学・広島市立大学をはじめとする中国地域内の各大学など）

○受講者の知識・スキルと演習内容のミスマッチ解消について

・サイバーセキュリティに関する知識やスキルなどに応じた、受講対象者区分の検討

・演習カリキュラム構築時における、対象者の明確化

・告知募集時における分かりやすいアナウンスと、事前のカリキュラム内容（詳細）提示

第3章　中国地域サイバーセキュリティセミナー2022

中小企業のサイバーセキュリティに対する意識向上と対策強化を促すため、最新動向を踏まえたサイバーセキュリティセミナーをオンラインで開催した。

【セミナーにおける作業内容】

企画・準備	・講師との調整　・広報用チラシ（電子媒体）の作成及び広報 ・オンライン配信ツールの手配、事前調整（配信手法の協議、各種手続き） ・講師謝金支払いの調整　・マニュアル／進行台本の作成
事務局対応	・申込み受付　・セミナー資料準備　・各講師との事前調整／接続テスト ・講義資料の配信、参加URL等の案内
セミナー運営	・配信機材の設営／テスト　・オンラインセミナー当日の運営及び司会 ・配信オペレート業務
事後業務	・アンケートのとりまとめ　・各種支払等手続

1. 開催内容

1－1. セミナー名称等

名称：中国地域サイバーセキュリティセミナー2022
主催：経済産業省中国経済産業局
共催：総務省中国総合通信局、中国地域サイバーセキュリティ連絡会
運営：株式会社アシスト

1－2. 日時・場所・定員

開催方法	オンライン配信　※配信ツールは　Cisco Webexミーティング
開催時期	令和4年3月2日（水）　13：00～16：00
開催概要	12：30～　参加者入室開始 13：00～　開会・主催者挨拶 13：10～14：40　基調講演（90分間） 14：40～14：50　休憩（10分間） 14：50～15：35　情報提供（45分間） 15：35～15：55　事例発表（20分間） 15：55～16：00　閉会挨拶

1－3. 広報

申　　込 ： 事前申込必要 （申込方法:メール）

費　　用 ： 無料

参加状況 ： 事前参加申込者数　142名

募集方法 ： 告知チラシ(A4サイズ、両面カラー、電子媒体にて)
中国経済産業局より、関係機関・団体等に対してDMおよびメルマガ配信、
中国経済産業局HPへの掲載等にて募集告知を行った。
また、(株)アシストより、プレスリリース(計91件)、経済レポートへの
掲載依頼を行った。

▲セミナー告知チラシ

1－4. 実施運営担当者および講師

担当	氏名	所属
主催者	森脇　渉	中国経済産業局　地域経済部 製造・情報産業課
実施運営・司会	伊達　一徳	㈱アシスト　プロモーション事業部

	氏名	所属
主催者挨拶	大倉　司郎	中国経済産業局　地域経済部 製造・情報産業課長
基調講演	名和 利男　氏	株式会社サイバーディフェンス研究所 専務理事/上級分析官
情報提供	佐藤　裕一　氏	独立行政法人情報処理推進機構　IPAｾｷｭﾘﾃｨｾﾝﾀｰ 企画部　中小企業支援ｸﾞﾙｰﾌﾟ　研究員
事例発表	有賀　成一　氏	リカザイ株式会社　経営管理統括　取締役統括部長

2. 実施結果

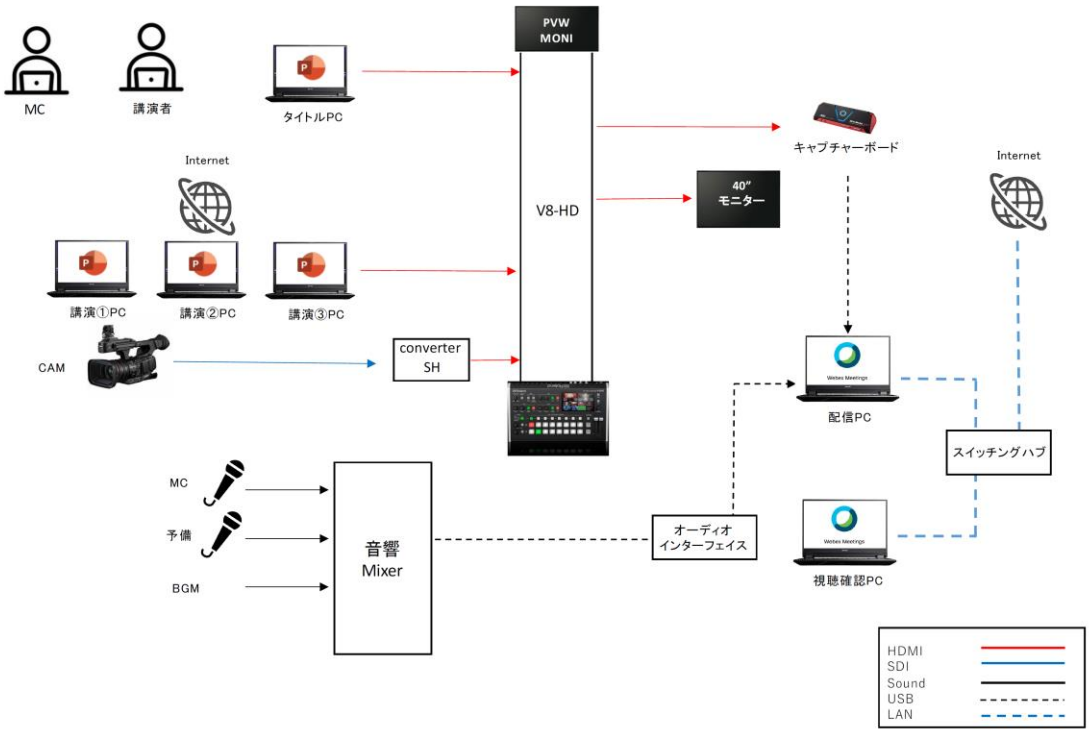
2－1. 参加者数

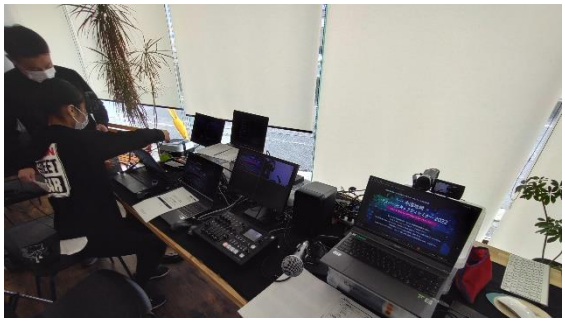
セミナー参加者　132名

2－2. 本番実施状況

当日配信会場に関しては、映像・音響・配信担当の（株）コネクトライン内会議スペースにて配信。（広島県広島市西区大宮3丁目2-7　104）

【配信システム図】





▲会場設営・セッティング状況①

▲配信開始時（スタンバイ画面）

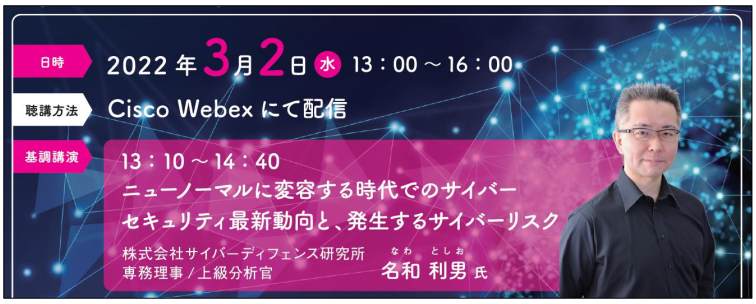
2. 実施結果

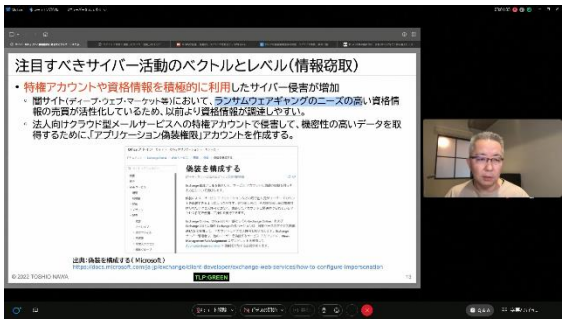
2－3. 参加者数

セミナー参加者　132名

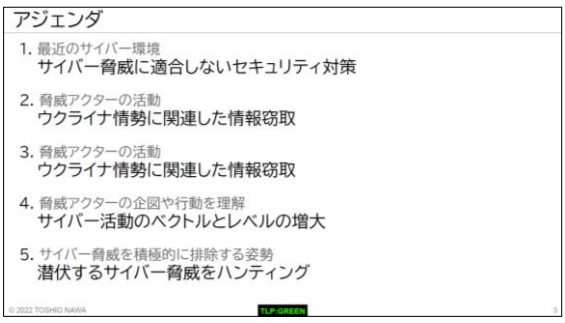
□基調講演　実施概要

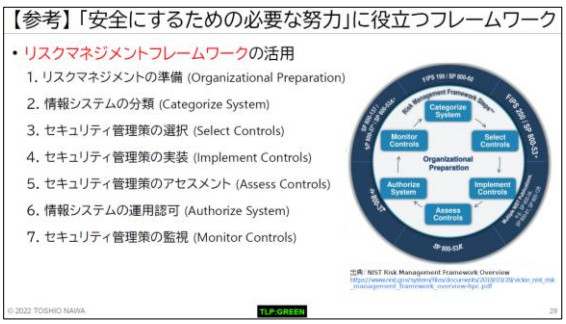
講　　師　：株式会社サイバーディフェンス研究所　専務理事/上級分析官
　　名和　利男(なわ　としお)氏
タイトル　：「ニューノーマルに変容する時代でのサイバーセキュリティ最新動向と、
　　発生するサイバーリスク」
講演時間　：13:10～14:40（90分間）
概　　要　：最新のロシア・ウクライナ情勢を踏まえながら、サイバー攻撃の最新動向から、
　　脅威アクターの活動内容やサイバー脅威を積極的に排除する方法などについて、
　　ご講演をいただいた。





▲基調講演の様子





▲講義資料

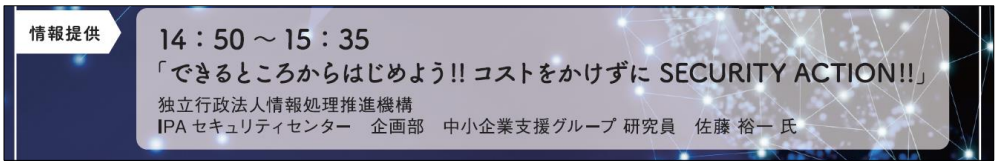
2. 実施結果

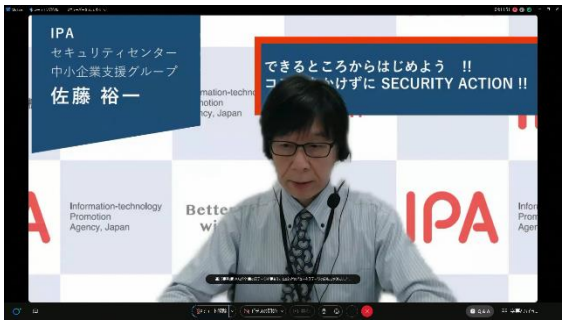
2－3. 参加者数

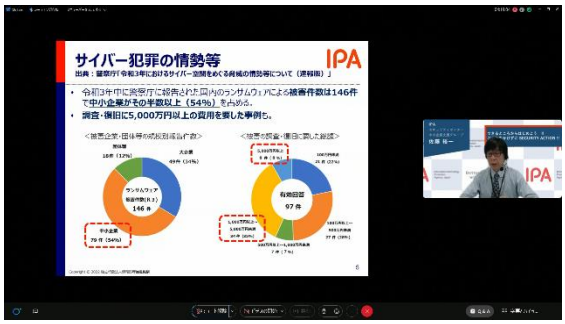
セミナー参加者　132名

□情報提供　実施概要

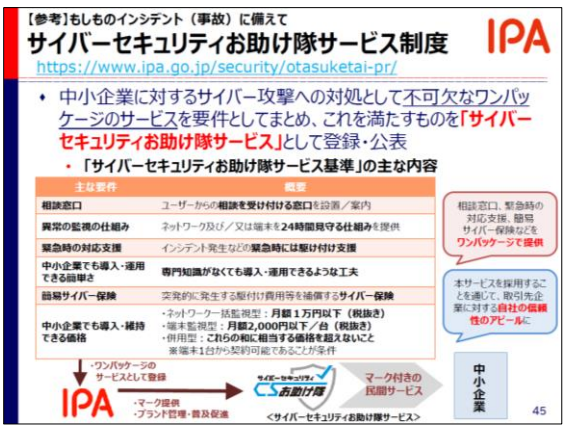
講　　師　：独立行政法人情報処理推進機構　IPAセキュリティセンター
　　企画部　中小企業支援グループ　研究員　佐藤　裕一(さとう　ゆういち)氏
タイトル　：「できることからはじめよう!!コストをかけずにSECURITY ACTION!!」
講演時間　：14:50～15:35（45分間）
概　　要　：サイバー犯罪の情勢や2022情報セキュリティ10大脅威などについて説明いただいたのち、SECURITY ACTION制度を踏まえながら、中小企業の情報セキュリティ対策について情報提供をいただいた。







▲情報提供の様子



▲講義資料

2. 実施結果

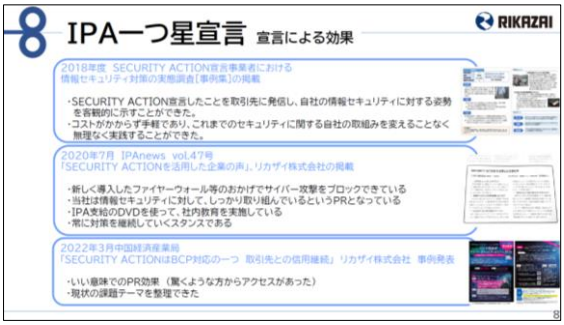
2－3. 参加者数

セミナー参加者　132名

□事例発表　実施概要

講　　師　：リカザイ株式会社　経営管理統括　取締役統括部長　有賀　成一(ありが　せいいち)氏
タイトル　：「SECURITY ACTION はBCP対応の一つ、取引先との信用継続」
講演時間　：15:35～15:55（20分間）
概　　要　：中小企業におけるサイバーセキュリティ対策実践の事例紹介として、IPA一つ星宣言に至った経緯から、自社におけるサイバーセキュリティ対策や今後の課題などについて発表を頂いた。

▲事例発表の様子



▲講義資料

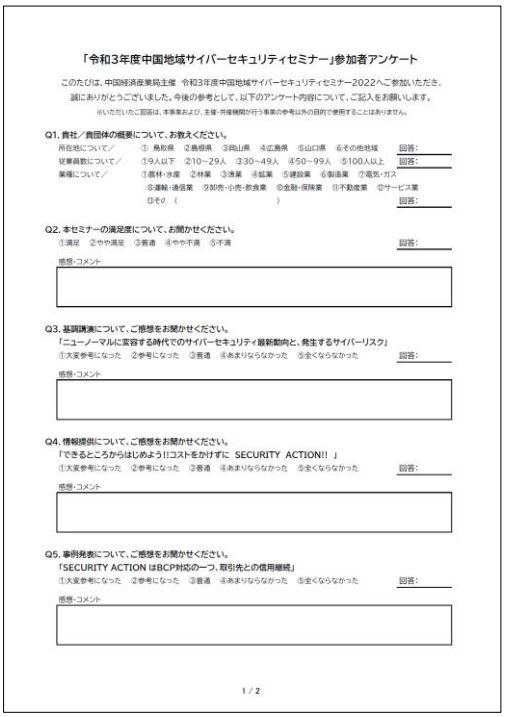
2. 実施結果

2－4. セミナー資料

・各講師資料（事前にセミナー参加者に対し、事務局よりメール送付）

・セミナー参加者アンケート（セミナー終了後に、参加者へ事務局よりメール送付・回収）

○セミナー参加者アンケート



「令和3年度中国地域サイバーセキュリティセミナー」参加者アンケート

このたびは、中国経済産業局主催 令和3年度中国地域サイバーセキュリティセミナー2022へご参加いただき、誠にありがとうございました。今後の参考として、以下のアンケート内容について、ご記入をお願いします。

※いただいたご回答は、本事業および、主催・共催機関が行う事業の参考以外の目的で使用することはありません。

Q1. 貴社／貴団体の概要について、お教えください。

所在地について／　①鳥取県　②島根県　③岡山県　④広島県　⑤山口県　⑥その他地域　回答：

従業員数について／　①9人以下　②10～29人　③30～49人　④50～99人　⑤100人以上　回答：

業種について／　①農林・水産　②林業　③漁業　④鉱業　⑤建設業　⑥製造業　⑦電気・ガス　⑧運輸・通信業　⑨卸売・小売・飲食業　⑩金融・保険業　⑪不動産業　⑫サービス業　⑬その（　）　回答：

Q2. 本セミナーの満足度について、お聞かせください。

①満足　②やや満足　③普通　④やや不満　⑤不満　回答：

感想・コメント

Q3. 基調講演について、ご感想をお聞かせください。

「ニューノーマルに変容する時代でのサイバーセキュリティ最新動向と、発生するサイバーリスク」

①大変参考になった　②参考になった　③普通　④あまりならなかった　⑤全くならなかった　回答：

感想・コメント

Q4. 情報提供について、ご感想をお聞かせください。

「できるところからはじめよう!!コストをかけずに SECURITY ACTION!! 」

①大変参考になった　②参考になった　③普通　④あまりならなかった　⑤全くならなかった　回答：

感想・コメント

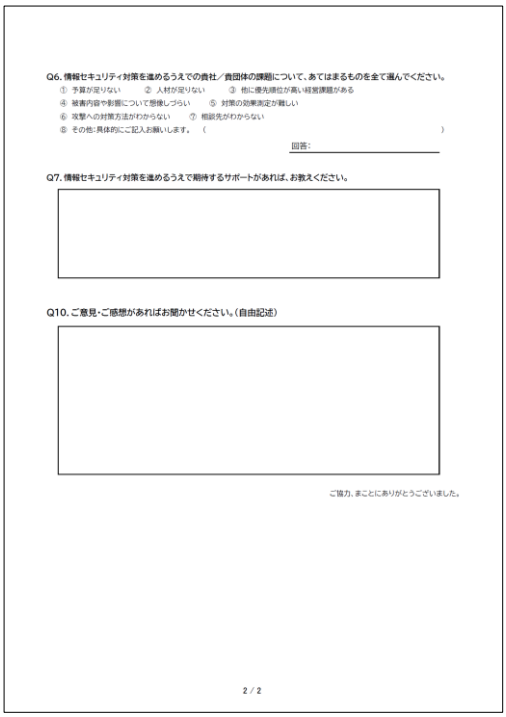
Q5. 事例発表について、ご感想をお聞かせください。

「SECURITY ACTION はBCP対応の一つ、取引先との信用継続」

①大変参考になった　②参考になった　③普通　④あまりならなかった　⑤全くならなかった　回答：

感想・コメント

1 / 2



Q6. 情報セキュリティ対策を進めるうえでの貴社／貴団体の課題について、あてはまるものを全て選んでください。

① 予算が足りない　② 人材が足りない　③ 他に優先順位が高い経営課題がある

④ 被害内容や影響について想像しづらい　⑤ 対策の効果測定が難しい

⑥ 攻撃への対策方法がわからない　⑦ 相談先がわからない

⑧ その他：具体的にご記入お願いします。（　）

回答：

Q7. 情報セキュリティ対策を進めるうえで期待するサポートがあれば、お教えください。

Q10. ご意見・ご感想があればお聞かせください。（自由記述）

ご協力、まことにありがとうございました。

2 / 2

2－5. アンケート集計結果

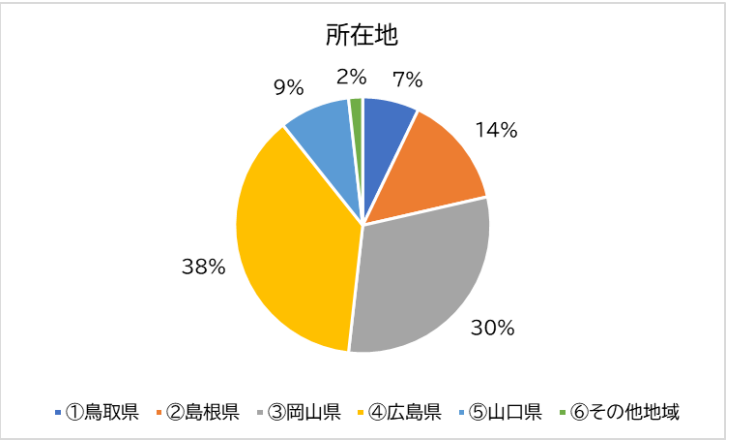
アンケート回答者数　56件　／　回収率　42.4%

Q1. 貴社／貴団体の概要について、お教えください。

1)所在地

項目	人数	割合
①鳥取県	4	7%
②島根県	8	14%
③岡山県	17	30%
④広島県	21	38%
⑤山口県	5	9%
⑥その他地域	1	2%
合計	56	100%

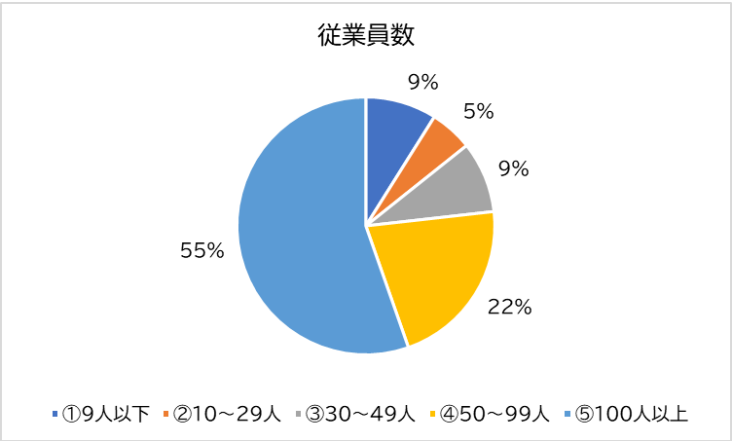
広島県内の参加者が38%と一番多く、続きて岡山県内が30%となっている。中国地域の参加者が98%を占めるなか、中国地域外からの参加も2%あった。
（東京都、大阪府、計4名）



2)従業員数

項目	人数	割合
①9人以下	5	9%
②10～29人	3	5%
③30～49人	5	9%
④50～99人	12	22%
⑤100人以上	31	55%
合計	56	100%

100名以上の事業者規模が55%、100名未満の事業者規模が45%と、幅広い事業者規模の参加があったことが見受けられる。



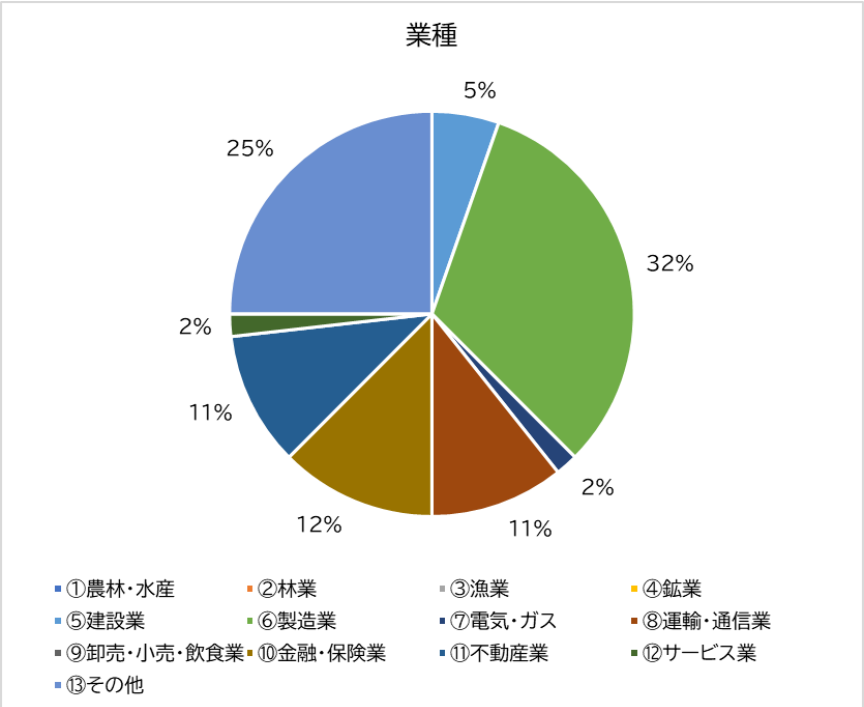
2－5. アンケート集計結果

3)業種

項目	人数	割合
①農林・水産	0	0%
②林業	0	0%
③漁業	0	0%
④鉱業	0	0%
⑤建設業	3	5%
⑥製造業	18	32%
⑦電気・ガス	1	2%
⑧運輸・通信業	6	11%
⑨卸売・小売・飲食業	0	0%
⑩金融・保険業	7	12%
⑪不動産業	6	11%
⑫サービス業	1	2%
⑬その他	14	25%
合計	56	100%

「製造業」が32%と一番多く、「運輸・通信業」「金融・保険業」「不動産業」で34%となり、製造業と合わせると66%と半数以上を占める。

（その他業種について）
・情報サービス業　・放送業
・研究開発　・ITソフトウェア開発
・自営業　・情報処理業
・行政サービス／公的支援団体　など

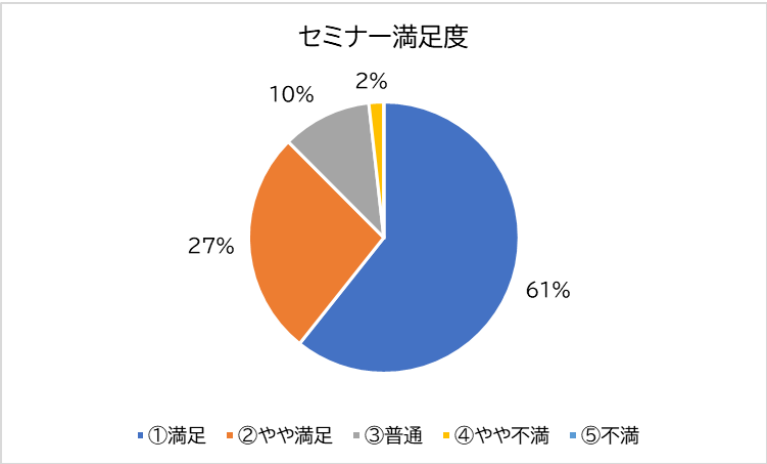


2－5. アンケート集計結果

Q2. 本セミナーの満足度について、お聞かせください。

項目	人数	割合
①満足	34	61%
②やや満足	15	27%
③普通	6	10%
④やや不満	1	2%
⑤不満	0	0%
合計	56	100%

「満足」「やや満足」を合わせると88%となり、
おおむね参加者の満足度は高かった。



■感想・コメント

○セキュリティ対策を考える上で、最新の情報を聞けるのは大変参考になりました。

○現在当社でも、IPAの情報セキュリティ関連規定をもとにルール作りを行っているので、とても参考になった。

○セキュリティに関する現在厳しい状況について、認識させて頂きました。

○基調講演内容が衝撃的で興味深かった。

○当社は、ランサムウエア被害の徳島の病院と同じFortiGateを使っており、Emotetの攻撃が増えてきていたりと
いつ被害を受けるかヒヤヒヤしている中、最新動向を入手出来て大変参考になりました。

○参考になることばかりでした。ネットワークの知識が乏しく、ネットワークの基礎から始まる講座もあると非常に助かります。

○弊社の取引先でサイバー攻撃があったばかりのタイムリーなセミナーで非常にためになりました

○昨今のウクライナ情勢について詳細に話をしてもらい、知見を深めることができよかった。

○その他さまざまなセミナーと比較して、特にIPA様にご説明頂いた内容は具体性を感じた。
また、インシデント発生時にの対応についても、具体的でわかりやすかった。

○情報セキュリリティを考えるうえで重要なことを分かりやすく説明して頂き、また実際に問題が起こった時に
どこに相談すれば良いか不安であったが、それもIPAに相談できることがわかり大変有益であった。

○改めて最近のマルウェアなどを利用したサイバー攻撃についてや、それに対する対策というものが理解できた。

○直近の世界情勢の脅威インシデントについての説明は危機感を持てた。IPA殿のサイバーセキュリティ―お助け隊や
無償に近いサイバーセキュリティ資料など、社内展開しやすい情報で有益と考えます。

○現状の世界情勢に合わせてセミナーが進み、セキュリティ状況について理解できました。

○事前に資料をいただけたことで目を通すことができた。内容も全般的にわかりやすく理解できた。

○脅威に対する対応はそれぞれ異なるというのもわかるのですが、もう少し具体的な対策をきいてみたかったです。

○中小企業でもできる具体的な対策について、もう少し時間があれば良かったと思います。

○現在も続々と攻撃メール(EMOTET)が届いており、緊張感の中で視聴させて頂いた。

○費用対効果や人や時間が限られた中で、具体的かつ段階的に何をしていくのかがもっと分かりやすいとよい。

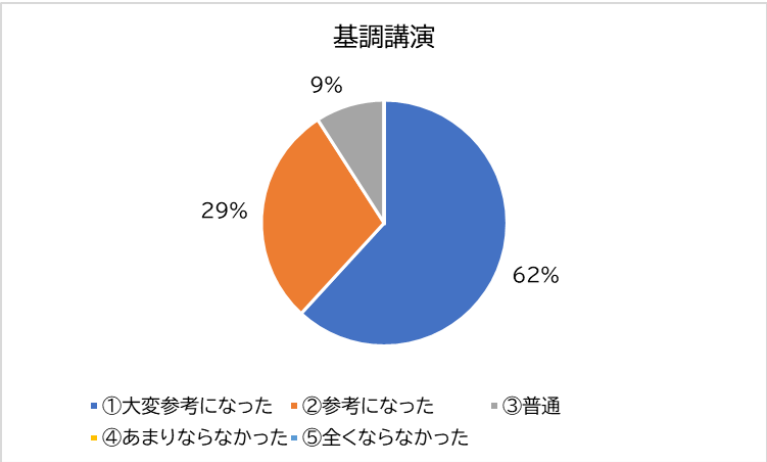
2－5. アンケート集計結果

Q3. 基調講演（名和氏）について、ご感想をお聞かせください。

項目	人数	割合
①大変参考になった	34	62%
②参考になった	16	29%
③普通	5	9%
④あまりならなかった	0	0%
⑤全くならなかった	0	0%
合計	55	100%

※都合により聴講できず：1名あり

基調講演に関しては、「大変参考になった」「参考になった」を合わせると91%にのぼり、多くの方が講演内容に満足していることが伺える。



■感想・コメント

○名和様の講演は非常に生々しく、たいへん参考になりました。

○最新のウクライナ情報が聞けて、セキュリティに対する考え方を、改めて検討する機会を与えてもらいました。

○昨年から増えているウィルス被害の理由と世界の動きの動向がよく分かりました。

○サイバー攻撃の流れを把握することができました。

○ウィルス対策とサーバー攻撃の対策は別物ということがよくわかり、今後の対策方法に役立てたいと思いました

○ウクライナ侵攻の裏で動いていたサイバー部分を興味深く聞かせていただいたと共に、さまざまな対策を講じる必要性を感じました。

○マスコミでは、聞かれなかったロシアでのウクライナに対するランサムウェア攻撃の準備段階からの様子に興味をもった。

○最近の事例とともに説明があったため、サイバーリスクが身近に潜んでいることを改めて感じた。

○直近の世界情勢の脅威インシデントについての説明は危機感を持てた。感覚として年2回ほど同様の直近のサイバー情勢を教わる機会があると良いなと考えています。

○本当の専門家の講義で、非常に参考になりました。ニューノーマルについても興味があったので、その視点でも講義があればと思います。

○現在進行形で発生しているサイバー侵害を交えての話で非常に危機感を感じました。今後セキュリティ対策に関して、対策ソフトを入れるではなく、今の脅威は何か考える、それに対してどんな手を打つことが必要か考えながら取り組みます。

○現状抱えている課題とギャップが大きいのですが、大変興味深く伺うことができました。
リスクマネジメントフレームワークについて、利用方法を教えていただけるとありがたいです。

○情報量と情報の鮮度は良いが、中小企業レベルで何をどうすれば良いかを判断する上で、具体的なアクションをとるための判断がしにくいと思った。

○弊社が攻撃されたら一溜まりもないと思いました。C2通信とか勉強になりました。

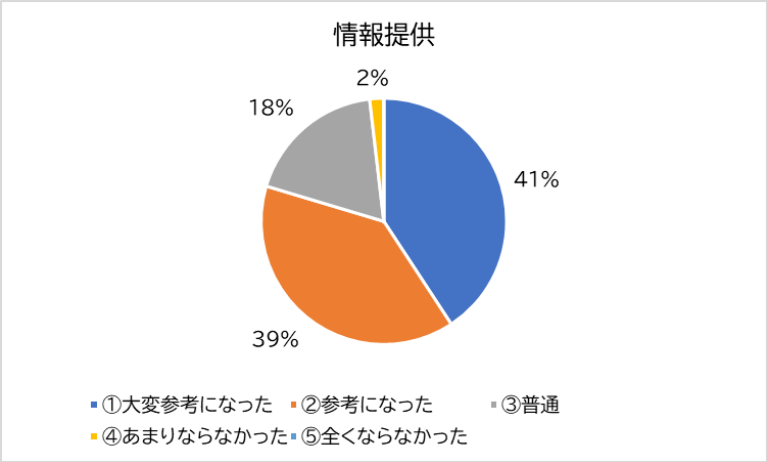
2－5. アンケート集計結果

Q4. 情報提供(佐藤氏)について、ご感想をお聞かせください。

項目	人数	割合
①大変参考になった	22	41%
②参考になった	21	39%
③普通	10	18%
④あまりならなかった	1	2%
⑤全くならなかった	0	0%
合計	54	100%

※都合により聴講できず：2名あり

情報提供に関しては、「大変参考になった」「参考になった」を合わせると80%となり、おおむね参加者の満足度は高かった。



■感想・コメント

○メールアドレス・パスワードが流出しているか？確認できるサイトは大変参考になりました。

○早速、自己診断を行い、自社の弱いところが確認できました。今後の取り組みの参考にさせていただきます。

○紹介されたメールアドレス流出を早速確認したところ、社員数名の流出があり驚きました。
コストはかけにくいですが、紹介された内容を参考に一つずつ対策を施していこうと感じました。

○非常に参考になりました。情報を整理して、貴社においてもセキュリティについて考えたいと思います。

○バックアップの重要性について、弊社でも2重3重にバックアップは行っていたがバックアップの時にだけ接続する意味が重要と改めて理解できてためになった。

○IPAさんの情報はいつも参考にさせていただいてます。資料を社員教育にも使わせてもらってます。

○できるところからはじめようは、中小企業にとっては実効性が高い。

○今後、社内でセキュリティに関する規定などを策定・展開予定でしたので大変参考になりました。

○SECURITY ACTIONを実施しようと考えていたのですが、運用上どうしても「情報セキュリティ5か条」ができないものがあり、そこから先をどうすればよいか迷っています。

○弊社は1年以上前よりIPA様のご指導を受け情報セキュリテイについて対応を進めているところです。
新型コロナ等の影響もあり進捗は不十分ですが重要性を認識しているところです。

○サイバー犯罪の最初の攻撃の9割以上はメールから始まるという事を再認識しました。

○SECURITY ACTION制度等、利用しやすい制度・ツールや資料等をご紹介いただいて、大変参考になりました。

○中小企業におけるサイバー攻撃のリスクや損害は他人事ではなくいつ自社に降りかかるか危機感を感じた。

○今回SECURITY ACTIONという制度を初めて知った。そしてSECURITY ACTIONコストをかけずに出来るところから見直し・対策する、これは基調講演の中でもありましたが、今ある脅威を見つけそれについてできるところから対策をするということの一歩になるのではないかと思い情報セキュリティ5か条や自社診断等を行ってみたいと思います。

○サーバーのバックアップもウィルスに感染するという事自体、考えもしませんでした。

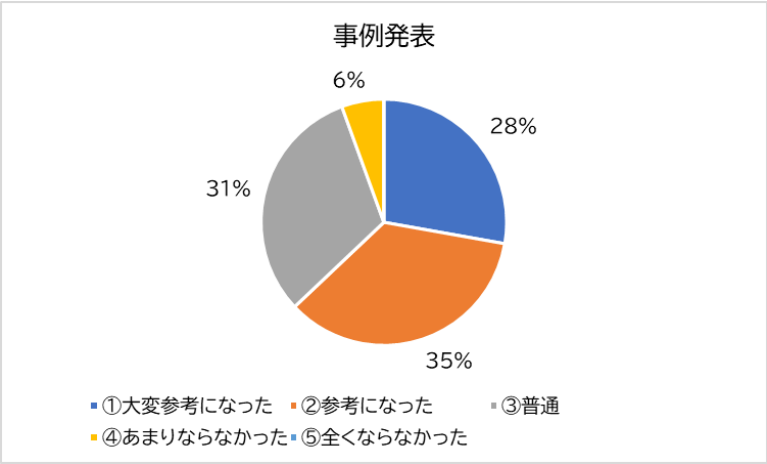
2－5. アンケート集計結果

Q5. 事例発表(有賀氏)について、ご感想をお聞かせください。

項目	人数	割合
①大変参考になった	15	28%
②参考になった	19	35%
③普通	17	31%
④あまりならなかった	3	6%
⑤全くならなかった	0	0%
合計	54	100%

※都合により聴講できず：2名あり

事例発表に関しては、「大変参考になった」「参考になった」を合わせると64%だった。また、「あまり参考にならなかった」が6%となっている。



■感想・コメント

〇被害にあったあとの対策をどのようにやっていったか？参考になりました。

〇経営トップの意思・判断の大切さを感じました。

〇取り組み中での苦労点等、もっと具体的なものが聞けると良かったと思う。

〇25名の企業でも、こんなに取り組めることはあるという内容で、自社を振り返るきっかけになった。

〇弊社でもコロナ過で同様な経緯で同様なIT化を進めてきた経緯もあり共感できた

〇少人数でもセキュリテイ対策をしっかりとやられていて、見習わなくてはと感じました。

〇中小企業においても、サイバーセキュリティに対し先行し取り組んでおられる企業で興味深く聞くことができた。

〇実際に実施したIT化の内容やSECURITY ACTIONの取組みについて、大変勉強になりました。

〇企業規模の違いはあるが、早い時期からの問題意識、実行、主体的な継続活動は、まさに見習うべきものを感じた。

〇分かり易かった。現状に則した身近な環境を整えていることが分かって良かった。

〇中小企業だとなかなか横の情報が入ってこないので大変参考になりました。

〇弊社でもIT化を進める中でセキュリティ対策が追いついておらず参考になった。

〇テレワーク等導入にあたっての問題点等、もう少し具体的に御聞きしたかったです。

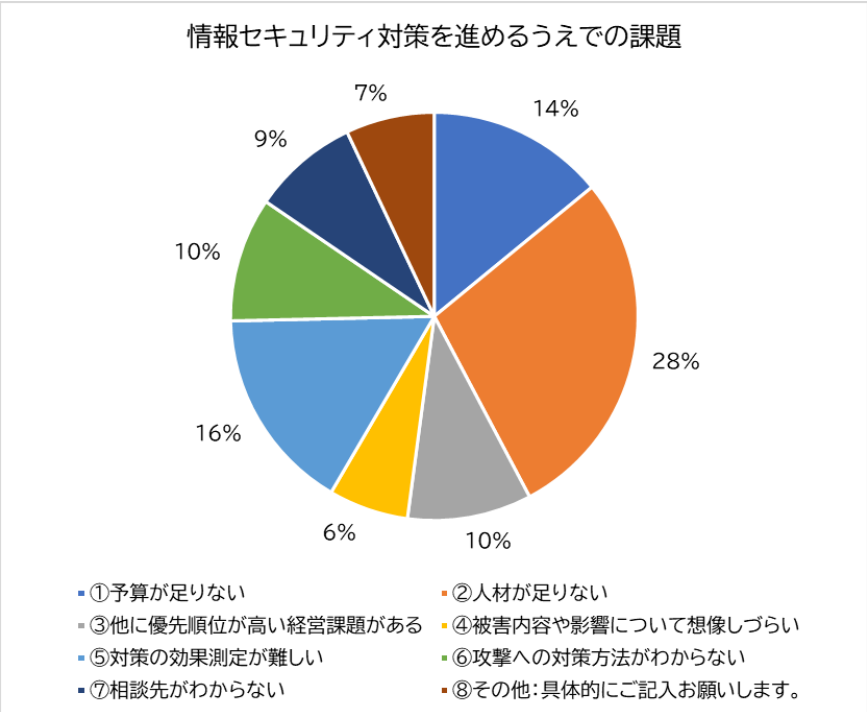
〇セキュリティー対策を実践されている方の声を聞くことができ、取引先からの信用を得る手段に
なっていることがわかりました。

2－5. アンケート集計結果

Q6. 情報セキュリティ対策を進めるうえでの貴社／貴団体の課題について、あてはまるものを全て選んでください。 ※複数回答可

項目	人数	割合
①予算が足りない	20	14%
②人材が足りない	40	28%
③他に優先順位が高い経営課題がある	14	10%
④被害内容や影響について想像しづらい	9	6%
⑤対策の効果測定が難しい	23	16%
⑥攻撃への対策方法がわからない	14	10%
⑦相談先がわからない	12	9%
⑧その他：具体的にご記入お願いします。	10	7%
合計	142	100%

「人材が足りない」が28%と最も多く、続いて「対策の効果測定が難しい」が16%、「予算が足りない」が14%と具体的な課題についての声も多くみられた。



■その他記載内容

○対応するリソースと対応した効果のバランス→限られたリソースの中でどこに対策をしていくか
○経営層への正しい意識づけ
○全職員の一層の意識向上が必要。
○被害内容や影響について想像してもらいづらい
○モバイルワークのさらなる円滑化
○支援機関として各事業者で課題は様々
○経営層にリスク、コスト、費用対効果の説明が難しい
○セキュリティ脅威への経営層の認識が低いため、対応方針が対処的なもので終わる。

2－5. アンケート集計結果

Q7. 情報セキュリティ対策を進めるうえで期待するサポートがあれば、お教えください。

○最新のセキュリティ対策と、サイバー攻撃の事例紹介があるとうれしいです。

○情報セキュリティ対策の定期的なウェビナー期待致します。

○社内PCの個別監視が急務と思われますが、行こうな監視システムなどの実用例があれば参考にしたいので情報提供いただけると助かります。(ID／パスなどの漏洩対策含む)

○今後も、セキュリティー被害の最新動向の公開と、その対策について情報提供をお願いします。

○今後もサイバーセキュリティに対する人材育成が必須となる思いますので、人材育成に重きを置いた研修の開催を期待します。

○今回のような情報提供や、トレンドの紹介などがあると嬉しいです。

○役員含む、全従業員に対する「行動意識付け」を効果的に進める方法の指導

○経営者層が重要さを認識していない様に感じています。トップに向けて情報の発信をお願いいたします。

○しなければならないが、人材が足りない。外部発注で進めたいと思うが費用に対して割高で手が付けれない、上司への提案資料も作成時間や効果測定の表現などできずで停滞する。社内の人的ソースを掛けずに費用安で進める提案・サポートをお願いできるところがあればお話できればと思う。※社内に情報インフラ専門部署は無し。

○最新のセキュリティのバージョンが更新された等の情報が入手し辛いです。特に脆弱性の部分は知っておいた方が良いと思います。メールマガジン等で最新版の情報が知れたら良いです。

○万が一、サイバーセキュリティ事件・事故が発生した場合、調査いただける事業者、連絡先などを関係団体のWebサイトなどで公開いただけたらありがたいです。

○社内でのセキュリティ対策、サイバー攻撃で被る被害の甚大さの共有ができておらず、危機感が植え付けらていないため、他人ごとになっている。社内での効果のある啓蒙活動を行いたい。

○無料で教えてもらうのは無理だと思いますが、例えば、サイバーディフェンス研究所がコンサルを行う場合に、具体的にはどんなことをお勧めされているのか興味があります。

○PGPの推進活動 IT機器使用の免許制度

○各企業の状況に合わせたサービス、特に社員教育とセットでサポートしてもらえるサービスが欲しいです。

○若手や経営層でも判りやすい内容。情報リテラシー教育素材など。

○基調講演の中で、「対策で何をすればよいというものはない」という言葉が印象に残っています。IPAでは重要なセキュリティ情報を発信されていますが、サイバー脅威についての具体的な詳細事例や対処法・対策を発信いただければ参考になります。

2－5. アンケート集計結果

Q8. ご意見・ご感想があればお聞かせください。（自由記述）

〇リアリティのある話を聞くことができて、サイバーセキュリティの重要性を再認識しました。

〇資料が充実していました。

〇補助金制度の充実。（補助金額）

〇参考になる部分が多く、勉強になりました。ありがとうございました。Webexでのセミナーは、参加しやすいため、大変助かります。
当方の勝手な都合ですが、業務中に参加しているため、もう少しコンパクトに2時間程度で行っていただけると大変ありがたいです。

〇最近では大手の子会社・関連会社がサイバー攻撃を受け、そこから大手に影響が波及し甚大な被害が出るなどニュース等で見ます。
零細、中小企業はセキュリティ対策への予算や、意識も低く、ハッカーからすれば安易に突破できるということは弊社も他人ごとではなく明日は我が身だなと感じました。社内全体で意識の向上を図り、対策をしなければならないと意識を高める機会となりました。

〇専門家のタイムリーなお話は、非常に興味深く、参考になりました。アンケートを添付ファイル以外の方法（例えばWebサイトや、
本文でやり取りする等）でお願いしたいです。

〇投資効果が測りにくい中で、モチベーションになるような目標を設定できるようになると良い。

〇今回のようなセミナーを引き続き開催してくだされればうれしく思います。身の回りに潜む危険を知ることで、危機意識を
刺激したいと思っています。

〇サイバーセキュリティについて意識を高める貴重な機会をいただきありがとうございました。様々な分野（警察、通信会社、
機器メーカー、専門家など）からの情報を定期的に開催していただけると幸いです。

3. 考察と展望

3－1. 考察

中国地域サイバーセキュリティセミナー2022については、日本におけるサイバーセキュリティに関する第一人者である名和利男氏の基調講演など、参加申込者数も定員を大きく上回り、聴講者の満足度も高かった。サイバー攻撃の脅威やセキュリティ対策の必要性を強く感じる声が多くあがった反面、「サイバー脅威についての具体的な詳細事例やその対処方法」や、「セキュリティ人材育成における具体的な手法・手順」「外部サポート事業者や団体の情報」など、より具体的かつ自社での取組につながる情報を求める声もあった。

3－2. 今後の展望

社会人セキュリティ人材育成講座と同じく、参加対象者のサイバーセキュリティに関する知識・スキルや、事業者内で担う役割、ポジションに応じてニーズが幅広く存在する。また、定期的な学習機会、情報提供の場を求める声もあることから、今後の検討・課題として以下の内容が考えられる。

〇サイバーセキュリティに関する情報提供の場として、セミナーの定期的な開催
〇対象者を絞ったセミナー内容の検討　※例）経営者層向け、実務担当者向け（上級・初級）など
〇セキュリティ対策に関する支援窓口や、最新動向などの情報提供窓口の周知・広報

開催手法に関しては、新型コロナウイルス対策や参加者の利便性などから総合的に判断しても、現在主流となりつつあるオンライン方式での開催が好ましいと考えられる。

令和3年度中小企業サイバーセキュリティ対策促進事業

（中国地域におけるセキュリティコミュニティ形成事業）

事業報告書

令和4年3月

業務発注者　中国経済産業局　地域経済部 製造・情報産業課
〒730-8531　広島県広島市中区上八丁堀6－30
電　　話　082-224-5630

業務受託者　株式会社アシスト
〒730-0051　広島県広島市中区大手町3－13－18　松村ビル2階
電　　話　082-541-5888