令和２年度補正
中小企業サイバーセキュリティ対策促進事業
（北海道におけるサイバーセキュリティ対策の付加価値向上に向けた調査）

調査報告書

2021 年 3 月

株式会社 道銀地域総合研究所

目　　次

Ⅰ　事業の概要

1. 事業の目的

全国各地におけるサイバーセキュリティ施策の普及に向けて、地方自治体、教育機関、地元企業、関係省庁等との連携や、地域特性・物理的距離を考慮したローカル単位での「セキュリティコミュニティ」形成の必要性が指摘されている。

北海道では、平成 26 年度、北海道経済産業局・北海道総合通信局・北海道警察が連携し、情報セキュリティ意識の向上等を目的とした「北海道地域情報セキュリティ連絡会（以下、HAISL）」を発足させ、会員企業を中心にセミナー等を開催してきた。

そうした中、近年のサイバー攻撃の高度化やサイバーセキュリティ意識の高まり等を背景に、地域のサイバーセキュリティ対策強化や人材育成が急務となっており、本ネットワークは北海道において極めて重要な存在となっている。

また、新型コロナウイルス対応の一環として中小企業がテレワーク等の業務デジタル化を進める中、中小企業におけるサイバー攻撃の脅威と脆弱性はこれまで以上に増大。新型コロナウイルスの混乱に乗じたフィッシングメールや、コロナ対策を行っている事業所等に対するサイバー攻撃も確認されている等、地域中小企業も例外なくサイバー攻撃の脅威にさらされており、迅速な対策強化が求められている。

本事業では、コロナ禍におけるサイバーセキュリティ対策に向けた意識醸成を図るとともに、本ネットワークのさらなる深化・拡大に向けて、関係者の理解促進や新たなプレーヤー発掘、人材育成の拡充等を通じ、当該コミュニティの付加価値向上を目指した。

2. 事業の内容

（1）サイバーセキュリティ意識に関する調査

道内中小企業のサイバーセキュリティ対策への理解度把握や、対策レベルに合わせた導入支援方法等の検討を目的に、アンケート調査を実施し、アンケート結果の集計・分析・とりまとめを行った。

（2）道内におけるセキュリティベンダー・専門家等の発掘

本ネットワークの強化・拡充を目的に、「道内」もしくは「道内ゆかり」のセキュリティ専門家について、文献調査・ヒアリングなどを通じてリスト化した。

（3）一般向けサイバーセキュリティセミナーの開催

本調査の取組内容や得られた成果等を活用し、HAISL と連携したセミナー形式等による情報発信を通じて、道民に広くサイバーセキュリティに関する意識向上に向けた普及啓発を行った。

（4）サイバーセキュリティ人材育成に向けたカリキュラム検討・開発・実証

一般社団法人 LOCAL と連携し、一定程度のセキュリティ知識を有する 30 歳以下を対象とする「集中講座」の実施に向けたカリキュラムの検討・開発・実証等を行った。

（5）実践型競技会の域内展開に向けた広報等

サイバーセキュリティ分野の各種実践型競技会（Cyder、Hardening 等）の域内展開に向けて、当該競技会について域内企業や関係団体等への周知を行い、域内における意識の醸成を図るとともに、当該競技会への域内参加者に加えて、協賛・協力等が可能な企業の掘り起こし等を行った。

（6）道内における持続的なセキュリティコミュニティのあり方に関する検討

今後、更に重要性を増すサイバーセキュリティ対策の持続的かつ自立的地域展開に向けて、他地域の自立型コミュニティ事例なども参考に、HAISL の民営化に向けた道筋や次年度取組の構想等を整理・検討した。

（7）HAISL の運営

HAISL 連絡会にて本事業の報告を行った。また、HAISL の会員企業の増加に向けて、活動内容等を記載したチラシを作成し、企業への PR を行った。

（8）調査報告書の作成

上記（1）～（7）の結果について、報告書を作成した。

Ⅱ　サイバーセキュリティ意識に関する調査

1. 企業向けアンケート調査の結果

道内中小企業のサイバーセキュリティ対策への理解度を把握するとともに、今後、対策レベルに合わせた支援方法等の検討を行うための情報を収集することを目的として、アンケート調査を実施した。

・調査方法
郵送発送・郵送及びウェブ回収のアンケート調査

・調査対象
(株)東京商工リサーチに登録されている道内中小企業のうち、製造業・非製造業それぞれ売上上位 500 社（計 1,000 社）
※中小企業とは中小企業基本法上の「中小企業の範囲」による

・調査時期
令和 2 年 9 月～10 月

・回収率
有効回答　281 件（有効回答率 28.1%）

・調査項目
・回答者属性（所在地、業種、資本金、従業員数、売上高）
・サイバーセキュリティ対策担当者、対策担当部署の有無
・サイバーセキュリティ対策の現状に対する認識
・これまでに受けたことのあるサイバーセキュリティ被害
・現在実施しているサイバーセキュリティ対策の現状
・今後実施すべきと思うサイバーセキュリティ対策
・サイバーセキュリティに関する情報の収集先
・サイバーセキュリティに関して知りたい情報
・サイバーセキュリティに関する課題　等

【アンケート調査票】

中小企業のサイバーセキュリティ対策等に関する調査

【調査票記入上のご注意】
1．ご回答は、それぞれの質問に従い、該当する選択肢番号を○印で囲んでください。
2．本調査票は、同封の返信用封筒により○月○日（○）までにご投函ください。
　または、別紙のＱＲコードより専用の回答用ウェブサイトにアクセスし、ウェブ上からご回答ください。
3．本調査は、経済産業省北海道経済産業局が株式会社道銀地域総合研究所に委託して実施するもので、個別の回答内容についての秘密は厳守致します。
　なお、回答の内容について、調査実施主体である経済産業省北海道経済産業局より、ご連絡をさせていただく場合があります。

問1　貴社の概要について下欄にご記入ください。選択項目は該当するもの1つを○印で囲んでください。

①所在地	1．札幌市 2．札幌市以外の市→（市名：　　）	3．その他町村→（町村名：　　）
②業種	1．農業、林業 2．漁業 3．鉱業、採石業、砂利採取業 4．建設業 5．製造業 6．電気・ガス・熱供給・水道業 7．情報通信業 8．運輸業、郵便業 9．卸売業、小売業 10．金融業、保険業	11．不動産業、物品賃貸業 12．学術研究、専門・技術サービス業 13．宿泊業、飲食サービス業 14．生活関連サービス業、娯楽業 15．教育、学習支援業 16．医療、福祉 17．複合サービス事業 18．サービス業（他に分類されないもの） 19．公務（他に分類されるものを除く） 20．分類不能の産業
③資本金	1．5千万円以下 2．5千万円超1億円以下	3．1億円超3億円以下 4．3億円超
④従業員数	1．10人以下 2．11人以上 20人以下 3．21人以上 30人以下 4．31人以上 50人以下	5．51人以上100人以下 6．101人以上 200人以下 7．201人以上 300人以下 8．301人以上
⑤売上高 ※直前1期の売上高を選択してください。	1．1千万円未満 2．1千万円以上 3千万円未満 3．3千万円以上 5千万円未満 4．5千万円以上 1億円未満	5．1億円以上 5億円未満 6．5億円以上 10億円未満 7．10億円以上

問2　貴社のサイバーセキュリティ対策担当者について、該当するもの1つを○印で囲んでください。

1．専任者を配置している	3．配置していない
2．兼任者を配置している	

問3　貴社のサイバーセキュリティ対策担当部署について、該当するもの1つを○印で囲んでください。

1．専任部署を設置している	3．設置していない
2．他部門と兼務で設置している	

問4　貴社のサイバーセキュリティ対策について、現在の対応で十分だと感じていますか。
　該当するもの1つを○印で囲んでください。

1．十分である	5．不十分である
2．やや十分である	6．対策は不要である
3．どちらともいえない	7．わからない
4．やや不十分である	

問5　貴社が受けたことのあるサイバーセキュリティ被害について、該当するもの全てを○印で囲んでください。

1．機密情報や個人情報の漏洩・紛失	6．DDos 攻撃
2．コンピュータウィルス感染	7．その他
3．フィッシング詐欺による情報流出	（　　）
4．自社ホームページへの不正ログイン	8．被害を受けたことはない
5．自社ホームページの改ざん	

1

問6　貴社が実施しているサイバーセキュリティ対策について、該当するもの全てを○印で囲んでください。

1．ウイルス対策ソフトの導入	9．取引先や委託先への対策依頼
2．データの暗号化	10．セキュリティ専門人材の雇用・育成
3．アクセス権限の制御	11．リスクアセスメントの実施
4．社員教育・研修の実施	12．セキュリティ専門部署の設置
5．外部専門家からのアドバイス	13．その他
6．セキュリティ認証の取得	（　　）
7．セキュリティポリシーの策定	14．対策は実施していない
8．事故対応マニュアルの策定	

問7　貴社が今後実施すべきと思うサイバーセキュリティ対策について、該当するもの全てを○印で囲んでください。

1．ウイルス対策ソフトの導入	9．取引先や委託先への対策依頼
2．データの暗号化	10．セキュリティ専門人材の雇用・育成
3．アクセス権限の制御	11．リスクアセスメントの実施
4．社員教育・研修の実施	12．セキュリティ専門部署の設置
5．外部専門家からのアドバイス	13．その他
6．セキュリティ認証の取得	（　　）
7．セキュリティポリシーの策定	14．対策は実施していない
8．事故対応マニュアルの策定	

問8　貴社のサイバーセキュリティに関する情報の収集先について、該当するもの全てを○印で囲んでください。

1．ウェブサイト	7．テレビ・ラジオ
2．セミナー、シンポジウム、勉強会	8．新聞・雑誌（一般紙）
3．社内の専門人材	9．新聞・雑誌（業界紙・業界誌）
4．社外の専門家	10．メールマガジン
5．公的機関	11．その他（　　）
6．SNS	12．情報収集はしていない

問9　サイバーセキュリティに関して知りたい情報について、該当するもの全てを○印で囲んでください。

1．攻撃を受けた際の対処方法	7．セキュリティポリシーの策定方法
2．攻撃の種類と内容	8．取引先や委託先への協力依頼方法
3．被害に遭った際の法的措置	9．専門人材の獲得方法
4．対応マニュアルの作成方法	10．その他
5．攻撃を受けた際の被害額	（　　）
6．社員の教育・研修・訓練方法	11．特に知りたい情報はない

問10　貴社におけるサイバーセキュリティに関する課題について、該当するもの全てを○印で囲んでください。

1．経営者の危機意識が低い（ない）	6．対策について相談する社外の相手・企業がいない
2．従業員の危機意識が低い（ない）	7．被害を受けたとき相談する社外の相手・企業がいない
3．対策を行うことのできる人材がいない	8．その他
4．対策を行うための費用が少ない	（　　）
5．忙しく対策を行うための時間の余裕がない	9．とくに課題はない

問11　御社の情報システムにサイバー攻撃等を監視する機器を設置し、セキュリティ状況を把握する外部サービスが無償で提供される場合、活用の意向はありますか？該当するもの1つを○印で囲んでください。

1．活用したい	2．必要ない	3．判断できない

問12　北海道経済産業局・北海道総合通信局・北海道警察の3機関では、「北海道情報セキュリティ連絡会（略称：HAISL）」を設立し、サイバーセキュリティに関する情報を発信しています（添付資料ご参照）。今後、HAISLからの情報提供を希望しますか？該当するもの1つを○印で囲んでください。

1．希望しない	2．希望する

■ご連絡先をご記入ください。

貴　社　名			
記入者氏名	所属・役職：	氏名：	
連　絡　先	TEL：	FAX：	mail：

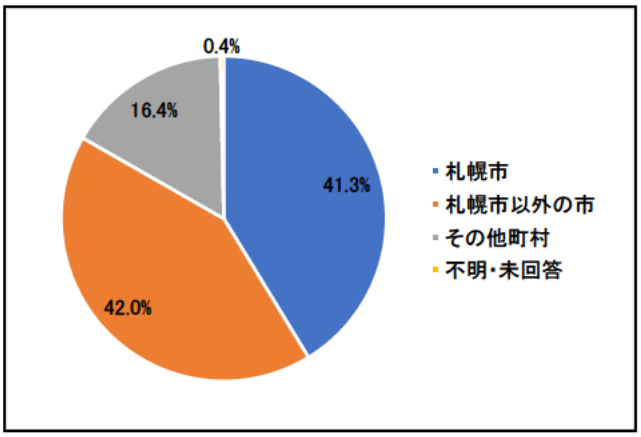
ご協力ありがとうございました。

2

（1）全体の集計

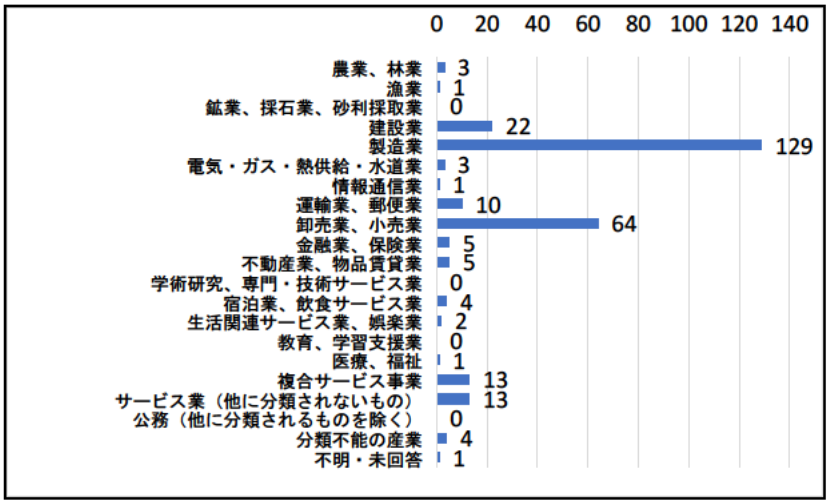
■回答属性

・所在地



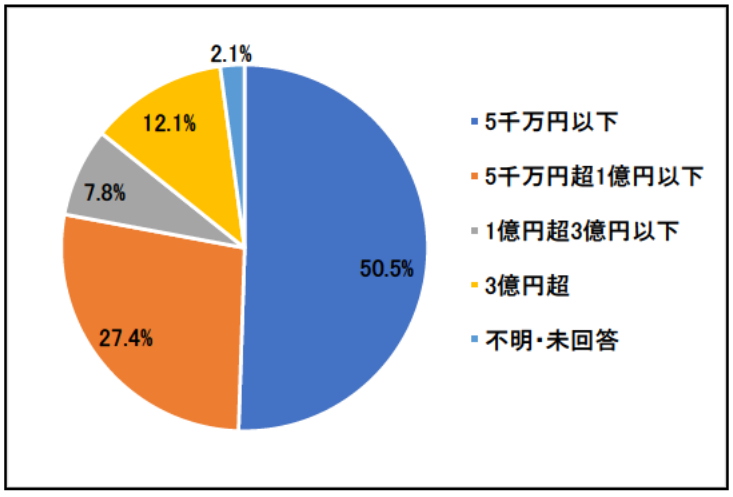
回答企業の所在地は、「札幌市」が 41.3%、「札幌市以外の市」が 42.0%、「その他町村」が 16.4%であった。

・業種（社数）



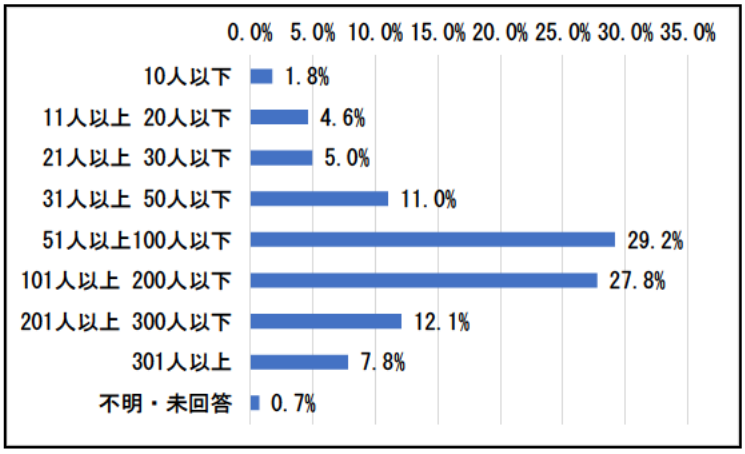
回答企業の業種は、「製造業」が最も多く 129 社、次いで「卸売業、小売業」が 64 社、「建設業」が 22 社であった。

・資本金



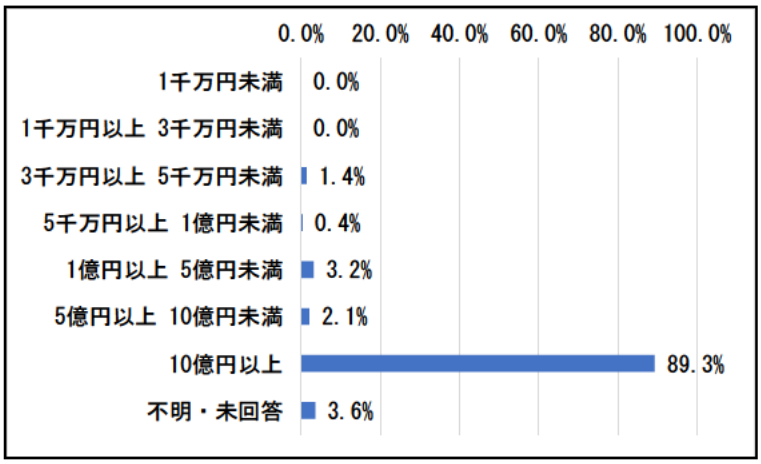
資本金は「5 千万円以下」が 50.5%と最も多く、「5 千万円超 1 億円以下」が 27.4%、「1 億円超 3 億円以下」が 7.8%、「3 億円超」が 12.1%であった。

・従業員数



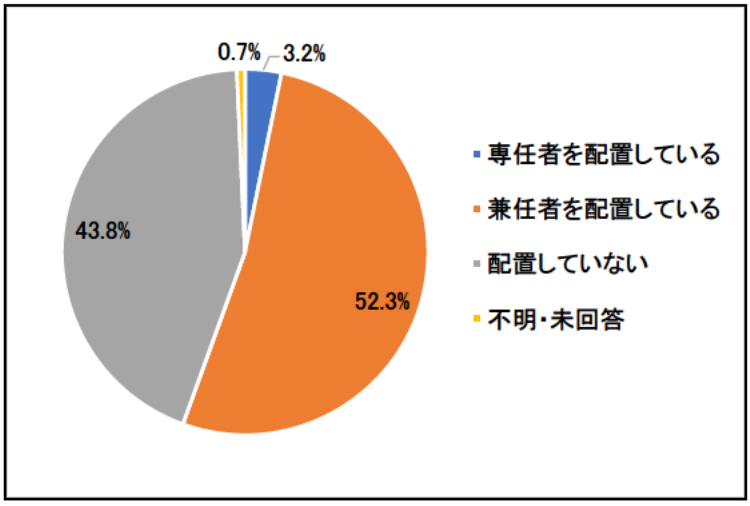
従業員数は「51 人以上 100 人以下」が 29.2%と最も多く、次いで「101 人以上 200 人以下」が 27.8%であった。

・売上高



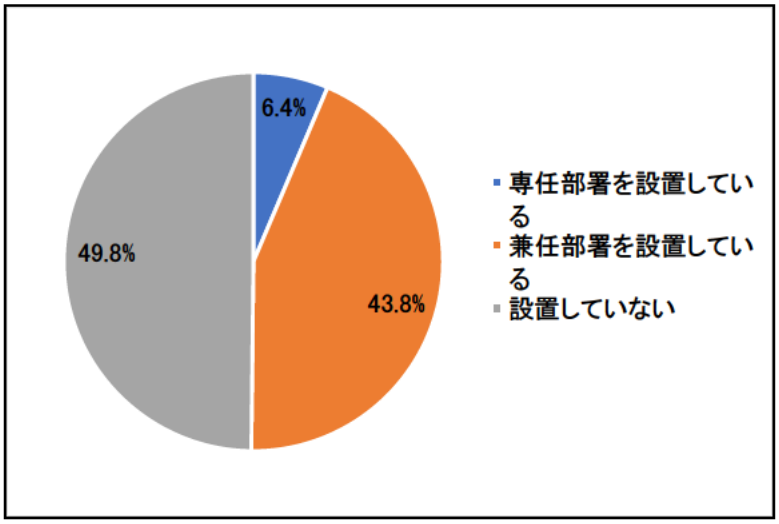
売上高は「10 億円以上」が 89.3%と多数を占めた。

■サイバーセキュリティ対策担当者の配置



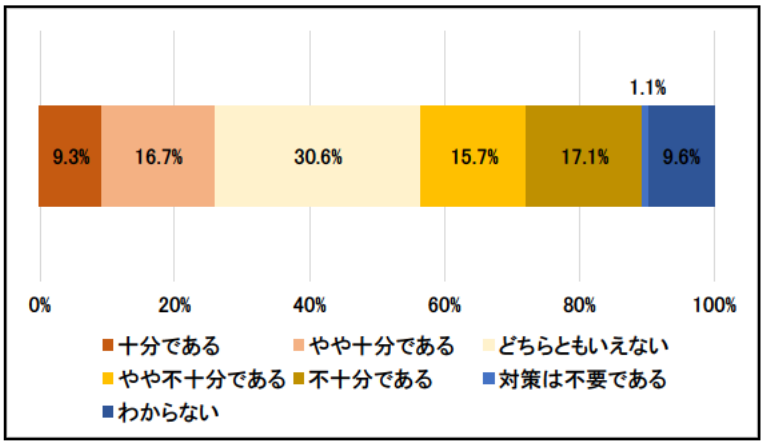
サイバーセキュリティ対策担当者の配置については、「専任者を配置している」が 3.2%、「兼任者を配置している」が 52.3%と、半数以上の企業が担当者を配置している。

■サイバーセキュリティ対策担当部署の設置



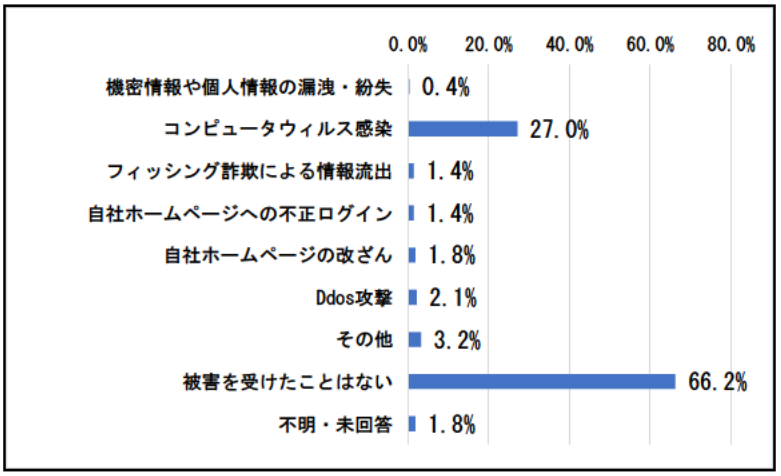
サイバーセキュリティ対策担当部署については、「専任部署を設置している」が 6.4%、「兼任部署を設置している」が 43.8%と、半数以上の企業が担当部署を設置している。

■サイバーセキュリティ対策に関する現在の対応



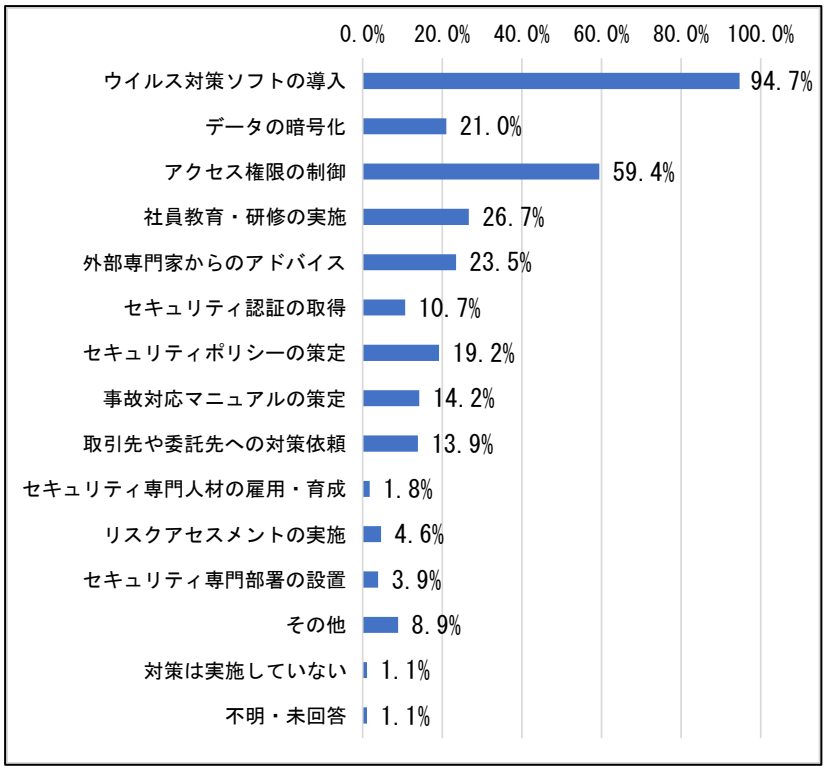
サイバーセキュリティ対策に関する現在の対応については、「十分である」が 9.3%、「やや十分である」が 16.7%（両者合計で 26.0%）であるのに対し、「やや不十分である」が 15.7%、「不十分である」が 17.1%（両者合計で 32.8%）と、不十分と感じている企業のほうが多い。

■これまでに受けたことのあるサイバーセキュリティ被害（当てはまるもの全て）



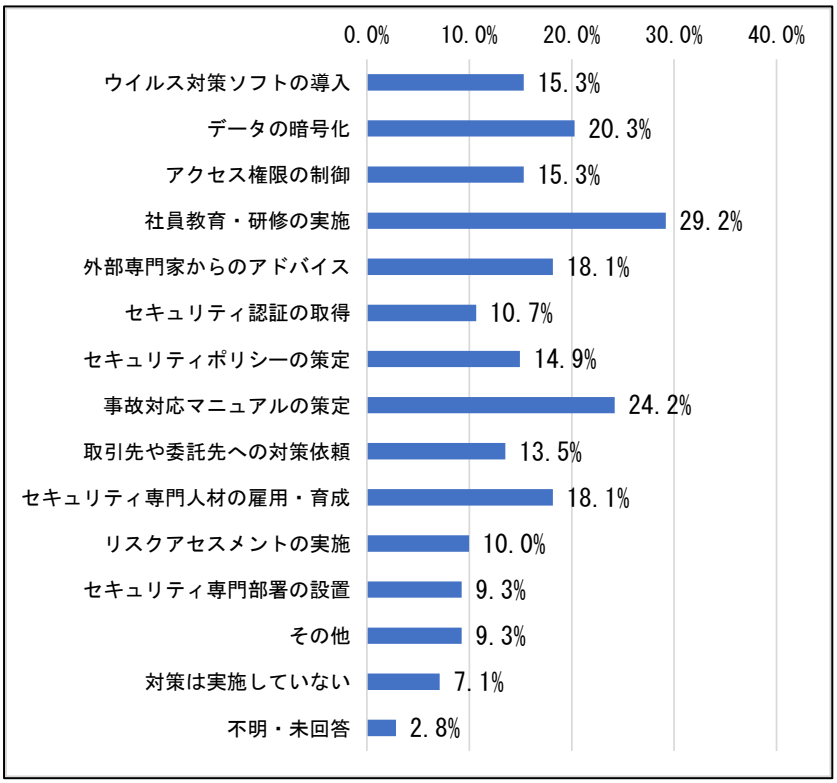
「被害を受けたことはない」は 66.2%であり、3 割以上が被害を受けた経験を有している。最も多い被害は「コンピュータウイルス感染」(27.0%)である。

■現在実施しているサイバーセキュリティ対策（当てはまるもの全て）



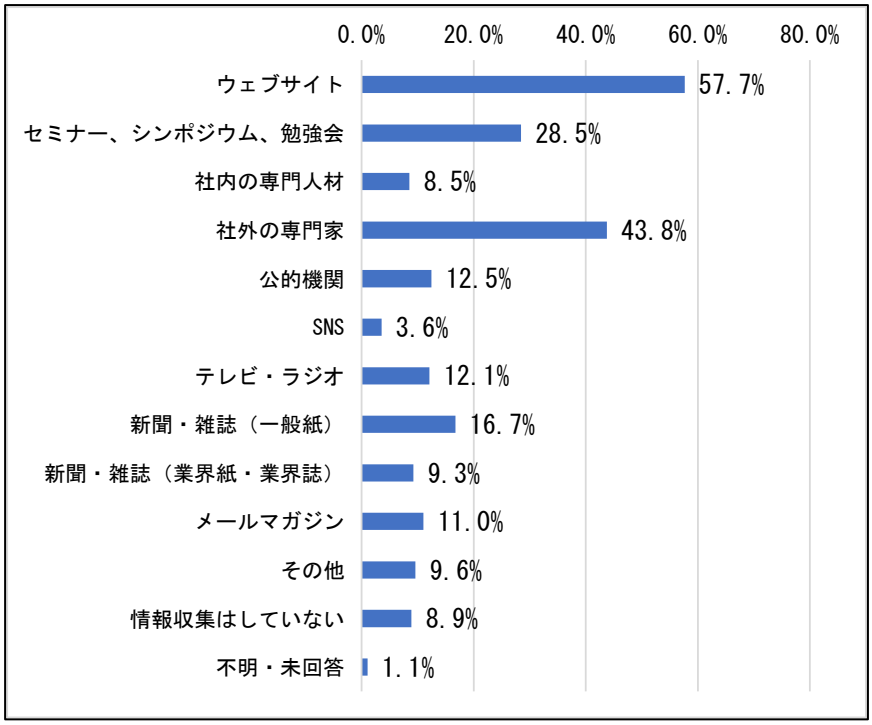
現在実施しているサイバーセキュリティ対策は「ウイルス対策ソフトの導入」が 94.7%と最も多く、次いで「アクセス権限の制御」が 59.4%となっている。

■今後実施すべきと思うサイバーセキュリティ対策（当てはまるもの全て）



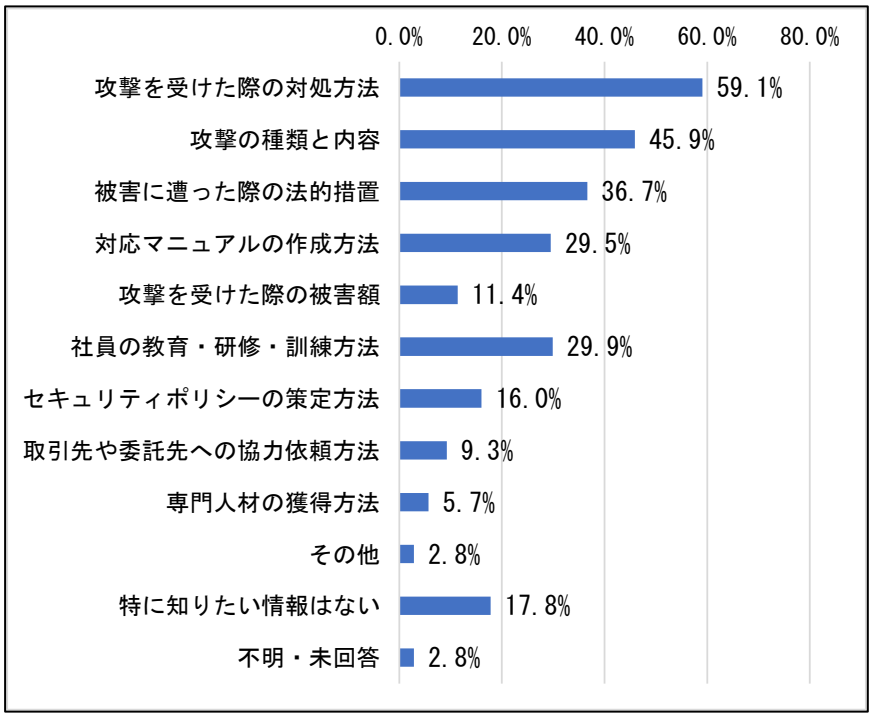
今後実施すべきと思うサイバーセキュリティ対策は、「社員教育・研修の実施」が 29.2%と最も多く、次いで「事故対応マニュアルの策定」(24.2%)、「データの暗号化」(20.3%)、「セキュリティ専門人材の雇用・育成」(18.1%) の順となっている。

■サイバーセキュリティに関する情報の収集先（当てはまるもの全て）



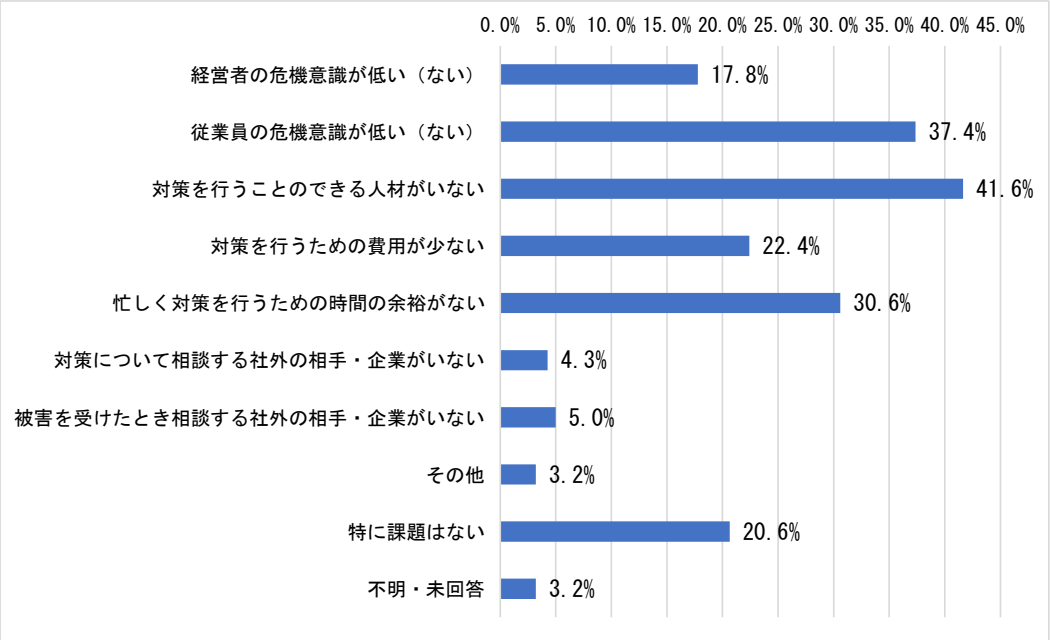
サイバーセキュリティに関する情報の収集先は「ウェブサイト」が57.7%と最も多く、次いで「社外の専門家」が43.8%、「セミナー、シンポジウム、勉強会」が28.5%の順である。

■サイバーセキュリティに関して知りたい情報（当てはまるもの全て）



サイバーセキュリティに関して知りたい情報は「攻撃を受けた際の対処方法」が 59.1%と最も多く、次いで「攻撃の種類と内容」(45.9%)、「被害に遭った際の法的措置」(36.7%)、「社員の教育・研修・訓練方法」(29.9%)、「対応マニュアルの作成方法」(29.5%) の順である。

■サイバーセキュリティに関する課題（当てはまるもの全て）



サイバーセキュリティに関する課題は「対策を行うことのできる人材がいない」が 41.6%と最も多く、次いで「従業員の危機意識が低い（ない）」（37.4%）、「忙しく対策を行うための時間の余裕がない」（30.6%）、「対策を行うための費用が少ない」（22.4%）の順となっている。

【北海道内のサイバーセキュリティに関する概況】

これらの集計の結果から、道内中小企業のサイバーセキュリティに関する概況として、以下の事項が導き出される。

○企業の対応

- ウイルス対策ソフトの導入など、一般的な対応はなされている。
- 約半数の企業が、サイバーセキュリティ対応の担当者や、担当部署を置いている。
- 課題としては「対策が行える人材不足」や「経営層や従業員の危機意識を高めること」があげられる。

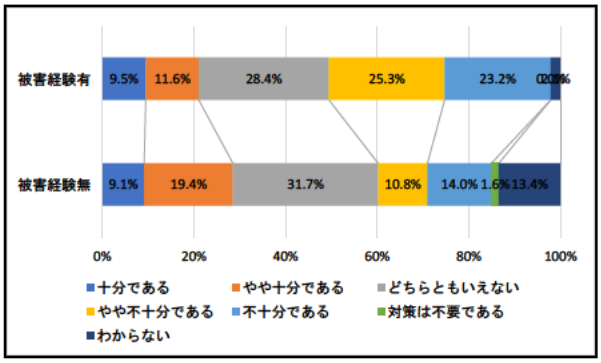
○被害や対策

- 3 割以上の道内企業が被害を受けた経験を有している。
  ちなみに、全国の企業を対象にした調査（トレンドマイクロ社「法人組織におけるセキュリティ実態調査 2019 年版」）では、36.3%の企業が被害経験を有している。
- 現状の対策では不十分であると感じている企業が多い。
- 今後の対策としては、社内体制や、有事の際の対応が課題となっている。

(2)項目ごとの集計

①被害経験の有無ごとの違い

■サイバーセキュリティへの対応状況

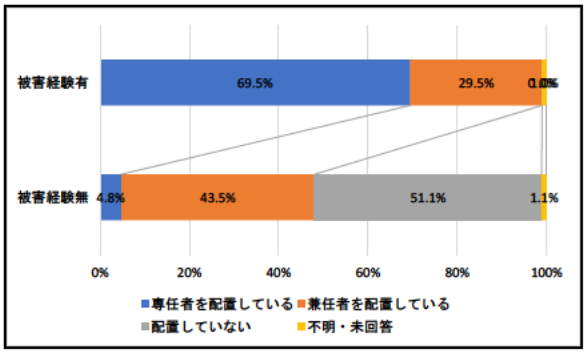


現在のサイバーセキュリティ対策について、「十分である」「やや十分である」の合計は、被害を受けた経験のある企業では 21.1%であるのに対し、被害を受けた経験のない企業では 28.5%である。一方、「やや不十分である」「不十分である」の合計は、被害経験のある企業では 48.5%であるのに対し、被害経験のない企業では 24.8%である。

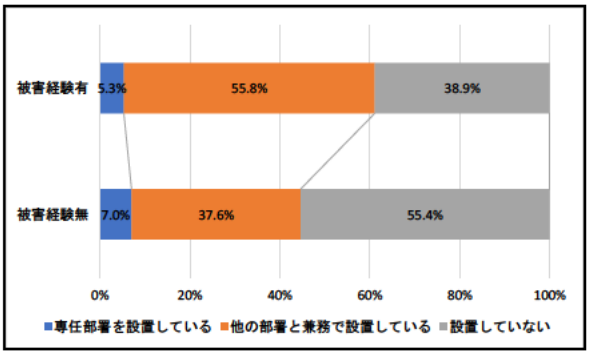
実際に被害を受けた経験のある企業は、自社の現在のサイバーセキュリティ対策に危機感を覚えていることがうかがえる。

■担当者の配置状況、担当部署の設置状況

【担当者の配置状況】

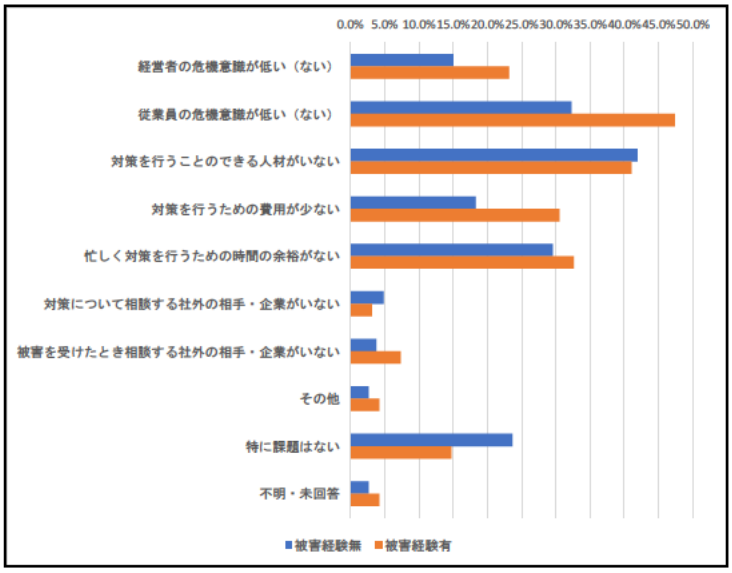


【担当部署の設置状況】



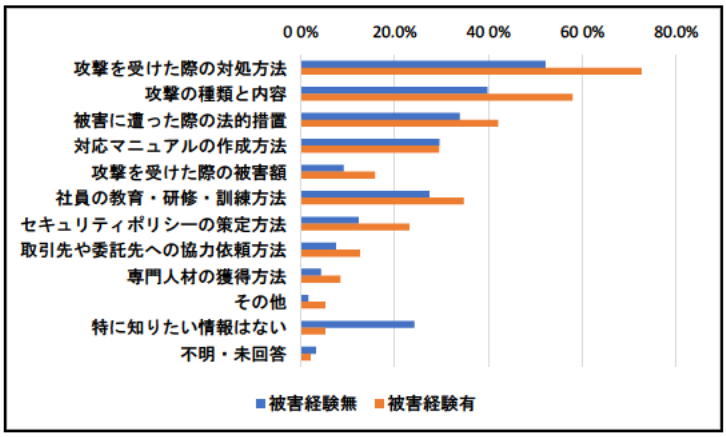
被害経験のある企業では、担当者を配置している割合や、担当部署を設けている割合が、被害経験のない企業に比べて高い。

■サイバーセキュリティに関する課題



また、被害経験の有無にかかわらず「対策を行うことのできる人材がいない」が共通の課題となっている。また、被害経験のある企業では、経営者や従業員の危機意識を高めることを課題として意識している割合が比較的高い。

■サイバーセキュリティに関して知りたい情報



各項目について被害を受けた経験のある企業のほうが関心が高い。とくに「攻撃を受けた際の対処方法」「攻撃の種類と内容」について高い関心がみられる。
一方、被害を受けた経験のない企業では「特に知りたい情報はない」との回答が比較的多い。

【被害経験の有無による企業対応の違い】

これらの集計の結果から、被害経験の有無による企業の対応等の違いとして、以下の事項が導き出される。

○被害経験のある企業

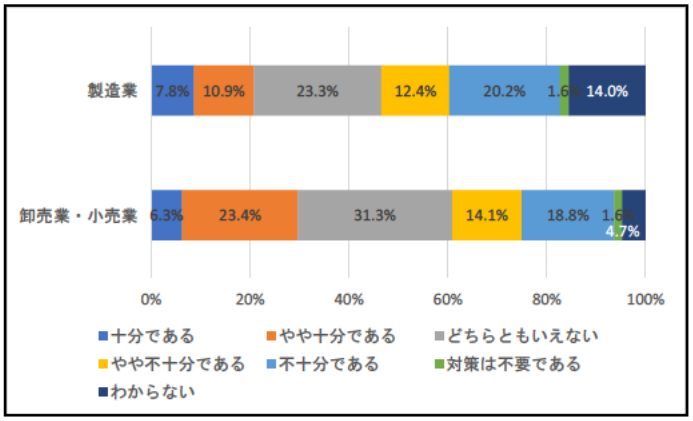
・ 担当者や担当部署を設けている率が、被害経験のない企業に比べて高い。
・ 情報収集に関心が高い傾向がある。
・ 社内の意識の向上や、有事の際の対策・対応、人材の不足を課題としている。

○被害経験のない企業

・ 現時点で被害を受けた経験がないためか、関心が薄い傾向がある。
・ また、課題に対する意識も、比較的低い。
・ 人材の不足については、被害経験のある企業と同様に、課題としている。

②業種ごとの違い

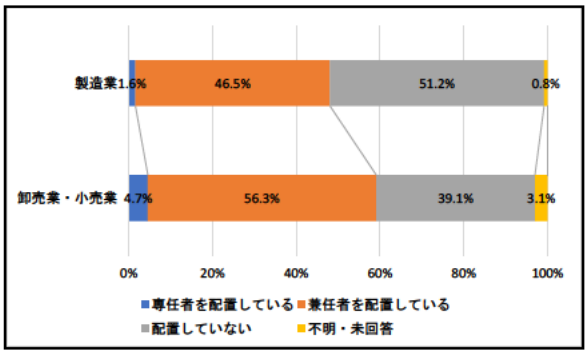
■サイバーセキュリティへの対応状況



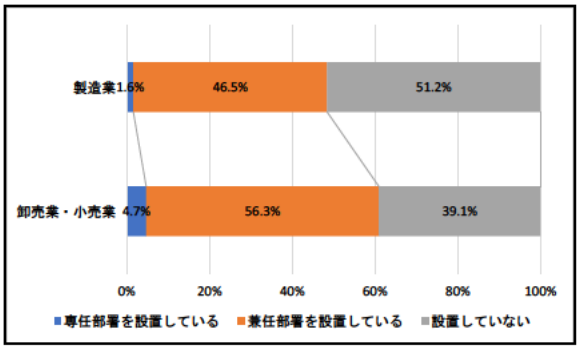
「十分である」「やや十分である」の合計をみると、製造業は 18.7%であるのに対し、非製造業は 29.7%であり、製造業のほうが現在の対策に満足していないことがうかがえる。
ただし、業種の違いから求めるセキュリティレベルに違いがある可能性も考えられる。

■担当者の配置状況、担当部署の設置状況

【担当者の配置状況】

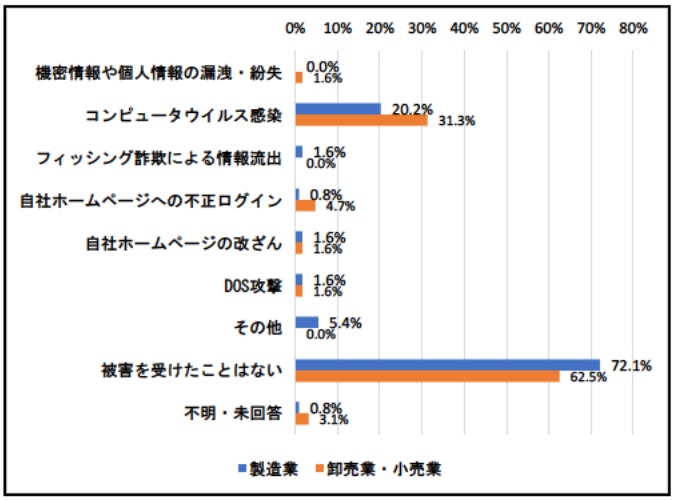


【担当部署の設置状況】



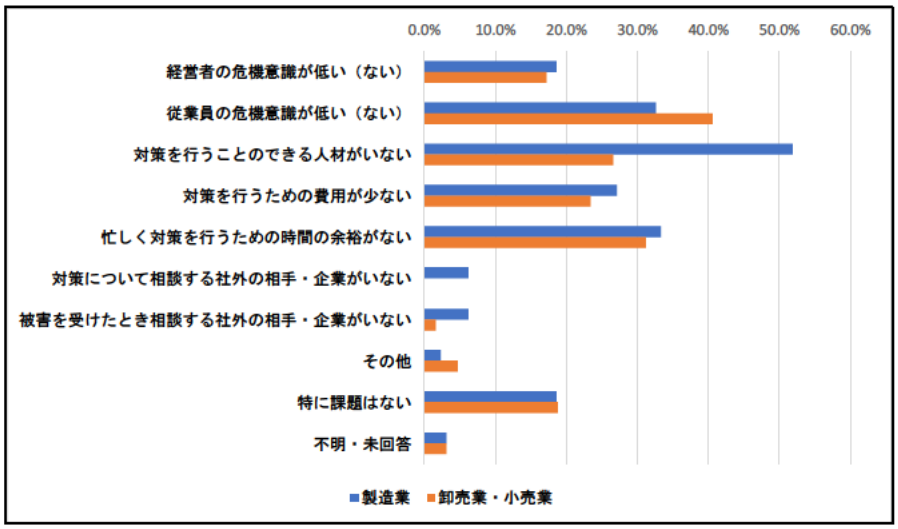
卸売業・小売業のほうが、配置、設置している割合が高い。

■受けたことのあるサイバーセキュリティ被害



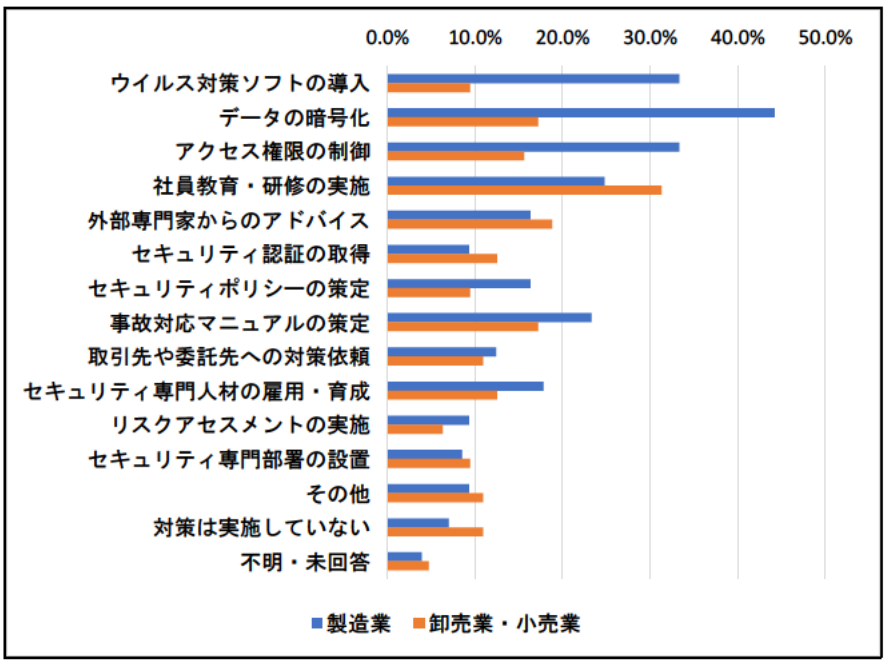
製造業と卸売業・小売業との間で顕著な差はみられない。

■サイバーセキュリティに関する課題



製造業で「対策を行うことのできる人材がいない」の割合が高い。

■今後実施すべきサイバーセキュリティ対策



製造業で「ウイルス対策ソフトの導入」「データの暗号化」「アクセス権限の制御」など、システムやインフラ面を課題としている割合が高い。

【業種による企業の状況の違い】

これらの集計の結果から、業種による違いとして、以下の事項が導き出される。

○全体

・ 特定の業種が攻撃を受けているとはいえない。
・ 課題については、製造業で人材の不足が顕著である以外は、製造業、卸売業・小売業とも、ほぼ同じである。

○製造業

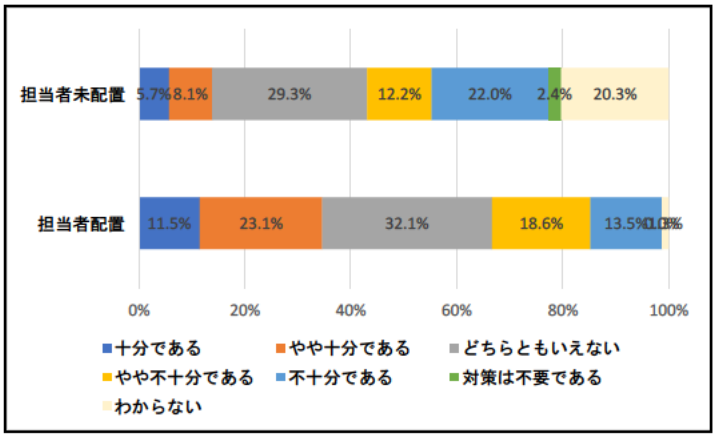
- 製造業は、業務の性格上、保有する機器等の数や種類が比較的多いことから、求めるセキュリティレベルが卸売業・小売業に比べて高い可能性もあるが、セキュリティ対応に不安を感じている割合が高い。
- 「ウイルス対策ソフトの導入」や「データの暗号化」など、社内システム面が課題であると感じている割合が高い。
- 卸売業・小売業に比べて、人材の不足を課題とする割合が高い。

○卸売業・小売業

- 卸売業・小売業は、製造業に比べて、担当者配置や対応部署設置を行っている割合が高い。ただし、IPA「企業の CISO や CSIRT に関する実態調査 2017」では、全国では62.6%の企業が対応部署を設置しており、これに比べると、道内企業の設置率は低い。
- 今後の実施すべき対策として「社員教育・研修」をあげる割合が製造業に比べて高い。

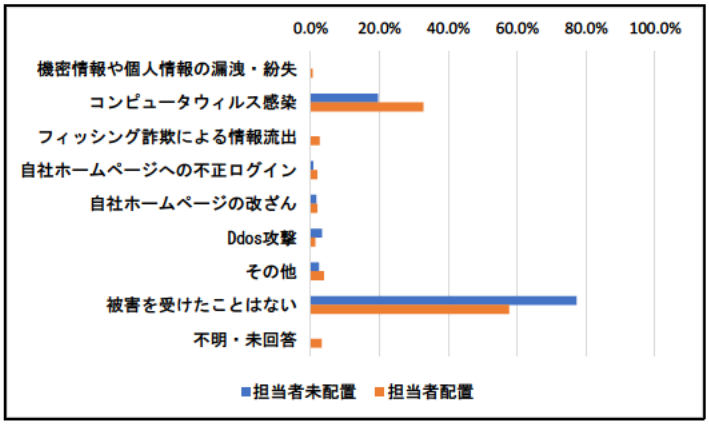
③担当者の有無による違い

■サイバーセキュリティへの対応状況



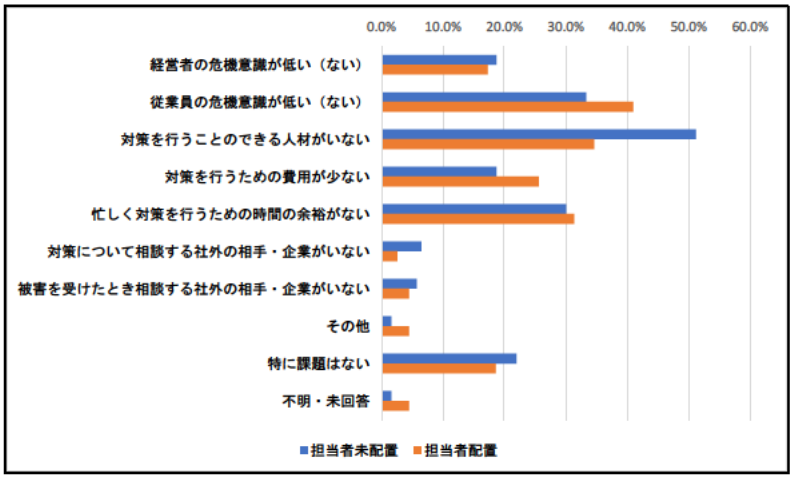
担当者を配置している企業のほうが、担当者を配置していない企業に比べて「十分である」「やや十分である」の割合が高い。

■受けたことのあるサイバーセキュリティ被害



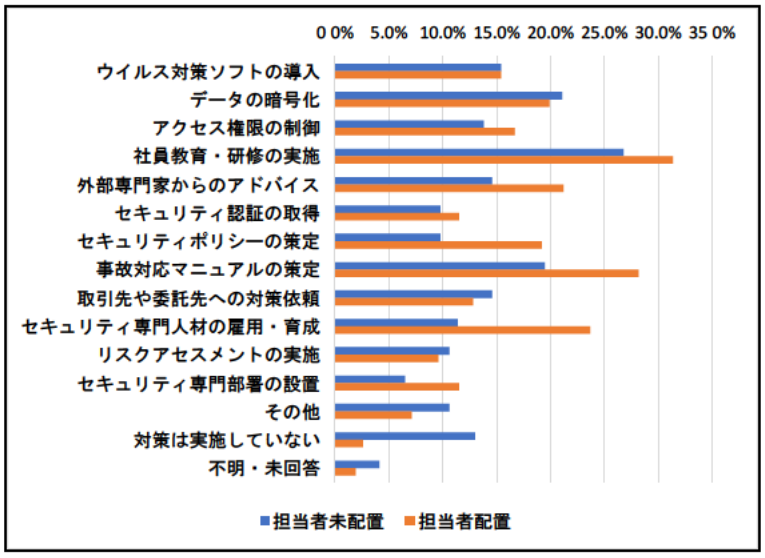
「コンピュータウイルス感染」を受けたことのある割合は、担当者を配置している企業で高く、一方、「被害を受けたことはない」と回答した割合は、担当者を配置していない企業で高い。これは、担当者を配置していない企業では、被害を受けていても気づいていないためである可能性も考えられる。

■サイバーセキュリティに関する課題



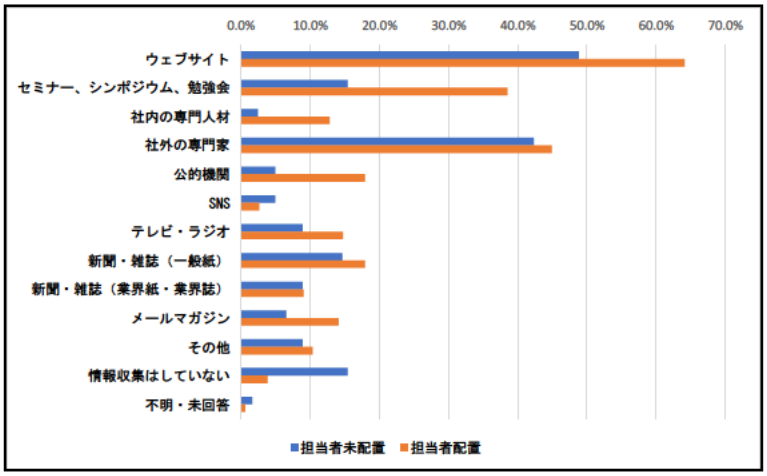
担当者を配置していない企業において「対策を行うことのできる人材がいない」との回答割合が高い。

■今後実施すべきサイバーセキュリティ対策



担当者を配置している企業はさまざまな対策を検討しているのに対し、担当者を配置していない企業では「対策は実施していない」の割合が高いのが目立つ。

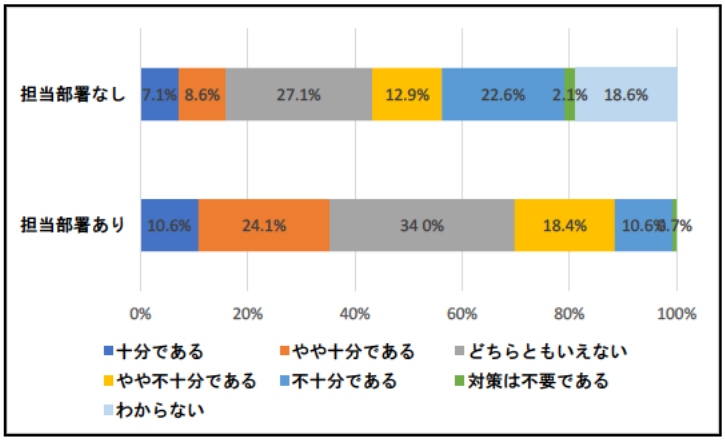
■関連情報収集先



担当者を配置している企業のほうが情報収集に積極的な傾向がみられる。担当者を配置していない企業では「情報収集はしていない」との回答の割合が高い。

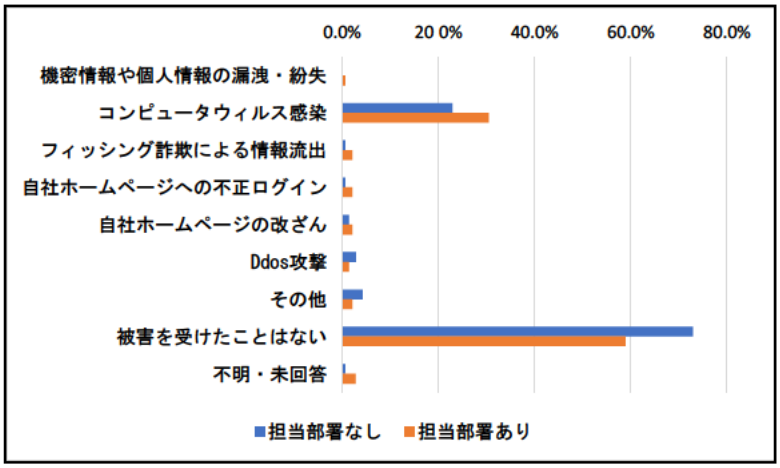
④担当部署の有無による違い

■サイバーセキュリティへの対応状況



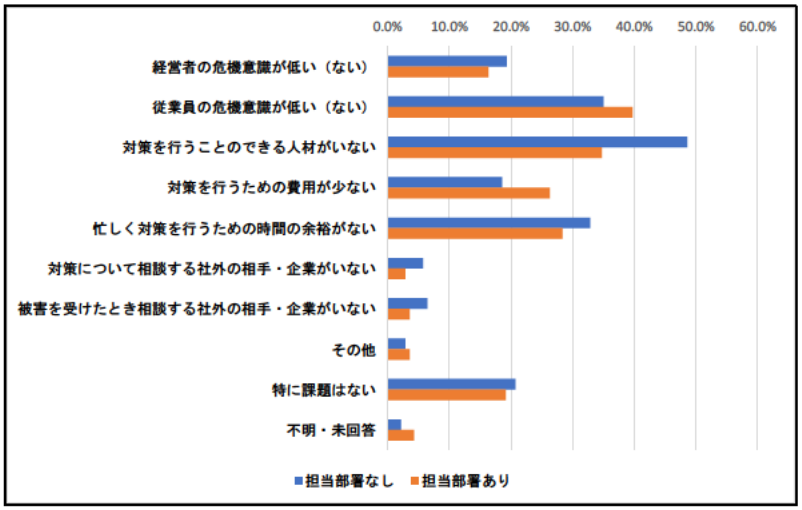
担当部署がある企業では「十分である」「やや十分である」の割合が高い。

■受けたことのあるサイバーセキュリティ被害



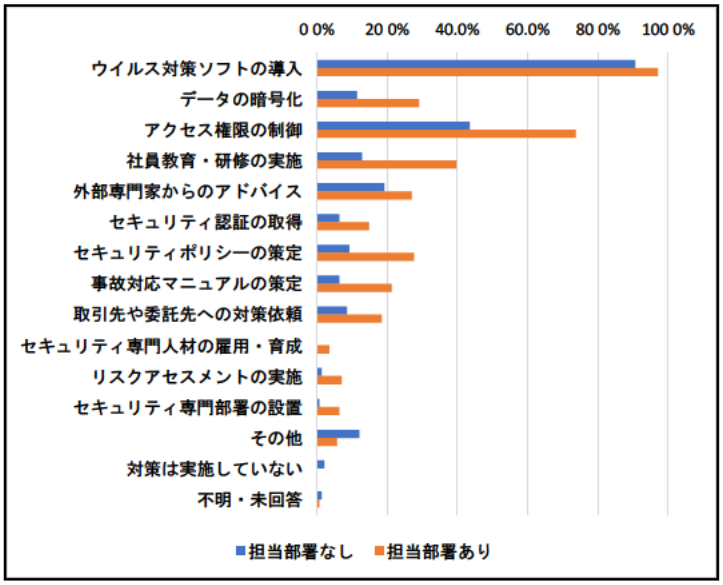
担当部署のない企業では「被害を受けたことはない」の割合が高いが、担当部署がないことから実際には被害を受けていても気づいていない可能性も考えられる。

■サイバーセキュリティに関する課題



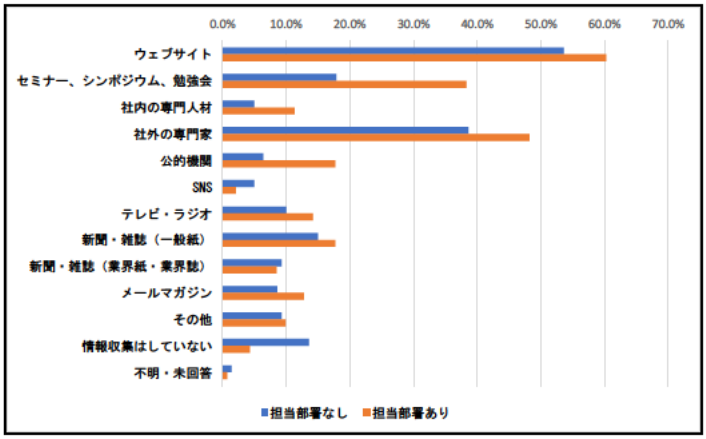
担当部署のない企業において「対策を行うことのできる人材がいない」の割合が高い。

■今後実施すべきサイバーセキュリティ対策



担当部署がある企業では、担当部署がない企業に比べて、さまざまな対策への取組を検討していることがうかがえる。

■関連情報収集先



担当部署がある企業のほうが、情報収集を積極的に行っていることがうかがえる。担当部署がない企業では「情報収集はしていない」割合が高い。

【担当の有無による企業の状況の違い】

これらの集計の結果から、担当の有無による違いとして、以下の事項が導き出される。

○担当者や担当部署が存在する企業

- 現在のサイバーセキュリティ対策に満足している傾向がみられる。
- 今後の対策としては、「社員教育・研修の実施」「外部専門家からのアドバイス」「セキュリティ専門人材の雇用・育成」など人材面、「セキュリティポリシーの策定」、「事故対応マニュアルの策定」など社内体制の整備に取り組もうとする姿勢がみられる。
- 情報の収集についても、比較的積極的に行っている。

○担当者や担当部署が存在しない企業

- 被害経験のない割合が高い。

・ 人材の不足が課題としてあげられている。
・ 担当者や担当部署が存在する企業に比べて、情報収集や対策の実施など行っていない割合が高い。

（3）企業向けアンケート調査のまとめ

以上の結果を整理すると、以下の 2 点が道内企業の課題であるといえる。

①セキュリティ人材の不足への対応
・ 全体集計、項目ごとの集計のいずれにおいても、「人材の不足」が課題となっている。
・ 被害の有無については、特定の業種等の偏りはみられなかった。
・ セキュリティ対策を行える人材が不足している一方で、業種等に関わらず被害を受ける可能性があることを踏まえると、いかなる企業であっても、被害を受けないとは限らない。人材がいないことで対応ができないのであれば、企業のニーズに合わせて、必要な知識や技術を持ったセキュリティ人材を育成・確保していくことが求められる。

②経営者の意識の向上
・ 全体集計、項目ごとの集計のいずれにおいても、社内（経営者、従業員）の危機意識の低さが課題とされている。
・ 危機意識が低いことは、昨今増加している標的型メールによる被害につながる可能性がある。また、特に経営者の危機意識が低いことは、必要とする対策に人員や費用をかけることに対して経営者が理解を示さず、その結果、対策が遅れることにもつながりかねない。
・ 担当者や専門部署が存在する企業であっても、被害を受けている例は少なくない。しかし、担当者や専門部署が存在する企業は、情報収集をより積極的に行っている傾向がみられ、セキュリティに対する意識は、担当者や専門部署が存在しない企業に比べて高いことがうかがえる。
・ まずは経営者の意識を高めていくことが重要である。そのうえで、経営者が、担当者や専門部署の配置などの対策を進めていくことで、企業のセキュリティ対策のレベルが上がっていくことが期待される。

2. 個人向けアンケート調査の結果

企業向けアンケート調査の結果、道内中小企業のサイバーセキュリティ対策における課題として、経営者や従業員の危機意識の不足が示唆された。

ただし、企業向けアンケート調査においては、アンケートの回答者が経営者である場合や従業員である場合など、さまざまな立場である可能性がある。このため、経営者と従業員との間でのサイバーセキュリティに関する理解や意識の差を把握することを目的に、「会社役員」及び「会社員」の区分で、個人向けのアンケート調査を実施した。

・調査方法
インターネット調査（楽天インサイト）

・調査対象
北海道内に事業所を有する企業の会社役員及び会社員（パート・アルバイト、契約社員、公務員を除く）

・調査時期
令和 3 年 3 月

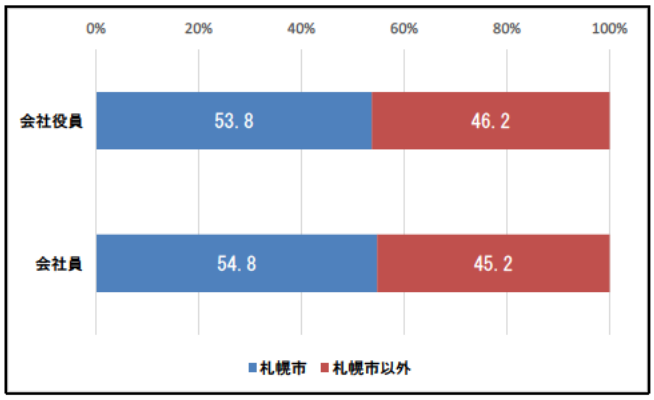
・回収数
会社役員 80 件、会社員 2000 件

・調査項目
- ・回答者属性（勤務先所在地、業種、従業員数）
- ・サイバーセキュリティに対する認知
- ・サイバーセキュリティ対策の現状
- ・これまでに受けたことのあるサイバーセキュリティ被害、被害を受けた際の対応
- ・勤務先におけるサイバーセキュリティ担当者の有無
- ・勤務先のサイバーセキュリティ対策の現状に対する認識
- ・勤務先でのサイバーセキュリティ関連の指導等の状況

（１）回答結果

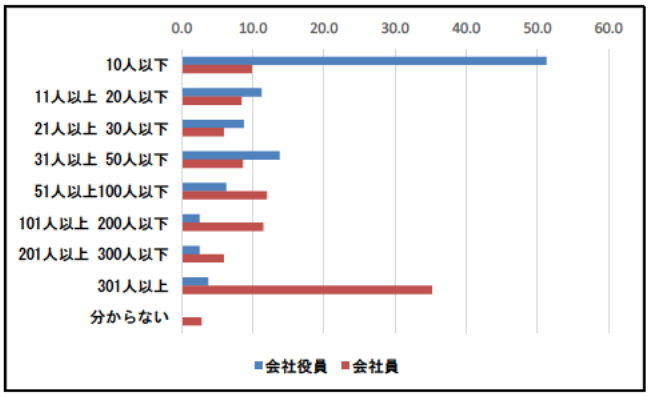
■回答属性

・勤務先所在地



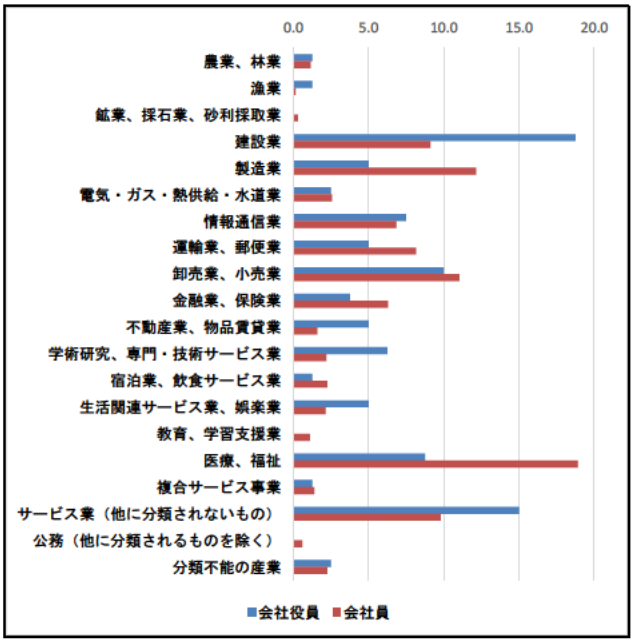
回答者の勤務先の所在地は、会社役員では「札幌市」が 53.8%、「札幌市以外」が 46.2%であった。また、会社員では「札幌市」が 54.8%、「札幌市以外」が 45.2%であった。

・勤務先従業員数



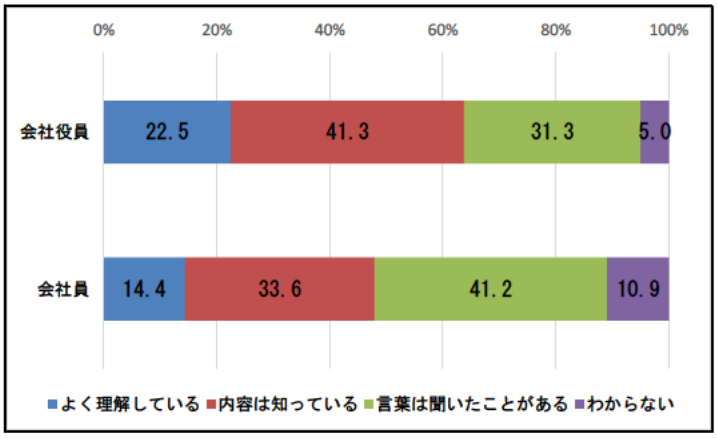
回答者の勤務先の従業員数は、会社役員では「10 人以下」(51.3%) が最も多い。会社員では「301 人以上」(35.2%) が最も多い。

・勤務先業種



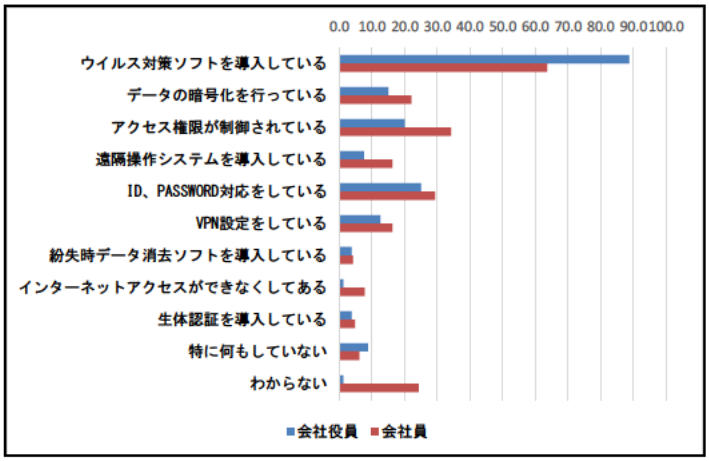
回答者の勤務先の業種は、会社役員では「建設業」(18.8%) が最も多く、次いで「サービス業」(15.0%)、「卸売業、小売業」(10.0%) の順であった。
会社員では「医療、福祉」(18.9%) が最も多く、次いで「製造業」(12.2%)、「卸売業、小売業」(11.1%) の順であった。

■サイバーセキュリティの認知度



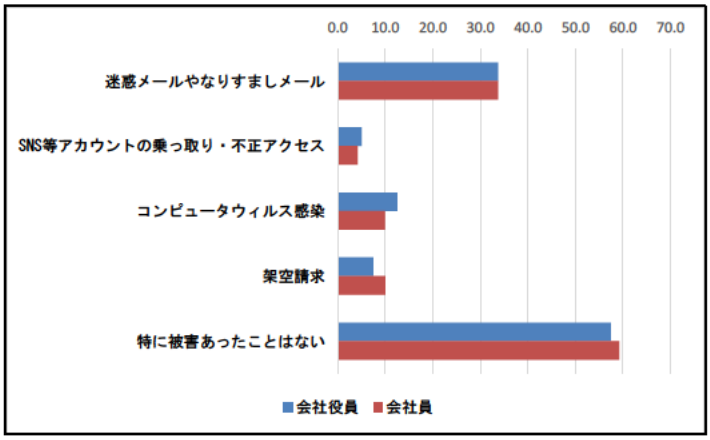
「サイバーセキュリティ」という言葉については、会社役員は「内容は知っている」(41.3%)が最も多く、次いで「言葉は聞いたことがある」(31.3%)、「よく理解している」(22.5%)の順であった。一方、会社員は「言葉は聞いたことがある」(41.2%)が最も多く、次いで「内容は知っている」(33.6%)、「よく理解している」(14.4%)の順であった。

■仕事で利用している端末（PC 等）のセキュリティ対策の現状



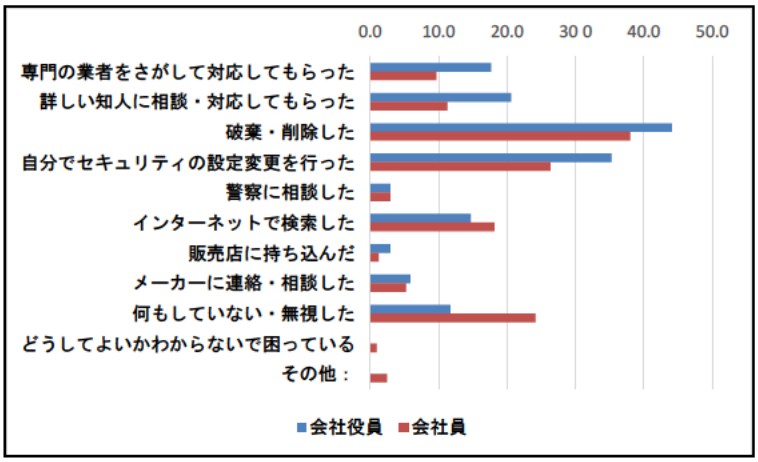
仕事で利用している端末(PC 等)のセキュリティ対策は、会社役員、会社員のいずれにおいても「ウイルス対策ソフトを導入している」が最も多い。
会社員では「わからない」が比較的多い。

■被害を受けた経験



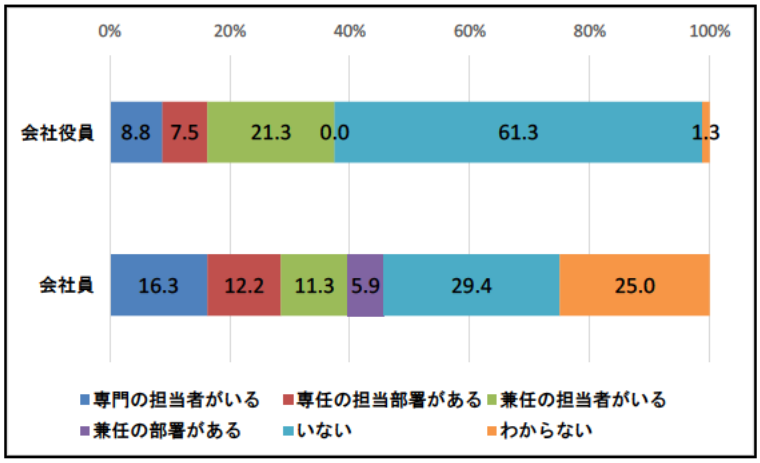
被害を受けた経験では、会社役員、会社員のいずれも「特に被害にあったことはない」が最も多い。被害を受けた中では、会社役員、会社員のいずれにおいても「迷惑メールやなりすましメール」が最も多い。

■被害にあったときの対応



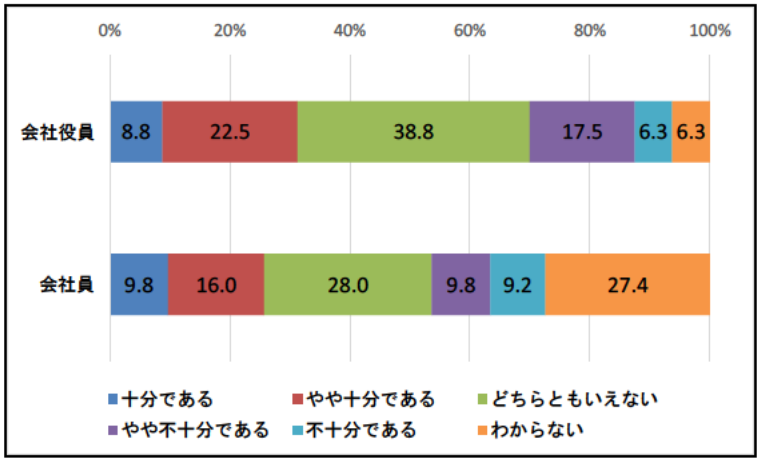
被害にあったことのある回答者に対して、被害にあったときの対応について尋ねたところ、会社役員、会社員のいずれにおいても「破棄・削除した」が最も多く、次いで「自分でセキュリティの設定変更を行った」が多い回答となった。
また、会社員では「何もしていない・無視した」が比較的多い。

■勤務先におけるサイバーセキュリティ担当者の有無



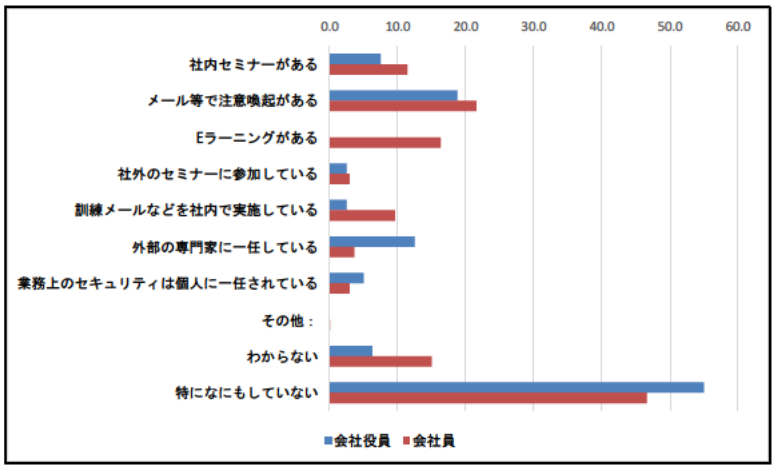
勤務先におけるサイバーセキュリティ担当者の有無については、会社役員では「いない」が最も多く、6割以上となっている。会社員でも「いない」が最も多いが、その割合は29.4%にとどまる一方、「わからない」が25.0%となっている。

■勤務先のサイバーセキュリティ対策の現状に対する認識



勤務先のサイバーセキュリティ対策の現状については、会社役員、会社員のいずれにおいても、「どちらともいえない」が最も多い。また、会社員では「わからない」が多くなっている。

■勤務先におけるサイバーセキュリティ教育の現状



勤務先におけるサイバーセキュリティに関する指導やセミナーについては、会社役員、会社員とも「特に何もしていない」が最も多い。

（2）まとめ

- サイバーセキュリティの認知度について、「よく理解している」「内容は知っている」との回答割合は、会社役員では半数以上、会社員でも半数近くに達しており、役職や立場に関わらずサイバーセキュリティはある程度認知されているといえる。
- また、勤務先におけるサイバーセキュリティ対策の現状に対する認識は、会社役員、会社員のいずれにおいても、「十分である」「やや十分である」が「やや不十分である」「不十分である」を上回っている。
- 一方、会社役員では、サイバーセキュリティ担当者について「いない」との回答が 6 割以上に達した。また、会社員では、仕事で利用している PC 等のセキュリティ対策について「わからない」との回答が 2 割以上に及んだ。
- 会社役員、会社員とも、サイバーセキュリティのことは知っており、現在の対策について比較的満足度が高い反面、勤務先におけるサイバーセキュリティ教育を特にしていないとの回答が最も多いなど、サイバーセキュリティに対する危機意識は、必ずしも十分であるとはいえない。

Ⅲ　道内におけるセキュリティベンダー・専門家等の発掘

道内におけるサイバーセキュリティ対策に関する人的ネットワークを強化・拡充するため、「道内」または「道内ゆかり」のセキュリティベンダー・専門家について、業界団体や学識経験者への聞き取り、インターネット検索、文献調査等を通じて、以下のリストを作成した。

【道内在住者】※五十音順

氏　名	所属等	備　考
飯田 勝吉	北海道大学　情報基盤センター サイバーセキュリティ研究部門 准教授	
大石　憲且	株式会社ネクステック代表取締役	
蒲田 拓也	専門学校講師	LOCAL 安全部部長
岸谷 隆久	株式会社イエラエセキュリティ取締役	
seigo (齋藤 聖悟)	株式会社澄川工作所	元 IIJ エンジニア、SECCON 実行委員
佐々木　伸幸	有限会社サンビットシステム代表取締役	
實吉 智裕	株式会社アットマークテクノ代表取締役	
砂原 悟	公立千歳科学技術大学　メディア教育センター 助教	
土居 茂雄	苫小牧工業高等専門学校 創造工学科 准教授 ・学術情報センター	
広奥　暢	北海道情報大学 情報メディア学部 情報メディア学科 准教授	
深町 賢一	公立千歳科学技術大学 専任講師	
福光 正幸	北海道情報大学 情報メディア学部 情報メディア学科 准教授	
前田 章博	ビットスター株式会社代表取締役	
三谷 公美	さくらインターネット株式会社	せきゅぽろ副代表
南 弘征	北海道大学 情報基盤センター サイバーセキュリティ研究部門 教授	
八巻 正行	株式会社クレスコ	せきゅぽろ代表

【「北海道ゆかり」の道外在住者】※五十音順

氏　名	所属等	備　考
磯原 隆将	株式会社 KDDI 総合研究所	北海道勤務経験あり
柏崎 礼生	国立情報学研究所 サイバーセキュリティ研究開発センター 特任准教授	北大出身、北大助教経験あり
坂 明	東京オリンピック・パラリンピック競技大会組織委員会 CISO	元北海道警察本部長
園田道夫	国立研究開発法人情報通信研究機構（NICT）	北海道内のイベント、講演等多数参加
Tessy (寺島 崇幸)	株式会社ディアイティ	北大出身
名和　利男	PwCJapan グループサイバーセキュリティ最高技術顧問	北見出身、航空自衛隊にてサイバー防衛を担当
西原 翔太	サイボウズ株式会社	旭川出身
西村　宗晃	株式会社リクルートテクノロジーズ　シニアセキュリティエンジニア	苫小牧高専出身
西本 逸郎	株式会社ラック代表取締役社長	北海道内のイベント、講演等多数参加
花岡 弥生	トレンドマイクロ株式会社	道警アドバイザー
平原 伸昭	クラウドセーフ株式会社代表取締役	札幌出身
藤田 優貴	合同会社 Georepublic Japan	室蘭出身、セキュリティミニキャンプ in 北海道講師
町村 泰貴	成城大学 法学部 教授（サイバー法）	北大出身
松田 和樹	日本マイクロソフト株式会社	札幌出身、せきゅぽろ元代表
八尾 崇	内閣サイバーセキュリティセンター（NISC）	せきゅぽろ創設に尽力
吉田 パクえ (吉田 雄哉)	日本マイクロソフト株式会社	札幌出身

Ⅳ　一般向けサイバーセキュリティセミナーの開催

道民一人ひとりのサイバーセキュリティの意識を全体的に底上げすることを目的として、北海道地域情報セキュリティ連絡会（HAISL）との連携により、以下のセミナーを開催した。

なお、開催にあたっては、新型コロナウイルス感染拡大の影響を考慮し、オンライン形式で実施した。

【開催概要】

●名　称：北海道地域情報セキュリティセミナー
●日　時：2020 年 12 月 1 日（火）13:15～16:20
●場　所：TKP 札幌カンファレンスセンター（札幌市中央区北 3 条西 3 丁目 1-6）カンファレンスルーム 6A にて撮影・配信
●形　式：YouTube Live によるオンライン配信
●主　催：北海道地域情報セキュリティ連絡会（HAISL）
●共　催：経済産業省北海道経済産業局、㈱道銀地域総合研究所、東日本電信電話㈱、北海道中小企業サイバーセキュリティ支援ネットワーク（通称「Cyber-道 net」）
●運　営：㈱道銀地域総合研究所

【プログラム】

１．主催あいさつ
北海道地域情報セキュリティ連絡会会長・北海道大学情報基盤センター教授
高井　昌彰　氏
２．情報提供
（１）コロナ情勢下におけるサイバー犯罪発生状況
北海道警察サイバーセキュリティ対策本部対策班長
坂野　雅樹　氏
（２）中小企業のサイバーセキュリティ対策等に関する調査 中間報告
株式会社道銀地域総合研究所　地域戦略研究部
大熊　一精
（３）人材育成（SC4Y）の取組等について
一般社団法人 LOCAL　理事
三谷　公美氏
３．講演
DX With CyberSecurity
グローバルセキュリティエキスパート株式会社　CSO
萩原　健太　氏

４．サイバーセキュリティお助け隊（北海道）中間報告
東日本電信電話株式会社　北海道事業部　ビジネスイノベーション部
担当課長　　苫米地　崇之
５．演習『サイバー攻撃演習～ゲームで学ぶ対処手順～』
東日本電信電話株式会社　経営企画部　営業戦略推進室
主査　　山崎　浩由

【参加者数等】

●当日ライブ配信閲覧数：90 名
●アーカイブ配信（後日視聴）閲覧数：61 名

●内容（要旨）

１．主催あいさつ
（北海道地域情報セキュリティ連絡会会長・北海道大学情報基盤センター教授
高井　昌彰　氏）
・ 新型コロナに対応した生活が日常となるなか、企業においては、テレワークやオンライン取引、3 密回避の取り組みなど、経営改革の手段として、デジタルトランスフォーメーション（DX）への関心が高まっていると感じている。
・ 一方、大企業の基幹システムが、マルウェア感染による被害を受け、情報が流出するニュースも頻繁に耳にするなど、サイバー攻撃の驚異も増大している。
・ 政府のサイバーセキュリティ戦略 2020 で提言されているように、「DX　with　サイバーセキュリティ」の考え方が重要となっている。こうした中、北海道において HAISL は、サイバーセキュリティの普及啓発活動を行っているが、今年度は実証的な取り組みも進めている。
・ 本日のセミナーがウィズコロナ時代におけるサイバーセキュリティを考えるきっかけとなり、セキュリティ対策の取り組みが加速する一助となることを期待する。

２．情報提供
（１）コロナ情勢下におけるサイバー犯罪発生状況
（北海道警察サイバーセキュリティ対策本部対策班長　坂野　雅樹　氏）
・ 犯罪件数全体では、平成 15 年以降連続で減少しているが、今年はとくに大幅な減少となっている。正確な検証はされていないが、コロナの影響が大きいとみている。
・ そうした中で、特殊詐欺は警察で認知しているものだけでも 7.9%増と増えている。その手口には、電話やはがきを使ったもののほか、「インターネットのバナー広告をクリックした」「SNS を通じてメールが送られてきた」などを発端として行われているものもある。特にインターネットの利用者は増加していると思われ、ネットの利用に不案内な高齢者を中心に被害が多い。
・ また、マスクの品薄に乗じた偽サイトを開設し、商品が届かないという詐欺や、政府

が配るマスクの抽選に当選したといった内容のメールによるフィッシングサイト誘導から不正アプリをダウンロードさせられて個人情報が盗まれる、ウイルスに感染する、などの被害も多数発生している。

- バナー広告をクリックすると、「ウイルスに感染しました」との警告が表示され、そこに記載されている連絡先に連絡すると、海外の関係企業を名乗り、ウイルス除去のサポート代金として電子マネーを要求してくるものもある。この手口は以前から存在しているが、今年はとくに多発している。
- 最近は、大手家具メーカーのニトリの偽のインターネットに関する相談が多い。偽サイトは日本語の記載や漢字の表記、文章がおかしい、値段が安すぎるなど、おかしな箇所があるので、そういったところを疑ってみてほしい。

（2）中小企業のサイバーセキュリティ対策等に関する調査 中間報告

（株式会社道銀地域総合研究所　地域戦略研究部　大熊　一精）

- 北海道経済産業局からの委託として 9 月に実施した「中小企業のサイバーセキュリティ対策等に関する調査」の結果について、中間報告を行った。

（3）人材育成（SC4Y）の取組等について

（一般社団法人 LOCAL　理事　三谷　公美 氏）

- 一般社団法人 LOCAL は北海道における技術系地域コミュニティを支援して、コミュニティ間の連携を通して地域を盛り上げていくことを目指して活動中。所属や年齢・立場の垣根を越えて、多数の技術者や学生が所属している。
- セキュリティ人材の育成は、まず、IT リテラシーやセキュリティ意識を高めて、情報の活用能力を高めていくことから始まる。次に、好きな IT 関連分野の能力を育てる。プログラミングや、電子工作などが代表例だが、好きなものを楽しんでもらえばよい。その次の段階として、セキュリティ人材への階段を登ってもらう。
- セキュリティ人材の不足はとても深刻な問題。次世代のエンジニアたちに機会を提供することで、セキュリティ人材を増やし、更に高みを目指せるようにしたい。
- インターネット安全教室を行っている。保護者も対象に、スマートフォンやインターネットを安全に適切に利用するため、情報モラル、情報セキュリティを説明する。
- さらにレベルの高いものとしては、オンラインでのディスカッションイベントを開催した。「新しい生活様式と IT 活用法」をテーマに、19 名が参加。通常のイベントでは参加者が札幌在住者に偏る傾向があるが、今回はオンラインであったため、函館からも参加があった。
- IT 関連分野などの能力を育てるためには、U-16 プログラミングコンテストを開催している。参加する若者たちには「楽しい」「嬉しい」「同じようなことが好きな仲間と出会ってほしい」といったことを期待している。今年はオンラインで開催。
- スキルのある人材を育てていくことを目的に、セキュリティミニキャンプを開催。これは、25 歳以下の大学院生や学生を対象とした情報セキュリティ人材の発掘育成イベントであり、LOCAL は北海道大会の主催団体として参加学生を支援している。従

来は、膝を突き合わせていろいろなプログラミングをしていたが、今年はオンラインを組み合わせたハイブリット開催となった。

・ こうした年齢層よりも高い年齢層を育てるイベントを開催したいと考え、セキュリティカレッジ・フォー・ユース、略して SC4Y というイベントを開始した。ここでは、社会のさまざまな分野で活躍する学生や青年層に、サイバーセキュリティに関する試験や技術体験をしてもらい、将来のセキュリティリーダー、ホワイトハッカーになりえる人材を発掘、育成していき、社会全体のセキュリティ対処能力の底上げをしていくことを目指している。

3．講演「DX With CyberSecurity」

（グローバルセキュリティエキスパート株式会社　CSO 萩原　健太 氏）

・ デジタルトランスフォメーション（DX）について、きちんと理解されていない方も多いとの印象を持っている。単純には IT 化だが、データ化したものを活用するため、使えるように変換することであり、そこからさらに自分の想像力によるクリエイティブが重要になってくる。その創造の連続性が必要。
・ DX を導入すると、当然、知識や技術など必要な部分が出てくる。想像力を最大限に働かせないと、実際の DX はきちんとできない。
・ 大企業ほど進んで DX に取り組んでいると言われているが、本当にできているのかは疑問。今まで成功してきた企業では、現状維持へのバイアスがかかりがち。変革には勇気が必要。DX に対するこのバイアスを排除していく必要がある。
・ DX とはどういうことか。データ化したデータをさらに分析して、そのデータから新しい事業を生み出す、そのための作業になる。組織内で DX を進めるためには、目標の設定が大事。
・ セキュリティ運用はできることからやっていくことが大事。セキュリティ強化には、グループポリシーの強化などすぐにできることもたくさんある。それをやらずにセキュリティ製品を新しくするというのは、少し違うのではないか。製品をバージョンアップするだけでも日々できることがある。ソフトウェアはアップデートが前提なので、更新していない、できない環境という発想は企画段階から甘い。
・ セキュリティの本質は、インシデントが 1 つ発生しても被害を最小限にすること。説明責任を果たすためのセキュリティ対策ができているのか、という視点で見極めていく必要がある。
・ 事業を継続するために行うことがセキュリティ対策。自分の PC にもサーバにもあるデータがすべて。失ってしまった場合には、事業継続自体に影響がある可能性もある。バックアップのとり方も含めて、事業を継続するためのセキュリティを選んでいるか、というところを、是非考えてほしい。

4．サイバーセキュリティお助け隊（北海道）中間報告

（東日本電信電話株式会社　北海道事業部　ビジネスイノベーション部担当課長
苫米地　崇之　氏）

・ 経済産業省の補助を受け、中小企業のサイバーセキュリティ対策の不安を解消するための「サイバーセキュリティお助け隊」事業を行っている。具体的には、「参加した中小企業から相談を聞いてリモートサポートを行う」、「その相談窓口となる」、「相談内容に対応した対応機器を設置する」、「対応復旧を支援する」という 4 つの事業を行っている。
・ セキュリティが経営上のリスクであるということを認識している割合は、全国では 25%であるのに対し、北海道は 41%と非常に高い。一方、セキュリティ対策に対する意識は、全国平均 34%に対して、北海道は 24%と低い。そのため、実証事業を通じてセキュリティ意識の向上を図っていきたい。
・ 提供しているコンテンツは大きくわけて 4 つ。ホームページの脅威診断、スキミング耐性、サイバーセキュリティ対策、入口対策である。
・ 中小企業のセキュリティ意識向上には従業員の教育を重視している。その一環として、標的型メール訓練を抜き打ちで行うこともある。
・ 短期間の事業だが、10 月の結果だけでも非常に多くの脅威にさらされていることがわかった。参加企業へのスパムメールは 11 社で計 516 件検知され、1 社で 400 件の受信の例もあった。規模の大小に関係なくさまざまな企業が標的となっており、中小企業でも大企業と同様なリスクを抱えている。

5．演習『サイバー攻撃演習～ゲームで学ぶ対処手順～』
（東日本電信電話株式会社　経営企画部　営業戦略推進室　主査　山崎　浩由 氏）
・ 東日本電信電話（株）の専用エクセルファイルを用いて、サイバー攻撃に関する演習を実施。本演習では、実際にサイバー攻撃を受けた際に、適切な行動を取るために何をどう判断したらよいか、をゲーム感覚で体験。仮想ではあるが、結果として被害想定額という目安が出てくる。

Ⅴ　サイバーセキュリティ人材育成に向けたカリキュラム検討・開発

1. 現状調査

全国の先進事例を対象に、サイバーセキュリティ人材育成の現状について文献調査やヒアリング（オンライン）による調査を実施した。

(1)特定非営利活動法人日本ネットワークセキュリティ協会

【概要】

名　　称	特定非営利活動法人日本ネットワークセキュリティ協会
設　　立	2001 年
所 在 地	東京都港区西新橋 1－22－12　JC ビル 4F
代 表 者	会長　田中英彦（情報セキュリティ大学院大学　名誉教授）

- 我が国の情報セキュリティを護る企業の先駆的な集まりとして、最新課題のワークショップや勉強会、情報セキュリティの啓発セミナー等を開催。
- カリキュラムのテーマや内容は、協会内に設置されている専門部会で決めている。基礎的なことだけでなく、時代のトレンドに合わせた話題なども考慮している。
- 専門の講師を派遣することも可能。地域で勉強会などを開催されるのであれば、声をかけていただければ協力する。

（2）一般社団法人京都スマートシティ推進協議会

【概要】

名　　称	一般社団法人京都スマートシティ推進競技会
設　　立	2018 年
所 在 地	京都府京都市下京区中堂寺南町134 京都産業支援センター 2階
代 表 者	代表理事　重松千昭

- ハッキングコンテストは、主として初心者向けの内容で開催。完全な初心者でも対応できる内容を中心としつつ、上級者向けの課題も含めた。
- 初心者向けの内容は、ネット検索を行いながら取り組めば回答できるようなレベル。
- 多くの方に参加いただくよう主として初心者向けの内容とした。将来的には専門的な内容にしていきたいが、現状ではまだまだと思われる。
- カリキュラムは PwC Japan グループの協力を得て策定した。

（3）特定非営利活動法人情報セキュリティ研究所（サイバー犯罪に関する白浜シンポジウム）

【概要】

名　　称	特定非営利活動法人情報セキュリティ研究所
設　　立	2002 年
所 在 地	和歌山県田辺市新庄町 3353-9 Big･U 内 104 号室
代 表 者	代表理事　臼井　義美（臼井技術士事務所）

- 1997 年にスタートした「サイバー犯罪に関する白浜シンポジウム」に携わるスタッフを中心として、シンポジウムを継続して運営する核となる組織を作る必要があると考え、NPO 法人「情報セキュリティ研究所」を設立した。
- 代表理事の臼井氏は、ソフトウェア会社の出身。取引先である和歌山県警の仕事に携わるうち、警察が扱うコンピュータ関係の犯罪が増えているが、警察自身は、ハイテク犯罪の知識も経験もなく、全く対応できないという実態がわかった。そこで、従事していた警察のシステム完成記念として、全国の警察関係者に最新のハイテク犯罪の概要とその捜査技術を勉強する機会を提供しようと「コンピュータ犯罪に関するシンポジウム」の開催を提案した。
- 当初、警察関係者は　コンピュータ犯罪について全く理解ができず、講師も説明に苦慮していたが、回を重ねるにつれて、 コンピュータ犯罪の国際性とセキュリティ対策の重要性が理解されるようになった。
- その後、「情報セキュリティワークショップ in 越後湯沢」、「サイバーセキュリティシンポジウム道後」、「サイバー防衛シンポジウム熱海」、「九州サイバーセキュリティシンポジウム」と各地で特色のあるシンポジウムが開催されるようになり、これらを情報セキュリティの温泉シリーズと呼ぶようになり、それぞれの実行委員会や事務局とは、情報交換を行っている。
- 北海道でも登別温泉で開催を検討したことがあるが、現地との接点が見つからず、実現には至っていない。
- シンポジウムのテーマや講師は、実行委員会で議論して決定するが、会場の無線システムの構築や、参加者の受付、危機管理コンテストの運営、セキュリティ道場の運営などは、実行委員の所属団体によるボランティアや、役務協賛、業務委託により作業をお願いしている。

（4）サイバーセキュリティシンポジウム道後実行委員会

【概要】

名　　称	サイバーセキュリティシンポジウム道後実行委員会 （事務局　一般社団法人テレコムサービス協会四国支部事務局内）
所 在 地	愛媛県松山市大手町 1-11-4（一般社団法人テレコムサービス協会四国支部）
代 表 者	実行委員長　小林 真也（愛媛大学大学院　教授）

- 今年で 10 回目の開催。当初は道後温泉のホテル近傍を使っていたが、参加者が増えたことや、スポンサー企業の展示スペースが足りなくなってきたこともあり、2018 年からは同じ道後地区にある愛媛大学に場所を移してより多くの人に見ていただけるようにした。
- 参加者は 90～95%が四国外。その中でも三大都市圏が多い。
- 10 年前に総合通信局からの働きかけで始まったが、現在は、愛媛県警をはじめセキュリティ企業との繋がりも深い。なお、SEC 道後以外にもセキュリティ関連イベントとして、県警を中心に、地元向けのワークショップなどを、年間を通じて行っている。講師選定はプログラム検討委員会が担当。テーマは実行委員会で決めている。最新のセキュリティ動向に関するものだけでなく、地元の人たちにとって身近な題材を使った愛媛県警によるセミナーもある。

（5）九州サイバーセキュリティシンポジウム実行委員会

【概要】

名　　称	九州サイバーセキュリティシンポジウム実行委員会
所 在 地	（連絡窓口）株式会社ラック　新規事業開発部 福岡県北九州市小倉北区浅野 3-8-1 AIM ビル 8F ラック テクノセンター北九州
設　　立	2018 年
代 表 者	尾家　祐二（国立大学法人九州工業大学）

- 温泉地のシンポジウム（当時は白浜、越後湯沢、道後の 3 ヶ所で開催）の 4 つ目を別府でやりたいとのことで始まった。
- 開催を検討し始めた当初は、ネガティブな反応が多かった。地域でイベントをしていくときにハブになってもらう企業がない、中小企業が多いこともありセキュリティに対する関心や意識が低い、などが背景にある。
- 先行していた白浜、越後湯沢、道後は、いずれも東京からの参加者が半数以上を占め、そこに地域のセキュリティ関係者が集まってきているが、こちらは九州に主眼を置いてやりたいと考えており、広報なども九州を中心にやっている。
- ワーキンググループやセミナーは地域の特性に合わせてやっている。九州工大の学長が委員長に立ったこともあり、大学向け、学生向けも多少意識するものとなった。シンポジウムには東京からの参加者も多いが、地域の特性を考えて、その地域に合わせた内容とすることが大事。

（6）九州大学サイバーセキュリティセンター

【概要】

名　　称	九州大学サイバーセキュリティセンター
所 在 地	福岡市西区元岡 744
設　　立	2014 年
代 表 者	センター長　岡村　耕二

- 厚生労働省の事業を活用し、社会人向けのサイバーセキュリティ教育を実施。
- 大学院レベルを想定。受講者の一部から「難しい」との声はあったが、入門用の事前教材の作成や、参考図書の案内などによってカバーした。とにかくレベルを下げることはせず、ここが到達点だと示してなんとかたどり着いてもらうことを目指した。
- カリキュラムは、検討委員会で大枠を決めたうえで、各分野に詳しい先生と話をして進めてきた。最新の内容を盛り込むなど、途中で変えることもあった。
- 修了証を発行し、ここを出たことがブランドの一つになるようにしていきたい。

(7)各団体のカリキュラム

これらの6団体が提供しているサイバーセキュリティ人材育成に向けたカリキュラムについて、直近の開催内容を以下に整理する。

団体名	主な開催テーマ
日本ネットワークセキュリティ協会	・デジタル社会におけるトラスト(変貌するトラストアーキテクチャ、デジタルトラストにおける法と技術のあり方) ・デジタル社会に不可欠なサイバーセキュリティ標準化動向 ・情報セキュリティマネジメント・セミナー(サイバーセキュリティにおける ISMS の役割、ISOIEC 27000 ファミリー規格の最新動向、実践かつ効果的なセキュリティ教育等) ・新しい働き方のサイバーセキュリティ対策 ・産業分野におけるサイバーセキュリティ政策
京都スマートシティ推進協議会	・海外におけるスマートシティ×デジタルリスク ・改正法案など昨今の動向から考えるプライバシーリスクとその対応 ・スマートシティ×個人情報における法律観点の考慮点について ・With コロナの時代に求められるゼロトラスト確立にむけて ・ゼロトラストを実現するためのポイントと事例を踏まえて
情報セキュリティ研究所(サイバー犯罪に関する白浜シンポジウム)	・この1年のサイバー関連法制の動向を振り返る ・安心・安全で信頼性のある AI の社会実装に向けて ・スマートサイバー　AI 活用時代のサイバーリスク管理 ・機械学習による、ダークウェブの匿名マーケットに関する研究 ・AI(Artificial Intelligence)活用の現状と課題
サイバーセキュリティシンポジウム道後実行委員会	・With／after コロナで加速するDXとセキュリティ ・わたしのかんがえたさいきょうのフィッシング対策 ・システム・モニタリング×セキュリティ～システム設計・運用者の視点から～ ・ニューノーマル・サイバーセキュリティ経営ガイドライン ・なぜでひも解くサイバーセキュリティの基礎～オンライン時代に何が変わって何が変わっていないのか～
九州サイバーセキュリティシンポジウム実行委員会	・LINE Fukuoka でのエンジニアの働きかた～これからのエンジニアに求められること ・人文系学部から始める、不思議のエンジニアキャリア～セキュリティに関係したりしなかったり ・未来から学ぶ～AI と量子コンピュータに取り組む企業が感じていること～
九州大学サイバーセキュリティセンター	・サイバーセキュリティ法制 ・サイバーセキュリティとイノベーション ・BCP 体験型 TTX 机上演習

2. カリキュラムの検討・開発・実証

道内において情報交換や勉強会等を実施している IT コミュニティ「一般社団法人 LOCAL」の協力により、サイバーセキュリティ人材育成のためのカリキュラム案を開発し、学生等を対象として、その実証を行った。

カリキュラム案及び実証の結果については、以下のとおりである。

(1)カリキュラムの概要

「セキュリティ人材の育成」を大きなテーマとし、情報セキュリティ技術に興味のある学生および若手人材をターゲットとして、以下 3 項目を目的としたカリキュラムの開発を行った。

- 今後、社会の様々な分野で活躍する学生、青年層にサイバーセキュリティに関する知見、技術を体系的に身につけてもらう
- 将来のセキュリティリーダーやホワイトハッカーになり得る人材の発掘と育成
- 知見や技術のある青年層を輩出することによる社会全体のセキュリティ対処能力の底上げ

上記の目的達成のため、「定期的な勉強会を開催し、段階的に知識を身につける」→「競技会や CTF（Capture The Flag＝旗取りゲーム、情報セキュリティの技術を競う競技・ゲーム）などへ参加し、勉強会の結果を発揮する力試しを行う」→「その結果を振り返り、更なる学習のための反省を行い、教訓とする」のサイクルを実現するものとし、これらの要件を満たすための情報セキュリティ関連イベントの開催を行った。

(2)カリキュラムの内容

①Security College for Youth の開催

「Security College for Youth」(以降、「SC4Y」) と題し、北海道内在住の 30 歳以下を対象として、3 カ年計画で毎回テーマを設けた定期的な勉強会を開催した。開催回数は計 4 回。それぞれの概要は以下のとおり。

名称	テーマ
SC4Y ('20#1) サイバーセキュリティ 脆弱性対応 (防災訓練)	bash の脆弱性対応を例に、未来の脆弱性に対しての知識と心構えを学ぶ。 また、脆弱性が発見された際、実際の情報セキュリティ担当者はどのように振る舞い、対応するのか、参加者に追体験してもらうことで情報セキュリティ担当者の役割と仕事を理解してもらう。
SC4Y ('20#2) Web システムにまつわる脆弱性の検査手法	SQL インジェクション、OS コマンドインジェクション等を例に Web システムの脆弱性検証の実習を行う。 これらの脆弱性の動作原理を理解し、今後システムを設計、開発するうえで必要となる教養を習得する。
SC4Y ('20#3) IT・情報系 北海道まったり LT 大会	「LT」とは「ライトニングトーク (Lightning Talks)」の略で、5 分程度の決められた時間中でのプレゼンテーションである。若手に登壇と発表の機会、トレーニングの場を提供し、楽しみながらも積極的にアウトプットする習慣を身につけてもらう。 また、様々なバックグラウンドを持つ現役の IT 技術者、IT 勉強会コミュニティ運営者との交流の場を設け、学内だけでなく、社会人コミュニティにも学習の場と勉強仲間が存在することを知ってもらい、視野を広げてもらう機会とする。 ※ 発表と交流会への参加障壁を低減するため、勉強会のタイトルは緩いものとする。
SC4Y ('20#4) Ghidra ハンズオン・ワークショップ	ソフトウェアリバースエンジニアリングツール「Ghidra」を用いて、マルウェア解析の実習を行う。 また、情報セキュリティ業界の第一線で活躍する講師陣より直接解説、手解きを受けることで、将来なりたい姿と目標をイメージする機会とし、更なる学習意欲の向上をねらう。

当初は、講師、運営、受講者が一カ所の会場に集まる集合研修方式での開催を予定していたが、新型コロナウイルス感染防止対策を講じる必要性が生じたため、全 4 回の講義をすべて、Zoom を利用したオンライン形式で開催した。

また、講義の模様は YouTube Live による同時配信を行った。YouTube Live による視聴は年齢制限無しとし、情報セキュリティを学びたい広い年齢層と職業人に対して学習機会を提供した。

運営にあたっては、講師、オンライン配信係、司会進行係に加え、リアルタイムで受講者のサポートができるよう TA（ティーチング・アシスタント）を設けた。Zoom に加え Slack を併用して受講者と双方向のコミュニケーションをとることで、受講者が講義内容に躓いても置き去りにされないようサポートを行った。

②[特別講義]サイバーセキュリティ オンライン・カンファレンス in NoMaps の開催

特別講義として、毎年札幌市で開催されるイベント「NoMaps」に出展し、「サイバーセキュリティ オンライン・カンファレンス in NoMaps 『Digital World beyond Pandemics』」を企画・開催した。

本カンファレンスのねらいは、情報セキュリティに関する知見を一般向けに広く共有することである。コロナ禍における産・学・官・民の取り組みをサイバーセキュリティの視点から振り返り、その知見を共有すると共に、これからの未来像を考察して将来に備えることをテーマに、カンファレンスとディスカッションを行った。

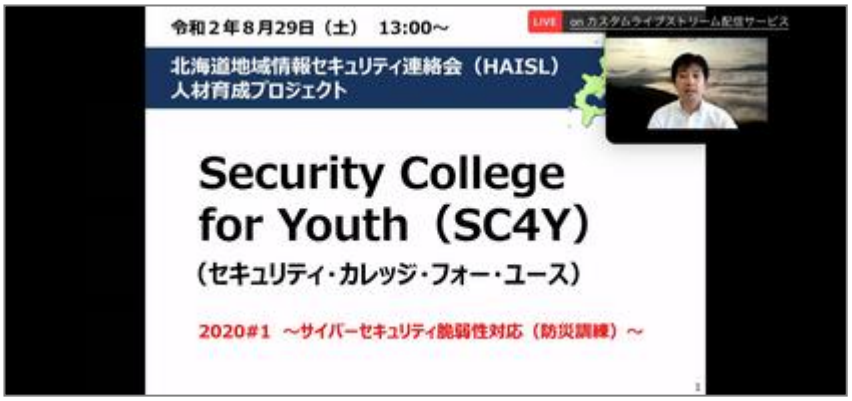
また、カンファレンスではコミュニティ運営の立場を代表して LOCAL の西原理事が登壇し、「with コロナのオンラインイベント運営」と題し、SC4Y の運営、取り組みについても紹介した。

(3)カリキュラム実施報告

①第 1 回 SC4Y

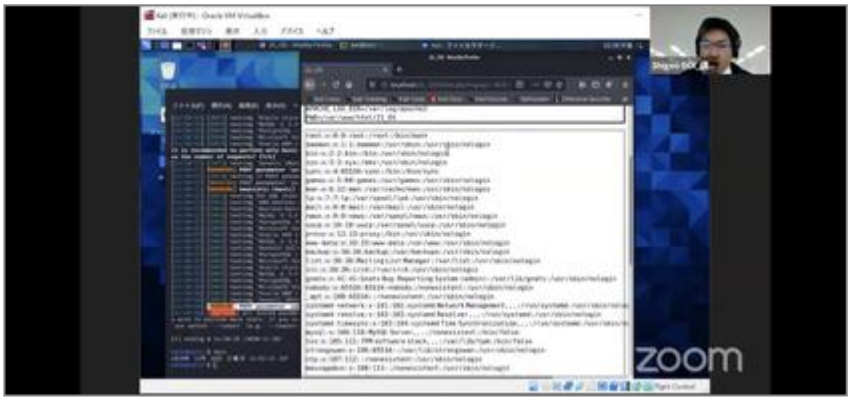
開催名称	SC4Y ('20#1) サイバーセキュリティ 脆弱性対応（防災訓練）
開催日時	2020/8/29（土） 13:00 - 17:00
場所	オンライン、千歳科学技術大学
主催・共催	主催：北海道地域情報セキュリティ連絡会（HAISL）
後援・協力等	協力：一般社団法人 LOCAL
講師	北海道警察 サイバーセキュリティ対策本部、 砂原 悟（千歳科学技術大学）
告知 URL	https://sc4y.connpass.com/event/184894/
参加人数	50 名（Zoom：15 名、YouTube Live：35 名）
イベント概要	2014 年に世の中を騒がせた bash の脆弱性「shellshock」の対応を追体験することで、未来の脆弱性に対しての知識と心構えを学ぶ。 講師および配信スタッフは千歳科学技術大学より講義コンテンツの配信を行い、TA・運営はオンラインにて受講者をサポートする。
プログラム内容	13:00 - 13:05 SC4Y 趣旨説明 13:10 - 13:30 サイバーセキュリティと倫理 ・北海道警察 サイバーセキュリティ対策本部 より ・法とサイバーセキュリティ技術について 13:35 - 16:00 サイバーセキュリティ 脆弱性対応（防災訓練） ・千歳科学技術大学 砂原 先生より 1. shellshock の概要 2. 技術的な要素の紹介(OS, bash, apahce, HTTP Header 等) 3. ラボ環境の解説 4. [ハンズオン]ラボ環境にて PoC(Proof Of Concept)を実行 5. [ハンズオン]攻撃が成立した場合の証拠集め(ログ検索) 6. [ハンズオン]不完全なアップデートという罠について 7. 脆弱性対策のための情報収集について 8. 脆弱性対応の優先度について 9. この脆弱性はどのように発見されたのか 10. 脆弱性を作りこまないために私たちができること 16:00 - 17:00 参加者交流会 ・Zoom 参加者のみでの交流会、意見交換
参加者からの質問等	【質問】 基礎技術が大事であることはわかっているが、学び続けるモチベーションが保てない。

	【回答】 「ものを作る活動」に軸を置いて、その製作物の完成度をあげる取り組みの中でセキュリティを意識したつくりとするような形で学習するとよい。セキュリティそのものを学ぶというよりは、要素技術としてセキュリティを意識できる素養をつけていくほうがやる気も保てるのではないか。
主催者所感	【砂原 悟（千歳科学技術大学）より】 今回は shellshock という事例から、「LAB（検証）環境の構築や、PoC を使った検証、ログ調査の方法」をメインに進めていきましたが、実は「脆弱性が発見されたときの組織的な対応・対策をどのように進めたらよいかを考える」という隠れたテーマがありました。未知の被害を防ぐことは難しいのですが、既知の事例を学び、日頃の備えにつながればと考えております。 【南 弘征（北海道大学）より】 若人に CSIRT 組織論を語ってもなかなかピンとこない（自分が仕切る側に回ることは社会構成上、おそらく少ないし、いきなりそうなったら可哀そうすぎる）と思うため、とりあえずは公知脆弱性の情報入手→管理下機器の状況確認(→穴の影響の実地検証)→穴塞ぎまでを会得してもらうべく、そのバックグラウンドを身につけてもらう、ということになるのだろうと思います。 終了後のコメントにあった「基礎的な話ではモチベーションが続きにくい」は、このあたりのストーリーが沁み込んでいないところで、知らない話が飛び交うとついていけないということかな、と想像するため、そのあたりの建付けから語らないと、ゲーム要素というかドラマ仕立てみたいに万事捉えてしまうようでは、黒い方に行きたくなったりするかもしれず、まずいかもしれませんね。

当日の様子	   

②第 2 回 SC4Y

開催名称	SC4Y ('20#2) Web システムにまつわる脆弱性の検査手法
開催日時	2020/11/28（土） 13:00 - 16:30
場所	オンライン、千歳科学技術大学
主催・共催	主催：北海道地域情報セキュリティ連絡会（HAISL）
後援・協力等	協力：一般社団法人 LOCAL
講師	土居 茂雄（北海道苫小牧工業高等専門学校）
告知 URL	https://sc4y.connpass.com/event/194241/
参加人数	39 名（Zoom：8 名、YouTube Live：31 名）
イベント概要	SQL インジェクション、OS コマンドインジェクション等を例に Web システムの脆弱性検証の実習を行う。 事前に LAB 環境を構築しておくことに加え、課題として「サイバーセキュリティと倫理」の動画を視聴することとした。
プログラム内容	13:00 - 13:10 SC4Y 趣旨説明 13:35 - 15:45 Web システムにまつわる脆弱性の検査手法 1.Web の脆弱性の要素 2.要素やツールの紹介(Apache, PHP, etc) 3.仮想環境の解説 4.脆弱性の検証 5.脆弱性をなくすためのコーディング技法 6.脆弱性をなくすための運用 15:45 - 16:30 参加者交流会 ・Zoom 参加者のみでの交流会、意見交換
参加者からの質問等	【質問】 セキュリティ技術を学ぶには何から手をつけたらよいか。 【回答】 CTF に取り組んでみると感じると思うが、コンピューターサイエンスやプログラミング、ネットワークなど多岐に渡って知識が必要となるため、まずはある特定の分野に絞ってやり始めるのがよい。SECCON などの CTF やセキュリティ・キャンプ、SecHack365 などのイベントに参加することも意義深い。
主催者所感	【西原 翔太（一般社団法人 LOCAL 理事）より】 第 2 回は Web に関する脆弱性診断の実践演習を行った。ねらいは、参加者が Web に関する脆弱性について知識を得て、実践形式で理解を深めることである。このテーマはサイバーセキュリティを専攻する大学等を除けば、授業演習では取り扱われることのないテーマで、参加者は日頃の学習と別の観点からの学びがあったのではないかと感じた。SC4Y の参加学生は所属学科や知識背景も様々であるが、短時間で実施可能な内容に落とし込んでいただ

	いた土居先生のご尽力あっての会であった。
当日の様子	  

③第 3 回 SC4Y

開催名称	SC4Y ('20#3) IT・情報系 北海道まったり LT 大会
開催日時	2021 年 2 月 10 日（水） 19:00 - 21:00
場所	オンライン
主催・共催	主催：北海道地域情報セキュリティ連絡会（HAISL）
後援・協力等	協力：一般社団法人 LOCAL
講師（発表者）	事前募集した参加者 15 名 （学生、教員、IT 技術者、IT コミュニティ運営者 等）
告知 URL	https://sc4y.connpass.com/event/202331/
参加人数	51 名（Zoom：15 名、YouTube Live：36 名）
イベント概要	北海道内の IT 勉強会コミュニティ「IoTLT 札幌」「Java Do」「LOCAL 学生部」「ゆる Web 勉強会 札幌」とコラボレーションし、LT 大会を行う。発表内容は IT・情報系に関連することであれば何でも OK とし、特に学生、若手による発表を歓迎する。
プログラム内容	19:00 - 19:10 各団体からのご挨拶 19:10 - 19:55 LT 第 1 部 1.セキュリティについての何か(仮) [shigyo] 2.Docker Rootless mode を使ってみよう (仮) [haibara] 3.高専の学生実験を作った話 [ns] 4.PHP で個人ブログを作りました [うーたん] 5.スマートな在寮管理システムを作りたい [ツジナガ] 6.技術ブログのススメ(仮) [pipinosuke] 7.小学校でプログラミング教育してきました [松浦康士郎] 20:00 – 20:55 LT 第 2 部 8.いまどきの暗号 [mfuku] 9.空港の気象レーダに邪魔されない無線 LAN を作りたい [ravicot] 10.SBC ユーザに伝えたい、IPA で命を落としかけた話 [イオティ] 11.新しい Web サービスの開発 [シシオタ] 12.OCR について調べてみた [takapiro_99] 13.レゴプログラミングで学ぶ、7 歳からのセキュリティ(仮) [gishi_yama] 14. MySQL 8.0 で変わった DATE 型のやべぇ挙動 [けんつ] 15. 茶の間 Co-KoNPILe [tomio2480] 20:50 - 20:55 クロージング 20:55 - 22:00 参加者交流会 ・Zoom 参加者のみでの交流会、意見交換

参加者からの質問等	【質問】 日本人って機械相手に話すのが苦手なような印象がありますが、子供たちもスマートスピーカーに呼びかけるのに抵抗がありましたか？ 【回答】 子供たちは恥ずかしがらずに使っていたが、活舌でなかなか認識しないなどがあった。 ※ 他、交流会では多数の質問と回答あり。
主催者所感	【三谷 公美（一般社団法人 LOCAL 理事）より】 北海道で活動している IT コミュニティと連携することにより、登壇者は社会人が 7 名、学生・U30 は 8 名という、とても賑々しい会となりました。 道内でコミュニティを運営している人、活動に参加している人を中心に、電子工作からプログラミングまで、様々な分野での登壇があり、知識の共有や幅広い交流が発生していました。 また、LT 大会後には、参加者ひとりひとりへ、有識者からの全体を俯瞰した振り返りとコメントがあり、ゆったりとした雰囲気で発言の多くない参加者からの言葉も引き出すことができ、フィードバックを得るための有効な手法に気づきました。 コミュニティを運営する人たちに、セキュリティの視点から考える機会を与えることができること、また、様々な分野、層へのアプローチにより、普段あまりセキュリティを意識していなかった人に、セキュリティの視点を知ってもらうことができるのは、社会にとって、大変有意義な活動につながるため、定期的な開催も検討していきたいです。
当日の様子	

当日の様子	   

④第 4 回 SC4Y

開催名称	SC4Y ('20#4) Ghidra ハンズオン・ワークショップ
開催日時	2021 年 2 月 28 日（日）12:50 - 16:20
場所	オンライン
主催・共催	主催：北海道地域情報セキュリティ連絡会（HAISL）
後援・協力等	協力：一般社団法人 LOCAL 協力：北海道情報セキュリティ勉強会（せきゅぽろ）
講師	中島 将太（Allsafe） 原 弘明（Allsafe）
告知 URL	https://sc4y.connpass.com/event/204104/
参加人数	58 名（Zoom：7 名、YouTube Live：51 名）
イベント概要	米国家安全保障局（NSA）が公開したソフトウェアリバースエンジニアリングツール「Ghidra」を用いて、マルウェア解析の基礎から Yara ルールの作成まで行う。 マルウェア解析初学者向けの内容であるが、前提として Ghidra 動作環境を構築しておく必要あり。
プログラム内容	12:50 - 13:00 SC4Y 趣旨説明 13:00 - 13:30 Basic of Malware Analysis ・マルウェア解析とは何なのか、具体的にどのように行うのか、解析の基礎部分を学ぶ 13:30 - 15:00 Static Analysis with Ghidra ・サンプルプログラムの解析を通じて、Ghidra の基礎的な使い方や実践的な静的解析手法を学ぶ 15:10 - 16:10 Write Yara Rule with Ghidra ・静的解析のアウトプットとして、マルウェアを識別および分類するための Yara ルールを作成する
参加者からの質問等	【質問】 講師のお二人のように、セキュリティ業界で活躍できるようになるためには、学生時代にどんなことをやっておけばよいか？どのように勉強したのか？ 【回答】 学生のうちは、特にコンピュータ工学の基礎をしっかり勉強しておいたほうが良い。加えて、C 言語、アセンブラの知識も必要である。 最初は市販されている日本語書籍から学習を開始して問題ないが、公式マニュアルや詳しいドキュメントは英語で書かれていることが多いため、英語を読めるようになるとワンランク上の学習が可能となる。

	「プレイ時間がものをいう」という言葉どおり、自分よりもできる人が何をやっているか観察したとき、多くの場合、自分よりも多くの時間を使って学習している。少しくらい躓いても、諦めずに頑張ってほしい。
主催者所感	【八巻 正行（北海道情報セキュリティ勉強会 代表）より】 北海道情報セキュリティ勉強会協力のもと、情報セキュリティ業界の第一線で活躍する講師陣を招いてハンズオンを行った。マルウェア解析および今回題材としたリバースエンジニアツール「Ghidra」は難易度が高く、万人が使いこなせる類のものではないが、その反面、学習意欲が高い少数精鋭の受講者が集まった印象を受けた。 運営面では、PC の環境起因でうまく動作しない受講者に対し、講師と TA が Slack を通じてリアルタイムでサポートを行った。受講者の作業状況に合わせてハンズオンの進行を調整する等、全体を通して柔軟な対応ができた。 セミナーとハンズオンによるマルウェア解析の知識習得に加え、受講者にとって将来の目標である「情報セキュリティのプロ」の姿を見せ、直接言葉を届けることができた点は、大きな意味のある機会であったと思う。今回刺激を受けた受講者の中から、将来、情報セキュリティ界を牽引していく人材が一人でも輩出されることを願う。
当日の様子	 

⑤サイバーセキュリティ オンライン・カンファレンス in NoMaps

開催名称	サイバーセキュリティ オンライン・カンファレンス in NoMaps 「Digital World beyond Pandemics」
開催日時	2020 年 10 月 17 日（土） 14:00 - 15:50
場所	オンライン
主催・共催	主催：北海道地域情報セキュリティ連絡会（HAISL） 共催：北海道経済産業局、株式会社道銀地域総合研究所、 一般社団法人 LOCAL、NoMaps 実行委員会
後援・協力等	-
講師（登壇者）	入澤 拓也（エコモット株式会社 代表取締役） 南 弘征（北海道大学 情報基盤センター サイバーセキュリティ研究部門 教授） 坂野 雅樹（北海道警察 サイバーセキュリティ対策本部 班長） 西原 翔太（一般社団法人 LOCAL 理事, サイボウズ株式会社 コネクト支援チーム） 岡田 良太郎（株式会社アスタリスク・リサーチ 代表） 門林 雄基（奈良先端科学技術大学院大学 教授） 髙井 昌彰（北海道地域情報セキュリティ連絡会 会長）
告知 URL	https://no-maps.jp/program/conference/digital_world https://local.connpass.com/event/191547/
参加人数	86 名（YouTube Live による視聴）
イベント概要	NoMaps と連携して「Digital World beyond Pandemics」と題した、サイバーセキュリティに関するオンライン・カンファレンスを開催する。本カンファレンスでは、コロナ禍に何があったのか振り返るとともに、急速に進展するデジタル社会の中でサイバーセキュリティの将来像を考察する。
プログラム内容	開会ご挨拶 第 1 部　コロナ禍をふりかえる ～Pandemic そのときに社会は？～ コロナ禍における産・学・官・民の取り組みについて、それぞれの立場から解説する ・入澤 拓也（エコモット株式会社 代表取締役） ・南 弘征（北海道大学 情報基盤センターサイバーセキュリティ研究部門 教授） ・坂野 雅樹（北海道警察 サイバーセキュリティ対策本部 班長） ・西原 翔太（一般社団法人 LOCAL 理事/サイボウズ株式会社 コネクト支援チーム） 第 2 部 「もうひとつの DX」で見通す、コロナ後のフューチャービジョン

	第 1 部の内容を踏まえたうえで、今後の未来像を考察する （パネルディスカッション形式） ・part1. 岡田 良太郎（株式会社アスタリスク・リサーチ 代表） ・part2. 門林 雄基（奈良先端科学技術大学院大学 教授） 総括 ・髙井 昌彰（北海道大学 情報基盤センター 教授/ 北海道地域情報セキュリティ連絡会 会長）
主催者所感	【三谷 公美（一般社団法人 LOCAL 理事）より】 NoMaps のテーマが "beyond" であったことから、このイベントのテーマを "Digital World beyond Pandemics" ～コロナ禍を乗り越えたわたしたちが見るものとは～ とし、サイバーセキュリティの視点から経験してきた 7 ヶ月を振り返るとともに、これからの未来像を考察して、デジタル社会に興味ある方、一般の方に、わかりやすく伝えることを目的としました。 前半は振り返りの時間とし、4 人の有識者によるビデオ登壇(録画)を紹介し、コロナ禍の中で IT 企業(エコモット 入澤社長)、教育機関(北大 南教授)、警察(道警 坂野氏)、コミュニティ(一社 LOCAL 西原理事)、各々が社会からどのような影響を受け、どのように対応していったのかを共有しました。 後半は、コロナ後の世界を見通すため、HAISL 会長の高井教授をホストに、OWASP Japan 代表 岡田氏、NAIST 門林教授を迎え、オンラインでの鼎談の様子を紹介しました。 当日、配信スタジオである札幌市民交流プラザには、出演する高井会長、タイムキーパーに三谷副会長が入り、タイムキーパーは、前半・後半の登壇者他、当日の関係者と Slack で連絡とりながら、配信の様子を確認しながら NoMaps 運営チームと連携して、オンライン配信（StreamYard + YouTube)を行いました。 【西原 翔太（一般社団法人 LOCAL 理事）より】 オンラインイベントの運営をするにあたり、イベントのプロでなくともできることにどんなことがあるかをスライドにまとめ、録画で発表をした。オンラインという言葉に引っ張られて、技術で課題の解決を試みる場面によく遭遇する。しかし実は、基本に立ち返って打ち合わせや資料の読み込みなど、事前にやるべきことをやるだけでも、多くの失敗を防ぐことができる。SC4Y はこういった運営以外にも、講師や TA の皆さんのご尽力もあって成り立っている。安心してコンテンツを展開していただくためにも、我々の運営が安定する必要があり、引き続きよりよい配信、運営を目指して知見を蓄えていきたい。

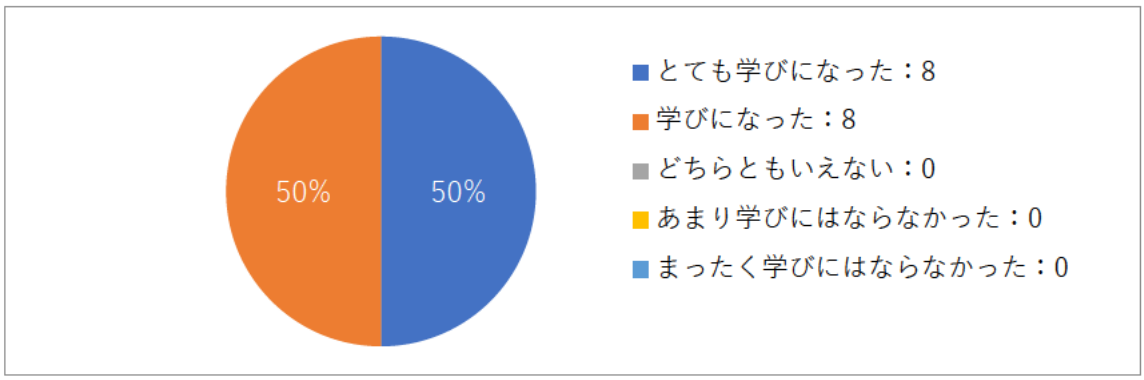
当日の様子	 NoMaps 10/17 サイバーセキュリティ オンライン・カンファレンス in NoMaps Digital World beyond Pandemics ゲスト 高井 昌彰 入澤 拓也 南 弘征 坂野 雅樹 西原 翔太 岡田 良太郎 門林 雄基  コロナ情勢下における サイバー犯罪発生状況 北海道警察サイバーセキュリティ対策本部 Cyber Security Control Task Force  サイバーセキュリティ オンライン・カンファレンス in NoMaps Digital World beyond Pandemics

当日の様子	 参考：当日のグラフィックレコーディング（@flytetyme2 氏） https://twitter.com/flytetyme2/status/1317357492498702336 

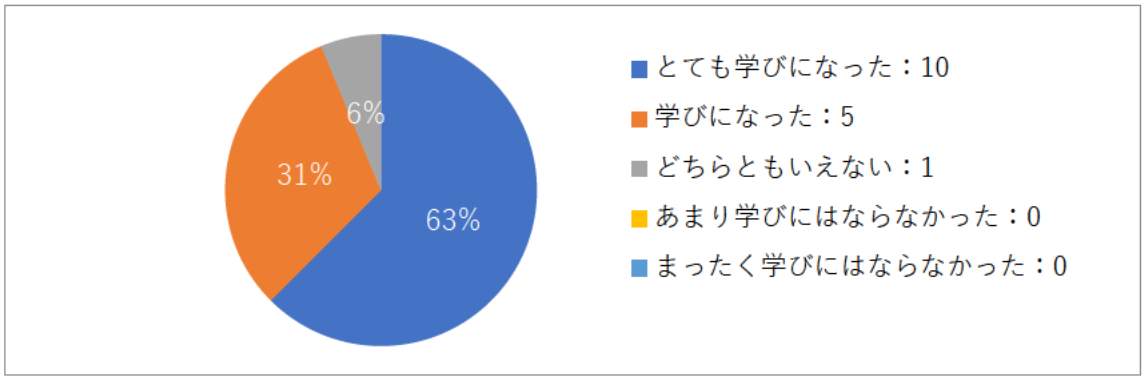
(4)受講者アンケートの結果

①第 1 回 SC4Y アンケート結果
回答数：16（Zoom による受講者のみ回答）

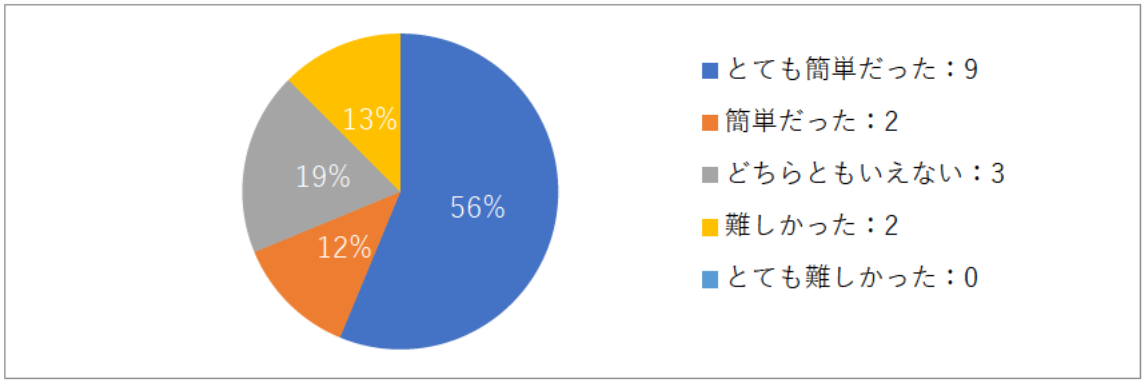
Q1. 「サイバーセキュリティと倫理」は自身の学びにつながりましたでしょうか？



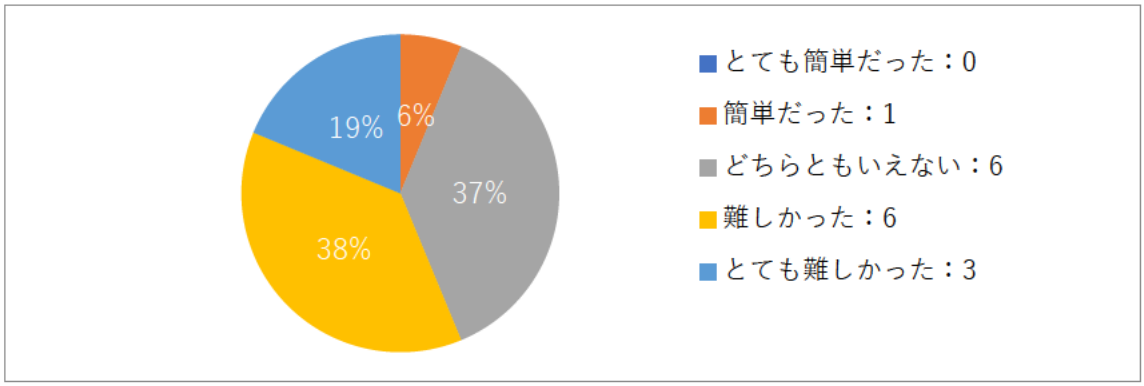
Q2. 「サイバーセキュリティ 脆弱性対応（防災訓練）」は自身の学びにつながりましたでしょうか？



Q3. 事前作業（VirtualBox 構築）の難易度はどうでしたでしょうか？



Q4.「サイバーセキュリティ 脆弱性対応（防災訓練）」の難易度はどうでしたでしょうか？



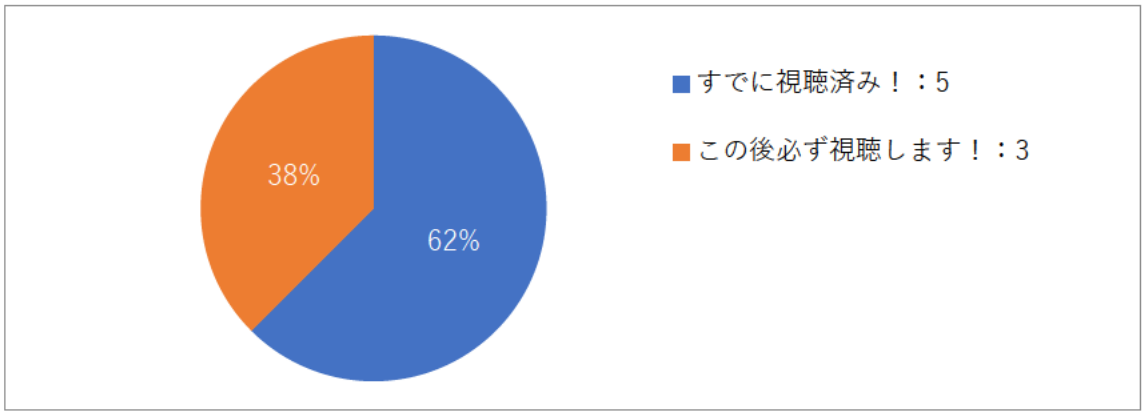
Q5. 今後、情報セキュリティの分野で学びたいことがありましたら、そのキーワードの記述をお願いします。

No	回答
1	ペネトレーションテスト
2	プログラマーとして成長に必要なもの
3	AI をどのようにセキュリティ分野で活かすのか
4	パケット解析
5	フォレンジック近辺
6	DDos
7	他の攻撃や対策を細かく勉強したい
8	code red
9	ASLR や NX ビットなどのメモリ保護機能とその回避方法について
10	コンテナセキュリティ、インシデントレスポンス、ゼロトラスト
11	ネットワーク、サーバー
12	ネットワークセキュリティ
13	XSS
14	難読化、バイナリ解析など
15	VPN
16	Web

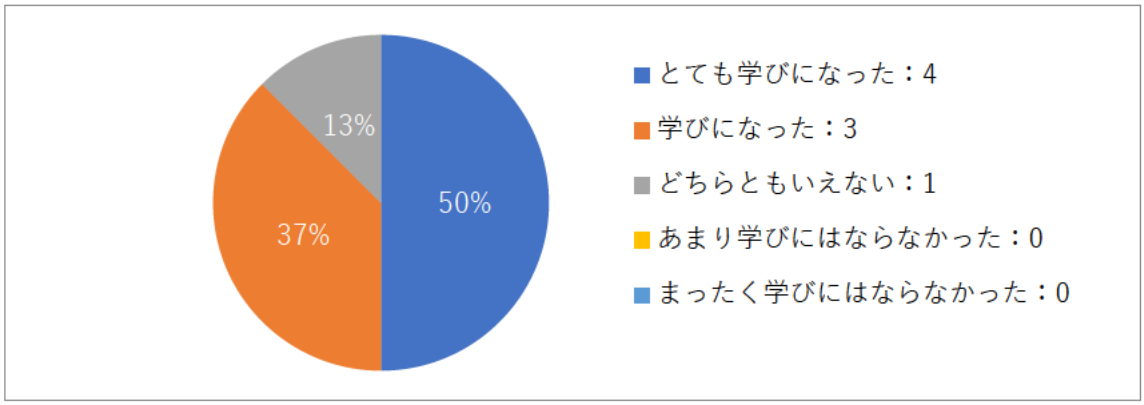
②第 2 回 SC4Y アンケート結果

回答数：8（Zoom による受講者のみ回答）

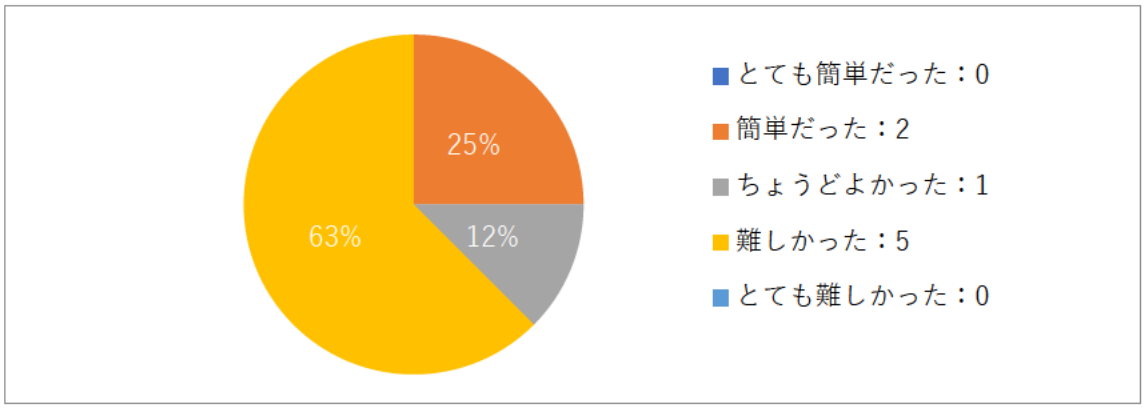
Q1. 「サイバーセキュリティの情報倫理」について、必ずご確認をお願いします。



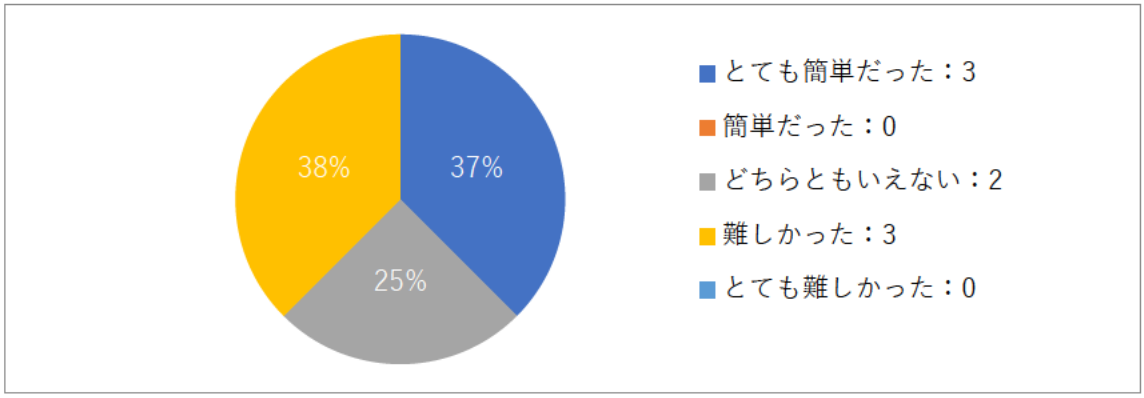
Q2. 「Web システムにまつわる脆弱性の検査手法」は皆さんの学びにつながりましたでしょうか？



Q3. 「Web システムにまつわる脆弱性の検査手法」の難易度はどうでしたでしょうか？



Q4. VirtualBox の構築および操作の難易度はどうでしたでしょうか？



Q5. 今回の演習を受けて，自分で Web システムを組む際にどんなことに注意して製作を進めようという意識が働きましたか？

No	回答
1	悪用しない。
2	自分の作った web サイトなどの脆弱性などの確認などを、怠らないようにしたいと思います。
3	実際に自分のサーバーを攻撃してみることで自分の作ったシステムが安全かどうか確かめようと思います。
4	想定されている動きが出来ているかどうかだけではなく、想定外の動きをする可能性を考えること。
5	今回学んだ、脆弱性に関する事を活かし、SQL・Web アプリを制作するときは防げるようにしたいと考えています。
6	脆弱性を埋め込まないことを意識するほかにもペネトレーションテストも行うことで確認したい。
7	自分でシステムを作る場合、Web に公開する前に必ず脆弱性テストをしたいと思いました。
8	インジェクションが成立しないように気をつけようと思いました。

Q6. 今後、情報セキュリティの分野で学びたいことがありましたら、そのキーワードの記述をお願いします。

No	回答
1	特になし
2	ブルートフォース攻撃などの攻撃関係
3	パスワードの脆弱性について
4	暗号通信
5	(分野とは言えないですが)CTF をやる機会があると良いなと思いました。
6	CSIRT やインシデント対応あたりを学んでみたいです。
7	ネットワークの解析
8	ありません

Q7. 今日参加されての感想があれば、一言お願いします。

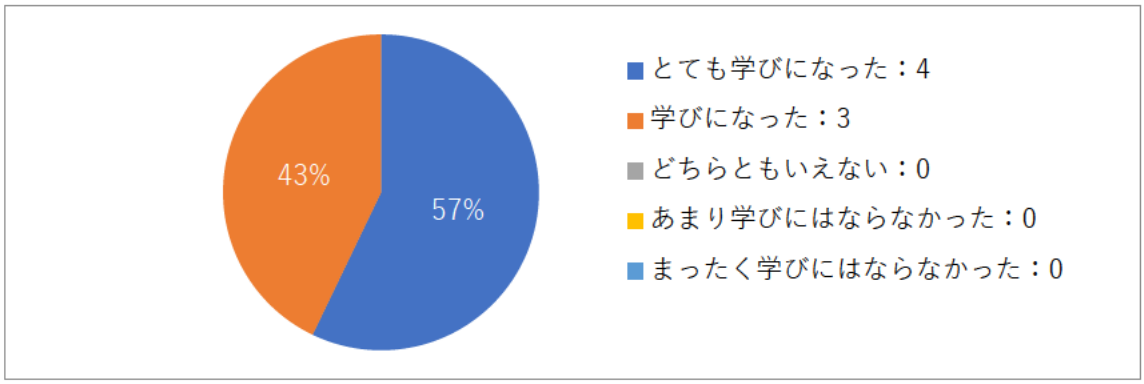
No	回答
1	-
2	今日はとても有意義な授業でした。ありがとうございました。
3	初期知識があまりない状態での参加だったのでところどころ内容理解が及ばないところもありましたが、pdf を見直すなどして勉強したいと思います。
4	実際に手を動かすことで話を聞いているだけよりも、よい学習になったと思う。
5	前半は大学やそれ以前に学んだ事を使いつつの話だったため、それほど難しく感じませんでしたが、後半になるにつれてちょっと追いつくのに時間がかかったりしていました……ですが、とても勉強になりました。ありがとうございました。
6	今まで知らなかったことを知ることができました。次回も参加したいです。
7	スライドがとても分かりやすく、復習もできるので、大変ありがたいです。ありがとうございました。
8	体調不良のため大半は見ることが出来なかったのですがアーカイブが限定公開されるとの事なので後で視聴しなおそうと思います。この度はありがとうございました。

※第 3 回 SC4Y については、発表と交流を主目的としたことを踏まえ、今後の IT 勉強会イベントへ積極参加を促すため、参加者の作業負担・心理的負担の軽減を考慮して、アンケートは実施しなかった。

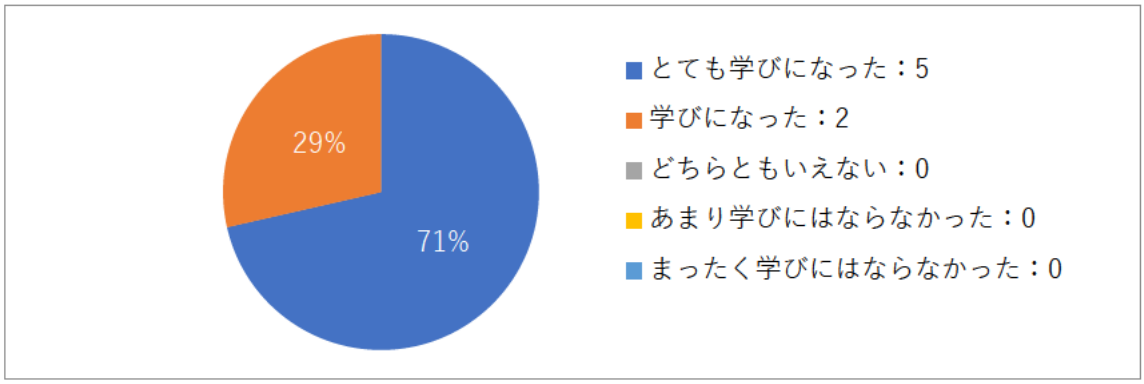
③第 4 回 SC4Y アンケート結果

回答数：7（Zoom による受講者のみ回答）

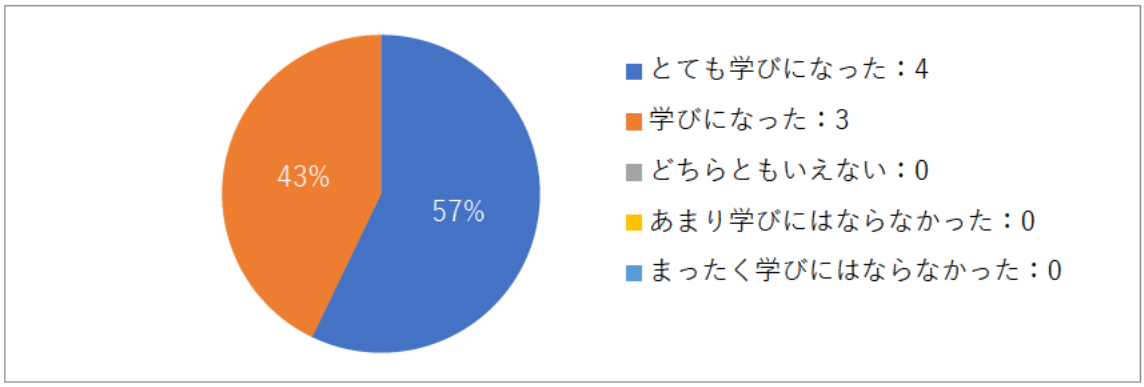
Q1. 「Basic of Malware Analysis」は皆さんの学びにつながりましたでしょうか？



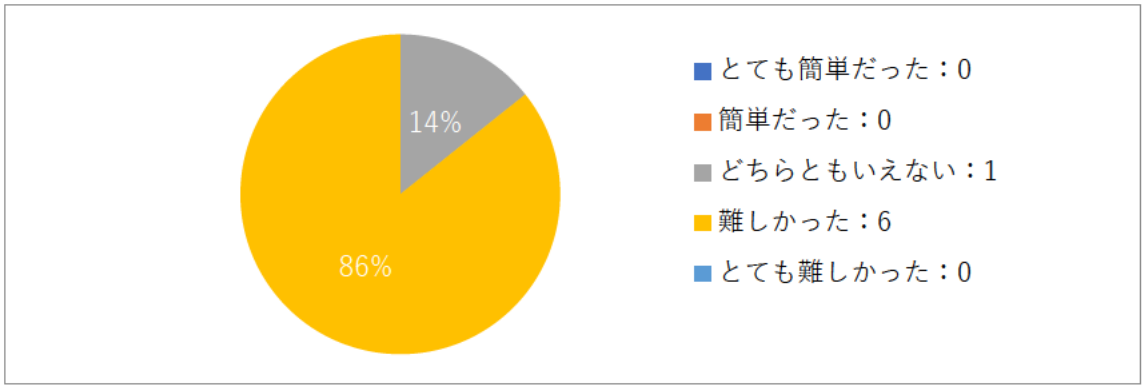
Q2. 「Static Analysis with Ghidra」は皆さんの学びにつながりましたでしょうか？



Q3. 「Write Yara Rule with Ghidra」は皆さんの学びにつながりましたでしょうか？



Q4. 全体を通して難易度はどうでしたでしょうか？



Q5. 今回の演習を受けて、今後どんなことを行ってみたいと思いますか？

No	回答
1	CTF の rev の問題にチャレンジしていこうと思います。
2	-
3	Ghidra の使い方を復習してもっと使えるようにしたい。
4	さらに詳しいマルウェア解析をしてみたい。
5	-
6	ハンズオンの資料を見直しながら、手を動かして理解を深めたい。
7	CTF のリバースエンジニアリングの問題を、Ghidra を使って解いてみようと思いました。

Q6. 今後、情報セキュリティの分野で学びたいことがありましたら、そのキーワードの記述をお願いします。

No	回答
1	スタックオーバーフローや GOT 書き換えなどのプログラムの脆弱性を突きたい。
2	-
3	脆弱性診断
4	パケット解析
5	-
6	マルウェア解析についての知識を深めたい。
7	脆弱性診断、ネットワーク解析（Wireshark）

Q7. 今日参加されての感想があれば、一言お願いします。

No	回答
1	yara ルールの定義は難しかったけど、windowsAPI の調べ方や Ghidra の使い方を教えてもらって rev の苦手意識が少しなくなった。
2	-
3	Ghidra のような解析ツールの使い方は独学しようとしても最初で躓き先に進まないため、今回のようなセミナーはとても参考になりました。
4	難しかったですが学びになりました。
5	-
6	こうしたツールに実際に触れられるのは新鮮で、独学では敷居が高く感じがちな部分なので、とても勉強になりました。今回の講義をもとに、低レイヤ周りの知識を深めていきたいと感じました。
7	とても難しかったですが、今後も Ghidra の勉強を続けていこうと思います。

(5)総括

第 1 回 SC4Y のアンケートでは、「サイバーセキュリティと倫理」「サイバーセキュリティ 脆弱性対応（防災訓練)」ともに、「とても学びになった」「学びになった」と回答した受講者が 90%を超えており、難易度については「難しかった」「とても難しかった」と回答した受講者が 47%であった。受講後の振り返りで参加者から得られた感想からも、難易度は高めであったものの満足度は高く、受講者にとって有益な学びを提供することができたと言える。特に防災訓練の講義内容は、普段学校で習うことがない実務に即した内容であり、受講者にとって新鮮な内容であった。

第 2 回 SC4Y のアンケートでは、「とても学びになった」「学びになった」と回答した受講者が第 1 回と同程度の 87%であった。難易度については「難しかった」が 63%である一方、「簡単だった」「ちょうどよかった」と回答した受講者が 38%存在した。第 2 回のテーマである Web システムの脆弱性については、情報系の授業で学習済みの受講者が一定数存在しており、理解度の割合が分散した理由の一つとして考えられる。ただし、今回は授業で行うような机上学習ではなく、実際にハンズオン形式で手を動かし、その動作を確認しており、各種脆弱性による事象をよりリアルなものとして実感することができている。受講後のコメントでは今後 Web システムを構築するにあたって、必ず脆弱性対策を考慮したいと回答している受講者が大半を占めていることから、これまで開発時にあまり意識していなかった Web の脆弱性について、身近なリスクとして捉えられるようになったことが伺える。

第 3 回 SC4Y はこれまでと趣向を変え、ライトニングトーク大会兼交流会という形式をとっている。講師から一方的に知識を教わるだけでなく、自ら学んだことを発信し、周囲からフィードバックを得ることで、更なる研鑽へと繋げていくことが目的である。発表は終始楽しく好奇心旺盛な雰囲気で進行し、交流会では普段口数の少ない参加者からも積極的に言葉や考え方を引き出すことができた。これらの経験は参加者にとって、今後の学びを継続するうえで少なからず自信になったはずである。

また、学校という枠組み、情報セキュリティというテーマを超え、様々な分野で活躍する IT 技術者、IT 勉強会コミュニティと交流し、繋がりを持つことができた点において、参加者は新たな刺激を得て知見と視野が広がること、学びへの行動がよりアクティブな方向へ変化することが期待できる。

第 4 回 SC4Y のアンケートでは、「とても学びになった」「学びになった」と回答した受講者が 100%であった一方、講義の内容は「難しかった」と回答した受講者が 86%となった。難易度は非常に高かったものの、受講者は充実した学びを得ることができたことを示している。今後どんなことをやってみたいかという回答でも、講義でわからなかった点の復習や更なる応用に挑戦したいという言葉が大半を占めており、受講者の学習意欲が高まったことが伺える。従来、マルウェアの解析は非常に難易度が高く初見で諦

めてしまう初学者も多かったが、Ghidra という強力なツールの利用方法を習得したことに加え、情報セキュリティの第一線で活躍するプロの振る舞いを目の当たりにし、その学習方法や心構えを知ったことで、更なる目標意識の高まりと学習の継続が期待できると感じた。

特別講義として開催した「サイバーセキュリティ オンライン・カンファレンス in NoMaps」では、視聴者数が 86 名に達し、札幌市内で開催する大規模な情報セキュリティ関連イベントと遜色ない集客数を獲得することができた。一方向の配信であったため視聴者から直接フィードバックを得ることは叶わなかったが、各界での実績十分で注目度の高い登壇者陣による意見交換は、情報セキュリティのプロから一般人まで、幅広く響く内容であった。

また、今回初めて NoMaps との連携イベント開催の実績をつくることができた点は、今後、情報セキュリティ啓発に関連する事業を展開するにあたって、更なる普及チャネルの拡大と選択肢の幅を広げる布石となった。

全体をとおして､SC4Y 全 4 回と特別講義を加えた 5 回のカリキュラム実施において、それぞれの開催テーマに沿った学習成果と、受講者の高い満足度が伺えた。

一方で、SC4Y の受講者数は回によって 2 倍近くの差があり、集客の面では課題を残している。これは、コロナ禍によって各学校での学習日程が圧迫された結果、レポートやテスト日程等と重複し、土日であっても時間が取れない学生が多く存在した点も一因にある。また、年齢制限を排除した YouTube Live による視聴では、Zoom による受講者の 2.5～7 倍近くの申し込みがあった。現状、北海道地域の情報セキュリティ啓発状況、学習状況をみると、積極的に活動、学習を行っている地域には必ずキーマンとなる人材（教員、生徒、IT 技術者、民間コミュニティ）が存在している。若手に対して情報セキュリティ学習の裾野を広げることは重要であるが、同時に年齢にとらわれず将来キーマン、リーダーとなりえる突出した人材を 1 人でも多く輩出するため、年齢や立場にとらわれないカリキュラム構成についても引き続き検討していくことが求められる。

また、SC4Y のアンケートでは、受講者より今後情報セキュリティの分野で学びたいキーワードを収集している。その結果は多岐にわたり大きな偏りは見受けられないが、ネットワークパケット解析や CTF の実施など、本年度実施できなかった内容も多く含まれている。これらの貴重な意見は次年度以降のカリキュラムに活かしつつ、今年度の実施結果を踏まえ更なる改善を加えて、今後の活動につなげていくことが必要である。

Ⅵ 実践型競技会の域内展開に向けた広報等

サイバーセキュリティ分野の実践型競技会について周知を行うことで道内の参加者拡大や競技会等への協賛・協力企業の発掘に努めることを目的に、アンケート調査の回答企業など下記の 4 社を訪問し、実践型競技会の広報を行うとともに、サイバーセキュリティの現状や課題について意見交換を行った。

企業名	所在地	業種	従業員数
A 社	札幌市	卸売業	150 名
B 社	札幌市	建設業	45 名
C 社	札幌市	食料品製造業	70 名
D 社	札幌市	電気・ガス・熱供給・水道業	800 名

（主な意見）

【A 社】

- 2018 年にオフコンからクラウドに切り替えた。それとともに、全従業員がメールを利用できる環境になったが、対策が十分にできるとはいえない。何も考えずに添付ファイルを開いてしまう人もいる。
- 大塚商会のメールシステムを使っているため、何かがが起きたときにはそのシステムからアラートがシステム管理者に届く仕組みがあり、今のところ業務に支障が生じたことはないが、BCP の中にシステム障害対策を入れるべく、準備を進めている。
- 社内にはセキュリティに詳しい人はいないが、IPA のビデオを全従業員に見せたことがあり、その後は意識が高まって安直に添付ファイルを開封することなどは激減した。

【B 社】

- セキュリティ対策は必要だと思っているが、なかなか手がまわらない。セキュリティに通じた人材を採用しようと考えたこともあるが、当社の規模ではそれだけやっていればいいということにはならない。現場や営業の仕事もしてもらうとなると、なかなか適当な人は見つからない。また、内部で人材を育てようと考えたこともあるが、専業でないと、本人もあまり力が入らない。そうした試行錯誤の結果、総務担当者が自主的に勉強して担当しているのが現状。
- 協力会社の職人さんが施工事例を勝手に SNS に紹介し、依頼主からクレームが入ったことがある。そのときは当社から社長が訪問して謝罪した。SNS に写真を載せた職人さんには悪意はなく、むしろ、宣伝になると思ったという善意でやったことだった。自社の従業員でなく、また、システム的な問題でもないだけに、こうしたことはコントロールしていくのがとても難しい。
- セキュリティ対策といっても、何をすればよいのかわからないというのが正直なところ。随時、情報提供をいただけると、大変ありがたい。

【C 社】

- 直近でコンピュータウイルス（Emotet）の被害を受けたばかり。
- 送信者名が取引先の担当者であるメールに Excel ファイルが添付されており、受信者がそれを開いて感染した。後で見たら、送信者の名前は取引先の担当者であったものの、メールアドレスの@以下が違っていた。
- 感染が発覚したのは、別の取引先からの連絡。その時点で数時間が経過しており、まず、社内のネットワークの社外との接続をすべて切った。
- その後、まず、プロバイダーやシステム構築会社に連絡したが、いずれも「東京から担当者を派遣するので日数がかかる」との回答であり、それを待っていると当社の業務が止まったままになってしまうため、社内で担当者 3 名を決めて、インターネットに接続されているすべての機器を一つ一つ調べて、感染していると思われるファイルの削除を行った。担当者 3 名は連日深夜まで勤務、休日出勤も続け、1 ヶ月経ってようやく元の姿に戻った。
- 総務部にたまたま IT ベンダーからの転職者がおり、その人にすべてを任せてやってもらえたので、このような対応が可能になった。感染に気づくのがもう少し遅れていただけでも、多くの取引先などに感染を広げ、大変な被害になっていたと思う。

【D 社】

- ウイルスメールは来ているが被害は出ていないという状況。各従業員のメールボックスまではどうしても来てしまうが、それを押した事例は出ていない。
- DDos 攻撃を受けたこともある。被害は出なかったが、一時的にアクセスが重くなった。
- CSIRT を準備している。その一環として、CSIRT 側の監視の一つで、振る舞い検知を導入した。内部で何か起きても外へ出る前に止めることができる。
- 人の教育はいくらやっても足りない。スキルも足りない。外部のコンサルを入れて分析をしたうえで、標的型攻撃メール訓練をやっている。今までは不定期だったが、今年度はオリンピックの予定があったので去年から厚くやっている。訓練は抜き打ち、グループ会社を含めた全社員が対象。テストで訓練メールを踏んだ人は多かった。周知は頻繁にしているつもりだったが、引っかかる人は引っかかる。
- 定期的なトレーニングの機会があるといい。セミナー＋訓練のセットのようなものが頻繁にあれば、事務系以外の職場の従業員も参加できる。今はシステム部門の従業員しか行けていない。そういった人材教育の場がたくさんあるといい。
- より多くの事例、情報をいただけるとありがたい。IPA からもいろいろ来るが全部は目を通せないので、セミナーのような場で、オンラインでもいいので、提供してもらえるとよい。機会が多ければいろいろな部署の人が参加できる。

Ⅶ　道内における持続的なセキュリティコミュニティのあり方に関する検討

サイバーセキュリティ対策の持続的かつ自立的地域展開に向け、他地域の事例調査を行ったうえで、HAISL の民営化に向けた道筋や次年度以降の取組の可能性を検討、整理した。

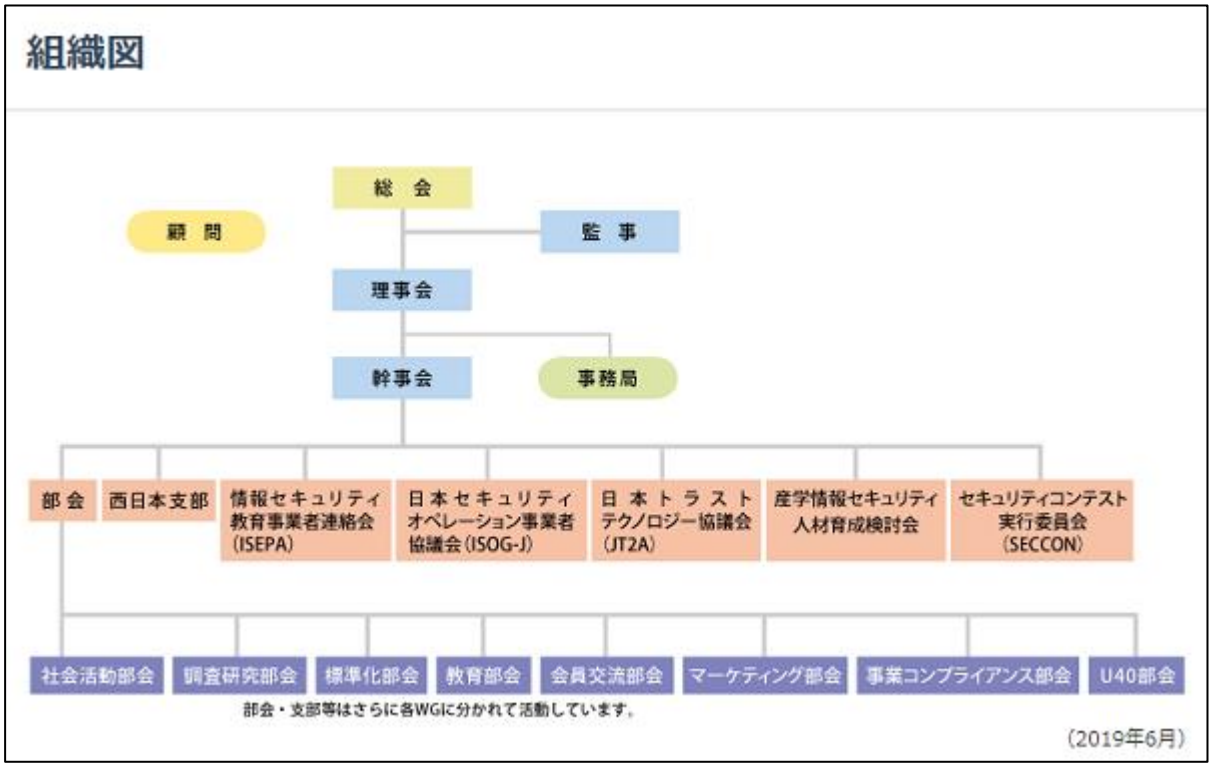
1. 先進事例調査

全国の先進事例を対象に、地域のセキュリティコミュニティやセキュリティ人材育成事業を実施する団体について、ヒアリング（オンライン）による調査を実施した。

(1)特定非営利活動法人日本ネットワークセキュリティ協会

【概要】

名　　称	特定非営利活動法人日本ネットワークセキュリティ協会
設　　立	2001 年
所 在 地	東京都港区西新橋 1－22－12　JC ビル 4F
代 表 者	会長　田中英彦(情報セキュリティ大学院大学　名誉教授)



（ヒアリング結果）

- 中小企業のサイバーセキュリティの意識を高めることは長年の課題。さまざまな取組をしてきたが、解決には至っていない。
- 専門家のいない企業からの相談では、発生した問題がセキュリティに関するものなのか、それとも一般的な IT に関することなのか、理解できていないことも少なくない。
- しかし、社員数が 100 人以下の企業では、サイバーセキュリティのための人材を置くことは負担感が大きい。参考として、当協会ではないが、一般の利用者に向けてセキュリティ対策をサポートするためにサポータ認定を行って、一般の利用者をサポートすることを推進している「一般社団法人セキュリティ対策推進協議会」（SPREAD）がある。この団体は一般利用者が対象となっているが、この仕組みは零細企業向けの活動として参考になるのではないか。

（2）一般社団法人京都スマートシティ推進協議会

【概要】

名　　称	一般社団法人京都スマートシティ推進協議会
設　　立	2018 年
所 在 地	京都府京都市下京区中堂寺南町134 京都産業支援センター 2階
代 表 者	代表理事　重松千昭（元京都府商工労働観光部　理事）

（ヒアリング結果）

- 京都府と京都府内企業等が、京都の基幹産業である観光分野を軸にデータ利活用を促進するために設立した。組織会員は民間企業、大学・教育機関、行政等で構成されている。運営経費には、会費や、所有するデジタルサイネージの広告収入等を充当。
- 情報収集などのために、他地域との連携を積極的に行っていきたい。北海道のセキュリティ団体などとの連携もお願いしたい。

(3)特定非営利活動法人情報セキュリティ研究所

【概要】

名　　称	特定非営利活動法人情報セキュリティ研究所
設　　立	2002 年
所 在 地	和歌山県田辺市新庄町 3353-9 Big･U 内 104 号室
代 表 者	代表理事　臼井 義美（臼井技術士事務所）

（ヒアリング結果）

- 1997 年にスタートした「サイバー犯罪に関する白浜シンポジウム」に携わるスタッフを中心として、シンポジウムを継続して運営する核となる組織を作る必要があると考え、NPO 法人「情報セキュリティ研究所」を設立した。
- ・代表理事の臼井氏は、ソフトウェア会社の出身。取引先である和歌山県警の仕事に携わるうち、警察が扱うコンピュータ関係の犯罪が増えているが、警察自身は、ハイテク犯罪の知識も経験もなく、全く対応できないという実態がわかった。そこで、従事していた警察のシステム完成記念として、全国の警察関係者に最新のハイテク犯罪の概要とその捜査技術を勉強する機会を提供しようと「コンピュータ犯罪に関するシンポジウム」の開催を提案した。

（4）サイバーセキュリティシンポジウム道後実行委員会

【概要】

名　　称	サイバーセキュリティシンポジウム道後実行委員会 （事務局　一般社団法人テレコムサービス協会四国支部事務局内）
所 在 地	愛媛県松山市大手町 1-11-4（一般社団法人テレコムサービス協会四国支部）
代 表 者	実行委員長　小林 真也（愛媛大学大学院　教授）

（サイバーセキュリティシンポジウム道後 2020　協賛及び出展の企業・団体）

（ヒアリング結果）

- スポンサー企業の協賛金とシンポジウム参加者の参加費で運営。
- シンポジウムは 10 年前に総合通信局からの働きかけで始まったが、現在、シンポジウム以外の部分では、総合通信局よりも愛媛県警との繋がりが深い。県警を中心に、地元向けのワークショップなどを、年間を通じて行っている。

（5）九州サイバーセキュリティシンポジウム実行委員会

【概要】

名　　称	九州サイバーセキュリティシンポジウム実行委員会
所 在 地	（連絡窓口）株式会社ラック　新規事業開発部 福岡県北九州市小倉北区浅野 3-8-1 AIM ビル 8F ラック テクノセンター北九州
設　　立	2018 年
代 表 者	尾家　祐二（国立大学法人九州工業大学）

（ヒアリング結果）

- 九州経済連合会、九州電力、株式会社ラックなどが中心となって実施。ただし、組織ありきではなく、企画に関わった個人が所属していた組織の名前が出ているのが実態。他のシンポジウム事務局やセキュリティ関連団体との意見交換、情報交換についても、組織として行っているというよりは、個人のネットワークで行われている。
- 運営経費は、スポンサーの協賛金と参加者からの参加費でまわしているが、人件費は実行委員が所属している企業が負担している。

（6）特定非営利活動法人新潟情報セキュリティ協会

【概要】

名　　称	特定非営利活動法人新潟情報セキュリティ協会
所 在 地	新潟県新潟市中央区弁天 3 丁目 3 番 5 号　新潟マンション 209 号室
設　　立	2002 年
代 表 者	代表理事　一戸　信哉

（ヒアリング結果）

- 法人設立前の 1998 年から「情報セキュリティワークショップ in 越後湯沢」を開催。当初はワークショップの実行委員会や運営委員会のスタッフを中心とした任意団体として立ち上がったが、ワークショップの参加者の増加を受け、法人化した。
- ワークショップの恒常的な開催・運営、及び、ネットワークやセキュリティ関連の啓蒙活動や技術の開発を行うことを目的として、情報やネットワークに関するコンサルティング事業や調査研究事業を行っている。

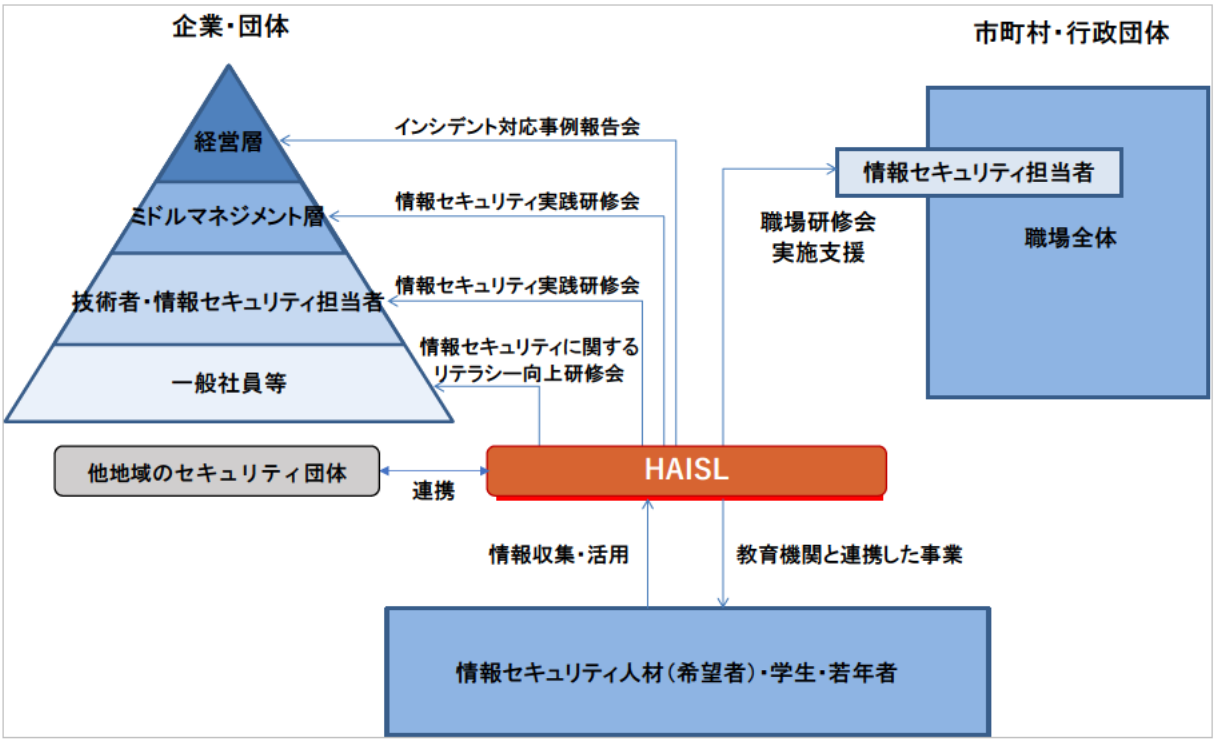
2. 道内における持続的なセキュリティコミュニティ形成に向けた展開イメージ

セキュリティ人材の育成のためには、教育・意識喚起の取組を継続的に実施していく必要があるが、そのためには、官民一体となったサイバーセキュリティの推進体制を構築し、これを核に実施していくことが重要である。ここでサイバーセキュリティに関するネットワークを広げ、関係機関で情報の共有や対応策の検討を進め、更なる意識喚起に繋げていくことも可能となる。

また、本事業でリストアップした専門家リストの活用等、発掘・育成されたセキュリティ人材が企業等と適切にマッチングされる仕組みづくりも有用と考えられる。

一方、行政機関や企業にとってはセキュリティ人材の確保・育成に大きなコストがかけられない現状であり、短期的には研修参加費への助成制度を拡充するなどしてセキュリティ人材の育成を促進し、中長期的には必要なコストを企業、個人が応分に負担する自立した運営となることが望ましい。

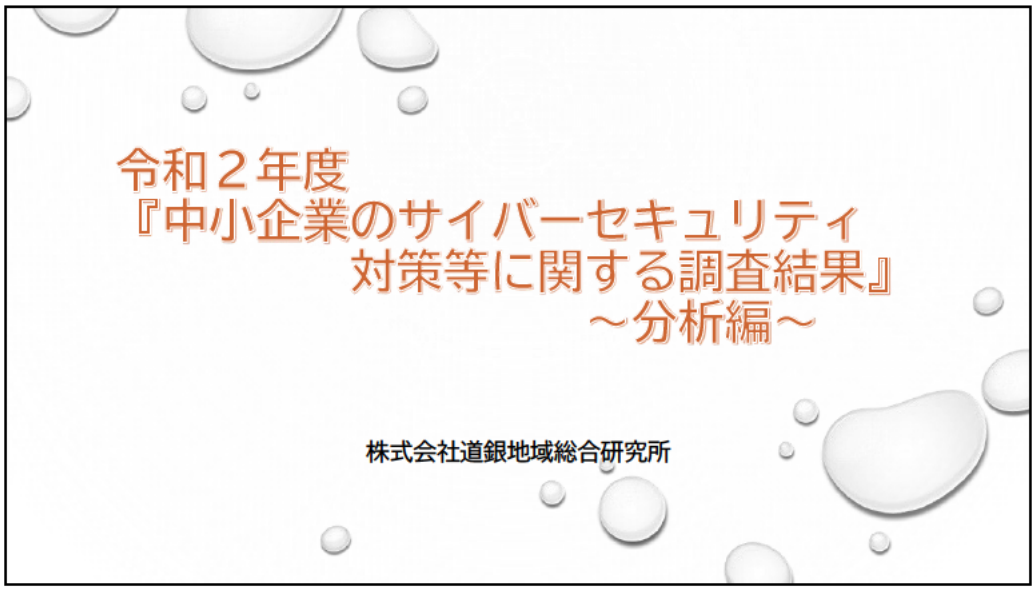
●道内における持続的なセキュリティコミュニティ形成に向けた展開イメージ



Ⅷ　HAISL の運営

1. HAISL 連絡会での報告

３月 4 日に開催された HAISL 連絡会（オンライン形式で開催）において、アンケート調査の集計結果と分析結果について報告を行った。説明に用いた資料は以下のとおり。



全 体

調査の概要

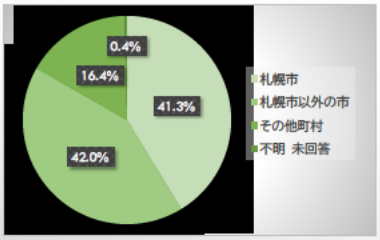
- 目的
  道内中小企業のサイバーセキュリティ対策への理解度を把握するとともに、今後、対策レベルに合わせた導入支援方法等を検討するための基礎資料として。
- 実施時期
  令和2年9月～10月
- 対象企業/回答数
  道内中小企業を対象に、TSRの企業リストから製造業・非製造業それぞれ売上上位500社/回答合計281社（返答率28.1%）
- 調査手法
  対象企業に郵送にて調査票を送付。
  同封用紙の郵送、もしくは、専用WEBサイトにて回答を得る。

3

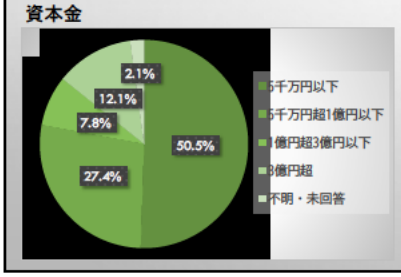
全 体

回答者属性

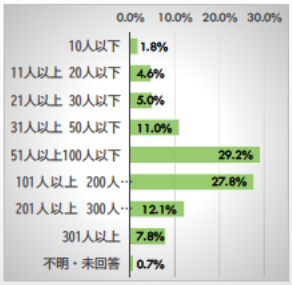
所在地



資本金



従業員数



業種

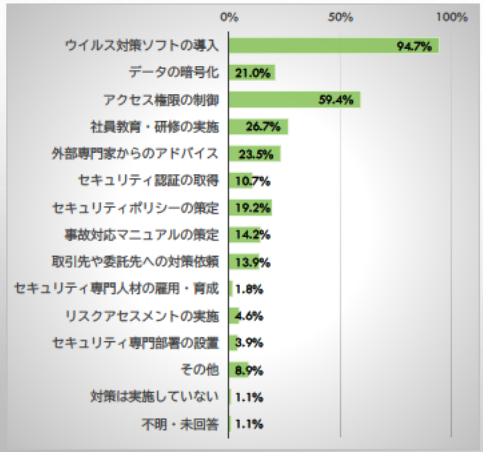
回答者の業種は、「製造業」が46.0%、「卸売業・小売業」が22.9%であった（不明を除く）。 N=281

4

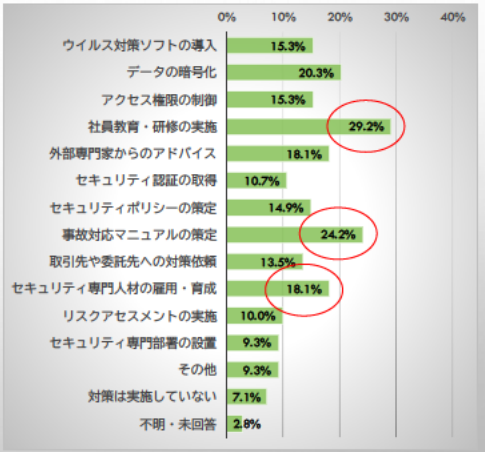
全 体

サイバーセキュリティへの対応状況について

現在実施しているサイバーセキュリティ対策



今後実施すべきサイバーセキュリティ対策



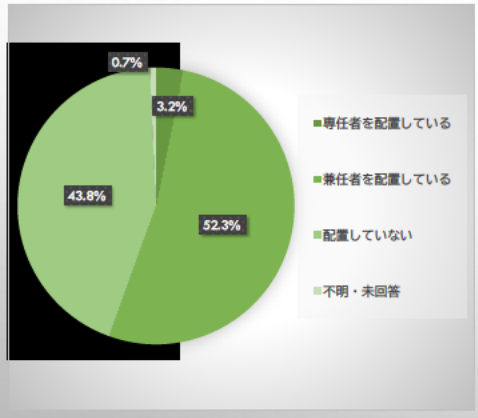
- 「ウイルス対策ソフトの導入」「アクセス権限の制御」を実施している回答者は多い
- 今後については、社内の対応力強化（人材・対応策・教育）を検討している企業が多い

複数回答
N=281

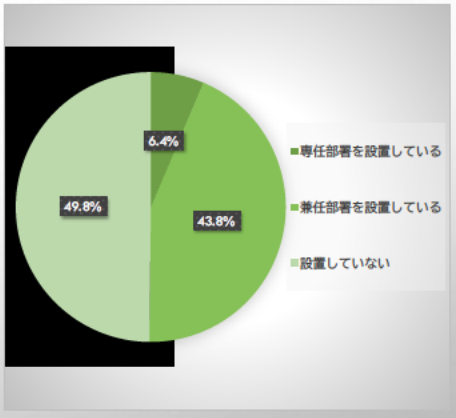
サイバーセキュリティへの対応状況について

全 体

サイバーセキュリティ対策担当の配置状況



サイバーセキュリティ担当部署の設置状況



- 回答者の約半数がサイバーセキュリティの担当者（専任・兼任）を置いている。
- サイバーセキュリティを担当する部署についても約半数が設置している。

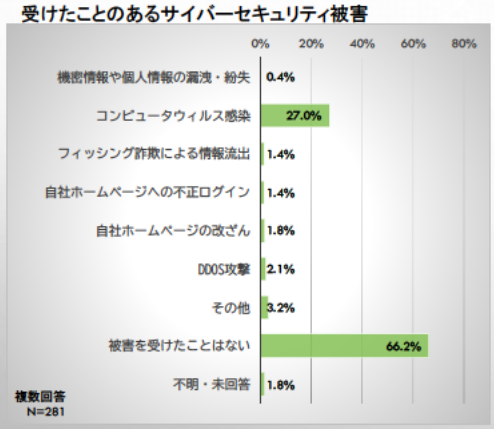
N=281

6

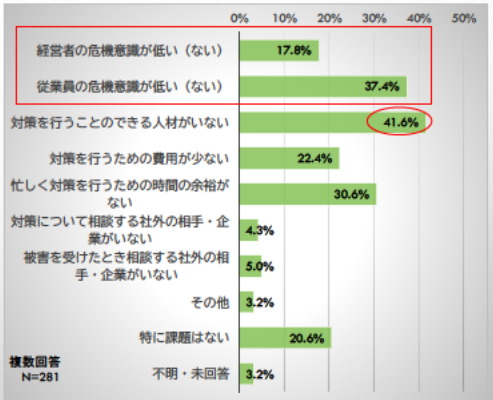
サイバーセキュリティ被害状況と関心の高い情報

全 体

受けたことのあるサイバーセキュリティ被害



サイバーセキュリティに関する課題



対象者の3割以上が被害を受けた経験がある。
最も多い被害は、「コンピューターウイルス感染」。
また、そのうち4%は『EMOTET』に関連。

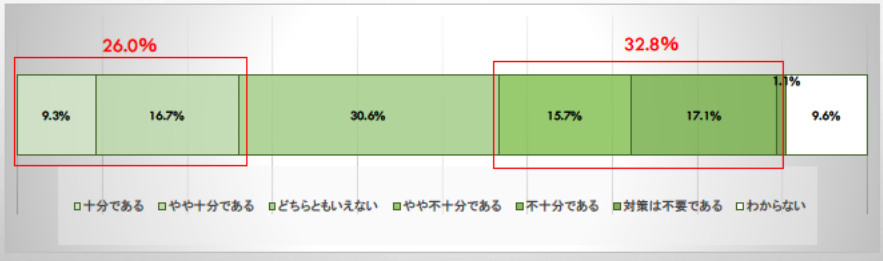
人材の不足と、サイバーセキュリティに関する危機意識が課題。

7

サイバーセキュリティへの対応状況について

全 体

現在のサイバーセキュリティ対策を十分と感じるか



- 対策については不十分と感じている回答者の方が多い。

N=281

8

北海道内のサイバーセキュリティに関する概況

全 体

【企業対応】

- 一般的な対応（ウイルス対策ソフトの導入）はされている
- 約半数で対応担当や部署を置いている
- 課題としては、「対策が行える人材不足」「経営層/従業員の危機意識の低さ」があげられる

【被害や対策】

- 道内企業でも全国と同様（※）に3割以上が被害経験あり
- 現状の対策では、不十分と感じている企業が多い
- 今後の対策として、社内体制や対応を課題としてあげている

※全国36.3%「法人組織におけるセキュリティ実態調査2019年版（トレンドマイクロ社）」より

被害経験の有無や、業種、担当の有無は、サイバーセキュリティ対策や意識に違いを生じさせているか？

9

目次

10

比較項目

被害経験の有無

・被害経験の有無

サイバーセキュリティ被害経験のある企業　95社
サーバーセキュリティ被害経験のない企業　186社

・業種による違い

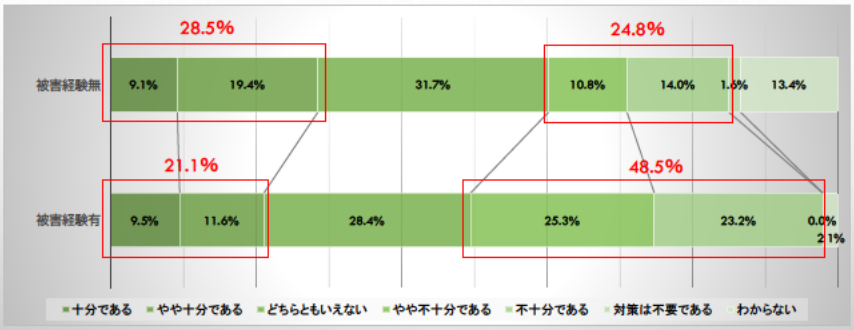
・担当者/担当部署の有無

11

サイバーセキュリティへの対応状況について

被害経験の有無

現在のサイバーセキュリティ対策を十分と感じるか



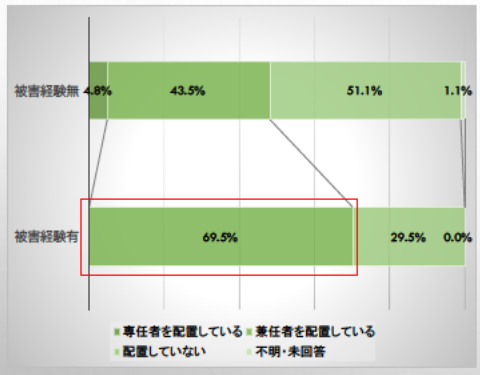
実際に被害を受けた経験のある企業は、現在のサイバーセキュリティ対策に危機感を感じている

12

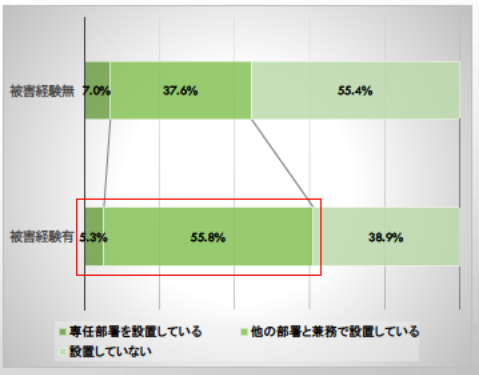
サイバーセキュリティへの対応状況について

被害経験の有無

担当者の配置状況



担当部署の設置状況



被害を受けた企業では、担当者や担当部署を設けているところが多い。

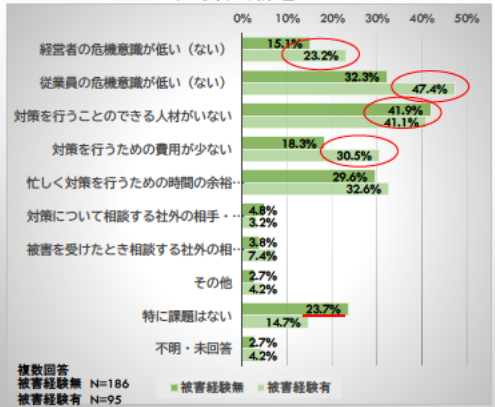
被害経験無 N=186
被害経験有 N=95

13

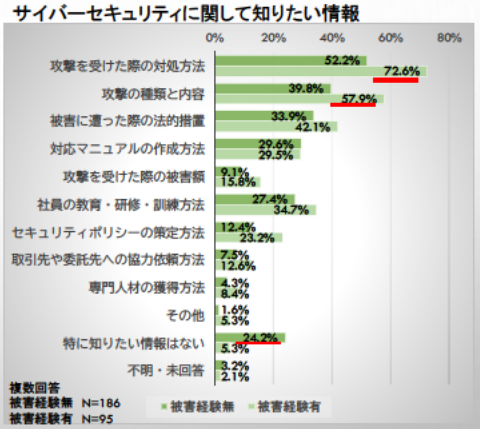
サイバーセキュリティに関する課題と知りたい情報

被害経験の有無

サイバーセキュリティに関する課題



サイバーセキュリティに関して知りたい情報



被害を受けた企業では、「社内の意識」や「対策費用」に課題がある。被害経験のない企業では「特に課題はない」という回答が多い。一方、「最適人材がいない」は共通の課題。

被害を受けた企業の方が、各項目で関心が高いが、特に「被害時の対処方法」や、「種類・内容」に関心が高い。被害経験のない企業では「知りたい情報がない」という回答が多い

14

被害経験による企業対応の違い

被害経験の有無

【被害経験のある企業】

- 被害経験のある企業は、対応者や対応部署を設けている率が2割ほど高い
- 担当部署/担当者がいることで、情報収集に関心が高い傾向が見受けられる
- 社内での意識の向上や有事の際の対策・対応について課題と感じている
- また、「人材の不足」が課題となっている

【被害経験の無い企業】

- 現時点で被害がないことから関心が薄い傾向がある
- 関心が薄く、課題意識が低い
- 被害経験に関係なく「人材の不足」は課題としている

15

比較項目

業種による違い

・被害経験の有無

・業種による違い
製造業　　129社
卸売・小売業　64社

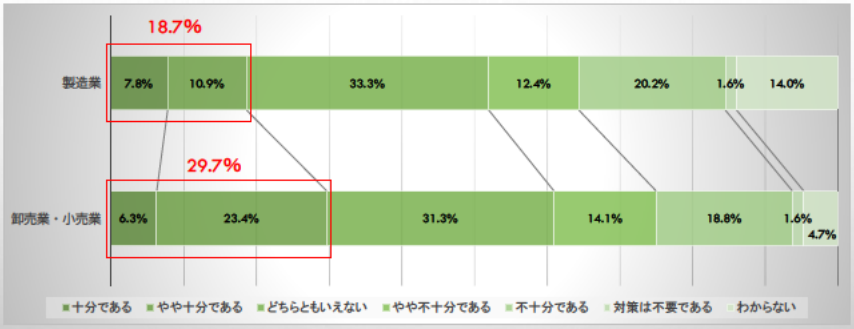
・担当者/担当部署の有無

16

サイバーセキュリティへの対応状況について

業種による違い

現在のサイバーセキュリティ対策を十分と感じるか

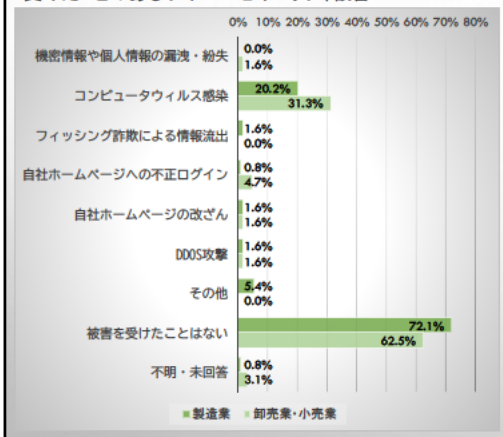


製造業の方が、現在の対策に満足していない。
ただし、業種の違いから求めるセキュリティレベルに違いがある可能性もありうる。

サイバーセキュリティ被害状況と関心の高い情報

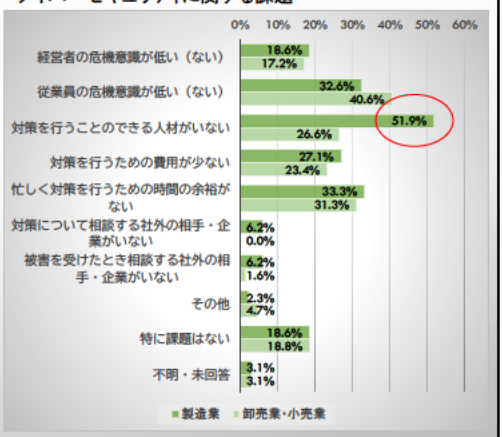
業種による違い

受けたことのあるサイバーセキュリティ被害



業種による差は大きく見られない。

サイバーセキュリティに関する課題



製造業では、人材不足が課題。

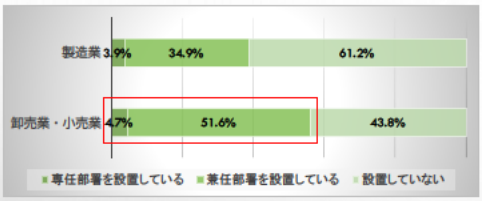
複数回答
製造業 N=129
卸売・小売業 N=64

18

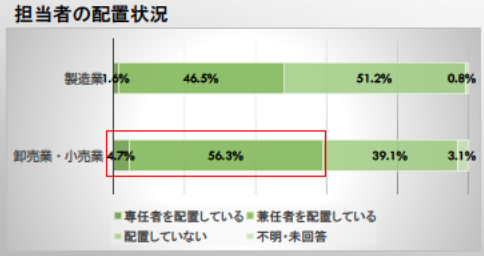
サイバーセキュリティへの対策と意識

業種による違い

担当部署の配置状況



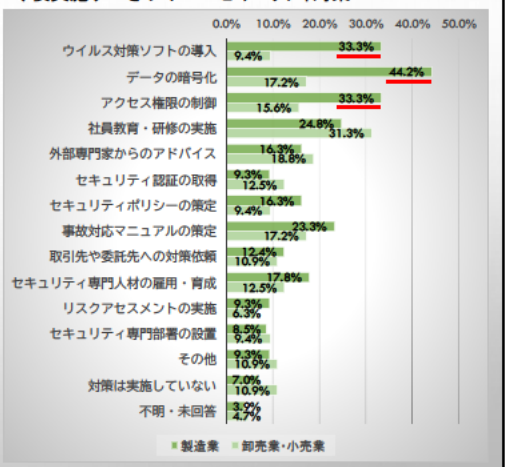
担当者の配置状況



製造業 N=129
卸売・小売業 N=64

卸売・小売業の方が担当設置率が高い

今後実施すべきサイバーセキュリティ対策



製造業はシステム・インフラ面を課題としている率が高い

19

業種による企業状況の違い

業種による違い

【全体】

- 特定の業種が攻撃されている、というわけではない
- 課題については、「人材不足」以外はほぼ同じ

【製造業】

- 機器などを抱える製造業は、求めるセキュリティレベルが他産業より高い可能性もあるが、セキュリティ対応に不安を感じている
- 「ウイルス対策ソフトの導入」や「データの暗号化」など、社内システム面を課題としている
- 卸売・小売業に比べて、「人材の不足」を課題する率が高く、約半数が課題としている

【卸売・小売業】

- 製造業に比べて、担当者・部署の配置している企業が多い
- 今後の実施すべき対策については、製造業よりも「社員教育・研修」に関心が高い
- 担当部署/担当者の配置率は高いが全国平均に比べるとまだ低い（※）

※全国では62.6%（専任27.9%、兼任34.7%）「企業のCISOやCSIRTに関する実態調査2017（IPA）」より

20

比較項目

担当者の有無

担当部署の有無

・被害経験の有無

・業種による違い

・担当者/担当部署の有無

① 担当者未配置　123社
　担当配置　156社

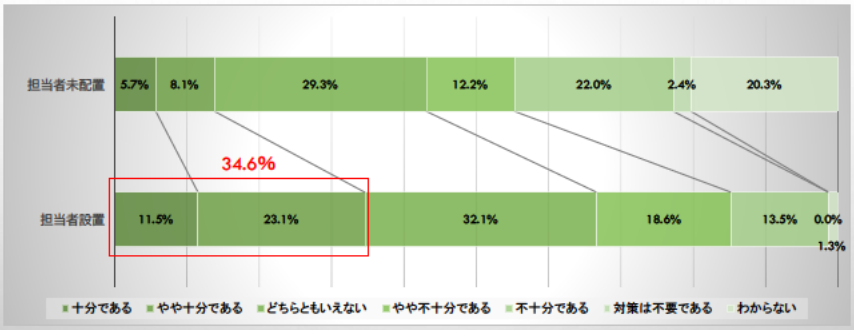
② 担当部署未配置　140社
　担当部署配置　141社

21

① サイバーセキュリティへの対応状況について

担当者の有無

現在のサイバーセキュリティ対策を十分と感じるか



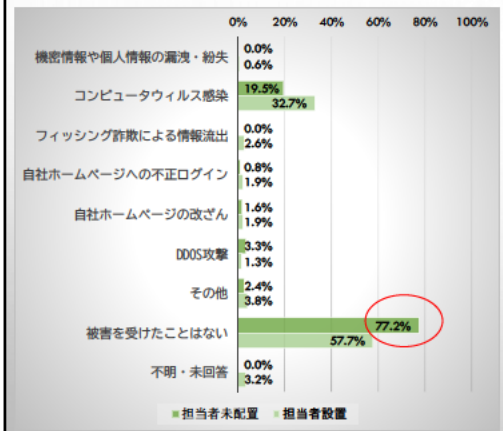
担当配置によりセキュリティ対策の充足度は高まるようである。

22

① サイバーセキュリティ被害状況と関心の高い情報

担当者の有無

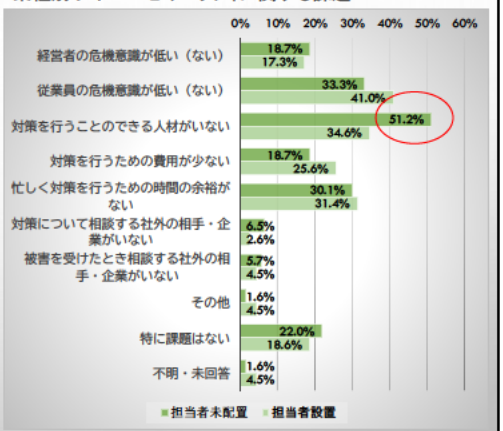
受けたことのあるサイバーセキュリティ被害



複数回答
担当者未配置　N=123
担当者配置　N=156

担当未配置により、被害に気がついていない可能性もある。

業種別サイバーセキュリティに関する課題



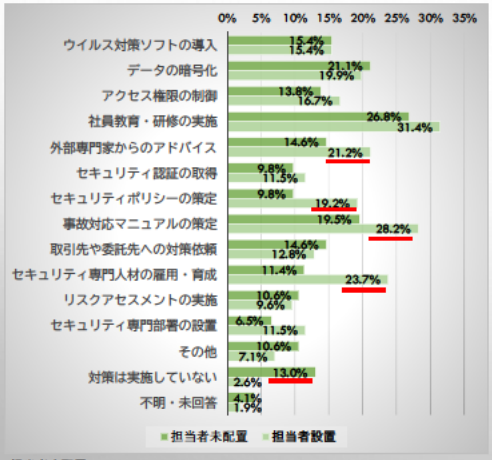
担当未配置の課題としては、人材不足があげられる。

23

① サイバーセキュリティへの対策と意識

担当者の有無

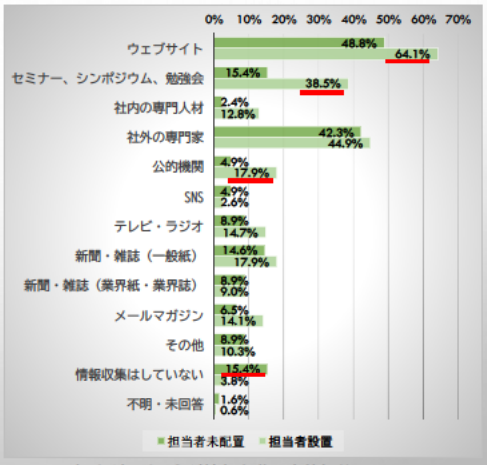
今後実施すべきサイバーセキュリティ対策



担当者未配置 N=123
担当者配置 N=156

担当配置企業は様々な対策を検討している
未配置企業は何もしていない率が高い

関連情報収集先



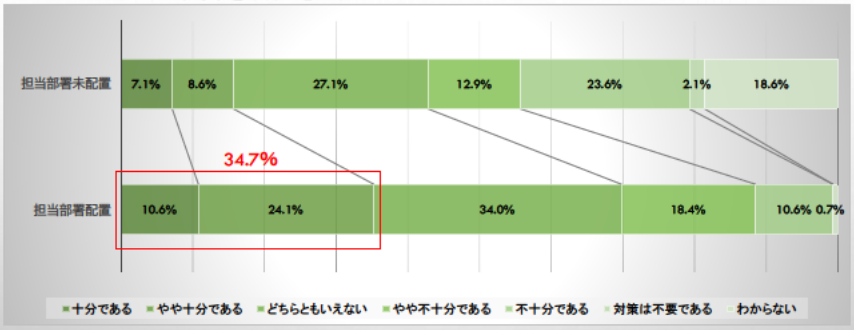
担当がいるほうが情報収集にも積極的
未配置企業は情報収集もしていない率が高い

24

② サイバーセキュリティへの対応状況について

担当部署の有無

現在のサイバーセキュリティ対策を十分と感じるか



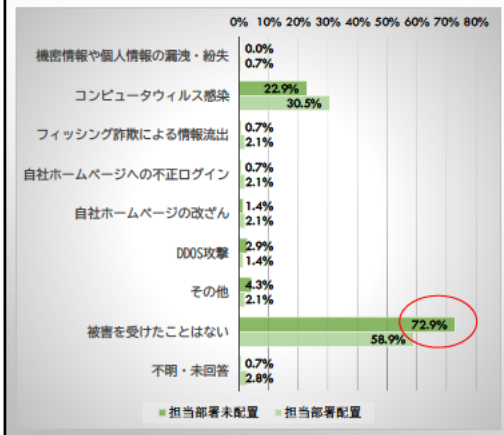
担当部署によりセキュリティ対策の充足度は高まるようである。

25

② サイバーセキュリティ被害状況と関心の高い情報

担当部署の有無

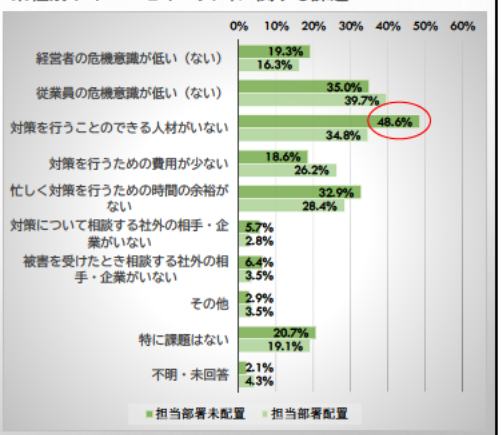
受けたことのあるサイバーセキュリティ被害



複数回答
担当者未配置 N=140
担当者配置 N=141

担当部署未配置により、被害に気がついていない可能性もある

業種別サイバーセキュリティに関する課題



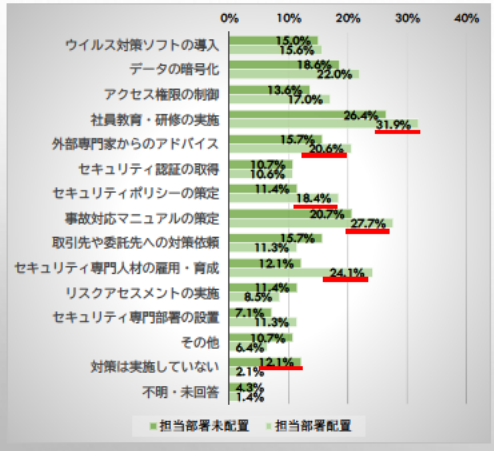
未設置企業の課題としては、人材不足があげられる。

26

② サイバーセキュリティへの対策と意識

担当部署の有無

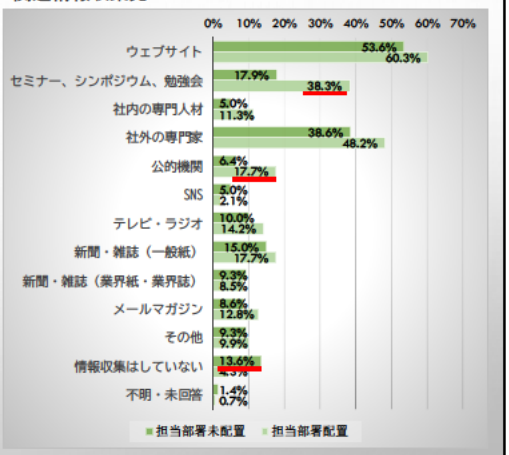
今後実施すべきサイバーセキュリティ対策



担当者未配置 N=140
担当者配置 N=141

担当部署配置企業の方が様々な対策に取り組もうとしている

関連情報収集先



担当部署配置企業のほうが情報収集に積極的
担当部署未配置企業は情報収集をしていない率が高い

27

担当の有無による企業状況の違い

担当者の有無
担当部署の有無

【担当者/担当部署配置企業】

- 現状のセキュリティ対策を満足している傾向にある
- 今後の対策として「人材育成」や、「セキュリティポリシー」「対応マニュアル」など社内体制に力を入れる傾向が高い
- 情報の収集も未配置企業に比べて積極的

【担当者/担当部署未配置企業】

- 被害経験のない率が高い
- 「人材の不足」が課題としてあげられている
- 配置企業に比べて、情報収集や対策の実施などを行っていない率が高い

28

目次

29

各種比較のまとめ

【企業が組織として抱える課題】

- 被害の有無について、特定の業種等の偏りは見受けられなかった
- 被害経験を有する企業では、セキュリティ担当を配置している傾向がある
- どの分析でもセキュリティ人材の不足が認識されている

被害を受けない、受ける可能性が低い、という業種はあまりない。
その一方、「対策を行える人材がいない」ことが、企業が対策を行う上での課題となっている。
企業のニーズに合わせて、必要とされる様々な知識や技術を保有するセキュリティ人材が求められている。

【企業内部としての課題】

- 社内の危機意識の低さがどの分析でも課題とされている
- 主体で動く人材・部署がある場合、社内の意識向上や人材の育成が課題として認識されている
- 意識が高まり積極的に情報取得されれば、危機意識の向上、最新対策の反映などが見込まれる

危機意識の低さは、昨今の標的型メールによる被害を発生させる可能性や、担当者を設置していても、必要とする対策に、経営層が理解を示さないことなどの課題もある。
そのため、特に経営層の危機意識の低さは、企業内の危機意識の低さや、セキュリティ対策の低下につながる課題といえる。

【まとめ】

- セキュリティ人材の不足が大きな課題となっている
- 道内企業内での経営層・従業員の危機意識の低さが明確化した

30

目次

31

【参考】地域未来牽引企業/地域経済牽引事業計画承認企業

経済産業省では、地域経済の中心的な担い手として、地域の特性を生かして高い付加価値を創出し、地域の事業者等に対する経済的波及効果を及ぼすことにより地域の経済成長を力強く牽引する事業を更に積極的に展開すること、または、今後取り組むことが期待される企業を選定している。

今回の調査で選定企業の一部から回答があったので参考までに抽出・集計したものを提示。
回答社数　　28社（地域未来牽引企業＋地域経済牽引事業計画承認企業）
選定企業以外　253社

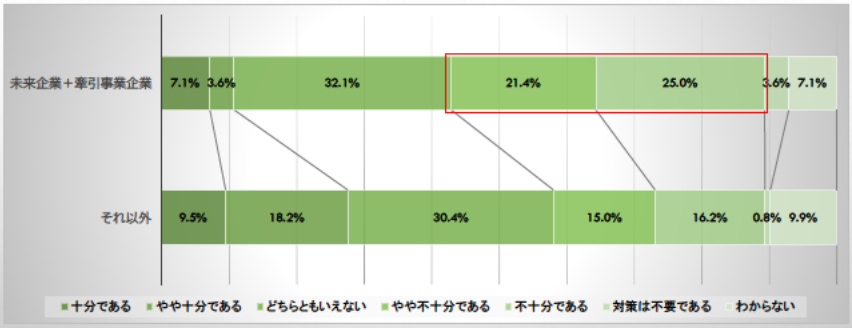
地域未来牽引企業でも、サイバーセキュリティに関して有している課題は同じような状況

32

サイバーセキュリティへの対応状況について

未来牽引企業＋牽引事業計画承認企業

現在のサイバーセキュリティ対策を十分と感じるか



未来牽引企業＋計画事業承認企業 N=28
その他の企業 N=253

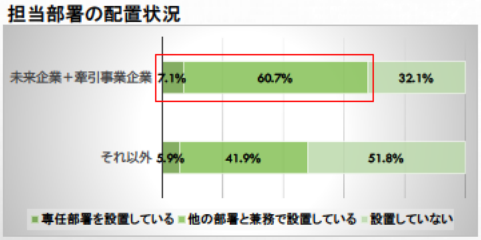
対応は不十分という回答が、未来牽引企業・牽引事業承認企業では多い

33

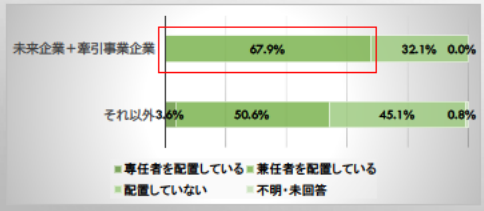
サイバーセキュリティへの対応と被害経験

未来牽引企業＋牽引事業計画承認企業

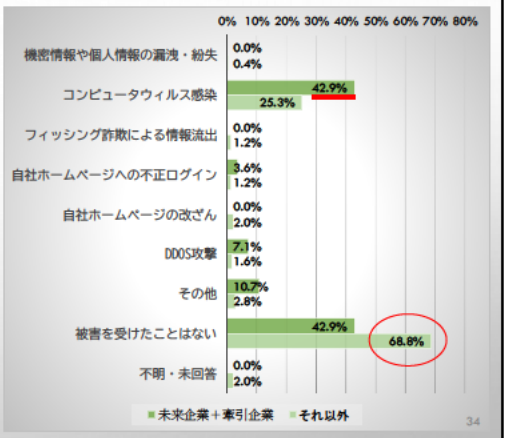
担当部署の配置状況



専任者の配置状況



受けたことのあるサイバーセキュリティ被害



34

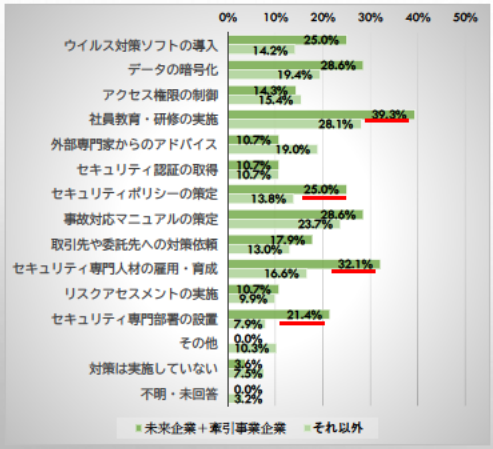
担当の設置率も高い

未来牽引企業＋計画事業承認企業 N=28
その他の企業 N=253

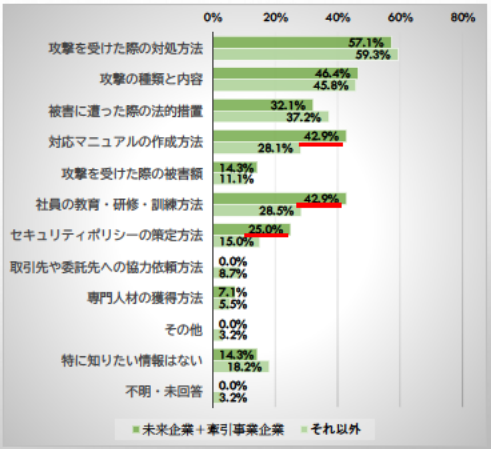
サイバーセキュリティへの対策と意識

未来牽引企業＋牽引事業計画承認企業

今後実施すべきサイバーセキュリティ対策



サイバーセキュリティに関して知りたい情報



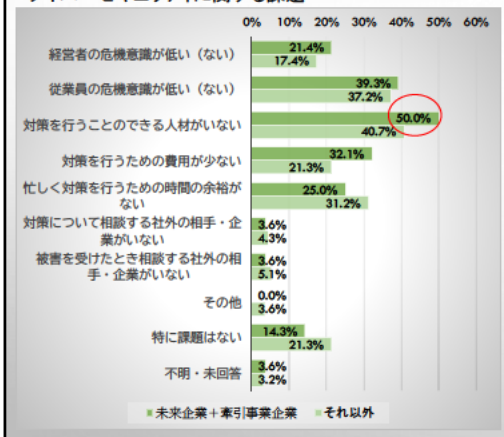
未来牽引企業＋計画事業承認企業 N=28
その他の企業 N=253

35

サイバーセキュリティ被害状況と関心の高い情報

未来牽引企業＋牽引事業計画承認企業

サイバーセキュリティに関する課題



人材不足は同じ

未来牽引企業＋計画事業承認企業 N=28
その他の企業 N=253

36

北海道銀行グループ
株式会社 道銀地域総合研究所
DOGIN REGIONAL RESEARCH INSTITUTE Co., Ltd.

以上になります。
ありがとうございました。

37

2. チラシの作成・配付

HAISL の会員企業の増加に向けて、HAISL の活動内容や入会方法等を記載したチラシを作成し、ヒアリング等の場を通じて配付を行った。

HAISL

北海道地域情報セキュリティ連絡会

Hokkaido Area Information Security Liaison

サイバーセキュリティ対策は十分ですか？

北海道地域情報セキュリティ連絡会は情報セキュリティに役立つ情報を発信しています！

コミュニティ設立の経緯・狙い

北海道地域情報セキュリティ連絡会（HAISL）は、サイバー空間における脅威が増大し、情報セキュリティ対策の重要性が高まる中、北海道総合通信局・北海道経済産業局・北海道警察の３機関を事務局として平成 26 年９月に発足しました。産業界・学術界・官公庁のいわゆる産学官が保有する幅広い情報を共有するとともに、これらの情報を広く発信することにより、道民の情報セキュリティ意識の向上等を図ることを目的に活動しています。

団体概要

会　長　北海道大学情報基盤センター 教授　高井 昌彰

副 会 長　（一社）北海道IT推進協会 副会長　河崎 泰弘
（アイ・ティ・エス(株) 代表取締役）

北海道セキュリティ勉強会 副代表　三谷 公美
（(一社) LOCAL 理事）

(一社) テレコムサービス協会 北海道支部 会長　佐々木 浩一
（NEC ソリューションイノベータ(株) 北海道支社長）

会　員　企業、団体、大学、官公庁など 46 機関（令和2年8月1日現在）

事務局

▶ 総務省北海道総合通信局サイバーセキュリティ室

▶ 経済産業省北海道経済産業局地域経済部製造・情報産業課
TEL: 011-709-2311 (内線 2566)
E-mail: hokkaido-seizojoho@meti.go.jp

▶ 北海道警察サイバーセキュリティ対策本部

入会のお申し込み、またはご不明な点がある場合は、
経済産業省北海道経済産業局へご連絡ください

令和元年度の活動実績

●「Hardening Project（ハードニングプロジェクト）SUII」の共催
（2019 年7月）参加者を仮想 EC サイトのサーバ保守管理チームに編成し、様々なサイバー攻撃に対処しながら、安定的な稼働と売り上げの獲得を競う競技会を北海道で初めて開催しました。

●北海道地域情報セキュリティセミナーの開催
（2019 年9月）「北海道におけるサイバーセキュリティの "今" と "これから" を考える」をテーマに北海道経済センターで開催し、154 名の皆様にご参加いただきました。

●「Micro Hardening for youth（マイクロハードニングフォーユース）」の開催
（2019 年 11 月）「マイクロハードニングフォーユース（MH4Y）」とは「ハードニングプロジェクト」を若者向けに企画、立案したイベント。参加者からは「自分の実力を見つめ直し、今後の目標ができた」等の感想が寄せられました。

令和２年度の活動予定

●「HAISL 人材育成プロジェクト（SC4Y）」の推進
「Security College for Youth（セキュリティカレッジ・フォー・ユース）」では、学生、青年層を対象に情報セキュリティ人材の発掘・育成を行います。

●「中小企業サイバーセキュリティ対策促進事業（サイバーセキュリティお助け隊）」の実施協力
中小企業向けセキュリティ対策支援の仕組みの構築を目的とした実証実験を行います。

●「実践的サイバー防衛演習（CYDER）」の実施協力
仮想の市の情報担当職員として、情報流出事案への対処方法について、実機を用いた演習を通じて体得する講座です。

Ⅸ 課題と今後の方向性

1. 課題

本事業で実施した調査等の結果、明らかになった課題を以下に整理する。

○サイバーセキュリティに対する意識の低さ

アンケート調査からは、道内の中小企業のサイバーセキュリティに対する意識の低さが明らかとなった。意識の低さは、経営層、従業員に共通しているが、従業員の意識が高まったとしても、経営層がサイバーセキュリティ対策の重要性を認識しない限り、対策に必要な人員の配置やコストの負担は行われないことから、より重要なことは経営層の意識を高めることにある。

ちなみに、東日本電信電話株式会社が行った「令和 2 年度中小企業サイバーセキュリティ対策支援体制構築事業」では、実証事業に参加した企業を対象に標的型攻撃メール訓練を実施したが、1 人以上のユーザが訓練メールに添付されたファイルを開封した企業の割合は 11.4%、訓練メールの本文中に記載された URL をクリックした企業の割合は 17.9%であった。この結果は、標的型攻撃メールの受信及び開封に伴いその被害を受ける可能性のある企業が潜在的には 1～2 割程度存在していることを示しており、道内中小企業のセキュリティ意識の向上が急務であることがあらためて浮き彫りになった。

○セキュリティ人材の不足

アンケート調査では、現状のセキュリティ対策のレベルに関わらず、企業においてはセキュリティの知識を持った人材の不足が課題であることが明らかになった。

一方、人材育成カリキュラムの開発・実証においては、年齢制限を排した YouTube Live による視聴申込数が、主に学生を対象とした Zoom による受講者数を大幅に上回る現象が生じた。これは、セキュリティ教育に対するニーズが幅広い年代層に潜在していることを示しているといえる。セキュリティ人材の育成・確保のためには、若年層に対する情報セキュリティ学習の機会を提供するだけでなく、年齢や立場にとらわれない学習機会を提供していくことも重要である。

○セキュリティに関する啓発や人材育成を担う主体の存在感

道外では、セキュリティコミュニティが人材育成機能を有している例が少なくない。コミュニティの運営は、補助金等に頼らずに企業等からの協賛金を財政基盤として、IT 企業出身者が事務局機能を担っている場合が多い。

一方、道内のセキュリティコミュニティである HAISL は、公的機関が中心となって運営されており、産業界との結びつきはけっして強いとはいえない現状にある。道内企業のセキュリティに対する意識が高まることによって、HAISL の重要性が認知されて、HAISL の存在感が増していくことが望まれる。

2. 今後の方向性

○企業・団体におけるサイバーセキュリティの重要性の啓発促進

道内において持続的なセキュリティコミュニティが形成されるためには、資金面や人材面などから、多くの道内企業の協力が不可欠である。本事業で作成した専門家リストのブラッシュアップを行いつつ、リスト化した専門家等も活用し、企業・団体に対しサイバーセキュリティの重要性を強く訴えていくことが重要である。

○セキュリティ人材のスキルアップ機会の創出

セキュリティに関する知識・情報を有し、サイバー攻撃等に対し的確に対処できる人材を育成・確保していくためには、多様な層が参加可能なスキルアップの機会の創出が必要である。本事業では試行的に 30 歳以下を対象としたカリキュラムを開発し、実証を行ったが、今後、これを改良・拡充することによって、セキュリティ人材の層を厚くしていくことが望まれる

○セキュリティコミュニティとしての HAISL の活動の充実

地域におけるサイバーセキュリティの啓発促進や、人材の育成・確保に向けた取組をコーディネートする主体として、HAISL の役割は、今後、より重要性を増すことが予想される。現在は公的機関が中心である HAISL の運営を民間中心にシフトしていくことや、道外のセキュリティ関連団体との連携により効率的に事業を拡充する方策などについて、更なる議論を進めていくことが期待される。