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
（北海道におけるサイバーセキュリティ
コミュニティ強化に向けた調査）

調査報告書

2022 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

経済産業省が令和 2 年 12 月に公表した「DX レポート 2」によると、コロナ禍において従業員・顧客の安全を守りながら事業継続を可能なものとするために企業が直ちに取り組むべきアクションとして、経営のリーダーシップの下、オンライン化、デジタル化など DX の推進が必要としており、今後、道内の中小企業においても更なる DX の推進が必要になると考えられる。

DX の推進により、あらゆるものが繋がるということは、新たな価値創造の可能性が高まる一方で、外部から攻撃を受ける起点が増えることにもなり、これまで以上にセキュリティリスクが増大する可能性がある。そのような状況において、昨年度、北海道経済産業局が実施したアンケート調査から、道内中小企業の経営層、従業員ともにサイバーセキュリティに対する意識が低いことが明らかとなった。中小企業においては、社内方針や予算確保に決定権を持つ経営層の意識改革がサイバーセキュリティ対策の強化に必要不可欠なことから、経営層のサイバーリスクリテラシー向上が喫緊の課題である。

また、同様にアンケートから、セキュリティの知識を持った人材の不足も判明した。現在、道内ではサイバーセキュリティにかかる地域コミュニティとして「北海道地域情報セキュリティ連絡会（HAISL）」※1 が活動しており、人材育成プロジェクトとしては「Security College for Youth（SC4Y）」※2 が教育機関と連携して勉強会等を実施している。しかしながら、これら活動は行政が主導となった取組となっており、道外におけるセキュリティコミュニティのように産業界との連携による体制強化が必要であると考えられる。

本事業では、これら課題に対応するための必要な調査・検討等を行い、DX の推進とともに車の両輪の役割を果たすことが期待される「DX with Cybersecurity」の実現に必要なモデルケースを構築することによって、道内経済の持続発展可能な競争力強化に繋げていくことを目指した。

※1　2014 年に北海道総合通信局、北海道経済産業局、北海道警察が北海道地域における情報セキュリティ意識の向上と情報セキュリティ人材の育成を目的として設立。
※2　HAISL が運営する次世代育成プロジェクト。道内教育機関と連携し、主に学生の人材育成を目的として活動している。

2. 事業の内容

（1）サイバーセキュリティ意識に関する実態調査

道内中小企業の DX への取り組み状況や、サイバーセキュリティ対策への理解度把握及び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に、アンケート調査を行い、結果の集計・分析・とりまとめを行った。

（2）サイバーセキュリティセミナーおよび対策実証モデル構築

昨年度のアンケート調査結果から、道内中小企業においては、経営者層のサイバーセキュリティに対する意識が低いこと、また、サイバーセキュリティの重要性に対する認知に大きな課題があることがわかった。これを踏まえ、道内中小企業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に、セミナーを開催した。

また、中小企業の経営体力に見合った予算規模でセキュリティ対策を実現するための実証を実施し、その結果を整理したうえで広く周知するためのセミナーを開催した。

（3）サイバーセキュリティ人材育成に向けたコミュニティ体制の検討等

道内におけるセキュリティ人材の確保・育成を進めていくには、持続的なセキュリティコミュニティが形成されることが求められる。そのためには、現在の活動の中心を担っている HAISL 等について、公的機関が支えるだけでなく、より多くの民間企業がそこに参画し、セキュリティコミュニティと産業界との結びつきを強めていくことが必要である。

そこで、従来 HAISL 等に積極的に関与してきた各機関と、民間企業等の間で意見交換を行う場を設定し、今後の道内におけるセキュリティコミュニティのあり方や方向性などについて、意見交換を実施、現在は公的機関主導で進められているセキュリティコミュニティの活動について、民間企業を主体とした自立的な運営としていくこと等を検討した。

また、道内の学生等を対象にセキュリティ人材の育成を行っている Security College for Youth（SC4Y）と連携し、サイバーセキュリティ人材育成支援を行った。

（4）道外のセキュリティコミュニティとの連携強化支援

昨年度の北海道経済産業局「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）」においてヒアリング調査の対象とした道外のセキュリティコミュニティの先進事例等について、今後の連携を視野に入れたうえで HAISL などとの情報共有を実施するとともに、必要に応じて意見交換を行った。

（5）調査報告書の作成

上記（1）～（4）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実態調査

道内中小企業の DX への取り組み状況や、サイバーセキュリティ対策への理解度把握及び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に、アンケート調査を行い、結果の集計・分析・とりまとめを行った。

・調査方法
郵送発送、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 3 年 9 月～10 月

・回収率
有効回答　236 件

・調査項目
・回答者属性（所在地、業種、従業員数、売上高）
・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
・サイバーセキュリティ被害を受けたときの損害額
・現在実施しているサイバーセキュリティ対策
・サイバーセキュリティ対策を実施している理由
・サイバーセキュリティ対策の現状に対する認識
・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対策に支出可能な金額
・サイバーセキュリティ対策担当者または担当部署の有無
・サイバーセキュリティに関する課題
・導入または検討している DX（デジタルトランスフォーメーション）の取組　等

【アンケート調査票】

サイバーセキュリティ意識に関する調査

※経営者またはそれに準ずる方がご回答いただくようお願いします。

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
④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	5．DDos 攻撃
2．コンピュータウイルス感染 （具体的に　　）	6．その他 （　　）
3．フィッシング詐欺による情報流出	7．被害を受けたことはない
4．自社ホームページへの不正ログイン	8．わからない

問3　「問2」で1～6を選択した方のみお答えください。
貴社がサイバーセキュリティ被害を受けたときの損害額について、該当するもの1つを○印で囲んでください。
※複数回の被害を受けたことがある場合は、1回あたりの最大の損害額に該当するものを選んでください。

1．50 万円未満	5．1,000 万円以上～5,000 万円未満
2．50 万円以上～100 万円未満	6．5,000 万円以上～1 億円未満
3．100 万円以上～500 万円未満	7．1 億円以上
4．500 万円以上～1,000 万円未満	8．わからない

問4　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5　「問4」で1～13 を選択した方のみお答えください。
貴社がサイバーセキュリティ対策を実施している理由について、該当するもの全てを○印で囲んでください。

1．機密情報を奪われないため	6．社会的信用の喪失を避けるため
2．個人情報保護法への対応	7．特に理由はない
3．サイバーセキュリティ対策が売上に影響するから	8．その他（　　）
4．顧客からの信用を得るため	
5．顧客からの要請があるから	

1

問6　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．対策は必要ない
8．事故対応マニュアルの策定	15．何をしていいかわからない

問8　貴社がサイバーセキュリティ対策に支出可能な金額について、該当するもの1つを○印で囲んでください。

1．月間１万円未満	5．月間１０万円以上
2．月間１万円以上３万円未満	6．費用はかけられない
3．月間３万円以上５万円未満	7．わからない
4．月間５万円以上１０万円未満	

問9　貴社のサイバーセキュリティ対策担当者または担当部署について、該当するもの1つを○印で囲んでください。

1．専任者（部署）を配置している	3．必要だが配置していない
2．兼任者（部署）を配置している	4．必要ないので配置していない

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

問 11　貴社が導入または検討している DX（デジタルトランスフォーメーション）の取組について、該当するもの
全てを○印で囲んでください。

1．執務環境のリモートワーク対応	7．活動量計等を用いた作業員の安全・健康管理
2．社内外との会議等のオンライン化	8．チャットボット等の電話対応業務の自動化
3．紙書類の電子化、ペーパーレス化	9．生産工程における AI や IoT の活用
4．営業活動のデジタル化	10．工場におけるロボット等の導入
5．RPA を用いた定型業務	11．その他（　　）
6．オンラインバンキングツールの活用	12．必要ないため導入（または検討）していない
	13．何をすればよいか分からない

問 12　北海道経済産業局では、道内中小企業にセキュリティ対策機器を数ヶ月程度設置し、セキュリティ診断等を
行う実証事業を予定しています。実証事業への参加を希望しますか？該当するもの1つを○印で囲んでください。

1．希望する	2．希望しない

■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：

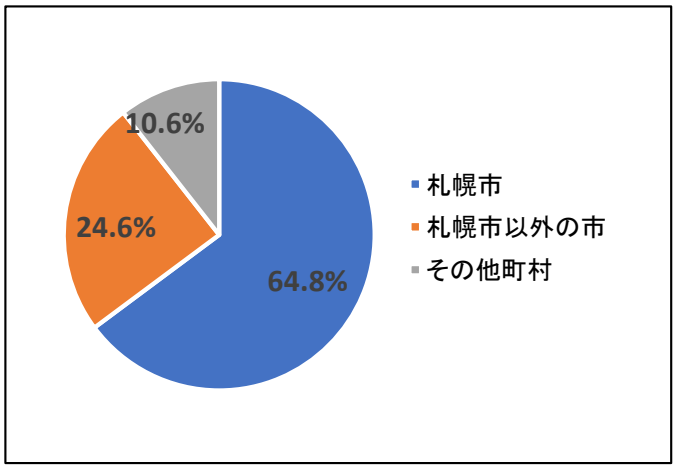
ご協力ありがとうございました。

2

（1）集計結果

■回答属性

・所在地

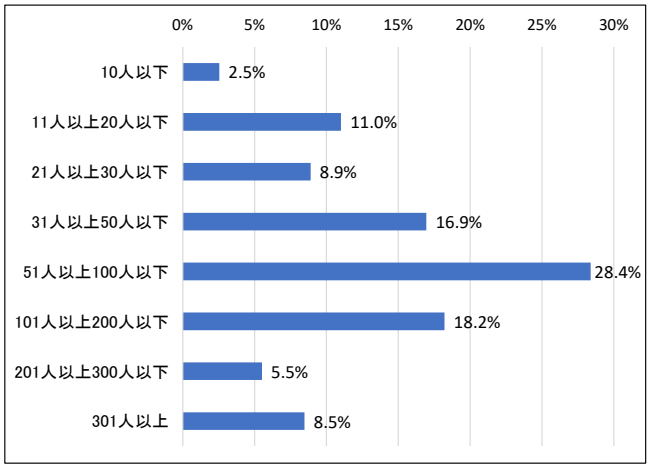


回答企業の所在地は、「札幌市」が 64.8%、「札幌市以外の市」が 24.6%、「その他町村」が 10.6%であった。

・業種（社数）

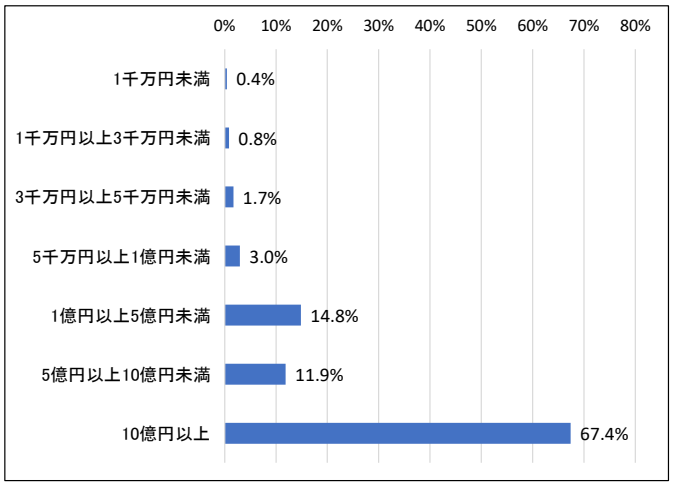
回答企業の業種は、「製造業」が最も多く 102 社、次いで「卸売業、小売業」が 56 社、「建設業」が 31 社であった。

・従業員数



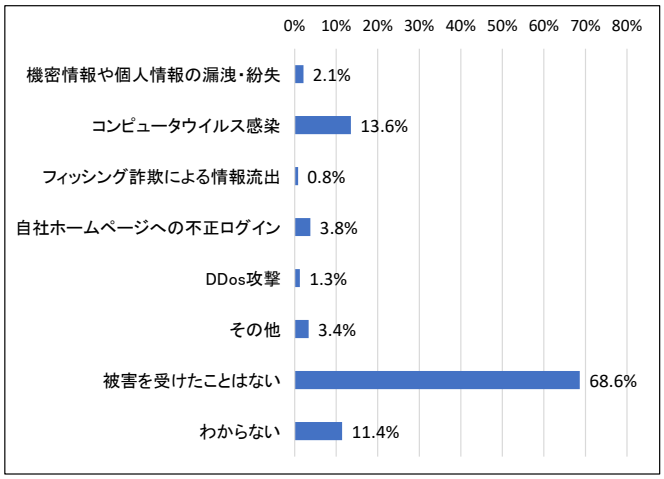
従業員数は「51 人以上 100 人以下」が 28.4%と最も多く、次いで「101 人以上 200 人以下」が 18.2%、「31 人以上 50 人以下」が 16.9%の順である。

・売上高



売上高は「10 億円以上」が 67.4%と多数を占めた。

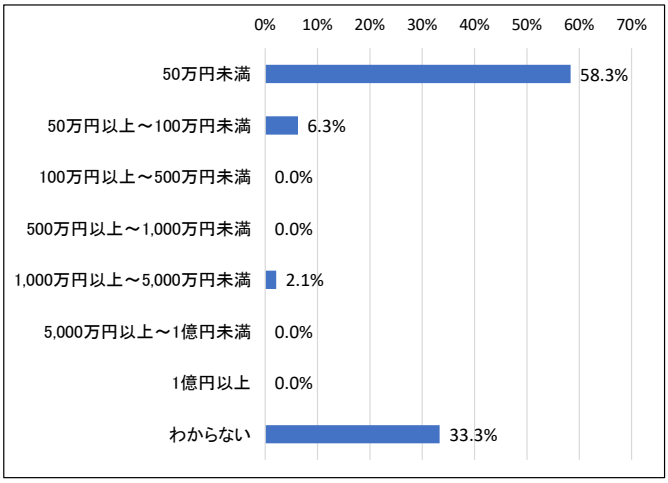
■受けたことのあるサイバーセキュリティ被害（当てはまるもの全て）



受けたことのあるサイバーセキュリティ被害は「コンピュータウイルス感染」が 13.6%最も多かった。具体的な内容（自由記入）では「エモテット」「トロイの木馬」の回答があった。また、「その他」（3.4%）では、具体的な内容（自由記入）として、「アカウント乗っ取り」「ランサムウェア」があった。

一方、「被害を受けたことはない」との回答が 68.6%、「わからない」との回答が 11.4%あった。

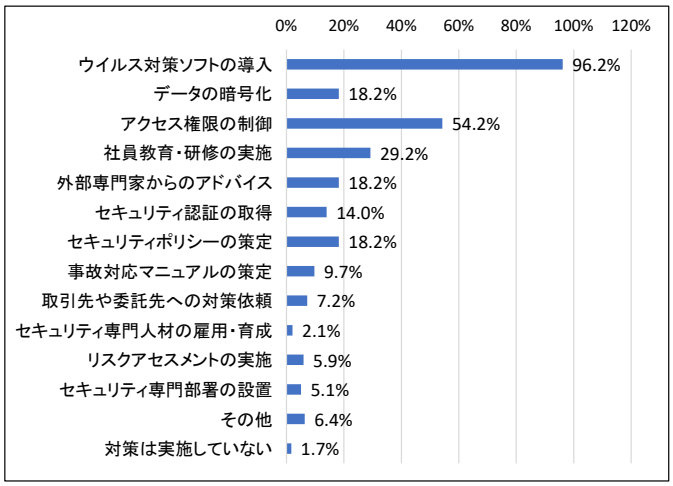
■サイバーセキュリティ被害による損害額



サイバーセキュリティ被害による損害額は「50 万円未満」が 58.3%と最も多く、次いで「50 万円以上 100 万円未満」が 6.3%であった。

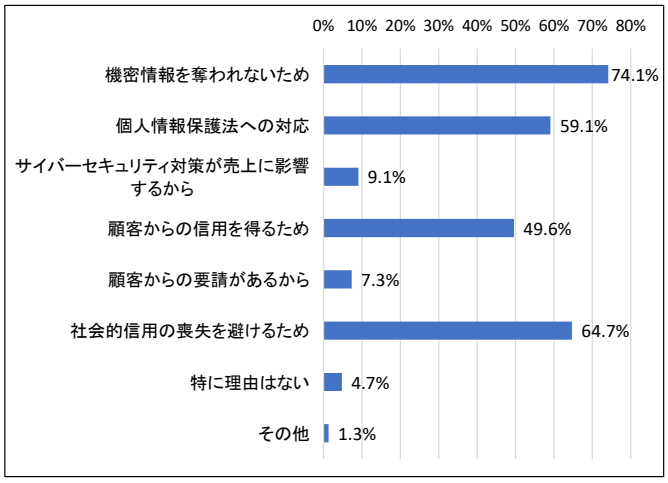
一方、「わからない」との回答が 33.3%あった。

■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）



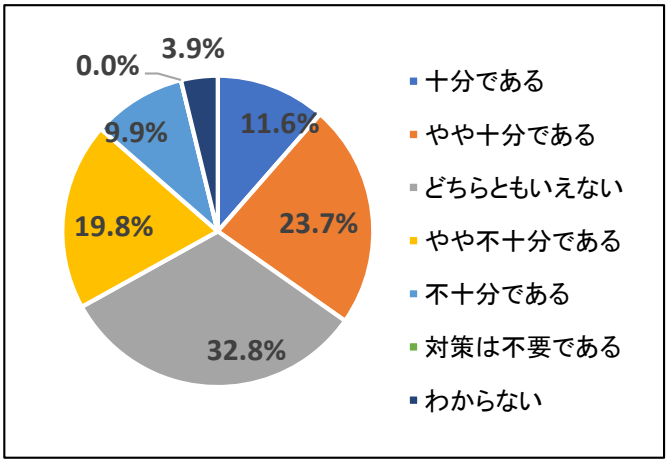
実施しているサイバーセキュリティ対策は「ウイルス対策ソフトの導入」が96.2%と最も多く、次いで「アクセス権限の制御」(54.2%)、「社員教育・研修の実施」(29.2%)の順である。

■サイバーセキュリティ対策を実施している理由（当てはまるもの全て）



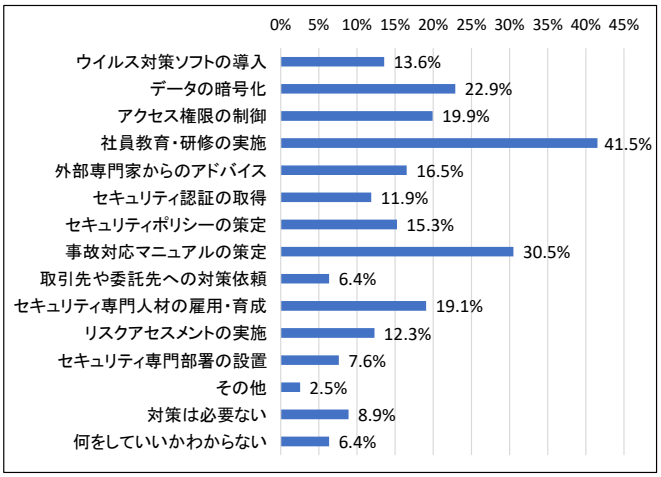
サイバーセキュリティ対策を実施している理由は「機密情報を奪われないため」が74.1%と最も多く、次いで「社会的信用の喪失を避けるため」(64.7%)、「個人情報保護法への対応」(59.1%)、「顧客からの信用を得るため」(49.6%)の順である。

■サイバーセキュリティ対策の現状に対する認識



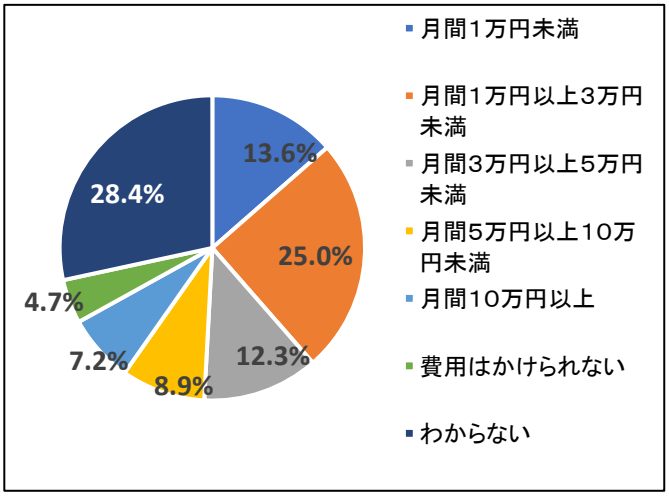
自社のサイバーセキュリティ対策の現状については「十分である」(11.6%)と「やや十分である」(23.7%)の合計が35.3%であったのに対し、「やや不十分である」(19.8%)と「不十分である」(9.9%)の合計が30.7%と、「十分」または「やや十分」が、「不十分」または「やや不十分」を上回った。一方、3分の1近く(32.8%)は「どちらともいえない」との回答。

■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）



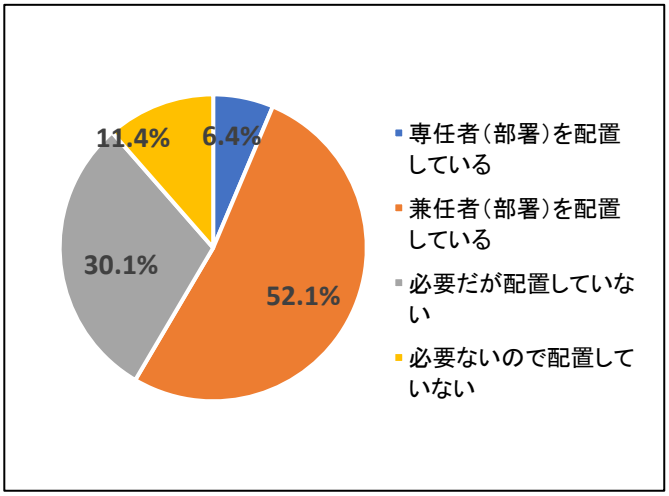
今後実施すべきと思うサイバーセキュリティ対策は「社員教育・研修の実施」が41.5%と最も多く、次いで「事故対応マニュアルの策定」（30.5%）、「データの暗号化」（22.9%）、「アクセス権限の制御」（19.9%）、「セキュリティ専門人材の雇用・育成」（19.1%）の順であった。

■サイバーセキュリティ対策に支出可能な金額



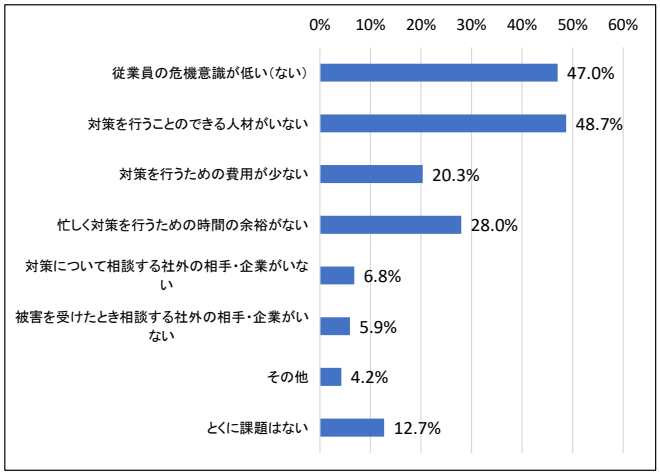
サイバーセキュリティ対策に支出可能な金額は、「月間1万円以上3万円未満」が25.0%と最も多く、次いで「月間1万円未満」（13.6%）、「月間3万円以上5万円未満」（12.3%）の順である。これらを合計すると、全体の半数以上が月間5万円未満との回答である。

■サイバーセキュリティ担当者（または担当部署）の配置



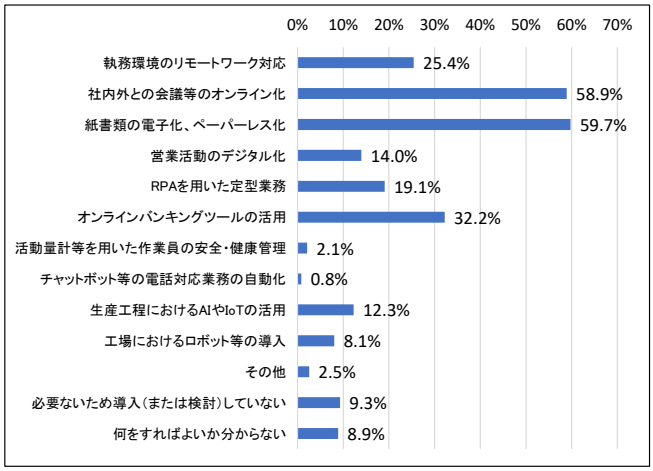
サイバーセキュリティ担当者（または担当部署）の配置については、6.4%が専任者（部署）を配置しており、52.1%が兼任者（部署）を配置している。一方、「必要だが配置していない」が30.1%、「必要ないので配置していない」が11.4%となった。

■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 48.7%と最も多く、次いで「従業員の危機意識が低い（ない）」（47.0%）、「忙しく対策を行うための時間の余裕がない」（28.0%）、「対策を行うための費用が少ない」（20.3%）の順である。

■導入または検討している DX の取組（当てはまるもの全て）



導入または検討している DX の取組は「紙書類の電子化、ペーパーレス化」が 59.7%と最も多く、次いで「社内外との会議等のオンライン化」（58.9%）、「オンラインバンキングツールの活用」（32.2%）、「執務環境のリモートワーク対応」（25.4%）の順である。

（2）考察

以上の結果から、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。

■サイバーセキュリティに対する意識

①担当者（または担当部署）の配置状況

サイバーセキュリティの担当者（または担当部署）を配置している企業は、専任・兼任を合わせて約 6 割に上る一方、必要であると感じていながらも配置していない企業が約 3 割となっている。

担当者（担当部署）を配置している企業が多い一方で、必要性を感じながらも配置できていない企業が一定数存在しているといえる。

②サイバーセキュリティ対策を行う理由

サイバーセキュリティ対策を行う理由としては、情報漏洩対策が約 7 割、社会的信用の喪失に対する抑止が約 6 割、個人情報保護法への対応が約 6 割、顧客からの信用を得るためが約 5 割となっている。

多くの企業が対外的な目を高く意識しており、また、法対策に対する意識も比較的高いといえる。

③現在のサイバーセキュリティ対策に関する認識

自社の現在のサイバーセキュリティ対策に関する認識は「十分」または「やや十分」が約 3 割、「不十分」または「やや不十分」が約 3 割、「どちらともいえない」が約 3 割と、回答が拮抗した。

サイバーセキュリティ対策はどこまでやればよいかという正解が得られにくい事項であり、企業自身も自社の対策が妥当であるかどうかに迷いがあることがうかがえる。

以上から、サイバーセキュリティに対する意識については、対外的な信用や法対策からサイバーセキュリティ対策の必要性は一定程度の認識を持ちつつも、専任がいない、対策が不十分、自社にとって必要な対策を理解できていない等の企業も多いことがわかる。

道内中小企業では、サイバーセキュリティに対する意識と、実際の対策の間にギャップが生じていると思われる。

■サイバーセキュリティの対策状況等

サイバーセキュリティ対策の実施状況では、ウイルス対策ソフトの導入は 9 割以上が実施しており、また、半数以上の企業がアクセス権限の制御を行っている。一方、社員教育・研修を実施している企業は、約 3 割に留まっている。

インターネットの利用や社内データの共有化等に対する対策は取られているものの、コンピュータウイルスへの感染経路として多いものは、不審なメールに添付されたファイルを開くことや、不審なサイトへのリンク先 URL をクリックすること、不審なソフトウェアをインストールすること等であることから、ハードやソフトの対策と併せて、これらを利用する従業員に対する教育については不足していると思われる。

■サイバーセキュリティ対策を行う際の課題等

サイバーセキュリティ対策を行うための課題としては、社内の意識が低いが約 5 割、適当な人材がいないが約 5 割、対策を行う時間の余裕がないが約 3 割となっており、「意識」「人材」「社内リソースの割り当て」が多くの企業で課題となっている。

セキュリティに対する理解不足、知識を有する社内人材の不在、本業との兼ね合いから対策が後回しになっていると考えられる。また、どのような対策手法が存在するのかの周知も必要と思われる。

Ⅲ　サイバーセキュリティセミナーおよび対策実証モデル構築

昨年度、北海道経済産業局が実施した「中小企業のサイバーセュリティ対策等に関する調査」の結果から、道内中小企業においては、経営者層のサイバーセキュリティに対する意識が低いこと、また、サイバーセキュリティの重要性に対する認知に大きな課題があることがわかった。これを踏まえ、道内中小企業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に、セミナーを開催した。

また、中小企業の経営体力に見合った予算規模でセキュリティ対策を実現するための実証を実施し、その結果を整理したうえで広く周知するためのセミナーを開催した。

1．サイバーセキュリティセミナーの開催

昨今の中小企業に対するサイバー攻撃の状況や被害の実例を紹介するとともに、中小企業にとって現実的なセキュリティ対策の解説等を行うため、NoMaps※と連携して、オンライン形式でのセミナーを開催した。

※「NoMaps」とは、米国テキサス州オースティンで毎年開催される世界最大級のビジネスイベント SXSW（サウス・バイ・サウス・ウエスト」の日本版として、最先端のテクノロジーやアイディア等を通して北海道から新たな産業の創出を目指すビジネスコンベンション。

【開催概要】

●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
●日　時：2021 年 10 月 15 日（金）15 時～16 時
●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）
●運　営：㈱道銀地域総合研究所

【プログラム】

１．講演Ⅰ
　情報セキュリティ関連の最新情報について
　　講師：ＰｗＣコンサルティング合同会社 シニアアソシエイト　宇田川辰也氏

２．講演Ⅱ
　中小企業が実施すべきサイバーセキュリティ対策について
　　講師：ＮＴＴ東日本　北海道事業部　マーケティンググループ
　　第一マーケティング担当課長　住本政隆氏

３．ディスカッション
　中小企業に求められるサイバーセキュリティ対策とは
　　ＰｗＣコンサルティング合同会社　宇田川辰也氏
　　ＮＴＴ東日本　北海道事業部　住本政隆氏
　　コーディネーター：道銀地域総合研究所　執行役員　地域戦略研究部長
　　清水友康

●内容（要旨）

1．講演「情報セキュリティ関連の最新情報について」
（ＰｗＣコンサルティング合同会社 シニアアソシエイト　宇田川辰也氏）

・ 急激なテレワーク推進の影響で、組織のテレワークへの移行やウェブ会議の活用等を狙った攻撃が急増している。
・ IPA が発表した情報セキュリティの 10 大脅威の第 1 位は、ランサムウェアによる被害。近年では身代金要求に応じる可能性の高い企業を標的として、企業ネットワークに侵入してシステム構成や重要情報を探索後にランサムウェアを感染させる攻撃が主体となっている。身代金を支払ってもデータが復旧される、または重要情報等のデータが公開されない保証はないため、身代金支払いをせずにバックアップ等からデータ復元を図ることが望ましい。
・ 10 大脅威の第 2 位は、標的型攻撃。直接的な対応は難しいが、攻撃対象となりうるインフラやアプリなどの脆弱性を可能な限り迅速に塞いでおくことで、攻撃を受けるリスクを最小限にすることができる。
・ 10 大脅威の第 3 位は、テレワーク等のニューノーマルな働き方を狙った攻撃。在宅で勤務するテレワーカーが世界中で急増し、個人の端末や家庭のネットワークが仕事に使われる状況は「侵入口が増えて鍵が減った新しい職場」とも形容される。利用中の製品、特に外部ネットワークと通信する機器については、脆弱性対応の徹底が必要。
・ 経営者は、経済産業省と IPA が示す「サイバーセキュリティ経営ガイドライン」に記載された「経営者が認識する必要がある 3 原則」を確認し、自社にどのような不備や不足があるかを特定し、その課題を解決するための対策を行うことが重要。
・ 大事なことはセキュリティ事故に遭わないことではなく、すばやくセキュリティ事故に気づけること。役員がセキュリティ事故の可能性を疑い、適切に指示・対処することで、業務への影響を最小化できる。

2．講演「中小企業が実施すべきサイバーセキュリティ対策について」
（ＮＴＴ東日本　北海道事業部　マーケティンググループ　第一マーケティング担当課長　住本政隆氏）

・ サイバーセキュリティの動向は、近年、自身の技術力を誇示する「愉快犯」から、金銭や換金性の高い情報を搾取する「経済犯」へと移りつつあるが、さらに新型コロナウイルス感染拡大の影響で急激なテレワークの増加が進んだことで、「攻撃起点」の拡大が新たな脅威となっている。
・ 対策は「侵入させない」（入口対策）・「外部通信させない」（出口対策）・「活動させない」（内部対策）の 3 つの「させない」と、「ルール」と「社員教育」。
・ 前年度に道内中小企業 143 社にサイバー攻撃の監視装置を設置する実証事業を行った。その結果、不正侵入は実証参加企業の約 80%、スパムメールは実証参加企業の約 69%で検知され、多くの企業で身近にサイバーセキュリティ脅威が潜んでいる状況が明らかとなった。

・ 実証期間内でランサムウェアを 129 件検知した参加ユーザもおり、集中的にサイバー攻撃を受けている企業も存在している。
・ こうしたセキュリティ脅威を防ぐために、基本的なセキュリティ対策として出入口対策が必要。
・ 実証参加企業に対するメール訓練では、全体の 2 割程度がメールを開封・クリック。しかし、訓練や研修後のアンケートでは、大半の企業が「意識が向上」と回答。
・ 一方、今後の対策に投じる費用は、ほとんどの企業が「1 万円以下」と回答しており、セキュリティ対策における費用対効果の高いサービス提供が事業者に求められている。

3．ディスカッション

中小企業に求められるサイバーセキュリティ対策とは

ＰｗＣコンサルティング合同会社　宇田川辰也氏

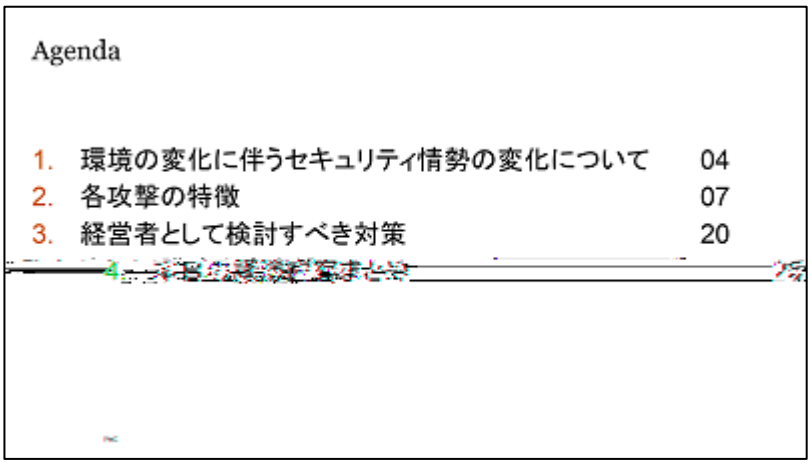
ＮＴＴ東日本　北海道事業部　住本政隆氏

コーディネーター：道銀地域総合研究所　執行役員　地域戦略研究部長　清水友康

・ 中小企業の場合は、人材、時間、費用などの理由から、サイバーセキュリティ対策が後回しになっているのが現状。
・ サイバー攻撃は世界的な有名企業や大企業に対してのみではなく、多くの中小企業に対しても行われている。しかし、中小企業の側では、攻撃を受けていても気づいていないことも多い。
・ サイバー攻撃を受けたときに生じる損害は非常に大きい。システムが使えなくなる、業務が止まるだけでなく、復旧までに数日以上の時間を要することになれば売上にも大きく影響する。また、取引先や顧客へ影響が及ぶことで、対外的な信用を失う可能性もあるなど、サイバーセキュリティのリスクは経営の根幹に関わるもの。
・ 従業員ひとりひとりの意識も大事だが、まずは経営者がサイバーセキュリティ対策の重要性を認識し、サイバーセキュリティ対策を経営課題の一つとして捉えることが必要。それに応じた金額の投資もしていかなければならない。
・ 中小企業ではサイバーセキュリティに長けた人材を配置することは難しいかもしれないが、教育や研修により、セキュリティ担当者、セキュリティ担当部署を育てていくことが大事。

（資料）

1．講演「情報セキュリティ関連の最新情報について」



新型コロナ後の世界の構築に影響をもたらす主な「変動要

新型コロナウイルスの世界的流行に伴い、人々の生活や、社会に大きな影響が生じており、ビジネスにおいても変化が求められています。この変化の一部は、一過性のものではなく、ニューノーマルとして定着する可能性があります。以下4つの主な「変動要因」が、Afterコロナの構築に大きな影響をもたらすと予想されます。

変動要因	概要
リモート環境でのコラボレーション	• リモートワーク環境が恒久的に必要に • オフィスのあり方も変化し、場所を問わず、人の移動や集合を伴わない形でコラボレーション可能な環境が求められる
変化に対応するスピード感	• 不確実性への対応に重心が置かれ、変化に俊敏に対応できることがビジネス推進の必須要素に • ビジネスモデルプロセスはデジタルが前提にとなり、これまでの業務等の社内業務等は変更を余儀なくされる
非接触・オートメーション	• 全ての業務が人間との接触を極力なくす方向にシフト • サプライチェーンの見直しが急速に進み、製造、物流、配送等のオートメーションが必要に • 非接触によるモノや代金のやり取り拡大、キャッシュレス化
全体的な投資抑制・不確実性対応への投資増加	• 不確実性に対処するため、手元資金を高める動き • IT投資も限定的となり、既存システムの保守や維持、不要不急の開発需要が減少する一方で、クラウドや自動化といった不確実性への対応に関わるIT投資は積極的に

各企業にて新型コロナウイルスの影響によりテレワークの促進やDXの推進等、環境の変化が急速に進んでいる。一方で変化のスピードにセキュリティが追従できず、それらを狙ったサイバー攻撃集団による巧妙な攻撃活動が増加。

情報セキュリティ10大脅威について

2021年3月18日、独立行政法人 情報処理推進機構（IPA）より「情報セキュリティ10大脅威2021[組織編]」が公表されました。国内組織における10大脅威は以下の通りです。

■情報セキュリティ10大脅威2021（IPA）

順位	脅威種別（組織）	昨年順位
1位	ランサムウエアによる被害	5位 ↑
2位	標的型攻撃による機密情報の窃取	1位 ↓
3位	テレワーク等のニューノーマルな働き方を狙った攻撃	– NEW
4位	サプライチェーンの弱点を悪用した攻撃	4位 —
5位	ビジネスメール詐欺による金銭被害	3位 ↓
6位	内部不正による情報漏えい	2位 ↓
7位	予期せぬIT基盤の障害に伴う業務停止	9位 ↓
8位	インターネットからのサービス への不正ログイン	10位 ↑
9位	不注意による情報漏えい等の被害	7位 ↓
10位	脆弱な管理画面の公開に伴う悪意ある第三者による被害	14位 ↑

（出典：2021年3月 IPA「情報セキュリティ10大脅威 2021」 https://www.ipa.go.jp/security/vuln/10threats2021.html）

- 標的型ランサムウエア攻撃と二重脅迫により、ランサムウエアによる被害が昨年の5位から1位に急上昇
- 急激なテレワーク推進の影響で、組織のテレワークへの移行やWeb会議の活用等を狙った攻撃が急増、当脅威が初登場で3位に
- 本講演では「情報セキュリティ10大脅威2021」を基にTOP3に対する概要及び対策や対応方法について説明を実施する

2 各攻撃の特徴

TOP1:ランサムウェアによる被害

IPA「情報セキュリティ10大脅威2021[組織編]」にて、第1位である「ランサムウェアによる被害」は、昨年と比較し脅威が高まっています（昨年順位5位）。概要は以下の通りです。

攻撃手口

ウイルス（ランサムウェア）に感染させて金銭を要求
＜攻撃に使われる手口＞
- メールの悪用
- 脆弱性の悪用
- ウェブサイトの悪用
- 不正アクセス

経営層の対策

組織としての対応体制の確立
- 対策の予算の確保と継続的な対策の実施

従業員の対策

被害の予防
- バックアップの取得
- 標的型攻撃対策報告の全般的なセキュリティ対策の実施　など

被害を受けた後の対応
- 迅速な隔離を行い、関連組織、取引先への被害拡大の防止
- バックアップからの復旧　など

TOP1:ランサムウェアとは

サーバやPCのデータを暗号化して使用不可とし、復号することと引き換えに身代金（Ransom）を要求するソフトウェアです。昨今では重要システムがランサムウェアの攻撃を受け、事業の継続を脅かす大規模な被害が発生しています。

ランサムウェアに感染すると

1 データ暗号化
- ファイルを下記形式に変更し、利用できなくする
【ランダムな文字】【不正な拡張子】

2 脅迫文表示
- ファイルの修復に対する身代金支払を求める上記のような脅迫画面が自動で起動される
- 身代金を支払えば、ファイル修復が可能となる

ランサムウェア攻撃による被害事例

事業停止	・製造エネルギー企業はランサムウェア攻撃により**業務停止** 復旧に**10日以上**有している （複数システムも被害を受け、手動復旧で対処）
復旧コスト （身代金、対応費用含む）	・ランサムウェア攻撃を受けた場合、復旧にかかるコストは**平均2.3億円**
二重脅迫	・事前にデータ窃盗しておき、身代金要求に応じない場合、**機微・機密情報のデータ公開を更に脅迫**

- 身代金要求に応じてもファイルが修復できないケースも
- ランサムウェア攻撃を受けた場合、不正アクセスや不正操作等、**抜本的なセキュリティ対策の見直しが必要**

TOP1:ランサムウェア攻撃手口の高度化（暴露型ランサムウェアへの進化）

~~従来の~~ランサムウェア攻撃は**不特定多数にランサムウェアを直接感染させ、身代金を要求する攻撃**が主体でしたが、近年では**身代金要求に応じる可能性の高い企業を予め標的**とし、攻撃者が様々な攻撃手法を駆使して**企業ネットワークへ侵入、システム構成や重要情報を探索後にランサムウェアを感染させる攻撃**が主体となっています。

従来のランサムウェア攻撃

不特定多数へ攻撃（不特定多数へフィッシングメールを送信）
↓
データの暗号化、システム停止（データの暗号化、システム停止を生じさせ身代金を要求）

近年のランサムウェア攻撃

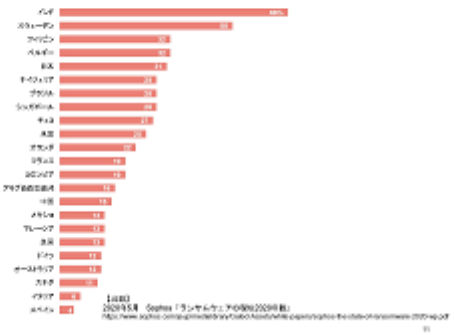
1 攻撃対象企業を選定（身代金要求に応じる可能性のある企業・組織を対象に選定し、調査開始）
↓
2 ネットワークへの侵入（インターネットからアクセス可能な機器の脆弱性等を利用し、侵入）
↓
3 ネットワーク内の情報窃盗探索（機微情報が保存されているサーバや重要システムを探索し、窃盗対象を調査）
↓
4 データの暗号化、システム停止（ランサムウェアを使用して、データの暗号化、システム停止を生じさせ、身代金を要求）
＋
データの窃盗（［二重の脅迫を行っているケース］データを窃盗しておき、身代金要求に応じない場合、更に機微情報の公開を脅迫）

【これまでとの違い】
1. 従来の不特定多数をターゲットしていた攻撃から、近年は身代金要求に応じる可能性のある企業や組織を明確に標的としている
2. 企業ネットワークへ侵入し、ランサムウェアを展開する前に企業内の情報を探索
3. 事前に探索した機微情報や機密情報等を窃盗しておき、データ公開を人質とした二重脅迫

TOP1:身代金支払いに関する国内外動向

ランサムウェアの身代金支払いに関する国内外の動向は以下の通りです。

- 日本でランサムウェアの被害にあった組織のうち、31%の企業が身代金を犯行グループに実際に支払った（支払い率は世界で5位） 右図参照
- 支払い率を国別でみると、サイバー衛生が発達していないインドが1位、次いでスウェーデン、フィリピン、ベルギー、日本の順であった
- 一方、スペインは、わずか4%の企業しか身代金を支払っていない
- ランサムウェアの被害者の28%が、身代金を支払うことでデータを回収



TOP1:ランサムウェアの身代金支払いに関する推奨事項

ランサムウェアに感染時、身代金支払いを検討するケースが増加傾向にあるものの、支払い後に追加の身代金を要求されるケースやデータが復旧されない、又はデータが公開されないという保証はないため、身代金支払いをせずにバックアップ等からデータを復元することを強く推奨します。

推奨事項	**身代金支払いをしないことを強く推奨** （理由） ▪ データが復旧されない、又はデータが公開されないという保証はない ▪ 支払いに応じた場合、犯行グループからの更なる攻撃の対象になる ▪ 犯罪組織への資金提供とみなされる （米国では、金銭の支払いを行った企業に対して、外国資産管理局から制裁が課される可能性あり）

#	対応チェックリスト	チェック
1	どのシステムが影響を受けたか特定し、速やかに隔離する。	☐
2	デバイスをネットワークから切断できない場合にのみデバイスの電源を切り、ランサムウェアの感染拡大を防止する。	☐
3	復旧及び復元のため、影響を受けたシステムを確認・保証する。	☐
4	インシデント対応チームと連携し、初期分析に基づいて発生した事象の初期情報を深め、文書化する。	☐
5	インシデントの検知、対応、復旧のために関与される支援内容を理解したうえで、組織内外のチーム及びステークホルダーを関与させる。	☐
6	影響を受けたデバイス（例：ワークステーションやサーバ）のサンプルからシステムイメージやメモリキャプチャを取得する。	☐
7	セキュリティ研究者がいくつかのランサムウェア亜種が使用する暗号アルゴリズムをすでに解読しているため、利用可能な解読ツールについて法執行機関に相談する。	☐

（参考）No More Ransomプロジェクト

世界の司法当局やセキュリティベンダが運営する「No More Ransom」プロジェクトでは、身代金を支払わないように訴えています。また、当該プロジェクトでは、復号化の研究を行い、暗号化されたファイルを復号できるよう情報発信・支援を実施しています。

【参考URL】 No More Ransom: https://www.nomoreransom.org/jp/index.html

TOP2:標的型攻撃とは

IPA「情報セキュリティ10大脅威2021[組織編]」にて、第2位である「標的型攻撃による機密情報の窃取」は昨年に引き続き高い脅威です(昨年順位1位)。概要は以下の通りです。

攻撃手口

メールやウェブサイトからウイルスに感染させる

<攻撃に使われる手口>
- メール(標的型攻撃メール)の悪用
- ウェブサイトの悪用
- 不正アクセス

経営層の対策

組織としての対応体制の確立
- 迅速かつ継続的に対応できる組織内体制(CSIRT)の構築
- 対策予算の確保と継続的な対策の実施
- セキュリティポリシーの策定

従業員の対策

組織としての体制の確立
- セキュリティ教育の受講
  - ✓「メールの添付ファイルやURLを安易に開かない」
  - ✓「Officeファイルのマクロを安易に有効にしない」
  - ✓「被害を受けた際は速やかに連絡」

被害を受けた後の対応
- CSIRT等所定の連絡先への連絡

TOP2:標的型攻撃とは

標的型攻撃とは、「組織的・規則的な意図をもって外部から行われる情報の窃取・破壊等の攻撃」を指します。
攻撃者は標的とする組織の様々な情報を収集し、取引先に成りすましてメールを送ったり、標的組織の従業員が良く利用するWebサイトにウイルスを仕込んだりして攻撃の起点を作ろうとします。

パソコン端末を狙うサイバー攻撃の9割以上はメール経由のため、メールセキュリティ製品の導入や従業員教育(不審なメール・添付ファイルは開かない)等を実施することが重要です。

事例紹介

TOP2:ファイル共有サーバ不正アクセス被害で個人情報流出

社員が外部とファイルの送受信をする際に使うファイル共有サーバに不正アクセスがあったと発表しました。不正アクセスを受けたファイルに含まれていた個人情報が流出した可能性があるとのことです。調査からゼロデイ攻撃の痕跡が見つかりました。

ゼロデイ攻撃への直接的な対応は難しいが、攻撃対象となりうるインフラやアプリなどの脆弱性を可能な限り迅速にふさいでおくことで、被害を受けるリスクを最小限にすることができる。自ごろからサーバやネットワーク関連機器等の修正パッチが公開されたら、速やかに適用することが重要

TOP3:テレワーク等のニューノーマルな働き方を狙った攻撃

IPA「情報セキュリティ10大脅威2021[組織編]」にて、第3位である「テレワーク等のニューノーマルな働き方を狙った攻撃」は今年初めて登場した脅威です（昨年順位なし）。概要は以下の通りです。

攻撃手口

テレワーク環境や管理体制の不備

＜攻撃に使われる手口＞
- テレワーク用ソフトの脆弱性を悪用した不正アクセス
- 急なテレワーク移行による管理体制の不備
- 私物PCや自宅ネットワークの利用 ※私物PCからの情報漏えいのおそれ

経営層の対策

組織としての対応体制の確立
- 迅速かつ継続的に対応できる組織内体制（CSIRT）の構築
- 対策予算の確保と継続的な対策の実施
- テレワークのセキュリティポリシーの策定

従業員の対策

情報リテラシーや情報モラルの向上
- セキュリティ教育の受講

被害の予防
- 組織のテレワークルールを順守（使用する端末、ネットワーク環境、作業場所等）

被害を受けた後の対応
- CSIRT等規定の連絡先への連絡

TOP3:テレワークは格好の攻撃標的に

在宅で勤務するテレワーカーが世界中で急増する中、サイバー攻撃の被害が増大する危険はかつてなく高まっています。個人の端末やスマートフォン、管理されないまま脆弱性が放置された家庭用Wi-Fiルータやネットワーク、そうした環境が「仕事に使われる状況は「侵入口が増えて鍵が減った新しい職場」とも形容されています。

テレワーク拡大に伴いツールやソフトウェアの脆弱性をついた攻撃の増加

- ✓ 社内に遠隔で接続を行うためのツール（VPN製品等）の脆弱性をついた攻撃
- ✓ WEB会議ソフトの活用が拡大する中、偽参加依頼メールやWEB会議のハイジャック
- ✓ 自宅ネットワークや公衆Wi-Fiの脆弱性を突いた盗聴や不正アクセス 等

狙われている機器・環境

事例紹介

TOP3:VPN製品を利用する国内企業の認証情報が流出

ハッカーフォーラム上で、900社を超える（内、国内企業数十社）VPN認証情報が流出していることを確認しました。情報流出した企業は共通して、VPN製品の脆弱性を放置したまま利用していました。攻撃者はこれらの情報を基に、企業への不正アクセス等を実施するため、利用製品の管理・脆弱性対応の徹底が必要です。

概要	• VPN製品について、認証情報窃取に繋がる脆弱性を公表。 当該エクスプロイトコードもWEB上に公開されていた。 • ハッカーフォーラム上でエクスプロイトにより取得したと思われる認証情報が公開された。
原因	• 脆弱性修正パッチを未適用の企業が存在したため、認証情報の流出に繋がった。
イメージ	
対策	• VPNサービス等を利用して社外から社内NWにアクセスする場合、多要素認証が必要。 ※万が一認証情報が流出した場合でも、正規ユーザ以外が社内NWにアクセスできない状態とすることでリスク低減 • 利用中の製品（特に社内NWと通信する機器）について、脆弱性対応の徹底が必要。

3 経営者として検討すべき対策

経営者が認識する必要のある「3原則」

経済産業省とIPA（独立行政法人情報処理推進機構）にて発刊された「サイバーセキュリティ経営ガイドライン」には経営者が認識する必要がある「3原則」が記載されております。

経営者が認識する必要がある「3原則」

経営者は、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要

セキュリティへの経営資源投下に係る適切な判断のため、サイバーリスク管理に、内外の脅威動向把握、自社のセキュリティ対策状況把握など各種情報の整理、管理が必要

自社のみならず、ビジネスパートナーや委託先も含めたサプライチェーンに対するセキュリティ対策が必要

ビジネスへの影響を最小化する観点から、サプライチェーン全体を踏まえたリスク管理/セキュリティ構想が必要

平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報開示など、ステークホルダー（顧客、株主等）との適切なコミュニケーションが必要

「お客様や株主を守る」という姿勢とそのための対策状況をアピールすることが必要

出典：2017年11月 経済産業省サイト「サイバーセキュリティ経営ガイドライン」https://www.meti.go.jp/policy/netsecurity/downloadfiles/guideV2.0.pdf

サイバーセキュリティ経営ガイドラインとは

「サイバーセキュリティ経営ガイドライン」とは、経済産業省とIPA（独立行政法人情報処理推進機構）により策定されたものであり、「サイバーセキュリティは経営問題である」というメッセージの下に、サイバー攻撃から企業を守る観点で、経営者が認識、および実施すべき内容を記載しています。

背景	ビジネスの現場において、ITの利活用は企業の収益性向上に不可欠なものとなっている一方、 企業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続けている。 これに例い、企業戦略としてのIT投資やセキュリティ投資などの程度行うかなど、経営者による判断が必要となっている。
目的	経営戦略上ITの利活用が不可欠である企業の経営者のリーダーシップの下で、サイバーセキュリティ対策を推進させる

引用元：経済産業省サイト「サイバーセキュリティ経営ガイドラインの概要」

サイバー攻撃から企業を守る観点で、以下を定めている。

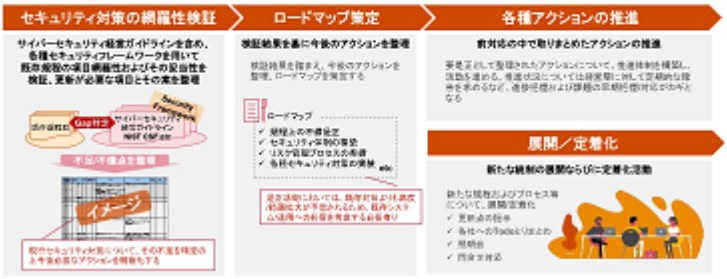
- ✓ 経営者が認識する必要のある「3原則」
- ✓ 経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO等）に指示すべき「重要10項目」

出典：2017年11月 経済産業省サイト「サイバーセキュリティ経営ガイドラインの概要」https://www.meti.go.jp/policy/netsecurity/mng_guide.html

情報セキュリティ担当幹部（CISO等）に指示すべき「重要10項目」

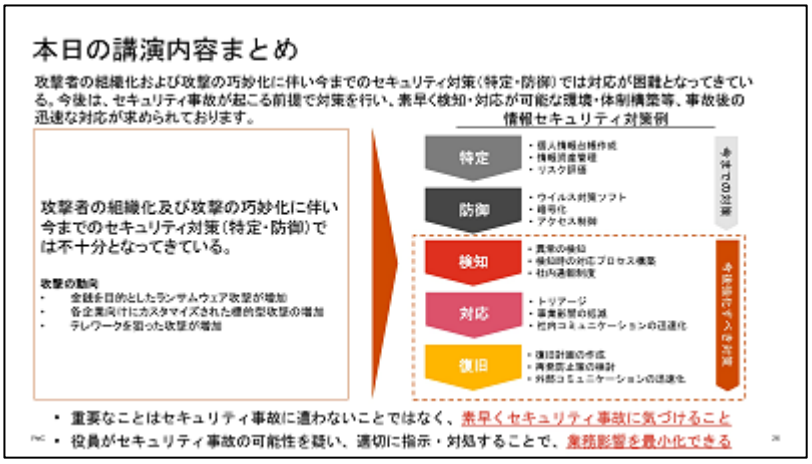
網羅性を持ったセキュリティ対策を行うために

「サイバーセキュリティ経営ガイドライン」に記載されている各項目について、まずはどのような不備／不足があるのか把握されていない場合は、その特定が急務となります。セキュリティアセスメントを通して、課題を特定し、その後必要な対策を推進するという活動が有効です。

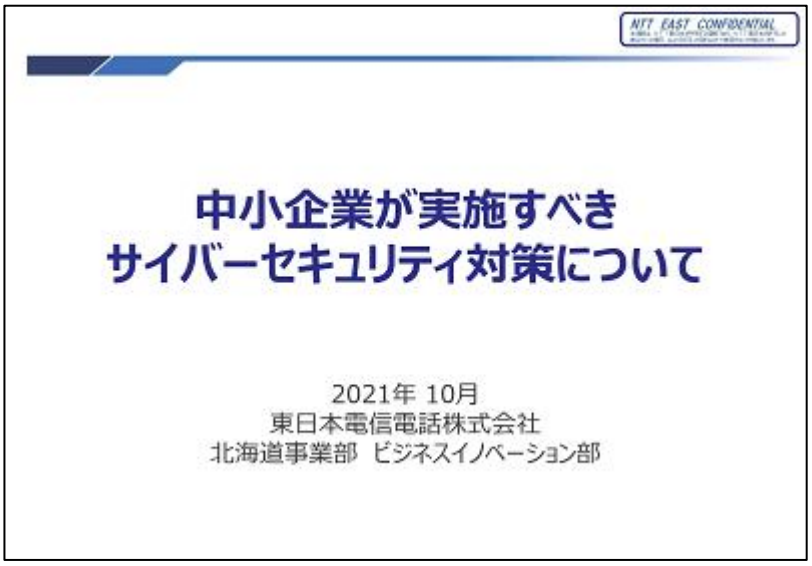


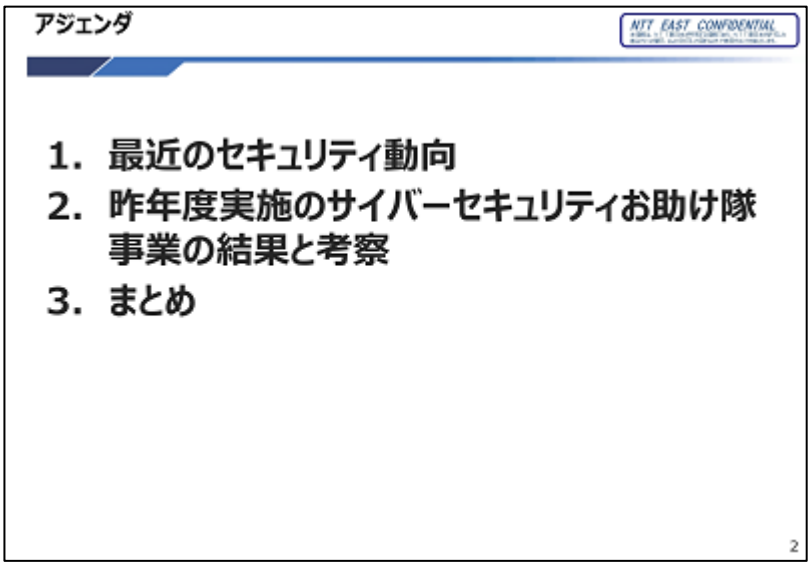
4

本日の講演内容まとめ



２．講演「中小企業が実施すべきサイバーセキュリティ対策について」

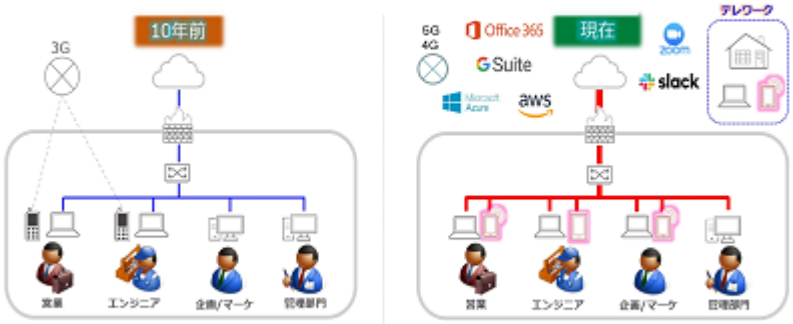




1．最近のセキュリティ動向

1．最近のセキュリティ動向

ICTがもたらす働く環境の変化



- 外出時の通信手段はガラケーが主流（3G）
- ネットワーク帯域幅による大容量データ転送の限界
- インターネット接続はHTTP中心
- 内勤業務の人はオフィスに出社するのが当然

- 社内からインターネットアクセスするデバイスの増加
- 多様なクラウドサービス利用によるトラフィック増
- インターネット通信の80%以上がHTTPS化
- 働き方改革やテレワークによる境界の多様化

4

1．最近のセキュリティ動向

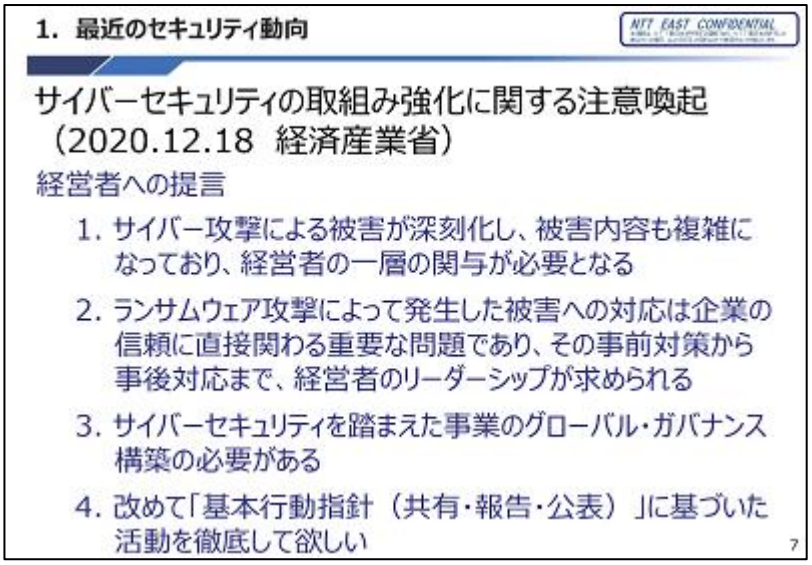
サイバーセキュリティの取組み強化に関する注意喚起（2020.12.18　経済産業省）

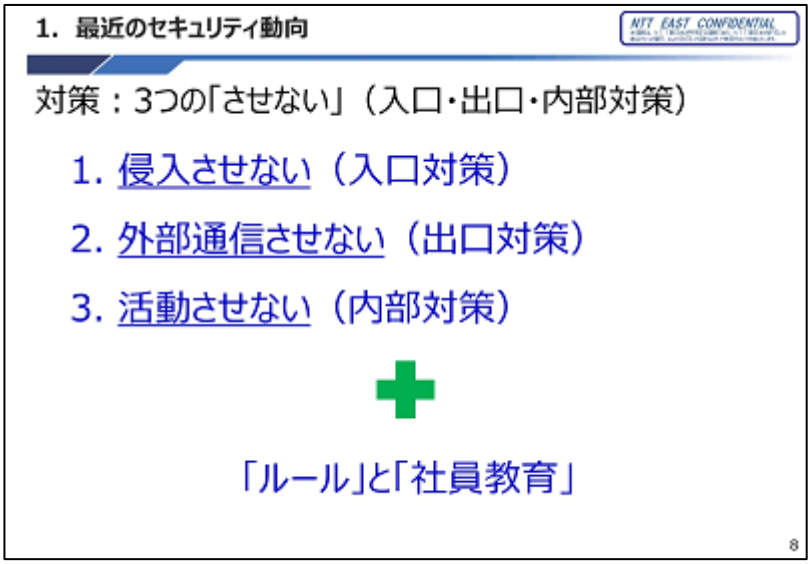
セキュリティ脅威

1. 中小企業を巻き込んだサプライチェーン上での攻撃パターンの急激な拡がり
2. 大企業・中小企業等を問わないランサムウェアによる被害の急増
3. 機微性の高い情報の窃取等を目的としたと考えられる海外拠点を経由した攻撃

5


1. 最近のセキュリティ動向
NTT EAST CONFIDENTIAL
愉快犯
【主な目的】
自身の技術力の誇示
経済犯
【主な目的】
金銭,換金性の高い情報搾取
急速なテレワークの増加
・Covid-19の急速な拡大
・働き方改革
【新たな脅威】
「攻撃起点」の拡大


1. 最近のセキュリティ動向
NTT EAST CONFIDENTIAL
サイバーセキュリティの取組み強化に関する注意喚起
（2020.12.18 経済産業省）
経営者への提言
1. サイバー攻撃による被害が深刻化し、被害内容も複雑になっており、経営者の一層の関与が必要となる
2. ランサムウェア攻撃によって発生した被害への対応は企業の信頼に直接関わる重要な問題であり、その事前対策から事後対応まで、経営者のリーダーシップが求められる
3. サイバーセキュリティを踏まえた事業のグローバル・ガバナンス構築の必要がある
4. 改めて「基本行動指針（共有・報告・公表）」に基づいた活動を徹底して欲しい
7


1. 最近のセキュリティ動向
NTT EAST CONFIDENTIAL
対策：3つの「させない」（入口・出口・内部対策）
1. 侵入させない（入口対策）
2. 外部通信させない（出口対策）
3. 活動させない（内部対策）
「ルール」と「社員教育」
8

NTT EAST CONFIDENTIAL

2. 昨年度実施のサイバーセキュリティお助け隊事業の結果と考察

2. 実証事業概要

NTT EAST CONFIDENTIAL

◆サイバーセキュリティお助け隊事業 とは
（中小企業向けサイバーセキュリティ対策支援構築事業）

- 経済産業省の補助による独立行政法人情報処理推進機構(以下、IPA)の請負事業です。
- 地域の請負事業者(北海道はNTT東日本)が事業主体となり、損害保険会社、地域の団体・企業等と連携し、中小企業のサイバーセキュリティ対策支援を行う地域実証事業です。

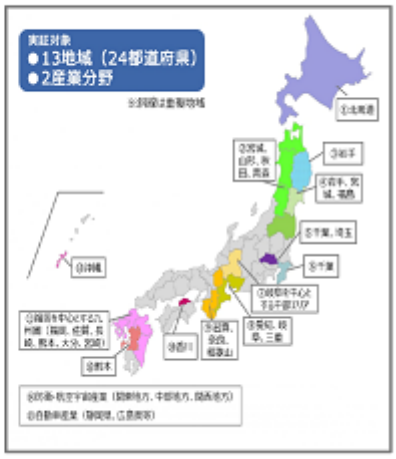
10

2. 実証事業概要

NTT EAST CONFIDENTIAL

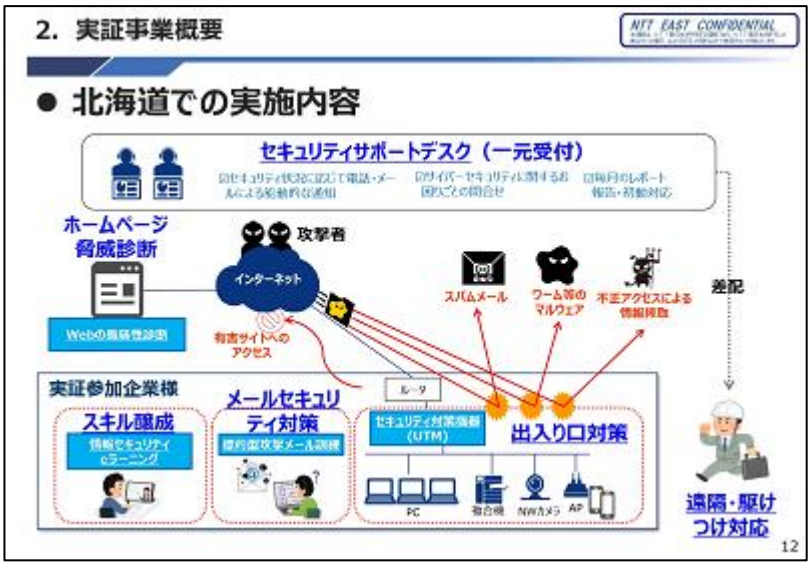
● 目的・対象地域等

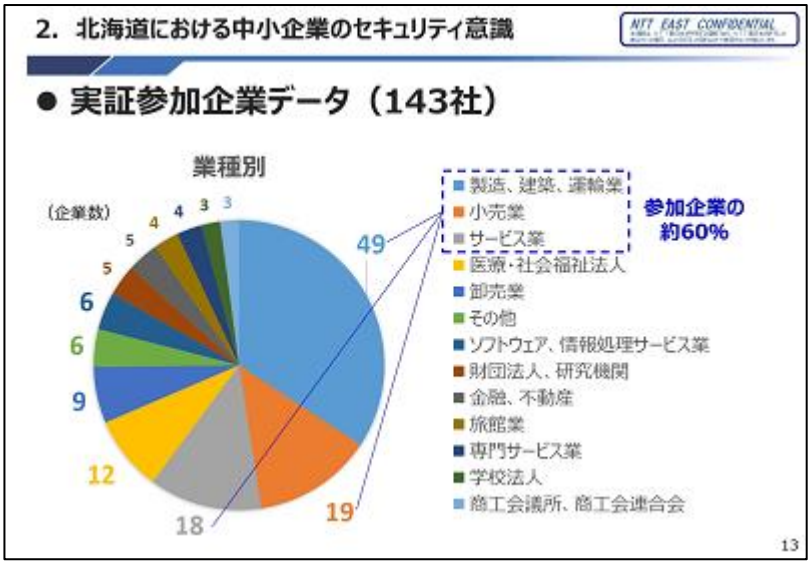
- サイバーセキュリティに関する悩みやニーズ、実態の把握
- 各種セキュリティサービスの導入負荷の低減
- セキュリティ普及啓発
- 中小企業が利用しやすい支援内容等の検討

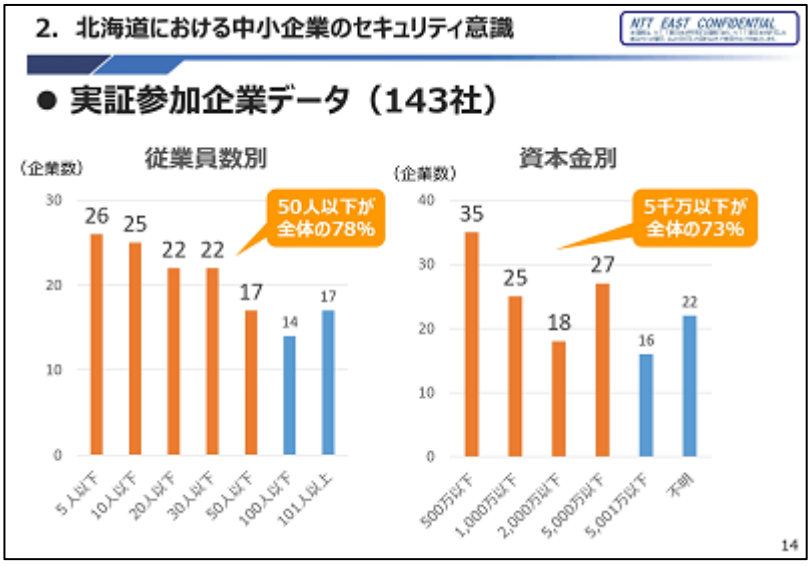


※出典：独立行政法人情報処理推進機構（IPA）ホームページ　https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html

11


2. 実証事業概要
NTT EAST CONFIDENTIAL
● 北海道での実施内容
セキュリティサポートデスク（一元受付）
ホームページ脅威診断
攻撃者
インターネット
Webの脆弱性診断
有害サイトへのアクセス
スパムメール
ワーム等のマルウェア
不正アクセスによる情報搾取
差配
実証参加企業様
スキル醸成
情報セキュリティeラーニング
メールセキュリティ対策
標的型攻撃メール訓練
ルータ
セキュリティ対策機器（UTM）
出入り口対策
PC
複合機
NW カメラ
AP
遠隔・駆けつけ対応
12


2. 北海道における中小企業のセキュリティ意識
NTT EAST CONFIDENTIAL
● 実証参加企業データ（143社）
業種別
（企業数）
49
19
18
12
9
6
6
5
5
4
4
3
3
製造、建築、運輸業
小売業
サービス業
参加企業の約60%
医療・社会福祉法人
卸売業
その他
ソフトウェア、情報処理サービス業
財団法人、研究機関
金融、不動産
旅館業
専門サービス業
学校法人
商工会議所、商工会連合会
13

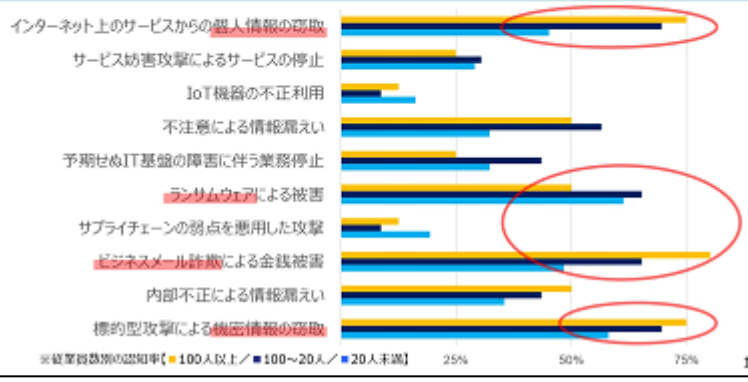

2. 北海道における中小企業のセキュリティ意識
NTT EAST CONFIDENTIAL
● 実証参加企業データ（143社）
（企業数）
従業員数別
30
20
10
0
26
25
22
22
17
14
17
50人以下が全体の78%
5人以下
10人以下
20人以下
30人以下
50人以下
100人以下
101人以上
（企業数）
資本金別
40
30
20
10
0
35
25
18
27
16
22
5千万以下が全体の73%
500万以下
1,000万以下
2,000万以下
5,000万以下
5,001万以下
不明
14

2. 北海道における中小企業のセキュリティ意識

NTT EAST CONFIDENTIAL

● サイバーセキュリティ脅威の認知状況

メール詐欺・ランサムウェアや情報の窃取という脅威の認知度が高い。
総じて会社規模が大きい方が、主要なサイバー攻撃の認知度が高かった。



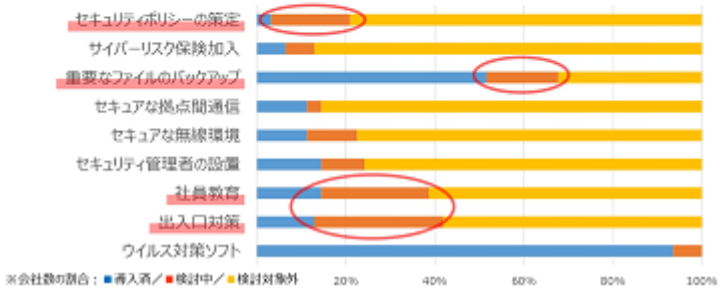
15

2. 北海道における中小企業のセキュリティ意識

NTT EAST CONFIDENTIAL

● 導入済み・検討中のセキュリティ対策

ウイルス対策ソフト・重要ファイルのバックアップは、パソコン導入時の設定やデータ破損全般の備えとして**多くの企業が導入済。**
サイバー攻撃自体は認知しているものの、予防的措置をとるほどの脅威は感じていないようだが、**出入口対策・社員教育**を**検討中**の会社も比較的多い。



16

2. 北海道における中小企業のセキュリティ意識

NTT EAST CONFIDENTIAL

● セキュリティ対策導入に向けた優先度について

中小企業にとって、**取引先企業との契約継続に影響**を及ぼすような**サイバーセキュリティ対策**導入の**優先度が高い。**

＜今後導入を検討しているサイバーセキュリティ対策＞

1. **出入口対策** **21社**
2. **社員教育** **18社**
3. **セキュリティポリシー策定・重要なファイルのバックアップ** **11社**

＜過去に取引先企業から義務付けられた対策＞

1. ウイルス対策ソフト 25社
2. **社員教育・重要なファイルのバックアップ**・セキュリティ管理者の設置 **5社**
3. **出入口対策・セキュリティポリシー策定** **4社**

17

2. 出入口対策（UTM）設置結果

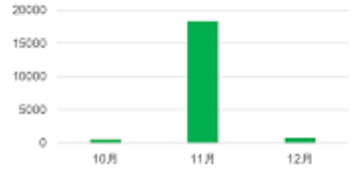
N=134ユーザ

①不正プログラム検知は76件、②不正侵入防止(IPS)は19,650件

①不正プログラム検知

・総検知数　76件
・検知企業数　14ユーザ

②不正侵入防止（IPS）



・総検知数　19,650件
・検知企業数　107ユーザ

18

2. 出入口対策（UTM）設置結果

①「不正プログラム／スパイウェア」

結果

・検知件数：10月⇒0件、11月⇒50件、12月⇒26件
・「load-scripts.php」を合計34件検出
⇒Java/CSSで大量Load読み込みをさせるDoS攻撃、ブラウザが応答しなくなる、OSハングする等の被害あり
・「COMPANY PROFILE.doc」を合計10件検出
⇒悪意のあるマクロを利用する、Microsoft Office用の特異なローダー（不正プログラム読み込み）

考察

・危険なサイト（広告含む）に誘導され、攻撃スクリプトをLoadさせられている
・英語圏の人が開きたくなる英語タイトルのファイルを添付したメールが検知されている（英語ファイルの他、漢字ファイルも検知あり）

19

2. 出入口対策（UTM）設置結果

②「不正侵入防止（IPS）」

結果

・検知件数：10月⇒539件、11月⇒18,328件、12月⇒783件
・検出した主なルール
・INVALID HTTP VERSION ⇒ HTTPバージョンが異なる要求で脆弱性を攻撃
・OpenSSL ChaCha20-Poly1305 ⇒ OpenSSLの暗号化の脆弱性を攻撃
・MS Windows SMB Server Buffer Overflow ⇒ SMBサーバの脆弱性攻撃
・MS DNS Server NAPTR Record Sign Extension Memory Corruption (CVE-2011-1966)
・WEB Linux /etc/shadow File Download:CVE-2002

考察

・Webサーバが主な攻撃対象
・2002年の古い脆弱性攻撃から2020年の新しい脆弱性攻撃まで無作為に実施
・MSサーバ、Linux、Openソースなど主要ソフトへ網羅的に攻撃
⇒これらの攻撃で「穴」を見つけられると、ヒントを与え、標的攻撃を受けることになる

20

2. 出入口対策（UTM）設置結果

NTT EAST CONFIDENTIAL

②「不正侵入防止（IPS）」

（参考）JVN iPediaで注目されている脆弱性（期間：2021/1/10 - 1/16）

1. JVNDB-2021-000003
   「**SKYSEA Client View** のインストーラにおける DLL 読み込みに関する脆弱性」

2. JVNDB-2020-010390
   「**WordPress 用 WooCommerce** プラグインの NAB Transact エクステンションにおけるデータの整合性検証不備に関する脆弱性」

3. JVNDB-2020-010389
   「**DesignMasterEvents Conference Management** における SQLインジェクションの脆弱性」

⇒ **お使いのソフトに危険な脆弱性が残っていないか確認しましょう。**

21

2. 出入口対策（UTM）設置結果

NTT EAST CONFIDENTIAL

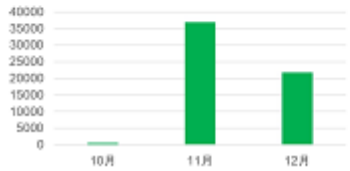
N=134ユーザ

③不正サイトアクセスブロックは710件、④スパムメール検知は59,182件

③不正サイトアクセスブロック

- ・総検知数　**710件**
- ・検知企業数　**45ユーザ**

④スパムメール検知



- ・総検知数　**59,182件**
- ・検知企業数　**92ユーザ**

22

2. 出入口対策（UTM）設置結果

NTT EAST CONFIDENTIAL

③「不正サイト」

結果

- 検知件数：10月⇒18件、11月⇒441件、12月⇒251件
- 検出された主なサイト
  - m.hcloset.com ⇒ 韓国系の安い洋服の詐欺サイトという評判
  - www.masksjp.xyz ⇒ 中国福建省サーバを使った安いパソコンの詐欺サイト
  - survey-smiles.com ⇒ マルウェアが誘導するサイト（危ない兆候）

考察

- 詐欺サイトはショッピング決済前に人が評判を確認して注意することで防げる
- 知らない間にアクセス履歴があるような場合、マルウェアに誘導されている可能性もあり

※（参考）日本サイバー犯罪対策センターより
2021年 1月 8日　総務省を騙った**特別定額給付金に関するフィッシング**についての注意
2020年12月22日　広告表示により誘導する**悪質なショッピングサイト**についての注意
2020年12月 3日　様々な**金融機関等を狙ったフィッシング**についての注意

23

2. 出入口対策（UTM）設置結果

NTT EAST CONFIDENTIAL

④「スパムメール」

結果

・検知件数：10月⇒516件、11月⇒36,903件、12月⇒21,763件

考察

・件数としては全項目の中で一番多いが、クリックしなければさほどリスクは高くない
⇒ただし、時間とITリソースをロスする

・一度届いたら継続的にも送られてしまうため「フィルタ」で対処するしかないやっかいもの

・不注意のPC操作ミスで誘導される恐れもあり、「一人ひとりの意識」で守るしかない

24

2. 出入口対策（UTM）設置結果

NTT EAST CONFIDENTIAL

N=134ユーザ

⑤ランサムウェア検知は223件、⑥C&Cコールバック検知は609件

⑤ランサムウェア検知

・総検知数　223件
・検知企業数　6ユーザ

⑥C&Cコールバック検知

・総検知数　609件
・検知企業数　1ユーザ

25

2. 出入口対策（UTM）設置結果

NTT EAST CONFIDENTIAL

⑤「ランサムウェア」

結果

・検知件数：10月⇒6件、11月⇒67件、12月⇒150件

考察

・JPCERT/CC によると、10月以降おさまっていたが12月21日にEmotetの感染に繋がる多くのメール配布が確認されたというのが国内の全体状況

・Emotet、IcedID、Zloaderなど国内で確認されているマルウェアの感染経路はメールの添付とLINKが原因（メールへのケアが重要）

・Emotet が Trickbot や Qbot といった他のマルウェアをダウンロードし、それを足掛かりに更なる攻撃が行われることもあり、被害が見つかった場合早期対処が必要

26

2. 出入口対策（UTM）設置結果

NTT EAST CONFIDENTIAL

⑥「C&Cコールバック」

結果

・検知件数：10月⇒0件、11月⇒609件、12月⇒0件

考察

すでに感染している状態に近いので早期ケア推奨（ウイルススキャン、PC設定再点検等）
⇒C＆C接続をする不正アプリがあるか、レジストリ等の設定を変えられHttp自動接続する状態になっている恐れがある

27

2. 出入口対策

NTT EAST CONFIDENTIAL

- ✓ 不正侵入（IPS）は実証参加企業の**約80%**、スパムメールは実証参加企業の**約69%**で検知され、多くの企業で**身近にサイバーセキュリティ脅威が潜んでいる**状況
- ✓ ランサムウェアを実証期間内で**129件**検知した参加ユーザもおり、**集中的にサイバー攻撃を受けている企業も存在**
- ✓ 上記のセキュリティ脅威を防ぐために、基本的なセキュリティ対策として**出入口対策が必要**

28

NTT EAST CONFIDENTIAL

3. まとめ

3. まとめ

NTT EAST CONFIDENTIAL

✓実証の結果、ランサムウェア等**多くの脅威を検出**
✓メール訓練においても、**全体の2割程度**の企業様が開封・クリック
✓実証により**「意識が向上」**とほとんどの企業様が事後アンケートで回答されており、当初の目的の一つである**「意識の向上・育成」は達成**
✓一方で、今後の対策に投じる費用感として殆どが「1万円以下」となっており、**セキュリティ対策における費用対効果の高いサービス提供**が事業者に求められている

30

3. まとめ（参考）

NTT EAST CONFIDENTIAL

参考：企業におけるサイバーセキュリティ対策費の考え方

IT化による想定利益＞IT化投資額（IT導入、運用、セキュリティ対策費）
セキュリティ侵害による想定被害額（経済的損失、社会的信用）＞セキュリティ対策費
セキュリティ侵害発生時に支出可能な対策費＞残留リスクによる想定被害額

参考：サイバーセキュリティ対策の具体的項目

分類	具体的な項目の例
人的対策	・セキュリティポリシーの策定 ・各種社内規定、マニュアルの整備 ・社員教育・訓練 ・アクセス管理
組織的対策	・管理組織の設置・運用 ・情報資産の分類・持ち出し管理 ・サイバー攻撃対応マニュアルの整備 ・事業継続管理
物理的対策	・コンピュータの情報資産の保護 ・重要情報の一元管理、入退室管理 ・アクセスできる区域の制限 ・クリアデスク、クリアスクリーン
技術的対策	・本人認証・アクセス制御、権限管理 ・ウイルス対策 ・脆弱性対策 ・暗号技術や認証技術の利用 ・ファイアーウォールやコンテンツフィルターの設定

自社の対策を棚卸し脅威を把握、費用対効果を検証しながら対策を講じる必要

31

NTT EAST CONFIDENTIAL

セキュリティ脅威は、
今この瞬間にも迫っています。
また、被害者だけではなく、
加害者になりえることもあります。
セキュリティ対策にご不安があれば、
NTT東日本や専門の事業者様に、
一日でも早くご相談ください。

32


NTT EAST CONFIDENTIAL
本件に関するお問い合わせは下記までお気軽にご連絡ください
【お問い合わせ先】
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：住本、井村
Mail：ntt_hkd-cyber-ml@east.ntt.co.jp
33

2．サイバーセキュリティ対策実証モデル構築

中小企業の経営体力に見合った予算規模でセキュリティ対策を実現するための実証を道内中小企業の協力を得て実施した。また、その結果を整理したうえで、広く周知するためのセミナーを開催した。

なお、実証については、東日本電信電話（株）に委託して実施した。

（1）実証事業の概要

●実施時期：令和３年１１月～令和４年３月

●実施対象：道内中小企業、製造業・非製造業各４社（計８社）

●内容：

・対象の企業にセキュリティ対策機器（UTM）を設置、ログを管理することにより、サイバー攻撃の有無や内容をチェックし、サイバー攻撃の状況を把握した。

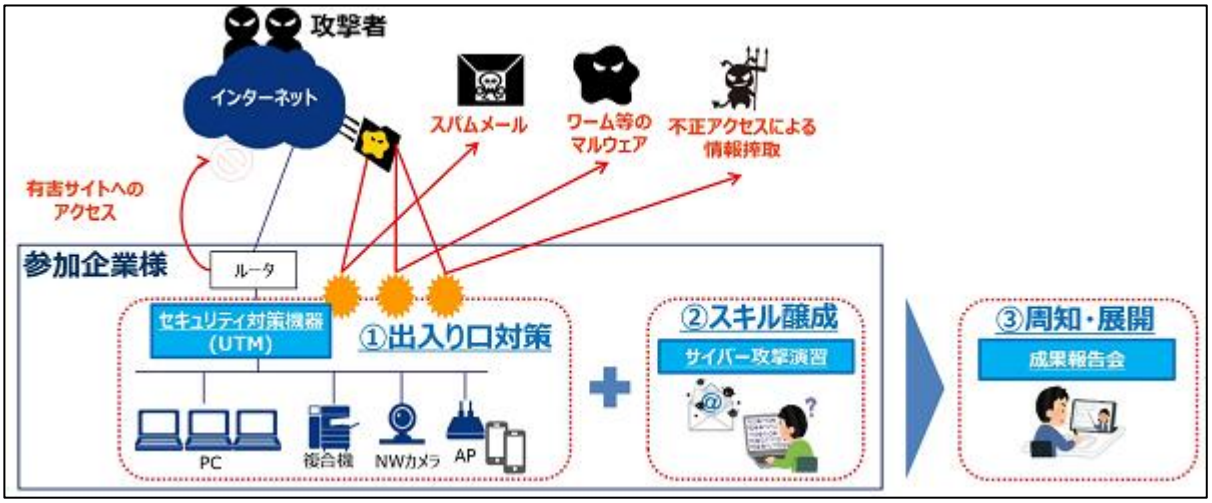
・サイバー攻撃に対する事前の準備、実際に攻撃を受けた場合の対応、事後の復旧等についてシミュレーションを実施するなどのサイバー攻撃演習を行うことを通じ、中小企業のサイバーセキュリティ対策に対する知識や対処スキルの習熟を図った。

・実証の結果をオンラインセミナーで道内の中小企業等へ周知することにより、サイバーセキュリティ対策の意識の向上や普及啓発を図った。

＜実施スケジュール＞

＜参加企業の属性（業種別・従業員数別）＞

＜実施イメージ＞



（2）サイバー攻撃の状況

実証を行った 8 社のレポートを抽出し分析した結果を下表にまとめた。8 社のうち 7 社に対してサイバー攻撃の可能性が疑われる可能性を確認した。また、製造業の企業に対しては、無差別的・集中的なサイバー攻撃も確認された。

＜表：サイバー攻撃の状況＞

		最大接続端末数※	設置期間	対策機能			
				不正プログラム対策	不正侵入検知（IPS）	不正サイトアクセスブロック	スパムメール対策
製造業	A社	53台	11月上旬～3月上旬	○(3件)	○(41件)	-	○(525件)
	B社	62台	11月下旬～3月上旬	-	○(10件)	○(18件)	○(440件)
	C社	215台	1月下旬～3月上旬	○(4件)	○(127件)	○(42件)	○(1030件)
	D社	65台	2月上旬～3月上旬	-	-	-	○(172件)
非製造業	E社	39台	1月下旬～3月上旬	-	○(1件)	-	○(296件)
	F社	7台	2月上旬～3月上旬	-	-	-	-
	G社	87台	2月中旬～3月上旬	-	-	○(76件)	-
	H社	18台	2月中旬～3月上旬	-	○(4件)	-	○(109件)

※PCの他にタブレットやスマートフォン等のデバイスも含む端末数

以下、サイバー攻撃の種類別に、想定されるリスクと、実証事業での検出数と内容について説明する。

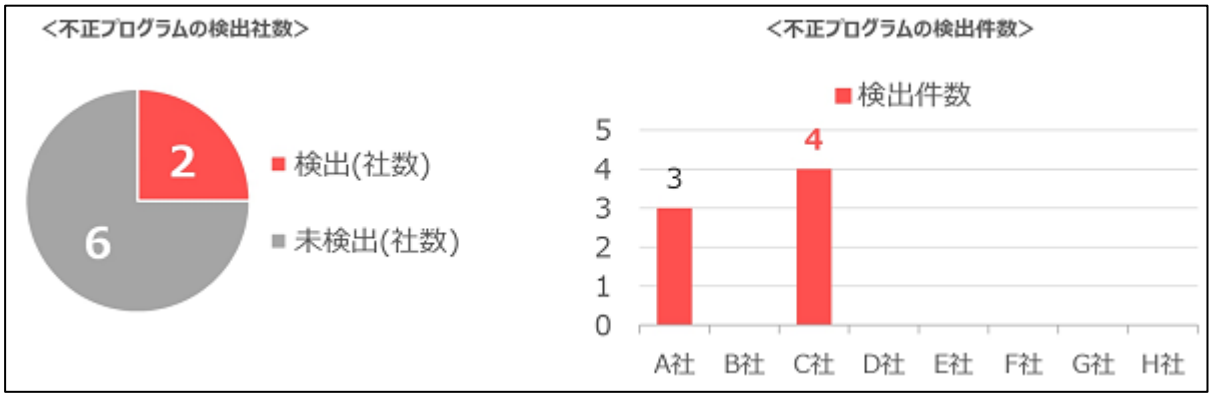
①不正プログラム

不正プログラムとは、ウイルスやスパイウェアなど、コンピュータにとって有害な働きを

するプログラムである。代表的な不正プログラムとしては、「ワーム」「ウイルス」「トロイの木馬」などがある。

■想定されるリスク
・パソコン内のデータを破壊される。
・他のサイバー攻撃の攻撃元として踏み台にされる（＝加害者にされる）。

■実証事業における検出数
・対象 8 社のうち、2 社で検出された。
・検出された 2 社の 1 ヵ月あたりの平均検出数は約 1.7 件／社であり、これは東日本管内の平均検出数（0.4 件／社）を上回っている。



■検出された不正プログラムの例
・実証事業で確認された不正プログラムの例は、以下のとおりである。

○Possible_Powload-VBS35
不正なファイルをダウンロードして実行するマクロ型不正プログラム。

○TROJ_FRS.0NA103C222
システム設定の変更、任意のファイルのダウンロードと実行及び情報収集といった不正活動を展開するトロイの木馬。

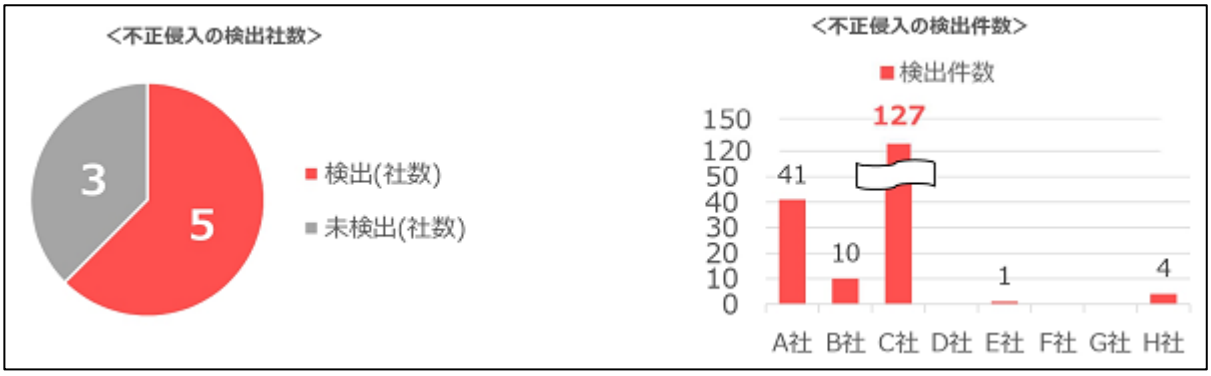
○Trojan.XF.EMOTET.YXCBY
端末やブラウザに保存されたパスワード等の認証情報及びメール本文、アドレス帳の情報を搾取しようとする Emotet ウイルス。全世界的に流行中。

②不正侵入

不正侵入とは、システムやネットワークに対する不正な通信である。アプリや OS の脆弱性を狙った通信攻撃であり、外部からの不正通信や、内部の機密情報を外部へ持ち出そうとする通信がある。

■想定されるリスク
・機密情報を盗まれ、売買される。
・アカウントを乗っ取られ、他社への詐欺行為に使用される。

■実証事業における検出数
・対象 8 社のうち、5 社で検出された。
・検出された 5 社の 1 ヵ月あたりの平均検出数は約 20.9 件／社であり、これは東日本管内の平均検出数（35 件／社）の 3 分の 2 程度である。



■検出された不正侵入の例
・実証事業で確認された不正侵入は、2007 年に発見されている古い脆弱性に対する攻撃から、2021 年に発見された新しい脆弱性に対する攻撃まで、無作為に実施されている。
・Microsoft Office、サーバ、ルータなど、主要な端末やソフトウェアへ網羅的に攻撃されている。
・具体的には、以下のとおりである。

＜脆弱性を狙った不正な通信＞
○WEB Dasan GPON Routers Command Injection -1.1 (CVE-2018-10561)
○FILE Microsoft Excel rtWindow1 Record Hardling Code Execution -1 (CVE-2007-3029)
○WEB Apache HTTP Server Path traversal (CVE-2021-41773)
　いずれも、端末機器やサーバ、ソフトウェア等の脆弱性を狙い不正アクセスするような攻撃と見られる通信。

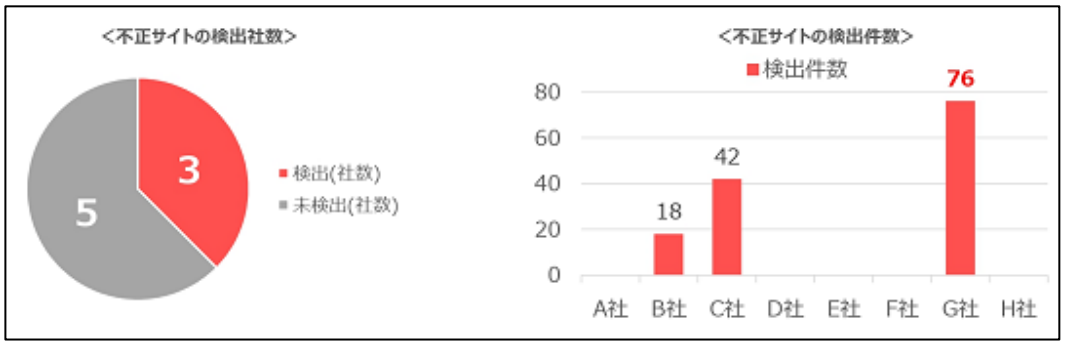
＜その他の不正な通信＞
○Bad TCP Flag
　不正な TCP パケット（通信用として利用されるデータ）を外部から送付し、そのリアクションから機器への進入経路を探索している可能性がある通信。

③不正サイトへのアクセス
不正サイトとは、本物そっくりに偽造されたフィッシングサイトや、不正に改ざんされて

しまっているウェブサイトである。偽のウェブサイトにアクセスさせて情報を入力させることによって、ID やパスワードなどの情報を不正に入手することが目的である。

■想定されるリスク
・フィッシングサイトへのアクセスによる情報流出。
・改ざんサイトへのアクセスによるマルウェア感染。

■実証事業における不正サイトへのアクセス数
・対象 8 社のうち、3 社でアクセスが確認された。
・検出された 3 社の 1 ヵ月あたりの平均アクセス数は約 62 件／社であり、これは東日本管内の平均（35 件／社）を大幅に上回っている。特に G 社では 76 件と突出して多い。

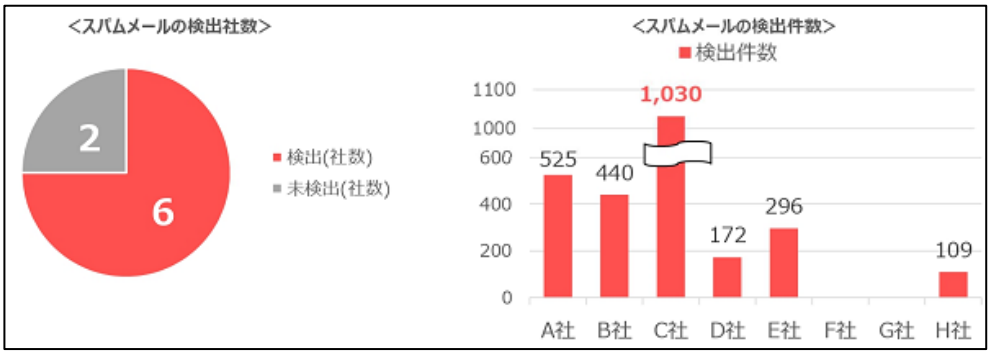


④スパムメール

スパムメールとは、一方的に送信される迷惑メールである。偽の URL や不審な添付ファイルなどが送信される場合が多い。

■想定されるリスク
・不正なリンクへのアクセスによる情報流出。
・添付ファイルの開封によるマルウェアへの感染。

■実証事業における検出数
・対象 8 社のうち、6 社で検出された。
・検出された 6 社の 1 ヵ月あたりの平均検出数は約 258.7 件／社であり、これは東日本管内の平均検出数（156 件／社）を大幅に上回っている。特に C 社で突出して多い。



■受信されたスパムメールの例

・実証事業で受信されたスパムメールでは、実在する企業の名を騙っているものが多いが、それらは送信元アドレスを確認することによって不審なメールであると判断することが可能である。

・特に受信が多かった部署・担当は、製造業では「購買担当」、非製造業では「総務担当」であった。前者は、資材調達のためにオンラインショッピング等の利用が多いため、また、後者は、メールマガジン等の購読が多いため、メールアドレスが流出していることが想定される。

・具体的な例は、以下のとおりである。

メールの件名	メールの送信者
【某メガバンク】から緊急のご連絡	****@pdkrlfz.cn
【某外資系ネットショッピングサイト】の情報更新をお願いしております。	****@zh.com
【某鉄道会社】アカウントの自動退会処理について	****@lgangdan589.cn

実在する企業名を用いたメールの件名

アドレスのドメイン以降が企業と無関係のもの

以上を総括すると、不正な通信は実証参加企業の約 63%、スパムメールは約 75%で検知されており、多くの企業に対して、システムや機器の脆弱性を突いたサイバー攻撃の脅威が潜んでいる状況であるといえる。

また、Emotet などの不正プログラムを検知した参加企業もあった。集中的にサイバー攻撃を受けていると思われる企業もみられた。

これらのセキュリティ脅威を防ぐためには、基本的なセキュリティ対策として、出入口対策、エンドポイントセキュリティ（ネットワークに接続されている末端の機器＝PC・スマートフォン・タブレットなどの端末機器＝や、それらに保存している情報を、サイバー攻撃から守るためのセキュリティ対策）に加え、従業員に対するセキュリティ意識の醸成が求められる。

（3）サイバー攻撃発生時の対応

①サイバー攻撃の特徴

サイバー攻撃の発生時には、攻撃者・企業・顧客それぞれでさまざまな事象が発生する。その際、企業側が把握できる情報は少ないため、企業は少ない情報を元にその状況に応じた的確な判断を行うことが必要となる。

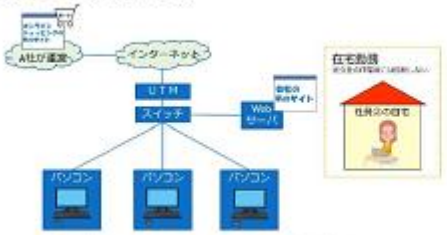
<サイバー攻撃発生時の事象イメージ>

時系列	実際の事象	企業で把握可能な発生事象	企業の対応
07:21	✓ Webサイトが改ざん		
09:13	✓ Webサイトを見たお客様がウイルスに感染		
10:31	✓ Webサイトを見た社員がウイルスに感染 ✓ ウイルス対策ソフトがウイルス検出	✓ Webサイトを見た社員がウイルスに感染 ✓ ウイルス対策ソフトがウイルス検出	**感染経路特定→ウイルス拡散防止**
10:47			✓ 社員に連絡 - 端末をNWから切断 - 感染経路を確認
11:51	✓ お客様よりクレーム ✓ SNSで拡散	✓ お客様よりクレーム	**お客様影響確認→広報対応決定**
12:10			✓ Webサーバを停止
12:21			✓ ベンダへウイルス調査依頼
13:40	✓ 社員がSNSの書き込みを発見	✓ 社員がSNSの書き込みを発見	**ベンダ調査→システム復旧**
以降	✓ 新聞に掲載	✓ 新聞に掲載	✓ 端末・Webサーバ復旧 ✓ お客様対応

②サイバー攻撃演習によるセキュリティ対策実証の概要

サイバー攻撃を受けた場合は、被害拡大の防止からシステムの復旧、その後の社外対応までを迅速に行い、影響を極小化する必要がある。本事業では、参加企業に対するサイバー攻撃のテストを行う演習を実施し、インシデント発生時の企業の行動の傾向をみた。

<サイバー攻撃演習のイメージ>



仮想の企業でサイバー攻撃が発生

経営者としてインシデントに対するアクションを選択

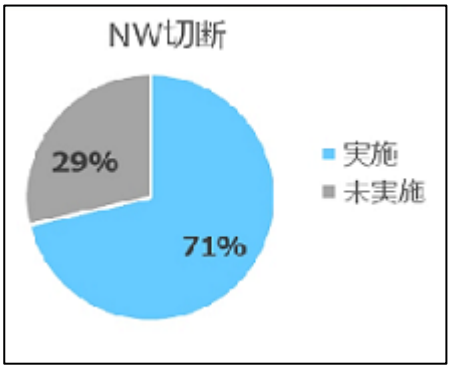
③インシデント発生時における初期対応

サイバー攻撃を受けてインシデントが発生した際の初期対応として、参加企業における以下 3 項目の実施状況を調査した。

■ネットワークの切断（被害拡大防止のため）

パソコンがウイルス等に感染したと疑われる場合は、当該端末を速やかにネットワークから切り離し、被害拡大を防止することが重要である。

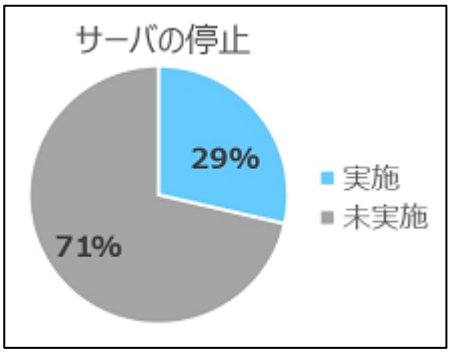
演習では、参加企業の 71%が初期対応でネットワークの切断を実施した。



■サーバの停止（被害拡大防止のため）

自社のウェブページが攻撃を受けている場合、閲覧した顧客等にも被害が及ぶ可能性があるため、ウェブサーバの停止を速やかに行うことが必要である。

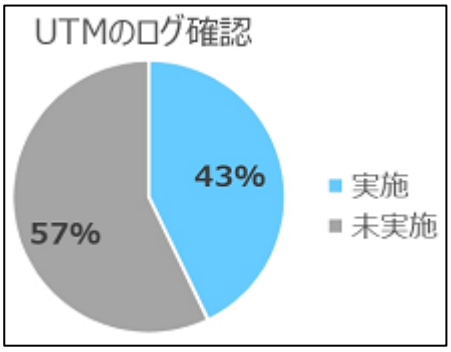
演習では、参加企業の 29%が初期対応でサーバの停止を実施した。



■UTM のログ確認（外部への影響確認のため）

サイバー攻撃の可能性が確認された場合、ウイルス等を取引先などに拡散していないかどうかを調査することが重要であり、その際には UTM のログを確認することが有効である。

演習では、参加企業の 43%が初期対応でサーバの停止を実施した。



③復旧に向けた対応

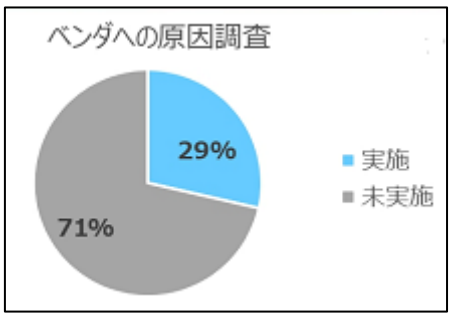
サイバー攻撃を受けてインシデントが発生した後の復旧に向けた対応として、参加企業に

おける以下 3 項目の実施状況を調査した。

■ベンダーへの調査依頼（原因調査のため）

ウイルス等の感染が疑われる場合は、ウイルス対策ソフト等のベンダーに対し原因調査を依頼することが重要である。それにより、新種のウイルスであっても、ワクチンソフト提供が早期に行われることに繋がる。

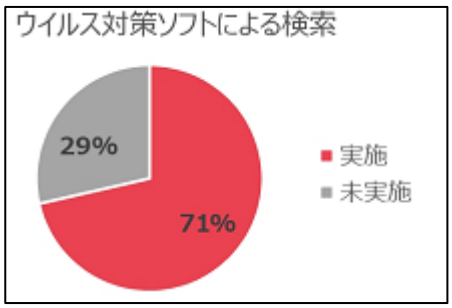
演習では、参加企業の 29%がベンダーへの調査依頼を実施した。



■ウイルス対策ソフトでの検索（原因調査の遅延を引き起こす）

ウイルス等の感染が疑われた際に、ウイルス対策ソフトで検索を行っても、ソフトのバージョンアップがされていない場合や、新種のウイルスに感染した場合は、検知ができない可能性がある。そのため、ウイルス対策ソフトでの検索を行うことは、その後の対応の遅延の原因となり得る。

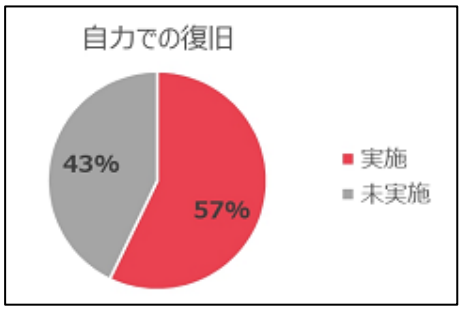
演習では、参加企業の 71%がウイルス対策ソフトの検索を実施したことで、その後の対応に遅延が生じた。



■自力での復旧（復旧の遅延を引き起こす）

サイバー攻撃に対しては、自力での復旧や原因調査はきわめて困難である。ベンダーやシステムエンジニア等の専門家への報告・相談が有効である。

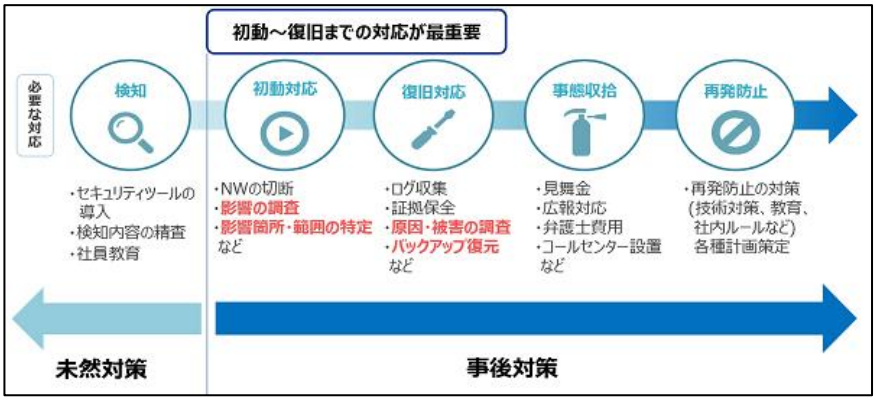
演習では、参加企業の 71%がインターネットでの類似事象検索等により自力での復旧を試みようとした。



以上の総括として、道内中小企業は、特に以下 2 点を強く意識すべきであるといえる。

・インシデント発生の可能性はゼロにはならないため、被害が生じた際の「事後対応」に関する事前の検討が重要である。

・被害防止拡大に向けた取組や社内の報告・相談体制など内部対応と、原因特定やログの調査など外部対応の両方について実施していくことが重要である。



（4）実証事業のまとめ

サイバー攻撃は、量・種類ともに世界的に増加傾向にあるが、本実証事業を通じて、道内の中小企業に対しても数多くのサイバー攻撃が行われていることが確認された。

今後も、テレワークの拡大や、さまざまな業務の DX 化の進展により、サイバー攻撃の経路が増加し、その結果、サイバー攻撃はさらに増加していくことが予想される。基本的なセキュリティ対策を怠ることなく実施していくことに加え、必要な対策について常にアップデートしていくことが必要である。

（5）オンラインセミナーの開催

実証結果を中小企業者等に周知することを目的に、オンラインセミナーを実施した。

なお、本セミナーは、本事業の目的が「DX の推進とともに車の両輪の役割を果たすことが期待される『DX with Cybersecurity』の実現に必要なモデルケースを構築することによって、道内経済の持続発展可能な競争力強化に繋げていく」ことであることを勘案し、北海道経済産業局「令和 3 年度地域経済産業活性化対策調査（地域・産業の DX 化促進に向けたエコシステムの創出）」の成果報告会と合わせて実施した。

【開催概要】

●名　称：中小企業に求められるデジタル化への対応セミナー
●日　時：2022 年 3 月 24 日（木）13 時 30 分～16 時 30 分
●形　式：YouTube Live によるオンライン配信
●主　催：経済産業省北海道経済産業局
●運　営：㈱道銀地域総合研究所

【プログラム】

＜DX 関連報告＞

１．報告

道内の DX 取組実態と今後必要な支援体制

講師：㈱道銀地域総合研究所　主任研究員　春日 智章

２．ケーススタディ

道内企業の DX 取組事例

・流通取引のデジタル化による受注処理業務省力化から製品管理への挑戦
㈱イークラフトマン
・「生産計画に自動化が目標」製造現場の生産性向上を図る業務改善システム導入
㈱ビックボイス
・AI による介護現場の安全性向上を図る見える化サービス
㈱サンクレエ

＜セキュリティ関連報告＞

３．道内中小企業のサイバーセキュリティリスク
講師：ＮＴＴ東日本　北海道事業部　マーケティンググループ　井村　洋介　氏

４．サプライチェーンでのセキュリティ対策
講師：ＮＴＴ東日本　北海道事業部　テクニカルソリューショングループ
内藤　裕貴　氏

＜その他＞

５．北海道経済産業局からの情報提供

●セキュリティ関連報告内容（要旨）

＜道内中小企業のサイバーセキュリティリスク＞
（講師：ＮＴＴ東日本　北海道事業部　マーケティンググループ　井村　洋介　氏）

・ 現実的なコストで効果的なセキュリティ対策を行うためのモデル事業を実施した。内容は、①セキュリティ対策機器（UTM）の設置によるサイバー攻撃の状況把握、②サイバー攻撃演習によるサイバーセキュリティ対策に関する知識や対処スキル習熟、③成果発表によるサイバーセキュリティ対策の意識向上・普及啓発。
・ 道内の 8 社に対して実証モデルを導入。そのうち 7 社に対してサイバー攻撃が疑われる通信が確認された。多くの企業に対して、システムや機器の脆弱性を突いたサイバー攻撃の脅威が潜んでいる状況であるといえる。
・ サイバー攻撃発生時に、攻撃を受けた企業が把握できる情報は少ない。このため、企業は少ない情報で適切な判断を行う必要がある。その観点から上記の 8 社についてサイバー攻撃演習を実施したところ、初期対応、復旧対応とも、必ずしも適切な対応が行われたとはいえなかった。被害が生じた際の事後対策について、日頃から準備をしておくことが必要である。

＜サプライチェーンでのセキュリティ対策＞
（講師：ＮＴＴ東日本　北海道事業部　テクニカルソリューショングループ
内藤　裕貴　氏）

・ 今月、トヨタ自動車の主要取引先がサイバー攻撃を受けて、トヨタが生産ラインを止めるに至ったとの報道があった。このように、中小企業をターゲットとした「サプライチェーン攻撃」は全世界的に流行している。大企業を狙うのではなく、比較的対策が手薄でセキュリティレベルの低い関連企業が狙われている。

- IPA が発表する「情報セキュリティ 10 大脅威　2022」において、「サプライチェーンの弱点を悪用した攻撃」は 3 位に位置づけられた。この項目は、2021 年には 10 大脅威に入っておらず、最近になって急増したことがわかる。
- サイバー攻撃を受けると、攻撃による業務の停止に加え、取引先の情報が漏洩するなど、信用の低下も発生し、大きなダメージを受ける。
- トヨタの事例では、取引先企業がサイバー攻撃を受けたことにより、トヨタ国内 14 工場のすべてで生産がストップした。無差別攻撃によるランサムウェアの被害を受けた可能性が高く、他の企業でも同様の被害が生じるリスクがある。
- また、2014 年には、通信教育大手企業で、再委託先の派遣社員が盗んだ個人情報 2900 万件を名簿業者に売却した内部不正があった。これにより当該企業は特別損失 260 億円、会員数 40%減、株価 30%下落等のダメージを受けた。
- サイバーセキュリティ対策は、ウイルス対策ソフトだけでは不十分。ファイアウォールや UTM の設置などの「技術的対策」、防犯対策や入退室管理などの「物理的対策」、規程や手順書等ルールの整備や社員教育などの「人的対策」を実施し、多層的に防御していくことが必要。ネットワークに関する技術的なセキュリティ対策で十分だと思われがちだが、社員教育も非常に重要な要素である。

●会場写真

講師：井村　洋介　氏

講師：内藤　裕貴　氏

Ⅳ サイバーセキュリティ人材育成に向けたコミュニティ体制の検討等

道内におけるセキュリティ人材の確保・育成を進めていくには、持続的なセキュリティコミュニティが形成されることが求められる。そのためには、現在の活動の中心を担っているHAISL 等について、公的機関が支えるだけでなく、より多くの民間企業がそこに参画し、セキュリティコミュニティと産業界との結びつきを強めていくことが必要である。

そこで、従来 HAISL 等に積極的に関与してきた各機関と、民間企業等の間で意見交換を行う場を設定し、今後の道内におけるセキュリティコミュニティのあり方や方向性などについて、意見交換を実施、現在は公的機関主導で進められているセキュリティコミュニティの活動について、民間企業を主体とした自立的な運営としていくこと等を検討した。

また、道内の学生等を対象にセキュリティ人材の育成を行っている Security College for Youth（SC4Y）と連携し、サイバーセキュリティ人材育成支援を行った。

1. 意見交換の実施

(1)第 1 回意見交換会

●日　時：2022 年 2 月 15 日（火）16:00～17:00
●形　式：オンライン会議（Microsoft Teams）
●内　容：
　１．開　会
　２．説　明
　　①意見交換会の開催について
　　②今後における HAISL の活動について（案）
　３．意見交換
　４．閉　会
●配付資料：
　　資料１　サイバーセキュリティコミュニティ強化に向けた意見交換の実施について
　　資料２　HAISL の今後の方向性（案）
　　資料３　他地域のセキュリティコミュニティ
　　資料４　中小企業のサイバーセキュリティ意識に関する調査 結果概要

●出席者
【HAISL 役員】
　会　長　髙井　昌彰　北海道大学情報基盤センター 情報ネットワーク研究部門 教授
　副会長　三谷　公美　北海道情報セキュリティ勉強会　副代表
　　河瀬　恭弘　一般社団法人北海道 IT 推進協会　副会長
　　岡崎　一智　一般社団法人テレコムサービス協会　北海道支部長

【HASIL 事務局】

澤口　洋一郎　総務省北海道総合通信局　サイバーセキュリティ室　室長
佐々木　　励　総務省北海道総合通信局　サイバーセキュリティ室　室長補佐
鯰江　　和弘　総務省北海道総合通信局　サイバーセキュリティ室　主査
高橋　佳奈美　総務省北海道総合通信局　サイバーセキュリティ室
高橋　　孝佳　北海道警察　サイバーセキュリティ対策本部　管理官
坂野　　雅樹　北海道警察　サイバーセキュリティ対策本部　対策班長
小林　　昌平　北海道警察　サイバーセキュリティ対策本部　対策係長
小塚　　隆　経済産業省北海道経済産業局　地域経済部　製造・情報産業課長
石川　　幸司　経済産業省北海道経済産業局　地域経済部　製造・情報産業課課長補佐
種田　　美穂　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
阿部　　辰彦　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
宮田　　悠　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

【受託事業者】

清水　　友康　(株)道銀地域総合研究所　執行役員地域戦略研究部長
大熊　　一精　(株)道銀地域総合研究所　地域戦略研究部　特別研究員
春日　　智章　(株)道銀地域総合研究所　地域戦略研究部　主任研究員

(2)第 2 回意見交換会

●日　時：2022 年 3 月 16 日（水）13:00～14:00
●形　式：オンライン会議（Microsoft Teams）
●内　容：
　１．開　会
　２．説　明
　３．意見交換
　４．閉　会
●配付資料：
　サイバーセキュリティコミュニティの強化に向けて

●出席者

【北海道経済団体連合会】

佐々木　聡一　産業振興グループ　部長
渡辺　　康之　産業振興グループ　部長

【HASIL 事務局】

佐々木　　励　総務省北海道総合通信局　サイバーセキュリティ室　室長補佐
鯰江　　和弘　総務省北海道総合通信局　サイバーセキュリティ室　主査

高橋　佳奈美　総務省北海道総合通信局　サイバーセキュリティ室
坂野　　雅樹　北海道警察　サイバーセキュリティ対策本部　対策班長
林　　克芳　北海道警察　サイバーセキュリティ対策本部　対策係長
小林　　昌平　北海道警察　サイバーセキュリティ対策本部　対策係長
石川　　幸司　経済産業省北海道経済産業局　地域経済部製造・情報産業課課長補佐
種田　　美穂　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
阿部　　辰彦　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
宮田　　悠　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
【受託事業者】
清水　　友康　　(株)道銀地域総合研究所　執行役員地域戦略研究部長
大熊　　一精　　(株)道銀地域総合研究所　地域戦略研究部　特別研究員
春日　　智章　　(株)道銀地域総合研究所　地域戦略研究部　主任研究員

Ⅴ　道外のセキュリティコミュニティとの連携強化支援

道外のセキュリティコミュニティの先進事例である NPO 情報セキュリティ研究所（和歌山県）と、今後の連携を視野に入れたうえで、オンラインで意見交換を実施した。

●意見交換概要

実施日：2021 年 11 月 9 日）

先方：NPO 情報セキュリティ研究所（和歌山県田辺市新庄町 3353-9）

代表理事　臼井　義美　氏

内容：運営資金、人員体制、行政との連携、事業概要など

Ⅵ 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。

(1)継続的なサイバーセキュリティ対策の必要性

アンケート調査からは、ウイルス対策ソフトはほぼ全ての企業で導入済みであり、アクセス権限の制御も約 5 割の企業で実行されていることがわかった。

一方、実証モデル構築事業に参加した企業の多くが、多くのサイバー攻撃を受けていることも確認された。基本的なサイバーセキュリティ対策を実行していくのみならず、今後ともサイバーセキュリティ対策のアップデートを続けていくことが重要である。

なお、直近では、ロシアのウクライナ侵攻を受けて世界中でサイバー攻撃の脅威が高まっており、日本企業が標的となって深刻な被害を受けるケースもみられる。大企業の主要取引先においてサイバー攻撃によるシステム障害が発生し、当該企業の生産が停止するといったサプライチェーンへの影響も起きている。こうした点からも、サイバーセキュリティ対策を継続的に実施することの重要性はさらに高まっているといえる。

（2）サイバーセキュリティ対策の理解への不足

アンケート調査からは、サイバーセキュリティの担当者（または担当部署）について、約 6 割の企業が配置できている反面、約 3 割の企業では必要と感じながらも配置できてないことが明らかになった。

また、自社のサイバーセキュリティ対策の現状について、「十分」または「やや十分」とする企業は 3 割に留まり、「不十分」「やや不十分」とする企業が約 3 割存在する。さらに、「どちらともいえない」とする企業も約 3 割に上っており、サイバーセキュリティ対策として何をすればよいのかが明確でない企業が少なくないこともうかがえる。

実証モデル構築事業に参加した企業に対する演習においても、サイバー攻撃を受けたときの初期対応としてサーバの停止や UTM のログ確認といった適切なアクションを起こすことのできた企業は半数以下にとどまっており、サイバーセキュリティ対策への理解は依然として不足していると考えられる。

（3）より一層の社員教育の必要性

アンケート調査からは、「サイバーセキュリティ対策を行う際の課題等」として、「人材がいない」との回答が約 5 割に上った。また、サイバーセキュリティ対策として「社員教育・研修の実施」を行っている企業は約 3 割にとどまっている。

実証モデル構築事業において検知された多くのセキュリティ脅威から企業を守るためにも、従業員に対するセキュリティ意識のより一層の醸成が求められる。

２. 今後の方向性

以上から考えられる中小企業のサイバーセキュリティ対策の今後の方向性について、以下に整理する。

（１）「DX with Cybersecurity」に向けた取組の展開

今後、道内の中小企業が成長を続けていくためには、業務のオンライン化やデジタル化など DX の推進が不可欠である。DX の推進によって外部との接点が増えていくことに伴い、サイバーセキュリティリスクの高まりも生じることとなる。大企業のサプライチェーンを構成する中小企業を標的としたサイバー攻撃も急増しており、中小企業にとって費用面等で現実的な範囲での対策を進めていくことが必要である。

（２）社内人材の育成とセキュリティベンダーの活用

サイバーセキュリティ対策を実施するにあたっては、UTM の設置などの「技術的対策」のみならず、セキュリティポリシーの策定や社内における人材教育が重要となる。昨今、サイバー攻撃の手口が巧妙化している状況をふまえ、外部からの脅威に直接さらされる機会が多いエンドポイントにおけるセキュリティ対策を進める必要がある。また、複雑かつ高度化が進むセキュリティの対策や不幸にもサイバー攻撃の被害に遭遇してしまった場合、被害の拡大防止や事業のュ　　画　　昨今、