News Release

経済産業省
北海道経済産業局

道内中小企業における
サイバーセキュリティ対策の現状

～求められる企業経営者の危機意識～

2021年1月26日

経済産業省

北海道経済産業局

【お問い合わせ先】

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　竹野、宮本、種田

TEL：011-700-2253

E-mail：hokkaido-seizojoho@meti.go.jp

はじめに

◆新型コロナウイルスの感染拡大に伴い、テレワーク等のデジタル化（DX）を進める企業が増加しており、企業規模を問わず、サイバー攻撃の高度化等に伴うリスク・被害も増大。

◆経済産業省では、昨年6月、昨今の産業を巡るサイバーセキュリティに係る現状の認識と、今後の取組の方向性について示した※1ほか、先月には、最近のサイバー攻撃の状況を踏まえ、企業経営者に対し、サイバーセキュリティの取組の一層の強化を促した※2ところ。

◆こうした中、道内では、当局・北海道総合通信局・北海道警察の3者が連携した「北海道地域情報セキュリティ連絡会（HAISL）」※3の活動を通じ、中小企業等のサイバーセキュリティに関するリテラシー向上に努めている。

◆全国的にもDXの進展とサイバーセキュリティ対策の重要性が叫ばれる中、今般、当局では、道内中小企業のサイバーリスクへの対応等について把握すると共に、今後の支援策等の検討に向け調査を実施したもの。

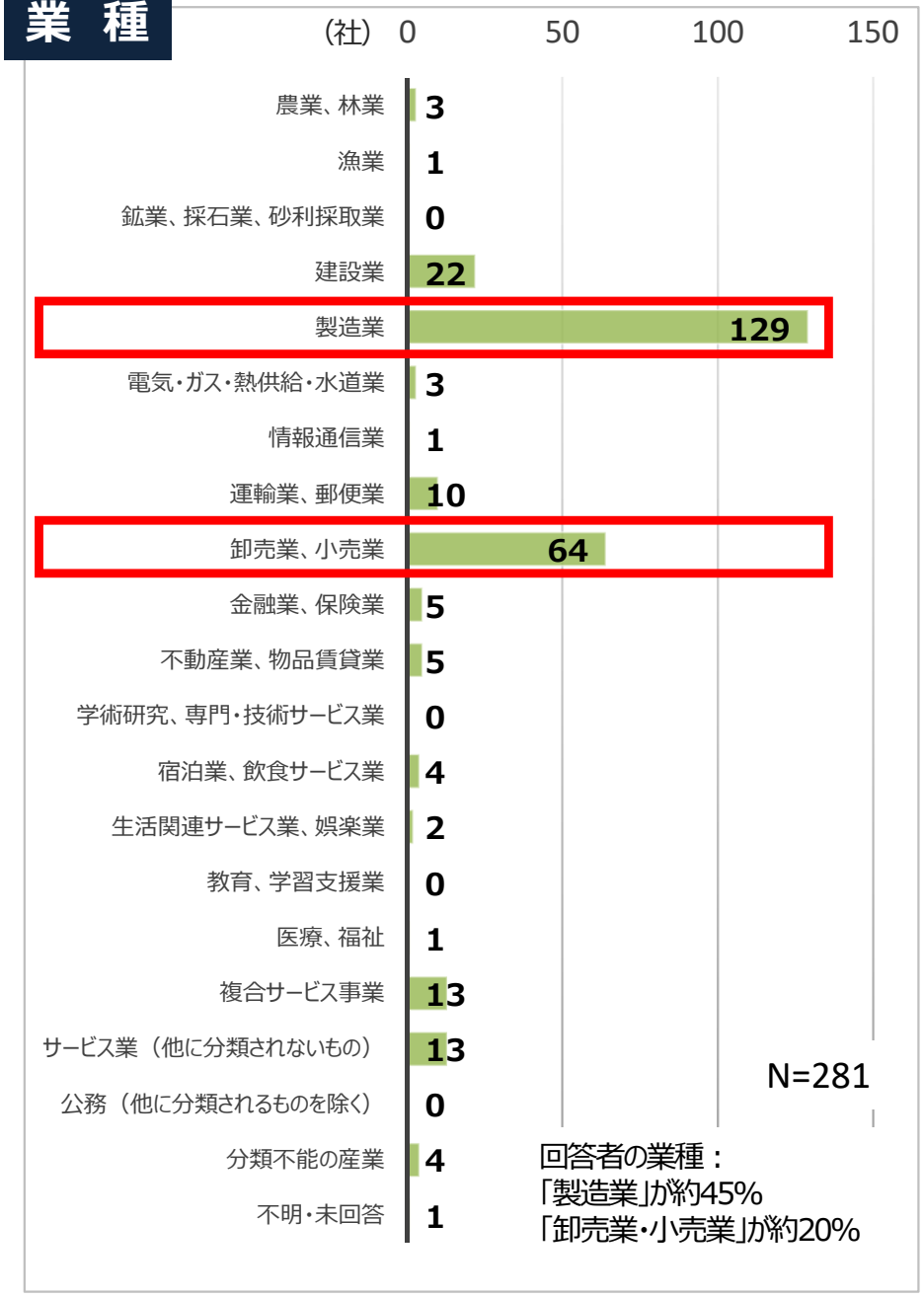
※1 経済産業省『昨今の産業を巡るサイバーセキュリティに係る状況の認識と、今後の取組の方向性について』（2020年6月12日）
https://www.meti.go.jp/press/2020/06/20200612004/20200612004.html
※2 経済産業省『最近のサイバー攻撃の状況を踏まえ、経営者の皆様へサイバーセキュリティの取組の強化に関する注意喚起』（2020年12月18日）
https://www.meti.go.jp/press/2020/12/20201218008/20201218008.html
※3 道内のサイバーセキュリティ推進機関として、当局、北海道総合通信局、北海道警察の3機関が2014年9月に共同で設置（会長：北海道大学　髙井昌彰　教授）
https://www.hkd.meti.go.jp/hokim/20140924/index.htm

アンケート調査概要

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
調査方法	郵送（調査票）およびインターネット調査（専用webサイト）
調査期間	2020年9月～10月
回答率	**281社 ／ 1,000社（28.1%）**
実施機関	(株)道銀地域総合研究所 ※令和2年度『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事業』（北海道経済産業局）
その他	本アンケートに係る最終とりまとめは3月（予定）

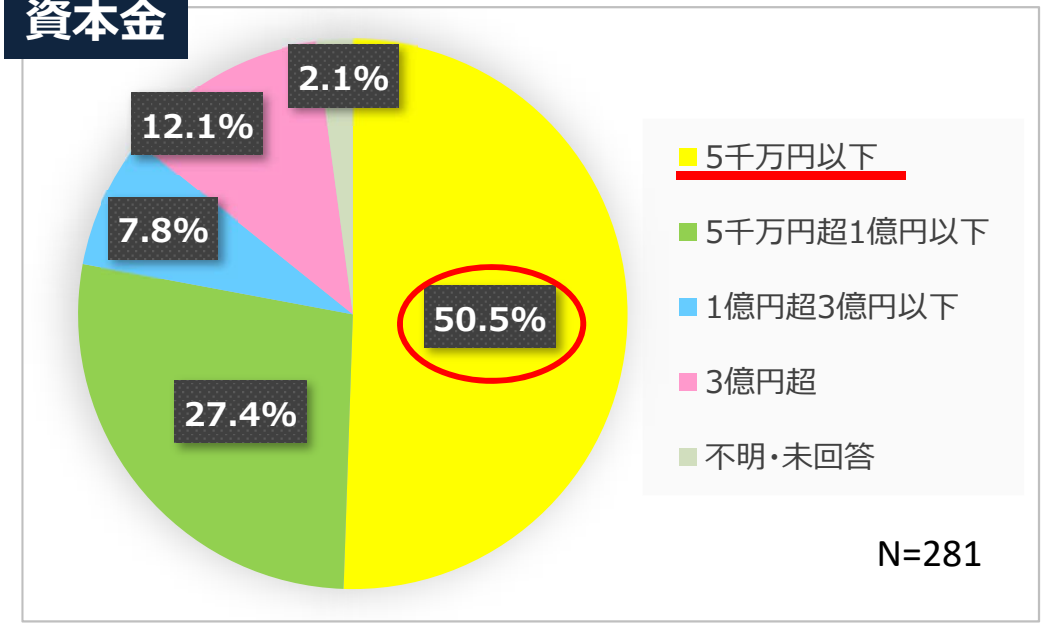
回答企業属性

業　種

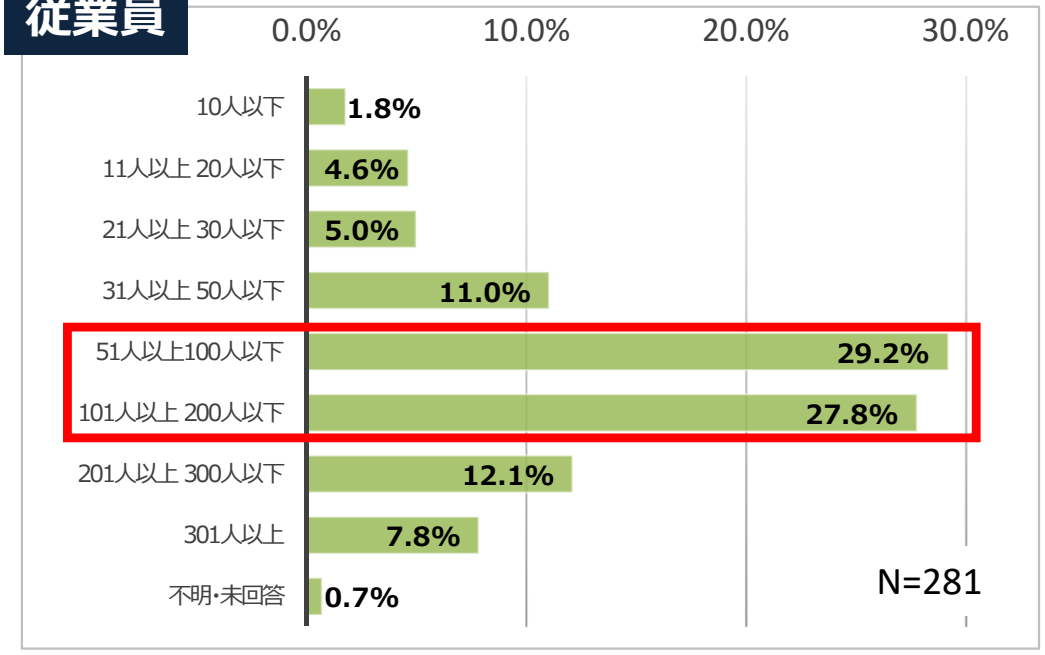


回答者の業種：
「製造業」が約45%
「卸売業・小売業」が約20%

資本金



従業員

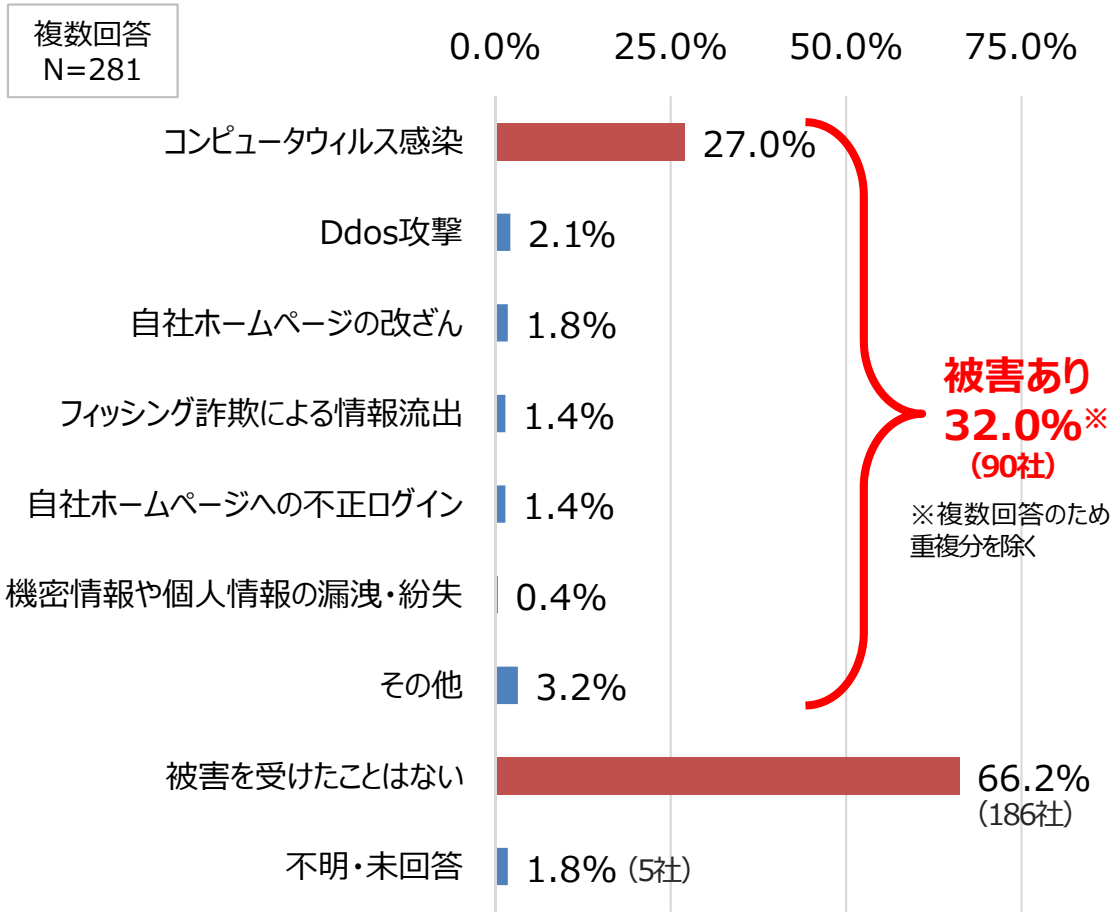


【出典】北海道経済産業局『中小企業のサイバーセキュリティ対策等に関する調査』（速報）

サイバー攻撃の被害状況

- **3割以上（32.0%）がサイバー攻撃の被害に遭っている**ことが判明。最も多い被害は「コンピュータウイルス感染」（27.0%）で、2020年全国的に被害が急増した"Emotet"の感染事例も見られた。
- 「被害を受けたことはない」（66.2%）と回答した企業についても、近年のサイバー攻撃の巧妙化等により、**攻撃を受けていることに気付いていない可能性※**が考えられる。

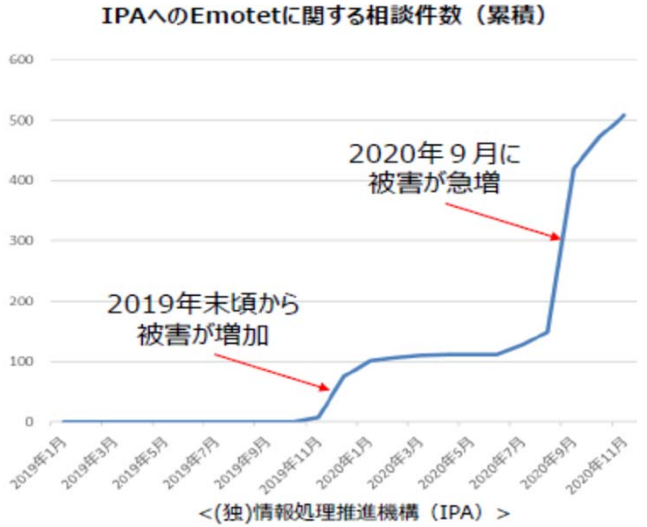
Q：貴社が受けたことのあるサイバーセキュリティ被害は？



【出典】北海道経済産業局『中小企業のサイバーセキュリティ対策等に関する調査』（速報）

Emotet（エモテット）とは

- 電子メールを媒介に感染するマルウェア。情報窃取等の直接攻撃や、他のウイルス等による攻撃の侵入口として悪用されるウイルスで、一度感染すると拡散していく傾向。2020年7月から国内外で感染メールの配信活動が活発化。



【出典】経済産業省『最近のサイバー攻撃の状況を踏まえた経営者への注意喚起』（2020年12月18日）を元に当局が編集
https://www.meti.go.jp/press/2020/12/20201218008/20201218008.html

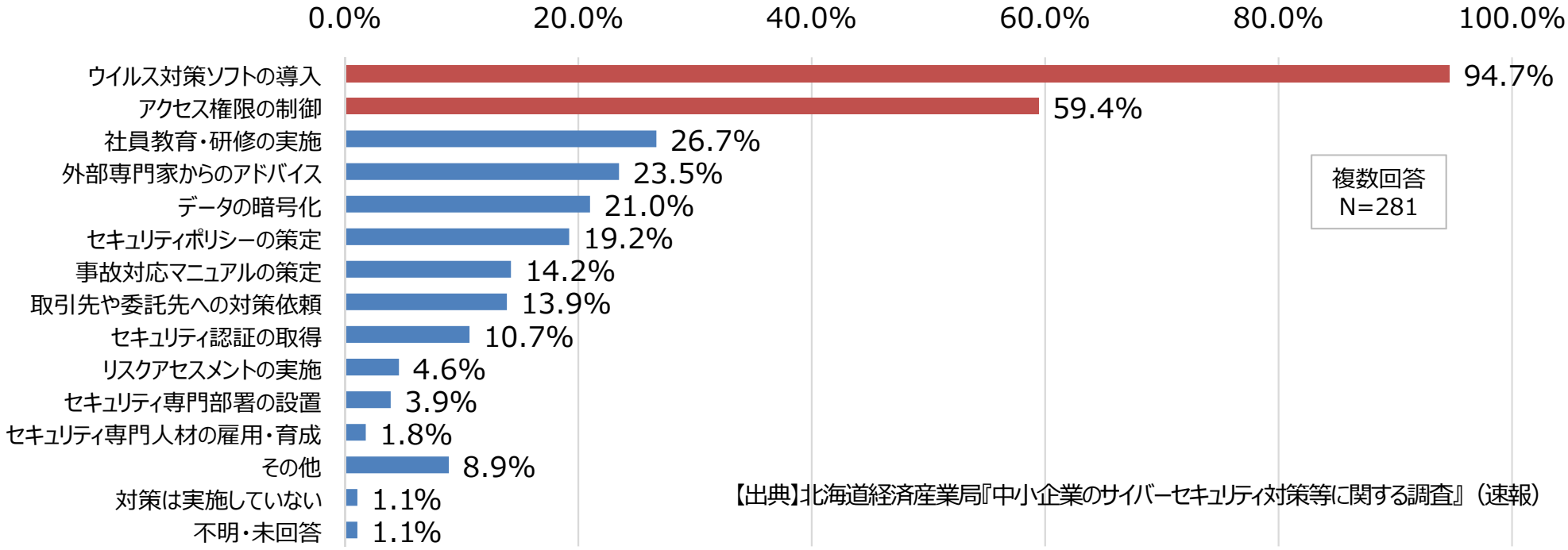
※大阪商工会議所の調査では、対象30社全てが「マルウェア対策ソフトの導入」「ソフトウェアのバージョンを常に最新」等の対策を実施済だったにもかかわらず、「外部から社内端末をリモート操作」「社内端末と悪性サイトとの通信」「DDoS攻撃を目的としたパケット受信」といった事象が複数確認される等、「サイバー攻撃自体に気づいていない」「被害にも気づいていない」可能性を指摘している。

【出典】大阪商工会議所『平成30年度中小企業に対するサイバー攻撃実態調査（報告）』（令和元年7月）
https://www.osaka.cci.or.jp/Chousa_Kenkyuu_Iken/press/20190703cyber_h30.pdf

サイバーリスクへの対策状況

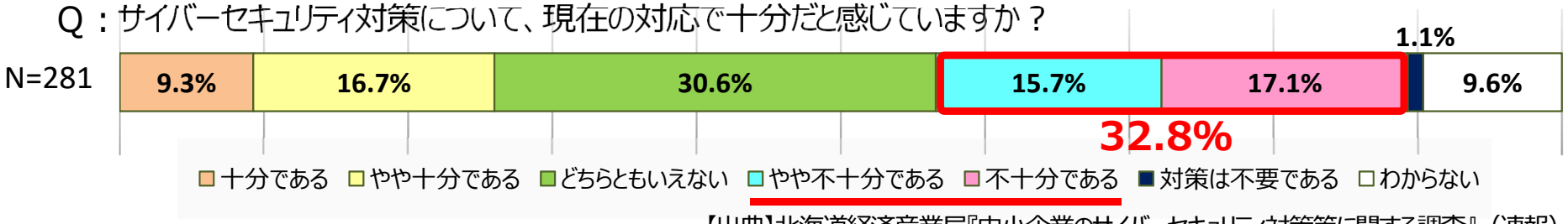
- サイバーセキュリティ対策として、「ウイルス対策ソフトの導入」（94.7%）が最も多く、次いで「アクセス権限の制御」（59.4%）など、**大半の企業でセキュリティ対策を実施済み。**（「対策は実施していない」と回答した企業は1.1%）
- 一方、**自社の対応を「不十分・やや不十分」と感じる企業が3割以上（32.8%）を占める。**

Q：実施済みのサイバーセキュリティ対策は何ですか？



【出典】北海道経済産業局『中小企業のサイバーセキュリティ対策等に関する調査』（速報）

Q：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？

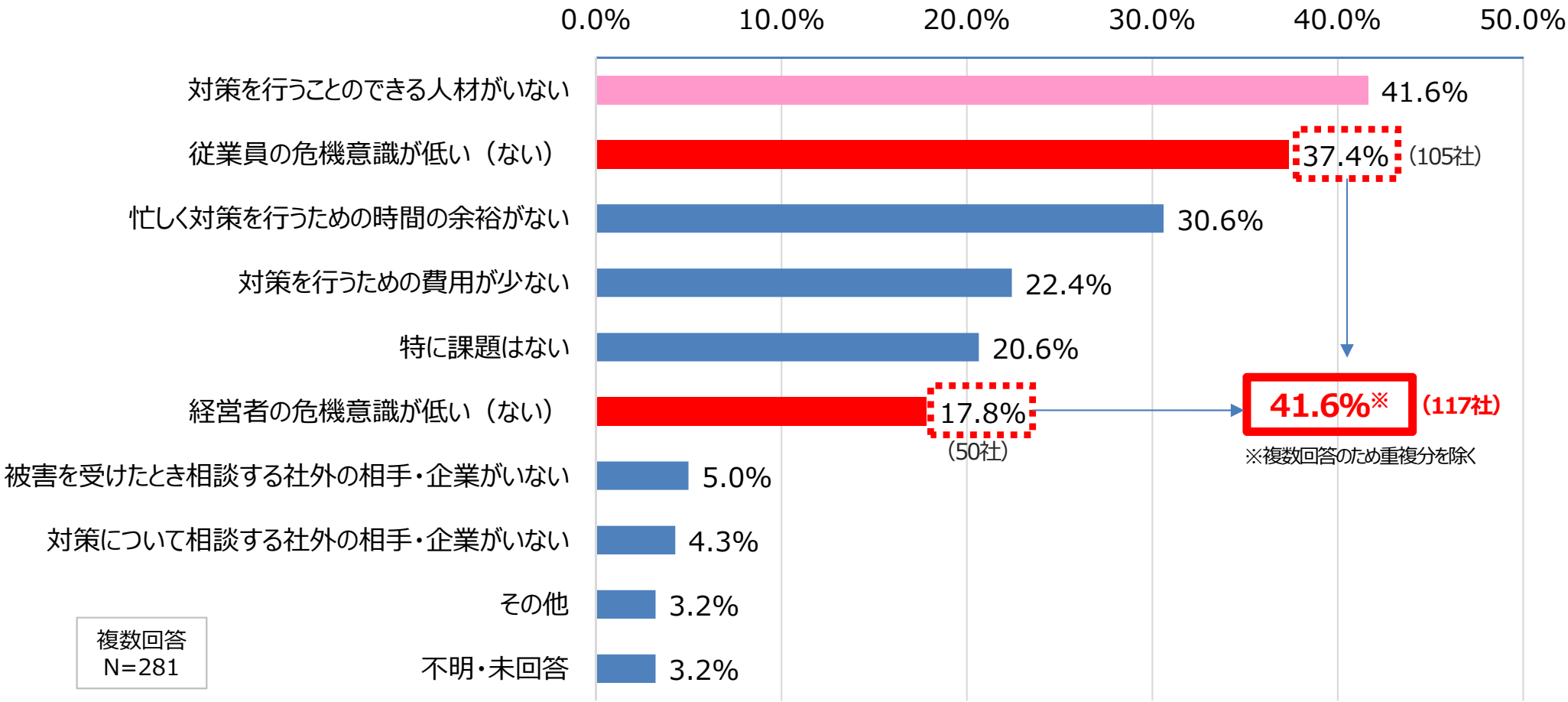


【出典】北海道経済産業局『中小企業のサイバーセキュリティ対策等に関する調査』（速報）

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する課題について、4割以上の企業が「対策を行うことのできる人材がいない」と回答しており（41.6%）、**セキュリティ分野の人材不足が浮き彫り**となった。
- また、「経営者・従業員の危機意識が低い」と回答した企業も多く（41.6%）、**経営者・従業員の意識醸成の必要性も明らかになった。**

Q：サイバーセキュリティに関する課題は？



【出典】北海道経済産業局『中小企業のサイバーセキュリティ対策等に関する調査』（速報）

最近のサイバー攻撃の状況を踏まえた経営者への注意喚起（2020年12月18日発表）

- 経済産業省では、サイバー攻撃の起点の拡大や烈度の増大が続いていることを受け、最近の攻撃の特徴と目的を明らかにし、企業やその関係機関等が対応する際に注意すべき点を整理することで、**企業の経営者の方々に対し、サイバーセキュリティの取組の一層の強化を促す**こととしました。

経営者の方々へ

【出典】経済産業省『最近のサイバー攻撃の状況を踏まえた経営者への注意喚起』（2020年12月）
https://www.meti.go.jp/press/2020/12/20201218008/20201218008.html

●サイバー攻撃は規模や烈度の増大とともに多様化する傾向にあり、実務者がこれまでの取組を継続するだけでは対応困難になっている。
●アップデート等の基本的な対策の徹底とともに、**改めて経営者のリーダーシップが必要に。**

① **攻撃は格段に高度化し、被害の形態も様々な関係者を巻き込む複雑なものになり、技術的な対策だけではなく関係者との調整や事業継続等の判断が必要に。改めて経営者がリーダーシップを。**

② **ランサムウェア攻撃による被害への対応は企業の信頼に直結。経営者でなければ判断できない問題。**
- 「二重の脅迫※」によって、顧客等の情報を露出させることになるリスクに直面。日常的業務の見直しを含む事前対策から情報露出に対応する事後対応まで、経営者でなければ対応の判断が困難。
- 金銭支払いは犯罪組織への資金提供とみなされ、制裁を受ける可能性のあるコンプライアンスの問題。

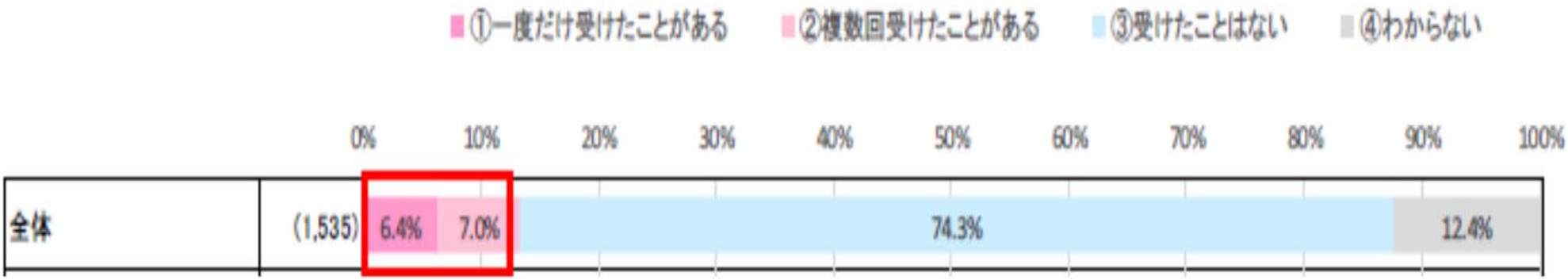
③ **海外拠点とのシステム統合を進める際、サイバーセキュリティを踏まえたグローバルガバナンスの確立を。**
- 国・地域によってインターネット環境やIT産業の状況、データ管理に係るルール等が異なっており、海外拠点とのシステム統合を通じてセキュリティ上の脆弱性を持ち込んでしまう可能性も。
- 拠点のある国・地域の環境をしっかりと評価し、リスクに対応したセグメンテーション等を施したシステム・アーキテクチャの導入や拠点間の情報共有ルールの整備等、グローバルガバナンスの確立が必要。

④ **基本行動指針**（高密度な情報共有、機微技術情報の流出懸念時の報告、適切な場合の公表）**の徹底を。**

※攻撃者が、被攻撃企業が保有するデータ等を暗号化して事業妨害をするだけではなく、暗号化する前にあらかじめデータを窃取しておいて支払いに応じない場合には当該データを公開することで、被攻撃企業を金銭の支払いに応じざるをえない状況に追い込む攻撃形態。

【参考】全国統計に見るサイバーセキュリティ

●サイバー攻撃の被害経験について



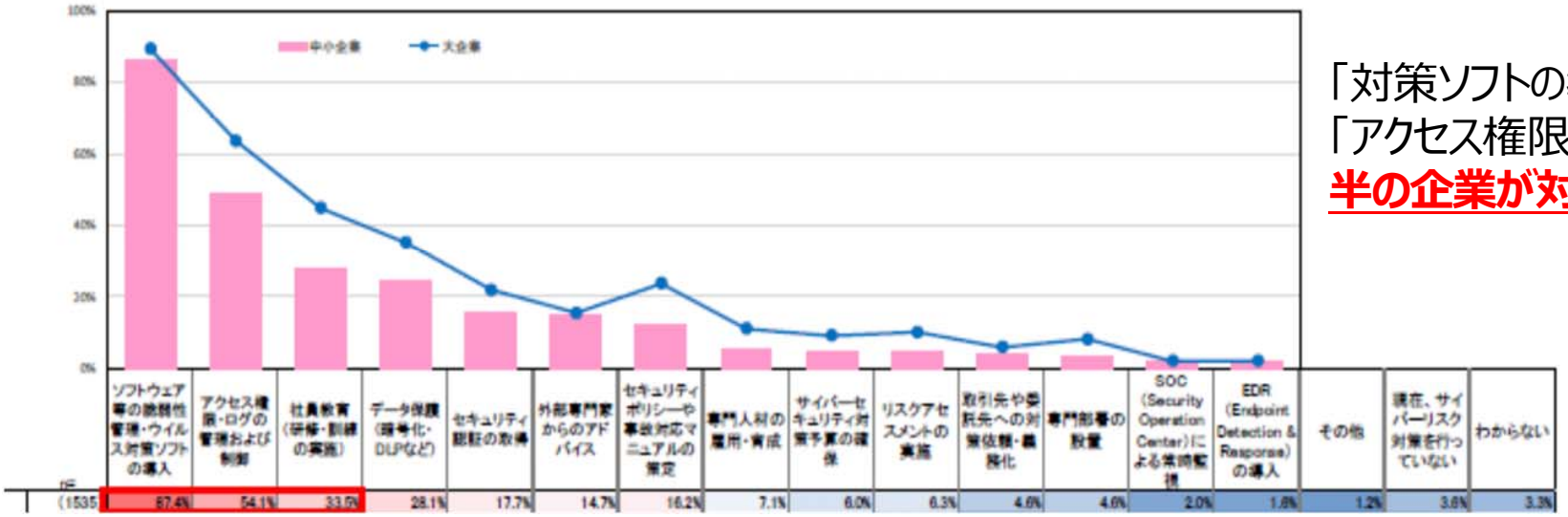
【出典】（一社）日本損害保険協会『国内企業のサイバーリスク意識・対策実態調査2020』（2020年12月）
https://www.sonpo.or.jp/cyber-hoken/data/2020-01/

全体の13.4%（205社）がサイバー被害を受けている。このうち、116社は中小企業であり、複数回被害にあっている企業も多い等、**企業規模を問わずサイバー攻撃の被害**が発生。

※上記調査結果において、以下にも触れられている。
・攻撃の手口として「マルウェア」「ランサムウェア」といったコンピュータウイルス感染が多かった。
・中小企業でも「1000万円以上」の被害事例が見受けられた。

【参考】全国統計に見るサイバーセキュリティ

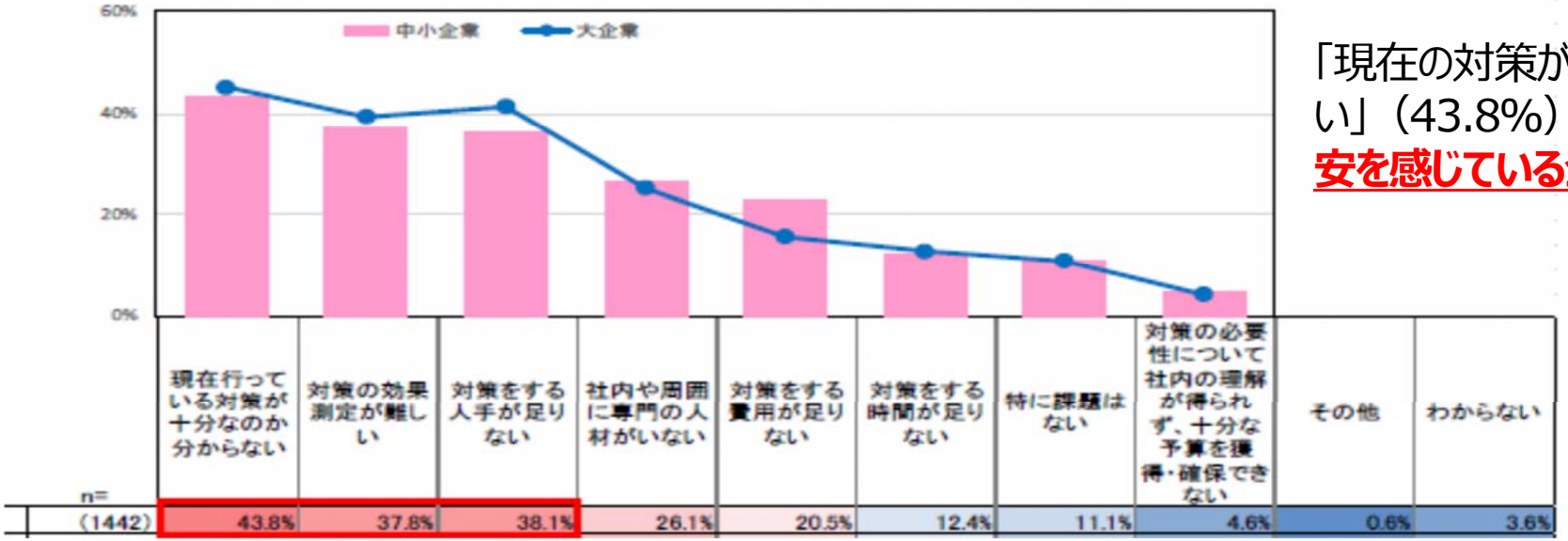
●自社で実施済みのサイバーセキュリティ対策について



「対策ソフトの導入」（87.4%）、「アクセス権限」（54.1%）など**大半の企業が対策済み。**

【出典】（一社）日本損害保険協会『国内企業のサイバーリスク意識・対策実態調査2020』（2020年12月）https://www.sonpo.or.jp/cyber-hoken/data/2020-01/

●自社のサイバーセキュリティ対策の課題について

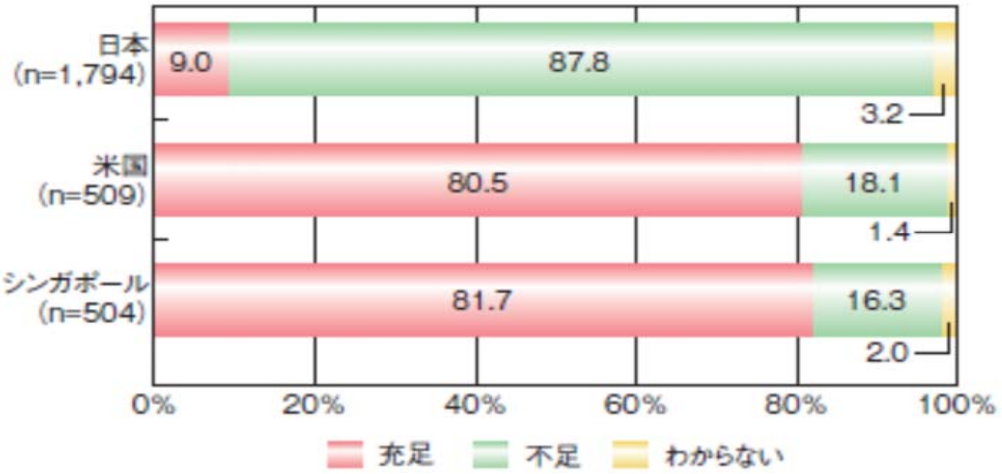


「現在の対策が十分なのかわからない」（43.8%）と**自社の対策に不安を感じている企業が多い。**

【出典】（一社）日本損害保険協会『国内企業のサイバーリスク意識・対策実態調査2020』（2020年12月）https://www.sonpo.or.jp/cyber-hoken/data/2020-01/

【参考】全国統計に見るサイバーセキュリティ

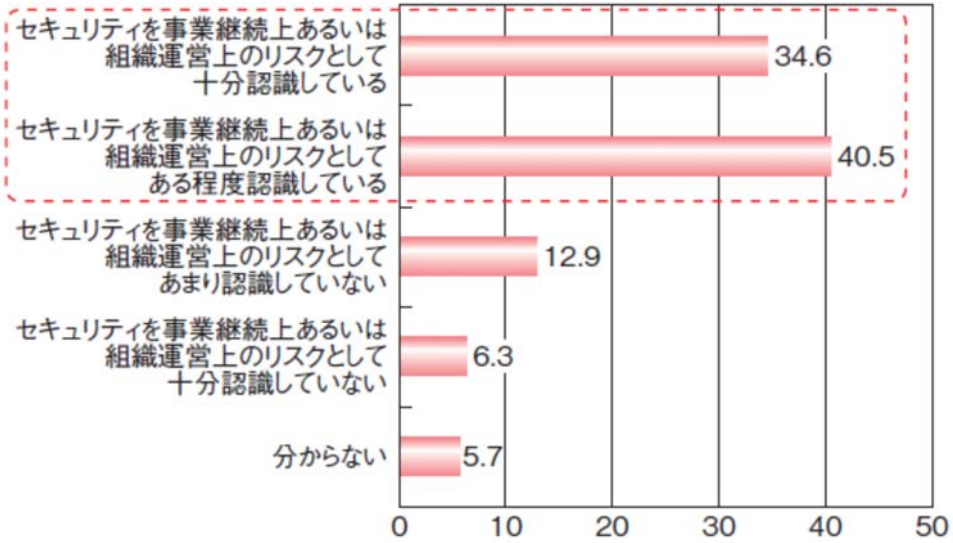
●セキュリティ人材について



NRIセキュアテクノロジーズ(株)の『NRI Secure Insight2019』によると、**日本企業の約9割がセキュリティ対策に従事する人材不足**と指摘。

【出典】（独）情報処理推進機構『情報セキュリティ白書2020』（2020年8月）
https://www.ipa.go.jp/security/publications/hakusyo/2020.html

●情報セキュリティに関する経営層のリスク認識について



■図 2-4-2　情報セキュリティに関する経営層・上層部のリスク認識
(n=1,431)

トレンドマイクロ(株)の『法人組織におけるセキュリティ実態調査2019』によると、セキュリティを事業継続上あるいは組織運営上のリスクとして認識している経営者の割合は75.1%と、**全国的にセキュリティ対策への意識は高い。**

【出典】（独）情報処理推進機構『情報セキュリティ白書2020』（2020年8月）
https://www.ipa.go.jp/security/publications/hakusyo/2020.html

※（一社）日本損害保険協会『中小企業の経営者のサイバーリスク意識調査2019』（2020年1月）によると、「サイバー攻撃への対策が必要と感じている」と回答した中小企業は22.9%。大企業の66.7%に対して**中小企業の方が意識が低い傾向**にある。

【参考】主なサイバー攻撃の類型

	サイバー攻撃の種類	主な攻撃の手口	被害事例等
1	標的型攻撃による機密情報の窃取	業務に関連するような件名、本文、添付ファイル名を偽装したメールの添付ファイルを開いたり、本文に記載したリンク先にアクセスすることでウィルスに感染し、重要技術や個人情報等の機密情報を窃取される。	プラント関連業者において、アイコンや拡張子の偽装、特定のセキュリティソフトの停止、不正接続先から特定の応答が得られないと動作を止める等の仕掛けが施されたウィルスが確認。
2	ビジネスメール詐欺による金銭被害	攻撃者が取引先になりすまし、攻撃者の用意した口座に差し替えた偽の請求書等をメールで送りつけ、振り込ませる。	マフィアが関与していると思われる犯罪グループが、海外企業の会社代表のメールアドレスを乗っ取り、同社の口座があるスイスの銀行へメールし、日本国内の金融機関に振り込ませた。
3	サプライチェーンの弱点を悪用した攻撃	サプライチェーン内にセキュリティ対策を適切に実施していない委託先がある場合、攻撃者はその弱点を攻撃し、連鎖して委託元組織に被害が及ぶことで、委託先は被害者であると同時に加害者にもなる。	スポーツ関連団体の新システム開発委託先の再委託先が不正アクセスを受け、動作検証用に構築したサーバー内のデータベースから、競技関係者の姓名、性別、生年月日などを含む個人情報が削除。
4	ランサムウェアによる被害	メールの添付ファイルやメール本文中のリンクを開かせることで、ファイルの暗号化や画面ロック等を行うウィルス（ランサムウェア）に感染させ、復旧と引き替えに金銭等を要求される。	市立高校が利用している校内ネットワークサーバーがランサムウェアに感染。ワードドキュメントが暗号化され、生徒が作成した成果物等のデータが使用不可能に。
5	インターネット上のサービスからの個人情報の窃取	ＥＣサイト等のインターネット上のサービスの脆弱性等を悪用した不正アクセスや不正ログインにより、サービスに登録している個人情報等を窃取される。広く共通的に使われる市販のソフトウェアや、開発時に作り込んだウェブアプリケーションの脆弱性が悪用されている。	ファイル転送サービス「宅ファイル便」に対する不正アクセスにより、４８０万件以上の個人情報が漏洩。
6	ＩｏＴ機器の不正利用	「オフィス機器」や「産業機器」等に使用されているＩｏＴ機器の脆弱性を悪用し、インターネット経由で不正アクセスや、ウィルス感染させ、搭載機能の不正利用、制御対象の誤作動、機能不全を起こす。	自治体が設置した河川監視カメラをホームページで公開していたところ、このカメラへの不正アクセスが発生。外部からのアクセス用パスワードも変更され、制御不能に。
7	サービス妨害攻撃によるサービスの停止	企業や組織が提供しているインターネット上のサービスに対して大量のアクセスを一斉に仕掛けることで、ウェブサイト等のレスポンスの遅延や機能停止状態とさせる（ＤＤｏＳ（分散型サービス妨害）攻撃）。	マンション居住者向けのインターネット接続サービスがＤＤｏＳ攻撃を受け、一部マンションにて断続的に通信異常が発生。時間経過とともに攻撃元のＩＰアドレスが変化し、通信障害が長期化。
8	脆弱性対策情報の公開に伴う悪用増加	公開したソフトウェア製品の脆弱性対策情報を攻撃者に悪用され、当該ソフトウェア製品を利用した対策前のシステムを狙い、ウェブサイトの改ざん等を引き起こす。	脆弱性情報がウェブサイトに公開された２日後に、パッチの適用をしていない利用者のウェブサイトが改ざんされる被害が多数発生。

【出典】情報セキュリティ10大脅威2020・2019・2018（（独）情報処理推進機構））をもとに当局にて編集

【参考】サイバーセキュリティお助け隊事業（経済産業省・IPA）

- 当省・情報処理推進機構（IPA）では、令和元年度から、地域中小企業のサイバーセキュリティに対する意識向上と、中小企業の実態・ニーズにあった対策の定着を目的に「サイバーセキュリティお助け隊」を実施。
- 昨年度は**全国1,064社が参加し重大インシデント128件に対処する等、地域の中小企業でもサイバー攻撃に遭っている**ことが顕在化。令和2年度は北海道地域を含め、全国13地域・2産業分野で実証中。

「サイバーセキュリティお助け隊」の結果（R1FY）

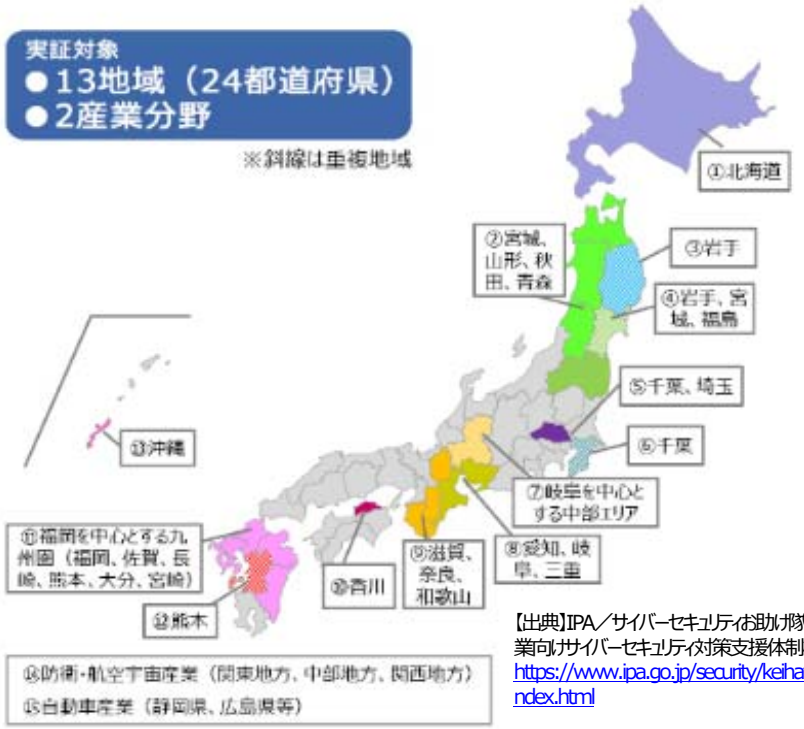
➢ 1,064社が参加した実証期間中に、全国8地域で**計910件のアラート**が発生。重大なインシデントの可能性ありと判断し、**対処を行った件数**は**128件**。対処を怠った場合の**被害想定額**が**5,000万円を超える**事案も。

＜駆け付け支援の対象となった特徴的な対応事例＞

古いOSの使用	サプライチェーン攻撃
●Windows XPでしか動作しないソフトウェア利用のために、**マルウェア対策ソフト未導入のWindows XP端末を使用**。 ●社内プリンタ使用のために、社内LANに接続したことで、意図せずにインターネット接続状態になり、マルウェアに感染。 ●検知・駆除できていなかった場合の**想定被害額は5,500万円**。	●実証参加企業でマルウェア添付メールを集中検知。 ●**取引先のメールサーバーがハックされてメールアドレスが漏えい**し、それらのアドレスからマルウェア添付メールが送付されていた。 ●メールは賞与支払い、請求書支払い等を装うなりすましメールであり、**サプライチェーンを通じた標的型攻撃**であった。

【出典】経済産業省『昨今の産業を巡るサイバーセキュリティに係る状況の認識と、今後の取組の方向性について』（2020年6月）を元に当局が編集
https://www.meti.go.jp/press/2020/12/20201218008/20201218008.html

「サイバーセキュリティお助け隊」の実施状況（R2FY）



【出典】IPA／サイバーセキュリティお助け隊（令和2年度中小企業向けサイバーセキュリティ対策支援体制構築事業）
https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html

【北海道】東日本電信電話(株)北海道事業部

・連携機関：札幌商工会議所、北洋銀行、中小企業診断協会北海道
　北海道地域情報セキュリティ連絡会（総通局、経産局、道警）
・実施期間：2020年9月～2021年1月
・実証内容：UTM監視・レポート、メール訓練、e-ラーニング、web診断、
　駆けつけサポート等
・対象企業：道内中小企業（約150社に実証中）