経済産業省
九州経済産業局

中小製造業向け体験型演習開催
に向けた事前説明セミナー

サイバー攻撃を受けたら・・・
生産停止する工場ですか？生産継続する工場ですか？

中小製造業の事業継続に向けた対策の重要性

令和５年２月１日

経済産業省　九州経済産業局

デジタル経済室

サイバーセキュリティ戦略の課題と方向性

【出所】サイバーセキュリティ戦略
（令和3年9月28日）の概要から抜粋

2020年代を迎えた日本を取り巻く時代認識 ： 「ニューノーマル」とデジタル社会の到来

- デジタル経済の浸透、**デジタル改革**の推進
- **新型コロナウイルス**の影響・経験 テレワーク、オンライン教育等の進展
- 厳しさを増す **安全保障**環境
- **SDGｓ**への デジタル技術の貢献期待
- **東京オリンピック・パラリンピック**に向けて行ってきた取組

サイバー空間をとりまく課題認識 ： 国民全体のサイバー空間への参画

- サイバー空間は、国民全体等**あらゆる主体が参画し公共空間化**
  サイバー・フィジカルの垣根を超えた各主体の相互連関・連鎖の深化
  攻撃者に狙われ得る弱点にも
- 地政学的緊張を反映 **国家間競争**の場に 安全保障上の課題にも
- 不適切な利用は 国家分断、人権の阻害へ
- 官民の取組の 活用

あらゆる主体にとってサイバーセキュリティの確保は自らの問題に
５つの基本原則※は堅持

「Cybersecurity for All」
～誰も取り残さないサイバーセキュリティ～

デジタルトランスフォーメーション（DX）とサイバーセキュリティの同時推進

安全保障の観点からの取組強化

公共空間化と相互連関・連鎖が進展する サイバー空間全体を俯瞰した 安全・安心の確保

「自由、公正かつ安全なサイバー空間」の確保

※情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携

経済社会の活力の向上及び持続的発展

【出所】サイバーセキュリティ戦略（令和3年9月28日）の概要から抜粋

課題認識と方向性　ーデジタルトランスフォーメーションとサイバーセキュリティの同時推進 ー

- 本年9月に「デジタル庁」が設置され、デジタル化が大きく推進される絶好の機会。
  そのためにも、サイバー空間への信頼を醸成し、参加・コミットメントを得ることが重要。
- また、業務、製品・サービス等のデジタル化が進む中、サイバーセキュリティは企業価値に直結する営為に。
  「セキュリティ・バイ・デザイン」の重要性は一層増し、デジタル投資とセキュリティ対策の一体性は高まる。

⇨ デジタル化の進展と併せて、サイバーセキュリティ確保に向けた取組を、あらゆる面で同時に推進。

主な具体的施策

① 経営層の意識改革

→デジタル経営に向けた行動指針の実践を通じ、サイバーセキュリティ経営のガイドラインに基づく取組の可視化・インセンティブ付けを行い、更なる取組を促進。

② 地域・中小企業におけるDX with Cybersecurityの推進

→地域のコミュニティの推進・発展、中小企業向けサービスの審査登録制度を通じ、デジタル化に当たって直面する知見や人材等の不足に対応。

③ 新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり

→Society5.0に対応したフレームワーク等も踏まえ、各種取組を推進。

- サプライチェーン：　産業界主導のコンソーシアム
- データ流通　　：　データマネジメントの定義、「トラストサービス」によるデータ信頼性確保
- セキュリティ製品・サービス：　第三者検証サービスの普及
- 先端技術　　：　情報収集・蓄積・分析・提供等の共通基盤構築

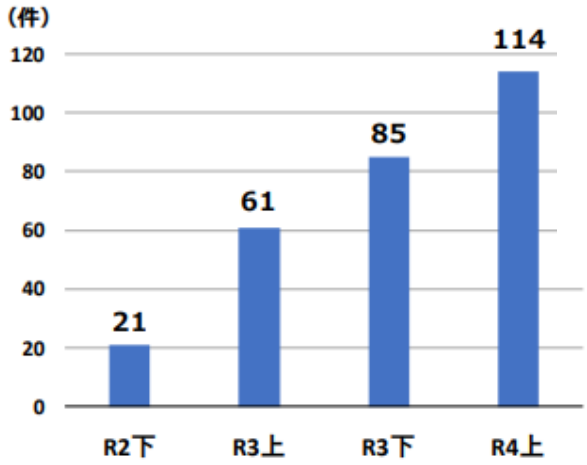
④ 誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着

→情報教育推進の中、「デジタル活用支援」と連携して、各種取組を推進。

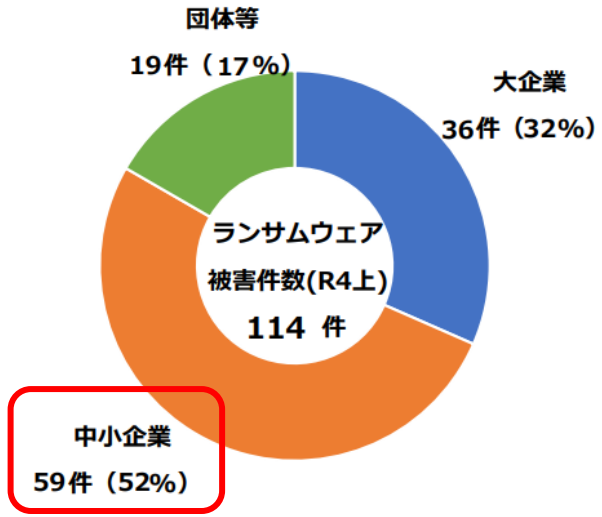
サイバー攻撃による被害の実態（令和４年上半期の警察庁調査結果）

- ランサムウェア：感染すると端末等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価として金銭を要求する不正プログラム。
- 令和４年上半期の報告件数は116件。令和２年下半期以降、右肩上がりで推移。
- **被害報告の52%は中小企業で、業種別では製造業が32%と突出。**

被害報告件数の推移

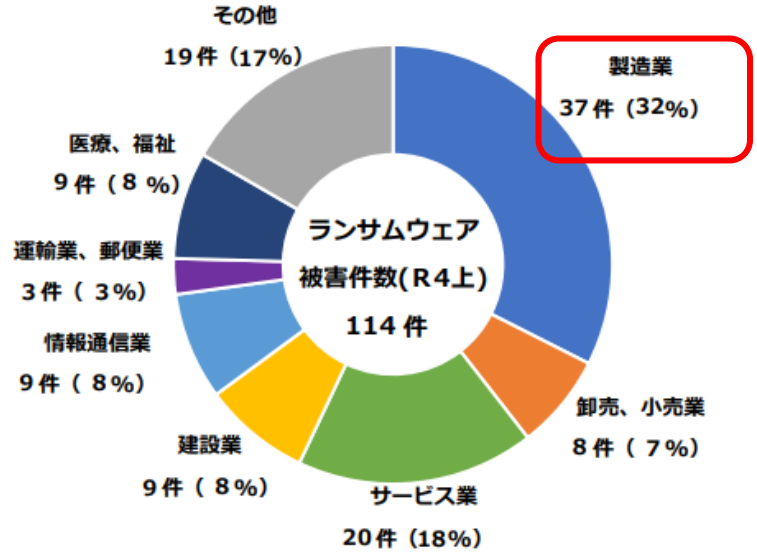


企業・団体等の規模別報告件数



注　図中の割合は小数第１位以下を四捨五入しているため、総計が必ずしも100にならない。

企業・団体等の業種別報告件数



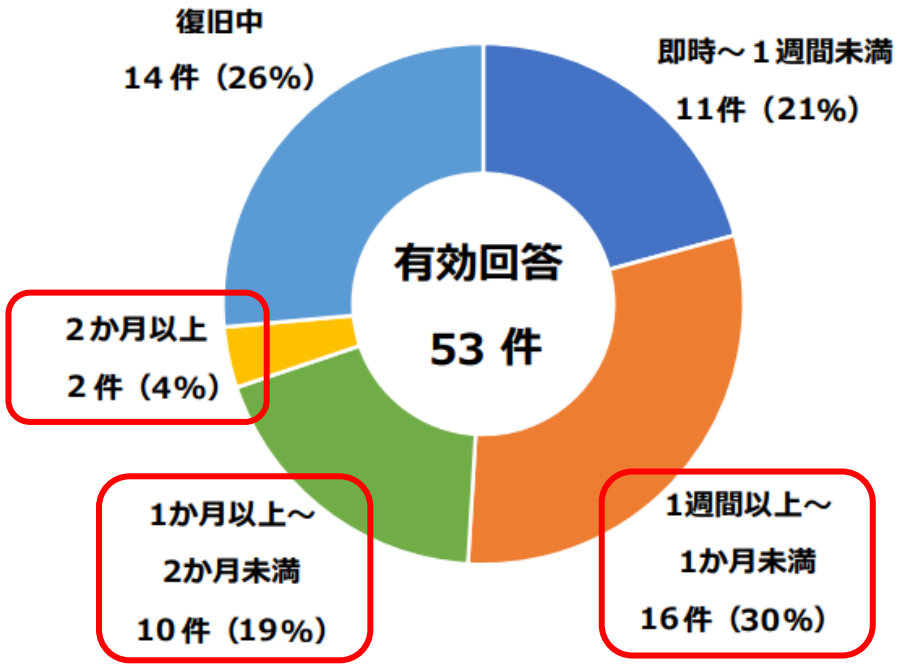
注　図中の割合は小数第１位以下を四捨五入しているため、総計が必ずしも100にならない。

出典：警察庁「令和４年におけるサイバー空間をめぐる脅威の情勢等について」（令和４年９月１５日）

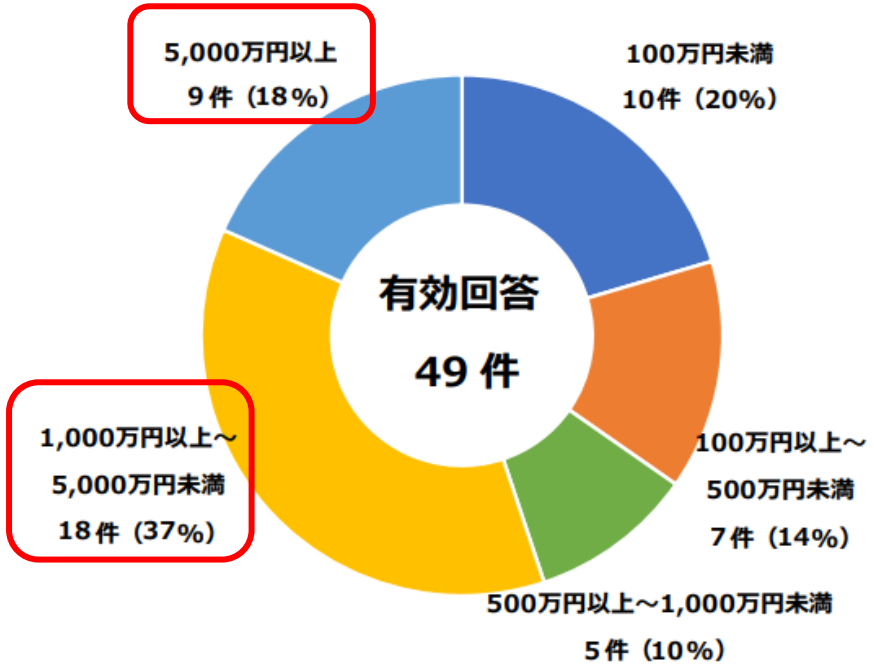
サイバー攻撃による被害の実態（令和４年上半期の警察庁調査結果）

- ランサムウェアへの感染後、調査・復旧費用には**1,000万円以上を要したものが55%。**
  全体の２割程で**5,000万円以上**の費用を要した事例も確認されている。
- **復旧に１週間～2ヶ月・２ヶ月以上の期間を要したものが全体の半数（53%）に及んでおり、ビジネスへの影響・被害は極めて甚大。**

復旧に要した期間



調査・復旧費用の総額



注　図中の割合は小数第１位以下を四捨五入しているため、総計が必ずしも100にならない。

出典：警察庁「令和４年におけるサイバー空間をめぐる脅威の情勢等について」（令和４年９月１５日）

事業継続力強化計画認定制度

- 「事業継続力強化計画」とは、中小企業が、自然災害や感染症などへの防災・減災対策の第一歩として取組内容等をとりまとめて作成する計画。
- 経済産業大臣の認定を受けると、融資・税制、補助金採択等における優遇措置あり。

【計画認定のスキーム】

中小企業・小規模事業者

連携して計画を実施する場合：
大企業や経済団体等の連携者

①計画を策定し申請 ↓

↑ ②認定

経済産業大臣（地方経済産業局）

認定対象事業者

- 中小企業・小規模事業者

認定を受けた企業に対する支援策

- 防災・減災設備の導入に対する**税制措置**
- 低利融資、信用保証枠の拡大等の**金融支援**
- **補助金**（ものづくり補助金）の加点措置
- **中小企業庁ＨＰでの認定企業の公表**
- 認定企業にご活用いただける**ロゴマーク**
  （会社案内や名刺で認定のＰＲが可能）

事業継続力強化に関する基本方針の改正（R2年10月1日施行）

- あらたに自然災害以外のリスク（サイバー攻撃、感染症その他）についても、事業継続力強化における支援措置の対象に追加。

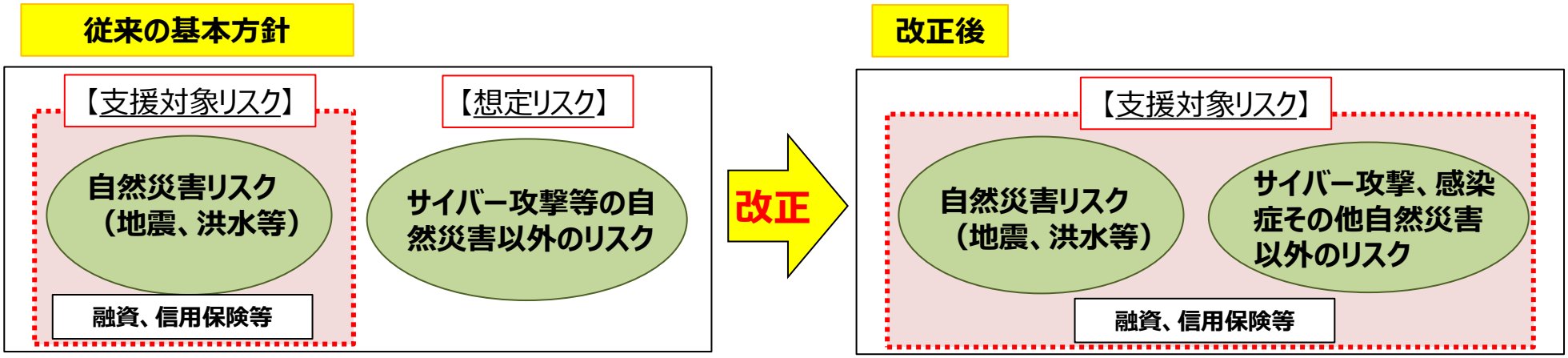
【改正項目①：支援対象の拡大】

○従来の運用上、法に紐付く融資、信用保険等の支援措置の適用は、「自然災害リスク」のみに限定。

事業活動に影響を与える自然災害等のリスクとして、暴風、竜巻、豪雨、豪雪、洪水、崖崩れ、土石流、高潮、地震、津波、噴火、地滑りその他の異常な**自然現象に直接又は間接に起因するリスク**が想定される。～（略）～。そのため、中小企業者の事業継続力強化については、**右に掲げる自然災害のリスクを踏まえた事前対策を実施する取組を支援対象**とする。

○一方、感染症への対応は喫緊の課題であることから、支援対象に感染症等の「自然災害以外のリスク」を追加。

事業活動に影響を与える自然災害等のリスクとして、暴風、竜巻、豪雨、豪雪、洪水、崖崩れ、土石流、高潮、地震、津波、噴火、地滑り、**サイバー攻撃、感染症その他の異常な現象に直接又は間接に起因するリスク**が想定される。～（略）～。そのため、中小企業者の事業継続力強化については、自然災害等のリスクを踏まえた事前対策を実施する取組を支援対象とする。



２２．事業継続力強化計画の認定状況

- 令和元年7月に中小企業強靭化法が施行され、令和４年12月末時点で、全国で50,153件、**九州7県で4,616件**の事業継続力強化計画申請書を認定済み。
- 他方、複数の事業者が連携して取り組む、連携事業継続力強化計画の認定は、全国で643件、九州7県では61件である。

<全国の認定実績>

地域	認定件数
北海道	１，８６２
東北	２，１６７
関東	１９，０２４
中部	７，２１２
近畿	９，７８４
中国	３，２２８
四国	１，８７２
九州	４，６１６
沖縄	３８８
合計	５０，１５３

※令和４年１２月末時点の認定実績

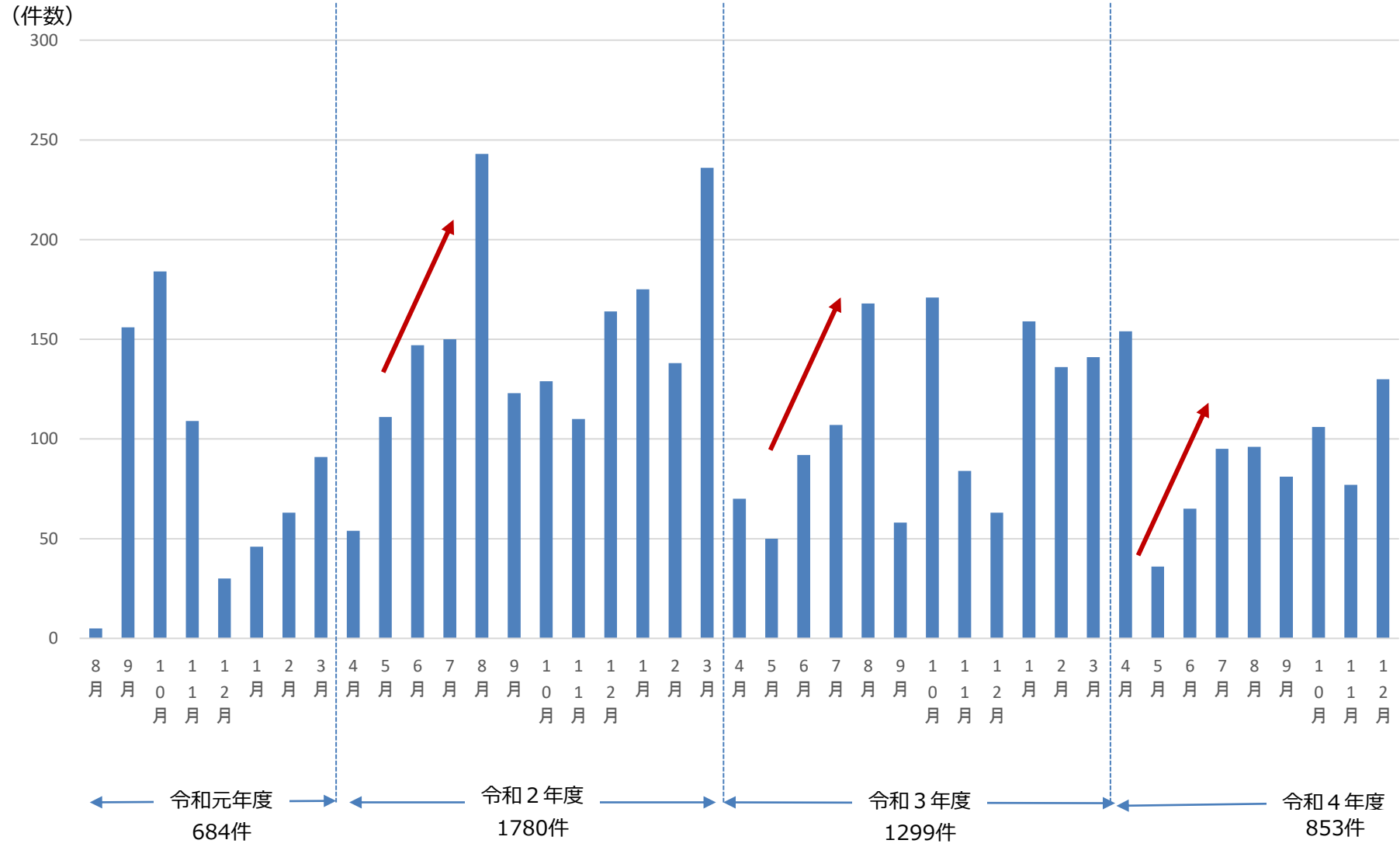
<九州の認定実績内訳>

県	認定件数 (事業者1000者あたり※の認定件数)	うち連携 事業継続力強化計画
福岡	1,951（14.4）	17
佐賀	375（15.4）	7
長崎	548（13.1）	5
熊本	577（12.1）	12
大分	396（11.4）	13
宮崎	398（11.4）	5
鹿児島	371（ 7.4）	2
合計	4,616（12.5）	61
全国	50,153（14.0）	643

※事業者数は、2016年６月時点の中小企業・小規模企業の数。
資料：中小企業庁「中小企業・小規模事業者数（2016.6月時点）の集計結果」（平成28年経済センサス活動調査データ）
https://www.chusho.meti.go.jp/koukai/chousa/chu_kigyocnt/2018/181130chukigyocnt.html

【参考】月別認定状況（九州）

- 事業継続力強化計画の認定件数は例年５月から８月に増える傾向。
- 豪雨や台風シーズンへの備えや行政の支援措置が要因として考えられる。



九州経済産業局における
中小企業向けサイバーセキュリティ対策促進事業

中小企業のサイバーセキュリティ対策促進に向けた取組

- 近年、中小企業等のサプライチェーン上の脆弱な部分が狙われるサイバー攻撃が増加しており、**「事業継続のリスク（引き金事象）」**として課題が顕在化。
- 九州経済産業局は、**業種ごとの特徴を踏まえたセキュリティ対策が行えるよう専門家、関係企業との共助関係を構築**する「地域SECUNITY（セキュリティ・コミュニティ）」活動を推進。

*「SECUNITY」はSECURITYとCOMMUNITYをかけあわせた造語

＜地域SECUNITYのコンセプトと事業計画＞

これまで･･･

地域にセキュリティについて相談できる相手がいない

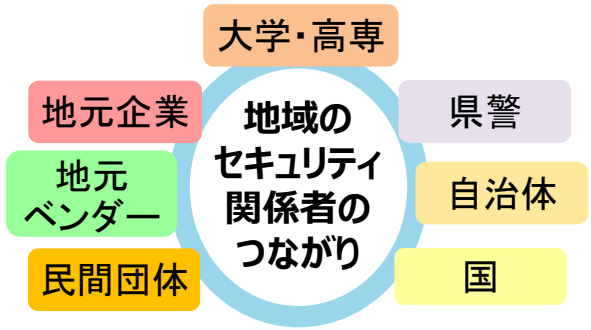
地域にセキュリティを学ぶ機会が少ない

地域のベンダーを知らない

地域SECUNITYがない状態

令和2～3年度

・地域特性も考慮しながら産業分野ごとに“地域SECUNITY”を形成
・活動の牽引役となるキーパーソン、インフルエンサーを発掘！



地域SECUNITY（セキュリティ・コミュニティ）形成

令和4年度～

・**「EC・海外ビジネス」「医療・調剤関連産業」「衛星データ利活用産業」を重点**としたマッチングを実施。
・普及啓発（セミナー）と実践的教育機会の提供（少人数のワークショップ等）を通して、課題解決を促進。

セミナー（基礎編）
ワークショップ（ECサイト活用編）
ワークショップ（衛星データ利活用編）
ロールプレイ形式の演習（インシデント発生しても事業継続できるようBCPを演習）

地域のニーズとシーズのマッチングによる課題解決・付加価値創出の場へ

中小製造業向け体験型演習について（経緯）

- 令和３年度から、九州大学サイバーセキュリティセンターが取り組む**社会人リカレント教育プログラム（SECKUN）との連携で、“サイバーセキュリティインシデント対応机上演習”の特別無料視聴参加プログラムを提供。**
- 地域企業からの要望を受け、令和５年度から「中小製造業向け」を開催予定。
- 地域企業、地域団体等と九州大学側とのネットワークを繋げていくことで、**中小企業の人材育成に向けた実践的教育の機会を提供**。

九州大学
KYUSHU UNIVERSITY

SECKUN「サイバーセキュリティインシデント対応机上演習」
実施イメージ

提供：九州大学サイバーセキュリティセンター

今後の中小製造業向け体験型演習の開催予定

工場の緊急時生産管理体制を共に考える！

「中小製造業向け体験型演習」in 北九州

令和５年
３月８日(水)

13:00～
17:00

参加費　無料

オンライン聴講者募集！
（Webex Meeting）

北九州市IoT実践研究会に参画する中小製造業７社を中心にモデル演習として実施し、その様子をオンライン配信します

オンライン参加者からの質問や意見もOK！
中小製造業以外の方の参加ももちろんOK！

主催：九州大学サイバーセキュリティセンター、一般財団法人九州オープンイノベーションセンター、九州経済産業局
共催：公益財団法人北九州産業学術推進機構

公益財団法人
北九州産業学術推進機構
との共催

本日からオンライン参加者の募集を開始しています！ぜひ当局HPからお申し込みください！
https://mm-enquete-cnt.meti.go.jp/form/pub/kyusyu-johoseisaku/ttx1

令和５年度は福岡、長崎のほか、全国でも開催予定

「中小製造業向け体験型演習」の狙い

狙い

- 水害、地震、サイバー攻撃・・・予防措置を取っていても、未曾有な事態は起こるもの
- 防げなかったとき、生産や事業の継続に支障が出たら・・・？
- 何が起こりうるのか・・・危機管理を模擬体験することで「気付きや疑問」が生まれる

①企業の皆様へ

演習で得られた「気付き」を持ち帰っていただき、
経営層、生産管理部門、製造部門、システム部門、広報部門、総務部門含め、
会社全体で緊急生産管理体制を再度検討する機会に繋げてください！
（例：「緊急連絡網」「対策本部での役割分担」「緊急生産管理マニュアル」等の見直し）

②支援機関、業界団体の皆様へ

本演習の開催希望があれば九州経済産業局デジタル経済室までご相談ください。
来年度の演習開催を通して、今後、各団体が九州大学と連携し自主的に
実施できるよう関係構築を図ります。

＜参考＞中小企業向けセキュリティ対策ツール

● 中小企業の情報セキュリティ対策ガイドライン

中小企業が情報セキュリティ対策に取り組む際の経営者が認識し実施すべき指針、社内において対策を実践する際の手順や手法をまとめたもの。

経営者向けの解説

経営者が認識すべき３原則と実施すべき重要７項目を解説

実践者向けの解説

企業のレベルに合わせて**段階的にステップアップ**できるような構成で解説

● 「SECURITY ACTION」

中小企業自らが、セキュリティ対策に取り組むことを自己宣言する制度。20万者を超える中小企業が宣言（2022年6月末）。

★一つ星

情報セキュリティ５か条に取り組む

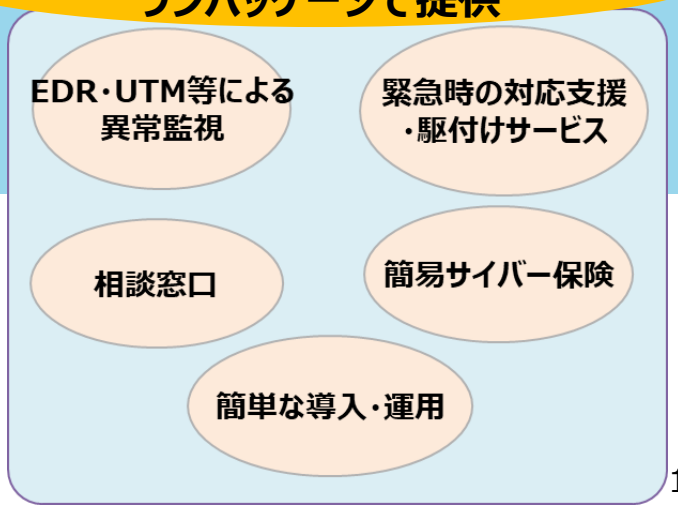
★★二つ星

情報セキュリティ自社診断を実施し、基本方針を策定

● サイバーセキュリティお助け隊サービス

相談窓口、システムの異常の監視、緊急時の対応支援、簡易サイバー保険など中小企業のサイバーセキュリティ対策に不可欠な各種サービス内容を要件としてまとめた基準を満たすワンパッケージサービス。
（2022年11月時点で25サービス）

中小企業でも導入・維持できる価格でワンパッケージで提供



IT導入補助金「セキュリティ推進枠」
で最大２年分のサービス利用料を補助
✓ 補助額：5万円～100万円
✓ 補助率：1/2以内

サイバーセキュリティ お助け隊

■上記対策ツールの詳細はIPAのHPをご覧ください
https://www.ipa.go.jp/security/keihatsu/sme/index.html