経済安全保障
中小企業向け
入門ガイド

愛知県

はじめに

昨今、「経済的な手段で他国の安全を揺るがす動き」が全世界で活発化しています。例えば、業務の妨害、機密情報の搾取、金銭の獲得などを狙ったサイバー攻撃が国内外で常態化しており、インターネットに繋がる全ての事業者のシステムが被害を受けるリスクにさらされています。

事件に巻き込まれる日本企業が増加していることを背景に、**経済的な手段で平和を維持（安全を保障）しようとする「経済安全保障」と呼ばれる取り組みに、大企業・中小企業を問わず向き合うこと**が求められています。

愛知県では、2022年5月に成立した経済安全保障推進法の施行に伴い、技術情報管理を始めとする経済安全保障を推進し、日本一のものづくりの集積地として、実効性のある地域の備えを構築すべく、2022年10月に「愛知県経済安全保障に関する協議会」を創設しました。

また、県内事業者を対象に「愛知県経済安全保障に関するシンポジウム」を開催し、経済安全保障に関する取組や対策等について普及啓発を図るなど、安全・安心にビジネスを営めるよう施策を推進しています。

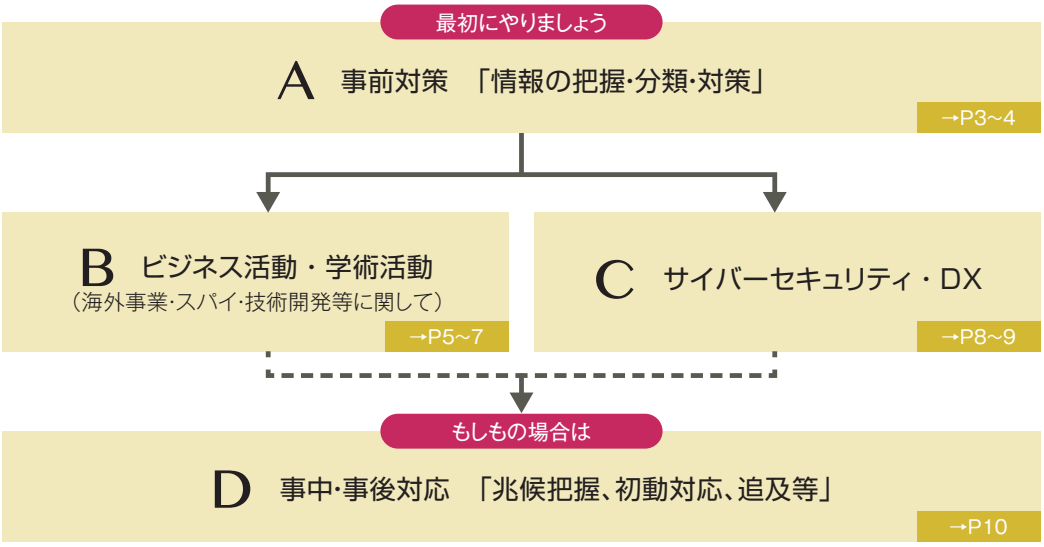
経済安全保障に関する周知や啓発を一層推進すべく、**特に中小企業で活躍される方々が「経済安全保障とは何か」、「自社とどう関係があるのか」、「何をしたらよいのか」などの概要を理解できる**よう、本冊子「経済安全保障　中小企業向け入門ガイド」を制作しました。

社内での対策会議や研修における説明資料として利用いただくだけでなく、有事に備えてお手元で控えておいていただくなど、本書が皆様のビジネスの一助となりましたら幸いです。

目　次

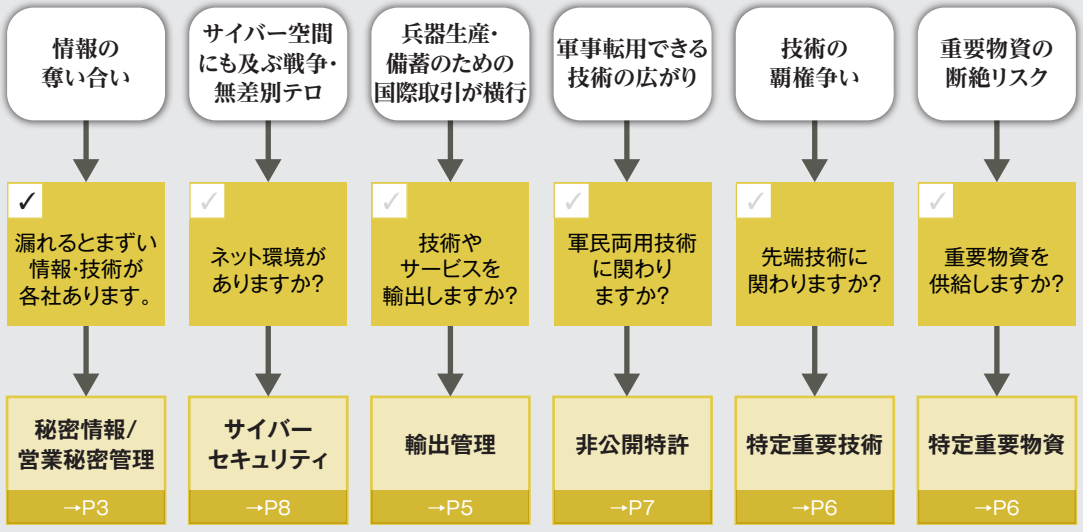
経済安全保障のリスクから企業を守るために
～技術･情報の流出防止と管理方法～

□ 経済安全保障に関する様々なリスクがある中、多くの事業者が関係する問題に「情報流出･技術流出」があります。顧客情報の流出による信用喪失や技術流出による取引消滅など、収益事業の継続が困難になり経営に深刻なダメージを与えます。
□ 全ての事業者様に確認してほしい対策を本紙ではまとめましたので、是非お目通しください。



□ 経済安全保障に関連して、下記のような動きがあります。自社とどんな関係があるのか、チェックをしてみましょう。

- サイバー空間にも戦争･テロの影響が及び、ネットに繋がる全ての事業者のシステムが攻撃の対象になっています。
- 国家間で先端技術の開発競争が激化し、技術や情報の奪い合い･流出が生じています。
- 輸出した製品やサービスが、兵器の生産･備蓄等を目的に使われる可能性が生じています。
- 軍事用途にも使える技術（デュアルユース技術）の種類が増えてきていると考えられます。
- 供給が途絶えると、安全･安心な暮らしや経済活動が脅かされることに繋がる物資があります。



経済安全保障に関する他のトピックス……セキュリティ･クリアランス（P7）、基幹インフラの機能維持、研究インテグリティ、投資管理、経済制裁、入国管理

A 事前対策「情報の把握・分類・対策」

情報流出や技術流出を防ぐために、①保有情報の把握、②情報の分類、③分類に応じた対策を行います。

① 保有情報の把握 → ② 情報の分類 → ③ 分類に応じた対策

①保有情報の把握

- 保有情報の全体像を把握すべく、情報を洗い出します。
- 情報は書面やデータなどに見える化されていない個人が記憶している状態のものも含みます。
- 事業上重要な情報が浮かび上がってくることで属人的な重要情報の存在に気づきを得たり、部署内・部署間で新たなアイデアが生まれるなど、好影響も期待できます。

技術情報

研究開発情報（実験データ、試作品情報等）
製造関連情報（製品図面、製品テストデータ、製造プロセス、工場設備・レイアウト等）

営業情報

顧客情報（顧客リスト、クレーム情報、顧客別製品等情報）
市場関連情報（市場分析情報、競合先分析情報）
価格情報（仕入れ値、製品価格、利益率等）
取引先情報　**顧客マニュアル**　等

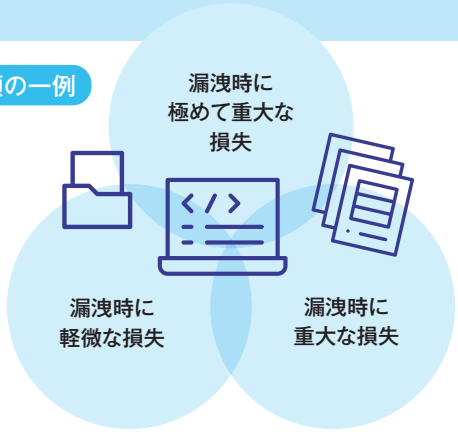
②情報の分類（秘密情報の抽出）

- 保有情報を分類しましょう。
- 抽出した数々の情報を「情報流出時の損失の程度」などの視点で仕分け（評価）を行いましょう。

参考：仕分けの観点

- 情報の経済的価値、自社事業への貢献度
- 漏洩時の競争力の低下、競合から見た有用性
- 漏洩時の社会的信用の低下、他社・顧客の預託情報

分類の一例



- 仕分けた情報について、**「秘密（クローズ）」**として扱うのか、**「公開（オープン）」**のものとして扱うのかを戦略的に検討しましょう。
- 「秘密」として運用していきたい情報に対して経済安全保障の観点から、強奪・盗用・流出の被害にあう可能性があると認識する必要があります。情報流出・技術流出は、経営に深刻な影響を及ぼしかねず、会社・社員・顧客を守るためにも対策を行いましょう。
- **情報や技術が流出する経路**は、「従業員」、「退職者」、「取引先」、「その他の外部者」があることを念頭に、対策を進めていきましょう。

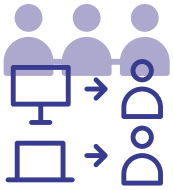
公開（オープン）	or	秘密（クローズ）
部品構造 （容易に把握可能） 動作性能評価方法		生産プロセス 素材配合 顧客情報・個人情報

強奪・盗用・流出のリスクが拡大中

具体的な対策は、次ページ参照

③分類に応じた対策

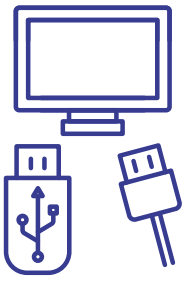
物理的・技術的な防御



近接の制御

■秘密情報にアクセスできる人は最小限にとどめましょう。

□アクセス権の適切な設定
□退職者のアクセス権を速やかに削除
□秘密情報の開示に関する社内規定を設定
□工場見学等で外部者を受け入れる場合、ルートを適正に限定
□ネット接続時はウイルス対策ソフトの導入や、ソフトを最新版にアップデートするなどの対策を実施



持ち出しの困難化

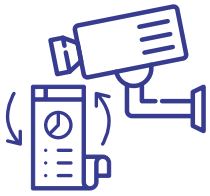
■情報の持ち出しを物理的・技術的に防ぎましょう。

□USBメモリやカメラ等の利用・持込制限
□会議資料等の回収
□業務用ノートPCの固定や持ち出しの制限
□記録媒体への複製制限や組織が許可した以外のオンラインストレージの利用制限
□遠隔操作によるデータ消去機能の担保　　等

■テレワークに関連し、下記のような対策を行いましょう。

□重要情報のレベルに応じたアクセス制限
□PC等へのデータ格納制限
□実施場所の吟味と覗き込み防止フィルムの利用
□組織ネットワークに接続する際にはVPN等を用いて暗号化を実施

心理的な抑止



視認性の確保

■行動記録・操作記録をとりましょう。
従業員の身の潔白を証明する手段にもなります。

□秘密情報を取り扱う職場レイアウトを工夫
□資料・ファイルの通し番号を管理
□入退室の記録を管理
□秘密情報へのアクセス履歴を管理
□メール送受信の記録を管理
□防犯カメラを設置　　等

秘密情報に対する認識向上

■秘密情報の流出・不正利用に対して、
言い逃れをされないための対策を行いましょう。

□何が秘密情報か一目でわかる表示を行い、情報取扱のルールを周知
□入社時・異動時・重要プロジェクトへの配属時・転出時・終了時も、秘密保持契約を締結
□退職者には、秘密保持契約だけでなく、競業避止義務契約を締結することも選択肢
□取引先等の外部者に対しては、近接の制御、持ち出しの困難化、視認性の確保の対策を優先実施
※秘密情報を開示せざるを得ない場合は、秘密保持の対象となる情報をできる限り明確化した、秘密保持契約等を締結することが重要

従業員との信頼関係の維持・向上

■従業員が情報漏洩をしようという気持ちにならないための対策が重要です。働きやすい職場環境を整備し、仕事へのモチベーション向上を通じ、従業員のモラルを高めましょう。

□ワークライフバランスの推進適正な評価
□適切な対価の支払い
□能力や希望に沿う配属
□帰属意識の醸成　　等

詳細情報

【てびき】秘密情報の保護ハンドブック～企業価値向上にむけて～　（経済産業省）
https://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html

解説資料　「秘密情報の保護ハンドブック～企業価値向上に向けて～」　（経済産業省）
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/1706blueppt.pdf

秘密情報の保護ハンドブック～企業価値向上にむけて～　（経済産業省）
https://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html

B ビジネス活動・学術活動

□ **事業展開の可能性を高めたり、事業収益の拡大を図るためには、共同研究の実施、海外輸出、合弁企業の設立などを他国や他国企業と関わりながら行うことも、今日のビジネスシーンでは、重要な選択肢です。**

□ **そうした活動をはじめ、ビジネスシーンにおいて、経済安全保障に関連してどのようなリスクがあるのか、また国はどのような支援策を講じているのか、主なポイントを押さえておきましょう。**

海外との取引・連携

- 取引先の情報を確認しましょう。
- 外国企業との取引の内容（売買、共同研究、合弁・買収等）が、間接的に技術流出や平和（安全保障）を脅かすことがあるので、注意しましょう。
- 自社で判断できないものについては、専門家や相談機関（巻末参照）のサポートを受けつつ、先方の活動実態をチェックすることも有効です。

輸出管理 ～平和（安全保障）を脅かすことに間接加担するリスク～

平和を脅かすことに間接加担するリスクが拡大中

- 輸出する製品やサービス（技術指導）が、兵器の生産・備蓄等を目的に使われる可能性が生じています。
- このため、日本では輸出や海外進出に際してそうしたケースに当てはまるかどうか確認の手続きを行うことが輸出者の責任となっています。規制対象外となっている27か国（2023年現在）以外への輸出に関しては、多くの品目に対して輸出管理が求められています。
- 契約前のサンプル提供や、メールでのデータ送信、日本での技術指導等も管理対象の行為となっているため、注意が必要です。
- 違反時には、懲役や罰金、行政処分、輸出や技術提供の制限などを受けるため、気を付けましょう。

詳細情報

安全保障貿易管理ガイダンス［入門編］（経済産業省）
https://www.meti.go.jp/policy/anpo/guidance.html

輸出管理の基礎 （一般社団法人 安全保障貿易情報センター）
https://www.cistec.or.jp/export/yukan_kiso/index.html

契約 ～技術流出のリスク～

他国への技術流出につながるリスクが拡大中

- 取引に際して契約を締結する際、条項・条文の確認を怠らないようにしましょう。
- 特に契約書修正の過程で、「持ち寄る技術・ノウハウの取り扱い」や「知り得る情報や成果の取り扱い」、「輸出管理に関する条項」等の内容を吟味しましょう。

実例1 共同開発で開発の多くを日本側が実施したにもかかわらず、成果である特許権は共有となり、その後、相手方が製造受注を独占するようになってしまった。

実例2 海外では雇用の流動性が高く、独資・合弁企業の従業員が競合へ転職し、ノウハウが流出した。

詳細情報

営業秘密関係の基本資料 【参考資料2】 各種契約書等の参考例 （経済産業省）
https://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html

他国への技術流出につながるリスクが拡大中

スパイ工作

〈こんなアプローチに注意〉

- スパイは、プライベートやSNSであなたを調べたうえで、偶然を装って近づいてきます。
  彼らは、あなたを様々な手法で誘惑し、技術や秘密情報を奪取しようとします。
  ·個人のSNSへ、接点のない外国企業からメッセージが届いた
  ·道端で見知らぬ外国人に声をかけられた
  ·付き合いのある外国企業の人から、お礼としてプレゼントやご馳走をされた
  ·外国企業の人から、アクセス制限のある情報の提供をお願いされた

〈アプローチへの対策〉

- 情報提供を依頼された際にご自身の身勝手な考えで応じてしまうと、秘密情報の流出に加え、法律違反に問われる可能性もあります。不審な点を感じたら、「個人」で対応することなく、「組織」で対応するよう心がけましょう。
  □金品·飲食の提供などの見返りに、技術や情報の提供を求められる可能性があることを想定する。
  □個人での面会は避け、複数人で面会する。
  □可能な範囲で、相手方の業務内容や業務目的を、具体的に把握することに努める。
  □自身や同僚の担当業務について詳細な言及は避ける。
  □SNSへの個人情報の掲載は慎重に判断する。

詳細情報

技術流出の防止に向けて（パンフレット）（警察庁）
https://www.npa.go.jp/bureau/security/economic-security/index.html

経済安全保障の確保に向けて2022～技術·データ·製品等の流出防止～（公安調査庁）
https://www.moj.go.jp/psia/keizaianpo.leaflet.html

技術開発　～日本の安全保障に貢献する～

- 国家間での技術の覇権争いや、重要物資の確保に関する駆け引きを背景に、日本では「特定重要技術」や「特定重要物資」を定め、経済安全保障を確保·強化しようとしています。

特定重要技術

- 先端技術の開発競争が激化し、技術や情報の奪い合い·流出が生じています。
- 日本政府は、特定重要技術に該当する技術を持つ事業者·研究機関を対象に、研究プロジェクトの公募·支援を行っています。

海　洋	宇宙・航空	サイバー空間	バイオ	各種先端製造技術	等
ロボット工学（無人機）	先端センサー技術	AI 技術	量子技術	先端エネルギー技術	

参考：経済安全保障重要技術育成プログラム（通称：K Program）（内閣府）https://www8.cao.go.jp/cstp/anzen_anshin/kprogram.html

特定重要物資

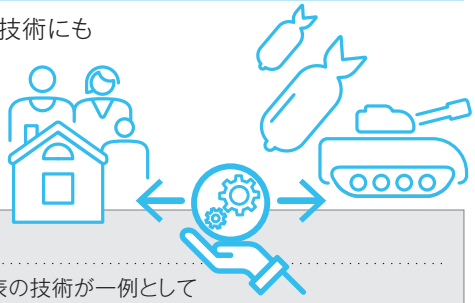
- 供給が途絶えると、安全·安心な暮らしや経済活動が脅かされることに繋がる重要物資があります。
- 該当する物資を供給する事業者には、助成·利子補給·融資などの支援措置が用意されています。

抗菌性物質製剤	肥　料	永久磁石	工作機械・産業用ロボット	航空機の部品	船舶の部品
半導体	蓄電池	クラウドプログラム	天然ガス	重要鉱物	

参考：重要物資の安定的な供給の確保に関する制度（内閣府）https://www.cao.go.jp/keizai_anzen_hosho/supply_chain.html

平和を脅かすことに
間接加担するリスクが拡大中

新規事業・新規開発を行う　～その技術は機微技術?～



- 新規事業や新規開発にチャレンジする際、もしかしたら軍事技術にも転用できる領域の取り組みとなっているかもしれません。
- 近年、「デュアルユース」と呼ばれる軍民両用の技術について、整理が進んでいます。どのような技術が該当するのか、把握をしておきましょう。

デュアルユース（軍民両用）の技術、特許非公開制度

- 日本における、デュアルユース（軍民両用）の技術に関しては、下表の技術が一例として挙げられます。「将来の戦闘様相を一変させかねない武器に用いられ得る先端技術や、宇宙・サイバー等の比較的新しい領域における深刻な加害行為に用いられ得る先端技術等」が列挙されています。
- 日本や日本国民の安全を損なう恐れの大きい発明・技術は、下表の技術を一例に「特定技術分野」として定められました。
- 当該技術に関する特許出願を行い、保全審査の対象になり安全保障上拡散すべきでないと判断されると、出願内容は非公開の扱いになります。出願人等は実施・開示・適正管理等に関する保全措置を講じる必要が生じます。実施には国の許可が必要となり、外国出願が原則禁止となる一方、先願の地位を確保できたり、損失の補償がなされる制度が、2024年より運用開始となります。

我が国の安全保障の在り方に多大な影響を与え得る先端技術が含まれ得る分野	
航空機等の偽装・隠ぺい技術	スクラムジェットエンジン等に関する技術
武器等に関係する無人航空機・自律制御等の技術	固体燃料ロケットエンジンに関する技術
誘導武器等に関する技術	潜水船に関する技術
発射体・飛翔体の弾道に関する技術	無人水中航走体等に関する技術
電磁気式ランチャを用いた武器に関する技術	音波を用いた位置測定等の技術であって潜水船等に関するもの
例えばレーザ兵器、電磁パルス（EMP）弾のような新たな攻撃又は防御技術	宇宙航行体の熱保護、再突入、結合・分離、隕石検知に関する技術
航空機・誘導ミサイルに対する防御技術	宇宙航行体の観測・追跡技術
潜水船に配置される攻撃・防護装置に関する技術	量子ドット・超格子構造を有する半導体受光装置等に関する技術
音波を用いた位置測定等の技術であって武器に関するもの	耐タンパ性ハウジングにより計算機の部品等を保護する技術
	通信妨害等に関する技術

出典：経済安全保障法制に関する有識者会議 第7回（2023年6月）資料2 特許出願の非公開制度の運用開始に向けた検討状況について

※上表右列の技術は、発明の経緯、研究開発の主体等の状況に応じて、保全審査の対象となるか否かが決定されます。

セキュリティ・クリアランス制度

- 軍事転用可能な機微な技術情報をはじめ、政府が保有する「安全保障上重要な情報として指定された情報（CI:Classified Information）」にアクセスする必要がある政府職員や、民間事業者の従業者等に対して、政府による調査を実施し、当該者の信頼性を確認した上でアクセスを認める「セキュリティ・クリアランス制度」について、日本における導入が議論されています。
- 民間で事業を展開していく上で、CIに関与する場合、特別の情報管理ルールを定めて運用していく必要があります。通例としては、当該情報を漏洩した場合には厳罰が科されることとなっています。

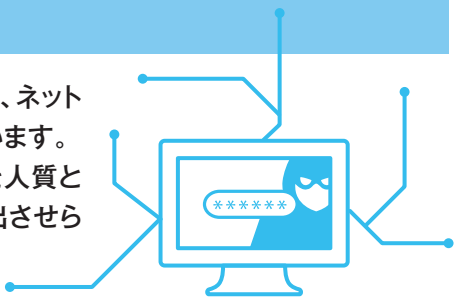
詳細情報

経済安全保障法制に関する有識者会議 第7回　「特許出願の非公開に関する基本指針（案）」、「特許出願の非公開制度の運用開始に向けた検討状況について」　（内閣官房）
https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/4index.html

経済安全保障分野におけるセキュリティ・クリアランス制度等に関する有識者会議「中間論点整理」　（内閣官房）
https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo_sc/index.html

C サイバーセキュリティ・DX

□ サイバー空間にも戦争・無差別テロの影響が及んでおり、ネットに繋がる全ての事業者のシステムが攻撃対象となっています。
□ システムダウンに伴う操業の停止や、システムや情報を人質とした身代金の要求、漏らしてはいけない情報・技術が流出させられるなどの事件が発生しています。



実例1 休み明けに大量のメールを確認しなければならない中、取引先からのメールの添付ファイルを開封した。実際は取引先になりすましたウイルス付きメールであり、メールアカウントを乗っ取られたほか、メールボックス内の情報やブラウザの認証情報、ネットワークの認証情報が流出してしまった。

参考：インターネットの安全・安心ハンドブックVer 5.00<中小組織向け抜粋版>（内閣官房）
https://security-portal.nisc.go.jp/guidance/handbook.html

実例2 リモートデスクトップ接続に脆弱性があり、攻撃者が侵入後に管理者権限を取得してID・パスワードを窃取し、9台へ不正接続を行い、うち6台がランサムウェア（身代金要求型ウイルス）によって、ファイルにロックがかけられ、事業がストップしてしまった。

参考：独立行政法人情報処理推進機構　11.コンピュータウイルス・不正アクセスの届出事例［2022年上半期（1月～6月）］
https://www.ipa.go.jp/security/todokede/crack-virus/about.html

まずは現場でできることを、全社意識の改めとともに

- サイバーセキュリティ対策を行う上では、従業員一人一人の意識・モラルを高めることが重要です。
- 社内外での出来事（インシデント）を共有しつつ、まずは下表に示す基本的な知識・対策について、社内への周知・展開を行いましょう。

OSやソフトウェアは常に最新の状態にする	偽メール・偽サイトに騙されないよう注意する
ウイルス対策ソフトを導入する	メールの添付ファイルや本文中のリンクに注意する
パスワードを強化する、多要素認証を利用する	外出先では紛失・盗難・覗き見・聞き耳に注意する
ファイルの共有設定や情報の公開範囲を見直す	大切な情報は失う前にバックアップをする
脅威や攻撃の手口を知る	困った時は相談をする

参考：インターネットの安全・安心ハンドブックVer 5.00<中小組織向け抜粋版>（内閣官房）

何をすればよい?

- サイバーセキュリティ対策として実施すべき事項として、「特定→防御→検知→対応→復旧」という一連のプロセスがあることを認識しましょう。
- 会社としてサイバーセキュリティに対処できるよう、経営者自身も含めて、関わる管理職・担当者がだれか、社内で相談をしましょう。

これらの、見通しを持ちましょう

Identify 特定 → Protect 防御 → Detect 検知 → Respond 対応 → Recover 復旧

参考：NIST（米国国立標準研究所）サイバーセキュリティフレームワーク
https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-20/ipd

もう少し詳しく

- サイバーセキュリティに関する、代表的な対策としては以下のようなものが考えられます。
- 組織のリスク管理責任者である経営者自身が、現状・課題の把握、対策方針の検討、予算や人材の割当等を通じてリーダーシップを発揮することが求められます。

Identify 特定	サイバーセキュリティ**リスクの認識、組織全体での対応方針の策定**	• 対応方針（セキュリティポリシー）の作成 • 対応方針の社内周知・社外公開
	サイバーセキュリティ**リスクの把握とリスク対応に関する計画の策定**	• 経営上重要な情報を特定・把握 • 様々なリスク種別に応じた対策の想定
	ビジネスパートナーや委託先等を含めた**サプライチェーン全体の対策及び状況把握**	• 各社が、サイバーセキュリティ対策上の責任・役割を理解し、対策漏れを予防
	サイバーセキュリティに関する**リスク管理体制の構築**	• 自社内で対応する事項と、外部の専門人材に任せるものを切り分け
	サイバーセキュリティ対策のための**資源（予算、人材等）確保**	• セキュリティの人材育成費・人材活用費の確保 • 事業遂行の安全担保に必要なIT費用の確保
Protect 防御	サイバーセキュリティリスクに**対応するための仕組みの構築**	• 重要業務を行う端末等には多層防御を実施 • システム停止に備えバックアップや代替手段の確保
Detect 検知	サイバーセキュリティ対策における**PDCA サイクルの実施**	• 必要に応じて、外部の助言・サービスを利用し、現状のシステムやサイバーセキュリティ対策の問題点を検出・改善
Respond 対応	インシデント発生時の**緊急対応体制の整備**	• 緊急連絡網の整備、関係機関・外部専門家の確認 • 証拠保全が行える体制を構築
	情報共有活動への参加を通じた**攻撃情報の入手とその有効活用及び提供**	• システム提供事業者や専門団体の発信情報を、自社のサイバーセキュリティ対策に活かす
Respond 復旧	インシデントによる被害に備えた**復旧体制の整備**	• サイバー攻撃からの復旧手順・復旧体制を想定 • 自然災害等だけでなく、サイバーセキュリティリスクも設備投資計画の要求仕様に反映

NIST（米国国立標準研究所）サイバーセキュリティフレームワークと、
経済産業省サイバーセキュリティ経営ガイドラインver3.0に基づきMURC（株）作成

サイバーセキュリティ対策はDXと両輪で

- デジタル活用を通じて企業の提供価値を拡大させようとするDX（デジタル・トランスフォーメーション）の取り組みが盛んに行われ、その支援も多様になっています。
- DXに関する支援制度を利用する場合、サイバーセキュリティ対策も同時に行える可能性がありますので、攻守両面に配慮した投資計画・事業計画を心がけましょう。

詳細情報

インターネットの安全・安心ハンドブックVer 5.00＜中小組織向け抜粋版＞（内閣官房）
https://security-portal.nisc.go.jp/guidance/handbook.html

サイバーセキュリティ経営ガイドラインと支援ツール（経済産業省）
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

サイバーリスクハンドブック 取締役向けハンドブック 日本版（日本経済団体連合会）
https://www.keidanren.or.jp/policy/cybersecurity/CyberRiskHandbook.html

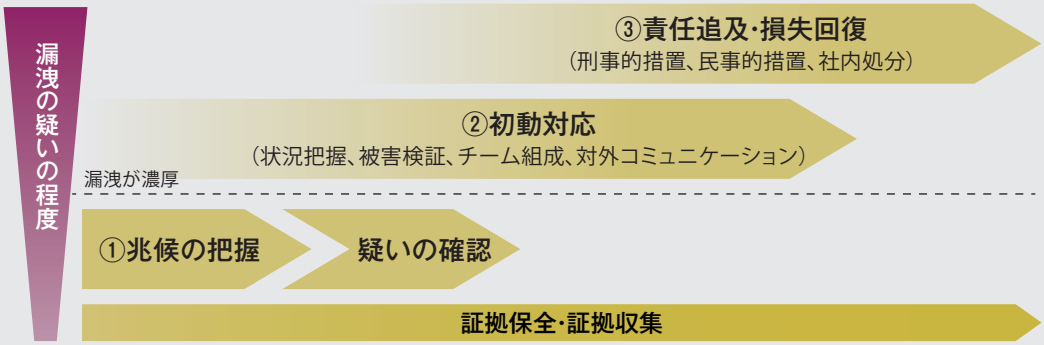
中堅・中小企業等向け「デジタルガバナンス・コード」実践の手引き2.0　（経済産業省）
https://www.meti.go.jp/policy/it_policy/investment/dx-chushoguidebook/contents.html

DXセレクション（経済産業省）
https://www.meti.go.jp/policy/it_policy/investment/dx-selection/dx-selection.html

中部DX推進コミュニティ（中部経済産業局）
https://www.chubu.meti.go.jp/b21jisedai/chubudx/index.html

D 事中・事後対応「兆候把握、初動対応、追及等」

□ サイバー攻撃を始め、情報漏洩・技術流出の手口が高度化されており、情報漏洩を完全に防ぐことは難しくなっています。
□ 万が一、情報や技術が流出した際、迅速に対応できるか否かが、事業運営を左右します。下記3点の対策ポイントを把握しておきましょう。



経済産業省「秘密情報の保護ハンドブック　～企業価値向上にむけて～」を参考にMURC（株）作成

①兆候の把握、疑いの確認

• 以下のような経験・事象はありませんか?疑わしいと思ったら、速やかに情報漏洩を確認しましょう。

兆候の例	「不自然な時間帯に出勤している」、「業務上必要のないアクセスがある」、「秘密情報へのアクセス数が大幅に増えた」、「自社製品の類似品が話題になっている」、「ウイルス対策ソフト等で検知された」、「事業所内で盗聴器を発見した」等
確認方法の例	「サーバーへのアクセスやメールのログ、ダウンロードデータを確認する」、「流出情報の利用が疑われる商品を調べる」、「監視カメラの記録を確認する」、「セキュリティ解析を行い、不正アクセスやサイバー攻撃の有無を確認する」等

②初動対応

• 情報漏洩の疑いを確認し、対応が必要だと判断した場合、できるだけ早く適切な対応を取りましょう。

- 社内調査、状況の正確な把握、原因究明
- 被害の検証（自社・取引先・消費者等への損失を、最悪の事態を想定して検証）
- 初動対応（流出情報の拡散防止、法律に基づく手続き、企業イメージ毀損の最小化等）
- 社内における対策チームの設置、外部専門家のアサイン

③責任追及・損失回復

• 自社被害の回復と、将来的な漏洩抑止のため、責任追及を行います。
• 刑事・民事の片方又は両方の措置を採るかは、相互に関係はなく、警察や弁護士等の専門家に相談しつつ、個別の事情に応じて決定されるものとなります。

詳細情報

秘密情報の保護ハンドブック　～企業価値向上にむけて～　（経済産業省）
https://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html

渉外事案の適用関係の概要と民事訴訟における考えられる主張ポイント集　（経済産業省）
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/202006_pointcollection.pdf

■相談先一覧

気になること、困ったことがあれば、下記の窓口をご活用ください。

相談事項	相談機関	TEL
経済安全保障全般	愛知県 経済産業局 産業部 産業科学技術課 研究開発支援グループ https://www.pref.aichi.jp/soshiki/san-kagi/	052-954-6370
情報・技術流出に関するご相談	愛知県警察本部 https://www.pref.aichi.jp/police/soudan/mail/jumin/kujou.html	052-951-1611
経済安全保障に関するご相談、講演会の実施依頼等	中部公安調査局 https://www.moj.go.jp/psia/kouan_mail_keizaianpo.html	左記URLより お問い合わせください
外国投資家による投資等に関するご相談	東海財務局「対内直接投資審査制度相談窓口」 https://lfb.mof.go.jp/tokai/kigyou/index-tainai.html	052-951-1797
輸出入に関する税関手続き	名古屋税関 業務部 税関相談官室 https://www.customs.go.jp/nagoya/otoiawase/index.htm	052-654-4100
外為法に基づく輸出許可等	中部経済産業局 地域経済部 国際課 https://www.chubu.meti.go.jp/b61boueki/index.html	052-951-4091
サイバーセキュリティ対応	IPA「情報セキュリティ安心相談窓口」 https://www.ipa.go.jp/security/anshin/about.html	03-5978-7509
営業秘密・知財戦略 特許（秘密特許）	INPIT「愛知県知財総合支援窓口」 https://chizai-portal.inpit.go.jp/madoguchi/aichi/	052-753-7635

■関連資料集

経済安全保障に関して、下記の情報もぜひご覧ください。

機関名	情報リソース名（一例）
警　察　庁	技術流出の防止に向けて（パンフレット） https://www.npa.go.jp/bureau/security/economic-security/index.html
公安調査庁	経済安全保障の確保に向けて2022　～技術・データ・製品等の流出防止～ https://www.moj.go.jp/psia/keizaianpo.leaflet.html
	内外情勢の回顧と展望 https://www.moj.go.jp/psia/kouan_kaiko_index.html
	サイバー空間における脅威の概況2023 https://www.moj.go.jp/content/001396422.pdf
内閣官房	経済安全保障法制に関する有識者会議　会議資料 https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/4index.html
内　閣　府	研究インテグリティの確保に係る対応方針（概要） https://www8.cao.go.jp/cstp/kokusaiteki/integrity.html
N I S C	インターネットの安心・安全ハンドブック Ver 5.00（中小組織向け抜粋版） https://security-portal.nisc.go.jp/guidance/handbook.html
経済産業省	営業秘密関係の基本資料 https://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html
	安全保障貿易管理とは（説明会資料、安全保障貿易管理ガイダンス） https://www.meti.go.jp/policy/anpo/gaiyou.html
	外国投資家から投資を受ける上での留意点について https://www.meti.go.jp/policy/anpo/shiryo-toushikanri.pdf
	サイバーセキュリティ経営 ガイドライン・手引き https://www.meti.go.jp/policy/netsecurity/mng_guide.html
J E T R O	地域・分析レポート「経済安全保障、8割の日本企業が経営課題と認識」 https://www.jetro.go.jp/biz/areareports/special/2022/1002/2c2eecd972c6c47e.html
I N P I T	海外展開知財支援窓口 eラーニング教材 https://faq.inpit.go.jp/gippd/service.html
I　P　A	サイバーセキュリティ経営 プラクティス集 https://www.ipa.go.jp/security/economics/csm-practice.html
	中小企業の情報セキュリティ対策ガイドライン https://www.ipa.go.jp/security/guide/sme/about.html
	情報セキュリティ白書 https://www.ipa.go.jp/publish/wp-security/index.html
総　務　省	ICTサイバーセキュリティ総合対策2023 https://www.soumu.go.jp/main_content/000895981.pdf

発行：愛知県（協力：三菱UFJリサーチ&コンサルティング株式会社）

本書の内容は2023年10月時点の情報に基づいています。