■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	電話連絡先等
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://www.mof.go.jp/policy/international_policy/gaitame_kawase/fdi/index.htm	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「企業組織向けサイバーセキュリティ相談窓口」 https://www.ipa.go.jp/security/support/soudan.html	cs-support@ipa.go.jp
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/	0570-082100 （ナビダイヤル）

※全国47都道府県に設置されたお近くのINPIT知財総合支援窓口に自動でおつなぎいたします。

■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　～技術・データ・製品等の流出防止～ https://www.moj.go.jp/psia/keizaianpo.top.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 https://www.moj.go.jp/psia/20130807.html
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
	インターネットの安全・安心ハンドブックVer 5.10<中小企業等向け抜粋版> https://security-portal.cyber.go.jp/guidance/handbook.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
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
	技術流出対策ガイダンス 第1版 https://www.meti.go.jp/policy/economy/economic_security/guidance.pdf
	経済安全保障上の課題への対応（民間ベストプラクティス集）ー第2.0版ー https://www.meti.go.jp/policy/economy/economic_security/best_practice2.0.pdf
	経済安全保障経営ガイドライン（第1版） https://www.meti.go.jp/policy/economy/economic_security/260123_guideline.pdf
	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/toushikanri1.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
JETRO	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
INPIT	海外展開知財支援窓口 eラーニング教材 https://www.inpit.go.jp/jinzai/ipeplat/index.html
IPA	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政策の中期重点方針 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00219.html
財　務　省	対内直接投資審査制度について https://www.mof.go.jp/policy/international_policy/gaitame_kawase/fdi/index.htm

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2026年1月時点の情報に基づいています。

経済安全保障 中小企業向け 入門ガイド

愛知県

第２版
2026年1月改訂版

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。

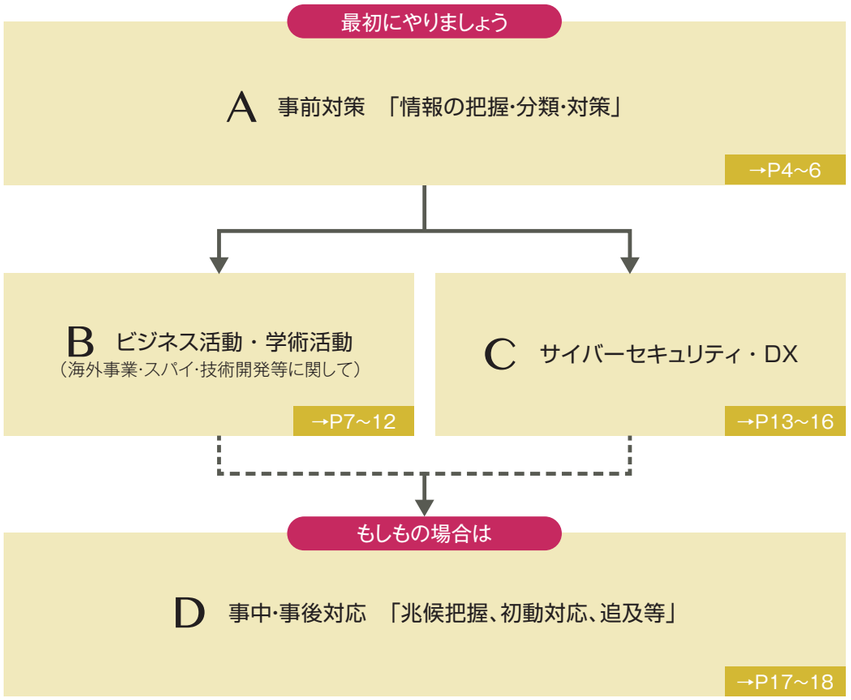
愛知県では、2022年5月に成立した経済安全保障推進法の施行に伴い、技術情報管理を始めとする経済安全保障を推進し、日本一のものづくりの集積地として、実効性のある地域の備えを構築すべく、2022年10月に「愛知県経済安全保障に関する協議会」を創設しました。

また、県内事業者を対象にシンポジウムやセミナーを開催し、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・改訂しました。第2版の制作においては、初版制作後の経済安全保障に係る社会情勢や各省庁が新たに策定した指針、法令改正等の情報を反映しています。

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に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。

本書の構成



目　次

3 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～
4 A.事前対策 「情報の把握・分類・対策」
7 B.ビジネス活動・学術活動
13 C.サイバーセキュリティ・DX
17 D.事中・事後対応 「兆候把握、初動対応、追及等」
巻末 相談先一覧、関連資料集

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中心に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。

情報の奪い合い	サイバー空間にも及ぶ戦争･無差別テロ	兵器生産･備蓄のための国際取引が横行	軍事転用できる技術の広がり	技術の覇権争い	重要物資の断絶リスク
✓ 漏れるとまずい情報･技術が各社あります。	✓ ネット環境がありますか?	✓ 技術やサービスを輸出しますか?	✓ 軍民両用技術に関わりますか?	✓ 先端技術に関わりますか?	✓ 重要物資を供給しますか?
秘密情報/営業秘密管理 →P4	サイバーセキュリティ →P13	輸出管理 →P11	特許出願の非公開制度 →P10	特定重要技術 →P8	特定重要物資 →P8

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（P9）、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、④社内のルール整備･研修を行います。

① 保有情報の把握 → ② 情報の分類 → ③ 分類に応じた対策 → ④ 社内のルール整備･研修

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。

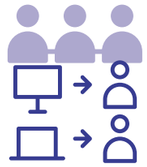
公開（オープン）	or	秘密（クローズ）
部品構造（容易に把握可能） 動作性能評価方法		生産プロセス 素材配合 顧客情報･個人情報

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

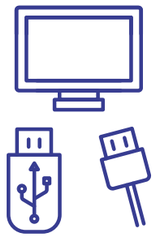
物理的・技術的な防御



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

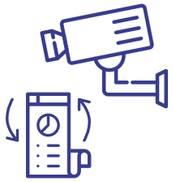
■情報の持ち出しを物理的・技術的に防ぎましょう。

□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

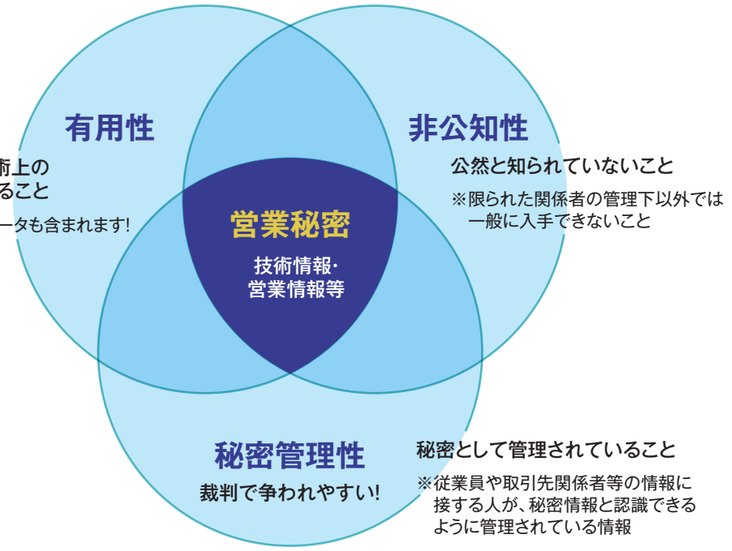
■従業員が情報漏洩をしようという気持ちにならないための対策が重要です。働きやすい職場環境を整備し、仕事へのモチベーション向上を通じ、従業員のモラルを高めましょう。

□ワークライフバランスの推進や適正な評価
□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

④社内のルール整備・研修

他国への技術流出につながるリスクが拡大中

- 保護すべき技術やノウハウ等の情報は、以下の「3要件」を全て満たすと「営業秘密」として法律（不正競争防止法）で保護されます。
- 流出を防ぎたい情報が真に守られる状態となっているのかを確認するために、専門家や 支援機関（ INPIT 知財総合支援窓口等）を利用することも検討しましょう。
- 支援機関等を利用しつつ、社内ルール（営業秘密管理規程・情報管理規程）を整備することで、従業員への流出抑止や紛争時の立証等の面で効果が期待されます。



詳細情報

秘密情報の保護ハンドブック～企業価値向上に向けて～（経済産業省）
【てびき】秘密情報の保護ハンドブック　（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

生産拠点の海外進出に伴う技術流出への対策

- 海外拠点で生産や製品開発を行う場合、日本国内のみで事業活動を行う場合に比べて、技術流出の対策に向け、さらに下記のポイントなどに注意することが求められます。

■体制整備・事前調査
- 日本社内の情報管理体制の整備　- 相手国の制度の確認、相手国の技術的関心の確認
- 相手国の労働法制・慣習・雇用情勢等の確認　- 情報管理体制等に関する取引先DD（デューデリジェンス）の実施

■将来を見据えた対応
- 技術情報提供後の情報管理の徹底　- 製造設備のメンテナンス管理の徹底
- 撤退計画に対応した適切な情報管理の徹底　- 製造設備の適切な管理・処分
- 撤退後のフォローアップ

■開示領域の選定
- 技術情報の取扱いに係る遵守事項の明確化　- コア技術の特定、提供技術の内容等の明確化
- 段階的な技術提供、情報のブラックボックス化

参考:技術流出対策ガイダンス 第1版　https://www.meti.go.jp/policy/economy/economic_security
経済安全保障上の課題への対応（民間ベストプラクティス集）－第2.0版－（経済産業省）
https://www.meti.go.jp/policy/economy/economic_security/index.html

B ビジネス活動・学術活動

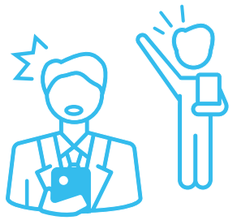
□ 事業展開の可能性を高めたり、事業収益の拡大を図るためには、共同研究の実施、海外輸出、合弁企業の設立などを他国や他国企業と関わりながら行うことも、今日のビジネスシーンでは、重要な選択肢です。
□ そうした活動をはじめ、ビジネスシーンにおいて、経済安全保障に関連してどのようなリスクがあるのか、また国はどのような支援策を講じているのか、主なポイントを押さえておきましょう。

スパイ工作

他国への技術流出につながるリスクが拡大中

〈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　～技術·データ·製品等の流出防止～
https://www.moj.go.jp/psia/keizaianpo.top.html

技術開発　～契約で技術·知財の流出を防ぐ～

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。

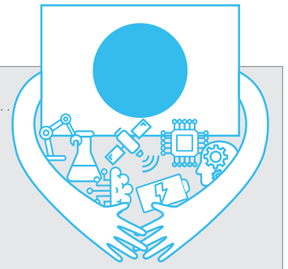
実例1	共同開発で開発の多くを日本側が実施したにもかかわらず、成果である特許権は共有となり、その後、相手方が製造受注を独占するようになってしまった。
実例2	海外では雇用の流動性が高く、独資·合弁企業の従業員が競合へ転職し、ノウハウが流出した。

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

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
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

等

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、船体
半導体	蓄電池	クラウドプログラム	天然ガス	重要鉱物	
先端電子部品（コンデンサー·ろ波器·磁気センサー）	人工呼吸器	無人航空機	人工衛星	ロケットの部品	

参考：サプライチェーン強靱化の取組（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/suishinhou/supply_chain/supply_chain.html

技術開発　～革新的技術の国際共同研究開発～

重要経済安保情報保護活用法（≒経済安保分野のセキュリティ・クリアランス制度）

- 民間事業者が、行政機関から重要経済安保情報の提供を受けるために、民間の事業者と従業者の適格性を認定する制度が2025年5月に施行されました。
- 革新的な国際共同研究開発に参画する場合において、技術情報へのアクセスをするための要件となるケースも想定されています。

重要経済安保情報の具体例

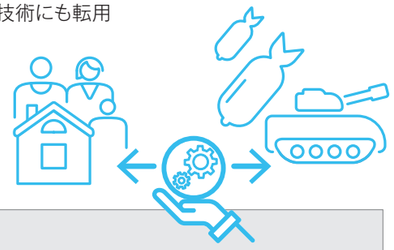
• 日本の重要なインフラ事業者の活動を停止又は低下させるようなサイバー攻撃等の外部からの行為が実施された場合を想定した政府としての対応案の詳細に関する情報
• 日本にとって重要な物資の安定供給の障害となる外部からの行為の対象となりかねないサプライチェーンの脆弱性に関する情報
• 日本政府と外国政府とで実施する安全保障に関わる革新的技術の国際共同研究開発において、外国政府から提供され、当該外国において本法による保護措置に相当する措置が講じられている情報

参考:重要経済安保情報保護活用法の概要
https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/hogokatsuyou.html

新規事業・新規技術開発　～デュアルユース（軍民両用）の技術～

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）の技術の一例

- 海外への輸出等の局面や、技術の特許化の局面などにおいて、デュアルユース（軍民両用）の技術は取り扱いに注意がなされる必要があり、法令順守が求められます。
- 一方、防衛分野においては、先端的な民生技術の活用が必要とされることが多い側面もあり、スタートアップ企業や中小企業にとってもビジネスチャンスと捉える動きがあります。

民生技術	軍事用途
商用ドローン・ロボット	偵察機・無人攻撃機
ろ過器	細菌兵器製造のための細菌抽出
合成繊維	化学兵器の防護服
センサー	索敵・探知、戦況監視
暗号技術	秘匿通信、機密情報の秘匿

参考:デュアルユース・スタートアップのエコシステム構築に向けて（防衛装備庁・経済産業省）
https://www.meti.go.jp/policy/mono_info_service/mono/aerospace/5_startup.pdf

特許出願の非公開制度

- 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の運用が開始されました。

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。

詳細情報

特許出願の非公開制度（特許庁）
https://www.jpo.go.jp/system/patent/shutugan/hikokai/index.html

特許出願の非公開制度（内閣府）
https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/patent/patent.html

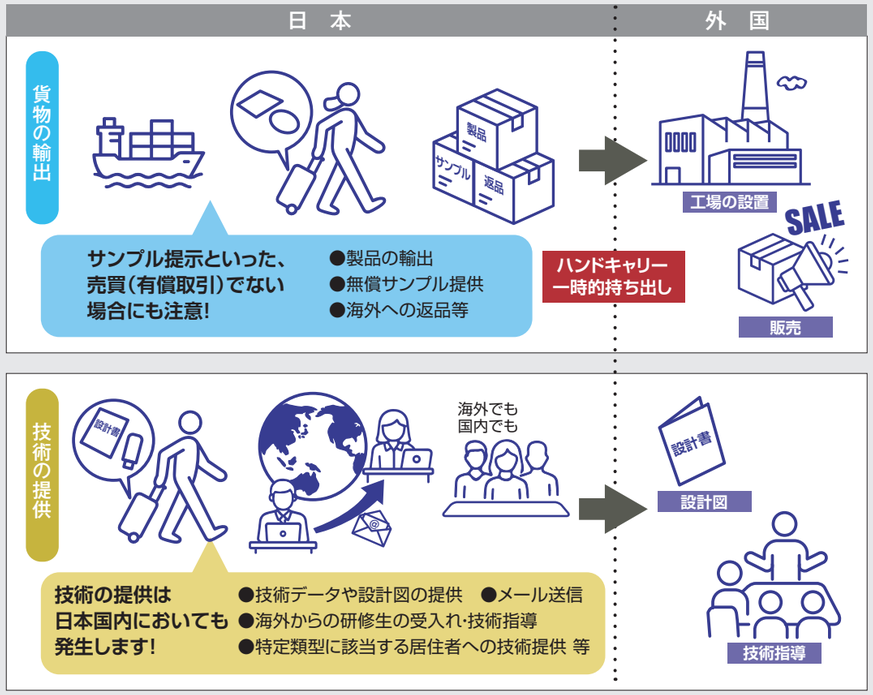
海外との取引･連携　～輸出管理（安全保障貿易管理）～

- 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（2025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

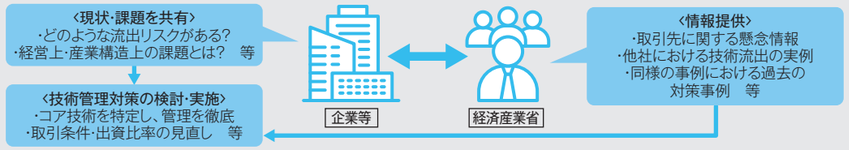
輸出管理の基礎（一般社団法人 安全保障貿易情報センター）
https://www.cistec.or.jp/export/yukan_kiso/index.html

安全保障貿易管理　～技術管理強化のための官民対話スキーム～

- 安全保障上の観点から管理を強化すべき、指定された重要な技術（※2025年11月時点で19種）について、国外（非居住者）への「技術移転」が生じる場合には、技術移転の契約前に経済産業省への簡易な書式で報告することが、外為法に基づき義務づけられています。

積層セラミックコンデンサ	巨大磁気抵抗効果若しくはトンネル磁気抵抗効果を利用するセンサー（素子、素子周辺の磁気回路又は磁気回路を制御するための構成物）
弾性表面波フィルタ又はバルク弾性波フィルタ	スポンジチタン
電解銅箔	リチウムイオン電池の正極集電体又は負極集電体と活物質等を固定又は結合させる目的で使用される物質
誘電体フィルム	リチウムイオン電池の材料として使用される硫化物固体電解質
チタン酸バリウム粉体	リチウムイオン電池のセパレータの製造に用いられる二軸押出機の部分品（スクリュー構成）
炭素繊維のプリカーサー	量子ドット
炭化ケイ素繊維のプリカーサー	有機ELディスプレイに用いられる熱活性化遅延蛍光特性を有する材料
非鉄金属のターゲット材	位相差フィルム
走査型電子顕微鏡又は透過型電子顕微鏡	軟性内視鏡（先端硬性部の直径が16ミリメートル以下のもの）の挿入部

- 事前報告の対象となる場面としては、他国での製造、製品開発を可能とする技術移転（現地子会社･合弁会社への製造移転、他国企業への製造委託･ライセンス供与など）が対象となります。
- 技術移転を止めることではなく、適切な技術管理を徹底することが目的されているため、官民が対話を通じて現状や課題を共有した上で、官側からの情報提供や助言がなされるほか、政策的支援策の模索がなされる仕組みとなっています。



参考：安全保障貿易の概要>技術管理強化のための官民対話スキーム（経済産業省）　https://www.meti.go.jp/policy/anpo/anpo08.html

海外との取引･連携　～対内直接投資審査制度～

- 防衛･先端技術･インフラ･情報等の産業をはじめ、経済安全保障に関わる指定業種の日本企業（上場･非上場）においては、外国投資家から投資等を受ける場合に、財務省･所管省庁へと事前に届出を行い、審査を受けることが求められます。
- 主に「投資家の属性」「業種」「投資等（の類型）」の観点で、事前届出（事前審査）が必要かを判断していきます。
- 事前届出が必要か否かの判断基準は随時更新される可能性があるため、最新の法令･財務省資料を確認しましょう。なお、各地域の財務局に相談をすることも選択肢です。

■外国投資家 に該当しますか?
① 非居住者である個人
② 外国法令に基づき設立された法人その他の団体
③ ①･②に株式･議決権の過半数を保有されている会社
④ ①･②が50%以上出資する組合又は業務執行組合員の過半数を占める組合 等
⑤ ①が役員の過半数を占める法人その他の団体

外国人投資家の一例
- 日本以外の国･地域に居住する個人（日本国籍を有する者も含む）
- 外国で設立された法人やファンド、外国に主たる事務所を有する法人
- 外国法人の本邦における100%子会社
- 外国法人が50%以上出資する投資ファンド　等

■投資等 に該当しますか?
- 株式･持分の取得
- 上場会社の総議決権の1%以上の取得
- 非上場会社の1株以上の株式取得 ※端株の取得も含む
- 事業目的の実質的な変更、役員の就任等の経営上重要な事項に関して行う同意
- 支店等の設置等
- 償還期間が1年を超える金銭の貸付
- 事業の譲受け　等

投資等の行為の一例
- 上場会社の株式を10%まで買い増す場合
- 外国投資家自ら又はその関係者が役員に就任することについて、株主総会において同意する場合
- 外国投資家が事業承継する場合　等

■業種 は該当しますか?

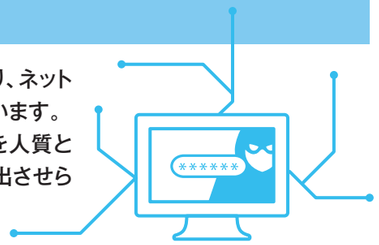
指定業種に該当するか否か、下記財務省HPをご参照ください。

詳細情報

対内直接投資審査制度について（財務省）
https://www.mof.go.jp/policy/international_policy/gaitame_kawase/fdi/index.htm

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。

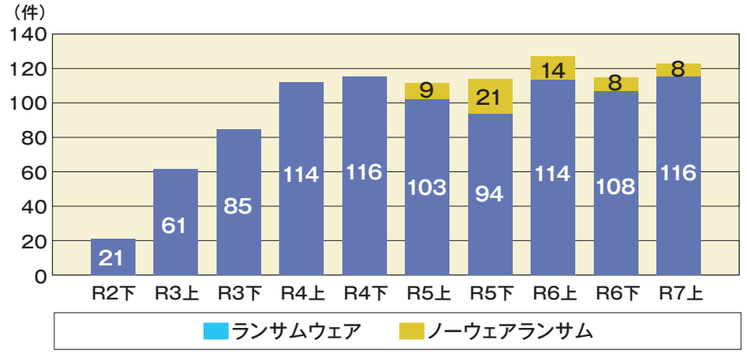
参考：インターネットの安全・安心ハンドブックVer 5.10 <中小企業等向け抜粋版>
https://security-portal.cyber.go.jp/guidance/handbook.html

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

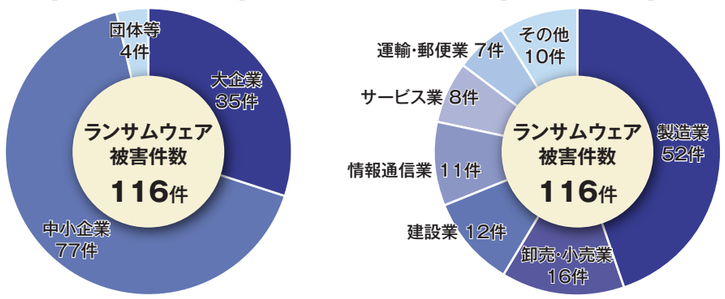
企業・団体等における被害の報告件数の推移

※ ノーウェアランサムの被害については、令和5年上半期から集計。



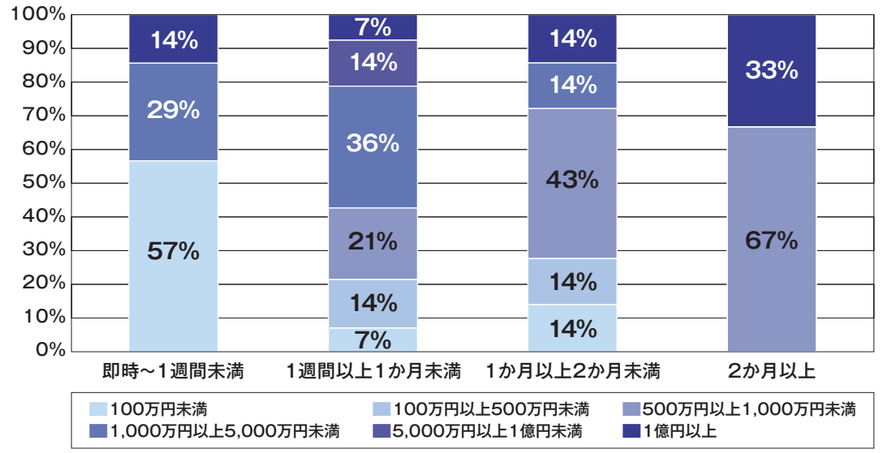
出典：令和7年上半期におけるサイバー空間をめぐる脅威の情勢等について（警察庁）
https://www.npa.go.jp/publications/statistics/cybersecurity/index.html

被害企業・団体等の規模別／業種別報告件数



出典：令和7年上半期におけるサイバー空間をめぐる脅威の情勢等について（警察庁）
https://www.npa.go.jp/publications/statistics/cybersecurity/index.html

ランサムウェア被害からの復旧期間と費用の関係性



※ 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：令和7年上半期におけるサイバー空間をめぐる脅威の情勢等について（警察庁）
https://www.npa.go.jp/publications/statistics/cybersecurity/index.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 5.10 <中小企業等向け抜粋版>
https://security-portal.cyber.go.jp/guidance/handbook.html

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
Protect 防御	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
	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に基づき三菱UFJリサーチ&コンサルティング（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 5.10 <中小企業等向け抜粋版>
https://security-portal.cyber.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

TICS（技術情報管理認証制度）（経済産業省）

- サイバーセキュリティだけでなく、人的対策・物理対策も含めた、総合的な情報管理の体制構築を支援する事業である「技術情報管理認証制度（TICS:Technology Information Control System）」を経済産業省が実施しています。
- 認証機関の指導・助言を受けつつ情報管理の対策を進めることができるとともに、対策をした情報管理体制を客観的に審査・認証されることで、取引先からの信頼性向上などが期待されます。

認証マーク

Ⅰ 共通項目	
1	自社の情報セキュリティ対応方針の策定及び周知を実施している。
2	守るべき情報を特定し、ファイル名の一部や文書の冒頭にマル秘マークやラベルを付する等により、他の情報と識別ができるようにしている。
3	守るべき情報や情報機器の機密性に応じた管理方法を規則に定め、それに従って管理している。
4	情報セキュリティの責任者を選任し、情報セキュリティ事件・事故時の対応を行う体制や手順を整備している。
5	従業員に対して、注意すべき情報管理と基本的な情報セキュリティに関する社内教育を行っている。
6	守るべき情報が流出したり、暗号化されて使えなくなった場合に、自社が受ける影響や被害をシミュレーションしている。
7	自社のパソコン等の機器が外部情報システム（サプライヤー等の関係団体の情報システムやクラウドサービス等）に接続している場合は、接続状況やデータの流れを把握している。
8	取引先などから提供を受けた情報は、その取引先の意向を踏まえた、情報漏えい防止対策を行っている。
9	守るべき情報の持出し、複製、廃棄等の状況を管理するための管理簿を作成し、施錠したロッカー内やアクセス権が厳重に管理されたサーバー領域等で適切に保管している。
10	守るべき情報を廃棄する場合には、守るべき情報の形態やその性質に応じて、復元不可能な方法により廃棄をしている。
Ⅱ アクセス権	
11	守るべき情報へのアクセスについてのルールを設け、必要最小限のアクセス権を設定し、アクセス権を設定した者との間で当該ルールの遵守を含む秘密保持に係る誓約書の取得等を行っている。
12	守るべき情報を施錠された区域で保管し、鍵や警備体制等を適切に管理するとともに、守るべき情報を持ち出す際の手順を定めている。
13	守るべき情報にアクセスする場合のパソコンへのログイン方法等の利用手順を定め、ログインIDやパスワードを適切に保管している。
14	サーバ等が施錠等された区域に設置されている。
15	守るべき情報を取り扱う情報システム（クラウド含む）は、信頼できるメーカーやベンダーによって構築されており、必要なサポートを受けられる体制が構築されている。
16	パソコン等への不正なアクセスに対応するため、OS等を常に最新の状態にし、ウイルス対策ソフトを常時稼働させている。
17	守るべき情報を外部に送信する場合には、電子メールの添付文書の暗号化や誤送信防止の手順を踏まえて適切に送信されている。
18	守るべき情報が保存されたパソコンや記録媒体の持ち出しを管理している。
19	守るべき情報を取り扱う情報システムの保守や点検を第三者に行わせる場合に、秘密保持契約を締結し、作業時には従業員を立ち会わせている。
Ⅲ 守るべき情報を外部委託先などに渡す場合	
20	守るべき情報を外部委託先や取引先等に取り扱わせる場合、外部委託先等の情報管理体制を確認し、秘密保持契約等を結んでいる。

出典：TICS（技術情報管理認証制度）（経済産業省）
https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/

サプライチェーン強化に向けたセキュリティ対策評価制度（案）（2025年12月時点）

- 取引先に影響を与えるようなサイバー攻撃が発生していることを背景に、サプライチェーン全体でのサイバーセキュリティ対策の強化が求められています。
- そこで、各企業のIT基盤に関するセキュリティ対策のレベルを、3段階（★3・★4・★5（※））で評価していくことが予定されています。
- 今後例えば、2社間の取引契約等において、発注元企業が、委託先企業側に適切なセキュリティ対策の段階（例：★3・★4）を提示するとともに、示された対策を促すとともに実施状況を確認することが想定されています。

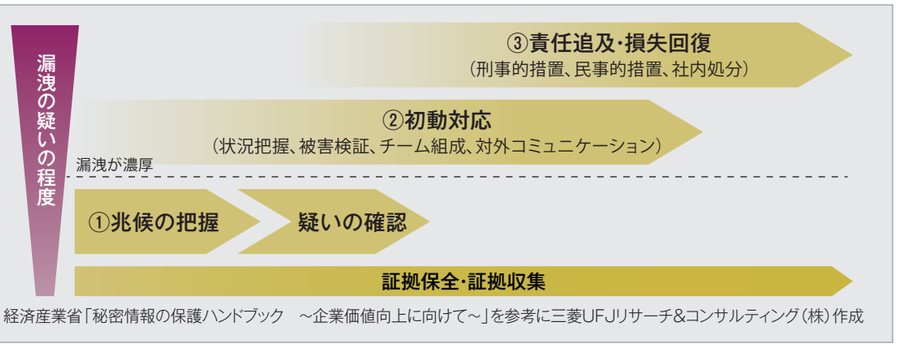
段階	対策の基本的な考え方、評価方法	備考
★3	全てのサプライチェーン企業が最低限実装すべきセキュリティ対策（専門家確認付き自己評価）	基礎的なシステム防御策と体制整備を中心に実施。
★4	サプライチェーン企業等が標準的に目指すべきセキュリティ対策（第三者評価）	包括的な対策を実施。（組織ガバナンス・取引先管理、システム防御・検知及びインシデント対応等）
★5	サプライチェーン企業等が到達点として目指すべき対策（第三者評価）	国際規格等におけるリスクベースの考え方に基づき、自組織に必要な改善プロセスを整備した上で、システムに対しては現時点でのベストプラクティスに基づく対策を実施。

備考：今後、★3及び★4については令和8年度末の制度開始を目指されているとともに、
「サイバーセキュリティお助け隊サービス」（新類型）の創設も予定されています。

（参考）サプライチェーン強化に向けたセキュリティ対策評価制度（案）について（経済産業省）
https://www.meti.go.jp/press/2025/12/20251226001/20251226001.html

D 事中・事後対応「兆候把握、初動対応、追及等」

□ サイバー攻撃をはじめ、情報漏洩・技術流出の手口が高度化しており、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　～企業価値向上に向けて～」を参考に三菱UFJリサーチ&コンサルティング（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。
- 役職員から技術流出した場合には、就業規則に基づく懲戒処分のほか、不正競争防止法に基づく民事上の責任や、雇用契約時の誓約書等に基づく債務不履行責任を追及することも選択肢です。
- 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。
- 国内で管理されている日本企業の営業秘密の侵害が国外で発生した場合、日本の裁判所で不正競争防止法に基づいて訴訟提起できる旨が、令和5年の同法の改正により明確化されています。

証拠の保全・証拠収集について

- 秘密情報の流出に、内部者の関与が疑われる場合、疑いに関する情報は対策チーム等の関係者に限定し、証拠の散逸・隠滅を防ぎましょう。証拠が不十分な段階で、疑わしい従業員へと不用意に接触・事情聴取をすると、証拠隠滅を助長する恐れがあります。
- 漏えいされた秘密情報が「営業秘密」に該当するための要件として、①秘密管理性、②有用性、③非公知性が挙げられます。不正競争行為があったことの証拠となり得るものの一例として、以下のような資料を揃えることができるか、事前に想定をしておきましょう。

営業秘密の要件該当性（特に秘密管理性）の証明に有効な資料の一例

□情報の管理水準が分かる資料（就業規則、情報管理規程、管理状況に関する社内文書等）
□漏えいが疑われる者と自社との間で交わされた秘密保持誓約書
□情報の取扱いに関する社内研修等の実施状況に関する社内記録
□特定の情報に対するマル秘マークの付記、アクセス制限、施錠等の情報の管理状況に関する社内記録（教育マニュアル等）
□漏えいが疑われる者が、漏えいに係る情報が秘密であることを認識できたことを裏付ける陳述書（社内における実際の管理状況、口頭での情報管理に係る注意喚起の状況、示談文書等）

不正競争防止法違反のその他の要件該当性の判断に有効な資料の一例

□漏えいが疑われる者の立場（アクセス権の保有者であったか、会議等で資料を配付された者であったか、外部者であるか）に関する社内記録
□漏えいが疑われる者が自社従業員である場合には、どのような秘密保持に係る任務を負っていたかが分かる就業規則、秘密保持誓約書
□漏えいが疑われる者が委託先である場合、委任契約書、秘密保持契約書
□情報持出しの具体的行為態様が分かるアクセスログ、メールログ、入退室記録、複製のログ
□漏えいが疑われる者の行為目的が窺える他社とのメールや金銭のやりとりに関する書面
□情報漏えいの発覚の経緯を、社内調査等に基づき時系列的にまとめた文書

- 電子情報などは時間経過で失われやすく、時機を逃すと確保できないため、迅速な保全をすべく、社内のシステム担当者と早期に連携を行いましょう。
- 専門家を通さず、自社だけで闇雲に保存を試みると、場合によっては情報破損や改ざん疑いにより証拠価値が失われるリスクがあるため注意が必要です。
- 状況に応じて、警察への相談・通報や専門業者（デジタルフォレンジック解析等）の活用など、専門家・専門機関との連携が安全な対応に繋がることが多いと考えられます。
- 漏えいした秘密情報にインサイダー情報が含まれる場合、外部のフォレンジック解析を支援する担当者にも厳格な秘密保護・管理を求め、インサイダー取引につながらないよう注意しましょう。

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
技術流出対策ガイダンス第1版（経済産業省）
https://www.meti.go.jp/policy/economy/economic_security/

再発防止策の策定・徹底について

情報の漏洩事案が生じた場合、事案の原因を分析し、その根本要因を明確にした上で、再発防止策を策定する必要があります。その上で、社内研修や監査にも反映させ、重点的にチェックをしていく体制を整えることで、対策を徹底していくことが求められます。

漏洩事案の詳細な原因分析	外部弁護士等による社内規程の確認	定期的な研修	監査

参考：技術流出対策ガイダンス第1版（経済産業省）　https://www.meti.go.jp/policy/economy/economic_security/