

# 情報管理も企業力

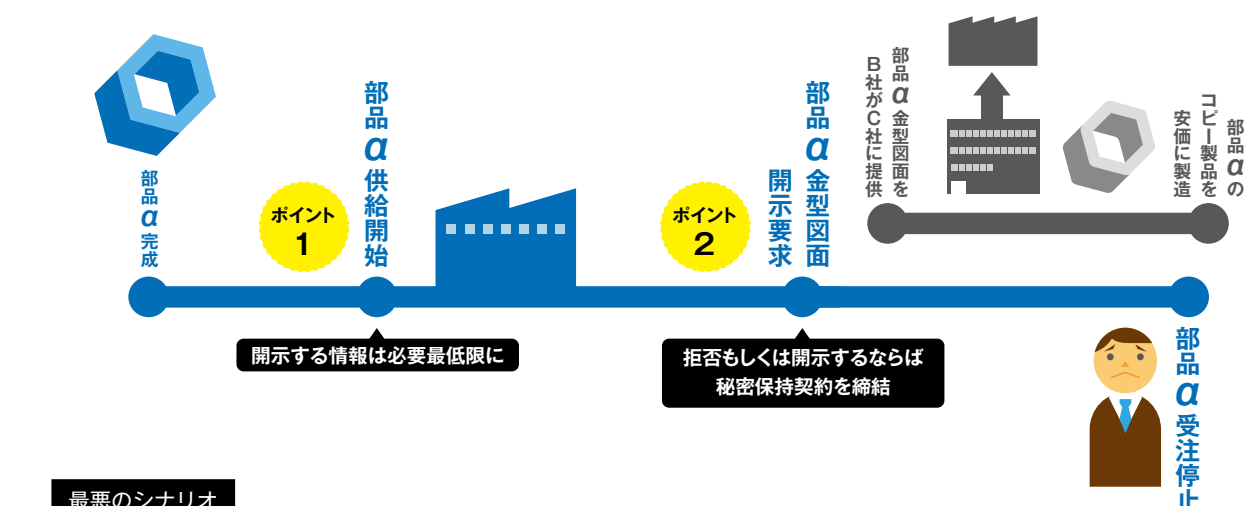
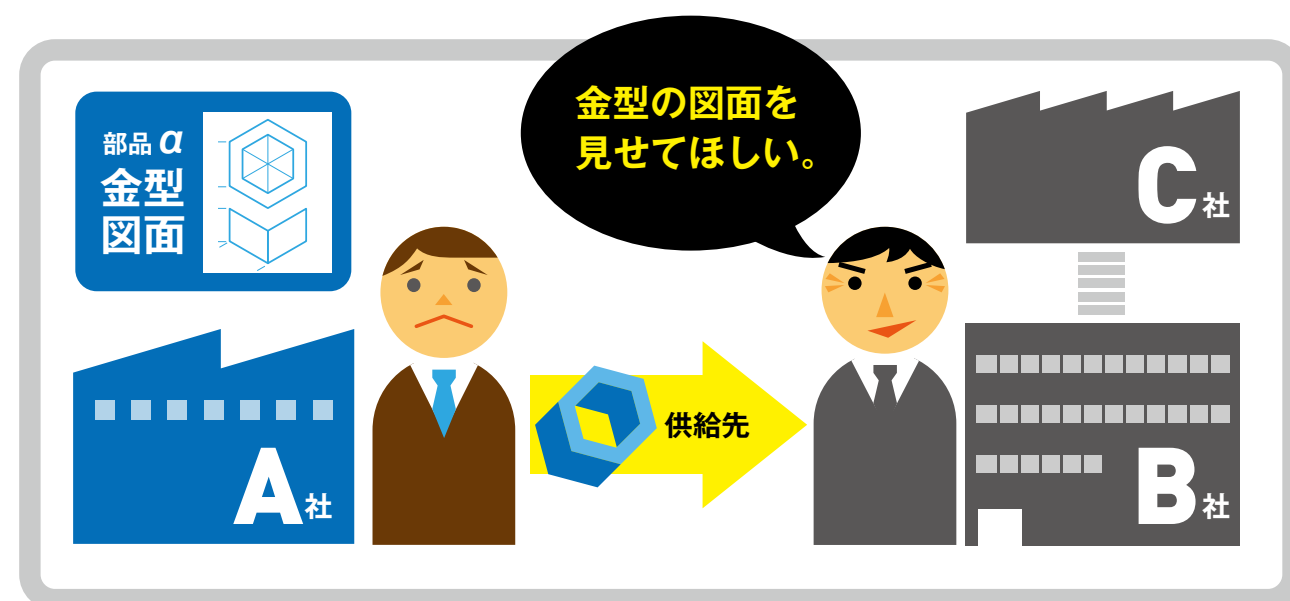
～秘密情報の保護と活用～

秘密情報の保護ハンドブックのてびき



## 大口の取引先から図面を見せてほしいと言われて提示したら……

取引先から求められた図面の提示。大口の取引先だからと泣く泣く提示したけれど、情報を盗まれてしまって……



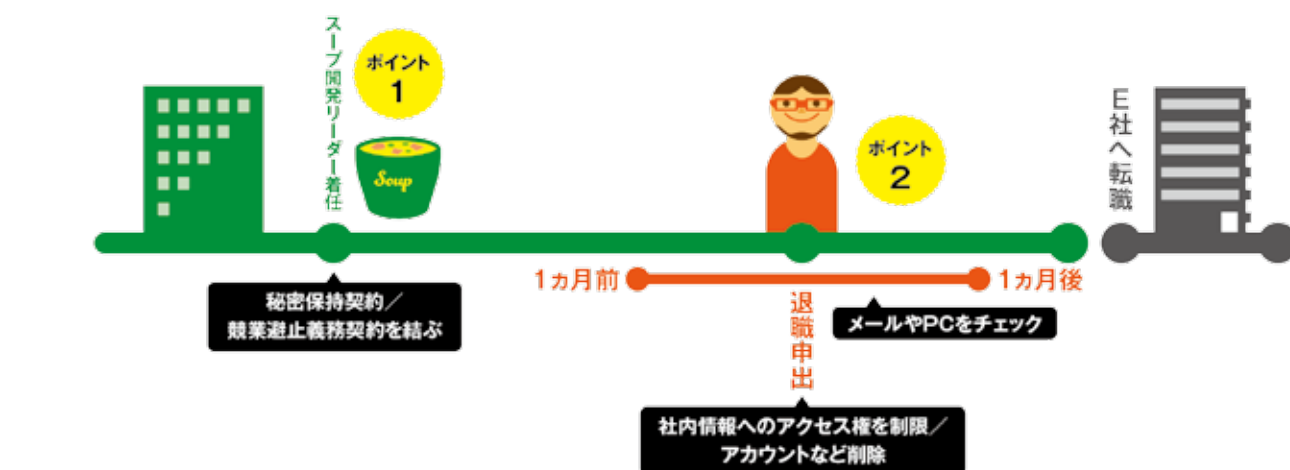
最悪のシナリオ

金型の図面は競合のC社に渡し、安価で部品αのコピーが製造されるようになり、A社への発注がなくなりました！

では、どのような対応をしていればよかったのか？【解説はP.11 CASE 3】

## プロジェクトの開発リーダーだった従業員が退職を申し出てきたが、転職先は競合他社で……

ある日突然退職を申し出てきた従業員の転職先は、なんと競合他社。自社の情報を持ち出すのではないかと不安で……



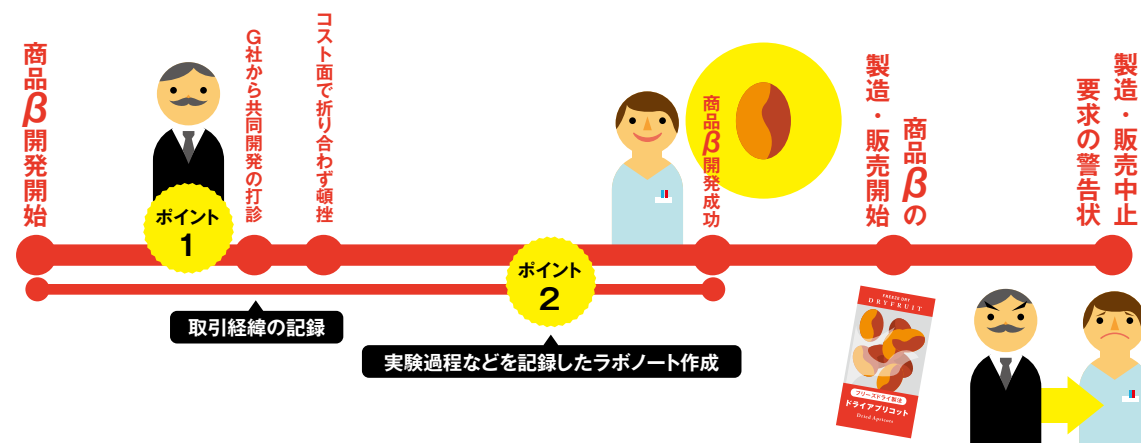
最悪のシナリオ

開発リーダーが持ち出したレシピを活用し、E社はD社よりも安く商品を開発！D社のスープ商品は売れなくなりました！

では、どのような対応をしていればよかったのか？【解説はP.10 CASE 2】

## 自社開発の技術にもかかわらず、 他社から「盗まれた!」と言われた。

自社の技術でつくった商品なのに、過去に一度共同で開発をしたいと売り込みをしてきた他社から「技術を盗んだ!」と言いがかりをつけられた。独自の技術を使用したのだと証明したいけど……



### 最悪のシナリオ

F社独自の技術を使用したと証明することができず、新商品の販売・製造が中止に追い込まれた!

では、無実を証明するにはどのようにすればよいか? 【解説は P.12~ CASE 5】

トラブルに巻きこまれないよう、  
社内の秘密情報をうまく把握し、  
活用させて企業力を高めていきましょう!

「秘密情報なんて自分たちには関係ない」と思っていないですか? 実はそれ、大きな間違いです。

技術情報、営業情報、顧客情報はもちろん、市場分析情報や人事・財務情報などの日頃何気なく扱う情報も立派な「情報資産」です。そしてそれらの「情報資産」の中には、秘密としておくことが最善のものが 있습니다。たとえば、取引価格や顧客情報、技術ノウハウなどは、秘密として保持されることでこそ、他社との差別化を図ることができる情報です。

秘密にしておくべき情報(=秘密情報)は、一度漏えいしてしまうと、資産としての価値が失われるだけでなく、企業経営にも致命的な影響を及ぼしかねません。

ここまでお話ししてきても「狙われるような情報はないし、情報を持ち出されたことなんてない」とお感じの皆さまこそご注意ください! 情報が漏えいしてしまった企業の多くもそのように考えていたのです!

「最近、不必要な休日出勤をする従業員が増えたなあ」  
「長年取引をしてきた会社から突然、理由もなく取引を打ち切られた!」

一見すると無関係なこうした出来事も、もしかしたら、あなたの会社の大切な情報が漏えいしてしまう兆候かもしれません。

重要な情報を適切に守ることは、会社の成長や利益に大きく貢献します。まずは一度、何が大事な情報かを社内で見直し、秘密として保持すべきものを明らかにすることが大切です。その上で、漏えいを予防する適切な対策を講じましょう。重要な情報を適切に守ることは、会社の成長や利益に大きく関わってくるものです。

とはいえ、使ってこそ価値を発揮するのが「情報」。有効利用と管理のバランスを大切に、上手に活用するため、このパンフレットで漏えい対策のポイントを知り、企業力を高めていきましょう!

大切な情報を守るために、私たちはどのようなことができるのでしょうか。ここでは経済産業省が作成するハンドブック『秘密情報の保護ハンドブック～企業価値向上に向けて～』※1の中から、特に大切な3つについて説明します。

※1 [www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html#handbook](http://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html#handbook)

## A

まずは、自社にどのような情報があるのか一つひとつ洗い出し、社内の情報を把握しましょう。

## B

洗い出した情報がどのくらい重要な情報なのかを見極め、秘密とする情報を決定しましょう。

## C

情報の重要度に応じて対策の選択・決定をし、管理と有効利用のバランスを取りましょう。

## A 保有する情報を洗い出します

自社が保有している情報をしっかりと把握するために、社内にあるような情報があるのか洗い出していきます。 →第2章2-1 (1) ※2

※2『秘密情報の保護ハンドブック～企業価値向上に向けて～』の該当箇所

情報の洗い出しには、ふたつのポイントがあります。

ひとつ目は、紙や電子データなどの目に見える情報だけでなく、従業員が記憶したノウハウ、工場ライン、金型、試作品等も重要な情報だと認識をするということです。そしてふたつ目は、それらの情報をリストにするなど「見える化」し、財産として把握することです。情報は整理すれば社内でも共有することもできますし、そこに従業員からのアイデアも加わって、情報の価値が高くなるというメリットもあるのです。

例) 自社の強みとなる情報資産の例

|      |                                                                                                                                                                                    |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 技術情報 | <p>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)</p>                            |
| 営業情報 | <p>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、接客マニュアル</p>  |

## B 秘密とする情報を決めましょう

持っている情報を洗い出したら、秘密とする情報を決めて、その活用方法について考えていきましょう。

### 決定のフロー

#### 1. 大事な情報を見つけましょう

Aで洗い出した情報について、「その情報が生み出す経済価値は?」「漏えいしたときの損失はどのくらい?」「これは他社から預かっている情報?」といった視点で、どのくらい大事な情報なのかを見極めましょう。 →第2章2-1 (2)

相対的な階層化と絶対的な評価のイメージ～情報を損失で評価した場合～

| 相対的な階層化<br>(損失の大きさ順に情報を序列化) | 相対的な階層化<br>(損失の大きさを評価)                                                                                                                                    |               |  |            |   |            |       |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|--|------------|---|------------|-------|
| 高<br>a<br>b<br>c<br>d<br>低  | <table border="1"> <tr> <td>漏えい時に極めて重大な損失</td><td></td></tr> <tr> <td>漏えい時に重大な損失</td><td>a</td></tr> <tr> <td>漏えい時に軽微な損失</td><td>b c d</td></tr> </table> | 漏えい時に極めて重大な損失 |  | 漏えい時に重大な損失 | a | 漏えい時に軽微な損失 | b c d |
| 漏えい時に極めて重大な損失               |                                                                                                                                                           |               |  |            |   |            |       |
| 漏えい時に重大な損失                  | a                                                                                                                                                         |               |  |            |   |            |       |
| 漏えい時に軽微な損失                  | b c d                                                                                                                                                     |               |  |            |   |            |       |

#### 2. 活用する方法を考えましょう

見極めた情報について、その情報を「秘密」として扱うのか、それとも「公開」して自社の強みとして打ち出し活用するのかを考えます。たとえば技術情報なら、標準化、特許化、ノウハウ管理などにより、その強みを発揮することができます。逆に顧客情報などは、個人情報保護法など法令に基づく管理が必要です。 →第2章2-2

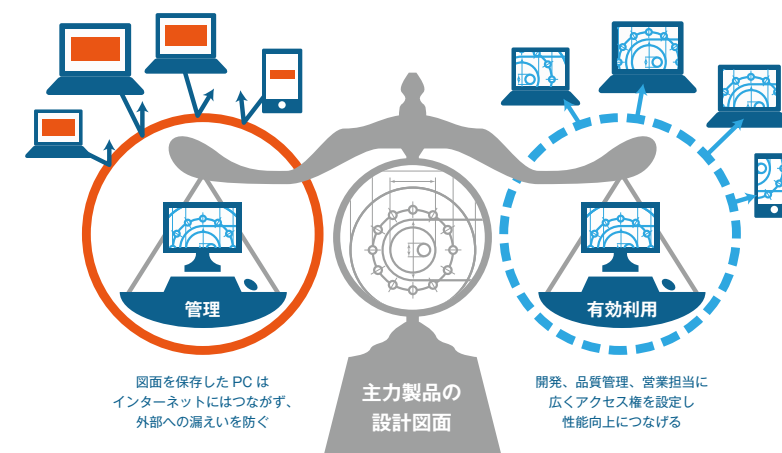
企業の情報活用例  
～ある機械メーカーの機械製品に関する技術情報～

| 公開(標準・特許)                      | 秘密(ノウハウ)       |
|--------------------------------|----------------|
| 機械の動作性能評価方法<br>部品構造(他者が容易に把握可) | 生産プロセス<br>素材配合 |

### 管理と有効利用の バランスが大事

社内で秘密として保持する情報「秘密情報」が見つかったら、その管理方法を考えましょう。ですが一方で、秘密情報からといってしまっておいては宝の持ち腐れとなってしまうこともあります。自社の武器ともなる情報は、管理と有効利用のバランスも大事にしましょう。

→第3章3-1、3-2



## C 情報に合わせた対策の選択と決定をしましょう

# 5つの 対策 と、その 目的

### 物理的・技術的な防御



1

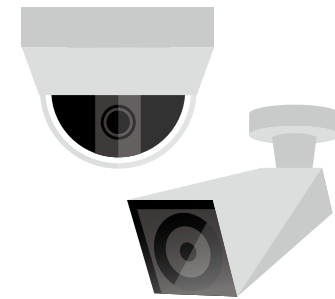
秘密情報に近寄りにくく  
するための対策



2

秘密情報の持ち出しを  
困難にするための対策

### 心理的な抑止



3

漏えいが見つかりやすい  
環境づくりのための対策



4

秘密情報だと思わなかった！  
という事態を  
招かないための対策

### 働きやすい環境の整備



5

社員のやる気を高め、  
秘密情報を持ち出そうという  
考えを起こさせないための対策

#### 1. 近寄りにくくする対策

##### 接近の制御

秘密情報にアクセスできる人は最小限にとどめ、漏えいのリスクを少なくしましょう。退職者に対しては、速やかにアクセス権を削除することが大切です。また、取引先から図面や金型、工程サンプル、工場の内部などを見せるよう要請があっても秘密情報は開示できないときちんと伝えましょう。もしも工場見学で外部者を受け入れなければならないときには、ルートを適正に限定することが大切です。インターネット経由で情報が外部に漏れる可能性もありますので、秘密情報を保存したPCをインターネットにつながらないことも考えましょう。インターネットにつなぐ場合は、サイバーセキュリティ対策として少なくとも以下の対応はしておきましょう。

→ 第3章3-4「接近の制御」

- ・アンチウィルスソフトを導入
- ・ソフトは最新版にアップデート
- ・ファイアーウォールを設定

#### 2. 持ち出しを困難にする対策

##### 持ち出し困難化

たとえば、私物USBメモリの社内使用を禁止することで、秘密情報の社外への持ち出しを難しくすることができます。また、電子データについては暗号化することも効果的です。万が一漏えいしても解読されにくくなります。

→ 第3章3-4「持ち出し困難化」

#### 3. 漏えいが見つかりやすい環境をつくる

##### 視認性の確保

秘密情報を取り扱う場所のレイアウトを工夫したり、防犯カメラを設置するなどの対策をしましょう。防犯カメラの設置は、従業員の行為の正当性を証明するのに役立ちます。また、PC等の情報システムのログのチェックも行いましょう。そして、チェックを行っていることは社内にきちんと周知しましょう。この対策は、情報漏えいの疑いの確認にも効果的です。

→ 第3章3-4「視認性の確保」

#### 4. 秘密情報に対する認識を高める

##### 秘密情報に対する認識向上

どれが秘密情報なのか、ひと目でわかるように表示しましょう。適切なタイミング（入社時やプロジェクト参加時、退職時等）での秘密保持契約の締結も重要です。また情報は日々変わっていくものなので、それに応じて秘密情報の取り扱い方法についても皆で話し合い共有しましょう。情報の取扱い方法についてはルール化することも一案です。

→ 第3章3-4「秘密情報に対する認識向上」

#### 5. 社員のやる気を高める

##### 信頼関係の維持・向上等

社員のモチベーションを高めることは、業績アップだけでなく漏えい対策にもつながります。漏えいをしようという気持ちにさせないために、ワークライフバランスや社内でのコミュニケーション、従業員の能力の多面的な評価など、もう一度見直してみましょう。

→ 第3章3-4「信頼関係の維持・向上等」



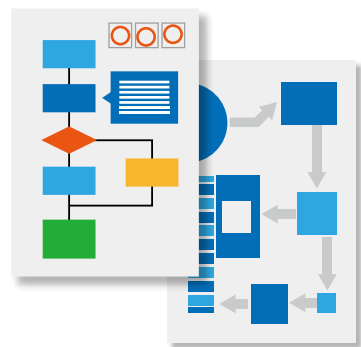
## case - 1

## 従業員向けの対策

## フィルムメーカーJ社の例 製造ラインを新設したいと思っているが……

J社は近々、耐熱性フィルムの製造ラインを新設する予定になっています。その新製造ラインでは、設備の改良や配置の仕方の工夫によって、他社に比べて高効率なフィルム製造システムが実現できるので、その製造ラインや工場のレイ

アウトといった情報が他社に漏れないようにしたいと考えています。ですが、その対策の仕方でも方法わかりません。一体どのようなことが対策としてできるでしょうか。



## ポイント1

## ✔ 秘密情報の全体を把握できる人数を制限しましょう

工場の作業ライン等については一連の流れを複数人で分担するなど、工程全体の情報を1人の作業員が把握できないようにすると効果的です。(接近の制御) ➡第3章3-4(1)①a

## ポイント2

## ✔ 情報に接する従業員が情報を持ち出しにくい対策を考えましょう

工場内へのカメラ等の撮影機器の持込みを制限します(ポケットのない作業着の着用の義務づけや、私物持込みの際は透明バッグに入れて入室するなどの工夫をすることも大切です)(持出し困難化) ➡第3章3-4(1)②j

## case - 2

## 従業員・退職者向けの対策

## 食品メーカーD社の例 中心核の従業員から退職の申出があった

即席麺を製造しているD社では、スープの配合レシピの情報が大切な競争力です。最近、ニュースで、「ある企業の退職者が転職先で営業秘密を不正使用して逮捕された」との報道を見ましたが、他人事ではありません。D社でも先日、

スープ開発担当者の一人から退職の申出があったのです。転職先は競合他社のE社だといいます。大事な配合レシピを持ち出されないようにするためにはどのような対策を取ったらよいのでしょうか。



## ✔ 退職に伴う漏えいリスクを低減する対策を考えましょう

## ポイント1

退職時だけでなく、入社時はもちろん、プロジェクト開始時にも秘密保持契約を締結。退職者がキーパーソンの場合は、秘密保持を徹底するために競業禁止義務契約を締結することも考えられます(秘密情報に対する認識向上) ➡第3章3-4(2)④a、b

## ポイント2

退職の申出があったら、速やかに社内情報へのアクセス権を制限。退職時にはすぐにID・アカウントを削除しましょう(IDカード、入館証も回収)(接近の制御)

➡第3章3-4(2)①a

退職申出前後のメールやPCのログを集中的にチェックしたり、退職後もOB会の開催などで本人の近況を調査するなどして、転職先の商品情報をチェックしましょう(視認性の確保) ➡第3章3-4(2)③q、r

## ポイント3

働きやすい職場環境や公平な人事評価制度を整備して従業員の企業への愛着を高めておけば、貴重な人材を失わずにすむだけでなく、漏えいリスクも低減します(信頼関係の維持・向上等)

➡第3章3-4(1)⑤

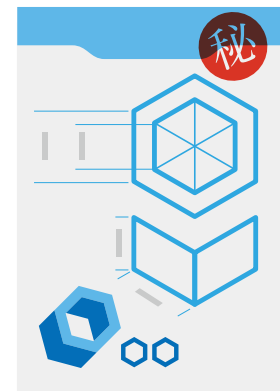
## case - 3

## 取引先向けの対策

## 部品メーカーA社の例 取引先から金型図面の提供を求められた

A社が精密機械メーカーB社に供給する部品αは、A社が独自に開発したもので、精巧な部品であると評判です。ある日、大口の取引先・B社から部品αの金型の図面を求められ提供したところ、その後B社から部品αの発注が来なく

なりました。どうやら、B社がA社の部品αの金型図面をA社の競合他社のC社に渡し、安価で部品αのコピー品を製造させているようです。A社はどのような対策を取っておくべきだったのでしょうか。



## ポイント1

## ✔ 開示する情報は必要最低限にしましょう

B社との取引で、金型図面の情報を開示するのが必要なければ、開示を拒否することも大切です。また、事前に見積書や取引契約書に“金型図面の開示はできない”旨を記載しておくことも効果的です。(接近の制御) ➡第3章3-4(3)①a

## ポイント2

## ✔ 開示する場合は、秘密保持契約を締結しておきましょう

金型図面に関する秘密保持契約には、秘密保持、目的外使用の禁止、契約終了時の金型図面の返還・消去義務等を定めておくといでしょう(秘密情報の認識向上)(持出し困難化) ➡第3章3-4(3)④a、②a

## case - 4

## 外部者向けの対策

## 繊維メーカーK社の例 不審なメールが届いた!

K社は、素材を仕入れて高性能繊維を製造し、顧客に販売する企業です。ある日、製造部門の従業員L宛てに顧客を装ったメールが届きました。従業員Lがその内容に違和感を覚え、添付ファイルを開かずに社内セキュリティ部門に相談したところ、ウィルスが仕込まれた攻撃型メールであることがわかりました。

今回従業員が不審に感じてファイルを開きませんでしたが、誤って添付ファイルを開けばK社の顧客情報や製造ノウハウといった情報のみならず、調達先からの情報まで外部へ漏えいしてしまう恐れがあります。不正アクセスや攻撃型メールの被害に遭わないためには、どのような対策をすればいいのでしょうか。



## ポイント1

## ✔ できる限り、外部への接続を切断しましょう

可能な限り秘密情報は外部ネットワークにつながらない機器に保存しましょう(接近の制御)

➡第3章3-4(4)①e

## ポイント2

## ✔ 不正アクセスや、攻撃型メールの被害を最小限にする対策を考えます

外部ネットワークにつながったPC等に秘密情報を保管する場合は、ファイアウォール、アンチウィルスソフトを導入し、ソフトウェアのアップデートをしっかり行うことが大切です。(接近の制御) ➡第3章3-4(4)①f また、秘密情報の電子データを暗号化することも効果的です(持出し困難化) ➡第3章3-4(4)②c

※標的型攻撃メールを見分けるためのポイント等については、ハンドブックP89の「コラム③ 標的型攻撃メールってどんなもの?」にも掲載しています。

## 備えあれば憂いなし! 自社の立場を守るためにできること

健全に事業を行っている企業でも、不幸にも争いごとに巻き込まれてしまう可能性はゼロではありません。ここでは争いに巻き込まれにくくするために日頃からできる予防策や、正當に自社の立場を守るための方策を紹介します。

case - 5

## 自社技術で商品をつくったのに、 他社の技術を使ったと言われた!

食品メーカーF社の例

野菜のフリーズドライにより具たくさん味噌汁を製造するF社は、新商品として日本の果物を使ったドライフルーツを開発しています。商談会で名刺を交換した食品加工機器メーカーG社から、G社の保有するフリーズドライ技術を使った共同開発の提案を受けました。しかしコスト面で折り合わず、G社の申出をF社は断りました。結局、F社は自社技術を転用して新たなドライフルーツ商品βを開発し、販売を開始しました。

すると突然、商品βはG社の技術を用いて製造されたものであると、その製造・販売中止を求める警告状が送られてきました。ですがF社がG社から共同開発の打診を受けた際には、具体的な技術の開示は受けていなかったため、G社の秘密情報など使っ

た覚えはありません。

F社が自社の独自技術であるとの潔白を示すには、どうしたらよいのでしょうか。



point

### 独自技術だと証明できるように、 開発の内容や日時等を記録しておきましょう

他社から秘密情報の侵害を理由に警告されたり、提訴されたりした場合には、自社の用いている情報が独自のものであるということを客観的に証明できるように、情報の取得過程や更新履歴等の記録を保存するなど、日頃からの備えが重要になります。

➡第5章5-1

ポイント1

☑ 他社の情報は、できる限り受け取らない

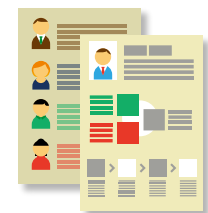
ポイント2

☑ 自社技術の開発経緯等を記録する

- ・ 技術情報であれば、技術が生まれるまでの実験過程等を記録したラボノートを作成・保存する
- ・ 日付確定のための公正証書（公証人が作成する公文書）などを利用する
- ・ その他、電子メールや検討文書、議事録など関連資料を保管する

⚠ 取引経緯の記録も大事です

顧客名簿であれば顧客になるに至った経緯を記録したり（来店・購入の履歴、会員登録時のWeb登録内容申込書等）、取引情報であればその取引経緯を記録しましょう（仕入や販売の際の価格、数量等が記載された伝票の原本等）。



### 営業秘密侵害品に関する規制が新設されました!

民事【2条1項10号】 刑事【21条1項9号】

平成27年の不正競争防止法改正によって、営業秘密を不正に使用することによって生じた物（営業秘密侵害品）の取引が新たに規制の対象となりました。 ➡第5章5-3

point

疑わしいと思われる場合には、適切な確認等の対応を取りましょう。

▶ 疑わしい状況の例

- ・ 自社の販売する商品について、「営業秘密侵害品である」との警告を受けた場合
- ・ 自社の販売する商品について、「営業秘密侵害品である」との判決の報道がなされた場合
- ・ 自社の取引相手が営業秘密侵害を行っている、との情報を耳にした場合

▶ 考えられる対応の例

- ・ 警告や報道の真偽について、取引先に問い合わせる
- ・ 取引を継続する場合は、取引先から「営業秘密を侵害して生産したものではない」旨の誓約書を取得する
- ・ 営業秘密侵害品であるとの疑いが高いと思われる場合は、取引を中止する

## 他社の秘密情報を 意図せず侵害しないために

他社の秘密情報を意図せず侵害しないために重要なことは何でしょうか。  
case-6の事例を参考に、社内での周知徹底を行いましょう。

### case - 6

## 転職者を受け入れて新製品を開発したら、 秘密情報の侵害だと訴えられた

### 容器メーカーH社の例

H社は、軽量で強度の高い樹脂製の食品保存容器の開発に力を入れたいと考え、競合他社I社で容器開発経験のあるM氏を迎えました。そのM氏を開発部のリーダーとして開発を進めたところ、これまでになく軽量で強度の高い容器γの開発に成功。販売を開始しました。しかし、γを販売してから数ヵ月後に、M氏の転職元であるI社から「γはI社の秘密情報を不正使用して製造されたものであるため、販売を中止してほしい」との通知を受けました。これを受けてH社がM氏に確認し

たところ、I社の技術の一部用いてγを開発したことを認めたのです。H社はM氏の採用にあたり、どのような対応をすべきだったのでしょうか。



### point

### 転職者を受け入れる際には、 採用前後の業務内容等を確認しましょう

転職者を受け入れる場合にはその知識や経験の中に転職元の秘密情報が存在する場合があります。意図せぬかたちで他社の秘密情報を取得してしまう可能性があります。特に、競合他社のキーパーソンと呼べるような人物を受け入れる場合には慎重な対応が必要です。転職者の受け入れにあたっては、下記の点などに十分注意しましょう。

#### → 第5章5-2(1)

#### ポイント1

#### ☑ 転職者の負っている義務をきちんと確認する

採用時の面接を通じて、転職者が転職元との関係で負っている秘密保持義務、競業禁止義務といった義務の有無や、その内容を確認しましょう。その際、議事録等を記録・保存しておくにより効果的です。

#### ポイント2

#### ☑ 転職者の採用時には、転職元の秘密情報を 持ち込ませないようにする

転職者に転職元の秘密情報を持ち込ませないよう注意喚起をしましょう。秘密情報を持ち込まない旨の誓約書を転職者から取得しましょう。※具体的な誓約書の文言は、たとえば以下などが考えられます。  
一 第三者の秘密情報を含んだ媒体（データ、資料）を一切持ち出していない  
一 第三者の保有するあらゆる秘密情報を持ち込まない

#### ポイント3

#### ☑ 転職者の採用後も、 その業務内容等をしっかり管理する

転職者が従事する業務内容を定期的に確認しましょう。私物のUSBメモリ等の記録媒体の業務利用や持込みを禁止することも効果的です。また、「I社の製造プロセスに関する情報を知っているが、H社の設備の内容及び仕様等に照らして、当該情報を転用できるような状況にはない」ことを書面上で約束してもらうのもいいでしょう。

⚠ 共同研究開発等で他社の秘密情報を受け取る場合には、受領した情報の取り扱いについて書面上での確認や、自社の情報との分離管理を適切に行いましょう

### 情報の分離管理とは？

他社の情報を受領した場合、自社独自の情報との分離管理が必要といっても、具体的に何をすればよいのでしょうか？ → 第5章5-2(2)③ 以下のことを参考にしてみましょう。

#### ▶ 人の管理

- ・ 自社開発と共同研究開発の担当者を分ける
- ・ 他社情報を取り扱う自社内の関係者から、「当該情報を共同研究開発目的以外で使用しない」という誓約書を取得する

#### ▶ 情報の管理

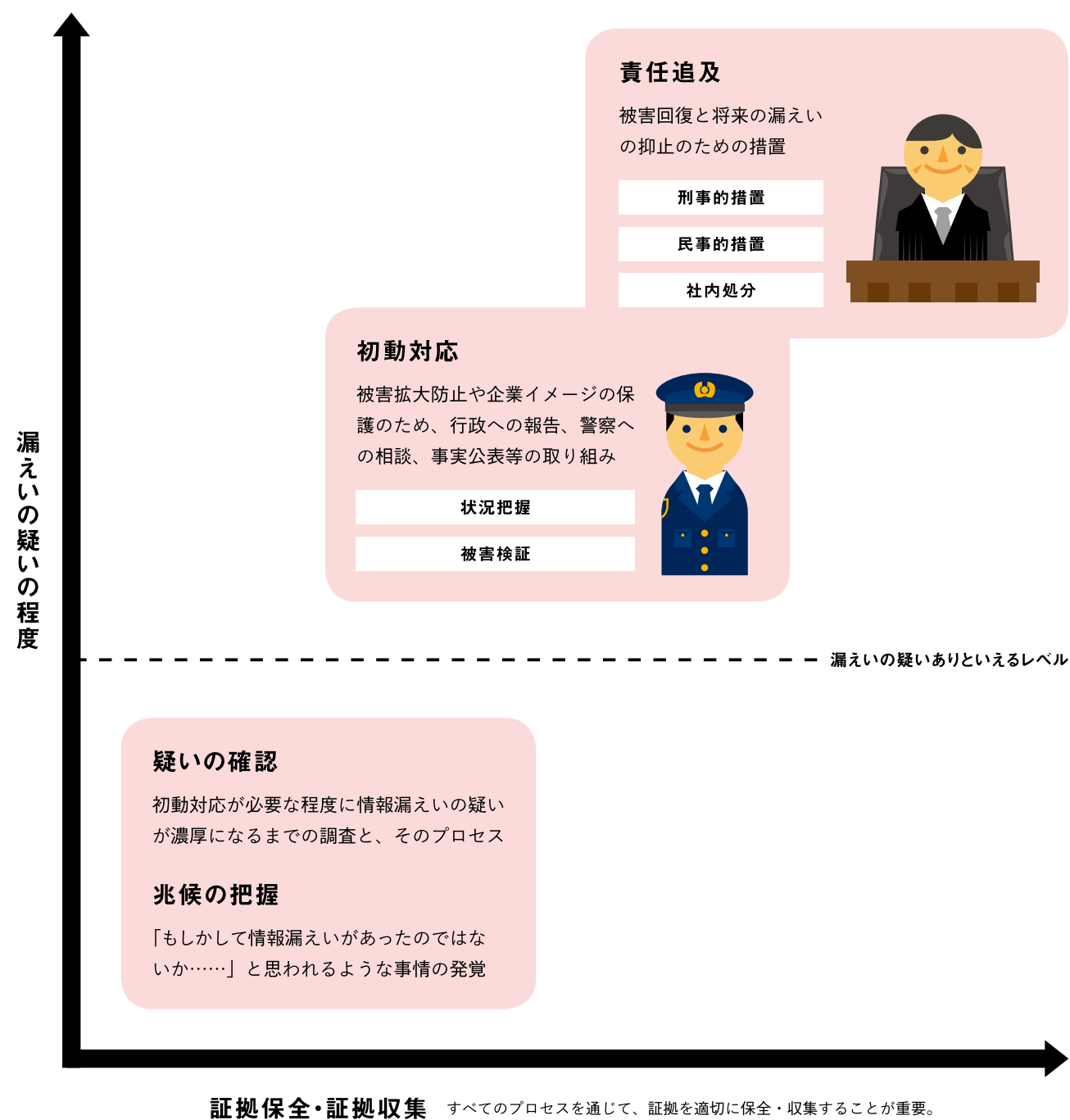
- ・ 取得した他社情報の内容、日時、経緯を記録しておく
- ・ 他社情報の電子データは別フォルダで分離し、ID、パスワード等でアクセス制限をする
- ・ 必要に応じて、他社との共同研究開発には専用の初期化されたPCを使用する

#### ▶ 物の管理

- ・ 化合物等の物自体が他社の秘密情報の場合、当該他社専用のキャビネットや倉庫等で分離管理する



いくら企業が情報管理を徹底しても、近年のサイバー攻撃などは手口が高度化しているため、情報漏えいを完全に防ぐことは難しくなっています。そのため、万が一情報漏えいがあったときに、いかに迅速な対応ができるかが大切になってきます。ハンドブックでは、漏えい事案への対応に応じた対策を説明しています。



## 1 情報漏えいには兆候があります！

定時に処理可能な業務量であるはずの従業員が、深夜に職場に戻って来ている……

インターネットの掲示板で、自社商品の類似品とみられる製品が話題になっている……

このような経験はありませんか？

このようなささいな事象も、自社の情報の漏えいにつながったり、もしかするとすでに漏えいしているかもしれません。疑わしいと思ったら、情報漏えいがあったかどうか速やかに確認をしましょう。漏えいの場面ごとに、考えられる兆候やその疑いを確認するための方法を合わせて紹介します。 →第6章6-1

### ・従業員等からの漏えいの場合

| 兆候                                                                                                                                                                             |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>・秘密情報を保管しているサーバーや記録媒体へのアクセス回数が大幅に増えたり、業務上必要のないアクセスがある</li> <li>・業務量に比べて異様に長い残業時間や、余裕がある時期でも休暇を取ろうとしない</li> <li>・不必要な休日出勤が増えた</li> </ul> |

| 疑いの確認                                                                                                 |
|-------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>・漏えいの兆候のある従業員の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の内容の確認をする</li> </ul> |

### ・退職者等からの漏えいの場合

|                                                                                                                                                                                 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>・同僚内の会話やOB会等で、退職者の転職先企業での業務内容が転職前の研究内容と似ていると話題になっていたり、そういったうわさがある</li> <li>・退職者の転職先企業が、製造・販売を開始した商品の品質や機能が、特に転職後、自社商品と同水準になった</li> </ul> |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>・漏えいの兆候のある退職者等に未返却のものがないか確認する</li> <li>・退職者等の退職前後一定期間のサーバーへのアクセス記録や、メールのログ、ダウンロードデータの内容を確認する</li> </ul> |
|------------------------------------------------------------------------------------------------------------------------------------------------|

### ・取引先からの漏えいや不正使用の場合

|                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>・取引先から、突然、取引を打ち切られた</li> <li>・取引先から、取引内容との関係では必ずしも必要ではないはずの業務資料のリクエストを受けた</li> <li>・通常の取引に比べて異様に詳細な情報照会を求められた</li> <li>・インターネット掲示板等で、自社の非公開情報や自社製品の類似品が話題になっている</li> </ul> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                                                                                                                                                      |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>・情報を不正使用している疑いのある取引先等が製造・販売している商品をチェックする</li> <li>・顧客名簿に意図的に入れたダミーデータ等の使用履歴を確認する</li> <li>・漏えいの兆候のある取引先に自社のサーバーを使わせていた場合には、そのアクセスやダウンロードの履歴をチェックする</li> </ul> |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### ・外部者からの漏えいや不正使用の場合

|                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>・競合他社等における秘密情報漏えいや、不法侵入等の事件が発生した</li> <li>・ウィルス対策ソフト、セキュリティ対策機器によって検知された</li> <li>・「競合他社からの売り込みがあった」との顧客からの連絡</li> <li>・オフィスや会議室での盗聴器を発見した</li> </ul> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                                                                                                                                                                                               |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>・情報の不正な使用の疑いのある者が製造・販売している商品をチェックする</li> <li>・顧客名簿に意図的に入れたダミーデータ等の使用履歴を確認する</li> <li>・書類や記録媒体等の持出しの有無を確認する</li> <li>・不法侵入等がないかどうか、監視カメラの記録を確認する</li> <li>・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</li> </ul> |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## 2 漏えいの疑いがあったらできるだけ早く適切な対応を取りましょう

情報漏えいの疑いを確認し、対応の必要があると判断した場合には、被害拡大の防止や企業イメージの保護を図るとともに、迅速かつ適切な被害回復のために、できるだけ早く適切な対応を取りましょう。 ➡ 第6章6-2、6-3

1. 社内調査、  
状況の正確な把握、原因究明

2. 被害の検証

3. 初動対応

- ・さらなる情報拡散の防止（インターネット上の情報の削除要請や、不正アクセス等が疑われる場合のネットワーク遮断等）
- ・法律に基づく手続（個人情報保護法に基づく行政庁への報告等）
- ・企業イメージの損失の最小化（事案に応じ速やかな対外公表、関係者や取引先への相談等）

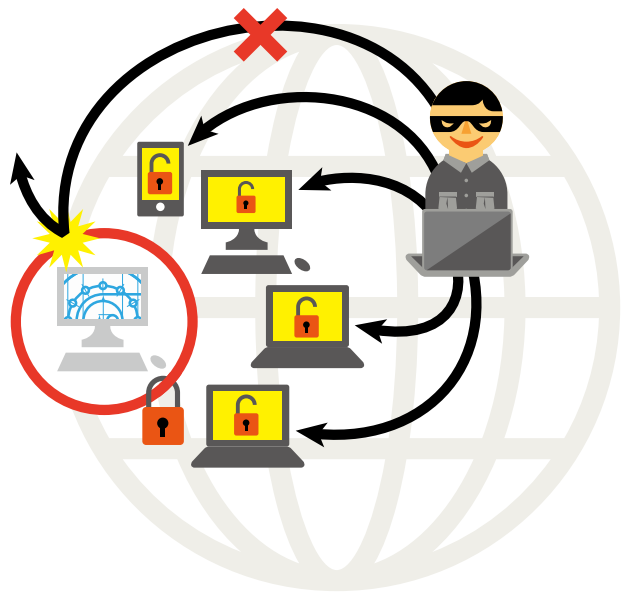
4. 社内における対策チームの設置等



不安を感じたらすぐに相談しましょう

情報の漏えいがあったかもしれないと思ったときには、早めにお近くの警察（各都道府県警本部の営業秘密保護対策官）、弁護士等の専門家にご相談ください。刑事と民事でいずれの措置（または双方の措置）を取るかについては、具体的事情に応じて判断しましょう。

※各種窓口一覧は秘密情報の保護ハンドブックの参考資料3にも掲載されています。



## 3 被害回復のためにも日頃からの備えが大切です

万が一秘密情報の漏えいが発生してしまったとき、適切に被害回復ができるようにするために、最低限、以下のことには留意しましょう。

➡ 第6章6-4

☒ 重要な情報へはアクセス制限（パスワードの要求等）をする。マル秘マークを付する

☒ 自社の就業規則や秘密保持誓約書等においてどの情報が秘密保持の対象となるかを明示、特定した上で、従業員等との間でしっかりと確認しておく

☒ 自社のシステム内での履歴（アクセス・メールのログ等）を記録、保存しておく

秘密情報の扱いについて正しい知識を持ち、

上手に活用して、これまで以上に企業の価値を高めていきましょう！

## 4 情報漏えいしたら早めの相談を！

自社の情報が漏れてしまったかも？ と思ったときは、こちらにご相談ください。その他、営業秘密管理や、知財戦略に関するご相談も、知的財産戦略アドバイザーや知財専門家が無料でおこなえます。

### ■ INPIT（（独）工業所有権情報・研修館）

#### 営業秘密・知財戦略相談窓口（営業秘密110番）

・営業秘密・知財戦略ポータルサイト

[www.inpit.go.jp/katsuyo/tradecret/index.html](http://www.inpit.go.jp/katsuyo/tradecret/index.html)

・全国47都道府県の知財総合支援窓口

<http://chizai-portal.jp>

全国共通ナビダイヤル 0570-082100（お近くの支援窓口につながります）

・相談窓口

03-3581-1101（内線3844）

（平日9:00-17:45（受付17:30まで））

[trade-secret@inpit.jpo.go.jp](mailto:trade-secret@inpit.jpo.go.jp)

### ■ IPA（（独）情報処理推進機構）

・情報セキュリティ安心相談窓口

コンピュータウィルス及び不正アクセスなどの情報セキュリティに関する、技術的な相談窓口

[www.ipa.go.jp/security/anshin](http://www.ipa.go.jp/security/anshin)

・営業秘密関連情報サイト（営業秘密のツボ）

営業秘密官民フォーラムメールマガジンバックナンバー

[www.ipa.go.jp/security/economics/mailmag/index.html](http://www.ipa.go.jp/security/economics/mailmag/index.html)



### ■ 全国都道府県警察 営業秘密侵害事犯窓口

自社の情報漏えいに対して刑事的措置を検討するときには、各都道府県警察本部の不正競争防止法違反（営業秘密侵害事犯）を担当する課（生活経済課、生活環境課など）にご相談ください。

| 警察名            | 代表電話         |
|----------------|--------------|
| 北海道警察本部生活経済課   | 011-251-0110 |
| 北海道函館方面本部生活安全課 | 0138-31-0110 |
| 北海道旭川方面本部生活安全課 | 0166-35-0110 |
| 北海道釧路方面本部生活安全課 | 0154-25-0110 |
| 北海道北見方面本部生活安全課 | 0157-24-0110 |
| 青森県警察本部保安課     | 017-723-4211 |
| 岩手県警察本部生活環境課   | 019-653-0110 |
| 宮城県警察本部生活環境課   | 022-221-7171 |
| 秋田県警察本部生活環境課   | 018-863-1111 |
| 山形県警察本部生活環境課   | 023-626-0110 |
| 福島県警察本部生活環境課   | 024-522-2151 |
| 警視庁生活経済課       | 03-3581-4321 |
| 茨城県警察本部生活環境課   | 029-301-0110 |
| 栃木県警察本部生活環境課   | 028-621-0110 |
| 群馬県警察本部生活環境課   | 027-243-0110 |
| 埼玉県警察本部生活経済課   | 048-832-0110 |
| 千葉県警察本部生活経済課   | 043-201-0110 |
| 神奈川県警察本部生活経済課  | 045-211-1212 |
| 新潟県警察本部生活保安課   | 025-285-0110 |
| 山梨県警察本部生活安全捜査課 | 055-235-2121 |
| 長野県警察本部生活環境課   | 026-233-0110 |
| 静岡県警察本部生活経済課   | 054-271-0110 |
| 富山県警察本部生活環境課   | 076-441-2211 |
| 石川県警察本部生活環境課   | 076-225-0110 |
| 福井県警察本部生活環境課   | 0776-22-2880 |
| 岐阜県警察本部生活環境課   | 058-271-2424 |

| 警察名           | 代表電話         |
|---------------|--------------|
| 愛知県警察本部生活経済課  | 052-951-1611 |
| 三重県警察本部生活環境課  | 059-222-0110 |
| 滋賀県警察本部生活環境課  | 077-522-1231 |
| 京都府警察本部生活経済課  | 075-451-9111 |
| 大阪府警察本部生活経済課  | 06-6943-1234 |
| 兵庫県警察本部生活経済課  | 078-341-7441 |
| 奈良県警察本部生活環境課  | 0742-23-0110 |
| 和歌山県警察本部生活環境課 | 073-423-0110 |
| 鳥取県警察本部生活環境課  | 0857-23-0110 |
| 島根県警察本部生活環境課  | 0852-26-0110 |
| 岡山県警察本部生活環境課  | 086-234-0110 |
| 広島県警察本部生活環境課  | 082-228-0110 |
| 山口県警察本部生活環境課  | 083-933-0110 |
| 徳島県警察本部生活環境課  | 088-622-3101 |
| 香川県警察本部生活環境課  | 087-833-0110 |
| 愛媛県警察本部生活環境課  | 089-934-0110 |
| 高知県警察本部生活環境課  | 088-826-0110 |
| 福岡県警察本部生活保安課  | 092-641-4141 |
| 佐賀県警察本部生活環境課  | 0952-24-1111 |
| 長崎県警察本部生活環境課  | 095-820-0110 |
| 熊本県警察本部生活環境課  | 096-381-0110 |
| 大分県警察本部生活環境課  | 097-536-2131 |
| 宮崎県警察本部生活環境課  | 0985-31-0110 |
| 鹿児島県警察本部生活環境課 | 099-206-0110 |
| 沖縄県警察本部生活保安課  | 098-862-0110 |



※ 秘密情報の保護ハンドブックと併せてご活用ください。

---

経済産業政策局 知的財産政策室

[www.meti.go.jp/policy/economy/chizai](http://www.meti.go.jp/policy/economy/chizai)

電話：03-3501-3752（直通） FAX：03-3501-3580