

参考資料 4

営業秘密を適切に管理するための

導入手順について

～はじめて営業秘密を管理する事業者のために～

目次

1.	はじめに	2
2.	導入手順例の流れ	3
3.	具体的な導入手順例	5
(1)	自社の強みとなる情報資産の把握	5
①	知的資産経営と自社の強みとなる情報資産の把握	5
②	自社の強みとなる知的資産とそれを構成する情報資産の把握方法例	5
(ア)	自社の強みとなる知的資産・情報資産を把握する	5
(イ)	営業秘密として管理する情報資産を把握する	7
(2)	実践例における自社の強みとなる情報資産及び営業秘密として管理すべき情報資産の把握の方法	8
4.	事業者における営業秘密の管理体制の構築・管理ルールの導入	10
(1)	管理状況及び管理水準の現状把握	10
(2)	営業秘密・管理ルールの指定・周知・実施	15
①	目標とする管理水準を検討する	16
②	管理方法を選択する	16
(ア)	実践例における基本的な考え方	17
(イ)	営業秘密（とそのアクセス権者）を指定する	18
(ウ)	書面等の管理及びコンピュータ管理	20
(エ)	従業者等の管理	25
(オ)	取引先等	26
③	営業秘密・管理ルールの周知・実施	27
(3)	チェック・見直しの実施	28
5.	(参考) 実践例において導入された営業秘密管理体制の全体像	30

1. はじめに

自社の重要な情報資産として把握したもののうち、秘密として管理すると判断した情報資産は、適切に管理されることによってはじめて営業秘密としての法的保護を受けることができる。そこで、主として、営業秘密を管理する体制を整備していない中小企業等を対象として、適切な管理体制を構築するための導入手順を具体的な事例（実践例）に則して紹介する。

本指針では、「第3章 営業秘密を保護するための管理の在り方」において、事業者の重要な情報資産を営業秘密として管理するための具体的な管理方法等について説明しているところであるが、事業者において、実際にその保有する情報資産を実効的に秘密管理するためには、自社の情報資産の中から、秘密として管理すべき情報資産を適切に把握した上で、これを確固たる方針に基づいて適切に管理する体制を構築することが重要である。

しかしながら、これまで明確な経営方針に基づいて営業秘密の管理策や情報セキュリティ対策を講じてこなかった事業者においては、そもそも秘密として管理すべき情報資産を把握していないことが多い上、そのような情報資産を営業秘密として管理するために適した具体的な手法及びその導入方法についての知識・理解が十分でないことも多いことから、「どの情報をどのように営業秘密として管理すべきか分からない」という状況から脱却することは必ずしも容易ではないと思われる。そこで、これから重要な情報資産を営業秘密として管理すべき体制を構築しようとする事業者にとって、参考となり得る導入手順の一例について、具体的な事例に則して紹介する。

したがって、以下の記述は、全事業者にとって参考となる点を含むものの、主として、営業秘密を管理する体制を整備していない事業者（特に中小企業）を対象としている。

なお、事業者ごとに営業秘密として管理すべき情報資産の種類・性質・数量、それを把握するための適切な方法、秘密管理の目的、求める管理水準、適切な管理方法及びその組合せなどは異なり得るものであり、適切な導入手順もまた一律に決まるものではないことから、ここにおいて紹介する導入手順例は、多種多様な導入手順の中の一例を示すものにすぎず、営業秘密の管理体制を構築する際には、あくまで事業者ごとの個別事情を勘案した上で行うべきことに留意する必要がある。

<実践例について>

以下においては、**営業秘密の管理体制を構築する手順の例を実践的な事例に則して紹介する。これらの事例においては、業務の効率性を極力損なうことなく、営業秘密の要件である秘密管理性を満たす可能性の高い管理水準であって、かつ、導入に当たって格別の費用を要しない管理体制を構築することを目標としている。**

2. 導入手順例の流れ

営業秘密管理体制を構築するための導入手順としては、自社の強みとなる情報資産の把握（営業秘密として管理する情報資産の把握） 現状の管理状況及び管理水準の把握 営業秘密及び管理ルールの指定・周知・実施 チェック・見直し、という流れが考えられる。

営業秘密管理体制を構築するための導入手順について、自社の強みとなる情報資産の把握（営業秘密として管理する情報資産の把握） 営業秘密として管理すべき情報について、現状の管理状況及び管理水準の把握 営業秘密及び管理ルールの指定・周知・実施 チェック・見直し、という順序で実践例に則して具体的に説明する。より詳細な流れは以下のとおりである。

自社が保有する情報資産の中から、例えば、事業者の競争優位を実現させている要素に着目した方法などを用いて、「自社の強みとなる情報資産」を把握する。これにより把握した情報資産について、営業秘密として管理するかなどを判断する。

営業秘密として管理すると判断した情報資産について、その管理状況（取扱状況、保管状況等）を把握した上で、現状の管理体制がいかなる水準にあるのか、参考資料1の営業秘密管理チェックシートを利用するなどして認識する。

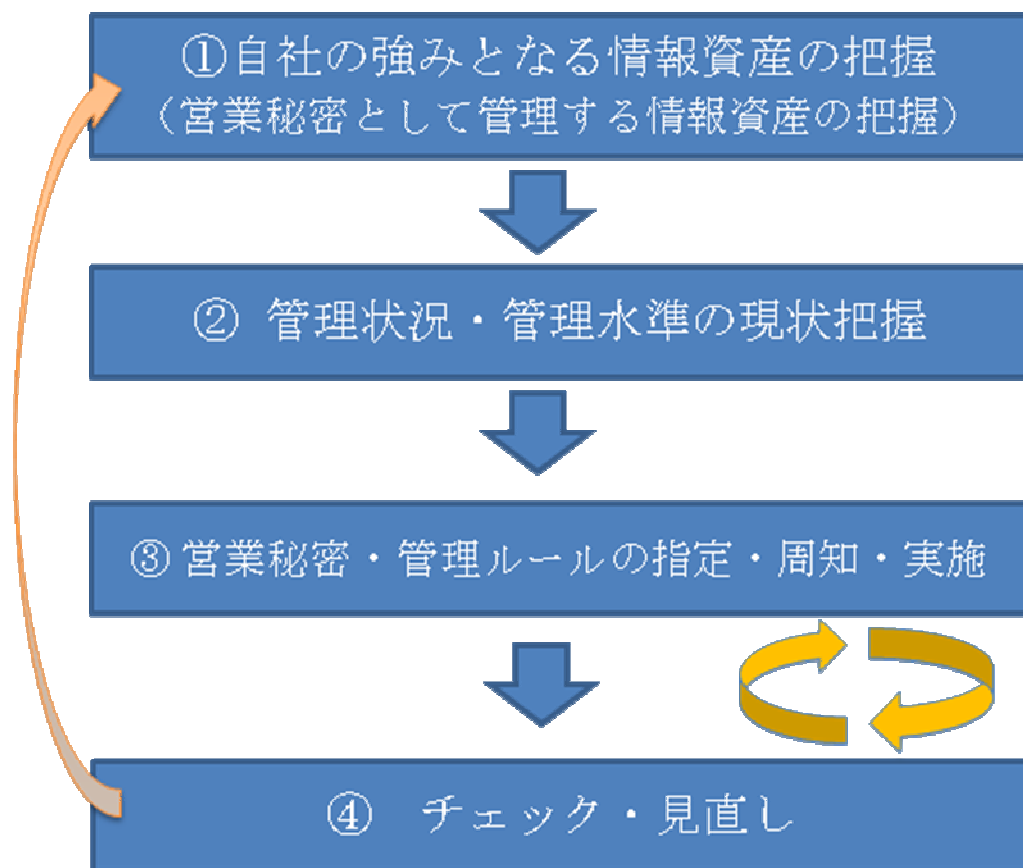
事業者の規模、業種、営業秘密として管理すると判断した情報資産の数量、その取扱状況等を踏まえ、実効的な管理をするために適切と考えられる方法により、その情報資産を営業秘密として指定（その特定方法等の決定手続の規定を含む。）するとともに、その管理ルールを具体的に指定し、これらを周知し、実践する。

営業秘密管理体制を構築した後、指定された管理ルールが適切に実践されているかについて、日常的にチェックし、それに基づき見直しを行う（できる限り、そのようなチェック・見直しに関するルールを管理体制の中に組み込むことが望ましい。）。また、新しい事業分野に進出するため、営業秘密として指定すべき新たな情報資産が創出される場合等、必要に応じて、自社の強みとなる情報資産を適切に把握するための見直しを行うことが望ましい。

事業規模・人的資源等に乏しい中小企業等においては、自社の現状を考慮することなく、いたずらに複雑な管理体制を構築した場合、現場において十分に実践できないことなどにより、かえって実効的な管理とはいえない状況に陥るおそれもあることから、各事業者の実情に応じた組織的な管理体制を構築することが望ましいことに留意すべきである。

なお、管理体制を構築する初期の段階に用いた管理方法等が、事業者内で実効的に行われていることが確認できた際に、必要に応じて、追加的な管理方法等の導入を検討するなど、段階的に管理体制を充実させていくことが望ましい。

【導入手順の流れのイメージ図】



3. 具体的な導入手順例

(1) 自社の強みとなる情報資産の把握

(営業秘密として管理する情報資産の把握)

自社の事業活動の流れに沿って「自社の強みとなる情報資産」を把握する。その際、自社の売上高に占める割合の高い製品・サービスについて、高い売上げを達成するに至った様々な「強み」を把握し、それを構成する情報資産を把握することが取り組みやすいと考えられる。

知的資産経営と自社の強みとなる情報資産の把握

営業秘密として管理すべき情報資産の把握方法として、ここでは自社の強みとなる情報資産を把握する方法を用いて、以下説明する。

自社の強みとなる情報資産を把握することは、営業秘密として管理すべき情報資産を把握することのみを目的とするものではなく、より広く事業者の重要な情報資産を把握することによって、事業者が保有する無形の知的資産を活用し、それらの組合せによって新たな価値を創造し、利益を生み出すという知的資産経営を行うことを目的としている。すなわち、昨今、金融機関が中小企業の保有する知的資産に関わる非財務情報を融資判断時に重要視しているとの実態もあるところ、知的資産経営は、より積極的な事業展開をも可能とするものであり、その実践のために、各事業者は、自社の他社に対する優位性の根源である、自社の強みを構成する技術上・営業上の情報資産を明確に認識した上で、その扱いを適切に選択する必要があるものといえる。

なお、本作業は、経営者を始めとした事業者全体の判断で決定されることが望ましいことから、経営者の関与の下に行われるものとし、経営者の指示の下に担当者（担当チームを組むことなども考えられる。）が行うとしても、最終決定は経営者が行うことが望ましい。

自社の強みとなる知的資産とそれを構成する情報資産の把握方法例

(ア) 自社の強みとなる知的資産・情報資産を把握する

「自社の強みとなる情報資産の把握」のためには、まず「自社の強みとなる知的資産」を把握し、その後、それを得るために必要な情報資産を把握するという手順を踏むことが効率的であると考えられる。

通常、事業者の一連の事業活動は、経営方針や理念に基づき、社内体制を整備し、保有する技術・ノウハウやネットワークを用いて製品・サービスを提供し、その結果が業績に表れるという流れになる。自社の強みとなる知的資産・情報資産を把握するためには、一連の事業活動の成果物である、製品・サービス等（以下「製品等」という。）から分析することとする。これは、製品等から分析していくこと、特に、事業者が生み出している製品等の中で相対的に高い売上げを上げているものを分析していく方法が最も取り組みやすいと考えられるからである。

すなわち、製品等の中で他社と比較して個性が強いもの（他社が模倣することが困難な製品等）や、製品等自体に強い個性がなくても、高い売上げに結びつく

特徴的な性質をもつものは、事業者の強みの源泉である可能性が高く、この作業により、「高い水準の技術力」や「顧客ネットワーク」といった「自社の強みとなる知的資産」を把握することができる。

例えば、自社の主力製品が高い売上げを達成している理由として、その製品等が高い技術水準を有しているために他社の製品等と比べて競争優位性がある場合は、まずその技術自体が「自社の強みとなる知的資産」といえ、その技術（水準）の実現を基礎付けている「設計情報」、「製造ライン情報」、「人材育成プログラム」、「報酬体系情報」等が「自社の強みとなる情報資産」と判断することができる。

以下においては、製品等から把握した「自社の強みとなる知的資産」の例と、それを基礎付ける「自社の強みとなる情報資産」の例¹を記載する。

【製品等から把握した「自社の強みとなる知的資産」及びそれを基礎付ける「自社の強みとなる情報資産」の例】

「自社の強みとなる知的資産」	「自社の強みとなる情報資産」
個性的な製品等を完成させるための技術/ノウハウ	<ul style="list-style-type: none"> ・製造プロセス・段取りに関する情報 ・研究開発情報(技術開発・試験記録等) ・製品仕様書(構造・成分内訳等・規格書) ・独自開発の技術情報 ・工場設備情報・レイアウト情報 ・製造協力先・下請事業者の情報
品質や中長期的な安定的存在感、中長期的な取引関係等に基づく信頼に裏打ちされた製品等/事業者のブランド力	<ul style="list-style-type: none"> ・有力販売先情報 ・市場動向・トレンド(分析)情報 ・営業日誌(訪問履歴・報告等) ・製品・商品・サービスに対する利益額(率) ・仕入先・販売先・品目・数量・価格情報等 ・販売協力先(代理店・FC等)情報 ・競合先(分析)情報(動向・販売価格等) ・セールス資料(見積書・プレゼン資料等)
顧客のニーズにかなった製品等を提供する営業力	<ul style="list-style-type: none"> ・顧客との打合せ資料 ・顧客から受け取る各種資料及び情報 ・顧客との各種契約情報及び契約内容 ・顧客企業(個人)情報リスト、担当者情報 ・顧客からのクレーム資料 ・顧客別に紐付いた製品・商品・サービス販売(提供)情報及び履歴 ・顧客の経営計画情報等
高い技術を有する従業者	<ul style="list-style-type: none"> ・技術者教育・育成に関する情報(教育プログラム・資料等)

¹ 「オープンイノベーション時代の知的財産の活用の在り方に関する調査研究」(平成22年3月(財)企業活力研究所)参照。

(イ) 営業秘密として管理する情報資産を把握する

把握した「自社の強みとなる情報資産」の取扱いについては、経営戦略上重要であり、経営者をはじめとした事業者全体の判断で決定されることが望ましい。事業者の競争優位の源泉が知恵やノウハウなどに変遷しつつある昨今の知識経済においては、情報資産の管理に対する姿勢そのものが経営戦略と密接に関わってくるため、このような判断は極めて重要である。また、このことは、保有する情報資産を営業秘密として管理するという観点のみならず、情報セキュリティレベルを高める、知的資産経営を促進するなど、経営上の様々な観点で有益である。

「自社の強みとなる情報資産」の取扱方法の類型について

事業者は、保有する情報資産について、IR等を利用し積極的に公表していくべきものであるか、特許権等を取得し保護すべきものであるか、ノウハウとして秘匿し適切な秘密管理下に置くべきものであるかを判断する必要がある。

自社の技術情報を保護する方法としては、特許権等を取得する方法と、ノウハウとして秘匿する方法が考えられ、特許権等を取得する情報資産と、営業秘密として管理する情報資産とを選別し、適切な方法を組み合わせることが有効な経営戦略となる²。両者の選択に当たっては、以下の表などを参照されたい。

	特許権等の知的財産権を取得する	営業秘密として管理する
メリット	法により認められた譲渡可能な排他的独占権を取得できる	・営業秘密を中核とした自社の事業戦略の方向性が他社に明らかにならない ・特許になじまないノウハウも営業秘密として保護対象となり得る ・期間制限もなくリバースエンジニアリング等によって明らかにならない限り他社との差別化を図ることができる
デメリット	特許権取得の有無にかかわらず、原則として特許出願の内容は特許出願の日から1年6月を経過すると公開されるため、他社に模倣されたり、周辺特許を取得されたりする可能性がある	適切に情報を管理しない場合には営業秘密としての法的保護を受けることができない可能性がある

² なお、特許権として保護され得る情報資産（発明）をノウハウとして秘匿することを選択した場合は、発明を実施している（事業を行っている）又はその準備をしていれば、その後、他社が特許権を取得したとしても、無償の通常実施権が得られる制度、いわゆる先使用权制度が設けられており、当該制度を活用することにより、事業者は継続的に事業実施を行うことが可能である。先使用权については、「先使用权制度の円滑な活用に向けて - 戦略的なノウハウ管理のために -」（平成18年6月特許庁）を参照されたい。

(2) 実践例における自社の強みとなる情報資産及び営業秘密として管理すべき情報資産の把握の方法

【実践例1（取引先情報）】

事業者	ソフト販売・ソフトウェアの受託開発を主たる事業とする株式会社
営業秘密	取引先情報（「取引先情報データベース」）

（重要な情報資産の把握）

- 1) 自社にとって相対的に高い売上げを上げている製品等が何かを検討する。
自社の売上げが最も高いのは ソフトウェアに関する受託開発である。
- 2) 1) の製品等の売上げが高い理由を分析する。
取引先事業者の細かいニーズに迅速かつ丁寧に対応することによって、信頼を得ている。このような対応を可能にしているのは、長年をかけて、取引先に関する詳細な情報（取引先事業者名、受注内容、対応経過等）をデータベース化し、それを活用しているからである。よって、取引先ニーズに迅速かつ丁寧に対応できることが自社の強みとなる知的資産であり、その強みを生み出すための詳細な取引先情報（取引先情報データベース）が自社の強みとなる情報資産である。
上記ソフトウェア開発を受託するにあたり、著名な検索サイトに広告を掲載するなど効果的な広報を行っていることも、高い売上げに貢献していると判断される。よって、時宜にかなった広報戦略も自社の強みとなる知的資産であり、それを構成する資料（新規プロモーションの方針等）が自社の強みとなる情報資産である。

（営業秘密として管理すべき情報資産の把握）

- a) 取引先に関する情報は、有名企業との間で長期にわたる取引があることなどは広報（自社が開設するホームページに掲載等）したり営業活動に利用したりするなど、自社の信用度を高めるために活用することが考えられる。他方で、その詳細な内容（蓄積された取引履歴、個別の取引先のニーズ等）は、公開したり営業活動に利用したりすることにはなじまず、その予定もない。
詳細な取引先情報については、秘密として管理すべき情報資産であると判断することが考えられる。
- b) 広報戦略に関する委託先の選定基準は、社内の機密事項であるため、外部に漏れてはならず、秘密として管理すると判断する。他方で、新規プロモーション等の方針を表す資料は、既にホームページ等でその資料に基づいた広報が行われているため、公開されているものと判断し、秘密として管理しないものと判断する。
詳細な委託先情報については、秘密として管理すべき情報資産であると判断することが考えられる。

実践例1では、把握した「自社の強みとなる情報資産」の中から、秘密として管理すると判断した「取引先情報（取引先情報データベース）」について、その管理体制の構築手順を述べることとする。

【実践例 2（設計情報）】

事業者	各種検査機器の製造販売、受託開発を主たる事業とする株式会社
営業秘密	自社が製造する各種検査機器の設計情報

（重要な情報資産の把握）

- 1) 自社にとって相対的に高い売上げを上げている商品が何かを検討する。
自社の売上げが最も高い商品は に関する検査機器「M-01」である。
- 2) 1) の製品等の売上げが高い理由を分析する。
同業他社の同種検査機器と比較し、精密な検査が可能である上、その品質が安定していることが相対的な優位性を有していると判断される。
精緻な検査が可能：ミクロン単位で検査位置を調節できる技術によって実現
品質の安定性：製造工程、設計図面及び人材教育によって実現
よって、ミクロン単位で検査位置を調節できるために用いられている技術（及びその関連技術）及び安定した品質を保持するための製造工程、設計図面及び人材教育が自社の強みとなる知的資産であり、それを構成する検査機器「M-01」の設計に関する技術情報、製造工程、設計図面（に記載された情報）、人材教育のためのマニュアルが自社の強みとなる情報資産である。

（営業秘密として管理すべき情報資産の把握）

- a) ミクロン単位で検査位置を調節できるための技術は、特許性が高い発明である上、製品（検査機器「M-01」）をリバースエンジニアリングすることによって比較的容易に特定することができる。
営業秘密として保護することよりも特許権を取得する方が望ましいと判断することが考えられる。
- b) 製造工程、設計図面（に記載された情報）については、当該情報を不正に使用（侵害）された場合の立証が困難である上、製品（検査機器「M-01」）のリバースエンジニアリングなどによって判別することは非常に困難である。
特許権等を取得するのではなく、営業秘密として管理する方が望ましいと判断することが考えられる。
なお、他の自社製品（各種検査機器）について同様の検討を行った結果、それらの設計図面等についても同様に営業秘密として管理する方が望ましいと判断することが考えられる。
- c) 人材教育のためのマニュアルについては、一般的な教材等を基に作成しており、むしろ人材確保のために自社の人材育成に関する取組内容を詳細に宣伝したい。
自社が開設するホームページの採用情報欄に掲載するなどして人材確保のために活用することが考えられる。

実践例 2 では、把握した「自社の強みとなる情報資産」の中から、秘密として管理すると判断した「自社が製造する各種検査機器の設計情報」の管理体制の構築手順について述べることとする。

4. 事業者における営業秘密の管理体制の構築・管理ルールの導入³

(1) 管理状況及び管理水準の現状把握

営業秘密として管理すると判断した情報について、管理状況及び管理水準の現状を把握する。この際、営業秘密管理チェックシート(参考資料1)などを利用する。
(営業秘密管理チェックシートを用いることにより、秘密とすべき情報資産の管理における問題点の「気づき」を得るなど、現状把握に資するものと考えられる。)

事業者が営業秘密として管理すると判断した情報を管理する体制を構築するに当たり、現状の管理状況及び管理水準を把握することで、より効率的、効果的に管理体制を構築することが可能となると考えられる。

そこで、このような現状把握のため、秘密管理性に関して判断をした裁判例の分析を踏まえ、営業秘密の管理の観点から、様々な管理項目についてチェック項目及び配点をしている「参考資料1 営業秘密管理チェックシート」を利用することなどが考えられる。営業秘密管理チェックシートを用いて、各管理項目の実施の有無を確認することで、管理の問題点の「気づき」を得るとともに、現状の管理水準(秘密管理性が肯定される可能性の大小)を把握することが可能となるものと考えられる。

以下においては、実践例1及び2について、営業秘密管理チェックシートを用いて確認した現状の管理状況及び管理水準から判明した問題点を紹介する。

³ 【実践例1】及び【実践例2】のいずれの事業者においても、前記「3. 具体的な導入手順例」において述べた把握方法を実施することにより、重要な情報資産はもちろん、営業秘密として管理すべき情報資産についても、更に多くのものを把握することができると考えられる。ただし、以下においては、便宜的に営業上の情報資産としての典型例である取引先情報と技術上の情報資産としての典型例である設計情報のみについて、その管理体制の構築の在り方について紹介するにとどめる。

【実践例 1（取引先情報）】

取引先情報を含む社内情報が社外に漏えいしないための管理を一応実施している（業務時間外は事務所の玄関を施錠、パソコン起動時にパスワード制限を導入）が、未実施の管理項目が多く、当該情報について、他の一般情報と異なり、営業秘密として管理すべき情報であることを認識させるための管理を実施していない。

具体的な管理状況（「-」は具体的な管理方法を規定・実施していない項目）

事業者	ソフト販売・ソフトウェアの受託開発を主たる事業とする株式会社	
従業者数（役員等含む）	6名（社長、事業部長、その他従業者4名）	
秘密指定		
アクセス者（取扱者）	全従業者6名	
アクセス権者の指定	明確な指定なし	
使用場所	事務室（ビルの一室を賃貸し、社長室等をパーティションで分けて使用しており、オフィススペースは小さい）	
存在形態	電子データ、書面	
主な使用実態等	社長及び営業担当者1名が、営業活動において、当該取引先（新規の場合は、同業種・同規模等、類似する取引先）からの過去の受注内容やその対応経緯・結果、製品に対する嗜好などを踏まえ、より取引先のニーズにあった製品を提案するために主に事務所で活用	
取引先等への開示	開示の有無	（事実上開示したことはない）
書面の管理	作成過程等	営業担当者が定期的に「取引先データベース」に追加した情報を印刷し、ファイルに追加的に綴り原本として管理
	秘密表示	
	保管（場所・状態）	原本は営業担当者がファイルに綴り、事業部長の座席の背後にある書棚（無施錠）に他のファイル（秘密として管理する必要のない一般情報を記載した書面を綴っている）とともに保管
	持ち出し	
	複製	
	回収・廃棄	原本は原則として廃棄しない

電子データを記録した媒体の管理	作成過程等	<ul style="list-style-type: none"> ・営業活動に基づき得られた情報（取引先の受注内容、取引先の製品に対する嗜好など）及び、従業者に聞いて把握した受注した製品の進捗状況などについて、営業担当者が定期的に、営業担当者のパソコンに格納されている「取引先データベース」に入力して作成 ・月に一回程度、DVD-Rにバックアップデータを保存
	秘密表示	
	保管（場所・状態）	<ul style="list-style-type: none"> ・パソコンは営業担当者の机上に常時設置 ・DVD-Rは営業担当者の引き出しに保管（無施錠）
	持ち出し	
	複製	
	回収・廃棄	データ再現不能処理を施した上で廃棄
保管施設の管理	施錠	業務時間外は事務所の玄関を施錠
コンピュータ管理（コンピュータ自体の物理的管理は除く）	パスワード等	<ul style="list-style-type: none"> ・パソコン起動時パスワード制限あり ・データベース起動時パスワード制限なし
	外部接続	（外部接続あり）
	その他	ウイルス対策ソフトを導入している
従業者への指導・教育		

【実践例 2（設計情報）】

自社が製造する全ての検査機器の設計図面について、設計開発部及び製造部に限定した取扱いとするなど、社外に漏えいしないための管理をある程度実施している（保管場所以外への持出禁止、設計図面データを保存しているメインコンピュータ等へのアクセス時にパスワード制限を導入等）が、未実施の管理項目が多くある。

具体的な管理状況（「-」は具体的な管理方法を規定・実施していない項目）

事業者	検査機器の製造販売、受託開発を主たる事業とする株式会社	
従業者数（役員等含む）	52名（社長、副社長、部長（4名）設計開発部（10名）製造部（18名）営業部（8名）総務部（10名））	
秘密指定	就業規則に「会社の秘密情報」という記載あり	
アクセス者（取扱者）	30名（設計開発部11名（部長含む）、製造部19名（部長含む））	
アクセス権者の指定	明確に指定した規程等はないが、事実上設計開発部と製造部の従業者のみアクセス可能	
使用場所	設計開発室 製造室	
存在形態	電子データ、書面	
主な使用実態	新たな機器を設計する際に参照（設計開発部） 機器を製造するために使用（製造部）	
取引先等への開示	開示の有無 秘密保持契約 等	<ul style="list-style-type: none"> ・原則として開示しない ・主要取引先から強く要望された場合等には、口頭にて、競合他社等第三者には開示しないよう依頼
書面の管理	作成過程等	<ul style="list-style-type: none"> ・電子データとして作成された設計図面を印刷して原本として設計開発部長が管理 ・設計図面情報を利用する場合には、電子データのまま利用することを推奨しているが、印刷した書面（複製）の利用も多い
	秘密表示	
	保管 （場所・状態）	<ul style="list-style-type: none"> ・原本は設計開発部長の引き出しに保管（無施錠） ・複製は各保管者がその引き出しに保管（無施錠）
	持ち出し	設計開発室、製造室の外部への持出禁止
	複製	
	回収・廃棄	保有者が適宜シュレッダーで廃棄

電子データを記録した媒体の管理	作成過程等	<ul style="list-style-type: none"> ・メインコンピュータ（サーバー）に作成した電子データ（図面、マニュアル）を保存 ・サーバーに保存された電子データに、各アクセス者のパソコン（30台）からアクセスして使用 ・外付けHDD（ハードディスクドライブ）1台にバックアップデータを記録して保管
	秘密表示	
	保管（場所・状態）	<ul style="list-style-type: none"> ・メインコンピュータ（1台）は総務室の机上に常時設置 ・HDDは書面（原本）と同じ
	持ち出し	設計開発室、製造室の外部への持出禁止
	複製	
	回収・廃棄	データ再現不能処理を施した上で廃棄
保管施設の管理	施錠	<ul style="list-style-type: none"> ・業務時間外は施設全体（事務所）の玄関を施錠 ・設計開発室、製造室の出入口の扉は未施錠
コンピュータ管理（コンピュータ自体の物理的管理は除く）	パスワード等	<ul style="list-style-type: none"> ・コンピュータ起動時にパスワード制限あり ・サーバーアクセス時にパスワード制限あり ・サーバー内にある設計情報フォルダ（設計図面、マニュアルが入っている）アクセス時にパスワード制限なし
	外部接続	（外部接続あり）
	その他	ウイルス対策ソフトを導入している
従業者への指導・教育		

(2) 営業秘密・管理ルールの指定・周知・実施

営業秘密として不正競争防止法上の保護を受けるためには、具体的な管理方法を適切に組み合わせることにより合理性のある秘密管理を実施していることが重要である。

セキュリティコストの負担能力に乏しい中小企業等においては、従業員等に対し、日常的に指導することなどによって、自社の秘密を守ることの重要性について意識を向上させたり、秘密管理ルールを周知徹底したりすることなどを特に重視すべきである。

上記の観点を踏まえ、以下のとおり、営業秘密の指定及び管理ルールの導入手順の例を紹介する。

(ア) 目標とする管理水準を検討する。

(イ) 管理方法を選択する(営業秘密の指定・具体的な管理ルールの指定)。

(ウ) 管理ルールを周知・徹底する。

事業者において、営業秘密として管理すると判断された情報について、営業秘密として不正競争防止法上の保護を受けることを目的とする場合には、営業秘密の要件である秘密管理性が肯定される可能性の高い水準の管理体制を構築することが重要である。そのような管理体制を構築するに当たり、営業秘密として管理すると判断された情報については、リスト化するなどして営業秘密として指定するとともに、個別の管理方法を適切に組み合わせることにより合理性のある秘密管理を実施していることが重要である。

営業秘密として不正競争防止法上の保護を受けるための管理体制を構築するためには、本指針「第3章2．営業秘密の管理のために実施することが望ましい秘密管理方法」に例示している手法を参照することが考えられるが、これらを網羅的に実施していない限り保護を受けられないものではなく、裁判所における法的判断においては、事業規模、業種、情報の性質等を踏まえつつ、合理性のある秘密管理を実施していたかが総合的に考慮されているものと考えられる。

また、営業秘密の漏えいは、故意(わざと)によるものかミスによるものかを問わず、内部者等の関与によって発生することが多いところ、これをできる限り防止するという観点から、ハイテクノロジーを用いたセキュリティツールを導入することが考えられる。しかしながら、中小企業等においては、情報管理のために負担することができる資金が限られており、セキュリティツールを導入するために高額なコストを負担することが困難である場合が多い。そこで、このような中小企業等においては、営業秘密の人為的な流出をできる限り防止するため、日常的な指導等により従業員等の秘密管理の重要性等への意識を向上させたり、秘密管理ルールを周知徹底したりすることなどを特に重視すべきである。

このような観点を踏まえつつ、実践例として、ある事業者における営業秘密の指定方法及び管理ルールの導入手順の例を紹介する。

目標とする管理水準を検討する

具体的な管理方法を選択するに当たり、目標とする管理水準を検討する。目標とする管理水準は、その情報（群）の価値・重要性、性質、取扱方法、業務上の効率性、負担可能なセキュリティコスト等の要素を考慮して決定することが望ましい。

なお、目標とする管理水準を検討するに当たって営業秘密管理チェックシートを利用することによって、営業秘密の要件である秘密管理性が認められる可能性がどの程度ある管理水準を目標とすべきか判断するために有益な示唆を得ることができる⁴。

【実践例 1（取引先情報）】・【実践例 2（設計情報）】

各実践例においては、当該秘密情報を用いた業務の効率性を損なうことなく、かつ、具体的な管理方法の導入に当たって格別な費用を要しないものとするを前提として、秘密管理性が認められる可能性が高い水準を目標とした。

管理方法を選択する

目標としている管理水準に達せられるように管理方法の選択を行う。

営業秘密管理チェックシートなどを参考として、管理項目については、できる限り網羅的に管理ルールを決定することが望ましいが、個別のルールを設ける際には、業務の効率性や現場において実践することの容易さなどを十分に考慮すべきであって、いたずらに厳重な管理ルールを設けるべきではない。

なお、各実践例においては、取り組みやすさを考慮し、導入に際して格別の費用を要することなく講じることができる管理方法を選択しているが、事業者においては、上記 に記載した要素を考慮し、必要に応じてよりセキュリティ効果の高い管理方法を導入することも考えられる⁵。

⁴ ただし、営業秘密管理チェックシートにおける得点は、各管理項目において、ハイテクノロジーを用いたセキュリティツールを用いた場合の効果とそのようなツールを用いない管理ルールとの間で点数の差異を明確に設けていないことなどから、必ずしも点数の高低と管理水準の高低とが比例するものではないことに留意すべきである。

⁵ この点については、本指針「第 3 章 2 . 営業秘密の管理のために実施することが望ましい秘密管理方法」に記載している「高度な管理方法」等が参考になるものと考えられる。

(ア) 実践例における基本的な考え方

【実践例 1 (取引先情報)】

オフィス面積の小さい事務所で保管場所が限られており、従業員数が少ないため、従業員内でのアクセス権限の有無を定めたり、その他の情報(を記載した資料)と保管場所(保管庫)を分離して保管したりすることは行わず、営業秘密の指定を明確にし、その秘密表示をした上で、秘密保持の重要性や管理ルールの周知・指導を徹底することによって、秘密であることの認識可能性を高めている。

また、外部者によるアクセスを制限するために、上記に加え、電子データ・書面の複製を原則として禁止することによって情報の拡散を防止するとともに、その社外持ち出しを禁止している。社内の書棚や引き出しは施錠可能なものではないため、保管庫を施錠管理することはできないが、保管庫への保管を徹底するとともに、その付近に外部者が立ち寄ることがないように配慮している。

【実践例 2 (設計情報)】

事業者の組織が複数の部門に分かれていることから、営業秘密の指定とアクセス権者の指定を明確にし、電子データへのアクセス制限を実施した上で、秘密保持の重要性や管理ルールの周知・指導を徹底することによって、秘密であることの認識可能性を高めている。

また、権限のない者によるアクセスを制限するために、上記に加え、電子データを保存しているコンピュータを外部接続せず、その複製も原則として禁止し、更に書面等を含め媒体を保管場所外へ持ち出すことを禁止している。さらに、保管場所(設計開発室・製造室)については、外部者の立入禁止を明確にしている。

(イ) 営業秘密（とそのアクセス権者）を指定する⁶

秘密として管理すると判断された情報はリスト化するなどして営業秘密として経営者等により指定されることが望ましい。秘密管理の対象となる情報を特定することは事業者と従業員双方の認識を共通化し、管理の実効性を高めることになる。

また、指定した営業秘密を取り扱う者（部署、役職等）を限定できる場合には、その者（部署、役職等）をアクセス権者として指定することが望ましい。

営業秘密の指定は、従業員等がその取り扱う情報が営業秘密であると容易に認識できるために、可能な限り具体的に特定することが望ましいが、事業者と従業員等の認識が一致する程度に特定されているか否かがポイントである。

したがって、必ずしも個別具体的に特定せずとも、概括的な概念や情報を記録した媒体によって特定したり、これらを併用して特定したりすることなどによっても、そのような認識を一致させることができる場合があると考えられる。

【実践例1（取引先情報）】

取引先情報については、「取引先情報データベース」を作成することによって一元化していることから、これに記録されている情報のうち、公開されているものを除き、秘密として管理すべき情報と判断した。

そこで、極秘として取り扱うべき情報として「取引先情報データベースに記録された情報（取引先事業者名、受注内容、対応経過等）のうち、当社ホームページに掲載されたものを除く。」を指定し、これをその他の管理方法と併せて「取引先情報の取扱いについて」と題する書面に記載し、周知することとした。

なお、従業員数が少なく、秘密として管理する情報ごとにアクセス制限を行うことは、担当者不在時や緊急時などに業務上の支障が生じかねないことから、従業員全員がアクセスすることができることとしたため、アクセス権者の指定はしていない。

営業秘密の指定手続	社長、事業部長の2名で指定すべき秘密情報及びその管理ルールについて協議し、「取引先情報の取扱いについて」と題する書面において指定 (「取引先情報の取扱いについて」と題する書面において「極秘」と指定。なお、本書面には管理ルールも規定されている)
文書等による営業秘密の指定・特定	「取引先情報の取扱いについて」と題する書面において、極秘として取り扱う情報として「取引先情報データベースに記録された情報（当社ホームページで公表されたものを除く）」を指定 (就業規則、秘密保持契約書には「会社の秘密情報」と記載)
アクセス権者の指定	(全員がアクセスできることが前提のため)
アクセス権者	全従業員6名

⁶ 本指針「第3章2(1)秘密指定、アクセス権者の指定」参照。

【実践例 2（設計情報）】

主力製品である検査機器「M-01」の設計情報のうち、設計図面と設計マニュアルに記載された情報を秘密として管理すべき情報であると判断するとともに、その他の各種検査機器もまた同社の経営戦略上重要な製品であり、その設計図面等も秘密として管理すべきである情報であると判断した。

そこで、営業秘密管理規程（参考資料 2【各種契約書等の参考例】を参照）の別紙に営業秘密として「自社製品である検査機器の設計情報（設計図面、設計マニュアル（いずれも電子データを含む。）に記載された情報）」を指定した。

なお、本規程は、策定した際に、その電子データを共有フォルダに格納し、従業員全員がいつでも閲覧できるようにするとともに、そのことを従業員全員に書面で通知し、その後の朝礼でも連絡することによって周知徹底を図った。

また、アクセス権者については、自社製品である検査機器の設計情報を業務上利用する必要がある「設計開発部、製造部に配属された従業員」と指定することとし、これをその他の管理方法と併せ、設計開発部長が作成した「設計図等に関する取扱いについて」と題する書面に記載し、周知することとした。

営業秘密の指定手続	社長、副社長、各部長（4名）の6名で指定すべき秘密情報について協議し、営業秘密管理規程の別紙において指定
文書等による営業秘密の指定・特定	営業秘密管理規程の別紙において「自社製品の検査機器の設計情報（設計図面、設計マニュアル（電子データ含む））」と指定 （ 秘密情報の管理について一般的な注意事項を記載し、具体的な保管方法等については責任者等によって指示する旨規定） （ 就業規則、営業秘密保持誓約書には「会社の機密事項」と記載）
アクセス権者の指定	設計開発部長作成の「設計図等に関する取扱いについて」と題する書面において、「設計開発部及び製造部に所属する従業員」と指定
アクセス権者	30名（設計開発部11名、製造部19名）

(ウ) 書面等の管理及びコンピュータ管理⁷

(秘密表示、分離保管)⁸

営業秘密が秘密として管理されている情報であることを客観的に認識することができるように、営業秘密が記載・記録されている媒体に秘密であることを示したり(秘密表示)、その他の情報が記載・記録されている媒体と分離して保管したり(分離保管)する。

(保管、持ち出し・複製の制限)⁹

営業秘密が記載・記録されている媒体については、アクセス権者以外の者がアクセスできないように、施錠して保管することが望ましい。また、持ち出しや複製については、客観的認識可能性やアクセス制限を高めるため、できる限り制限的な措置を講じることが望ましい。

(回収・廃棄)¹⁰

営業秘密が記載・記録されている媒体を廃棄する際は、復元不可能な形で実施することが望ましい。

(施設等の管理)¹¹

営業秘密の保管場所については、アクセス権者以外の者がアクセスできないよう管理されていることが重要である。

(コンピュータ管理)¹²

コンピュータ起動時や営業秘密が記録されているファイルに、パスワードを設定することにより、アクセス権者以外からのアクセスを防ぐことができ、またアクセス権者にも秘密であることを客観的に認識することができる。

また、外部ネットワークから遮断するなど、外部からの不正なアクセスを防ぐための対策を講じることが望ましい。

⁷ 本指針「第3章2(2)物理的・技術的管理」参照。

⁸ 同「(ア)秘密表示、分離保管」参照。

⁹ 同「(イ)媒体の保管、持ち出し、複製の制限、廃棄」参照。

¹⁰ 同「(エ)データの消去、廃棄」参照。

¹¹ 同「(ウ)施設等の管理」参照。

¹² 同「技術的管理」参照。

【実践例 1（取引先情報）】

管理方法の選択及びその考え方

（秘密表示、分離保管）

電子データ（データベース）を閲覧することによる利用が中心である上、これを印刷した書面については、オフィス面積の小さい事務所で保管場所が限られているため、その他の資料ファイルなどと保管場所（保管庫）を分離して保管することは困難であった。

そこで、秘密表示することを徹底することとし、データベース名を「取引先情報データベース^{極秘}」と表示することとした。また、書面については、営業担当者が定期的に電子データを印刷したものを原本として「取引先情報^{極秘}」というシールを貼付したファイルに綴ることとした。

（保管、持ち出し・複製の制限）

媒体の持ち出しについては原則禁止としているが、過去の取引状況を参照しつつ営業を行うことで、より効果的に営業活動を行うことができる場合等、持ち出す必要があるケースが存在する。そのようにどうしても持ち出す必要がある場合は、事業部長から許可を得ることを必須とした。

なお、許可を得た場合についても、あくまで従業者の手持ちとしての使用に限り、顧客に見せることは禁止している。

複製については、原則禁止とし、やむを得ない場合は事業部長による許可が必要ということとした。

（回収・廃棄）

廃棄については、従前どおり実施する。

（施設等の管理）

頻繁に来客があるため、営業時間中に事務所を施錠することはできなかったが、原本管理をしている事務担当者の席を奥にし、外来者がその付近を通ることがないようにした。

（コンピュータ管理）

バックアップ作業時には、社長、事業部長、営業担当者のみが知るパスワードを必要とした。ただし、従業者数が少なく、秘密として管理する情報ごとにアクセス制限を行うことは、担当者不在時や緊急時などに業務上の支障が生じかねないことから、データベースにパスワード制限は設けていない。

なお、営業秘密を保存しているパソコンは、営業担当者が外部とのやり取りを頻繁に行う必要があることから、外部接続のまま使用している。

選択した管理方法に基づく管理状況

書面の管理	作成過程等	営業担当者が定期的に「取引先データベース」に追加した情報を印刷し、背表紙に「取引先情報 ^{極秘} 」というシールが貼付されたファイルに追加的に綴り、原本として管理
	秘密表示	書面の右上に ^{極秘} と表示
	保管 (場所・状態)	背表紙に「取引先情報 ^{極秘} 」というシールが貼付されたファイルに綴り、事業部長の座席の背後にある書棚(無施錠)に他のファイル(秘密情報以外の書面を綴っている)とともに保管
	持ち出し	<ul style="list-style-type: none"> ・社外持ち出しは原則禁止 ・営業活動に必要であるなど、やむを得ない場合は事業部長から許可を得て必要な範囲で持ち出す
	複製	<ul style="list-style-type: none"> ・原則禁止 ・やむを得ない場合は事業部長による許可が必要
	回収・廃棄	原本は原則として廃棄せず
電子データを記録した媒体の管理	作成過程等	<ul style="list-style-type: none"> ・営業活動に基づき得られた情報(取引先の受注内容、取引先の製品に対する嗜好など)及び、従業員に聞いて把握した受注した製品の進捗状況などについて、営業担当者が定期的に自己の管理するパソコンに格納されている「取引先データベース」に入力して作成 ・定期的にDVD-Rにバックアップデータを保存
	秘密表示	
	保管 (場所・状態)	<ul style="list-style-type: none"> ・パソコンは各人の机上に常時設置 ・DVD-Rは事業部長の引き出しに保管(無施錠)
	持ち出し	社外持ち出し禁止
	複製	<ul style="list-style-type: none"> ・原則禁止 ・ただし、バックアップ作業は、社長、事業部長、営業担当者のみが知っているパスワードを用いて定期的実施
	回収・廃棄	データ再現不能処理を施した上で廃棄
保管施設(保管場所)の管理	施錠	業務時間外は事務所の玄関を施錠
	その他	事業部長の座席は、事務室の奥にあり、外来者がその付近を通ることがないように配慮している
コンピュータ管理 (コンピュータ自体の物理的管理は「記録媒体の管理」に記載)	パスワード等	コンピュータ起動時パスワード制限あり
	外部接続	(外部接続あり)
	その他	ウイルス対策ソフトを導入している

【実践例 2（設計情報）】

管理方法の選択及びその考え方

（秘密表示、分離保管）

電子データについては、これを保存している「設計・製造情報」フォルダ（メインコンピュータ（サーバー）に保存されている。）へのアクセスのために、アクセス権者のみが知るパスワードを必要とすることによって、（アクセス制限に加えて）秘密であることの認識可能性を高めている。

また、情報の拡散による流出のおそれを防止するため、印刷した書面の利用ではなく電子データによる利用を推奨しているが、従業者によっては電子データを印刷した書面の利用を希望する者がおり、業務上の効率性等の観点からこれを認めることとしている。

ただし、原本と外付けHDD（ハードディスクドライブ）については、秘密文書を保管する専用のキャビネットに分離保管することで、秘密であることの認識可能性を高めることとした。

（保管、持ち出し・複製の制限）

従前どおり、設計開発室、製造室の外部への持ち出しを禁止としている。

原本と外付けHDDについては、秘密文書を保管するキャビネットに施錠することにより分離保管することとした。

（回収・廃棄）

廃棄については、従前どおり実施する。

（施設等の管理）

従前の管理に加え、設計開発室及び製造室の扉に「関係者以外立入禁止」と表示し、業務時間外は出入口の扉を施錠することで、関係者以外の者が無用に立ち入ることがないようにした。

また、外来者が来た場合は、別室で対応することで、営業秘密を見られないよう配慮した。

（コンピュータ管理）

従前から実施していたアクセス制御に加え、バックアップ作業時には、設計開発部長のみが知るパスワードを必要とし、また、サーバー内にある設計情報フォルダ（設計図面、マニュアルが入っている。）にアクセス制限を加えた。ただし、様々な図面に頻繁にアクセスする必要があり、各ファイルにパスワード制限を設けると非効率になるため、ファイルへのアクセス時のパスワード制限は設けていない。

また、営業秘密が保存されているメインコンピュータ及びそれにアクセスすることができるコンピュータを外部ネットワークから遮断した。

選択した管理方法に基づく管理状況

書面の管理	作成過程等	<ul style="list-style-type: none"> 電子データとして作成された設計図面を印刷して原本として設計開発部長が管理 設計図面情報を利用する場合には、電子データのまま利用することを推奨しているが、印刷した書面（複製）の利用も多い
	秘密表示	
	保管（場所・状態）	<ul style="list-style-type: none"> 原本は設計開発部長が秘密文書を保管するキャビネットにファイルに綴って施錠保管 複製は取扱者各人がその引き出しに保管（無施錠）
	持ち出し	設計開発室、製造室の外部への持出禁止
	複製	
	回収・廃棄	<ul style="list-style-type: none"> 原本は原則として廃棄しない 複製は取扱者が適宜シュレッダーで廃棄
電子データを記録した媒体の管理	作成過程等	<ul style="list-style-type: none"> メインコンピュータ（サーバー）に作成した電子データ（図面、マニュアル）を保存 サーバーに保存された電子データに、各アクセス者のパソコンからアクセスして使用 外付けHDDにバックアップデータを記録し保管
	秘密表示	
	保管（場所・状態）	<ul style="list-style-type: none"> メインコンピュータは総務室の机上に常時設置 外付けHDDは設計開発部長が秘密文書を保管するキャビネットの中に施錠保管
	持ち出し	設計開発室の外部への持出禁止
	複製	<ul style="list-style-type: none"> 他の記録媒体への複製は原則禁止 ただし、バックアップ作業は、設計開発部長のみが知っているパスワードを用いて定期的実施
	回収・廃棄	データ再現不能処理を施した上で廃棄
保管施設（保管場所）の管理	施錠	業務時間外は設計開発室及び製造室の出入口の扉を施錠
	その他	<ul style="list-style-type: none"> 設計開発室と製造室の扉には「関係者以外立ち入り禁止」と表示 外来者は、応接室（別室）で対応
コンピュータ管理（コンピュータ自体の物理的管理は「記録媒体の管理」に記載）	パスワード等	<ul style="list-style-type: none"> コンピュータ起動時にパスワード制限あり サーバー内にある設計情報フォルダ（設計図面、マニュアルが入っている）アクセス時にパスワード制限あり（アクセス権者のみ知っている）
	外部接続	外部接続なし（特定のコンピュータのみ接続）
	その他	サーバーに集中して保存

(工) 従業者等の管理¹³

就業規則・契約等により秘密保持義務を明確化するとともに、秘密管理の重要性、自社の秘密管理ルール等について、教育・研修を実施する。

【実践例 1 (取引先情報)】

管理方法の選択及びその考え方

まず、従業者の秘密保持義務を明確化するために、就業規則に秘密保持義務規定を設けた上、更に全従業者との間で秘密保持契約を締結することとした。

その上で、従業者に対し、各人が取り扱う営業秘密の価値、秘密を保持することの重要性、具体的な管理の在り方について教育することとした。具体的には、定期的に行う朝礼において注意喚起したり、日常業務の際に適宜指導したりすることとした。

選択した管理方法に基づく管理状況

従業者への指導・教育	<ul style="list-style-type: none">・朝礼において、定期的に社長が営業秘密の取扱いに関する注意喚起をする(顧客情報の漏えいが報道された際などに、取引先情報を管理する必要性について説明したり、「取引先情報の取扱いについて」に記載した具体的な管理方法の説明やその実施の徹底を指導したりする)・社長において、日常的に管理ルールが守られているか確認を行い、適切に実施されていない場合は、その都度指導する
秘密保持義務の明確化	<ul style="list-style-type: none">・就業規則に秘密保持義務規定を設ける・従業者全員との間で秘密保持契約書を締結する(営業秘密については「会社の秘密情報」と記載)

【実践例 2 (設計情報)】

管理方法の選択及びその考え方

従前から就業規則に秘密保持義務規定を設けていたことに加え、実践例 1 と同様、従業者全員との間で秘密保持契約を締結することとした。

また、実践例 1 と同様に従業者に対する教育に取り組むこととした。具体的な在り方としては、一般的な研修として、従前から実施していた従業者全員を対象とする定期研修(年 1 回)の中に営業秘密管理の重要性等に関するカリキュラムを導入することとし、個別的な指導については、各部長が日常業務において指導を徹底することとした。

¹³ 本指針「第 3 章 2 (3) (ア) 従業者等に対する教育・研修の実施、(イ) 就業規則・契約等による従業者、退職者等への秘密保持の要請」参照。

選択した管理方法に基づく管理状況

従業者への指導・教育	<ul style="list-style-type: none"> ・年1回の社内研修において、秘密管理の重要性に関する意識を向上させる ・各部長において、日常的に管理ルールが守られているか確認を行い、適切に実施されていない場合は、その都度指導する
秘密保持義務の明確化	<ul style="list-style-type: none"> ・就業規則に秘密保持義務規定を設ける ・従業者全員との間で秘密保持契約書を締結する (営業秘密については「会社の機密事項」と記載)

(オ) 取引先等¹⁴

取引先に開示する場合であっても秘密管理性を維持することが必要なため、開示する場合には、秘密保持契約を締結することが重要である。

【実践例1 (取引先情報)】

管理方法の選択及びその考え方

従前から取引先等の外部者に対して開示していなかったが、特段の内部ルールがなかったことから、外部者に開示してはならないことを書面(前記「取引先情報の取扱いについて」と題する書面)において明確にした。

選択した管理方法に基づく管理状況

取引先等への開示	開示の有無	開示してはならない
----------	-------	-----------

【実践例2 (設計情報)】

管理方法の選択及びその考え方

従前は、取引先から開示を求められた都度責任者が判断しており、開示しなくてはならない場合には、口頭で秘密保持を依頼するように指示していたが、特段の内部ルールがなかったことから、内部ルールを書面(前記「設計図等に関する取扱いについて」と題する書面)において明確化した。具体的には、原則として開示してはならないが、開示する必要がある場合には、取引先が秘密保持義務を負うことを明確にするため、秘密保持契約を締結しなければならないこととした。

選択した管理方法に基づく管理状況

取引先等への開示	開示の有無	<ul style="list-style-type: none"> ・原則として開示してはならない ・開示する必要がある場合には秘密保持契約を締結した上で開示しなければならない (秘密保持契約では営業秘密を「提供した製品に関する設計図面及びその電子データ」と指定)
----------	-------	---

¹⁴ 本指針「第3章2 (3)(オ)取引先」参照。

営業秘密・管理ルールの周知・実施¹⁵

事業者において、営業秘密として指定すべき情報を特定し、目標とする管理水準に到達する管理ルールを決定した場合には、関係者間において適切に認識を共有し、その管理の実効性を確保することができるように、これらを書面に記載するなどして従業者等に周知徹底し、従業者等に管理ルールを適切に実行させるようにすることが重要である。

【実践例 1（取引先情報）】

前記「取引先情報の取扱いについて」と題する書面において、「取引先情報データベース」を「極秘」として取り扱わなくてはならないことと、その具体的な管理ルールについて明記した。

当該書面は、その写しを従業者全員に配布するとともに、電子データについては共有ドライブに保存し、従業者全員がアクセスできるようにした。

また、朝礼における注意喚起や日常業務における指導の中で、秘密管理の重要性に対する理解を高めるとともに、管理ルールの周知及びその徹底した実施の指導を行うようにした。

【実践例 2（設計情報）】

前記「設計図等に関する取扱いについて」と題する書面において、アクセス権者が「設計開発部及び製造部に所属する従業者」であることと、その具体的な管理ルールについて明記した。

当該書面は、その写しを設計開発部及び製造部の従業者に配布するとともに、電子データについてはメインコンピュータ（サーバー）に格納し、アクセス権者全員がアクセスできるようにした。

また、定期研修や日常業務における指導の中で、秘密管理の重要性に対する理解を高めるとともに、管理ルールの周知及びその徹底した実施の指導を行うようにした。

¹⁵ 本指針「第3章3（3）（イ）実施（責任者の設置、従業者への周知徹底）<Do>」参照。

(3) チェック・見直しの実施¹⁶

構築した管理ルールが現場で実践されず、実効性を欠く事態に陥っている場合には、営業秘密として認められないおそれがあるため、経営者等が日常的に現場の管理状況を確認することにより、実効的な管理がなされているかをチェックすることが望ましい。その結果、管理ルールが現場で守られていないなど、実効的な管理が損なわれている場合には、その要因に応じて対応策を講じる必要がある。

また、必要に応じて、自社の強みとなる情報資産を適切に把握するための見直しを行うことが望ましい。

構築した管理ルールが現場で実践されず、実効性を欠く事態に陥っている場合には、営業秘密として認められないおそれがある。そのため、秘密管理の実効性が確保されているかを確認し、問題とすべき状況が生じた場合には、その状況を改善することが必要である。

この場合、経営者等が日常的に現場の管理状況を確認することにより、管理ルールに基づいて実効的な管理がなされているかをチェックすることが望ましい。その結果、何らかの問題点があり、管理の実効性が損なわれていると判断された場合には、その問題点が管理ルールそのものにあるのか、管理ルールそのものではなく、適切に実施・運用すべき人（個人、部門、組織）の意識等にあるのかなどの要因を検討する。

管理ルールそのものに問題がある場合には、現状のルールの問題点を洗い出した後、ルールを見直しし、周知・徹底を行う必要がある。

管理ルールそのものではなく、実施・運用する人の意識等が要因である場合には、その関係する者に対し、秘密管理の重要性に対する意識の向上や管理ルールを遵守するための指導を徹底する。

このほか、管理ルール構築後に秘密として管理すべき情報を創出・取得しているにもかかわらず、これを指定・管理していないことに問題がある場合や、もはや秘密管理する必要がなくなっているにもかかわらず厳重な管理をすることによって無駄が生じている場合等にあっては、営業秘密として管理すべき情報を改めて判断すべきである。この際、再度「自社の強みとなる情報資産の把握」を行うことも考えられる。

また、新しい事業分野に進出するため、営業秘密として指定すべき新たな情報を創出・取得する可能性が高い場合等においては、必要に応じて、自社の強みとなる情報資産を適切に把握するための見直しを行うことが望ましい。

¹⁶ 本指針「第3章3(3) (ウ)(エ)」参照。

【実践例 1（取引先情報）】

オフィスが狭く、従業員（役員等を含む。）も少数（6名）であるため、社長において、日常的に従業者全員に目を配り、管理ルールが守られているか確認し、従業員の怠慢など、管理ルールに問題はないが適切に実施されていない場合は、その都度指導し、必要に応じて朝礼において注意喚起することとした。管理ルールに基づく管理の実効性が確保されていなかった場合には、従業員にヒアリングするなどして、その要因を検討し、必要に応じて管理ルールを見直し、周知・徹底を行うこととした。

また、受託開発を業務の中心としているものの、今後は自社製品の開発・販売を促進し、拡大していきたいと考えていることから、営業活動や研究開発を通じて新たなニーズ・アイデアが掘り起こされることによって新製品の構想が具体化した際などには、指定の見直しを兼ねて「自社の強みとなる情報資産の把握」を行うことを考えている。

チェック・見直し	<ul style="list-style-type: none">・社長において、日常的に管理ルールが守られているか確認を行い、適切に実施されていない場合は、その都度指導する・管理ルールに基づく管理の実効性が確保されていなかった場合は、従業員にヒアリングするなどして、その要因を検討し、必要に応じて管理ルールを見直し、周知・徹底を行う・事業展開に向けて新製品の開発構想が具体化した際などには、指定の見直しを兼ね、「自社の強みとなる情報資産の把握」を行う
----------	---

【実践例 2（設計情報）】

事業者の組織が、複数の部門に分かれており、従業員（役員等を含む。）も52名と比較的規模が大きいため、経営者自らが日常的に確認することが難しいことから、各部長において、実践例1と同様の視点で、管理ルールが守られているかを日常的に確認することとした。

なお、現時点においては、新しい事業分野に進出したり、これまで製造してきた検査機器と種別を全く異なる機器を製造したりする予定はないが、今後そのような事業展開がなされて営業秘密として指定すべき新たな情報資産を創出・取得する可能性が高い場合などには、必要に応じて自社の強みとなる情報資産を適切に把握するための見直しを行うことを考えている。

チェック・見直し	<ul style="list-style-type: none">・各部長において、日常的に管理ルールが守られているか確認を行い、適切に実施されていない場合は、その都度指導する・管理ルールに基づく管理の実効性が確保されていなかった場合は、従業員にヒアリングするなどして、その要因を検討し、必要に応じて管理ルールを見直し、周知・徹底を行う・事業展開がなされて営業秘密として指定すべき新たな情報資産を創出・取得する可能性が高い場合等においては、必要に応じて自社の強みとなる情報資産を適切に把握するための見直しを行う
----------	--

5. (参考) 実践例において導入された営業秘密管理体制の全体像

【実践例1 (取引先情報)】

事業者	ソフト販売・ソフトウェアの受託開発を主たる事業とする株式会社	
従業者数 (役員等含む)	6名 (社長、事業部長、その他従業者4名)	
営業秘密	取引先情報 (「取引先情報データベースに記録された情報 (当社ホームページで公表されたものを除く)」)	
組織的管理	基本方針等	就業規則 (秘密遵守、秘密保持義務を規定)
	指定、実施	<ul style="list-style-type: none"> ・ 社長、事業部長の2名で指定すべき秘密情報及びその管理ルールについて協議し、「取引先情報の取り扱いについて」と題する書面において指定 (本書面には管理ルールも規定されている) ・ 同書面及び指導に基づき、実施
	チェック・見直し	<ul style="list-style-type: none"> ・ 社長において、日常的に管理ルールが守られているか確認を行い、適切に実施されていない場合は、その都度指導する ・ 管理ルールに基づく管理の実効性が確保されていなかった場合は、従業者にヒアリングするなどして、その要因を検討し、必要に応じて管理ルールを見直し、周知・徹底を行う ・ 事業展開に向けて新製品の開発構想が具体化した際などには、指定の見直しを兼ね、「自社の強みとなる情報資産の把握」を行う
文書等による営業秘密の指定・特定	「顧客情報の取り扱いについて」と題する書面において、極秘として取り扱う情報として「取引先データベースに記録された情報 (当社ホームページで公表されたものを除く)」を指定 (就業規則、秘密保持契約書には「会社の秘密情報」と記載)	
アクセス権者の秘密保持義務の明確化	<ul style="list-style-type: none"> ・ 就業規則 ・ 秘密保持契約書 	
アクセス権者の指定	(全員がアクセスできることが前提のため)	
アクセス権者	全従業者6名	
使用場所	事務室 (ビルの一室を賃貸し、社長室等をパーティションで分けて使用しており、オフィススペースは小さい)	
存在形態	電子データ、書面	

主な使用実態等		社長及び営業担当者1名が、営業活動において、当該取引先（新規の場合は、同業種・同規模等、類似する取引先）からの過去の受注内容やその対応経緯・結果、製品に対する嗜好などを踏まえ、より取引先のニーズにあった製品を提案するために主に事務所内で活用
取引先等への開示	開示の有無	開示してはならない
書面の管理	作成過程等	営業担当者が定期的に「取引先データベース」に追加した情報を印刷し、背表紙に「取引先情報[極秘]」というシールが貼付されたファイルに追加的に綴り、原本として管理
	秘密表示	書面の右上に「[極秘]」と表示
	保管 (場所・状態)	背表紙に「取引先情報[極秘]」というシールが貼付されたファイルに綴り、事業部長の座席の背後にある書棚（無施錠）に他のファイル（秘密情報以外の書面を綴っている）とともに保管
	持ち出し	<ul style="list-style-type: none"> ・社外持ち出しは原則禁止 ・営業に必要な場合など、やむを得ない場合は事業部長より許可得て必要な範囲で持ち出す
	複製	<ul style="list-style-type: none"> ・原則禁止 ・やむを得ない場合は事業部長による許可が必要
	回収・廃棄	<ul style="list-style-type: none"> ・原本は原則として廃棄せず
電子データを記録した媒体の管理	作成過程等	<ul style="list-style-type: none"> ・営業活動に基づき得られた情報（取引先の受注内容、取引先の製品に対する嗜好など）及び、従業員に聞いて把握した受注した製品の進捗状況などについて、営業担当者が定期的に、自己が管理するパソコンに格納されている「取引先データベース」に入力して作成 ・定期的にDVD-Rにバックアップデータを保存
	秘密表示	
	保管 (場所・状態)	<ul style="list-style-type: none"> ・パソコンは各人の机の上に常時設置 ・DVD-Rは営業担当者の引き出しに保管（無施錠）
	持ち出し	社外持ち出し禁止
	複製	<ul style="list-style-type: none"> ・原則禁止 ・ただし、バックアップ作業は、社長、事業部長、営業担当者のみが知っているパスワードを用いて定期的に実施
	回収・廃棄	データ再現不能処理を施した上で廃棄

保管施設（保管場所） の管理	施錠	業務時間外は事務所の玄関を施錠
	その他	事業部長の座席は、事務室の奥にあり、外来者がその付近を通ることがないように配慮している
コンピュータ管理 （コンピュータ自体の 物理的管理は「記録媒 体の管理状況」に記載）	パスワード 等	コンピュータ起動時パスワード制限あり
	秘密表示	
	外部接続	（ 外部接続あり）
	その他	ウイルス対策ソフトを導入している
従業者への指導・教育		<ul style="list-style-type: none"> ・朝礼において、定期的に社長が営業秘密の取扱いに関する注意喚起をする（顧客情報の漏えいが報道された際などに、取引先情報を管理する必要性について説明したり、「取引先情報の取扱いについて」に記載した具体的な管理方法の説明やその実施の徹底を指導したりする） ・社長において、日常的に管理ルールが守られているか確認を行い、適切に実施されていない場合は、その都度指導する
秘密保持義務の明確化		<ul style="list-style-type: none"> ・就業規則に秘密保持義務規定を設ける ・従業者全員との間で秘密保持契約書を締結する （ 営業秘密については「会社の秘密情報」と記載）

【実践例 2（設計情報）】

事業者		検査機器の製造販売、受託開発を主たる事業とする株式会社
従業者数（役員等含む）		52名（社長、副社長、部長（4名）、設計開発部（10名）、製造部（18名）、営業部（8名）、総務部（10名））
営業秘密		自社製品の検査機器の設計情報（図面、マニュアル（電子データ含む））
組織的管理	基本方針等	就業規則（秘密遵守、秘密保持義務を規定） 営業秘密管理規程の別紙において営業秘密を指定（秘密情報の管理について一般的な注意喚起を記載し、具体的な保管方法等については責任者等によって指示する旨規定）
	指定、実施	<ul style="list-style-type: none"> ・社長、副社長、各部長（4名）の6名で指定すべき秘密情報について協議し、営業秘密管理規程の別紙において指定 （就業規則、営業秘密保持誓約書には「会社の機密事項」と記載） ・当該営業秘密の管理方法については、設計開発部長作成の「設計図等に関する取扱いについて」と題する書面において規定 ・同書面及び指導に基づき、実施
	チェック・見直し	<ul style="list-style-type: none"> ・各部長において、日常的に管理ルールが守られているか確認を行い、適切に実施されていない場合は、その都度指導する ・管理ルールに基づく管理の実効性が確保されていなかった場合は、従業者にヒアリングするなどして、その要因を検討し、必要に応じて管理ルールを見直し、周知・徹底を行う ・事業展開がなされて営業秘密として指定すべき新たな情報資産を創出・取得する可能性が高い場合等においては、必要に応じて自社の強みとなる情報資産を適切に把握するための見直しを行う
秘密指定（文書等）		<ul style="list-style-type: none"> ・営業秘密管理規程の別紙において「自社製品の検査機器の設計情報（図面、マニュアル（電子データ含む））」と指定 （秘密情報の管理について一般的な注意事項を記載し、具体的な保管方法等については責任者等によって指示する旨規定）

		<ul style="list-style-type: none"> 取引先との秘密保持契約書では「提供した製品に関する設計図面及びその電子データ」と指定 就業規則、秘密保持誓約書には「会社の機密事項」と記載
アクセス権者の秘密保持義務の明確化		<ul style="list-style-type: none"> 就業規則、営業秘密管理規程 秘密保持誓約書 秘密保持契約書（取引先）
アクセス権者の指定		設計開発部長作成の「設計図等に関する取扱いについて」と題する書面において、「設計開発部及び製造部に所属する従業者」と指定
アクセス権者		30名（設計開発部（部長含む）11名、製造部（部長含む）19名）
使用場所		設計開発室 製造室
存在形態		電子データ、書面
主な使用実態		新たな機器を設計する際に参照（設計開発部） 機器を製造するために使用（製造部）
取引先等への開示	開示の有無 秘密保持契約等	<ul style="list-style-type: none"> 原則として開示してはならない 開示する必要がある場合には秘密保持契約を締結した上で開示しなくてはならない （秘密保持契約では営業秘密を「提供した製品に関する設計図面及びその電子データ」と指定）
書面の管理	作成過程等	<ul style="list-style-type: none"> 電子データとして作成された設計図面を印刷して原本として設計開発部長が管理 設計図面情報を利用する場合には、電子データのまま利用することを推奨しているが、印刷した書面（複製）の利用も多い
	秘密表示	
	保管 (場所・状態)	<ul style="list-style-type: none"> 原本は設計開発部長が秘密文書を保管するキャビネットにファイルに綴って施錠保管 複製は取扱者各人がその引き出しに保管（無施錠）
	持ち出し	設計開発室、製造室の外部への持出禁止
	複製	
	回収・廃棄	<ul style="list-style-type: none"> 原本は原則として廃棄しない 複製は取扱者が適宜シュレッダーで廃棄

電子データを記録した媒体の管理	作成過程等	<ul style="list-style-type: none"> ・メインコンピュータ（サーバー）に作成した電子データ（図面、マニュアル）を保存 ・サーバーに保存された電子データに、各アクセス者のパソコン（30台）からアクセスして使用 ・外付けHDD1台にバックアップデータを記録して保管
	秘密表示	
	保管（場所・状態）	<ul style="list-style-type: none"> ・メインコンピュータは総務室の机上に常時設置 ・外付けHDDは設計開発部長が秘密文書を保管するキャビネットの中に施錠保管
	持ち出し	設計開発室の外部への持出禁止
	複製	<ul style="list-style-type: none"> ・他の媒体等への複製は原則禁止 ・ただし、バックアップ作業は、設計開発部長のみが知っているパスワードを用いて定期的を実施
	回収・廃棄	データ再現不能処理を施した上で廃棄
保管施設（保管場所）の管理	施錠	業務時間外は設計開発室及び製造室の出入口の扉を施錠
	その他	<ul style="list-style-type: none"> ・設計開発室と製造室の扉には「関係者以外立ち入り禁止」と表示 ・外来者は、応接室（別室）で対応
コンピュータ管理（コンピュータ自体の物理的管理は「記録媒体の管理」に記載）	パスワード等	<ul style="list-style-type: none"> ・コンピュータ起動時にパスワード制限あり ・サーバー内にある設計情報フォルダ（設計図面、マニュアルが入っている）アクセス時にパスワード制限あり（アクセス権者のみが知っている）
	秘密表示	
	外部接続	外部接続なし（特定のコンピュータのみ接続）
	その他	サーバーに集中して保存
従業者への指導・教育		<ul style="list-style-type: none"> ・年1回の社内研修において、秘密管理の重要性に関する意識を向上させる ・各部長において、日常的に管理ルールが守られているか確認を行い、適切に実施されていない場合は、その都度指導する
秘密保持義務の明確化		<ul style="list-style-type: none"> ・就業規則に秘密保持義務規定を設ける ・従業者全員との間で秘密保持契約書を締結する（営業秘密については「会社の機密事項」と記載）