

営業秘密の保護・活用について

平成29年 6月 経済産業省 知的財産政策室

1-1 情報流出の現状(主な事例)

基幹技術など企業情報の漏えい事案が多発。サイバー空間での窃取、拡散など漏えい態様も多様化。

抑止力向上と処罰範囲の整備が必要。

新日鐵住金

高額報酬(数億円)で外国ライバル企業へ漏えい →約1000億円の賠償請求

(2012年提訴)

【漏えい】変圧器用の電磁鋼板※の製造プロセスおよび製造設備の設計図等 ※注 20年以上の開発期間を要し、送配電口スを大幅に軽減可能。



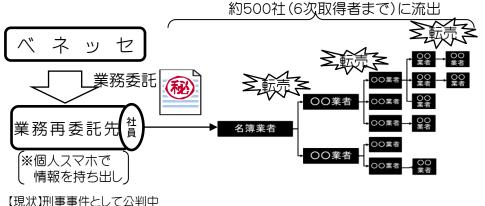
【現状】賠償請求・差止め請求→2015年9月30日に和解(300億円) 米国、韓国の訴訟は取り下げ

ベネッセ

業務委託先からの漏えい・転売

(2014年発生)

【漏えい】氏名・住所等の個人情報(約2億件)



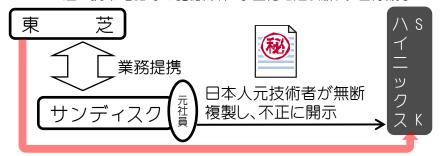
芝 東

提携先から外国ライバル企業へ漏えい

→約330億円で和解

(2012年発生)

【漏えい】NAND型フラッシュメモリ※の仕様およびデータ保持に関する検査方法等 ※注 携帯電話等の記憶媒体。小型化を巡り激しい国際競争。



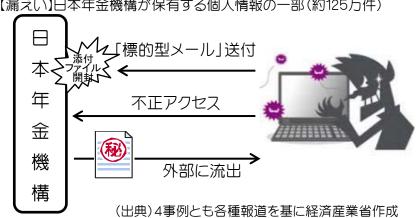
【現状】・賠償請求(約1100億円) → 2014年12月に和解(約330億円) ・元社員の逮捕(懲役5年(実刑)、罰金300万円(2015年9月:東京高裁))

日本年金機構

サイバー攻撃による漏えい

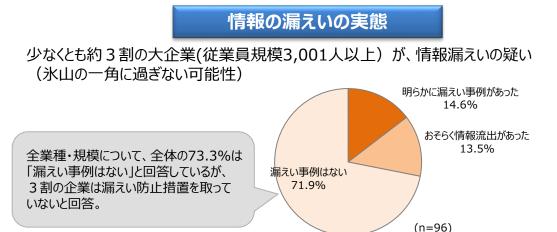
(2015年発生)

【漏えい】日本年金機構が保有する個人情報の一部(約125万件)



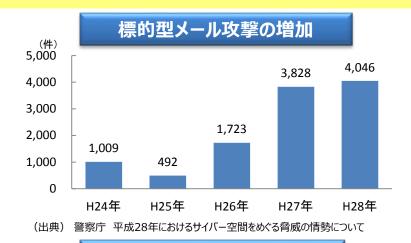
1-2 情報漏えいの態様

漏えいのルートは内部社員による者が多数。近年、サイバー攻撃による漏えいも内外で急増する傾向。



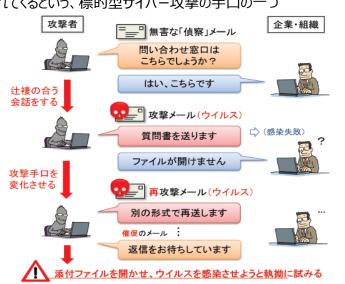
(出典) 平成28年度IPA調査「企業における営業秘密管理に関する実態調査」を元に作成

情報漏えいルート 現職従業員等のミスによる漏えい 43.8% 中途退職者(正規社員)による漏えい 24.8% 前回調査(※)では26.9% 取引先や共同研究先を経由した漏えい 11.4% 前回調査では50.3% 現職従業員等による具体的な動機をもった漏えい 7.6% 前回調査では9.3% 外部からの社内ネットワークへの侵入に起因する漏えい 4.8% 中途退職者(役員)による漏えい 3.8% ※平成24年度「人材を通じた技術流出に関する調査研究」 (経済産業省委託調査事業) 取引先からの要請を受けての漏えい 3.8% (http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf 2.9% 外部者の不正な立ち入りに起因する漏えい 2.9% 退職した契約社員による漏えい 退職した派遣社員による漏えい 1.9% 定年退職者による漏えい 1.0% わからない 4.8% (n=105)その他 9.5%



巧妙化の例: やりとり型攻撃

一般の問い合わせ等を装った無害な「偵察」メールの後、ウイルス付きのメールが送られてくるという、標的型サイバー攻撃の手口の一つ



(出典) IPA:組織外部向け窓口部門の方へ:「やり取り型」攻撃に対する注意喚起 ~ 国内5組織で再び攻撃を確認 ~

2. 不正競争行為類型「営業秘密」の概要

営業秘密の侵害

(第2条第1項第4号~第10号)

窃取等の不正の手段によって営業秘密を取得し、自ら使用し、若しくは第三者に開示する行為等



秘密であることに価値。 公開前提の特許では 守りにくい。 企業の研究・開発や営業活動の過程で 生み出された様々な営業秘密 (例)

- ・顧客名簿や新規事業計画、価格情報、対応マニュアル(営業情報)
- ・製造方法・ノウハウ、新規物質情報、設計図 面(**技術情報**)

不正取得不正使用不正開示



競争秩序ひいては日本全体のイノベーションに悪影響

事例

投資用マンションの販売業を営む会社の従業員が、退職し独立起業する際に、営業秘密である顧客情報を持ち出し、その情報に記載された顧客に対して、転職元企業の信用を毀損する虚偽の情報を連絡した事案。損害賠償請求が認められた。(知財高裁平24.7.4)

事例

石油精製業等を営む会社の営業秘密であるポリカーボ ネート樹脂プラントの設計図面等を、その従業員を通じて 競合企業が不正に取得し、さらに中国企業に不正開示し た事案。その図面の廃棄請求、損害賠償請求等が認めら れた。(知財高裁平23.9.27)

2. 不正競争行為類型「営業秘密」の概要(営業秘密の3要件)

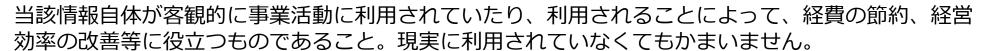
【不競法第2条第6項】この法律において「営業秘密」とは、秘密として管理されている生産方法、販売方法その他事業活動に有用な技術上又は営業上の情報であって、公然と知られていないものをいう。

技術やノウハウ等の情報が「営業秘密」として不競法で保護されるためには、以下の3要件を全て満たすことが必要です。

【秘密管理性】秘密として管理されていること

営業秘密保有企業の秘密管理意思が、秘密管理措置によって 従業員等に対して明確に示され、**当該秘密管理意思に対する 従業員等の認識可能性が確保される必要**があります。

【**有用性**】有用な営業上又は技術上の情報であること





- ・設計図、製法、製造ノウハウ
- ・顧客名簿、仕入先リスト
- ・販売マニュアル



・有害物質の垂れ流し、脱税等の反社会的な活動についての情報は、法が保護すべき正当な事業活動ではないため、有用性があるとはいえない。

【非公知性】公然と知られていないこと

保有者の管理下以外では一般に入手できないこと。



・第三者が偶然同じ情報を開発して保有していた場合でも、当該第三者も当該情報を秘密として管理していれば、非公知といえる。



- ・刊行物等に記載された情報
- ・特許として公開

(参考) 営業秘密管理指針(平成27年1月全部改訂)

(http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/20150128hontai.pdf)

(旧:営業秘密管理指針)

○法解釈に加え、高度な管理方法や普及啓発的事 項も網羅的に紹介。

> 人的管理 (情報管理規程、 守秘契約)

物理的・技術的管理 (アクセス制限、 ⊛マーク)

組織的管理 (情報管理 体制)

○裁判例においての考え方も、不統一ではないかとの 指摘。



- 何をどこまでやればいい?
- ・旧指針を全て行うのは困難
- ・要件を明確化してほしい!

営業秘密管理指針全部改訂:法解釈への特化

○法的保護を受けるために**必要となる最低限の水準の対策を示す** ことに特化するものとして全部改訂。



(旧指針)
漏えい防止レベル
法的保護
レベル **営業秘密管理指針**

<法的保護レベル>

営業秘密保有企業の秘密管理意思(*1)が秘密管理措置によって従業員等に対して明確に示され、当該秘密管理意思に対する従業員等の認識可能性(*2)が確保される必要。(新指針p.5)

※1)特定の情報を秘密として管理しようとする意思。※2)情報にアクセスした者が秘密であると認識できること。

⇒情報に接することができる従業員等にとって、

秘密だと分かる程度の措置



※企業の実態・規模等に応じた合理的手段でよい

- < 秘密だと分かる程度の措置の例>
 - ・紙、電子記録媒体への「マル秘郷」表示
 - ・化体物(金型など)のリスト化
 - ・秘密保持契約等による対象の特定

上記はあくまで例示であり、認識可能性がポイント。



2. 不正競争行為類型「営業秘密」の概要(営業秘密として肯定された事例)

事例

投資用マンションの販売業を営む会社の従業員が、退職し独立起業する際に、営業秘密である顧客情報を持ち出し、その情報に記載された顧客に対して、転職元企業の信用を毀損する虚偽の情報を連絡した事案。損害賠償請求が認められた。(知財高裁平24.7.4)

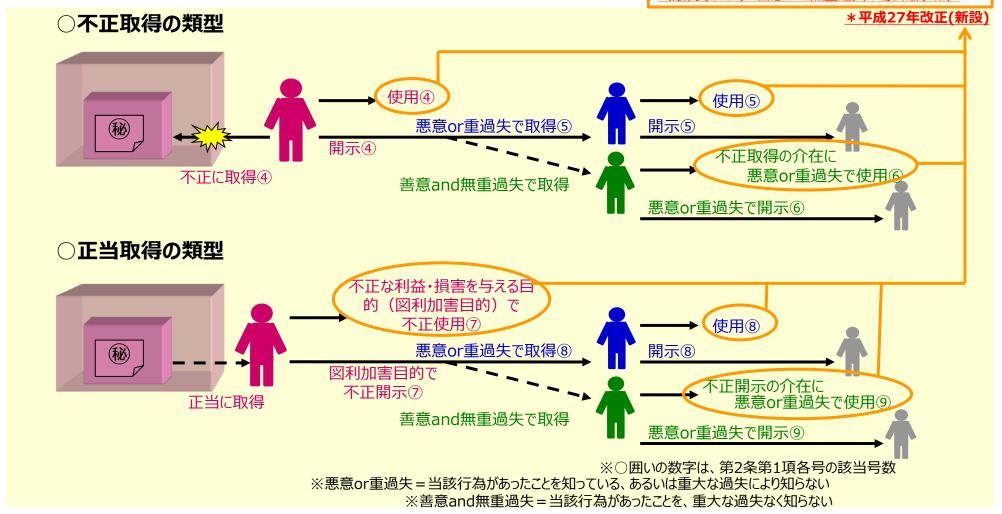
事例

石油精製業等を営む会社の営業秘密であるポリカーボ ネート樹脂プラントの設計図面等を、その従業員を通じて 競合企業が不正に取得し、さらに中国企業に不正開示し た事案。その図面の廃棄請求、損害賠償請求等が認めら れた。(知財高裁平23.9.27)

	事 例 1	事 例 2
営業秘密	顧客情報(氏名・年齢・勤務先・年収・所有物件・賃 貸状況などで構成)	ポリカーボネート樹脂プラントの設計図面
秘密管理性	・入室が制限された施錠付きの部屋において保管・その利用は、営業本部の従業員等に限定←営業のため自宅に持ち帰られたりしていた事情があっても、秘密であることの認識を失わせるものではない	・情報を記録したフロッピーディスクのケース表面に「持ち出 し禁止」のシールが貼付
有用性	この顧客情報を使って営業を行えば効率的に契約を成立させ得るもの	プラントの運転・管理等に不可欠な情報
非公知性	一般に知られていない情報	社外の者に開示されることがおよそ想定されていない情報

(参考) 営業秘密侵害行為類型 (民事)

④~⑨の行為により生じた物の譲渡・輸出入等⑩ (譲り受けた時に善意and無重過失の場合を除く。)



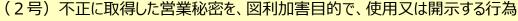
適用除外(第19条)

- ・④~⑨については、その営業秘密が不正取得されたり、不正開示されたりしたものであることについて善意・無重過失で、その営業秘密をライセンス契約などの取引により取得した者が、そのライセンス契約などの範囲内で、その営業秘密を使用・開示する行為には適用されない(取得後に悪意となった場合も含む)。(第19条第1項第6号)
- ・⑩については、時効の成立や除斥期間の経過により差止請求ができなくなった営業秘密の使用行為により生じた物には適用されない。(同項第7号)

(参考) 営業秘密侵害罪の類型 (刑事) (第21条第1項、第3項) ①

○不正な手段(詐欺・恐喝・不正アクセスなど)による取得のパターン

(1号) 図利加害目的で、詐欺等行為又は管理侵害行為によって、 営業秘密を不正に取得する行為

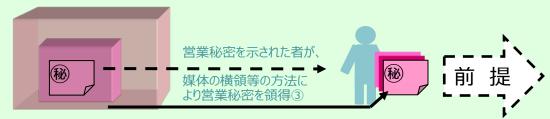






○正当に営業秘密が示された者による背信的行為のパターン

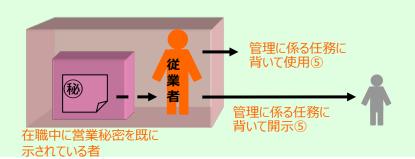
(3号) 営業秘密を保有者から示された者が、図利加害目的で、その営業秘密の管理に 係る任務に背き、(イ) 媒体等の横領、(ロ) 複製の作成、(ハ) 消去義務違反 + 仮装、のいずれかの方法により営業秘密を領得する行為



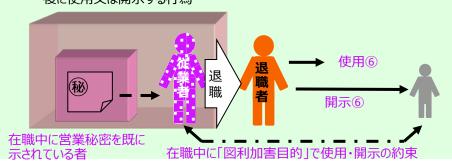
(4号) 営業秘密を保有者から示された者が、第3号の方法によって領得した営業秘密を、図利加害目的で、その営業秘密の管理に係る任務に背き、使用又は開示する行為



(5号) 営業秘密を保有者から示された現職の役員又は従業者が、図利加害目的で、その営業秘密の管理に係る任務に背き、 営業秘密を使用又は開示する行為



(6号) 営業秘密を保有者から示された退職者が、図利加害目的で、在職中に、 その営業秘密の管理に係る任務に背いて営業秘密の開示の申込みを し、又はその営業秘密の使用若しくは開示について請託を受け、退職 後に使用又は開示する行為

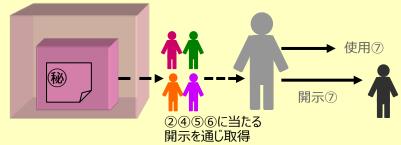


8

(参考) 営業秘密侵害罪の類型 (刑事) (第21条第1項、第3項)②

○転得者による使用・開示のパターン

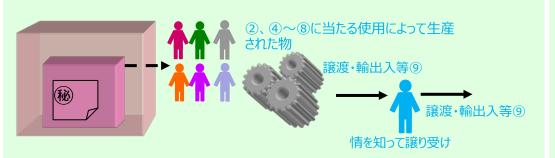
(7号) 図利加害目的で、②、④~⑥の罪に当たる開示(海外重罰の場合を含む)によって取得した営業秘密を、使用又は開示する行為 (2次的な転得者を対象)



○営業秘密侵害品の譲渡等のパターン

<u>* 平成27年改正(新設)</u>

(9号) 図利加害目的で、②、④~⑧の罪に当たる使用(海外重課の場合を含む)によって生産された物を、譲渡・輸出入する行為



刑事規定(第21条第1項、第3項)

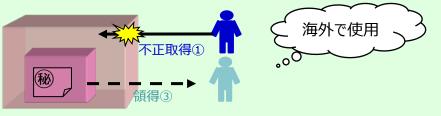
*平成27年改正(罰金額引上げ)

罰 則:10年以下の懲役若しくは2000万円以下の罰金(又はこれの併科) 法人両罰は5億円以下の罰金(第22条第1項第2号)

※海外使用等は個人が3000万円以下、法人は10億円以下。

○海外重罰のパターン(21条3項) * 平成27年改正(新設

(1号)日本国外で使用する目的での①又は③の行為_



(2号)日本国外で使用する目的を持つ相手方に、それを知って ②、④~⑧に当たる開示をする行為

(3号)日本国外で②、④~⑧に当たる使用をする行為



3. 不正競争防止法改正(平成27年7月3日成立)の概要



刑事上・民事上の保護範囲の拡大 (規制の隙間となっていた部分を規制対象とする)

営業秘密の転得者処罰範囲の拡大 📩

最初の不正開示者から開示を受けた者(2次取得者)以降 の者から不正開示を受けた者(3次取得者以降の者)の不正 使用・不正開示行為を処罰対象に追加。

> <2次取得者><3次取得者><4次取得者><5次取得者><6次取得者> ex.新日鐵

改正法:三次取得者以降も

未遂行為の処罰 ★

I Tの高度化により、営業秘密が一旦不正取得されるとインターネットを 通じて瞬時に拡散する危険性が高まったことを踏まえて、営業秘密の不正 取得や不正開示等の未遂を処罰。

営業秘密侵害品の譲渡・輸出入等の規制 ★ ☆

特許権侵害品と同様に、他人の営業秘密の不正使用により生産し た製品の譲渡・輸出入等を禁止。(民事上の損害賠償請求と差止 請求の対象とするとともに、刑事罰の対象にも追加)

国外犯処罰の範囲拡大 ★

不正取得行為を国外犯処罰の対象とすることにより、海外サーバー (クラウドなど) 等に保管された営業秘密を海外において不正取得す る行為を処罰対象とすることを明確化。

<具体例>	日本国内でのサイバー攻撃	海外でのサイバー攻撃
国内サーバー	0	0
海外サーバー	0	?→○

罰則の強化等による抑止力の向上

罰金刑の上限引上げ等 ★

営業秘密侵害罪を犯した個人及び法人に対する罰金刑の上限を引 上げ(海外における不正使用など一定の場合には重罰化)。また、営 業秘密侵害罪を非親告罪化。

任意的没収規定の導入 ★

営業秘密侵害罪により生じた犯罪収益を、裁判所の判断により没収 することができる規定を導入。

民事救済の実効性の向上

損害賠償請求等の容易化(立証負担の軽減) ☆

一定の場合に、生産技術等の不正使用の事実について民事訴 訟上の立証責任を転換。侵害者(被告)が「違法に取得した技 術を使っていないこと を立証。

※注 民訴法上は原告が立証することが原則。

除斥期間の延長

営業秘密の不正使用に対する差止請求の期間制限(除斥期 間)を延長(10年→20年)。

【経過】閣議決定 : 平成27年3月13日、衆議院可決 : 同6月11日、参議院可決・成立 : 同7月3日 【施行】平成28年1月1日。(除斥期間の延長に関する部分のみ公布即施行)

(参考)営業秘密保護法制に関する各国比較 :改正後 ドイツ 日本 (不競法、產業技術流出防止法) (経済スパイ法等) (不正競争防止法) (不正競争防止法) 処罰対象行為 取得·使用·開示 ・取得(制限なし)、その他(送信、郵送等 取得·使用·開示 取得·使用·開示 を含む) (二次取得者まで) (制限なし) (制限なし) 制限撤廃 海外での行為の ・日本企業の営業秘密の ・米国民又は米国法に基づく法人等に 韓国企業の営業秘密の ・ドイツ企業の営業秘密の 処罰 処罰範囲 海外での使用・開示 よる国外における侵害行為の場合 海外での取得・使用・開示 海外での取得・使用・開示 ・米国内において侵害を助長する 海外での窃取行為 (furtherance) 行為が行われた場合 (取得)の追加 犯罪成立時期 共謀•未遂 陰謀•予備•未遂 共謀•未遂 既遂のみ 共謀者のうちの1人以上が目的達成のため 未遂の追加

5年、5000万ウォン(約500万円)以下

・違反行為による利得額の10倍に相当

・国外使用目的の漏えい10年、1億ウォ

ン(違反行為による利得額の10倍に相

当する額が1億ウォンを超える場合は、

×

不要

0

不当利益額の2~10倍以下。

不当利益額の2~10倍)以下

個人と同様

する額が5000万ウォンを超える場合は、

3年以下(罰金は上限なし)

を知っていた場合

100万ユーロ(約1.3億円)以下

(個人・法人とも)

不要

特別の公共の利益がある場合

制度なし

杳察命令

①職業上行う場合

以下の重大な事例は5年以下

②開示の場合にはその秘密が

外国で利用されるであろうこと

③使用を自らが外国で行う場合

の何らかの行為をなす必要

500万ドル(約5億円)又は

10年、罰金の上限なし(※)

※量刑ガイドラインの量刑表に従う額又

は価値の2倍のいずれか高い額以下

価値の3倍のいずれかの大きい額以下

 \circ

(個人・法人とも)

不要

0

ディスカバリ

※量刑ガイドライン上の海外重課あり

自然人

10年、1000万円以下

・懲役:変更なし

•犯罪収益没収

•5億円以下

3億円以下

制度なし→

制度なし →

制度なし →

必要

- 罰金:2000万円以下

[海外重罰∶10億円] ▪犯罪収益没収

(親告罪) → (非親告罪)

創設

(再掲)

創設

立証責任

の転換

海外重罰:3000万円

刑

法定刑

法人

犯罪収益の没収

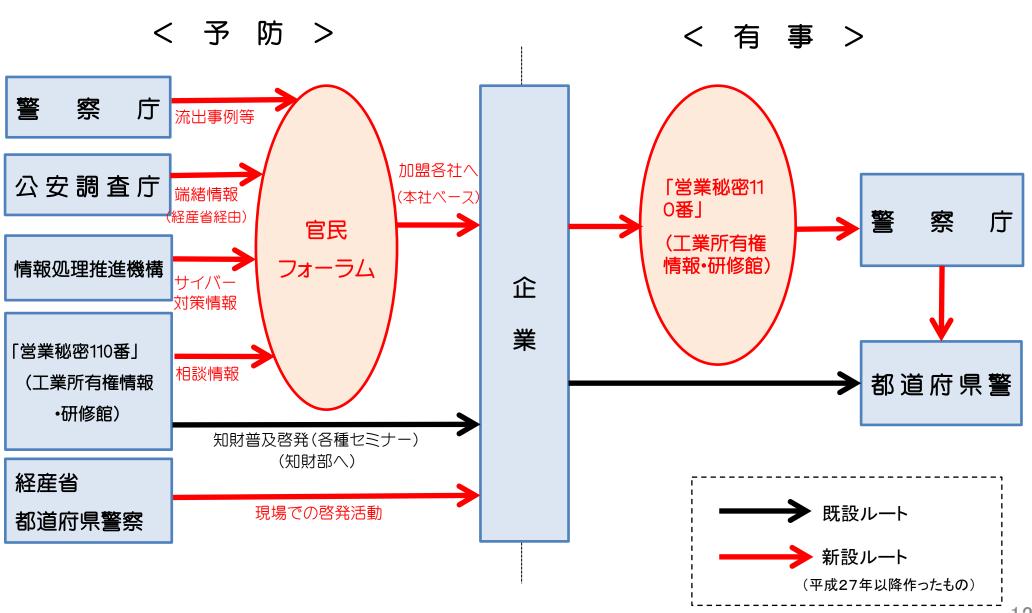
告訴の必要性

輸入禁止

営業秘密侵害物品の

立証責任/証拠収集

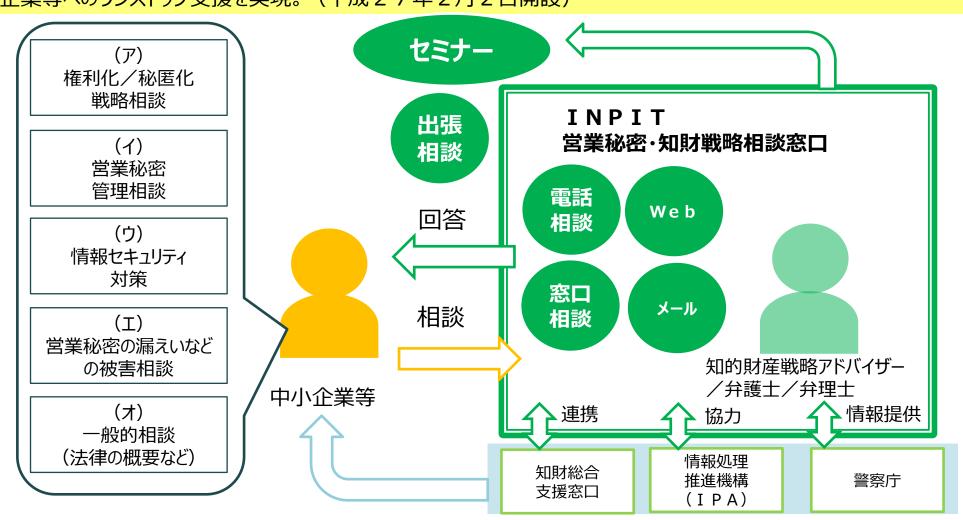
4. 官民の連携の強化



12

(参考) 営業秘密・知財戦略相談窓口(営業秘密110番)

「オープン・クローズ戦略の推進」「営業秘密の保護強化」のため、中小企業等へのワンストップ支援を実現。(平成27年2月2日開設)



相談時間:平日AM9:00-PM5:45

電話番号: 03-3581-1101 内線3844

メール : trade-secret@inpit.go.jp

※営業秘密110番相談件数

平成27年度:250件 平成28年度:450件

(参考)営業秘密官民フォーラムの活動

- 実務者レベルによる継続的な官民連携を通じ、情報漏えい対策の高度化を推進。
- 業界団体、職能団体を経由して「窃取動向」「対策手法」「問題意識」の共有を図る。
- これまでに営業秘密官民フォーラムを2回開催。
- 平成28年7月より、「営業秘密官民フォーラムメールマガジン [営業秘密のツボ] 」の配信を開始 (バックナンバー http://www.ipa.go.jp/security/economics/mailmag/)

「窃取動向」の共有

- 政府からの情報提供
- 業界団体、職能団体からの情報提供

「問題意識」の共有

• 制度・運用に関する課題の把握

営業秘密官民フォーラム (実会合、研修、メルマガ)

「対策手法」の共有

- 政府等からの情報提供、要請 (サイバーセキュリティ対策など)
- 業界団体、職能団体からのグッドプラクティスの紹介、共有
- 具体的手法に関する研修の実施 (労務対策、子会社管理など)



5. 「秘密情報の保護ハンドブック」の検討経緯

営業秘密の漏えい防止対策、漏えい時に推奨される高度な対策を含めた包括的対策を示す「営業秘密保護マニュアル(仮称)」を策定する。

知的財産推進計画 2 0 1 5 (H27.6.19)

漏えい防止レベル

法的保護レベル

営業秘密管理指針 (平成27年1月)

「秘密情報の保護ハンドブック~企業価値向上に向けて~」で対応

より良い漏えい対策を講じたい企業の方々に、企業の実情に応じて対策を取捨選択したり、 参考としていただけるよう、

- 秘密情報の漏えい対策
- 漏えいしてしまった場合の対応策
- 各種規程・契約等のひな形、窓口

など様々な対策を網羅的に紹介。

営業秘密として法的保護を受けるために 必要となる最低限の水準の対策を提示

(検討経緯)

平成27年 1月 『営業秘密管理指針』全部改訂

7月 改正不正競争防止法成立 (平成28年1月1日施行)

平成28年 2月 『秘密情報の保護ハンドブック~企業価値向上に向けて~』策定・公表

http://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html#handbook

12月 『秘密情報の保護ハンドブックのてびき-情報管理も企業力-』策定・公表

http://www.meti.go.jp/policy/economy/chizai/chiteki/2016 11 29 12 08 41/index.html

(参考) ハンドブックの全体構成

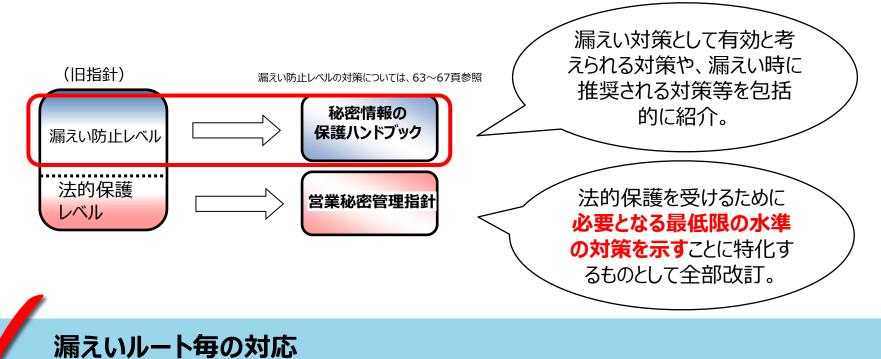
・目的及び全体構成 1章 ・保有する情報の把握・評価、秘密情報の決定 2章 ・秘密情報の分類、情報漏えい対策の選択及びそのルール化 3章 ・秘密情報の管理に係る社内体制のあり方 4章 ・他社の秘密情報に係る紛争への備え 5章 ・漏えい事案への対応 6章 ·各種契約書·規程等の参考例、各種相談窓口等の連絡先、営業秘密侵害罪にかかる刑事訴訟手続、 競業避止義務契約の有効性について 等を掲載 参考資料

16

5-2. 「秘密情報の保護ハンドブック」のポイント



ハンドブックの位置づけ



がおんていいと しょせんシンショルし

①従業員等、②退職者等、③取引先、④外部者 毎に対策が必要。

5-2. 「秘密情報の保護ハンドブック」のポイント



企業の拠り所となる考え方の紹介

- 「管理」と「有効利用」のバランス
- 効率よく講じるための「5つの対策の目的」の設





新たに充実させた内容

- 他社からの訴えに対する備え
- 有事における対応

5-3. 「秘密情報の保護ハンドブック」情報漏えい対策 ~全体像~

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、管理と有効活用のバランスを取りましょう。

例) 自社の強みとなる情報資産の例

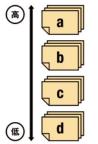
研究開発情報(実験データ、試作品情報等)、製造関連情報(製品図面、製品テストデータ、製造プロセス、工場設備・レイアウト)

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

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 (損失の大きさ順に情報を序列化)

相対的な階層化 (損失の大きさを評価)





企業の情報活用の例

~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 部品構造(他者が容易に把握可)	生産プロセス素材配合

Y. 他社の情報も保護

乙. もしも情報漏えいが発生したら

「秘密情報の保護ハンドブック」情報漏えい対策 5 - 3. ~効率よく講じるための5つの「対策の目的」~

- 漏えい要因を考慮した5つの「対策の目的」を設定。
- 各社の状況に応じ、ルートごと、目的ごとにムリ・ムダ・ムラのない形で対策を取捨選択。

物理的・技術的な防御

接近の制御

持出し困難化

心理的な抑止

視認性の確保

秘密情報に対する認 識向上

働きやすい環境の整備

信頼関係の 維持・向上等



秘密情報に近寄りにくく するための対策



秘密情報の持ち出しを 困難にするための対策



漏えいが見つかりやすい 環境づくりのための対策



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

- □ マル秘表示
- ルールの策定・周知
- 秘密保持契約の締結
- 無断持出禁止の張り紙 □ 研修の実施



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

- ワーク・ライフ・バランスの推進
- □ コミュニケーションの促進
- □ 社内表彰
- □ 漏えい事例の周知

- □ アクセス権の設定
- 秘密情報を保存したPCを不必 要にネットに繋がない
- □ 構内ルートの制限
- □ 施錠管理
- □ フォルダ分離
- □ ペーパーレス化 ■ ファイアーウォールの導入 等
- 私用USBメモリの利用・持込 み禁止
- □ 会議資料等の回収
- 電子データの暗号化
- □ 外部へのアップロード制限 等
- 座席配置・レイアウトの工夫
- 防犯カメラの設置
- 職場の整理整頓
- 関係者以外立入禁止看板(窓口 明確化)
- PCログの記録
- 作業の記録(録画等)

(参考) 秘密情報の漏えい対策の5つの目的~犯行の段階に応じた対策の選択~



悪意の発現

実行の決意

実行の着手

既遂 (持ち出し)

社員のやる気を高めるための対策

【信頼関係の維持・向上等】⑤

(例:ワークライフバランス、社内コミュニケーション)

「秘密情報と思わなかった」という事態を招かないための対策 【秘密情報に対する認識向上(不正行為者の言い逃れの排除)】 ④ (例:マル秘表示、規程類・管理ルールの策定・周知、教育・研修の実施)

漏えいが「見つかりやすい」環境づくりのための対策 【視認性の確保】③ (例:レイアウトの工夫(座席配置)、防犯カメラの設置、アクセスログの記録)

秘密情報に「近よりにくくする」 ための対策 【接近の制御】①

(例:アクセス権の限定、秘密情報を保存したPCはインターネットにつながない)

秘密情報の「持出しを困難にする」 ための対策【持出し困難化】② (例: 私物USBメモリ等の利用・持込み禁止)





窃取行為の回避/断念/失敗

【対策の取捨選択の考え方】

- ・アクセス可能な者が多数に設定されている場合には、視認性の確保」や「持出し困難化」が対策の中心。
- ・従業員の多様化の程度が大きいほど、「信頼関係の維持・向上等」の対策の困難度が増す。 など

5-3. 「秘密情報の保護ハンドブック」 新たに充実させた内容

X. 秘密情報の管理を実効的なものとするための社内体制の構築

経営層の関与

経営層が関与して秘密情報の管理のリーダーシップを取るとともに、その実施状況をフォローアップ。(例:全社員での実施状況確認、部署横断的な会議体の設置)

各部門の役割分担

各部門の役割分担を決定する際の参考となる例を提示。

5-3. 「秘密情報の保護ハンドブック」 新たに充実させた内容

Y. 他社の情報も保護 (訴えられないために)

紛争を未然に防止するとともに、意図せずに争いに巻き込まれてしまった場合への備えを紹介。こうした取組は、 他社からの信頼向上、多様な人材の獲得にもつながる。

自社情報の独自性の立証

他社から秘密情報の侵害を理由に訴訟を提起された場合には、それが自社の独自情報であることを客観的に立証できるよう、日頃から備えておくことが重要。

(例:経緯書類の保存)

他社の秘密情報の侵害の防止

(1)転職者の受入れ

(例:転職者の前職での契約関係確認)

(3)取引の中での秘密情報の授受

(例:サンプル等の受領時の書面確認)

(2)共同·受託研究開発

(例:他社の秘密情報の分離保管)

(4)秘密情報の売込み

(例:情報の出所の誓約書での確認)

営業秘密侵害品に係る紛争の未然防止

疑わしい状況が生じている場合に相当の注意を払ったということが証明できる程度の対策が必要。

5-3. 「秘密情報の保護ハンドブック」 新たに充実させた内容

Z. もしも情報漏えいが発生したら

- 情報管理を徹底しても、情報漏えいを完全に防ぐことは困難。
- 万が一情報漏えいが発生した場合に迅速に対応できるよう、その手順を紹介。

兆候の把握及びその確認

- (1)漏えいにつながる兆候の把握
- (2)漏えいの疑いの確認

初動対応

- (1) 社内調査・状況の正確な把握・原因究明
- (2)被害の検証
- (3)初動対応の観点
- (4)対策チームの設置等

責任追及

(1) 刑事的措置 (2)民事的措置 (3)社内処分





証拠の保全・収集

6. 実際にあった?!事例と対策とそのポイント ケース1. 部品メーカーA社の例 [取引先向けの対策] 取引先から金型図面の提供を求められたが・・・

- A社が、精密機械メーカーB社に供給する部品a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。
- ある日、B社から部品aの金型の図面を求められ、大口の取引先だからと泣く泣く提供した。
- その後、B社から部品αの発注が来なくなってしまった。どうやらB社がA社の部品αの金型図面を、A社の競合他社であるC社に渡し、安価で部品αをコピーした部品を製造させているようだ。
 A社はどのような対策を講じておくべきだったのだろうか。

A社の秘密情報 : 部品aの金型図面



ケース1. 部品メーカーA社の例【解説】

ポイント1 開示する情報は必要最低限にしましょう。

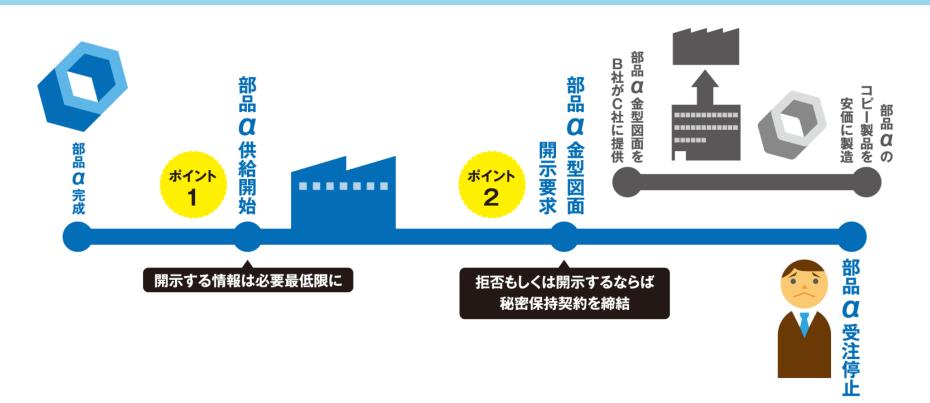
(接近の制御)【ハンドブック第3章3-4(3)①a】

- B社との取引で、金型図面の情報を開示する必要がなければ、開示を拒否することも大切です。
- 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書いておくことも効果的です。

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。

(秘密情報の認識向上) (持出し困難化) 【ハンドブック第3章3-4(3)④a、②a】

● 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よいでしょう。



6. 実際にあった?!事例と対策とそのポイント ケース2. 食品メーカーD社の例 [従業員・退職者向けの対策]従業員から退職の申出があったのだが・・・

- 即席めんを製造しているD社では、スープの配合レシピの情報が競争力の源泉である。
- 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」との報道を見たが、他人事ではない。最近、D社でも、スープ開発リーダーから、退職したいとの申出があった。転職先は競合他社の E 社だという。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、どのような対策を講じたら良いか。

D社の秘密情報 : スープの配合レシピ



ケース2. 食品メーカーD社の例 【解説】

退職に伴う漏えいリスクを低減する対策を講じましょう。

ポイント1

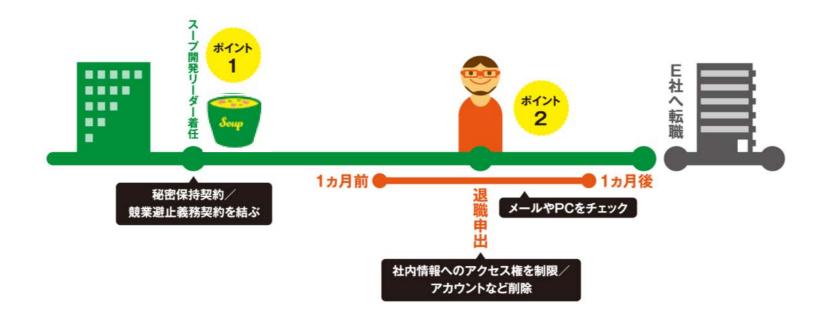
● 退職時だけでなく、入社時はもちろん、プロジェクト開始時にも秘密保持契約を締結。キーパーソンの場合は、競業避止義務契約を締結することも考えられます。(秘密情報に対する認識向上)【ハンドブック第3章3-4(2)④a、b】

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 I D・アカウントを削除(I Dカード、入館 証も回収)(接近の制御)【ハンドブック第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(視認性の確保)【ハンドブック第3章3-4(2)③g、r】
- 退職後もOB会の開催などで本人の近況を調査したり、転職先の商品情報をチェック

ポイント3

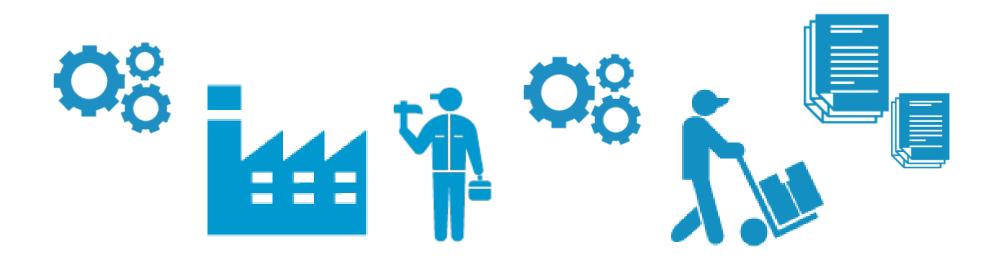
● 働きやすい職場環境や公平な人事評価制度を整備し、従業員の企業への愛着を高めておけば、貴重な人材を失わずに済み、漏えいリスクも低減します。(信頼性の維持・向上等)【第3章3-4(1)⑤】



6. 実際にあった?!事例と対策とそのポイント ケース3. フィルムメーカーJ社の例 【従業員向けの対策】 製造ラインを新設したいのだが・・・

- 1 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る。
- その新製造ラインでは、設備の改良や配置の工夫によって、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。そのため、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なければならない。対策として、どういったことができるだろうか。

J社の秘密情報 : 耐熱性フィルムの製造工程や工場レイアウト



ケース3. フィルムメーカーJ社の例【解説】

秘密情報の全体を把握できる人数を制限しましょう。

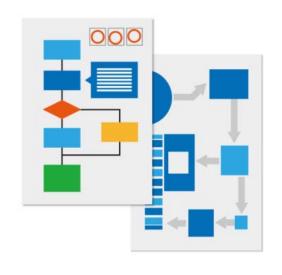
(接近の制御)【ハンドブック第3章3-4(1)①a】

● 工場の作業ライン等について、作業の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します。

情報に接する従業員が情報を持ち出しにくい対策を講じましょう。

(持出し困難化) 【ハンドブック第3章3-4(1)②j】

● 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、私物持込みは透明 バッグに入れて入室するなどの工夫をすると効果的。)







6. 実際にあった?!事例と対策とそのポイント ケース4. 繊維メーカーK社の例 【外部者向けの対策】不審なメールが届いたが・・・

- K社は素材を仕入れて高機能繊維を製造し、顧客に販売する企業である。
- ある日、製造部門の従業員 L あてに、顧客を装ったメールが届いた。従業員 L がメール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った。
- 今回は運良く従業員が不審に感じてファイルを開かなかったが、今後、このような攻撃を受けて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、調達先から開示されている情報まで外部へ漏えいしてしまう恐れがある。
- 不正アクセスや、攻撃型メールの被害にあわないためにはどのような対策をしておけばよいか。

K社の秘密情報: K社情報(高機能繊維製造ノウハウ、顧客情報など)

調達先から開示された素材情報



ケース4. 繊維メーカーK社の例【解説】

ポイント1 できる限り外部への接続を切断しましょう。

(接近の制御)【第3章3-4(4)①e】

● 可能な限り外部ネットワークにつながない機器に秘密情報を保存しましょう。

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する対策を講じましょう。

(接近の制御)【第3章3-4(4)①f】

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、 ファイアーウォール、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。

(持出し困難化)【第3章3-4(4)②c】

秘密情報の電子データを暗号化することも効果的です。

※標的型メールの見分けるためのポイント等については、 ハンドブック89頁の「コラム③ 標的型攻撃メールって どんなもの?」に掲載しています。



6. 実際にあった?!事例と対策とそのポイント ケース5. 食品メーカーF社の例 [トラブルに巻き込まれないための対策]自社技術で作ったのに・・・

- 野菜のフリーズドライにより具だくさんの味噌汁を製造するF社では、日本の果物を使ったドライフルーツを新商品として開発中。
- ある日、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た。しかしコスト面で折り合わず、G社の申出は断ることに。
- その後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。すると突然、新商品βが G社の技術を用いて製造されたものであり、その製造・販売中止を求める警告状が送られてきた。
- しかし F 社は、共同開発の打診を受けた際には、具体的な G 社技術の開示は受けておらず、G 社の秘密情報など使った覚えは一切ない。F 社が、商品βは独自技術で開発したという潔白を示すには、どうしたらいいのだろうか。

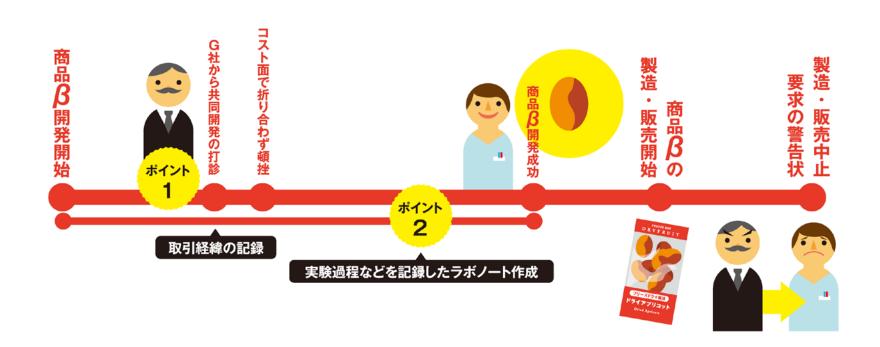


ケース5. 食品メーカーF社の例【解説】

ポイント1 他社の秘密情報は、できる限り受け取らないようにしましょう。

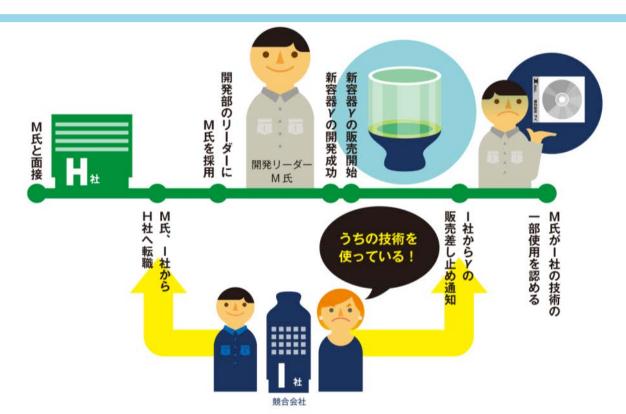
ポイント2 独自技術を証明できるように開発の内容や日時等を記録しておきましょう。 【第5章5-1】

- 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の作成・保存
- 日付確定のための公正証書(公証人が作成する公文書)等の利用
- その他関連資料の保管(電子メール、検討文書、議事録等)
- 顧客名簿であれば、顧客になるに至った経緯の記録(来店・購入の履歴、会員加入時のWeb、申込書等)
- 取引情報であれば、その取引経緯の記録(仕入や販売の際の価格や数量等が記載された伝票の原本等



6. 実際にあった?!事例と対策とそのポイント ケース6. 容器メーカーH社の例 [転職者向けの対策]転職者を受け入れて新製品を開発したら・・・

- 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氏を迎えた。
- 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の開発に成功し、販売を開始した。
- しかし、γを販売してから数か月後に、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、販売を差し止めてほしい」との通知を受けた。これを受けてH社がM氏に確認したところ、I社の技術の一部を用いてγを開発したことを認めた。
- H社としては、M氏の採用にあたり、どのような対応をすべきだったのだろうか。



ケース 6. 容器メーカーH社の例【解説】

ポイント1 転職者の負っている義務をきちんと確認しましょう。

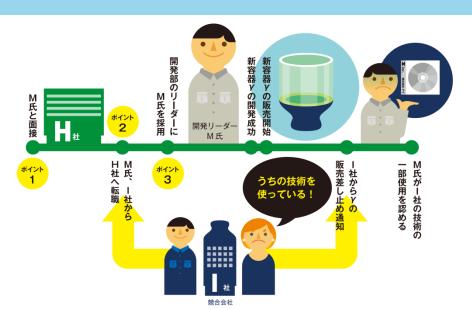
● 採用時の面接を通じて、転職者が転職元との関係で負っている秘密保持義務、競業避止義務といった義務の有無やその内容を確認しましょう。その際、議事録等を記録・保存しておくと効果的です。

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ないよう確認しましょう。

- 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、例えば以下のとおり。
 - 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
 - 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しましょう。

- 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。
- 「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。



自社ノウハウは財産。他社の情報の管理も徹底し取引先からの信頼も向上

概要

高精度設備とIT化による最先端プレス技術で、金属の難加工形状品や微細加工品を提供。20年以上前に、取引先に、金型を作るノウハウである「工程サンプル」の提示を求められ、泣く泣く渡したところ、取引が打ち切られた経験(取引先はアジアの金型メーカーに情報を渡し、安く作らせたと推測)を踏まえ、自社・他社の情報の管理の徹底を図り、取引先に対しても、その方針を示した。こうした取組により、取引先から信頼され、事業にも好影響が出ている。

- ○「接近の制御」に資する対策【 C. ① 】
 - 工場の入口は内部からのみ解錠可能な扉
 - 取引先の部品・金型も、第三者に特別に入室を許可する場合、当事者以外の部品等は目に触れないよう、覆いを掛けて目隠し管理 (他社の情報もしつかり管理)
 - 図面等の重要データはインターネットに繋がっていない P Cで管理
 - 「自社の**ノウハウ**(図面・工程サンプル)は、財産であり、提供しない」と取引先との契約書に明記
- ○「視認性の確保」に資する対策【 C. ③ 】
 - 金型やプレス機のある現場には「立入禁止」、 「撮影禁止」等の掲示

- ・自社と同レベルで 取引先の情報管 理を行うことで取 引先からの信頼が 向上
- ・業績にも好影響



企業における秘密情報の管理の事例② しのはらプレスサービス株式会社

(プレス機械のメンテナンスサービス) 千葉県船橋市

ノウハウの見える化・ビッグデータの集積で知識集約型企業へ

概要

修理前よりも能率が向上すると評判の企業。社長自らが経営理念として「知識集約型」を掲げる。各工場を訪問し散在するプレス機械のカタログ・図面データを、点検時に経年劣化した機械の現状データを、修理時に作業データを収集・蓄積。このデータを活用し、唯一無二のサービスを実現。また、社員の現場での工夫を作業マニュアル化し、社内で共有。その際、工夫を発案した社員の名前を明記・登録し、「自分も会社の知的財産を作り出している」と従業員に当事者意識が芽生え、やる気も向上。

具体策

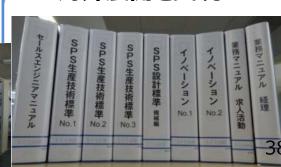
- ○保有する情報の洗い出し【 A 】
 - 市場製品のカタログデータ(4000機種以上)を収集・利用し、 経年劣化した機械の現状データ・修理ノウハウを独自に文章化し て、

知的資産として共有

- ○信頼関係の維持·向上等【 C. ⑤ 】
 - 経営者自らが「社員の知恵が我が社の財産」と内外に発信

- 作業ノウハウを文章化する際、アイデアを提案した **社員名を明記・登録**

- ・従業員のやる気、当事者意識向上
- ・同業他社への転職 者無し
- ·顧客満足、信頼向上
- ・メンテサービスの 海外展開を実現



厳格な情報管理と作業の見える化で顧客の信頼向上、高付加価値サービスを実現

概要

蓄積した製品・作業のデータを活用し、通常では繊維を傷めるため**水洗浄ができず水溶性の汚れを落とせない衣** 類の**水洗浄を可能とする技術**(特許技術とノウハウで管理)を生み出した。この技術と、データベースによる<u>徹底し</u> た顧客管理・接客で、顧客ニーズに対応した世界唯一のケアメンテというクリーニングとは異なるサービスを実現。

- |○保有する情報の洗い出し【 A 】
 - 取り扱った**衣類の素材、ブランド、洗浄方法**を全てデータ化
- ○「接近の制御」に資する対策【 C. ① 】
 - 従業員ごとにアクセスできるデータを管理・制限
 - **従業員ごとに毎日更新**されるパスワードを付与
 - 作業で使用する**溶剤の性質等は従業員にも非開示**
- ○「持出し困難化」に資する対策【 C. ② 】
 - 作業場への携帯電話の持込み禁止
- ○「視認性の確保」に資する対策【 C. ③ 】
 - 全ての作業工程をカメラで撮影・録画
- ○信頼関係の維持·向上等【 C. ⑤ 】
 - 作業スキルを見える化。技能認定&昇給でやる気向上

- ・顧客の信頼向上
- ・高価格でも、満足度の 高いサービスを提供
- ・従業員のやる気向上
- ・作業の録画を、クレーム 対応(従業員保護)、従 業員自身でのスキル チェックに活用



厳格な情報管理によりグローバルな生産体制を実現し、世界シェアトップ

概要

1993年に、明るさや残光時間において従来の蓄光顔料の約10倍の輝度を有しながら、放射性物質を全く含まない蓄光顔料(製品名:「ルミノーバ」)を世界に先駆けて開発し、**各国で物質特許を取得**。以来、同製品は、夜光時計の針や文字盤、避難誘導標識、安全標識など幅広く活用されている。社長自らが知財の重要性を謳い、**社長の直下の法務・知財室が中心となり知財戦略を立案**。ルミノーバは特許期間の満了を迎えたが、**商標の登録、技術ノウハウの秘匿化などに戦略的に取り組み**、高い競争力を維持。

コア技術である製法や原材料情報は秘密情報として管理。海外の生産工場には調合済の原料を供給し、製法・原材料情報は社内であってもブラックボックスにして明らかにしないなど、生産現場での徹底した情報管理により、 グローバルな生産体制を実現し、世界シェアトップを実現。

- ○「接近の制御」に資する対策【 C. ① 】
 - 海外の生産工場には**調合済の原料を供給し、** 製法や原材料情報は社内であっても開示しない
 - 取引先・共同研究開発相手にも製法や原材料情報は開示しない
 - 社内で秘密情報を取り扱うエリア・取扱い者を限定
 - 電子データについては、社内においてもアクセス制限
- ○「視認性の確保」に資する対策【 C. ③ 】
 - 秘密情報が含まれる電子情報は**タイムスタンプで管理**し、 不正なアクセスや複製を検知
- ○「信頼関係の維持向上等」に資する対策【 C. ⑤ 】
 - ノウハウの発案に対しても特許取得と同様に社内報奨

- ・グローバルで効率的な生産体制を実現
- ・世界シェアトップを実現
- ・従業員のやる気向上









(製品設計・試作品製作)愛知県みよし市

チームでの話合いにより発想力と意識を高め、他社情報も徹底的に管理

概要

従業員の自由な発想力と、チーム力を育む職場環境とで、自動車メーカー等の様々なニーズに的確に対応した高品質の部品設計を生み出す。**部品設計のために顧客から提示される設計仕様、新車開発スケジュール等の秘密情報を、社内で厳格に管理。各部署のメンバーで構成される「機密管理実行委員会」**の下、漏えい対策を統一的に進める。加えて、全社朝礼において従業員自らが経験した**ヒヤリハット事例を共有**したり、従業員同士が**定期的にアイディア**

を出し合って漏えい対策を提案・検討する仕組みを設けたりするなど、従業員の発想力とチーム力とを活用し、きめ細かけい情報管理体制を構築するとともに、意識の向上を実現している。こうした取組により、**顧客からの信頼を獲得**している。

旦体策

○「接近の制御」に資する対策【 C. ① 】

- 設計に関する情報は、**限定されたプロジェクトメンバーのみがアクセス**
- 秘密情報が記録された**書類は従業員が立ち会い、専門業者が焼却処分**
- 顧客との電子データのやりとりは、**専用回線**を使用
- ○「持出困難化」に資する対策【 C. ② 】
 - 社内でのカメラ付き携帯の持込みを禁止
 - 電子メールは、<u>秘密情報の送信時は暗号化</u>。全ての電子メールの文中に 情報取扱いに関するチェック項目を記載し、送信時に確認
- ○「視認性の確保」に資する対策【 C. ③ 】
 - 秘密情報を取り扱うエリアの出入口に**監視カメラを設け**入退管理
- ○「秘密情報に対する認識向上」に資する対策 C. ④ 】
 - 全社朝礼で、毎日、**情報管理対策の6項目を唱和**
 - 従業員が自らの<u>ヒヤリハットの実経験を紹介・共有</u>。従業員同士がチームに分かれ 情報漏えい対策のアイディアコンテストを実施するなど、<mark>従業員の意識を高めている</mark>

・顧客の情報を徹底 的に管理し、取引先 の信頼を獲得



機密唱和(6項目)

- ・メール本文下にチェックシートを添付します。 「添付資料有無」「暗号化しパスワード設定 有無」「車名併記無」「転送・引用文有無」
- 新規受入れ者の指導を必ず行います。
- ・違反が発覚したら即時に上司に報告します。
- ・カメラ付き携帯電話は持ち込みません。
- ・機密書類は持ち出しません。

・お客様の入退室記入を必ず行います。

企業における秘密情報の管理の事例⑥ 株式会社北海道バイオインダストリー

(食品研究開発・販売)北海道札幌市

技術情報の管理手法を使い分け、高付加価値の食品を開発

概要

北海道産の農産物だけを用いて、健康改善作用と美味しさを兼ね備えた食品("**コンディショニング食品**")として 北海道食品機能性表示制度に基づく認定を受ける商品や、中小企業庁長官奨励賞(平成26年度)を受賞 した商品等を開発・製造する。

戦略的に管理手法を使い分けることにより、協力・連携の拡大と、独自技術の保護・他社との差別化を実現。例えば玉ねぎの加工に関して、加熱処理方法と加工生成物質については、特許を取得している。加工委託先への生産工程の条件設定等については、営業秘密(技術ノウハウ)として秘密保持契約を結び情報を提供。また、設定条件の生成方法は社内でも限定した社員のみしか知らない。

一方で、ヤーコン(北海道産の根菜)については、**地域活性化や生産者の収益増に向け、認知度の向上や食材の用途拡大を図る**べく、**自社の技術を無償公開**。

- ○秘密とする情報の決定【B】
- 技術の重要性・性質等に応じ、①特許出願、
 - ②社内でもアクセス権を制限、③秘密保持契約を締結した上で 他社に提供等の**管理手法を決定**
- ○接近の制御【 C. ① 】
- ノウハウの重要な部分は社内でもアクセス限定(電子情報を 外づけハードディスクだけに保存し、当該ディスクは限定された 社員しか知らない場所に保管)

- ・管理手法の使い分けにより、 協力・連係の拡大、独自技 術保護・他社との差別化を実 現
- ・技術の無償提供で、地元の 経済活性化、農業生産者の 収益増を目指す



企業における秘密情報の管理の事例での株式会社ガイア環境技術研究所

(炭化加工機等の開発・製造)宮城県仙台市

知財を活用したブランディングにより資源循環型社会の構築に貢献

概要

"地球が喜ぶテクノロジー"という企業理念の下、炭づくりの匠の技を参考に、もみ殻、食品加工残渣といった廃材から高品質な炭を連続的に生み出す技術を開発。炭化処理の方法や炭化機基本構造については特許を取得する一方、装置自体は処理する廃材の種類や装置の設置現場の状況に応じた個別の設計が必要となることから、炭化機内の構造や配管を含む最適設計技術はノウハウとして秘密管理。

また、炭化機から生み出される炭(油吸着材、調湿材など)自体でも、特許権と商標権を取得し、炭化機ユーザーに対し「SUMIX」の<u>商標と品質評価結果の結果などをライセンス提供</u>することにより、互いにWin-Winの関係での炭の品質確保とブランド構築がなされ、高品質な炭の市場を開拓。

- ○「接近の制御」に資する対策【 C. ① 】
 - 最適設計のノウハウは社長のみが管理
 - 秘密情報が記載された**紙媒体は施錠管理**
 - 秘密情報は、メールでのやりとりを禁止
- ○「秘密情報に対する認識向上」に資する対策【 C. ③ 】
 - 秘密情報にはマル秘マークを表示
 - 入社時と退職時に秘密保持を契約
 - 装置の納入先や製造委託先とも秘密保持を契約

- ・コア技術の秘匿化により技術的優位性確保
- ・知財を活用しユーザーと共に高品質市 場を構築
- ・知財を活用したブランディングにより資 源循環型社会の構築に貢献





オープン・クローズ戦略の実践により、長期にわたり製品の競争力を確保

概要

配線用遮断器などのいわゆる"ブレーカー"を開発・製造するメーカーで、地元ではブレーカーが社名の「テンパール」の通称で呼ばれるほど親しまれている会社。1951年の創業当時から「会社の宝は技能と技術」とうたい、製品技術の特許を多数取得し、技術を知財で守ることをいち早く実践。1965年には、その当時10個の特許権を保有、特許は真珠のように大切なものとの思いから、10(テン)の真珠(パール)として、社名を変更した。

現在では、インフラを支える機器であり同型の製品が長く販売されるという特性にあわせて、<u>リバース・エンジニアリン</u>グによって判明する技術は特許化する一方で、分からない技術については、ノウハウとして秘密管理を行いグループ企業であっても情報共有も最低限とするなど、オープン・クローズ戦略を実践し、技術流出に細心の注意を払っている。

具体策

- ○「秘密とする情報の決定」に資する対策【 B 】
 - 製品寿命が長いため、代々の担当者間の情報の継承が確実に行えるよう、製品ごとに関連情報を一元化して保管
- ○「接近の制御」に資する対策【 C. ① 】
 - 開発データは厳格なアクセス制限 (開発部へ立入禁止)
- ○「秘密情報に対する認識向上」に資する対策【 C. ④ 】
 - グループ企業への情報共有であっても、製造に必要な最低限の情報の みを提供。 開示した情報については取引基本契約のなかで秘密保持 を規定

・特許と営業秘密と を組み合わせること により、長期にわた る競争力の維持を 実現





顧客から信頼される情報管理体制を構築し売上げを伸ばす

概要

経営層も含め社員全員が、情報管理の重要性や情報漏えいの損害を十分に認識し、リスクを徹底的に排除しながら、顧客の信頼を獲得し、成長を遂げてきたモバイルコンテンツの開発・配信会社。2008年に情報セキュリティマネジメントシステム国際標準規格(ISMS)の認証を取得し、顧客から要求されるセキュリティレベルへの迅速な対応が可能に。

また、社内の**情報管理ルールを分かりやすくまとめた簡易マニュアルを作成**。その中で、報道された<u>他社の漏えい事案を示し</u>、最悪のケースでは、**経営陣の引責辞任、数百億円規模の損害賠償、顧客喪失などにつながることを紹介**し、それを研修や社内テストにおいても確認し、社員全員が情報管理の認識を高めている。また、横断的な情報セキュリティー確保の体制や社外による監査体制などが構築されていることも、信頼を高め顧客の獲得につながっ、ている。

具体策

- ○継続的かつ適切に実施するための社内体制の構築【 X 】
 - 横断的な部署が参加する「情報セキュリティ委員会」の設置
 - **外部**コンサル**が参画**する「**監査委員会**」の設置
 - -情報管理ルールの「**簡易マニュアル**」の作成
- ○「秘密情報に対する認識向上」に資する対策【 C. ④ 】
 - 進行段階に応じ事業範囲に応じた情報の取扱いを規定
 - -情報管理の理解を確認するチェックテストや **社内チームディスカッションを実施**
 - 業務開始・終了時に自社・共同開発先の従業員 との秘密保持を契約
 - 退職時に競業避止義務を契約



概式会社メディア・マグック ISMSマニュアル 簡易版





キュリティ要求にも 迅速に対応し、売 上げ 1.5 倍増 設問】会社で管理している個人

ISMS認証の取得

により顧客からのセ

【設問】会社で管理している個人情報が外部へ流出してしまった場合、どのような問題が発生すると考えられるでしょうか。想定されるリスクを具体的に3つ以上記載してください。

【回答例】

- ・クライアントや社会的な信用の失墜
- •取引停止、売上減少
- ・多額の損害賠償費用の発生

企業における秘密情報の管理の事例⑩

三浦工業株式会社

(小型貫流ボイラ製造・販売・メンテナンス事業)愛媛県松山市

生産性向上のためのデジタル化により、サービスの質の向上・情報管理の強化を実現

・小型貫流ボイラに搭載したセンサで、顧客のボイラの<u>運転状況をリアルタイムでモニタリング</u>を行うことで、単に製品、 の販売を行うだけではなく、<u>故障の予兆を検知し工場の稼働を停止することなく修理</u>を行ったり、複数台のボイラの 最適な運転管理による燃料消費の削減の提案などの顧客のニーズに応える付加価値の高いサービスも併せて提 供することで、小型ボイラーの国内シェア6割以上を獲得。

また、自社のボイラの納入・稼働の**台数が拡大しつつ**も、**サービスの質を維持・向上**させるため、顧客へのメンテナンスサービスや省エネの提案に必要な情報の最新版が客先からでも常に見られるように、客先からでも直接専門の技術社員と相談するために全社員の所属・連絡先の検索を可能とするように、情報・ノウハウの見える化・デジタル化を進めるとともに、タブレット等の情報端末を全サービススタッフに装備させた。こうした取組みにより、営業力の強

化、一人あたりの**生産性の大幅向上**を実現している。

具体策

- |○「接近の制御」に資する対策【 C. ① 】
 - 業種や役職に応じた<u>アクセス権を設定</u>。顧客情報は担当<u>エリア</u> 内では共有しつつ、エリア外の情報についてはアクセス制限
 - -情報へのアクセスは、**ログをとり、その旨を社員へ周知**
- ○「持ち出し困難化」に資する対策【 C. ② 】
 - 会議資料は全て<u>情報端末で閲覧</u>、<u>印刷不可</u>。<u>情報端末</u>の<u>紛失対</u> 策とし、一定時間が経過すると<u>自動的にアクセスを遮断</u>
- ○「秘密情報の認識向上」に資する対策【 C. ④ 】
 - 社員が発案・作成した法令ハンドブック「法令の"ほ"」を頒布
- ○「社員のやる気向上」に資する対策【 C. ⑤ 】
 - <u>年2回</u>、<u>全国のメンテナンススタッフ</u>を愛媛県の本社で<u>研修</u>。 スキル向上により、**生産性向上&給与UP**を図っている

顧客のニーズに応え、現場の生産性の向上を図るために、情報のデジタル化を進めた結果、サービスの質の向上・情報管理の強化が実現され、業界シェア6割を獲得



ご静聴ありがとうございました。

経済産業省HPでは、

「逐条解説 不正競争防止法~平成27年改正版~」、「営業秘密管理指針」、「秘密情報の保護ハンドブック」、平成27年改正概要資料など、

不正競争防止法に関するさまざまな資料を掲載しております。



不正競争防止法 知的財産政策室

http://www.meti.go.jp/policy/economy/chizai/chiteki/















http://www.meti.go.jp/policy/econo my/chizai/chiteki/pdf/hbtebiki.pdf

不正競争防止法に関するご質問はこちらまで

経済産業省 経済産業政策局 知的財産政策室

〒100-8901 東京都千代田区霞が関1丁目3番1号

TEL: 03-3501-3752

E – m a i l : chitekizaisan@meti.go.jp