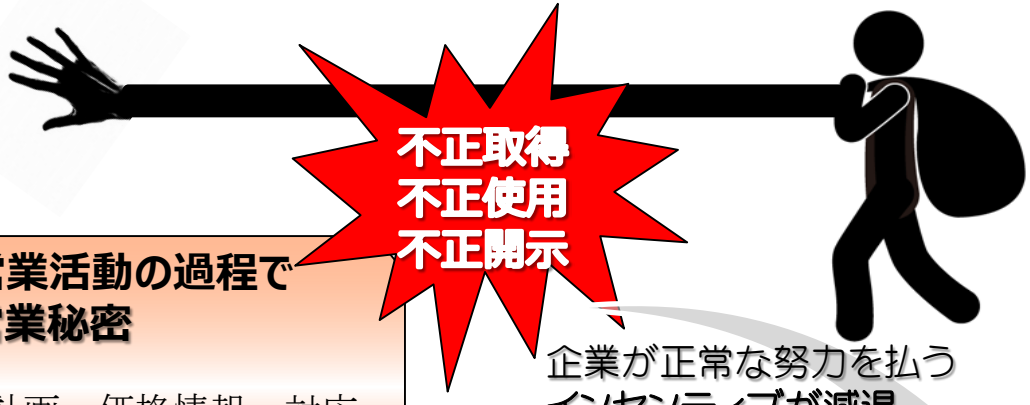
5．不正競争行為類型の概要（4）

④営業秘密の侵害
（第２条第１項第４号～第１０号
・第21条第1項、第3項）

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）

企業が正常な努力を払う**インセンティブが減退**

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(民事)

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。（知財高判平24.7.4）

事例(民事)

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。（知財高判平23.9.27）

事例(刑事)

通信教育業を営む会社でシステム開発に従事する者（派遣労働者）が、約3000万件の顧客データを私物スマートフォン等に複製して持ち出し、このうち約1000万件のデータをインターネット上にアップロードして名簿会社等に開示した事案。懲役2年6月、罰金300万円が言い渡された。
（ベネッセ事件控訴審判決―東京高判平29.3.21）

事例(刑事)

フラッシュメモリの共同開発に携わっていた東芝連携企業従業員の技術者が、東芝のデータベースからフラッシュメモリ開発にかかる営業秘密データを記録媒体に複製して持ち出し、韓国企業に開示した事案。懲役5年、罰金300万円の実刑が科された。
（東芝フラッシュメモリ事件ー東京高判平27.9.4）

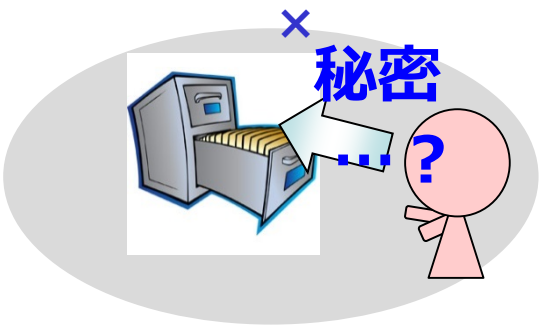
「営業秘密」として法律による保護を受けるための３つの要件

不正競争防止法第２条第６項

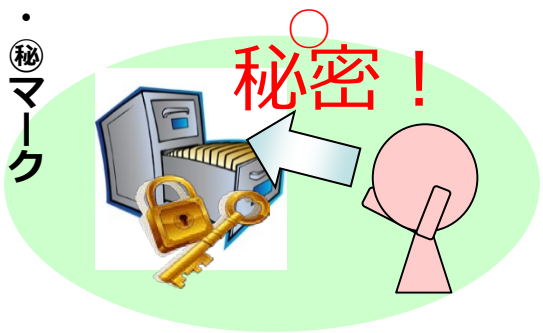
この法律において「営業秘密」とは、**①秘密として管理されている**生産方法、販売方法その他の**②事業活動に有用な技術上又は営業上の情報**であって、**③公然と知られていないもの**をいう。

①秘密として管理されていること（秘密管理性）

その情報に合法的かつ現実に接触することができる従業員等からみて、その情報が会社にとって秘密としたい情報であることが分かる程度に、アクセス制限やマル秘表示といった秘密管理措置がなされていること。（「営業秘密管理指針」（次項参照））



・㊙マーク
・施錠管理　など



② 有用な営業上又は技術上の情報であること（有用性）

脱税情報や有害物質の垂れ流し情報などの公序良俗に反する内容の情報を、法律上の保護の範囲から除外することに主眼を置いた要件であり、それ以外の情報であれば有用性が認められることが多い。現実に利用されていなくても良く、失敗した実験データというようなネガティブ・インフォメーションにも有用性が認められ得る。

③公然と知られていないこと（非公知性）

合理的な努力の範囲内で入手可能な刊行物には記載されていないなど、保有者の管理下以外では一般に入手できないこと。公知情報の組合せであっても、その組合せの容易性やコストに鑑み非公知性が認められ得る。

（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）

営業秘密管理指針全部改訂：法解釈への特化

（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！

○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平成27年1月に全部改訂。

（旧指針）

漏えい防止レベル → 秘密情報の保護ハンドブック

法的保護レベル → 営業秘密管理指針

漏えい防止レベルの対策については、65～71頁参照

＜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。

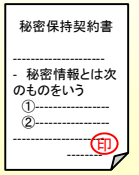
⇒情報に接することができる従業員等にとって、

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㊙」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。