経済産業省

【公表予定】

資料１３

最新の営業秘密侵害事例から見えてくる「営業秘密」保護のポイント

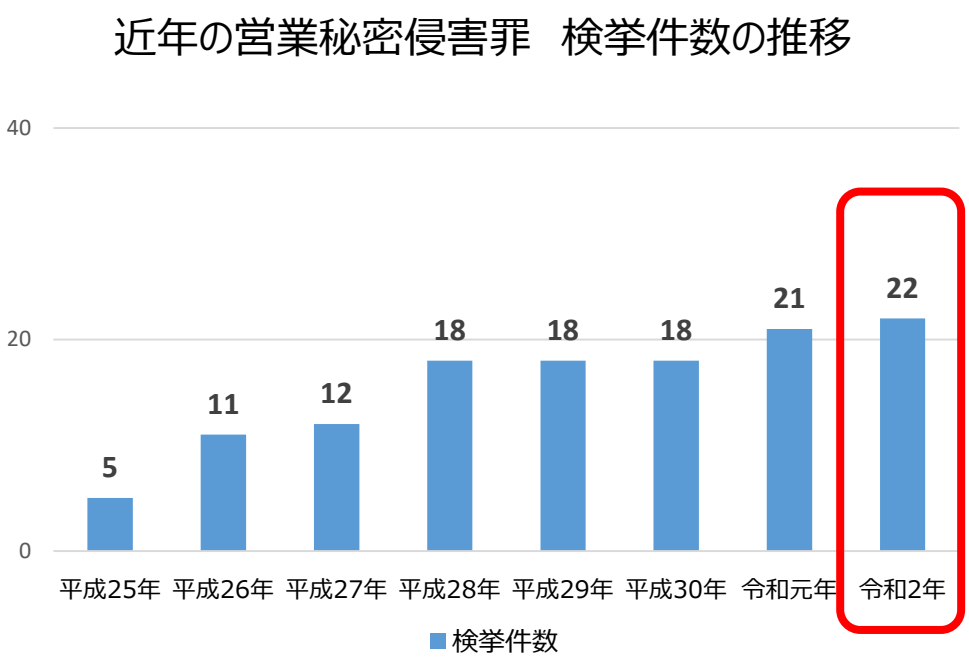
～「営業秘密」を保護するために企業はどのような対策が必要か～

経済産業省知的財産政策室

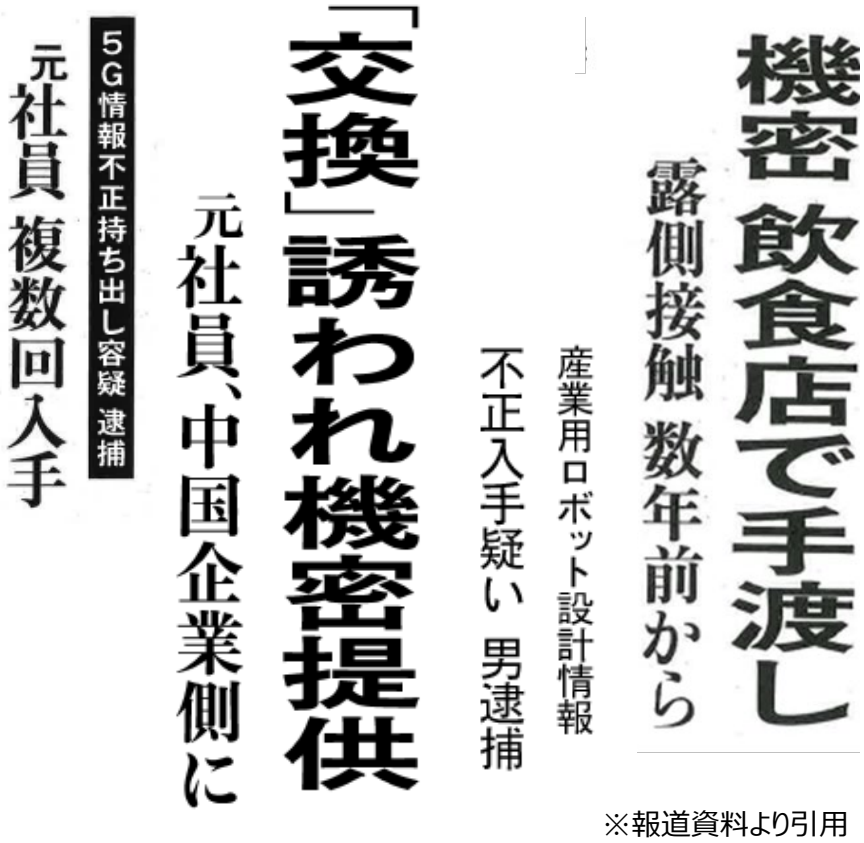
令和３年６月２日

はじめに・・・

- 企業における秘密情報の漏えい対策は着実に進展していると考えられるものの、依然として従業員・退職者による競業会社への持ち出し、海外への流出が散見される。
- こういった状況を受け、継続する典型事案に対する課題・対策について情報共有を行い、秘密情報保護の実効性を高める機会としたい。



※「令和２年における生活経済事犯の検挙状況等について」に基づき作成

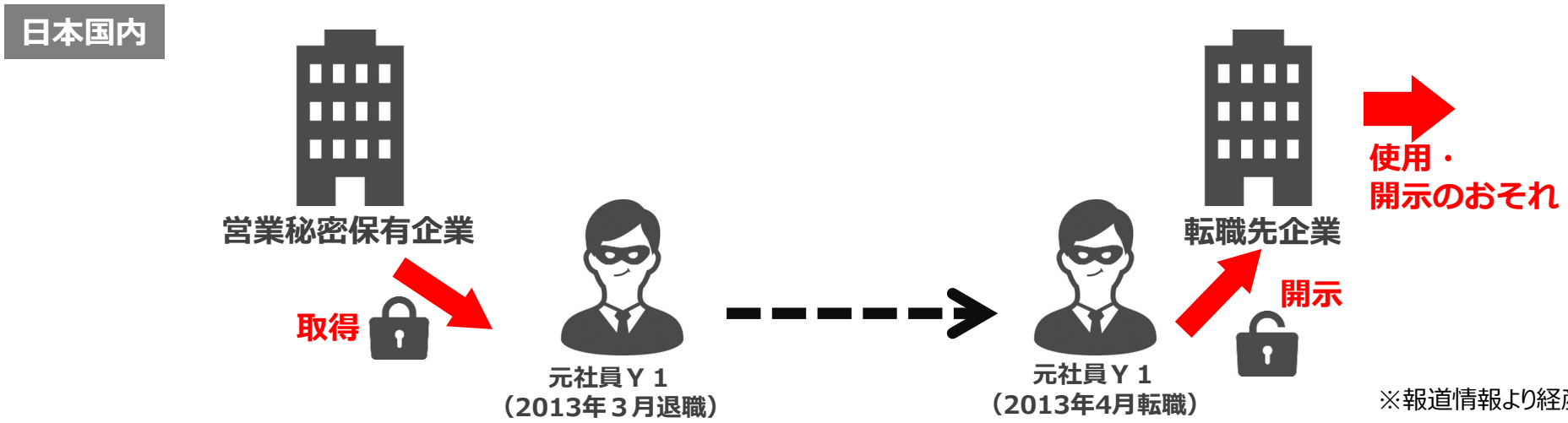


※報道資料より引用

事例①：従業員等による競業会社への持ち出しケース

日本ペイント（大阪府）（刑事）

- 塗装大手である日本ペイントの元役員が、同社の主力商品の営業秘密（建築用塗料「水性ケンエース」の設計情報）を複製し、ＵＳＢメモリーに保存して持ち出したとして、不正競争防止法違反（営業秘密の開示）の疑いで逮捕（2016年2月17日）。
- 元役員は日本ペイント執行役員を経て、2010年4月～2013年3月、子会社に出向。子会社を退職後の2013年4月、菊水化学工業の顧問に就任した。
- 元役員に対し、懲役2年6月（執行猶予3年）、罰金120万円の判決（2020年3月27日名古屋地裁）。



※報道情報より経産省作成

内部不正による漏えい割合は増加傾向（IPA調査：営業秘密実態調査2020より）

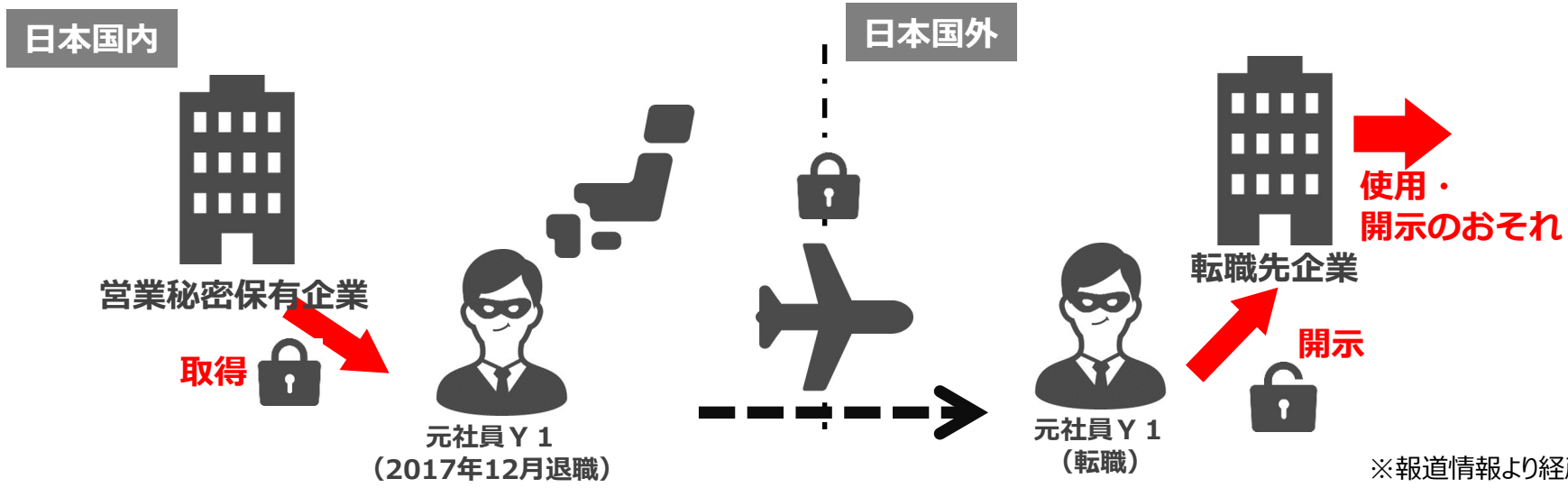
- ✓ 漏えいルートの多くが中途退職者であり（36.3%）、内部不正による漏えい割合は増加傾向
- ✓ テレワーク環境での他社との情報共有ルールやクラウドサービスでの秘密情報の扱いなどについては他の項目に比べて対策が進んでいない状況

(参考)
営業秘密実態調査2020

事例②：海外への流出（海外からの接触）ケース

NISSHA（京都府）（刑事）

- 電子部品製造大手「NISSHA」の元従業員が、関連会社の事務所で、同社の主力商品であるスマートフォンなどに使用されるタッチセンサー技術に関する情報を、自身のハードディスクに不正に複製したとして、不正競争防止法違反（営業秘密領得・海外重罰適用）の疑いで逮捕（2019年6月5日）。
- 元従業員は2017年12月、同社を退職後、中国にある競合他社で働いていた。
- 元従業員に対し、懲役2年、罰金200万円の実刑判決（2021年3月17日京都地裁）。



※報道情報より経産省作成

この他、以下のような事例もあり、<u>接触の手口は多様化・巧妙化</u>。

- ✓ 大手通信会社の元社員は在日ロシア通商代表部元職員の男と街中で出会い、当初会社パンフレットなどに記載されているような情報の公開資料を要求され、報酬として現金を受け取ったところからやりとりが始まった。
- ✓ ビジネス向けSNSで中国企業の社員が、大手化学メーカーの元社員の経歴や勤務先を見てメッセージを送信したことで、やりとりが始まった。

営業秘密の持ち出しに対する基本的な対応策（事例①・②共通）

- 従業員・退職者からの漏えいリスクを低減する対策を。
- 企業等は多様な情報を保有しており、これらを見渡した効果的・効率的な対策を。

ポイント１　（秘密情報に対する認識向上）☞保護ハンドブック 第3章 3-4（P48-50、P60）参照

- 入社時・退職時や、プロジェクト開始時等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有効。

（参考）秘密情報の保護ハンドブック

ポイント２　（接近の制御、 持出し困難化、視認性の確保）☞保護ハンドブック 第3章 3-4（P26-32、P35、P57-59）参照

- 適切に情報へのアクセス権の範囲を設定し、「知るべき者だけが知っている」という状態を実現することが重要。
- 私物の記録媒体の持ち込みを制限するとともに、秘密情報が記載された媒体等に「持ち出し禁止」等の表示を行うことも効果的。
- 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。（ＩＤカード、入館証も回収）
- 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。

ポイント３　（信頼関係の維持・向上等）☞保護ハンドブック 第3章 3-4（P53-54）参照

- 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。

従業員等による競業会社への持ち出しケース（事例①）に対する対応策

- テレワークの普及（原則化）や人材の流動化、内部不正の発生リスク等を折り込んだ重用情報保有企業による「被害防止」と、受入企業による「侵害抑止」に向けた取組の実効性をどう確保するか。

◇情報保有企業による「被害防止」に向けた取組

（参考）テレワーク時における秘密情報管理のポイント（Q&A解説）

ポイント１　（社内規程の見直し）☞テレワークQ&A　Q１、Q５、Q９参照

- テレワークへの切り替えにあたって、改めて、秘密情報の管理の態様や諸規程の整備状況を確認し、秘密情報の持出や外部クラウドの利用、オンライン会議利用等の記載について、必要に応じて見直しを図ることが重要。

テレワーク対応・内部不正対応については依然課題（IPA調査：営業秘密実態調査2020より）

- ✓ テレワークにおける情報管理ルールを定めていない企業が相当数存在（29.5%）
- ✓ 社内規定の見直しは進んでいるものの、個別の従業員・退職者からの書面徴求は低水準

◇人材受入企業による「侵害抑止」に向けた取組

ポイント２　（他社の秘密情報の持込を防ぐ）☞保護ハンドブック 第５章（P108-120）参照

- 転職者受け入れの際には、転職元との関係で負っている義務を確認。
- 転職者採用時には、転職元の秘密情報を持ち込ませないように注意喚起するとともに、誓約書の取得をしておくことも有効。
- 採用後も転職者が従事する業務内容を定期的に確認し、私物のUSBメモリ等の記録媒体の持ち込みを禁止。
- 取引の中で秘密情報の授受が発生する場合は、使用目的の制限、秘密保持の期間などについて、書面確認を実施。
- 技術情報・営業情報の売込みがあった場合、その売り込まれた情報の出所について確認し、誓約書等を取得。
- 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、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、情報の取得過程や、更新履歴、関係する資料を保管しておくことが有効。

海外への流出（海外からの接触）ケース（事例②）に対する対応策

- 接触の手口が多様化・巧妙化していることに鑑み、対策を考える上で「危険を知る」。
- その上で、社内規程の見直し、情報管理措置・体制の見直し、社員向け啓発が必要。

情報流出の契機として「不正アクセス」より「持ち出し」が課題（IPA調査：営業秘密実態調査2020より）

✓ 不正アクセス対策で「何もしてない」は激減（前回：34.0%→今回：6.1%）。
✓ 一方、不正持ち出し対策で「何もしていない」は高水準（25.4%）。

ポイント１　（秘密情報に対する認識向上）☞保護ハンドブック 第3章 3-4（P46-48）参照

- 社内規程で秘密情報の定義・取扱い方法等について規定し、適切に周知することで従業員等の秘密情報に対する認識向上を図ることが重要。必要に応じてSNS使用時における注意点を盛り込むことも有効。
- 社内研修などを通じて、最新の漏えい事例等を従業員に対して周知し注意喚起を行う。

参考：現地での営業秘密の持ち出しに対する対応策

- 企業の国際展開・国際交流に伴い、日本での管理に加え、各国の法制度、事業環境などを踏まえて、各国の状況に応じた対策を。

◇例えば、中国での対策ポイントは以下のとおり

（参考）
中国における
営業秘密管理
マニュアル

ポイント１　（物理的管理体制の整備）☞管理マニュアル P31-33、40-42参照

- 管理性要件の基準は日本と大きく変わらないため、日本と同等の管理を実施
- 日本とは比較にならないほど、携帯電話及びSNSが業務上利用されていることが多いため、携帯電話管理（写真撮影やＳＮＳ利用）の対策が必須

ポイント２　（人的管理体制の整備）☞管理マニュアル P39-40、42参照

- 人材流動性が相対的に高く、会社への帰属意識が日本と比べると高くないため、従業員の退職時の対策が重要
- 退職の申し出があった時点で、当該従業員に対する監視を強化したり、営業秘密へのアクセスを制限するなど、早めの対策が必要
- 法律的、形式的な対応にとどまらず、競業避止義務を課した退職者のその後の足取りを、調査会社を利用するなどして追跡、確認する等、現実的な対応も検討が必要