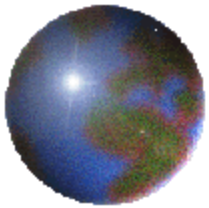
2015年10月度 関東部会



営業秘密官民フォーラムについて

2015/10/20
ベルサール八重洲

世界から期待され、世界をリードするJIPA

Introduction

- 不正競争防止法改正を受けて、第１回営業秘密官民フォーラムが開催された。
- 本フォーラムは、官民の実務者で構成され、営業秘密の漏洩に関する手口やその対応策について情報交換を行うことを目的としている。
- 今回は警察庁から最新の手口の紹介、IPAからサイバーセキュリティ対策の最新状況の紹介などがあったので、JIPA会員への情報提供として報告する。

営業秘密官民フォーラム：本年１月に開催した「技術情報等の流出防止に向けた官民戦略会議」において、企業情報の漏えいに関する最新の手口やその対応策に関して、関係府省・産業界の実務者による情報交換を緊密に行う場として創設が決定されたもの。

議事次第

- **日時**：平成27年7月7日（火）10：00～12：00
- **場所**：経済産業省本館17階西2 国際会議室
- **議題**：
  1. 技術情報等の流出防止を巡る現状と課題（経済産業省）
  2. 相談窓口活用状況（INPIT）
  3. 営業秘密侵害事犯への 対処方法等について（警察庁）
  4. 技術情報窃取の動向等（公安調査庁）
  5. サイバーセキュリティ対策（IPA）
  6. 今後の運営等について

参加者

- **産業界**：
  - 日本経済団体連合会
  - 日本商工会議所
  - 日本知的財産協会
  - 国際知的財産保護フォーラム
  - 弁護士知財ネット
  - 日本サイバー犯罪対策センター
  - 日本化学工業協会
  - 日本化学繊維協会
  - 日本機械工業連合会
  - 日本自動車工業会
  - 日本製薬工業協会
  - 日本鉄鋼連盟
  - 経営法友会
  - 電子情報技術産業協会
- **政　府**：
  - 経済産業省関係各局
  - 内閣官房知財事務局
  - 公安調査庁
  - 内閣サイバーセキュリティセンター
  - 農林水産省
  - 警察庁生活安全局・警備局
- **独　法**：
  - 工業所有権情報・研修館
  - 情報処理推進機構
  - 産業技術総合研究所

議題１

技術情報等の流出防止を巡る現状と課題

（経済産業省）

資料2

技術情報等の流出防止を巡る現状と課題

平成27年7月

経済産業省

目　次

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。**

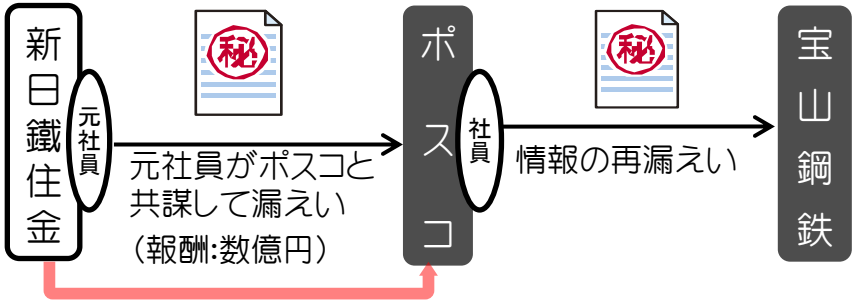
⇨ 抑止力向上と処罰範囲の整備が必要。（現行:懲役10年以下、罰金1000万円以下（法人3億円））

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、送配電ロスを大幅に軽減可能。



【現状】賠償請求・差止め請求（日本、米国、韓国で係争中）

東　芝

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。

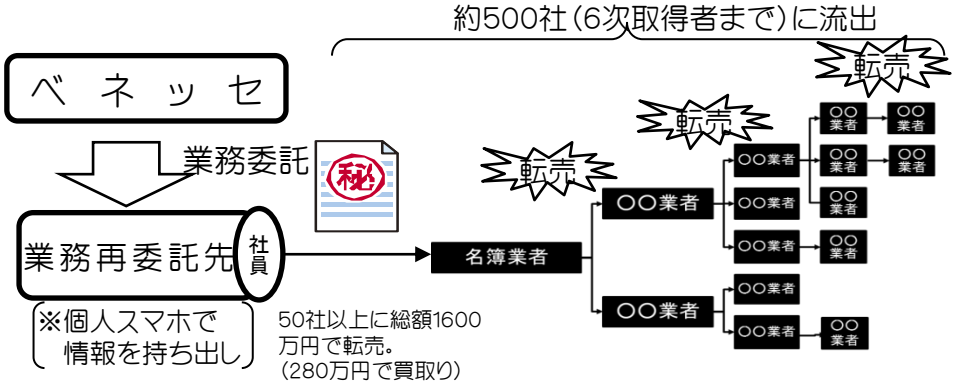
【現状】・賠償請求（約1100億円）　→　2014年12月に和解（約330億円）
・元社員の逮捕（懲役5年（実刑）、罰金300万円（2015年3月:東京地裁））

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）



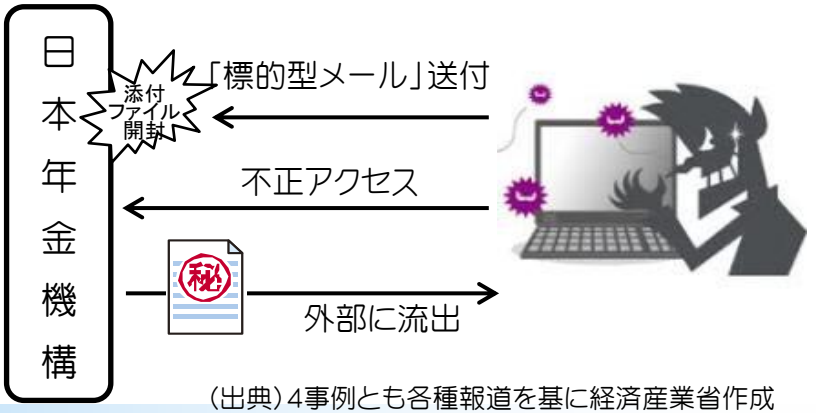
【現状】刑事事件として東京地裁にて公判中

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）

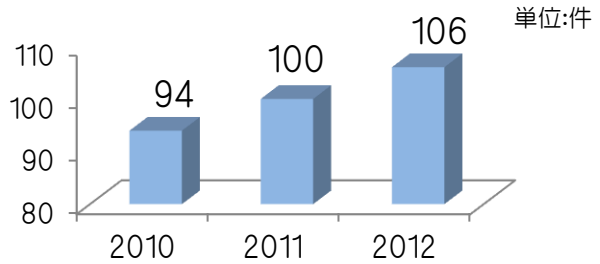


（出典）4事例とも各種報道を基に経済産業省作成

（参考）諸外国の状況

【米国】

FBIにおける営業秘密関連事案の進行調査件数



※捜査件数は、2008年に制定された、“Intellectual Property Act”に基づき集計されたもの
出典: FBI, PRO IP ACT ANNUAL REPORT 2012　等

経済スパイ法による代表的な判決事例

問題となった時期（摘発時期等）	漏えい企業（漏えい情報）	流出先	刑罰
2005年	GM社（ハイブリッド電気自動車の開発に関する文書）	ミレニアム・テクノロジース・インターナショナル社（中）	懲役3年、罰金2万5000ドル（1832条）
2006年	グッドイヤー社（タイヤ組立て機械の設計）	ワイコ社（米）	自宅監禁4ヶ月、執行猶予4年、社会奉仕150時間（1832条）
2009年	ボーイング社（スペースシャトルや戦闘機などの航空・軍事技術）	企業への流出なし中国出身従業員（エンジニア）	懲役188ヶ月、保護観察3年（1831条及び1832条）
2011年	フォード社（フォード社の車両に独特の詳細な性能要件に関する試験方法等が記載されたシステム設計仕様書：約4000点）	上海汽車工業社（中）	約6年の懲役、保護観察2年、罰金1万2500ドル（1832条）
2011年	モトローラ社（第2世代携帯電話技術）	サン・カイセンス社（中）	懲役48ヶ月（1832条）
2012年	デュポン社（二酸化チタンに関する営業秘密）	バンガン社（中）	15年の懲役刑、2780万ドルの違法収益の没収（1831条）

【韓国】

韓国警察庁による摘発件数

出典:産業技術の流出防止及び保護に関する総合計画（2013）

不正競争防止法及び営業秘密保護に関する法律による代表的な判決事例

摘発時期等	漏えい企業	流出先	漏えい情報
2004年	韓国企業A	台湾企業B	プラズマディスプレイパネルの技術情報
2007年	韓国企業F	中国企業G	自動車自動変速機技術
2008年	韓国企業H	オーストラリア企業I	亜鉛精錬工法の技術
2009年	韓国企業J	韓国企業K	真空乾燥装置及び度厄供給装置に関する技術
2009年	LG電子社	中国ベンチャー企業L	エアコン工場の配置図面
2010年	韓国企業M	中国企業N	両開き冷蔵庫の製造技術
2010年	韓国企業O	中国企業P	3D技術
2011年	韓国企業Q	韓国企業R	回路図、品質管理に関する資料
2011年	韓国企業S	中国企業T	医薬品原料製造技術
2012年	サムスン社	中国企業U	ディスプレイの技術情報
2012年	韓国企業V	中国企業W	船舶部品の設計技術
2013年	家電メーカー	中国企業X	ロボット掃除機に関する営業秘密

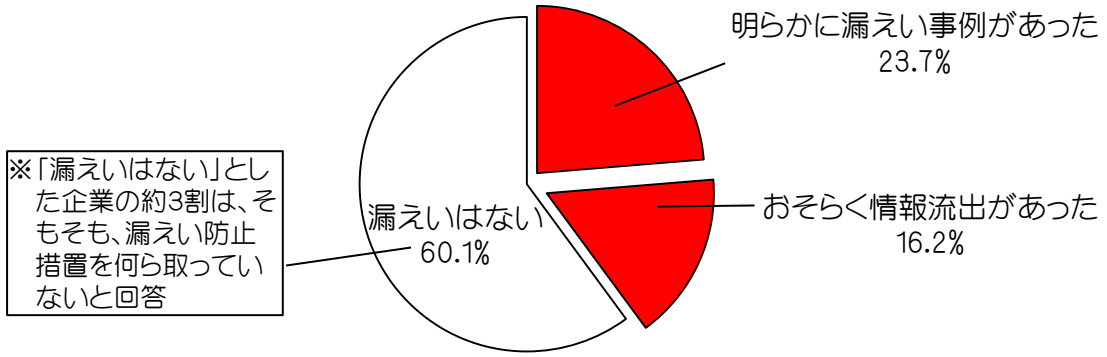
出典:　経済産業省「諸外国における営業秘密保護制度に関する調査研究報告書」（2014）
知的財産協会　「国際知財制度研究会資料」　より抜粋

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洩も内外で急増する傾向。

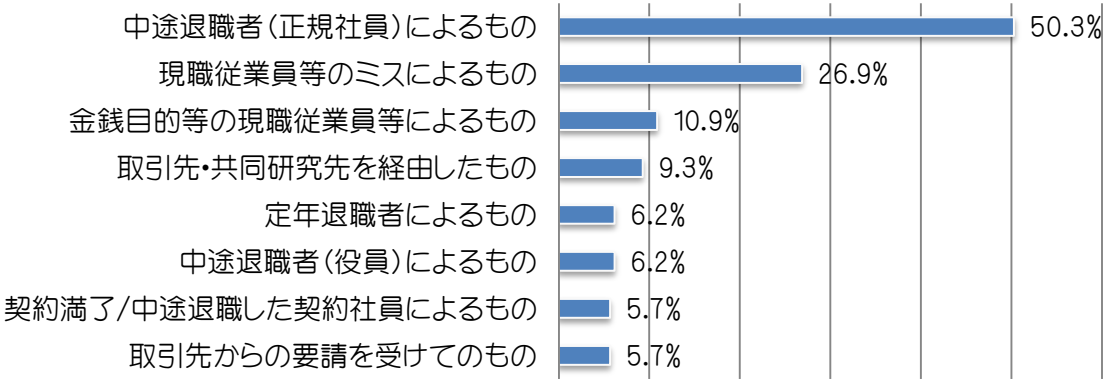
情報の漏えいの実態

少なくとも約4割の大企業（全企業で約14%）で情報漏えいの疑い（これも氷山の一角に過ぎない可能性）



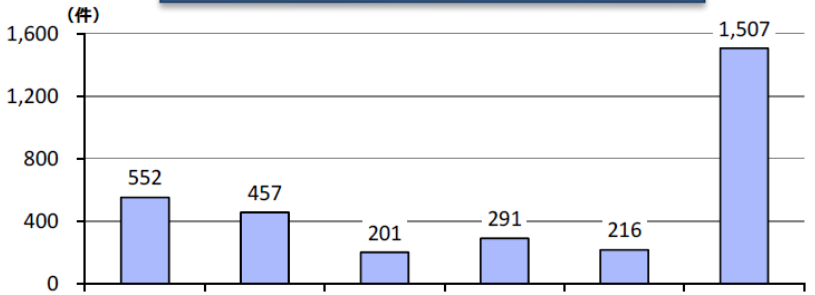
（出典）経済産業省『平成24年度　人材を通じた技術流出に関する調査研究』アンケート調査（回答約3000社）

情報漏えいルート



（出典）経済産業省『平成24年度　人材を通じた技術流出に関する調査研究』アンケート調査（回答約3000社）

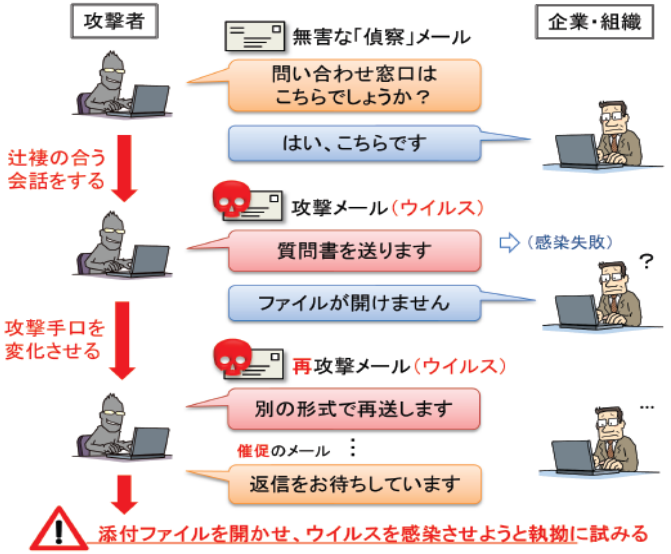
標的型メール攻撃の増加



（出典）警察庁　平成26年中のサイバー空間をめぐる脅威の情勢について

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 ～

2－1　今後の対策（技術情報等の流出防止に向けた官民戦略会議）

我が国企業の重要技術等の国内外への流出を断固として許さない社会を創出するため、「技術情報等の流出防止に向けた官民戦略会議」を本年1月に開催し、「行動宣言」を発出（平成27年1月28日）。

行動宣言のポイント

- 企業独自の製造ノウハウ等（営業秘密）は競争力の源泉。
- その重要性は増大する一方で、窃取され、価値を喪失する懸念が深刻化（内外での流出事例の増加、手口の高度化）。

営業秘密侵害を断固として許さない社会を創出

1．企業情報の防御（予防策の徹底）

- 技術の秘匿化、情報の電子化、外国人従業員の増加を含む雇用環境の変化が進む中で、必要な対策を講じる必要。
- 予防策の実施に当たっては、経営層自身のリーダーシップの下、全社的な対策が不可欠。
- 従業員を能力主義・成果主義に基づき適正に評価する人事制度の構築も重要。

＜政府・各団体の取組の宣言＞
- ○各種団体による啓発活動の加速
- ○営業秘密管理指針の全部改訂、営業秘密保護マニュアルの策定
- ○営業秘密に関する相談窓口の設置
- ○中小企業等に対する普及・啓発
- ○サイバー攻撃の手口情報の共有の促進

2．情報漏えいへの断固とした対処（一罰百戒）

- 「有事」の際には、それを恥じることなく、行為者に対する厳正な措置が必要（民事、刑事）。
- 政府は、抑止力向上のための制度整備、被害企業への相談対応、捜査力の充実強化を実施。

＜政府・各団体の取組の宣言＞
- ○抑止力向上のための制度整備
- ○営業秘密に関する相談窓口の設置（再掲）
- ○深刻なサイバー攻撃被害への復旧支援の促進

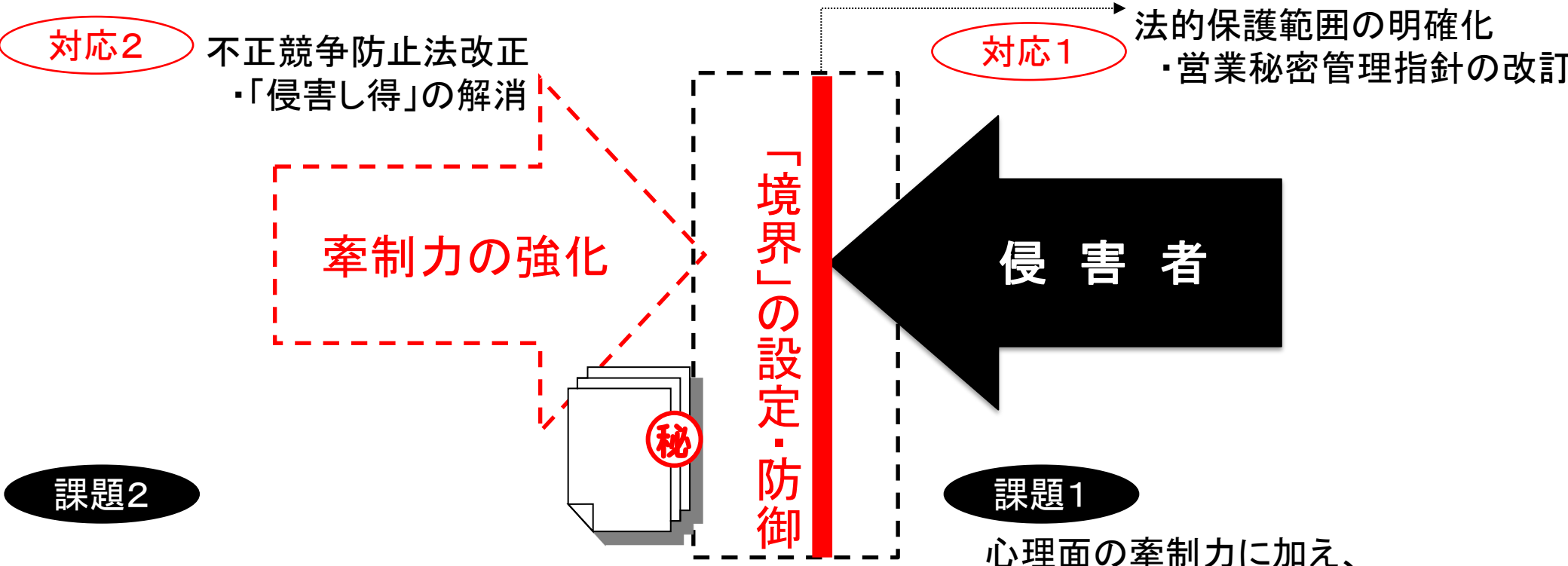
3．攻撃手法の高度化への対応（官民連携）

- 手口の高度化・複雑化への対応のため、「営業秘密官民フォーラム」で最新手口や被害実態の情報共有を実施。

＜政府・各団体の取組の宣言＞
- ○実務者による官民での緊密な情報交換の実施
- ○政府による情報収集・提供
- ○各団体の取組の推進

2－2　「行動計画」の進展と今後の展望

法的枠組みの整備は進展。今後は、企業内における実効的な対策と法執行が課題。



課題2

「一罰百戒」により現実の牽制力を引上げ

○「営業秘密110番」による被害者と捜査実施との調整
○民事による責任追及の容易化

課題1

心理面の牽制力に加え、
「予防」のための「全社的対策」を推進

○「営業秘密保護マニュアル」策定
○現実の侵害動向を踏まえたメリハリのある対策
○業界・企業のプラクティスの共有

3　法的枠組みの整備(1)　不正競争防止法改正(平成27年7月3日成立)

我が国企業の競争力や雇用の源泉である営業秘密の不正な窃取・利用に対して、「侵害し得」を是正。刑事・民事の両面で抑止力を高め、諸外国と遜色がない水準とする。(公布後半年以内に施行)

抑止力の向上

(営業秘密の価値上昇・侵害懸念の増大)

法定刑の引上げ

	現　行		改正案
・実行行為者	10年以下 1000万円以下	→	(変更無し) 2000万円以下 (海外重課3000万円以下) 不当な「報酬」の没収
・主犯企業	3億円以下	→	5億円以下 (海外重課10億円以下) 不当収益没収
・告訴の要否	親告罪	→	非親告罪

23年改正(刑訴手続の特例)実施、中小企業の製造ノウハウの取引先による不正使用(現状は泣き寝入り)や、顧客情報の漏えい(真の被害者は個人)を踏まえたもの。

賠償請求等の容易化(立証負担の軽減)

生産技術等の不当な使用について民事訴訟上の立証責任を転換。窃取者(被告)が「窃取した技術を使っていないこと」を立証。

※注　民訴法上の原則は原告が立証。→営業秘密訴訟の勝訴率約15%
(民訴全体7割以上)

侵害品の譲渡・輸出入禁止

特許権侵害品と同様に、他人の営業秘密を侵害した製品の譲渡輸出入を禁止(悪意・重過失の場合)。

処罰範囲の整備

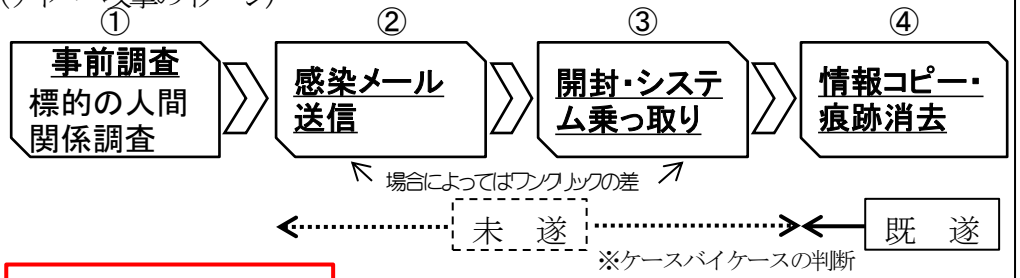
(IT環境の変化)

□:刑事
□:民事

未遂行為

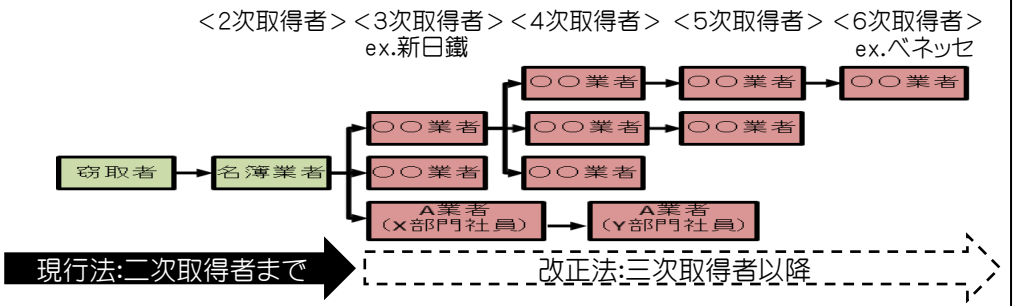
サイバー攻撃などIT技術の高度化に対応し、情報窃取や転売等の未遂を処罰(例:PC乗っ取りなど危険性の高い行為)。

(サイバー攻撃のイメージ)



情報の転売行為

営業秘密の転売利用を処罰対象に追加。



インターネット上の情報の窃取行為(クラウド)

インターネット上に保管された情報の窃取を処罰対象として明確化。

※注　クラウドの多くは、物理的所在地(サーバー)が海外であり、国外での犯罪行為と評価される可能性が高い(不可罰)

（参考）営業秘密保護法制に関する各国比較

□ :改正

			日本 （不正競争防止法）	米国 （経済スパイ法）	韓国 （不競法、産業技術流出防止法）	ドイツ （不正競争防止法）
刑事	処罰範囲	処罰対象行為	取得・使用・開示 （二次取得者まで） → 制限撤廃	取得 （制限なし）	取得・使用・開示 （制限なし）	取得・使用・開示 （制限なし）
		海外での行為の処罰	・日本企業の営業秘密の海外での使用・開示 → 海外での窃取行為（取得）の追加	・米国企業の営業秘密の海外での取得	・韓国企業の営業秘密の海外での取得・使用・開示	・ドイツ企業の営業秘密の海外での取得・使用・開示
		犯罪成立時期	既遂のみ → 未遂の追加	共謀・未遂 共謀者のうちの1人以上が目的達成のための何らかの行為をなす必要	陰謀・予備・未遂	共謀・未遂
	法定刑	自然人	10年、1000万円以下 → ・懲役：変更なし ・罰金：2000万円以下〔海外重課：3000万円〕 ・不当収益没収	10年、罰金の上限なし（※） ・外国政府・機関のための取得は、15年、500万ドル以下 ・犯罪収益没収 ※量刑ガイドライン上、25万ドル以下又は価値の2倍、のいずれか大きい額	5年、5000万ウォン（約500万円）以下 ・違反行為による利得額が500万ウォンを超える場合は、不当利益額の2～10倍以下。 ・国外使用目的の漏えい10年、1億ウォン以下	3年以下（罰金は上限なし） 以下の重大な事例は5年以下 ①職業上行う場合 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を知っていた場合 ③使用を自らが外国で行う場合
		法人	3億円以下 → ・5億円以下〔海外重課：10億円〕 ・不当収益没収	500万ドル（約5億円）以下 外国政府・機関が関与する場合は、1000万ドル又は価値の3倍以下	個人と同様	100万ユーロ（約1.3億円）以下
	犯罪収益の没収		制度なし → 創設（再掲）	○ （個人・法人とも）	×	○ （個人・法人とも）
	告訴の必要性		必要（親告罪） → 不要（非親告罪）	不要	不要	不要 〔特別の公共の利益がある場合〕
民事	営業秘密侵害物品の輸入禁止		制度なし → 創設	○	○	制度なし
	立証責任／証拠収集		制度なし → 立証責任の転換	ディスカバリ	―	査察命令

3　法的枠組みの整備(2)　営業秘密管理指針の全部改訂

産構審小委員会での議論
(産業界、裁判所、連合、法曹等の20名の有識者)
パブリックコメントには経団連等21者が意見提出

多くの企業にとって、営業秘密管理は未知の分野

企業における営業秘密管理強化を支援

【産業界】

営業秘密管理指針(平成15年→H27年全面改訂)

約100の裁判例
(秘密管理性等)

分類・整理

裁判／捜査の参考に？

利用

各社の管理策

【考え方】

「秘密管理性」を満たす要件 ＝ 「境界の設定」秘密と分かったはず(客観的認識可能性) ＋ 予防策の徹底(アクセス制限)

(アクセス制限は「認識可能性」のための一つの手段)
秘密管理性要件の趣旨は、秘密情報性を社員に明示し、不測の嫌疑を回避

【具体的対策】

人的管理	組織的管理	物理的管理
「秘」表示、研修、組織管理体制、ISOの取得、朝礼等の従業者教育、工場見学制限、守秘契約等	管理方針の作成、従業員や取引先との秘密保持契約の締結、内部監査の実施等	施錠保管、入室制限、パスワード設定、社内規程による対象情報の明確化等

※全97項目

- 最低限必要な対策が不明
  大企業でも指針記載事項の半分も実現不能。
- (地裁、高裁)裁判例に混乱。
  「鉄壁」の管理を要求する例も。
  (例:ファイルに「社外秘」と記載するだけでは不十分。営業時間中に当該ファイルを保管する書棚の常時施錠が必要)

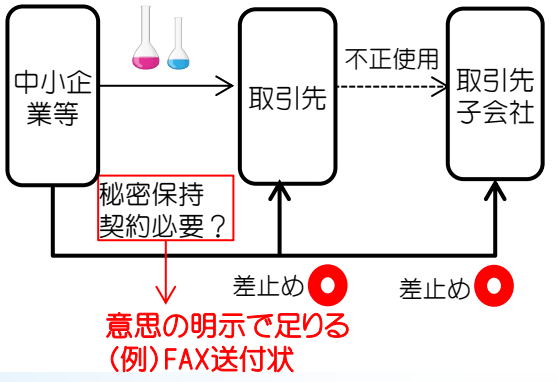
〔 指針改訂後の実務イメージ 〕

企業内の営業秘密管理

企業の業態、規模等に応じた合理的手段(アクセス制限等)で達成。従業員にとっての予測可能性確保が重要。

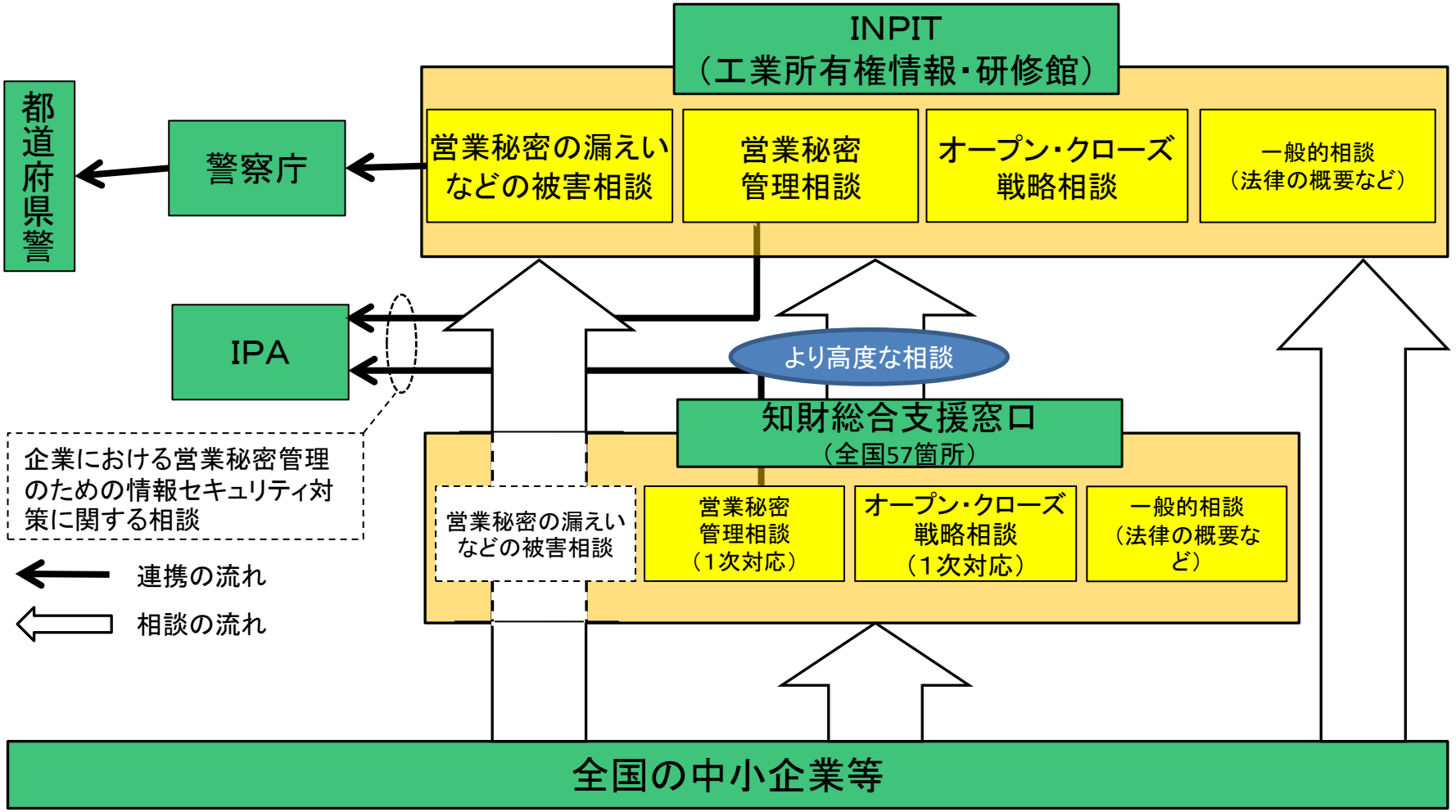
(合理的手段の例)
- 紙媒体　：合理的区分と「秘」表示
- 電子媒体：記録媒体へのマル秘表示の貼付
- 化体物(金型、デザイン)：営業秘密たる物をリスト化。
- 媒体外の情報：・転職可能性を阻害しないよう、原則、可視化。
  ・営業秘密カテゴリーのリスト化も有効。

取引先による不正使用防止



4－1　企業における営業秘密管理への支援（1）　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）



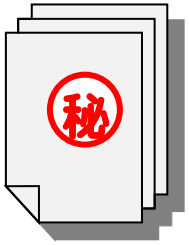
オープン・クローズ戦略相談：「特許化」「秘匿化」や、何をオープンにして、何をクローズするかについての相談
営業秘密管理相談：情報セキュリティ等、営業秘密の管理手法・システムに関する相談
※相談の対応は、事案に応じて、企業OB、弁護士、弁理士等の専門家が行う
※営業秘密110番相談件数　：　103件（2月～6月30日まで）

4－2　企業における営業秘密管理への支援(2)　「営業秘密保護マニュアル」の作成(予定)

対策は、企業の業態・規模・雇用形態により千差万別であるが、法務、人事、情報セキュリティ、知財等、多くの部門の総合力で構築する必要。　→　「営業秘密保護マニュアル」を今後作成予定

守るべき情報の特定

- 作業工程書
- 設計図
- 金型
-
-
-



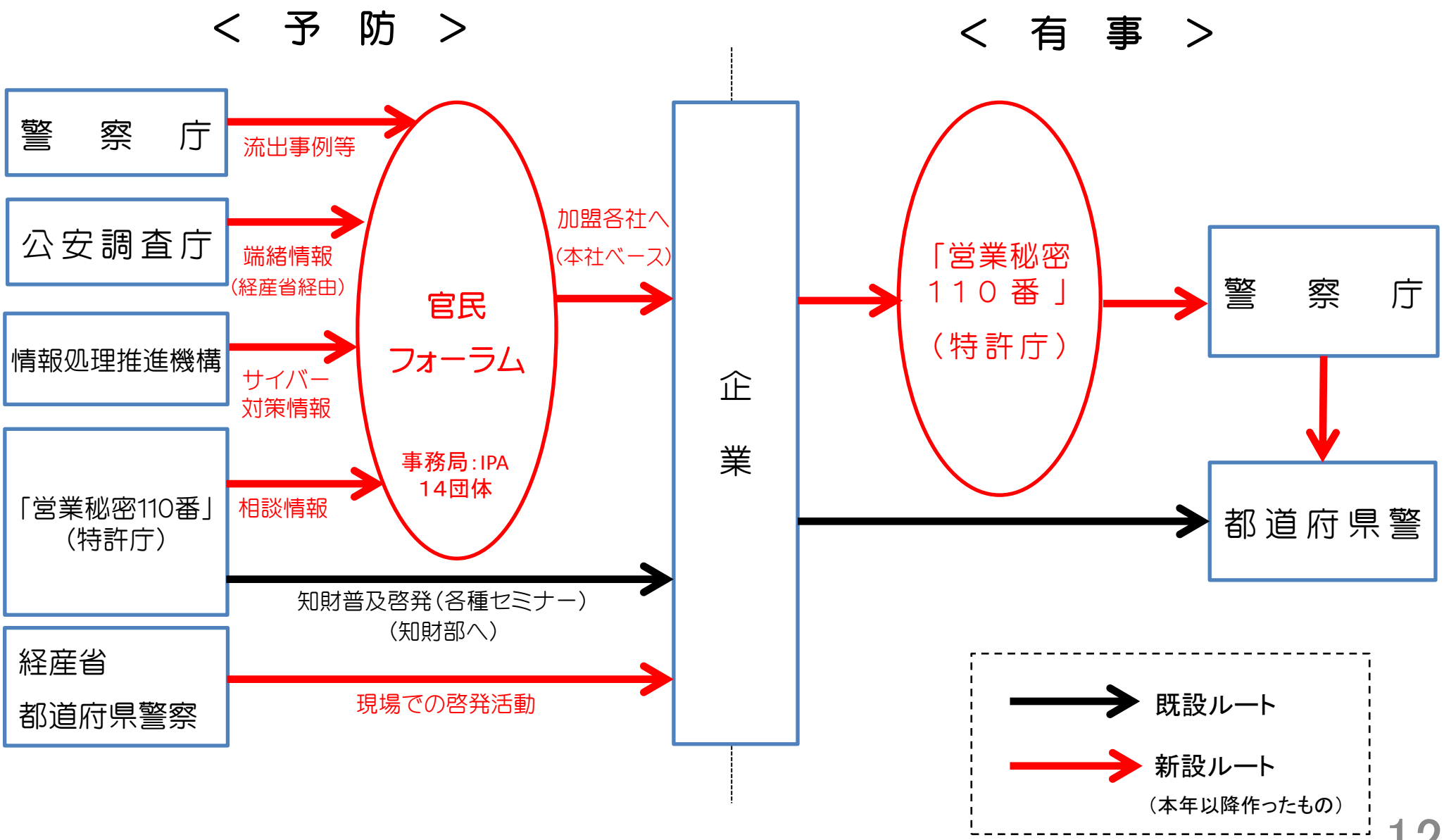
＜　平　時　＞
～窃取動向を踏まえた対応が効率的～

社員	・守秘義務契約 ・就業規則、文書規程等の整備（秘密管理措置の実施） ・教育、研修 ・適正な人事評価 ・転職受入時の意図せぬ侵害防止
子会社 ライセンス先 共同研究先	・秘密保持契約 ・教育、研修 ・セキュリティ監査 ・コンタミネーションの防止
情報 セキュリティ	・ファイアーウォールの構築 ・営業秘密へのアクセス制限の徹底 ・ログの保存、検知システムの導入

＜　有　事　＞
～刑事・民事の責任追及が重要～

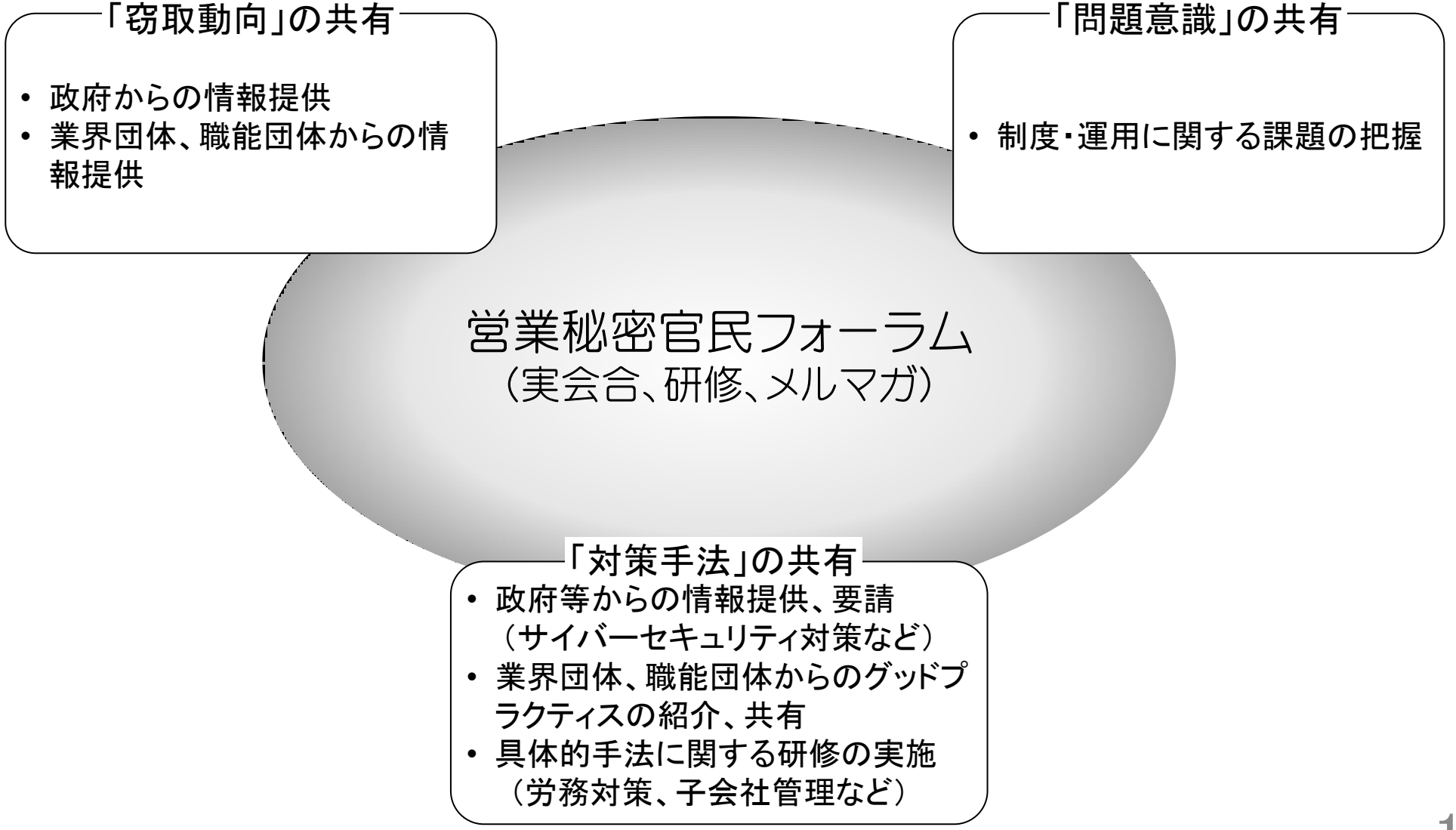
初動	・ネットワークの分断 ・アクセスログの確認 ・証拠保全
刑事	・営業秘密110番への相談 ・所轄警察署への相談
民事・ その他	・仮処分申請(差止請求) ・損害賠償請求 ・社内処分

5　関係省庁間の連携強化



6　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。



（参考）経団連要望書「海外競合企業による技術情報等の不正取得・使用を抑止するための対策強化を求める」（抄）（平成26年2月）

3. 官民フォーラムの早期創設と実効ある運営

「本フォーラムによって、こうした問題に関する官民の情報交換・意識涵養が進められることは極めて重要であり、早期の立ち上げが期待される。」

「本フォーラムは、諸外国の取組みを参考に、政府トップレベルの理解と支持のもと、警察を含む幅広い政府関係機関が積極的に関与し、ワンストップサービスを実現することが不可欠である。」

「産業界としても、官民フォーラムを始めとする政府の取組みに積極的に協力するとともに、適切な情報管理に努める所存である。」

（参考）知的財産推進計画2014（抄）（平成26年7月知的財産戦略本部決定）

第1. 産業競争力強化のためのグローバル知財システムの構築

3. 営業秘密保護の総合的な強化

（2）今後取り組むべき施策

（官民の情報共有）

- 産業界全体の実態把握と課題の抽出・情報共有や企業経営者に向けた啓発等を進めていくため、情報提供した企業が不利益を被らないような情報の匿名化・一般化が必要であることに留意するとともに、上記のワンストップ支援体制も活用しつつ、内外の漏えい事例やベストプラクティスなどの対策事例の情報の共有を可能とするための官民連携を進める。他方、政府においても、諸外国の漏えい実態や官民の対応策等についての情報等の企業との積極的な共有に努める。

議題2

相談窓口活用状況

（工業所有権情報･研修館）

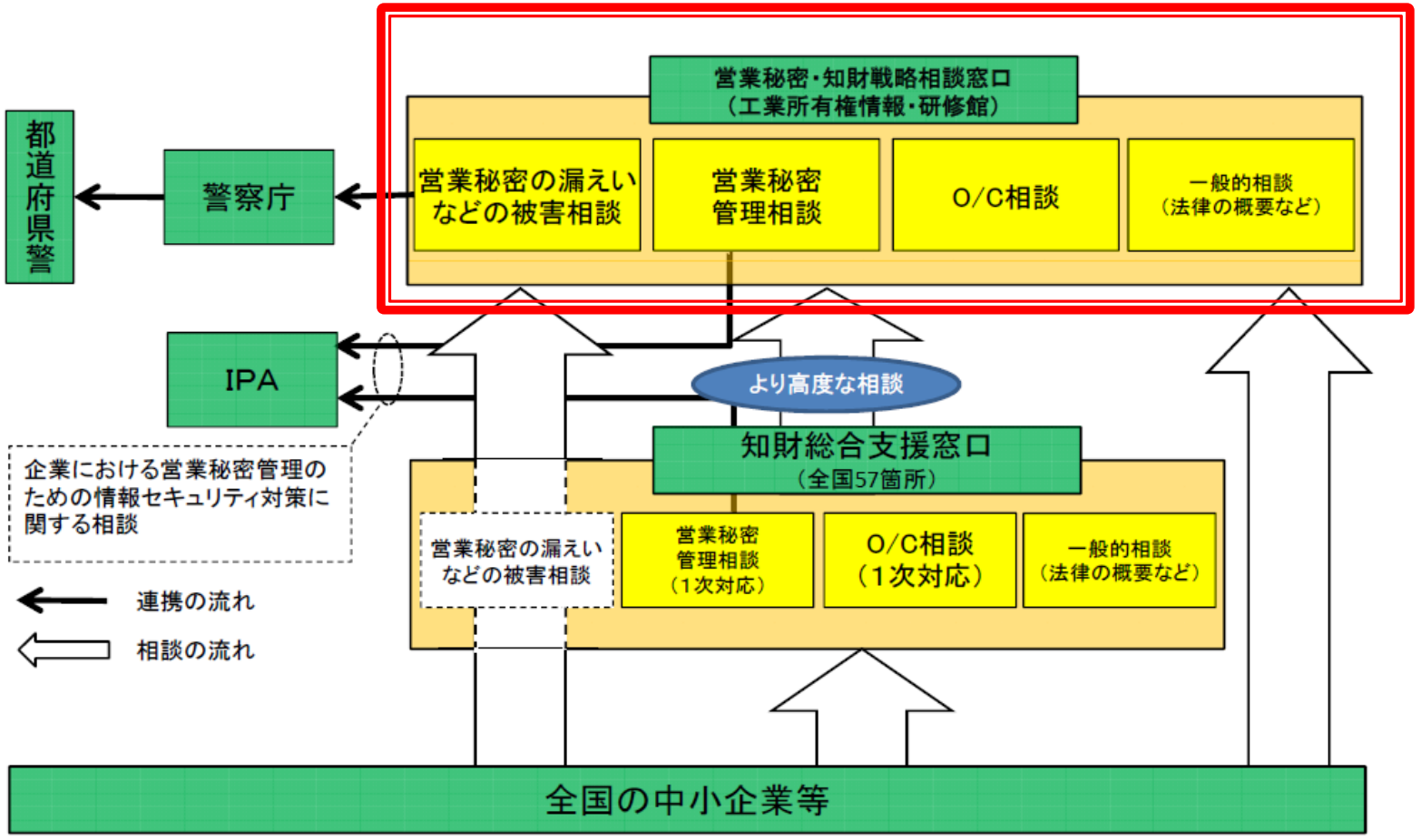
資料3

相談窓口活用状況

独立行政法人 工業所有権情報・研修館（INPIT）

中小企業等への専門家による相談体制の構築

本年２月２日に「営業秘密・知財戦略相談窓口」（営業秘密１１０番）を新設し、全国４７都道府県の「知財総合支援窓口」と連携して、中小企業等の相談に応じる体制を構築。



Ｏ／Ｃ相談：「特許化」「秘匿化」や、何をオープンにして、何をクローズするかについての相談
営業秘密管理相談：情報セキュリティ等、営業秘密の管理手法・システムに関する相談
※相談の対応は、事案に応じて、企業OB、弁護士、弁理士等の専門家が行う

INPITにおける営業秘密相談の受付状況

＜相談受付状況＞

INPIT全体での営業秘密相談の受付状況

・**営業秘密・知財戦略相談窓口**（２月２日～６月３０日）　　１０３件

（参考）

・海外展開知財支援窓口（平成２６年度、営業秘密関係）　　７８件

・知財総合支援窓口（平成２６年度、営業秘密関係）　　２０３３件

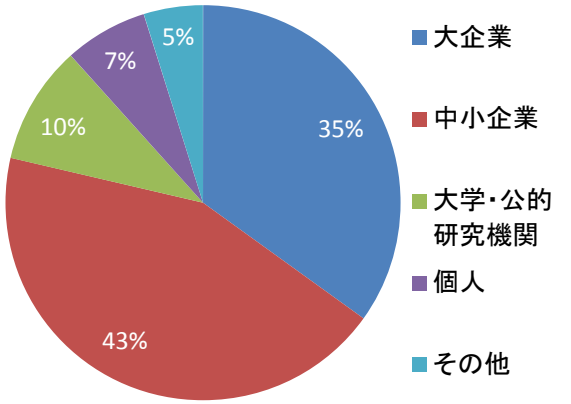
＜連携状況＞

・営業秘密・知財戦略相談窓口から警察庁　　０件

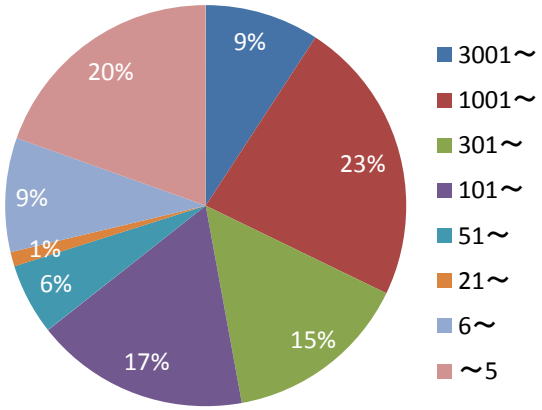
・営業秘密・知財戦略相談窓口から情報処理推進機構（ＩＰＡ）　　３件

■ 営業秘密・知財戦略相談窓口の相談者の属性等

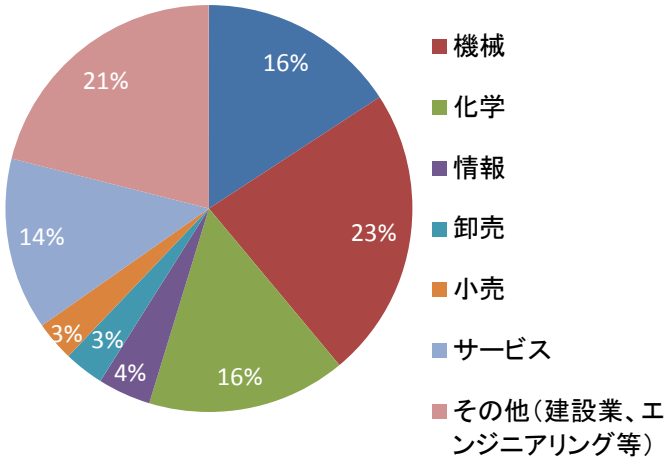
【属性】



【従業員数】



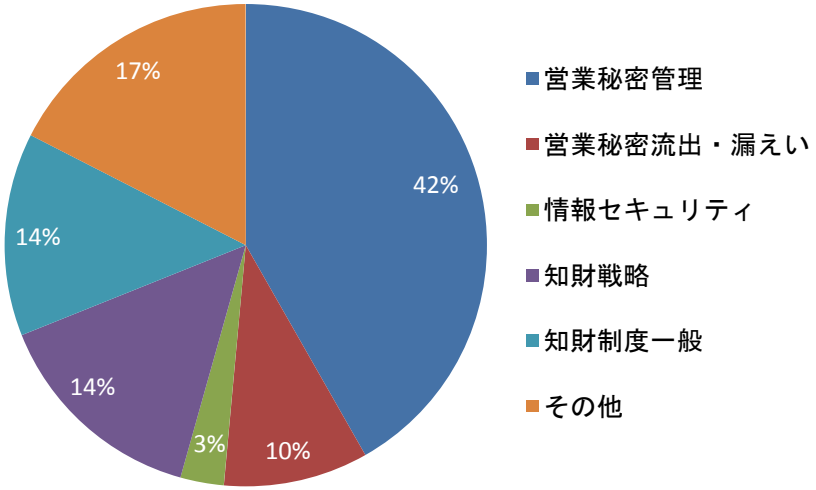
【企業の業種】



◆「大企業」には、建設会社の子会社等、大企業であるがこれまで知財戦略に対して十分な取組ができていなかったと考えられる企業が見受けられる。

営業秘密・知財戦略相談窓口の相談内容

■ 相談内容の概要

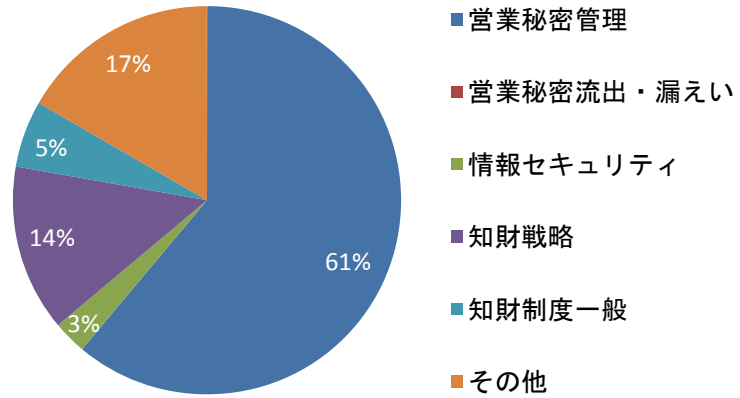


◆ 「中小企業」では営業秘密流出・漏えい（被害相談）が多いのに対して、「大企業」では被害相談はなく、事前に対策を行うための具体的な管理方法に関する相談が多くなっている。

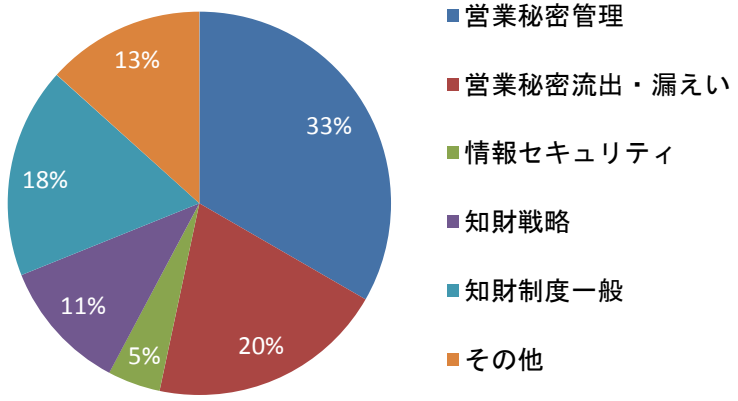
※「知財制度一般」は、不正競争防止法の法改正や、特許等の制度に関する一般的な相談を含む。

■ 相談者の属性別の相談内容

【大企業】



【中小企業】



相談窓口に寄せられた具体的相談事例

大企業

- ■ 営業秘密管理
  - ➢ 昨年、会社で営業秘密管理の仕組み作りをするWGを立ち上げた。秘密情報の層別化（「マル秘」、「極秘」、「社外秘」等）の基準や運用について教えてもらいたい。
  - ➢ 改訂された営業秘密管理指針に沿って、営業秘密管理体制を導入しようと準備中である。当社の体制案についてアドバイスをもらいたい。
  - ➢ 先使用権を確保するための資料のまとめ方、収集すべき資料の種類を教えてほしい。
- ■ 知財戦略
  - ➢ 保有特許の維持／放棄の判断基準又は仕組み作りについてアドバイスをもらいたい。
  - ➢ 自社開発ソフトの権利の守り方について教えてほしい。

中小企業

- ■ 営業秘密管理
  - ➢ 社員がライバル会社に転職した。秘密保持契約書を作成したが押印を断られ、競業避止契約書も用意していなかった。将来的な情報の流出を危惧しているが、法的な対策をとる必要があるか？
  - ➢ 成分の解析が難しい物質を開発した。特許出願せずに秘密として守りたいと考えているが、他者に権利を取られては困るので、どうしたらよいか相談したい。
- ■ 営業秘密流出防止
  - ➢ 退職者が起業した会社に仕事をとられた。技術情報を利用されているのではないか？
  - ➢ 解雇通知した従業員のパソコンからデータが消失していた。データが持ち出されたかもしれない。
  - ➢ 金型の情報を顧客（発注者）が他社に流出させた。不正競争防止法による保護が受けられるのか？

大学・公的研究機関

- ■ 営業秘密管理
  - ➢ 営業秘密管理のためのチェックシート、管理規定案を作成している。アドバイスが欲しい。

知的財産戦略アドバイザーによるセミナー

全国20箇所以上で知的財産戦略アドバイザーによるセミナーを開催中。

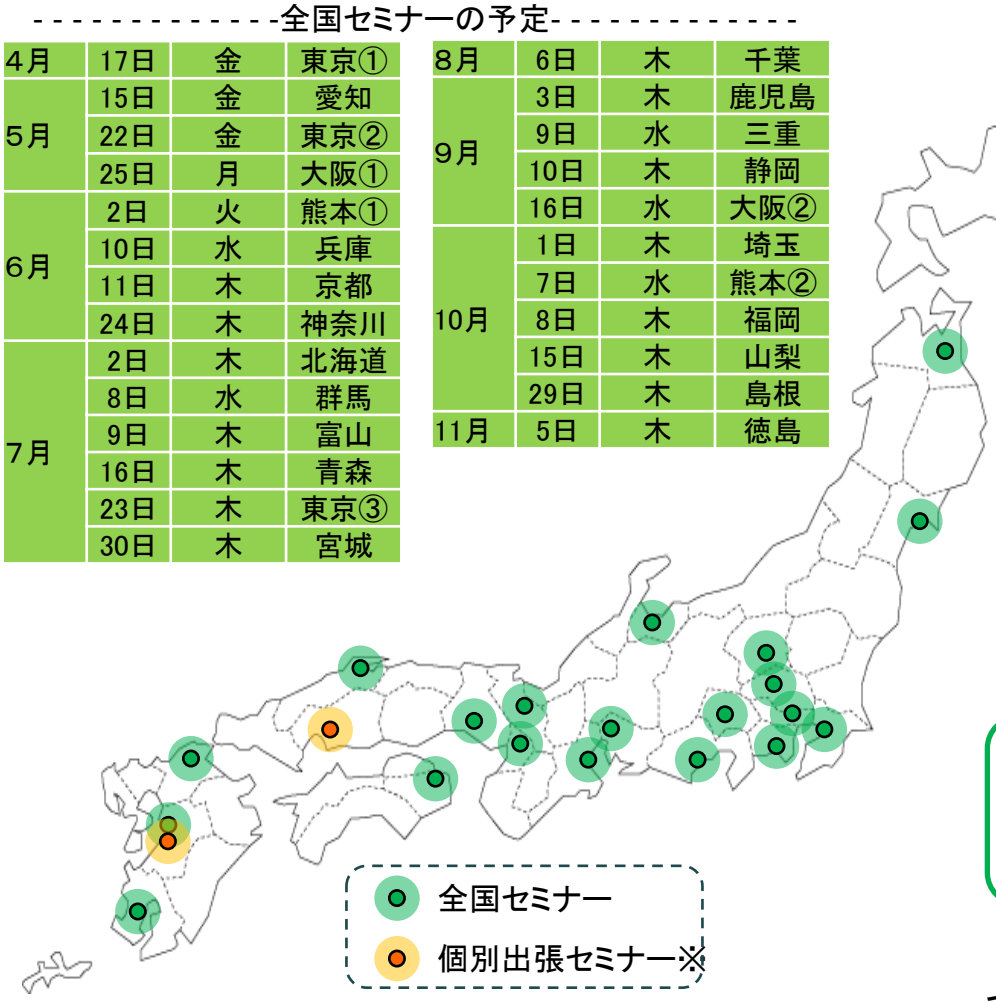
平成27年度　営業秘密・知財戦略セミナー
～あなたの会社の独自技術をシッカリ守り、活かすために～

テキストを用いた座学形式によるセミナーを開催。
（90分又は60分の講義、内容は下記のとおり）

- 企業内情報の流出が疑われる最近の事例
- はじめての営業秘密管理
- 営業秘密として「法的保護」を受けるためには
- 営業秘密の民事的保護／刑事的保護
- 特許化と秘匿化
- オープン＆クローズ戦略 等

-全国セミナーの予定-

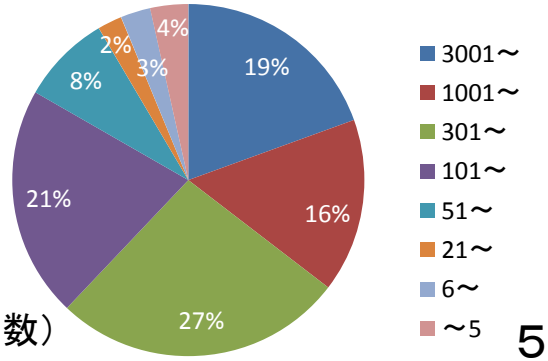
4月	17日	金	東京①
5月	15日	金	愛知
	22日	金	東京②
	25日	月	大阪①
6月	2日	火	熊本①
	10日	水	兵庫
	11日	木	京都
	24日	木	神奈川
7月	2日	木	北海道
	8日	水	群馬
	9日	木	富山
	16日	木	青森
	23日	木	東京③
	30日	木	宮城
8月	6日	木	千葉
9月	3日	木	鹿児島
	9日	水	三重
	10日	木	静岡
	16日	水	大阪②
10月	1日	木	埼玉
	7日	水	熊本②
	8日	木	福岡
	15日	木	山梨
	29日	木	島根
11月	5日	木	徳島



※希望に応じて個別企業等への出張セミナーも実施中。

全国セミナー
参加者数
712名
（平成26年度）

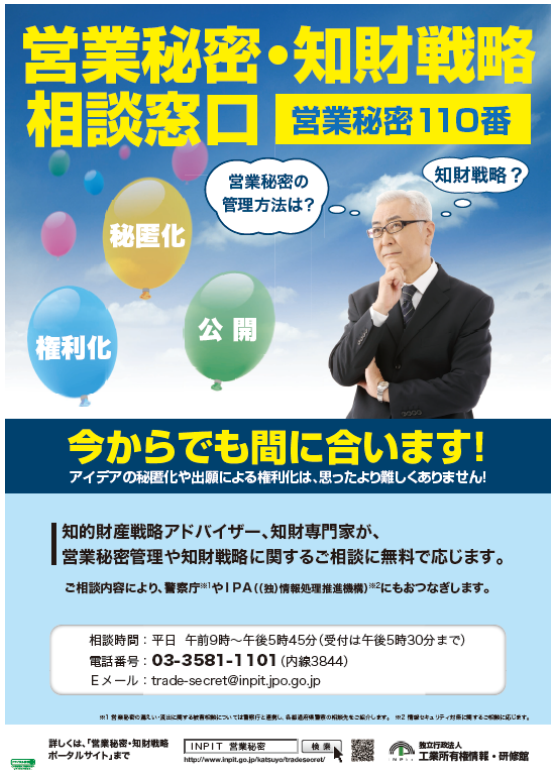
セミナー参加者所属
企業の規模（従業員数）



普及啓発の強化　～Ｗｅｂ、ポスター、パンフレット、eラーニング～

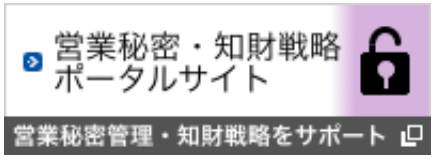
中小・ベンチャー企業等の様々な経営課題と密接に関連する営業秘密・知財戦略の重要性に関する理解増進を図るため、営業秘密・知財戦略ポータルサイトのコンテンツの拡充、eラーニングコンテンツの開発・提供（計画中）等の普及啓発活動強化を進めている。

ポスター／パンフレット



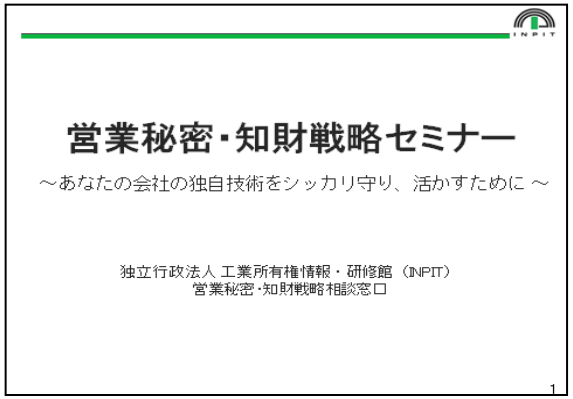
全国の知財総合支援窓口、商工会議所等に、パンフレット約6万枚、ポスター約700枚を配布。

ポータルサイト



営業秘密１１０番の紹介、営業秘密・知財戦略についての紹介、セミナー開催案内、資料等を掲載。

eラーニング（計画中）



営業秘密・知財戦略の重要性に関する理解促進を図るため、eラーニングコンテンツの開発、提供を計画。

要点

相談窓口の開設

- 知的財産推進計画2014を受けて、本年2月2日に「営業秘密・知財戦略相談窓口」（営業秘密110番）を（独）工業所有権情報・研修館（INPIT）に開設し、相談対応と営業秘密管理の重要性についての普及啓発活動を開始。

窓口に寄せられた相談の概要と特徴

- 営業秘密・知財戦略相談窓口には、中小企業（43%）のみならず、大企業（35%）からも相談が寄せられている。営業秘密の管理・保護については、中小企業だけが遅れているわけではない様子。大企業では、建設系会社の子会社やエンジニアリング会社等（知財分野での対応が遅れていたと思われる企業）からの相談が見受けられた。
- 相談内容別では、中小企業では営業秘密流出・漏えい（被害相談）が多いのに対して、大企業では被害相談ではなく、具体的な管理方法に関する相談が多い。中小企業では、実害が生じてから相談するなど、対応が後手に回っているケースが認められたが、大企業では実害が生じる前に体制を整えようとする動きが出ている。
- 昨今の情報流出事件に触れて社内で対策を始めた企業に加え、営業秘密・知財戦略セミナーに参加して必要性を感じ、対応を始めた企業からの相談が増えてきている。

今後の方針等

- 中小企業のみならず大企業も対象に含め、営業秘密・知財戦略セミナーの継続開催、啓発用各種資料等の充実等によって普及・啓発活動を展開・強化する方針。
- 全国各地の知財総合支援窓口の支援担当者等にも啓発活動を行う等、相談支援を「点から面」に拡張し、営業秘密に関する問題意識を持たない事業者層に対しても気づきを与える方針。
- 引き続き、警察庁、IPAとの連携によって営業秘密漏えい等の被害への対応を強化する方針。

議題３

営業秘密侵害事犯への 対処方法等について

（警察庁）

資料４－１

営業秘密官民フォーラム資料

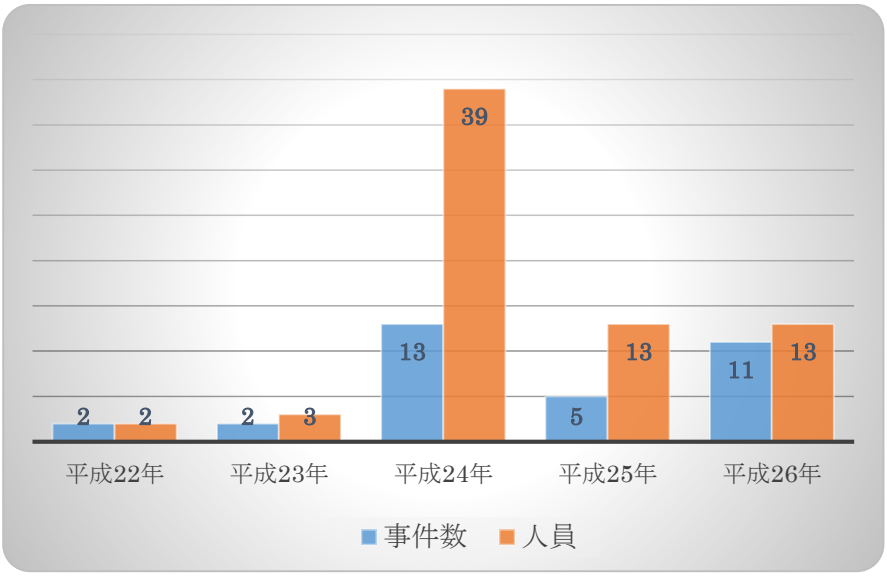
平成 27 年 7 月 7 日(火)
警察庁生活安全局
生活経済対策管理官

営業秘密侵害事犯への対処方法等について

１　最近における営業秘密侵害事犯の相談・検挙の状況

（１）相談（警察庁に報告のあったもの）
平成 25 年　12 件
平成 26 年　29 件

（２）検挙事件数・人員



２　平成 26 年中の主な検挙事例

事例１　自動車製造・販売等会社従業員による営業秘密の領得に係る不正競争防止法違反事件

自動車製造・販売会社従業員（37）は、同業者に転職する直前の平成 25 年 7 月、不正の利益を得る目的で、同社のサーバコンピュータにアクセスし、同社の営業秘密である自動車の商品企画に関する情報等 13 件を自己所有のハードディスクに転送して複製を作成し、営業秘密を領得するなどした。

平成 26 年 5 月、同人を不正競争防止法違反（営業秘密の領得）で逮捕した。（神奈川）

事例２　システムエンジニアによる営業秘密の領得・開示に係る不正競争防止法違反事件

通信教育会社のデータベース改修に従事していた派遣システムエンジニア（39）は、平成 26 年６月、２回にわたり、不正の利益を得る目的で、同社のサーバコンピュータにアクセスし、同社の営業秘密である顧客情報合計約 3,000 万件を自己所有のスマートフォンの内蔵メモリに記録させて複製し、営業秘密を領得した。また、当該顧客情報約 1,000 万件を大容量ファイル送信サービスを使用して、名簿業者に送信し、営業秘密を開示（販売）した。

平成 26 年８月までに、同人を不正競争防止法違反（営業秘密の領得・開示）で検挙した。（警視庁）

３　事案認知時の対処方法（過去の事件や相談事例から）

（１）認知の端緒

○　どのような場面で把握しうるか？

多くの場合、退職、転職をきっかけとした会社の調査から発覚

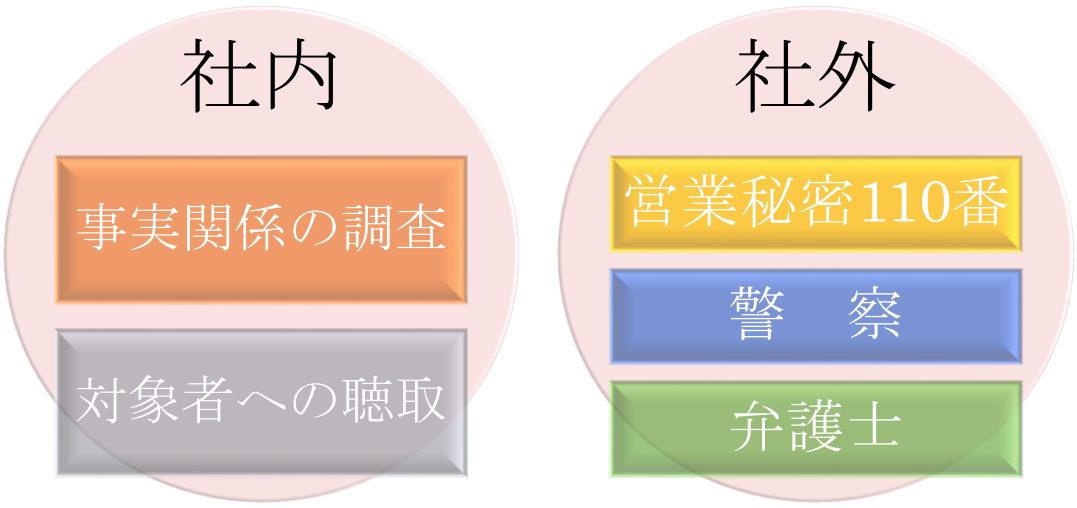
○　その他の場面としては？

取引先からの連絡

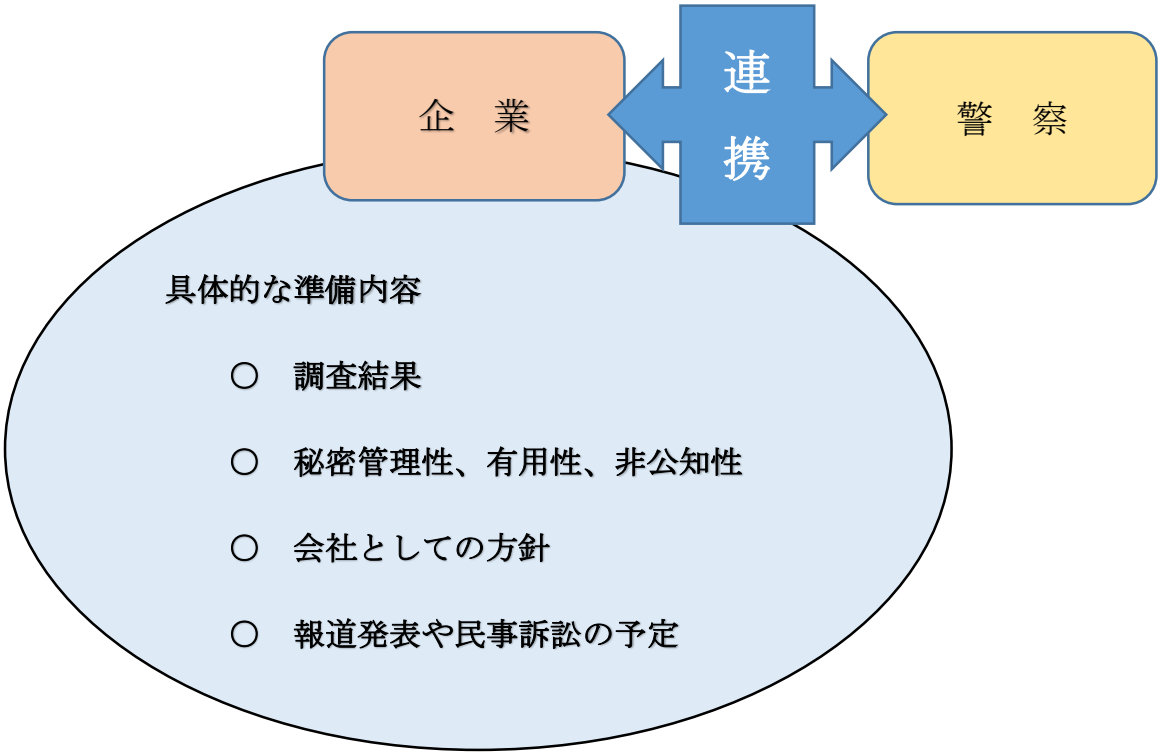
顧客からの苦情

匿名の通報

（２）認知後の初動措置



（３）警察に相談されるに際して



（４）証拠保全についてのお願い

○　データの保存先を確認し早急に保全措置を

○　データの内容を限定することなく保全を

○　データを確認し調査した経過を明らかに

４　立証上問題があった事例

（１）秘密管理性

（２）図利加害目的

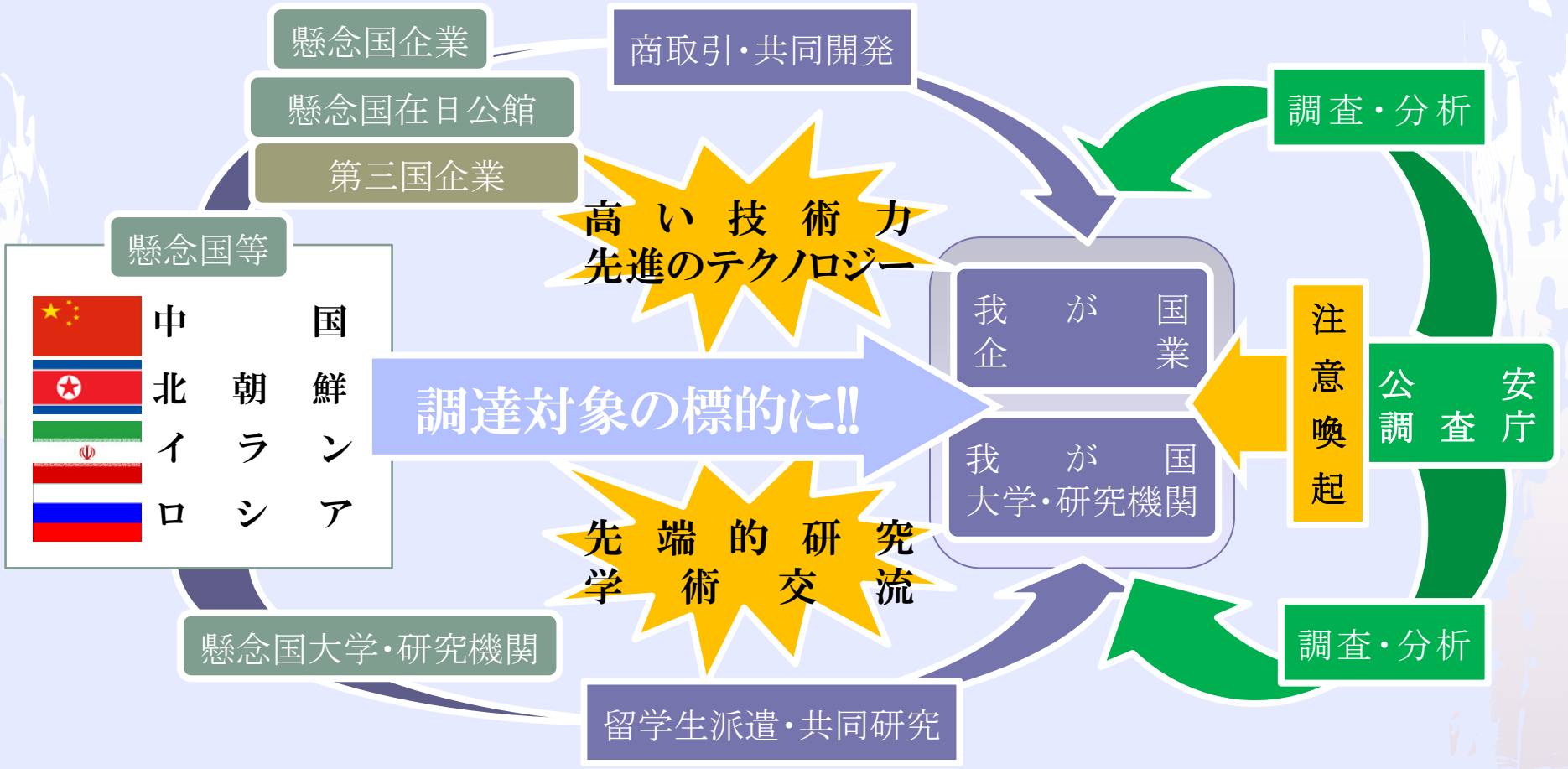
議題４

技術情報窃取の動向等

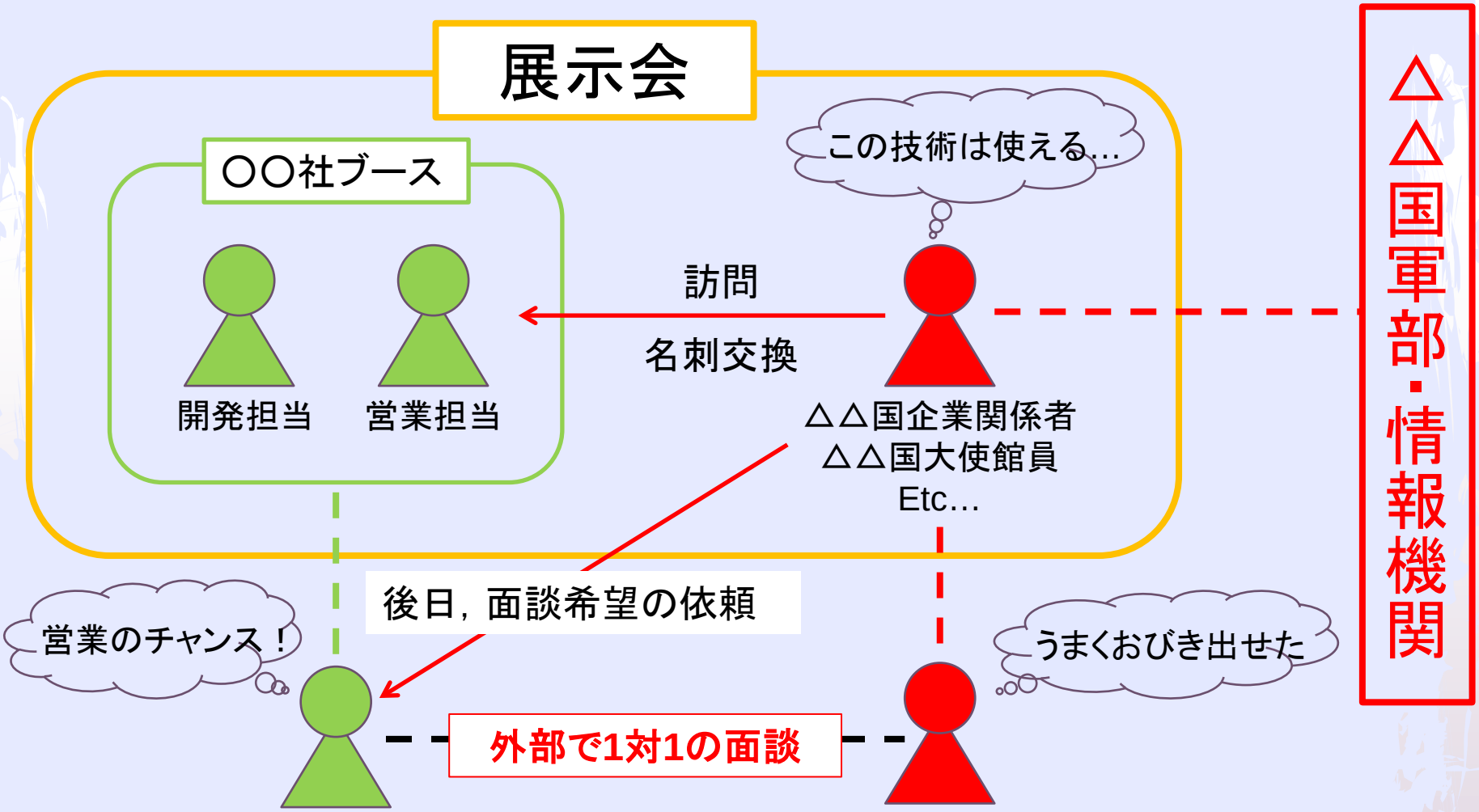
（公安調査庁）

資料5

大量破壊兵器等の拡散防止に向けた取組

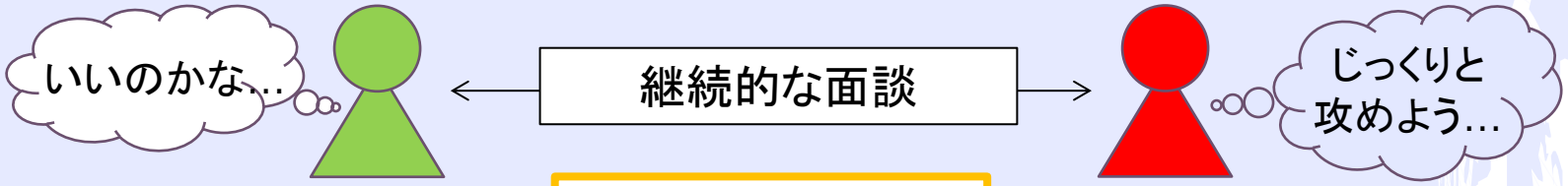


展示会を契機とした情報窃取の危険性(1)



展示会を契機とした情報窃取の危険性(2)

企業側の対策



報告聴取
状況把握

序盤:関係構築

○ 対象の話(特に業務内容，金銭関係，異性関係)を親身に聞く
→*業務上の関係から個人的な関係へ，そして対象の弱点を把握*
○ 一般的な質問や軽い依頼をし，その謝礼として食事代等を奢る
→*謝礼を受けることへの抵抗感を薄める*

情報管理

中盤:要求のエスカレーション

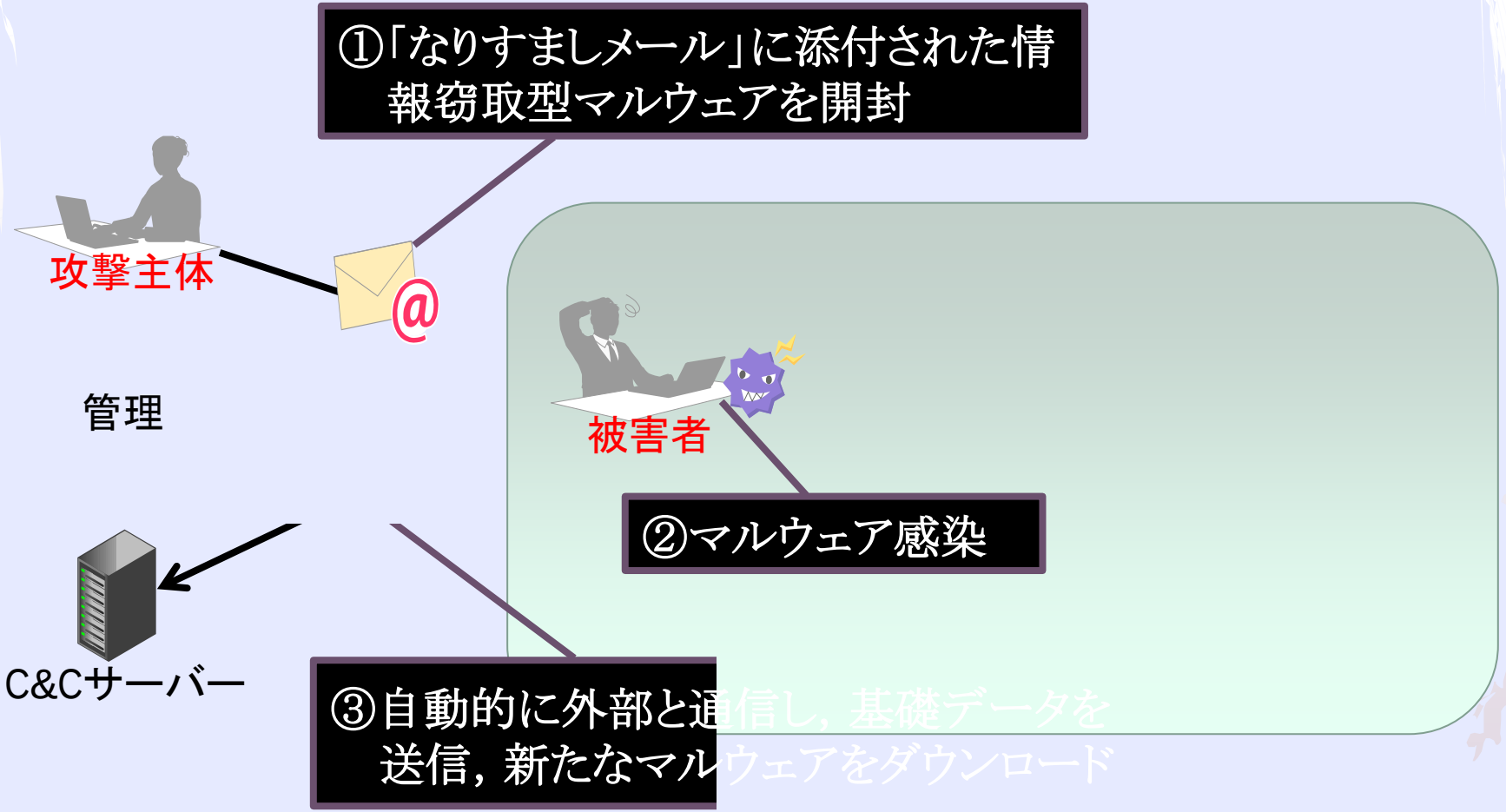
○ より専門的な情報や資料を要求し，謝礼も増やしていく
→*「情報・資料を提供すれば，謝礼がもらえる」ことに慣れさせる*

**最早
手遅れ**

終盤:重要情報の窃取

○ 営業秘密に該当するような重要情報を要求
→*構築した人間関係を利用(「この人の言うことは聞いてあげたい」)*
場合によっては，把握した弱点で脅迫
「一線」を越えさせれば共犯者意識を強調

サイバー攻撃による情報窃取の危険性(1)



サイバー攻撃による情報窃取の危険性(2)

＜巧妙な「なりすましメール」＞

送信者: Y課長補佐 xxxx@XXX.co.jp
日時: 2013年5月14日 14:45
宛先: xxxxxxx@XXX.co.jp
件名: 【至急!】情勢検討会議レジュメ
添付: 情勢検討会議レジュメ.pdf (548 KB)

A 様

情勢検討会議(15時，5階大会議室)に関しまして，修正が入りましたので，至急，ご確認願います。

➡ 内部会合の名称，開催時間，関係者，社内ルールが把握されている。(既に，基礎情報を収集されている恐れ)

議題５

サイバーセキュリティ対策

（情報処理推進機構）

資料6

IPA Better Life with IT

サイバーセキュリティ対策
～高度化・巧妙化する攻撃～

営業秘密官民フォーラム　2015.7.7

独立行政法人 情報処理推進機構　参与
兼セキュリティセンター長
伊藤　毅志

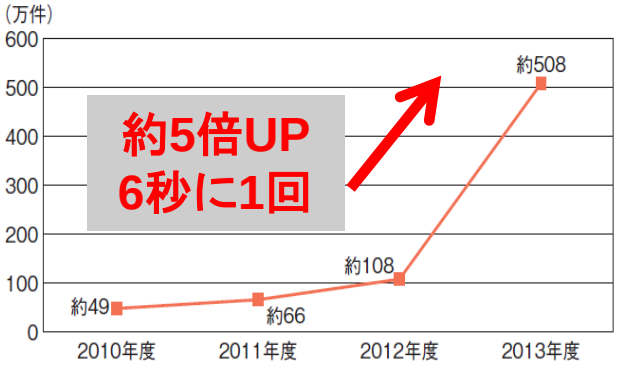
内容

- サイバーセキュリティの状況
- 標的型攻撃の状況
  - 執拗に狙う攻撃者の例
  - 標的型メールの例
- 内部者による不正
  - 内部不正防止ガイドライン
- 経営者の関与、ダイナミックなインシデント対応が必要
- IPAの取り組み

サイバーセキュリティの状況 ～増大する脅威～

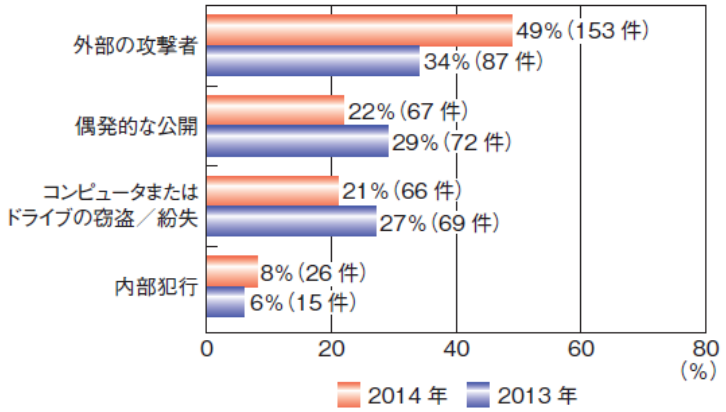
IPA

GSOCセンサーで認知された政府機関への脅威の件数の推移



出典：NISC　2014

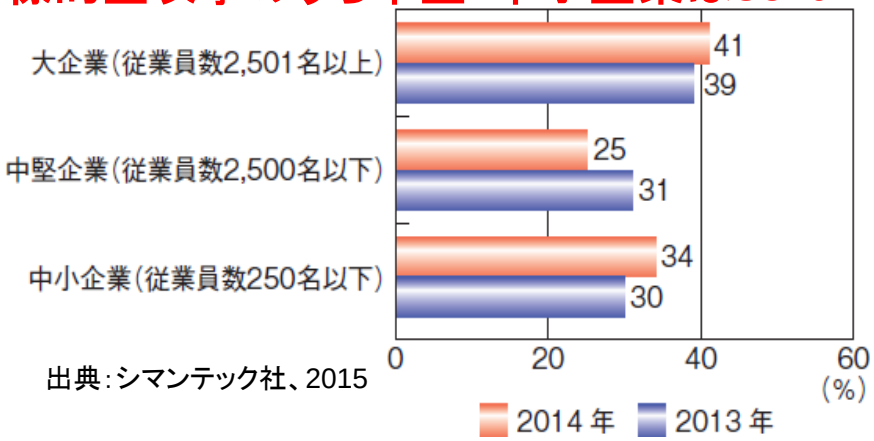
データ侵害の原因別比較（2013年～2014年）



出典：シマンテック社、2015

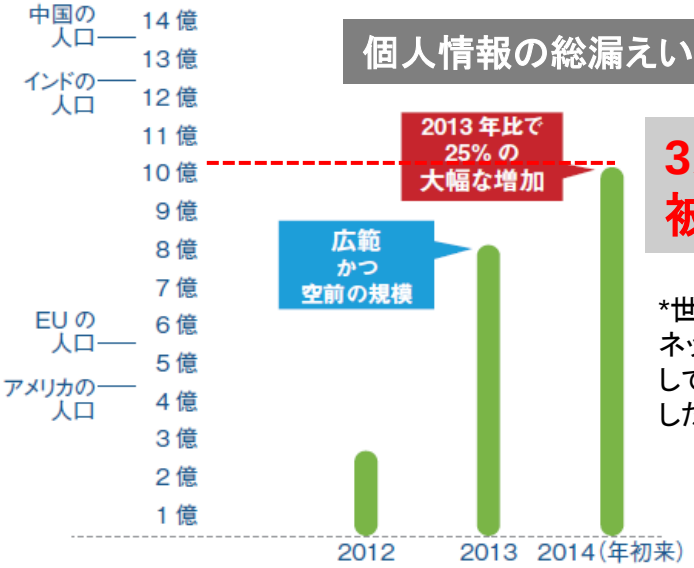
中堅・中小企業も狙われています

標的型攻撃のうち中堅・中小企業は59%



出典：シマンテック社、2015

個人情報の総漏えい人数



3人に1人が被害*

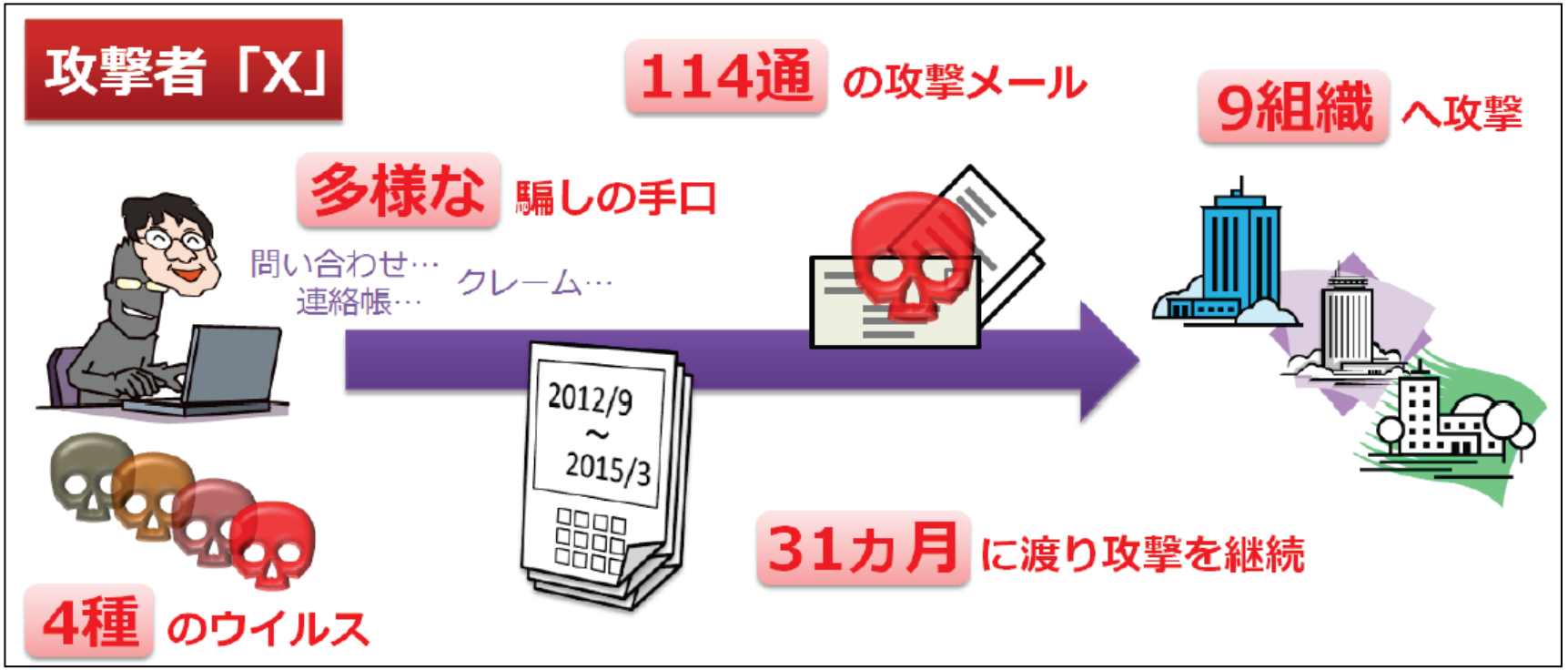
*世界のインターネット人口を30億として、重複を無視した場合

出典：日本IBM社、2015

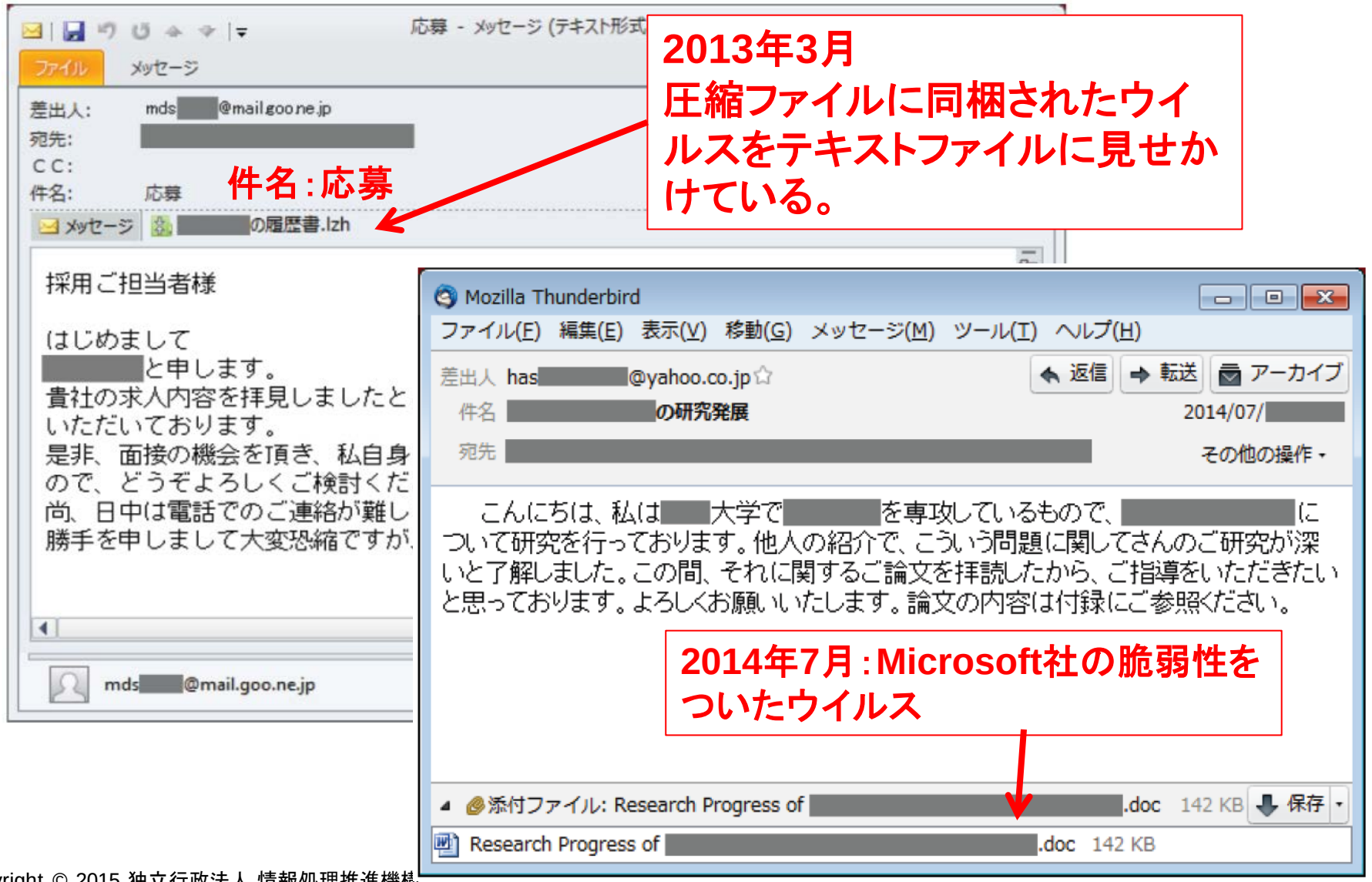
標的型攻撃の状況

- 同一攻撃者が31か月間で114通のメールを9組織へ攻撃（2012年度～2014年度までの観測，IPA）

問い合わせや求職、製品へのクレーム等を装った巧妙な内容のメールで受信者をだまし、遠隔操作ウイルスを侵入させ、組織の重要情報窃取を試みる。



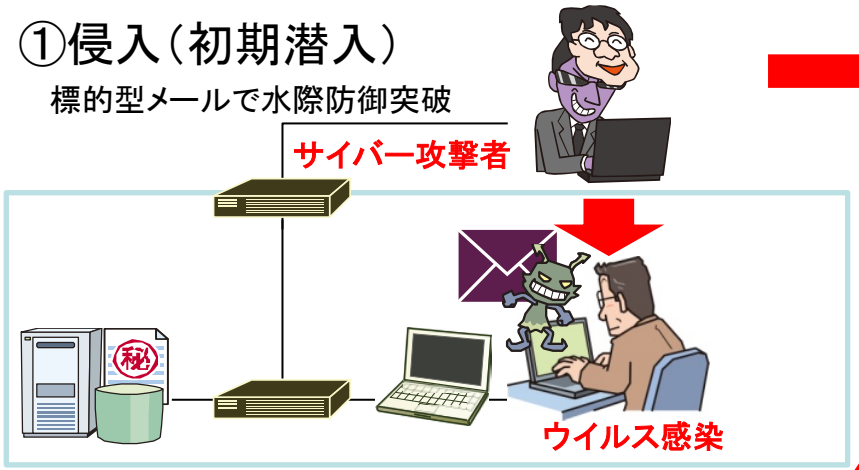
標的型攻撃メールの例



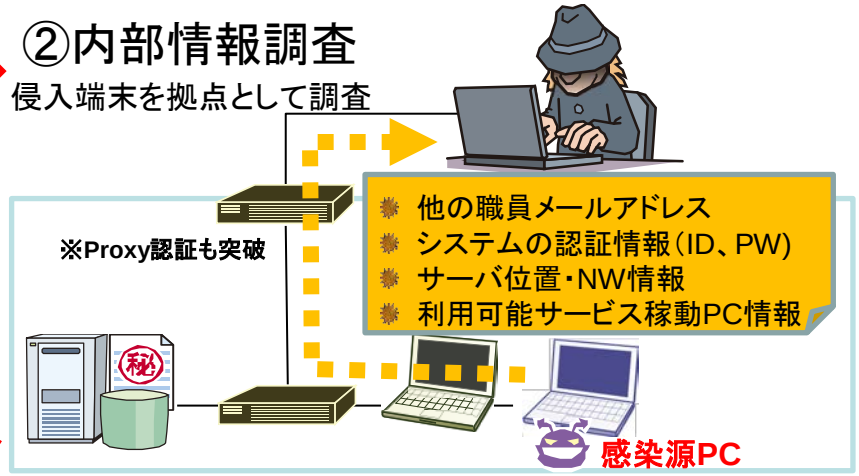
外部攻撃により情報漏洩に至る過程
～水際対策は限界　内部対策も含め多重防御を

IPA

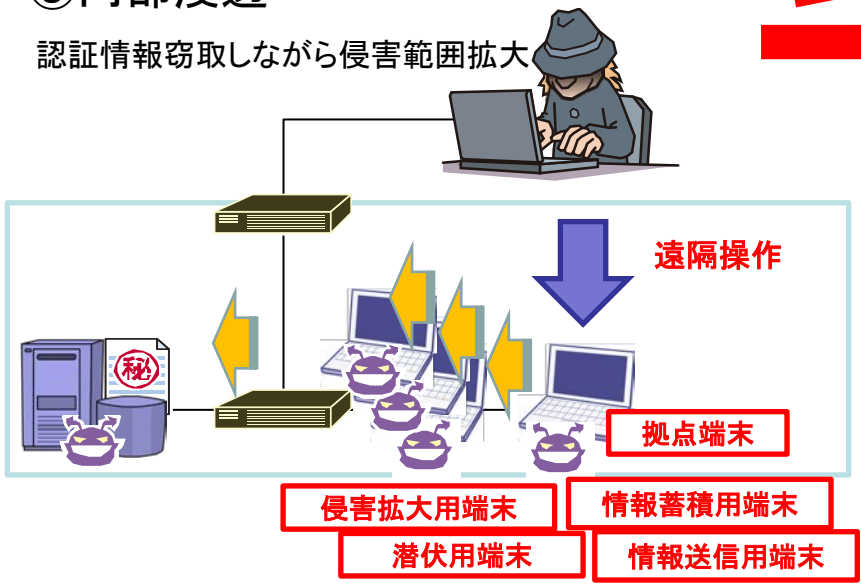
①侵入（初期潜入）
標的型メールで水際防御突破



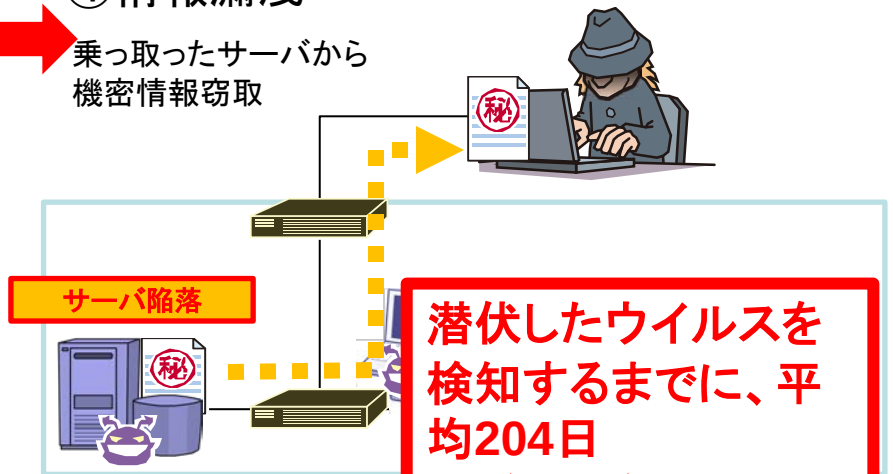
②内部情報調査
侵入端末を拠点として調査



③内部浸透
認証情報窃取しながら侵害範囲拡大



④情報漏洩
乗っ取ったサーバから
機密情報窃取



潜伏したウイルスを検知するまでに、平均204日
ファイア・アイ,2015

内部者による不正
～相次ぐ不正競争防止法違反～

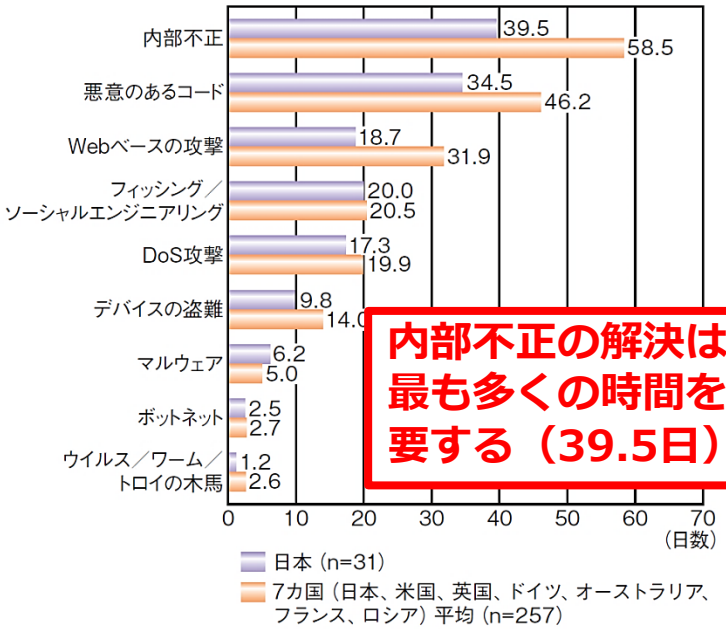
- 技術情報等の営業秘密の流出は、組織における内部者（退職者を含む）によるものが多い。

内部者による犯行事例の一部

報道年月	事件の概要	不正行為者	動機
2014年7月	株式会社ベネッセコーポレーションの顧客データベースを保守管理するグループ会社の業務委託先の元社員が、約3,504万件の個人情報を流出させたとして逮捕された。	委託先元社員	金銭の取得
2015年1月	家電量販大手エディオンの子会社の元役員が遠隔操作ソフトを使い、エディオンの営業秘密に当たる4件のデータを不正に入手したとして逮捕された。	退職者	転職先で役立てたかった

▲内部者による情報漏えいの主な原因
- 処遇への不満等の動機
- 機密情報へのアクセス権限の悪用
- 監視体制が不十分

サイバー攻撃別の平均解決日数



■図 3-1-1　サイバー攻撃別の平均解決日数
（出典）Ponemon「2014 Global Report on the Cost of Cyber Crime」「2014 Cost of Cyber Crime Study:Japan」（提供：HP Enterprise Security）※9 を基に IPA が編集

内部不正の防止対策
内部不正防止ガイドライン

①対策の指針、ポイントを理解する
リスクに対する具体的な対策を立案するためのヒントとする

②具体的な実施策を立案する
製品・ソリューションの利用等を検討

組織における内部不正防止ガイドライン → JNSA※内部不正対策ソリューションガイド

【目次】
1章 背景
2章 概要
3章 用語の定義と関連する法律
4章 内部不正防止のための管理の在り方
付録Ⅰ 内部不正事例集
付録Ⅱ チェックシート
付録Ⅲ Q&A集
付録Ⅳ 他のガイドライン等との関係
付録Ⅴ 基本方針の記述例
付録Ⅵ 基本5原則と25分類の対策例
付録Ⅶ 対策の分類

2013年3月初版、2015年3月第3版

製品・ソリューション
掲載企業数：16社
掲載製品数：156品
（2014年8月現在）

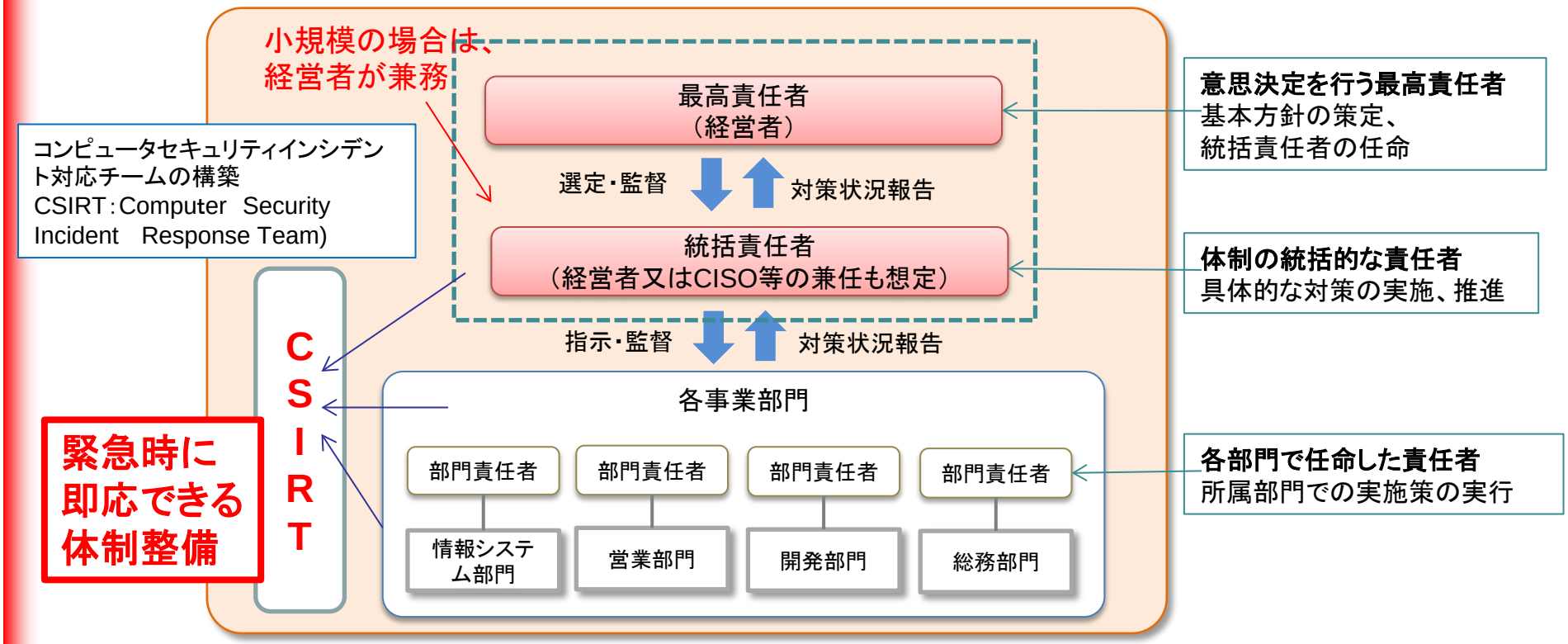
JNSAソリューションガイド（オンライン版）
内部不正防止・抑止サービス

ガイドラインの各対策を実現するための製品やサービスをまとめたソリューションガイド。30の対策項目にマッピング。

※JNSA：特定非営利活動法 人日本ネットワークセキュリティ協会

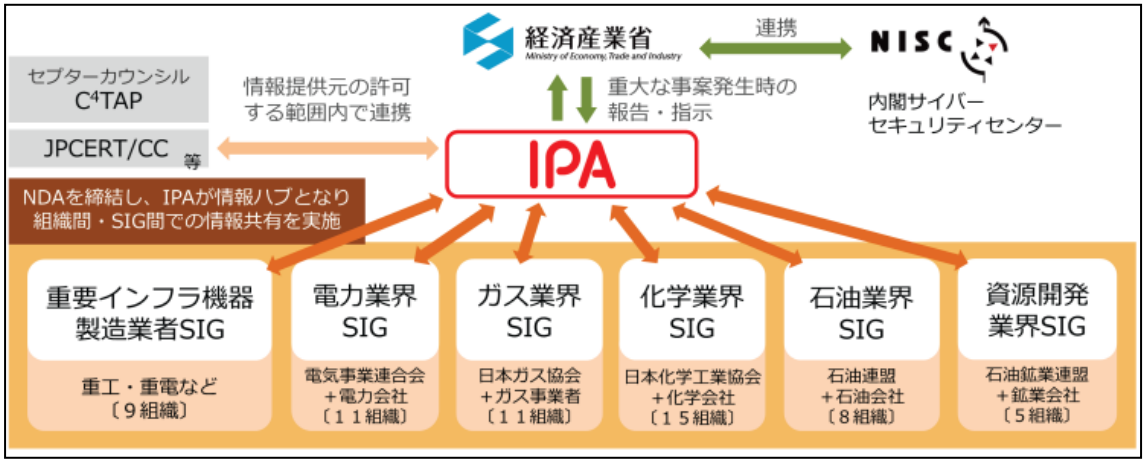
トップの関与による組織体制とダイナミックなインシデント対応が必要

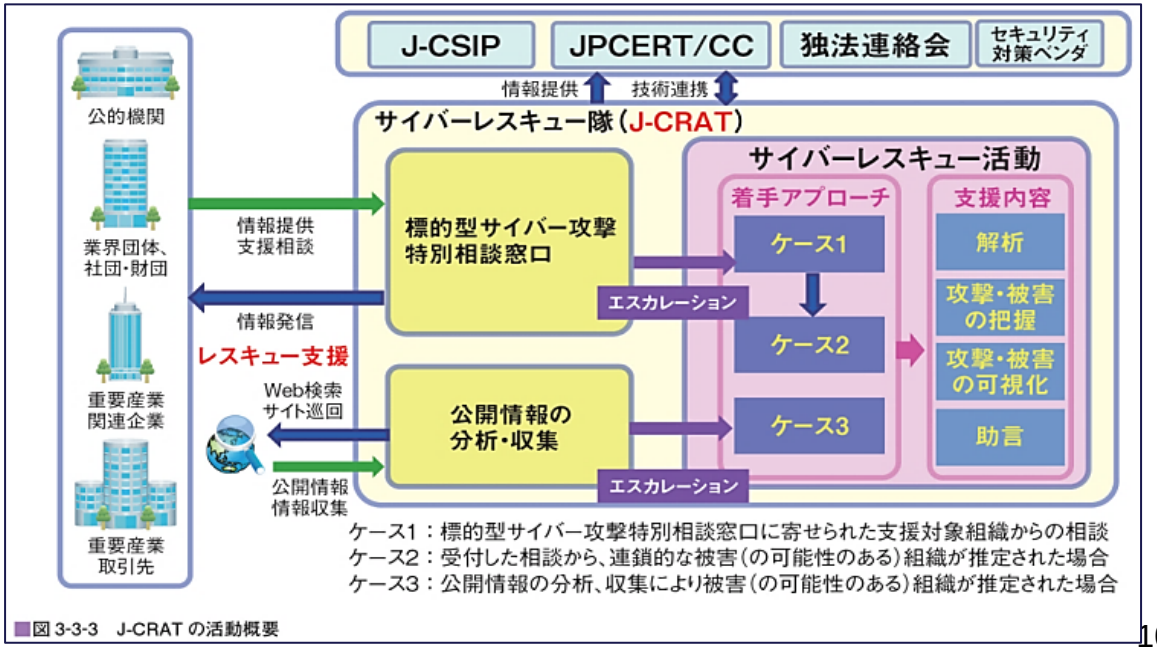
- 経営者による意思決定が会社全体に伝わり、実施状況が把握できる管理体制を構築（企業の規模により体制は柔軟に検討する）
- 緊急時に即応できる体制（CSIRT)を整備



IPAの取り組み
～情報共有（J-CSIP）とインシデント対応（J-CRAT）～

- **J-CSIP**
  - -2011年10月25日発足、2012年4月重要インフラ機器SIG（Special Interest Group）を開始し、2015年5月時点、6SIG・参加組織59からなる
  - **-IPAに報告された累計1257件のうち共有数535件、標的型攻撃は989件（2014年度末現在）**
- **J-CRAT**
  - -サイバーレスキュー隊
  - 2014年7月発足。
  - -公共性の高い機関・組織等への攻撃に対してオンサイトでの緊急支援を実施。





■図 3-3-3　J-CRAT の活動概要

議題6　今後の運営について

【今後の活動】

○ 来年春頃 第2回の実会合を開催。

○ 実会合とは別に、参加団体の会員企業等を対象として、研修（サイバー、人事・労務、有事対応、などがテーマ案）やメールマガジンの配信等も検討。具体的内容や参加方法等については別途ご相談。

【体制・役割分担】

○ 今後の活動については、

幹事：JIPA　　事務局：IPA

の体制で任意団体「官民フォーラム」として実施。経産省をはじめ行政は全面的に活動をバックアップ。

営業秘密官民フォーラムについて

ご清聴、ありがとうございました。

世界から期待され、世界をリードするJIPA
Creating IP Vision for the World