「重要な秘密」保護ガバナンス・マネジメントチェックリスト開発
～経過報告～

株式会社NTTデータ経営研究所エグゼクティブスペシャリスト　三笠武則
（営業秘密保護推進研究会 事務局長）

2023年10月23日

APPTraS

取組みの概要

APPTraS
営業秘密保護推進研究会

■「重要な秘密」に対する企業の「秘密情報漏えい／内部不正防止管理」の実効性を高めるためには、各社様の役職員１人ひとりが**リスク（外からの脅威や内在するぜい弱性の深刻さ、影響の大きさ等）をきちんと認識し、危機感を共有**していることが重要。

■ チェックリストは上記を実現するために：
- ✓ 構築したガバナンスとマネジメントが現在どの程度成熟しているかを
- ✓ ツールを用いて診断することで
- ✓ 各社様が自らの課題を認識し
- ✓ その改善に効果的に取り組むことを

目的として開発している。

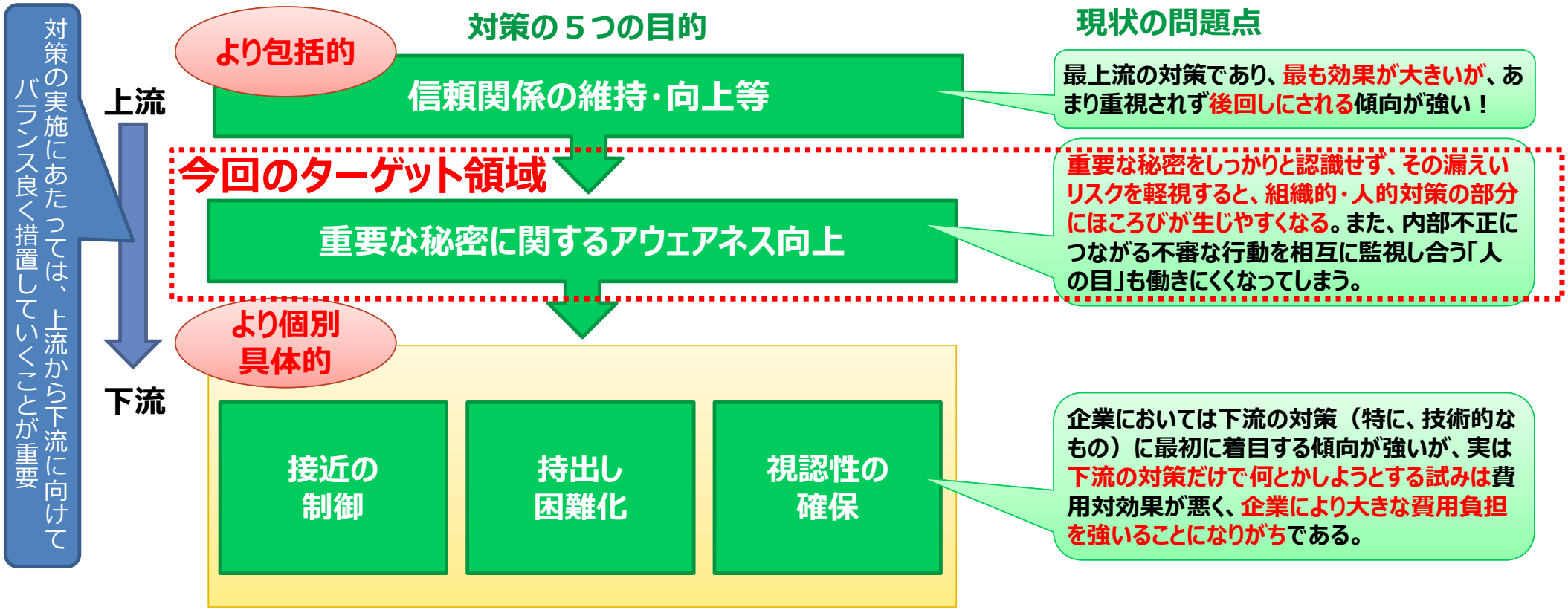
■ チェック項目の作成にあたっては、毎年の改善（PDCA）を促すためのモニタリング指標の数値化を目指す。

※但し、これらのモニタリング指標が、経営指標としてのKPIに直結しない場合もある。

チェックリストの開発目標（１）　～アウェアネスとリテラシーを向上させる～

APPTraS 営業秘密保護推進研究会

■ 今回、「重要な秘密に関するアウェアネス」を役職員１人ひとりに浸透させるためのチェックリストを目指す。
■ チェックリストに回答し、集計することで、上記の進展状況を定量的にモニタリングできるようにする。

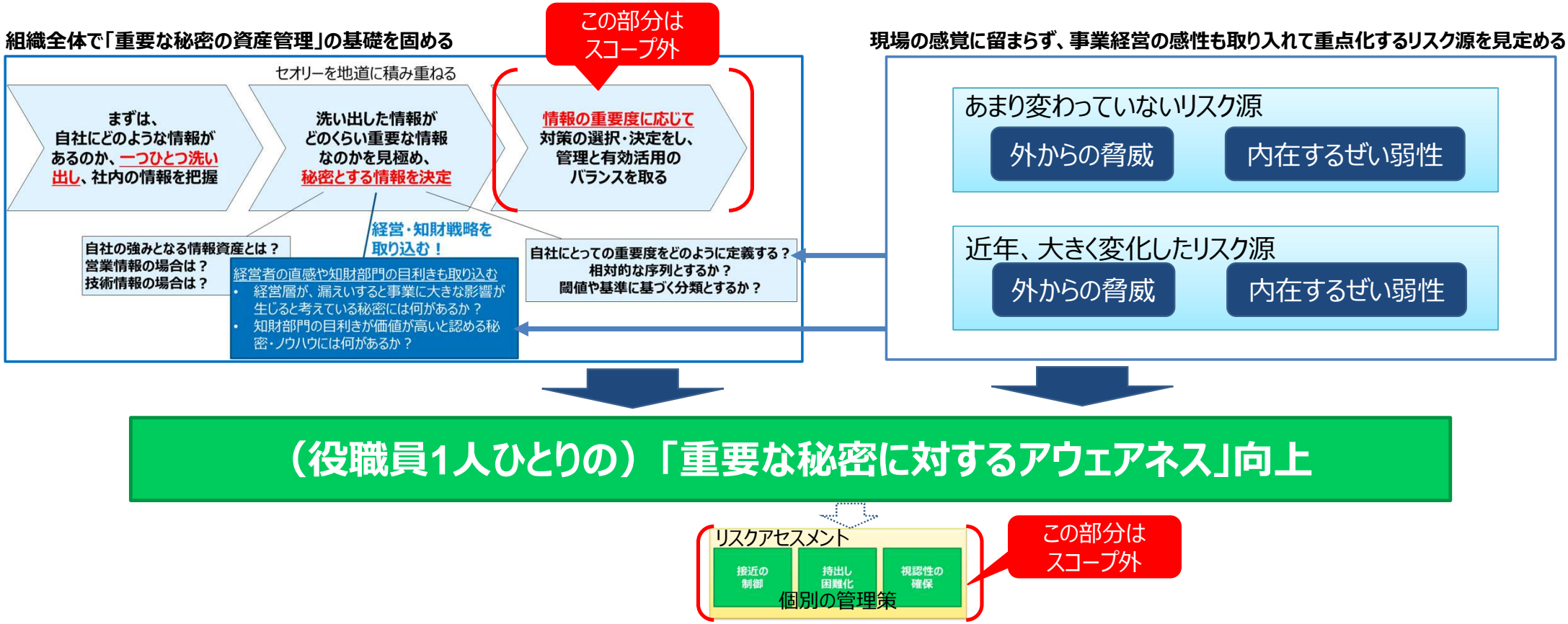


チェックリストの開発目標（２）　～アウェアネスを高める対象を見定める～

APPTraS 営業秘密保護推進研究会

「重要な秘密に関するアウェアネス」を役職員1人ひとりに浸透させるため：

1. 「重要な秘密の資産管理」の基礎固めを促し、こうして管理された資産に関する役職員のアウェアネスを高めることに貢献する。
2. 経営層の感性も取り入れて事業に大きな影響を与えうるリスク源に焦点を絞り、これに対する役職員のアウェアネスを高めることに貢献する。



チェックリストの開発目標（３）　～ガバナンスとマネジメントを充実させる～

APPTraS 営業秘密保護推進研究会

「重要な秘密に関するアウェアネス」を役職員１人ひとりに浸透させるため：

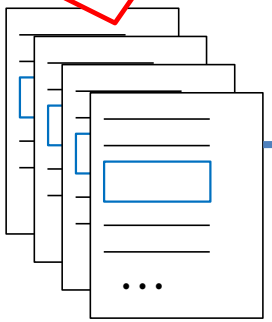
■ 経営層が事業に大きな影響を及ぼしうる「重要な秘密」と「重大なリスク」を認識し、役職員１人ひとりにこれらについての「アウェアネス」を定着させるべく、経営層を頂点としたガバナンスの構築に努めているか、その到達レベルを分かりやすく評価できるようにする。

■ 「重要な秘密の資産管理」「重点的に対処するリスク源の選択」等の、「アウェアネス」の浸透に不可欠な基盤を管理するとともに、現場で発生する「ヒヤリハット」等が管理者層を通じて経営層にスムーズにエスカレーションされるべく、必要なマネジメントシステムの構築に努めているか、その到達レベルを分かりやすく評価できるようにする。

チェックリストの利用イメージ（当初の設計）

社内／各部署の現状調査結果に基づき、ガバナンスチェックリストとマネジメントチェックリストの各成熟度の設問に〇か×で回答する。すべての設問の回答が〇になった成熟度は「達成された」と評価し、次の成熟度を目指す。
（「設問に〇か×で回答するのは難しい」というご意見があり、枠組みの変更を検討中）

チェックリストに同梱されたワークシートを用いて社内や各部署の現状を調査・集計し、その結果に基づいて設問に〇 or ×で回答



ガバナンスチェックリスト（イメージ）

＜成熟度１＞（短期対応）	
１．経営層による重要な秘密の認識	〇
２．経営層による重要な秘密の定義と特定の指示（中長期戦略）	〇
３．知財・無形資産ガバナンス構築への経営層の取組み	×
＜成熟度２＞	
1. 各部署で重要な秘密をすべて挙げられるか	〇
2. 重要な秘密漏えい時の事業損失に関する各部署内の共通認識の現状	×
3. 重要な秘密のオーナーが全て特定できるか	×
＜成熟度３＞	
1. 他部署の重要な秘密を識別できるか	×
2. 識別に関する情報の他部署との共有	×
3. リテラシー構築による、重要な秘密漏えいに関するリスク認識の全社での共有	×
4. 事案に応じた行うべき初動対応の理解に加え、警察への相談、民事的措置等を行う基準と体制の整備	×

マネジメントチェックリスト（イメージ）

＜成熟度１＞（合格） 自社で取り扱う重要な秘密の種別の特定	〇
＜成熟度２＞（合格） ■ 重要な秘密を取扱う業務とプロセスの特定	〇
■ 従業員の誰にでも分かる重要な秘密のラベリングと、業務プロセス毎の、共有可能範囲の厳格な管理	〇
＜成熟度３＞	
■ 重要な秘密保護のため対応するリスク選択	×
■ 重要な秘密の共有可否プロセスの構築と部署を超えた調整の仕組み	〇
■ リスク低減対策や事後対応のトリアージ（法的措置の選択等）の実効性の測定と管理職による管理	×
＜成熟度４＞ リスク低減対策の実効性を経営層に報告する体制の構築	×

【評価結果】
次に目指すべき成熟度

ガバナンス	1
マネジメント	3

（参考）ガバナンスチェックリストの初期案　※現在、改善を検討中

営業秘密保護推進研究会

重要な秘密の漏えい

成熟度レベル	設問	回答
1	１．経営層は、社外への漏えいや、社外からの意図しない混入によって、「事業経営に重大な影響を及ぼす秘密」（以後、「重要な秘密」を認識していますか。	
	２．経営層は、社内の各部署において「重要な秘密」を特定できるように、必要な定義、識別基準等を周知徹底するとともに、これらに基づいて「重要な秘密」の特定を行うことを全社に指示していますか。	
	３．経営層は、知財・無形資産ガバナンスの構築に積極的に取り組んでおり、知的財産権や重要ノウハウ（経営ノウハウ、事業・ビジネスノウハウ、技術ノウハウ、データを含む情報財等）を全社で掌握して戦略的な活用に投資するとともに、その取組を投資家・金融機関に情報開示して資金を集め、中長期に亘って企業の成長を維持し続けることに取り組んでいますか。	
2 部署毎	１．各部署内で生み出された「重要な秘密」（文書やファイルとして作成・管理されている形式知、特定個人の頭の中にある暗黙知）を、全て提示することができますか。	
	２．各部署の全体に亘り、「重要な秘密」が社外に漏えいしたら、自社の事業に大きな損失を生じ、事業経営に重大な影響を及ぼしてしまうという共通のリスク認識が共有されていますか。	
	３．各部署内で生み出された「重要な秘密」の「所有者」（作成者、管理責任者、保有者等）が誰かを全て特定できますか。	
3 全社での連携等	１．各部署内の全員が、他部署が所有する「重要な秘密」を、「重要な秘密」であると識別できますか。	
	２．各部署が所有する「重要な秘密」を識別するための情報を、他部署と広く共有していますか。	
	３．組織全体のリテラシー教育・訓練によって、「重要な秘密」の社外漏えいリスクの重大さに関する共通認識を、全社で構築・共有できていますか。	
	４．「重要な秘密」が社外漏えいした際に、事案の特徴に応じた初動対応を実行できる体制がありますか（CSIRTなど）。 さらには、事後対応として、警察への相談、民事的措置等を行うための判断基準と、これを実施できる体制を整備していますか。	

他社の重要な秘密の侵害

成熟度レベル	設問	回答
1	１．経営層は、社外への漏えいや、社外からの意図しない混入によって、「事業経営に重大な影響を及ぼす秘密」（以後、「重要な秘密」を認識していますか。	
	２．経営層は、社内の各部署において「重要な秘密」を特定できるように、必要な定義、識別基準等を周知徹底するとともに、これらに基づいて「重要な秘密」の特定を行うことを全社に指示していますか。	
	３．経営層は、知財・無形資産ガバナンスの構築に積極的に取り組んでおり、知的財産権や重要ノウハウ（経営ノウハウ、事業・ビジネスノウハウ、技術ノウハウ、データを含む情報財等）を全社で掌握して戦略的な活用に投資するとともに、その取組を投資家・金融機関に情報開示して資金を集め、中長期に亘って企業の成長を維持し続けることに取り組んでいますか。	
	４．他社から受領する「重要な秘密」を可能な限り制限し、最小限に止めるための規則を制定し、運用していますか。	
	５．やむをえず他社の「重要な秘密」を受領した時は、その経緯や日時や誰から受領したかを記録し、保管することを義務付けていますか。	
2 部署毎	１．各部署内にある「重要な秘密」の「所有者」（作成者、管理責任者、保有者等）が誰かを全て特定できますか。	
	２．各部署内にある、他社から受領した「重要な秘密」を全て特定できますか。また、他社から受領した「重要な秘密」に対しても、「所有者」を決めて管理していますか。	
3 全社での連携等	１．各部署内で所有する、他社から受領した「重要な秘密」を識別するための情報を、他部署と広く共有していますか。	
	２．組織全体のリテラシー教育・訓練によって、他社から受領した「重要な秘密」の侵害リスクの重大さに関する共通認識を、全社で構築・共有できていますか。	
	３．他社から受領した「重要な秘密」の侵害を指摘されて紛争が生じた際に、事案の特徴に応じた初動対応を実行できる体制がありますか（知財・法務部門など）。 さらには、事後対応として、他社との紛争を解決するための体制を整備していますか。	

（参考）マネジメントチェックリストの初期案　※現在、改善を検討中

APPTraS 営業秘密保護推進研究会

重要な秘密の漏えい

成熟度レベル	設問	回答
1 各部署の管理責任者による基礎的管理	１．各部署における「重要な秘密」の管理責任者は、取り扱う情報の種別（個人情報、その他の営業情報、技術情報、重要ノウハウ（経営ノウハウ、事業・ビジネスノウハウ、技術ノウハウ、データを含む情報財等））を知っており、各種別のリスク管理上の特質に従って管理していますか。	
2 「重要な秘密」を取り扱う業務・プロセス及び秘密共有範囲の特定と情報共有	１．各部署における「重要な秘密」の管理責任者は、従業員の誰にでも分かる「重要な秘密」のラベリングを指示・徹底していますか。	
	２．各部署における「重要な秘密」の管理責任者は、情報の種別ごとに、「重要な秘密」を取り扱う業務とその業務プロセスを特定していますか。	
	３．各部署における「重要な秘密」の管理責任者は、業務プロセスに基づいて「重要な秘密」を共有できる範囲を指示・管理するとともに、当該秘密の共有範囲の情報を他部署と広く共有していますか。	
3 リスクへの対応、組織間連携等	１．各部署または組織全体として、「重要な秘密」の窃取に係るリスク源のうち、どれに対応しますか。	
	２．「重要な秘密」を他部署の要員に共有しても大丈夫なのかが判別しにくい場合に、部署を超えて、当該秘密の「所有者」と調整を行う業務プロセスをルール化し、順守していますか。	
	３．リスクを低減するための対策や、法的措置の選択（事後対応におけるトリアージに相当）の実効性を測定し、管理職がきちんと管理していますか。	
4 経営層への報告体制	１．リスク低減のために実施した対策や法的措置の実効性等について、現状を経営層に報告する体制が構築されていますか。	

他社の重要な秘密の侵害

成熟度レベル	設問	回答
1 各部署の管理責任者による基礎的管理	１．各部署における、他社から受領した「重要な秘密」の管理責任者は、当該秘密を受領した経緯、日時、誰から受領したか等の記録を漏れなく管理し、いつでも最新情報にアクセスできるようにしていますか。	
2 「重要な秘密」を取り扱う業務・プロセス及び秘密共有範囲の特定と情報共有	１．各部署における「重要な秘密」の管理責任者は、自社が生み出した「重要な秘密」が自社オリジナルであることを証明する記録・証跡※を管理していますか。 ※作成者、作成の経緯等の記録（実験ノート等）、タイムスタンプ追加による作成時刻の証跡等	
	２．各部署における、他社から受領した「重要な秘密」の管理責任者は、他社から受領した「重要な秘密」に、従業員の誰にでも分かるラベリングを行い、自社情報と分離保管することを指示・徹底していますか。また、当該秘密を受領した経緯を必ず記録するとともに、当該秘密の開示範囲を指示・管理し、開示範囲の情報を他部署と広く共有していますか。	
3 リスクへの対応、組織間連携等	１．他社の「重要な秘密」の侵害リスクに対応するため、どのリスク源に対応しますか。	
	２．他社の「重要な秘密」の侵害リスクを低減するための対策や、他社との紛争解決手法の実効性を測定し、管理職がきちんと管理していますか。	
4 経営層への報告体制	１．リスク低減のために実施した対策や他社との紛争解決手法の実効性等について、現状を経営層に報告する体制が構築されていますか。	

（参考）考慮しているリスク

APPTraS 営業秘密保護推進研究会

- リスク源を「あまり変わっていないもの」と「近年、大きく変化したもの」に大別している。
- さらに、外部から来る「脅威」と内在する「ぜい弱性」に分けて整理している。

【あまり変わっていないリスク源】

外からの脅威

- 産業スパイ
- ターゲット組織要員のハンティング
- 脅迫
- サプライヤー／バイヤーのトラッピング
- トラッピング目的の共同研究／開発
- 役職員の不注意・ミス

内在するぜい弱性

組織的ぜい弱性
- 各種管理の不備・不徹底
- 採用時評価の不備

技術的ぜい弱性
- 社内システムの不備
- セキュリティ設定の不備

【近年、大きく変化したリスク源】

外からの脅威

- 外国政府による日本の技術情報を対象とする行為の脅威が増大
- 外国人採用（中途、インターンシップを含む）による海外組織からの脅威の増大
- 他社からの提訴（目的：不正競争是正 or 嫌がらせ）の増加
- 役員やシステム関係者のハンティング
- システム関係の委託先要員のハンティング
- 個人の弱みをネタにする脅迫
- 転職によるステップアップに役立てるための秘密持ち出し増加　等

内在するぜい弱性

組織的ぜい弱性
- 海外拠点管理不徹底
- 雇用の流動化、兼業の緩和
- リモートワーカーの急増
- 他社との紛争への準備不足　等

技術的ぜい弱性
- クラウド利用の拡大
- BYODの拡大
- 見える化が不十分なリモートワーク環境　等

レビュー及び検討の実施体制

本取り組みは、民間企業、有識者及び学識経験者のご協力を得て実施しています。
検討会を３回開催して議論することで、成果の質を高めるとともに、民間企業の実務に直結した内容とすることを目指しています。

本取り組みの事務局

弊研究会事務局委員2名
＋
関連実務経験が豊富な民間企業の支援者2名

民間企業の有志

（非公表）

有識者・学識経験者アドバイザー：6名

公的機関、弁護士、大学教授、セキュリティベンダー、コンサルタント

検討会 3回開催予定
（構成員・オブザーバーは今後公開する予定）

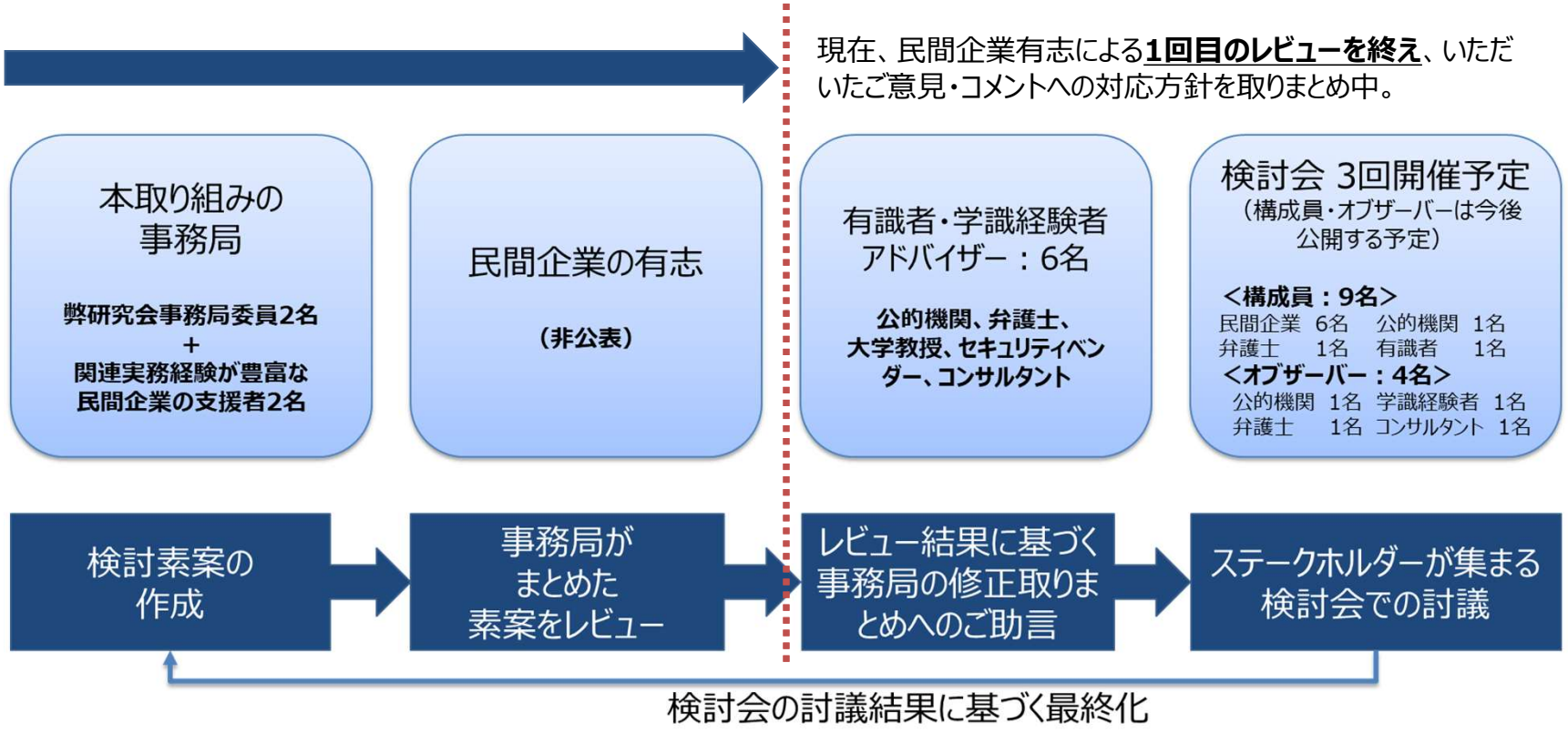
＜構成員：9名＞
民間企業　6名　公的機関　1名
弁護士　1名　有識者　1名
＜オブザーバー：4名＞
公的機関　1名　学識経験者　1名
弁護士　1名　コンサルタント　1名

検討素案の作成 → 事務局がまとめた素案をレビュー → レビュー結果に基づく事務局の修正取りまとめへのご助言 → ステークホルダーが集まる検討会での討議

検討会の討議結果に基づく最終化

現在の進捗状況

- 民間企業有志による1回目レビューは完了。チェックリストの枠組みに関するご意見や、実務を踏まえた改善点などの貴重なご指摘を多数いただいた。
- いただいたご意見／ご指摘にていねいに対応していること、チェックリストの構造変更を見込んでいること等を考慮すると、検討期間の見直しが必要になる見込み。



主たるご意見・ご指摘（１）　～第1回レビュー結果より～

APPTraS 営業秘密保護推進研究会

【チェックリスト開発の目的について】

（ご意見）チェック項目作成にあたっては、社内の体制整備の指標となる数値目標や具体的な内容があることが望ましい。（企業組織全体における秘密管理活動において、定量的な管理を行うためのKPIとして使えるようなものを希望する）

（対応方針）「重要な秘密に対するアウェアネス」向上に関する毎年の改善（PDCA）を促すためのモニタリング指標を数値化できるようにする。他方で、これが経営指標としてのKPIに直結するとは限らないと考えている。

【チェックリストの想定利用者】

（ご意見・ご指摘）

- 想定利用者の例には、可能性のある部門・担当部署の名称を網羅的に記入する方が良い。役職レベルまでの言及は不要と考える。
- 全社のガバナンスのなかで事業部単位への権限委譲を含めて統制を実施している場合もあるため、想定利用者の例示に（コーポレート全体としてのリスク管理部長、総務部長のほかに）各業務体の事業部長を加えてもらえると、よりフィットする。また、情報を扱う部署も例示する方が良い。
- 社内規程や、毎年の自己点検に供するチェック基準を作成する部門の基準レビューにも活用できる。

（対応方針）

- 「ぜひ読んで欲しい利用者」に絞って例示する。
- 部門名等は企業規模によって変わること、事業所やグループ企業でも当てはめられるようにすること等を念頭に、「担っている役割・機能や責任」による例示に変更する。

主たるご意見・ご指摘（２）　～第1回レビュー結果より～

APPTraS 営業秘密保護推進研究会

【対象とする秘密の定義】

（ご意見）「重要な秘密」の特定に際して、その利活用の確保の観点も記載して欲しい。重要であるほどその秘密は通常の企業活動や研究開発で使われるので、短絡的に厳しいアクセス制限を課してしまうと企業活動のオペレーションを阻害してしまう。重要な秘密としての保護と企業活動の円滑な実施のバランスを考慮した上で、「重要な秘密」と特定することが必要と考える。

（対応方針）本チェックリストは、「重要な秘密に対するアウェアネス」向上をスコープとする。リスクアセスメントや個々の管理策の適用については、場を改めて議論させていただく方針。上でいただいたご指摘は「重要な秘密」の具体的な管理や取扱いに関するものと理解できるので、場を改めて検討すべき事項と整理した。

（ご意見・ご指摘）

■ 現行案では全編に亘って、「他社にとっての重要な秘密を漏洩しない」という観点と「自社にとっての重要な情報に対し他社秘密の流用であるとの嫌疑をかけられない（いわゆるコンタミリスク）」という観点の両方が含まれているのか、あるいは片方しか含まれていないのかが明確ではない書き方になっている。両者の概念、認識は分けて記載すべき。

（対応方針）

■ ご指摘の通り、現在の書き方は明確ではない。さらには、「他社にとっての重要な秘密を漏洩しない」という観点では、考慮すべきシーンを共同研究・開発に限定せず、業務提携全般に広げるべきとのご意見もいただいている。

■ 本チェックリストが「重要な秘密に対するアウェアネス」向上をスコープとしていることを考慮し、本チェックリストでは**ベースラインとして、「他社の秘密を自社の情報と分離できること」がきちんと確保されているか、あるいはこれを確保することの必要性をきちんと理解できているかというところまでをカバーすれば良い**と整理した。換言すれば、様々な業務提携形態ごとに設問を区別して書くことはしない。

主たるご意見・ご指摘（３）　～第1回レビュー結果より～

APPTraS
営業秘密保護推進研究会

【チェックリストの構造について】

（ご意見）

- 設問がYes/Noで答える形式であるため、未実施の内容がわかりやすく良いと思うが、設問数が多くなる傾向にある。また、YesかNoかの判別が微妙な状況であることも想定される。５段階評価で回答する形式の可能性も検討してはどうか。成熟度別に設問を分ける必要がなく、設問数を減らすことができ、YesかNoかの二者択一では回答しにくい場合にも対応できる。
- 成熟度１～３に書かれている内容全てを全て必要な要件とし、「成熟度①無い」→「②有る」→「③指標化されている」→「④指標に沿って問題が把握されている」→「⑤是正される仕組みが整っている」という方向で、成熟度合いをはかるという考え方もあるのではないか（ガバナンス、マネジメントの両方に共通）

（対応方針）

- 設問への回答（現在の到達レベル）を5段階から選択できるように変える。どの段階にあるかを判断する基準やエビデンスを提示することを検討する。
- 5段階のレベル設定例として以下を想定することができるが、これに拘らない。
  （例）「方針あり」→「責任組織／責任者あり」→「組織的な統制／マネジメントあり」→「各部署のリテラシー底上げを実現」→「全社戦略的な活用を実践」
- 現在は成熟度ごとに設問が用意されているが、この構造の変更を検討する。成熟度（到達度）を確認すべき項目をカテゴリーに分け、各カテゴリーの確認項目ごとに設問を設け、これに対する到達度を5段階で回答していただく建付けを検討する。こうすることで、カテゴリーごとに各社のレベルアップのストーリーを具体化することができるようになる。

主たるご意見・ご指摘（４）　～第1回レビュー結果より～

APPTraS 営業秘密保護推進研究会

【ガバナンスチェックリスト：成熟度２】

（ご意見）「重要な秘密の所有者を全て特定」できるかは、「重要な秘密」の定義次第と言える。技術的な営業秘密には対応できるが、その他の経営的なノウハウなどはリスト化が難しく、「全て」と言われると厳しい（本当にそれができるのであれば、成熟度３のレベルだと思われる。）。

（対応方針）

- ノウハウであっても形式知として文書化されていればリスト化は可能。しっかり形式知化することが重要。設問や評価基準等でこの示唆を伝えることを検討する。
- 「重要なノウハウ」については資料化した上で、その資料を管理する責任者を決める（そのノウハウについて知りたければ●●さんに聞けばよいというような状況を作る）ことの有効性と実現性を検討する。

【ガバナンスチェックリスト：成熟度３】

（ご意見・ご指摘）

「重要な秘密保護に関する組織としての役割」の項目を追加してはどうか。態勢として、経営層の関与とともに、1線・2線・3線のリスク管理体制・ガバナンス構築が求められると想定する。この観点から、チェック対象を[1線：現業部門向け]、[2線：リスク管理部門向け]、[3線：内部監査部門向け]に分けてみてはどうか。なお、3線（内部監査部門）は1線、2線がルールに従い、実行できているかを牽制する目的で監査を行う役割なので、チェック対象から外してもよいと考える。

設問例）重要な秘密保護に関する、リスク管理部門の役割（規程類等のルールを制定する部署）、各現業部門の役割を整理のうえ、各関連部署がその役割（責任）を有しているか。また内部監査部門が、重要な秘密保護に関する内部監査を役割（責任）として有しているか。

（対応方針）

- 今回のチェックリストはリテラシーとして全社で同じ認識や理解を共有しているかを確認することに重点を置いている。この設計意図は変えない方向。
- 従って、「組織ごとの役割に応じてこれをやるべき」という評価はしない方針である。当面は、設問への回答にあたり、到達レベル選択の基準として、「主要部署が自分の役割を果たしていること」を考慮することにとどめる。

主たるご意見・ご指摘（５）　～第1回レビュー結果より～

APPTraS 営業秘密保護推進研究会

【ガバナンスチェックリスト：成熟度３】

（ご意見）「警察への相談、民事的措置等を行うための判断基準」は事前に必要か。あってもよいが、それほど頻繁にあることではないし、定めたとしても結局ケースバイケースで判断せざるを得ないのではないか。（事前に定めた基準に従うかどうかを個別判断することになりそうな気がする。）

（対応方針）

■ ご指摘のとおり、事案ごとの個別対応にならざるを得ない。他方で、将来的に法的措置が採られ得るという点を意識しておくことは有益。秘密漏洩等が起こったときは緊急時であることが多く、事実調査や更なる漏洩の防止、法的措置の点も含め迅速に動けるようにあらかじめチーム編成や基本的な進め方を考えておくことが必要であり、これを求める方向で検討する。

【マネジメントチェックリスト：成熟度１など】

（ご意見・ご指摘）

■ 他社資料の取得経緯を記録・保管していたとしても、「他社から受領した重要な秘密」という情報分類がない限り、（物量が多すぎて）秘密情報そのものを分けることは困難。

■ 他社の秘密の重要性の評価が難しいと感じた。他社との秘密情報契約においても、どの程度重要なのかは不明である。

（対応方針）

■ ベースラインとして、他社からもらった秘密にもラベルを付けることができれていればよい。秘密の重要度を示すラベルは必ずしも必要ではなく、他社の秘密であることを示すラベルで良い。内容は見なくても、ラベルを見るだけで重要そうとピンと来るようであればとても望ましい。

■ また、他社からもらった秘密にも管理責任者を割り当て、社内で問い合わせれば管理責任者が特定できるようにすることを求めていく。

主たるご意見・ご指摘（６）　～第1回レビュー結果より～

APPTraS 営業秘密保護推進研究会

【リスク源について】

（ご意見）地政学的なリスク（中国にある子会社に中国政府から情報を出すように言われてしまう、サーバーごと没収されてしまうなど）、法律法規の改正リスク（法律が変わってしまい、コンプライアンスに支障をきたす：例えば個人データ漏えい時の報告義務など、不競法でもこうした観点はありうるか？）も追記すべき。

（対応方針）下記のとおり、今回は大企業向けに焦点を絞ることとしている。このため、海外関係国の法制を調べ、モニタリングすることの必要性を問うことを検討する。

【その他】

（ご意見）できれば、企業の規模感に応じてどの程度の成熟度を目指すべきか、それを達成するために組織構造をどのようにすべきか等の指針・指標的なものもあるとありがたい。

（対応方針）大企業向けと中小企業向けでは、一定程度の書き分けが必要と考えている。今回の検討では一旦大企業向けに焦点を絞ることとし、中小企業向けのチェックリストは機会を改めて検討することにしたい。

（ご意見）

- リスクを特定した後、特定したリスクに対して取るべきアクションまでが分かるツールであると使いやすいと感じた。
- リスク源への対策を網羅的に実施することが難しい場合を想定し、各リスク源に対して、漏えいした場合の自社への影響（リスク）を評価するモデルを整理してはどうか。　※（モデルの要件）　- 自社への影響として、金銭的被害、事業継続への影響等、いくつかのパターンが整理できること　- 秘密とするノウハウ種別ごとに、個々のリスク源に伴う漏えいによる自社への影響の過多を評価することを通じて、どのリスク源への対応を強化すべきかを特定できること

（対応方針）

- 「重要な秘密に関するアウェアネス向上」というリテラシー面に焦点を当て、個別の対策は次のステップと割り切ることで、次のステップを担うコンサルタントとの役割分担が明確になるはず。他方で、「自社への影響（リスク）を評価するモデル」の考え方は、設問に対する評価基準にも繋がるものであり、前向きに検討する。

今後の予定

民間企業有志からの貴重なご意見／ご指摘にしっかりと対応するため、検討期間が延びることを恐れず、質にこだわってチェックリスト等の修正に取り組みたいと考えている。

1. いただいたご意見／ご指摘を踏まえたチェックリストの修正が、枠組みの変更を含むかなり大幅なものとなる見込みであるため、**検討会で議論する前に、もう一度民間企業有志にレビューをお願いする**ことを検討している。

2. これと**並行して、弁護士・有識者・学識経験者・公的機関からなるアドバイザーに諮り、助言を集約**する予定。

3. 上記を前提に、**チェックリスト開発の全体工程を見直し**、その結果を本取組の関係者に改めて展開する予定。

この資料についてのお問合せ先

この資料で紹介した弊研究会の新しい取り組みへのご関心、ご質問、ご協力希望、その他のお問い合わせ等については、下記連絡先までお願いします。お気軽にご連絡ください。

弊研究会では、「重要な秘密」保護ガバナンス・マネジメントチェックリスト開発にご協力下さる民間企業の方を、引き続き募集しています。

【お問い合わせ先】

株式会社NTTデータ経営研究所　エグゼクティブスペシャリスト　三笠武則（みかさたけのり）
（営業秘密保護推進研究会 事務局長）

E-mail: mikasat@nttdata-strategy.com　　TEL: 090-1459-0597