明日できる秘密情報管理と漏えい対策

～既存の社内ITシステムを駆使して即時実行可能な防衛策～

制作／Business & Law 編集部

営業秘密、技術情報から知財まで、情報資産保全（セキュリティ）の重要性がDX／IT化の流れに乗り加速度的に高まる中、CGコードや「知財・無形資産ガバナンスガイドライン」が改訂（それぞれ2021年、2023年）され上場企業を対象とした知財に関する取組み・経営戦略および知財投資の重要性にかかる具体的な情報の開示・提供が求められることとなった。広く無形資産を源泉とする日本の国際競争力の復権に向け、国が推進する技術情報漏えい対策の概況（マクロ）と、日本企業が当該資産の管理・利活用を促進する手近なツールとして、既に広範に採用されているMicrosoft 365の諸機能（ミクロ）を駆使することの有用性について、二人の有識者にポイントを整理いただいた。

Ⅰ 国が推進する五つの技術情報漏えい対策（萩原弘之弁護士）

1．営業秘密等の侵害の現状

営業秘密の侵害事案は10年以上にわたり増加傾向にあり、刑事事件化した件数も4年連続で過去最高を更新しています。しかし、当事者が被害の全容を把握できたのは毎年10％程度に留まります。被害により、競争力（顧客）が奪われ、風評リスクに晒されるばかりでなく、被害立証が困難となると司法救済の道も閉ざされます。また、特許権（知財）侵害の放置による損失についても、能動的な侵害調査を怠れば深刻な権利毀損につながりかねないことはご承知のとおりです。

2．国が推進する五つの漏えい対策

このような現状を受け、国（警察庁）は日本企業に五つの漏えい対策、すなわち、秘密情報に対して、

①**近寄りにくくする（接近の制御）**

②**持出しを困難にする（困難化）**

③**漏えいが見つかりやすい環境づくり（視認性確保）**

④**「秘密情報と思わなかった」事態を招かないための対策（秘密保持に対する意識向上）**

⑤**社員のやる気を高める対策（信頼関係の維持・向上）**

を提唱しています。①②は物理的・技術的防御、③④は心理的防御、⑤は全社的なコンプライアンス対策に該当します。加えて、経産省にて、上記①～⑤の各項目に対応して従業員、退職者、取引先、外部者それぞれに向けた実践的なセキュリティ対策が具体化されています。

3．情報資産保全のための組織最適化の方策

まず、無形資産の適切な管理・投資を行うプロフェッショナルとして、関係部門が組織・連携立てコンプライアンスの一環として実施するべきこと。続けて、社内の管理体制（ルール）を形骸化させず、Ⅱで後述するITツールも含めて積極的に運用し、裁判でも勝てる仕組みづくりを行うこと。退職者に課す競業避止義務の有効性等にかかる裁判例をウォッチし、適法な管理体制のアップデートを続けること。さらに、〝営業秘密〟要件を充足するための漏えい防止・救済措置が十分であるか、外部専門家による監査等を通じ

増田 崇之 Takayuki Masuda
Epiq Systems合同会社
IGプラクティス　シニアコンプライアンス&セキュリティビジネスアナリスト

萩原 弘之 Hiroyuki Hagiwara
ポールヘイスティングス法律事務所・外国法共同事業
パートナー弁護士

て客観的な観点を導入すること。監査事項は多岐にわたりますので、秘密情報の出入り状況の把握や対象従業員の部署異動による秘密情報のコンタミおよびNDA違反等による訴追リスクを効果的に検知することが期待されます。

Ⅱ 明日実行できる秘密情報管理と漏えい対策 ―Microsoft 365を駆使した防衛策―（増田崇之氏）

1．Microsoft Purview Compliance（MPC）とは

既にMicrosoft 365を導入済みの企業も多いと思いますが、改めて復習します。365は、ビジネス・コミュニケーション機能とコンプラ・セキュリティ機能とを包含したサブスクリプション・プラットフォームであり、このうち本日は、365に装備されたコンプライアンス機能であるMPCの各概念・機能について詳説します。

MPCの概念は、セキュリティの考え方から分化・発展したもので、両者は近しいものです。すなわち、外部的脅威から組織を守る従来型のセキュリティに加え、組織内部（内部者同士・内部者と外部者間）での悪意やミスをIT面でどう抑止するか、というコンプライアンス的観点が融合しています。MPCは「情報保護とガバナンス」「内部リスクの管理」「検出と対応」という三つの構成に分類されており、それぞれに対応する機能が図表1のとおり搭載されています。

365の志向する姿は〝モダン・コミュニケーション〟、すなわち、これまで個人のアクセス権を中心として、メール、ファイルサーバー等のデータ保存領域に個別独立して管理されていた状況を統合し、時間軸や役割に応じたアクセス権管理と一体的な運用を行うことにあり、コピーデータの氾濫を防げる点でも有効です。コロナ禍でのハイブリッドワーク普及やITシステムの世代交代（25年の崖）を背景に、日本でも急激な導入が進んでいます。そして、組織面では、欧米や一部の日本企業において、ルール／経営管理とデータ／操作管理の双方を担う部門の登場が注目されています。

図表1 Purview Compliance ラインナップ

情報保護とガバナンス	内部リスクの管理	検出と対応
データライフサイクル管理とレコード管理（DLM & MRM） データ保持・破棄ルール	情報バリア（MIB） 通信に人的境界を作る	監察（Audit） アクションログの取得と調査
データ損失防止（DLP） 外部へのデータ流出の阻止	コミュニケーションコンプライアンス（MCC） コンプラ違反の可能性がある通信をキャッチ	電子情報開示（eDiscovery） ディスカバリ・内部不正調査対応ツール
情報保護（MIP） データの分類、ラベル付け	内部リスクの管理（IRM） コンプラ違反のあるユーザー挙動をキャッチ	

2．国の政策に基づく具体的対応策

MPCに基づく各機能は、Ⅰで説明した「国が推進する五つの漏えい対策」と符合する部分が大きく、ポイントを絞って説明します。

まず、セキュリティの〝一丁目一番地〟であるアクセス権限については、社内ルールに基づく適切な付与・管理のため、特権アクセス権（管理者権限）の適時・適切な管理、（アカウント単位ではなく）役割ベースでの管理、および問題発生時の顧客の明示的承認に基づくベンダーエンジニアの顧客コンテンツへのアクセスを保証します。

次に、漏えい時の水際対策については、対象情報に設定したトリガー（ラベル等）に反応して開示範囲を限定したり、暗号化を即座に実施しつつ無断転送等を禁止したりする機能が作動します。いざ情報漏えい（のおそれ）が生じた段階でも、対象者（ユーザー）のシステム上での言動やアクションを捕獲・捕捉することができます。

さらに、設定した〝文書保持・破棄ポリシー〟に基づき、電子データの性質に応じて保存年限を設定する機能や、不競法上の〝営業秘密〟要件を補強するために秘密管理性を可視化（透かし、ラベル、ヘッダー設定等）する機能、セキュリティの別機能を用いた一部別のセキュリティ機能を用いてデータの遠隔消去を可能にする等、端末上のデータのセキュリティ対策の自在性を高める機能等も有用と考えます。

日本企業の法務や知財部門は、業務の専門性の高さ故に電子文書管理のコーディネートまで手が回らない傾向にありますが、既存のMPCや365のパッケージを用いて、電子文書管理の先進国たる欧米に引けをとらないセキュリティ・コンプライアンス体制づくりを無理なく推進いただけることを期待しています。