Vol.2014-EIP-63 No.7
2014/2/21

営業秘密と情報資産の統合管理に関する考察

渡邉　晴方[†1]　　原田　要之助[†1]

営業秘密の保護と適切な管理は、営業秘密の漏えいが発覚した際の対応を含め、企業・組織が現代社会を生き抜くために、重要性が高いとされている。
しかしながら、営業秘密の適切な管理は行われているとは言い難い現状が有る。
この現状を踏まえ、経済産業省の「営業秘密管理指針（2011.12.1 改訂）に記載されている営業秘密の管理における秘密度に応じた区分と、JIS Q 27002:2006(ISO/IEC 27002:2005)に記載されている情報資産の適切な保護レベルに応じた分類の二つの関係を比較し検討する。更に現状の問題を拾い上げて更なる分析をするために、企業組織に対する情報セキュリティアンケート調査を実施した。

A study of the integrated management of trade secret and asset

HARUKATA WATANABE[†1]　　YONOSUKE HARADA[†2]

The protection of the trade secret and the appropriate management are high in importance for a company and an organization to survive the modern society including correspondence when the leak of the trade secret is found out.
However, the present conditions is hard to say that it is properly managed of the trade secret.
Based on these present conditions、compare with two of the classification that the secret degree in the management of a trade secret listed in a trade secret management guidance (2011.12.1 revision, issued by of Ministry of Economy, Trade and Industry), and the appropriate protection level of information assets listed in JIS Q 27002: 2006(ISO/IEC 27002: 2005), and consider the relation of two.　In addition to this, the information security survey for the company and organization is performed to make clear the present problems and the further consideration with.

1. はじめに

営業秘密の保護は、企業にとって営業秘密の漏洩が発覚した際の対応を含め、重要性の高いことから適切な管理が求められる。
一方で、2009 年 9 月に経済産業省が発表した「営業秘密の管理に関するアンケート調査と裁判例調査の結果分析」aによると、争点となったケースの中で、裁判所に最も多く否定されているのは、物理的管理 bにおける「アクセス権者の特定」であり、次に「情報の秘密区分の表示」であるとされており、営業秘密の適切な管理は行われているとは言い難い現状がある。

2. 研究の目的

本研究では営業秘密の取扱いについて、営業秘密の管理における秘密性のレベルに応じた区分(以下、秘密度の区分とする)と情報資産の管理における「情報資産の分類とラベル付け」の観点から、営業秘密の管理における問題点と課題を少しでも明確に解決策の提案を行うことで、我が国の産業競争力維持､向上の一助にすることを目的としている。

3. 研究の範囲

営業秘密の漏洩リスクを低減することや、営業秘密に係る訴訟が発生した際に、営業秘密として法的な保護を受けるための可能性を高いものとするために、経済産業省「営業秘密管理指針(平成 25 年 8 月 16 日改訂)」に記載されている営業秘密を適切に管理するための方法として「情報セキュリティマネジメントシステム（ISMS） 」の推奨が述べられているが、その取組みにおける手引き(整合性)については明記されていない現状がある。

本稿では、「営業秘密の管理と情報セキュリティマネジメントシステム(ISMS)との整合性の推奨」[１]を切り口に、営業秘密を適切に管理するための方策ついて、情報資産の分類に基づくラベル付けの観点から考察を行う。

まず、第 4 章で「営業秘密の管理と秘密管理性」について、第 5 章では「情報資産の管理における分類とラベル付け」について述べる。
本稿で論じている情報資産及びその管理ついては､ISO/IEC 27001:2005 及び ISO/IEC 27002:2005(JIS Q 27002:2006) cの標準に基づいて論じている。

†1 情報セキュリティ大学院大学　情報セキュリティ研究科
INSTITUTE of INFORMATION SECURITY

a　裁判例調査は、「判例検索システム及び文献などで「不正競争防止法」や「知的財産」に関する判例中に「営業秘密」や「トレードシークレット」といった言葉が用いられている裁判例を抽出し、営業秘密に関する争点を精査して、最終的に 85 件の裁判例における 95 争点についてまとめた。」ものである。

b　物理的管理とは、経済産業省が公開している「営業秘密管理指針(平成 23 年 12 月 1 日改訂)」によると、「客観的に認識可能な表示(営業秘密及び区分の表示)」と「媒体の分離保管」とされている。

c ISO/IEC 27002：2013 には、「情報資産」という名称が「情報」に変更されている。

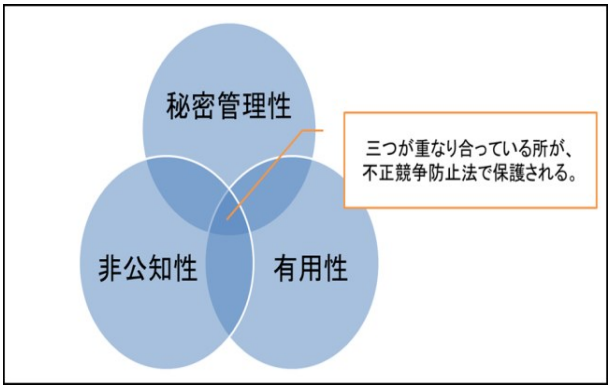
4. 営業秘密の管理

営業秘密は以下①～③の「性質」があり、適切な管理が求められる。
①無形の技術・ノウハウ・アイディア等の保護の重要性。企業活動を支える現場の労働者・技術者が生み出す技術情報等の営業秘密は、企業の長年の取組や多額の投資の結集であり、収益を生み出す源としての価値を有していること(根源性)。
②一度侵害されてしまうと回復が極めて困難であること(不可逆性・回復困難性)
③人的・組織的な管理といった安定性を欠く管理に頼らざるを得ないことから侵害に対する予防には限界があるという性質を内包していること(予防困難性)。とされている。[2]

4.1 営業秘密とは

営業秘密とは、「秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないものをいう」と不正競争防止法dに記載されている。
同法上で営業秘密として保護されるためには、以下の 3 つの要件が必要とされている。
①秘密として管理されていること(秘密管理性)
②有用な情報であること(有用性)
③公然と知られていないこと(非公知性)
また、秘密管理性の要件については、「情報にアクセスするものを制限すること(アクセス制限)」の存在や「情報にアクセスした者にそれが秘密であることを認識できること(客観的認識可能性)」の存在が求められている。」とされている
また、「情報にアクセスした者にそれが秘密であることを認識できること」と記載されている部分は、本稿 6 章で述べる情報資産のラベル付けと同義と捉えられる。
3 つ要件は、営業秘密の三要件と言われ、その三要件を満たした形を図で示すと以下の図 1 のようになる。

図 1：営業秘密の三要件



d 不正競争防止法第 2 条 6 項

(出典：経営法友会 法務ガイドブック等作成委員会、「営業秘密管理ガイドブック 全訂第 2 版」、商事法務、2010 年 11 月 13 日、p21、出典を参考に筆者が作成)

4.2 秘密管理性について

営業秘密が侵害された事例の内、判例上の争点となりやすく、重要とされているものが、秘密管理性であるとされている。[Ⅱ]その理由として、営業秘密に関する裁判例の内、秘密管理性について判断しているものは 81 件あるとされ、その中で秘密管理性を肯定したものは 23 件に留まり、全体の 7 割強が否定されている現状がある。[1]
この現状に対して、「営業秘密管理指針(平成 25 年 8 月 16 日改訂) 」によると秘密管理性の要件について肯定的な判断要素として、以下のような管理策が示されている。
A．アクセスできる者が限定され、権限のない者によるアクセスを防ぐような手段が取られている（アクセス権者の限定・無権限者によるアクセスの防止）
B．アクセスした者が、管理の対象となっている情報をそれと認識し、またアクセス権限のある者がそれを秘密として管理することに関する意識を持ち、責務を果たすような状況になっている（秘密であることの表示・秘密保持義務等）
C．それらが機能するように組織として何らかの仕組みを持っている（組織的管理）
肯定的な判断要素とされた具体的な管理方法としては以下のものが挙げられる。
【Aについて】
□ アクセス権者の限定
□ 施錠されている保管室への保管
□ 事務所内への外部者の入室の禁止
□ 電子データの複製等の制限
□ コンピュータへの外部者のアクセス防止措置
□ システムの外部ネットワークからの遮断
【Bについて】
□ 「秘」の印の押印
□ 社員が秘密管理の責務を認知するための教育の実施
□ 就業規則や誓約書・秘密保持契約による秘密保持義務の設定等
【Cについて】
□ 情報の扱いに関する上位者の判断を求めるシステムの存在
□ 外部からのアクセスに関する応答に関する周到な手順の設定とされている。
しかしながら、上記の管理策については、細部にわたる説明まで(具体的にどの程度行うべきなのか) はされていない点があると考えられ、管理策を実際に取り入れる上で

の問題点として挙げられる。

4.3 営業秘密の適切な管理

「営業秘密を適切に管理しようとする事業者において、侵害態様等の事後的な事情をあらかじめ考慮することは必ずしも容易とはいえない。そこで、事業者においては、具体的な管理方法を適切に組み合わせ、その管理水準を一定以上にすることにより、秘密管理性に関する法的判断における事後的な事情への依存度を軽減させ、営業秘密として法的保護を享受し得る可能性を高くすることが望ましい。」とされ、営業秘密の適切な管理を考える上で、自社の営業秘密の侵害における事後的事象について重点をおくべきではないと考えられる。

また、留意する点として「事業者の保有する多くの情報を適切に管理することは重要であるが、大量の情報をやみくもに営業秘密として管理しようとすることは、管理コストを高めるのみならず、管理の実効性や業務効率を低下させることとなり、結果的に秘密管理性が認められないことにもなりかねない。」としている。[1]

4.4 営業秘密として管理すべき情報資産

営業秘密として管理すべき情報資産の例示として、以下の表 1 が参考になる。

表 1：裁判例において営業秘密と主張された情報

技術情報	製造方法（ノウハウ）	・製造機の製造工程 ・白アリ駆除剤製造方法（配合割合、加熱温度、攪拌方法・攪拌時間、冷却温度等） 等
	図面	・金型図面 ・組立図面 ・部品図面 等
	その他	・ソフトウェアのプログラム ・機械効率のデータ 等
営業情報	経営情報	・ソフトウェアの開発方針 ・取締役会議事録 等
	仕入先/販売先に関する情報	・野菜の輸入先目録（生産者の氏名、住所、連絡先等） ・商品の原価 ・顧客目録（顧客の名称、住所、連絡先、過去の取引実績及び支払状況等） ・電話帳より抜粋した顧客名簿（ただし、電話帳頭の原の反転、成約に至る見込みなども記載） 等
	その他	・従業者（システムエンジニア）の情報（連絡先、売上高、報酬額、その基礎である取引記録等） ・派遣会社における派遣社員情報（氏名、連絡先、年齢、性別、経歴、取得資格、派遣実績等） 等

(出典：経済産業省　「営業秘密管理指針の概要　平成 23 年 12 月 1 日改訂版」)

「営業秘密管理指針(平成 23 年 12 月 1 日改訂)」における「営業秘密の管理のために実施することが望ましい秘密管理方法」では、以下のように述べられている。

「営業秘密として管理すべき情報資産が大量にあり、各情報資産の秘密性(機密性)のレベルに応じて異なる管理水準による管理体制を構築・実施することが可能である場合には、自社の情報資産を情報の秘密性のレベルに応じて区分し、区分ごとの管理水準・管理方法を設定することが望ましい。」とされている。

5. 情報資産の管理 (分類とラベル付け)

本稿における情報資産の管理とは、組織の保有する情報から、情報資産を洗い出し、洗い出した情報資産を重要度のレベルに応じて分類し、分類に基づいたラベル付けを行い、ラベルごとに事前に定められた管理策に従い情報資産を取扱うものとする。

5.1 情報資産とは

情報資産とは､「企業の業務遂行の過程で生み出される価値あるもののことです。資産には、不動産や商品など、目に見えるものもあれば、財務情報、人事情報、顧客情報、技術情報などの目に見えないものもあります。」[3]とされている。すなわち、情報に関連する全ての有形、無形のものが情報資産であるといえる。情報資産の例示を表 2 に示す。

表 2：情報資産の例示

分類	例示
情報	データベース及びデータファイル、契約書及び同意書、システムに関する文書、調査資料、利用者マニュアル、訓練資料、運用手順又はサポート手順、事業継続計画、監査証跡、保存情報
ソフトウエア資産	業務用ソフトウエア、システムソフトウエア、開発用ツール、ユーティリティソフトウエア、
物理的資産	コンピュータ装置、通信装置、取外し可能媒体、その他の装置
サービス	計算処理、通信サービス、一般ユーティリティ
人、資格等	人、保有する資格・技能・経験
無形資産	無形資産(組織の評判・イメージなど)

(出典：財団法人 日本情報処理開発協会「ＩＳＭＳユーザーズガイド-JIS Q 27001:2006(ISO/IEC 27001:2005)対応-リスクマネジメント編」2008 年 1 月 31 日)

5.2 情報資産の分類とラベル付けの定義

JIS Q 27002 : 2006(ISO/IEC 27002 : 2005) [4]によると､「情報の必要性，優先順位及びその情報を取り扱う場合に期待する保護の程度を示すために，情報を分類すること」と目的が示され､「情報は､組織に対しての価値, 法的要求事項, 取扱いに慎重を要する度合い及び重要性の観点から分類する」とされ､「情報によっては，保護レベルの引上げ又は特別な取扱いが必要なこともある。情報の分類体系は，一連の適切な保護レベルを定め，〈中略〉保護レベルは，対象とする情報についての，機密性，完全性，可用性及びその他の特性を分析することによって評定できる。」としている。

情報資産のラベル付けについては､「組織が採用した分類体系に従って策定し，実施すること」と管理策で述べ､「情報のラベル付けに関する手順は，物理的形式及び電子的形式の情報及び情報処理施設と関連する資産に適用できる必要がある。」とされ､「〈電子的形式の文書のようなある種の情報には物理的なラベル付けをすることはできず，電子的手段によるラベル付けが必要となることもある」とされている。

上記の内容を基に､「情報資産の分類とラベル付け」の定義を以下のように整理した。

①情報資産の分類

企業・組織の保有する情報から、洗い出された情報資産の重要度ごとに分類する。

重要度は、機密性、完全性、可用性の観点から考え、レベル分け(「政府機関の情報セキュリティ対策のための統一管理基準」では、「格付」に相当する)し、分類を行う。

②情報資産のラベル付け

重要度ごとに分類された情報資産にラベル付けを行う。

このとき､情報資産の機密性に応じた重要度に対しては、極秘、社外秘など具体的に表すことや、保管期限などの情報を情報資産自体に明示することとされている。

5.3 情報資産の分類基準について

各企業が独自の方法で分類基準を設けており、業界ごと等の統一的な分類や重要度に応じたレベル分けの基準はない。

以下に分類の基準を説明する上で、統一的な基準として記載がされている「政府機関の情報セキュリティ対策のための統一管理基準(以下、統一管理基準とする)」の中で用いられている「分類の基準」と「格付の区分」を示す。

統一管理基準は、各府省庁を対象としている為、企業にそのまま当てはめることができるわけではない。しかし、広範囲の政府業務に横断的に利用できるような特性もあるため、活用も可能である。なお、各企業が利用するには、企業の状況を考慮した判断が必要である。

・分類の基準と格付の区分

「統一管理基準」では､分類と格付けの基準を､機密性、可用性、完全性の三つの観点から､「格付の区分」を記載している。機密性は 3 段階、可用性は 2 段階、完全性は 2 段階の段階的な区分で、分類と格付けの基準が明記されている。

以下の表 3 は、統一管理基準に記載されている「分類の基準」と「格付の区分」を、機密性、可用性、完全性の観点から段階的に表したものである。

表 3：「分類の基準」と「格付の区分」

格付の区分	分類の基準
機密性3情報	秘密文書に相当する機密性を要する情報
機密性2情報	秘密文書に相当する機密性は要しないが漏えいにより、国民の権利が侵害され又は行政事務の遂行に支障を及ぼすあそれがある情報
機密性1情報	機密性2情報又は機密性3情報以外の情報
可用性2情報	滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は行政事務の安定的な遂行に支障(軽微なものを除く。)
可用性1情報	可用性2情報以外の情報
完全性2情報	改ざん、誤びゅう又は破損により、国民の権利が侵害され又は行政事務の適格な遂行に支障を(軽微なものを除く。)を及ぼす恐れがある情報
完全性1情報	完全性2情報以外の情報

(出典:政府機関の情報セキュリティ対策のための統一管理基準　2011 年 4 月 21 日)※「秘密文書」とは、情報公開法に基づく政府特有の表現である。

6. 営業秘密と情報資産の統合管理について

営業秘密の漏洩リスクを低減することや、営業秘密に係る訴訟が発生した際に、営業秘密として法的な保護を受けるための要素として営業秘密管理指針に述べられている営業秘密の適切な管理方法を情報セキュリティマネジメントシステム(ISMS)で定める管理策に取り込むことは、営業秘密の適切な管理を行うことに繋がると考える。

情報セキュリティ大学院大学原田研究室では、2013 年 8 月にプライバシーマーク、ISMS 認証企業及び大学、公官庁(4,500 組織）にアンケート調査を実施し、367 件（8.2%）の回答を得て、集計・分析した調査結果を示す。

6.1 営業秘密管理指針に述べられている営業秘密の適切な管理方法(秘密度の区分)を情報セキュリティマネジメントシステム(ISMS)で定める管理策に取り込むことについて

情報セキュリティマネジメントシステム(ISMS)で定める管理策に取り込むことについて、仮説を考えた。

仮説 1

企業の扱う秘密情報は、知的財産図面などの情報が主体であり、法務部門が中心となって、情報セキュリティ部門と協力して進めている。

仮説に対する調査結果：

調査結果のうち、各企業・組織で営業秘密と考えている情報の種別版)を図 1、営業秘密を管理している部門を図 2 に示す。従業員・仕入先・取引先情報が多い。

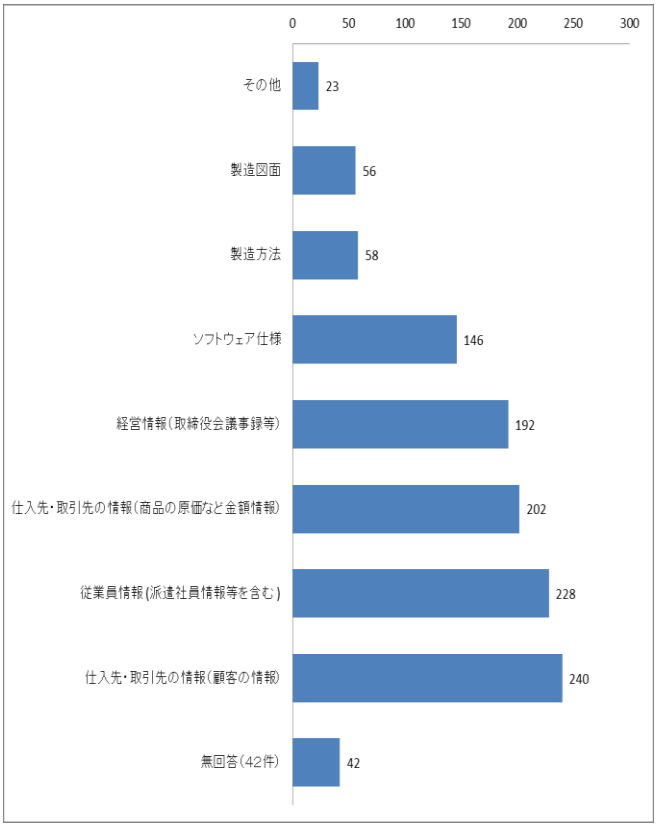


図 2：営業秘密とされる情報(複数回答) (n ＝367)

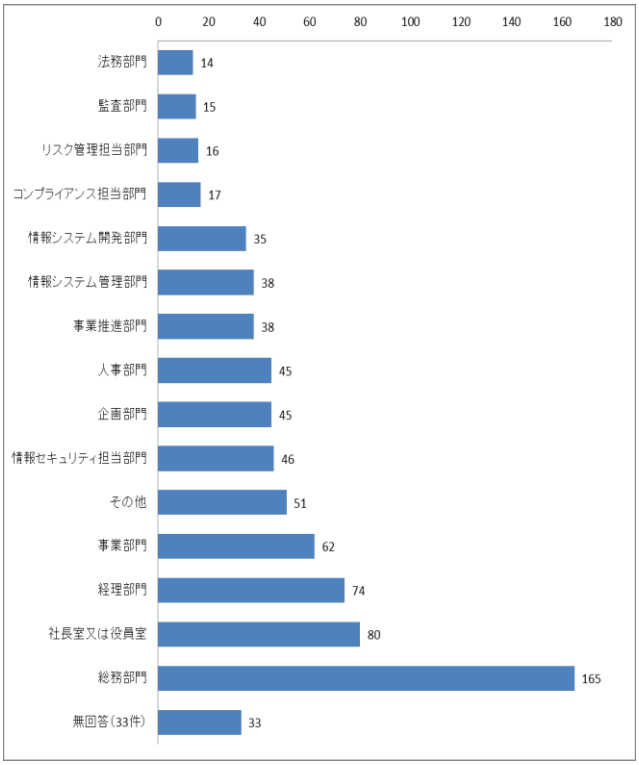


図 3：営業秘密を管理している部門(複数回答)（n＝367)

管理している部門では、総務部門、社長室又は役員室の順であり、営業秘密の管理について法的な観点からのアプローチが行われているとは言い難いと考える。

発見事項と考察：

調査結果から、営業秘密については、経済産業省などの想定（製造図面やノウハウが対象で、法務部門が関わる）とは異なっており、総務部門、社長室、経理部門など全体を担当する部門や事業部門が直接関与していることが多く、情報セキュリティ担当部門の関与は比較的少なく、多くの部門に分散管理されていることが判った。情報セキュリティの観点を踏まえた集中的な管理は難しいことが判った。次に、「営業秘密管理指針」にある秘密性のレベルに応じて区分することが望ましいとされていることから、仮説 2 が成り立つと考えた。

仮説 2

営業秘密は企業においてガイドラインなどで適切に区分(極秘、秘、社外等)されている。

仮説に対する調査結果：

仮説 2 に対するアンケート調査の結果を図 4 に示す。

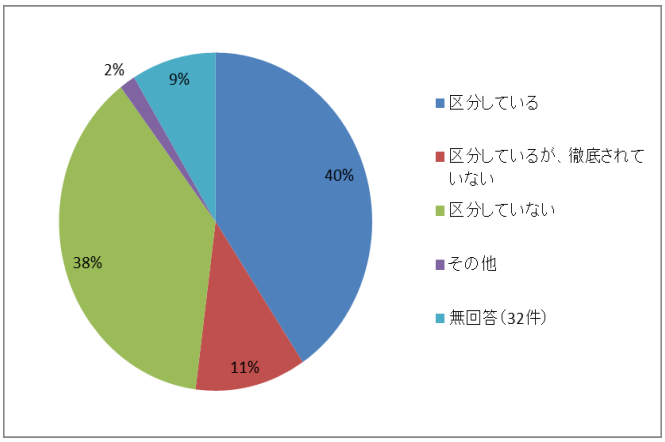


図 4：営業秘密の秘密度の区分(極秘、秘、社外秘等)状況(n＝367)

発見事項と考察：

営業秘密の秘密度の区分が行われている企業は、40%であり、徹底されていないの 11%と区分していないの 38%を含めると 49%の企業で十分に行われていないことから、仮説 2 は棄却されると考える。これは、図 3 の結果から、営業秘密の管理が総務部門や情報システム管理部門などで実施されており、営業秘密について詳しい法務部門が中心となっていないこと、全社的な取り組みに成っておらず各部門単位で行われているなどが理由として考えられる。企業内部での統一的な営業秘密の管理体制を確立し、秘密情報の区分を普及させることが喫緊の課題と考える。

仮説 3

営業秘密を秘密度の区分できている企業は、情報資産の機密度との関連(ひもづけ)付けも行われている。

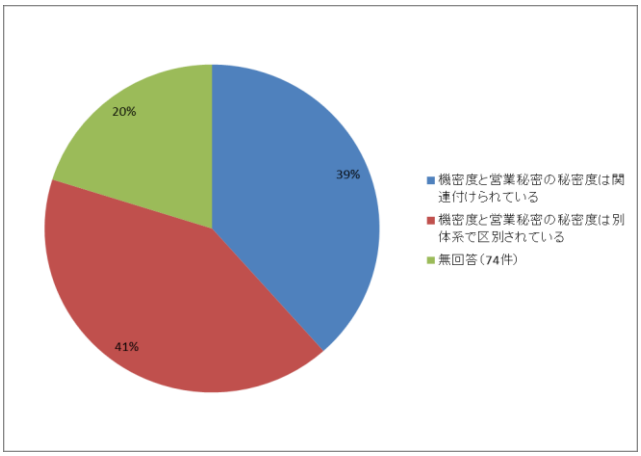


図 5：情報資産の機密度と営業秘密の秘密度の関連付けの状況。(n＝367)

仮説に対する調査結果：

情報資産の機密度と営業秘密の秘密度の関連づけを確認した図 5 によると、39%の企業が関連していることが判った。

発見事項と考察：

これは、図 2 で示した通り、仕入先・取引先の情報(顧客や単価情報)や従業員個人情報が対象と考えられていることから、関連付けが有っても個別単位であると考えられる。また図 3 で示した総務部門などが営業秘密の管理部門であることが多数であることや法務部門や情報セキュリティ部門が関わっていない為と想定され、以下の表 4 の関係付けが難しいのが実態と考える。

表 4 ：「情報資産の機密度」と「営業秘密の秘密度」における整合性

機密度		秘密度	
	4		極秘
	3		秘
	2		社外秘
	1		公開

(※第 6 章 3 節で述べた「統一管理基準」を参考に作成)

以上の仮説の検証から、「営業秘密の秘密度」と「情報資産の機密度」における関連付けについて再検討する必要があると考える。

また、「情報資産の機密度」と「営業秘密の秘密度」における対応関係について確認した図 5 によると、39%の企業が「秘密度に機密度を対応させる必要がある」と考えていることが判った。

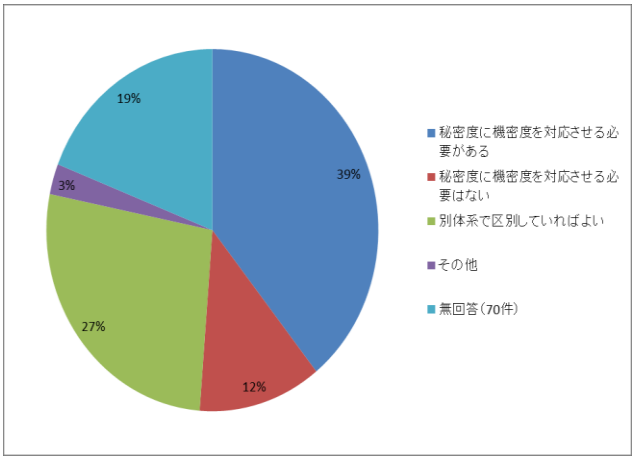


図 6：情報資産の機密度と営業秘密の秘密度との対応関係について、どのような考えをお持ちですか。(n＝367)

発見事項と考察：

企業において「別体系での区別」及び「秘密度に機密度を区別させる必要がない」と回答した企業が 39%である。

また、「秘密度に機密度を対応させる必要がある」と回答した企業については、機密度と秘密度を一体化させて、管理を合理化（営業秘密管理性を担保）したいとの思いがあると考える。

8. まとめ

営業秘密と情報セキュリティマネジメントシステムの対応は理想像であり、7 章に述べたように実際の企業では、「営業秘密管理指針」の通りには営業秘密の管理がされていない実態が判った。

特に、ISMS に営業秘密の適切な管理方法を取り込むための手引きとなる事例等が、存在しておらず、更に、「営業秘密の秘密度」と「情報資産の機密度」における整合性についても明記されていない現状がある。

本研究によって判ったことを以下に述べる。

①アンケートの調査結果では、営業秘密を管理する部門と情報資産を管理する部門が異なっていることや、責任が異なっていることが判った。

②裁判所に多く否定されている裁判例の内、秘密管理性の要件に関係する「秘密区分の特定と表示」に対して、アンケート調査結果によると、実際に「区分している」企業が少ないことが判った。

③「営業秘密の秘密度」と「情報資産の機密度」間の整合性については、経済産業省のガイドラインをそのまま用いた現状では整合性があるとは言い難く、実際に管理を行う上での手順等(「秘密性」と「機密性」の違いを踏まえたもの)の整備が必要であると感じた。

今回の研究の成果として、営業秘密と情報資産については、管理対象の粒度や管理主体の違いによって、統合して実施できる場合と分けた管理を行う場合があり、経済産業省のガイドラインで述べられている「ISMS との推奨」のようにはいかないことがアンケート調査で確認できた。後者の場合について、どのように管理するのが良いかについては更に検討が必要であると考える。

謝辞 本研究にあたり、アドバイスや支援を頂きました情報セキュリティ大学院大学の関係者各位、関係組織の関係者の皆様に、感謝の意を表す。

参考文献

1) 経済産業省、「営業秘密管理指針(平成 25 年 8 月 16 日改訂)」、2013 年 8 月 26 日アクセス、http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/111216hontai.pdf
2) 経済産業省、「営業秘密に係る刑事的措置の見直しの方向性について」(平成 21 年 2 月)
3) 「経済産業委託事業：NPO 日本ネットワークセキュリティ協会」、「情報資産とは」〈http://www.jnsa.org/ikusei/basis/02_01.html〉2013 年 9 月 5 日アクセス
4) JIS Q 27002：2006(ISO/IEC 27002：2005)、〈http://kikakurui.com/q/Q27002-2006-01.html〉、2013 年 9 月 5 日アクセス pp.19-22
5) 土居範久監修、「情報セキュリティ教本(改訂版)」、IPA 実教出版、2011 年 11 月
6) 経済産業省、「営業秘密の管理に関するアンケート調査と判例調査の結果分析」、2009 年 9 月
7) 内閣官房情報セキュリティセンター、「政府機関の情報セキュ

リティ対策のための統一管理基準」、2011 年 4 月 26 日
8) 岡野靖丈、「営業秘密に関する情報セキュリティ管理　改正不正競争防止法など相次ぐ立法措置と企業の課題」、野村総合研究所
9) 原田季栄、半田哲夫、「ラベルに基づくセキュリティの限界とその補完 : TOMOYO Linux の設計思想と試み(<特集>Linux のセキュリティ機能)」、情報処理 Vol.51 No.10、2010 年 10 月 15 日、p35 pp.1276-1277
10) 経済産業省、「営業秘密に係る刑事的措置の見直しの方向性について」、2008 年 12 月
11) 鈴木武俊・真田大志、「情報セキュリティポリシー運用における課題と対策」UNISYS TECHNOLOGY REVIEW 第 98 号、2008 年 11 月
12) 大木栄二郎、田村仁一、清水惠子、佐野智己、芹沢大地、「経営に役立つ情報セキュリティ会計の提案」、情報セキュリティ・マネジメント学会誌、第 25 巻第 2 号、2011 年 9 月
13) 船越洋明、「特集[文書管理から始める情報資産管理]重要情報資産の所在管理のポイント―ISO27001 認証取得企業の実例から―」、野村総合研究所、 IT ソリューションフロンティア Vol.28 No.5 、2011 年 5 月、p9
14) 経営法友会 法務ガイドブック等作成委員会、「営業秘密管理ガイドブック 全訂第 2 版」、商事法務、2010 年 11 月 13 日