日本経営倫理士協会との協同シンポジウム開催概要

情報システム学会
会長　伊藤重隆

2017 年 7 月 7 日（金）午後に協同シンポジウムが開催されました。
シンポジウムテーマは「情報セキュリティ～いま問われる企業力」でした。
シンポジウム当日は炎天下にも拘わらず 100 名ほどの参加がありました。
午後 1 時半から開始され基調講演、パネリスト講演、パネルディスカッションが行われ
午後 5 時半過ぎには閉会となりました。その後、名刺交換会が行われました。下記に概要をお伝えします。

基調講演
題目：改正個人情報保護法、ＧＤＰＲの概要と企業における課題
講演者：髙野　一彦氏（関西大学　社会安全学部教授・博士（法学）

はじめに過去の主な情報セキュリティで問題となった情報流出事件の事例を取り上げ、具体的には、ヤフーBB 顧客情報流出事件（2004 年、460 万件）や年金機構事件（2015 年、標的型メールによる）などで、内部者による犯行が多いものの、最近ではウイルス・不正アクセスが目立っていると指摘。個人情報の不正取得による漏えい事件例として、委託先社員によって 3504 万件ものデータが流出したＢ社は、特別損失 260 億円を出し初の赤字決算となって大きなリスクが顕在化し会社業績に大きな影響があったと報告がされた。

こうした情報不正取得行為への法的制裁では、営業の秘密管理性が争点となり、法の間隙をどう埋めるかの法制度について各国の例を検証した。結論として日本でも指針（ガイドライン）が出されたが法的拘束力がないと考えられるので、民事での差し止め請求権の行使や社内・組織での情報棚卸し、専任管轄部署設置の必要性が強調された。

日本の経済政策と情報法の国際的な整合性については、ＩＣＴ（情報通信技術）発展に伴い発生・顕在化した諸課題に対し、国際的な整合性を図る必要から検討した。日本では 2015 年９月に改正個人情報保護法が成立、17 年５月 30 日に施行された。また、欧州連合ＥＵでは 2012 年にＥＵ一般データ保護規則（General Data Protection Regulation:GDPR）提案があり、2018 年５月施行される。GDPR は新しい個人情報保護の枠組みで、個人データの処理と移転に関するルールを定めた規則であり、日本企業への影響もあるので日本の個人情報保護法との比較がされた。今後、関係企業は具体的に取り組みの必要があるとのこと。

最後に今回の改正個人情報保護法で導入された匿名加工情報やトレーサビリティの確保などについて内容も詳細に検証し、繁雑な法体系に対してどの様に企業として体制をつくって取り組むかと言う点についての問題提起がされた。

ACBEE 特別シンポジウムに参加して

杉野　隆

日本経営倫理士協会 ACBEE の特別シンポジウムが 2017 年 7 月 7 日に開催され，私はパネリストの一人として参加しました。シンポジウム及びパネルディスカッションの模様をご報告いたします。

ACBEE は，経営倫理士の研修，資格認定，研鑽，普及を目的とする協会です。ISSJ 監事の松平さんが常務理事を務めていらっしゃいます。ACBEE では年に一回特別シンポジウムを開催されていますが，今回は情報システム学会との協同開催となり，「『情報セキュリティ』　いま問われる企業力　―　＜個人データ　コンプライアンス＞と＜組織データ防衛＞」をテーマとしています。情報システム学会にシンポジウムでの報告者の依頼があり，私が指名された次第です。

皆様ご承知のように，10 年ぶりに個人情報保護法が改正され，今年 5 月 30 日に全面施行されました。さらに 2018 年 5 月には EU 一般データ保護規則の導入が予定されており，企業実務における個人情報保護とプライバシ保護に，内外から大きな影響が及ぶものと予想されています。企業レベルにおけるネットビジネスの急拡大，個人レベルでの SNS の急拡大に促される形で，これらの改正，導入は行われています。さらに，IoT の進展によって企業，個人が活動するサイバー空間は爆発的に拡大し，また AI 技術などの進歩によって，企業や個人の活動に当たって安全確保，プライバシ確保に留意することの重要性が喧伝されています。さらに，企業や組織を狙うサイバー攻撃は近年増加，インフラの機能停止，顧客情報の漏えいやその不正利用など重大な被害が続発し，事業継続への影響も深刻化しています。グローバル化が進むなか，情報セキュリティは大きな社会問題となっています。
私自身は，基調講演に続く，4 名の各パネリストに与えられた 20 分の報告の中で「サイバー攻撃とセキュリティ経営」というテーマで報告しました。

私の報告の趣旨は次のようなものでした。企業の情報システムは企業経営における生命線ですが，シームレスにインターネットに接続されており，結果として，すべての情報システムがサイバー攻撃に曝されています。サイバー攻撃の被害は，経済的損失ばかりでなく，個人情報の流出，風評被害，（重要インフラが標的になると）生命・社会生活の危険にも及ぶ虞があります。さらに，サイバー攻撃は大規模化，巧妙化しており，すべての攻撃を未然に防止することは現実的ではないし，技術的対策にも限界があります。したがって，経営陣は，サイバー攻撃を経営上のリスクとして捉え，情報セキュリティ対策のプロセス，要員，ガバナンスに目を向けたセキュリティ経営を確立しなければなりません。そのためには，当然，最高情報セキュリティ責任者（CISO）を中心にした情報セキュリティ組織の確立が必要ですが，その組織を確実に運用するためには，情報セキュリティ要員の育成，強化がさらに重要であります。その前提として，組織全員の情報セキュリティ意識の向上を図ることがカギであり，結局は人を育てるということが最も基本的な課題です，といった話でした。

その後パネルディスカッションでは，ファシリテータの差配に従って，参加者からの質問に答えたり，パネリスト相互にディスカッションしたりしました。そこでは，情報セキュリティ監査にも言及し，監査に先立ち，各部門が自己点検・自己評価によって情報セキュリティ上の課題を自ら発見し，当事者又はその管理者などが，必要な改善策を実施するという姿勢が今後重要になると申し上げました。

経営倫理士は，組織経営におけるコンプライアンス，リスク管理，CSR，ダイバーシティといった経営課題に即応し，解決する能力を期待されています。その中で，セキュリティ経営といった課題にも強い関心を持っていただいていると感じました。