資料３

2016年12月7日

普及啓発・人材育成専門調査会

サイバーセキュリティと法務

オリック東京法律事務所・外国法共同事業　訴訟部代表パートナー
髙取 芳宏　弁護士（日本・米国ニューヨーク州登録）
英国仲裁人協会上級仲裁人（ FCIArb. ）

orrick

1. 訴訟・コンプライアンスのための戦略的対応
—サイバーセキュリティ経営ガイドラインの法的な意味を含めて

—サイバーセキュリティは、技術によるprotectionや対処のみでなく、法律的な対処が必須。

- ガイドラインは、そのまま法的な拘束力を持つものではない。
- ***しかしながら***、訴訟・仲裁等で取締役の情報セキュリティにかかる善管注意義務が問題となるケース（ex. ベネッセの株主代表訴訟）において、ガイドラインの遵守が重要なポイントとなってくる可能性もあり。
  - ✓ 証拠作りの観点からは、ガイドラインに準拠した体制・規程等を整備・運用することが重要。特に「3原則」において経営者による認識とリーダーシップの表明が求められている点は今回のガイドラインの新しい要素であり、その点を意識したセキュリティポリシーや取締役会等の議事録の作成等の証拠作りが必要。
  - ✓ 「重要10項目」については、従前のISMS認証等とおおむね重なるものであるが、従前認証を求めるための要素であったに過ぎない情報セキュリティマネジメントシステムの導入が、企業としてより積極的に求められる事項になっていると評価できる。
- 国境を超えたデータの性質（データの属性、国籍、居住地等）により、国境を超えた紛争に巻き込まれる可能性＝「被害者だったはずが加害者に」
- 例）米国の（集団）訴訟で、広く行なわれるデポジションの対象として経営陣を呼び出す根拠が増えた。

2. 情報セキュリティガバナンス
―紛争等に備えて、どう「証拠」を残していくか。

①予防段階、②発覚・戦略構築段階、③紛争・調査対応遂行段階の、いずれの段階でも「証拠」がキーワードであり、弁護士の参画が望まれる。

例）営業（企業）秘密の管理、脆弱性テスト（への対応）、コンプライアンス、インシデント・シミュレーション等の訓練等。

- インシデント対応プランの構成例

Phase 0	**インシデントへの準備、評価** リスク評価、対応チームの組成、専門家・外部機関との連絡確保	① 予防段階
Phase 1	**検出、選別、スコーピング、封じ込め** 情報収集及び重要性の評価、外部専門家の選任、初期的な通知	② 発覚・戦略構築段階
Phase 2	**フォレンジック調査、復旧** 包括的なフォレンジック調査の実施、封じ込め・復旧、証拠保全	
Phase 3	**通知、外部公表** 関係者への通知、PRプランの準備、法的リスクの検討	③ 紛争・調査遂行段階
Phase 4	**インシデント後の分析、再評価** 調査結果の分析・公表、内部規程等の再検討	

3.1グローバル・ビジネスへの影響と対策
ー日本企業と海外企業の意識の違い
グローバル対応

- **グローバル対応の必要性**
  - ✓ 経営ガイドラインは、企業として行うべきサイバーセキュリティ対策の基準を示すものであるが、これだけを満たせば十分というものではなく、それ以上の対応が求められる。
  - ✓ 特に、グローバルに活動する企業においては、EUや米国等の海外の法規制にも目を配る必要がある。
  - ✓ ある情報漏洩が日本のみならず、国境をまたがって発生した場合、通知の要否やその内容については関係国ごとにその取扱も異なることが想定され、その対応は非常に複雑となる。

3.1 グローバル・ビジネスへの影響と対策
ー日本企業と海外企業の意識の違い
グローバル対応

- **EU 「ネットワーク情報セキュリティ指令」（Network and Information Security Directive）**
  - ✓ 加盟国にセキュリティ対策の強化を求めるとともに、エネルギー、交通、銀行、ヘルスケア等の重要インフラ事業者に、ハイレベルのリスク管理を求めるもの。
  - ✓ 2015年12月にEU議会での合意に達し、今後、正式な制定手続きが進められる予定。
- **EU 「一般データ保護規則」（General Data Protection Regulation ）**
  - ✓ 2016年4月に、欧州議会による可決がなされ、正式文書として公表後、20日後に発効。発効日から2年後（2018年5月）には、EU各国での適用が開始される予定。
  - ✓ EU圏内の個人に対して商品・役務を提供する事業者に対して適用。
    →該当する日本企業は対応の必要あり
  - ✓ 違反企業には最高でその企業の世界全体の売上高の4%または2000万ユーロのいずれか高い方の課徴金。

3.1 グローバル・ビジネスへの影響と対策
ー日本企業と海外企業の意識の違い
グローバル対応

- **EU 「一般データ保護規則」（General Data Protection Regulation ）**
  - ✓ 欧州委員会から「十分な保護措置」を備えているとして認定された国や地域以外への個人データの移転については、一定の要件を満たす必要あり。
    →日本は現在のところ十分性認定を受けておらず、政府は認定取得の意向を示しているものの、いつ認定が受けられるかは未定

    ①本人（データ主体）の同意

    →雇用関係に基づく同意の場合、自由な意思に基づかない同意として有効性が問題になる可能性あり

    ②標準契約条項（Standard Contractual Clause）の利用

    →モデルの条項に従う必要があり。また、個別に契約を締結する必要あり。

    ③ 拘束的企業準則（Binding Corporate Rules）の利用

    →関連規程や体制を整備し、管轄のデータ保護機関による承認を経る。承認手続きには、1年以上を要するとされる。

3.1 グローバル・ビジネスへの影響と対策
ー日本企業と海外企業の意識の違い
グローバル対応

- 他方、米国ではプライバシー保護法制が存在しておらず、「医療」や「金融」といった分野ごとのプライバシー保護法がモザイク的に制定されている。情報漏洩時の通知についても、各州によって要求が異なる状況にある。
- そのため、民間の自主規制による解決が重視される傾向にある。
  - ✓ 2014年2月12月に、米国商務省傘下の国立標準技術研究所（NIST）が公表したUS「重要インフラのサイバーセキュリティを 向上させるためのフレームワーク」（Framework for Improving Critical Infrastructure Cybersecurity）が事実上のスタンダードになっている。

3.2 グローバル・ビジネスへの影響と対策
ー弁護士・依頼者間秘匿特権（Attorney Client Privilege）の活用

- **<u>弁護士依頼者秘匿特権(Attorney Client Privilege) の活用</u>**
    - Discovery の例外
        - Attorney Client Privilege
        - Attorney Work Product
        - Anticipation of Litigation
    - どのようにして最大限確保するか

①外部の（インハウスではない）

②当該管轄において法曹資格を有する

③弁護士に早期に依頼し

④「リーガルアドバイス」を得るための報告ないし指示にする

＋Waiver（放棄）や誤提出に注意。

3.2 グローバル・ビジネスへの影響と対策
ー弁護士・依頼者間秘匿特権（Attorney Client Privilege）の活用

- **<u>弁護士依頼者秘匿特権(Attorney Client Privilege) の活用</u>**
  - ✓ 内部的なコミュニケーションや、関係者とのコミュニケーションの内容は、訴訟・仲裁、調査等において不利な証拠としても用いられる可能性がある。欧米の訴訟・調査では、広範な証拠開示が行われることも多く、内部的なコミュニケーションも開示の対象となる可能性が高い。

    例：セキュリティ対策の向上のため、専門業者に依頼して脆弱性テストを行い、その結果セキュリティの脆弱性を指摘する報告書が作成された場合や、セキュリティ担当者間で「うちの秘密管理はなってないね」というようなコミュニケーションが残された場合

    例：データ漏洩等の事実が発覚し、調査を遂行する段階において、専門業者によるフォレンジック調査が行われた場合、当該取得したログは、セキュリティや秘密管理の不備を立証する証拠として、訴訟の相手方や行政当局によって用いられる可能性

3.2 グローバル・ビジネスへの影響と対策
ー弁護士・依頼者間秘匿特権（Attorney Client Privilege）の活用

- **弁護士依頼者秘匿特権(Attorney Client Privilege) の活用**
  - ✓ 内部のIT担当者間や外部セキュリティ監査人等とのやり取りが秘匿特権の対象となるよう、外部弁護士によるリスクやコンプライアンスについての法的助言の一環としてサイバーセキュリティ監査・評価を指揮することが得策。
  - ✓ また、緊急時対応において、対応過程が秘匿特権の対象となるよう、速やかに外部弁護士への委任を行い、その弁護士が専門業者等を指揮するかたちをとることが得策。

4.「チーム」によるサイバーセキュリティの必要性

—IT、セキュリティ対策室などに加えて、法務、知財、人事、広報、各事業部の参画が必須。

—それを経営陣が束ねて、直接の責任を持ち、所管の狭間等が生れないような体制（ポリシー）を作るだけでなく、実際の運用が重要。

例）インシデントが発生した時にのエスカレーションプログラムが実際に機能するのか、たらい回しにならないか。

例）クラウドサービス提供企業の場合＝ブラックボックスの中身について誰が責任を持つか。顧客との契約書等の法的な対応、広報の対応等。

ご質問等がございましたら、下記連絡先までお願い致します。

オリック東京法律事務所・外国法共同事業　訴訟部代表
弁護士　髙取芳宏　ytakatori@orrick.com

髙取　芳宏

取り扱い分野
国際紛争解決
知的財産権
製造物責任訴訟
民事･商事訴訟
労働法

学歴
1998年　ハーバード大学ロースクール法学修士(LL.M.)取得
1989年　早稲田大学法学部　法学士取得

法曹資格
弁護士(第一東京弁護士会)
米国ニューヨーク州
英国仲裁人協会上級仲裁人(FCIArb.)

髙取芳宏弁護士は、東京オフィスのパートナーであり、同オフィス訴訟グループの代表である。主に複数の管轄にまたがる民事、商事、知的財産権、製造物責任、独占禁止法等の国際訴訟・仲裁を扱い、FCPA、UKBA、内部通報等のコンプライアンス事案やサイバーセキュリティー事案、労働法関連紛争などを手掛ける。

過去の代表的な案件としては下記のようなものがある。

- 日本企業約150社が被害にあった、いわゆるクレスベール証券（プリンストン債）事件において、複数の日本企業を代理し、米国ニューヨーク州及び日本における裁判、和解手続で中心的役割を果たした。
- 米国、アジア諸国およびヨーロッパにおける商標、模倣品、特許侵害などの知的財産権関連訴訟を遂行し、知的財産高等裁判所における画期的な判決獲得を含む実績を挙げている。近時では、諸外国商標権侵害について、諸外国法及び法の適用に関する通則法による日本法の適用による損害賠償認定を勝ち取り、注目されている。
- 米国カリフォルニア州における、懲罰的損害賠償を含む約2800億円の認定判決に基づき、日本の裁判所における保全処分を獲得するなど、国境を超える執行及び裁判、国際仲裁において、多くの実績をあげている。

さらに、髙取弁護士は日本商事仲裁協会による推薦仲裁人名簿及びシンガポール国際仲裁センター（SIAC）の仲裁人名簿に掲載されている他、英国仲裁人協会における上級仲裁人（FCIArb.）の資格を有し、公益法人日本仲裁人協会の常務理事、英国仲裁人協会日本支部の共同代表等、国際仲裁の分野でも要職を務める。

訴訟グループ

東京

連絡先
81 3 3224 2911
ytakatori@orrick.com

髙取　芳宏（続き）

著書・著作

- 「最新　クロスボーダー紛争実務戦略」（2016年6月　レクシスネクシス・ジャパン）編者
- 「訴訟・コンプライアンスのためのサイバーセキュリティー戦略」（2015年4月　NTT出版）編者/共著
- 「国際仲裁教材」　(2015年6月　信山社) 監修
- 「企業間紛争解決の鉄則20」（2012年9月 中央経済社） 著書
- 「サイバーアタック等への対処と法的戦略」（2016 年9月Business Law Journal）著書
- 「国際商事仲裁の法と実務」（2016年8月　丸善雄松堂）　著書

主な講演

- 「不可分となったサイバーセキュリティと経営」、情報セキュリティマネジメントフォーラム2016（2016年11月）
- 「紛争解決弁護士の目から見たサイバーセキュリティ」、Cyber3 Conference Tokyo 2016 （2016年11月）
- 「人工知能によるグローバルイノベーション先行事例」、イノベーション・ファインダーズ・キャピタル共同セミナー（2016年9月）
- 「弁護士・依頼者間秘匿特権に関する諸問題及び実務的処方箋」（2016年9月Monthly Seminar Series – The Orrick Library-）
- 「Racing against the clock:アジア太平洋地域における事業再生およびリストラクチャリング2016年の見通し」（2016年6月）
- 「サイバーセキュリティ経営ガイドライン」から考える経営と情報セキュリティ　–訴訟・コンプライアンスのための戦略的対応策–」(2016年4月Monthly Seminar Series – The Orrick Library-)


orrick