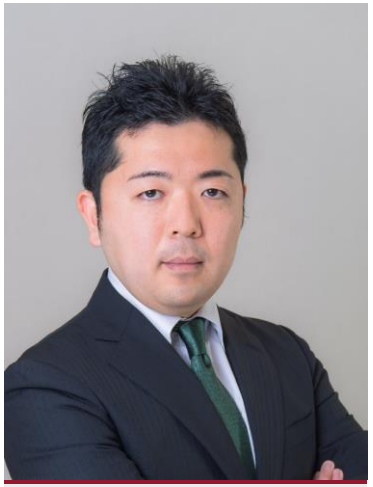
サイバーセキュリティセミナー ‘23 in 東北

インシデント対応の法律実務とサイバーセキュリティ関係法令

2023年12月19日

森・濱田松本法律事務所 弁護士
慶應義塾大学大学院 政策・メディア研究科 特任准教授（非常勤）
蔦　大輔

Lawyer profile



蔦　大輔

Daisuke Tsuta

カウンセル

東京弁護士会所属

主要な取扱分野

サイバーセキュリティ、個人情報保護、IT・ICT

- サイバーセキュリティ、個人情報保護・データ利活用、電気通信事業等のインターネット事業に関するサポートに取り組む
- サイバー攻撃の予防、攻撃を受けた後の対応に関する助言、サポート、従業員による内部不正についての対応（訴訟を含む）
- 「サイバー攻撃被害に係る情報の共有・公表ガイダンス」、「サイバーセキュリティ関係法令Q&Aハンドブック」の策定に関与

著作・論文

- 「クロスセクター・サイバーセキュリティ法」（商事法務NBLで連載中、2023年）
- 『類型別　不正・不祥事への初動対応』（中央経済社、2023年、共著）
- 『情報刑法Ⅰ　サイバーセキュリティ関連犯罪』（弘文堂、2022年、共著）
- 『60分でわかる！改正個人情報保護法超入門』（技術評論社、2022年、共著）
- 『事例に学ぶサイバーセキュリティ 多様化する脅威と法務対応』（経団連出版、2020年、共著）

その他、著書・論文・講演多数

経歴

2007年　京都大学法学部卒業
2009年　神戸大学法科大学院修了
2014年　財務省近畿財務局 統括法務監査官 法務監査官
2015年　総務省行政管理局 情報公開・個人情報保護推進室 副管理官
2016年　情報ネットワーク法学会理事（～2020年）
2017年　内閣官房内閣サイバーセキュリティセンター(NISC)　上席サイバーセキュリティ分析官
2021年　総務省 IPネットワーク設備委員会 事故報告・検証制度等タスクフォース　構成員
2022年　筑波大学大学院 人文社会ビジネス科学学術院 ビジネス科学研究群 非常勤講師
2022年　サイバーセキュリティ協議会 サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会 委員
2022年　警察庁 サイバー被害の潜在化防止に向けた検討会 委員
2023年　慶應義塾大学大学院政策・メディア研究科 特任准教授
2023年　日本弁護士連合会 弁護士業務における情報セキュリティに関するワーキンググループ 委員
2023年　経済産業省 サイバー攻撃による被害に関する情報共有の促進に向けた検討会 委員
2023年　サイバーセキュリティ法制学会理事
2023年　警察庁 キャッシュレス社会の安全・安心の確保に関する検討会　委員

アジェンダ

1．サイバーセキュリティリスクへの対応

2．インシデント対応（対外対応を中心に）

3．サイバーセキュリティ関連法令の紹介

1

サイバーセキュリティリスクへの対応

サイバーセキュリティに関する様々なリスク

1. **情報セキュリティリスク**
   - 企業が保有する機密情報や個人情報が漏えい等するおそれ
2. **システムリスク・事業継続リスク**
   - 利用している情報システムが停止し、業務に影響を及ぼすおそれ
3. **サプライチェーンリスク**
   - 製品製造の過程で悪意ある機能が組み込まれるおそれ
   - 製品、情報などの一連の商流の中で、脆弱な組織が狙われるおそれ
4. **リーガルリスク**
   - 情報漏えいや業務停止等により、規制当局による法執行や、関係者に対する賠償問題となるおそれ
5. **レピュテーションリスク**
   - インシデントの発生が明るみに出ることで企業のレピュテーションに影響を及ぼし、株価等や取引関係に影響を生じるおそれ

サイバーセキュリティは様々な観点からの問題

■ 広がるサイバーセキュリティ

- ✓ システム・IT・OT・製品・施設の管理
- ✓ リスク管理・危機管理
- ✓ ガバナンス（組織統治）・コンプライアンス（法令遵守）
- ✓ （経済）安全保障

■ 関係する法令やガイドラインも様々

- ✓ 経営、体制整備に関する法令・ガイドライン
- ✓ データ保護に関する法令・ガイドライン
- ✓ 製品の安全性、施設の保安に関する法令・ガイドライン
- ✓ インシデントに関する法令・ガイドライン

■ 脅威は日々刻々と変化する

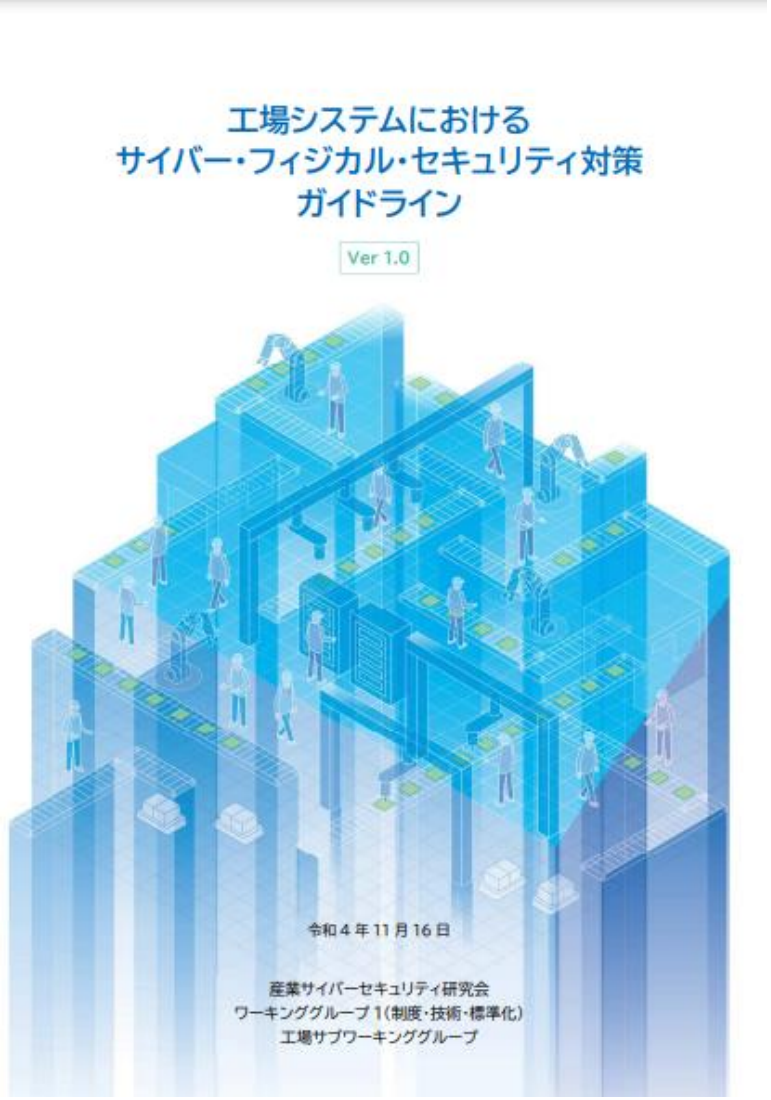
- ✓ 変化する脅威に対応する必要・必要な対策を変える必要
- ✓ 変化に対応するための情報収集も重要

サイバー・フィジカル・セキュリティ

- **サイバー空間とフィジカル空間が高度に融合**
  - **サイバー空間における攻撃がフィジカル空間に影響**
    - サイバー攻撃による工場等の機能停止　→工場セキュリティ
    - サイバー攻撃によるIoT製品の停止、不正挙動　→製品セキュリティ
  - **フィジカル空間で複雑化するサプライチェーン**
    - サプライチェーン・リスク対策
    - 取引先、委託先管理
  - **サイバー空間における大量のデータ流通・連携**
    - 不正アクセスによるデータ漏えい、改ざん、破壊
    - 個人データ・プライバシー保護
    - クラウドサービス

工場システムガイドライン

- **工場システムにおけるサイバー・フィジカルセキュリティ対策ガイドライン ver1.0（2022年11月16日）**
  - 工場のIoT化によりサイバー攻撃リスクが増加。
  - 業界団体や個社が自ら対策を企画・実行するに当たり、参照すべき考え方やステップを示した「手引き」
  - 工場の事業継続・生産継続、安全確保、品質確保、納期遵守、コスト低減という価値がサイバー攻撃により毀損されることを防止
  - 特に実施が求められる具体的な対策について、準備、組織的対策、運用的対策、技術的対策、工場システムサプライチェーン管理の5つのカテゴリでまとめ（付録E：チェックリスト）



工場システムを取り巻く社会的要件

【参考】付録B　工場システムを取り巻く社会的要件

- 工場システムを取り巻く社会的要件や要求を、法規則や標準規格・ガイドライン準拠、国・自治体産業界など、さまざまな視点から整理する。

B-1	法規制、標準規格、ガイドライン準拠に関わる要件	**B-1.1　法規制によるセキュリティ対策の要求** ● 取締役がサイバーセキュリティに関する体制整備を怠ったことが原因で企業に損害が発生した場合には、善管注意義務や忠実義務に対する違反を理由に、取締役個人が会社に対する任務懈怠（けたい）責任や第三者に対する損害賠償責任を問われる可能性がある。また、サイバーセキュリティ攻撃に対して迅速かつ的確な対処を怠った場合にも、同様に不法行為として問われる場合がある。 **B-1.2　セキュリティに関わる標準規格・ガイドライン準拠の要求** ● 何をどの程度実施すべきかの参照情報として、国内外の規格やガイドライン更に法規などがあり、更に取引先が規定している要件などもある。
B-2	国・自治体からの要求	● 法令(労働安全基準法、環境基本法など) やガイドラインに関わる問題がないかを確認する必要がある。 ● 国や自治体と工場システムを介する場合など、相互のシステムを連携する場合に、セキュリティ要件が規定されている場合がある。 ● 国や自治体が導入する製品の調達基準の中に、製品自体のセキュリティ対策要件や、製品の生産システム／工程におけるセキュリティ確保を目的とした要件が明示される場合がある。
B-3	産業界からの要求	● 経団連は「経団連サイバーセキュリティ経営宣言」を公表し、経済界が全員参加でサイバーセキュリティ対策を推進することで、安全・安心なサイバー空間の構築に貢献することを表明するとともに、経団連「サイバーリスクハンドブック(取締役向けハンドブック)」として、取締役がセキュリティ脅威による企業経営リスクへの対処策を検討・議論する際に考慮すべき事項を整理し、サイバーリスク管理の5原則を示している。
B-4	市場・顧客からの要求	● 標準規格「IEC62443」や、サイバーセキュリティに関わるグローバルに参照されている米国「NIST SP 800シリーズ」、経済産業省の産業分野別セキュリティ対策ガイドラインなどへの対応が要求される場合も増えている。
B-5	取引先からの要求	● 取引先から、供給する製品・部品に不正なハードウェアやソフトウェア(プログラム)が含まれることのないように、工場の製品生産過程におけるセキュリティ対策を要求される場合もある。
B-6	出資者からの要求	● 工場システムのセキュリティ対策を検討・企画するときに、出資者からセキュリティ対策要求を求められる場合がある。

https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline_gaiyou.pdf

サイバーセキュリティ対策における留意点

■ インシデントの発生をゼロにすることは不可能

✓ 予防策は重要だが完璧な予防は不可能

例）ゼロデイ攻撃、兆候のない内部不正、過失によるインシデント

■ インシデントの発生を前提とした対策も重要

✓ 被害の拡大を防止し、最小限に抑える

✓ 早期の発見、緊急時対応のルール化とルールに沿った行動

■ ベースラインアプローチ／リスクベースアプローチ

✓ ベースラインとしての最低限の対策

– ソフトウェアのアップデート、不審なメールを開かない

– 情報持ち出しへの対策（アクセス制御、USBメモリの使用制限等）

✓ 組織としてリスク評価、リスクの重大性に応じた対策を実施

– 保有している情報のランク付け及びランクに応じた対策

– 経営に重大な影響を与えるリスクシナリオの検討

セキュリティ対策における最大の弱点

■ 最も脆弱なのは「人」である

- ✓ **常に正常な判断能力を発揮できるのか**

  油断、疲労、「慣れ」による判断能力の低下

- ✓ **全ての従業員がその判断能力を発揮できるのか**

  「まさか自分は当事者にならないだろう」という油断

- ✓ **攻撃者は正常な判断能力を奪うための様々な手段を講じる**

  攻撃者は人を起点とする攻撃の「コスパ」が良いと認識

- ✓ **ヒューマンエラーをなくすことは困難**

  決してなくならないメールの誤送信・記録媒体紛失

- ✓ **人による作業自体がリスク要因となりうる**

  自動化・システム化による対策

2

インシデント対応（対外対応を中心に）

セキュリティインシデント対応の流れ（概要）

■ 自社による検知／第三者からの連絡

- ✓ 一般的に自社による「検知」は困難（数か月気付かないケース）
- ✓ 攻撃のトレンドを理解し、検知又は予防につなげる

  例）海外子会社への攻撃、VPN製品の脆弱性、Emotet

■ トリアージ

- ✓ セキュリティ担当部署（CSIRT等）で事実関係を確認
- ✓ 対応を要するインシデントか否か・対応優先順位を判断

■ インシデント対応の一例

- ✓ 初動対応及び詳細の調査
  - ➢ 被害拡大防止措置（隔離・一部停止等）
  - ➢ 専門機関への相談
  - ➢ 原因究明、影響範囲の特定、証拠保全（フォレンジック調査）
- ✓ 復旧対応
- ✓ 対外対応（当局、警察、取引先、被害者、メディア）
- ✓ 再発防止策の策定、実行

インシデント対応：対外対応サマリー

大まかには以下の３つの類型に分類できる

１．法的拘束力のある義務

（１）法令に基づく義務

（２）契約・約款上の義務

２．ガイドライン等に基づく推奨事項（法的拘束力なし）

３．その他任意の対応

1．法的拘束力のある義務

（1）法令に基づく義務

個人データの漏えい・滅失・毀損（漏えい等）の報告義務	一定の要件を満たす(報告対象事態)個人データの漏えい等について個人情報保護委員会等への報告義務（個人情報保護法26条） ※1公表は「望ましい措置」、ただし本人通知の代替措置に注意 ※2分野別の規定に留意 例）銀行法施行規則13条の6の5の2
特定個人情報の漏えい等の報告義務	一定の要件を満たす特定個人情報（マイナンバーを含む個人情報）の漏えい等について個人情報保護委員会への報告義務（番号利用法29条の4）
業法に基づく事故報告義務	各業法に基づく事故（サイバーセキュリティインシデントを含む）発生時の所管省庁等への報告義務 例）電気通信事業法28条（通信の秘密の漏えい・重大事故）
報告等の求めへの対応義務	➢ 当局から法令に基づく報告等の求めがあった場合、原則として対応する義務あり（情報提供・資料提出の求め等） 例）サイバーセキュリティ基本法17条3項 ➢ 報告徴収をベースとした事故報告義務 例）電気通信事業報告規則7条の3（事故の四半期報告）

1．法的拘束力のある義務

■ （2）契約・約款上の義務

上場会社の適時開示	上場会社（またはその子会社等）においてサイバーセキュリティインシデントが発生し、それが投資判断に著しい影響を及ぼす場合、適時開示が必要（有価証券上場規程（東京証券取引所）402条2項x、403条2項l）
認定個人情報保護団体対象事業者	認定個人情報保護団体（個人情報保護法54条）の対象事業者は、認定団体が定める指針に基づき、認定団体に個人情報の取り扱いに関する事故報告が求められる場合がある 例）JIPDEC個人情報保護指針　※負担軽減の措置あり
プライバシーマーク付与事業者	プライバシーマーク付与事業者は、個人情報に関する事故等の発生時に関係審査機関に報告しなければならない（プライバシーマーク付与に関する規約12条）　※負担軽減の措置あり ※「事故等」の範囲は個人データの漏えい等以外も含む
その他契約に基づく義務	➢ NDA、委託契約、データ取引契約等において、事故発生時等に契約の相手方に報告する義務があるケース ➢ 情報共有体制等の約款において、一定の条件の下での情報提供が求められるケース ※一般論であり、ケースとしては少ないと考えられる

2．法的拘束力はないが推奨される事項

警察への通報／相談等の検討	➢ サイバー犯罪被害者としての対応 ✓ 通報・相談・被害届提出・告訴
重要インフラ事業者による情報連絡	重要インフラ事業者は、重要インフラサービス障害を含むシステムの不具合等に関する情報を所管省庁を通じてNISCに連絡 （重要インフラのサイバーセキュリティに係る行動計画）
不正アクセス等に関する届出	コンピュータウイルス・不正アクセス検知時にIPAへ届出 「コンピュータウイルス対策基準」（平成7年通商産業省告示第429号） 「コンピュータ不正アクセス対策基準」（平成8年通商産業省告示第362号）
脆弱性発見時の届出	汎用性のある製品の脆弱性発見時にIPAへ届出 「ソフトウエア製品等の脆弱性関連情報に関する取扱規程」（平成29年経済産業省告示第19号）
分野別ガイドライン等	個人情報保護関係やセキュリティ関係のガイドラインにおいて、所管省庁等への報告や公表が求められる場合がある 「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針 」 「信用分野における個人情報保護に関するガイドライン」 「医療情報システムの安全管理に関するガイドライン」　等

3．その他任意の対応

■ インシデントに関する相談・情報提供先等

IPA	➢ 情報セキュリティ安心相談窓口 ➢ J-CRAT（サイバーレスキュー隊）
JPCERT/CC	インシデント対応依頼
情報共有体制	➢ サイバーセキュリティ協議会 ➢ J-CSIP（IPA） ➢ CISTA（JPCERT/CC） ➢ 各ISAC　等

■ その他関係者

- セキュリティベンダ
- 保険会社（サイバー保険）
- フォレンジック事業者
- システムの運用・保守事業者
- 委託先・委託元

3

サイバーセキュリティ関連法令の紹介

サイバーセキュリティに関係する法令

- **法令上の「サイバーセキュリティ」の定義がかなり広い**
  - ✓ サイバーセキュリティ関連法令の範囲も広く、毎年のように増加
- **通則法がない**
  - ✓ 事業者に通則的に適用され、具体的に義務等を課すサイバーセキュリティ法令はない　（cf.個人情報保護法）
  - ✓ 現状、様々な法令にサイバーセキュリティに関する規定が散在

例）サイバーセキュリティ関係法令Q&Aハンドブックで言及した法令等の抜粋

サイバーセキュリティ基本法　デジタル社会形成基本法　会社法　民法　個人情報保護法　不正競争防止法　刑法　不正アクセス禁止法　電気通信事業法　電子署名法　電子帳簿保存法　特許法　実用新案法　意匠法　商標法　著作権法　労働基準法　番号利用法　割賦販売法　労働基準法　労働安全衛生法　製造物責任法　国立研究開発法人情報通信研究機構法　情報処理の促進に関する法律　プロバイダ責任制限法　産業競争力強化法　金融商品取引法　外為法　独占禁止法　GDPR　etc…

サイバーセキュリティ経営ガイドライン

- 経済産業省とIPAが策定（2023年3月にver3.0公開）
- サイバーセキュリティ経営の重要10項目（経営者が指示すべき項目）
- 2023年10月に、IPAよりVer3.0実践のためのプラクティス集が公開

指示１	サイバーセキュリティ**リスクの認識、組織全体での対応方針**の策定
指示２	サイバーセキュリティ**リスク管理体制**の構築
指示３	サイバーセキュリティ対策のための**資源（予算、人材等）確保**
指示４	サイバーセキュリティ**リスクの把握とリスク対応に関する計画**の策定
指示５	サイバーセキュリティ**リスクに効果的に対応するための仕組み**の構築
指示６	**PDCAサイクル**によるサイバーセキュリティ**対策の組織的改善**
指示７	インシデント発生時の**緊急対応体制**の整備
指示８	インシデントによる被害に備えた**事業継続・復旧体制**の整備
指示９	ビジネスパートナーや委託先等を含めた**サプライチェーン**全体の状況把握及び対策
指示10	**サイバーセキュリティに関する情報の収集、共有及び開示の促進**

サイバーインシデント発生時の損害賠償

（1）被害企業への損害賠償請求

- 個人データの漏えい　←　本人による慰謝料請求
- 委託元や取引先のデータ等の漏えい←　委託元・取引先による損害賠償請求
- 製品・サービスの利用不能　←利用者からの損害賠償請求

（2）被害企業役員に対する損害賠償請求

被害企業が被った損害（上記損害賠償のほか、企業が負担した復旧費用や事業停止により被った損害等）について、株主代表訴訟による役員に対する責任追及

サイバー攻撃における「被害者」と「加害者」

■ サイバー攻撃の主な関係者間の法的な関係

誰が「加害者」で誰が「被害者」か、誰が法的責任を負うか

	立場	ありうる法的責任
攻撃者	加害者	➢ 被害企業、個人データ主体からの損害賠償が理論的には成立するが、実際に請求を行うことが極めて困難
被害企業	被害者／加害者	➢ サイバー攻撃を受けた被害者 ➢ 情報漏えいがあった場合、その情報主体との関係で加害者となり得る。情報の安全管理に過失があれば責任あり
被害企業役員	被害者／加害者	➢ サイバー攻撃を受けた被害者 ➢ 情報の安全管理体制（内部統制システム）の構築義務違反など、役員としての過失があれば会社への責任あり
漏えい個人データ主体／取引先等	被害者	➢ サイバー攻撃による影響を受けた被害者 ➢ 本来は攻撃者が直接の加害者（賠償請求先）だが、実際の請求が極めて困難→被害企業等への請求

会社法とサイバーセキュリティ

会社法とサイバーセキュリティの関係性
➡ **内部統制システム構築義務**としてのセキュリティリスク管理体制

- **内部統制システムとは**
  会社が営む事業の規模、特性等に応じたリスク管理体制
- **内部統制システムにおける「リスク」**
  - 対応すべきリスクの一つとしてサイバーセキュリティに関することも含まれ得る
- **内部統制システムに関する義務**
  - 大会社等の取締役（会）に内部統制システム構築に関する事項の決定義務（会社法348条3項4号など）
  - それ以外の会社の取締役も、内部統制システムを構築しない場合に、会社に対する善管注意義務・忠実義務違反とされる可能性

サイバーセキュリティと内部統制システム

（1） 決定すべき内部統制システムの類型

- ✓ 法令等遵守体制
- ✓ 損失危険管理体制
- ✓ 情報保存管理体制
- ✓ 効率性確保体制
- ✓ 企業集団内部統制システム

- サイバーセキュリティ体制と内部統制システム
  - サイバーセキュリティリスクの管理：**損失危険管理体制**
  - インシデントに起因する情報漏えいや棄損の防止：**情報保存管理体制**
  - 個人情報保護法等の法令に基づく情報の安全管理：**法令等遵守体制**
  - グループ全体のセキュリティ体制：**企業集団内部統制**

（2） 具体的にどこまで決定する必要があるか

- 内部統制の体制の在り方は、各会社が営む事業の規模や特性等に応じて、その必要性、効果、実施コスト等を勘案して、各会社にて決定

➡ サイバーセキュリティに関する具体例

- セキュリティ規程、個人情報保護規程などの規程類の整備
- CSIRTなどのサイバーセキュリティを含めたリスク管理を担当する部署の構築

義務違反による役員の責任

（3） 義務違反により情報漏えい等が発生した場合の責任

- 内部統制システムの不備によりセキュリティ事故が発生し、会社に損害
  →役員が会社に対する損害賠償責任を負う可能性
  ① 会社に対する責任（会社法423条）
  ② 第三者に対する責任（会社法429条）
- 義務の水準は事業内容や規模等を踏まえた実務の標準によって決まる
- 責任の有無は、社会通念、つまり、企業経営における脅威の高まり、セキュリティ確保の重要性及び企業が果たすべき役割の重要性の高まりといった現状も勘案されると考えられる

◆広島高判令和元年10月18日LEX/DB25564819

「…グループにおいては、事業会社経営管理規程等の各種規程が整備され、それらに基づき、人事や事業計画への関与、グループ全体のリスク評価と検討、各種報告の聴取等を通じた一定の経営管理をし、法令遵守を期していたものであるから、企業集団としての内部統制システムがひととおり構築され、その運用がなされていたといえる。そして、会社法は内部統制システムの在り方に関して一義的な内容を定めているものではなく、あるべき内部統制の水準は実務慣行により定まると解され、その具体的内容については当該会社ないし企業グループの事業内容や規模、経営状態等を踏まえつつ取締役がその裁量に基づいて判断すべきものと解される」

個人情報保護法とサイバーセキュリティ

個人情報保護法とサイバーセキュリティの関係
➡ 個人データの安全管理措置義務、漏えい等への対応義務

- **個人データの安全管理措置義務（23条）**
  - 漏えい、滅失又は毀損その他の安全管理のために必要な措置
  - 漏えい等のリスクに応じた内容の措置をとる必要
- **個人データ漏えい等への対応義務（26条）**
  - 一定の個人データ漏えい等発生時の個人情報保護委員会への報告義務
  - 報告義務と同時に生じる本人への通知義務
- **保有個人データに関する開示と「外的環境の把握」（32条）**
  - 保有個人データの安全管理措置を本人の知りうる状態に置く必要
  - 「外的環境の把握」の関係：個人データを保存している国に注意

個人データの安全管理措置

■ リスクベースの対策が求められる

個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容としなければならない。

■ 具体的な措置

① 基本方針の策定
② 個人データの取扱いに係る規律の整備：③～⑥の内容を織り込んだ規律の整備
③ 組織的安全管理措置：組織体制整備、②に従った運用など
④ 人的安全管理措置：従業者に対する適切な教育
⑤ 物理的安全管理措置
　個人データを取り扱う区画、機器等の盗難防止、電子媒体等の廃棄
⑥ 技術的安全管理措置
　アクセス制御、外部からの不正アクセス防止など
⑦ 外的環境の把握

個人データ漏えい等発生時の対応義務

■ 個人情報保護委員会への報告義務・本人への通知義務

- 一定の要件を満たす個人データの漏えい・滅失・毀損（漏えい等）が発生した場合の**個人情報保護委員会への報告**と**本人通知**義務（26条）
- その他、個人情報取扱事業者は、漏えい等又はそのおそれのある事案（以下「漏えい等事案」という。）が発覚した場合は、漏えい等事案の**内容等に応じて、**次の（1）から（5）に掲げる事項について**必要な措置を講じなければならない。（GL通則編）**

（１）事業者内部における報告及び被害の拡大防止

（２）事実関係の調査及び原因の究明

（３）影響範囲の特定

（４）再発防止策の検討及び実施

（５）個人情報保護委員会への報告及び本人への通知

事実関係及び再発防止策等は、速やかに公表することが**望ましい。**

漏えい等の定義と報告対象事態

- **漏えい・滅失・毀損の定義**（GL通則編）
  - 漏えい：個人データの外部流出
    ○第三者に閲覧されないうちにすべてを回収した場合は漏えい非該当
  - 滅失：個人データの内容が失われること
  - 毀損：個人データの内容が意図せず変更・利用不能
    ○バックアップから復元できる場合は滅失・毀損非該当

- **報告対象事態：漏えい等報告・本人通知を要する事態**（施行規則7条）
  - 要配慮個人情報を含む個人データの漏えい等（医療情報、犯罪被害事実など）
  - 財産的被害が生じるおそれがある個人データの漏えい等（クレジットカード番号、ネットバンキングのID・パスワードなど）
  - 不正な目的をもって行われたおそれのある個人データの漏えい等（外部からのサイバー攻撃、従業員の内部不正）
  - **1,000人を超える個人データの漏えい等**
    - ○　漏えい等**「のおそれ」**がある事態についても対象とする
    - ○　仮名加工情報については報告義務等は課せられない

漏えい等の「おそれ」

■ 漏えい等の「おそれ」の意義（GL通則編）

おそれ：漏えい等が疑われるものの確証がない場合
その時点で判明している事実関係に基づいて**個別の事案ごとに蓋然性を考慮して判断**

- 可能性がある事態全般を指すものではない
- 抽象的な可能性では認められない

■ サイバー攻撃事案における漏えい等の「おそれ」（GL通則編）

- **個人データを格納しているサーバ**等において、**外部からの不正アクセスにより何らかのデータが窃取された痕跡**が認められた場合
- 個人データを格納しているサーバ等において、**情報を窃取する振る舞いが判明しているマルウェアの感染**が確認された場合
- C&Cサーバーが使用しているものとして知られているIPアドレス等**への通信が確認**された場合
- 不正検知を行う公的機関、セキュリティ・サービス・プロバイダ、専門家等の**第三者から、漏えいのおそれについて、一定の根拠に基づく連絡**を受けた場合

報告の手続（施行規則8条）

- **速報**と**確報**の二段階
- 個人情報保護委員会ウェブサイトのフォームでの報告が原則

◆報告の起算点

- 報告対象事態を「知った」とき

法人の場合、いずれかの部署（経営層ではない）が当該事態を知った時点

◆速報：法律上の時間制限なし。3～5日以内が目安（GL通則編）

- 報告事項は、**その時点で把握しているもの**を速報

◆確報：30日以内（サイバー攻撃等の場合は60日以内）

- 報告事項は速報と同様
- **合理的努力を尽くした上で、一部の事項が判明しておらず、全ての事項を報告することができない場合**には、その時点で把握している内容を報告し、判明次第、報告を**追完**するものとする（GL通則編）

本人への通知

■ 本人への通知義務

- 本人への通知は事態の状況に応じて速やかに行う（施行規則10条）
- 本人への通知が困難な場合、権利利益保護のための代替措置が認められる

■ その時点で通知を行う必要があるとはいえない例

- 事案がほとんど判明しておらず、その時点で本人に通知したとしても、本人が権利利益保護措置を講じられず、かえって混乱が生じるおそれ

■ 通知が困難である事例

① 保有する個人データの中に本人の連絡先が含まれていない場合
② 連絡先が古いために通知を行う時点で本人へ連絡できない場合

■ 代替措置の例

① 事案の公表
② 問合せ窓口の設置および連絡先の公表

報告・通知事項

		報告	通知
①	概要（漏えい等の発生日、発覚日、発生事案、発見者、規則第7条各号該当性、委託元及び委託先の有無、事実経過など） **※サイバー攻撃の場合、外部機関による調査実施状況**	○	○
②	漏えい等した（おそれのある）個人データの項目（住所、電話番号、メールアドレス等）	○	○
③	漏えい等した（おそれのある）個人データの本人の数	○	
④	発生原因	○	○
⑤	二次被害又はそのおそれの有無及びその内容	○	○
⑥	本人への対応の実施状況（本人への通知を含む）	○	
⑦	公表の実施状況	○	
⑧	再発防止のための措置　※実施済み／今後実施予定	○	
⑨	その他参考となる事項	○	○

不正競争防止法とサイバーセキュリティ

不正競争防止法とサイバーセキュリティの関係
➡ 営業秘密の保護、限定提供データの保護 など

- **「営業秘密」の保護（不正競争防止法2条6項）**
  - 秘密管理性・有用性・非公知性という3要件を満たす情報に法的な保護が与えられる
  - 侵害行為に対する民事措置、刑事措置
  - 営業秘密管理指針、秘密情報の保護ハンドブック
- **「限定提供データ」の保護（不正競争防止法2条7項）**
  - 限定提供性・相当蓄積性・電磁的管理性という３つの要件を満たす情報に法的な保護が与えられる
  - 侵害行為に対する民事措置（刑事罰はない）

営業秘密：秘密管理性

■ 「営業秘密」の保護を受けるための3要件（不正競争防止法2条6項）

① 秘密として管理されている **（秘密管理性）**

② 事業活動に有用な技術上又は営業上の情報 **（有用性）**

③ 公然と知られていないもの **（非公知性）**

■ 秘密管理性

- 営業秘密保有企業の秘密管理意思が、秘密管理措置によって従業員に対して明確に示され、**従業員が当該秘密管理意思を容易に認識できる**必要
- ベースは秘密管理意思（主観）。秘密管理措置（客観）で意思を従業員に示す
- 刑事事件において秘密管理性を否定して無罪としたものも相応にある

■ 秘密管理性を肯定するための秘密管理措置の典型例

- 秘密情報・機密情報に関する規程類の整備
- データに対する秘密であることの表示（マル秘など）
- 適切なアクセス制御、入退室管理
- 誓約書の提出（入社時・プロジェクト開始時・退職時など）
- セキュリティに関する教育・研修の実施

情報持ち出しを含む内部不正予防のための5つの原則

1. **犯行を難しくする**：対策強化
   - ✓ アクセス制御等の防御策強化、出入り制限・検査、メールやインターネットの監視など
2. **捕まるリスクを高める**：管理、監視の強化
   - ✓ 監視の強化（技術・物理）、ID管理（匿名性を減らす）、通報制度整備、単独作業の制限など
3. **犯行の見返りを減らす**：「割に合わない」ようにする
   - ✓ アクセス権限設定、データの完全消去、暗号化など
4. **犯行の誘因を減らす**：犯罪を行う気持ちにさせない
   - ✓ 公正な人事評価、適正な労働評価、円滑なコミュニケーション推進など、模倣犯の阻止
5. **犯罪の弁明をさせない**：犯人による行為の正当化理由を排除
   - ✓ 規程類の整備、指示の掲示、コンプライアンス強化など

＜参考＞　情報処理推進機構（IPA）「組織における内部不正防止ガイドライン」（第5版）（2022年4月改訂）
付録VI：内部不正防止の基本5原則と25分類

ご清聴ありがとうございました