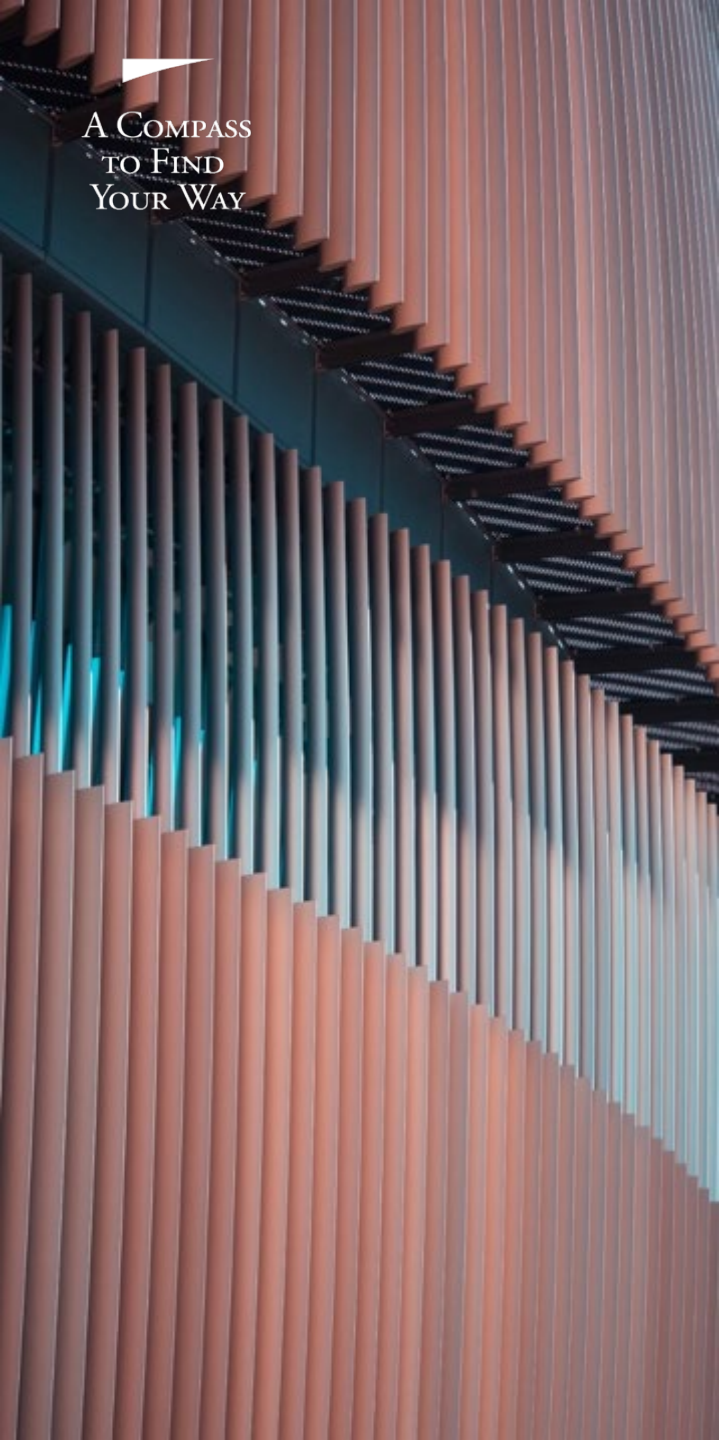

渥美坂井法律事務所・外国法共同事業

サイバーセキュリティの有事・平時の対応と役員の責任

弁護士　松岡　史朗
パートナー

Atsumi & Sakai

本日のセミナーの趣旨

サイバーセキュリティの平時の対応は非常に不十分

例①：重要インフラ分野の事業者でも、経営層との定期的なレポーテリングは18.8%のみ。

例②：リスクが経営会議に付議されていない会社は46.5%にのぼる（重要インフラにおける安全基準等の浸透状況等に関する調査について（2021年度）p41）。

サイバーセキュリティインシデント発生

平時の対応をせずにサイバーセキュリティインシデントが生じた場合、役員責任が発生

「情報セキュリティについての企業内での体制の整備は、会社法でいう内部統制システムの構築・運用の一部をなす」「企業価値の保全、企業の社会的責任のいずれの観点からも、情報セキュリティ体制は喫緊の課題といえる」（大杉謙一教授「月刊監査役No.739p3（羅針盤）」）

役員責任が生じないようにするためには、十分な平時の対応が必要

平時の対応を検討するためには、有事の対応の把握が必要

システム、個人情報保護法、会社法が関係するので、複雑

目次

1. 情報セキュリティ10大脅威2022

独立行政法人情報処理推進機構　IPA（Information-technology Promotion Agency）
情報セキュリティ10大脅威2022

1位	ランサムウェアによる被害
2位	標的型攻撃による機密情報の窃取
3位	サプライチェーンの弱点を悪用した攻撃
4位	テレワーク等のニューノーマルな働き方を狙った攻撃
5位	内部不正による情報漏えい
6位	脆弱性対策情報の公開に伴う悪用増加
7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
8位	ビジネスメール詐欺による金銭被害
9位	予期せぬIT基盤の障害に伴う業務停止
10位	不注意による情報漏えい等の被害

Source: https://www.ipa.go.jp/security/vuln/10threats2022.html

2. インシデントが生じた場合の対応（有事対応）

1 個人情報保護委員会への速報
（個人情報保護法ガイドライン（通則編）3－5－3－3）

個人情報取扱事業者は、報告対象事態を知ったときは、速やかに、個人情報保護委員会に報告しなければならない。・・・報告期限の起算点となる「知った」時点については、個別の事案ごとに判断されるが、個人情報取扱事業者が法人である場合には、いずれかの部署が当該事態を知った時点を基準とする。「速やか」の日数の目安については、個別の事案によるものの、個人情報取扱事業者が当該事態を知った時点から概ね3～5日以内である。

POINT

（１）令和2年改正により法的義務化
（２）「3～5日以内」の厳しい期限

2. インシデントが生じた場合の対応（有事対応）

2 個人情報保護委員会への確報（個人情報保護法ガイドライン（通則編）3－5－3－４）

個人情報取扱事業者は、報告対象事態を知ったときは、速報に加え（※1）、30日以内（規則第7条第3号の事態においては60日以内。同号の事態に加え、同条第1号、第2号又は第4号の事態にも該当する場合も60日以内。）に個人情報保護委員会・・・に報告しなければならない。

POINT

1. 確報の期限は30日または60日。この期限までに原因究明のための調査及び調査結果に基づく再発防止策（例：システムの強化、内部規程・ポリシーの改訂・作成・実務の見直し、契約書の雛形の作成）の策定が必要。
2. 「規則第７条第３号」＝不正の目的をもって行われたおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態
   具体例（個人情報保護法ガイドライン（通則編）3－5－3－１）
   1）不正アクセスにより個人データが漏えいした場合
   2）ランサムウェア等により個人データが暗号化され、復元できなくなった場合
   3）個人データが記載又は記録された書類・媒体等が盗難された場合
   4）従業者が顧客の個人データを不正に持ち出して第三者に提供した場合

▶サイバーセキュリティインシデントの場合は、60日の場合が多い。

2. インシデントが生じた場合の対応（有事対応）

3 本人への通知の時間的制限（個人情報保護法ガイドライン（通則編）3－5－4－2）

個人情報取扱事業者は、報告対象事態を知ったときは、当該事態の状況に応じて速やかに、本人への通知を行わなければならない。
「当該事態の状況に応じて速やかに」とは、速やかに通知を行うことを求めるものであるが、具体的に通知を行う時点は、個別の事案において、その時点で把握している事態の内容、通知を行うことで本人の権利利益が保護される蓋然性、本人への通知を行うことで生じる弊害等を勘案して判断する。

【その時点で通知を行う必要があるとはいえないと考えられる事例（※）】
事例1）インターネット上の掲示板等に漏えいした複数の個人データがアップロードされており、個人情報取扱事業者において当該掲示板等の管理者に削除を求める等、必要な初期対応が完了しておらず、本人に通知することで、かえって被害が拡大するおそれがある場合
事例2）漏えい等のおそれが生じたものの、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、本人がその権利利益を保護するための措置を講じられる見込みがなく、かえって混乱が生じるおそれがある場合

POINT

本人による損害賠償請求とのバランス

2. インシデントが生じた場合の対応（有事対応）

4 本人への通知の例外
（個人情報保護法ガイドライン（通則編）3－5－4－5）

本人への通知を要する場合であっても、本人への通知が困難である場合は、本人の権利利益を保護するために必要な代替措置を講ずることによる対応が認められる。

【代替措置に該当する事例】
事例1）事案の公表
事例2）問合せ窓口を用意してその連絡先を公表し、本人が自らの個人データが対象となっているか否かを確認できるようにすること

代替措置として事案の公表を行わない場合であっても、当該事態の内容等に応じて、二次被害の防止、類似事案の発生防止等の観点から、公表を行うことが望ましい。

POINT

本人の権利利益保護と会社のレピュテーションとのバランス

3. 内部統制システム整備義務と平時の対応

1 内部統制システム整備義務

会社の取締役は、善管注意義務・忠実義務の一内容として、会社の業務の適正な確保するために必要な体制（内部統制システム）の整備をする義務を負う（大阪地判平成12年9月20日判時1721号3頁〔大和銀行事件〕、最判平成21年7月9日判時2055号147頁〔日本システム技術事件〕）。
内部統制システムを整備していない場合、任務懈怠に基づく損害賠償責任（会社法423条）を問われ得る。

2 内部統制とサイバーセキュリティ

会社法348条3項4号は、「取締役の職務の執行が法令及び定款に適合することを確保するための体制その他株式会社の業務」の適正を確保するために必要な体制の整備に関して、取締役会で決議することを義務づけている。
この「必要な体制」の中には、情報保存管理体制、損失危険管理体制、効率性確保体制、法令等遵守体制、企業集団内部統制が含まれる（会社法施行規則100条）。
サイバーセキュリティに関する平時の対応は、情報保存管理体制、損失危険管理体制、法令等遵守体制に関係。

POINT

サイバーセキュリティに関する平時の対応がなされない場合、
任務懈怠に基づく損害賠償責任を問われ得る

4. 内部統制システム整備義務と裁判例

大阪地判平成12年9月20日判時1721号3頁〔大和銀行事件〕

A銀行NY支店の従業員Xが、トレーディングの失敗による損失を補填すべく、「預かり証券」を無断で売買した事案

- A銀行は、B銀行に「預かり証券」の再保管を委託しており、B銀行は定期的にA銀行NY支店に「預かり証券」の残高証明書をNY支店に送付していた。
- 従業員Xは、残高証明書を改ざん
- A銀行NY支店では、定期的に、内部監査部門、監査役および会計監査人による監査。この監査では、改ざん後の残高証明書とNY支店の帳簿の照合にとどまり、B銀行に対して直接残高を確認するものではなかったため、無断売買は判明しなかった。
- NY支店の支店長であった取締役について、内部統制システム整備義務違反を認めた。

POINT

1. 内部不正により、取締役の内部統制システム整備義務違反ありとされた
2. 内部不正は、IPAの情報セキュリティ10大脅威の常連であり、少なくとも内部不正によるサイバーセキュリティインシデントに平時から対応していない場合、内部統制システム整備義務違反となる

4. 内部統制システム整備義務と裁判例

最判平成21年７月９日判時２０５５号１４７頁〔日本システム技術事件〕

従業員らが架空の売上げを作出し、有価証券報告書に不実の記載がなされた事案

- 会社の取締役に従業員らによる架空売上げの計上を防止するためのリスク管理体制構築義務違反があるか否かが問題
- 会社は、職務分掌規程等を定めて事業部門と財務部門を分離し、事業部について、営業部とは別に注文書や検収書の形式面の確認を担当するBM課及びソフトの稼働確認を担当するCR部を設置し、それらのチェックを経て財務部に売上報告がされる体制を整え、監査法人との間で監査契約を締結し、当該監査法人及び財務部が、それぞれ定期的に、販売会社あてに売掛金残高確認書の用紙を郵送し、その返送を受ける方法で売掛金残高を確認することとしていた
  ➡ 通常想定される架空売り上げの計上等の不正行為を防止し得る程度の管理体制は整えていたものということができる
- 本件の架空の売上げの作出は、事業部部長と部下が共謀して、販売会社の偽造印を用いて注文書等を偽造し、BM課の担当者を欺いて財務部に架空の売上報告をさせ、監査法人及び財務部が販売会社あてに郵送した売掛金残高確認書の用紙を未開封のまま回収し、偽造印を押捺した用紙を監査法人または財務部に送付し、会社の売掛金額と販売会社の買掛金額が一致するように巧妙に偽装するという、通常容易に想定し難い方法によるものであった
- 本件の架空の売上げの作出の発生を予見すべきであったという特別な事情も見当たらない
- リスク管理体制を構築すべき義務に違反した過失があるということはできない

POINT

1. 内部規程の整備、事業部以外の部門・監査法人の実務の重要性
2. 「通常の不正行為を防止し得る」と「特別な事情」という基準

5. 裁判例に鑑みた場合に求められる平時の対応

サイバーセキュリティに関して整備すべき体制を検討する際には、以下の点を考慮する必要がある

観点1

- 「通常想定されるサイバーセキュリティインシデントを防止し得る程度の管理体制の整備」が必要

  - 日本システム技術事件の事案は、従業員による架空売上げ作出
  - この事案に応じて「通常想定される架空売り上げの計上等の不正行為を防止し得る程度の管理体制は整えていた」と判示

観点2

- インシデントが生じた場合の被害の最小化（会社の情報資産及びレピュテーション、本人の経済的利益に対する被害を最小化）
  ※ サイバーセキュリティインシデントの場合、インシデント後の対応が被害の大きさに影響（cf. 従業員による架空売上げ作出）

観点3

- 個人情報保護法や個人情報保護委員会などのガイドラインの遵守
  ※ サイバーセキュリティに関しては、詳細な関連法令が存在（cf.従業員による架空売上げの作出）

観点4

- システム部門から経営層への報告において、インシデントを予見すべき事実関係や改善すべきシステムがあれば、積極的に検討する必要
- 自社のみならず、同業他社においてインシデントが生ずれば、同様のインシデントが生じないように対応する必要

  - 日本システム技術事件の「本件の架空の売上げの作出の発生を予見すべきであったという特別な事情」の判示は、サイバーセキュリティに関する体制にもあてはまる

5. 裁判例に鑑みた場合に求められる平時の対応

1 システムの運用・保守

システムの脆弱性対応

- 一般的な脆弱性情報を把握
- 定期的な脆弱性テスト・ペネトレーションテスト
- 速やかかつ適切なパッチの適用

バックアップ

- 「インシデントの場合にもデータを利用可能とする」という観点から重要
- ストレージの容量及びコストが問題、また、バックアップが漏えいする危険

監視

- システムが停止しないように異常の早期発見

ログの取得・保管

- インシデントの後の事実解明や訴訟等の重要な証拠となる。
- バックアップと同様に長期の保管には問題を伴う。

適正なデータ・ハードウェアの廃棄

- 適正に廃棄しなければ、データの漏えいの危険

5．裁判例に鑑みた場合に求められる平時の対応

2 委託先との契約

サイバーセキュリティインシデントは、委託先を原因として生じることが多い

1 委託契約書雛形の準備

- 個人データの国外移転の規律
- 外国会社の雛形

2 委託契約の期間に関する契約条項

委託契約中に委託先に何らかの行為を委託先に求める場合、契約条項に記載しておく必要

例：
- 監査
- インシデント対応

3 再委託、再々委託の場合の条項

再委託、再々委託の利用を委託元として、どのような場合に認めるか

- 再委託先、再々委託先が負う義務
- 再委託先、再々委託先のアクセス権限

5. 裁判例に鑑みた場合に求められる平時の対応

3 社内規程の整備・運用

責任者・責任部門の権限の規定

- システム部門と総務部門・法務部門の役割分担 ※1
- システム部門によるリスクの把握・特定
- システム部門から経営層に対する報告 ※2

改正個人情報保護法対応

- 社内規程が改正法に対応していない場合、社内規程を遵守していたとしても、違法となるおそれがある
- 個人データの漏えい、個人データの国外移転、個人関連情報

※1 日本システム技術事件の判旨を参照
（「会社は、職務分掌規程等を定めて事業部門と財務部門を分離し、事業部について、営業部とは別に注文書や検収書の形式面の確認を担当するBM課及びソフトの稼働確認を担当するCR部を設置し、それらのチェックを経て財務部に売上報告がされる体制を整え」）

※2 重要インフラにおける安全基準等の浸透状況等に関する調査について（2021年度）
（重要インフラ分野の事業者でも、経営層との定期的なレポーテリングは18.8%のみ。リスクが経営会議に付議されていない会社は46.5%にのぼる）。
日本システム技術事件の判旨を参照
（「本件の架空の売上げの作出の発生を予見すべきであったという特別な事情」）

5. 裁判例に鑑みた場合に求められる平時の対応

3 社内規程の整備・運用

個人情報保護法以外の関連法対応

- 例：マイナンバー法
- 重要な国内法であるにも関わらず、反映されていないケースが散見

海外法対応

- 社内規程が海外法を反映していない場合、社内規程を遵守していたとしても、海外法違反となるおそれがある
- 例：GDPR、中国個人情報保護法、CCPA・CPRA

改正法以外の新しいガイドラインなどへの対応

- 例：カメラ画像利用

※3

※3 デリバティブ取引に関するリスク管理体制が問われた東京地判平成16年12月16日判例タイムズ1174号150頁（ヤクルト事件東京地裁判決）を参照（「リスクの把握や構築すべきリスク管理体制の内容、さらにはリスクを踏まえてどのような措置をとるべきかは、リスクが顕在化して生じる様々な損失事例の蓄積や、リスク管理に関する実務上ないし行政上の研究・指導の発展によって充実していくものである」）

5. 裁判例に鑑みた場合に求められる平時の対応

4 従業員の教育

日本DPO協会認定データ保護実務者

「日本のデータ保護実務家には日本の個人情報保護法を土台としながらも、それを超えた幅広い分野に対する知識と能力が求められています。」
https://dpo.or.jp/certification/

公式教科書

プライバシーの基礎、マイナンバー法、コンプライアンスの実務対応、GDPR、中国個人情報保護法も含む。
https://dpo.or.jp/exam-text/

認定教育事業者

https://www.aplawjapan.com/news-events/20221110

ご清聴いただき
誠にありがとうございました

お問い合わせ

弁護士　松岡　史朗

（第一東京弁護士会）

E-mail:

fumiaki.matsuoka@aplaw.jp

渥美坂井法律事務所･外国法共同事業
〒100-0011　東京都千代田区内幸町2-2-2
富国生命ビル（総合受付 16階）
Tel: 03 5501 2111（代表）　Fax: 03 5501 2211

※ 本セミナーの内容は、一般的な情報提供を目的としており、個別案件についての法的助言ではありません。お問い合わせ等は、上記弁護士までご連絡くださいますようお願い申し上げます。

当事務所に関するリーガル・ノーティス

1.渥美坂井法律事務所・外国法共同事業について

渥美坂井法律事務所・外国法共同事業（当事務所）は、①渥美坂井法律事務所弁護士法人（第二東京弁護士会所属、代表社員弁護士渥美博夫）（以下「当弁護士法人」といいます。）と当事務所に所属する多くの外国法事務弁護士とが、外国弁護士による法律事務の取扱いに関する特別措置法（以下「外弁法」といいます。）に定める外国法共同事業を行い、②当弁護士法人と、日本の民法上の組合である渥美坂井法律事務所・外国法共同事業（代表弁護士坂井豊）（以下「組合組織」といいます。）の各弁護士とが、共同事業を行い、法律事務所を共にするものです。さらに当弁護士法人と、組合組織の各弁護士は、ヤンセン外国法事務弁護士事務所のマークース・ヤンセン外国法事務弁護士（ドイツ連邦共和国法）と外弁法に定める外国法共同事業を行います。 当事務所とその外国法共同事業は、日本の弁護士（イングランド及びウェールズ事務弁護士である者を含みます。）に加え、ニューヨーク州、カリフォルニア州、インド、オーストラリア クインズランド州の法を原資格国法とする外国法事務弁護士を擁しています。州法を原資格国法とする外国法事務弁護士はその国の連邦法についても助言を提供することができます。当事務所では、弁護士と、それぞれの登録に係る原資格国法に関する法律事務を行うことを職務とする外国法事務弁護士とが協働して業務を行っています。

当弁護士法人はまた、ロンドンオフィスとして英国子会社たるAtsumi & Sakai Europe Limited（Director: 金久直樹日本国弁護士）を有するとともに、ニューヨーク提携オフィスとしてAtsumi & Sakai New York LLP（代表パートナー：バニー・L・ディクソン外国法事務弁護士（ニューヨーク州法））を有し、これらのオフィスを通じても助言を提供しています。また日本においてA&S福岡法律事務所弁護士法人（パートナー：臼井康博弁護士）と提携関係を有するとともに、フランクフルトオフィスたるドイツ連邦共和国における法務・税務サービス提供法人たるAtsumi & Sakai Europa GmbH - Rechtsanwälte und Steuerberater（現地代表：フランク・ベッカー ドイツ連邦共和国弁護士及び花岡美幸 ドイツ連邦共和国税理士）とも提携関係を有しています。

2.法律問題に関する助言等について

当事務所による別段の明示がない限り、法律問題に関する当事務所のいかなる助言その他意見の表明も、(i) 日本法、又は当事務所の外国法事務弁護士の登録に係る原資格法以外の外国法に関するものは当事務所の特定された弁護士の、(ii) かかる原資格国法に関するものは当該法をその登録に係る原資格国法とする当事務所の特定された外国法事務弁護士の、判断においてされるものです。