Smith Gambrell Russell

企業を取り巻くサイバーリスク
～現状とベスト・プラクティス～

配信：2023年2月8日

SGR法律事所　弁護士　小島　清顕・木村 勇人

SGR

講師紹介　Smith, Gambrell & Russell, LLP（SGR）

いつでもお気軽にお問い合わせください。

小島　清顕
Kiyoaki (Kiyo) Kojima
Partner

Smith, Gambrell & Russell, LLP
Address Suite 1000
1105 W. Peachtree St. N.E.
Atlanta, GA 30309
Telephone 404-815-3893
E-mail kkojima@sgrlaw.com

小島清顕 名刺
Eight QRコード

【経歴】
日本出身。実家は神奈川県、小田原市。幼少期から米国在住。ロチェスター大学で政治学・経済学、同時期にイーストマン音楽学校にてファゴットを学ぶ。二重学位取得後、インディアナ大学ロースクールと音楽校に同時進学。JD取得後、2003年からホームタウンのジョージア州アトランタ市を拠点に米国各地で弁護士業務を営む。

法人設立・再編やコンプライアンス、M&A・JV等各種取引アドバイス、雇用・労務案件、ポリシー作成、紛争対応（特に調停と仲裁）、企業誘致・土地選定・助成金の交渉と文書化、その他各種法務に対応。

＜その他所属＞（着任時系列順）
- 経産省 Healthcare Innovation Hub（通称:InnoHub）アドバイザー
- 厚生省MEDISO 非常勤サポーター
- JETRO 中小企業海外展開現地支援プラットフォーム
- Greater Tokyo Innovation Ecosystem GAP ファンドプログラム
- 東北グローバルアクセラレーション(TGA) スタートアップ支援

SGR

講師紹介　Smith, Gambrell & Russell, LLP（SGR）

木村　勇人
Hayato Kimura
Exchange Attorney

Smith, Gambrell &Russell LLP
Address Suite 1000
1105 W. Peachtree St. N.E.
Atlanta, GA 30309
E-mail hkimura@sgrlaw.com

【Career】
日本出身（茨城県土浦市）。2009年東京大学教養学部卒業、2011年東京大学法科大学院修了。2012年弁護士登録。同年より渥美坂井法律事務所・外国法共同事業にて執務、2021年同事務所パートナー昇格。

不動産ファイナンス、銀行業務、証券化、再生可能エネルギー、事業再生、国内外の訴訟対応等を主たる業務分野として対応。

2022年米国ミシガン大学ロースクール（LL.M.）修了。2022年8月より、SGR法律事務所にて交換弁護士として執務。

主要著作として、『TMKの理論と実務【改訂版】―特定目的会社による資産の流動化』（金融財政事情研究会、2021年）。

SGR

本講演の概要

SGR

Smith Gambrell Russell

I. 会社を取り巻くサイバーリスクの現状

SGR

I. 会社を取り巻くサイバーリスクの現状

- 米国はサイバー攻撃の「**激戦区**」
  - ✓ サイバー攻撃の**頻度**や**金額規模**が増加するのはもちろん、手法も極めて**高度化**
  - ✓ ランサムウェア攻撃の結果、企業が数百～数千万ドル規模の「**身代金**」を支払うに至る事件も多数発生（後述の実例参照）
  - ✓ 犯罪組織のみならず、政府機関もその展開に関与しているとされ、現代社会において、もはや回避できない「**Business Reality**」となっている
- 企業にとって「**IF**」ではなく「**WHEN**」の問題に
  - ✓ 「**起きないようにどうするか**」も重要であるが、「**起きてしまった場合にどうするか**」について具体的な回答を用意しておく必要あり
  - ✓ 米国において事業を遂行する場合は「対岸の火事」とはいえず、また、日本が米国のようなサイバー攻撃**「激戦区」にならない保証はどこにもない**

I. 会社を取り巻くサイバーリスクの現状

❑ 米国におけるサイバー攻撃対策の「勘所」

1. Awareness of Legal Risks by Board and Management
   ☞ サイバー攻撃を取り巻く**法的リスクを経営陣が正しく把握**すること
   - **なぜ経営陣**にとってのリスクになるのか／どのような場合に**個人責任**に発展するのか

2. Administrative & Technological Safeguards
   ☞ 企業における**適切な防衛策**の整備
   - 個々人／組織としての防衛策の**周知徹底**
   - 技術面でのサポート

3. Best Practices in Responding to Incidents & Recommended Procedures
   ☞ 有事対応の「**Best Practice**」～平時の準備／心構えの重要性
   - 有事に「**何をすべきか**」の事前把握と実務上の注意点
   - 米国特有の事情（ディスカバリー制度や証拠保全義務）
   - 有事の発生を見越した平時からの**意識付け**の重要性

Smith Gambrell Russell

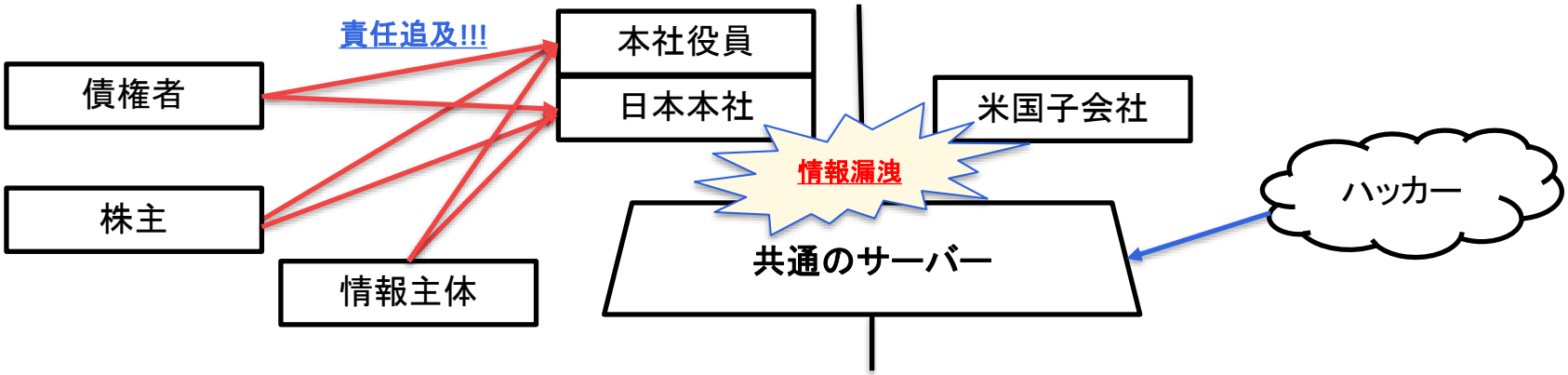
II.サイバーリスクに伴う会社の法的責任

SGR

II.米国法人の責任と日本法人の責任
～米国子会社のリスク=日本本社のリスク～

- 米国（海外）子会社のリスク＝日本親会社のリスク
  - ✓ 米国（海外）子会社と**共有している日本の顧客情報**の窃取
  - ✓ 米国（海外）子会社を入口とした**日本親会社サーバーへの侵入**

☞日本親会社による、**米国（海外）子会社の管理責任**（グループガバナンス）



II. 取締役会及び役員の責任

- ❑ サイバーリスクと取締役会及び役員の責任がどのように関係するか
  - ✓ 企業（経営陣）の責任：**企業活動に通常内包されるリスク**を**認識**し、**回避**する
    - サイバー攻撃との関係での**リスク**：例えば以下の事情はリスク要素
      - システム・サイバーセキュリティに関する社内体制／情報管理体制の脆弱性
      （例：第三者に機密情報等を共有している場合の契約書上の手当の薄さ等）
    - リスクの「認識」：
      - 「知らなかった」では済まない⇒「**知りうべき**／**認識すべき**」リスクは責任範囲と考えるべき
      - 「知りうべき／認識すべき」範囲は日々変わりゆくもの＝義務範囲の拡大
        - サイバー攻撃が「日常化」する中で**認識すべき範囲は拡大**している
    - 回避措置の実施：
      - 想定されるリスクを前提とした**具体的な施策**を講じることが求められる
      （例：「システムの脆弱性による外部侵入」リスク　⇒　「脆弱性の解消」が義務内容）
  - ✓ これらを怠った場合、「**善管注意義務違反**」として経営陣の責任が発生！

II. 取締役会及び役員の責任発生例

- ❑ 具体例1：HDDへの**物理的アクセス**
  - ❖ 個人向け介護サービスを展開するA社：**社内の特定PC**を使用
  - ❖ PCを保管している部屋へは従業員・関係者は誰でも出入り可能な状態（**リスク**）
  - ❖ 特段物理的アクセスを制限する措置はとられないまま放置（回避措置の**懈怠**）
  - ❖ ある日**PCが盗難されるも、誰が持ち出したかは不明。顧客のプライバシー侵害**
- ❑ 具体例2：受託先での**情報漏洩**
  - ❖ 保険サービスを提供するB社は、**商品のポータルサイトの運営を外部業者に委託**
  - ❖ 契約書上、サイバーセキュリティに関する義務について明確な規定なし（**リスク**）。
  - ❖ B社は**契約書の見直しや保険加入を行わず**、サーバーの脆弱性等を確認しなかった（回避措置の**懈怠**）
  - ❖ **サーバーに外部第三者が侵入、個人情報が漏洩**

II. いかにして責任を回避する？

- 構造のおさらい‥経営陣の責任＝リスクを前提とした回避措置実施
  - ✓ **責任**＝認識すべきであった「**常識**」×これに伴う「**リスク**」
- リスクを低減するために‥社内体制整備の必要
  - ①セキュリティに関する事案発生防止を志向した**危機管理体制**
  - ②有事を想定した**事前準備**　（※サイバーセキュリティ／その他保険加入を含む）
  - ③迅速かつ適格な**有事対応**
- 危機管理体制：前提としての組織的な「**心構え**」の構築
  - ①**取締役の役割**として明確化：取締役の監督すべきトピック
  - ②取締役会・経営会議での**議題化**：自社の状況を確認
  - ③**関連法人間の調整行程**：グループガバナンス：承認制度の採用

III. 実務上の「事前対策」

III. 実務上の事前対策～組織上の対策～

- **人材教育**:「Proper Practice with Your People!」
  - ✓ 現場担当者
    - 定期的な**講習**の実施(Eラーニング、セミナー等の講習会への参加義務付け)
    - 日常的な**トレーニング**(例:仮想フィッシングメールへの従業員の対応をチェック)
  - ✓ 管理部門(役員・管掌部門の上長):上記に加えて
    - 有事対応の体制構築
      - **対内的な指示**／**対外的な説明**・**報告**
    - 具体的な**シミュレーション**
  - ✓ 外部との連携:
    - セキュリティのプロフェッショナル・法律専門家による講習実施
    - 有事に迅速に相談できる**関係性の構築**

III.実務上の事前対策～組織上の対策～

- 内部規定の整備:「Policies」
  - ✓ **外部規定**(例:Privacy Policy)のみでは不十分
  - ✓ Information Security Policy等の内部規定を整備～以下を規定:
    - ❖ 従業員／担当者の**一般的責務**
    - ❖ **適用対象**となる情報等の画定
    - ❖ 具体的なセキュリティ対策の内容(**取扱方法**／**禁止事項の設定**)
    - ❖ **有事対応**(情報漏洩等の発生時の対処手順等)
    - ❖ **社内教育**その他一般的な事項　等
- 契約条項の見直し
  - ✓ 第三者に提供している**機密情報の安全**が**契約上確保**されているか
  - ✓ 有事の場合の**当事者間の責任分担**の確認

III.実務上の事前対策～内部規程（例）～

- サイバーセキュリティに関する内部規程（サンプル）
  - ✓ **従業員／担当者の一般的責務**
    ⇒以下のような一般的な責務の他、各社担当部署やサイバーセキュリティに関する**委員会を設置**し、役割を具体化

SAMPLE

■General Duty
All Company employees, agents, and representatives (“**Company Personnel**”) must use security measures designed for protection of **Information Assets** that are based on best practices principles to: (i) **identify potential threats and other risks to Information Assets** and (ii) **resolve them as early as practicable upon discovery of all such potential threats**. As soon as such potential threats are identified, Company Personnel must immediately notify his/her supervisor of such threats and seek guidance so that [XXXX（担当部署）] may be able to analyze such threats, implement best practices, and work with critical vendors, legal counsels and industry experts, if necessary, in order to prevent a breach of **Confidential Information** and/or protect the Company’s Information Assets through encryption or other appropriate means.

※“Information Assets”は情報資産を指すものとして別途定義
例：any data related to the Company’s assets, business, information systems, or personnel, together with the development, implementation, maintenance, or operation of such Company assets
※適用対象を画定する“Confidential Information”の設定は**会社ごとに検討**（参考例は次頁）

III.実務上の事前対策～内部規程（例）～

- サイバーセキュリティに関する内部規程（サンプル）
  - ✓ **従業員／担当者の一般的責務**

■**General Duty**	■**一般的な義務**
All Company employees, agents, and representatives ("Company Personnel") must use security measures designed for protection of Information Assets that are based on best practices principles to: (i) identify potential threats and other risks to Information Assets and (ii) resolve them as early as practicable upon discovery of all such potential threats. As soon as such potential threats are identified, Company Personnel must immediately notify his/her supervisor of such threats and seek guidance so that [XXXX（担当部署）] may be able to analyze such threats, implement best practices, and work with critical vendors, legal counsels and industry experts, if necessary, in order to prevent a breach of Confidential Information and/or protect the Company's Information Assets through encryption or other appropriate means.	当社のすべての従業員、代理人、及び代表者（以下「当社従業員」）は、(i)情報資産に対する潜在的脅威及びその他のリスクを特定し、(ii)そのような潜在的脅威が発見されたら、できるだけ早くそれを解決するために、情報資産を保護するために設計された、ベストプラクティスの原則に基づくセキュリティ対策を取らなければならない。このような潜在的な脅威が確認された場合、機密情報の侵害を防ぎ、暗号化やその他の適切な手段で当社の情報資産を保護できるよう、[XXXX（担当部署）]がその脅威を分析し、ベストプラクティスを実施し、必要に応じて重要なベンダー、法律顧問、業界の専門家と協力ができるように、当社従業員は、当該脅威を直ちに上司に報告し、指導を求めなければならない。

III.実務上の事前対策～内部規程（例）～

- サイバーセキュリティに関する内部規程（サンプル）
  - ✓ **適用対象**

    ⇒サイバーセキュリティで何を守るのか？という観点から、どのような情報を自社が事業遂行上取得し、それらはどのように分類可能かという検討が必要

SAMPLE

■“**Confidential Information**”の例
Confidential Information is **information that may cause harm to the Company, its customers/clients, employees, or other entities or individuals if improperly disclosed**, or that is not otherwise publicly available. Harms may relate to an individual's privacy, the Company's marketplace position or that of its customers/clients, or legal or regulatory liabilities.

■ (より繊細な取扱いを要するカテゴリとして“**Highly Confidential Information**”を設定する場合)
Highly Confidential Information is **information that may cause serious and potentially irreparable harm to the Company, its customers/clients, employees, or other entities or individuals if disclosed or used in an unauthorized manner**.
Highly Confidential Information is a subset of Confidential Information that requires additional protection.

■(適用対象とならないカテゴリ（**Public Information**）についても具体的に定義することが有用)
Public Information is **information that the Company has made available to the general public**. Information received from another party (including a customer/client) that is covered under a current, signed non-disclosure agreement must not be classified or treated as Public Information

III.実務上の事前対策～内部規程（例）～

- サイバーセキュリティに関する内部規程（サンプル）
  - ✓ **適用対象**
    ⇒一般的な“**Confidential Information**”の規程例

■“Confidential Information”の例	■“Confidential Information”の例
Confidential Information is information that may cause harm to the Company, its customers/clients, employees, or other entities or individuals if improperly disclosed, or that is not otherwise publicly available. Harms may relate to an individual's privacy, the Company's marketplace position or that of its customers/clients, or legal or regulatory liabilities.	Confidential Informationとは、不適切に開示された場合、当社、当社の顧客/クライアント、従業員、その他の事業体若しくは個人に損害を与える可能性がある情報、又は、一般に入手できない情報のことをいう。損害は、個人のプライバシー、当社又は当社の顧客/クライアントの市場での地位、又は法的若しくは規制上の責任に関係するものをいう。

III.実務上の事前対策～内部規程（例）～

- サイバーセキュリティに関する内部規程（サンプル）
  - ✓ **適用対象**
    ⇒より繊細な取扱いを要するカテゴリとして“**Highly Confidential Information**”を設定する場合

■**Highly Confidential Information**	■**Highly Confidential Information**
Highly Confidential Information is information that may cause serious and potentially irreparable harm to the Company, its customers/clients, employees, or other entities or individuals if disclosed or used in an unauthorized manner. Highly Confidential Information is a subset of Confidential Information that requires additional protection.	Highly Confidential Informationとは、許可されていない方法で開示又は使用された場合、当社、当社の顧客/クライアント、従業員、その他の事業体若しくは個人に重大かつ回復不可能な損害を与える可能性のある情報をいう。 Highly Confidential Informationとは、追加的な保護を必要とするConfidential Informationの一部となる。

III.実務上の事前対策～内部規程（例）～

- サイバーセキュリティに関する内部規程（サンプル）
  - ✓ **適用対象**

    ⇒適用対象とならないカテゴリ（Public Information）についても具体的に定義することが有用

■**Public Information**	■**Public Information**
Public Information is information that the Company has made available to the general public. Information received from another party (including a customer/client) that is covered under a current, signed non-disclosure agreement must not be classified or treated as Public Information	Public Informationとは、当社が一般に公開した情報をいう。 他の当事者（顧客/クライアントを含む。）から受領した情報で、現在締結されている秘密保持契約の対象となっているものは、Public Informationとして分類し、又は、取り扱ってはならない。

III.実務上の事前対策～内部規程（例）～

- サイバーセキュリティに関する内部規程（サンプル）
  - ✓ 具体的なセキュリティ対応：情報の重要性に応じた取扱いが必要
  - ✓ Highly Confidential Informationの取扱例（一部）は以下のとおり

SAMPLE

■Authentication: 電子的に保管されたHighly Confidential Informationは、会社のネットワークにログインでき、特定の承認を得た個人のみがアクセスできるようにする必要がある。

■Copying/Printing/Faxing/Scanning: 必要な場合を除き、Highly Confidential Informationをスキャン、コピー又は配布しないこと。業務上特に知る必要のない者が当該情報を閲覧しないように、合理的な手段を講じること。

■Encryption: 外部に対して又は内部に対してかにかかわらず、Highly Confidential Informationを送信する場合、あるいは、ノートパソコン、スマートフォン、その他のモバイル機器（USBドライブなどのモバイル記憶装置を含む。）にHighly Confidential Informationを保存する場合は、暗号化する必要がある。

■Mailing: 必要な場合を除き、Highly Confidential Informationを郵送しない。Highly Confidential Informationを社外に送付する場合は、受領署名が必要なサービスを利用する。Highly Confidential Informationを社内に送付する場合は、“ Highly Confidential Information ”と表示され、厳封された封筒を使用する。Highly Confidential Informationを電子媒体で郵送する場合は、暗号化し、パスワードで保護する必要がある。

■Network Segmentation: Highly Confidential Informationは、会社のネットワークのうち業務上必要のある領域でのみ利用できるようにすること。Highly Confidential Informationは、ファイアウォール、アクセス制御リストその他のセキュリティメカニズムなどを使用して、会社の他のネットワークからセグメント化する必要がある。

III.実務上の事前対策～内部規程（例）～

- サイバーセキュリティに関する内部規程（サンプル）
  - ✓ 具体的な**セキュリティ対応**
    ⇒サイバーセキュリティ関連ではより詳細に**禁止事項等**を設定する（以下項目と大まかな規定内容のご紹介）

SAMPLE

■Desktop, Laptop, and End-User Controls
❖ **企業の設定する基準を満たしたデバイスのみ使用可能**（満たしていない場合にはアクセスを拒絶）／**付与されたアカウント**のみ使用／離席時の対応

■Information Handling and Storage
❖ 各種情報について**定められた方法・期間の保管**を実施／**個人のサーバーへのファイル保存の禁止**（設定上不可能にする）／**ハード面**の対応

■Internet Use: Email, Messaging, Social Media, and Cloud Computing
❖ **アクセス可能なサイトの制限**／**SNS**の使用制限／**メールの使用ルール**（Confidential Informationの提供ルール）／**クラウドサービス**への注意喚起

■Mobile Devices and Bring Your Own Device to Work
❖ 個人の機器使用に関して**個別の承認**を要求する等／**保護されていないインターネットサービス**への接続禁止（ブロック）

■Remote Access
❖ **多要素認証**／**アクセス可能なデータやサービスの限定**／一定期間動作がない場合の**タイムアウト設定**

■External Network Connections
❖ **IT担当者による事前承認**／（ネットワークを使用することとなる）外部者との間の**契約**締結

■Wireless Network Connections
❖ （企業として許可したものを除き）**原則として接続禁止**

III.実務上の事前対策～内部規程（例）～

- サイバーセキュリティに関する内部規程（サンプル）
  - ✓ **有事対応**
    ⇒他の規程（例：Risk Management Policy）と連動させるような形で規定

SAMPLE

■Reporting a Security Incident
If any Company Personnel know or suspect that a **Security Incident** has occurred, they **may not attempt to investigate the matter themselves**. In such a case, they must immediately contact their supervisor, manager, or [XXXX（担当部署や役員）]. Such Company Personnel should preserve all evidence relating to the potential Security Incident.
[XXXX（担当部署や役員）] should, in accordance with the Company's Risk Management Policy, appropriately deal with the Security Incident.

※"Security Incident"：どのような場合が「有事」かという観点で定義
例：any act or omission that **compromises, or could have the effect of compromising, the security, confidentiality, or integrity of Information Assets, or the physical, technical, administrative, infrastructure, or organizational safeguards** the Company or a third-party service provider has put in place to protect Information Assets. Any actual or threatened loss of or unauthorized access to, disclosure, use, or acquisition of Information Assets is a security incident.

III.実務上の事前対策～内部規程（例）～

- サイバーセキュリティに関する内部規程（サンプル）
  - ✓ **有事対応**
    ⇒他の規程（例：Risk Management Policy）と連動させるような形で規定

■Reporting a Security Incident If any Company Personnel know or suspect that a Security Incident has occurred, they may not attempt to investigate the matter themselves. In such a case, they must immediately contact their supervisor, manager, or [XXXX（担当部署や役員）]. Such Company Personnel should preserve all evidence relating to the potential Security Incident. [XXXX（担当部署や役員）] should, in accordance with the Company's Risk Management Policy, appropriately deal with the Security Incident.	**■Reporting a Security Incident** 当社従業員は、Security Incidentが発生したことを知り、又は、疑った場合は、自分自身で当該問題を調査しようとしてはならない。そのような場合、直ちに上司、マネージャー、又は、[XXXX（担当部署や役員）]に連絡しなければならない。当社従業員は、潜在的なSecurity Incidentに関連する全ての証拠を保存しなければならない。 [XXXX（担当部署や役員）]は、当社のリスク管理方針に従って、Security Incidentを適切に対処しなければならない。

III.実務上の事前対策～内部規程（例）～

- サイバーセキュリティに関する内部規程（サンプル）
  - ✓ **有事対応**

    ⇒“Security Incident”：どのような場合が「有事」かという観点で定義

■**Security Incident**	■**Security Incident**
any act or omission that compromises, or could have the effect of compromising, the security, confidentiality, or integrity of Information Assets, or the physical, technical, administrative, infrastructure, or organizational safeguards the Company or a third-party service provider has put in place to protect Information Assets. Any actual or threatened loss of or unauthorized access to, disclosure, use, or acquisition of Information Assets is a security incident.	情報資産のセキュリティ、機密性、完全性、又は当社若しくは第三者のサービスプロバイダーが情報資産を保護するために導入している物理的、技術的、管理上、インフラ上若しくは組織的な安全対策を損なう、又は損なう効果を有するいかなる作為又は不作為。情報資産の現実の損失若しくは損失の脅威、情報資産への許可されないアクセス、開示、使用若しくは取得は、Security Incidentとなる。

III.実務上の事前対策～内部規程（例）～

- サイバーセキュリティに関する内部規程（サンプル）
  - ✓ その他**社内教育**等
    ⇒他の規程同様、社内教育や第三者との取決め、規程内容のアップデートに関する一般的な定めを用意

SAMPLE

■Training
会社は、**警戒心**が強く**洞察力**のある**従業員**が**最良の防衛線**であることを認識している。[XXXX（担当部署や役員）]は、PolicyとInformation Assets及びConfidential Informationの取り扱いについて、会社の**全従業員を教育し、訓練**しなければならない。

■Third-Party Service Provider への対応（社内の情報に触れる可能性のあるベンダー等を想定して定義）
Confidential Informationを**Third-Party Service Providerに委託**する場合は、会社とThird-Party Service Providerの間で締結される、守秘義務規定を有する適切な契約により、**委託先におけるInformation Assetsの取扱い**を**適切に管理及び監督**できるようにする必要がある。従業員の監督又はThird-Party Service Providerの監督に責任を有する会社の従業員は、従業員及びThird-Party Service Providerに対する**監督を行うための訓練を受け**、これに**習熟**しなければならない。

■Policy の見直し／違反時の罰則
Committeeは、 **Policyの遵守と有効性**を評価するために、**定期的なレビューと監査**を実施する。 Policy及びInformation Assetsを保護し、Policyを実施するために設計された関連するガイドライン又は手続に**違反した従業員**は、**解雇を含む懲戒処分の対象**となる。

III.実務上の事前対策～技術的な対策～

- ❑ 自社のサイバーセキュリティの状況を正確に**把握・評価**する
  - ✓ 自社のシステムに関する**専門業者によるチェック**委託
- ❑ システム上の対策
  - ✓ **メール送信**時の最終確認（送信先の確認、添付ファイルの確認等）
  - ✓ **送金**時の電話確認
  - ✓ 端末にログオンする際の**Multi-Factor Authentication**（多要素認証）導入
- ❑ その他の対策～保険による対応も要検討
  - ✓ リスクの金銭評価
  - ✓ 対応の現実性（経済合理性）を欠くリスクへの対応としての検討
  - ✓ **サイバー保険**・**E&O保険**・**D&O保険**・**Business Loss保険**等

IV. 平時の心構えと有事対応
～Best Practiceを目指して～

IV. 有事対応を見越した平時の心構え

- ❑ 有事の時にこそ**迅速かつ適切**な対応が必要
  - ✓ 有事を意識した**平時のトレーニング・内部規定整備**の重要性
- ❑ 有事対応のポイント①：**全ステークホルダー**向けの迅速な対応
  - ✓ 顧客・取引先：個別対応／**プレスリリース**等による経緯説明
  - ✓ 従業員：社内向け**通知文書**／必要に応じて個別対応
  - ✓ 株主：**プレスリリース**／**株主総会**での説明準備等
  - ✓ 情報主体・その他一般社会向け：**メディア対応**／**プレスリリース**
- ❑ 有事対応のポイント②：**ディスカバリー制度**
  - ✓ 広範な証拠等開示義務が課される米国特有の制度
  - ✓ 弁護士が関与しているコミュニケーションをディスカバリーの**対象外**とする

IV. 有事対応の具体～社内外の対応事項～

- 対内的なコミュニケーション
  - ✓ 事前に構築された手順をもとに社内での適切な指示
  - ✓ 内部告発者（Whistleblower）への対応（法令遵守も意識）
    - 告発を理由とした不利益取扱いの禁止
    - 告発者の匿名性確保等
- 対外的なプレスリリース
  - ✓ 発生・発覚経緯の説明
  - ✓ 被害状況の確認
  - ✓ 対応（治癒）状況の報告
  - ✓ 未確定な情報の提供は避ける
  - ✓ レピュテーションリスクの適切なコントロール

IV. 有事対応の前提：米国特有の事情

❑ ディスカバリー制度とは？

- ✓ **事実審理（トライアル）の前**の**証拠開示手続**
  - 訴訟当事者が、相手方又は第三者から、**証拠を入手**するための手続
  - 米国では、事実審理（トライアル）まで手続が進むことは稀であり、その**前段階（プリ・トライアル）**で、**「和解」**するか、陪審手続を経ずに裁判所の判断を得る**「サマリージャッジメント」**によって終結することほとんど
- ✓ 事実審理（トライアル）の前に**勝負は決まってしまう？**
  - 勝負を決める要素は、**ディスカバリー**によって、どれだけ**有利、不利な証拠**が開示されるかにかかってくる。

IV. 有事対応の前提：米国特有の事情

❑ ディスカバリー制度と証拠保全の重要性

- ✓ 証拠開示（ディスカバリー）を前提に紛争当事者は証拠保全義務を負う
  - 訴訟が開始された時点／紛争が始まった時点で存在する証拠をそのままの形で残す義務（「訴訟ホールド」）
  - 提訴以前であっても、「合理的に訴訟を予測できる」（reasonably foreseeable）時点で訴訟ホールドが発生すると考えられており、自社がまだ訴訟に巻き込まれていないからといって証拠保全義務がないと判断するのは大きな誤り
- ✓ 証拠保全の対象
  - 訴訟と潜在的に関連性があれば、あらゆる文書／電子データが対象（メタ・データやバックアップデータも含む）
  - 電子データの自動削除機能が存在する場合、これを解除する必要

IV. 有事対応の前提：米国特有の事情

❑ 証拠保全の実務

- ✓ 証拠保全義務に違反した場合の**ペナルティ**
  - 帰責性の大きさや相手方への影響に応じて以下を含む不利益のおそれ

①**追加のディスカバリー**　②本来は相手方が負担すべき**費用の転嫁**　③不利な事実の**推認**
④自社の請求した**証拠の排除**　⑤**欠席判決**（一方的な敗訴）　⑥**訴え却下**（※原告の場合）
⑦特別な**陪審説示**（自社に不利な事実を推定することの許容等）等
（※いずれも裁判所の広い裁量）

- ✓ ペナルティを避けるために：**速やかにかつ適切な証拠保全**の必要
  - 紛争の発生が想定される事象が起きた場合、速やかに弁護士へ連携、弁護士から依頼者である企業への証拠保全に関するサポート
  - 「**Litigation Hold Letter**（文書保全通知）」を活用

※Litigation Hold Letterの実際使用されたサンプルをご希望の場合はご連絡ください

IV. 有事対応の前提：米国特有の事情

❑ 秘匿特権の活用による情報保護

✓「秘匿特権」とは

- ディスカバリー制度では広範な文書・資料（メールを含む）が開示対象となるところ、**秘匿特権の対象となる文書・資料に関しては開示義務を免れる**
- 典型的には弁護士と依頼人との間のコミュニケーション：**Attorney-Client-Privilege**
- 一定の**要件**（法的助言を受ける目的のコミュニケーションであること等）が存在

✓ 秘匿特権の活用例

1) 紛争可能性のある事象（例：情報漏洩の発生）が生じた場合、**直ちに弁護士へ連絡**
2) 以後の連絡（技術面での検証状況の確認・報告を含む）については、**全て弁護士をコミュニケーションに含める**
3) 具体的な紛争が予測される場合の作成文書については、**ワーク・プロダクト**（Work-Product）として開示対象から外すことも可能（※例外的に開示義務が生じる場合も）

SGR

IV. 有事対応の前提：米国特有の事情

- ❑ 身代金（ランサム）を支払うことで、米国当局から制裁を受ける恐れ
  - ✓ 2021年9月21日付けUpdated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC)
    - 米国政府は、私企業に対して、ハッカー集団からの身代金（ランサム）支払要求に対しては、控えることを**強く要請**
    - 2021年9月、OFACは、身代金（ランサム）の支払を促進したとして、仮想通貨交換業者SUEX OTC, S.R.O.を**Malicious Cyber Actor**に認定
  - ✓ 早期解決のために、身代金（ランサム）をハッカー集団に即時に支払うことは、米国当局からの制裁を受ける新たなリスクを招く恐れ
  - ✓ 身代金（ランサム）支払の意思決定プロセスの**事前決定**、**明確化**の必要性

URL：https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf

V. ケーススタディ

V. 近時のサイバー攻撃事例

- 元従業員による**Cash App利用者データ**の侵害（2022年4月）
  - ✓ Cash App（送金アプリ）利用者の口座情報を含む個人情報が2021年12月に**元従業員**によって漏洩していたことが**2022年4月のSECに対する報告書によって発覚**
  - ✓ 正確な被害状況は未確認（800万人以上が確認対象となっている）
- **Microsoft**に対する**ハッカー集団**によるサイバー攻撃（2022年3月）
  - ✓ 2022年3月20日：ハッカー集団であるLapsus$がMicrosoftへのハッキングを公表
  - ✓ **2日後**、2022年3月22日にMicrosoftが当該攻撃を認め、顧客情報の漏洩がないことを報告
  - ✓ なお、Lapsus$は2022年3月23日にはOkta, Inc.へのサイバー攻撃も公表
- **Crypto.com**に対するハッキングによる仮想通貨の盗難（2022年1月）
  - ✓ 2022年1月17日にハッカーにより483人のCrypto.com利用者のウォレットが侵害され、30万米ドル超に相当する仮想通貨が盗まれる
  - ✓ 企業は当初仮想通貨が盗まれてはいないとしつつ、**後日盗まれたことを認め**、ユーザーに対して全額補填を実施

V. 近時のサイバー攻撃事例

- Equifaxの例（2017年）
  - ✓ 米国内の三大消費者信用情報サービスの1つであったEquifax社が保有する**約1.5億件（アメリカ国民の約半数）の個人情報が漏洩**した事案
    - 同社の使用するWebアプリケーションフレームワークの**脆弱性が公開**（2017年3月）され、その約2ヶ月後に侵入を受け、4ヶ月後の同年7月にはサイトが完全停止。2017年9月に情報公開した際、株価は約35%下落
    - 事故対応費用：2018年12月末までの1年半で**約5億6250万ドル**を要する（保険でのカバー：1億2500万ドル）
    - 内部の調査チームに加え、（法律事務所を含む）**外部専門家による検証**を実施
  - ✓ 脆弱性発覚後の対応の遅れ、内部でのIT組織構造の不備（社内セキュリテイチームとITチームの連携の悪さ）、**経営陣によるサイバーセキュリティの軽視**（経営会議では四半期に1度しか取り扱わず）等を指摘
- JBS Foodsの例（2021年）
  - ✓ ブラジルに本社を置く、食肉加工業大手のJBS Foodsの米国子会社が、ロシアのサイバー犯罪組織REvilによるものと思われるランサムウェア攻撃により**工場施設の操業停止に追い込まれた**事案
    - サーバーに対する攻撃を受け、北米及びオーストラリアのITシステムに障害が発生、工場施設が操業停止
    - 犯罪組織に対して**約1100万ドル相当の身代金**が仮想通貨により支払われる（未回収）
    - 施設操業は早期に再開されたものの、一時**世界的な食肉不足**が懸念される事態に

V. 近時のサイバー攻撃事例

- コロニアル・パイプラインの例（2021年）
  - ✓ アメリカ東海岸の燃料供給の約45%を担う民間企業であるコロニアル・パイプライン社が、犯罪グループ「DarkSide」からの**ランサムウェア攻撃**を受け、1週間にわたる**操業停止**に追い込まれた事案
    - 2021年4月29日、システムに侵入したDarkSideはわずか2時間で100GB 以上の企業データを窃取、情報をネット上で公開すると脅迫し、**身代金の支払いを要求。**同社CEOはこれを容認し、**440万ドルを仮想通貨で支払う**（その後FBIが約85%を回収）
    - 操業停止の発表により**ガソリンのパニック買い**が発生
  - ✓ コロニアル・パイプライン社の**MFA（多要素認証）が適用されていない未使用のVPNプロファイル放置**が要因とされる

（参考リンク）

https://firewalltimes.com/recent-data-breaches/
https://www.akamai.com/resources/state-of-the-internet/soti-security-pirates-in-the-outfield
（サイバー攻撃による映画やドラマ等の海賊版の流通）

V. 近時のサイバー攻撃事例

- プレス・リリース
  - ✓ いかなる情報を、どのようなタイミングで開示するかは、**難しい経営判断**となる
  - ✓ **コールセンター**の迅速な設置、**サイバー保険**の事前の加入は、あらかじめの準備が必要

言及項目	Colonial Pipeline	Illinois Attorney General	Campbell Conroy & O'Neil
回数	2021年5月8日から5月17日（10日間）までで、9回	2021年4月13日、4月29日の2回	1回
コールセンターの設置	無し	有り	有り
サイバー保険加入	言及有り	言及無し	言及無し
身代金（ランサム）の支払	言及有り（具体的な金額$4.4 Millionも明示）	言及無し	言及無し

Smith Gambrell Russell

VI. 最後に：心構え

SGR

VI. 最後に：心構え

- 起こりうることは**起こる**
  - ✓ 慌てないために、今できることを。
- **事前・事後の対応**は顧客のためでもあり、自社のためでもある
  - ✓ 事前の対策、有事を想定した、身代金（ランサム）の支払の**意思決定プロセス**の明確化、**証拠保全**、**プレス・リリース**の準備等は、顧客情報の保護のみならず、有事後の自社の企業価値の毀損回避にも有用
- 管理職への話の持って行き方
  - ✓ 「**知らなかった**」が理由にならない、経営責任の問題
  - ✓ **内部規程**の策定、**サイバー保険**の準備等、事前の準備、**予算**が必要な事項

すみません、最後に宣伝です。

書籍についての詳細:
サイバーリスクマネジメントの強化書ー経団連「サイバーリスクハンドブック」実践の手引きー 梶浦 敏範(監修) - 日刊工業新聞社 | 版元ドットコム (hanmoto.com)

紹介:IT部門としての対策ではなく、経営主導による全社的なリスク管理の観点からサイバーセキュリティを確保する体制構築の勘どころを説く。

オンライン書店で購入

- 紀伊國屋 Web Store
- ヨドバシ.com
- 楽天ブックス
- HonyaClub.com
- オムニ7
- e-hon
- HMV
- TSUTAYA
- Yahoo!ショッピング
- アマゾン

ご清聴ありがとうございました

Questions???

小島清顕 名刺
Eight QRコード

E-mail
kkojima@sgrlaw.com

ご質問等、お気軽にご連絡ください。

SCAN ME

弊社では米国の法律に関わる**最新情報**・**ウェビナーの案内**等のニュースレターを配信しております。ご希望の方は、上記QRコードまたは柿内のメールアドレス skakiuchi@sgrlaw.com からお申し込み下さい。

SGR

事務所紹介　Smith, Gambrell & Russell, LLP（SGR）

スミス ガンブレル ラッセル法律事務所（SGR法律事務所）は、1893年に創設された創業130年の米国ジョージア州アトランタ市発祥の総合法律事務所です。ニューヨーク、ロサンゼルス、ワシントンDC、フロリダ、テキサス、イリノイ、ロンドン、ミュンヘン等主要都市にオフィスを構え、約400人の弁護士が所属しています。

取扱分野は、法人設立、各種契約、M&A・合弁・業務提携、雇用・労務、訴訟・紛争、企業誘致・助成金交渉、貿易・通商関連、環境、建設、不動産、知財、倒産、税務、遺産相続計画、年金・福利厚生、海事、サイバーセキュリティ・情報保護法、移民法・ビザ等、企業法務全般をカバーしています。全米法律事務所ランキング・トップ200（Am Law 200）にも継続して選出されています。日本チームは、上記の総合法律サービスを日本語により提供しています。詳しくは、SGR法律事務所の日本語ページをご参照ください。ご不明な点、ご質問等ございましたら、正式にご起用いただくまで費用は発生いたしませんので、お気軽にご相談ください。

日本語ページ　https://www.sgrlaw.com/practices/japan-practice-team/

＊弊所では、米国の法律に関わる最新情報・ウェビナーの案内等ニュースレターを配信しております。ご希望の方は、右記QRコード、またはジャパンデスク 柿内のメールアドレス skakiuchi@sgrlaw.com からお申し込み下さい。

SCAN ME

SGR