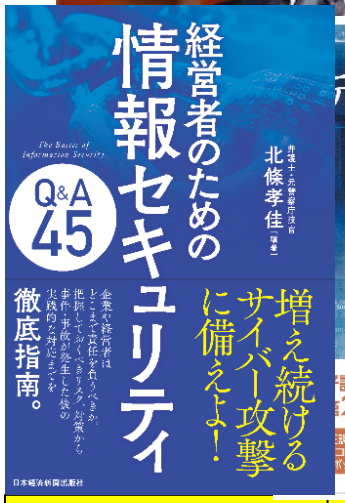
企業と経営層の法的責任の問題

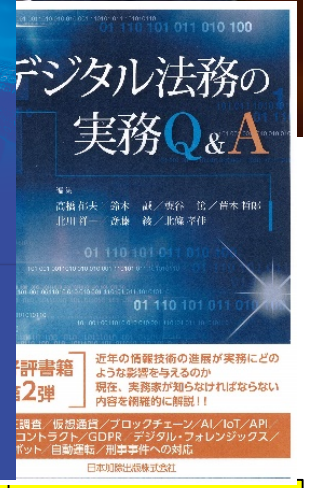
2020年2月26日(水)

西村あさひ法律事務所
弁 護 士　北 條 孝 佳

北條 孝佳
ほうじょう　たかよし

- 元警察庁技官(10年以上)
- 東京弁護士会所属
- NCA(日本シーサート協議会)
  専門委員
- NICT(情報通信研究機構)
  招へい専門員
- JNSA(ネットワークセキュリティ協会)
  適正な事業遂行検討会　委員
- NISC(内閣サイバーセキュリティセンター)法令集　TF構成員
- IDF(デジタル・フォレンジック研究会)　幹事
- 全国都道府県警察での講演、経営者向け講演等





経営者のための情報セキュリティ　Q&A45	デジタル法務の実務Q&A

1. 事前対策の必要性
取り巻く環境

ゼロトラスト：信頼しないことを前提とし、全てを確認する
DFFT：Data Free Flow with Trust(情報の自由な流通)

1. 事前対策の必要性
重要インフラ事業者

- 「重要インフラ」
  - ✓ 代替困難なサービスを提供する事業
  - ✓ 機能が停止等の状態に陥った場合、国民生活又は社会経済活動に多大なる影響を及ぼすおそれ
- 内閣サイバーセキュリティセンターが公表した第4次行動計画(2018年7月25日)では、重要インフラ分野として、「情報通信」、「金融」、「航空」、「空港」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む）」、「医療」、「水道」、「物流」、「化学」、「クレジット」及び「石油」の14分野を特定

1. 事前対策の必要性
重要インフラ事業者

重要インフラ事業者等の経営層は、以下の項目の必要性を認識し、実施できていることが求められている

情報セキュリティの確保は経営層が果たすべき責任であり、経営者自らがリーダーシップを発揮し、機能保証の観点から情報セキュリティ対策に取り組むこと

自社の取組が社会全体の発展にも寄与することを認識し、サプライチェーン(ビジネスパートナーや子会社、関連会社)を含めた情報セキュリティ対策に取り組むこと

情報セキュリティに関してステークホルダーの信頼・安心感を醸成する観点から、平時における情報セキュリティ対策に対する姿勢やインシデント発生時の対応に関する情報の開示等に取り組むこと

上記の各取組に必要な予算・体制・人材等の経営資源を継続的に確保し、リスクベースの考え方により適切に配分すること

1. 事前対策の必要性
時代の変化

- 世界の時価総額ランキング

	平成元年(億ドル)	平成30年(億ドル)
1	NTT(1638.6)	アップル(9409.5)
2	日本興業銀行(715.9)	アマゾン・ドット・コム(8800.6)
3	住友銀行(695.9)	アルファベット(8336.6)
4	富士銀行(670.8)	マイクロソフト(8158.4)
5	第一勧業銀行(660.9)	フェイスブック(6092.5)

出典：ダイヤモンドオンライン
https://diamond.jp/articles/-/177641?page=2

2. 経営層が意識すべきこと①
デジタル化・IT化

- 時代が変化、企業は全てIT化
  →デジタライゼーションへ対応
  - デジタイゼーション
  - デジタルトランスフォーメーション
- 次々と登場する新たなサービスの**提供**、
  新たなサービスを**取り入れる**際の**注意**
- 先端技術やサービスの導入にはリスク・脅威も
  含まれる
- 試験的導入＋リスクの低減方策
  (被害の最小化、代替手段の検討・準備)
- 導入に際する議論(範囲、責任)

2. 経営層が意識すべきこと①
リスクマネジメント

- **リスクマネジメント**の必要性
  - 企業の価値を維持・増大するため、**リスク**と**影響**を**正確に把握**し、事前対策を講じることで**危機発生の回避**＋**危機発生時の損失最小化・極小化**
  - 業務の複雑化によりアウトソーシング
  - 外注先の業務停止が自社にも影響
  - 従業員の法令違反により企業の経営をゆるがす
- リスクとは…
  - 従来は、**悪い事象が起こる可能性**のこと
    →ダウンサイドリスクのみ
  - 現在は、**将来の不確実性**のこと
    →アップサイドリスクも含む

2. 経営層が意識すべきこと①
リスクの種類

- リスクの種類
  - ☑環境リスク・災害リスク
  - ☑戦略リスク・開発リスク
  - ☑法務リスク・財務リスク
  - ☑システムリスク
  - ☑犯罪リスクなど
- サイバーセキュリティの確保は
  - ☑**外部**からの対策
  - ☑**内部**からの対策

2. 経営層が意識すべきこと①
サイバー攻撃に遭う確率

- サイバー攻撃の被害に遭う確率
  - 情報処理推進機構
    - 2014年度　調査対象企業全体の19.3%
  - トレンドマイクロ社
    - 2015年　調査対象企業全体の38.5%
    - 2016年　調査対象企業全体の41.9%
    - 2017年　調査対象企業全体の42.3%
    - 2018年　調査対象企業全体の36.3%
  - 英国デジタル・文化・メディア・スポーツ省
    - 2018年　調査対象企業1,566社の32%

2. 経営層が意識すべきこと②
クラウドへのデータ移行

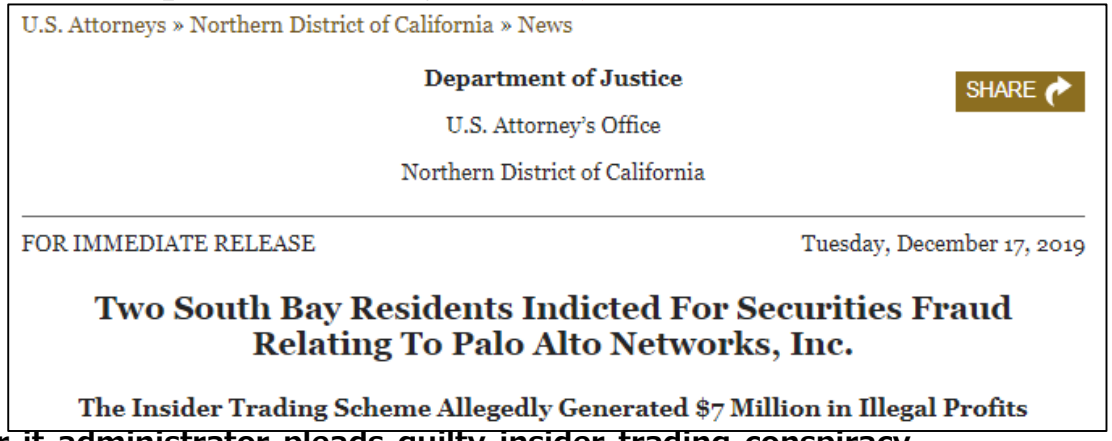
- クラウドにデータが集約され始めている
- クラウドサービスの提供事業者視点
  - これまでとは異なるサービス体系
  - これまでとは異なる開発体系
  - クラウドサービスは複数の顧客に同一のサービスを提供
- クラウドサービスの利用事業者視点
  - クラウドサービスに対応可能な知識や能力が必要
  - 多様化するクラウドサービスの選定
  - 進化に追随する変革意識

2. 経営層が意識すべきこと②
サイバーセキュリティの確保

- 全てがつながるシステム・機器の登場・導入
  (OA機器、IoT機器、自動運転車等)
- 利用者、利用企業、社会生活、経済活動への影響大
- 様々な機器がネットワーク化、**脆弱な部分が増加**するおそれ
  →攻撃されれば、他のシステムへの被害拡大と他社/他者への損害が発生するおそれ
- 対策の必要性
  - 近時の脅威動向の把握
  - 体制整備、組織改革、規程類の見直し
  - 人材育成など

2. 経営層が意識すべきこと③
内部不正(インサイダー取引)

- 世界有数の**セキュリティ企業P社**のIT部門従業員が、インサイダー取引により$700万(約7億6000万円)の利益を不正に取得
- 米司法省はP社に関連する証券詐欺で2名を起訴したと発表(2019/12/17)
- 四半期ごとの財務実績に関する**機密情報へアクセス**して悪用
- 3年間で不正な800回の株取引



U.S. Attorneys » Northern District of California » News

Department of Justice

U.S. Attorney's Office

Northern District of California

SHARE

FOR IMMEDIATE RELEASE — Tuesday, December 17, 2019

Two South Bay Residents Indicted For Securities Fraud Relating To Palo Alto Networks, Inc.

The Insider Trading Scheme Allegedly Generated $7 Million in Illegal Profits

出典：米司法省
https://www.justice.gov/usao-ndca/pr/former-it-administrator-pleads-guilty-insider-trading-conspiracy-relating-palo-alto

2. 経営層が意識すべきこと③
内部不正対策

- 情報の持ち出し、機器の持ち出し
  例)教育関連企業、HDD廃棄企業
- 情報の売却、腹いせのためデータ削除
- 転職時のお土産
- 退職者、短期アルバイト等、利用していない者のアカウント管理
- 委託先管理、再委託先管理、再々委託先管理、再々々…
- インターネットの炎上(SNS利用)
  内部からの炎上、部外者による炎上
- データ改ざん、不正取引

2. 経営層が意識すべきこと③
内部不正:従業員、元従業員

- 2019年　不正アクセス禁止法違反
  - 子会社の従業員による犯行
  - 135人のIDを使って電子ギフト券を不正に入手
  - お金が欲しかったという**動機**
- 2019年　電子計算機損壊等業務妨害罪
  - 社長や会社の対応に**不満**があり、建設会社のパソコンに不正にアクセスし、**全データ消去**
  - 退職後もIDやパスワードの変更をしていなかったため、不正アクスが可能
- 2019年　窃盗罪
  - 神奈川県がリースしていたHDDが**オークションで転売**され、情報流出
  - リース会社の委託先従業員を窃盗で逮捕

3. 内部統制システムの構築
内部統制の意義

- サイバーセキュリティの確保は、適切なリスク管理の実施→内部統制システムの構築・運用
- 内部統制の意義は…
  消極的意義：法令遵守や不正防止
  積極的意義：業務の有効性や効率性の確保
- 内部統制システムを適切に構築・運用することは、取引先や消費者等を含む多様なステークホルダーへの利益にもつながる
  - ☑信用の確保、取引先との良好な関係構築
  - ☑企業価値を支える社会的責任
  - ☑ブランド価値・レピュテーションの維持や向上

3. 内部統制システムの構築
内部通報制度

- 内部通報制度…公益通報者保護法を踏まえ、従業員が**企業内の不正を発見**したり、**コンプライアンス違反**の疑いがあったりする場合に**企業内外**に設置された窓口に通報する制度
- 整備
  - 窓口、**内部規程**、経営幹部からの独立、**通報者の保護**、**不利益取扱の禁止**
- 運用
  - 通報の受領、通報内容の検討・調査、是正措置、通報制度の評価や改善

3. 内部統制システムの構築
コーポレートガバナンスコード

- コーポレートガバナンスコード　原則2-5

上場会社は、その従業員等が、不利益を被る危険を懸念することなく、**違法**または**不適切な行為**・情報開示に関する情報や真摯な疑念を伝えることができるよう、また、伝えられた情報や疑念が客観的に検証され適切に活用されるよう、**内部通報に係る適切な体制整備を行うべき**である。**取締役会**は、こうした体制整備を実現する責務を負うとともに、その**運用状況を監督**すべきである。

補充原則２－５①
上場会社は、内部通報に係る体制整備の一環として、**経営陣から独立した窓口の設置**（例えば、社外取締役と監査役による合議体を窓口とする等）を行うべきであり、また、**情報提供者の秘匿と不利益取扱の禁止に関する規律を整備すべき**である。

3. 内部統制システムの構築
内部通報制度認証

- 内部通報制度認証(自己適合宣言登録制度)
  - 事業者が自らの内部統制制度を評価して認証基準に適合している場合
  - 事業者からの申請に基づき指定登録機関がその内容を確認した結果を登録し、WCMSマークの使用を許諾する制度
- 自己適合宣言制度
- 今後は第三者認証制度

商事法務研究会：https://wcmsmark.secure.force.com/

4. 経営者らが考慮すべき責任
2種類の責任

- 責任
  - ① 企業が負う責任
    第三者に損害が発生した場合には、企業が損害賠償責任を負う可能性
  - ② 経営者らが負う責任
    会社に損害が生じ、経営者らが負う善管注意義務に違反した場合、
    会社に対して負う責任＋
    第三者に対して負う責任の両方の責任を負う可能性

4. 経営者らが考慮すべき責任
①企業が負う責任

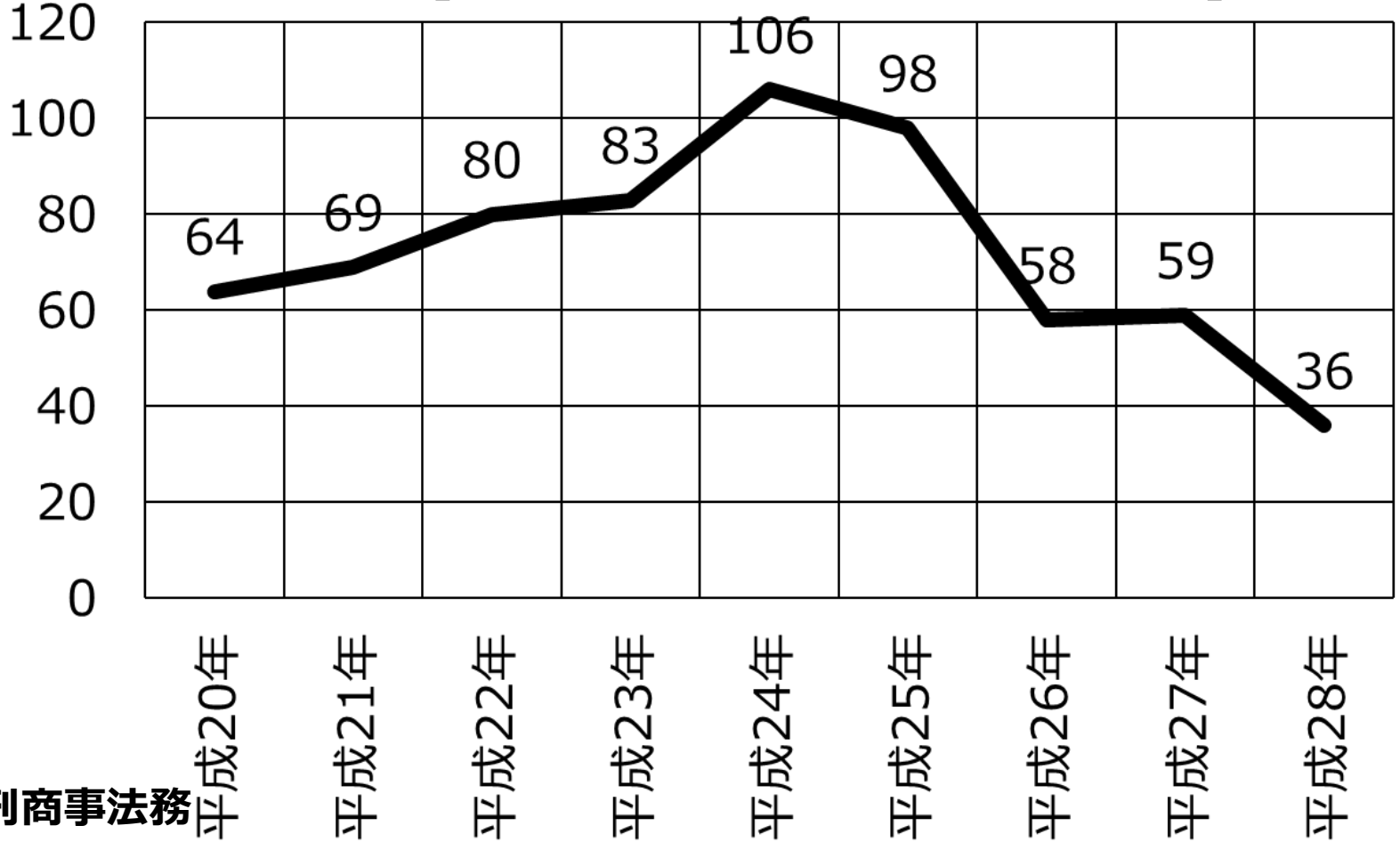
- 企業の行為により、**第三者**に損害が発生した場合には、企業が**損害賠償責任**を負う可能性
  - 個人情報、クレジットカード情報の流出
  - 開発企業として開発した納品物の不備
  - 運用、保守管理による対策不備
- 内部不正による
  - データ改ざん、粉飾決算等の不正会計

  →製品の認証、認定の取消

  →上場廃止のおそれ

4. 経営者らが考慮すべき責任
②経営者らが負う責任

- 株主代表訴訟(経営者への責任追及)



引用元：旬刊商事法務

4. 経営者らが考慮すべき責任
②経営者らが負う責任

- 会社に**損害**が生じ、経営者らが**善管注意義務に違反**する場合には、経営者らも責任を負う可能性
  - ☑ 会社から**委任**を受け、**善良な管理者として注意義務**(会社法330条、民法644条)
  - ☑ 法令、定款等を遵守し、会社や株主に対して**最も有利**となるように職務遂行
    →経営者らは法令を遵守し、会社にできるだけ損失を与えないように**適切なリスクマネジメントを行う**こと
  - ☑ グループ会社のガバナンスも必要
  - ☑ 具体的法令違反
  - ☑ 抽象的法令違反

A) 経営判断の原則(責任を否定する方向に働く)
B) 監視・監督義務違反
C) 内部統制システム構築義務違反

4. 経営者らが考慮すべき責任
②経営者らが負う責任

C)内部統制システム構築義務

- セキュリティ**脅威**の**把握**
- セキュリティリスクの**内部**チェック
- セキュリティリスクの**第三者**チェック
- **同業他社**のセキュリティ事案の分析
- セキュリティ**脅威**に対する**対策**
- セキュリティ対策の**ガイドライン**の把握
- セキュリティ対策の**知識**や**理解**
- セキュリティ対策の**検討**、**採用**、**運用**
- 運用状況、不足状況、修正可能性
- 適合性、充足性、過剰性

4. 経営者らが考慮すべき責任
サイバーリスクハンドブック日本版(経団連)

原則1：取締役は、サイバーセキュリティを、単なるITの問題としてではなく、**全社的なリスク管理**の問題として理解し、対処する必要

原則2：取締役は、自社固有の状況と関連付けて、**サイバーリスク**の**法的意味を理解**すべき

原則3：取締役会は、サイバーセキュリティに関する十分な**専門知識を利用**できるようにしておくとともに、**取締役会の議題**としてサイバーリスク管理を定期的に取り挙げ、十分な時間をかけて議論を行うべき

原則4：取締役は、**十分な人員と予算**を投じて、**全社的**なサイバーリスク管理の枠組みを確立すべき

原則5：サイバーリスクに関する取締役会における議論の内容として、**回避すべきリスク**、**許容するリスク**、保険等によって**軽減・移転すべきリスク**の特定や、それぞれのリスクへの対処方法に関する具体的計画等を含めるべき

5. サイバーセキュリティの確保
具体的内容

- **事前対策・準備**として
  - ☑ 法務部、顧問弁護士・専門弁護士との連携＋**管理・対応体制**の構築
    例)データ利活用の企画・設計、取得、加工・分析、実装・運用、廃棄の全ての管理・対応体制
  - ☑ チェック＝技術的【内部・外部】チェック＋**法的評価**
    規程の整備は当然、その**内容・中身**の網羅性や**技術的・法的・経営的**視点
  - ☑ 契約書関連(守秘義務、誓約書)
  - ☑ 訴訟関連(適切な証拠保存の整備、ログ集約)
  - ☑ インシデント対応業者の選定
  - ☑ 模擬的内部不正を行い、不備のある箇所の見直し・改善など

5. サイバーセキュリティの確保
具体的内容

- **事後対応**として
  - ☑ インシデント対応業者への依頼
  - ☑ 被害に遭った情報・機器の**主体・手段・開示・使用等**の特定
  - ☑ インシデント発生の原因・分析
  - ☑ 訴訟を見据えた**情報収集・証拠収集**
  - ☑ **法執行機関**との連携、**監督官庁**等への報告・連絡
  - ☑ 広報活動・公表活動
  - ☑ 情報の取り戻し・使用禁止の検討
  - ☑ 再発防止策の提案(技術面、体制面)
  - ☑ 被害賠償、補償問題

    など

5. サイバーセキュリティの確保
CISOの設置

- CISOを設置するに当たり地位と権限を決定
  取締役か執行役か執行役員か
- CISOはサイバーセキュリティのプロフェッショナルでなくても構わない
  →**配下**にプロフェッショナル人材を確保
- 現在のシステムのセキュリティ確保＋
  将来のシステムのセキュリティ確保のために
  最適となる計画(プロセス、リソースの確保)の策定
- **各部門**へサイバーセキュリティを確保する意識、リスクを認識させること