

【第2回】

サイバーセキュリティ法制

～イノベーション、エコノミック・ステイトクラフトを読み解くために

令和2年11月25日(水)

講師：藤岡 福資郎



自己紹介

藤岡 福資郎(Fujioka Fukujiro)

＜これまでのあゆみ＞

- 九州工業大学で脳情報を専攻後、東京大学大学院学際情報学府でインターネット関連法規を研究
- NTT東日本 本社経営企画部、群馬支店、千葉支店(＝投資・医療・映像サービスの広告宣伝)
- 株式会社カンキョーアイ 執行役員(＝特許取得のマッチング技術で幸せを広げるお手伝い)
- 九州大学 サイバーセキュリティセンター 学術研究員(＝SECKUNの開発・運営)
- 九州工業大学 情報工学部 情報関連法規 非常勤講師

＜資格＞

- 1級知的財産管理技能士(コンテンツ専門業務、特許専門業務)
- PRプランナー
- 2級WEBデザイン技能士
- 行政書士
- プロフェッショナルCFO 他

→例えば、戦略(知財とか)を考えて、／誰にどのように動いてほしいかPRプランニングして、／WEBデザインに落とし、展開する。みたいな合わせ技で生きてきました。

AGENDA

1. 日本のジレンマ
2. サイバーセキュリティ基本法の素読から読み解く。今、なすべきこと
3. サイバーセキュリティ法制とLSMAP3+1
4. セキュリティビジネスとオープン&クローズ戦略
5. ご意見をお寄せください

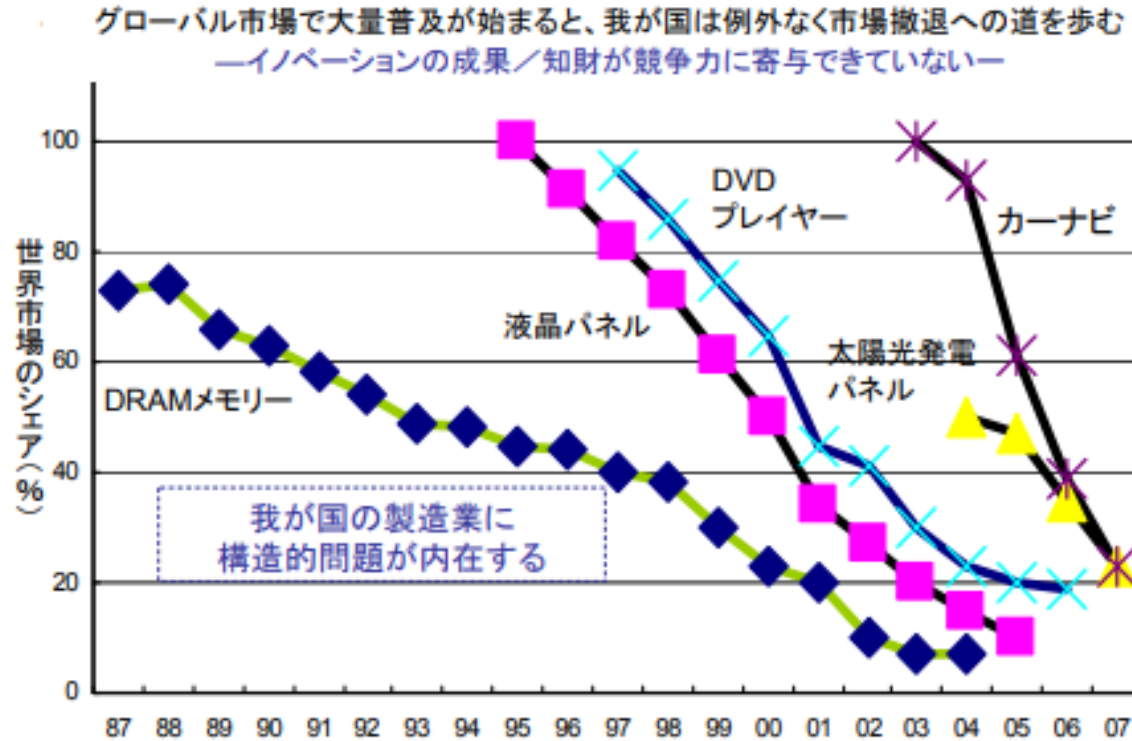
1. 日本のジレンマ

技術・特許で勝利、事業に敗北したエレクトロニクス分野の失敗を繰り返さないために

1. 日本のジレンマ ～エレクトロニクスを例に

製品アーキテクチャのダイナミズムと日本型イノベーション・システム

図1 日本企業のシェア推移（エレクトロニクス製品市場）



- エレクトロニクス産業が弱体化した理由は、
 - 第一にこれまでのような先端技術の開発や工場中心のものづくりで競争力が決まる時代が終わり、
 - 第二にグローバルなビジネス・エコシステムの構造や競争ルールを決めるための仕組み作りで競争力が決まる時代が到来したからであり、
 - そして、第三に技術の伝搬・着床スピードをコントロールする知的財産マネジメントや国の制度設計で競争力が決まる時代に移行したことである。
 - この変化に2000年代までの日本のエレクトロニクス産業が対応できなかった。

【出所】小川紘一「オープン＆クローズ戦略」P36

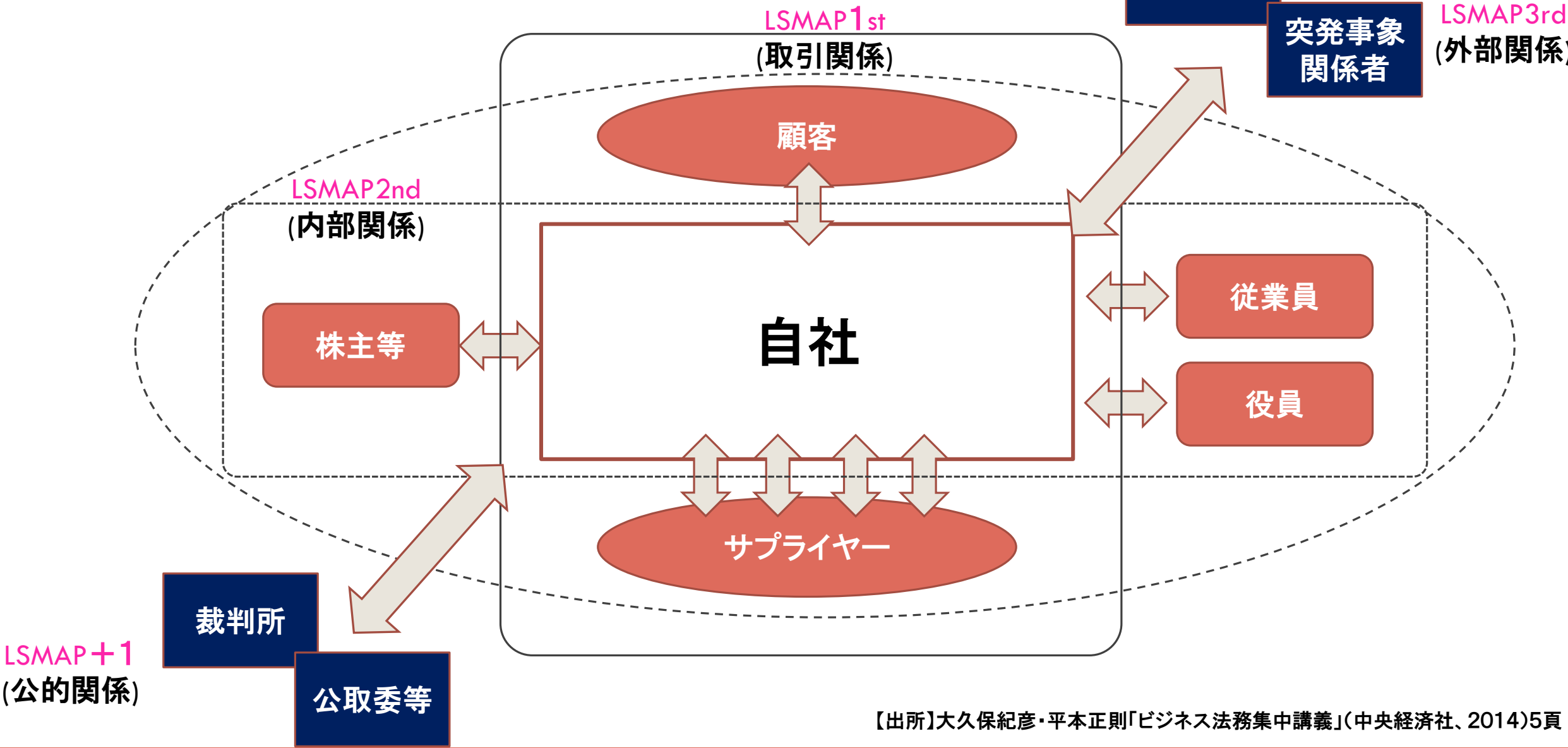
【出所】小川紘一「製品アーキテクチャのダイナミズムと日本型イノベーションシステム」(2009)赤門マネジメント・レビュー 第8巻2号41頁

1. 日本のジレンマ ～エレクトロニクスを例に

- 日本の電機産業で起きた産業構造の転換
- 大企業を中心とするフルセット垂直統合型の企業制度が、1990年代から経済合理性を失う。デジタル化によって産業構造がビジネス・エコシステム型へ転換し、価値形成のメカニズムが変わってしまったからである。エコシステム・パートナーが持つ多くのコンポーネントを組み合わせ結合させて全体最適へ向かう、いわゆるアーキテクチャー思考によるイノベーションが、価値形成で重要な役割を担うようになった。
- ここからグローバル市場の競争ルールが一変し、いわゆる“技術進歩”が経済成長に貢献するメカニズムも変わった。要素技術や完成品など、コンポーネントのイノベーションが経済成長に直結することを想定したイノベーション論が、1990年代後半の電機産業で機能不全となったのである（アメリカでは1980年代の後半から）。
- それまでの、要素技術のレベルや中間財のレベル、あるいは完成品のイノベーションが付加価値生産性を高めて国の雇用や経済成長に貢献するはず、という旧来型のイノベーションモデルが終焉した。
- 少なからぬ識者や経営者が電機産業の衰退をイノベーションの不足のせいにし、あるいは後知恵でリーマンショックのせいにしてきた。しかしながら1990年代の日本は、電機産業に自動車産業とほぼ同等の研究開発投資をしてきたのであり、それでも多くの主要製品で、リーマンショック前の2000年代初期からすでに貿易収支が赤字に転落していた。また同時に日本の地方から工場が消え、電機産業が国の雇用にも経済成長にも貢献しなくなっていたのである。我々が、新たな成長モデルあるいは新たなイノベーションモデルを必要とする時代を迎えたことが、ここから理解されるであろう。

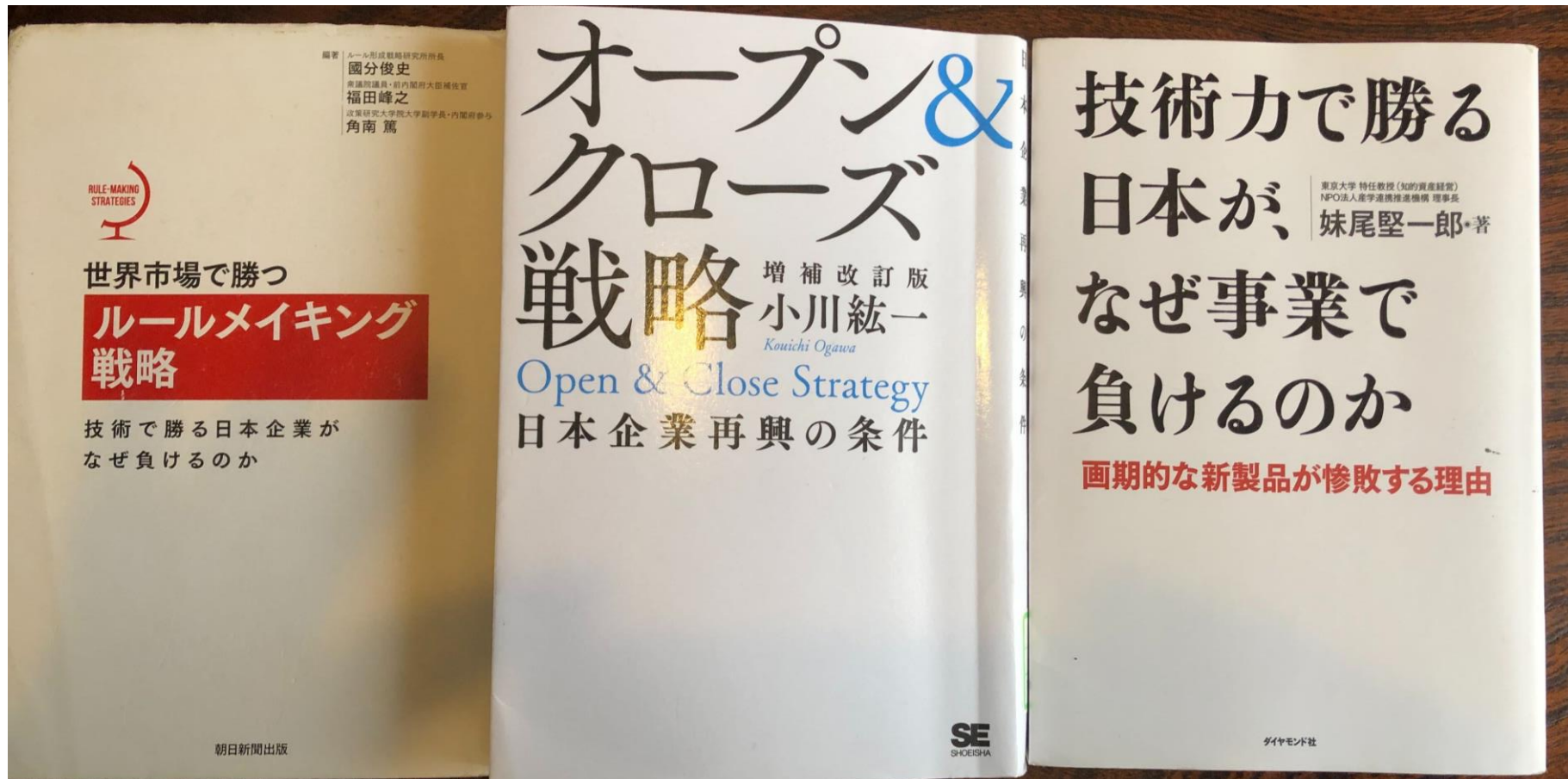
【出所】小川紘一「IoT時代に向けた我が国のイノベーションモデルの再構築に向けて」(2018)PP5-6

2. 企業を取り巻く法制度 ～LSMAP3+1



【出所】大久保紀彦・平本正則「ビジネス法務集中講義」(中央経済社、2014)5頁

(参考)おすすめ図書



2. サイバーセキュリティ基本法の素読から読み解く 今、なすべきこと

条文素読体験

「書いていること」「解釈が分かれること」「書いていないこと」の意味

1. サイバーセキュリティ基本法の見取り図

第I章. 総則

■ 目的 (第1条)

■ 定義 (第2条)

⇒ 「サイバーセキュリティ」について定義

■ 基本理念 (第3条)

⇒ サイバーセキュリティに関する施策の推進にあたっての基本理念について次を規定

- ① 情報の自由な流通の確保を基本として、官民の連携により積極的に対応
- ② 国民1人1人の認識を深め、自発的な対応の促進等、強靱な体制の構築
- ③ 高度情報通信ネットワークの整備及びITの活用による活力ある経済社会の構築
- ④ 国際的な秩序の形成等のために先導的な役割を担い、国際的協調の下に実施
- ⑤ IT基本法の基本理念に配慮して実施
- ⑥ 国民の権利を不当に侵害しないよう留意

■ 関係者の責務等 (第4条～第9条)

⇒ 国、地方公共団体、重要社会基盤事業者(重要インフラ事業者)、サイバー関連事業者、教育研究機関等の責務等について規定

■ 法制上の措置等 (第10条)

■ 行政組織の整備等 (第11条)

第II章. サイバーセキュリティ戦略

■ サイバーセキュリティ戦略 (第12条)

⇒ 次の事項を規定

- ① サイバーセキュリティに関する施策の基本的な方針
- ② 国の行政機関等におけるサイバーセキュリティの確保
- ③ 重要インフラ事業者等におけるサイバーセキュリティの確保の促進
- ④ その他、必要な事項

⇒ その他、総理は、本戦略の案につき閣議決定を求めなければならないこと等を規定

第III章. 基本的施策

■ 国の行政機関等におけるサイバーセキュリティの確保 (第13条)

■ 重要インフラ事業者等におけるサイバーセキュリティの確保の促進 (第14条)

■ 民間事業者及び教育研究機関等の自発的な取組の促進 (第15条)

■ 多様な主体の連携等 (第16条)

■ 犯罪の取締り及び被害の拡大の防止 (第17条)

■ 我が国の安全に重大な影響を及ぼすおそれのある事象への対応 (第18条)

■ 産業の振興及び国際競争力の強化 (第19条)

■ 研究開発の推進等 (第20条)

■ 人材の確保等 (第21条)

第III章. 基本的施策 (つづき)

■ 教育及び学習の振興、普及啓発等 (第22条)

■ 国際協力の推進等 (第23条)

第IV章. サイバーセキュリティ戦略本部

■ 設置等 (第24条～第35条)

⇒ 内閣に、サイバーセキュリティ戦略本部を置くこと等について規定

附則

■ 施行期日 (第1条)

⇒ 公布の日から施行(ただし、第II章及び第IV章は公布日から起算して1年を超えない範囲で政令で定める日)する旨を規定

■ 本部に関する事務の処理を適切に内閣官房に行わせるために必要な法制の整備等 (第2条)

⇒ 情報セキュリティセンター(NISC)の法制化、任期付任用、国の行政機関の情報システムに対する不正な活動の監視・分析、国内外の関係機関との連絡調整に必要な法制上・財政上の措置等の検討等を規定

■ 検討 (第3条)

⇒ 緊急事態に相当するサイバーセキュリティ事象等から重要インフラ等を防御する能力の一層の強化を図るための施策の検討を規定

■ IT基本法の一部改正 (第4条)

⇒ IT戦略本部の事務からサイバーセキュリティに関する重要施策の実施推進を除く旨規定

【出所】<https://www.nisc.go.jp/conference/seisaku/dai40/pdf/40shiryou0102.pdf>

第一章. 総則 【目的】

第一章 総則

（目的）

第一条 この法律は、インターネットその他の高度情報通信ネットワークの整備及び情報通信技術の活用の進展に伴って世界的規模で生じているサイバーセキュリティに対する脅威の深刻化その他の内外の諸情勢の変化に伴い、情報の自由な流通を確保しつつ、サイバーセキュリティの確保を図ることが喫緊の課題となっている状況に鑑み、我が国のサイバーセキュリティに関する施策に関し、基本理念を定め、国及び地方公共団体の責務等を明らかにし、並びにサイバーセキュリティ戦略の策定その他サイバーセキュリティに関する施策の基本となる事項を定めるとともに、サイバーセキュリティ戦略本部を設置すること等により、高度情報通信ネットワーク社会形成基本法(平成十二年法律第百四十四号)と相まって、サイバーセキュリティに関する施策を総合的かつ効果的に推進し、もって経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現を図るとともに、国際社会の平和及び安全の確保並びに我が国の安全保障に寄与することを目的とする。

第一章. 総則【定義】

(定義)

第二条 この法律において「サイバーセキュリティ」とは、電子的方式、磁気的方式その他の知覚によっては認識することができない方式(以下この条において「電磁的方式」という。)により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置(情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体(以下「電磁的記録媒体」という。)を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。)が講じられ、その状態が適切に維持管理されていることをいう。

第一章. 総則 【基本理念】

(基本理念)

第三条 サイバーセキュリティに関する施策の推進は、インターネットその他の高度情報通信ネットワークの整備及び情報通信技術の活用による情報の自由な流通の確保が、これを**通じた表現の自由の享有、イノベーションの創出、経済社会の活力の向上等にとって重要**であることに鑑み、サイバーセキュリティに対する脅威に対して、国、地方公共団体、重要社会基盤事業者(国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものに関する事業を行う者をいう。以下同じ。)等の**多様な主体の連携**により、積極的に対応することを旨として、行われなければならない。

2 サイバーセキュリティに関する施策の推進は、**国民一人一人のサイバーセキュリティに関する認識を深め、自発的に対応することを促す**とともに、サイバーセキュリティに対する脅威による被害を防ぎ、かつ、被害から迅速に復旧できる強靱(じん)な体制を構築するための取組を積極的に推進することを旨として、行われなければならない。

3 サイバーセキュリティに関する施策の推進は、インターネットその他の高度情報通信ネットワークの整備及び情報通信技術の活用による**活力ある経済社会を構築**するための取組を積極的に推進することを旨として、行われなければならない。

4 サイバーセキュリティに関する施策の推進は、サイバーセキュリティに対する脅威への対応が国際社会にとって共通の課題であり、かつ、我が国の経済社会が国際的な密接な相互依存関係の中で営まれていることに鑑み、サイバーセキュリティに関する国際的な秩序の形成及び発展のために先導的な役割を担うことを旨として、**国際的協調**の下に行われなければならない。

5 サイバーセキュリティに関する施策の推進は、**高度情報通信ネットワーク社会形成基本法の基本理念**に配慮して行われなければならない。

6 サイバーセキュリティに関する施策の推進に当たっては、**国民の権利を不当に侵害しないように留意**しなければならない。

第一章. 総則 【関係者の責務等】

（国の責務）

第四条 国は、前条の基本理念（以下「基本理念」という。）にのっとり、サイバーセキュリティに関する総合的な施策を策定し、及び実施する責務を有する。

（地方公共団体の責務）

第五条 地方公共団体は、基本理念にのっとり、国との適切な役割分担を踏まえて、サイバーセキュリティに関する自主的な施策を策定し、及び実施する責務を有する。

（重要社会基盤事業者の責務）

第六条 重要社会基盤事業者は、基本理念にのっとり、そのサービスを安定的かつ適切に提供するため、サイバーセキュリティの重要性に関する関心と理解を深め、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。

（サイバー関連事業者その他の事業者の責務）

第七条 サイバー関連事業者（インターネットその他の高度情報通信ネットワークの整備、情報通信技術の活用又はサイバーセキュリティに関する事業を行う者をいう。以下同じ。）その他の事業者は、基本理念にのっとり、その事業活動に関し、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。

（教育研究機関の責務）

第八条 大学その他の教育研究機関は、基本理念にのっとり、自主的かつ積極的にサイバーセキュリティの確保、サイバーセキュリティに係る人材の育成並びにサイバーセキュリティに関する研究及びその成果の普及に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。

（国民の努力）

第九条 国民は、基本理念にのっとり、サイバーセキュリティの重要性に関する関心と理解を深め、サイバーセキュリティの確保に必要な注意を払うよう努めるものとする。

第一章. 総則 【法制上の措置、行政組織の整備等】

（法制上の措置等）

第十条 政府は、サイバーセキュリティに関する施策を実施するため必要な法制上、財政上又は税制上の措置その他の措置を講じなければならない。

（行政組織の整備等）

第十一条 国は、サイバーセキュリティに関する施策を講ずるにつき、行政組織の整備及び行政運営の改善に努めるものとする。

第三章. 基本施策

(国の行政機関等におけるサイバーセキュリティの確保)

第十三条 国は、国の行政機関、独立行政法人(独立行政法人通則法(平成十一年法律第百三号)第二条第一項に規定する独立行政法人をいう。以下同じ。)及び特殊法人(法律により直接に設立された法人又は特別の法律により特別の設立行為をもって設立された法人であって、総務省設置法(平成十一年法律第九十一号)第四条第十五号の規定の適用を受けるものをいう。以下同じ。)等におけるサイバーセキュリティに関し、国の行政機関及び独立行政法人におけるサイバーセキュリティに関する統一的な基準の策定、国の行政機関における情報システムの共同化、情報通信ネットワーク又は電磁的記録媒体を通じた国の行政機関の**情報システムに対する不正な活動の監視及び分析**、国の行政機関におけるサイバーセキュリティに関する**演習及び訓練**並びに国内外の関係機関との**連携及び連絡調整**によるサイバーセキュリティに対する脅威への対応、国の行政機関、独立行政法人及び特殊法人等の間における**サイバーセキュリティに関する情報の共有その他の必要な施策を講ずるものとする。**

第三章. 基本施策

（重要社会基盤事業者等におけるサイバーセキュリティの確保の促進）

第十四条 国は、重要社会基盤事業者等におけるサイバーセキュリティに関し、**基準の策定、演習及び訓練、情報の共有その他の自主的な取組の促進その他の必要な施策**を講ずるものとする。

（民間事業者及び教育研究機関等の自発的な取組の促進）

第十五条 国は、中小企業者その他の民間事業者及び大学その他の教育研究機関が有する**知的財産に関する情報**が我が国の国際競争力の強化にとって重要であることに鑑み、これらの者が自発的に行うサイバーセキュリティに対する取組が促進されるよう、サイバーセキュリティの重要性に関する関心と理解の増進、サイバーセキュリティに関する相談に応じ、必要な情報の提供及び助言を行うことその他の必要な施策を講ずるものとする。

2 国は、国民一人一人が自発的にサイバーセキュリティの確保に努めることが重要であることに鑑み、日常生活における電子計算機又はインターネットその他の高度情報通信ネットワークの利用に際して適切な製品又はサービスを選択することその他の取組について、**サイバーセキュリティに関する相談に応じ、必要な情報の提供及び助言を行うことその他の必要な施策**を講ずるものとする。

第三章. 基本施策

（民間事業者及び教育研究機関等の自発的な取組の促進）

第十五条 国は、中小企業者その他の民間事業者及び大学その他の教育研究機関が有する知的財産に関する情報が我が国の国際競争力の強化にとって重要であることに鑑み、これらの者が自発的に行うサイバーセキュリティに対する取組が促進されるよう、サイバーセキュリティの重要性に関する関心と理解の増進、**サイバーセキュリティに関する相談に応じ、必要な情報の提供及び助言を行うことその他の必要な施策を講ずるものとする。**

2 国は、国民一人一人が自発的にサイバーセキュリティの確保に努めることが重要であることに鑑み、日常生活における電子計算機又はインターネットその他の高度情報通信ネットワークの利用に際して適切な製品又はサービスを選択することその他の取組について、サイバーセキュリティに関する相談に応じ、必要な情報の提供及び助言を行うことその他の必要な施策を講ずるものとする。

（多様な主体の連携等）

第十六条 国は、関係府省相互間の連携の強化を図るとともに、**国、地方公共団体、重要社会基盤事業者、サイバー関連事業者等の多様な主体が相互に連携して**サイバーセキュリティに関する施策に取り組むことができるよう必要な施策を講ずるものとする。

第三章. 基本施策

（犯罪の取締り及び被害の拡大の防止）

第十七条 国は、サイバーセキュリティに関する犯罪の取締り及びその被害の拡大の防止のために必要な施策を講ずるものとする。

（我が国の安全に重大な影響を及ぼすおそれのある事象への対応）

第十八条 国は、サイバーセキュリティに関する事象のうち我が国の安全に重大な影響を及ぼすおそれがあるものへの対応について、関係機関における体制の充実強化並びに関係機関相互の連携強化及び役割分担の明確化を図るために必要な施策を講ずるものとする。

第三章. 基本施策

（産業の振興及び国際競争力の強化）

第十九条 国は、サイバーセキュリティの確保を自立的に行う能力を我が国が有することの重要性に鑑み、サイバーセキュリティに関連する産業が雇用機会を創出することができる成長産業となるよう、新たな事業の創出並びに産業の健全な発展及び国際競争力の強化を図るため、サイバーセキュリティに関し、先端的な研究開発の推進、技術の高度化、人材の育成及び確保、競争条件の整備等による経営基盤の強化及び新たな事業の開拓、技術の安全性及び信頼性に係る規格等の国際標準化及びその相互承認の枠組みへの参画その他の必要な施策を講ずるものとする。

（研究開発の推進等）

第二十条 国は、我が国においてサイバーセキュリティに関する技術力を自立的に保持することの重要性に鑑み、サイバーセキュリティに関する研究開発及び技術等の実証の推進並びにその成果の普及を図るため、サイバーセキュリティに関し、研究体制の整備、技術の安全性及び信頼性に関する基礎研究及び基盤的技術の研究開発の推進、研究者及び技術者の育成、国の試験研究機関、大学、民間等の連携の強化、研究開発のための国際的な連携その他の必要な施策を講ずるものとする。

第三章. 基本施策

（人材の確保等）

第二十一条 国は、大学、高等専門学校、専修学校、民間事業者等と緊密な連携協力を図りながら、サイバーセキュリティに係る事務に従事する者の**職務及び職場環境がその重要性にふさわしい魅力**あるものとなるよう、当該者の適切な処遇の確保に必要な施策を講ずるものとする。

2 国は、大学、高等専門学校、専修学校、民間事業者等と緊密な連携協力を図りながら、サイバーセキュリティに係る人材の確保、養成及び資質の向上のため、資格制度の活用、若年技術者の養成その他の必要な施策を講ずるものとする。

（教育及び学習の振興、普及啓発等）

第二十二条 国は、国民が広くサイバーセキュリティに関する関心と理解を深めるよう、サイバーセキュリティに関する教育及び学習の振興、啓発及び知識の普及その他の必要な施策を講ずるものとする。

2 国は、前項の施策の推進に資するよう、サイバーセキュリティに関する啓発及び知識の普及を図るための行事の実施、重点的かつ効果的にサイバーセキュリティに対する取組を推進するための期間の指定その他の必要な施策を講ずるものとする。

（国際協力の推進等）

第二十三条 国は、サイバーセキュリティに関する分野において、我が国の国際社会における役割を積極的に果たすとともに、国際社会における我が国の利益を増進するため、サイバーセキュリティに関し、国際的な規範の策定への主体的な参画、国際間における信頼関係の構築及び**情報の共有の推進、開発途上地域のサイバーセキュリティに関する対応能力の構築の積極的な支援その他の国際的な技術協力、犯罪の取締りその他の国際協力を推進するとともに、我が国のサイバーセキュリティに対する諸外国の理解を深めるために必要な施策を講ずるものとする。**

第四章. サイバーセキュリティ戦略本部

(設置)

第二十四条 サイバーセキュリティに関する施策を総合的かつ効果的に推進するため、内閣に、**サイバーセキュリティ戦略本部(以下「本部」という。)**を置く。

(所掌事務等)

第二十五条 本部は、次に掲げる事務をつかさどる。

- 一 サイバーセキュリティ戦略の案の作成及び実施の推進に関すること。
 - 二 国の行政機関及び独立行政法人におけるサイバーセキュリティに関する対策の基準の作成及び当該基準に基づく施策の評価(監査を含む。)その他の当該基準に基づく施策の実施の推進に関すること。
 - 三 国の行政機関で発生したサイバーセキュリティに関する重大な事象に対する施策の評価(原因究明のための調査を含む。)に関すること。
 - 四 前三号に掲げるもののほか、サイバーセキュリティに関する施策で重要なものの企画に関する調査審議、府省横断的な計画、関係行政機関の経費の見積りの方針及び施策の実施に関する指針の作成並びに施策の評価その他の当該施策の実施の推進並びに総合調整に関すること。
- 2 本部は、サイバーセキュリティ戦略の案を作成しようとするときは、あらかじめ、高度情報通信ネットワーク社会推進戦略本部及び国家安全保障会議の意見を聴かなければならない。
- 3 本部は、サイバーセキュリティに関する重要事項について、高度情報通信ネットワーク社会推進戦略本部との緊密な連携を図るものとする。
- 4 本部は、我が国の安全保障に係るサイバーセキュリティに関する重要事項について、国家安全保障会議との緊密な連携を図るものとする。

第四章. サイバーセキュリティ戦略本部

(組織)

第二十六条 本部は、サイバーセキュリティ戦略本部長、サイバーセキュリティ戦略副本部長及びサイバーセキュリティ戦略本部員をもって組織する。

(サイバーセキュリティ戦略本部長)

第二十七条 **本部長**は、サイバーセキュリティ戦略本部長(以下「本部長」という。)とし、**内閣官房長官**をもって充てる。

2 本部長は、本部の事務を総括し、所部の職員を**指揮監督**する。

3 本部長は、第二十五条第一項第二号から第四号までに規定する評価又は第三十条若しくは第三十一条の規定により提供された資料、情報等に基づき、必要があると認めるときは、関係行政機関の長に対し、**勧告することができる**。

4 本部長は、前項の規定により関係行政機関の長に対し勧告したときは、当該関係行政機関の長に対し、その勧告に基づいてとった措置について**報告を求めることができる**。

5 本部長は、第三項の規定により勧告した事項に関し特に必要があると認めるときは、内閣総理大臣に対し、当該事項について内閣法(昭和二十二年法律第五号)第六条の規定による**措置がとられるよう意見を具申**することができる。

(サイバーセキュリティ戦略副本部長)

第二十八条 本部に、サイバーセキュリティ戦略副本部長(以下「副本部長」という。)を置き、**国務大臣**をもって充てる。

2 副本部長は、本部長の**職務を助ける**。

第四章. サイバーセキュリティ戦略本部

(サイバーセキュリティ戦略本部員)

第二十九条 本部に、サイバーセキュリティ戦略本部員(次項において「本部員」という。)を置く。

2 本部員は、次に掲げる者(第一号から第五号までに掲げる者にあつては、副本部長に充てられたものを除く。)をもって充てる。

一 国家公安委員会委員長

二 総務大臣

三 外務大臣

四 経済産業大臣

五 防衛大臣

六 前各号に掲げる者のほか、本部長及び副本部長以外の国務大臣のうちから、本部の所掌事務を遂行するために特に必要があると認める者として内閣総理大臣が指定する者

七 サイバーセキュリティに関し優れた識見を有する者の中から、内閣総理大臣が任命する者

第四章. サイバーセキュリティ戦略本部

(資料提供等)

第三十条 **関係行政機関の長は**、本部の定めるところにより、**本部に対し**、サイバーセキュリティに関する資料又は情報であつて、本部の所掌事務の遂行に資するものを、**適時に提供しなければならない**。

2 前項に定めるもののほか、**関係行政機関の長は**、本部長の求めに応じて、本部に対し、本部の所掌事務の遂行に必要なサイバーセキュリティに関する資料又は情報の提供及び説明その他**必要な協力を行わなければならない**。

(資料の提出その他の協力)

第三十一条 **本部は**、その所掌事務を遂行するため必要があると認めるときは、地方公共団体及び独立行政法人の長、国立大学法人(国立大学法人法(平成十五年法律第百十二号)第二条第一項に規定する国立大学法人をいう。)の学長、大学共同利用機関法人(同条第三項に規定する大学共同利用機関法人をいう。)の機構長、日本司法支援センター(総合法律支援法(平成十六年法律第七十四号)第十三条に規定する日本司法支援センターをいう。)の理事長、特殊法人及び認可法人(特別の法律により設立され、かつ、その設立等に関し行政官庁の認可を要する法人をいう。)であつて本部が指定するものの代表者並びにサイバーセキュリティに関する事象が発生した場合における国内外の関係者との連絡調整を行う関係機関の代表者に対して、**資料の提出、意見の開陳、説明その他必要な協力を求めることができる**。

2 **本部は**、その所掌事務を遂行するため特に必要があると認めるときは、前項に規定する者**以外の者**に対しても、**必要な協力を依頼することができる**。

(地方公共団体への協力)

第三十二条 **地方公共団体は**、第五条に規定する施策の策定又は実施のために必要があると認めるときは、本部に対し、情報の提供その他の協力を**求めることができる**。

2 本部は、前項の規定による協力を求められたときは、その求めに**応じるよう努めるものとする**

第四章. サイバーセキュリティ戦略本部

(事務)

第三十三条 本部に関する事務は、内閣官房において処理し、命を受けて内閣官房副長官補が掌理する。

(主任の大臣)

第三十四条 本部に係る事項については、内閣法にいう主任の大臣は、内閣総理大臣とする。

(政令への委任)

第三十五条 この法律に定めるもののほか、**本部に関し必要な事項は、政令で定める。**

附則

（施行期日）

第一条 この法律は、**公布の日から施行する**。ただし、第二章及び第四章の規定並びに附則第四条の規定は、**公布の日から起算して一年を超えない範囲内において政令で定める日から施行する**。

（本部に関する事務の処理を適切に内閣官房に行わせるために必要な法制の整備等）

第二条 政府は、本部に関する事務の処理を適切に内閣官房に行わせるために**必要な法制の整備**（内閣総理大臣の決定により内閣官房に置かれる情報セキュリティセンターの法制化を含む。）**その他の措置を講ずるものとする**。

2 政府は、前項の措置を講ずるに当たっては、専門的知識を有する者を内閣官房において任期を定めて職員又は研究員として任用すること、情報通信ネットワーク又は電磁的記録媒体を通じた国の行政機関の情報システムに対する不正な活動の監視及び分析並びにサイバーセキュリティに関する事象に関する国内外の関係機関との連絡調整に必要な機材及び人的体制の整備等のために必要な法制上及び財政上の措置等について検討を加え、その結果に基づいて**必要な措置を講ずるものとする**。

（検討）

第三条 政府は、**武力攻撃事態等における我が国の平和と独立並びに国及び国民の安全の確保に関する法律**（平成十五年法律第七十九号）第二十四条第一項に規定する緊急事態に相当するサイバーセキュリティに関する事象その他の情報通信ネットワーク又は電磁的記録媒体を通じた電子計算機に対する不正な活動から、**国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるもの等を防御する能力の一層の強化を図るための施策について、幅広い観点から検討するものとする**。

（高度情報通信ネットワーク社会形成基本法の一部改正）

第四条 **高度情報通信ネットワーク社会形成基本法の一部を次のように改正する**。

第二十六条第一項中「**事務**」の下に「（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二十五条第一項に掲げる事務のうちサイバーセキュリティに関する施策で重要なものの実施の推進に関するものを除く。）」を加える。

（内閣総理臨時代理・総務・外務・経済産業・防衛大臣署名）

2. サイバーセキュリティ基本法で定まっていること・いないこと

項目	内容
定まっていること	<ul style="list-style-type: none"> 基本方針 関係者の責務(国・地方自治体・重要インフラ事業者等) 情報共有化(戦略本部・NICS) 犯罪防止、安全保障 産業振興、研究開発 人材育成 国際協力
定まっていないこと	<ul style="list-style-type: none"> 何をもってサイバー攻撃とするか？ サイバーセキュリティと通信の秘密 サイバー攻撃の被害者である民間企業の対抗手段 セキュリティクリアランス 実効性を持たせるための制度 <p><守></p> <ul style="list-style-type: none"> ①情報システム運用側の保護義務 ②情報システム攻撃側への罰則 <p><攻></p> <ul style="list-style-type: none"> ①新技術の発展を促進する法制度の調査&利活用 ②新技術の発展を阻害する法制度の調査&改正

書いていない(書けない)
ことは、検討すべき
という大事なシグナル

- 何をもってサイバー攻撃とするか？
- サイバーセキュリティと通信の秘密
- サイバー攻撃の被害者である民間企業の対抗手段

詳しく知りたい方
林紘一郎先生の論文が
まとまっています。

<https://www.iisec.ac.jp/proc/vol0012/hayashi-tagawa20.pdf>
<https://www.iisec.ac.jp/proc/vol0011/hayashi-tagawa19.pdf>
<https://www.iisec.ac.jp/proc/vol0010/hayashi-tagawa18.pdf>

【関連講義】伊藤先生の授業「【第三回】サイバーセキュリティ法制」もご覧ください。

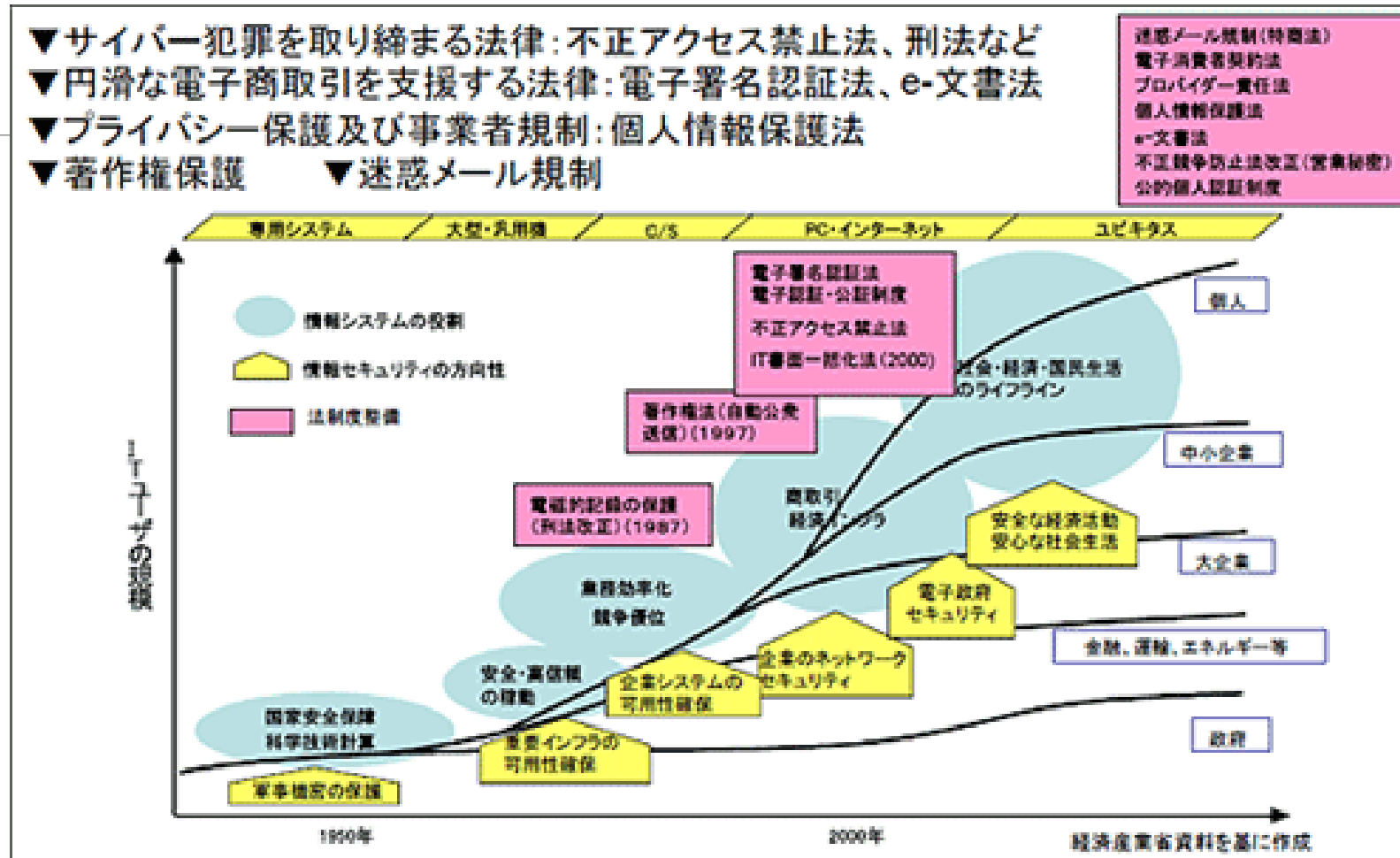
3. サイバーセキュリティ基本法に実効性を持たせるには？

側面	項目	内容
守り ※1	情報システム運用側の保護義務	<ul style="list-style-type: none"> 個人データに関する個人情報保護法上の安全措置義務(20条) 行政機関個人情報保護法上の安全確保措置義務(6条) 電気通信事業者に課せられる、通信の秘密の保護義務(4条) 会社法上の情報保存管理体制を含めた内部統制システム構築義務 等
	情報システム攻撃側への罰則	<ul style="list-style-type: none"> 個人情報保護法上の個人情報データベース等提供罪(83条) 行政機関個人情報保護法上の営業秘密にかかる個人情報ファイル提供罪および保有個人情報提供罪(53条、54条) 不正競争防止法上の営業秘密にかかる一連の罰則(21条1項各号) 不正アクセス禁止法における不正アクセス行為に関する罪(11条・3条) 刑法上の電磁的記録不正作出及び供用罪(161条の2) 不正指令電磁記録に関する罪(168条の2、3)
攻め	新技術の発展を促進する法制度の調査&利活用	<ul style="list-style-type: none"> 海外サイバーセキュリティ法制度調査 オープン&クローズ戦略の検討(=伸びゆく手を生む知財戦略) マイナンバーカード(=JPKI)とコラボしたビジネス展開可能性検討(=国内・海外) セキュリティクリアランス制度(=世界市場に参入できなくなり技術の発展が阻害される懸念あり)
	新技術の発展を阻害する法制度の調査&改正 ※2	<ul style="list-style-type: none"> ビジネスや学術研究における法的なグレーゾーン マルウェア検体の保持(=「正当な目的の有無」の判断がグレー coinhive事件など →刑法(不正指令電磁的記録に関する罪、刑法168条の2第1項各号) ジャミング技術と電波法 海外企業のログ解析とGDPR など

※1【出所】板倉陽一郎「AIネットワーク社会におけるセキュリティの諸相」 250P
 ※2【出所】経済産業省「サイバーセキュリティビジネスの現状と今後の取組の方向性」23P

3. サイバーセキュリティ法制とLSMAP3＋1

1. サイバーセキュリティ法制の生成と展開



【出所】<https://www.ipa.go.jp/security/manager/known/law1.html>

2. サイバーセキュリティ法制は、一意ではない。

	主な掲載法令	サイバーセキュリティ関連法令Q&Aハンドブック (NICS)※1	情報セキュリティ関連の法律ガイドライン (総務省)※2
1	サイバーセキュリティ基本法	○	○
2	民法	○	—
3	会社法	○	—
4	個人情報の保護に関する法律	○	—
5	不正競争防止法	○	—
6	著作権法	○	○
7	労働基準法	○	—
8	電気通信事業法	○	○
9	有線電気通信法	—	○
10	電波法	—	○
11	電子署名及び認証業務に関する法律	○	○
12	電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律	—	○
13	情報処理の促進に関する法律	○	—
14	国立研究開発法人情報通信研究機構法	○	—
15	刑法	○	○
16	不正アクセス行為の禁止などに関する法律	○	○
17	特定電子メールの送信の適正化等に関する法律	—	○

※その他、**通信の秘密(主権概念)**、**米国IoT法**、**ソーシャルエンジニアリング対策**、**割賦販売法**、**官民データ活用推進法**、**電力に関する省令やガイドライン**など受講生の職種業態に応じ多種多様な法制度挙げられた。

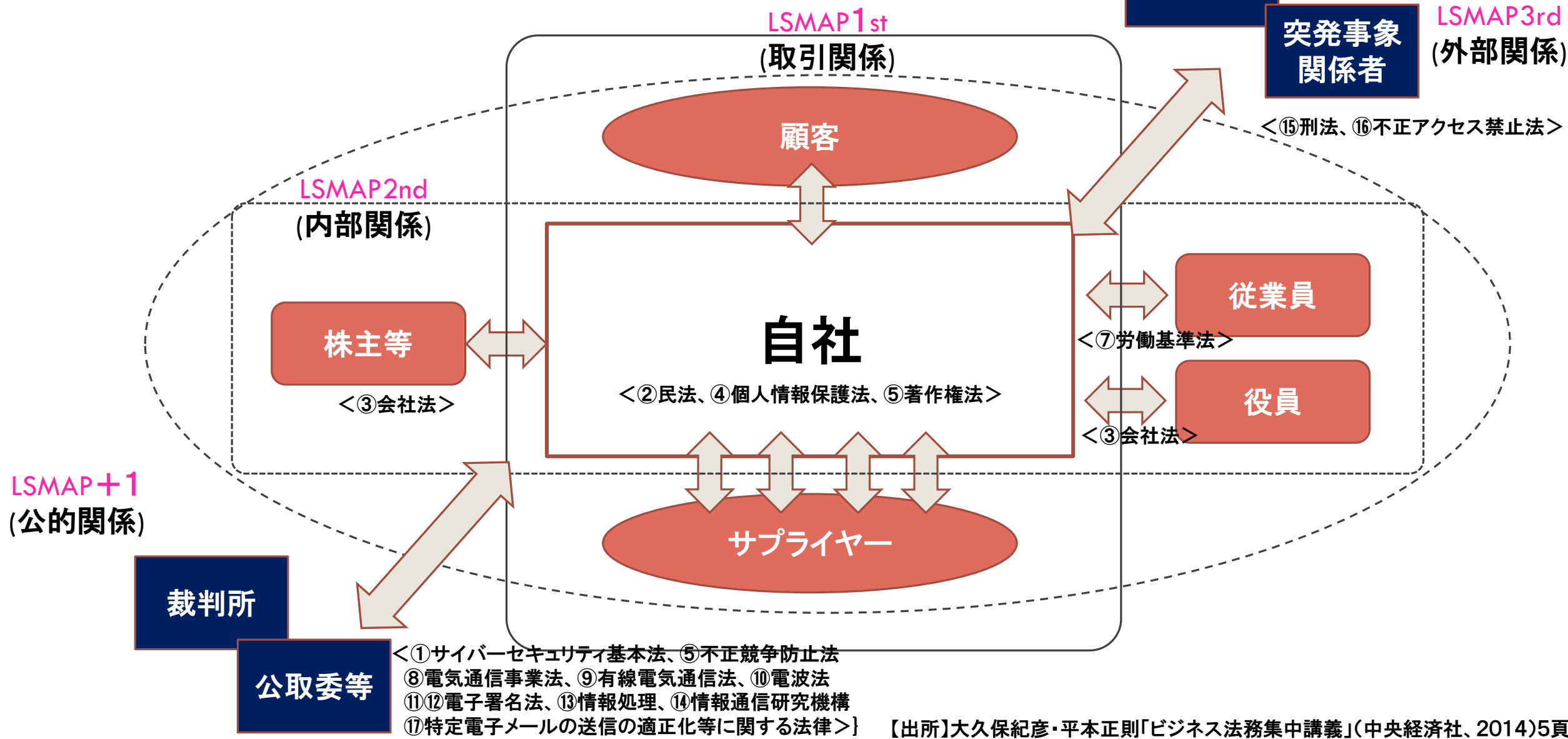
※また、**エコノミックストイックラフト(経済安全保障)**の観点への対策への言及も有。

→対策には、法制度整備に加え、インシデント発生時の株価の過度な下落を防ぐ、PR戦略(経営者含む。平時・危機)及び究極の選択を迫られた際の倫理を身につけることが要諦。

※1:https://www.nisc.go.jp/security-site/law_handbook/index.html

※2:https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/legal/index.html

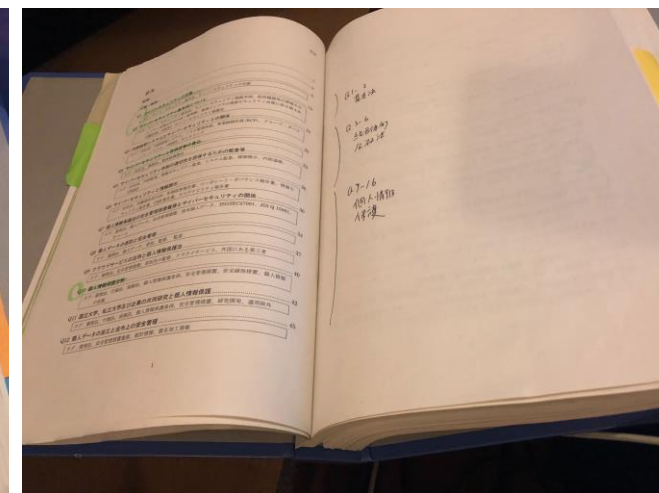
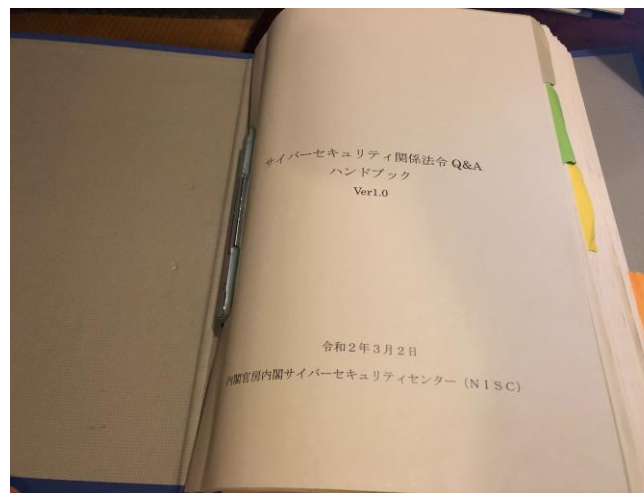
3. LSMAP3+1へのマッピング(一例)



4. 困ったときの強い味方！サイバーセキュリティ関連法令ハンドブック ～シーンから逆引きできる！根拠条文がわかる！

Q&Aで取り上げている主なトピックスについて

1. サイバーセキュリティ基本法関連
2. 会社法関連(内部統制システム等)
3. 個人情報保護法関連
4. 不正競争防止法関連
5. 労働法関連(秘密保持・競業避止等)
6. 情報通信ネットワーク関連(IoT関連を含む)
7. 契約関連(電子署名、システム開発、クラウド等)
8. 資格等(情報処理安全確保支援士等)
9. その他各論(リバースエンジニアリング、暗号、情報共有等)
10. インシデント対応関連(デジタルフォレンジックを含む)
11. 民事訴訟手続
12. 刑事実体法(サイバー犯罪等)
13. 海外法令(GDPR等)



※片面印刷にして見開きにすると、ノート替わりになり便利です。

【出所】https://www.nisc.go.jp/security-site/law_handbook/index.html

活用のポイント

○はしがきを必ず初版のところから最新のところまで読みましょう。

→筆者の問題意識の変遷や背景。明らかになっていたこと、未だ明らかになってないことが分かります。

○目次に分野を書き込みましょう

→P4ページにQのカテゴリー分けが記載されています。一目でわかるように目次に書き込むと調査するときにスムーズです。(また、どんな法律なのかをP3で押さえましょう)

○シーンから解説を読んで理解しましょう。何をしたら(=要件)、どうなるのか(=効果)理解し、条文に**必ず**あたりましょう。(=ログを見るのと同じです。)

→主体、客体、時期、場所、手続き、権利・義務を負うのか？但し書き。

○条文の番号を挙げられるようになると上司や経営陣からの信頼度が増すだけでなく、法改正があった際にも対処が容易です。



(参考)経済戦について

エコノミック・ステイトクラフト 経済安全保障の戦い

(日本語) 単行本 – 2020/5/9

國分 俊史 (著)

- EUは、米国のクラウドに支配されることで情報が筒抜けになることを前提として見ることが可能であるが、**巨額の制裁金を科すルールを形成することによって、盗み見ることを躊躇させる手段がGDPRだったのだ。**つまり、GDPRは、個人情報保護を錦の御旗にしつつ、真の目的は、EUの機密情報を盗み見ることを防ぐ**安全保障戦略**そのものだったのである。
- 2017年時点、多くの日本企業が「GDPRは、手間がかかりあんなルールを本当に実行するなんて想像できない」と言っていた。だが、**GDPRは安全保障目的のルール形成であったことから、躊躇なく運用が開始された。**

【出所】國分俊史「エコノミック・ステイトクラフト経済安全保障の戦い」日本経済出版社(2020)154ページ

【関連講義】別所直哉先生の授業では、「個人情報保護法とルール形成戦略」を取り扱います。

技術規格政策とクラウド競争軸

◆NISTIR 8074 Volume 1 Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity

<https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v1.pdf>

◆セキュリティ関連NIST文書(IPA翻訳版)

<https://www.ipa.go.jp/files/000057365.pdf>

◆セキュリティとルール形成戦略の解説(富士通)

<https://www.fujitsu.com/jp/services/knowledge-integration/insights/20180702/>

<https://www.fujitsu.com/jp/solutions/business-technology/security/secure/event/nist-seminar/>

◆サプライチェーンサイバーセキュリティに関する海外の動き(経済産業省)

https://www.meti.go.jp/committee/kenkyukai/shoujo/sangyo_cyber/wg_1/pdf/001_05_00.pdf

【関連講義】有本先生の授業(本科目第4回)では、「海外サイバーセキュリティ法制」を取り扱います。

4. セキュリティビジネスとオープン&クローズ戦略

1. アップルの成功要因 ～カリスマ経営者？ものづくり？

- アップルの成功をものづくりの成功と言う人さえいる。しかしながらこれは、いずれもアップルの一断面に過ぎない。というより企業経営の中の製品開発という側面の議論でしかない。
- **スティーブジョブスのような人が育たない**ので、あるいは日本企業から消えたので良い製品が生まれない、だから日本のエレクトロニクス産業が衰退した、という意見は依然として多い。
- その背後に潜むのが、「**世に広く受け入れられる商品を開発できれば企業収益に直結する**」という牧歌的なリニアモデルである。
- …しかしながら、このような**技術起点のリニアモデルは、ソフトウェアリッチ型の製品産業のほぼ全域で、1990年代から通用しなくなっている**。
- …例えば、2000年代にアップルから出願・登録された特許の数が年間せいぜい200件以下であって、日本の大手エレクトロニクス企業よりはるかに**少ないという事実**(10分の一以下)がある。
- …なぜアップルは取得している特許の数が非常に少ないにも関わらず**価格が維持**できるのか。
- …あるいは、**携帯電話関連の特許をほとんど持たなかったアップルが、なぜiphoneでビジネス参入できたのか**。
- アップル躍進の本質は、製造業のグローバルイゼーションが生み出す大規模なビジネス・エコシステムの中で、技術や製品を長期にわたって企業収益に結びつけるための**目に見えない仕組みを完成させた点にある。これがアップルによる伸びゆく手の形成である**。

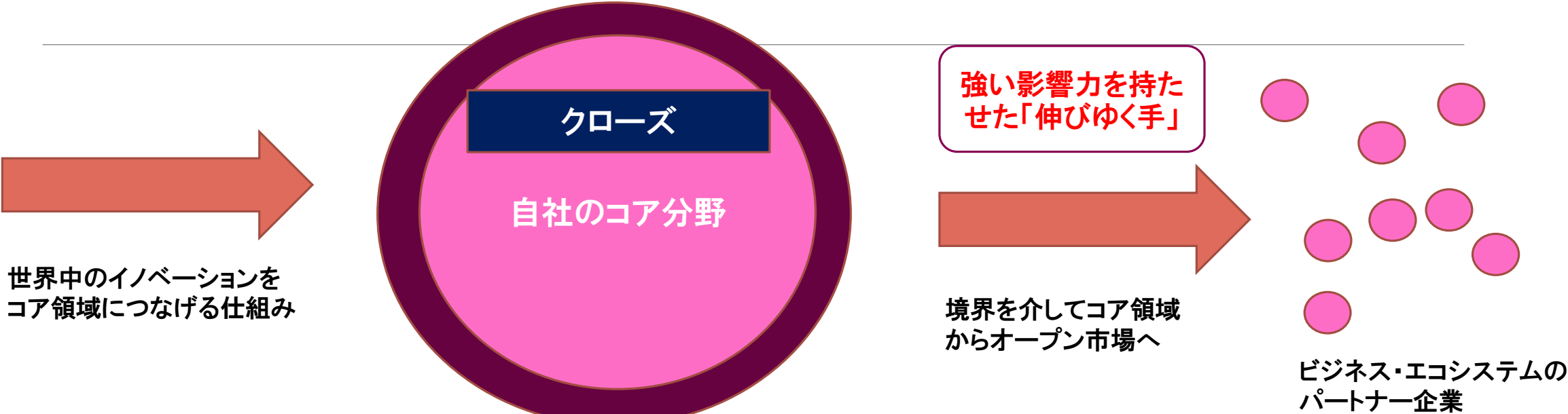
【出所】小川紘一「オープン&クローズ戦略」P176-177

※この他、GAFAや二面市場については、白川聖明「デジタル・プラットフォーム規制について」公正取引NO824（2019）が詳しく整理している。 → **【白川先生の講義を復習してみましょう！】**

【関連講義】白川先生の「デジタルプラットフォーム規制とセキュリティーEUの競争政策の実務を中心に」

2. オープン&クローズ戦略と伸びゆく手 ～欧米企業が自社に有利なルールを形成し市場を席捲

オープン市場



【出所】小川紘一「オープン&クローズ戦略」P12

	アップル (米)	インテル (米)	ボッシュ (独)
オープン / 標準化領域	スマートフォン端末の製造工程を EMS 企業に開示 (オープン化)	PC 周辺機器 (マザーボード) の製造技術をアジア企業に開示 (オープン化)	自動車 ECU 基本ソフトウェア「Autosar」の標準化を主導 (標準化)
クローズ領域	デザイン (意匠権) タッチパネル技術 (特許・他社にライセンスせず)	MPU (ブラックボックス化)	アプリケーション開発の制御パラメータ (ブラックボックス化)

資料：経済産業省作成

【出所】経済産業省「2013年版ものづくり白書」P108

(参考)知的財産の時代の本当の意味

- 知的財産の時代になると、知的財産権によって保護された製品が工業製品に比べて、より有利に超過利益をとるという時代になった。
- 工業時代のチャンピオン国の米国が日本の工業製品に負けたのです。米国は、同じ土俵で日本と争う代わりに、何が富を具現するかという、【富のルール】そのものを変えて、工業製品の代わりに知的財産で超過利益を獲得するべく、知的財産保護ということを、1985年のヤング・レポートの頃から言い始めた。
- そして、米国の司法は、知的財産を保護した。米国は日本に負けない2つの理由がある。一つは、米国は、大陸間弾道弾と核兵器を持っているから、軍事力で日本に負けない。もう一つは、法の支配、裁判所の力によって、知的財産の所有者に有利な判決を出す。
- 【工業製品で日本に凌駕されても、米国は心配することはない】、というのが米国の戦略だった。
- 実際にその通りになっていますよね。GMやフォードの株価よりは、グーグルやアップル、フェイスブック等の知的財産の保護を享受している会社の方が、株価が高いでしょう。株価に如実に表れていますよね。
- 中国が工業製品でいくらいいものを作っても、知的財産にはかなわない。というのは、知的財産の時代(2000年以降)になると【富のルール】が、知的財産を持っている者が、知的財産を持っていない者より大きな利益を取るという【富のルール】に変更がされてしまっているからです。

【出所】升永英俊「職務発明訴訟と今回の法改正について」パテントVol. 69 No. 6 P17(2016)

https://system.jpaa.or.jp/patents_files_old/201604/jpaapatent201604_014-020.pdf

(参考)超LSI技術研究組合(=ゆるやかな独占禁止法)

- 超LSI技術研究組合が発進した1976年の国内のIC売上高はたったの1649億円・・・**国家を挙げての超LSI開発に1100億円の巨額を投入**・・・この成果は1980年代に入ってニッポン半導体の超爆裂成長につながっていく。
- 1983年には国内半導体メーカー大手30社の全生産額は前年度比41%増の1兆9311億円を記録し、実質上米国を抜いて世界のトップに躍り出る。1988年には1M DRAM戦線で日本勢が圧勝し、世界シェア9割を握る。1989年、つまり平成元年にはニッポン半導体は世界シェアの53%を占有し、まさに半導体王国を築くことに成功したのだ。
- 「しかし90年代に入りニッポン半導体の後退が顕著になっていく。これには様々な理由があったが、その1つには**1986年の日米半導体協定の締結があった。何と1992年末までに日本市場における外国系半導体のシェアを20%以上にするという約束をさせられた。**しかしこの頃、ある半導体カンパニーの部長さんは、こともなげにこう言い放っていた。**“購入した米国製品は、輸入途中の太平洋に捨ててきてもいいのですよ。日本の半導体製品の方がはるかにいいのですから”。**このとき私は米国のポテンシャルを考えない単純な優越感に危惧を抱いたのだ」(垂井氏)。
- 周知のように家電製品で切り開いた日本の半導体は、その後パソコン、スマホの世界に入ってからデファクトスタンダードを取れなくなり、見事なまでに負け戦が続く。日本の半導体製品の良品率や寿命の長さは世界に認識されていたが、とにもかくもコスト高で、台湾・韓国などの製品に対抗できなかったのである。そしてまた、メモリーに続く大型製品であるシステムLSIの分野でクアルコム、ブロードコム、エヌビディアに叩きのめされる。もちろんパソコンのCPUではインテルに対し全く歯が立たなかった。

【出所】「1976年の超LSI技術研究組合がニッポン半導体を世界一にした」電子デバイス産業新聞 2018/9/28
<https://www.sangyo-times.jp/article.aspx?ID=2763>

3. 今、なすべきこと

- エレクトロニクス産業が弱体化した理由は、
 - 第一にこれまでのような先端技術の開発や工場中心のものづくりで競争力が決まる時代が終わり、
 - 第二にグローバルなビジネス・エコシステムの構造や**競争ルールを決めるための仕組み作りで競争力が決まる時代が到来**したからであり、
 - そして、第三に技術の伝搬・着床スピードをコントロールする**知的財産マネジメントや国の制度設計で競争力が決まる時代**に移行したことである。
 - この変化に2000年代までの日本のエレクトロニクス産業が対応できなかった。

【出所】小川紘一「オープン＆クローズ戦略」P36

- 技術寄りと言われる日本のサイバーセキュリティ業界。しかしながら、開発型で世界を席巻しているだろうか？
- ウイルス対策ソフトは、どうだろうか？
- エレクトロニクス業界の衰退は、オープン＆クローズ戦略など競争ルール戦略よりも、「数」に着目した知財戦略により、必要以上に特許公開を通じ、技術の全容に全世界からアクセスできる環境を自ら作ってしまった。
- 円高の影響により、液晶やLED等世界のイノベーションに資する製品を海外生産。モジュール化により新興勢力に市場を投資回収前に席巻されてしまった。

しかしながら、サイバーセキュリティの分野は、セキュリティという特性上クローズの部分に対する関心が比較的高いため、競争ルールを検討し、マイナンバーカード等の認証インフラを輸出するなどプラットフォーマーとして日本が活躍できる可能性があるのではないだろうか【大胆な仮説】

(復習)セキュリティ関連ビジネス類型

開発型セキュリティベンダー

輸入型セキュリティベンダー

サイバーセキュリティ教育産業

CISO派遣人材ビジネス

ネットワーク型本人認証

デバイス型本人認証

サイバーセキュリティ保険

サイバーセキュリティコンサルティング

セキュリティ監査

セキュリティクリアランス発行

【出所】福田峰之先生 「セキュリティ関連ビジネスの類型」SECKUN 講義資料

(復習)社会課題からのビジネスモデル づくり

どんな社会が望ましいのか？

何故望ましくない社会になっているのか？

社会的課題解決は誰が担えるか？

どのようなビジネスモデルで解決できるか？

ビジネスモデルに関する既存ルールを理解しているか？

同様のビジネスを行っている企業はあるのか？

競合他社に対して優位性をどう担保するか？

Bサービスをいつ提供するか？

Bを作るためにいくら資金が必要か？

事業化までのスケジュールは、どこまで描けているか？

【出所】福田峰之先生 「社会課題からのビジネスモデルづくり」SECKUN 講義資料

(復習)ルールに対する対応

- ①既存のルールに従う
- ②既存のルールの解釈変更を求める
- ③新規ルールを作る
- ④グレーゾーンは、「先ずやってみる」

ルールに対して・・・

【従うなら】

- ・誰かに有利になる状況にのるだけ
- ・厳しい価格競争、利益幅の少ない範囲でのビジネス（アプリマーケット手数料30%→15%）

【つくるなら】

- ・標準化と規制の組み合わせ
- ・結果的に自分たちが選択される独占的ビジネス（経済安全保障）

【出所】福田峰之先生「ルールに従うのか？つくるのか？」SECKUN 講義資料

(参考)マイナンバー法とマイナンバーインフラ

1. マイナンバー利活用のポイント

1. 年金、労働、医療、福祉などの社会保障を 公平・公正に享受できる社会へ
2. ポイント 1: マイナンバーの利活用は、「社会保障」、「税」、「災害対策」の行政手続きに限られる
3. ポイント 2: マイナンバー カードの IC チップを使った個人認証機能が、多様なサービス創出のカギ
4. ポイント 3: マイナポータルを通じて、国が積極的に国民の生活と命を救済することも可能
5. ポイント 4: マイナンバーの安全性に対する誤解
6. ポイント 5: 災害などで各種証明書を失っても、「自己を証明し、権利を守る」ことが可能
7. ポイント 6: 世界最先端のビッグ プロジェクトとしての価値
8. たゆまぬセキュリティへの取り組み。各 IT 企業には、信頼できるプラットフォームづくりへの協力を期待

【出所】<https://www.microsoft.com/ja-jp/mscorp/corporateaffairs/interview-fukuda.aspx>

2. マイナンバーカードインフラ優位性と世界観

business leaders square wisdom

検索 メルマガ登録 マイページ

トップ 事例 特集 連載 ワークショップ/セミナー イベントレポート

Orchestrating a brighter world NEC

2018年03月22日

マイナンバーカードは安全・便利・低コストなインフラ！ 新ビジネスや医療連携への応用事例とは

意外と知られていないことだが、マイナンバーカードには世界最高レベルのセキュリティを有する電子証明書が格納されている。この機能を利用して様々なサービスを提供する一般企業もセキュアな公的個人認証サービス（JPKI）を利用できるため、新たなビジネスチャンスへの期待が高まっている。ここでは既に実証実験が進んでいる、このセキュアな仕組みを活用したデジタルチケットへの応用や、地域をまたいだ医療情報連携のユースケースの紹介をはじめ、社会の仕組みや様々な業界での新しいビジネスの可能性を探る。

デジタル空間で「自分が自分であることを証明する」には

新着記事

- 金融×DXはNew Normalなこれからの社会の基盤を築く
- 「お世話する」から「自立支援」へ。新しい介護のあり方への挑戦
- 多くの企業がデータ活用の前に「うんざりする理由」とその解決策
- 備えない防災「フェーズフリー」が今後のまちづくりの力主を握る
- NEC Visionary Week 特集：パートナーと挑むDX



【出所】<https://wisdom.nec.com/ja/business/2018032201/index.html>

○世界観が分かる動画

https://www.youtube.com/watch?v=0SUpb0s7wD8&feature=emb_logo

おわりに

サイバーセキュリティ法制は、守る(＝罰則を与える。義務を課す)以外に攻める(＝ルール形成をする。新たな競争軸を作る)側面が重要であることがサイバーセキュリティ基本法をスタートに理解いただけたと思います。

経営者目線に加え、安全保障の目線も必要となります。

そこに最もよい提言ができるのは、他でもないセキュリティ専門家の皆様なのです。

是非、「ここは、海外と比較して・・・」とか「なぜ、できないのだろう」とか「よくわからないよな」を大事にして、SECKUNで培った講師や受講生人脈を通じて、よりよいルール形成の動きを作っていきましょう！

(参考)改めて・・・。SECKUNのこだわり

◆全科目

○0から生み出すこと。実務課題の解決につながる学問的研鑽・訓練

◆技術科目

○1次情報・自力での高い壁を乗り越えること

◆マネジメント科目

○高度な技術を重視しながら、ルール、ビジネスを生み出す。

◆ブリッジ科目

○人間・社会の理解：セキュリティ心理学、インテリジェンスと地政学、TTX(命のはなし)

○人間・社会との関係づくりと対応：PR戦略演習、セキュリティ倫理

あたらめて全体を見渡して、受講したくなかった科目は、オンデマンドで見直してみてください。気づきがあるはず。
その後、出せてなかった演習や課題を出す相談をいただいても大丈夫です。

5. ご意見をおよせください

1. ご意見をおよせください

セキュリティビジネスを推進する上で必須だがグレーゾーンと言われるシーン
とがった技術を海外では当たり前展開できる環境があるのに日本にはないシーン
海外法令との関連でよくわからないシーン
など……。法令名がわからなくても大丈夫です。
いただいたご意見は、藤岡にて整理して、福田峰之先生他専門家チームにお伝えし、
方策を検討します。
改善にむけた一步を踏み出しましょう！
連絡先：prosec-it-staff@cs.kyushu-u.ac.jp 担当：藤岡