AIとサイバーフィジカルシステムの進化と社会
―SF 映画を題材に―

弁護士　高橋郁夫

（なお、映画の画像は、公式ページ等より）

2001年宇宙の旅

- モノリス
- HALの暴走
  - 至上最高の人口知能
  - HALの思考部を停止させるべくした乗組員を殺害

CPSとAIとしてのHAL

- スターゲートを通じてのスターチャイルドへの進化

- なお、映像はイギリス映画協会でのトレーラーより

サイバーフィジカルシステムについて (NIST Frameworkより)

- 定義
  - 有体物（physical）および電子計算コンポーネンツを内包するスマートシステム
  - IoTとの相違
    - I o Tは物理世界にあるものを中心とした見方－インターネットにつながることを重視　vs　CPSは物理世界の情報とサイバー世界の情報が融合することに重点
    - 法的には、この表現（CPS）を支持したい
  - 従来との相違点
    - サイバーとフィジカル、その連携が重要である。センサー、コンピュータ、稼動部が必要である。
    - CPSは、情報技術と伝統的な操作技術(operational technology (OT))を必要とする。システムのシステムとして存在しうる
    - 相互流用性、管理進化、緊急対応などの必要性
    - …

IoT v. CPS

- IoT定義
  - 「インターネットに多様かつ多数の物が接続され、及びそれらの物から送信され、又はそれらの物に送信される大量の情報の円滑な流通が国民生活及び経済活動の基盤となる社会の実現」
- 民法85条
  - この法律において「物」とは、有体物をいう。
- IoTの問題
  - インターネットの問題<有体物性による問題
- 有体物としてみえてくる問題

番号	名称	メモ	法	
1	スケートボード	JVNDB-2015-002216 Boosted Boards	消費生活用製品 (消安法)	METI
2	自動車	自動車のリコール制度など	道路運送車両法	MLIT
3	医療ロボット		医薬品医療機器等法	MHLW
4	産業ロボット		労働安全衛生法	MHLW(労働基準局安全衛生部)

Things v. System

物のインターネット

- 「 IT pro「CIA」の視点で見るIoT機器のセキュリティ（後編）
  2016/02/16 高倉 弘喜 」

Security(CIA) v. Safety

サイバーフィジカルシステム

- 意義
  - 一定の目的のために機能するような統一体
  - 法的には、どのような意味をもつのか？
- 「ハザード対応」の視点でみるCPSのセーフティ

「産業用ロボットの使用等の安全基準に関する技術上の指針」
磁気テープ等の管理
(1) 事業者は、産業用ロボットの作動プログラムが記憶されている磁気テープ、フロッピーディスク、せん孔テープ等（以下「磁気テープ等」という。）又はその容器に当該プログラムの内容を表示すること等により、磁気テープ等に係る選択誤りを防止するための措置を講ずること。(略)

AIについて

- 定義
  - 人口知能の定義は、専門家の間でも定まっていない。「知能」の定義が明確でないので、人口知能を明確に定義できない。
  - ひとつの考え方
    - 「入力に応じて適切な出力をする」という定義
- AIのレベル

	用語	意義
1	単純な制御プログラム	ごく単純な制御プログラムを登載しているだけの家電製品
2	古典的な人工知能	振る舞いのパターンがきわめて多彩なもの
3	機械学習人工知能	推論の仕組みや知識ベースが、データをもとに学習されているもの
4	ディープラーニング	データをもとに、コンピュータがみずから特徴量をつくりだす（変数自体を学習）。

AIのレベル　強いAIと弱いAI

- 強いAI
  - 「正しい入力と出力を備え、適切にプログラムされたコンピュータは、人間が心を持つのと同じ意味で心をもつ」
- 弱いAI
  - 「限定された知能によって一見知的な問題解決が行えればよい」

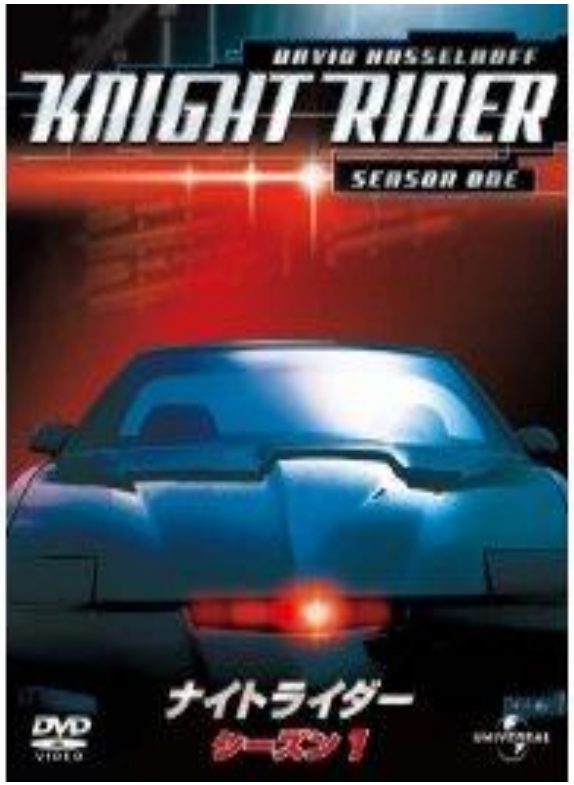
どこからが「強い」のか？ー心をもつのか

- チューリング・テスト
  - 人間の判定者が、一人の（別の）人間と一機の機械に対して通常の言語での会話を行う。判定者が、機械と人間との確実な区別ができなかった場合、この機械はテストに合格したことになる。

- ブレードランナー
  - Nexusというアンドロイドが地球に脱走　それを処分する

弱いAIとCPSの法律問題
ー自動運転自動車／手術ロボット

- ナイトライダー



- ドリーム・カー『ナイト2000』
  - 人間の言葉を話し特殊装備を搭載
- K.I.T.T.（Knight Industrial Two Thousand）
  - ナイト2000に搭載された人工知能
  - マイケルの相棒
  - 基本的にマイケルの命令で行動

Prometheus（2012）

- 『エイリアン』（1979年）の前日譚（？）
  - 「正体不明の生物に寄生され、それが急速に成長していると確信したショウ」
  - 全自動手術装置で帝王切開術を受けようとする。
  - 男性専用の装置だったために堕胎は不可能と処置を拒否される
  - 腹部の異物摘出に指示を変更して手術に成功。
  - 体中から取り出されたのはイカのような姿をした肌色で軟体の生命体であった。

医療用ロボット（手術ロボット）

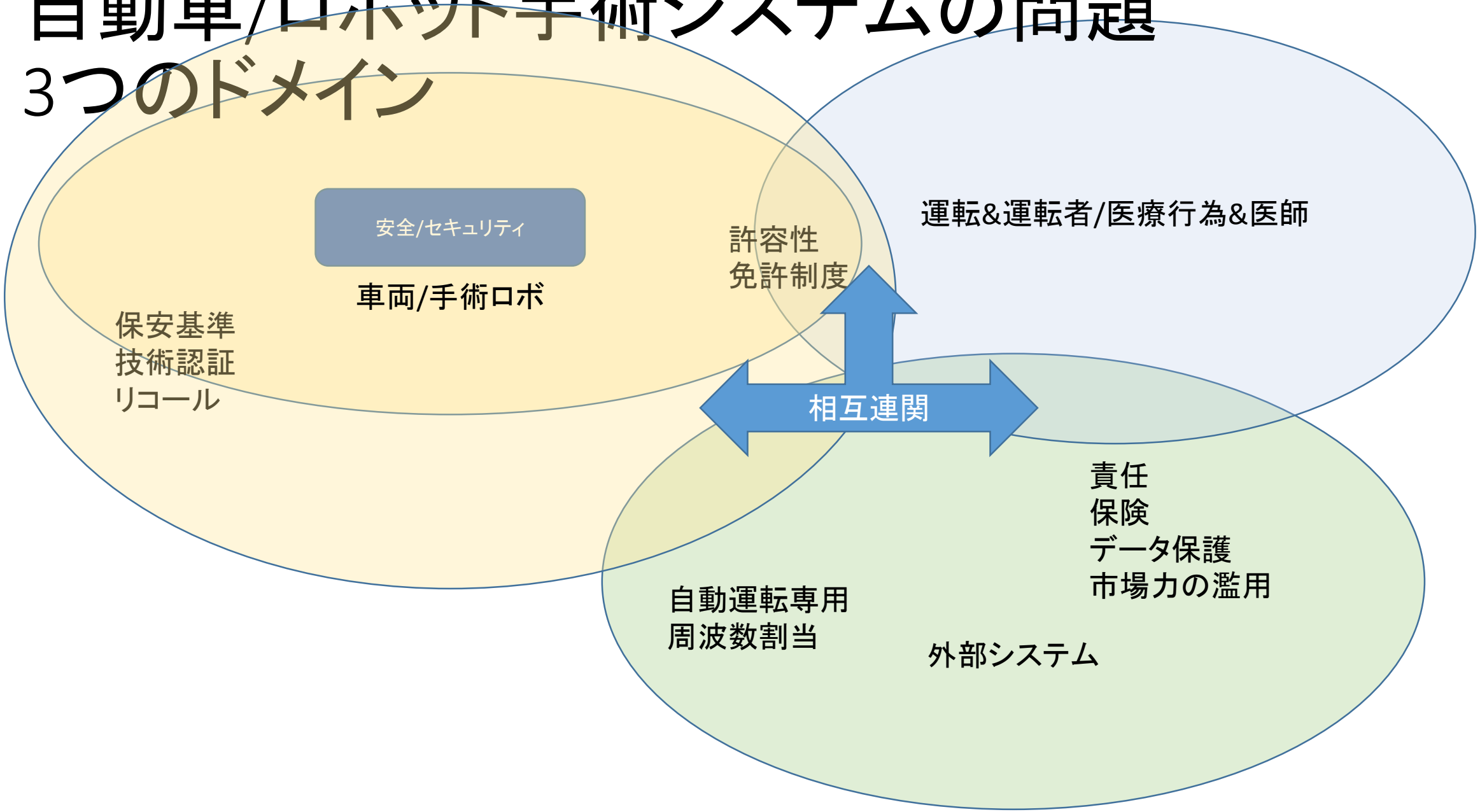
- 医療用システム
  - 手術用ロボット、追加機器、周辺サービスをすべて含むものに対する一体
- DaVinci
  - Intuitive Surgical社
  - 手術ｼｽﾃﾑ

Intuitive surgical社　HPより

いま、おきている法律問題

- 自動運転自動車/手術ロボットのセキュリティと安全の問題
- 自動運転自動車/手術ロボットの事故の問題
- データ駆動における「プライバシー」の意味と問題(自動車/医療)
- 人口知能と証券取引

自動車/ロボット手術システムの問題
3つのドメイン



自律走行自動車の検討

- 「日本再興戦略」改訂２０１５において、次の取組を進め、「完全自動走行の早期の実現を目指す」という方針
  - 公道実証実験を積極的かつ安全に行うための環境を整備すること
    - 公道実証実験を積極的かつ安全に行うための環境を整備すること、道路交通法等を含め、事故時の責任関係のほか、運転者の義務等の在り方について検討することが必要である
  - 道路交通法等を含め、事故時の責任関係のほか、運転者の義務等の在り方について検討することが必要である
- 「自動走行の制度的課題等に関する調査研究報告書」（NPA報告書）
  - 株式会社日本能率協会総合研究所
  - 公道実験に関するガイドライン（省略）を含む

官民ITS構想・ロードマップ2015の分類

【表１】安全運転支援システム・自動走行システムの定義

分類		概要	左記を実現するシステム	
情報提供型		ドライバーへの注意喚起等	「安全運転支援システム」[4]	
自動化型	レベル１：単独型	加速・操舵・制動のいずれかの操作をシステムが行う状態		
	レベル２：システムの複合化	加速・操舵・制動のうち複数の操作を一度にシステムが行う状態	「準自動走行システム」	「自動走行システム」[5]
	レベル３：システムの高度化	加速・操舵・制動を全てシステムが行い、システムが要請したときのみドライバーが対応する状態		
	レベル４：完全自動走行	加速・操舵・制動を全てドライバー以外が行い、ドライバーが全く関与しない状態	「完全自動走行システム」	

自動運転の許容性

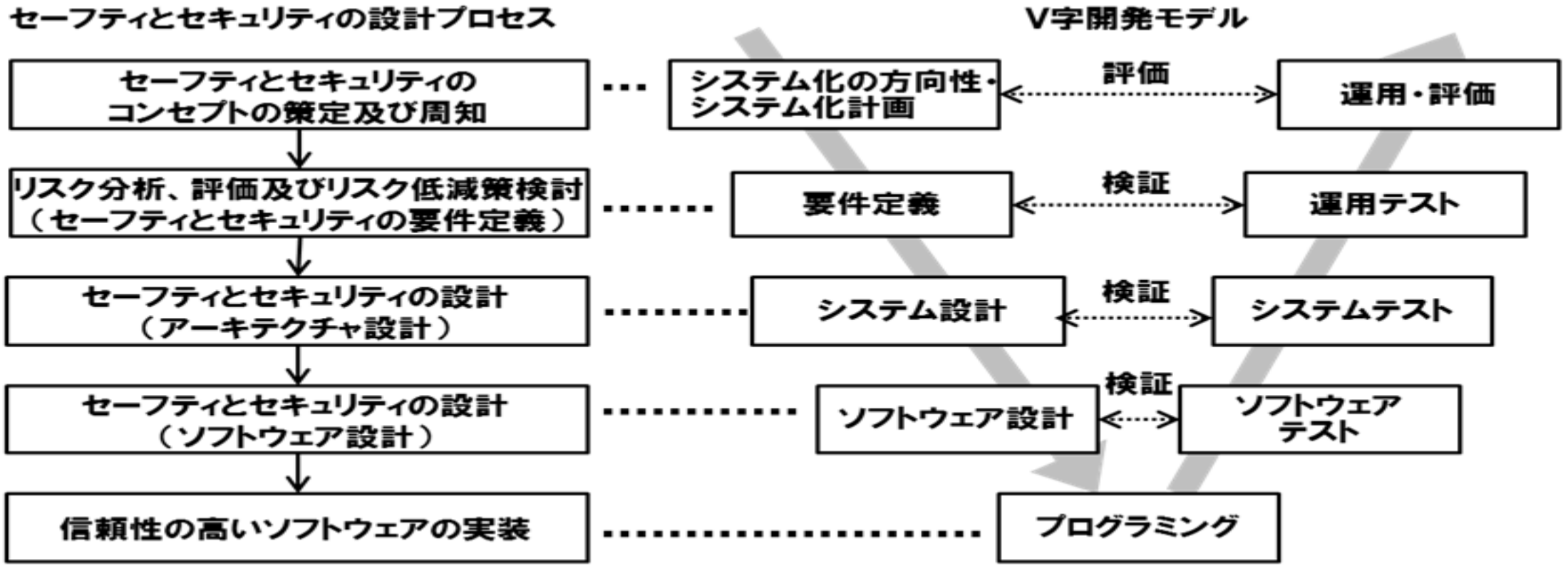
- １９４９年ジュネーブ交通条約（道路交通に関する条約）
  - 第8.1条：
    - 一単位として運行されている車両又は連結車両には、それぞれ運転者がいなければならない。
  - 第8.5条：
    - 運転者は、常に、車両を適正に操縦し、又は動物を誘導することができなければならない。運転者は、他の道路使用者に接近するときは、当該他の道路使用者の安全のために必要な注意を払わなければならない
  - 第10条：
    - 車両の運転者は、常に車両の速度を制御していなければならず、また、適切かつ慎重な方法で運転しなければならない。運転者は、状況により必要とされるとき、特に見とおしがきかないときは、徐行し、又は停止しなければならない。
- 道路交通法70条（安全運転の義務）
  - 「車両等の運転者は、当該車両等のハンドル、ブレーキその他の装置を確実に操作し、かつ、道路、交通及び当該車両等の状況に応じ、他人に危害を及ぼさないような速度と方法で運転しなければならない。」

クライスラー・ジープのリコール問題（カスペルスキーブログより）

安全/セキュリティ

- 安全の問題
  - 生命・身体・財産に影響を与えうるおそれに関する問題
    - 「安全とは、受容できないリスクから免れている状態」(JIS Z 8051:2004 の定義 3.1)
    - 安全とは、「安全、死、傷害、職業病、備品・財産に対する損傷・消失、または、環境に対する損傷を惹起しうる状況から免れていること」MILSTD882E
- セキュリティ
  - 設計された機能について、機密性・完全性を保ちながら、これを果たしうる状態

安全を考慮した設計手法



総務省「IoT セキュリティガイドライン ver 1.0（案）」37頁より

保安基準

- 安全性確保のための法的仕組み
  - 国土交通省自動車局
  - 根拠法令は道路運送車両法
- 同法は、「道路運送車両に関し、（略）安全性の確保（略）を図」ることを目的とする。そして、「自動車は、次に掲げる装置について、国土交通省令で定める保安上又は公害防止その他の環境保全上の技術基準に適合するものでなければ、運行の用に供してはならない。」（41条）
  - 原動機及び動力伝達装置、車輪及び車軸、操縦装置、制動装置等について、「道路運送車両の保安基準」を満たすもの
  - 保安基準では、自動車の構造・装置について、安全確保及び環境保全上の技術基準を定め、その他の詳細事項については省告示で定めている

保安基準と情報セキュリティの交錯

- 脆弱性
  - 「ソフトウエア等において、コンピュータウイルス、コンピュータ不正アクセス等の攻撃によりその機能や性能を損なう原因となり得る安全性上の問題箇所」
    - 「外部からの攻撃の誘引」「セキュリティに関するもの」「問題個所（不具合）」
  - 上記脆弱性が原因で、保安基準をみたさなくなった場合、どのような対応が必要になるのか

リコール制度

- リコール制度
  - 「（国土交通大臣は、）その構造、装置又は性能が保安基準に適合していないおそれがあると認める同一の型式の一定の範囲の自動車（略）について、その原因が設計又は製作の過程にあると認めるときは、当該自動車（略）を製作し、又は輸入した自動車製作者等に対し、当該基準不適合自動車を保安基準に適合させるために必要な改善措置を講ずべきことを勧告することができる」（道路運送車両法、63条の2・1項）
- 勧告に従わないとき
  - 改善措置（同5項）
  - 命令に違反した際は懲役又は罰金（106条の4・1項）。
- 自動車のソフトウェアに瑕疵があった場合もリコールの対象となる。

技術基準が条文に融合へ

- 技術基準省令にサイバーセキュリティの確保を要請
- 省令条文案
  - （サイバーセキュリティの確保）
  - 第十五条の二 電気工作物（一般送配電事業、送電事業、特定送配電事業及び発電事業の用に供するものに限る。）の運転を管理する電子計算機は、当該電気工作物が人体に危害を及ぼし、若しくは物件に損傷を与えるおそれがないよう、又は一般送配電事業に係る電気の供給に著しい支障を及ぼすおそれがないよう、サイバーセキュリティ（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）第二条に規定するサイバーセキュリティをいう。）を確保しなければならない。

- （参考）技術基準への位置づけ
- 解釈条文案
  - 【サイバーセキュリティの確保】（省令第１５条の２）
  - 第３６条の２ 省令第１５条の2に規定するサイバーセキュリティの確保は、次の各号によること。
    - 一 スマートメーターシステムにおいては、日本電気技術規格委員会規格 JESC Z0003（２０１６）「スマートメーターシステムセキュリティガイドライン」によること。
    - 二 電力制御システムにおいては、日本電気技術規格委員会規格JESC Z0004（2016）「電力制御システムセキュリティガイドライン」によること。
- JESC規格を解釈で引用。（省令に適合するものであることの明確化）

テスラの「自動運転」中に事故が発生

- 報道(2016年6月)
  - 米テスラ・モーターズの主力車種「モデルS」が半自動運転のオートパイロット機能での走行中に衝突事故を起こし、運転手が死亡
  - モデルSが中央分離帯のある幹線道路を走行中、対抗してきた大型トレーラーが左折し、モデルSと直角方向に道路を横切った時に、その側面にモデルSが突っ込んだ
- テスラの主張
  - 「オートパイロットとドライバーはどちらも、晴れた青空が背景だったため大型トレーラーの真っ白な側面部分を認識できず、ブレーキが作動しなかった。トレーラーの車高が高いという極めて珍しい状況が重なって、モデルSはトレーラーの下を通る形になり、トレーラーの底部がモデルSのフロントガラスにぶつかった」
  - レベルとしては、レベル2の自動運転(補助)

保険の設計と自動運転技術の採用

- 交通事故を減少-保険料を減少-自動車保険の意義
- 運転手の責任の概念
  - 薄まってくるのではないか
- プログラミングのエラーから事故が発生
  - 損害額が多大
- 自動車両の運転の任が、運転者から、運転車両に移転
  - 事故時における法的な責任が、製造業者に移転
  - 完全自動運転や部分的自動運転の場合
    - 当初-そのような自動車を運転することが危険
- 損害の予測可能性
  - 製造業者-技術の採用に臆病になる「萎縮効果」

データのセンサーとしての自動車とそのシステム

- 自動運転
  - 少なくとも数百メートル先の道路状況等の検知が必要
  - 必然的にITインフラによる連続的なデータ提供を必要
  - 運転の自動化が実現されればそのデータ量は比較にならないほど膨大/データの内容も個人のセンシティブなプライバシーに関わる
- システムとしてのとらえ方
  - 自動車にデータを供給する部分に問題があったならば、「自動車」（？）としてリコールの対象になるのではないか？

人口知能による証券取引

- 種々の現れ方
  - ロボ・アドバイザー取引（客に対して資産運用のアドバイスを行うために人工知能を用いる）
    - （一定の場合）投資助言・代理業の登録が必要となる（金融庁）
  - 顧客のID等の利用を委託され 自動売買プログラムにもとづき取引をなしていた業者
    - 投資運用業に係る業務を行ったものとして行政処分を課す事例が出現（インベストメントカレッジに対する行政処分　平成27年10月20日　金融庁）
  - 証券取引のアルゴリズム自体を人工知能による特徴量の生成にゆだね、株価の動向を予測し取引をおこなう

人工知能による株価予測

- 実用化
  - 株価騰落予測システム
  - 時系列株価データをRNN（リカレントニューラルネットワーク）により解析
- 理論的
  - モメンタム取引戦略への応用
  - 自然言語解析を用いたイベント基盤の株価予測への応用

ディープラーニングの進化と証券市場へのリスク

- (1) 証券取引システムの自律性
  - 運用者は誰か
    - 投資家orシステムの提供者（投資一任業務）
    - 具体的な事情による（by　金融庁「金融商品取引業者等向けの総合的な監督指針」（平成28年９月）　Ⅶ－３　諸手続（投資助言・代理業）　１　登録　）
      - 投資家の自主的な判断をアシスト-「不特定多数の者を対象として、不特定多数の者が随時に購入可能な方法により、有価証券の価値等又は金融商品の価値等の分析に基づく投資判断を提供する行為」
      - 登録が必要(販売業者等から継続的に投資情報等に係るデータ・その他サポート等の提供を受ける必要がある場合)
      - 投資運用業の場合(前述)
  - 個人の保護の必要は？
    - 想定を超えるリスクの可能性

ディープラーニングの進化と証券市場へのリスク(2)

- (2)証券取引システム自体の問題
  - 市場の価格変動(ボラ)の進行の可能性(フラッシュ・クラッシュ)
    - サーキットブレーカー
  - 情報セキュリティ上の問題点と修正権限
- (3)証券取引と市場との関連
  - ファンダメンタルとは関係のないアルゴリズムの一般化
  - 北越紀州製紙株価操縦事件
    - 取引誘引の認定
- (4)市場の専門化・参加者の偏り？

これから起きる(？)法律問題

- シンギュラリティ
  - 人口知能が自分の能力を超える人口知能をみずから生み出せるようになる時点を指す
  - 数学者ヴァーナー・ヴィンジ/発明者・フューチャリストのレイ・カーツワイルにより提示(2005ころ)
- シンギュラリティの可能性
  - 科学としてはありうるのか(？)-「人口知能は人間を超えるか」(松尾 豊)

	特徴	問題点
人口知能をロボット生命化	人工知能の主体行動/自己保存欲望のインストール	ロボット工場の製造が困難
ウイルスによる生命化	自分自身のプログラムをコピーして増殖	こんな巨大なプログラムは、困難。例外や環境変化に弱い
人口生命に知能	人工的な生命体に人工知能を組み込む	いったい何億年待つのか？

シンギュラリティを越えた時点におきる問題点

- 社会システムの決定権の移行
  - 権利･義務の体系(主体は、自然人及び法人)に機械人が加わるのか
  - 体系の決定権が移行するのではないか
- そもそも、有機生命体が存続しうるのか
  - 物理力と情報力のヒエラルキーの逆転

権利･義務の体系(主体は、自然人及び法人)に機械人が加わるのか

- ロボット税の議論(EU)
- 有機生命体とは、異なる種としての認識
- 恋愛感情が発生するのか
- 相続問題はどうか

体系の決定権が移行するのではないか

- 自律的な人工知能が、武力(Armed Force)を行使しうることを認めうるのか
- 人工知能の生み出す財・有形力が大きければ、有機生命体は、生き延びれるのか
- SkyNetは、人類を守るためのネットワークのはずであった。

自律的な兵器をめぐる議論

- 自律型致死兵器システム（Lethal Autonomous Weapons System,LAWS)または、「致死性自律型ロボット(Lethal Autonomous Robotics, LARs)」
  - 近時の動向
    - 「司法外、略式又は恣意的な処刑に関する特別報告者の暫定報告書」(2010)
    - 「ヒューマン・ライト・ウォッチ報告」(2012)
    - 「米国防省指令 3000.09(兵器システムにおける自律性)」(2012)
    - 「ヘインズ報告書(2013)」
    - 国連における特定通常兵器使用禁止制限条約（CCW）自律型致死兵器システム（LAWS）第3回非公式専門家会議(2016)
- ユス・アド・ベルムやユス・イン・ベロの規定を自律的に判断をなしうるのか、その判断の正当性の検証は？

有機生命体の限界を越えた知性は？

- 「2001年宇宙の旅」に戻ることにしよう