資料３－３

サイバーセキュリティタスクフォース第3回(2017/3/27)

# IoTセキュリティ対策の法的側面

弁護士
京都大学大学院医学研究科講師（非常勤）
岡村　久道

# IoTセキュリティ制度対応を検討する際の前提問題

- IoTといっても多様
  - コネクティッドカーと産機セキュリティを同一線上で論じられるか？
- 関係者が複数
  - メーカー（設計・製造者）↔販売・輸入業者↔電気通信事業者（媒介者）↔エンドユーザー（法人・個人の利用者）
- 時間軸の問題
  - 上記流通ステップのほか、時間の移行に伴って新たな脅威が出現するのに対し、IoT製品はライフサイクルが長いものがあるという問題
- 責任境界線の問題
  - 具体例として、車載システムに欠陥があった場合と、ユーザーによる整備怠慢
- その他
  - 接続端末たるIoT機器が、ユーザー側（事務所・自宅）で「むき出し状態」
  - どこからでも、どこに対しても、いつでも攻撃されるおそれ
  - IoT通信量増加によるバンド幅の圧迫←可用性の問題
  - データ保有による市場支配力形成等の可能性（但しセキュリティの問題ではない）

# 時間軸の問題 1

- 問題の概要
  - 時間の移行に伴って新たな脅威が出現して対抗を要するが、製造業者等が負う製造物責任は重い。
- 製造物責任法（PL法）の概要
  - 製造、加工、輸入等した製造業者等に対し、製造物の「欠陥」に関し、損害賠償責任を負わせる（3条）。
  - 責任期間は、出荷から原則10年間（5条）。
  - 「製造物」は動産に限るので、ソフトウェアそれ自体は該当しないが、それが動産に組み込まれると、組み込まれたソフトウェアを含めて全体として該当（通説・判例）。
  - 「欠陥」とは「当該製造物の特性、その通常予見される使用形態、その製造業者等が当該製造物を引き渡した時期その他の当該製造物に係る事情を考慮して、当該製造物が通常有すべき安全性を欠いていること」等をいう（2条）。
  - 無過失責任だが、「当該製造物をその製造業者等が引き渡した時における科学又は技術に関する知見によっては、当該製造物にその欠陥があることを認識することができなかった」場合等は免責（4条）。これを「開発危険の抗弁」という。
  - 免責特約では対抗不可。

# 時間軸の問題 2

- IoT機器との関係
  - ネット接続されることによって新たに脅威にさらされ、時間とともに脅威が高度化し、セキュリティアップデートが必要となる。
  - しかもスキルが比較的低いエンドユーザーが対象。
  - 従来のPCやスマホでは製品のライフサイクルは比較的短いので問題になりにくい。これに対し、冷蔵庫等のライフサイクルは比較的長い。
  - 途上国との激しい製品価格競争の中で、コストダウンのため積載メモリー量も限られているので、その意味でもセキュリティアップデートには限界。
  - メーカー倒産の場合にはセキュリティアップデートが物理的に不可能。
  - 「開発危険の抗弁」は、立証責任が製造業者等の側にあり、どこまで免責を受けられるか疑問。
  - 場合によっては、ユーザーが自らネットから切断して、普通の冷蔵庫として安全・安心に使えるようにすべきではないか？

# 参考ーセキュリティ水準論（但しIoTに限らず）

- セキュリティ水準論
  - 法的に守るべきセキュリティ水準は、医療過誤紛争における医療水準論と同様に、IT等の現場における水準を考慮して、その時点におけるIT等の実践におけるセキュリティ水準を基準とすべきことになろう（拙著「情報セキュリティの法律〔改訂版〕」224頁）。
- TBC顧客情報漏えい事件の東京地判平19・2・8
  - 「本件情報流出事故が発生した平成14年ころにおいても、個人情報を取り扱う企業に対しては、その事業内容等に応じて、個人情報保護のために安全対策を講ずる法的義務が課せられていた」が、委託先は、その提供する業務に関する技術的水準として、個人情報を含む電子ファイルについては、一般のインターネット利用者からのアクセスが制限されるウェブサーバの「非公開領域」に置くか、「公開領域」に置く場合でも、アクセスを制限するための「アクセス権限の設定」か「パスワードの設定」の方法によって安全対策を講ずる注意義務があったが、これを怠ったとして損害賠償責任を認めた。
- 東京地判平26・1・23判時2221号71頁
  - Xの発注によりYが設計、製作したアプリケーションのSQLインジェクションに対する脆弱性によって、Xの顧客のクレジットカード情報が漏えいしたため、Xによる顧客対応等が必要となったために損害を被った事案で、経済産業省等からの注意喚起に照らし、前記システム発注契約締結時点で、漏えい防止対策としてバインド機構の使用またはエスケープ処理を施したプログラムを提供すべき債務を負っていたが、これを怠ったとして、YのXに対する損害賠償責任を認めた。

# 責任境界線の問題－コネクティッドカーを素材に

- レベル4時代でも交通事故原因は多様
  1. ハードウェア（自動車）の欠陥
  2. ソフトウェアのバグ
  3. ソフトウェアのセキュリティホール－サイバー攻撃
  4. データの誤り・未更新
  5. 通信途絶
  6. 整備不良
  7. 道路の欠陥
- 誰が責任を負うべきか？
  - これをサービス提供とみれば、被害者との関係では、1～5はすべて提供者側の契約責任の問題（ISP等はサービス提供者の履行補助者）。
  - 損害保険でカバーすべきか？
  - ちなみに6はユーザー側の責任だが、ブラックボックス化している状態なら、車検制度に組み込む必要がないか？

# 関係者が複数という問題－多重防御の必要性

- メーカー（設計・製造者）
  - SBDの啓発、学べる仕組み作り
- 販売・輸入業者
  - 医療でいうインフォームドコンセントの発想
- 電気通信事業者（媒介者）
  - 見守りサービスの提供
  - 通信の秘密との関係では同意・緊急行為
- エンドユーザー（法人・個人の利用者）
  - 家庭等の入り口での防御機器
  - 教育－学生向け「e－ネットキャラバン」を従来の違法有害情報＋セキュリティ教育へ拡大

# IoTセキュリティの制度的実装

- 機器の定期検査義務
  - 車検がモデル
  - 政省令でリアルタイムにセキュリティ水準に合わせるが、猶予期間を置く
- 温故知新？ーモデルとしての消費生活用製品安全法

第1章　総則（1条・2条）
第2章　特定製品
　第1節　基準並びに販売及び表示の制限（3条ー5条）
　第2節　事業の届出等（6条ー15条）
　第3節　検査機関の登録（16条ー19条）
　第4節　国内登録検査機関（20条ー29条）
　第5節　外国登録検査機関（30条・31条）
　第6節　危害防止命令（32条）
第2章の2　特定保守製品等
　第1節　特定保守製品の点検その他の保守に関する情報の提供等（32条の2ー32条の17）
　第2節　特定保守製品の点検その他の保守の体制の整備（32条の18ー32条の20）
　第3節　経年劣化に関する情報の収集及び提供（32条の21・32条の22）
第3章　製品事故等に関する措置
　第1節　情報の収集及び提供の責務（33条・34条）
　第2節　重大製品事故の報告等（35条ー37条）
　第3節　危害の発生及び拡大を防止するための措置（38条・39条）
　　《以下省略》