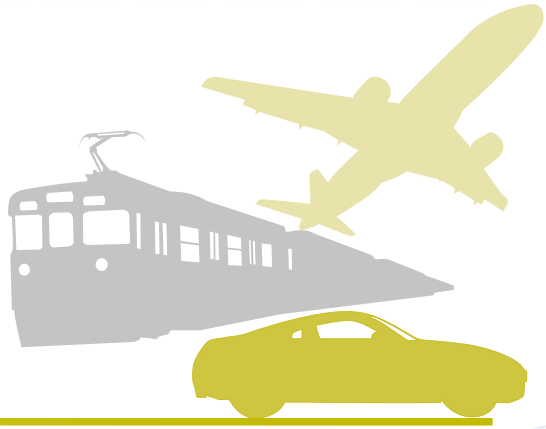
情報セキュリティと乗り物 基般



大久保 隆夫（情報セキュリティ大学院大学）

情報セキュリティの基本概念

近年，自動車や航空機，ドローンなど，乗り物に対するハッキングの事例が相次いで公開され，話題となっている．これらの乗り物は，従来から安全性等を考慮して設計され，安全性基準をクリアした上で，発売，運用されているはずである．それなのに，なぜこのように次々とハッキングを許すことになっているのだろうか．その原因は，「安全性」には 2 つの概念が存在し，従来は主にその一方しか考慮されてこなかったためである．考慮されてきた方の安全性は英語では「セーフティ（safety）」，考慮されてこなかった方は「セキュリティ（特に情報セキュリティ（information security））」と呼ばれる．両者の違いについては次の記事に譲るとして，ここではそれを考えるための情報セキュリティの基本的な概念の紹介からはじめたい．

CIA

情報セキュリティの基本概念は，CIA という言葉で表現される．CIA といっても，ドラマに出てくるアメリカの中央情報局ではなく，Confidentiality（機密性），Integrity（完全性），Availability（可用性）の 3 つの頭文字をとったものである．

C（機密性）：情報の秘密が保たれ，第三者に漏洩しないこと．
I（完全性）：情報が第三者に改ざんや破壊されずに，一貫性が保たれること．
A（可用性）：情報が必要とされるときに利用できること．

上記の観点で保護対象になる情報を，情報資産と呼ぶ．情報資産の例としては，個人情報や会社の機密情報，購買履歴や契約などの抽象的な情報，システムログなどのシステム上の具体的なデータも含まれる．

情報資産に対して，攻撃者は，上記の CIA を破る攻撃をしかけてくる．たとえば，機密性の保持が必要な個人情報に対しては盗聴されたり漏洩する，完全性に対しては情報を改ざんする，可用性に対しては情報を参照できない状態にするなどの脅威が考えられる．したがって，システムや製品を構築する際には，システムや製品が持つ情報資産に対してどのような攻撃の脅威が存在するか，またそのリスクはどのくらいかを分析し，リスクを低減，回避等する対策を設計，実装する．これが情報セキュリティ的な安全性を保全するための活動である．

セキュリティ対策として実現される技術には，暗号化や認証技術がある．情報を暗号化することで，復号のための鍵を持つ当事者以外に漏洩しないようにする「機密性（CIA の C）」を保持することができる．また，認証も，情報資産にアクセスできる人間を制限することで，第三者への漏洩や改ざんを防ぐ（CIA の I）．DoS 攻撃など，多数の通信の一斉送信により負荷を集中させ，サービスの可用性（CIA の A）を低下させる攻撃に対しては，特定の通信の排除（フィルタリング）や，負荷に対する耐性の強化などの対策が考えられる．

weakest link と多層防御

weakest link とは，英語のことわざ「A chain is no stronger than its weakest link.」に由来する．鎖の強さはその最も弱い結合部の強さによって決まるという意味である．システムや機器のセキュリティにおいても同様なことが言え，システムや機器の中で攻撃者は

最も脆弱な個所を狙ってくる．したがって，「平均的な安全性」という基準は意味を持たない．このようなweakest link への対策アプローチの 1 つが多層防御である．多層防御（defence in depth）とは，セキュリティを脅かす脅威に対して，1 つの層だけでなく，多重の層で防御を行うという考え方である．たとえば，組織ネットワークの入口をファイアウォールで守ればよし，とするのではなく，いったんファイアウォールを突破されてしまった場合を考慮して次の防御策を考慮しておく，といったものである．

乗り物とセキュリティ

では，乗り物においては，情報セキュリティ上どのような脅威が存在するのか．自動車を例に考えてみる．自動車は，昔の機械というイメージとは異なり，現在ではコンピュータのかたまりである．1 台の車には，100 種以上の ECU と呼ばれるコンピュータが搭載されており，各 ECU はアクセス，ブレーキ，エンジン，トランスミッション，カーナビなどの制御をつかさどり，これらは ECU 上で動作するソフトウェアによって行われる．また，各 ECU はほかの ECU の制御に情報を信号として渡す．すなわち，自動車であってもサーバやパーソナルコンピュータがネットワークを介して通信しているシステムと構造的には同じであり，コンピュータシステム上で起きている脅威（データの盗聴（CIA の C）や改ざん（CIA の I）など）はそのまま自動車にもあてはまることが推測できる．また，最近の車載システムはカーナビとも接続されているため，ナビの持つ位置情報や移動経路情報を持つことになるが，これらの情報は運転者のプライバシー情報になるため，位置情報などが意図しない形で漏洩しないように対策する必要がある（CIA の C）．たとえば，要人の乗る車の位置が外部から追跡できたら…　と考えてみれば，分かりやすいだろう．しかし，乗り物は，動力を使って移動するというサービスを提供し続けなければならない以上，CIA のうち，乗り物にとって最も重要なのは可用性（CIA の A）である．エンジンやモータを始動するための信号が第三者によって妨害された場合，乗り物は動かなくなり，その役割を果たすことができなくなってしまう．

乗り物のセキュリティ事例

では，具体的にセキュリティ脅威となるような事例はどれだけ起きているのか．

自動車の例では，2013 年にハッカーグループが，ハッカーの国際会議「DEF CON」で，車内のコネクタ経由で車載のネットワークにアクセスし，ECU に偽の信号を送ることで車の制御を一部乗っ取るハッキングに成功したことを発表した．この例では，走行中にスピードメータを 0 にするだけでなく，急加速，ブレーキ，ハンドル制御の奪取などを行う様子が動画で公開された☆1．2015 年にはこの制御の乗っ取りが無線 LAN 経由で行われた例が発表された☆2．

また，航空システムやドローンに対するハッキングの成功例も国際会議等で発表されている．もはや，狙われていない乗り物はないといった状況である．なぜ，このような事態になっているのかについては，次以降の記事が参考になるはずだ．

（2016 年 3 月 30 日受付）

☆1 https://www.youtube.com/watch?v=oqe6S6m73Zw
☆2 http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

大久保隆夫（正会員）　okubo@iisec.ac.jp
1991 年東京工業大学物理情報工学専攻修了．同年（株）富士通研究所入社．2013 年より情報セキュリティ大学院大学准教授，2014 年より同大教授．博士（情報学）．専門はソフトウェア工学，システムセキュリティ．