社会学的安全性と数学的安全性

パナソニック電工株式会社　EMITプラットフォーム開発センター
福田　尚弘

情報セキュリティの世界に触れ15年くらいが経つが、今後の情報セキュリティとどう向き合っていくべきか悩ましい限りだと思っている。情報セキュリティを守るために会社で「ガミガミ」言われることがある。「うんざり」という人も多いだろう。永遠にこんなことが続くのだろうか？

ここでは5年～20年先の情報セキュリティを見据えたところで、情報セキュリティ分野での社会学的研究が進んでいる。そういった研究結果が得られた後の世界を予測し、過去の数学的な安全性の試みと合わせた見方で情報セキュリティの未来を考えてみた。

◆ コンピュータの普及

今から60年前、情報理論で有名なクロード・シャノン（Claude Shannon）は「暗号理論」の先駆者であり、特に発明したワンタイムパット暗号の安全性を、「情報理論」を用いて証明した。この安全性は、「情報理論的安全性」と呼ばれる。一方、約30年以上前にディフィー（Bailey Diffie）とヘルマン（Martin Hellman）の研究者によって「公開鍵暗号」が発明された。以降、数値上での変換が可能なRSAと呼ばれる公開鍵暗号が、リベスト（Ron Rivest）、シャミア（Adi Shamir）、エーデルマン（Len Adleman）らによって発明された。この暗号の安全性は解読のための計算量が多項式時間に収まらない（膨大な時間がかかる）場合にその暗号は計算量的に安全という考えに基づいている。この安全性は、「計算量的安全性」と呼ばれる。

一方、この暗号は計算機の能力は時間と共に向上するという「ムーアの法則」と並行して普及している。これは興味深い。

「計算量的安全性」は「情報理論的安全性」よりも弱いとされている。しかし「計算量的安全性」は「情報理論的安全性」よりも「経済的」であることから、盛んに使われているのが現状だ。情報理論的安全性では、一般に鍵長が長くなるため使われることが少ない。加えて、「計算量的安全性」に基づく公開鍵暗号は「公開鍵」を相手が「信用」するという条件によって成立するモデルにより鍵配布や鍵管理が簡便となり、様々なセキュリティ・プロトコルで採用されている（例えばSSL、IPsecなど）。これは通信での「利便性」においても役に立っている。

◆ インターネットの普及

セキュリティ・プロトコルであるSSLやIPsecなどは、インターネットの普及により盛んに利用されてきた。プロトコルの安全性はプロトコル手順そのものが安全であるという以外にも、暗号の安全性とも係わることがあり、その組み合わせによっては極端に弱くなる可能性を秘め大変難しい。

RSAの公開鍵暗号と時を同じくして、約30年以上前にロジャー・ニーダム（Roger Needham）とミカエル・シュローダー（Michael Schroeder）により、NS（Needham Schroeder）プロトコルが発明され、これは後に有名なKerberosプロトコルの原型となったが、この時代にプロトコルの安全性が問題となり、セキュリティ・プロトコルの形式的検証（Dolev-Yaoモデル、BAN論理、機能的手法）が登場し [1]、近年では汎用結合性（Universal Composability）という安全なプロトコルの合成方法も提案されている。

ここで、形式手法による検証法は、一般にモデル検査と呼ばれる「意味論的」な方法と、「証明論的」な方法があり、「意味論的」な方法では、検査したいセキュリティ・プロトコルの全ての実行過程をトレー

スし網羅的に分析するものであり（虱潰し）、「証明論的」な方法は全ての実行過程で成り立つ性質（ノンスがフレッシュであるなど）から論理推論で証明するものである。

セキュリティ・プロトコルの形式的検証で、「意味論的」な方法は具体的な攻撃を発見するのに有効とされ、一方「証明論的」な方法は、そのプロトコルの形式的な証明に適しているとされる。どちらで評価しているのかによって、セキュリティ・プロトコルへの評価、安全性への考え方も変わってくるとも言えるだろう。

どちらであっても、セキュリティ・プロトコルの安全性の証明において「前提条件」が重要となってくる。「前提条件」とは実は厄介な代物である。たとえば、プロトコルの中で一回きりしかない数という意味である「ノンス」、またランダムな値を発生させる「乱数生成」などの条件である。これらは現実には作り出すことや維持することは難しいが、これらセキュリティ・プロトコルの安全性の議論では、大抵が「前提条件」の限り安全であるということが安全性の基礎となっている。特に「乱数生成」などは真の乱数は作るのは困難であり、それに近いセキュアな乱数を生成するのにも専用ハードウェアが必要など、コストがかかる代物だ。

◆ システムの普及

ここではSSLなどを用いたWebシステムを考えるが、SSLは上記の暗号アルゴリズムとセキュリティ・プロトコルとが結合したもので、それらはユーザー、すなわち「人」と関わるシステムで使われるということである。ここでは実際にシステムが運用されると問題が発生する、例えば「パスワード」である。

パスワードは暗号鍵同様に、推測されれば「おしまい」である。参考文献 [2]（IPA 小松文子氏）を解釈すればこうなる。社会学的に百人いれば、そのうち数十人（約36%）は真面目にパスワードを更新するが、そうでないユーザーはほとんど（約64%）である。これは、津波の警報で逃げない人々は約20%、火災報知器の例では、これは法律で定められているにもかかわらず、平均約60%の達成率である。残りの40%は強制的な法律にも従わないということだ。

> 情報セキュリティでの社会学はイギリスの功利主義、数学はドイツの理想主義ともダブる。理想主義は普遍的理念による体系として構築し、把握しようとするのに対し、功利主義は結果として生じる有用性によって決定されるものである。最大多数の最大幸福を求める総和主義でもある。
> 数学（理想主義）は「情報理論」、および「セキュリティ・プロトコル」を説明するもので、社会学（功利主義）は「人の一般行動」を説明するものとすれば、数学的安全性とは「情報理論的安全性」、および「セキュリティ・プロトコルの安全性」を示し、社会学的安全性とは「人の一般行動」から導くシステムの安全性を示せるのではないかと考える。
> 歴史的にイギリスとドイツは切磋琢磨し、それぞれ世界を制覇してきた。どちらがいいともいえないが、それらはお互い補完関係にあるかもしれない。

脆弱性はどうか？これは現在ではプログラマーは「人」であることが多いので、「人」に依存する。脆弱性はバグ密度などで表され、どのようなプログラマー（人）がどのような欠陥を何%くらい導入するかなどは今後明確にわかってくるかもしれない。

また、参考文献 [3]（ニコラス・クリスティン教授）によれば、脆弱性はお金にならないなら攻撃されない可能性もあるということ。これも計算可能かもしれない。ならば脆弱性があっても対策不要ということも社会学的な見地から可能かもしれない。

例えば、ゲーム理論を使って検討してみる（表１）。パスワードを更新する場合を3点、しない場合を１点とする、攻撃者がやる気満々である場合を－3点、やる気が薄い場合を－１点とする。合計の点数が組合せとすると、パスワードを更新して、攻撃者はやる気が薄い場合が最も高得点となる。

表１　攻撃者とパスワードの表

	パスワードを更新する	パスワードを更新しない
攻撃者がやる気満々である	(−3、3)=0	(−3、1)=−2
攻撃者はやる気薄い	(−1、3)=2	(−1、1)=0

これに社会学的な値を入れてみる。パスワードを更新するとしても実際には36％しか更新しないわけであるから、パスワードを更新するに0.36倍し、同様に攻撃者は金銭にならなければやらないとすれば、やる気薄いに0倍する。

表２　攻撃者とパスワードの表
（社会学的な配慮を行う）

	パスワードを更新する	パスワードを更新しない
攻撃者がやる気満々である	(−3、3×0.36)=−1.92	(−3、1)=−2
攻撃者はやる気薄い	(−1×0、3×0.36)=1.08	(−1×0、1)=1

表２で見れば、攻撃者はやる気薄い場合は、パスワードを更新しようとしまいと大して変わらないという結果を得る。

同様にワンタイムパスワードをパスワードの代わりに導入するかどうかも検討できる。

表３　攻撃者とワンタイパスワードの表
（社会学的な配慮を行う）

	ワンタイム導入	パスワードを更新する
攻撃者がやる気満々である	(−3、3)=0	(−3、3×0.36)=−1.92
攻撃者はやる気薄い	(−1×0、3)=3	(−1×0、3×0.36)=1.08

表３で見れば、攻撃者はやる気薄い場合は重要であるが、ワンタイムパスワードを導入すれば、最高点3の結果を得る。ワンタイムパスワードの導入よって、社会学的な影響が消えたことになる。これはシステムの対策によっては数学的安全性を増したことで社会学的影響を消すことができたとも言える。

このように、通常の考え、すなわち観念的に考えれば「パスワードを更新するべきだ」ということになるが、社会学的なフィードバックし、功利的に考えれば「パスワードを更新しようとしまいと大して変わらない」ということも得られる。

ただし、社会学的な見方は、時間、場所、人数、人材などが違えば変わってくるのであくまで一般的な話となろう。ではあっても、より功利的な結果を導きうると考える。

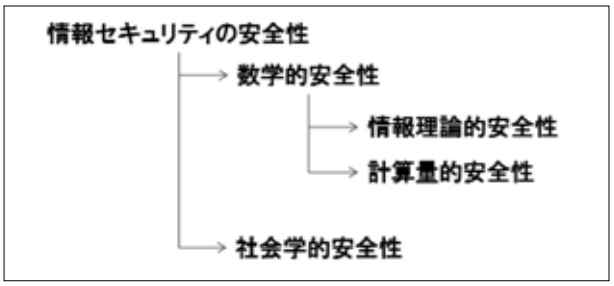
システムの問題は、「人」と関わるということだ。ここでの安全性としては「人と関わる」ために、現実には、暗号、プロトコルなど、前記の内容をはるかに超えた「リスク受容」を含むのではないか？

将来は人の代わりとなる「ボット」なども登場すると思われるが、基本的にシステムは人のためにある（もしマシンのためにあるならターミネータの世界である）、だから「人と関わる」ことへの研究が重要視されるだろう。

◆ 社会学的安全性と数学的安全性について

数学的安全性は「計算量的安全性」、「情報理論的安全性」、および「セキュリティ・プロトコルの安全性」を示し、社会学的安全性は「人の一般行動に基づく安全性」を示すことにする（図１。）

図１　情報セキュリティの安全性



一方、図２は社会学的安全性と数学的安全性の関係を図示したものである。ここでは、それぞれ安全性には「高い」と「低い」状態があって、低い場合には「レッドゾーン」としたが、ここに陥ると安全性が担保できないという線（ライン）を示した。

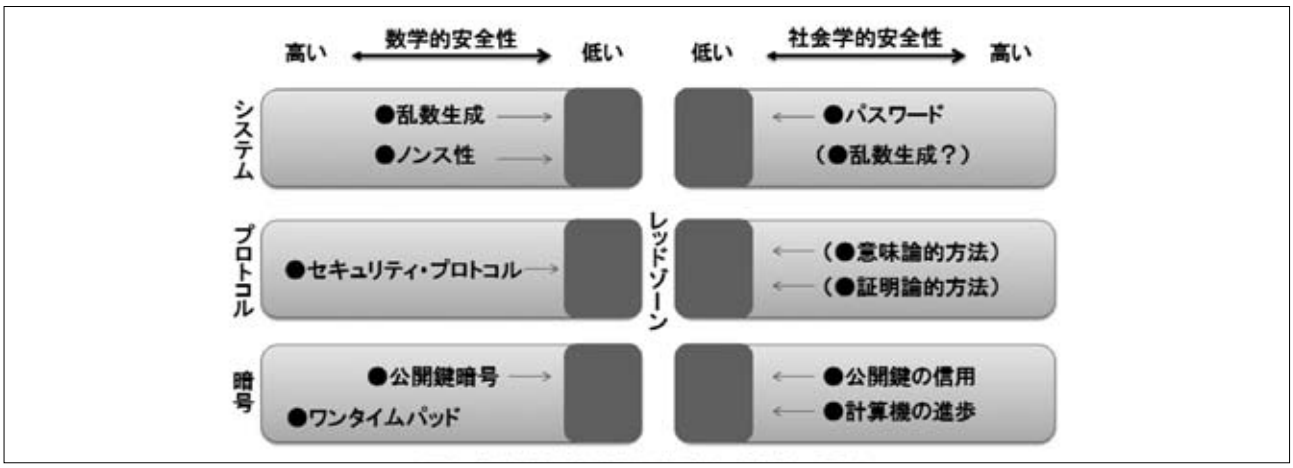
前に書いた通り、ワンタイムパッドは「情報理論的安全性」に基づく。しかし、鍵長の問題からそれより弱いとされる「計算量的安全性」に基づく公開鍵暗号が使われている。これは、数学的安全性で考えればワンタイムパッドよりも公開鍵暗号は弱い（低い）ということになる。それでも使うのは「経済性」を優先するからだ。

ところで、公開鍵暗号は「利便性」としてユーザーによる公開鍵の「信用」を用いて利用される。ところが、この「公開鍵の信用」は曲者だ。なぜならユーザーがこの公開鍵を用いて多対多の通信をしたとしよう、これは社会学的な側面を持つだろうからだ。だれをどこまで信用したらよいかという問題、詐欺にあうかもしれないという問題、これは社会学である。

これらもセキュリティ社会学または社会学的セキュリティの研究が進めばその傾向などは一目両全かもしれない。たとえば、信用しやすい人がいたら、その連鎖にある人々は一蓮托生の運命をたどるかもしれない。ここで、公開鍵暗号を使ったセキュリティ・プロトコルがあったとしよう。このセキュリティ・プロトコルの安全性は、公開鍵の信用がレッドゾーンに達したとき、セキュリティ・プロトコルが前記の「前提条件」を超えてしまい、セキュリティ・プロトコル自身の安全性も引きずられてレッドゾーンに入るかもしれない

また、「社会学的」に計算機の進歩を見逃し、20年経っているのにシステムを使い続ければ、公開鍵暗号が「計算量的安全性」を満たさないことになる。これも論理の飛躍はあるが、過去の例に戻れば、有名な「2000年問題」は予期できたのに、事前対応できなかった。これも「社会学的問題」かもしれない。とすれば、「乱数生成」の安全性を怠るのは「社会学」なのかもしれない。

図２　社会学的安全性と数学的安全性の関係



セキュリティ・プロトコルの安全性に影響する「乱数生成」、「ノンス性」の担保であるが、これらは数学的安全性であるが、企業のコストダウンの論理から、すなわち企業を含んだ社会学の見地から仕方がない話かもしれない。

言いたいことは、自己努力を促しても「できなかったこと」は必然要素であると考えるということである。このような時代が来るかもしれないと言いたい。テレビで有名な脳神経学者さんが「人間のこのような行動は当然です」となるのであれば、自己努力を超越した話であって、情報セキュリティでの対策、「自己努力」はセキュリティ上、意味のない「言い訳」であるということになる。

問題は、世間の認識で、情報セキュリティと言ったときに社会学的安全性と数学的安全性があって、それらは明確に認識できるかもしれない。そうであっても、社会学的安全性と数学的安全性それぞれ関係があるだろうということである。

また、数学的安全性でのリスクに比べて、社会学的安全性でのリスクはヒューマンファクターによって（直感的に）大きいと考えられる。つまりボトルネックは社会学的安全性となると考えられる。また、社会学的安全性での要因が数学的安全性に影響を及ぼす可能性も考えられる（逆に、数学的安全性でカバーできない要因を社会学的安全性に移植したとも言える）。システムの実効的安全性を考えると数学的安全性と社会学的安全性とはお互いに補完関係にあるかもしれない。

◆ まとめ

ここで、冒頭にあるように、従来であれば「人」に対して情報セキュリティを守るために「努力しろ」としていたと思われる。しかし、現実にはバグ密度、パスワード更新も人間のなせる業であり、これらはセキュリティ社会学の発展によって具体的にわかってきたならば、世界はどう変わるのだろうか？

この会社でパスワードを守らない人は「何人」であるとわかっている、社会学的にこの会社はこの程度のランク（例えば「S」）である。これではセキュリティ保険のランクは「B」である。実際にパスワードを守る人はAさん、Bさん、守らない人はC〜Zさんであるとすれば、よりセキュアなシステムにC〜Zさんを押し込むということで対応する。または、C〜Zさんの何人かはコストがかかるのでリストラの対象である、など。

（安全性の計算が正確にできるようになれば、保険も成立するだろうし、コストも見積もれる可能性が出てくる。ただし人のプロファイル化も行われ、人事への影響もあるかもしれない。）

実は、「数学的安全性」よりも、「社会学的安全性」の内容のほうが、明らかにシステムにおける「リスク」が高いと直感できると思われる。「社会学的」に人間の行動が明らかでどうしようもないとすれば、「努力目標」を掲げ「P・D・C・A」を回すという話は、セキュリティの社会学が明らかとなれば、そもそも不毛な対策であって、もともと「達成できない」代物であると考えることもできる。あるとすれば、人を縛ることによる効果であろう、「システムでの改善の余地はあるにもかかわらず」である。もちろん社会学は生き物なので、一般化が難しい面はある。ただ、今後の情報セキュリティの安全性はセキュリティの社会学が明らかになるにつれて、そのような議論が発展するのではないか。

従来の数学的安全性と結びついてより定量的な安全性議論に発展する可能性があると思われる。このような議論によって、低コストのセキュリティ、人の縛りを不要とするセキュリティが育って欲しいと願う。

[1] セキュリティ・プロトコルの論理的検証法
長谷部浩二(筑波大学大学院システム情報工学研究科)、バナゲルゲイ(リスボン工科大学数学科)、
岡田光弘(慶應義塾大学文学部哲学科)2009
http://www.math.upenn.edu/~bana/kyouritsu-security-survey.pdf

[2] 「IPA　情報セキュリティと行動科学研究会　作業部会」活動報告
小松文子氏ら、IPA情報セキュリティと行動科学ワークショップ、2010年10月15日
http://www.ipa.go.jp/security/event/2010/isec-workshop/index.html

[3] IPA招待講演「Frauds, Framing, and Behavioral Biases in Information Security」
カーネギーメロン大学　ニコラス・クリスティン教授、IPA情報セキュリティと行動科学ワークショップ、2010年10月15日
http://www.ipa.go.jp/security/event/2010/isec-workshop/index.html

[4] 連載：最新セキュリティ調査報告、第3回 情報セキュリティ対策への行動科学からの探求
著者：小松 文子、2009年、Software Developer' s Think IT
http://thinkit.co.jp/article/1073/1

[5] 「情報セキュリティの社会技術」研究シーズに関する調査
財団法人　未来工学研究所(IFTECH)、2002
http://www.iftech.or.jp/projects/2002/h14_21.pdf