「通信のための理論」を使って「セキュリティの本質」をあぶり出す

セコム株式会社 IS 研究所
甘利　康文

1．はじめに

太平洋戦争が戦雲急を告げていた1941年、電信が発明されて100年以上、電話についても60年以上の歳月が流れ、既にこれらの通信手段は世の中において広く使われるようになっていた。ちょうどその年、世界最大の電信電話会社の研究所に就職した一人の青年がいた。名をクロード・シャノンという。新しい職場から彼に与えられた研究テーマは、なんと「通信の正体を明らかにすること」。「通信において伝えられているものとは何なのか」、「ノイズなどで通信に支障をきたすときに伝達されなくなるものとは一体何なのか」、これらの疑問への答を見出すことだった。その当時、「通信」サービスの当事者である電信電話会社は、驚くべきことに自社が提供しているそのものの正体を知らずに、それを世の中に提供していたのだ [1], [2]。そのため、何か問題が起こった場合も、対応は都度、対症療法的なものにならざるを得ない状況 [3] であり、通信の本質を明らかにすることは、「通信」をサービスとして提供している当事者としては、解決しなければならない重要な課題だったのだ。

それからしばらく経った1948年、彼は、研究論文「通信の数学的理論」[4]を発表。それまで曖昧だった、通信によって伝えられる「そのもの」である「情報」の概念を明確化、その大きさである情報量を定式化したうえで、その考え方をベースに通信を扱う理論を提唱した。彼、シャノンが考案した理論はやがて「情報理論」と呼ばれるようになり、現在では、世の中で使われているすべての情報技術の礎となっている。コンピュータやネットワーク、暗号化などの情報セキュリティの技術も、全てが彼の理論のうえに成り立っていると言っても決して言い過ぎでは無いだろう。

さて、ここで人々が広く「セキュリティ」と呼んでいるそのものを考えてみよう。情報セキュリティに限らない、防犯、食やエネルギーの安定供給、国家の安全保障などの意味を含む「広い意味でのセキュリティ」[5]である。現在、「セキュリティ」に関しては、シャノンの理論が発表される前の通信と同様の状況にある。すなわち、「セキュリティが確保されているとき、行われていることの本質は一体何なのか」、「事故でセキュリティが崩れるときに、維持されないものは何なのか」などの問いかけに対する答は、まだ誰も見出していない。

往時の通信と同じで、このことは「セキュリティ対策が対症療法的になること」への、直接的、間接的な要因になっている。世の中でよく見られる「セキュリティ対策が“場当たり的”、“泥縄”になること」は、起こるべくして起こっているのだ。今般、この状況の打開を目指し、シャノンの考え方をベースにして、メタな観点から「セキュリティの何たるか」を読み解くべく試みた[6]。本稿[1]では、出来るだけ解りやすく、その概要を紹介する。

2．分野を限らない形のセキュリティの定義

セキュリティを、場当たり的な対応から解き放ち、エンジニアリングの観点から体系的に考えられるようにするためには、世の中でセキュリティという言葉が使われているあらゆるケースを言い当てる形で「セキュリティとは何か」について定義する必要がある。

食糧やエネルギー供給に支障が生じると、一国の政府は国を円滑に運営することが難しくなる。それゆえ食やエネルギーの安定供給は、「国家のセキュリティ（安全保障）の問題」となる。情報セキュリティにおいては、情報の「機密性」、「完全性」、「可用性」が担保されない状況では、組織はビジネスの円滑な運営が難しくなる。それゆえこれらの担保は、「その組織にとってのセキュリティの問題」となる。

これらの例から解るように、セキュリティという概念は、その分野によらず「どのような事件や事故が起こ

[1] 本稿の内容は、筆者の私見であり、必ずしも筆者の勤務先の見解と一致するものではない。

ろうとも、対象となるオペレーション（OP）が、あらかじめのプラン通り円滑に運営できていること」と一般化することができる [5]。本稿では、これを「セキュリティの定義」と位置付け、これをベースにしてその本質を考えていく。

3．オペレーションの前、プランニングのフェーズにおけるセキュリティ対策

「OPがあらかじめのプラン通りに円滑に運営されていること」実現の第一歩は、そのプランにある。そもそものプランにOPが波瀾万丈になる要因が隠れている場合、「OPの円滑な運営」を恒常的に行うこと（すなわちセキュリティの維持）は難しくなる。

劇を例に考えよう。波瀾万丈の劇（OP）は、一寸先は闇、何が起こるか判らないため、見ている方は面白いかもしれないが、劇中の人物は心が休まる暇がない。すなわち、この場合のセキュリティレベルは低い。一方、何も事件や事故が起こらない、つまらない劇（OP）では、淡々とした日常が繰り返され、見ている方は退屈かも知れないが、この「つまらない劇」の劇中人物は安心して日々を送れる。すなわち、この場合のセキュリティレベルは高いということになる。それでは、どうしたら劇から波瀾万丈の要素を取り除き、つまらなくできるか。そのためには、まずは何と言っても「シナリオをつまらなくすること」である。

ここで、シャノンが見出した情報という観点から考えてみよう。「波瀾万丈のシナリオ（OPプラン）」は、様々な出来事が起こることから「シナリオ全体を平均的に見た場合の情報量」は多い。一方、「つまらないシナリオ」は、何も変わったことが起こらないため「平均的な情報量」は少ない。このことは「多くの楽器が様々な形で登場する大編成オーケストラの交響曲」の複雑で分厚い楽譜と、「子どもがピアノを始めたばかりのバイエル練習曲」の単純でわずかな分量しかない楽譜を想像すると直観的に理解できるだろう。もちろん、「平均的な情報量」は、前者は大きく、後者に関しては小さい。

「OPプランというシナリオをつまらなくすること」、すなわち「OPプランの“平均的に見た情報量”を小さくすること」は、OPを行う前、プランニングの段階で、変わったこと（波瀾万丈につながる事件や事故）を「出来るだけ起こらないようにする」（Risk Mitigation: 事故の生起確率の低減に相当）、「もし起きたとしても大事件に至らないようにする」（Crisis Management: 事故発生時のOP致死率の低減に相当）こと [7]である。

「OPのプランから波瀾万丈の要因を取り除くこと」、「OPを劇とみなした場合、淡々と進む、見ていてつまらない劇にすること」、「その劇（OP）のシナリオ（OPプラン）の“平均的にみた情報量”を小さくすること」、これらはすべて同じことである。これらをビジネスのプランニングフェーズにおいて行うこと、これがビジネス分野においてBCP: Business Continuity Planningと呼ばれているセキュリティ対策の本質である。

4．シャノンの通信モデル

さてここで、情報を伝える手段である「通信」について、シャノンがどう考えたかを簡単に紹介しよう。彼が通信の本質を明らかにする際にベースとした「通信のモデル」[4]を図1に示す。情報に関する一大理論体系の大本にもなっているのがこのモデルである。

このモデルでは、まず「①送信情報（メッセージX）」が「②送信器」に送られる。送信器ではそれを「③信号」の形に変換した後、「④通信路」に送り出す。その通信路では「⑤ノイズ源」からある確率で発生した「⑥ノイズ」が混入することがあり、そのノイズが混入したかもしれない信号が「⑦受信信号」として「⑧受信器」でキャッチされる。受信器では、その信号を情報の形に戻して、それを「⑨受信情報（メッセージY）」とする。

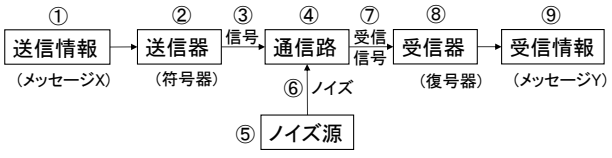

図1　シャノンの通信モデル

「ある地点で選ばれた“送信情報（メッセージX）”を、“受信情報（メッセージY）”の形で，別の地点で正確にまたは近似的に復元すること」、このモデルを元にした、シャノンによる通信の定義 [4]である。もし、「④通信路」に「⑤ノイズ源」からの「⑥ノイズ」が全く混入しなかったとしたら、「⑧受信器」で復元した「⑨受信情報（メッセージY）」は、「①送信情報（メッセージX）」と同じになるはずである。しかしながら、実際には、通信路では大なり小なりノイズが混入し、メッセージYはメッセージXと正確に同じにはならない。この場合、「送信側のメッセージXの情報量から、ノイズによって失われた情報量を差し引いた情報量」が、「通信で伝達できた情報量」である。

5．オペレーションの最中、実施のフェーズにおけるセキュリティ対策

さてここで話を元に戻し、今回の「セキュリティの定義」に則ったOPのモデル [6]を考えよう。今回の定義では「あらかじめのOPプラン通りの円滑なOPが行われていること」が、セキュリティが維持出来ていることだったので、OPの実施状況を評価するために、それを記録することを考える。この場合、OPのモデルは図2に示した通りになる。

このモデルでは、まず「①OPプラン（メッセージX’）」がOPの「②実施者」に渡される。実施者は、それに則る形で「③OPプランを具現化するための行為」を「④実世界」に対して起こし、そのOPを実施しようとする。その際、OP阻害の潜在要因である「⑤リスク」から「⑥インシデント（事故）」が発生し、実世界で行われようとしているOP実施行為に影響を与えることがある。その結果、実現されるのが「⑦実際に行われるOP」である．これを「⑧観察者」が観測し「⑨OP実施記録（メッセージY’）」として記述するというのがこのモデルである[2]。なお、実施者はOPプランに完全に忠実な形で実世界に働きかけ、観察者は実際に行われているOPを一切の加除無く記述するものとし、エラーは、全てOPに関係するリスクとインシデントの要素に帰することを仮定している。

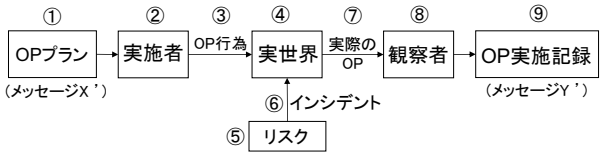

図2　セキュリティを考える場合のOPのモデル

図1の「シャノンの通信モデル」と図2の「セキュリティを考える場合のOPモデル」を見比べて欲しい。①～⑨のそれぞれの要素が一対一で対応しており、両者の構造には「同一性」があることが理解できるだろう。この通信モデルとOPモデルの同一性から、一般化したセキュリティの概念、すなわち「あらかじめのOPプラン通りの円滑なOPが行われていること」は、次のように理解することが可能となる。

通信では、受信情報（メッセージY）が、送信情報（メッセージX）に類似していればしているほど、ノイズが少ない「良い通信」が行われているということであった。これと同様に、「実世界において行われるOPの実施記録（メッセージY’）」が、「OPプラン（メッセージX’）」に類似していればしているほど、事故が少ない、すなわちセキュリティが高く維持された「良いOP」が行われていることになる。

ここで、通信モデルとOPモデルの同一性を使って、先のシャノンの「通信の定義」を読み替えてみよう。この読み替えにより、セキュリティを維持する対象としての「OPの何たるか」を知ることができる。セキュリティを考える際のOPとは「あらかじめのプランに記述された所作を，実世界において正確にまたは近似的に出現させること」に他ならない。

もし、「④実世界」において、「⑤リスク」が具現化して姿を現す「⑥インシデント」が全く起こらなかったとしたら、「⑧OP観察者」が記録した「⑨OP実施記録（メッセージY’）」は、「①OPプラン（メッセージ

[2]「“①楽譜”が “②演奏者”に渡され、“⑦奏でられた音”を “⑧採譜者”が耳で聞いて再び “⑨楽譜”に落とす」例を考えると解りやすいだろう。

X’）」と同じになるはずである。しかしながら、実際には、実世界では大なり小なり何らかのインシデントが発生し、メッセージY’はメッセージX’と正確に同じにはならない。この場合、「OPプランの情報量からインシデントで失われた情報量を差し引いた情報量」が、「実際のOPで実現できた“OP実施度合い”」となる。

この「OP実施段階において事故（インシデント）が起こった場合の影響度を下げ、実際のOPで実現できた“OP実施度合い”を大きくすること」が、ビジネス分野においてBCM: Business Continuity Managementと呼ばれているセキュリティ対策の本質である。

BCPとBCMは、しばしば同じ取組の前半と後半のような形で捉えられ、必ずしも明確に区別されてはいない。しかしながら、両者は適用される先、そしてそのフェーズが異なっている。BCPは「OPの計画段階で、プランを検討し、そこに内在する波瀾万丈の要因を小さくすること」、一方BCMは「OPの実施段階で、OPそのものをマネジメントすることで、“OPプラン”と“OPの実際”間に存在する差異を小さくすること」である。

再び劇の例で考えよう。劇では、シナリオ（OPプラン）から波瀾万丈の要素をできるだけ取り除いた（BCP）としても、その上演（OP中）において何らかの事故が起こる可能性はゼロには出来ない。それゆえ、上演中の状況にも注意し、様々な対応を行うことで、劇の「シナリオと実際との差異を出来るだけ小さく」なるようにしよう（BCM）ということである。

6．おわりに

通信を考える道具である情報理論では、本稿で取り上げた「送信側の平均的な情報量」、「ノイズ」、「通信で伝達できる情報量」は厳密に数式（数理モデル）化されている。「通信モデル」（図1）と「セキュリティを考える際のOPのモデル」（図2）の同一性から、セキュリティにおいてこれらに対応する「OPプランの平均的な情報量（波瀾万丈の要因がどれほど内在しているか）」、「インシデント」、「OP実施度合い」も、情報を扱う場合と同様の数式（数理モデル）で表すことが出来る。また、今回示した「通信とOPとの構造的な同一性」は、これら3つの場合に限定されずに常に成り立つことから、情報理論の数式（数理モデル）は、セキュリティを考える際の数学的な道具としても活用することが可能となるといえる。

このことは、セキュリティを体系的に、工学的に扱ううえで，大きな便益をもたらすはずである。これまで情報を扱うために情報理論の分野で案出されてきた様々な技法を、BCP/BCM、ISMSなどにおいて、セキュリティを考えるための道具として、そのまま活用することが出来るようになるからである。

一般化すれば、セキュリティとは「OP中に現れる（可能性のある）波瀾万丈（インシデント、事故）の影響を、ある許容レベルを超えないように低減し、それを保つこと」である。これは「OPの秩序を作り出し（BCP），それを維持すること（BCM）」と同義である。すなわち、セキュリティとは，ある「プラン」（すなわち前もってのルール）の下で、OPがどれほど秩序立っているかで評価されるべきものとなる。それゆえ、あらゆる分野において、セキュリティのための対策は、「OP実施前の施策（BCP）、そしてOP実施中の対応（BCM）によって、OPをどれだけ秩序立たせたか」で定量的に評価される対象となる。（そして、これらの評価に関する詳細は情報理論において既に示されている）

シャノンを祖とする情報理論では、情報の尺度を「メッセージを選ぶ際の自由度」[4], [8]としており、情報の「意味」は扱っていない。このことから情報理論は「情報の意味」によらずに成り立つ理論となっている。（そのため、「男の子が生まれた」、「コイン投げで表が出た」という2つの情報の大きさは同じとして扱われる）

通信モデルとOPモデルの同一性から、これと同様のことがセキュリティについても言える。きわめて抽象化した視点からは、セキュリティの大きさとは、「対象OPの状態が取りうる自由度」だけで決まる尺度であり、それにはOPの種類は関係ない。それゆえ、今回紹介した考え方は適用先を選ばない。JNSAのメインスコープである情報セキュリティに留まらず、防犯、組織における不正、食やエネルギーの安定供給、国家

の安全保障など、およそ「セキュリティ」という言葉が現れるすべての場面に適用できるということである。

究極まで抽象化すると、「セキュリティの大きさ」は「OPが取りうる状態に関する“場合の数”のみによって決まる値」であり、セキュリティ対策とは、「OPが取りうる状態の場合の数を少なくすること」、すなわち「OPの自由度を小さくすること」に相当する。それゆえ、OPに内在する自由度の減少分が、対象となるOPに施されたセキュリティ対策を定量化した尺度になるわけである。

パスワードの設定や、施錠、新たなルールの策定や監査の徹底など、セキュリティの対策は、その種類や分野によらず、それをすると「自由が制限されて利便性が失われる」という声を聞くことがある。これは、「OPに内在する自由度を減少させる」というセキュリティ対策の本質に関係して宿命的に起こっていることである。「OPに内在する自由度を減らす」ことで、必然的に「インシデント（事故）が起こる自由度」も減少するがゆえに、その対策はセキュリティのための対策となる。

本稿の主旨は、シャノンによる「通信の理論」の視座から見た「セキュリティの本質」に関する理解 [6]を概説することであった。文脈依存性を排した「一般化したセキュリティ」を、「OPを阻害する波瀾万丈があろうとも、あらかじめのプランに則った円滑なOPがなされていること」とし、それを「通信とOPの同一性」の観点から見ることで、セキュリティはあいまい性を排して理解出来る対象となる。また、そこに「通信の理論」として考案された情報理論を適用することで、セキュリティは体系的に扱うことが出来るようになり、エンジニアリングの対象にもなり得る。

本稿が、様々な分野の色々な場合において、セキュリティを科学的に分析、考察し、実現するためのきっかけとなれば幸いである。

本稿は、世の中において様々な形でセキュリティに関わっているできるだけ多くの方に「セキュリティの本質」を直観的に理解して頂くことを意識し、内容については例示を多用した簡単な記述に留めている。本稿の詳細に関しては文献 [6] を参照頂きたい。

【参考文献】

[1] ハワード・ラインゴールド（日暮雅通訳）：新・思考のための道具　知性を拡張するためのテクノロジー その歴史と未来，第6章「情報の中にあるもの」，パーソナルメディア (2006)
"Tools for Thought" by Howard Rheingold　http://www.rheingold.com/texts/tft/06.html#Chap06

[2] 高岡詠子：シャノンの情報理論入門　価値ある情報を高速に、正確に送る，講談社 (2012)

[3] ジミー・ソニ，ロブ・グッドマン（小坂恵理 訳）：クロード・シャノン　情報時代を発明した男，筑摩書房 (2019)

[4] Shannon, E. C.: A Mathematical Theory of Communication, Bell Labs Technical Journal, Vol.27, No.3, pp.379-423, No.4, pp.623-656 (1948)　http://people.math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf

[5] 甘利康文：セキュリティの本質　医療／医学，そして技術は何のためにあるのか，日本情報経営学会誌 Vol.38, No.3, pp.40-52 (2018)　https://doi.org/10.20627/jsim.38.3_40

[6] AMARI, Yasufumi: Comprehending Security through Shannon's Communication Model, International Journal of Affective Engineering, Vol.19, No.3, pp.177-187 (2020)　https://doi.org/10.5057/ijae.IJAE-D-19-00021

[7] 甘利康文：「リスクの本質」を考える体系構築のために，リスク工学研究，Vol.16, pp.9-14 (2020)
https://www.risk.tsukuba.ac.jp/pdf/bulletin16.pdf#page=13

[8] Weaver, W.: Recent Contributions to the Mathematical Theory of Communication,
http://waste.informatik.hu-berlin.de/Lehre/ss11/SE_Kybernetik/reader/weaver.pdf (1949)
文献[4], [8]は、書籍 “The Mathematical Theory of Communication,” University of Illinois Press (1998)として出版されている。そのWeb版は以下にて公開されており、邦訳版も上梓されている。
https://pure.mpg.de/rest/items/item_2383164/component/file_2383163/content
（邦訳）クロード・E. シャノン，ワレン・ウィーバー（植松友彦訳）：通信の数学的理論，筑摩書房 (2009)