■特別寄稿論文

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

The Essence of Security: The Goal that Medicine and Technology Should Pursue

セコム株式会社　甘利　康文*
Intelligent Systems Laboratory, SECOM CO., LTD.　Yasufumi AMARI

Abstract : *The term "security" covers a wider concept than simply crime prevention or countermeasures against information leakage. Although security is one of the most important considerations for modern society, security has not uniquely defined and is used in a variety of contexts which can often lead to misunderstandings. To address this problem, we propose a context insensitive concept of security and a new systematic approach for embodying the security which is applicable in any case. Generalized security can be viewed as maintaining smooth operations even in the face of disturbances. Using this context insensitive notion of security and by taking hints from some philosophical methodology, we can ponder the essential meaning of security, or the common goal that medicine and state-of-the-art information technologies such as AI, IoT, Cloud, Big Data, Mobile, etc. should pursue.*

Keywords : *security, definition, implementation, value, metaphysics*

1. はじめに

「セキュリティ」，それによって実現される「安全」，「安心」は，物理的な実体を持つ存在ではない．これらは形而上の存在であり，何かを見たり感じたりした時に，人々の心の内，意識の前に立ち現れる「何ものか」である．

本論では，まず実務的な観点から見た「セキュリティのなんたるか」，そしてそれを実現するための方法論について概説する．つづいて，実務家の立場を一旦離れて，これまでになされている哲学分野の論考も勘案しながら，人の心の内に立ち現れる観念である，これらの言葉によって指し示されている「そのもの」の本質について概観する．さらに，様々な技術や医療/医学が，そこにどう関係してくるかを俯瞰し，「その先」についての私見を述べる．

2. セキュリティとは何か

「セキュリティ」という言葉は，本来，一般の人やビジネスマンが思い描くことの多い犯罪対策や情報セキュリティ対策を超える幅広い概念を包含する．その概念は，現代社会を成り立たせるのに欠くべからざる要件の一つであるにもかかわらず，言葉としての「セキュリティ」は，多義的で

＊セコム株式会社　IS 研究所
本論は，あくまでも筆者の私見であり，必ずしも筆者の勤務先の見解と一致するものではない．

あって，現れる文脈によって色々な意味合いで使われることが多い．実際に，「セキュリティ」は，犯罪，情報漏洩，エネルギー問題，食糧問題，国防問題など，それが必要となる課題が存在する分野によって，異なった意味合いで使われている．ここからも「セキュリティ」が，幅広い概念を表している言葉であることが理解できるだろう．

一般化すると，セキュリティとは【「対象となる営み」（オペレーション，以降「OP」と表記）が，何事が起ころうとも，計画通りに続けられるようになった状態】のことである（甘利，2006; Amari, 2008）．世にある全てのセキュリティ対策は，「（『ある主体』，多くの場合『なんらかの組織』の）OPが，何事が起ころうとも，出来る限り計画通りに問題無く続けられるようにする」ために行われている．どのようなセキュリティ対策であったとしても，真に守るべきは，人や物，現金といった具体的なものではなく，それらを使って実現される，（ある主体の）「OP」という無形の対象である．すなわち，毎日のビジネスや生活といったOPの連続性が維持されている状態こそが「セキュリティ」であり，様々なセキュリティ対策で維持すべきは，その「OPの連続性」ということになる．このOPの連続性を乱す自然災害や新興感染症のパンデミック（急な大流行），犯罪や火災，テロ，情報漏洩などの阻害要因が，「インシデント（事故）」と呼ばれるものの本質である．

一般に危機管理（BCP/BCM）といった場合，震災や風水害などの自然災害，テロ，大停電や致死性感染症の大流行，そして国際紛争などの人間が絡む比較的大きな事件や事故などが想定され，これらのインシデントが，短い時間のうちにOPに重大なる影響を与えるケースを考えることが多い．

これは，「危機」が，「インシデントが短い時間でOPに大きな影響を及ぼす事態」を想起させる言葉であることによる．そのため，危機管理というと，「万が一のこのような事態の発生に備えて，それに対応する準備（BCP）を行い，危機発生時には遅滞なくそれを実行すること（BCM）」を考えることが多い．一方，「OPが，何事が起ころうとも，出来る限り計画通りに問題無く続けられるようになった状態」を，本質的な観点からの「セキュリティ」と捉えると，「セキュリティ対策」は，一般に危機管理（BCP/BCM）という言葉で表されている諸施策を包含する大きな概念を指し示す言葉となる．

世の中一般では，セキュリティを考える際には，人・物・金，そして情報をインシデントから守る必要があると言われる（日本セキュリティ・マネジメント学会，1998など）．これらは，OPを維持するために必要なリソースプロパティ（以降「リソース」と表記）である．リソースが守られないと，その組織のOPは，あらかじめ定めた通り回らなくなる．それゆえ「組織のOPが回り続ける状態」を実現するために，これらのリソースを守る必要が生じる．

しかし，「（人・物・金，そして情報などの）リソースをインシデントから守ること」が必要になるのは，ひとえにそれが組織のOPが回り続ける状態を維持するために欠かせないからであり，このことは本質的にはセキュリティの最優先事項ではない．セキュリティ対策をその本質から考え，実現していくためには，この基本スタンスが重要となる．

何か問題が起こった場合，その直接原因となるインシデントにばかり目が行って，問題の本質を見失ってしまうことがよく起こる．世の中を見ていると，この「インシデントへの対応」からセキュリティ対策に入っていく例がほとんどである．しかしながら，インシデント対応から考えていくと，セキュリティ対策が「場当たり的」になるため，注意が必要である．すなわち，震災，風水害などの自然災害，新型感染症，火災，犯罪被害，情報漏洩のようなインシデントへの対応のみに目を奪われてはいけないということである．

インシデントによってリソースが毀損を受け，そのリソース毀損によってOPが影響を受ける，事態はこの順序で進行するが，体系的にセキュリティ対策を考える際には，その過程を逆にたどっ

て，OP，リソース，インシデントの順番で考えることが重要である．

ここまでで，次の2点，すなわち，全てのセキュリティ対策が「どのようなインシデントが起ころうとも，組織のOPが出来る限り計画通りに問題無く続けられるようにする」ために行われること，そして，本質的観点から体系的にセキュリティ対策を考える際には，OP，リソース，インシデントの順番で考える必要があること，が理解できるであろう．

3. セキュリティを実現する手順

前章で述べた，一般化された（文脈によらない）定義によるセキュリティを実現するためには，次の各項目を，順を追って検討していく必要がある（甘利，2006; Amari, 2008）．

(1) 運営主体，及び守る対象であるOP（営み）が明確にされていること．
(2) OPのプランがあらかじめ定められていること．
(3) OPをプラン通り遂行するのに必要な要素であるリソースが，有形無形を問わず，網羅的に洗い出されていること．
(4) リソースに影響を与える阻害要因（インシデント）が網羅的に洗い出されていること．
(5) 各インシデントに対するリスクマネジメント（リスク低減とクライシスマネジメント）がなされ，その影響が最小化されていること．

先にあげたセキュリティの基本的な定義と，それを実現するための上記各項目を考えることで，世の中で「セキュリティ」という言葉が使われている全てのケースを理解することが可能となる．また，ここにあげた各要件項目を検討する一連のプロセスは，「あらゆる場合に適用可能なセキュリティを実現するための汎用フレームワーク」となる．

以下，各項目について概説する．

3.1 運営主体と対象オペレーション

セキュリティを体系的に実現するには，まず「組織の運営主体，及び対象OPを明確化」する必要がある．これらが曖昧であると，考えるべきことが拡散し，体系的にセキュリティを扱うことが出来なくなる．

家庭という組織であれば，運営主体の多くは「夫婦」，対象OPは「（つつがない）日々の生活」，企業の場合は，運営主体は社長や最高経営責任者などの「経営陣」，対象OPは「定款に定めた内容」となるだろう．一般に会社組織では，全体として見た場合には，運営主体やOPは明確である．一方，部，課などの組織内部署の場合，必ずしもそうではない例が散見される．

演劇上演の例で考えると解りやすい．演劇の場合，運営主体はプロデューサー，対象OPは劇の興行そのものである．

3.2 オペレーションプラン

体系的なセキュリティの実現で，次に必要なのが，明確化された「OPプラン」である．

可能ならば，このOPプランは，定性的な表現に留まらず，定量化された尺度で表記されていることが望ましい．プランと現実との乖離が起こった場合，誰もが判る形で一目瞭然に見えるからである．

特に企業の場合，各部署のプランは何らかの定量化された尺度で明確化するのが基本である．営業や製造などのライン部門ではこれを行っている例は多い．一方で，広報や総務などのスタッフ部門では，その業務の特質上，プランを数値尺度で明確化することが難しい．しかしながら，プランの定量表現が難しい部署においても，最低限，各人が持っている暗黙知を洗い出し，形式知として書き出した後，関係者間でそれを共有する必要がある．このプランは，定量表記が難しい場合でも，（可能な限り）何らかの方法で客観評価出来る形にすることが望ましい．

家庭の場合，「日々の生活」というOPの内容とプランが明確化されている例はまれかもしれな

い．プランという考え方が「個人の生活」には合わないという向きもあるが，（自宅の防犯や個人情報漏えい対策などに限らない）広い意味の「家庭のセキュリティ」を，生活科学（家政学）などの学の対象として体系的に考えようとする場合には，このプロセスが最初の一歩になる．

演劇の例では，プランとは，上演に必要な原作，脚本，監督，俳優，美術等の各種の要件，さらには興行そのもの，そして初日に向けた準備のスケジュールが明確に記述されたもののことである．

3.3　リソース

OP プランを明確にしたら，次は，それを遂行するために必要なもの，すなわち「リソース」を，有形無形を問わず，網羅的に洗い出す必要がある．

守るべき OP を，平穏な（個人の）「生活」として考えた場合，健康，住まい，家族，収入源などがリソースの代表的なものとなる．製造業の場合，生産設備，販売チャネル，固定客，従業員，株主，キャッシュフロー等々がリソースに当たる．企業の場合，OP を回すのに必要なリソースは業種によって異なってくる．

世の中において（特にコンピュータやネットワークなどの，いわゆるサイバーセキュリティの分野で）情報セキュリティを過度に追求するあまり，組織における円滑な OP が損なわれているケースを見ることがあるが，これは本末転倒である．情報セキュリティの 3 要件[1]，情報の機密性，完全性，可用性は，組織の OP を回すために必要な（無形の）リソースに相当する．組織にとって，これらが重要なのは言うまでも無い．しかし，あらゆる組織にとって，セキュリティを考えるうえでの最重要要件は，これら 3 つではなく，あくまでも「円滑な OP の維持」である．サイバーセキュリティ，情報セキュリティと呼ばれる分野も，あくまでも「セキュリティ」という大きな領域の一分野であることに注意が必要である．

演劇の例では，役を演ずる俳優，衣装，大道具，小道具，照明，音声等々，どれが欠けても舞台が成り立たなくなる要素の一つひとつが下位のリソース，「舞台上に作り出される環境」が，これらによって作られる上位のリソースとなる．

3.4　阻害要因（インシデント）

プラン遂行に必要なリソースを洗い出した後は，各々のリソースに対して「影響を与える要因」であるインシデントを網羅的に想定していく．

平穏な（個人の）「生活」という OP に必要な「住まい」というリソースへの影響を考えた場合，例えば，火災，風水害や震災のような物理的インシデント，インフレ等により家賃支払やローン返済が出来なくなるといった社会的インシデントが，その OP を阻害する要因として考えられる．製造業の OP に必要な「工場」というリソースに影響を与える阻害要因には，個人の生活と同様の火災などの物理的インシデント，当局から操業停止命令を受けるなどの社会的インシデントが考えられる．

演劇の例では，OP に必要なリソースである俳優が体調を壊す，劇場設備の故障等の物理的インシデント，俳優や演劇内容にまつわるスキャンダルといった社会的インシデントが，OP に影響を及ぼすインシデントに当たる．

3.5　阻害要因の影響低減（リスクマネジメント）

OP のリソースごとに，それに影響するインシデントを洗い出したら，次はそのインシデントの一つひとつに対して，リスクマネジメントの方法論で対応方法を考えていく．

リスクマネジメントに関しては色々な考え方があるが，本論では，リスクマネジメントを，「インシデントが起こる可能性（潜在的に存在する損失発生の可能性）を出来る限り取り除くこと」（リスク低減，リスクコントロール）と，「インシデント発生直後の初動対応をあらかじめ定め，すぐに実行できるようにしておく準備しておくこと（BCP）で，インシデント生起時のダメージを小さくする活動（BCM）を適確に実施できるようにすること」（クライシスマネジメント），そして「リスクがインシデントとして具現化し損失（ダ

メージ）が発生した際にOPに大きな影響を及ぼさないような金銭的手当をしておくこと」（リスクファイナンス[2)]）の3つの要素からなるものとして考える．これら3つが，インシデント対応で人が出来ることの全てである．想定されるインシデントが明確な場合，これら3つの手をすべて打つことで，人事を尽くした状態となる．

インシデントに対しては，これら3つの手段で，リソースの重要度・代替性，インシデントの発生頻度（確率）と，それがリソースに与える影響度の大小を勘案し，優先順位を考えながら対応していく．実務のうえでセキュリティ対策を考える際には，それに必要なコストも考慮し，その時々に合わせて，最適なコストで最適なソリューションを適用することで対象となるOPを守っていく必要がある．

演劇上演というOPで，「俳優」というリソースに影響を与える「病気」というインシデントを考えた場合，健康管理の徹底がリスク低減，代役の用意がクライシスマネジメント，代役起用によるコスト増等を事前想定し，金銭的に対応準備しておくことがリスクファイナンスとなる．リソースとして「劇場の設備」を考えた場合は，「保守管理の徹底」によってリスクを低減し，「代替機器の用意」で万が一の事態（クライシス）に備えることとなる．加えて不意の修理に備えた損保付保などのリスクファイナンスも行っておく．

・・・・・・・・・・・・・・・

本章ではここまで，セキュリティの基本的考え方として，一般化したセキュリティ定義と，それを実現するためのフレームワーク，セキュリティ対策としてのリスクマネジメントの基本的な方向性について考えてきた．実務家の立場で，企業などの具体的な組織におけるセキュリティを検討する場合には，これらの考え方，方法論は大きな力となるだろう．

4.「セキュリティ“学”」の課題

本章では，ここまで概説した考え方の中に，依然として残る「学」としての課題について考える．

時刻 t_0 に発生したインシデントにより，あるOPの操業度が落ち，復旧の努力によって時刻 t_r に復旧したとする．そのイメージを図1に示す．

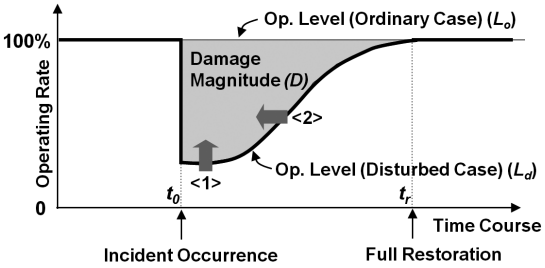

図1　インシデント発生時におけるクライシスマネジメントの2つの方向性とダメージの大きさ

セキュリティ対策には「インシデントの生起確率を下げる」（リスクコントロール，リスク低減）だけでなく，それにもかかわらずインシデントが発生した場合の対応として，「OP操業度低下をなるべく抑えること」（図1中の<1>），及び「OP操業度低下期間を出来るだけ短縮すること」（<2>）の2つが求められる．これら2つの総称がクライシスマネジメントである．

世に言うBCP/BCMとは，インシデント生起に対抗するために，これら2つの備えを行い（BCP），いざという時に遅滞なく実施できること（BCM）である．この際，図1に示したグラフの落ち込みの部分の面積の大きさDは「インシデントが発生した場合のOPへの影響度（ダメージの大きさ）」と説明されている．

図1のグラフで示される考え方（内閣府，2013など）は，世の中において，セキュリティ対策としてのクライシスマネジメント（BCP/BCM）を考える際のベースとなっており，実際，具体的対策の多くが，この考え方に準拠して行われている．

しかしながら，図1はいわゆる科学的な意味を持つグラフではなく，「既に発生してしまったインシデントによるダメージ」を基にして，クライシスマネジメントの2つの方向性（図1<1>，<2>）を理解するための概念図である．そのため，この図に示される考え方では，「まだ発生していない

インシデントによるダメージの大きさ」の評価は難しい．

たとえば，全く同じセキュリティ対策（BCP）があらかじめ講じてあり，周囲へ及ぼす影響の大きさが等しいインシデントが発生したとしても，インシデント発生時のOPへの影響（ダメージ）は偶然性に左右され，一意には定まらない．

また，世の中一般では，何らかの事故（インシデント）が発生した際のダメージは，金額ベースで評価され，損失額として表されることが多い．すなわち，ダメージという対象は，売買当事者間の合意で決まるモノやコトの値段[3]と同じように，何らかの価値観のもと，関係者間の合意をベースとして主観的に評価される対象[4]ということである．

これらの理由により，リスクの影響度の大きさ，すなわち，インシデント生起の際のダメージの大きさを，実務において評価する際には，図1に示す方法論は使われず，多くの場合，評価者の経験や直感によってなされている．

すなわち，インシデント生起に関する科学的な評価は，確率論に基づく方法論で相当程度可能である一方で，未だ発生していないインシデントによるダメージに関しては，必ずしも科学的，体系的に扱われているわけではないということである．

リスクは，「インシデントが生起する頻度」と「インシデント生起の際のダメージ（影響度）」の2つの尺度で評価[5]される．後者が，評価をする人間の経験や直感によって評価されているということは，リスクについても，体系的，科学的観点から評価されているわけではないということを意味している．

リスクを定量化し，数理モデル（数式）にのせて理解する多くのアプローチ（A. J. McNeil, et al., 2005など）では，リスクが影響を与える客体の「価値」，そしてその価値の毀損（ダメージ）を，所与のものとして変数として扱っており，「価値のそもそもの何たるか」には触れていない．

これが，セキュリティ，及びその実現手法であるリスクマネジメントを，特に「学の対象」として考える場合において，依然として残る大きな課題である．

5. セキュリティの本質 組織とは，オペレーションとは

「セキュリティ」というコトバ[6]によって指し示される「そのもの」は，概念であり実体を持たない．そのため，「セキュリティの何たるか」についての認識は，その人間の背景に依存し，また，それが現れる文脈などにも左右されて人それぞれバラバラとなる．これが，本論序盤で触れたように，「セキュリティ」というコトバが，それが現れる文脈によって様々な意味合いで使われる理由の一つとなっている．

これに対して，セキュリティを「対象となる組織の日々の営み（OP）が，運営主体によってあらかじめ定められたプランに則って運営され，理由の如何によらず，それが阻害されないこと」と捉えることで，先述した（「学」としての）課題は残るものの，実務的には大きな問題が生じない形で，体系的にセキュリティを扱うことが出来るようになるというのが，ここまでの本論における主張であった．

一方，前述したセキュリティの定義では，「組織」そして「OP」というコトバが，何を指し示すのか明確にされることなく現れる．セキュリティについての理解を深めるためには，その定義に現れる「組織」，「OP」，加えて，組織のOPが阻害されることで生じる「価値の毀損（ダメージ）」の何たるか，さらにはその大本である「価値」そのものについての考察が欠かせない．

本章では，先人によってなされた哲学的論考の理路[7]も勘案しつつ，「価値のそもそも何たるか」について考察し，それを基点に「組織」，そして「OP」の本質を考えていく（甘利，2015，2016）．

5.1　人が本能的に持つ欲求

人は，一個体として自らの命を維持したり，自らの遺伝子を次世代に引き継いだりする行為への

生物的な欲求を持っている．さらに，自身の同族，仲間に始まり，ひいてはヒトという種にまで拡がる「自分が関心をもつ人々」の命や遺伝子の維持への関心も併せもつ．この「自分が関心をもつ他者に関する欲求」（ヒューマニティに関する欲求）までをも併せもつのが，「ヒト」が「人」たる所以である．このヒューマニティに関する欲求は，時として他の欲求に勝る形で，私たちの意識に立ち現れてくる．

人は，これらの欲求へのインセンティブ体系として，欲求が満たされたときに「心地良さ」，「快」を，満たされないときに「心地悪さ」，「不快」を感じるような本能的特質（報酬系）を持っている．これが，「『【生】[8]に近づくこと』から『快』を感じ，『【生】から遠ざかること』からは『不快』を感じる」という人の意識が本能的に持つ根源的な特質につながっている．

あらゆる個人は，内なる意識に支配され，【生】を求めることで「心地良さ（快）」を得るように，また，【生】から遠ざかることで感じる「心地悪さ（不快）」を避けるように行動する．どのような人間であっても，人の意識が持つこの特性に例外はない[9]．人が生きていくために，またヒトという種の維持のために欠かせないこの本能的な欲求は，「矢も楯もたまらず『○○をしたい』という強烈な思い」として，私たちの意識に立ち現れてくる．

あらゆる人の意識は，（無意識のうちに）「快」を求め，「不快」を避けるように振る舞っている．金銭欲[10]，所有欲を始めとして，好奇心や向上心，自由欲，支配欲，名誉欲なども，直接，間接に「快」を求め「不快」を避ける（すなわち【生】を求める）という意識の特性が姿を変えたものである．

私たちの意識が欲求をもつ，すなわち「快を求め不快を避ける特質をもつ」ということは「人間は，一人ひとりが，一個人として【生】に少しでも近づきたい存在である」ということに他ならない．人は，どのような情況にあっても（意識に立ち現れる）「心地良さ（快）」に支配され，その「損得感情で動く」ということである．誤解を恐れずこれを表現すれば，結局のところ「人間は『自分』がかわいい」のである．

5.2　組織，そしてオペレーションの本質

万人の意識が持つ「快という感覚を求め，逆に不快を避ける」（【生】を求める）という本能的な共通特質は，先にあげた「価値のそもそもの何たるか」に関係し，世の中の人間事象，社会事象の多くに影響を与えている．

複数の（自分がかわいい）「個人」によって構成された存在である「組織」は，基本的には関係する各個人が感じる「快」（心地良さ）の総和を最大化，「不快」（心地悪さ）の総和を最小化するように行動する．ベンサムが「最大多数の最大幸福」と表現した「功利主義」的な行動様式を示すということである．

「組織」というコトバで指し示されている「そのもの」には，物理的な実体はない[11]．組織とは，あくまでも，「ある目的」を達成するために，複数の「個人」（ステークホルダー）が，様々な形でそれぞれの力を合わせるために集合した概念上の存在である．

例えば，その組織が「ある自動車メーカーA社」である場合を考えよう．この場合，「ある目的」とは「『良い車を提供すること』で，組織に関係する各ステークホルダーが得る『快』，『不快』の総和を，それぞれ最大化，最小化すること」である．

すなわち，(1) 顧客には，良い車の提供により，「対価支払い（お金の減少）による『不快』に勝る『快』（満足）を感じてもらうこと」，(2) 働く人間には「労務提供やストレスなどによる『不快』に勝る賃金を支給し，同時にやりがいなどの従業員満足（労働者にとっての『快』）を感じてもらうこと」，そして，(3) 組織の活動資金を出している株主には「そのリスク（不快）に勝る配当とキャピタルゲイン（お金の増加）を提供し，投資家としての『快』を感じてもらうこと」，これらの関係する各個人，ステークホルダーの「目的」を達成するために，概念として存在するのが，「あ

る自動車メーカーA社」という「組織」である．

考える対象の組織が，例えば自動車メーカーA社からホテルB社に変わっても，目的を実現するための手段が，「良い車の提供」から「快適な宿泊環境の提供」のように変わるだけで，「組織に関係する各ステークホルダーが得る『快』/『不快』の総和を最大化/最小化すること」という，組織の目的自体は変化しない．

これを敷衍することで，あらゆる組織は，「組織に関係する各ステークホルダー（個人）が得る『快』，『不快』の総和を，それぞれ最大化，最小化する」というOPを実現するために（概念として）存在しているという理解が可能となる．組織がそのOPによって生み出す「価値」（利）の本質は，その組織に関係する各個人が感じる「快（心地良さ）の最大化・不快（心地悪さ）の最小化」にある．価値は，私たちの内にあるもので，外の世界にある何ものかではない．セキュリティを，その本質に遡って考える場合には，「価値」が，無形の（形而上の）存在であり，「人の意識に立ち現れる『現象』[12]」である点に注意しなければならない．

5.3　セキュリティの本質

組織は，前節で述べた「価値」を生み出すための営み（OP）を行う際に，それを妨げる犯罪被害や情報漏洩などの阻害要因（インシデント）に遭遇することがある．それゆえ組織には，インシデントがOPを妨げることを想定して，その影響を最小化するための施策（セキュリティ対策）を講じる必要性が生じる．「セキュリティ」とは，これらの概念を包括して指し示すコトバである（甘利，2015，2016）．すなわち，組織が行う「関係する個人が感じる快（心地良さ）の最大化・不快（心地悪さ）の最小化」行為（OP）を，邪魔されることなく円滑にできるようにすること，これこそが「セキュリティ」というコトバで表されている概念（コト）の本質ということである．

6. 技術とセキュリティ

ここまで述べたように，組織は，その種類によらず，「関係するステークホルダーの一人ひとりの意識が感じる快を最大化・不快を最小化する（価値創造の）営み」（以後「ハピネス追求の営み」と表記）であるOPを行うために存在する．「様々なインシデントに遭遇しようとも，この『営み』が乱されない」ということが「セキュリティの本質」である．

「世の中で行われているOP，すなわち『ハピネス追求の営み』を，より良く，より効率的に行うためにあみ出されたノウハウ（知）」を，私たちは何と呼んでいるか．これが，世において「技術」と呼ばれている方法論（コト）の本質である．

太古の昔，人は，親族やごく親しい人間で集団を作り，木の実や山菜，小動物や魚などを狩って暮らしていた．人々は，必死になって日々の糧を探し，野山を歩き回っていたことだろう．食糧が得られるかどうかは，今日の命を存えられるかどうかを決める重要なことであったに違いない．

この情況を根本から変え，人々を日々の糧への心配から解放した画期的な知が，現在「農」と呼ばれている技術である．この知が広まることで，人類は飢えの恐怖に苛まれることがなくなった．これが，当時の人々のハピネスを大いに高めたことに異を唱える向きはいないだろう．その意味で．農はまさに世の中に革新をもたらし，人々の生活を根本から変える「技術」であった．

これは農に限らない．着火法，調理，車輪，冶金，製糸紡績，織布，製紙，印刷，電池，原動機，熱ポンプ，発送電，電灯，電信電話，防疫，予防接種，抗生物質，樹脂，情報ネットワーク等々，少し考えただけでも人類の発展に大きく影響を与えた知，「大粒の技術」は枚挙に暇がない．これらは全て「人々のハピネスを大きく高め，今なおそれをし続けている」という共通点（共通の構造）を持っている．

さて，今現在，人々のハピネスを大きく高揚させ，世の中に真の革新をもたらす知，往時の農に

匹敵するインパクトを与える「大粒の技術」はどれくらい生まれているのだろうか.

最近，マスコミなどで人々の目に触れることが多くなっているAI，IoT，Cloud，Big Data，Mobileなどのコトバで括られる「情報に関係する新しい手法」（以降「新興IT」と表記）は，シャノンによる「情報の理論」，ノイマンらによる「計算機の概念」，マルコーニによる「無線通信」などの「大粒の技術」の延長線上にある．しかしながら，新興ITを指し示すコトバは，まだ「世の中に大きな変化をもたらす可能性」という文脈で登場することが多い．新興ITが，農に匹敵する規模で「人々のハピネス追求」に貢献しているかというと，未だそこまでは至っていない．すなわち，真の意味での「大粒の技術」にまではなっていないということである．

新興ITが一時的なバズワードを超え，本当の意味での「大粒の技術」になるためには，世の中で行われているOP，人々の「ハピネス追求の営み」に，目に見える形で大きく寄与する必要がある．その概念，手法が，それが生み出される前と比して「人々が感じるハピネス」をどれだけ向上させたのかが問われているということである．

この観点から見ると，新興ITは，現時点においては，研究段階を超えて実用化されている分野はあるものの，総じては萌芽の段階にあり，期待が先んじている状態にあるといえよう．

7. セキュリティと医療，医学

世の中では多種多様なOPが回っており，それらの連続性が維持されている状態が，「セキュリティが保たれた状態」であるのは前述した通りである．

世の中と同様，一個人の体においても，種々様々なOPが回っている．「健康」とは，それらのOPの連続性が維持されている状態のことである．ここから，健康とは「体のセキュリティが保たれた状態」のことであり，病気・ケガは，健康，すなわち「体のOPの連続性」に影響を与えるインシデントだと考えることができる．「ヘルスケア」の意を含む「医療」とは，体のOPに影響するインシデント（病気，ケガ）へのセキュリティ対策の総称である．人体におけるOPやインシデントの何たるかを明らかにし（生理学や病理学などの基礎医学），それらインシデントへのセキュリティ対策（内科や外科などの臨床医学）を進化させる営みは，総称して「医学研究」と呼ばれる．「医学」とは，これら一連の取組によって構成された体系的な知，「医療」はその知を，実地において実施，展開（Implement）することである．

このような視座に立つと，健康，ヘルスケア，医療，医学などの一連のキーワードで表される対象が，セキュリティの考え方と深い関係を持つことが理解できるだろう．

また，健康がセキュリティに関連するのは，「一個人の体におけるOP連続性の維持」というミクロ視点に留まらない．「健康」は，家庭における「つつがない生活」，企業における「生産活動」など，組織やOPの種類を問わず，そのOPの維持に欠かせない（無形の）リソースの一つである．世の中で回るOPの連続性維持，すなわち「社会のセキュリティ」に欠かせない要件に人々の「健康」があるということである．

世の中のOPに不可欠なリソースである人々の健康を守るための営み，これが一般に医療（ヘルスケアを含む）と呼ばれている対象を，社会というマクロ視点から見た場合の本質である．

ジェンナーに始まりパスツールによって体系化された予防接種，フレミングを始祖とする抗生物質の知見，手法は，人体におけるOP連続性の維持に寄与し，一人ひとりの命を救ったという観点だけでなく，世の中で回るあらゆるOPに不可欠なリソース，「人々の健康」を守ったという視点からも，セキュリティのための画期的な技術であった．

メタな視点からも，人々を感染症の不安から遠ざけたこれらの医療技術は，人類を「【生】に近づけること」に寄与し，人々に「快」の感覚をもたらした「大粒の技術」であったことは間違いない．すなわち，あらゆるOPが共通して持つ「ハ

ピネス追求」という本質を，より良く回すことに貢献した，そして今なおそれをし続けているということである．

この例からも解るように，医学研究，そしてその成果である医療の進歩は「人々の命を存える」ことに寄与，人々を「死への恐怖」から遠ざけることで，そのハピネス追求に大きく貢献している．

過去，医療/医学は，物理学が明らかにした自然現象「X 線」を要素技術として取りこむことで劇的に姿を変え，人々の命を存えるための，すなわちハピネス追求のための力強い味方として大いなる進化を遂げた．今では，X 線は医療/医学に欠くことのできない要素技術の筆頭になっており，万人がその恩恵に預かっている．この例のように，医療/医学の進歩には，それ以外の分野の科学技術の発展を土台とするところも大きい．

現在，人々は，新興 IT に，X 線が医療/医学に果たした役割と同様の役割を期待し始めている．一方，今現在，新興 IT は，X 線と同レベルで人々のハピネスを向上させているとはまだいえず，期待が先走りしている感は否めない．医療/医学のための要素技術という観点からも，新興 IT はまだ黎明期にあり，大いに発展の余地があるといえるだろう．

8.「命を守る」のその先

ここまで述べたように，「人々の命を守り，それを存える」ための医療/医学は，物理学などの科学の知見を要素技術として取りこみながら，さらなる進化を続けている．今や多くの人々が，その恩恵にあずかれるようになり，結果として，人は年齢を重ねてもなかなか死ななくなった．これが人々のハピネスを高めたのは間違いない．一方で，長生きが当たり前になった昨今，単に「命を存える」だけでは，必ずしも「人々が感じる快（心地良さ）を高める」という，OP の本質にかなう形でセキュリティ対策を十分に実現しているとは言いきれなくなりつつある．

社会の高齢化などで最近になって注目を浴びてきた「老年学（Gerontology）」という学術分野がある（大内ほか編，2010 など）．医学に留まらず，生物学，心理学，社会学，生活科学，工学などの視点から，「齢を重ねること」，「老いること」について横断的に考え，より良い「人生の最終章」を追求しようとするものである．また，齢を重ねること，老いることのさらにその先を見すえた「死生学（Thanatology）」という学術分野（島薗ほか編，2008；平山，1991；山本，1992 など）もある．これからの時代，医療/医学は，「人々の命を存える」ためだけでなく，「より良く齢を重ねる」ための老年学，「より良くお迎えを受け入れる」ための死生学などの知見も取り入れながら進んでいく必要がある．

時代が進み，世の中が変遷しても，「人々のハピネスを高める」ことが「世で回っている OP」の本質であることは変わらない．そのため，医療/医学には，いつの時代にも，世の中で回る OP を維持するための（すなわち世の中の「セキュリティ」のための）大いなる力となることが期待されている．これらに鑑みても，今後の医療/医学にとって，老年学や死生学と協調することが重要なこととなるのは間違いないだろう．

古の時代から人類は「死」を相手にして永い戦いを続けてきた．多くの人々の努力によって，一時的に有利に戦えるようにはなったものの，この戦いに人類が勝利することはない．

医療/医学は，人が本能的に抱える「死への恐怖」の克服を目指して進歩してきた．実際，これまで永い間，人々の病気を治し，健康を保つことは，「世の中で回る様々な OP を守ること」，すなわち「人々のハピネスを高める」ことであった．これはこれからも変わらない．しかし一方で，最後には必ず負けてしまうこの戦いにおいて，一時的な勝利を収めることだけが「人々のハピネスを高める」わけではないことが判ってきた．近年，医療/医学に加えて，老年学，死生学といった学術分野に世の中の目が集まってきているのは，人々の注意が「いかに負けるか」に向いてきているということである．

「老い」や「お迎え」などの分野の基礎研究，

実務（臨床）応用は，長い歴史のある医療/医学と比して，始まったばかりである．「齢を重ねること」，そして「その先」は，だれもが経験する避けえない宿命として頑として存在する．一方，これらのプロセスをより良く（「心地良さ」を伴う形で）進めるための科学的研究，およびその知見の応用研究は，最近にいたるまで，ほとんどなされてこなかった．

一般的な感覚から,「老い」,そして「お迎え」は，これまで，文字通り「【生】から遠ざかること」，すなわち「快ではないもの」と考えられてきた．一方，最近の死生学研究（京田ほか，2009，2010；諸岡ほか，2008 など）によって，この考え方が必ずしも 100% 現実を言い当てているわけではないことも判ってきている．

世の高齢化などの背景から,「いかに(心地よく)齢を重ね，さらにその先を迎えるか」を考え，これらのプロセスにおける「人々のハピネスを最大化する営み」，すなわち「OP とは何か」を明らかにする必要が生じ始めている．これは「OP とは何か」に限らない．その OP をつつがなく回すための新しいセキュリティのパラダイム,そして，それを助ける技術が求められ始めているということでもある．

衆目を集めている新興 IT には，世の中で回っている OP の連続性を維持するという，これまでのセキュリティのための役割に加え，今後，老年学，死生学などの知見を活かすための応用技術として,「より良く齢を重ねる」,「より良く旅立つ」を実現する力となることが期待されるようになるだろう．

IT 分野では，日本は他国の先行を許しているという声も聞く．一方で日本は，これから世界の国々が直面する高齢化という課題に直面している課題先進国である．この課題に，IT などの技術を応用しながら対応し，各国に先んじてベストプラクティスを示す．「人々のハピネス」の幅が拡がるこれからの世界において，日本はこのような形で大いに貢献し，その先進性を示すことができるだろう．私たちの前には，開拓を待つ未開の大地が広がっている．

9. おわりに

セキュリティ実務の場にいると，しばしばセキュリティ対策が，体系的ではなく，絆創膏的，泥縄的に行われる情況に遭遇する．セキュリティへの認識や理解がバラバラで，セキュリティ対策として，目の前のインシデントへの対応を行う施策が一般的に行われているからである．

本論序盤で紹介した「(組織の）OP の連続性を維持する」というセキュリティの基本的考え方，そしてそれを実現するためのフレームワークは，どのような業種で，どのようなインシデントへの対応を考えるうえにおいても有効に機能する．実務者の立場から，現実の組織の（本当の）セキュリティを実現するためには，本論で述べた基本を踏まえて諸施策を策定し，それを粛々と実行していくことが重要である．

本論中盤では，セキュリティについての（メタな視点からの）本質を探るために，現象学などの哲学分野における知見も意識しつつ，実務からは距離をおいて，セキュリティという概念を構成する要素である「組織」,「OP」，そして「価値」とその毀損について論じた．

あらゆる組織は，その種類によらず「関係するステークホルダーの一人ひとり，各個人の『ハピネス』総和を最大化する営み」である OP を行うために存在する．OP は「ハピネスという価値」を生み出すために行われる．そのハピネスとは，人間が【生】に近づくことで感じる「心地良さ」,「快」の，一人ひとりの総和である．

「どのようなインシデントが起ころうとも，この営み（OP）が乱されず，そこから生み出される価値，すなわち人々のハピネスが影響を受けない」ということが（よりメタな視点からの)「セキュリティの本質」である．

この OP を「より良く行う」，すなわち「より多くの個人（出来れば万人）に，より多くの心地良さ，ハピネスを提供する」ための力となる方法論が（医療/医学を含む)「技術」であり，その

ために存在するのが「組織」，そして，その障害を取り除きOPが円滑に回るようにしようとする努力が「セキュリティ対策」である．

本論終盤では，この考え方をベースに，「技術」のなんたるか，医療/医学，そして老いやその先を考える学である老年学や死生学について考え，さらに，これらのなかで，衆目を集めているAI，IoT，Cloud，Big Data，Mobileなどの新興ITが，どのような立ち位置にあるかについての私見を述べた．

結婚式で，これから新しい家庭を構える新郎新婦に対して「『幸せな家庭』を作ってください」とスピーチする来賓は多い．人間は，個人として自らの人生を「幸せ」（「心地良さ」の多いもの）にし，充実した人生を送るために生きている．世の中を構成している組織の最小単位である「家庭」に限らず，あらゆる組織は，一人ひとりのそこに関係する人間が，個人として自らの人生を幸せにし，充実した人生を送るために存在している．これは組織という概念に留まらない．形而上/形而下，実体の有無によらず，人が生み出す森羅万象は，その目的のために存在するといっても過言ではないだろう．

近江商人に伝わる「売り手よし，買い手よし，世間よし」の「三方よし」の商いの理念は，本論で述べた「人々が感じるハピネス（心地良さ）の最大化」という「OPの本質」と同じものである．「経営」も人が作り出した概念の一つである．すなわち経営というコトバで表される方法論は，「関係するステークホルダーの一人ひとり，各個人が感じる『ハピネス』の総和を最大化する営み」であるOPをより良く回すためのものであり，決して，見栄えの良い損益計算書や貸借対照表など（より端的に言えば「銭金」）を，近視眼的に追求するためだけに作り出されたテクニックではないはずである[13]．

経営学は，組織のOPをより良く回すための知見，すなわち「より多くの個人に，より多くのハピネスを提供する」ための手法を見出し，それを実務家に提供する重要な役割を担っている．現代社会の基幹をなす要件である「情報」をベースに，組織のOPとしての「経営」を考える学術団体，日本情報経営学会に期待されるところは大きい．

本論で紹介，考察した手法や知見，考え方が，「本当のセキュリティ」実現のための一助となり，組織のOP，そしてこれらの総体として存在する日本社会がさらに発展するための，そしてなによりも，それを構成する私たち一人ひとりの「心地よさ」，ハピネスがより高まるためのきっかけとなれば幸いである．

注

1）（1）機密性（Confidentiality）：情報が不用意に漏れないように保つこと，（2）完全性（Integrity）：情報が改竄されないように保つこと，（3）可用性（Availability）：情報を使えるように保つこと．各々の頭文字から，俗に「情報セキュリティのCIA」とも呼ばれる．

2）リスクファイナンスは，リスクがインシデントとして具現化し，損失が発生した際に，金銭面からその影響を小さくする手段であり，クライシスマネジメントの一と考えることもできる．本章以降では，リスクファイナンスをクライシスマネジメントに含めて扱う．

3）売買当事者の合意で，価値の評価がなされる場所の代表に「オークション会場」がある．そこでは，「これにこの値段が付くのか」と驚くような落札がなされる事例が見られる．

4）例えば地震による建物倒壊を考えた場合，物理的な観点からは，地盤の揺れという外力によって，物質の形状が変わるという事象が起こっているに過ぎない．その物理的な「物質変形」をどう評価するかは，関係する人間が持つ価値観に大きく左右される．

5）例えば，保険数理の分野では「インシデントの生起確率」と何らかの手段で評価した「インシデントの影響度」の積，すなわち影響度の期待値として表される．

6）本論では，「ある対象」を指し示す役割をするコード（表記：近代言語学におけるシニフィアン）を「コトバ」，そのコトバが指し示す対象（シニフィエ）を「モノ（有形）」ないし「コト（無形）」と表している．

7）現象学や構造主義，それらをベースにした科学哲学である構造主義科学論（池田，1998），構造構成主義（西條，2009）など．

8）【生】：自身の命や遺伝子をはじめとして，関心を持つ人々の命やその遺伝子を含む「広義の生」の意．

9）歴史上，聖人とされる人物が行った，無私に見える尊敬される行動も，その人間にとっては，その行動で得

られる「心地良さ（快）」が，しなかったときの「心地悪さ（不快）」よりも大きいと感じられたからである．

10) 現代社会では，お金は「日々の糧」が姿を変えたものであり，これが増えることは【生】に近づくこと，減ることは遠ざかることである．それゆえ，人は手元にあるお金が増えることに「心地良さ（快）」を，減ることに「心地悪さ（不快）」を感じる．

11) この世の中に「A 社が存在する」と思うのは，私たちの思い込みである．私たちは，A 社の社屋，社長，従業員，工場などについては，指で指し示すことが出来る．一方で，A 社そのものについてはそれが出来ない．A 社というコトバが指し示している対象（組織）に物理的な実体がないからである．

12) 現象学（哲学）でいうところの「現象」，すなわち「意識への立ち現れ」であって，「物理的に起こる出来事」の意味ではない．

13) 世の中に多くある営利を目的とした組織が追求する「利」の本質は，組織に関係する各個人（ステークホルダー）の「心地良さ」にあり，決して，経営を行う側，その資金を投じる側の「お金の増加」だけにあるわけではない．「お金の増加」は，それを手にする人間の「心地良さを増大させる」がゆえ「利」と捉えられていると考えるのが妥当である．

参考文献

甘利康文（2006）「セキュリティの上位概念的考え方について」『電子情報通信学会技術研究報告』Vol. 105，No. 687，pp. 5-8.

甘利康文（2015）「セキュリティとは何か？ 安全，安心を実現する原理をその本質から理解する」，日本ネットワークセキュリティ協会設立 15 周年記念論文，http://www.jnsa.org/seminar/2015/nssf15/data/103_AmariYasufumi.pdf.

甘利康文（2016）「セキュリティとは何か？ 安全，安心を実現する原理をその本質から理解する」『日本セキュリティ・マネジメント学会誌』Vol. 29，No. 3，pp. 15-29.

池田清彦（1998）『構造主義科学論の冒険』講談社学術文庫.

大内尉義・秋山弘子・折茂肇（編）（2010）『新老年学 第 3 版』東京大学出版会.

京田亜由美・加藤咲子・中澤健二・瀬山留加・武居明美・神田清子（2009）「死を意識する病を抱える患者の死生観に関する研究の動向と課題」『群馬保健学紀要』Vol. 30，pp. 49-58.

京田亜由美・神田清子・加藤咲子・中澤健二・瀬山留加・武居明美（2010）「死を意識する病を抱える患者の死生観に関する研究内容の分析」『The KITAKANTO Medical Journal』Vol. 60，pp. 111-118.

西條剛央（2005）『構造構成主義とは何か 次世代人間科学の原理』北大路書房.

島薗進・竹内整一（編）（2008）『死生学 1 死生学とは何か』東京大学出版会.

内閣府（2013）「事業継続ガイドライン　あらゆる危機的事象を乗り越えるための戦略と対応」http://www.bousai.go.jp/kyoiku/kigyou/pdf/guideline03.pdf.

日本セキュリティ・マネジメント学会（編）（1998）『セキュリティハンドブック Ⅰ～Ⅲ』日科技連.

平山正実（1991）『死生学とはなにか』日本評論社.

諸岡了介・相澤出・田代志門・岡部健（2008）「現代の看取りにおける〈お迎え〉体験の語り」『死生学研究』Vol. 9，pp. 223-205.

山本俊一（1992）『死生学のすすめ』医学書院.

Amari, Y.（2008）“The Fundamental Definition of Security,” *Proc. BUEE2008（The 9th International Symposium on Building and Urban Environmental Engineering), Hong Kong*, pp. 203-207.

McNeil, A. J., et al.（2005）*Quantitative Risk Management: Concepts, Techniques and Tools*, Princeton University Press（塚原英敦ほか訳（2008）『定量的リスク管理　基礎概念と数理技法』共立出版）.