ORIGINAL ARTICLE

Comprehending Security through Shannon's Communication Model

Yasufumi AMARI

Intelligent Systems Laboratory, SECOM CO., LTD., 8-10-16 Shimorenjaku, Mitaka, Tokyo 181-8528, Japan

Abstract: Security in almost every field has often been implemented in a haphazard manner because a systematic approach has not yet been developed. To address this problem, we propose a context insensitive definition of security from a phenomenological perspective as well as its mathematical model through which we can understand the essence of security. Formalized syntax on security can be viewed as maintaining smooth operations even in the face of disturbances. Applying information theory to this syntax, we derive a mathematical model applicable to any situation where the term “security” appears and can understand what security is. Syntactic similarity between communication and security allows us to understand the essence of security and also to quantify security. These understandings free security from ad-hoc ways or best practices, limited to a single domain and not well-defined, depending on the Kansei, or intuition of the person in charge.

Keywords: *Security, Syntax, Information theory*

1. INTRODUCTION

The term “security” has often been seen in the press lately due to increased social awareness of IT incidents or terrorism. However, “security” can be used in various contexts, such as crime prevention, information security, national security, or food or energy security. Although many attempts have been made to define “security” [1,2], the term “security” remains ambiguous from a scientific viewpoint, and security itself is difficult to define and treat as an object for systematic management or engineering practice. For this reason, makeshift security practices are often implemented in a haphazard manner depending only on the Kansei of the person in charge. The term security has a wider concept [2] than simply crime prevention or information security. Security is one of the most important considerations for modern society. Unfortunately, “security” is used in a variety of contexts which can lead to misunderstandings.

In Chapter 2, we introduce formalized syntax and underlying essentials of security and propose a new systematic approach for specifying the fundamental meaning of the security [3-5]. These are phenomenologically derived from our various empirical experiences [Note 1] as a security service provider supplying security service in diverse areas from private life up to including governmental activities [6].

[Note 1] We provide security service, covering from physical world up to information, ranging over various kinds of industry or personal life, for more than 3.3 million subscribers all over the world. (See “<https://www.secom.co.jp/english/corporate/outline/>” and “<https://www.secom.co.jp/english/corporate/outline/about.html>.”)

Next, we ponder a mathematical model for the formalized syntax on security introduced above using information theory, which is applicable to any domain. Finally, we examine the structural similarity between the communication model proposed by Shannon [7] and our model for expressing the syntax on security to reinforce the validity of applying information theory to security.

Although quantitative evaluation methods on security have been proposed for specific domains such as information infrastructure [8-11], building crime prevention [12,13], energy supplies [14,15], and food security [16], these conditional quantitative evaluation metrics are domain-limited and are not suitable for a holistic evaluation of security. In addition, although various metrics for safety [17], such as STAMP or STPA, have been developed in the field of safety engineering, they assume that the main objective of these metrics is safety. Security and safety are often considered similar by the general public where the key difference is intent. However, this does not capture all the situations where the term security is used, for example, when security is used in a sense of availability. We will formalize security and show that the basic syntax on security is substantially different from safety in the next chapter.

Security is often assessed using best practices or ad-hoc methodologies derived from qualitative viewpoints in the real world, depending only on the Kansei of the person in charge, because quantitative evaluation methods for security in general have not yet been established.

Quantitative evaluation metrics are indispensable for scientific improvement [18]. Although security is one of the most important considerations for modern society, a

generalized method for quantitative evaluation has never been proposed.

The purpose of this paper is to show a unified conceptual bridgehead which is applicable to all fields where the term security is used, that formulates and describes security in a context insensitive manner. For this purpose, we will contemplate mathematical expression for the syntax on security. Note that the mathematical formulas in this paper are used not to discuss the mathematical rigor of security, but to find its essence through the modeling process.

Since the beginning of the twenty-first century, the rapid and growing number threats have led to Business Continuity Planning/Management (BCP/BCM) [19] as a technique to implement security. However, BCP/BCMs have often been implemented in an ad-hoc manner probably and one cannot objectively evaluate damage, as mentioned in Section 3.2. Herein we present BCP/BCM applications throughout as a case study of how the insights gained from our model of the syntax on security may be broadly useful.

(Note: This paper is a revised version of a report presented at SSI2015 [20].)

2. THE FORMALIZED DEFINITION [Note 2] FOR SECURITY

To systematically and syntactically handle security as an engineering object and to free security from haphazard implementations, we have abstracted the structural concept of security in all cases where the term “security” was used and define security [4,5] as follows.

Security: The operation of the entity, as planned by the subject, undisturbed by any inhibitors.

In this definition, *entity* refers to the organization, *operation* to the daily business or working of the organization, *subject* to the management or executive level of the organization and *inhibitors* to incidents which prevent the entity from operating according to plan. If the supply of food or energy is inhibited, a government cannot operate a nation. This is why the stability of food or energy supplies is regarded as an issue of the national security. For information security, unless “confidentiality,” “integrity” and “availability” are fully satisfied, an organization will face difficulties and cannot

[Note 2] This definition and the following implementation steps for security are inductively and empirically derived from our various experiences in the security industry through the phenomenological science logics [21,22], and are verified in many business cases in our practice. Note that this is not necessarily equivalent to the term “security” as used by the general public. In this paper, we will ponder security under the premise that this formalized syntax, or the definition and the framework, is an axiom on security.

keep its business smoothly. In other words, the formalized syntax on security is *maintaining smooth operations under a plan even in the face of disturbances against the operations*, or keeping homeostasis in an operation.

To implement this syntax on security, the following steps must be taken [4,5].

- (1) Identification of the operation and the subject
- (2) Creation of a clear operational plan
- (3) Identification of the resources indispensable for the operational plan execution
- (4) Identification of the resource inhibitors
- (5) Risk management (risk mitigation and crisis management) to minimize the influence of the inhibitors

This sequence is the framework [Note 3] to systematically and syntactically implement security from the fundamental definition, which is applicable to all situations. Although security has been a controversial subject for a long time [1,2] and even if security in the twenty-first century consists of many dimensions and is covering wide range of areas such as: public health, energy systems, aging society, information security, food and culture security [2], the above definition and the implementation steps empirically derived from our security business are unique and cover them all, as far as the syntax is concerned.

3. MATHEMATICAL EXPRESSIONS FOR THE FORMALIZED SYNTAX ON SECURITY [Note 4]

Hereafter, we will introduce our mathematical model to express our formalized syntax on security mentioned above.

3.1 Basic Views of the Mathematical Expressions

In information theory, self-information expresses the degree of rarity of an event's occurrence. If event E occurs with probability $P(E)$, and we have information about the event's occurrence, self-information $I(E)$, i.e. the quantified magnitude of information, is expressed as

$$I(E) = \log_2[1 / P(E)] = -\log_2 P(E). \quad (1)$$

[Note 3] Although this framework is empirically derived from our experience and has been brushed up in our security business, independently from any existing standard, it has relationship with the cybersecurity frameworks such as ISMS [23] or the U.S. NIST cybersecurity framework [24]. For instance, Steps (1)-(4) involve identifying the components mentioned in our proposed definition, similar to the recent U.S. NIST Cybersecurity Framework's first step of “identify.” Step (5) is analogous to the rest of the NIST Framework at a high level. Besides the above, a recent standard for risk management procedure [25] is also related to our framework.

[Note 4] Chapters 3 and 4 are the consideration to the “formalized syntax on security” mentioned in Chapter 2, not to so-called “security” as used by the general public.

Self-information [Note 5] is intentionally defined and formulated to satisfy three axiomatic conditions: (i) the magnitude must be monotonically decreasing as the occurrence probability of an event increases, (ii) the magnitude of an event which consists of mutually independent sub-events is equal to the sum of the magnitudes of each sub-event or $f(p_1 \cdot p_2) = f(p_1) + f(p_2)$, and (iii) the function is continuous over the entire range of the occurrence probability.

Self-information is a function of the occurrence probability of the event and has no relation to how the event may influence its surroundings. Thus self-information has no relation to meaning of the information.

Suppose that the event in consideration is the failure of an operation, O , or obstruction by some incident. In this case, self-information describes the rareness of the occurrence of the operation failure. Since the probability of the operation failure, $P(O)$, must logically be equivalent to the probability of how smoothly an entity operates as intended, self-information expresses the degree to which the entity operates according to the plan, or in the case of security, the quantified magnitude of security.

Countermeasures against an obstruction, which disturbs the operation and leads it failure, will lower the probability of the operation failure thus enhancing security for the operation. Since the quantified security magnitude increases as the operation failure probability decreases, condition (i) is satisfied. The probability of multiple independent obstructions occurring either simultaneously or sequentially can be expressed as the product of each obstruction probability. In this case, it is reasonable and convenient to treat the security magnitude as the sum of the security magnitudes of each incident, satisfying condition (ii). Furthermore, the security magnitude must be continuous over the entire range of the occurrence probability for some obstruction since discontinuous changes in the quantified security magnitude are unnatural, satisfying condition (iii).

Thus, the conditions for the quantified security magnitude are identical to the conditions for self-information. Consequently, the quantified security magnitude M for an operation can be modeled mathematically as

$$M = -\log_2 P(O), \quad (2)$$

[Note 5] When we think that a crime occurrence in the physical world is the target event E in information theory, cities where we live can be regarded as the information sources in the theory. In this case, self-information of each emergency phone call to report some crime occurrence to the police from the citizen, $-\log_2 P(E)$, expressing the degree of rarity of the crime occurrence, can be regarded as a security metric of the city where the call is placed. This is a beginning we intuit that Shannon's information theory should be a tool to consider security.

where $P(O)$ is the operation failure probability, or the probability of obstruction O to the operation, similar to self-information in information theory.

Note that this mathematical expression is intentionally modeled so that the quantified security magnitude M can satisfy the three conditions, not because it spontaneously satisfies the conditions. Although this mathematical model is intuitively formularized for our convenience [Note 6] so as not to conflict with the three conditions, namely the postulates to contemplate security, standing on this start point, we can develop a consistent understandable logical story regarding the formalized syntax on security as described later.

To apply the manner of thinking in information theory to security, we have to pay attention to the following. In information theory, thinking about occurrence probability of "a," or normalized appearance frequency of "a" in English sentences, for example, we do not need to define "what 'a' is" because of its obviousness. On the other hand, when viewing security, we must define the obstruction O , or "what 'failure of the operation' is," in advance, as a logical proposition to be able to decide success or failure of the target operation [Note 7].

Here, let $P(I)$ be the occurrence probability of an incident I . In addition, we assume every failure of the target operation (the obstruction O within the operation) is always brought by some incident I . We also assume that an incident during the operation does not always cause the obstruction. These assumptions are expressed as $O \subseteq I$ as shown by a Venn diagram in Fig. 1.

Under these assumptions, we obtain $P(O) = P(O, I)$, $P(I|O) = P(O, I) / P(O) = 1$, and $P(O|I) = P(O) / P(I)$.

Then $P(O|I)$ means the probability that the operation irreversibly stalls, develops permanent failures, or is

The operation develops failure only in this case.

Figure 1: Venn Diagram of the Relationship between the Incident Set and the Obstruction Set in the Target Operation

[Note 6] This is the same stance as Shannon took for mathematically modeling information in his work on information theory [7].

[Note 7] In case of the operation of marine or aviation transport, "failure of the operation" must be sinking or crash. When thinking about healthcare, we could consider decrease as the "failure of the operation." Generally, "failure of the operation" is that the operation irreversibly discontinues and is unrecoverable with some incident.

otherwise unrecoverable due to obstruction O resulting from incident I .

Accordingly, when thinking about security, we need to evaluate risk with both the occurrence probability of the incident $P(I)$ and the probability $P(O|I)$. In general, security measures to restrain the risk influences consist of two elements; one is lowering the occurrence probability of an incident $P(I)$, or “risk mitigation,” another is suppressing $P(O|I)$, the obstruction probability against the operation in the case of the incident occurrence, or “crisis management.” Crisis management is controlling $P(O|I)$, the influence of the incident against the operation, that the incident could make the operation failure.

As an example of these probabilities and suppression measures, we can think about disease control. Until the middle of the 19th century, appendicitis was feared as a fatal disease [26]. Although from the 19th century until now, almost the same incidence rate, $P(I)$, for appendicitis has been recorded (7%), the mortality rate, $P(O|I)$, has been lowered remarkably from 60% to 0.3% over this period through medical progress [27]. Meanwhile, in the case of smallpox, even now, although the mortality rate, $P(O|I)$, is still high when infected, the infection rate, $P(I)$ has been reduced to almost zero [28].

3.2 Mathematical Modeling for Damage to the Operation: Understanding Damage without Depending on Kansei

As mentioned above, measures of the risk management are classified into two categories,

- (1) Risk Mitigation: lowering the occurrence probability of incidents, and
- (2) Crisis Management: suppressing damage of the operation in the case of the incident occurrence.

In business fields, especially in the case of considering BCP/BCM [29,30], the damage evaluation may be understood as follows.

Suppose that the operating rate of some operation deteriorates at time t_0 due to an incident, and is restored at t_r , as shown in Fig. 2. Security aspects to lower the influence degree of the incident are depicted in the figure by $\langle 1 \rangle$ and $\langle 2 \rangle$.

Damage suppression, or crisis management, consists of two ways; one is restraining the operation deterioration, $\langle 1 \rangle$, and another is shortening the term of the deterioration, $\langle 2 \rangle$. In these conditions, we have believed that the damage magnitude D will be expressed as

$$D = \int_{t_0}^{t_r} [L_0 - L_d] dt, \quad (3)$$

where L_0 and L_d are the normal and deteriorated operating rates, respectively.

Figure 2: Operating Rate from Deterioration to Restoration (Controlling $\langle 1 \rangle$ and $\langle 2 \rangle$ will lower the damage.)

However, in actual cases, we will encounter difficulties and easily be stranded when comprehensively evaluating the damage magnitude D . For example, evaluating disease suppression metrics in this manner is impractical. This is because that Fig. 2 is just drawn as a conceptual image sacrificing many details. Therefore, the damage magnitude is often in practice determined not through (3), but through an arbitrary method or by intuition. This is not a sound evaluation method, then.

In addition, it should be noted that even if the same security measures for suppressing the influence of an incident are applied to two identical situations, the damage magnitude of each incident will differ since it is dependent on probabilistic contingencies. Namely, (3) ignores that the damage occurs with contingencies. The damage magnitude should be evaluated through some model including a certain probabilistic perspective.

Furthermore, “damage” is physically intangible and always appears in our consciousness under some sense of values – that is, it corresponds to economic utility. We often use an amount of money to express the damage magnitude. This habit tells us that the damage is not physical being same as the price. Monetary value is neither a physical quantity nor objective. Actually, thinking about damage is a philosophical matter in ontology. We have been under the fallacy that the damage magnitude should scientifically be evaluated through (3).

Thus, to address the issues above, by taking hints from *phenomenology* [Note 8] we consider and evaluate the damage magnitude as follows.

Although the so-called damage magnitude is strongly affected by subjectivity, or the Kansei, of an observer and often has ambiguity mentioned above, $P(O|I)$ can be scientifically observed or, at least, objectively determined under some assumption.

[Note 8] *Phenomenology*, established by Edmund Husserl (1859-1938), is the philosophical discipline considering the structures of experience and consciousness so that we can discuss perception especially for the intangibles. When we face difficulties to contemplate intangible entity, an attitude based on phenomenology can be a considerable helpful option to find out reasonable solution [31].

When $P(O|I)$ is large, it is intuitively obvious that we feel the damage is large [Note 9]. Conversely, when $P(O|I)$ is small, the damage must be felt small. In such manner, we put forward a hypothesis that the damage magnitude will monotonically increase with the value of $P(O|I)$. Therefore, considering this premise as a postulate of the way of thinking, we propose employing $P(O|I)$ as the impact index against the operation, or the normalized quantity representing the comprehensive damage magnitude. In other words, in real-world scenarios we should specify the damage magnitude by $P(O|I)$, observable with some statistical view point, not by (3). Otherwise, we will be trapped in the curse of the conceptual image shown in Fig. 2 and unable to scientifically identify the damage magnitude.

Note that this stochastic modeling for the damage magnitude is based on a statistical perspective of multiple operations with the same or similar attributes, which are affected by certain incidents with the same or similar attributes as well. For this reason, we must distinguish between operations or incidents with different attributes and not mix up them together, similarly to the case of social or epidemiologic studies.

Incidentally, representing the damage magnitude by $P(O|I)$ is similar to expressing gray shade in monochrome printing by using dot density, or appearance frequency of black dots in an unit area. Although each dot just has the binary values, black or white, we can see gray shade as a whole. Similarly, the understanding of the damage magnitude by $P(O|I)$ is based on a statistical perspective. Although the operations take the binary values, failure or success, we can see $P(O|I)$, as a certain value in the interval $[0, 1]$, representing the damage magnitude. This is the same as in the case of the mortality rate of a disease.

Besides the above, although it may seem like this view cannot be applied to crimes or other incidents with some intent, when enough and appropriate observations are taken, this statistical perspective, or expressing the damage magnitude by $P(O|I)$ will work well. We have used statistics to analyze not only unintentional incidents but also criminal actions or artificial incidents for a long time.

Now, let us get back on track. Since the probability of obstruction within the operations, or the operation failure probability [Note 10], given by

$$P(O) = P(I) \cdot P(O|I), \quad (4)$$

by substituting $P(O)$ into (2), it follows that the mathematical model of quantified security M is

$$M = -\log_2 P(I) - \log_2 P(O|I). \quad (5)$$

The first term is related to the frequency of the occurrence of the incident, and can be lowered by “risk mitigation” measures. The second term is related to the level of impact of the incident against the operation and can be suppressed by “crisis management” measures.

Here, let us think about an example of electric supply malfunction, with the same occurrence probability $P(I)$ at a hospital building and a private house. If power supply malfunction happens, private life, or the operation in home, is easily obstructed. On the other hand, because hospitals have private power generating systems in many cases, their medical practices, or the operation in the hospital building, might not be obstructed even if electric supply from the outside stops. Hence, the vulnerability of hospital to power supply malfunction, $P_{Hospital}(O|I)$, is smaller than $P_{Home}(O|I)$, that of a private home, because of these countermeasures. Therefore, $P_{Hospital}(O) < P_{Home}(O)$ and then the security level at hospital against a power supply standstill, $M_{Hospital}$ is larger than the one at home, M_{Home} , or $M_{Hospital} > M_{Home}$.

If a hospital's operation is obstructed by a power failure, the effect on the surrounding neighborhood would be much larger than one in the same case at private home. Hence, treating both cases in the same way in security consideration ought to raise doubts from readers. However, this way of thinking misreads what formalized security is. If you find yourself considering an incident's indirect influence on others, recall the definition of the formalized syntax on security again. In any case, the formalized syntax on security is *maintaining smooth operations under a plan even in the face of disturbances against the operations*, as highlighted in Chapter 2. It is defined by demarcating the entity, or the subject.

Whenever considering security, we always have to just focus on the operation itself as the object to secure, without considering the impact of the operation failure on others [Note 11]. The aftermath might cause an incident, other than the first one, against some operation by another subject, but that will be a separate story from the first target operation.

[Note 9] For instance, a serious state, we recognize in medical fields, is a situation with a high mortality rate, or $P(O|I)$, as can be seen from the example in Section 3.1.

[Note 10] This probability stands for the essence of a risk, or combination of the probability of occurrence of harm and the severity of that harm [32], often simply formulated by the multiplication of the both [33-35].

[Note 11] Needless to say, two operations, or medical practice in a hospital building and individual life at a house in the neighborhood of the hospital are completely different. However, it often happens to consider security in these dissimilar sites in the same manner because we tend to think about the aftermath by the same incident.

3.3 Multiple Incidents against the Operation

Consider an operation whose outcome is just either success ($\bar{O}$) or failure (O) [Note 12]. If p is the probability of failure resulting from an operational disturbance, $p=P(O)$. The degree of uncertainty in the operation, the security entropy $H_{Security}$, is given by following binary entropy function similar to information:

$$H_{Security} = -p \cdot \log_2 p - (1-p) \cdot \log_2 (1-p). \quad (6)$$

Binary entropy monotonically increases over the interval $p \in (0, 0.5]$, is maximized at $p=0.5$, and monotonically decreases over the interval $p \in [0.5, 1)$ [7] as shown in Fig. 3. As for security, the failure probability can be assumed to be small, i.e. $p \ll 0.5$, so entropy monotonically increases with p within the interval $p \in (0, 0.5]$ (See the solid line part in Fig. 3). Therefore, the small security entropy means that the operation tends to be in order and to work well. Conversely, if the security entropy, $H_{Security}$ goes large, the operation becomes tottering.

If an operation with a general probability of failure p with multiple failure factors O_i exist, the security entropy $H_{Security}$ is,

$$H_{Security} = - \left[\sum_{i=1}^n p_i \cdot \log_2 \sum_{i=1}^n p_i + \left(1 - \sum_{i=1}^n p_i \right) \cdot \log_2 \left(1 - \sum_{i=1}^n p_i \right) \right], \quad (7)$$

assuming that the failure probability of each factor is exclusive, or, at least, we can classify the failure factors so that each failure probability will become exclusive, i.e. $p = \sum p_i$. In this formula, n represents the total number of incidents and p_i is the probability that the i -th incident disturbs the operation, $p_i = P(O_i)$. The second term is dominant because $1 - \sum p_i$ expresses the operation success ($\bar{O}$) probability, and is ordinarily much larger than the

Figure 3: Security Entropy and the Assuming Probability Interval

[Note 12] This corresponds to that we regard the operation as a binary information source.

failure (O) one, $\sum p_i$, or $1 - \sum p_i \gg \sum p_i$, when considering security. $H_{Security}$ is the quantified degree of uncertainty in the operation. In security, we are primarily interested in the situations where the operation is successful, so we can assume that each probability p_i is sufficiently small so that $\sum p_i \ll 1/2$. Since each term of (7) is non-negative, uncertainty increases as the number of incidents n and the failure probability of each factor p_i increase.

Thus, when interested in just the outcome of the operation, success or failure, we can derive the security entropy just by substituting p with $\sum p_i$ in (6).

On the other hand, when taking each failure factor into account, we need to replace the first term of (7), entropy regarding the operation failure overall, with the sum of $-p_i \cdot \log_2 p_i$, entropy for each failure factor. Then, in this case, the security entropy will be

$$H_{Security} = - \left[\sum_{i=1}^n p_i \cdot \log_2 p_i + \left(1 - \sum_{i=1}^n p_i \right) \cdot \log_2 \left(1 - \sum_{i=1}^n p_i \right) \right]. \quad (8)$$

The model to employ depends on whether we are interested in simply failure/success or each failure factor in the operation.

Applying security measures to an operation lowers $P(I_i)$ and/or $P(O_i|I_i)$. Thus we can see that good security practices lower the entropy because p_i is the product of $P(I_i)$ and $P(O_i|I_i)$, as shown in (4). This decrease is the quantified value of the security measures applied against possible incidents. This enables the evaluation of security measures through their effect on entropy.

Thus, security measures impart negative entropy to an operation and its magnitude is the quantified efficacy of the security measures. Supplying the negative entropy to an operation, or suppressing the whole entropy in the operation, means lowering the occurrence probability of each incident I_i , $P(I_i)$, and/or the probability of the impact factors of each incident, $P(O_i|I_i)$. The former is the risk mitigation and the latter is the crisis management.

4. VALIDITY OF APPLYING INFORMATION THEORY TO SECURITY

The structural similarities, moreover, the essential identity, between communication and the formalized syntax on security allow the use of information theory for security.

4.1 Communication through Noisy Channels

Information theory has been developed by Shannon based on the *communication model* [7] shown in Fig. 4.

Figure 4: Model of Communication

Shannon's definition of communication is *reproducing at one point either exactly or approximately a message selected at another point* [7]. In general communication, even if we have the received information Y, we cannot know all of the source information X, because noise disturbs the transmission in the communication channel.

Mutual information between the source information X to be sent and the received information Y,

$$I(X;Y) = H(X) - H(X|Y), \quad (9)$$

represents the degree to which the received information Y contains the source information X. $H(X|Y)$ expresses conditional entropy, the remaining uncertainty about the source information X even when the received information Y is known. This is the degree to which we cannot reproduce the source information at the receiver, representing noise or disturbances in the communication channel. $H(X|Y)$ is zero only in the ideal case.

4.2 Structural Similarity between Communication and Security

Figure 5 shows a model of the formalized syntax on security in which we record the operational state in order to continuously evaluate the operations.

In this model, an *operation plan* (message X'), marked by ⟨A⟩ in the figure, is delivered to an *executor*, ⟨B⟩, in charge of the operations. The executor generates *operating actions*, ⟨C⟩, to implement the operation plan in the *real world*, ⟨D⟩. *Incidents*, ⟨E⟩, emerge stochastically (with the occurrence probability $P(I)$) from *risks*, ⟨F⟩, i.e. latent factors that disturb the operations and also stochastically (with the impact factor probability $P(O|I)$) affect the implementation of the operation plan in this phase. As the result, *actual operations*, ⟨G⟩, appear in the real world. An *observer*, ⟨H⟩, scrutinizes the operations as they actually occur and describes them as *operating records* (message Y'), ⟨I⟩.

Figure 5: Model of Security

Table 1: Parallels between Elements of Communication and Security Models

	Communication (Fig.4)	Security (Fig.5)
⟨A⟩	Info. to be Transmitted (Message X)	Operation Plan (Message X')
⟨B⟩	Transmitter (or Encoder)	Executor
⟨C⟩	(Transmitting) Signal	Operating Action
⟨D⟩	Channel	Real World
⟨E⟩	Noise	Incident
⟨F⟩	Noise Source	Risk
⟨G⟩	Received Signal	Actual Operation
⟨H⟩	Receiver (or Decoder)	Observer
⟨I⟩	Received Information (Message Y)	Operation Record (Message Y')

It is assumed that the executor provides actions to the real world without deviating from the operation plan and that the observer faithfully describes the operating situations. Namely, we assume that all errors in the operations described by this model can be attributed to the risks and incidents that latently exist inside the operations.

Comparing the *communication model* shown in Fig. 4 with the *security model* in Fig. 5, we can see a strong structural similarity, outlined in Table 1.

Using the structural similarity between these models shown in this table, we extend our comparison to information theory, which is derived from the communication model, and apply its logic to the formalized syntax on security. The more similar the operation record of the actual operations in the real world (Message Y'), corresponding to the received information (Message Y), is to the operation plan (Message X'), corresponding to the information to be transmitted (Message X), the higher the security degree of the operations is. This comparison between the two models suggests that it is appropriate to use information theory to evaluate security.

4.3 Comprehending an Operation in the Formalized Syntax on Security through Information Theory

We have, thus far, used the term "operation" without definition. Considering the correlation between communication and security shown in Table 1, we can define an "operation." Our definition of an operation is *generating situations planned by the subject, either exactly or approximately, in the real world*, which is similar to Shannon's definition of communication [7].

The mathematical model for the formalized syntax on security discussed above is an application of information handling methods to security in which information

entropy occurrences are regarded as disturbances during operations. For this reason, the security entropy (7) or (8) defines the measure of latent uncertainty inside operation plans before actual operations are performed. Thus, we can see that the security entropy expressed by (7) or (8) corresponds to the source entropy in communication.

Suppressing operational uncertainty at the planning stage corresponds to lowering entropy in the plans which can be considered as “risk mitigation” in the context of the BCP process. Since we are considering security under the assumption that, in a real-world operational system, failure cases are rare ($\sum p_i \ll 1/2$), the decrease in entropy is the quantified magnitude of the security measures applied to the operation in the planning stage. Decreasing the magnitude of the entropy inside the operational plan is the aim of security measures and risk management implemented in the planning stage.

In the ideal case, the operation records will be equal to the operation plans. However, the operation record Y' will not always equal the operation plan X' due to incidents from risks. Mutual information for security can be defined in the same way as (9),

$$I_{Security}(X'; Y') = H_{Security}(X') - H_{Security}(X'|Y'), \quad (10)$$

and can be used to evaluate an operation. $H_{Security}(X')$, defined in (7) or (8), is the entropy inside the operation plan, and $H_{Security}(X'|Y')$ is the entropy due to the uncertainty in the actual operation, independent from the operation plan. Concretely, $H_{Security}(X'|Y')$ represents the degree to which the executor cannot generate situations given by the operation plan, and may be considered a measure of disturbances (incidents that might occur from risks within the operation), or noise within the operation.

In BCP/BCM processes in actual business practices, one does not always distinguish between BCP and BCM. These are often considered the first half and the second half in the same procedure and are not necessarily clearly classified. However, as mentioned above, BCP is used for decreasing $H_{Security}(X')$, security entropy in the plans at the planning stage, whereas management procedures in the BCM framework are designed to suppress $H_{Security}(X'|Y')$, during the operation stage. Note that conditional entropy, $H_{Security}(X'|Y')$ is the degree to which we cannot execute the plan on site, and represents disturbances in the operation. Similar to the case of communication, $H_{Security}(X'|Y')$ is zero only in the ideal case.

4.4 Grounds Why We Can Apply Information Theory to Security

Communication, as defined by Shannon, can be understood as a special case of security. Communication is the operation to reproduce a source message as correctly as possible at a receiver side. Conversely, formalized syntax on security can also be considered as a sort of communication: the transmission of information from plans (Message X') before the operation to records (Message Y') after the operation, using the operation actions in the real world as communication signals.

The basic idea comes from consideration of flag semaphore signaling, a primitive remote visual communication method. In this method, a flag waver encodes information, such as some document to be transmitted, into signals in the form of flag motions. A watcher stares at the motions by the flag waver, decodes them, understands the information, and jots it down as a received document.

These actions done by the flag waver and the watcher suggest what the formalized syntax on security is. This sequence for remote communication is at the same time the operation in syntax on security. The flag waver as the signal transmitter (Fig. 4) can be understood as the operation executor (Fig. 5) in the operation called communication. Similarly, the watcher is both the signal receiver and the operation observer. Thus, flag semaphore signaling can be modeled with not only the communication diagram in Fig. 4 but also the security one in Fig. 5.

All of information theory is formulated on the principle model for communication shown in Fig. 4, as Shannon stated in his seminal work on the subject [7] (the first premise). Additionally, for the point considering above, we can say that communication and the formalized syntax on security are essentially identical (the second premise). Hence, because these two premises form a syllogism, it is deductively valid to consider information theory as an applicable framework for security.

From a security perspective, this comparison is especially beneficial, because information theory is a mature field, the result of many years' work. Since we have shown the strong structural similarity, or essential identity between security and communication in syntax, we will now be able to apply various information theory techniques to security development processes, such as BCP/BCM, ISMS, and even STAMP.

5. CONCLUSION

In this paper, we have introduced a basic concept for security with its implementation steps and a mathematical expression for the concept of the formalized syntax on security. The main contributions of the consideration in this paper are summarized as follows.

- (1) Showing the strong structural similarity, more precisely, the essential identity, between Shannon's model of communication and our model of the formalized syntax on security, we claim validity of our application of information theory, and discuss how information theory properties and definitions can be applied to security without domain limitations.
- (2) Our discussion of the application of information theory to security allows for information theory to be applied to security development, such as business continuity planning and management, etc., without field limitations.

Our model is constructed by applying information theory to syntax on security. In general, security means lowering and/or maintaining the entropy of a system so as not to exceed some limit. This can be equated to making and keeping order in a system. Security should be evaluated by observing the extent that a system deviates from its plan, a rule in advance. Security measures may be quantitatively determined by the degree to which order is imposed on the target system.

In any given system, whether physical or information [Note 13], entropy will naturally increase over time as the second law of the thermodynamics states. Consequently, entropy must be continuously removed from a system in order to maintain an entropy magnitude under the allowable limit. Every operation will gradually lose order and cannot continue to operate correctly without continuous efforts such as security measures or maintenance to reduce the entropy.

As Weaver remarked at the beginning of the first instructional textbook for Shannon's theory [36], "the word communication includes all human behavior, for example, not only written and oral speech, but also music, the pictorial arts, the theater, the ballet." This holds true for an operation, the object of security proposed in

this paper. He emphatically stated that "the theory is exceedingly general in its scope, fundamental in the problems it treats, and of classic simplicity and power in the results it reaches." Owing to these powerful characteristics of information theory, our proposed mathematical views for the formalized syntax on security are applicable to any domain.

As is well known, Shannon's theory does not deal with meaning of information and is context insensitive because "information is a measure of one's freedom of choice when one selects a message in the theory [36]." Similarly, from a syntactical, very abstract viewpoint, "security magnitude is a measure of the target operation's degree of freedom," namely, security magnitude is an index of the number of cases of the operating situations that the target operation implicitly has. Security measures correspond to lowering this degree of freedom, or the number of cases [Note 14]. Then, the decrease in entropy is the quantified magnitude of the security measures applied to the operation. Thus, our mathematical models are also context insensitive, allowing evaluation of security without domain limitations.

Security is unambiguously defined thus enabling mathematical modeling and treatment as an engineering object. This consideration for the formalized syntax on security makes it possible to scientifically view, evaluate, and design security in a wide variety of fields, enabling the systematic handling of security across different disciplines and organizations.

In this paper, we have introduced the generalized definition and the mathematical models for the formalized syntax on security which allow us the quantitative evaluation for security without distinction of domains. We expect that our view of security and the basic ideas through its mathematical expression will be useful in understanding security, enabling it to be developed and handled scientifically.

Meanwhile, the mathematical scope of this paper is limited to just proposing a conceptual framework to comprehend security under the premise that it is syntax [Note 15], a "level A communication problem [36]." As for future work, the formalized syntax on security and the basic ideas for its mathematical expression, as described in this paper, might be actually applied to quantitative analysis of security.

[Note 13] Information itself is logical, metaphysical entity and does not have a physical body. Consequently, in order to physically exist in the real world, it must be coded by some physical way, or spatiotemporal placement of substances, phenomena, or events. Namely, information recorded, transmitted, or sensible with our five senses is always physically tangible.

In such context, in spite of metaphysical entity by itself, any information cannot be free from the order of nature. This perspective is important to consider engineering fields' security measures, or "maintenance."

[Note 14] "Maintenance" in engineering fields also corresponds to this "lowering the number of cases." Hence, maintenance can be regarded as security measures in engineering field.

[Note 15] Although the scope of this paper is limited to syntax of security, as for security, semantics is still important. The author has semantically contemplated security [37].

REFERENCES

1. Rothschild, E.; What is security?, Daedalus, 124(3), The Quest for World Order, pp.53-98, 1995.
http://www.peacepalacelibrary.nl/ebooks/files/Rothschild_What-is-security.pdf
2. Kamprowski, R.; The essence and meaning of security towards the modern threats of the twenty-first century, Proceedings of the 2nd Electronic International Interdisciplinary Conference, pp.312-315, 2013.
<http://www.eiic.cz/archive/?vid=1&aid=3&kid=20201-92&q=f1>
3. Amari, Y.; Basic concept of the security and relationship between the security and the risk management, Technical Report of IEICE, 104(528), pp.17-20, 2004. (in Japanese)
4. Amari, Y.; A metaconcept of the security, Technical Report of IEICE, 105(687), pp.5-8, 2006. (in Japanese)
5. Amari, Y.; The fundamental definition of security, Proceedings of the 9th International Symposium on Building and Urban Environmental Engineering (BUEE2008), pp.203-207, 2008.
6. Itao, K. (ed.); Crisis management business in practice, In: Crisis management methodology and applications, (Kikikanri houhouon to sono ouyou), Chap.11, CMC Publishing, 2013. (in Japanese)
7. Shannon, E. C.; A mathematical theory of communication, Bell Labs Technical Journal, 27(3), pp.379-423, 27(4), pp.623-656, 1948.
<https://www.tnt.uni-hannover.de/edu/vorlesungen/InfoTheor/download/shannon1948.pdf>
8. Lie, D., and Satyanarayanan, M.; Quantifying the strength of security systems, Proceedings of the 2nd USENIX Workshop on Hot topics in Security (HotSec'07), 2007.
https://www.usenix.org/legacy/event/hotsec07/tech/full_papers/lie/lie.pdf
9. Madan, B.B., et al.; A method for modeling and quantifying the security attributes of intrusion tolerant systems, Performance Evaluation, 56(1-4), pp.167-186, 2004.
<https://www.sciencedirect.com/science/article/pii/S0166531603001342>
10. Fall, D., et al.; Security risk quantification mechanism for infrastructure as a service cloud computing platforms, Journal of Information Processing, 23(4), pp.465-475, 2015.
https://www.jstage.jst.go.jp/article/ipsjjip/23/4/23_465/_pdf
11. NPO Japan Network Security Association, Working Group for Vulnerability Quantification Study; Study report for vulnerability quantification, 2007. (in Japanese)
http://www.jnsa.org/result/2006/tech/vulnera/report_tv070518.pdf
12. Tatsumi, Y., et al.; Concept of crime risk evaluation for buildings based on crime PML, Summaries of Technical Papers of Annual Meeting, E-1, Architectural Institute of Japan, pp.953-954, 2009. (in Japanese)
13. Kondo, M., et al.; Evaluation of building vulnerability against invasion, Summaries of Technical Papers of Annual Meeting, E-1, Architectural Institute of Japan, pp.957-958, 2009. (in Japanese)
14. Kainou, K.; A study for quantification of the energy security, Research Institute of Economy, Trade and Industry, Government of Japan, 2004. (in Japanese)
<http://www.rieti.go.jp/users/kainou-kazunari/X0820GKApt1.pdf>
15. Ren, J., and Sovacool, B.K.; Quantifying, measuring, and strategizing energy security: determining the most meaningful dimensions and metrics, Energy, Vol.76, pp.838-849, 2014.
16. Fader, M., et al.; Spatial decoupling of agricultural production and consumption: quantifying dependences of countries on food imports due to domestic land and water constraints, Environmental Research Letters, 8(1), 014046, pp.1-15, 2013.
<https://iopscience.iop.org/article/10.1088/1748-9326/8/1/014046>
17. Leveson, N.G.; Engineering a safer world: systems thinking applied to safety, The MIT Press, 2011.
<http://sunnyday.mit.edu/safer-world.pdf>
18. Thomson, W. (Lord Kelvin); Electrical units of measurement, In: Popular lectures and addresses, Volume 1, pp.73-74, Macmillan and Co., 1889.
<https://archive.org/details/popularlecturesa01kelvuoft>
19. ISO 22301:2012, Societal security – Business continuity management systems – Requirements, 2012.
20. Amari, Y.; What is the essence of security? – Attempt to understand security from its mathematical expression, Proceedings of SSI2015, pp.245-250, 2015. (in Japanese)
21. Ikeda, K.; On the method of science – thoughts on a structuralist philosophy of science, Kampo Medicine, 57(2), pp.173-184, 2006. (in Japanese)
22. Saijo, T.; Constructing a theoretical basis for the human science via structural constructivism – through solving the difficult problems in the philosophy of science, Journal of the Japan Association for Philosophy of Science, 40(2), pp.37-58, 2013. (in Japanese)

23. ISO 27001:2013, Information Security Management System, 2013.
24. NIST; Cybersecurity framework.
<https://www.nist.gov/cyberframework>
25. ISO 31000:2009, Risk Management – Principles and Guidelines, 2009.
26. Williams, G.R.; A history of appendicitis, *Annals of Surgery*, 197(5), pp.495-506, 1983.
<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1353017/>
27. Søreide, O., et al.; Appendicitis – a study of incidence, death rates and consumption of hospital resources, *Postgraduate Medical Journal*, 60(73), pp.341-345, 1984.
<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2417863/>
28. World Health Organization; Smallpox, 2014.
<http://www.who.int/biologicals/vaccines/smallpox/en/>
29. Ranghieri, F., and Ishiwatari, M. (eds.); Business continuity plans, In: *Learning from Megadisasters: Lessons from the Great East Japan Earthquake*, Chap.9, pp.83-89, World Bank Publications, 2014.
30. Cabinet Office, Government of Japan; Business continuity guidelines: strategies and responses for surviving critical incidents (Third edition), 2013.
http://www.bousai.go.jp/kyoiku/kigyoku/pdf/guide-line03_en.pdf
31. Merleau-Ponty, M.: *Phénoménologie de la perception*, La Librairie Gallimard, 1945. (in French), English translation: *Phenomenology of perception*, Routledge & Kegan Paul, 1962.
32. ISO/IEC GUIDE 51:2014(E), Safety aspects – Guidelines for their inclusion in standards, 2014.
http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=53940
33. Akdeniz, C.; *Risk management explained*, First Publishing, 2015.
34. Ciobanu, M., and Mazilu, M.; Environmental crisis management through risk management, *Proceedings of the 1st International Conference on Tourism and Economic Development (TED'11)*, pp.537-541, 2011.
<http://www.wseas.us/e-library/conferences/2011/Drobeta/TED/TED-94.pdf>
35. Ogunsanmi, O.E., et al.; Risk classification model for design and build projects, *Journal of Engineering, Project, and Production Management*, 1(1), pp.46-60, 2011. http://www.ppml.url.tw/EPPM_Journal/volumns/01_01_July_2011/ID_003.pdf
36. Weaver, W.; Recent contributions to the mathematical theory of communication, In: Shannon, C.E., and Weaver, W., *The mathematical theory of communication*, pp.1-28, University of Illinois Press, 1998.
https://pure.mpg.de/rest/items/item_2383164/component/file_2383163/content
One can independently see the Weaver's comment below.
<https://pdfs.semanticscholar.org/c4ee/686f5dd14ac83c4b10a8bce9a62341ea0a3a.pdf>
37. Amari, Y.; What is security? – Understanding of the semantical essentials of security to accomplish safety and the peace of mind –, *Security Management*, 29(3), pp.15-29, Japan Society of Security Management, 2016. (in Japanese)

Yasufumi AMARI (Member)

Yasufumi Amari is a group leader of the risk management group at Intelligent Systems Laboratory (ISL), SECOM CO., LTD., Japan's largest security service firm in the private sector. He received the B.S. and M.S. degrees from Keio University, Japan, in 1984 and 1986, respectively. Since 1987, he has worked at ISL, Tokyo, Japan and was a research affiliate at Media Laboratory, Massachusetts Institute of Technology dispatched from ISL from 1990 to 1991. His interests include concept of security and risk analysis/management, and philosophy of science in the security field. He is tackling research to reveal essence of security itself and security related conceptual entity, such as risk. He is a part-time professor at "Master's/Doctoral Program in Risk and Resilience Engineering," University of Tsukuba.
His email address is "y-amari" at "secom" dot "co" dot "jp."