⇨解説

基般

情報理論的暗号技術について

四方順司　渡邉洋平（横浜国立大学大学院環境情報研究院／学府）

情報理論的安全性

暗号は今日まで長い歴史を持つが，1949 年に発表された Shannon の論文[10] によって初めて理論的立場から数理体系的に捉えられたといえる．また，彼は 1948 年の情報理論に関する論文[9] で，さまざまな情報に関する概念の定式化を行っており，その中でも情報量の定式化としてのエントロピーの導入は，情報理論の主題である情報源符号化や通信路符号化において重要なだけでなく，暗号を理論的に捉える上でも大きな役割を担っている．この情報量の定式化としてのエントロピー，あるいはその他の情報理論的指標を用いて暗号システム（プロトコル）のモデルやセキュリティを理論的に捉えようというのが，情報理論的暗号理論である．

現代暗号理論における安全性は，主に計算量理論的安全性（計算量的安全性）と情報理論的安全性（情報量的安全性）に大別される．前者においては，素因数分解問題，あるいは離散対数問題といったような，ある種の計算困難な数学的問題を仮定して，対象の暗号システムの安全性を証明する方法論がとられる．Diffie, Hellman によって公開鍵暗号が発表されて以来[4]，今日に至るまで，多くの計算量的安全性を有する暗号技術が研究開発されてきた．一方，後者は，そのような数学的問題の計算困難性に関する仮定を必要とせずに，攻撃者が知り得ない情報量を担保にして情報理論的あるいは確率論的立場からシステムの安全性を証明する方法論がとられる．後者の情報理論的安全性の議論において，前者と異なる点は攻撃者の計算能力にある．つまり，前者における攻撃者の計算能力は高々多項式時間であると仮定するのに対して，後者の攻撃者の計算能力は無制限であると想定する．したがって，計算困難な問題を利用しても，攻撃者は無尽蔵に計算資源をかけて計算すればその解が存在する限り解けてしまうため，計算困難な問題だけで情報理論的安全性を達成することは本質的に不可能であろう．通常，情報理論的安全性は，特定の計算モデル，計算困難性に直接的に依存することなく定式化されているため，計算の高速化，アルゴリズムの改良，新たな計算メカニズム（量子計算機等）の登場によって，安全性が損なわれることはない．

ここで，直感的に，上記の 2 種類の安全性の基礎となる仕組みの例示を考えてみよう．まず，2 つの素数 p, q とその積 $n(=pq)$ を考え，公開情報 n から秘密情報 p, q を求める問題（素因数分解の計算問題）を考えてみよう．数学的には素因数分解の一意性から $n=pq$ を満たす素数 p, q の組合せは一意に決まるため，無尽蔵に計算資源を費やせばいつかは解が求まるであろう．しかし，攻撃者の計算能力が多項式時間しかなく，素因数分解問題が多項式時間では解けないと仮定すれば，一般に攻撃者にはこの解を求めることができない．この仕組みを暗号技術の安全性に利用する考え方が計算量理論的安全性の考え方である．次に，$\mathbb{F}_q$ を q 個の元からなる有限体とし，$x, y \in \mathbb{F}_q$ とその和 $z=x+y \in \mathbb{F}_q$ を考える．そして，公開情報 z から秘密情報 x, y を求める問題を考えてみよう．この場合は先の素因数分解とは異なり，$z=x+y$ を満たす解 (x, y) は q 個ある．ここで，いくら計算資源を費やしてもこの解の候補が減るわけでもなく，この中の 1 つが正しい解ならば最後は推測するしかないであろう．ただし，q が非常に大

きな数（素数ベキ）であれば推測が当たる確率はほとんど 0 に近い．この仕組みを暗号技術の安全性に利用する考え方が情報理論的安全性の考え方である（「暗号化」の節のバーナム暗号の記述も参考にせよ）．

上述したように，情報理論的安全性は計算の高速化，アルゴリズムの改良，新たな計算メカニズムの登場によって，安全性が損なわれることはないという利点を持つが，一般的に，この安全性を持つ暗号システムでは，各ユーザが持つべき秘密情報（秘密鍵）が多くなるため，その情報量を正確に評価することは重要である．そのため，秘密鍵サイズの下界，最適な構成法[☆1]に関する議論は重要である．また，実用性または応用的な観点から見て解決すべき研究課題も多い．本稿では，情報理論的安全性に基づく基本的な暗号技術（暗号化，認証）のモデルを解説するとともに，必要な秘密鍵サイズの下界，最適な構成法に関しても解説する．また，実用的・応用的な観点からの研究動向についても簡単に紹介する．

情報量にかかわる概念：エントロピー

情報量の定式化としての Shannon エントロピーは，Shannon[9] によって導入され，情報理論だけでなく，情報理論的暗号技術を考える上でも重要である．$\mathcal{X}$を有限集合とし，$|\mathcal{X}|$ を$\mathcal{X}$の元の個数（cardinality）とする．X は$\mathcal{X}$に値をとる確率変数とし，その確率分布を P_X とする．このとき，X の Shannon エントロピー（以下，エントロピーと呼ぶ）は

$$H(X) := -\sum_{x\in\mathcal{X}} P_X(x)\log_2 P_X(x)$$

で定義される（記号 := は左辺を右辺で定義することを意味する）[☆2]．ただし，上記の和において $0\log 0 := \lim_{t\to 0} t\log t = 0$ とする．ここで，$H(X)$ は X のとり得る値をビット表現（2 進表現）するときの平均的な桁数（期待値）を表していると解釈でき，$H(X) = \mathbb{E}_X\left[-\log P_X\right]$ とも書ける．確率分布 P_X が一様分布に近ければ近いほど $H(X)$ が大きくなることから，$H(X)$ は X の不確定性の尺度（曖昧さ）と考えられる．また，X の曖昧さをなくすことは，結局は X の情報を得ることであると考えられ，このようにして $H(X)$ は X の情報量を定式化したものであるとみなせる．

また，X のとり得る値の中で最も生起しやすい値の曖昧さを最小エントロピー（min-entropy）といい，次のように定義される．

$$H_\infty(X) := \min_{x\in\mathcal{X}}(-\log_2 P_X(x)) = -\log_2 \max_{x\in\mathcal{X}} P_X(x).$$

$H_\infty(X)$ は，とりわけ，暗号理論においてよく利用される尺度である．ここで，定義より，$H_\infty(X)\le H(X)$ の関係が成り立つことにも注意しよう．

また，1 つの確率変数のみを考えるのではなく，互いに相関を持った複数の確率変数に対してもエントロピーは定義される．X, Y を有限集合 $\mathcal{X}$, $\mathcal{Y}$ にそれぞれ値を持つ確率変数とする．また，X, Y はそれぞれ確率分布 P_X, P_Y を持つものとし，(X, Y) を結合確率分布 P_{XY} を持つ 1 つの確率変数と考える．このとき，エントロピー $H(X, Y)$ は

$$H(X,Y) := -\sum_{x\in\mathcal{X},y\in\mathcal{Y}} P_{XY}(x,y)\log_2 P_{XY}(x,y)$$

により定義される．同様にして，一般的に $H(X_1, X_2, \cdots, X_m)$ も定義される．これらを結合エントロピー（joint entropy）と呼ぶ．

また，X, Y をそれぞれ有限集合 $\mathcal{X}$, $\mathcal{Y}$ に値をとる確率変数とするとき，条件付きエントロピー（conditional entropy）が

$$H(X|Y) = \sum_{y\in\mathcal{Y}} P_Y(y)H(X|Y=y)$$

で定義される．$H(X|Y)$ の定量的意味合いは，Y の情報が分かっているときに X をビット表現するために必要な平均的な桁数を表していると解釈できる．このことから，$H(X)$ の場合と同様に考えて $H(X|Y)$ は Y の情報を獲得するときの X の持つ情報量を表現している．

最後に $H(X)$, $H(X, Y)$, $H(X|Y)$ の性質を述べる．

☆1 最も短いサイズの秘密鍵により，安全なシステムを構成する方法．

☆2 ここでは情報を測る単位をビットで考えているため，対数の底は 2 としている．ナット，ディット（ハートレー）の場合はそれぞれ底を e，10 とする．

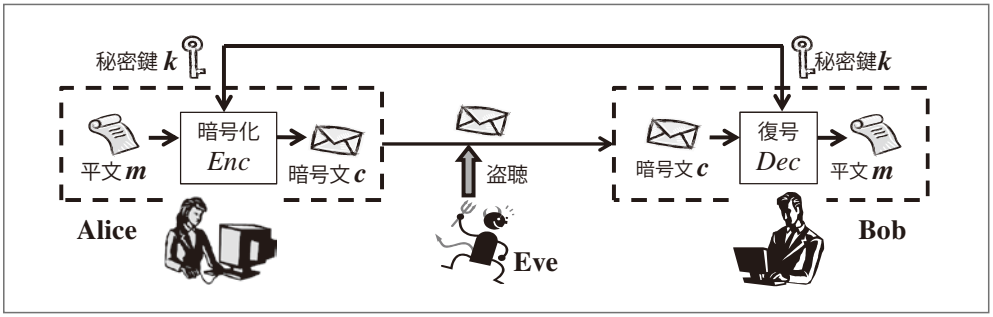

図 -1　暗号化技術

これらの証明，およびエントロピーに関するさらなる詳述については本稿では割愛する．

エントロピーの性質

1) 値域：$0 \leq H(X) \leq \log_2 |\mathcal{X}|$，左の等号成立のための必要十分条件は，ある $x \in \mathcal{X}$ に対して $P_X(x)=1$（つまり，P_X が自明であるとき）が成り立つこと，また右の等号成立のための必要十分条件は，すべての $x \in \mathcal{X}$ に対して $P_X(x)=1/|\mathcal{X}|$（つまり，一様分布のとき）が成り立つこと．
2) 単調増加性：$H(X) \leq H(X, Y)$.
3) チェイン・ルール：$H(X, Y)=H(X)+H(Y|X)$. 一般に，$H(X_1, X_2, \ldots, X_m)= H(X_1)+H(X_2|X_1)+H(X_3|X_1, X_2)+\cdots+H(X_m|X_1, X_2, \ldots, X_{m-1})$.
4) 条件付きエントロピーの性質：$H(X|Y) \leq H(X)$，等号成立の必要十分条件は，X と Y が独立であること．つまり，任意の $x \in \mathcal{X}$, $y \in \mathcal{Y}$ に対して，$P_{X,Y}(x, y) = P_X(x)P_Y(y)$ が成り立つこと．

情報理論的暗号技術

情報理論的暗号技術では，計算困難な数学的問題に関する仮定を必要としない代わりに，特有のモデルもしくは仮定が必要となる．その代表的なものとして，TI モデルを紹介する．これはシステムの開始時にだけ，信頼できる第三者機関 TI（Trusted Initializer）とその機関からユーザへの安全な通信路を仮定したモデルであり，TI はシステムで必要な秘密鍵を生成し，それらを対応するユーザへ安全に配送する．情報理論的暗号技術の中には，明確にこのモデルと言及していなくても，暗にこのモデルを利用している方式も少なくない．本章では，情報理論的安全性に基づく暗号基礎技術として暗号化およびメッセージ認証技術に関して解説するが，これら暗号技術はすべて TI モデルを利用しており，各説明の中で特に言及はしないので注意されたい．

⇨ 暗号化（Encryption）

情報理論的暗号技術では公開鍵暗号は実現できないことが知られている．したがって，暗号化鍵は公開できず，ユーザの秘密鍵でないといけない．ここでは，Shannon による共通鍵（送受信者間で共通の秘密鍵）を用いた暗号化方式を紹介する（**図 -1** も参照）．

$\mathcal{K}$ で秘密鍵全体の集合を，$\mathcal{M}$ で平文全体の集合を，さらに $\mathcal{C}$ で暗号文全体の集合を表す．秘密鍵 $k \in \mathcal{K}$ は Alice と Bob のみが知っているものとし，Alice と Bob の間には盗聴可能（改ざんは不可）な通信路があるとする．Alice は平文 $m \in \mathcal{M}$ を秘密鍵 k を用いて暗号化し，その結果，暗号文 $c \in \mathcal{C}$ を得る．これを，$c=Enc(m, k)$ と書き，Enc は暗号化アルゴリズムを表す．その後，Alice は c を上記の通信路で Bob に送信する．このとき，盗聴者 Eve は c を見ることができる．Bob は受け取った暗号文 c を秘密鍵 k を用いて，もとの平文 m を復号し，これを $m=Dec(c, k)$ と書く．ただし，Dec は復号アルゴリズムを表す．また，任意の $m \in \mathcal{M}$, $k \in \mathcal{K}$ に対して，$m=Dec(Enc(m, k), k)$ とする．つまり，復号時にエラーは起こらないものとする．

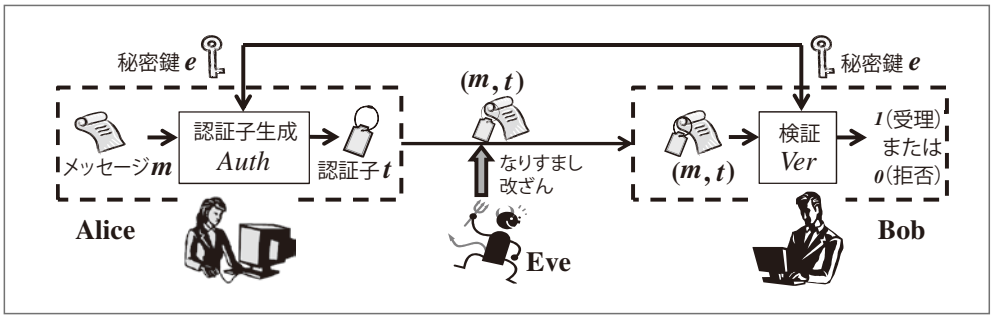

図 -2
メッセージ認証技術

ここで，上記のモデルが完全秘匿性（Perfect Secrecy）を持つとは，平文 m とその暗号文 c に対して盗聴者 Eve が，c から m のいかなる部分情報も得られないときをいう．以下では，K, M, C をそれぞれ $\mathcal{K}, \mathcal{M}, \mathcal{C}$ に値をとる確率変数とし，上記の暗号化方式の完全秘匿性をエントロピーを用いて定式化すると，

$$H(M|C) = H(M) \tag{1}$$

と表せる．これは，通信路上を流れる暗号文を見たとしても，平文に関する情報を何も得ることができないということを表している．

一般に，完全秘匿性を有する暗号化方式において，秘密鍵と平文のエントロピーに関して，不等式

$$H(K) \geq H(M) \tag{2}$$

が成り立つことが以下のように示される．

$$\begin{aligned} H(M) &= H(M|C) && \text{（完全秘匿性の定義 (1) より）} \\ &\leq H(M, K|C) && \text{（単調増加性より）} \\ &= H(K|C) + H(M|C, K) && \text{（チェイン・ルールより）} \\ &= H(K|C) && (3) \\ &\leq H(K). && \text{（条件付きエントロピーの性質より）} \end{aligned}$$

ただし，(3) は秘密鍵と暗号文から復号エラーなしに一意的に平文を復号できることから従う．このことから完全秘匿性を持つ暗号化方式においては，秘密鍵のエントロピーは平文のエントロピー以上であることが分かる．ここで不等式 (2) の等号成立という意味で，最適な構成方法として，バーナム暗号（Vernam's cipher, one-time pad）が知られている．バーナム暗号では，平文 m を n ビットのデータ，秘密鍵 k を n ビットの乱数として，Alice は $c = Enc(m, k) := m \oplus k$ を計算する．ただし，$\oplus$ はビットごとの排他的論理和を表す．Bob は受け取った暗号文 c と自身の秘密鍵 k から，$Dec(c, k) := c \oplus k$ を計算することで，平文 m を復号する．

⇨メッセージ認証（Authentication code）

本節では，情報理論的に安全なメッセージ認証（Authentication code：以下，A-code と略記）について解説する（**図 -2** も参照）．A-code は通信路上で情報の改ざんが行われたか否かを検出するための方式であり，Gilbert らによって初めて提案され [5]，Simmons によって 1980 年代に大きく発展した [11]．暗号化の場合と同様に，送受信者間で共通の秘密鍵を用いた A-code のモデルを次のように記述する．$\mathcal{E}$ で秘密鍵全体の集合，$\mathcal{M}$ でメッセージ全体の集合，さらに $\mathcal{T}$ で認証子全体の集合を表す．ここで認証子とは，メッセージと一緒に通信相手に送る冗長な情報のことで，通信路上でのメッセージの改ざん検出に利用するための重要なディジタルデータである（後述）．Alice は秘密鍵 $e \in \mathcal{E}$ を使い，メッセージ $m \in \mathcal{M}$ に対する認証子 $t \in \mathcal{T}$ を生成し，これを $t = Auth(m, e)$ と書く．ただし，$Auth$ は認証子生成アルゴリズムである．その後，Alice はメッセージと認証子の組 (m, t) を通信路を介して Bob に送る．このとき，攻撃者 Eve は送信者になりすましてメッセージを通信路に挿入したり（なりすまし攻撃と呼ぶ），通信路を流れる (m, t) を見てほかのものに置き換えようとする（改ざん攻撃と呼ぶ）．Bob は，受け取ったメッセージと認証子の組 (m, t) が正当なものかどうか（Eve によって，なりすま

されたり，別のものに置き換えられたりしていないかどうか）を秘密鍵 e を用いて検証することができ，正当なものであれば $Ver(m, t, e)=1$，そうでなければ $Ver(m, t, e)=0$ と書く．ただし，Ver は検証アルゴリズムである．

ここで，なりすまし攻撃，改ざん攻撃の成功確率は，次のように定式化される．

なりすまし攻撃：送信者になりすまして，偽造したメッセージと認証子の組 (m, t) を受信者に送り，受理させようとする攻撃（なりすまし攻撃）の成功確率は，

$$P_I = \max_{(m,t)} \Pr(Ver(m,t,e)=1)$$

で定義される．

改ざん攻撃：送信者が送った正当なメッセージと認証子の組 (m, t) を見た後で，偽造したメッセージと認証子の組 (m', t') を受信者に送り，受理させようとする攻撃（改ざん攻撃）の成功確率は，以下で定義される．

$$P_S = \max_{(m',t')} \max_{(m,t)\neq(m',t')} \Pr(Ver(m',t',e)=1 \mid (m,t)).$$

なりすまし攻撃の成功確率が ϵ 以下であり，改ざん攻撃の成功確率が ϵ 以下であるとき（$P_I \leq \epsilon$ かつ $P_S \leq \epsilon$ のとき），その A-code は ϵ-secure（ϵ-安全である）という．さらに，証明は割愛するが，このモデルにおける攻撃成功確率に関して，不等式 $\max(P_I, P_S) \geq |\mathcal{E}|^{-\frac{1}{2}}$ が成り立つ．これにより，ϵ-安全な A-code では $\max(P_I, P_S) \leq \epsilon$ であることから，容易に鍵集合に関する下界

$$|\mathcal{E}| \geq \epsilon^{-2} \tag{4}$$

が示される．ここで，不等式 (4) において等号を与える最適な構成法として，次のシンプルなものが知られている．$\mathbb{F}_q$ を q 個の元からなる有限体とし，$\mathcal{M}=\mathcal{T}=\mathbb{F}_q$ とする．また，Alice と Bob の秘密鍵 e は，一様ランダムに選ばれた $a, b \in \mathbb{F}_q$ により，$e=(a, b)$ とする．さらに，アルゴリズム $Auth$, Ver を以下のように構成する．$Auth(m, a, b)=am+b$．$Ver(m, t, a, b)=1$ となるのは $t=am+b$ が満たされるときであり，満たされないときは $Ver(m, t, a, b)=0$ とする．この構成法において，P_I, P_S を計算すると，$P_I=P_S=1/q$ となり，したがって，この A-code は $1/q$-安全であることが分かる．また，この構成法では $|\mathcal{E}|=q^2$ となり，不等式 (4) において $\epsilon = 1/q$ とおくと，等号を満たしていることも分かる．

A-code では送信者と受信者は不正を行わないことを前提とするモデルであるが，送信者または受信者のどちらか一方が不正することを考慮し，調停者（arbiter）を加えた A^2-code (authentication code with arbitration) や，さらにその調停者のある種の攻撃も考慮した A^3-code (A^2-code protecting against arbiter's attacks) も知られている．

また，送信者から複数の受信者へのメッセージ認証技術である MRA-code（multireceiver authentication code）や，その拡張方式である MRA^2-code, MRA^3-code，およびさらに強い安全性を持つ電子署名（ディジタル署名）に関する研究等がある．

情報理論的暗号理論におけるモデル

本章では，情報理論的暗号理論において，TI モデル以外によく利用されるモデルを紹介する．

Bounded Storage Model（BSM）[7]：攻撃者は一時的に記憶容量（メモリ）が制限されるという仮定のもと，（攻撃者が制御できない）乱数源から発生した長い乱数列をすべてのエンティティ（ユーザだけでなく攻撃者も含む）が利用できるモデルである．ただし，攻撃者は一時的な記憶容量の制限から乱数列すべてを記憶できないと仮定するが，その計算能力には制限を加えず，また乱数列の配信後では攻撃者の記憶容量が制限されることもない．また，BSM の暗号プロトコルでは，ユーザは乱数のすべてを記憶しなくともプロトコルを正常に実行可能である．このモデルの例示として，しばしば，人工衛星から長い乱数列をブロードキャストする場合が挙げられる．

雑音通信路を利用するモデル[12]：通常，暗号理論では，利用する通信路には雑音は生じないと

仮定して[☆3]，議論する場合が多い．このモデルでは，ユーザ間で雑音通信路（noisy channel）を利用して情報伝達を行い，また盗聴している攻撃者はこの雑音通信路から情報を得ることができる．ただし，ユーザ間の雑音と，ユーザと攻撃者間の雑音の生じ方には差があり，この差を利用して暗号システムを構成することが可能である．そのため，このモデルでは特性が既知の雑音通信路が利用される．

量子通信路を利用するモデル：これまで，量子通信路（quantum channel）を利用して暗号システムを構成する試みが多く行われてきた．このモデルでは，理想的な量子通信路を仮定し，暗号システムの安全性は物理学（量子力学）の原理や量子情報理論によって示すアプローチがとられる．量子通信路を利用した暗号システムのうち，最も著名なものとして，Bennet, Brassard によって提案された量子鍵配送[2]が挙げられ，この方式は BB84 プロトコルとも呼ばれている．

実用と応用に向けて

TI モデルや「情報理論的暗号理論におけるモデル」の章で紹介したモデルを利用できれば，攻撃者の計算能力に依存しない非常に強い安全性を持つ情報理論的暗号技術が実現できる．しかし，一般に，情報理論的暗号技術では，特有のモデルや仮定の工学的実現可能性，また鍵長が長くなってしまうことなど，実用的観点から考察すべき研究課題もいくつか存在する．本章の 1 つ目の節では暗号化方式に焦点をあてて，実用的観点から見た理論的研究課題とその研究動向を紹介し，本章の 2 つ目の節では工学的応用として物理層セキュリティ（Physical Layer Security）を紹介する．

⇨ 理論的研究課題と研究動向

「情報理論的暗号技術」の章，「暗号化」の節で解説した完全秘匿性は最も強い安全性という意味で，いわば暗号化方式の究極の安全性である．しかし，完全秘匿性を実現するにおいて，以下の内容が必要であったことを思い出そう．

(1)（TI モデルまたはそれに相当する）鍵共有のメカニズムを効率的に実現することが必要．
(2) 鍵のエントロピーが平文のエントロピー以上である．

まず，(1) に関して，社会的なインフラで TI モデルが実現できない場合にも，「情報理論的暗号理論におけるモデル」の章で紹介したモデル等を利用して鍵共有のメカニズムを実現するための研究が進められている．実際，BSM での鍵共有，雑音通信路を用いた鍵共有，そして量子通信路を用いた量子鍵配送等の研究成果がすでに発表されている．紙面の都合上，その詳細について本稿では割愛する．

次に，(2) について考察してみよう．完全秘匿性を考える限り，(2) の結論に至ることは仕方がない．そこで，安全性の定義を以下のように再考し，完全秘匿性よりも少し弱い安全性にすることで，鍵サイズの削減を可能にする研究成果（安全性と効率化のトレードオフ）が発表されている．

ϵ -Secrecy：「情報理論的暗号技術」の章，「暗号化」の節の解説と同じ方法により，完全秘匿性を少し弱めることで（すなわち，$H(M) - H(M|C) \leq \epsilon$），鍵のサイズを平文のサイズより，少し小さくできる（すなわち，$H(K) \geq H(M) - \epsilon$）．この安全性は，しばしば ϵ -secrecy と呼ばれる．

Entropic Security[8]：n ビットの平文の確率変数 M の最小エントロピーが大きいとき，完全秘匿性を弱める安全性を考えることで鍵サイズの削減が可能である．具体的には，M の最小エントロピーが $n - l$ 以上のとき（すなわち，$H_\infty(M) \geq n - l$），完全秘匿性から安全性を ϵ だけ弱めて，鍵のビット長を $l - \log \epsilon$ の定数倍まで短くすることができる．

Guessing Secrecy[1]：最小エントロピーにより，$H_\infty(M|C) = H_\infty(M)$ で定義する安全性．この定義は，Shannon による完全秘匿性よりも弱い安全性定義であるため，その分，鍵サイズも小さくできる．

さらに，最近，岩本・四方によって，Shannon

☆3 実際の通信路には雑音が生じるので，誤り訂正符号等の手法を適用して雑音を除去した後の通信路が想定されている．

エントロピーではなくRényiエントロピーを用いた安全性定義による暗号化の理論体系も提案されており，この理論的枠組みは，「情報理論的暗号技術」の章，「暗号化」の節の内容，上述のϵ-Secrecy, Guessing Secrecy すべてを包含する一般的な理論体系となっている[6]．

⇨ 応用：物理層セキュリティ

無線通信の技術は，テレビ・ラジオの放送や携帯電話等，我々の日常生活において広く利用されている身近な技術の1つである．特に近年，その利便性からパソコンの通信ネットワーク（無線LAN）や家電等において同技術の利用が急速に広がっており，我々の生活に欠かせない重要な技術となりつつある．

無線通信は，オープンな空間で電波を用いて情報のやりとりを行うという性質上，不特定多数の人に受信される可能性があることが前提である．そのため，有線の通信に比べて，通信内容の盗聴等の危険性が高いことが問題となっている．このような盗聴等の不正行為への対策としては，無線LAN環境向けのセキュリティ規格であるIEEE802.11iや，インターネット上で行うサーバ認証から暗号通信の一連の処理手順であるSSL/TLS等の規格に基づき，共通鍵暗号（AES）や公開鍵暗号（RSA，楕円曲線暗号）等の計算量的安全性に基づく暗号技術の利用が，実用的観点からも一般的である．

無線通信においては有線通信と同様，通信相手との互換性を維持するために，階層構造により定義されているOSI参照モデルやTCP/IPアーキテクチャ等のネットワークアーキテクチャ規格に基づき設計されている．従来，通信全体の安全性を確保するために用いられる共通鍵暗号や公開鍵暗号は，上位層（アプリケーション層やトランスポート層等）で用いられるのが一般的である．一方，最下層である物理層では，電波や光等の通信媒体を介して行われる通信の信頼性確保（誤り訂正機能等）が重要視され，通信内容の安全性確保（特に，秘匿性）に関する議論はあまり行われていなかった．近年，この物理層において，信頼性に加えて安全性も同時に実現させることにより，無線通信全体の安全性をより柔軟に設計することを目的とした新たな安全性の枠組みとして，物理層セキュリティ（Physical Layer Security）が提案されている[3]．

物理層セキュリティの枠組みにおいては，情報理論的に安全な暗号技術（「情報理論的暗号技術」の章や，「情報理論的暗号理論におけるモデル」の章で紹介した基本的な枠組みに基づく）や通信路符号化技術を応用した，物理層における通信路の信頼性と安全性をともに実現可能な技術に関する研究が行われており，これまでに無線通信路の特性（位置情報や雑音等）を利用した鍵共有方式や暗号化方式等が提案されている．特に，近年，Blochらにより2者間の雑音（無線）通信路を想定したモデルのもとで，事前の情報共有やエンティティ間の相互通信を行わずに（すなわち，一方向通信のみで）秘密鍵を共有できる方式（鍵共有方式）が提案された[3]．一般に，無線通信の特性を利用した鍵共有方式を，実際に物理層の通信に実装することにより，(1) 物理層の通信を利用し共有した秘密鍵を，上位層で行う認証や暗号化処理に利用することで，上位層において改めて公開鍵暗号を用いた鍵共有等を行う必要がなくなるため処理効率が向上する，(2) 上位層で利用していた計算量的安全性に基づく暗号技術の安全性が危殆化したとしても，物理層において情報理論的安全性を確保しているため，全体として一定の安全性を確保できる等，無線通信における可用性や安全性の向上といった効果が期待される．上記のBlochらの提案方式は，2者間での通信のみを想定した方式であったが，実際の無線LAN等の無線通信では，多人数の利用者が同じ無線通信環境を利用して通信を行う形態が一般的である．しかし，この利用形態では，各利用者の回線容量等は通信同士で大きく干渉を受けるため，各通信の安全性を確保しつつ通信が干渉しないように設計することは容易ではないことが知られている．したがって，このような多人数の利用者を想定したより現実的なモデルのもとでBlochらの方式と同等の安全性を実現できる方式の検討等が課題として挙げられる．

今後も，無線通信技術はその利便性から我々の生活には欠かせない重要な技術として広く普及していくと考えられ，同通信における信頼性と安全性の確保は重要な課題である．そして，物理層セキュリティに基づく暗号技術は，このような課題を解決するための有用な技術の１つとして，今後も研究が進められていくであろう．

まとめ

本稿では，情報理論的暗号技術の中でも，最も基礎的な技術である暗号化・認証技術を解説した．現在，このほかにも，さまざまな用途や状況に応えられる多種多様な情報理論的暗号技術が研究発表されている．また，実用化に向け，若干，安全性を弱めることで鍵サイズの削減を行う研究にも触れ，応用例として，物理層セキュリティを紹介した．

情報理論的安全性は，計算モデルや攻撃者の持つ計算資源に依存せずに安全性を保証できるほどの強い安全性であるが，それを実用的に実現するためには，それを支える理論研究とその内容を実現する工学的技術が必要である．また，将来的には，計算量的安全性の危殆化問題や量子計算機の登場等のため，計算量的安全性を持つシステムから情報理論的安全性を持つシステムに移行することも考えられる．その場合，その移行メカニズムを研究開発しておくことも重要である．

Shannon の論文[10] から今日まで，多くの理論研究者の努力により，情報理論的暗号理論は発展し，多くの興味深い成果が発表されてきた．筆者は，本研究分野がさらに発展し，今後の情報社会において，その応用がさらに広がることに期待したい．

謝辞　本稿を執筆するにあたり，貴重なご意見をいただきました日本銀行金融研究所の清藤武暢氏に感謝いたします．

参考文献

1) Alimomeni, M. and Safavi-Naini, R. : Guessing Secrecy, ICITS2012, LNCS 7412, pp.1-13, Springer (2012).
2) Bennett, C. H. and Brassard, G. : Quantum Cryptography : Public Key Distribution and Coin Tossing, IEEE International Conference on Computers Systems and Signal Processing, pp.175-179 (1984).
3) Bloch, M., Barros, J., Rodrigues, R. D. M., McLaughlin, S. W. : Wireless Information-theoretic Security, IEEE Trans. on Information Theory, Vol.54, No.6, pp.2515-2534 (2008).
4) Diffie, W. and Hellman, M. : New Directions in Cryptography, IEEE Trans. Information Theory, Vol.22, No.6, pp.644-654 (1976).
5) Gilbert, E. N., MacWilliams, F. J. and Sloane, N. J. A. : Codeswhich Detect Deception, Bell System Technical Journal53, pp.405-414 (1974).
6) Iwamoto, M. and Shikata, J. : Information-theoretic Security for Encryption based on Conditional Rényi Entropies, ICITS2013, LNCS, Springer, 2013. (To appear) The Full Version is Available at : http://eprint.iacr.org/2013/440
7) Maurer, U. : Conditionally-perfect Secrecy and a Provably-secure Randomized Cipher. J. Cryptology, Vol.5, No.1, pp.53-66 (1992).
8) Russell, A. and Wang, H.: How to Fool an Unbounded Adversary with a Short Key, Advances in Cryptology -EUROCRYPT'02, LNCS 2332, pp.133-148, Springer (2002).
9) Shannon, C. E. : A Mathematical Theory of Communication, Bell System Technical Journal 27, pp.379-423, pp.623-656 (1948).
10) Shannon, C. E. : Communication Theory of Secrecy Systems, Bell System Technical Journal 28, pp.656-715 (1949).
11) Simmons, G. J. : Authentication Theory/Coding Theory, Advances in Cryptology - CRYPTO '84, LNCS 196, pp.411-431, Springer (1985).
12) Wyner, A. D. : The Wire-tap Channel, Bell System Technical Journal 54, pp.1355-1387 (1975).

(2013 年 8 月 4 日受付)

⇨**四方順司**（正会員）　shikata@ynu.ac.jp

京都大学理学部数学科卒業．同大学院理学研究科数学・数理解析専攻修士課程修了，大阪大学大学院理学研究科数学専攻博士課程修了．博士（理学）．その後，東京大学研究員，横浜国立大学講師，助教授を経て，現在，横浜国立大学大学院環境情報研究院准教授．2008 ～ 09 年，スイス連邦工科大学（ETH Zurich）客員研究員．専門は，暗号理論，情報理論，理論計算機科学，計算数論等の分野．これまで，第 19 回電気通信普及財団賞（テレコムシステム技術賞），2006 年度英国計算機学会 Wilkes Award，平成 22 年度科学技術分野の文部科学大臣表彰・若手科学者賞等を受賞．

⇨**渡邉洋平**（学生会員）　watanabe-yohei-xs@ynu.jp

横浜国立大学工学部電子情報工学科卒業，同大学院環境情報学府情報メディア環境学専攻博士課程前期修了．2013 年 4 月より，日本学術振興会特別研究員（DC1）として，同博士課程後期在学．専門は，暗号理論，特に，情報理論的暗号理論．