暗号化鍵の寿命について†

岡本栄司†† 中村勝洋††

暗号システムにおいて，暗号化鍵はシステム全体の安全性の要であり，暗号化鍵の保護には十分な注意が必要である．長い間同一の鍵を使用していると，悪意の第三者に知られる可能性が高くなる．このため，暗号化鍵は時々変える必要がでてくる．そこで，データを暗号化する鍵（ワーク鍵）を随時変更し，別の上位の鍵（鍵暗号化鍵）で暗号化して相手に送る方法が用いられている．さらにこの鍵暗号化鍵を多段階層にすることもある．しかしながら，これらの暗号化鍵，特に最上位の鍵（マスタ鍵）の変更をどの程度に行うべきかに関する「鍵の変更周期」あるいは「鍵の寿命」については，まだ議論が少ない．これでは，実際に暗号システムを導入する際，運用上不安が残る．そこで，本論文ではアメリカ標準暗号 DES を想定して，暗号化鍵（ワーク鍵，マスタ鍵）の変更周期を調べた．解読方法には，例として最も単純な全鍵探索法（Exhaustive Key Search）を用いた．この結果，マスタ鍵は毎年，ワーク鍵はメッセージごとあるいはセッションごとに変更したほうが良いことがわかった．なお，本論文で示した考えは，暗号アルゴリズムと解読法を変えても基本的に適用できるものである．また本結果は，最も単純な解読法を仮定しているため，一般に守るべき最低基準を示していると考えられる．

1. はじめに

近年，社会の情報化，ネットワーク化が急激に進みつつある．これに伴って電話の盗聴，プライバシーの侵害あるいはコンピュータウィルスなどのコンピュータ犯罪，情報犯罪が増加している．これらの脅威から社会を守るために，技術的，制度的あるいは社会的な面から様々な努力が各機関で払われている．技術的対策に限っても多くの方式を用いて安全性の向上がはかられている．このなかで，認証技術と暗号技術は要素技術として重要視されており，既にコンピュータシステムや通信システムに良く使用されている．

現代の暗号や認証においては暗号化鍵をパラメータとして用いており，この暗号化鍵を安全に保管すればシステム全体の安全性が保たれるように設計されている．逆に言えば，暗号化鍵がシステムの安全性の要となっており，暗号化鍵の保護には十分な注意が必要である．

一つの暗号化鍵を長い間使用していると，何らかの手段で悪意の第三者に知られる可能性が高くなる．このため，暗号化鍵は時々変える必要がでてくる．ただし，毎回マニュアルで変更していては運用が大変である．そこで，データを暗号化する鍵（ワーク鍵）を随時変更し，別の上位の鍵（鍵暗号化鍵）で暗号化して相手に送る方法が用いられている．さらにこの鍵暗号化鍵を多段階層にすることもある．しかしながら，これらの暗号化鍵，特にマニュアルで変えることの多い最上位の鍵（マスタ鍵）の変更をどの程度に行うべきかに関する「鍵の変更周期」あるいは「鍵の寿命」については，一部のアタックに対して筆者らが発表しているが十分とはいえない[1),2)]．これでは，実際に暗号システムを導入する際，運用上不安が残る．

そこで本論文ではアメリカ標準暗号 DES[3)] を想定して，暗号化鍵（ワーク鍵，マスタ鍵）の変更周期を調べる．鍵階層は SNA (System Network Architecture)[4)] などで最も良く用いられている2階層を中心に議論する（3階層以上でも同様の議論が成立する）．また暗号アルゴリズム解読法には，例として最も単純な全鍵探索法（Exhaustive Key Search）を用いた．

なお，本論文で示した考えは，暗号アルゴリズムとその解読法を変えても基本的に適用できるものである．また本結果は，最も単純な解読法を仮定しているため，一般に守るべき最低基準を示していると考えられる．

2. 暗号化鍵配送機構とアタック法

2.1 暗号化鍵配送機構

一般化した暗号化鍵配送機構を**図1**に示す．暗号化鍵は図に示すように階層化されている．階層レベル数を L とする．実際のデータを暗号化する鍵をデータ暗号化鍵あるいはワーク鍵といい K_1 または KW と表す．鍵 K_{i-1} を配送するためにその鍵をさらに暗号化する鍵を鍵暗号化鍵といい，K_i とおく．ここで，

† Lifetimes of Cryptographic Keys by EIJI OKAMOTO and KATSUHIRO NAKAMURA (C&C Information Technology Research Laboratories, NEC Corporation).

†† 日本電気(株)C&C 情報研究所

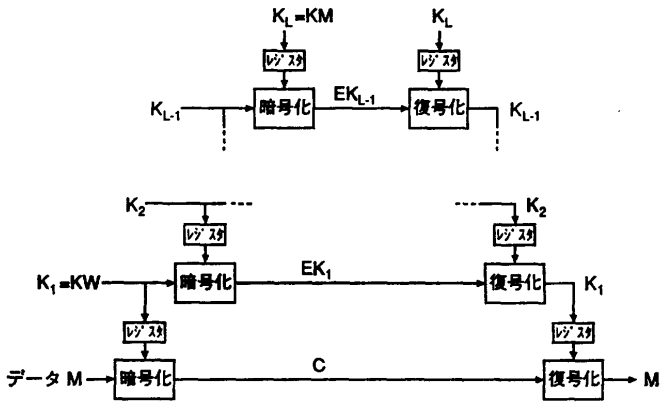

図 1 暗号化鍵配送機構
Fig. 1 Key distribution scheme.

暗号化鍵 K_{i-1} を一つ上位の暗号化鍵 K_i で暗号化したビットパターンを EK_{i-1} で表す．この EK_{i-1} は解読者も知り得るビットパターンである．最上位レベルの鍵暗号化鍵をマスタ鍵といい，K_L または KM と表す．マスタ鍵は自動配送されず，何らかの手段で暗号化側と復号化側でセットされる．暗号化鍵はすべて乱数から生成される．

本論文では，鍵 K による X の暗号化変換を $E(K, X)$，鍵 K による Y の復号化変換を $D(K, Y)$ で表す．

2.2 解 読 法

解読者は，図1の暗号化側から復号化側に送られる全情報 EK_i $(i=1,2,\cdots,L-1)$ と C を持っており，さらに解読者は元データを部分的に持っているか，または元データに冗長性があると仮定する．

アタック法として，2種類取り上げる．

1) 下降的アタック

マスタ鍵の候補を選び，それが実際に使われているか否かを下位レベルの暗号データの情報から判断する．暗号アルゴリズムの解読を全鍵探索法（虱潰し法）に限るとすればこの下降的アタックは有効である．

下降的アタック法

S1) マスタ鍵候補を一つ選び K_L' とする．

S2) $K_{i-1}'=D(K_i', EK_{i-1})$ とする（ただし，$i=L, L-1, \cdots, 2$）．

S3) $M'=D(K_1', C)$ が元データか，正しい冗長性を持っているなら，終了．さもなければ S1 へ．

終了したときの K_i' $(i=1,2,\cdots,L)$ は実際に使われている暗号化鍵であり，特にマスタ鍵は K_L' である．

2) 上昇的アタック

上昇的アタックは下位のレベルの鍵から順次上位レベルの鍵を見いだしてゆく方法である[1,2]．暗号アルゴリズムの解読が虱潰しよりもかなり効率的な場合は有効な方法である．例えば，既知平文攻撃（いくつかの平文と対応する暗号文対がわかっているとき，鍵を求める）に弱い暗号アルゴリズムでも現実には用いられるが，これに対しては極めて有効である．

上昇的アタック法

S0) 平文 M と暗号文 C から，あるいは平文 M の冗長性と暗号文 C から，K_1 を求める．

S1) K_1 と EK_1 から，K_2 を求める．

⋮

SL) K_{L-1} と EK_{L-1} から，K_L を求める．

このアルゴリズムにより，全暗号化鍵 K_i $(i=1,2,\cdots,L)$ が求められる．

暗号アルゴリズム自身の解読法としては，本論文では最も単純な全鍵探索法（虱潰し法）を採用する．したがって，アタックには上記の下降的アタックが適している．しかし，現実には解読は虱潰し的には行われず，もっと有効な方法が用いられるので，上昇的アタックも重要である．そこで本文では，暗号アルゴリズム解読は虱潰し法ながら，下降的アタック，上昇的アタック共に採用して，暗号化鍵の寿命を計算してみる．

2.3 解 読 率

解読に関する評価として，解読率を「データが解読されている時間の割合」と定義する．

$$\text{解読率 } \varepsilon = (\text{ある時間 } T \text{ 内にデータが解読されている平均時間})/T \qquad (1)$$

解読率は後に示すように，暗号化鍵を頻繁に変更するほど小さくなる．したがって，解読率と鍵の寿命にはトレードオフの関係がある．用途に応じて許容できる解読率が定まり，そこから暗号化鍵の寿命が定まる．

3. 暗号化鍵寿命

ここでは，鍵の変更周期 T を解読率 ε と暗号化鍵の階層数 L の関数で与える．結果は下降的アタックと上昇的アタックで大きく異なる．

3.1 下降的アタックによる解読率と鍵寿命

1) 解読率の計算

すべての暗号化鍵は最初にセットされ，時刻0から

暗号システムが稼働開始したとする．そして，マスタ鍵 K_L は時刻 T_L で変更されるものとする．

さて，マスタ鍵 K_L は，確率的にある時刻で解読されるとして，その解読時刻を t_L とする．t_L は確率変数である．解読試行は，マスタ鍵が変更される時点まで行われ，変更後は新しい鍵に対する鍵探索が行われるものとする．

マスタ鍵 K_L が解読される確率密度 $p(t)$ は一様と仮定する．このとき，一つのマスタ鍵候補の真偽を判定するのに，下降的アタック法で示したように，L 回の復号を必要とする．したがって，1回の復号時間を A とすると，一つのマスタ鍵候補に対して，真偽判定に LA 時間要する．鍵の個数を N とすると，すべてのマスタ鍵を検査するのに NLA 時間かかることになる．ここで，マスタ鍵の変更時刻 T_L は NLA よりも大きくては意味がないので，

$$T_L < NLA$$

とする．

以上により，マスタ鍵の解読確率密度 $p(t)$ は

$$p(t)=\begin{cases}1/(NLA); & 0\leqq t\leqq NLA\\ 0 & ;\text{それ以外}\end{cases} \quad (2)$$

で与えられる．

暗号化鍵数 N は，例えば DES の場合は，$N=2^{56}$ となる．

時刻 t_L にマスタ鍵が解読されたとすると，t_L から T_L までは，元データは読まれていることになる．したがって，平均解読時間は

$$E[T_L-t_L]=\int_0^{T_L} p(t_L)\cdot(T_L-t_L)dt_L$$
$$=T_L^2/(2NLA) \quad (3)$$

で与えられ，解読率は

$$\varepsilon=E[T_L-t_L]/T_L=T_L/(2NLA)$$
$$=c_L/(2L) \quad (4)$$

となる．ここで，一般に c_i $(i=1,2,\cdots,L)$ は

$$c_i=T_i/(NA) \quad (5)$$

であり，レベル i の暗号化鍵 K_i の正規化鍵寿命あるいは正規化鍵変更周期と呼ぶ．

2) 正規化マスタ鍵寿命

上式(4)により，正規化マスタ鍵寿命は次式で与えられる．

$$c_L=2L\cdot\varepsilon \quad (6)$$

図2は，階層数 L をパラメータとして，解読率 ε と正規分マスタ鍵寿命 c_L の関係を図示したグラフである．マスタ鍵を頻繁に換えるほど解読率も小さくなる．

3) 2階層配送システムにおけるマスタ鍵寿命

実際に良く用いられている2階鍵配送システムにおけるマスタ鍵の寿命を式(6)から試算してみる．DES を想定して，$A=10^{-6}$，$N=2^{56}$ とし，解読率を例えば 10^{-4}（1年のうちで，約1時間解読されている程度）とすると，マスタ鍵寿命は0.9年となる．すなわち，0.9年に一度はマスタ鍵を変更すべきことがわかる．暗号アルゴリズム解読法として，最も効率の悪い全鍵総当たりを想定しているので，この変更周期は最低限を示していると考えられる．

3.2 上昇的アタックによる解読率と鍵寿命

1) 解読率の計算

下位レベルの暗号化鍵から順番に解読して，最後にマスタ鍵を見いだす上昇的アタック法を用いたときの解読率を計算する．すべての暗号化鍵は最初にセットされ，時刻0から暗号システムが稼働開始したとする．

レベル j の鍵 K_j の変更周期を T_j とし，その鍵 K_j が解読された時刻を t_j とする．このときデータが解読されている時間は，**図3**に示すように，時刻 t_j から T_j となる．ここで，t_j は確率変数であり，その確率密度関数 $q(t_j)$ は

$$q(t_j)=\begin{cases}0 & ;t_j<0,\ t_j>NA\\ 1/NA & ;0\leqq t_j\leqq NA\end{cases} \quad (7)$$

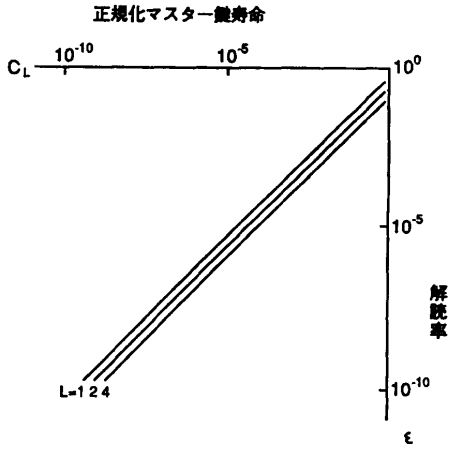

図2 マスタ鍵寿命（下降的アタックに対して）
Fig. 2 Lifetime of master key.

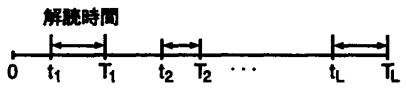

図3 解読時間分布
Fig. 3 Distribution of t_i and T_i.

で与えられる．

データが解読されている時間平均の割合，すなわち解読率 ε は，したがって，

$$\varepsilon=\{E[I(T_1-t_1)] +E[I(T_2-t_2)]-E[I(T_1-t_2)] +\cdots +E[I(T_L-t_L)]-E[I(T_{L-1}-t_L)]\}/T_L \tag{8}$$

となる．ここで，E は期待値を示し，I は

$$I(t)=\begin{cases}t; & t\geqq 0\\ 0; & t<0\end{cases} \tag{9}$$

を表す．式(8)の負項は，図3における矢印部分が重なった場合の重なり部分である．ここで，NA は大きいという仮定：

$$T_i<NA \tag{10}$$

とおくと，$E[I(T-t_i)]$ は

$$\begin{aligned}&E[I(T-t_i)]\\ &=\int_0^T q(t_1)dt_1\int_{t_1}^T q(t_2-t_1)dt_2\cdots\\ &\int_{t_{i-1}}^T q(t_i-t_{i-1})(T-t_i)dt_i\\ &=1/(NA)^i\cdot\int_0^{\min(T,NA)}dt_1\int_{t_1}^{\min(T,t_1+NA)}dt_2\\ &\cdots\int_{t_{i-1}}^{\min(T,t_{i-1}+NA)}(T-t_i)dt_i\\ &=1/(NA)^i\cdot\int_0^T dt_1\int_{t_1}^T dt_2\cdots\int_{t_{i-1}}^T(T-t_i)dt_i\\ &=1/(NA)^i\cdot\int_0^T dx_1\int_0^{X_1}dx_2\cdots\int_0^{X_{i-1}}x_i dx_i\\ &=T^{i+1}/\{(i+1)!(NA)^i\}\end{aligned} \tag{11}$$

となる．ここで，積分変数を $x_i=T-t_i$ と変更した．上式を用いれば，式(8)は次式で表される．

$$\varepsilon=\left\{\sum_{i=1}^{L}(c_i{}^{i+1}-c_{i-1}{}^{i+1})/(i+1)!\right\}/c_L \tag{12}$$

ただし

$$\begin{aligned}&c_i=T_i/(NA)<1\\ &c_0=0\end{aligned} \tag{5}$$

である．

上式(12)が，上昇的アタックを用いたときの解読率と全レベルの鍵変更周期（寿命）の関係を示す式である．

2) 正規化マスタ鍵寿命 c_L の最大値

マスタ鍵はマニュアル的に変更しなければならないので，マスタ鍵の寿命はできるだけ長いほうが運用しやすい．そこで，解読率 ε を定数とみなしたとき，マスタ鍵の寿命 c_L の最大値を求める．

式(12)を変形すると，次のようになる．

$$c_L{}^{L+1}/(L+1)!-\varepsilon\, c_L =-\sum_{i=2}^{L}c_{i-1}{}^i/i!\cdot\{1-c_{i-1}/(i+1)\} \tag{13}$$

この式の左辺は，c_L が

$$0\leqq c_L\leqq\{(L+1)!\cdot\varepsilon\}^{1/L} \tag{14}$$

の範囲ならば非正であり，それより大きくなると，正になる．一方，正規化鍵寿命は式(10)より1以下なので，式(13)の右辺は非正である．したがって c_L は不等式(14)の範囲でなければならない．すなわち，

$$\max c_L=\{(L+1)!\cdot\varepsilon\}^{1/L} \tag{15}$$

である．なお，c_L が最大のとき，式(13)の左辺は0であり，一方，同式の右辺が0になるのは，$c_1=c_2=\cdots=c_{L-1}=0$ のときそのときに限る(同式の右辺の各項はすべて非正である)．したがって，c_L の最大値は $c_1=c_2=\cdots=c_{L-1}=0$ のときに達成される．実際には，c_i は正であるが，式(13)の右辺は $c_i=0$ での偏微分が0なので，c_i が小さければ，c_L はほぼ最大値と考えられる．

最大 c_L と解読率 ε の関係を，レベル数 L をパラメータとして，図4に示す．鍵を頻繁に変えるほど解読率は小さくなる．また，レベル数 L を大きくする効果は，L が小さいときが顕著である．

3) 2階層配送システムにおける鍵寿命

一般に用いられている場合にあわせて，以下，鍵階層数 L を2とする．

式(12)は

$$\varepsilon=c_1{}^2/(2c_2)+(c_2{}^3-c_1{}^3)/(6c_2) \tag{16}$$

となる．解読率 ε をパラメータとして，c_1 と c_2 の関係を図5に示す．

この図からも，c_1 が小さければ c_2 は最大値

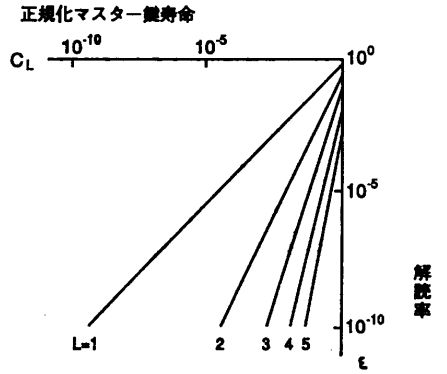

図4 マスタ鍵寿命（上昇的アタックに対して）
Fig. 4 Lifetime of master key.

$$\max c_2=(6\varepsilon)^{1/2} \quad (17)$$

に近いことがわかる．運用上は，c_2 が最大値付近で，c_1 もできるだけ大きくしたほうがよい．図から目視で判断すると，c_1 がグラフ上×を結んだ線より小さければ，c_2 はほぼ一定（最大値）と見なせる．その線を境界とする領域は

$$\log(c_1)-\log 10^{-1}\leqq 1.5(\log(c_2)-\log(6\cdot 10^{-1})^{1/2}) \quad (18)$$

となる．したがって，マスタ鍵寿命 c_2 が最大値に近いという条件のもとでのワーク鍵寿命 c_1 の最大値は，式(17)を式(18)に代入して，次式で与えられる．

$$\max c_1=0.56\varepsilon^{0.75} \text{（実験式）} \quad (19)$$

図6に，式(17)，(19)による最大正規化マスタ鍵寿命 c_2 と最大正規化ワーク鍵寿命 c_1 を示す．

図から，解読率 ε を 10^{-4}（1年のうちで，約1時間解読されている程度）とすると，マスタ鍵は 56 年ごとに変えれば良いが，ワーク鍵は 84 日ごとに変える必要があることがわかる．できることならメッセージごとあるいはセッションごとに変更したほうがよい．この場合変更は自動で行えるので，マニュアル操作は必要なくなるが，これは2階層にしたメリットである．

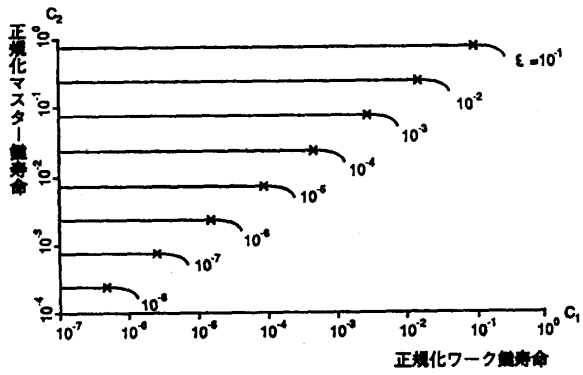

図5 マスタ鍵寿命とワーク鍵寿命の関係（上昇的アタックに対して）
Fig. 5 Relation between c_1 and c_2.

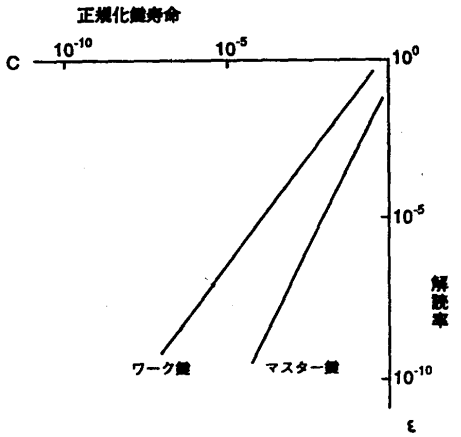

図6 最大鍵寿命（鍵階層数2，上昇的アタックに対して）
Fig. 6 Maximum lifetime of key.

4. おわりに

暗号システムにおいて，暗号化鍵をどの程度の時間間隔で変えれば良いか，という暗号化鍵変更周期すなわち「暗号化鍵寿命」を定義し，ある条件のもとで数量的に考察した．この鍵寿命は解読手法と解読率に大きく依存するので一般的結論は導けないが，最も効率の悪い暗号アルゴリズム解読法を仮定しているので，少なくとも鍵変更に関し守るべき最低限は求められたと考えられる．

運用にあたっては，本論文で示した暗号化鍵寿命の概念を把握しておき，実際の場へ暗号システムを導入する際に適宜修正して，鍵寿命をもとめ，他の運用条件等を勘案して実際の鍵変更周期を定める必要がある．

なお，本論文では，暗号解読法として全鍵探索法を用いているため，解読者にとって上位鍵から攻略する下降的アタックが有利な結果が出ている．しかし，実際には統計量その他の情報を用いて暗号アルゴリズムを解読するので解読者にとって下位鍵から攻略する上昇的アタックが有利な可能性もあることを注意しておく．

参考文献

1) 岡本，中村：暗号キー管理システムにおけるマスターキーの変更周期，第7回情報理論とその応用研究会予稿集，pp. 169-173 (1984).
2) Okamoto, E. and Nakamura, K.: Lifetimes of Keys in Cryptographic Key Management Systems, *Proc. of CRYPTO '85*, pp. 246-259, Springer-Verlag (1985).
3) National Bureau of Standards, Data Encryption Standard, Federal Information Processing Standards Publication No. 46 (1977).
4) Lennon, R. E.: Cryptography Architecture for Information Security, *IBM Syst. J.*, Vol. 17, No. 2, pp. 138-150 (1978).

(平成3年3月 7 日受付)
(平成3年9月 12 日採録)

岡本 栄司（正会員）

昭和48年東京工業大学工学部電子卒業．昭和53年同大大学院博士課程修了．同年日本電気(株)入社．大学院ではグラフ理論的回路網理論を研究．入社後はディジタル無線通信の研究を経て，現在，情報セキュリティの研究に従事．情報数理分野全般に興味を持つ．平成元年情報処理振興事業協会技術センター研究員兼務．平成2年電子情報通信学会論文賞受賞．IEEE シニア会員．電子情報通信学会，情報理論とその応用学会，応用数理学会，システム監査学会，日本セキュリティ・マネジメント学会，IACR 各会員．

中村 勝洋（正会員）

1967年東京大学工学部計数工学科（数理工学コース）卒業．同年日本電気(株)に入社．中央研究所にて，ディジタル通信，特に符号理論・暗号理論・情報セキュリティ関係の研究開発に従事．AI 基礎/生体情報処理/大規模数値・システムシミュレーション等にも興味を持つ．現在，同社 C＆C 情報研究所情報基礎研究部長．1988～89年情報処理学会「アルゴリズム研究会」幹事．IEEE (IT)，電子情報通信学会，情報理論とその応用学会各会員．