Vol.37 No.6　　情 報 処 理　　June 1996

解 説

暗号安全性の最近の動向

3. 社会での暗号技術の取り扱いと Clipper Chip について†

満保雅浩††　岡本栄司††

1. はじめに

我々は今，情報の集積・活用の仕組みに関する大きな変革期に突入しつつある．情報を収集，蓄積，加工，活用する力は，体力，知力などと同様に，「情報力」とでも表現される社会生活を営む上での1つの能力(個人，もしくは，団体が所有している計算機などから派生するものも含む)であり，この仕組みに関する変革は，情報力という権利を誰がどのような形態で保持するのか，もしくは，誰にも保持させないのかという事柄についての新しい大きなうねりである．この変革は，情報の価値に重きを置く社会へのパワーシフトが実際に進んだ場合に，社会全体の構造に強烈な影響を及ぼすまでになると予想される．ジョージ・オウェルは小説「1984」において，双方向スクリーンを通して個人の生活を監視する強力な体制権力(Big Brother)を描いてみせたが，変革の方向付けの仕方によっては，この小説上のできごとが小説でなくなる可能性すらあるのである．よりいっそう高度化した情報通信ネットワークとその上での情報セキュリティ関連技術の利用は，それ程までの潜在的な能力を持ち得ると考えられる．我々は，現在進行し始めているこの変革の現状とその進展によってもたらされる未来の社会像を可能な限り正確に捉え，また同時に，情報収集の対象となる一般の人々の，それらに対する認知度を高めるべきである．そのことを通して，情報力の社会での位置付けを人々が自ら規定していくことができる．

学校や会社の名簿の収集，個人の消費動向調査など，情報の争奪戦は1996年現在までにすでに始まっていると言えるのかもしれない．しかし，現在から近い将来にかけて，もっと組織立った情報の収集が可能となり得るのである．たとえば，1993年4月にアメリカ政府によって発表された Clipper Chip 構想や，近年富に開発が盛んになってきている電子現金(電子貨幣)があげられる．

前者は，電話などの通信機器に暗号機能を有する Chip(Clipper Chip と呼ばれる)をあらかじめ仕掛けておくものである．通常の通信においては，この Chip を用いて暗号通信が行われる．暗号通信に使用される鍵は鍵保管機関に預けられ，捜査機関が犯罪捜査において法の執行上必要と認められる盗聴を行う際に，捜査機関に供出される．暗号が掛けられていない現在の通信では，合法・非合法を問わないならば，盗聴は技術的に可能である．ところが，一般の人，さらには，反社会的な集団が，技術発展にともない生み出される高度で，安価な暗号製品を無秩序に利用し始めたならば，たとえ合法な盗聴であっても実施が困難になると予想される．そこで，鍵供託の施された暗号を用いてネットワークを事前に作り出し，暗号が掛けられたとしても，正当な手続きを経て鍵を入手したならば，情報の復号，収集を可能にしようというものである．このような暗号システムは鍵供託方式，もしくは，鍵供託暗号と呼ばれる．

また，後者は，偽造が困難な形を持つ情報にお金としての価値を持たせ，文字通り電子現金として利用するものである．プライバシー保護の観点から，電子現金では追跡不可能性という性質が大切である．電子現金は，多くの場合，まず，ユーザが自分の口座からお金を引き落とし，対応する電子現金を入手する．そして，購入にともない商店に払い込みをし，最後に，商店が入手した電子現金を銀行に提示し，相当するお金を自己の口座に振り込んでもらう．電子現金が追跡不可能性を

† On the Treatment of Cryptographic Techniques in the Society and Clipper Chip by Masahiro MAMBO, Eiji OKAMOTO (School of Information Science , Japan Advanced Institute of Science and Technology).

†† 北陸先端科学技術大学院大学情報科学研究科

有する場合，銀行は引き落とされた電子現金の払い込み先を特定できない．プライバシー保護には理想的といえるこの性質は，逆に，ギャングによるマネーロンダリングや，誘拐の身代金として悪用される恐れがあった．そこで，鍵供託暗号と同様に，鍵供託機能を設けることにより，捜査機関が電子現金の使用者を特定できるような方式も考え出されている．電子現金は，単に暗号技術の一応用としての位置付けがあるだけでなく，流通形態の変化など，経済活動にまで及ぶ社会的にも大変重要な技術といえる．日常生活に密接するこの技術に個人を特定する機能を付加することは，鍵供託暗号とともに，情報力を強化する社会基盤を新たに導入することにつながる．

両者において注意が必要なのは，鍵を入手できる特定の人だけが復号，もしくは，対応付けを行えるという点であり，この性質が情報力の集中を促進する．鍵供託はアメリカ政府が導入を切望しているものであるが，国家という単位でなく，企業といった団体内において鍵供託暗号を利用することも考えられる．導入の利点として，社員が暗号用の鍵を紛失した際に予備の鍵として働くこと，管理職が一般社員の仕事の進捗状況をいつでも確認できる環境を提供することなどがあげられる．また，電子現金においても，捜査機関だけが追跡を許されるのではなく，他の団体，個人が追跡することもあり得るのではないだろうか．たとえば，会計監査が考えられる．現在のところ電子現金は主に小額の決裁に活用されると見なされているが，技術が進み，電子貨幣による決裁が企業間決裁の主流を占めるようになれば，会計監査委員が監査上必要と判断するお金の流れを追跡することも考えられよう．また，独立採算制を採用している企業内で，監査役のセクションが個々の部局の採算をチェックすることも考えられる．庶民の生活レベルで言えば，子供に与えた電子現金の使用動向調査を，養育義務のある親が行えた方が，時として，望ましいことはなかろうか．消費動向調査を専門とする信頼のおける業者に，支障をきたさないと判断される電子現金の追跡を行わせるといった状況も想定できよう．

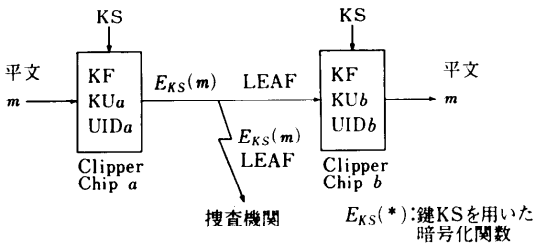
鍵供託暗号，電子現金以外にも，超流通という概念に代表される情報の新しい流通の仕組みも新たな情報力を生み出すことになると考えられる．超流通では，ソフトウェアの使用に対して課金が行われる．このため，ソフトウェアごとの使用回数，使用時間といった非常に細かい情報の管理が行われることになる．電話や電子現金における鍵供託機能導入の理由は元来，犯罪防止であり，その意味において，鍵供託を運用した際に，行政や裁判所などが介在する．一方，超流通は，商業上の理由により導入が検討されているため，行政や裁判所が必然的に介在するわけではない．このため，超流通を通して集められた情報を握るか否かは，ビジネスを進める上で大きな差異を生み出す．無論，暗号技術などを応用して個人のプライバシーを保護しながら，課金する方式も検討されている．ダイレクトメールを便利だと思う人もいれば，迷惑だと思う人もいるため，超流通を通して得られる詳細な個人情報も，情報収集者と個人の両方が利益を享受できるような活用方法を模索すべきである．その際，最終的に，ユーザが納得する形態をとることが望ましいのは言うまでもないことである．

上記の各技術は，個人にとって，プライバシーを守る，利益を守る，効率化を図る，便利さを提供するなどのプラス面があると同時に，その逆の，個人のプライバシーを侵害する，(目に見えない形で)利益を剥奪する，システム利用を回避した場合に非効率，かつ，不便な状況を強いるといったマイナス面も内包しているのである．

このように，各個人が納得して生活できる情報社会環境を構築していく上で，我々が直面している技術の現状を把握することは大変重要である．今から始めるのならば，十分議論が尽くされた上で，社会における情報力の取り扱い方を規定できるであろう．本稿では，Clipper に焦点を当て，そこで用いられている暗号技術の安全性について解説する．また，Clipper に纏わる話題についても議論する．

2. Clipper Chip とは

1993 年のクリントン大統領による構想発表を受けて，1994 年 2 月には供託暗号化標準(Escrowed Encryption Standard, EES)[1]が発表された．文献 1)によれば，Escrow とは「第三者に預けられ，条件が成立した場合のみに，第三者から受け手に渡されるもの(証書や暗号鍵など)」



図－1 Clipper Chip を用いた鍵供託暗号

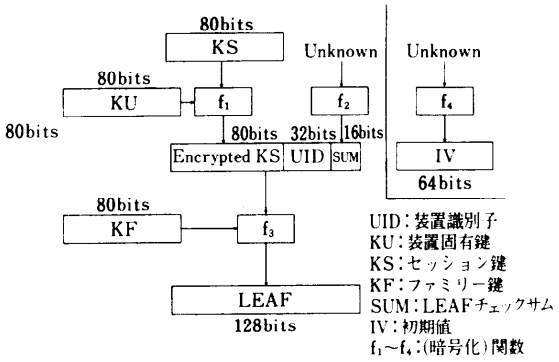
のことを意味する．

EES を導入する理由は，ディジタル通信への移行と，高性能で安価なディジタル暗号装置の普及により，捜査機関が解読不可能となるような暗号通信を犯罪組織が行う可能性が出てきたことによる．鍵供託機能をすべての通信機器に導入し，Clipper Chip で用いられる Skipjack と呼ばれる暗号以外の使用を法律でいっさい禁止することにより，盗聴を滞りなく遂行が可能になると期待したのである．

本章以降では，供託暗号化標準に基づく開発中間段階の方式(Interim System)について解説を行う．Interim System としては，Clipper Chip を利用したもの以外にも，Fortezza(元来 Tessera と呼ばれていた)という PCMCIA card に Capstone Chip を載せたものがある．Capstone Chip は Clipper Chip の機能に加えて，鍵配送のアルゴリズム(Key Exchange Algorithm, KEA)，ディジタル署名のアルゴリズム(Digital Signature Algorithm, DSA)，ハッシュ関数のアルゴリズム(Secure Hashing Algorithm, SHA)，高速冪乗計算アルゴリズムや乱数発生器を内蔵し，エレクトロニック・コマースなどへの応用を目指したものである．アメリカの Defence Messaging System における Mosaic 上の Email の暗号化にも採用が検討されている．このような違いがあるものの，鍵供託の基本は Clipper Chip における方式にある．

2.1 Clipper の動作原理

図－1 に Clipper Chip を用いた鍵供託暗号の概観を示す．Clipper Chip の動作には 2 つの段階がある．メッセージの暗号化に用いられるセッション鍵 *KS*(Session Key)が入力され，初期値 *IV*(Initial Value)が送受信装置間で共有される段階と，*KS* と *IV* を用いてメッセージの暗号化，復号化が行われる段階である．*KS* は公開鍵配送法などにより共有される．*IV* は送受信装置間の一方で生成され(図－1)，他方に送られる．



図－2 LEAF の生成法

暗号化された送信メッセージ $E_{KS}(m)$ には LEAF(Law Enforcement Access Field)が付加されている．この LEAF には暗号化に用いられた *KS* 自体が暗号化されて格納されており，捜査機関(FBI)は *KS* の復号化に必要な鍵を鍵保管機関から入手することにより，法の執行上必要な盗聴を実行できる．正しい LEAF が付加されていない場合，盗聴に支障をきたす．このため，受信側の装置は，正しい LEAF が付加されていないと動作しないように設計されている．

2.2 LEAF の生成法

LEAF は図－2 のように生成される．LEAF の偽造を防ぐため，公開されていない個所がいくつかある．関数 f_1 ～ f_4 や，f_2 と f_4 の入力値などである．*KS* は装置個別鍵 *KU*(Device Unique Key)により暗号化された後に，装置識別子 *UID*(Device Unique Identifier)と LEAF チェックサム *SUM* とともにファミリー鍵 *KF*(Family Key)により暗号化される．生成された LEAF の長さは 128 ビットとなる．*KF* はすべての Clipper Chip に共通の値であり，*KU* は Clipper Chip ごとに異なる．捜査機関は LEAF より入手した *UID* を鍵保管機関に渡し，鍵保管機関は *UID* に対応する *KU* を取り出し，捜査機関に渡す．LEAF の正当性の確認は，16 ビットの *SUM* を検査することにより実行される．

2.3 供託鍵と Clipper Chip の製造法

LEAF の中に格納される情報と，捜査機関が鍵保管機関から入手するセッション鍵復号用の情報

は対応付けがなされていなければならない．このため，LEAF生成に用いられるClipper Chip内の情報*KF*, *UID*, *KU*と，鍵保管機関が保管する情報は図－3に示されるように決定される．鍵保管機関であるEscrow Agentには，NIST (National Institute of Standards and Technology) と国税庁が指定されており，各々が生成，保持する情報が揃って初めて，Clipper Chipの生成，もしくは，*KS*のLEAFからの摘出が行えるように設計されている．たとえば，Escrow Agent iは乱数の種RS_i(Random Seed)，任意の入力AI_i(Arbitrary Input)，*KCK*の要素KN_i(Key Number)，*KF*の要素KFC_i(Family Key Component)を個別に生成し，製造装置に入力する．その後，KN_iはEscrow Agent iに保管され，KFC_iはファミリー鍵保管機関に保管される．f_5は疑似乱数発生用の関数，f_6は*UID*生成用の関数，f_7は暗号化関数であり，その処理は公開されていない．

*KS*の暗号化に利用される*KU*はKC_1とKC_2(Key Component)に分解された後に，KN_1とKN_2から生成される*KCK*を鍵とするf_7により暗号化される．その出力EKC_iは，任意の入力AN(Arbitrary Number)を入力値とするf_6の出力*UID*とともにEscrow Agent iに渡される．Escrow Agent iは先に生成したAI_i, RS_i, KN_iとともに*UID*, EKC_iを保管する．保管にあたり，これらの値は暗号化され，その暗号化鍵をEscrow Agentの2名の職員が，分割し，それぞれ分散して管理するといった配慮がなされる．さらに，これらの保管情報が納められるディスクは，包装され，開封された場合に，その事実が後日分かるようになっている．一方，生成された*KF*, *UID*, *KU*はClipper Chipの中に格納される．

2.4 (合法な)盗聴の手順

誘拐，テロなどの強悪な犯罪に対抗する手段として盗聴を行う場合，捜査機関は，まず，裁判所に盗聴の許可を申請する．裁判所が合法と認め，許可を出した段階で，捜査機関はファミリー鍵保管機関に連絡し，ファミリー鍵保管機関はKFC_iを格納したディスクを復号用装置に挿入する．*KF*は復号用装置内で再構成された後に，LEAFの復号に用いられる．そして，復号された情報の中から，*UID*が装置のディスプレイに表示される．

捜査機関は*UID*と裁判所の捜査許可証をEscrow Agent iに提示し，*UID*に対応するKN_iとEKC_iを入手する．KN_i, EKC_iを入力された復号用装置は，$KCK(=KN_1 \oplus KN_2)$を復元する．そして，生成された鍵*KCK*によりEKC_iを復号化してKC_iを取り出し，$KU(=KC_1 \oplus KC_2)$を計算する．

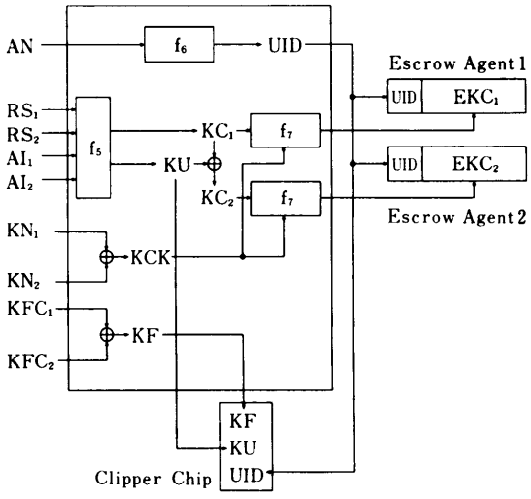
*KU*が求められた段階で，対応するClipper Chip間で通信される暗号文を復号用装置によって復号化することが可能となる．まず，*KF*, *KU*を用いてLEAFより*KS*を計算する．この際，LEAF中のチェックサム*SUM*が正しいことが確認される．正しい場合にのみ，*KS*を鍵として送信メッセージ$E_{KS}(m)$の復号化処理が実行される．そして，平文mが得られ，盗聴が成功する．

3. 安全性について

2. に示したEESの安全性についていくつかの解析がなされている[2)-5)]．

3.1 Skipjackについて

鍵供託暗号化標準に採用されている暗号はSkipjackと呼ばれる．DESが16段構成で，64



AN：任意の数(Arbitrary Number)
RS：乱数の種(Random Seed)
AI_1：任意の入力(Arbitrary Input)
KN_1：KCKの要素(Key Number)
KFG：KFの要素(Family Key Component)
KC_1：KUの要素(Key Component)
EKC_1：暗号化されたKC_1
KCK：KG暗号化用の鍵
(Key Component Enciphering Key)
f_5～f_7：関数(乱数発生器，暗号化関数)

図－3 供託鍵とClipper Chipの製造法

ビットの鍵(実質56ビット)により64ビットの入力を64ビットの出力に変換するのに対して，Skipjackは32段構成であり，80ビットの鍵により64ビットの入力を64ビットの出力に変換する．DESが提供するECB(Electronic Code Book)，CBC(Cipher Block Chaining)，64ビットOFB(Output FeedBack)，1,8,16,32,64ビットCFB(Cipher FeedBack)のいずれのモードにも対応している．国家安全保障局(National Security Agent, NSA)が設計し，アルゴリズムは非公開となっている．これは，暗号としての強度を高めるためではなく，鍵供託機能を回避されないための措置であるとの説明がなされている[2]．しかしながら，開発を行ったNSAのみが解読に成功するような秘密がSkipjackに隠されているのではないかという疑問が拭いきれないため，一部の暗号の専門家により，Skipjackのアルゴリズムの審査が1993年の上半期に行われた．その結果，安全性を脅かすような欠陥は発見されなかったとの報告がなされている[2]．また，計算コストが3年で1/4の割合で減少した場合に，Skipjackの総当たり攻撃に対する強度が，DESの現在の強度と同程度に落ちるまでに36年かかるとも予測している．

しかし，DESとの強度比較は，あくまで，総当たり攻撃に関するものであり，鍵の長さがDESよりも24ビット長い(DESの実質鍵長は56ビットである)という関係から単純に試算した値である．Skipjack特有の性質を利用した攻撃が存在した場合には，強度が低いこともあり得る．

Skipjackの出力は十分乱数として振る舞うことや，暗号文の平文や鍵との相関関係には顕著な特性が現れなかったとされている．

また，DESにおいて，$DES(k, DES(k, m))=m$ を満たす鍵の存在や($DES(k, m)$は，鍵 k をとるDESで平文 m を暗号化することを示す)，$\overline{DES(k,m)}=DES(\bar{k},\bar{m})$ を満たす鍵の存在(バーはビット反転を表す)などが知られている．このような特殊な性質の存在を調べたが，発見されなかったとされている．

暗号化関数が関数演算に関して閉じていると攻撃に悪用される余地を残す．たとえば関数 SJ において，任意の暗号化鍵 k_2, k_3, k_4 に対して $SJ(k_3, SJ(k_2, m))=SJ(k_1, m)$ や $SJ(k_4, SJ^{-1}(k_3, SJ(k_2, m)))=SJ(k_1, m)$ を満たす k_1 が存在する場合は，トリプルDESなどのように暗号を繰り返し使用したとしても暗号の強度を高められないこととなる．既知平文攻撃に対しても明らかに弱くなる．そこで，暗号化関数は関数演算に関して閉じていないことが望まれる．文献2)では，Skipjackが関数演算に関して閉じているか否か確かめるために，鍵空間の大きさ N を 2^{10}, 2^{16}, 2^{24}, 2^{32}, 2^{40}, 2^{48}, 2^{56} としてCyclic Closure Testを行ったところ，期待されるサイクル長 $\sqrt{\pi N/8}$ に近い値が得られたとされている．ところが，$N=2^{40}$ までの値は誤差も少ないが，$N=2^{48}$, 2^{56} の値にはかなりの隔たりがあり，しかも，これらの大きな N については試行回数が少なく，示されている値の統計値としての信頼性が低い．このため，鍵の長さが，最低40ビットであることしか保証できていない．もし，$N=2^{56}$ において，Cyclic Closure Testが期待される値を導き出したとしても，DESの鍵の長さ56ビットを保証することにしかなっていない．このため，80ビットの内の有効なビット数についてさらなる考察が必要である．

また，文献2)の検査には，差分攻撃に対して安全性を考察したとの記述はあるが，線形攻撃に対する記述はない．線形攻撃は，1993年頃からにわかに注目を集め，秘密鍵暗号に対する現在最も強力な攻撃法と考えられており，検査する必要があろう．

3.2 LEAFの偽造

ランダムに発生したLEAFをClipper Chip内で鍵 KF により復号化すると，復号後の SUM もランダムな値をとると予想される．LEAFの正当性を検査するために設けられた SUM は16ビットしかないため，与えられた KS, IV に対して 2^{16} 個程度のランダムなLEAFを順次検査することにより，受理されるLEAFを偽造できる．KS を用いて生成された暗号文にこの偽造LEAFを付けて送ると，受信側のClipper Chipは正当なLEAFが添付されていると判断し，暗号文の復号を行う．一方，偽造LEAFを受け取った捜査機関は，KS を求めることができない．Tessera PCMCIAカードを用いて実験したところ，約42分で偽造に成功したことが報告されている[3]．よって，この攻撃は，即時性の少ないEmailやファ

ックスなどに有効である．

Tessera カードは Tessera という名前が登録商標であることが判明したために，Fortezza という名前のカードに変更された．上記の偽造に対抗するため，不正な LEAF を数回受け取った場合に停止し，リセットされない限り再動作を行わないといった変更も加えられている．

3.3 LEAF feedback による LEAF の送信回避

送受信者間で使用される KS が決定された段階で，送信側の Clipper Chip は送信すべき LEAF や IV を送らずに暗号文 $E_{KS}(m)$ のみを送信する．受信側の Clipper Chip は，独自に新しい LEAF と IV を生成し，受け取った $E_{KS}(m)$ の復号化にこの LEAF と IV を利用する．この LEAF は，他の Clipper Chip と暗号通信する際に実際に利用されるものであるため，Clipper Chip 自身が受け取ったとしても受理される．このため，LEAF を送らずとも暗号文の復号化が開始され，しかも，捜査機関は盗聴に必要な KS を入手することができない[3]．

しかし，この回避方法では，平文が正しく復号されない恐れがある．なぜなら，LEAF とともに送信されるべき IV は，暗号化アルゴリズム Skipjack にも利用されていると予想されるためである．IV はユーザが外部から設定できないようになっており，受信側の装置は $E_{KS}(m)$ の計算に用いられる IV と異なる値を非常に高い確率で生成するため，Skipjack による復号化が失敗に終るという懸念が残る．そこで，暗号モードごとに復号化が成功するか否かについて検証してみよう．

ECB モードは IV を必要としないため，問題なく復号化される．CBC モードも CFB モードも自己同期型であり，正しく復号されないブロックは最初の 1 ブロックにとどまり，その後のすべてのブロックは正しく復号化される．

OFB モードは自己同期型でなく，異なる IV に対して異なる値が復号化される．そこで，OFB モードを他のモードを用いてシミュレートすることにより復号化を試みる．第 1 の方法として，ECB モードにシフトレジスタとビットごとの排他的論理和演算(xor)を用意し，OFB モードを直接構成してしまう方法である．この際，送信側が利用した IV を送ってもらう必要があり，その IV を ECB モードでの入力文の役割を果たすシフトレジスタ値として設定する．その他に，CFB モードを利用する方法がある．まず，受信側で生成した IV' を用いて 1 ブロック分の暗号文 c_1 を CFB モードにより生成する．その後，送信側で利用され，送られてきた IV に c_1 を xor したもの $(IV \oplus c_1)$ を n ブロック分の 0 の系列の先頭に付加する．その系列を IV' を初期値とする CFB モードの Skipjack を用いて先頭の $IV \oplus c_1$ から順番に復号化する．そして，その出力の 2 ブロック目以降の値を n ブロックの暗号文 $c_{01},\ldots,c_{0n}$ と xor する．以上の処理により，LEAF' を受理させるために設定されていた Clipper Chip 内の初期値 IV' を送信者の利用した IV に交換する処理，および，CFB モードによる OFB モードのシミュレーションが成功する．

以上のように，LEAF feedback 攻撃を用いると，Clipper Chip により暗号化をかけながら，しかも，平文を捜査機関に盗聴されずに通信ができる．しかし，LEAF を送信していない事実が捜査機関に判明する．暗号文 $E_{KS}(m)$ に付加された LEAF を取り去ることは容易であるため，暗号文 $E_{KS}(m)$ のみが LEAF feedback 攻撃を遂行したことの証拠と認められるか否かは定かではないが，捜査機関は逮捕の理由とするかもしれない．よって，捜査機関が不正行為を発見できないような攻撃がより強力な攻撃といえる．そこで，次のような方法が考えられる．送受信両方の Clipper Chip 間で一方向性関数 $h:M \rightarrow M$ (M はメッセージ空間)を用意し，秘密にする．そして，$h(KS)$ を鍵として $LEAF(h(KS))$ をあらかじめ計算しておき，KS を共通鍵として求められる暗号文と $LEAF(KS)$ の内の $LEAF(KS)$ を $LEAF(h(KS))$ に置き換えて送信する．受信側は，LEAF feedback の手法により $LEAF(KS)$ を生成し，$LEAF(h(KS))$ を再び $LEAF(KS)$ に戻して復号化する．鍵供託により求められる $h(KS)$ を鍵と見なして捜査機関が暗号文を復号化しても，意味を持たないランダムな値しか再生できない．結託している Clipper Chip の利用者が乱数を送ったと言い張れば，捜査機関は不正行為を立証できなくなる[4]．$h(\cdot)$ を用いることにより，必要ならば，受信側は $LEAF(h(KS))$ の正当性を確認できる．

3.4 Squeezing 攻撃

他人 A の $LEAF_A$ をユーザ B が自己の $LEAF_B$ として横領し，その他のユーザ C と暗号通信する攻撃である[4]．共通鍵 KS を用いて A と暗号通信を行った B は A が生成した IV_A と $LEAF_A$ を入手する．その後，B は自己で暗号化を行い，暗号文 c_B と $LEAF_B$，IV_B を生成する．$LEAF_B$，IV_B を先に入手した IV_A，$LEAF_A$ と入れ換え，A，B 間で用いられた共通鍵 KS を流用することにより，C との暗号通信を実行する．c_B の生成の際に用いられた IV_B と，復号の際に用いられる IV_A の違いは，LEAF feedback において考察した手法により復号化が成功する．もし，B が多数のユーザと交信する場合，Squeezing 攻撃を利用して，捜査機関に対して他人になり済ましつつ，暗号通信が行える．この攻撃において，他人になり済まして，犯罪に関与する趣旨の会話を行うと，他人を陥れることさえ可能となる．逆に，盗聴記録を証拠として提出された犯罪者は，誰かに LEAF を悪用されたと言い張ることもできる．

3.5 不正の証拠

電話向けの EES 装置に OFB モードだけをサポートするものが多いが，EES 装置が OFB モードで動作している場合に，暗号文 c は平文 m と OFB モードで動作する Skipjack の出力 out の xor($c=m \oplus out$)で計算される．よって，捜査機関が合法な盗聴を実施して，平文 m を入手した段階で，捜査機関は $out(=c \oplus m)$ も計算可能である．このため，任意の平文 m' を用いて，新しい偽造暗号文 $out \oplus m'$ を生成可能である．このことは，逆に言えば，裁判で犯罪の証拠として示される暗号文と平文は，何ら信頼のおけるものではないことになる[5]．

4. おわりに

本稿では，序論において，我々が突入しつつある，情報の集積・活用の機構に関する変革について簡単に解説し，2. 以降その代表例といえる Clipper について焦点を当て，その仕組みを紹介し，安全性について議論した．供託暗号化標準は発表から 2 年程度経過した．その間，Clipper の安全性の議論，改良方式の提案など様々な技術的な研究がなされている．それと並行的に，憲法，政治，経済などの技術以外の分野での議論も盛んである．国家と暗号の係わり合いという視点からの論争も多い．

憲法第 21 条第 2 項に「検閲はこれをしてはならない．通信の秘密は，これを侵してはならない．」と記されている．有線電気通信法には，有線電気通信の秘密の保護として，第九条「有線電気通信の秘密は侵してはならない．」と記されており，第十四条には，「第九条の規定に違反して有線電気通信の秘密を侵した者は，一年以下の懲役あるいは二十万円以下の罰金に処する．」との罰則規定もある．ネットワークへの依存度が高くなるとともに，Clipper に顕著に見られるように，情報セキュリティ関連技術への社会の依存度も高くなると予想される．今後，ここで規定されている「秘密」の指す内容を，様々な角度から考察していく必要もあろう．

冒頭にも述べたように，犯罪からの保護，プライバシーの保護，さらには，便利さの享受と，その逆の待遇を受けることとの兼ね合いを，今後，どの程度のものに設定するかを，「情報力」の所在も含めて，真剣に検討していかなければならない．

参考文献

1) National Institute of Standards and Technology: Escrowed Encryption Standard(EES), Federal Information Processing Standards Publication(FIPS) 185, U.S. Dept. of Commerce(1994).
2) Brickell, E., Denning, D.E., Kent, S.T., Maher, D. and Tuchmann, W.: SKIPJACK Review: Interim Report, Posted to the "sci.crypt" newsgroup on August 1 (1993).
3) Blaze, M.: Protocol Failure in the Escrowed Encryption Standard, Proc. of The 2nd ACM Conf. on Computer and Communications Security, pp. 59-67 (1994).
4) Frankel, Y. and Yung, M.: Escrow Encryption Systems Visited: Attacks, Analysis and Designs, Advances in Cryptology - Crypto '95,Lecture Notes in Computer Science 963, Springer-Verlag, pp. 222-235 (1995).
5) Lomas, M. and Roe, M.: Forging a Clipper Message, Comm. ACM, Vol.37, No.12 (Dec. 1994).

(平成 8 年 1 月 25 日受付)

満保 雅浩（正会員）

昭和64年金沢大学工学部電気・情報工学科卒業．平成2年東京工業大学理工学研究科電気・電子工学専攻修士課程修了．平成5年同博士課程修了．博士（工学）．同年より北陸先端科学技術大学院大学情報科学研究科助手．現在に至る．情報セキュリティの研究に従事．

岡本 栄司（正会員）

昭和25年生．昭和48年東京工業大学工学部電子工学科卒業．昭和53年同大学理工学研究科電子工学専攻博士課程修了．工学博士．同年日本電気（株）中央研究所入社．平成3年より北陸先端科学技術大学院大学情報科学研究科教授．平成5-6年文部省在外研究にてテキサスA & M大学数学科客員教授．グラフ理論，通信理論，数理計画，アルゴリズム，情報セキュリティをはじめとする情報数理工学の教育・研究に従事．平成2年電子情報通信学会論文賞，平成5年本会Best Author賞受賞．著書「暗号理論入門」など．IEEEシニアセキュリティ・マネージンメト学会，システム監査学会，IACR (International Association for Cryptologic Research) 各会員．