2. e-Societyを推進する暗号技術

4. 著作権・個人情報保護と暗号技術

笠原 正雄
大阪学院大学 情報学部
kasahara@utc.osaka-gu.ac.jp

佐々木 良一
東京電機大学 工学部
sasaki@im.dendai.ac.jp

サイバー社会への道

将来のサイバー社会を支える重要なインフラストラクチャはブロードバンドの通信・記憶を可能とする情報システムである．サイバー社会は，この意味でブロードバンド社会でもある．21世紀に入って，我が国においてもブロードバンドへの動きが，以下のように急激に加速されている．

- 一般公衆回線網の高速化
- アナログTV放送のディジタル化
- ケーブルTVの高度化

このようなブロードバンド化とともに，コンテンツの質的向上が歩調を合わせて進められねばならないが，現状ではディジタル衛星放送受信機の普及等は，従来どおりオリンピック開催，ワールドカップ等の大きな行事に依存している．このことは，ハードの充実とともにコンテンツの充実をより強力にはかることがきわめて大切で，国家的重要課題と言っても決して過言ではないことを教えている．

21世紀サイバー社会では，群雄割拠の状況で無数のベンチャー企業的なコンテンツ・プロバイダが競いあうであろう．NHK，民間放送をはじめとした現時点での強力なコンテンツ・プロバイダは，改革の時期であることを強く認識し，単に日本だけでなく，世界に向け国際的に通用する豊かな内容のコンテンツ創出に全精力を傾けて取り組まなければ，ドッグイヤーで進むサイバー社会で生き残ることは難しい．サイバー社会への道は想像を絶するほど険しいことを，私達は強く認識しなければならない．

コンテンツの創出・育成のために

音，映像等のコンテンツが21世紀サイバー社会の主役となることは疑う余地がない．そしてこれらの著作権を保護することが最重要なテーマとなろう．コンテンツの充実をサポートするために著作権を強力に守るという立場から，以下のことが望まれよう．

- 正当なコンテンツが与えられたとき，正当なユーザ端末においてのみ再生可能となること．
- 不正なコンテンツが与えられたとき，正当なユーザ端末では再生不可能となること．

これらの不正を防止するために，以下の手法が広く知られている．

●電子透かし

従来の電子透かしにおいては，その多くがコンテンツに（目立たない程度の）歪みを加えることによって，さまざまな情報を埋め込むという手法をとっている．しかし，周知のように，DVD等あるいは次世代CDとしてのSACD（Super Audio CD）等においては著作権保護のための情報を当該ディスク上に埋め込むことによって，違法な再生等を防止している点が注目される[1)]．

●コピー制御

BSディジタル放送等が対応可能なコンテンツにかかわる著作権保護のために，放送局側からコピー制御情報が放送波とともに送られている．

●電子署名と認証

著作権にかかわる改ざん，なりすまし等はそれぞれ，

コンテンツおよびプロバイダの真正性にかかわるものであり，これを防止する手法としては，電子署名の手法が効果的に適用されよう．なお，電子署名をより有効なものにするために，現在，時刻認証にかかわる問題が火急のこととして取り上げられ，注目されている．この時刻認証が将来のコンテンツ配布の際に，ますます精密化されたかたちで必須となることは火を見るよりも明らかなことである．

著作権保護のための総合的手法の可能性

将来のブロードバンド社会においては，音あるいは映像のコンテンツそのものが非常に多種多様となり，同時に不正なコンテンツを生み出す要因も非常に多岐にわたる．

来たるべきサイバー社会において，コンテンツの健全な創出，育成環境をつくるために，著作権を保護することが，第一に望まれる．このためには汎用性に富みかつ単純明快，しかも強力な手法を編み出すことが希求される．

●ライツマネージメントの新しい手法（K法）

上述の要求に応えるものとして，ライツマネージメントについての新しい手法(K法)を紹介する．

時間t_iにおいて，ストリーミングのかたちで配信されるスクランブルドコンテンツに付加されるヘッダを$K_{S_i}+R_i$とする．ただし，K_{S_i}はデスクランブル用鍵であり，R_iはこの鍵を隠蔽するための乱数である．

ユーザAはヘッダに$K_{S_i}+R_i$を受信すると，副鍵x_Aおよびy_Aを用いて，

$$(K_{S_i}+R_i)\,x_A \equiv \tilde{x}_{A_i} \bmod n_A \qquad (1)$$

$$(K_{S_i}+R_i)\,y_A \equiv \tilde{y}_{A_i} \bmod n_A \qquad (2)$$

を算出する．次に，

$$\tilde{x}_{A_i}+K_{S_i}+R_i+a_j=K_{S_i} \qquad (3)$$

すなわち，

$$\tilde{x}_{A_i}+R_i+a_j=0 \qquad (4)$$

を満たすa_jを主鍵集合$\{a_j\}$の中から全探索により探し出す．同様に，

$$\tilde{y}_{A_i}+R_i+a_j=0 \qquad (5)$$

を満たすa_jを主鍵集合の中から探し出す．K_S法を記述するには5つの式，実質的には(1)と(3)の2つの式で記述されることは注目に値しよう．この手法は以下のような特徴を有する．

- メモリを積極的に利用するが，所要総メモリ量を著しく削減するよう工夫していること．
- 主鍵集合の中にユーザIDを埋め込むことにより，違法ユーザ端末の追跡を可能としていること．

具体例として，コンテンツ配信システムを以下のように設定しよう．

コンテンツ配信システム
- 加入ユーザ数　：　1億
- コンテンツ・スクランブル周期　：　1秒
- ヘッダサイズ，鍵サイズ　：　20B

このとき，プロバイダ（たとえば放送局）が用意すべきメモリ容量は，以下のように与えられる．

- 全ユーザID情報　：　332MB
- 全ユーザ副鍵情報　：　6GB
- 1年間に使用する全ヘッダ情報：
  - ・デスクランブル用鍵情報　：　631MB
  - ・鍵隠蔽用乱数情報　：　631MB

加入ユーザ数が1億であり，しかもすべてのユーザに相異なりかつ消去困難なIDが埋め込まれた鍵を使用させているにもかかわらず，プロバイダが用意すべきメモリ容量は驚くほどわずかであることが明らかである．なお，加入者側で必要となるメモリ容量も同様に計算すると，年間当たり631MBである．

一方，スクランブル周期はライツマネージメントの立場から考えて，短くなるほど理想的である．詳細については文献2）に委ねるが，ヘッダサイズが従来法においては，少なくとも数百ビットの大きさとなるのに対し，K法においては，このヘッダサイズを限りなく1ビットに近づけることが可能である．通信回線の速度向上は当分見込めそうもないので，スクランブル周期は（仮にK法を用いるとしても）10^{-6}秒が今後少なくとも10年間における，現実的な限界値となろう．

個人情報保護と暗号技術

●個人情報の保護[3)]

個人情報の漏洩は，大きな社会問題となっている．個人情報の対象者が被害を受けるだけでなく，個人情報を漏洩させた企業が，数十億円の対策費用が必要となる場合があるからである．

個人情報の漏洩では，氏名，識別番号，性別，生年月日，住所などの個人を識別する基本的情報と，職業・職歴，地位・役職，学業・学歴，資格，賞罰，資産・収入・借金・預金・カード決済などの信用情報，思想，信条，宗教のような属性の対応付けが行われ，匿名性が失われて

しまうことが最大の問題であると考えられる．

最近では，個人を識別する基本的情報であっても漏洩が大きな問題になっている．(1) 住所と氏名を知られることにより架空の請求書が送られてくるといったことが現実に起こっているからであるとともに，(2) 自己情報コントロール権という概念がプライバシー権として一般に認識され始めたからであろう．

したがって，個人情報の保護のためには，基本的情報そのものの漏洩を防止するとともに，基本的情報と対応付けられた属性情報が漏洩することがないようにする必要がある．

さらに，これらの情報が漏洩しなくても，誰がやっている行為か不必要に分かってしまい，匿名性が維持できなくなる仕組みであるなら個人情報の保護上問題となる．

●個人情報漏洩対策

個人情報漏洩対策は，自分が管理する個人情報が，管理範囲外に出て行くのを防止する技術である．個人情報の漏洩は，(1)外部からの侵入者による場合と，(2)内部の人間による場合に大別できる．最近の漏洩は (2) によるものが非常に多いといわれている．

外部からの侵入対策は，いわゆるセキュリティ対策と同じになる．すなわち，第三者の不正侵入などを防止すればよいので，アクセス制御技術，暗号技術，セキュリティ監視技術などを用いることになる．大部分は，従来とほとんど同じ技術でよいが，次のようなものは少し対応が異なる．すなわち，従来のアクセス制御や情報フロー制御は一般ユーザの不正を防止するためのものであった．今後，情報管理者が，収集した情報を目的外に使用するのを防止する技術も大切になってくると考えられる．

内部の人間による犯罪では，情報の入手までは容易であるので，入手した情報の不正な持ち出しを防止するため，以下のような対策が必要になる．

(1)オンラインによるファイル流失の防止機能
- (a)メールによる個人情報送出の自動チェック機能
- (b)ファイアウォールによる内部から外部へのFTPなどの禁止
- (c)ペアオペレーション機能
- (d)ログ保管・回復・分析機能など

(2)オフラインによるファイル流失の防止機能
- (a)入退出管理システム
- (b)行動監視システム
- (c)持ち出し管理システム
- (d) USBポートの使用不可能化など

●匿名性の維持対策

行為を行っている人の匿名性を維持するには次のような技術があり，いずれも暗号技術をベースとするものである．

(a) 匿名通信路技術：メッセージの送信者や受信者，あるいはその両者を分からなくする技術であり，家庭からの電子投票などを実施する際に不可欠となる技術である．匿名中継者を用いる方法，MIX-NETを用いる方法，秘密分散する方法などが知られている[4]．

(b) 誰が署名者か分からなくする署名技術：電子投票や内部告発などにおいては，確かに該当するグループの人が行ったのだが，誰が行ったか秘密にしたい場合がある．このような署名方式に，グループ署名や，リング署名などがあることが知られている[4]．

セキュリティ対策と個人情報保護対策

上述したようにセキュリティ対策を実施することが，個人情報保護対策になる場合もあるが，セキュリティ対策を実施することが，個人情報の漏洩につながる場合もある．

たとえば，セキュリティ対策のための暗号化やディジタル署名のために公開鍵証明書を利用するが，ここに書かれた，住所や生年月日が，個人情報の流失につながるとの批判もある．これを防ぐために，公開鍵証明書の代わりに，権利があるかどうかだけを保証する属性証明書を用いる試みなどが行われている．

また，インターネット上でメールの覗き見などを防止するためには，暗号をかけたメールの送信が不可欠である．一方，暗号化メールを許すと，従業員が個人情報を不正に外部に送り出すのをチェックすることができなくなってしまう．このため，筆者らは従来の暗号メールソフトに改良を加え，**図-1**のような，システムの開発を行った[5]．

従来のS/MIME型の暗号化メールでは，メールの内容Mを共通鍵Kで暗号化したもの$K(M)$とそのKをメールの送信先のBobの公開鍵P_Bで暗号化した$P_B(K)$だけを送っていた．ここでは，サーバ側で安全に復号し，内容をチェックできるようにするため，メールサーバ用の公開鍵P_{MA}で，メールメッセージ用の鍵Kを暗号化したものである$P_{MA}(K)$を追加する方式を採用している．

また，復号したメールデータに個人情報が含まれない

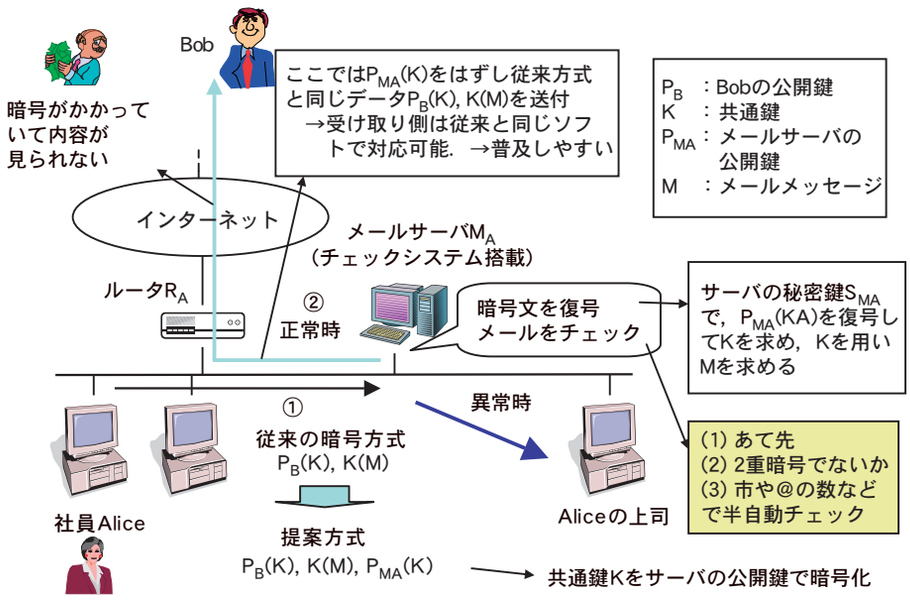


図-1　個人情報不正送出チェック機能付き暗号化メールシステムの概要

か，キーワードチェック機能や統計解析などを用い自動チェックする方式などを開発した．ここでは，チェックを行い，個人情報の送出の可能性があれば，Aliceの上司に送付し，問題なければ，$P_{MA}(K)$の部分を取り除き，従来のS/MIMEと同じ形式にし，Bobに送信する．

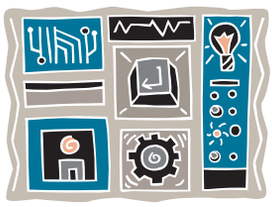
これらの方式の基本部分を実装したプログラムを開発し，実験を行い，基本的有効性を確認している．

以上見てきたように，個人情報保護のためにはセキュリティ対策との両立技術を含めたいろいろな対策が必要であり，暗号技術を利用するものも多い．

むすびにかえて

コンテンツの健全な育成，流通をはかるために，すなわちブロードバンド社会の基盤を強固なものにするために，著作権管理技術のより一層の発展が希求される．万が一にも著作権管理技術の分野で諸外国に遅れるようなことがあれば，我が国は，著作権保護等に問題がありコンテンツの流れに大きな不安を伴う国として位置づけられ，このことがブロードバンド社会の健全な発展を阻害することとなる可能性を否定することはできない．

なお，本稿前半およびむすびにかえてを笠原が執筆し，後半（個人情報保護と暗号技術以降）を佐々木が執筆した．

参考文献
1) 笠原正雄：ライツマネジメント，認証およびセキュリティ，映像情報メディア学会誌，Vol.57, No.5, pp.557-559（2003）．
2) 笠原正雄：ディジタル情報権利管理問題に関わる二，三の方式ー情報セキュリティの立場からの考察と提案ー，電子情報通信学会技術研究報告，ISEC2002-65（Nov. 2002）．
3) 佐々木良一：セキュリティと個人情報保護の関係に関する考察，電子情報通信学会，信学技報SITE2003-14, pp.1-6（Oct. 2003）．
4) 日本情報処理開発協会：次世代情報通信環境におけるヒューマンインタフェース技術に関する調査研究報告書，pp.23-43（Mar. 2003）．
5) 安　健司，赤羽泰彦，佐々木良一：個人情報不正送出チェック機能をもつ暗号メールの構想と基本部の開発，情報処理学会CSS2003（Oct. 2003）．

（平成16年9月30日受付）