「電子割符」のデジタル社会への応用

保倉　豊　　川城 三治

グローバルフレンドシップ株式会社

概要：電子情報のセキュリティを確保するために、新しい「電子割符」の概念を提案した。電子割符を用いることにより、重要な情報や鍵などのデータが分割管理でき、オリジナル情報のすべてが他に漏れることなく、アプリケーションの利用時点で利用者が保有する割符でオリジナル情報を復元することにより、極めて安全な情報のセキュリティツールとなる。この割符を既存の暗号技術と組み合せることで機能は相互補完されセキュリティがさらに向上する。また、分散管理の保存手段に IC カードを利用する方法がある。これらの応用事例を示してデジタル社会での実用性を述べる。

Applications of "e-Tally"

Yutaka YASUKURA, Sanji KAWASHIRO

Global Friendship, Inc.

Abstract：We propose a new idea of "e-Tally" to ensure the security of electronic data.
The utilization of e-Tally enables us to administer the data, such as important information and key, in a dispersed form, and to restore the original information, without leaking out any of the original information, in using the e-Tally.
This function therefore makes e-Tally most reliable security tool in keeping information. Moreover, combining the e-Tally with existing crypt-technology, the security of e-Tally will be kept at higher level. The utilization of IC card is another option as a means of storing the dispersed data In this paper, we describe such applications of e-Tally in detail.

1．はじめに

インターネットのようなオープンなネットワークでの電子商取引が普及し始めているが、そこにおける情報のセキュリティを確保することが重要な課題となっている。これは今までネットワーク

管理者の課題であると考えられていた。そして情報そのものは暗号化技術を用いれば解読されないとしてきた。しかし、暗号だけに頼っているといつかは解読され、或いは暗号の鍵を盗られると短時間にしてすべての情報を解読されてしまう恐れがある。したがって、この問題はネットワーク管理者の課題であると同時に、情報そのものを管理する情報管理者の課題であるとの認識が求められる。

情報そのものを管理するには、情報管理者が管理し易いツールが提供されることが望ましい。このニーズに用いる目的で、しかも簡単に使用出来るものとして、かつて勘合貿易の照合に使用された割符の概念を現在のデジタル情報に適用する手法を考案した。これを「電子割符（e-Tally）」と呼ぶことにする[1]。

電子割符は重要な情報や鍵などのデータを分割管理でき、オリジナル情報のすべてが他に漏れることなく、アプリケーションの利用 時点で利用者が保有する割符でオリジナル情報を復元するので、情報を管理する上で安全なセキュリティツールとなる。この割符を既存の暗号技術と組み合せるとセキュリティはさらに相互補完される。また、分散管理の保存手段に IC カードを利用する方法がある。これによって、割符データが盗られてもオリジナルデータは解読されることなく安全である。さらに本人が割符の一つを持つだけで本人がデータのセキュリティを管理できることになる。情報の全部を保持することなく情報セキュリティを管理でき、外部に情報の部分しか置かないため、セキュリティは高度に保てる。

本論文では、デジタル社会において暗号技術と相互補完することが出来るセキュリティツールとして提案した電子割符について、その技術的構成と応用における実用性ついて研究した結果を報告する。

2．既存セキュリティの課題

データ管理の責任主体は誰なのかということが IT 世界のセキュリティにおける根本的な課題と考えられる。既存のシステム構築概念での情報管理では、インターネットを社会基盤として機能させる社会システム構築に対応できない状況にある。

情報管理の責任主体を、正当権限者、情報管理受託者、情報正規受領者の 3 つに区分してその権限と責任における課題を考察する。

(1)正当権限者

ここでの管理者は、一般に個人、企業代表であるが、情報管理意識レベルがスキルアップされていない場合が多く、また管理ツールが専門技術者用のものしか無いため管理を他の人に任せていて、被害や損害が発生して始めて管理の甘さを知る状況にある。

情報の漏洩（コピー）、著作権の侵害等を防できる管理ツールが提供されて、正当権限者の管理意識レベルを高められることが期待される。

(2)情報管理受託者

ここでは多くの場合、情報が技術的専門家によって管理されるが、システムが大きくなると、一元管理に限界が生じ、内部犯罪が発生する土壌を作ってしまう。

情報の正当権限者が参画できるようなツールを組込んだ管理システムが求められる。

(3)情報正規受領者

情報を正当な手段で入手しようとする正規の受領者において、たとえ暗号を使用したとしても起こり得る問題として、

①情報を入手するまでの過程で、第三者に複製（コピー）されたり、内容を改竄される場合、

②情報を入手した後に複製や改竄される場合がある。これを防止する使い易くて安全なツールが提供されることが望まれている。

以上の課題を解決するためには、安心して使用できるセキュリティツールが必要だと言える。

3. 電子割符

電子割符は、情報の盗聴や改竄を防止するための情報の分割管理が出来るようにしたデジタル情報の割符である。すなわち、オリジナルデータ

を非線型分割して第 3 者に情報を見られないように、また改竄されたときにオリジナルデータに復元されないようにするものである。これらの原理、構成、機能について述べる。

3.1 電子割符の原理

オリジナルデータを非線型分割して第 3 者に情報を見られないように、また改竄されたときにオリジナルデータに復元されないようにするものである。そのために、電子割符は次の３つの基本原理を使用する[2]。

(1) デジタル非線型分割

勘合貿易に使用されたアナログ割符と異なり、分割数を割符の数以上に設定して分割を行うことが可能である。

(2) ブロックデータ（割符）の形成

非線型分割したデータから割符を形成する。（個々の割符の情報からオリジナルデータを数学的に類推することを困難にする）

(3) 復元時のチェック

復元時に改竄等のチェックを行う。

電子割符の基本動作を確認するための体験版ソフトウェアは参考文献を参照されたい[3]。

3.2 構成

(1) 電子データの構造と電子割符の構成

オリジナル情報の電子データと電子割符の関連イメージを図１に示す。

(2) 電子割符の生成とデータの復元

オリジナルの電子データを分割して複数の割符を生成する。割符からオリジナルデータへの復元は、分割したすべての割符を統合ソフトウェアで統合することによって行う。

3.3 機能

電子割符の分割・統合機能、及びセキュリティ機能についてのべる。

(1) 分割・統合機能

・オリジナル情報の制約

対象情報がデジタルデータであれば、文書、画像、動画、コンピュータプログラム、音楽ソフト等のあらゆる情報に適用できる。

・分割数

今回の実験では、割符の数を最大 99 とした。

・復元条件

割符のすべてを揃えることで統合ソフトウェアが機能する。統合時に ID 等のセキュリティ条件を設定できる。

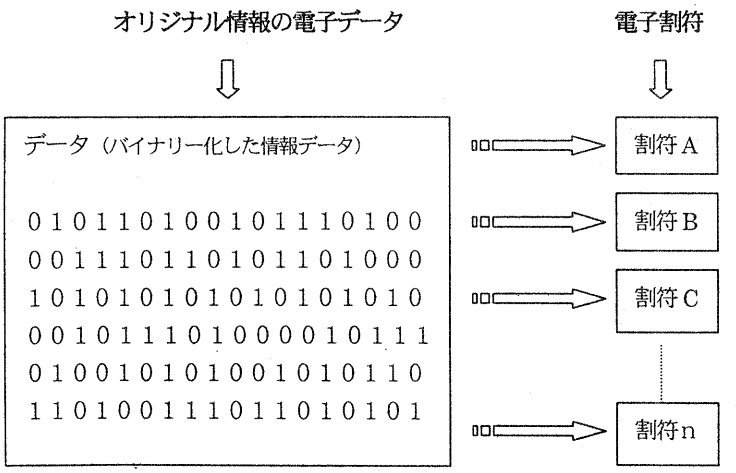

図１ オリジナル情報の電子データと電子割符の関連イメージ

(2) セキュリティ機能

電子割符が持つセキュリティ機能は、複雑に階層化することが出来るが、基本的な機能を以下に述べる。

① 割符単独では情報価値がない

個々の割符内のデータは不連続分割された形で構成されているので、単独の電子割符の内容データは情報価値を持たない。また数学的類推が困難である。

② 復元時のチェック機能

オリジナルデータを復元するための割符が統合されるときに、それぞれの割符をチェックする機能を備えている。

③ 第 3 者機関に全データを開示しない電子公証機能

作成した複数の割符の中から一つだけを公証機関に預けることで公証機能を持たせられる。

④ IC カードに分割保存

電子割符の幾つかのデータを IC カードに保存し、IC カード所有者が IC カードデータを提供しないとオリジナルデータは復元できない。(復元あるいは類推出来るデータが他に存在しない)

⑤暗号技術との組み合せ

オリジナルデータや割符化したデータに既存の暗号を用いることができる。

4．適用事例

電子割符の応用範囲は情報や鍵など分割管理したいもの、たとえば、契約書、注文書、内容証明文書、コンテンツの著作権、暗号鍵などに利用できる。ここでは、コンテンツの配信、鍵配布の管理、IC カードによる鍵の分割管理の事例について述べる。

4.1 コンテンツの配信 [Web からの受信の例]

インターネットで音楽ソフトや電子出版のようなコンテンツを配信する場合、コンテンツのデータをそのまま配信すると、データ量が多くネットワーク負荷が大きくなると同時に著作権管理の問題が発生している。電子割符はコンテンツ配信におけるこの問題を解決するアプリケーションに適用される。

ここでは、インターネットでのコンテンツを配信する応用事例として、割符のいくつかを CD で配布し、後の割符を WEB から受信する実験について述べる。

(1)フロー

図 2 のフローに示すように、コンテンツの大部分の割符を CD で入手し、決済が終われば WEB にアクセスして残りの割符をダウンロードする。

コンテンツ購入者は電子割符ソフトウェアでオリジナルのコンテンツデータを復元して利用する。

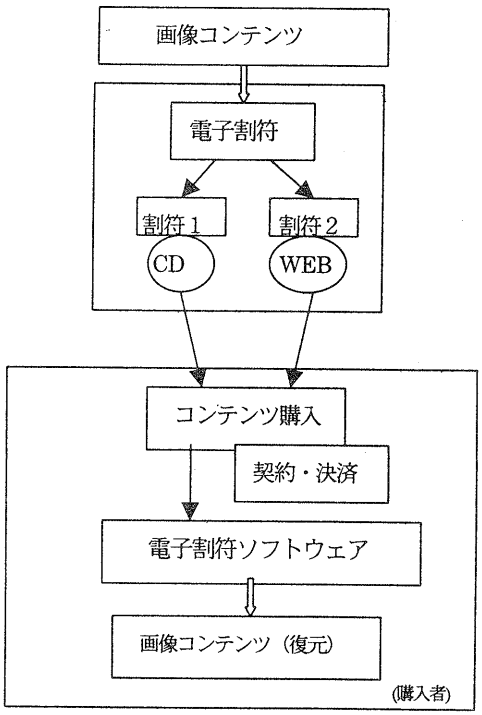

図 2 コンテンツ配信のフロー

(2)実用性と効果

①コンテンツの著作権管理

・CD のコピーでは、利用出来る情報価値が得られない。
・Web からのダウンロード情報だけでは、利用出来る情報価値がない。（ここに著作権の管理機能を持つことが出来る。）

②証明書等への応用
・各種の電子証明書を送信するときに、不正コピーを防止できる。
・電子証明書を受け取る時の認証手段にも応用できる。

③ネットワークの負荷を軽減
・コンテンツの一部だけをダウンロードして、残りの大半のデータを他の手段（CD）で配信できる。

4.2 鍵配布の管理

電子割符を鍵（ID パスワード）配布の管理に応用した事例を述べる。これは従来鍵の配布を FD(または CD)で行っていたアプリケーションで鍵管理のセキュリティに問題が生じる恐れが出たため電子割符に切り替える試みである。この応用事例の背景には、B to B、B to C の電子商取引において鍵の流出は被害が大きいだけに暗号だけに頼ることの不安と相俟って、鍵の配布方法の安全が EC の普及に欠かせない理由があった。

(1)フロー

鍵データ（ID パスワード）配布のフローを図３に示す。鍵配送者がオリジナルの鍵データを管理し、これを分割して電子割符とし、独立した異なる配送手段と配送チャネルで受信者に転送する。受信者は割符を統合して元データに復元し、アプリケーションに使用する。復元鍵データの管理は受信者が行う。

(2)実用性と効果

①鍵データの盗難を防止
・鍵の配布時に盗難があっても、鍵情報のすべてを盗られる可能性は少なく、盗難を防止に役立つ。

②電子商取引の安全な運用
・電子商取引に使用する鍵がセキュアに配布され、安全な運用を実現できる。

③パスワード更新への応用
・パスワードの更新がセキュアに行える。

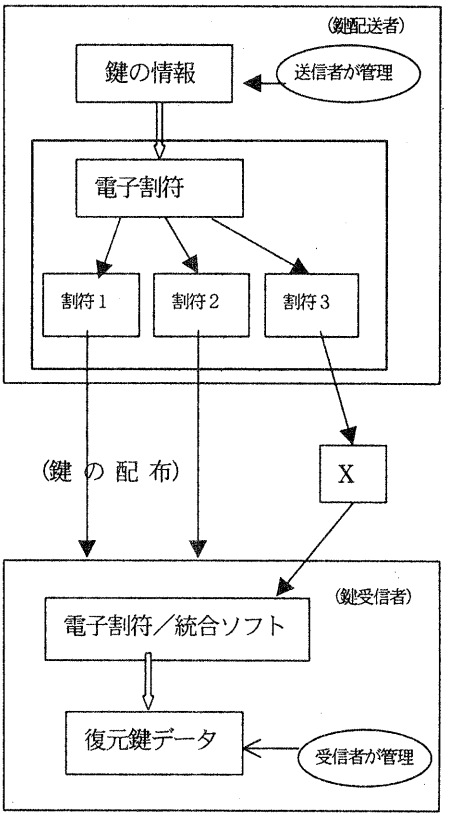

図３ 鍵データ(電子割符)の配布フロー

4.3 IC カードによる鍵の分割管理

鍵を本人が管理するアプリケーションでは、鍵データの割符の一つを IC カードに保存して本人が保持し、鍵の使用時には本人の IC カード電子割符を提示しない限り錠データは復元されない。

(1) フロー

IC カードを割符として使用する鍵の分割管理を行うアプリケーションでのデータの流れを図４に示す。

(IC カード電子割符作成)
・電子割符でオリジナルデータの割符を作成し、

ICカードに書込み、割符カードを発行する。
・電子公証が必要な場合は、割符の一つを電子公証機関に保存する。
(オリジナルデータの復元)
・ICカード認証後にカード内の割符データを電子割符ソフトウェアに提供する。
・すべての割符を揃えてから統合ソフトウェアで復元する。

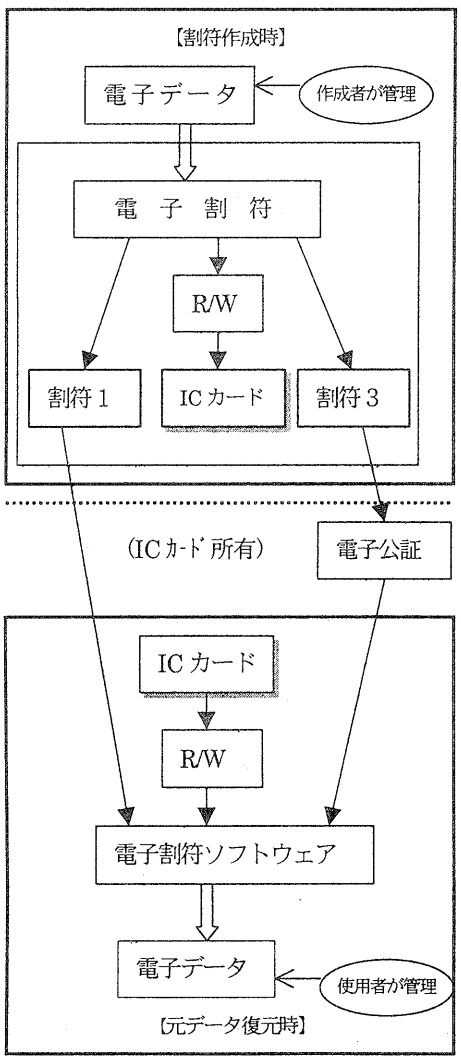

図4 ICカード電子割符におけるデータの流れ

(2) 実用性と効果
①情報管理責任者が情報を管理できる
・割符を本人が保持できる(サーバーにデータが残らない。また、処理中のデータは外部に出ない。
・カード内の割符データはICカードのセキュリティでガードされている
・本人だけのロックを掛けられる(紛失・盗難に対して管理者責任の意識ができる)
②本人認証
・ICカードの本人認証に電子割符の機能を使用できる。(「なりすまし」や「否認」の防止に役立つ。)
・認証データを本人しか持っていない。
③電子公証
・電子割符の一つを第3者(公証)機関に保存する方法で電子公証の手段となる。
・第3者(公証)機関にはオリジナルデータの一部しか保存されないから、アタックに強い電子公証が実現できる。

5. まとめと今後の課題

インターネットのようなオープンなネットワークを基盤とする社会システムで、情報管理についての新しいセキュリティ概念として提案した「電子割符」が、情報管理責任者にとって有効なツールであることを応用事例での実験結果で示すことが出来た。これらの結果は当初目的とした機能を実現出来たことを示している。また電子商取引実証推進協議会(ECOM)認証・公証WGの報告書[4]で「各レベルにおける具体的な秘密鍵管理方法の考察」において「鍵の分割管理」がガイドラインとして提言されているが、「電子割符」は、鍵の分割管理を有効に行えるツールでもあることを検証した。今後これらの結果を基盤として、新しいアプリケーションについて実用に向けた実証実験を重ねて、デジタル社会に向けたインフラ構築の役割を果たしたい。

【謝辞】
本研究の一部分は、中小企業総合事業団からの委託研究調査「電子商取引における本人認証の高度化に関する研究調査」として実施しました[5]。関係の各位にお礼を申しあげます。

【文献】

1．商標登録「電子割符」及び「e-Tally)」
2．出願特許（グローバルフレンドシップ株式会社社長の電子割符関連出願特許）
3．「電子割符（e-Tally)」体験版、INTERNET magazine 2000年3月号p.387及び付録CD（インプレス社）
4．電子商取引実証推進協議会（ECOM）認証・公証WG 報告書(平成12年3月発行)<認 証のレベルと本人確認方式に関する提言>
5．平成10年度課題対応新技術研究調査事業成果報告書 p46、中小企業総合事業団（平成11年12月発行）