交渉ゲームにおける鍵自己暴露戦略のインパクト —電子署名技術の利用に係る新たな課題

宮崎邦彦[†1,†2] 岩村充[†3] 松本勉[†4]
佐々木良一[†5] 吉浦裕[†6] 松木武[†7]
秦野康生[†1] 手塚悟[†1] 今井秀樹[†2]

電子署名技術の利用にあたっては，署名者は秘密鍵を安全に管理する必要がある．一般には，秘密鍵を安全に管理することは署名者自身にとって利益となると考えられているが，署名者の状況によっては，安全に管理することが利益とならないケースも生じうる．本稿では，署名者が債務超過に近い状態にある債務者である場合を例にあげて，署名鍵の自己暴露が債権者に対する攻撃となることを指摘する．さらに債務者が鍵自己暴露の可能性を持つことが，債権者–債務者間の債務縮減交渉に与える影響について分析を行い，この問題への対策の方針と例を示す．

Impact of the Key Self-compromise Strategy in a Bargaining Game The New Problem Affecting Application of Digital Signature Technology

Kunihiko Miyazaki,[†1,†2] Mitsuru Iwamura,[†3]
Tsutomu Matsumoto,[†4] Ryoichi Sasaki,[†5] Hiroshi Yoshiura,[†6]
Takeshi Matsuki,[†7] Yasuo Hatano,[†1] Satoru Tezuka[†1]
and Hideki Imai[†2]

In application of digital signature technology, a signer needs to manage his/her private key safely. Keeping the private key safely is seemingly profit for the signer him/herself, but this may not true in certain situation. In this paper, the case where the signer is an obligor who is almost crushed by debt is mentioned as an example and we point out that self-compromising the signing private key by the obligor serves as an attack on a creditor. Furthermore, we analyze how it affects on the debt curtailment bargaining between a creditor and an obligor that the obligor has private key self-compromising, and show examples for countermeasure.

1. はじめに

インターネット等の情報ネットワーク発展にともない，ネットワーク上での電子商取引の適用範囲がますます広がってきている．このような分野においては，従来の紙による契約書に対する署名あるいは押印とは異なり，電子データに契約者の署名をつける必要がある．この目的のために利用される技術として，電子署名技術が用いられている．

電子署名は，秘密鍵と呼ばれる特別な情報を知るものだけが生成することができ，また，その正当性は，公開鍵と呼ばれる誰もが入手可能な情報によって確認することができるという特徴を持つ．したがって，この秘密鍵が通常の印鑑としての意味を持つことになる．このため秘密鍵の管理には十分な注意を要する．

署名用秘密鍵の安全な管理については，これまでに

†1 株式会社日立製作所システム開発研究所
Systems Development Laboratory, Hitachi Ltd.
†2 東京大学生産技術研究所
Institute of Industrial Science, The University of Tokyo
†3 早稲田大学大学院アジア太平洋研究科
Graduate School of Asia-Pasific Studies, Waseda University
†4 横浜国立大学大学院環境情報研究院
Graduate School of Environment and Information Sciences, Yokohama National University
†5 東京電機大学工学部
Faculty of Engineering, Tokyo Denki University
†6 電気通信大学人間コミュニケーション学科
The Department of Human Communication, The University of Electro-Communications
†7 日立電子サービス株式会社
Hitachi Electronics Services Co., Ltd.

さまざまな研究が行われている．たとえば，耐タンパ性の高い鍵管理装置に関する研究[1]や，秘密分散手法を応用して安全性を高めた署名方法[3),5),8),10)]や，鍵を定期的に更新して安全性を高めた署名方式[2),4)]に関する研究等がある．また，暗号解読技術の進歩等によって，秘密鍵が漏洩してしまった場合の影響や，その対策技術に関する研究[6),7),12),13)]も行われている．

これらの研究では，署名者とは異なる攻撃者によって秘密鍵が危険にさらされる場合を対象としており，署名者自身が，悪意を持って，自らの秘密鍵を公にさらす行為については考えられていなかった．これは，署名者が自身の秘密鍵を安全に管理することは，署名者自身にとっての利益であり，これに反する行為をする動機がない，と考えられていたためである．

しかし，署名者の状況によっては，自ら秘密鍵を公にさらすことが，署名者自身にとってメリットとなるケースもありうる．そこで本稿では，署名者が自ら秘密鍵を公にさらす攻撃を「鍵自己暴露攻撃」と呼び，攻撃の方法と影響の分析を行い，対策について検討する．

鍵自己暴露攻撃は，電子署名技術が利用されるさまざまな場面に幅広く適用可能であると考えられる．本稿では，以下，署名者が債務超過に近い状態にある債務者である場合を典型的な具体例としてあげて分析を行い，この攻撃がもたらす問題点を明らかにする．

鍵自己暴露攻撃は，それ自体が攻撃として意味を持つだけではなく，債務者（署名者）が鍵自己暴露の可能性を持つことにより，債権者に対する債務縮減交渉の材料としても利用できる．いい換えると，実際に鍵を暴露しなくても，鍵自己暴露の可能性を示すだけで，債務者が利益を得ることができる．実際，本稿では，債権者–債務者間の債務縮減交渉ゲームにおいて，債務者が鍵自己暴露を戦略として持つことによって，従来は得られなかった債務者にとって有利な均衡解が，得られるようになることを示す．

本稿の構成は以下のとおりである．まず 2 章において鍵自己暴露攻撃の概要について述べる．次に 3 章において，ゲーム理論[11),14)]を用いて債務者が鍵自己暴露の可能性を持つことによる債務縮減交渉に与える影響について分析し，4 章において，この分析結果を考察し，対策技術の方針と例を示す．最後に 5 章においてまとめを述べる．

2. 鍵自己暴露攻撃

本節では，鍵自己暴露攻撃の概要について例を用いて説明する．以下，本稿を通じて，Alice，Bob は，次のようなエンティティとする．

Alice 債権者．金銭借用書の検証者であり，結果的に被害者となる．

Bob 債務者．金銭借用書に対する署名者であり，最終的に攻撃者となる．

なお本稿では以降，Alice は正直かつ合理的であるとする．すなわち，Alice は与えられた条件の中で，最も自身にとって有利となる振舞いをするものと仮定する．

今，Bob は，Alice から 100 万円借りており，そのように書かれた Bob の署名つき金銭借用書を Alice が持っているものとする．

Bob の Alice に対する鍵自己暴露攻撃とは，次のような攻撃のことである．

［鍵自己暴露攻撃の流れ］

(1) Bob は自分の秘密鍵を暴露する．

(2) Bob は以下のように振る舞う Cathy に協力を依頼する（結託する），あるいは以下のように振る舞う Cathy が現れることを期待する．なお，このような Cathy は複数人存在してもよい．
Cathy が Bob に成りすまして「Bob が Cathy に 200 万円の借金がある」という金銭借用書を偽造する．Cathy は，偽造した金銭借用書を保持し，Bob に対して返済を迫る．

(3) Bob は Alice に対し以下のように主張する．
「鍵が漏洩したらしい．その結果 Cathy という債権者が現れて身に覚えのない借金の返済を迫られることになった．しかし自分には Cathy に対する債務の不存在を示すためのコストを負担する余裕がない」．

Bob が資産を十分に持っている場合は，Bob のこの一連の行為は，Alice にとって脅威とはならない．なぜなら，上述のような Cathy が現れようが，現れまいが，Alice との間の金銭借用関係にはなんら影響がないからである．

しかし，もし Bob が債務超過に近い状態にある場合（たとえば純資産 50 万円の場合）には，Alice に損害を与えられる．

なぜなら，Bob は債務超過の状態に陥るため，Alice と Cathy に対して全額返済することができなくなるからである．Bob の資産は，各債権者（ここでは Alice と Cathy）の債権額の割合に応じて清算され，その結果として，Alice が本来受け取るはずの返済金の一部が，Cathy の手に渡ってしまう．

たとえば，上記の例では，ただちに清算した場合で

あれば，Alice は 50 万円返金されるはずが，Bob が鍵自己暴露攻撃を実行したあとになると，16.6 万円（= 50 万円 × (100 万円/(100 万円+200 万円))）しか返金されない．これを避けるためには，Alice は Cathy の債権の不存在を示すためのコストを払わなければならず，いずれにしても Alice は損害を受ける．

すなわち，鍵自己暴露攻撃とは，署名者が自身の鍵を暴露することにより，相手（債権者）の財産を希薄化する攻撃である，といえる．

3. 債務縮減交渉ゲームにおける鍵自己暴露の影響

本章では，鍵自己暴露という手段を債務者の 1 つの戦略として利用した場合に，債務者–債権者間の債務縮減交渉に与える影響について述べる．

前章では，鍵自己暴露という行為が相手（債権者）に損害を与える可能性について述べた．このような可能性があること自体，電子署名利用において望ましいとはいえないが，前章に示した攻撃だけでは，攻撃者である署名者が直接利益を得られるわけではない．その意味では，鍵自己暴露に対するインセンティブとしては弱く，電子署名利用に対する影響度は小さいと考えられる．

しかし，一度，鍵自己暴露攻撃の可能性が示されると，これを債務者が 1 つの戦略として利用することにより，債権者との間の債務縮減交渉を有利に進めることができる．すなわち，鍵自己暴露の可能性が，攻撃者にとって利益をもたらす．そのため，電子署名利用に対する影響も大きい．

以降，典型的な状況の下で，攻撃者が鍵自己暴露の可能性がある場合とない場合で，債務縮減交渉ゲームの均衡解が変化（攻撃者である債務者にとってより有利な解が均衡解となる）ことを示す．

3.1 債務縮減交渉ゲーム

本稿で考える債務縮減交渉ゲームとは，次のようなゲームである．なお，以下のゲームにおいては，Alice と Bob の双方に対して，債務縮減案を提示する第三者である仲裁者を導入する．これはたとえば，裁判外紛争解決制度の 1 つである調停において，紛争当事者に対して解決策案を提示する調停人に相当する☆．

☆ これに対し，もし債務縮減案を Alice または Bob が与えるケースを考えると，このゲームは最後通牒ゲーム[14] と呼ばれるゲームと同じになる．この場合，本文中に数値例を示した状況設定の下では，Alice が与えるならば X は 80 に，Bob が与えるならば X は 50 に決定される．仲裁者を導入したゲームと，最後通牒ゲームとの関係についての考察は文献 15) 等に見られる．

(1) 第三者である仲裁者から債務縮減案（債務を X 円に縮減する）が提示される．
(2) Alice と Bob は提示額に対してそれぞれ受入/拒絶のいずれかを回答する．
(3) Alice と Bob の双方がともに「受入」を回答した場合には，交渉は成立し，そうでなければ交渉は決裂する．

以下では，議論を分かりやすくするために，具体的な数値例として次のような状況をあげ説明する．

［状況設定］

- Bob は Alice に対し 100 万円の債務を負っており，それ以外の債務はない．
- Bob の現在の資産評価額は，もし破産せずに存続した場合は 80 万円と評価され，破産し清算された場合は 50 万円と評価される．

3.2 鍵自己暴露の可能性がない場合

はじめに Bob が鍵自己暴露の可能性がない場合を考える．この場合，提示額 X を Alice，Bob 双方が受け入れ，交渉が成立したときには，Alice，Bob それぞれの資産は，

Alice X (if $X < 80$)，50 (if $X \geq 80$)
Bob $80 - X$ (if $X < 80$)，0 (if $X \geq 80$)

と評価される．なぜなら，提示額 X が 80 万円未満であれば，Bob は存続可能でありその資産は 80 万円と見積もられ，80 万円以上であれば，たとえ交渉が成立しても Bob は債務超過に陥り，破産し清算されるためである．また，Alice または Bob が拒絶したときは交渉決裂となり，Bob は破産する．その結果，Alice，Bob それぞれの資産は，

Alice 50
Bob 0

と評価される．**表 1** は $X = 40$，60 の場合を例として，Alice と Bob が，提示額 X に対し「受入」または「拒絶」したときの，それぞれの資産を示した表である（このような表を利得表と呼ぶ）．

この表から分かるように，$X = 60$ のとき Alice は，Bob がどちらの戦略をとろうと，自身は「受入」戦略をとった方が有利になる（少なくとも不利にはならない）．このように，相手の選択にかかわらず，自身が有利になる戦略のことを支配戦略と呼ぶ．この場合は，Bob にとっても「受入」が支配戦略である．したがって $X = 60$ のときは，Alice，Bob 双方が合理的に振る舞うとすれば，(Alice，Bob) =（受入，受入）という戦略の組が選ばれることになり，交渉は妥結に至る．

一方，$X = 40$ の場合は，Alice にとっては「拒絶」が支配戦略であり，Bob にとっては「受入」が支配戦

表 1 鍵自己暴露の可能性がないときの利得表
Table 1 Payoff table (Without key self-compromise).

$X = 60$ の場合		Alice	
		受入	拒絶
Bob	受入	Alice: 60 Bob: 20	Alice: 50 Bob: 0
	拒絶	Alice: 50 Bob: 0	Alice: 50 Bob: 0
$X = 40$ の場合		Alice	
		受入	拒絶
Bob	受入	Alice: 40 Bob: 40	Alice: 50 Bob: 0
	拒絶	Alice: 50 Bob: 0	Alice: 50 Bob: 0

表 2 鍵自己暴露の可能性があるときの利得表
Table 2 Payoff table (With key self-compromise).

$X = 60$ の場合		Alice	
		受入	拒絶
Bob	受入	Alice: 60 Bob: 20	Alice: 0 Bob: 0
	拒絶	Alice: 0 Bob: 0	Alice: 0 Bob: 0
$X = 40$ の場合		Alice	
		受入	拒絶
Bob	受入	Alice: 40 Bob: 40	Alice: 0 Bob: 0
	拒絶	Alice: 0 Bob: 0	Alice: 0 Bob: 0

略である．したがってこの場合，交渉は決裂する．

一般に，Alice にとっては，$X \geq 50$ なら受け入れた方が有利であり，$X < 50$ なら拒絶した方が有利になる．また，Bob にとっては，X の値によらず，つねに受け入れた方が有利になる．したがってこのゲームは，$50 \leq X < 80$ のときには交渉が成立し，$X < 50$ のときには交渉が決裂することになる．また，$X \geq 80$ のときには，Alice と Bob がどのように振る舞っても無意味である（Alice の資産は 50 になり，Bob の資産は 0 になる）．

3.3 鍵自己暴露の可能性がある場合

次に Bob が鍵自己暴露の可能性がある場合を考える．

この場合は，交渉が決裂したときに Bob が鍵自己暴露を行う可能性がある．さらに，Bob が鍵自己暴露を行ったときには，他の Alice 以外の債権者（Cathy）が現れる可能性がある．そこで，Bob の鍵自己暴露確率を P，またそのときの Cathy の債権額を C と書く☆．

ここで Bob の鍵自己暴露確率 P は，Bob が選択する値ではなく，本来 Bob が属性として持つ値であり，たとえば Bob がどのような署名生成方式，装置等を利用しているか等の要因に依存する．以降で，Alice が自身の戦略を決定するために利得表を作成する際には，この Bob の持つ属性である鍵自己暴露確率を，外部からの観察によって Alice が主観的に評価した結果に基づき，主観確率として設定した値を用いる．また Cathy の債権額 C についても同様に Bob の属性であるとする．

このとき，提示額 X に対し，Alice，Bob 双方が受け入れるとすると，それぞれの資産は，

Alice X (if $X < 80$)，50 (if $X \geq 80$)

Bob $80 - X$ (if $X < 80$)，0 (if $X \geq 80$)

と評価され，また，交渉が決裂したときは，

Alice $50 \times (100/(100 + C)) \times P + 50 \times (1 - P) = 50 \times (1 - (CP/(100 + C)))$

Bob 0

と評価される．いま仮に，$P = 1$（i.e. Bob は必ず鍵自己暴露をする），$C = \infty$（i.e. 一度鍵が暴露されると無限の債権者が現れる）と仮定すると，交渉決裂時の Alice の資産は，X の値によらず，つねに 0 になる．**表 2** は $P = 1$，$C = \infty$ を仮定した場合の $X = 40$，60 における利得表である．

$X = 60$ のときは，鍵自己暴露の可能性がない場合と同様，（Alice，Bob）=（受入，受入）が選ばれる．

一方，$X = 40$ のときを見てみると，鍵自己暴露の可能性がない場合には交渉が決裂したのに対し，鍵自己暴露の可能性がある場合には，Alice にとっても「受入」が支配戦略となり，（Alice，Bob）=（受入，受入）が選ばれる．

一般に，$P = 1$，$C = \infty$ という仮定の下では，Alice にとっても，Bob にとっても，X の値によらず，拒絶するより受け入れた方が有利になることが分かる．したがってこのゲームは，X の値によらず交渉が成立することになる．これは，Bob から見ると，鍵暴露戦略の可能性があることにより，ないときには妥結できなかった，より有利な条件（より低い金額）で，債務縮減交渉が妥結できるようになったことを示している．

$P = 1$，$C = \infty$ 以外の，より一般の鍵自己暴露確率 P と Cathy の債権額 C に対しては，$X > 50 \times (1 - (CP/(100 + C))$ を満たす X が提示されたときは，Alice は受け入れたほうが有利であり（したがって Bob にとってみれば債務縮減交渉が成功し），そうでなければ Alice は拒絶したほうが有利となる．

図 1 は，Cathy の債権額に対する，妥結可能な交渉額の最低値の変化を示したグラフである．Cathy の

☆ 一般には，Alice 以外の債権者である Cathy は複数人存在しうる．このときは，C はすべての Cathy の債権額の合計とする．

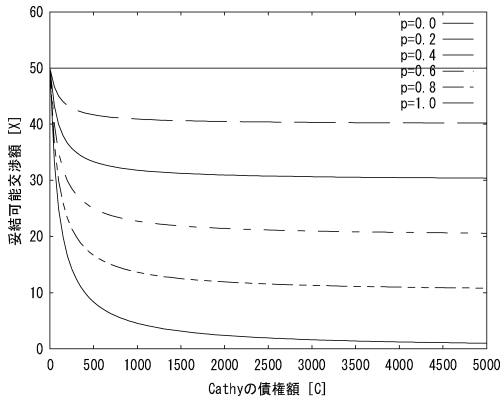

図 1 妥結可能交渉額の変化
Fig. 1 Agreement price of the bargaining game.

債権額 C が大きいほど，また，Bob の鍵自己暴露確率 P が大きいほど，低い額での妥結が可能となることが分かる．さらに $C = \infty$ における，妥結可能額の極限は $50 \times (1 - P)$ となる．また，Alice の債権額の 4 倍に相当する債権額が Cathy との間に存在したとき（$C = 400$ のとき）ですでに極限の 8 割に相当する $40 \times (1 - P)$ まで妥結可能額は下がることが分かる．

4. 考　　察

4.1 電子契約と紙契約との比較

前章で述べたように，鍵自己暴露の可能性を考慮すると Bob は債務削減交渉をより低い額で折り合いをつけられる可能性があり，鍵自己暴露確率 P と Cathy の債権額 C が大きいほど，その妥結可能額は下がる．

以下に説明するように，このことは，自己暴露という行為の電子署名利用に与える影響が，紙文書に対する捺印，署名の利用に与える影響と比較して，大きいことを示唆している．

電子署名用の秘密鍵を自己暴露することと，契約用印鑑を自己暴露することのどちらが容易であるかは，それぞれの管理状態に依存するため，一概には判断しがたいが，秘密鍵の方が電子データであり，印鑑のほうが物理的な実体を有することを考慮すれば，一般には署名用秘密鍵の方が暴露しやすい，と考えられる．さらには，署名用秘密鍵の場合には，暴露されていないことの確認は著しく困難であろう．したがって Bob の鍵自己暴露に関する，Alice の主観確率 P は，秘密鍵の場合のほうが高いと考えられる．

また秘密鍵の場合は容易かつ大量にコピー可能であるので，いったん暴露された場合に，それを悪用した Alice 以外の債権者 Cathy が現れる可能性が高いのは電子契約の場合であろう．したがって，C も電子契約のときのほうが大きいといえる．

すなわち，鍵自己暴露（に相当する行為）は，紙文書の契約のときにも生じる問題であるが，電子署名技術の利用において，より影響が大きく，問題として顕在化する可能性が高いといえる．

なお，攻撃者 Bob が電子契約と紙契約を併用しているような場合には，電子契約における鍵自己暴露攻撃が，書面による紙契約の内容に対しても影響する可能性があることに注意を要する（いったん，鍵自己暴露攻撃によって Bob の財産が希薄化してしまえば，紙，電子を問わず，Bob の関与する契約すべてに影響が生じる）．

4.2 法律的な議論

本節では，鍵自己暴露攻撃に関して法律的な考察を試みる．なお，鍵自己暴露攻撃は，特定の国の法律に依存するものではないが，本稿では，特に日本の法律を前提として議論を行う．

まず，前節までに説明した鍵自己暴露攻撃が，電子署名および認証業務に関する法律（電子署名法）[9),19)] の観点から見て，攻撃として成立しうるか否かについて考察を行う．

電子署名法の第 3 条によれば，「これ（注：電子署名）を行うために必要な符号および物件を適正に管理することにより，本人だけが行うことができることとなるもの」について有効であると推定される，と規定されている．

この条文では，「署名鍵を適正に管理しなかった場合」の電子署名の有効性がどうであるかについては，述べられていないことに注意する．

これはすなわち，電子署名法の第 3 条が，「実際に適正に管理されていたこと」等の証明の難しさを軽減するために，「署名鍵のような重要なデータは適正に管理されていることが多い」等の経験則に基づき，「適正な管理をすれば本人だけが使用可能な電子署名技術」を使用していれば，「その電子署名が署名者本人によって使用された」という推定を与えるものであると理解できる．もちろんこれは推定であるので，適正に管理されていなかった（i.e. 署名鍵が自己暴露されていた）ことが別途証明できれば，これを覆すことが可能な場合もあるであろうが，すくなくとも，署名者が鍵を自己暴露した，あるいは自己暴露を示唆したことによって，ただちに電子署名法による推定が成立しなくなるわけではないと考えられる．

次に，2 章で述べた鍵自己暴露攻撃の流れに沿って，より具体的な考察を試みる．まず，鍵自己暴露攻撃開

始以前に Bob が Alice から借金をした時点（これを時刻 T_0 とする）においては，Bob は鍵自己暴露を行っていない．したがって，この時点で取り交わされた金銭借用書に付された Bob の電子署名については，すくなくとも時刻 T_0 においては，有効な電子署名であると推定されるものと考えられる．

それからのちに，Bob が自分の秘密鍵を暴露し，Cathy が金銭借用書を偽造した時点（これを時刻 T_1 とする）を考える．この Cathy が偽造した金銭借用書が，時刻 T_1 以降において有効な電子署名であると推定されるか否かによって，鍵自己暴露攻撃が，法的な意味で攻撃として成立しうるか否かが決まる．

ここで，時刻 T_0 から T_1 の間で，署名生成装置そのものに変化はなく，その利用者である Bob のインセンティブだけが変化していることに注意する．また，Bob が時刻 T_0 で作成した金銭借用書（これを D_1 とする）も，Cathy が Bob に成りすまして時刻 T_1 で作成した金銭借用書（これを D_2 とする）も電子文書であるので，それらが実際に作成されたのが，いつ，だれによるものであったのかを判断することは困難である．したがって，D_1 と D_2 に対して異なる判断（一方が有効であり，他方が無効であると推定する等）を与えることは困難であろう．

上述したように，鍵の自己暴露によってもただちに電子署名法による推定が成立しなくなるわけではないこと，さらには D_1 がすくなくとも時刻 T_0 においては有効な電子署名であると推定されると考えられること，をあわせて考えると，結果として，D_1，D_2 ともに有効である☆との推定が成立する可能性はあると考えられる．すなわち，鍵自己暴露攻撃は法的に成立しうると考えられる．

次に，鍵自己暴露攻撃が電子署名法の観点から成立した場合に，さらなる法的な対抗策があるかどうかについて，考察を行う．

鍵自己暴露攻撃は，署名者が，自らの有する資産を故意に希薄化することによって，債権者に対して損害を与える行為，と見なすことができる．このような行為を防止するための対抗策として，現在でも，法制度面からの制約が設けられている．

たとえば，民法[16] 第 424 条や，破産法[17] 第 160 条☆☆では，いわゆる詐害行為，すなわち債務者が，無資力の状態にあるときに，故意に自らの有する資産の財産価値を落とすような行為の，取り消しや否認が認められている．

また，Bob が企業の取締役や監査役であれば，鍵自己暴露という行為自体，会社に損害を与える行為であり，商法[18] の特別背任の罪に問われる可能性も否定できない．

したがって，債務縮減交渉のときに，誰の目にも明らかな方法で鍵を自己暴露するというのは，法的な意味でのリスクが大きく，攻撃としては有効に機能しない可能性が高い．

しかし，電子署名用の秘密鍵の場合は，ディジタルデータであるので，明らかな方法によらずに暴露することも可能であろう．たとえば以下のような方法が考えられる．

> 秘密鍵の値であるということは明かさずに，秘密鍵の値をインターネット上の匿名掲示板等に公開しておき，あとからそれが秘密鍵であることを Alice に知らせる（あくまでも Bob は「自分は気がつかなかったが誰かが私の秘密鍵を不正入手して掲示板に公開したらしい」と主張する）．

また Bob の目的が，債務縮減交渉を有利に進めること，であることを考えると，Bob は実際に秘密鍵を自己暴露しなくても（できなくても），自己暴露可能であることを Alice に信じさせればよい．この点に着目すると，次のような方法も考えられる．

> 鍵管理システムに脆弱性が見つかったので秘密鍵が漏洩する恐れがあると Alice に主張する．この場合は，Bob は債務の削減を要求するというよりは，システム更新費用を（必要以上に）要求すると考えられる．

これらの行為はもちろん不正な行為ではあるが，上述した民法，破産法，商法等の範囲で対抗できるかどうかは微妙であろう．いい換えると，電子契約における鍵自己暴露攻撃は，少ない法的リスクで行える可能性がある．

4.3 対 策 例

ここでは，既存技術を組み合わせた対策案を例示する．3 章で示したように，債務縮減交渉の成功は，鍵自己暴露確率 P と，鍵を暴露した場合に現れる Alice 以外の債権者 Cathy の債権額 C に依存する．したがって，対策の方針としては，P を下げる方法と，C

☆ 仮に，両方が無効であると判断される場合には，これは本稿で考察したのとは別のタイプの鍵自己暴露攻撃となる．すなわち，本来有効であった金銭借用書を，鍵自己暴露により，後から無効にする攻撃であるといえる．この攻撃の詳細および影響の考察については，今後の課題である．

☆☆ 2005 年 1 月の改正前の旧破産法においては第 72 条に規定されていた．

を下げる方法が考えられる．

［P を下げる方法例］

- 契約書には当該契約にかかわる当事者の署名に加えて，必ず第三者の署名やタイムスタンプも付与することとする．
  → 第三者の署名が必要となるため，Bob が自分で鍵を暴露しただけでは攻撃として成立しない．
- 契約にかかわる当事者はすべてヒステリシス署名方式[12] を利用し，契約書には必ず当該契約にかかわる当事者双方の署名を付与することとする．
  → ヒステリシス署名を利用しているため，仮に Bob が自分で鍵を暴露したとしても，それだけでは過去の署名を新たに偽造することはできない．

［C を下げる方法例］

- 契約書に付する署名は相手ごとに異なる鍵を使うものとする（例：Bob は Alice から借金をする場合には，Alice との取引用に生成された Bob の秘密鍵を用いて署名を付与する）．
  → 仮に Bob が自分で Alice との取引用の鍵を暴露したとしても，Alice とは異なる Cathy との取引には利用できない．また後から架空の Cathy が現れることも期待できない．
- 契約書に付する署名に Key-Insulated Signature[4] を利用し，一定期間ごとに異なる鍵を利用するようにする．
  → 契約書の発行（したとされる）日時が限定されるため，架空の契約書の不存在を示しやすくなる（不存在を示すためのコストが低くなる）．

なお，これらの対策案が有効に機能するためには，単に，これらの技術を利用するだけではなく，定められた形式と異なる契約書は無効であることを当事者間で同意し，同意したことの表明をあらかじめ行っておくべきである．そうでなければ，より鍵が漏洩しやすい，あるいは架空の契約書が存在するかのように振る舞いやすい，方法，形式に従って架空の契約書が作成されてしまう可能性がある．

4.4 電子署名技術利用への影響

4.3 節に示したように，鍵自己暴露攻撃の可能性をふまえた今後の電子署名技術に基づく契約においては，署名検証者が，署名者の署名生成環境（鍵管理方法，署名方式等）の確認を行ったうえで，その署名生成環境において生成された契約だけが有効であることを双方で同意し，表明することが，従来以上に重要となるといえる．

さらに，署名生成環境に応じて鍵自己暴露攻撃によるリスクを評価し，契約条件等を変更することは，鍵自己暴露攻撃への有効な対策の 1 つとなるであろう．

5. ま と め

本稿では，署名者自身による秘密鍵暴露問題について考察を行った．一般に，秘密鍵を安全に管理することは署名者自身にとって利益となると考えられているが，署名者の状況によっては，安全に管理することが利益とならないケースも生じることを指摘し，署名者が自ら秘密鍵を公にさらす攻撃を「鍵自己暴露攻撃」と呼んだ．本稿では，この攻撃がもたらす問題点を明らかにするために，特に，署名者が債務超過に近い状態にある債務者である場合を具体例にあげて，攻撃方法を示した．さらに債権者–債務者間の債務縮減交渉を，一種の交渉ゲームとして形式化し，債務者が鍵自己暴露の可能性を持つことが，債務縮減交渉に与える影響について分析したうえで，鍵自己暴露問題への対策の方針と例を示した．また，鍵自己暴露攻撃が電子署名技術の利用に与える影響について考察した．

本稿で形式化した交渉ゲームの記述は，一例であり，他にもたとえば「多数の交渉額 X の案があって，Alice と Bob とが案を選ぶ．Alice が，Bob の選択よりも Bob に不利な X を選んでしまうと Bob は暴露攻撃をする」という枠組みで記述するなど，さまざまなバリエーションが考えられる．どのような記述がより現実的であるかについては，今後の課題である．また本稿では Alice は正直で合理的であると仮定したが，Alice が不正な振舞いをした場合についての検討も今後必要である．その他の課題としては，鍵自己暴露問題に対する，より抜本的な対策案を示すことがあげられる．

謝辞 本稿の改良に際し，多数の有益なコメントを下さった査読者，担当委員の方々に謹んで感謝の意を表します．

参 考 文 献

1) Anderson, R.: *Security Engineering*, John Wiley & Sons, Inc. (2001).
2) Bellare, M. and Miner, S.: A forward-secure digital signature scheme, *Proc. CRYPTO '99*, LNCS Vol.1666, pp.431–448, Springer-Verlag (Aug. 1999).
3) Cerecedo, M., Matsumoto, T. and Imai, H.: Efficient and Secure Multiparty Generation of Digital Signatures Based on Discrete Logarithms, *IEICE Trans. Fundamentals*, Vol.E76-A, No.4, pp.532–545 (Apr. 1993).
4) Dodis, Y., Katz, J., Xu, S. and Yung, M.: Strong key-insulated signature schemes, *PKC*

'03, LNCS Vol.2567, pp.130–144, Springer-Verlag (2003).
5) Gennaro, R., Jarecki, S., Krawczyk, H. and Rabin, T.: Robust Threshold DSS Signatures, *Proc. Eurocrypt'96*, LNCS 1070, pp.354–371, Springer-Verlag (1996).
6) 小森 旭，松浦幹太，須藤 修：電子商取引における紛争解決のための電子証拠物に関する分析，2002 年暗号と情報セキュリティシンポジウム予稿集，pp.627–632, 電子情報通信学会 (2002).
7) 松本 勉，岩村 充，佐々木良一，松木 武：暗号ブレイク対応電子署名アリバイ実現機構（その 1）—コンセプトと概要，情報処理学会コンピュータセキュリティ研究会第 8 回研究発表会 (2000).
8) Miyazaki, K. and Takaragi, K.: A Threshold Digital Signature Scheme for a Smart Card Based System, *IEICE Trans. Fundamentals*, Vol.E84-A, No.1 (Jan. 2001).
9) 夏井高人：電子署名法，リックテレコム (2001).
10) Park, C. and Kurosawa, K.: New ElGamal Type Threshold Digital Signature Scheme, *IEICE Trans. Fundamentals*, Vol.E79-A, No.1, pp.86–93 (Jan. 1996).
11) 鈴木光男：ゲーム理論入門，共立出版 (2003).
12) 洲崎誠一，松本 勉：電子署名アリバイ実現機構—ヒステリシス署名と履歴交差，情報処理学会論文誌，Vol.43, No.8, pp.2381–2393 (2002).
13) 洲崎誠一，宮崎邦彦，宝木和夫，松本 勉：暗号ブレイク対応電子署名アリバイ実現機構（その 2）—詳細方式，情報処理学会コンピュータセキュリティ研究会第 8 回研究発表会 (2000).
14) 渡辺隆裕：図解雑学ゲーム理論，ナツメ社 (2004).
15) Zeng, D.: An amendment to final-offer arbitration, *Mathematical Social Sciences*, Vol.46, No.1, pp.9–19 (2003).
16) 民法．http://law.e-gov.go.jp/htmldata/M29/M29HO089.html
17) 破産法．http://law.e-gov.go.jp/htmldata/H16/H16HO075.html
18) 商法．http://law.e-gov.go.jp/htmldata/M32/M32HO048.html
19) 電子署名および認証業務に関する法律（電子署名法）．http://law.e-gov.go.jp/htmldata/H12/H12HO102.html

(平成 16 年 11 月 29 日受付)
(平成 17 年 6 月 9 日採録)

宮崎 邦彦（正会員）

1973 年神奈川県生．1998 年東京大学大学院数理科学研究科修士課程修了．同年（株）日立製作所入社．現在に至るまで，同社システム開発研究所にて，暗号，情報セキュリティの研究に従事．2003 年 4 月より東京大学大学院情報理工学系研究科博士課程在学中．2004 年暗号と情報セキュリティシンポジウム（SCIS2004）論文賞受賞．電子情報通信学会会員．

岩村 充

1950 年東京都に生まれる．1974 年 3 月東京大学経済学部卒業．1974 年 4 月日本銀行入行，ニューヨーク駐在員等を経て 1996 年 12 月企画局兼信用機構局参事．1998 年 1 月より早稲田大学大学院アジア太平洋研究科教授（現職）．2002 年 3 月早稲田大学博士．専門は社会情報学および金融論．「法とコンピュータ学会」理事．著書に『銀行の経営革新』（東洋経済新報社），『サイバーエコノミー』（東洋経済新報社），『新しい物価理論』（岩波書店），『企業金融講義』（東洋経済新報社）等がある．

松本 勉（正会員）

1986 年東京大学大学院博士課程修了．工学博士．同年横浜国立大学工学部専任講師．同助教授，教授を経て，2001 年より同大学大学院環境情報研究院教授．1981 年より暗号や情報セキュリティの研究に従事．「明るい暗号研究会」創設メンバ．現在，情報セキュリティ，暗号アルゴリズム，認証プロトコル，ディジタル証拠性，情報ハイディング，バイオメトリクス，人工物メトリクス，耐タンパー技術等に広く関心を持つ．国際暗号学会 IACR 理事．暗号技術検討会構成員．CRYPTREC 暗号モジュール委員会委員長．INSTAC 耐タンパー性標準化調査研究委員会委員長．電子情報通信学会より「情報セキュリティの基礎理論」への貢献に関して業績賞を受賞．

佐々木良一（フェロー）

1971 年 3 月東京大学卒業．同年 4 月日立製作所入所．システム開発研究所にてシステム高信頼化技術，セキュリティ技術，ネットワーク管理システム等の研究開発に従事．同研究所第 4 部長，セキュリティシステム研究センタ長，主管研究長等を経て 2001 年 4 月より東京電機大学工学部教授．工学博士（東京大学）．1998 年電気学会著作賞受賞．2002 年情報処理学会論文賞受賞．著書に，『インターネットセキュリティ』（オーム社，1996 年），『情報セキュリティ事典』（代表編，共立出版，2003 年），等．IEEE，電子情報通信学会等の会員．情報処理学会フェロー．日本セキュリティ・マネージメント学会常任理事，IFIP TC11 日本代表．

吉浦　裕（正会員）

1981 年東京大学理学部情報科学科卒業．同年日立製作所入社．日立研究所，システム開発研究所勤務．2003 年より電気通信大学電気通信学部人間コミュニケーション学科助教授．自然言語処理，知識処理の研究を経て，現在，情報セキュリティ，著作権保護の研究に従事．理学博士．電子情報通信学会，システム制御情報学会，人工知能学会，IEEE 各会員．1990 年情報処理学会学術奨励賞，2004 年度情報処理学会論文賞，2005 年システム制御情報学会産業技術賞受賞．

松木　武

1977 年 3 月東京農工大学大学院工学研究科修士課程修了．同年 4 月日立製作所入社，情報システム事業部，i.e. ネットサービスグループ，情報・通信グループに勤務．2005 年 4 月より，日立電子サービス（株）首都圏支社金融本部副本部長．開発支援システム，証券・保険システムの開発・構築や，IT 関連・セキュリティ関連の新サービス開発に従事．

秦野　康生

1979 年埼玉県生．2004 年東京理科大学大学院理工学研究科修士課程修了．同年（株）日立製作所入社．現在に至るまで，同社システム開発研究所にて，暗号，情報セキュリティの研究に従事．2002 年暗号と情報セキュリティシンポジウム（SCIS2002）論文賞受賞．電子情報通信学会会員．

手塚　悟（正会員）

1984 年慶應義塾大学工学部数理工学科卒業．同年（株）日立製作所入社．マイクロエレクトロニクス機器開発研究所に勤務し，パーソナルコンピュータのオペレーティング・システム，デバイス・ドライバ，LAN システム等の研究開発に従事．その後，システム開発研究所に勤務．以来，パーソナルコンピュータを中心とした LAN システムの構築・運用管理の研究開発，さらにセキュリティシステムの研究開発に従事，現在に至る．東京工科大学非常勤講師（2005 年）．2004 年度情報処理学会論文賞受賞．工学博士．著書に『Inside CORBA』（共訳，アスキー出版，1998 年），『インターネットコマース—新動向と技術』（共著，共立出版，2000 年）『インターネット時代の情報セキュリティ—暗号と電子透かし』（共著，共立出版，2000 年）．

今井　秀樹（正会員）

1966 年東京大学工学部電子工学科卒業．1971 年同大学大学院博士課程修了．工学博士．1972 年横浜国立大学助教授．1984 年同教授．1992 年東京大学教授（生産技術研究所）．2005 年産業総合研究所セキュリティセンター長兼務．現在に至る．この間，符号理論，情報セキュリティ，通信方式等の研究に従事．電子情報通信学会著述賞，論文賞，米澤メダル，猪瀬賞，業績賞，功績賞，IEEE シャノン記念論文賞，総務大臣表彰，経済産業大臣表彰等受賞．著書『情報理論』『符号理論』『暗号のおはなし』等．信学会理事，監事，IEEE 情報理論ソサイエティ会長，国際暗号研究学会理事，情報理論とその応用学会会長，CRYPTREC 委員長等を歴任．IEEE，信学会フェロー．名誉博士（韓国，仏国）．