電子セキュリティトークンとその派生商品

松浦幹太†

情報セキュリティ技術のおかげで，様々な電子トークンが電子取引可能となる．それらのトークンには，たとえば購入時に検証に合格した証明書が使用時にも合格するとは限らないなどの理由により，予測不能な価格変動以外の価値変動リスクが存在する．このような不確定性に起因するリスクに対処する方策として，派生商品の導入によるリスクヘッジがある．残念ながら，完全に電子化されたネットワークの世界では，古典的な理論のモデルや仮定がすべて利用できるとは限らない．本論文は，ネットワーク社会に即したリスク管理理論の基礎を提示し，その工学的応用の可能性を示すことを目的とする．この目的を達成するため，まず電子トークンを抽象化し，価格だけでなく予測不能な時間的変化をする価値も属性として持つセキュリティ・トークン（セトック）としてモデル化する．そして，セトックを特徴づけるための諸性質を定義し，価値に関する基本的な派生商品を導入してその価格評価方程式を導く．さらに単純化された場合の解析解に関する数値評価と，リスク計測への工学的応用について考察する．

Digital Security Token and Its Derivatives

Kanta Matsuura†

With the help of applied cryptography, we can trade various kinds of digital tokens over an open network. In addition to their prices, these tokens have stochastic risk sources; for example, a certificate of a token may be invalid when the owner of the token wishes to use it. A typical strategy to hedge such a risk is the introduction of derivatives. In a completely digitized world, unfortunately, some conventional assumptions and models can no longer be used. The purpose of this paper is to provide a basic framework of network risk management and to show possibilities of its engineering applications. Specifically, we model the digital token as a security token (setok), which has stochastic values as well as its price. A set of setok properties are defined, and then a basic derivative written on the value is priced. In a more simplified case, a closed-form solution of the pricing equation is analyzed in detail. Finally, an indirect measurement of risk parameters is discussed as an application.

1. はじめに

情報セキュリティ技術のおかげで，ネットワークを介して様々な電子トークンが取引可能となる．それらのトークンについて，予測不能な価格変動に起因するリスクが存在しうるのは通常の商品と同様である．しかし，信頼できるディレクトリにすべてのエンティティが実時間アクセスできるとは限らないネットワークの世界では，価格変動以外にも不確定性リスクがともなう．

一例として，公開鍵基盤に基づく一連の電子証明書によって機能が保証されるトークンを考えよう．トークンの購入者は，購入時にすべての証明書を検証し，無効化済み証明書リスト（CRL: Certificate Revocation List）もチェックして，まったく問題がなかったとする．しかしそれでも，実際にそのトークンを利用するときに検証者が行う同様の作業にすべて合格するとは限らない．理由は，いくつか考えられる．まず，購入から利用までの間に一連の証明書のいくつかが有効期限以外の予期せぬ理由で無効になっている可能性がある．また，無効化チェックの精度を上げるため検証にオンラインサーバが必要な実装ならば，サーバが混雑やサービス妨害攻撃で閉塞している可能性もある．あるいはまた，一連の証明書から何らかの信頼度（trust metric）[1)~4)]が算出できるように定義されているシステムならば，トークンを利用しようとしたときにその信頼度が（0 まではいかなくとも）かなり低下しており，もはや利用不可と判定されるかもしれない．信頼度として保険金額に相当する数値が用いられていれば[5),6)]，この利用不可判定は，必ずしもトークンを受け付ける側でなく利用する側でなされる可能性もあ

† 東京大学生産技術研究所・大学院情報学環
Institute of Industrial Science, Interfaculty Initiative in Information Studies, The University of Tokyo

る．いずれにせよ，この種の変化は予測不能であり，リスクが生じる．しかも，利用実績に応じたポイント制度や各種の事前登録会員割引などの複雑な付加的サービスをそれぞれディジタル署名で実現すれば，そのつど付随する証明書に起因するリスクが生じうる．

このような不確定性に起因するリスクに対処する方策として，派生商品の導入によるリスクヘッジがある．従来の金融の世界では，Black-Scholes のオプション価格評価方程式[7]などに触発され，派生商品に関する理論と応用が発展した．しかし残念ながら，完全に電子化されたネットワークの世界では，古典的な理論のモデルや仮定がすべて利用できるとは限らない[8]．本論文は，ネットワーク社会に即したリスク管理理論の基礎を提示し，その工学的応用の可能性を示すことを目的とする．この目的を達成するため，まず 2 章で電子トークンをモデル化する．続いて，その基本的な派生商品を 3 章で定義し，価格評価方程式を導く．4 章では，さらに単純化された場合の数値評価と，リスク計測への工学的応用について考察する．

2. モデル化

2.1 電子流通環境

情報セキュリティ技術のおかげで利用可能となる電子トークンの流通環境を考えよう．特殊な管理業務（たとえば著作権管理や鍵管理，証明書管理，CRL 管理，信用審査など）が必要なため，誰もがトークンを生産・供給できるわけではない．限られたエンティティだけが作成する．業務審査基準を満たして認可を受けたような（少なくともその意味では信頼できる）組織が典型的であろう．トークンに付随する価格以外の重要な数値を価値（value）と呼ぶことにし，不確定価値（implicit value）と呼ばれる確率過程に支配されているとする．トークンには，発行時の不確定価値の実現値（occurrence）に依存した確定価値（explicit value）が書き込まれる．1 つのトークンが複数種類の価値を持つこともありうる．

購買者は信用できない．しかるべき認証を経なければ情報セキュリティの観点から信用できないのは当然であるが，通信回線品質やしたがって不確定価値の把握度，さらには経済的信頼性も高いとは仮定できない．不特定多数の購買者を扱い，しかも匿名性のある電子支払い手段を容認するので，現存の金融機関と顧客の関係のように「事前あるいは事後的に経済的主体としての顧客を特定したり顧客ごとの取引履歴を管理したりすることができる」と仮定することはできない．よって履歴などに数値を記載して任意に細かい額をやりとりすることは仮定せず，トークン単位（1 個，2 個，…）の制約を受けるとするのが自然である．

適切に管理されているため，トークンは一般には複製自由ではない．いったん供給されたら，その後の流通は，無秩序な複製ではなく何らかの取引として実現される．その取引は，確定価格だけでなく確定価値や不確定価値にも依存しうる．

2.2 セキュリティトークン

前節で述べた流通環境を念頭にし，不確定性リスクのある電子トークンを以下のようにセキュリティ・トークン（セトック）としてモデル化する．

定義 2.1（セトック）

セトック（setok: security token）とは，4 つの属性

内容（contents）： 必要ならばメッセージ認証子や電子署名なども含む，

確定価格（explicit price）： 顧客が購入時に支払った非負☆の価格．$\bar{S}$ で表す，

確定価値（explicit values）： 購入時における内容の質を表現する非負の数値の組．$\bar{V}_1, \bar{V}_2, \cdots, \bar{V}_m$ で表す．m を確定価値の**次元**と呼ぶ．各要素 $\bar{V}_i$ が大きければ大きいほど，高い質を表す，

時刻印（timestamp）： 購入時刻 t_0 を信頼できる方式で示す，

を額面に持ち，2 つの確率過程

不確定価格（implicit price）： 非負の確率過程．S で表す，

不確定価値（implicit values）： 非負の確率過程の組．$V_1, V_2, \cdots, V_n$ で表す．n を不確定価値の**次元**と呼ぶ，

と次のように関連づけられているディジタルオブジェクトである．

- 確定価格は**価格解釈過程**（price-interpretation process）$Y(t) = y(t, S(t))$ の購入時における実現値である．価格解釈過程は非負過程である．$y = (t, s)$ は**価格解釈関数**（price-interpretation function）と呼ばれ，s に関して単調増加である．確定価格を書き換えることはできない．
- 確定価値は**価値解釈過程**（value-interpretation processes）$H_1(t) = h_1(t, V_1(t), V_2(t), \cdots, V_n(t))$, $H_2(t) = h_2(t, V_1(t), V_2(t), \cdots, V_n(t)), \cdots, H_m(t) = h_m(t, V_1(t), V_2(t), \cdots, V_n(t))$ の購入時における実現値である．すべての価値解釈過程は非負過程である．$h_1(t, v_1, v_2, \cdots, v_n), h_2(t, v_1, v_2, \cdots,$

☆ ネットワーク社会では，付随させる広告に収入源を求めて無料「配布」されるトークンもビジネスモデルとして存立しうる．そのため，価格 0 のトークンもモデルに含めている．

$v_n), \cdots, h_m(t, v_1, v_2, \cdots, v_n)$ は**価値解釈関数**（value-interpretation functions）と呼ばれる．どの確定価値も，書き換えることはできない．

システムとしてのセトックは，表記法（notation）を明示したいときには $(S, Y; V, H, n, m)$ などと書く．発行済みの個々のデータオブジェクトとしてのセトックは**シェア**（share）と呼ばれ，$(\bar{S}; \bar{V}_1, \bar{V}_2, \cdots, \bar{V}_m; t_0)$ などと表記される．

定義 2.2（一次元価値セトック） セトックは，その確定価値が 1 次元である場合かつその場合に限り，**一次元価値である**（single-valued）といわれる．このとき，添字を省略して $\bar{V} = H(t_0) = h(t_0, V_1(t_0), V_2(t_0), \cdots, V_n(t_0))$ などと書くことができる．

2.3 諸性質定義用の語彙

本節では，個々の具体的なセトックやシェアを特徴づける際に用いる用語を定義する．

定義 2.3（払戻可能性） セトックのシェア $(\bar{S}; \bar{V}_1, \bar{V}_2, \cdots, \bar{V}_m; t_0)$ は，条件「時域 $\boldsymbol{T}$内ならばいつでも，そのシェアを確定価格 $\bar{S}$ で売却できる」が満たされる場合かつその場合に限り，**$\boldsymbol{T}$-払戻可能である**（$\boldsymbol{T}$-refundable）といわれる．$\boldsymbol{T}$は**払戻可能期間**（refundable period）と呼ばれる．払戻可能期間は確定的であるとは限らず，連続的でなくてもよい．確率変数 T_L と T_U を用いて $[T_L, T_U]$，$[T_L, T_U)$，$(T_L, T_U]$，(T_L, T_U) のどの形式でも可能で，それらの集合も可能である．特に，$[t_0, \infty)$-払戻可能である場合には，**無期限払戻可能である**（∞-refundable）といわれる．同じく $[t_0, t_0 + T_R)$-払戻可能である場合には，払戻可能期間の長さ T_R を（太字にせず）用いて T_R-払戻可能（T_R-refundable）と書いてよい．払戻可能期間を特に明示しない場合は，単に「払戻可能」という．

定義 2.4（厳格な払戻可能性） セトックは，以下の 3 つの条件が満たされる場合かつその場合に限り，**厳格に $\boldsymbol{T}$-払戻可能である**（strictly $\boldsymbol{T}$-refundable）といわれる．

- 任意のシェアが払戻可能である．
- どのシェアについても，払戻可能期間は確定的である．
- 所有者は，払戻可能期間外にはいかなる価格でもシェアを売却できない．

特に，厳格に $\emptyset$-払戻可能なセトックは，**払戻不可能である**（unrefundable）といわれる．ここに，$\emptyset$ は空集合である．

価格解釈過程が恒常的に値 0 をとるセトックであっても，著作権管理や倫理的な理由のため払戻不可能なものはありうる．

定義 2.5（取引可能性） 一次元価値セトックのシェア $(\bar{S}; \bar{V}; t_0)$ は，以下の 2 つの条件が満たされる場合かつその場合に限り，**$\boldsymbol{T}$-取引可能である**（$\boldsymbol{T}$-tradable）といわれる．

- $\bar{V} > 0$ である．
- 時域 $\boldsymbol{T}$内ならばいつでも，価値解釈過程が正であって所有者は**価値比例価格**（value-proportional price）

$$S_p = \frac{\bar{V}}{h(t, V_1(t), V_2(t), \cdots, V_n(t))} y(t, S(t))$$

でそのシェアを売却できる．

$\boldsymbol{T}$ は**取引可能期間**（tradable period）と呼ばれる．取引可能期間は確定的であるとは限らず，連続的でなくともよい．特に，$[t_0, \infty)$-取引可能である場合には，**無期限取引可能である**（∞-tradable）といわれる．同じく $[t_0, t_0 + T)$-取引可能である場合には，取引可能期間の長さ T を（太字にせず）用いて T-取引可能（T-tradable）と書いてよい．取引可能期間を特に明示しない場合は，単に「取引可能」という．

定義 2.6（厳格な取引可能性） セトックは，以下の 3 つの条件が満たされる場合かつその場合に限り，**厳格に $\boldsymbol{T}$-取引可能である**（strictly $\boldsymbol{T}$-tradable）といわれる．

- 任意のシェアが取引可能である．
- どのシェアについても，取引可能期間は確定的である．
- 所有者は，取引可能期間外にはいかなる価格でもシェアを売却できない．

特に，厳格に $\emptyset$-取引可能なセトックは，**取引不可能である**（untradable）といわれる．

定義 2.7（オンライン分割可能性） セトック $(S, Y; V, H, n, m)$ は，条件

- 価格解釈課程の実現値が正である時点 $t = t_0$ においては必ず，誰もが任意の**注文価格** (order price) $S_c (> 0)$ を指定して，それに対する**比例確定価値**（proportional explicit values）

$$\frac{S_c}{Y(t_0)} h_i(t_0, V_1(t_0), V_2(t_0), \cdots, V_n(t_0)) \quad (i = 1, 2, \cdots, m)$$

を記載されたシェアを購入できる．

を満たす場合かつその場合に限り，**オンライン分割可能である**（online-divisible）といわれる．オンライン分割可能でないセトックは，**オンライン分割不可能である**（online-indivisible）といわれる．

定義 2.8（オフライン分割可能性） 正の確定価格 $\bar{S}$ を有するシェア $(\bar{S}; \bar{V}_1, \bar{V}_2, \cdots, \bar{V}_m; t_0)$ は，所有

者がそのシェアを**価格比例的に**（price-proportional manner）任意の割合で 2 分割できる場合かつその場合に限り，**オフライン分割可能である**（offline-divisible）といわれる．ここに，価格比例的であるとは，$(\bar{S}^1;\bar{V}_1^1,\bar{V}_2^1,\cdots,\bar{V}_m^1;t_0)$ と $(\bar{S}^2;\bar{V}_1^2,\bar{V}_2^2,\cdots,\bar{V}_m^2;t_0)$ に分割した際に次式が成立することである：

$$\bar{S}^1+\bar{S}^2=\bar{S},\ \bar{S}^1>0,\ \bar{S}^2>0,$$
$$\bar{V}_j^i=\frac{\bar{S}^i}{\bar{S}}\bar{V}_j,\ (i=1,2;j=1,2,\cdots,m)$$

オフライン分割可能でないシェアは，**オフライン分割不可能である**（offline-indivisible）といわれる．

定義 2.7 や定義 2.8 における価格比例性は単純すぎると考える読者もいるかもしれないが，本論文では「複雑な状況は価値解釈関数や価格解釈関数でモデル化する」という立場をとっている．

定義 2.9（価値の失効可応性） セトック $(S,Y;V,H,n,m)$ が 1 つ以上の不確定価値に関して単調増加である価値解釈関数を 1 つ以上持っているとする．それらの不確定価値すべてを $\{V_{j_1},V_{j_2},\cdots,V_{j_s}\}$ とする．このセトックは，$V_{j_1}(t)=V_{j_2}(t)=\cdots=V_{j_s}(t)=0$ であるときかつそのようなときに限って，**失効した**（compromised）といわれる．そして，以下の条件が満足される場合かつその場合に限り，**価値に関して失効可応である**（compromise-responsive in value）といわれる：

- $V_{j_1},V_{j_2},\cdots,V_{j_s}$ のうち 1 つ以上の不確定価値に関して単調増加である任意の価値解釈関数 h_i が，「$V_{j_1}(t)=V_{j_2}(t)=\cdots=V_{j_s}(t)=0$ ならば必ず $H_i(t)=0$ となる」を満たす関数である．

$H_i(t)$ が実現値として 0 をとるとき，そのセトックは i 番目の確定価値に関して**無効化された**（revoked）という．

定義 2.10（価格の失効可応性） セトック $(S,Y;V,H,n,m)$ が 1 つ以上の不確定価値に関して単調増加である価値解釈関数を 1 つ以上持っているとする．それらの不確定価値を $\{V_{j_1},V_{j_2},\cdots,V_{j_s}\}$ とする．このセトックは，以下の条件が満足される場合かつその場合に限り，**価格に関して失効可応である**（compromise-responsive in price）といわれる：

- $V_{j_1}(t)=V_{j_2}(t)=\cdots=V_{j_s}(t)=0$ ならば必ず $Y(t)=0$ である．

3. トークン派生商品

3.1 コールオプション

ネットワーク生活では，支払いも電子的に済ませたいであろう．一般に電子マネーなどの支払い方式では，使用可能な通貨単位のきめ細かさと効率がトレード・オフの関係にある[9]．したがって，購入単位の価格が固定されていれば，利用可能な支払い方式の選択肢が広がる．そこで，ここでは基礎理論の手始めとして，価格解釈過程が単位プロセスである一次元価値セトックを扱う．

従来の金融理論では，取引可能性や分割可能性，そしてショート・ポジション（当該証券を所有していることにしてそれを「売却」し，短期的に無利子で資金を得ること）の可能性が，市場の完備性や効率性を考えるうえで重要である[10)~12)]．しかし我々は，2.1 節で述べた流通環境を念頭に据え，セトックに関しては分割可能性はいっさい仮定せず，ショート・ポジションも許さない．その他の種々の性質も含め，次の仮定を置く．

仮定 3.1（無効化リスクのあるセトック） 本章以降では，以下の性質を満たす一次元価値セトック $(S,Y;V,H,n,1)$ を考察する．

(1) 価格解釈過程は単位プロセス $Y(t)=1$ である．
(2) オンライン分割不可能である．
(3) どのシェアもオフライン分割不可能である．
(4) セトックに対するショート・ポジションは認められない．
(5) T-取引可能であって，取引可能期間の長さ $T=\tau_T(t,H(t))$ は次の確率過程で表される．

$$\tau_T(t,h)=\begin{cases}T_0 & (\text{if } h>0)\\ 0 & (\text{if } h=0)\end{cases}$$

ここに，$T_0>0$ は確定的な正定数である．
(6) T_R-払戻可能であって，払戻可能期間の長さ $T_R=\tau_R(t,H(t))$ は次の確率過程で表される．

$$\tau_R(t,h)=\begin{cases}0 & (\text{if } h>0)\\ T_1 & (\text{if } h=0)\end{cases}$$

ここに，$T_1>0$ は確定的な正定数である．
(7) 失効が起こらない限り，$H(t)$ の実現値は正の有限値である．
(8) 失効は，強度 λ のポアソン過程に従って生起する．
(9) 価値に関して失効可応である（したがって，失効リスクはすなわち無効化リスクとなる）．

価格は一定と仮定したので，価格に関する派生商品を定義することはできない．そこで，価値に関して権利を約束するタイプの派生商品を考える．

定義 3.1（ヨーロッパ型コールオプション） 時刻 $t=t_0$ に発行される**ヨーロッパ型コールオプション**

（European call option）とは，「将来の指定された時刻 $T_m(< t_0 + \min\{T_0, T_1\})$ において当該セトックのシェアを 1 つ，約束した確定価値 K を記載して固定単位価格で購入することができる」という権利を所有者に与える派生商品である．T_m は**満期**（maturity），K は**行使価値**（strike value または exercise value）と呼ばれる．

3.2 価格評価

派生商品は標準化された市場で売買される．そこでは，短期無リスク金利（確定的正定数 r_f とする）の融資が利用でき，派生商品に関するショート・ポジションが許される理想的な市場環境を仮定する．すなわち，派生商品に直接関与するのは大口投資主体であるとする．これは，無体物デリバティブの既存市場を考えても，不自然なことではない．その他の一般的な事項もあわせて，次のような仮定をおく．なお，本論文中の金融用語で不明なものについては，文献 10)〜13) などを参照されたい．

仮定 3.2（市場環境） 本論文では，簡単のため，以下のように単純化した市場環境を考える：

(1) 通信には時間的にも経費的にもコストがかからない．
(2) セトックに関する仮定 3.1 以外には，どの参加者も，取引量の規制を受けない．したがって，銀行と無リスク利率 r_f で任意の金額の資金を出し入れできる．
(3) 無リスク資産の価格過程 B は，方程式 $dB(t) = r_f B(t)dt$ で記述される．
(4) どの時点でも，購買価格と売却価格は同一である．
(5) 裁定取引は存在しない．

さて，満期 T_m のヨーロッパ型コールオプションの価格過程を $C(t)$ とし，価格評価のための連続時間確率過程モデルとして次のようなものを考える．

仮定 3.3（連続時間モデル） 以下の性質が成り立つ状況で関数 $c(t,h)$ を用いて価格過程が $C(t) = c(t, H(t))$ と書けるとする：

- 関数 $c(t,h)$ は $C^{1,2}$-級であって，定義域は $\boldsymbol{R}_+ \times \boldsymbol{R}_{++}$（ただし $\boldsymbol{R}_{++}$ は正の実数の集合，$\boldsymbol{R}_+$ は非負の実数の集合）である．
- 任意の $t \in \boldsymbol{R}_+$ に対して $c(t,0) = 0$ である．
- 価値解釈過程のダイナミクスは次式で与えられる．

$$\begin{aligned} dH = (1 - \lambda(t,H(t))dt)\,\{\mu(t,H(t))Hdt \\ +\sigma(t,H(t))HdW\} \\ +\lambda(t,H(t))dt\cdot(-H) \end{aligned}$$

ただし $\mu(t,H(t))$ と $\sigma(t,H(t))$ はそれぞれドリフト（drift）係数とボラティリティ（volatility）を表す適合過程であって，W は今とっている確率測度（objective measure）の下での Wiener 過程である．適合過程 $\lambda(t,H(t))$ で表されるポアソンジャンプのリスクは系統的（systematic）である．

- 適合過程 $G(t) = \{H(t)\}^{-1}$ を定義し，対応する実現を $g = 1/h$ と書く．c を t と g の関数と見なす場合に混乱を避けるため，$\hat{c}(t,g) = c(t,1/g)$ という表記法を用いる．関数 $\hat{c}$ も $C^{1,2}$-級であるとする．

$c(t,0) = 0$ であることは，不確定価値の失効に起因する無効化がオプションを無意味にするということを表現している．

Wiener 過程に関してよく知られている関係式 $dt \cdot dt = 0$ と $dt \cdot dW = 0$ を用いれば，H のダイナミクスは次式のように書き直すことができる．

$$dH = (\mu - \lambda)Hdt + \sigma HdW \tag{1}$$

セトックのシェア 1 つと M 個のオプションから成るポートフォリオを考える．長さ dt の十分短い期間の期初に

$$F = 1 + MC \tag{2}$$

を支払ってポートフォリオを構成する．仮定 3.1，仮定 3.2，仮定 3.3 を用いれば，F のダイナミクス

$$\begin{aligned} dF = \{M(\hat{c}_t - \mu G\hat{c}_g + \sigma^2 G\hat{c}_g + \frac{\sigma^2}{2}G^2\hat{c}_{gg} \\ -\lambda\hat{c}) + \lambda - \mu + \sigma^2\}dt \\ -\sigma\,(MG\hat{c}_g + 1)\,dW \end{aligned} \tag{3}$$

を得ることができる．ここに，下付の添字はその添字変数による偏微分を表す．さらに仮定 3.2 を用いれば，

$$M = -\frac{1}{G\hat{c}_g}, \tag{4}$$

を満たすようにオプション量を選び，

$$\begin{aligned} M\left(\hat{c}_t - \mu G\hat{c}_g + \sigma^2 G\hat{c}_g + \frac{\sigma^2}{2}G^2\hat{c}_{gg} - \lambda\hat{c}\right) \\ +\lambda - \mu + \sigma^2 \\ = r_f F(t) \\ = r_f(1 + MC) \end{aligned} \tag{5}$$

が成り立てば無裁定環境下での無リスクポートフォリオを構成できる．無効化が生起しない限り式 (4) を式 (5) に代入した方程式が G の任意の実現値について成り立つので，偏微分方程式

$$\frac{\sigma^2}{2}g^2\hat{c}_{gg} + (r_f - \lambda)\,g\hat{c}_g - (r_f + \lambda)\hat{c} + \hat{c}_t = 0 \tag{6}$$

を境界条件

$$\hat{c}(T_m, g) = \max\{0, Kg - 1\} \ (0 < g < \infty) \quad (7)$$

の下で解けばよい．この結果は，次の定理のようにまとめることができる．

定理 3.1（価格評価の境界値問題） 無裁定条件を満たす $C(t) = c(t, H(t))$ という形の価格過程は，

$$c(t,h) = \begin{cases} \hat{c}(t, 1/h) & \text{for } h > 0 \\ 0 & \text{for } h = 0 \end{cases}$$

に限られる．ただし $\hat{c}(t,g)$ は境界値問題

$$\frac{\sigma^2}{2} g^2 \hat{c}_{gg} + (r_f - \lambda)\, g \hat{c}_g - (r_f + \lambda)\hat{c} + \hat{c}_t = 0$$
$$\hat{c}(T_m, g) = \max\{0, Kg - 1\}$$

の定義域 $[0, T_m] \times \boldsymbol{R}_{++}$ における解である．

4. 考　　察

4.1 失効リスクのない場合の解析解

価値に関して書かれたオプションの基本的な性質を考察するため，本節では，解析解導出の容易な単純化した状況を考える．すなわち，失効リスクがなく（$\lambda = 0$）係数 μ と σ が確定的定数という状況で，境界値問題を解く．証明書は認証にパスするかどうかという 2 値的な判断であるから，失効リスクなしで価値の微妙な時間変動を考察しても無意味であると考える読者もいるかもしれない．しかし，より一般的な「複数の認証局がネットワークをなし，信頼度（trust metric）[1)~4)]が定義されているシステム」を考えれば，考察する意味はある．

境界値問題を解いた結果として，次の定理が得られる．

定理 4.1（単純化された状況のオプション価格） μ と σ が確定的定数であって，かつ，$\lambda = 0$ ならば，オプション価格は次式で与えられる：

$$c(t,h) = \frac{K}{h} N\left[d_1(t,h)\right] - \exp\left\{-r_f(T_m - t)\right\} N\left[d_2(t,h)\right]$$

ただし N は正規分布の累積分布関数

$$N[d] = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{d} \exp\left(-\frac{x^2}{2}\right) dx$$

であって，

$$d_1(t,h) = \frac{1}{\sigma\sqrt{T_m - t}} \times \left\{ \ln\left(\frac{K}{h}\right) + \left(r_f + \frac{\sigma^2}{2}\right)(T_m - t) \right\},$$
$$d_2(t,h) = d_1(t,h) - \sigma\sqrt{T_m - t}.$$

である．

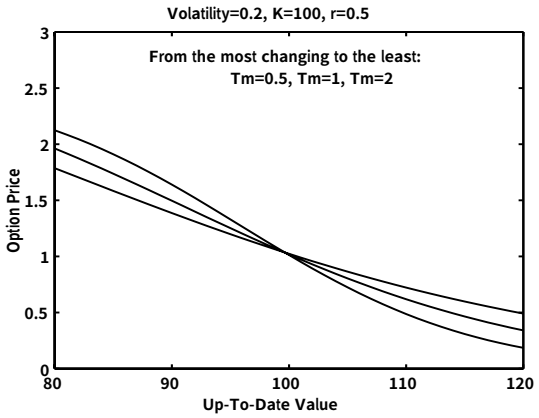

図 1 現在価値に対するオプション価格の変化．右下がりグラフの変化が激しいものから順に，満期を $T_m = 0.5$，1，2 とした場合の様子を示している

Fig. 1 Option price against up-to-date value of the setok. The curves for the maturities $T_m = 0.5$, 1, and 2 are shown. Further maturities bring less changing curves.

ここで，$H(0) \in [80, 120]$ の範囲で様々なパラメータ値に対して $C(0)$ を計算し，定理 4.1 で与えられる解析解の性質を数値的に調べる．以降では，$C(0), H(0)$ をそれぞれ単に C，H と書く．1 年を時間の単位とし，無リスク利率 r_f は

$$r = \exp(r_f) - 1 \quad (8)$$

によって年率 r に換算する．基本的なパラメータ設定は以下のとおりである：

満期： $T_m = 1$ [year]
ボラティリティ： $\sigma = 0.2$
行使価値： $K = 100$
無リスク利率： $r = 0.5$ [%]

パラメータを動かす着眼点を変えて，3 つの図を示す．どの図でも，横軸 H の値（セトックの現在価値）に対して縦軸にオプション価格 C をプロットし，単調減少のグラフが得られている．これは，行使価値を固定すれば，現在価値が低ければ低いほどオプションが有利になるためである．

まず，満期 T_m を $T_m = 0.5$，1，そして 2 とした場合の結果を**図 1** に示す．満期が遠ければ遠いほど，直感的には，不確かさが増す．この影響が，オプション価格の（現在価値に対する）変化を緩和している．すなわち，現在価値が行使価値より小さい領域 $H < K = 100$ では大きな T_m の方が低いオプション価格をもたらしており，現時点でのオプションの有利さが（小さな T_m と比べて）相対的に小さい．逆に，現在価値が行使価値より大きい領域 $H > K = 100$ では大きな T_m の方が高いオプション価格をもたらして

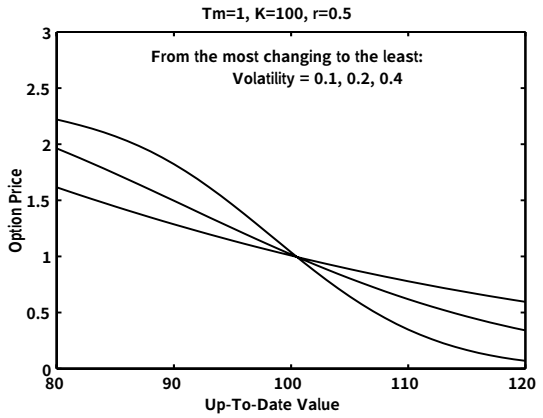

図 2 現在価値に対するオプション価格の変化．右下がりグラフの変化が激しいものから順に，ボラティリティを $\sigma = 0.1$，0.2，0.4 とした場合の様子を示している

Fig. 2 Option price against up-to-date value of the setok. The curves for the volatilities $\sigma = 0.1$, 0.2, and 0.4 are shown. Larger volatilities bring less changing curves.

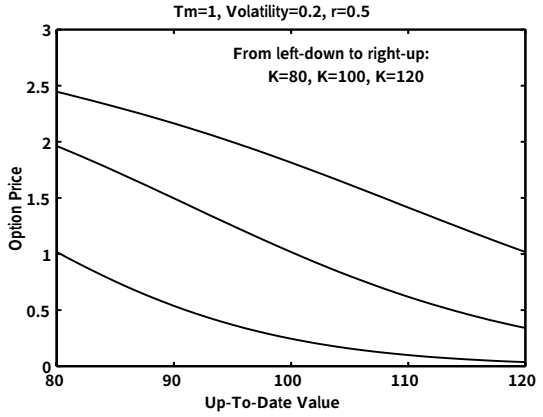

図 3 現在価値に対するオプション価格の変化．行使価値を $K = 80$，100，120 とした場合のグラフをそれぞれ示す．行使価値が高いほどオプション価格も高い

Fig. 3 Option price against up-to-date value of the setok. The curves for the exercise values $K = 80$, 100, and 120 are shown. Higher exercise values mean currently better positions of the option holders, and hence bring higher option prices.

おり，現時点でのオプションの不利さが（小さな T_m と比べて）相対的に小さい．

次に，価値の変動の激しさを表現するボラティリティを $\sigma = 0.1$，0.2，0.4 としてその影響を調べた結果を**図 2** に示す．ボラティリティが大きいほど直感的には不確かさが増し，先ほどと同様に，オプション価格の（現在価値に対する）変化の程度が緩和されている．

最後に，行使価値を $K = 80$，100，120 としてその影響を調べた結果を**図 3** に示す．行使価値が大きい方がオプションが有利となるので，高いオプション価格が得られている．

4.2 リスク計測への応用

まだ起きていない無効化のリスクを表すパラメータ λ の値をネットワーク社会がどうとらえているか，合理的に知る方法はあるだろうか．リスク調査として最も簡便なものは意見を求めるアンケート調査だが，残念ながら主観の入り込む余地がきわめて大きい．そのような主観的要素を避けるため，直接計測はできなくても推定いわば間接計測の方法を構築したい．本節では，本論文で導入した価格評価のアプリケーションとして，この間接計測法について簡単に考察する．すなわち，λ 以外のパラメータが市場観測から得られている場合に λ を推定する問題である．

λ が既知でオプション価格 C が未知ならば，定理 3.1 の境界値問題を数値的に解いて C を求めればよい．これを順方向の計算とすれば，今考えている C が既知で λ が未知の問題は，逆問題である．最も単純な逆問題解法は，次のように C の観測値と計算値の誤差を繰返し計算で十分小さくする方法である．

（方法 1）（1） 最近の市場観測データから r_f，σ を定める．

（2） リスク λ の初期推定値を定める．

（3） 現在の市場観測値 H とリスク推定値を入力して，定理 3.1 からオプション価格の計算値を得る．

（4） オプション価格の計算値と現在の観測値の誤差が十分小さいかどうかを調べる．着目しているセトックについて，満期や行使価値の異なるオプション銘柄が複数あれば，それらのデータをすべて用いて各銘柄に関する誤差の二乗和を考える．

（5） 誤差が十分小さければ終了し，現在の推定値を解とする．

（6） 誤差がまだ十分小さくなければ，リスク推定値を修正して同様のプロセスを繰り返す．直感的には，オプション価格の計算値が観測値と比べて高過ぎる傾向にあればリスク推定値を上方修正して計算値を下げるようにする．これは，無効化が起きればオプションが無意味（オプションを行使してセトックを購入しても，同じ価格の払戻が可能なだけであって，ペイオフは 0）となってしまうからである．

繰返し計算の回数や，方法 1 のステップ (3) で解く境界値問題の数値解法に求める精度次第では，十分

迅速にリスク推定値が得られないかもしれない．しかし，リスクがある値 λ^* を超えているかどうかを知りたいだけならば，繰返しをせずに済ますことができる可能性がある．すなわち，方法1のステップ(6)で用いた着眼点を利用して，次のような方法を考える．

（方法2） (1) 方法1のステップ(3)に同じ．

(2) $\lambda = \lambda^*$ とする．

(3) 現在の市場観測値 H と $\lambda = \lambda^*$ を入力して，定理3.1からオプション価格の計算値を得る．

(4) オプション価格の計算値が現在の観測値よりも高いかどうかを調べる．着目しているセトックについて，満期や行使価値の異なるオプション銘柄が複数あれば，それらのデータをすべて用いて統計的検定で判別する．

(5) 計算値が高いと判別されれば，リスクが λ^* よりも高いと判断する．

なお，本節は応用の可能性を指摘することが目的なので概略のみを述べたが，実際に測定する場合には測定期間の設定が問題となる．特に，理想的な市場環境で十分長い測定期間を確保した場合と比べ実証研究で用いた測定期間がどの程度誤差を生むかを評価する感度解析が，将来の重要な研究課題となろう．また，その際には精度と効率のトレードオフが予想される．よって，何らかの最適化問題を解いたり，大量の実証研究によって経験的な数値設定のノウハウを検討したりする研究がなされると予想される．

5. おわりに

本論文では，情報セキュリティ技術を応用したネットワーク取引で避けられないであろうリスクについて基礎理論を展開し，応用の可能性の1つを示した．理論で用いるモデル化では，取引される電子トークンを，価格以外にも予測不能な時間的変化をする価値を属性として持つオブジェクトとして定義した．このオブジェクトをセトックと名付け，その諸性質を定義した．既存の金融取引の世界との違いに留意しつつ本質を逃さない範囲でできる限り単純化したセトックの価値に関して，リスクをヘッジする派生商品としてヨーロッパ型コールオプションを定義した．そして，セトックの無効化リスクを系統的なリスクであると仮定して，オプション価格を決める方程式を導出した．

無効化リスクなどがないと単純化した状況では，方程式の解析解を導出し，オプション価格の基本性質を調べた．結果は，「将来の不確かさが増せば現在の有利さや不利さが緩和される」という直感的理解のできるものであった．

無効化リスクのある場合には，オプション価格評価理論の応用として，そのリスクの間接計測法を簡単に考察した．主観の入り込む余地が大きいアンケート調査と比べて，間接計測法はその客観性だけでなく，自動化できる可能性という利点がある．詳細は今後様々な研究が必要となろうが，「情報セキュリティシステムで知りたいけれども今までは知る術のなかったパラメータ」を間接的にでも計測できる可能性を示したという点が重要である．この間接計測のためには，逆問題解法アルゴリズムを考えるという工学的な研究が必要である．計測に適したオプション契約を設計するという研究に発展すれば，さらに工学的要素が増すと予想される．

情報セキュリティは，本質的に社会科学と無縁ではありえない．実際，社会科学的な分析の重要性は，近年，より強く認識されるようになっている[14),15)]．また，経済的損失補償システムに関する研究の重要性も指摘されるようになっている[16)]．本論文から得られる重要な教訓は，このような学際的研究が分析（analysis）だけでなく設計・統合（synthesis）の方向性ももちうるということである．

参考文献

1) Maurer, U.: Modelling a Public-Key Infrastructure, *Computer Security — ESORICS'96*, Bertino, E., Knuth, H., Martella, G. and Montolivo, E. (Eds.), Lecture Notes in Computer Science 1146, pp.325–350, Springer-Verlag, Berlin, New York, Tokyo (1996).
2) Essin, D.J.: Patterns of Trust and Policy, *Proc. New Security Paradigms Workshop '97*, pp.38–47 (1997).
3) Reiter, M.K. and Stubblebine, S.G.: Resilient Authentication using Path Independence, *IEEE Trans. Comput.*, Vol.47, No.12, pp.1351–1362 (1998).
4) Kohlas, R. and Maurer, U.: Confidence Valuation in a Public-Key Infrastructure Based on Uncertain Evidence, *Proc. 3rd International Workshop on Practice and Theory in Public Key Cryptosystems* (*PKC 2000*), Imai, H. and Zheng, Y. (Eds.), Lecture Notes in Computer Science 1751, pp.93–112, Springer-Verlag, Berlin, New York, Tokyo (2000).
5) Reiter, M.K. and Stubblebine, S.G.: Toward acceptable metrics of authentication, *Proc. 1997 IEEE Symposium on Security and Pri-*

vacy, pp.10–20 (1997).
6) Reiter, M.K. and Stubblebine, S.G.: Authentication Metric Analysis and Design, *ACM Trans. Information and System Security*, Vol.2, No.2, pp.138–158 (1999).
7) Black, F. and Scholes, M.: The Pricing of Options and Corporate Liabilities, *Journal of Political Economy*, Vol.81, May-June, pp.637–654 (1973).
8) Matsuura, K.: Digital Security Tokens and Their Derivatives, *7th International Conference of the Society for Computational Economics* (*SCE'01*), New Haven, CT (2001).
9) Eng, T. and Okamoto, T.: Single-Term Divisible Electronic Coins, *Advances in Cryptology — EUROCRYPT'94*, Santis, A.D. (Ed.), Lecture Notes in Computer Science 950, pp.306–319, Springer-Verlag, Berlin, New York, Tokyo (1995).
10) Merton, R.C.: *Continuous-Time Finance* (Revised Edition), Blackwell Publishers, Cambridge, MA (1992).
11) Björk, T.: *Arbitrage Theory in Continuous Time*, Oxford University Press, New York (1998).
12) ジョン・ハル（著），東京三菱銀行金融商品開発部（訳）：ファイナンシャルエンジニアリング〈第4版〉—デリバティブ商品開発とリスク管理の総体系，金融財政事情研究会，東京 (2001).
13) ジョン・C・ハル（著），小林孝雄（監訳），株式会社オーパス・ワン（訳）：先物・オプション取引入門，ピアソン・エデュケーション，東京 (2001).
14) 佐々木良一，宝木和夫：印鑑と電子印鑑の歴史と類似性の分析，情報処理学会論文誌，Vol.42, No.8, pp.1968–1974 (2001).
15) 山根信二，村山優子：暗号技術を位置づける社会的枠組みについての考察，情報処理学会論文誌，Vol.42, No.8, pp.1975–1982 (2001).
16) 山根信二，白田秀彰，辰己丈夫：保険におけるセキュリティ格付け機関についての検討，コンピュータセキュリティシンポジウム 2001（CSS2001）論文集，情報処理学会シンポジウムシリーズ，Vol.2001, No.15, pp.253–258 (2001).

(平成 13 年 11 月 28 日受付)
(平成 14 年 6 月 4 日採録)

松浦 幹太（正会員）

昭和 44 年生．平成 9 年東京大学大学院工学系研究科電子工学専攻博士課程修了．同年東京大学生産技術研究所助手．平成 10 年同講師．平成 12 年 4 月東京大学大学院情報学環講師（生産技術研究所兼担）．平成 12 年度英国ケンブリッジ大学客員研究員．平成 14 年 4 月東京大学大学院情報学環助教授（生産技術研究所兼担）．情報セキュリティ，ネットワークプロトコル，電子商取引等の研究に従事．博士（工学）．著書に「情報セキュリティ概論」（共著，昭晃堂，1999），「ネットワークセキュリティ—学術情報の発信と保護」（共著，丸善，1999）等．電子情報通信学会，IEEE，ACM，Society for Computational Economics 各会員．