第5回バイオメトリクスと認識・認証シンポジウム
2015年11月12日〜13日（東京大学　本郷キャンパス　武田先端知ビル）

計算機能力のエイジングと不正者のエフォートによる安全性への影響を考慮した計算量的安全性の定式化

Formularization of Computational Security with consideration of Aging of CPU Performance and Effort of Attackers

神農泰圭 † 兼子拓弥 † 本部栄成 † 高橋健太 ‡ 西垣正勝 †
† 静岡大学 ‡ 株式会社日立製作所

Yasuyoshi JINNO† Takuya KANEKO† Eisei HONBU†
Kenta TAKAHASHI‡ Masakatsu NISHIGAKI†
†Shizuoka University ‡Hitachi, Ltd.

アブストラクト　計算量的安全性に基づくセキュリティシステムにおいては，CPU の計算機能力の時間的変化 (エイジング要因) と不正者の計算コスト (エフォート要因) の両方を考慮して秘密情報のエントロピを確保する必要がある．そこで本稿では，現在の計算量的安全性の定式化を拡張し，エイジング/エフォートの各要因に対応する安全性を切り分けて扱える枠組みを提案する．この結果，「不正者が負担する計算コスト」に対して「安全となる秘密情報のエントロピ」をある時点で決定してやれば，将来計算機能力が向上しても秘密情報のエントロピを一定に保ったまま安全性を維持することが可能となる．なお，本稿は CSS2014 の内容 [1] がベースとなっている．

1　はじめに

計算量的安全性に基づくセキュリティシステムにおいては，CPU の計算機能力の時間的変化 (エイジング要因) と不正者の計算コスト (エフォート要因) の両方を考慮して秘密情報のエントロピを確保する必要がある．しかし，計算機能力の進化は，不正者，正規ユーザの両者に恩恵を与えるものであるため，時間的に変化することのない安全性の決定要因として，エフォート要因こそが本質的に重要であろう．

また，従来の計算量的安全性の定式化では，エイジング要因，エフォート要因を 1 つのセキュリティパラメータで表している．そのため，従来の定式化では，「その時代の計算機能力に応じた計算コストの負担を不正者にも正規ユーザにも一律に要求する」という考えに基づいたセキュリティシステム（bcrypt [2] や PBKDF2 [3]，計算機援用ユーザ認証 [4] など）の安全性を適切に表現することができない．

そこで本稿では，エイジング/エフォートの各要因に対応する 2 つのセキュリティパラメータを導入した定式化，秘密情報のエントロピがエフォート要因のみに依存する仕組みの定式化を行う．エイジング要因については，その時代の計算機能力に応じた計算コストの負担を不正者にも正規ユーザにも一律に要求することによって，必要なエントロピを補填する方式に変更する．秘密情報の情報源が限られる場合（パスワード，生体情報，PUF など）や，秘密情報の記録容量が限られる場合（軽量チップなど）など，CPU の進化に従って秘密情報のエントロピを増加させることが困難であるアプリケーションにおいては，本定式化が特に有効であると期待される．

2　新しい計算量的安全性の定式化

計算量的安全性の従来の定式化と，本稿で提案する新しい定式化をまとめたものを表 1 に示す．

従来の定式化では，セキュリティパラメータは k のみであり，正規ユーザの所持している秘密情報は $p\,(k[bit])$ である．正規ユーザ，不正者の計算能力は，任意の多項式時間アルゴリズム $Poly(k)$ によりモデル化される．$Adv(k)$ は不正者の優位性であり，「当て推量で攻撃した場合の成功確率と，$Poly(k)$ で努力する不正者の成功確率との差分」で定義される．

従来の定式化に対して，セキュリティパラメータをエフォート要因に対応する k_u とエイジング要因に対応する k_r という 2 つに分離したのみ（$k = k_u|k_r$）である定式化が，表 1 のパラメータ分離型である．

パラメータ分離型の定式化に対して，エイジング要因に関する k_r については，「その時代の計算機能力に応じた計算コストを不正者にも正規ユーザにも一律に要求する」という仕組みを導入することにより，表 1 の相対型となる．k_r に対応する秘密情報 p_r は，セキュリティシステムを使用する際に，その都度，相応の計算コストを払って正しい値を発見するという形式となるため，不正者，正規

ユーザ両者の計算能力が $Poly(k_u, k_r) \cdot SPoly(k_r)$ に変わる．$SPoly(k_r)$ とは，k_r に対する任意の多項式より漸近的に大きな関数である．正規ユーザは，p_r を覚える必要はなくなり，それに伴い不正者の優位性の定式化も $Adv(k)$ から $Adv(k_u)$ となる．$Adv(k_u)$ が無視できるほど小さい場合（ε (k_u) 未満）に，計算量的安全性が保証される．

3 新定式化の具体例

3.1 従来の計算量的安全性

従来型では，$k[bit]$ の秘密情報に対し，不正者が $A[bit]$ 分の情報を分析する能力を有している場合，$Adv(k) = 1/2^{k-A} - 1/2^k$ であり，$Adv(k) < \varepsilon$ (k) となるように，k の大きさを設定する必要がある．

3.2 パスワードベース鍵生成関数

bcrypt および PBKDF2 はパスワードを入力として暗号鍵を出力する関数である．反復演算回数を可変とすることにより，不正者の攻撃試行の速度を減速させ，入力のエントロピの不足を補っている．

bcrypt の計算手順を要約すると，P（パスワード），S（ソルト），c（コスト）を入力し P，S の暗号化を 2^c 回繰り返し，暗号化された P，S を用いて，シード文字列を ECB モードで暗号化する作業を 64 回繰り返す．その結果を鍵として出力する．ここで，P のビット長を n_p として，相対型の定式化に当てはめると $k_u = n_p$，$k_r = c$ となり，計算能力は，$Poly(n_p) \cdot 2^c$ となる．

一方 PBKDF2 の計算手順を要約すると，P（パスワード），S（ソルト），c（反復回数）を入力し P，S を任意のハッシュ関数に入力し，U_1 を得て，P，U_1 を同じハッシュ関数に入力し，U_2 を得て，P，U_2 を再び同じハッシュ関数に入力し，U_3 を得る．これを，U_c を得るまで繰り返す．そして，U_1〜U_c の排他的論理和を求め，これを鍵として出力する．ここで，P のビット長を n_p，反復回数 c については $n_c = \log_2 c$ として相対型の定式化に当てはめると $k_u = n_p$，$k_r = n_c$ となり，計算能力は，$Poly(n_p) \cdot 2^{n_c}$ となる．

$k_u[bit]$ の秘密情報に対し，不正者が 2^{k_r} 回の演算を繰り返しながら，$A[bit]$ 分の情報を分析する能力を有している場合，$Adv(k_u) = 1/2^{k_u - A} - 1/2^{k_u}$ であり，$Adv(k_u) < \varepsilon$ (k_u) となるように，k_u の大きさを設定する必要がある．

3.3 計算機援用ユーザ認証

計算機援用ユーザ認証とは，認証情報の一部を総当たり試行によって求めるという認証方法である．手順を要約すると，登録フェーズにて $H(H(P))$ が認証サーバに登録されており，サーバはクライアント端末に $H(H(P))$ を送信し，ユーザはクライアント端末に，P_u を入力する．クライアント端末は $H(H(P_u|P_r))$ と $H(H(P))$ が一致するような P_r を総当たり試行によって探索し，一致した P_r を用いて，$H(P_u|P_r)$ を求め，サーバに送信し，サーバは $H(H(P_u|P_r))$ と $H(H(P))$ が一致したらユーザを認証する．ここで，$H(\cdot)$ はハッシュ関数である．P_u，P_r のビット長をそれぞれ n_u，n_r として相対型の定式化に当てはめると $k_u = n_u$，$k_r = n_r$ となり，計算能力は，$Poly(n_u + n_r) \cdot 2^{n_r}$ となる．

計算機援用ユーザ認証における，$k_u[bit]$ の秘密情報に対する $Adv(k_u)$ については，3.2 節と同様である．

4 まとめと今後の課題

セキュリティパラメータをエイジング要因とエフォート要因に切り分けて扱う枠組みを提案した．従来の計算量的安全性の定式化を相対型へ拡張し，既存のパスワードベース鍵生成関数や計算機援用ユーザ認証の計算量的安全性を記述することができた。今後は，生体認証システムに対して，本定式化に基づいた検討を行っていく．

参考文献

[1] 兼子拓弥他,“計算機能力のエイジングと不正者のエフォートによる安全性への影響を考慮した計算量的安全性の定式化” **コンピュータセキュリティシンポジウム** *2014* **論文集**, No. 2, pp.442-449, Oct., 2014.

[2] Provos,N. and Mazieres,D. ,“A Future-Adaptable Password Scheme” *Annual Technical Conference 1999*, Jun., 1999.

[3] Turan,M. , Barker,E. , Burr,W. and Chen,L. ,“NIST Special Publication 800 -132 Recommendation for Password -Based Key Derivation”

[4] 兼子拓弥他,“計算機援用ユーザ認証” **情報処理学会論文誌**, Vol. 55, No. 9, pp.2072-2080, Sep., 2014.

表 1: 計算量的安全性の定式化のまとめ

	従来型	パラメータ分離型	相対型
セキュリティパラメータ	k	k_u，k_r	k_u，k_r
秘密情報	$p(k[bit])$	p_u，p_r(それぞれ $k_u, k_r[bit]$)	$p_u(k_u[bit])$
正規ユーザの計算能力	$Poly(k)$	$Poly(k_u, k_r)$	$Poly(k_u, k_r) \cdot SPoly(k_r)$
不正者の計算能力	$Poly(k)$	$Poly(k_u, k_r)$	$Poly(k_u, k_r) \cdot SPoly(k_r)$
不正者の優位性	$Adv(k)$	$Adv(k_u, k_r)$	$Adv(k_u)$