8

リスク工学シリーズ

暗号と情報セキュリティ

工学博士 岡本 栄司
博士（工学） 西出 隆志
共著

コロナ社

刊行のことば

世界人口は現在65億人を超え，わずか100年で4倍にまで増加し，今も増え続けています。この間の経済成長は，日本を例にとると44倍にまで達しています。現代社会は約80万年の人類史上から見ると凄(すさ)まじい成長を遂げており，その成長はグローバル化の進展と技術革新によって加速されています。

膨張し続ける社会の人間活動によって世界の持続可能な発展が懸念されています。地球規模ではエネルギーの大量消費による地球環境問題や資源ナショナリズムが台頭し始めています。一方，国レベルでは都市化の進展によって交通渋滞，地震や洪水被害の拡大，水・環境汚染といった問題が発生しています。また，変化の速さがあまりにも速いために経済や技術の格差が社会にもたらされています。そういったひずみは世界各国にさまざまなリスクを生み出しています。グローバル経済による金融リスク，グローバル化した人や物の移動によるBSEや鳥インフルエンザなどの感染症リスク，情報化によるサイバーリスクなど人為的なリスクも広がっています。リスクの不確実性と影響の大きさは増大する傾向にあり，それぞれが複雑に絡み合っています。

世界が持続可能な発展を遂げていくためには，地球規模かつ地域で直面しているさまざまなリスクを解決していくための処方箋を何枚も何枚もつくり，解決に向けて行動していかなければなりません。また，多様なリスクを科学的・工学的な方法により解明できる能力をもった研究者や技術者の養成も求められています。

そういった社会のニーズに応えるために，筑波大学では2002年に全国の大学で初めてリスク工学専攻を設置しました。専攻の教育目標として，① リスク工学の解析と評価のための基礎理論と情報処理技術の習得，② 現実のリスク問題

についての豊富な知識の習得，③ リスク問題に対して広い視野と強いリーダーシップをもって問題設定から解決までの一連のプロセスを理解し，具体的な解決手段を考案・開発する能力育成，を掲げています。設立から 6 年が経ちカリキュラムも次第に充実してきており，これを機会に，本専攻で実施されている教育内容を本学以外の多くの学生や研究者にも役立たせたいと考えました。

本シリーズ発行の目的は，社会のリスク問題を工学の立場から解決していくことに関心のある人々に役立つテキストを世に出すことです。本シリーズは全 10 巻から構成されています。1 巻から 4 巻まではリスク問題を総論的に捉えており，リスク工学の勉強を登山に例えれば，1 巻は「登山の楽しさ」，2 巻は「どんな山があるのか」，3 巻は「山に登るための道具」，そして 4 巻は「実際に登るときの道具の使い方」に対応しています。5 巻から 10 巻までは各論として，「トータルリスクマネジメント」，「環境・エネルギーリスク」，「サイバーリスク」，「都市リスク」の四つの専門分野からリスク工学の基礎と応用を幅広く紹介しています。

本シリーズは，大学生や大学院修士課程の学生はもとより，リスクに関心のある研究者や技術者，あるいは一般の人々にも興味をもっていただけるよう工夫した画期的なものです。このシリーズを通じて，読者がリスクに関する知識を深め，安全で安心した社会をどのように築いていけばよいかを考えていただければ幸いです。

2008 年 2 月

リスク工学専攻長　内山 洋司

ま　え　が　き

現代のネット社会において，情報セキュリティはキーテクノロジの一つであることは間違いない。ネットワークはきわめて重要なインフラであるが，それを有用にするもしないも情報セキュリティ次第である。ネットワークがすべてのものに浸透しつつある現在，もしセキュリティで守られていなかったらどうなるであろうか。すべての機器が丸見えである。機器の数は膨大だからチェックしきれないと思うかもしれないが，現在の検索能力からすればどうということはない。個人情報も丸見えだけでなく，個人がどこでなにをしたかも一目瞭然である。クラウドももちろんセキュリティなしには成立しえない。情報セキュリティ技術があるからこそ，ネット社会が成り立っているのである。

しかし，それで100%守れるわけではないことに注意する必要がある。100%に近づくと急激に費用が上昇するため，実現不可能となる。そこで，リスク的な考え方が必要となってくる。リスクでは確率を加味して議論する。本リスク工学シリーズではさまざまな分野におけるリスク工学手法を提供しているが，本書の「暗号と情報セキュリティ」もその重要な応用の一つとなる。例えば暗号技術を例にとってみよう。非常に解読に強い暗号はいくらでも作ることができる。しかし，度がすぎると処理時間がかかるようになり装置も大きくなってしまう。それでも，100%完全とは言えない。鍵長が k ビットなら 2^k 通りのパターンを全数探索すれば解読可能なので，k を大きくすれば解読成功の可能性は限りなく小さくなるが完全に零ではない。リスク的考え方が必要となるゆえんである。

さて，本書ではリスク工学の一環として情報セキュリティ技術を取り上げる。じつは情報セキュリティといっても対象は広く，全部をカバーするには何冊もの解説書が必要となる。そこでここでは，核となる技術，すなわち「暗号技術とその周辺」を中心に，その基礎と応用を解説していく。

Part Ⅰの基礎編では暗号技術の基礎をわかりやすく解説する。Part Ⅱの応用編ではまず一般論として情報セキュリティの必要性，すなわち情報に対する脅威を述べ，つぎにその対策を解説する。さらには標準化動向についても触れる。また暗号だけでなく，関連するネットワークセキュリティについてもある程度カバーしていく。

なお，本書の執筆は，Part Ⅰを西出が，Part Ⅱを岡本が担当した。

本書は情報セキュリティを専門にしている人を対象にしているが，大学や大学院の教科書として使えるように記述してある。皆様のお役に立てれば幸いである。

2016 年 3 月

岡本　栄司

目　　次

—— Part I（基礎編）——

1.　暗号の数学的基礎

2.　公開鍵暗号の構成と関連技術

3. 暗号の安全性

4. 素　数　生　成

5. ゼロ知識対話証明と秘匿計算

—— Part II（応用編）——

6. 情報に対する脅威事例

7. 情報セキュリティ対策技術の応用

8. 標　準　化

— Part I（基礎編）—

1 暗号の数学的基礎

本章では情報セキュリティの基盤技術の一つである暗号について，公開鍵暗号を中心に，その基礎となる数学的知識について述べる。公開鍵暗号技術はネットワーク上での安全性確保に必要な認証や電子署名などの要素技術となっており，暗号を専門としない研究者や技術者にとってもその概念を正しく理解することは重要と考える。

本章では数学的に厳密な記述は必ずしも追求せず，例を含めた直観的な記述も多く用いている。それにより初学者が，公開鍵暗号の数理的側面の理解に必要な最小限の知識を，短期間で得ることを目的としている。

暗号研究は，セキュリティ基盤技術として社会への大きな貢献をなし得るという実用的な重要性と同時に，理論的な美しさももち，魅力的でパズルを解くような楽しさをもつ研究分野である（と筆者らは感じている）。本書で基礎知識を得ることで，暗号研究に興味を抱かれた読者には，より高度な暗号技術や，本書で触れなかった内容を含む論文，文献[†1]などで，さらに暗号研究に触れられることを期待する。

1.1 モジュロ演算

公開鍵暗号の世界で利用するモジュロ演算[†2]について説明する。これは割り

---

†1 例えば巻末の文献7), 13), 23), 24), 27), 29), 32), 35), 36), 41), 42), 44), 47)〜49), 64) などがある。

†2 剰余演算，mod 計算など呼び方は複数ある。

算と余りからなる計算の世界である。まず記号 | について説明する。

$$n|a$$

と書くとき整数 n が整数 a を割り切ることを意味する。例えば $4|8$ である。

つぎにモジュロ演算でよく使用される $\equiv$ という記号について説明する。整数 a, b, n があるとき

$$a \equiv b \bmod n$$

は $n|(a-b)$ が成り立つことを意味する。別の言い方をすると a と b は n で割ったときに余りが同じであるともいえる。例えば以下が成り立つ。

$$17 \equiv 7 \bmod 5$$

ときに誤解を招かない状況では $\equiv$ の代わりに $=$ が用いられる場合もある。ときに以下のような表記も行う。

$$7 \bmod 5 = 2$$

簡単に確認できることとして，例えば以下のようなことが成り立つ。

$$a \equiv a \bmod n$$

$$a \equiv b \bmod n \Rightarrow b \equiv a \bmod n$$

$$a \equiv b \bmod n \ \wedge \ b \equiv c \bmod n \Rightarrow a \equiv c \bmod n$$

mod n の計算では n が 0 となる世界を考え，n で割った余りを値として用いるため n 種類の数のみが存在すると想像するとわかりやすい。つまり，$\{0, 1, 2, \cdots, n-1\}$ の種類の値のみが存在すると考えるとわかりやすい†。例え

† 暗号研究では場合によっては，（ここでは n が奇数として）$\{0,\ 1,\ 2, \cdots,\ n-1\}$ の代わりに $\left\{-\dfrac{n-1}{2}, -\dfrac{n-1}{2}+1, \cdots, -1,\ 0,\ 1, \cdots, \dfrac{n-1}{2}-1, \dfrac{n-1}{2}\right\}$ を考えることもある。

ば mod 5 の世界を考えたとき，7 は 5 を引いて 2 と考えればよく，−1 は 5 を足して 4 と考えればよい（つまり 7 は 2 と，−1 は 2 と同一視する）。つまり mod 5 の世界では 5 = 0 と考え，ある値に 5 を足したり引いたりしてもその値の意味は変わらないのだと直観的には理解するとよい[†1]。

また簡単に確認できるが以下のようなことも成り立つ。

$$(a_1 + a_2) \bmod n \equiv \{a_1 \bmod n + a_2 \bmod n\} \bmod n$$

$$(a_1 - a_2) \bmod n \equiv \{a_1 \bmod n - a_2 \bmod n\} \bmod n$$

$$(a_1 \times a_2) \bmod n \equiv \{a_1 \bmod n \times a_2 \bmod n\} \bmod n$$

つまり余りを計算する処理は，途中の計算結果に行っても，最後に行ってもよいということである（計算結果はどちらで行っても変わらない）。

以下に加算の例を見てみよう（mod 5 の場合）。

$$(7 + 8) \bmod 5 \equiv 15 \bmod 5 \equiv 0 \bmod 5$$

これは最後に余りを計算した例である。つぎに

$$(7+8) \bmod 5 \equiv (7 \bmod 5 + 8 \bmod 5) \equiv (2+3) \bmod 5 \equiv 5 \bmod 5 \equiv 0 \bmod 5$$

これは 7 + 8 を計算する前に 7 と 8 に対して余りを先に計算している例である[†2]。また別の例として

$$3^3 \equiv 27 \equiv 2 \bmod 5$$

であり

$$3^3 \equiv 9 \times 3 \equiv 4 \times 3 \equiv 12 \equiv 2 \bmod 5$$

となる（$9 \equiv 4 \bmod 5$，$10 \equiv 0 \bmod 5$ であることを使った）。

†1 そのような計算が成り立つ数学的構造を公開鍵暗号では扱う。
†2 厳密に証明しなくても，このような例から直観的には成り立つことが理解できよう。

1.2 最大公約数

ここではモジュロ演算に関連する知識として**最大公約数**（gcd，greatest common divisor）について復習する。

ここでは記号 gcd を以下のように使う。例えば $\gcd(15, 21) = 3$ である。これは $15 = 3 \times 5$, $21 = 3 \times 7$ より明らかである。つまり最大公約数は，この例の場合 15 と 21 の両方を割り切る最大の整数である。

また例えば $\gcd(8, 15) = 1$ である。このように gcd が 1 の場合，8 と 15 は「たがいに素」であるという。

gcd の定義より $\gcd(a,\ b) = \gcd(b,\ a)$ は明らかである。

じつは，最大公約数はこのような素因数分解を行わなくても求めることができる。その方法は**ユークリッド互除法**と呼ばれている。ユークリッド互除法は以下の性質を用いている。

$$\gcd(a,\ b) = \gcd(b,\ a \bmod b)$$

これは以下のように証明できる。

証明　a を b で割った商を q，余りを r としたとき $a = qb + r$ となる。よって $a \bmod b = r$ である。よってここで示したいことは $\gcd(a,\ b) = \gcd(b,\ r)$ である。

いま $d_1 = \gcd(a,\ b)$ としよう。$r = a - qb$ であるから r は d_1 の倍数であり，$d_1 | r$ である。また $d_1 | b$ でもある。よって $d_1 \leqq \gcd(r,\ b)$，つまり

$$\gcd(a,\ b) \leqq \gcd(b,\ r) \tag{1.1}$$

である。つぎに $d_2 = \gcd(b,\ r)$ としよう。$a = qb + r$ であるから a は d_2 の倍数であり，$d_2 | a$ である。また $d_2 | b$ である。よって $d_2 \leqq \gcd(a,\ b)$，つまり

$$\gcd(b,\ r) \leqq \gcd(a,\ b) \tag{1.2}$$

である。式 (1.1) と (1.2) より $\gcd(a,\ b) = \gcd(b,\ r)$ がいえる。　□

この性質を使うと，例えば $\gcd(63, 27)$ は以下のようなアルゴリズムで計算できる（素因数分解を必要としないことに注意されたい）。

$$\gcd(63,27) = \gcd(27, 63 \bmod 27) = \gcd(27,9) = \gcd(9, 27 \bmod 9)$$
$$= \gcd(9,0) = 9$$

1.3 拡張ユークリッド互除法

モジュロ計算の世界での乗算に関する逆数を考える[†1]。通常整数の世界では $8 \times x = 1$ となるような整数 x は存在しない。では mod 11 の世界ではどうだろうか。つまり，$8 \times x \equiv 1 \bmod 11$ となる整数 x は存在するだろうか。

例えば $8 \times 7 \equiv 1 \bmod 11$ であることが確認できる。

一般的に $a \times a' \equiv 1 \bmod n$ であるとき a' は a の**逆数**（あるいは**逆元**）といい，a^{-1} という記号で表す。つまり

$$a \times a^{-1} \equiv 1 \bmod n$$

である[†2]。

公開鍵暗号の計算において a と n が与えられたときに，a^{-1} を計算しなければならないことがしばしばある。a と a^{-1} は整数上においては定義より

$$a \cdot a^{-1} + k \cdot n = 1 \tag{1.3}$$

を満たしている。ここで k もある整数である。つまり a と n から a^{-1} を計算することは，式 (1.3) を満たすような整数 a^{-1} と k を計算することと同じである。

ここでまず a が a^{-1} をもつ条件を考えてみよう。式 (1.3) より $\gcd(a,n) = 1$ であることが必要であることがわかる。なぜなら $\gcd(a,n) \neq 1$ であれば式 (1.3) の右辺は $\gcd(a,n)$ の倍数となり，1 とはなりえないからである。また $\gcd(a,n) = 1$ であれば，後述する拡張ユークリッド互除法により式 (1.3) を満たす整数 a^{-1}, k を求めることができ，a は mod n で逆数 a^{-1} をもつ。

[†1] a の加算に関する逆数 x は，$a + x \equiv 0 \bmod n$ となる x で簡単に $-a$ と計算できる。例として，$3 + x \equiv 0 \bmod 5$ なる 3 の逆数 x は $-3 (\equiv 2 \bmod 5)$ である。

[†2] 乗算は $a \cdot a^{-1} \equiv 1 \bmod n$ のように書くこともある。

索　　引

—— 著者略歴 ——

岡本　栄司（おかもと　えいじ）

1973 年　東京工業大学工学部電子工学科卒業
1978 年　東京工業大学大学院理工学研究科博士課程修了（電子工学専攻）
　　工学博士（東京工業大学）
1978 年　日本電気株式会社勤務
1992 年　北陸先端科学技術大学院大学教授
1999 年　東邦大学教授
2002 年　筑波大学教授
2016 年　筑波大学名誉教授

西出　隆志（にしで　たかし）

1997 年　東京大学理学部情報科学科卒業
1997 年　日立ソフトウェアエンジニアリング株式会社（現株式会社日立ソリューションズ）勤務
2003 年　南カリフォルニア大学修士課程修了
2008 年　電気通信大学大学院電気通信学研究科（社会人博士課程）単位取得退学
　　博士（工学）（電気通信大学）
2009 年　九州大学助教
2013 年　筑波大学准教授
　　現在に至る

暗号と情報セキュリティ
Cryptography and Information Security

2016 年 5 月 2 日　初版第 1 刷発行　★

検印省略

著　者　岡本　栄司
　　西出　隆志
発行者　株式会社　コロナ社
　　代表者　牛来真也
印刷所　三美印刷株式会社

112–0011　東京都文京区千石 4–46–10
発行所　株式会社　**コロナ社**
CORONA PUBLISHING CO., LTD.
Tokyo Japan
振替 00140–8–14844・電話(03)3941–3131(代)
ホームページ　http://www.coronasha.co.jp

ISBN 978–4–339–07928–9　（高橋）（製本：愛千製本所）
Printed in Japan