

電子政府行政情報化事業

将来の暗号技術に関する安全性要件調査

調査報告書



2004 年 2 月
独立行政法人 情報処理推進機構

目 次

第 1 章 背景と目的.....	1
第 2 章 前提条件.....	3
第 3 章 既存事例・研究.....	4
3.1 DES 解読コンテスト	4
3.2 DES Cracker (1998 年)	4
3.3 共通鍵暗号の安全な鍵長に関する研究事例.....	6
3.3.1 Lenstra & Verheul (1999 年)	6
3.3.2 暗号利用技術ハンドブック (2000 年)	10
3.3.3 Silverman (2000 年)	12
3.4 まとめ.....	12
第 4 章 予測モデル.....	13
4.1 共通鍵暗号の解読法.....	13
4.2 解読計算システム.....	14
4.3 予算.....	17
第 5 章 予測モデルにおける要素パラメータの予測.....	18
5.1 鍵探索チップに関する予測.....	18
5.1.1 鍵探索チップの価格	18
5.1.2 鍵探索チップの集積度およびクロック周波数.....	18
5.1.3 鍵探索回路の規模と性能	19
5.1.4 鍵探索チップの単価当たり性能	21
5.2 予算.....	23
5.2.1 経済規模最大国の GDP 予測.....	24
5.2.2 世界の GDP 予測.....	24
5.2.3 予算の予測値	25
5.3 解読計算時間および許容解読確率.....	26
第 6 章 予測結果.....	27
6.1 安全な鍵長の計算式.....	27

6.2 安全な鍵長の下限の計算結果.....	28
第7章 考察.....	30
7.1 ブロック長.....	30
7.2 価格性能の過剰見積りの程度.....	31
7.2.1 価格性能見積りの精度.....	31
7.2.2 価格性能の比較（対：DES 解読専用マシン）.....	32
7.2.3 価格性能比較（対：汎用 MPU、スパコン）.....	33
7.3 解読専用マシン以外の解読計算システム.....	36
7.4 運用費用について.....	36
7.5 イノベーティブ計算方式による解読について.....	37
参考文献・URL	39
付録 A 半導体技術ロードマップについて	41
A.1 半導体技術ロードマップとは.....	41
A.2 最新の技術ロードマップ	41
A.3 最新の技術ロードマップの概要.....	42
A.4 参考：ムーアの法則の限界について	42
付録 B スパコン性能のトレンド	44
B.1 過去からのトレンド	44
B.2 現状と今後の方向	46
付録 C 機密保持期間内の安全性の確保.....	48

第1章 背景と目的

本調査は、暗号技術の安全性を脅かす一つの要因である計算機の処理能力の増大に注目して、10～15年先の暗号技術の安全性に関する要件を調査することを目的とする。本調査で対象とするのは、最も幅広く用いられている共通鍵ブロック暗号である。

暗号の安全性を脅かす主な要素としては、

- (1) 暗号アルゴリズムの脆弱性（設計上の瑕疵など）
- (2) 攻撃法の進歩（既存攻撃法の改良、新たな攻撃法の開発）
- (3) 計算機性能の向上（解読計算能力の増大）
- (4) 運用上の脆弱性（不適切な使用法、鍵の漏洩、など）

がある。

これらのうち、項目(1)および(2)は、CRYPTREC¹の暗号技術評価委員会において調査検討がなされており、また(4)については、個々の用途・システムにおける運用の問題である。運用ガイドラインも整備されつつある。本調査の目的は、項目(3)を検討することである。

以上をまとめると、本調査の趣旨は以下の通りとなる。

- ・ 計算機性能の向上に伴って、解読計算能力が増大して行く。
- ・ 計算量的安全性に基づく暗号の安全性を確保するためには、暗号強度は時間とともに増して行かなければならない。
- ・ 共通鍵ブロック暗号を対象として、このことを具体的に検討する。

本調査は、暗号技術分野および計算機分野の専門家をメンバーとする「暗号技術の安全性要件検討会議」により実施され、検討結果を基に本報告書が取りまとめられた。「暗号技術の安全性要件検討会議」の参加者は以下の通りであった。

¹ Cryptography Research & Evaluation Committees の略称で、電子政府で安全に利用できる暗号技術の評価を目的として、2000年度からプロジェクトが開始された。総務省及び経済産業省が事務局を務める暗号技術検討会と情報処理振興事業協会(IPA)及び通信・放送機構(TAO)が事務局を務める暗号技術評価委員会から構成され、2003年2月に「電子政府推奨暗号リスト」が公表された。

有識者(暗号技術分野)	
金子 敏信	東京理科大学 理工学部 電気電子情報工学科 教授
花岡 悟一郎	東京大学 生産技術研究所
有識者(計算機分野)	
近山 隆	東京大学 新領域創成科学研究科 教授
中島 浩	豊橋技術科学大学 情報工学系 教授
石川 裕	東京大学 大学院情報理工学系研究科 助教授
関口 智嗣	(独)産業技術総合研究所 グリッド研究センター長

第2章 前提条件

本調査において以下のような前提条件を置く。

◆ 暗号に関する前提

- 暗号方式は、共通鍵ブロック暗号とする。
- 共通鍵ブロック暗号における個別の暗号アルゴリズムは仮定しない。
- 想定する共通鍵ブロック暗号は、ショートカット攻撃法が無いことを仮定する。すなわち、全数探索による攻撃よりも効率的な攻撃が存在しないものとする。全数探索による攻撃とは、鍵空間に属する全ての鍵について、それを用いて暗号文を復号し、有意性検定（復号結果が求める平文であるかどうかを判定）するものである。平均的には、（鍵の全数 $\times$ 1 回の復号時間 $\div 2$ ）の時間があれば、鍵を求めることができる。

◆ 計算機性能の予測に関する前提

- 半導体ベースの現状の計算機技術の延長を前提とする。
シリコン半導体に替わる計算機技術（量子計算、DNA 計算、バイオ計算などの「イノベーティブ計算方式」[1]）については、現在、基礎研究が進んでいるが、まだ実用化の目途が立っていないため、今回の調査対象とはしない。
- 現時点の見通しでは、過去 30 年余りの計算機性能向上の最大要因であったシリコン半導体集積技術の進歩は、今後 10 年以上継続するとされている。（より定量的に言えば、半導体集積度の向上速度に関するムーアの法則は、若干のスローダウンは伴うが、今後最低 10 年は継続すると予想されている。）

◆ 解読に用いる計算機資源に掛けられるコストについての前提

- 安全性の検討において、単一の解読予算を設定するのではなく、想定解読予算に対して安全な暗号強度を求められるような計算式を導くものとする。
- 例示的に、大規模な解読予算を想定した場合の暗号強度を示す。
（世界全体の 1 年間の GDP を上限とした。）

第3章 既存事例・研究

本章では、共通鍵暗号の全数探索による解読に関する主な研究事例を記す。

3.1 DES 解読コンテスト

DES 解読コンテスト (DES Challenge[2]) は、RSA Security 社が実施した、公開の DES 解読コンテストである。

当コンテストは、DES 暗号[3]による暗号文 (CBC モードで暗号化) 平文の最初の数十文字および初期ベクタが与えられ、暗号鍵を発見するという問題 (既知平文攻撃) である。

表 3-1に第 1 回～第 4 回 DES 解読コンテストの結果概要を示す ([11] P112, [4])。DES が公開で全数探索によって解読されたのは、第 1 回 DES 解読コンテストが初めてである。

表 3-1 DES 解読コンテストの結果

	コンテスト開始日	解読方法	平均鍵検証個数/秒	解読時間 (鍵全体に対する 検証した鍵個数比率)
第 1 回	1997/ 1/28	約 1 万台の PC	約 17 億個	約 140 日 (約 25%)
第 2 回	1998/ 1/13	約 4 万台の PC	約 184 億個	約 40 日 (約 88%)
第 3 回	1998/ 7/13	DES Cracker	約 888 億個	約 56 時間 (約 25%)
第 4 回	1999/ 1/18	DES Cracker + 10 万台の PC	約 2450 億個	22 時間 15 分 (約 27%)

3.2 DES Cracker (1998 年)

DES Cracker は、DES 解読用に設計された専用マシンで、Electronic Frontier Foundation (EFF)が中心となり、DES 暗号の安全性の不十分さを証明する目的で開発された[6]。詳細設計・実装は、

- ・ Cryptography Research 社 (ハード/ソフト設計)
- ・ Advanced Wireless Technologies 社 (チップデザイン、実装)

が担当した[7]。

DES Cracker は、全数探索による攻撃を行い、DES の平均解読時間 1 週間以内を設計目標とした。

実際に、DES Cracker は、1998 年の第 3 回 DES 解読コンテストにおいて、56 時間で暗号文を解読し、第 4 回 DES 解読コンテストではさらに性能を向上させた[5]。

以下に、DES Cracker のハードウェアの概要を述べる。

DES Cracker の要は DES 解読用の専用チップである。専用チップは、カスタムチップで、CMOS 0.8 μ m ルール、動作周波数は 40 MHz である。チップには探索ユニットが 24 個実装されている。² 暗号利用モードは、ECB モードの他に、CBC モードもサポートする[6][8]。

探索ユニットは、DES のラウンド数と等しい 16 クロックで一つの鍵をテストすることができる。したがって、探索ユニットの鍵探索性能は $40\text{M}/16 = 2.5 \text{ M 鍵/秒}$ であり、チップ全体の鍵探索性能は 60M 鍵/秒 となる。

さらに、基板 (VME バス基板サイズ) 上に、64 チップを実装し、1 つのラックに 12 枚の基板を収納している。DES Cracker 全体は、2 個ラックからなる。

DES Cracker 全体のチップ数は、 $64 \times 12 \times 2 = 1536$ チップであり、全体性能は $64\text{M} \times 12 \times 2 = 921$ 億 6 千万鍵/秒となる。

DES Cracker の構築コストは、21 万ドルと報告されており、その内訳は、設計・組立・テスト 8 万ドル、ハード直接経費 13 万ドルである。チップ当たりで換算すると、137 ドル (設計等含む) ないし 84.6 ドル (ハード直接経費のみ) となる。後者をドル当たり性能に換算すると、709K 鍵/秒・ドルとなる。

なお、DES Cracker は、製造された 1998 年時点の最新技術を用いていない。仮に、1998 年の半導体先進技術 (300MHz, 210nm) を用い、同じ回路を実装できたとすると、性能は約 109 倍となる。また、大量生産により同一コストでチップ製造できたとすれば、ドル当たり性能も約 109 倍となる (77.2M 鍵/秒・ドル)。

この高性能探索チップを使って、100 億ドル (約 1 兆円。13 万ドルの 7.7 万倍) の予算を掛ければ (ただし、設計費用、システム化コストを無視) 全体性能は約 800 万倍となる。これは 79 ビット鍵を平均 1 週間以内に解読可能な性能である。³

²探索ユニットの回路サイズは直接の記述ないが、チップ集積度を 4M トランジスタとすると、探索ユニット回路規模は $4\text{M}/24 = 166\text{K}$ トランジスタとなる。

³ 鍵長が長くなることによる、探索回路の規模増大を無視した場合。

3.3 共通鍵暗号の安全な鍵長に関する研究事例

3.3.1 Lenstra & Verheul (1999 年)

A. K. Lenstra と E. R. Verheul は、共通鍵ブロック暗号と公開鍵暗号の商用目的での安全な鍵長の下限を、将来に向けて予測する研究を行った [9]。これらの暗号の安全性は、解読のために膨大な計算量を必要とすることによっているが、毎年 of 計算機性能の向上に伴って、解読能力が向上するため、安全を保証するための鍵長も長くなる。

当論文では、検証可能な客観的モデルを設定し、適当と考えられるパラメータ (デフォルト・パラメータ) を挿入して、結果を外挿するという単純明快な方法で、安全な鍵長のデータを具体的に求めている。

以下、同論文の予測モデルと予測結果を紹介する。

◆ モデル

鍵長の決定は以下に依存する。

1. 寿命 (Life span): いつまで安全であるべきか
2. 安全マージン (Security margin): 攻撃が成功しない度合い
3. 計算環境 (Computing environment): 暗号解読に使える計算資源の予想
4. 暗号解析 (Cryptanalysis): 暗号解析技術の予想される進歩

それぞれに関する仮定は次の通りである。

(a) 寿命 (Life span)

- ・ 安全性を確保すべき期間を x 年とする。同論文の出版された 1999 年を起点として、 $1999 + x$ 年までの安全性を確保するという要件である。

(b) 安全マージン (Security margin)

- ・ 利用者や目的によって安全マージンが異なるため、パラメータとして与えられるようにする。
- ・ 具体的には「DES の安全性を西暦 y 年まで信頼する」という形で、安全マージンを設定する。

ここで、 $y \geq 1977$ (DES 標準が制定されたのは 1977 年) である。 y のデフォルトは 1982 とする。 $y = 1982$ とは、「1982 年における DES の安全性と同等な安全性を要請する」という意味になる。)。

なお、1982 年とは、1977 年に FIPS 標準となった DES に対する 5 年毎の安全性見直しの初回の年に当たる。

(c) 計算環境 (Computing environment)

- ・ Moore の法則 (IC の集積度は 18 ヶ月毎に倍増する) の非技術的な解釈「1 ドル当たりの計算能力とメモリ量は 18 ヶ月毎に倍増する」を採用する。
- ・ もう一つの仮定: 解読用計算環境に掛けられる予算額は 10 年で倍増する。
(10 年で 2 倍は年率 7.1% 成長に相当する。)

(d) 暗号解析 (Cryptanalysis)

- ・ 以下のような理想化された共通鍵ブロック暗号アルゴリズムを仮定する:
 - ・ DES と同等の暗号化 / 復号速度。
 - ・ 任意のビット数を鍵長にできる。
 - ・ 鍵空間の全数探索より高速な攻撃がない。

◆ 鍵長決定モデルの適用

- ・ 問題: 1999 + x 年における安全な鍵長を求める。
要求する安全性は西暦 y 年における DES の安全性と同等とする。
- ・ 計算
 - $z = 1999 + x - y$ と置く。1999 + x 年は、 y 年と比べて、
 - ◇ 1 ドル当たり $2^{\frac{12}{18}z} = 2^{\frac{2}{3}z}$ 倍の計算能力が得られる。
 - ◇ 暗号攻撃予算額は $2^{\frac{1}{10}z}$ 倍だけ増加している。
 - ◇ 対象となるブロック鍵暗号の復号速度は DES の復号速度と同等。
 - 暗号攻撃は $2^{\frac{2}{3}z + \frac{1}{10}z} = 2^{\frac{23}{30}z}$ 倍だけ強力になっている。
 - 鍵空間のサイズは $2^{\frac{23}{30}z}$ 倍だけ大きくなければならない。
- ・ 結論
 - DES (有効鍵長 56 ビット⁴) より $\frac{23}{30}z$ ビット大きい鍵長を使う必要がある。

当モデルに従った 1999 年から 2040 までの安全な鍵長の予測結果を表 3-2 に示す。一番左の列は西暦年であり、次の列は上記計算で求められた共通鍵暗号の安全な鍵長である。(3 列目以降は公開鍵暗号の安全な鍵長である。参考のため含めた。)

⁴ DES の鍵長は 64 ビットだが、8 ビットがパリティなので、有効鍵長は 56 ビットである。

表 3-2 安全な鍵長 (Lenstra & Verheul)

Year	Symmetric Key Size	Classical Asymmetric Key Size (and SDL Field Size)	Subgroup Discrete Logarithm Key Size	Elliptic Curve		Infeasible number of Mips Years	Lower bound for Hardware cost in US \$ for a 1 day attack (cf. (4.5))	Corresponding number of years on 450MHz PentiumII PC
				Key Size				
				progress				
				no	yes			
1999	70	915 672	123	130	130	$4.19 * 10^9$	$1.29 * 10^8$	$9.31 * 10^6$
2000	70	952 704	125	132	132	$7.13 * 10^9$	$1.39 * 10^8$	$1.58 * 10^7$
2001	71	990 736	126	133	135	$1.21 * 10^{10}$	$1.49 * 10^8$	$2.70 * 10^7$
2002	72	1028 768	127	135	139	$2.06 * 10^{10}$	$1.59 * 10^8$	$4.59 * 10^7$
2003	73	1068 800	129	136	140	$3.51 * 10^{10}$	$1.71 * 10^8$	$7.80 * 10^7$
2004	73	1108 832	130	138	143	$5.98 * 10^{10}$	$1.83 * 10^8$	$1.33 * 10^8$
2005	74	1149 864	131	139	147	$1.02 * 10^{11}$	$1.96 * 10^8$	$2.26 * 10^8$
2006	75	1191 896	133	141	148	$1.73 * 10^{11}$	$2.10 * 10^8$	$3.84 * 10^8$
2007	76	1235 928	134	142	152	$2.94 * 10^{11}$	$2.25 * 10^8$	$6.54 * 10^8$
2008	76	1279 960	135	144	155	$5.01 * 10^{11}$	$2.41 * 10^8$	$1.11 * 10^9$
2009	77	1323 1024	137	145	157	$8.52 * 10^{11}$	$2.59 * 10^8$	$1.89 * 10^9$
2010	78	1369 1056	138	146	160	$1.45 * 10^{12}$	$2.77 * 10^8$	$3.22 * 10^9$
2011	79	1416 1088	139	148	163	$2.47 * 10^{12}$	$2.97 * 10^8$	$5.48 * 10^9$
2012	80	1464 1120	141	149	165	$4.19 * 10^{12}$	$3.19 * 10^8$	$9.32 * 10^9$
2013	80	1513 1184	142	151	168	$7.14 * 10^{12}$	$3.41 * 10^8$	$1.59 * 10^{10}$
2014	81	1562 1216	143	152	172	$1.21 * 10^{13}$	$3.66 * 10^8$	$2.70 * 10^{10}$
2015	82	1613 1248	145	154	173	$2.07 * 10^{13}$	$3.92 * 10^8$	$4.59 * 10^{10}$
2016	83	1664 1312	146	155	177	$3.51 * 10^{13}$	$4.20 * 10^8$	$7.81 * 10^{10}$
2017	83	1717 1344	147	157	180	$5.98 * 10^{13}$	$4.51 * 10^8$	$1.33 * 10^{11}$
2018	84	1771 1376	149	158	181	$1.02 * 10^{14}$	$4.83 * 10^8$	$2.26 * 10^{11}$
2019	85	1825 1440	150	160	185	$1.73 * 10^{14}$	$5.18 * 10^8$	$3.85 * 10^{11}$
2020	86	1881 1472	151	161	188	$2.94 * 10^{14}$	$5.55 * 10^8$	$6.54 * 10^{11}$
2021	86	1937 1536	153	163	190	$5.01 * 10^{14}$	$5.94 * 10^8$	$1.11 * 10^{12}$
2022	87	1995 1568	154	164	193	$8.52 * 10^{14}$	$6.37 * 10^8$	$1.89 * 10^{12}$
2023	88	2054 1632	156	166	197	$1.45 * 10^{15}$	$6.83 * 10^8$	$3.22 * 10^{12}$
2024	89	2113 1696	157	167	198	$2.47 * 10^{15}$	$7.32 * 10^8$	$5.48 * 10^{12}$
2025	89	2174 1728	158	169	202	$4.20 * 10^{15}$	$7.84 * 10^8$	$9.33 * 10^{12}$
2026	90	2236 1792	160	170	205	$7.14 * 10^{15}$	$8.41 * 10^8$	$1.59 * 10^{13}$
2027	91	2299 1856	161	172	207	$1.21 * 10^{16}$	$9.01 * 10^8$	$2.70 * 10^{13}$

Year	Symmetric Key Size	Classical Asymmetric Key Size (and SDL Field Size)	Subgroup Discrete Logarithm Key Size	Elliptic Curve		Infeasible number of Mips Years	Lower bound for Hardware cost in US \$ for a 1 day attack (cf. (4.5))	Corresponding number of years on 450MHz PentiumII PC
				Key Size				
				progress				
				no	yes			
2028	92	2362 1888	162	173	210	$2.07 * 10^{16}$	$9.66 * 10^8$	$4.59 * 10^{13}$
2029	93	2427 1952	164	175	213	$3.52 * 10^{16}$	$1.04 * 10^9$	$7.81 * 10^{13}$
2030	93	2493 2016	165	176	215	$5.98 * 10^{16}$	$1.11 * 10^9$	$1.33 * 10^{14}$
2031	94	2560 2080	167	178	218	$1.02 * 10^{17}$	$1.19 * 10^9$	$2.26 * 10^{14}$
2032	95	2629 2144	168	179	222	$1.73 * 10^{17}$	$1.27 * 10^9$	$3.85 * 10^{14}$
2033	96	2698 2208	169	181	223	$2.95 * 10^{17}$	$1.37 * 10^9$	$6.55 * 10^{14}$
2034	96	2768 2272	171	182	227	$5.01 * 10^{17}$	$1.46 * 10^9$	$1.11 * 10^{15}$
2035	97	2840 2336	172	184	230	$8.53 * 10^{17}$	$1.57 * 10^9$	$1.90 * 10^{15}$
2036	98	2912 2400	173	185	232	$1.45 * 10^{18}$	$1.68 * 10^9$	$3.22 * 10^{15}$
2037	99	2986 2464	175	186	235	$2.47 * 10^{18}$	$1.80 * 10^9$	$5.49 * 10^{15}$
2038	99	3061 2528	176	188	239	$4.20 * 10^{18}$	$1.93 * 10^9$	$9.33 * 10^{15}$
2039	100	3137 2592	178	189	240	$7.14 * 10^{18}$	$2.07 * 10^9$	$1.59 * 10^{16}$
2040	101	3214 2656	179	191	244	$1.22 * 10^{19}$	$2.22 * 10^9$	$2.70 * 10^{16}$

出典：Arjen K. Lenstra, Eric R. Verheul, "Selecting Cryptographic Key Sizes", 1999.

いくつかの補足を記す。

◆ 鍵当たりの暗号化 / 復号の計算量

Lenstra-Verheul 論文では、鍵当たりの攻撃に要する計算量（暗号化ないし復号、および結果チェックのための計算量）は、DES と同等と仮定しているが、実際には、攻撃対象となるブロック鍵暗号に依存する。したがって、具体的な予測においては、用いる暗号アルゴリズムの鍵当たり攻撃時間が DES に対する攻撃時間と比較して、どの程度の比率であるかを見積もる必要がある。

Lenstra-Verheul 論文では、実測値から 450MHz Pentium II (PC) による DES 攻撃に要する時間を 1200 年としている。Pentium II プロセッサにおいてクロック当たり平均 2 命令が実行されるとすると、 $1200 \times 450 \times 2 = 1,080,000$ となるので、DES の鍵空間全体の探索計算量を 1MMY (Million MIPS Year) としている。

◆ モデルのパラメータ

Lenstra-Verheul の予測モデルのパラメータには、計算機価格性能の伸び率、解読予

算の成長率、安全性の基準などのパラメータに関する仮定がある。これらは、必要に応じて変更することができる。Lenstra と Verheul の予測表は、妥当と思われる一つのパラメータセットによる計算結果を示したものである。

Lenstra-Verheul 論文は、妥当な仮定に基づいた定量的モデルを提示しており、目的に応じてパラメータ変更も可能であるなど、予測モデルとして優れている。同論文は、その後、後述の「暗号利用技術ハンドブック」、欧州の NESSIE プロジェクトの第 1 次評価資料[10]などで参照されており、妥当な予測として認められていると言えよう。

同論文への批判としては、RSA 社の R.D.Silverman のものがある[12]。これについては3.3.3節で触れる。

3.3.2 暗号利用技術ハンドブック（2000 年）

電子商取引推進協議会⁵（ECOM）セキュリティ WG による「暗号利用技術ハンドブック（第 2 版）」[11]は、その 5 章で暗号の安全性を扱っており、共通鍵ブロック暗号の安全な鍵長に関する検討が記述されている。

同ハンドブックでは、安全性を評価するための前提条件を次のように定めている。

◆ 暗号の安全性を評価する際の前提条件

- アルゴリズム高速化に関する仮定
 - ・ DES に対するアルゴリズム高速化の程度は最大 100 倍程度であり、ビット換算では最大 7 ビット程度となる。
- 線形解読法による計算量の低減に関する仮定
 - ・ 最大 12 ビット分程度
（DES では、線形解読法によって、約 12 ビット分だけ探索空間が小さくなったことを根拠とする。）
- 解読法に関する仮定
 - ・ 効率の良い解読法が極力無いように設計されている。
- 計算機性能に関する仮定
 - ・ 計算機性能は「同一コストで 18 ヶ月で 2 倍になる」という Moore の法則が、これまでも、今後も成り立つ。

⁵ ハンドブック出版当時の名称は「電子商取引実証推進協議会」である。

同ハンドブックでは、鍵長を 90 ビットとした場合に、いくつかの予算規模を想定した総当り法による共通鍵暗号の解読時間がまとめられている（表 3-3）。

表 3-3 鍵空間探索時間（鍵長 = 90 ビット）

攻撃者	個人	企業	国家
予算	100 万円	10 億円	1 兆円
解読装置	1000 台の P C 又は F P G A	F P G A / A S I C	A S I C
1995 年	257 億年	20 万年	196 年
1998 年	64 億年	5 万年	49 年
2001 年	16 億年	1.2 万年	12.2 年
2004 年	4 億年	3,064 年	3 年
2007 年	1 億年	766 年	280 日
2010 年	2,560 万年	191 年	70 日
2013 年	640 万年	48 年	17.5 日
2016 年	160 万年	12 年	4.4 日
2019 年	40 万年	3 年	1 日
2022 年	10 万年	273 日	6.5 時間

なお、Moore の法則が今後も変わらず適用可能とすると、計算量的安全性に基づく暗号は、どのような鍵長を用いても、いずれは破られることになる。しかしながら、計算機速度の向上には物理的限界が存在する。そこで、同ハンドブックでは、絶対的な上限についての議論も行っている。

結果だけ述べると、計算機性能の向上の相対論的限界は、クロック速度について、あと 10^9 程度（ビット数換算で 30 ビット程度）、集積度の向上についての量子論的限界もあと 10^9 程度（ビット数換算で 30 ビット程度）としている。また、情報操作に伴うエネルギー損失の議論と太陽からの熱放射エネルギーの値から、1 年間の太陽エネルギーを用いて 187 ビットの鍵空間を探索するのが限界としている。

これらの考察から、共通鍵ブロック暗号の鍵長は百数十ビット程度あれば十分と結論づけている。

ただし、上記は暗号解読に関する現状のトレンドを前提としており、暗号解読の研究が画期的に進んだり、量子計算機が実現したりすると、その前提が崩れる。しかしながら、その場合、単に鍵長を長くすれば安全が確保されるということではなくなるため、別の次元の議論が必要となる。

3.3.3 Silverman (2000 年)

R.D.Silverman は、RSA 暗号の安全な鍵長の下限について、Lenstra-Verheul 論文を批判している[12]。

具体的には、Lenstra-Verheul 論文では、1024 ビットは 2002 年において RSA 暗号の安全な鍵長と言えないとされているが、実際には最低 20 年は安全であると述べている。その根拠は、RSA 暗号解読法（素因数分解）におけるメモリ量とメモリアクセスコストであり、そのために、方程式解法計算における並列処理が困難であると述べている。

ただし、Silverman の論文は共通鍵暗号については触れておらず（メモリ量とメモリアクセスコストの問題は、共通鍵暗号の全数探索の並列化計算には、当てはまらない）当該部分については暗に認めていると思われる。

なお、RSA 暗号を解読するハードウェアの構成について述べた論文も発表されており、それが実現すれば、Silverman 論文は覆されることになる[13]。

3.4 まとめ

共通鍵ブロック暗号の全数探索による解読計算は、鍵候補のテストという処理単位が互いに独立しており（いわゆる *embarrassingly parallel* 処理）、大規模並列化が容易である。このことは、全数探索による解読計算の能力は、使用する計算機能力に比例することを意味する。

DES 解読コンテストでは、PC による大規模計算、専用機（DES Cracker）を用いた全数探索による DES 解読が行われ、高並列計算により DES が実際に解読されることが示された。また、暗号解読における専用マシンの有効性が実証されたことにも意義がある。

安全な鍵長を将来に向けて予測した研究として、Lenstra-Verheul 論文がある。当論文の予測モデルは、非常に単純だが、その限りにおいて妥当性を持っており、また予測モデルを構成する前提条件は全て具体的客観的であり、反証したり、パラメータ値について修正を加えたりすることができる。その後、複数の文献で参照されており、一部を批判する論文が発表されているものの、調べた限りでは、共通鍵ブロック鍵に関する予測については特に反論はないようである。

このように、Lenstra-Verheul 論文の問題設定は有効と考えられるので、本調査検討でも、同論文と同様な議論を展開する。ただし、本調査では、安全性の基準点を先端的な半導体技術を前提とした性能値の積み上げにより予測するものとする。また、攻撃側の能力（解読計算システムに投入できる予算）として、通常の商用用途で想定されるより大きな能力を複数段階設定して、安全な鍵長を算出するものとする。

第4章 予測モデル

本章では、共通鍵暗号の安全性要件の予測方法を述べる。具体的には、

- (1) 攻撃者が投入可能な予算をもって実現できる解読計算システムの鍵探索性能を求め、
- (2) その解読計算システムによってしても解読不可能な安全性のレベル（安全な鍵長の下限）を求める

という手順を踏む。

ステップ(1)では、単価当たりの鍵探索性能を求め、それに攻撃者の投入可能な想定予算を掛けることによって、全体システムの鍵探索性能を予測する。単価当たりの鍵探索性能の算出には、チップ集積度、クロック周波数等の半導体技術の予測値を用いる。また、攻撃者の能力（解読計算システムに投入できる予算）として、複数レベルを想定した。

ステップ(2)においては、解読計算システムを用いて一定の時間内に鍵が解読できる確率が一定の値（許容解読確率）以下であるための、鍵長に関する条件を算出する。

なお、予測における個々の前提条件に不確定性がある時は、基本的に、攻撃者にとって有利な条件を採用するものとする。したがって、結論は、安全側に倒れたものとなる。

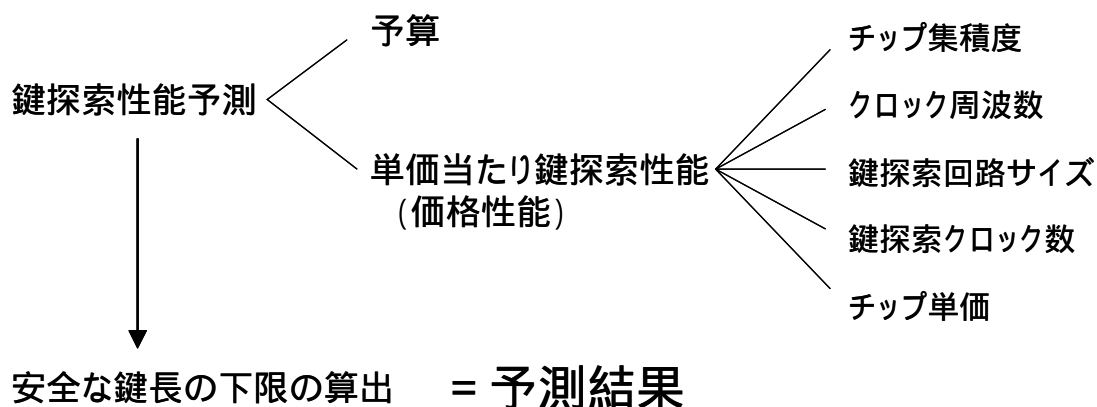


図 4-1 安全な鍵長下限の算出の流れ

4.1 共通鍵暗号の解読法

解読法について以下を仮定する。

◆ 全数探索を用いる。

前述のように、対象となる共通鍵ブロック暗号に対しては、全数検索（総当り法）よりも効率の高い解読法が存在しないと仮定し、攻撃者は全数検索により共通鍵暗号の解読を試みることを前提とする。

◆ 有意性検定のコストは無視できるとする。

共通鍵暗号に対する典型的な攻撃形態は、攻撃者が暗号文を入手し、対応する平文を推測するという状況である。全数探索では、攻撃者は可能な全ての鍵を用いて、暗号文を復号することになるが、正しく復号できたことの判断のための手がかりが必要である。平文が ASCII のプリント可能文字からなること、日本語コードの文字列と解釈できることなどが手がかりの例である。また、平文のヘッダ部が常に一定の形をしていることが、攻撃者にとって既知であれば、それも手がかりとなる。このように、平文の持つ何らかの特徴によって、ランダムなデータから区別することを、有意性検定という。

暗号文への攻撃では、鍵の候補を順に生成し、それによって暗号文を復号し、有意性検定によって平文（ないし平文候補）を抽出する。鍵候補当たりの処理時間は、復号時間、有意性検定の時間、その他のオーバーヘッド時間の和となるが、有意性検定に要する時間はゼロとみなすものとする。

事例：DES Cracker における有意性検定の方法

DES Cracker の探索ユニットは、“興味深い” バイトを定義した表を持つことができ、復号したテキストの最初のブロックを構成する 8 バイトが全て「興味深い」否かを高速に判定する回路を持っている[6]。

例えば、69 文字（英数字、句読点など）が「興味深い」と定義されているとすると、ランダムな文字が「興味深い」確率は $69/256 \approx 1/4$ であり、ランダムなブロックの 8 バイト全てが「興味深い」確率は、約 $1/65536 (1/4^8)$ となる。8 バイト全てが「興味深い」と判定された場合、例外処理により次のブロックの復号をすることができ、それがさらに「興味深い」場合に、上の階層に信号を上げるようにすることができる。この機構により、有意性検定のコストをほとんど無視できるようにできる。

4.2 解読計算システム

攻撃者は投入可能な予算によって構築可能な最高性能の解読計算システムを構築して、解読計算を行うものとする。

全数探索は、鍵空間を分割することによって並列処理が可能である。この計算は、部分計算間に依存性のない、いわゆる embarrassingly parallel な処理であり、大規模並列処理に最も適した計算の一つである。

なお、embarrassingly parallel な処理であっても、システム全体の初期化、末端処理における鍵発見のトップレベルへの通知、鍵発見後の全体システムの終了処理において、若干の通信が発生する。しかしながら、膨大な鍵空間の探索計算と比べると、無視できるオーバヘッドである。

耐故障性について

大規模な計算機システムを構築する場合、耐故障性が重要な課題となる。特に、今回想定するような超大規模な解読計算システムは、数百万ないし数億のチップから構成されることになり、毎日のように、どこかに障害が起きることを想定しなければならない。

ところが、今回のような全数探索では、解読計算中に一部のサブシステムに障害が起きたとしても、そのサブシステムが担当している鍵空間の探索が行われただけである。仮に、障害の起きるサブシステムの割合が 5% であれば、残り 95% の鍵空間の探索は正常に行われ、95% の確率で鍵が発見されることになる。また、障害の起きたサブシステムに割り当てられていた鍵空間を他の部分システムに動的に割り当てる仕組みを用意すれば、正解の鍵が常に発見できることになる。

いずれにしても、攻撃側にとって、解読計算システムが超大規模計算であることに伴うシステム障害は技術的に軽微な問題である。暗号の安全性を守る側としては、攻撃者は(予算の許す限りにおいて)大規模システムを容易に構築できると想定しなければならない。

したがって、解読計算システムが、 N 個の解読ユニットから成るとした場合、全体の解読性能は、解読ユニットの性能の N 倍になると考えてよい。

解読計算システム全体の構築費用については、解読ユニットのコストの N 倍と見なせると仮定する。実際には、全体システムの構築のためには、全体設計のコスト、製造に必要な固定コスト、システム統合・管理のためのコストなど、規模に比例しない部分があるが、非常に大規模なシステムを想定することにより、設計コストや製造に必要な固定コストは相対的に小さなものとして無視できる。想定する解読計算システムの構成は単純であり、システム統合・管理のためのコストも相対的に大きくないと予測されるため、無視することにする(前述のように、これは安全側に倒した仮定である。)

これらの仮定、すなわち、解読計算システムが N 個の解読ユニットから成るとした場合、

- ◆ 全体の性能は、解読ユニットの性能の N 倍である。
- ◆ 全体の構築コストは、解読ユニットのコストの N 倍である。

から、

- ◆ 解読計算システム全体の価格性能は、解読ユニットの価格性能に等しい。

という重要な結論が導かれる。

DES 解読専用マシンに関する研究、特に DES Cracker で実証されたように、非常に高い性能を持つ解読計算システムを実現するためには専用マシンを構築することが必須である。特に、解読計算のための専用のチップ（鍵探索チップ）の設計・実装が最重要である。

解読計算システム全体の具体的な構成は、現在の計算機構成技術を前提とすると、

- ・ 解読用の鍵探索チップ
- ・ ボード（チップ数：数十）
- ・ 筐体（ボード数：10～20 枚程度）
- ・ 全体システム（筐体数：数個～数万個）

という階層からなると想定される。⁶

全体システムが非常に大規模になる場合、複数サイトに分散配置することも可能である。筐体間の通信は、解読計算上はほとんど不要であり⁷、分散計算実施上の問題はない。

解読ユニット、すなわち解読計算システムの価格性能を算出する基本単位としては、単一の解読計算回路（本当の最小単位）（解読計算回路の集積した）チップ、（複数のチップを集積した）ボード、（ボードを集積した）筐体、（筐体の集積した）サブシステム、など様々なレベルを考えらることができる。統合コストを無視し、できるだけ単純な構成要素の性能と価格を見積もるという方針に従い、解読計算専用のために設計された鍵探索チップを、解読ユニットとして採用する。⁸

解読ユニットの実際の価格性能予測は次章で行う。

⁶ 高密度実装を目的とする最近のブレードサーバでは、ブレード（細長い小型のボード）を、数枚～20枚程度、エンクロージャ（小型のケース）に格納し、さらにいくつかのエンクロージャを筐体に縦積みするという形を取る。解読計算システムの筐体も、同様ないしさらに高密度な実装となろう。今回の目的のためには、性能・価格に関する仮定が変わらなければ、システムの実装に関する詳細は不明でも構わない。

⁷ 最低限、必要と思われる通信は、鍵空間の初期割り当て（トップダウンの方向）、解候補の報告（ボトムアップの方向）、解発見時の終了指示（トップダウンの方向）である。その他、管理上の情報のやり取りが考えられる。いずれにせよ、通信頻度・量とも、非常に小さいものである。

⁸ 鍵探索チップ上の個々の鍵探索回路は、物理的に切り離すことができず、単価を直接に計算できないため、価格性能比計算の単位としては採用しない。

まとめ： 解読計算システム

- ◆ 全数探索計算を行う専用の大規模並列システム。
 - 多数（ N 個）の解読計算ユニットから構成。
 - 耐故障性の問題は小さい。
- ◆ 性能・価格とも、解読計算ユニットの N 倍。故に、
 - 全体システムの価格性能は解読計算ユニットの価格性能と等しい。
- ◆ 解読計算ユニットとして、解読計算専用の鍵探索チップを想定。
 - その想定価格、想定性能は次章で算出。

4.3 予算

暗号解読のために投入する予算は、攻撃者および攻撃の目的によるが、ここでは、非常に強力な攻撃者が、国家機密データを解読するといった最大級の攻撃を想定することとする。

具体的には、

- | | |
|------------|------------------------------|
| 1．＜中規模予算＞ | 1000 万ドル（約 10 億円） |
| 2．＜大規模予算＞ | 100 億ドル（約 1 兆円） |
| 3．＜超大規模予算＞ | 経済規模最大国の GDP の 4%（国防予算にほぼ匹敵） |
| 4．＜限界規模予算＞ | 世界の年間 GDP |

の 4 通りの予算を想定する。

第5章 予測モデルにおける要素パラメータの予測

前章で記述した解読計算システムを仮定して、本章では、具体的に、単価当たりの鍵解読性能と予算の予測値を算出する。

5.1 鍵探索チップに関する予測

5.1.1 鍵探索チップの価格

鍵探索チップの設計目標は、絶対性能の最大化ではなく、単価当たり性能を最大化することにある。その際のチップ単価がどの程度になるかの予測は非常に難しい。ここでは、一つの目安として、普及価格帯の CPU の単価を想定する。普及価格帯の CPU は、価格性能が高いからである。具体的には、50 ドル（5,000 円強）と想定する。

表 5-1 普及価格帯の CPU 価格（2003 年 11 月）

メーカー	CPU 名	クロック 周波数	市場価格
AMD	Duron	1.3GHz	5,040 円
Intel	Celeron	1.4GHz	5,100 円

（価格.com（<http://www.kakaku.com/>）の公開データより）

普及価格帯の CPU の場合、ゼロからの回路設計が不要であるため、設計コストが安く、また最新の製造ラインを使わないために単価が小さくなっている。それに対して、専用チップは、普及価格帯の CPU のように大量に生産されないため、設計や製造ライン構築の固定コストの比率が大きい。ただし、今回は予算上限規模として、非常に大規模な解読計算システムを想定しており、数千万～数億というオーダーの鍵探索チップが用いられるとしているため、普及価格帯のチップ単価と同等とした。

5.1.2 鍵探索チップの集積度およびクロック周波数

鍵探索チップの集積度（トランジスタ数）およびクロック周波数については、半導体技術ロードマップ[14]の値（表 5-2）を採用する。ロードマップで明記されていない年については、前後の値から成長率一定と仮定して内挿した。

表 5-2 2002 年版半導体ロードマップによるチップ集積度・周波数の予想

年	チップ 集積度 (トランジスタ数)	チップ・ クロック周波数 (GHz)
2003 年	153,000,000	3,088,000,000
2004 年	193,000,000	3,990,000,000
2005 年	243,000,000	5,173,000,000
2006 年	307,000,000	5,631,000,000
2007 年	386,000,000	6,739,000,000
2008 年	486,539,422	8,055,663,604
2009 年	613,265,826	9,629,576,509
2010 年	773,000,000	11,511,000,000
2011 年	973,918,972	13,686,342,233
2012 年	1,227,061,013	16,272,779,404
2013 年	1,546,000,000	19,348,000,000
2014 年	1,947,837,943	22,078,778,237
2015 年	2,454,122,026	25,194,978,727
2016 年	3,092,000,000	28,751,000,000
2017 年	3,895,675,886	32,808,918,392
2018 年	4,908,244,052	37,439,571,704

(ハッチングのある年は、予想値がないため、内挿・外挿値である。)

5.1.3 鍵探索回路の規模と性能

鍵探索チップは、鍵探索回路を半導体チップ上に集積することで構成される。鍵探索チップの集積度(トランジスタ数)を I_c 、鍵探索回路の規模(トランジスタ数)を S_u 、鍵探索回路の性能を P_u とすると、鍵探索回路間の配線を見捨てた場合、鍵探索チップの性能は、 $(I_c / S_u)P_u = I_c(P_u / S_u)$ となる。ここで、 I_c は所与とすると、鍵探索チップの性能は、 P_u / S_u 、すなわち、鍵探索回路のトランジスタ数当たりの性能に比例することになる。したがって、鍵探索回路はトランジスタ数当たりの性能を最大化するように設計すべきということになる。つまり、鍵探索チップと同様、鍵探索回路についても、絶対性能ではなく、資源対性能を最大化するように設計すべきということである。

トランジスタ数当たりの性能を最大化するような鍵探索回路の実際の回路規模と性能を予測するのは、非常に難しいが、ここでは、公開されているデータの中で、優れていると思われるものを採用することとした。

具体的には、Camellia 暗号[15]である。文献[16]の評価によると、高速実装に関して

は比較対象の中で DES 暗号を除いて、最も回路規模当たりの性能が高い（表 5-3）。さらに、小型実装では、より高い回路規模当たりの性能が実現されている（表 5-4）。すなわち、約 11 K ゲートである。トランジスタ数に換算して、約 50 K トランジスタである。

表 5-3 ハードウェア実装比較評価結果（高速実装）

暗号 アルゴリズム名	回路規模[Gate]			鍵セットアップ ブタイム[ns]	クリティカル パス[ns]	スループット [Mb/s]
	Enc.&Dec.	Key expan.	Total logic			
DES	42,204	12,201	54,405	-	55.11	1161.31
Triple-DES	124,888	23,207	128,147	-	157.09	407.4
MARS	690,654	2,245,096	2,935,754	1740.99	567.49	225.55
RC6	741,641	901,382	1,643,037	2112.26	627.57	203.96
Rijndael ⁹	518,508	93,708	612,834	57.39	65.64	1950.03
Serpent	298,533	205,096	503,770	114.07	137.4	931.58
Twosh	200,165	231,682	431,857	16.38	324.8	394.08
Camellia	216,911	55,907	272,819	24.36	109.35	1170.55

出典：青木和麻呂他，「*Camellia*：様々な環境に適した 128 ビットブロック暗号」

表 5-4 ハードウェア実装比較評価結果（ASIC 小型実装）

暗号 アルゴリズム名	回路規模[Gate]			鍵セットアップ ブタイム[ns]	クリティカル パス[ns]	スループット [Mb/s]
	Enc.&Dec.	Key sched.	Total logic			
Camellia	6,367	4,979	11,350	110.2	27.67	220.28

出典：青木和麻呂他，「*Camellia*：様々な環境に適した 128 ビットブロック暗号」

主だった共通鍵ブロック暗号は、全て Feistel 型・SPN 型など、シフト・転置等の処理を R 段（ラウンド）繰り返す構造をしている。そのハードウェア実装は、1 クロックで 1 段分の処理を行う回路を設計して、それをループ処理によって、時間軸に R 回繰り返す方式（小型実装）と、ループ処理を行わずに全段数の処理を展開して、1 度に行う回路を設計する方式（高速実装）とがある。後者の方が繰り返し処理のオーバーヘッドがなく、高速だが、 R 倍の性能は得られず（クリティカルパスが長くなるため、クロック周期が長くなることも原因）、また前者と比べて R 倍以上の回路規模となるため、トランジスタ数当たりの性能は低下する。

高速性が必須条件となる場合も多いと思われるが、今回のように回路規模当たりの性能を最大にする目的のためには、小型実装が適当である。小型実装であれば、クロック周波数も非常に高くできる可能性がある。

共通鍵ブロック暗号のラウンド数は、16 段が多い (DES、CAST、Camellia 等) が、鍵長 128 ビット、ブロック長 128 ビットの場合の AES (Rijndael) のラウンド数は 10 段である。予測に幅がある場合、鍵探索回路の性能を高い方向で見積もる方針に従い、鍵探索回路のラウンド数は 10 段と仮定する。

また、4.1 節で述べたように有意性検定コストは無視するものとし、したがって、有意性検定のために余分のクロック数を要することを想定しない。

まとめると、鍵探索回路について、

- ・ 鍵探索回路の価格は 50 ドル (年によらず固定)。
- ・ 共通鍵ブロック暗号アルゴリズムのラウンド数は 10 段。
- ・ 鍵探索回路は、半導体ロードマップに示された周波数で動作し、1 クロックで 1 段分の処理を行う。
- ・ 有意性検定のために余分のクロック数を要しない。
- ・ したがって、鍵探索回路は 10 クロックで 1 つの鍵の探索処理を行う。

ということを想定する。

5.1.4 鍵探索チップの単価当たり性能

前節より、鍵探索回路の鍵探索性能は、チップ・クロック周波数を f 、ラウンド数を R とすると、

$$f / R \text{ (鍵 / 秒)}$$

となり、一つのチップ上にある鍵探索回路の数は、

$$I / S \text{ (個)}$$

だから、鍵探索チップの鍵探索性能は、

$$(I / S) f / R \text{ (鍵 / 秒)}$$

となる。したがって、チップ価格を C (ドル) とすると、鍵探索チップの単価当たり性能は、

$$P / C = (I / S) (f / R) / C \text{ (鍵 / 秒・ドル)}$$

となる。

この算出式の各変数に 5.1.1 節 ~ 5.1.3 節の予測値を代入した結果を表 5-5 に示す。

⁹ 2002 年 11 月に米国連邦政府向け次期共通鍵暗号 AES として制定。

表 5-5 鍵探索チップの価格性能の計算（半導体ロードマップに従った性能向上）

年	チップ 集積度 I (M トランジ スタ)	チップ・ クロック 周波数 f (GHz)	鍵探索回路 規模 S (K トランジ スタ)	ラウンド数 R	鍵探索性能 $(I/S)*f/R$ (ギガ鍵 / 秒)	チップ価格 C (ドル)	チップ価格 性能 P/C (ギガ鍵 / 秒・ドル)
2003 年	153	3.09	50	10	945	50	18.90
2004 年	193	3.99	50	10	1,540	50	30.80
2005 年	243	5.17	50	10	2,514	50	50.28
2006 年	307	5.63	50	10	3,457	50	69.15
2007 年	386	6.74	50	10	5,203	50	104.05
2008 年	487	8.06	50	10	7,839	50	156.78
2009 年	613	9.63	50	10	11,811	50	236.22
2010 年	773	11.51	50	10	17,796	50	355.92
2011 年	974	13.69	50	10	26,659	50	533.18
2012 年	1,227	16.27	50	10	39,935	50	798.71
2013 年	1,546	19.35	50	10	59,824	50	1,196.48
2014 年	1,948	22.08	50	10	86,012	50	1,720.24
2015 年	2,454	25.19	50	10	123,663	50	2,473.26
2016 年	3,092	28.75	50	10	177,796	50	3,555.92
2017 年	3,896	32.81	50	10	255,626	50	5,112.52
2018 年	4,908	37.44	50	10	367,525	50	7,350.50

- ・チップ集積度 I 、チップ・クロック周波数 f ... 半導体ロードマップより（5.1.2節）
- ・鍵探索回路規模 S ... 50K トランジスタ（固定）と仮定（5.1.3節）
- ・ラウンド数 R ... 10 ラウンド（固定）と仮定（5.1.3節）
- ・チップ価格 C ... 50 ドル（固定）と仮定（5.1.1節）

なお、上記の集積度と周波数は、各年における最新技術を使った場合であり、絶対性能よりも価格性能の最大化を追求する解読計算システムでの利用は不適當である可能性もある。したがって、上記の価格性能は過剰評価である可能性が高い。ただし、一方、鍵探索回路は小型であり、普及価格帯の CPU よりもクロック周波数を高められる可能性もあり、過剰評価の程度を減じているかも知れない。

Lenstra-Verheul モデルとの比較のため、2003 年における見積りを同じとして、2004 年以降、価格性能比が 1.5 年で 2 倍の率で向上するとした時の予測値を計算した。半導体ロードマップによる性能向上と比較したものを表 5-6 に示す。半導体ロードマップは、性能向上速度の鈍化を予想しているため、後者の価格性能向上速度の方が大きく、10 年後で 1.6 倍、15 年度で 2.6 倍の差となっている。

表 5-6 鍵探索チップの価格性能 ～Lenstra-Verheul モデルとの比較～

年	チップ価格性能 P/C (ギガ鍵 / 秒・ドル)		チップ価格性能 予測の比較 LV/RM
	半導体ロード マップ RM	Lenstra-Verheul モデル LV	
2003 年	18.90	18.90	1.0
2004 年	30.80	30.00	1.0
2005 年	50.28	47.62	0.9
2006 年	69.15	75.59	1.1
2007 年	104.05	120.00	1.2
2008 年	156.78	190.49	1.2
2009 年	236.22	302.38	1.3
2010 年	355.92	479.99	1.3
2011 年	533.18	761.94	1.4
2012 年	798.71	1,209.51	1.5
2013 年	1,196.48	1,919.97	1.6
2014 年	1,720.24	3,047.77	1.8
2015 年	2,473.26	4,838.03	2.0
2016 年	3,555.92	7,679.90	2.2
2017 年	5,112.52	12,191.08	2.4
2018 年	7,350.50	19,352.13	2.6

4.2節で述べたように、本節で予測した鍵探索チップ（解読ユニット）の価格性能を、解読計算システム全体の価格性能として採用する。

5.2 予算

前述（4.3節）のように、予算上限として

- 1．＜中規模予算＞ 1000 万ドル（約 10 億円）
- 2．＜大規模予算＞ 100 億ドル（約 1 兆円）
- 3．＜超大規模予算＞ 経済規模最大国の GDP の 4%(国防予算にほぼ匹敵)
- 4．＜限界規模予算＞ 世界の年間 GDP

の 4 種類を仮定する。予測が必要なのは、経済規模最大国の GDP と世界の年間 GDP である。

5.2.1 経済規模最大国の GDP 予測

今後 15 年にわたる経済規模最大国として、アメリカ合衆国を想定する。

前述の世界銀行 2002 年データでは、米国の GDP は 10,416,818 百万 US ドルとなっている。一方、日本経済研究センター長期経済予測（2002 年 3 月）[19]によると、米国の GDP 成長率下表のようになっている。この成長率を採用する。（なお、2016 年以降も便宜的に 2010 年～2015 年の成長が続くものとする。）

表 5-7 経済規模最大国の GDP 成長率予測

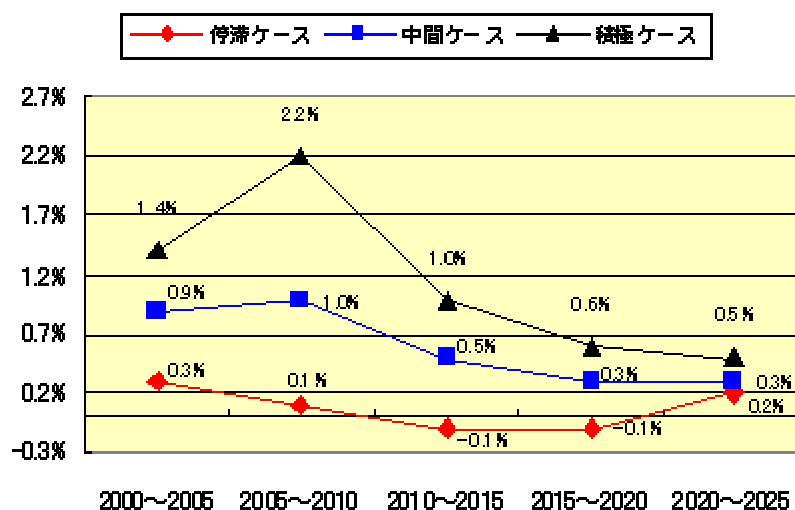
期間	年間 GDP 成長率
2000 年～2005 年	1.8 %
2005 年～2010 年	3.5 %
2010 年～2015 年	3.0 %

5.2.2 世界の GDP 予測

世界銀行による 2002 年の世界全体 GDP の推計データ[17]によると、世界の GDP 合計は 32,252,480 百万 US ドルである。

また、民間の調査機関である日本経済研究センターの長期予測（2001 年 3 月）によると、GDP 成長率は下表のようになっている。

表 5-8 世界 GDP の成長率予測



攻撃側に有利となるように、最も楽観的な「積極ケース」を想定するものとする。

5.2.3 予算の予測値

上記を用いて、予算の予測値を計算した結果を表 5-9に示す。

表 5-9 予算の予測

	中規模予算 (百万 ドル)	大規模予算 (百万 ドル)	超大規模予算 (百万 ドル)	限界規模予算 (百万 ドル)
2003 年	10	10,000	450,007	32,704,015
2004 年	10	10,000	458,107	33,161,871
2005 年	10	10,000	466,353	33,626,137
2006 年	10	10,000	482,675	34,365,912
2007 年	10	10,000	499,569	35,121,962
2008 年	10	10,000	517,053	35,894,645
2009 年	10	10,000	535,150	36,684,328
2010 年	10	10,000	553,881	37,491,383
2011 年	10	10,000	570,497	37,866,297
2012 年	10	10,000	587,612	38,244,960
2013 年	10	10,000	605,240	38,627,409
2014 年	10	10,000	623,397	39,013,683
2015 年	10	10,000	642,099	39,403,820
2016 年	10	10,000	661,362	39,640,243
2017 年	10	10,000	681,203	39,878,084
2018 年	10	10,000	701,639	40,117,353

また、Lenstra-Verheul モデルとの比較のため、2003 年を起点として、その後、予算が 10 年間で 2 倍の率で向上するとした時の予測値を表 5-10に示す。

表 5-10 予算の予測（10 年間に 2 倍の増加率）

	中規模予算 (百万 ドル)	大規模予算 (百万 ドル)	超大規模予算 (百万 ドル)	限界規模予算 (百万 ドル)
2003 年	10	10,000	450,007	32,704,015
2004 年	11	10,718	482,305	35,051,295
2005 年	11	11,487	516,922	37,567,048
2006 年	12	12,311	554,023	40,263,365
2007 年	13	13,195	593,787	43,153,206
2008 年	14	14,142	636,405	46,250,461
2009 年	15	15,157	682,082	49,570,017
2010 年	16	16,245	731,038	53,127,829
2011 年	17	17,411	783,507	56,940,997
2012 年	19	18,661	839,742	61,027,849
2013 年	20	20,000	900,013	65,408,029
2014 年	21	21,435	964,610	70,102,590
2015 年	23	22,974	1,033,844	75,134,096
2016 年	25	24,623	1,108,046	80,526,730
2017 年	26	26,390	1,187,574	86,306,412
2018 年	28	28,284	1,272,811	92,500,922

5.3 解読計算時間および許容解読確率

通常、暗号研究者は、暗号の安全性を理論的に検討する場合、千年ないし 1 万年程度のオーダーの時間を掛けて解読計算を実行しても暗号が完全に解読されない場合に安全と判断する。

一方、現実の暗号攻撃者は、そのような長い時間に渡って解読計算しない。

本検討では、現実的な時間内での解読確率が非常に低いことをもって安全とみなすものとする（事実上、暗号研究者による評価と同様の安全性への要請となる。）

具体的には、1 年間の解読計算によって解読される確率が 0.1% 未満であることをもって安全であるとする。これは、「解読計算を 1000 年間行っても、鍵空間が探索し尽くせない」ことに相当する。

第6章 予測結果

前章で示した解読計算システムの単価当たり性能と予算の予測値を用いて、安全な鍵長の下限を計算する。

6.1 安全な鍵長の計算式

まず、安全な鍵長の下限の計算式を与えておく。

安全な鍵長とは、想定する解読計算システムを用いて、想定する解読計算時間内に鍵を発見する確率が、許容解読確率以下になるような鍵長のことである。すなわち、

$$\text{鍵探索速度} \times \text{解読計算時間} \leq \text{鍵空間サイズ} \times \text{許容解読確率}$$

である。鍵空間サイズ $= 2^{\text{鍵長}}$ だから、

$$\text{鍵長} \geq \log_2(\text{鍵探索速度} \times \text{解読計算時間} / \text{許容解読確率})$$

となる。

また、鍵長は整数値なので、

$$\text{安全な鍵長の下限} = \lceil \log_2(\text{鍵探索速度} \times \text{解読計算時間} / \text{許容解読確率}) \rceil$$

となる。

6.2 安全な鍵長の下限の計算結果

前章で示した解読計算システムの単価当たり性能と予算の予測値を用いて求めた安全な鍵長の下限の計算結果を表 6-1に示す。また、2003 年を起点とする、Lenstra-Verheul モデルに従った予測を表 6-2に示す。

表 6-1 安全な鍵長の下限の予測結果

	対 中規模予算 攻撃	対 大規模予算 攻撃	対 超大規模予算 攻撃	対 限界規模予算 攻撃
2003 年	93	103	108	114
2004 年	93	103	109	115
2005 年	94	104	110	116
2006 年	95	105	110	116
2007 年	95	105	111	117
2008 年	96	106	111	118
2009 年	96	106	112	118
2010 年	97	107	113	119
2011 年	98	108	113	119
2012 年	98	108	114	120
2013 年	99	109	115	121
2014 年	99	109	115	121
2015 年	100	110	116	122
2016 年	100	110	116	122
2017 年	101	111	117	123
2018 年	101	111	117	123

表 6-2 安全な鍵長の下限の予測結果（Lenstra-Verheul モデルによる将来への外挿）

	対 中規模予算 攻撃	対 大規模予算 攻撃	対 超大規模予算 攻撃	対 限界規模予算 攻撃
2003 年	93	103	108	114
2004 年	94	103	109	115
2005 年	94	104	110	116

	対 中規模予算 攻撃	対 大規模予算 攻撃	対 超大規模予算 攻撃	対 限界規模予算 攻撃
2006 年	95	105	111	117
2007 年	96	106	111	117
2008 年	97	107	112	118
2009 年	97	107	113	119
2010 年	98	108	114	120
2011 年	99	109	114	121
2012 年	100	110	115	121
2013 年	100	110	116	122
2014 年	101	111	117	123
2015 年	102	112	117	124
2016 年	103	113	118	124
2017 年	104	113	119	125
2018 年	104	114	120	126

今回の予測は、攻撃側の能力（予算規模、利用する技術水準）として、現実的に考え得る限界とも言える高い水準を想定した。また、解読計算システムの性能予測においても、固定コストを無視するなど、価格性能が高くなる方向での予測を行った。この結果として、今回の予測結果は既存研究の予測結果と比べて、かなり鍵長が長くなった。

なお、過剰見積りの程度、既存事例・研究との比較などは、第 7 章で述べる。

第7章 考察

本章では、前章までに得られた結果の妥当性について考察を行う。鍵長と共に共通鍵ブロック暗号を特徴付ける数であるブロック長に関する要請、予測モデルとパラメータにおける価格性能の過剰見積の程度の評価、既存研究における専用マシン、汎用 MPU などを用いた場合の価格性能との比較、イノベティブ計算方式の現状などである。

7.1 ブロック長

本調査では、もっとも基本的な脅威である、鍵空間の全数探索による暗号鍵の発見に対する安全性を検討した。共通鍵ブロック暗号に対しては、

- ・ 辞書攻撃
- ・ 暗号文一致攻撃

という別種の全数攻撃が知られている。

これらは同一の鍵によって暗号化された多数の暗号文を入手して、その情報を元に攻撃を行おうとするものである。

辞書攻撃

辞書攻撃は、通常、パスワード解析に用いられる攻撃手法である。パスワードを暗号化したパスワードファイル（例：Unix の/etc/passwd）が入手できた場合に、パスワードとして用いられそうな文字列（辞書に載っている単語等）を大量に発生させ、それぞれを暗号化した結果と、パスワードファイルに収められた暗号化されたパスワードが一致するかをチェックし、一致すればパスワードが判明する[20]。同様に、大量の平文と暗号文の対応関係表を作成しておき、解読したい暗号文が与えられた時に、この表の中から一致を探すことにより攻撃するものを辞書攻撃という[21]。これを利用して、チャレンジ・レスポンス型認証において、なりすましをすることが可能な場合もある。

暗号文一致攻撃

暗号文一致攻撃とは、同一の暗号文ブロックが2度現われた時に平文に関する情報が得られるという攻撃である[21]。

ブロック長を b ビットとすると、ブロックの可能性は $N = 2^b$ 通りあり、暗号文ブロックは高いランダム性を持つので、同一の暗号文ブロックが2度出現するためには N に比例するオーダーの数のブロックを観測しなければならないように思われる。しかしなが

ら、バースデー・パラドックス¹⁰により、 N の平方根オーダーのブロックがあれば、その中に同一のブロックが 2 度出現する可能性が高くなる ($n = \sqrt{2N}$ 個のブロックがあれば、当該確率はほぼ 1 となる¹¹)。ブロック長が 64 ビットとした場合、 $n = \sqrt{2} \cdot 2^{32}$ 個の暗号文ブロックを観測すれば、その中に一致するものがほぼ 1 つ存在することになる。 $\sqrt{2} \cdot 2^{32}$

6 G 個の 64 ビット・ブロックの総サイズは 48GB であり、利用の仕方によっては十分に危険が存在すると言えよう。

128 ビット・ブロックとすると、上記の n は $\sqrt{2} \cdot 2^{64} = 2^{32}$ E (エクサ) 個であり、総サイズはおよそ 350 EB (エクサ・バイト) となる (テラバイトの 3.5 億倍、ペタバイトの 35 万倍)。これだけのオーダーの量のデータを同一の鍵で暗号化しなければ、暗号文一致攻撃の危険性は低い。

したがって、ブロック長は 128 ビット以上が望ましいと言えよう。AES、Camellia など、近年に開発され、今後有力と思われる暗号アルゴリズムは 128 ビット・ブロックをサポートしている。

7.2 価格性能の過剰見積りの程度

7.2.1 価格性能見積りの精度

今回の予測モデルにおける解読計算システムの性能見積りに関する各要素パラメータは、想定し得る幅の中で、解読計算システムの性能が高くなる値を採用している。また、予想の難しい固定コストや統合コストは無視している。この結果、解読計算システムの性能は過剰に評価されている。その度合いを見積もっておくことは、他の研究等との比較の上で意味があろう。

以下に、性能過剰評価の箇所と程度を示す。

- ・ チップ集積度
 - 回路の不規則性や配線オーバーヘッドのため、実際には集積度 (トランジスタ数) が落ちる。
(また、通常は、最先端技術が大量生産にすぐに使えるとは限らない。)
 - 性能過剰見積り度： 2 倍 ~ 10 倍程度

¹⁰ 人が集まった時に、同じ誕生日を持つペアが居る確率が 0.5 を超すのは、365 の半分の 183 人よりもずっと小さい 23 人である。直感に反するという意味で、これを「バースデー・パラドックス」と呼ぶ。

¹¹ N 個のランダムな値を取り得る独立な確率変数が、 $n = \sqrt{2N}$ 個あった時、これらの中で値が一致する対の出現数の期待値は $1 - \frac{1}{n}$ である (n が大きければ、ほぼ 1)。ブロック長が b ビットであれば、ブロックの取り得る値は $N = 2^b$ 通りであり、 $n = \sqrt{2N} = 1.4 \times 2^{b/2}$ である。

- ・ 探索回路規模
 - 制御回路等のオーバヘッドが加わるが、相対的に小さい。
 - 性能過剰見積り度： 比較的軽微

- ・ システム実装コスト
 - チップ製造コスト以外のコストを無視している。
 - 性能過剰見積り度： 2 倍～10 倍程度

- ・ 有意性検定のオーバヘッド
 - 今回の想定では、有意性検定のオーバヘッドを無視している。
 - ただし、有意性検定のコストは非常に小さくて済む可能性がある。
 - 性能過剰見積り度： 比較的軽微（と仮定）

逆に、過少見積りの箇所はほとんどないと思われる。（仮にあったとしても、他の箇所における過剰見積りの程度が大幅に上回る。）

これらを総合すると、全体として、価格性能比を、数倍～100 倍程度高く見積もっている可能性がある。鍵長に換算すると、2 ビット～7 ビット程度の差である。

7.2.2 価格性能の比較（対：DES 解読専用マシン）

DES 解読専用マシンに関する主な既存研究事例との比較を表 7-1 に示す。（Lenstra-Verheul の予測モデルに従って、2003 年時点の価格性能に置き換えて比較した。）なお、この中で実際に構築されたのは DES Cracker のみである。

表 7-1 鍵探索に関する価格性能の比較（対 DES 解読専用マシン）

発表年	設計者	コスト (ドル)	56bit 鍵空間 全数探索時間 (秒)	鍵探索価格 性能 (鍵/秒・ドル)	鍵探索価格 性能 2003 年外挿値 (鍵/秒・ドル)
1980	Diffie	50,000,000	345,600	4.2E+03	1.7E+08
1993	Wiener	1,000,000	25,200	2.9E+06	2.9E+08
1996	Blaze	300,000,000	24	1.0E+07	2.5E+08
1998	EEF (DES Cracker)	130,000	806,400	6.9E+05	6.9E+06
1999	Brazier	280,000,000	1.678	1.5E+08	9.7E+08
2003	本検討における 解読計算システム			1.9E+10	1.9E+10

表からわかるように、今回の見積りは、価格性能が 20 倍～100 倍程度高くなっている（実装に先端技術を用いなかった DES Cracker を除く）。これは、前述の価格性能見積りの過剰見積り度の予想範囲内である。

このように、今回想定した解読計算システムは、鍵解読専用マシンとの価格性能比較において、1 桁～2 桁の過剰な評価をしている。しかしながら、今後 10 年～15 年間の設計技術・実装技術の進歩により、実際の価格性能が今回の見積りに近づく可能性を否定できない。このため、安全性を確保するという目的に鑑みると、今回の見積りは妥当であると思われる。

7.2.3 価格性能比較（対：汎用 MPU、スパコン）

前節と同様、今回の解読計算システムの価格性能を汎用 MPU、スパコンの価格性能と比較する。価格性能比の高い最近のコモディティ・スパコン（特に PC クラスタ）、グリッド計算システムとの比較も示す。

比較に当たって、以下の仮定をおいた。

- ・ DES 全数探索に要する命令数は 1 MMY（Lenstra-Verheul 論文[9]）
MMY とは Million MIPS Year（1MIPS の計算機による百万年の計算量）のことである。鍵一つ当たりの命令数に換算すると、 $MMY / 2^{56} = 438$ 命令/鍵となる。（Pentium 上で約 500 命令/鍵という実装事例がある。）
- ・ 汎用 MPU ・スパコンのピーク FLOPS 値を MIPS 値とみなす。

近年の汎用 MPU およびスパコンのピーク FLOPS 値は、整数演算性能と同等のものが多く、それを近似的に MIPS 値とみなすことは自然である。ただし、実際の計算における実効性能は、ピーク FLOPS 値より、数倍程度低い可能性がある。

比較結果を表 7-2に示す。

表 7-2 鍵探索に関する価格性能の比較（対 汎用 CPU、スパコン、グリッド）

発表年	設計者	コスト (ドル)	56bit 鍵空間 全数探索時間 (秒)	鍵探索価格 性能 (鍵/秒・ドル)	鍵探索価格 性能 2003 年外挿値 (鍵/秒・ドル)
汎用 MPU					
2003	Celeron (2GHz)	62.5	15,768,000,000	7.3E+04	7.3E+04
2003	Pentium 4 (2.4GHz)	166.7	6,570,000,000	6.6E+04	6.6E+04
スパコン					
2002	地球シミュレータ	333,333,333	769,922	2.8E+02	4.5E+02
2002	GRAPE-6	4,166,667	492,750	3.5E+04	5.6E+04
2002	ASCI Q	200,000,000	1,539,844	2.3E+02	3.7E+02
2002	MDM	6,500,000	404,308	2.7E+04	4.4E+04
2002	MCR Linux Cluster	10,000,000	2,851,356	2.5E+03	4.0E+03
2005	ASCI Purple	216,000,000	315,360	1.1E+03	4.2E+02
2005	Blue Gene/L	100,000,000	85,929	8.4E+03	3.3E+03
グリッド					
2003	TeraGrid (Grid)	88,000,000	1,576,800	5.2E+02	5.2E+02
2007	NAREGI (Grid)	250,000,000	105,120	2.7E+03	4.3E+02
2003	本検討における 解読計算システム			1.9E+10	1.9E+10

上記表によると、今回の解読計算システムは、価格性能比が 5 桁～8 桁程度高い。この差の内訳を分析する（全て 2003 年時点の比較である。）。

- ・ 汎用 MPU との差
 - CPU 集積度の差： 3000 倍
汎用 MPU がチップ上に 1 個～数個の CPU を搭載するのに対し、鍵探索チップはチップ上に 3000 個の鍵探索回路を搭載する。

- 鍵探索クロック数：約 40 倍
復号処理をソフトウェアで実現しているか（438 クロック/鍵と仮定）、ハードウェアで実現しているか（10 クロック/鍵と仮定）の差である。
 - その他：～2 倍
上記の新しい MPU が必ずしも最先端のトランジスタ集積度とクロック周波数を採用しているとは限らない。
 - 全体として：5 桁強程度の差
- ・ コモディティ・スパコン（PC クラスタ等）との差
 - 今回の解読計算システムではシステムの統合コストを無視したが、コモディティ・スパコンにおいて、MPU のコストとシステム全体のコストの間には、10 倍程度の差がある。
差の内容としては、1U 計算サーバであれば、メモリ、周辺チップを含むボード、電源、ケースなどのオーバヘッドがあり、その上に筐体、ネットワークなどのコストなどが加わる。¹²
 - 全体として：6 桁程度の差
- ・ 「本格」スパコンとの差
 - 高性能 MPU コスト対低価格 MPU コスト：数倍～数十倍
本格的なスパコンでは、高性能 MPU や専用プロセッサ（特にベクトルスパコンの場合）を要素プロセッサとしており、絶対性能は高くなるが、相対性能（価格性能）は落ちる。
 - システム全体コスト/MPU コスト：10 倍～数十倍
筐体、高速ネットワークなどを含めたシステム全体コストは MPU コストの 10 倍～数十倍程度になる。
 - その他（少数生産なので相対的に設計等の固定コストが大きい。）
 - 全体として：7 桁程度の差

以上のように、要素 MPU が汎用であるか専用であるかの違い、および統合コストによって鍵探索についての価格性能に大きな差が生じている。

ただし、コモディティ・スパコンが普及しつつあり、また、2005 年に完成予定の BlueGene/L では価格性能の高い実装方式が実現される。今後、現状より 1 桁程度以上価格性能の高いスパコンが普及して行くと思われる。

¹² 今後、BlueGene/L のように、価格性能の高い実装方式を採用するスパコンが増える可能性はある。

7.3 解読専用マシン以外の解読計算システム

今回の検討では、もっとも強力な解読計算システムの形態として、解読専用マシンを想定した。他の形態による解読計算システムとして、インターネット上の PC による大規模並列計算、スパコン、計算グリッドなどが考えられる。

しかしながら、前節で見たように、上記の全ての形態において、今回想定の特用マシンより価格性能比が5桁以上劣る。したがって、専用の解読計算システム以上の脅威となり得ないと言って良い。

なお、小規模な予算を持った攻撃者がインターネット接続された多数の PC の無償協力を得て、解読計算をすることが考え得る。現状考え得る上限として、10 億台の PC が参加した場合、PC の価格を 500 ドルとすると、5000 億ドルの予算を持っているのと同等だが、5 桁の価格性能比で換算すると、5 百万ドルの解読専用システムの性能に相当することになる。これは予測モデルにおける中規模予算（表 5-9）の半分に過ぎない。すなわち、インターネット上の多数の PC を用いた大規模分散解読計算は、攻撃者の実質予算を大幅に大きくするが、最大規模でも、今回の予測モデルにおける中規模予算に満たない水準の脅威であることが分かる。

7.4 運用費用について

今回の検討では、解読計算システムに掛かる費用として、構築費用のみを考えた。しかしながら、実際には、構築後の運用にも費用が掛かる。ここでは、運用費用のうち、電力費用について若干の見積をする。一般には、運用費用には、電力費用、ハードウェアのメンテナンス、運用要員、その他管理的な費用が含まれるが、（攻撃者にとって）理想的な状況では、ハードウェアは故障せず、また一旦、暗号文を設定して稼働を開始すれば、暗号鍵が発見されるまで、人的介入は不要となる。そこで、電力費用のみについての試算を示す。

単純化のための仮定として、解読計算システムの電力消費は、全て鍵探索チップによるものとする。また、チップ当たり電力消費を 10W とする。¹³

国内の大口産業用電力料金は 1kWh 当たり約 9 円である。例えば、東京電力での高圧休日高負荷電力 B2 型（平日と休日の負荷を平均化する場合の電力供給契約）の電力量料金（円 / kWh）は以下の通りである（基本料金以外の変動部分）。

¹³ 実際には、クロック周波数が非常に速く、また全ての鍵探索回路が常に動作しているため、電力消費は、1 桁以上大きいオーダーになる可能性がある。

表 7-3 産業用電力量料金の例

季節	平日 / 休日	電力量料金 (円 / kWh)
夏季 (7月1日～9月30日)	平日	9.50
	休日	7.70
その他の季節 (上記以外)	平日	8.65
	休日	7.00

出典：電力料金のご案内「ビル・工場の料金メニュー」(東京電力株式会社) [22]

したがって、チップ当たりの電力料金は、1年で788円となる。約7年でチップ単価50ドル(約5500円)に相当する費用が発生することになる。

なお、大規模予算(1兆円規模)の場合、チップ数は約2億個であり、解読計算システムの総電力消費は20億W(=200万kW)となる。これは、中規模の発電所1つ分に相当する。

7.5 イノベティブ計算方式による解読について

今回の検討は、従来の計算機技術の延長を想定し、量子計算などのイノベティブ計算方式[1]を用いた解読計算システムの可能性は考慮しなかった。量子計算以外のイノベティブ計算方式については、何が計算可能であるかについての理論研究や、試作装置による実験をしている段階にある様子である(例えば、[27]を参照)。実用化に向けては克服すべき課題が多く、定量的な性能予測の出来る段階にない。また、暗号解読向けの高速アルゴリズムもまだ知られていない。このため、今回の調査では考慮外とした。

ただし、量子計算については、公開鍵暗号に対する高速アルゴリズムが発見されており、脅威の可能性が存在するため、若干の考察を行う。

量子計算とは、量子状態の重ね合わせの法則により、複数の可能性を同時並行的に計算する方法である。この並列度には上限がなく、時間に対して指数オーダー量の計算をすることが原理的には可能である。(詳しくは、[23][24][25]などを参照。)

ただし、量子状態の重ね合わせから最終的な解を高い確率で観測して取り出す方法を問題毎に個別に設計しなければならないこと(必ずしも簡単ではない)や、ビット数が増えると量子状態の制御が非常に困難であることから、現時点では、実用化への道のりはまだ長いと言われている(十年～数十年)。

公開鍵暗号に対しては、量子計算アルゴリズムとして、素因数分解を行う Shor の多項式時間アルゴリズム[26]、および離散対数問題に対する多項式時間アルゴリズムが知

られている。量子計算機が実現した場合、Shor のアルゴリズムは RSA 暗号にとって脅威となる。

一方、共通鍵暗号に対しては、現時点では、量子計算による共通鍵暗号の解読方法は知られていない。ただし、不可能と言い切ることはできない。

上記から、今回の検討においては、以下を一応の結論とする。

- ・ 共通鍵暗号の解読に関する量子計算アルゴリズムは知られていない。
- ・ 研究の進展により、量子計算による共通鍵暗号の解読法が発見される可能性は否定できない。
- ・ 量子計算システムは、ビット数の大きいものを実現することが非常に難しく、研究の進展にともない困難が克服されていくとしても、数十ビット以上のビット数を扱える計算システムが急に実現する可能性は極めて低く、実際には、扱えるビット数が徐々に増えていくと予想される。したがって、量子計算システムが具体的な脅威になることは事前に予期できる。¹⁴
- ・ したがって、共通鍵暗号に対する量子計算システムの脅威への対策は、量子計算の実用化が進展し、技術進歩のトレンドが現われきた段階で行えば十分である。¹⁵

¹⁴ どの程度「事前に予期」できるかは予想できないが、大きなブレークスルーがない限り、1年に1ビットないし数ビットであろう。安全性マージンのビット数との比較で、安全性が脅かされる可能性のある時期を予期して、対策を考えることになる。

¹⁵ Moore の法則は、半導体集積回路技術について正にこのことを行ったものと言える。

参考文献・URL

- [1] 「情報処理学会論文誌」原稿執筆案内, <http://www.ipsj.or.jp/toukou/kitei/shippitu.html>.
- [2] "Cryptographic Challenges", RSA Security, <http://www.rsasecurity.com/rsalabs/challenges/index.html>
- [3] "DATA ENCRYPTION STANDARD (DES)", FIPS PUB 46-3, <http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>.
- [4] "Project DES", distributed.net, <http://www.distributed.net/des/>.
- [5] "RSA's DES Challenge III is solved in record time", RSA Security, <http://www.rsasecurity.com/rsalabs/challenges/des3/index.html>.
- [6] EFF (Electronic Frontier Foundation), "Cracking DES" (Jan 1999), <http://www.eff.org/descracker> (和訳「DES をクラック」, <http://www.genpaku.org/crackdes/cracking-desj.html>).
- [7] "Record-Breaking DES Key Search Completed", <http://www.cryptography.com/resources/whitepapers/DES.html>.
- [8] John R T Brazier, "Possible NSA Decryption Capabilities", <http://jya.com/nsa-study.htm>.
- [9] Arjen K. Lenstra, Eric R. Verheul, "Selecting Cryptographic Key Sizes", Journal of Cryptology (1999, 2001), <http://www.win.tue.nl/~klenstra/key.pdf>.
- [10] B. Preneel, et al., "Security Evaluation of NESSIE First Phase" (September 2001), <https://www.cosic.esat.kuleuven.ac.be/nessie/deliverables/D13.pdf>.
- [11] 電子商取引実証推進協議会 (ECOM) セキュリティ WG「暗号利用技術ハンドブック (第2版)」(2000年3月).
- [12] R.D.Silverman (RSA), "A Cost Based Security Analysis of Symmetric and Asymmetric Key Lengths" (Apr 2000), <http://www.rsasecurity.com/rsalabs/bulletins/bulletin13.html>.
- [13] A.Shamir, E.Tromer, "Factoring Large Numbers with the TWIRL Device (preliminary draft)" (Jan 2003).
- [14] Semiconductor Industry Association (SIA), eds., "International Technology Roadmap for Semiconductors (ITRS) 2002 Update", <http://public.itrs.net/Files/2002Update/Home.pdf>.
- [15] Camellia ホームページ, <http://info.isl.ntt.co.jp/camellia/index-j.html>.
- [16] 青木和麻呂他, 「Camellia: 様々な環境に適した 128 ビットブロック暗号」, <http://info.isl.ntt.co.jp/camellia/CRYPTREC/2001/01jeval.pdf>, <http://info.isl.ntt.co.jp/camellia/Publications/camellia.pdf>.
- [17] World Bank, "Total GDP 2002", <http://www.worldbank.org/data/databytopic/GDP.pdf>.
- [18] US Department of Defense, "National Defense Budget Estimates for FY2004", <http://www.defenselink.mil/comptroller/defbudget/fy2004/>.

- [19] 日本経済研究センター「長期経済予測」(2002年3月)。
- [20] 「ネットワークセキュリティ関連用語」情報処理振興事業協会 セキュリティセンター,
http://www.ipa.go.jp/security/ciadr/word_idx.html.
- [21] 谷口文一, 太田和夫, 大久保美也子「Triple DES を巡る最近の標準化動向について」,
IMES Discussion Paper Series 99-J-6, 日本銀行金融研究所 (1999),
<http://www.imes.boj.or.jp/jdps99/99-J-06.pdf>.
- [22] 電力料金のご案内「ビル・工場の料金メニュー」(東京電力株式会社),
http://www.tepco.co.jp/e-rates/custom/b_and_f/index-j.html.
- [23] 「量子計算機の研究動向に関する調査」調査報告書, 情報処理振興事業協会 (2000),
<http://www.ipa.go.jp/security/fy11/report/contents/crypto/crypto/report/QuantumComputers/>.
- [24] 今井 浩「量子情報科学の過去・現在・未来— 量子計算・量子情報—」(2003),
<http://www.imai.is.s.u-tokyo.ac.jp/~imai/lecture/lecture.html>,
<http://www.imai.is.s.u-tokyo.ac.jp/~imai/lecture/algo1.pdf>.
- [25] Centre for Quantum Computation, <http://www.qubit.org/>
- [26] P. W. Shor, "Algorithms for quantum computation: discrete log and factoring",
Proceedings of the 35th Annual Symposium on the Foundations of Computer Science,
S. Goldwasser (editor), IEEE Computer Society Press, Los Alamitos, 1994, pp.
124-134.
- [27] 分子計算機プロジェクト,
<http://hagi.is.s.u-tokyo.ac.jp/MCP/moco-final-html/index.html#contents>
- [28] The International Technology Roadmap for Semiconductors web site,
<http://public.itrs.net/>.
- [29] 「Intel 研究者も予言する「ムーアの法則の限界」」, ZDNet ニュース 2003/12/3,
http://www.zdnet.co.jp/news/0312/02/ne00_intel.html.
- [30] David Klepacki (IBM T. J. Watson Research Center), "Blue Gene — Towards
Petascale Computing" (April 2003), p9,
<http://scv.bu.edu/SCV/Archive/IBM/BGL-BU.pdf>.
- [31] 地球シミュレータ開発センター「地球シミュレータ」, p 13,
<http://www.es.jamstec.go.jp/esrdc/jp/public/ESP.pdf>.
- [32] "Slides concerning TOP500 06/2002", <http://www.top500.org/slides/2002/06/#>.
- [33] The Advanced Simulation and Computing Program (ASCI),
<http://www.lanl.gov/projects/asci/>.
- [34] "Networking and Information Technology Research and Development – Supplement
to the President's Budget FY2003" (Bluebook 2003), <http://www.itrd.gov/pubs/blue03/>
(和訳: <http://www.icot.or.jp/FTS/Ronbun/BlueBook2003-J.PDF>) .

付録A 半導体技術ロードマップについて

A.1 半導体技術ロードマップとは

世界の半導体産業は過去 40 年にわたり、急速な集積度向上を実現してきた。これは、集積回路を製造する際の minimum feature サイズの指数関数的縮小に多くを負っている。これはムーアの法則（チップ上のコンポーネント数は 18 ヶ月毎に倍増する）という形で、広く知られている。

この集積度向上のトレンド（スケーリング・トレンド）は、巨大な研究開発投資によって可能となっている。半導体国際技術ロードマップ（International Technology Roadmap for Semiconductors, ITRS[28]）は、半導体産業における今後 15 年間にわたる研究開発ニーズの現時点での見通しに関する産業界ワイドのコンセンサスを述べたものである。言い換えると、これまでと同等なペースでの集積度向上を実現し、産業としてさらに発展して行くために、半導体産業全体として、どのような研究開発を何時までにしなければならぬか、ということを書いたタイムチャートである。

A.2 最新の技術ロードマップ

半導体技術ロードマップは、米国半導体産業協会（Semiconductor Industry Association, SIA）が 1992 年に、半導体国家技術ロードマップ（National Technology Roadmap for Semiconductors, NTRS）を作成したのが始まりで、その後、1994 年、1997 年にロードマップが作成された。

半導体技術の国際化に伴い、1998 年にヨーロッパ（欧州半導体産業協会）日本（日本電子情報技術産業協会）、韓国（韓国半導体産業協会）、台湾（台湾半導体産業協会）に参加への呼び掛けがあり、産業界の国際的協力で ITRS 1998 年改訂版が出された。その後、1999 年版、2000 年改訂版、2001 年版、2002 年改訂版と続いている。（改訂版は、技術ロードマップ発行後の技術進歩を反映した変更を施したものである。予測対象期間は改訂前と変わらない。）最新の技術ロードマップは、2002 年改訂版である。2003 年版は 2003 年 12 月に公開される予定である。¹⁶

¹⁶ 本記述は、2003 年 11 月時点のものである。その後、2003 年 12 月に 2003 年版の技術ロードマップが公開された。

A.3 最新の技術ロードマップの概要

2002 年改訂版の技術ロードマップによると、2016 年までの MPU におけるゲート長の縮小トレンド（正確には 1/2 ピッチ）とクロック周波数の高速化トレンドは表 A-1、表 A-2 の通りである。

表 A-1 チップ性能（短期）

製造年	2001	2002	2003	2004	2005	2006	2007
DRAM 1/2 ピッチ (nm)	130	115	100	90	80	70	65
MPU/ASIC 1/2 ピッチ (nm)	150	130	107	90	80	70	65
チップ周波数 (MHz)	1,684	2,317	3,088	3,990	5,173	5,631	6,739

表 A-2 チップ性能（長期）

製造年	2010	2013	2016
DRAM 1/2 ピッチ (nm)	45	32	22
MPU/ASIC 1/2 ピッチ (nm)	45	32	22
チップ周波数 (MHz)	11,511	19,348	28,751

2003 年のクロック数は 3.088GHz、10 年後の 2013 年のクロック周波数は 19.348GHz と予想されている。ピッチが半分になる間隔は従来の 3 年よりも長く 5 年～6 年掛かるように予想されている（そのような技術開発が目標となっている）。すなわち、Moore の法則は、スローダウンすることが予定されているのである。

A.4 参考：ムーアの法則の限界について

ムーアの法則がいつかは限界に達することは、ほぼ明らかである。問題は、その限界が何処にあり、いつ限界に達するかということである。専門家は、過去に何度も、ムーアの法則が限界に達しようとしているという予測を表明し、その度に、予測が外れてきた。

最新の予測では、Intel の研究者が 2018 年に登場するとされている 16 ナノメートル製造プロセスないし、その 1～2 世代後（2025 年頃）が、トランジスタ・サイズ縮小の限界であると述べている（[29]）。

ただし、ゲート長縮小の限界に達したとしても、チップサイズの拡大や LSI3 次元実装などによって、集積度（チップ上のトランジスタ数）をさらに増大できる可能性はある。また、カーボンナノチューブ等、CMOS 以外のデバイスの実用化によって、次の限界に進むことが出来る可能性もある。

したがって、半導体集積度の増大は、2018 年頃までは技術的に見えているが、その先は非常に困難になる、ただし、さらなる向上を実現させる方向性が模索されている、というのが現状と言えよう。

付録B スパコン性能のトレンド

B.1 過去からのトレンド

各時点における最高速スパコンの性能（理論性能）をプロットしてトレンドを示したグラフを掲載する（図 B-1、図 B-2）。

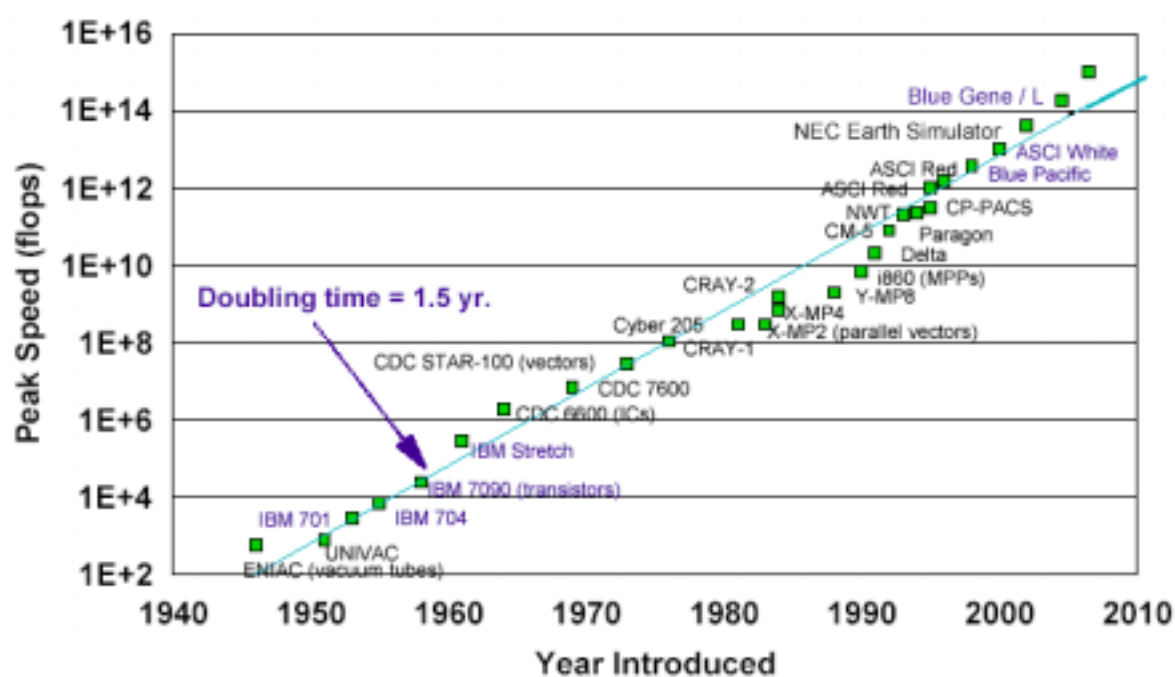


図 B-1スパコン・ピーク性能のトレンド（１）
出典：[30]

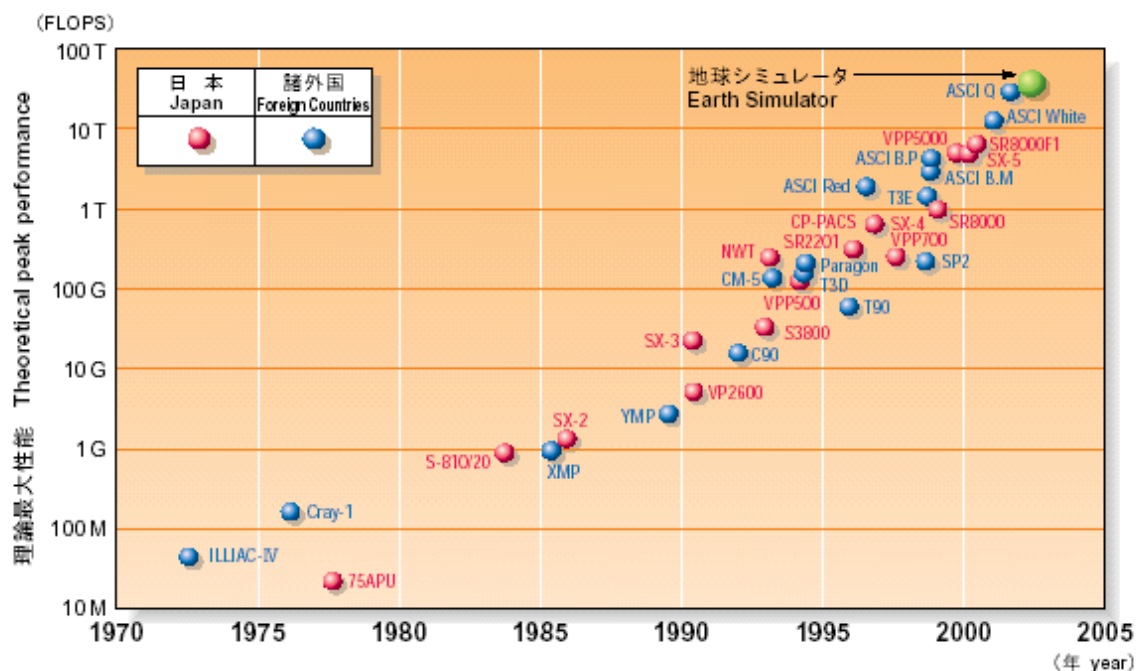


図 B-2 スパコン・ピーク性能のトレンド (2)
出典 : [31]

図 B-3では 1950 年頃から 2000 年頃までのスパコン性能の上昇速度を「1.5 年間で性能が 2 倍」(10 年で 100 倍)としているが、トレンドを見ると 1990 年以後は理論性能の上昇速度が上がっている。具体的には、10GFLOPS (1990 年頃) から 10TFLOPS (2000 年頃) までの 1000 倍の性能上昇に約 10 年と、1 年に 2 倍の割合で理論性能が上昇している。図 7 3 は、スパコン TOP500 の性能推移 (1993 年 6 月 ~ 2002 年 11 月) である。これは理論性能ではなく、LINPACK 性能 (問題サイズを調整して得られる最高性能、TPP) である。これによると、トップ 1 の性能は 1993 年 6 月の 60GFLOPS (CM-5) から、現在の 36TFLOPS (地球シミュレータ) まで、10 年間で 600 倍上昇している。

TOP500 - Performance

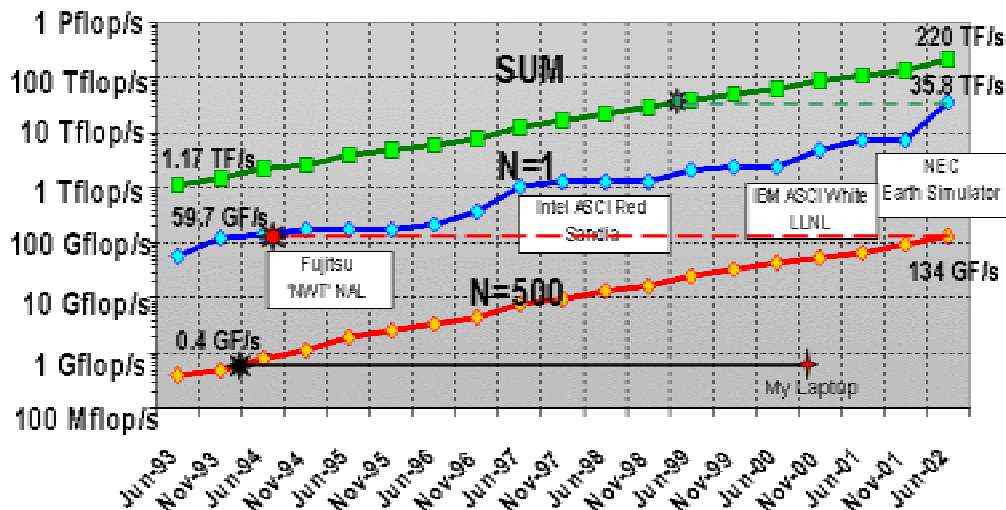


図 B-3 TOP500 スーパーコンピュータ性能（合計、N=1、N=500）
出典：[32]

1990年代のスパコンの性能上昇速度が増加した主要因は、並列化である。1990年以前のスパコンが、単一ないし少数のCPU構成のベクトル型スパコンであったのに対し、1990年代初めに、Intel Touchstone Delta(CPU数 512)、CM-5(CPU数 1024)、数値風洞(NWT、CPU数 140)など、CPU数が100～数百のオーダーの高並列計算機が登場し、性能上位を占めるようになった。2000年時点のトップであるASCI RedのCPU数は9632個である。ほぼ1990年代全体を通じて、汎用MPUを用いたスカラー並列型スパコンが性能リーダーであったが、その単一CPUのピーク性能上昇が1桁強(数10MFLOPS→数100MFLOPS)であったのに対し、CPU数の増加は2桁弱であった(数100程度から10,000)。

B.2 現状と今後の方向

1990年代以降、大規模並列化がスパコン性能上昇の主要因だったが、CPU数の増大に伴い、スパコンの価格や設置面積が非常に増大しており(米国ASCI計画[33]のスパコンや地球シミュレータなど、大きなスパコン用の建屋に設置されている)、これまでのペースでの規模拡大は困難になっていると思われる。例えば、米国連邦政府の情報通信分野の研究開発推進状況を報告しているBluebook 2003では、

「現在の米国のハイエンド・プラットフォームは、何千平方フィートもの床面積と何

メガワットもの電力を必要とする。1 つの大型システムに多数の汎用のマルチプロセッサノードを詰め込むというこのアプローチは、拡張性と価格の妥当性の点で限界に達しようとしている。」

と述べている([34]、日本語訳 p17)。このような現状において、主に以下の 4 つの方向が追求されている。

1. 従来からの方向（専用スパコン）
現在のスパコン技術の延長での性能向上（～数年後？）
（例）地球シミュレータ、ASCI 計画のスパコンなど。
2. 最近の傾向（コモディティ・スパコン）
（例）大規模 PC クラスタ
3. 新アーキテクチャ（本格稼働：数年後？～）
半導体技術にベースに、アーキテクチャ上の革新を実現
（例）BlueGene/L（IBM 社、2005 年本格稼働予定）
4. 新計算方式（実用化：10 数年後？～）
量子計算機、DNA 計算機、バイオ計算機などイノベーティブ計算方式の研究

今回の調査検討は、(1)～(3)をカバーしている。(4)については、前述のように、今回の調査検討には含めなかった。現時点では、実用化時期を精度良く予測することが不可能だが（性能はさらに予測不能）5 年後ないし 10 年後には、技術進歩のトレンドが現われている可能性があり、その時点で予測をすることが適当と思われる。

付録C 機密保持期間内の安全性の確保

5.3節で想定した解読計算時間は1年であった。これは、暗号化されたデータを攻撃者がすぐに入手して、すぐに（1年以内に）解読することを想定していることになる。

一方、暗号化されたデータがある程度長い一定期間（機密保持期間）内に解読されないことが求められることもある。

機密保持期間が s 年であったとすると、その期間内の安全性確保のためには、解読計算時間を s 年として、前述の方法に従って計算を行えばよさそうに思われる。しかしながら、機密保持期間がある程度の長さになると、その間の計算機性能向上と予算規模増大の効果が無視できなくなる。すなわち、データ入手直後に使用可能な解読計算システムで計算を行うよりも、一定の遅延の後に使用可能な解読計算システムを用いて、残りの期間で計算を行う方が、より大きな鍵空間を探索できるのである。

例として、機密保持期間が10年間の場合を考える。Lenstra-Verheulモデルのように価格性能比は1.5年で2倍、予算は10年で2倍の割合で増加するものとする。初年度の初めに価格性能比が1、予算が1であったとすると、構築できるシステムの能力は1になる。解読計算に掛けられる時間は10年なので、総計算量は10（単位・年）となる。同様に、システム構築時期を第2年度～第9年度とした時の価格性能比、予算、構築できるシステムの能力、解読計算時間、そして総計算量を求めたのが、表C-1である。

表 C-1 システム構築時期による処理量の違い

システム 構築時期 (年度)	性能/価格	予算	システム 能力	解読計算 時間 (年)	総計算量
0	1.000	1.000	1.000	10	10.000
1	1.587	1.072	1.701	9	15.312
2	2.520	1.149	2.895	8	23.156
3	4.000	1.231	4.925	7	34.472
4	6.350	1.320	8.378	6	50.270
5	10.079	1.414	14.254	5	71.272
6	16.000	1.516	24.251	4	97.006
7	25.398	1.625	41.260	3	123.780
8	40.317	1.741	70.197	2	140.394
9	64.000	1.866	119.428	1	119.428

これによると、10 年間の解読期間があった場合、8 年目にシステムを構築するのが攻撃者にとって最善であり、すぐにシステム構築をする場合と比べて総計算量は約 14 倍となることが分かる。

より一般に、一定期間内の任意の時点に任意量の予算を分散投入することができる場合（連続投資モデル）における考察を下に示す。計算能力と予算は、Lenstra-Verheul モデルと同様、指数関数的に増大するとする。

◆ 問題設定

現時点での価格あたり解析能力を p_0 とすると、現在を 0 としたときの時刻 t における最新技術では、価格あたりの解析能力 $p(t)$ は時と共に指数関数的に向上し、

$$p(t) = p_0 e^{at}$$

で与えられるものとする。

時刻 t において、時間あたり $x(t)$ だけの量のシステムを新たに構築するものとし、ある時刻 0 からシステム構築を開始して、時刻 t_1 までに解析できる総量を考える。時間あたり必要な費用は時間あたりの構築量 $x(t)$ に比例するものとする。その時点での最新技術を用いるので、時間あたり $p(t)x(t)$ の能力増強が行なわれることになる。能力増強はいつ行ってもよく、また、運用コストは無視する。

◆ モデル 1: 投じる総費用の上限 c のみが制約である場合

$$\text{【制約条件】 } \int_{t=0}^{t_1} x(t) dt = c$$

$$\text{【目的関数】 } \int_{t=0}^{t_1} \int_{u=t}^{t_1} x(t) p(t) du dt$$

【モデル 1 の最適解】

もっとも効果的な投資機会にすべてを投資するのが最適なのは明白である。つまり $x(t)$ はデルタ関数とするのがよい。投資が最適な時点は:

$$f(t) = \int_{u=t}^{t_1} p(u) du$$

を最大とする t である。

$$p(t) = p_0 e^{at}$$

だから、

$$f(t) = p_0(t_1 - t)e^{at}$$

となり、

$$f'(t) = p_0\{a(t_1 - t)e^{at} - e^{at}\} = p_0(at_1 - at - 1)e^{at} = 0$$

を満たす、すなわち

$$t = (at_1 - 1) / a$$

なる t の時点で全額を投資するのが最適、ということになる。

Lenstra-Verheul モデルと同様、価格性能比向上率を 1.5 年ごとに 2 倍とすると、

$$e^{at} = 2^{t/1.5} = (e^{\log 2})^{2t/3} \text{ すなわち } a = \frac{2 \log 2}{3} = 0.462098... \text{ となる。}$$

10 年後までかけて解読しようとするなら $t_1 = 10$ であるから、最適な t は

$$t = (at_1 - 1) / a = (0.462098 \times 10 - 1) / 0.462098 = 7.83596...$$

と、8 年経過後より少し前にシステムを作るのが最適ということになる。これを代入して、

$$f(t) = p_0(t_1 - t)e^{at} = 80.8794... \times p_0$$

となり、時刻 0 でシステムを構築して 80 年間運用した程度の処理を実現できる。すなわち、7.83...年後にシステムを構築して残る 2 年強の間運用するのは、当初からシステムを構築して 10 年間運用するのに比して 8 倍程度の費用対効果を得られるということになる。

この計算では運用コストを考慮に入れていないが、運用コストまで考慮すればこの差はさらに広がることになる。

◆ モデル 2: 投資可能な資金が年々増える場合

経済成長などの恩恵により、システムに投資可能な資金が刻々と増える場合を考える。現在の手元資金が一定の利率で増えると考えても同じことである。時刻 t における投入資金を $y(t)$ とし、現在からの資金増加係数を $g(t)$ とすると、投入資金の現在額は $y(t)/g(t)$ である。その積分値が現在の手元資金 c になる。また、時刻 t における時間当たり能力増強は $p(t)y(t) = p(t)g(t)x(t)$ であるから、制約条件と目的関数は以下の通りとなる。すなわち、

$$\text{【制約条件】 } \int_{t=0}^{t_1} y(t)/g(t)dt = c$$

$$\text{【目的関数】 } \int_{t=0}^{t_1} \int_{u=t}^{t_1} y(t)p(t)dudt$$

ここで、 $X(t) = y(t)/g(t)$, $P(t) = g(t)p(t)$ とおけば、

$$\text{【制約条件】 } \int_{t=0}^{t_1} X(t)dt = c$$

$$\text{【目的関数】 } \int_{t=0}^{t_1} \int_{u=t}^{t_1} X(t)P(t)dudt$$

となり、モデル 1 に帰着する。

Lenstra-Verheul モデルと同様、10 年間に 2 倍の経済成長とすると、上記のパラメータ算出式は

$$e^{at} = 2^{t/1.5} \times 2^{t/10} = \left(e^{\log 2}\right)^{23t/30} \text{ すなわち } a = \frac{23 \log 2}{30} = 0.531412...$$

となり、最適な t は

$$t = (at_1 - 1)/a = (0.531412 \times 10 - 1)/0.531412 = 8.11822...$$

と、さらに少し遅くにシステム構築をした方がよいということになる。このとき達成できる処理量は、

$$f(t) = p_0(t_1 - t)e^{at} = 140.6598... \times p_0$$

と、いきなりシステムを構築するより約 14 倍高い費用対効果を得られることになる。もちろん運用コスト面でも有利さは広がる。

結論として、計算システムの価格性能比の向上と解読に掛けられる予算規模の増大が Lenstra-Verheul モデルに従うと仮定した場合、機密保持期間を 10 年間とすると、約 8.1 年後に実現可能な解読計算システムを約 1.9 年間稼働させることによって、最大の鍵空間が探索できることになる（現時点で実現可能な解読計算システムを 10 年間稼働させる場合と比べて、約 14 倍の鍵空間の探索が可能）。