招待論文

ディジタル革命とその未来を支える基盤技術

森 亮一†

DRAM の集積度にならって 3 年間に 4 倍（10 の 0.6 乗），すなわち毎年 1.6 倍（10 の 0.2 乗）をディジタル革命の速度とする評価は広く認められているが，これはディジタル技術の進歩を的確に表しているとはいえない．きわめて過小な評価である．本稿では，演算装置の進歩を支えるナノ技術を中心とする様々な関連技術が「共進性」を持つことにより，技術の進歩が無数に生まれ，それらが共進的に助け合って，毎年 3 倍の猛烈な進歩がすでに 50 年間続き，その結果の性能の改善は 10 の 24 乗倍に達していることを示す．次に，ディジタル革命の社会的影響について分析する．人類に寄与する正の効果は計り知れないが，それを享受するためには，負の影響を解消するための基盤技術の研究開発が急務である．今後，長く続くこの激烈な進歩を支える不可欠な技術は，(1) 提供者の指定する支払いなどの条件と，ユーザの利便，たとえばコピーと利用の自由，との両立を実現するシステム，(2) 高位管理権者によるものを含めて，不正な記載変更が行われていないことを物理的に保証するシステム，(3) 正当な所有者が書きこんだ秘密の数値が分からない限り，誰にもやぶれないことを物理的に保証する保護容器，であることを述べる．

Emerging Technologies for the Digital Revolution

Ryoichi Mori†

The number of elements on a IC chip is quadrupling every three years, but computer performance as a whole is quadrupling annually. In this paper we demonstrate how nanotechnology and other closely related technologies reinforce each other to generate that higher growth rate, which has prevailed for the last half century and which has resulted in an astounding improvement in performance of 10^{24} over that time frame. These gains have made the digital revolution possible. The potential benefits to society of the digital revolution exceed our imagination, but to realize those benefits we must use competition among relevant technologies to prevent undesirable side effects. Superdistribution, the indispensable technology for gaining those benefits, depends on the availability of reliable, tamper-proof systems whose security is ensured through physical means. The Strong Tamper-Resistant Module (STRM), an improved version of our TRM (Tamper-Resistant Module), achieves that objective by using strong protection to ensure that only the possessor of a secret key can modify its behavior. Not even the STRM designers, manufacturers, or maintainers can gain unauthorized access to the module or modify its information or operation in any way. This level of security is what is needed for legal contracts and for system logs.

1. ディジタル革命の本質と社会的影響

1.1 年 3 倍の進歩

筆者は進行中のディジタル革命が史上最大の革命であると考える．この革命をそれほど重大とする主な理由の 1 つは，演算装置の進歩を支えるナノ技術を中心とする様々な関連技術が「共進性」を持つからである．ここで重要な点は，技術の進歩が無数に生まれ，それらが共進的に助け合って，毎年 3 倍の猛烈な進歩がすでに 50 年間続き，その結果の性能の改善は 10 の 24 乗倍に達していることである．「毎年 3 倍の継続」は誤植ではない．

DRAM の集積度にならって 3 年間に 4 倍（10 の 0.6 乗）したがって毎年 1.6 倍（10 の 0.2 乗）をディジタル革命の速度とする評価は広く認められている．総合的な性能が 1 桁変われば状況は一変する．集積度の進歩が年に 10 の 0.2 乗ならば 1 桁の進歩には 5 年かかる．秋葉原の様子が一変するのに 5 年かかるか．もちろん No である．したがって，毎年 1.6 倍をディジタル革命の速度とする評価は適切ではない．より実態を反映した速度は以下のように求められる．

† 超流通研究所，株式会社ナムコ顧問
Superdistribution Laboratory, Advisor to NAMCO LIMITED

まず，性能の向上は集積度の進歩だけではない．集積度が n の 2 乗倍大きくなるとき，演算速度の上限は n 倍速くなる．なぜならば平面型の集積回路において，チップ面積を一定とし，集積度が n の 2 乗倍になったとすれば，素子の寸法は n 分の 1 になる．演算速度の上限は素子の中での光の速度で決まるので，n 倍になる．すなわち集積度で n の 2 乗倍の進歩は，速度で n 倍の進歩をともなう．これで n の 3 乗倍の進歩である．

次に消費電力について考えよう．表面温度が同一ならば，放散できる熱量は面積あたり不変である．ゆえに集積回路の消費電力の上限はチップ面積あたりほぼ一定である．したがって n の 2 乗の集積度の上昇は，1 素子あたりの消費電力が n の 2 乗分の 1 に改善されていることを意味する．これと速度が n 倍になることを考えると，1 演算あたりの消費電力は n の 3 乗分の 1 になる．結局性能の向上は n の 6 乗になる．

1 年で 3 倍☆の進歩とすれば，2 年 1 カ月で 1 桁の進歩が起きる．秋葉原の様子が一変する時間としては，5 年より 2 年 1 カ月のほうが明らかに実態に近い数値である．

上の解析には，いくつかの補足説明が必要であろう．単位エネルギーあたりの計算処理量の進歩は，本稿の値より，実際の値が小さい．その理由は，年月とともに，材料の温度耐性および，熱放散技術の進歩などによる実用可能な放熱量の増加，演算速度の上昇を求めての注入エネルギーの増加などによって本稿が指摘する「単位エネルギーあたりの計算処理量の進歩」とは逆の傾向が共存するからである．このことは，高性能型の素子に多く見られる．そして統計や報道で多く取り上げられる傾向が強いのは高性能型の素子である．

また，単位時間あたりの計算処理量の進歩は，本稿の値より，過去の実績による進歩の値が大きい．本稿の値は，素子総数と，素子寸法と光速の関係による演算速度の上限との積である．過去には，このような素子寸法とは独立な別な上限があった．たとえば，トランジスタの初期には，可聴周波数での動作がやっとであった．

しかし，現在まではもちろん，未来はますます本稿の上限の値に接近してゆくであろう．そこで，過去の値が低いので，実績をそれから算出すると，本稿の値よりも大きい進歩の値が得られる．

☆ 本文中で述べたとおり，DRAM の集積度は 1 世代を 3 年として，4 倍/世代の割合で増大しているが，それにはチップ面積の拡大（約 1.3 倍/世代）が含まれている[1]．ここでの議論ではそれを差し引いて 3 倍/世代として計算した．

このような激烈な進歩は，我々の社会を支える基盤が，有体物社会における，メリットが拮抗し合う産業製品群から，共進的良さをもった産業製品群に一転したことを意味する．この共進性こそが，これまでは神の手によって，すなわち数十億年の偶然のゆらぎによって，生物にのみ実現できた性質なのである．

1.2 100 年以上継続する革命

進歩の最基礎部分が生命体的なものに，共進的なものになったことは人類史上初めてである．後述するように，この進歩は今後 100 年以上持続する．

ディジタル革命の影響の大きさを示そうとして，産業革命や津波あるいは集中豪雨にたとえる場合があるが，どれも不適切である．産業革命はエネルギーの工業生産を可能にしたけれども，質量・エネルギー保存則が核心であることには変わりがなかった．その意味で産業革命はディジタル革命の初期微動であるとたとえるほうがむしろ適当である．

津波や集中豪雨などで「緊急対策」と呼ばれるものの多くは，実は単なる「緊急避難」にすぎない．最悪の事態は長く続かないことを我々は経験的に知っているので，本格的対策が事態の峠がすぎてからになるのはこれまでは自然であった．ディジタル革命の場合に同様な対応は致命的である．なぜならば，この革命は今後 100 年以上にわたって継続する明瞭な理由があるからである．ディジタル革命では，今すぐに根本的かつ長期的対策を立て，至急に実行を始めることが正しいのであって，従来のような緊急避難で乗り切ろうとすれば大きな誤りになる．

津波や集中豪雨と違って，ディジタル革命は「絶対的な」限界に達するまで止まらない．現在の速度でナノテク化が進むとして，人間の技術が「神の」すなわち自然が数十億年の偶然のゆらぎによって創ったナノ構造の水準と比較できる程度になるまでに，100 年以上にわたって進歩が続くだろう．鳥のように飛ぶことの次にはジェット機を発明したように，さらに進むのではないかと思うが，その前までだけでも認識に価する．

もしディジタル革命を無理に集中豪雨にたとえるならば，それは降りが毎日前日よりも強くなる，そしてやむことのない豪雨である．その結果としては,「陸地などというものはなくなる」というたとえの方がよいであろう．そのときでも有体物は確かに存在するであろうが，それは情報の海の上に浮くハウスボートのようなものだろう．

1.3 有体物中心社会からの脱却

従来の産業製品には共進性がなく，各性能は拮抗的

であった．たとえば，自動車の定員（貨物自動車ならば積載量）は 1 つの性能である．価格も，速度も，単位燃料あたりの走行距離もそれぞれ 1 つの性能であるが，価格が半分に，定員が 2 倍に，速度が 2 倍に，そして燃料消費が半分になる，などという技術はない．

そこで有体物の産業では，大きな進歩は滅多にない．そのような進歩は「画期的」であり，この言葉そのものが「滅多にない」ことを示している．画期的な進歩から次の画期的な進歩までは妥協と折衷の長い期間である．したがって，年平均 10%を超えるような進歩は例外であった．このような環境が長く続いたから，社会も産業も学問も画期的な成果だけが最も重要であるとするようになった．

有体物中心社会の長い歴史の中で，比較的容易に達成できる共進的な改善はほとんど尽くされてしまった．そこで，有体物では，日々の設計の大部分は妥協点の発見になる．妥協による解は本質的に中途半端であり，その結果すぐに閉塞状態に達する．きわめてまれな高度なブレークスルーのみがこの閉塞情況の突破をもたらす．そのため，従来の社会では，高度な成果といえば困難なものに決まっており，ついには，何も良い結果をもたらさなくとも，高度に困難であるだけで高く評価されるような風潮になった．

1.4 情報処理が産業の中心になる

ディジタル革命が長く続く理由は，世界中の人間と資本がディジタル情報の分野に流入を続けるからである．ますます多くの人々が，ディジタル情報の分野が有利な投資先であることに気づいて，自分とその財産を投入する．それは，ある時間の遅れをともなって結果として現れ，さらに正のフィードバックを引き起こす．

農業，漁業，自動車産業などの何をとっても，それらの産業のある部分は特有であるがある部分は情報処理である．

漁業を例にとろう.「操業地までのルートの決定」から始まり,「どの市場に送るのが最も有利かの計算」などを含めて，漁業の半分程度は情報処理であると考えられるだろう．あらゆる産業の半分は結局は情報処理である．そのためのコンピュータシステムの生産は，ディジタル革命の進歩とともに，他のハードウェアたとえば農業のための農地や潅漑施設，自動車工場のための生産ライン，などの総和に匹敵する産業規模になる．

これだけであれば，GDP のたとえば 50%がコンピュータシステムになるだろう，で話は終わる．けれども実際にはその先がある．コンピュータシステムを研究・開発・設計・製造する技術と，量産されたそのシステムを効率よく利用する技術とは，関係はあるが別のものである．

これは自動車を研究・開発・設計・製造する技術と，自動車を運転・利用する技術とが，関係はあるが別なものであるのと同様である．現在および将来の社会では，コンピュータを作る人々の数に比べて使う人々の数の方が圧倒的に多い．これは他の産業分野でも同様である．漁業のための各種装置を効率良く使用することは 1 つの教育である．この教育のかなりの部分は現在でもディジタル情報処理である．マルチメディア技術やバーチャルリアリティ技術の進歩によって，教育はますますディジタル情報処理の直接の応用になってゆく．これらのことを考慮すると，GDP のたとえば 4 分の 3 がコンピュータシステムの生産とディジタル情報処理とであるという状況が起こるだろう．

1.5 少数の勝利者，迅速な交代

ネットワーク革命の進行にともなって，少数の勝利者が市場の大きな割合を占有するようになる．ユーザから見てより優れた品質を提供する新しい勝利製品によって，品質の急激な改善が持続される．新たな勝利者の出現する間隔は急激に詰まり続ける．理由は次のとおりである．

ディジタル革命の世界では，毎年 3 倍の進歩がある．そこで，的を射た質の良い総合的予測の価値がきわめて高くなる．個人の天与の資質に依存する点で，芸術やスポーツの世界に似てきた．いかに難行苦行しようと，資質のない人には良い芸術や高い記録が作れないのと同様なことが，産業の中心的分野で起きる．

社会にとって予測者が重要になる．このことは，証券・為替の取引などではすでに起きている．予測者にとって最重要な能力は，芸術家やスポーツマンと同様に，第 1 に天与の資質，第 2 に努力する才能である．これらを担保するのは，過去に完成された学問の暗記や理解ではなく，過去に行った創作・競技・予測の成績である．従来の学問や就職条件として第 1 であった暗記や理解は第 3 位以下にすぎない．このことの理解と実行がその社会の先進度を決め，どの集団が世界に卓越するかを決めるようになるだろう．

1.6 先見性と経営判断

進行中のディジタル革命のような激動期では，先見性と経営判断の適切な組合せが求められる．人々は，有能であるほど，ふつう後者に投入される．なぜならば，いつ，何を，いくらで，どのように製造し，契約し，市場展開するかなどのあらゆる事柄は，その 1 つを誤るだけでも致命的になりかねず，しかも，完全な

判断根拠なしに，十分とはいえない時間的余裕で次々と決定を求められるからである．このような経営判断をやり抜いて初めて，競争における勝者となる．したがって，迅速な経営判断の能力が経営の神髄とされるのは妥当であろう．

一方，先見性は，十分に考え，可能な枝分かれは読み切ることによって正確になる．ところが，社会はそのような時間を許さない．たとえば，メディア上の討論では，即座に返事ができることが重要であり，散会後の答えは正しくても無効である．しかし，迅速な応答が正確であるという保証はまったくないし，程度を超えて迅速な応答は大きな誤りを含む．

では，どうしたらよいのか．適切なチームを組むことが答えであろう．そこでは，各種のスポーツのように，考えるよりも早く，反射的に体が動く神経を，生まれながらに，また訓練によって持つことが競技の神髄であり，そのような人々が中核プレイヤーである．同時に，実技はしないが，適切なコーチの有無がチームの勝敗を決めるだろう．

1.7 不正義・不平等の阻止が世論になるか

コンピュータ・リテラシーによる不平等でさえ，現代社会にとってすでに重大な問題である．少数の勝利者，迅速な交代は，リテラシーの不平等を著しく激化する．これは不正義であって阻止すべきであるという意見がある．

しかしこれは本当に不平等だろうか．次のたとえが有効と思う．普通の人，たとえば筆者やその仲間がいる．特別な人，たとえばオリンピックのゴールドメダリストや，芸術界のトップにいる人がいる．普通の人の方が，特別な人よりも多い．

収入や社会での待遇にはかなり相違がある．しかし，必ずしも不平等ではないだろう．速く走れば，私でも，ゴールドメダリストになれるのであれば．

これに対して次のような反論も想定できる．ゴールドメダリストや，各界のトップは少人数である．しかし，このネットワーク・リテラシーの問題では，小学校のクラスの，半分は上位階級の家族，残りは下位階級の家族で社会に中位階級が存在しないというようなことが起こって，大規模な問題になるのではないかという考えが現れるだろう．結論は時間を必要とする．

1.8 社会への 2 種類の影響——個別性能と普及度

個別性能とは，上で，毎年 3 倍の進歩がある，とした性能を示す．普及度については，1 万台の電話機に比べて，10 万台の電話機は少なくとも 10 倍，おそらくはさらに大きく価値があるといいたい．しかし，普及度には，個別性能で展開できた議論のような，明快な定量的評価がまだない．それでも，個別性能だけでなく普及度も考慮すべきであり，そうすれば革命による性能の改善はさらに巨大になる．このことが，適切に認識されるべきだろう．

2. ディジタル革命の負の影響

質量・エネルギー保存則は重要な物理法則の 1 つであるが，情報には質量・エネルギーのような保存則がない．このことの正の影響は大きく，それについての人々の理解はまだ十分とはいえないことは，上述したとおりである．さらに一方で，負の影響についての多くの人々の理解には，まだ根本的に欠けたところがあるように思われる．

読者の財布が，私のポケットにあれば他所にはないのは，保存則による．飛行士が，月面に居れば地球上に存在しないことも，保存則による．犯罪が起きたとき，証拠は現場にあって，たぶん読者のポケットにはない．これも保存則による．

保存則の有無によって，次のような違いが起きる．財布を金庫にしまうと，原理的に独立な 2 種類の防御機能が実行される．第 1 に，金庫によって，財布を盗むことが妨げられる．第 2 に，金庫を開けて財布があれば，それは財布が盗まれていないことの証明になる．この 2 つは「直交する」すなわち「互いに独立な」事象である．その証拠に，情報を金庫にしまう場合を考えてみるとよい．金庫にしまうことによって，情報を盗むことを妨げる防御機能は働くが，金庫を開けてそこに情報があっても，情報が盗まれていないことの証明にはならない．

このような負の影響が顕著に現れたのが，ディジタルコンテンツの不正利用，プライバシー侵害，ネットワーク犯罪の深刻化である．これらを解決するための未来志向の研究開発が急務である．ディジタル革命を支える基盤技術を考えるとき，次の 3 つの技術に集約できる．

超流通 提供者の指定する支払いなどの条件と，ユーザの利便，たとえばコピーと利用の自由，との両立を物理的に保証できる流通システム．

潔白性 高位管理権者によるものを含めて，不正な記載変更が行われていないことを物理的に保証できる性質．文書一般，なかでも特に契約書・システムログに適する☆．

☆ 似ているが次のことはできない．「不正な記載変更が物理的に不可能であることを保証できる装置」は，記載変更が抹消を含むことを考えると実用的な装置では不可能である．どんな実用的な装置でも，その装置そのものを盗みまたは消滅させることを，確実に防止すると保証することはできないからである．

強防御 正当な所有者が書き込んだ秘密の数値が分からない限り，強い攻撃者，たとえばその強防御装置の製造者，修理者にも破れないことを物理的に保証できる防御．

3. 超 流 通

知的財産の保護・流通については「超流通」[2)~4)] が基盤技術となることが，以下に述べるように広く認められつつある．

3.1 超流通の特徴

3.1.1 特 徴 1

「提供者の知らないところでの自由なコピーからでも，コンテンツ利用料が，提供者に，自動的に適切に分配される．」

超流通でしか実現できない，超流通の最大の利点である．提供者にとっては，究極の魅力的な課金構造である．このため，大規模な市場が確立してからは，主流になる可能性が大きい．

3.1.2 特 徴 2

- コンテンツは，保護された形で電子的に配布することができる．
- コンテンツ利用料が提供者に適切に分配される．
- 利用の条件を自由に設定することができる．
- 利用者は，無料またはきわめて低価格でコンテンツを入手することができる．提供者が許せば試用することもできる．

コンテンツの質と同時に，利用者の利便を考慮した利用条件の設定が重要視されるようになる．

3.1.3 特 徴 3

「複数のコンテンツがハイパーリンクされた状況でも自動的課金が可能」

マルチメディアコンテンツ開発においても，利用許諾および課金の自動化ができる．

3.1.4 特 徴 4

構造はある程度複雑で，初期には，その分だけ余分な費用がかかるように見え，ユーザにも提供者にもそのことへの心理的抵抗がある．ディジタル革命の進行にともなって，超流通を運用するためのコストはきわめて低くなる．それと同時に，ディジタルコンテンツ流通規模が巨大に，そして単価が低くなるので，他の方式では不十分であることが事実によって証明されつつある．

3.2 超流通への評価

超流通は未来を示した．その認識は米国の方が早かった．

1989 年の米国 “BYTE”（1 月号，pp.343–351）は特集企画で人工知能，IC，高級言語，UNIX と C，のそれぞれの創始者である Minsky，Kilby，Hopper，Ritchie に続けて超流通の Mori をあげた[5)]．

1990 年の米国 “BYTE”（9 月号）は，15 周年記念の特集で，パーソナルコンピューティングに最も影響力がある世界の 63 人を選び，表紙にその名前，テーマ，所属をあげた．Mori と超流通がそれに選ばれた[6)]．

1992 年の “Dr. Dobb’s Journal”（10 月号，pp.44–48）に，OOPS（Object Oriented Programming System）の仕掛人の 1 人である Cox が書いた論文の表題は “Superdistribution and Electronic Objects” であった．彼は超流通を彼自身のテーマより前において彼の評価を示し，超流通を “Revolutionary Approach” であると述べている[7)]．

また，Cox は 1996 年に，“Superdistribution – Objects as Property on the Electronic Frontier” と題する書籍を出版し，超流通が重要な基盤技術であるとの評価を維持している[8)]．

米国 “Wired”（1995 年 3.06 号）の “Reality Check” において，超流通を含む 5 つのソフトウェア技術について，Novell，OMG，Microsoft などの専門家が評価した．その結果，専門家の大多数が「2005 年までには，超流通のためのハードウェアが PC の標準的な構成要素になるだろう」と考えていると結論した[9)]．

『日経エレクトロニクス』（1999/3/8 号）は，コンテンツ流通特集を組み，大手など 6 グループの事業計画などについて述べた．その中で,「ここにきて，システム全体の基本的な枠組みがみえてきた」として超流通をあげた[10)]．

また，研究レベルでは，発案者のグループ以外の研究者による論文も，電子情報通信学会，情報処理学会などの論文誌で出版され[11)]，実用化レベルでは，音楽コンテンツ流通を中心とする，しかしそれに限られない民生応用がいくつかの大会社の連合企業によって間もなく始められる段階にある．

4. 潔白性と強防御

ここでは，ネットワークセキュリティの現状を分析し，潔白性と強防御が不可欠であることを解説しよう．

4.1 セキュリティにおける直交性

ある会社の社長 P が身分証明書を紛失しまたは盗まれたとする．この場合に「あの人 P は身分証明書を持っていないがしかし我が社の社長である」という確認が身分証明書と独立にできるならば，その社のセキュリティは，身分証明書による座標に加えて直交す

る別の 1 つの座標を持っている．このときまた,「あの人 S は我が社の社長の身分証明書を持っているがしかし我が社の社長ではない」ことを確認する手段があれば，これも身分証明書による座標と直交する 1 つの座標である．

セキュリティを構築するとき，このように直交する複数の座標が実用上不可欠であることは明らかである．しかし，その必要は我々の経験によって認められるのであって，セキュリティに関する厳密な証明，すなわち，公理に基づく証明でその必要が導き出されることはない．なんとなれば，厳密な証明では，公理が正しいか否かについての議論は原理的に不可能だからである．

ディジタル情報技術は著しく若い．秘密鍵暗号方式や公開鍵暗号方式におけるこれまでの高度な議論はほとんどが厳密な証明に基づいている．それに対して，ディジタル革命が実現する社会のセキュリティは，そのような厳密な技術に加えて，それと直交する多様性のあるセキュリティを不可欠のものとして求める．

厳密な暗号は計算機技術の 1 つの中核として正当な注目を得て推進されているが，それと直交する多様性のあるセキュリティは，まったく異なる発想と，破壊されたセキュリティの実例と，ユーザの快適さについての今後の長い経験と知識の集積によって提供され改善されてゆく性質のものである．

4.2 セキュリティの最大の穴は人間である

セキュリティの最大の穴が人間であることについては専門家の間でも異論はないように思われる.「セキュリティの鎖はその中の最も弱い輪で切れる」こともまたよく知られた事実である．これら 2 つの表明が事実であるならば，この穴をふさぐための電子技術の研究・開発がセキュリティにとって最も重要なはずである．実際にそうなっているだろうか．答えは No であるように見える．

この穴をふさぐための電子技術がまだない理由を検討しよう．原子力の例を考える．物理的な式やマニュアルの記述があっても，人間がそれを適切に守るとは限らない．そして実際そのようにして事故が起こった．にもかかわらず，この課題への取組みは最重要なものとは設定されなかった．その理由は，おそらく原子力の場合，万一事故が起こったときの悪影響は恐るべきものなので，そのようなことが起こらないようにすること，すなわち，人間が穴になることがないように物理的，機構的に対策することに力点がおかれたためであろう．それでも現在になってみると，人間という穴をふさぐことが投資対策として最大の価値があったことが明らかであるように筆者には見える．

ネットワークセキュリティでは，原子力のような致命的で長期に影響する事故の可能性が本質的に小さいと考える人々がいるかもしれない．しかし次のことを忘れてはならない．原子力の事故では，事故がより一層凄惨になることを希望する組織や人々はほとんどいないことを前提にできる．ネットワークセキュリティではそうではない．巨大で，優れた能力を持ちそして存在そのものも知られていない組織が事故を計画し，事故の拡大に努める可能性がある．また，そのような組織による小手試しなどがあっても，それによる損失が巨大すぎて隠蔽できなくなるまでは，被害を受けた機関自身が隠蔽につとめる可能性も存在する．

4.3 ディジタル社会の証拠性を確立する潔白性と強防御

他の例を考えよう．ディジタル革命以前において，直交したなるべく多様な防御機能が必要であるという認識とその実践とが目立たなかった理由は，特段の措置をしなくとも，それがほぼ自動的に行われたからである．たとえば事件があったとすると，そこで血液，DNA，指紋などの証拠が「自然に」発生する．犯人がそれを避けようとして手袋をしたりしても，ある金庫が破られたとき，それを破った人間が金庫の近くにいただろうことは確かであった．

ディジタル革命によって，このような確かさはどんどん少なくなる．一方で，適切に設計されていないシステムでは，証拠を抹消し改竄することがますます容易になる．ここでもやはり，人間という穴をふさぐことが最も重要であると筆者は考える．そのための電子技術が，ネットワークセキュリティのための新しい技

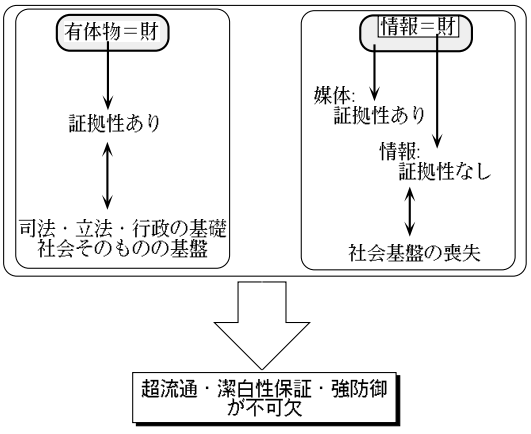

図 1 超流通・潔白性・強防御の必要性
Fig. 1 Need of superdistribution, cleanliness, and the strong tamper registant module.

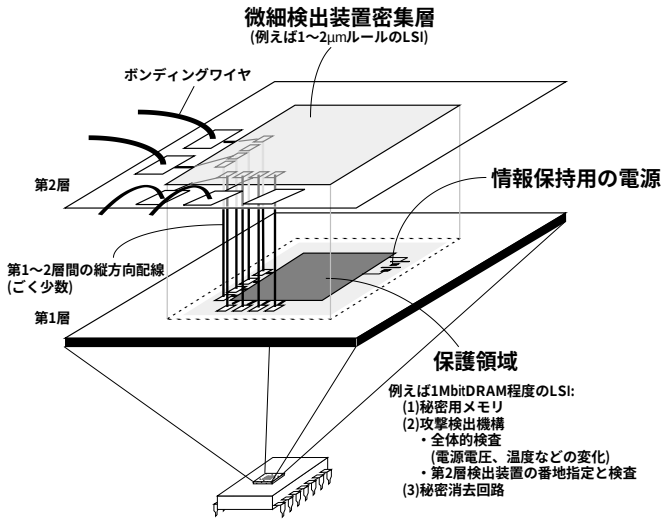

図 2 3 次元 IC を利用した強防御の例
Fig. 2 Example of three-dimentional IC implemetation of strong tamper registant module.

術分野になるだろう.

社会におけるディジタル情報の重要度と，必要なセキュリティの種類は，**図 1** に示すように変化してゆくことは明らかであり，強防御と潔白性の保証とが不可欠である．これを実現するための要素技術として，**図 2** に示した保護容器がある．これを利用した，ログ管理システムが提案されており，ログの証拠性とプライバシーの保護の両立を目指すものとして，今後が注目される[12].

5. む す び

本稿では，進行中のディジタル革命を分析した．演算装置の進歩を支えるナノ技術を中心とする様々な関連技術が「共進性」を持ち，それらが助け合って，猛烈な進歩がすでに 50 年間続き，その結果の性能の改善は 10 の 24 乗倍に達していることを解説した．これは，毎年 3 倍の進歩を意味しており，この進歩が今後 100 年以上継続することを述べた.

そして，この革命の恩恵を享受するためには，超流通，潔白性保証，強防御の 3 つの基盤技術の研究開発が急務であることを示した.

ディジタル革命で機械の処理能力とエネルギー効率は激烈な進歩を続ける．革命はますます加速する．その一方で，人間が考え，行動する基本的な速度は変わらない．人間性の豊かさも，人間の思索・判断能力も，急には変わらない．道徳心や優しさは，改善されるかもしれないが，ゆっくりであろう．上の 3 つの基盤技術は，このギャップを埋めるものであり，研究開発および制度の整備が，重要な仕事になる.

参 考 文 献

1) 徳山 巍, 橋本哲一（編著）：VLSI 製造技術，日経 BP 社 (1989).
2) Mori, R. and Kawahara, M.: Superdistribution: The Concept and the Architecture, *Trans. IEICE. Japan*, Vol.73, No.7, pp.1133–1146 (1990).
3) 森 亮一，河原正治：歴史的必然としての超流通，情報処理超流通・超編集・超管理のアーキテクチャシンポジウム論文集，Vol.95, No.1, pp.67–76 (1994).
4) Mori, R. and Kawahara, M.: Superdistribution: An Electronic Infrastructure for the Economy of the Future, *Trans. IPS. Japan*, Vol.38, No.7, pp.1465–1472 (1997).
5) Mori, R.: What Lies Ahead, *BYTE*, Vol.14, No.1, pp.343–351 (1989).
6) Mori, R.: On Superdistribution, *BYTE*, Vol.15, No.9, p.344 (1990).
7) Cox, B.: Superdistribution and Electronic Objects, *Dr. Dobb's Journal*, No.193, pp.44–48 (1992).
8) Cox, B.: *Superdistribution – Objects as Property on the Electronic Frontier*, Addison-Wesley (1996).
9) Pescovitz, D.: *Reality Check*, http://www.wired.com/wired/3.06/reality_check.html (1995).
10) 特集 音楽配信マッタナシ，日経エレクトロニクス，1999 年 3 月 8 日号，p.96 (1999).
11) 末松俊成，今井秀樹：ユーザのプライバシー保護が可能な超流通ラベル配送形超流通システム，電子情報通信学会論文誌，Vol.J81-A, No.10,

pp.1377–1385 (1998).
12) 河原正治，大瀧保広：超流通技術に基づくアクセスログ管理方式の提案，情処研報，Vol.2000, No.56, pp.33–40 (2000).

(平成 12 年 7 月 18 日受付)
(平成 12 年 9 月 7 日採録)

森　　亮一（正会員）

東京大学工学部卒業．同大学院（旧制）特別研究生．スタンフォード大学客員研究員．通商産業省電子技術総合研究所論理システム研究室長．筑波大学情報学類長，筑波技術短期大学教授．神奈川工科大学情報工学科長等．筑波大学名誉教授．（株）ナムコ顧問．工学博士．

【ゲストエディターからの補足説明】

この論文について，特集号編集委員会において理解しやすさのチェックを行った際，論文の最初に書かれている性能の向上の速度については根拠が十分説明されていないので読者に誤解を与える恐れがあるとの指摘がありました．そこで，特集号編集委員会としては，この性能向上速度に関する理論はあくまでも「仮説である」ことを明記していただくことを著者にお願いしました．これに対し，修正原稿では一部数値の変更がありましたが，仮説であるとの明記は行われませんでした．しかし，本論文の価値はその性能向上速度の数値にあるのではなく，きわめて急速な性能向上によって「史上最大の革命」が起きているという主張とそれを支える基盤技術に関する記述にあり，そのことについて読者が誤解をする可能性は少ないと判断して修正原稿を採録することにしました．

【著者からの補足説明】

本稿は，我々が経験しているディジタル革命の速度を，集積度の向上速度とそれにともなう共進性によって説明しようとする理論であり，本理論の主要な論旨が正しいか，誤っているかは今後のディジタル革命によって明らかになると考えています．