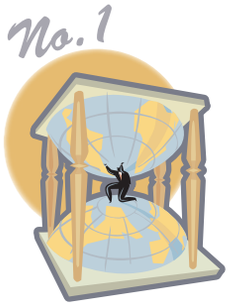

社会情報インフラの安全と信頼

坂井修一　東京大学 大学院情報理工学系研究科

~~~~~ 社会情報インフラのディペンダビリティ ~~~~~

安心・安全という言葉が金科玉条のように使われているが，中でも社会情報インフラの安全と信頼は最も重要なものの１つと言えるだろう．近年では，安全性（safety）や信頼性（reliability）とセキュリティ（security）☆1 を統合する考え方として，ディペンダビリティ（dependability）という言葉がよく使われるようになった．

情報システムのディペンダビリティは，“提供するサービスに見合う情報システムの信頼性”と定義される[2]．これは，従来の安全性・信頼性・セキュリティ・可用性・完全性・保守性を統合する概念であり[3]，さらに拡張性や頑健さを含むと考えられる[4]．

信頼性は，故障（fault）・誤り（error）・障害（failure）という経路で損なわれる[5]．これにセキュリティが損なわれる経路を合わせると，**図-1** のようになる．外部からの攻撃（attack）や故障によって，システムに誤りが起こり，これが外部から見える障害となる．階層的なシステムでは，下位階層の障害が上位階層への攻撃や故障となって伝播してゆく．これが，ディペンダビリティ阻害の基本経路である．

~~~~~ なぜ今，情報ディペンダビリティか ~~~~~

今，情報ディペンダビリティをとりあげるのは，言うまでもなく社会における情報インフラの重要性がかつてとは比較にならないほど大きくなっているからである．情報システムは職場や家庭のあらゆる場所に浸透し続けている（グローバル化・ユビキタス化）．それとともに，情報システムは我々の生命や財産に直結したライフラインとなっている．端的に言えば，「ネットには人命がかかっている」のである．

☆1 狭義の安全性は，「機械の故障，ソフトウェアのバグ等による誤動作，誤操作，自然災害等によって確率的に生じるリスクを最小化すること」，セキュリティは，「意図的・組織的な犯罪行為・不正行為，大規模災害等によって非確率的に生じるリスクを最小化すること」と定義される[1]．

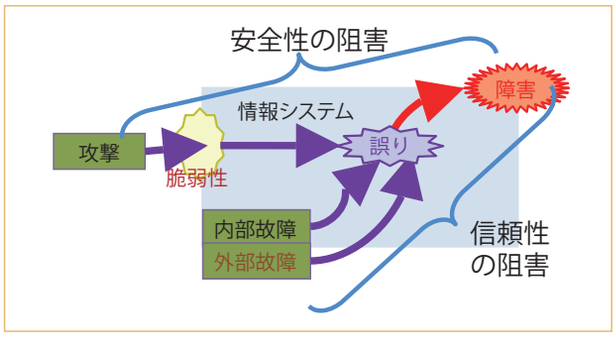

図-1　ディペンダビリティ阻害の経路

~~~~~ ディペンダビリティ阻害要因と事件 ~~~~~

情報インフラは，その発展とともに不確実性を増している．その要因を以下に記す．

(1) VLSI の微細化・高集積化による設計・テストの複雑化と PVT（Process, Voltage, Temperature）耐性の低下
論理ミスやマージン不足などの設計ミス，製造のばらつき，クロストークやリーク電流などの内部ノイズ，粒子線・熱・電源電圧の変動などの外部ノイズ，経年変化など．

(2) ソフトウェアの複雑化による検証困難と脆弱性の混入

(3) 悪意あるユーザの遍在
不正アクセス，ウィルス，タンパリング，DoS（Denial of Service）攻撃，サイバーテロなどの起点となる．

(4) ヒューマンファクタの増大・増加
うっかりミスや認識不足による誤操作．

(5) 情報システムのブラックボックス化
中身を知らずに使うことによって，誤動作や情報漏洩が起こる．

(6) ベストエフォート文化の浸透による生産者の責任を問えない体制
インターネット接続速度やソフトウェアのサービス提供で一般的となった“ベストエフォート”の契約は，生産性・利便性を高める効果があるが，同時にディペンダビリティを低下させる元にもなる．

事件	詳細	損害
Intel Pentium（1994）	除算器の設計ミス	全数リコール，損害 4.75 億ドル
ウィルス，ワーム	Code Red, NIMDA，Netsky など	情報流出，スパムメール発信，データ破壊，システム不安定化（2005 年の損害 1 社平均約 1.3 億円[6]）
東証オンラインシステム障害（2005）	システム障害	午前中の取引完全停止
東証ジェイコム株大量誤発注（2005）	誤操作（＋仕様ミス）	損害 414 億円（係争中）インタフェースを含む仕様の改善
東証取引停止（2006）	ライブドア事件による過負荷	全銘柄取引停止
ANA システム障害（2007）	スイッチの物理故障＋ゲートウェイプログラムのバグ	130 便欠航，306 便遅延（79,000 人に影響）
政府・官公庁へのサイバーアタック	官公庁 Web ページ改竄，エストニア事件（2006）	行政サービス停止など
Winny を介した情報流出	国土交通省，国税庁，陸上自衛隊，京都府警，郵便局，NTT 東日本，東京電力，朝日新聞社など	個人情報流出

表 -1　情報システムの障害による事件（例）

	省庁・機関	組織
政府	内閣府	情報セキュリティセンター（NISC）
	総務省	情報通信政策局　セキュリティ対策室
	経済産業省	商務情報政策局　情報セキュリティ政策室
	文部科学省	研究振興局　情報課
	法務省	情報化推進会議
	防衛省	情報本部
	警察庁	総合セキュリティ対策会議
協会など	日本学術会議	拡大情報委員会　セキュリティ・ディペンダビリティ分科会
	情報処理開発機構（IPA）	セキュリティセンター（ISEC）
	科学技術振興機構（JST）	研究開発戦略センター
	日本情報処理開発協会（JIPDEC）	情報マネジメントシステム推進センター
	情報サービス産業協会（JISA）	情報セキュリティ部会
	日本情報システム･ユーザー協会（JUAS）	情報セキュリティ委員会
学会	情報処理学会	コンピュータセキュリティ研究会，ISO 関係標準化
	電子情報通信学会	ディペンダブルコンピューティング研究会，情報セキュリティ研究会，信頼性研究会
	日本ソフトウェア科学会	ディペンダブルシステム研究会

表 -2　政府・学協会組織（2007.11 時点）

表 -1 に，これらが原因で起こった事件・事故の例をあげた．

~~~~~　政府・学協会などの取り組み　~~~~~

表 -2 に，情報ディペンダビリティに関する政府・学協会の組織をあげた．これ以外にも，JPCERT や地方自治体・企業・大学の機関内の組織などがある．

表 -2 より，以下の問題点が指摘できるだろう．

(1) 政府に数多くの縦割り組織がある．中には，CRYPTREC（Cryptography Research and Evaluation Committees，総務省・経済産業省の協力による暗号の評価・監視機構）のように省庁間の協力による組織はあるものの，いまだ統合的・合理的な動きが取りにくいように見える

(2) セキュリティと耐故障性（＝狭義のディペンダビリティ）の分野統合が十分でない

(3) 政府系組織にセキュリティ関係が多いが，耐故障性部門が少ない

学会関係でも，セキュリティとディペンダビリティは別研究会として活動している．本会の論文誌でも，「セキュリティ」「ディペンダブル情報処理」と 2 種類の特集号が組まれており，そのほかでもディペンダビリティ関連の記事はさまざまなイベントや特集の一部をなしていることが多い．ジャーナル論文誌に掲載されたディペンダビリティ関係の記事を総計すると，2006 年では 66 件であり，全体の約 13%になる[4]．

政府系においても，学協会においても，統合的・合理的な動きが必要であり，また，政府と学協会の密な協力が大切になっているといえる．

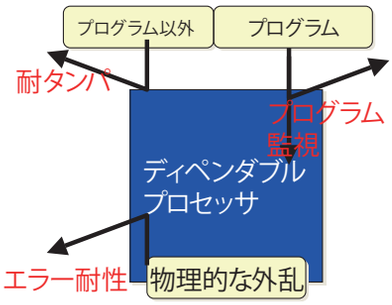

図 -2　プロセッサのディペンダビリティ機能

課題と実現

我々の課題は，ユーザの立場でどのようなディペンダビリティがどの程度必要かを知り，そのための手段を講じることである．そこで，ユーザからの要求の定式化，ディペンダビリティのモデル作成，実現手段の検討，コスト評価という一連の作業が必要となる．

情報ディペンダビリティは，原理，デバイス，ディジタル回路，アーキテクチャ，オペレーティングシステム，アプリケーションソフトウェア，ヒューマンインタフェースのそれぞれの技術階層で必要になる．1 つのディペンダビリティ機能がどこか 1 つの階層で実現される場合もあれば，複数の階層の協力ではじめて達成される場合もある．ディペンダビリティのためにはどのような機能・技術が必要か，ある機能はどの階層で実現されるのが最適か，などが課題となる．

表 -1 を見ても分かる通り，故障や攻撃には人間的なミスや社会常識の問題が大きくかかわっていることが多い．したがって，ソフトウェアを含む技術の問題に加えて，リスクマネジメント（Risk Management, 危機管理）や教育・啓蒙など人間的な課題の解決が重要となるだろう．

技術的課題とアプローチ

ディペンダビリティの実現は，原理的に 3 つの方法がある．故障や攻撃の発生を予防する「回避」(prevention)，故障や攻撃の数や程度を減少させる「除去」(removal)，故障や攻撃が生じても正しいサービスを提供する「耐性」(tolerance) がこれである．このうち，一般に，回避が最も予測困難でコストがかかると考えられている．

情報システムのディペンダビリティは，検証，テスト，冗長化・多重化，暗号化，仮想化などの技術によって向上する．セキュアプロセッサや侵入検知ハードウェアの活用，特殊な命令セットや通信プロトコルの導入など，高度な手段を講じることが必要な場合もある．

一例として，プロセッサのディペンダビリティ機能を**図 -2** に示す [7]．プロセッサの場合，ディペンダビリティ機能は，エラー耐性，タンパ耐性，プログラム監視の 3 つを総合したものとなる．

ディペンダブルなプロセッサのために必要な要素技術は次のようなものである．

(1) エラー耐性
　ソフトエラー防止機構：ECC による冗長化など
　タイミングエラー防止機構：遅延クロックの導入など
　永続エラー耐性：冗長化・多重化・再構成可能回路の導入など
(2) タンパ耐性
　データ暗号化回路
　アドレス分散化機構
　インテグリティチェック機能
(3) プログラム解析・監視
　コンパイラによる静的解析
　タグ付けと伝搬によるデータの動的監視

プロセッサへの要求に応じて，これらを実現することになるが，実際には，ハードウェア実装規模（VLSI 上の面積），消費電力，性能への影響，コストなどを検討しながら，最適な構成をとることとなる．また，これらすべてを活用し，故障・攻撃の検知から障害回避・回復までを制御するための機構が必要となろう．

リスクマネジメント

リスクマネジメントは一般的なビジネス用語であり，“リスクを認識・予測し，深刻さとコストに応じて回避・対処などの手段を講じること”と考えられる．特に情報処理の世界では，これは「情報セキュリティマネジメント」と呼ばれる [8] が，これからはさらに広く「情報ディペンダビリティマネジメント」と呼ぶべきかもしれない．簡単に言えば，前章までで述べた個別の課題と要素技術を念頭に置きながら，企業など組織においてシステム管理・組織管理を行うことである．

情報セキュリティマネジメントを行う主体となるのが，情報セキュリティマネジメントシステム（ISMS, Information Security Management System）であり，日本では（財）日本情報処理開発協会（JIPDEC）が ISMS 適合性評価制度により普及を推進している [9]．

ISMS の基本は，Plan（目標・計画策定），Do（対策導入・運用），Check（監視・見直し），Act（改善・処置）の PDCA をサイクルとして繰り返し，螺旋状にセキュ

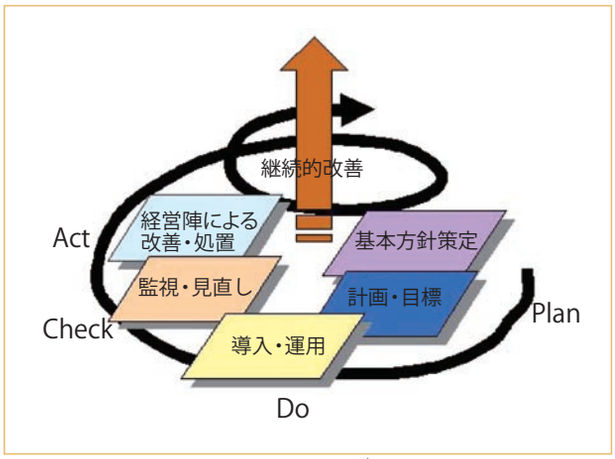

図 -3　ISMS における PDCA サイクル [9]

リティを向上させていくところにある（**図 -3**）．

標準化

ISO/IEC JTC 1 は，情報技術分野の標準化を担当する国際技術委員会であり，その下に置かれている分科会 SC 27 では，情報セキュリティ技術の標準化を進めている．SC 27 には，5 つの WG があり，それぞれ次の役割を負っている．

(1) WG 1：情報セキュリティマネジメントシステム
(2) WG 2：暗号とセキュリティメカニズム
(3) WG 3：セキュリティ評価技術
(4) WG 4：セキュリティコントロールとサービス
(5) WG 5：アイデンティティ管理とプライバシー技術

前章で述べた ISMS にかかわる国際規格は，WG 1 で議論され，ISO27000 シリーズとして体系化がはかられている．本会では，情報規格調査会が SC 27 に対応した活動を積極的に行っている．詳細な活動内容については，文献 10）などを参照していただきたい．

教育と教養

初等中等教育において「情報」を的確に教えることの大切さは言うまでもない．「情報」が高校教育で必修となったのは当然のことである．一方で，ディペンダビリティに関する教育として，「ウィルス対策ソフトウェアを導入せよ」というだけでは，情報システムのブラックボックス化が進むことになり，安心・安全な情報社会のためには不十分だろう．コンピュータやインターネットでやっていいことと悪いことを体系的・具体的に教える必要があり，そのための人材を育成することが急務となっている．

ディペンダビリティの基本は，社会を構成する人間の信頼性・安全性である．そこには法律や制度の問題もあるが，モラルや人間理解の問題も大きいだろう．文献 4）で述べたように，昨今，大学においても教養水準の低下が目に見えるようになっており，これがモラルや人間理解にマイナスになることが懸念される．

未来へ

セキュリティを含む統合概念としてのディペンダビリティは，情報システムを構築し，維持し，発展させる上で最も重要なものの 1 つであり，要素技術の開発，ISMS の策定と運用，標準化，教育の充実などが情報処理に携わる我々のミッションとなっている．

社会情報インフラは，単独で成り立つものではなく，電力網，通信網，交通網，金融網，行政サービスなどと協力して我々の生活を支えているものであるから，これらの社会インフラとの連携が必須である．さらに，弁護士会や保険会社，社会心理学者などとの協力も大切になってきているだろう．

「政府・学協会などの取り組み」の章で述べたように，ディペンダビリティを扱う公的機関が分散しており，情報の流通や総合的対策の策定などに支障をきたす可能性がある．NISC などを核として，安全・安心の中心となる政府機関の設立が急務である．

産業界にとっては，ディペンダビリティのためのコストをどこまで払えるかが課題となる．適正なコストをかけるためには，品質に対する価格設定が有効になる仕組みが必要である．従来，これはブランド力など漠然とした言葉で語られることが多かったが，権威ある認定機構によって情報システムのディペンダビリティをランクづけし，その結果を広くユーザの目に触れるようにするべきだろう．ランクづけの対象は，マイクロプロセッサ，ルータ，オペレーティングシステム，アプリケーションソフトウェアなどの個々の要素であり，また ISMS を含む統合システムとなるだろう．

今の社会では環境ビジネスが急速に発展しつつあるが，情報ディペンダビリティについても優れたビジネスモデルが望まれる．その際，セキュリティソフトウェアのベンダだけでなく，ハードウェアとソフトウェアの一次的な開発者に利益が還元されることが必要であろう．

教育・教養は大きな問題である．単なる押しつけの道徳教育ではなく，自立した社会人としての自覚を促すような教育が望ましいのは，情報処理の分野でも当てはまる．特に，我々には WWW というネットワーク DB 型の知識コミュニティを作った責任がある．今ある情報インフラをどう使い，新しい情報インフラをどう作り上

げていくか，さらには人類の持つ知識そのものについてこれをどう使いどう増やしていくか，文科系の専門家とともにイニシアティブをとって考えていくことが必要になっている．

謝辞　本稿執筆にあたり，学術会議拡大情報委員会セキュリティ・ディペンダビリティ分科会のメンバ各位，科学技術振興機構（JST）CREST 研究領域「情報社会を支える新しい高性能情報処理技術」「ディペンダブル VLSI システムの基盤技術」，文部科学省「先導的 IT スペシャリスト育成推進プログラム」および半導体理工学研究センター（STARC），ならびに東京大学の五島正裕准教授，入江英嗣助教には，大変お世話になりました．お礼申し上げます．

参考文献

1）苗村憲司：SC 27 における情報セキュリティ標準化の動向，http://www.itscj.ipsj.or.jp/forum/naemura.pdf (2001).
2）IFIP WG10.4 Dependable Computing and Fault Tolerance, http://www.dependability.org/wg10.4/
3）Avizienis, A., Laprie, J-C., Randell, B. and Land, C. : Secure Computing, IEEE Trans. on Dependable and Secure Computing, Vol.1, No.1, pp.11-33 (2004).
4）坂井修一：ディペンダブル情報社会へ，情報処理，Vol.48, No.7, pp.783-785 (July 2007).
5）米田友洋，土屋達弘，梶原誠司：ディペンダブルシステム —高信頼システム実現のための耐故障・検証・テスト技術（単行本），共立出版 (2005).
6）情報処理推進機構，2005 年企業における情報セキュリティ事象被害額調査，http://www.ipa.go.jp/security/fy17/reports/virus-survey/documents/2005_model.pdf (Nov. 2006).
7）入江英嗣，荻野　健，勝沼　聡，清水一人，栗田弘之，五島正裕，坂井修一：超ディペンダブル・プロセッサアーキテクチャの構想，電子情報通信学会技術研究報告 CPSY, Vol.106, No.3, pp.49-54 (Apr. 2006).
8）情報処理振興事業協会（現情報処理推進機構）セキュリティセンター，情報セキュリティ・マネジメント概論，http://www.ipa.go.jp/security/awareness/manage- ment/management.pdf (2001).
9）日本情報処理開発協会（JIPDEC），情報セキュリティマネジメントシステム (ISMS) とは，http:// www.isms.jipdec.jp/isms/ (2006).
10）寶木和夫，SC 27（IT Security Techniques ／セキュリティ技術）総会報告，http://www.itscj.ipsj.or.jp/report/27_200705.html (2007).

（平成 20 年 2 月 15 日受付）

坂井修一（正会員）
sakai@mtl.t.u-tokyo.ac.jp

1981 年東京大学卒業．1986 年同大学院修了．工学博士．電総研，MIT，筑波大学などを経て，現在，東京大学大学院情報理工学系研究科教授．専門はコンピュータシステムとその応用．現在はディペンダブル情報基盤に最も関心がある．日本 IBM 科学賞（1991），市村学術賞（1995），IEEE Outstanding Paper Award（1995）など受賞．本会では，研究賞（1989），論文賞（1991），論文誌編集委員（1998 ～ 2002），学会誌編集委員（2003 ～ 2007），卓越 DB 小委員会主査（2006 ～），理事（2006 ～）など．その他，日本学術会議連携会員，電子情報通信学会コンピュータシステム専門委員会副委員長，日本学術振興会学術専門委員など．電子情報通信学会，人工知能学会，IEEE，ACM 各会員．