提　　言

安全・安心を実現する情報社会基盤の普及に向けて

平成２０年（２００８年）６月２６日

日　本　学　術　会　議
情報学委員会
セキュリティ・ディペンダビリティ分科会

本提言は、日本学術会議情報学委員会セキュリティ・ディペンダビリティ分科会における審議結果をとりまとめ公表するものである。

日本学術会議情報学委員会セキュリティ・ディペンダビリティ分科会

委員長	今井　秀樹	（第三部会員）	中央大学理工学部 教授
副委員長	田中　英彦	（第三部会員）	情報セキュリティ大学院大学情報セキュリティ研究科研究科長、教授
幹事	坂井　修一	（連携会員）	東京大学大学院情報理工学系研究科教授
幹事	宮地　充子	（連携会員）	北陸先端科学技術大学院大学附属図書館長・教授
	井上　克郎	（連携会員）	大阪大学大学院情報科学研究科 教授
	岩野　和生	（連携会員）	日本ｱｲ･ﾋﾞｰ･ｴﾑ株式会社 執行役員/大和ｿﾌﾄｳｪｱ開発研究所 所長
	片山　卓也	（連携会員）	北陸先端科学技術大学院大学教授
	佐々木良一	（連携会員）	東京電機大学教授
	管村　昇	（連携会員）	工学院大学教授
	南谷　崇	（連携会員）	東京大学先端科学技術研究センター教授
	西関　隆夫	（連携会員）	東北大学情報科学研究科副研究科長・教授
	林　　弘	（連携会員）	㈱富士通研究所常務取締役
	深澤　良彰	（連携会員）	早稲田大学理工学術院教授
	松田　晃一	（連携会員）	独立行政法人情報処理推進機構（IPA） IT人材育成本部長
	松本　勉	（連携会員）	横浜国立大学大学院環境情報研究院教授
	安浦　寛人	（連携会員）	九州大学大学院システム情報科学研究院教授
	米崎　直樹	（連携会員）	東京工業大学教授

要　旨

１　作成の背景

情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、及び物流のいわゆる重要インフラ（以下、社会基盤という。）は、コンピュータシステムやインターネットなどのいわゆる情報インフラ（以下、情報社会基盤という。）の普及とともに大きな変化を遂げている。これまで独立に存在したこれらの社会基盤は、情報社会基盤を介して互いに関与し、今後ますます密かつ複雑に相互に関係するであろう。また、情報社会基盤の普及は、各種業務の効率化とともに、人を介したビジネスからインターネットを介した電子ビジネスという新しい商取引を生み出し、電話や手紙に代表される１対１のコミュニケーションから電子メールやブログなどの１対不特定多数のコミュニケーションを可能にするなど、我々の生活基盤そのものを急激かつ大きく変容させた。

情報社会基盤の普及は我々の経済活動の効率を大幅に改良したが、逆にこれまでの社会基盤では起こりえなかった事故が起こるようになった。例えば、金融機関の巨額な損失事件や後を絶たない個人情報流出事件、さらに情報社会基盤を利用したサイバー犯罪の増加等である。しかも、現在、世界は情報社会基盤で繋がり、一国のサイバー犯罪が他国に与える影響は無視できない。このような状況を受けて、安全・安心を実現する情報社会基盤に対する国家的な取組みが米国をはじめとし、シンガポール、韓国などのアジア各国でも進められている。我が国においても、もはやその取組みの遅れは許されない状況にある。

情報社会基盤の安全・安心を実現する研究分野が「セキュリティ」と「ディペンダビリティ」である。セキュリティは、広義には、危険な状態から人の生命・財産等を守り安全を保つ、また社会の秩序を守ることを意味し、警備もセキュリティの範疇になるが、本提言では、セキュリティは情報セキュリティを意味し、情報と情報システムの安全・安心が目的となる。ディペンダビリティも同様の目的を持つが，セキュリティが主として意図的な攻撃への対処であるのに対し，ディペンダビリティは主として偶発的な故障や人の過誤などへの対処である点が異なり、この二つの分野はほとんど独立に研究されてきた。

そこで、日本学術会議情報学委員会セキュリティ・ディペンダビリティ分科会では、「セキュリティ」分野と「ディペンダビリティ」分野の代表的な研究者を集結し、 情報社会基盤の安全・安心実現に向けて検討を行い、行政、学協会、企業が行うべき方策案を提言としてまとめた。

２　現状及び問題点

法律・倫理及び教育など我々の社会生活の規範となる土台は、情報社会基盤の急激な普及に伴う社会変化に追い付けない現状にある。また、情報社会基盤に関する事故及び重大インシデントの原因を科学的に究明する組織化された

独立の常設調査機関が存在せず、再発防止のための枠組みも確立されていない。さらに、情報社会基盤に関与する行政、研究、国内・国際標準化機関などが独立に機能し、方向性や成果の適用先などを決定する一元的な機関が存在しないことは、情報社会基盤がもたらす急激な社会変化に対する国家的な取組みの遅れにも繋がる。一方、学術面では、情報と情報システムの安全・安心を実現する研究分野であるセキュリティとディペンダビリティは独立に研究されてきたが、両者を融合することで初めて解決される問題も多く、二つの研究分野の協力が求められる。

3　提言

上記の背景及び問題を鑑みて、緊急に対処を要する情報社会基盤の重要案件及びその情報社会基盤の重要案件等を取り扱う一元的な機関の設立に向けて、以下のような提言を行う。

(1) 緊急に対処を要する重要案件

早急に検討が必要な重要案件は、以下の 4 件である。

① 情報社会基盤に関する法制度及び資格認定制度の整備
② 安全で安心な情報社会基盤の管理・運用体制の整備
③ 情報学に関する教育制度の構築
④ 情報システムの脆弱性に関わる事故調査委員会の設置

(2) 情報社会基盤の問題を取り扱う一元的な機関の設立に関して

前項の重要案件への対処にも、今後の安全・安心な情報社会基盤の普及のためにも情報社会基盤に関わる課題を一元的に扱う機関が必要と考えられる。情報社会基盤に関わる問題は、技術の問題、管理の問題、法律の問題、倫理の問題と複数の専門領域にまたがっている。そこで、情報社会基盤に関わる問題に対処するために、これらの各専門家及び利用者となる団体の代表者を含む「安全・安心を実現する情報社会基盤政策機関（仮称)」[1)]の設立に向けての検討を開始するべきである。

この機関の設立にむけて、行政、企業、学協会、公的機関それぞれの協力を求める。

4　今後の日本学術会議情報学委員会セキュリティ・ディペンダビリティ分科会の対応

日本学術会議情報学委員会セキュリティ・ディペンダビリティ分科会は、関連分科会と連携し情報社会基盤政策機関の設立の体制を整備するよう努める。

[1)] 以下、情報社会基盤政策機関という。

目　次

はじめに

情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、及び物流など我が国の国民生活または社会経済活動に多大な影響を及ぼすいわゆる重要インフラ（以下社会基盤という。）は、コンピュータシステムやインターネットなどのいわゆる情報インフラ（以下情報社会基盤という。）の普及とともに、密接かつ複雑に相互に関与するようになった。いまや情報社会基盤は、我が国の社会的経済基盤及び社会的生産基盤の効率化を進めるだけでなく、電子商取引などの新しい産業形態や e-tax などの電子行政の進展など、生活基盤そのものを急激かつ大幅に変容させ、我々の生活に必要不可欠なものとして定着しつつある。

しかし、法律・倫理及び教育など社会生活の規範が十分対応できない状況で、情報社会基盤が急激に普及したため、これまでの社会基盤では起こりえなかった事故が起こるようになった。このような情報社会基盤が引き起こす事故の特徴は、異なる複数の社会基盤が接続していることから、一つの機関の事故が他の機関へ波及する可能性があること、そして、その汎用的な普及性から全国民が被害者あるいは逆に加害者になる可能性があることである。

情報社会基盤は重要かつ汎用性の高い社会基盤であるため、我が国においては、関与する行政機関、研究機関、標準化機関が複数設立され、それぞれ独立に最先端の研究や国際・国内標準化の成果を挙げてきた。しかし、今後、情報社会基盤がもたらす急激な社会変化に対する国家的な取組みを早急に決定し、それを実行に移すためには、これら全機関の方向性、成果の適用先などを決定する一元的な機関が必要と考えられる。

そこで、日本学術会議情報学委員会セキュリティ・ディペンダビリティ分科会では、情報社会基盤の安全・安心を実現する２つの研究分野である、「セキュリティ」分野と「ディペンダビリティ」分野の代表的な研究者を集結し、 情報社会基盤の安全・安心の実現に向けて検討を行った。本提言は、我が国における情報社会基盤の現状の問題点を踏まえ、今後、行政、学協会、企業が行うべき方策案について提案するものである。

本提言の構成は下記の通りである。第１章で提言の背景について述べ、第２章でセキュリティとディペンダビリティについて解説する。第３章、第４章では提言の背景となった具体的な情報社会基盤の脆弱性の影響度を示す事例及び我が国のセキュリティ・ディペンダビリティの現状について解説する。その後、第５章では現状及び問題点についてまとめて、第６章で本提言について述べる。第７章では具体的な政策機関案に関して述べ、最後にむすびでまとめる。

１　提言の背景

情報社会基盤の普及は、ワープロや表計算など個人の情報処理の効率化・高速化とともに、これまでの人を介したビジネスからインターネットを介した電子ビジネスという新しい商取引を生み出し、電話や手紙に代表される１対１のコミュニケーションから電子メールやブログなどの１対不特定多数のコミュニケーションを可能にするなど、生活基盤そのものを急激にかつ大幅に変容させた。この情報社会基盤の普及は我々の経済活動の効率を大きく改良したが、逆にこれまでの社会基盤では起こりえなかった事故が起こるようになった。

例えば、金融機関の巨額損失事件は、金融システムの信頼性が情報社会基盤の信頼性に大きく依存することを露呈した事件といえる。また、後を絶たない個人情報流出事件は、ユーザデータの取り扱いが必須であるガス、電力、上下水道などの社会基盤の信頼性も情報社会基盤の安全性を抜きに議論できないことを示唆する。このように、現在では、異なる複数の社会基盤がネットワークで接続しているため、一つの事故の他の機関への波及効果を無視することはできない。実際に１億個以上の素子からなる半導体チップの中の１つの設計ミスや動作不良が、社会基盤全体を麻痺させる事故につながることもある（３(1)参照）。

また、情報社会基盤が実現した１対不特定多数のコミュニケーションの一例であるウェブサイトでは、一般ユーザが巻き込まれる不正行為や犯罪が多発している。例えば、ウェブサイトを利用したいじめやウェブサイトの脆弱性を利用した犯罪などはその一例である。一方、ファイル交換ソフトである Winny を介したファイル流出事件も一般ユーザが引き起こす不正の典型である。このような情報社会基盤を利用した犯罪（サイバー犯罪）や不正行為の増加は、重要な社会問題であり、情報社会基盤が全国民に普及している現在、全国民がその不適切な利用に伴う被害者あるいは逆に加害者になる可能性があることを意味する（３(2)参照）。

しかし、法律・倫理及び教育など我々の社会生活の規範となる土台は、情報社会基盤の急激な普及に伴う社会変化に追い付けない現状にある。実際、高度情報通信ネットワーク社会形成基本法（IT 基本法）が平成 13 年に施行され、高度情報通信ネットワーク社会の形成に関する施策を迅速かつ重点的に推進することが決まったが、細部の法律整備は未だ進行中の状態である（４(1)参照）。

一方、初等教育から高等教育の現場では、情報通信倫理やセキュリティなどを含む情報学に関する一貫教育が行われていない。つまり、情報社会基盤が全国民に普及しているにも拘らず、それに関する必要不可欠な正しい知識を全国民に教育する機会がない。この結果、国民一人一人が情報システムの脆弱性の温床になり、サイバー犯罪増加の人的要因にもなりかねない状況にある（４(5)参照）。

また、航空、鉄道に関しては、事故及び重大インシデントの原因を科学的に究明し、公正・中立の立場から事故の防止に寄与するための独立した常設機関として航空・鉄道事故調査委員会が存在するのに対し、情報社会基盤に対しては、組織化された独立の常設調査機関に対応するような社会的枠組みが確立されていない。独立行政法人情報処理推進機構(IPA)[2)]ではソフトウェア製品およびウェブアプリケーションの脆弱性に関する情報の届出を受け付けているが、事故や重大インシデントの実態を独自に現場調査し報告するための仕組みを持ってはいない（４(2)参照）。

その一方で、情報社会基盤に関与する行政機関、研究機関、標準化機関などは複数存在し、それぞれ着実に成果を挙げている。しかしながら、これら全機関の方向性、成果の適用先などを決定する一元的な機関が存在しないことが、結果的に上述のような、情報社会基盤がもたらす急激な社会変化に対する国家的な取組みの遅れの原因にもなっている（７(4)、４(3)、４(4)参照）。

情報社会基盤の安全・安心を実現する研究分野が「セキュリティ」と「ディペンダビリティ」である。セキュリティとディペンダビリティの研究は、ともに、現代の多様な環境のもとで、人の生活と社会の活動が安心して依存できるような良質で信頼できるサービスを提供する情報システムを構築することを目標とするが、これまでセキュリティとディペンタビリティの研究は分離して行われてきた。しかし、真に安全・安心な社会の実現には両者を融合した技術体系が必要であるという考えから、両者の融合が進められている（第２章参照)。

また、安全・安心を実現する情報社会基盤の国家的な取組みはすでに米国ではじめられており（文献[12])、シンガポールや韓国などのアジア各国でもその動きが見られる。現在、世界は情報社会基盤で繋がっており、一国のサイバー犯罪が他国に与える影響を無視できない。この観点からも、安全・安心の実現に向けた我が国の取組みが遅れることは許されない状況にある。情報社会基盤に係る整備の遅れに関しては、社団法人日本経済団体連合会からも指摘されている（文献[17])。

[2)] 以下、IPA と略称する。

２　セキュリティとディペンダビリティ

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」（文献[９]）と定義され、情報の可用性、守秘性、完全性の維持がその主要な要件とされる[1]。一方、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」（文献[10]）と定義され、信頼性、安全性、保守性などの維持が主要な要件とされる。共に情報と情報システムの安全・安心を目的としているが、セキュリティが意図的な攻撃を主な対象としてきたのに対し、ディペンダビリティでは意図的ではない過誤や偶発的な故障などを主な対象としてきたという点で異なっていた。しかし、近年、セキュリティ、ディペンダビリティの両分野とも、その対象を広げつつあり、両分野統合の試みがなされている。そのような試みの一つとして、ニュー・ディペンダビリティという言葉が提唱されている（文献[６]）。

従来、セキュリティとディペンダビリティは安全を主目的としたが、近年では安心、つまり人が安心して情報や情報システムを利用できることも重要な目的になった。このためには、安全性が確保されていることはもちろんであるが、さらにその安全性を明確に理解できるようにすることも重要である。逆に、実際には安全でないシステムを安全だと考え安心して使うようなことがあってはならない。このような観点から、セキュリティやディペンダビリティの分野では人の問題を様々な観点から扱うようになってきた。例えば、安心を重要な評価軸の一つとするヒューマンクリプトが一つの研究分野を形成しているし、ニュー・ディペンダビリティにおいては、安全と安心の実現のために認知科学と心理学との連携が重要とされている。このため、本提言では安全と安心を一括し、安全・安心として論じる。

[1]セキュリティに関する詳細な用語解説は、文献[７、８、11]を参照されたい。

３　情報社会基盤の脆弱性の影響

本章では情報社会基盤の脆弱性が引き起こす国民生活への影響度を示す事例について記述する。

(1) 情報社会基盤に関する事故事例

情報社会基盤は、現在では主要なライフラインの一部をなすものであり、そのセキュリティ、ディペンダビリティが一部でも失われると、生産者・利用者の双方に深刻な悪影響を及ぼし、さらに社会全体に情報社会基盤そのものへの信頼性を失わせ、生活の安心感をも損なうことになる。以下、これまでに起こった実例によってこれを示す。

①　プログラムの不具合による国民生活への影響

平成 19 年 10 月、Suica と PASMO に対応した 16 事業者 662 駅で、自動改札機 4378 台（PASMO 470 駅 3050 台、Suica192 駅 1328 台）がプログラムの不具合により起動しないという問題が発生した。通常は駅構内のサーバから集中的に自動改札機を起動する仕組みだが、これが不可能になった。各駅はサーバから改札機を切り離し、単体起動に切り替えるなどの対応を行ったが、PASMO で約 160 万人、Suica で約 100 万人の客に影響が出たと報告されている。

自動改札機システムは、Suica、PASMO だけでなく ICOCA、PiTaPa、SUGOCA 等複数システムが存在し、その全利用者数は今後ますます増加すると考えられる。今後、相互乗り入れ等の進展とともにシステムはますます複雑化することが予想され、同種のシステム事故が発生しないように対応する必要がある。

②　マイクロプロセッサの設計ミス

情報システムの基盤となるマイクロプロセッサは、現在、数億個以上の素子で作られる複雑なシステムであり、その複雑さは年を追って増していることから、設計の正当性検証が次第に困難になってきている。平成６年、Intel 社のマイクロプロセッサ Pentium の浮動小数点除算回路に設計ミスが発見された。同社によるとこの設計ミスの影響は限られたものであり、27,000 年に一度の障害しか起こさないとのことであったが、ユーザの同社への信用失墜は顕著なものがあり、該当する全商品のリコールを余儀なくされた。このことによる同社の損失は、4 億 7500 万ドルであったと報告されている。

③　ソフトウェアの脆弱性

Microsoft Windows のような巨大なソフトウェアを脆弱性やバグなしに作ることは現実的には不可能であるといってよい。この脆弱性をついて、ウイルス、ワーム、トロイの木馬、ボットなどの攻撃が、特に今世紀に入ってから頻繁に行われるようになった。ソフトウェアの利用契約によって、Microsoft 社などのソフトウェアベンダが損害賠償することは免れているが、ソフトウェアの利用者である企業や官公庁、一般ユーザの損害は甚大であり、その額は平成 17 年の場合 1 社あたり平均約 1.3 億円と報告されている（文献[13]）。

④　巨大システムの障害

情報社会基盤に関して近年もっとも大きな事件であった東京証券取引所のシステム障害は、多くが負荷の集中による不安定化によって起こされており、ライブドア・ショックによる売り注文の殺到による取引全面停止(平成 18 年 1 月 18 日)などはその顕著な例であった。一日あたり 100 万件超の取引を行うこともあり、システムダウンで一般ユーザがこうむる損失の総額も莫大なものとなっている。一方で、証券会社によるジェイコム株大量誤発注事件（平成 17 年 12 月 8 日）のような単純な操作ミスによって巨額の損失を出した事件もあった。ジェイコム株の事件は、61 万円 1 株の売り注文を 1 円 61 万株と誤入力したことから起こったものであり、操作ミスを行った証券会社はもとより、発注取消を行うことができなかった東証も責任が問われている（証券会社側から東証に対して 414 億円の損害賠償を求める訴訟が起こされ、現在係争中である)。システム製作を行ったベンダでは、これ以後、ソフトウェア開発の信頼性・安全性を飛躍的に高めるために、カスタマとの役割分担の明確化や仕様書作成の明確化、開発チーム以外のエキスパートの検査などを義務づけるようにしている。東証側も、これに応じるように責任範囲を明確化し、今後のシステムでは外部仕様などは自社で作成することなどを決定している。

また、航空会社におけるシステム障害(平成 19 年)では、通信スイッチの物理的故障とゲートウェアプログラムのバグによるシステムダウンにより、130 便が欠航、306 便が遅延する事態となり、約 79,000 人に影響が及んだ。同様の障害は、省庁や地方公共団体、銀行、電力・ガス会社など社会基盤のあらゆるところで起こる可能性がある。

⑤　サイバーアタック

③で述べた脆弱性をついた不正侵入やデータの窃取を、特定サイトに対して大規模に起こすのがサイバーアタックと呼ばれる攻撃である。官公庁や企業のホームページの改竄などが主な例であるが、平成 19 年 4 月にエス

トニアの政府や銀行の Web サイトへの大規模な DDoS 攻撃(分散サービス拒否攻撃）に代表されるように、政府・銀行など国家の中枢機能を同時に麻痺させるような集中攻撃も起こっており、先進各国ではサイバーアタックに対する抜本的な対策をたてることが急務となっている。

(2) 情報社会基盤の不適切な利用事例

情報社会基盤は、１対不特定多数のコミュニケーションという新しいコミュニケーションの手段を提供するとともに、誰でもいつでもどこでも利用できる簡易性は、急激な利用者数の増加をもたらした。しかし、法制度及び教育が不十分なままでの急激な利用者の増加にともない、全国民がその不適切な利用に伴う被害者あるいは逆に加害者となる事件が頻繁に起こっている。以下､警察庁によりまとめられた平成 19 年度前期の情報社会基盤を利用した犯罪状況を用いてこれを示す。

サイバー犯罪とは、情報社会基盤を利用する犯罪である。大きく、パスワード不正アクセス禁止法違反、コンピュータ・電磁的記録対象犯罪、ネットワーク利用犯罪に分けられる｡平成 19 年上半期のサイバー犯罪の検挙状況等については､文献[1]に警察庁がまとめたデータが記載されている｡警視庁の報告資料によると､平成 19 年度上半期のサイバー犯罪の検挙数は 1,808 件であり、平成 18 年の上半期とほぼ同数のようである。平成 19 年度の検挙内容の特徴としては､児童買春事犯及び青少年保護育成条例違反が平成 18 年同期に比べて 61.1％の増加､著作権法違反が平成 18 年同期に比べて 176.1％ほど増加していることが挙げられる。

児童および青少年が関わる事件では、青少年が被害者になった事件だけでなく、青少年が誹謗中傷を自分のブログサイトにあげるなどの名誉毀損、オンラインゲームの他人の ID やパスワードを入手し､不正アクセスを行うなど加害者になった事件も数多く報告されている。このような青少年が関与するサイバー犯罪の増加は、青少年が情報社会基盤を利用する機会が増えたにも拘らず、その正しい利用方法を教育されていないことも一因と考えられる。

一方、著作権法違反に関連して、海賊版 DVD の販売や、違法複製物をインターネット上に公衆送信する等の犯罪が問題になっている。例えば、平成 19 年５月までに､携帯電話用のウェブサイトを利用して約 25,600 点の映画やテレビ番組の海賊版 DVD を販売していた衣料品販売業者らによる著作権法違反（頒布）や、平成 19 年５月、インターネット上のレンタル掲示板に 1,000 曲以上の「着うた」用ボーカル入り楽曲ファイルを蔵置し、不特定多数に配信していた会社員による著作権法違反（公衆送信権の侵害）等の事件が報告されている。詳細は文献[15,16]を参照されたい。また、Winny を介した情報漏えいも大きな社会問題となっている。例えば、平成 19 年 6 月に警視庁の捜査資料 1 万件がインターネットに流出した事件も Winny を介した情報漏えい

であった。 このような情報漏洩の危険性は平成 16 年に指摘されているにも拘らず、毎月約 1,600 件、年間で約 20,000 件の情報漏洩が Winny を介して起こっており、その 95%が自宅で起こっている、つまり一般ユーザによる事故であるのが現状である。詳細は文献［２］を参照されたい。 このような著作権法違反や情報漏洩事件の増加も、広く国民が情報社会基盤を利用するようになったにも拘らず、情報社会基盤の正しい利用方法を教育されていないことが大きな原因になっていると考えられる。

4　我が国のセキュリティ･ディペンダビリティの現状

(1) 情報社会基盤と法整備及び資格認定制度

第１章で述べたように、情報社会基盤が関与する事故は、不特定多数の国民が被害者あるいは加害者となる危険性をもち､非常に深刻である｡しかし、現在の法整備状況では、サイバー犯罪の加害者を法律で適切に罰することは必ずしも容易ではない。

一つの事例として､平成 18 年９月８日に起こった某社の情報漏洩事件が挙げられる。本事件は、従業員が会社から持ち出した顧客情報を知人に渡し、さらに知人はその顧客情報を第三者に渡し、その第三者が顧客情報を用いて某社に金銭を要求した事件である。本事件では、金銭を要求した第三者が恐喝未遂容疑で逮捕されたが、最初に情報を持ち出した従業員の不正行為に対して、刑法の処罰を問うことができなかった。これは現在の法整備で規定されている著作物が、現実の情報社会基盤の中での利用、あるいは流通形態に則していないことが原因である。これらに関する具体的な事例に関しては、文献[３]を参照されたい。

このように、サイバー犯罪では、著作物などの対象が既存の社会基盤で規定されていた範疇と異なるだけでなく、多岐にわたるため、現在の法律の下では被害者を保護し、加害者を適切に罰することが難しいのが現状である。

また、情報社会基盤の技術は非常に重要であるにも拘らず、構築あるいは管理・運用する技術者のレベルを法的に保証する資格認定制度が整備されていない。情報社会基盤のセキュリティに関する資格としては、国際情報システムセキュリティ認証コンソーシアムが認定する情報システムセキュリティプロフェッショナル(CISSP)、情報システムコントロール協会（ISACA)が認定する情報セキュリティマネージャー(CISM)、情報システムコントロール協会が認定する情報システム監査人(CISA)、NISM 推進協議会が認定するネットワーク情報セキュリティマネージャー(NISM)、日本セキュリティ監査協会(JASA)が認定する情報セキュリティ監査人などがある。しかしながら、どの資格も実際に情報社会基盤を構築あるいは管理・運用する技術者の免許制度とはなっていないため、現状では、情報社会基盤技術やその管理・運用を客観的に評価・保証することができないのが現状である。

(2) 情報社会基盤のバグや脆弱性の現在の報告制度

情報社会基盤は、主にコンピュータとインターネットから成る。システムの個々の構成要素も複雑であるが、これらが合体した複合システムの構成はさらに複雑であり、しかも日々に更新、新規参入、統廃合などを繰り返す動的なシステムである。

個々の構成要素については、メーカやベンダによるバグレポートやリコー

ル、Microsoft Update に代表されるようなインターネットを介した自動更新などによる脆弱性やバグの修正などが行われている。一方で、社会基盤の公共性を考えれば、こうした報告・修正はメーカやベンダや一部のユーザなど一次的な当事者だけでなく、公共の場で第三者にまんべんなく周知されるようにしなければならない。また、個々のバグや脆弱性に対するメーカやベンダの対応はその都度公正に評価されなければならないし、脆弱性の発見者や研究者は適切に保護されなければならない。

このようなことを行う機関として、IPAセキュリティセンター（http://www.ipa.go.jp/security/）がある。同センターでは、ウイルス及び不正アクセスの被害状況の把握と対策情報の発信、情報システムの脆弱性対策、暗号技術調査・評価、システムのセキュリティ評価・認証、セキュリティを高めるための技術開発・調査研究などを行っている。

同センターでは、平成16年以後、ソフトウェア製品およびウェブアプリケーションの脆弱性に関する（電子メールやWWW経由などによる）情報の届出を受け付けている。発見された脆弱性については、製品開発者の対応状況、対策情報をポータルサイトJVN(http://jvn.jp/)で公開している。同事業は 有限責任中間法人JPCERT コーディネーションセンター(JPCERT/CC)[3)]と共同で運営され、脆弱性の概要や対策情報からなる脆弱性対策情報データベースJVN iPedia (http://jvndb.jvn.jp)も公開している。同センターは、その他にも、情報セキュリティに関する意識の啓発、脅威に対する具体的な対策方法と情報の提供、安全で快適な電子政府・電子自治体の実現に向けた支援活動などを行っている。

しかし、脆弱性などの届出は義務付けられておらず、法的根拠なども定められていない。このため、本格運用にはさらなる整備が必要である。今後は、航空・鉄道事故調査委員会のような積極的・能動的な調査公開制度によるバグおよび脆弱性の報告・処置と今後の対策の策定が総合的に行える機関の設立が必要であろう。

なお、事故調査委員会の設置に関しては、JST の社会技術研究開発センターからも設置に向けた状況調査に関する報告及び情報システム事故調査委員会設置への提言がある（文献[４]）。また事故の公表に関しては、JST が提供している「失敗知識データベース」等も参考にするべきである（文献[５]）。

(3) 内閣官房情報セキュリティセンター

平成17年４月、情報セキュリティ対策の中核組織の必要性を重視した政府は、我が国における情報セキュリティ政策の基本戦略を決定する「情報セキュリティ政策会議」と、その遂行機関である「内閣官房情報セキュリティセンタ

3) 以下、JPCERT/CC と略称する。

ー(NISC)」とを設置した（http://www.nisc.go.jp)。内閣官房情報セキュリティセンターは質的に優れた活動を維持しているが、セキュリティ・ディペンダビリティを取り扱う唯一の機関でないため、対象分野の大きさや流動性に対し組織として十分な大きさと予算および権限を持っているとは言い難い。今後、各省庁に独立に存在するセキュリティ関連の機関との連携・統合、あるいはセキュリティとディペンダビリティの統合的な運用等を検討する必要がある。

(4) 情報社会基盤に関与する機関

現在、情報社会基盤を取り扱う行政及び公的機関としては、４(3) で述べた情報セキュリティ政策会議や内閣官房情報セキュリティセンターに加えて、情報社会基盤の運用・利用に関する案件を取り扱うIPA、電子政府推奨暗号を選定・監視する暗号技術検討会等(CRYPTREC)[4]、JPCERT/CCなどの機関や情報社会基盤の最新の情報収集や研究を行う独立行政法人情報通信研究機構(NICT)、独立行政法人産業技術総合研究所(AIST)などの研究機関がある。さらに独立行政法人科学技術振興機構（JST)[5]も情報社会基盤に関する案件を取り扱うことがある。これらの機関はそれぞれ独立であり、現状では、これら全機関の方向性、成果の適用先などを決定する一元的な機関が存在しない。このため、同じような案件を独立に別の機関で検討するなどの非効率な運営もなされている。また、案件によっては、複数の機関で統合的に検討すべき場合や他機関の成果の共有など、情報社会基盤を取り扱う全機関の総合的な質及び効率の向上が重要な課題である。

(5) 情報学に関する現在の教育カリキュラム

セキュリティ・ディペンダビリティの真の実現のためには、情報教育を一貫教育として初等・中等・高等教育において教えることが必須である。現在、文部科学省は、ⅰ)小・中・高と各学校段階を通じて、各教科等や「総合的な学習の時間」においてコンピュータやインターネットの積極的な活用を図るとともに、ⅱ)中・高等学校において、情報に関する教科・内容を必修としている（文献[14])。たとえば、高等学校においては、「情報」は２単位の必修科目であり、情報活用の実践力獲得をめざす「情報Ａ」、問題解決においてコンピュータを効果的に活用するための科学的な考え方や方法の取得を目指す「情報Ｂ」、情報化の進展が社会に及ぼす影響を理解し、その上で情報社会に参加する上で望ましい態度を育成する「情報Ｃ」のどれかを取ることになっているが、現在、「情報Ａ」を教えるのが主流になっている。「情報」教育の問題点としては、受験科目でないために数学など他教科の授業に振り替えら

[4] 以下、CRYPTREC と略称する。
[5] 以下、JST と略称する。

れるなど、しばしば実質的には教えられていないことがある。教えられている場合でも、そのほとんどがノウハウやリテラシ（メール、WWW ブラウズ、ワープロ、表計算ソフトなどの使い方）に終始しており、情報機器で真に何ができるのか、やっていいことといけないことの区別をどうつけるのか、など、ユーザとして最も大切なことは教えられていないのが実情のようである。これは新科目を立ち上げるにあたっての教員の人材不足なども大きな原因であるが、「情報」を手先の技と考えがちな社会の風潮にも一因があると言わねばならない。たとえば、Winny を介した情報流出は、「暗号化して情報を共有する」というノウハウだけが広く伝わり、ネット上の「情報共有」とはそもそも何なのか、これを安全に使いこなすにはどういう注意が必要なのかが理解されていないことによって起こっている。後者に対するきちんとした認識があれば、著作権法違反や個人情報流出は激減すると考えられる。

今後は、情報社会基盤の真の「歩き方」を示すような初等・中等・高等教育が必須と考えられる。具体的には、パソコンや携帯電話などの情報機器の原理・操作法とともに、その上でやってよい事といけない事の区別、外部からの攻撃の予防法・対処法を実例とともに明確に教えることがこれにあたる。

５　現状及び問題点

第３章及び第４章で述べたように情報社会基盤が引き起こす事故が非常に重要な問題であるにも拘らず、現在の我が国は、次の深刻な問題を抱えている。

第一の問題は、情報システム社会基盤の行政に関する以下の問題である。

- 情報社会基盤に関わる事故を調査し、再発防止に向けた取組みを行う法的に確立された組織が存在しない。
- 様々なサイバー犯罪に適切に対処できる法律が十分に整備されていない。
- 情報社会基盤の脆弱性対策に関する国家的に統一されたガイドラインや国家的な取組みに関する統一的ロードマップなどの作成が難しい。

第二の問題は教育の問題である。教育の現場では情報ネットワークを用いた情報収集、レポート作成などが必須項目となっている。また、パソコンを含めた情報社会基盤の普及に伴い、自宅においてインターネットにアクセスすることが日常のこととなりつつある。しかし、小･中学校の義務教育において、情報に関わる教育はキーボードの打ち方などの技術（ノウハウ）の教育が中心であり、高校以上の高等教育においてもパソコンを利用したファイルの作成方法などの技術（ノウハウ）の教育が中心となる。これは情報学の学問としての一貫した教育体系が義務教育及び高等教育において構築されていない、つまり、情報社会基盤が全国民に普及しているにも拘らず、適切な利用法や脆弱性などの必要不可欠な正しい知識を全国民に教育する機会がないことを意味する。この結果、個人が、情報システムの脆弱性の温床になり、児童や生徒を含む全国民が被害者になる事件、あるいは逆に加害者になる事件の要因になっている。

６　提言

我が国の情報社会基盤に関して緊急に対処を要する重要案件及び情報社会基盤に関わる課題を一元的に取り扱う情報社会基盤政策機関の設立に向けての提言を行う。

(1) 緊急に対処を要する重要案件

①　情報社会基盤に関する法制度及び資格認定制度の整備

サイバー犯罪による被害者の法的保護や加害者を適切に罰する法律を整備する。また、情報社会基盤の脆弱性の発見者や研究者の保護に関する法制度を整備する。さらに、情報社会基盤を構築あるいは管理・運用する技術者に求められる知識・技術に対する資格認定制度を整備する。関連組織は内閣官房をはじめとした関係省庁等である。

②　安全で安心な情報社会基盤の管理・運用体制の整備

情報社会基盤の脆弱性等の問題に対処し管理・運用するための適切なガイドライン、ロードマップを早急に提供し、必要に応じ、指導・管理を行う体制を整備する。また、上記ガイドライン、ロードマップに基づいた情報社会基盤の運用に必要な具体的手順・モデルケースの作成や、指導・管理を行う人材の知識･技術を客観的に評価できる資格認定制度を整備する。関連組織は内閣官房情報セキュリティセンター、IPA、JPCERT/CC 等である。

③　情報学に関する教育制度の構築

情報社会基盤は、急速に全国民に普及したため、学校教育のみならず全国民に対する情報学あるいは情報社会基盤に関する教育体制を構築する必要がある。以下、小中高を対象とした情報学教育と企業及び国民を対象とした情報社会基盤に関する教育の構築に必要な事項について記載する。

ア　学校教育における情報学教育の構築

(ｱ) 小中高で一貫教育を行うための情報学の体系化を目指し、情報学の教育目標の設定及び情報学の大学受験科目への導入を視野に入れた教育カリキュラムの構築を、以下のような項目を重点にして行う。

ａ　義務教育における情報学の教育では情報倫理を必ず学ばせる。

ｂ　高等学校教育における情報学の教育では、義務教育で行った情報倫理教育に加えて、大学の情報学関連の基礎・基盤教育としての教育カリキュラムを編成する。

(ｲ) 上記(ｱ)で設定された教育体系化に沿った教育者の育成。

関連組織は、文部科学省、初等中等高等教育機関、大学である。

イ　社会人教育における情報社会基盤教育の構築

(ｱ) 情報通信倫理や情報社会基盤の原理と脆弱性などに関する公開講座の各地方自治体や企業等での定期的な実現。

(ｲ) 上記(ｱ)の企業内教育制度の促進。

関連組織は、関係省庁及び地方自治体、民間企業等である。

④　情報システムの脆弱性に関わる事故調査委員会の設置

情報システムが主原因となる事故及び重大インシデントの原因を科学的に究明し、公正・中立の立場から事故の防止に寄与する事故調査委員会を設置する。事故調査委員会の設置には、情報システムに関わる事故の原因調査を行う委員の匿名性確保や権限及び義務に関する規定の整備が必要である。また、事故調査委員会は情報システムに関わる事故の原因の調査と事故情報の管理及び適切な公表を行う機能を有する必要がある。関連組織は、内閣官房情報セキュリティセンター、IPA、JPCERT/CC、JST である。

(2) 情報社会基盤政策機関の設立

情報社会基盤に関わる課題を一元的に扱う機関の設立に向けて、行政、企業、学協会、公的機関に関しそれぞれ提言を行う。

①　行政に関して

ア　技術、管理、法律、倫理と複数の専門領域にまたがる情報社会基盤に関する問題に対処するには、これらの各専門家及び利用者となる団体の代表者により構成される情報社会基盤政策機関の設立に向けての検討を開始するべきである。

イ　上記の情報社会基盤の利用者となる団体としては、各省庁、地方自治体、企業、教育機関が挙げられる。また、最大数の利用者はこれらの団体に属さない国民となるため、その実情を把握することも重要である。

ウ　情報社会基盤は世界と繋がった重要な社会基盤であるため、その遅れが他国に与える影響は大きい。このことから、上記情報社会基盤政策機関は、予算と権限が十分に与えられる独立機関であることが望ましい。

エ　情報社会基盤政策機関の目的の一部を実現する組織として情報セキュリティ政策会議及び内閣官房情報セキュリティセンターが存在するが、

真に効果的・効率的な情報社会基盤政策機関設立に向けて、これらと関連する公的機関である IPA、CRYPTREC、産業技術総合研究所、情報通信研究機構などとの関係、機能分け、位置づけの検討を行うべきである。

② 企業に関して

ア 情報関連企業は、情報社会基盤政策機関の設立に向けての検討に対して、行政機関・学会および他の企業との連携を深めて協力することが求められる。また、情報社会基盤に関する事故が発生した際には、その報告、連絡、相談を行い、必要に応じて、情報社会基盤政策機関が執り行う議論、ロードマップ作りなどに協力することも重要である。

イ 企業は、自社の情報システムあるいは自社が提供する情報システムの各機能の脆弱性に対する責任部署（自社内あるいは外注先、納入先など）を明確にすることが求められる。

ウ 企業は、自社の提供する社会的影響度の高い情報システムに関しては、自社外の第三者機関による脆弱性有無の検証を行い、必要に応じ、その結果を情報社会基盤政策機関に報告することが求められる。

③ 学協会に関して

情報社会基盤に関連する学協会は、専門分野間の隔たりを越えて、情報を交換し、情報社会基盤政策機関の設立に向けての検討に協力することが求められる。特に、電子情報通信学会、情報処理学会、日本ソフトウェア科学会などの担当部門は横断的な研究会の開催や特集号の刊行、フォーラムの設立など、分野間の隔たりを越えた情報交換が可能になるような機会創出に向けての検討の開始が求められる。

④ 公的機関に関して

IPA、CRYPTREC 等は互いに連携し、情報社会基盤政策機関の設立に必要な情報を収集し提供する。また、産業技術総合研究所、 情報通信研究機構等は互いに連携し情報社会基盤政策機関の設立に必要な情報の提供を行う。

⑤ 今後の日本学術会議情報学委員会セキュリティ・ディペンダビリティ分科会の対応

日本学術会議情報学委員会セキュリティ･ディペンダビリティ分科会は、安心・安全・リスク検討分科会や情報学教育分科会などの関連分科会と連携し、情報社会基盤政策機関の設立の体制を整備するように努める。

7　情報社会基盤政策機関構成案

本提言の核である情報社会基盤政策機関の構成案について記述する。

(1) 構成員

情報システム事故の対象者となる地方自治体、民間企業、学校教育の代表者、及び、対策案を策定するセキュリティ技術者・研究者、ディペンダビリティ技術者・研究者、情報社会基盤技術者、弁護士、法律・倫理専門家などを含む。

(2) 組織運用

情報社会基盤政策機関は、重要な問題に特定化した部会を必要に応じて設立することで、対応策を迅速に策定できるようにする。また、定期的に、各部会は状況を情報社会基盤政策機関に報告し、情報社会基盤政策機関は、懸案事項を各部会へ相談するなどの有機的な関係を目指す。

(3) 情報社会基盤政策機関と部会の役割

①　情報社会基盤政策機関の役割

ア　情報社会基盤に関する技術・法律・管理運用などの方向性を検討・決定し、情報社会基盤に関するプロジェクト予算投入のポートフォリオなどを検討する。

イ　国民全体に対する啓発・広報活動、産学官連携の枠組み作りなどを検討する。

ウ　セキュリティとディペンダビリティに関する国際的な動向に対応する。

エ　情報社会基盤に関わる重要案件を取り扱う部会を設立する。

オ　必要に応じ、部会の検討事項として各部会に検討を指示する。

カ　各部会からの報告を受けて、長期的/包括的な政策立案を行う。

キ　重要案件に対する検討事項解決時には部会を終了（廃止）する。

②　各部会の役割

ア　情報社会基盤政策機関からの検討事項に対して、必要に応じ部会を招集し、具体策を決定する。

イ　部会の決定事項を情報社会基盤政策機関に報告する。

(4) 情報社会基盤政策機関と他の関連機関との関係

情報社会基盤政策機関と他の関連機関との関係図について記述する。現在、その役割に近い組織として情報セキュリティ政策会議と内閣官房情報セキュリティセンターがある（４(2)参照）。情報社会基盤政策機関の設立方法としては、情報セキュリティ政策会議と内閣官房情報セキュリティセンター を中核として、情報社会基盤政策機関に発展させることが一つの方法と考えられる（図１）。

内閣官房情報セキュリティセンター以外の情報社会基盤に関与する行政及び公的機関として IPA、CRYPTREC、JPCERT/CC、JST、情報通信研究機構、産業技術総合研究所などがあり、国内/国際標準化機関として情報技術分野における標準化事業の充実と強化を行う財団法人日本規格協会 情報技術標準化センターや社団法人情報処理学会・情報規格調査会・技術委員会の傘下にある ISO / IEC JTC1 / SC27 国内委員会等が存在する。これらは、それぞれ別の組織の傘下に配置されている。例えば、IPA は経済産業省の傘下、CRYPTREC と JPCERT/CC は経済産業省と総務省の傘下、内閣官房情報セキュリティセンター は内閣官房の傘下、情報通信研究機構は総務省の傘下、産業技術総合研究所は経済産業省の傘下である。このため、これら全機関の効率的な運用（取り扱う案件の重複の管理、複数機関による共同体制の組織化や、各機関の情報共有など）を行う一元的な機関が存在しなかった。

情報社会基盤政策機関の目的は、これら異なる組織を有機的に結合することで、情報社会基盤に対する国家的な取組みの負荷を最小限に抑えるとともに、安全・安心の実現に不可欠な情報社会基盤政策をいち早く実行に移すことである。情報社会基盤政策機関の設立により、情報システムがもたらす急激な社会変化に対する国家的な取組みを現在よりも低コストでかつ早急に決定することが可能になると考えられる。

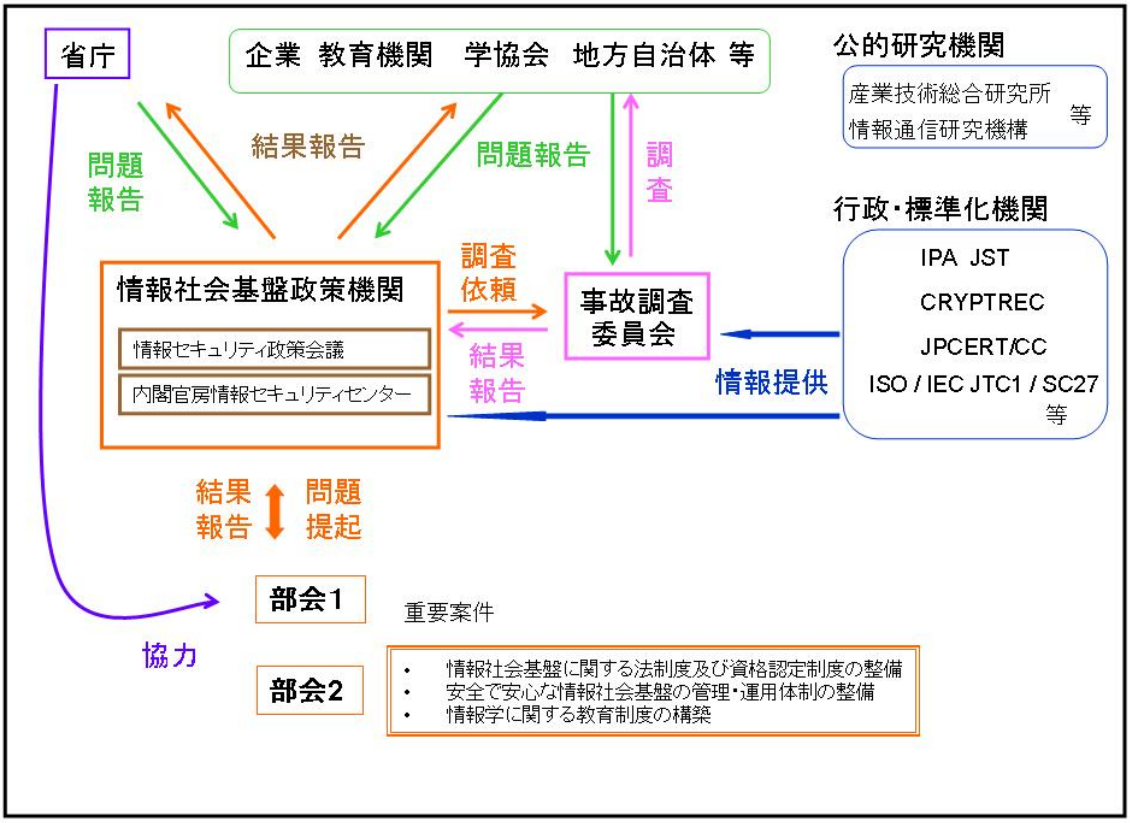

図１ 情報社会基盤政策機関の組織図

むすび

本提言では、情報社会基盤の観点から、情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、物流などの社会基盤を国民が安心・信頼して利用するための課題解決に向けて、緊急に対処を要する情報社会基盤に関わる法制度・管理運用体制・教育の整備および事故調査委員会の設置の提言、および情報社会基盤政策機関の設立に向けて行政、企業、学協会、公的機関に関する提言を行った。なお、 情報社会基盤政策機関の設立に向けては、検討、具体案の策定、そして組織設立の段階を踏む必要がある。本提言は検討開始に向けての提言である。

本提言を実現することにより、情報社会基盤を利用して、各社会基盤をより安全かつ効率的に機能させることが可能となり、安全・安心な社会の実現に向けて大きな一歩を踏み出せるであろう。また、情報社会基盤政策機関の実現に当たっては、多数の機関が複雑に関与しているため、大きなブレークスルーが必要になると思われる。このため、本提言では可

能な限り、今後の検討が容易になるように詳細な案を提示した。今後は、本提言をもとに具体的な組織設計を行うとともに、提言の実現に向けての法整備・組織整備を段階的に進めることが課題となる。さらに、情報社会基盤に限らず、全てのシステムに完全な安全・安心はありえないことを認識し、達成すべきレベルに関する幅広く深い議論に基づいて検討を進めるべきである。

最後に、本提言に記載された情報社会基盤政策機関の設立は、情報システム社会基盤を利用した効率的な社会の構築のための最初の第一歩であり、本提言を出発点として、今後、さらにセキュリティ・ディペンダビリティの研究・開発を深めていく必要があることを強調しておきたい。

＜引用文献＞

[1] 警察庁「平成 19 年上半期のサイバー犯罪の検挙状況等について」 広報資料、平成 19 年８月 23 日 http://www.npa.go.jp/cyber/statics/h19/pdf37.pdf

[2] スキャン・ネットセキュリティ「警視庁の捜査資料などが Winny 上に流出、巡査長の私有 PC から」 https://www.netsecurity.ne.jp/1_9400.html

[3] 岡村久道「法律は助けてくれない」日経コミュニケーション 2006 年 10 月 15 日号-12 月 15 日号 http://itpro.nikkeibp.co.jp/article/COLUMN/20061201/255707/

[4] 科学技術振興機構・社会技術研究開発センター「情報と社会」研究開発領域計画型研究開発「高度情報社会の脆弱性の解明と解決」
http://www.ristex.jp/examin/infosociety/advanced/index.html

[5] 科学技術振興機構「失敗知識データベース」
http://shippai.jst.go.jp/fkd/Search?fn=1&dt=2&cat=TZ00000006

[6] 科学技術振興機構・研究開発戦略センター戦略イニシアティブ「情報化社会の安全と信頼を担保する情報技術体系の構築---ニュー・ディ ペンダビリティを求めて---」 http://crds.jst.go.jp/output/sp.html#1

[7] 警視庁「セキュリティポータルサイト用語集」
http://www.cyberpolice.go.jp/words/

[8] 情報処理推進機構・セキュリティセンター「ネットワーク関連用語集」
http://www.ipa.go.jp/security/ciadr/crword.html

[9] 苗村憲司「SC27 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

[10] IFIP WG10.4, “Dependable Computing and Fault Tolerance,”
http://www.dependability.org/wg10.4/

[11] A. Avizienis, J-C. Laprie, B. Randell and C. Land, “Secure Computing,” IEEE Trans. on Dependable and Secure Computing, Vol.1, No.1, pp.11-33, 2004.

[12] Yonah Alexander and Michael S. Swetna, “Cyber Terrorism and Information Warfare: Threats and Responses (Terrorism Library Series),” Transnational, June 1, 2001

[13] 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

[14] 文部科学省「情報化への対応」
http://www.mext.go.jp/a_menu/shotou/zyouhou/main18_a2.htm

[15] 警察庁生活安全局生活環境課「平成 19 年中における生活経済事犯の検挙状況について」 http://www.npa.go.jp/safetylife/seikan43/h19_seikeijihan.pdf

[16] 日本インターネットプロバイダー協会 「著作権を守ろう」
http://www.keidanren.or.jp/japanese/policy/2008/018/index.html

[17] 日本経済団体連合会「国民視点に立った先進的な電子社会の実現に向けて」 2008.4.15 http://www.jaipa.or.jp/midori/copyright/violation_rule.html

＜用語解説*＞

○インシデント

英語の incident に対応。日本語として使われている「インシデント」は、重大事故に至る可能性がある事態が発生し、なおかつ実際には事故につながらなかった潜在的事例のことをさす。

○ウイルス（コンピュータウイルス）

ユーザが意図しない動作を行うプログラムで、伝染機能、潜伏機能、発病機能のいずれか一つ以上の機能を持つ。多くの場合は、何らかの被害を及ぼすように悪意を持って作られる。

○改ざん

文書等に記述された字句等を、作成者等の許諾を得ないで不正に書き直すこと。例えば、他者の管理する Web ページを書き換え信用失墜に陥れたり、他者からのメールの内容を書き換えて欺いたりすることなど。

○可用性

可用性（availability）とは、情報セキュリティの要件のひとつで、必要なときに適時にアクセス可能であり、利用可能である状態を維持することを言う。

○完全性

完全性（integrity）とは、情報セキュリティの要件のひとつで、データとそれを格納する情報システムが正確で完全であり、偽造や改ざんされていない状態を維持できることを言う。一貫性とも呼ぶ。

○個人識別番号(PIN)

個別のユーザに割り当てられる一意の番号。

○サイバー犯罪

情報社会基盤を利用した犯罪。

○事故

人や物などに損傷や損害を与える偶発的な出来事。

○守秘性

守秘性（confidentiality）とは、情報セキュリティの要件のひとつで、認可された人（主体）に対してのみ認可された条件で開示され、権限のない（認可されていない）ユーザが情報にアクセスできないという状態を維持できることを言う。機密性、秘匿性などとも呼ぶ。

○証明書

証明書は、デジタル署名を検証するのに使用されるデータであり、通常、信頼できる

---

*用語解説は以下を参考にしている。

- 警視庁 「セキュリティポータルサイト用語集 http://www.cyberpolice.go.jp/words/
- 情報処理推進機構セキュリティセンター「ネットワーク関連用語集」
  http://www.ipa.go.jp/security/ciadr/crword.html

とされる機関が発行する。証明証と呼ぶこともある。証明書を用いて、ある署名が正当と検証された場合、「この証明書を発行した機関によれば、この署名者は本人(その名前)である」ということができる。

〇スパイウェア

コンピュータ利用者の IP アドレスや Web の閲覧履歴等の個人情報を、ひそかに収集して外部へ送信するプログラムのこと。広告やマーケティングのためにデータを集めるものが多い。他のソフトウェアと共に配布、インストールされるため、利用者はインストールされたことに気づきにくい。一般のウイルス対策ソフトでは検出されない場合も多く、その発見と駆除には専用のスパイウェア対策ソフトが用いられる。

〇スパムメール

不特定多数のユーザに対し、承認を得ずに送られる迷惑メール。送信元を隠すため、セキュリティの弱いメールサーバが、スパムメールの発信に不正利用されることがある。

〇セキュリティ

本提言では、情報セキュリティの意味で用いる。これは、情報システムにおいて、意図的・組織的な犯罪行為・不正行為、大規模災害等により非確率的に生じるリスクを最小化することと定義され、情報の可用性、守秘性、完全性の維持がその主要な要件となる。さらに、真正性、責任追跡性、否認防止性や信頼性などを要件とすることもある。

〇セキュリティホール

ソフトウェアのバグや設定ミス等セキュリティ上の弱点をいう。ソフトウェアのバグの場合、発見後配布されるセキュリティパッチを直ちに適用し、セキュリティホールを塞ぐことが重要である。脆弱性と同義で用いられることもある。

〇セキュリティポリシー

安全を確保するために何をどのように守るかを決めた方針のこと。情報システムにおける「情報セキュリティポリシー」を指すことが多く、情報資産、情報ネットワークのセキュリティを確保する際に、守るべき範囲、それに必要となる対策、規約等を定めたものをいい、これに則ってシステムの構築と運用を行う。また、運用に即した定期的な見直しが必要となる。

〇脆弱性

セキュリティ分野において通常、脆弱性（vulnerability）とは、システム、ネットワーク、アプリケーション、または関連するプロトコルのセキュリティを損なうような、予定外の望まないイベントにつながる可能性がある弱点の存在、設計もしくは実装のエラーのことをいう。オペレーティングシステムの脆弱性である場合もあれば、アプリケーションシステムの脆弱性である可能性もある。またソフトウェアの脆弱性以外に、セキュリティ上の設定が不備である状態においても、脆弱性があるといわれることがある。セキュリティホールと呼ばれることもある。

〇ディペンダビリティ

システムの信頼性に関する包括的概念を表す用語。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、信頼性、安全性、保守性などの維持が主要な要件とされる。

偶発的な故障や人の過誤などから情報システムの安全・安心を守ることを主要な目的としてきたが、最近では、情報システムに対する意図的攻撃も含めて論じることがあり、セキュリティと融合する面が見られる。

〇電子署名（デジタル署名）

メッセージの発信者のなりすましや内容の改ざんの有無を確認するためのもの。様々な方法があるが、例えば、発信者はメッセージとともに自らの秘密鍵でメッセージのダイジェストを暗号化したもの（認証子）を添付し、受信者は受信したメッセージから作成したダイジェストと、発信者の認証子から公開鍵で復号したダイジェストとを比較することによりメッセージ発信者及びそのメッセージの正当性を担保するなどの方法で行われる。なお、電子署名とデジタル署名は同義で用いられることもあるが、電子署名をより広義に、電子的な手段で行う署名程度の意味で用いることもある。

〇なりすまし

ネットワーク上で他人のふりをすること。なりすましは、他人のパスワードや Cookie の使用、電子メールの発信アドレスの詐称、偽の Web サイトなどにより行われる。例えば、他人の ID とパスワードを用いてなりすました場合には、なりすまされた人の預金を引き出したり、偽の情報を発信したりするなどの行為が可能で、なりすまされた人が被害を受ける可能性がある。

〇認証／本人認証

認証もしくは本人認証は、ユーザが本人であることを証明する過程をいう。認証のプロセスは、典型的には、本人であることの証拠として、ユーザの名前とパスワードやパスフレーズの入力を要求する。近年、スマートカードなどユーザの持ち物や、ユーザの身体的特徴（バイオメトリクス）に基づく認証機構も普及しつつある。

〇ハッカー

コンピュータやネットワークに非常に詳しい人のことをいう。それらの知識を悪用して不正アクセスや破壊行為を行うクラッカーと同じ意味で使用されることもある。

〇ヒューマンクリプト

暗号・認証システムを，セキュリティの観点から人も含めて最適化することを目的とする技術．安心が重要な評価軸の一つとなる．

〇ファイアウォール

ネットワークの内部と外部の境界に設置して通信を監視し、許可されない通信を遮断することによって、セキュリィを高める装置。アプリケーション・ゲートウェイとパケット・フィルタリングの 2 種類の方式がある。

〇フィルタリング・ソフト

ウェブサイト上の違法・有害情報へのアクセスを制御するために、受信者側でこれらの情報を受信するかどうかを選択できるソフトウェアをいう。

〇踏み台

スパムメールの発信や他サーバへの不正アクセスを行うことを目的として不正に利用されるサーバのこと。セキュリティ管理の甘いサーバが狙われる。踏み台にされたサー

バの管理者が被害を受けた側から責任を問われる場合もある。

○ワーム

ウイルスの一種。ネットワークを利用して、他のホストに自分自身のコピーを送り込んで自己増殖する。ファイルには感染せずに、単独のプログラムとして動作する。

○AIST

産業技術総合研究所(Advanced Industrial Science and Technology)の略称。経済産業省の傘下にある。

○CISA

情報システムコントロール協会（ISACA)が認定する情報システム監査人（Certified Information System Auditor）の略称

○CISM

情報システムコントロール協会（ISACA)が認定する情報セキュリティマネージャー（Certified Information Security Manager）の略称

○CISSP

国際情報システムセキュリティ認証コンソーシアムが認定する情報システムセキュリティのプロフェッショナル（Certified Information Systems Security Professional）の略称

○CRYPTREC

Cryptography Research and Evaluation Committees の略。電子政府推奨暗号の安全性を評価・監視し、暗号モジュール評価基準等の策定を検討する暗号技術検討会、暗号技術監視委員会、暗号モジュール委員会などの総称であるが、これらが行うプロジェクトの意味でも用いられる。経済産業省と総務省の傘下にある。

http://www.cryptrec.jp/about.html

○Edy

Edy（エディ）は、ビットワレット株式会社が提供する電子マネーで、ソニーが開発した非接触 IC カード FeliCa の技術を用いている。

○ICOCA（イコカ）

西日本旅客鉄道（JR 西日本）が 2003 年 11 月 1 日に近畿地方のアーバンネットワークで最初に導入した、主に乗車カードや電子マネー、ロッカーの鍵として利用できる IC カードで、ソニーの非接触型 IC カード FeliCa の技術を用いている。ICOCA の名称は JR 西日本の登録商標である。

○IETF Security Area （Internet Engineering Task Force セキュリティエリア）

IETF は、インターネット技術の標準化を行っており、技術プロトコル仕様文書のほか情報提供文書は、RFC（Request For Comments）として発行される。セキュリティ分野においてもワーキンググループが複数あり、これらの標準化過程統括統して IESG （運営グループ）に参画するディレクターがいる。

http://www.ietf.org/html.charters/wg-dir.html#Security_Area

http://web.mit.edu/network/ietf/sa/

○INSTAC

財団法人日本規格協会 情報技術標準化センター（Information technology research and Standardization Center）の略称。経済産業省の傘下にある。

○IPA

情報処理推進機構(INFORMATION-TECHNOLOGY PROMOTION AGENCY,JAPAN)の略称。経済産業省の傘下にある。

○ISACA

情報システムコントロール協会(Information Systems Audit and Control Association)の略称。

○ISO / IEC JTC1 / SC27

ISO は International Organization for Standardization（国際標準化機構)、IEC は International Electro technical Commission（国際電気標準会議)、JTC1 は、ISO と IEC が共同で設置した情報処理関連技術の国際規格の作成を担当する技術委員会、その下部組織であるSC27は､情報セキュリティ技術全般の国際標準を決定する委員会である。

○ JASA

日本セキュリティ監査協会(Japan information Security Audit association) の略称。

○ JPCERT/CC

有限責任中間法人 JPCERT コーディネーションセンター(Japan Computer Emergency Response Team Coordination Center)の略称。経済産業省の傘下にある。

○JST

独立法人科学技術振興機構(Japan science and Technology Agency)の略称。文部科学省の傘下にある。

○NICT

情報通信研究機構(National Institute of Information and Communications Technology)の略称。総務省の傘下にある。

○NISC

内閣官房情報セキュリティセンター(National Information Security Center)の略称。内閣官房の傘下にある。

○NISM 推進協議会

通信機械工業会、社団法人テレコムサービス、社団法人電波産業会、社団法人日本インターネットプロバイダー協会、財団法人日本データ通信協会、ネットワークセキュリティ登録事業者協議会、社団法人電気通信事業者協会が合同で設立した協会である。総務省の傘下にある。http://old.netsecurity.ne.jp/article/1/1939.html

○NISM

ネットワーク情報セキュリティマネージャー(Network Information Security Manager)の略称

○PASMO

PASMO（パスモ）は、2007年3月18日からサービスを開始した電子マネー機能を有する非接触型ICカード方式の日本の鉄道・バス共通乗車カードである。PASMOの名称は株式会社パスモの登録商標である。

○PiTaPa

PiTaPa（ピタパ）は、関西圏の鉄道・地下鉄・バス事業者が加盟するスルッとKANSAI協議会が導入した非接触型ICカードによるストアードフェアシステムとショッピングなどの決済サービスに対応したカードの名称である。PiTaPaは「Postpay IC for ″Touch and Pay″」の略称である。

○SUGOCA

SUGOCA（スゴカ）は、九州旅客鉄道（JR九州）が2009年春に導入予定のICカード方式の乗車券である。

○Suica

Suica（スイカ）は、2001年11月18日に東日本旅客鉄道（JR東日本）が東京近郊区間で最初に導入した、ソニーの非接触型ICカードFeliCaを搭載したカードで、主に乗車カードや電子マネーとして利用できる。Suicaの名称はJR東日本の登録商標である。

○SSH （Secure Shell）

BSD系 UNIX の r* コマンドを、チャレンジレスポンスの仕組みによってセキュアにしたプロトコル。遠隔地のマシンでコマンドを実行したり他のマシンへファイルを移したりするために使われる。プロトコルとして、SSH1 と SSH2 の 2つのバージョンがある。

○SSL （Secure Socket Layer）

Web 上でデータを暗号化して通信を行う技術。認証機能によるなりすまし防止と、暗号化による盗聴防止に有効である。多くのオンラインショッピングサイトでクレジットカード番号入力時に利用されている。ネットスケープコミュニケーション社によって提案された汎用セキュアプロトコルスキーム。より上位層の HTTP や POP、 IMAP などのアプリケーションプロトコルにセキュリティ機能を与える。SSL ハンドシェイクプロトコルと SSL レコードプロトコルから構成される。

○TLS（Transport Layer Security）

SSL 後継のセキュアプロトコルスキーム。RFC 2246 TLS v1 参照。

○WEP（Wired Equivalent Privacy）

無線LANの規格である IEEE 802.11 においてセキュリティ機能を実現するオプションの一つで、パケットの暗号化を行う。秘密鍵のデータ長により 64bit(実効 40bit)と128bit（実効 104bit)のものがある。複数の脆弱性が報告されており、Fast Packet Keying などアルゴリズムを改良した新しい暗号化方式が開発されている。

○Winny

P2Pの技術を利用したファイル共有ソフト。

＜参考資料＞

１　情報学委員会セキュリティ・ディペンダビリティ分科会審議経過

平成 18 年 11 月 22 日　日本学術会議幹事会（第 29 回）
　○セキュリティ・ディペンダビリティ分科会設置
平成 18 年 11 月 22 日　日本学術会議幹事会（第 29 回）
　○セキュリティ・ディペンダビリティ分科会委員決定
平成　19 年　1 月　29 日セキュリティ・ディペンダビリティ分科会（第１回）
　○委員長等の選出について
平成　19 年　3 月　30 日セキュリティ・ディペンダビリティ分科会（第２回）
　○本分科会が取り組むべき課題
平成 19 年 6 月 21 日　セキュリティ・ディペンダビリティ分科会拡大役員会（第１回）
　○今後の活動について
平成 19 年 9 月 25 日　セキュリティ・ディペンダビリティ分科会拡大役員会（第２回）
　○社会システム構成要素としての重要社会基盤の情報セキュリティとその課題について
平成 19 年 11 月 5 日セキュリティ・ディペンダビリティ分科会（第３回）
　○企業の情報事故対策について
　○対外報告について
　○リスク検討分科会との連携について
平成 20 年 2 月 29 日セキュリティ・ディペンダビリティ分科会（第４回）
　○対外報告　「安全・安心を実現する情報社会基盤の普及に向けて」（案）

平成 20 年 6 日 26 日本学術会議幹事会（第 58 回）
　○提言「安全・安心を実現する情報社会基盤の普及に向けて」（案）について承認