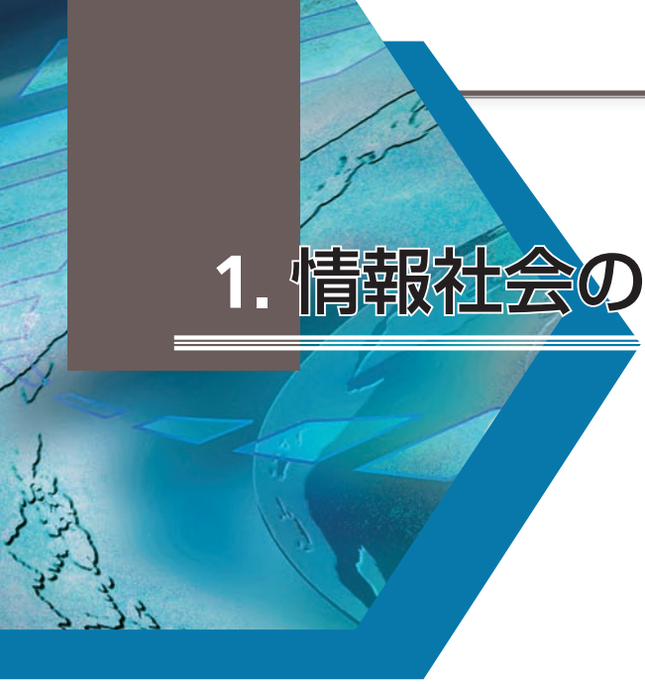

1. 情報社会の脆弱性について

（株）三菱総合研究所 情報セキュリティ研究部
村瀬 一郎　murase@mri.co.jp

中央大学理工学部
土居 範久　doi@doi.ics.keio.ac.jp

高度情報社会においては，情報システムが社会のさまざまな分野に浸透している．そして，情報システムは，広く深く根付き複雑化しており，多くの構成要素と構成要素間の複雑な関係を有するに至り，その結果として莫大な数の脆弱性を抱えていることが推察される．脆弱性は，情報システムを構成する個々の機器・ソフトウェアから大規模システム・業務に至るまで，さまざまなレイヤに内在している．

本稿では，こうした脆弱性の定義，種類，およびそれらの対策の動向，関連する研究動向について述べる．

脆弱性とは

◆脆弱性の定義

近年，脆弱性という言葉は，情報セキュリティにおいて頻繁に用いられる．経済産業省告示第二百三十五号[1]においては，脆弱性を「ソフトウェア等において，コンピュータウィルス，コンピュータ不正アクセス等の攻撃によりその機能や性能を損なう原因となり得る安全性上の問題個所．Web アプリケーションにあっては，Web サイト運営者がアクセス制御機能により保護すべき情報等に誰もがアクセスできるような，安全性が欠如している状態を含む」と定義している．この定義は，脆弱性の範囲を，コンピュータウィルスや不正アクセスにより機能や性能を損なう原因となる安全性上の問題個所として限定している．

総合科学技術会議では[2]，「脆弱性とは，情報通信システムやその運用体制において，第三者に悪用されるおそれのあるセキュリティ上の欠陥や問題点をいう」と定義し，経済産業省告示による定義より，運用を視野に入れている点とウィルス等の直接の原因に限定していない点で，いくぶん範囲を広げている．

一方，防災分野では，従来から脆弱性という言葉が利用されている．国連は，「脆弱性とは，『ハザードの影響に対するコミュニティの感受性を増加させる，物質的，社会的，経済的，環境的要因，もしくはそれらのプロセスにより決定づけられる状況』である」と定義している[3]．なお，ハザードとは，「人命の損失，負傷，財産への損害，社会的・経済的崩壊，もしくは環境破壊を引き起こす可能性のある，潜在的に有害な自然事象・現象，人間活動」のことである[3]．この定義は，脆弱性に関して，ハザードを増長させる要因であると述べており，ハザードの存在を前提としている部分に特徴がある．

情報セキュリティの文脈における脆弱性という言葉は，悪意ある攻撃者が利用する性質であることが一般的である．しかし，本稿および本特集においては，国連の定義を勘案した上で，ハザードを情報システム事故全般と捉え，脆弱性をそうした情報システム事故全般を増長させる要因であると定義する．

◆脆弱性とバグ

脆弱性とバグは，どのように異なるかという議論がある．ソフトウェアの脆弱性に限定した場合，脆弱性とはバグであるといえる．これは，ソフトウェアの脆弱性が，バッファオーバーフローやメモリリーク等ソフトウェアのプログラミング上のミスから生ずるものが圧倒的に多いためである．他のバグと異なり，特殊な入力値を必要とする等の理由により発見が困難であるため，バグと区別されていることもある．

しかし，情報システム全体や重要インフラを考えた際，構成要素はソフトウェアのみではなく，ハードウェアや人間系がかかわり，これらも脆弱性を有していると考える．その際の脆弱性とは，バグとは区別されるものである．

本稿においては，脆弱性に関して，こうした定義があることを念頭に置きつつ，さまざまなレイヤの脆弱性を紹介し，脆弱性にかかわる研究の全体像を総括するものとする．

脆弱性の名称	対策を検討する際に考慮すべき主なポイント
他人受入	・誤受入率や誤合致率等の認証精度指標とその評価
狼（Wolf）	・誤受入率や誤合致率等の認証精度指標とその評価 ・脆弱性を引き起こす可能性がある生体情報を有する個人が存在する割合，および，その影響度
子羊（lamb）	
類似性	
偽生体情報	・生体情報の物理的な偽造の難易度の評価
公開	・生体情報補足の難易度
推定	・生体情報とその照合結果を外部に漏洩させない手段
利用者状態	・品質の低い固有パターンの登録を回避する手段
入力環境	
認証パラメータ	・パラメータの適切な選択とその設定に関する管理・運用方法
登録	・登録時における本人確認方法
データ漏洩	・システム内部で処理・保管されるデータの機密性，一貫性を確保するとともに，後日再度の検証を可能にする手段
単独	・生体認証システムおよびその代替認証手段に求められるセキュリティ要件と，適切なセキュリティ評価
代替手段	
提供	・脅迫等による脅威への対策
サイドチャネル	・想定されるサイドチャネル攻撃への対策
センサ露出	・センサに生体情報が残留しない手段　・生体検知機能の採用
構成管理	・生体認証システムの設計・テスト・評価

表 -1　生体認証システムにおけるなりすましに関する脆弱性と対策のポイント
（http://www.fsa.go.jp/singi/singi_fccsg/gaiyou/f-20050415-singi_fccsg/02.pdf より引用）

デバイスの脆弱性

◆バイオメトリクスデバイス

松本によれば[4]，生体認証における脆弱性は，表 -1 に総括することが可能である．

松本は，特に偽生体情報の入力にかかわる脆弱性の研究を行っており，グミにより指紋が偽造可能であり，指紋認証デバイスがグミの指紋も正規の指紋として誤認識する事実を指摘している[5]．

◆情報家電

2004 年 10 月に，東芝の DVD レコーダが，スパムメールの踏み台となる脆弱性を有することが発表された[6]．これは，当該 DVD レコーダが，proxy サーバ機能を実装しており，かつ工場出荷時の設定ではパスワードを付与されていなかったため，家庭外の外部ネットワークと直接接続した場合，Open Proxy 状態となり，スパムメールの踏み台となる脆弱性を有していたことに起因する．

この脆弱性の露見により，情報家電がコンピュータであること，それらにサーバ機能が搭載されていること，セキュリティ対策が必ずしも万全ではないことなどを，我々は再認識させられた．

現在，ネットワークに接続される家電は，DVD レコーダ以外にも，テレビ，カーナビゲーション等が存在しており，今後，IPv6 の普及に伴い，多くの家電製品がネットワークに接続されることを念頭に置くと，情報家電における脆弱性対策は必須であることを痛感させられる．

ただし，ソフトウェア製品と異なり，社会全体としての脆弱性の対策においては，以下を勘案する必要がある．

- 情報家電の場合，脆弱性の修正に際し，ソフトウェアの修正のみでとどまらない場合があり，ハードウェアの交換を伴う
- ソフトウェアの修正のみで対応可能な場合でも，情報家電の利用者全員に対して，パッチを当てることを期待することは無理がある
- こうした条件を勘案すると，情報家電ベンダや小売店が協力して，脆弱性を含む故障修理体制を構築する必要がある

◆携帯電話

携帯電話は，電話のみならず，インターネットへのアクセス，電子メール等でも広く利用されているが，ソフトウェア製品ほどの脆弱性の報告はない．現在までに，確認されている脆弱性は以下のようなものがある．

- A 社のブラウザには，制御用の HTML タグを解釈する機能があり，これを利用することで，メールを開くだけで強制的に指定した先にメールを送信させたり，電話を発信させることができる脆弱性が存在した
- 海外の Bluetooth 対応携帯電話において，アドレス帳，カレンダー予定表，メールメッセージ等を入手すること，メモリに偽のテキストメッセージを埋め込むこと，

携帯を盗聴器に変え音声を拾うことが可能となる脆弱性が存在した
- 海外の Java 対応の携帯電話にて，悪質な Java プログラムをダウンロードし実行した場合に，データの送信，メモリの消去，ネットへの接続等が行われる可能性がある脆弱性が存在した

近年の携帯電話は，独自 OS から汎用 OS の流れがあり，Symbian 等の OS の利用が活発になっている．Symbian には，ワーム型ウィルスやトロイの木馬が発見されており，社会的な脆弱性の対策が必須な状況となっている．

ソフトウェア製品の脆弱性

ソフトウェア製品とは，ソフトウェア単体またはソフトウェアを組み込んだ形式で幅広く流通している製品である．ソフトウェア製品の脆弱性の特徴は，以下に挙げることが可能である．

- ソフトウェア製品において，脆弱性は避けて通れない問題である
- ソフトウェアの製造者にとって，ソフトウェアの流通先をすべて把握できるわけではない
- 多くのソフトウェアの場合，パッチを当てることにより，脆弱性を修正することが可能となる
- 現代においては，パッチを，インターネットを活用して広く配布することが可能である

ソフトウェア製品においては，こうした特徴を踏まえた上で，情報セキュリティ早期警戒パートナーシップの運用が開始された[7), 8)]．ソフトウェア製品の脆弱性対策の特徴は，以下の通りである．

- ゼロデイアタック（当該脆弱性に対する対策が公表される以前の攻撃）を防止することを最大の目的とする
- インターネットにより，パッチや設定変更等の対策にかかわる情報を発信する

Web アプリケーションの脆弱性

Web アプリケーションとは，インターネット上の特定の Web サイト上で稼働するアプリケーションのことである．Web アプリケーションの脆弱性に関しては，本特集で，「Web アプリケーションにおける脆弱性」として記述されている[17)]．Web アプリケーションの脆弱性の特徴は，以下の通りである．

- ソフトウェア製品と同様に，Web アプリケーションにおいても脆弱性は不可避の問題である
- 電子商取引サイト等では，個人情報を扱っていることも多く，脆弱性の影響を見過ごすことはできない
- 脆弱性の種類はクロスサイトスクリプティング等が多く[6)]，ソフトウェア製品とは質的な違いがある

こうした特徴を踏まえた上で，社会として Web アプリケーションの脆弱性を削減しようとする際には，以下の事項が重要となる．

- Web アプリケーションの運用者は，大手事業者から個人までさまざまであり，それらに一律に対策を求めることは困難である
- 個人情報を大量に扱う等の Web サイトにおける Web アプリケーションの脆弱性に関しては，緊急の措置が必要な場合がある
- Web アプリケーションを構成するソフトウェア製品の脆弱性の場合，他の Web サイトの Web アプリケーションも同様の脆弱性を有することが想定されるため，ソフトウェア製品の開発者による対応が必要となる

情報システムの脆弱性

情報システムの脆弱性に関しては，さまざまな面から論ずることができる．情報システムは，ソフトウェア・ハードウェア・ネットワーク・インフラストラクチャ・運用する人間により構成されるものであり，それぞれに脆弱性が内包されている．ここでは，ハードウェア・インフラストラクチャ・運用，にかかわる脆弱性について述べる．

◆ハードウェアにかかわる脆弱性

情報システムにおけるハードウェアの脆弱性とは，以下のように分類することができる．

火災や自然災害・破壊など物理的脅威にかかわる脆弱性

ハードウェアは，火災や自然災害，悪意を有する破壊などにより，正常な稼働に影響が及ぶという脆弱性を有している．これに対する対策は，以下のようなものがある．

- 建物等インフラストラクチャを強化すること（これについては，インフラストラクチャの項で述べる）
- ハードウェア自体の強度を強化すること（筐体の強度強化や，転倒防止等の技術）
- ハードディスクやメモリ上の状態を瞬時にバックアップすること
- ハードウェアの 2 重化・冗長構成を行うこと

悪意を有する物理的な覗き見や改竄にかかわる脆弱性

ハードウェアにかかわる覗き見や改竄に関する研究としては，暗号のサイドチャネル解析が知られている[9)]．サイドチャネル解析とは，コンピュータが暗号の処理を行

う過程で放出するさまざまな情報を使い，暗号鍵を取得しようとする試みである．電力解析，フォールト・ベース解析，タイミング解析，TEMPEST などがある．電力解析とは，暗号モジュールで消費される電力や入出力データから，鍵を推定する攻撃法である．フォールト・ベース攻撃は，暗号モジュールに対する意図的な誤動作を利用する．平文と処理速度の関係を利用するタイミング攻撃などが研究されている．TEMPEST とは，ディスプレイ，ケーブル等から発生する電磁波を介した情報漏洩に関する技術である．

こうした脆弱性を悪用する技術を阻止するために，日本規格協会で耐タンパー性技術の標準化が図られている[10]．

◆インフラストラクチャにかかわる脆弱性

情報システムが稼働するためのインフラストラクチャとは，電力基盤および電源装置，通信基盤，建物，上下水道を指す．これらにかかわる脆弱性を列挙すると，以下となる．

- 情報システムは，電力基盤に依存しており，電力供給がストップすると，情報システムの稼働に大きな影響が出る
- サーバが設置されているデータセンタには，自家発電装置等が付設されているが，クライアント側の電力供給が途絶えると代替手段に欠くという脆弱性が存在する
- 建物に関しては，地震によるコンピュータや情報通信機器の物理的破壊に伴う脆弱性がある

◆運用にかかわる脆弱性

運用にかかわる脆弱性は，非常に幅広く，多種多様である．ここでは，ISMS 情報セキュリティマネジメントシステム適合性評価制度 ISMS 認証基準を参照し[11]，それらを総括して述べる．

組織体制にかかわる脆弱性

- 組織における情報システム事故にかかわる体制が明確でない場合，情報システム事故の発生時の対応等が曖昧となる
- 外部に情報システムの開発や運用を委託する場合，緊急時の対応・判断，機密情報の管理等の側面に問題が生ずることがある

情報資産の管理にかかわる脆弱性

- 情報資産が，その重要度に沿って適切に分類されていない場合，それらの取り扱いに際して問題が生ずることがある

人員にかかわる脆弱性

- 関係する人員の情報システム事故にかかわる意欲や能力に問題がある場合，脆弱性の原因となる
- 関係する人員との契約に，情報システム事故にかかわる事項，機密保持にかかわる事項がない場合，脆弱性の原因となる

緊急時の対応にかかわる脆弱性

- 情報システム事故発生時の対応手順が定められていない場合，事故の局所化を行うことができないことがある

物理的セキュリティにかかわる脆弱性

- 重要な機器等が認可された人員のみがアクセス可能となる区域に設置されていない場合，問題が発生することがある
- 記憶装置を処分する前に，記憶内容を廃棄しなければ，問題が発生する

システムの計画にかかわる脆弱性

- システムの容量や性能に関して，未来も予測した上で計算し，それが反映されたものでない場合，問題が発生することがある
- 新しいシステムを導入する場合，その受入基準を明示し，それに沿った試験がなされていない場合，問題が発生することがある

システムの維持管理について

- データおよびソフトウェアのバックアップを定期的に実施し，かつその検査を行わない場合，問題が発生することがある
- 運用担当者が自らの作業を記録し，保管しない場合，問題が発生することがある
- システムに関する文書が適切に管理されていない場合，問題が発生することがある

情報およびソフトウェアの交換について

- 組織間の情報やソフトウェアの交換は，正式な契約締結後に行われない場合，問題が発生することがある

アクセス制御について

- 情報システムにアクセスするための利用者にかかわる，正式な利用者登録および登録削除の手続きがない場合，問題が発生することがある
- 利用者のパスワード設定に関して，セキュリティ慣行（誕生日や電話番号と絡めず，1 カ月に 1 度は変更する，メーカ設定パスワードを利用しない等）に遵守していない場合，問題が発生することがある
- 不要なサービスやポートを閉じない場合問題が発生することがある
- 利用者 1 人 1 人に ID を割り当てない場合問題が発生

することがある
- 端末のタイムアウト機能を実装していない場合問題が発生することがある
- 情報セキュリティにかかわるイベントを記録し，一定期間保存しない場合問題が発生することがある
- 情報システムに接続可能な移動型端末（ノート型 PC，携帯電話等）に関する管理方針が明確になっていない場合問題が発生することがある

システムの開発および保守について

- 入力値の妥当性を確認しない場合，問題が発生することがある
- 出力データの妥当性を確認しない場合，問題が発生することがある
- 取り扱いに慎重を期すべき情報に関して，暗号化を行っていない場合，問題が発生することがある
- 運用システムでのソフトウェアの実行管理を適切に行わない場合，問題が発生することがある
- 試験データの厳密な管理を行わない場合，問題が発生することがある
- ソフトウェアの変更に関して厳しく管理しない場合，問題が発生することがある

事業継続性管理について

- 重大な情報システム事故発生時に，事業を継続させるための計画を保持していない場合，問題が発生することがある
- 事業継続計画の適切な試験と定期的な見直しがない場合，問題が発生することがある

適合性について

- 法令への適合性に関して，適切に管理することがない場合，問題が発生することがある

◆個々の情報システムの脆弱性

本節においては，（独）科学技術振興機構・社会技術研究システムのミッション・プログラム II「高度情報社会における脆弱性の解明と解法の研究」[12] での取り組みの中から，暗号基盤と DRM（Digital Rights Management）の脆弱性に関する研究を取り上げる．

暗号基盤[13]

多くの情報システムにおいて，暗号は日常的に利用されており，こうした利用により社会には暗号基盤が形成されている．暗号基盤の脆弱性は，暗号アルゴリズムの脆弱性，暗号モジュールの脆弱性，さらには暗号利用システムの脆弱性に分けることが可能である．暗号アルゴリズムの脆弱性とは，学問的に暗号アルゴリズムが解読される可能性があることを言うことが一般的である．暗号モジュールの脆弱性とは，暗号アルゴリズムを実装したモジュールからサイドチャネル攻撃等により秘密鍵等の秘密データが漏洩する可能性があることを言う．暗号利用システムの脆弱性とは，暗号を利用するシステムにかかわる一般的な脆弱性であり，物理的な脆弱性，暗号アルゴリズムにかかわる脆弱性，暗号モジュールにかかわる脆弱性，鍵にかかわる脆弱性，証明書にかかわる脆弱性，法制度にかかわる脆弱性などに分けることが可能である．

DRM[14]

DRM とは，ディジタル著作権管理と訳されることが多く，情報技術を用いてディジタル化可能なコンテンツの著作権を保護しようとするシステムである．DRM にかかわる脆弱性は，DRM システムそのものの脆弱性ではなく，以下のディジタルコンテンツに関係する脆弱性を認識すべきである．

- ディジタルコンテンツの違法な利用が進む場合，ディジタルコンテンツの供給者の経済的基盤が危うくなり，ディジタルコンテンツの流通量が減少する可能性がある
- ディジタルコンテンツの違法な改竄が進む場合，ディジタルコンテンツの利用者が著作権侵害に加担する可能性がある

脆弱性を克服するための取り組み

近年，脆弱性を克服するための取り組みが進められている．ここでは，（独）情報処理推進機構（IPA）と JPCERT/CC を中心として構築されている情報セキュリティ早期警戒パートナーシップ，およびミッション・プログラム II における取り組みを述べる．

◆情報セキュリティ早期警戒パートナーシップ

2004 年 7 月に，情報セキュリティ早期警戒パートナーシップは，開始された．情報セキュリティ早期警戒パートナーシップとは，ソフトウェア製品と Web アプリケーションの脆弱性に焦点を当て，IPA が受付機関，JPCERT/CC が調整機関となって，関係者の中で脆弱性対応のための調整を行い公表するという枠組みである[7]．

◆ミッション・プログラム II における取り組み

ミッション・プログラム II においては，情報システムの脆弱性を可視化するために，情報社会におけるハザードマップ作成を行っている．ハザードマップは，首都圏で大規模電力障害が発生したことを仮定し，情報システムへの影響をシミュレーションしている．図 -1 は，シミュレーションのイメージである．赤色が情報システ

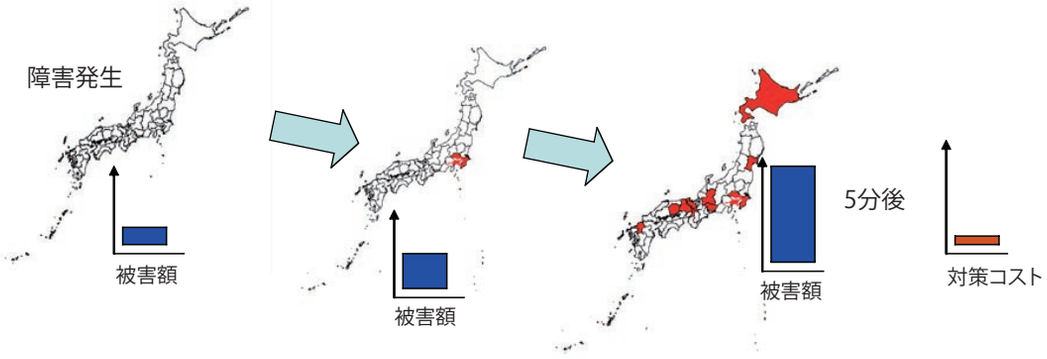

図-1　ミッション・プログラムIIにおける情報社会のハザードマップ

ムの障害が発生している部分を表している．全国に展開する情報システムが，首都圏の電力基盤に過度に依存していることを主張しようとするものである．詳細は，文献15）を参照のこと．

このハザードマップは，情報化社会における情報システムを中心とした脆弱性が，一般の人々だけではなく専門家にも理解できない部分が多いことに着目したものである．特に，情報システムを地図上にマッピングし，大規模電力障害が情報システムに地理的に及ぼす影響を明示しようとするものであり，今後の展開が注目される．

さらに，ミッション・プログラムIIにおいては，社会の脆弱性を解決するための手段として，多重リスクコミュニケータの研究を行っている．多重リスクコミュニケータは，原発等の社会的リスクに絡み，利益の異なる当事者間でのコミュニケーション（リスクコミュニケーション）を支援するためのツールである[16]．これにより，社会における脆弱性を軽減することができる．

まとめ

情報社会には，脆弱性が満ちている．ソフトウェア製品やハードウェアの脆弱性をはじめとし，それらを利用する情報システムには運用を含む脆弱性が存在し，さらにそうした情報システムを活用する業務には人間システムを含む脆弱性が存在する．このことは，1つのソフトウェア製品の脆弱性が，大規模な情報システムに多大なる影響を及ぼし，情報システムを基盤としている多くの業務の継続が困難となることを示すものである．2003年8月のMS/Blasterと呼ばれるコンピュータウィルスによりお盆明けの企業は大混乱に陥ったが，2005年4月に発生したウィルス対策ソフトウェアのウィルス定義ファイルの不具合による一連の騒動も，情報社会の脆弱性を痛切に感じさせるものであった．

現在は，ソフトウェア製品とWebアプリケーションに関して情報セキュリティ早期警戒パートナーシップという制度的枠組みができ上がっている．しかし，情報社会の脆弱性は目に見えない性質のものであり，ミッション・プログラムIIで行われているような脆弱性を可視化する取り組みにより，広く脆弱性の所在が明らかになるとともに，それらに対して適切な対策が施されることを願ってやまない．

参考文献

1）平成十六年度経済産業省告示第二百三十五号「ソフトウェア製品等脆弱性関連情報取扱基準」（平成16年7月7日），http://www.meti.go.jp/policy/netsecurity/downloadfiles/vulhandlingG.pdf
2）ソフトウェア懇談会：ソフト的な分野において推進すべき事項　補足資料，平成15年7月1日，http://www8.cao.go.jp/cstp/torikumi/soft3.pdf
3）国連防災会議：プログラム成果文書（兵庫行動枠組2005-2015）（Jan. 2005）．
4）松本　勉：金融取引における生体認証について，金融庁 第9回偽造キャッシュカード問題に関するスタディグループ，2005年4月15日，http://www.fsa.go.jp/singi/singi_fccsg/gaiyou/f-20050415-singi_fccsg/02.pdf
5）宇根正志，松本　勉：生体認証システムにおける脆弱性について―身体的特徴の偽造に関する脆弱性を中心に―，日本銀行金融研究所ディスカッションペーパー 2005-J-2（Apr. 2005），http://www.imes.boj.or.jp/japanese/jdps/2005/05-J-02.pdf
6）JVN#E7DDE712 東芝製 HDD&DVD ビデオレコーダーへ認証なしでアクセス可能：http://jvn.jp/jp/JVN%23E7DDE712/index.html
7）早貸淳子：脆弱性情報の取り扱いについて―情報セキュリティ早期警戒パートナーシップの概要と運用の状況―，情報処理，Vol.46, No.6（June 2005）．
8）歌代和正，鎌田敬介：ソフトウェア製品における脆弱性，情報処理，Vol.46, No.6（June 2005）．
9）（独）情報処理推進機構，（独）情報通信研究機構：CRYPTREC REPORT 2004（Mar. 2005），http://www.ipa.go.jp/security/enc/CRYPTREC/fy16/documents/C04mod.pdf
10）（財）日本規格協会情報技術標準化研究センター：平成15年度 経済産業省委託（基準認証研究開発事業）耐タンパー性に関する標準化調査研究開発実証実験報告書（Mar. 2005）．
11）（財）日本情報処理開発協会：ISMS 情報セキュリティマネジメントシステム適合性評価制度 ISMS 認証基準 ver2.0，2005/4/21，http://www.isms.jipdec.jp/doc/JIP-ISMS100-20.pdf
12）ミッション・プログラムII Webページ，http://www.ristex.jp/modules/activity/article.php?articleid=3
13）岡本栄司，松浦幹太，冨高政治，猪俣敦夫：暗号における脆弱性について，情報処理，Vol.46, No.6（June 2005）．
14）山口　英，金野和弘：DRMにおける脆弱性について，情報処理，Vol.46, No.6（June 2005）．
15）村野正泰，江連三香，村瀬一郎：脆弱性を視覚化するハザードマップとコストモデルについて，情報処理，Vol.46, No.6（June 2005）．
16）佐々木良一：脆弱性問題を解決するための多重リスクコミュニケータ，情報処理，Vol.46, No.6（June 2005）．
17）高木浩光：Webアプリケーションにおける脆弱性，情報処理，Vol.46, No.6（June 2005）．

（平成17年5月16日受付）