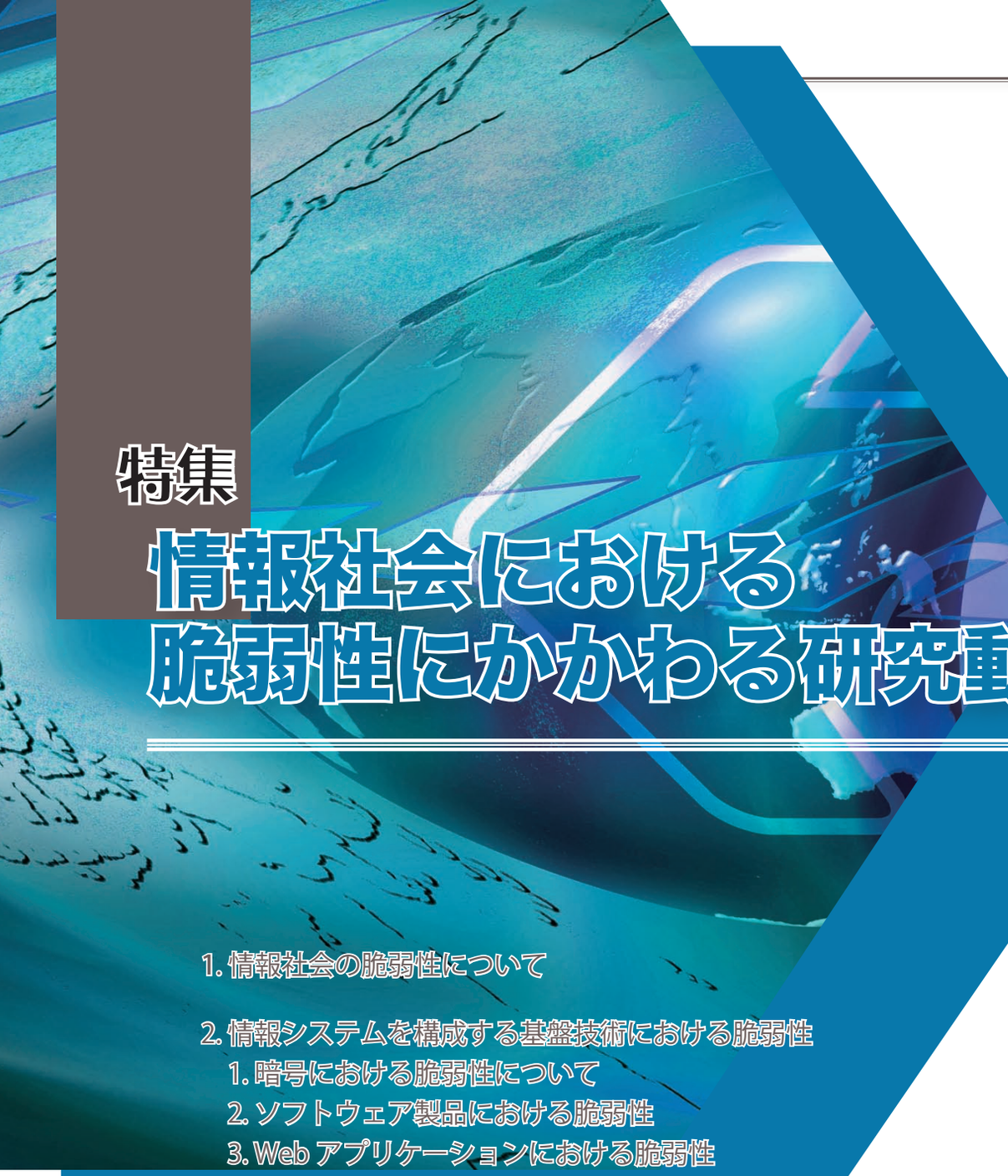

特集

情報社会における脆弱性にかかわる研究動向

1. 情報社会の脆弱性について

2. 情報システムを構成する基盤技術における脆弱性
   1. 暗号における脆弱性について
   2. ソフトウェア製品における脆弱性
   3. Web アプリケーションにおける脆弱性

3. 大規模なシステムにおける脆弱性
   1. DRM における脆弱性について
   2. 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

4. 脆弱性を克服するために
   1. 脆弱性にかかわる法的側面について
   2. 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―
   3. 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

編集にあたって

（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

世の中は，脆弱性に満ち溢れている．建造物には構造や材料にかかわる脆弱性が存在し地震に対して倒壊の可能性がある．活断層の存在は地震発生にかかわる大きな脆弱性である．さらには，報道によれば，自動車に脆弱性が発見され，日々リコールの対象となっている．小中学校の警備は，悪意ある犯罪に対してあまりにも脆弱である．

近年，情報技術の世界において注目を集めている脆弱性とは，インターネットの脆弱性に代表される情報セキュリティ上の問題を抱えるという意味での脆弱性である．OSやブラウザの脆弱性は頻繁に発見され，パッチと呼ばれる修正プログラムがインターネットを通じて配布されている．製品化されているソフトウェアだけではなく，オープンソースソフトウェアにかかわる脆弱性も頻繁に発見されている．また，バイオメトリクスデバイスの脆弱性，ICカードの脆弱性，携帯電話の脆弱性なども報告されている．

こうした事象が意味するところは，ソフトウェアにおいても，デバイスやハードウェアその他においても，製作段階での脆弱性の混入を防止することはきわめて困難であることである．そのため，脆弱性が発見された段階で，対策を講ずることが重要であるとの合意がなされている．この合意の下に，運用が開始された制度が，経済産業省告示に基づく情報セキュリティ早期警戒パートナーシップであり，独立行政法人情報処理推進機構，有限責任中間法人JPCERTコーディネーションセンター，製品開発者が一体となった取り組みを行っている．

ところで，脆弱性の対策を検討するにあたり，個々のソフトウェアやデバイス等の内部のみの脆弱性を扱うのみでは不十分であり，脆弱性の外部への影響度にかかわる情報を収集し，影響度を分析・可視化する技術が望まれている．防災分野においては，脆弱性の影響度の可視化技術は古くから積極的に研究されており，その多くは防災ハザードマップとして実用化されている．地震，津波などに関するハザードマップが，多くの自治体で作成されている．対して，情報システムの脆弱性の影響度の可視化は可能であろうか？　こうした問題意識の下，独立行政法人科学技術振興機構の傘下にある社会技術研究システムのミッション・プログラムIIでは，「高度情報社会の脆弱性の解明と解法の研究」をテーマに，情報システムのハザードマップ作成を進めている．

こうした脆弱性を取り巻く状況を俯瞰すべく，本特集を企画した．特集は，9つの記事からなる．

1つ目の記事では，「情報社会の脆弱性について」と題して，脆弱性の定義，さまざまな脆弱性の動向，対策の動向を概観している．2つ目の記事から4つ目の記事では，「情報システムを構成する基盤技術における脆弱性」をテーマにしている．2つ目の記事は，「暗号における脆弱性について」であり，暗号基盤の脆弱性について，暗号の危殆化を中心として，その定義・影響等について概要を示すとともに対策のあり方を解説している．3つ目の「ソフトウェア製品における脆弱性」においては，ソフトウェア製品における脆弱性の具体例，ソフトウェアにおける脆弱性の取り扱い方法，国際連携のあり方等について述べている．4つ目の「Webアプリケーションにおける脆弱性」では，Webアプリケーションの脆弱性の技術的概要，社会的問題点を踏まえつつ，対策にかかわる最先端の研究動向を述べている．5番目と6番目の記事は，「大規模なシステムにおける脆弱性」をテーマにしている．5番目の「DRMにおける脆弱性について」では，DRMの動向を踏まえた上で，DRMにおける技術的，社会的，法的な脆弱性を明らかにするとともに，対策の方向性を示している．6番目の「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」では，重要インフラ間の脆弱性を視覚化するハザードマップと，それと連動するコストモデルについて述べている．7番目から9番目の記事のテーマは，「脆弱性を克服するために」であり，脆弱性の対策にかかわるさまざまな問題を記述している．7番目の「脆弱性にかかわる法的側面について」では，情報社会の脆弱性に関しては，法的問題点の整理が重要であり，不正アクセス禁止法のみならず，電波法，不正競争防止法，民法，民事訴訟法等さまざまな観点での検討が必要であることを示している．8番目の「脆弱性情報の取り扱いについて」では，2004年7月に発足した情報セキュリティ早期警戒パートナーシップにおける脆弱性の考え方，取り扱い方法を概観している．最後の9番目の「脆弱性を解決するための多重リスクコミュニケータ」では，情報社会の脆弱性を，対話により解決するための仕組みである多重リスクコミュニケータを解説している．

本特集が情報社会および情報システムの脆弱性への興味と関心を呼び起こすことになれば幸いである．

なお，本特集の編集に際し，執筆者を始め関係者の方々には多大なるご協力をいただいた．特に，和田英一編集長と情報処理学会後路氏および綿谷氏には，記事の詳細個所までチェックをしていただいたとともに進捗に関して多大なるご心配をおかけした．この場を借りて深く感謝するとともに，ご心配をおかけしたことに対してお詫び申し上げたい．（平成17年5月18日）