## 2. 目指すべき国際健康危機管理における情報通信ネットワーク

### 1) 感染症

World Health Report (2004)によると、世界の主要死因は上位から、心循環器疾患 30%、感染症 26%、悪性腫瘍 12%、事故 9%、周産期異常 4%となっている（図 1)。また、感染症の内訳について見てみると、急性呼吸器感染症（Acute Respiratory Infection：ARI)、エイズ、下痢症、結核、マラリアと続く（表 1)。途上国に限定すると、死亡者の半数がこれらの感染症による死亡しているといわれており、感染症は現在最も人類の生命および健康を脅かす要因といえる。

新しい病原体による新興感染症、最近になり再び流行しはじめた再興感染症が、公衆衛生上の大きな問題になっている。今日では、国際交通網が整備され、地球規模で人や物が急速に移動するため、ある地域で発生した感染症が、ごく短時間で世界各国に拡大する危険性が増大している。これは 2003 年 Severe Acute Respiratory Syndrome（SARS；重症急性呼吸器症候群）が世界中に広がった原因の一つでもある。このように現代の感染症は発生地域・発生国だけの問題ではない。感染症早期制圧のためには国際社会が緊密な連携を図り、アウトブレイクから、いち早く正確な情報を収集し、共有し、迅速かつ適切な対策を立てることが重要となる。このような観点から、感染症発生の際に政府や関係研究者間などがリアルタイムに情報を収集・共有できるネットワーク基盤を構築・整備することが急務の課題である。

### 2) 求められているグローバル情報通信ネットワーク

感染症の発生予防、拡大防止等を行うためには、必要な情報をリアルタイムに収集・共有できるプラットフォームが必要となる。前述の厚生労働省の「健康危機管理」の定義を考慮すると、グローバル情報通信ネットワークには、世界規模で感染症に関わる情報を迅速に収集・共有し、その情報を活用した支援を安全かつ効率的に実施するためのプラットフォームを提供することが求められている。

また、グローバル情報通信ネットワークは、感染症の蔓延防止・予防のための一連のサイクルを管理するための基盤でもある。このサイクルは、図 2 に示すような step が想定される。

### 3) グローバル情報通信ネットワークのシステム構築に必要となる技術

図 3 は、図 2 の step 内容に基づいた、感染症の発生予防、拡大防止等のためのグローバル情報通信ネットワークのサブシステムのイメージと必要技術である。

以下に、構築の際に必要となる主な技術（1~5）と、対応する step を列挙する。ここに挙げる必要技術の番号は図 4 中の番号（1~5）と対応している。

1. 感染症の発生を早期に発見するためのセンシング技術（step1）
2. センシング情報の収集や関連情報の共有のための基盤システムの構築（step2、step3、step4）
3. 収集された情報を効率的に活用するための情報管理システム（step3、step5）
4. 感染症発生時の対処・支援内容決定、評価などの一連の活動を管理するイベント管理システム（step3、step4 、step5、step6）
5. システムを安全に運営するための高度なセキュリティ技術（step 全般）

## 3. WHO の動向

現在、WHO では感染症対策のための GOARN（Global Outbreak Alert & Response Network：国際感染症対策ネットワーク）が本格的に始動し、それをサポートするイベント管理システム（2nd GEMS※：Global Event Management System）の構築について検討中である。以下にその状況について紹介する。

### (1) GOARN

国際的な感染症対策の取り組みとして、WHO を中心に、世界的な集団発生事例に対する警戒と対応のためのネットワーク、GOARN（Global Outbreak Alert & Response Network：国際感染症対策ネットワーク）が運用されている。GOARN は、国際的に重要なアウトブレイクに対して、迅速な同定、確認、対応をするため、人材や技術的資源を有している機関やネットワークを連携させたものである。このネットワークは、国際社会に常時アウトブレイクの脅威を警告し、対応出来るようにするため、専門家と技術を繋げるための実行体制を提供している。GOARN は、2000 年 4 月ジュネーブ（スイス）で最初の会議が開かれ、SARS 発生時に初めて本格的に発動した。地球規模での流行サーベイランスのネットワーク、地球規模アウトブレイク警戒対策ネットワーク

① GOARN の目的

・アウトブレイクの国際的な広がりと闘う
・適切な技術協力が迅速に影響するよう確保する
・長期流行への準備と能力開発への貢献

②パートナー

メンバー国の科学機関、医学およびサーベイランス機関、地域の技術的なネットワーク、研究所のネットワーク、国連機関（UNICEF；国連児童基金、UNHCR；国連難民高等弁務官）、赤十字（赤十字国際委員会、国際赤十字社・赤新月社国際連盟）、国際人道的な非

※ 2nd GEMS：すでにある略語 GEMS(Great Explorations in Math and Science)と差別化するために仮につけられた名称であり、運用時には変更されている可能性がある。

政府組織（国境なき医師団、国際救済委員会など）

③国際的な原則

疫学、研究所、病院管理、研究、通信、ロジスティックス支援、セキュリティ、非難と連絡体系を標準化し、操作プロトコルを策定する。

GOARN のパートナーによって、現地レベルの努力を国際的に支援するためのコーディネイトをする。

④生物剤の意図的な使用への対応

検出、確認、流行の封じ込めを目的としたグローバル健康セキュリティの主な柱である。生物剤の意図的な放出に対して、これらの活動は効果的、国際的封じ込めのために不可欠であろう。

(2) GEMS

WHO が各国政府や研究機関から感染者や調査報告などの情報を収集すると同時に、重要情報を世界に向けて発信し、情報の共有を図るための情報サイトを提供している。WHO は GOARN を使って、国際的なアウトブレイク対応をコーディネイトする。また CSR（感染症調査・対策部）のパートとして、GOARN に対して事務サービスも行っている。

WHO では、GOARN を SARS 以外の新興・再興感染症やバイオテロの発生時にも活用する意向である。そのため、世界の主要研究機関をネットワークで結び、ウイルスの早期特定支援を行う等、様々な機能の導入を推進している。これに伴い、WHO では GOARN をさらに効果的に活用できるよう、新たなイベント管理システム（2nd GEMS※：Global Event Management System）の構築について検討中である。

① 2nd GEMS の目的

WHO の各国オフィスや関係研究者など、WHO と関係するパートナーの全てが協力し、感染症に関わる重要情報を更新、共有、評価するためのソフトウェアプラットフォームを提供する。

② メイン機能

a) すべての感染症に対して、発生検知から制圧、対処の評価にいたるまで一連の対応を体系的に支援する。

b) ユーザがそれぞれの感染症発生の動向を知ることができるようにする。

・自分の住む地域の安全性を地図情報として視覚的に確認できるようにする。

c) e-mail や文書処理等の通常業務の自動化を支援する。

d) 全情報フロー（意思決定過程、コスト管理等）を記録する。

③ システムの特徴

・リアルタイムに情報と警報を配信する（アウトブレイクと連絡先データベースに基づき e-メールを自動生成する等）。

---

※ 2nd GEMS：すでにある略語 GEMS(Great Explorations in Math and Science)と差別化するために仮につけられた名称であり、運用時には変更されている可能性がある。

・感染症発生情報を系統立てて生成し、維持管理する。
・WHO およびパートナー内でデータを交換する。また共有データや資料の管理とその所有権の移動を行う。
・社会、特殊ネットワーク、ワーキンググループ等様々な対象に対して体系的に情報を流す。
・WHO 加盟国、公衆衛生局、メディアおよび社会に対する情報を標準化する。
・フィールド配置（GOARN）のための人材データベースを備える。
・GOARN パートナーおよび各ワーキンググループへ共有ワークスペース・ウェブサイトを提供する（事前に確立しておくか、あるいは感染症発生の間短期的に作成する）。
・強化サーチエンジン（評価・分析プログラム）を備える。
・発生国など現地の在庫の管理をし、配置分布や購入過程を電子的に管理する。
・発生現地において、物資の要求および配達状況および資産の状況とその利用可能性を管理する。
・資料を電子ファイル化し、保管する。
・Health Mapper や Global Atlas 等、データ管理のため WHO が開発したマッピングツールを統合する。

このように、WHO では、2nd GEMS として、体系だった支援を行うためのプラットフォームを想定している。また、このシステムの実用化に向けて、大量データへの対策、アウトブレイク時の対応の標準化、利用者支援の充実も挙げられている。
a) 体系的な支援、b) ユーザ支援、c) 通常業務支援、d) 情報フロー管理、対応と危機管理計画。

## 4. まとめ

国際健康危機管理とは、健康危険情報を世界規模で収集し、共有し、迅速に対応することで、国際的な健康被害の発生予防や拡大防止等を図ることである。健康を脅かす主要因の感染症を早期に制圧するためには、国際社会が緊密な連携を図り、アウトブレイクから、いち早く正確な情報を収集し、共有し、迅速かつ適切な対策を立てることが重要である。そのため、国際的な健康危機管理ネットワークが必要である。本稿では、「WHO の動向」と「国際健康危機管理ネットワークの役割」について検証した。

なお、本調査論文は、厚生労働省の平成 16 年度厚生労働科学研究費補助金（国際健康危機管理ネットワーク強化研究推進事業）による「国際健康危機管理のための情報ネットワークのあり方に関する研究：主任研究員　喜多悦子」の一環である。

参考文献


[1] Shun-ichi Akazawa, "Present situations and security issues of WHO/HQ Strategic Operation Centre", An Information Consultation on the Establishment of a Network for Infectious Disease Surveillance and Health Risk Management – Focus on the Western Pacific Region, 9-10 February 2005.

[2] Ryo YAMAGUCHI, "Situation and issues of infectious diseases surveillance system and international health risk management in the Western Pacific Region", An Information Consultation on the Establishment of a Network for Infectious Disease Surveillance and Health Risk Management – Focus on the Western Pacific Region, 9-10 February 2005.

[3] Mami Furukubo, "Network and sensor for infectious disease prevention", International Symposium on Trends in Transmission Model for Infectious Diseases -2005 – Modeling Biology Focusing to Social Risk Assessment-, 15 February 2005.

[4] 竹内勤・中谷比呂樹[編著]、「グローバル時代の感染症」、慶應義塾大学出版会、2004年6月

[5] WHO GOARN 公式ホームページ http://www.who.int/csr/outbreaknetwork/en/

[6] 国立感染症研究所 感染症情報センター 公式ホームページ http://idsc.nih.go.jp/index-j.html

[7] 岡田晴恵・田代真人、「感染症とたたかう」―インフルエンザと SARS―、岩波出版、2003年12月

[8] 畑中正一、「キラーウイルスの逆襲」、日経BP社、2003年11月

[9] 橋本宗明・野村和博、「バイオチップの可能性」、日経バイオビジネス pp.40-53、2003年12月

[10] 三宅亮・稲波久雄・他、「医療・バイオ分野に向けた MEMS 技術」、日立評論 pp.67-70、2004年7月

[11] タカラバイオ　公式ホームページ http://www.takara-bio.co.jp/news/2004/07/14.htm

[12] 日系ネット http://it.nikkei.co.jp/it/utility/word.cfm?wordid=266

http://www.fukushihoken.metro.tokyo.jp/tthc/kikakuchousei/kikikanrikeikaku_an.pdf

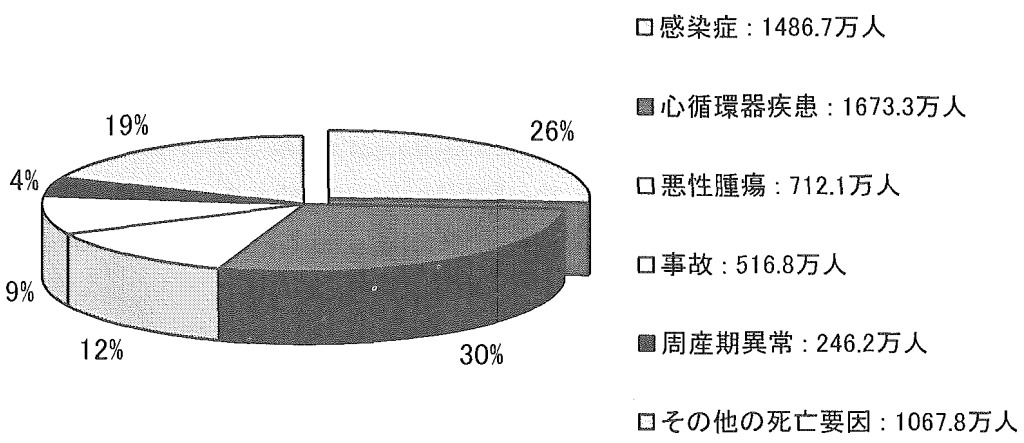


図１　世界の主要死因

資料：WHO, World Health Report 2004

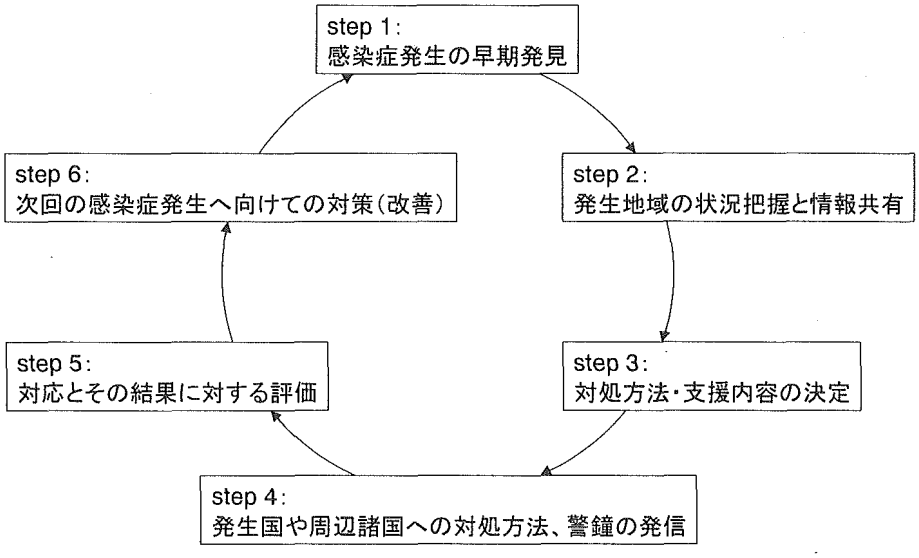


図2 感染症の蔓延防止・予防のための一連のサイクル

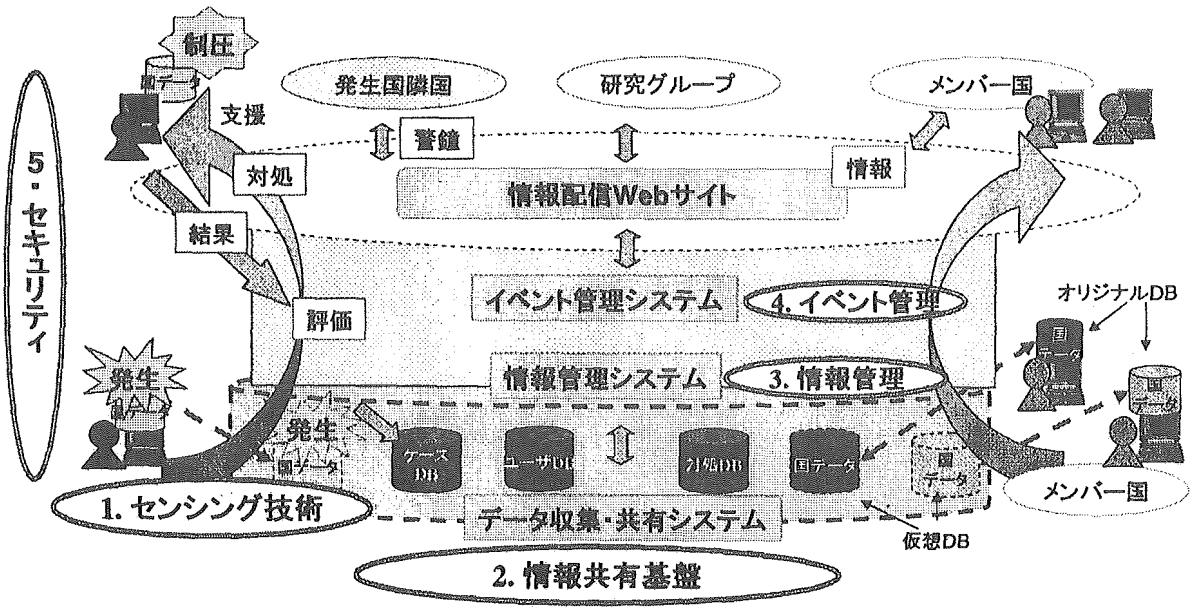


図 3　グローバル情報通信ネットワークシステムとサブシステムのイメージ

表 1　感染症の内訳（万人）

| | |
|---|---|
| 呼吸器感染症： | 396.3 |
| HIV/AIDS： | 277.7 |
| 下痢症： | 179.8 |
| 結核： | 156.6 |
| マラリア： | 127.2 |
| 小児期疾患： | 112.4 |
| 性感染症（HIV を除く）： | 18.0 |
| 髄膜炎： | 17.3 |
| B 型・C 型肝炎： | 15.7 |
| 熱帯病： | 12.9 |
| デング熱： | 1.9 |
| その他の感染症： | 170.9 |

# Strategic Approach to Information Security and Assurance in Health Research

Shunichi AKAZAWA, Manabu IGARASHI[1],

Hirofumi SAWA[2] and Hiko TAMASHIRO[1]

*Kyoto University Graduate School of Medicine &*

*World Health Organization (WHO) Headquarters*

[1]*Hokkaido University Graduate School of Medicine*

[2]*Hokkaido University Research Center for Zoonosis Control*

Reprint requests to: Hiko TAMASHIRO

Department of Health for Senior Citizens, Division of Preventive Medicine,

Social Medicine Cluster, Hokkaido University Graduate School of Medicine

North 15 West 7, Kita-ku,Sapporo 060-8638 Japan

Tel: (81) 11-706-5051, Fax: (81) 11-706-7374, E-mail: tamashiro@med.hokudai.ac.jp

**Running title:** Strategic Approach to Information Security

***Keywords:*** security and assurance, health research information, proactive measures, ISMS, CSO/CISO

**Abstract**

Information security and assurance is an increasingly critical issue in health research. Health research deals with information that is highly sensitive, be it genetic, new drugs, disease outbreaks, bio-chemical, or radiation effects, and could be targets by rogue individuals or groups, corporations, national intelligence agencies, or terrorists, looking for financial, social, or political gains. The advent of the Internet and advance in recent information technologies have also dramatically increased opportunities for attackers to exploit sensitive and valuable information, by leaps and bounds.

Government agencies have deployed legislative measures to protect privacy of health information, and developed information security guidelines for epidemiological studies. However, risks are grossly underestimated and little efforts have been made to strategically and comprehensively protect health research information by institutions, governments and international communities.

There is a need to enforce a set of proactive measures to protect health research information locally and globally. Such measures should be deployed at all levels, but will be successful only if research communities collaborate actively, governments

enforce appropriate legislative measures at national level, and international community develops quality standards, concluding treaties if necessary, at global level.

The best information security and assurance proactive measure would be through a rigorous management process with a cycle of "plan, do, check, and act". Each health research entity, such as hospitals, universities, institutions, or laboratory centers, should implement this cycle, and establish an authoritative security and assurance organization, program and plan coordinated by a designated *Chief Security Officer* who ensures implementation of the above process and putting appropriate security controls in place, with key focus areas such as *policies and best practices, enforcement and certification, risk assessment and audit, monitoring and incident response, awareness and training, and modern protection method and architecture.* Governments should enforce comprehensive scheme, and international health research communities should adopt standardized innovative methods and approaches.

**Risks involved in health research information**

Information security and assurance is an increasingly critical issue in health research. Health research deals with information that is highly sensitive, be it health care record of individuals/populations, genetic epidemiology, disease outbreak information of nations, or data on new drugs/bio-chemicals. They are targets by rogue individuals or groups, corporations, national intelligence agency, or terrorists, looking for financial, social, or political gains. Insurance companies are eager to discover detailed medical history of their customers and families to define most cost effective insurance premium. Corporations could recruit new staff, decide assignments, or select future executives, based on genetic profile of employees. Early disease outbreak news has extremely advantageous value to stock exchange traders and speculators, whereas terrorists and intelligence agencies may have political agenda to interfere with early outbreak alert and response operations. Or a mere unwarranted disclosure of outbreak information could have profound impact on the economy of nations who depend on tourism. Web sites posted by health scientists describing impact of new deadly bio-chemical or radiation material could be a textbook for terrorists.

The advent of the Internet and advance in recent information technologies have revolutionalized the way health research is conducted, and have made it extremely

efficient to collect, store, exchange and process vast amount of scientific information, yet have dramatically increased opportunities for attackers to exploit sensitive and valuable information to their ends through sophisticated but rogue technological means, by leaps and bounds. To make matters worse, research scientists tend to pay little attention to security of their data. Laboratory systems are much less protected compared to operation systems.

**Current countermeasures and their problems**

Some government agencies have deployed legislative measures to protect privacy of health information, especially in the health care sector, and developed standard information security guidelines for epidemiological studies. However, the risks are grossly underestimated and little efforts have been made to strategically and comprehensively protect the health research information of universities, hospitals, institutions, government agencies, and international communities, through adequate security management process. There are hardly any health research centers in the world today, except those dealing with highly confidential military intelligence or counter-terrorism health data, for example, where authoritative information security program has been established and implemented. Not to mention that these centers lacks institutionalized information security risk assessment process. They have, simply, no

idea what critical assets are there to protect, from who and why, when it comes to health research information.

There is a need to promote and enforce set of proactive measures to strategically and comprehensively protect health research information both locally and globally. Such measures should be deployed at all levels, but will be successful only if research communities collaborate actively, supporting governments enforce legislative measures at national level, and international community develops quality standards, concluding treaty if necessary, at global level. The international collaboration is necessary particularly to address security issues involved in unprecedented free flows of, and easy access to, scientific information across the Internet.

**Strategic approach**

The best proactive measure would be through a rigorous security management process where a cycle of "plan, do, check, and act" is enforced (Figure 1). The approach described is based on the British Standard Institute's BS7799-2:2002[1], to be superseded by International Standard Organization's ISO/IEC27001. (ISO/IEC27001 Information Security Management System (ISMS), could be considered as one of key quality assurance standards along with ISO9001 for Quality Management System

(QMS), ISO14001 for Environment Management System (EMS), and OHSAS18001 for Health and Safety Management System (HSMS).)

The ISMS cycle consists of: the PLAN phase, where the ISMS scope is defined, ISMS policy is developed, risk assessment is conducted, risk management/risk treatment strategy is determined, security objectives and controls are selected, and selected controls are justified against risk assessment (i.e. statement of applicability (SOA)); the DO phase, where preventive plans are implemented, security controls are actually operated, security incidents are to be promptly detected and responded; the CHECK phase, where check are made to ensure that security controls are firmly in place and are achieving goals, residual risk levels are reviewed, security processes are reviewed, metrics for evaluation are determined, monitoring and response capacity is checked, learning from others, such as CERT/CC[2], is done, ISMS audit is conducted, and management review is executed; and the ACT phase, where actions are taken to correct, prevent and improve (e.g. improvement of security processes, refinement of risk mitigation plans, development of new policies and refinement of existing policies, and design and implementation of new security controls).

Each health research entity, such as hospitals, universities, institutions, or laboratory centers, should implement this ISMS cycle, and establish an authoritative

security and assurance management organization. Such an organization should be headed by a *Chief Security Officer* (CSO), or a *Chief Information Security Officer* (CISO), who takes charge of all information security and assurance issues and develops a security plan, coordinating security program, ensuring implementation of ISMS process and manage/coordinate appropriate security controls, with key focus areas such as: *policies and best practices, enforcement and certification, risk assessment and audit, monitoring and incident response, awareness and training, and modern protection method and architecture*[4]. These six areas are particularly important because:

**Policy and best practices**: Policy describes exact rules and steps to be followed in order to improve the security, whereas best practices are the behaviors which are considered to be effective by most industries, public and experts, and followed often without formal assessment. Since security is not an exact science, both are needed.

**Enforcement and certification**: Policies and best practices are not effective unless they are enforced. Certification is to accredit officially and authoritatively compliance to policies, and is one of most effective methods of enforcement.

**Risk assessment and audit**: Risk is a multitude of [asset value] x [threat likelihood] x [threat impact] x [vulnerability], where critical assets could be tangible assets such as infrastructure - hardware and software, people, data, knowledge and services, or intangible assets such as privacy, reputation, credibility and absence of legal liability. Risks are moving targets, which change in time. Risk assessment is a key to understanding current state of security at an organization, and should be conducted regularly. Audit verifies successful implementation of security control.

**Monitoring and incident response**: In security, prevention, detection, and response are all necessary. Most of information security is preventive in nature, which is a countermeasure to provide two things: a) barrier to over come and b) time to overcome the barrier. Without detection and response, however, the preventive countermeasure is much less effective. In security, detection and response are often more effective, and more cost effective than more prevention.

**Awareness and training**: In security, "awareness and training" is critically important. After all, security is people's problem, or it is said that 70% of security problem is attributed to human (people, process, and politics & culture). Without security conscious and educated staff, much of security measures, or security technology, could be useless. Social engineering and taking advantage of human

errors/negligence, continues to be one of most effective attacks against information networks.

**Modern protection method and architecture**: Although it is said that only 30% of security problem is related to technology, that 30% could still be significant. Choices and adoption of appropriate modern and innovative protection technology methods and architecture, based on international and industry "best practices" and standards, could improve security substantially.

Only through such an authoritative and comprehensive program, could the information security and assurance of highly sensitive health research information be systematically and successfully protected from increasing threats and risks in the modern world.

What is vital is that in order to ensure that this strategic approach prevails, governments should enforce the scheme throughout all its agencies, and international health research communities should conclude a formal agreement to adopt standard methods and approaches. There already exist in the world a vast amount of scientific health research information not properly protected and in danger, and we must take action promptly to prevent them from misuse, modification, loss/destruction, or unwarranted disclosure.

The e-Health is becoming prevalent around the world, from highly sophisticated hospital information systems to Internet health portals, to telemedicine helping poorest countries or regions. Information security and assurance issues should seriously be addressed in e-Health[5]. There are emerging communication applications on the Internet such as networked virtual offices for scientists to collaborate globally, ubiquitous RFID-based sensors to collect health data over wide area, internationally federated identity management systems between collaborating research centers, and unimaginably powerful search engines which provide keys to almost any information people, or terrorists, are looking for. These new applications and tremendous depository of digital information being accumulated and processed will force us to take coordinated effort to push for strategic approach to protecting health research information on a global scale.

## Conclusion

This paper proposes a formal and comprehensive approach to protection of the security and assurance of health research information. The health research information has high level of security requirements for: 1) confidentiality, 2) business continuity, 3) integrity, 4) quality, 5) availability, 6) authenticity, 7) accountability, 8) confidence, 9) credibility, and 10) absence of legal liability.

We believe that the approach described herein addresses collectively these issues and requirements, and facilitate a step forward toward a proactive global security process for the health research community.

## References


1. British Standard Institute: BS7799-2:2002 Information Security Management Systems – Specification with Guidance for Use, ISBN 0-580-40250-9: September 2002 (To be superseded by ISO/IEC27001, November 2005).

2. Carnegie Mellon University Software Engineering Institute, Computer Emergency Response Team/Coordination Center (CERT/CC): Available at URL: http://www.cert.org/

3. International Standard Institute: ISO/IEC17799: 2005: Information Technology - Code of Practices for Information Security Management: 2005.

4. World Health Organization: WHO Global Information Security Policy and Implementing Guidelines: 2005.

5. Akazawa, Y and Akazawa, S: WHO Strategy on 'e-Health' (and Information Security), Global Burdon of Impaired Glucose Tolerance – Present and Future Strategy, Nihon Rinsho. 2005; 63(S2): 600-2.