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.

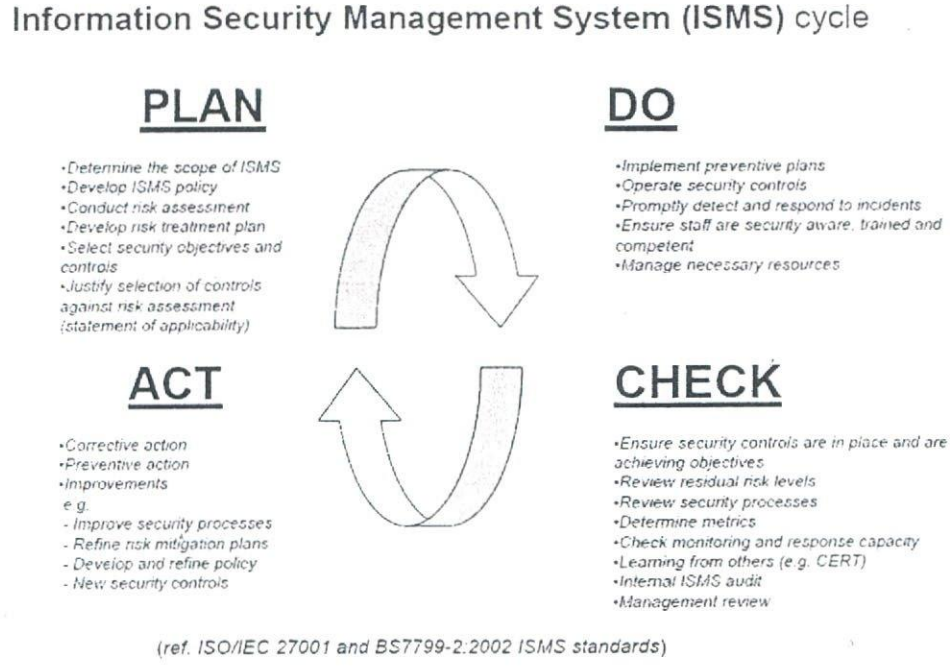
5. Akazawa, Y and Akazawa, S: WHO Strategy on 'e-Health' (and Information Security), Global Burdon of Impaired Glucose Tolerance – Present and Future Strategy, Nihon Rinsho. 2005; 63(S2): 600-2.

Special note from authors:

This paper solely reflects the views of the authors. It does not necessarily reflect the "official" views of the organization, WHO, or institutions they belong.

Figure 1

Information Security Management System (ISMS) Cycle



(ref. ISO/IEC 27001 and BS7799-2:2002 ISMS standards)

Note: Information Security Controls and Best Practices are categorized by ISO/IEC17799:2005[3] as: 1) security policy, 2) organization of information security, 3) asset management, 4) human resources security, 5) physical and environmental security, 6) communications and operations management, 7) access control, 8) information systems acquisition, development and maintenance, 9) information security incident management, 10) business continuity management, and 11) compliance.

Security control measures would include: 1) governance, technical and end-user policies; standards and reference architecture, 2) auditing and compliance assessment, certification, 3) vulnerability management, anti-malware (virus, worms, Trojan horses, SPASMS, spyware) systems, 4) access-control enforcement (firewalls/IPS (intrusion prevention systems), authentication, authorization, accounting systems, etc.), 5) monitoring, surveillance and response, incident response teams, and 6) awareness and training programs.

JOURNAL OF VIROLOGY, July 2004, p. 7270–7273
0022-538X/04/$08.00+0 DOI: 10.1128/JVI.78.13.7270–7273.2004

Vol. 78, No. 13

Inhibition of Virus Production in JC Virus-Infected Cells by Postinfection RNA Interference

Yasuko Orba,[1,2] Hirofumi Sawa,[1,2,3]* Hiroshi Iwata,[1,2] Shinya Tanaka,[1,2] and Kazuo Nagashima[1,2]

Laboratory of Molecular and Cellular Pathology[1] and 21st Century COE Program for Zoonosis Control,[3] Hokkaido University Graduate School of Medicine, Kita-ku, Sapporo 060-8638, and CREST, JST, Sapporo,[2] Japan

Received 25 February 2004/Accepted 30 March 2004

RNA interference has been applied for the prevention of virus infections in mammalian cells but has not succeeded in eliminating infections from already infected cells. We now show that the transfection of JC virus-infected SVG-A human glial cells with small interfering RNAs that target late viral proteins, including agnoprotein and VP1, results in a marked inhibition both of viral protein expression and of virus production. RNA interference directed against JC virus genes may thus provide a basis for the development of new strategies to control infections with this polyomavirus.

JC virus (JCV) belongs to the polyomavirus family of double-stranded DNA viruses and causes progressive multifocal leukoencephalopathy (PML) in humans (23). PML is often observed in immunosuppressed individuals, such as those with AIDS or advanced malignancies. Although highly active antiretroviral therapy, which includes treatment with protease inhibitors, improves the survival rate of patients with AIDS-related PML (2, 7), current therapeutic approaches to PML are not satisfactory. Treatment with cytosine arabinoside (8) or cidofovir (15) has failed to prove efficacious in individuals with PML. Trials of topotecan, which inhibits DNA topoisomerase and blocks JCV replication in vitro (11), are currently under way in such individuals. RNA interference (RNAi) with small interfering RNAs (siRNAs) has recently become a widely used approach for repressing cellular or viral gene expression (5, 6, 10, 16). Although several studies have shown that virus infections can be prevented by a prior or concomitant administration of siRNAs, the elimination of established infections from cells or tissues by RNAi has not been demonstrated (1).

To attempt to inhibit JCV production in infected cells, we designed the following siRNAs (Dharmacon) to target three different JCV proteins (Fig. 1a): VP274 and VP691 for VP1, Ag122 and Ag147 for agnoprotein, and LT78 and LT134 for the large T antigen (T-Ag). The JCV early and late RNAs are generated by alternative splicing. The early RNAs encode T-Ag and the small t antigen (14), whereas the major late RNA encodes both agnoprotein and VP1 (21). We introduced the JCV-specific siRNAs into cells of the SVG-A (simian virus 40 [SV40]-transformed human fetal glial cells) line (13) that had been inoculated with JCV (Mad-1/SVEΔ strain; 1,024 hemagglutination activity units per 3×10^5 cells) 4 days previously. JCV late proteins, including VP1 and agnoprotein, were detected by an immunoblot analysis at 2 days postinfection (dpi) and were abundant at 4 dpi (Fig. 1b). At 4 and 6 dpi, each siRNA (120 pmol per 6×10^4 cells) was introduced individually into SVG-A cells by the use of Lipofectamine 2000 (Invitrogen) (Fig. 1c). About 80% of the SVG-A cells were successfully transfected with a fluorescein-conjugated Ag122 siRNA (data not shown). The abundance of JCV proteins in siRNA-transfected cells was examined 48 h after the second transfection by an immunoblot analysis with antibodies specific for agnoprotein (3, 18, 19), VP1 (12, 22), or SV40 T-Ag (Ab-2; Oncogene Research Products) (20). Cells transfected with Ag122, Ag147, or VP274 manifested a marked depletion of viral proteins compared with cells transfected with a control siRNA with a scrambled sequence which is not present in mammalian cells (Dharmacon) (Fig. 1d). Ag122 inhibited the expression of VP1 as well as that of agnoprotein in a dose-dependent manner, but it did not affect the abundance of T-Ag, lamin A/C, or actin (Fig. 1d and e). The antibodies to SV40 T-Ag did not allow for differentiation between JCV T-Ag and SV40 T-Ag in SV40-transformed cells, as these two proteins share >70% amino acid sequence identity (4). We therefore assessed the effects of LT78 and LT134 on JCV T-Ag expression by reverse transcription (RT) and PCR; the abundance of JCV T-Ag mRNA was not affected by the transfection of cells with either siRNA (data not shown).

We also examined the effects of Ag122 and VP274 siRNAs by an indirect immunofluorescence analysis in JCV-infected cells. At 48 h posttransfection, methanol-fixed cells were stained with antibodies to VP1 or agnoprotein and then with Alexa Fluor 488-conjugated goat antibodies to rabbit immunoglobulin G (Molecular Probes). Cells positive for VP1 or agnoprotein were visualized with a laser-scanning confocal microscope (Olympus) and counted in six fields of view. The proportion of agnoprotein-positive cells was significantly reduced for cells transfected with Ag122, VP274, or both siRNAs compared with the value for cells transfected with the scrambled siRNA (Fig. 2a). Similarly, the percentage of VP1-positive cells was also reduced by transfection with Ag122, VP274, or both Ag122 and VP274. We confirmed the inhibition of the expression of agnoprotein and VP1 in cells transfected with

* Corresponding author. Mailing address: Laboratory of Molecular and Cellular Pathology, Hokkaido University School of Medicine, N15, W7, Kita-ku, Sapporo 060-8638, Japan. Phone: 81-11-706-5053. Fax: 81-11-706-7806. E-mail: h-sawa@patho2.med.hokudai.ac.jp.

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

初年度　日本人研究者の外国派遣事業成果

(様式11)

外国への日本人研究者派遣事業

研究実績報告書

1. 派遣研究者

所属・職名 ： 国立感染症研究所感染症情報センター研究員

氏　　名 ： 新井 智

2. 研究に従事した派遣先の機関

名　　称　(和文)：ハワイ大学 John A. Burns 医学部 太平洋新興感染症センター

(英文)：Pacific Center for Emerging Infectious Diseases Research, John A. Burns School of Medicine, University of Hawaii at Manoa

所 在 地　(和文)：米国ハワイ州、ホノルル

(英文)：Honolulu, Hawaii, USA

3. 研究に従事した派遣先の研究指導者

所 属 機 関 (和文)：ハワイ大学 John A. Burns 医学部 太平洋新興感染症センター

(英文)：Pacific Center for Emerging Infectious Diseases Research, John A. Burns School of Medicine, University of Hawaii at Manoa

職名・氏名　(和文)：リチャード ヤナギハラ(教授)

(英文)：Richard Yanagihara, Director

4. 派 遣 期 間 ： 平成17年4月1日～平成17年9月18日

5. 研究課題　： 多国間に拡大したアウトブレイク発生時の対策と情報ネットワークに関する研究

6. 研究活動の概要(目的、活動内容を具体的に)

目的

平成17年3月からの研究を継続して発展させた。遠隔地とのネットワーク会議システムや、ハワイ州が進めているウエストナイルウイルスに対する取り組み、またデングウイルス対策として一般市民や総合的な対策として進めている取り組みの情報収集と解析を目的とした。また、 ハワイ州は、米国本土から離れていることから、その対応は国際的な感染症ネットワークにおける日本の役割の非常に良いモデルとなっており、ハワイにおけるシステムやネットワークだけでなく、基礎研究分野や疫学分野の研究者のネットワークの解析が非常に重要である。更に、米国ハワイ大学、太平洋新興感染症センターでは、新興感染症の野外調査や基礎研究だけでなくワクチンの効果やサーベイランスの効果について総合的に研究し、しかも地域の感染症対策の要となる、ハワイ州保健所とも協力体制を

確立し、相互に協力体制を進めているため、これらの取り組み状況を調査し、これらのネットワークへの参加の可能性を探った。事例ごとに重要な役割を果たしてきた研究者それぞれの個人的なネットワークを解析し、国際的に開かれたネットワークとして確立することが可能かどうかについても情報収集を進めることを目的とした。

活動内容

① 米国ハワイ州でのウエストナイルウイルスにおけるサーベイランス体制の評価と今後の対策について検討した。ハワイ州は、米国本土から約 4000 キロ離れている 100 島を超える島々で、これまでウエストナイルウイルスの侵入は明らかないなってない。しかしながら、ハワイ州は毎日 3 隻以上のコンテナ船舶と、60 機以上の航空機が米国本土から来ている。更に渡り鳥の渡りルートも確認されている。そのため、ハワイ州のサーベイランス体制やその評価は今後の日本にとって貴重な情報である。ハワイ州保健所では、現在までのところ、空港周辺および、特定地域の蚊を対象とした蚊のサーベイランス、ヒトの血清抗体保有状況調査、ウマの血清抗体保有調査、死亡鳥を対象とした死亡鳥サーベイランスと複数のサーベイランスを実施している。現在までに実施しているサーベイランスの実施状況の把握とその評価に重点を置いて検討を進めた。また、ハワイ大学やハワイ州保健所、民間企業の Hawaii Biotech 社など複数の研究機関で共同で開発を進めているウエストナイルウイルスワクチンの開発状況についても情報収集とその利用法に関する検討を進めた。

② これまでに得られている知見だけでなく、新たに確認された知見のサーベイランスへの応用を検討した。これまでウエストナイルウイルスのサーベイランスの検討では、血清抗体価の上昇を基にした血清サーベイランスや、患者発生を把握する患者サーベイランスが進められてきた。しかしながら、ウエストナイルウイルスに感染したにもかかわらず十分な抗体価の上昇が認められない患者や、急性期と回復期の二点での抗体価の上昇有無を確認できない患者など、感染は疑われるものの実際に感染したかどうか疑わしい症例も多く、実際の感染率を明らかにすることができない場合も少なくない。しかし最近我々のグループはウエストナイルウイルスに感染した患者の尿から感染後 100 日を越えてウイルスゲノムを PCR で確認することに成功した。この結果を患者発生の検索やサーベイランスに応用可能か検討した。

③ 複数の国にまたがって発生し、更に拡大を続ける感染症の対策とサーベイランスの検討を進めた。蚊媒介性ウイルスの一つであるデングウイルスは、1970 年ごろは中南米やアフリカ地域では、1 型および 2 型のみの発生であったが、その後ウイルスが拡大し、現在では、赤道付近のほとんどの国でデングウイルス 1 型から 4 型までの発生が報告されている。この様な拡大しつつある感染症の対策について、過去に発生したアウトブレイクでの疫学調査および研究室診断の取り組みに着目してその対策について検討した。具体的には、プエルトリコでのデングウイルス4型の流行を題材に流行発生とそのウイルスタイプのダイナミックな変化の関連について検討した。プエルトリコでは1986年から毎年夏季にデングウイルスの流行が確認されており、1994年から19

95年の流行では確認されているだけで20000例以上の感染が確認されている。この時のウイルス遺伝子性状を他の年に流行したデングウイルス流行株と比較し、多様性の大きなゲノム領域を明らかにし、今後のサーベイランスやウイルス多様性の比較対象部位の決定や、その結果と集団における病原性の関係を解析した。

④ 新しいワクチンの開発とワクチン開発のネットワークへの参加の可能性について検討した。デングウイルス感染症はウイルス感染であるため、その対策として最も有効な対策はワクチンの開発である。しかしながら、デングウイルスには少なくとも4種類以上の血清型が報告されており、ワクチンを用いた場合、4種類全てのウイルスに対して有効なワクチンが必要であるものの、全てのウイルスに対して均等に効果のあるワクチンを開発するのが極めて難しく、現在までヒト用のワクチンは開発されていない。遺伝子組み換え技術を応用し、ウイルスゲノム上の病原性に関与する部位を決定し、組み換えウイルスを作成してより安全で、有効性の高いワクチン株の選出が進められ、現在までに複数のワクチン候補株が提案されている。我々のグループでは、5年以上前からワクチン開発に尽力し、東南アジア地域でこれらの複数のワクチン候補を用いてフィールドトライアルを進めている。これらフィールドや実験室で得られたデータを基に遺伝子組み換え技術を用いたワクチンの有用性について検討した。ワクチン候補の一つは、デングウイルスと黄熱病ウイルスの遺伝子組み換えワクチン株を用いている、黄熱病ウイルスベースの遺伝子組み換えデングウイルス生ワクチン、デングウイルスの病原性に関与していると考えられている 3 'end 非翻訳領域の約 30bp を欠損させたデングウイルスを用いたΔ30rDEV、Δ30rDEV のうち比較的に病原性が低いと考えられている 4 型をベースにした遺伝子組み換え弱毒デングウイルス株を用いたΔ30rDEV4 である。これらの組み換えウイルス株のうち、ΔrDEV4 株を用いたワクチンについて現在進めている単身のフィールドトライアル、4 種混合ワクチンについてのフィールドトライアルなど複数の臨床レベルでの検討について情報収集とネットワークへの参加の可能性を検討した。臨床研究は、現在から今後少なくとも 5 年程度継続して実施される必要があるため、今回の派遣期間だけでなく、これらの臨床研究やネットワークに参加できるよう継続した関係が確立できるかについても検討した。

⑤ 米国のような先進国で発生した侵入感染症を原因としたアウトブレイク発生時のサーベイランスと情報ネットワークの構築方法の解析を行った。具体的には、米国ハワイ大学が導入、使用しているビデオ会議システム「Click to Meet」を用いたリアルタイム情報共有システムの評価を行った。このシステムは、マイクロソフト社が提供している MSN messenger に非常に似通ったシステムで、マイクロソフト社の Windows でも、アップルコンピューター社のマッキントッシュでも使用することが可能である。実際にこのシステムを用いて複数地点との情報共有を行い。その有用性について検討した。

これら実験で得られた情報と疫学情報の共有や、その評価に加え、実際に実験室での研究に参加しつつ、国際的な大規模アウトブレイク発生時の実験室を基本としたサーベイランスと積極的疫学調査およびこれらの情報の共有における問題点と情報ネットワークの効果の解析を目標

に研究者個人のネットワークへの参加と開かれたネットワークへの発展性について検討した。

7. 派遣事業の成果

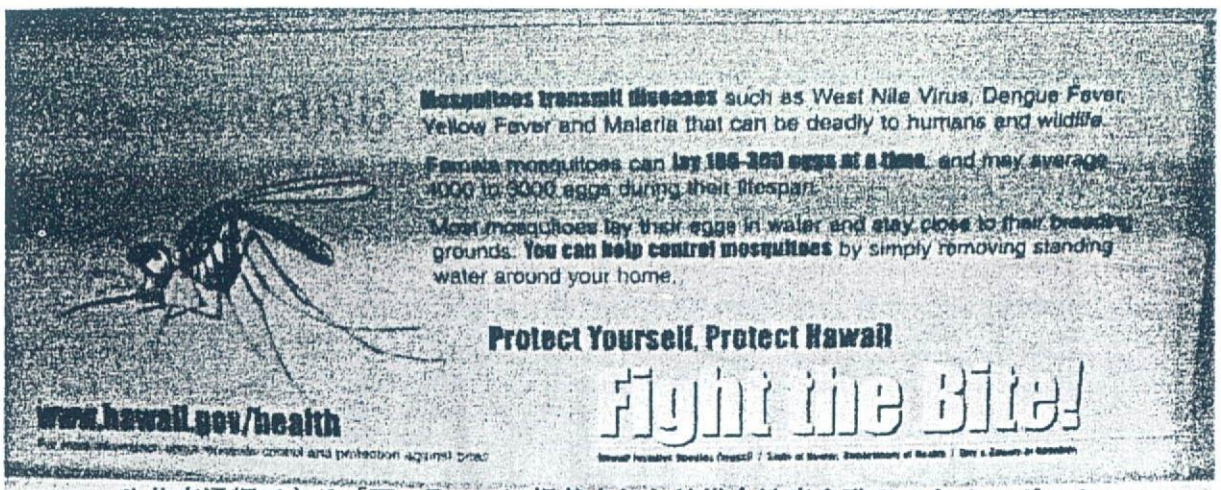
サーベイランスシステムについては、ハワイ州で実施しているウエストナイルウイルスサーベイランスについて情報を入手することができた。ハワイ州にはウエストナイルウイルスを媒介する蚊の生息が確認されており、常にウエストナイルウイルスの侵入の危険にさらされている。この様な状況の中でハワイ州では、次のようなサーベイランスを実施していた。一つ目は、空港周辺を含めた複数地点での蚊のサーベイランスである。これは、トラップを用いて蚊を収集し、RT-PCR を用いてウイルス感染の有無を調べるものである。日本でも空港周辺の蚊のサーベイランスが実施されているが、日本では主に形態学的な違いによって蚊の分類を実施している。一方ハワイ州では、Real time PCR を用いて蚊の 18S rRNA 遺伝子を調べることで迅速に蚊の分類を行い、より少人数でしかもシステマニックに実施できるよう検討が加えられていた。また、死亡鳥を対象にしたサーベイランスとして、一般市民に対し dead bird hotline を設定して、死亡鳥を収集しサーベイランス対象としていた。ここでも短縮ダイヤルを用いてより簡便に、しかもより多くの市民に認知されるよう配慮されていた。ヒトを対象とした血清サーベイランス、ウマを対象とした血清サーベイランスでは、偽陽性率を低下させ、感度の向上と正確性の向上を目指してキャプチャーELISA システムを用いて行っていた。キャプチャーELISA を用いることで、特異性を確保しながら感度の向上を進めることができていた。現在、これらのサーベイランスを継続して実施しているものの、ウマ、ヒト、鳥においてこれまでのところ明らかな陽性例は認められていない。今後継続してサーベイランスを実施されていく予定である。これらの情報を継続して共有できるシステムの可能性が得られた。

サーベイランスだけでなく、サーベイランスへ応用できる可能性のある事象の検索も進めた。ウエストナイルウイルスは通常、ヒトを代表とする脊椎動物に対して持続感染しない。しかしながら、患者の中には、感染・回復後も尿中にウイルスゲノムが検出される患者が認められた。ウエストナイルウイルス感染の確認された患者から継時的に尿を採取し、ウイルスゲノムの検出を試みた。その結果、感染後 100 日を越えてウエストナイルウイルスゲノム RNA が患者の尿中に排出されている事実が明らかになった。これは、感染形態によってはウエストナイルウイルスが宿主に持続感染する可能性があることを示しており、ウイルス感染環を理解する上での貴重な情報であると共に、血清抗体の十分な上昇の認められないような患者の確定診断の補助資料とできる可能性が得られた。しかしながら、尿中ウイルスゲノム RNA は患者全てに認められるわけではなく、ゲノム RNA が RT-PCR で確認されるものの、ウイルスは分離できず、ウイルス量としては極めて微量であった。このメカニズムは、ウエストナイルウイルスの越冬メカニズムとも関連しており、まだ明らかになっていない日本脳炎ウイルスの越冬メカニズムとも関連していることが予想される。そのため、終末宿主であるヒトよりも自然宿主の鳥での持続感染の解析が必要である。今後は、自然宿主である鳥での持続感染の詳細な解析を進める予定である。

一方、予防方法に関する情報の共有も進めることができた。これはハワイ州に拠点を置いている、Hawaii Biotech 社と複数の研究機関の共同で進められているウエストナイルウイルスに

対するワクチン開発に関するものである。Hawaii Biotech 社のグループが進めているウエストナイルウイルスワクチンは、ウエストナイルウイルスの構造蛋白質である preM および Envelop の約 80%を用いたサブユニットワクチンで、現在、動物実験での効果判定と今後のフィールドトライアルに向けての体制作りを進めている。このワクチンを接種したゴールデンハムスターは、ワクチン接種後 6 ヶ月たっても、ウエストナイルウイルス感染を 100%予防することが明らかになった。対象群では、約 53%の個体が死亡したのに対し、ワクチン接種群では 100%が生存し臨床学的な症状も認められなかった。現在は、このワクチンの鳥への接種実験が進められている。鳥は、ウエストナイルウイルスの主な自然宿主であるため、これらの動物を完全に免疫することが可能であればそのウイルス感染環を阻止することも可能である。もちろん、野生動物である鳥類を完全に免疫することには困難が伴い、現実的ではないが、ハワイ州では、過去に外来動物の持ち込みや侵入により生態系の大きな変化を経験しているため、ワクチンによる鳥類への免疫は、生態系保護の一つの方法として検討されている。今後これら生態系への効果だけでなくヒトへの接種に向けて臨床データの蓄積が進められ、ヒトへのフィールドトライアルも含めて検討が進められる予定である。

ハワイ州での蚊媒介性疾患の公衆衛生学的な対応としては、2001-2002 年のデングウイルスの事例を教訓に、一般市民に向けて継続した啓発活動を続けている。本年 7 月初めには、蚊に対する注意喚起としてポスターを公共交通網である「The Bus」に掲載した。幸い、2001-2002 年のアウトブレイク以来ハワイ州でのデング熱の発生は確認されていないため、これらの啓発運動がどの程度効果を得られているか評価することはできていない。しかし、デングウイルスやウエストナイルウイルスを媒介する蚊の生息は明らかであり、今後も 2001-2002 年の事例のような輸入例を発端とする集団発生の発生リスクがあり、継続した対応を実施していく必要性が示されている。日本もハワイ州と同様で、ウエストナイルウイルスの媒介蚊が存在している。実験室診断の開発に加え、一般市民に向けた蚊媒介性疾患に対する継続した啓発運動が必要であると示唆された。



公共交通網である「The Bus」に掲載された蚊媒介性疾患啓発のためのポスター

多国間に拡大する感染症の解析では、プエルトリコでのデングウイルスのアウトブレイクを解析し、それぞれの年の流行株の塩基配列と流行の関係に着目し、ウイルスの多様性および集