Contents

Page

Introduction

Organizations of all kinds are increasingly concerned with achieving and demonstrating robust biosafety and biosecurity practices controlling their biorisks consistent with their own biorisk policy and objectives. They do so in the context of increasing concern expressed by a variety of stakeholders and, in many countries, by a regulatory system that is becoming increasingly stringent.

Many organizations have undertaken biorisk "reviews" or "audits" to assess their biorisk performance. On their own, however, these "reviews" and "audits" may not be sufficient to provide an organization with the assurance that its performance not only meets, but also will continue to meet, its legal and policy requirements. To be effective, they need to be conducted within a structured systematic approach integrated throughout the organization.

CWA 15793:2008 specifies requirements for a biorisk management system that will enable an organization to develop and implement a biorisk policy, establish objectives and processes to achieve the policy commitments and improve its performance. It follows a risk based approach taking in legal requirements and current knowledge and is intended to apply to all types and sizes of organizations and to accommodate diverse geographical, cultural and social conditions. The success of the system depends on commitment from all levels and functions within the organization, and especially from top management. The overall aim of CWA 15793:2008 is to support and promote good biorisk practices, including self regulation.

This guidance is in the form of notes in association with the pertaining requirements clause and uses the terms "should" (recommendation), "may" (allowance) and "can" (possibility). Organizations wishing to implement this CWA 15793:2008 would be expected to consider all recommendations where the term "should" is used.

The management system approach enables an organization to effectively identify, monitor and control the laboratory biosafety and biosecurity aspects of its activities.

An effective management system approach should be built on the concept of continual improvement through a cycle of planning, implementing, reviewing and improving the processes and actions that an organization undertakes to meet goals. This is known as the PDCA (Plan-Do-Check-Act) principle:

Plan: Planning, including identification of hazard and risk and establishing goals,

Do: Implementing, including training and operational issues,

Check: Checking, including monitoring and corrective action,

Act: Reviewing, including process innovation and acting to make needed changes to the management system.

This document was written as a guide to the CWA 15793:2008 Laboratory biorisk management standard, wich aims to support organizations and biosafety professionals to implement a biorisk management system that is both practicable and robust.

1 Scope

For the purposes of this document, the scope given in the CWA 15793:2008 Laboratory biorisk management standard, applies to this guidance document.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

CWA 15793:2008, *Laboratory biorisk management standard*

NOTE In 2011, the workshop 31 participants renewed the CWA 15793:2008 for another three years without any technical changes. The only editorial changes implemented involved the replacement of the word "standard" in the original document with the words "CWA" or "Agreement" wherever appropriate, based on a request to CEN by the CEN National Members. Therefore, the application of this guidance document is relevant to CWA 15793:2011 as well.

3 Terms and definitions

For the purposes of this document, the terms and definitions given in CWA 15793:2008 apply.

4 Biorisk management system

4.1 General requirements

4.1.1 Biorisk management system

The organization shall establish, document, implement and maintain a biorisk management system in accordance with the requirements of this laboratory biorisk management standard.

This CWA 15793:2008 requirement is a general statement concerning the establishment and maintenance of a biorisk management system within an organization. "Establish" implies a level of permanency, and the system should not be considered established until all its elements have been demonstrably implemented. "Maintain" implies that, once established, the system continues to operate. This requires active effort on the part of the organization. The elements of CWA 15793:2008 (such as self-audit programme and corrective action and management review) aim to ensure proactive maintenance of the system.

The priority should be on protecting employees, their community and environment from accidental or unauthorized intentional release of biological materials from the facility.

The level of detail and complexity of the biorisk management system, the extent of documentation and the resources devoted to it will be dependent on the nature (size, structure, complexity) of an organization and its activities.

An organization may choose to implement CWA 15793:2008 for its entire facility or specific units or laboratories as long as any boundaries set do not exclude specific activities that have an impact on biorisk management for those units or laboratories implementing CWA 15793:2008.

Establishing a biorisk management system should consider the following:

— policy and objectives relevant to the organization's business as a whole;

— legal and other requirements;

— historical and current performance by the organization;

— needs of other interested parties;

— opportunities and need for continual improvement;

— resources needed;

— contributions of employees;

— contributions of contractors and other external personnel; and

— integrations with the specific requirements of e.g. ISO 9001, ISO 14001, ISO 15189:2007, ISO 17025, ISO/IEC 27001, ISO 22000, ISO/IEC 20000, ILO-OSH 2001, OHSAS 18001, and PAS 99:2006 (for more information see Bibliography).

An organization seeking to establish a biorisk management system that conforms to CWA 15793:2008 should determine its current position with regard to its biorisk by undertaking an initial review. In determining how it will fulfill the requirements of CWA 15793:2008, the organization should consider the conditions and factors that may affect how it will manage the biosafety and / or biosecurity of the facility.

4.1.2 Continual improvement

The organization shall continually improve the effectiveness of the biorisk management system through the use of the policy, objectives, self-audit programme, audit results, analysis of data, risk assessment, corrective and preventive actions and the management review.

The organization should strive to continue to develop and refine the systems in place to ensure that further opportunities to improve are identified and implemented. This may be achieved through goal setting and targets placed upon those working within the facility and monitoring progress to ensure the goals are achieved.

4.3.1.2 Risk assessment timing and scope

The organization shall ensure the approach to risk assessment is defined with respect to its scope, nature and timing so that it is proactive rather than reactive.

Risk assessments should be carried out before new activities begin. Risk assessment also should be conducted whenever there is a change that affects the work environment, or in response to a laboratory incident. Risk assessments should be applied to all procedures and activities in the facility, including normal operations, periodic or rare laboratory procedures, and cleaning and maintenance.

The scope of the risk assessment should be focused on specific procedures and agents; multiple risk assessments may be required to adequately identify the risks and use the assessment to support risk control efforts.

Conducting risk assessments requires a comprehensive understanding of the organization's activities.

The following should trigger either a new risk assessment or review of an existing one:

a. *commencement of new work or changes to the programme of work, including the introduction of new biological agents or alterations to work flow or volume;*

b. *new construction / modifications to laboratories, plant and equipment or its operation;*

c. *introduction of altered* or *unplanned staffing arrangements (including contractors, visitors, and other non-core personnel);*

d. *significant alterations to Standard Operating Procedures (SOPs) or working practices (e.g. disinfection / waste management methodologies, Personal Protective Equipment (PPE) provision / usage entry / exit protocols, etc.);*

e. *when unexpected events that may have relevance for the management of biorisks are observed,* such as accidents, incidents (near misses) or changes in the security threat environment*;*

f. *when actual or potential non-conformity with internal / external rules and regulations is identified (e.g. introduction of new legislation or major accident exposure);*

g. *when considering emergency response and contingency planning requirements;* and

h. *as part of the existing management system review process (e.g. annually or at another appropriate and predetermined frequency).*

The scope, nature, and timing of the organization's risk assessments should be documented and be consistent with the initiation and completion of actual risk assessments.

4.3.1.3 Hazard identification

The hazards associated with proposed work shall be identified and documented.

e) *the need is identified for formal transfer documents signed by the responsible management representative authorizing movement of materials;*

f) *document control that allows traceability of material movements;*

g) *identifying and implementing adequate and proportionate emergency response and contingency plans associated with transportation, including adequate precautions for handling suspicious packages, quarantine areas and appropriate explosive stand-offs; and*

h) nominating and training a transport safety advisor who should be aware of the specific carrier requirements for a biological agent shipment.

Documents that should be available as a result of the above include:

— written acknowledgement by the receiving organization that the material was delivered and in a safe and secure condition (the document audit trail);

— written acknowledgement from carrier that they have an appropriate security plan for the materials being transported; and

— documentation of staff training in transport of biological agents (Transport of Dangerous Goods training).

4.4.4.10 Personal security

The organization shall have a policy in place to provide personal security support services to staff members that include, where appropriate, personal security awareness training.

Personal security is concerned with staff security during off-duty hours while away from the facility. During these times, staff members are vulnerable because of their function or position.

Personnel may be vulnerable to threats, physical attacks, etc. to themselves or their families or property by virtue of their function or position at the facility. The organization should take steps to identify and assess these vulnerabilities and can implement a process to address these issues, such as general personal security awareness training and counterintelligence training when considered appropriate. As the external and political environment may change over time, regular reviews of these threats, vulnerabilities, and mitigation measures should be conducted.

4.4.5 Emergency response and contingency plans

The organization shall establish and maintain plans and procedures to identify the potential for incidents and emergency situations involving biological agents, toxins and materials, to prevent their occurrence, to respond to emergency situations and to limit the likely illness or other damage that may be associated with them.

Emergency planning shall cover all aspects of biorisk and include general safety, security and medical issues.

To ensure the safety of staff members, visitors, vendors and the surrounding community, the organization should actively assess potential incident and emergency response needs, develop procedures and processes to cope with them, and continually aim to improve the effectiveness of responses.

Emergency response plans may include but are not limited to:

— risk assessment data necessary to begin the emergency response planning process;

— identifying and assigning roles to and responsibilities of staff members in the event of an emergency;

— identifying roles and responsibilities of people involved in emergency management;

— identifying and listing (inventory) of readily accessible emergency equipment, including location and maintenance status;

— assessing the availability of local emergency responders;

— a list of regulatory bodies to report to, depending on the level of emergency;

— information from consultation and planning sessions with local emergency responders;

— experience from previous accidents or incidents at the facility or from similar facilities;

— accident and incident investigation reports (lessons learned);

— review of emergency drills and exercises;

— informational signage related to emergency response such as evacuation routes, exit signage, location of emergency response equipment, etc.;

— development of emergency plan(s) using risk assessments, scenarios and consultation with local responders;

— identifying necessary emergency equipment provided to responders and periodically testing its suitability;

— procedures for reviewing and capturing lessons learned following each incident or emergency response event in order to improve future performance;

— procedures for coordinating response plan processes and resources across organizational, municipal, governmental levels, etc.; and

— providing training to staff in indigenous language.

Emergency plans will include evacuation procedures and maps, communication plans (including phone numbers, frequencies and other contact information), operational continuity plan, plans for hazardous materials in the event of an emergency, creation of emergency equipment inventory (threat detection, fire fighting, safety, security, communication and power back up) and storage of emergency equipment in a safe and accessible location.

4.4.5.1 Emergency scenarios

The organization shall ensure that all credible and foreseeable emergency scenarios that may impact the organization's biorisks have been identified.

The organization should identify potential accident and emergency scenarios in order to develop and validate planned responses.

In order that emergency planning can take place, it is necessary to consider all credible emergency scenarios. It is unlikely that all potential scenarios will be credible; however, all reasonable threats should be considered and recorded and, where appropriate, the rationale as to why issues were dismissed.

A list of possible emergency *scenarios* that could affect the facility might *include:*

— *infected / potentially infected worker or other contact (e.g. family member, emergency responder or community member;*

— *accident or illness to worker and need for evacuation;*

— *fire;*

— *flood;*

— *breach of security;*

— *explosion;*

— *potential loss of biological agents or toxins through theft or any other reason;*

— chemical spill;

— *unexpected virulence (unknown biological agents or biological agents expected to be avirulent);*

— theft or spill of radioactive materials;

— *physical facility and equipment failure, including control system failure;*

— *failure of disinfection regime;*

— *utility failure including electricity, gas, steam and water supplies;*

— *major spillage / aerosol release;*

— *environmental release;*

— *natural disaster (e.g. earthquake, extreme weather conditions, disease pandemics etc.);*

— *act of terrorism or deliberate vandalism;*

— *intense media attention; and*

— loss of communication systems.

Review all possible scenarios, document conclusions, and move forward for those deemed credible to your facility.

4.4.5.2 Emergency plans

The organization shall ensure that biorisks are taken into account when preparing and implementing emergency plans.

The organization shall ensure a system is established to effectively manage medical and/or environmental emergencies, including, but not limited to, the identification of potentially infected workers and provision of immediate medical care to exposed, ill or injured workers.

The organization shall also ensure that control measures in place can be demonstrated as being reasonable and proportionate to the scale and nature of the emergency.

Emergency plans shall be effectively communicated to all employees and relevant third parties, and tested, with the intention that everyone is aware of their obligations.

The organization should develop emergency response procedures for all credible scenarios and continually aim to improve the effectiveness of responses.

Components of an emergency plan may include:

— Development of emergency plans scenarios using:

  — identification of the location of hazardous materials and the emergency action required;

  — *risk assessments data;*

  — lessons learned from previous emergency response activities to improve effectiveness of response procedures;

  — information from consultation and planning sessions with local emergency responders;

  — identifying measures to control environmental impacts;

  — making relevant information available during the emergency (building layouts, location and nature of hazardous materials data where examples include material safety data sheets, laboratory containment level, contacts information); and

  — information from emergency and practice evacuation drills.

— Assignment of roles and responsibilities and a chain of command and consider:

  — identification of people in charge during the emergency (chain of command in accordance with the level of the emergency). It also should include designation of authority of people with specific roles during the emergency (wardens, first aid staff, spill teams, maintenance, interaction with first responders, etc.);

  — involvement of relevant management levels depending on the type of emergency;

  — *the need to respond during out-of-hours emergencies as well as those that occur during normal working hours;*

  — *provision for periods of reduced staff availability (e.g. during weekends and holiday periods);*

  — *identification of those responsible for devising, implementing and testing the control measures specified*; and

- *identification, roles and availability of emergency responders:*
  - *consulting external agencies which might be involved in the response and establish their role in responding to a given situation. These may include:*
    - *police and security services;*
    - *fire services;*
    - *ambulance and local hospitals / healthcare providers;*
    - *transport providers / couriers;*
    - *local and national government officials; and*
    - *environmental authorities;*
  - *documenting contact information and making it available to personnel responsible for coordinating the emergency response activity;*
  - *informing and educating external services in their roles and any risk exposures they may face and ensure their actions will not unnecessarily increase the risk associated with the emergency (e.g. uncontrolled use of fire water);* and
  - *reviewing options to sign a memoranda of understanding or agreements with key responders;*
- *evacuation plans to include:*
  - *the need for emergency access / exit, including the ability to override access controls as appropriate and emergency exit routes to avoid evacuating people through areas of higher biosafety or biosecurity;* and
  - *provision for safe removal, transport, transfer, treatment and accommodation of contaminated persons, objects,* etc.*;*
- worker health and first aid:
  - *procedures to address worker health needs in the event of an accident or emergency situation. This provision should extend to first responders and their families, members of the broader community and to environmental conditions that may have been affected by the incident. This should include the identification of emergency scenarios, including infected worker / family member, together with the necessary support measures (e.g. liaison with emergency services / local authorities), provision of equipment and other resources required to manage the emergency (e.g. prophylaxis, post-exposure treatment, disinfectants, isolation requirements, vaccines, etc.). The necessary plans and other materials for managing medical emergencies should be prepared, tested and maintained;*
  - *adequacy of first aid provision in relation to credible accident scenarios identified during risk assessment. The procedures should address the need for adequate provision of trained personnel and their availability, as well as equipment and other materials that may be required in the provision of treatment;* and
  - *identification of additional available competent medical support (e.g. hospitals, isolation units, etc.);*
- communication:
  - identifying personnel knowledgeable in risk communication responsible for communicating on behalf of the facility with

- — the community;
- — the general public;
- — the authorities; and
- — the employees;

- — developing communication plans and procedures for communicating specific actions to be taken by personnel at the site of the emergency, including contractors and visitors; and
- — informing and educating external services in their roles and any risk exposures they may face to ensure their actions will not unnecessarily increase the risk associated with the emergency (e.g. uncontrolled use of fire water, receipt by hospital emergency of patients possibly infected with biological agents).

— emergency equipment:

- — determining the needs for/purchase of emergency equipment such as alarm systems, emergency lighting and power, means of escape, safe refuges, critical isolation valves, firefighting and first aid equipment, safety, security and backup power equipment, communication facilities; and
- — testing and documentation of emergency equipment;

4.4.5.3 Emergency exercises and simulations

The organization shall ensure that structured and realistic emergency exercises and simulations, including security drills are conducted at regular intervals, based on risk, to test the plans, prepare personnel, and learn from any good practices or deficiencies identified.

The organization should actively test its emergency plans with *exercises* involving all pertinent employees and staff *in order to provide an assurance that plans are effective and to learn from any lessons that arise*.

— Practice drills should test the effectiveness of the most critical parts of the emergency plan and the completeness of the emergency planning process. Inclusion of external organizations or agencies (e.g. local fire-fighters, police department, and county or state emergency management teams) during practice drills should be considered.

— The starting point should be the emergency plans and considerations developed under section 4.4.5.2.

Elements of emergency exercises and simulations may include:

— *planning exercises,* (e.g. desktop exercises, mock exercises, practice drills*), that are realistic representations of the events they are designed to simulate* and verify that the actions planned are effective in the event of a real emergency*;*

— *conducting exercises under controlled conditions so they are not allowed to become a source of risk in their own right;*

— evaluating *results from exercises* and drills, including security drills after each exercise and having a process *of lessons learned* in place to identify and implement modifications to the plan to ensure effectiveness and completeness;

— *providing feedback to appropriate personnel on performance;*

— *recording any actions that have arisen and allocate to named individuals;*

— *ensuring measures set in place are closed out effectively;*

— determining the frequency and type of emergency exercises and simulations, including security drills based on the likelihood of the event; and

— conducting personnel training programmes on emergency equipment use;

4.4.5.4 Contingency plans

The organization shall ensure that in the event of an emergency, adequate contingency measures shall be in place to ensure the safety and security of continued operations.

In the event of an emergency or unforeseen event there may be disruption to normal operating conditions. This could range from the need to safely shut down work in the event of a power failure, to obtaining alternative storage conditions in the event of a breakdown. Such eventualities should be considered proactively and contingency plans set in place. Activities should address plant and utility failure*, the need for adequate redundancy, replacement and other measures, which could involve the availability of alternative facilities or personnel, the introduction of backup systems (e.g. power supplies) alternative means of decontaminating materials in the event of failure of critical systems or equipment (e.g. kill tanks or autoclaves), or the complete safe shut down of operations in extreme situations.*

Contingency plans may include:

— identification of possible emergencies considered under section 4.4.5.2;

— availability of vital records and equipment and ensuring their protection;

— risk assessment data;

— lessons learned from past events;

— identifying individuals who should be notified if the contingency plan is activated, the best method for contacting them and their contact information;

— storage of critical material in two secure places;

— a list of equipment and systems that would be affected by an emergency or unforeseen events that may cause a partial or full disruption of normal working conditions;

— identification of critical areas and systems for priority response;

— identification of the possible reasons for a partial or full disruption to normal operating conditions. Prioritise these from most likely to least likely to help determine the extent and length of the disruption (i.e. power failure maybe in just one area [circuits, electrical boards], in one building, the whole area or even the entire region);

— procedures for identifying affected areas including physical locations as well as functions. These may include identification of the warning indicators (for a power failure indicators may include lights and electrical equipment not working);

— the team performing the audit should have defined roles and responsibilities and be selected through an agreed, documented process;

— agreement on the procedure for audits / inspections which may include check-lists, and written scope;

— relevant personnel should be interviewed; determine if all personnel will be subject to interviews;

— relevant documentation should be examined; determine which are these documents (e.g. policy, objectives, emergency procedures, permits, training records, etc. depending on the described scope);

— agreement on how results of the inspection or audit will be measured and reported and who would receive the report;

— agreement on the frequency of audits based on the facility's risk (determined by risk assessment); additional audits may be conducted after an incident; and

— whether unannounced audits and inspections may be performed under specific circumstances.

Corrective action plans, implementation timelines and any follow-up actions should be developed and incorporated in the report.

Typical result may include an inspection and audit programme that, depending on the scope, develops a clear concise report detailing the identification of nonconformities:

— documentation about the audit and auditing team;

— assessments of the effectiveness of biorisk management procedures and practices;

— detailed assessments of levels of compliance with procedures and practices; and

— corrective procedures where nonconformities are identified by the audit.

The report should be documented and shared with relevant personnel, as appropriate.

4.6 Review

4.6.1 Biorisk management review

Top management shall review the organization's biorisk management system at planned intervals, to ensure its continuing suitability, adequacy and effectiveness. The review shall include assessing opportunities for improvement and the need for changes to the system, procedures, policies and objectives. Records from the management review shall be maintained.

Top management should establish a programme for periodic review of the biorisk management system, to assess its implementation, to ensure it remains appropriate and suitable for achieving the organization's biorisk management policies and objectives, and consider any appropriate changes.

The management review should be conducted at a defined frequency determined by the needs of the organization, but at least annually.

The biorisk management review process should be documented to describe:

— frequency, based upon risk (typically, a best practice may be at least annually);

— topics to be addressed;

— who will participate in the review and who will receive the completed review;

— roles and responsibilities in relation to the review; and

— expected outcome.

The topics addressed during the review may include:

— adequacy of the current biorisk policy;

— goals and objectives to determine any needs for modification or need to establish new ones;

— adequacy of the risk assessment system, including levels of risk and control measures;

— adequacy of resources (financial, people, materials, physical facilities);

— effectiveness of inspection process;

— effectiveness of the hazard reporting process;

— data related to accidents / incidents;

— effectiveness of SOPs;

— results of the audits and inspections;

— effectiveness of the corrective and preventive actions;

— preparedness of the organization to deal with emergencies; and

— assessment of the effects of foreseeable changes to operations, resources (e.g. human, material, financial), legislation or technology.

The management review may be divided into components that are conducted at different time intervals during the defined period. However, the results of the partial reviews should be combined to create an overall view of the suitability, adequacy and effectiveness of the management system.

The review input should include information on:

— *results of audits;*

— *compliance to SOPs and work instructions;*

— *status of risk assessment activities;*

— *status of preventive and corrective actions;*

— *follow-up actions from previous management reviews;*

— *changes that could affect the system;*

— *recommendations for improvement; and*

— *results of accident / incident investigations.*

The review output should include decisions and actions related to:

— *improvement of the effectiveness of the biorisk management system;*

— *improvement related to the requirements and risk assessments; and*

— *resource needs.*

厚生労働科学研究費補助金（新型インフルエンザ等新興・再興感染症研究事業）
分担研究報告書

高圧蒸気滅菌処理の条件と温度に関する検討

研究分担者　杉山和良（国立感染症研究所バイオセーフティ管理室）
研究協力者　伊木繁雄（国立感染症研究所バイオセーフティ管理室）

研究要旨

病原体の不活化の際汎用されるのが高圧蒸気滅菌器であるが、被滅菌物の状態によっては滅菌が不十分となる可能性が懸念される。本研究では昨年度の研究報告書にて、効率の良い高圧蒸気滅菌を行うためにはオートクレーブバッグの容積に合わせた適量の水を加えることが望ましいとの報告を行った。今回はオートクレーブバッグ内の被滅菌物として昨年度使用した実験衣にラテックスグローブを加えた。またオートクレーブバッグ内への水の添加方法について、直接添加する場合と耐熱性プラスチック容器に添加する場合の２通りで水蒸気量と滅菌効果に差が生じるか否かを設定温度及び時間ごとに検討した。これらについて温度と時間を様々に設定した上で高圧蒸気滅菌処理を施し、温度記録計、バイオロジカルインジケーター（BI）及びケミカルインジケーター（CI）により効果を判定した。また処理後オートクレーブバッグ内に残存する水蒸気量を重量により測定した。

その結果、グローブ内側の温度や滅菌効率は外側に比べ有意に低くなる傾向が見られた。水の添加については、オートクレーブバッグに直接添加した場合に比べプラスチック容器に添加した場合の方が内部での発生水蒸気量が少なく、これらは温度や滅菌効率にも影響を及ぼした。

オートクレーブによる滅菌は温度と時間のみではなく、オートクレーブバッグ内に発生または取り込まれる水蒸気量の影響を受けるが、グローブの内側など水蒸気が入りにくい場所への影響は顕著であった。グローブは使用後裏返して処理されるため、廃棄にあたってはグローブ内側の滅菌を踏まえより厳しい条件設定が必要と考えられた。またオートクレーブバッグ内に水を添加する際は直接添加することが必須であり、フラスコ内の培地等に含まれる水分がこれに代わることはないことが示唆された。今回得られた結果は、教育訓練の場で大いに活用できるものであると考えられた。

A. 研究目的

病原体取扱後には、用いた材料や器具等の消毒・滅菌処理が必須であるが、この際汎用されるのが高圧蒸気滅菌器である。高圧蒸気滅菌は121℃、2気圧以上の高温・高圧の条件下で飽和水蒸気が被滅菌物に接触した際に放出される凝縮熱を利用して微生物を殺滅するが、被滅菌物の形状や配置によっては水蒸気が十分に行き渡らないことが想定され、この場合滅菌が不十分となる

可能性が懸念される。したがって本研究では、想定される幾つかの条件下において高圧蒸気滅菌処理を行い、装置内の温度分布について調査を行っている。昨年度は、オートクレーブバッグと実験用防護服（以下、ガウン）を用いた処理において、オートクレーブバッグの口の開放とオートクレーブバッグへの水の添加が滅菌効率を高めることを報告した[1)]。

今回は使用後のグローブが裏返しの状態で外されることと、さらに一方のグローブがもう一方のグローブの中に包み込まれて滅菌処理されることを踏まえ、昨年度と同様の実験系にグローブを加え、グローブの内側と外側での滅菌効率を比較した。また2通りの水の添加方法で温度、水蒸気量と滅菌効果に差が生じるか否かについて、設定温度及び時間ごとに比較検討した。

B. 研究方法

被滅菌物としてガウン2着とラテックスグローブ4双を用いた。ガウンは縦に重ね、グローブは使用後の状態を想定し、一方を丸めた状態でもう一方の内側に挿入した。これを、①ガウン最上部、②ガウン中心部、③下側ガウン中心部及び④ガウン最下部に設置した。これらはポリプロピレン製オートクレーブバッグ（容積約35,000cm^3）中にて入れ、⑴設定温度(121, 124, 128, 132℃)、⑵設定時間(10～180 分)、⑶オートクレーブバッグの口(開放, 密閉)、⑷オートクレーブバッグ内への水の添加量(0, 50, 100, 200ml)及び⑸オートクレーブバッグ内への水の添加方法（直接または耐熱性プラスチック容器への添加；100ml のみで検討）の各条件を組み合わせ、高圧蒸気滅菌器による処理を行った。オートクレーブバッグの口は上向きとし、開放の場合は口径を3cmとした。

温度の検証には高温・高圧条件にて測定可能な温度記録計を使用し、1分ごとに計測した。滅菌の指標には市販のバイオロジカルインジケーター（BI）及びケミカルインジケーター（CI）を用いた。温度記録計と各インジケーターはグローブの設置箇所に置き、それぞれグローブ外横及びグローブ内最深部に設置した。またバッグ内への水蒸気の流入量と内部での水蒸気の発生量についても重量にて計測した。

C. 研究結果

いずれの設定条件においても、グローブ内側の温度や滅菌効率は外側に比べ有意に低くなる傾向が見られた。⑴、⑶、⑷及び⑸の条件が同じものどうしで滅菌効果を比較した場合（⑷は0及び100ml での比較、⑸は添加しないものと直接添加との比較）、グローブ内側の滅菌には外側に比べ 121℃処理で 1.25～1.5 倍、124℃処理で 1.3～1.67 倍、128℃処理で 1.375～2 倍、132℃処理で1.5～3倍の設定時間を要した（図2a～c）。またオートクレーブバッグの口を密閉した場合のグローブ外側における滅菌効果と、オートクレーブバッグの口を開放した場合のグローブ内側における滅菌効果が一致する結果となった（図2d）。

グローブ内側の滅菌に必要とされた最短設定時間は30分（132℃設定,オートクレーブの口を開放し 100ml の水を添加した場合）で、グローブ内側における実際の到達温度は 123.0℃であった。一方最長設定時間は 150 分（121℃設定,オートクレーブの口を密閉し水を添加しなかった場合）で、グローブ内側における実際の到達温度は114.3℃であった（図2a及びc）。

オートクレーブバッグへの水の添加方法

による比較の検証結果を図 3 に示す。水をプラスチック容器に添加した場合、直接添加した場合に比べ滅菌に要した設定時間は121℃及び 124℃処理で 2 倍、128℃処理で2.5 倍、132℃処理で 3 倍であった。前者におけるプラスチック容器からの水の蒸発量は 1～3ml であり、滅菌効率はオートクレーブバッグの口を開放し水を添加しなかった場合（図 2b 上段）と同じであった。

D／E. 考察と結論

高圧蒸気滅菌は水蒸気が持つ凝縮熱を利用した滅菌方法であるが、十分量の水蒸気が被滅菌物に直接触れることが効率的な滅菌へと繋がることから、多くの高圧蒸気滅菌器は釜の内部を水蒸気で飽和するために工程初期の段階で内部の空気が除去される仕組みとなっている。しかし、条件によっては部分的に空気が残り、その結果温度にむらが生じ十分な滅菌効果が得られない可能性がある。特にラテックスのように水蒸気の透過性を持たない素材を処理する場合、これに覆われた部分の滅菌効率が覆われていない部分と同等であるとは考えにくい。

一方医療現場では、使用後のグローブは安全上裏返して外され、さらにこれをもう一方のグローブの中に包み込んだ状態でオートクレーブバッグ等に入れられ、他の被滅菌物と共に滅菌処理される。このため今回は、二重に包まれたグローブが他の被滅菌物に覆われた状態を想定し、図 1 に示すように被滅菌物を設置した。

その結果、グローブの内側の滅菌効率は外側に比べ大きく劣ることが明らかとなった。特にオートクレーブバッグ内で水蒸気を発生させ、グローブの外側部分に十分量の水蒸気が触れる状態では、同じ設定温度で比較した場合滅菌に要する設定時間に最大で 3 倍の開きが生じた（図 2a)。これに対し、オートクレーブバッグの口が密閉され水蒸気が不足する状態では、最大でも 1.5 倍の開きに留まった。これは、前者ではグローブの外側部分において凝縮熱を利用した効率のよい滅菌が達成されたのに対し、後者では少ない水蒸気量のためにグローブの外側部分が既に非効率的な状態であったことから、グローブ内外での滅菌効率の差が前者に比べ小さかったことに起因すると考えられる。

またいずれの比較でも、設定温度の低い方がグローブ内外での滅菌効率の差が大きく、設定温度が高くなるほどその差は縮まった。設定温度が高いほどこれと実際の到達温度との差が大きく、また処理時間も短時間で滅菌が達成されていることから、グローブの外側部分における滅菌効率が高く処理時間が短いほど、一方で水蒸気が入り込みにくく熱伝導性が非効率的なグローブ内部では短時間処理での温度上昇が叶わないことを示唆している。

このためグローブの外側の滅菌に必要な処理時間には 10～120 分と差が生じているのに対し、これにグローブという条件が加わったことにより増加した処理時間は、いずれの場合も 20～40 分と一定であり、グローブ外側の温度や水蒸気量の違いによる差は認められなかった。

以上の考察から、グローブを滅菌する際には条件にかかわらずグローブの外側に設置されたインジケーターにより滅菌が確認される処理時間よりも 40 分程度長めに設定する必要があるものと考えられた。

昨年度の報告書にて、オートクレーブバッグへの水の添加が滅菌効率を高めるこ

とを報告した。一方実験室由来の廃棄物には培地等の水分を含んだものが多数存在することから、これらが高圧蒸気滅菌処理の際にどの程度水蒸気発生に関与するのかを検討した。微生物実験に使用した培地は一般的にフラスコ等のプラスチック容器に入った状態で処理されることから、プラスチック容器に水を加えて高圧蒸気滅菌処理を行った。

BI 及び CI による判定の結果、いずれの設定温度の場合もオートクレーブバッグ内に水を添加しなかった場合と同じ滅菌効率であることが示された。プラスチック容器に添加された水の蒸発量はごくわずかであったことから、内部における湿度上昇には繋がらなかったものと思われた。これは、プラスチック容器の熱伝導性が低いことに由来するものと考えられる。この結果から、高圧蒸気滅菌処理時におけるプラスチック容器内の水分からの水蒸気の発生は期待できないものと考えられた。

高圧蒸気滅菌は水蒸気が持つ凝縮熱により、有害物質を発生させることもなく安全に感染性物質を不活化できる優れた滅菌法である。ただし条件によっては水蒸気が十分に行き渡らず、滅菌が不十分となる可能性がある。凝縮熱を被滅菌物に対し効率よく作用させるには、オートクレーブバッグ内部をできる限り斑のない水蒸気量で満たすことが要求されるが、グローブの内側のように水蒸気の到達が困難な場合は、その性質を十分理解した上での適切な対応が望まれる。今回得られた結果は、国際的な高圧蒸気滅菌の基準をさらに詳細に検討したものであり、病原体等の無害化のモデルとして活用できるものであると考えられた。

参考文献

1) 厚生労働科学研究費補助金新型インフルエンザ等新興・再興感染症研究事業　バイオリスク管理の包括的強化及び必要な教材等の開発と実践の評価に関する研究：平成 23 年度総括・分担研究報告書, 17-21, 2012.

F．健康危険情報

なし

G．研究発表

1．論文発表

1)伊木繁雄：バイオセーフティの原理と考え方. バムサ会誌, 第 24 巻第 3 号, 19-27, 2012

2．学会発表

1) Iki S and Sugiyama K. An examination of autoclave conditions and the resultant effectiveness of sterilization. The American Biological Safety Association, 55th Annual Biological Safety Conference. October, 2012

H．特許出願状況

なし