皇居三の丸尚蔵館紀要　第２号（31）抜刷
〔 192-179 頁〕

ミュージアムにおける情報セキュリティ
―インシデント事例と近年の動向から

三島　大暉

2026 年 3 月
皇居三の丸尚蔵館

ミュージアムにおける情報セキュリティ
―インシデント事例と近年の動向から

三島 大暉

1. はじめに

近年ミュージアムでは、デジタルアーカイブやミュージアムDXといったデジタル事業の取り組みが注目されている。筆者らはそれらの前提となるミュージアムのITインフラの重要性を本誌前号で述べたが(註1)、それにくわえて情報セキュリティの要素もデジタル事業では欠かすことができない。もちろん情報セキュリティはデジタルに限ったものではないが、様々なデジタル技術が社会に浸透し、インターネットで世界とつながる現在においてはデジタル世界の情報セキュリティをより意識する必要があるだろう。

情報セキュリティ研修などを通じて、基本的な情報セキュリティ対策について知る機会があるが、ミュージアムに限定されない一般的な注意事項から演繹的にミュージアムにおける情報セキュリティを当てはめる傾向にある。もちろんそのような方法も次々と移り変わる情報セキュリティの傾向に対応するために重要であるが、ミュージアムにおける現場の活動とは結び付かない情報セキュリティの対応が求められる場面がある。そのため、本稿ではミュージアムにおいて実際に発生した情報セキュリティインシデントを分析し、ミュージアムの活動に引き付けながら、ミュージアムにおける情報セキュリティの特徴や留意点を明らかにすることを目的とする。また、近年クラウドサービスや生成AIといった新しい情報環境が日常となりつつあり、それらに対するミュージアムにおける情報セキュリティについても検討を行う。なお、情報セキュリティインシデントは、どのミュージアムでも発生しうるものであり、本稿で取り上げる情報セキュリティインシデントは教訓として参照するものである。

2. 情報セキュリティの概要

情報セキュリティとは、情報セキュリティマネジメントシステム（ISMS）のJIS規格（JIS Q27000：2019）によれば、「情報の機密性、完全性、可用性を維持すること」であり、機密性は「認可されていない個人、エンティティ又はプロセスに対して、情報を使用させず、また、開示しない特性」、完全性は「正確さ及び完全さの特性」、可用性は「認可されたエンティティが要求したときに、アクセス及び使用が可能である特性」である。簡単に言い換えれば、情報セキュリティとは、情報にアクセス・使用する権限がある者にのみアクセス・使用できるようにし（権限がなければアクセス・使用させない）、情報の正確性や完全性を保ち、情報にアクセス・利用する権限がある者が希望した際は（いつでも）アクセス・利用できるようにすることである。なお、本稿では具体的に情報セキュリティ対策などと表現しない限り、情報セキュリティをその捉え方、対策、リスクなどを含む包括的な概念として述べる。

また、情報セキュリティにおける脅威とは、「システム又は組織に損害を与える可能性がある、望ましくないインシデントの潜在的な原因」（JIS Q27000：2019）である。日本国内では、独立行政法人情報処理推進機構（IPA）が毎年その年の「情報セキュリティ 10大脅威」を公開しており、組織向け脅威と個人向け脅威に分けて、前年に発生した社会的に影響が大きかったと考えられる情報セキュリティ事案から選出している(註2)。脅威は一般に標的型攻撃やDDoSといった外的脅威と、内部不正による情報漏えいといった内部脅威に分けられる。脅威と並んで情報セキュリティのリスクの算定に使用される脆弱性とは、「一つ以上の脅威によって付け込まれる可能性のある、資産又は管理策の弱点」（JIS Q27000：2019）である。このような脅威や脆弱性、対象となる情報資産、発生可能性などを参考に情報セキュリティのリスクを分析・評価し、情報セキュリティ対策が実施される。情報セキュリティインシデント（情報セキュリティ事故）が発生した場合は、インシデントレスポンス（情報セキュリティ事故対応）として、その内容に応じて基本的に、検

知・初動対応、報告・公表、復旧・再発防止が行われる[註3]。

日本国内においては、「サイバーセキュリティ基本法」（平成26年法律第104号）[註4]が定められ、政府機関等や地方公共団体の責務、国民の努力が述べられている。政府機関等（国の行政機関や独立行政法人等）では、主に「政府機関等のサイバーセキュリティ対策のための統一規範」（サイバーセキュリティ戦略本部）[註5]により「政府機関等のサイバーセキュリティ対策のための統一基準」や「政府機関等の対策基準策定のためのガイドライン」に準拠した情報セキュリティ対策が実施されている。地方公共団体では、主に「地方公共団体における情報セキュリティポリシーに関するガイドライン」（総務省）[註6]に対応する情報セキュリティ対策が実施されている。民間企業に対しては、経済産業省が情報セキュリティに対する情報提供を行っているほか、IPAが「中小企業の情報セキュリティガイドライン」[註7]などを公開している。これらに沿って、あるいは参考にして、各組織は自組織の情報セキュリティポリシーや規則等を整備して情報セキュリティを確保するようにしている。近年では、クラウドサービスや生成AI利用などへの対策も加わっているとおり、情報セキュリティは情報技術の進展や社会の変化にあわせて適応することが求められる。

3. ミュージアムにおける情報

ミュージアムにおける情報セキュリティの対象となる情報は、様々な区分が可能であるが[註8][註9][註10]、おおよそ収蔵するコレクションに関する情報、ミュージアムの活動に関する情報、ミュージアムの管理運営に関する情報に区分される。ただし、いずれも排他的関係ではなく、展示に関する情報が、展示というミュージアムの活動に関する情報に該当するだけでなく、コレクションに関する情報や管理運営に関する情報にも該当する場合がある。以下、それぞれのミュージアムにおける情報について、博物館法（昭和26年法律第285号）とICOM（国際博物館会議）によるミュージアムの定義も踏まえて具体的に述べる。

・博物館法が定義するミュージアム
「歴史、芸術、民俗、産業、自然科学等に関する資料を収集し、保管（育成を含む。以下同じ。）し、展示して教育的配慮の下に一般公衆の利用に供し、その教養、調査研究、レクリエーション等に資するために必要な事業を行い、併せてこれらの資料に関する調査研究をすることを目的とする機関」[註11]

・ICOMが定義するミュージアム
「博物館は、有形及び無形の遺産を研究、収集、保存、解釈、展示する、社会のための非営利の常設機関である。博物館は一般に公開され、誰もが利用でき、包摂的であって、多様性と持続可能性を育む。倫理的かつ専門性をもってコミュニケーションを図り、コミュニティの参加とともに博物館は活動し、教育、愉しみ、省察と知識共有のための様々な経験を提供する。」[註12]

(1) コレクションに関する情報

ミュージアムは何かしら資料等を収集・保管してコレクションを形成しており、資料自体の情報（美術工芸品の場合、名称、作者、制作年代、員数、寸法、形態、状態など）と、資料を収集・保管（保存）するための情報（美術工芸品の場合、管理番号、配置（移動履歴）、修理履歴、展示履歴、貸出履歴など）がある。そのほか、コレクションに関連して収集・保管する図書や刊行物等に関する情報（掲載履歴などを含む）がある（別の情報区分とする考え方もある）。実際の情報の形態としては、資料カードや資料台帳、資料管理システム等において、文字や画像で記録・保管されている。

(2) ミュージアムの活動に関する情報

ミュージアムにおける活動は様々であるが、博物館法およびICOMによるミュージアムの定義を踏まえて、ここでは調査研究活動、展示活動、教育普及活動、情報発信活動、コミュニティ活動について取り上げる。これらの情報の形態は多種多様であり、形態にあわせて記録・保管されている。

・調査研究活動に関する情報

ミュージアムは、資料等を収集する際または収集した後、資料等の価値付け（美術的価値や歴史的価値、学術的価値など）や資料等の状態確認を行うために調査研究活動を行う。この活動を通して得られた情報は、調査研究活動の成果報告書等のほか、調査研究活動を行う中で集められた関連資料や文献、赤外線画像やX線分析データなどが該当する。

・展示活動に関する情報

ミュージアムは、調査研究活動の成果を社会に還元したり、広く一般の人々に様々な経験を提供したりするために資料等の展示活動を行う。展示活動では、展示趣旨や展示計画、展示パネルやキャプション、展示映像コンテンツ、模型などが制作される。また、チラシやポスター、図録、ミュージアムグッズなども制作される。これらの企画・制作過程、成果物に関連する情報が展示活動に関する情報に該当する。そのほか、展示期間中には展示環境の温湿度データの取得、来館者数の記録、来館者に対するアンケートが実施され、これらも展示活動に関する情報といえる。

・教育普及活動に関する情報

ミュージアムは、資料等の魅力、調査研究活動の成果、展示の見どころなどをターゲット（来館者や非来館者）にあわせて分かりやすく伝えるために教育普及活動を行う。講演会やギャラリートーク、出前講座、体験教室などが企画され、講演資料やワークシートなどが制作される。これらの企画・制作過程、成果物、記録写真、アンケートデータなどが教育普及活動に関する情報といえる。

・情報発信活動に関する情報

ミュージアムは、資料等、調査研究活動、展示活動、教育普及活動などを館外へ周知・広報するために情報発信活動を行う。ウェブサイトへの掲載、ソーシャルメディア（XやInstagramなど）への投稿、ポスターやデジタルサイネージの掲出、広告の掲載などが行われるが、これらの企画・制作過程、成果物、人々の反応（コメントやアクセス数）といったフィードバックなどが情報発信活動に関する情報といえる。また、コレクション検索や様々なデジタルアーカイブに関連する手法により資料等の情報を公開・機関連携する活動が見られるが、このような活動に関する情報も情報発信活動に関する情報と位置づけられるだろう。

・コミュニティ活動に関する情報

ミュージアムは、上記の様々な活動をコミュニティと関わって行う。ミュージアムが所在する地域や学校、所属する国内外のミュージアムネットワーク（例えば、千代田ミュージアムネットワーク、全国美術館会議、ICOMなど）における活動に関する情報、ミュージアムを支援する賛助会やボランティアなどの活動に関する情報が該当する。

(3)　ミュージアムの管理運営に関する情報

ミュージアムは一つの組織または組織の一部であり、組織を経営・運営するために様々な管理事務が必要となる。組織を成立させるための法律や条例、内部の規則や規定、組織体制、人事などに関する情報、組織を経営・運営するための予算（収入・支出）や契約といった財務・会計に関する情報、方針を決定する打合せや会議に関する情報、建物や電気・空調設備といった各種施設設備に関する情報などが該当する。

なお、以上の情報資産の中には個人情報や特定個人情報が含まれ、それぞれ個人情報保護法等によって適切に管理される。

4. ミュージアムにおける情報セキュリティ

(1) ミュージアムにおける情報セキュリティの言及事例

ミュージアムにおける情報セキュリティについては、ミュージアムのリスク管理の文脈で取り上げられている場合[(註13)]が多く、例えば文部科学省が公開する平成19年度「博物館における施設管理・リスクマネージメントに関する調査研究報告書」(基礎編後半)[(註14)]では施設の物理的なセキュリティが中心となるが、リスクごとの対応「情報漏洩」において情報セキュリティが取り上げられている。また、国外においてはIATM(国際交通・通信博物館協会)[(註15)]やICOM-SECURITY(国際博物館会議・博物館セキュリティ国際委員会、旧名ICOM-ICMS)[(註16)]においてミュージアムにおけるサイバー攻撃への対応などが取り上げられている。そのほか、ミュージアムにおける個人情報保護[(註17)(註18)]、情報のバックアップや長期保存[(註19)]、情報倫理[(註20)]の文脈で情報セキュリティに関連する言及が見られる。しかしながら、ミュージアムの活動に引き付けた情報セキュリティの検討は明確には見られない。

(2) ミュージアムにおける情報セキュリティインシデント事例

ミュージアムにおける情報セキュリティについては、基本的に設置者である国や地方自治体、財団法人等と同じ情報セキュリティ対策が実施されており、考慮すべき脅威についてもIPAが公開する情報セキュリティ10大脅威等を参照できるが、ミュージアムの活動に引き付けて具体的な特徴や留意点を明らかにするため、次のとおり情報セキュリティインシデント事例(以下、インシデント事例という。)を収集した。まずインターネット上で参照可能な情報セキュリティニュースサイト(Security NEXTなど)から美術館、博物館、動物園、水族館といったミュージアム(植物園は日本博物館協会会員館が少ないため対象外)で実際に発生したインシデント事例を収集し、次にできる限り確認可能な新聞社のインターネットニュースサイトにおいて情報セキュリティニュースサイトで見られないインシデント事例を収集した結果、44事例を収集することができた(2025年8月末時点)。なお、収集したインシデント事例は、公表されるに至った、またニュースサイトが取り上げるに至ったインシデントであることに留意が必要である一方、発生すると注目されやすい(影響が大きい)インシデントであるともいえる。

以下、3章で区分したミュージアムの活動ごとにインシデント事例を見ていく(図1、表1)。なお、ミュージアムの複数の活動に関連づけられるインシデント事例は最も関連性のある活動に割り当てている。また、調査研究活動に関連づけられるインシデント事例は今回収集した事例の中では見当たらなかったため取り上げていない。

収集したインシデント事例の中で多く関連づけられるミュージアムの活動は、教育普及活動(14事例)と情報発信活動(13事例)である。情報セキュリティインシデントの多くが外部との接触点で発生することから、来館者等と接触する機会の多い教育普及活動と、インターネットや広報活動で外部と接する情報発信活動に関連づけられるインシデント事例が多いのは当然とも考えられる。

教育普及活動に関連づけられるインシデント事例では、イベント(教育普及的なイベントといえない可能性があるイベントも含む)参加希望者や当選者へのメール連絡の際に一斉送信の宛先をBCCで隠して送信すべきところを、TOやCCで送ってしまい受信者全員が他人のメールアドレス等を閲覧できてしまった事例がほとんどである。イベント関係者へ個人情報が記載されたファイルを添付して送信してしまった事例、個人情報が記載された当選結果をウェ

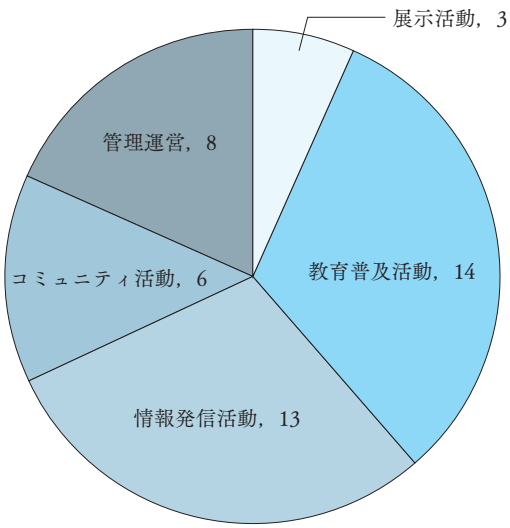


図1 ミュージアムにおける情報セキュリティインシデント事例の各活動の内訳(全44事例)

ブサイトに掲載してしまった事例、イベント案内状を誤送付してしまった事例も、イベント関係者への案内時や連絡時にインシデントが発生してしまったという点で共通している。その逆に、イベント参加申込時に使用する申込フォームの設定不足によるインシデント事例も見られる。また教育普及活動の別の場面として、イベント参加者が使用する館内PCのウイルス感染事例（イベント参加者が持ち込んだUSBメモリ等が感染媒体になった可能性がある）、ワークショップ参加者の個人情報を保存したUSBメモリを紛失した事例は、イベント会場での情報機器の管理不足によるインシデント事例といえる。

教育普及活動と同じようなインシデント事例が見られるのがコミュニティ活動（6事例）である。具体的には、メールの宛先、本文、添付ファイルを誤って送信してしまった事例であり、ボランティアや市民活動グループ、関係団体といった各コミュニティへの案内時や連絡時にインシデントが発生してしまったものである。

教育普及活動と並んでインシデント事例が多く関連付けられる情報発信活動では、不正アクセス等によるウェブサイトの停止や改ざんの事例が見られる。改ざんにより不正なサイトに誘導されるなどしてウェブサイト利用者のPC等がウイルスに感染する可能性があった事例、政治的・社会的な主張のために活動するハクティビストによる攻撃を受けた事例（実際にその主張が掲載された事例もある）、サーバから個人情報が奪取された事例など、インターネットで世界からアクセス可能なウェブサイトは様々な目的のサイバー攻撃に晒されており、その中で発生してしまったインシデントといえる。また、FAXの誤送信で取材内容が流出してしまった事例、広報委託先へのサイバー攻撃で情報が漏えいしてしまった事例のように広報活動において発生したインシデント事例もある。くわえて、公式のチケット購入サイトと見せかけたフィッシングサイトが検索エンジンの上位に見つかるという、ミュージアムを訪れようとする人に被害を及ぼす可能性がある事例も見られる。

展示活動に関連づけられるインシデント事例（3事例）では、教育普及活動やコミュニティ活動の事例と類似する、当選者に別の当選者の情報を記載した観覧券を誤送付してしまった事例やミュージアムショップ委託先からのメールの誤送信で図録予約者のメールアドレスが流出してしまった事例があるほか、展示室で個人情報が記載された展示資料を紛失するという展示資料そのものに関連する事例も見られる。

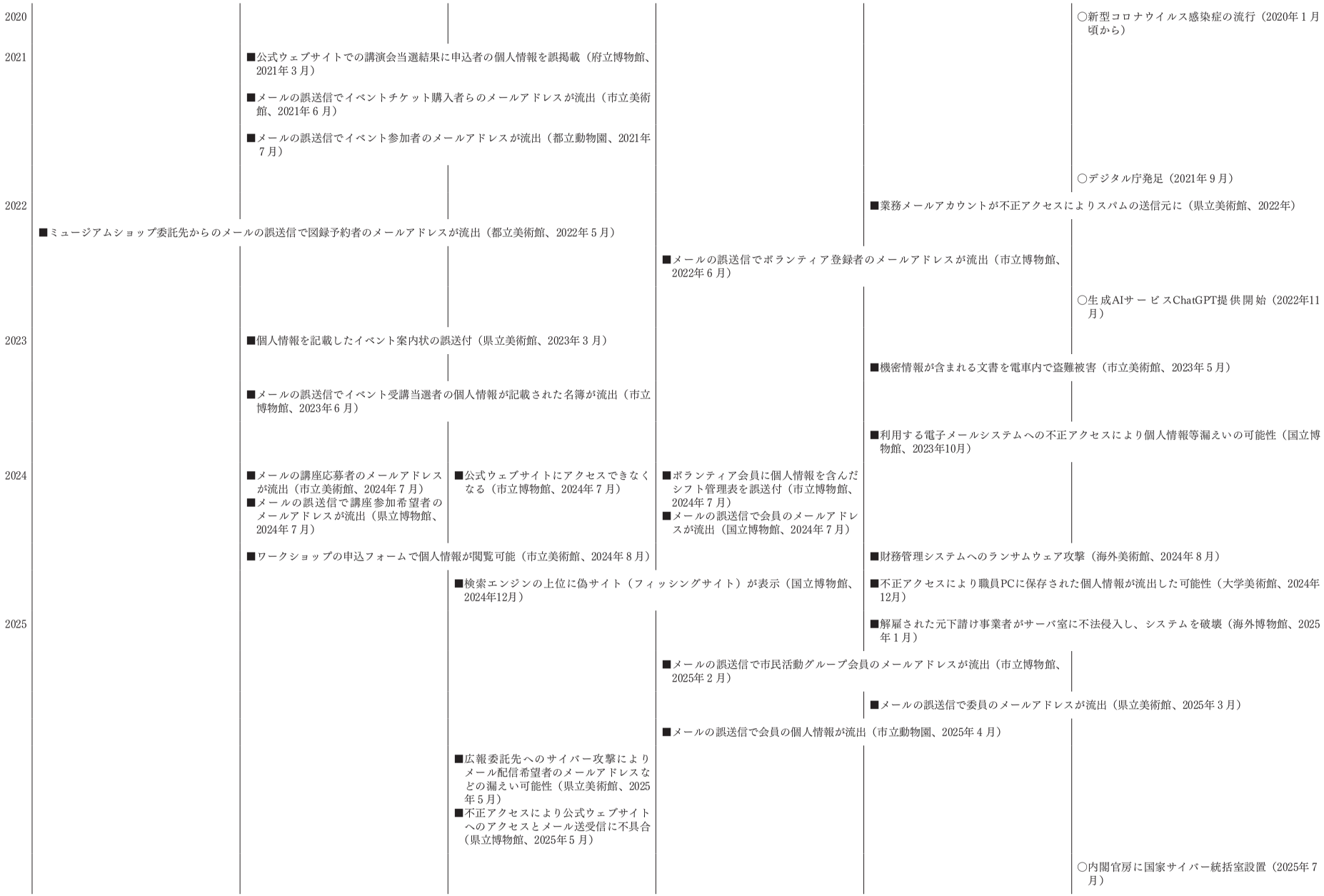
上記のほか、ミュージアムの管理運営に関連づけられるインシデント事例（8事例、ミュージアムの活動全般に関連づけられる事例を含む）では、機密情報が含まれる文書を電車内で盗まれてしまった事例やメールの誤送信で委員のメールアドレスが漏えいしてしまった事例といった職員のミスによるもの、財務管理システムへのランサムウェア攻撃、メールシステムや職員PCへの不正アクセスにより個人情報等が漏えいした可能性があるサイバー攻撃によるものが見られる。2024年に発生した、大英博物館で解雇された元下請け事業者がサーバ室に不法侵入してシステムを破壊し、一部展覧会の公開停止に追い込まれた事例[註21]は、ほとんど内部不正といえるものである。ミュージアムの管理運営に関連づけられるインシデント事例は、ミュージアム全体への影響範囲がより大きい傾向にあるといえる。

(3)　ミュージアムにおける情報セキュリティの特徴・留意点

上記のとおりミュージアムの活動に引き付けて情報セキュリティインシデント事例を見ていくと、ミュージアムにおける情報セキュリティは、少なくとも（a）教育普及活動と情報発信活動において特に留意する必要があること、（b）管理運営に係るインシデントはミュージアム全体の活動に深刻な影響を及ぼしうることが特徴と言えるだろう。また、ミュージアムの各活動における情報セキュリティの留意点は以下のことが考えられる。

表1　ミュージアムにおける情報セキュリティインシデント事例

発生年	展示活動	教育普及活動	情報発信活動	コミュニティ活動	管理運営	（参考）情報セキュリティに関係する社会動向
2005以前						○中央省庁ウェブサイト改ざん（2000年１月） ○内閣官房に情報セキュリティ対策推進室設置（2000年２月） ○個人情報保護法制定（2003年５月）
2006	■展示室で個人情報記載の展示資料を紛失（大学博物館、2006年６月）					
2007				■メールの誤送信でボランティア登録者の氏名とメールアドレスが流出（市立美術館、2007年９月）		
2008						○SNSサービスTwitter（現在X）日本語版提供開始（2008年４月）
2009						
2010			■過去の展覧会特設ウェブサイトが改ざん（国立美術館、2010年１月）			
		■ワークショップ参加者の個人情報含むUSBメモリを紛失（県立博物館、2010年５月）	■公式ウェブサイトが改ざん（市立美術館、2010年５月）			
		■イベント参加者が使用する館内PCがウイルス感染（公財立博物館、2010年８月）				
2011						
2012			■不正アクセスにより公開データベースが改ざん（国立博物館、2012年８月）			
2013			■不正アクセスにより公開データベースが改ざん（県立博物館、2013年１月）			
			■不正アクセスにより公式ウェブサイトが改ざん（県立動物園、2013年３月）			
2014		■メールの誤送信でイベント参加希望者のメールアドレスが流出（県立博物館、2014年２月）				
						○ベネッセ個人情報漏えい（2014年７月）
						○サイバーセキュリティ基本法成立（2014年11月）
2015					■アクセス集中による不具合で購入サイトで個人情報の誤表示（企業立水族館、2015年５月）	
						○日本年金機構情報漏えい（2015年６月） →自治体NWの三層分離
		■メールの誤送信でイベント参加者のメールアドレスが流出（市立動物園、2015年７月）				
2016			■アクセス集中によりウェブサイトが停止（県立博物館、2016年９月）			○IoT機器の脆弱性を突くMiraiボットネットの確認（2016年）
2017			■サイバー攻撃により公式ウェブサイトが停止（企業立水族館、2017年５月）			○ランサムウェアWannaCryの確認（2017年５月） ○クラウド・バイ・デフォルト閣議決定（2017年５月）
			■不正アクセスにより公式ウェブサイトの改ざんと個人情報の流出（都立動物園・水族館、2016年７月）			
2018	■当選者に別の当選者の情報を記載した観覧券を誤送付（都立動物園、2018年５月）					
2019		■メールの誤送信でイベント参加者のメールアドレス等が流出（特殊法人立博物館、2019年２月）				
			■FAXの誤送信で取材内容が流出（都立動物園、2019年７月）			
		■メールの誤送信でイベント参加者の個人情報が流出（県立博物館、2019年10月）				○標的型攻撃で利用されるEmotetの国内感染事例（2019年）


2020
2021
2022
2023
2024
2025
○新型コロナウイルス感染症の流行（2020年１月頃から）
■公式ウェブサイトでの講演会当選結果に申込者の個人情報を誤掲載（府立博物館、2021年３月）
■メールの誤送信でイベントチケット購入者らのメールアドレスが流出（市立美術館、2021年６月）
■メールの誤送信でイベント参加者のメールアドレスが流出（都立動物園、2021年７月）
○デジタル庁発足（2021年９月）
■業務メールアカウントが不正アクセスによりスパムの送信元に（県立美術館、2022年）
■ミュージアムショップ委託先からのメールの誤送信で図録予約者のメールアドレスが流出（都立美術館、2022年５月）
■メールの誤送信でボランティア登録者のメールアドレスが流出（市立博物館、2022年６月）
○生成AIサービスChatGPT提供開始（2022年11月）
■個人情報を記載したイベント案内状の誤送付（県立美術館、2023年３月）
■機密情報が含まれる文書を電車内で盗難被害（市立美術館、2023年５月）
■メールの誤送信でイベント受講当選者の個人情報が記載された名簿が流出（市立博物館、2023年６月）
■利用する電子メールシステムへの不正アクセスにより個人情報等漏えいの可能性（国立博物館、2023年10月）
■メールの講座応募者のメールアドレスが流出（市立美術館、2024年７月）
■メールの誤送信で講座参加希望者のメールアドレスが流出（県立博物館、2024年７月）
■公式ウェブサイトにアクセスできなくなる（市立博物館、2024年７月）
■ボランティア会員に個人情報を含んだシフト管理表を誤送付（市立博物館、2024年７月）
■メールの誤送信で会員のメールアドレスが流出（国立博物館、2024年７月）
■ワークショップの申込フォームで個人情報が閲覧可能（市立美術館、2024年８月）
■財務管理システムへのランサムウェア攻撃（海外美術館、2024年８月）
■検索エンジンの上位に偽サイト（フィッシングサイト）が表示（国立博物館、2024年12月）
■不正アクセスにより職員PCに保存された個人情報が流出した可能性（大学美術館、2024年12月）
■解雇された元下請け事業者がサーバ室に不法侵入し、システムを破壊（海外博物館、2025年１月）
■メールの誤送信で市民活動グループ会員のメールアドレスが流出（市立博物館、2025年２月）
■メールの誤送信で委員のメールアドレスが流出（県立美術館、2025年３月）
■メールの誤送信で会員の個人情報が流出（市立動物園、2025年４月）
■広報委託先へのサイバー攻撃によりメール配信希望者のメールアドレスなどの漏えい可能性（県立美術館、2025年５月）
■不正アクセスにより公式ウェブサイトへのアクセスとメール送受信に不具合（県立博物館、2025年５月）
○内閣官房に国家サイバー統括室設置（2025年７月）

まずミュージアムにおける教育普及活動やコミュニティ活動では、ワークショップなどの教育普及イベントへの参加者や参加希望者、コミュニティ（ボランティアの方や賛助会の会員等）の個人情報を扱っていることを十分認識し、特にそのようなイベント参加者等と連絡を取る場合は誤送信・誤送付に注意することが求められる。また、ワークショップなどで使用するPCといった情報機器、申込フォームなどのウェブサービスについては情報セキュリティの観点から設定等に問題ないか適切に確認・管理することが求められる。

次にミュージアムにおける情報発信活動では、サイバー攻撃によるウェブサイトの停止や改ざん、情報漏えいへの対応と、サイバー攻撃の踏み台に利用されないようにすることなどが求められる。特に、国立博物館のウェブサイトが改ざんされ、領土の主張が為された事例があるように、ミュージアムのウェブサイトは政治的・社会的な主張のために世界中からサイバー攻撃のターゲットになる可能性があることを認識する必要がある。世界中の利用者に対して安全なミュージアムのウェブサイトを継続的に提供するために、サイバー攻撃に耐えられるウェブサイト基盤を選定し、脆弱性への対応などを放置せずに適切に管理運用していくことが求められる。また、万が一サイバー攻撃を受けても被害を最小にできるよう、ウェブサイト基盤に個人情報などを保存しないなどのシステム構成や運用の工夫も考えられる。さらにフィッシングサイトなどの不正なウェブサイトが本物のウェブサイトとして誤解されないように、人々に行きわたるSNSを含めた情報発信方法を継続的に工夫していくことが求められる。

ミュージアムにおける展示活動では、インシデント事例で見られた展示作品の盗難は情報セキュリティにとどまらない問題であるが、特に美術系・歴史系ミュージアムではコレクションの資料等自体に人に関する情報が含まれる場合があり、個人情報など機微な情報を含む資料等を展示する場合は展示方法を一層考慮する必要があるだろう。ただし、その前提として、資料等をできる限り正しく理解し、文化的背景等を考慮して判断・説明するための調査研究がミュージアムに求められる。

ミュージアムにおける管理運営では、業務で使用するPCや情報システム等がサイバー攻撃や内部不正の被害を受ければ、特定の活動に限らずミュージアム全体の活動に影響する深刻な状態になりうることを認識する必要がある。ミュージアムにおける情報セキュリティの留意点だけでなく、管理運営に関しては公共機関や民間企業等と共通する内容もあることから、広く公共機関や民間企業等で求められる情報セキュリティ対策が有効と考えられる。また、内部不正への対策は技術的な情報セキュリティ対策では十分に対応できないため、不正の3要素（機会、動機、正当化）への対策を組織運用上実施することが求められる。

以上のミュージアムにおける情報セキュリティの留意点は、もちろん網羅的なものではなく、今回インシデント事例として関連づけられなかった調査研究活動においても、調査研究協力者へのメールの誤送信などに十分注意する必要がある。このようなミュージアムにおける情報セキュリティの留意点は、情報セキュリティ研修等で扱われる広く公共機関や民間企業等で求められる情報セキュリティの留意点や基本的な行動指針（「慌てて作業しない」「複数人が確認する」「自分を過信せず周りに相談する」など）とあわせて、ミュージアムの様々な活動を円滑に進め、ミュージアムの社会的使命やそれぞれの設置目的を実現し、来館者に満足してもらうために必要な基本的行動（特別な行動ではなく、ミュージアムの職員として備えておくべき行動）として認識される必要があるだろう。また、広報やミュージアムショップなどの委託先のインシデント事例で見られるように、委託したとしても委託先の選定や情報セキュリティ対策状況等の確認に関する委託者責任は免れないため、委託先（再委託先等を含む）についても適切に管理・監督できる体制が求められるだろう。

5. これからのミュージアムにおける情報セキュリティ

ミュージアムを取り巻くデジタル環境は、情報技術の進展や社会の変化にあわせて変化しており、直面する新たな課題も見られる。本章では、近年のミュージアムを取り巻くデジタル環境から特に社会への影響が増しているクラウドサービス、生成AI、フェイク情報を取り上げ、これからのミュージアムにおける情報セキュリティについて検討する。

(1) クラウドサービス

クラウドサービスは、データセンターなどに設置されたサーバ等情報機器を利用してインターネットや閉域ネットワーク等を経由して利用者にサービスを提供するものである。IaaS（Infrastructure as a Service）、PaaS（Platform as a Service）、SaaS（Software as a Service）といったサービスの提供範囲やサービス提供企業等によって内容は異なるが、組織のサーバ室内に情報機器を設置してサービスを提供するオンプレミスと異なり、IaaSの場合はサーバ等情報機器や電源等のインフラまで、PaaSの場合はアプリケーションを動作させるOSやミドルウェアまで、SaaSはアプリケーション（サービス）の提供自体までクラウドサービス提供企業等に基本的に管理運用と各提供範囲に応じた情報セキュリティ対応を任せることができる。また、オンプレミスで導入する場合はサーバ等情報機器の調達・構築に費用がかかるが、クラウドサービスは比較的導入ハードルの低いサービス利用料を支払うことで利用できる。ミュージアムにおいては、コレクション管理・公開システムのSaaS型クラウドサービスが見られるほか、ウェブサイトをAWSやAzure、さくらインターネットなどのクラウドサービスを利用して構築している例も見られる。

クラウドサービスは、特にSaaSの場合は導入が容易であるために、オンプレミスとは別の視点で情報セキュリティに留意する必要がある。まずサービスで取り扱う情報（コレクションに関する情報、ミュージアムの活動に関する情報、管理運営に関する情報）やサービスの利用方法に対して、当該クラウドサービスの仕様が情報セキュリティ要件を満たしているか確認することである。どこまで当該クラウドサービスや提供企業等を信頼できるか、情報漏えい等の情報セキュリティインシデントにどのように対応するか、どの程度リスクを許容できるかなど、ミュージアム側で情報セキュリティについて判断することが重要となる。また、イベント参加申込時に使用する申込フォームの設定不足で情報漏えいが発生したインシデント事例があるように、クラウドサービスは設定ミス1つで、非公開にすべきところを世界中に公開してしまう、容易に不正アクセスされてしまうといった危険がある。クラウドサービス側でもフールプルーフの設計（誤って操作しても深刻な状況を防ぐ設計）がされている場合があるが、ミュージアムにおいても、初めて使用するクラウドサービスについては、特に情報セキュリティに関わる設定に注意し、思い込みや自己判断ではなくクラウドサービス提供企業等に確認しながら適切に対応することが求められる。

(2) 生成AI

生成AIとは、テキスト、画像、音声などを自律的に生成できるAI技術の総称であり、多様な形式で出力できるものはマルチモーダルとも呼ばれる(註22)。このようなマルチモーダルな生成AIの代表的なものに、ChatGPT、Gemini、Copilotといった対話型生成AIサービスがある。これらはインターネット上の情報など膨大なデータを学習しているとされ、利用者は質問や指示などのプロンプトを入力することで、その回答として生成されたテキストや画像などを得ることができる。生成AIサービスは民間企業をはじめ公共機関等ですでに利用され始めているが(註23)、生成AIサービス利用における情報セキュリティの留意点として、主に入力情報と出力情報の課題が指摘されている(註24)。各生成AIサービスの仕様や設定内容にもよるが、生成AIサービスの品質向上のため自身の入力情報が学習されてしまう可能性がある。文章や画像等の入力情報に個人情報や機密情報が含まれていた場合、それらも生成AIに学習されてしまい、当該情報にアクセス権限のない人が生成AIサービスを利用した際の回答に含まれて情報漏えいが発生してしまう可能性がある。基本的に学習されたデータはAIモデルから削除できないため、自身の入力情報を学習されたくない場合は適切な設定を行うか、オフライン環境やプライベート環境といった閉じた環境で、それに適したAIモデルを選択することが求められる（自身の知的財産（IP）を学習されたくない場合も同様）。一方、出力情報に関しては、学習された情報から誤った情報や存在しない情報をもっともらしく回答してしまうハルシネーション（幻覚）や学習された情報の偏りによるバイアス（偏見や差別）といった課題が指摘されている(註25)。生成AIサービスを利用する場合や生成AIを使用したサービスを提供する場合は、ハルシネーションやバイアス

への対応に加え、個人情報や機密情報の漏えいを防ぐ設計や運用方法が求められる。

ミュージアムにおいても、福岡市博物館では館内の大型デジタルサイネージでAIによる施設案内を行う実証実験（2025年7月1日～9月30日）[註26]、日本科学未来館では「対話型AIロボット」実証実験（2025年8月25日～8月31日）[註27]が見られ、館内案内や展覧会案内で生成AIを活用する際に求められる情報セキュリティ対応が現実のものとなってきた。また、森美術館で開催された「マシン・ラブ：ビデオゲーム、AIと現代アート」展（2025年2月13日～6月8日）では、生成AIを利用したアート作品が展示されるとともに、作品で使用されている技術や作品の背景などに関する重要な単語の用語集をChatGPTで生成し、森美術館が編集を加えて作成した事例がある[註28]。用語集作成に見られる生成AIと人との協働は、生成AIサービスのハルシネーションやバイアスがコレクションに関する文化や歴史を誤って伝えてしまうといった、知識インフラであるミュージアムにとって致命的なことを防ぐだけでなく、個人情報や機密情報の漏えいを防ぐ情報セキュリティ対応としても求められるだろう。

上記のほか、生成AIを利用してマルウェアが作成された事例[註29]があるように、生成AIを悪用した、攻撃者の拡大と攻撃の効率化によるサイバー攻撃の拡大・高度化は差し迫った問題である。人間が具体的に指示をせず、自律的に活動するAIエージェントも出現しており、それを悪用したサイバー攻撃も懸念される。小規模なミュージアムであってもインターネットとつながる限り、世界中から攻撃されるリスクへの対応がより重要となってくる。

(3) フェイク情報

フェイク情報（偽情報）は、誤解にもとづく誤情報とは異なり、特定の思想・信条や思惑、娯楽的な目的等で、意図的に発信された偽の情報である。情報拡散力の高いX（旧Twitter）といったソーシャルメディアによりフェイク情報が各段に広まりやすくなっており、生成AIの利用により本物と見間違えるほどの写真や映像が容易に作成できるようになったことも深刻なフェイク情報の氾濫につながっている。フェイク情報の拡散は組織外の出来事のため、組織内の情報セキュリティを中心に考えた場合はその対象外となるが、可能な範囲でインターネット上のミュージアムに関する情報の完全性を保ち、その情報にアクセス・利用する権限のある世界中の利用者がアクセス・利用できるようにするものと情報セキュリティを捉えた場合はその対象となりうる。ミュージアムの利用者に安心安全な来館体験と正確な情報を提供していくという点で、ミュージアムはフェイク情報への対応に積極的に取り組むことが求められるだろう。インシデント事例で取り上げた国立博物館のチケット購入サイトに見せかけたフィッシングサイトも組織外の出来事であるが、ミュージアムが注意喚起を行わざるを得ない状況であることと類似する。

フェイク情報に対して、インターネットを利用する広く一般の人々の情報リテラシーの向上が期待されるが、ミュージアムが実施可能な対応としては、偽サイトへの対応と同じく、SEO対策等によりGoogleといった検索エンジンの検索結果の上位にミュージアムの公式ウェブサイトが表示されるようにすること、公式ウェブサイトやソーシャルメディアなどあらゆる情報発信ツールを利用して注意喚起や正確な情報を発信することなどが考えられる。また、生成AIサービスがインターネット上のフェイク情報を情報源として学習し、利用者に二次的にフェイク情報を提供してしまう可能性や、情報不足を起因とするハルシネーションによって誤った情報を提供してしまう可能性を小さくするために、ミュージアムに関する正確な情報と、可能な範囲で多くのコレクションに関する情報を、生成AIサービスが参照できるような形でウェブサイトなどを介してインターネット上に提供していくことも考えられる。それは同時にインターネットを利用する広く一般の人々にフェイク情報を見分けるための信頼できる情報を提供する面をもつだろう。このようにミュージアムの情報を積極的に発信することもフェイク情報が氾濫する生成AI時代の情報セキュリティの対応として求められるだろう。

6. まとめ

本稿では、まず情報セキュリティの基本的な考え方や国内の取り組み状況を整理した。また、ミュージアムにおける情報セキュリティの対象となるミュージアムの情報について、コレクションに関する情報、ミュージアムの活動に関する情報、ミュージアムの管理運営に関する情報に区分して、その内容を明らかにした。そのうえで、ミュージアムの活動（管理運営を含む）に引き付けて、実際にミュージアムで発生した情報セキュリティインシデント事例を分析した。その結果、ミュージアムにおける情報セキュリティについて、ミュージアムの活動の中でも教育普及活動と情報発信活動において特に留意する必要があり、管理運営に係るインシデントはミュージアム全体の活動に深刻な影響を及ぼしうるという特徴と、ミュージアムの各活動における情報セキュリティの留意点を具体的に示した。また近年ミュージアムを取り巻くデジタル環境として、クラウドサービス、生成AI、フェイク情報について取り上げ、これからのミュージアムにおける情報セキュリティの対応について検討を行った。その中で、フェイク情報が氾濫する生成AI時代の情報セキュリティは、サイバー攻撃から防御するという広く一般に認識されている受け身の情報セキュリティだけではなく、ミュージアムに関する正確な情報と、可能な範囲で多くのコレクションに関する情報を、広く一般の人々や生成AIサービスが参照できるような形でウェブサイトなどを介してインターネット上に提供していくといった積極的な情報発信活動としての情報セキュリティが求められることを指摘した。

当館（皇居三の丸尚蔵館）は、令和8年（2026年）秋にリニューアルオープン（全面会館）を予定している。これまでより多様なミュージアムの活動が展開される見込みのため、本稿で取り上げたミュージアムにおける情報セキュリティの特徴や留意点、近年のデジタル環境を踏まえた情報セキュリティを考慮する場面が増えることが予想される。ミュージアムにおける情報セキュリティは、情報セキュリティ部門や担当者が単独で行う活動ではなく、ミュージアムの様々な活動を滞りなく進め、ミュージアムの社会的使命やそれぞれの設置目的を実現し、来館者に満足してもらうために必要な、ミュージアムの職員として備えておくべき基本的行動である。各個人はそれぞれのミュージアムの活動において、どのような情報／どのような関係者の情報を取り扱っているか自覚し、どのように取り扱うべきか情報セキュリティを考慮して活動することが求められる。ミュージアムにおける展示活動の情報セキュリティの留意点でも少し述べたが、特に美術系・歴史系ミュージアムにおいては、そのコレクションの資料等自体に人に関する情報が含まれる場合があるほか、作者やそのご子孫と著作権者等関係者、資料等の使用者、寄贈者、寄託者、資料等の背景にある思いや文化に関する情報があることを考慮して活動することが求められるだろう。

本稿で収集したミュージアムにおけるインシデント事例は、動物園や水族館の事例を含んでいるが、著者が所属する当館は美術系・歴史系のミュージアムであるため、ミュージアムにおける情報セキュリティに対する認識や捉え方は限定的である可能性がある。そのため、様々な種類のミュージアムや、ミュージアムと同じく知識インフラである図書館や公文書館等における情報セキュリティに対する認識や捉え方を比較することで、ミュージアムにおける情報セキュリティがより具体的かつ明確になる可能性がある[(註30)]。また、ICOM-SECURITYが対象とするミュージアムにおけるセキュリティの議論に情報セキュリティを積極的に位置づけることで相互に重要な視点を交換することができる可能性がある。

（みしま たいき　当館学芸部管理・情報課研究員）

註

(1) 三島大暉・澁谷完滋「皇居三の丸尚蔵館におけるITインフラの整備―ミュージアムDXに備えて」『尚蔵―皇居三の丸尚蔵館紀要』創刊号（通号30号）、2025年3月31日、p.68-65

(2) IPA「情報セキュリティ 10大脅威」
https://www.ipa.go.jp/security/10threats/index.html（2025-11-25アクセス）

(3) IPA「中小企業のためのセキュリティインシデント対応の手引き」（2023.4.26 Version 1.0）
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/security-incident.pdf（2025-11-25アクセス）

(4) e-Gov法令検索「サイバーセキュリティ基本法（平成二十六年法律第百四号）」
https://laws.e-gov.go.jp/law/426AC1000000104（2025-11-25アクセス）
(5) 国家サイバー統括室「政府機関等のサイバーセキュリティ対策のための統一基準群」https://www.nisc.go.jp/policy/group/general/kijun.html（2025-11-25アクセス）
(6) 総務省「地方公共団体における情報セキュリティポリシーに関するガイドラインの改定等に係る検討会」
https://www.soumu.go.jp/main_sosiki/kenkyu/chiho_security_r03/index.html（2025-11-25アクセス）
(7) IPA「中小企業の情報セキュリティ対策ガイドライン」
https://www.ipa.go.jp/security/guide/sme/about.html（2025-11-25アクセス）
(8) 大堀哲・水嶋英治編『新博物館学教科書　博物館学Ⅲ―博物館情報・メディア論＊博物館経営論』学文社、2012年、p.15、35
(9) 水嶋英治「1章　博物館情報学の三大原則」『博物館情報学シリーズ…1　ミュージアムの情報資源と目録・カタログ』樹村房、2017年、p.13-47
(10) 佐藤琴「第7章　博物館情報・メディア論」『現代博物館学入門』ミネルヴァ書房、2019年、p.215-244
(11) e-Gov法令検索「博物館法（昭和二十六年法律第二百八十五号）」
https://laws.e-gov.go.jp/law/326AC1000000285/（2025-11-25アクセス）
(12) ICOM日本委員会「新しい博物館定義、日本語訳が決定しました」2023-01-16
https://icomjapan.org/journal/2023/01/16/p-3188/（2025-11-25アクセス）
(13) 大堀哲・水嶋英治編、前掲書（註8）、p.164
(14) 株式会社三菱総合研究所「平成19年度　文部科学省委託　地域と共に歩む博物館育成事業　博物館における施設管理・リスクマネージメントに関する調査研究報告書　博物館における施設管理・リスクマネージメントガイドブック基礎編」
https://www.bunka.go.jp/seisaku/bijutsukan_hakubutsukan/shinko/hokoku/h19/（2025-11-25アクセス）
(15) “Museums in Danger: A closer look at cyber security”, IATM, 2024-04-23.
https://www.iatm.museum/museums-in-danger-a-closer-look-at-cyber-security/, (2025-11-25 Accessed).
(16) “Agenda ICMS Meeting, September 26th, 2024 at the Getty Villa, LA | 3:15pm until 5:00pm”, ICOM ICMS.
https://icms.mini.icom.museum/wp-content/uploads/sites/57/2024/09/ICMS2024_v3.pdf, (2025-11-25 Accessed).
(17) 大堀哲・水嶋英治編、前掲書（註8）、p.40、41、56-70
(18) 佐藤琴、前掲書（註10）
(19) 高田祐一「第6章　文化財デジタルデータの長期保存と管理」『デジタルアーカイブ・ベーシックス　デジタルデータの長期保存・活用　その理論と実践』勉誠社、2025年、p.168-183
(20) 阿児雄之「0-5-2. 博物館における情報倫理」『ミュージアムの未来をつくる　博物館情報・メディア論』美学出版、2025年、p.46-50
(21) 近年のミュージアムにおいては、チケット販売や入館予約の電子化が進み、映像システムなどを組み合わせた展示も広がっているため、情報システムの停止は発券・検札といった開館に必要な機能の停止や一部展示の中止につながりかねない。
(22) 総務省「令和6年度版　情報通信白書　第3章デジタルテクノロジーの変遷」
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r06/pdf/n1310000.pdf（2025-11-25アクセス）
(23) 総務省情報流通行政局地域通信振興課・自治行政局行政経営支援室「自治体におけるAI活用・導入ガイドブック〈別冊付録〉先行団体における生成AI事例集」（令和6年7月）
https://www.soumu.go.jp/main_content/000956981.pdf（2025-11-25アクセス）
(24) NTT Data「技術トレンド／展望　生成AI活用におけるセキュリティリスク対策の勘所」2025-01-15
https://www.nttdata.com/jp/ja/trends/data-insight/2025/0115/（2025-11-25アクセス）
(25) 染谷実奈美・菅和聖・大塚玲「生成AIの実社会への導入と乗り越えるべき壁（デジタルプラクティスコーナー）：生成AIのセキュリティリスクと研究動向」『情報処理』Vol.66、No.2、2025年1月15日、p.d36-d49
https://doi.org/10.20729/00241930（2025-11-25アクセス）
(26) mirai@city.fukuoka「福岡市博物館でAIによる施設案内」
https://mirai.city.fukuoka.lg.jp/project/1167/（2025-11-25アクセス）
(27) 日本科学未来館「対話型AIロボットの実証実験を実施」2025-08-08
https://www.miraikan.jst.go.jp/news/press/202508084183.html（2025-11-25アクセス）
(28) 森友亮「アート展レポート②森美術館「マシン・ラブ：ビデオゲーム、AIと現代アート」展」『人工知能』40巻、3号、2025年5月1日、p.380-383
https://doi.org/10.11517/jjsai.40.3_380（2025-11-25アクセス）
(29) Trend Micro「生成AIでランサムウェアを作成した容疑者の摘発事例を考察」2024-05-29（2025-05-01更新）
https://www.trendmicro.com/ja_jp/jp-security/24/e/breaking-securitynews-20240529-02.html（2025-11-25アクセス）
(30) 例えば、図書館における情報セキュリティについては次の論考が参考になる。

原田隆史「図書館におけるITインフラとセキュリティ：開かれた公共空間を守るための安全性と利便性のバランス」『情報の科学と技術』75巻、10号、2025年10月1日、p.476-487

表1の参照先一覧　※URLはいずれも2025-11-26アクセス

展示活動

Security NEXT「京都大学、博物館展示室で個人情報記載の展示資料を紛失」2006-06-13
https://www.security-next.com/003811
Security NEXT「GWパンダ観覧券の一部で他当選者名を記載―上野動物園」2018-05-08
https://www.security-next.com/093033
サイバーセキュリティ .com「委託先が誤送信で106名のアドレス流出、東京都歴史文化財団」2022-05-17（2022-05-18更新）
https://cybersecurity-jp.com/news/66797

教育普及活動

Security NEXT「ワークショップ参加者の個人情報含むUSBメモリを紛失―岐阜県の博物館」2010-05-31
https://www.security-next.com/012658
Security NEXT「館内PC9台にウイルスが混入、イベント参加者に感染のおそれ―鉄道博物館」2010-08-17
https://www.security-next.com/014149
Security NEXT「抽選結果通知メール誤送信でアドレス流出―神奈川県立歴史博物館」2014-03-07
https://www.security-next.com/047060
Security NEXT「市立動物園でメール誤送信、参加者のメアドが流出―神戸市」2015-07-24
https://www.security-next.com/060908
Security NEXT「上野動物園でメールの誤送信が発生―東京動物園協会」2021-08-10
https://www.security-next.com/128804
Security NEXT「案内状を誤送付、作業複雑化やチェック漏れ重なる―愛媛県美術館」2023-04-13
https://www.security-next.com/145351
Security NEXT「美術館でメール誤送信、講座応募者のメアド流出―稲沢市」2024-07-17
https://www.security-next.com/159707
Security NEXT「写真教室参加希望者宛のメールで誤送信―宮城県東北歴史博物館」2024-07-23
https://www.security-next.com/160054
Security NEXT「WS申込者の個人情報が閲覧可能に、設定ミスで―宇都宮美術館」2024-08-20
https://www.security-next.com/160942
サイバーセキュリティ .com「誤送信で51名分のメールアドレスが流出、NHK放送博物館」2019-02-13（2024-09-26更新）
https://cybersecurity-jp.com/news/29928
サイバーセキュリティ .com「大阪府立博物館で963名の個人情報を誤掲載、マニュアル欠如が原因か」2021-03-19（2024-09-24更新）
https://cybersecurity-jp.com/news/50467
サイバーセキュリティ .com「掛川市文化財団、電子メール誤送信でチケット購入者らのアドレス流出」2021-06-16
https://cybersecurity-jp.com/news/53731
サイバーセキュリティ .com「イベント関連メール誤送信で個人情報流出｜愛知県」2021-10-03
https://cybersecurity-jp.com/news/33670
サイバーセキュリティ .com「出水市、博物館職員が個人情報リストを39名に誤送信」2023-07-05（2024-09-25更新）
https://cybersecurity-jp.com/news/84943

情報発信活動

Security NEXT「東京国立近代美術館で開催された「ゴーギャン展2009」のサイトが改ざん」2010-02-04
https://www.security-next.com/011976
Security NEXT「「神戸ファッション美術館」のサイトが「Gumblar」亜種で改ざん」2010-05-13
https://www.security-next.com/012557
Security NEXT「奈良国立博物館のサイトが改ざん―尖閣関連でサイバー攻撃」2012-08-20
https://www.security-next.com/033104
Security NEXT「鳥取県立博物館のサイトが改ざん―個人情報漏洩は発生せず」2013-01-28
https://www.security-next.com/036803

Security NEXT「いしかわ動物園のサイトが改ざん被害―閲覧でウイルス感染のおそれ」2013-04-09
https://www.security-next.com/039084
Security NEXT「琵琶湖博物館のウェブサイトが復旧―アクセス集中で停止」2016-09-27
https://www.security-next.com/074229
Security NEXT「不正アクセスで個人情報が流出した「東京ズーネット」が復旧」2016-11-04
https://www.security-next.com/075430
サイバーセキュリティ .com「鳥羽水族館HPにサイバー攻撃、イルカ漁抗議を続けるアノニマスの犯行か」2017-05-31（2024-09-17更新）
https://cybersecurity-jp.com/news/15921
サイバーセキュリティ .com「滋賀の県立博物館ホームページやメールサーバーに障害発生｜不正アクセス原因」2025-05-30
https://cybersecurity-jp.com/news/109973
ScanNetSecurity「上野動物園でFAX誤送信、取材記録と報道機関の個人情報が漏えい（東京都、東京動物園協会）」2019-07-12
https://scan.netsecurity.ne.jp/article/2019/07/12/42619.html
セキュリティ対策Lab「東京国立博物館の偽サイト（フィッシングサイト）に注意」2025-07-02（2025-09-30更新）
https://rocket-boys.co.jp/security-measures-lab/tokyo-national-museum-phishing/
朝日新聞「各地の自治体ホームページに障害　アクセスできず、エラーメッセージ」2024-07-30
https://www.asahi.com/articles/ASS7Z0HBNS7ZUTIL001M.html
茨城新聞クロスアイ「茨城県陶芸美術館　135人分の個人情報漏えいの可能性　広報委託先にサイバー攻撃」2025-05-09
https://ibarakinews.jp/news/newsdetail.php?f_jun=17467923969517

コミュニティ活動

Security NEXT「横浜美術館で個人情報が流出―市へ報告せず公表遅れる」2007-12-21
https://www.security-next.com/007349
サイバーセキュリティ .com「電子メール誤送信で222件のメールアドレス漏えい｜国立科学博物館」2024-07-29
https://cybersecurity-jp.com/news/98460
ScanNetSecurity「会員台帳更新作業中に他会員のアドレスに変更～天王寺動物園でメール誤送信」2025-04-24（2025-04-26更新）
https://scan.netsecurity.ne.jp/article/2025/04/24/52744.html
セキュリティ対策Lab「セキュリティインシデント　事例【2022年】｜電子メール誤送信による個人情報の漏えい事例｜大阪歴史博物館（2022年6月）」2024-08-16（2024-08-17更新）
https://rocket-boys.co.jp/security-measures-lab/security-incidents-case-study-2022/

管理運営

Security NEXT「個人情報を誤表示、アクセス集中による不具合で―うみの杜水族館」2015-05-21
https://www.security-next.com/058539
Security NEXT「新潟県立近代美術館に不正アクセス―スパムの踏み台に」2022-02-28
https://www.security-next.com/134418
Security NEXT「電車内で機密文書が盗難被害、その後回収―名古屋市美術館」2023-05-30
https://www.security-next.com/146504
Security NEXT「付属美術館の端末から個人情報が流出した可能性―尾道市立大」2024-12-18
https://www.security-next.com/165355
Security NEXT「新潟県立近代美術館でメール誤送信―後任担当者が気付く」2025-04-09
https://www.security-next.com/169117
サイバーセキュリティ .com「国立科学博物館のメール関連システムが不正アクセス被害」2023-10-24
https://cybersecurity-jp.com/news/90387
セキュリティ対策Lab「パリ　オリンピック期間中にグラン・パレ美術館や複数の施設へサイバー攻撃」2024-09-06（2024-09-07更新）
セキュリティ対策Lab「大英博物館、解雇された元職員がシステムを破壊　一部展示が中止に」2025-01-27（2025-01-31更新）

謝辞

本稿では、表1の社会動向および註21に関して当館総務課情報システム係長・澁谷完滋氏よりご助言をいただいた。ここに記して深く感謝申し上げます。

本紀要の投稿原稿は、編集委員会において査読を経た審査をし、採用決定したものを掲載しています。

掲載内容は、収蔵品および館の業務に関わるものを題材とし、関連諸学（美学・美術史学、歴史学、考古学、博物館学、博物館教育、博物館情報、保存科学等）における研究、および上記以外の館の活動に関わる事業・事例等報告とします。

このうち、事業・事例等報告や調査概報については、査読はないものとします。

尚蔵——皇居三の丸尚蔵館紀要　第二号（通号三一号）
二〇二五（令和七）年度

編集・発行　独立行政法人国立文化財機構
皇居三の丸尚蔵館
東京都千代田区千代田一―八

制作　株式会社アイワード
北海道札幌市中央区北三条東五―五―九一

翻訳　株式会社 Dosh in EC

二〇二六年三月三〇日発行