Monday (November 11th)	Track A	Track B	Track C	Track D
	Venue: [Palace Hall East]	Venue: [Palace Hall West]	Venue: [Crown]	Venue: [Lilac]
09:45 A.M. - 10:00 A.M.	**Opening**			
10:00 A.M. - 11:00 A.M.	**A1-1-Keynote** **M3AAWG, AI, and the future of anti-abuse** The Messaging, Malware, and Mobile Anti-Abuse Working Group (M3AAWG) is an organization that brings the industry together to develop best practices and fight online abuse. Members collaborate to address existing and emerging threats, which now include AI. AI is already being used as an attack vector but can also be used in our work fighting online abuse. Sharon Kent (Co-Vice Chair, Board of Directors, M3AAWG)			
11:00 A.M. - 00:00 P.M.	**A1-2-Keynote** **Google Bulk Sender Guide line** Major mailbox providers have stepped up to fight email abuse. Gmail's Security Manager explains the purpose and implementation details of No auth No entry action for bulk senders. Emil Gustafsson (Google LLC)			

Monday (November 11th)	Track A Venue: [Palace Hall East]	Track B Venue: [Palace Hall West]	Track C Venue: [Crown]	Track D Venue: [Lilac]
00:00 P.M. - 01:00 P.M.	**A1-Lunch** **Global Threat Report Commentary** The cybersecurity environment in recent years has seen a wide range of important developments that have a significant impact on the digital attack surface. Most notable of these is the increase in advanced targeted attacks against large organizations and critical infrastructure. This session will explore the most prevalent email-related threats globally. Fumiaki Ito (Fortinet, Inc.)			**D1-Lunch** **Consultation session** This is a lunch session where people involved in email operations can discuss their everyday concerns. By interacting with not only JPAAWG members but also other participants, you may be able to share your concerns and come closer to a solution. There will be no presentations prepared, and the session will be centered around an open mic. Please feel free to join us while eating lunch. Masaki Kase (TwoFive, Inc.) Hibiki Tazawa (EmberPoint Co., Ltd.)
01:00 P.M. - 02:00 P.M.	**A1-3** **The current state of phishing and countermeasures (2024)** Phishing damage continues to increase, with a record high of about 180,000 reports received in July 2024. The methods of lure and fraudulent use are also constantly changing, and the cat-and-mouse game of countermeasures and avoidance continues, so various organizations need to cooperate with each other to respond. In the first half of this session, we will talk about the latest trends in phishing and the distribution status and countermeasures of phishing emails, which account for the majority of lures, and in the second half, we will talk about the phishing countermeasures activities that JC3 is working on, including activities to promote awareness of takedown execution, and recent trends in smishing. Nobuyo Hiratsuka (JPCERT/CC) Go Kajikawa (JC3 Japan Cybercrime Control Center)	**B1-3** **Lightning Talks 2024** The Lightning Talks will be held again this year. What kind of opinions and thoughts from new perspectives will emerge? This time, not only will there be talks by JPAAWG members, but general participants will also be able to participate. This is an on-site only session, but please come to the venue!	**C1-3** **The evolution of hacktivism and recent hacktivists** Hacktivists are threat actors who carry out politically motivated hacking and cyber attacks. In recent years, in addition to hacktivists with a relatively long history such as Anonymous, many hacktivists associated with war and conflict have appeared, and many cases of attacks on Japanese companies and organizations have been observed. In this presentation, we will share the results of our research on the characteristics of hacktivists and their recent activities. First, we will review the evolution of hacktivism from its birth to the present, and show the traditional values of hacktivists. Next, we will report the results of our research on hacktivists active in recent years and their activities. Based on recent cases, we will show what kind of beliefs hacktivists have and what kind of organizations are likely to be targeted. Finally, we will analyze and introduce the recent activities of hacktivists on social media. Here, we will show that hacktivists have a strong obsession with repercussions for their attacks, and that caution is required when publishing information about outages and sharing information. Hiromasa Saito (LY Corporation)	**D1-4** **How to deal with RBL and improve email deliverability** In order for the email you send to reach its destination, it is important to follow the Google guidelines and M3AAWG Sender BCP, but it is also important to know how to deal with RBLs (Real time Block Lists) such as Spamhaus. In this session, we will share the manners and know-how you need to keep in mind to improve email deliverability. Nobuhiro Suemasa (JPAAWG Secretary General)

Monday (November 11th)	Track A Venue: [Palace Hall East]	Track B Venue: [Palace Hall West]	Track C Venue: [Crown]	Track D Venue: [Lilac]
02:00 P.M. - 03:00 P.M.	**A1-4** We will be introducing the latest trends in spam messages that Proofpoint (Cloudmark Team) has analyzed over the past year. Proofpoint Japan K.K.	**B1-4** **Is it difficult to comply with BIMI? Panel discussion by companies complying with BIMI** BIMI (Brand Indicators for Message Identification) has the function of displaying a logo mark on emails that have been successfully DMARC authenticated. As a technology that can communicate DMARC results in a way that is understandable to end users, an increasing number of companies in Japan, particularly in the e-commerce and financial fields, are adopting it. In this session, we will invite people from companies that have implemented BIMI to talk about the know-how, effects, and difficulties of BIMI adoption in a panel discussion format. Teruaki Homma (JSSEC/KDDI CORPORATION) Masato Hayashi (DigiCert Japan G.K.) Kanae Takata (Rakuten Group, Inc.)	**C1-4** **Operational Best/Bad Practices** Not only for email settings and operations, but for various operations and configuration topics, there are some things that used to be standard methods but have changed as circumstances have changed them from "recommended" to "better not do this." In this session, we will focus on such bad practices that "used to be common sense, but now..." and overwrite your knowledge by updating it with "these days...". That said, I think there are various perspectives on how "practices" are evaluated, so I hope to come up with ideas and discuss "practices" together with the audience. Manabu Kondo (Parongo Corporation)	**C1-4** **Tabletop exercises for dealing with fraudulent websites – lessons learned to overcome fraudulent websites** The Anti-Phishing Council has developed a "Tabletop Exercise Kit for Dealing with Fraudulent Sites." This is one of the measures aimed at giving business operators who adopt a "brand strategy" the opportunity to develop a playbook and gain awareness, even if they have never been a victim of fraud. Participants in this workshop will form impromptu teams and participate in tabletop exercises in groups. In the exercise, a fictitious company (BtoC business) will encounter a wide range of fraud incidents. Participants will play the role of employees and discuss the basic flow of incident response, how to report to management, and how to request a response. Noriaki Hayashi (Council of Anti-Phishing Japan)
03:00 P.M. - 03:15 P.M.	Coffee Break			
03:15 P.M. - 04:15 P.M.	**A1-5**	**B1-5** **Telecommunications carriers' approach to DMARC countermeasures against spoofed emails** DMARC is said to be effective against domain spoofing, which is often used in phishing emails that have been attracting attention recently, but have you completed the countermeasures by setting p=none in the DMARC record? Recently, it seems that p=none domains are being used by spammers to send spoofed emails. So what does it mean to "support DMARC"? We will introduce the response of telecommunications carriers and future plans. Kenichiro Masaki (NTT DOCOMO) Akio Kumazawa (SoftBank Corp.) Naoki Nakajima (KDDI CORPORATION)	**C1-5** **Transparent SMTP proxy for improved visibility into outgoing email** For mail hosting and cloud vendors, the decline in IP reputation is an issue due to users' mail accounts being used to send spam mail. A decline in IP reputation leads to an increase in recovery work and operational costs. In this session, we will propose a method to solve this problem by processing outgoing mail with a transparent SMTP proxy. We will also introduce the results of a demonstration experiment, the unique advantages and disadvantages of a transparent proxy, and future challenges. Tomohisa Oda (SAKURA Internet Research Center)	**C1-5** **Tabletop exercises for dealing with fraudulent websites – lessons learned to overcome fraudulent websites** The Anti-Phishing Council has developed a "Tabletop Exercise Kit for Dealing with Fraudulent Sites." This is one of the measures aimed at giving business operators who adopt a "brand strategy" the opportunity to develop a playbook and gain awareness, even if they have never been a victim of fraud. Participants in this workshop will form impromptu teams and participate in tabletop exercises in groups. In the exercise, a fictitious company (BtoC business) will encounter a wide range of fraud incidents. Participants will play the role of employees and discuss the basic flow of incident response, how to report to management, and how to request a response. Noriaki Hayashi (Council of Anti-Phishing Japan)

Monday (November 11th)	Track A Venue: [Palace Hall East]	Track B Venue: [Palace Hall West]	Track C Venue: [Crown]	Track D Venue: [Lilac]
04:15 P.M. - 05:15 P.M.	**A1-6** **Gathering of operators supporting email services Fall 2024 (Part 1)** This is a panel session that has become a regular feature of every event. People who operate systems related to email, such as email sending services and ISP email services, will talk about their operational know-how and struggles! Mihyon Hirano (QUALITIA) Hayato Serizawa (Internet Initiative Japan Inc.) Katsuyuki Takeuchi (CyberSolutions Inc.) Yu Hirokawa (GMO Pepabo, Inc.)		**C1-6** **Security incident consultation service begins operation** Targeted attacks, ransomware attacks, phishing, DDoS... How do you respond to cyber attacks that you may encounter when using the Internet? There may be cases where you just endure them without being able to consult with anyone, or ask for help from those around you but get no response. Recently, cyber attacks have become more sophisticated and are exceeding the level that a single organization or individual can face and deal with. JPCERT/CC has opened a consultation desk for people, companies, and vendors who are suffering from cyber attacks. Since opening, we have received several consultations. In this presentation, we will introduce the background to the establishment of the consultation desk and how it is used, along with actual examples, including how JPCERT/CC responded to consultations based on actual consultations received. Shoko Nakai (JPCERT/CC)	
05:15 P.M. - 06:15 P.M.	**A1-7** **IIJ's new initiative "Defensive Response"** There is no end to the cases where email services are misused to send phishing (fraudulent) emails. From the perspective of ISPs, identifying these hijacked accounts and stopping the sending of spam emails is a daily headache. Users can also be victims and perpetrators as their email accounts are misused without their permission. In this session, we will introduce new measures that IIJ has undertaken to put an end to this battle. Isamu Koga (Internet Initiative Japan Inc.)	**B1-7** **SMS phishing (smishing) prevention panel** Damage caused by phishing attacks is increasing year by year, and recently, damage caused by attacks using short messages and SMS has become serious. One of the reasons for this is thought to be that short messages are being used for multi-step and multi-factor authentication due to stricter login authentication for Internet services, making them a valuable communication infrastructure for attackers. We will talk about the latest information on countermeasures taken by mobile carriers. Sakiko Mitani (NTT DOCOMO) Hideyuki Koto (KDDI CORPORATION) Keisuke Honda (Rakuten Mobile, Inc.) Tatsuhiko Matsuzaki (SoftBank Corp.)	**C1-7** **Hatena's email infrastructure and DMARC support** In August 2023, Gmail announced new sender guidelines. For various reasons, Hatena operates an email infrastructure that combines Sakura Cloud and Amazon ECS Anywhere. In this presentation, we will talk about the measures Hatena is taking to comply with DMARC, how to monitor compliance status using Grafana, CloudWatch, and Mackerel, and DMARC-related RFCs that you should be aware of. Mitsuru Takigahira (Hatena Co., Ltd.)	
06:30 P.M. - 08:00 P.M.	**Social gathering** **Venue: Hotel Emisia Sapporo 2F Pastel**			

Tuesday (November 12th)	Track A Venue: [Palace Hall East]	Track B Venue: [Palace Hall West]	Track C Venue: [Crown]	Track D Venue: [Lilac]
09:45 A.M. - 10:00 A.M.	**A2-Orientation** In the Open Round Table session, participants actively participate in a discussion on a single topic, and the session owner summarizes the discussion. During the orientation, we will explain the rules before participating and how to have a good discussion.			
10:00 A.M. - 11:00 A.M.	**A2-1** **The difficulties of migrating to a new email service and a recommendation for "new-age email"** KDDI not only provides carrier email, but also fixed-line ISP email and corporate email services. We will talk about the difficulties faced in various cases of email service migration, and what we feel while providing a wide variety of email services. What are the email service specifications that are suitable for the current era? 曽我 展世 (KDDI CORPORATION) Masashi Watanabe (KDDI CORPORATION)	**B2-1** **Measures against improper use of telecommunications services (Ministry of Internal Affairs and Communications)** We will introduce the Ministry of Internal Affairs and Communications' measures against spam emails and fraudulent phone calls. Seira Tanaka (Ministry of Internal Affairs and Communications) **Initiatives to ensure safety and security in a cashless society (National Police Agency)** While many people enjoy the benefits of "cashless" in their daily lives, the amount of cashless payments used daily is increasing year by year. On the other hand, when we look at the damage caused by a cashless society, the threats in cyberspace are becoming more serious, with the amount of damage caused by fraudulent use of credit cards and fraudulent transfer damage via internet banking reaching an all-time high last year. In this seminar, we will explain the current situation surrounding cyberspace and introduce the efforts of the National Police Agency to ensure safety and security in a cashless society. Maroka Neki (National Police Agency.)	**C2-RT1** **Open Round Table** **Topic 1: What to be careful of when using DKIM** As DMARC has been introduced since the end of last year, it has become necessary to support DKIM signatures when sending emails and related operations. Let's discuss together the issues, tips, and points to note related to DKIM, which we have not paid much attention to until now.	**D2–RT1** **Open Round Table** **Topic 2: How to know about and prevent “EchoSpoofing”** We will look back at what actually happens with EchoSpoofing, a technique reported in July 2024 that sends spam emails that legitimately bypass sending domain authentication, and discuss countermeasures against this technique.

Tuesday (November 12th)	Track A Venue: [Palace Hall East]	Track B Venue: [Palace Hall West]	Track C Venue: [Crown]	Track D Venue: [Lilac]
11:00 A.M. - 00:00 P.M.	**A2-2** **Talk about recent trends in SPAM and phishing** TwoFive members will talk about the latest trends in SPAM and phishing emails and the insights they have gained in the process of analyzing them. Naoya Takahashi (TwoFive, Inc.) Tomohiko Sasaki (TwoFive, Inc.) Jumpei Oki (TwoFive, Inc.)	**B2-2** **The threat of cyber attacks involving nation-state actors (Public Security Intelligence Agency)** This seminar will discuss the characteristics of state-sponsored and state-sponsored cyber attacks, including recent trends related to Volt Typhoon, the activities of North Korean IT engineers, and targeted email attacks carried out by states. Ippei Toyama (Public Security Intelligence Agency) **Overview of the Ministry of Internal Affairs and Communications' ICT Cybersecurity Policy and Three Guidelines (Ministry of Internal Affairs and Communications)** As the importance of cybersecurity increases, we will introduce the latest initiatives being promoted by the Ministry of Internal Affairs and Communications. In the first half, we will explain the background and objectives of the cybersecurity-related projects being carried out by the Ministry of Internal Affairs and Communications. In the second half, we will provide an overview of the guidelines for three network security technologies, RPKI, DNSSEC, and DMARC, which were investigated and considered through the Ministry of Internal Affairs and Communications project. These guidelines were compiled based on the challenges and necessary information faced by demonstration operators when introducing and operating the technologies, and were formulated based on common challenges and concepts. Ministry of Internal Affairs and Communications Hirohisa Ogawa (Mitsubishi Research Institute, Inc.)	**C2-RT2** **Open Round Table** **Topic 1: What to be careful of when using DKIM** As DMARC has been introduced since the end of last year, it has become necessary to support DKIM signatures when sending emails and related operations. Let's discuss together the issues, tips, and points to note related to DKIM, which we have not paid much attention to until now.	**D2-RT2** **Open Round Table** **Topic 2: How to know about and prevent “EchoSpoofing”** We will look back at what actually happens with EchoSpoofing, a technique reported in July 2024 that sends spam emails that legitimately bypass sending domain authentication, and discuss countermeasures against this technique.

Tuesday (November 12th)	Track A	Track B	Track C	Track D
	Venue: [Palace Hall East]	Venue: [Palace Hall West]	Venue: [Crown]	Venue: [Lilac]
00:00 P.M. - 01:00 P.M.	**A2-Lunch** **Current status of "sender domain authentication" after applying "sender guidelines"** **Sharing "real customer information" gained from a configuration support negotiation held in a webinar with over 400 applicants** On June 1st, Google's revised mail sender guidelines were applied, and we have been receiving many inquiries from customers saying, "I can no longer send mail to Gmail." How advanced is sending domain authentication in the Japanese market? What is the situation, particularly with customers with low IT literacy and small and medium-sized enterprises? We would like to share the "realities of our customers" at this point in time using the data below and consider how to popularize it. - Contents of the survey and Q&A at the emergency webinar held in August with over 400 participants - Customer feedback from the SPF/DKIM/DMARC setting support service we actually implemented - Differences between customers who were told the same work fee was high and those who were told it was low, etc. Yasunori Tsujimura (QUALITIA)			**D2-Lunch** **More! Lightning Talks 2024** In addition to the lightning talks on the first day, we will also be holding a lunch LT!

Monday (November 11th)	Track A Venue: [Palace Hall East]	Track B Venue: [Palace Hall West]	Track C Venue: [Crown]	Track D Venue: [Lilac]
01:00 P.M. - 02:00 P.M.	**A2-3** **Email and AI Series: Next-generation technology for privacy protection: The future of NLP and how to use large-scale language models** This presentation will provide a detailed explanation of data privacy and anonymization technologies, which are important for email security providers. We will introduce the basic concepts of data anonymization, specific technologies and methods, and explain their advantages and trade-offs. We will also explain the characteristics of small language models and large language models, and how each is used to anonymize email data. In particular, we will focus on the importance of prompt engineering in LLM and its specific methods, and will also provide a demonstration using actual prompts. We will also touch on LLM adapter technology. We will consider the possibility of applying it to email data anonymization, and introduce the results of applying it to actual email data. Yoshihisa Hirano (Vade Japan) Nuwan Senevirathne (QUALITIA)	**B2-3** **The impact of Google guidelines: A look into what has changed!** The new email sender guidelines announced by Google and Yahoo! in 2023 will affect many organizations. In this session, we will discuss with panelists the current status and challenges of email on the ground, based on the results of a survey conducted mainly among companies that use email on a daily basis. Genki Taniguchi (SAKURA internet Inc.) Rina Heito (SPIRAL Inc.) Daisuke Kodama (CyberSolutions Inc.) Yuri Nawata (OpenWave)	**C2-3** **Domain names used for phishing, past and present** In the past, URLs used to direct users to phishing sites have often used brand imitation strings to deceive users. However, the methods have changed significantly, making it difficult to detect them or take countermeasures using traditional methods. Based on the results of an analysis of the phishurl-list provided by JPCERT/CC, we will show the actual situation and explain what should be considered in terms of detection and countermeasures. Tsuyoshi Taniguchi (FUJITSU DEFENSE & NATIONAL SECURITY LIMITED) Kazumi Suzuki (Macnica, Inc./Council of Anti-Phishing Japan)	**D2-3** **DMARC Beginners Course** The training content will be updated at a later date. Shuji Sakuraba (JPAAWG leader)
02:00 P.M. - 03:00 P.M.	**A2-RT4** **Open Round Table Overall Summary** The contents of the discussions at the two tables will be summarized and reported and shared by each session owner. Yoshihisa Hirano (Vade Japan) Masaki Kase (TwoFive, Inc.) Yusuke Imamura (Internet Initiative Japan Inc.)	**B2-4** **Phishing Hunter (Hokkaido Talk Night)** We're doing it again this year! The Phish Hunter Panel! Phishing hunters, who conduct research on the front lines, will talk about the latest phishing scam trends and things you should be careful of when it comes to phishing scams. にゃんたく KesagataMe つぼっく サイバー侍KAZUMI	**C2-4** **Collaboration efforts and DMARC introduction in Hokkaido municipalities** Thanks to the efforts of the Hokkaido Prefectural Government and other organizations, the adoption rate of DMARC among municipalities in Hokkaido is now nearly 100%, but I would like to talk about how this adoption was promoted. Naoya Tajima (HOKKAIDO GOVERNMENT)	**D2-4** **How does email arrive? RFC review: SMTP** This is the second training session in which we review the basics of email by looking at source material. Last time, we looked at common mistakes people make when formatting email messages. This time, we'll review the definition of SMTP and aim to understand how email gets to the recipient's mailbox. Akihiro Sekine (Vade Japan)
03:00 P.M. - 03:15 P.M.	Coffee Break			

Tuesday (November 12th)	Track A Venue: [Palace Hall East]	Track B Venue: [Palace Hall West]	Track C Venue: [Crown]	Track D Venue: [Lilac]
03:15 P.M. - 04:15 P.M.	**A2-5** **Live reports from France ~ Summary of email threats at the Paris Olympics. What kind of cyber attacks occur at global events?** As a company with origins in France, we will be sharing live information on cyber threats surrounding the Paris Olympics. Global events such as the Olympics are inevitably targets of cyber attacks. With the Osaka-Kansai Expo scheduled for next year in Japan, please use this as a reference for countermeasures. Iyona Izumida (Vade Japan)	**B2-5** **Domain life cycle** **Domain management at NTT Docomo** We will introduce our response to the "Docomo Account Domain Auction Listing" and the current state of Docomo's domain management in response to this. Mirai Miura (NTT DOCOMO) Miki Takata (dnsops.jp/NTT Communications Corporation)	**C2-5** **JPAAWG BoF** We will introduce JPAAWG's organization and past activities, as well as explain JPAAWG's future policies and the procedure for joining. During the Q&A session at the end of the session, we would like to hear from participants about their requests and expectations for JPAAWG. We would appreciate your valuable opinions. If you have any questions about what JPAAWG does, or if you are interested in JPAAWG's activities, we look forward to your participation. Shuji Sakuraba (JPAAWG leader) Nobuhiro Suemasa (JPAAWG Secretary General) Hibiki Tazawa (JPAAWG) Yuri Nawata (JPAAWG)	
04:15 P.M. - 05:15 P.M.	**A2-6** **Gathering of operators supporting email services Fall 2024 (Part 2)** This is a panel session that has become a regular feature of every event. People who operate systems related to email, such as email sending services and ISP email services, will talk about their operational know-how and struggles! Rihito Kato (BIGLOBE Inc.) Haruhiko Uchida (COMMUNITY NETWORK CENTER INCORPORATED.) Toshitaka Miura (FreeBit Co., Ltd.) Daichi Kitagawa (JCOM Co., Ltd.) Daiki Watanabe (KDDI CORPORATION) Ryo Saita (NTT DOCOMO)			
05:15 P.M. - 05:30 P.M.	**Closing**			