

日本のサイバーセキュリティを「連携」「学び」「創造」



# JNSA国際連携部会2025年度活動計画

2025,7,25

NPO法人日本ネットワークセキュリティ協会

国際連携部会 伊藤 整一

# 目 次

---

## I. プロローグ

1. AJCCA
2. ASOCIOと市場連携

## II. 国際連携部会について（振り返り）

1. 設立趣意
2. 活動目的

## III. 2024年度の国際連携部会の活動報告

1. 活動方針
2. 活動結果

## IV. 2025年度の活動方針案及び計画について

1. 活動方針
2. 活動計画

## V. その他連絡事項

1. 「第二回AJCCAカンファレンス in Tokyo」の開催

# 「AJCCA創立による国際官民連携の基盤確立とその可能性について」

～ 国際環境におけるJNSAの役割 ～

－ ASEAN各国の官民連携の実現に向けて －

JNSAは昨年10月に結成された日ASEAN 10ヶ国のサイバーセキュリティ業界民間団体アライアンス

「AJCCA」の副会長協会としての活動を通して、ASEAN各国の民間協会連携による市場開放に寄与するだけでなく、NCOが主催する「日ASEANサイバーセキュリティ政策会議」と連動することによりASEAN地域のサイバーセキュリティに関する「官民連携」体制構築の支援を行っています。

# MOU締結

ASEANと日本の9つのサイバーセキュリティ・コミュニティ  
2023年10月5日にMOUを締結 → 2025年現在10ヶ国



<https://www.japantimes.co.jp/news/2023/10/05/japan/japan-asean-cybersecurity/>

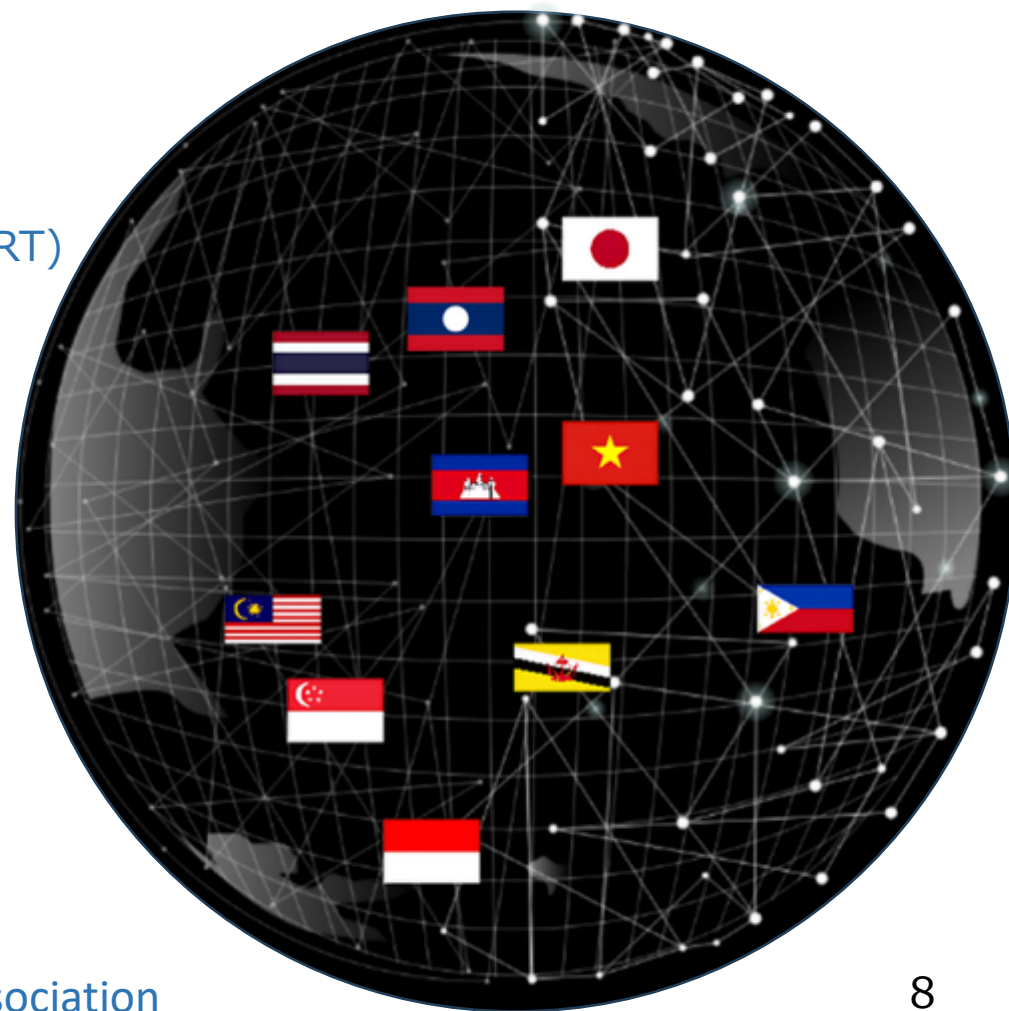
Copyright Japan Network Security Association

**JNSA**

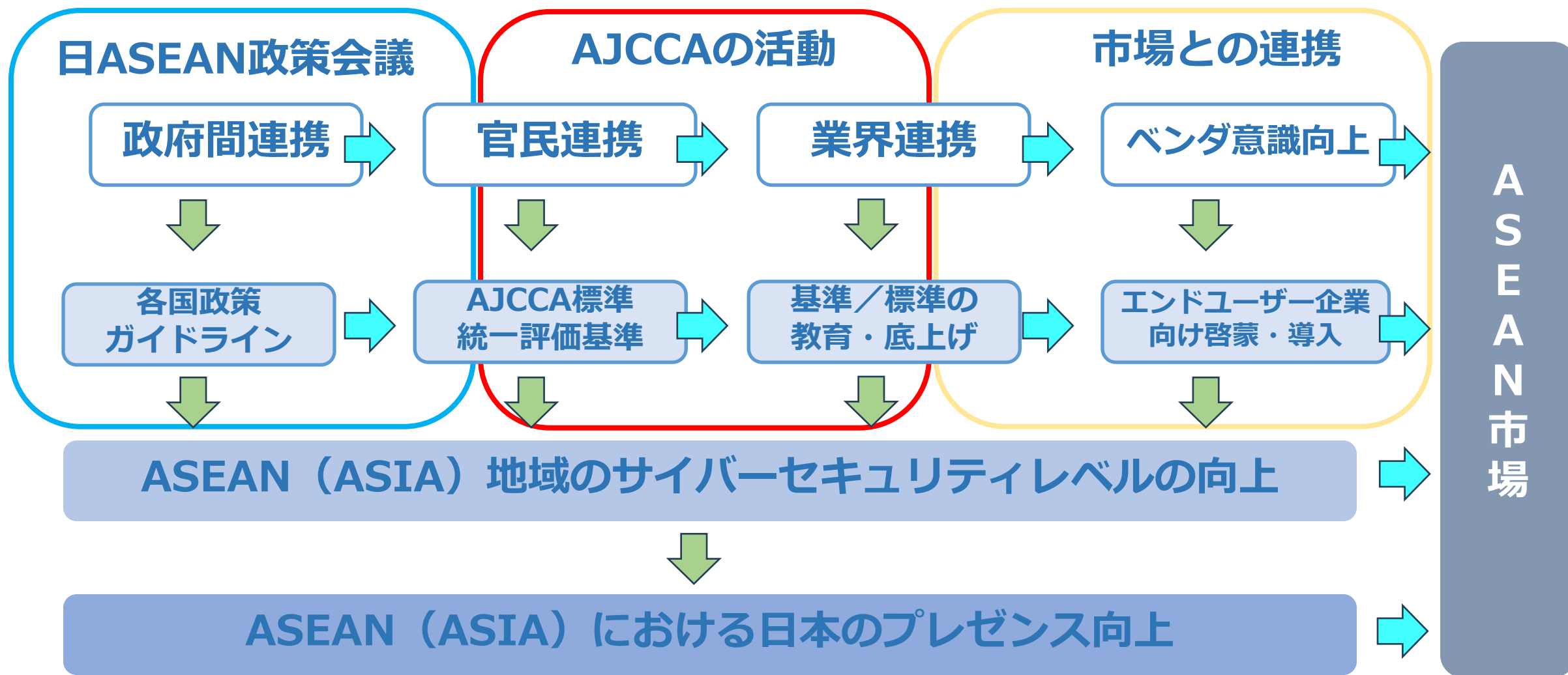
# アライアンスの設立

- 1.Brunei - Brunei Cyber Security Association (BCSA)
- 2.Cambodia - ISAC-Cambodia
- 3.Indonesia - Indonesia Network Security Association (idNSA)
- 4.Japan -日本ネットワークセキュリティ協会 (JNSA)
- 5.Malaysia -Malaysia CyberSecurity Community ( rawSEC)
- 6.Philippine - Philippine Computer Emergency Response Team (PH-CERT)
- 7.Singapore - Association of Information Security Professionals (AiSP)
- 8.Thailand - Thailand Information Security Association (TISA)
- 9.Vietnam - Japan Network Security Association (VNISA)
- 10.Laos - Lao Cybersecurity Community (LCSC) 2024年10月～

ASEAN Japan Cybersecurity Community Alliance  
(AJCCA) のアライアンス名称に、全ての締結組織が  
MOU締結後に合意した。



# ASEANサイバーセキュリティ環境における連携の可能性



## ▶ ASOCIOについて

ASOCIOは、アジア・オセアニア24ヶ国のDX、AI、IoT、サイバーセキュリティなどのITサービスを提供する関連企業団体が加盟する組織。設立から40年を迎える。

企業会員数の合計は約18,000社。（24ヶ国）（JISAが共同創立）  
ASEAN地域の10ヶ国においては、約5,500社以上のITサービスベンダー企業会員

また、ビジネス市場が既に確立されているため、エンドユーザーへの直接アプローチが可能。

市場には製品やサービスへの既存の需要があり、それらを消費者に直接提供するためのメカニズムやチャネルも整っている組織です。

ASOCIO: <https://www.asocio.org>

## Ⅱ．国際連携部会について

### 1. 設立趣意 **国際連携（業界・官民・市場）**

～冒頭省略～

会員企業の海外連携のニーズと施策を検討するとともに、関係省庁からの情報収集と協調を行う。  
また、各国サイバーセキュリティ関連団体の情報収集と連携を行い、我が国の国際連携の一翼を担い、ひいては会員企業の海外進出やセキュリティ人材の確保に資する活動を定着させる。

### 2. 活動目的

#### ①**各国団体との定期交流（MOUベース） - 活発なコミュニケーション**

- ・ 国対国：韓国（KISIA）シンガポール（AiSP）インドネシア（idNSA）
- ・ 対ASEAN:AJCCA（**10ヶ国連合**）

#### ②**情報共有 国内・海外**

- ・ JNSAの方針政策を海外へ発信
- ・ 国内外の政策共有
- ・ 国内外のインシデント共有
- ・ 海外イベント情報の共有

#### ③**コンテンツの共有 - 各国間**

- ・ 各国協会の所有するコンテンツの共有プラットフォーム

#### ④**JNSA内のWGとの連携（役割別）**

## Ⅲ. 2024年国際連携部会の活動報告

### 1. 2024年度の活動方針

- ・基本方針 ➡ **国際連携活動情報の適時公開** （メーリングリスト、Slack）
- ・AJCCA副会長協会として理事会運営 **(C10)** に参加。（江崎会長、伊藤、永野氏）
- ・年4回 AJCPM & WG会議と連動 ※ AJCPM: 日ASEANCS政策会議

### 2. 2024年度の活動結果

- ・4回のAJCPM国際会議及びAJCCA理事会に参加した  
タイ（2月）、カンボジア（5月）、大阪（8月OT/WGより中尾副会長及び佐々木氏講演）、シンガポール（10月）
- ・「第一回AJCCAカンファレンス2024 in Singapore」への参加  
JNSAからの参加 ➡ OT/WGより藤原氏講演、NTTテクノクロス様、GMO様  
JNSAからのアワード受賞者 ➡ 江崎会長、中尾副会長
- ・JNSAコンテンツの英語版をAJCCAサイトにて共有

# ① AJCCA Conference 2024 in Singapore - レポート

Date: 17 Oct 2024

Venue: Suntec Singapore Convention & Exhibition Centre



AJCCA会長 Rudi Lumanto博士による開会挨拶



Rahayu Mahzam氏  
シンガポール政府  
デジタル開発・情報省大臣



佐々木淳一企画官  
NISC



Sounetto XAPHAKDY氏  
Deputy Director General, Department of  
Cyber Security, Ministry of Technology and  
Communications, ラオス



Nicholas Lee氏  
SGTech 会長 - ASOCIO



## IV. 2025年度の活動計画

### 1. 2025年度の活動方針

- ・情報発信 ➡ 情報発信 + 具体的な活動へ

### 2. 2025年度の活動計画

※ NCO : 国家サイバー統括室 (旧NISC)

#### ①参加予定会議 NCOのAJCPMとの連動

- ・ 5月 : AJCCA Board Meeting (フィリピン) 終了
- ・ 8月 : AJCCA Board Meeting (インドネシア) + CIIPワークショップ
- ・ 10月 : 「**第2回AJCCAカンファレンス in 東京**」 (JNSA主催)
- ・ 10月 : **AJCCA Board Meeting & 年次総会 (AGM) in 東京**
- ・ 2026年2月 : AJCCA Board Meeting (マレーシア) + **ワークショップ (テーマ企画中)**

#### ②その他の活動

- ・ AJCCA TI/WG が発刊する「CTIレポート」のJNSA会員への共有 (英語版)
- ・ JNSA OT/WGの活動とAJCCAとの連携窓口
- ・ AJCCA連携WGを設置 (案) ⇒ 「**第2回AJCCAカンファレンス in 東京**」の開催運営

# AJCCA-TI/WG Activities

## 脅威情報の共有

### AJCCA - Threat Intelligence Report

#### Oracle Cloud Data Breach Threat Actor

**Date:** 15 April 2025  
**Source:** cloudsek.com  
**Prepared and Analyzed by:** IdNSA  
**TLP :** GREEN  
**Appendix :** -

#### Executive Summary

In March 2025, a significant data breach involving Oracle Cloud's Single Sign-On (SSO) and Lightweight Access Management (LWAM) systems was identified as "rose87168," claimed responsibility for exploiting vulnerabilities in Oracle Cloud's SSO and LWAM systems. The compromised data includes Java KeyStore files, and Enterprise Manager Java Platform Security files, affecting over 140,000 tenants, raising substantial concerns. While Oracle initially denied any breach, subsequent disclosures from CloudSEK and CybelAngel corroborated the incident, underscoring the critical importance of robust security measures for organizations relying on cloud services.

Given Oracle's significant investments and expansion in the cloud market, ASEAN must prioritize cloud security to protect sensitive data and maintain trust.

#### Threat Overview

**Threat Actor:** "rose87168"  
**Date of Discovery:** March 21, 2025  
**Method of Attack:**

- Exploitation of a vulnerability in Oracle Cloud's login.(region-name).oraclecloud.com.
- Potential exploitation of CVE-2021-35587, a critical vulnerability in Oracle Access Manager, messages mimicking legitimate communications from local bank accounts

### AJCCA - Threat Intelligence Report

#### Be Aware of Miyako: The Initial Access Brokers Threat Actor

**Date:** 17 April 2025  
**Source:** cyberint.com, IAB Report 2025  
**Prepared and Analyzed by:** IdNSA  
**TLP :** GREEN  
**Appendix :** -

#### Executive Summary

Initial Access Broker (IAB), has emerged as a critical threat actor with a sophisticated arsenal of exploitation techniques, compromised networks, which are then sold to threat actors active on dark web forums such as Breachforums. Operations are global, but recent activities show a strong focus on Indonesia.

Targeting a wide array of industries such as education, government, energy, healthcare, and telecommunications in the USA, China, France, and Indonesia. This report details the impact in ASEAN, and recommended mitigation strategies.

Incidents like "mommy". Vulnerabilities (e.g., CVE-2024-45409 in GitLab,

gang Hellecat, known for double extortion attacks (e.g., CVE-2024-50), making it accessible for many malicious actors.

applications. Application abuse. Persistence.

### AJCCA - Threat Intelligence Report

#### The Darcula Campaign's Stealthy Assault on ASEAN's Digital Defences

**Date:** 11 March 2025  
**Source:** Beyond Identity  
**Prepared and Analyzed by:** rawSEC (Malaysia Cyber Security Community)  
**TLP :** GREEN

#### Executive Summary

Phishing-as-a-Service (PhaaS) is rapidly advancing, making it easier for cybercriminals to execute highly sophisticated phishing attacks. The emergence of the Darcula PhaaS platform exemplifies this trend, offering automated tools to create customized phishing kits that mimic any brand. Darcula highlights how threat actors are continuously refining their techniques to circumvent multi-factor authentication (MFA) and other security measures. This evolution underscores the growing need for organizations to adopt more robust and adaptive defences to counter these ever-evolving threats.

#### Threat Overview

Malaysian organizations, especially in the telecommunications and banking sectors, are heavily targeted due to their high mobile penetration and reliance on SMS-based authentication. Attackers use compromised accounts to impersonate legitimate entities, such as banks, to steal sensitive information.

## 1. WGのミッション

- ・ JNSAとAJCCAの活動の連携を推進する。
- ・ AJCCA関連再委託案件の共同作業（受託）

## 2. 活動内容

- ・ AJCCAの活動
  - － OT Security WGとの連携
  - － アニュアルレポート調査・編集
  - － プロモーション／マーケティング
  - － AJCCAのイベント企画／運営等の事務局支援 ※ 「AJCCAカンファレンス」
  - － 年4回のC10会議でのプレゼンテーション
  - － ASOCIOとのJV／WGへの参加 OT/WG、TI/WG

### 1. 「第二回AJCCAカンファレンス in Tokyo」の開催

2025年10月10日 東京大学で開催

# 2nd AJCCA Conference in Tokyo 2025



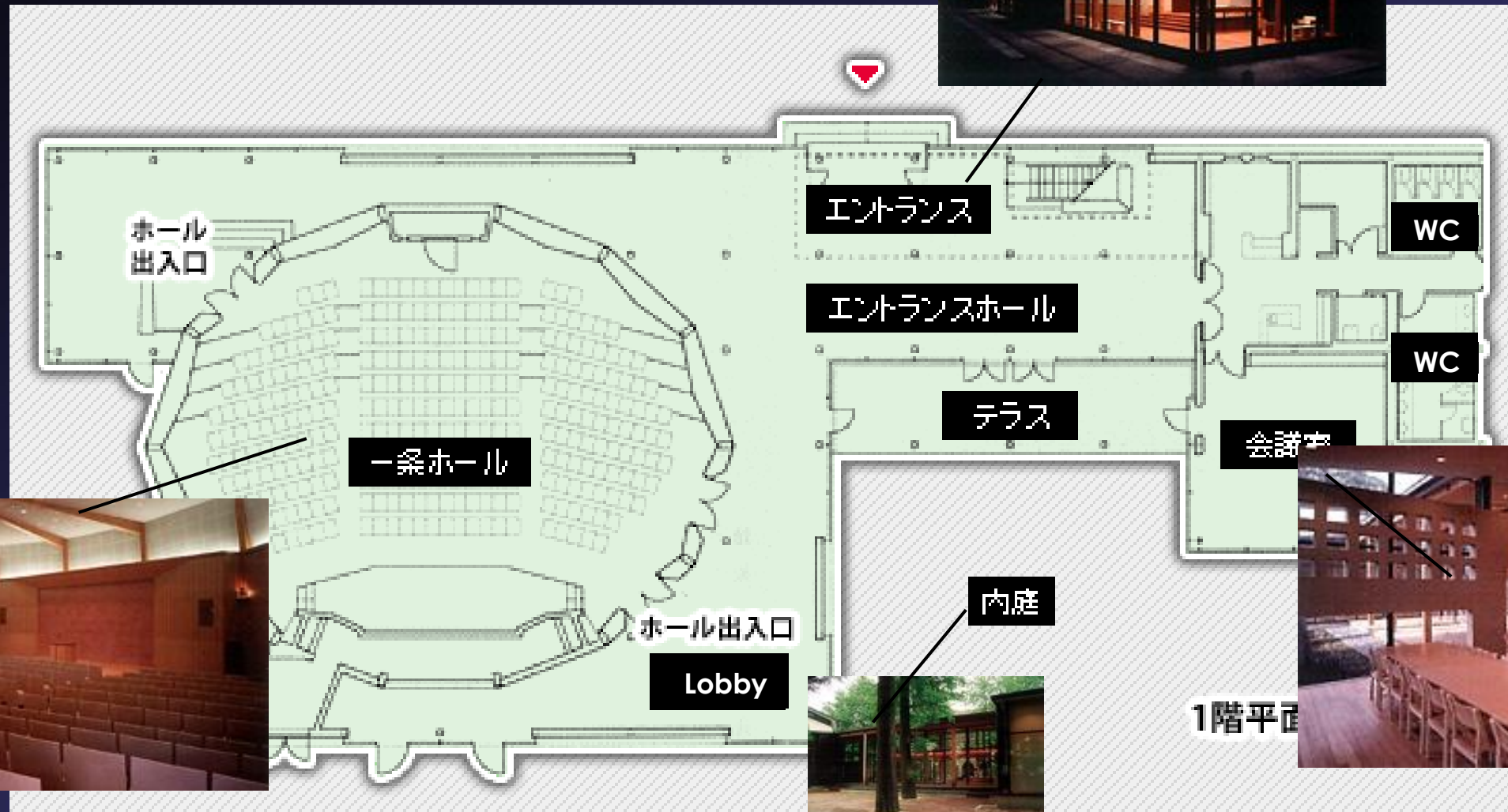
日時：2025年10月10日

会場：東京大学 弥生講堂一条ホール

Copyright Japan Network Security Association

1. イベント名：「**2<sup>nd</sup> AJCCA Conference 2025 in Tokyo**」
2. テーマ：“Securing the Future with AI Driven Cybersecurity and Resilient Supply Chain”
3. 開催目的：
  - ASEAN各国と日本のサイバーセキュリティコミュニティによる連携強化
  - AJCCA活動の2024年度の成果と今後の取り組み発表
  - テーマに沿った活動状況のご報告とソリューション紹介
  - Cybersecurity関連企業のソリューション展示会
4. 日時：令和7年10月10日（開場：9:30、開始：10:00、終了：17:20 予定）
5. 場所：東京大学 弥生講堂一条ホール
6. 運営：
  - 主催：特定非営利活動法人 日本ネットワークセキュリティ協会（JNSA）
  - 後援：ASEAN Japan Cybersecurity Community Alliance（AJCCA）  
内閣府国家サイバー統括室NCO（旧NISC）（申請予定）
  - 協賛：募集中
7. 来場予定者：200名（最大300名）
  - AJCCA各国の代表団体・組織
  - 一般企業、JNSA会員企業他
  - 日ASEANサイバーセキュリティ政策会議各国政府責任者及び担当者
  - 日本政府官公庁関係者
  - サイバーセキュリティ専門家、研究者
  - 関連産業界関係学術機関

# 開場レイアウト



## ➤ 基調講演1 講演者

**Rudi Lumanto 氏** : AJCCA会長、インドネシア・ネットワーク・セキュリティ協会(iIdNSA) 創設者兼顧問

・2011年から2020年3月までインドネシアの国内CSIRTであるId-SIRTII/CCの前会長。1988年から2020年3月まで、技術の応用と評価機関（BPPT）、通信情報省、国立サイバー暗号庁（BSSN）に勤務。2011年に IdNSAを設立しました。現在はIdNSAのアドバイザーであり、インドネシア大学工学部情報セキュリティ大学院の講師でもあります。OIC-CERT Global Cybersecurity Awardの審査員であり、2020年にITU AJ賞を受賞。日本で工学学士、工学修士、博士号を取得。

## ➤ 基調講演2 講演者

**Stan Singh 氏** : Asian-Oceanian Computing Industry Organization - アジア・オセアニアコンピュータ産業機構（ASOCIO）会長、The National ICT Association of Malaysia - マレーシア国家情報通信技術協会（PIKOM）理事

・英国でコンピュータサイエンスの学位を取得後、37年にわたりIT管理、事業経営に携わってきました。製造、流通、不動産、金融など多様な業界での経験を有し、AI、クラウド、ブロックチェーン、サイバーセキュリティ等の分野でも企業を支援しています。英国やアジア諸国でのグローバルな業務経験もあり、2025年にはASOCIOの会長に就任しています。

---

今年の「AJCCAカンファレンス」の開催はJNSAが主催となります。  
皆様のご参画とご協力をよろしくお願い申し上げます。

