2026 年 11 月 13 日作成

1 日目 11 月 17 日（火）

●トラック 1（HALL B）

時間	カテゴリ・キーワード	タイトル	スピーカー（敬称略）	言語
09:00 - 09:55	基調講演（AI、国際法、教育）	フロンティア AI 時代のサイバーセキュリティと能力構築（仮）	クリスチャン・ヴァン・ホーク ヤニス・アグラフィオティス	EN
10:10 - 10:50	テクニカル（AI、Web App セキュリティ、バグバウンティ）	[Pwn2Own Berlin 2026 にて 20,000 ドル獲得] Agent2Shell：あなたの AI コーディングエージェントは、すでに攻撃者のコードを実行している	辻 知希	JA
11:00 - 11:40	テクニカル（AI、バグバウンティ、サイバー犯罪）	AI vs. AI： AI を用いた Google Pixel の AI コプロセッサーにおける特権昇格バグの研究	フー・カンユー	EN
11:50 - 12:30	テクニカル（AI）	ChatMate： サンドボックス脱出を介した AI アシスタント上でのリモートプロンプト実行	オリー・ラハヴ	EN
13:40 - 14:20	テクニカル（AI）	敵対的 AI の進化： 脅威インテリジェンス最前線からの物語	ダニエル・カペルマン・ザフラ	EN
14:30 - 15:10	ジェネラル（AI、バグバウンティ）	「PleaseFix」によるエージェント型ブラウザーの完全攻略：ゼロクリックでの乗っ取りを可能にする新たな脆弱性クラス	スタヴ・コーエン マイケル・バーグリー	EN
15:30 - 16:10	ジェネラル（AI、デジタルフォレンジック）	AI 時代におけるインシデント対応の品質保証	朝長 秀誠 矢野 雄紀	JA
16:20 - 17:00	テクニカル（AI、Web App セキュリティ、バグバウンティ）	In Origin We Trust： 特権サイドから Chromium を攻略する	オレンジ・ツァイ	EN
17:10 - 17:50	テクニカル（重要インフラ、認証）	Pass-the-Device： エンドポイント侵害後における SASE/VPN の「信頼」の移植	ルスラン・サイフィエフ	JA
18:00 - 18:40	サイバー犯罪対策（サイバー犯罪、教育）	「反乱都市」からの報告： イランの APT グループはいかにして自国民を監視するのか	エリアド・キムヒ スバジート・シンハ	EN

●トラック 2（HALL A）

時間	カテゴリ	協賛企業・タイトル	スピーカー（敬称略）	言語
10:00 – 10:30	Open Talks	[三井物産セキュアディレクション株式会社] AI エージェントの脅威動向と境界防御（Secure AI Gateway）による多層防御	高江洲 勲 幸田 奨平	JA
10:40 – 11:10	Open Talks	[OffSec] 低コスト化するサイバー攻撃、問われる人間の判断力： 日本の能動的サイバー防御時代におけるレジリエンス	ティム・ノーマン	EN
11:20 – 12:05	Open Talks	[株式会社日立システムズ] 第一部：なぜフロンティア AI がサイバー戦争を書き換えるのか？～矛にも盾にもなるフロンティア AI への備え～ 第二部：中国による AI の軍事利用	第一部：仲小路 博史 第二部：小原 凡司（笹川平和財団 上席フェロー）	JA
13:00 – 13:45	Open Talks	[パナソニック ホールディングス株式会社] Threat Intelligence との付き合い方	中野 学	JA
13:55 – 14:40	Open Talks	[GMO インターネットグループ株式会社] 絶え間ない脆弱性ニュースの裏で、止まらない悪性パッケージ公開 - 1,900 万検体の解析から見るソフトウェアサプライチェーン攻撃の実態	豊田 恵二郎	JA
15:00 – 15:30	Open Talks	[SCSK セキュリティ株式会社] 日本の事例と国際標準から学ぶ、フロンティア AI のリスクとガバナンス	武井 滋紀	JA
15:40 – 16:10	Open Talks	[株式会社マクニカ] 見知らぬアセット、待てない KEV：AI 時代の ASM とリスクベース脆弱性対処、その現実と限界	山﨑 剛弥 矢原裕大	JA
16:20 – 16:50	Open Talks	[NRI セキュアテクノロジーズ株式会社] 熟練アナリストを超える Agentic SOC への挑戦 - 組織知の注入とハーネスによる統制	芳賀 夢久	JA

●トラック 3（Room3）

時間	カテゴリ・キーワード	タイトル	スピーカー（敬称略）	言語
12:00 – 12:40	Bluebox（AI）	Antigent: An Autonomous Counter-Agent Against Agentic AI Attacker	豊田 宏明	JA
13:00 – 13:40	Bluebox（AI）	1 つのハーネス、3 つのセキュリティエージェント：再帰的言語モデルの実践	シュエシャン・スー	EN
14:00 – 14:40	Bluebox（AI）	Turncoat：コーディングエージェントから C2 エージェントへ	マイケル・テロイヤン	EN
15:00 – 15:40	Bluebox（AI）	vwhois: WHOIS の魔境に挑む全 TLD に対応した実用的な WHOIS パーサー	羽田 大樹	JA
16:00 – 16:40	Bluebox（AI）	AI アプリケーションの静的解析：テイントトラッキングからエクスプロイト生成まで	アリーシャ・グプタ	EN
17:00 – 17:40	Bluebox（AI、データ保護、認証）	AgentShield：Linux カーネルにおける暴走 AI エージェントの封じ込め	ウェイシャオ・ジー チンジャー・ジャン レアンドロ・リー	EN

2日目 11月18日（水）

●トラック 1（HALL B）

時間	カテゴリ・キーワード	タイトル	スピーカー（敬称略）	言語
09:00 – 09:40	テクニカル（マルウェア対策）	Shade Core：ハイパーバイザーで保護された現代の PC における UEFI 攻撃の復活	松尾 和輝	JA
09:50 – 10:30	テクニカル（バグバウンティ）	脆弱性、アッセンブル！ Windows カーネル内のクロスコンポーネント脆弱性製造工場	Angelboy ヤン	EN
10:40 – 11:20	サイバー犯罪対策（AI、マルウェア対策、デジタルフォレンジック）	5 年間の GitHub 定点観測で明らかにした悪性 PoC と販売 PoC の流通ライフサイクル	芳村 涼介	JA
11:30 – 12:10	サイバー犯罪対策（マルウエア対策、サイバー犯罪、デジタルフォレンジック）	Operation ShadowCommit - GitHub 上の隠密作戦	イ・ジュンヒョン イ・デフ	EN
13:20 – 14:00	テクニカル（AI、重要インフラ、ハードウェアハッキング）	Too Close to the Metal： 内外からの GPU ネオクラウドへの攻撃	マイケル・カチンスキー ヤキール・カドコダ	EN
14:10 – 14:50	法と政策（重要インフラ、国際法・政策）	The Code IS the Law： 宇宙空間のサイバーセキュリティガバナンスにおける民間企業の規範形成	ジョアンナ・クレシャ	EN
15:00 – 15:40	法と政策（重要インフラ、国際法・政策）	ソルト・タイフーンの影：日本と隣り合う攻撃拠点	クリストファー・ブラッチャ	EN
15:50 – 16:30	ジェネラル（重要インフラ、サイバー犯罪）	Physical-to-Cyber Attack への対策： 重要インフラ拠点に対する物理侵入テストと CPSF を活用した経営リスク評価	大田 大輔	JA
16:40 – 17:20	ジェネラル（重要インフラ、OT、IoT セキュリティ、DoS 対策）	スペクトラムが戦場となるとき： 電波妨害下における都市 IoT の防衛	パブロ・チェルニコフ	EN
17:30 – 18:10	ジェネラル（重要インフラ、マルウェア対策、DoS 対策、国際法・政策、サイバー犯罪）	ハイブリッド脅威下における国家重要インフラの防衛	イヴァン・カラバシキン	EN

●トラック 2（HALL A）

時間	カテゴリ・キーワード	協賛企業・タイトル	スピーカー（敬称略）	言語
09:00 – 09:40	U25（WebApp セキュリティ）	No Context, No Consent： Firefox の内部リクエストパスにおける LNA バイパスの体系的分析	川杉 倫太郎	EN
09:50 – 10:30	U25（バグバウンティ、AI）	Out of LINE： QR コードから LINE クライアントにおけるワーム型 RCE へ	リン・ホンテン	EN
10:50 – 11:20	Open Talks	[SSD Labs Japan] MIBleed： あらゆるツールが見逃してきた 11 年前から存在するバグ	アーロン・チョ	EN
11:30 – 12:00	Open Talks	[株式会社 NTT データ先端技術] フロンティア AI 時代の脆弱性管理 — 攻撃者と防御者の間に生まれたギャップをどう埋めるか	藪根 茂樹	JA
13:00 – 13:30	Open Talks	[MS&AD インターリスク総研株式会社] サイバーインシデント発生！まずは何をするべきか？ ～弁護士と考える実務対応～	寺門 峻佑（TMI 総合法律事務所パートナー） 遠藤 宣孝 松森 純	JA
13:40 – 14:10	Open Talks	[NTT セキュリティ・ジャパン株式会社] OSINT を使った攻撃者の特定 2026	真鍋 太郎	JA
14:20 – 14:50	Open Talks	[日本電気株式会社] ManageEngine 悪用サーバからつながる ValleyRAT・AtlasRAT の C2 分析	大芝 大 杉生 貴成 前田 大輔	JA
15:00 – 15:30	Open Talks	[株式会社ハイヤールー] 118 万件の実データで見る、組織の AI エージェントの安全性とガードレール設計	葛岡 宏祐	JA