SANS
CYBERVANTAGE
サイバーバンテージ

無償でご参加いただけます！

2026年6月30日（火）13:00-18:30

ベルサール
神保町アネックス

東京都千代田区神田神保町
2丁目36−1 住友不動産千
代田ファーストウィング 1F

アクセス	地下鉄半蔵門線・東西線・新宿線「九段下駅」5番出口から徒歩5分	地下鉄半蔵門線・新宿線・三田線「神保町駅」A2出口から徒歩2分	JR東日本「水道橋駅」西口から徒歩8分

Jason Dely
Northern Strong Security, Instructor

JasonDelyは、Northern Strong SecurityやSANSでコンサルタント・講師を務めるICSセキュリティ専門家です。フォード車両の電子機器・プログラミング改良、サイランス社ICSプラクティス・ディレクターとしての手法開発・管理を経て、初心者から専門家まで幅広いスキル向上を支援しています。

吉岡克成
横浜国立大学大学院環境情報研究

横浜国立大学大学院環境情報研究院・先端科学高等研究院准教授、同学CISO情報システムセキュリティを専門とし、総務省サイバーセキュリティタスクフォースなど政府。有識者会議の委員を歴任。文部科学大臣表彰・科学技術賞、総務大臣賞、情報セキュリティ文化賞を受賞。

Tim Conway
Fellow, Professor

TimConwayは、制御システムインフラを支えるEMSコンピュータシステムエンジニ。アとして、ノーザン・インディアナ・パブリック・サービス・カンパニーに15年勤務。管理職・リーダー職に加え、公的委員会の議長などを歴任し、現在はSANS Technology Instituteの教員として、業界向けリソース、コース、資格開発にも携わっています。

進化する脅威に、進化で対抗せよ。ITだけでなく、OT/ICSまで踏み込む実践的サイバー防衛を考える。

日々、進化、複雑化するサイバー攻撃に対して、どのような備えが出来るでしょうか？

昨今のシステムは様々な技術が複合的に組み合わさっており、サイバー攻撃からシステムを防御するために必要な知識やスキルも多岐にわたります。

本セミナーでは、IT技術だけではなく、OT/ICSといった技術も踏まえて、これからのシステム防衛に必要な知識や技術とは何か？を事例を交えてご紹介させて頂きます。

サイバーセキュリティ業務に携わる方、社内システムの設計、検討を行う方、サイバーセキュリティ人材を育成、採用される方々に、是非参加いただき、今後の計画立案の参考にしていただければと考えております。

渡辺慎太郎
株式会社 JCOM サイバーセキュリティ本部 副本部

渡辺慎太郎氏は、株式会社JCOMのサイバーセキュリティ部門でシニアエキスパートを務める。LAN/WAN、ISPシステム、放送設備のセキュリティ対策を推進し、インシデント対応、デジタルフォレンジック、SOC運用の指導・監督にも従事。ICT-ISAC、CRICCSF、JCTAなどの活動にも参加している。

飯島　秀俊
国家サイバー統括室
審議官（能動的サイバー防御運用担当）

神奈川県横浜市出身。1995年防衛庁（当時）入庁。在米国日本大使館、内閣官房に出向。防衛省では、調査課長（インテリジェンス政策担当）、防衛政策課長を経て、2023年から内閣官房にて、2025年5月に成立したサイバー対処能力強化法等（能動的サイバー防御法）の制定作業に従事。現在、内閣官房国家サイバー統括室で内閣審議官として能動的サイバー防御の運用総括を担当されています。

申込方法

営業担当者にご連絡を頂くか、セミナー申込みサイトに必要事項をご記入のうえ、お申し込みください。

スキャン

DAY 1 SEMINAR SESSION | 講演プログラム

TIME	SESSION
12:30–13:00	**開 場・受 付**
13:00–13:10	**開会のご挨拶** 小柳 修二 (SANS Training Japan合同会社 カントリーディレクター)
13:10–14:00	**「問い」が立てられる人材、「解」が引き出せる環境** **渡辺 慎太郎（JCOM株式会社情報セキュリティ本部 副本部長）** 生成AI技術の飛躍的な進歩により、私たちが持てる問題解決能力は大きく向上しました。その結果、適切な問いが立てられる能力が、以前にも増して重要になっています。そして、立てた問いに取りかかるためにはデータが必要です。この講演では組織運営者を対象に、サイバーセキュリティ業務の中から身近な例を用い、人材育成とデータ整備の方法について論じます。
14:00–14:50	**サイバー脅威把握のための国産インテリジェンス構築 ～大学における研究開発と実践的人材育成～** **吉岡 克成 (横浜国立大学 大学院環境情報研究院)** 本講演では、国家プロジェクトである経済安全保障重要技術育成プログラム「先進的サイバー防御機能・分析能力の強化」において横浜国立大学が担当するサイバー攻撃観測、脅威アクタ観測に基づく国際インテリジェンス構築の活動について説明し、それらの活動を通じた実践的教育と人材育成の取り組みについて紹介する。
14:50–15:00	**休 憩**
15:00–16:10	**組織システム環境におけるネットワーク可視化と監視** **Jason Dely (Northern Strong Security, Instructor)** ICS/OT環境がますます複雑化する中で、ログ集約はセキュリティ監視、インシデント対応、運用の可視性を確保するために不可欠となっています。しかし、その実現は決して容易ではありません。本講演では、レガシーシステム、ベンダー制約のある機器、セグメント化されたアーキテクチャにまたがるログ集約の特有の課題を探ります。これらの環境では、ログ機能が制限されていたり一貫性が欠けていることが多くあります。さらに、ICS/OTにおいてログ集約がなぜ重要なのか、こうした制約が検知やトラブルシューティングにどのような影響を与えるのかを考察します。その上で、目標の定義方法や、集中化された可視性とレジリエンス向上に向けたスケーラブルなアプローチを構築するための実践的な方法について解説します。
16:10–16:20	**休憩**
16:20–17:30	**サイバーインシデント全領域での対応：教訓、落とし穴、ベストプラクティス** **Tim Conway (Fellow, SANS)** サイバーインシデントは、単独で発生するものではありません。新たな脆弱性の発見から、大規模な影響を及ぼす攻撃まで、その形態は多岐にわたり、状況に応じた対応が求められます。 本講演では、こうした幅広いインシデントが実際の現場でどのように対応されてきたのかを、具体的な事例を通じて紹介します。その中から得られた教訓や、陥りがちな課題、効果的な対応のポイントを整理します。また、技術的な対応だけでなく、関係者間の連携、限られた時間の中での意思決定、復旧に向けた取り組みといった組織的な側面にも焦点を当てます。これにより、サイバーインシデントの発生前から復旧後まで、組織がどのように備え、対応力を高めていくべきかについて、実践的な示唆を提供します。
17:30–18:20	**我が国のサイバー安全保障 －国家安全保障の観点からサイバーを考える－** **飯島　秀俊（国家サイバー統括室審議官（能動的サイバー防御運用担当）** 戦後最も厳しく複雑な安全保障環境に直面する中、サイバー空間を取り巻く情勢も深刻化している。国家の関与が疑われる攻撃も顕在化し、質・量の両面でサイバー攻撃の脅威は増大し、国民生活や経済活動、ひいては国家安全保障に深刻な影響を及ぼしている。こうした状況に対する我が国としての取り組み、特に能動的サイバー防御を可能とする新法等やサイバーセキュリティ戦略の制定作業のエピソードを交え、分かりやすく説明する。
18:20–18:30	**閉会のご挨拶** **Suresh Mustapha (APAC Managing Director, SANS)**

SANS

CYBER VANTAGE

サイバーバンテージ

Tabletop Exercise

経営判断が試される“その瞬間”を、事前に体験する

2026年7月1日開催!

テーブルトップエクササイズ（TTX）とは？

サイバーインシデント発生時に問われるのは、技術力ではなく**経営判断の質とスピード**です。

SANSのテーブルトップエクササイズは、経営層・幹部が中心となり、リアルなインシデントシナリオの中で

「何を優先し、どう判断し、どう説明するか」を実践的にシミュレーションします。

技術的な対応力ではなく、**有事の際に組織としてどのように判断し、連携し、対応するか**に焦点を当てています。実際のインシデントをもとにしたシナリオが段階的に展開され、参加者は状況を評価し、優先順位を判断しながら意思決定とコミュニケーションを行います。

なぜ今必要なのか？

多くの組織が計画を持っています。

しかし実際の危機では、「計画通りに動けるか」ではなく「その場で判断できるか」が問われます。

この演習では、以下を明らかにします：

- 意思決定の遅れやボトルネック
- 経営層と現場の認識ギャップ
- 不明確な責任・権限・エスカレーション
- 対外コミュニケーションの脆弱性

「問題が起きてから気づく」のではなく、事前に可視化し、対処することができます。

また、エネルギー、通信、金融、製造など異業種の参加者とともに実施することで、**業界を越えた知見の共有や連携強化**も期待できます。

サイバーインシデントはサプライチェーンや社会インフラに波及するため、こうした横断的な視点は非常に重要です。

経営層にもたらす価値

- 危機下でも機能する意思決定プロセスの確立
- 組織全体の対応力とスピードの向上
- 経営としての説明責任への備え（株主・顧客・社会）
- 経営チームとしての共通認識と即応力の強化

これは単なる訓練ではなく、「**経営リスクへの投資**」です。

SANSのTTXの特長

実際のインシデント対応を経験してきたSANSの専門家が主導します。

今回担当Cyber Vantageの担当をするTim Conwayはウクライナ電力網攻撃（CRASHOVERRIDE）など、国家レベルの重大インシデント分析に関わった実績をもっており、**現実に即した意思決定の難しさ**を再現します。

さらに：

- 日本の事業環境・規制・リスクを踏まえた設計
- アクティブ・サイバー・ディフェンスの視点を反映
- アジア各国での実績に基づくベストプラクティス

机上の理論ではなく、**実際に通用する判断力**を養います。

サイバーインシデントは「起こるかどうか」ではなく、「いつ起こるか」の問題です。

そのとき、経営として「**適切に判断できる準備ができているか**」

この演習は、その問いに答える機会です。

詳細は**Japan@sans.org**
または担当者へご連絡ください。

+81 3 3242 6276 japan@sans.org @SANS_JAPAN

DAY 2 TABLETOP EXERCISE SESSION

プログラム

経営判断が試される“その瞬間”を体験する。

今回、SANSでは、日本ではあまりなじみのないテーブルトップ・エクササイズを、弊社で準備した模擬シナリオを用いて、参加者の皆様にテーブルトップ・エクササイズを行う目的やポイント、方法などを擬似的に体験していただきます。

お申し込みは組織関係チームの皆様複数名でも、お一人の参加でも問題ありません。

各国で多くの政府機関、企業、組織に対して、トレーニングを行った経験豊富な講師が皆様の疑問に答えながら、

実践的なトレーニングの方法について解説をします。

参加費無料でこのようなトレーニング体験は、あまりない機会ですので是非積極的に参加をして頂き、皆様の組織の対応力強化に繋げて頂ければ幸いです。

Tabletop exerciseとは？

サイバーインシデント発生時に問われるのは、技術力ではなく 経営判断の質とスピードです。

SANSのテーブルトップエクササイズは、経営層・幹部が中心となり、リアルなインシデントシナリオの中で

「何を優先し、どう判断し、どう説明するか」

を実践的にシミュレーションします。

技術的な対応力ではなく、有事の際に組織としてどのように判断し、連携し、対応するかに焦点を当てています。実際のインシデントをもとにしたシナリオが段階的に展開され、参加者は状況を評価し、優先順位を判断しながら意思決定とコミュニケーションを行います。

なぜ、いま必要なのか？

多くの組織が計画を持っています。

しかし実際の危機では、「計画通りに動けるか」ではなく「その場で判断できるか」が問われます。

この演習では、以下を明らかにします：

- 意思決定の遅れやボトルネック
- 経営層と現場の認識ギャップ
- 不明確な責任・権限・エスカレーション
- 対外コミュニケーションの脆弱性

「問題が起きてから気づく」のではなく、事前に可視化し、対処することができます。

また、エネルギー、通信、金融、製造など異業種の参加者とともに実施することで、業界を越えた知見の共有や連携強化も

期待できます。サイバーインシデントはサプライチェーンや社会インフラに波及するため、こうした横断的な視点は非常に重要です。

テーブルトップエクササイズ タイムテーブル

10:00–10:30	開場・受付
10:30–11:00	テーブルトップエクササイズ概要説明
11:00–12:00	Move 1 – ITに焦点を当てた影響について
12:00–13:00	休憩（昼食）
13:00–13:50	Move 2 - ITからICS/OTへの転換、運用上の見通しの欠如
13:50–14:00	休憩
14:00–15:30	Move 3 -ネットワークおよびエンドポイントのフォレンジック調査、制御機能の運用上の操作
15:30–15:40	休憩
15:40–16:30	Move 4 – 復旧と情報共有
16:30–17:00	まとめ

詳細は**Japan@sans.org**
または担当者へご連絡ください。

+81 3 3242 6276　japan@sans.org　@SANS_JAPAN

SANS | CYBER VANTAGE サイバーバンテージ

楽しみながら実践力を鍛えよう!

2026年7月2日開催!

Capture the Flag (CTF) とは?

情報セキュリティのスキルを向上させるために、ゲーミフィケーションのスキームを利用します.知識のみならず、実際の情報セキュリティの問題を解決していくことで、実践的なスキルを身に付けることができます.

今回は特別に無償でご参加いただけます!

システム要件
- **プロセッサー:** 64-bit, x86, 2.0 GHz+
- **メモリ:** 16GB
- **ハードディスク:** 40GB以上の空き容量
- **OS:** Windows、Mac、Linux
- **VMWare**

実践的なサイバーセキュリティ演習を、ゲーム感覚で体験!

実践的にスキル向上

攻撃・防御・解析など、実際のセキュリティ課題を解くことで、実践力が身につきます.

段階的にレベルアップ

初心者から上級者まで楽しめる難易度設計.

ヒントシステムを活用し、解いていくことによって、知識をつけることができます.

チームで協力

仲間と協力してフラグを獲得.チームワークやコミュニケーション能力も向上します.

ランキング

スコアボードやで自分のスキルレベルを可視化.得意分野や不得意な分野を見つけることができます.

Cyber Vantage CTFの特徴

今回の演習では、実践型サイバー演習「GRID NetWars」を採用しています.

GRID NetWarsは、電力の生成・供給を支える技術をベースに、社会インフラを狙うサイバー攻撃への対応力を実践的に鍛えるトレーニングです.

演習では、電力システムに関連するプロトコルやアーキテクチャを題材に、リアルなインシデントシナリオに挑戦.参加者は、実際の攻撃や障害を想定しながら、検知・分析・対応といった一連のインシデントレスポンスを体験的に学びます.

サイバー攻撃やシステム障害が社会に与える影響を理解しながら対応力を磨けるため、現場で求められる実践力が身につきます.

さらに、ここで得られるスキルは電力分野にとどまらず、交通・通信・製造など、あらゆる重要インフラ分野で活用可能です.

“止めてはいけない社会”を守る力を、実践で身につけませんか?

Exercise Cyber Star 2025

シンガポールにおける過去最大規模かつ最も集中的な国家サイバー危機管理演習「Exercise Cyber Star 2025 (XCS25)」にパートナーとして参画しました.11の重要インフラ分野から約500名が参加し、実践的なサイバー危機対応訓練を実施.

申込方法

営業担当者にご連絡を頂くか、セミナー申込みサイトに必要事項をご記入のうえ、お申し込みください.

+81 3 3242 6276 japan@sans.org @SANS_JAPAN

DAY 3 CAPTURE THE FLAG SESSION

プログラム

サイバーセキュリティ技術者の方の訓練として、昨年夏にシンガポールサイバーセキュリティ庁主催で行われた

「Exercise Cyber Star 25」で行われたCapture the Flag (CTF)の環境を日本に持ち込みました.

サイバーセキュリティ技術者・アナリストの方々は、実際のOT（オペレーショナルテクノロジー）および重要インフラのシナリオに基づいて設計された、実践的な「キャプチャー・ザ・フラッグ」演習の体験が可能です.もちろん、技術的に自信のない方でもご参加いただけます.

本演習は、電力網、海事、製造業の環境に焦点を当てており、参加者は現代の攻撃手法を反映した模擬サイバーインシデントを調査し、対応します.インタラクティブな課題を通じて、参加者は脅威の検知、分析、および是正を行い、インシデント対応、脅威ハンティング、およびクロスドメイン（IT/OT）運用における実践的なスキルを強化します.

この演習環境では、単にCTFを行うだけではなく、実際のサイバー攻撃が広まっていく状況などをシミュレーションしており、単なる技術演習だけではなく、客観的な目線のサイバー攻撃を実感することができます.

参加申込み要領:

- チームでお申し込みください.1チームは4名～5名とさせていただきます.
- 参加登録の際にリーダーの方のみお名前、電話番号、メールアドレスをいただきます.
- チームメンバーの方はお名前、メールアドレスのみで結構です.
- 会場には演習参加用Wi-Fiネットワークの準備はありますが、PCについてはチームでご準備をお願いします.
- 申込みは本チラシ最後のURLもしくはQRコードから申込みWebサイトから申込みいただくか、担当営業にご連絡ください.

CTF タイムテーブル

9:00–9:30	開場・受付
9:30–10:00	本日のCTFに関する概要説明・システムへのアクセス確認・質疑応答
10:00–16:00	CTF体験（チーム毎に適宜休憩を入れながら実施）
16:00–16:15	質疑応答
16:15–16:30	総　括・結果発表

シンガポール「Exercise Cyber Star 25」で使用した機材

申込方法

営業担当者にご連絡を頂くか、セミナー申込みサイトに必要事項をご記入のうえ、お申し込みください.

+81 3 3242 6276　japan@sans.org　@SANS_JAPAN