日本サイバーディフェンス株式会社 主催

Japan Cyber Master Classes 2018

日本サイバーマスタークラス２０１８

〜英国・合衆国のサイバーマスターによる〜

受講お申し込みは申込書をメールで送付してください。

CyberMasterClass@NihonCyberDefence.co.jp

*60 名限定とさせていただきます。

*定員に達した場合には、他日程でのご案内をさせていただく場合がございます。予めご了承ください。

サイバーマスター

オリバー・ホアー（セッション１,２）– ２０１２年 UK オリンピックゲーム、サイバー長官

英国空軍小将 ジョン・フィリバン (セッション１,２) – UK 防衛相サイバープログラムダイレクター２０１３－２０１７

ジェイミー・サンダース (セッション２) – UK 国家犯罪対策省サイバー局長, インテリジェンス局長, ＧＣＨＱ勤歴２０年

ジョン・ノーブル CBE（セッション１) – UK 国家サイバーセキュリティセンター局長(NCSC)、８００件以上のサイバー攻撃への対策をリード

ハンク・ボンド海軍少将（合衆国海軍、退役）（セッション１,２) – 北アメリカ航空宇宙防衛司令部 (NORAD)、最高情報責任者兼サイバースペースオペレーション局長

開催日程

セッション１：　２０１８年７月２３日(月)から７月２７日(金)午前９時〜午後５時

セッション２：　２０１８年７月３０日(月)から８月３日(金) 午前９時〜午後５時

セッション１、セッション２は同じフォーマットで行われます。

開催会場

１日目から４日目	５日目
赤坂インターシティ AIR 東京都港区赤坂 1-8-1 https://www.intercity-air.com	駐日英国大使館 – British Embassy Tokyo 東京都千代田区一番町 1 https://www.gov.uk/world/organisations/british-embassy-tokyo

2018 年 7 月 18 日（水）までにお申し込みください。

プログラム

日本サイバーディフェンスが世界をリードするサイバーマスター講師の協力の元、国内で今までにない最も広い分野をカバーしたサイバーマスタークラスを開催します。サイバーマスター講師は、脅威

インテリジェンス、脅威分析、脅威対応の分野の世界的な専門家です。サイバーセキュリティにおける様々な分野のスキルを持ち寄り、サイバー事項を幅広く取り扱います。複雑な脅威や敵対者と向き合ってきた各々のキャリアから得た実際のオペレーション例、ケーススタディと経験を組み合わせた内容となります。日本サイバーディフェンスでは日本に日本人のためのサイバー拠点を設立しようとしています。参加者の皆様にはサイバーマスターとぜひ積極的に交流し、経験と関係性を築いていただけたらと思います。企業、個人、政府からのサイバーセキュリティへのそれぞれの経験、見解を併せ持つことで、参加者の皆様の２０１８年のそしてこれからのサイバーセキュリティに対する、より包括的な理解につながることと考えます。

日本サイバーディフェンスのコースは、政府、企業、個人どのレベルにおいても、日本が近い将来必要となるサイバー装備に必要な知識を作り上げることを目標としています。

トレーニングのセッションごとに質疑応答の時間を設けますので、積極的にご参加ください。

対象

日本で日本のためのサイバー知識を持ちたいと思われている方。

日本語・英語の双方通訳のご用意があります。

COMPONENT	朝のセッション	午後のセッション
A **23/07/2018** **John Noble CBE** **AVM John Phillibanl**	UK の国家サイバーセキュリティ戦略とナショナル・サイバーセキュリティセンター（NCSC）の設立。NCSC の役割の拡張とセンターの立ち上げに伴った NCSC シニアチームとしての体験。実体験を通して、何が上手くいった点、学んだ事項など。このセッションでは、他の政府機関の役割もカバーする。また、政府・プライベートセクターとのコラボレーションについても扱う。	様々な国家主体についてと、国家的セキュリティ脅威がどう進化してきたかについてのプレゼンテーション。サイバー犯罪が重複してくる部分、また、主要な相違点などについて説明する。このセッションでは、多くのケーススタディを参考にする。
B **24/07/2018** **John Noble CBE** **AVM John Phillibanl**	なぜ団体（機関・企業）が信用を落としてしまうのかについてのプレゼンテーション。このセッションでは、NCSC が対処した８００の重大なサーバーインシデントから見える、８つの根元について考察する。これが団体を守る責任のある役員、サイバー専門家にとって、どのような意味があるのか明らかにしていく。	サイバーインシデントへの良い対応とは？成功した対応に役立った主要因を探していく。ここでは、インシデントの（技術的な）対応と、インシデントの及ぼす幅広い影響にどう対処するか、という両方をカバーする。このセッションは、実際に起きたインシデントから様々なケーススタディを紹介する。
C **25/07/2018** **John Noble CBE** **AVM John Phillibanl**	なぜ団体（機関・企業）が信用を落としてしまうのかについてのプレゼンテーション。このセッションでは、NCSC が対処した８００の重大なサーバーインシデントから見える、８つの根元について考察する。これが団体を守る責任のある役員、サイバー専門家にとって、どのような意味があるのか明らかにしていく。	サイバーインシデントへの良い対応とは？成功した対応に役立った主要因を探していく。ここでは、インシデントの（技術的な）対応と、インシデントの及ぼす幅広い影響にどう対処するか、という両方をカバーする。このセッションは、実際に起きたインシデントから様々なケーススタディを紹介する。
D **26/07/2018** **Oliver Hoare** **John Noble CBE**	イントロダクションと UK におけるサイバーセキュリティへのアプローチの簡単な背景：このセッションでは、政府、警察、プライベートセクターでの事例を含む、サイバーセキュリティの主要点を見るとともに、日常のサイバーセキュリティとの相違点を検証する。	このセッションでは、政府機関、民間企業ともに、戦略的なサイバーリスクを識別する具体的な方法についてみていく。
E **27/07/2018** **Oliver Hoare** **AVM John Phillibanl**	このセッションでは、ロンドン２０１２オリンピックのケースで、何が起き、どう対処されたか、検証する。	これまでの主要なイベントから学んだレッスンとは？日本の２０１９年ラグビーワールドカップ、２０２０年東京オリンピックへの考えられるリスク・要因とは？
F **30/07/2018** **Oliver Hoare** **AVM John Phillibanl**	このセッションでは、ロンドン２０１２オリンピックのケースで、何が起き、どう対処されたか、検証する。	これまでの主要なイベントから学んだレッスンとは？日本の２０１９年ラグビーワールドカップ、２０２０年東京オリンピックへの考えられるリスク・要因とは？

G **31/07/2018** **Jamie Saunders** **AVM John Philliban**	脅威：このセッションでは、サイバー犯罪の脅威が過去五年においてどのように進化してきたのかについて扱う。低レベルな犯罪者からその多くが国家組織に関係するエリート犯罪者まで様々な人物が関与している。このような人物たちと並んで、サイバー犯罪サービスの不法マーケットの増大があり、これにより新しいプレイヤーがサイバー犯罪に安く、簡単に参加できるようになってきている。この「サイバー犯罪エコシステム」を理解することがサイバー犯罪に対応する戦略を立てる上では必須である。これについては、セッション２で深めていく。	サイバー犯罪に対抗する国家戦略。このセッションでは、国際的に他国でも採用されつつあるUKで開発されたアプローチを説明する。このアプローチは元々テロ対策として考案され、現在他の重大犯罪に適用されているUKの４P戦略に基づいている。多国籍サイバー犯罪グループを打ち破るには、国際的なパートナーシップが必須である。このセッションでは、近年の成功例、失敗例を見ていく。
H **01/08/2018** **Jamie Saunders** **AVM John Philliban**	サイバー犯罪に対抗するビジネス戦略。このセッションでは、各ビジネスレベルに焦点を当てる。この５年でサイバー脅威に対する認識は多大に向上したが、対応に関しては各企業ごとに大きな差がある。サイバーセキュリティーに巨額がつぎ込まれる中、リスク主導のアプローチを企業が開発していくことが必要である。これは、基幹情報財産の明確なアセスメントの元に投資決定すること、、サイバーイベントが経営にどのような形で影響するかということを理解すること、IT、セキュリティ部門の内外で明確な責任の線引きをすることなどを意味する。ベストプラクティスを認識することを目的とした、UKの金融セクターでの最近のリサーチの結果もこのセッションで取り扱う。	行政、民間とのパートナーシップ。政府機関もビジネスも、それぞれだけではこの脅威に立ち向かうことはできない。この分野において行政と民間のパートナーシップを向上させる新しい方法が必要である。多くのグッドプラクティスが、日本、UK、ヨーロッパ、北アメリカで開発されているが、まだまだ課題は多い。このセッションでは、近年の成功例を見るとともに、政府、ビジネスがともに共同のリジリエンスを向上させていくステップを認識していく。
I **02/08/2018** **AVM John Philliban**	戦略の必要性、リスク、そこにあるチャレンジを考察し、サイバー空間において増大する脅威に立ち向かうため、MODが政府機関をまたがった戦略を立ち上げた根拠を考える。	脅威の種類、攻撃の周期、様々な攻撃の動機を検証し、幾つかの事例となぜ攻撃者に遅れを取らない事が重要であるかを見ていく。
J **03/08/2018** **AVM John Philliban**	リスクマネジメント戦略、ビジネス継続計画と企業幹部が役員会審議で考えるべき事について検討する。	ケーススタディを使い、MODがどう防衛部のリスクを緩和してきたか、またその防護的、攻撃的、そして技術と資格への責任を検証し、ここまでに出た教訓の要約を行う。

費用 - 1 COMPONENT のトレーニング参加費用

申請書は http://nihoncyberdefence.co.jp/japan-cyber-master-classes/ でも見ることができます。

トレーニング受講料(税抜き) COMPONENT A B C D F G H I:	50,000 円
消費税(8%):	4,000 円
合計 (税込み):	54,000 円

駐日英国大使館 – British Embassy Tokyo トレーニング受講料(税抜き) COMPONENT E J:	70,000 円
消費税(8%):	5,600 円
合計 (税込み):	75,600 円

お支払方法は受講申し込み確認後、事務局よりご案内いたします。

警察庁、経済産業省、内閣サイバーセキュリティセンター、防衛相を含む、政府官庁は、２５％の割引がございます

申込書　全てご記入ください

ご連絡先	e-Mail		
	電話番号 (お勤め先)		
	電話番号 (携帯)		
ご希望日程 (ご希望される日程に 〇を付けてください)		セッション 1 7 月 23 日(月) – 7 月 27 日 (金) COMPONENT □ A :7 月 23 日 □ B :7 月 24 日 □ C :7 月 25 日 □ D :7 月 26 日 □ E :7 月 27 日	セッション 2 7 月 30 日(月) – 8 月 3 日 (金) COMPONENT □ F :7 月 30 日 □ G :7 月 31 日 □ H :8 月 01 日 □ I :8 月 02 日 □ J :8 月 03 日
お名前 (漢字)		姓	名
(ローマ字)			
お勤め先			
お勤め先 ご住所			
ご希望の言語		□ 英語 □ 日本語	

申請は http://nihoncyberdefence.co.jp/japan-cyber-master-classes/ でも見ることができます。

英国空軍（RAF）ジョン・フィリバン 空軍少将

John Philliban is a Director of Nihon Cyber Defence.

年間計 348 百万ポンドに上る多様なプロジェクトとプログラムのポートフォリオを持つプログラムディレクター。国内、派遣先で効果的な攻撃・防御作戦を実施するために必要な人員、トレーニング、スキル及び能力へのアプローチを転換するために、国家サイバー攻撃プログラム（NOCP）の一部を含む、国防省の先駆け的サイバープログラムを実施するための政府横断チームの指揮において卓越した指導力を発揮。

統合情報部隊（JFIG）の副司令官として、ワイトンのパスファインダー施設の立上げに対する、様々な情報分野及び多国籍機関にわたる 3200 人規模の多様な組織にわたる大規模な抵抗を克服。これは英国の情報コミュニティがこれまでに達成したプロジェクトの中で最も成功し変革をもたらすものとなった。

第９０通信部隊（90SU）において、英空軍の遠征要求にかかる作戦計画、準備及び世界的支援について日々責任を負い、900 名の英空軍及び文官を指揮。これには、人員の配備継続も含まれ、非常に速い作戦スピードにおいて調和の低下につながることも多かった。結果として、強力な指導と家族との緊密な関わりを通じて道徳的要素の重要性が強化された。

広範な経験に基づき、国防参謀総長補（VCDS）のストックテーキング（C4ISR 1とサイバーの全領域を網羅）において定期的に国防情報局長（CDI）の代理を務めるとともに、統合要求監督委員会（Joint Requirements Oversight Committee）に出席。これらの上級委員会において、参加者は、国防省の一番のリスクと問題を正確に理解するだけでなく、国防省の戦略的能力要件及び将来の調達のオプションに関する指示及びガイダンスを提供することも求められる。

C4ISR の実施にかかわるあらゆる問題に関して参謀総長補（Deputy Chief of Staff）に戦略的助言及びガイダンスを提供。

宇宙（米国開催の第 31 回宇宙シンポジウム）、C4ISR（中東サミット）、及び防衛通信フォーラム（イタリア開催）等のテーマについて、国際舞台にて定期的に講演を行う。これにより、他国の戦略的方針及び計画に関する卓越した視点を得た。

---

1 訳者注 C4ISR ：指揮（Command），統制（Control），通信（Communications），コンピューター（Computers），情報（Intelligence），監視（Surveillance） 偵察（Reconnaissance）

現職を通じて、オーストラリア及びカナダを含む多くの国々に、英国がどのように政策及びプログラムの実施してきたか、戦略的助言及びガイダンスを提供し、サイバー、情報及び電子戦（EW）の分野におけるベストプラクティスの共有を可能にしてきた。
重要な国家インフラの問題から、オープンソース等の防衛イニシアチブをどうしたら政府が最大限に活用できるのかという事まで、様々な問題に関する政府横断の取り決めにおいて極めて重要な役割を担ってきた。これには、政府全域及び軍ごとでの、最高位での協議を含む。
プログラムに関する責務の一環として、国家サイバー攻撃プログラム（NOCP）に関する戦略的業務論点概要分析が関係者すべてにとって受入れ可能であるだけでなく、上級職員がプログラムの焦点及びプログラムにおける金額の割当を支持する態勢にあるよう、内閣府／大蔵省／外庁にわたり非常に効率的に業務を推進。
サイバー共同ミッションを通じて、提案されている統合サイバー部隊の見込まれる形態及び規模の定義や調査に従事。これには慎重かつ繊細な協議が必要であり、複数の関係者との間で合意に達するための説得力及び訴求力ある交渉を要する。
多文化の学術環境に積極的に従事し、しっかりと馴染んでいる。世界中からの同僚との豊かなネットワークを作り上げ、複数の職員に個人的に助言を提供、現在も連絡を取り合う仲である。
政府通信本部（GCHQ）及びその他の外庁との間で築いた関係を通じて説得力ある対人スキルを示し、文化的障壁を除去し、否定的なステレオタイプ化に対処。これらは繊細な交渉の妨げとなる可能性もあったが、むしろ、防衛の必要性及び国が主要な脆弱性に取り組むうえでの合議アプローチにつながった。
実績ある政策立案・企画者及び変革主導者であり、複雑な問題への同時対処能力で知られる。さらに、国防情報局長（CDI）の「Understand」計画の主執筆者として、統合戦力コマンド（JFC）コマンダーの戦略的防衛セキュリティーレビュー（SDSR）の提出に対する説得力ある助言を生み出すうえで重要な人員関連スキルを示す。これにより、国防情報参謀部の防衛タスクへの貢献を著しく向上させる新たな取組にかかる財源を大幅に向上させた。
上級大臣／将校／事務次官へのブリーフィングに精通。（情報及び重要な国家インフラ関連問題について定期的に大臣にブリーフィングを行い、国防長官の着任時のブリーフィングに主要な役割を果たした。）

オリバー・ホアー

Oliver Hoare is a Non-Executive Director of Nihon Cyber Defence.

サイバーセキュリティ・ソシューションを専門とし、ストラテジー及びキャパシティー・ビルディングのコンサルティングを行うダイサート・ソリューションズ株式会社の創業者であり現 CEO。
2012 年にダイサートを設立させる以前は、政府機関で長年勤務し、2012 年ロンドンオリンピック・パラリンピックゲームにおいては、UK 政府のインフォメーションセキュリティ最高責任者を務める。その充実した四年の間、UK の重要な国内のインフラ、オリンピックをささえるネットワークを含む、全競技に関わるストラテジー開発、リスクアセスメント、数億単位のサイバープログラムの請負などの責任を担った。
公務員としてのキャリアの中（1991－2012）では、テクノロジー、セキュリティの分野で幅広く大臣、政府高官などへのアドバイスを行い、2008 年には、UK 首相によるデータ処理管理の見直しにて主要な役割を担うとともに、オリンピックゲーム運用期間中には、UK 首相を議長とする国家危機管理センター、“COBR”（内閣府のブリーフィング部屋）で、サイバー主担当者を務めた。
オリバーは、これまでのキャリアの大半を UK 内閣府にて、セキュリティ政策、テロリズム対策、サイバーセキュリティ、情報保証を担当してきた。この経験により、統合的かつ総体的であるセキュリティ・リスク管理の本質に深い理解を持つ。これは、2007－08 年の UK 政府のセキュリティ政策の幅広い見直しを行った事、また、この見直しによりテロリズム対策からサイバーセキュリティまで全般におよぶ、政府のセキュリティ政策の基準となった英国政府セキュリティ政策枠組み（SPF）を彼が作成するに至ったことに最も表されている。
現在、複数の企業、政府へのサイバーセキュリティのコンサルティング・アドバイザーとしてのキャリアポートフォリオを持つが、この一部として、2020 年夏のオリンピック、パラリンピックへむけた準備として、日本政府の内閣セキュリティーセンターへ戦略的リスクアドバイスを提供している。
又、アメリカ合衆国政府のナショナル・サイバーセキュリティ―・センター・オブ・エクセレンス（NCCoE）を管理する MITRE コーポレーションの特別アドバイザーも務める。
オリバーは、経験豊かなアソシエイトコンサルタントたちを少数先鋭で管理しているが、その多くが UK のセキュリティ分野において、上層部もしくは技術的な役職についており、それぞれの分野において UK のリーディング・エキスパートであると認識されている。

出版経験のある著者であり、熟達した指導者、講演者でもある。 - 国際的にソートリーダーであると認識されており、頻繁に学会での公演の要望を受け、定期的にセキュリティ、サイバーに関する事項のインタビューを受けている。
ロンドン・キングスカレッジの戦争学を卒業。地元の地域関心会社（非営利団体）の取締役を務め、自治体、スポーツ、テクノロジー教育イニシアティブなどに関与している。又、国際的なデジタル・フォレンジック会社の社外取締役も務める。

ジェイミー　サンダース博士

Jamie Saunders is a Senior Executive Advisor to Nihon Cyber Defence.

サイバーセキュリティ、サイバーインテリジェンスの分野で国際的に認識されるリーダー。29 年の公的機関での経験をもち、現在、民間で戦略的セキュリティコンサルタントとして、幅広い見識と、政府、ビジネスが直面するサイバーの課題に広範囲な経験をもつ。
政府機関での経験は、以下を含む。

- UK 国家犯罪対策庁（NCA）

  重役員会へ採用され、国家サイバー犯罪ユニットの局長として、NCA のサイバー犯罪対策能力の拡大をリードする。業界との連携を向上することに直属的にかかわり、UK 内の主要なサイバー犯罪捜査を監督した。後に、NCA の情報局長と任命され、NCA の新しく設立された情報部隊で、急務であった広い分野の情報機能の近代化を担った。
- 外務及び英連邦省

  国際サイバー政策局長として、UK・国際的なサイバー政策要件を遂行する外交職員の国際的なネットワークを構築し、主導する。ビジネス、政府、主要国家インフラに対する脅威に国際的パートナーとともに取り組み、数多くのサイバー政策に関する国際的イニシアチブを手掛けた。在ワシントン英国大使館のサイバー分野の主導者として、ホワイトハウス、国務省サイバー政策チームとの関係性を築くとともに、US と UK の主要機関間の運営・能力ベースのコラボレーションを開発・継続を担った。
- 政府通信本部（GCHQ）

  1988 年に GCHQ に採用され、この機関での 20 年に及ぶキャリアの中で、運営、政策、法人的役割など広い分野を担当してきた。2004 年、UK 上部公務員に昇進。

政府業務から昨年退職し、現在、戦略セキュリティ・コンサルタントとして活動。UK 政府のクライアントは、外務省、貿易省を含む。又、マーシュ・アンド・マクレナンの支部マーシュ・リスク・コンサルティングの顧問コンサルタントであり、ユニバーシティー・カレッジ・ロンドンの招へい教授を務める。
ジェイミーは、既婚で四人の子供を持つ。聖アンドリュー大学より数学の優等学士学位・博士号を持ち、UK 防衛アカデミー上級司令官・社員コースの卒業生でもある。音楽、演劇、アート、いい食事とワインが趣味。日本文化にも興味があり、日本茶の大ファンである。

ジョン・ノーブル CBE

John Noble is a Senior Executive Advisor to Nihon Cyber Defence.

2018 年 2 月末にジョン・ノーブルは、UK 政府のナショナル・サイバーセキュリティ・センター(NCSC)を退職。
NCSC は、2016 年 10 月に UK の主要なサービスをサイバーアタックから守り、サイバー事件を管理し、UK のインターネットの安全確保を目指すために発足した機関である。
ジョンは、運営の実行と戦略的ビジネスの変革に強い経歴を持つ、経験豊富な上部リーダーであり、40 年にわたる政府勤務の間に、コラボレーティブ、多様かつ高パフォーマンスなチームを築いており、効果的なパートナーシップを作り上げることに優れている。
又、ジョンは 2012 年から 2016 年にかけて、ワシントンの英国大使館に駐任し、国家セキュリティーに関する幅広い案件をリードした。
2016 年 7 月に NCSC の役員に選ばれ、このインシデント管理局長としての役職の中で、800 件ほどの重大なサイバー事件を確立し、その対応をリードしている。これらの仕事を通して、サイバー事件の原因を理解し、それに対処する、他に類を見ない経験を持つ。
特記すべき功績、責任は以下を含む:

- NCSC の発足において主要役員レベルの役割を果たす
- CERT(CERT-UK と GOV-CERT)とインテリジェンス機能を融合する事業改革をリードする
- 英国の国家サイバーインシデントマネジメント計画のデザインと実行
- ８００件以上の重大なサイバーアタックに対し、NCSC による対応をリードする。その中の４０件ほどは C2 レベル - 広いセクターに影響がある、と分類される。C2 インシデントのうち、公になっているものの一部は以下を含む

    - WannaCry ランサムウェアによる NHS（国家健康サービス）の信用ダメージ
    - 英国政府は NotPetya ランサムウェアをロシア軍に帰するものとする。（APT28）
    - Cloud Hopper－MSP（マネッジド　サービス　プロバイダー）の信用ダメージ
    - UK 議会の信用ダメージ
- 多くの上級政治家、被害を受けた企業役員会とのブリーフィング
- NCSC の国家サイバー演習計画の構築
- 企業と政府によるサイバー脅威に関する情報交換のイニシアティブである CISP の開発を監督する
- イングランド銀行へのサイバーセキュリティプログラムのアドバイス
- EU 法の英国での採用に関してインシデント管理の開発を監督
- 英国の次世代暗号キーの開発プログラムの SRO(上級責任者)を務める

英国政府事業を離れてからは、数多くの英国また国際的な企業にアドバイスを行うほか、幅広く主要なサイバー産業イベントで講演を行っている。

ハンク・ボンド海軍少将（合衆国海軍、退役）－R9B

R9B are a strategic partner of Nihon Cyber Defence.

ハンク・ボンド少将、合衆国海軍（退役）、は Root9B のグローバルエンゲージメントの上席副会長を務める。

サイバースペース・オペレーションの長官、北アメリカ航空宇宙防衛司令部（NORAD）、及び合衆国北部司令部（USNORTHCOM）の最高情報責任者を含む、海軍での 31 年以上にわたる現役勤務から移行した。これらの任務以前にも、イラクでの合衆国軍の最高情報責任者を務めるとともに、コミュニケーションと情報システムの長官を務めた経歴を持つ。

海軍のキャリアは、原子力潜水艦での任務から始まり、のちに海軍の情報技術システムの運用へと変遷。海軍、共同司令部の双方と、海上、陸の情報ネットワークを運用し、防御する幅広い経験を持つ。

合衆国海軍兵大学を卒業し、ジョージワシントン大学、合衆国防衛大学からも学士を取得。