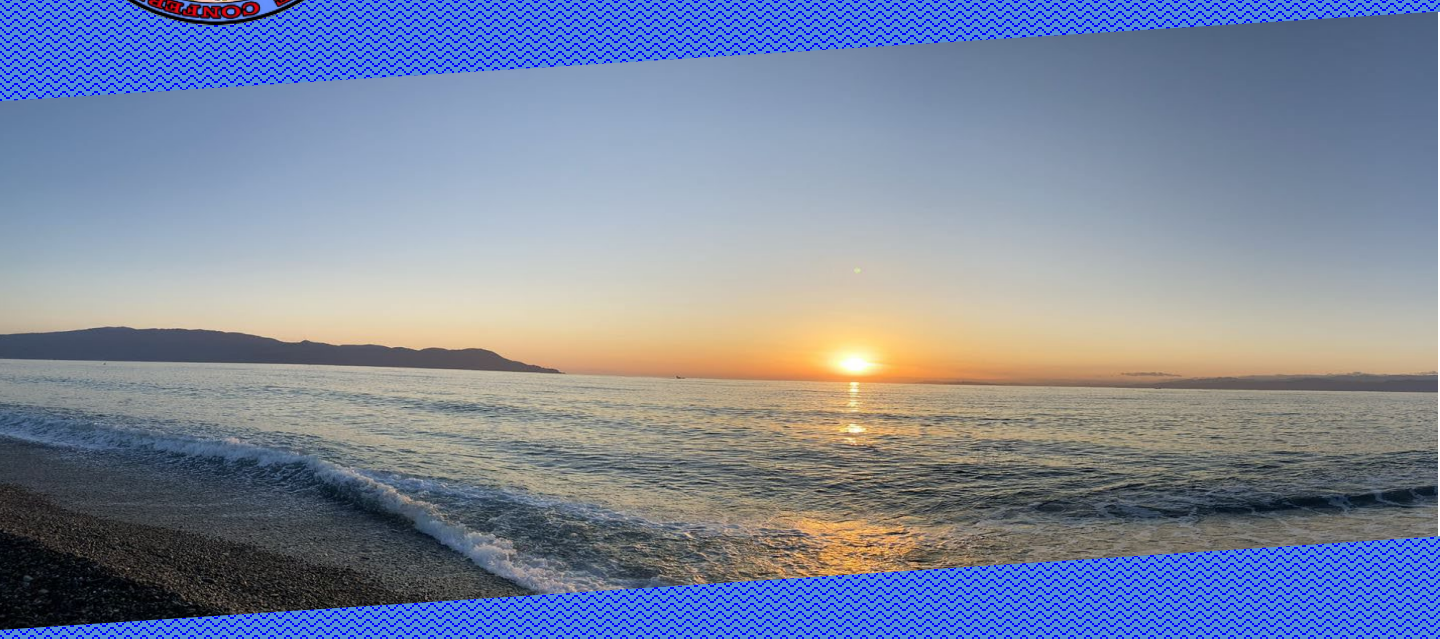
CYDEF2020



Cyber Defense Conference Japan

2020-DEC-2, Wed.
Thru
2020-DEC-3, Thu.

CYDEF Executive Committee

This page intentionally left blank.

目　次

Table of Contents

ご挨拶

CYDEF2020 実行委員会を代表して、一言ご挨拶申し上げます。

CYDEF2020 は、「NATO 加盟国等と日本の有識者がサイバーディフェンスに関して自由に意見交換を行い、日本のサイバーディフェンスの能力の向上と専門的な知識・経験の普及教育並びに国際交流に資する」ことを目的とし、2018 年から開催され、今年で第 3 回目となります。

今年はあいにくコロナ禍のためオンラインでの会議が主となり制約もありますが、自由な意見交換が活発に行われるよう実行委員会スタッフ一同、準備を進めてまいりました。今回は、現在世界共通の差し迫った課題となっているコロナ禍を踏まえ、「コロナ後の世界を読み解く」をテーマとしております。

サイバーディフェンスは、コロナ後のネットワーク中心の世界が、安全性と利便性を両立させつつ発展していく上でのキーテクノロジーとなるものと確信しております。

平和と安全保障のための科学プロジェクトである CYDEF の特色を生かし、CYDEF2020 が、コロナ後の世界でのサイバーディフェンスの在り方について、政策面、技術面を含め幅広く論じられる、意義ある会議となることを念じております。

最後になりましたが、CYDEF2020 のためお忙しい中、ご参加頂く講師と聴衆の皆様、共催並びに後援を賜りました諸団体の皆様、準備と開催に当たりご尽力いただきました関係者の皆様に御礼申し上げ、ご挨拶とさせて頂きます。

2020 年 12 月 1 日

CYDEF2020 実行委員会代表　矢野義昭

矢 野 義 昭

Opening Remarks

As a representative of Executive Committee of CYDEF2020, please allow me to make a brief greeting words.The objective of the CYDEF2020 is to exchange the opinions freely between the NATO side specialists and the Japanese side ones contributing to raising the capabilities and the deployment of the expertise and experience of the cyber defense in Japan, as well as to facilitating the international exchanges. The CYDEF has been held since 2018. This is the third time of the CYDEF.

There would be some limitations this time as the result of the online conference because of the Covid-19. The Executive Committee has been preparing for the conference to smoothly conduct the conference and actively exchange the opinions among the experts. We have chosen the theme that Power Shift after Corona, basing on the phenomenon of the worldwide infection of the virus that has become the emergent challenge to the international society.

The cyber defense will surely become the key technology for the coexistence of the security and the convenience in the post corona network centric world. Taking advantage of the characteristics of the CYDEF as a project for the peace as well as the security, it would be expected that the active opinion exchange will be realized in the CYDEF2020 in the area of the political aspects as well as the technological ones, and also expected to become a fruitful conference.

Finally, I would like to appreciate the many lectures and the audience joining the conference in spite of their busy daily works, the organizations providing the cosponsor and the assistance, and the staff members preparing and conducting the conference.

Thank you.

December 1,
2020

Yoshiaki Yano, MG (ret.) 矢野義昭

Chairman of the Executive Committee, CYDEF 2020

開催に際して

CYDEF へようこそ

世界は現在、世界的なパンデミックのより差し迫った脅威に関心を示しています。それは私たちの政治的関心の大部分を占めていますが、他のリスクや脅威は今なお存在し、パンデミックの結果としてそれらはその形を変えようとしています。そしてサイバーセキュリティもその一つです。

現在の危機の早い段階で、フランスのマクロン大統領はパンデミックとの戦いの間に世界的な平和を求めましたが意味あるものではありませんでした。我々が歴史から学ぶことは、我々が歴史から学ぼうとしないということであっても、過去を少し振り返れば世界経済の危機がしばしばより物理的な危機に拍車をかけたという事実に気付くはずです。その理由は明らかであり、現在目にしているところの貧困の脅威、同盟関係の変化、その文脈の中での経済的征服のような形で表れています。もちろん、これは過去と同じ形では起こりません。また世界的な核抑止力は、現在の議論で頻繁に忘れられていますが、まだ存在しています。それは今なお大きな危険を孕みながら地下のバンカーに鎮座しています。

そしてサイバーセキュリティがあります。 紛争、エスカレーション、権力の投影、干渉などのより深い技術についての興味深い点は、我々は「大きな戦争」を行うことなく戦争を学んだという事実です。サイバーオペレーションと情報操作は、主に時間の経過とともに侵食的な影響を及ぼす可能性がありますが、物理的なエスカレーションや政治的報復のリスクが高い場合は、それを用いることで従来の紛争とほぼ同じ目的を達成できます。 そして、Covid-19 の経済状況の悪化により、サイバー防衛が危機後の最も重要な次の問題になる理由もそこにあります。

例えば、多くの既に貧しく失敗した国家がついに崩壊することが考えられます。 公務員の給与はもはや支払われず、教育、経済、税金はもはや維持されず、警察と軍隊は武装した反乱者、腐敗した日和見主義者または犯罪集団になります。 隣国は、彼ら自身支援する余裕もなく、地域紛争が起こり、古い国家関係が崩壊する可能性があります。 国連、北大西洋条約機構(NATO)、EU などの大規模な国際財閥は、財政的に弱体化し、加盟国のナショナリズム的傾向(すでに強い傾向)によって支配されている可能性があり、散発的にも象徴的にも助けることができないでしょう。したがって、小さな国の多くは、経済的にも政治的にも安定するための新しい手段を探さなければならないかもしれません。これらの新しい手段の多くは破壊的で直接的であり、まさにこれらの手段によって貧困と孤立から脱出した他の国々の高い成功に続いて、サイバー作戦の実質的な使用を伴う可能性があります。

これは、核抑止力と同様に、多くの戦略的配慮で見落とされてきたものですが、サイバーは最近の多くの成功事例で重要な役割を果たしました。 北朝鮮は、国際的に孤立したときにお金を稼ぐ方法を示しています。 同国は長年にわたりサイバー恐喝やサイバー銀行強盗に従事しており、国を存続させてきました。 魅力的な前例となるモデルは、少なくともそのような活動は投資収益率が高く、追跡が困難であり、厳しく取り締まることができません。ほとんど無料に近い費用で、中国は工業化のためにコスト削減と制御の強化の素晴らしいモデルを提供してきました。知財の窃取、そのコピーペーストに呵責を感じないメンタリティ、破壊的な貿易慣行と人口を完全に制御する権威主義資本主義の迅速な建設、そしてそのようなことに対して国際的な処罰がほとんどないことが、各国がそのような形を通じての、自己再建を図るもう一つの背景を提供します。 特に、資本と統制の相互強化の二重性は興味深いインセンティブとなるでしょう。その多くはサイバーオペレーションによって達成できます。そして主な関心事が金銭的ではなく防衛とセキュリティであるならば、さまざまな種類のサイバー作戦が効果的で興味深いことが証明されています。核兵器を保有していない間に

抑止力を作ることを目指す国々は、イランのようにサイバー破壊活動の実質的な可能性を見出すかもしれません。そして、これはもちろん、他の支配的な種類のサイバー操作、すなわち情報操作をも含みます。政治プロセス、特に民主的なプロセスの不安定化を目的として、この新しい形態の高速かつ非常に拡張性があり、外科的に正確なプロパガンダは、戦争の下の将来の戦争の重要なツールを追加することになります。

しかし、崩壊した国家だけが問題を引き起こすわけではありません。先進国もまた、少なくとも経済的に、今後数年間ではるかに厳しい戦いをしなければならないわけです。経済政策と技術政策は、より競争力を高め、貧困と失業から多くの場所で生じるナショナリズム的傾向は、まだ予期せぬ形で結びつく可能性があります。新しい権力政治的ブロックをもたらす明示的または潜在的な貿易戦争は、新たな秩序を形作る可能性があります。そして、それらはまた破壊的な行為を伴うでしょう。産業スパイ活動と破壊活動は困難で永続的な問題であり、残念ながら主に良好な防護技術ではなく、国際的な抑制によって抑えられています。先鋭化する活動、国際協力の低下、暴力を伴わぬ活動の増加により、通常の容疑者だけでなく、あらゆる可能な方向からこのような活動は大幅に増加する可能性があります。サイバー産業スパイは技術と投資政策の一般的なツールとなり、サイバー産業破壊活動は競合他社を排除し、後で低価格で購入し、重要なサプライチェーンを制御するような意図的に企業に害を与えるための活動として使用することもできます。

これらはもちろん、単なる架空の展開であり、これらが不適切で終末的なシナリオと考える人もいるかもしれません。しかし、これらのことは小規模であれ、あるいは少し異なる形であれ存在しているのです。それらは破綻しかけの国家の経済を構築したり、戦略を安定させる価値を証明しました。そして、それらは実際に戦争やリスク報復に行くことなく、戦争のすべての利益を得るための選択肢を提供しています。歴史は完全に繰り返されることはありませんが、同じような過去の話は今また繰り返されるのかもしれません。

今回の CYDEF2020 で、このような発展に警戒しなければならないのは、我々参加者でありその話を聴講する皆様です。思想家、発明家、アナリスト、サイバーセキュリティのストラテジスト。そして、少なくとも部分的には、世界の平和、公平性、安定のために Covid-19 の脱落の中長期的な動向を監視しなければならないのは我々なのです。

この文脈において、注意を喚起し、議論を深めていくこの会議が非常に重要であると考えています。Covid-19 とサイバーディフェンスの関連を議論し、専門的な知見を見出します。そして、同じ価値観を持つ国々が集うことで、真に世界的な意識と協力の覚醒のみならず、早期に脅威に対処することを可能にします。

この精神の中で、主催者一同、非常に成功したカンファレンスとなることを願っています。

2020 年 12 月 1 日

デジタルソサエティ研究所長（ESMT ベルリン）
サンドロ・ガイケン

Opening Remarks

Welcome to CYDEF.

The world may currently be focused on the more imminent threat of the global pandemic. But while that occupies the larger part of our political attention, other risks and threats did not stop to exist of course and are about to change their shape as a consequence of the pandemic as well.

Cybersecurity is one of them.

Early-on in our current crisis, French president Macron called for a worldwide peace during the fight against the pandemic. This was not for no reason. Even if the only thing we can learn from history is that we don't learn from history, a glimpse into our political past easily unveils the fact that global economic crises frequently spurred more physical crises. The reasons are obvious and present in our current scenario as well. Poverty or the threat thereof, a change in the global array of attitudes, allies and alignments, a lack of clear options, and, in that light, the more obvious and straightforward alternative of potentially profitable conquest. This, of course, will not happen in the same way it did in the past. The global nuclear deterrent, although frequently forgotten in our present debates, still exists, it sits majestically and quietly in its subterranean bunkers and will most likely still render any calculations involving larger aggressive activities unprofitable or at least too risky.

But exactly here comes cybersecurity. The interesting thing about the more deep tech versions of conflict, escalation, projections of power, interference etc is the fact that we learned to wage war without waging „big war". Cyberoperations and information operations can, mostly in erosive effects over time, achieve almost the same aims as conventional conflict did, but without the high risk of physical escalation or stronger political retaliation. And this is why, depending on how bad the economical fallout of Covid-19 will be, cyberdefense will be the most important next problem after the crisis.

It is plausible, for example, that many already poor and failing states will finally go to ruin. Public servants will no longer be paid, education, the economy and taxes will no longer be maintained, and the police and military will become armed putschists, corrupt opportunists or criminal gangs. Neighbors will not help these new failed states because they themselves cannot. Regional conflicts may arise, and old rivalries and nationalisms may be broken up. The large international conglomerates such as the UN, NATO and the EU may be financially weakened and dominated by nationalistic tendencies of their members - already a strong trend - and will also not be able to help little more than sporadically and symbolically. Accordingly, many of the smaller states will have to look for new means to stabilize themselves economically and politically. Many of these new means will be subversive and direct - and may involve substantial use of cyberoperations, following the high success of other countries who pulled themselves out of poverty and isolation by exactly these means.

This, like the nuclear deterrent, is something that has been overlooked as well in many strategic considerations, but cyber played a significant role in many recent success stories. North Korea has shown how to make money when internationally isolated. The country has been engaged in cyber blackmail and cyber bank robbery for years and has kept itself going. A model that will serve as an attractive precedent - not least because such activities have a high return on investment, are difficult

to track and will not result in tough countermeasures due to disproportionality. Free money, so to speak. For countries who are still able to invest into an industrialization, China has provided a great model of cutting costs and increasing control in that process. The theft of industrial knowhow, the copy-paste mentality while keeping wages low, the high speed version of authoritarian capitalism in combination with subversive trade practices and full control over the population - and all of that with little to no international punishment - will provide another backdrop against which countries may aim to rebuild themselves. Especially the mutually reinforcing duality of capital and control will be an interesting incentive. And again, much of that can be achieved by cyberoperations. And finally, if or once the main concern is not monetary but defense and security, different kinds of cyberoperations have proven effective and interesting as well. Countries aiming to create a deterrent while not in possession of nuclear arms may follow Iran's lead and develop substantial potential for cybersabotage. And this of course can be supported by the other dominant kind of cyberoperation: information operations. Aimed at a destabilization of political processes, in particular democratic processes, this new version of high speed, highly scalable and surgically precise propaganda will be another important addition in the toolbox of future warfare below warfare.

But not only failed states will bring problems. The large, established industrial nations will also have to fight much harder, at least economically, in the coming years. Economic policy and technology policy will become much more competitive, and the nationalistic tendencies arising in many places from poverty and unemployment may become intertwined in as yet unforeseeable ways. Trade wars, explicit or latent, which will result in new power-political blocs, could soon be the order of the day. And those will also involve subversive measures. Industrial espionage and sabotage are already a hard and persistent problem, which unfortunately is not kept in check primarily by good protection technologies but rather by international restraint. With sharper front lines, reduced relevance of international cooperation and greater tolerance of harsh measures below the threshold of physical violence, such activities may increase significantly. And from every possible direction, not only by the usual suspects. Cyber industrial espionage will become a common tool of technology and investment policy, cyber industrial sabotage will eliminate annoying competitors and can also be used to deliberately harm companies in order to buy them cheaply later and thus gain control over critical supply chains.

I will stop here. These are just hypothetical developments of course and some of you may consider them unwarranted and rather doomsday-ish scenarios. But they do exist in smaller or different forms. They have proven their value to build an economy or stabilize a strategy. And they do offer the option to gain all the benefits of war without actually going to war and risk retaliation. Concluding this little argument: while history may never entirely repeat itself, a new version of the same old story may soon unravel in a different form.

It is us, here at this conference, who have to be vigilant towards such developments. The thinkers, the inventors, the analysts and the strategists of cybersecurity. And, at least in part, it is us who will have to monitor the mid-term and long-term developments of the fallout of Covid-19 for global peace, fairness and stability.

December 1, 2020

Dr. Sandro Gaycken
Director, Digital Society Institute Berlin (ESMT Berlin)

サイバーディフェンスカンファレンス CYDEF 2020

1. 趣 旨

CYDEF は、2018 年より安全保障領域を中心としたサイバーセキュリティに関する議論の深化、知見の普及を図るため、国内外の学術・産業・政府、それに防衛部門の有識者を集めて開催している国際会議です。

今回の CYDEF2020 では現在世界の大きな脅威となっているコロナ禍を契機に国際環境、社会情勢が劇的に変化していることを議論できればと考えています。現在企業等の組織活動ではこれまでにない速度でテレワーク化が図られ、学校等の研究教育活動でも遠隔教育化が進み、政府の行政サービスのオンライン化も加速しています。リアルな関係からバーチャルな連携へ、それは可逆的なものではなく、不可逆的なものに思われますが、その先にある世界はどのようなものになるのでしょうか。

また社会の急激な変化は混乱を招きます。コロナウィルスの脅威からの退避のために、十分な準備のないままサイバー領域に持ち込まれつつある大量の情報は、格好の攻撃対象となっています。そのような現実にどのように対応していくべきなのでしょうか。

さらに 0 と 1 のバイナリで世界が形作られるサイバー領域にあっては、曖昧さは排除され、空間的バッファーは消散し、対立は先鋭化します。国家の活動も大きくサイバー領域に移りつつある今日、国家間の関係は緊張の度を高めつつありますが、それは今後どう進展していくのでしょうか。

このような話題等を、国内外の有識者と共に日英両語で広くオンラインにて議論し、理解を深め、協力の素地を作るための機会になればと考えています。

注：昨年開催した CYDEF2019 のプログラムは下記をご参照下さい。
http://cydef-j.com/CYDEF2019/CYDEF2019_main_ja.html

2. テーマ

「コロナ後のパワーシフトを読み解く」～変容する社会様相、ビジネス形態、安全保障環境～
“Power Shift after Corona- Taking life to the cyber domain”

コロナ禍以後の社会の変化とサイバー領域を中心とした社会のあり方の変容を検討し、様々な視座からそれに如何に対応していくべきかを議論できればと思います。

3. 主 催

サイバーディフェンス研究会、政策研究大学院大学
European School of Management and Technology Berlin
サイバーセキュリティ研究所、明治大学

4. 後 援

サイバーセキュリティ戦略本部
総務省
外務省
文部科学省
経済産業省
防衛省
CCD COE（Cooperative Cyber Defense Center of Excellence）
米陸軍サイバー研究所
在日本アメリカ合衆国大使館
在日本インド大使館
在日本エストニア共和国大使館

在日本オーストラリア連邦大使館
在日本ドイツ連邦共和国
在日本フランス共和国
新技術振興渡辺記念会
横須賀市
横須賀リサーチパーク
横須賀海洋・IT 教育の会
一般財団法人 機械振興協会 日本経済研究所
レンジフォース株式会社

注:府省庁等(建制順)、軍事機構、大使館(国名五十音順)、諸団体の順

5. 日 程
2020 年 12 月 2 日(水)～3 日(木) 16:00-23:20 (両日共)

6. 場 所
6.1 オンライン開催
インターネット上の接続要領(URL 等)は、あらかじめ参加登録者にお知らせします。
6.2 本 部
政策研究大学院大学に本部を置き、運営します。

7. プログラム

第 1 日目 (12 月 2 日 (水))

時間	イベントとテーマ	登壇者
16:00-16:15	ご挨拶 1-1	サイバーディフェンス研究会顧問, 衆議院議員(元防衛大臣) 中谷元 氏
	ご挨拶 1-2	ESMT Berlin 大学 サンドロ・ガイケン 博士
	ご挨拶 1-3	公益財団法人笹川平和財団理事長 角南篤 氏、
16:15-16:20	注意事項連絡	スタッフ
16:20-16:40	基調講演 1-1	NATO サイバー防衛部長 クリスチャン・リフランダー 氏
16:40-17:00	基調講演 1-2	統合幕僚監部 指揮通信システム部長 田浦尚之 陸将補
17:00-17:10	基調講演 1-3A	NATO CCDCOE 所長 ヤーク・タリエン 大佐
17:10-17:20	基調講演 1-3B	システムチェンジ財団・ HUS社社長 創業者 ルドルフ・ヒルティ氏,
17:20-18:40	パネルディスカッション 1-1 【サイバー防衛/外交】	MD: ESMT Berlin 大学 サンドロ・ガイケン 博士 MIT CSAIL 研究員 ジョン・マレリー 博士 エストニア外務省サイバー政策担当大使 ヘリ・ティルマ・クララ 氏 日本国外務省総合外交政策局審議官 兼 国連・サイバー政策担当大使 赤 堀 毅 氏
18:40-19:00	基調講演 1-4	米陸軍サイバー研究所 ジェシカ・ダウソン 少佐
19:00-19:20	基調講演 1-5	富士通システム統合研究所 田中達浩 元陸将補
19:20-19:40	基調講演 1-6	米海軍兵学校客員教授 クリス・イングリス 氏
19:40-20:50	パネルディスカッション 1-2 【日米豪印のネットワーク】	MD:政策研究大学院大学副学長、道下徳成 教授 広島大学・東海大学客員教授 佐々木孝博 元海将補 インド・オブザーバーリサーチ財団 トリシャ・レイ CNAS シニアフェロー マーチン・ラッサー博士 国家安全保障大学学長 ローリー・メドカルフ博士

21:00-21:20	基調講演 1-7	米国国家安全保障会議 サイバーセキュリティ部長代理　マイケル・クリップスタイン 博士
21:20-21:40	基調講演 1-8	宇宙安全保障研究所理事（元防衛装備庁長官） 渡辺秀明 氏
21:40-22:00	基調講演 1-9	豪州サイバー・クリティカルテクノロジー大使 トビアス・ファーキン 氏
22:00-23:10	パネルディスカッション 1-3 【サイバー法制】	MD：情報セキュリティ大学院大学 学長補佐、湯浅墾道 教授 駒澤綜合法律事務所長・代表弁護士 高橋郁夫 氏 MIT 国際関係研究センター主任研究員 ジョエル・ブレナー博士 ハザウェーグローバルストラテジー社長 メリッサ・ハザウェー 氏、
23:10-23:20	ご挨拶 1-4	スタッフ

第 2 日目（12 月 3 日（木））

時間	イベントとテーマ	登壇者
16:00-16:15	ご挨拶 2-1	明治大学学長 大六野 耕作 教授
	ご挨拶 2-2	政策研究大学院大学 副学長 道下 徳成 教授
	ご挨拶 2-3	機械振興協会経済研究所長 林良造 教授、
16:15-16:20	注意事項連絡	（スタッフ）
16:20-16:40	基調講演 2-1	ブリュッセル外交アカデミー経済外交部長 バーナード・バシル・シモン氏
16:40-17:00	基調講演 2-2	国立情報学研究所／東海大学情報通信学部、前内閣官房内閣サイバーセキュリティセンター副センター長　三角育生教授
17:00-17:20	基調講演 2-3	セキュア・アイシー代表取締役　北アジア担当営業ディレクター、マーケティングディレクター　クロシャール・威安太郎 氏
17:20-18:40	パネルディスカッション 2-1 【高等教育における サイバー防衛教育】	MD：近藤玲子氏、総務省　国際戦略局 通信規格課長 フランス陸軍士官学校サイバー作戦及びサイバー危機訓練教官ディデェール・ダネ 博士 ソルブ・レジーナ大学 フランチェスカ・スピダリエリ 教授、 東洋大学 満永拓邦 准教授 NATO 通信学校・イノベーション・開発学部長 タンピノンゴール・セバスチャン教授、
18:40-19:00	基調講演 2-4	情報経営イノベーション専門職大学 平山敏弘 教授
19:00-19:20	基調講演 2-5	米海軍大学、サイバーイノベーション政策研究所 クリス・デムチャック博士
19:20-19:40	基調講演 2-6	日本オラクル株式会社 松岡秀樹 元一等海佐
19:40-20:50	パネルディスカッション 2-2 先進的なサイバー技術（仮）	MD：サイバーディフェンス研究所 CTO ラウリ・コルツパルン 氏 アイテルファウンデーション社長、イミュニティ社創設者 デイブ・アイテル 氏 マージンリサーチ社創設者 ソフィア・ダントニ 氏、 株式会社モノリスワークス 最高技術責任者 吉村孝広 氏
21:00-21:20	基調講演 2-7	CSIS ジェームス・ルイス 上級副社長
21:20-21:40	基調講演 2-8	慶応義塾大学 手塚悟 教授
21:40-22:00	基調講演 2-9	元米国国土安全保障長官、チャートフグループ会長 マイケル・チャートフ 氏
22:00-23:10	パネルディスカッション 2-3 【企業におけるサイバー地政学の影響】	MD：早稲田大学 池上 重輔 教授 フランス国立音楽院（LeCNAM） フィリップ・ボマード 教授 ジェオエコノミクス社長 ロバート・コップス 氏 弁護士 近藤剛 氏
23:10-23:20	ご挨拶 2-4	CYDEF2020 実行委員長 矢野 義昭

8. 講 師

講師一覧及び講師略歴等は、別紙のとおり。

9. 案内・成果発表等

9.1 案内（Leaflet）
プログラム、登壇者等、会議の概要を記したリーフレットをオンランで配布します。

9.2 冊子（Brochure）
プログラム、登壇者等、会議の詳細を記したブローシャをオンラインで配布します。

9.3 プロシーディングス（Proceedings）
イベント終了後、希望される登壇者の方の論文を掲載する会議録を発簡します。

9.4 メディア
本イベントの内容を衆知するために、メディアの方々の取材を歓迎します。

9.5 アンケート
イベント終了後、ご感想を伺うアンケートを実施します。ご協力をお願い申し上げます。

10. 経 費
参加経費は無料です。

11. 備 考
使用言語は日本語と英語で、同時通訳をつける予定です。
視聴できなかった方のために、当日録画したビデオのなかで、登壇者にご了解いただけた者に関しては、終了後、年末（2020.12.31）までネット上で視聴できるように調整します。

講師一覧

別紙

1. 海外講師（Alphabetical order 敬称略、組織名略称使用）

アイテル、デイブ	アイテル・ファンデーション社長 イミュニティ創業者
ボマード、フィリップ	仏国立音楽院
ブレナー、ジョエル	MIT 国際問題研究所 上級研究員
チャートフ、マイケル	元米国土安全保障長官、チャートフグループ会長
クローチャード、慰安太郎	セキュア・アイシー代表取締役 北アジア担当営業ディレクター、マーケティングディレクター
ダネ、ディデェール	フランス陸軍士官学校サイバー空間作戦・サイバー危機訓練教官
ダントニ、ソフィア	マージンリサーチ創業者
ダウソン、ジェシカ	米陸軍サイバー研究所
ガイケン、サンドロ	ESMT ベルリン デジタルソサエティ研究所長
ハザウエー、メリッサ	ハザウエーグローバルストラテジー社長
ヒルティ、ルドルフ	システムチェンジ財団 & THE HUS 社長・創業者
イングリス、クリス	米海軍兵学校（サイバー担当）客員教授
クリップスタイン、マイケル	米国家安全保障会議サイバーセキュリティ部長代理
コエップ、ロバート	ジオエコノミックス社長
コルツパルン、ラウリ	サイバーディフェンス研究所 CTO
ルイス、ジェームス	CSIS 上級副社長
リフランダー、クリスチャン	NATO エマージング安全保障サイバー防衛部長
マルリー、ジョン	MIT 電算機科学・人工知能研究所 研究員
メドカルフ、ローリー	国家安全保障大学学長
ラッサー、マーチン	CNAS 上級研究員
レイ、トリシャ	インド・オブザーバーリサーチ財団
タンピノンゴール、セバスチャン	NATO 通信学校・イノベーション・開発学部長
シモン、バシール・バーナード	ブリュッセル自由大学 ブリュッセル政策アカデミー 金融政策部長
スピダリエリ、フランチェスカ	ソルブ・レジーナ大学教授
タリエン、ヤーク	NATO CCD COE 所長、エストニア空軍大佐
ティルマ＝クララ、ヘリ	エストニア国特命大使（サイバー政策担当）

2. 国内講師（五十音順、敬称略、組織名略称使用）

赤堀 毅	赤堀 毅　総合外交政策局審議官 兼 国連・サイバー政策担当大使
池 上 重輔	早稲田大学教授
近藤 剛	弁護士
近 藤 玲子	総務省 国際戦略局 通信規格課長
佐々木 孝博	株式会社富士通システム統合研究所、元海将補
角南 篤	公益財団法人笹川平和財団理事長
大六野 耕作	明治大学学長、教授
田 浦 尚之	防衛省 統合幕僚監部指揮通信システム部長、陸将補
高 橋 郁夫	駒澤綜合法律事務所長・代表弁護士
田 中 達浩	株式会社富士通システム統合研究所、元陸将補
手塚 悟	慶應義塾大学 環境情報学部 教授
中谷 元	サイバーディフェンス研究会顧問、衆議院議員（元防衛大臣）
林 良造	機械振興協会 経済研究所長
平 山 敏弘	iU 情報経営イノベーション専門職大学教授
松 岡 秀樹	日本オラクル株式会社、元一等海佐
三 角 育生	東海大学客員教授、前内閣審議官／経済産業省サイバーセキュリティ・情報化審議官
満永 拓邦	東洋大学 准教授
道 下 徳成	政策研究大学院大学副学長、教授
矢 野 義昭	CYDEF2020 実行委員長、元陸将補
湯 淺 墾道	情報セキュリティ大学院大学学長補佐、教授
吉 村 孝広	株式会社モノリスワークス 最高技術責任者
渡 辺 秀明	宇宙安全保障研究所理事（元防衛装備庁長官）

Cyber Defense Conference (CYDEF 2020)

1. Statement

CYDEF is an international conference held by experts from domestic and overseas academic, industrial, and government sectors as well as experts in the defense to deepen discussions and disseminate knowledge about cybersecurity centering on the security domain.

The first of these conferences, CYDEF2018, was held in April 2018. The theme was "Cyber Defense Capability Building" and had 35 speakers, including 17 from abroad and about 200 participants. The second conference, CYDEF2019, was held in October 2019. It had 58 speakers, 21 from overseas, and about 350 participants. The theme was "Assessing National Risk and Establishing Multi Stakeholder Cooperation in Cyber Defense".

In CYDEF2020 we hope to discuss the dramatic changes in the international environment and social conditions triggered by the Coronavirus disaster, which is currently a major threat to the world. Teleworking is being promoted at an unprecedented rate for organizational activities in companies; remote education is being promoted for research and educational activities in schools, while the online presence of government administrative services is accelerating. Moving from a real relationship to a virtual one seems to be an irreversible trend, but what will the future be like?

Rapid changes in society are also a cause for confusion. The large amount of information brought into cyberspace to avoid the coronavirus threat, often without adequate preparation, is a prime target for attacks. How should we deal with such reality?

Furthermore, in the cyber realm, ambiguity is often eliminated, spatial buffers are dissipated, and conflicts are sharpened. Nowadays, as the activities of nations are largely moving to the cyber sphere, relations between nations are becoming tenser. How will that develop in the future?

We hope that this will be an opportunity to discuss such topics with a wide range of experts online, deepen their understanding, and lay the groundwork for further cooperation.

Note: Please show program of CYDEF 2019 as follows,
http://cydef-j.com/CYDEF2019/CYDEF2019_main_en.html

2. Theme

“Power Shift after Corona – Taking Life to the Cyber Domain”

3. Program Organizations

The Cyber Defense Study Group, National Graduate Institute for Policy Studies (GRIPS)
Digital Society Institute, European School of Management & Technology, Germany
Meiji University, Cybersecurity Laboratory

4. Sponsoring Organizations

National center of Incident readiness and Strategy for Cybersecurity
Ministry of Internal Affairs and Communications

Ministry of Foreign Affairs of Japan
Ministry of Education, Culture, Sports, Science and Technology
Ministry of Economy, Trade and Industry
Ministry of Defense
Cooperative Cyber Defense Center of Excellence (CCD COE)
Army Cyber Institute (ACI), U.S. Army
Australian Embassy in Japan
Embassy of the Republic of Estonia in Japan
Embassy of France in Japan
Embassy of Germany in Japan
Embassy of India in Japan
U.S. Embassy in Japan
City of Yokosuka
The Watanabe Memorial Foundation for the Advancement of TechnologyYokosuka Research Park
The Educational Association for Ocean and Information Technology in Yokosuka
Japan Economic Research Institute, Machinery Industry Promotion Association
Rangeforce, Inc

Note: Central government of Japan, Military Organizations, Embassies in Japan
(Alphabetical order of Nation-name.)

5. Days
December 2 to December 3, 2020

6. Place
6.1 Online Cnference thru the Internet Channels
6.2 Staff Rooms
National Graduate Institute for Policy Studies (GRIPS)

7. Programm

DAY 1(2nd Dec. (Wed)): National Security after Corona

TIME	THEME	SPEAKERS
16:00-16:15	Greeting 1-1	Hon. Mr. Gen Nakatani, Advisor, Cyber Defense Study Group, a member of the House of Representatives, Former Minister of Defense
	Greeting 1-2	Dr. Sandro Gaycken, ESMT Berlin
	Greeting 1-3	Dr. Atsushi Sunami, President of Sasagawa Peace Foundation
16:15-16:20	Cautions Remark1	STAFF
16:20-16:40	Keynote Speech 1-1	Mr. Christian Lifländer, Head of the Cyber Defence Section, Emerging Challenges Div., NATO
16:40-17:00	Keynote Speech 1-2	MG Naoyuki Taura, Director General, J-6/JJS, Ministry of Defense
17:00-17:10	Keynote Speech 1-3A	Col. Jaak Tarien, Director, NATO Cooperative Cyber Defence Centre of Excellence
17:10-17:20	Keynote Speech 1-3B	Mr. Rudolf Hilti, Founder & Presidentof The System Change Foundation & THE HUS
17:20-18:40	Panel Discussion 1-1 【Cyber Defense /Diplomacy】	Moderator / Dr. Sandro Gaycken, ESMT Berlin
		Mr. John Mallery, Research Affiliate, MIT Computer Science & Artificial Intelligence Laboratory (CSAIL)
		Ms. Heli Tiirmaa-Klaar, Estonian Ambassador-at-Large for Cyber Diplomacy

		Mr. Takeshi Akahori, Ambassador (United Nations Affairs, Cyber Policy), Deputy Assistant Minister, Foreign Policy Bureau, Ministry of Foreign Affairs of Japan (MOFA)
18:40-19:00	Keynote Speech 1-4	Maj Jessica Dawson, Army Cyber Institute, U.S. Army
19:00-19:20	Keynote Speech 1-5	MG (ret) Tatsuhiro Tanaka, Fujitsu System Integration Laboratories Ltd.
19:20-19:40	Keynote Speech 1-6	John C. (Chris) Inglis, Visiting Professor of Cyber Studies, United States Naval Academy
19:40-20:50	Panel Discussion 1-2 【Quad Corporation】	MD: Dr. Narshige Michishita, Vice President/Professor, National Graduate Research Institute for Policy Studies
		RADM(ret.) Takahiro Sasaki, Visiting Professor, Hiroshima University and Tokai University,
		Ms. Trisha Ray, Observer Research Foundation
		Dr. Martijn Rasser, Senior Fellow, CNAS
		Dr. Rory Medcalf, Head of College, National Security College Austlaria
21:00-21:15	Keynote Speech 1-7	Dr. Michael Kripstein, Acting Director of Cybersecurity, United States National Security Council
21:20-21:40	Keynote Speech 1-8	Dr. Hideaki Watanabe, former Acquisition Technology and Logistics Agency
21:40-22:00	Keynote Speech 1-9	Dr Tobias Feakin, Ambassador for Cyber Affairs and Critical Technology
22:00-23:10	Panel Discussion 1-3 【Law Enforcement】	MD: Harumichi Yuasa, Deputy President, Professor, Institute of Information Security
		Mr. Ikuo Takahashi, CEO and Lawyer, Komazawa Legal Chambers
		JD. Joel Brenner, Senior Research Fellow of MIT Center for International Studies
		Melissa Hathaway, President, Hatherway Global Strategies
23:10-23:20	Greeting 1-4	STAFF

DAY 2(3rd Dec. (Thu)): Citizen Life after Corona

TIME	THEME	SPEAKERS
16:00-16:15	Greeting 2-1	President, Professor Kosaku Dairokuno, Meiji University
	Greeting 2-2	Dr. Narushige Michishita, Vice President/Professor, National Graduate Institute for Policy Studies
	Greeting 2-3	Dr. Ryozo Hayashi, Chairman of Economic Research Institute, Machinery Industry Promotion Association
16:15-16:20	Cautions Remark	STAFF
16:20-16:40	Keynote Speech 2-1	Bashir Bernard Siman, O.B.E. Associate Professor Department of World Politics Koninklijke Militaire School/ecole royale militaire/ Royal Military Academy Belgium
16:40-17:00	Keynote Speech 2-2	Dr. Ikuo Misumi, Visiting Professor of National Institute of Informatics/ Tokai University, Former Councillor (NISC), Deputy Director-General for Cybersecurity and IT (METI)
17:00-17:20	Keynote Speech 2-3	Mr. Yan-Tarō Clochard, North Asia Sales Director, Corporate Marketing Director, Secure-IC
17:20-18:40	Panel Discussion 2-1 【Cyber Education in High Education】	MD: Dr. Reiko Kondo, Councillor, Director, ICT Standardization Division, Global Strategy Bureau, Ministry of Internal Affairs and Communications
		Dr. Didier Danet, Training Officers to Cyber Operations and Cyber Crisis, Military Academy of Saint-Cyr
		Professor Francesca Spidalieri, Salve Regina University
		Dr. Takuho Mitsunaga, Toyo University
		Professor Tampinongkol Sebastiaan, Head of Learning Innovation and Development of NATO Commmunication & information Academy
18:40-19:00	Keynote Speech 2-4	Professor Toshihiro Hirayama, Professional University of Information and Management for Innovation (i-University)
19:00-19:20	Keynote Speech 2-5	Dr. Chris Demchak, U.S. Naval War College, Cyber and Innovation Policy Institute
19:20-19:40	Keynote Speech 2-6	CAPT(ret.) Hideki Matsuoka, Oracle Corporation Japan
19:40-20:50	Panel Discussion 2-2 【Cyber Advanced Technology】	MD: Mr. Lauri Korts-Pärn, CTO, Cyber Defense Institute
		Mr. Dave Aitel, President, Aitel Foundation, Founder, Immunity Inc.
		Ms. Sophia D'Antoine, Founder, Margin Research
		Mr. Takahiro Yoshimura, CTO of Monoris Works
21:00-21:20	Keynote Speech 2-7	Mr. James Lewis, Senior Vice President, CSIS
21:20-21:40	Keynote Speech 2-8	Professor Satoru Tezuka, Keio University
21:40-22:00	Keynote Speech 2-9	JD. Michael Chertoff, Former Secretary Department of Homeland Security, Executive Chairman and Co-Founder, The Chertoff Group
22:00-23:10	Panel Discussion 2-3 【 Impact of Cyber Geopolitics on Industrial security and Companies】	MD: Proffesor Jusuke JJ Ikegami, Waseda Univercity
		Dr. Philippe Baumard, LeCNAM
		Mr. Robert Koepp, Principal of Geoeconomix
		Mr. Go Kondo, Attorney-at-Law, UTOKU LAW OFFICES &Res. LTC
23:00-23:20	Greeting 2-4	MG(ret.) Yoshiaki Yano, Chairman of Executive Committee, CYDEF 2020

8. Speakers

See Appendix A for the speakers and their profiles.

9. Public affair and products

9.1 Leaflet

Leaflet including program, list of speakers and outlines of workshop, was promulgated by online.

9.2 Borochure

This Borochure including program, speakers' cv and details of workshop, was promulgated by online.

9.3 Proceedings

Proceedings including papers of speakers, will be published.

9.4 Mass Media

We welcome to the interview to publicize this event.

9.5 Questionnaire

We will prepare short questionnaires after workshop. Your understanding and cooperation are greatly appreciated.

10. Attending fee

None

11. Others

In workshop, Speakers will use Japanese or English, so we will prepare the simultaneous interpreting. For the people who couldn't attend this workshop, we will publish key video files on CYDEF 2020 website until end of this year.

Appendix A: Speakers

In this appendix the CVs and other information of Speaker are listed upon by alphabetical order of their family name initials. Titles omitted these tables as below.

1. Oversea speakers by the alphabetical order.

Aitel, Dave	President, Aitel Foundation, Founder, Immunity Inc.
Baumard, Philip	LeCNAM
Brenner, Joel	Senior Research Fellow, MIT Center for International Studies
Chertoff, Michael	Former Secretary Department of Homeland Security; Executive Chairman and Co-Founder, The Chertoff Group
Clochard, Yan-Taro	Director, Secure-IC
Danet, Didier	Training Officers to Cyber Operations and Cyber Crisis, Military Academy of Saint-Cyr
D'Antoine, Sophia	Margin Research
Dawson, Jessica	Army Cyber Institute, US Army
Gaycken, Sandro	Director, Digital Society Institute Berlin (ESMT Berlin)
Hathaway, Melissa	President, Hathaway Global Strategies
Hilti, Rudlf	Founder & Presidentof The System Change Foundation & THE HUS
Inglis, John Chris	Visiting Professor of Cyber Studies, USNA
Klipstein, Michael	Acting Director Cybersecurity, United States National Security Council
Koepp, Robert	Principal, Geoeconomix
Korts-Pärn, Lauri	CTO, Cyberdefense Institute, Inc., Japan
Lewis, James	Senior Vice President, CSIS
Lifländer, Christian	of the Cyber Defence Section, Emerging Challenges Div., NATO
Mallery, John	Research Affiliate, MIT Computer Science & Artificial Intelligence Laboratory (CSAIL)
Medcalf, Rory	Head of College, National Security College Austlaria
Rasser, Martijn	Senior Fellow, CNAS
Ray, Trisha	Observer Research Foundation
Sebastiaan, Tampinongkol	Professor, Head of Learning Innovation and Development of NATO Commmunication & information Academy
Siman, Bashir Bernard	Associate Professor Department of World Politics Koninklijke Militaire School/ecole royale militaire/ Royal Military Academy Belgium
Spidalieri, Francesca	Salve Regina University
Tarien, Jaak	Director of NATO Cooperative Cyber Defence Centre of Excellence
Tiirmaa-Klaar, Heli	Ambassador-at Large for Cyber Diplomacy at the Estonian Ministry of Foreign Affairs

2. Japanese speakers by alphabetical order.

Akahori, Takeshi	Ambassador (United Nations Affairs, Cyber Policy) /Deputy Assistant Minister, Foreign Policy Bureau, MoFA
Ikegami Jyusuke,	Professor Waseda Univ.
Kondo, Go	Lawyer
Kondo, Reiko	Director, ICT Standardization Division, Global Strategy Bureau, Ministry of Internal Affairs and Communications
Sasaki, Takahiro	Visiting Professor, Hiroshima University and Tokai University, RADM (ret.)
Sunami Atsushi,	President of Sasagawa Peace Foundation
Dairokuno, Kosaku,	President, Professor, Meiji University
Taura, Naoyuki	Director General, C4 Systems Department(J-6), Joint Staff, MoD, MG Matsuoka,
Takahashi, Ikuo	CEO and Lawyer, Komazawa Legal Chambers
Tanaka, Tatsuhiro	Fujitsu System Integration Laboratories Ltd., MG (ret.)
Tezuka Satoru	Professor of Environment and Information Studies, Keio University
Nakatani, Gen	Advisor, CDSG, a Member of the House of Representative, Former Minister of Defense
Hayashi Ryozo,	Japan Society for the Promotion of Machine Industry Economic Research Institute
Hirayama Toshihiro	Professor of Information Management Innovation Professional graduate school
Matsuoka Hideki	Oracle Corporation Japan, CAPT (ret.)
Misumi, Ikuo	Dr. Ikuo Misumi, Visiting Professor of National Institute of Informatics/ Tokai University, Former Councillor (NISC), Deputy Director-General for Cybersecurity and IT (METI)
Michishita, Narushige	Vice President, Professor, National Graduate Institute for Policy Studies (GRIPS)
Mitsunaga Takuho	Associate Professor, Toyo University
Yano, Yoshiaki (ret.)	Chairman, Executive Committee, CYDEF2020, BG
Watanabe, Hideaki	Director, Japan Institute for Space and Security
Yuasa Harumichi	Professor, Institute of Information Security
Yoshimura, Takahiro	CTO, Monolith Works Inc.

Aitel アイテル

1.　氏名及び役職名等（Name and Title）

デイブ・アイテル、アイテル・ファウンデーション、イムニティ創業者
Mr. Dave Aitel, Aitel Foundation, Founder, Immunity, Inc.

2.　略歴（CV）

国家安全保障局（1997 年）
@ステーク（2000 年）
Immunity（2002 年）
Cyxtera（2018 年）

National Security Agency (1997),
@stake (2000),
Immunity (2002),
Cyxtera (2018)

3.　参加枠（Time Slot）

Day 2, 19:40-20:50: Panel Discussion 2-2

4.　講義要約（Abstract）

高度技術
Advanced Technology

サイバーセキュリティにおけるリスクを測ることは、特に国家規模の脅威が発生したとき、高度な攻撃者とその背後に潜む者とのバランスを見ることにある。わたしの講演では、幾つかの実例を挙げて速度と規模のリスク尺度を見る。ブラウザー攻撃の尺度、ビデオゲームのサプライチェーンの脆弱性、さらに重要度が希なものから戦略的なものまで幾つかの攻撃事例を示す。

Scaling risks is the balance between understanding advanced attackers and falling behind when it comes to national-grade threats. In this talk we will discuss several examples of how risks scale in either speed or scope.　Browser attacks at scale, the risks of supply chain weaknesses in video games, and other attacks that can go from rare to strategic in importance.

Baumard バーマード

1. 氏名及び役職名等（Name and Title）

フィリップ・バーマード
Philip Baumard, LeCNAM

2. 参加枠（Time Slot）

Day 2, 22:00-23:10: Panel Discussion 2-3

Brenner ブレナー

1. 氏名及び役職名等（Name and Title）

ジョエル・ブレナー、マサチューセッツ工科大学国際問題研究所 上級研究員
Joel Brenner, Senior Fellow, MIT Center for International Studies

2. 略歴（CV）

元・国家安全保障庁（NSA）観察総監
元・国家情報長官官房カウンターインテリジェンス局長
元・連邦検事、長期間地方検事を務め機微な国際取引の経験を有す。
著書『脆弱な米国：デジタルスパイ、犯罪及び戦争の内側』

Former Inspector General, National Security Agency;
former head of U.S. counterintelligence, Office of Director of National Intelligence;
former federal prosecutor and longtime attorney in private practice specializing in sensitive international transactions; author of *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*

3. 参加枠（Time Slot）

Day 1, 22:00-23:10: Panel Discussion 1-3

Chertoff チャートフ

1. 氏名及び役職名等（Name and Title）

   マイケル・チャートフ博士、元米国土安全保障長官、チャートフグループ会長
   JD Michael Chertoff, Former Secretary Department of Homeland Security;
   Executive Chairman and Co-Founder, The Chertoff Group

2. 参加枠（Time Slot）

   Day 2, 21:40-22:00：Keynote Speech 2-9

Clochard クロシャール

1. 氏名及び役職名等（Name and Title）

クロシャール・威安太郎、セキュア・アイシー代表取締役 北アジア担当営業ディレクター、マーケティングディレクター
Mr. Yan-Tarō Clochard, North Asia Sales Director, Corporate Marketing Director, Secure-IC

2. 略歴（CV）

かれの前職は在日フランス大使館職員として、科学技術の二国間協力（特にサイバーセキュリティ、5G、AI等）を推進してきた。また、通信事業者ノキアのモバイルネットワークのプリセールスマネージャとして勤務した。フランスの国立高等電子応用大学院（ENSEA）において電子工学を専攻、ESSEC ビジネススクール（仏・星）においてビジネス修士号を取得している。

He is a former member of the French Embassy in Japan, developing Science and Technology bilateral cooperation (especially on cybersecurity, 5G, AI, etc.). He previously worked in the Telecommunication industry for Nokia as presales manager for Mobile networks. He graduated in electronics engineering from "École Nationale Supérieure de l'Électronique et de ses Applications" (ENSEA) in France and holds a Master in Business from ESSEC Business school (France/Singapore).

3. 参加枠（Time Slot）

Day 2, 17:00-17:20: Keynote Speech 2-3

4. 講義要約（Abstract）

コロナウイルスの襲来後、緊要な資材の供給が危機的になったことが明白化した。国際サプライチェーンにおける（ハードウエア・トロイのような）弱点を議論し、それを発見する方法を導く。旅行の制約と、増大する国　際間の緊張により、信頼すべきパートナーを得て、地域における国家安全保障チップセットを形成する能力が重視される。従って、国際的なサイバーセキュリティ企業においては、マルチ・ローカルな主要ステークホルダを緊密に支援する試みが課せられている。

**Clearly after Corona virus hit, the way to supply critical secure components is becoming critical.
There are questions to be addressed in the weak points of international supply chains (such as the presence of Hardware Trojans) and the way to detect that.
Also, with travel restrictions and increased international pressure, there is a need to have local capability for national security chipsets with trusted partners.
International cybersecurity companies must therefore reinforce their multi-local approach to support key stakeholders in the closest possible way.**

Danet　ダネ

1. 氏名及び役職名等（Name and Title）

ディデェール・ダネ博士、サン・シール陸軍士官学校 サイバー作戦及びサイバー危機訓練教官
Dr. Didier Danet, Training Officers to Cyber Operations and Cyber Crisis, Military Academy of Saint-Cyr

2. 参加枠（Time Slot）

Day 2, 17:20-18:40: Panel Discussion 2-1

3. 講義要約（Abstract）

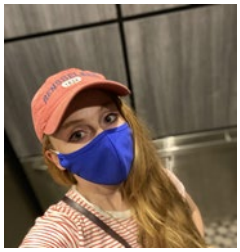
サイバー運用とサイバー危機に対する人材の育成:
Training Officers to Cyber Operations and Cyber Crisis:

サイバー運用の計画と実施 (防御的・攻撃的な運用の両方) には、技術的な専門知識以上のものが必要である。担当人材は、サイバー空間の重要性の高まりに関連する機会の全範囲をつかむために、社会科学の知識と軍事運用経験を統合する必要がある。

Planning and implementing Cyber operations (both defensive and offensive) require more than just technical expertise. Officers in charge must integrate social sciences knowledge and military operational experience in order to seize the whole range of opportunities associated with the growing importance of cyber space for the armed forces.

d'Antoine　ダントニ

1. 氏名及び役職名等（Name and Title）



ソフィア・ダントニ、マージンリサーチ
Ms. Sophia d'Antoine, Margin Research

2. 略歴（CV）

ソフィア・ダントニはニーヨークにサイバーセキュリティ・ファームのマージンリサーチ社を創業し、脆弱性検知　のプログラム分析に関する教育を開始した。彼女は（ブラックハット、DEFCON を含む）何十ものセキュリティ・カンファレンスにおいてハードウェアハッキング、CPU 最適化攻撃などについて講演した。また、モバイルデバイス、SCADA システムほか、特殊なアーキテクチャについても経験がある。国家安全保障局（NSA）から、民間企業に至る経験により、彼女はセキュリティ課題に関する幅広い理解を提供できる。

Sophia d'Antoine founded and runs Margin Research, a cybersecurity firm out of New York City, and runs a training on program analysis for vulnerability researchers. She has spoken at dozens of global security conferences worldwide including Blackhat, and Defcon on topics such as hardware hacking, and exploiting CPU optimizations. In the past she has worked extensively on mobile devices, SCADA systems, and other unique architectures. Her work at the National Security Agency (NSA) as well as private sector companies, has provided her with a broad understanding of security issues across the spectrum.

3．参加枠（Time Slot）

Day 2, 19:40-20:50: Panel Discussion 2-2

4. 講義要約（Abstract）

「オープンソースのコードベースにおける情報作戦」
Information Operations in Open Source Codebases

情報作戦は規模と複雑性を増大させている。殆どの分析努力は SNS やメディアに向けられ、そのコンテンツ、政策面、世論を見ている。この講義においては、さらに曖昧な応用的攻撃であるオープンソースコミュニティへの攻撃を取り上げる。これらコミュニティにおいても、同様の情報作戦の戦術が適用され、偽の貢献者に対する尊敬の集中、複合した要求への承認が行われる。これらの作戦の帰結について議論し、オープンソース・エコシステムの弱体化を暗示する脆弱点を考察する。

Information operations has only grown in scale and complexity. Most of the analysis has focused on social or media platforms, looking at content, politics, and opinions. In this presentation we will cover a far more obscure application of these attacks --open source communities. In these communities the same information operation tactics can be seen being applied to raising a fake contributor's respect in the community or in raising support for a merge request approval. We will discuss the consequences of these operations and look at the vulnerability implications weakening our open source ecosystem

Dawson ダウソン

1. 氏名及び役職名等（Name and Title）

ジェシカ・ダウソン少佐、博士 米陸軍サイバー研究所 研究員
Jessica Dawson, Maj, Ph.D, Research Scientist, Army Cyber Institute,U.S. Army

2. 略歴（CV）

ジェシカドーソン少佐は、メイン州出身で、1995年に陸軍に入隊し、1等軍曹迄承認した後、OCSを経て通信部隊の将校になった。 MAJドーソンは、韓国、ドイツ、イラク、フォートフッドで勤務に就いた。 現在は陸軍サイバー研究所の情報戦チームの主任研究員を務め、ウェストポイントの行動科学とリーダーシップ学科で社会学を教えている。彼女はデューク大学で社会学の博士号を取得し、現在、ソーシャルメディアと過激主義と社会プロセスのデジタル破壊の影響を研究している。

MAJ Jessica Dawson is a native of rural Maine who enlisted in the Army in 1995 and reached the rank of Sergeant First Class before she commissioned into the Signal Corps in 2007 through OCS. MAJ Dawson has served in Korea, Germany, Iraq and Fort Hood. She is currently serving as the lead research scientist for the Army Cyber Institute's Information Warfare team and teaches sociology in the Department Behavioral Sciences and Leadership at West Point. She holds a Ph.D. in sociology from Duke University and is currently researching social media and extremism along with the implications of the digital disruption of social processes.

3. 参加枠（Time Slot）

Day 1, 18:40-19:00：Keynote Speech 1-4

4. 講義要約（Abstract）

ポストCOVID時代の情報操作と信頼
Misinformation and Trust in a Post COVID world

Demchak デムチャック

1. 氏名及び役職名等（Name and Title）

クリス・デムチャック陸軍中佐（退役）、米海軍大学教授
Professor Chris Demchak, LTC(ret.) , U.S. Naval War College

2. 略歴（CV）

戦略・作戦研究部、米海軍大学（旧戦略研究部）
グレース・ホッパー准将サイバーセキュリテイ講座教授、2017 年から現在
グレース M. ホッパー准将サイバーセキュリティ教授、2014 年から現在
教授職拝命、2011 年から現在
准教授、2009 から 2011 年
サイバー・イノベーション政策研究所、米海軍大学
上級サイバー学者、2018 年 9 月から現在
サイバー紛争学研究所、米海軍大学
部長、2016 年 2 月から 2018 年 8 月
副部長、2011 年から 2016 年 1 月
オックスフォード・マーチン校サイバーセキュリティ能力構築グローバルセンター、2015 年から現在
オックスフォード・マーチン・アソシエイト 作業部会1 国家サイバー政策及び防衛、2013 年から 2015 年
アリゾナ大学行政及び政策学、並びにアリゾナ大学政策科学部（統合）
准教授、1998 年から 2009 年

Strategic and Operational Research Department, US Naval War College (formerly Strategic Research Department)
RDML Grace Hopper Chair of Cyber Security, 2017 – present
RDML Grace M. Hopper Professor of Cyber Security, 2014 – present
Full Professor, 2011 – present
Associate Professor, 2009 – 2011
Cyber and Innovation Policy Institute, US Naval War College
Senior Cyber Scholar, September 2018 – present
Center for Cyber Conflict Studies, US Naval War College
Director, February 2016-August 2018
Co-Director, 2011 – 2016 January
Oxford Martin School, Global Centre for Cyber Security Capacity Building 2015-present
Oxford Martin Associate, WG1 National Cyber Policy and Defence, 2013–2015
School of Public Administration and Policy, University of Arizona
and (joint) Department of Political Science, University of Arizona
Associate Professor, 1998 – 2009.

3. 参加枠（Time Slot）

Day 2, 19:00-19:20: Keynote Speech 2-5

Feakin　ファーキン

1.　氏名及び役職名等（Name and Title）

トビアス・ファーキン博士、豪州サイバー問題・クリティカルテクノロジー大使
Tobias Feakin, Australian Ambassador for Cyber Affairs and Critical Technology

2.　略歴（CV）

トビアス・ファーキン博士は豪州のサイバー問題・クリティカルテクノロジー大使の任にある。かれは 2017 年にサイバー問題大使に就任し、その後、地政学的な技術問題に役割が広がった。かれは豪州の国家安全保障、外交政策、経済通商を推進、保護し、サイバー空間及び緊要な技術領域における国益を拡大するため、豪州政府全体による国際的な交流を推進している。

ファーキン大使は、豪州の「サイバーセキュリティ戦略」（2016 年）の策定につながる「豪州安全保障見直し」を支援した独立専門家委員会の一員であった。さらに、引き続き豪州の「国際サイバー関与戦略」策定にも貢献した。大使に指名される前は、豪州戦略政策研究所において、2012 年から 2016 年の間、国家安全保障部長を勤め、研究所内に国際サイバー政策センターを創設した。これ以前の 2006 年から 2012 年の間、かれはロンドンの連合王国軍事研究所の国家安全保障・抗堪性部長を勤めた。
ファーキン大使は、連合王国軍事研究所の主任研究員、カーネギー国際平和基金の金融サイバー支援グループに属し、サイバーセキュリティ及び国際金融システムに関する国際戦略を検討している。
ファーキン大使は安全保障の優等学士、国際政治及び安全保障学の哲学博士号をブラッドフォード大学で取得した。

Dr Tobias Feakin is Australia's inaugural Ambassador for Cyber Affairs and Critical Technology. He commenced as Ambassador for Cyber Affairs in January 2017, before having his mandate expanded to reflect the central role that technology issues have in geopolitics.
He leads Australia's Whole of Government international engagement to advance and protect Australia's national security, foreign policy, economic and trade, and development interests in cyberspace and critical technology.

Ambassador Feakin was a member of the Independent Panel of Experts that supported the Australian Cyber Security Review to produce Australia's 2016 Cyber Security Strategy. Following that, he led the creation of Australia's International Cyber Engagement Strategy.
Prior to his Ambassadorial appointment, Dr Feakin was the Director of National Security Programs at the Australian Strategic Policy Institute from 2012 to 2016 where he established the Institute's International Cyber Policy Centre. Prior to this he was Director for National Security and Resilience at the Royal United Services Institute in London from 2006-2012.
Ambassador Feakin is a Senior Fellow with the Royal United Services Institute and a member of the Carnegie Endowment for International Peace's FinCyber Advisory Group which focuses on developing an International Strategy for Cybersecurity and the Global Financial System. Ambassador Feakin holds an Honours Degree in Security Studies and a Doctorate of Philosophy in International Politics and Security Studies, both from the University of Bradford.

3.　参加枠（Time Slot）

Day 1, 21:40-22:00: Keynote Speech 1-9

4.　講義要約（Abstract）

国際的な視点から見たサイバーセキュリティ　COVID-19とオーストラリアの対応
International cyber security, COVID-19 and Australia's response

Gaycken　ガイケン

1. 氏名及び役職名等（Name and Title）

サンドロ・ガイケン博士、デジタルソサエティ研究所長（ESMT ベルリン）
Dr. Sandro Gaycken, Director, Digital Society Institute Berlin (ESMT Berlin)

2. 略歴（CV）

サンドロ・ゲイケン博士は、ESMTベルリンのデジタル社会研究所の創設者兼ディレクターである。彼は5つの科学的なモノグラフ、３つのサイバー戦争に関する研究、およびサイバーセキュリティに関する60以上の科学出版物を発表している。彼はオックスフォード・マーティン・スクール・フェローで、ハーバード・MITのサイバー防衛とサイバー規範に関する会議の委員であり、ハーバード・ケネディ・スクールのAIイニシアチブのシニアアドバイザーであり、フランスのエリート大学CNAMでプログラム横断サイバー部門で活躍しており、IEEEの査読者でもある。ドイツ政府顧問として、ドイツの対外サイバー政策戦略を策定し、ドイツ議会での発言も多い。ドイツの首相のドイツと中国のスパイなしの合意、産業スパイを軽減するためのホワイトハウスUSTRの努力、および核サイバーセキュリティを制御するためのIAEAとG8の取り組みにも貢献した。サイバー軍事問題では、ドイツ国防省で部門間のサイバー調整の取り組み行った。北大西洋条約機構(NATO)の軍事サイバーカウンターインテリジェンス問題の専門家として、中東地域において国家サイバー防衛戦略と技術を開発し実施するNATOのSPSプログラムのディレクターを務めている。また産業顧問として、スマートガンや半導体部品のセキュリティ評価から戦略的な産業開発問題に至るまで、9つの主要な業界調査を実施してきた。アンマーパートナーズやアリアンツベンチャーなどの大規模なドイツのサイバー投資家にアドバイスを提供し、アリアンツのサイバーリスク評価方法論を開発し、IT製品のセキュリティ品質を評価するための120の外部基準をリストするドイツのDIHKとSMEコミュニティのバイヤーズガイドを作成した。組み込みシステムと高度に安全な実行環境を提供する高保証セキュリティ会社SECURE ELEMENTS Ltd.を設立した。オープンな言説と公共の啓蒙に専念し、彼はドイツの主要な新聞に頻繁に投稿し、主流メディアのサイバー問題について定期的にコメントしている。

Dr Sandro Gaycken is founder and director of the Digital Society Institute at ESMT Berlin. He has published five scientific monographs, three on cyberwarfare, and more than 60 other scientific publications on cybersecurity. Sandro is an Oxford Martin School Fellow, a program committee member of Harvard-MIT's annual conference series on cyber defense and cyber norms, a Senior Advisor for the AI Initiative at Harvard Kennedy School, co-lead "Programme Transverse Sécurité Défense, Sec. Cybersecurity" at elite French university CNAM, an EastWest Senior Fellow, a Senior Fellow of the German Council on Foreign Relations, a member of the Conversation Circle Intelligence Services in Germany, and an IEEE permanent reviewer. As an advisor to the German government, he developed the German foreign cyber policy strategy, testified numerous times in German parliament, and conducted many parliamentary dialogues. He was instrumental in bringing about the German chancellory's German-Chinese No-Spy agreement, in the White House USTR's effort to mitigate industrial espionage, and in IAEA and G8 efforts to control nuclear cybersecurity. In cyber military affairs, Sandro served as part of the German MoD's cyber defense white book process, and moderated interdepartmental cyber coordination efforts. He serves as an expert witness in NATO military cyber counterintelligence cases, and as director in NATO's SPS program, which develops and implements national cyberdefense strategies and technologies in the Middle East region. As an industrial advisor, Sandro has conducted nine major industry studies, ranging from smartgun and semiconductor component security assessments to strategic industry development issues. He advises large German cyber investors such as ammerpartners and Allianz ventures, developed Allianz's cyber risk assessment methodology, and produced a buyer's guide for the German DIHK and SME community, which lists 120 external criteria to assess the security quality of an IT-product. Sandro also founded the high

assurance security company SECURE ELEMENTS Ltd., which offers impenetrable embedded systems and highly secure execution environments. Devoted to an open discourse and public enlightenment, he writes frequent op-eds in leading German newspapers, and he comments regularly on cyber matters on mainstream media outlets.

3. 参加枠（Time Slot）

Day 1, 16:05-16:10: Greeting 1-2
Day 1, 17:20-18:40: Panel Discussion 1-1

Hathaway ハザウエー

1. 氏名及び役職名等（Name and Title）

メリッサ・ハザウエー、ハザウエーグローバルストラテジー社長
Ms. Melissa Hathaway, President, Hathaway Global Strategies

2. 略歴（CV）

メリッサ・ハザウエーはサイバー空間政策及びサイバーセキュリティに関する指導的な専門家である。彼女は米大統領府の二つの要職に就いた。その一はバラク・オバ
マ大統領の「サイバー政策レビュー」の作成指揮を執り、ジョージ W.ブッシュ大統領の「包括的国家サイバーセキュリティイニシアチブ（CNCI）」作成の指導的立場にあった。ハザウエーグローバルストラテジー合
同会社の社長として、官民の顧客に対して戦略的コンサルティング及び戦略形成に関する学際的、多機関的な展望を提供した。三つの民間会社及び三つの NPO の取締役会に参加している。また、多数の官民組織の戦略的顧問に就任している。メリッサは政策と技術的専門性の特異な結合をもたらし、役員会において　は政府政策との交差を助言し、技術的及び産業界におけるトレンドを開発し、この分野における調達及び業務開発を推進する経済的な駆動者である。彼女は企業や国家に対応したサイバーセキュリティ関連の書物を出版した。彼女の主要な著作は、以下のウエブサイトで確認が可能であ
る 。 http://belfercenter.ksg.harvard.edu/experts/2132/melissa_hathaway.html

***MELISSA HATHAWAY* is a leading expert in cyberspace policy and cybersecurity. She served in two U.S. presidential administrations, spearheading the Cyberspace Policy Review for President Barack Obama and leading the Comprehensive National Cybersecurity Initiative (CNCI) for President George W. Bush. As President of Hathaway Global Strategies LLC, she brings a multi-disciplinary and multi-institutional perspective to strategic consulting and strategy formulation for public and private sector clients. Having served on the board of directors for three public companies and three non-profit organizations, and as a strategic advisor to a number of public and private companies, Melissa brings a unique combination of policy and technical expertise, as well as board room experience to help others better understand the intersection of government policy, developing technological and industry trends, and economic drivers that impact acquisition and business development strategy in this field. She publishes regularly on cybersecurity matters affecting companies and countries. Most of her articles can be found at the following website: http://belfercenter.ksg.harvard.edu/experts/2132/melissa_hathaway.html**

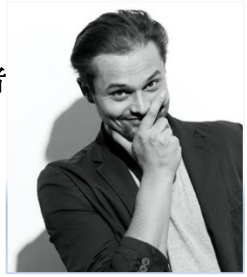
3. 参加枠（Time Slot）

Day 1, 22:00-23:10: Panel Discussion 1-3

4. 講義要約（Abstract）

「法令・規則上の強化」
Legal and Regulatory Enhancements

Hilti ヒルティ



1. **氏名及び役職名等（Name and Title）**

   ルドルフ・ヒルティ、システムチェンジファウンデーション & THE HUS 社長・創業者
   Rudolf Hilti, Founder & Presidentof The System Change Foundation & THE HUS

2. **略歴（CV）**

3. **参加枠（Time Slot）**
   Day 1, 17:10-17:20, : Keynote Speech 1-3B

4. **講義要約（Abstract）**

   システムとマインドセットの変更
   Systems and Mindset Change

Inglis イングリス

1. 氏名及び役職名等（Name and Title）

ジョン・クリス・イングリス 米海軍兵学校客員教授
John C. („Chris“) Inglis, Visiting Professor of Cyber Studies，United States Naval Academy

2. 略歴（CV）

米国海軍兵学校サイバーサイエンス学部客員教授、米国サイバースペースソラリウムミッション理事
米国国家安全保障局副長官

Visiting Professor of Cyber Studies , United States Naval Academy; Commissioner on the U.S. Cyberspace Solarium Commission; and former Deputy Director of the US National Security Agency

3. 参加枠（Time Slot）

Day 1, 19:20-19:40: Keynote Speech 1-6

4. 講義要約（Abstract）

2021 年のサイバーセキュリティに対する 2019 年パンデミックの教訓
Lessons from the 2019 Pandemic for 2021 Cybersecurity

全世界的パンデミックへの備えと公共衛生の防衛、全世界に拡散したサイバー脅威への備えと公共安全の　防衛を並行して説明する。
Describe the parallels between preparing for and defending public health in the face of a global pandemic, and the challenges of preparing for and defending public saftey in the face of global spread of cyber threats.

Klipstein クリップスタイン

1. 氏名及び役職名等（**Name and Title**）

マイケル・クリップスタイン、米国国家安全保障会議 サイバーセキュリティ部長代理
Maj Michael Klipstein, Acting Director Cybersecurity, United States National Security Council

2. 略歴（**CV**）

マイケル・クリップスタイン博士は、陸軍サイバー研究所の研究員、加えて卓越研究の主任でもある。彼の研究対象には、サイバー戦のリスク、国家レベルの政策、破壊的テクノロジーが含まれる。米サイバー軍、国家安全保障局（NSA）、国家サイバー任務部隊に勤務している。クリップスタイン博士は研究者として、将来の陸軍サイバーインフラが、よく情報を踏まえた開発ができるよう助言している。マイケルの博士論文、攻撃的サイバー作戦のリスク定量評価は、米陸軍で採用が検討されている。

Dr. Michael Klipstein is a researcher at the Army Cyber Institute in addition to being the Chief of Outreach. His research interests include risk in cyber warfare, national level policy, and disruptive technologies. He has worked in US Cyber Command, the National Security Agency, and the Cyber National Mission Force. As a researcher, Dr Klipstein looks to the future of Army cyber infrastructure to better inform development. Michael's dissertation on quantifying risk for offensive cyber operations is being evaluated by the US Army for implementation.

3. 参加枠（**Time Slot**）

Day 1. 21:00-21:15: Keynote Speech 1-7

4. 講義要約（**Abstract**）
国際的な海事サイバーセキュリティのコンセンサスをを構築する
Builing International Consensus for Maritime Cybersecurity

Koepp　コップ

1. 氏名及び役職名等（Name and Title）

ロバート・コップス氏、ジェオエコノミクス社長
Mr. Robert Koepp, Principal, Geoeconomix

2. 略歴（CV）

ロバート・コップス氏は、ロサンゼルスを拠点とするGeoeconomixの創設者兼社長である。ジェオエコノミクスでは、世界市場を動かし、技術を推進し、政府の力に影響を与える経済学についての洞察を得るための研究機関。また、香港を拠点とするフィンテック企業である**FinFabrik**の諮問委員会、およびシンガポール国立大学の人類人工知能技術センター（**AITH**）の諮問委員会にも参加しています。グローバルサイバーセキュリティの分野での最近の活動の中で、彼は「一帯一路イニシアチブにおけるデジタルシルクロードの特定」の章を、2021年春に国際戦略研究所（IISS）から出版される「中国のデジタル拡張：デジタルシルクロード」との本に寄稿します。www.geoeconomix.com

Robert Koepp is the founder and Principal of Los Angeles-based Geoeconomix, an independent source for insights into the economics moving global markets, driving technology, and influencing government power. He also serves on the Advisory Board for the Hong Kong-based fintech company, FinFabrik, and on the Advisory Council of the Center on AI Technology for Humankind (AITH) at National University of Singapore. Among his recent activities in the area of global cybersecurity, he is contributing the chapter, "Locating the Digital Silk Road in the Belt and Road Initiative," to *China's Digital Expansion: The Digital Silk Road*, being published by The International Institute of Strategic Studies in Spring 2021. www.geoeconomix.com

3. 参加枠（Time Slot）

Day 2, 22:00-23:10: Panel Discussion 2-3

Korts-Pärn　コルツパルン

1. 氏名及び役職名等（Name and Title）

ラウリ・コルツパルン、サイバーディフェンス研究所 CTO
Mr. Lauri Korts-Pärn, CTO, Cyberdefense Institute, Inc., Japan

2. 略歴（CV）

エストニア人で、20 年前前からセキュリティに関わりずつ、多数プログラミングも自然言語も操りながら日本の企業のセキュリティを攻撃者、教育者やディフェンダーの目線で支援しています。

As Estonian who has been involved in security for 20 years, and writing and speaking multiple programming and nartural languages, he has been supporting the security of Japanese companies from the perspective of an attacker, educator, and defender.

3. 参加枠（Time Slot）

Day 2, 19:40-20:50: Panel Discussion 2-2

4. 講義要約（Abstract）

「コロナ時代におけるサイバー攻撃脅威の技術状態」
State of cyber attack and threats at the age of Covid-19

コロナ時代に使われている攻撃手法や驚異を訪ねながら、この時代にサイバー空間でも安全にいられるために必要な選択肢を検討する

Looking at the risks of cyber attack technologies utilized at the age of COVID19, with the aim of bringing some clarity of what would be the most effective ways to combat threats and stay safe in cyber-space.

Lewis ルイス

1. 氏名及び役職名等（Name and Title）

   ジェイムス・アンドリュー・ルイス、CSIS 副所長
   Mr. James Andrew Lewis, Senior Vice President, CSIS

2. 参加枠（Time Slot）

   Day 2, 21:00-21:20: Panel Discussion 2-2

3. 講義要約（Abstract）

   「悪性サイバー行動の帰結」
   Consequences for Malicious Cyber Actions

   悪性サイバー活動の頻度は増大しつつあり、これに対抗するにはペナルティを与えるしかないというコンセンサスが増加しているが、複雑な運用課題が残されている。

   The pace of malicious cyber activity continues to increase and there is growing consensus that this will change only if there are penalties, but this poses difficult operatoinal issues.

Lifländer リフランダー

1. 氏名及び役職名等（Name and Title）

クリスチャン・リフランダー氏、NATO エマージングセキュリティ対策本部
サイバー防衛部長
Mr. Christian Lifländer, Head of the Cyber Defence Section,
Emerging Security Challenges Division, NATO

2. 略歴（CV）

クリスチャン・マーク・リフランダー氏は、NATO 国際スタッフの上級サイバー政策職員である。サイバー防衛部門の長として、NATO 横断的なサイバー防衛政策の作成及び徹底を図る立場にある。リフランダー氏は、エストニア国防軍予備役将校（歩兵科）であり、国防軍殊勲章及びエストニア防衛省殊勲章を叙勲している。リフランダー氏は米陸軍士官学校において科学学士号を、ジョージタウン大学 CSS において安全保障修士号を取得した。

Christian-Marc Lifländer serves as the senior cyber policy official of NATO's International Staff. As head of the Cyber Defence Section, he is responsible for leading the development and implementation of cyber defence policy across NATO.
Mr. Lifländer received a direct commission in the Estonian Defense Forces (Infantry) and has been awarded with the Estonian Defence Forces Distinguished Service Decoration as well as Distinguished Service Decorations of the Estonian Ministry of Defence
Mr. Lifländer received his Bachelor of Science Degree in Engineering from the United States Military Academy, West Point. He received his Master of Arts in Security Studies from Georgetown University's Center for Security Studies (CSS) in the Edmund A. Walsh School of Foreign Service.

3. 参加枠（Time Slot）

Day 1, 6:20-16:40: Key Note Speech 1-1

4. 講義要約（Abstract）

「コロナ後の国家安全保障」
National Security after Corona

われわれは業務の手法、人生の在り方が何度も変化するのを見てきた。大きな地政学的な変動について言及するのは、まだ、早い。しかし、ここに巨大であり、防衛すべき表層の転移が起こった。そして、われわれがすべきことは変わらない。リスク管理、資産管理等の以前と同じ基盤はまだ有効である。実際、レジリエンスを確保することが大切だ。どのネットワークも、サイバー攻撃者に便益を与えないよう構築され、運用されるべきだ。それはネットワークの性能が劣化した状況下でも同じである。同時にサイバーとは、もう、単独の能力ではない。サイバー空間の成熟により、「サイバー関連」の突出した脅威に対しては、サイバー能力が鍵となる推進者であり、戦力倍増効果をもたらすものである。サイバーツールが新しい方策、または、強化された方策により展開されるときでさえ、この変化が戦略・国家レベルで何を意味するかを明晰な視点で判断すべきである。多数の国家が法制を定義しようと試み、物理的暴力や戦争が消えないなか、サイバーは依然としてツールとして残る。COVID は、これらの伏在する国家の統制及び権力の力学を変化させない。最も大きな構造的変化は、グローバル化への抵抗、地域重視、サプライチェーンの国内化であると言われている。

While we've witnessed many changes in the way we do business and conduct our lives, it's likely somewhat early to talk big geopolitical shifts. While there is now a bigger and more diverse surface area to defend, what we need to do is not entirely new. The same fundamentals still apply—risk management, asset management, etc. Indeed, one constant will be the need to remain resilient. Any network must be built and operated in ways that deny benefits to cyber attackers. This includes being able to run

networks in a degraded environment. At the same time, cyber is no longer a standalone capability. The maturation of cyberspace has seen cyber capabilities become a key enabler, and force multiplier, for a protracted set of 'cyber-enabled' threats. Even as we see cyber tools being deployed in new or enhanced ways, however, we must remain clear eyed about what this change really means at a strategic/nation-state level. Cyber still remains one tool among many, states still get to define norms, and kinetic violence/warfare is not going anywhere. COVID isn't going to change these underlying dynamics of state control and power. That said, one of the larger structural changes could be a greater desire for less global, more regionalized and domestic supply chains.

Mallery　マルリー

1.　氏名及び役職名等（Name and Title）

ジョン・マルリー、マサチューセッツ工科大学（MIT）電算機科学・人工知能研究所（CSAIL）研究員
Mr. John Mallery, Research Affiliate, MIT Computer Science & Artificial Intelligence Laboratory（CSAIL）

2.　略歴（CV）

ジョン C. マルリーは、1980 年から MIT 電算機科学・人工知能研究所の研究員である。加えて、オックスフォード大学マーチン校の客員研究員、フランス国立工芸院（CNAM、パリ）の安全保障・防衛研究所の上級研究員、デジタルソサエティ研究所（ESMT ベルリン）の客員研究員でもある。かれの研究実績は、世界秩序へのサイバーインパクト、国家サイバー戦略、知財のサイバー窃盗防止、サイバー国際法及び信頼性醸成措置（CBM）、軍事的サイバー安定化措置、サイバー保全事故の経済論、サイバー防衛の技術的戦略などである。2016 年から、トラック 1.5 会議を開催し、同志同盟による政軍サイバー国際法を議論している。1990 年代には、ホワイトハウスの電子出版システムの主任アーキテクト及び開発者であった。さらには人工知能の専門家として、クリントン・アドミニストレーション（1992 年-2001 年）の機械学習及び自然言語解析などに尽力した。

John C. Mallery has been a researcher at the MIT Computer Science & Artificial Intelligence Laboratory since 1980. Additionally, he is an Oxford Martin School Associate, a Senior Fellow at the Security and Defence Research Centre of the Conservatoire National des Arts et Métiers (CNAM) in Paris, and an affiliate of the ESMT Digital Society Institute in Berlin. His recent research involves cyber impacts on world order, national cyber strategies, countering cyber-enabled theft of intellectual property, cyber norms and CBMs, military cyber stability, economics of cyber insecurity, and technical strategies for cyber defense. Since 2016, he has organized track 1.5 conferences with like-minded allies on political- military cyber norms. During the 1990s, he was the principal architect and developer of the White House Electronic Publications System that He is also an expert in Artificial intelligence, served the Clinton Administration from 1992-2001.machine learning, and natural language understanding.

3.　参加枠（Time Slot）

Day 1, 17:20-18:40: Panel Discussion 1-1

Medcalf　メドカルフ

1.　氏名及び役職名等（Name and Title）

ローリー・メドカルフ博士、国家安全保障大学学長
Dr. Rory Medcalf, Head of College, National Security College Austlaria

2.　参加枠（Time Slot）

Day 1, 19:40-20:50: Panel Discussion 1-2

Rasser ラッサー

1. 氏名及び役職名等（Name and Title）

マーチン・ラッサー博士、CNAS シニアフェロー
Dr. Martijn Rasser, Senior Fellow, CNAS

2. 略歴（CV）

マーティン・ラッサーは、新アメリカ安全保障センター(CNAS)の技術と国家安全保障プログラムのシニアフェローである。CNAS に入社する前は、中央情報局の上級情報部員兼アナリストを務め、外国の新興技術、技術革新、武器の研究開発に携わっていた。また、国防長官室の上級顧問、中東の上級軍司令官の特別顧問、イラクの米軍部隊とのテロ対策責任者連絡役、国家情報会議(NIC)ワーキンググループの副議長も務めた。
政府を離れると、ビジネス詐欺、会計詐欺、根本的な問題の調査に焦点を当てた投資調査会社、マディ・ウォーターズ・キャピタルの首席補佐官を務めた。 最近では、シリコンバレーのベンチャー支援 AI スタートアップ、キンディで分析ディレクターを務めた。
彼の解説と研究は、外交政策、ローファーレ、国益、サンフランシスコクロニクル、サイエンティフィックアメリカンに登場しており、アクシオス、ブルームバーグ、フォーチュン、ナショナルジャーナル、ニューヨークタイムズ、サウスチャイナモーニングポスト、米国ニュースと世界レポート、ウォールストリートジャーナル、WIRED などで定期的に引用されている。ラッサー氏はベイツ・カレッジで人類学の学士号を、ジョージタウン大学で安全保障研究の修士号を取得した。

Martijn Rasser is a Senior Fellow in the Technology and National Security Program at the Center for a New American Security (CNAS).Prior to joining CNAS, Mr. Rasser served as a senior intelligence officer and analyst at the Central Intelligence Agency, where he worked on foreign emerging technologies, technology innovation, and weapons research & development. He also served as a senior advisor in the Office of the Secretary of Defense, special advisor to a senior military commander in the Middle East, chief counterterrorism liaison to a U.S. military unit in Iraq, and vice chairman of a National Intelligence Council (NIC) working group.
Upon leaving government service, Mr. Rasser served as Chief of Staff at Muddy Waters Capital, an investment research firm focused on investigating business fraud, accounting fraud, and fundamental problems. More recently, Mr. Rasser was Director of Analysis at Kyndi, a venture-backed AI startup in Silicon Valley.
His commentary and research have appeared in Foreign Policy, Lawfare, The National Interest, the San Francisco Chronicle, and Scientific American, and he is regularly quoted in outlets such as Axios, Bloomberg, Fortune, National Journal, the New York Times, South China Morning Post, U.S. News and World Report, the Wall Street Journal, and WIRED. Mr. Rasser received his B.A. in anthropology from Bates College and his M.A. in Security Studies from Georgetown University.

1. 参加枠（Time Slot）

Day 1, 19:40-20:50: Panel Discussion 1-2

4. 講義要約（Abstract）

「クアッドテクノロジー政策の青写真」
A Blueprint for Quad Technology Policy

共通の民主的価値に根ざした肯定的かつ積極的な多国間技術協定のための実行可能な計画。

An actionable plan for an affirmative and proactive multilateral technology pact rooted in shared democratic values.

Ray レイ

1. 氏名及び役職名等（Name and Title）

トリシャ・レイ氏、インド・オブザーバーリサーチ財団
Ms. Trisha Ray , Observer Research Foundation

2. 参加枠（Time Slot）

Day 1, 19:40-20:50: Panel Discussion 1-2

3. 講義要約（Abstract）

「レジリエンスと接続されたインド太平洋地域」
Resilient and Connected Indo-Pacific

インド太平洋地域は活気に満ち、拡大を続けるデジタル・エコシステムの母体である。この地域はシステムの衝撃に耐える能力を有しているだろうか。技術領域において、接続性、スキル、作成の国レベルのギャップを生み出しているものは何か。

The Indo-Pacific region is home to a vibrant and growing digital ecosystem. Does the region have the capacity to withstand systemic shocks? What are some country-level gaps in connectivity, skills, manufacturing etc in the realm of tech?

Sebastiaan　セバスチャン

1. 氏名及び役職名等（Name and Title）

タンピノンゴール・セバスチャン教授、NATO 通信学校・イノベーション・開発学部長
Tampinongkol Sebastiaan, Head of Learning Innovation and Development at NATO Commmunications and Information Academy

2. 略歴（CV）

タンピノンゴール・セバスチャン氏は NATO 通信学校の教育イノベーション開発の責任者として、コスト効率と効果の高い教育・kE&T の提供のためのデジタル技術を実装することにより、新しいトレーニング方法への移行を推進している。さらに、C4ISR とサイバーに焦点を当てた NATO 通信・情報機関とその関係組織(NATO 機関、NATO 諸国およびパートナー国、共通の価値を持つ他の国際機関)のための新しい学習ソリューションの開発を担当している。2017 年に NATO に入る前は、石油・ガス、金融サービス、各種コンサルティング会社を対象に、デジタル学習とパフォーマンス向上に重点を置き、業界におけるL&D 関連の幅広い役割を担ってきた。

As the Head of Learning Innovation and Development in the NCI Academy, Sebastiaan drives the transition to new training methods by implementing digital technology for the delivery of cost-efficient and effective E&T. In addition, Sebastiaan is responsible for the development of new learning solutions for the NCI Agency and its customers (NATO entities, NATO Nations and Partner Nations, other International organizations with shared values, e.g. UN, EU), with a focus on C4ISR and Cyber. Before joining NATO in 2017, Sebastiaan worked in a broad range of L&D related roles in industry, covering Oil & Gas, Financial services, and various consultancy agencies with a focus on digital learning and performance improvement.

3. 参加枠（Time Slot）

Day 2, 17:20-18:40: Panel Discussion 2-1

4. 講義要約（Abstract）

「21 世紀の NATO サイバー組織の構築」
Building a NATO Cyber workforce for the 21st century

サイバー攻撃は、北大西洋条約機構(NATO)の使命を損ない、協議を可能にし、集団的防衛を提供する同盟の能力を妨げる可能性を秘めている。高レベルの政治指導に基づき NATO 通信学校は、NATO と EU とともに多数のサイバーディフェンダーを訓練するために 21 世紀のカリキュラムを構築している。このプレゼンテーションでは、このような幅広いカリキュラムが必要な理由と、今後数年間で NCI アカデミーがどのように構築されているかを概説する。我々はカリキュラム設計、革新的な学習方法論に関するビジョンに触れ、産学業界の国際的なパートナーとの関わり方について議論し、堅牢で効果的で魅力的なカリキュラムの構築を図っている。

Cyber attacks have the potential to undermine NATO's mission, and hamper the Alliance's ability to enable consultation and deliver collective defense. Following high-level political guidance, the NATO Communication and Information Academy (NCI Academy) is building a 21st century curriculum to train large numbers of Cyber Defenders in NATO, and potentially in the EU.This presentation outlines why such a broad curriculum is required, and how the NCI Academy is building it in the next few years. We will touch on our vision on curriculum design, innovative learning methodologies and discuss the way we engage with international partners in Industry and Academia to build a robust, effective and engaging curriculum.

Siman シモン

1. 氏名及び役職名等（Name and Title）

バシール・バーナード・シモン、大英帝国受勲者（O.B.E.）
ブリュッセル自由大学 ブリュッセル政策アカデミー 金融政策部長
Dr. Bashir Bernard Siman, O.B.E., Head, Financial Diplomacy, Brussels Diplomatic Academy, Vrije Universiteit Brussel, Belgium

2. 略歴（CV）

元・金融サービス特別代表
IT、ハイブリッド戦及び国際地政学リスクに関する企業、政府及び投資家への助言者　地中海地域及び西アジア地政学の専門家

Formerly Special Representative for Financial Services
Adviser to corporates, governments and investors on technology, hybrid warfare and global geopolitical risks
Specialist in Mediterranean and West Asian geopolitics

3. 参加枠（Time Slot）

Day 2, 16:20-16:40: Keynote Speech 2-1

4. 講義要約（Abstract）

「イスラムの活動と関連した人工知能による深層フェイク、金融市場を含む地政学及び安全保障上の脅威」
Geopolitical & Security Threats, including to financial markets, of A.I. DeepFakes in Asia and Europe with reference to Islamist activities

最近、広域のアジア及び中東国家の市街地で発生した仏大統領マクロン氏と仏政府の言論の自由に関するスタンスへの抗議行動は、この講義を強調するものである。信頼性が高い人工知能深層フェイクの容易性及び低コストは、マクロン大統領や他の指導者が事実、どのような発言をしたかに関わらず、同様に不安定な環境を作り出すことができる。多数の人々を暴力へと扇動する能力は、海外テロリストの活動と同様に国内の安全保障上のリスクを生み出す。同様に、それによって引き起こされる反発（縁を切りたい、又は他の行動を促す圧力）は、突然の予期しない地政学的なシフト及び脅威を導く。このような深層フェイクは、国家主体、非国家主体、又は国家支援を受けたアクターのいずれの戦果にもなり得る。攻撃者は、例えば、銀行への殺到、株式市場の売り行為、政府債務への価値及び信頼への疑念などを通して、金融安定性の弱体化を図ることができる。地理的には、南アジア、インドネシア及びフィリピンが、アジア及びヨーロッパの金融リスクに関連する可能性として、特別な関心を引く。

The recent widespread street protests across several Asian and Middle Eastern countries against President Macron and France's stance on freedom of speech underscore the message of this presentation. The ease and low cost of creating credible A.I. DeepFakes could've also created the same circumstances leading to such instability without in fact President Macron, or other leaders, uttering any words themselves. The ability to incite large numbers of people to violence creates domestic security threats as well as overseas terrorist activity potential. Simultaneously the reactions (such as pressures to cut off relations or other action) could lead to sudden unanticipated geopolitical shifts and threats. Such

DeepFakes can be the product of state, non-state, or state-backed actors. They could also be used to undermine financial stability through e.g. inciting runs on the banks, sell offs at stock markets or undermining the value and credibility of government debt. Geographically, South Asia, Indonesia and the Philippines should be of particular interest, as are the possibilities relating to the financial risks in Asia and Europe.

Spidalieri　スピダリエリ

1.　氏名及び役職名等（Name and Title）

フランチェスカ・スピダリエリ教授、ソルブ・レジーナ大学
Professor Francesca Spidalieri, Salve Regina University

2.　略歴（CV）

フランチェスカ・スピダリエリは、サルベ・レジーナ大学のペル国際関係・公共政策センターでサイバーリーダーシップのシニアフェローを務め、サイバーリーダーシップ研究プロジェクトとロー　ドアイランド企業サイバーセキュリティイニシアチブ(RICCI)を率いている。フランチェスカはまた、ハサウェイ・グローバル・ストラテジーズ(LLC)のサイバーセキュリティコンサルタントであり、ポトマック政策研究所のサイバーレディネスインデックス2.0プロジェクトの共同主任研究者でもある。また、フィレンツェ大学(イタリア)サイバーセキュリティ国際関係研究センターの研究員、コシウシュコ研究所(ポーランド)の非居住者フェロー、ポネモン研究所(米国)の特別研究員を務める。彼女の学術研究は、サイバーリスク管理、サイバーセキュリティ教育、国家サイバーレディネスとレジリエンスに焦点を当てている。米国やヨーロッパのサイバー関連イベントで定期的に講演を行い、世界中の国や組織に影響を及ぼすサイバーポリシー、プライバ　シー、サイバーレジリエンスに関するジャーナル記事やその他の出版物に寄稿している。

Francesca Spidalieri is the Senior Fellow for Cyber Leadership at the Pell Center for International Relations and Public Policy at Salve Regina University, where she leads the Cyber Leadership research project and the Rhode Island Corporate Cybersecurity Initiative (RICCI). Francesca is also a cybersecurity consultant for Hathaway Global Strategies, LLC, and the Co-Principal Investigator for the Cyber Readiness Index 2.0 project at the Potomac Institute for Policy Studies. In addition, she serves as a Research Associate at the Center for Cyber Security and International Relations Studies at the University of Florence (Italy), a Non-Resident Fellow at the Kosciuszko Institute (Poland), and a Distinguished Fellow at the Ponemon Institute (USA). Her academic research and publications have focused on cyber risk management, cybersecurity education and awareness, and national cyber preparedness and resilience. She lectures regularly at cyber-related events in the United States and Europe, and contributes to journal articles and other publications on cyber policy, privacy, and cyber resilience matters affecting countries and organizations worldwide.

3.　参加枠（Time Slot）

Day 2, 17:20-18:40: Panel Discussion 2-1

4.　講義要約（Abstract）

「米国民間・軍事高等教育におけるサイバーセキュリティ教育」
Cybersecurity Education in U.S. Civilian and Military Higher Education

Tarien　タリエン

1.　氏名及び役職名等（Name and Title）

ヤーク・タリエン、NATO CCD COE 所長、エストニア空軍大佐
COL Jaak Tarien, Director, CCD COE, NATO, Estonian Air Force

2.　略歴（CV）

ヤーク・タリエン大佐は、CCD COE に赴任前の 2012 年 8 月から 2018 年 7 月は、エストニア空軍司令官として勤務している。それ以前は NATO の変革連合軍（ACT）の幕僚勤務、地域的航空宇宙監視調整センターの副所長、在リトアニア BALTNET 地域空宇宙監視調整センターのエストニアチーム指揮官などを歴任した。
タリエン大佐は、米空軍士官学校に就学、米空軍大学指揮幕僚課程で修士号を取得している。また、米国防大学においても国家資源戦略の修士号を取得した。

Prior to joining CCDCOE Colonel Tarien served as Commander of Estonian Air Force from August 2012 to July 2018. Among other assignments he has also served as Staff Officer with NATO's Supreme Allied Command Transformation (ACT), as Deputy Director of the Regional Airspace Surveillance Coordination Centre and as Commander of the Estonian team at the BALTNET Regional Airspace Surveillance Coordination Centre in Lithuania.
Colonel Tarien, a graduate of the United States Air Force Academy, earned his Master's degree from the Air Command and Staff College of the USAF Air University. He recently also acquired Master of Science degree in National Resource Strategy at the U.S. National Defence University.

3.　参加枠（Time Slot）

Day 1, 17:00-17:20: Keynote Speech 1-3

Tiirmaa-Klaar ティルマ＝クララ

1. 氏名及び役職名等（Name and Title）

ヘリ・ティルマ＝クララ、エストニア国特命大使（サイバー政策担当）
Heli Tiirmaa-Klaar，Ambassador-at Large for Cyber Diplomacy at the Estonian Ministry of Foreign Affairs

2. 略歴（CV）

ヘリ・ティルマ=クララは、エストニア外務省のサイバー大使である。エストニア国防省とタリン大学で様々な管理職を歴任した後、2007年からエストニアのサイバーセキュリティ戦略の開発に貢献した。2008年から2010年にかけて、エストニアの戦略の実施を調整し、国家サイバーセキュリティ評議会を管理し、エストニアの国家サイバーシステムの開発とサイバーセキュリティのための官民パートナーシップの開発を主導した。2011年、北大西洋条約機構(NATO)国際スタッフに配任され、新しいNATOサイバー防衛政策を策定した。2012年から2018年秋まで、EU対外支援庁のサイバー政策調整責任者を務め、サイバー問題に関するEUの対外関係を調整した。彼女はジョージワシントン大学のフルブライト奨学生であり、彼女のキャリアを通じていくつかの学術雑誌に掲載されている。

Heli Tiirmaa-Klaar is Ambassador at Large for Cyber Diplomacy at the Estonian Ministry of Foreign Affairs. Up to Fall 2018, she was as a Head of Cyber Policy Coordination at the European External Action Service where she steered and coordinated EU external relations on cyber issues since 2012. She has been working on cyber security since 2007 when she led the development of the Estonian Cyber Security Strategy. In 2008-2010 she coordinated the implementation of the Estonian strategy, managed the National Cyber Security Council and led the development of Estonia's National Cyber System as well as public-private partnerships for cyber security. In 2011, she was assigned to the NATO International Staff to develop the new NATO Cyber Defence Policy. In her earlier career, she has held various managerial positions at the Estonian Ministry of Defence and the Tallinn University. She was a Fulbright Scholar at the George Washington University and has published in several academic journals throughout her career.

3. 参加枠（Time Slot）

Day 1, 17:20-18:40: Panel Discussion 1-1

Akahori　赤堀

1.　氏名及び役職名等（Name and Title）

赤堀 毅 外務省総合外交政策局審議官兼サイバー政策担当大使
Mr. Takeshi Akahori, Ambassador(United Nations Affairs, Cyber Policy)/Deputy Assistant Minister, Foreign Policy Bureau, MoFA, Japan

2.　略歴（CV）

1989．４ 外務省入省
1996．２ 総合外交政策局国連政策課 課長補佐
1998．２ 大臣官房総務課 課長補佐（総括）
1999．11 条約局法規課 首席事務官
2002．１ 北米局北米第一課 首席事務官
2004．８ 在アメリカ合衆国日本国大使館 一等書記官，（06年から）参事官
2007．８ アジア大洋州局北東アジア課日韓経済室長 兼 朝鮮半島政策調整官
2009．７ 大臣官房広報文化交流部文化交流課長
2011．４ 外務大臣秘書官
2012．12 国際法局条約課長
2015．９ 国際連合日本政府代表部 政務公使 （2016年1月から2年間、日本は安保理理事国）
2018．７ 大臣官房参事官兼G20サミット事務局長（大使）
2019．７ 総合外交政策局参事官 兼 国際安全保障・サイバー政策担当大使
　　サイバー空間に関する国連政府専門家会合（GGE）構成員（継続中）
2020．８ 総合外交政策局審議官 兼 国連・サイバー政策担当大使

March 1989	Bachelor of Law, University of Tokyo, Tokyo, Japan
April 1989	Joined the Ministry of Foreign Affairs of Japan (MOFA)
February 1996	Deputy Director, UN Policy Division, MOFA
February 1998	Deputy Director, General Affairs Division, MOFA
November 1999	Principal Deputy Director, Legal Affairs Division, MOFA
January 2002	Principal Deputy Director, First North America Division, MOFA
August 2004	First Secretary (later Counsellor), Embassy of Japan in the USA
July 2007	Director, Japan-Korea Economic Affairs Division, MOFA
	(Concurrently) Senior Policy Coordinator for the Korean Peninsula
July 2009	Director, Cultural Affairs Division, MOFA
April 2011	Executive Assistant to the Foreign Minister
December 2012	Director, Treaties Division, MOFA
	(Taught at Kyushu University and International University of Japan)
September 2015	Political Minister, Permanent Mission of Japan to the United Nations
July 2018	Ambassador, Secretary-General for the G20 Osaka Summit
July 2019	current position
	Member of the UN Group of Governmental Experts on Cyberspace

3.　参加枠（Time Slot）

Day 1, 17:20-18:40: Panel Discussion 1-1

Ikegami 池 上

1. 氏名及び役職名等（Name and Title）

池上 重輔 早稲田大学教授
Professor Jusuke JJ Ikegami, Waseda University

2. 略歴（CV）

早稲田大学商学部卒業。一橋大学より博士号（経営学）を取得。ボストン・コンサルティング・グループ（BCG）、MARS JAPAN、ソフトバンク EC ホールディングス、ニッセイ・キャピタルを経て 2016 年より現職。Academy of International Business (AIB) Japan chair、国際ビジネス研究学会（JAIBS）理事・国際委員会委員、異文化経営学会　理事。早稲田ブルー・オーシャン戦略研究所 所長、早稲田グローバル・ストラテジック・リーダーシップ研究所 幹事。2015 年より東洋インキ SC ホールディングス社外監査役。英国ケンブリッジ大学ジャッジ経営大学院 MBA、英国国立シェフィールド大学 政治学部 大学院修士課程国際関係学修士、英国国立ケント大学 社会科学部 大学院修士課程国際関係学 修士。

Professor Ikegami received Doctor of Business Administration from Hitotsubashi University in 2015. After working for Boston Consulting Group (BCG) Tokyo office, he joined MARS Japan. While he is working for Softbank EC Holdings as a Director of New Business Development, he also served as BOD of several subsidiaries. He also worked for Nissay Capital Co. Ltd., before joining Waseda Business School. His research interest includes corporate strategy, global management, new business development and global leadership. He is a member of international committee of JAIBS (Japan Academy of International Business Studies). He is also an outside company auditor of Toyo INK SC Holdings.
Edcucation: D.B.A., Hitotsubashi University (Japan) 2015

3. 参加枠（Time Slot）

Day 2, 22:00-23:10: Panel Discussion 2-3

4. 講義要約（Abstract）

「企業におけるサイバー地政学の影響」
Impact of Cyber Geo-politics on firms

従来、地政学(GEO-POLITICS)は、石油、ガス、海洋資源、土地などの重要な資源の流れをいかに国に有利にするかに焦点を当ててきたが、近年のサイバー地政学では、データの流れも重要な資源の一つに加えている。また、防衛産業技術基盤を中心とした企業や、外資規制のある一部の産業にとっても、産業安全保障は重要なテーマとなっている。現在、多くの日本企業にとって、(1)ビジネスのグローバル化、(2)デジタル　トランスフォーメーションによる事業創造が大きな課題となっている。Huawei 問題は、地政学、政治、経済が絡み合うサイバー地政学の代表的な例の一つともいえよう。
グローバルに事業を展開する日本企業にとって、重要性が高まっている課題は 2 つある。一つは、デジタルトランスフォーメーションを通じたデジタル依存度の高い戦略を追求する中で、サイバーセキュリティにどのように対処していくか、もう一つは、日本を含めたグローバルビジネスのバランスをどのようにとっていくか、ということである。本シンポジウムでは、以下のトピックについて議論する。(1)企業はサイバー地政学をどのように捉えるべきか（各国の市場、生産、イノベーション、ビジネスパートナー、競合相手としての立場がどのように変化するか）、(2)企業におけるサイバーセキュリティの現状と国際比較、(3)企業におけるサイバーセキュリティと地政学の教育・知識共有。

Traditionally, Geopolitics has focused on how to make the flow of oil, gas, ocean resources, land and other important resources to the advantage of a nation, but in recent years Cyber Geopolitics has added the flow of data to its list of important resources. Industrial security has also been an important topic for companies primarily involved in the defense industrial technology base and some industries with

foreign investment restrictions. Nowadays, the main challenges for many Japanese companies are (1) business globalization and (2) business creation through digital transformation. The Huawei issue may be one of a major examples in the cyber Geopolitics, where geopolitics, politics and economics are intertwined with cyber security.

There are two issues of growing importance for Japanese companies operating globally. The first is how to deal with cyber security as they pursue a more digitally dependent strategy through digital transformation, and the second is how to balance their global business across globe including Japan. In this symposium, the following topics will be discussed: (1) How companies should view cyber geopolitics (how each country's position as a market, production, innovation, business partner and competitor will change), (2) Current status of cyber security in companies and international comparison, (3) cyber security and geopolitics education/ knowledge sharing in companies.

Kondo　近藤

1. 氏名及び役職名等（Name and Title）

近藤 剛 弁護士
Mr. Go Kondo, Attorney-at-Law, UTOKU LAW OFFICES ＆Res. LTC

2. 略歴（CV）
予備自衛官二佐、京都先端科学大学講師（サイバーセキュリティ）
Reserve L.C., Assistant Professor, Kyoto University of Advanced Science

3. 参加枠（Time Slot）

Day 2, 22:00-23:10: Panel Discussion 2-3

4. 講義要約（Abstract）

「企業におけるサイバー地政学の影響」
Increasing Cyber Incidents with Japanese Enterprises

2020 は日本を代表する大企業が深刻なサイバー被害を受けた年となった。自動車業界の新たな ISAC 組成など対策は進むが追いついてない。国家安全保障の見地からは、Six Eyes が名目だけで立ち消えぬよう、引続き取組みを加速する必要がある。

Large Japanese Enterprises experienced serious Cyber Attacks in 2020.While countermeasures including launch of AUTO ISAC is underway, Japan needs to expedite its efforts so its inclusion in Six Eyes would not end up nominal.

Kondo　近藤

1. 氏名及び役職名等（Name and Title）

近藤 玲子 総務省 国際戦略局 通信規格課長
Dr. Reiko Kondo, Director, ICT Standardization Division, Global Strategy Bureau, Ministry of Internal Affairs and Communications

2. 略歴（CV）

（独）情報通信研究機構情報セキュリティ研究所推進室長（2009 ）、内閣官房情報セキュリティセンター企画調整官（2011 年）、総務省情報流通行政局放送技術課技術企画官（2014 年）、総務省総合通信基盤局電波部重要無線室長（2016 年）、総務省総合通信基盤局電波部電波環境課長（2017 年）、サイバーセキュリティ統括官付参事官（2018 年）等を経て、2020 年より現職。東京大学大学院理学系研究科情報科学専攻修了、スタンフォード大学大学院経営学修士（MBA）、学術博士。

Dr. Kondo graduated from the Graduate School of the University of Tokyo and got Master's degree in Computer Science. She also got MBA at Stanford Graduate School of Business and Ph.D. at Tokyo Institute of Technology.
Since Dr. Kondo joined the Ministry of Internal Affairs and Communications, she has contributed to the policy development in information and communications technology and held such positions as Director of Public Safety Communication Office from 2016 to 2017, Director of Electromagnetic Environment Division from 2017 to 2018, and Director of Office of the Director-General for Cybersecurity from 2018 to 2020. She also held a position in National Institute of Information and Communications Technology (NICT) as Director of Policy Planning Office of the Cybersecurity Research Institute from 2009 to 2011 and in National Information Security Center (NISC) of the Cabinet Secretariat as Counselor for International Strategy from 2011 to 2014.

3. 参加枠（Time Slot）

Day 2, 17:20-18:40: Panel Discussion 2-1

4. 講義要約（Abstract）

「高等教育におけるサイバー防衛教育」
Cyber Defense Education in Higher Education

サイバーセキュリティ人材が不足するなか、若年層をターゲットとしたサイバーセキュリティ教育の強化が求められている。一方で、高度なセキュリティ技術を習得した若者が、その能力を適切に生かせるよう、情報モラル教育も合わせて行うことが重要である。本セッションでは、高等教育におけるサイバー防衛教育について、日米欧の課題を比較するとともに、課題解決のためのベストプラクティスを共有する。

With a shortage of cybersecurity talent, there is a need to strengthen cybersecurity education targeting young people. On the other hand, it is important to provide information moral education so that young people who have acquired advanced security skills can make appropriate use of their abilities. In this session, Compare issues in Japan, the U.S., and Europe on cyber defense education in higher education, and share best practices for solving them.

Sasaki 佐々木

1. 氏名及び役職名等（Name and Title）

佐々木 孝博 元海将補 広島大学・東海大学客員教授
RADM(ret.) Takahiro Sasaki, Visiting Professor, Hiroshima University and Tokai University

2. 参加枠（Time Slot）
Day 1, 19:40-20:50: Panel Discussion 1-2

3. 講義要約（Abstract）

「サイバー脅威に対する QUAD 協力」
QUAD Cooperation for Cyber Threat

近年ますます増大している中国の脅威（多くの安全保障の分野で協調するロシアの脅威も含む）に対抗するため、1 国のみが対抗することは困難である。そのような見地から、日本、米国、オーストラリア及びインドの安全保障協力（いわゆる QUAD 関係）は重要である。4 か国それぞれの安全保障関係のレベルが違うために、4 か国をまとめて、全体として、どのような協力関係を追及すべきかを言及することは難しいかもしれない。しかしながら、サイバー空間における中国やロシアに対抗するためには、少なくとも発表で述べるような5つ分野において、段階的にでも協力関係を深めていかなければならないだろう。

It is difficult for only one country to counter the increasing threat of China (including the threat of Russia cooperating in many security areas) in recent years. Accordingly, security cooperation between Japan, the United States, Australia, and India (the so-called QUAD relationship) is vital. Because these four countries have different levels of security relations, it is difficult to say what kind of cooperative relations they should pursue as a whole. However, in order to compete with China and Russia in cyber space, it will be necessary to deepen cooperation, at least in the five areas which I will recommend in the session, step by step

Sunami 角 南

1. 氏名及び役職名等（Name and Title）

角南 篤 公益財団法人笹川平和財団理事長
Dr. Atsushi Sunami, President, Sasagawa Peace Foundation

2. 略歴（CV）

1988 年、ジョージタウン大学 School of Foreign Service 卒業、89 年株式会社野村総合研究所政策研究部研究員、92 年コロンビア大学国際関係・行政大学院 Reader、93 年同大学国際関係学修士、97 年英サセックス大学科学政策研究所（SPRU）TAGS フェロー、2001 年コロンビア大学政治学博士号（Ph.D.）取得。2001 年から 2003 年まで独立行政法人経済産業研究所フェロー。2003 年政策研究大学院大学助教授、2014 年教授、学長補佐、2015-2018 年内閣府参与（科学技術・イノベーション政策担当）、2016 年副学長、2019 年学長特別補佐、2020 年 SciREX センター長（現在に至る）。
その他、文部科学省 科学技術・学術審議会委員、外務省 科学技術外交推進会議委員、内閣府総合科学技術・イノベーション会議基本計画専門調査会委員、等。

Professor Sunami holds BSFS from Georgetown University. He obtained MIA and PhD in Political Science from Columbia University. He is currently Adjunct Professor, Executive Advisor to the President , and Director, The Science for RE-designing Science, Technology and Innovation Policy (SciREX) Center at National Graduate Institute for Policy Studies, Japan. Before joining GRIPS, he was a Fellow at Research Institute of Economy, Trade and Industry established by the Ministry of Economy, Trade and Industry, Japan between 2001 and 2003. He also worked as a researcher in the Department of Policy Research at Nomura Research Institute, Ltd. from 1989 to 1991. He was a visiting researcher at Science Policy Research Unit, University of Sussex, and Tsinghua University, China. He is also a members of the Advisory Board for the Promotion of Science and Technology Diplomacy in Ministry of Foreign Affairs of Japan, the Council for Science and Technology in Ministry of Education, Culture ,Sports, Science and Technology and the Expert Panel on Basic Policy in Council for Science, Technology and Innovation of Cabinet office. He served as Special Advisor, Cabinet Office responsible for Science and Technology and Innovation from 2015 to 2018.

3. 参加枠（Time Slot）

Day 1, 1610-1615: Greeting 1-3

Dairokuno 大六野

1. 氏名及び役職名等（Name and Title）

大六野 耕作 明治大学学長、教授
Kosaku Dairokuno, President, Professor, Meiji University

2. 略歴（CV）

1977 年 明治大学法学部卒業
1979 年 明治大学大学院政治経済学研究科博士前期課程修了（政治学修士）
1982 年 明治大学大学院政治経済学研究科博士後期課程単位取得退学
1982 年 明治大学政治経済学部専任助手
1984 年　同　　専任講師
1988 年　同　　専任助教授
1995 年　同　　専任教授（現在）＜担当科目：比較政治論＞
2008～2015 年 明治大学政治経済学部長
2016～2020 年 明治大学副学長（国際交流担当）

1977: Graduated from School of Law, Meiji University
1979: Received a Master of Political Science from Graduate School of Political Science and Economics, Meiji University
1982: Completed all the necessary credits of Graduate School of Political Science and Economics, Meiji University (Withdraw)
1982: Appointed Research Associate of School of Political Science and Economics, Meiji University
1995: Appointed Professor of Political Science and Economics, Meiji University
2008~2015: Served as Dean of the School of Political Science and Economics, Meiji University
2016~2020: Served as Vice President (International Affairs), Meiji University

3. 参加枠（Time Slot）

Day 2, 16:00-16:05: Greeting 2-1

Taura 田 浦

1. 氏名及び役職名等（Name and Title）
   田浦 尚之 陸将補、防衛省統合幕僚監部指揮通信システム部長
   MG Naoyuki Taura, Director General, J-6/JJS, Ministry of Defense

2. 略歴（CV）

平成 25 年 12 月	統合幕僚監部防衛計画部防衛計画課防衛班長
平 成 27 年 4 月	東部方面通信群長
平 成 28 年 7 月	陸上幕僚監部防衛部情報通信・研究課長
平 成 29 年 3 月	陸上幕僚監部指揮通信システム・情報部指揮通信システム課長
平 成 30 年 8 月	陸上自衛隊通信学校長
令和　元年 12 月	現 職

December 2013	**Chief of Defense Policy & Program Section, Defense Policy and Programs Division, Defense Policy and Programs Department, JJS**
April 2015	**Commander, Eastern Army Signal Group**
July 2016	**Director, C4 Systems and Research Division, Plans and Operations Department, GSO**
March 2017	**Director, C4 Systems Division,C4 Systems and Intelligence Department**
August 2018	**President, JGSDF Signal School**
December 2019-	**Director General, J6/JJS**

3. 参加枠（Time Slot）

   Day 1, 16:40-17:00: Keynote Speech 1-2

4. 講義要約（Abstract）

「防衛省・自衛隊における取組と今後の方向性」
Efforts being made by JMOD/SDF and Our way ahead

CYDEF2020 の問題認識にあるとおり、昨今のコロナ禍により、国内においてもテレワークの拡大、オンラインによる会議やコミュニケーション機会の増大といった、対面での接触機会の局限や三密の回避といった、新たな生活様式の実践が求められている。我が国の安全保障を担う防衛省・自衛隊についても例外なくこの影響の渦中にあり、多数の隊員が集合する訓練の中止、または対面形式を避けるための実施要領の再検討を余儀なくされている。
他方、コロナ禍の如何によらず、伝統的な脅威は変わらず存在し、安全保障環境はより一層複雑化している。さらに、目覚ましい科学技術の発展を背景として顕在化、先鋭化しているサイバー領域への対応は、防　衛省・自衛隊においても最優先課題の一つとなっており、脅威認識に基づいた各種取組を推進しているところである。
本講演では、サイバー領域における脅威認識を列挙し、それに対する防衛省・自衛隊としての取組を概説　するとともに、将来的な取組について言及する。

As collectively acknowledged at CYDEF2020, the ongoing COVID-19 pandemic calls on us to practice the "new normal" by encouraging tele-work and making use of web-based meetings and other online communication means in order to minimize in-person contact and avoid the three Cs (closed spaces, crowded places and close-contact). JMOD/JSDF, responsible for national security of Japan, are not an exception and caught in this vortex; we are forced to cancel exercises in which a large number of personnel would gather or to modify procedures for conducting exercises to avoid the usual in-person format.
In the meantime, traditional threats are still out there and the national security landscape continues to be increasingly more complicated in disregard of COVID19. Furthermore, as the cyberspace threat has

been rapidly emerging and evolving against the backdrop of remarkable scientific and technological advances. JMOD/JSDF attaches highest priority to our response to cyber threats. Thus, we are carrying forward various initiatives based on our understanding on threats.
This briefing provides an overview of such efforts that JMOD/JSDF are making by listing threats we see in the cyber domain and talks about our planned initiatives in the future.

Takahashi 高 橋

1. 氏名及び役職名等（Name and Title）

高橋 郁夫 駒澤綜合法律事務所長・代表弁護士
Mr. Ikuo Takahashi, CEO and Lawyer, Komazawa Legal Chambers

2. 参加枠（Time Slot）

Day 1, 22:00-23:10: Panel Discussion 1-3

3. 講義要約（Abstract）

「グレイゾーンのサイバー攻撃についての日本政府の方針」
Japan's Policy against

武力攻撃にいたらないサイバー攻撃（グレイゾーン）に対する日本政府の対応の方針について分析するとともに、国家実行、および法解釈について検討する。

Analysing the Japan's policy and state practice against Cyber attacks under the armed attack threshold. Also making the suggestions from legal aspects.

Tanaka 田 中

1. 氏名及び役職名等（Name and Title）

田中達浩 元陸将補 富士通システム統合研究所株式会社富士通システム統合研究所主席研究員
MG(ret.) Tatsuhiro Tanaka, Research Principle, Fujitsu System Integration Laboratories Limited

2. 略歴（CV）

田中達浩氏は富士通システムインテグレーション研究所研究主任である。防衛大学校を卒業し、1975年に任官した。湾岸戦争中の1990~1991年にはアメリカ海兵隊大学Joint War 、1994年には統幕学校、9.11直後の2001年にはヘンリー・L・スティムソンセンターの研究員として教育を受けた。 2012年から2014年までハーバード大学アジアセンターで日本の国際関係とサイバー戦争のサイバー抑止力をシニアフェローとして学 んだ。2009年に陸自通信学校長を最後に退官し、現在富士通株式会社で勤務している

Major General (retired) Tatsuhiro Tanaka is Research Principal, Fujitsu System Integration Laboratories, LTD. He graduated from the Japan National Defense Academy, and was commissioned in 1975. He received several education courses including US Marine Corps Command and Staff College in 1990~1991 during the Gulf War, Joint War College of Japan Self Defense Force in 1994, and Henry L. Stimson Center as Fellow Researcher in 2001 soon after 9.11. He has studied the international relations for Japan and the cyber deterrence for cyber warfare at Harvard University Asia Center since 2012- 2014 as Senior Fellow.He retired as commanding general of JGSDF Signal School in 2009, and joined Fujitsu Limited.

3. 参加枠（Time Slot）

Day 1, 19:00-19:20: Keynote Speech 1-5

4. 講義要約（Abstract）

「サイバー戦の再定義」

Redefining “Cyber Warfare”

「前方防衛」は、**2018** 年の米国の新サイバー戦略の主要なフレーズであり、サイバー戦に関して大きなインパクトを与えている。国際法や制度的な体制に関する多くのサイバー研究者や専門家は、現国際武力紛争法のような既存の規範の範囲内でその考えを捉えようとしている。しかし、我々はまた、武力紛争法を適用するような事態が現在まで生起していないことを理解し認識している。そして、大国間競争の時代が継続し、グレーゾーンが常態化するために今後も生起しないと予想している。
今回は二つの考えを簡単に紹介する。一つは、サイバー戦の再定義が必要な理由であり、もう一つは、グレーゾーンにおける規範として、あるいは前方防衛のように自衛権行使の特別の規範と手段として、サイバー戦に適用する新たな「規範」の基本的な考え方である。

“Defending Forward” is a main phrase of US new Cyber Strategy (2018) and has a great impact on cyber warfare. Most cyber researchers and experts on international laws and institutional regime are discussing and trying to understand it within/according to their current common knowledge like existing “Law of International Armed Conflict (LIAC)” is applied in cyber warfare. But we also understand and recognize the situation applying LIAC has never occurred in cyber domain (cyber-physical-system) until now, and we anticipate it will not happen in the future because “Great Power Competition” is continuing and “Always Gray Zone” becomes common.
I will introduce/propose two ideas for this speech, one is the reason why redefining “cyber

warfare" is required, another one is a basic idea for newly required "Norms" applying in cyber warfare as a gray-zone discipline or as the specific norms/measures of executing the right of self-defense like "Defending Forward"."Defending Forward" is a main phrase of US new Cyber Strategy (2018) and has a great impact on cyber warfare. Most cyber researchers and experts on international laws and institutional regime are discussing and trying to understand it within/according to their current common knowledge like existing "Law of International Armed Conflict (LIAC)" is applied in cyber warfare. But we also understand and recognize the situation applying LIAC has never occurred in cyber domain (cyber- physical-system) until now, and we anticipate it will not happen in the future because "Great Power Competition" is continuing and "Always Gray Zone" becomes common.

I will introduce/propose two ideas for this speech, one is the reason why redefining "cyber warfare" is required, another one is a basic idea for newly required "Norms" applying in cyber warfare as a gray- zone discipline or as the specific norms/measures of executing the right of self-defense like "Defending Forward".

Tezuka　手塚

1.　氏名及び役職名等（Name and Title）

手塚 悟 慶応義塾大学教授
Professor Satoru Tezuka, Keio Univsersity

2.　略歴（CV）

1984 年慶應義塾大学工学部数理工学科卒。(株)日立製作所システム開発研究所を経て，2009 年東京工科大学コンピュータサイエンス学部教授。

3.　参加枠（Time Slot）

Day 2, 21:20-21:40: Keynote Speech 2-8

4.　講義要約（Abstract）

「トラストサービス ―安全保障から社会保障まで支える―」
Trust Service for supporting National Security & Social Security

コロナ禍やコロナ後において、安全保障から社会保障まで支えるトラストサービスの状況について説明する。

Explanation about the Trust Service situation for supporting National Security and Social Security during and after COVID-19.

Nakatani　中谷

1. 氏名及び役職名等（Name and Title）

   中谷 元 サイバー防衛研究会顧問、衆議院議員（元防衛大臣）
   Hon. Mr. Gen Nakatani, Advisor, Cyber Defense Study Group,
   a member of the House of Representatives, Former Minister of Defense

2. 略歴（CV）
   1957 年 10 月 14 日生 高知県高知市、土佐高校。
   1980 年 03 月、防衛大学校卒業。
   1980 年 04 月、陸上自衛隊普通科連隊 小銃小隊長 3 等陸尉。
   1982 年 04 月、レンジャー教育教官。
   1984 年 12 月、二等陸尉で退官。
   1985 年 1 月、衆議院議員秘書。
   1990 年 2 月、第 39 回総選挙において初当選。
   以来、連続当選を果たし、10 期目。

   Born october 14, 1957 14 in Kochi City, Kochi Prefecture
   Graduated from the National Defense University in March 1980.
   In April 1980, he was a third-class lieutenant of the Small Gun Platoon Platoon Leader of the JgsDf Normal Division Regiment.
   In April 1982, he was a Ranger Education Instructor.
   In December 1984, he 12 retired as a second-class lieutenant.
   In January 1985, he was secretary to the House of Representatives.
   1990 年 2 月、第 39 回総選挙において初当選。Since then, he has been elected consecutively andis in his 10th term.

3. 参加枠（Time Slot）

   Day 1, 16:00-16:05: Greeting 1-1

Hayashi 林

1. 氏名及び役職名等（Name and Title）

林 良造 機械振興協会経済研究所長
Dr. Ryozo Hayashi, Chairman of Economic Research Institute, Machinery Industry Promotion Association

2. 略歴（CV）

武蔵野大学特任教授、国際総合研究所長。機械振興協会経済研究所長。東京大学公共政策大学院客員教授。経済産業省官房長、経済産業政策局長を歴任。日 ASEAN サイバーセキュリティ政策会合議長。その他、キャノングローバル戦略研究所理事、Bosch GH International Advisory Board など企業・公的機関の顧問などを務める。1970 年京都大学法学部卒業。1976 年ハーバードロースクール LLM。1991 年ケネディスクールフェロー。

Mr. Hayashi is Director of Musashino Institute for Global Affairs（MIGA） at Musashino University. He is also Director of Economic Research Institute at Machinery Industry Promotion Association. He has a long career at METI (formerly known as MITI) and held positions such as Deputy Vice Minister of METI and Director General of Economic Policy Bureau. He has been teaching at Graduate Schoolof Public Policy of University of Tokyo as a visiting professor and co-chairing Japan-ASEAN Information Security Policy Meeting.He is a graduate of Kyoto University (LLB), and earned his LLM from Harvard Law School.He serves as an Member of International Advisory Board of Bosch GH, as well as several advisory positions in both public and private organizations including Canon Institute of Global Strategy and Citi Japan.

3. 参加枠（Time Slot）

Day 2, 16:10-16:15: Greeting 2-3

Hirayama 平 山

1. 氏名及び役職名等（Name and Title）

平山 敏弘 情報経営イノベーション専門職大学（iU） 教授
Proffesor Toshihiro Hirayama, Professional University of Information and Management for Innovation (i-University)

2. 略歴（CV）

IT 企業に入社以来、UNIX を中心とした大規模分散システムのシステム設計・構築業務を多く経験。Web システムや商用インターネットシステムを手がけた後、セキュリティ分野に転身し、コンサルティング会社にてセキュリティプリンシパルディレクターとして勤務。現在、専門職大学教授
また、複数の大学・大学院の非常勤講師として、情報セキュリティや IT キャリアパスなどに関する講義を行うなど、産学連携教育や人材育成に関する活動を行っている。

Have been experiencing a lot of tasks of system design and build for large-scale distributed systems with a central focus on UNIX since joining an IT company. Worked Web systems and commercial Internet systems, and then moved to the security field. and worked as a security principal director in a consulting company. Currently, professor of professional university
Also, engage in activities regarding business-academia cooperation education and human resource development through the work such as giving lectures about information security, IT career path, etc. as a part-time lecturer in several universities and graduate schools.

3. 参加枠（Time Slot）

Day 2, 18:40-19:00: Keynote Speech 2-4

4. 講義要約（Abstract）

「コロナ後、さらに必要となる「プラス・セキュリティ人材」育成
～SecBoK 利用の視点より～」

Post-Corona, the development of "Plus Security Human Resources" is more essential
～From viewpoint of SecBoK(Security Body of Knowledge) usage

アフターコロナ時代では、リモートワークの推進や、出張に行かずにオンライン会議の増加など、一層のデジタル化が推進される。一方デジタル化の推進は、標的型攻撃などにより、セキュリティスキルの低いユーザーがさらに狙われる傾向になる。よって今後はセキュリティ専門家以外でも広くセキュリティスキルが求められる時代となり、その様な人材を「プラス・セキュリティ人材」と命名した。
当講演では、日本発のセキュリティの知識項目（BoK）である SecBoK を利用した、「プラス・セキュリティ人材」育成を紹介する。

In the after-covid-19, further digitalization will be driven by the promotion of remote work and the increase in online meetings without traveling to work. On the other hand, the promotion of digitalization will also make users with low security skills more vulnerable to targeted attacks. Therefore, we are entering an era in which security skills will be widely demanded, not only by security experts, but also by users with low security skills.
In this talk, I will introduce the nurturing of "Plus Security Human Resources" using SecBoK(Security Body of Knowledge), a Body of Knowledge of Security that originated in Japan.

Matsuoka　松岡

1.　氏名及び役職名等（Name and Title）

松岡 秀樹 元一等海佐 日本オラクル株式会社
CAPT(ret.) Hideki Matsuoka, Oracle Corporation Japan

2.　略歴（CV）

2006 年 護衛艦しらね艦長
2008 年 システム通信隊群司令部首席幕僚
2011 年 中央システム通信隊司令
2013 年 海上自衛隊を定年退職。2014 年、日本オラクル株式会社に入社、安全保障領域を担当。
指揮統制理論、ネットワーク戦及びサイバーセキュリティの専門家。
著書『指揮統制理論の変遷：NCW/NEC の C2 理論について』NPAP、2020 年。

In Japan Navy, He took command of DDH Shirane, 2006, had duty of The Chief Staff Officer, Communications Command, 2008, took command of The Central System Communications Station (Former NAVCOMMSTA Tokyo), 2011. He retired Navy on 2013, and soon after he joined Oracle Corporation Japan
as a business developper in National Security areas. He has the expertise for C2 Theory, Network Enabled Capability Operations, and Cyber Security.
Author, *Transition of Command Control Theory: C2 Theory in NCW/NEC*. Japanese edition, NPAP. 2020.

3.　参加枠（Time Slot）

Day 2, 19:20-19:40: Keynote Speech 2-6

4.　講義要約（Abstract）

「トラストゾーンの終焉」
End of Trust Zone

急速に拡大するサイバーセキュリティに関する管理コストを削減するため、IT アーキテクチャーには多かれ少なかれ、トラストゾーンの概念が導入されていた。しかし、近年のサイバー攻撃の高度化、内部不正の拡大により、トラストゾーンは成立しなくなった。ゼロトラストに向かう IdAM 等の課題と、将来を展望する。

Most of enterprises employ “Trust Zone Concept” in their IT Architectures to reduce the management cost against emerging Cyber threats. But increasing intensity of Cyberattack, and Insider threat made this effort meaningless. I discuss the Zero Trust Approach、especially IdAM, and its future.

Misumi　三角

1. 氏名及び役職名等（Name and Title）

三角 育生 国立情報学研究所／東海大学情報通信学部客員教授、
前内閣審議官／経済産業省サイバーセキュリティ・情報化審議官
Dr. Ikuo Misumi, Visiting Professor of National Institute of Informatics/ Tokai University, Former Councillor (NISC), Deputy Director-General for Cybersecurity and IT (METI)

2. 略歴（CV）

2020-　　現職
2018-2020 内閣審議官／経済産業省サイバーセキュリティ・情報化審議官
2016-2018 内閣官房内閣サイバーセキュリティセンター副センター長 内閣審議官
2012-2016 内閣官房内閣サイバーセキュリティセンター（情報セキュリティセンター）内閣参事官
2009-2012 経済産業省貿易経済協力局貿易管理部安全保障貿易審査課長
2007-2009 経済産業省商務情報政策局情報セキュリティ政策室長
2005-2007 (独)情報処理推進機構セキュリティセンター長
2003-2005 内閣府科学技術政策担当政策統括官付企画官
2001-2003 基盤技術研究促進センター業務第1課長
1999-2001 経済産業省産業技術環境局（工業技術院）認証課課長補佐
1997-1999 通商産業省機械情報産業局電子機器課課長補佐
1995-1997 資源エネルギー庁長官官房国際資源課課長補佐
1992-1994 通商産業局貿易局安全保障貿易管理課課長補佐
1990-1992 国土庁大都市圏整備局計画官付主査
1988-1990 通商産業省機械情報産業局航空機武器課開発係長
1987-1988 通商産業省大臣官房情報管理課

2004 博士（工学）.東京大学大学院
1995 Claremont Graduate School MA in Management（カリフォルニア州）
1987 修士 東京大学大学院工学系研究科

Starting as an officer at the then Ministry of International Trade and Industry (MITI; currently the Ministry of Economy, Trade and Industry, METI), Dr. Misumi has long served in the Government of Japan, especially in the fields of security export control and cybersecurity policy. Most recently, he has served in the NISC since 2012 and was in charge of a number of important tasks, including the thorough revision of the"Management Standards for Information Security Measures for the Central Government Computer Systems," the establishment of the Basic Act on Cybersecurity of 2014 and its amendment in 2016, and the formation of the Cybersecurity Strategy (2015). Since 2016 to 2018, he served as Deputy Director- General and oversees the entire staff and operations of the NISC. Since August 2018 he serves as the current offices.

In the early stage of his career, he engaged in the international negotiation for the preparation of the Wassenaar Arangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies as a government expert in the mid 90s.

Prior to joining the NISC, he was the Director of Security Export License in METI (2009-2012). In this position, he contributed to making Japan's export control systems more effective and efficient by developing innovative approaches, such as reengineering the licensing processes and introducing an examination system with advanced DBs and achieved the reformation of these systems.

He received his master's degree in 1987 and Ph.D. in Engineering (Precision Machinery Engineering) in 2004 from the University of Tokyo. Also he has a master's degree in Management awarded from the Claremont Graduate School (CA,USA) in 1995.

3. 参加枠（Time Slot）

Day 2, 16:40-17:00: Keynote Speech 2-2

4. 講義要約（Abstract）

「ニューノーマル時代のサイバーセキュリティ」
Cybersecurity in New normal era

新型コロナウイルスの影響で、我が国の多くの企業、組織がリモートワークなどの導入を進めているが、そうした状況下でのサイバーセキュリティについて議論する。

Because of COVID19, many companies and organizations enhanced to introduce remote work. In the talk, he touches upon cybersecurity issues in such situations.

Michishita　道下

1.　氏名及び役職名等（Name and Title）

道下 徳成 政策研究大学院大学副学長、教授
Dr. Narushige Michishita, Vice President/Professor, National Graduate Institute for Policy Studies (GRIPS)

2.　略歴（CV）

ジョンズ・ホプキンス大学（SAIS）博士（国際関係学）。内閣官房副長官補付参事官補佐、防衛省防衛研究所主任研究官などを歴任。専門は安全保障論、日本の安全保障・外交政策。著書に **Lessons of the Cold War in the Pacific: U.S. Maritime Strategy, Crisis Prevention, and Japan's Role (Woodrow Wilson Center, 2016) (co-authored with Peter M. Swartz and David F. Winkler)** および『北朝鮮 瀬戸際外交の歴史、1966～2012 年』ミネルヴァ書房、2013 年がある。

Narushige Michishita is vice president and professor at the National Graduate Institute for Policy Studies (GRIPS) in Tokyo. He has served as a member of the National Security Secretariat Advisory Board of the Government of Japan, a global fellow at the Woodrow Wilson International Center for Scholars in Washington DC, senior research fellow at Japan's National Institute for Defense Studies (NIDS), Ministry of Defense, and as assistant counsellor at the Cabinet Secretariat for Security and Crisis Management of the Government of Japan. He acquired his Ph.D. with distinction from the School of Advanced International Studies (SAIS), Johns Hopkins University. A specialist in Japanese security and foreign policy as well as security issues on the Korean Peninsula, he is the author of "The US Maritime Strategy in the Pacific during the Cold War," in Conceptualizing Maritime and Naval Strategy: Festschrift for Peter M. Swartz, Captain (USN) retired (Baden-Baden: Nomos, 2020); Lessons of the Cold War in the Pacific: U.S. Maritime Strategy, Crisis Prevention, and Japan's Role (Woodrow Wilson Center, 2016) (co-authored with Peter M. Swartz and David F. Winkler), and North Korea's Military-Diplomatic Campaigns, 1966-2008 (Routledge, 2009).

3.　参加枠（Time Slot）

Day 1, 19:40-20:50：Panel Discussion 1-2
Day 2, 16:05-16:20: Greeting 2-2

Mitsunaga　満永

1.　氏名及び役職名等（Name and Title）

満永拓邦 東洋大学准教授
Professor Takuho Mitsunaga, Toyo University

2.　参加枠（Time Slot）

Day 2, 17:20-18:40: Panel Discussion 2-1

Yano 矢 野

1. 氏名及び役職名等（Name and Title）

矢野 義昭 元陸将補 CYDEF2020 実行委員長
MG(ret.) Yoshiaki Yano, Chairman of the Executive Committee, CYDEF 2020

2. 略歴（CV）

1950 年 大阪生
京都大学工学部機械工学科卒、同文学部中国哲学史科卒、
陸上自衛隊に一般幹部候補生として入隊後、第 6 普通科連隊長兼美幌駐屯地司令、第一師団副師団長兼練馬駐屯地司令等を歴任、2006 年に陸上自衛隊小平学校副校長をもって退官（陸将補）
現在、岐阜女子大学特別客員教授、米国ミシガン大学客員講師、元拓殖大学客員教授、東京工業大学客　員講師、国家生存戦略研究会会長、日本安全保障戦略研究所上席研究員、防衛法学会理事、日本国史学会会員、拓殖大学博士（安全保障）、2014 年、フランス戦争経済大学において研究。

1950 Born in Osaka
Graduated from the Department of Mechanical Engineering, Faculty of Engineering, Kyoto University, graduated from the Department of Chinese Philosophy History, Faculty of Letters,
After joining the Ground Self-Defense Force as a general cadet, he served as commander of the 6th General Regiment, Commander of bihoro Garrison, Deputy Division Manager of the 1stDivision and Commander of NerimaGarrison, etc., and retired in 2006 as deputy principal of the Ground Self-Defense Force Kodaira School (Assistant General)
Currently, he is a visiting professor at Gifu Women's University, a visiting lecturer at the University of Michigan in the U.S., a visiting professor at Takushoku University, a visiting lecturer at Tokyo Institute of Technology,a president of the National Association for Survival Strategies, a senior researcher at the Japan Institute for Security Strategy, a board member of the Japan Society for Defense Law, a member of the Historical Society of Japan, and a Ph.D. in Security at the French University of War Economics in2014.

2. 参加枠（Time Slot）

Day 2, 23:00-23:20: greeting 2-4

Yuasa 湯 淺

1. 氏名及び役職名等（Name and Title）

湯淺 墾道、情報セキュリティ大学院大学学長補佐・情報セキュリティ研究科教授
Dr. Harumichi Yuasa, Deputy President, Professor, Institute of Information Security

2. 略歴（CV）

1970 年生。青山学院大学法学部卒業。九州国際大学法学部教授、副学長を経て 2011 年より情報セキュリティ大学院大学情報セキュリティ研究科教授。2012 年より学長補佐。研究領域は個人情報・プライバシー保護、電子投票、情報公開等サイバーセキュリティに関係する法律。情報ネットワーク法学会副理事長等を務める。

Prof. Harumichi Yuasa has been the Deputy President and Professor at the Institute of Information Security since 2012. Previous academic positions include Vice President of Kyusyu Kokusai University, Professor in the Department of Law, Kyusyu Kokusai University and assignments as lecturer at Nagoya Syoka University and Keio University. His research is focusing on legal and political aspects of internet and information society including protecting privacy and personal information, administrative information handling and disclosure, regulation of cyber police and defense activities, internet election campaign and e-voting.Prof. Yuasa is also serving as Vice President of the Information Network Law Association, Japan as well as Director of the Japan Election Study Association.

3. 参加枠（Time Slot）

Day 1, 22:00-23:10: Panel Discussion 1-3

Yoshimura 吉 村

1. 氏名及び役職名等（Name and Title）

吉村 孝広 株式会社モノリスワークス 最高技術責任者
Mr. Takahiro Yoshimura, CTO, Monolith Works Inc.

2. 略歴（CV）

株式会社モノリスワークス CTO であり共同設立者。2012 年に経済産業省主催のCTF、「CTF チャレンジジャパン 2012」へ有志とともにチーム Enemy10 として参戦し、関東予選優勝・決勝 3 位入賞。2013 年にはチーム Sutegoma2 の一員として DEFCON 21 CTF へ参戦し、6 位入賞。2017 年 7 月、逆コンパイラを一切使わないことで難読化耐性を持ちつつ OWASP Mobile Top 10 (2016)準拠での診断を行なう Android アプリ自動診断ツール（Trueseeing）の研究について DEF CON 25 Demo Labs ならびに CODE BLUE 2017 で発表した。また 2019 年 8 月、LipNet 関連の実績を基に行なっていた監視カメラ映像を対象にした並列自動読唇ツール (Clairvoyance) の研究について DEF CON 27 AI Village で発表を行なった。2019 年 11 月には、高いレベルの診断を自動的かつ反復可能な形で開発者の手に与えるために研究していた Web 侵入ツールキット（shatter）についても CODE BLUE 2019 において発表、それを用いて多段 CAPTCHA を用いるダークウェブ上のサービスをリアルタイムで解読しつつ攻撃するデモを行ない注目を集めた。2020 年 10 月には当時米中摩擦を引き起こしていた動画共有 SNS、TikTok を iOS/Android 両者について独自に解析、その深度や精度が評価され大学や研究機関において講義を行ない現在に至る。趣味はバイナリやデバイスの解析。GSD が好き。Keybase: https://keybase.io/alterakey

He is Co-founder and Chief Technology Officer of Monolith Works Inc. In 2012 METI-coodinated CTF, Challenge CTF Japan 2012, his team (Enemy10) had won local qualification round at the 1st prize. In 2013, his team (Sutegoma2) took the 6th prize in DEF CON 21 CTF. In 2017, he wrote Trueseeing, the non-decompiling Android application vulnerability scanner and gave talk at DEF CON 25 Demo Labs and following CODE BLUE 2017. In July 2019, he wrote Clairvoyance, concurrent lip reader and gave talk at DEF CON 27 AI Village. In November 2019, he wrote Shatter, an automatic and repeatable Web penetrating toolkit, demonstrating that it can attack hidden services armed with multiple staged CAPTCHAs, solving them in real-time. In 2020, he independently and comprehensively analyzed iOS/Android versions of TikTok, a controversial movie-sharing SNS causing some friction between US and China that time, and gave talks at universities and research institutions. He like to read binaries and hack things. He loves a GSD.
Keybase: https://keybase.io/alterakey

3. 参加枠（Time Slot）

Day 2, 19:40-20:50: Panel Discussion 2-2

4. 講義要約（Abstract）

自己紹介ののち、セッションではスマートフォンアプリケーションセキュリティ(appsec)領域から見た主題へ触れる。
After self-introduction, take a look at the theme from smartphone application security (appsec) perspective in my session.

「サイバー領域における先進的技術」について appsec 領域から見ると、「諜報を潜在化させる技術」であると考える。セッションでは、TikTok を例に様々な情報を秘密裏に採取する中で猜疑の目をくぐり抜けてきたケースとして考察し、マルウェアと一般アプリケーションとの境界線がより曖昧になっていることとそれによりmass-surveillance が現実的な脅威になっていることを示す。また各プラットフォームの現状では一般ユーザによる自衛が困難であることを示し、「挙動の可視化」が重要な方策であることに触れたい。

From appsec view, Cyber Advanced Technology contains technologies that make reconnaissance more coverter. In the session, take a look of TikTok as a case that it has gathered a lot of information, slipping through scrutiny, showing that borderline between malwares and regular apps are becoming blurry these days and it brings threat of mass-suveilance into reality. Then take a look at the current situation of mobile platform, showing that it is not sufficient to protect users against the problem, concluding that timely informing of actual behavior is an important factor in protection against the problem.

Watanabe 渡 辺

1. 氏名及び役職名等（Name and Title）

渡辺 秀明 日本宇宙安全保障研究所理事
Dr. Hideaki Watanabe, Director, Japan Institute for Space and Security

2. 略歴（CV）

2013 年 防衛省技術研究本部長
2015 年 防衛装備庁長官
2017 年政策研究大学大学院客員研究員 多摩大学客員教授
2019 年日本宇宙安全保障研究所理事

2013 Director general of technical research and development,
2015 Commissioner of Acquisition, technology and Logistics Agency
2017 Visiting Scholar GRIPS, Visiting professor Tama University
2019 Japan Institute for Space and Security

3. 参加枠（Time Slot）

Day 1, 21:20-21:40：Keynote Speech 1-8

4. 講義要約（Abstract）

「宇宙におけるサイバーセキュリティ」
Cybersecurity in Space

宇宙におけるサイバーセキュリティ対策は、最近注目を集めている。米軍は、本年ホワイトハッカーに軌道上の実衛星をハッキングさせる競技を実施させるなど、対策を本格化させている。一方、民間衛星に関しては、セキュリティ対策上の基準は現在のところ、決められたものは特にない状態となっている。
民間衛星は、今後利用が促進され、多くの衛星が宇宙に打ち上げられる傾向となっているが、サイバーセキュリティ対策が脆弱であると、宇宙利用の安全対策が全体として不十分となる可能性があり、大きな課題と　なっている。米国は、SPD5（Space Directive 5）を発出し、連符政府に対し、民間企業セクターとサイバーセキュリティに関する情報共有するように指示した。我が国も同様の施策を行う必要があると思われる。

Cybersecurity for Space is center of interest. The US military promoted an event named Hack-a-Sat contest in which ethical hackers compete with each other to hack real satellite in orbit. On the other hand, as for commercial satellites, there is no regulation about cybersecurity. A lot of commercial satellites will be launched in coming years. If they are vulnerable to cybersecurity, it will be a big problem for safety of Space. The US government issued Space Directive 5 which asks Federal agencies to work with the commercial sector and other non-government space operators to define best practices, establish norms, and promote improved cybersecurity behaviors. Japan needs to make a similar kind of policy.

2020 月 12 月 1 日発行

CYDEF 実行委員会

〒105-0011 東京都港区芝公園 3-5-8
一般財団法人 機械振興協会 経済研究所 気付
サイバーディフェンス研究会

問合せ先：yokoso.cydef@gmail.com

This page intentionally left blank.

CYDEF2020

December 1, 2020

CYDEF Executive Committee 2020