2025 年 4 月 18 日 第 3508 回例会

於： 横須賀商工会議所

＜点鐘・開会＞ １２：３０ 高 橋 会長
＜斉　　唱＞ 「それでこそロータリー」
＜ゲスト紹介＞ ＊久里浜駐屯地司令 陸将補 奈良岡 信 一 様
＊米山奨学生 朴 栽 潤 様
＊青少年交換留学生 Lualy Rehen HOFER TURCATO さん
＜米山奨学生へ奨学金授与＞ 会長より朴 栽潤様へ
＜青少年交換留学生へ小遣い授与＞ 会長より Lualy Rehen HOFER TURCATO さんへ

米山奨学生 朴 栽潤 さん

青少年交換留学生 Lualy さん

＜会 長 報 告＞ ＊第１０回理事役員会報告
＊ガバナー事務所から
・２０２５学年規定審議会報告会開催のご案内について
開催日時：５月１６日(金)１５:００～１６:３０（１４:３０受付開始）
場　　所：藤沢商工会館ミナパーク６Ｆ「多目的ホール１＆２」

＜幹 事 報 告＞ ＊第１６回米海軍第７艦隊バンド&横須賀交響楽団フレンドシップ・コンサート
アメリカン・サウンド・イン・ヨコスカのご案内
開催日時：９月１４日(日)１５:００開演
会　　場：横須賀文化会館大ホール
チケット：３，２４０円/枚
＊例会後第４回被選理事役員会 開催（例会場）

＜出 席 報 告＞ ＊出席委員会 角井副委員長から４月１８日の出席報告

会 員 数	出席対象者数	出席数(ZOOM 出席数)	欠 席 数	ﾒｰｸｱｯﾌﾟ数	出 席 率
１１２名	１０４名	７２名(３名)	３２名	１５名	82.08%

メークアップ：浅葉、Enora、岡田(英)、小保内、笠木、加藤(元)、木村、竹株、平松、堀川、
前田、森、吉田(久)、若麻績 各会員 ＩM出席
新倉会員 横須賀ＲＡＣ例会主出席

＜ニコニコ報告＞

・三　　役　久里浜駐屯地司令兼システム通信・サイバー学校長　陸将補　奈良岡信一　様、本日はお忙しい中､卓話をお引受け戴き有難うございます｡貴重なお話し楽しみにしています。宜しくお願いします。

・児　玉、岡田㊐、梁　井、北　村、梶　木、井　上、八　巻、植　田、
鈴木㊄、松本㊊、田　邉、徳　永、杉　浦、澤　田、真　野、八　木、
齋藤㊎、谷、飯　塚、比　護、瀬　戸、萩　原、三　堀、杵　渕、岩　﨑　各会員
久里浜駐屯地司令兼システム通信・サイバー学校長　陸将補　奈良岡信一　様、ようこそお越しくださいました。本日の卓話を楽しみにしております。どうぞよろしくお願いいたします。

・三　　役　米山奨学生　朴　栽潤様、青少年交換留学生　ルアリーさん本日の例会も楽しんで下さい。朴さん２年間宜しくお願いします。

・大　石、小林㈠、小　澤、角　井、八　巻、野　坂、小山㊍、加藤㊌、植　田、江　口、
濱　田、小林㊏、柴　田、澤　田、八　木、齋藤㊎、佐久間、長　尾、土　田、藤　村　各会員
米山奨学生　朴　栽潤様、青少年交換留学生Lualy Rehen HOFER TURCATOさんようこそお越しくださいました。朴さん、これからよろしくお願いいたします。ごゆっくり例会をお楽しみください。

・岩　﨑、土　田　両会員　入会月祝いとして。

・８番テーブル齋藤㊎マスター、勝見サブマスター　先日の８番テーブルミーティングにご出席いただき有難うございました。高橋会長、渡邉副会長にもご出席いただき有難うございました。

・大野㊓、徳　永、田　中、山　下、高　橋、渡　邉　各会員
メルキュールホテルにて4/15(火)８番テーブルMTが行われました。齋藤㊎マスター、勝見サブマスター楽しい会をありがとうございました。高橋会長、渡邉副会長ご出席頂きありがとうございました。齋藤マスター、シャンパン、マグナムの差し入れありがとうございました。美味しかったです。

・６番テーブル齋藤㊏マスター、鈴木㊄サブマスター　昨日は大変多くの方々の参加で楽しい時間を過ごす事が出来ました。兼城幹事ご参加頂きありがとうございました。

・椿、根　岸、小佐野、兼　城　各会員　昨日、凛にて６番テーブルミーティングが行われました。ご参加頂いた兼城幹事、齋藤愼太郎マスター、鈴木之一サブマスター楽しく美味しい時間を有難うございました。

・石　田、苅　山、権　田、濱　田、三　井、小山㊋　各会員　安くなるかと思いきや、また品薄となったお米。株価や物価も、世界の発言ひとつで大きく揺れる日々が続いています。先の見えにくさを感じる今こそ、地域と共に協力する信頼関係が大切ですね。

＜卓　　話＞　　「 防衛省・自衛隊のサイバー防衛態勢等 」について

久里浜駐屯地司令
陸将補　奈良岡　信　一　様

私は、陸上自衛隊システム通信・サイバー学校長を兼ねまして、久里浜駐屯地司令の奈良岡でございます。本日はどうぞよろしくお願いいたします。本日、横須賀ロータリークラブ様においてお話しする機会をいただきましたこと、本当にありがとうございます。

皆様ご案内の通り、当学校については昨年の３月に名前が通信学校からシステム通信・サイバー学校という名前に変わりまして、学校の組織もサイバー教育部を立ち上げて改編をいたしました。まだ1年しか経っておりませんが、我々このサイバー人材を、どうやって効率的・効果的に育成していくのか検討しておりますけれども、やはり産・官・学の連携、これが大変重要だと思っています。特に産業分野でさまざまな企業さんが悩まれているところ、あるいは企業さんが研究している分野、そういったところの連携、情報共有がこれから大事になってくるだろうと思っています。そういった観点から、このロータリークラブの会員の方々との懇談の機会を得たことは非常に有意義だと思っております。ご紹介していただいた齋藤先輩どうもありがとうございます。

本題に入ります前に私の自己紹介と久里浜駐屯地についてご紹介したいと思います。私は防衛大学校の３５期生で、齋藤先輩の２１期後輩になります。（齋藤先輩はもう雲の上の存在なのです・・・）私は青森の津軽の出身でございます。現在は青森市に合併いたしましたが、昔は浪岡町というところでございました。私の名前は奈良岡ですけどもこの奈良岡というのは津軽の地方に多いです。私は先ほどご紹介がありましたとおり、応用物理学専攻、それから陸上部ですけれども、齋藤先輩と同じでございます。齋藤先輩も応用物理、それから陸上部、齋藤先輩は短距離、私は長距離でございますけれども、非常につながりを感じております。防衛大学校を平成３年３月に卒業いたしました。ですから、陸上自衛隊には３４年間勤務しているということになります。今年で５７歳になります。これまで様々なところで勤務いたしましたが、実は久里浜駐屯地が一番南で、そこから下に行ったことはありません。いわゆる中方西方、それから沖縄を含めた地域では勤務したことはありません。久里浜から全部上、いわゆる東方、それから東北・北海道で勤務をいたしました。私は、もともと陸上自衛隊の通信科幹部として育ってきましたので、通信関係は何となくわかりますが、学校の名前にサイバーがついたことで大変になりました。サイバーというのは非常にわかりづらいです。コンピューター技術が分からないといけませんし、いわゆる電子技術、そういうものの総合です。ネットワークの成り立ちも含めて勉強していかないとサイバーって何ですか、となってしまうものだと思います。皆様各会社等では、ご苦労されている部分もあるかと思いますが、こういったネットワーク、コンピューター関連の事をしっかり意識の向上をしていかないとサイバーには対応できないということをご理解いただければと思っております。

次に久里浜駐屯地についてですが、この久里浜駐屯地は皆様ご承知の通り、久里浜海岸ペリー公園の近くに所在しています。もともとは埋め立て地でございまして、昭和１４年、旧海軍通信学校がそこに開校し、それが始まりです。時を経まして一度、米軍に接収されましたが、解放されて昭和２５年、久里浜駐屯地となりまして今年で７５周年になります。陸上自衛隊では最も古い駐屯地の一つということになります。今我々が勤務している建物は８５年経っています。久里浜駐屯地は年３回、一般開放しています。先般、３月末開催しました桜祭り、７月には納涼祭、１１月には久里浜駐屯地の記念行事です。ホームページ等でアナウンスしていますので、お時間ありましたらぜひご参加いただければありがたいと思います。

それでは、長々と前座がありましたが、本題に沿っていきたいと思います。

まず、サイバー空間における脅威の動向ということでお話したいと思います。サイバーは非常に高度で難しい分野ですが、このサイバー分野というのは魅力的です。一般的な火砲などの兵器よりも、技術を習得で

きれば簡単に敵を倒すことができるというものでございますけれども、これの人材を作るためには相当な労力がかかりますし、相当詳しい教官も育成しなければいけません。現在、かなり力を入れてサイバーの部隊の関係者を育成しているところでございます。また、サイバーというのは、秘匿性が高く、知らないうちに様々なことができる特性がございますので、しっかりと対策を取っていかないと、とんでもない状況に陥っていきます。そういったことを理解した上で様々な対策をやっているところでございます。

各国のサイバー部隊の規模増強ですが、皆様列国のサイバー部隊の人数はどのくらいいると思いますか。アメリカは約６，２００名います、中国は約３万人で、ロシアは約１，０００名と言われています。ロシアの部隊としての人数は１，０００名ですが、その他の一般のいわゆるハッカーなどを集めると相当な数になると思います。それから北朝鮮は約６，８００名と言われています。サイバー攻撃というのは、メインはランサムウェア、いわゆる身代金攻撃ですね。それが主体になって外貨を稼いで、それが北朝鮮ではメインになっています。そういった方たちがこんなにたくさんいるのだということです。一方、我が国は、今のところ約２，３００名くらいです。この２，３００名をあと３年で４，０００名まで増やしていく。そういった目標を掲げていますので、残り約１，７００名ですね。これを３年間で増員しなければならないということになります。では、この１，７００名を当校のシステム通信・サイバー学校で養成するのかといったら、それは物理的に無理です。したがって、我々としてできる限りの人数は養成していきますけれども、陸上自衛隊だけではなくて、海上自衛隊、航空自衛隊もそれぞれ養成しますし、一般の方から募集するなど、あらゆる手段を尽くして目標である態勢を構築していくということになります。

続きまして、重要インフラやサプライチェーンを狙ったサイバー攻撃です。私たちは普通に生活するにもインフラがないとできません。電力、ガス、いろいろなインフラがありますけれどもこのインフラを攻撃して機能を発揮できなくしてしまうことで、簡単に国家としての機能を麻痺させる、そういったことになります。代表例といえば、３年前に起こったロシアによるウクライナ侵攻において、ロシアが攻撃の前にウクライナに対してサイバー攻撃をやってインフラを麻痺しようとした実績があります。そこに対抗したのがアメリカです。おそらくウクライナからの要請によると思うのですけども、アメリカは、ウクライナのインフラが簡単にロシアの攻撃によって破壊されないよう、米国のサイバー要員の中からチームを組んで行っていると言われています。いろいろなインフラのコンピューターの中を調べて、ウイルスがあったらウイルスを駆逐していく、そういった地道な対応をアメリカがやってくれたおかげで、ウクライナはインフラを保持しながらロシアに対応できているというのが現状でございます。そういった対応ができる人たちをきちんと作っていかないと、とんでもないことになります。我が国の重要インフラに対する攻撃があった場合はどうするのかということで、今、国会で議論されています。能動的サイバー防御、いわゆるアクティブサイバーディフェンスと呼ぶのですが、これが先般４月１１日にＡＣＤ法案ということで、衆議院を通過いたしました。まもなく可決成立するのだろうかと思います。この法案は、攻撃元のサーバー等に対してアクセスし、無害化の措置を実行できるよう定めている法案です。

次に、政府としてのサイバーセキュリティの取り組みについてですが、しっかりと対応していかなければならないということで政府が対応しています。まず国全体としてのサイバーセキュリティですが、サイバーセキュリティ戦略本部が立ち上がっており、内閣官房長官が本部長を努めております。そこに関係省庁、例えば総務大臣、経産大臣、防衛大臣、そういった関係閣僚が本部員となっていろいろな取り組みをしていくということになります。これを支えているのが、内閣サイバーセキュリティセンター、通称ＮＩＳＣ（ニスク）というところです。このＮＩＳＣが処理をして、この戦略本部の事務局として数々の取り決め等を遂行しているということになります。今後は、国家サイバー総括室（仮称）に改組されて、国のサイバーに関する施策を取りまとめていく機能の強化をこれから補っていくということになります。役割は能動的サイバー防御の法整備を推進すること、それからサイバーセキュリティ政策の支援として各省庁横断的な取り決めをしていくということになります。今、このＮＩＳＣに相当な人数を集めていると聞いております。

この政府のさまざまな取り組みの中で、安全保障３文書、と聞いたことがあるかと思いますが、この中で最上位の政策文書が国家安全保障戦略になります。これは防衛に限らず、外務・経済、さまざまな安全保障を記載しているものでございまして、この中にサイバー安全保障分野のところも明記されています。すなわ

ち、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上するのだというふうに書いてあります。ということは、今は同等以上ではないということです。アメリカから言わせると、今の日本のサイバーセキュリティの能力は子供のようなものと言われているのです。これは致し方ないと思います。我々もサイバーに関しては相当前から手をつけて、いろいろなことをやってきたのですが、アメリカのやっているサイバーに関わる分野は幅広く、攻撃の分野も行っています。我々は攻撃に全然手をつけていませんから、アメリカはそういう分野の遅れを指摘して、まだまだ子ども、と言っているのだと認識をしています。このように、サイバーに関する能力を上げていかなければならないと、安全保障政策の中でしっかりと明記をしているということになります。

次にそこから防衛戦略にブレイクダウンしていくのですけれども、そこではあらゆるサイバー脅威から自らを防護すること、これは防衛の分野ですので、我々防衛省・自衛隊が活動するにあたって、さまざまなネットワーク、情報システムを駆使して戦闘を行っていきます。そういった自らのシステムをしっかりと防護することが記載されています。そして、我が国全体のサイバーセキュリティの強化への取り組みについてですが、これは先ほど申し上げたＮＩＳＣがいろいろな政策をやっていることに対してしっかりと協力をしていく、とされています。

続きまして、防衛力整備計画になります。この防衛力整備計画については、具体的に今後の態勢・体制しっかりと記載された文書でございますけれども、そこには先ほど申し上げました２０２７年度、あと３年でサイバー専門部隊を４，０００名に拡充しますと明記されました。それから、陸上自衛隊通信学校を今のシステム通信・サイバー学校に改編しますと明記をされています。そうしたことでこの我が校のシステム通信・サイバー学校の改編は滞りなく５年度末、令和６年３月に改編をしたということになります。何が変わったかと言いますと、サイバー教育部が新編され、サイバー人材を育成していく能力をしっかりと強化したということと、それから人材を育成するためには、教官要員も大事ですがそのためにどういった教育をやるのかという研究も大事です。そういった研究機能の強化ということになります。

こうした戦略３文書で書かれた内容を今どのようにやっているのかと、実際の現場について説明します。先ほどは防衛省・自衛隊もアメリカと同様に以前からやっていると言いましたが、その一番最初のとっかかりとして、防衛省ホームページの改ざん事案というのが平成１２年に起こりました。これを機に、平成１７年、陸上自衛隊にシステム防護隊ができました。これは防衛省として初めてでした。一方で、アメリカはいつからサイバーに関わる事項を運用し始めたかというと２０１０年です。実は我々はアメリカの運用開始の５年前からサイバーに関わるシステムの防護に取り組んでいるのです。

アメリカは２０１０年運用を開始して以降、急激に発展したのですが、我々とは運用の考え方の違いがあります。ネットワーク外から入ってくる悪いウイルスを遮断する装置をファイアウォールといい、この装置をつけて悪いウイルスがネットワークに入ってこないような防護体制を取り、万が一入ってきた時にはそれを検知してそれを駆逐して元の体制に戻していこうと取り組んでいます。我々がやってきた分野は防護しかやってないのです。これから議論になってくるのは能動的サイバー防御ですから、何かあった時には敵が悪さをしたところに探りに行って、悪さをできないように処理するということです。そういったものがこれから任務として来るわけです。我々は、これまでそういった分野はやってこなかったので、人材も含めてこれからしっかりと作っていかなければなりません。

平成２６年、自衛隊指揮通信システム隊（令和４年に自衛隊サイバー防衛隊に改称）が新編され、令和６年、陸自システム通信・サイバー学校改編となります。それぞれの役割ですけども、自衛隊システム防衛隊（自衛隊サイバー防衛隊）は、防衛省・自衛隊のインターネットの窓口において、外部からいろいろなメールなどを全部チェックして、悪さをしているものは全部排除しています。そういった装置もありますし、アラームが鳴れば端末を調べて、見つけて削除して外部からの侵入をここでシャットアウトします。それでも侵入してくるものは、陸上自衛隊サイバー防護隊が、その外部から侵入してきた様々なウイルスを検知して、それぞれに個別で対応していく体制をとっています。そのようにご理解いただければと思います。

サイバー攻撃の発信源で一番多いのがアメリカ、２番目が日本、３番目がイギリスと言われています。２番目に多い日本ですが、これは日本から攻撃しているわけではなく、外国人が日本のサーバーを利用して発信しているということです。簡単に日本のサーバーに侵入しているということですので注意が必要です。

最後に今後サイバーに必要な能力についてご説明したいと思います。

ネットワークへの侵入を遮断してやればいいんだという昔からの防御（境界型防御）はもう古いです。侵入されてしまったら、もうどうすることもできません。今はインターネット社会でどこにでも脅威があり、このネットワーク情報システムはどこに行っても信用できないという考え方で対応します。これをゼロトラストと言います。これからゼロトラストの概念でセキュリティ機能の強化をやっていかなければいけません。一つはスレットハンティングという技術です。脅威（スレット）をハントする（狩る）ですね。様々な誤動作、そういったものが発生した場合には現象としてすぐ分かりますが、そうじゃないときに困るのです。何も現象が現れなくてもどこかに何かが潜んでいるのではないか、それを探りに行く、そういった技術がスレットハンティングです。結構高度な技術になっていますけれども、こういった技術をしっかりと確立しなければなりません。それから、ペネトレーションテストというのがあります。自分たちのこれから作るシステムの脆弱性をテストし、脆弱性を見つけたら、そこにしっかりとパッチを当てて強化していく、そういった技術です。このような技術をもってこれからゼロトラストの世界に対抗していく者をこれから育成していきます。

本日はご清聴ありがとうございました。

＜閉会・点鐘＞　１３：３０　高　橋　会長

週報担当　松　川　太　郎