ここに地終わり,空始まる
安全・安心なサイバー空間をめざして

日立製作所
グローバル渉外統括本部 産業政策本部
加藤 兼司

大航海時代と海洋法

ユーラシア大陸最西端，ポルトガルのロカ岬には，眼前に広がる大西洋に向けて「ここに地終わり，海始まる」と刻まれた石碑が立つ。同国の代表的詩人ルイス・デ・カモンイスが大航海時代の祖国の偉業を詠んだ詩の一節だ。事実，大航海時代はポルトガルとスペインが幕を開けた。

両国はイスラム勢力が覇権を握る地中海ではなく，大西洋に目を向けた。1488年にポルトガルのバルトロメウ・ディアスが喜望峰に達し，1492年にはスペインの支援を受けたコロンブスが，西インド航路を開拓した。

両国の競争を抑制するため，トルデシリャス条約（1494年）により，世界の大洋が二分割された [1]。この両大国に挑戦したのが，新興国の英国とオランダである。英国では最初に，エリザベス1世の支援する私掠船※1) と呼ばれる一種の海賊船が，スペイン船から南米の金銀などを略奪して富を蓄積した。スペインは航路を極秘にしたが，エリザベス1世の秘書長官で，英国スパイマスターの元祖と言われるフランシス・ウォルシンガムのネットワークが，これらを把握した。

インド洋航路開拓をめざしたオランダは，権益を独占するポルトガルに対抗するため，1609年にグロティウスが海洋自由論を唱える。国際法の始まりである。私掠船を展開した英国も豊かになり，オランダとの競争になると，法を駆使し始める。英国は領海の概念を定めた閉鎖海論で，海洋自由論に対抗し，1651年には航海法を制定する。18世紀まで海の秩序は戦争法を中心に発展したが，次第に安全・安心な海の利用をめざした法へと転化する。

1945年，米国のトルーマン大統領は，海底油田や漁業資源を念頭に大陸棚の権利などを謳ったトルーマン宣言を行う。この宣言は世界に大きな影響を及ぼし，大陸棚条約や排他的経済水域の概念へと発展した。1958年に国連海洋法会議が開催され，海の憲法と言われる国際海洋法が1994年に発効した。トルデシリャス条約から500年，安全・安心な海洋活用の国際ルールが定められた。

※1）一国の政府から許可を得て，敵国の船を攻撃し，積み荷を奪う許可（私掠免許）を得た船。

[1] トルデシリャス条約

竹田いさみ『海の地政学 覇権をめぐる400年史』を基に作成

大サイバー空間時代の海賊，ハッカー

大航海時代に活躍したキャラベル船に形が似るため「ポルトガルの軍艦」と呼ばれる海洋生物がいる。電気クラゲの俗称を持つカツオノエボシだ。昨年，この猛毒を持つ生物の俗称を冠した映画『電気海月のインシデント』が公開された。福岡を舞台に携帯電話の個人情報を盗みとるマルウェアを仕込んだハッカーと，それを追うホワイトハッカーの戦いを描いたものだ。

マルウェアは，コンピュータウイルスなどの不正なプログラムの総称である。ファイルやプログラムに寄生して自己増殖するウイルスや，単体で動作し自己増殖するワーム，有用なソフトウェアを装い悪意のある動作をする「トロイの木馬」などいくつかの種類がある。ハッカーは，もともとプログラミングなどに精通した人への尊称だったが，現在はネットワークに不正にアクセス（ハッ

キング）する，いわばサイバー空間の海賊を表す。ホワイトハッカーは，ハッカーに対抗するセキュリティ人財だ。またインシデントは，ハッキングやデータ破壊などネットワークの安全を脅かす事象を言う。前述の映画はフィクションだが，実際のインシデントは書籍や映画にできるほどの事件になることもある。日系人の下村努氏は，十代の頃からロスアラモス国立研究所などでコンピュータセキュリティの専門家として活躍していた。1995年，彼はホワイトハッカーとして，FBI（連邦捜査局）が追う大物ハッカーの居場所を突き止め，逮捕に協力した。この事件は，ちょうどインターネットが一般に普及した時期でもあり，世間の注目を集め，その顛末を描いた書籍『テイクダウン―若き天才日本人学者vs超大物ハッカー』が出版され，『ザ・ハッカー』として映画化もされた。

世界初のハッカーは，インターネットもコンピュータもない1903年に現れた。無線電信の発明者マルコーニは，この年イングランド最西端のコーンウォールから，300マイル離れたロンドンへの公開送信実験を行った。すると何者かがこの実験をハッキングし，マルコーニを嘲笑するメッセージを送りつけた。当初ハッカーは正体不明だったが，英国のマジシャンのネヴィル・マスケリンが，公共性の高いインフラである無線電信の脆弱性を示すためにハッキングしたと名乗り出た。

世界の海洋を制覇した英国は情報ネットワークの重要性を認識しており，電信が実用化されると，1850年代に海底電信ケーブルの敷設を始め，欧米や世界各地の植民地を中心に電信ネットワークを築いた。第一次大戦中，英国情報部がこのネットワークを使って，ドイツのツィンメルマン外相がメキシコ政府に打った対米参戦提案の暗号電報をハッキングした。英国はこの事実を隠して米国に電報の内容を伝えた。ハッキングなどのサイバー攻撃の実行犯・組織を特定することをアトリビューションと言うが，このアトリビューションは容易ではなく，また被害の大きさや被害にあった事実にさえ，当事者が気が付かない場合もあるのでやっかいだ。

ロンドン，リオデジャネイロなど近年はオリンピックの開催ごとに大規模なサイバー攻撃が起きている。ロンドンでは2億回のサイバー攻撃があったと言われる。延期が発表されたが，2020年は東京オリンピックが予定されていたため，前述の映画の公開など，一般にも徐々にサイバー攻撃やセキュリティの意識が高まっている。

サイバー空間の攻防

父親と同じく有名マジシャンだった息子ジャスパー・マスケリンは，第二次大戦中に英国陸軍に志願し，トリックを駆使して，戦車の偽装から，アレキサンドリア港の移動，スエズ運河の消失といった奇策を展開し，ロンメル将軍のドイツ・アフリカ軍団を散々に翻弄した。ジャスパーは，マジックを人間の行動に関する知識と科学の応用だと述べている。こうした考えをソーシャルエンジニアリングと言うが，サイバー空間の攻防でもこれが応用される。

サイバー攻撃は無差別型と標的型に大別できる。無差別型はマルウェアを添付ファイルにして電子メールでばらまいたり，ウェブサイトにマルウェアを潜ませたりするなどの方法がある。潜入したコンピュータをロックしたり，コンピュータ内のデータを暗号化し，ユーザーに解除の対価として金銭などを要求するランサムウェアには，無差別型が多く見られる。ソーシャルエンジニアリングを使ってユーザーの心理の隙を巧みに突き，添付ファイルを開かせるよう誘導する。

標的型では政府機関や企業，特に重要個人情報を大量に持つホテル・航空会社・病院などが狙われやすい。この場合でも最初に偽メールでマルウェアを仕込んだうえで，被害者側のデータを十分調査し，攻撃を仕掛けてくることが多い。

ジャスパーは偽の港や折り畳み式潜水艦を使って，敵の攻撃から重要インフラを守ったが，サイバー上の防御でもこうした方法がとられる。サンドボックスは，添付ファイルに潜むプログラムがマルウェアかどうかをコンピュータ上の安全な仮想環境で確認する手法である。ハニーポットはOS（Operating System）などの脆弱性を残

して，囮として攻撃させる機能だ。

重要インフラへの具体的攻撃事例は枚挙に暇がない。2012年に中東の石油プラントで，制御システム用のPC3,000台がマルウェアに感染した。2016年の米国大統領選挙後には，米国やカナダの電力システムが攻撃を受けている。また政府機関への攻撃として有名な事例は，IT立国エストニアが，2007年に受けたDDoS（Distributed Denial of Service）攻撃がある。DDoS攻撃は攻撃対象のサーバなどに複数のアドレスから大量のデータ送信などを行い，攻撃対象のサービスを停止に追い込むものだ。

こうしたサイバー攻撃の裏には，大航海時代の私掠船のように国家の支援がある場合や，ジェームズ・ボンドが活躍する映画「007シリーズ」のように謎の国際テロ組織が暗躍している場合なども考えられるが，攻撃者の正体を突き止めることは困難であるし，攻撃を完全に防ぐことも難しい。

トップのサイバーセキュリティ意識

ところで007シリーズといえば，大女優ジュディ・デンチ氏が演じた英国情報部のトップMは，何度かボンドや敵役に，自分のPCをハッキングされる。情報機関のトップとして，そのセキュリティ意識の低さはいかがなものかと思うが，Mがハッキングされることで一つのインシデントが，映画一本分の大騒動に発展してしまう。

これを映画の話と笑い飛ばすわけにはいかない。現実にも2016年には欧州の航空機部品メーカーでCEO（最高経営責任者）からのメールを装うビジネスメール詐欺が発覚した。財務担当者が指示に基づきM&A資金4,200万ユーロを緊急送金し，詐取された。メーカーが回収できたのは1,090万ユーロだけだったという。Mはハッキングにもめげず職務を全うしたが，この部品メーカーのCEOは，任務懈怠を理由に長年務めたCEO職を解任された。

敵役も負けていない。映画のクライマックスは，敵の秘密基地でのボンドと敵役の対決シーンだが，まずボンドは，秘密基地に易々と侵入する。何かの拍子に施設が出火すると，わずか数カットのうちに，広大な基地全体に延焼し大爆発を起こすという，見た目が豪奢な割にとんでもない安普請の基地だ。敵役は攻撃には莫大な投資をするが，基地はコストセンターと思っているのか，ろくにセキュリティ投資をしていないようで，結局その野望は挫かれる。

（物理的攻撃とサイバー攻撃の違いはあるが）これも現実には似たインシデントが起きている。2009年に経営破綻した北米のIT機器メーカーでは2000年頃からサイバー攻撃を受けていたとみられる。2004年にCEOを含む経営幹部のアカウント乗っ取りが判明した。セキュリティ担当者が経営幹部に対策を進言したが受け入れられず，その後も数年にわたって攻撃を許し，研究開発や事業計画などの重要文書が盗まれ，同社の倒産の一因を作ったと言われている。

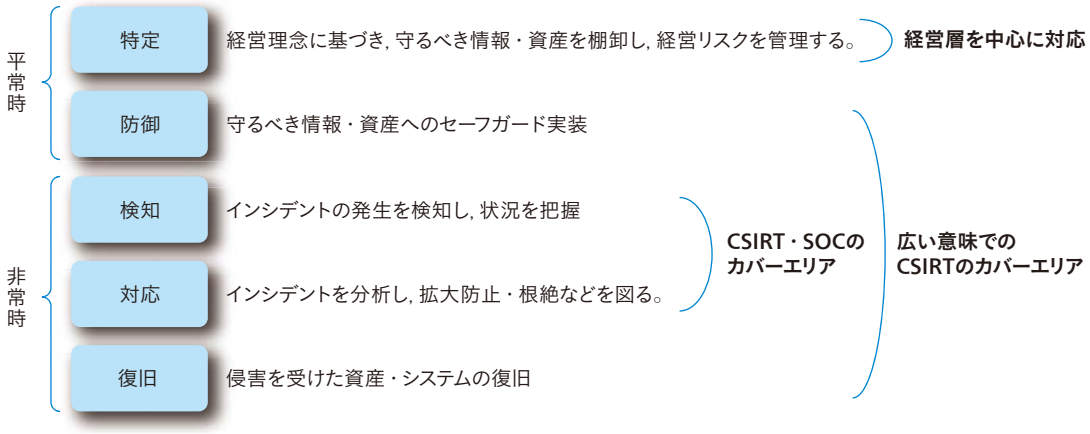
今や，サイバーセキュリティを経営の問題として捉えることと，経営層のセキュリティ意識の向上が世界共通の課題である。そこで経団連では「サイバーセキュリティ経営宣言」を2018年に発表し，2019年には取締役向けの「サイバーリスクハンドブック」を発行している。

サイバーセキュリティのフレームワーク

企業や経営層へのセキュリティ理解に役立つのがサイバーセキュリイティのフレームワークである。中でもよく知られるのが，米国のNIST（国立標準化技術研究所）が，2014年2月に初版を公開したサイバーセキュリティフレームワークだ[2]。2013年の一般教書演説で当時のオバマ大統領が重要インフラへのサイバー攻撃のリスクに言及し，さらに同年2月，大統領令13636（重要インフラへのサイバーセキュリティ向上）を発布した。これを受けてNISTが作成したのが，このフレームワークである。

そこではコアとなる（1）特定，（2）防御，（3）検知，（4）対応，（5）復旧の五つの機能が定められている。特定はサイバー攻撃から守るべき資産・情報などを決定することだ。これは，自社のコアコンピタンス，優位性の根源

[2] NISTサイバーセキュリティフレームワーク



鎌田敬介『サイバーセキュリティマネジメント入門』ほか各種資料を基に作成

注：略語説明
CSIRT（Computer Security Insident Response Team），SOC（Security Operation Center）

が何かを経営視点で確認し，それが侵害・破壊などされた場合の経営リスクを加味し，守るべき資産・情報を棚卸する作業である。防御は具体的な施策を展開することだが，完璧な防御は不可能という前提に立ち，検知，対応，復旧を検討していく必要がある。

特定は経営層が中心になり企業理念などに従い決めるものだが，それ以外の機能で活躍するのがCSIRT（Computer Security Incident Response Team）やSOC（ソック）（Security Operation Center）と呼ばれる専門家だ。CSIRTは，1988年に初めてワームが発生し，大規模なインターネット障害が起きた際，インシデント情報などを迅速に組織全体に伝えるチームが必要との反省から生まれた。CSIRTはインシデント対応の管制塔として機能するが，その守備範囲は組織によってさまざまである。またSOCはインシデントの検知，対応に当たる専門チームである。

日立では1998年にインシデント対応のプロジェクトが設置され，2004年にHIRT（Hitachi Incident Response Team）として組織化された。HIRTでは，インシデント対応だけでなく，システムの脆弱性対策，また自社の情報セキュリティへの取り組みに加え，顧客の情報・制御システムを対象とした日立製品・サービスのセキュリティ確保の視点から，日立のサイバーセキュリティ活動を支援している。SOCは2017年10月から，24時間365日のサイバー攻撃監視を担っている。また，顧客向けのMSS（Managed Security Service）ほかとして現在は世界4拠点で，四つの言語（英語・フランス語・スペイン語・日本語）により世界50か国以上に向けて提供している。

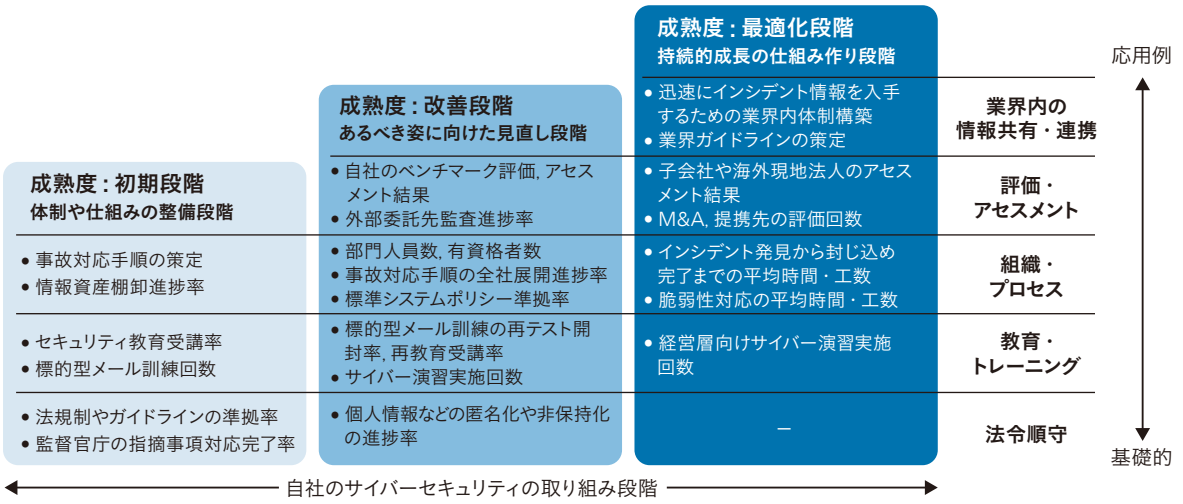
セキュリティを見える化する

ホワイトハッカー下村努氏の父親である下村修博士は，オワンクラゲの緑色に光る物質GFP（緑色蛍光タンパク質）の研究により2008年にノーベル化学賞を受賞した。GFPは，観察したい細胞内のタンパク質にこれを組み込み，緑色発光させることで，観察対象を見える化するのに役立つ。

企業トップのセキュリティ意識を向上させるうえで，昨今課題となっているのが各企業のサイバーセキュリティ成熟度の見える化である。繰り返しになるが，セキュリティは技術的な問題ではなく，経営課題なのだ。

この点，サイバーセキュリティ専門のシンクタンクJCIC（一般社団法人日本サイバーセキュリティ・イノベーション委員会）では，セキュリティを経営課題として捉えやすくするため，金額（損失額）を用いたKPI（重

[3] JCICによるサイバーセキュリティのKPIモデル



出典：JCIC『損失額を減らすための「サイバーセキュリティのKPIモデル」（試論）』

注：略語説明
M&A（Mergers and Acquisitions）

要業績評価指標）モデルを提案している[3]。JCICのKPI案では，自社のセキュリティの取り組み（成熟）段階を，初期／改善／最適化に分類し，また施策の種類を法令順守／教育・トレーニング／組織・プロセス／評価・アセスメント／業界内の情報共有・連携に分類したマトリクスで見える化している。

また英国では2014年，政府が企業などのセキュリティの基本活動を示した「サイバーセキュリティエッセンシャルズ」認証制度を公表した。機微な情報が関わる政府調達の応札条件に，この認証取得が示されている。さらに2018年に改訂されたNISTフレームワークでは，サプライチェーンリスクマネジメントをコアに加えている。サプライヤ，顧客は他社ともつながっており，ゆえに自社の成熟度の向上だけでは不十分なのはもちろん，サイバー空間とフィジカル空間が高度に融合したSociety 5.0の時代では，なおさら社会全体のサイバーセキュリティ成熟度向上が重要となる。

日立では，モノ／人・組織／社会の三つがつながるという観点で，「セキュリティエコシステムの構築」を新たな戦略とした。Society 5.0の実現に向け，より人々が安全・安心に暮らすために，日立は企業内に加え産・官・学が協創した社会全体でのセキュリティエコシステムの構築を推進し，サイバーレジリエンス強化に取り組んでいる。

安全・安心なサイバー空間の活用をめざして

2019年のダボス会議で安倍首相は，来るべきデータ駆動型社会におけるデータガバナンス（Data Free Flow with Trust）の重要性を説き，「データガバナンス大阪トラック」を提唱した。同年のG20サミットでも首相は国境を越えた自由なデータ移動を認める「データ流通圏構想」を提唱するなど，国際ルールの形成を呼び掛けた。

Trust（信頼）と日立創業の精神の一つ「誠」の関係について，創業期の幹部，高尾直三郎は，誠は古今東西を問わず人間社会の基本的道義であり，一方，重要インフラは長く使用されるだけに信頼が第一であるため，誠の努力の積み重ねにより得た信頼こそが最上である旨を述べている。そして，誠で造った製品には誠が宿り，誠の宿った製品を使う会社には誠が宿る，誠が宿った会社は繁栄すると語っている。高尾の考える誠の連鎖こそが，マルウェアなどの悪意のあるサイバー攻撃を凌ぐ力となり，また信頼に基づいた安全・安心なサイバー空間活用の国際ルールの礎となる。

「ここに地終わり，海始まる」の石碑とロカ岬から眺める大西洋

今，我々の眼前にはフィジカル空間とサイバー空間が高度に融合されたSociety 5.0の大空間が広がっている。日立では，JCIC理事長や日本シーサート協会運営委員長などのセキュリティ人財を供給しており，エコシステムのセキュリティ成熟度の底上げや人財供給に貢献している。また，グローバルにおいても標準化団体（ISO/IEC JTC1/SC27，OASIS CTI，IEC　TC65/WG10,WG20，ほか[※2)]）に参画し，今後も，この誠の精神を製品・サービスの提供だけでなく，あらゆる機会を通じてエコシステム全体，社会全体に広めていきたいと考える。

ここに地終わり，空始まる（Onde a terra se acaba e o espaço começa）。

※2）略語注記
ISO：国際標準化機構，IEC：国際電気標準会議，ISO/IEC JTC1/SC27：ISOとITCによる合同技術委員会（JTC1）のサブコミッティ（SC27），OASIS CTI：構造化情報標準促進協会のサイバー脅威インテリジェンス，TC65：IECの工業用プロセス計測制御，WG：ワーキンググループ

参考文献など

1）株式会社ICS研究所：サイバー攻撃の事例集（2019.2）
2）NTTサイバーセキュリティ研究会：経営としてのサイバーセキュリティ，日経BP社（2015.10）
3）鍛忠司：社会インフラの安心・安全を確保するためのセキュリティ技術の研究開発，情報処理，Vol.55，No.7，国立情報科学研究所（2014.7）
4）鎌田敬介：サイバーセキュリティマネジメント入門，きんざい（2017.10）
5）古賀衛：近代海洋法の発展過程，海洋法の歴史的展開，有信堂高文社（2004.10）
6）下村修：クラゲに学ぶ ノーベル賞への道，長崎文献社（2010.10）
7）下村努，外：テイクダウン 若き天才日本人学者vs超大物ハッカー，徳間書店（1996.5）
8）高尾直三郎：日立回想録，日立印刷（1985.2）
9）竹田いさみ：海の地政学 覇権をめぐる400年史，中公新書（2019.11）
10）竹田いさみ：世界史をつくった海賊，ちくま新書（2011.2）
11）土屋大洋：サイバーセキュリティの地政学，ITUジャーナル，Vol.47，No.9（2017.9）
12）デヴィッド・フィッシャー（金原瑞人 他訳）：スエズ運河を消せ トリックで戦った男たち，柏書房（2011.10）
13）中尾康二：歴史を紐解くセキュリティ技術，その現在，そして未来，情報処理学会デジタルプラクティス，Vol.9，No.3（2018.7）
14）JCIC：損失額を減らすための「サイバーセキュリティのKPIモデル」（試論）（2019.4）
15）日立製作所：情報セキュリティ報告書2018
16）日立製作所：日立 統合報告書 2019（2019年3月期）
17）ブループラネットネットワークス：決定版 サイバーセキュリティ 新たな脅威と防衛策，東洋経済新報社（2018.11）
18）松原実穂子：サイバーセキュリティ 組織を脅威から守る戦略・人材・インテリジェンス，新潮社（2019.11）
19）宮尾健，外：社会インフラのデジタライゼーションを支えるセキュリティ，日立評論，100，3，313～317（2018.5）
20）Dory Gascueña：Nevil Maskelyne vs Marconi: a hacker in 1903,
https://www.bbvaopenmind.com/en/technology/visionaries/nevil-maskelyne-vs-marconi-a-hacker-in-1903/ （2020年3月参照）