・本文中の〔　〕は訳者による補足を示す。

プロローグ　3つの汚名

1990年代の終わり、オーストラリアに住んでいたジュリアン・アサンジは、フリーソフトウェアの開発に明け暮れていた。[1] 彼がウィキリークスを立ち上げるのは6年後のことだったが、情報セキュリティに関する彼の知識はすでに確立されていた。それまでの5年間、彼はコンピュータをハッキングしたとして有罪判決を受けたり、若いコンピュータハッカーグループの活躍を描いた本の出版に協力したりしていた。[2] またアサンジは、商用のコンピュータセキュリティ製品を開発する会社を共同で設立していた。[3]

彼は情報セキュリティに関心を持ち、いくつかの電子メールのディスカッションリストにも登録していた。その中に「インフォメーション・セキュリティ・ニュース」というメーリングリストがあり、そこには情報セキュリティに関する主要な報道機関のニュース記事が掲載されていた。[4] このリストのメンバーは、他にもさまざまな関心事を投稿したり、情報セキュリティについてメンバー同士で議論

したりしていた[5]。

２０００年6月13日、メーリングリストに1つのメッセージが投稿された。そこにはコンピュータセキュリティに関する研究のうち、最も早く発表されたものの1つへのリンクが貼られていた[6]。タイトルは「コンピュータシステムのセキュリティ管理」で、投稿者はそれを「すべての始まりとなった論文」と評していた。これを見たアサンジは、次のように返信した。「人類にとって悲しむべき日だ。これは肛門性格のパラノイド〔肛門性格とは、フロイトが主張した心理発達の5段階における2番目の時期「肛門期」に固執することによって生まれる性格で、強情や潔癖といった特徴を持つ〕のための機械化されたスキームだね。それを使えば、認可されていない予想外の創造的な行為を自動的に粉砕するという権威主義的な夢を実現することができるというわけだ[7]」。この返答は大げさで辛辣、おそらくは皮肉でもあったが、「情報は自由を求める」というハッカー文化の思想を支持しており、後にアサンジが残すことになる遺産の小さな一部となった[8]。

しかしアサンジは間違っていた。情報セキュリティの研究は、社会に多大な価値をもたらしたのである。ネットにおいて、プライベートで匿名性の高いコミュニケーションを可能にするのは、セキュリティのテクノロジーと手法だ。それによって反体制派の人々は連帯し、政府による監視から身を守ることが可能になる。内部告発者は、企業や政府の不正や違法行為をより安全に暴露することができる。ウィキリークス自体、情報セキュリティの研究から生まれた技術や運用方法なしには成り立たなかっただろう。

アサンジは、情報セキュリティを研究する取り組みを単に「白か黒か」で表そうとしたが、それは

間違いだった。そこには明らかに、利益とコストの両方が存在するからだ。レオン・トロツキーは、「あなたは戦争に興味がないかもしれないが、戦争はあなたに興味がある」と言ったとされる。その意味するところは、自分に影響を与える可能性のある事柄を無視してはならないということであり、そして情報セキュリティの問題は、いまや日常生活の中にまで浸透している。最初のデジタルコンピュータの誕生は、コンピュータと情報セキュリティの両方の新時代の始まりを告げた。世の中の情報がますますデジタル化されていく中で、その情報を保護できることが最優先事項となっている。情報セキュリティの重要性は高まる一方だが、それを実現するための取り組みはまだ道半ばだ。情報セキュリティの重大な欠陥が常態化している上、それは深刻な構造的問題に根ざしている。

知的財産や顧客の機密データの保護、情報セキュリティに関する法律に準拠していることの証明を目的として、さまざまなセキュリティ製品やサービスに数十億ドルが費やされている[9]。しかし数十億ドルを投じてなお、データ漏洩は頻繁に発生し、広範囲に及んでいる。２００５年、米国の百貨店ＴＪマックスの顧客1億人以上のデビットカードとクレジットカードの情報が、ハッカーによって奪われた[10]。２０１３年、ヤフーでデータ漏洩が発生し、30億人のユーザーアカウントの情報が流出した[11]。データ漏洩によって個人情報が盗まれると、個人や流出元となった組織に悪影響が及ぶ。

世界的に見ても、コンピュータハッキングは、知的財産の窃盗、選挙の操作、スパイ活動などを目的として、それぞれの国家で研究、開発、利用されてきた。２０１０年に発見されたコンピュータウイルス「スタックスネット」は、核物質の生産に使用されるイランの遠心分離機を感染させ、損傷を与えることを目的として開発された[12]。同じ年、中国政府が大規模なコンピュータハッキングを行い米

国企業から知的財産を盗み出したことを示す、強力な証拠が提示された。[13] さらに米国家安全保障局（ＮＳＡ）と英政府通信本部（ＧＣＨＱ）が、コンピュータと電子通信を国境を越えて広く盗み見るために、コンピュータハッキングの手法を用いていたことが発覚した。[14]

データ漏洩とコンピュータハッキングという対を成す問題は、現代の情報セキュリティ分野が根本的な原因を解決しようとするのではなく、セキュリティ問題への「対症療法」の繰り返しに陥ることで、ますます深刻化している。これは、対応しなければならない新しい技術や新しいセキュリティの脆弱性が次から次へと出てくるというだけでなく、新しいものに対して人間がバイアスを持つためでもある。新しいものはファッショナブルであり、なにより望まれる。しかし流行に乗り遅れまいとする気持ちは、物事の本質を見極める機会を台無しにしてしまいかねない。バッファオーバーフロー〔コンピュータ上の特定の領域において、上限を超えた量のデータが書き込まれることで、その領域のデータが破壊されてしまう現象〕、フィッシング〔銀行口座番号やクレジットカード番号など、経済的価値のある情報を、対象者から盗み取ろうとする行為〕、ＳＱＬインジェクション〔アプリケーション上の脆弱性を利用して、データベースを操作する言語「ＳＱＬ」を読み込ませ、不正な操作を行おうとする行為〕など、現在のコンピュータシステムのセキュリティを脅かしているさまざまな脆弱性は、実は新しいものではない。これらを解説した記事が、バッファオーバーフローについては１９７２年に、フィッシングについては１９９５年に、ＳＱＬインジェクションについては１９９８年に発表されている。[15] 情報セキュリティの分野における、この「認知的閉鎖」（人々が現実から逃避し、作り物の世界に引きこもっている状態を表す用語）は、現在を優先し過去を切り捨てるという状況をもたらした。その結果、不幸にも膨大な機会費用〔ある選択をすることで失ったものの価値のこと〕が発生してしまったのである。

この３つの重大な失敗、すなわちデータ漏洩、国家によるコンピュータハッキングの利用、認知的閉鎖は、情報セキュリティの分野を特徴づける、明白な汚名だ。症状ではなく原因に向き合うことで、この３つの汚名を返上することができるが、そのためにはこれらがどのようにして生まれたのかを理解する必要がある。

アサンジは、情報セキュリティに関する初期の研究を即座に否定したが、情報セキュリティ分野における課題は、１９７０年代に行われた基礎的な研究に根差している。この時代、少数の学者や研究者が、未来への道筋を示すアイデアを生み出していた。それらをもたらしたのは、ランド研究所などのシンクタンク、米中央情報局（ＣＩＡ）やＮＳＡなどの政府機関、ロッキード・ミサイル・アンド・スペースなどの防衛関連企業だった。

彼らはテクノクラートであり、「コンピュータシステムは合理的で科学的な法則に従えば保護できる」という信念で結ばれていた。そしてこの取り組みに、知的な純粋さを持ち込んだ。彼らのビジョンは、安全と秩序を約束するものだった。しかし彼らは、自分たちの取り組みの核心部分に、最初から危険な欠陥があることに気づいていなかったのだ。その欠陥が、情報セキュリティ分野の発展と、現代における情報セキュリティの実現に大きな影響を与えることになる。

1　情報セキュリティの「新次元」

コンピュータの登場

１９６０年代後半から70年代前半にかけて、少数の学者や研究者が、現代の世界に大きな影響を与えるアイデアを生み出した。彼らの夢は、コンピュータの世界において、情報が守られる未来をつくることだった。彼らは人間が合理的な機械の歯車として機能し、それを米軍が動かすことが可能になると信じていたのだ。その取り組みは確かに世界を変えたが、それは彼らが意図したような形ではなかった。

そうした背景から今日の情報セキュリティが生まれた。彼らの働きにより、情報セキュリティというゲームの盤面が用意されたのだ。プレイヤーとなるのは、コンピュータハッカーを迎え撃つ組織、内部の人物による情報漏洩を防ごうとする政府、そして個人情報を守ろうとするすべての人々である。

盤面の反対側には、コンピュータハッカー、スパイ、テロリストなどがいるが、彼らもまたプレイヤーだ。

このような学者や研究者を集めたのは、初期のコンピュータをはじめとする新たなテクノロジーを取り入れてきた歴史を持つ米軍であった。米軍が情報セキュリティの発展に与えた影響は、彼らがコンピュータ自体の開発に与えた影響とかたく結びついている。１９４３年、米陸軍は世界初の「電子計算機」であるＥＮＩＡＣの設計・開発への資金提供を開始した[1]。ＥＮＩＡＣを設計したのは、Ｊ・プレスパー・エッカートとジョン・ウィリアム・モークリーである。エッカートは電気技師、モークリーは物理学者で、２人とも戦時中の計算機研究の中心地だったペンシルベニア大学ムーア電気工学スクールに勤務していた。彼らはＥＮＩＡＣコンピュータを販売するために、１９４８年にエッカート・モークリー・コンピュータ・コーポレーションを設立する[2]。

陸軍はＥＮＩＡＣを使い、大砲の射表〔大砲を発射する際に照準の計算をするために使われる表。コンピュータがなかった時代には人力による計算でその作成が行われた〕を計算した[3]。ＥＮＩＡＣは、この作業に最適のマシンだった。射表の計算では、似たような複雑な数式を繰り返し処理しなければならないからだ[4]。砲弾の弾道を理解し予測することは、第２次世界大戦を戦うために新型の大砲を大量に開発していた陸軍にとって、大きな関心事だった。

ＥＮＩＡＣは驚異的な機械だった。重さは30トンあり、１万８０００本の真空管、騒がしい電動タイプライター、うなりを上げるテープドライブなどで、部屋全体が埋め尽くされた[5]。そこには膨大な量のケーブルが使われ、空腹のネズミたちが天敵だった。ＥＮＩＡＣの設計時、エッカートとモーク

リーは、さまざまな種類のケーブルの絶縁体が入った箱に、数匹のネズミを入れる実験を行った。そこで最もネズミに齧られなかった絶縁体が採用されたのである。[6]

ＥＮＩＡＣのオペレーターは、史上初のコンピュータプログラマーと言っても過言ではないだろう。それは、ペンシルベニア大学から米軍に採用された６人の先駆的な女性たちであった。[7]彼女たちに与えられた仕事は、数学的知識を駆使して、コンピュータのさまざまな部分を配線し、ＥＮＩＡＣの設定を行うことだった。そうすることで、必要な計算ができるようになるのである。[8]彼女たちのＥＮＩＡＣとコンピュータ分野への貢献は、近年になってようやく認識されるようになった。[9]

１９５０年、エッカート・モークリー・コンピュータ・コーポレーションはレミントンランドに買収された。この複合企業は軍事市場とも関わりが深く、現在では同社を象徴する拳銃となった「１９１１」をはじめ、さまざまな通常兵器を製造・販売していた。

第２次世界大戦終了後、米軍は戦争の遂行とは直接関係のない、新たな課題に直面していた。その多くは、人員や機材をいかに効率的に移動させ、世界中に新設した膨大な数の米空軍基地に供給するかという、ロジスティクスに関する課題であった。これらの課題を解決するために、ＥＮＩＡＣの後継機であるＵＮＩＶＡＣの採用が検討された。[10]ＵＮＩＶＡＣはUniversal Automatic Computer（汎用自動計算機）の略で、この名称は、マシンが全般的な問題を解決でき、特定のタイプの計算に限定されないことを示すために注意深く選ばれたものだ。[11]マシンに柔軟性を持たせるこうしたイノベーションには価値があり、特に解決すべき問題の種類が多い米軍にとって、ＵＮＩＶＡＣは魅力的

であった。

最初に製造された10台のＵＮＩＶＡＣコンピュータのうち、３台が米軍の施設に設置された。陸軍、海軍、空軍が、それぞれに固有の問題に対応するために、ＵＮＩＶＡＣを導入したのである。[12]空軍に納入されたＵＮＩＶＡＣは、１９５２年６月にペンタゴンに設置された。[13]このＵＮＩＶＡＣは、「プロジェクトＳＣＯＯＰ（Scientific Computation of Optimal Problems：最適問題の科学技術計算）」というコードネームが付けられた活動で使用された。プロジェクトＳＣＯＯＰでは、ＵＮＩＶＡＣを使って１０００近い変数を含む数学的計算を行い、ロジスティクス問題の解決に役立てた。人間の数学者と違い、ＵＮＩＶＡＣはそうした計算の答えを素早く出すことができた。このプロジェクトの成功が高く評価されたため、ＵＮＩＶＡＣは１９６２年になってもまだ使われ続けていた。その頃には、より洗練されたコンピュータがあったにもかかわらず、である。プロジェクトＳＣＯＯＰのメンバーの１人は、「このデジタル計算機がきっかけとなって、実現しうるものとして、あるビジョンが生まれました」と語っている。[14]

そのビジョンは広大なものだった。米軍は、暗号化されたメッセージの解読、新兵器の開発支援、ロジスティクス問題の解決、その他数百もの大小さまざまな課題にコンピュータを活用しようと考えた。[15]さらに、人工衛星の軌道の計算など、まだ実現されていない技術をコンピュータでサポートすることも考えていた。[16]米軍はコンピュータがもたらす恩恵を理解し、世界全体が電子化されていくことを予期していたのである。実際に、１９５０年代の終わりから60年代の初めにかけて、コンピュータへの依存度は高まっていった。またこの時期は、コンピュータが大きく進化した激動の時代であり、

その発展は、情報セキュリティにも大きな影響を与えることになる。

１９５０年代後半のコンピュータは、現在の基準から考えるとバロック様式とも言えるものだった。大聖堂でパイプオルガンを演奏するオルガン奏者のように、１人のオペレーターが機械に囲まれて操作するのである。コンピュータは指示されたことだけを行い、オペレーターが考えるのを止めたときには、おとなしく待っていた。しかしこれでは非効率的だった。コンピュータは非常に高価であったため、コンピュータが計算を実行していない「ダウンタイム」を発生させないことが理想的だったのである。この問題を解決したのは、画期的なイノベーションだった――タイムシェアリングが可能なコンピュータの開発である。タイムシェアリング型のコンピュータでは、あるユーザーが作業を中断している間、他のタスクを実行することができる。キー入力の間のわずかな時間も、生産的に利用できるのだ。複数のユーザーが同時にコンピュータを使うことができるようになり、またそれぞれのユーザーは、マシンが自分のタスクに集中していると感じられるような形でコンピュータを操作することができた[17]。コンピュータを使うことは、個々人の孤独な体験から、共有された協力的な体験へと変化した。この変化は、まったく新しい種類のセキュリティリスクを生み出した。１台のコンピュータに複数のユーザーが同時にアクセスできるようになったため、ユーザー同士が互いのプログラムを妨害したり、見てはいけない機密データを見てしまったりする可能性が生じたのである。

米軍が情報を保護する上で中心に据えるのが、「分類」という考え方だ。文書には、トップシークレット（機密）、シークレット（極秘）、コンフィデンシャル（秘）などの分類レベルが与えられる。人々は、自分に与えられた権限よりも高い分類の情報を見ることはできない。たとえばコンフィデンシャルの権限しか持たない人物は、トップシークレットに分類された情報は閲覧できないのである。タイムシェアリング型コンピュータを使用する際、あるユーザーはトップシークレットの閲覧権限を持っていて、別のユーザーは持っていなかったとしよう。こうした場合、トップシークレットの情報を公開することなく、そのコンピュータに保存して処理するには、どうすればよいのだろうか？　タイムシェアリング型が開発される前、コンピュータは決まった部屋に据え付けられ、ドアには警備員が配置されていた。しかしタイムシェアリング型のシステムでは、ユーザーがコンピュータを操作するための端末はいくつもあり、それらを建物内に分散して配置することが可能になった。そのためタイムシェアリング型コンピュータでは、物理的なセキュリティやユーザーの監視が、非常に難しくなったのである[18]。

タイムシェアリング型コンピュータは経済的なメリットをもたらすことから普及する可能性が高く、そのため、コンピュータに革命を起こすと期待されていた。しかし、コンピュータに保存される情報のセキュリティへの潜在的な危険性は飛躍的に増え、その危険性に対する不安は、米軍や彼らが契約している防衛関連企業にまで波及した。彼らはこうした動きを、情報セキュリティという課題の「新次元」と捉えていた[19]。それは米軍が解決しなければならない課題だったが、彼らは自分たちだけでは解決できないと考え、パートナーを募った。そのパートナーとは、ＣＩＡ（中央情報局）やＮＳＡ（国家安全保障局）などの米政府機関や、大手防衛関連企業、シンクタンクなどである。シンクタンクの中でも際立っていたのがランド研究所だ。ランド（ＲＡＮＤ）という名称は、研究開発（research and development）を縮めたものである。ランド研究所はアイデアを生み出す工場といった存在で、

すでに米政府に戦争の進め方や勝ち方について助言していた。

ランド研究所

ランド研究所は、１９４２年に陸軍航空軍大将のヘンリー・〝ハップ〟・アーノルドによって創設された[20]。第２次世界大戦の終結に際して、戦争のために集められた科学者や学者たちが散り散りになり、米軍が彼らの専門知識を利用できなくなるのではないかという懸念が広まった[21]。そこでアーノルドは、未使用の戦費から１０００万ドルを確保してランド研究所を設立し、研究者たちに居場所を提供した[22]。それから数十年間、陸軍航空軍（のちに空軍）はランド研究所に対し、実質的に無制限の資金を提供する――米軍が直面する最も厄介な問題を解決するための、白地小切手が与えられたというわけだ[23]。

ランドの研究者たちは当初、カリフォルニア州サンタモニカのクローバーフィールド空港にある航空機工場内のオフィスで勤務していた[24]。１９４７年、ランドはサンタモニカのダウンタウンにある、白砂のビーチから徒歩５分の場所に位置するビルに移転した[25]。新しい施設の内装は、ランドのスタッフ同士の偶然の出会いを最大限に生み、コラボレーションが促されるように設計されていた[26]。これは今日でもアップルをはじめとする多くの企業で採用されている手法である[27]。ランド研究所の建物は一見何の変哲もないが、米政府の正式な最高機密の研究施設であり、武装した警備員が24時間体制で常駐していた。ランドの従業員は、政府のセキュリティ・クリアランス〔機密情報を扱う人物に対し、その資格があるかどうかを判断するための経歴調査を行うこと。あるいはそれによって得られた資格を指す〕を受けなければならず、クリアランスを受けるまでは、建物内のどこにいても、トイレにさえも付き添われた[28]。

ランド研究所は当初、陸軍航空軍の中でも研究開発を担当する部署の監督下に置かれ、それがきっかけでカーチス・ルメイ大将の後援を受けることになる[29]。ランドの歴史の中でも中心人物とも言えるのが、このルメイだ。彼はランドの発展において重要な役割を果たし、自分の考え方と世界に対するアプローチをこの組織に吹き込んだ。ルメイを現代の目で見ると、冷戦時代の典型的な将軍のパロディのように見える。彼はぶっきらぼうで、「決して降伏しない」という姿勢を貫き、葉巻を咥えながら部下に詰め寄った[30]。しかし自ら作り上げたこうしたイメージの裏側には、冷酷な判断を下す人物がいた。第２次世界大戦中、ルメイは１９４５年３月10日の東京大空襲をはじめとする、日本への爆撃作戦を指揮した。ルメイは、３２５機のＢ－29スーパーフォートレスに搭載されていた防御のための機銃を撤去して、ナパーム弾などの弾薬類をより多く搭載するよう命じ、合計約２０００トンの爆弾を東京に投下した。東京大空襲では10万人近くの民間人が犠牲になったが、同じくルメイが指揮した日本への大規模な爆撃作戦では、その５倍の犠牲者が出たと推定されている。

ルメイの「敵に情けをかけない」という姿勢は、生涯を通じて一貫していた。冷戦時代、彼はソ連への大規模な先制攻撃を主張した。彼の計画は、米国が保有するすべての核兵器をソ連の70都市に投下するというもので、彼はそれを「サンデー・パンチ」と呼んだ[31]。映画監督のスタンリー・キューブリックは、後に映画『博士の異常な愛情』の中で、ルメイをモデルとして狂気に満ちた空軍大将を描いたが、同作品には「ブランド研究所」という組織も登場する[32]。ルメイは「他のすべての考慮すべき点を犠牲にして、勝利という実際的な目標だけに焦点を当てた」と非難された際、「すべての戦争は

不道徳だ。それを気にしていては、良い兵士にはなれない」と言い、後悔するそぶりを見せなかった[33]。ルメイは戦争を合理的で、科学的に解決すべき問題と考えていたのだ。爆弾をたくさん落とせば落とすほど、敵を倒せる確率は高くなる。敵を一掃する核による先制攻撃は、敵に反撃の機会を与えないという点で合理的な判断であった。感情を極限まで排した、分析的な考え方だ。この哲学は、その後数十年にわたり、ルメイが支配するランド研究所の研究に浸透していくことになる。ランドのアナリストで、後にノーベル経済学賞を受賞するトーマス・シェリングは、著書『軍備と影響力』（斎藤剛訳、勁草書房、２０１８年）の中で、戦争に勝つには交渉力が必要であり、交渉力は「相手に危害を加える能力から生まれる」と記している[34]。

ランドのアナリストたちは、抽象的な理論と、彼らが「最大かつ最も困難な問題」であると見なすものに惹かれていた。彼らは自分たちが立案・提唱した政策やその副作用に対して、倫理観を差し挟まないアプローチを取った[35]。ランド研究所は、米軍の最も差し迫った課題に取り組むために、数字に基づくテクノクラシー的なアプローチを採用したのだ。その中で、彼らはまったく新しい分析手法を生み出した。

２人のプレイヤーが互いに競い合う単純なゲームは、より複雑な紛争、さらには国家間の核戦争のモデルにもなり得る。このようなゲームを数学的に研究することを「ゲーム理論」といい、この分野で著名な人物の多くが、ランドで勤務した経歴を持つ[36]。ランドのアナリストは、ゲーム理論を用いて米ソの核対立をモデル化し、そのモデルを使ってゲームの最善の手を予測しようとしていたのである[37]。

ランド研究所は、ゲーム理論を土台として、独自に新しい手法を開発した。１９４７年にエドウィ

ン・パクソンが考案した「システム分析」は、問題を構成要素に分解するものだ[38]。そして、それぞれの要素を分析し、得られた分析結果をまとめてハイレベルな結論を導き出す。これは米軍のように、多くの変動要素と、多くの未解決問題を持つ複雑なシステムについて意思決定を行う必要のある組織にとって、有用なツールだった。たとえばカーチス・ルメイ大将に近いテーマとして、戦略爆撃の問題がある。敵に対して爆撃機の編隊を展開する際に、最も効果的な方法は何か？　爆撃機をどのくらいの高度で飛行させれば、投下される爆弾による被害を最大にし、かつ撃墜される味方機の数を最小にすることができるか？　そのような爆撃作戦を実行するために必要なロジスティクス活動のコストはどの程度か？　システム分析は、このような質問に答えられるように設計されている[39]。

システム分析には多くの困難な数学的作業が求められるため、それを実行するコンピュータが必要となった。１９５０年当時、ランドのアナリストはＩＢＭが設計した初期のコンピュータ２台を使っていたが、もっと大きな計算能力が必要だと判断した[40]。彼らは最新の技術を調査するために、いくつかのコンピュータメーカーを訪問した。その中にはＩＢＭやエッカート・モークリー・コンピュータが含まれていたが、ランド研究所は彼らの仕事は「気まぐれすぎる」もので、先進性に欠けると判断し、自分たちでコンピュータを開発することに決めた[41]。

彼らが作ったマシンは「ＪＯＨＮＮＩＡＣ」と名付けられ、１９５３年に運用が開始された[42]。ランド研究所は、中途半端なことはしなかった――ほんの数年で、ＪＯＨＮＮＩＡＣは世界で最も洗練されたコンピュータの１つとなったのだ[43]。ＪＯＨＮＮＩＡＣは複数のユーザーのサポート、回転ドラム式プリンターと世界最大のコアメモリの装備、数百時間にも達するとされた稼働時間など、数々の

「世界初」を成し遂げた[44]。ＥＮＩＡＣが稼働５～６時間ごとにリセットしなければならないことを考えると、これは大変な偉業だった[45]。ＪＯＨＮＮＩＡＣに導入されたイノベーションの１つが、機械を冷やすための強力な空調システムである。メンテナンスのために機械を開けると、冷気がオペレーターのいる作業室に流れ込んでしまい、スキージャケットを着用しなければならないほどだった。そのためＪＯＨＮＮＩＡＣの愛称の１つは、「ニューモニアック」（肺炎を意味する形容詞「ニューモニク」をもじったもの）だった[46]。

システム分析やＪＯＨＮＮＩＡＣの開発も大きな成果だったが、ランド研究所がよく知られるようになった最大の理由は、米軍が現在でも一部を機密扱いにしているほど影響力の強い研究成果だ[47]。１９５０年代、ランドのアナリストのケネス・アローは、「人は合理的な自己利益のために行動する」という仮定に基づく理論を考案した[48]。人は自分が欲しいものを最大に、欲しくないものを最小にする選択をする、という直感的な仮定だ。アローが目指したのは、ソ連の指導者たちの意思決定を予測できるような数理モデルを構築することだった。米政府は、国際的な出来事や戦争におけるソ連の行動を予測できるようにしたいと考えていた。彼らは、ソ連が近隣のどの国に侵攻するか、あるいは紛争時にどのような行動を取るかといった問題に答えようとしていたのである[49]。アローの研究以前には、ソ連政府の決定を予測することは基本的にできなかった。「ソビエト学者」と呼ばれた人々でさえ、クレムリンが公開したプロパガンダ写真の中で、それぞれの役人がどれだけスターリンの近くに写っているかを分析することで、どの役人が有力者なのかを推測する程度だった[50]。

システム分析やゲーム理論など、ランド研究所が開発・導入した分析手法は非常に成功したと考えられていた。それは問題に対して、数字に基づくアプローチを可能にした。世界の混沌とした複雑さを、数学的モデルや方程式のような、扱いやすいものに還元したのである。世界の理解と未来の予測を可能にするようなこの手法は、核戦争すら起こりうる状況に直面するアナリストや米軍幹部にとって、心強いものだった。その魅力に惹かれたランドは、その後何十年にもわたって、社会計画や医療、教育政策など、他の複雑な問題領域を研究する際にもこのアプローチを用いることになる[51]。

１９５０年代の終わりから60年代の初めにかけて、タイムシェアリング型コンピュータの数が増加し、計算能力の爆発的な増加が予想される中、ランドのアナリストたちは情報セキュリティの問題を研究し始めた[52]。彼らは核戦争研究で培った分析的洞察力と合理的アプローチを、この分野に持ち込んだ。彼らの取り組みは、現代における情報セキュリティ研究の幕開けを告げることとなった。