サイバーリザーブ（予備役）の研究

― エストニア　サイバーディフェンスユニットと IT 職種で採用された予備自衛官の意識の比較を通じて ―

日髙　智雄
井手　達夫

はじめに

有事において、サイバー領域で戦うのは正規の軍人だけではない。2007 年のエストニア、2008 年のグルジア、また 2014 年のクリミア・ウクライナでも国家の意図を体して、あるいは自発的に多くの民間人等がサイバー領域での戦いに参加した[1]。

そのため、各国とも軍隊内だけでなく外部にもリザーブ等の形で、有事に備えた人材を確保しようとしている。英国でも、数百人規模のコンピュータのエキスパートをサイバーディフェンスの最前線で勤務するリザーブとして採用し[2]、中国ではサイバー民兵の数は 1,000 万人を超えている[3]。他方日本では自衛隊内のサイバー人材も少ない上にリザーブそのものが国家の規模に比して少数であり、議論の俎上に上ることも多くはない[4]。しか

[1] 廣瀬陽子「ロシアが展開するハイブリッド戦争の脅威」現代ビジネス、2019 年 7 月 8 日、https://gendai.ismedia.jp/articles/-/65415?page=2。
[2] 防衛省『平成 28 年版　防衛白書』2016 年、158 頁。
[3] Nigel Inkster "*China Cyber Power* (Routledge, 2016)," p. 104. Nigel Inkster は英国 MI6 元副長官。
[4] 平成 30 年度第 196 回国会では「諸外国のサイバー関連部隊について、米国は六千二百人規模、北朝鮮は約六千八百人、中国に至っては十三万人規模などの情報がある中で、日本の約四百三十人というのはあまりに手薄」との指摘がなされている。日本郷友連盟「新防衛大綱策定への提言　－新「防衛計画の大綱」はどう描くべきか？－」2008 年 12 月 23 日、http://www.ssri-j.com/SSRC/ssrc/20-proposal2008.12.23.html。この中では「中国は現役約 220 万人に対して予備役約 80 万人、人民武装警察約 150 万人、民兵（基幹民兵のみで）約 1,000 万人、併せて千数百万人以上（現役比率 560%以上）、北朝鮮は現役約 110 万人に対して約 470 万人（同 420%）、韓国は現役約 69 万人に対して約 450 万人（同 652%）、台湾は現役約 29 万人に対して約 165.7 万人（同 571%）の予備役をそれぞれ保有しているのに対し、わが国は、陸海空自衛官総計約 24 万人に対して予備自衛官、即応予備自衛官および予備自衛官補を合わせて約 4.4 万人に過ぎず、規模的には現役比率にして 20%に満たない予備要員の備えしかない。」とされている。

しながら他国がリザーブも含めて充実させている以上、その動向にも関心を払う必要がある。

では、なぜサイバーリザーブの構成員はそれに志願するのか。またその効果的な運用にはどのような考慮が必要か。本研究では世界初の国家に対するサイバー攻撃を受けた[5]という教訓から、先進的な取り組みを行っているエストニアのサイバーリザーブであるサイバーディフェンスユニットを取り上げ、日本の予備自衛官において IT 職種で採用された者との意識を比較する中に、それを明らかにしようとするものである。

論述の順序として第 1 節では、エストニアの国情、サイバーディフェンスユニットの役割、それに日本の予備自衛官制度を紹介したのち、第 2 節では、これまでの先行研究を吟味する事と併せて今回行ったアンケート調査の内容を説明し、第 3 節では実施結果を明らかにするとともに、第 4 節でそれに対する考察を行う形で論を進めることとする。

1　研究背景

(1)　エストニアの国情

エストニアは小国ではあるが、先進的な政府 IT システムを導入しており、世界初の国家に対するサイバー攻撃を受けたことから、サイバー防衛への取り組みに関しても熱心に取り組んでいる。

歴史を振り返ると近代以降、エストニアは長らくロシアの支配下にあった。1917 年の帝政ロシアの崩壊に伴い、一時的に独立を果たしたものの、ソ連の成立とともに再びその勢力圏に組み込まれ、ソビエト連邦を構成する共和国の 1 つとなった。第 2 次世界大戦時には、一時的にドイツ勢力下におかれるが、戦後再びソ連の構成国の一部に戻ることになる。この体制は 1991 年まで続き、ソ連の崩壊をもってエストニアは再び独立を果たした[6]。

独立当初、目ぼしい産業も天然資源もなく、森林に覆われ、多くの離島を持つエストニアは、政府の公的サービスを国全体に広めるのに非常に厳しい環境下にあった[7]。そこで当時普及し始めたインターネット技術に目をつけ、情報通信技術に資本を集中させることで問題解決を図ろうとした。2002 年には、eID カードを 15 歳以上の国民へ配布し、2005 年には世界に

[5] 伊東寛『「第 5 の戦場」サイバー戦の脅威』祥伝社、2012 年、142 頁。
[6] 小森宏美『エストニアを知るための 59 章』明石書店、2012 年、111 頁。
[7] 同上、39 頁。

先駆けて地方政府の選挙で初めて自宅からインターネットを介して電子投票を行ったことで世界の注目を集めた[8]。

そうした中、2007 年 4 月にエストニア政府が首都タリンの中心部にある第 2 次世界大戦でのソ連軍の勝利を記念した銅像の移設を決定し、それに対するロシア系住民の反発から街頭で暴動が発生、それを契機にエストニアに対するサイバー攻撃が生起した[9]。世界初の国家に対するサイバー攻撃ともいわれるこの攻撃は、当初政府機関やニュースポータルをターゲットとした比較的単純な DoS 攻撃（Denial of Service：大量のデータを送り、機器の処理能力をマヒさせるもの）だったが、次第に激しさを増し、数日後には重要インフラをも対象とするボットネット（他人の PC に遠隔操作するためのウィルスを送って乗っ取ったもの）を使った非常に高度で大規模の攻撃へと移行していった。攻撃は 3 週間にわたって行われ、あらゆる面で電子化が進んでいたエストニア国民にとって、大きな衝撃を与える結果となった。

一連の事件を受け、エストニアは当時はまだ米国、ドイツ、スウェーデンの 3 か国しか採用していなかった「サイバーセキュリティ戦略[10]」を打ち出し[11]、国家安全保障委員会の下にサイバーセキュリティ審議会が新設され、国家のサイバーインシデントに対応することとした。またエストニア情報センターには情報インフラ保護部門が創設される等、重要な情報インフラのリスク分析と保護対策を実施した。さらに、国家のサイバーセキュリティを高めるより具体的な実行的部門として、準国防組織のエストニア防衛連盟の下部にサイバーディフェンスユニットを編成することとなった[12]。

---

[8] ラウル・アリキヴィ、前田陽二『未来型国家エストニアの挑戦　－電子政府がひらく世界－』インプレス R&D、2017 年、50-53 頁。

[9] 同上、126 頁。

[10] サイバーセキュリティ戦略は、エストニア国防省が 2007 年の大規模サイバー攻撃の被害を受けてから関係各省と協力し、2008 年に「サイバーセキュリティ戦略 2008-2013」を策定した。2011 年にはサイバーセキュリティ政策に関わる権限が国防省から経済通信省に移管され、現行のサイバーセキュリティ戦略としては、経済通信省が出した「サイバーセキュリティ戦略 2014-2017」がある。

[11] Piret Pernik and Emmet Tuohy, “Cyber Space in Estonia: Greater Security, Greater Challenges,”Internatinal Cetre for Defense Studies, August 2013, p. 2.

[12] Ibid., pp. 60-61.

(2) サイバーディフェンスユニットについて

サイバーディフェンスユニットの存在意義は、エストニアの「重要インフラを保護し、広範な国防の目標を支援することによって、エストニアのハイテクな生活を保護すること」にある[13]。

エストニア国防軍は陸海空軍の軍種からなり、平時においてその規模は約 6,000 人であり、その半分は徴兵から成り立ち、有事ではリザーブが動員され、その規模は 60,000 人に増大する[14]。

また国防軍の他に、主に 16,000 人の民間人で構成される[15]国防連盟というボランティアから成る準国防組織が存在する。同組織は「エストニア防衛連盟法」によって、有事においては国防軍の指揮下に入るものと定められ[16]、図 1 に示すとおり、同連盟下には 15 の地域別ユニットとサイバーディフェンスユニットがある[17]。

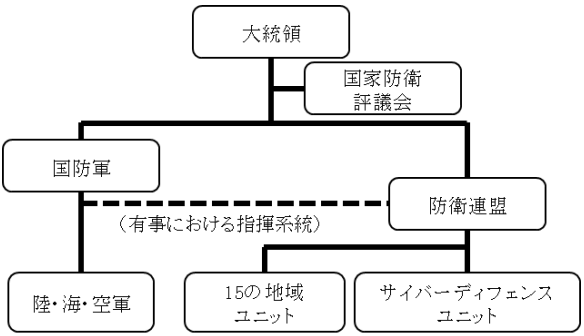


図 1　エストニア国防組織の概要

（出所）山口嘉大「サイバー防衛における官民連携の強化についてーエストニア共和国との比較を通じてー」196 頁を元に筆者作成

サイバーディフェンスユニットでは、以下の 3 つの主要な目標を掲げている[18]。

---

[13] Kaitseliit, “Estonian Defence League’s Cyber Unit,” http://www.kaitseliit.ee/en/cyber-unit?ncid=txtlnkusaolp00000618.

[14] Estonian Defence Forces HP, “Estonian Defence Forces,” http://www.mil.ee/en/defence-forces.

[15] Kaitseliit HP, http://www.kaitseliit.ee/en/edl.

[16] 山口嘉大「サイバー防衛における官民連携の強化について　―エストニア共和国との比較を通じて―」『防衛研究所紀要』第 21 巻第 1 号、2018 年、197 頁。

[17] 同上、196 頁。

[18] Kaitseliit, “Estonian Defence League’s Cyber Unit,” http://www.kaitseliit.ee/en/cyber-unit?ncid=txtlnkusaolp00000618.

・資格認定されたボランティア IT スペシャリスト間の協力関係を強化するとともに、危機発生時に官民の専門知識を融合させるための、ネットワークを構築すること
・定期的に脅威認識とそれに対する処置手順を共有すること、そして危機発生時の準備態勢を強化することにより、重要な情報基盤のセキュリティレベルを上げること
・隊員に対して継続的にサイバーセキュリティ教育・訓練の機会を提供するとともに、国際的なサイバーセキュリティ訓練への積極的な参加を促進すること

これらの目標を達成するために、サイバーディフェンスユニットは以下の 2 つの主要な任務を課している[19]。

・教育と訓練
サイバーディフェンスユニットの目標を達成するために隊員の知識、スキル、経験、サイバーセキュリティに対する意識を向上させること。
・国民のサイバーセキュリティの強化と確保
各種公的及び民間機関のサイバーセキュリティ体制構築支援を行うこと。

その具体的な活動として、以下のような事業を行っている。

・学校のコンピュータのスクリーニング
・電子投票システムのセキュリティ構築・検証支援[20]
・エストニアで開催されているサイバー演習のための準備作業
・軍事演習（Spring Storm[21]、Locked Shield[22]等）への参加

入隊するためには、サイバーセキュリティに関する知識と経験が必要とされ、入隊希望者はすでにサイバーディフェンスユニットで勤務している

[19] Kadri Kaska, Anna-Maria Osula and Jan Stinissen, "The Cyber Defence Unit of the Estonian Defence League - Legal, Policy and Organisational Analysis," *NATO Cooperative Cyber Defence centre of Excellence*, 2013, pp. 22.
[20] Ibid., pp. 22-23.
[21] 山口「サイバー防衛における官民連携の強化について」190 頁。
[22] 2019 年の演習では約 30 か国から、1,200 人以上の専門家が参加している。各国のチームがそれぞれ 2,500 を超えるサイバー攻撃に対応しつつシステムを維持すると同時に、戦略的決定、法的処置、メディアへの対応などの現実に起こった場合の対処を仮想システムの中で実施し、その技量を競い合っている。

隊員の 2 人から身分を保証するために推薦を得る必要があり、当該 2 名の推薦者は、入隊希望者の任務遂行上の適合性について、責任を負うことになっている[23]。

また隊員がサイバーディフェンスユニットの特定の活動に対して参加することは義務ではなく、隊員の自主的な判断により参加することが認められている[24]。

(3) IT 職種で採用された予備自衛官について

日本のリザーブの中で、エストニアのサイバーディフェンスユニット制度に近似するのは予備自衛官補の中の IT 職種で採用された者である。これは情報通信技術（IT）革命や自衛隊の役割の多様化等を受け、自衛官未経験者であっても、その優れた専門技能を有効に活用し得るよう設けられた制度である[25]。

自衛隊のリザーブ制度には、予備自衛官、即応予備自衛官及び予備自衛官補がある。

予備自衛官制度は 1954 年、諸外国と同様に予備の要員が必要[26]とされたことから自衛隊の創設と同じくして発足した。隊員は自衛官として 1 年以上の勤務経験がある者からなり、年間 5 日の訓練を受け、防衛召集命令等が発令された場合、駐屯地警備等の任務が与えられる。その定数は 47,900 名である。

即応予備自衛官は 1997 年、予備自衛官陸上自衛隊の人員削減を補い、予備自衛官より高い即応性を担保するべく発足した。隊員は同じく自衛官として 1 年以上の勤務経験がある者からなり、年間 30 日の訓練を受け、防衛召集命令等が発令された場合、第一線部隊の任務が与えられる。その定数は 8,075 名である。

予備自衛官補は 2001 年、将来的に予備自衛官数を確保するとともに民間の専門技能の活用を図るため発足した。隊員は自衛官としての経験がなくても任命され、後方地域警備等に従事する「一般」と各種技能を通じて従事する「技能」に分かれ、前者は試験、後者は選考により採用される。各種技能には衛生、語学、整備、情報処理、通信、電気、建設、放射線管

---

23 山口「サイバー防衛における官民連携の強化について」199 頁。
24 Kaska, Osula, Stinissen, “The Cyber Defence Unit of the Estonian Defence League,” p. 18.
25 「予備自衛官補」防衛省、
https://www.mod.go.jp/gsdf/reserve/yobijiho/index.html。
26 防衛省「平成 16 年版　防衛白書」2014 年、308 頁。

理、法務、船舶がある。「一般」は 3 年以内に 50 日、「技能」は 2 年以内に 10 日の教育訓練を修了すれば、予備自衛官に任用される。その定数は 4,621 名である[27]。

このうち情報処理の枠組みで採用されるのに必要な資格は、国内で行われている経済産業省の認定する情報処理技術者資格であり、国外で著名な CompTIA、(ISC)[2] 等の IT 資格である[28]。

また平時において求められるのは、予備自衛官に任用されたのち職種訓練を含む基本教練や射撃検定、制度教育等[29]の 5 日間（場合によっては 2 回に分けることも可）の訓練を受けることである。

2　研究方法

(1)　先行研究

国外ではパダー（Andrus Padar）が、エストニアの国情やサイバーディフェンスユニットの活動を言及し、成功の要訣は技術と人に投資し、それを柔軟性を失わない範囲で法的枠組みの中に組み入れることとしている[30]。カスカ（Kadri Kaska）他の研究は、エストニア国防省が NATO サイバー防衛研究所に委託し、サイバーディフェンスユニットをモデルとして他の同様な活動を支援するため行われたもので、サイバーディフェンスでボランティアを使用する法律等の、制度的側面等について議論している[31]。ルイツ（Monica Ruiz）は、歴史を振り返り米国にもボランティアが国防の任に当たったことに言及しながら、米国との比較の中でエストニアのサイバーディフェンスユニットを取り上げ、サイバーディフェンスに求められ

---

27 「予備自衛官制度の概要」防衛省、https://www.mod.go.jp/gsdf/reserve/yobiji/index.html ; 防衛省『令和元年版　防衛白書』防衛省、2019 年、534 頁。各種予備自衛官の定数は 2019 年 3 月 31 日現在。

28 「予備自衛官補採用案内（技能公募）」防衛省、https://www.mod.go.jp/gsdf/jieikanbosyu/pdf/y/31yobihoginouy.pdf。

29 「予備自衛官の訓練」防衛省、https://www.mod.go.jp/gsdf/reserve/yobiji/training.html。

30 Andrus Pader “Cyberspace Defence: The Estonian Kaitseliit Model,” *NATO Science for Peace and Security Series E-Human and Societal Dynamics,* Vol. 141, February 2019, pp. 159-167.　Pader はサイバーディフェンスユニット隊長。

31 Kaska, Osula, Stinissen, “The Cyber Defence Unit of the Estonian Defence League.”

ている社会全体の取組としてそれを米国としても検討する価値があるものとしている[32]。

国内では、佐藤が米国のサイバー予備構成部隊を取り上げ、自衛隊において高い技術力と専門性を有したサイバー攻撃対処要員を長期にわたり確保することは困難であることなどから、米国をモデルとした予備自衛官制度の有効活用と制度設計」について議論している[33]。また山口は日本とエストニアの比較の中で、サイバーリザーブの有用性を指摘し、サイバーディフェンスユニット制度の有効部分の導入には政府主導によるボランティア組織の設立を推進するとともに、既にある予備自衛官等の制度を活用して、民間のエキスパートが国防に関与できる枠組みを構築するのが適当としている[34]。

しかしながらそのいずれもサイバーリザーブ等の制度等に関して議論するもので、アンケートを通じて個々の構成員の所見等から最良慣行等を導き出すような議論は見当たらなかった。

(2) 研究手法

本研究の研究課題は、「なぜサイバーリザーブの構成員はそれに志願するのか。またその効果的な運用にはどのような考慮が必要か。」を実際の構成員の所見を通じて明らかにすることである。そのため関係者に対してアンケートを送り、回答を得ることとした。

研究対象としたのは、エストニアのサイバーディフェンスユニットの構成員 19 名と、日本の予備自衛官の中で情報処理技術によって採用された者 12 名である[35]。

回答時期は、2019 年 8 月から 9 月にかけてであった。

質問の内容は以下のとおりである。

---

[32] Monica M. Ruiz " Establishing volunteer US cyber defense units: A Holistic Approach," *The Cyber Defense Review,* Vol. 4 No. 1, 2017, pp. 45-58.

[33] 佐藤智美「サイバー人材不足の解決策に関する一考察～米国のサイバー予備構成部隊（ＲＣ）をモデルとした提言～」『情報セキュリティに関する懸賞論文受賞作品』防衛基盤整備協会、2015 年、39-52 頁。

[34] 山口「サイバー防衛における官民連携の強化について」161-209 頁。

[35] 本来であれば無作為抽出の多数の標本を選ぶべきであるが、関係者の協力を得てそのコミュニティに回答を依頼した。

（回答者の背景）

Q1：あなたの年齢はおいくつですか？

（選択肢）～19 歳／20～29 歳／30～39 歳／40～49 歳／50～59 歳／60 歳～

Q2：あなたの性別はどちらですか？

（選択肢）男性／女性

（回答者の入隊前の状況）

Q3：予備役[36]になった理由はなんですか？（複数回答可）

（選択肢）国防のため／社会への貢献／社会的な評価があるから／会社が勧めるから／家族（親戚）が参加しているから／自身のスキル向上のため／その他

Q3-1：「自身のスキル向上のため」と答えた方に尋ねます。あなたはどういったスキルの向上を考えていますか？（記述）

Q3-2：「その他」と回答した方に尋ねます。あなたはどういった目的で予備役になったのですか？（記述）

Q4：予備役になる前に不安はありましたか？

（選択肢）はい／いいえ

Q4-1：「はい」と答えた方にお伺いします。その不安はどういったものでたか？（記述）

（回答者の活動現況）

Q5：予備役としての活動頻度はどれくらいですか？

（選択肢）週に 3 回以上／週に 1 回以上／月に 1 回以上／3 か月に 1 回以上／半年に 1 回以上

Q6：1 度の活動時間は平均するとどれくらいになりますか？

（選択肢）1 時間未満／1～2 時間／2～3 時間／3 時間以上

（回答者の入隊後の所感）

Q7：あなたは予備役としての活動に満足していますか？

（選択肢）はい／いいえ／どちらともいえない

[36] 本論の中で予備役を「リザーブ」の語で揃えようと考えたが、アンケートに関しては実施時に使用したとおり「予備役」の語を用いた。

Q7-1：「はい」と回答した方にお伺いします。満足できた理由はなんですか？（記述）

Q7-2：「いいえ」と回答した方にお伺いします。満足できない理由はなんですか？（記述）

3　研究結果

アンケートを集計し、以下の結果を得た。

（1）（回答者の背景）

Q1：あなたの年齢はおいくつですか？

年齢層は、図 2 のとおり、サイバーディフェンスユニットでは 30 代を中心に、20 代から 50 代まで多くの世代を含んでいるのに対し、予備自衛官は 20 代が 8%（1 名）いるほか、すべて 40 代であった。

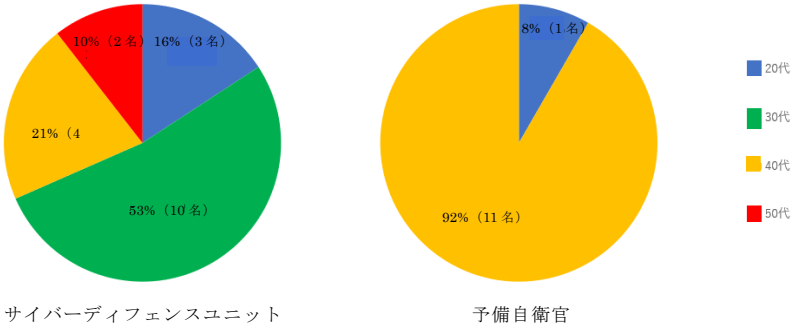


図 2　構成員の年齢

（出所）筆者作成

Q2：あなたの性別はどちらですか？

性別は、図 3 のとおり、サイバーディフェンスユニットには女性隊員も 11%（2 名）存在していたのに対し、予備自衛官では 100%（12 名）男性であった。

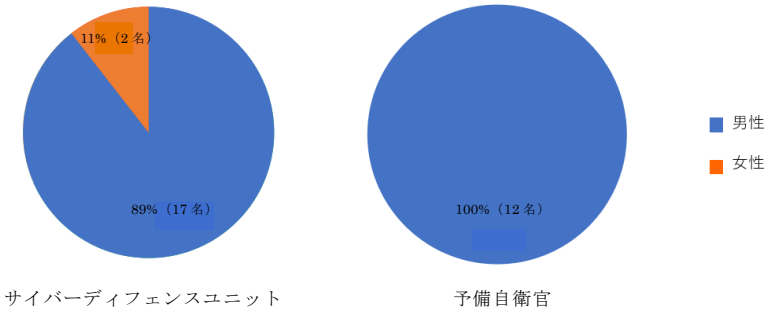


図 3　構成員の性別

（出所）筆者作成

（2）回答者の入隊前の状況

Q3：予備役になった理由はなんですか？（複数回答可）

予備役への志望理由は、図 4 のとおり、サイバーディフェンスユニットでは第 1 位に「国防のため」（17 名）、次いでそれとほぼ同数の「自身のスキル向上のため」（16 名）を挙げているのに対し、予備自衛官で第 1 位は同じく「国防のため」であるが、第 2 位には突出したものは特になかった。

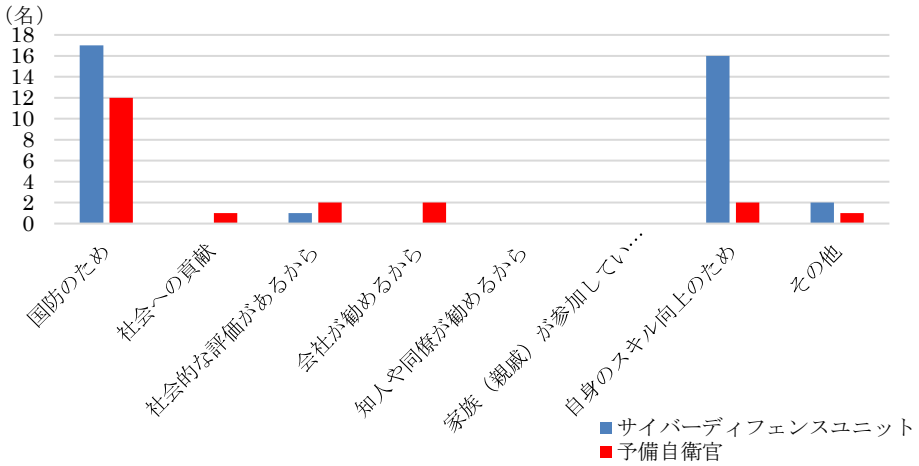


図 4　予備役への志望理由

（出所）筆者作成

Q3-1：「自身のスキル向上のため」と答えた方に尋ねます。あなたはどういったスキルの向上を考えていますか？

スキルの向上についての具体的な内容に関しては、サイバーディフェンスユニットでは以下のような記述があった。

・セキュリティソリューションに関する技術（12 名）
・軍に関するスキル（2 名）
・組織や法に関する技術
・チームワーク
・重要インフラなしで生き残る技術

これに対し予備自衛官では以下のような記述があった。

・業務でつけているサイバーセキュリティの知見に、国防の観点を加えスキルの幅を広げたい。
・予備役一般が取得すべきスキル

Q3-2：「その他」と回答した方に尋ねます。あなたはどういった目的で予備役になったのですか？

志望理由の「その他」に関しては、サイバーディフェンスユニットでは以下のような記述があった。

・サイバー攻撃から国家を守ることに関心のある IT エキスパート同士のコミュニティを作りたい。
・他の人々の成長を促したい。

これに対し予備自衛官では以下のような記述があった。

・自衛隊の現状と国および周辺との関係性の現実を知るため。

Q4：予備役になる前に不安はありましたか？

図 5 のとおり、サイバーディフェンスユニットでは 5%（1 名）の者だけが入隊前に不安を感じていたのに対し、予備自衛官では 67%（8 名）の者が不安を感じたと答えた。

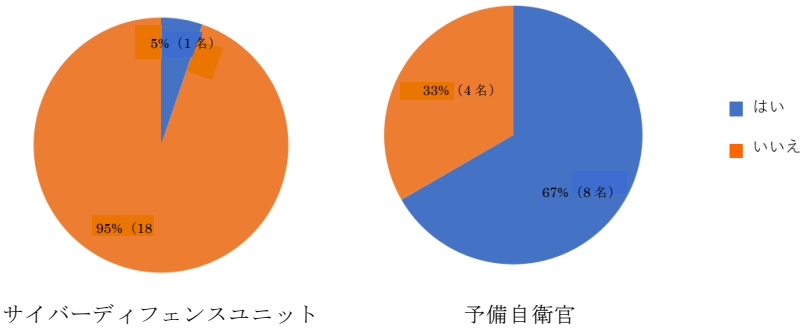


図 5　予備役入隊前の不安の有無

（出所）筆者作成

Q4-1：「はい」と答えた方にお伺いします。その不安はどういったものでしたか？

不安の具体的な内容に関しては、サイバーディフェンスユニットでは以下のような記述があった。

・新たな人に出会うこと

これに対し予備自衛官では以下のような記述があった。

・訓練参加の時間の確保（2 名）、
・体力的な不安（2 名）
・サイバーセキュリティに関連する訓練や招集の可能性が小さい点
・周囲の理解が得られるか。

（回答者の活動現況）

Q5：予備役としての活動頻度はどれくらいですか？

活動頻度は、図 6 のとおり、サイバーディフェンスユニットでは 3 か月に 1 回以上のところが大半であるのに対し、予備自衛官では全員半年に 1 回以上のところに回答があった。

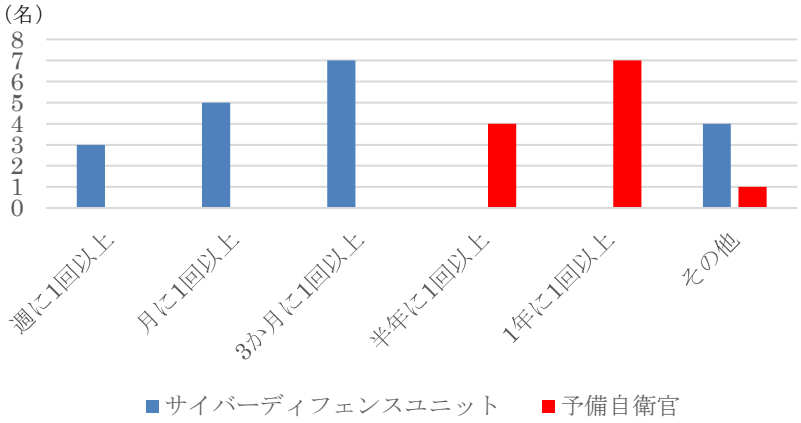


図 6　活動の頻度

（出所：筆者作成）

Q6：１度の活動時間は平均するとどれくらいになりますか？

活動時間の平均（1 回あたり）は、図 7 のとおり、サイバーディフェンスユニットでは大半が 3 時間以下であるのに対し、予備自衛官では全員が 3 時間以上であった。

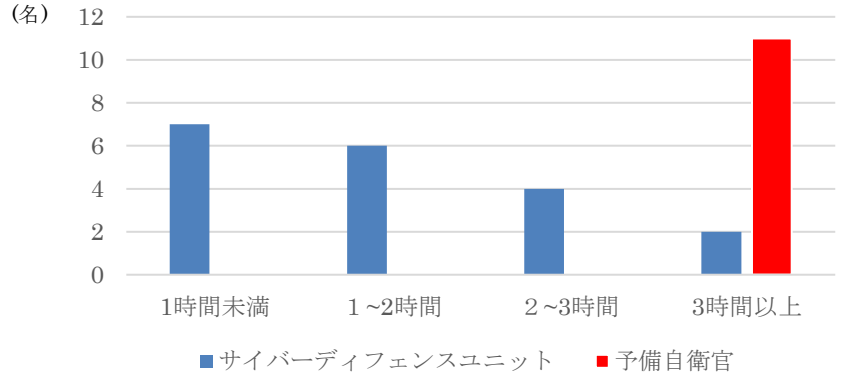


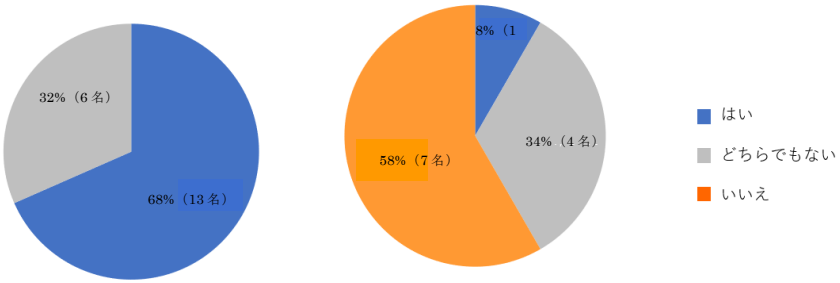
図 7　活動時間の平均（1 回あたり）

（出所）筆者作成

（回答者の入隊後の所感）

Q7：あなたは予備役としての活動に満足していますか？

予備役としての満足度は、図 8 のとおり、サイバーディフェンスユニットでは「はい」という肯定的な回答が 68%（13 名）であるのに対し、予備自衛官では「いいえ」という否定的な回答が 58%（7 名）であった。



サイバーディフェンスユニット　　予備自衛官

図 8　予備役としての満足度

（出所）筆者作成

Q7-1：「はい」と回答した方にお伺いします。満足できた理由はなんですか？

満足できた具体的な理由に関しては、サイバーディフェンスユニットでは以下のような記述があった。

・新たな知識・技術が得られるから。（4 名）
・国の安全保障に貢献できるから。（2 名）
・時間に関して柔軟であり、多くの活動に参加できるから。
・イベントが多くあるから。
・メンバーが素晴らしいから。

これに対し予備自衛官では以下のような記述があった。

・国防の一端を国民として担うことができているという実感があること。
・自身の技能を活かし、国防に寄与できている。
・コミュニティや知識の幅が広がったから。

Q7-2：「いいえ」と回答した方にお伺いします。満足できない理由はなんですか？

満足できなかった具体的な理由に関しては、サイバーディフェンスユニットでは以下のような記述があった。

・人々からより多くを得るには、より集中的なトレーニングが必要である。

これに対し予備自衛官では以下のような記述があった。

・サイバーセキュリティの専門知識を活かせる訓練をしたい。（4 名）
・実際の運用に向けた訓練を受けられない。（2 名）
・日本における予備の使用計画、育成・維持計画が不十分でありその点が改善されないこと。（2 名）

4　分析・考察

以上の結果から、研究課題に対し、以下の分析・考察を行った。

(1) なぜサイバーリザーブの構成員はそれに志願するのか

国防への強い関心とともに、スキルの向上が見込めるとき、エキスパートは志願を検討するものと考えられる。

入隊前の予備役への志望理由（Q3）に対し、サイバーディフェンスユニット隊員の多くは「国防のため」の次に「自身のスキル向上のため」と答え、その具体的な内容は多くが「セキュリティソリューションに関する技術（12 名）」としている。また入隊後の予備役としての満足度（Q7）についてもその満足とする理由（Q7-1）についてサイバーディフェンスユニット隊員は「国の安全保障に貢献できるから。」（2 名）と併せて「新たな知識・技術が得られるから。」（4 名）としている。

これらはサイバーディフェンスユニットにおいてその 3 つの主要な目標の中に「隊員に対して継続的にサイバーセキュリティ教育・訓練の機会を提供するとともに、国際的なサイバーセキュリティ訓練への積極的な参加を促進すること」が掲げられ、主要な任務の一つに「サイバーディフェンスユニットの目標を達成するために隊員の知識、スキル、経験、サイバーセキュリティに対する意識を向上させること。」と示され、実際 Spring Storm、Locked Shield 等の国際的な軍事演習にも参加させていることの成果と言える。

一方、予備自衛官では、予備役入隊前の不安の理由（Q4-1）として「サイバーセキュリティに関連する訓練や招集の可能性が小さい点」が挙げられ、予備役としての満足できない理由（Q7-2）に「サイバーセキュリティの専門知識を活かせる訓練をしたい。」（4 名）、「実際の運用に向けた訓練を受けられない。」（2 名）とあり、改善の余地があるものと考えられる。

(2) サイバーリザーブの効果的な運用にはどのような考慮が必要か

高度な技量を持つ志願者の能力を活用するためには、民間において多忙な彼らの参加を促すために、多くのオプションを与えて訓練時間に対する柔軟性を確保とするとともに、エキスパートの連携を可能とする彼等を中心としたコミュニティを育む配慮が求められると考えられる。

先述のようにサイバーディフェンスユニット隊員の参加は義務ではなく、自主的な判断に任せられており、1 回あたりの教育訓練の時間は短く（Q5）、頻度は高い（Q6）。満足とする理由（Q7-1）に「イベントが多くあるから。」とあるように教育訓練の機会が数多く設けられ、「時間に関して柔軟であり、多くの活動に参加できるから。」とあるように、そのよう

な数多くのイベントを柔軟に選択しながら活動できることが満足度を向上させている。

また頻繁な接触機会は、コミュニティ構築を促すものである。予備役への志望理由に関する具体的な内容（Q3-1・2）に「チームワーク（のスキルを向上させたい）」、「サイバー攻撃から国家を守ることに関心のある IT エキスパート同士のコミュニティを作りたい。」とあることから、エキスパートである彼等もまたそれを重要と認識しているものと考えられる。満足である理由に「メンバーが素晴らしいから。」（Q7-1）とあるのは、高い技量を持った者同士が相互にその技量を認め合う環境を構築することが満足度を向上させ、それはまたコミュニティの持続的な運営を可能とするものであることと推察する。

一方予備自衛官では、予備役入隊前の不安（Q4-1）として「訓練参加の時間の確保」が挙げられるように、年 5 日（場合によっては 2 回に分けることも可）の集中した訓練のため平均活動時間（Q6）は長く、また活動頻度（Q5）も最大年 2 回でしかなく、柔軟な参加やコミュニティ構築の配慮は必ずしも十分ではない。

そもそも、IT 職種で採用された予備自衛官は、既存の有事における駐屯地警備、後方地域の任務での活躍を期待されている予備自衛官制度を基に制度設計されており、先述のように 5 日間の訓練の内、職種訓練は 1 日しかなく、他は基本教練や射撃検定、制度教育等、既存の組織に馴染ませることに主眼が置かれたもののように見受けられる。その発想が新たな領域での活動に適切なものか否か、検討の余地があるものと考えられる。

おわりに

本論は「なぜサイバーリザーブの構成員はそれに志願するのか。その効果的な運用にはどのような考慮が必要か」を明らかにするため、第 1 節では、研究背景としてエストニアの歴史的背景等を明らかにしたのち、そのサイバーディフェンスユニット及び IT 職種で採用された予備自衛官について、それぞれの位置付け、目的、活動等を紹介した。第 2 節では、研究方法として先行研究を吟味した上で、今回の調査状況とアンケートの質問内容を説明した。第 3 節では、調査結果として、質問に対する回答の集計結果を提示した後、第 4 節では、それを分析・考察し、「なぜサイバーリザーブの構成員は志願するのか」という課題に対しては、高い国防意識と併せて所属することで高い技術が得られるからであり、また「サイバーリザ

ーブの効果的な運用にはどのような考慮が必要か」という課題に対しては、訓練時間に対する柔軟性の確保と、エキスパートの連携に対する配慮が必要とした。

調査したアンケート結果に関しては、標本数が共に 2 桁と少なく、必ずしも全体の所見を反映していない可能性も否定できないが、防衛分野の研究の常として、組織としてではなく、研究者の私的な研究として実施できることは限られていることを理解いただければと考える。

また結果としてエストニアのサイバーディフェンスユニットと、日本の中でそれに一番近似した IT 職種で採用された予備自衛官の者と比較し、後者に低い評価を与えることとなった。しかし後者にはサイバーセキュリティに関心の高い者もいる一方で、他の分野で任用された者もおり、セキュリティ専任の制度であるわけではない中で、それも致し方のない面もあることと考える。

冒頭に述べたようにこれからの紛争は、民間／防衛、平時／有事等の境界が明確でないハイブリッド戦となる。それを助長しているのは、デュアルユーステクノロジーであり、また今日の社会全体を支えるサイバー関連技術であり、そのため各国とも産官学それに軍が連携してサイバー能力の増強を図っている。他方日本の自衛隊では予備役入隊前の不安の理由（Q4-1）に「周囲の理解が得られるか」が挙げられているように、国内に自衛隊に対する忌避感がまだ根強くあり、社会に十分溶け込んでいない。また自衛隊は隊内のネットワークに責任を負っても、重要インフラ等の防護は一義的に金融庁、総務省、厚生労働省等の各所掌官庁の所管であり、さらに国家公務員の数は減らすことが求められても、増やすのは困難である。

民間／防衛、平時／有事に柔軟に対応できる高度な技術を有するサイバーリザーブは、いまだ備えが十分でない日本におけるこれらの問題の解決の一助となるものである。自衛隊に忌避感があるのであれば、平時にはセキュリティクリアランスを確認の上、内閣サイバーセキュリティセンターの所属として活動し、有事には海上保安庁のように自衛隊と行動を共にすることなども考えられてよい。いずれにせよ少ないリソースを、どう補強していくかは緊喫の課題である。そのような中、本研究が、日本におけるサイバーリザーブ制度充実の資となれば幸いである。