東戸塚9条の会NEWS

2024.9.5 No.227
発行：東戸塚9条の会事務局
☎045-823-9211(伊藤)
peace@higashitotsuka9.org

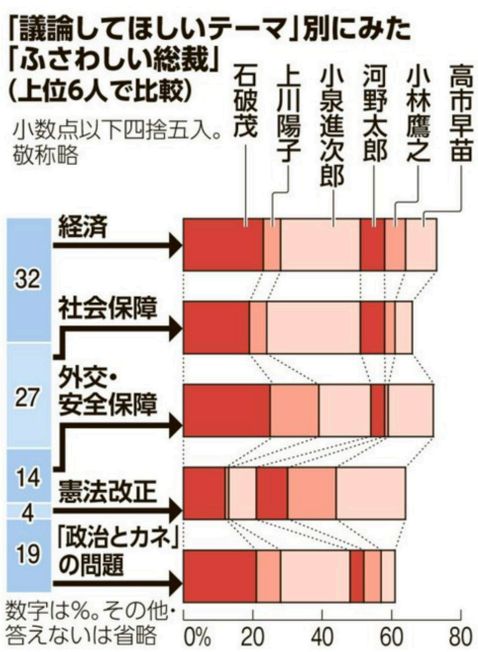
岸田首相　総裁選不出馬を表明

総裁選　「憲法改正」を政治利用するな!

岸田文雄首相は、9 月の総裁任期満了までに憲法改正を目指すと繰り返して述べていました。しかし、自民党派閥の政治資金パーティー裏金問題で追い詰められ、8 月 14 日、記者会見を開き、自民党総裁選への立候補を見送る意向を明らかにしました。

憲法改正について、自衛隊の明記と緊急事態条項については「条文の形で詰め、初の発議までつなげていく」、「今月末までにこの論点整理をするよう指示し、着実に実行していく」と語り、「私の政治人生、そして政治生命をかけて、一兵卒として引き続きこうした課題に取り組んでまいります」と述べました。

いち早く総裁選に立候補を表明した小林鷹之前経済安保相は、憲法改正について「先送りできない課題であり、最大限の熱量で取り組む」とし、他の候補たちも精力的に改憲への意欲を発信しています。



朝日新聞社の世論調査（8/24、25）で、自民党総裁選で一番議論してほしいテーマでは「経済」が 32% と最も多く、「憲法改正」は 4% と最も低い結果が出ています。

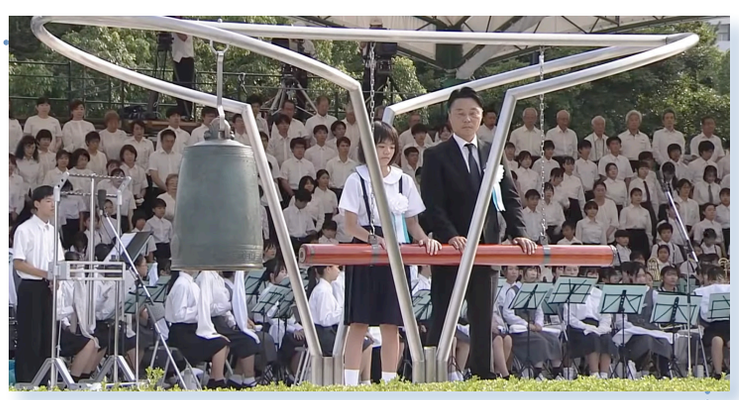
保守層の支持を集めるための「改憲」論議や、総裁選を利用して「改憲」をアピールする等のように、「憲法改正」が政治利用されていないか、自民党総裁選を厳しく見ていく必要があります。

被爆７９年の「原爆の日」の平和記念式典

イスラエル不招待で政治問題化

米国による原爆投下から 79 年目の「原爆の日」を迎え、広島と長崎では、それぞれ 8 月 6 日と 9 日に、平和記念式典が開かれました。

長崎では式典にイスラエルを招待しませんでした。それに反発した米英など主要 6 カ国と EU の大使級が式典への不参加を決めました。「イスラエルをロシアなどと同列に扱うのは誤解を招く」との理由ですが、違和感があります。


鐘を打つ子ども代表と遺族代表(広島)

一方、広島ではイスラエルを式典に招待し、ロシアやベラルーシ代表は招待しない対応をとりました。

①「原爆の実相に触れ、平和を祈る場として、希望する全ての国・地域を招待する、②「国際法への明白な違反行為や核威嚇を行う国は、式典招待から除外する――という 2 つの対応が考えられます。

広島県被団協は「式典にあらゆる国を招待すべきだ」と表明。イスラエルの招待は、ジェノサイドの容認になると批判する市民団体もあります。ウクライナとガザの戦争に対する立場や対応により、平和記念式典が政治問題化されました。

東戸塚9条の会 勉強会
9月14日(土)10:00～12:00
東戸塚地区センター
参加費無料・事前申込不要

9の日宣伝
9月9日(月)17:00～18:00
JR東戸塚駅改札口付近
ビラまき･アピールなど

平和川柳「歴史を学び未来の糧に」
■ 学説の 虐殺スルー 都知事どの
● 不出馬は 総選挙向け 奇襲策
▼ 原発を 止めず地震の 注意報

東戸塚9条の会HP

通信の秘密を脅かし、市民監視を強化する恐れ

能動的サイバー防御（ACD）

2022年12月に閣議決定された安保関連3文書に書き込まれ、今年6月に始まった「能動的サイバー防御」に関する有識者会議が8月6日、「これまでの議論の中間整理」を公表しました。

通信情報を国に提供する「能動的サイバー防御」

「能動的サイバー防御（ACD）」とは、発電所や公共交通機関など国が重要インフラと位置づける施設や政府機関への他国によるサイバー攻撃を防ぐため、平時からインターネット空間を監視し、サイバー攻撃を受ける前に相手側サーバーへの侵入・無力化などで対抗する措置です。

その導入のため、政府は通信事業者からインターネット上の通信情報の提供を可能とする新法を制定する方向です。今秋の臨時国会への新法提出を想定しています。

憲法21条が保障する通信の秘密は守られるのか

能動的サイバー防御のためには、平時からサイバー空間を監視し、不審な通信、システムやネットワークへの侵入を探知する必要があります。政府によるネットワークへの侵入は市民監視やプライバシー侵害につながる危険があり、「通信の秘密」の保護を定めた憲法21条との整合性をいかに確保するのかが問われます。

政府が召集した有識者会議による論点整理では、「公共の福祉のためには通信の秘密も一定の制限を受ける」としただけで、具体的にどのような場合に適用するかは明らかでありません。収集した情報の目的外使用や漏えいは許されません。

監視対象の厳格な限定は可能なのか?

監視対象については、「外国が関係する通信」の必要性が特に高いとしたうえで、「メールの中身を逐一全て見るようなことは適当とは言えない」として、やりとりの個別具体的な中身には立ち入らないとの考えを示しました。

通信日時やIPアドレスといった付属的な情報（メタデータ）を想定しているのですが、本当に個人の特定につながることはないのか、政府による目的外使用や情報漏洩を防げるのか、監視対象の厳格化という点が問題となります。

サイバー侵入・無害化実施は自衛隊・警察が担当

論点整理では、相手のサーバーに侵入し、無害化する措置を「安全なサイバー空間を守る観点で必要」と認め、その実施機関については防衛省・自衛隊や警察を活用する方向を示しました。

行政監視の独立機関は機能するのか

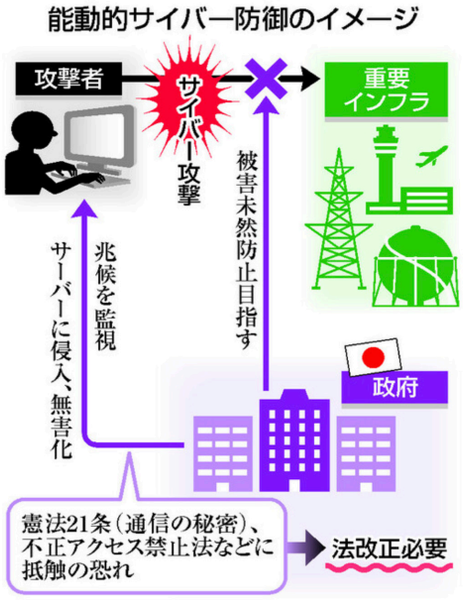
論点整理では、主要先進国においては通信情報の利用は独立機関が監督していると指摘したうえで、日本でも行政側の対応を監視する独立機関の設置を求めました。

サイバー監視から不審通信への侵入・無害化までの絶大な権限を行使する行政機関側の運用に対しては、厳格かつ徹底した監視を行う独立機関を整備することが求められます。

能動的サイバー防御の導入を巡る主な論点

官民連携の強化	民間事業者との情報共有や支援体制整備と政府の司令塔機能強化
通信情報の活用・監視	サイバー空間の平時からの監視と、憲法21条が保障する「通信の秘密」など法令との関係性
無害化措置	攻撃者サーバーへの侵入・無害化措置の発動要件や手段

能動的サイバー防御のイメージ



能動的サイバー防御での自衛隊の活用イメージ