平成２３年（ワ）第８８６号浜岡原子力発電所運転終了・廃止等請求事件

原告　石垣清水　外３３名

被告　中部電力株式会社

原告　準備書面　３１

平成２８年１０月７日

静岡地方裁判所　民事第２部　合議係　御中

原告ら訴訟代理人を兼ねる

弁護士　鈴　　木　　敏　　弘

弁護士　河　　合　　弘　　之

弁護士　青　　山　　雅　　幸

弁護士　大　　石　　康　　智

弁護士　南　　條　　　　潤

外

第１　はじめに

１　原子力発電所におけるシビアアクシデントの起因事象としては，内部事象（機械故障・ヒューマンエラーなど），外部事象（地震，津波，台風等），人為的事象（テロ等）が考えられるが，従前，日本では，内部事象を対象としたシビアアクシデント対策が主に検討され，外部事象，人為事象に関しては対策が乏しかった。[1]

２　２００１年９月１１日に発生した米国同時多発テロ事件を機に，ハイジャックされた大型航空機が原子力発電所や再処理工場などの原子力施設を攻撃する可能性が懸念され，米国では原子力発電に関する規制において航空機の衝突に対する評価が盛り込まれる等した。（「季報エネルギー総合工学 Vol.24 No4」甲 E 第７４号証４０頁）

他方，我が国では，航空機の墜落について，そのような墜落の発生確率が十分に低いという確率論を展開し，防護措置その他の必要な措置を講じてこなかった。[2]

３　しかし，福島第一原子力発電所で発生した事故により，これまで堅固な建物（防護区域）の中にある設備で安全・各セキュリティが確保されると思われてきたものが，防護区域外の複数の設備の同時損傷などにより，全交流電源の喪失や原子炉施設・使用済燃料貯蔵プールの冷却機能の喪失を意図的に発生させ得ることが公知となり，テロに対する原子力発電所の脆弱性が明らかとなった。[3]

すなわち，同事故は，テロによる周辺機器（一部は防護区域外の重要設備）の破壊がシビアアクシデントにつながる可能性を示唆しているものであり，福島第一原子力発電所に対して自然が与えた影響を人為的に与えることによって著しい損害を与えるか，あるいはそのような状況の直前の状況にまで至らしめた上で

---

[1] 国会事故調（甲 D 第１号証）１１６頁。
[2] 国会事故調（甲 D 第１号証）１９４頁～１９５頁。国会事故調・参考資料［添付 CD-ROM 収録］（甲 D 第１５号証）４９～５０頁。
[3] 学会事故調最終報告書（甲 D 第１６号証）２６２頁。

脅迫することによって，極めて有利な交渉条件を作ることが可能であると潜在的テロリストが学んだものと考えなければならない。[4]

4　このような中で，原子炉等規制法の平成２４年改正により，第１条（目的）において「大規模な自然災害及びテロリズムその他の犯罪行為の発生も想定した必要な規制を行う」という点が付加された。

したがって，原子力発電に関し，国及び事業者において，テロリズムを始めとした人為的事象についても，想定・対策が必要なことは言うまでもない。

5　本書面は，想定・対策が必要なテロ行為等を具体的に挙げた上，被告においてこれらの対策が不十分であることを主張する。

第２　原子力発電所がテロの標的となり得ること

１　原子力発電所におけるテロ事例

実際に原発に対しテロが行われた事例は，世界中に複数存在する。

２００７年１１月２日には，米国アリゾナ州にあるパル・ベロテ（Pal Verde）原発で，施設に入ろうとした契約従業員の車両からパイプ爆弾が発見され，施設が一時封鎖される事態に陥った。

また，同年１１月８日には，南アフリカ共和国プレトリア西部のペリンダバ（Pelindaba）原子力研究施設を，銃を所持した４人組が襲撃する事件が発生した。（甲 E 第７５号証 TRC EYE vol.154。）

米国同時多発テロでは，原子力発電所が標的になっていたという情報もある。

このように，既存の原子力発電所におけるテロ事件及びそれ以外の重要施設に対するテロ攻撃事例を踏まえ，本件原子力発電所においても，テロ行為による攻撃等を想定する必要がある。

２　原子力発電所が標的とされる理由

この点については，昭和５８年度外務省委託研究報告書「原子炉施設に対する

[4] 学会事故調最終報告書（甲 D 第１６号証）２６４頁。国会事故調（甲 D 第１号証）１９４頁。

攻撃の影響に関する一考案」（甲Ｅ第７６号証）と題する報告においても言及されている。

まず，今日の近代社会において，電力は不可欠のエネルギー源であり，それゆえ主要電源施設を攻撃し破壊することは，その国の総合戦力を低下せしめるとの観点から十分予想されるところである。（上記報告書１頁目１０行目）

もっとも，原子力発電所のもつ発電能力を失わせるためには，必ずしも格納容器とその内部にある原子炉自体を攻撃する必要はない。

もしも復旧の困難さを狙うのであれば，タービン発電機を攻撃目標とすることもありうる。

しかし，これらの事情にもかかわらず，原子炉ないし格納容器の破壊に至るような攻撃を行うならば，それは単に発電能力阻止が目的ではなく，炉内の大量の放射性物質の放散による効全交流電源の喪失や原子炉施設・使用済燃料貯蔵プールの冷却機能の喪失果を狙ったものと見なさざるをえない。

その攻撃が通常兵器によるによるものであっても，炉内に蓄積されている放射能の大きさを知れば，事の重大性を推測することができよう（上記報告書８頁目）。

福島第一原発事故による影響を鑑みれば明らかように，テロリストは，核兵器そのものを用いずとも，原子力発電所に対する攻撃により故意に炉心損傷を生じさせることによって国土に甚大な被害をもたらすことが可能となることから，原子力発電所はテロ攻撃の対象となり得るのである。

第３　テロ対策を求められる施設（原子炉建屋に限られないこと）

前述のとおり，福島第一原子力発電所事故は，区域外の複数の設備の同時損傷により，全交流電源の喪失や原子炉施設・使用済燃料貯蔵プールの冷却機能の喪失を生じさせ得ることを明らかにしてしまった。

テロにおいても，外部電源，非常用発電機，直流電源，海水ポンプなどの喪失，電源車不能などが単一または複合した事象またはそれ以上の事象が発生するこ

とは十分考えられるところである。

したがって，テロ対策においては，原子炉建屋の健全性のみならず，テロによる周辺機器（防護区域外の重要設備を含む）の破壊によってシビアアクシデントがひき起こされる可能性も含め，様々なシナリオを想定し過酷な事象への対策をすることが不可欠である。[5]

第４　想定すべきテロ行為・軍事攻撃等

１　総論（米国における想定を踏まえて）

(1) 米国では，２００１年９月１１日に発生した同時多発テロを踏まえ，本格的に航空機テロの検討・対策がなされており，２００９年には米国原子力委員会（NRC）が事業者に航空機衝突影響評価（Aircraft Impact Assessment）を求め，２００９年７月１３日以降に発行される新設プラントの建設許可書，運転認可書にこの航空機衝突影響評価の規制が適用され，さらに，既設の運転プラントには「B.5.b」[6]が適用されることとなった。

この航空機衝突影響評価の目的は，大型民間航空機の衝突による施設への影響についての評価を行い，その結果を設計へ反映し，限られた運転要員による対応で，以下のことを維持できるようにすることである。

① 炉心の冷却が確保され，格納容器が健全であること。

② 使用済み核燃料の冷却，または，使用済み燃料プールの健全性が保たれること。

（以上につき，国会事故調・参考資料［添付 CD-ROM 収録］（甲 D 第１５号証）４９頁。）

(2) また，その他テロ行為による人事的事象についても，米国では９．１１以降

---

[5] 学会事故調最終報告書（甲 D 第１６号証）２６４頁。

[6] ２００１年９月１１日の同時多発テロの後，２００２年２月に NRC（米国原子力規制委員会）が策定したテロ対策。全電源喪失を想定した機材の備えと訓練を米国の全原子力発電所に義務付けている。国会事故調（甲 D 第１号証）１１頁注釈参照。

の原子力発電所の防護設備を，以下の状況（DBT:Design Basis Threat）を想定し構築している。

① テロリストグループは専門の軍事訓練を受けた戦闘要員から構成。

② 殺傷することにもされることにもためらいがなく（自爆テロ），効果的な攻撃を全うするための目標について知識を有する者。

③ 同時に複数のチームで複数の箇所から進入・攻撃（同時多発テロ）。

④ 内部の者によるほう助（攻撃目標に関する情報提供，進入・脱出の案内，警報装置や通信装置の破壊，及び戦闘参加を含む）も想定。

⑤ 侵入路の確保，原子炉や非常用設備等を破壊するための各種武器（爆弾，自動小銃，サイレンサー付き狙撃銃など）を所持。

⑥ 大量の爆薬を搭載した４輪自動車の使用。

⑦ 陸路からのみならず，水路からも同時に攻撃（空路からのジャンボジェット機による攻撃は，DBT の範囲からは除外）。

⑧ サイバーテロ。

上記のような想定のもと，米国では２００１年以降１０億ドルを投入し，警備員の増員，設備の強化，訓練の強化など，原子力発電所（重要区域）の警備を行っている。

その結果，原子力発電所専属の戦闘要員は全米で８０００人，各発電所あたり約１２５人が配属され，そのうち６７％が保安警備の業務訓練者，１７％が大学卒の学歴を有しており，また，配備時訓練２７０時間，再訓練９０時間/年，対テロ戦闘訓練３０時間/年，高性能兵器の使用訓練，机上訓練（Table-Top Exercise），模擬戦闘（FOF:Force-on-Force）などを行い，警備能力を担保するに至っている。

（以上につき，国会事故調・参考資料［添付 CD-ROM 収録］（甲 D 第１５号証）５０頁。）

(3) シビアアクシデント対策としてのテロ想定・対策に関しては，我が国におい

ても米国における上記想定を排除する根拠は何ら見当たらず，少なくとも同程度の想定は必要不可欠である。

以上を前提に，以下にいくつか具体的想定を適示し，問題点を指摘する。

２　航空機の衝突による攻撃

(1) 米国における対策状況を踏まえて

ア　２００１年９月１１日の米国同時多発テロにおいては，ハイジャックされた大型航空機が国際貿易センタービルに突入している。

これを受け，米国では，前述のとおり NRC（米国原子力委員会）が２００２年に暫定保障措置命令 EA-02-26 を発出し，その中の B.5.b 項において，原子力発電所の航空機衝突時の影響緩和措置及び対応手順書の策定を求めている。

また，規制基準の 10CFR50.54(hh)(2)では，爆発または火災によってプラントの大部分が喪失した状況でも，炉心冷却，格納容器及び使用済燃料プール冷却の機能を維持または復旧することを目指したガイダンス及び対策計画を作成し，実施することを求められている（学会事故調最終報告書［甲 D 第１６号証］３０２頁）。

イ　テロ対策の重要性が上記米国同時多発テロに端を発している以上，本件原子力発電所を含む我が国の原子力発電所においても，大型航空機による意図的な衝突について，想定すべきテロ行為の代表の１つとして挙げるべきことは言うまでもない。

(2) ドイツにおける調査報告

ドイツにおいても，ハイジャック機が原子力発電所に衝突するというテロ攻撃への懸念が焦点になっていた。

ドイツ原子炉安全委員会（RSK）の仮報告書では，ドイツ国内の全原子力発電所は，大型旅客機の意図的な衝突に耐えることに疑問であるという結論を出した（「季報エネルギー総合工学 Vol.24 No4」甲 E 第７４号証４２頁）。

原子力発電所において，大型旅客機が原子炉建屋に直撃した場合のリスクについて，真摯に調査を行ったものと評価できる。

(3) 日本における対策の不備

ア　ドイツでは，１９７３年以降の原子力発電所においては，その設計段階において，軍用機の衝突に耐えられる強度を要求されていたが[7]，日本では，原子力発電所の設計要件において，航空機の衝突は特段考慮されていなかった。

新規制基準においては，意図的な航空機の衝突などへの対策も求められているが，その内容は，可搬設備を中心とした対策であり，航空機が衝突した場合の建屋や格納容器の健全性については考慮されていない。

しかも，バックアップ対策として求められている特定重大事故等対処施設の設置については，「工事計画」の認可から５年間猶予される状況であり，到底不十分である。

(4) 本件原子力発電所における対策の不備

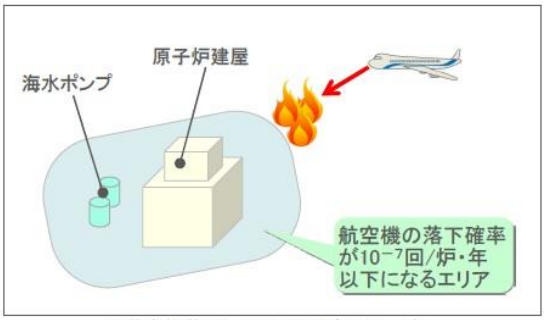
本件原子力発電所４号機については，被告により，すでに新規制基準適合性審査の申請がなされている。

しかし，そこでは，外部火災の影響評価として，航空機の落下確率が 10^{-7} 回/炉・年以下になるエリアの外側で航空機落下による火災が生じるとの仮定に基づく評価しか行っておらず，建屋や海水ポンプ等に直撃した場合の影響については，現状何らの評価も示していない。

[7] 国会事故調・参考資料［添付 CD-ROM 収録］（甲 D 第１号証）４９頁。

［図：被告ホームページより引用］[8]

影響評価 対象事象	影響評価結果
①森林火災	重要な原子炉施設（原子炉建屋、海水ポンプ等）に影響が及ばないよう、火災の延焼を防ぐために防火帯を確保する
②工場等の火災	発電所周辺に考慮すべき石油コンビナート等はない
③航空機落下に伴う火災	航空機燃料による火災の発生を仮定して、それによって安全機能を損なわないことを確認（火災は、航空機の落下確率が10^{-7}回/炉・年以下になるエリアの外側で起きると仮定します）



<航空機落下についての評価イメージ>

これは，フィンランド・オルキルオト３号機において，航空機の直撃を現実に生じ得る事象と捉え，格納容器保護のため二重の格納容器として設計していること（甲Ｃ第１０号証１７頁）などと対照的である。

(5) 小括

航空機の衝突が生じた場合における原子力発電所の健全性評価においては，まず航空機が建屋そのものや原子炉冷却の要である海水ポンプの直撃した場合の影響について適切に評価・対策することが必要不可欠であるにも関わらず，現状，新規制基準もかかる評価を求めておらず，被告が自主的にかかる評価を行うこともしていない。

したがって，本件原子力発電所各号機については，航空機の衝突という重大な脅威に対し適正な対策がなされているとは到底いえず，その安全性はなんら担保されていない。

２　ミサイルによる軍事的攻撃について

(1) 昭和５８年度時点ですでに指摘がなされていたこと

原子力発電所に対し，シビアアクシデントを意図的にひき起こす攻撃の位置態様として，ミサイル攻撃が考えられる。

この点については，先に指摘した昭和５８年度外務省委託研究報告書「原子

[8] ２０１４年２月１４日プレスリリース「浜岡原子力発電所４号機に係る新規制基準への適合性確認審査のための申請について（説明資料）」より引用。
http://www.chuden.co.jp/corporate/publicity/pub_release/press/3238400_19386.html

炉施設に対する攻撃の影響に関する一考案」（甲 E 第７６号証）においても，「格納容器が爆撃（ないし砲撃）され，破損する場合」について想定されるシナリオの１つとして挙げられている。

上記昭和５８年度の時点の報告書１３頁以下においても「今日の誘導型爆弾（ミサイル）のもつ命中精度は極めて高いので，格納容器攻撃が一旦実行されれば，その器壁が破壊される危険性は高いと考えねばならない。」と指摘されている。

加えて，同報告書は，ミサイル攻撃がなされた場合の被害想定として，「原子炉容器から出ている配管系（１次冷却系）が破損して LOCA（冷却材喪失事故）が発生し，かつ ECCS 系も破壊された場合や，格納容器攻撃と併せて電源系統も破壊されたり，あるいは余熱除去系の末端が破壊されたりした場合には，やがて炉心は溶融するに至り，すでに破損している格納容器を通り抜けて大気中に放射性物質が放散される。」とも指摘している。

さらに，第３のシナリオとして，複数発のミサイルが着弾することにより，炉心そのものが破壊・粉砕されるケースにも触れられている。

したがって，本件原子力発電所においても，シビアアクシデントを意図的にひき起こす攻撃の一態様として，軍事的ミサイル攻撃を想定することも必要である。

(2) 北朝鮮によるミサイル攻撃

我が国において，想定すべき脅威の１つとして，北朝鮮からのミサイル攻撃が挙げられる。

１９９８年には，北朝鮮の発射した「テポドン１」の先端部の覆いが太平洋側における日本の排他的経済水域（EEZ）内に落下した事例がある。

また，本年（平成２８年）８月３日には，北朝鮮西岸の黄海南道・殷栗（ファンヘナムド・ウンリュル）付近から発射された「ノドン」とみられる中距離弾道ミサイル発射され，同ミサイルは約 1000km 飛行し，秋田県の男鹿半島

沖約250kmの日本の排他的経済水域内に同ミサイル弾頭部が落下している。

北朝鮮は，本年９月５日にも弾道ミサイル３発を発射し，同ミサイルは約1000kmを飛行し，北海道西方の排他的水域内（北海道・奥尻島から西へ200～250kmの日本海上）に落下したとみられている。

これらのミサイルについては，本件原子力発電所も十分射程圏内にあるといえる。

福島第一原発事故と同規模の事故が本件原子力発電所で発生した場合，訴状１２３頁以下で述べたとおり，我が国の東西を繋ぐ交通網は寸断され，経済的にも甚大は被害が予想される。

そのため，我が国の国土に壊滅的なダメージを与えることを企図して，本件原子力発電所がミサイル攻撃の標的とされることも十分考えられるところである。

しかも，本年９月９日には，北朝鮮は核爆発実験を行った上，「弾道ミサイルに装着できるようにした核弾頭の性能などを確認した」などと発表しており，予断を許さない状況にあるといえる。

(3) 本件原子力発電所において何ら想定・対策がなされていないこと

このように，他国からのミサイル攻撃も想定すべき脅威の１つであるにも関わらず，本件原子力発電所においては，特段の想定・対策はなされていない。

ミサイル攻撃により格納容器が破損した場合はもとより，原子炉建屋上層階に位置する使用済燃料プールが損壊することによっても，放射性物質の飛散や再臨界が生じ得る。

３　サイバーテロについて

(1) 総論

本書面第４の１(2)で触れた米国のテロ対策でも触れられているとおり，サイバーテロも想定すべき現実的な脅威の１つである。

本書面では，シビアアクシデントを生じさせ得るサイバー攻撃として，

「SCADA」等の汎用的な産業制御システムを標的とした攻撃について指摘する。

(2) 産業制御システムが攻撃された場合のリスク

ア　SCADA（Supervisory Control And Data Acquisition）とは，地理的に分散した制御対象を，広域ネットワークを介して遠隔集中監視するシステムを指すが，日本では，PLC（Programmable Logic Controller）などの制御機器の監視を，マンマシンインターフェース（HMI）である汎用パーソナルコンピュータ上で実行するためのソフトウェアを SCADA と呼ぶ場合が多い。

イ　制御システムは，電力，ガス，石油パイプライン，水道，通信，大型プラントなど，米国を始めとした各国の重要インフラで用いられている。

制御システムは，もともと独立した専用システムとして設計され，使用される製品や技術もベンダ個別仕様のものであった。

これらの重要インフラには多くの技術者が関与しているが，各事業者はそれぞれ独自のシステムを採用しており，制御システムのデータのやりとりにはインターフェースやデータ形式のカスタマイズが必要であった。

近年になり，コスト削減などの経済性や，状況に応じた迅速なフィールドプロセスの制御というユーザーニーズを背景に，システム間の相互接続性の確保が求められるようになった。

パーソナルコンピュータの高性能化，Windows や Linux の普及，インターネットや無線などネットワーク技術の高度化などにより，リモート環境でのリアルタイムでのデータ通信ができる技術的環境が整い，制御システム全体において，他事業者を含むシームレスなデータ連携が図られるようになった。

このような背景により，米国では，個別の開発や維持費用が不要である汎用製品の採用，また，接続性が担保されている標準プロトコル（TCP/IP や

イーサネットなど）の採用という，制御システムのオープン化が進展している。

（以上につき，独立行政法人情報処理推進機構セキュリティセンター作成の調査報告書［甲Ｅ第７７号証］９頁，１２頁，１８頁。）

ウ　システムがオープン化され汎用製品が採用されるようになった結果，これらの汎用製品におけるハードウェア/ソフトウェアの脆弱性の課題も引き継ぐこととなった。

ネットワーク経由やリムーバブル・ストレージ（USB メモリ等）を介し，ワームやマルウェアが侵入する脆弱性を孕むようになったのである（上記調査報告書２１頁）。

エ　日本においても，制御システムへの汎用製品と標準プロトコルの採用は進展していることから，米国における場合と同様のセキュリティ上の課題を抱えているといえる（上記調査報告書４３頁。）。

(3) 原子力関連施設の産業制御システムが攻撃された事例

ア　米国オハイオ州 Davis Besse 原子力発電所の事例

２００３年１月，オハイオ州 Davis Besse 原子力発電所において，マイクロソフト社の SQL サーバ[9]を狙った「Slammer」ワームが，VPN（Virtual Private Network）接続[10]を介して侵入・感染し，SCADA システムを５時間にわたり停止させた。

同施設のプロセス・コンピュータも停止し，再運用までに約６時間を要したほか，ほかの電力施設を結ぶ通信トラフィックも混乱し，通信の遅延や遮断に追い込まれた。

---

[9] SQL Server とは，マイクロソフト社が開発・販売しているリレーショナルデータベース管理システム（RDBMS）であり，windows 上で動作する。

[10] VPN=仮想プライベートネットワーク。通信事業者の公衆回線を経由して構築された仮想的な組織内ネットワーク。
企業内ネットワークの拠点間接続などに使われ，あたかも自社ネットワーク内部の通信のように遠隔地の拠点との通信を行うことができる。

発電所のサーバはファイアウォールで外部ネットワークと遮断されていたが，ファイアウォール内部のネットワークに接続した，発電所のコンサルタント会社の端末が感染源となった（上記報告書２２頁)。

イ　イランのウラン燃料濃縮施設の事例

イランのナザンツに所在するウラン燃料濃縮施設においては，マルウェア「stuxnet」（スタクスネット）により，同施設内に設置されている遠心分離機約９０００基のうち約１０００基が物理的に破壊されるに至っている。

この際，stuxnet は，ネットワーク経由で侵入したのではなく，USB メモリを介して感染したものとみられている。

stuxnet が標的としたのは，windows 上で動作するドイツ・シーメンス社の監視制御ソフトである「SIMATIC STEP7」または「SIMATIC WinCC」が導入されたシステムであった。

上記ウラン燃料濃縮施設において，stuxnet は，ドイツ・シーメンス社製の制御システム（SCADA）に感染し，同システムにより制御された周波数制御変換器の周波数を断続的に変化させ，これにより遠心分離機器の回転数が大幅に増減し過大な負担がかかったことにより，遠心分離器が物理的に損壊するに至った。

このような stuxnet の性質に照らし，stuxnet は，コンピュータだけでなく制御システムに関する専門知識を有する者によって，特定の制御システムを攻撃するためだけに作成された不正プログラムである可能性があると指摘されている。(「コンピュータウィルス stuxnet によるイラン核関連施設攻撃」甲 E 第７８号証。「日本経済新聞電子版２０１３年７月４日」甲 E 第７９号証。情報技術解析平成２２年報［甲 E 第８０号証］１０頁以下。)。

(4) 原子力発電所がサイバー攻撃を受けるリスク等

この点について，イギリスの王立国際問題研究所（RIIA）が民生用原子力施設におけるサイバー・セキュリティについて分析した報告書を公表し，以下

の点を指摘した上で，警鐘を鳴らしている。（甲Ｅ第８１号証）

原子力施設でデジタル･システムへの依存が高まり，ハッキングが容易な市販ソフトの利用が増えるにつれて，サイバー・セキュリティ上のリスクも増大している。

原子力施設は公のインターネットから完全に切り離されていて，サイバー攻撃から防護されているという幻想が広がる一方で，その防護空隙は stuxnet 事件の際，ＵＳＢドライブ程度のもので簡単に破られており，ハッキングは一層容易かつ広範に行わるようになっているといえる。

(5) 本件原子力発電所設備が攻撃され感染する危険性

本件原子力発電所３号機・４号機・５号機はいずれも東芝が製造・納入したものであり[11]，同形式の BWR 及び ABWR は国内の他の原子力発電所においても採用されている。

上記原子炉の製造元･採用状況等に照らすと原子炉の各機器を制御する制御システムについても，完全に被告専用・独自のものであるとは考えにくく，ある程度の汎用的な製品を用いているものと思われる。

そのため，本件原子力発電所においても，ネットワークを介して，または，USB メモリ等のリムーバブルメディアにマルウェアが混入すること等により，制御システムまで感染が及び，機器の意図せぬ動作・誤動作をひき起こす可能性は否定できない。

第５　結論等

以上に述べたとおり，米国同時多発テロや福島第一原子力発電所事故という事実を教訓とすれば，本件原子力発電所においても，大型航空機の突入やミサイル攻撃などの悪意ある攻撃をも想定する必要があるにも関わらず，被告は（対策以

11 東芝ホームページ「原子力事業部」より。
https://www.toshiba.co.jp/nuclearenergy/jigyoubu/nounyu.htm

前に）そのような想定自体を行っていない。

また，サイバーテロに対する対策の決して十分とはいえない。

かかる状況にまま，本件原子力発電所各号機を稼動させることは，重大事故のリスクを顧みず経済性のみを先行させるものであり，到底許容できるものではない。

以　上