資料６－２

サイバー安全保障分野での対応能力の向上に向けた有識者会議
アクセス・無害化措置に関するテーマ別会合　第１回
事務局資料

令和６年７月１日

内閣官房

サイバー安全保障体制整備準備室

国家安全保障戦略（令和４年12月16日 国家安全保障会議決定・閣議決定）【抜粋】

- **武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃**のおそれがある場合、これを**未然に排除**し、また、このようなサイバー攻撃が発生した場合の**被害の拡大を防止**するために**能動的サイバー防御を導入**する。そのために、サイバー安全保障分野における情報収集・分析能力を強化するとともに、能動的サイバー防御の実施のための体制を整備することとし、以下の(ア)から**(ウ)**までを含む必要な措置の**実現に向け検討**を進める。

  (ア) 重要インフラ分野を含め、民間事業者等がサイバー攻撃を受けた場合等の政府への情報共有や、政府から民間事業者等への対処調整、支援等の取組を強化するなどの取組を進める。

  (イ) 国内の通信事業者が役務提供する通信に係る情報を活用し、攻撃者による悪用が疑われるサーバ等を検知するために、所要の取組を進める。

  (ウ) **国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃**について、**可能な限り未然に攻撃者のサーバ等への侵入・無害化ができる**よう、政府に対し必要な権限が付与されるようにする。

サイバー攻撃の特性

特性①：攻撃者の優位性

攻撃元隠蔽の技術的容易性

- マルウェアに感染させるなどして***不正に外部から制御できるようになった通信機器***を多数、多段的に組み合わされて構成された***攻撃用のネットワーク（いわゆるボットネットワーク）を構成***し、攻撃に利用
- 攻撃の受け手側からの***追跡が困難***

攻撃側と防御側の非対称性

- 攻撃側：***手法や対象を自由に選択可能*** ⇔ 防御側：広範な攻撃手法や攻撃対象を想定した防御策が必要
- 攻撃側と防御側の***非対称性***から、防御側はサイバー***攻撃が行われていることを認識することさえ困難***な可能性

特性②：瞬 時 拡 散 性

- グローバルなサプライチェーンを経由する製品・サービスの拡大・浸透、産業分野でのIoT機器の利用拡大（あらゆるモノがネットワークに接続されるようになること）等により、***サイバー攻撃が発生した場合の経済社会活動への影響は、瞬時に、かつ、より広範に、多様な主体・場面に及ぶおそれ***

特性③：越　　境　　性

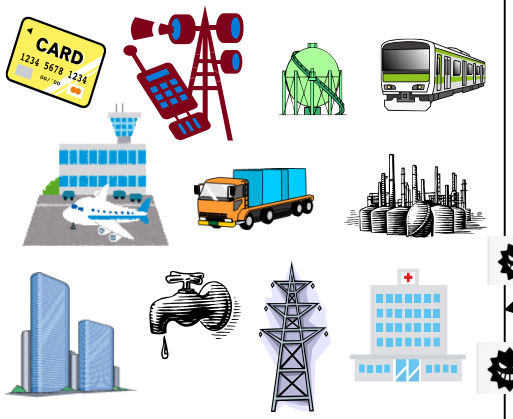
- サイバー攻撃は、攻撃元と被害発生地との***地理的なつながりが希薄***、***国境を越えて事案が発生***
- 安全保障環境の激しさが増す中、サイバー攻撃による重要インフラの機能停止や破壊、身代金の要求、機微情報の窃取等は、***国家を背景とした形でも平素から行われている***

「国民生活の基盤をなす経済活動」や「社会の安定性」をサイバー攻撃から守るため、能動的なサイバー防御を実施する体制を整備する。

全てのステイクホルダーがメリットを実感できるサイバー攻撃対応のエコシステムを官民を横断して構築

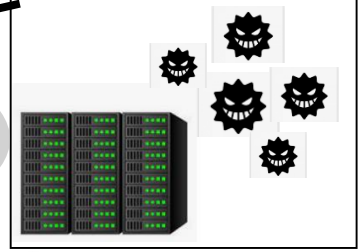
本テーマ別会合の射程

守る対象（例）

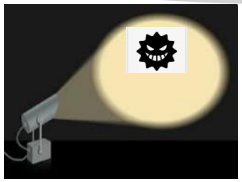


Internet

攻撃者



通信事業者



通信情報の活用
攻撃サーバ等を検知するため、明確な法的根拠を設けた上で、通信情報を活用

アクセス・無害化措置
確認された攻撃サーバ等に対し、 必要に応じ無害化

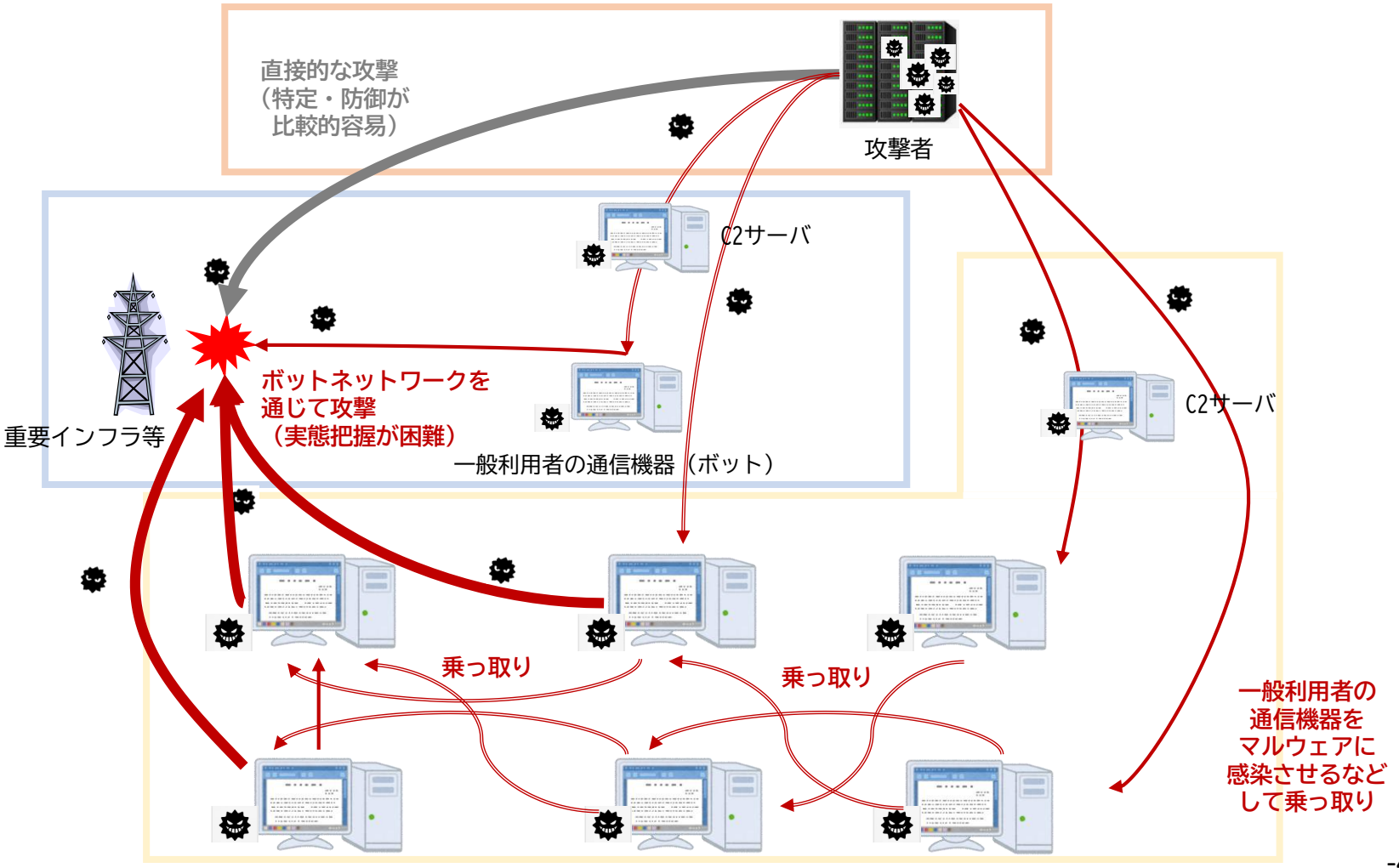
官民連携の強化
官民の情報共有により、事案の未然防止、対処支援強化を図る

政　　府

想定されるサイバー攻撃の実態

攻撃者は、攻撃元を隠蔽するため、一般利用者の通信機器をマルウェアに感染させるなどして乗っ取り、これらの通信機器（ボット）を多数、多段的に組み合わせて構成された攻撃用のネットワーク（ボットネットワーク）を利用することが通常。しかも、当該ボットの多くは、国外にも所在すると考えられている。このような状況で被害を防止するためには、ボットネットワークの実態把握が必要。

確認された攻撃サーバ等に対し、必要に応じて、無害化措置を実施



アクセス・無害化措置のイメージ

<C2サーバ・ボットのIPアドレスを特定等>

C2サーバ・ボットにアクセス

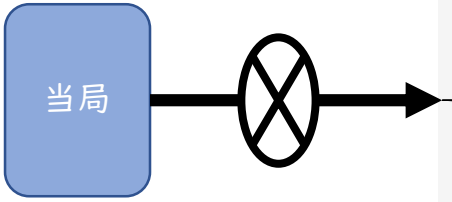
▼

C2サーバ・ボット内の不正プログラム等の確認

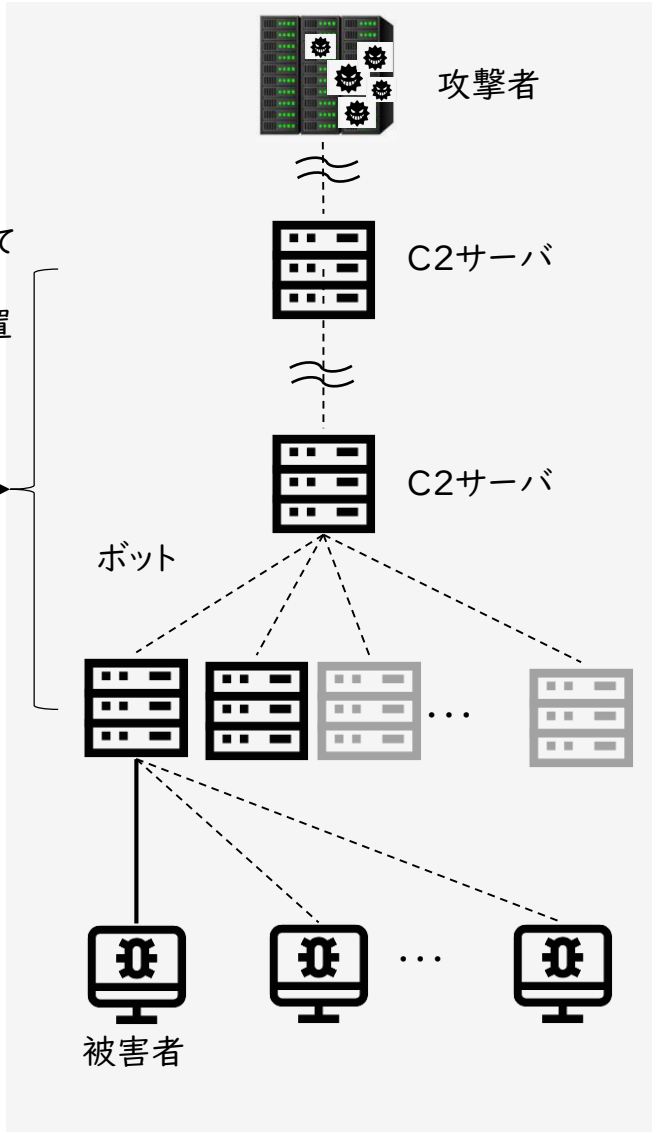
▼

C2サーバ・ボット内の不正プログラムの除去等

具体的措置の例
- 不正プログラムそのものの消去
- 不正プログラムの停止のための変更
- 不正プログラムのみの停止
- 不正プログラムを消去するための通信機器の再起動　など

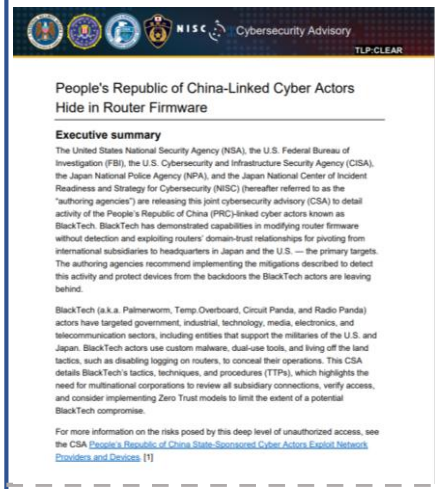


インターネットを介して
必要に応じた
アクセス・無害化措置



これまでの攻撃側への対処の主な例

パブリック・アトリビューション等の外国機関と連携した対処


Cybersecurity Advisory
TLP:CLEAR

People's Republic of China-Linked Cyber Actors Hide in Router Firmware

Executive summary

The United States National Security Agency (NSA), the U.S. Federal Bureau of Investigation (FBI), the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the Japan National Police Agency (NPA), and the Japan National Center of Incident Readiness and Strategy for Cybersecurity (NISC) (hereafter referred to as the "authoring agencies") are releasing this joint cybersecurity advisory (CSA) to detail activity of the People's Republic of China (PRC)-linked cyber actors known as BlackTech. BlackTech has demonstrated capabilities in modifying router firmware without detection and exploiting routers' domain-trust relationships for pivoting from international subsidiaries to headquarters in Japan and the U.S. — the primary targets. The authoring agencies recommend implementing the mitigations described to detect this activity and protect devices from the backdoors the BlackTech actors are leaving behind.

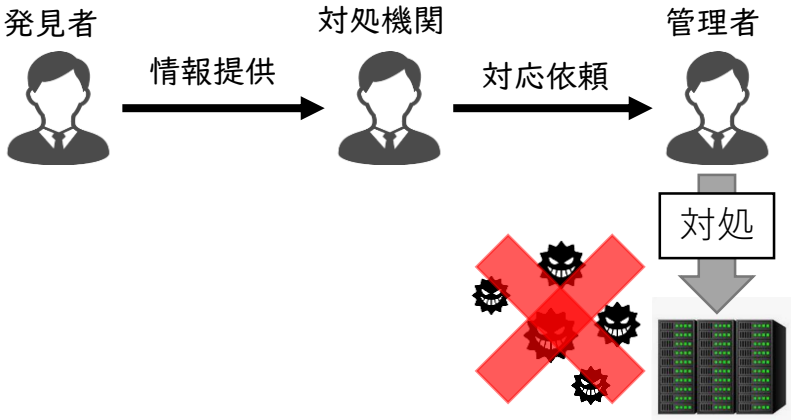
BlackTech (a.k.a. Palmerworm, Temp.Overboard, Circuit Panda, and Radio Panda) actors have targeted government, industrial, technology, media, electronics, and telecommunication sectors, including entities that support the militaries of the U.S. and Japan. BlackTech actors use custom malware, dual-use tools, and living off the land tactics, such as disabling logging on routers, to conceal their operations. This CSA details BlackTech's tactics, techniques, and procedures (TTPs), which highlights the need for multinational corporations to review all subsidiary connections, verify access, and consider implementing Zero Trust models to limit the extent of a potential BlackTech compromise.

For more information on the risks posed by this deep level of unauthorized access, see the CSA People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices. [1]

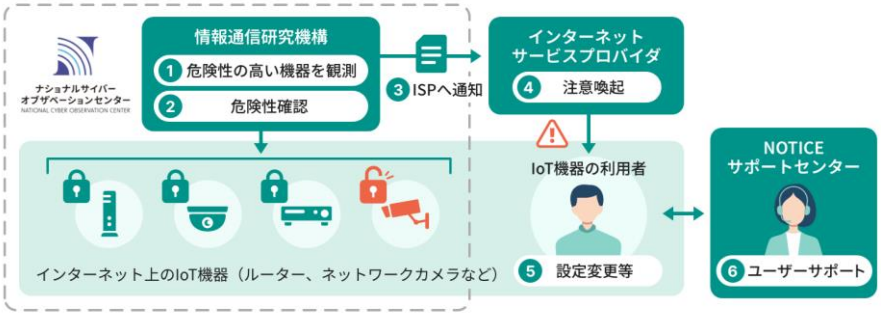
サイバー攻撃を受けた機器やサイバー攻撃に使用された不正プログラムを解析するなど、総合的な分析を行い、攻撃者や手口に関する実態解明を進め、サイバー攻撃の攻撃者を公表し、非難することでサイバー攻撃を抑止

任意のテイクダウン

サイバー攻撃に使用されたサーバ等を把握し、不正な機能を停止（テイクダウン）するよう、サーバ管理者に依頼



攻撃に利用され得る機器への対処

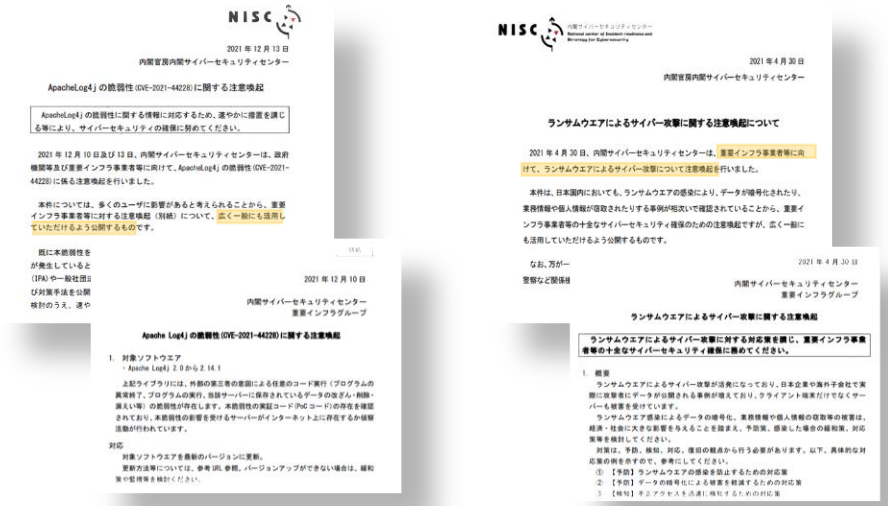


出典：https://notice.go.jp/about#overview

総務省及びNICTは、NICT法に基づき、電気通信事業者等と連携して、インターネットに直接接続されている機器がサイバー攻撃に悪用されるおそれのある場合に、利用者への注意喚起等により対処を促進

攻撃手口の公表

攻撃手口を公表し、広く一般に、あるいは、特定の事業者に対策を促すことで、サイバー攻撃を抑止


NISC
2021年12月13日
内閣官房内閣サイバーセキュリティセンター
「ApacheLog4j」の脆弱性（CVE-2021-44228）に関する注意喚起

NISC
2021年4月30日
内閣官房内閣サイバーセキュリティセンター
ランサムウエアによるサイバー攻撃に関する注意喚起について

2021年12月10日
内閣サイバーセキュリティセンター
重要インフラグループ
Apache Log4j の脆弱性（CVE-2021-44228）に関する注意喚起

2021年4月30日
内閣サイバーセキュリティセンター
重要インフラグループ
ランサムウエアによるサイバー攻撃に関する注意喚起

【事例】米当局による取組

- 2023年5月、米国、カナダ、豪州、ニュージーランド及び英国は、中国の支援を受けたハッカーグループであるVolt Typhoonによるルータへの侵入や更なるハッキング、情報窃取への利用を合同で注意喚起。
- 米当局は、Volt Typhoonによる感染ルータがKV Botnet（ボットネット：マルウェアによるネットワーク）を構成していると特定。感染ルータに対し、**マルウェアの通信プロトコルを用いて、マルウェアを当該ルータから削除するコマンドを送信**するなど、必要な措置を実施。

（注）本事例のほか、

- **英当局**による**特定のAPT（高度な持続的な脅威）が用いる技術の弱体化**等の取組
- **カナダ当局**による政府ネットワークからの情報窃取防止を目的とした**サイバー犯罪者の海外サーバの無効化**等の取組

等が行われていることが公開資料等から明らかとなっている。

他方、こうした活動は**秘密の活動**として行われているものが多く、**以上についても詳細は明らかになっていない**。

外国におけるアクセス・無害化に関する主な制度①

英国

1994年情報機関法第5条「（注：国務大臣が発行する）許可状（warrant）」

(1) 本条に基づき***国務大臣***が発行した許可状によって許可された場合、財産への立入り若しくは干渉又は無線通信への干渉は、違法とならない。

(2) 国務大臣は、***保安局***、***秘密情報部***又は***GCHQ***の申請により、本条に基づき、以下の場合に、許可状に記載する財産又は無線電信に関して、許可状に記載する措置をとることを許可する許可状を発行することができる。

(a) 次に掲げる場合であって、国務大臣が、その補佐を目的とし次の機関が以下の行為を遂行することが必要であると考える場合―

(i) 保安局が、1989年保安局法に基づく任務（※国家安全保障の防護等）を実行する場合；

(ii) 秘密情報部が、本法第1条の規定に基づく任務（※国家安全保障等を目的とした情報収集や他の任務）を実行する場合；

(iii) GCHQが、本法第3条(1)(a) の規定に定める任務（※国家安全保障等を目的とした情報収集や監視等）を実行する場合；

(b) 措置を実施することが、当該措置が達成しようとすることと均衡がとれていると国務大臣が認める場合

(c) （略）

(2A) 許可状を発行する場合において、前項(a)及び(b)の要件が満たされているか否か、検討する際に考慮すべき事項には、許可状で許可された措置を実施することによって達成する必要があると考えることが、他の手段によって合理的に達成され得るか否か、という事項を含めなければならない。　　（以下略）

2016年調査権限法第229条「主要な監督機能」

(1)・(2) （略）

(3) 調査権限コミッショナー（※）は、以下の事項を審査（監査、検査及び調査を手段として実施する場合を含む。）しなければならない。

（※）首相が任命。公的機関の通信傍受、通信データの取得・保持、機器の干渉等の機能の行使を監視。

(i) 1994年情報機関法第5条から第7条に基づく国務大臣による権限の行使（無線電信への干渉、財産への立入り及び干渉のための許可状等）（以下略）

公表済みの各国法令の条文を参照して作成。各国政府の確認を経たものではなく、これら以外に存在しないという趣旨ではない。

外国におけるアクセス・無害化に関する主な制度②

米国

合衆国法典第18編「犯罪及び刑事手続」第1030条「コンピュータと関係する詐欺及び関連行為」

(a) 以下に該当する者は、何人も、本条第(c)項に定めるところに従い処罰される。

(1)～(4) （略）

(5) (A) 故意に、プログラム、情報、コード又は（コンピュータに与える）コマンドの送信を引き起こし、当該行為の結果として、意図して、許可なく、保護されたコンピュータに対し損害を発生させた者；

(B) 意図して、許可なく、保護されたコンピュータにアクセスし、当該行為の結果として、結果を顧みることなく、損害を発生させた者；又は、

(C) 意図して、許可なく、保護されたコンピュータにアクセスし、当該行為の結果として、損害及び損失を発生させた者

(6)・(7) （略）

(b)～(e) （略）

(f) 本条は、***合衆国、州又はその下部組織の法執行機関***、又は***合衆国の情報機関***の適法に認められた***捜査活動***、***防御活動***又は***諜報活動***を禁止するものではない。

(g)～(j) （略）

合衆国法典第10編「国軍」第394条「軍事サイバー作戦に関する権限」

(a) 総則

国防長官は、外国勢力によって米国又は米国の個人に対して行われる悪意あるサイバー活動に対応する場合を含め、米国及びその同盟国を防衛するために、サイバー空間における秘密軍事行動又は作戦を含め、***サイバー空間における軍事活動又は作戦***を開発、準備、調整し、その目的のためにすべての***軍隊を準備させ、適切な権限を与えられた場合には、これを実施***するものとする。

(b)～(f) （略）

公表済みの各国法令の条文を参照して作成。各国政府の確認を経たものではなく、これら以外に存在しないという趣旨ではない。

外国におけるアクセス・無害化に関する主な制度③

豪州

2001年情報機関法第7条「通信情報局(ASD)の職務」

(1) ASDの職務は:

(a) 情報を求める政府の要求、特に国防軍の要求を満たすために、誘導、非誘導、又はその両方を問わず、又は、電気、磁気又は音響エネルギーの形で、豪州国外の人々又は組織の能力、意図又は活動に関する情報を入手すること;及び (中略)

(c) ***豪州国外の人々又は組織が行うサイバー犯罪を、電子的又は同種の手段で防止し、妨げること***;及び (中略)

(d) ***軍事作戦を支援するために国防軍に支援を提供***し、情報に関して国防軍に協力すること;及び (以下略)

1986年情報セキュリティ監査官(IGIS)法第8条「情報セキュリティ監査官による情報機関への調査機能」

(1) (略)

(2) 本条に従い、(中略)ASDに関する情報セキュリティ監査官の機能は: (中略)

(c) 法務大臣若しくは担当大臣[国防大臣]の要請又はIGIS自身の発意により、当該機関[ASD]の活動の合法性又は適正性に関する当該機関[ASD]の手続の有効性及び妥当性を調査すること。 (以下略)

2004年監視装置法第27KA条「データ破壊許可状(warrant)の申請」

(1) オーストラリア連邦警察又はオーストラリア犯罪委員会の法執行官(又はその代理人)は、法執行官が以下のことを合理的な根拠に基づいて疑っている場合、***データ破壊許可状***の発行を申請することができる。

(a) 特定の種類の1つ以上の関連犯罪が行われた、行われている、行われようとしている、又は行われる可能性がある。;及び

(b) それらの犯罪が、コンピュータ(対象コンピュータ)に保持されるデータに関与しているか、又は関与している可能性がある。;及び

(c) ***対象コンピュータに保持されるデータの破壊***が、以下の1つ以上の関連犯罪の実行を阻止することを実質的に支援する可能性がある。:

(i) 対象コンピュータに保持されるデータに関与する、又は関与する可能性がある。;及び

(ii) (a)で言及された関連犯罪と同種である。

申請の手続

(2) 前項の申請は、資格を有する裁判官又は指名されたAAT[行政不服審判所]委員に対して行わなければならない。(以下略)

公表済みの各国法令の条文を参照して作成。各国政府の確認を経たものではなく、これら以外に存在しないという趣旨ではない。

外国におけるアクセス・無害化に関する主な制度④

カナダ

通信安全保安部（CSE）法第29条「ディフェンシブ・サイバー・オペレーションの許可」

(1) ［国防］*大臣は*、国内外のいかなる法律にかかわらず、*CSEに対して*、その任務であるディフェンシブ・サイバー・オペレーション［注1］の促進のため、グローバルな情報基盤において、又は、それを通じて、［国防大臣が発出する］許可に明記された活動を実施することを許可する*ディフェンシブ・サイバー・オペレーションの許可*を発出することができる。

(2) ［国防］大臣は、*外相と協議した場合に限り、許可*を発出することができる。

注1：グローバルな情報基盤において、又は、それを通じて、連邦政府機関の電子情報及び情報インフラ、そしてカナダ政府にとって重要であるものと指定される電子情報及び情報インフラの保護を支援する活動。

通信安全保安部法第30条「アクティブ・サイバー・オペレーションの許可」

(1) ［国防］*大臣は*、国内外のいかなる法律にかかわらず、*CSEに対して*、その任務であるアクティブ・サイバー・オペレーション［注2］の促進のため、グローバルな情報基盤において、又は、それを通じて、［国防大臣が発出する］許可に明記された活動を実施することを許可する*アクティブ・サイバー・オペレーションの許可*を発出することができる。

(2) ［国防］大臣は、*外相の要請又は同意があった場合に限り、許可*を発出することができる。（以下略）

注2：グローバルな情報基盤において、又は、それを通じて、外交、防衛又は安全保障に関連する外国の個人、国家、組織又はテロリスト集団の能力、意図又は活動を低下、妨害、影響、対処又は干渉する活動。

通信安全保安部法第31条「許可された活動」

第29条(1)又は第30条(1)に基づく許可がCSEに実施することを許可する活動及び活動の種類は、次に掲げる事項を含めることができる。

(a) グローバルな情報基盤の一部にアクセスすること；

(b) グローバルな情報基盤において、又は、それを通じて、*あらゆる情報*をインストール、維持、コピー、配布、検索、*修正、妨害、削除*又は傍受すること；（以下略）

国家安全保障・情報審査局法第8条「審査及び調査」

(1) 審査機関[国家安全保障・情報審査局]の任務は、以下に掲げるものとする。

(a) 治安情報局［CSIS］又は通信安全保安部［CSE］により行われたあらゆる活動の審査 (以下略)

公表済みの各国法令の条文を参照して作成。各国政府の確認を経たものではなく、これら以外に存在しないという趣旨ではない。

（ウ）国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃について、可能な限り未然に攻撃者のサーバ等への侵入・無害化ができるよう、政府に対し必要な権限が付与されるようにする。

- 無害化措置を誰が運用するのかという点について、諸外国における**無害化の運用主体**としては、軍や情報機関、法執行機関となっていることを踏まえれば、我が国においては、**防衛省・自衛隊、警察がその保有する能力を活かす**とともに、**その能力の高度化**を図ることが極めて重要。
- **無害化を講じる事案の優先順位付け**を考える必要がある。能力やリソースが限られることを勘案すれば、対処すべき事案の優先順位を付けていくことが大事。
- 無害化措置を実施するに当たっては、インテリジェンス活動も重要。

- 制度整備に当たっては、実際に機能するものとする必要がある。そのため、理念法・組織法ではなく、**具体的な権限法として規定を整備する必要**があり、**従来の法執行システムと接合的で連続性のあるものとすることが必要**。
- 法令の新規制定や改廃に当たっては、**国内法体系での整合性**のほか、**国際基準にも目配りした措置がとられることが望ましい**。能動的サイバー防御に係る国際基準を国内法に導入することを検討することが必要ではないか。
- この会議の結果として策定される国内法令やそれに基づく国内措置は、サイバー安全保障に係る我が国の国家実行として、**国際法規範の形成に大いに貢献していくものになるということを強く意識すべき**。

検討に当たってのポイント

強 化 す べ き 取 組

サイバー攻撃においては、攻撃側が圧倒的に優位という攻撃側と防御側との間の「非対称性」から、サイバー安全保障分野における対応能力の向上に当たっては、***政府としてサイバー攻撃の実態を的確に把握***し、防御側に対する施策の強化にとどまらず、***アクセス・無害化措置を含め、攻撃側への対処を強化する必要***

検討に当たってのポイント

① 攻 撃 者 の 優 位 性

- 攻撃側は多数、多段的に組み合わされたボットネットワークを使用
- 攻撃側は手法や対象を自由に選択可能

→ ***実効的・効果的な対処に留意する必要***

②サイバー攻撃の越境性

- サイバー攻撃は地理的なつながりが希薄 、国境を越えて発生
- 安全保障環境の激しさが増す中、国家を背景とした形でも敢行

→ ***国際法との関係に留意する必要***

③サイバー攻撃の瞬時拡散性

- サイバー攻撃が発生した場合の経済社会活動への影響は、瞬時に、かつ、より広範に、多様な主体・場面に及ぶおそれ

→ 速やか、かつ、臨機応変な対応に留意する必要

④サイバー攻撃の秘匿性

- 第三者の通信機器をマルウェアに感染させるなどした上で、攻撃に用いるボットネットワークを構成して敢行

→ 第三者への影響等に留意する必要