

サイバー安全保障分野での対応能力の向上に向けて

令和 6 年 6 月 7 日

内閣官房

サイバー安全保障体制整備準備室

現在の情勢

- ・サイバー空間、海洋、宇宙空間、電磁波領域等において、自由なアクセスやその活用を妨げるリスクが深刻化している。特に、相対的に露見するリスクが低く、攻撃者側が優位にあるサイバー攻撃の脅威は急速に高まっている。
- ・サイバー攻撃による重要インフラの機能停止や破壊、他国の選挙への干渉、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。そして、武力攻撃の前から偽情報の拡散等を通じた情報戦が展開されるなど、軍事目的遂行のために軍事的な手段と非軍事的な手段を組み合わせるハイブリッド戦が、今後更に洗練された形で実施される可能性が高い。

公開サーバへの攻撃

エストニア・2007年

2005年 内閣官房情報セキュリティセンター設置

ウェブサーバ・外向けサービスへの大量送信
SQLインジェクションによる情報漏えい 等

ウェブサイト・
インターネットバンキング等の
停止

IT系システムの侵害

Wannacry・2017年
コロニアルパイプライン・2021年
大阪急性期・総合医療センター・
2022年

2015年 サイバーセキュリティ基本法施行（NISCも改組）

情報システム内部への侵入・暗号化
(主に既知の脆弱性を悪用)

暗号化・システム障害
身代金要求

有事に備えた重要インフラ等への侵入

ウクライナ・2015年/2022年等
Volt Typhoon・2023年

最深部・制御系システムに至る高度な侵入能力
(ゼロデイ脆弱性の積極活用など)
高度な潜伏能力
(Living-off-the-Landなど)

インフラ機能停止

機微情報の窃取の危険

Black Tech・2023年

情報システムへの権限外アクセス・利用

機密情報の漏えい・悪用

侵略開始以前

- ✓ ロシアは、侵略開始の1年以上前から、ウクライナの政府機関や重要インフラ等の情報システム・ネットワークに侵入し、破壊的サイバー攻撃を準備。侵略開始の1月程度前から、破壊的なサイバー攻撃等を開始。
- ✓ 特に侵略前日には約300のシステムを対象とした大規模な破壊的サイバー攻撃を実施。

2022年2月 衛星通信に対する攻撃

- ✓ 2022年2月24日、米Viasat社が提供する衛星通信サービス(KA-SAT network)が利用不能に。ウクライナ国内に限らず、ドイツの風力発電所等にも影響が拡大。

2022年4月 高圧変電所に対する攻撃

- ✓ 2016年の攻撃に用いられたマルウェアの亜種（Industroyer2）による高圧変電所への攻撃が確認されているが、ウクライナサート（CERT-UA）等の支援により、大規模停電には至らず。

2022年10月 変電所に対する攻撃

- ✓ 2022年10月、ウクライナの変電所が攻撃を受け、停電が発生。攻撃者は同年6月までにはシステムへの侵入に成功。
- ✓ 侵入先の正規ツールを悪用する「現地調達型の攻撃」(living-off-the-land)により変電所のブレーカーを遮断し、ミサイル攻撃と同時に停電が発生。その後、マルウェア“CaddyWiper”を展開し、システムを破壊。

2023年5月、ファイブ・アイズ5か国及びマイクロソフト社が、中国背景とされるサイバー攻撃グループVolt Typhoonについて、注意喚起を発出。概要以下のとおり。

- 有事における機能不全を念頭に置いた、**重要インフラへの事前のアクセス確保**（pre-positioning）を目的としたサイバー攻撃が発生
- 長期間の潜伏に必要な**高度な検知回避能力**が特徴
 - ✓ ネットワーク機器の脆弱性を突いて侵入。ゼロデイ脆弱性も悪用
 - ✓ マルウェアを使わず、正規ユーザになりすまし、正規ツールを駆使（Living off the Land）
 - ✓ 侵入痕跡となるログの消去 等
- 米国においては、本土及び島嶼部の米軍基地にサービスを提供する重要インフラ（通信、エネルギー、水道など）への攻撃の脅威が高まっている



サイバー空間の安全かつ安定した利用、特に国や重要インフラ等の安全等を確保するために、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させる。

【略】

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。

能動的サイバー防御を含むこれらの取組を実現・促進するために、内閣サイバーセキュリティセンター（NISC）を発展的に改組し、サイバー安全保障分野の政策を一元的に総合調整する新たな組織を設置する。そして、これらのサイバー安全保障分野における新たな取組の実現のために法制度の整備、運用の強化を図る。

○ 令和6年度における取組

- サイバー安全保障関連予算については、従来の内閣サイバーセキュリティセンター（NISC）予算を土台としつつ、これまでデジタル庁一括計上としてきた事業、各省庁からの財源拠出を受けて新たに取組む事業と合わせ、令和6年度において一定の増強を図った。

25.6 億円 → 56.0 億円（R6年度NISC予算）デジタル庁一括計上含む
いわゆる「四経費」のうちサイバー安全保障に関する経費は 124.5 億円（他省庁計上分を含む）

- 令和6年度においては、特に、政府機関等の情報システムのサイバーセキュリティ確保に関する施策を中心に、事業を計画中。
 - 政府関係機関におけるセキュリティインシデントの監視・分析（GSOC）の機能強化
 - 政府関係機関における情報システム・IT資産に関するリスク常時評価、監査強化等の施策（新規）
- 昨今のサイバー空間を巡る深刻な脅威に対応するため、NISCを抜本的に強化。
 - 複数の幹部職員を新たに措置し、指揮命令系統を強化。

部長級 1、課長級 2 → 次官級 1、局長級 2、部長級 3、課長級 9
その他 サイバー準備室に 局長級 1、部長級 1 を手当て

「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。

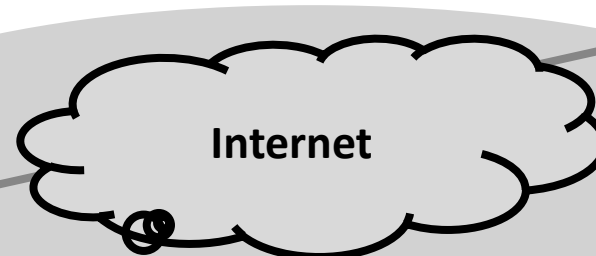
守る対象（例）



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

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

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

攻撃者



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

政府



- ✓ 欧米主要国は、近年、高度な攻撃に対する支援・情報提供や、ゼロデイ脆弱性の早期対処に必要な枠組みを強化。脅威ハンティング部門の設置やクリアランス活用のほか、製品ベンダの役割明確化等が進められている。
- ✓ 同時に、政府の対処・情報収集能力を支えるためのサイバー対応機能の一元化や、重要インフラ事業者に対するインシデント報告の義務化が進められている。

	英国	EU	米国	豪州
高度な攻撃に対する支援・情報提供	脅威情報のオンライン共有基盤 (CISP, 2013) クリアランスを保有する産業界関係者との協業 (Industry 100)	主に各々の加盟国が実施	CISAに脅威ハンティング部門を設置 企業との情報共有枠組みの設置 (JCDC, 2021)	脅威情報のオンライン共有基盤 (CTIS, 2021)
ゼロデイ脆弱性の対処	NCSCによる脆弱性情報の収集・分析・公開 製品ベンダによる脆弱性窓口設置等を義務化 (PSTI法, 2022)	製品ベンダに対する脆弱性悪用時の報告義務化等を検討中 (サイバーレジエンス法草案)	CISAによる脆弱性情報の収集・分析・公開 製品ベンダの責任を明記 (国家サイバーセキュリティ戦略, 2023)	ACSCによる脆弱性情報の収集・分析・公開 重要システムに対する脆弱性評価の実施義務化 (SOCI法, 2022)
政府の情報収集・対処等を支える制度	国家サイバーセキュリティセンター(NCSC)設置(2016) 重要インフラ事業者の報告義務化(NIS規則, 2018)	重要インフラ事業者の報告義務化(NIS指令, 2016)	サイバー対応機能を国土安全保障省CISAに集約 (CISA法, 2018) 重要インフラ事業者の報告義務化(CIRCSIA法, 2022 ※未施行)	豪州サイバーセキュリティセンター(ACSC)設置(2014) 重要インフラ事業者の資産登録・報告義務化 (SOCI法, 2021)

CISP【英】: サイバーセキュリティ情報共有パートナーシップ

PSTI法【英】: 製品セキュリティ及び通信インフラ法

NIS規則【英】: ネットワーク及び情報システム規則

NIS指令【EU】: ネットワーク及び情報システム指令

CISA【米】: サイバーセキュリティ・インフラセキュリティ庁

JCDC【米】: 官民サイバーセキュリティ協力枠組

CTIS【豪】: サイバー脅威情報共有枠組

SOCI法【豪】: 重要インフラ保安法

主要国における通信情報の活用の制度概要

9

	英国	ドイツ	米国	豪州
主な対象通信	<u>海外関連通信</u> (英諸島外の個人により送受信される通信)	<u>外国の電気通信</u>	<u>国外所在の 非米国人</u> (の通信)	<u>外国の通信</u> (国外で送受信される通信)
通信情報の取得の要件	・<u>安全保障上の必要性</u>又は重大犯罪の検知等の必要性 ・(取得目的のリストは首相が<u>レビュー</u>)	・<u>安全保障上の必要性</u> ・<u>重大な危険分野</u>(マルウェアによる国際的犯罪・テロ・<u>国家攻撃</u>、<u>重要インフラ</u>に対する脅威等)に関する情報の入手のために必要	<u>外国インテリジェンス情報</u> (外国勢力等の活動・安保関連情報)の収集のために必要	・<u>安全保障上の必要性</u> ・<u>外国インテリジェンス情報</u>(外国組織等の能力・意図・活動に関する情報)の収集のために必要
取得後の利用制限	・閲覧・複製・開示は最小限 ・国内通信内容の分析を原則禁止	・外部提供可能な場合を法令上限定 ・自国民等の個人データの分析を原則禁止	・裁判での証拠としての利用を原則禁止 ・米国人関連情報を必要最小限とする措置	・裁判での証拠としての利用を原則禁止 ・国内通信記録のスクリーニング及びその原則廃棄
独立機関の監督	<u>あり</u>	<u>あり</u>	<u>あり</u>	<u>あり</u>
法令名	<u>調査権限法</u>	<u>連邦情報庁法</u>	<u>外国情報監視法</u>	<u>電気通信</u> (傍受及びアクセス)法

※1 上記の制度は、主要国において、個別具体的な調査対象を事前に特定せず、通信情報を調査できる法的枠組の例。(これら以外に存在しないという趣旨ではない)

※2 公表済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、また、各国政府による対策の実態まで示すものではない。

【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。

官民連携の強化 (ア)関係

- 高度な侵入・潜伏能力に対抗するため、政府の司令塔機能、情報収集・提供機能の強化が不可欠

- ◆ 整理が必要な法令の例:サイバーセキュリティ基本法、各種業法

通信情報の活用 (イ)関係

- 悪用が疑われるサーバー等の検知には、「通信の秘密」を最大限に尊重しつつも、通信情報の活用が不可欠

- ◆ 整理が必要な法令の例:憲法21条(通信の秘密)

アクセス・無害化措置 (ウ)関係

- 重大なサイバー攻撃の未然防止・拡大防止を図るためには、政府に侵入・無害化の権限を付与することが不可欠

- ◆ 整理が必要な法令の例:不正アクセス禁止法

- 上記の取組を実現・促進するため、強力な情報収集・分析・対処調整機能を有する新たな司令塔組織を設置することが必要。

- 本有識者会議における、検討の進め方、重点的に検討すべき点、検討に当たって留意すべき点などについて、ご議論をお願いしたい。