株式会社Geolocation Technology

IP Geolocation技術を活用した能動的サイバー防御

証券コード：4018

能動的サイバー防御とは？

概念

サイバー攻撃を**未然に防ぐ**ために、攻撃者のネットワークに対して積極的に対処する手法です。

従来との違い

攻撃の兆候を早期に検知し、事前に無害化措置を講じることを目指します。

必要性

高度化するゼロデイ攻撃やサプライチェーン攻撃などのサイバー攻撃から組織を守るために不可欠です。

グローバルトレンド

米国や欧州では既に導入が進み、日本でも急務となっています。

欧米主要国が先行する主な取組

官民連携関係

- 主要国は、2010年代後半から最近にかけ、**政府からの情報提供、重要インフラ事業者による報告の義務化を制度化**

国家ｻｲﾊﾞｰｾｷｭﾘﾃｨ戦略(2023年)
重要ｲﾝﾌﾗｻｲﾊﾞｰｲﾝｼﾃﾞﾝﾄ報告法(2022年)

豪州ｻｲﾊﾞｰｾｷｭﾘﾃｨ戦略(2023年)
重要ｲﾝﾌﾗ保安法(2018年)

国家ｻｲﾊﾞｰ戦略(2022年)
ﾈｯﾄﾜｰｸ情報ｼｽﾃﾑ規則(2018年)

ｻｲﾊﾞｰﾚｼﾞﾘｴﾝｽ法(2024年)
ﾈｯﾄﾜｰｸ情報ｼｽﾃﾑ指令(2016年)

通信情報の利用関係

- 主要国は、**以前より、国家安全保障等の目的のために外国関係の通信情報を利用**
- 政府における通信情報の利用について **専門の独立機関が監督**

英国：調査権限法
(2016年制定)

米国：外国情報監視法
(2008年改正)

ドイツ：連邦情報局法
(2016年改正)

豪州：通信情報傍受及び
アクセス法(2021年改正)

アクセス・無害化関係

米国：Volt Typhoonによるボットネットワーク（感染ルータ群）に対する**無害化措置**（2024年）

カナダ：政府ネットワークからの情報窃取防止目的で、攻撃者の海外サーバに対する**無害化措置**（2019年以降）

英国、豪州も同様の取組を推進。

＊ 各国の法制及び実態の全てを網羅するものではない。

米国の取り組み

脅威インテリジェンスを積極的に活用しています。
官民連携による情報共有体制を構築しています。
攻撃の兆候に基づく事前対応を重視しています。

欧州の取り組み

GDPRを背景に予防的アプローチを採用しています。
早期検知システムの開発に注力しています。
公的機関と民間セクターの協力体制を強化しています。

日本での動き

関連法案の可決

2025年4月8日に**「能動的サイバー防御（Active Cyber Defense, ACD）」関連法案**が可決されました。

内閣サイバー官の新設

サイバー空間のリスク評価から対策の指揮まで一元的に担います。

戦略本部の格上げ

サイバーセキュリティ戦略本部は首相をトップとする体制になります。

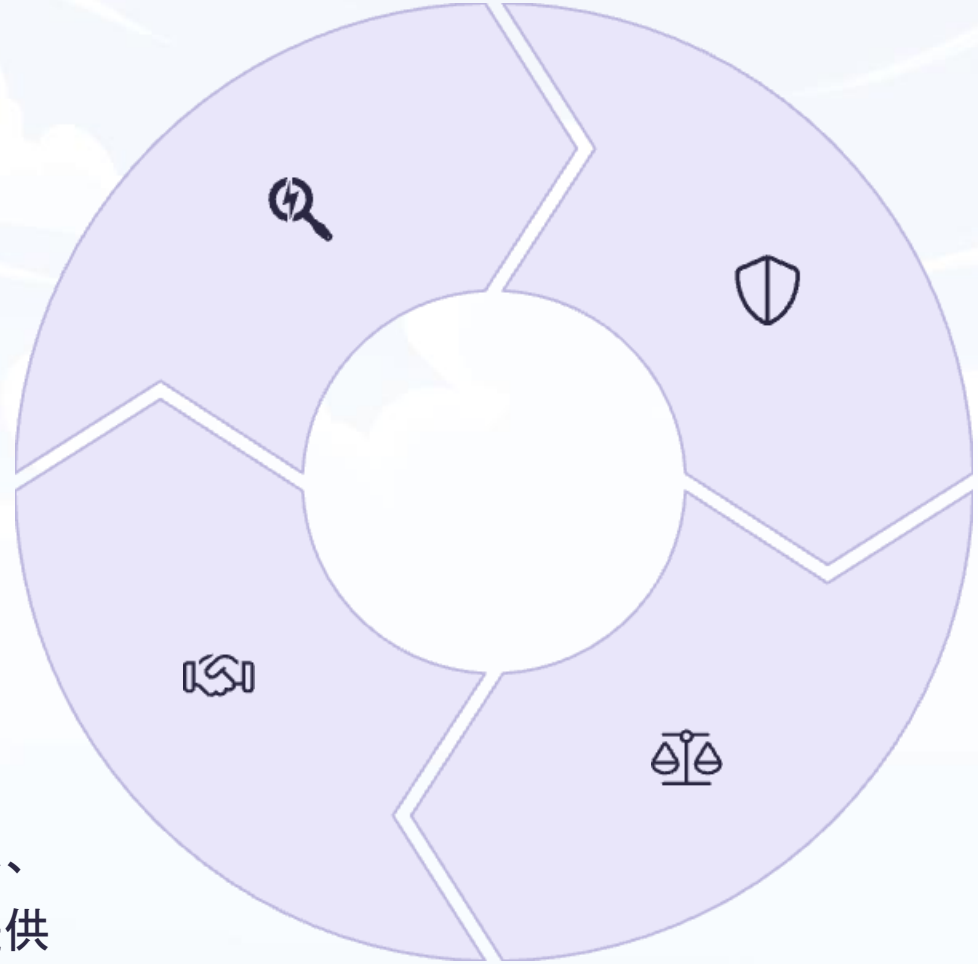
官民連携の強化

重要インフラ事業者との情報共有・対応体制が強化されます。

能動的サイバー防御 関連法案

通信情報の収集・分析

政府は通信情報を収集し、サイバー攻撃の兆候を早期に発見します。



無害化措置の実施

警察や自衛隊は、攻撃元のサーバーに侵入し、悪意あるコードを削除できます。

基幹インフラ事業者との連携

電力や通信などの事業者は、政府と協定を結び、情報提供が義務化されます。

独立機関による監視

「サイバー通信情報監理委員会」が政府の運用を監視します。

アクセスの無害化措置に問題はないのか？

多段階プロセス

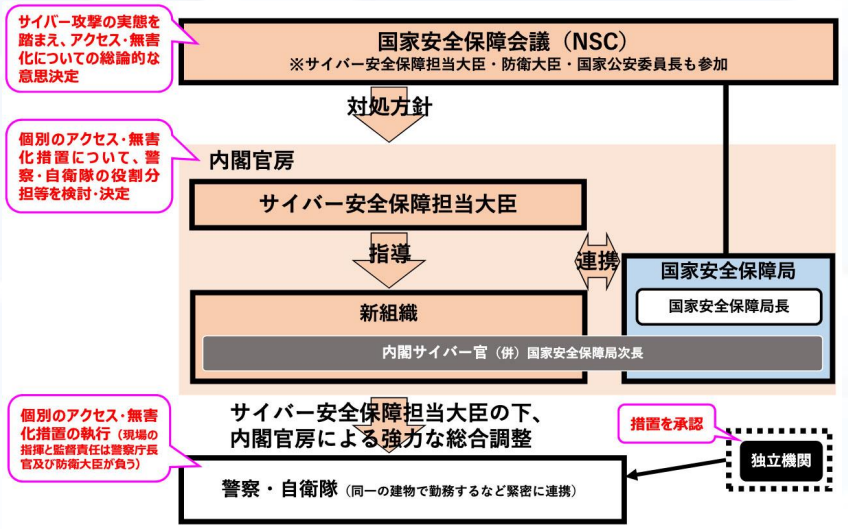
個別のアクセス・無害化措置は多段階のステップを経て執行されます。

攻撃のためのプログラム等の確認が行われてから実施されます。

国際法上の配慮

国外のサーバに対しては「緊急状態」等の国際法上の法理を援用します。

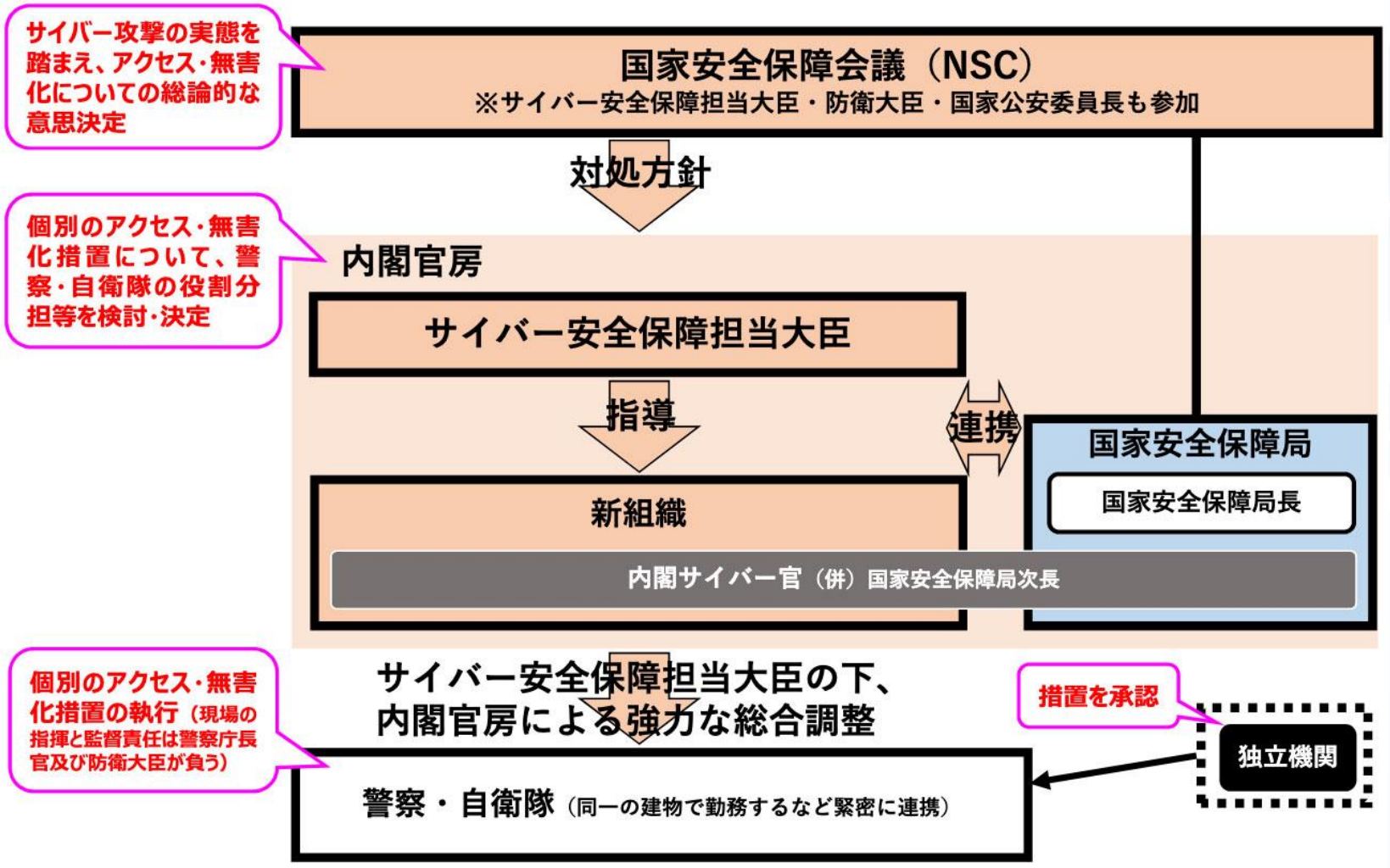
国際法上許容される範囲内で実施します。



緊急状態（Necessity）の概念

重大かつ急迫した危険から不可欠の利益を守るための唯一の手段であり、相手国等の不可欠の利益を深刻に侵害しないといった一定の要件を満たす場合に適用されます。

アクセスの無害化措置に問題はないのか？



出典元：https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/index.html
内閣官房　**サイバー安全保障に関する取組**
（能動的サイバー防御の実現に向けた検討など）

IP Geolocation技術を活用した能動的サイバー防御

IPアドレスからの情報取得

通信元の国・地域・ISP・組織などの属性情報を特定します

傾向分析と予測

過去の悪質IPや地理的傾向から将来的脅威を予測します

早期検出と対策

攻撃前段階でリスクの高いIPを把握し通信制限を行います

株式会社Geolocation Technology の取り組み

高度データ分析

脅威情報に対する
IP Geolocation分析を提供
しています。

アライアンス連携

LACが主導する
「SecureGRIDアライアンス」
に情報提供しています。

リアルタイム共有

IPアドレスの脅威情報を
即時共有するシステムを
構築しています。

強固な防御構築

協調型セキュリティ基盤
を補完し、防御体制向上
に貢献しています。

ソリューション紹介

お客様のセキュリティニーズに合わせた
カスタマイズ可能なソリューションをご
提案します。

株式会社Geolocation Technology

IP Geolocation技術を活用した能動的サイバー防御

Presented by
Geolocation Technolgy