1999 年 10 月１日シンポジウム「重要社会インフラのセキュリティ」　　江畑謙介

インフォメーション・ウオーフェアの脅威

１：テロの時代

●ユーゴスラビア空爆で初めて（？）実施されたサイバー・アタック戦術

「偽情報」の投入、交換、改竄によるユーゴ軍コンピュータ、レーダー映像操作

湾岸戦争が端緒となった「インフォメーション・ウオーフェア」(InforWar, IW)

米国防総省による「防御上電子的攻撃」：ブラウザーを強制閉鎖

●サイリー(Siri)グループによるインターネットのセキュリティ調査

1998 年 12 月：イスラエル、日本、ロシア、ブラジル、メキシコから８台のコンピュータを使い、214 ヶ国の 3600 万のサイトを調査（全サイトの 85%）、730,213 個のセキュリティ・ホールを発見。１万人のボランティアによるインターネット侵入監視システム(International Digital Network : IDDN)建設を提案。

米国防総省は 1999 年 12 月 15 日までに、インターネットへのゲートウエイ(gateway)を６箇所に限定して、侵入を監視する方法を採る。

●ロシアのテロ事件、キルギスの邦人拉致事件：民族、宗教、麻薬

テロの時代：プラント停止・暴走、原子力発電所（暴走せずとも停電に）

台湾の大停電：一時は中国の物理的、電子的攻撃か？とパニックに

脆弱になった現代社会：東京・大阪証券取引所のコンピュータ停止

新幹線列車集中制御装置（ＣＴＣ）の通信回線異常

中央線信号システムの故障

●価値観の編かと境界の曖昧化

冷戦の終結に伴う世界、価値観の多様化：民族、宗教、経済が中心

国家対国家の戦いから民族、集団、個人の戦いに：テロが主力手段に

境界の曖昧化：交通・情報の発達、ブロック構造の消滅（国境の希薄化：ＥＵ）

国家対個人、軍事と犯罪、軍隊と警察、時間、空間

技術の進歩：個人でも行えるテロ攻撃、社会インフラに対する（電子的）攻撃

●テロの時代

米国防総省コンピュータ・ネットワーク・ディフェンス統合タスクフォース：

５年以内に国家によるインフラに対するテロ攻撃の可能性は低いがテロ

リストによる攻撃の可能性は現在でも高い。

1996 年 10 月、イスラエル国防省はハマスが米国内でインターネットのチャットルームを使ってテロ攻撃の計画を立て、ガサ地区での共同作戦に電子メールを使用と発表。

暗号の使用により監視が困難に。

インターネットにより過激派のリクルートが。

電子取引をマネーロンダリングに利用。

コンピュータ・シミュレーションにより高度なテロ知識と兵器の扱い訓練が容易になる。

ネットワークの利用でテロ組織の分散化、少数化が可能に。

アマチュアによる「ニュー・テロリズム」の登場：ネットワーク・テロ

２：インフォメーション・ウオーフェアの種類と特徴

米国防大学（ＮＵＤ）の分類

①**指揮統制戦** (Command and Control Warfare)

②**電子戦** (Electronic Warfare)

③**心理戦** (Psychological Warfare)

④**ハッカー戦** (Hacker Warfare)

⑤**諜報基盤戦** (Intelligence-based Warfare)

⑥**経済情報戦** (Economic Information Warfare)

⑦**サイバー戦** (Cyber Warfare)

（①～③は在来型戦争方式と重複）

特徴　（１）境界が曖昧：国境（地理的条件）、時間、空間、映像

国家対個人、戦争対犯罪、戦場（前線）対後方

敵の意図・能力の特定、攻撃と戦果判定、抑止機能と報復効果

（２）少ない経費、設備で実施可能

個人でも実施ができる：軍事作戦、テロ、いたずらの判定が難しい

（３）民間施設に対する攻撃と軍事機能

軍用通信機能の民間システム依存：通信衛星、商業用コンピュータ利用

使用言語・プログラムの共用：ハッカー、ウイルスの攻撃が容易

ハッカーの例：1994 年３月「データストリーム・カウボーイ」事件

1998 年２月「ソーラー・サンシャイン」事件

1998 年 10 月「マスターズ・オブ・ダウンロード」事件

米陸軍指揮統制防護部門の調査

米国防総省のネットワーク侵入試行(hit)数は月 60～100 万件

（内１％は調査の必要がある）

毎日 100 件のアタック、その内 10%は調査対象との統計も

３：ネットワーク依存社会とセキュリティ

基本重要インフラと相互依存

通信・情報システム、電力、石油・ガス貯蔵供給、水・食糧供給、交通輸送、銀行・金融、非常時サービス、行政機能維持（これらは相互に依存）

ネットワークセキュリティ３要素

プロテクト、モニター、リアクト（法的問題）

まずプロテクトを：暗号の利用、アラート（警報）・システムの構築

参考資料：インフォメーション・ウオーフェアの種類

（米国防大学の分類に従う内容説明）

①指揮統制戦

指揮官、指揮司令部に対する攻撃：地下司令部攻撃用貫徹型兵器の開発

指揮通信システムに対する攻撃：電力供給施設に対する攻撃（ソフト爆弾）

ハッカーやコンピュータ・ウイルスによる電子的攻撃（④と重複）

偽情報の流布、投入（⑦と重複、一部③と重複）

②電子戦

通信妨害、電波妨害（広義には赤外線なども含む電磁波に利用妨害）

携帯電話の脆弱性（電波妨害、位置暴露）

③心理戦

噂、流言、宣伝ビラ、活字メディア、電波メディア、インターネットの利用または妨害

民主国家におけるメディア利用の問題

④ハッカー戦

ハッカー（主にリアルタイム)、コンピュータ・ウイルスの投入（時間差攻撃）

ハッカーによるコンピュータ・ウイルスの投入

いたずら、犯罪、軍事的攻撃の区別ができ難い

ハッカーによるホームページの書き替えは心理戦とも重複

ハッカー、ウイルスは一国の経済、交通、通信システムを破壊できる（可能性が）

複合ウイルスの開発（ＣＶＷ)：生物兵器と同様な伝播の懸念

単純な電子メール爆弾だけでインターネットを飽和できる

暗号の利用と解読の危険性

⑤諜報基盤戦

情報収集、戦場監視などのセンサーの機能妨害（②電子戦と重複）

煙幕、偽装、レーザーによる光学装置の破壊

ハッカー、ウイルスによる情報伝達、処理機能の妨害（④と重複）

電子マニュアル、データベース書き替え、破壊の危険性

ＥＭＰ(電磁パルス)による電子回路、データベースの破壊：ロシア製兵器の拡散

マイクロウエーブ兵器（ロシアでは実用化)：「非致死性兵器」と重複

⑥経済情報戦

一国、地域の経済基盤を破壊する：ユーゴスラビア攻撃（戦略爆撃）

経済インフラの相互依存増大が脆弱性を助長：通信、交通、電力、金融

インターネットへの依存率増大＝脆弱性増大？

非常事態発生時の対応期間、責任部局が曖昧に

⑦サイバー戦

サイバースペース内での戦い：情報インフラの物質的空間＋ソフトウエアの仮想空間

最も高度なインフォメーション・ウオーフェアー

偽情報の投入により相手を自由に動かす：テレビ放送の乗っ取り（③と重複）

データベースの書き替えで、戦闘シミュレーション結果を変更できる？

空中に神を出現させて大衆を動かせる？ホログラフィー技術、立体映像技術

ポケモン兵器（脳周波数に近い赤と青の点滅による平衡感覚失調）

攻撃対象となる主な重要インフラ

軍事	指揮統制システム
	防空システム
	兵器
	弾薬貯蔵所
基本重要インフラ	（遠距離）通信・情報システム
	電力
	石油・ガス貯蔵供給
	水・食糧供給
	交通運輸
	例：航空管制、航空機、整備、滑走路
	銀行・金融
	非常時サービス
	行政機能維持
その他	地理的要衝
	人員
	住居
	保安

重要インフラの相互依存性