

サイバーテロをめぐる情勢

攻撃の手口

情報通信システムは、過剰な負荷が掛かったり、不正プログラムに感染したりした場合、正常に動作しなくなってしまいます。

高度情報通信ネットワークが発達した現代社会では、政府機関を含む重要インフラの基幹システムを機能不全に陥れるサイバー攻撃（サイバーテロ）が発生した場合、国民生活や社会経済活動に重大な支障が生じるおそれがあります。

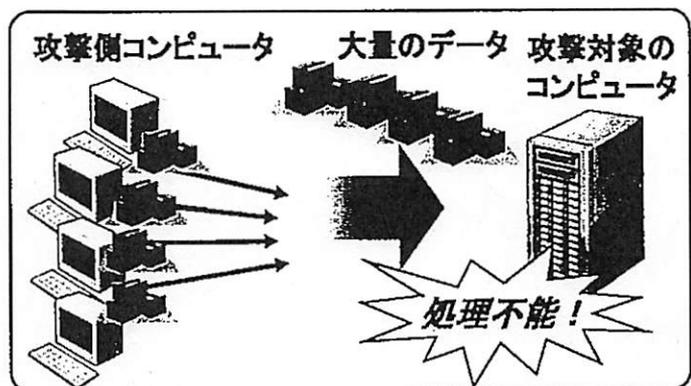
サイバーテロに用いられるおそれのある攻撃の主な手口としては、①コンピュータへのアクセス集中、②不正プログラムへの感染、③コンピュータへの不正アクセス等が挙げられます。また、これらのうち複数を組み合わせた攻撃手法も存在します。

① コンピュータへのアクセス集中 (DoS攻撃)

特定のコンピュータに大量のデータを送信して負荷を掛けるなどして、そのコンピュータによるサービスの提供を不可能にする攻撃をDoS攻撃といい、複数のコンピュータから一斉に行われるDoS攻撃をDDoS攻撃といいます。

* DoS : Denial of Service の略

DDoS : Distributed Denial of Service の略



② 不正プログラムへの感染

不正プログラムとは、コンピュータに感染し、コンピュータ内部に保存された電子データを破壊したり外部に流出させたりするなど、利用者の意図しない動作を引き起こすプログラム（コンピュータ・ウイルス等）です。電子メールの添付ファイルやUSBメモリを通じてコンピュータに侵入するなど、感染の方法は様々です。

③ コンピュータへの不正アクセス

他人のIDやパスワードを盗用したり、セキュリティ上の脆弱性を悪用することなどにより、コンピュータ内部に不正に侵入し、利用者の意図しない動作をコンピュータに命令する手口です。

第1章 【特集】サイバー攻撃の情勢と対策

基幹システムの機能障害

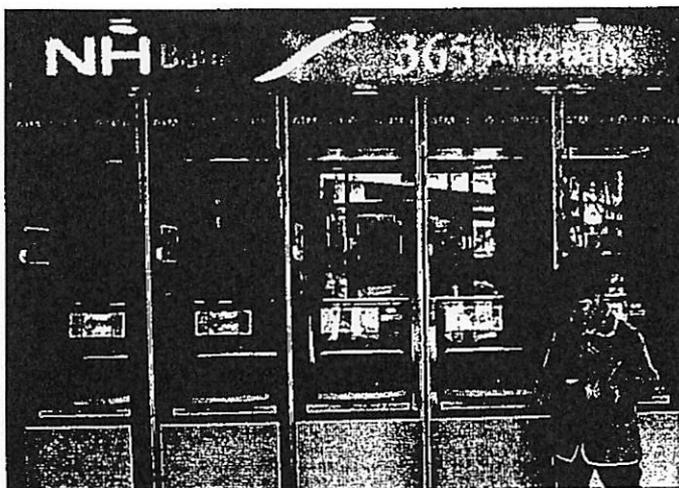
これまでのところ、我が国ではサイバーテロは発生していないものの、諸外国では金融機関のシステムや原子力発電所の制御システムの機能不全を引き起こすサイバー攻撃事案が発生しており、サイバーテロの脅威は正に現実のものとなっています。

【事例1】 韓国の政府機関等に対するサイバー攻撃(23年3月・4月)

韓国では、平成23年3月、政府機関や銀行等の40のウェブサーバ(ウェブサイト閲覧サービスを提供するコンピュータ)に対する大規模なサイバー攻撃が発生しました。

本事案では、韓国当局から捜査協力要請があったことから、警察で捜査を行った結果、我が国所在の複数のコンピュータが攻撃の踏み台となっていた可能性が高いことが判明しました。

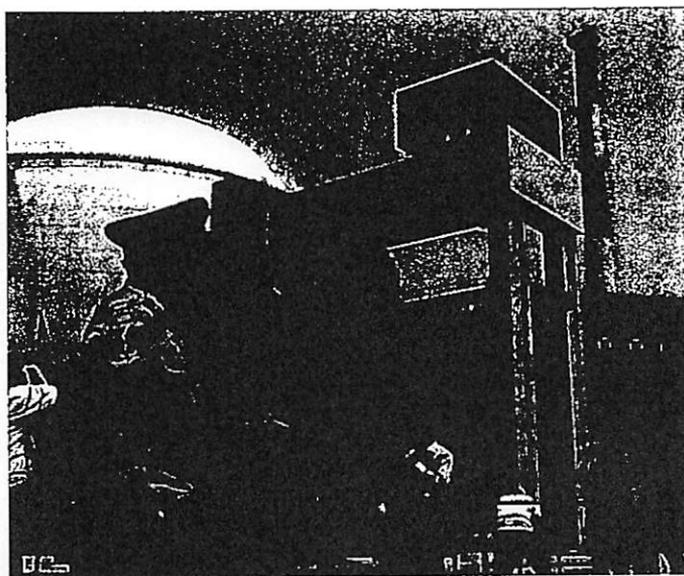
また、4月には、韓国の農業協同組合中央会の電算システムがサイバー攻撃を受け、全国の店舗の現金自動出入機で半月にわたり預金の引き出しや預け入れができなくなる事案が発生しました。いずれについても、韓国当局は北朝鮮による犯行であると結論付けており、同年2月末から実施された米韓合同軍事演習への反発であるとの見方も報道されています。



攻撃を受けた韓国の農協のATM(時事)

【事例2】 イランの原子力発電所等に対するサイバー攻撃(22年9月)

22年9月、イランの原子力発電所等のコンピュータ約3万台が、産業用システムを標的とする「スタックスネット」と呼ばれる不正プログラムに感染していた旨が報道されました。原子炉が制御不能に陥り、暴走するおそれがあった旨も指摘されています。「スタックスネット」は、インターネットに接続していないシステムにもUSBメモリ等を介して感染することがわかっています。我が国では、産業用システムにおける被害は確認されていませんが、複数のコンピュータが「スタックスネット」に感染したとされています。



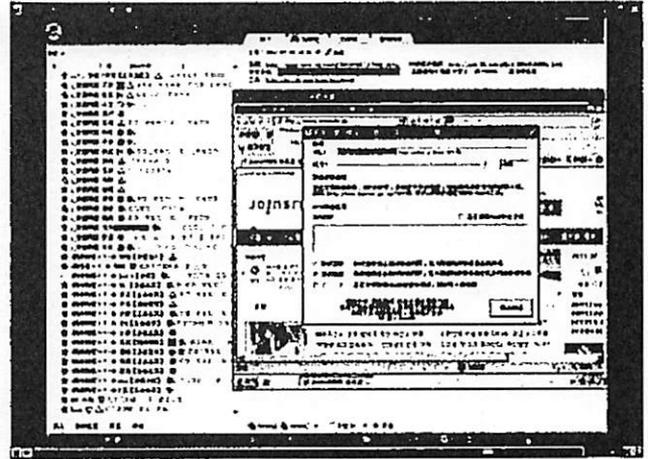
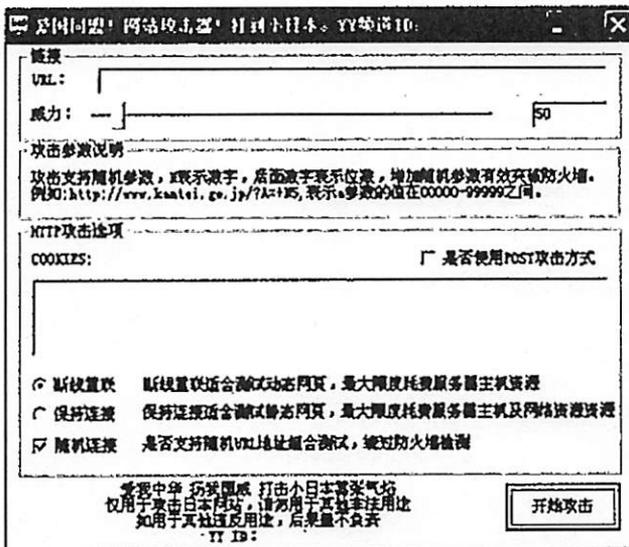
攻撃を受けたイランのブシェール原子力発電所(時事)

ウェブサイトの閲覧障害等

23 年中も、我が国の政府機関等のウェブサーバに対してDDoS攻撃がなされ、ウェブサイトの閲覧に支障が生じる事案等が続発しました。

【事例1】警察庁に対するサイバー攻撃(23年7月)

7月、警察庁のウェブサーバに対し、主に中国所在のIPアドレスから、複数の攻撃ツールを使用したとみられるサイバー攻撃が行われ、警察庁のウェブサイトの閲覧に支障が生じました。



攻撃に使用されたツール(左)と操作説明画面(右)。攻撃対象のウェブサイトのURLを入力して実行ボタンを押すだけで、攻撃対象に大量のアクセスを集中させることができます。このような攻撃ツールがインターネット上に氾濫していることが確認されています。

【事例2】人事院、内閣府等に対するサイバー攻撃(23年9月)

9月、中国の大手チャットサイト「YYチャット」等において、満州事変 80 周年を契機としたサイバー攻撃が呼び掛けられ、人事院、内閣府等に対してこれに関連したとみられるサイバー攻撃が発生し、ウェブサイトの閲覧に支障が生じました。

【事例3】東京電力株式会社に対するサイバー攻撃の呼び掛け(23年4月)

4月、国際ハッカー集団「アノニマス」は、福島第一原子力発電所事故を捉え、環境保護を名目として、インターネット上で東京電力株式会社等を標的とするサイバー攻撃(作戦名:「オペレーション・グリーンライト」)を扇動しました。



東京電力への攻撃を呼び掛けるサイト