A2／AD 環境下における サイバー空間の攻撃及び防御技術の動向 ②

木村　初夫

株式会社 NTT データ　公共システム事業本部
第一公共システム事業部　第三システム統括部　嘱託

4．サイバー空間の攻撃技術の動向

サイバー空間の攻撃技術の動向については、概要として、サイバー攻撃技術の進化と予測、サイバー攻撃プロセス、サイバー兵器のアーキテクチャ及びサイバー攻撃技術の分類について述べている。さらに、分類したサイバー攻撃技術の論理兵器、物理兵器及び心理兵器の主要な技術について述べている。

4.1　サイバー攻撃技術の概要

(1)　サイバー攻撃技術の進化と予測

サイバー攻撃技術の進化と予測については、図4.1-1に示すとおり、1980年代初めに不正ソフトウェアが出現し始めている。1990年代中頃までには、ウィルス、ワーム、トロイの木馬及び

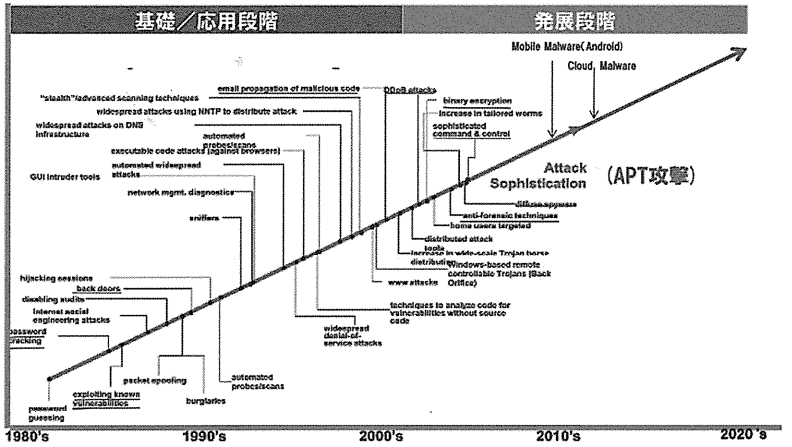


図4.1-1　サイバー攻撃技術の進化と予測

出典：Software Assurance：Mitigating Risk of Zero-Day Attacks with Software Security Automation, DHS and NIST, Oct. 31, 2011（一部加筆）

情報窃取目的のマルウェアが開発されている。2000年代初めに不法ビジネスとしての金銭目的の不正ソフトウェアの価値とその適合性が組織犯罪に認識された。2003年から2004年にかけて大量のデータや不正パケットを送りつけるなどの不正な攻撃であるDoS攻撃(サービス拒否攻撃)及び踏み台と呼ばれる複数のコンピュータが、標的とされたサーバ等に対して攻撃を行うDDoS攻撃(分散サービス拒否攻撃)の出現により不正ソフトウェアからサイバー兵器へ遷移した。さらに、2004年以降、サイバー攻撃はランダムな活動からよく計画された詳細な実施方針に基づくサイバー攻撃技術の統合化が急速に発展し、APT攻撃技術として現在に至っている[1]。また、モバイル技術及びクラウド技術の発展とともに、それらに関連する脆弱性が急増しており、APT攻撃の増加及び巧妙化が予測される。

(2) サイバー攻撃プロセス

APT攻撃のサイバー攻撃プロセスについては、Jason Andress氏等によると、表4.1-1に示すとおり、偵察、走査、アクセス、エスカレーション、情報窃取、攻撃及び維持プロセスに加えてプロセス全体に共通なプロセスとして混乱プロセスが定義されている[2]。

また、サイバー攻撃プロセスは、Kevin Coleman氏によるとJason Andress氏等のプロセスと同様に図4.1-2に示すとおり偵察、走査、システムアクセス、攻撃活動及び情報窃取プロセスとして定義されている[3]。

サイバー攻撃は、偵察及び走査で得られた目標システムに関する脆弱性情報を用いてサイバー攻撃作戦計画立案を行い、攻撃任務に対応したサイバー兵器を予め登録されているサイバー兵器庫としてのサイバー兵器登録簿から選択してサイバー攻撃設計が行われる。また、サイバー攻撃起動後の収集情報及び指示に基づいてサイバー攻撃の方法及び技法の見直し及び更新が連続的に行われる。サイバー攻撃をネットワーク速度で対応するためにはサイバー兵器登録簿及びサイバー兵器としてのマルウェアをデータベース化したサイバー兵器データベースが必要である。

表4.1-1 サイバー攻撃プロセス

プロセス	概要	備考
偵察 (Reconnaissance)	・目標環境に関する具体的レベルの情報収集 ・ソーシャルエンジニアリングによる具体的情報(共有パスワード)の収集	
走査 (Scanning)	・アプリケーションの詳細情報及びOSのシステム情報の走査 ・データベースバージョン、ユーザー名、パッチ情報等による脆弱性識別	
アクセス (Access)	・特権アクセス奪取による種々のツールと手法の使用 ・クライアント側の攻撃手段:不正Webサイト誘導、電子メール及び可搬記録媒体(USB) ・脆弱性分析ツールの使用による脆弱性識別	
エスカレーション (Escalation)	・特権アクセスのエスカレーション:垂直エスカレーション(高位レベルへの拡大)及び水平エスカレーション(同一レベルのアカウントへの拡大)	
情報窃取 (Exfiltration)	・収集情報のバックドア通信による外部からアクセスできる場所へ移動 ・または、収集情報の外部の指揮統制(C&C)サーバーへの直接送信	FTP,SCP,XMPP,HTTP等
攻撃 (Assault)	・情報作戦ドクトリンで定義されている欺瞞(Deception)、中断(Disruption)、拒否(Denial)、低下(Degradation)及び破壊(Destruction)の攻撃	
維持 (Sustainment)	・特権アクセス権奪取後の将来アクセス維持のためのアクセス環境の再構成	
混乱 (Obfuscation)	・侵入証拠の隠蔽または削除並びに調査者による誤探知	

出典:Cyber Warfare, Techniques, Tactics and Tools for Security Practitioners, Jason Andress and Steve Winterfeld, Syngress, 2011

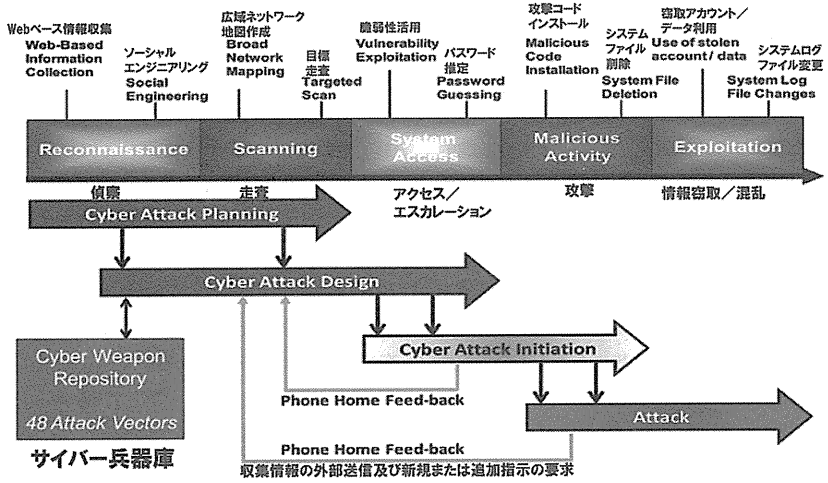


図4.1-2 サイバー攻撃プロセス

出典:The Cyber Commander's eHandbook, Kevin Coleman, technolytics, 2012

(3) サイバー兵器のアーキテクチャ

サイバー攻撃の最大の脅威であるAPT攻撃マルウェアによるサイバー兵器のアーキテクチャは、運搬システム、誘導システム及びペイロードから構成される弾道ミサイルのアナロ

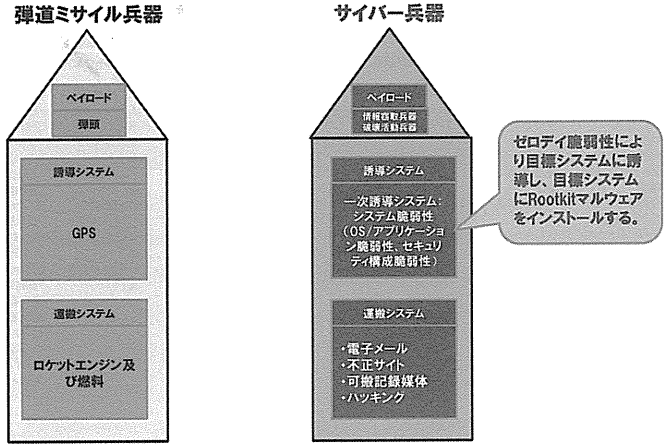


図4.1-3 サイバー兵器のアーキテクチャ

ジーに基づき、図4.1-3のように対応させることができる。この図から、OS／アプリケーション脆弱性、セキュリティ設定脆弱性が、サイバー兵器における最も重要な一次誘導システムの役割を果たすことがわかる。特に、ゼロデイ脆弱性が、目標システムの特権アクセス権限を奪取するために必須である。

(4) サイバー攻撃技術の分類

サイバー攻撃技術は、論理兵器、物理兵器及び心理兵器に分類される。さらに、論理兵器は、サイバー攻撃プロセスに基づき表4.1-2に示すとおり細分類される。物理兵器は、偽造ハードウェア及びハードウェアバックドアのサプライチェーン攻撃、HEMP(High-altitude Electromagnetic Pulse)、EMP (ElectroMagnetic Pulse) 及び HPM (High Power Microwave) の侵入電磁波攻撃、TEMPEST の漏洩電磁波盗聴、及び米空軍の航空ネットワーク攻撃システム (Suter) と米陸軍の TECWD (Tactical Electromagnetic Cyber Warfare Demnstration) 計画のような電磁サイバー攻撃に分類される。心理兵器は、ソーシャルエンジニアリングのことである。

4.2 主要なサイバー攻撃技術

(1) 論理兵器

論理兵器の主要技術としては、偵察プロセスにおいてインターネット上の標的のホスト情報収集を行う検索エンジン／検索サービス (SHODAN 及び ERIPP)、アクセス及びエスカレーションプロセスにおいて特権アクセス権限奪取のためのステルス攻撃技術 (Rootkit 及び Bootkit) 及びパスワード解析を行うパスワードツール (Thc-Hydra 及び CloudCracker) 並びに脆弱性情報収集及びエクスプロイト／ペイロード設定のための脆弱性攻撃自動化ツール (Metasploit Project 及び Immunity CANVAS)、未知の脆弱性発見のためのファジングツール、攻撃プロセスにおけるソフトウェア攻撃 (マルウェア) 及び混乱プロセスにおける位置混乱のための匿名性実現ツール (The Onion Router／Tor) がある。

表4.1-2 サイバー攻撃技術の論理兵器の分類

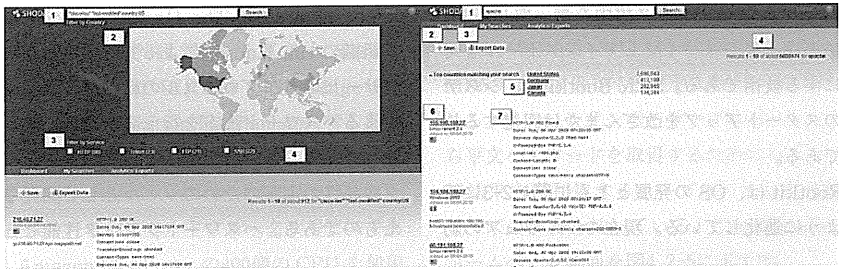
項目	偵察	走査	アクセス及びエスカレーション	情報窃取	維持	攻撃	混乱
ツール	①一般情報収集 ・Webサイト ・Google Hacking ・個人情報検索 ・SNS ②ドメイン名等検索 ・Whois ③DNS検索 ・nslookupコマンド ④ホスト検索エンジン ・SHODAN ・ERIPP ⑤メタデータ収集 ・Metagoofil ・Exiftool ・FOCA ⑥大量情報収集 ・Maltego	①セキュリティスキャナ ・Nmap ②脆弱性スキャナ ・Nessus ③Web AP 脆弱性検索エンジン ・PunkSPIDER	①ステルス攻撃ツール ・Rootkit ・Bootkit ②パスワードツール ・Thc-Hydra ・John The Ripper ・CloudCracker ③脆弱性攻撃自動化ツール ・Metasploit Project ・Immunity CANVAS ④攻撃者向けAV走査サービス ・Virtest.com ・scan4you.net ・chk4me.com ⑤ファジングツール ・DEFENSICS ・beSTORM	①物理的移転 ・超小型可撤媒体 ②暗号化及びステガノグラフィ ・暗号化 ・Puff ・Outguss ③共通プロトコル使用 ・HTTP及び種々の電子メールプロトコル ・Corkscrew ・OzymanDNS	①正規アクセス追加 ②バックドアインストール ・Netcat	①ソフトウェア攻撃 ・コマンドツール ・RAT(ホスト遠隔制御ツール) ・マルウェア ② ファームウェア攻撃 ・ファームウェア遠隔書き換え ・ドライバ改ざん	①位置混乱 ・ Onion Router (Tor) ・Bitblinder ②ログ操作 ・テキストエディタ (Unix系OS) ・Zapper (Windows系OS) ③ファイル操作 ・システム込み込みコマンド(目標システム上に自己ファイル隠蔽) ・slackerツールを有するRootkit(特権記憶領域に自己ファイル隠蔽) ・システム構成ファイルのタイムスタンプ改ざん

ア SHODAN 及び ERIPP

インターネットに接続された標的を探索するためのツールとしては、接続ノード情報の検索エンジンである SHODAN 及び通常のブラウザではすべて探索できないポート80 (Web サービス) の IP アドレスの検索サービスである ERIPP (Every Routable IP Project) がある。

SHODAN は、John Matherly 氏が2003年に構想し、2009年に開発したインターネット接続ノード検索エンジンで、バナー情報をインデックス化したものである。攻撃者の立場からは、国名、ホスト名またはドメイン、ネット (IP アドレス範囲またはサブネット)、OS、ポートを指定して、特定の脆弱性を有するホストを容易に検索することができる。SHODAN のサービス概要を図4.2-1に示す[4]。

また、SHINE(SHodan Intelligence Extraction)プロジェクトにおいて、セキュリティ研究者 Bob Radvanovsky 氏と Jake Brodsky 氏は、SHODAN を使って、インターネットに接続された制御システム関連機器を探し、約50万台の制御システム関連機器を発見している。SHINE の目的は、セキュリティ意識の向上を促すことであり、SHODAN を使用して、誰でもこれらの機器を見つけ、制御システムに不正アクセスで



SHODAN の入力画面　　SHODAN の出力結果

図4.2-1 SHODAN のサービス概要

出典：http://www.shodanhq.com/help

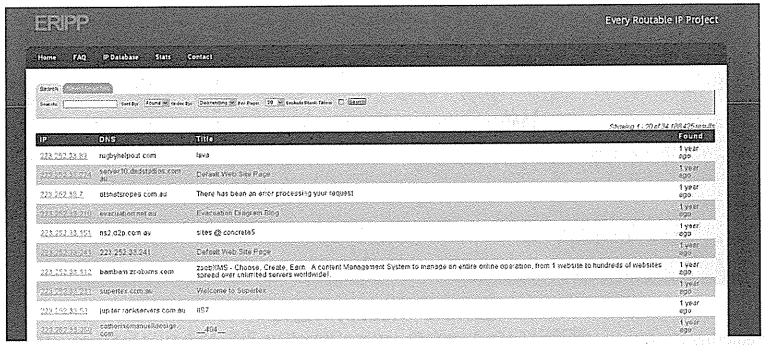


図4.2-2 ERIPP のサービス概要　　出典：http://eripp.com/

きてしまう危険性を警告することである。ICS-CERTでは、両氏からの報告を受けて調査し、米国内のものについては、最終的には約7,200が制御システム関連の機器と判明している[5]。

一方、ERIPPは、ポート80のIPアドレスをデータベース化し、その検索サービスを提供するものである。約40億の中継可能なIPアドレスに対してそれらの応答を取得できるサイトは一部であり、2013年7月31日現在の取得ホスト数は、34,188,425である。ERIPPのサービス概要を図4.2-2に示す[6]。

イ　Rootkit及びBootkit

Rootkit及びBootkitは、サイバー兵器の中でも最も検知の困難なステルス攻撃技術である。Rootkitは、特権アクセス権限を乗っ取り、追加ソフトウェアやスパイウェアインストールを可能にする技術である。また、Bootkitは、システムのスタートアップを改ざんまたは回避する技術である。

Rootkitは、OSの発展とともに図4.2-3に示すように進化している。現在のマルウェアの約10%は、Rootkitを使用している。Rootkitは32bit Windows用が最も使用されている。64bitファミリのRootkitは、まだ扱いにくい。Rootkitは、64bit OS Kernelに次に示す方法によって侵入することができる[7]。

・ドライバ信号検査のバイパス（例．試験モードの使用）
・Windowsブートパスの修正（MBR等）
・Windows kernelのKernelエクスプロイトまたはサードパーティドライバ
・正当な電子証明書の窃取（Stuxnetと同様）

一方、Bootkitも図4.2-4に示すようにOSの発展とともに進化している[8]。

ウ　パスワードツール

Thc-Hydraは、The Hacker's Choiceという組織のvan Hauserによって開発された種々のサービス及びプロトコルの行う辞書クラックによるパスワード推定を行う高速パスワードクラッカである。これは、貧弱なパスワードクラック容易性の実証のためのツールとして開発されたものである。パスワードクラック性能としては、IMAP／POP3認証で使用されているCRAM-SHA256（CRAM：Challenge-Response Authentication Mechanism）でも解読可能である[9]。

CloudCrackerは、インターネットのWeb上で提供されるパスワードクラックサービスであり、Amazon E2 Clusterの400個のCPUを使用している。解析対象パスワードとしては、WPA／WPA2、NTLM、SHA-512（Unix）、MD5（Unix）及びMS-CHAP V2（PPTP）である。また、レインボーテーブル（ハッシュから平文パスワードを取得するためにハッシュ計算結果を再利用するテーブル）として3億フレーズの辞書を持っている。CloudCrackerのホームページ画面を図4.2-5に示す[10]。

エ　脆弱性攻撃自動化ツール

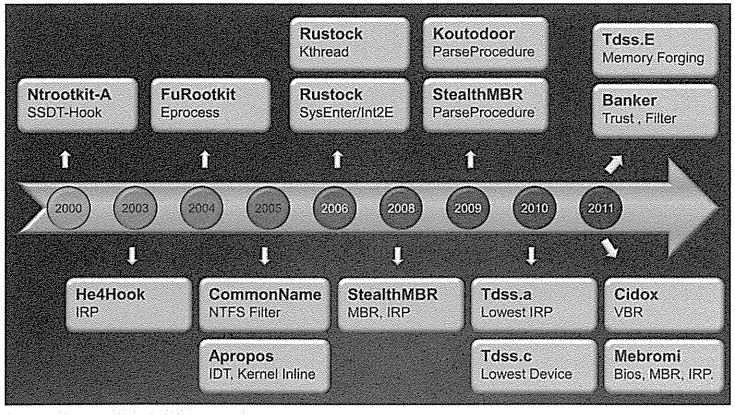
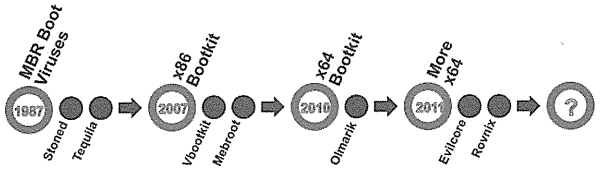


図4.2-3　Rootkitの進化

出典：Predicting the future of stealth attacks, McAfee Labs, Aditya Kapoor and Rachit Mathur, VB 2011, Oct. 5-7, 2011



○ **Bootkit PoC evolution:**
- ✓ **eEye Bootroot (2005)**
- ✓ **Vbootkit (2007)**
- ✓ **Vbootkit v2 (2009)**
- ✓ **Stoned Bootkit (2009)**
- ✓ **Evilcore x64 (2011)**

○ **Bootkit Threats evolution:**
- ✓ **Win32/Mebroot (2007)**
- ✓ **Win32/Mebratix (2008)**
- ✓ **Win32/Mebroot v2 (2009)**
- ✓ **Win64/Olmarik (2010/11)**
- ✓ **Win64/Rovnix (2011)**

図4.2-4　Bootkitの進化

出典：Modern Bootkit Trends: Bypassing Kernel-Mode Signing Policy, Aleksandr Matrosov and Eugene Rodionov, eset, VB 2011, Oct. 5-7, 2011

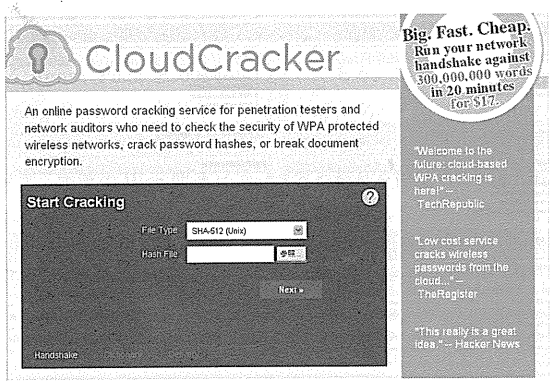


図4.2-5　CloudCrackerのホームページ画面

出典：https://www.cloudcracker.com/

情報システムの脆弱性を検査するために開発された侵入試験ツール（Penetration Test Tool）が、攻撃者の脆弱性攻撃自動化ツールとして使用され、攻撃者の攻撃技術力の障壁を低下させている。この代表的なツールとしては、Metasploit Project及びImunity CANVASがある。

Metasploit Projectは、2003年にHD Moore氏によって開発されたオープンソースセキュリティツール集であり、2009年に米国Rapid7社により買収された。現在、Metasploit Projectには、フリー版のMetasploit Framework並びに商用版としてベースライン侵入試験用のMetasploit Express及び高度侵入試験用のMetasploit Proがある。Metasploit Frameworkは、コマンドラインインタフェース(CLI)によって、nmap及びNessusのようなそれぞれネットワークスキャナ及び脆弱性スキャナを用いた目標システムの脆弱性情報収集、脆弱性を突くエクスプロイト（攻撃コード）の選定及び構成、脆弱性攻撃後に実行するペイロード(リモートシェルを含む）の選定及び構成、侵入防止システム回避のためのペイロード暗号化技術の選択、エクスプロイトとペイロードの実行を手動で行う。Metasploit Express及びMetasploit Proは、既知脆弱性及びセキュリティ設定をチェックする脆弱性スキャナであるnexposeによって脆弱性を探査し、GUIを用いて、発見した特定の脆弱性を目標としてコマンド列を実行するエクスプロイトの自動化を行うことができる。Metasploit Frameworkが保有するエクスプロイトデータベースに、Windows、Linux／Unix及びMac OS Xを対象としてエクスプロイト名、概要、ランク、作者、脆弱性参考情報（CVE等）、開発（ソースコード、履歴）、適用情報、モジュールオプションからなるエクスプロイトデータが約900件登録されている。Metasploit Proのダッシュボードを図4.2-6に示す[11]。

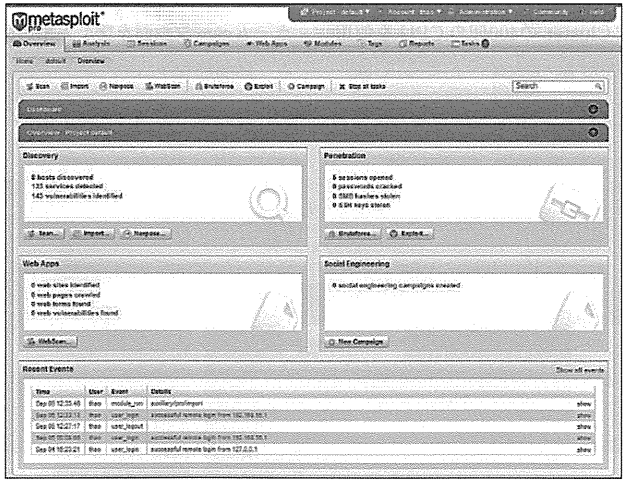


図4.2-6　Metasploit Proのダッシュボード
出典：Metasploit User Guide Release 4.5, Rapid 7

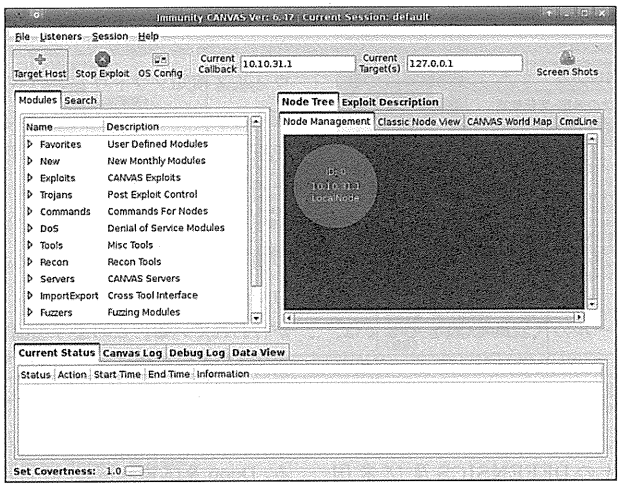


図4.2-7　Immunity CANVASのダッシュボード
出典：Tutorial : CANVAS 101 Part 1, Immunity

Immunity CANVASは、2002年設立の米国Immunity社が販売する侵入試験ツールである。Imunity CANVASのダッシュボードを図4.2-7に示す[12]。Immunity社は、この製品を全世界に販売しており、ロシアのGLEG社は、Immunity社と協業して、CANVASにアドオンして使用するゼロデイ脆弱性を含むエクスプロイトパックであるAgora Packを2008年から提供している。Agora Packは、毎月3～7モジュール程度の新しいゼロデイ脆弱性を含むエクスプロイトの提供、主流のWeb関連ソフトウェアモジュールの提供、防御の打破、データベースハッキング等の付加価値モジュールの提供、及び新しい攻撃技法の提供を行っている。現時点の最新バージョンは、Agora2.18である。また、GLEG社は、制御システムの公開された脆弱性（ゼロデイ脆弱性含む）を突くエクスプロイトを一つに集約したAgora SCADA+Packを CANVAS用に提供している。

オ　ファジングツール（Fuzzer）

ファジングツールは、ソフトウェア製品出荷前の脆弱性検査ツールであるが、ゼロデイ脆弱性発見ツールとしても使用できる。ファジング(Fuzzing)は、Wisconsin-Madison大学のBarton Miller教授が1989年にUNIXアプリケーションの堅牢性試験のために最初に適用したものである。ファジングとは、脆弱性検査の対象ソフトウェアにファズ(fuzz)と呼ばれる問題を起こしそうなデータを大量に送り込み、その応答や挙動を監視することで脆弱性を検出する検査手法である。ファジングは、バッファオーバーフロー、DoS、SQLインジェクション、クロスサイトスクリプティング（XSS）及びフォーマットストリングの脆弱性発見に有効であるが、情報漏洩、暗号化欠陥等の他の脆弱性発見には有効ではない。ファジングツールは、一般に、図4.2-8に示すようにファズの生成から送り込

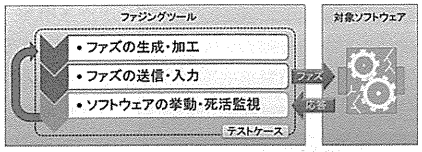


図4.2-8　ファジングツールの概要
出典：ファジング活用の手引き、IPA、2012年９月

み、ソフトウェアの監視まで自動化されている[13]。

ファジングツールの代表的COTSとしては、フィンランドのOulu大学セキュアプログラミンググループ（OUSPG）のPROTOS試験ツール研究成果に基づき2001年に設立されたCodenmicon社のDEFENSICS及び米国Beyond　Security社のbeSTORMがある。DEFENSICSは、200以上の異種通信プロトコル、ファイルフォーマット及びXMLアプリケーションをサポートするゼロデイ脆弱性発見のためのファジングツールである。beSTORMは、有効な入力覆域をサポートする優先度アルゴリズムに基づくファジングツールであり、既知の通信プロトコルだけでなく、特別な要求に基づく通信プロトコルもカスタマイズできる[14)15)]。

カ　マルウェア

ソフトウェア攻撃に使用されるマルウェアは、「NIST SP 800-83 Revision 1マルウェアインシデント防止及び対処指針」によると自己複製能力、自己完結性及び混合性に基づき、プログラム及びデータに伝染し自己複製能力を有するウィルス、自己完結性及び自己複製能力を有するワーム、自己完結性及び非複製のトロイの木馬、不正なモバイルコード及び混合攻撃に分類される。ウィルスは、プログラム及びデータを媒介として病原体の特性と同様に広範囲に拡散する[16)]。また、高度なマルウェアとしては、商用ソフトウェア製品のゼロデイ脆弱性を利用したAPT攻撃マルウェア、シグネチャーベースウィルス検知ソフトウェアの不正コード検知回避のためにソフトウェアコードの暗号化／復号化を行うマルウェア及びサーバ側多相性を用いた不正コード自動変更マルウェアがある。

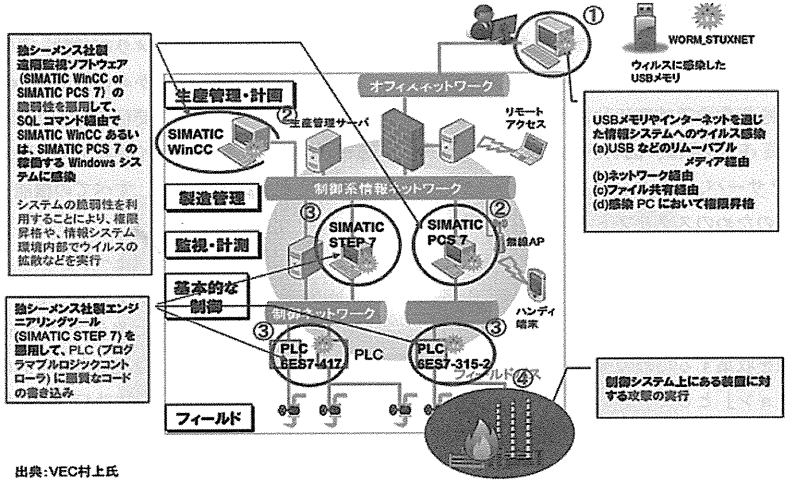
ゼロデイ脆弱性を含むAPT攻撃マルウェアの開発には、豊富な資金による組織的な開発能力が必要であり、国家をスポンサーとする開発が行われている。このような国家主導開発の代表的なAPT攻撃マルウェアとしては、表4.2-1に示すとおり破壊活動目的のStuxnet並びに情報窃取目的のDuqu、Flame及びGaussがある。Duqu及びFlameはStuxnetからの派生であり、GaussはStuxnetとFlameの両方からの派生として開発されている。Stuxnet、Flame及びGaussは、Windowsシェルの脆弱性を利用してマルウェアのUSBメモリ拡散が可能となっている[17)18)19)20)21)]。

StuxnetによるAPT攻撃は、「制御システム運用者の制御システムのディスプレイの表示情報に対する信頼の特性（弱点）」と「制御システムの監視・計測データのUSBメモリによるオフィス系（オープン系）との情報共有（弱点）」を狙って、マルウェア拡散及び権限昇格に必要な４個のゼロデイ脆弱性を活用して情報欺瞞及び破壊活動を行ったものである。Stuxnetは、図4.2-9に示すとおりインターネットに接続されたオープン系のオフィスネットワーク経由で業務パソコンがマルウェアに感染し、USBメモリ経由でクローズ系の制御系情報ネットワーク上の独シーメンス社製遠隔ソフトウェアの脆弱性を利用してWindowsの特権アクセス権限奪取及びマルウェア拡散並びに制御系情報ネットワークの情報欺瞞を実行した。さらに、独シーメンス社製エンジニアリングツールを利用して

表4.2-1　国家主導開発のAPT攻撃マルウェア

項目	Stuxnet	Duqu	Flame	Gauss
発見年月	2010年7月	2011年10月	2012年5月	2012年8月
攻撃目的	破壊活動 （制御システムの破壊）	情報窃取	破壊活動のための情報窃取（大量情報）	情報窃取（大量情報）
攻撃対象（オープン系／クローズ系）	オープン系／クローズ系	オープン系	オープン系／クローズ系	オープン系／クローズ系
能力	・ネットワーク共有拡散 ・P2P ・USB拡散 ・PDF拡散 ・ウィルス対策API検出回避 ・Windows用ルートキット ・PLC用ルートキット ・サーバー検出 ・バックドア通信（HTTP） （注1）	・ルートキット ・情報収集（システム情報、ネットワーク情報、キーストローク、スクリーンショット） ・送受信データ暗号化 ・バックドア通信（HTTP、HTTPS、Custom） ・時限自己削除（36日） （注2）	・ネットワーク共有拡散 ・USB拡散 ・HTTPサーバー ・SQL　DBサーバー ・Proxyサーバー ・バックドア通信（HTTPS） ・スクリプトインタプリタ（Lua） ・アプリケーションストア ・Bluetooth ・Cell ・情報収集（システム情報、ネットワーク情報、利用者情報、各種ファイル、ファイルメタデータ、AP、ネットワークトラヒック情報） （注3）	・USB拡散 ・情報収集（利用者パスワード、クッキー及びブラウザー履歴、ネットワーク情報、プロセス情報、フォルダ情報、BIOS情報、CMOS RAM情報、媒体情報） ・窃取情報暗号化 ・バックドア通信（HTTPS） ・追加モジュールダウンロード ・暗号化ペイロード（機能不明） （注4）
ゼロデイ脆弱性	使用	使用	使用	使用
相互関係（注5）	オリジナル	Stuxnetから生成	Stuxnetから生成	Stuxnet及びFlameから生成
規模 （ファイルサイズ）	500kB（15ks）	500kB	20MB	200KB（主モジュール）

注1. Symantec Security Response, "W32.Stuxnet", July 13, 2010
注2. Symantec Security Response, "W32.Duqu", November 23, 2011
注3. Symantec Security Response, "W32.Flamer", June 5, 2012
注4. Kaspersky Lab Global Research and Analysis Team, "Gauss: Abnormal Distribution", Kaspersky Lab, August 9, 2012
注5. Kaspersky Lab Expert,"Gauss: Nation-state cyber-surveillance meets banking Trojan", Kaspersky Lab, August 9, 2012



出典：VEC村上氏

図4.2-9　StuxnetによるAPT攻撃（破壊活動）の手法
出典：制御システムの今あるセキュリティ脅威と対策について、IPA、IPAグローバルシンポジウム、2012年５月24日

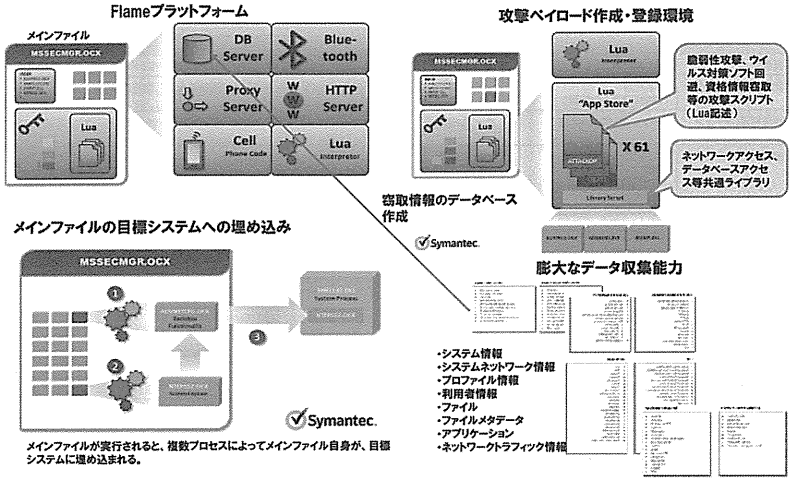


図4.2-10　Frameによる APT 攻撃（大規模情報窃取）の手法

出典：W32.Flamerについての詳しい続報、Symantec、2012年6月5日

PLC（プログラマブルロジックコントローラ）の特定のメモリ領域にマルウェアを挿入し、制御システム上にあるウラン濃縮用遠心分離機の回転数を操作する破壊活動の攻撃を実行した[22]。

一方、Flameは、図4.2-10に示すとおりHTTPサーバ、DBサーバ、Proxyサーバ、命令変更のためのスクリプトインタプリタとアプリケーションストア、Bluetooth及び大規模情報収集管理機能を有し、ファイルサイズもStuxnetの40倍になっている。侵入先から膨大な情報を収集するためのモジュールは、「アプリケーション」としてアプリケーションストアからダウンロード及び更新が可能である。Flameは初期段階でいくらかの予備情報を収集し、その情報に基づいてさらにデータの収集を続ける。たとえば、Flameには、文書の要約データであるメタデータだけを先に抽出する機能がある。攻撃者は、そのメタデータに基づいて文書の内容に興味を持った場合、文書全体を抽出する。

また、Flameは、Bluetooth無線技術によるコンピュータのマイク／カメラの起動、キーボード操作のログ記録、画像から位置情報の抽出及びコマンド／データの送受信を行うことができる[23]。Gaussは、暗号化ペイロードの暗号解読ができていないため、まだ、すべての機能が把握できていない。

キ　Onion Router／Tor（トーア）

Onion Router／Torは、インターネット上の通信匿名性保証のために米海軍調査研究所（NRL）が開発したものである。本来目的の用途は、米海軍のOSINT収集、法執行機関の監視及びインテリジェンス収集、組織及び個人のプライバシー、及び通信の秘密保護であるが、現在、インターネット上で公開されており、匿名性技術として攻撃者に利用されている。この原理は、図4.2-11に示すとおり複数ノード経由で「たまねぎ状」の多層仮想回線接続により匿名性を実現する[24][25]。

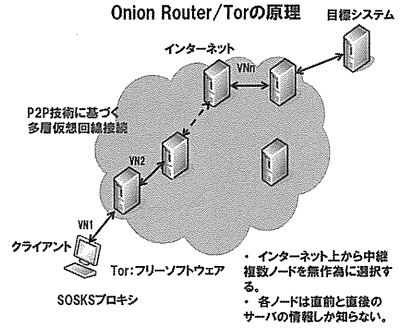


図4.2-11　Onion Router／Torの原理

(2)　物理兵器

物理兵器の主要技術としては、本論文では、電子戦技術を除いて、サプライチェーン攻撃技術及び電磁波利用攻撃技術に絞って、偽造ハードウェア及びハードウェアバックドア並びに航空ネットワーク攻撃システム（Suter）及びTECWD計画について述べる。

ア　偽造ハードウェア[26]

偽造ハードウェアの代表事例としては、「Cisco Routerに関するFBI犯罪調査報告書（2008年1月11日）」によると、Ciscoのルータ、スイッチ、ギガビットインタフェースコンバータ及びWANインタフェースカードの偽造がある。図4.2-12に示す写真の偽造ルータと正規品ルータを価格で比較すると、それぞれ＄234及び＄1,375であり、偽造ルータは約1／6の価格である。偽造ルータの問題としては、次の点が挙げられている。

・低製造標準
・高故障率
・ルータ及びスイッチの二重MACアドレスによる全ネットワークのシャットダウン（ピッツバーグにおける利用者LANの二重MACアドレスによるシャットダウン（2002年））

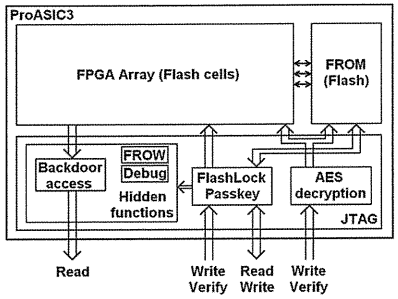
イ　ハードウェアバックドア

ハードウェアバックドアの事例としては、ケンブリッジ大学計算機研究所が初めて発見した軍用フラッシュFPGA（Field Programmable Gate Aray）に埋め込まれたバックドア並びにX86系マシンのセキュリティ脆弱性を利用したハードウェアバックドアの実証例がある。

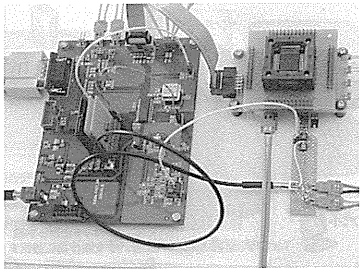
中国で生産されたCiscoルータ偽造品の例

図4.2-12　偽造ハードウェアの例

出典：http://www.usedcisco.com/press-my-esm_used_cisco_identifying_fake_chisco.aspx



ICチップの構造



ハードウェアバックドア検出環境

図4.2-13　軍用ICチップのハードウェアバックドア

出典：Breakthrough silicon scanning discovers backdoor in military chip, Sergei Skorobogatov and Christopher Woods, University of Cambridge, CHES 2012 Workshop, Sept. 9-12, 2012

前者は、図4.2-13に示すとおりActel／Microsemi社の軍用の高信頼ICチップであるProASIC3 A3P250 FlashFPGAに隠蔽機能を埋め込んだものであり、隠蔽機能のアクセス解除には、バックドアキーが使用されている。また、AES暗号器は、FROMフラッシュの送信データのみを暗号化している。パスキーはFROMフラッシュの読み取りだけを解除している[27]。

一方、後者は、図4.2-14に示すとおり、一般的なX86系マシンにCoreboot（公式にはLinuxbios）、SeaBios（16bit x86Biosのオープンソース実装）及びiPXE（オープンソースブートファームウェア）を含むクリーンなBIOSファームウェア及びOS独立のBootkitを組み込んだRakshasaアーキテクチャは、どのようなOSに対してもセキュリティレベルを下げて、バックドアとしてのペイロードをリモートブートできる。現在、Rakshasaアーキテクチャは、230のマザーボードをサポートし、Bootkitとし

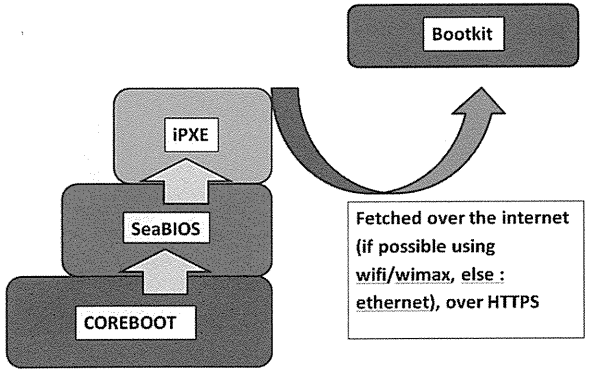


図4.2-14　X86系マシンのハードウェアバックドア（Rakshasa）

出典：Hardware Backdooring is pratical, Jonathan Brossard, Toucan System, DEFCON 20, July 28, 2012

てPiotr Bania氏作成のKonbootの使用によりWindows 32bit／64bitのどのバージョンに対してもブートキット化が可能である。2012年7月に米国で開催されたBlackHat 2012及びDEFCON20において、このBIOSまたはPCIファームウェアのバックドアによって、HTTP接続によるリモートペイロードのブートが隠密にできることを実証した[28]。したがって、このようなハードウェアバックドア作成は技術的に可能であり、最近、米国の下院情報特別委員会報告書でも問題提起されているように中国の通信機器会社による通信機器のハードウェアバックドアの潜在的可能性があると考えられる。

ウ　航空ネットワーク攻撃システム（Suter）[29]

Suterは、彼の防空システムに電磁波利用によって侵入し、情報監視、制御奪取及び目標情報の欺瞞を行う米空軍の航空ネットワーク攻撃システムである。これは、彼の防空システムに対する電磁波利用による出力データ監視部及び入力データ挿入部から構成される。出力データ監視技術によって、彼のレーダーが監視している目標情報を我のオペレータが監視することができる。また、入力データ挿入技術によって、マルウェアを挿入し、我のオペレータが彼の防空システムの制御奪取及び目標情報の欺瞞を行うことができる。出力データ監視用プラットフォームには、KC-135 Rivet Joint SIGINT機がある。入力データ挿入用プラットフォームには、EC-130 Compass Call電子妨害機がある。また、Suterは米空軍の無人機にも搭載されている。さらに、新しい技術としては、移動弾道ミサイルランチャのような時間制約があり戦術的に捕捉困難な目標の管制ネットワーク侵入技術が開発されている。

イスラエルは、2機の新型Gulfstream G550特殊任務航空機モデルを導入した時、Suterと同様のシステムアーキテクチャを複製したものと見られている。1機は、彼の電子信号を監視するものであり、他の1機はフェイズドアレイレーダーから侵入データを送信するものである。

特に、入力データ挿入技術を開発するためには、電磁波利用によるパケットで彼の防空システムに侵入するための監視ネットワークのインタフェース仕様並びに特権アクセス権限奪取のために脆弱性を特定する処理装置のハードウェア及びソフトウェア構成仕様に関する情報を事前にインテリジェンス活動等により取得しておく必要があると考えられる。

エ　TECWD計画[30]

TECWD（Tactical Electromagnetic Cyber Warfare Demonstrator）計画は、2012年11月28日に米陸軍のI2WD（Intelligence and Information Warfare Directorate）が秘密会議で発表した、「クローズ系のシールドされた有線ネットワークから航空プラットフォーム及び陸上プラットフォームの電磁波利用によりデータ挿入及びマルウェア挿入並びに情報窃取を行う」デモンストレーションの種々のタスクを実行できるレディメードシステムの開発計画である。この技術は電磁サイバー戦のための技術であり、情報窃取は電磁場の歪みを検知するTEMPESTが基本となっている。また、電磁波利用によるデータ挿入及びマルウェア挿入は、理論的には、有線ケーブルはアンテナとして動作するので、電磁信号を設計し当該ケーブル上を伝送させることができる。専門家によると、現在、このような技術は存在するが、まだ、データ挿入には主に近接性と帯域において制約があり、複雑なデータには挿入のための長い期間が必要であると言われている。

(3)　心理兵器（ソーシャルエンジニアリング）[31]

ソーシャルエンジニアリング（Social Engi-

neering：SE)は、標的とする人間の行動に影響を及ぼす技法（騙し技法）であり、標的とする情報システムへのアクセス権限を奪取するために彼の感情の操作、または彼の信頼獲得及び裏切りを介して行うものである。これは、電話、電子メール、SNS（Social Networking Site）または種々の手段を用いて人間において実行されるものである。SE攻撃の目標は、関係の創成、標的の信頼獲得及び標的に対するセキュリティポリシーを逸脱する行動または情報提供の強制である。このSE攻撃は、APT攻撃の偵察段階において使用される技法である。

SEによる標的へのアプローチには、攻撃度の低い程度から観測（Observe）、会話（Conversation）、インタビュー（Interview）、尋問（Interrogation）及び拷問（Torture）がある。最初は、電子的または物理的観測である。2番目は、攻撃者が標的の人間を決定するための電子、電話または人での会話である。3番目は、インタビューまたは尋問であり、標的を攻撃者に服従させるものである。これは、意思決定のために必要な情報のカスタマーであることを詐称して行う。これらのすべてのアプローチには、信頼に基づく関係の構築が必要である。最後に、拷問があるが、これはSEの範囲外である。

参考文献

1）DHS and NIST：Software Assurance：Mitigating Risk of Zero-Day Attacks with Software Security Automation, 31 Oct. 2011
2）Jason Andress and Steve Winterfeld：Cyber Warfare：Techniques, Tactics and Tools for Security Practitioners, Syngress, 2011
3）Kevin Coleman：The Cyber Commander's eHandbook, Version 3, technolytics 2012
4）SHODAN：http://www.shodanhq.com/、2013年2月1日アクセス
5）ICS-CERT：ICS-CERT Monthly Monitor, October／November／December 2012
6）ERIPP：http://eripp.com/、2013年2月1日アクセス
7）Aditya Kapoor and Rachit Mathur：Predicting the future of stealth attacks, McAfee Labs, VB 2011, 5-7 Oct. 2011
8）Aleksandr Matrosov and Eugene Rodionov：Modern Bootkit Trends：Bypassing Kernel-Mode Signing Policy, eset, VB 2011, 5-7 Oct. 2011
9）Thc-Hydra：http://www.thc.org/thc-hydra/、2013年2月1日アクセス
10）CloudCracker：https://www.cloudcracker.com/、2013年2月1日アクセス
11）RAPID7：Metasploit Pro User Guide Realease 4.5, 6 Dec. 2012
12）Immunity：Tutorial：CANVAS 101 Part 1：http://www.immunityinc.com/documentation/tutorials/canvas101-part1.pdf、2013年2月1日アクセス
13）IPA：ファジング活用の手引き、2012年9月
14）Codenmicon：Defensics：http://www.codenomicon.com/resources/whitepapers/Defensics_Brochure.pdf、2013年2月20日アクセス
15）Beyond Security：beSTORM Fuzzer Whitepaper：http://www.beyondsecurity.com/bestorm_whitepaper.html、2013年2月20日アクセス

16）NIST：NIST SP800-83 Guide to Malware Incident Prevention and Handling for Desktops and Laptops, Revision 1, July 2013
17）Symantec Security Response, "W32.Stuxnet", 13 July 2010
18）Symantec Security Response, "W32.Duqu", 23 November 2011
19）Symantec Security Response, "W32.Flamer", 5 June 2012
20）Kaspersky Lab Global Research and Analysis Team, "Gauss：Abnormal Distribution", Kaspersky Lab, 9 August 2012
21）Kaspersky Lab Expert, "Gauss：Nation-state cyber-surveillance meets banking Trojan", Kaspersky Lab, 9 August 2012
22）IPA：制御システムの今あるセキュリティ脅威と対策について、IPAグローバルシンポジウム、2012年5月24日
23）Symantec：W32.Flamerについての詳しい続報、2012年6月5日
24）Jason Andress and Steve Winterfeld：Cyber Warfare：Techniques, Tactics and Tools for Security Practitioners, Syngress, 2011
25）Tor project：Tor Overview：https://www.torproject.org/about/overview.html.en、2013年3月19日アクセス
26）Raul Roldan：FBI Criminal Investigation：Cisco Routers, FBI, 11 Jan. 2008
27）Sergei Skorobogatov and Christopher Woods：Breakthrough silicon scanning discovers backdoor in military chip, University of Cambridge Computer, Laboratory, CHES 2012 Workshop, 9-12 Sept. 2012
28）Jonathan Brossard：Hardware Backdooring is practical, Toucan System, DEFCON 20, 26-29 July 2012
29）Richard B Gasparre：The Israeli 'E-tack' on Syria−Part II, airforce-technology.com, 11 March 2008
30）Zachary Fryer-Biggs：DoD Looking to 'Jump the Gap' Into Adversaries' Closed Networks, DefenseNews, 15 Jan. 2013
31）Christopher Hadnagy：Social Engineering：The Art of Human Hacking, Wieley Publishing, Inc., 2011