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 ①

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

1．はじめに

軍事における情報通信は、指揮中枢から末端部隊に至る指揮統制のための基盤であり、IT 革命によって情報通信ネットワークへの依存度が増大している。このような軍事の情報通信ネットワークへの依存を狙って、多くの外国軍隊がサイバー空間における攻撃能力を開発している。また、国家主体によるサイバースパイ活動として他国の情報通信ネットワークへの侵入及び情報窃取並びに重要インフラ等の制御システムへの脆弱性攻撃による破壊活動が行われている。このような状況において、国家主導開発による高度なマルウェアを用いた APT（Advanced Persistent Threat）攻撃の出現により、サイバー空間における脅威レベルが飛躍的に上昇している。我が国においても、立法府、政府機関、防衛関連の民間企業等が情報窃取目的の APT 攻撃を受けている。

米国では、2008年の国防総省の SIPRNET に接続された情報システムへの APT 攻撃を契機に2010年10月にサイバー軍が創設されている。また、2011年７月に公表された「国防総省サイバー空間作戦戦略」では、外部の脅威行為者及びインサイダーからのサイバー脅威、サプライチェーンの脆弱性等に対応するために、サイバー空間の作戦領域化、サイバー防御のための新しい防衛作戦概念である能動サイバー防衛（Active Cyber Defence）の採用等の５つの戦略方針を挙げている。能動サイバー防衛とは、サイバー脅威と脆弱性の発見、探知、分析及び軽減する国防総省の同期化されたリアルタイム能力である。さらに、2012年１月に公表された「新国防戦略」では、サイバー攻撃による情報の欺瞞や遮断並びに高強度電磁波兵器による電子機器の破壊までを含むネットワークアクセス阻止攻撃を手段とした彼の接近阻止／領域拒否（A2／AD）戦略への対応の１つとして、ネットワーク中心戦（NCW）に不可欠な通信ネットワークを含むサイバー空間及び宇宙アセットへのアクセスの実効性の確保を挙げている。

このようなサイバー空間の状況において、サイバー空間を防御するためには、サイバー攻撃は完全には防御できないという基本的考え方による情報セキュリティリスク管理に基づくサイバー空間の彼の脅威及び我の脆弱性のリアルタイム状況認識が必要である。さらに、これらの

リアルタイム状況認識により任務及び業務レベルのリスクアセスメントに基づく適時な意思決定を支援できる。

従来、サイバー空間の脅威の状況認識能力については、整備が行われてきたが、ネットワーク速度のAPT攻撃に実効性のあるリアルタイムな脆弱性の状況認識能力の実現が必要である。我が国でも、静的な定期的情報セキュリティ監査に基づく脆弱性の状況認識から米国が推進しているセキュリティ常時監視（Continuous Monitoring）に基づくリアルタイムな脆弱性の状況認識への革新が必要である。

本論文では、このような背景を踏まえて、サイバー空間の脅威の動向、サイバー攻撃に対する脆弱性の動向、サイバー空間の攻撃技術の動向、サイバー空間の防御技術の動向及びA2／AD環境下における米軍のサイバー関連技術動向について紹介する。

2．サイバー空間の脅威の動向

A2／AD（接近阻止／領域拒否）環境下のサイバー空間の脅威を導出するために、サイバー脅威の一般動向及び軍事分野のサイバー脅威動向について分析・整理した結果を述べる。

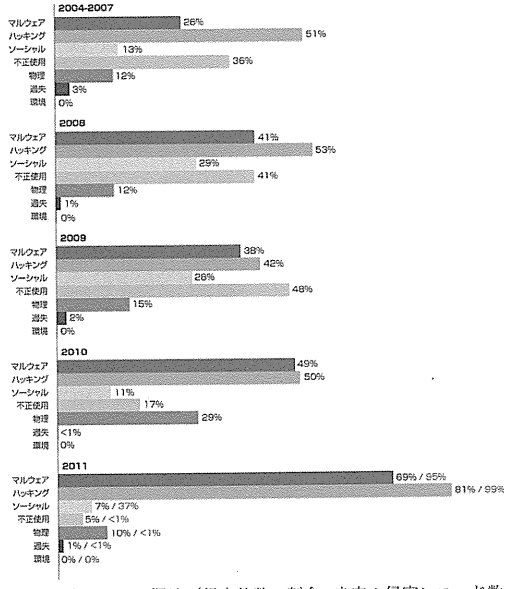
2.1　サイバー脅威の一般動向

サイバー脅威の一般動向については、サイバー脅威の現状、最大のサイバー脅威であるAPT（Advanced Persistent Threat）攻撃の国内及び国外の現状及び主要な民間セキュリティ会社による2012年のサイバー脅威の予測情報に基づき、今後の想定されるサイバー脅威を示している。

ア　サイバー脅威の現状

サイバー脅威の現状については、米国ベライゾン社の発表した「2012年度データ漏洩／侵害調査報告書」によると、図2.1-1に示す脅威アクション・カテゴリ別では、マルウェアが年々増加し2011年度では約70％を占めている。不正使用（インサイダー）は、セキュリティ対策の実施により減少しているが、影響の大きな脅威である。物理的脅威は、物理的な改変であるタンパリングの割合が高い。また、図2.1-2に示すマルウェアの機能別発生傾向から、その2／3は情報窃取型APT攻撃マルウェアであり、1／4は破壊活動型APT攻撃マルウェアであることがわかる。情報窃取型APT攻撃マルウェアは、ユーザのキー操作を監視して、パスワードなどの入力データを収集するソフトウェアであるキーロガー／ユーザの行動や個人情報などを収集するソフトウェアであるスパイウェア、データの送信及びバックドアに相当する。一方、破壊活動型APT攻撃マルウェアは、セキュリティ管理策の無効化及び妨害に相当する[1)]。

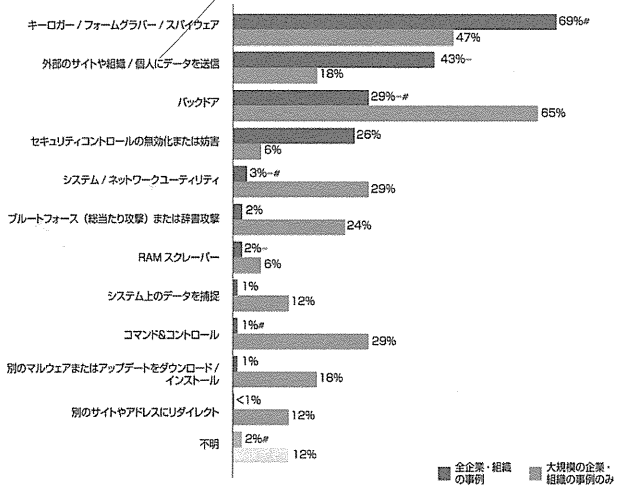
APTという用語は、2006年に米空軍の分析者が、民間関係者とサイバー侵入活動の議論を円滑にするために作った用語である。APTのそれぞれの構成単語は、「Advanced：敵の独自な情報窃取能力の開発力」、「Persistent：敵が任務達成を意図していること」及び「Threat：組織的な資金提供に基づく敵の脅威」を意味している[2)]。APTの攻撃目的は、当初は情報窃取



注．黒字：データ漏洩／侵害件数の割合、赤字：侵害レコード数の割合

図2.1-1　脅威アクション・カテゴリ別発生傾向

出典：2012年度データ漏洩／侵害調査報告書、ベライゾン社、2012年



注．① 情報窃取型APT攻撃マルウェア：キーロガー／スパイウェア、データの送信及びバックドア

② 破壊活動型APT攻撃マルウェア：セキュリティ管理策の無効化または妨害

図2.1-2　マルウェアの機能別発生傾向

出典：2012年度データ漏洩／侵害調査報告書、ベライゾン社、2012年

目的であったが、現時点では、破壊活動目的も含むものと考えられる。我が国では、APT攻撃は、執拗な標的型攻撃と呼ばれている。

イ　国内外の主要なAPT攻撃事例

国内の主要なAPT攻撃事例は、メール添付型の情報窃取目的がほとんどであり、2011年の防衛関連企業事例、2012年の政府機関事例（JAXA、農林省、特許庁、原子力安全基盤機構、財務省）がある。警察庁の報告によると、2012年上半期に報告されたメール添付型APT攻撃件数は、552件（2011年4月から2012年6月：1,604件）で、バックドア接続先は中国が36%で最も多い[3]。

国外の主要なAPT攻撃事例は、表2.1-1に示すとおり「クローズ系のセキュリティの安全神話」を崩壊させた可搬媒体利用型の情報窃取APT攻撃であるOperation Buckshot Yankee（攻撃対処作戦名）、Flame及びGauss並びに可搬媒体利用型の破壊活動APT攻撃であるStuxnetがある。Operation Buckshot Yankeeは、米国防総省のSIPRNETに接続される情報システムから兵器設計情報、作戦計画及び監視情報を大量に窃取したものであり、米国サイバー軍創設の契機となったAPT攻撃事例である。

Stuxnetは、2012年6月1日のニューヨークタイムズ紙（電子版）によると、ジョージ・ブッシュ政権時代にイランの核兵器開発を遅らせるために開始された秘密工作「オリンピックゲーム」のサイバー攻撃手段として米国とイスラエルが共同開発したものであると言われている[4]。Stuxnetは、イランのナタンズ核施設の地下に設置されたウラン濃縮用遠心分離機の可変周波数装置を最終標的として、4個のゼロデイ脆弱性を用いてオープン系及びクローズ系の両方に侵入し、9,000台の遠心分離機の内1,000台を破壊し、イランの核兵器開発能力を一時的に低下させたと見られている[5]。また、Flameも、2012

表2.1-1　国外の主要なAPT攻撃事例

攻撃事例	報告年	開始年	攻撃型	攻撃目的	標　的
Operation Buckshot Yankee	2010	2008	可搬媒体利用型	情報窃取	米国国防総省（DoD）のSIPRNETに接続される情報システム（兵器設計情報、作戦計画及び監視情報）
Operation Aurora	2010	2009	不審サイト誘導型	情報窃取	Googleを含む30以上の企業（ソフトウェア構成管理システム）
Stuxnet	2010	2010	可搬媒体利用型	破壊活動（遠心分離機の破壊）	イランのナタンズ核施設（ウラン濃縮用遠心分離機の可変周波数装置）（マルウェアの不具合によりインドネシア、インド、アゼルバイジャン、米国、パキスタン等の標的以外の国にも拡散）
Ducu	2011	2011	メール添付型	情報窃取	制御システムメーカからの情報収集を目的とした特定の国の組織（仏、蘭、スイス、ウクライナ、インド、イラン、スーダン、ベトナム）
Night Dragon	2011	2009	Webサイト侵入型	情報窃取	エネルギー、石油業界、ペトロケミカル
Operation Shady RAT	2011	2006	メール添付型	情報窃取	米国等政府機関、情報技術、電子技術、衛星・通信、防衛、エネルギー、NGO、財務等の71組織（米国：49組織）
Nitro	2011	2011	メール添付型	情報窃取	化学、国防、人権NGO、自動車企業
Lurid/Enfal	2011	2006	メール添付型	情報窃取	旧ソ連の宇宙関連機関
Luckycat	2012	2011	不審サイト誘導型	情報窃取	インド及び日本の航空宇宙、エネルギー、軍事研究、運輸、エンジニアリング、チベット活動家
IXESHE	2012	2009	メール添付型	情報窃取、データ改竄または破壊活動	東アジア圏の政府機関、台湾の電機企業、ドイツの電気通信事業会社
Flame	2012	2007	可搬媒体利用型	破壊活動のための情報窃取（大規模情報収集）	イランの核施設の攻撃のための情報収集を目的とした特定の組織
Gauss	2012	2011	可搬媒体利用型	情報窃取他（暗号化されたペイロード能力不明）	レバノン、イスラエル、パレスチナ等の中東地域のオンラインバンキング
Shamoon	2012	2012	共有ファイル利用型	破壊活動（ファイル消去、MBR使用不能）	サウジアラビアのエネルギー企業（Saudi Aramco）（社内業務ネットワークの3万台のワークステーションに感染）、カタールの天然ガス会社（RasGas）
Elderwood	2012	2009	メール添付型／不審サイト誘導型	情報窃取	国防産業、人権関連NGO等
Operation Red October（ROCRA）	2013	2007	メール添付型	情報窃取	旧ソ連構成国、中央アジア、東欧諸国等の政府機関、外交機関・大使館、研究機関、貿易機関、核・エネルギー研究所、石油・ガス会社、航空、軍事組織
APT1/Comment Crew, Comment Group	2013	2006	メール添付型	情報窃取	米国を中心とした情報技術、ハイテク電子、衛星・通信、航空、輸送、エネルギー、財務、メディア、政府機関、国際機関等の141組織（米国：115組織）（米国Mandiant社報告書：APT1は中国人民解放軍61398部隊によるサイバースパイ活動に類似していると結論）

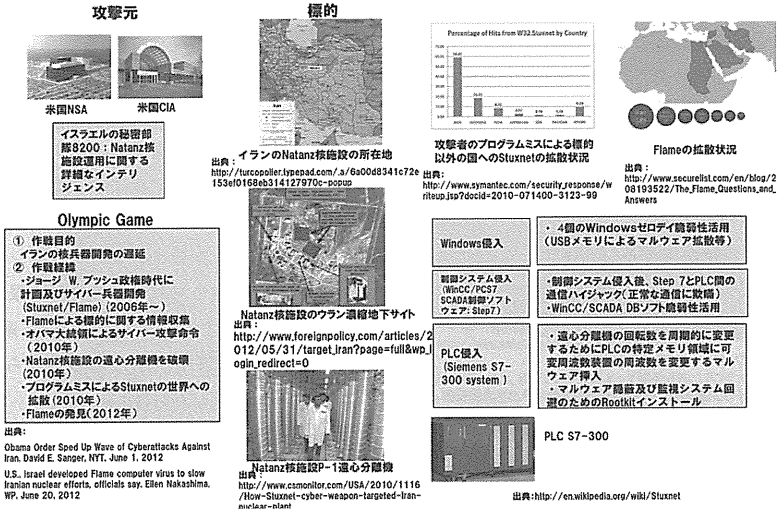


図2.1-3　クローズ系の破壊活動型／情報窃取型APT攻撃事例：Stuxnet／Flame

年6月20日のワシントンポスト紙（電子版）によると、「オリンピックゲーム」の一環でイランの核施設に対するサイバー破壊活動のために情報窃取を行うAPT攻撃マルウェアとして米国とイスラエルが共同開発したものであると言われている[6]。Stuxnet及びFlameのAPT攻撃事例の概要を図2.1-3に示す。

一方、オープン系のメール添付型の大規模な長期間にわたる情報窃取型APT攻撃（サイバースパイ活動）には、米国McAfee社が2011年に公表したOperation Shady RAT及び米国Mandiant社が2013年2月19日に公表したAPT1がある。Operation Shady RATは、2006年から米国を中心とした世界の政府機関、情報技術、衛星・通信、防衛企業等の71組織を標的とした情報窃取型APT攻撃である[7]。また、APT1は、2006年から現在も活動中である米国を中心とした情報技術、ハイテク電子、衛星・通信、航空、輸送、エネルギー、財務、メディア、政府機関、国際機関等の20分野の141組織を標的とした情報窃取型APT攻撃（数100テラバイトの情報窃取）であり、上海の中国人民解放軍61398部隊によるサイバースパイ活動に類似していると見られている。さらに、Operation Shady RATは、APT1と同一のものと見られている[8]。

オープン系の破壊活動型APT攻撃には、2012年8月に米国Symantec社が公表したShamoonがある。Shamoonは、サウジアラビアのエネルギー企業であるSaudi Aramcoの社内業務ネットワークの3万台のワークステーションを標的とした業務妨害であり、ワークステーションのファイルの破壊及びマスターブートレコーダー（MBR）の上書きにより使用不能にした。また、これは侵入先のIPアドレス等の感染情報を攻撃者に報告している[9]。

ウ　サイバー脅威の予測

サイバー脅威の予測については、主要な民間

セキュリティ会社3社(McAfee、Trend Micro及びアンラボ)の2012年の予測情報に基づき、2社以上の共通の脅威情報を識別し、可能性の高い脅威を抽出した[10][11][12]。これらのサイバー脅威の現状及びサイバー脅威に関する予測に基づき、一般動向としての「今後のサイバー脅威」を次に示す。

- APT攻撃の増大及び巧妙化
- 制御システムの脆弱性攻撃
- 組み込み機器に対する攻撃の増加
- クラウドへの攻撃本格化
- モバイル端末の脆弱性攻撃
- OSの発展に伴うサイバー攻撃技術の進化
- インサイダー攻撃
- ハクティビズム（社会的・政治的な主張に基づくハッキング活動）とアノニマス(ハクティビズムを行う集団）の活動の再活発化
- SNSを利用した攻撃
- タンパリング

2.2 軍事分野のサイバー脅威動向

軍事分野のサイバー脅威動向については、軍事施設等に関するサイバー攻撃事例及び彼の諸外国のサイバー戦能力の動向から「軍事システムに対して想定される脅威」を示す。

(1) 軍事施設等に関するサイバー攻撃事例

軍事施設等に関するサイバー攻撃事例については、軍事施設、重要インフラ、政府システム及び防衛関連企業を対象として公開情報に基づきシステム区分(オープン系／クローズ系)、発生年、攻撃種別(CNA／CNE)の観点から分析・整理した結果を表2.2-1に示す。

軍事施設のサイバー攻撃事例としては、米軍のクローズ系情報システムへの情報窃取攻撃事例である1998年のマスターズ・オブ・ダウンロード事件及び2008年のOperation Buckshot Yankeeがある。また、1998年のコソボ紛争での米軍によるセルビア軍防空システムへの不正アクセス・改竄及び2007年のイスラエル国防軍によるシリア軍防空システムへのサイバー攻撃がある。

表2.2-1 軍事施設等に対するサイバー攻撃事例

攻撃対象種別	攻撃事例	システム区分	発生年	攻撃種別
C4ISRシステム	マスターズ・オブ・ダウンロード事件(米国防総省DISNへの不正アクセス・情報窃取)	オープン／クローズ	1998	CNE
C4ISRシステム	セルビア軍防空システムへの不正アクセス・改ざん	クローズ	1999	CNA
C4ISRシステム	航空攻撃に合わせたシリア軍防空システムへのサイバー攻撃(電磁波経由)	クローズ	2007	CNA
C4ISRシステム	米国防総省のSIPRNETの情報システムへのAPT攻撃(USBメモリー経由)	クローズ／オープン	2008	CNE
兵站システム	米国防総省施設34箇所コンピュータシステムへの不正アクセス・プログラム破壊・改ざん	オープン	1990	CNA
兵站システム	データストリーム・カウボーイ事件(米空軍ローム研究所への不正アクセス・情報窃取)	オープン	1994	CNE
兵站システム	米海軍兵学校コンピュータシステムへの不正アクセス・改ざん	オープン	1994	CNA
兵站システム	ソーラー・サンライズ事件(米国防総省コンピュータシステムへの大規模不正アクセス)	オープン	1998	CNA
兵站システム	コソボ紛争時のNATO側システムへのDoS攻撃及び電子メールによるウィルス攻撃	オープン	1999	CNA
兵站システム	タイタン・レイン(APT攻撃による米軍関連施設等からの大量情報窃取)	オープン	2004	CNE
兵站システム	米国国防総省コンピュータシステムへの不正アクセス	オープン	2007	CNA
兵站システム	米国国防総省コンピュータシステムに中国製偽造ルーターの使用(サプライチェーンリスク)	オープン	2008	CNE
兵站システム	米国防総省コンピュータシステムへの不正アクセス及びF35の機密情報等の窃取(APT攻撃)	オープン	2008	CNE
重要インフラ	米国マサチューセッツ州ウースター空港の空港管制システムへのサイバーテロ(システム破壊)	オープン	1997	CNA
重要インフラ	ロシア・ガスプロムのパイプライン制御システムへのサイバー攻撃(トロイの木馬)	クローズ	1999	CNA
重要インフラ	米カリフォルニア州の電力会社の電力網システムへの不正アクセス	オープン	2001	CNA
重要インフラ	米国オハイオ州の原子力発電所制御システムのスラマーワームによる停止	クローズ	2003	CNA
重要インフラ	イラン原子力施設へのStuxnetによるUSBメモリー経由のAPT攻撃	クローズ	2010	CNA
政府システム	米国連邦捜査局(FBI)のウェブサイトへのDoS攻撃	オープン	1999	CNA
政府システム	日本政府機関ウェブサイトへのDoS攻撃	オープン	2004	CNA
政府システム	エストニア政府機関等への大規模DDoS攻撃(政府、報道機関及び主要金融機関への攻撃)	オープン	2007	CNA
政府システム	グルジア紛争時のグルジア政府への大規模DDoS攻撃	オープン	2008	CNA
政府システム	米国及び韓国へのDDoS攻撃	オープン	2009	CNA
政府システム	米国の政府機関、軍機関等へのAPT攻撃	オープン	2010	CNA
政府システム	日本の衆議院・参議院、政府機関へのAPT攻撃	オープン	2011	CNE
防衛関連企業等	オペレーション・オーロラ(Operation Aurora)によるAPT攻撃	オープン	2009	CNE
防衛関連企業等	日本の防衛関連企業へのAPT攻撃	オープン	2011	CNE

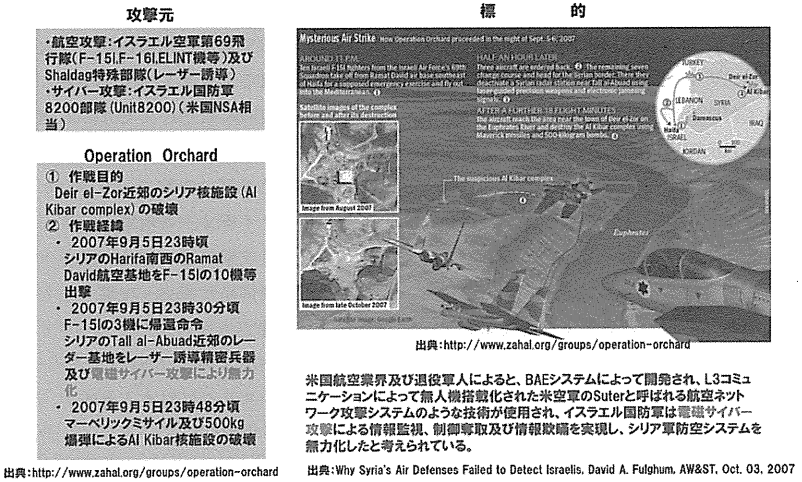


図2.2-1 シリア軍防空システムへの電磁サイバー攻撃事例：Operation Orchard

特に、後者はイスラエル空軍がシリア核施設への航空攻撃(Operation Orchard)を実施した際に、ロシア製のシリア軍防空システムに何も表示されなかった事例であり、無人機から防空システムへの電磁波利用による情報監視、制御奪取及び目標情報の欺瞞、工作員による活動の可能性等が示唆されている[13]。Opeartion Orchardの電磁サイバー攻撃事例の概要を図2.2-1に示す。

また、重要インフラのサイバー攻撃事例としては、電力、ガス等の具体事例があり、特にクローズ系の事例としては、1999年のロシアガスプロムのパイプライン制御システムへのトロイの木馬によるサイバー攻撃、2003年の米国オハイオ州の原子力発電所制御システムへのスラマーワームによる停止及び2010年のイランのナタンズ核施設の遠心分離機制御システムへのStuxnetによる可搬記録媒体の拡散能力を活用したAPT攻撃が挙げられる。

このように電磁波利用による侵入能力または可搬記録媒体の拡散能力を用いたクローズ系システムを標的としたAPT攻撃が、現時点における最大のサイバー脅威の1つと言える。

(2) 彼の諸外国のサイバー戦能力の動向

中国は、情報戦戦略及びドクトリンとして、それぞれ「陸、海、空及び宇宙における軍事作戦のサイバー空間を通じたネットワーク化による一体化した統合作戦」及び「統合ネットワーク電子戦（INEW：Integrated Network Electronic Warfare)」を持っている。中国のサイバー戦組織は、人民解放軍の総参謀部第4部(攻撃INEW担当)、総参謀部第3部、技術偵察局(地方)、情報戦民兵隊及びハッカー集団から構成される[14]。2013年2月19日に発表された米国Mandiant社のAPT1報告書によると総参謀部第3部第2局は、サイバースパイ活動を行う上海の中国人民解放軍61398部隊と見られている。また、サイバー戦能力としては、サイバースパイ活動としてのCNE能力並びにオープン系システムに対する標的データに基づくDDoS攻

撃、対衛星攻撃、衛星制御局サイバー攻撃等のCNA能力を保有している[15]。

ロシアは、サイバー戦戦略として、「国防省主管によるCND及びCNA並びに連邦保安庁主管によるCNEの実施」を規定した「情報空間(サイバー空間)におけるロシア軍の活動に関するコンセプト」を2011年に制定している。また、ロシア軍の軍事ネットワーク及びシステムを防護するための「サイバー軍」の創設並びにサイバー演習場導入のための高等軍事研究局設置計画を発表している[16]。ロシアは、サイバー戦能力として、サイバースパイ活動としてのCNE能力並びに大規模DDoS攻撃、大規模な高度ボットネット、電磁パルス兵器、偽造ソフトウェア、無線妨害・データ通信妨害、各種マルウェア等のCNA能力を保有していると見られている[17]。

(3) 軍事システムに対して想定される脅威

軍事施設等に関するサイバー攻撃事例及び彼の諸外国のサイバー戦能力の動向から「軍事システムに対して想定される脅威」を次に示す。

① C4ISRシステムに対する脅威
- APT攻撃(USBメモリ/電磁波経由)
- 制御システムの脆弱性攻撃
- インサイダー攻撃
- サプライチェーン攻撃
- 対衛星攻撃兵器
- 衛星制御局サイバー攻撃
- HEMP
- 電磁パルス兵器(非核)

② 兵站システムに対する脅威
- DDoS攻撃
- APT攻撃
- サプライチェーン攻撃

2.3 A2/AD環境下におけるサイバー空間の情報セキュリティリスク

「サイバー脅威の一般動向」から導出されたサイバー脅威及び「軍事分野のサイバー脅威動向」から想定される脅威に対して、クローズ系のC4ISRシステムに対する脅威を抽出し、「A2/AD環境下におけるサイバー空間の脅威」として次のとおり整理した。

- APT攻撃(USBメモリ/電磁波経由)
- 制御システムの脆弱性攻撃
- インサイダー攻撃
- サプライチェーン攻撃
- ネットワークアクセス阻止攻撃(対衛星攻撃兵器、衛星制御局サイバー攻撃、HEMP攻撃、電磁パルス兵器(非核)及びタンパリング)

このような「A2/AD環境下におけるサイバー空間の脅威」は、クローズ系のC4ISRシステムの脆弱性を狙って攻撃し、脅威の防護及び検知が失敗した場合、その脅威と脆弱性に基づく情報セキュリティリスク(影響)は図2.3-1のようにモデル化される。

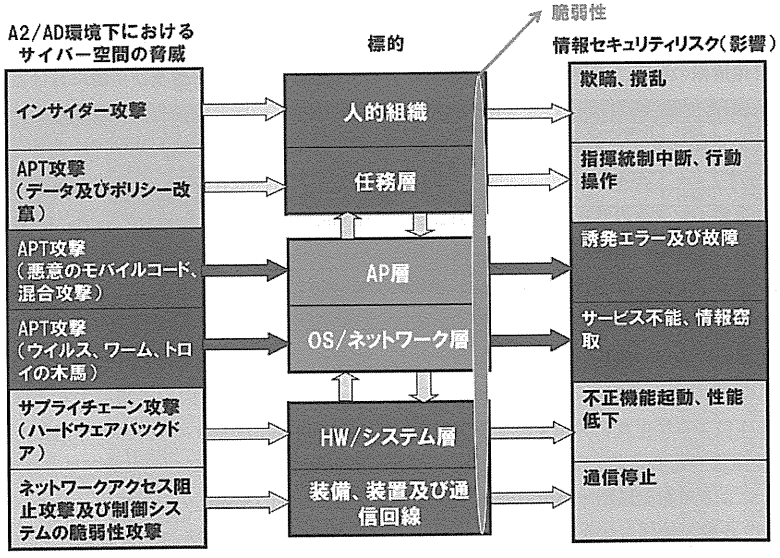


図2.3-1 A2/AD環境下におけるサイバー空間の情報セキュリティリスク

参考文献

1) Verizon:2012年度データ漏洩/侵害調査報告書、2012年
2) Beth E. Binde, Russ McRee, and Terrence J. O'Connor: Assessing Outbound Traffic to Uncover Advanced Persistent Threat, SANS Technology Institute, 22 May 2011
3) 警察庁警備企画課・情報技術解析課:サイバーインテリジェンスに係る最近の情勢(平成24年上半期)について、平成24年8月23日
4) David E. Sanger: Obama Order Sped Up Wave of Cyberattacks Against Iran, New York Times, 1 June 2012
5) David Albright, Paul Brannan, and Christina Walrond: Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment, ISIS, 22 Dec. 2011
6) Ellen Nakashima: U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say, Washington Post, 20 June 2011
7) Dmitri Alperovitch: Revealed: Operation Shady RAT, McAfee, 2011
8) APT1: Exposing One of China's Cyber Espionage Units, Mandiant, 19 Feb. 2013
9) Symantec Security Response: The Shamoon Attacks, Symantec, 16 Aug. 2012
10) McAfee Labs: 2012 Threat Predictions, Nov. 2011
11) Trend Micro: 12 Security Predictions for 2012, 16 Dec. 2011
12) アンラボ:2012年予想7大セキュリティ脅威トレンドを発表、2012年1月3日
13) David A. Fulghum: Why Syria's Air Defenses Failed to Detect Israelis, 3 Oct. 2007
14) Bryan Krekel: Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation, Northrop Grumman Corporation, 9 Oct. 2009
15) USCC: 2011 Report to Congress of the U.S.-China Economic and Security Review Commission, Nov. 2011
16) 佐々木孝博:ロシアのサイバー戦略:「サイバー戦コンセプト」を中心に、日本大学大学院総合社会情報研究科、日本大学大学院総合社会情報研究科紀要、No.13、2012年
17) Ward Carroll: Russia's Cyber Force, 27 May 2008

3．サイバー攻撃に対する脆弱性の動向

前章で述べたサイバー脅威は、C4ISRシステムの脆弱性を狙ってサイバー攻撃を行い、その効果としての影響を及ぼす。その脆弱性には、重要インフラの脆弱性、情報システムの脆弱性、制御システムの脆弱性、サプライチェーンの脆弱性及び人的資源の脆弱性がある。特に、重要インフラの脆弱性は、我が国で定義されている11分野の重要インフラにおいて、「情報通信分野（通信）は他の7分野と」「電力分野は他の10分野と」及び「水道分野は他の8分野と」相互依存性があることである[1)]。

3.1 情報システムの脆弱性

情報システムの脆弱性には、OS及びアプリケーションのソフトウェアの脆弱性並びにセキュリティ設定の脆弱性がある。また、未知及びベンダーが公表していない脆弱性であるゼロデイ脆弱性について述べる。

(1) ソフトウェア製品の脆弱性[2)3)4)]

ソフトウェア製品の脆弱性情報には、NVD（National Vulnerability Database）及びOSVDB（Open Source Vulnerability DataBase）並びに日本情報処理推進機構（IPA）が提供するJVN iPediaがある。NVDは、米国の国立標準技術研究所（NIST）が管理している脆弱性情報データベースであり、CVE（Common Vulnerabilities and Exposures）で命名された脆弱性情報の詳細情報を提供している。これは、他の脆弱性情報データベースと異なりCommon Vulnerability Scoring System（CVSS）に基づく危険度評価を行っている。OSVDBは、オープンソースプロジェクトによる脆弱性情報データベースで、OS、ソフトウェア製品、プロトコル、ハードウェア装置等の脆弱性を収集・蓄積したものである。JVN iPdiaは、我が国で主に使用されているソフトウェア製品の脆弱性情報を次の3つの情報源から収集・蓄積し、2007年4月25日から公開している。

- 我が国のソフトウェア開発者が公開した脆弱性情報
- 脆弱性対策情報ポータルサイトJVNで公開した脆弱性情報
- 米国NISTのNVDが公開した脆弱性情報

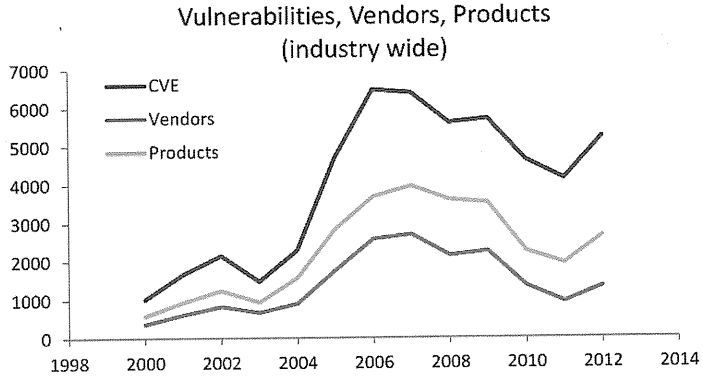


図3.1-1 NVDに登録された脆弱性情報件数の経年傾向

出典：Vulnerability Threat Trend, Stefan Frei, NSS Labs, Feb. 2013

報

NVDが2000年から公開している脆弱性情報件数の経年傾向を図3.1-1に示す。脆弱性情報件数の最大は2006年の6,462件であり、その後の5年間は減少し2011年には4,139件となっている。しかし、2012年には再び脆弱性情報件数は5,225件に増加している。2013年7月31日現在のNVDの累積脆弱性情報件数は、57,343件であり、1日あたりの脆弱性情報登録件数は16件である。

また、NVDが2000年から公開している脆弱性情報件数のCVSS危険度評価別（高：CVSS基本値＝7.0～10.0、中：CVSS基本値＝4.0～6.9及び低：CVSS基本値＝0.0～3.9）の経年傾向を図3.1-2に示す。2012年の高危険度評価の脆弱性情報件数割合は減少しているが、CVSS基本値が9.9の非常に高い危険度評価の脆弱性情報件数の割合が9.3%と大きい。

2012年に公開されたAPT攻撃に悪用される高危険度評価の脆弱性のあるソフトウェア製品の上位10社内訳を表3.1-1に示す。

また、過去25年間（1988年～2012年）における高危険度評価の脆弱性の内訳は、図3.1-3に示すとおりであり、「バッファオーバーフロー」及

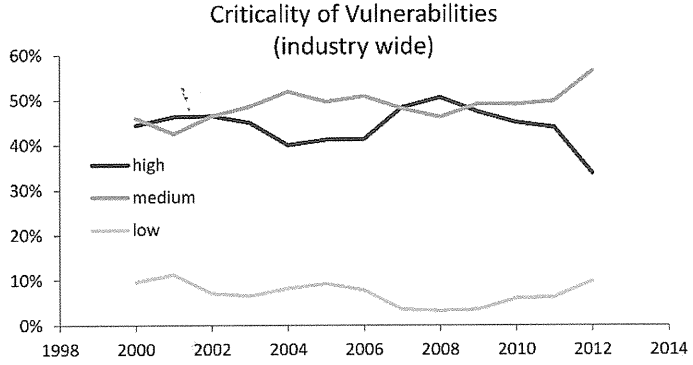


図3.1-2 NVDに登録された脆弱性情報件数の危険度評価別割合の経年傾向

出典：Vulnerability Threat Trend, Stefan Frei, NSS Labs, Feb. 2013

表3.1-1 高危険度評価の脆弱性のあるソフトウェア製品の上位10社内訳

#	Vendor	CVEs	Share	Products
1	Adobe	112	23%	Flash-player, Adobe-AIR, Acrobat-Reader
2	Mozilla	64	13%	Firefox, Thunderbird
3	Oracle	47	10%	Java JRE, Fusion Middleware
4	Google	40	8%	Google Chrome
5	FFmpeg	28	6%	FFmpeg
6	HP	24	5%	Sitescope, Data-Protector-Express
7	Novell	9	2%	iPrint, Groupwise, File-Reporter
8	GoForAndroid	9	2%	Multiple Apps/Widgets
9	Advantech	8	2%	Web Access, Modbus-RTU-OPC-server
10	Microsoft	7	1%	Windows XP to 8, Internet Explorer

出典：Vulnerability Threat Trend, Stefan Frei, NSS Labs, Feb. 2013

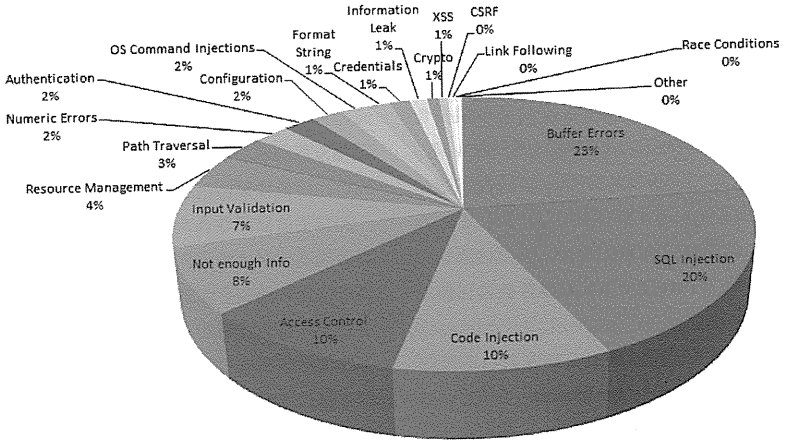


図3.1-3　過去25年間（1988年～2012年）における高危険度評価の脆弱性の内訳

出典：25 Years of Vulnerabilities: 1988-2012 Research Report, Yves Younan, SOURCEfire, 22 July 2013

び「SQL インジェクション」がそれぞれ23%及び20%を占めている。バッファオーバーフローとは、実行中のプログラムのメモリ（スタック領域、ヒープ領域及び静的領域）内に攻撃者の手による機械語プログラムが送り込まれ、コンピュータ全体の制御が奪われる脆弱性である。また、SQL インジェクションとは、アプリケーションが想定しない SQL 文を実行させることにより、データベース管理システムを不正に操作する攻撃を可能とする脆弱性である。

(2)　セキュリティ設定の脆弱性[5)]

米国国土安全保障省（DHS）は、2012年６月に「サイバー攻撃に使用されている脆弱性の80%は、既知のソフトウェアの脆弱性及びセキュリティ設定の脆弱性の利用である」と報告している。

(3)　ゼロデイ脆弱性

最も高度な APT 攻撃に使用されるゼロデイ脆弱性は、図3.1-4に示すとおり年間８件から15件程度の発見件数である。2012年のゼロデイ脆弱性発見件数は14件である[6)]。また、実際の APT 攻撃に使用されたゼロデイ脆弱性を表3.1-2に示す。特に、CWE-2010-2568（Windows シェルの脆弱性）は、Stuxnet、Frame 及び Gauss で使用されている「マルウェアの USB メモリ拡散」を実現し、「クローズ系の情報セキュリティ神話」を崩壊させたゼロデイ脆弱性である。

Stuxnet は、2010年に発見されたゼロデイ脆弱性14個の内の４個のゼロデイ脆弱性と１個の既知脆弱性を用いて最終標的であるイランのナタンズ核施設のウラン濃縮施設用遠心分離機の可変周波数装置を攻撃するためにオープン系業務ネットワーク並びに制御系情報ネットワーク及び制御ネットワークにマルウェアを拡散させ、遠心分離機の PLC の特定メモリ領域に可変周波数装置の周波数を変更するマルウェアを挿入したものである。

サイバー兵器の開発のためには、ゼロデイ脆弱性の発見または外部からの入手が必須であり、

Figure D.4. **Volume of Zero-day Vulnerabilities, 2006–2012**

Source: Symantec

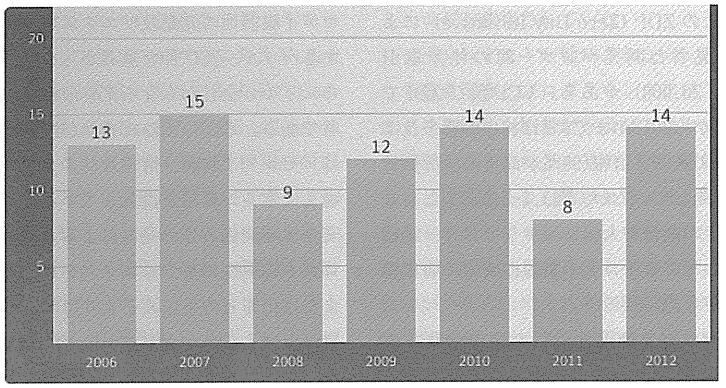


図3.1-4　ゼロデイ脆弱性の発見件数（件／年）

出典：Internet Security Threat Report, Symantec Appendix, Symantec, 2013

表3.1-2　実際の APT 攻撃に使用されたゼロデイ脆弱性

事案	脆弱性	概要	対策
Sykipot	CVE-2011-2462	Adobe Reader と Adobe Acrobat の脆弱性	JSSE無効化
Nitro/Poison Ivy	CVE-2012-4681	Javaの脆弱性	更新
Stuxnet	CVE-2008-4250 CVE-2010-2568 CVE-2010-2729 CVE-2010-2743 CVE-2010-3888	Windows Serverサービスの脆弱性 Windowsシェルの脆弱性(USBメモリ拡散) Windows印刷スプーラの脆弱性 Windowsカーネルモードドライバの脆弱性(特権昇格) Windowsタスクスケジューラの脆弱性(特権昇格)	更新
Duqu	CVE-2011-3402	Windowsカーネルの脆弱性	更新
Flame	CVE-2010-2568 CVE-2010-2729 CVE-2012-1875 CVE-2012-1889	Windowsシェルの脆弱性(USBメモリ拡散) Windows印刷スプーラの脆弱性 MS IEの脆弱性 MS XMLコアサービスの脆弱性	更新
Gauss	CVE-2010-2568	Windowsシェルの脆弱性(USBメモリ拡散)	更新
Elderwood	CVE-2012-0779 CVE-2012-1875 CVE-2012-1889 CVE-2012-1535 CVE-2011-0609 CVE-2011-0611 CVE-2011-2110 CVE-2010-0249	Adobe Flash Playerの脆弱性（電子メール／Web） MS IEの脆弱性(Web) MS XMLコアサービスの脆弱性 (Web) Adobe Flash Playerの脆弱性（電子メール） Adobe Flash Playerの脆弱性 Adobe Flash Playerの脆弱性 Adobe Flash Playerの脆弱性 MS IEの脆弱性	

ゼロデイ脆弱性情報は価値のある資産である。ゼロデイ脆弱性情報の取引には、ベンダー市場並びに闇市場及びグレー市場、が存在する。

ゼロデイ脆弱性情報のベンダー市場については、米国において Mozilla や Google のバグ報奨金としての有償による取引（$500～

$3,133.70)並びにiDefenseのVCP(Vulnerability Contributor Program)及びHP/TippingPointのZDI(Zero Day Initiative)によるバグ発見者と開発ベンダー間の仲介取引($500～$20,000)がある。VCP及びZDIでは、2001年から2012年までに211社に影響を及ぼす1,604件の脆弱性情報(99%が高危険度評価脆弱性)を公開しているが、図3.1-5に示すとおり2012年にその割合が大幅に減少しており、2012年に急増しているゼロデイ脆弱性情報の闇市場との相関が考えられる[7)8)]。

一方、ゼロデイ脆弱性情報の闇市場及びグレー市場については、その購入者の中に政府機関が存在する。米国連邦政府は、そのようなゼロデイ脆弱性の発見及びエクスプロイトを開発するハッカー及び仲介業者からなる闇市場やセキュリティ会社からなるグレー市場の最大購入者である。米国の国防総省及び国家安全保障局は、ゼロデイ脆弱性情報及びエクスプロイトの購入に多くの費用を投入している。米国の国家安全保障関係者等の発言によると、「それは、ゼロデイ脆弱性に基づくエクスプロイトが独裁者または犯罪者の手に渡るよりは米国連邦政府が買い上げることがよりよいことである」との米国の戦略論理に基づいている。ゼロデイ脆弱性情報のグレー市場には、ゼロデイ脆弱性に基づくエクスプロイトツールを販売するセキュリティ会社である、フランスのパリにあるVupen社ゼロデイ脆弱性情報を販売する米国のEndgame社、Netragard社、Exodus Intelligence社等がある。また、ゼロデイ脆弱性情報の闇市場には、セキュリティ研究者等のゼロデイ脆弱性情報提供者と購入者との間の取引の仲介業者も存在する。ゼロデイ脆弱性情報の闇市場価格を表3.1-3に示す[8)9)]。

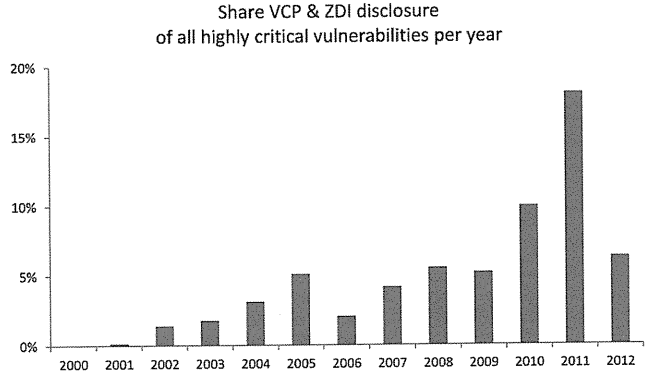


図3.1-5　VCP及びZDIの高危険度評価脆弱性情報公開件数割合の経年傾向

出典：Vulnerability Threat Trend, Stefan Frei, NSS Labs, Feb. 2013

表3.1-3　ゼロデイ脆弱性情報の闇市場価格

ADOBE READER	$5,000-$30,000
MAC OSX	$20,000-$50,000
ANDROID	$30,000-$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000-$100,000
MICROSOFT WORD	$50,000-$100,000
WINDOWS	$60,000-$120,000
FIREFOX OR SAFARI	$60,000-$150,000
CHROME OR INTERNET EXPLORER	$80,000-$200,000
IOS	$100,000-$250,000

出典：Shopping For Zero Days, Andy Greenberg, Forbes, March 23, 2012

3.2　制御システムの脆弱性

制御システムの脆弱性については、情報システムとは異なる潜在的な脆弱性、脆弱性傾向、セキュリティ研究者による脆弱性発見、脆弱性情報管理について述べる。

(1)　制御システムの潜在的な脆弱性[10)]

重要インフラに関連する制御システムの脆弱性については、米国のNISTが2013年7月に発表した「NIST SP 800-82 Rev. 1制御システムセキュリティ指針」において、制御システムの潜在的な脆弱性としてポリシー/手順脆弱性、プラットフォーム脆弱性及びネットワーク脆弱性に大別・整理され、次に示す主要な潜在的脆弱性が挙げられる。

- 制御システムの不適切なセキュリティポリシー
- 制御システム用セキュリティポリシーの不在
- 不適切なセキュリティアーキテクチャ及び設計
- 制御システムのセキュリティ監査の不在
- 制御システム独自の構成変更管理の欠如
- OS及びAPのパッチ管理の欠如
- デフォルトの構成が使用されること
- パスワード管理の欠如
- セキュリティ設定管理の欠如(デフォルト設定)
- ログが取得されていない
- インシデントが検知されない
- 構成管理とプログラミングソフトウェアへの不適切な権限付与及びアクセス

制御システムセキュリティは、情報セキュリティと比較すると、情報セキュリティの基本であるセキュリティ管理策、セキュリティ管理策に基づく対策の実施及びセキュリティ監査それ自身が不在のためそれらが脆弱性となっている。

(2)　制御システム製品の脆弱性傾向

制御システム製品の脆弱性の報告件数は、OSVDBによると図3.2-1に示すとおり2011年から急増しており、2011年及び2012年の報告件数はそれぞれ164件及び191件である[11)]。制御シ

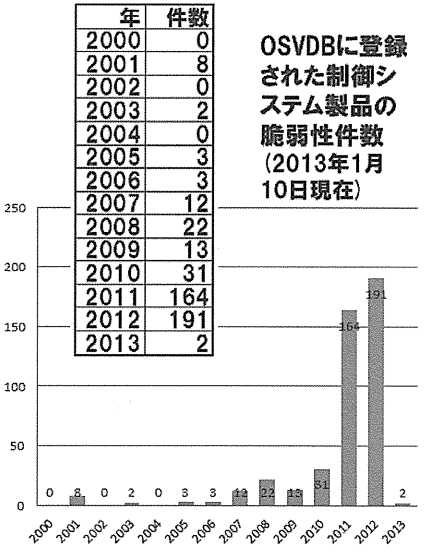


図3.2-1　OSVDBに基づく制御システム製品の脆弱性の報告件数

出典：制御システムセキュリティ：2012年度の動きを振り返る、宮地利雄、JPCERT、2013年2月18日

ステム製品ベンダーのパッチ実施状況については、実施率の高いベンダーと低いベンダーの2極に分かれており、エクスプロイトがあっても放置されているものがある。また、制御システム製品の脆弱性攻撃に利用可能なエクスプロイトがセキュリティ研究者によって公開されており、当該脆弱性に対応するパッチが未実施の場合はセキュリティリスクが高い。制御システム製品の脆弱性に対して35%にエクスプロイトが存在している[12]。制御システム製品の脆弱性は、2012年のICS-CERT（The Industrial Control Systems Cyber Emergency Response Team）の報告によると「バッファオーバーフロー」及び「不適切な入力確認」がそれぞれ全体（171件）の26%（44件）及び8%（13件）を占めている[13]。

(3) セキュリティ研究者による制御システムの脆弱性発見

セキュリティ研究者も制御システムの脆弱性に注目しており、表3.2-1に示すようにセキュリティ研究者がその脆弱性を公表している。制御システムの脆弱性は、一般にベンダーから公表されることは少ないためゼロデイ脆弱性の機会を創出している[14]。

最も脆弱性発見件数の多いセキュリティ研究者であるイタリアのLuigi Auriemma氏は、2011年3月に34件公表以降に次々と多数の脆弱性をブログで公表し、ベンダーには事前通知をしないままのゼロデイ脆弱性も公表している。また、実証のためのエクスプロイト及び脆弱性の探索に使用しているツールも公表している[15]。一方、Luigi Auriemma氏は、マルタをベースとするセキュリティ新興企業であるReVuln社を設立し、制御システムベンダーが脆弱性に対して適時なパッチを提供していない現状を解決するために、発見した脆弱性情報に関するパッチを開発し、脆弱性情報とパッチを制御システム製品利用企業に販売している。このパッチは、脆弱性コードをメモリ上で直接修正するホットパッチまたはランニングパッチと呼ばれるパッチであり、脆弱性のあるソフトウェアの再起動を必要としないため、制御システムを停止しなくてよい[16]。

また、米国のBilly Rios氏とTerry McCorkle氏は、無料でダウンロードできる制御システム製品76件を対象に余暇時間による脆弱性探索を行い、665件の脆弱性を発見し、その探索過程をDerbyCon 2011において発表している。発見した脆弱性の内360件は、ファジングによるものである[17]。

表3.2-1 セキュリティ研究者による制御システムの脆弱性発見件数

Researcher	Country	Vulnerability count
Luigi Auriemma	Italy	104
Billy Rios, Terry McCorkle	USA	24
GLEG	Russia	24
Eyal Udassin – C4	Israel	14
Ruben Santamarta	Spain	13
Lluis Mora	Spain	22
Jeremy Brown	USA	10
Dillon Beresford	USA	9
Digital Bond	USA	8
Shawn Merdinger	USA	7
Kuang-Chun Hung	Taiwan	6
44 other identified researchers		65

出典：Documenting The "Lost Decade": An Empirical Analysis Publicly Disclosed ICS Vulnerabilities since 2001, Sean McBride, Jan. 2012

ロシアのセキュリティ企業であるGLEG社は、公表されたすべての脆弱性をカバーすることを目標としたエクスプロイトパックであるAgora SCADA＋ Packを侵入試験ツールであるImmunity CANVASにアドオンして販売している[18]。

このようにセキュリティ研究者による制御システムの脆弱性発見に基づく脆弱性情報の公開についても、ゼロデイ脆弱性の機会創出を回避するために公的機関による統制管理及び規制が必要である。

(4) 米国の制御システムの脆弱性情報管理

制御システムの脆弱性情報管理については、米国では国土安全保障省（DHS）配下のICS-CERTが行っている。ICS-CERTは、制御システムの脆弱性情報の取扱ポリシーを改訂し、「ベンダーの未対応または合理的な改善スケジュールが設定されていない場合（パッチまたは影響のあるベンダーからの次善策の存在または可用性に係わらず）、ICS-CERTは最初の脆弱性情報の通知があった日から45日後に当該脆弱性情報を公開してもよい」といういわゆる「45日ルール」を明示した[19]。また、米国DHSが設立したICSJWG（Industrial Control Systems Joint Working Group）は、ベンダーのための制御システム脆弱性取扱ガイドラインとして、「共通制御システム脆弱性取扱フレームワーク（Common Industrial Control System Vulnerability Disclosure Framework）」を2012年6月に発表している[20]。

制御システムの脆弱性情報は、情報システムの脆弱性情報と同様にNISTが提供するNVD及びオープンソースプロジェクトが提供するOSVDBにも登録されている。

(5) 我が国の制御システムの脆弱性情報管理[21]

我が国の制御システムの脆弱性情報管理については、経済産業省の「制御システムセキュリティ検討タスクフォース」において日本版ICS-CERTの構築を検討中である。

また、JPCERT／CCの「制御システム用製品の脆弱性情報の取扱に関する研究会」において、情報セキュリティの脆弱性情報フレームワーク

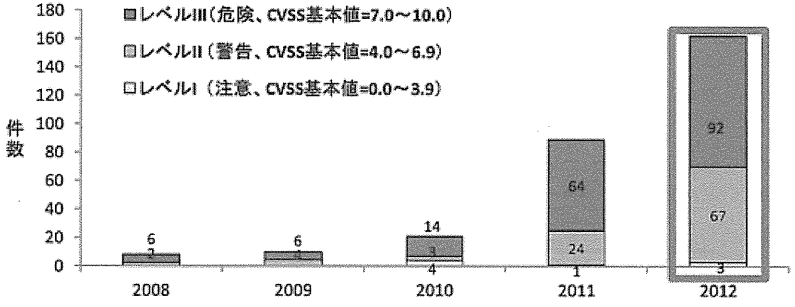


図3.2-2 JVN iPediaに登録された制御システムの脆弱性情報件数

出典：脆弱性対策情報データベースJVN iPediaの登録状況［2012年第4四半期（10月～12月）］別紙1、IPA、2013年1月21日

に準じた、制御システムに適した告示方法、早期警戒パートナーシップガイドライン、業界等の個別ガイドライン等のあり方について検討中である。

我が国のソフトウェア製品の脆弱性情報データベースであるJVN iPediaに登録された制御システムの脆弱性情報件数は、図3.2-2に示すとおりである。

3.3 サプライチェーンの脆弱性

サプライチェーンの攻撃対象としては、情報システムの構成部品である集積回路（IC）の製造段階及び製品のアセンブリ及び流通段階があり、それぞれ上流サプライチェーン及び下流サプライチェーンと呼び、これらの脆弱性について述べる。

(1) 上流サプライチェーンの脆弱性

上流サプライチェーンにおけるICを製造する半導体業界の供給モデルは、効率性、量産化及び収益性の企業目標のために従来のICの設計及び製造からアセンブルした最終製品までを一貫して製造する垂直統合型LSIメーカー（Integrated Device Manufactures：IDM）供給モデルから設計のみを行い、製造を外注するファブレス（fabless：工場を持たない）供給モデルまたは開発・設計のみを行い、製造を外注するファブライト（fab-lite）供給モデルに変わってきた。この製造を請け負う専門分野に特化した工場は、専業製造工場（merchant foundry）と呼ばれ、現在市場の88%を占めている。2010年の国際ファブレスICサプライヤの上位20社は、表3.3-1に示すとおり米国、台湾及び欧州連合（EU）に拠点を置いている。また、専業製造工場は、表3.3-2に示すとおり米国の4社以外に台湾、韓国及び欧州連合の同盟国及び非同盟国の中国（3社）に会社を置いている[22]。

このようなファブレスまたはファブライト供給モデルは、IC供給サプライヤの拠点が同盟国であっても、非同盟国にある一部の専業製造工場も含まれるためICチップ製造段階の上流サプライチェーンに脆弱性が存在する可能性がある。

表3.3-1 2010年上位20社国際ファブレスICサプライヤ

2010 Top 20 Fabless IC Suppliers

2010 Rank	2009 Rank	2008 Rank	Company	Headquarters	2008 ($M)	2009 ($M)	% Change	2010 ($M)	% Change
1	1	1	Qualcomm	U.S.	6,477	6,409	-1%	7,204	12%
2	3	2	Broadcom	U.S.	4,449	4,271	-4%	6,589	54%
3	2	—	AMD	U.S.	0	5,403	N/A	6,494	20%
4	6	4	Marvell	U.S.	3,055	2,690	-12%	3,592	34%
5	4	5	MediaTek	Taiwan	2,864	3,500	22%	3,590	3%
6	5	3	Nvidia	U.S.	3,660	3,151	-14%	3,575	13%
7	7	6	Xilinx	U.S.	1,906	1,699	-11%	2,311	36%
8	10	8	Altera	U.S.	1,367	1,196	-13%	1,954	63%
9	8	7	LSI Corp.	U.S.	1,795	1,422	-21%	1,616	14%
10	11	9	Avago	U.S.	905	858	-5%	1,187	38%
11	12	11	Novatek	Taiwan	829	819	-1%	1,149	40%
12	9	—	ST-Ericsson*	Europe	0	1,263	N/A	1,146	-9%
13	15	18	MStar	Taiwan	454	605	33%	1,067	76%
14	17	17	Atheros**	U.S.	472	543	15%	927	71%
15	16	12	CSR	Europe	695	601	-14%	801	33%
16	14	15	Realtek	Taiwan	534	615	15%	706	15%
17	13	10	Himax	Taiwan	833	693	-17%	643	-7%
18	18	16	PMC-Sierra	U.S.	525	496	-6%	635	28%
19	69	52	Trident	U.S.	149	85	-43%	558	556%
20	—	—	Lantiq	Europe	0	0	N/A	550	N/A
Top 20			—	—	30,969	36,319	17%	46,294	27%
Others			—	—	12,861	10,931	-15%	13,571	24%
TOTAL			—	—	43,830	47,250	8%	59,865	27%

*Represents the 50% share not accounted for by ST.
**To be purchased by Qualcomm in 2011.

Source: IC Insights' *Strategic Reviews Database*

出典：Occupying the Information High Ground：Chinese Capabilities for Computer Network Operations and Cyber Espionage, USCC, March 3, 2012

表3.3-2 2010年主要IC製造工場

2010 Major IC Foundries

2010 Rank	2009 Rank	Company	Foundry Type	Location	2008 Sales ($M)	2009 Sales ($M)	09/08 Sales (%)	2010 Sales ($M)	10/09 Sales (%)
1	1	TSMC	Pure-Play	Taiwan	10,556	8,989	-15%	13,307	48%
2	2	UMC	Pure-Play	Taiwan	3,070	2,815	-8%	3,965	41%
3	4	GlobalFoundries	Pure-Play	U.S.	0	1,101	N/A	3,510	219%
4	5	SMIC	Pure-Play	China	1,353	1,070	-21%	1,555	45%
5	9	TowerJazz	Pure-Play	Europe	252	300	19%	510	70%
6	7	Vanguard	Pure-Play	Taiwan	511	382	-25%	508	33%
7	6	Dongbu	Pure-Play	South Korea	490	395	-19%	495	25%
8	8	IBM	IDM	U.S.	400	335	-16%	430	28%
9	12	MagnaChip	IDM	South Korea	346	262	-24%	420	60%
10	10	Samsung	IDM	South Korea	340	290	-15%	400	38%
11	11	SSMC	Pure-Play	Singapore	340	280	-18%	330	18%
12	15	X-Fab	Pure-Play	Europe	368	212	-42%	320	51%
13	14	Hua Hong NEC	Pure-Play	China	280	240	-14%	295	23%
14	13	TI	IDM	U.S.	315	250	-21%	285	14%
15	16	Grace	Pure-Play	China	230	180	-22%	260	44%
—	3	Chartered*	Pure-Play	U.S.	1,743	1,540	-12%	0	N/A

*Purchased by GlobalFoundries in 4Q09.

Source: IC Insights, company reports

出典：Occupying the Information High Ground：Chinese Capabilities for Computer Network Operations and Cyber Espionage, USCC, March 3, 2012

(2) 下流サプライチェーンの脆弱性

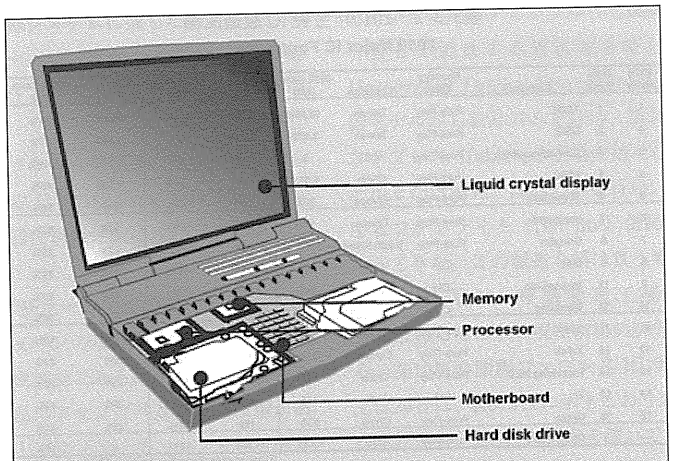
下流サプライチェーンへの攻撃可能性については、敵対者によるアセンブリ（組み立て）段階でのファームウェアまたはソフトウェアにバックドア機能を持つマルウェア（トロイの木馬）の組み込み並びに流通段階でのブランド機器の積み荷への完成品の偽造ハードウェアの混入が挙げられる。

ノートパソコンの構成部品のサプライヤが使用した可能性のある拠点の例については、米国会計検査院（GAO）の報告書によると図3.3-1に示すとおりマザーボードを除く構成部品に中国が含まれている[23]。

3.4 人的資源の脆弱性[24]

人的資源の脆弱性については、ソーシャルエンジニアリングの標的になるものであり、Ian Mann氏の「人間のハッキング：ソーシャルエンジニアリング技法及びセキュリティ対策（2008年）」において、人間の心理的弱点として次に示すものを挙げている。

- 命令に服従する。
- 相手の無知を用いて命令に準拠させる。
- 人間のだまされやすさは積極的な便益を漸次的に提示されると増加しやすい傾向がある。
- 好かれたい欲望は人間に共通であり、多くの囮捜査で使用されてきた（ハニーポット）。
- 職場では仲間に対して役に立つことを奨励されている（新しい職場で助けを求められると、役に立つために秘密情報でも提供する。）。



Component	Location of facilities potentially used by suppliers
Liquid crystal display	China, Czech Republic, Japan, Poland, Singapore, Slovak Republic, South Korea, Taiwan
Memory	China, Israel, Italy, Japan, Malaysia, Philippines, Puerto Rico, Singapore, South Korea, Taiwan, United States
Processor	Canada, China, Costa Rica, Ireland, Israel, Malaysia, Singapore, United States, Vietnam
Motherboard	Taiwan
Hard disk drive	China, Ireland, Japan, Malaysia, Philippines, Singapore, Thailand, United States

Source: GAO analysis of public information.

図3.3-1　ノートパソコンの共通サプライヤの潜在的生産地

出典：IT SUPPLY CHAIN：National Security-Related Agencies Need to Better Address Risks, GAO, March 2012

参考文献

1）NISC：2007年度相互依存性解析について、2008年4月22日
2）IPA：情報セキュリティ白書2012、2012年6月1日
3）Stefan Frei：Vulnerability Threat Trend, NSS Labs, Feb. 2013
4）Yves Younan：25 Years of Vulnerabilities：1988-2012 Research Report, SOURCEfire, 22 July 2013
5）DHS：Continuous Monitoring：Diagnostics & Mitigation, 8th Annual IT Security Automation Conference, 3-5 Oct. 2012
6）Symantec：Internet Security Threat Report, Symantec Appendix, 2013
7）Christopher Soghoian：The trade in security exploits：Free speech or weapons in need of regulation?, ACLU, VB2012, 26 Sept. 2012
8）Joseph Menn：Special Report：U.S. Cyber Strategy Stokes Fear of Blowback, Reuter, 10 May 2013
9）Andy Greenberg：Shopping For Zero-Days：A Price List for Hackers' Secret Software Exploits, Forbes, 23 March 2012
10）NIST：NIST SP 800-82 Rev. 1 Guide to Industrial Control Systems (ICS) Security, July 2013
11）宮地利雄：制御システムセキュリティ：2012年度の動きを振り返る、JPCERT、2012年2月18日
12）Gleb Gritsai：SCADA SAFETY IN NUMBER v1.1, Positive Technologies, 2012
13）ICS-CERT：ICS-CERT Monthly Monitor, October／November／December 2012
14）Sean McBride：Documenting the "Lost Decade," An Empirical Analysis of Publicly Disclosed ICS Vulnerabilities since 2001, S4 SCADA Security Scientific Symposium, 18-19 Jan. 2012
15）http://aluigi.altervista.org/、2013年2月1日アクセス
16）Lucian Constantin：Securing SCADA systems still a piecemeal affair, 23 Jan. 2013
17）Dale G Peterson：665 SCADA Bugs Presentation from DerbyCon, Digital Bond, Inc., 10 Oct. 2011
18）Agora Pack and Agora SCADA＋Pack：http://www.gleg.net/agora.shtml、2013年2月1日アクセス
19）ICS-CERT：ICS-CERT Vulnerability Disclosure Policy, 2012
20）ICSJWG：Common Industrial Control System Vulnerability Disclosure Framework, 8 June 2012
21）IPA：脆弱性対策情報データベースJVN iPediaの登録状況［2012年第4四半期（10月～12月）］別紙1、2013年1月21日
22）Bryan Krekel, Patton Adams and George Bakos：Occupying the Information High Ground：Chinese Capabilities for Computer Network Operations and Cyber Espionage, Northrop Grumman Corporation, 7 March 2012
23）GAO：Report to Congressional Requesters：IT SUPPLY CHAIN National Security-Related Agencies Need to Better Address Risks, March 2012
24）Ian Mann：Hacking the Human：Social Engineering Techniques and Security Countermeasures, Gower Publishing Company, 2008