重要インフラに対するサイバー攻撃の実態と分析

野口 睦夫　植田 啓文

要 旨

近年、重要インフラ、特に電力システムにおけるサイバー攻撃の報告が増えています。重要インフラに対する攻撃は、これまで制御システムの構成や運用業務に関する知識が必要なことやインターネット接続がないことから、サイバー攻撃を受けるリスクは低いとされていました。しかし、重要インフラへのサイバー攻撃が社会に大きなインパクトを与えている現状においては、その攻撃手法を分析することによって、リスクを再確認する必要があります。本稿では、いくつかの電力システムへのサイバー攻撃の事例を参考に、どのようにシステムの保護施策を回避し攻撃を成功させたか、そのポイントについて説明します。

KeyWords　重要インフラ／制御システム／電力セキュリティ／サイバー攻撃／インシデント事例

1. はじめに

近年、電気・ガス・水道などの重要インフラのなかで、特に電力システムに対するサイバー攻撃の報告が増えています。これらの原因の多くは、過去に重要インフラにおいてシステムメンテナンスの効率化やコスト低減のために導入されたICTのコンポーネントにあります。それらが攻撃の入口となり、マルウェア感染を伴って制御システムへと侵入されています。ICTは、標準仕様や汎用OSなどのオープン化された技術が多く用いられているため、ICTを導入した重要インフラは情報システムと同様のセキュリティリスクを内包することになります。そのため、重要インフラでは、インターネットなどの外部ネットワークと制御システムを接続せずに運用するという対策が取られてきました。加えて、サイバー攻撃によって重要インフラに物理的被害を与えるには、制御システムの構成や運用業務を熟知する必要があり、情報システムと比べて攻撃は容易ではない[1]と考えられていました。しかし、StuxnetやBlack Energyという制御システムを狙ったマルウェアが登場し、外部ネットワークを経由せずともマルウェアが感染、制御システムが不正に操作されることが現実となっています。重要インフラがサイバー攻撃によって機能を停止することは、関連する市民生活、企業活動などの停止につながり、社会的に大きなインパクトになるため、このような制御システムを狙った攻撃の手法を分析し、今後のセキュリティ対策に反映させていくことが重要となります。

本稿では、重要インフラに対するこれまでのサイバー攻撃の事例を基にその手法を分析し、どのようにして重要インフラの保護施策を回避し攻撃成功に至ったのか、そのポイントについて説明します。

2. 重要インフラに対するサイバー攻撃の実態と分析

2.1 インシデント数の変化

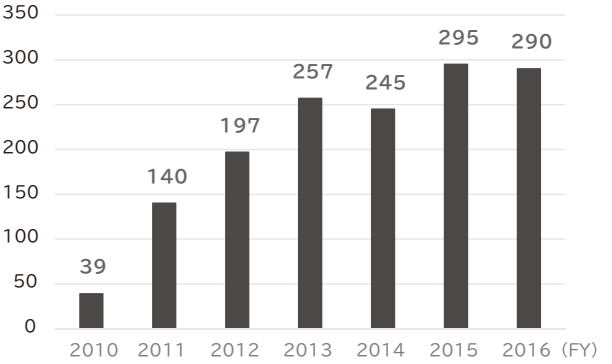
まず、**図1**で、近年の重要インフラにおけるインシデント数の変化を説明します。2010年にイランにあるウラン濃縮工場の遠心分離器を破壊したマルウェアStuxnetの登場以降、海外ではエネルギー分野や重要機器製造分野、通信分野などへのサイバー攻撃が増加しています。そのなかで、ウクライナでは電力システムを狙ったサイバー攻撃によって大規模停電が2015年と2016年に連続して発生しています[2]。このことから、電力など特に経済への影響が大きいエネルギー分野では、高度なサイバー攻撃を受ける恐れがあると考えられます。

2.2 サイバー攻撃によるインシデント事例とその原因

本節では、サイバー攻撃によって大きなインシデントが発生している電力などのエネルギー分野に着目し、**表1**にこれまでに発生したインシデント事例の一部を示します。2000年代は、ネットワークのブロードバンド化もあり世界中でICTの利活用が進み、重要インフラにおいては利便性や低コスト化の観点で制御システムのメンテナンス用にVPN接続機器の導入、Windowsなどの汎用OSを用いた制御機器の利用が拡大しました。その結果、従来は独自仕様だった制御システムがオープン化された標準仕様、汎用製品で構成されるようになりました。一方で、ICT導入がセキュリティリスクとなり、表1に示すようにVPNへの不正接続やUSBメモリを介したマルウェアの感染が多く発生するようになりました。この原因は、ICTの導入だけではなく、ソフトウェアの脆弱性が放置されていたことにもあります。制御システムにおいては、「システムの可用性を脅かす要因は極力排除する」という考え方があり、以下のような対応が困難な場合が多いという制御システム特有の事情があります。

・アンチウイルスソフトウェアの導入
・OSへのセキュリティパッチの適用
・導入されているソフトウェアの更新

また、マルウェア感染による被害に着目すると、当初は情報漏えいや過負荷による動作異常がありましたが、近年では物理的な被害が多くなっていることが分かります。このことから次節では、物理的な被害を出したサイバー攻撃手法について説明します。



FY：財政年度(10/1～9/30)
ICS-CERT Year in Review 2012-2016をもとに作成

図1　米国ICS-CERT[3]インシデント対応件数

2.3 物理被害を与えたサイバー攻撃手法の分析

本節では、制御システムの物理的な被害事例である(1) 2010年のイランで発生したマルウェアStuxnetを用いたサイバー攻撃と(2) 2015年にウクライナで発生したBlack Energy 3を用いたサイバー攻撃の手法の説明をします。

(1) イランのサイバー攻撃事例の分析

攻撃者の一連の行動を軍事行動になぞらえてモデル化するサイバーキルチェーン[4]を用いて、本サイバー攻撃の手順を**図2**に示します。「偵察」「武器化」の手法は明らかにされていませんが、一部では米国が事前

表1　重要インフラにおけるインシデント事例の一部

発生国	公表時期	事例内容	原因
米国	2001	SCADAシステム改修のため2週間停止	契約ベンダー向けVPN接続システムのアクセス保護の不備
米国	2003	デービス・ベッセ原子力発電所のSCADAシステムが約5時間、プロセスコンピュータが約6時間停止	Slammerが契約ベンダーが使用するVPN接続を介して侵入・感染
EU	2003	多数の配電変電所の管理機能が3日間喪失	分散SCADAシステムへのマルウェア感染
日本	2005	原子力発電所の機密情報がファイル共有ソフト経由で流出	従業員が機密情報を格納していた自宅PCにマルウェアが感染
日本	2006	火力発電所の機密情報がファイル共有ソフト経由で流出	従業員が機密情報を格納していた自宅PCにマルウェアが感染
米国	2006	ブラウンズ・フェリー発電所の再循環水ポンプの制御喪失	発電所統合ICSネットワーク上の過度のトラフィックによるSiemens Perfect Harmony VFDコントローラーの誤動作
米国	2010	コンピュータの誤作動により、ガスパイプラインからガスが漏えい	コンピュータの誤作動（誤作動の原因は不明）
イラン	2010	マルウェアStuxnetにより、ナタンズ燃料濃縮工場で遠心分離器が破壊	マルウェア感染
米国	2012	2つの発電所で制御システム環境内のコンピュータへマルウェアが感染し、片方は再稼働が3週間遅延、もう片方は運用制限が発生	作業用USBドライブへのマルウェア感染
米国	2014	米国とカナダの防衛航空会社や航空会社、EUを含めたエネルギー企業を標的とした攻撃による情報漏えい	DragonflyハッカーグループによるによってSCADAシステムにマルウェア（Havex）が感染
米国	2015	FirstEnergy社に対する大規模DoS攻撃（被害なし）	不明
ウクライナ	2015	ウクライナ西部（イヴァーノ＝フランキーウシク州）で数時間停電が発生	マルウェアBlack Energy 3を用いたサイバー攻撃
イスラエル	2016	コンピュータシステムの一部がサイバー攻撃対応のため、2日間停止	フィッシング攻撃によるマルウェア感染
ドイツ	2016	2013年または2014年頃にサイバー攻撃によって混乱が発生した事実の公表	不明
ウクライナ	2016	キエフ市内の電力供給先の5分の1が約1時間停電	マルウェアIndustroyer/Crash Overrideを用いたサイバー攻撃
ウクライナ	2017	チェルノブイリ原子力発電所の放射線モニタリングシステムへのマルウェアNotPetyaの感染によって手動制御を余儀なくされる	マルウェア感染（ランサムウェア）

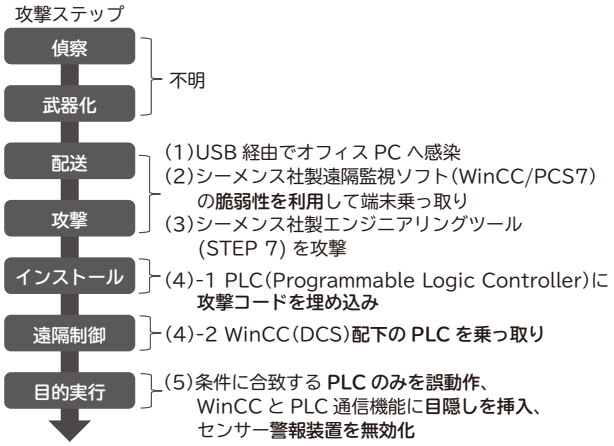


図2　Stuxnetを用いたサイバー攻撃の流れ

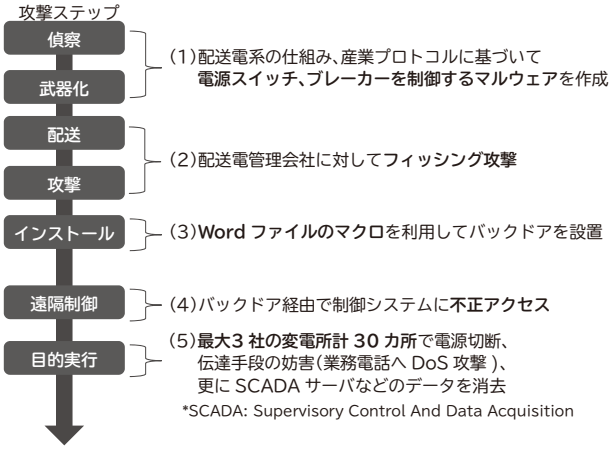


図3　Black Energy 3を用いたサイバー攻撃の流れ

に情報を収集し、リビアから接収した核施設設備を利用してStuxnetを作成したという情報[5]があります。この攻撃の特徴は「汎用化された制御機器の脆弱性を利用」と「攻撃を隠すための通信の隠ぺい及び警報装置を無効化」したことにあります。制御システムは、本来は警報装置や作業員が機器の稼働状況を監視していますが、それらを巧みに無効化した点がサイバー攻撃による物理的な破壊を成立させた要因と考えられます。

(2) ウクライナのサイバー攻撃事例の分析

ウクライナにおけるマルウェアBlack Energy 3の攻撃手順を (1) の事例と同様に**図3**に示します。本攻撃の特徴は「マルウェア作成に産業用プロトコルの知識を有した人間が関与」「変電所計30カ所に対する大規模な同時攻撃」「攻撃発生時のインシデント対応への妨害工作 (業務連絡手段の麻痺、データの削除)」の3点と言えます。これまでに制御システム機器への直接的な攻撃はあったものの、制御システム間の通信で用いられる産業用プロトコルを利用し、多数の制御システムが同時に攻撃されることはありませんでした。加えて、攻撃の隠ぺい方法が通信の隠ぺいから復旧業務を妨害する攻撃に変化しており、このことも被害拡大につながったと考えられます。そのために、制御システム及び運用業務への同時攻撃が攻撃成立の要因と考えられます。また本事例から、攻撃者は、サイバー攻撃で大規模停電を引き起こすことが可能なレベルにまで、制御システムの仕組みや運用業務に熟知してきていることが分かります。

2.4 重要インフラへのサイバー攻撃の成立条件

第2章2節、第2章3節で述べた重要インフラへの物理的被害を与えたサイバー攻撃の成立条件を下記にまとめます。

(1) オープン化された制御システム機器の利用
(2) 攻撃者による仕様や運用業務への理解
(3) 多重障害 (復旧業務の妨害を含む)

一部の制御機器は、汎用OSを用いており、第2章2節で述べたようにソフトウェアパッチの適用が困難であることを攻撃者は利用しています。また、攻撃者が制御システムの仕様や運用業務を把握していることで、的確に攻撃が組み立てられています。

なお、通常、制御システムは、IEC61508[6]を基本とする機能安全に基づきシステムの可用性維持の対策が行われており、偶発的な (単一的な) 故障に関しては非常に強いものとなっています。しかし、前述したようにサイバー攻撃は、攻撃者により意図的に多重障害を発生させることができます。このような多数の障害が同時に発生することは、機能安全の観点では確率が非常に低く見積もられてしまうため、多くの運用組織ではそれらを想定した対策はできていないと考えられます。そのため、多重障害を発生させ、機能安全の仕組みを回避することがサイバー攻撃を成功させるポイントになります。

3. 現状の電力システムの保護施策とその重要性

3.1 米国におけるセキュリティ対策

本節では、電力システムに対する現在の保護施策について説明します。第2章で述べたように、制御システムに対するサイバー攻撃の脅威が高まったことから米国では**表2**に示す規制、組織が整備されました。北米電力信頼度協議会（NERC）によって電力システムの最低限のセキュリティ（表2中（1））が策定され、電力会社は対策実施及び報告の義務が課されるようになり、また電力会社間の情報共有のための組織E-ISAC（Electricity Information Sharing and Analysis Center）が設置されました。更には、サイバー攻撃発生時に適切な対応が取れるようにトレーニングの実施が定められています（表2中（5））。このような政府主導で規制がかかった背景には、政府において重要インフラのセキュリティは国土の安全保障を揺るがすものという強い認識があったためと考えられます。

3.2 日本におけるセキュリティ対策

日本では、2014年に成立したサイバーセキュリティ基本法により、電力・ガスなどの重要インフラに関してもセキュリティ強化が考えられ、2017年に米国同様に電力事業者間のサイバーセキュリティに関する情報共有・分析を行う組織である電力ISAC（JE-ISAC）が設立されました。一方で、**表3**に示すように、米国とは対照的に対策基準などの検討は十分に進んでいません。その理由としては、日本国内の重要インフラでサイバー攻撃による重大インシデントが起きていないことが大きな要因と考えられます。加えて、頻繁に自然災害に見舞われる日本では、大規模停電からの復旧など、電力システムの維持、運用は諸外国に比べ安定しており非常に高いレベルのものとなっています。そのような状況も検討が進まない要因の1つとなっていると考えられます。

表2　米国における電力システムのセキュリティ規制

項目	米国
(1)基準	NERC CIP Standards version 6(標準ガイドライン) ※NERCが策定し、エネルギー規制委員会(FERC)が承認 11文書全383ページからなる電力分野の義務的な基準 その他、代表的なガイドライン NIST IR 7628(スマートグリッド向けガイドライン) ES-C2M2(マネジメント成熟度モデル) NIST Framework(重要インフラ全般向けガイドライン) NIST SP 800-82(制御系システム全般向けガイドライン)
(2)監査	北米電力信頼度協議会(NERC) ※州による規制がある場合は州政府も実施
(3)侵入検査	各事業者判断で実施 ※脆弱性アセスメント(机上あるいは動的なもの)については NERC CIPで実施を義務付け
(4)情報共有	Electricity ISAC(E-ISAC)
(5)演習	Grid Ex(系統事業者のセキュリティ演習)、Cyber Storm (米国大のサイバーセキュリティ演習)など 制御系システムセキュリティについての技術開発なども実施

表3　日本における電力システムのセキュリティ規制

項目	日本
(1)基準	電力制御システムセキュリティガイドライン ※JESC規格番号：JESCZ0004(2016) 2016/05/30制定、12ページ構成で概念的な基準
(2)監査	なし
(3)侵入検査	任意
(4)情報共有	電力ISAC(JE-ISAC)(2017/03発足)
(5)演習	任意

3.3 電力システムの保護施策の重要性

前節で述べたように、同じ先進国であっても米国と日本では対策状況が異なっています。そこで、電力システムの保護施策の重要性について、本節では経済的な被害額を指標として説明します。世界の主要な軍需企業である米国ロッキード・マーチン社とケンブリッジ大学からイギリスの電力システムへのサイバー攻撃を想定した社会的被害予測が報告されています[7]。本予測によれば、サイバー攻撃によって数週間にわたって停電した場合、インシデント発生から5年間にもわたり経済的な影響が継続し、損失額はGDPの2.3%相当と試算されています。先進国の経済成長率が数パーセント[8]であることを鑑みると、電力システムへのサイバー攻撃は経済成長に大きな停滞を引き起こす要因になり得ると考えられます。一方で、近年では特定企業や重要インフラを対象としたサイバー攻撃を実施している攻撃グループの背景に、特定の国家が関係しており、国家の思惑に基づいたサイバー攻撃が行われる[9)10)11)]など、サイバー攻撃を中心とした国家間の駆け引きが起きています。今後、ますます国家間の対立が深まり、サイバー攻撃による他国への介入が本格的に行われるようになると、社会的インパクトの大きい電力システムは明確な攻撃対象の1つとされ得ると考えられます。そのため、日本においても十分な保護施策の検討・策定が必要と言えます。

4. まとめ

電力システムをはじめとする重要インフラへのサイバー攻撃は経済的影響が大きく、また国家間の争いにおける攻撃対象とされる恐れがあります。一方で、重要インフラにおいて従来の「インターネットとつながっていない制御システムは安全」や「業務知識がないと攻撃は困難」などの考え方は通用する状況ではなくなりました。今後は、攻撃者にシステム構成や運用業務が把握されていることを前提に、電力システムのセキュリティ対策を考えていく必要があります。また、国家間の争いの対象となり得ることを考えると、E-ISACやJE-ISACのような業界の取り組みと国との連携だけでなく、他のISACとの連携を含め、更なる官民の深い連携が今後は重要になっていくと考えられます。

参考文献

1) 経済産業省：電力分野におけるサイバーセキュリティ対策について，2016.7
http://www.meti.go.jp/committee/sougouenergy/denryoku_gas/kihonseisaku/pdf/007_06_00.pdf
2) ArsTechnica：Hackers trigger yet another power outage in Ukraine，2017.1
https://arstechnica.com/information-technology/2017/01/the-new-normal-yet-another-hacker-caused-power-outage-hits-ukraine/
3) ICS-CERT
https://ics-cert.us-cert.gov/
4) サイバーキルチェーン
http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html
5) ArsTechnica：Confirmed: US and Israel created Stuxnet, lost control of it
https://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/
6) International Electrotechnical Commission：Functional Safety and IEC 61508
http://www.iec.ch/functionalsafety/
7) Kelly, S. et al.：Integrated Infrastructure: Cyber Resiliency in Society, University of Cambridge, 2016.01
8) United Nations：National Accounts Main Aggregates Database
https://unstats.un.org/home/
9) FBI Press Releases：Update on Sony Investigation, 2014.12
https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation
10) FBI Implicates North Korea in Destructive Attacks, 2014.12
https://www.crowdstrike.com/blog/unprecedented-announcement-fbi-implicates-north-korea-destructive-attacks/
11) WIRED：Your Guide to Russia's Infrastructure Hacking Teams, 2007.12
https://www.wired.com/story/russian-hacking-teams-infrastructure/

執筆者プロフィール

野口　睦夫
セキュリティ研究所
主任

植田　啓文
セキュリティ研究所
主任

NEC 技報のご案内

NEC 技報の論文をご覧いただきありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報（日本語）　NEC Technical Journal（英語）

Vol.70 No.2　ビジネスの安全・安心を支えるサイバーセキュリティ特集
～Futureproof Security　安心の先へ。～

ビジネスの安全・安心を支えるサイバーセキュリティ特集によせて
増大するサイバー犯罪の根源的な解決へ～“産学官”のオールジャパンで立ち向かう第三者機関の姿とは？～
サイバーセキュリティを取り巻く社会動向とNECの取り組み

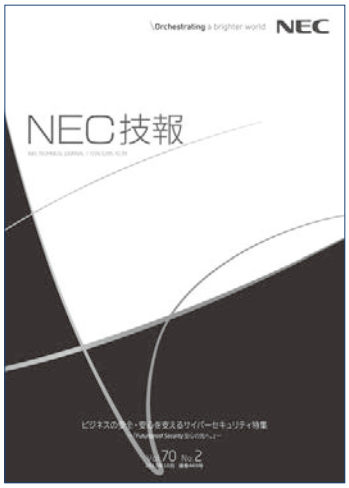
◇ 特集論文

社会の動向とNECの取り組み
重要インフラに対するサイバー攻撃の実態と分析
2017 サイバー攻撃最新動向 NEC Cyber Threat Intelligence活用モデル
サイバーセキュリティ対策の社内事例

サイバーセキュリティソリューション
複雑化 / 高度化するサイバー脅威に対抗するSOCとセキュリティ監視サービス
攻撃被害を極小化するためのインシデント対応支援ソリューション
サイバー演習によるインシデントハンドリング能力の強化
セキュリティ統合管理・対処ソリューション「NEC Cyber Security Platform」
クラウド型ファイル暗号化サービス －ActSecureクラウドセキュアファイルサービス－
セキュリティLCMサービス
EMMを活用したセキュアなモバイルワークソリューション
IoT 時代の経営を支援するサイバーセキュリティコンサルティング

サイバーセキュリティへのAI技術の活用
AI（人工知能）を活用した未知のサイバー攻撃対策
採るべき対策の「なぜ？」に答えるAIの可能性
オープンソースインテリジェンスを活用したサイバー脅威の検出と自動分析
犯罪捜査支援のためのサイバー・フィジカル統合分析技術

お客様に安全・安心を届けるための社内の取り組み
安全・安心な製品・サービスをご提供するための取り組み ～セキュア開発・運用～
サイバーセキュリティ人材のタレントマネジメント



Vol.70 No.2
（2017年10月）

特集TOP