

平成23年度

# 「情報セキュリティに関する懸賞論文」受賞作品

テーマ

- 1 災害時の情報システムのあるべき姿
- 2 PC機能を持った携帯情報端末、例えばスマートフォンによる  
ソーシャルメディア時代の情報セキュリティのあり方について
- 3 サイバーテロ攻撃への対応
- 4 自由課題  
(情報セキュリティ意識の向上に資する内容)

平成23年12月

財団法人 防衛調達基盤整備協会



## 発刊にあたって

財団法人防衛調達基盤整備協会は、情報セキュリティ意識の向上に資するため、情報セキュリティに関する懸賞論文を募集するという事業をおこなっており、今年度で第4回目となりました。この事業は、多くの方から論文を応募していただき、優秀な作品を表彰し発表する事により、広く国民各層に情報セキュリティに対する知識と技術を広め、ひいては防衛基盤の強化に寄与する事を目的としております。

今年度の懸賞論文テーマの選定に当たっては、大きく次の2点が背景となりました。

1 点目は、3月に発生した東日本大震災は人的、物的に未曾有の被害をもたらし、情報インフラにも大きな被害をあたえました。これにより事業継続に必要なデータを喪失した企業・公共団体が事業再建に向けて、事業再建のための実践可能な災害時に耐えうる情報システムはどうあるべきかについてです。

2 点目は、インターネットの普及に伴い、ネットワーク通信による情報・知識の利用が社会生活の多くの部分に浸透する反面、セキュリティ脅威も増大し、政府機関や防衛関連企業等に対する不正アクセスが行われており、昨年からは特定の企業や個人を標的とする新しいサイバー攻撃手法も出現しています。このようなネットワークを利用した組織的攻撃の脅威が高まっている状況をどのように捉え、どのように対処していけば良いのかについてです。

「情報セキュリティに関する懸賞論文」の選考に当たっては、当協会が委嘱した学術、電気通信研究、保全教育、インターネット、報道の各分野の有識者で構成された情報セキュリティ論文選考等委員会で厳正な審査を行い、優れた論文であると答申を受けた三つの作品を表彰させて頂くとともに、受賞作品を小冊子にまとめ、発表することといたしました。

受賞作品は、読み手が理解を深め意識を高められるよう、解り易い内容と思いますので、情報セキュリティに対する知識と技術の向上に役立てていただければ幸いです。

平成23年12月

財団法人 防衛調達基盤整備協会

理事長 宇田川 新一

## 論文選考にあたって

インターネットの普及は目覚ましく、様々なサービスにより国民生活や社会経済活動において本格的にインターネットを利用する時代になりました。さらに、PCの機能を持つ携帯情報端末、例えばスマートフォンは人々のコミュニケーションの手段だけでなく、ビジネスでの活用も進められています。そのような中、3月に発生した東日本大震災は情報インフラにも大きな被害を与え、インターネットや携帯情報端末の使用が制限されるとともに企業や自治体の事業継続にも大きな影響を与えています。

このような状況のなか、財団法人 防衛調達基盤整備協会は情報セキュリティ意識の向上に資するため、「情報セキュリティに関する懸賞論文」を募集し、優秀な作品を表彰し発表する事業を企画し、私どもが審査致しました。

作品の選考に当たっては、広く国民各層に情報セキュリティに対する知識と技術を広めることを目的として、読み手がそれぞれのテーマについての理解を深め意識を高められるよう、具体的かつ解り易い内容の論文で、且つ、新鮮度、実証度合、影響度などの審査基準により審査を行い、最終的に3点が選ばれました。

最優秀賞の戸木氏の作品は、災害時に耐えうる中小企業の情報システムを目指すため、可用性、完全性を主眼とした情報セキュリティ対策及び管理策として地域・コミュニティ・マルチという三つの視点など新規性に富んだ提案を評価したものです。

佳作（情報セキュリティ啓発賞）の猪股氏の作品は、Stuxnetによる新しいサイバー攻撃手法について分析したものであり内容も解り易く、具体的であり、社会に与える影響度も高いことを評価したものです。

佳作（情報システム復旧対策賞）の岩崎氏の作品は、大規模災害発生後の情報システムの災害対策に焦点を当て、復旧対策の手順について提案したものであり内容も解り易く、具体的であり、社会に与える影響度も高いことを評価したものです。

いずれも優れた論文であり、発表することによって情報セキュリティ意識の向上に貢献し、ひいては、防衛基盤の強化に寄与することを願っております。

平成23年12月

情報セキュリティ論文選考等委員会  
委員長 中 尾 定 彦

目 次

最優秀賞

表 題：災害時に耐えうる中小企業の情報システムを目指して  
日本ユニシス株式会社 サービス企画部  
セキュリティビジネス企画担当部長  
戸 木 貞 晴 氏・・・・・・・・ 1

佳 作(情報セキュリティ啓発賞)

表 題：Stuxnetの脅威と今後のサイバー戦の様相  
陸上自衛隊 通信団 システム防護隊技術隊  
分析設計専門官  
猪 股 晃 匡 氏・・・・・・・・ 15

佳 作(情報システム復旧対策賞)

表 題：東日本大震災を踏まえた災害時情報システムの復旧手順の  
ありかたについて  
情報セキュリティ大学院大学  
博士前期課程  
岩 崎 正 治 氏・・・・・・・・ 31

平成23年度情報セキュリティに関する懸賞論文募集要項・・・・・・・・ 45

## 最優秀賞

災害時に耐えうる中小企業の情報システムを目指して

日本ユニシス株式会社 サービス企画部  
セキュリティビジネス企画担当部長  
戸木 貞晴



## 1 はじめに

2011年3月11日に発生した東日本大震災は、わが国の観測史上最大となるマグニチュード9.0を記録した。この地震と津波により、多数の建物や設備が損壊、流失し、その被害は、当該地域の住民、学校、企業、インフラ、自治体、病院など極めて広範囲に及んだ。被災地域のオフィスや生産拠点に設置されていた多くの情報システムも被害を受け、多くの事業が継続困難に陥った。その原因のすべてが、情報システムにあるとは言えないまでも、情報システムの可用性(Availability)、完全性(Integrity)に関する対策実装は十分であったのか。言い換えれば、情報の機密性(Confidentiality)を偏重し、その結果、管理策の実装が不均衡になっているのではないか。

本稿では、中小企業が保有する情報システムの情報セキュリティに着目する。中小企業は、我が国の全企業数の99.7%を占め、約420万社にもなる。従業員数では、我が国の全従業員数の71%となる約2800万人が働いている。<sup>1</sup> 中小企業向けには、「中小企業BCP策定運用指針」が策定されているものの情報システムの可用性、完全性の実装に関する具体的な記載は少ない。一方、大企業は、多彩な人材、豊富な資金力により情報システムのディザスタリカバリ(disaster recovery)施策及び事業継続(BCP:business continuity plan)は、十分とは言えないまでも対策は考えられているはずである。また、重要インフラ事業者(情報通信、金融、電力、航空、鉄道、ガス、政府・行政サービス、医療、水道、物流等の事業に係わる者)は、情報セキュリティの管理的対策や技術的対策等について、「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針」に従い整備、運用がなされているであろう。

しかし、中小企業は、上述の通り、我が国の産業において重要なポジションであるにもかかわらず、情報セキュリティ対策は遅れている。今、中小企業の現場において、求められているのは、実行困難な原因の排除や実現への障壁が高い対策の提言ではなく、現実実践可能な解決の糸口であり、具体的かつ身の丈にあった管理策の選択肢である。そこで、本稿では、災害時に耐える中小企業の情報システムを目指すための具体的な施策を提言する。

## 2 災害の影響と中小企業の情報システムの実態

情報システムの災害対策の目的は、情報システムの罹災を起因とした業務停止の予

---

<sup>1</sup> 中小企業白書2011年版によれば、中小企業は全企業数の99.7%を占め、419.8万社、その従業員数は2784万人(我が国の雇用の71%)である

防、及び、情報システムが停止した場合、合理的な時間内で業務再開を可能とするための事前準備である。その為には、まず、情報システムが災害により受ける影響と中小企業の情報システムの実態を把握する必要がある。

## 2.1 災害が情報システムに及ぼす影響

災害とは、気象などの自然現象の変化、或いは、人為的な原因などによって、人命や社会生活に対する被害を生じる現象である。災害が情報システム及び情報資産に与える影響を表したのが表1である。災害の事象が発生した場合、情報システム及び情報資産の可用性、完全性、機密性のいずれかが侵害される可能性がある場合に○印をプロットした。例えば、地震により津波が襲来し、情報システムが水損、破壊された場合は、その情報システムの可用性は失われる。また、突如電力供給が停止した場合、ハードディスクの故障やデータの破損によりデータの完全性を失う可能性がある。表1からも読み取れるように、災害は、情報資産の機密性に対する影響よりも、可用性、完全性を侵害する可能性が高いことがわかる。したがって、災害対策は、可用性、完全性を主眼とした情報セキュリティ対策が有効であると言えよう。

一方、システム化されていない業務の場合には、取引情報、設計図、顧客情報などは、文書で保管されているはずである。一般的に、大企業よりもシステム化がなされていない中小企業では、これらの情報を通常業務で利用し、紙媒体として執務室等で保管しているケースが多い。ゆえに、中小企業の場合は、紙媒体で保管されている文書を災害からどのように守るかについても、同時に考える必要がある。

分類	災害の事象	被害対象							
		物理的環境及び情報システム (ハードウェア、ソフトウェア、 データ、媒体、ネットワーク、設備など)					紙情報(ドキュメント類)		
		完全性への影響			可用性 への影 響	機密性 への影 響	完全性、可用性への影響		
		水損	焼失	破損 減失			水損	焼失	破損 減失
台風・豪雨・ 風水害 低気圧・前線・ 集中豪雨 潮位上昇	高潮・高波	○			○		○		
	河川氾濫・堤防破壊	○			○		○		
	内水浸水	○			○		○		
	倒壊			○	○				○
	がけ崩れ・地すべり			○	○				○
	土砂災害・土石流			○	○				○
地震	震動			○	○				○
	津波	○		○	○		○		○
	地震火災		○		○			○	
	がけ崩れ			○	○				○
	液状化			○	○				○
火山	噴火・火砕流・溶岩流		○	○	○			○	○
	噴煙・降灰・火山弾・火山砂		○	○	○			○	○
	火山泥流		○	○	○			○	○
生物	インフルエンザ・Sars								
	虫害			○	○				○
	生物の異常発生			○	○				○
隕石	隕石被弾		○	○	○			○	○
フェーン現象	火災		○	○	○			○	○
工場災害	爆発		○	○	○			○	○
	火災		○	○	○			○	○
インフラ遮断・ 供給停止	電話・FAX				○				
	ネットワーク			○	○	○			
	電気			○	○				
	水道			○	○				
	ガス				○				
事故	交通事故・飛行機事故等								
	労働災害			○	○				○
風評	報道被害・風評被害								
人為的災害・ 犯罪	放火		○		○			○	
	漏電		○		○			○	
	失火		○		○			○	
	不正アクセス			○	○	○			○

表1 災害の事象と情報被災の関連表<sup>2</sup>

## 2.2 中小企業の情報システムの特徴

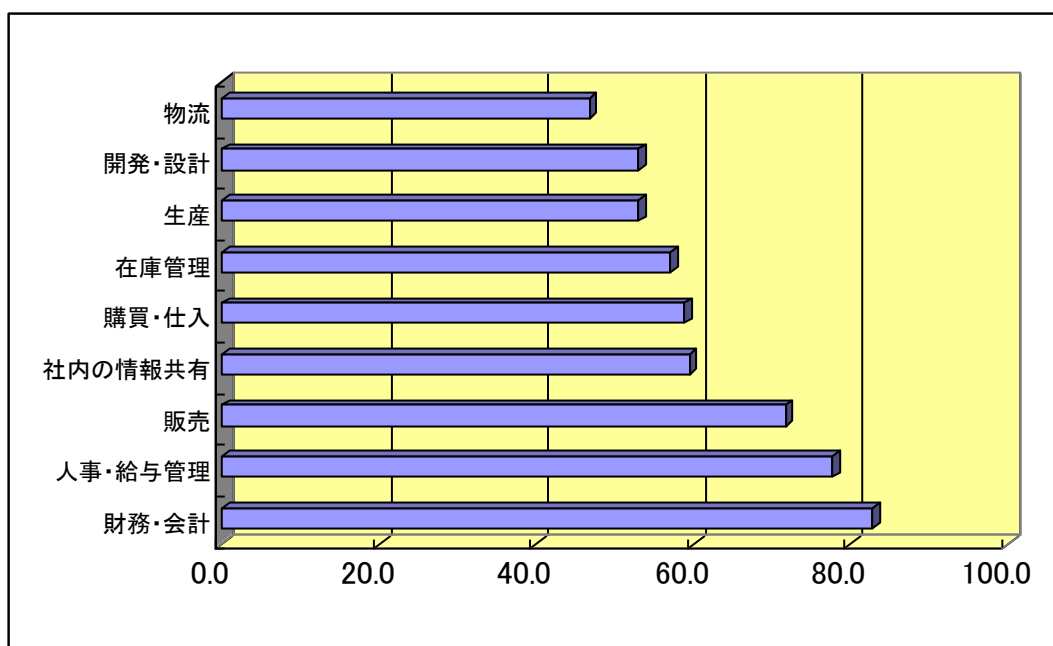
中小企業が持つ情報システムを災害から守るためには、大企業とは異なる情報システムの特徴を知る必要がある。それは、どのような業務がシステム化され、どのように運用されているのかを知ることにより、災害時でも耐えうる情報システムへの具体的なリスク管理方法を導き出せると考えるからである。

<sup>2</sup>総論：情報管理における危機管理のあり方 小川雄一郎 表1「災害と被害の関連」を参考に、筆者が独自に作成した

グラフ1は、中小企業が導入している情報システムの業務種別の調査結果である。中小企業は、財務会計、人事給与、販売システム、社内情報共有などのシステム化が進んでおり、調査対象の約6割の中小企業が導入済みであることがわかる。グラフ2は、中小企業におけるパッケージソフトウェアの利用率調査結果である。中小企業では、財務会計、情報共有、人事などにおいてパッケージソフトウェアの採用比率が高く、特に、財務会計業務では、約7割がパッケージソフトウェアを採用している。グラフ3は、中小企業のサーバ設置場所実態調査である。グラフ4は、ネットワーク回線及びデータのバックアップの実装率である。中小企業では、15%程度しかバックアップを実施していないことがわかる。上記4つの調査結果から、中小企業の現場で稼動している情報システムの運用イメージは以下の通りである。

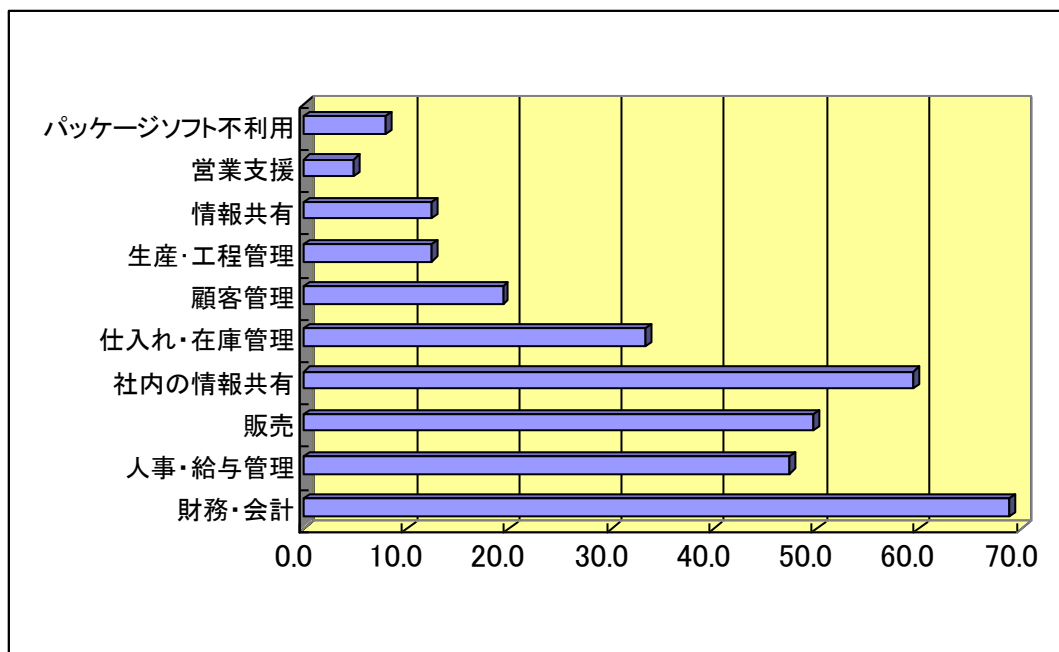
- ・ 財務会計、人事給与、販売、社内情報共有(メール、グループウェアなど)、購買仕入、在庫管理などの業務領域のシステム化が進んでいる
- ・ 定型業務もしくはパッケージソフトウェアに適合性の高い業務、財務会計、人事給与、販売、社内情報共有などの業務において、パッケージソフトウェアを積極的に採用している
- ・ 情報システム機器は、ほぼ100%事務所内に設置している
- ・ ネットワーク回線の二重化を実施している中小企業は、非常に少ない
- ・ データのバックアップを実施している中小企業は、非常に少ない

グラフ1 中小企業が導入している情報システム



資料:三菱 UFJ リサーチ&コンサルティング(株)「IT の活用に関するアンケート調査」  
 (2007 年 11 月)(ここでの中小企業とは従業員 300 人以下(卸売業、サービス業では 100 人以下、小売業では 50 人以下)を対象としている)

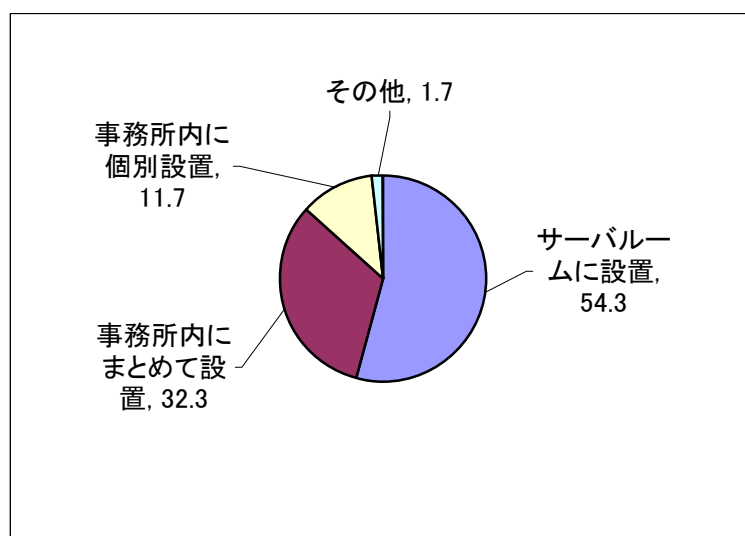
グラフ2 中小企業におけるパッケージソフトウェアの利用率



※財団法人全国中小企業情報化促進センター

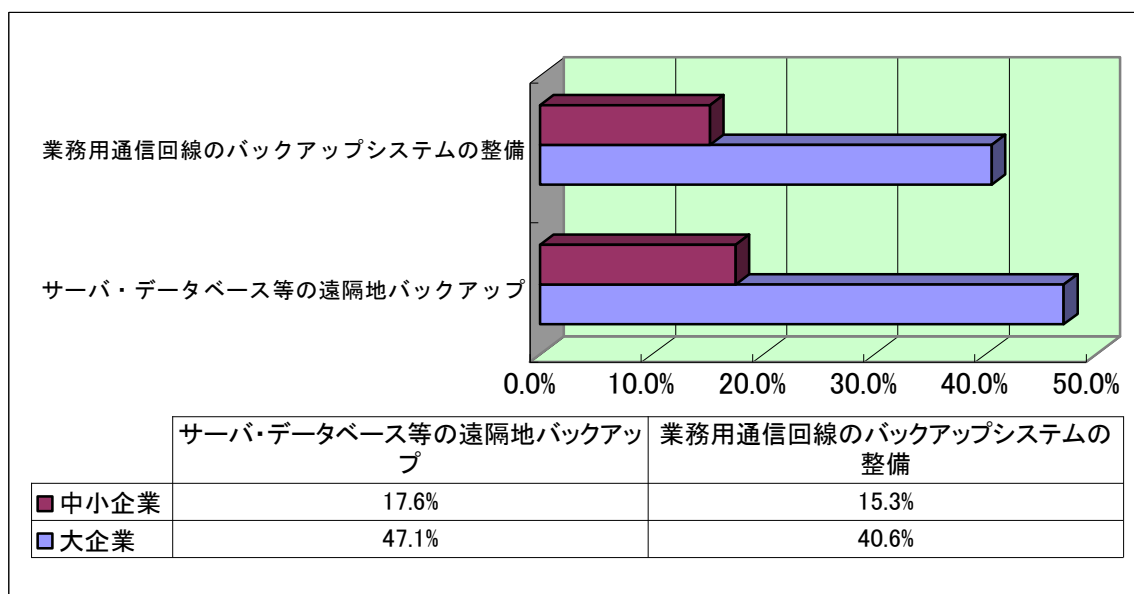
平成 19 年度(2007 年)中小企業のIT利活用実態調査P26 から引用

グラフ3 中小企業のサーバ設置場所実態調査



※出典 IT Pro 中堅・中小企業のIT導入実態調査(2007 年版)

グラフ4 中小企業の回線及びデータバックアップ実施比率



※出典 平成 18 年 6 月 名古屋商工会議所 名古屋地域における企業防災の実態調査 P17の資料から一部抜粋（回答社数大企業 156 社 中小企業 673 社）

### 3 災害対策における情報システムのリスクマネジメント

JIS Q 27002:2006 によれば、災害は、脅威の識別において、環境的脅威に分類され、地震、津波、台風などがあげられている。しかし、その脅威の発生そのものを人間の力でなくすことは難しい。加えて、多くの中小企業において、災害事象を網羅的に想定し、個々の管理策を実装することは現実的ではない。

また、リスク値は、資産の価値×脅威×脆弱性で算出する。災害発生率を脅威の算定に用いるため、自然災害、人為的災害いずれも、発生確率は低く、定量化された数値は低い数値になる。また、脆弱性についても、「環境的脅威に対するリスクが顕在化する恐れがない」、もしくは「最高水準の対策を実装済み」などの評価の根拠は乏しいのが現実である。したがって、災害対策の場合は、リスクを定量化し、その対策範囲を決定しても、実質的には、評価者の主観に依存してしまうケースが多い。

一方、ISO/IEC Guide51 によるリスクアセスメントの考え方を適用すると、「リスク＝危害の発生確率（頻度）×危害のひどさ」のように表される。危害のひどさは、評価者の被災者の被災イメージにより定量化する数値が異なり、大半が主観的な査定になってしまう。さらに、日常的に発生する小さな災害よりも、めったに起こらないが極端に大きい災害の方がニュース価値は高く、報道量も圧倒的に多くなる。こうして、災害に関するメディア報道は、危害のひどさの判定に査定者にバイアスを加える。また、危害のひどさはリスクの

大きさの決定に影響力が大きいですが、発生確率は、リスクの大きさを決定するほどの影響力はない。つまり、リスク、危害のひどさ、発生確率の間には有意性のある相関関係はみられない。このように、環境的脅威に対する合理的なリスクアセスメントは難しい。

セキュリティは、第一義的には、経済問題である。許容できるリスクと投資余力を判断し、その前提条件下で、どのような管理策を実装すれば最も効果的であるかを考える。しかし、大企業や官公庁、インフラ産業と同様のリスクアセスメント方法の採用は、多くの中小企業では無理がある。したがって、中小企業の情報システムの実態から、環境的脅威に対する一般的な解決策とこれからの時代に相応しい新しい考え方を提言したい。

### 3.1 中小企業の情報システムへの脅威と脆弱性及び推奨する管理策

情報システムが稼働できなくなる要因は、大きく 4 つある。まず、物理的損壊である。火災、水損、破壊などのダメージを受けると、業務継続に加え、再稼動も困難になる。2つめは、電力供給の停止である。雷や不安定な電力供給による瞬断、長時間に及ぶ停電などの両面から電力供給について対策が必要である。3つめは、通信網の寸断である。多くの情報システムは、ネットワークで接続され、その機能をもたらす。つまり、ネットワークの寸断は、その情報システムの稼働停止と同様となる。4つめは、データである。パッケージソフトウェアは勿論、自社独自開発のアプリケーションであっても、バックアップがあれば再稼動できる。しかし、日々のビジネス情報を蓄積したデータは、再調達することはできない。

前述の通り、中小企業の多くは、情報システム機器を自社管理下に設置し、パッケージソフトウェアの採用が多く、ネットワーク回線は単独契約であり、データバックアップは実施していない。このような情報システムを災害から守る一般的な管理策提案であれば、表2の通りである。しかし、本稿では、ごく一般的に導き出される解決提案ではなく、立案の視点を、「地域で考える」、「コミュニティで考える」、「マルチで考える」、という 3 つの視点で提案する。

表2 中小企業の災害に対する一般的な解決策

災害の事象	サーバ機器類に与える影響の原因	サーバ機器類に与える影響	中小企業でも実現可能な解決策
高潮・高波	水の浸入による 障害発生	稼働停止	機器類を移転する
河川氾濫・堤防破壊			水害発生の少ない地域に移転する
内水浸水			機器類をIDCに置く(ハウジング、ホスティング)
津波			レンタルサーバ、IaaS、SaaS/Aspにする
			機器類は移転しない
			機器類を上層階に置く
			防水扉を設置する
倒壊	異常な圧力による 物理的な破壊	稼働停止	機器類を移転する
がけ崩れ・地すべり			地震、がけ崩れなど発生の少ない地域に移転する
土砂災害・土石流			機器類をIDCに置く(ハウジング、ホスティング)
震動			レンタルサーバ、IaaS、SaaS/Aspにする
がけ崩れ			機器類は移転しない
液状化			機器類に耐震・免震装置類をつける 落下防止、転倒防止装置類をつける
ネットワーク寸断	想定外の圧力 物理的な 切断・破壊	電気(稼働停止) 水道(空調停止) ネットワーク (データ更新停止)	機器類を移転する
電気寸断			機器類をIDCに置く(ハウジング、ホスティング)
水道寸断			レンタルサーバ、IaaS、SaaS/Aspにする
			機器類は移転しない
			回線、電力を二重の供給契約をする UPS、水タンク等を設置する 落下防止、転倒防止装置類をつける
隕石被弾	想定外の圧力、 熱、火による物理 的破壊	稼働停止	機器類を移転する
火災・爆発			機器類をIDCに置く(ハウジング、ホスティング)
噴火・火砕流・溶岩流			レンタルサーバ、IaaS、SaaS/Aspにする
噴煙・降灰・火山弾等			機器類は移転しない
火山泥流			防火扉を付ける
地震火災			防火シャッター、防火戸を付ける
放火・漏電・失火			

### 3.2 地域で考える

インドでは、数社がまとまってハイテクゾーン、ビジネスゾーン、ハイテクパークなどという呼称で、同業、異業種問わず集積した地区にオフィスを構えることが多い。その目的の多くは、「シェア」である。共用化の効果が期待できる自家発電システム、停水に備えた給水システム、防犯上のセキュリティ設備など危機管理用の設備を共同利用するのである。電気が安定して供給されるというのは先進国だけの常識であり、多くの新興国は、公共のインフラに期待しすぎることはない。期待が薄いゆえに、自ら共同体を形成し、トラブルに備える習慣が身についている。新興国では、ごく当たり前の考え方を、日本の地域社会、中小企業が連携し、社会インフラが脆弱な新興国を逆に見習うのである。

日本の少ない停電回数、短い停電時間は、世界でも屈指である。しかし、今回の震災を契機にその品質の高さにも陰りが出ている。一方、中小企業単独で、自家発電装置の導入、運用準備は、現実性に乏しい。そこで、小水力発電、太陽光発電、風力発電、バイオマス発電など、エコエネルギー発電を地域の自治体と中小企業が協力するのである。

。その中でも、燃料の輸入も不要であり、安定した出力も得られる小水力発電を推奨したい。山が多く、雨も多く、農業用水、街の水路、砂防ダムなどの豊富な水源がある我が国の特徴を活用できる。すでに、京都嵐山の渡月橋では落差 1.7 メートルの落差の水流で最大出力 5.5 キロワットを発電している。この電力で、渡月橋の夜間照明を行い、余剰電力は電力会社に売電し維持管理費に充当している。夜間の安心と安全を維持し、景観を高め、環境に良い観光地をアピールすることで観光客、視察訪問など集客効果も高い。都市圏でも、挑戦する価値はあるはずであり、このように発電した電力を、平常時は、売電や地域の環境整備などに利用し、電力寸断時は、この電力を予め決めておいた地域の中小企業や自治体のコンピュータへ供給する仕組みを構築しておけば、必要最低限の情報システムを稼働できる。

京都嵐山 桂川の小水力発電装置



<http://d.hatena.ne.jp/KokusaiTourist/20110615/p1>

京都嵐山 渡月橋の夜景



[http://www.geocities.jp/dst\\_tx/rs037\\_togetukyou.html](http://www.geocities.jp/dst_tx/rs037_togetukyou.html)

### 3.3 コミュニティで考える

次は、災害時の情報収集を地域コミュニティで行う提案である。業務再開までの目標時間の設定には、以下の4つの視点で情報が必要になる。まず、従業員、設備等の被災状況、協力会社の被災状況、顧客の被災状況、事業インフラ(電気、水道、ガス、通信道路など)の情報を揃える必要がある。災害時は、正確、迅速な情報収集と分析が、適切な意思決定と行動を導く。万が一、通信網が遮断された場合は、これらの情報を入手することが困難になり、適切な意思決定と行動ができないことになる。

東日本大震災では、固定網、携帯網問わず、輻輳が発生、通信規制が自動発動された。携帯電話による電子メールの送受信も、メールサーバの処理能力を超過し、メール到着通知に音声域を利用していたため、届いていても自らがメールを確認しないとわからないという事態に陥った。このようにして、情報流通は途絶えたが、Twitter<sup>3</sup> は、被災地、被災地外問わず、アクセスが可能であった。パケット通信方式が、有効に稼動したからであるといえよう。そこで、地域コミュニティが主体となって情報収集するツールとして、SNS<sup>4</sup> を使うのである。しかし、その膨大な情報の中には嘘の情報、「デマ」も存在することを忘れてはならない。東日本大震災の事例では、Twitter の情報は、行動の指針となる情報か否かを見抜く方法がなかった。そこで、SNS ツールを利用し、気象情報会社の新サービスを参考にした地域災害情報共有コミュニティを提案する。ある気象会社では、日本中の多くの地域に居住する多数のボランティアを組織化し、現在地の天候情報、写真を携帯メールにて報告し、それらの情報と従来の天気図、レーダ情報を統合し、分析、ゲリラ豪雨などの予測を配信している。この仕組みを模倣し、地域で事前に募集した災害報告ボランティアを組織化し、SNS ツールを使い報告してもらおう。例えば、Twitter であれば、アカウント名や発言ルールを策定し、発信者が特定できれば、一次情報として利用できる可能性は高い。この仕組みを地域の自治体で取りまとめれば、地域全体に役立てることができる。地域の中小企業が連携して、情報交換をすれば、前述の4つの視点の情報を入手することができる。しかも、投資は最小であり、中小企業でも十分に対応できるはずである。

### 3.4 マルチで考える

多くの中小企業の情報システムは、単一の通信回線契約、データの単一保管という

---

<sup>3</sup> Twitter ツイッター 個々のユーザーが「ツイート」(tweet) と称される短文を投稿し、閲覧できるコミュニケーション・サービス

<sup>4</sup> SNS Social Networking Service、ソーシャルネットワーキングサービス

環境下で、現実のビジネスが行われている。しかし、それは、情報システムの可用性、完全性に大きな脆弱性を生んでいる。そこで、以下の方針で対策すべきである。データをマルチに保管すること、できれば、データは定期的かつ自動的に、暗号化され、クラウドに保管する。そのデータへのアクセスには、識別(identification)、認証(authentication)、認可(authorization)が、適切に課される仕組みでなければならない。この方法であれば、物理的損壊リスクから開放され、データバックアップの手間や媒体コストなどが不要になる。さらに、複数のクラウド事業者保管しておけば、クラウド特有の懸念(クラウド事業者の撤退、倒産、突発的な価格変更などのリスク)からも開放される。クラウド事業者の情報セキュリティが信頼できない場合は、信頼できるデータセンター事業者を保管場所に指定すればよい。

次に、インターネットへの接続方法を複数契約にすること、携帯網(3G、LTE 等)、光ファイバー網、CATV、WiMAX、Wi-Fi 網、IP-VPN 網などから複数の通信会社のデータサービスから選択し、多重化をしておく。同時に、多種類のデバイス(例えば、スマートフォン、タブレット PC など)からもアクセス可能にしておくべきである。クラウドにデータを保管するのであれば、インターネットに接続できるまでの経路を必要に応じて確保しておくことが重要になる。

#### 4 今後の展望

日本の産業を支える多くの中小企業は、大企業と比較すれば、十分な情報セキュリティ投資は難しい。ゆえに、ひとたび災害が発生すれば、情報の可用性、完全性、機密性は侵害され、事業継続に多大な影響を及ぼしてきた。

災害に強い企業、強い情報システムへ、これからのキーワードは、地域コミュニティとクラウドコンピューティングである。中小企業単独で情報セキュリティ対策を検討すれば、一般的に多額の投資と経験豊富な人材リソースが必要であり、現実的には難しい。ゆえに、実現できていないケースが散見されている。それを、地域の中小企業、自治体、住民等が協力し、それらの対策を実装すれば、共有化効果が生まれる。前例の無い小水力発電であっても地域が協力すれば実現できている。東日本大震災の被災地である三陸地方には、「おちゃっこのみ」という地域住民の茶飲みの習慣があり、人々はリアルに繋がっていた。しかし、被災後は、デジタルデバイドが情報入手の力量格差を生み出してしまった。ゆえに、つながりさえすれば、災害に関する情報の収集と分析が可能になり、クラウドコンピューティングに預けたデータをフェールバックし、情報システムを復旧させる工程、業務の再開スケジュールなどが見えてくる。

## 5 おわりに

東日本大震災は、日本経済の空洞化懸念を加速させてしまった。アジアを始めとする新興国需要の高まり、円高、コスト高に加え、震災リスク、電力不足とコスト高懸念は、中小企業の海外流出を促す。特に、過疎化、高齢化、地域経済の衰退傾向が強い地方産業の海外流出は、日本経済を確実に衰退の道に導いてしまう。今こそ、情報セキュリティをトリガーとし、クラウドコンピューティングを道具として有効に活用し、地域コミュニティを活性化させ、災害対策の共有化、地域情報共有を行うべきである。

もはや、中小企業単独で危機管理を行う時代ではない。地域全体で、人と人が手を繋ぎ、情報セキュリティを進めていく時代にしていくべきである。

### 参考文献

1. 小川 雄二郎. “総論:情報管理における危機管理のあり方”. 情報管理. Vol. 48, No. 6, (2005), 311-319
2. 災害時における避難所の情報収集プロセスについての考察 加藤健
3. 安全とリスクをおはなし 安全の理念と技術の流れ 日本規格協会 中島洋介
4. 名古屋地域における企業防災の実態調査 平成18年6月 名古屋商工会議所
5. 地域の発展と産業 放送大学大学院教材 河合明宣
6. 中小企業白書「2011年版」 中小企業庁  
[http://www.chusho.meti.go.jp/pamflet/hakusyo/h23/h23\\_1/h23\\_pdf\\_mokuji.html](http://www.chusho.meti.go.jp/pamflet/hakusyo/h23/h23_1/h23_pdf_mokuji.html)

佳作（情報セキュリティ啓発賞）

Stuxnet の脅威と今後のサイバー戦の様相

陸上自衛隊通信団システム防護隊技術隊  
分析設計専門官  
猪股 晃 匡



## 第1章 Stuxnet とは

### 1.1 Stuxnet の登場

2010年7月、イラン南部に位置する建設中のブシェール原子力発電所及び同年11月、同国中部に位置するナタンツのウラン濃縮施設が、これまで確認された中でも極めて高度な技術を使ったサイバー攻撃によって被害を受けていたことがわかった。この攻撃に使用された武器が、Stuxnet（スタックスネット）と名付けられたマルウェア（コンピュータウイルス及びワームなどの悪意のあるプログラムの総称）である。

Stuxnet は、イラン国内の工場などで使用される Windows パソコンの約3万台を感染させた。そして外部のネットワークから切り離され、セキュリティのレベルが相当高いであろう原子力施設等のコンピュータシステムに侵入し、両施設において相当のトラブルが発生したとの報道がなされた。

そしてこのマルウェアの解析をセキュリティ企業が進めるに従い、単なる情報搾取または詐欺目的で作られたものではなく、工場や発電所などで使用される制御系システムに感染し、その制御を誤作動させてしまう機能を備えている事が判明してきた。

つまり、今回 Stuxnet の登場によって、工場プラントの制御システムを誤作動させることや都市インフラで使用される制御システムを乗取り、甚大な被害を与えるといった大規模サイバー攻撃は、もはやフィクションの世界だけではないということを現実の世界に証明して見せたのである。また、これは軍事組織においても同様であり、我の指揮統制システムの無力化やその制御の奪取の可能性を示唆し、人命に係わるようなサイバー戦の姿が想像できる衝撃的な事案であったことは言うに及ばない。

### 1.2 狙われたシステム SCADA (Supervisory Control And Data Acquisition)

図1に SCADA 使用の一例を示す。

SCADA は、遠隔監視制御・情報取得のための制御システムの一つであり、工場プラントや電気、ガス及び水道などのインフラで幅広く使用される。従来、専用の遠隔制御・監視装置を使用していたが、情報通信技術が進み、コンピュータ上で集約したシステムの制御・監視が可能となった。それまで独自の技術、

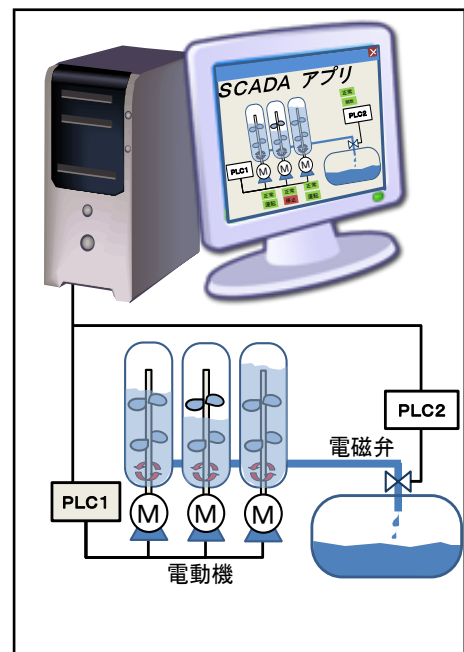


図1 SCADA の使用例

プロトコルなどで構成され、完全に独立したシステムであったものがコスト削減や効率性の観点から、共通規格化されたシステムへシフトしつつある。

欧米では比較的早い段階で汎用技術を使用しているのに対して、日本では欧米ほど採用はされていない現状にあるが、今後いっそう汎用技術の導入が進むと思われる。

SCADA は、イーサネット<sup>\*1</sup>等の回線を通じて PLC (programmable logic controller) にプログラムをアップロードし、送られたプログラムに従って PLC が被制御装置を制御・監視するものである。例えば図 1 に示すような、電磁弁の開閉や電動機の稼働を制御・監視でき、その情報を SCADA アプリケーションで視覚的に表示させることなどができる。

### 1.3 Stuxnet の特徴

Stuxnet は様々な特徴を持っているが、今回は 3 つ重要な特徴に注目する。

まず 1 つ目は、多様な感染手段と通信機能を持ち、そのほとんどが未知の脆弱性を悪用していることである。Stuxnet の感染活動と挙動について図 2 に示す。感染活動については、ネットワーク感染と USB による感染に分かれる。ネットワーク感染は、Server サービスの脆弱性 (MS08-067) <sup>\*2</sup>、印刷スプーラーサービスの脆弱性 (MS10-061) 及びパスワード未設定等のファイル共有を悪用している。次に USB による感染は Windows シェルの脆弱性 (MS10-046) を悪用している。また感染後に自身の実効権限を高めるため、Windows カーネルモードドライバの脆弱性 (MS10-073) 及びタスクスケジューラの脆弱性 (MS10-092) も悪用されていた。これらのほとんどは発生当初において未知の脆弱性であり、これほど多くの弱点を突くマルウェアの発生は極めて稀である。また外部の C&C サーバ<sup>\*3</sup>と通信することや、P2P<sup>\*4</sup>ネットワークを介して自身をアップデートする機能を持ち、適応能力が非常に高いといえる。

2 つ目の特徴は、限定したシステムを対象を絞った標的型攻撃ということである。Windows OS の脆弱性を悪用してマルウェアを実行した後、独 Siemens 社製 SCADA ソフトウェア SIMATIC WinCC/PCS7 に感染する。

次に PLC への不正な活動としては、まず PC 内で正常な DLL ファイル<sup>\*5</sup>をコピーし、新たに作った DLL ファイルに独自のプログラムを注入する。

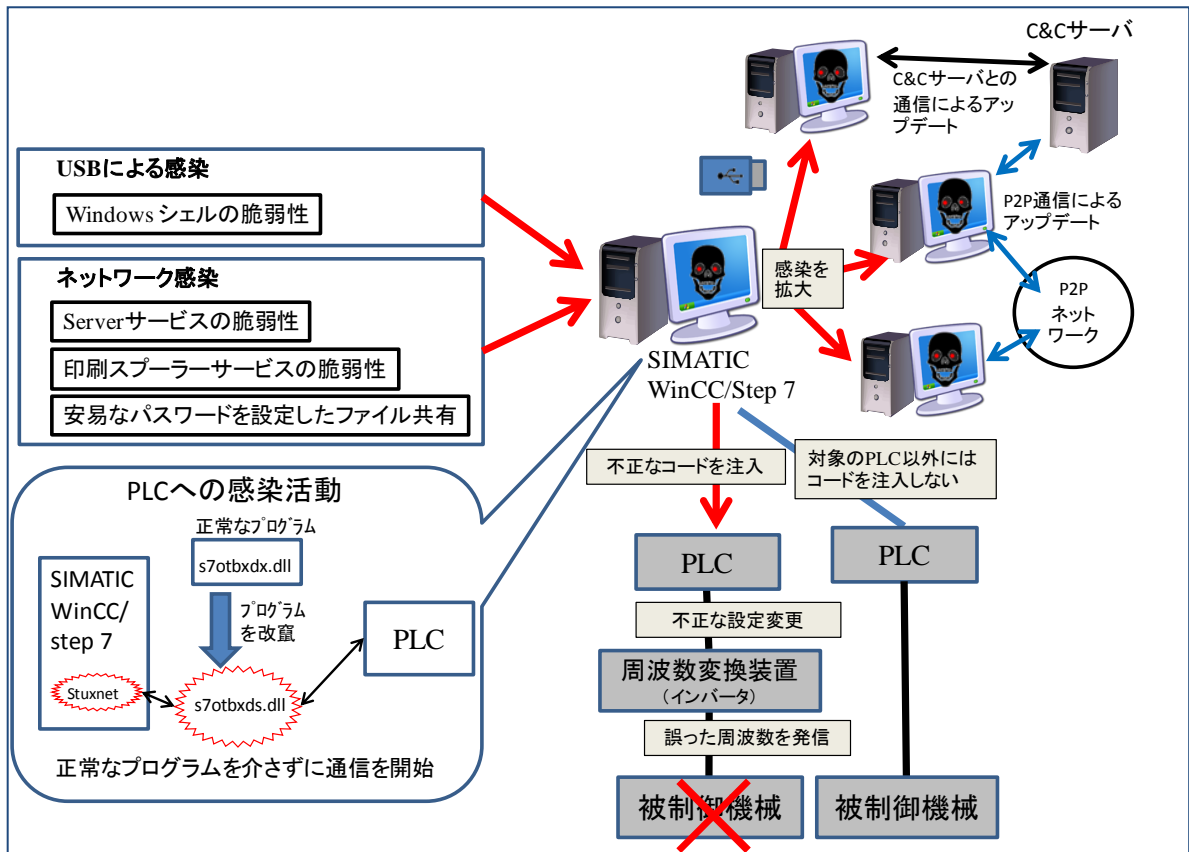


図2 Stuxnetの感染活動と挙動

これにより、Stuxnetは正常なDLLファイルを経由せずにPLCにアクセスできる環境を作り、コードを書き換え誤作動させて機能不全を起こさせる。また特定のPLCに搭載する通信プロセッサのみに活動を行うロジックが含まれている。現在判明している機能不全の方法は、電動機の回転数制御に必要なインバータ（可変周波数装置）をターゲットに、電動機に与える周波数を変更して回転数を不正に操作することがわかっている。

3つ目の特徴は、自身がマルウェアであることを秘匿するために、台湾にある2つの企業のデジタル署名を使用していたことである。デジタル署名は電磁的記録に付与する電子的な署名情報であり他人になりすましてデジタル署名をするには本人しかわからない秘密鍵で元データのハッシュ値<sup>※6</sup>を暗号化する必要がある。しかしそれを偽造することは非常に困難であるため、おそらく何らかの手段で不正に手に入れたものと推測される。

これらの挙動と状況証拠から攻撃者は、WindowsOS及びSIMATIC WinCC/PCS7のロジックを詳細に把握し、さらに電動機制御の知識までもが必要であるという非常に幅広く高度な技術を有していることがわかる。一般的なマルウェア開発に必要な知識は、ネットワーク技術やWindowsプログラミング技術などであ

るが、Stuxnet には、それらと大きく違う分野である電気制御技術や Siemens 製 PLC に特化したプログラミング技術までもが必要であり、おそらく関連技術者が開発に加わっているものと思われる。また、特定の PLC にのみに不正なコードを埋め込むロジックが入っていることから、何らかの明確な目的によって、攻撃対象をピンポイントに絞っていることがわかる。さらに台湾の企業のデジタル署名を盗用するなど偽装手段も非常に巧妙である。

Stuxnet の全容解明はまだ行われてはいないが、これらをまとめると開発する技術力の高さとは他分野技術との融合を実現させ、標的を確実に仕留めるような開発をしている、さらに巧みな偽装をしていることから、確実にターゲットを感染させ破壊しようとする強い意志と組織性を感じ取ることができる。

## 第2章 サイバー空間における脅威の変遷

コンピュータウイルスは、パーソナルコンピュータ及びインターネットの発達とともに増え、その目的や使用される技術も時間とともに変化してきた。世界初のウイルスは、1981年に発見された Elk Cloner と言われており、Macintosh マイコンに感染し意図せず画面に文字を表示するものであり、技術を誇示する目的で作られたものと思われる。1986年には IBM PC に感染する (c)Brain が登場した。フロッピーディスクから IBM PC に感染、メモリに常駐しメッセージを表示するというものである。これはパキスタンのソフト会社のプログラマーが、自分達が作ったソフトウェアが不正にコピーされていることを憂慮し作成したものといわれている。自己複製技術を応用し、不正コピーを警告する為に作成したプログラムであったが、アメリカで10万枚のフロッピーディスクが感染した。このようにコンピュータウイルスが初めて登場した当初は、主に人を驚かせたり、その作成技術を誇示するものや、警告するなどの目的で作成したものが多くあった。

1990年代に入るとインターネットの発達と共にメール添付型のものや、Microsoft office の VBA<sup>\*7</sup> で作られたマクロウイルスなどが増えた。1999年には Microsoft Word に感染、アドレス帳に記録されている大量の宛先に対し、ウイルス感染ファイルをメール送信するという Melissa がネットワークを介して爆発的に増え、各地のメールサーバをダウンさせるなどの大きな被害を引き起こした。作成目的は明らかでないが、その機能から推測すると愉快犯であり、自分の技術を誇示するなどの目的の可能性が高いと思われる。

2000年代に入るとトロイの木馬型<sup>\*8</sup>のウイルスやスパイウェア<sup>\*9</sup>が登場し、正常なプログラムであるかのように偽装してパソコンに入り込み WindowsOS の

制御を奪ったり情報を搾取する目的のものが登場した。ネットショップの運営者を狙って仕込んだマルウェアによって口座番号やパスワードが盗まれ、オンラインバンクから不正に預金が引き出されるなどの金銭的な被害が本格化してきた。このように個人情報（金銭関連）の搾取、営利犯罪目的のものなど主に詐欺的な商業活動を行うものが多く出現し、現在でもそれは主流であると言える。P2P ファイル共有ソフト「Winny（ウィニー）」を悪用する暴露ウイルス Antinny が登場したのも 2003 年～2006 年である。また多数のコンピュータに感染し、悪意を持った第三者がインターネットを通じて PC を外部から遠隔操作する Bot が増え始めたのも 2008 年頃であり現在でも感染に気付かずに潜伏しているものも多いといわれている。これは、特定の Web サイトなどに対する DDoS 攻撃、情報搾取及び新たな感染活動をするなど、インターネット上のサービスに深刻な被害をもたらすものである。

また金銭目的のサイバー犯罪の組織的活動も拡大しつつあり、一部の犯罪組織では、マネージャ、不正なハッカー、プログラマ及びデータ販売者が統括された組織によって運用され、目的のソフトウェアの脆弱性を発見して悪意のあるプログラムを蔓延させることも可能であるという。

このように、マルウェアは巧妙化かつ悪質化する傾向にあり、組織的なサイバー犯罪も台頭しつつある現状にある。

そしてその最たるものが Stuxnet である。開発の背後にはよりスケールの大きい組織性を感じさせ、設備や機械ひいては大規模な制御システムを破壊して、実際に人を傷つける恐れのある、物理的危険性を伴ったものである。まさに新しいタイプのマルウェアであり、これまでと違うかつてない脅威なのである。

### 第 3 章 Stuxnet の開発プロセス

#### 3.1 Stuxnet 開発プロセスの推測

Stuxnet の特徴から、非常に複雑なロジックで作られていることがわかる。そこで開発者（攻撃者）の視点で Stuxnet の開発プロセスを推測し、その開発にはどのような情報が必要なのか、またシステム全体の脆弱性がどこに存在し狙われたのかを侵入や偽装の方法などを具体的に検討し考察する。

##### 3.1.1 目的と目標

まず、開発プロセスを推測するにあたり、攻撃者が何のために何をターゲットにしようとしたのかを明らかにしておく必要がある。そこで今回被害を受けた施設の特性や現在報道されている施設の状況から想定するものとして、核技術開発を遅延させる事を目的とし、核関連施設の設備を誤作動させ機能を停止

することを目標として設定した。

### 3.1.2 方法

核関連施設の機能停止を実現するためには、白紙的に考えると航空機攻撃や砲撃等による直接的な攻撃あるいは、特殊部隊や作業員の侵入による破壊活動など様々な方法が考えられるが、今回は、費用対効果が高いと思われるマルウェアを使用したサイバー攻撃を選択した。

### 3.1.3 必要な情報

表 1 に Stuxnet を開発するために必要な情報を列挙する。

表 1 必要な情報

必要な情報	情報元
<ul style="list-style-type: none"><li>・ 制御システムの情報</li><li>・ 電動機制御の方法</li><li>・ PLC の種類</li><li>・ 監視用端末の情報</li><li>・ ネットワーク情報</li><li>・ 可搬記憶媒体の取扱状況</li></ul>	<ul style="list-style-type: none"><li>・ 原発施設の制御システムの開発企業</li><li>・ 出入りの業者</li><li>・ 対象施設の職員</li><li>・ 内部へ侵入し直接確認</li><li>・ 入札情報</li></ul>

まず攻撃対象のシステムがどの企業のものか、さらに誤作動させる対象の機械の構造などが分からなければならない。そのためには対象のシステムの設計や開発を行っている業者及び出入りしている関係者から情報を引き出す必要がある。また侵入経路や拡散方法の検討のためネットワーク情報、制御・監視用端末の情報、外部との接続及び可搬記憶媒体の取扱状況などが必要であり、これは対象施設の職員などからも情報を得ることができる。これらは内部関係者に対して個別に情報収集を行うことや、制御システム開発企業の関係者への働きかけ及び対象施設に対する直接的な侵入による方法で情報を取得することができる。また、過去の業者との契約に関する情報などがあれば参考にできるものと思われる。

### 3.1.4 収集した情報の集積

表 2 に実際に Stuxnet を作成するために収集したと思われる情報を列挙する。

表 2 収集したと思われる情報

項目	収集情報
制御システムのメーカー	独 Siemens 社
制御システムのソフトウ	独 Siemens SIMATIC WinCC/PCS7

エア	
制御用 PLC	独 Siemens SIMATIC PLC 6ES7-417 及び 6ES7315-2
制御・監視用端末の OS	WindowsXP SP3 であるが、セキュリティパッチを逐次適用しているかは不明
ネットワーク	部内ネットワークには TCP/IP (IPV4) を使用している事が濃厚であるが、インターネットとの接続は不明
制御機械の特性	制御する動力系の電動機にはインバータ制御の誘導電動機を使用し、インバータはフィンランド Vacon 社及びイラン Fararo Paya 社製を使用
可搬記憶媒体の取扱い状況	可搬記憶媒体の厳密な管理は行われていないと考えられる。

制御システムのメーカーは独 Siemens 社製であり Windows 用 SCADA ソフト SIMATIC WinCC/PCS7 を通して PLC を操作している。また制御・監視用端末の大部分は WindowsXP SP3 を使用している。ネットワークについては、制御用 PC の OS 等から TCP/IP (IPV4) によるごく普通の LAN で構成されているものと考えられるが、インターネットと接続しているかは不明である。制御機械の特性としては、インバータ制御の誘導電動機を動力系として使用し、PLC を通してフィンランド Vacon 社及びイラン Fararo Paya 社製インバータの周波数制御により誘導電動機の回転数を制御している。可搬記憶媒体の厳密な管理は行われていないと言われており、持ち込みなどは可能と考えられる。

### 3.1.5 情報の分析

制御・監視用に使用しているソフトウェアは独 Siemens 社 SIMATIC WinCC/PCS7 である。このソフト、PLC 及びインバータは米国などで一般に販売されているため取得は可能であるが輸出規制品目となっている。また PC の OS は WindowsXP を使用しているため現在出回っているマルウェアの機能の一部を転用できるが、セキュリティパッチを逐次適用しているかは不明であるため未知の脆弱性を発見する必要がある。外部ネットワークとの接続については、インターネットに接続しているかは不明であるため、確実に侵入させるには間接的に内部にマルウェアを持ち込ませる方法が必要である。施設内部で使用されている制御機械の特性としては、動力系に誘導電動機を使用し、インバータの周波数変換により回転数の制御をしていると思われる。このため独 Siemens 社 SIMATIC WinCC/PCS7 及び PLC へのプログラミング技術とインバータによる電動

機制御技術などの他分野の知識が必要であり、これらの技術者を含んだ開発チームの編成が必須である。

### 3.1.6 マルウェアの侵入方法の検討

外部ネットワークからの侵入は困難であるため、間接的にマルウェアを侵入させる方法を表3に示す。まずUSBによる方法としては、内部職員のミスを誘い、外部から感染したUSBメモリを持ち込ませる方法及び内通者や諜報員が施設へ直接侵入して感染させる方法がある。

次に外部からネットワーク経由で侵入させる方法としては、脆弱な暗号アルゴリズムを使用していたり、安易なパスワードを使用している無線LANがあればこれを利用することができる。

以上の方法を検討すると、マルウェア侵入の確実性を高めるには、内通者を利用することや、実際に人員を内部に侵入させることが最も効果的である反面、発見された場合の危険性は非常に高いため、この方法による場合は十分な訓練と経験を積んだ専門の要員が必要である。また内部職員のミスなどを利用する方法は、成功の可能性が不明であるが大量に行うことによって可能性が高まると思われる。その際心理的にミスを誘因させる方法を十分に検討しなければならない。脆弱な無線LANを利用する方法は、探索によって発見された場合は利用する価値は非常に高い。

表3 間接的にマルウェアを侵入させる方法

使用媒体	侵入方法	見積
USBメモリ等	インターネット上に内部職員に有用なツールを公開し、それにマルウェアを潜入	<ul style="list-style-type: none"> <li>・利点：安全性が高い</li> <li>・欠点：成功の確実性が不明</li> </ul>
	新品USBメモリにマルウェアを潜ませ、職員が外部で集まるような場所等で無料で大量に配布	<ul style="list-style-type: none"> <li>・利点：安全性が高い</li> <li>・欠点：成功の確実性が不明</li> </ul>
	内通者を利用して感染したUSBメモリを直接内部システムに接続	<ul style="list-style-type: none"> <li>・利点：成功の確実性が高い</li> <li>・欠点：内通者の養成に時間を要し、危険性が高い</li> </ul>
	人員を潜入させ感染したUSBメモリを直接内部システムに	<ul style="list-style-type: none"> <li>・利点：成功の確実性が高い</li> </ul>

	接続	・欠点：専門の要員の養成に時間を要し、危険性が高い
無線 LAN	脆弱な無線 LAN に接続	・利点：発見した場合は侵入しやすい ・欠点：施設まで近づく必要があり、危険性が高い

### 3.1.7 偽装方法

電子署名を利用し信頼性あるプログラムであるかのように偽装する。しかしこれに必要な秘密鍵の偽造は技術的に非常に困難であるため、盗用するなどの手段で入手する必要がある。

その方法としては、企業などが保有する秘密鍵のファイルを直接盗み取る方法とインターネット上にボットを拡散させて失効されていない秘密鍵ファイルを収集する方法、またはブラックマーケットなどで不正に入手する方法がある。

専門の要員を使って直接盗み取る方法は、確実性は高い反面、リスクが高く多くは収集できない。また盗まれた疑いが発見された場合にはすぐに失効手続きが行われる可能性がある。

ボットを使用する方法は、相手が気付きにくく、より多くの秘密鍵を収集できるため効果的であると思われる。

ブラックマーケットでの取引で入手する方法は、対象の電子署名の秘密鍵がない場合や費用の面で考慮する必要がある。

今回は、SIMATIC WinCC/PCS7 と PLC との親和性を考慮し、ワークステーションコンソール PC に搭載している通信モジュールを製造している台湾企業 Realtec Semiconductor Corp の秘密鍵を取得することを主眼とし、同社がある工業地区全体にボットを拡散させて取得するものとする。

また検討した他の方法も並行的に行うことによってより確実性が増すと思われる。

### 3.1.8 マルウェアの開発方針

WindowsXP の未知の脆弱性を発見し、可搬記憶媒体による感染とネットワーク感染の両方の感染活動を行う。またシステムの制御ソフトウェアである Siemens 社 SIMATIC WinCC/PCS7 の脆弱性を発見して PLC へコードを注入し Vacon 社及び Fararo Paya 社製インバータの設定を変更する。そしてインバータから発振される周波数を極端な値に変更し、誘導電動機の回転数を操作して破壊する。また対象のインバータに接続された PLC に対してのみ感染し挙動を開始す

る。作成したマルウェアには台湾企業から盗用した秘密鍵で電子署名をして信頼性あるプログラムを装う。

### 3.2 Stuxnet の開発プロセスの考察

前項のマルウェアの開発プロセスを見ると、単なる思いつきや、クラッカーの趣味で作られたマルウェアでないことが強く推察される。

それは単に技術的に優れているという理由だけでなく、広い分野の技術が必要であることや攻撃対象システムの情報収集を綿密に行うこと、外国企業の電子署名の秘密鍵を盗用するなどの幅広い諜報活動があつてこそ成し得るものだからである。そしてこれらのプロセスを統括する計画力・組織力がなければ開発は難しいからである。

そして、この開発プロセスを推測する中で2つの重要なポイントがある。まず1つ目はどのような情報が狙われ、マルウェアが開発されたかということである。使用している端末のOS、ソフトなど内部職員であれば誰もが知っているような、秘密情報ではない内部情報であっても、それは攻撃者にとって攻撃の焦点を絞り易く、マルウェアの開発時間を減らすことができるなど効率的・効果的な開発ができる重要な情報となり得るということである。もしこれらの情報の一つが抜けていた場合、複数の攻撃ロジックが必要であり開発には多くの時間と労力を要すると思われる。またこれらの情報の収集には内部の職員または納入業者等、施設に関連している者からの情報が不可欠である。おそらく人的つながりや諜報等によって情報を得たものと推測される。

次に重要なポイントは、今回狙われた核施設のような閉ざされたネットワークの中の独自のシステムに脆弱性が存在しサイバー攻撃に利用されたという点である。今回狙われた SCADA は、使用されるパスワードがハードコーディングされているなど不安全な設計をしていたことがわかっている。これまで独自の専用システムとして使用される場合が多く、一般で使われるインターネットに接続された PC のようなサイバー攻撃の脅威にさらされていなかった。このため悪意を持った第3者から攻撃を受けることを全く想定していない設計であった事がうかがえる。またこのマルウェアが侵入する段階においては、おそらく 3.1.6 表 3 に示すような方法がとられていることが推測される。セキュリティ意識の欠落などの人的な脆弱性も悪用している可能性は十分にあると言える。システムの性質上利用者が少ないこと、外部から隔離されているなどの理由から攻撃を受ける可能性が低いという今までの常識は通用しないということである。

## 第4章 Stuxnet の出現から予想される今後の様相

### 4.1 サイバー戦

米国防総省は2011年7月に発表した「サイバー戦略」の中でサイバー空間を陸、海、空、宇宙に次ぐ第5の新たな戦場と宣言している。そして、具体的な手段として今後のサイバー戦においては Stuxnet のようなマルウェアが使用されるであろう。

攻撃者は平時の段階においてどんなサイバー攻撃が可能か戦略的・戦術的な計画の立案及び情報収集をして適時適確に使用できるよう様々なタイプのマルウェアを整備していくと思われる。そしてその攻撃には、携帯電話、インフラ、工場プラント、自動車、航空機、人工衛星及び自衛隊が保有するシステムなど、隔離されたシステムや専用システム及び組み込み型のシステムなど、今まで攻撃を受けないと思われてきたものに対するサイバー攻撃の範囲が大きく広がる。そして計画的で組織的な開発によって生み出されたマルウェアの威力は大きく、経済への損害、社会の混乱及び科学技術の遅延など、その効果は大でありながら安全で安価に開発することができることが攻撃者側にとっての大きなメリットであると考えられる。

このように現在出回っている金銭をだまし取るような詐欺的なマルウェアなどとは全く違い、社会基盤を破壊できるようなサイバー兵器の開発が今水面下で行われうる状況にあり、もしそれが使用された場合の被害は甚大であるといえる。

これはサイバー空間における戦い方の変化であり、軍事組織においてもこれまでのような一般社会で出回っているマルウェアに対する対策のみでは新しいサイバー攻撃の変化に対応できない。

たとえば、指揮統制を行うシステム、射撃統制システム、無人機及び戦闘車両等へのマルウェア感染等によって、誤った目標に対する射撃が行われたりシステムそのものが暴走する等、直接戦闘に影響するような状況も生起する可能性がある。これからは、クローズ系の独自システムに対する標的型サイバー攻撃への蓋然性に着目した対策を強化する必要があると思慮されるため、その実施への一案を次に示す。

### 4.2 システムを防護するための一案

洗練された標的型のサイバー攻撃からは、パターンマッチング手法のウイルス対策ソフトはあまり有効ではなく、挙動を監視するジェネリック手法やヒューリスティック手法を使用した対策も必要となる。今後のさらなる発展が強く望まれる技術である。

ではこのような攻撃に対して今現在の有効な対策は、Stuxnet 開発プロセスの考察から2点挙げることができる。

まず1つ目は、攻撃者が正確で効果的な攻撃をするには、まず草の根を分けるほどの情報収集を行う点である。このため、どんなに小さな内部情報であってもその情報の流出がどのような脅威に繋がるか具体的に調査・研究をしておく必要がある。たとえばユーザが使用している端末のOSやソフトの種類、システムを開発した企業など、その情報だけではとてもサイバー攻撃につながらないような一般的な内部情報であっても重大な脆弱性を発見される一端となりえるのである。システムの管理者はもちろん、ユーザが知っているような情報であっても、守るべき情報の範囲を広げて具体的にその情報が漏れた場合の影響を考察する必要がある。今後は諜報活動と一体となったサイバー攻撃が活発になると思われるため、こういった情報の保全に対しても十分に考慮する必要がある。またユーザなどがこういった情報を知りえないような仕組みなど、システム情報を閲覧させない等の処置が必要である。

2つ目は、攻撃者がマルウェアを開発するにあたって、小さな「スキ」を大きな組織力と計画力をもって狙ってくるという点である。

その「スキ」を自らが探すには攻撃者と同じ立場に立った視点が必要であり、事前に脆弱性を発見しておくペネトレーション（侵入）テストが特に重要である。それは専門知識を有する組織によって十分に行われ、対象のシステムのみ限定しない、それを運用する組織と一体となった包括的な診断テストが必要である。ペネトレーションテストは一般的にも行われてはいるが、専門で行う組織は少ない。このため開発者自らがテストを行ったり、攻撃手法に関するセキュリティの着意が低い者が行うこととなり、備えるべき真の攻撃よりも弱いものになってしまう可能性が高いからである。そして発見された弱さを強化すべく運用上の改善や、システムの改善へフィードバックし、より強固なシステムにしてゆくことが必要である。

## 第5章 結論

Stuxnet の開発プロセスを推測することにより、攻撃者のバックグラウンドを想像することができた。今後のサイバー戦は諜報活動、綿密な計画及び組織力をもって行われ、サイバー兵器と言うべき破壊力のある、恐るべきマルウェアが秘密裏に開発されるであろう。もしそれが使用された場合、その影響力は攻撃を受けた一組織のみならず国民生活にも非常に大きな衝撃を与える。

さらに、これからのサイバー攻撃は、独自システムであることや、外部から

隔離されているなどの理由から、攻撃を受ける可能性が低いという今までの常識は通用しないのである。

これからのサイバー攻撃に対処するためには、あらゆる攻撃の可能性を研究して攻撃者の視点で対策を立てることのできる高い能力が求められるのである。

## 参考文献

- (1) Symantec Security Response W32.Stuxnet Dossier Version1.3(November 2010)
- (2) IPA 上水道分野用の SCADA セキュリティグッド・プラクティス
- (3) IPA 脆弱性を狙った脅威の分析と対策について Vol.5
- (4) IPA テクニカルウォッチ「新しいタイプの攻撃」に関するレポート (Stuxnet 等の新しいサイバー攻撃手法の出現)
- (5) JPCERT/CC Stuxnet 制御システムを狙った初のマルウェア
- (6) SIMATIC PCS7 Process Control System catalog ST PCS7・February2010
- (7) McAfee サイバー犯罪の 10 年間 (McAfee が振り返るサイバー犯罪の 10 年)
- (8) Symantec Official Blog(Stuxnet の PLC 感染プロセスの調査)
- (9) エフセキュアブログ <http://blog.f-secure.jp/>
- (10) カスペルスキーノート  
[http://ja-jp.facebook.com/note.php?note\\_id=408647905997](http://ja-jp.facebook.com/note.php?note_id=408647905997)

## 用語

- ※1 イーサネット：コンピュータネットワーク規格の 1 つで、世界中で最もよく使われている。
- ※2 MS00-000：Microsoft が見つけた製品の脆弱性に付与する番号
- ※3 C&C サーバ：マルウェアに対して動作指令を出すためにインターネット上に攻撃者が設置するサーバ
- ※4 P2P：ネットワーク上の対等な関係にある端末間を相互に接続しデータを送受信する方式
- ※5 DLL ファイル：Windows の複数のアプリケーションが共通して使用するプログラム
- ※6 ハッシュ値：あるデータをハッシュ関数で計算した結果であり基データを一意に識別できる。

- ※7 V BA : Microsoft Office 製品を機能拡張するための言語
- ※8 トロイの木馬 : 正体を偽ってコンピュータに侵入し情報流出や破壊活動等を行うプログラム
- ※9 スパイウェア : パソコンに格納されている個人情報などの情報を第三者へ送信するスパイ活動を行うプログラム

佳作（情報システム復旧対策賞）

東日本大震災を踏まえた災害時情報システムの  
復旧手順のありかたについて

情報セキュリティ大学院大学 博士前期課程

岩崎 正治



## 1. はじめに

2011年3月11日に発生した東日本大震災は、東日本を中心に深い爪痕を残した。情報システムもその例外ではなく、様々な事態に直面し、様々な課題が顕在化されることとなった。情報システムが事業を支える重要な役割を担うようになった今日、情報システムにおける災害対策は非常に重要なものとなっている。本論文では、東日本大震災を機に顕在化した情報システムにおける災害対策の課題について確認したうえで、今後の情報システムの災害対策のあり方について考察し、その中で、今まであまり重視されてこなかった復旧手順の在り方について述べる。

## 2. 情報システムにおける災害対策について

### 2-1. 顕在化した災害対策の課題について

情報システムに限らず災害時の対策としては、事業継続計画（BCP）[1]が一般的である。まず、東日本大震災によって顕在化したBCPの問題点について確認を行う。

東日本大震災におけるBCPの問題点について新聞記事やヒアリングの結果[2]を、以下の表1に整理している。今まで想定して来なかった問題が顕在化したことが見てとれ、中でもITが大きな問題となっていることがわかる。

表1：東日本大震災におけるBCPの問題点

No	問題点	No	問題点
1	BCPの発動	8	要員の問題
2	BCPの不備	9	計画停電の影響
3	DRP（復旧計画）の問題	10	外部電源
4	インフラの問題	11	個人情報の取扱い
5	通信インフラの問題	12	情報漏えい
6	サプライチェーンの問題	13	バックアップ
7	自社のセキュリティ環境の問題		

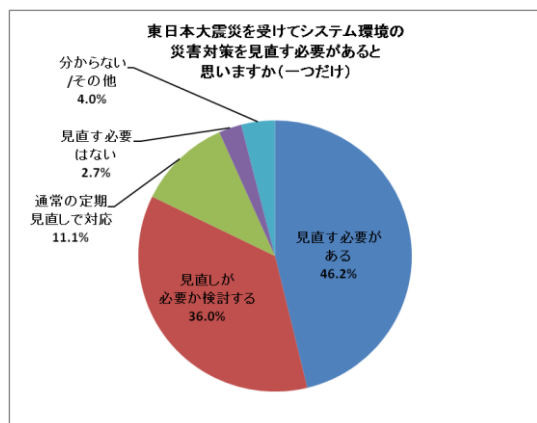
出典：情報セキュリティ大学院大学 原田研究室、

「東日本大震災におけるBCPの問題点について」、2011年5月[2]

## 2-2. 災害対策において見直したい点

それでは、企業はどのような点を災害対策の課題として考えているのでしょうか。

図1：システム環境の見直しの必要性



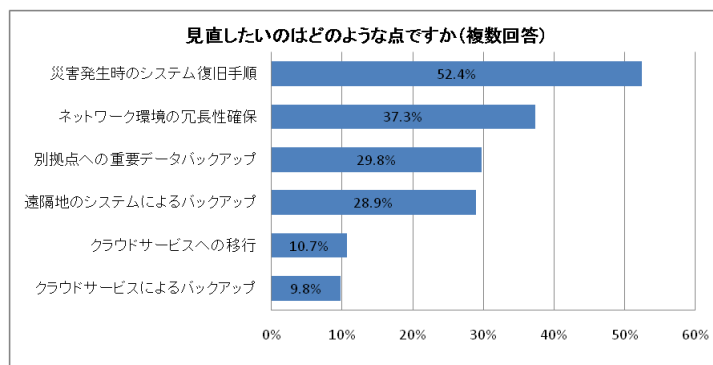
出典：日経BPマーケティング、「ITで実現する震災・省電力BCP完全ガイド」、2011年7月 P.22.

東日本大震災を受けて、システム環境における災害対策の見直しの必要性を感じている企業は多い。震災後に行なわれた日経BPの調査[3]によれば、「見直す必要がある」と回答した企業が46.2%あり、「見直しが必要か検討する」と回答した企業と合わせると、8割程度の企業が災害対策の見直しの必要性を感じている(図1参照)。

一方、ガートナー・ジャパンの調査[4]では、東日本大震災後にIT投資について予算を削減した企業は8%未満と少ない。多くの企業はIT投資における優先順位を変更し、アプリケーションへの投資を減らして、BCP対応に振り向けると述べている。また、日本情報システム・ユーザー協会の調査[5]では、BCPの見直しとして「外部データセンターの活用」を「導入中・検討中」の企業が3/4に達している。これらの調査から、企業はBCPにおけるITの重要性を強く認識していることがわかる。

上記の状況を踏まえ注目したいのは、[3]の調査において、見直したい点について最も多かった回答が「災害発生時のシステム復旧手順」であり、52.4%と半数以上の企業が回答していることである(図2参照)。企業がITの重要性を強く認識する中で、システムの復旧手順を大きな課題として認識していることがわかる。

図2：システム環境の見直しの必要性



出典：日経BPマーケティング、「ITで実現する震災・省電力BCP完全ガイド」、2011年7月、P.22.

### 2-3. 事前対策と事後対策

情報システムの災害対策については、経済産業省の IT サービス継続ガイドライン[6]および ISO/IEC27031[7]では、大きく以下の2つに分類している。

- (1) 災害発生前の対策
- (2) 災害発生後の対策

さらに、[6]では(1)として、

- ・バックアップシステムの構築
- ・非常用電源の設置
- ・ネットワーク環境の冗長化
- ・サーバの倒壊防止
- ・バックアップデータの遠隔地保管

などを挙げており、情報システムの停止を防ぐためのハードウェア的な対策が中心となっている。

また、[6]では、(2)として、BCPに従った

- ・リストア作業
- ・バックアップシステムへの切り替え
- ・本番システムへの切り戻し

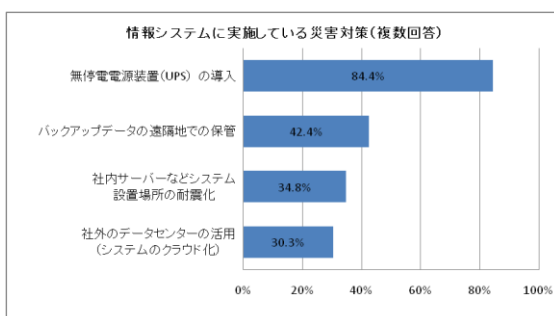
などを挙げており、情報システムの停止が発生した後の迅速なシステムの復旧を目的とした作業について述べている。

この分類を踏まえて、東日本大震災で起きた問題点[2]から、2-2を見返すと、災害発生前の対策よりも災害発生後の対策が十分でないこと、これらに対する見直しが課題と考えられる。

### 2-4. システム復旧手順の見直しの必要性

なぜ、事後対策であるシステム復旧手順の見直しが必要と考えられているのか。これについては、2つの理由が考えられる。

図3：情報システムに実施している災害対策



出典：日経新聞6月27日

第1に、災害発生前の対策が既にある程度普及していることが考えられる。日経新聞6月27日の記事[8]によると、情報システムに対して実施している災害対策として、無停電電源装置(UPS)の導入との回答が84.4%と最も多く、バックアップデ

一タの遠隔地での保管が 42.4%、社内のサーバなどシステム設置場所の耐震化 34.8%、社外のデータセンターの活用（クラウドサービスの利用を含む）が 30.3%と続いている（図 3 参照）。いずれも、災害発生前の対策に類するものであり、この点から災害発生前のハードウェア面での対策はある程度普及していると考えられる。しかし、ソフトウェアとしての手順については、[1]には、必要性は述べられているものの、組織ごとに異なることから、例示されていない。そのため、BCP のノウハウを持たない企業にとっては、ソフトウェアとしての手順の策定が、後まわしになっていたと考えられる。すなわち、多くの企業や組織において、BCP のハードウェア面の対策に比べ、未整備であったシステム復旧手順の必要性が認識されたためと考えられる。

第 2 の理由として考えられるのが、要員の問題である。東日本大震災の発生後数日は、スキルのある要員が地震や津波で失われただけでなく、交通網（道路、鉄道）の麻痺により、必要な箇所に要員を揃えることが困難な状況であった。さらに、多くの要員が他の重要業務の復旧の手伝いや長期間にわたった停電対策のために動員されたことより、情報システムの復旧やオペレーションに必要な要員を揃えることが困難な状況が続いた。このため、情報システムの復旧やオペレーションには、平常時の担当者以外による作業が要請される場面が多々発生した（[2]による）。しかし、事業継続計画における作業手順については、担当者以外の者が作業できるようなフレキシブルさについて、考慮されていないように見受けられる。例えば、事業継続計画策定ガイドライン[9]では、個別のシステム障害時の代替・復旧手順の確認は各箇所で行うものとされている。これは、平常時の担当者が復旧作業を行うことが前提となっている。すなわち、既存の手順は平常時の担当者（スキルや能力）を前提としているため、復旧手順を事前に策定していた企業でも、担当者不在のため復旧作業が円滑に進まない或いは作業が行えないという事態を招き、システム復旧手順の見直しが必要になったと考えられる。

### 3. 復旧手順について

#### 3-1. 必要な復旧手順について

復旧手順については、災害後の状況によって必要とされるものが異なる。[9]のフェーズに基づくと、以下のように整理できる。

①BCP 発動フェーズ：発生事象の確認手順

②業務再開フェーズ：バックアップシステムへの切り替え手順、バックアッ

プデータからのリストア手順、システム再構築手順、  
動作確認手順

③業務回復フェーズ：手作業などの代替作業手順、バックアップシステムの  
運用手順

④全面復旧フェーズ：本番システムへの切り戻し手順、代替作業により発生  
したデータの反映手順、動作確認手順

⑤復旧後フェーズ：システムの停止手順、システムの再開手順、動作確認手  
順

この中では、切り戻し手順と停電対策への考慮の必要性を強調したい。

### (1) 切り戻し手順

東日本大震災においては、切り替え手順が整備されていた企業においても、切り戻し手順については十分に整備されておらず、本番システムへの切り戻しに苦労した情報システムは多かった（[2]による）。バックアップシステムの場合には、本番のデータやシステムパラメータなどを運用していない情報システムに移すため、作業も容易である。また、万一ミスをしても、再度やり直すことができる。一方、バックアップシステムから本番システムに切り戻す場合には制約が多い。日本銀行の2010年の調査では、多くの金融機関の情報システムにおいて、切り戻し作業が未整備と述べている[10]。バックアップシステムで業務を再開しても、バックアップシステムは臨時のため、障害の発生の可能性も高く、停止すれば完全に業務が止まる。このため、早期に切り戻しが必要となるが、調査結果では、1～2週間で切り戻しが可能な金融機関が38%、1ヶ月以上必要な機関が17%となっている[10]。さらに、切り戻し作業が平日に実施できる金融機関は21%と少なく[10]、金融機関においても切り戻しは大きな課題とされている。一般の組織では、金融機関に比べて整備状況は進んでいないと想定される。以上から、復旧目標時間を想定する上では、切り戻しを考慮することが望まれる。

このことから、BCPでは、バックアップシステムへの切り替え手順に加えて、本番システムへの切り戻しも作業手順に加えた上で、切り戻しに必要な時間への考慮が必要である。

### (2) 停電に対する手順

東日本大震災では、電力会社による電源の安定供給という、システム稼動における従来の前提にない状況が発生した。更には、計画停電というITの被害想定にない事態も発生している。また、原子力発電所の安全対策の実施に伴い、

電力が逼迫し、突発的な停電のリスクが高まっている。UPS ではもちろん、停電に備えた臨時の発電機では、長期及び頻発する発電を前提としていない。また、これらの電源の供給には発電性能や燃料に配慮する必要がある。特に、データセンターなどでは、長時間の停電時における安定した電源供給は難しい（[2]による）。すなわち、短時間単発の停電しか想定していなかったことから、停電対応の手順を全面的に見なおさなければならない。

このことから、完全復旧フェーズ後においても、自組織や外部のデータセンターでの長期・短期の停電を想定して、システムをいつでも停止・再開するための手順が必要になる。

### 3-2. 復旧手順に求められる要素

2-4の内容を踏まえると、復旧手順の作成にあたり前提におかなければならない災害時の状況特性は、情報システムの日常運用を行い復旧に必要なスキルのある要員（以下、担当者という）が確保できないという問題を抱えるということである。このため、平常時の担当者以外でも作業を行うことを想定した手順が必要となる。この点を踏まえ、復旧手順に求められる要素は以下の4つとなる。

#### (1) 間違いがなく記載漏れのない手順

平常時の担当者であれば、手順に多少の記載漏れや間違いがあったとしても、臨機応変に対処することが可能である。しかし、担当者以外の者（以下、非担当者という）の場合、その場で担当者と同じ対応は期待できない。例えば、手順書の内容と実際の画面が少し異なったり、問題のない警告のポップアップメッセージが表示された場合において、非担当者では事象が重要な問題であるかという判断は難しい。都度、担当者への問い合わせや確認が発生することとなり、その間作業が滞ることとなる。手順書に文章表現の違いや誤字や脱字がある場合も同様である。起こりうる事象に対応できる作業手順の整備が必要となる。

#### (2) 分かりやすい手順

手順書は、平常時の担当者では予備知識や経験があるので問題なく使用できても、非担当者にとっては分かりにくい手順になっている場合がある。非担当者であっても、容易に使用できる手順である必要がある。また、災害時という逼迫している状況に加え、普段担当していないシステムの作業を行うということは、作業者に相当のストレスを与えることになる。一般に、高ストレス下で

の作業は作業ミスを生みやすいと言われており、ヒューマンエラー防止の観点からも、ミスを起こさせない分かりやすい手順であることが必要となる。例えば、手順書の手順は全て画面（イラスト）付きとし、チェックリスト兼用となっているとよい。文字だけの手順書（チェックリスト）や、作業手順書とチェックリストを別々にしてしまうと、作業が煩雑になりヒューマンエラーを招きやすくなる。なお、忘れがちであるが、復旧に必要な物（バックアップ媒体やインストール媒体）の一覧や保管場所についても、明記されている必要がある。

### （３）時間を意識した手順

復旧作業において、特に業務対応フェーズにおいては時間が大切であり、復旧目標時間内に目標復旧レベルを達成できるかが重要である。現在の作業の進捗具合を随時確認するため、作業項目ごとに目安時間が記載してあることが望ましい。

このことは、高ストレス下にある作業者の心理的負担を減らす効果もあり、結果ヒューマンエラーの防止の効果も期待できる。

### （４）作業ミスを想定した手順

復旧作業は、平常時と異なる状況下で行うことになり、作業者は担当者であれ、非担当者であれ、（２）で述べたように、ヒューマンエラーを引き起こす可能性は、平常時より高くなる。（３）でも述べているが、復旧作業において時間は重要な要素である。作業ミスがなく完全に遂行されることを前提にすることは、一度エラーが起きたとき、作業の遅延を招く上に、作業時間の遅れを取り戻そうとさらなるミスを引き起こし、その結果、重大なエラーにも繋がることもある。こうしたことから、作業ミスの発生をある程度想定した上で、前に戻ることができる作業手順、更にはそのリカバリ手順の記載が望まれる。一切のミスが許されないという緊張状況は、ミスを生みやすい上に、ミス発生時には作業者のパニックを引き起こし正常な判断ができなくなることがある。ミスを許容できる備えをしておくことは、担当者の心理的負担を下げ、結果的にミスを少なくし、円滑な作業に結びつく効果が期待できる。

## ３－３．復旧手順の作成で確認すべきこと

３－２で挙げたような要素を満たす手順を作成するためには、机上だけの作成では限界がある。このため、教育と併せて実際のシステムでのリハーサルを通して作成を進めていくことが必要となる。しかし、リハーサルは頻繁に行える作業ではないため、以下の３段階を考慮し、効率的なりハーサル計画を立

てる必要がある。

#### (1) 平常時の担当者による手順書の確認

第1段階として、手順の内容確認を、平常時の担当者が行う。手順の内容に不備はないか、机上検証時には想定されていなかったことが発生していないかの確認を行う。目的は手順の品質の向上である。

#### (2) 非担当者による手順書の確認

第2段階として、非担当者による手順の内容確認を行う。非担当者でも、問題なく使用できる手順となっているかの確認を行う。非担当者としては、まったくのシステム作業の素人であることが望ましいが、最低要件としては、対象システム以外の担当者とする。なお、可能であれば管理者による作業を追加することが望ましい。大抵の場合、管理者は非担当者である。また、管理者が非常時の実作業を把握しておくことは、作業管理の観点から有意義でもある。

#### (3) 非担当者による作業時間からの目標復旧時間の設定

第3段階として、非担当者が手順書に基づき作業を行った場合の、作業時間を計測する。目的は目標復旧時間までに作業が完了するかの確認である。なお、この検討においては、作業ミスがなく完了した場合の時間に加え、作業ミスによるリカバリも含めた時間も確認するべきである。このことにより、リカバリ時間も含めた作業時間の裏付けを取ることができ、復旧スケジュールの信頼性をあげる効果も期待できる。目標復旧時間を見積る場合、担当者による各作業での最短時間の合計を想定しがちであるが、これは前述の理由から問題がある。ミスや手戻りの発生を織り込んだ作業時間を見積もるべきである。

手順の作成の過程においては、問題点を炙り出すことを主眼とすべきである。特に、(1)と(2)でどれだけの問題点を炙り出せることができるかが、手順の最終的な品質に直結する。

もう一つ留意したいのは、(3)における時間の計測は必須であるということである。安易に他のシステムの容量から計算した値を用いることは行うべきではない。そもそも、ハードウェアの性能が異なれば当然処理時間は異なる。また、データ量のみならず、ファイル数やディレクトリ構造などに処理時間は依存する。また、今後、バックアップ対象に、圧縮データや監視画像などの動画データが多数含まれるようになると、同容量の非圧縮ファイルよりリストア時

間はかかることになる。以上のような要因から、バックアップやリストアにかかる時間は理論値を用いるのではなく、システムごとに実測値を測定して、バックアップやリストアの手順に追記する必要がある。

### 3-4. 復旧手順のメンテナンス

システムのソフトウェアやハードウェアに更新が発生した場合、作業手順も変更になる可能性があるため、都度のメンテナンスは必須である。その際も(1)、(2)、(3)の段階を踏むとよい。また、システムにおけるデータ量は常に変動する。パッチの適用やログの累積による恒常的な増加要因に加え、時季による変動(決算期と閑散期のデータ量の違い)が想定される。このことから、システムの更新がなくても定期的なリハーサルを行い、復旧時間の確認を行うべきである。

### 3-5. 今後復旧手順に求められるもの

今回の震災から、今まで想定されなかったさまざまな問題点も明らかとなった[2]。この中で特徴的な課題とその復旧手順への課題について述べる。

#### (1) 災害発生の時季への考慮の必要性

災害対策の手順自体については、今後は災害発生の時季を考慮した観点が必要となる。例えば、今回の震災は3月であったため、会計関連のシステムの復旧遅れが決算や業績発表の遅れに繋がり、さらに連結関係にある他社にも影響を与えた。今まで、BCPでは平常時を対象に作成しており、時季の特殊性を考慮していなかった。今後の手順には、決算期の場合は財務関係のシステムの回復を最優先するなど幾つかのパターンを想定しておく必要がある。

#### (2) 計画停電への対応

東日本大震災のあと、関東及び東北地域では、地域を分けて数時間停電するという計画停電が行われた。計画停電では、停電の対象地域・時間の場合、サーバなどの情報システムを事前にシャットダウンする必要があった。このため、情報システムの担当者は停電の事前準備や、電源回復後速やかに動作させる必要があり、通常の運用に加えて稼働が逼迫したなどの問題が報告されている([2]による)。

さらに、多くの組織には複数のオフィスがあり、ネットワークで接続されている。このような形態では、例えば、停電のない地域のサーバは稼働しているが、停電のあった地域のサーバは稼働していないことにより、システム内の

トランザクションがリアルタイムに実施できず、バッチで処理しなければならないなどのシステムの不均衡が起きた（[2]による）。今後の情報システムの運用では、計画停電を考慮した手順が必要となる。

#### 4. おわりに

今回の震災から言えることは、事故やミスを前提とした BCP の手順を考えることが必要ということである。本論文では、災害や事故が起きたときに、担当者でなくてもいつでもシステムを復旧できる BCP 手順の在り方を検討した。その結果、復旧手順には、記載漏れのないこと、分かりやすいこと、作業の時間を意識し、また、作業ミスをも前提とすることが必要であることを示した。さらに、実際にリハーサルの必要性、災害の時季や計画停電などの要素も手順に必要なことを示した。この研究が、今後、組織に必要な復旧手順の整備において、一助になれば幸いである。

最後に、この研究にあたっては、情報セキュリティ大学院大学の原田教授及び研究室仲間の温かい指導やコメントに感謝する。

#### (参考文献)

- [1] 内閣府 防災担当、「事業継続ガイドライン 第二版」、2009年11月
- [2] 情報セキュリティ大学院大学 原田研究室、「東日本大震災における BCP の問題点について」、2011年5月  
[http://lab.iisec.ac.jp/~harada\\_lab/BCP\\_20110518.pdf](http://lab.iisec.ac.jp/~harada_lab/BCP_20110518.pdf)
- [3] 日経 B P、「IT で実現する 震災・省電力 BCP 完全ガイド」、2011年7月、P. 22
- [4] ガートナー ジャパン、「東日本大震災後の国内 ICT 市場予測」、2011年7月11日  
<http://www.gartner.co.jp/press/html/pr20110711-01.html>
- [5] 日本情報システム・ユーザー協会、「「企業 IT 動向調査 2011」追加調査 結果のご報告」、2011年6月
- [6] 経済産業省、「IT サービス継続ガイドライン」、2008年9月
- [7] ISO、ISO/IEC27031 “Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity”、2011年3月
- [8] 日経新聞、「東日本大震災、事前対策は5割弱が機能」、2011年6月27

日、

<http://www.nikkei.com/tech/business/article/g=96958A9C938194>

99E0E6E2E2888DE0E6E2E4E0E2E3E3E2E2E2E2E2E2; p=9694E3EA

E3E0E0E2E2EBE0E4E2E2

[9] 経済産業省、「事業継続計画策定ガイドライン（企業における情報セキュリティガバナンスのあり方に関する研究会報告書・参考資料）」、2005年3月

[10] 日本銀行金融機構局、「業務継続体制の整備状況に関するアンケート調査結果」、2011年2月



# 平成23年度情報セキュリティに関する懸賞論文募集要項

## 1 目的

インターネットの普及は目覚ましく、様々なサービスにより国民生活や社会経済活動において本格的にインターネットを利用する時代になりました。

さらに、PCの機能を持つ携帯情報端末、例えばスマートフォンは人々のコミュニケーションの手段だけではなく、ビジネスでの活用も進められています。

そのような中、3月に発生した東日本大震災は情報インフラにも大きな被害を与え、インターネットや携帯情報端末の使用が制限されるとともに企業や自治体の事業継続にも大きな影響を与えています。

私ども財団法人防衛調達基盤整備協会としては、情報セキュリティ意識の向上に資するため、情報セキュリティに関する懸賞論文を募集するという事業を行っております。この事業は、多くの方から論文を応募していただき、情報保全意識を高め、優秀な作品を表彰し発表する事により、広く国民各層に情報セキュリティに対する知識と技術を広め、ひいては防衛基盤の強化に寄与することを目的として実施いたしております。

## 2 23年度懸賞論文のテーマ

23年度の懸賞論文のテーマは、四つの視点から選んでいただきます。

(1) 一つ目の視点は「災害時の情報システムのあるべき姿」です。

3月に発生した東日本大震災は情報インフラにも大きな被害・不安をもたらしました。インターネットや携帯情報端末装置が利用できなかつたり、データが損失したことによる企業・公共団体の事業継続への影響は甚大であります。さらに震災の被害や不安を悪用した偽情報を流すチェーンメールや募金活動を謳った偽サイトによるウィルス被害等も発生しています。

こうした状況から、今回は、情報セキュリティの3要素のうち、機密性だけではなく、完全性・可用性に焦点を当てた提言や意見を期待しています。

たとえば、「情報インフラを提供する事業者や自治体によるインフラシステム復旧に向けた取り組み」、「通信事業者に望まれる災害時の情報伝達手段を確保するための取り組みや対策」といったテーマに関する論文を期待

しています。

- (2) 二つ目の視点は、「PC機能を持った携帯情報端末、例えばスマートフォンによるソーシャルメディア時代の情報セキュリティのあり方について」であります。

スマートフォンやタブレットといった携帯情報端末は人々のコミュニケーションの一つの手段となっています。企業でも仕事の効率化のため、この携帯端末を実際のビジネスの中で活用していこうとしています。しかし、こうした携帯情報端末を標的にした不正ソフトはすでに国内外で確認されており、今後急激に感染範囲が拡大していくと懸念されています。しかしながら、こうした携帯情報端末においては、PC向けに採用されているような情報セキュリティ対策が十分に普及しているとは言い難い状況です。

携帯情報端末の利点やソーシャル・ネットワークの効果を活かしつつ、情報セキュリティを確保していくという課題に対する具体的な提言や意見を期待しています。

- (3) 三つ目の視点は、「サイバーテロ攻撃への対応」というテーマにしました。

2009年7月、韓国や米国の政府機関、金融機関等のWebサイトを標的に大規模なDDos（分散型サービス妨害）攻撃が行われました。グーグル社に代表される国際的企業に対する不正アクセスも目立ちます。

このように社会的インフラともいえるべき機関や企業に対する、コンピュータやネットワークを利用した組織的攻撃の脅威が高まっている状況を、どのように捉え、どのように対処していけばいいのか、具体的に取り上げて下さい。たとえば、「法人における組織的なサイバー攻撃に対する心構えと基本対策」、「一般市民がサイバーテロ攻撃から身を守るための基礎教育」、又は「政府が採るべきサイバー攻撃への対策」等といったテーマの提言や意見を期待しております。

- (4) 四つ目は、「自由課題」です。

上記のテーマの他に、「一般のユーザに対し、実効性のある情報セキュリティ対策を普及させるためにはどうあるべきか」や「コンピュータ社会と情報セキュリティ その問題点と対策」などがあります。増大し巧妙化する情報セキュリティの脅威に対し情報セキュリティ対策の重要性が増す一

方、この脅威に対して一般のユーザとしてどう対応すべきか。また、どのように考えていくべきなのか、ということであります。

情報セキュリティの意識向上について皆様が日ごろ重要だと考えておられる視点からの提言をお願いいたします。

なお、冒頭にも触れましたとおり、本啓発事業の目的は、広く国民各層に情報セキュリティに対する知識と技術を広めることにあります。読み手が、それぞれのテーマについての理解を深め意識を高められるよう、具体的かつわかりやすい内容の論文、提言を期待しております。

参考までに、過去3年間の受賞作品はBSKのホームページに掲載しておりますのでご参照下さい。

### 3 応募資格

情報セキュリティに関心のある方で、「情報セキュリティに関する懸賞論文募集要項」に同意した方。

### 4 応募規定

(1) 日本語の論文とし、6,000～8,000字以内。

(ただし、図表は含まない。)

(2) 表彰の対象は、募集要項により応募のあった懸賞論文。

ただし、国、地方公共団体その他これらに準ずる機関からの委託を受けたり、他に発表したものの転用は除く。

(3) 募集開始は4月28日(木)、締め切りは7月29日(金)到着分まで。

(4) 図表等を他の文献から転用した場合は、その出典元を明記してください。

(5) 応募作品の様式等

- ・ A4版 横書き 34行×36字を標準とし、文字は12ポイント。
- ・ PDF形式のものとし、
- ・ 論文の提出方法は、メールにてお願いします。なお、当選者には別途Microsoft Wordで提出をお願いします。

E-mail: [koueki@bsk-z.or.jp](mailto:koueki@bsk-z.or.jp)

- ・ 論文の提出にあたっては、応募原稿の表紙(字数制限に含まれません)

に、「ご自分の書かれた内容にふさわしい具体的なタイトル」を表示してください。なお、氏名、連絡先等を必ず記載してください。

#### 5 報奨の内容（贈賞・賞金）

報奨者（個人又はグループ）には、次の賞状等を贈呈。

- (1) 賞状
- (2) 賞金（最優秀賞1名に対し50万円、佳作は3名以内）

#### 6 選考等

「情報セキュリティ論文選考等委員会」において、公平、適正に審査し、結果の発表は、受賞者に対してのみ、平成23年11月中旬に通知します。

#### 7 作品の取り扱い

- (1) 応募された作品は返却いたしません。
- (2) 受賞作品の著作権は、当協会に帰属するものとし、当協会のホームページに掲載するとともに小冊子を作成、配布します。

本懸賞論文は、防衛調達研究センターの公益目的事業として行った、第4回目の成果を発表するものです。

また、本論文集は、当協会のホームページ(<http://www.bsk-z.or.jp>)でもご覧いただくことができます。このホームページには、皆様のお役に立つ情報を掲載しておりますので是非ご覧ください。

**平成23年度  
「情報セキュリティに関する懸賞論文」受賞作品**

平成23年12月 発行

非売品 禁無断転載・複製  
発行 : 財団法人防衛調達基盤整備協会  
編集 : 防衛調達研究センター論文選考等委員会

〒160-0003 東京都新宿区本塩町21番3-2

電話 : 03-3358-8754

FAX : 03-3358-8735

メール : [hozen@bsk-z.or.jp](mailto:hozen@bsk-z.or.jp)

H P : <http://www.bsk-z.or.jp>