サイバー保全のための情報管理
Managing Information for Cyber Space Security

溝口徹夫†
Tetsuo Mizoguchi

要旨
サイバー保全での二種類の脅威について、その事例を挙げ、その特性 を整理した後、脅威への対処方針を挙げ、情報管理という観点での対処方策を提案する。また、「インテリジェンス」型の脅威についての試行実験について触れ、今後の 残された課題について議論する。

1. はじめに

サイバー保全の議論が行われ、サイバー保全への方策が望まれる。しかし、サイバー保全の持つ特性の理解なしには、適切な方策が得られないであろう。本資料では、サイバー保全の持つ特性を整理し、サイバー保全への方策を考察する。

2. サイバー保全の概要

改めて言うまでもなく、世の中には多くの情報システムが存在する。その各々では内部に情報を保持し、また処理プロセスを実行している。これらの情報や処理プロセスは情報システムの外部からは一般にはアクセスはされないし、許可もしない。

外部者がこれらの情報や処理プロセスへ(不法に)アクセスすると、進入された側での(サイバー)保全性が失われる。従って、サイバー保全(保全性維持)はサイバー防御の一環であるといってよいであろう。また、サイバー保全活動の主体は防御側にあることになる。それは保持している情報や処理プロセスの内容を理解しているのは防御側だからである。この認識は、参考資料[1]に示されている内容が参考になる。とかく、サイバー攻撃(攻撃側の行動)に眼を奪われる傾向になるが、サイバー保全への出発点は防御側である必要がある。

本資料では、以上の認識から、第一段階として、防御側で保持している情報に焦点を当て、この情報の管理という視点で、サイバー保全を考察する。情報管理の視点を採用するのは、参考資料[2]に示されている論旨が妥当であろうということによる。

第二段階として、運用している処理プロセスを中心にサイバー保全を考察する。
Cyber-to-Physical Effectと称するものである。但し、本資料では第一段階に焦点を当てる。

2.1. サイバー保全損傷に至る脅威(threat)とその種類

サイバー保全は一般の保全性(security)とは次の 2 点で異なると言える。

- サイバー保全損傷が発生し得るきっかけは、攻撃者の意図的な行為(脅威)から始まることである。サイバー保全損傷は天災や人間の不注意によるものではない。
- 攻撃者の意図的な行為は情報システムの内部への進入によって内部から開始される。

情報システムにおいて、保全性が損傷(Breach)される、すなわち、保全損傷を生じる脅威とは、どのようなことであろうか。これまで多くの資料、例えば[3]、で報告されたものは次の二種類である。

① 金銭的利得を目的とした脅威(以下では Type I と呼ぶ)
② 上記の金銭的以外の利得を目的とした脅威(以下では Type II と呼ぶ)

上記の Type I の脅威は、目的がはっきりしており、その対処方法も具体化されやすいが、Type II の脅威は、金銭的以外の利得を目的として含む全てを指し、具体性に乏しい。更に、Subtype への区分が必要であるが、詳細については以後で触れる。

2.2. サイバー保全の課題

サイバー保全の課題は、脅威がいずれの目的であれ、保全損傷を防ぐことである。そのためには、保全損傷を生じる脅威の目的を理解し、有効な対処をせねばならない。脅威の目的、狙われる情報や処理プロセスの性質によって、対処の方法が異なるであろうことから、これらの理解を深める必要がある。以下では、まず、第 3 章で、保全損傷の事例を参照し、脅威の特性を整理す

る。第 4 章では、対処方針を、第 5 章では対処方法例を示す。

3. サイバー保全損傷の事例

3.1. 金銭的利得目的の脅威（Type Ⅰ）と保全損傷例

事例1: サイバー保全会社の報告[4(2014)]による、米国の小売業者へのサイバー攻撃の例がある。小売業のPOSシステム全店舗への進入がなされ、レジスタに記録されている顧客情報、特にクレジットカードデータが盗難にあった。クレジットカードデータはISO/IEC 7813 で規定された形式で、 ATMやクレジットカードで採用されている。そのTrack1データで、顧客氏名とカード番号が例示のように、表現されている(Wikipediaより)。6011898748579348^DOE/ JOHN

- AN: Primary Account Number, up to 19 digits
- FS: Separator "^"
- NM: Name, 2 to 26 characters

これは管理対象となる情報である顧客情報で、顧客名とカード番号の対応付けが、一目瞭然に示されている。本資料の生成者はこのような事例の存在を事前には知らなかったが、このような例の存在はごく自然であろうと思われる。

事例2:入手した顧客情報はどのような使い方がされるのであろうか。実情を示す例として公表されているものは少ないが、次の例が資料[4(2013)]に示されている。例では、二種類の攻撃がなされている。一つは顧客の口座情報の入手である。これは上記事例1にその例が示されている。この情報に基づいて、事例2では、カードの偽造が行われた。この情報だけでは有効ではない。なぜなら、一般に口座から現金を引き下ろすにはパスワードが必要である。第二の攻撃は、金融機関のパスワード管理担当者への攻撃で、担当者になりすまし、パスワードのリセットを行った。パスワードリセット後、短時間で複数口座から2MUS$(約2億円)が引き落とされた。

3.2. インテリジェンス(金銭的以外)取得目的の脅威(Type Ⅱ) と保全損傷例

電子メールアカウント情報流出

Type IIのサイバー攻撃の例として、Operation Auroraと称される事例[5]では、Googleの電子メールアカウント情報が流出した。Googleサーバーへの進入が行われ、特定個人の電子メール情報が流出した。Googleは知的所有権が侵害されたとして、サイバー攻撃があったことを公表した。資料[5]によれば、露見したのは電子メールのタイトルとアカウントの生成日付だけであったとされる。それが事実であれば、被害は少なかったと言ってよい。但し、以後、Googleは中国から撤退し、全体として、被害が少なかったとは言えない。この事例で、流出情報が限定されていることが事実であれば、Googleの電子メールアカウント情報は、情報流出防止の情報管理が行われていたとも受け取れる。アカウント番号からたどれるのは、アカウント生成日付とメールタイトルだけで、メール送信日付、メール宛先、メール本体、添付ファイル、は関連をつけることが出来なくなっているとみるべきであろう。もちろん、メール本体情報が流出する可能性もあるが、メール本体情報から誰がいつ送信したメールかが辿れないように仕組めば、被害は少なくできる。

別の事例で、話題となったWikileaksによるメールデータの流出のような場合では、このような仕組みが意図的に準備されたとすれば、メールデータが漏洩したとしても実質的な被害は少なくて済む。現在のメールソフトウェアでは、メール本体に差出人、宛先、メール内容、差出日付、等が自由形式で記載されているが、情報管理という観点から、メール情報を各要素に部品化して格納するような細工をする手もある。

金銭的利得目的の事例では、個別のデータを分析しなくても目的を達する(金銭を取得できる)のに対して、インテリジェンス取得目的の場合は、機械的な処理では、目的を達成できず、個々のデータを一つずつ人手で分析する必要がある。

3.3. 異なる型のサイバー保全損傷とその共通点と相違点

1) Type I 金銭的利得目的の脅威

この型の脅威の特徴は、主要な情報は、顧客氏名、口座番号、暗証番号等、構造化されており、値が与えられれば、金銭的利得目的を達成できる。脅威を与えるのは、「値」であって、メタデータは必ずしも要しない。脅威の実行は機械的な処理が可能で、短時間で多数の脅威が実行可能である。

2) Type II インテリジェンス(金銭的以外)取得目的の脅威

この型の脅威の特徴は、情報の内容は千差万別で、一概に特徴化は困難であるが、上記で示した電子メール情報を例として特徴を挙げてみる。電子メール情報は、送信者、受信者、メールタイトル、送信時刻、メール本体、添付資料などからなる。以上の情報単体だけでは、脅威を与えることは少ない。メール本体の内容が理解されることが脅威につながる。自然言語処理技術を駆使しても、脅威を与えるような理解は困難である。大量のメール文があっても、その内容は人が理解しなければならず、それも長期間にわたって、対象を追い続ける必要が出てくる。

3)Type I/II の共通点

① 上記 2 種類の、サイバー保全への脅威の第一の共通点は、進入の手法が同一であることである。

② 第二には、程度の差はあるが、少なくとも進入の初期において、誰が攻撃者か、何が目的か、どのような被害を蒙るかが判然としないことである。

以上の共通点から、目的が異なる Type I/II が判然と区別されずに議論されることがある。特に第一共通点から、攻撃の詳細に眼を奪われ、目的の区別がつかない。

4） Type I/II の相違点 Incident Reaction Team の必要性

Type II の特徴は、上記のように、人手による脅威の実行、損傷の防御が行われることである。資料[1] [6]に示されるように、Incident Response Team による適応型の防御の必要性がある。決まった手順での防御策は期待できない。

注　脅威に関する情報交換について

資料[6]のタイトルに、Intelligence という用語があるが、これは Threat Intelligence、つまり脅威の情報(インテリジェンス)のことで、脅威がどのようなものであったかを示すものである。脅威の情報は、広く関係者間で共有されることが望ましいとされるが、脅威を受けた個人や組織にとっては、脅威を受けたことが世間に広く知れ渡ることは、脅威からの直接の被害以上に避けたいことである。脅威情報の共有には、情報が有益であることと、個人や組織の特定がされない(匿名性)等のプライバシー上の問題を抱えており、容易ではない。日本政府が重要基盤事業者に、脅威を受けた場合の報告義務を課すことを計画しているとの一部マスコミの報道があったが、このような施策の実施は困難であろう。当面は、個人や組織での努力によるしかないが、本資料での最後にこの点について触れる。

4. サイバー保全の情報管理　対処方針

情報管理は、情報オブジェクトと処理プロセスが対象となるが、以下では、情報オブジェクトについての情報管理を主として考察する。

4.1. 情報オブジェクト情報管理の主要な方針

方針1: サイバー空間における保全運用上「重要な情報」は何かを明らかにしておかねばならない。この「重要な情報」を「管理対象オブジェクト」と以下で名付ける。

方針2: 管理対象オブジェクトは「容易に閲覧、複写できる形で記録されてはならない」。「容易に閲覧、複写できる形で記録しない方法」として、従来のデータベース技術でのサブスキーマ(:管理対象オブジェクトの一部:viewのみしか見えない)がある。管理対象オブジェクトは正規表現されたデータ部品からなる。管理対象オブジェクトはデータ部品の結合(join)による等の手法が存在する。ファイル形式でのデータ格納は危険である。

注　市販のソフトウェアパッケージをそのまま利用することは避けねばならない。また、方針2による管理対象オブジェクトの情報システム上での存在が方針1での保全運用上の危険がないことを確認することとする。

方針3: 管理対象オブジェクトはサイバー保全のためのみに情報管理を行うのではないので、日常業務と共用できなくてはならない。管理対象オブジェクトがサイバー保全以外の利活用との共

用を可能にするために、管理対象オブジェクトは利活用の必要がある度に生成(JIT: Just In Time生成)を行い、管理対象オブジェクト生成の痕跡を残さないこととする。生成から利活用までのリードタイムを短縮することで管理対象オブジェクトの露出・流出の可能性を減少する。

方針4: 管理対象オブジェクトを生成するのに、生成プロセスが利用するメタオブジェクトが必要であるが、メタオブジェクトは管理対象オブジェクトと隔離されて管理されることとする。いくつかの提案では、メタオブジェクトを管理対象オブジェクトに包含するというものがあるがサイバー保全上危険である。

5. サイバー保全の情報管理　対処方策例

5.1. 金銭的利得目的の脅威対処案:漏洩情報の組み合わせの可能性防止

以下では、上記の方針に基づいて、対処方策の例を示す。

図 1 の示すように、情報要素単体から管理対象を導出する経路を管理する。管理対象そのもの、および中間成果物(他の中間成果物相互の組み合わせの可能性あり)を記録することは避け、その経路も外部からは見やすいものであってはならない。

情報システムが成り立つには、情報要素単体(「値」)はシステムのどこかに記録されている。また、記録された情報は露見する可能性を零にはできない。ここでの主張は、記録された情報要素単体から管理対象情報が容易に導出できないことである。

また、ここで、注意すべきことは、顧客氏名/生年月日(中間成果物)が外部に流出しても、「管理対象への経路は露見することなく、被害はない」と断定することは出来ないことである。別途入手した情報と組み合わせれば、管理対象にたどり着く可能性がある。

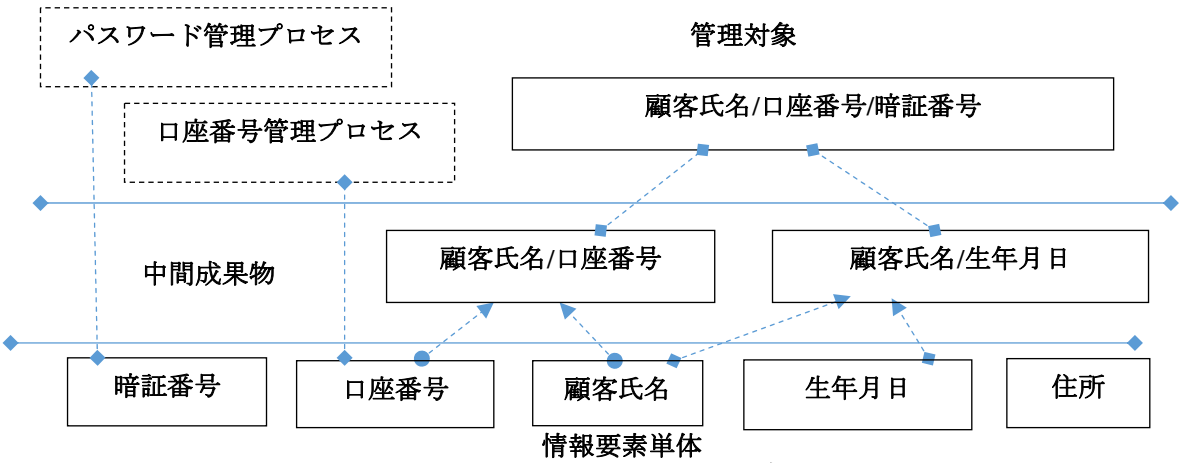

図 1　金銭的利得目的の脅威対処案

5.2. インテリジェンス取得目的の脅威対処案

インテリジェンス取得目的の脅威対処を画一的に提案できるわけではないが、電子メール文の例の場合では、上記顧客情報に類似して、メールタイトル、送信メールアドレス、送信者氏名、受信メールアドレス、受信者氏名、送信日時、メール本体、添付資料などの、情報要素単体から最終的な管理対象オブジェクトへの導出経路が容易になることを回避する。

6. 情報管理からインテリジェンス管理へ

上記の考察から、Type I の脅威は、直接的被害があり、対処が必要であるが、Type II の脅威は、特性も多様で、個別の対処が必要になると考えられる。そのような対処をインテリジェンス管理と呼び、仮想的な脅威や対処方策について考察してみたい。ここでいうインテリジェンスはビジネスインテリジェンスとでも呼ぶもので、上記での threat intelligence とは異なる。

6.1. 航空機システムへの仮想脅威

サイバー保全とは直接関係はないが、特殊な例として、参考資料[3]に次のような出来事が記載されている。(2015年)4月に、米国の航空会社パイロットがiPadで利用している「電子版カバン」シス

テム(パイロットが飛行前のチェックに使用するもので、13ポンドの紙のカバン資料の代替)がダウンし、関係する航空機の離陸が出来なくなった。また、同記事では、4月に、米国会計検査当局(Accountability Office)が「現代の航空機の接続性の良さは、不法な遠隔アクセスが航空機の電子システムに及ぶ可能性を持っている」とし、航空機でのWi-Fiアクセスはハッカーに狙われると報じている。航空機製造会社はすかさず「飛行計画はパイロットの確認なしには登録されない」という声明を出している。サイバー保全上、今すぐ情報管理を必要があるわけではないが、以上の記事と関連付けて、航空管制での仮想的に、データの値が時間と共に変動する場合での、サイバー保全に関する情報管理を検討してみる。

航空管制でのデータとしては、航空機の実飛行の位置と時間を示すデータが存在する。これらのデータは、航空機が衝突しないための航空管制に使用される。また、これらのデータは公開することで航空機の互いの位置を確認するために使用されることから、(自家用機も含まれる)民間航空では、これらのデータは機密保護を行わない。最近、米国で、走行中の自動車を乗っ取る実験を行い、乗っ取りが成功したことが報じられている。

航空管制のデータには他に異なる種類のものとして、飛行計画データがある。航空機の近い将来(2-3時間後など)の飛行軌跡予定を示す飛行計画データである。しかし、もしも、飛行計画が意図的に変更され、航空機同士が衝突するよう仕向けられたらどうであろうか。現実に発生し得る可能性があることが示されている。もっとも、最終的にはパイロットの判断による運航が行われ、危険回避が行われるので、被害はない。

6.2. 企業機密への脅威:電子メールに基づく企業インテリジェンス分析

Type II と上記で示した脅威は、多種多様な内容からなる。その中でも、最も数多く存在すると想定されるのが、企業機密への脅威である。この企業機密への脅威が足がかりとするものとして、企業内での電子メールを取り上げてみる。事実、電子メール文の漏洩による商談交渉条件の漏洩などの例が報告されている。企業内担当者が交換する電子メール文を外部者が入手、分析した場合、企業機密は浮き彫りになるであろうか、企業機密漏洩を防止するには何が必要であろうか、分析の必要がある。

結論として、以下のようにまとめられる。組織内で交換される電子メールの数は膨大であり、テーマを特定せず、何らかのンテリジェンスを得ようとしても、人間によるメール文の解釈をある程度の期間行うことが必要で、効率的でも効果的でもない。但し、メール文に対する短期間の解析であっても、誰がどのようなテーマを担当しているか、組織内で情報がどのように流れているか(各担当者の役割分担等)を理解することはできる。個々のメール文もさることながら、日報、週報などの内容は外部者から見て、業務の進み具合を把握するのに効果的である。

メール文の解析は、対象とするテーマの情報入手をする前の、担当者の特定に有効であり、特定のテーマについてはその担当者への接近が効果的と言える。対象とするテーマの詳細な情報を入手するには、メール文の解析は適さないと言える。その点で、電子メールの防御は、進入の第一段階である入口の防御と言える。

6.3. 政治・外交・軍事機密への脅威

本資料では触れない領域は、政治・外交・軍事等の機密への脅威である。これは企業機密と共通点もあるが、企業機密は互いに(Cyber Space 外で)競争関係にある企業での脅威であるが(追随をしよう/許さない)、ここで言う政治・外交・軍事機密は互いに(Cyber Space 内外で)衝突しあう同士間の脅威である(勝つ/負けない)。そのためもあって、脅威行為を行う側の目的も異なるであろう。この種の内容に関する資料として、参考資料[7]では、イランの原子力開発システムへの進入として有名になった事例を含む記述がある。

7. おわりに

本資料では、サイバー保全の特性を整理し、脅威目的の違いに対処する方策などを考察した。今後、考察が必要とされるのは、脅威目的がインテリジェンス入手の場合であろうと推定される。参考資料[8]では、米国内での、学会を中心とした討論集会(政府機関からの Cyber Security に関する研究計画についての意見集約)が、2015 年 5-7 月に、数か所で開催されたことが示されている。その

参照資料の中に、討議内容の記録がある。当該テーマの研究者には有益な内容となろう(上記で情報共有に関して触れた、脅威情報内容の有益性と個人・組織の匿名性の両立、設計段階からの保全の作りこみ、脅威からの修復・回復:resiliency 等は将来研究テーマとして挙げられている)。

本資料では、今後の課題としてインテリジェンス管理を挙げた。例えば、企業のインテリジェンスが漏洩したとすると被害が及ばないような対処が予め準備される必要がある。しかし、たとえ企業のインテリジェンスが漏洩したとしても、実質的な被害が生じるのであろうかは明確でなく、疑問が残る。例えば、企業が扱う製品やサービスは永年の蓄積によるであろうことから、ある瞬間にやり取りされている情報からのみその内容を理解するのは困難であるし、製品やサービスの実体から隔離された情報(インテリジェンス)のみによる理解は困難であろうと思える。但し、中には漏洩することが致命的なインテリジェンスも存在するかもしれない。

インテリジェンス(より一般的には情報)を入手して、それがどのような効果をもたらすのであろうか。現在は情報社会なのではなく、インテリジェンス社会と呼んだとしても、何が致命的ともなるインテリジェンスなのかの考慮がなされているとは思えず、単にサイバー保全という観点だけでなく、情報システム構築の面からも、その果たす価値、役割が何かを考え、認識する必要がありそうである。個人や組織が、自分の持つインテリジェンスを正確に評価することが求められる。

参考資料

注　参考資料は全て公開されたものである。

[1] Bruce Schneier, ‘The Future of Incident Response’ IEEE Security and Privacy, September/October 2014
[2] ‘Cyber Vision 2025 United States Air Force Cyberspace Science and Technology Vision 2012-2025’ . 2012
[3] Newsweek, ‘From Russia with Malware’, 2015, 13, May issue
[4] Mandiant社. ‘Attack the security gap’, 2013, ‘Beyond the Breach’, 2014, ‘A View from the Front Lines’, 2015, www.mandiant.com
[5] ‘Operation Aurora http://www.sophia-it.com/content/Operation Aurora
[6] Eric M. Hutchins, Michael J. Clopperty and Rohan M. Amin, ‘Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains’, the 6th Ann. Int’l Conf. Information Warfare and Security, 2011
[7]Hal Berghel, ‘Farewell to Air Gaps’, IEEE Computer, Part 1(June 2015), Part 2(July 2015)
[8] Terry Benzel, ‘A Strategic Plan for Cybersecurity Research and Development’, IEEE Security & Privacy, July/August 2015