

通商産業省委託事業

「対サイバーテロ・コンティンジェンシープラン立案の研究」

調査研究報告書

平成 12 年 3 月

情報処理振興事業協会

対サイバーテロ・コンティンジェンシープラン立案の研究

目次

はじめに	1
第1章 コンティンジェンシープランのあり方	2
1-1 コンティンジェンシープランとは	2
1-2 本調査研究の対象となるコンティンジェンシープランの定義	3
1-3 コンティンジェンシープランの構成	4
1-3-1 策定対象の定義とプライオリティの設定	5
1-3-2 継続・復旧のためのリソースの確保	7
1-3-3 シナリオに基く緊急時の行動計画	9
1-3-3-1 シナリオの作成	9
1-3-3-2 緊急時行動計画の策定	10
1-3-4 運用と見直し	11
1-4 サイバーテロリズムの定義	13
1-4-1 サイバーテロリズムとは	13
1-4-2 サイバーテロリズムの分類	13
1-4-3 サイバーテロリズムの手口の分類	14
1-4-4 本調査研究におけるサイバーテロリズムの定義	16
1-4-5 大規模プラントにおけるサイバーテロリズムの考え方	17
第2章 コンティンジェンシープラン策定の手引き	20
2-1 コンティンジェンシープランの必要性	20
2-2 前提条件	21
2-3 コンティンジェンシープラン策定手順	23
2-3-1 コンティンジェンシープラン策定の前にしておく作業	23
2-3-1-1 対象システムの抽出	23
2-3-1-2 システムの分析	26
2-3-1-3 既存のコンティンジェンシープランの分析	30
2-3-2 対サイバーテロ・コンティンジェンシープランの策定	33
2-3-2-1 基本方針の策定	33
2-3-2-2 組織・体制の整備	35
2-3-2-3 回復マニュアルの策定	37
2-3-2-4 緊急時行動計画の具体例	40
2-3-2-5 コンティンジェンシープランの運用と見直し	51
2-4 その他のセキュリティ対策へのフィードバック	52
2-4-1 セキュリティ対応体制への反映	52
2-4-2 セキュリティ教育への反映	53
2-4-3 セキュリティポリシーへの反映	53

第3章 コンティンジェンシープランのサンプル	56
------------------------------	----

おわりに	72
------------	----

付録

付録A トラッププログラム	A-1
付録B 検査ツール	B-1
付録C 主要な情報セキュリティ技術	C-1
付録D 緊急時行動計画一覧表	D-1

参考資料

はじめに

近年の情報化の進展に伴い、経済・社会の多くの分野がコンピュータ・ネットワーク・システムに依存するようになってきている。その結果、コンピュータ・ネットワーク・システムの機能が停止したり完全性が失われると、経済活動はもとより、国民生活全般に深刻な影響を及ぼすことになる。また、最近ではネットワークを通じて政府や産業に対して行われる敵対的な行為、いわゆるサイバーテロリズムの脅威も認識されてきている。そこで、今後、高度情報化社会を円滑に機能させていくためには、コンピュータ・ネットワーク・システムに対するセキュリティ対策が十分に行われることが必要になってきている。

このような状況を踏まえ、通商産業省では、大規模で広範な社会経済基盤におけるサイバーテロリズム・クラッキング対策のあり方について検討を行うために、平成 9 年 9 月より「大規模プラント・ネットワークセキュリティ対策委員会」（委員長 梅田富雄 千葉工業大学プロジェクトマネジメント学科教授）を設置している。そして、本委員会において石油プラントをはじめとする大規模プラント・ネットワークのセキュリティ対策についての検討が行われ、平成 10 年 3 月に「大規模プラント・ネットワーク・セキュリティについての中間報告書」がまとめられた。また、これを受けて情報処理振興事業協会では、「石油プラントのネットワーク安全性検証実験」を行い、平成 11 年 10 月に「安全性検証実験報告書」をとりまとめた。これらの報告書では、大規模プラント・ネットワーク向けのセキュリティ対策規準の策定、侵入経路別のリスク分析手法の開発、プラント用の暗号・認証技術の開発や疑似アタック実験による監査、リモートメンテナンスや無線 LAN 使用時における運用管理対策など数多くの有意義な成果を導出することができた。

一方で、万一の不測の事態が発生した場合を想定し、その際の被害を最小限に留め、迅速に元の状態に復旧するための方法についても事前に検討しておくことは、セキュリティ対策上重要な事柄の一つである。例えば、コンピュータ西暦 2000 年問題に際し、平成 11 年 4 月に政府の高度情報通信社会推進本部は「企業のための危機管理計画策定の手引き」を発行している。また米国では、既に 1981 年に FIPS (Federal Information Processing Standards) として「Guidelines For ADP Contingency Planning」が発行されている。このように、何か緊急事態が発生した場合の対応手順についてまとめられた文書は、危機管理計画書、あるいはコンティンジェンシープランと呼ばれている。これまで、コンティンジェンシープランは、自然災害や事故などの偶発的な脅威を対象として作成されるケースが多く見受けられた。しかし、インターネットの爆発的な普及を背景にして、近年、システムのネットワーク化、相互接続化が急速に進展する中で、新たにサイバーテロリズムの脅威に対するコンティンジェンシープラン策定を必要とする機運が高まってきている。このような、国内外の情報セキュリティをめぐる状況を踏まえ、情報処理振興事業協会では「対サイバーテロ・コンティンジェンシープラン立案の研究」を行うこととなった。

本研究は、「大規模プラント・ネットワークセキュリティに関する研究プロジェクト」の一環として実施されている。そのため、主として大規模プラントのコンピュータシステムをその対象として取り扱っている。しかし、本研究で検討された手法は、汎用のコンピュータシステムについても同様に適用できると考えている。本報告書が、政府や企業がサイバーテロリズムに対するコンティンジェンシープランを策定する際の手引き書としても、また利用されることを期待している。

第1章 コンティンジェンシープランのあり方

1-1. コンティンジェンシープランとは

コンティンジェンシープランとは、その策定対象が潜在的に抱える脅威が万一発生した場合に、その緊急事態を克服するための理想的な手続きが記述された文書である。ここで、コンティンジェンシープランを策定する目的については、例えば米国海軍省発行の Computer Incident Response Guidebook では、コンピュータシステムのコンティンジェンシープランを策定する目的として次の7項目を挙げている。（参考資料[6]参照）

コンティンジェンシープランで達成されるべき目的

緊急事態からの迅速で効果的な復旧をサポートすること。

リスクによるダメージを最小化すること。

整然とした計画的な対応を規定すること。

システムを守ること。

システムに関係する人々を守ること。

復旧のためのリソースを効果的に使用すること。

適切な法的手続きをとること。

コンティンジェンシープランの例としては、例えばオーストラリアの政府機関である Australian Maritime Safety Authority では、海上での原油流出時のコンティンジェンシープランを策定し、その内容は Web 上で公開されている。

<http://www.amsa.gov.au/ME/NATPLAN/Contplan/index.htm>

また、別の例としては、National Aeronautics & Space Administration(NASA)では宇宙ステーションで事故が発生した場合のコンティンジェンシープランを策定し、同様に Web 上で公開している。

<http://www.hq.nasa.gov/office/oig/hq/ig-99-oc9.pdf>

その他、最近では、各国の政府が 2000 年問題に関するコンティンジェンシープランを発表した。このようにコンティンジェンシープランは、その策定対象と策定対象に対して

想定される脅威の組み合わせによって、その記述内容も千差万別であると考えられる。しかし、いかなるコンティンジェンシープランであっても、脅威が発生した場合に、策定対象に対して実施されるべき最善の事後対応策について規定されたセキュリティ文書である、という点では共通である。

脅威が発生した後では、その対処方法について検討している時間はほとんど確保することができない。また、緊急事態の下では正常な判断機能が動作しないケースも十分に考えられる。そのため、組織において策定対象が提供する機能の重要性が極めて高い場合には、どんなにその脅威の発生確率が低かったとしても、万一の事態を想定して、あらかじめその場合の対処方法を策定しておくことは、重要なセキュリティ対策の 1 つであると考えられている。

1-2. 本調査研究の対象となるコンティンジェンシープランの定義

近年、政府や企業の様々な業務のシステム化が進展し、コンピュータシステムの果たす役割が漸増している。それに伴ない、策定対象をコンピュータシステムとした（実際のところはそのコンピュータシステムを利用して提供されている業務を対象とした）コンティンジェンシープランが多数出自している。例えば、米国では、1981 年に FIPS (Federal Information Processing Standards)としてコンピュータシステムのコンティンジェンシープラン策定のための標準的な手続きが示されている。FIPS PUB 87 Guidelines For ADP Contingency Planning（参考資料[1]参照）

また一方で、ここ数年のインターネットの爆発的な普及によって、政府や企業のコンピュータシステムがネットワーク化され、他のコンピュータシステムと相互接続されたり、インターネットをはじめとする公衆回線に接続される機会が増えてきた。その結果、これまでの事例が示唆するように、サイバーテロリズムが組織のコンピュータシステムにとって大きな脅威になりつつある。（「大規模プラント・ネットワーク・セキュリティについての中間報告書」第 1 章参照）

ここで、大規模プラント・ネットワーク・セキュリティの評価実験で対象としているコンピュータシステムは、プラントの制御システムであり、当該システムを介して提供される業務の重要度は極めて高いものである。また、この制御システムは、情報系システムを介してインターネットにも接続されているため、サイバーテロリズムという脅威が発生する可能性は否定できない。

このような状況から、大規模プラント用コンピュータシステムにおける対サイバーテロ用コンティンジェンシープランの希求度は高いものであると判断できる。

そこで、本調査研究では、大規模プラントの制御システムと、当該システムを介して提供されている業務を対象として、サイバーテロリズムに対するコンティンジェンシープランの立案に関して、その策定手法の検討を行う。ここで、特にコンピュータ犯罪に関するコンティンジェンシープランをコンピュータセキュリティインシデントレスポンスプラン（CSIR; Computer Security Incident Response Plan）と呼ぶこともある。

また、本調査研究で策定するコンティンジェンシープランは、「石油プラントのネットワーク安全性検証実験」によって検証、提供された様々な防御策を補完するセキュリティ対策に相当すると考えられる。

図 1-1 に本調査研究で策定するコンティンジェンシープランの位置付けを示す。

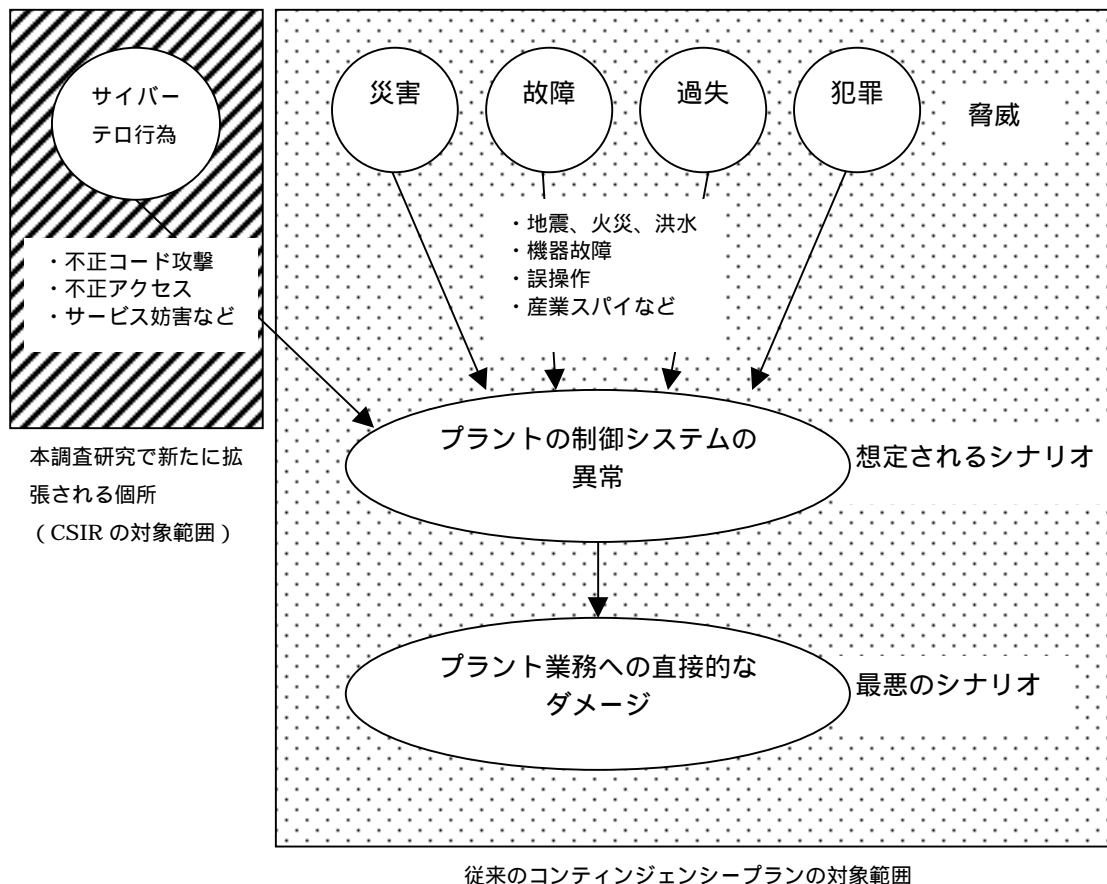


図 1-1 従来のコンティンジェンシープランと CSIR の対象とする範囲

本調査研究の対象とするコンティンジェンシープラン

大規模プラントを制御するコンピュータシステムを本調査研究の対象とする。そして、当該システムに対するサイバーテロリズムを想定したコンティンジェンシープランの策定手法に関して調査研究を行う。

1-3. コンティンジェンシープランの構成

次にコンティンジェンシープランに記載されるべき項目について調査を実施した。

例えば、前出の Guidelines For ADP Contingency Planning では、コンティンジェンシープランは以下の 4 つのパートから構成されている。

Part One Preliminary Planning

(予備計画：目的、記述範囲、仮定など)

Part Two Preparatory Actions

(準備行動：復旧作業に必要なリソース)

Part Three Action Plan

(緊急時行動計画)

Part Four Testing

(テスト)

また、NIST SP 800-12 An Introduction to Computer Security (参考資料[5]参照)では、コンティンジェンシープランで考慮されるべき内容として、次の6項目を挙げている。

Step1 Identifying the Mission- or Business-Critical Functions

(組織の事業上重要な業務の定義)

Step2 Identifying the Resource That Support Critical Functions

(業務を復旧させるために必要なリソースの定義)

Step3 Anticipating Potential Contingencies or Disasters

(潜在的に抱える脅威の想定)

Step4 Selectiong Contingency Planning Strategies

(基本的な戦略の選定)

Step5 Implementing the Contingency Strategies

(緊急時行動計画の策定)

Step6 Testing and Revising

(テストと改訂)

更に、U.S. Fish and Wildlife Service 発行の Guidelines for Contingency Plan Development (参考資料[2]参照)では、コンティンジェンシープランに記述されるべき7項目を以下のように挙げている。

1. Scope (記述範囲)
2. Recovery Priorities (復旧作業の優先順位)
3. Contingency Events (脅威の想定)
4. Security (緊急時行動手順のセキュリティ確保)
5. In-place Protections (バックアップ手続き)
6. Supplies (復旧作業に必要なリソース)
7. Testing the Plan (プランのテスト)

そして、これらの調査の結果、コンティンジェンシープランでは、次の4項目について記述されていないことがわかった。

- 第1部 策定対象の定義とプライオリティの設定
- 第2部 継続・復旧のためのリソースの確保
- 第3部 シナリオに基づく緊急時の行動計画
- 第4部 運用と見直し

以下、それぞれの項目で記載されるべき内容について述べる。

1-3-1. 策定対象の定義とプライオリティの設定

コンティンジェンシープランでは、まずはじめに当該プランで対象とする範囲について

定義しておく必要がある。具体的には、

対象となるコンピュータシステム
当該コンピュータシステムで提供されている業務
対象となる脅威

を明確にしなければならない。

まず、対象とするコンピュータシステムの範囲とそのシステム上で提供している業務について明らかにしておく。コンピュータシステムで提供している業務の定義が不明瞭な状態では、緊急時に業務の継続・復旧作業を行うことは困難だからである。また、当該システムで提供されている業務を定義するためには、事前に業務分析を行っておく必要がある。

対象とするコンピュータシステムと業務が定義されたら、次に定義した業務に対してそれぞれプライオリティを設定する作業を行う。それぞれの業務にプライオリティが設定されていなければ、どの業務から継続・復旧させればいいのかの判断を行うことができないからである。また、緊急時に、平常時に提供されている全ての業務を継続・復旧できるようなバックアップリソースを用意しておくことは、費用対効果の観点から考えても現実的ではない場合が多い。そこで、まず脅威が発生した場合には、ある程度の業務は停止するものだと認識しておく必要がある。そして、そのために、システムで提供している業務を定義した後に、それぞれの業務にプライオリティを設定する作業が必要になってくる。

プライオリティの設定は、「それぞれの業務が停止していることが許容される期間」、言葉を換えれば「それぞれの業務が復旧するまでに要することができる最大時間枠」によって行われなければならない。例えば、次のような表を作成しておくのもよい考えである。

表 1-1. 対象システムの業務定義とプライオリティの設定

業務名	重要度	復旧までの許容時間
業務 A	S	業務が停止することは許されない。
業務 B	A	24 時間以内に復旧しなければならない。
業務 C	B	3 日以内に復旧しなければならない。
業務 D	C	緊急事態の際は停止してよい。

そして、最後に当該コンティンジェンシープランで対象とする脅威についても、本項目で定義しておく。

業務のプライオリティ付けと対象とする脅威の定義作業を行うためには、事前にリスク分析を行っておく必要がある。

コンティンジェンシープラン記載項目(1)

< 策定対象の定義とプライオリティの設定 >

- (1) コンティンジェンシープランで対象とするコンピュータシステムについて定義する。
- (2) 対象としたコンピュータシステムで提供している業務について定義する。
- (3) 定義したそれぞれの業務に対してプライオリティ付けを行う。
- (4) コンティンジェンシープランで対象とする脅威について定義する。

1-3-2. 継続・復旧のためのリソースの確保

前節では、コンティンジェンシープランとして記述する対象範囲について定義することができた。次に、コンティンジェンシープランでは、各業務を継続・復旧させるために必要とされるリソースのリストに関する記述を行う。ここで、リソースのリストを作成するためには、事前に業務分析及びリスク分析を行っておく必要がある。

ここで、復旧作業のために必要なリソースについて、Guidelines For ADP Contingency Planning では次の10種類のリソースを挙げている。

1. People (要員)
2. Data (データ)
3. Software (ソフトウェア)
4. Hardware (ハードウェア)
5. Communications (通信手段)
6. Supplies (日用品)
7. Transportation (移動手段)
8. Space (作業場所)
9. Power and Environmental Controls (電力と環境調節機能)
10. Documentation (文書)

また、An Introduction to Computer Security では、同様に復旧作業のために必要なリソースとして、次の6種類のリソースを挙げている。

1. Human Resources (人的リソース)
2. Processing Capability (データ処理機能)
3. Automated Applications and Data (アプリケーションとデータ)
4. Computer-Based Services (データ通信サービス)
5. Physical Infrastructure (物理的インフラストラクチャ)
6. Document and Papers (文書)

そして、これらの調査結果をまとめると、緊急時に業務を継続・復旧させるために必要なリソースとしては、次の6種類のリソースが考えられる。

人的リソース

継続・復旧業務に従事する要員は、いつも同じメンバーとは限らない。ある特定の業務を継続させるためには、当該業務の専門知識を有する要員を必要とする場合がある。また、サイバーテロなどのそれぞれの脅威に対処するために特別に訓練された対応要員を必要とする場合も考えられる。各業務を緊急時の下で継続・復旧させるために必要な人材をリストアップしなければならない。

処理用リソース

特に自然災害や事故などの脅威を想定したコンティンジェンシープランでは、業務処理を行うコンピュータやネットワークなどの処理用のリソースがダメージを受ける場合も考えられる。各業務を継続・復旧するために必要な処理用のリソースをリストアップしなければならない。

アプリケーションとデータリソース

業務を継続・復旧させるためには、処理用リソースの上で稼動するアプリケーションとデータも必要である。ここで、もし緊急時には、アプリケーションが本番環境とは異なる種類のコンピュータ上で処理されるようならば、アプリケーションは異機種間での互換性を備えているものをリストアップしておかなければならない。

通信リソース

特に自然災害や事故などの脅威を想定したコンティンジェンシープランでは、電子メールや電話、FAX など通常時のコミュニケーション手段が、脅威発生時には使用できない場合も想定される。そこで、緊急時のコミュニケーションリソースの確保についても、事前に考慮しておかなければならない。

物理的なインフラストラクチャリソース

脅威発生時に、対応要員が安全に、かつ効果的に継続・復旧作業を行うために必要な物理的なインフラストラクチャリソースについても考慮しなければならない。物理的なインフラストラクチャリソースとは、例えば、作業空間、空調設備、電源、水道、食料、現金などが考えられる。

ドキュメントリソース

業務を継続・復旧させるために必要となる、重要な情報が用紙に記述されている場合もある。例えばベンダーとの保守契約書や保険会社の保険証券などが復旧作業の過程で必要とされる可能性は十分に想定される。また、電子媒体に記録されているデータのバックアップとして、データを用紙に印刷している場合なども必要リソースとしてリストアップしなければならない。もちろん、現在策定中のコンティンジェンシープランも当該リソースに含まれる。

ここでリストアップするリソースは、通常業務を行う際に必要とするリソースではなく、あくまで緊急時に業務を継続・復旧させるための最小構成リソースであることを確認しておかなければならない。平常時と全く同じリソースを確保することは、緊急時には困難な場合が多く、費用対効果の観点からも現実的ではない。

また、リストアップしたリソースは、それぞれその調達手段についても考慮しておかなければならない。自然災害や事故を想定したコンティンジェンシープランでは、社会的なインフラである輸送機能や移動機能が麻痺してしまうことも十分に考えられる。そこで、緊急時における各リソースの調達手段もリソースリストには記述しておくといよい。

コンティンジェンシープラン記載項目（２）

< 継続・復旧のためのリソースの確保 >

- （１）各業務毎にその業務を継続・復旧するための必要最小限のリソース構成をリストアップする。
- （２）リソースは、次の６つのカテゴリにおいて考慮されていなければならない。
 - 人的リソース
 - 処理用リソース
 - アプリケーションとデータリソース
 - 通信リソース
 - 物理的なインフラストラクチャリソース
 - ドキュメントリソース
- （３）リストアップしたリソースの調達手段を確保する。

1-3-3. シナリオに基く緊急時の行動計画

前節までに、コンティンジェンシープランの対象範囲が定義され、また、緊急事態の下で継続・復旧作業を行うために必要とされるリソースとその調達手段について定義することができた。次に、コンティンジェンシープランでは、脅威が発生した場合の具体的な行動計画について記述する。この際、まずはじめに何パターンかの脅威発生シナリオが作成され、行動計画はそれぞれのシナリオごとに策定される。

1-3-3-1. シナリオの作成

脅威発生シナリオは、1-3-1 節「策定対象の定義とプライオリティの設定」で定義した脅威が単発で生じた場合のシナリオから、複数の脅威が同時多発した場合のシナリオまで幅をもたせて作成する。ここで、シナリオを作成する際にも、リスク分析の結果をその作業に反映させる必要がある。もちろん、事前に起こり得る全ての脅威をシナリオとして取り上げておくことはできないが、可能性がありそうな範囲でシナリオを想定していく。

1-3-3-2. 緊急時行動計画の策定

脅威発生シナリオが準備できたら、次に各シナリオにおける行動計画を策定する。行動計画を策定するにあたって、その作業過程でいくつかの選択肢が考えられる場合がある。この際、適切な選択肢を選ぶための判断基準として An Introduction to Computer Security では次の3つ事柄を提示している。

- どの選択肢が最もダメージを最小化できるのか。(prevent and minimize)
- どの選択肢が最も実現性が高いのか。(feasibility)
- どの選択肢が最も費用対効果が高いのか。(cost effective)

行動計画の作成担当者は、これらの判断基準を元に脅威を克服するために最適な戦略を決定していかなければならない。

ここで、実際の行動計画について、例えば Guidelines For ADP Contingency Planning では、緊急時行動計画は3つの行動フェーズから構成されている。

- Phase1 Emergency Response (緊急対応)
- Phase2 Backup Operation (バックアップ)
- Phase3 Recovery Actions (復旧活動)

また、An Introduction to Computer Security では、同様に緊急時行動計画を3つの行動フェーズで規定しているが、こちらは緊急時対応から平常業務への移行までをその対象範囲としている。

- Phase1 Emergency Response (緊急対応)
- Phase2 Recovery (復旧)
- Phase3 Resumption (再開)

そこで、本調査研究では、Guidelines For ADP Contingency Planning の定義に倣って、緊急時行動計画は次の3つのフェーズから構成されているものとする。

緊急時対応フェーズ

脅威が発生した場合に、人命や組織の財産を保護し、そのダメージをできる限り軽減するために行われる初期動作、緊急手続きに関する行動計画が記述されたフェーズ。

バックアップフェーズ

業務を継続・復旧する作業に先駆けて実施される手続きに関する行動計画が記述されたフェーズ。例えば、関係者への連絡や次フェーズで利用するリソースの調達作業などが該当する。

継続・復旧フェーズ

緊急事態の下で、業務を復旧し継続するために実施される手続きに関する行動計画が記述されたフェーズ。

コンティンジェンシープランの各シナリオで想定している脅威によって、それぞれのフ

フェーズで記述される具体的な行動計画の内容も様々であるが、いずれの行動計画においても、前述の 3 つのフェーズに関する手続きが過不足なく規定された内容でなくてはならない。また、この行動計画はコンティンジェンシープランのメインパートに相当する。緊急事態発生時には、当該個所を参照しながら対応作業を行うことになる。そこで、この部分だけをプリントアウトして、クリアファイルやルーズリーフでまとめ、関係者がいつでも参照できるような場所に用意しておくのはよい考えである。また、緊急時には正常な判断機能が働かない場合も多いので、当該パートでは、できるだけ冗長性を排除した簡潔な記述を目標とする。具体的には、行動内容が箇条書きで実施順に並べられているようなフォーマットが望ましい。また、他の資料やコンティンジェンシープランの他の項目の参照を必要とするような記述も避けるべきである。

コンティンジェンシープラン記載項目 (3)

<シナリオに基く緊急時の行動計画>

- (1) リスク分析の結果を元にシナリオを作成する。
- (2) シナリオ毎に行動計画を策定する。行動計画では次の 3 項目を判断基準としてその戦略が決定される。
 - どの選択肢が最もダメージを最小化できるのか。
 - どの選択肢が最も実現性が高いのか。
 - どの選択肢が最も費用対効果が高いのか。
- (3) 行動計画は次の 3 つのフェーズから構成される。
 - 緊急時対応フェーズ
 - バックアップフェーズ
 - 継続・復旧フェーズ

1-3-4. 運用と見直し

前節までの作業により、コンティンジェンシープランを策定することができた。そして、最後にコンティンジェンシープランでは、プラン策定後に行う運用と見直し作業についても記述しておくといよい。コンティンジェンシープランが、それを必要とされる緊急時に真に有用なプランであるために、プラン策定後のメンテナンス作業は重要である。

実際、コンティンジェンシープランの調査のために参照した参考資料でも、全てプランのテストに関する記述が為されていた。その中でも Guidelines for Contingency Plan Development がテスト計画についてよくまとめられていたため、本調査研究でも当該参考資料の記述内容に倣うこととした。

テスト計画

策定したコンティンジェンシープランに対する定期的なテスト計画を立案する。テストを行っていないコンティンジェンシープランでは、その記述内容の正当性を保証すること

ができない。また、コンピュータシステムでは、機器やプログラム、関連文書などの仕様の変更が頻繁に発生する場合も多い。そこで、コンティンジェンシープランが現在のコンピュータシステムに対して、有効であることを保証し続けるために、定期的且つ継続的なテスト計画を立案しておく必要がある。特に、コンピュータシステムが提供する機能の仕様変更や、1-3-2 節「継続・復旧のためのリソースの確保」でリストアップされたリソースの構成変更が発生した場合には、直ちにテストを実施するようにしておかなければならない。

テストの実施と評価

テスト計画が立案されたら、その計画に沿ってテストが実行される。テスト方法としては、1-3-3 節「シナリオに基く緊急時の行動計画」で定義されたシナリオの 1 つまたは複数を選択したシミュレーションが有効である。この際、実際に想定脅威を発生させる必要までにはしないし、予算が許す範囲でなるべく現実性を高めたテストを実施するとよい。また、コンティンジェンシープランの記述内容の有効性を評価するための評価基準や評価ポイントも併せて設定しておくべきである。

更新作業

テストの結果、プランの内容に変更の必要性がある場合には速やかにその内容を反映し、変更の影響を受ける関係者には、その旨を通知し了承を得なければならない。

コンティンジェンシープラン記載項目 (4)

< 運用と見直し >

- (1) コンティンジェンシープランに対する定期的、継続的なテスト計画を立案する。
- (2) テストの実施方法と評価基準について検討する。
- (3) コンティンジェンシープランの更新作業に関する手続きについて検討する。

1-4. サイバーテロリズムの定義

本調査研究では、大規模プラントを制御するコンピュータシステムに対するサイバーテロリズムを想定したコンティンジェンシープランの策定手法に関して検討を行っている。

ここで、コンティンジェンシープランを策定するためには、まず当該プランで想定している脅威を正確に定義しておく必要がある。(1-3-1 節「策定対象の定義とプライオリティの設定」参照)そこで、本節では、本調査研究で対象とするサイバーテロ行為について検討を行う。

1-4-1. サイバーテロリズムとは

「大規模プラント・ネットワーク・セキュリティについての中間報告書」では、サイバーテロリズムを次のように定義している。

サイバーテロリズムとは

ネットワークを通じて政府や産業に対して行われる敵対的な行動であり、大規模で組織的な不正アクセスを試みることである。サイバーテロリズムは米国等の専門家によって「グローバルな情報戦争」と定義され、一定の政治・経済的目的により、行政、金融、航空管制、電力などの公共のコンピュータ・ネットワーク・システムに不正侵入し、システム自体の誤動作、停止、破壊及び重要情報の不正取得、改ざん、ウィルス投与等を引き起こすことである。

そこで、本調査研究で対象とするサイバーテロリズムの定義もこれに倣うものとする。

1-4-2. サイバーテロリズムの分類

前節の定義に従えば、サイバーテロリズムは、しばしば情報戦争(Information Warfare)と定義されることもある。ここで例えば、National Defense University(NDU)の MARTIN LIBICKI 博士は、What Is The Information Warfare? (参考資料[18]参照)の中で、情報戦争を次の7種類に分類している。

Command-and-Control Warfare (指揮系統戦争)

敵の司令部、あるいは司令部からの命令の伝達経路を攻撃、破壊し、相手の指揮系統を麻痺、あるいは混乱させる行為。

Intelligence-Based Warfare (諜報戦争)

高性能な情報収集装置によって、敵陣の配置や攻撃によるダメージの評価など相手の状況を的確に把握する行為。

Electronic Warfare (電子戦争)

暗号やアンチレーダーなどの技術を用いて、や のタイプの攻撃を防御する行為。

Psychological Warfare (心理操作戦争)

敵になりすましてデマ情報を伝達し、相手に心理的なダメージを与え士気を低下させたり、混乱させる行為。

Hacker Warfare (ハッカー(クラッカー)戦争)

不正コード(コンピュータウイルス、トロイの木馬など)や不正アクセス技術を用いて、敵の情報システムをネットワーク経由で攻撃、破壊する行為。

Economic Information Warfare (情報封鎖戦争)

敵の情報伝達基盤を破壊し、情報伝達機能を麻痺させ、外部との情報の出入を停止させる行為。相手国の社会基盤や経済基盤が、諸外国との情報交換によって成り立っている場合に有効とされる。

Cyber Warfare (情報兵器戦争)

敵の情報システム自体を兵器として操作、利用し、相手を攻撃させる行為。

本節で紹介した情報戦争は、情報システムを中心にした攻防について広く考察されている。そのため、物理的な破壊やソーシャルエンジニアリングまでも実際の情報戦争の攻撃手法として包含しており、本調査研究におけるサイバーテロリズムの定義とは完全には一致していない。しかし、サイバーテロリズム(情報戦争)の考え方や分類の仕方は、シナリオ想定作業の際などに参考にすることができる。

1-4-3. サイバーテロリズムの手口の分類

コンティンジェンシープランで想定されるサイバーテロリズムは、実際には各策定対象によって異なるものである。そこで、コンティンジェンシープラン策定に先立って、まずはリスク分析を行い、策定対象のシステムで発生する可能性のあるサイバーテロリズムを定義しなければならない。

一方で、本調査研究で対象とするサイバーテロリズムを、技術的な側面から捉えると「ネットワークを通じて行われる不正アクセス技術」と定義することができる。テロリストによって「ネットワークを通じて行われる不正アクセス技術」を行使された結果、もたらされるサイバーテロリズムは各コンピュータシステムやそのテロリストによっても異なってくるが、他方でその発端(手口)となる不正アクセス技術にはある一定の共通性を認めることができる。

ここで、不正アクセスをはじめとするコンピュータシステムに対する様々な技術的不正行為は、コンピュータセキュリティインシデント(Computer Security Incident)と呼ばれ

ている。本節では、テロリストがサイバーテロを引き起こす際に用いる技術的手法であるコンピュータセキュリティインシデントについて検討を行う。

コンピュータセキュリティインシデントとは、コンピュータシステムに対して行われる技術的な不正行為であり、テロリストはこれらの技術（手口）を巧みに駆使してサイバーテロ行為を引き起こすことができる。

ここで、Computer Incident Response Guidebook では、コンピュータセキュリティインシデントを次の7種理に分類している。

Malicious code attacks (不正コード攻撃)

コンピュータウィルスやトロイの木馬、ワームあるいはパスワードスニッファやログ消去プログラムなどの不正プログラムを使用した攻撃手法。

Unauthorized access (不正アクセス)

あるユーザのアカウントを断り無く奪取、使用しシステムにログインし、さらに上位の（通常は特権ユーザ）ユーザ権限を奪取したり、本来アクセス権限のないファイルやディレクトリ、あるいはシステムリソースにアクセスし、盗用、改ざん、破壊などの行為を行う攻撃手法。

Unauthorized utilization of services (サービスの不正使用)

不正アクセスと本質的には同様の攻撃手法であるが、システムの脆弱な設定やセキュリティホールを利用することによって、ログイン行為を行わずに不正アクセス同様の不正行為を行うことができる場合もある。不正アクセスとサービスの不正使用を併せて、不正アクセスと定義してもよい。

Disruption of service (サービス妨害)

DoS(Denial of Service)攻撃としても知られている攻撃手法。システムが予期せぬ不正な入力を与えたり、システムに処理能力以上の負荷をかけることによって、システムが提供している機能の一部または全部を麻痺させる攻撃手法。

Misuse (誤まった使用方法)

コンピュータシステムを本来の目的とは異なる用途で使用する攻撃手法。例えば、組織のシステムからインターネットのアダルトホームページを閲覧したり、組織のシステムを利用して個人的な商行為を行ったりすることが考えられる。

Espionage (スパイ行為)

産業スパイに代表されるように、例えば清掃員や社員などになりすまして、攻撃対象のシステムやその関係者への社会的な接触を利用して、システムに対して不正行為を行う攻撃手法。

Hoaxes (風説の流布)

デマ情報、あるいは特定個人や特定組織を誹謗中傷した内容をメールや電子掲示板、ホームページなどを使って流布し、相手を混乱させたり、相手のイメージダウンを画策する攻撃手法。

また、The SANS Institute 発行の Computer Security Incident Handling (参考資料[7] 参照) では、これらの定義に加えて、

Probes and Network Mapping (システム探査)

相手のシステム構成を探査する攻撃手法。コンピュータシステムに対する不正行為の初動や、あるいは不正行為の試みが失敗した痕跡として考えられている。具体的にはポートスキャンやピングスキャン、DNS レコード検索などがその手法としてよく知られている。

もコンピュータセキュリティインシデントとして追加されている。

1-4-4. 本調査研究におけるサイバーテロリズムの定義

前節では、サイバーテロ行為の手口として利用されるコンピュータセキュリティインシデントについて検討を行った。本調査研究では、サイバーテロ行為を「ネットワークを通じて行われる悪意ある侵入者による攻撃」と定義している。そこで、実際には前節で示した 8 つのタイプの攻撃手法のうち、次の 5 つのタイプの攻撃が本調査研究におけるサイバーテロ行為の手口として該当すると考えられる。

- 不正コード攻撃
- 不正アクセス (サービスの不正使用を含む)
- サービス妨害
- 風説の流布
- システム探査

コンティンジェンシープランの作成者は、まず対象となるシステムに対して、上記 5 つのタイプの攻撃が発生する可能性をリスク分析によって導出し、その結果もたらされるサイバーテロ行為とその場合の影響度を想定することができる。

本調査研究におけるサイバーテロリズムの定義

ネットワークを通じて政府や産業に対して行われる大規模で組織的な敵対行動。

サイバーテロリズムで利用される技術的な手口

不正コード攻撃
不正アクセス（サービスの不正使用を含む）
サービス妨害
風説の流布
システム探査

1-4-5. 大規模プラントにおけるサイバーテロリズムの考え方

前節までに、本調査研究におけるサイバーテロリズムと、その際に利用される手口について定義することができた。そこで本節では、本調査研究の対象である大規模プラントのコンピュータシステムで発生する可能性のあるサイバーテロリズムに関して具体的な検討を行う。なお、本節では「大規模プラント・ネットワークセキュリティについての中間報告書」で示された、大規模プラント・ネットワークにおけるシステム構成モデル（図 1-2 参照）をその検討に用いる。

図 1-2 が示すように、大規模プラントのコンピュータシステムは、業務処理に使用され、インターネットをはじめとする社外ネットワークにも接続されている情報系システムと、工場の運転、制御のために使用されている制御系システムの 2 種類のネットワークシステムから構成されている。

ここで、この 2 つのシステムは、システムが果たしている役割の重要度の違いから、そのセキュリティレベルを同列に扱うことはできない。特に制御系システムにおいては、当該システムに対してサイバーテロ行為が発生した場合には、人命が危険に晒される可能性や、社会的に大きな影響を及ぼす可能性が十分に考えられる。そこで、まず大規模プラントのコンピュータシステムのうち、制御系システムを対象としたコンティンジェンシープランを策定することが急務であると考えられる。

本調査研究の対象とするコンピュータシステム

大規模プラントのコンピュータシステムのうち、その果たしている役割の重要性から制御系システムを対象とする。

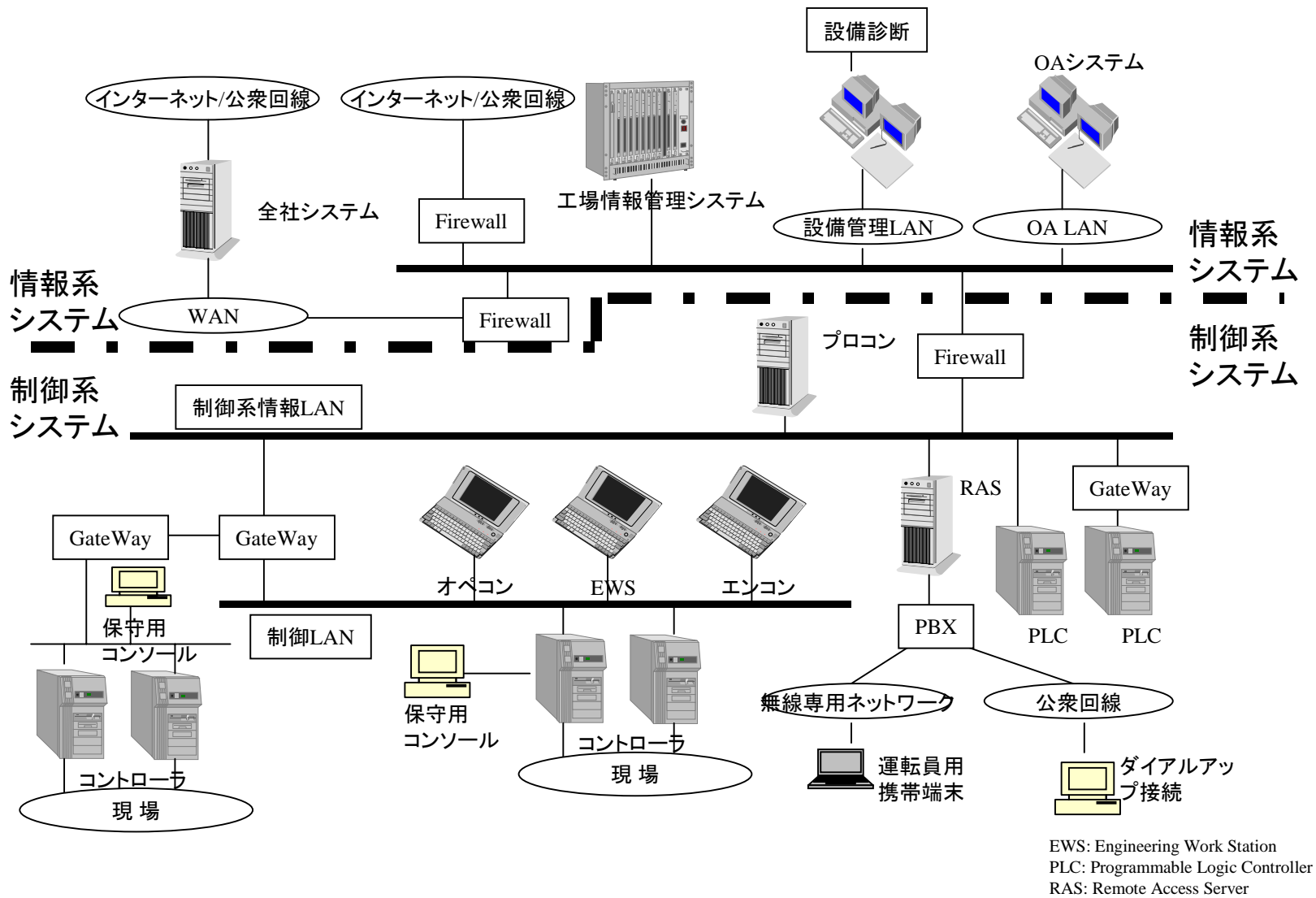


図1-2 大規模プラントネットワークにおけるシステム構成モデル

次に、「大規模プラント・ネットワーク・セキュリティについての中間報告書」では、制御系システムに発生する可能性のあるサイバーテロ行為として次の3点を指摘している。

不正侵入

情報系システムを経由した不正侵入、ダイヤルアップ接続を経由した不正侵入、無線 LAN を経由した不正侵入の3つの侵入経路による不正侵入の発生の可能性がある。

コンピュータ・ウィルスの侵入

制御系システムに接続されたホストがコンピュータ・ウィルスに感染する可能性がある。

ソーシャル・エンジニアリングによる侵入

制御系システムにソーシャル・エンジニアリングによって侵入される可能性がある。

また、この結果を受けて実施された「石油プラントのネットワーク安全性検証実験」では、制御系システムに対して次の3点が指摘された。

情報系システムに侵入された場合は、そこを踏み台としてプロコンの管理するコントローラの設定値を変更することができた。

制御系システムのうち、特に制御 LAN に接続されたホストには独自 OS が採用されており、その存在の発見すらも不可能であった。

電話回線経由の不正侵入は通信路上の暗号化とワンタイムパスワードが導入されていたために成功しなかった。

そして、これらの調査結果を考え合わせると、現時点でカスタム OS ベースの大規模プラントの制御系システムにおいて考えておかなければならないサイバーテロ行為としては、

大規模プラント制御系システムで想定しておかなければならないサイバーテロ行為

(カスタム OS の場合)

情報系システム経由の制御系情報 LAN への不正アクセス。とりわけ、プロコンが管理するコントローラの設定値の不正操作。

制御系情報 LAN に接続された汎用 OS を使用しているホスト (Firewall、プロコン、RAS) のコンピュータ・ウィルス感染による誤動作や重要ファイルの喪失。

以上2つが、特に発生する可能性が高いシナリオとして想定することができる。

なお、前節で示したように、本調査研究ではソーシャル・エンジニアリングをその対象とはしていない。

第2章 コンティンジェンシープラン策定の手引き

2-1. コンティンジェンシープランの必要性

第1章では、コンティンジェンシープランの構成とサイバーテロリズムについて検討を行った。その結果、コンティンジェンシープランは次の4部から構成されること、

コンティンジェンシープランの構成

- 第1部 策定対象の定義とプライオリティの設定
- 第2部 継続・復旧のためのリソースの確保
- 第3部 シナリオに基く緊急時の行動計画
- 第4部 運用と見直し

そして、本調査研究におけるサイバーテロリズムとは、

サイバーテロリズムの定義

ネットワークを通じて政府や産業に対して行われる大規模で組織的な敵対行動。

であり、また、テロリストがサイバーテロを引き起こす手口としては次の5つの手法があることがわかった。

サイバーテロリズムで用いられる手口

- 不正コード攻撃
- 不正アクセス
- サービス妨害
- 風説の流布
- システム探査

続いて、第2章ではコンティンジェンシープランの策定手順に関して検討を行う。

本調査研究では、大規模プラントの制御システムを対象とした対サイバーテロ用コンティンジェンシープランの策定手順を立案することを目的としている。ここで、コンティンジェンシープランとは、大規模プラントの制御システムに対して、サイバーテロ行為が発生した場合に、リスクによるダメージを最小化し、システムやシステムに関係する人員を保護し、迅速に業務を復旧するために作成された文書である。万が一緊急事態が発生した場合に、最善の事後手続きを実施するための行動手順書と考えることもできる。

もし、何らかの不測の事態が発生した場合、事態発生後には、その対応策について検討している十分な時間を確保することは難しい。また、非常事態の下では、必ずしも正常な判断基準が機能しない場合も十分に予想される。

大規模プラントの制御システムは、プラントの設備や装置の制御データをその処理対象としており、プラントの業務上、非常に重要な役割を担っている。そのため、大規模プラントの制御システムを対象としたコンティンジェンシープランの策定は、プラントで実施されなければならないセキュリティ対策の必須項目の 1 つであると考えられる。また、これまでのプラントの制御システムは他のシステムとは独立した構成になっていたため、コンティンジェンシープランで対象とする脅威も、自然災害や機器故障などのいわゆる偶発的脅威を重要視する必要があった。しかし、近年このプラントの制御システムが、他の複数の制御系システムや情報系システムと相互接続されるようになり、大規模なネットワークが構成されるようになってきた。また、インターネットをはじめとする公衆回線網への接続も積極的に行われ始めている。こうしたプラントの制御システムを取り巻く状況の変化は、当該システムで提供している業務の効率性、生産性をもたらすと同時に、新たな脅威の可能性もまた内包する結果になった。その中でも、ネットワークを通じてプラントに対して行われる大規模で組織的な敵対行動、いわゆるサイバーテロリズムは、昨今の国内外の情報セキュリティをめぐる状況から鑑みても最大の脅威と捉えることができる。このような背景からも、大規模プラントの制御システム用の対サイバーテロ・コンティンジェンシープランを整備することが急務であると考えられる。

2-2. 前提条件

第 2 章では、大規模プラントの制御システム用の対サイバーテロ・コンティンジェンシープランの策定手順について検討を行う。ここで、本調査研究で主として検討する策定手順は、既存のコンティンジェンシープランをサイバーテロリズム用に拡張するための作業手順である。そのため、既に、例えば自然災害や事故などの脅威を想定して作成された何らかの制御システム用のコンティンジェンシープランが用意されていることを前提としている。そして、その拡張作業のベースとなるコンティンジェンシープランは、1-3 節「コンティンジェンシープランの構成」で定義された項目が、過不足なく満足されていなければならない。

本報告書では、拡張作業のベースとなるコンティンジェンシープランが用意できない場合や、用意できていたとしてもその内容が 1-3 節で定義された記載項目を満足していない場合でも、本章の内容を参考にしながら、対サイバーテロ・コンティンジェンシープランの策定作業を進めることができるようにある程度は考慮されている。しかし、更に詳細な解説や具体的な情報を必要とする場合には、本報告書の巻末で紹介している参考文献を別途参照する必要がある。

また、本調査研究では主として大規模プラントの制御システムをその対象としているが、ここで紹介した考え方や策定手順は、そのまま他の汎用的なコンピュータシステムに対し

でも適用することができると考えられる。

図 2-1 に本調査研究で取り扱うプラン策定作業の範囲を示す。

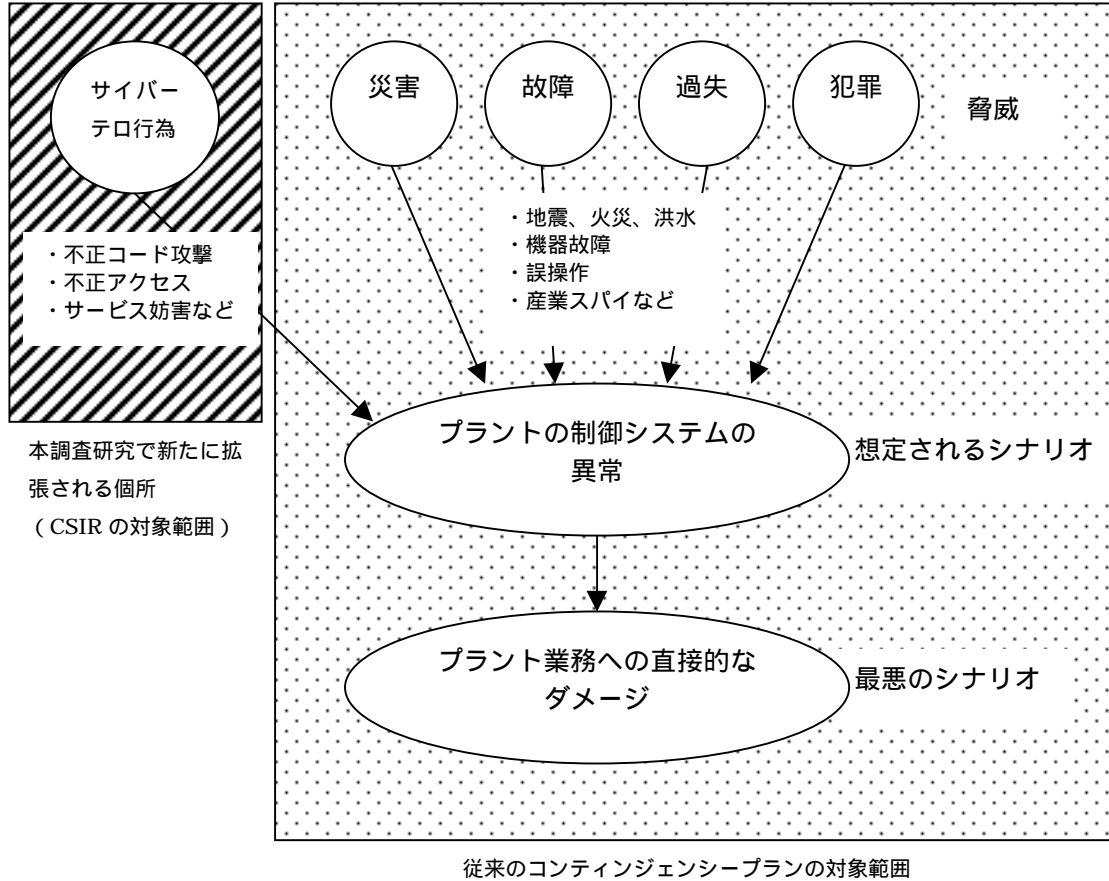


図 2-1 従来のコンティンジェンシープランと CSIR の対象とする範囲

図 2-1 において斜線で示した個所が、本調査研究で拡張される範囲である。特にサイバーテロ行為をはじめとするコンピュータ犯罪を対象としたコンティンジェンシープランは、コンピュータセキュリティインシデントレスポンスプラン (CSIR; Computer Security Incident Response) と呼ばれることがある。

2-3. コンティンジェンシープラン策定手順

図 2-2 にコンティンジェンシープランの策定手順を図示する。プラン策定作業は大きく 3 つのフェーズ、すなわち「プラン策定前の作業」「プラン策定作業」「プラン策定後の作業」に分けることができる。

「プラン策定前の作業」ではコンティンジェンシープランの記述範囲の定義と、プラン策定のための分析作業を行う。「プラン策定作業」では実際にサイバーテロが発生した場合のシナリオを想定し、そのシナリオに応じた対応手順を記述していく。「プラン策定後の作業」では策定したプランを定期的に見直す必要性について述べる。以下、手順の各項目について検討を行う。

2-3-1. コンティンジェンシープラン策定の前に行っておく作業

本節では、まずコンティンジェンシープランの策定に先駆けて行うべき作業について検討を行う。本作業はコンティンジェンシープランの記述対象とその範囲を定義するために必要である。

2-3-1-1. 対象システムの抽出

まずはじめに、当該作業で策定するコンティンジェンシープランで対象とするコンピュータシステムについて、その範囲を明確に定義しなければならない。ネットワーク図を用いて対象範囲を図示するのもよい考えである。また、策定対象以外のシステム上で発生したサイバーテロには対応していない旨の記述も付記しておくといよい。

例)

本コンティンジェンシープランでは、図 2-3 で示した大規模プラント・ネットワークにおけるシステム構成モデルのうち、制御系システムのみ対象とする。同図中に併せて示されている情報系システムは本プランの対象外とする。

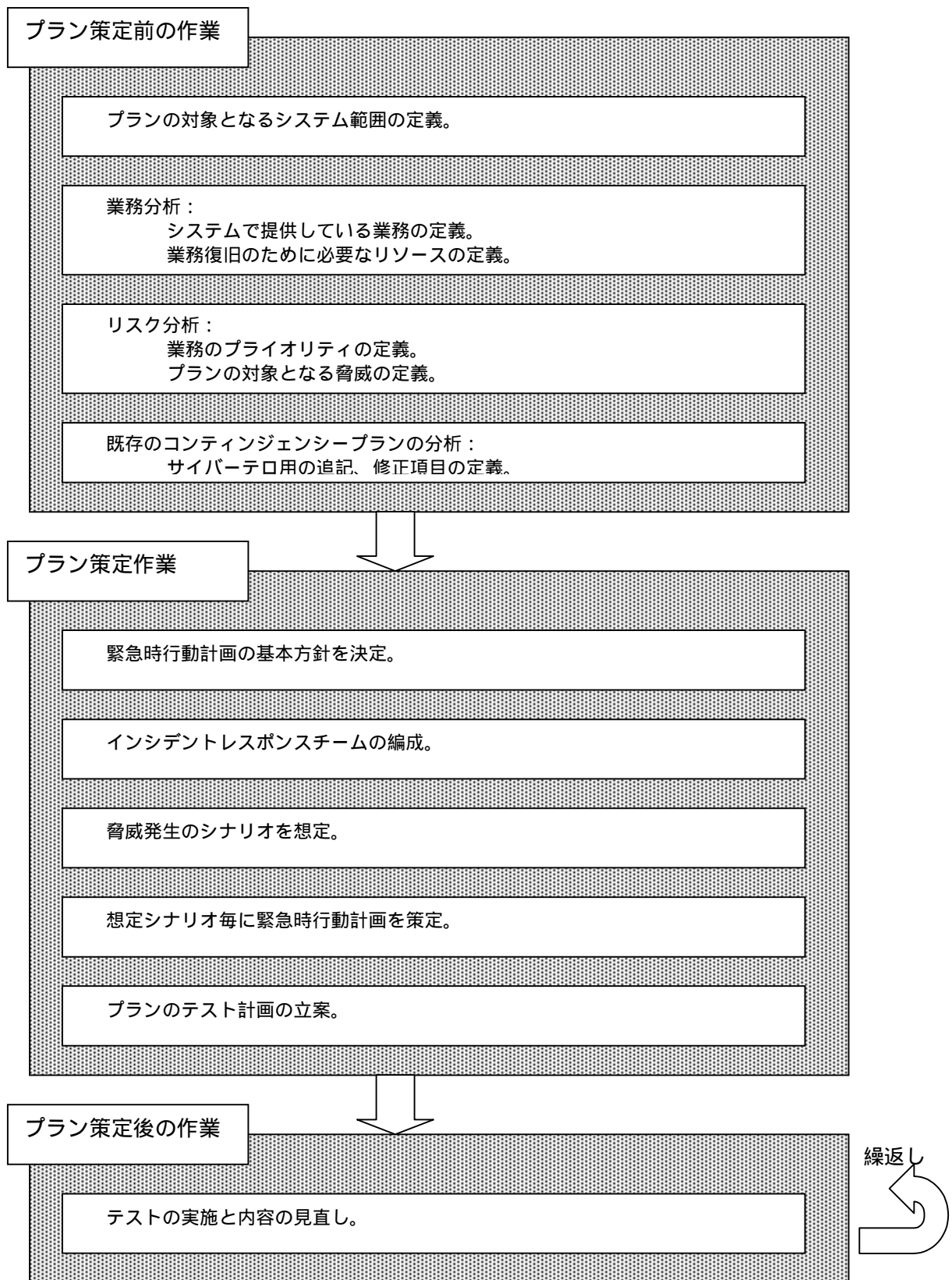


図 2-2 コンティンジェンシープラン策定手順

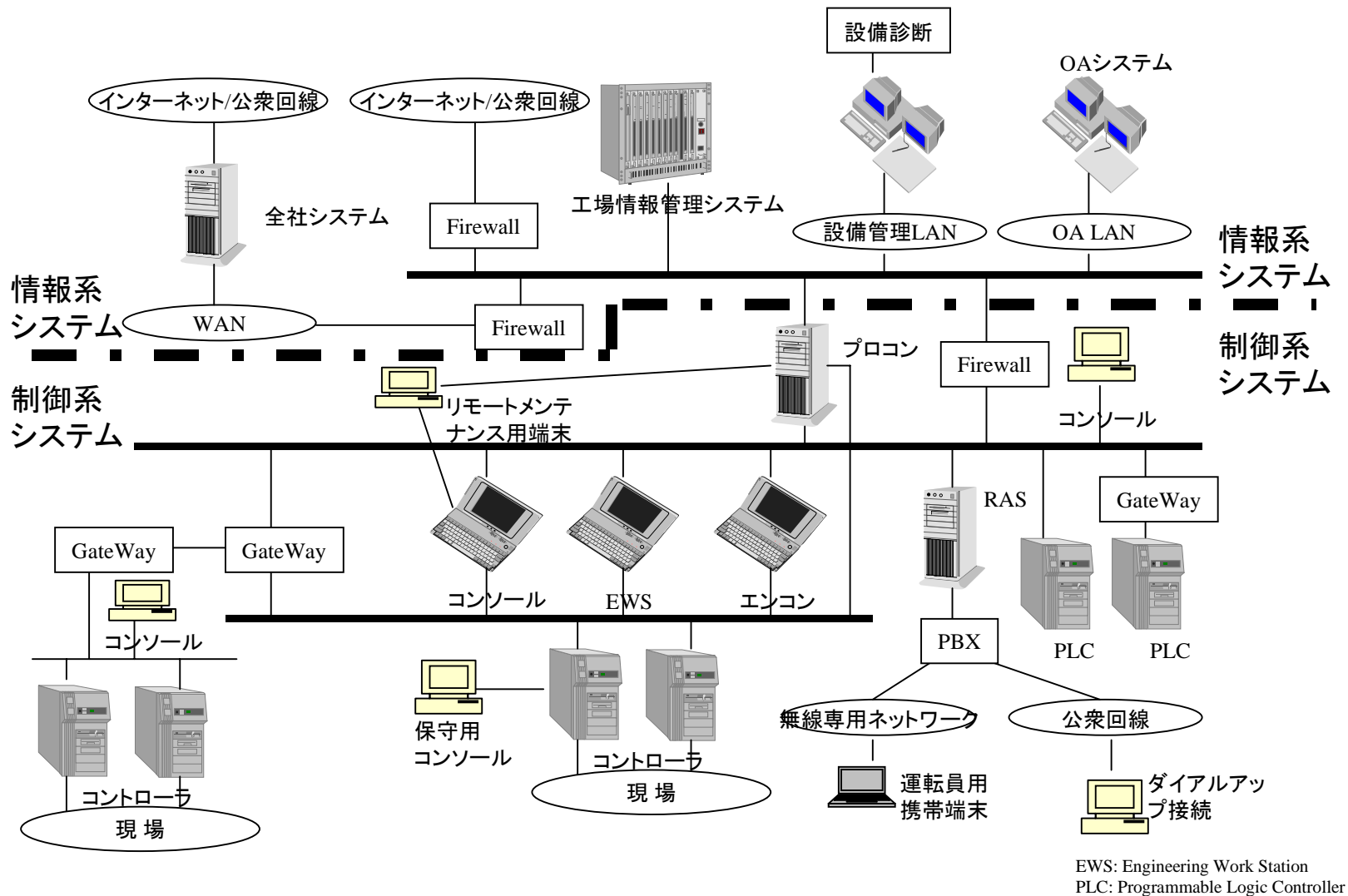


図2-3 大規模プラントネットワークにおけるシステム構成モデル

2-3-1-2. システムの分析

前節の作業において対象とするコンピュータシステムが定義されたら、次はその定義したシステムに対して、業務分析とリスク分析という2種類の分析作業を実施する。

(1) 業務分析

業務分析とは、対象となるシステムを使って提供されている業務を定義し、各業務の処理手順を明らかにする作業である。業務分析作業の結果は、主にコンティンジェンシープランの第2部「継続・復旧のためのリソースの確保」の項目で、各業務に必要なとされるリソースをリストアップする際に使用される。また、コンティンジェンシープランにおいて、実際に保護対象となるのはコンピュータシステム自体ではなく、そのシステムを使って提供されている業務である。従って、業務分析はコンティンジェンシープランにおける保護対象を明らかにするという意味でも重要である。

業務分析の手法に関する検討は、当調査研究の範囲外である。そのため、ここではその作業概要についてのみ触れることとする。

業務の定義

2-3-1-1 節「対象システムの抽出」で定義されたコンピュータシステムで提供されている全業務のリストアップを行う。

本作業では、システムの仕様書、設計書の調査とともに、必要に応じて当該システムを利用している関係部署へのヒアリング作業も要求される。

業務手順の抽出

リストアップされたそれぞれの業務について、その処理手順を洗い出す作業を行う。業務が発生してから終了するまでの一連の過程を、漏れなく具体的に抽出していかなければならない。またその際、当該業務が他の業務とどのような依存関係にあるのかも明らかにしておく。

処理手順を洗い出す作業では、各ステップで当該業務がどのようなリソースを使用しているかについても分析する。ここで、リソースとは1-3-2 節「継続・復旧のためのリソースの確保」で定義された、人的リソース、処理用リソース、アプリケーションとデータリソース、通信リソース、物理的なインフラストラクチャリソース、ドキュメントリソースの6種類である。

本作業では、システムの設計書や組織の資産管理台帳などが役に立つかもしれない。また、必要に応じて当該システムを利用している関係部署へのヒアリング作業も要求される。

必要リソースの最小構成のリストアップ

前段までの作業で、平常業務時に使用されているリソースをリストアップすることができた。しかし、リストアップされたリソースを、そのまま緊急事態の下でも必要とされるリソースとして定義することは現実的ではなく、費用対効果の面から考えても得策ではない。

そこで、次にリストアップされたリソースについてプライオリティの設定を行う。本作業によって、それぞれの業務を継続・復旧させる場合に必要となるリソースの最小構成を定義することができる。ここで、リソースの最小構成を定義する際には、リソースの依存関係に注意をしておく必要がある。

リソースの調達手段の確保

最小構成としてリストアップされたリソースについては、その調達方法についても定義をしておく。この際、自然災害や大規模な事故などを想定したコンティンジェンシープランでは、交通機関や輸送手段が物理的に麻痺してしまったケースも想定しておく必要がある。本調査研究はサイバーテロをその対象としているため当該事項に関しては詳しくは触れない。

また、コンピュータシステムでは、緊急時に調達するリソースは本番環境と全く同じ構成（例えば同一機種、同一オペレーティングシステム、同一アプリケーションなど）であったほうが、継続・復旧作業を容易に行うことができる。しかし、サイバーテロリズムをその脅威として想定している場合には、本番環境と同一構成のバックアップシステムでは、バックアップサイトに業務を切り替えた途端に、また全く同様の手口で再び攻撃を行われる可能性も考慮しなければならない。そのため、緊急時に使用されるバックアップサイトでは、本番環境との互換性を持った別構成のシステムを用意することが本来は理想的であると考えられる。もちろん当項目では経済的な制約を考慮しておかなければならない。

平常業務との差違分析

最後に、各業務の平常時と緊急時での差違についても分析しておかなければならない。場合によっては、通常はシステムで提供している機能を手動で提供することがあるかもしれない。また、緊急時には省略される処理ステップもあるかもしれない。本作業は緊急事態が終息した後に、平常業務へ復帰する際の作業で役に立つ。

(2) リスク分析

コンティンジェンシープランの策定に先駆けて行っておくべき作業の中で、業務分析とともに重要な作業がリスク分析である。

リスク分析とは、対象となるシステムが潜在的に抱えている脅威について定義し、各脅威の発生確率と発生した場合の影響度を見積もる作業である。リスク分析作業の結果は、主にコンティンジェンシープランの第3部「シナリオに基く緊急時の行動計画」の項目で、シナリオを想定する作業の際に使用される。

実際には、業務分析とリスク分析は相互の結果を参考にしながら、その作業を進めることが多いため、両分析は並行作業で実施してもよい。

リスク分析の手法に関する検討は、当調査研究の範囲外である。そのため、ここではその作業概要についてのみ触れることとする。また、「大規模プラントネットワークセキュリティについての中間報告書」では、大規模プラントの制御システムのリスク分析に適した手法として、HAZOP法やFTA法の検証が報告されているので、こちらを参考にしながらリスク分析作業をすすめてもよい。

脅威の定義

当該コンティンジェンシープランで想定している脅威について定義をする。例えば、本調査研究における脅威は次のように定義される。

例)

本コンティンジェンシープランでは、大規模プラント・ネットワークにおけるシステム構成モデルの制御系システムに対して、サイバーテロリズムが発生した場合を想定して作成されている。ここで、サイバーテロリズムとは、

「ネットワークを通じて制御系システムに対して行われる大規模で組織的な敵対行動。」であり、具体的には次の5つの手口を使って引き起こされる。

不正コード攻撃

コンピュータウィルスやトロイの木馬、ワームあるいはパスワードスニッファやログ消去プログラムなどの不正プログラムを使用して行われる攻撃。

不正アクセス

制御システムのユーザアカウントを断り無く奪取、使用しシステムにログインし、さらに上位のユーザ権限を奪取したり、本来アクセス権限のないファイルやディレクトリ、あるいは制御システムで操作している装置などにアクセスし、盗用、改ざん、破壊、不正操作などの行為を行う攻撃。また、同行為は、システムの脆弱な設定やセキュリティホールを利用することによって、ログイン行為が省略できる場合もある。

サービス妨害

制御システムが予期せぬ不正な入力を与えたり、システムに処理能力以上の負荷をかけることによって、制御システムが提供している機能の一部または全部を麻痺させる攻撃。

風説の流布

デマ情報や当組織、あるいは当組織の要員を誹謗中傷した文章などをメールや電子掲示板、ホームページなどを使って流布し、当組織を混乱させたり、当組織のイメージダウンを画策する攻撃。

システム探査

制御システムの構成を探査する攻撃手法。制御システムに対する不正行為の初動や、あるいは不正行為の試みが失敗した痕跡と考えられる。

プライオリティの設定

コンティンジェンシープランで対象とする脅威が定義されたら、次に対象システムで提供されている業務にプライオリティを設定する作業を行う。緊急事態発生時には、本作業で設定されたプライオリティが高い業務から順に継続・復旧作業が行われる。また、このプライオリティの値は、それぞれの業務が停止していることが許容される最大時間枠に基づいて設定されていなければならない。

ここで、各業務に設定されるプライオリティの値は、それぞれの業務が一定期間停止した場合に、組織に与えるダメージ（影響度）の度合いがどの程度のものなのかを見積もった分析結果を元に決定されなければならない。（例えば、ダメージの度合いを金額換算して、許容される損失額で評価する方法などが考えられる。）また、本作業は組織のビジネスプランと密接な関わりを持つため、その決定には経営層の判断を適宜仰ぐ必要もある。

業務プロセスにおける脅威発生確率の分析

前段までの作業で、当該コンティンジェンシープランで対象とする脅威の定義と、保護対象である業務のプライオリティ設定を行うことができた。次に、リスク分析作業では、それぞれの業務プロセスにおいて、どのような脅威がどの程度の確率で発生する可能性があるのかを詳細に洗い出す作業を行う。

本作業では、業務分析の作業「業務手順の抽出」で作成されたそれぞれの業務の処理手順がまとめられた文書と、リスク分析の作業「脅威の定義」で定義された本コンティンジェンシープランで対象とする脅威の定義を利用する。

具体的な作業としては、業務プロセスの各処理ステップで、先に定義したサイバーテロリズムで利用される5つの手口（不正コード攻撃、不正アクセス、サービス妨害、風説の流布、システム探査）が発生する可能性とその確率について検討を行う。システム構成によっては、ある手口の可能性については考慮しなくてもよい場合もあるし、またその逆にある手口についてはその発生が不可避な場合もあるかもしれない。対象業務毎に、想定されるサイバーテロリズムの手口が異なることを認識しておくことは重要である。本作業では、必要に応じて情報セキュリティの専門家の協力を得てもよい。業務関係者を集めて、分析結果のレビューを実施するのもよい考えである。

また、各手口の発生確率は、例えば、その手口を実行する場合の難易度によって評価する方法などが考えられる。例えば、次の表は各手口の実施難易度を元にその発生確率を4段階にレーティングした例である。システム構成や作業手順によって、同一の手口であっても、その発生確率が業務手順の各ステップ毎に異なる可能性があることに注意をしなければならない。

例)

表 2-1. 実施難易度による脅威の発生確率の評価

発生確率 A	誰でも容易にその手口を実行することができる。
発生確率 B	ある程度の知識を持った者がその手口を実行することができる。
発生確率 C	かなりの専門知識を持った者でないとその手口は実行することができない。
発生確率 D	当該処理ステップではその手口が発生する可能性は無い。

2-3-1-3. 既存のコンティンジェンシープランの分析

コンティンジェンシープラン策定の前に行っておくべき作業の最後は、既存のコンティンジェンシープランの分析作業である。本調査研究では、コンティンジェンシープランの策定対象となるコンピュータシステムには、既に何らかの脅威（例えば自然災害や事故など）を想定したコンティンジェンシープランが用意されていることを前提としている。そして、そのベースとなるコンティンジェンシープランをサイバーテロリズム用に拡張することを目的として、そのための手法について検討を行っている。

ここで、対サイバーテロリズムを目的としたコンティンジェンシープランでも、その記述内容の多くは、既に用意されているコンティンジェンシープランと共通に使用できる場合が多い。また、既存のコンティンジェンシープランによって、2-3-1-1 節「対象システムの抽出」や 2-3-2-1 節「システムの分析」で検討してきた事前の準備作業も、実際は大幅に省略化、あるいは簡略化できることが期待される。

そこで、本節では既存のコンティンジェンシープランを分析し、対サイバーテロリズム用に追記、あるいは修正しなければならない記述内容を定義する作業について検討を行う。

これまでの検討により、コンティンジェンシープランは、次の 4 部から構成されていることがわかった。

- 第 1 部 策定対象の定義とプライオリティの設定
- 第 2 部 継続・復旧のためのリソースの確保
- 第 3 部 シナリオに基く緊急時の行動計画
- 第 4 部 運用と見直し

そこで、以下では各部毎にその追記、修正する記述内容について検討を行う。

(1) 「策定対象の定義とプライオリティの設定」の記述項目の検討

第 1 部では、本コンティンジェンシープランで対象とする範囲を明確にするための 3 つの定義、

- 対象とするコンピュータシステムの定義
- コンピュータシステムを利用して提供されている業務の定義
- 対象とする脅威の定義

および、対象業務のプライオリティ設定について記述されている。

ここでは、まず「対象とする脅威の定義」の項目に、リスク分析作業「脅威の定義」（2-3-1-2 節「システムの分析」参照）で決定されたサイバーテロリズムの定義を新たに追記しなければならない。

また、対象業務のプライオリティ設定は、同一システムを対象としている限りは、当該システム上で提供されている業務のプライオリティもまた同一であると考えられる。そこで、大抵の場合は、既存のコンティンジェンシープランで設定されたプライオリティをそのまま流用することができる。対象とするコンピュータシステムや業務の定義に関しても、既存の記述内容がそのまま流用できる。

(2) 「継続・復旧のためのリソースの確保」の記述項目の検討

第2部では、緊急事態の下で業務を継続・復旧させるために最低限必要となるリソースと、その調達方法について記述されている。実際には、1-3-2節「継続・復旧のためのリソースの確保」で定義された6種類のリソースに基き、業務分析作業「必要リソースの最小構成のリストアップ」(2-3-1-2節「システムの分析」参照)で実施された作業結果が記述されている。ここでは、各リソース毎に追記、修正項目の検討を行っていく。

人的リソース

サイバーテロリズムに対応するためには、1-4-3節「サイバーテロリズムの手口の分類」に示した手法に代表される、コンピュータシステムに対する不正行為とその対策に精通したコンピュータセキュリティの専門家チームを編成しなければならない。この、サイバーテロリズムをはじめとするコンピュータシステムのセキュリティに関する問題に対応する専門家チームはIRT、インシデントレスポンスチーム(Incident Response Team)と呼ばれる。

また、自組織でインシデントレスポンスチームの要員を確保できない場合には、外部のIRT組織に協力を要請することもできる。

外部協力機関の例)

JPCERT/CC <http://www.jpccert.or.jp/>

しかし、外部のIRT機関では、即座の対応ができなかったり、組織の機密上、協力を要請できないような場合も考えられるので、特に重要なシステムを擁する組織では、自前でインシデントレスポンスチームを編成できるような手立てを講じておく必要がある。

私設IRTの例)

AFCERT	http://afcert.kelly.af.mil/	米国空軍のIRT
NAVCIRT	http://infosec.nosc.mil/	米国海軍のIRT
HOUSECIRT	http://www.house.gov/ushcert/	米国下院議会のIRT

ここで、サイバーテロの犯人に対して法的手続きを検討する場合には、コンピュータ犯罪に関する法務知識を有する要員(組織の法務部門や顧問弁護士など)も手配しておき、訴訟に向けた証拠集めなどの助言を継続・復旧作業中に適宜仰ぐ必要がある。

最後に、サイバーテロをはじめとするハイテク犯罪は、報道機関に大きく取り上げられる場合が多い。そこで、サイバーテロの被害を受けた事実を外部に公表する必要がある場合には、外部機関(とりわけ報道機関)との対応窓口となる要員(組織の広報部門など)を手配しておかなければならない。

処理用リソース

自然災害や事故などの脅威の場合とは異なり、サイバーテロリズムでは処理用のハードウェアが物理的なダメージを受ける可能性は低い。しかし、サイバーテロの被害を受けた業務が重要な役割を果たしており、業務停止が許されない、あるいはごく僅かしか停止期間が許されないような場合には、バックアップサイトとして、処理用リソースも確保して

おこななければならない。

その際、サイバーテロ特有の問題として、本番環境とバックアップサイトが同一構成であった場合、バックアップサイトも同様の手口でサイバーテロの被害を受けてしまう可能性が考えられる。そこで、可能ならば、バックアップサイトとして用意される処理用リソースは、本番環境と互換性を持つが別構成のリソースであることが望ましい。

アプリケーションとデータリソース

処理用リソースの場合と同様に、アプリケーションとデータリソースに関しても、バックアップサイトで使用されているものが、本番環境と同一構成の場合は、再び本番環境同様の手口でサイバーテロの被害を受ける可能性があるので注意しなければならない。

また、サイバーテロ特有の問題として、例えば不正コード攻撃により、コンピュータシステムにウィルスが蔓延した場合には、本項目の記載内容に従ってバックアップデータが調達されるが、その際、当該バックアップデータはウィルス感染していないことが保証されるような調達手段を確保しておかななければならない。

通信リソース

電子メールや Web は便利な通信手段であるが、サイバーテロの被害を受けた場合には、関係者間の連絡にこの種の通信リソースを使用してはならない。盗聴プログラムが設置されており、こちらの通信内容が全て相手側に伝わってしまっている可能性がある。同様の理由から、構内 PBX を介した内線電話での連絡にも注意が必要である。

しかし、自然災害などとは異なり、公衆電話網が機能していない可能性は低い。そこで、サイバーテロリズム発生時の通信手段には、公衆電話網に直結した電話機を使用した音声通信や FAX 通信を選択しておくのがよい。

物理的なインフラストラクチャリソース

サイバーテロリズムの被害を受けた場合には、インシデントレスポンスチームのメンバーが、被害を受けたシステムが設置されている現場に赴き作業を行うこともある。そのため、対象システムの設置場所には、数人の要員が作業するだけのスペースが要求される。

ドキュメントリソース

サイバーテロ特有のドキュメントリソースとしては、例えば、ウィルス保険や不正アクセス保険などに加入していた場合には、保険証券などそれに関連する書類を用意する必要があるかもしれない。

(3) 「シナリオに基く緊急時の行動計画」の記述項目の検討

第3部では、脅威発生シナリオと、各シナリオにおける緊急時の行動計画について記述されている。実際には、リスク分析作業「業務プロセスにおける脅威発生確率の分析」(2-3-1-2節「システムの分析」参照)の結果をもとに、当該業務で発生する可能性のあるシナリオを想定し、その際の行動手順について策定する作業を行う。

本項目では、新たにサイバーテロ専用のシナリオを想定し、その際の行動計画を立案していく必要がある。

(4) 「運用と見直し」の記述項目の検討

第4部では、コンティンジェンシープランの有効性を維持するために、プラン策定後に継続して行うメンテナンス作業について記述されている。具体的には、テスト計画とテスト時の評価基準、及びプランの更新作業の手続きについて記述されている。

本項目では、サイバーテロ用のテスト計画を新たに立案しておかなければならない。

コンティンジェンシープラン拡張のための追記項目

- (1) 策定対象の定義とプライオリティの設定
 - ・サイバーテロリズムの定義について記述する。
- (2) 継続・復旧のためのリソースの確保
 - ・サイバーテロリズムに対応するための体制について記述する。
 - ・その他の項目は必要に応じて追加、修正を行う。
- (3) シナリオに基く緊急時の行動計画
 - ・サイバーテロリズムの専用シナリオを想定し、その際の行動計画についても記述する。
- (4) 運用と見直し
 - ・サイバーテロリズム用のテスト計画について立案する。

2-3-2. 対サイバーテロ・コンティンジェンシープランの策定

2-3-1-3 節「既存のコンティンジェンシープランの分析」の作業により、ベースとなるコンティンジェンシープランを、対サイバーテロ用に拡張するための追記項目を明らかにすることができた。そこで、本節ではこの結果を受けて、前節で定義された追記項目を実際にコンティンジェンシープランに反映させていく方法について検討を行う。

2-3-2-1. 基本方針の策定

既存のコンティンジェンシープランをサイバーテロ用に拡張する作業に際し、まず始めに決定しなければならない事柄が基本方針である。基本方針とは緊急時の行動計画を策定する上での基本的な方向性を示すものであり、サイバーテロをその脅威に想定した場合には、次の2つの方針のうちいずれかを選択するのがよいと考えられる。

アクセス拒否と問題解決

犯人探しや証拠集めなどは行わず事態の収集を優先する作業方針。

経過の観察と情報収集

後々の法的手続きや犯人逮捕のために犯人追跡や証拠集めを優先する作業方針。

基本方針の選択基準であるが、例えば被害が深刻で一刻の猶予も得られないようなシナリオでは「アクセス拒否と問題解決」を選択するのが常識的な選択であろうし、逆にシステム探査やサービス妨害など、実被害が無かったり、あるいはその影響が軽微なシナリオでは、攻撃相手を特定するために「経過の観察と情報収集」を選択する場合も十分に考えられるであろう。

以下に2つの基本方針についてその詳細を示す。

基本方針（1）アクセス拒否と問題解決

当該基本方針は、可能な限り早く問題を解決し、平常業務に復帰することを最大目的とした簡潔な基本方針である。

具体的には、まず作業の第1フェーズとして、サイバーテロの被害を受けた業務へのアクセスを拒否する。アクセス拒否の方法としては、

- ・システム全体をネットワークから切り離して、そのシステム上で提供されている全ての業務を停止させてしまう方法と、
- ・ルータやファイアウォールのフィルタリング機能を利用して、攻撃者のIPアドレスのみアクセスを拒否する方法

が考えられる。どちらの方法を選択するかは、当該システムのバックアップサイトの有無や、当該業務のプライオリティ、更には発生したサイバーテロ行為の種類や、受けたダメージの度合いなどを判断材料としてその都度異なってくる。そして、いずれの方法を選択するにしても、それぞれ長所と短所が存在するので、各サイトの事情を加味しながら決定する必要がある。

第1フェーズでアクセス拒否を実現したら、第2フェーズでは問題解決のための作業を行う。サイバーテロリズムの原因となった手口の究明、およびその原因の除去、バックアップデータによるダメージの復元など、然るべき対策の実施を行った後に平常業務へと復帰する。

基本方針（2）経過の観察と情報収集

2番目の基本方針では、コンピュータセキュリティに関するより高度な知識と技術が要求される。

例えば、告訴や逮捕を検討しなければならないような被害を受け、その結果、当該組織で犯人を究明することを決定した場合には、最初の基本方針ではそのための十分な証拠を揃えることができない可能性が高い。

そこで、犯人逮捕や告訴のために十分な情報や証拠を収集するには、サイバーテロ行為を続行させて、その経過を観察する必要がある。この際、業務へのダメージを最小限に抑えるために、巧みにアクセス制限をはじめとするセキュリティ対策を実施しなければなら

ない。更に気を付けなければいけないのは、犯人にこちらの行動を気付かれてはいけないということである。そのため、コンピュータセキュリティに関する高度なスキルを擁する要員が確保されないと、選択することが不可能な方針である。もちろん、サイバーテロによる被害が甚大で、経過観察期間を設けることができない場合なども、当基本方針を選択することは難しい。

2-3-2-2. 組織・体制の整備

基本方針を決定したら、いよいよプランの具体的な拡張作業に入る。2-3-1-3 節「既存のコンティンジェンシープランの分析」では具体的な拡張項目について検討を行った（P33 枠内参照）。その内、「策定対象とプライオリティの設定」の項目で記述するサイバーテロリズムの定義については、既に 1-4 節で検討したのでここでは取り扱わない。

そこで本節では、まず「継続・復旧のためのリソースの確保」の項目をサイバーテロ用に拡張するための手法について検討を行う。

(1) インシデントレスポンスチームの編成

サイバーテロリズムに対応するために、コンピュータセキュリティの専門チームである IRT、インシデントレスポンスチーム(Incident Response Team)を編成する。ここで、インシデントレスポンスチームには次の 2 つの機能が要求される。

対応策の決定機能

サイバーテロ発生時には、その場の状況に応じて対応方法を即座に決定していく必要がある。例えば、前節の 2 つの基本方針のうち、どちらを採用するのかといった決定もこの種の判断の 1 つである。また、場合によっては組織の重要な業務を停止させるといった判断を下さなければならないこともある。インシデントレスポンスチームには、このように組織の事業活動に関連するような重要な決定を即座に迫られる場面が度々ある。

そこで、組織全体の活動にかかわる重要な判断を下す権限を持った経営陣が、インシデントレスポンスチームのメンバーとして選抜されているとよい。例えば、CIO(Chief Information Officer、情報システム担当役員)や CSO(Chief Security Officer、情報セキュリティ担当役員)などの役職に相当する経営陣を、インシデントレスポンスチームのトップとして任命しておくことはよい考えである。

現場での作業機能

インシデントレスポンスチームには、前出の「対応策の決定機能」によって決定された方針に基づき、サイバーテロが発生した現場で作業を行う実施チームも必要である。この作業実施チームは、当該システムのシステム管理者、及びサイバーテロへの対応に関する専門的なスキルを持ったセキュリティ技術者で編成されることが望ましい。コンピュータシステムの規模にもよるが、通常この作業実施チームは数人規模で構成される。

サイバーテロに対応するために、コンティンジェンシープラン第 2 部「継続・復旧のためのリソースの確保」の項目では、以上 2 つの機能を備えたインシデントレスポンスチームの編成について記述しておく。

ここで、策定対象のコンピュータシステムが大規模で、物理的なロケーションが世界各地に点在しているような場合には、サイバーテロに即座に対応するために、それぞれのサイトでインシデントレスポンスチームを編成しておいたほうがよい。

(2) インシデントレスポンスチームへの連絡方法

インシデントレスポンスチームの招集

インシデントレスポンスチームのメンバーとは、24 時間連絡可能な手段を用意しておかなければならない。例えば、仕事場と家の電話番号、そのどちらにもいない場合に連絡のつく場所の電話番号、ポケットベルや携帯電話の番号など、各メンバーの一連の連絡手段が記述された連絡リストの作成は必須である。また、個別に連絡を取っている時間を省略するために、例えばボイスメールボックスなどを利用して、関係者全員に一斉に情報発信できる手段を用意しておくのもよい考えである。

また、このリストとは別に、組織の重要人物と連絡をとるための連絡リスト（例えば、組織の経営陣と各部門の責任者リストなど）も作成しておく。通常、この種のリストは、既にベースとなるコンティンジェンシープランの方で用意されているはずである。また、サイバーテロが発生した場合に協力を要請したり、アドバイスを受けたりする外部協力機関の連絡先も連絡リストとして整備しておくもよい。

そして、これらの連絡リストは、電子データとしてだけでなく、例えばクリアファイルやルーズリーフなどに整理されてオフラインでも保管されており、咄嗟の場合に即時に閲覧できるようにしておかなければならない。インシデントレスポンスチームのメンバーはこれらの連絡リストを常時携帯しておくのもよい。

サイバーテロ対応作業中の通信手段

サイバーテロへの対応作業中のインシデントレスポンスチームとの連絡窓口は一元化されていなければならない。この際、コンピュータシステムや PBX は既に攻撃を受けている可能性があるため、その連絡手段には PBX を通さず直接外部と接続された電話線を用意しておく。もしくは、PGP や SSL などの暗号通信機能を利用してもよい。

インシデントレスポンスチームへの連絡手段

サイバーテロリズムの被害を受けたことは、コンピュータシステムのユーザや管理者からの報告によって発覚する場合も多い。そこで、システムに何か異常を感じた場合に、インシデントレスポンスチームへ連絡を取るための窓口を用意しておかなければならない。例えば、インシデントレスポンスチームの Web サーバを用意したり、ヘルプデスクなどを開設しておくこともよい。

(3) 広報部門、法務部門との連携

サイバーテロ行為を行った犯人に対して、法的手続きを行使する場合には、その対応作業中から慎重な証拠集めを行わなければならない。そこで、その場合には組織の法務部門

やあるいは顧問弁護士に協力を依頼し、証拠集めに関して助言を受けたり、証拠品（多くの場合はシステムのログ）の証人になってもらうなどの連携が必要とされる。

また、サイバーテロ行為は報道機関で大きく取り上げられる傾向にある。そこで、もしサイバーテロの被害を受けた事実を外部に公表する必要がある場合には、組織の広報部門、および法務部門と連携して、その対応方法を検討するとともに、正しい情報が外部に公表されるように窓口を広報部門に一元化しておかなければならない。サイバーテロ被害の外部公表先としては報道機関の他に取引先企業や顧客などが考えられる。

このように、サイバーテロリズムの対応作業中に広報部門や法務部門と連携する必要がある場合には、事前にその際の対応方法について検討を行っておくのも重要である。

2-3-2-3. 回復マニュアルの策定

「継続・復旧のためのリソースの確保」の項目を拡張したら、次に本節では、「シナリオに基く緊急時の行動計画」を対サイバーテロリズム用に拡張するための手法について検討を行う。（P33 枠内参照）

（１）シナリオの想定

本項目では、まずはじめに対象システムに対して脅威発生シナリオを想定し、次にそれぞれのシナリオに応じて緊急時の行動計画を策定していく。もちろん、起こり得る全ての可能性を事前にシナリオとして定義しておき、またその際の行動手順を策定しておくことは不可能であるが、事前に発生する可能性がありそうなシナリオを用意しておき、来るべき時に備えておくことには意味がある。

ここで、効果的なシナリオを想定するためには、2-3-1-2 節「システムの分析」で実施されたリスク分析の結果を用いる。通常、リスク分析の結果は「脅威が発生した場合の影響度」と「脅威の発生確率」の２つの指標で評価される。

そこで、まずはじめに「脅威の発生確率」の評価指標を用いて、各業務毎に発生する可能性がありそうな脅威を抽出し、またその脅威が複合的に発生する可能性（脅威の組み合わせ）について検討を行う。

そして次に、「脅威が発生した場合の影響度」の評価指標を用いて、前段の作業で抽出した脅威及びその組み合わせを評価し、当該脅威が発生してもその影響が軽微だと判断された場合は、コンティンジェンシープランのシナリオの対象から除外する。影響が軽微な脅威に関しては、コンティンジェンシープランではなく、平常業務時に使用されるオペレーションマニュアルや運用マニュアルで取り扱われるべきである。

同様に、その影響範囲や影響度があまりにも大きく、すぐには継続・復旧作業に取り掛かれないような脅威についても、コンティンジェンシープランからは除外する。そのような広範囲に渡る重大な脅威を想定したコンティンジェンシープランの作成は、困難であり現実的ではないからである。

（２）緊急時行動計画における５つの行動フェーズ

前段の作業により、脅威発生シナリオが想定されたら、次に各シナリオに応じた緊急

時の行動計画について策定する。ここで、緊急時行動計画は次の 3 つの行動フェーズから構成されることは、既に 1-3-3-2 節「緊急時行動計画の策定」で述べた。

緊急時対応フェーズ
バックアップフェーズ
継続・復旧フェーズ

しかし、特にサイバーテロリズムをはじめとするコンピュータセキュリティに関する非常事態に対処するための行動計画では、先述の 3 つの行動フェーズをより細分化した次の 5 つの行動フェーズでその計画が立案されていることが多い。

確認フェーズ

現状を正確に把握し、今回のサイバーテロリズムの概要を明らかにするための行動計画について記述されたフェーズ。

抑制フェーズ

サイバーテロリズムによるこれ以上の被害を最小限に抑制するための行動計画について記述されたフェーズ。

排除フェーズ

サイバーテロリズムが発生した原因を究明し、その原因を排除するための行動計画について記述されたフェーズ。

回復フェーズ

サイバーテロリズムによるダメージを修復し、コンピュータシステム、及び業務を通常状態に回復するための行動計画について記述されたフェーズ。

フォローアップフェーズ

サイバーテロリズム発生に伴う緊急事態が一通り終息した後で、今回の一連の対応状況を分析することによって、組織のセキュリティ対策強化のためのフィードバックを行うための行動計画について記述されたフェーズ。

そこで、本調査研究においても上記 5 つの行動フェーズに倣って、その行動計画を策定することとする。

図 2-3 に、緊急時行動計画における各行動フェーズの対応関係について示す。

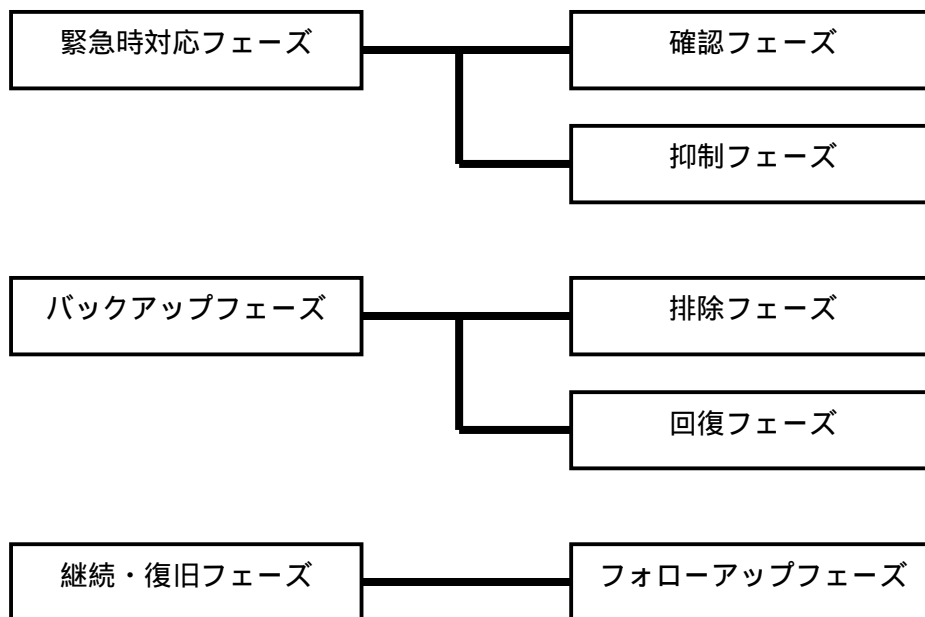


図 2-3 各フェーズの対応関係

2-3-2-4 節では、各フェーズの具体的な行動計画について例示、解説を行っている。利用者は 2-3-2-4 節で示された行動計画の内、各々の状況に該当するものを適宜選択、編集し、緊急時の行動計画の策定作業に利用することができる。

2-3-2-4. 緊急時行動計画の具体例

本節では、「シナリオに基く緊急時の行動計画」の項目に記述される行動計画について、その具体例を示す。利用者は、本節で示された行動計画の具体例から各々の状況に適合する例文を適宜選択、編集し、プラン策定作業に利用することができる。

(1) 確認フェーズにおける行動計画

サイバーテロが発生した場合、まず確認フェーズによって現在の状況を正確に把握しなければならない。具体的には、次のような行動計画が考えられる。

行動計画 1-1 今回のサイバーテロ対応の責任者を任命する。

緊急事態の下では、情報が錯綜したり、誤まって伝達されたりする場合も多い。そこで、連絡窓口、情報管理、指示系統を一元化するために、まずはじめに今回のサイバーテロ事件に対応する責任者を任命しなければならない。2-3-2-2 節「組織・体制の整備」で検討したインシデントレスポンスチームのメンバーの中で、対応策を決定する経営陣の中から責任者として任命されることが適当である。

行動計画 1-2 本当にサイバーテロかどうかを確認する。

サイバーテロリズムをはじめとするコンピュータセキュリティ関係の事件は、ユーザや各部門のシステム管理者からの連絡で発覚する場合が多い。しかし、同時に通報者はコンピュータセキュリティの専門家ではないので誤認識をしていることも考えられる。実際、その原因を調べてみると、システムの設定ミスやアプリケーションのエラーである場合も多い。そこで、まずはじめに今回の事態が本当にサイバーテロ行為によるものなのかどうかについて確認を行ったほうがよい。ここで、責任者は先行調査のための作業要員を現場に派遣することになる。

行動計画 1-3 証拠を慎重に集める。

調査の結果、サイバーテロが発生していることが確認されたら、次にその実態の概要を把握するための作業を行う。サイバーテロの実態を解明するためには、ログをはじめとした証拠の収集を行わなければならない。ここで、責任者は証拠収集作業のために新たに応援要員を現場に派遣してもよい。

行動計画 1-4 組織の法務部門や顧問弁護士へ協力を依頼する。

ここで、サイバーテロの犯人に対して逮捕や訴訟を検討している場合には、証拠の収集方法やその取扱いを特に慎重に行う必要がある。サイバーテロ事件では、その主たる証拠品はシステムに残されたログである。しかし、ログは電子データであるために容易に作成、改ざんが可能であり、その存在だけでは証拠性に乏しい場合も多い。そこで、本作業で収集されたログは、確かにその時点で集められたもので、証拠物件として有効であることを証明するために、サイバーテロに詳しい法務関係者の協力を得て、収集したログの証

抛物件としての正当性を証明してもらう必要がある。

例えば、ログの収集作業をビデオカメラで録画したり、収集したログは第三者の裏書きを行って保存するなどの助言を得ることができる。

行動計画 1-5 プロバイダーへの協力を依頼する。

巧妙な侵入者になるとログを消去してしまう場合も多く、犯人検逮捕のための十分な証拠が当該コンピュータシステム上には既に残されていない場合も多い。そこで、組織が契約しているプロバイダーに証拠となるログの収集作業の協力を依頼することも考えられる。

行動計画 1-6 関係者全員と連絡をとる。

2-3-2-2 節「組織・体制の整備」で準備された連絡リストを用いて、組織のコンピュータシステムに対して、サイバーテロが発生した事実を関係者に連絡する。

行動計画 1-7 確認フェーズレポートを作成する。

確認フェーズで収集した情報、実施した作業とその結果を作業レポートとして文書にまとめておく。

(2) 抑制フェーズにおける行動計画

確認フェーズの作業によってサイバーテロの概要が判明し、組織としての対応体制を整えることができたら、抑制フェーズへと作業を移行させる。抑制フェーズでは確認フェーズでの調査結果をもとに、サイバーテロの実態を明らかにするためにより綿密な調査を実施するとともに、サイバーテロによるこれ以上の被害の拡大を防止するための手立てを実施する。

行動計画 2-1 現場に作業チームを配置する。

確認フェーズの調査結果の報告を受けて、責任者は現場に作業チームを派遣する。作業チームは多くとも 4~5 人編成程度までが適当だと考えられる。ここで、この後現場で実施する作業では、システムの特権ユーザのアカウントを必要とする場合がある。しかし緊急時に、必ずしも特権ユーザのパスワードを管理している要員（通常は当該システムの管理者）と連絡が取れるとは限らない。そこで、各システムの特権ユーザのパスワードだけは、オフラインで保存されており、緊急時にはインシデントレスポンスチームのメンバーが利用できるようにしておく必要がある。

行動計画 2-2 確認フェーズレポートを検証する。

もし作業チームのメンバーと確認フェーズの作業を実施したメンバーが異なる場合は、もう一度確認フェーズで作成されたレポートを検証しておくといよい。

行動計画 2-3 不用意な追跡を行わない。

例えば、アクセスログなどを調査している過程で、不審な IP アドレスを発見しても、その IP アドレスに対して、不用意に ping や traceroute を実行したり、また DNS レコードを検索したり、telnet などアクセスを試みてはならない。このような行為の結果、相手にこちらの動きを察知され、証拠の隠滅を行われる可能性がある。

行動計画 2-4 不用意なシステム設定の変更を行わない。

十分な証拠が集まるまでは、例えば、ルータのフィルタリングルールを設定を変更したり、ネットワークサービスを停止したりするような不用意なシステム変更を行ってはならない。このようなシステム設定の変更は相手に不審感を抱かせることになる。

行動計画 2-5 トラップを仕掛ける。

より有効な証拠集めを行うために、トラッププログラムなどを仕掛けておいてもよい。(トラッププログラムについては付録 A を参照。)

行動計画 2-6 被害を受けたコンピュータ上のバイナリプログラムには注意する。

侵入者は不正アクセスに成功したホストに、よくトロイの木馬プログラムやスニッファプログラムを設置することが知られている。そのため、侵入を受けた可能性のあるコンピュータシステムには、不用意に特権ユーザ権限でログインしたり、またそのシステム上でコマンドを実行するような行為はなるべく避けなければならない。

インシデントレスポンスチームのメンバーは、サイバーテロ対応作業時に使用するような重要なコマンドは、リムーバブルメディアにバックアップを取っておき、随時持参するようにしておくことはよい考えである。また、事前に当該システム上のファイルに対してハッシュ値を計算しておき、必要に応じて適宜そのインティグリティを保証するようにしておくこともよい考えである。

行動計画 2-7 コンピュータシステムのフルバックアップを作成する。

サイバーテロの被害を受けたコンピュータシステムは、未使用のメディアにフルバックアップを作成しておかなければならない。これには、サイバーテロによる被害状況を証拠として保存しておくことと、システムの復旧作業の際に、作業結果を確認するための比較対象として利用することの 2 つの目的がある。そのため、可能ならばフルバックアップは 2 部作成しておくことが望ましい。ここで、未使用のメディアを用いてフルバックアップを作成するのはその証拠性を確保するためである。

行動計画 2-8 システムの切断ポイントを決定する。

抑制フェーズでは、サイバーテロによるこれ以上の被害を防止するために、ダメージを受けたコンピュータシステムをネットワークから切り離さなければならない。ここで、システムを切断するポイントを決定する際には、これまでの作業で収集されたログやその他の情報を利用することができる。例えば、ログを分析した結果、攻撃が外部から行われて

いた場合には、システムをインターネットとの接続点から分離することを検討しなければならない。また、ログを分析した結果、攻撃が内部から行われていた場合には、該当するサブネットからシステムを切り離すことを検討しなければならない。

ここで、システムを切り離すポイントによって影響を受ける業務の範囲が異なってくるので、切断ポイントの判断は慎重に行わなければならない。また、各業務の停止許容期間は、コンティンジェンシープラン第 1 部「策定対象の定義とプライオリティの設定」の欄で明確に定義されているため、切断の実施時期や切断後の対応についても配慮しておく必要がある。例えば、システム切断後に業務をバックアップサイトに切り替えて継続させるような場合や、システムを使用せずに手動で業務を継続させるような場合には、切断後の業務継続体制の準備が既に整っているかどうかを確認しておかなければならない。

行動計画 2-9 他のシステムへの影響を調査する。

ここで、サイバーテロのダメージが及んだ影響範囲を再確認するために、切断されるシステムと同じセグメントに設置されているコンピュータや、切断対象のシステムと定常的に接続のあったシステムを対象に、サイバーテロの被害を受けていないかどうかを確認しておく。この際、各システムの依存関係を把握するために 2-3-1-2 節「システムの分析」で実施された業務分析の結果が役に立つ。

行動計画 2-10 影響のある関係者へ通知する。

システムの切断によってその影響を被る利用者が発生する。また、システムの切断によって一時的にその業務機能が停止、縮小する場合もある。業務機能の停止や縮小は、程度の差こそあれ組織の事業活動に影響を及ぼす重大な事態である。そのため、システム切断によって影響を受ける利用者、及び組織の経営陣に対して業務が停止することについて事前に説明をしておかなければならない。

行動計画 2-11 被害を受けたシステムのパスワードを変更する。

システムの特権ユーザのパスワードは、侵入者にとって最も価値のあるリソースであり、まずはじめに不正利用の標的とされるものでもある。そのため、サイバーテロの被害を受けたシステムのパスワードは、念のため特権ユーザ以外のユーザのパスワードも全て変更したほうがよい。また、特にパスワードスニッファプログラムが検出されたり、検出はされなかったが様々な状況証拠からパスワードスニッファプログラムが設置されていた可能性が否定できないような場合には、被害を受けたシステムが接続されていたネットワーク上の全てのコンピュータのパスワードを変更しなければならない。

行動計画 2-12 抑制フェーズレポートを作成する。

抑制フェーズで収集した情報、実施した作業とその結果を作業レポートとして文書にまとめておく。

(3) 排除フェーズにおける行動計画

抑制フェーズまでの作業により、サイバーテロによる影響範囲を明確に定義することができ、これ以上の被害の拡大を防止するための措置として、ダメージを受けたシステムをネットワークから切断することができた。また、法的手続きのための十分な証拠も既に確保することができているはずである。

排除フェーズにおける作業は、サイバーテロの原因とそのプロセスを究明し、原因となった弱点を除去することと、システムに適切なセキュリティ機能を導入し、システム全体のセキュリティ強度の強化を図ることの2つを目的としている。

また、本行動計画フェーズと次行動計画フェーズで実施される作業には、コンティンジェンシープラン第1部「策定対象の定義とプライオリティの設定」の欄で、その作業期間があらかじめ設定されている。そのため、期間内に作業を完遂させるために用意周到な行動計画を作成しておくことが必要である。

行動計画 3-1 サイバーテロが行われたプロセスを明らかにする。

確認フェーズと抑制フェーズで収集されたログをはじめとする様々な証拠を元に、今回のサイバーテロがどのように実施されたのかについて、その原因とプロセスを究明する。ここで、もし有力な証拠が収集できなかったために、一意にその原因を定義することができなかった場合には、考えられる複数の候補を列挙しておいてもよい。

行動計画 3-2 疑似攻撃を行う。

サイバーテロの原因を究明するための方法として、検査ツールを用いてシステムに疑似攻撃を行ってもよい。検査ツールではシステムの設定ミスや脆弱な設定、あるいはセキュリティホールを発見することができる。(検査ツールについては付録Bを参照。)

行動計画 3-3 サイバーテロの原因を排除する。

ログの検証作業や疑似攻撃により明らかにされたシステムの脆弱性を除去する。具体的な除去作業の方法は、発生したサイバーテロで利用された手口の種類によって異なる。各手口に合った除去作業の方法については本節(6)以降で述べる。

行動計画 3-4 脆弱性分析作業の結果を他のシステムにも反映する。

ログの検証作業や疑似攻撃といった脆弱性分析の結果が、今回はサイバーテロの被害を受けなかった組織内の他のシステムにも該当することが判明した場合には、そちらのシステムに対しても併せて対策を実施しておく。例えば、組織内の他のコンピュータがダメージを受けたシステムと同じバージョンのソフトウェアを使用していたり、同様の設定を行っているケースは十分考えられる。

行動計画 3-5 最新でクリーンなバックアップデータを探す。

サイバーテロの原因を排除できたら、次はバックアップデータを使用してシステムを元の状態に復旧させる作業を行う。ここで、本作業で使用されるバックアップデータは、そ

の内容が最新であること、そしてサイバーテロの被害を受けていないクリーンな状態のものであることが保証されていなければならない。

仮に、長期間断続的にサイバーテロの被害を受け続けていた場合や、その被害が広範囲に及びダメージを受けた個所が明確に特定できないような場合には、バックアップデータからの復旧を諦め、システム全体を再インストールしなければならないこともある。

行動計画 3-6 適切なセキュリティ機能を導入する。

サイバーテロのプロセスを分析した結果、システムの設計上セキュリティ的に脆弱な機能や処理が発見された場合には、適切なセキュリティ機能を導入し、該当個所のセキュリティ強度の向上を行わなければならない。例えばファイアウォールや暗号化ツールなどを導入したり、OS を変更したり、またシステムで提供していた機能自体を変更する場合も考えられる。(現在、一般的に使用されているセキュリティ機能については付録 C を参照。)

行動計画 3-7 排除フェーズレポートを作成する。

排除フェーズで実施した作業とその結果を作業レポートとして文書にまとめておく。

(4) 回復フェーズにおける行動計画

回復フェーズでは、バックアップデータを用いてダメージを受けた個所を修復し、システムを元の状態に復旧させ、組織を平常業務に復旧するための行動計画を策定する。

行動計画 4-1 システムをバックアップデータから復元する。

行動計画 3-5 で用意されたバックアップデータを用いてシステムを復元する。また、場合によっては、初期バックアップデータを用いたシステムの再インストールが選択されることもある。

ここで、バックアップ作業の対象としてはソフトウェアとデータが考えられるが、特にソフトウェアをバックアップ作業の対象とする場合には、行動計画 3-3 で実施した作業結果までもが上書きされて、元の弱点を含んだ状態に戻ってしまわないように注意しなければならない。例えば、設定変更をした設定ファイルまでもがバックアップ作業によって上書きされないよう注意しなければならない。

行動計画 4-2 システムテストによって作業結果を確認する。

行動計画 4-1 の作業が終了すると、システムは既に通常状態に回復しているはずである。そこで、これまでの作業結果を確認するためにシステムの動作テストを行う。これは、排除フェーズで導入された新しいセキュリティ機能や、セキュリティホールを修正するために適用されたセキュリティパッチが原因となり、システムが正常に動作しなかったり、システムの使用方法が以前とは異なっている場合が考えられるからである。そこで、最後にシステムの動作テストを行い、システムが正常に動作するかどうかを確認しておかなければならない。システムテストでは、必要に応じてユーザに参加を要請するのもよい考えである。

行動計画 4-3 業務回復を関係者に通知する。

サイバーテロの対応作業が終了し、システムテストの結果が良好であった場合には、平常業務に復帰することを関係者に連絡する。

行動計画 4-4 稼働後のシステム監視を実行する。

システムが復旧し平常業務に戻った後も、しばらくの間はシステムの監視を実施しておいたほうがよい。本作業は、仮にトロイの木馬や裏口などを排除し損なっていた場合のフォローと、再びテロリストがサイバーテロを仕掛けてきた場合の予防線を張っておくことをその目的としている。

行動計画 4-5 回復フェーズレポートを作成する。

回復フェーズで実施した作業とその結果を作業レポートとして文書にまとめておく。

(5) フォローアップフェーズにおける行動計画

サイバーテロへの対応作業が一通り終息した後で、今回の一連の対応状況を検討し、検討結果を元に緊急時の行動計画を改善する作業を行う。

行動計画 5-1 一連の対応作業をまとめた報告書を作成する。

サイバーテロへの対応作業が一通り終息したら、あまり間を置かずに、今回実施した対応作業をまとめた報告書の作成にとりかかるとよい。本作業では、各フェーズ毎に作成しておいた作業レポートが役に立つ。また、単に事実関係を羅列するだけでなく、対応作業中に気付いた問題点に基く改善提案書の性質も備えた報告書であることが望ましい。

行動計画 5-2 報告書のレビューを行う。

作成した報告書は関係者の間で回覧し、その内容について合意を得ておくことよい。また、関係者全員を集めたミーティングを開催し、報告書で提案された組織のセキュリティ対策の改良点やその実施方法について検討を行うのもよい方法である。

行動計画 5-3 改善提案を実現する。

報告書及び関係者のミーティングでまとめられた改善提案は、早期に実現されなければならない。改善提案を実現するためには、組織の各部門と適宜連携を行っていく必要があるかもしれない。

(6) 不正コード攻撃に応じた行動計画

サイバーテロへの対応方法は、実際には各サイバーテロで利用された手口によって異なるものである。特に排除フェーズではその手口に応じた対応方法の違いが顕著に現れる。そこで、以下ではそれぞれのサイバーテロの手口別にそれぞれ実施される行動計画に関して検討を行う。

不正コード攻撃とは、コンピュータウイルスやトロイの木馬、ワーム、あるいはテロリストがシステムに対する不正行為の際に利用するパスワードスニッファやログ消去プログラムなどの不正スクリプト全般を利用した攻撃のことを指す。ここで通常、不正コードはその検出が困難になるように設計、設置されていることが多い。

行動計画 6-1 ウィルスチェックを行う。

不正コードの中で、最も一般的なものはコンピュータウイルスである。そこで、ウィルスの被害を受けた可能性がある場合には、ウイルス検出ツールを使用して、ウイルス感染しているファイルを検出しなければならない。また、ウイルス検出ツールが使用するウイルスデータベースは、ベンダーが提供している最新のバージョンのものを使用しなければならない。ここで、コンピュータウイルスのタイプによっては、ウイルス感染したファイルやプログラムからウイルス本体だけを駆除することが不可能な種類もある。そこで、ウイルス対策の基本は、ウイルスに感染したファイルは全てファイルごと削除し、バックアップデータから該当ファイルを復元することである。また、最近のウイルス検出ツールでは、コンピュータウイルスばかりでなくワームやトロイの木馬、あるいは不正スクリプトまでもその検出対象としているものが多い。

行動計画 6-2 システムから発信されるパケットを監視する。

トロイの木馬やバックドアなどのプログラムを検出するためには、当該システムによって送受信されているパケットを監視しておき、心当たりの無い不審な通信パケットがシステムから発信されていないかどうかを調査する方法が考えられる。特に、こうした不審な通信パケットはシステムを起動する時に観察される場合が多い。

(7) 不正アクセスに応じた行動計画

不正アクセスとは、何らかの手段を用いてシステムにアクセスし、当該システムの特権ユーザ権限を奪取したり、本来アクセス権限のないファイルやディレクトリ、あるいはシステムリソースなどにアクセスし、盗用、改ざん、破壊などの行為を行う攻撃である。更に、不正アクセスのプロセスは使用 OS やシステム上で提供しているサービスの種類などによって様々なパターンが想定され、一様な行動計画を策定することが難しい。そこで、ここでは対策のための基本的な手順の検討を行う。

行動計画 7-1 ネットワーク間のフィルタリングルールを確認する。

不正アクセスが発生した場合には、まずはじめにそのアクセス経路を特定するために、

ネットワーク間のフィルタリングルールを確認する。被害を受けたシステムには、どんな種類の通信サービスが到達可能であったのかを定義する。

行動計画 7-2 ネットワークサービスのアクセスログを確認する。

ネットワーク経由で当該システムに到達できる通信サービスの種別が特定できたら、該当する通信サービスに関連するログを検証し、不正アクセスの痕跡がないかどうかを調査する。

行動計画 7-3 検査ツールによってシステムに存在する弱点を明確にする。

これまでの作業では不正アクセスの原因が特定できなかった場合や、更に別の侵入パターンの可能性を調査するために、検査ツールを利用してシステムに存在する弱点を全て洗い出す。

行動計画 7-4 被害状況を明確にする。

通常、不正アクセスのプロセスには 2 つのフェーズが考えられる。不正アクセスの第 1 フェーズは、他人のパスワードを不正に使用したり、システム上に存在するセキュリティホールを利用してシステムにアクセスするフェーズである。通常、ここまでの行為なら、これまで検討してきた行動計画に沿って検出、排除することができる。

一方、不正アクセスの第 2 フェーズでは、特権ユーザ権限を奪取し、次回以降のアクセス手段を確保するためにバックドアを設置したり、該当個所のログを削除したり、各種のシステムリソースを改ざんしたりするような行為を行う。この段階まで実行された攻撃を特にルートキット攻撃(Root-Kit Attack)と呼ぶ場合もある。フェーズ 2 まで不正アクセスが進展してしまった場合には、その被害が広範囲に及び被害状況を明確に定義することが難しくなっている場合も多い。一応、事前にシステムリソースのハッシュ値を計算しておき、バックアップデータと逐一比較していく方法にはある程度の効果が期待できる。しかし、通常ルートキット攻撃が実行された可能性がある場合には、バックアップデータからの部分的な復旧プランは採用されず、念のためシステム全体を再インストールするプランが選択される場合が多い。

(8) サービス妨害に応じた行動計画

サービス妨害とは、システムが予期せぬ不正な入力を与えたり、システムの処理能力以上の負荷をかけることによって、その機能を一時的に麻痺させる攻撃である。当初、サービス妨害はシステムを再起動すればそのダメージから回復することができるので、あまり深刻な脅威として見積もられることはなかった。しかし、インターネットのビジネス利用が進展し、組織の業務をコンピュータシステムで提供する傾向が強まるにつれ、サービス妨害も無視できない脅威になってきている。例えば、顧客からの発注を Web サーバ経由で受注している組織などでは、Web サーバがサービス妨害によって麻痺することは、組織の事業活動に大きなダメージを及ぼすことが容易に想像できる。

また、特に最近では、分散協調型 DoS 攻撃(Distributed Denial Of Service)と呼ばれる、複数のサイトからある特定の攻撃対象に対して一斉にサービス妨害を行うタイプの攻撃が出現し、大きな脅威となっている。

行動計画 8-1 アドホックにフィルタリングルールを設定する。

サービス妨害には、システム上のセキュリティホールが原因で引き起こされるタイプの攻撃もある。その場合には、検査ツールで弱点を検出し、アプリケーションのバージョンアップや、セキュリティパッチを適用することによってその原因を除去することができる。

一方で、システムに処理能力以上の負荷をかけてその機能を麻痺させるタイプのサービス妨害の場合には、絶対的な対処方法が存在しない。このような状況が発生した場合には、その都度、攻撃元のサイトからのアクセスを拒否するようにフィルタリングルールの設定を変更していく方法が、ある程度の効果を期待できると考えられる。

行動計画 8-2 外部機関と連携する。

分散強調型 DoS 攻撃の場合は、その都度アクセス拒否のフィルタリングルールを設定する方法でもあまり効果は期待できない。この種の攻撃の場合は、セキュリティ対策が脆弱なサイトが踏み台にされて、そこから攻撃が行われている場合が多いので、該当する攻撃サイトの管理者とコンタクトを取り、事実を通知するとともにその対策を促すべきである。また、契約しているプロバイダとその対応策について協力を依頼するのもよい考えである。

(9) 風説の流布に応じた行動計画

風説の流布に分類される攻撃には次の 2 つのタイプが考えられる。1 番目のタイプは、不特定多数を対象としたデマ情報の流布である。例えば、Good Times Virus や Y2K Virus などが該当する。チェーンメールもこのタイプの攻撃に該当する。2 番目のタイプは、ある特定の相手を対象とした攻撃である。この場合には、相手を誹謗中傷した内容を Web ページやインターネットニュースなどを使ってインターネット上で公開するケースが多い。

行動計画 9-1 デマに関する情報を収集し関係者に通達する。

不特定多数を対象としたデマ情報の場合には、様々なセキュリティ機関からこの種のデマ情報に関する警告が公表されている。そこで、組織内でこのようなデマ情報が蔓延した場合には、これらの警告情報を収集し関係者に通達するとよい。

例)

デマ情報に関するページ

CIAC Internet Hoaxes

<http://ciac.llnl.gov/ciac/CIACHoaxes.html>

行動計画 9-2 組織としての見解を表明する。

2 番目の相手を特定したタイプの攻撃が組織に対して行われた場合には、当該の件に関する組織としての見解を表明する必要がある。この場合の対応は組織の経営陣、法務部門、広報部門の判断を仰ぐ必要がある。

(10) システム探査に応じた行動計画

システム探査は、攻撃対象のシステム構成を調査するための情報収集行為で、システムへの不正行為の初動として捉えることができる。そして、このことは当該システムに対して不正行為を行おうとしている何者かが存在していることを示す証拠でもある。

行動計画 10-1 組織のインシデントレスポンスチームに報告をする。

実際には被害がなくとも、組織のインシデントレスポンスチームにシステム探査行為があったことを連絡しておくのはよい考えである。また、その際に該当するログを一緒に添付し、その内容を確認してもらうとよい。

行動計画 10-2 被害を正確に見積もる。

インシデントレスポンスチームでは、システム探査が行われたことを示すログを検証し、実際に行われた行為が何かを正確に定義しなければならない。実被害はなくとも、例えば OS の種類やホストの IP アドレス、あるいはシステムで提供しているサービスの種類など、相手にシステム構成に関する何らかの情報が伝わったはずであり、このことは将来的な脅威になりうる可能性がある。そこで、攻撃者に何の情報も伝わったのかを把握しておくことは重要である。

2-3-2-5. コンティンジェンシープランの運用と見直し

本節では「事前の準備」の項目に、対サイバーテロ用として新たに追記する項目について検討を行う。(P33 枠内参照)

(1) テスト計画の立案

策定したコンティンジェンシープランが、サイバーテロ行為が発生した場合に真に有効な文書であるために、プラン策定後も定期的にテストを行い、その内容を検証していく作業が必要である。

コンティンジェンシープランのテストは、通常1年に1度、あるいは半年に1度といった周期で実施されるが、それとは別に、対象システムの構成に変更が発生した場合にも、その都度テストは実施されなければならない。テストを実施するタイミングとしては、

- システムで新しい業務が提供されることになった場合。
- システムで提供している業務の重要度に変更があった場合。
- システムの操作方法や処理手順などの仕様に変更があった場合。
- バックアップ用リソースの構成に変更があった場合。
- 要員の役割や責任に変更があった場合。

などが考えられる。

(2) テストの実施と評価

コンティンジェンシープランで想定したシナリオに基くシミュレーションテストを実施する。シミュレーションテストでは、関係者全員の参加を要請し、なるべく本番に近い環境を再現することが望ましい。また、テストの評価項目として、最低でも次の事柄を確認しておく必要がある。

- 適切なバックアップファイルが調達できたかどうかの確認。
- 調達したバックアップファイルを使ってシステムが復旧できたかどうかの確認。
- コンティンジェンシープラン第2部「継続・復旧のためのリソースの確保」でリストアップされたリソースに過不足がなかったかどうかの確認。
- シナリオで定義された行動計画通りに作業が進行したかどうかの確認。

(3) 更新作業

シミュレーションテストの結果、コンティンジェンシープランの内容を変更する必要性が認められた場合は、内容の更新作業を速やかに実行する。また、プランの内容に変更があったことを関係者に通知しておく。

2-4. その他のセキュリティ対策へのフィードバック

コンティンジェンシープランを策定するためには、その組織のセキュリティ対策として、別途整備されていなければならない様々な事柄が存在する。そこで、本節ではコンティンジェンシープラン策定時に、その組織で併せて検討されなければならないその他のセキュリティ対策について検討を行う。

2-4-1. セキュリティ対応体制への反映

(1) サイバーテロ報告体制の整備

サイバーテロリズムはユーザやシステム管理者からの通報によって発覚する場合も多い。そこで、サイバーテロの疑いのある事象を発見した場合には、どこにどのような手段で報告すればよいのかを組織の全員に周知させておく必要がある。ここで、組織の連絡網を整備したり、インシデントレスポンスチームのヘルプデスクを設置することはよい考えである。

また、報告活動を促進させるために、サイバーテロ発見に功績のあったユーザには報奨金を出したり、サイバーテロが発生した場合に確認される事象を事例集として作成しておき、該当する事例を発見したら報告させるようにしておくこともよい。また、報告の際には効率のよい情報伝達を実現するために、サイバーテロ発見報告書を用意しておき、必要事項をあらかじめ記入させてから報告する方法も考えられる。

(2) 法的対応体制の整備

サイバーテロの被害を受けた場合には、その犯人に対して法的手続きを執ることが考えられる。そこで、サイバーテロやハイテク犯罪に見識のある要員や外部協力者を確保しておかなければならない。特にサイバーテロの場合は、その証拠となるログが電子データであるために、証拠物件としての有効性を保持するためにはさまざまな手続きを踏まなければならない。そこで、法的手続きを見据えた行動計画を策定するためには、その内容についてアドバイスを受けておくこともよい。

また、システムのログイン画面に表示されるバナーメッセージとして、当該システムは組織の資産であり、不正な使用が禁止されている旨の内容を表示することは、法的観点から考えて非常に重要なことである。そこで、このバナーメッセージの内容について法的に検証しておいてもらうことも重要である。

(3) 広報体制の整備

システムが提供している業務によっては、サイバーテロの被害を受けた事実を外部に公表しなければならないかもしれない。その際の手続きについて、組織の広報部門と事前に対応方法や告知の文面などを決めておいた方がよい。

2-4-2. セキュリティ教育への反映

(1) ユーザ教育

サイバーテロへの対応作業期間は、業務形態が平常時とは異なることが予想される。そこで、ユーザには平常業務時とサイバーテロ発生時との業務形態の違いについてあらかじめ認識させておく必要がある。

また、サイバーテロ発生時に、組織内で根拠の無い噂が飛び交ったり、予想外の組織外への情報流出が発生することを防ぐために、ユーザにはサイバーテロ発生時の情報の取扱い方法についても教育しておかなければならない。

(2) インシデントレスポンスチームの要員育成

サイバーテロに対して適切に、そして迅速に対処するためには、組織でインシデントレスポンスチームを整備しておく必要がある。そこで、現段階ではコンピュータセキュリティに関する専門的なスキルを持った要員を確保できない場合には、要員の育成を行う必要がある。例えば、セキュリティエンジニアの教育、訓練を実施している企業もあるので、そうした企業に要員育成を依頼するのもよい。また、サイバーテロへの対応作業中は、対応チームのメンバーは厳しい労働条件を強いられることも多い。そこで、復旧作業中の特別手当など相応のサポートを雇用者側で用意しておくこともよい。

2-4-3. セキュリティポリシーへの反映

(1) パスワード管理

緊急事態が発生した場合に、すぐには関係者全員が集まるのが難しい場合も多い。そこで、対応作業で必要となるコンピュータシステムの特権ユーザのパスワードはオフラインで管理しておき、非常時にはインシデントレスポンスチームのメンバーがアクセスできるようにしておかなければならない。また、場合によっては暗号鍵やコンピュータシステムへの入退室管理システムの暗証番号などもその対象となることが考えられる。ここで、基本となる考え方は、緊急事態発生時に関係者全員が揃わなくとも、対応作業で使用するリソースは全て揃えることができる管理体制の保証である。

(2) プライバシーの保護

サイバーテロへの対応作業中には、例えば、ネットワークパケットを監視したり、ログファイルを検証したり、システムに保存されているファイルの中身を確認したりする作業が発生することが予想される。そして、こうした作業は組織のユーザのプライバシーを侵害する行為と受け取られることもある。そこで、事前に組織のセキュリティポリシーにおいて、システムは全て組織の資産であり、必要に応じて通信パケットを監視したり、ログ

を検証したりするようなユーザのプライバシーを越権する行為が行われることがある旨の記述を用意しておく必要がある。

(3) システム設計基準

組織に導入されるシステムは、二重化、冗長構成、コンポーネント化などあらかじめ緊急時下での運用が考慮された設計になっていなければならない。そのため、セキュリティポリシーでシステムの設計基準を示しておく必要がある。

(4) バックアップ

コンティンジェンシープランでは、当該システムの復旧作業で使用する適切なバックアップデータが存在することが大前提となっている。そこで、セキュリティポリシーではシステムのバックアップ作業に関する手続きが明言されていなければならない。

ここで、システムのバックアップデータには次の3種類が用意されている必要がある。

初期バックアップ

システムを最初にインストールした際に、システム全体を対象に作成されるバックアップ。サイバーテロの被害が甚大であったり、長期間に及んでいたために他のバックアップデータが全て汚染されているような場合に使用される。

フルバックアップ

バックアップの対象は初期バックアップと同じである。システムの稼働後、定期的に行われるバックアップ。サイバーテロの被害は甚大であったが、その時期を特定できるような場合は、当該データを用いて、ある時期より前の状況にシステム全体を戻すことができる。

インクリメンタルバックアップ

システム上のリソースに変更があった場合に、その差分だけを対象に行われるバックアップ。サイバーテロの被害範囲を一意的に定義することができた場合に使用される。

以上3種類のデータに対するバックアップ計画が適切に立案されており、その手順、頻度、そしてデータの保持期間が明示されているかどうかを確認しておかなければならない。また、履歴管理の適切性についても検証しておく必要がある。ここで、更にバックアップ対象である各ファイルのインテグリティを証明するために、ハッシュ関数などを併用しておくのもよい考えである。

(5) 日常の管理作業

サイバーテロによる被害を最小限に止める最良の方法は、日常のシステム管理を適切に

実施しておくことである。ログの収集・分析やセキュリティパッチの導入、セキュリティ情報の収集など日常の運用管理手続きが適切に規定されているかどうか検証しておかなければならない。

第3章 コンティンジェンシープランのサンプル

本章では、第1章「コンティンジェンシープランのあり方」及び、第2章「コンティンジェンシープラン策定の手引き」で検討を行ったプランの立案手法を用いて、対サイバーテロ用のサンプルコンティンジェンシープランを作成する。

なお、本章で示すサンプルプランは、図1-1 および図2-1 で示されたCSIRに該当するプランであり、プラント業務に対するコンティンジェンシープランの一部分である。

大規模プラントネットワークにおけるシステム構成モデルの 対サイバーテロ・コンティンジェンシープラン (サンプルプラン)

構成内容

第 1 部 策定対象の定義とプライオリティの設定

第 2 部 継続・復旧のためのリソースの確保

第 3 部 シナリオに基く緊急時の行動計画

第 4 部 運用と見直し

本サンプルプランでは、プラン拡張作業のベースとして使用された既存のコンティンジェンシープランの記述内容と共通する項目については、破線でその項目の策定方針を示すにとどめ、記述例までは掲載していない。

平成 年 月 制定

平成 年 月 改訂

株式会社

第 1 部 策定対象の定義とプライオリティの設定

1. 本コンティンジェンシープランで対象とするコンピュータシステム

本コンティンジェンシープランでは、図 3-1 に示した「大規模プラント・ネットワークにおけるシステム構成モデル」のうち制御系システムをその対象とする。同図中に併せて示されている情報系システムは、本プランの対象外である。

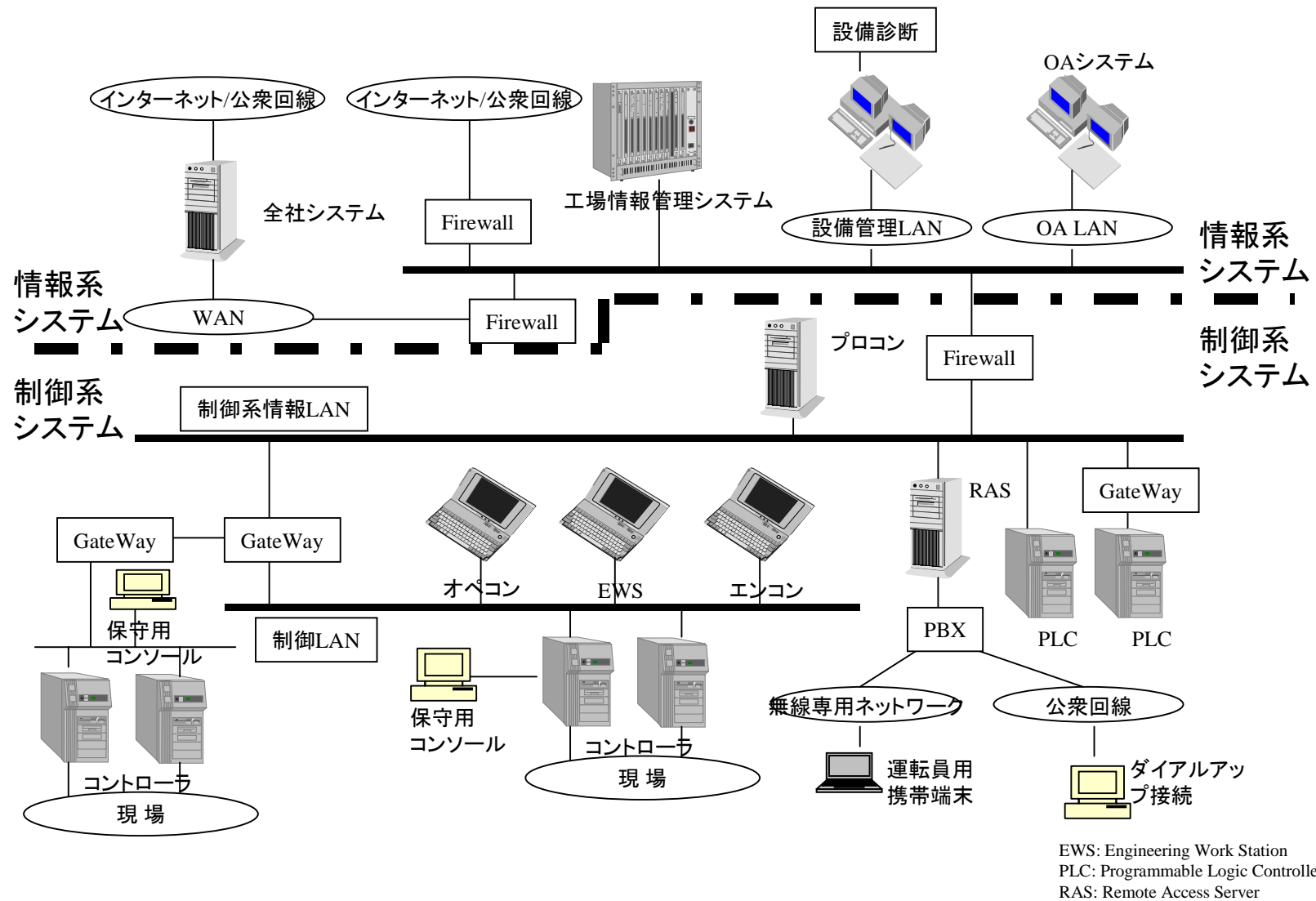


図3-1 大規模プラントネットワークにおけるシステム構成モデル

2. 本コンティンジェンシープランで対象とする業務

本項目は、既存のコンティンジェンシープランと共用することができる。

あるいは、2-3-1-2 節「システムの分析」で検討した業務分析の手法により、前節で定義したコンピュータシステムを利用して提供されている業務を抽出して列挙しておく。

3. 緊急時における業務の優先順位とその作業期間

本項目は、既存のコンティンジェンシープランと共用することができる。

あるいは、2-3-1-2 節「システムの分析」で検討したリスク分析の手法により、前節で定義された業務をその重要度が高い順に並べ替え、それぞれが復旧までに許容される作業期間を明示しておく。

次のような表形式で表記しておいてもよい。

表 3-1. 緊急時における業務の優先順位とその作業期間

優先順位	業務名	復旧に要する作業期間
1	業務 A	業務が停止後 24 時間以内の復旧が必要。
2	業務 B	業務停止後 3 日以内の復旧が必要。
2	業務 C	業務停止後 3 日以内の復旧が必要。
3	業務 D	業務停止後 1 週間以内の復旧が必要。
4	業務 E	緊急時には業務は停止してよい。

4. 本コンティンジェンシープランで対象とする脅威

本コンティンジェンシープランでは、制御系システムに対するサイバーテロリズムの発生をその脅威として想定している。ここで、サイバーテロリズムとは、

ネットワークを通じて制御系システムに対して行われる大規模で組織的な敵対行動

と定義し、具体的には次の5つの技術的な手口を利用して実行される行為である。

不正コード攻撃

コンピュータウィルスやトロイの木馬、ワームなどの不正プログラムを制御系システムに対して使用する攻撃手口。

不正アクセス

制御系システムのユーザアカウントを無断で使用してシステムにログインし、更に上位権限のユーザアカウントを奪取したり、システムが制御するリソースにアクセスし、不正操作を行う攻撃手口。システム上の弱点を利用して、ログイン行為を行わずに同種の行為を実行することができる場合もある。

サービス妨害

制御系システムが予期していない不正な入力を与えたり、制御系システムに処理能力以上の負荷をかけることによって、制御系システムが提供している機能を一時的に麻痺させる攻撃手口。

風説の流布

制御系システムに関するデマ情報や脅迫文などを、メールや電子掲示板、ホームページなどを使って流布し、当組織の混乱やイメージダウンを画策する攻撃手口。

システム探査

制御系システムの構成を探査する攻撃手口。制御系システムに対する不正行為の初動、あるいは不正行為の試みが失敗した痕跡と考えられる。

本コンティンジェンシープランで定義するサイバーテロリズムとは、上記5つの手口を制御系システムに対して単一で、あるいは複合的に用いることによって実行される当組織に対する敵対的な行為である。

第2部 継続・復旧のためのリソースの確保

1. インシデントレスポンスチームの任命

制御系システムに対してサイバーテロ行為が発生した場合に、係る行為に中心となって対処するインシデントレスポンスチームの要員を以下の通りに任命する。

指揮チーム

情報システム担当役員を指揮チームのメンバーとして任命する。

企画部部長を指揮チームのメンバーとして任命する。

情報システム部部長を指揮チームのメンバーとして任命する。

作業チーム

情報システム部セキュリティグループを作業チームのメンバーとして任命する。

サイバーテロの被害を受けたシステムの管理者を作業チームのメンバーとして任命する。

法務チーム

法務部部長を法務チームのメンバーとして任命する。

法務部訴訟担当を法務チームのメンバーとして任命する。

広報チーム

広報部部長を広報チームのメンバーとして任命する。

広報部社外対応担当を広報チームのメンバーとして任命する。

第2部では「インシデントレスポンスチームの任命」以外の記述項目は、既存のコンテンツジェネレーションプランと共用することができる。

ここで、構内 PBX を介さずに、直接、公衆電話網に接続している通信手段が確保されていない場合は、当該通信手段の確保に関する記述も追記しておく必要がある。

あるいは、2-3-1-2 節「システムの分析」で検討した業務分析の手法により、業務を復旧させるために必要なリソースの最小構成とその調達手段をリストアップし、その結果を記述しておく。

ここで、業務復旧のために必要とされるリソースには、

人的リソース

処理用リソース

アプリケーションとデータリソース

通信リソース

物理的なインフラストラクチャリソース

ドキュメントリソース

の以上6種類が考えられる。

第3部 シナリオに基づく緊急時の行動計画

本節で想定されるシナリオは、2-3-1-2 節「システムの分析」の作業で実施されるリスク分析の結果を用いて、策定対象に対して発生する可能性がありそうなシナリオを想定することが肝心である。

そこで、本サンプルプランでは平成 11 年 10 月に実施された「石油プラントのネットワーク安全性検証実験」で報告された実験結果に基づいて、脅威発生のシナリオを想定した。

また本節で策定された内容は、電子データとして保存しておくだけでなく、用紙に印刷したものをクリアケースやルーズリーフにファイリングしておき、いつでも必要なときにすぐに参照できるようにしておかなければならない。

脅威発生シナリオ 1

ファイアウォール上でコンピュータウィルスに感染したファイルが発見された。

基本方針 「経過の観察と情報収集」

*それほどリスク度合いの高いシナリオではないので、原因究明に可能な限り努める。

回復マニュアル

確認フェーズ

1. 指揮チームの _____ を責任者に任命する。
2. 作業チームの _____ はファイアウォールに対してウィルスチェックを行う。
3. 責任者は対応メンバーを編成する。
4. 確認フェーズレポートを作成する。

抑制フェーズ

5. 編成された作業チームで確認フェーズレポートを検証する。
6. 関係者に情報系システムと制御系システムが切断されることを連絡する。
7. ファイアウォールをネットワークから切り離す。
8. ファイアウォール上のファイルシステムのフルバックアップを2部作成する。
9. 制御系情報システムのうちカスタム OS を使用していないコンピュータ(プロコン、RAS) に対してウィルスチェックを行う。
10. 抑制フェーズレポートを作成する。

排除フェーズ

11. コンピュータウィルスの感染経路を特定する。
12. 感染ファイルを特定しすべて削除する。
13. ウィルス感染していないバックアップファイルを用意する。
14. 排除フェーズレポートを作成する。

回復フェーズ

15. バックアップファイルからシステムを復旧する。
16. ファイアウォールをネットワークに接続する。
17. システムの復旧を関係者に連絡する。
18. ファイアウォールから発信されるパケットを3日間観察する。
19. 回復フェーズレポートを作成する。

フォローアップフェーズ

20. 各作業フェーズで作成されたレポートをまとめ関係者間でレビューを行う。
21. 報告書の報告内容に従いセキュリティ対策を改善する。

脅威発生シナリオ 2

プロコン上で管理しているコントローラの制御データが改ざんされた。

基本方針 「アクセス拒否と問題解決」

*リスク度合いが非常に高いシナリオなので、事態の修復を最優先に作業を行う。

回復マニュアル

確認フェーズ

1. 指揮チームの を責任者に任命する。
2. 責任者はコントローラの動作に異常がないか確認する。
3. 作業チームの はプロコンの被害状況を確認する。
4. 責任者は対応メンバーを編成する。
5. 確認フェーズレポートを作成する。

抑制フェーズ

6. 編成された作業チームで確認フェーズレポートを検証する。
7. 関係者に制御系情報 LAN が切断されることを連絡する。
8. ファイアウォール、GateWay、RAS をネットワークから切り離す。
9. プロコン上のファイルシステムのフルバックアップを 2 部作成する。
10. プロコンのユーザのパスワードを変更する。
11. ファイアウォール、GateWay、RAS に対して不正アクセスの痕跡がないか確認する。
12. 不審なバイナリプログラム、ユーザの追加、ファイルの改ざんなどプロコン上の被害状況を特定する。
13. 抑制フェーズレポートを作成する。

排除フェーズ

14. FireWall、GateWay、RAS のフィルタリングルールを確認する。
15. プロコン上のログファイルを確認する。（特に制御データへのアクセス履歴）
16. 制御データへアクセス履歴のあるユーザアカウントの所有者と連絡をとり、アクセス履歴とアカウント所有者が実施した作業との突き合わせを行う。
17. 検査ツールを用いてプロコンに対して疑似攻撃を行う。
18. 不正アクセスの原因とプロセスを特定する。
19. 不正アクセスの原因を除去する。
20. 不正アクセス被害を受けていないバックアップファイルを用意する。
21. 排除フェーズレポートを作成する。

回復フェーズ

22. バックアップファイルからシステムを復旧する。
23. システムテストを実施しプロコンの動作を確認する。
24. 制御系情報 LAN をネットワークに接続する。
25. システムの復旧を関係者に連絡する。
26. プロコンから発信されるパケットを 3 日間観察する。
27. 回復フェーズレポートを作成する。

フォローアップフェーズ

28. 各作業フェーズで作成されたレポートをまとめ関係者間でレビューを行う。
29. 報告書の報告内容に従いセキュリティ対策を改善する。

脅威発生シナリオ 3

RAS で何度もログインに失敗したログが検出されていた。

基本方針 「経過の観察と情報収集」

*それほどリスク度合いの高いシナリオではないので、原因究明に可能な限り努める。

回復マニュアル

確認フェーズ

1. 指揮チームの _____ を責任者に任命する。
2. 作業チームの _____ はアクセスに利用されたアカウントの所有者と連絡を取り、ログの裏付けを行う。
3. 責任者は対応メンバーを編成する。
4. 確認フェーズレポートを作成する。

抑制フェーズ

5. 編成された作業チームで確認フェーズレポートを検証する。
6. ログインが成功しているかどうかと実被害があるかどうかを確認する。
7. RAS 上にトラッププログラムを仕掛け経過を観察する。
8. ログファイルのバックアップを 2 部作成する。
9. 抑制フェーズレポートを作成する。

排除フェーズ

10. 犯人を特定する十分な証拠が集まったら、今後の対応について法務チームと協議する。
11. RAS のアクセス番号やアカウントが攻撃者に伝わった経緯について検討する。
12. 攻撃者に伝わったシステム構成情報について検討する。
13. RAS のフィルタリングルールを変更する。
14. RAS のアクセスアカウントを変更する。
15. RAS のアクセス番号を変更する。
16. 排除フェーズレポートを作成する。

回復フェーズ

17. RAS に対するアクセスを一定期間観察する。
18. 回復フェーズレポートを作成する。

フォローアップフェーズ

19. 各作業フェーズで作成されたレポートをまとめ関係者間でレビューを行う。
20. 報告書の報告内容に従いセキュリティ対策を改善する。

第4部 運用と見直し

1. テスト計画

本コンティンジェンシープランは、毎年 月 日に、第3部で策定された脅威発生シナリオの1つを選択して、シミュレーションテストを行ない、その内容の有効性について検討を行う。その際、選択されるシナリオは によって（例えば組織のセキュリティ委員会など）決定される。

また、これとは別に、制御系システムに対して次の変更があった場合には、変更後1ヶ月以内に臨時のシミュレーションテストを行う。

臨時のシミュレーションテストを伴う制御系システムの変更

制御系システムで新たな業務が提供されることになった場合。
制御系システムの操作方法や業務の処理手順が変更になった場合
制御系システムに係る要員の人事異動があった場合

2. 評価基準

テスト計画に基づいて実行されたシミュレーションテストの結果は、次の評価基準によって判定される。

シミュレーションテストの評価基準

適切なバックアップファイルを調達することができたかどうか。
復旧作業用にリストアップされたリソースに過不足がなかったかどうか。
行動計画通りに業務の継続・復旧作業が進行したかどうか。

3. 更新手続き

シミュレーションテスト及びその結果の評価は、 によって（例えばシミュレーションテストの実施責任者）報告書としてまとめられ、その内容についてはテスト関係者間で同意を得なければならない。

コンティンジェンシープランの記述内容の更新、及びその旨の関係者への連絡は、 によって実施される。

4. 改訂履歴

年 月 コンティンジェンシープラン策定。

年 月 定期テストに伴うプランの内容更新。

年 月 組織の人事異動に伴う臨時テストの実施。臨時テストに伴うプランの内容更新。

おわりに

本調査研究では、大規模プラントの制御用コンピュータシステムにサイバーテロ行為が発生した場合に備え、対サイバーテロ用のコンティンジェンシープランを策定することを目的とし、その立案方法に関する調査研究を行った。

その結果、まずコンティンジェンシープランでは次の 4 つの内容について記述されていなければならないことがわかった。

コンティンジェンシープランの構成

第 1 部 策定対象の定義とプライオリティの設定

対象とするコンピュータシステム、当該システム上で提供されている業務とその重要度、及び対象とする脅威に関する記述。

第 2 部 継続・復旧のためのリソースの確保

緊急時対応に必要とされるリソースに関する記述。

第 3 部 シナリオに基く緊急時の行動計画

脅威発生シナリオと場合の緊急時行動計画に関する記述。

第 4 部 運用と見直し

プランのテスト計画に関する記述。

また、本調査研究の対象脅威であるサイバーテロリズムを次のように定義することができた。

サイバーテロリズムの定義

ネットワークを通じて政府や産業に対して行われる大規模で組織的な敵対行動であり、次の 5 種類の手口を用いて実行される。

- 不正コード攻撃
- 不正アクセス
- サービス妨害
- 風説の流布
- システム探査

ここで、本定義はあくまでも本調査研究にのみ適用される定義である。実際には、サイバーテロリズムに関する定義は、各サイト毎に検討、実施されなければならない。この時、

1-4-2 節「サイバーテロリズムの分類」や 1-4-3 節「サイバーテロリズムの手口の分類」で検討した内容が役に立つかもしれない。

そして、コンティンジェンシープランは次の手順で立案、策定することがわかった。

コンティンジェンシープランの策定手順

プラン策定前の作業

プランの対象となるシステムの範囲を明確にする。

業務分析により、システムで提供されている業務と業務復旧のために必要なリソースを明確にする。

リスク分析により、業務のプライオリティとプランで対象とするリスクを明確にする。

既存のコンティンジェンシープランの分析により、追記、修正する記述項目を明確にする。

プラン策定作業

緊急時行動計画を策定するための基本方針を明確にする。

組織でサイバーテロに対応する体制を整備する。

リスク発生のシナリオを想定し、シナリオ毎に行動計画を策定する。

プランのテスト計画を策定する。

プラン策定後の作業

テスト計画に沿ってテストを実行し、継続的にプランのメンテナンスを行う。

また、コンティンジェンシープランの策定作業と並行して、既に施行されている他のセキュリティ対策についても見直し作業を実施しておかなければならない。

その他のセキュリティ対策へのフィードバック

セキュリティ対応体制の見直し

連絡網の整備、法務、広報部門とのサイバーテロへの対応の事前検討について。

セキュリティ教育の見直し

サイバーテロに関するユーザ教育と、対応要員の育成について。

セキュリティポリシーの見直し

パスワードポリシー、プライバシーポリシー、バックアップポリシー、運用管理ポリシーについて。

そして、ここまでに検討してきた立案手法を用いて第 3 章「コンティンジェンシープランのサンプル」では、大規模プラントの制御システムを対象にサンプルプランを作成した。

本調査研究では、対サイバーテロ用のコンティンジェンシープランに関する調査研究を行い、その立案手法を明らかにすることができた。近年、組織の業務にコンピュータシステムが利用される機会が飛躍的に増加し、それに伴い、組織にとって重要な情報をシステム上で取り扱う機会も増えてきている。コンピュータシステムのセキュリティ対策としては、まずシステムが抱える様々な脅威を未然に防止するための防御策が重要である。そのため、「大規模プラント・ネットワークセキュリティに関する研究プロジェクト」では、「大規模プラント・ネットワーク・セキュリティについての中間報告書」及び「石油プラントのネットワーク安全性検証実験」において、数々の防御策に関する検討を行ってきた。

しかし、どんなに周到な防御策を事前に用意しておいたとしても、そのセキュリティ機構が機能せずに、コンピュータシステムがダメージを受けてしまう可能性は残存する。そこで、システムに対して脅威が発生した場合に、逸早くそのことを検出し、逸早く元の状態に復旧することを目的とした事後対策は、防御策を補完するセキュリティ対策として、事前対策同様に重要であると考えられる。

本調査研究において、その策定手法を検討したコンティンジェンシープランは、コンピュータシステムのセキュリティ対策の内、事後対策に相当するセキュリティ対策の一つである。そのため、システムに対して、サイバーテロ行為を未然に防ぐ防御策を必要十分に実施した段階で策定することによって、はじめてその意味を持つことができる。

最後に、本調査研究では、主に大規模プラントの制御システムをその対象として検討を重ねてきたが、ここで検討された手法は、そのまま他の汎用的なコンピュータシステムに対しても適用することができる。本報告書が、コンピュータシステムの対サイバーテロリズム用のコンティンジェンシープランを策定する際の手引書としても、また広く利用されることを期待している。

付録 A トラッププログラム

コンティンジェンシープラン第 3 部「シナリオに基く緊急時の行動計画」では、サイバーテロを引き起こした犯人に対して法的手続きを検討している場合には、法廷での証拠物件を集めるための行動計画を策定しなければならない。そこで、本報告書では証拠物件を集めるための行動計画の例として、抑制フェーズにおける行動計画 2-6「トラップを仕掛ける。」を策定した。

ここで、トラッププログラムとは、

システム上の指定されたネットワークサービスをシミュレートするプログラム

であり、ハニーポット(Honey Pot)やデコイ(decoy)などと呼ばれている。トラッププログラムは、指定されたネットワークサービスの振りをして、そのネットワークサービスに対して行われた全ての行為をログとして記録するように設計されている。このログには、キーストロークまで記録されるように設計されているトラッププログラムもある。

そこで、サイバーテロの被害を受けた場合には、その手口がネットワークサービスの脆弱性を利用した手口であった場合には、密かにネットワークサービスをこのトラッププログラムと置換えておくことによって、

- ・ 証拠として十分なログを収集することができる。
- ・ サイバーテロの手口や犯人のスキルレベルを明らかにすることができる。
- ・ 犯人の身許に関する情報を収集することができる。

などの効果を期待することができる。

現在、よく使用されているトラッププログラムとしては次のものが知られている。

[1] Deception Tool Kit (<http://www.all.net/dtk/>)

よく知れ渡った弱点を持つ様々なネットワークサーバの振りをして、攻撃者の行動をログとして記録する。

[2] Back Officer Friendly (<http://www.nfr.net/bof/>)

トロイの木馬プログラム BackOrifice のサーバの振りをして、攻撃者の行動をログとして記録する。

付録 B 検査ツール

コンティンジェンシープラン第 3 部「シナリオに基く緊急時の行動計画」では、サイバーテロの原因となった手口を究明して取り除くために、排除フェーズにおける行動計画 3-2「疑似攻撃を行う」で、検査ツールを用いてコンピュータシステムに疑似攻撃を行う行動計画の例を策定した。

ここで、検査ツールとは、システムに存在する脆弱な設定やセキュリティホールを検出するツールで、システムに対するサイバーテロ行為もこのようなシステム上の弱点を最初の手がかりとして展開される場合が多い。

検査ツールは、そのツールで想定している攻撃手法に応じて次の 3 種類に分類される。

(1) リモート攻撃用検査ツール

リモート攻撃とは、攻撃対象のシステムに対してユーザアカウントを所持していなくても実行可能な攻撃であり、その性質上、ネットワークサービスのサーバに対する攻撃が中心である。このリモート攻撃に利用されるシステム上の弱点を検出するツールを、リモート攻撃用検査ツールと呼ぶ。

リモート攻撃用検査ツールでは、ネットワーク上に疑似攻撃用のホストを用意し、そのホストから検査対象となるホストの弱点をネットワーク経由で探査する。そのため、ネットワーク間でフィルタリングルールが設定されている場合には、疑似攻撃用のホストの配置場所によって、検査結果が変化してくる可能性があるので注意しなければならない。

現在、よく使用されているリモート攻撃用検査ツールとしては次のものがある。

リモート攻撃用検査ツールの例)

[1] SATAN (Security Administrator Tool for Analyzing Networks)

<http://www.porcupine.org/satan/>

[2] Nessus

<http://www.nessus.org/>

[3] SAINT (Security Administrator's Integrated Network Tool)

<http://www.wwdsi.com/saint/>

[4] SARA (Security Auditor's Research Assistant)

<http://home.arc.com/sara/index.html>

[5] NMAP (The Network Mapper)

<http://www.insecure.org/nmap/index.html>

(2) ローカル攻撃用検査ツール

ローカル攻撃とは、攻撃対象のシステムに対してユーザアカウントを所持している状態で実行可能な攻撃であり、その性質上、更に上位のユーザアカウント（通常は特権ユーザアカウント）を奪取する攻撃が中心である。このローカル攻撃に利用されるシステム上の

弱点を検出するツールを、ローカル攻撃用検査ツールと呼ぶ。

ローカル攻撃用検査ツールでは、検査対象となるホストに検査ツールをインストールして、当該ホスト上で検査が実施される。そのため、検査を実施するには当該ホストの特権ユーザ権限が必要とされる。

現在、よく使用されているローカル攻撃用検査ツールとしては次のものがある。

ローカル攻撃用検査ツールの例)

[1] COPS (Computer Oracle and Password System)

<ftp://coast.cs.purdue.edu/pub/tools/unix/cops>

[2] Tiger

<ftp://net.tamu.edu/pub/security/TAMU/>

[3] TARA (Tiger Analytical Research Assistant)

<http://home.arc.com/tara/index.html>

(3) パスワード攻撃用検査ツール

パスワード攻撃とは、攻撃対象のシステムの脆弱なパスワードを持つユーザアカウントを奪取する攻撃である。パスワード攻撃の手法としては、攻撃対象のシステムから得られる様々な情報を頼りにパスワードを類推する推測攻撃や、よく使用されるキーワードが登録された辞書を用いる辞書攻撃、全ての文字の組み合わせを総当たりで試していくブルートフォースなどが知られている。

現在、よく使用されているパスワード攻撃用検査ツールとしては次のものがある。

パスワード攻撃用検査ツールの例)

[1] Crack

<ftp://ftp.ox.ac.uk/pub/comp/security/software/crackers/>

[2] L0phtcrack

<http://www.l0pht.com/l0phtcrack/>

付録 C 主要な情報セキュリティ技術

1. 情報セキュリティ対策技術の分類

現在、一般的に使用されている情報セキュリティ技術は、次の 6 つのカテゴリに分類できる。

暗号技術

保護対象となるデータを暗号化することによって、第三者からの不正な閲覧を防止するための技術。

アクセスコントロール技術

保護対象となるデータやシステムにアクセス権限を設定することによって、許可されていない第三者からの不正なアクセスを防止するための技術。

侵入検出技術

保護対象となるデータやシステムに対して、不正行為が行われた場合にその行為を検出するための技術。

アンチウィルス

保護対象となるデータやシステムをコンピュータウィルスやトロイの木馬、ワームなどの不正コードの被害から防止するための技術。

脆弱性検出技術

保護対象となるシステムに存在するアプリケーションの設定ミスやセキュリティホールを検出するための技術。

バックアップ技術

保護対象となるデータやシステムの複製を作成するための技術。

以下の節では、それぞれのカテゴリーに属する情報セキュリティ技術の解説を行う。

2. 暗号技術

暗号技術とは、保護対象となるデータを暗号化することによって、第三者からの不正な閲覧を防止するための技術である。暗号技術は主として、第三者から情報を秘匿するために用いられる。データを暗号化するためのアルゴリズムには秘密鍵暗号方式と公開鍵暗号方式の 2 つのアルゴリズムがある。

2-1. 秘密鍵暗号方式

情報を暗号化する暗号鍵と、情報を復号化する復号鍵が同一である暗号方式。情報を暗号化するスピードの点で優れている。通信で用いる場合には、送信者と受信者があらかじめ同じ鍵を共有しておく必要がある。対称暗号方式、慣用暗号方式とも呼ばれる。

2-2. 公開鍵暗号方式

情報を暗号化する暗号鍵と、情報を復号化する復号鍵が異なる暗号方式。送信者は受信者の公開鍵でデータを暗号化して送信する。受信者は自分だけが知っている秘密鍵でこれを復号する。公開鍵で暗号化された情報は秘密鍵でしか、秘密鍵で暗号化された情報は公開鍵でしか復号することができない。当事者間で何らかの秘密を前もって共有しておく必要がないので通信に適している。秘密鍵暗号方式に比べると暗号化処理に時間がかかる。非対称暗号とも呼ばれる。

2-3. ハイブリッド方式

保護対象であるデータの部分は秘密鍵暗号方式で暗号化し、その秘密鍵を公開鍵暗号方式で暗号化する方式。公開鍵暗号方式の処理速度が遅いという欠点を補った方式で、特に暗号化通信では頻繁に使用されている方法である。

3. アクセスコントロール技術

アクセスコントロールとは、保護対象となるデータやシステムにアクセス権限を設定することによって、許可されていない第三者からの不正なアクセスを防止するための技術である。アクセスコントロールは情報セキュリティ対策技術の中でも最も基本的な対策で、利用主体を判別する認証技術、ファイルシステムやデータのアクセス権限を設定するリソースパーミッション技術、ネットワークの境界に設置し、ネットワーク間の通信の出入を制限するフィルタリング技術の3種類に分けることができる。保護対象へのアクセスを適切に設定することによって、データやシステムへの不正行為を未然に防止することができる。

3-1. 認証技術

保護対象であるシステムやリソースの利用主体を識別する認証技術には、ホスト単位で認証を行うホスト認証と、ユーザ単位で認証を行うユーザ認証がある。認証技術には現在、様々な方式が提案されている。

IP アドレス認証方式

認証に IP アドレスを用いる。予めシステムファイルに登録された IP アドレスからの通信は信頼する方式。ホスト認証で使用される。

公開鍵暗号認証方式

送信側は自分のサインの部分を自らの秘密鍵で暗号化する。その後、情報の部分を受信側の公開鍵で暗号化して送信する。受信側は自分の秘密鍵で情報部分を復号化し、相手の公開鍵でサインの部分を復号化する。この作業により通信者間の認証を行うことができる。

認証局

公開鍵の安全な登録、管理を行なう第三者機関として認証局がある。認証局によって公開鍵の信頼性が保証される。そのため、認証局を介した認証手順が現在は最も安全度が高い認証方法だと考えられる。

パスワード認証方式

パスワード認証方式とは、認証側と被認証側で予め共有されたある特定文字列を入力することによって利用主体の認証を行なう、認証技術の中では最も基本的な方式である。パスワード認証には、固定パスワード方式とワンタイムパスワード方式の 2 種類がある。

固定パスワード方式

固定パスワード方式とは、認証時に常に同一のパスワードを使用する方式である。そのため脆弱なパスワードは推測される可能性があるため、適切なパスワード管理により、パスワードを保護する必要がある。

ワンタイムパスワード方式

ワンタイムパスワード方式とは、認証毎に使用するパスワードが異なる方式である。固定パスワード方式よりも強力な認証方式である。ワンタイムパスワードはその方式の違いから、更に S/Key 方式とチャレンジ&レスポンス方式とに分類される。

S/Key 方式

ユーザは予めパスワード生成プログラムでワンタイムパスワード群を作成しておく。そしてそれらを何らかの手段で記録しておき、認証の度にパスワード群の中から 1 つずつパスワードを使用していく方式である。作成されたパスワードの管理はユーザに依存され、また、パスワード生成プログラムにハッシュ関数を使用しているため、固定パスワードが使用されるためそのセキュリティ強度が運用に大きく依存する方式である。

チャレンジ&レスポンス方式

接続要求があったクライアントに対して、サーバはチャレンジコードと呼ばれるランダムな文字列を生成し、これを接続要求のあったクライアントの公開鍵で暗号化して送信する。クライアントは暗号化されたチャレンジコードを復号化し、その結果をサーバに送信する。この一連の仕組みをチャレンジ&レスポンス方式と呼ぶ。

所有物認証方式

ID カードなどユーザ本人であることを証明する物理的な代用物による認証方式である。この方式はあくまでも所有物を認識しているだけなので、パスワード認証と併用して認証強度を高める方式が採用されているケースもある。

バイオメトリクス方式

バイオメトリクスには、指紋、網膜などの生物学的な個人の特徴で認証するものと、サインなどの非生物学的な個人の特徴で認証するものがある。ユーザはほとんど労力を必要とすることはなく、また個人を特定する能力に優れている。

3-2. リソースパーミッション技術

リソースパーミッションとは、ファイルシステムやデータのアクセス権限を設定する技術である。既にマルチユーザ環境のオペレーティングシステムやデータベースには標準で備え付けられているセキュリティ機能である。例えば UNIX のファイルシステムでは、利用主体をユーザ、ユーザと同一グループ、その他のユーザの 3 つのグループに分けて、それぞれのグループ毎に読込権、書込権、実行権を設定することができる。

3-3. フィルタリング技術

フィルタリング技術とは、セキュリティポリシーの異なるネットワークの境界で、ネットワーク越しの通信パケットの出入を制限する技術である。フィルタリング技術には、パケットフィルタリングとプロキシサービスの 2 種類がある。

パケットフィルタリング

パケットフィルタリングとは、ネットワーク上のパケットに対して、選択的にその通過を許可、不許可にする技術である。パケットフィルタリングでは、IP アドレス、プロトコル、ポート番号などの TCP/IP ヘッダ情報を使用してフィルタリングを行う。

プロキシサービス

プロキシサービスとは、セキュリティポリシーが異なるネットワークの境界に置かれたホスト上で実行されるサーバプログラムであり、各ネットワークサービスへの代替接続サービスを提供する。

4. 侵入検出技術

侵入検出とは、保護対象となるデータやシステムに対して不正行為が行われた場合に、その行為を検出するための技術である。

4-1. ログ収集

侵入検出を効果的に行うためには、必要十分な種類のログを必要十分な量だけ記録しておかなければならない。オペレーティングシステムやサーバアプリケーションにもログ収集機能は装備されているが、システムへの不正行為を検出するためには、それだけではログの種類が不十分であることもある。ログ収集とは、ネットワークパケットや OS のシステムコールの起動など、システムが予め装備しているログ機能では収集できないログを記録する機能を提供する技術である。

4-2. 改竄検知

不正アクセスにより、データやシステムファイルの改ざんが行われた場合、それを検出するためには、オリジナルのデータやシステムファイルとの比較を行えばよい。しかし、複製を別途保存しての比較では、記憶媒体の容量的にも問題があり、その効率も悪い。また、電子メールなど通信相手先で改ざんを検出する必要がある場合には、オリジナルとの照合という手段は困難である。そこで、通常はデータやシステムファイルの改ざん検知にはハッシュ関数を用いる。その手順は、まずオリジナルのデータやシステムファイルを入力としてハッシュ値を計算しておき、次にその値と現在の保護対象のハッシュ値を比較し、同一値ならば改ざんはなく、またハッシュ値が異なれば、何らかの変更が保護対象に加えられたと判断できる。

4-3. 不正アクセス検知

保護対象のシステムへの不正アクセスを検知する技術は、その形態からネットワーク検出型とホスト検出型に分類することができる。また、侵入判定を行う推論方法の違いから Anomaly Intrusion Detection(AID)と Misuse Intrusion Detection(MID)の2つに分類することができる。

ネットワーク検出型

監視対象のネットワークセグメント上に監視端末を設置して、不正アクセスを監視、検出する方法である。このタイプの特徴は、監視対象にネットワーク上を流れるパケットを利用することである。ネットワークを通じて行われるリモートサイトからの攻撃を検出するのに適している。

ホスト検出型

監視対象である各ホスト毎にインストールされ不正アクセスを監視、検出する方法である。このタイプの特徴は、監視対象にシステム上で記録される様々なログを利用することである。システムのユーザによって行われるローカルでの攻撃を検出するのに適している。

AID(Anomaly Intrusion Detection)

システム上のユーザの行動記録のログを統計処理することによって、各ユーザ毎にジャーナルファイルを作成しておく。そして、そのユーザが通常とは異なる振る舞いを行った場合（例えば、平日の午前中にしかログインしないユーザが、休日の深夜にログインした等）を侵入と判定する。未知の侵入パターンにも対応できるという利点があるが、反面システムに負荷がかかるという欠点もある。

MID(Misuse Intrusion Detection)

予め、侵入パターンをデータベースとして保持しておき、パターンマッチ処理によって侵入の判定を行う。システムに負荷はかからないが、未知の侵入パターンには対応することができない。

5. アンチウィルス

アンチウィルスとは、保護対象となるデータやシステムを不正コードによる被害から防止するための技術である。アンチウィルスは不正コードを検知し、駆除する技術である。ここで、不正コードとは、システムに危害を及ぼすことを目的に作成されたプログラムを指し、コンピュータウィルスやトロイの木馬、ワームなどがその種類として挙げられる。アンチウィルスでは不正コードを、データベース登録されたパターンとのマッチング処理によって検出している。その為、未知の不正コードやデータベースに未登録の不正コードは検出することができないので、データベースはベンダーが提供する最新の内容を維持しておかなければならない。

5-1. ユーザ起動型

ユーザ起動型とは、ユーザがプログラムを起動した時点でのシステムに対して検査を行うタイプのアンチウィルスである。そのため定期的に行うと、被害が拡大してしまうおそれがある。システム常駐型に比べてシステムにかかる負荷が少ない。

5-2. システム常駐型

システム常駐型とは、アンチウィルスがシステムにデーモンとして常駐しており、シス

テム上のファイルにアクセス要求が発生する都度、そのファイルに対して自動的に検査を行うタイプのアンチウイルスである。そのためリアルタイムに不正コードの被害を検出することができるが、反面ユーザ起動型に比べてシステムに負荷がかかる。また、使用履歴のないファイルに対してはウイルス検査が実施されない。

6. 脆弱性検出技術

脆弱性検出とは、保護対象となるシステムに存在するアプリケーションの設定ミスやセキュリティホールなどの脆弱性を検出するための技術である。どんなに堅固なセキュリティ機能を備えたシステムであっても、適切な設定が施されていないならばその機能は無力化してしまう。また、システムにはバグが必ず含まれており、そのバグが原因でセキュリティ上重大な問題を引き起こすこともある。セキュリティ上重大な問題を引き起こすバグを特にセキュリティホールと呼ぶ。

6-1. リモート攻撃に対する脆弱性の検出

リモート攻撃とは、攻撃対象のシステムにアカウントを持たない状態で実行可能な攻撃である。リモート攻撃に対する脆弱性の検出では、ネットワーク上に攻撃用のマシンを用意し、そのホストからネットワーク経由で検出対象ホストに対して疑似攻撃を行い脆弱性を検出する。

6-2. ローカル攻撃に対する脆弱性の検出

ローカル攻撃とは、攻撃対象のシステムにアカウントを持っている場合に実行可能な攻撃である。ローカル攻撃に対する脆弱性の検出では、検出対象ホストに疑似攻撃用のツールをインストールして疑似攻撃を行い脆弱性を検出する。

6-3. パスワードに対する脆弱性の検出

パスワードに対する脆弱性の検出とは、パスワードが設定されていなかったり、設定されていても推測されやすい単純なパスワードを使用しているアカウントを検出する検査である。検出方法は、パスワードファイルに対して辞書攻撃を行う方法が一般的である。辞書攻撃とは、予め用意しておいた辞書に登録されているパスワードを、アカウントに対して1つずつ適用していく方法である。また、ツールによっては、単純にワードの比較を行うだけでなく、辞書に登録されたワードを組み合わせたり、その一部を変更したりする機能や、パスワードファイルに記述されている情報を利用して、独自にパスワードを生成して辞書攻撃を行うものもある。

パスワードファイルに対する攻撃方法には、辞書攻撃の他にブルートフォースと呼ばれる手法も知られている。これはインクリメンタルに文字列を変化させてパスワード照合を

行う総当たり攻撃である。しかし、大変効率の悪い手段なので、この手法が用いられることはほとんどない。

7. バックアップ技術

バックアップ技術とは、保護対象となるデータやシステムの複製を作成するための技術である。システムの運用中には、故障や過失あるいは不正アクセスなどによって、保護対象のデータやシステムが改ざんされたり、あるいは消滅してしまうことがある。このような不測の事態に備えて、保護対象にはバックアップを用意しておかなければならない。

初期バックアップ

保護対象であるデータやシステムを最初にインストールした時に、保護対象の全ての構成のコピーを作成しておくバックアップ方法。

フルバックアップ

保護対象であるデータやシステムの全ての構成のコピーを作成する方法。初期バックアップとの違いは、フルバックアップは定期的に行われるバックアップであるということ。

インクリメンタルバックアップ

保護対象であるデータやシステムに変更があった場合、その差分についてだけコピーを作成するバックアップ方法。

8. 情報セキュリティ技術一覧表

これまでに述べた内容をもとに、情報セキュリティ技術について整理分類を行い、一覧表として以下にまとめた。情報セキュリティ技術一覧を表 付 C-1 に示す。

表 付 C-1. 情報セキュリティ技術一覧

大項目	中項目	小項目
暗号技術	秘密鍵暗号方式	
	公開鍵暗号方式	
	ハイブリッド方式	
アクセスコントロール技術	認証	IP アドレス認証方式
		公開鍵暗号認証方式
		第三者認証方式
		パスワード認証方式
		所有物認証方式
	バイオメトリクス認証方式	
	リソースパーミッション	
	フィルタリング	パケットフィルタリング プロキシサービス
侵入検出技術	ログ収集	
	改ざん検出	
	不正アクセス検出	ネットワーク検出型
		ホスト検出型
	AID	
	MID	
アンチウィルス	ユーザ起動型	
	システム常駐型	
脆弱性検出技術	リモート攻撃検出型	
	ローカル攻撃検出型	
	パスワード検出型	
バックアップ技術	初期バックアップ	
	フルバックアップ	
	インクリメンタルバックアップ	

付録 D 緊急時行動計画一覧表

サイバーテロ用の緊急時行動計画の具体例について示す。利用者は以下に示す行動計画の例から、各々の状況に適合する行動計画を適宜選択、編集しプラン策定作業に役立てることができる。各例示の解説については本文 2-3-2-4 節「緊急時行動計画の具体例」を参照のこと。

確認フェーズにおける行動計画の例

手順	行動計画
	今回のサイバーテロ対応の責任者を任命する。
	本当にサイバーテロかどうかを確認する。
	証拠を慎重に集める。
	組織の法務部門や顧問弁護士へ協力を依頼する。
	プロバイダーへの協力を依頼する。
	関係者全員と連絡をとる。
	確認フェーズレポートを作成する。

抑制フェーズにおける行動計画の例

手順	行動計画
	現場に作業チームを配置する。
	確認フェーズレポートを検証する。
	不用意な追跡を行わない。
	不用意なシステム設定の変更を行わない。
	トラップを仕掛ける。
	被害を受けたコンピュータ上のバイナリプログラムには注意する。
	コンピュータシステムのフルバックアップを作成する。
	システムの切断ポイントを決定する。
	他のシステムへの影響を調査する。
	影響のある関係者へ通知する。
	被害を受けたシステムのパスワードを変更する。
	抑制フェーズレポートを作成する。

排除フェーズにおける行動計画の例

手順	行動計画
	サイバーテロが行われたプロセスを明らかにする。
	疑似攻撃を行う。
	サイバーテロの原因を排除する。
	脆弱性分析作業の結果を他のシステムにも反映する。
	最新でクリーンなバックアップデータを探す。
	適切なセキュリティ機能を導入する。
	排除フェーズレポートを作成する。

回復フェーズにおける行動計画の例

手順	行動計画
	システムをバックアップデータから復元する。
	システムテストによって作業結果を確認する。
	業務回復を関係者に通知する。
	稼働後のシステム監視を実行する。
	回復フェーズレポートを作成する。

フォローアップフェーズにおける行動計画の例

手順	行動計画
	一連の対応作業をまとめた報告書を作成する。
	報告書のレビューを行う。
	改善提案を実現する。

不正コード攻撃に応じた行動計画の例

手順	行動計画
	ウィルスチェックを行う。
	システムから発信されるパケットを監視する。

不正アクセスに応じた行動計画の例

手順	行動計画
	ネットワーク間のフィルタリングルールを確認する。
	ネットワークサービスのアクセスログを確認する。
	検査ツールによってシステムに存在する弱点を明確にする。
	被害状況を明確にする。

サービス妨害に応じた行動計画の例

手順	行動計画
	アドホックにフィルタリングルールを設定する。
	外部機関と連携する。

風説の流布に応じた行動計画の例

手順	行動計画
	デマに関する情報を収集し関係者に通達する。
	組織としての見解を表明する。

システム探査に応じた行動計画の例

手順	行動計画
	組織のインシデントレスポンスチームに報告をする。
	被害を正確に見積もる。

参考資料

- [1] FIPS PUB87 Guidelines For ADP Contingency Planning
U.S. Department of Commerce 1981
- [2] Guidelines for Contingency Plan Development
U.S. Fish and Wildlife Service 1998
- [3] Disaster Recovery Planning Encourages Better Management Decisions
M. E. Kabay, Ph.D. ICSA 1996
- [4] Information Security Policies Made Easy
Charles Cresson Wood, BASELINE software 1997
- [5] NIST SP 800-12 An Introduction to Computer Security
National Institute of Standards and Technology 1995
- [6] NAVSO P-5239-19 Computer Incident Response Guidebook
U.S. Department of The Navy 1996
- [7] Computer Security Incident Handling
The SANS Institute 1998
- [8] NRL IS Security Incident Response Plan
Naval Research Laboratory 1995
- [9] Coping with the Threat of Computer Security Incidents A Primer from Prevention through Recovery
Russell L. Brand 1990
- [10] NSWC Dahlgren Computer Security Incident Handling Procedure
Stephen Northcutt 1996
- [11] Handbook for Computer Security Incident Response Teams(CSIRTs)
Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski CMU/SEI-98-HB-001 1998
- [12] Responding to Intrusions
CERT Coordination Center 1999
- [13] Detecting Signs of Intrusion
CERT Coordination Center 1997
- [14] Preparing to Detect Signs of Intrusion
CERT Coordination Center 1998
- [15] Intruder Detection Checklist
CERT Coordination Center 1997
- [16] Steps for Recovering from a UNIX Root Compromise
CERT Coordination Center 1998
- [17] Forming an Incident Response Team
Danny Smith, Australian Computer Emergency Response Team 1994
- [18] What Is Information Warfare?
Martin Libicki National Defense University 1995
- [19] Results of the Distributed-Systems Intruder Tools Workshop
CERT Coordination Center, Software Engineering University, Carnegie Mellon University 1999
- [20] Intrusion Detection FAQ
The SANS Institute 1999
- [21] To Build A Honeytrap
Lance Spitzner 1999
- [22] 【コンピュータ西暦 2000 年問題】企業のための危機管理計画策定の手引き
高度情報通信社会推進本部 コンピュータ西暦 2000 年対策推進会議 1999
- [23] コンピュータセキュリティインシデントへの対応
JPCERT/CC 1999