

「新しいタイプの攻撃」の対策 に向けた設計・運用ガイド

改訂第2版

新しい脅威に立ち向かうための
安全性向上のための取り組み



IPA

独立行政法人 情報処理推進機構
セキュリティセンター

2011年11月

本書は、以下の URL からダウンロードできます。

「新しいタイプの攻撃」の対策に向けた設計・運用ガイド

<http://www.ipa.go.jp/security/vuln/newattack.html>

目次

目次.....	1
はじめに	2
本書の内容および位置付け	2
対象読者.....	2
1. エグゼクティブサマリ	3
1.1 組織への影響は何か	3
1.2 対策の考え方	3
2. 「新しいタイプの攻撃」の問題と背景.....	5
2.1 「新しいタイプの攻撃」とは.....	5
2.2 「標的型攻撃」の意味合いと整理.....	6
2.3 新しいタイプの攻撃の動作.....	11
2.4 「入口対策」ではできないこと	12
2.5 対策の考え方を再整理.....	13
3. 「新しいタイプの攻撃」の動作と問題整理.....	15
3.1 「新しいタイプの攻撃」の流れ	15
3.2 攻撃仕様の分析と整理.....	19
3.3 バックドア通信の種類（2011 年調査時点）	22
4. 新しい脅威に立ち向かうポイント.....	23
4.1 新たな対策発想で考える	23
4.2 入口対策と出口対策.....	25
4.3 「出口対策」の実現方法	26
4.4 バックドアへの設計における効果と課題.....	29
4.5 大切な情報をサイバー攻撃により漏洩させない8つの対策.....	30
付録1：実装項目における実証結果	47
付録2：対策要件定義テンプレート	51
付録3：情報セキュリティ対策の整理.....	57

はじめに

近年、メールや USB メモリ等の外部メディアを介した攻撃によって、組織の知財情報や個人情報などを窃取されるという事件が起きています。窃取された情報(製品の設計情報など)は組織にとって非常に重要な情報であり、一般的には外部からたどり着けないと思われる場所に保存されています。しかし、このような最近の攻撃では、たどり着けないと思われていた内部システムから重要な情報を窃取されてしまっています。

これらの攻撃は、組織がセキュリティ対策に無考慮であるために発生しているわけではなく、非常に巧妙で、一定のセキュリティ対策を行った組織であっても被害を受けていることが確認されています。このような攻撃の一部は、海外では APT(Advanced Persistent Threats)などと呼ばれることもあります。IPA ではこの攻撃を「新しいタイプの攻撃」と呼んでいます。

インターネットからの攻撃を防ぐことを考えた場合、その攻撃をファイアウォールやウイルス対策ソフトなどによって、組織のシステムに入り込まないように入口で防ぐことは重要な考え方です。しかし、これらの入口対策だけでは、組織内部の端末がウイルスに感染するなどの攻撃が成功してしまった場合、更なる情報窃取を行っている攻撃には有効に働かないことがあります。

重要な情報を窃取され、損失を起こさないためにも、ウイルスに感染することを前提とした対策を考える必要があります。ウイルスから攻撃者に送信する情報は、組織のネットワークを通過して外に出ます。この組織のネットワークから外に出ないようにする出口の対策が重要になります。出口対策では、ネットワーク設計や運用における防御が重要です。入口で何を防ぎ、出口で何を防ぐかということを適切に設計しておく必要があります。

本書は「新しいタイプの攻撃」の実態と、それに立ち向かうためのネットワークやシステムの設計方法および運用方法を提供します。

本書が、「新しいタイプの攻撃」のセキュリティ問題を解決する一助となれば幸いです。

本書の内容および位置付け

IPA「脅威と対策研究会」は 2010 年 12 月にテクニカルウォッチ Vol1「新しいタイプの攻撃」を発表し、これらの攻撃に対しての有効な対策を継続して検討しています。本資料は本研究会において「ウイルスの解析をしている者」と「ネットワークシステム設計を行う者」の双方が意見交換し、組織においてどのような対策が有効であるかを導き出されたネットワークシステム対策を紹介しています。

本書に示す内容は、あくまで解決策の一例であり、必ずしもこれらの実施を全て求めるものではありません。「新しいタイプの攻撃」へのセキュリティ問題の解決の参考にいただければ幸いです。

対象読者

本書では、対象読者が章ごとに次のように分かれています。

第 1 章: 経営者層等「新しいタイプの攻撃」に対して脅威を知り、経営面からの投資を判断する方々。

第 2 章: 「新しいタイプの攻撃」への対策の提案・指示等を行うプロジェクトを管理する方々。

第 3 章以降: 実際に「新しいタイプの攻撃」に対する対策を実施する方々。

1. エグゼクティブサマリ

情報セキュリティの対策を実施する際には、どのような攻撃から何を守るのかを明確にすることが肝要です。本書は、組織の深部にある情報まで窃取されてしまう「新しいタイプの攻撃」に対してどのようなアプローチで対策を導き出すかを示すガイドになっています。

1.1 組織への影響は何か

サイバー攻撃は、日々変遷しています。2000 年頃よりサイバー攻撃が目立ってきました。当時の攻撃は、攻撃しやすい公開されているサーバ等を狙った攻撃が行われていました。その結果、ウェブサイトの改ざんの被害や、ウイルスの蔓延というような被害が発生していました。これは、攻撃を単独の攻撃者が行っており、いたずら等の目的で行われていました。これらの攻撃に対して、組織ではファイアウォールやウイルス対策ソフトの導入、脆弱性対策など、外部から組織に入り込まれないような対策(入口対策)を行ってきました。

しかし、昨今の攻撃者はサイバー攻撃をビジネスとして行っており、組織的な攻撃をとなり、ソーシャルエンジニアリング¹やゼロデイ²の脆弱性などの手口を利用し、非常に巧妙で、攻撃が行われていることを発覚させない手口を使用しています。その結果、組織の知財や個人情報などの重要な情報を窃取されることや、組織の重要システムを破壊されてしまうことが行われます。しかも、従来入り込まれることはないであろう組織の深部で管理しているような重要情報が窃取される事案が顕在化しています。

1.2 対策の考え方

IPA「脅威と対策研究会」では、ウイルス解析等を中心の業務としている専門家と、組織のシステムやネットワークを設計、運用することを中心の業務としている専門家が密接に情報共有し、連携することで、攻撃が組織内の現実のシステムやネットワークでどのように動作するかを解析し、組織での有効な対策を考察しました。

攻撃を解析する専門家とシステム全体を設計・運用する専門家と連携することで、現実の組織において攻撃からどのように守ると効果的であるかを詳細に検討することができます。

それぞれの専門家は攻撃の全容とシステムの全容の全てを把握しているわけではありません。攻撃を解析する専門家は、その攻撃がどのように行われるか、攻撃を防ぐためにはどのようにする方法があるのか、という目で解析を行います。しかし、実際にシステム全体に対策を実施するために、どの程度効果的で、どの程度現実的であるのか、仮に対策をすり抜けてしまった場合は何が起こるのかまで解析しきれていないこともあるでしょう。それは、攻撃を解析する専門家では、現実組織のシステムの全容が把握しきれていないことがあります。また、システム設計・運用する専門家は、攻撃を解析する専門家の対策を鵜呑みにしがちになり、場合によってはシステムの全容にはそぐわないコストをかけ過ぎた対策を実施してしまいます。

このような対策の考え方は、「新しいタイプの攻撃」だけに有効なものではありません。更に巧妙な攻撃が今後行われた場合においても、各専門家間で連携をすることによる効果的な対策を打ち出すことに

¹ 話術や盗み聞き・盗み見等を利用し、人間の心理・行動の隙を突くことで情報を不正に取得する手段の総称。

² 対策版が公表されていない未知の状態の脆弱性

有効と考えています。

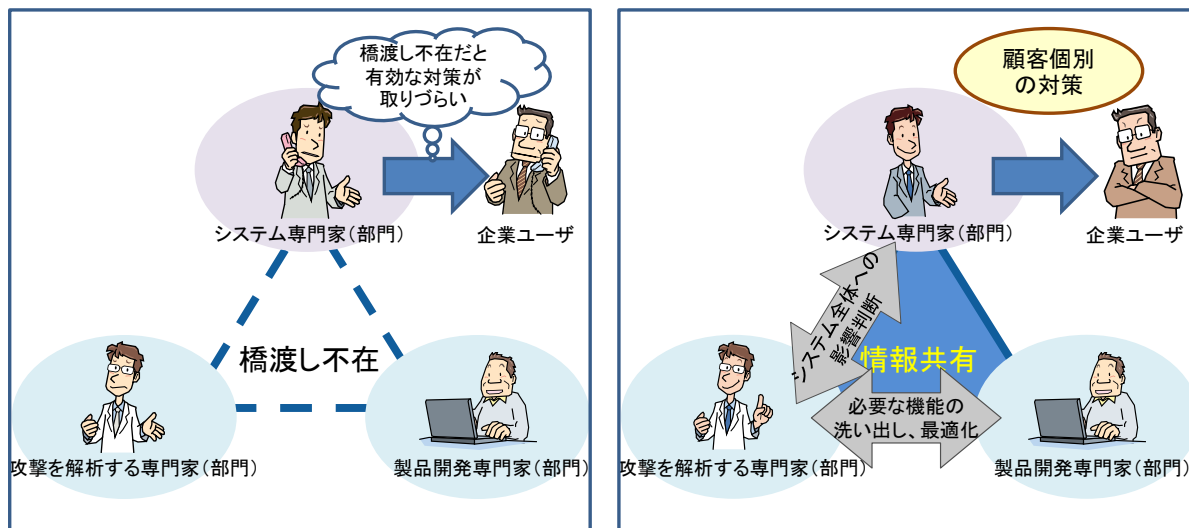


図 1-1: 橋渡しの効果イメージ

IPA「脅威と対策研究会」では、このような考えの下「新しいタイプの攻撃」の対策を検討しました。そして、その中で「新しいタイプの攻撃」には、ウイルスが攻撃者と通信を行う等の共通攻撃手法があることに着目しました。そして、従来の攻撃を防ぐための入口対策と、たとえ組織の中に攻撃の一部が入り込まれたとしても、共通攻撃手法部分を止め、外部にいる攻撃者に情報を窃取されないための対策(出口対策)が必要であると考察しました。組織の対策として、この出口対策を浸透していくことが重要になります。

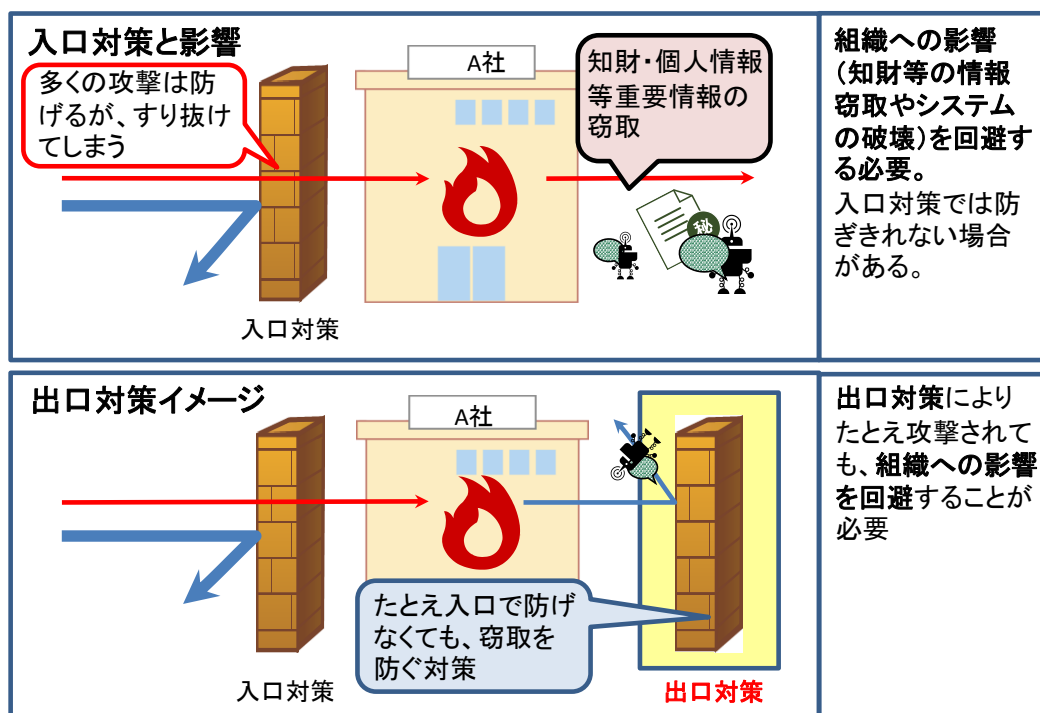


図 1-2: 入口対策と出口対策のイメージ図

2. 「新しいタイプの攻撃」の問題と背景

2.1 「新しいタイプの攻撃」とは

インターネット上では、毎日のように様々な攻撃が行われています。例えば、SQL インジェクションのようなウェブアプリケーションの脆弱性やサーバソフトウェアの脆弱性を悪用して、サーバ内の個人情報を取得するような攻撃や、悪意あるリンクをクリックすることでユーザから金銭を騙し取ろうとするフィッシング詐欺、利用者の端末に対して強制的に偽のウイルス対策ソフトを利用者にインストールさせるような攻撃など様々なものがあります。

近年、その中でも特に巧妙に行われている攻撃があります。それは標的型攻撃に代表される、メールや外部メディア等で組織内部の従業員（組織の幹部を含む）の端末に入り込むような攻撃です。この攻撃は、そこから組織の内部へ更に入り込んでいき、最終的に組織にとって非常に重要な情報（知財情報や個人情報）が知らぬ間に盗み出されるような事態に陥るものです。

従来、一定のセキュリティ対策を施していれば組織の内部まで入り込まれないであろうと考えられていました。しかし、標的型攻撃のような攻撃では組織のシステムの内部まで入り込まれてしまいます。これは、これらの攻撃は対策の状況に合わせて持続的に攻撃が続けられ、少しずつ目的の情報に迫るため、従来行っている対策をすり抜けてしまうためです。その結果、知財など組織にとっての非常に重要な情報を盗み出したり、組織の重要なシステムを破壊したりするような攻撃の事例が顕在化しています。海外ではこのような攻撃の一部を「Advanced Persistent Threats(APT)」等と呼んでいます。IPA ではこのような攻撃に対して「新しいタイプの攻撃」と呼んでいます。この「新しいタイプの攻撃」は、従来の対策が効かないような共通攻撃手法と、組織に特化する攻撃である個別攻撃手法で構成されています。この内共通攻撃手法が、対策としてキーワードになってきます。

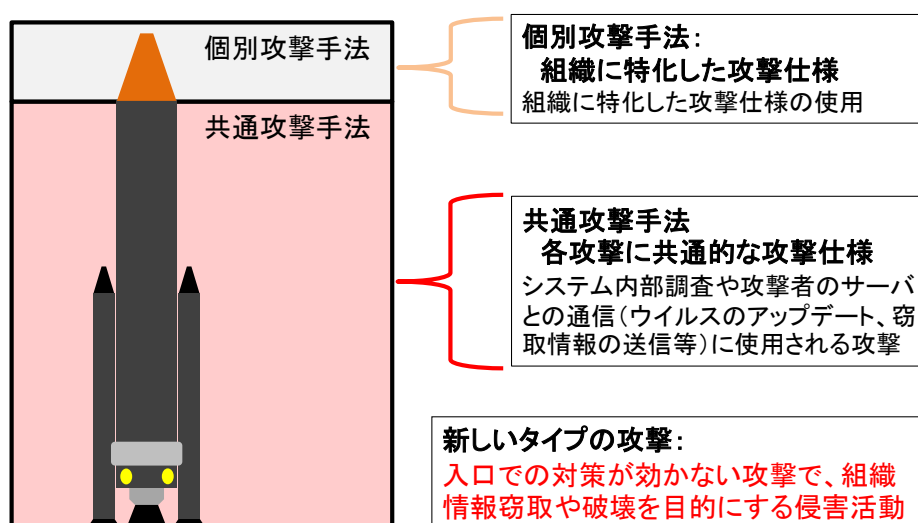


図 2-1: 「新しいタイプの攻撃」の概念

2.2「標的型攻撃」の意味合いと整理

「新しいタイプの攻撃」には標的型攻撃も含まれます。しかし、一口に標的型攻撃と言っても、その実態や意味合いにより様々なパターンが存在します。システムの設計対策を考える場合には、標的型攻撃を分類しそれぞれに応じた対策を考える必要があります。意味合いを間違えると、コスト的にも効果的にも意味のない対策を講ずる事に繋がり、問題解決に至らない事もあります。このため、本章では標的型攻撃の分類整理を行い、取るべき対策分野との関連性を整理します。

また、各種検討・調整の場において、何の問題を議論しているのかを明確にし、同じ問題認識の上で実のある対策効果に繋げ、攻撃耐性を上げるためにも、サイバーセキュリティ分野における標的型攻撃の位置付けと分類を基に検討を行うことが重要です。

このため、本ガイドでは標的型攻撃をその特徴等から2種類に分類しています。

2.2.1「標的型攻撃」の分類

標的型メール部分のみでなく全体の動作や意図性等の特徴から分類すると、標的型攻撃には以下の2種類が存在します。これらは、標的型メール本文のみでの判別でなく、意図や動作並びに攻撃活動全体から違いを判断すべきものです。

標的型諜報攻撃(APT)

国の経済や安全保障等に影響を及ぼす組織情報を窃取する活動を背景にし、特定目標組織を継続的に情報偵察する一連の攻撃。米国等で行われている「APT」は、この攻撃パターンの事。

不特定目標攻撃

不特定目標に対し、主に金銭目的のために個人情報などを窃取する攻撃。

また、「標的型諜報攻撃(APT)」にはその攻撃段階によって「情報偵察等攻撃」と、より高度で発見しにくい攻撃である「特定目標攻撃」が存在していると思われます。「情報偵察等攻撃」で用いられる標的型メールの中にはわざと発見させてアンチウイルスによる使い捨てウイルスの駆除を意図している可能性もあります。

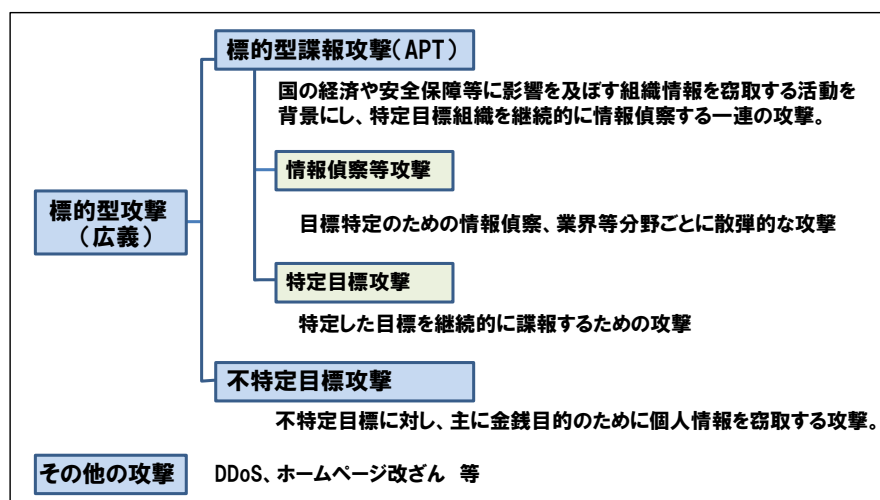


図 2-2-1-1:「標的型攻撃」の分類

2.2.2 標的型諜報攻撃の全体概念と特徴

「標的型諜報攻撃(APT)」では、周辺組織等への入念な事前情報偵察のもと、目標の選定と攻撃の準備を行います。この段階で、攻撃に用いるメール本文やメールアドレスなどを取得し、目標組織への攻撃に用いる標的型メールや攻撃ウイルス等の準備を行います。

その上で、システムの入口を突破するための標的型メールを用い、システムにバックドアを開通した後、バックドアを用いたリモートコントロールにより継続的に同一組織の情報諜報を行います。この攻撃パターンの特徴は、「特定の意図を持ち、同一目標に対する段階的な一連の攻撃(諜報)活動を行う」ことにあると言えます。また、組織内のUSBメモリ等の運用を計算にいたしたウイルスの使用により、クローズ系の情報も諜報対象にしています。

様々なサイバー攻撃の中でも、もっとも危険でかつ対策が困難な攻撃パターンであり、特定の業界、分野がその攻撃対象となります。国内外防衛産業、政府等サイバー攻撃事案はこれに該当し、これら一連の攻撃活動全体を指して「標的型諜報攻撃(APT)」と呼びます。

この攻撃では、不審なメール、ウイルス感染という視点ではなく、攻撃対象システムへの継続的ハッキングという部分に着目する事が重要で、組織における“人”、“システム”、“業務フロー”のバランスを根底から崩す攻撃と捉える必要があります。また、「標的型諜報攻撃(APT)」に対しては、従来の入口(既存)対策では攻撃の発見や防止を完璧に実施することが難しいため、情報が漏出されるのを止める出口対策が必要です。

「標的型諜報攻撃(APT)」に関しては、その背景や意図、全体としての特徴、組織や社会への影響判断やコスト見積りの上で対策優先度を判断する事になります。このため、従来の技術を中心としているCSIRT(Computer Security Incident Response Team)の対応方法も再考する事になると思われます。

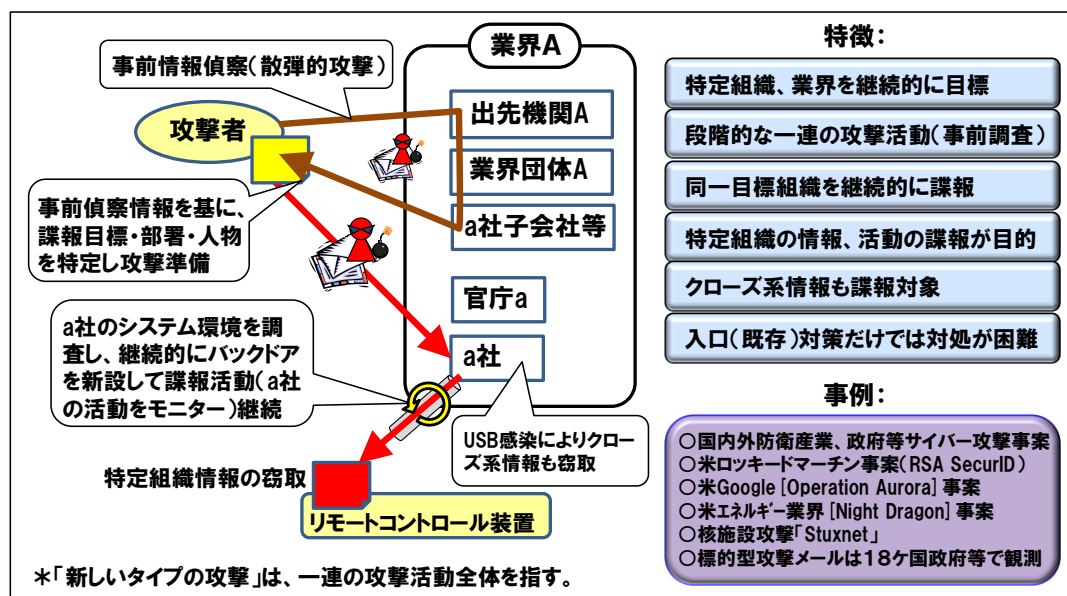


図 2-2-2-1:「標的型諜報攻撃(APT)」の全体概念と特徴

「標的型諜報攻撃(APT)」の全体攻撃シーケンス詳細を以下に示します。2005 年頃から顕在化し、世界各国で観測されている攻撃ですが、意図と動機「誰がなんの為に行っているか？」は未だに判明していません。最近の特徴としては、事前準備段階で関係団体や地方機関等への情報偵察で入手したメール本体、アドレス等を基にリモートコントロールツール(RAT: Remote Access Trojan/Remote Administration Tool)を仕込んだ標的型メールでシステム入口防御網を突破した後に、外部からのリモー

トコントロールにより目標とする組織端末の(メール等)情報及びシステム内部を搜索するケースが見られます。

また、従来からある手法としては、標的型メールでウイルスを送り込み、外部へのバックドアを開設し指示により情報を探索したり探索プログラムを更新したりするケースがあります。いずれも、同一組織内を継続的に諜報する事が可能な攻撃手段です。

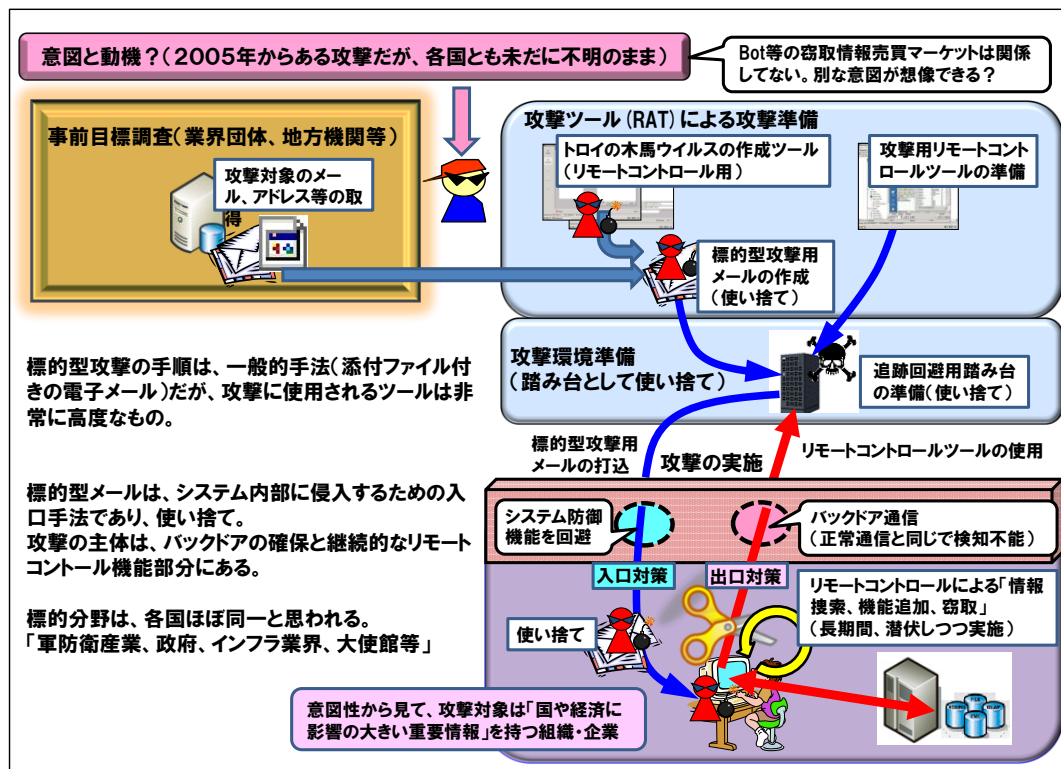


図 2-2-2-2:「標的型諜報攻撃(APT)」の全体攻撃シーケンス詳細

2.2.3 不特定目標攻撃の全体概念と特徴

不審メールが届くため「標的型諜報攻撃(APT)」と混同されやすいのがこの攻撃です。「不特定目標攻撃」の特徴は、目標が無作為(不特定多数)である事と目的が個人情報、金銭情報の取得にあるため、攻撃自体が単発である事にあります。無作為攻撃の結果として企業等アドレスへ到達する事がありますが、組織を対象にした攻撃とは別なものと考えていいでしょう。

不審メール本体からでは、「標的型諜報攻撃(APT)」との差を判断する事が難しいケースもありますが、攻撃活動全体から判断して「標的型諜報攻撃(APT)」とは別物として考える方が、「不特定目標攻撃」に対する有効な設計対策を判断しやすくなります。

「不特定目標攻撃」は、その意図背景から見て、国家や経済に多大な影響を及ぼす情報の窃取ではないため危険度や組織問題の視点で考えた場合、「標的型諜報攻撃(APT)」とは別な攻撃になります。また、「不特定目標攻撃」は従来の入口(既存)対策で対処ができることが多いです。攻撃事例としては、ボットウイルス付迷惑メール(SpyEye 等)、銀行認証番号を盗むフィッシングメール、フィッシング(偽)サイト誘導メール、Web サイトへの SQL インジェクション等が該当します。

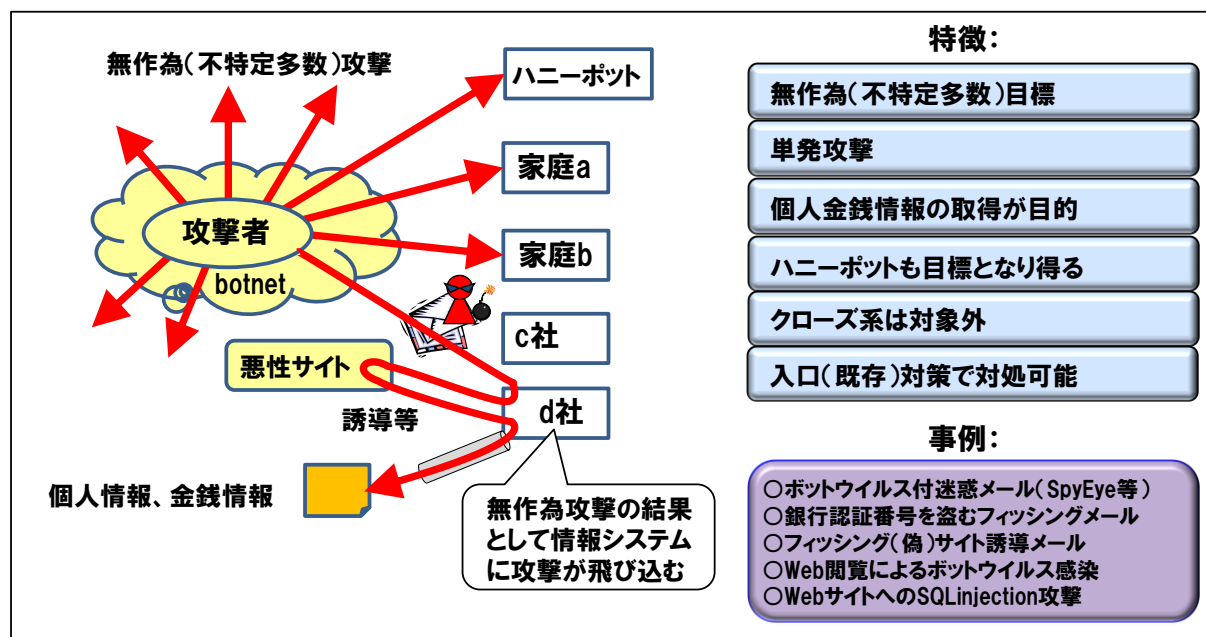


図 2-2-3-1:「不特定目標攻撃」の全体概念と特徴

2.2.4 情報セキュリティ各分野の分類と各対策の関係

情報セキュリティ各分野全体における「標的型諜報攻撃(APT)」の関係について整理すると下図のようになります。サイバー攻撃問題と情報漏洩等の情報管理問題は問題の質と対策が異なるため、分けて考える必要があります。また、サイバー攻撃は多種多様な事案が発生するため、どの攻撃パターンに対する対策なのか、何を守ろうとしているのかを明確にした上で、対策を考える必要があります。例えば、組織(情報システム)の問題と、家庭で利用されるPCの問題では自ずと対策が違ってきます。

特に、ここで取り上げている「標的型諜報攻撃(APT)」は、継続的な情報窃取等により、組織に対する重大な影響を与えることに加え、対策と発見が難しい攻撃であることから、組織の問題として取り組む必要があります。

「不特定目標攻撃」を念頭に置いた対策だけでは、「標的型諜報攻撃(APT)」の対策とはならない点にも注意が必要です。「標的型諜報攻撃(APT)」への対策を検討するにあたっては、自組織に対して「標的型諜報攻撃(APT)」が行われた際の影響を評価し、どのような対策を、どこまで行うのかについて、コスト面を含めた現実的に検討を行う必要があります。特に注意が必要なのは、単にサイバー攻撃対処として捉えるのではなく、自組織の特性を鑑みた、精度の高い判断が必要となる点です。この判断を誤ると、コストだけが増加し、効果が得られない結果になってしまいます。

標的型攻撃以外のサイバー攻撃及び「不特定目標攻撃」は、基本的に従来(入口)対策でカバーできる部分が多いのですが、「標的型諜報攻撃(APT)」は、特に危険で発見や対策が難しいことから、情報窃取を防ぎ、諜報的な活動を検知するための出口対策が必要となります。

本ガイドで示す「新しいタイプの攻撃と設計対策」は、情報システムへの「標的型諜報攻撃(APT)」を対象にしたシステム設計対策検討に繋がるように整理したのですが、「不特定目標攻撃」は、「標的型諜報攻撃(APT)」と共通した機能を有する物も少ないため、「不特定目標攻撃」に対しても、有効な対策に繋がります。

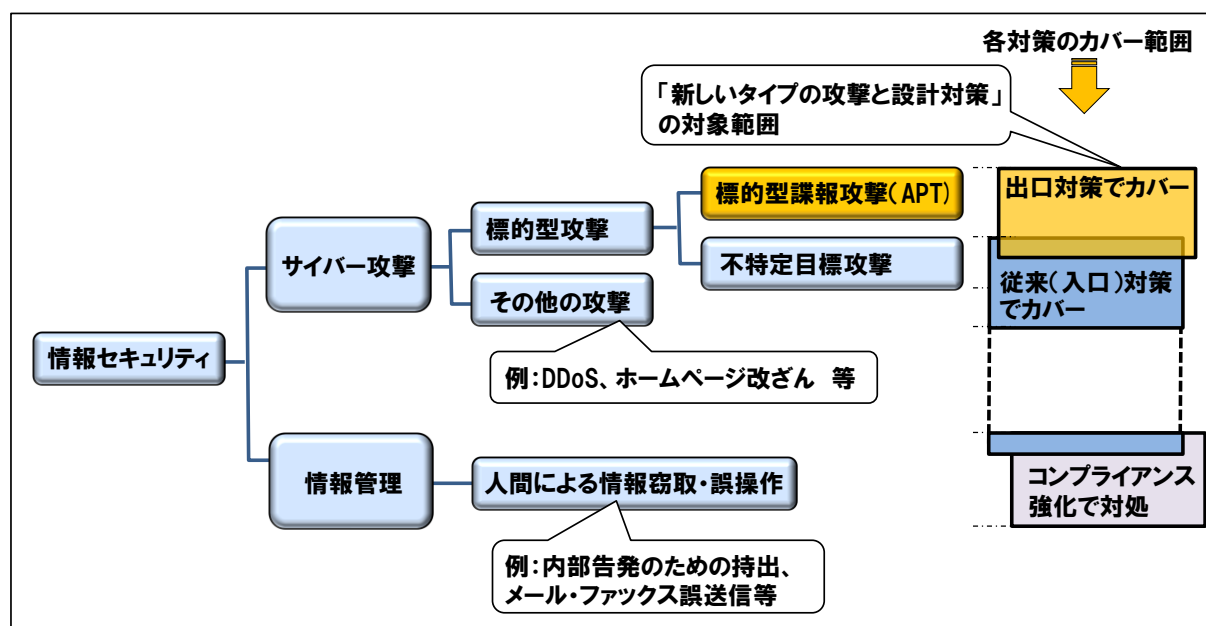


図 2-2-4-1: 情報セキュリティ各分野の分類と各対策の関係

2.3 新しいタイプの攻撃の動作

「新しいタイプの攻撃」がもたらしている影響には、知らぬ間に内部の重要な文書等を盗み出されることが挙げられます。このような攻撃の典型例では企業内で次のように攻撃が進行します。この流れにおける「③攻撃基盤構築段階」および「④システム調査段階」が共通攻撃手法に該当します。

① 攻撃準備段階

標的の情報を盗む前の準備段階として、標的の組織に関係のある組織へ攻撃を行います。そして、そこで得られたメールなどの情報を活用します。

② 初期潜入段階

準備段階で得られた情報を利用して組織内の特定のメールアドレスに対して、関係者を装ったメールを送付されます。添付されているファイルがウイルスでウイルス対策ソフトでは検知できない未知のウイルスです。ここで、ウイルスに感染してしまうことで次の段階に移行します。

③ 攻撃基盤構築段階

ウイルスは、更なるウイルスをダウンロードし、攻撃者と感染したウイルスが通信できるような環境を構築します。具体的には、組織の業務で使っている HTTP の通信を模倣してやり取りを行い、攻撃者とウイルスが通信できるようにします（バックドア通信）。

④ システム調査段階

ここでは、ウイルスが内部のシステムから情報を探します。この動作は数週間から数か月にわたり長い間組織のシステムに存在し、何度となく攻撃者とやり取りをして実施されることがあります。組織に併せたウイルスのアップデート等も行われます。

⑤ 攻撃最終目標の遂行段階

組織の知財などの重要情報を窃取し攻撃者へ送付します。また、取得した組織の内部情報（組織内のアカウント情報等）を利用して更なる攻撃を加える場合もあります。

攻撃者はこの流れにおいて攻撃最終目標の有用な資料を盗むために、何度となく攻撃者とウイルスがやり取りし、組織に特化して重要な情報を盗み出そうとします。このような標的型攻撃メールで盗まれた事例が日本や海外では発生しています。その中にはセキュリティ製品の重要情報や政府の重要情報を狙われた事例もあります。

また、このような攻撃はメールだけではなくありません。他にも USB 等の外部メディアを攻撃の入り口とした例もあります。USB 等の外部メディアを利用した攻撃では、インターネットにつながれていない端末で通常、外部から攻撃されないであろうと思われた箇所まで入り込んでいます。例えば Conficker(コンフィッカー)や Stuxnet(スタックスネット)の事例では外部メディアが使われています。

標的型攻撃や USB メモリ等を利用した攻撃に関しては、たとえ対策を実施していてもすり抜けてしまう場合があります。これは、受け取ったメールや USB メモリ等が被害を及ぼすものであると、受け取った側が分からないことが通常です。

そのため、攻撃を受けたことに全く気が付かないまま、企業の主力製品等の機密文書を盗み出されてしまい、それを悪用され、競争力の低下など損失に直結してしまう事態になってしまいます。

2.4「入口対策」ではできないこと

昨今組織においてセキュリティ対策が行われているのは当たり前になっています。しかし、このように対策をしているにもかかわらず、「新しいタイプの攻撃」において、組織のセキュリティ対策が有効に働かないことがあります。それは対策の多くが、外部からの攻撃を入口の部分で防ぐことを目的としているためです。攻撃を入口で未然に無効にするような対策を本書では「入口対策」と呼びます。

組織において、ウェブやメールなどを頻繁に使用します。「新しいタイプの攻撃」では、組織の内部に入り込むために、ウェブやメールなどを攻撃に利用します。もちろんこれらの攻撃への「入口対策」として、従来からファイアウォールや侵入検知システム、ウイルス対策ソフトの導入、パッチ適用による脆弱性対策等が行われています。

しかし、このような「入口対策」だけで十分ではありません。それは、入口からだけでは攻撃を防げない場合もあるためです。例えば、ゼロデイの脆弱性を狙った標的型攻撃のメールにおいては、そのメールに添付されているファイルがウイルスであったとした場合、ウイルス対策ソフトがそのウイルスを検知できない場合はウイルスに感染してしまいます。また、ウイルス対策ソフトについても、全てのウイルスを検知でき検知できるとは限りません。攻撃者は検出状況を確認し、検出されないファイルを作成してから攻撃を開始するためです。パッチ適用による脆弱性対策を行っても、ゼロデイの脆弱性を狙われた場合には有効ではありません。また、ゼロデイではなくても、攻撃者が組織で使用している多種多様のソフトウェアの脆弱性を狙っています。組織の中では全てのソフトウェアの脆弱性対策を実施することが難しくなっています。更に、ウイルスに備わっている通信機能は、ウェブで使う通信などを使用するため、流れている通信から異常を検知することは困難です。

そのため全ての対策をすり抜けられた場合、攻撃が成功してしまうことになります。もちろん、入口部でこれらの製品の導入・対策の実施を行うことで、攻撃の成功率を相当数下げることができます。これらの対策を実施しなければ、既知のウイルスや既知の脆弱性を悪用するようなウイルスですら攻撃が成立してしまいます。このように「入口対策」は重要ではあるものの、「入口対策」では防げない場合が存在します。その結果、組織の重要な情報を盗まれるような事態に陥ってしまいます。

表 2-4: 入口での対策の限界箇所

項目	入口での対策の限界箇所
ウイルスの種類の多様化	ウイルス対策ソフトでは、数多くのウイルスの全てを検知できるわけではない
ゼロデイ脆弱性が狙われる	パッチ運用を実施していても、攻撃が成立してしまう
多種のソフトウェアの脆弱性を狙われる	パッチ運用において、適応すべきパッチの種類が多すぎて管理できない場合がある
攻撃が成功した場合の攻撃者とウイルスとの通信	業務で使う通信経路を使い、通常の通信と悪意ある通信が区別できない

2.5 対策の考え方を再整理

2.4 章のように、「入口対策」では限界があります。したがって、入口以外の対策を実施することが必要になります。対策を実施する際には、攻撃による組織への損失を考慮しなければなりません。何が発生すると組織にとって損失が出てしまうのかを考えると、2.3 のように組織にとっての機密情報が外部に漏れるということや、重要なシステムを停止されることが損失につながると言えるでしょう。

「新しいタイプの攻撃」への対策を考えると、機密情報を攻撃者に渡さない、重要システムを操作させる機会を与えないことが対策に繋がります。この対策を考える際に、ポイントとなるのは、組織に入り込んだウイルスがどのような動作を行うかになります。

組織に入り込んだウイルスは、攻撃者に対して何らかの情報を送信します。この通信は、ウイルス自身が組織に入り込んだ状態であること通知することや、どのような情報が存在するのか、どのようなウイルスへアップデートすれば攻撃が有効になるのか、ということを攻撃者に通知するために行っていると考えられます。

組織への影響を回避するため、対策の考え方としては、これらの外部への通信を止めることで、結果的に攻撃者へ情報は渡らず、攻撃を不成立にすることができます。したがって、攻撃者が意図している通信を止め、組織への影響を回避するような出口対策をすることが重要になります。具体的な対策については、4 章で記載しています。

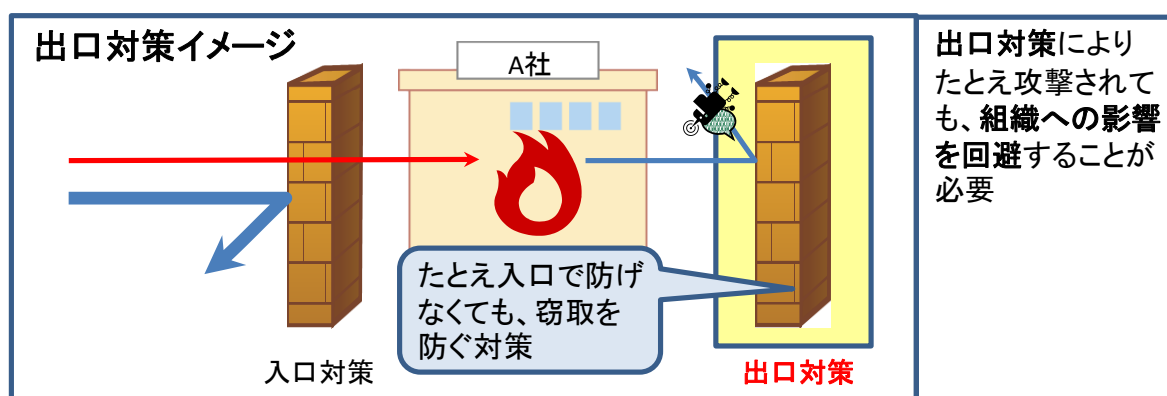


図 2-5: 出口対策イメージ

本書における「新しいタイプの攻撃」に限らず、進化していく攻撃においては、組織のシステム全体を見渡す部署と脅威実態を把握している部署とが連携し、組織への影響を分析する必要があります。そして、必要な対策を実施することが重要になります。また、実際の対策に当たって最も重要な点ですが、適切に運用できることで初めて有効に機能するものです。有効な対策を施すために、運用ができる対策を検討しましょう。

プロジェクト管理者は、対策を検討する際に、組織のシステムが「新しいタイプの攻撃」にどの程度対応できるかを見極める必要があります。そのために、まずは担当者が本脅威を理解しているかを把握し、理解していなければ、3 章以降を理解させる必要があります。その後、具体的な脅威を防げるかどうかの調査を指示します。その調査結果に基づいて、組織への影響を分析し、対策を実施すべきかどうかを判断することになります。

＜クローズ系システムへの対策の考え方の整理＞

製造業や金融業等では、インターネットに接続できるオープン系のシステムとインターネットには直接接続しないクローズ系のシステムがあります。このようなクローズ系システムにおいても、「新しいタイプの攻撃」における影響も考える必要があります。クローズ系システムは、インターネットには直接接続しないものの、USB 等の外部メディアでデータのやり取りを行います。攻撃者はそこに着目していると考えられます。

攻撃者はオープン系システムでウイルスに感染させ USB メモリ等に紛れ込ませます。その USB メモリ等を組織の人間がクローズ系システムに差し込むことで、クローズ系システムに対してもウイルスに感染することになります。そして、そのウイルスがクローズ系の情報を抜き取り、再び USB メモリ等がオープン系システムに差し込まれることによって、その情報を攻撃者に送られてしまいます。そのため、「クローズ系システムだから安全」と考えることは誤りです。

しかし、このような USB メモリ等の運用を業務で行っている以上、USB メモリ等の利用を禁止するわけにはいきません。そのため、クローズ系システムの情報を守るためにおいても、オープン系システムから情報を窃取されないようにする対策を考える必要があります。

情報窃取に関わるこれらの活動はオープン系システムを介して行われます。オープン系システムでの出口対策を行うことで攻撃者はクローズ系システムの情報を窃取することはできず、組織への影響は回避可能となるという考え方です。

＜対策のための予算の考え方の整理＞

サイバー攻撃事案は日々出現します。これに対し入口対策を追加していくと導入コストや管理コストは上がります。同じような対策をいくら厚くしても効果には限界が出てきます。攻撃の最終目的である情報の窃取と情報破壊の目的は変わりません。また、そのための共通的な攻撃仕様は 2011 年現在、大きな変化を見せません。これは情報を窃取するためには、必ず攻撃サーバとシステム深部に侵入した攻撃基盤との通信が不可欠なためだと言えます。

このため、対策は実害を回避するための出口対策により、システムの設計で対策をなす発想で考える事が重要です。対策はシステム全体経費のバランスの中で、実現可否判断に応じた必要かつ有効な対策を選択するアプローチを取る必要があります。

3. 「新しいタイプの攻撃」の動作と問題整理

本章では、「新しいタイプの攻撃」の特徴や攻撃パターンなどを具体的に説明していきます。

従来、サイバーセキュリティ(攻撃)を考える場合、どこの企業でどのような攻撃の結果、情報を窃取されたなど、その事案(インシデント)個々に着目してしまう傾向にありました。ここでは、これらを個々に考えるのではなく、共通的な動作とは何かについて考えてみましょう。この視点は、4章で対策を考える際に役に立つアプローチです。

3.1 「新しいタイプの攻撃」の流れ

「新しいタイプの攻撃」における侵入の流れを具体的に見ていきます。組織への侵入は、計画された4段階に分けて行われます。組織への侵入は情報の窃取などを目的としており、攻撃対象は当該組織の情報システムとなります。

第0段階: 攻撃準備段階

標的の情報を盗む前の準備段階として、標的の組織の情報を事前に調査します。そのために、標的の組織に関係のある組織へ攻撃を行い、初期潜入の基となる組織間でやり取りをしたメールなどの情報を収集します。これを利用して、標的の組織への初期潜入を成功率を上げるための攻撃を行います。

第1段階: 初期潜入段階

初期潜入段階においては、各種攻撃手法が使われます。不審(標的型)メールも一つの手段です。ここでの手法は組織深部にウイルスを送り込むために用いられますが、組織内で一人の社員がメールを開封するだけで目的は達します。初期潜入段階では、多数のシステムに感染させる必要はありません。また、この段階での攻撃手法は使い捨てであり、発見され駆除される事を想定していると考えられます。

第2段階: 攻撃基盤構築段階

システムへの侵入に成功したならば、素早く攻撃者の用意しているサーバ(C&C³)とのバックドア(裏口)通信経路を確保します。旧来のバックドアとは異なり、ここでのバックドアはファイアウォール等で遮断できない、業務で使用している HTTP 通信などを使ったものです。このバックドアを使い、システム内調査に必要な機能を追加し攻撃基盤を構築します。

第3段階: システム調査段階

攻撃基盤を使い、システム内情報の検索を行います。この際にもバックドアを用い攻撃者と通信をし、システム情報を確認しながら検索を続けます。

第4段階: 攻撃最終目的の遂行段階

目的の情報をバックドアから窃取します。この入手情報を基に再度攻撃を行うこともあります。目標組織内に構築した攻撃基盤は維持したまま、何度も侵入を繰り返し、情報を窃取します。何度も攻撃してくる攻撃です。

³ Command and Control: 攻撃者が用意している外部の指令サーバ

表 3-2:「新しいタイプの攻撃」の各段階の攻撃内容

段階	攻撃内容	特徴
攻撃準備段階	(1)攻撃対象に関連のある組織への攻撃 ・メール情報の窃取など	対象組織への初期潜入を成功させるため、ソーシャルエンジニアリングのためのメール文面や送付先を収集。
初期潜入段階	(1)各種初期攻撃 ・標的型攻撃メール添付ウイルス ・ウェブ改ざんによるダウンロードサーバ誘導 ・外部メディア(USB 等)介在ウイルスなど	入口の対策をすり抜け、システム深部に潜入。 素早く次の段階へ移行。 攻撃手法は使い捨て。
攻撃基盤構築段階	(1)バックドア(裏口)を使った攻撃基盤構築 ・ウイルスのダウンロードと動作指示 ・ウイルスの拡張機能追加 ・システム内部への攻撃基盤構築	構築した攻撃基盤は発見されない。 構築した攻撃基盤は再利用される。
システム調査段階	(1)組織のシステムにおける情報の取得 (2)情報の存在箇所特定	時間をかけて何度もしつこく行う。
攻撃最終目的の遂行段階	(1)組織の重要情報の窃取 (2)組織情報(アカウント等)を基に、目標を再設定	何度も攻撃を行うため情報窃取。 組織への影響を与える情報窃取。

以降、初期潜入段階における特徴を説明します。

【初期潜入段階の実例】

初期潜入段階で検知をすり抜けシステム（組織）深部に潜入する例を説明します。以下は、実際の福島原発事故に関連する標的型攻撃のメールの一例です。メールに添付されているウイルスが、攻撃を受けた時点で、各ウイルス対策ソフトにおいて検知できていないことを HispaSec Sistemas 社の「VIRUS TOTAL」で示したイメージです。

攻撃者は、ウイルス対策ソフトが検知しない事を確認した上で送信してくると思われます。同時に、その後構築されたバックドアを通じ拡張されたウイルスも検知する事はありません。このような手段を使えばシステムが準備した対策を突破できます。

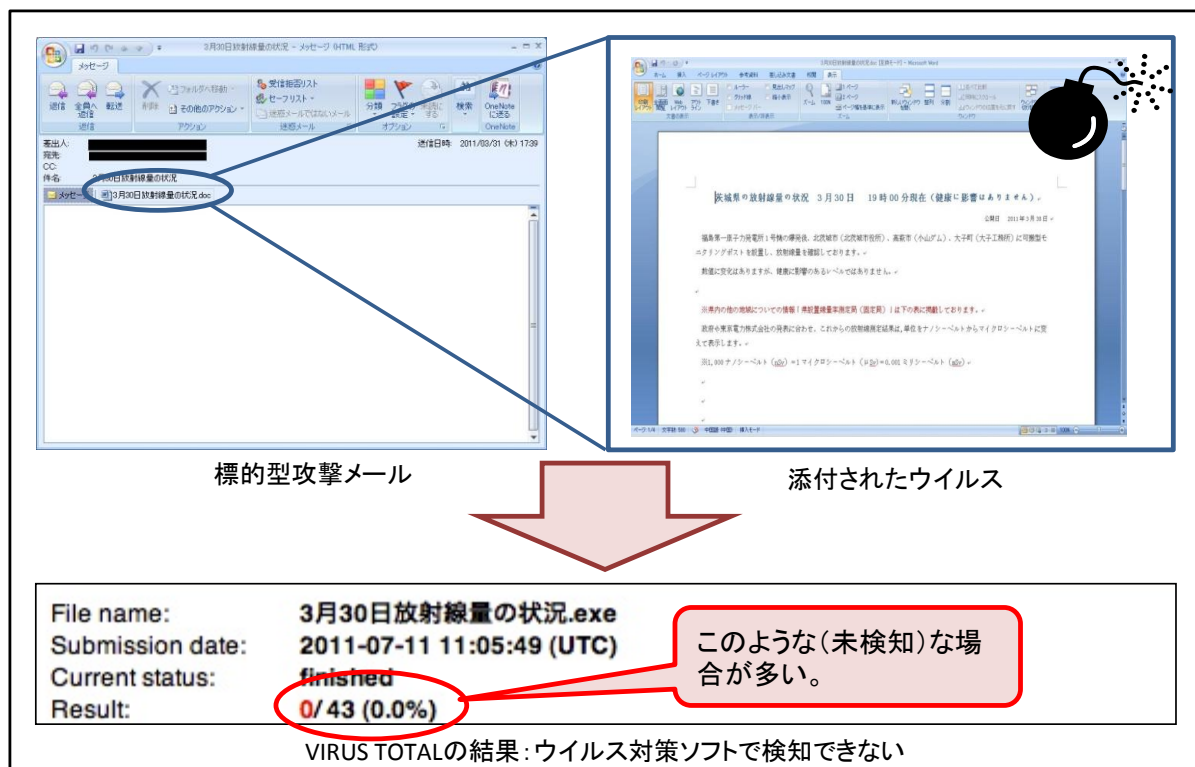


図 3-1-1：初期段階で検知できない結果イメージ

【攻撃基盤構築段階の例】

攻撃基盤構築段階では、組織に感染したウイルスと攻撃者のサーバと通信ができる状態になることを目的としており、次のような流れで行われます。

① 攻撃サーバ(C&C)との通信路を開設

初期潜入段階において組織の対策を突破した後に、攻撃サーバと通信経路を開設します。この通信路であるバックドアは、HTTP 通信です。社員の PC からインターネットにアクセスするのと同じ通信であるため、組織の対策で検知遮断できない可能性が高いと言えます。

② 拡張機能のダウンロード

このバックドアを使って当該組織を攻撃するのに見合った拡張機能がダウンロードされてきます。

これで組織深部に攻撃基盤を確保できた事になります。攻撃基盤とはバックドアの開設と攻撃サーバ(C&C)指示を受けるために進化したウイルスを指します。これ以降、攻撃者は構築基盤を温存しシステム内を調査、目的達成(情報窃取)のために繰り返しつこく侵入してくる事になります。

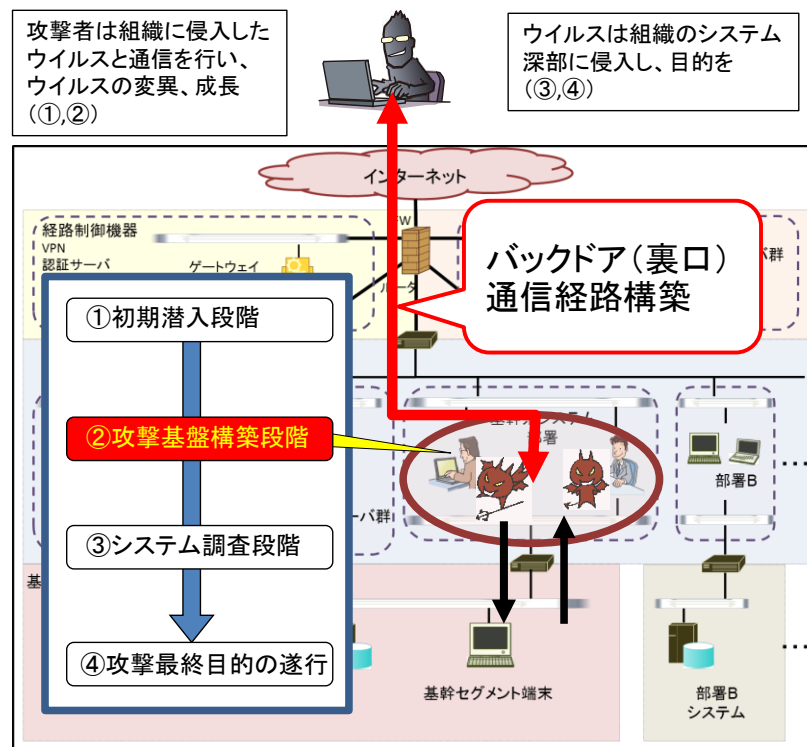


図 3-1-2: 検知をすり抜け、素早く次のステップ(攻撃基盤構築)に移行するイメージ

【攻撃基盤構築段階後の動作:システム調査段階、攻撃最終目的の遂行段階】

以下の通信の図は、組織(システム)深部に攻撃基盤を構築後に攻撃基盤と攻撃サーバ(C&C)とが実際にやりとりする様子です。構築したバックドアを使って自身が通信できる状態(Keep alive)であることを攻撃サーバへ送付し続け、指示に従いさらに拡張機能をダウンロードしてくる様子が観測されます。このような通信のやり取りを、長期にわたりしつこくやりとりし、機能を拡張しながら目的組織に深く侵入していきます。

keep aliveを打ち続けて潜伏、指示を受けて活動休眠を繰り返すつこい攻撃...					
不自然なkeep alive通信					
Date	SA	DA	Proto.	Size	IDS/AV
2011/*/* **:*	win-xp-sp2: 1865	*.com.br: 80	tcp	178	
2011/*/* **:*	*.com.br: 80 [BR]	win-xp-sp2: 1865	tcp	161600	(SF)Portable Executable binary file transfer (AV)Windows update-107

Keep aliveに対する応答により、実行ファイルがダウンロードされる

図 3-1-3: 新たなウイルスをダウンロードして実行するフロー

3.2 攻撃仕様の分析と整理

「新しいタイプの攻撃」の攻撃対象は組織のシステムです。そのため、「新しいタイプの攻撃」は、組織のシステムを対象とした問題として捉える必要があります。組織のシステムは、大規模になればなるほど、複雑となり、単純に PC やウェブサーバ単体の問題と捉える訳にはいきません。

システムの設計構造上での問題と対策を検討しやすくするために、実際に起きた各種サイバー攻撃事案をパターン化することが有効です。内閣官房情報セキュリティセンター(NISC)は「リスク要件リファレンスモデル作業部会報告書」で、サイバー攻撃における5つの「脅威タイプ」を整理しています。本パターンの整理は上記を基本として整理しました。

【「新しいタイプの攻撃」の5つの脅威タイプ】

タイプ1: 正規ウェブサイト閲覧によるウイルス感染(情報窃取)

改竄された正規ウェブサイトをシステム内ユーザが閲覧することにより、ウイルス配布サイトに誘導と感染が発生し、認証情報等の窃取とバックドアの設置が行われます。また、窃取された認証情報の利用により、攻撃利用基盤の拡大が図られます。

タイプ2: 標的型メール攻撃(情報窃取)

ウイルス付き騙しメールを送り、開封により攻撃サーバへのバックドア設置が行われます。この結果、情報システム内の情報の漏洩が発生します。特定組織を目標としたメールが送付されるので「標的型攻撃」と呼ばれます。

タイプ3: 正規Web改竄による誘導

サイト閲覧者をウイルス配布サイトに誘導し、自システムの正規ウェブサイトが改竄され閲覧者がウイルス配布サイトに誘導されます。攻撃の被害者であると同時に加害者になってしまいます。

タイプ4: 媒体介在ウイルス感染(情報窃取)、制御系システム攻撃

種々の場面で USB 媒体等に混入したウイルスが情報システムに混入。混入後、システム内へのネットワーク感染拡大と攻撃サーバへのバックドア設置が行われます。この結果、ネットワーク及びサーバ障害が発生すると同時に、システム内の情報の窃取が発生します。この攻撃は、社内基幹システム(オープン系)と制御系システム(クローズ系)の間の USB による情報交換運用を前提とした攻撃仕様も含まれます。

クローズ系内に感染したウイルスが収集した情報を USB に保存し、オープン系環境に戻った時に、攻撃サーバにアップロードするケースも見られます。その結果、社内基幹システムに設置したバックドア通信を使い攻撃サーバの指示を受け、情報窃取や制御系攻撃プログラムの機能追加などが行われます。

タイプ5: 複合 DDoS 攻撃における攻撃基盤部分

複合型の DDoS 攻撃は一般の DDoS 攻撃と異なり、複数の機能分散化されたウイルスが連携して各種攻撃動作を行います。ここでは DDoS そのものへの着目ではなく、その攻撃基盤部分に着目しています。この攻撃基盤では、感染した端末の情報を窃取が発生します。

【「新しいタイプの攻撃」における共通動作機能】

次に、これらの攻撃パターンから、情報システムへの影響と対策を検討し情報システムの対策設計に取り込みやすくするためには、これらのパターンから共通動作機能部分を導き出します。以下の4つは、攻撃者が「発見しにくく静かな攻撃」を実現するために組み込まれている4つの共通動作機能です。ここから、情報窃取及び情報破壊に関わるいずれの攻撃にも共通動作部分がある事が解ります。この共通動作機能部分は、4章のシステム対策に繋がってくる部分です。これらは、いずれも従来の対策では対処することが難しい攻撃仕様です。

- ① バックドア通信機能(複数種類)
- ② 侵入システム内感染拡大
- ③ 一斉バージョンアップ(P2P 等)機能
- ④ USB 利用型情報収集機能

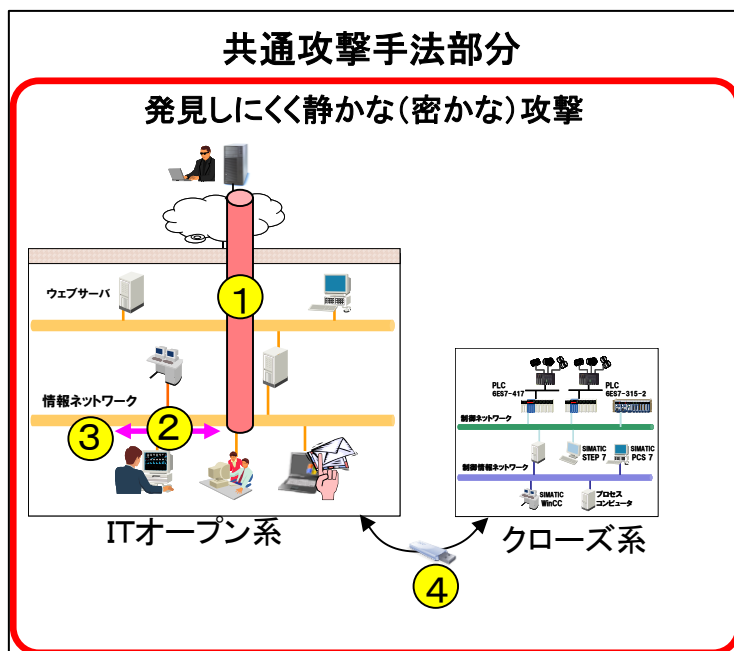


図 3-2-1: 4つの共通動作機能

これら共通動作機能へのシステム対策を考えるためには、組織内のシステム上で具体的な攻撃動作の流れを分析する必要があります。この攻撃動作の流れがシステム上のネットワーク等とどのような関係にあるかが解れば、システムの設計者は設計の中で影響と対策を考える事ができます。

表 3-2 は、各共通動作機能が、どのような役割を持ち、組織のシステム上でどのように機能するのかを示しています。

表 3-2: 共通動作機能の役割

共通動作機能	組織内のシステムでの動作	役割
バックドア通信機能	組織で利用する http 等、組織にとって必要とする通信プロトコルやポートを利用してバックドア通信を行う。 主に次の 4 つの種類の通信がある。 ・プロキシを介して行う HTTP プロトコルに類する通信 ・プロキシを介さない HTTP プロトコルに類する通信 ・プロキシを介さない独自プロトコルの通信 ・RAT 通信	ウイルスと攻撃者のサーバ (C&C) との通信を確立する。
システム内拡散	組織内ネットワーク感染により、脆弱性を利用したシステム内へウイルス拡散する。	システム内の情報をより効率的に窃取するためにより多くの端末へ感染させる。
一斉バージョンアップ (P2P 等) 機能	拡散したウイルスに、C&C からダウンロードされた拡張機能モジュールを一斉更新する。	システム内に拡散されたウイルスに対して効果的な攻撃を行わせる機能を持たせるようにする。
USB 利用型情報収集機能	USB を介してクローズ系システムに拡散し、クローズ系システム内情報を収集する。USB がオープン系システムに戻った時に収集情報を使って送信する。USB を介して攻撃サーバからの命令や更新機能をクローズ系システムに伝達する。	クローズ系の情報を収集などの攻撃を行うため、USB にウイルスを混入させて攻撃を行う。

【バックドア通信機能の動作例】

「バックドア通信機能」のシステム上での例を図 3-2-2 に示します。バックドアは、システム端末がインターネット上のウェブサイトへアクセスする時のプロトコルとアクセスルートを用いたウイルスによる裏口通信です。この通信は、正常なウェブサイト閲覧と同じに見えるため、通信経路は侵入検知システム等の対策をすり抜けてしまいます。これにより、攻撃サーバからの命令や追加機能のダウンロード、情報の窃取(攻撃サーバへの送信)が行われます。

この時、実際のアクセスルートは、業務上のウェブサイト閲覧と同じ経路をたどります。対策の考え方とは、経路上のいずれかの箇所で、ウイルスによるバックドア通信のみを遮断すれば、「組織情報を窃取される」という事象を回避できる事になります。

4 章で記載する対策では、たとえ、ウイルスが侵入したとしても「組織情報の窃取をさせない」という考え方で対策を示しています。このため、バックドア通信の特徴を基にシステム上のアクセスルート設計を行う等の設計対策アプローチを考えていきます。

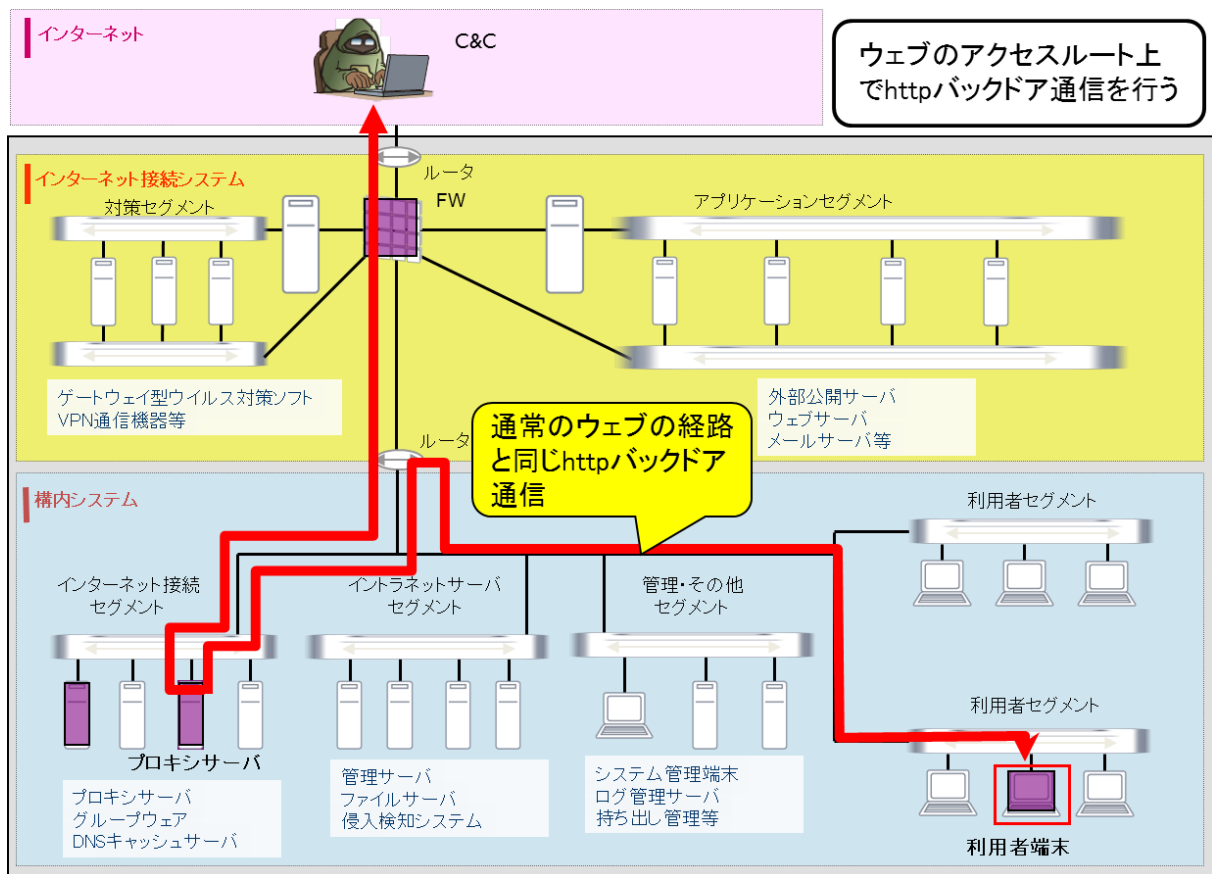


図 3-2-2: http バックドア通信機能のアクセスフロー(プロキシ経由・HTTP プロトコルに類する場合)詳細

3.3 バックドア通信の種類(2011 年調査時点)

「共通攻撃手法」において、「バックドア通信」があります。ここでは、バックドア通信がどのような種類があるかを紹介します。バックドア通信を遮断するための対策をしても、種類によって方法が異なります。下記はトレンドマイクロ社が、2011 年 4 月～10 月にかけて国内で収集した、標的型攻撃メールに添付されていたと思われるウイルスから 50 個をサンプル抽出し調査した結果です。

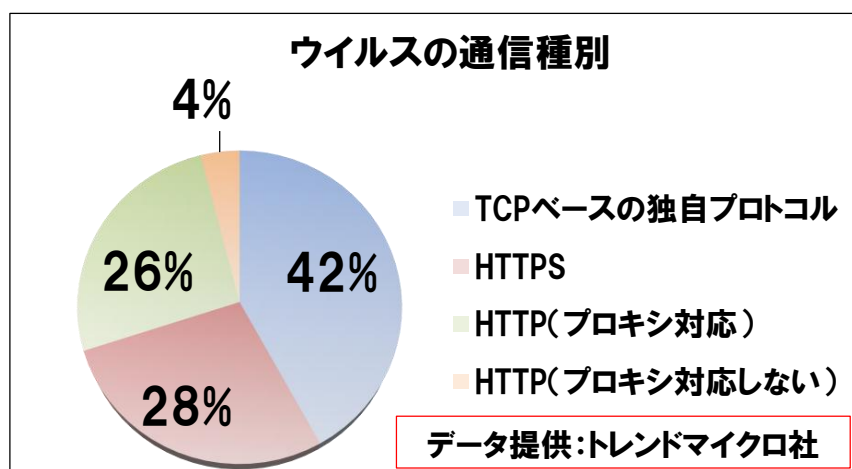


図 3-3-1:ウイルスの通信種別

これらの通信は、同じ実装では止められません。これらの通信ごとの対策についての対策を 4.4 および 4.5 にて紹介します。

4. 新しい脅威に立ち向かうポイント

4.1 新たな対策発想で考える

3章で見てきた従来の対策のアプローチでは防ぎ切れない攻撃に対して、組織の対策に対する考え方を考えてみる必要があります。

以下、新しい脅威に立ち向かうための新たな対策発想のポイントを整理します。

ポイント1: 組織への重大な被害を回避するための対策を考える

ポイント2: 出口対策を考える

ポイント3: システム設計者とセキュリティ対策担当の連携で対策を考える

【ポイント1: 組織への重大な被害を回避するための対策を考える】

組織への被害の本質は、ウイルスの侵入ではなく、「重要な情報が窃取される事」や「重要なシステムの稼働に障害を与えられる事」ですので、その最終被害を回避できるかが最重要課題です。最終被害の回避のためには、その被害に至るフローを阻止(寸断)することです。

ウイルスの侵入から、最終的に情報窃取やシステム破壊等へ続く一連の攻撃の流れを寸断できれば被害を食い止めることができます。そのためには、この一連の攻撃の流れの中で、入口対策で防御できなかった場合を想定して、外部との通信を断つこと(出口対策)が効果的です。図 4-1-1 に、その全体の考え方を示します。

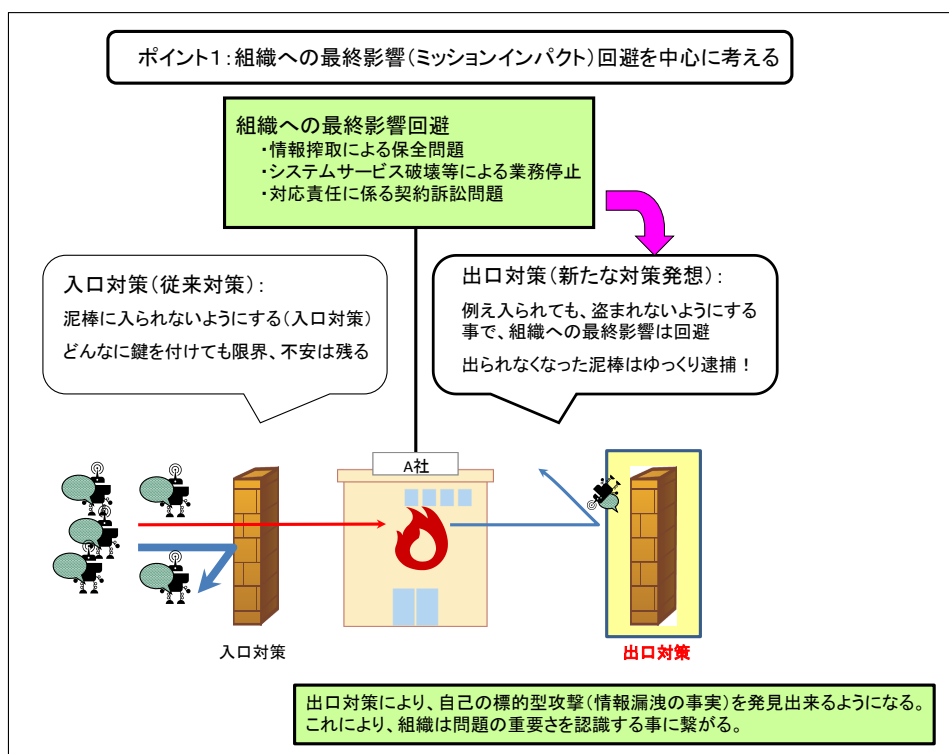


図 4-1-1: 組織への重大な被害を回避する方策

【ポイント2: 出口対策を考える】

従来の対策を乗り越えてシステムに侵入したウイルスは「共通攻撃仕様部分」の主要な機能として、バックドアの設置とそれを経由した外部との通信、更に内部ネットワークを経由してシステム深奥部へ侵攻します。そこで、この外部通信を抑止する出口対策を防御対象に考える事により、「新しいタイプの攻撃」への共通の対策となります。

【ポイント3: システム設計者とセキュリティ対策担当の連携で対策を考える】

システムの開発においては、設計構築の責任をプロジェクトマネージャ(PM)が持ちます。セキュリティ機能のみだけでなく、サービス機能含め全体機能としてのバランス、ユーザニーズ、必要コストなどを総合的に勘案して開発プロジェクトを進めていく責任者です。図 4-1-2 に示すように、開発にあたっては、PM の下に、サイバーセキュリティの対策担当(脅威アナリスト)や、製品プロダクト担当が配置されます。

これまでのセキュリティ対策はベンダ製品をネットワークシステムに配置する設計が主に行われてきました。そのため、PM がサイバー攻撃をよく理解していないケースが多く見受けられました。一方、情報セキュリティの担当は、システムの中核を狙った攻撃に対して、保護すべき対象のシステムの全体像がよく見えていません。双方が互いのポイントを理解する事によって、新しい発想での対策が浮かび上がってきます。

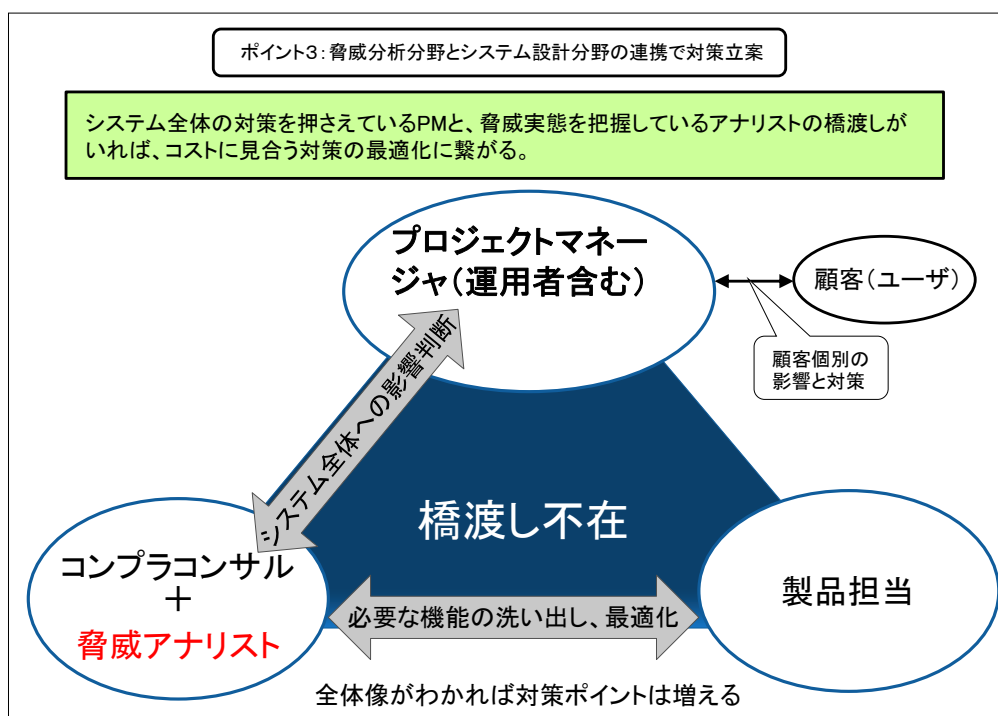


図 4-1-2: システム全体からみたセキュリティ対策の体制

4.2 入口対策と出口対策

従来取ってきた対策は、「脅威を中に入れない(境界防護)」の設計思想の対策です。これらをここでは、「入口対策」と呼びます。これらの対策は十分に取られて来た筈ですが、「新しいタイプの攻撃」はこれらの対策をすり抜けてシステム深部に到達するという現実があります。図 4-2-1 はその概念図です。従来の対策をすり抜けてくる理由はいくつかあります。パッチの無い脆弱性が使用される、一見正常通信を装うために従来の検知技術では検出できずログにも記録されない、アンチウイルスソフトに検知されないことを確認した上で侵入してくる等々です。

このような課題に対し情報システムの設計開発や運用管理の責任を有する人たちは、4.1 章の「ポイント1:組織への重大な被害を回避するための対策を考える」および「ポイント2:出口対策を考える」を念頭に置く必要があります。「脅威が入っても被害は防ぐ」という事で、この考えで検討された対策が「出口対策」です。「出口対策」は、侵入したウイルスの活動の増強や深部への侵攻を指令するバックドア通信を遮断する事により、最終的な実害(攻撃目的である情報の窃取と情報破壊)を回避する対策アプローチです。「出口対策」は、システムのネットワークフロー設計の視点で対策を考えるため、設計対策手法で防御する対策となります。4-3 で、この出口対策を具体的に掘り下げていきます。

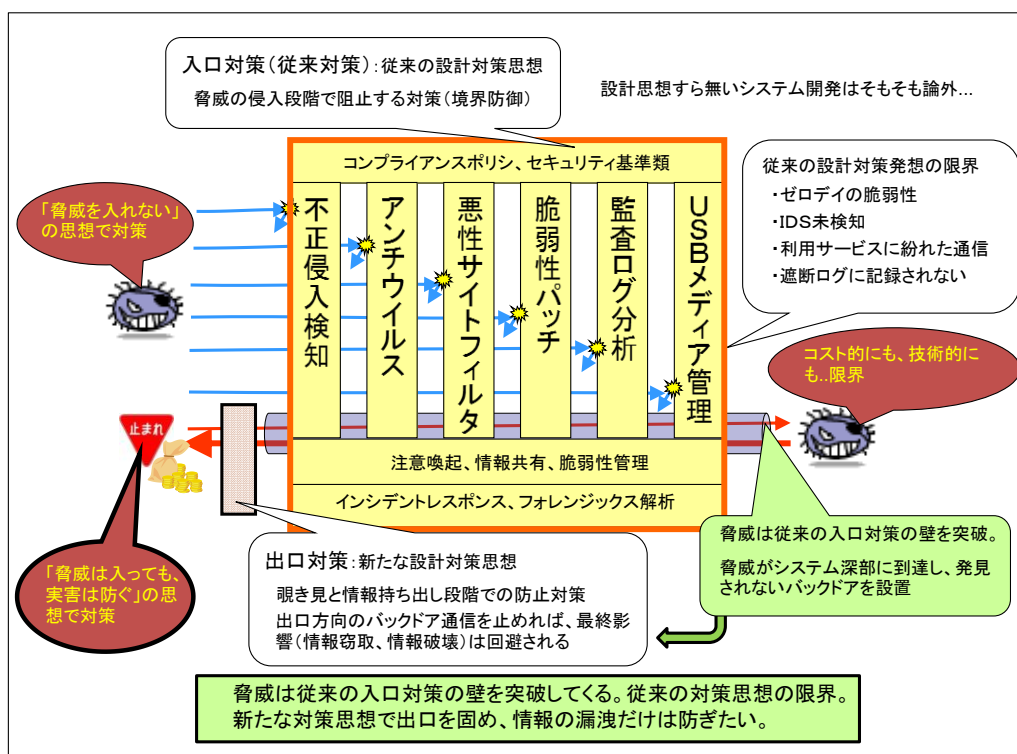


図 4-2-1: 従来の設計対策思想の限界と出口対策の位置づけ

4.3 「出口対策」の実現方法

本項では、4.1 章の「ポイント3:システム設計者とセキュリティ対策担当の連携で対策を考える」を基に出口対策の実現方法について示します。出口対策の策定にあたって、その実効性と実現性を重視し、以下を設計要件としています。

- ✓ 攻撃フロー分析結果の内、システムの対策設計に必要な情報のみを抽出して利用
- ✓ 最終被害を防ぐための出口対策に重点をおいた設計
- ✓ 共通攻撃手法の動作フローを基に、出口対策として効果の確認された方式の採用
- ✓ 攻撃における通信特性を基に、ネットワークポロジ設計に視点を置いた設計

(1)「出口対策」策定のアプローチ

IPA「脅威と対策研究会」において、以下のアプローチを実行しました。その全体像を図 4-3-1 に示します。このアプローチにおいては、実際の事案(インシデント)の解析を基に、「①実事案→②脅威5タイプ→③共通動作機能」と分類の整理を行い、最終整理である「③共通動作機能」を設計に用いる対象脅威と定義しています。表 4-3-1 にその要点を説明します。

表 4-3-1:「出口対策」策定アプローチ

アプローチ	実施事項・留意事項	該当
①実事案から脅威タイプ整理	従来の入口対策をすり抜けた攻撃を収集・分析 実攻撃事案の分析を通して「5つの脅威タイプ」に整理	3-2: 「5つの脅威タイプ」
②共通攻撃手法の抽出	ウイルス解析情報等を基に共通的な攻撃動作仕様を分析	3-2: 「共通動作機能」
③出口対策	「共通動作機能」を対象とした対策を策定 ・システム設計図上のネットワークフローを基に検討 ・実効性がありコスト面からも極力既存のネットワーク関連機器の設定で対応できる対策を採用	4-5: 「8つの出口対策」
④試験工程	「共通動作機能」から設計対象脅威として用いた「共通脅威6パターン」を試験確認項目として利用し、設計工程で選択した「共通脅威6パターン」に対する設計動作を確認する事を想定 設計結果の確認では模擬攻撃をかけて検証する手法以外に、ログやルールの提出(審査)する手法でも検証可能。例えば、「①サービス通信経路設計」の試験においては実際のバックドア通信を再現しなくても、FW がルール設計に従って設定されているかを検証確認する事で確認可能です。	4-5: 「8つの出口対策」

「共通動作機能」の中から、設計へ繋げる部分はどこか、ということを引き出したものが、「共通脅威6パターン」です。「共通脅威6パターン」は次の通りです。

共通脅威パターン1: http バックドア機能 (http プロトコル・プロキシ使用しない)
 共通脅威パターン2: http バックドア機能 (独自プロトコル・プロキシ使用しない)
 共通脅威パターン3: http バックドア機能 (http プロトコル・プロキシ使用)
 共通脅威パターン4: RAT 通信 (内部 proxy への CONNECT コマンドによる RAT のバックドア通信)
 共通脅威パターン5: システム内探索機能
 共通脅威パターン6: システム内拡散・機能更新機能

この設計に結びつく「共通脅威6パターン」を基に「出口対策」を考案しました。このようなアプローチから、次の利点が生れます。事案単位に分析をして対策設計を実施するのは多大な工数が発生しますが、共通的な攻撃動作仕様から抽出した「共通動作機能」を対策対象脅威と定義する事により、設計や試験が通常の製造工程フローの中で行う事が可能となります。試験工程においては、設計対象脅威として用いた「共通動作機能」を試験確認項目として利用し、設計工程で選択した「共通動作機能」に対する設計対策の動作を確認する事を想定しています。

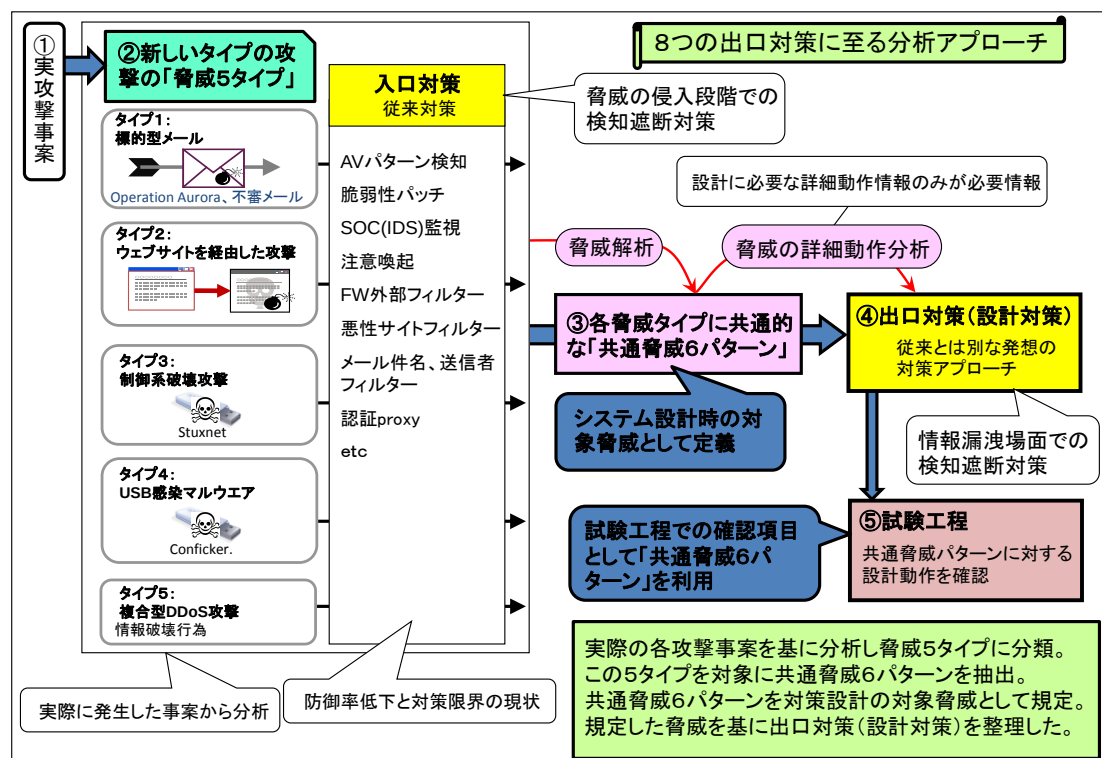


図 4-3-1: 「出口対策」策定のアプローチの全体像

(2) 8つの「出口対策」

前項で述べたアプローチに従って「共通脅威6パターン」毎に、標準的なシステム設計図上で脅威をトレースして設計内容を確認し、8つの「出口対策」を導き出しました。図 4-3-2 は、共通動作機能と8つの出口対策との関連の一覧を示しています。各8つの出口対策は以下です。この8つの設計対策は、脅威がシステム深部に侵入したとしても、外部攻撃サーバとの通信を絶つことによって実害を回避するものとなります。

対策①②: http バックドア検知遮断
 対策③: RAT の内部 proxy 通信(CONNECT 接続)の検知遮断
 対策④: サーバセグメントへの http バックドア開設防止
 対策⑤: 重要攻撃目標サーバの防護
 対策⑥: マルウェアの内部拡散防止 (⑦: 内部拡散監視)
 対策⑧: ローカルセグメント内感染拡大後の P2P による機能更新等防止

6つの設計対策を実際に設計/実装する場合は、一般的にプロジェクトマネージャの下、関連する複数の作業チームが連携して設計作業を進める事になります。また、各チーム間で対策を実装するためのすり合わせが必要になる場合もあります。これら各チームが同じ設計認識を持って作業に当たる事が重要となります。関連する複数の作業チームの一例は以下です。

ネットワーク設計チーム	トポロジ設計、回線性能等
セキュリティ設計チーム	ファイアウォールルール設計、ACL(Access Control List)設計等
業務フロー設計チーム	業務アプリケーション、業務データフロー等
運用基盤設計チーム	運用管理 COTS(Commercial off the Shelf)、運用ログ設計等
運用設計チーム	逐次／日次～月次の運用設計(監査内容/監査方法)等

各脅威タイプに共通的な「共通脅威6パターン」	出口対策（設計対策）
共通脅威パターン1:バックドア通信 ○httpプロトコルバックドア通信 ○port8080、内部proxy未使用	①サービス通信経路設計の実施 対策目的:経路ルール違反通信の遮断 1.FWの外向通信遮断ルール設定 2.FW,の遮断ログ監視 ② ブラウザ通信パターンを模倣するhttp通信検知機能の設計 対策目的: httpメソッド利用バックドア通信の遮断 ③ RATの内部proxy通信(CONNECT接続)の検知遮断設計 対策目的:RAT通信の遮断
共通脅威パターン2:バックドア通信 ○独自通信プロトコルバックドア通信 ○port8080、内部proxy未使用	
共通脅威パターン3:バックドア通信 ○httpメソッド(GET,POST,CONNECT)利用のバックドア通信 ○port8080、445、内部proxy使用	
共通脅威パターン4:RAT通信 ○内部proxyへのCONNECTコマンドによるRATのバックドア通信 ○port8080、内部proxy使用	
共通脅威パターン5: ○システム内情報の搜索脅威	④最重要部のインターネット直接接続の分離設計 対策目的:最重要部へのバックドア設置の回避 ⑤重要攻撃目標サーバの防護 対策目的:攻撃対象となる重要サーバの防護
共通脅威パターン6: ○バックドアマルウェアのシステム内拡散、機能更新脅威	⑥SW等でのVLANセッワーク分離設計 対策目的:バックドアマルウェアの拡散範囲の限定 ⑦容量負荷監視による感染動作の検出 対策目的:バックドアマルウェアの内部拡散検知 ⑧P2P到達範囲の限定設計 対策目的:バックドアマルウェアの一斉機能更新等の防止

28

4.4 バックドアへの設計における効果と課題

本項では、3.3 章のバックドア通信において、本書における対策がどの程度効果があるのかを示します。図 4-4-1 は 3.3 章で示したウイルスの通信種別です。

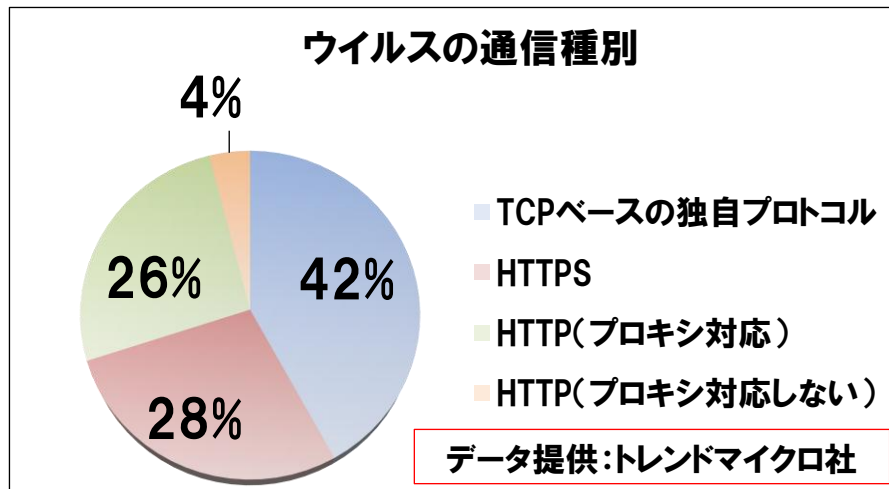


図 4-4-1:ウイルスの通信種別

この内、「TCP ベースの独自プロトコル」と「HTTP(プロキシ対応しない)」通信については、この後に示す 4.5 章の実装項目①で対策が可能な通信です。この実装を実施することで、46%の攻撃が防げることになります。また、この対策を実施することで組織に攻撃が来ているかどうかの気づく効果を与られます。実装項目①については、ネットワーク設計を大きく変更するような対策ではないため、すぐにできる実装であると言えます。

一方、「HTTP(プロキシ対応)」の通信と「HTTPS」の通信の対策については課題があります。「HTTP(プロキシ対応)」においては 4.5 章の実装項目②を対策として、「RAT 通信」においては実装項目③を対策として記載しています。しかし、有効な技術であると言えるかは検証や実験を行う必要があるものです。また、「RAT 通信や https 通信」の割合も多くなっており、これらのバックドア通信についても有効な対策を見つけなければならないものです。これらについては、IPA「脅威と対策研究会」で更に検討を重ねていきます。

4.5 大切な情報をサイバー攻撃により漏洩させない8つの対策

本章は、4.4 章までで洗い出した「共通脅威6パターン」に沿って対策をどのように実装するのかをまとめたものです。最初にバックドア通信の実装項目をまとめます。その次に、それぞれの実装項目について説明します。

【バックドア通信を防ぐための実装項目①～③の関係】

実装項目①から③は共通脅威6パターンの内、1～4までのウイルスのバックドア通信に関する対策です。これらの対策によるバックドア通信の対策のイメージは図 4-5-1 および図 4-5-2 です。

実装項目①で、「独自プロトコルの通信」と「HTTP プロトコルを使用する通信の内、内部プロキシを通らない通信」を遮断します。「HTTP プロトコルを使用し、内部プロキシを通る通信」を実装項目②で、「RAT 通信」を実装項目③で検討します。

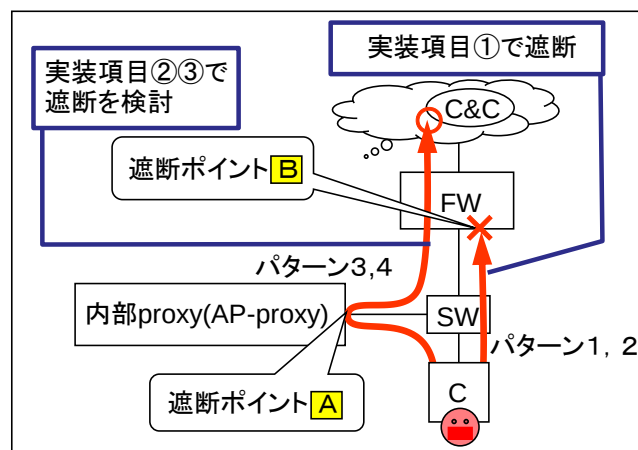


図 4-5-1: ウイルスのバックドア通信の対策イメージ(簡易)

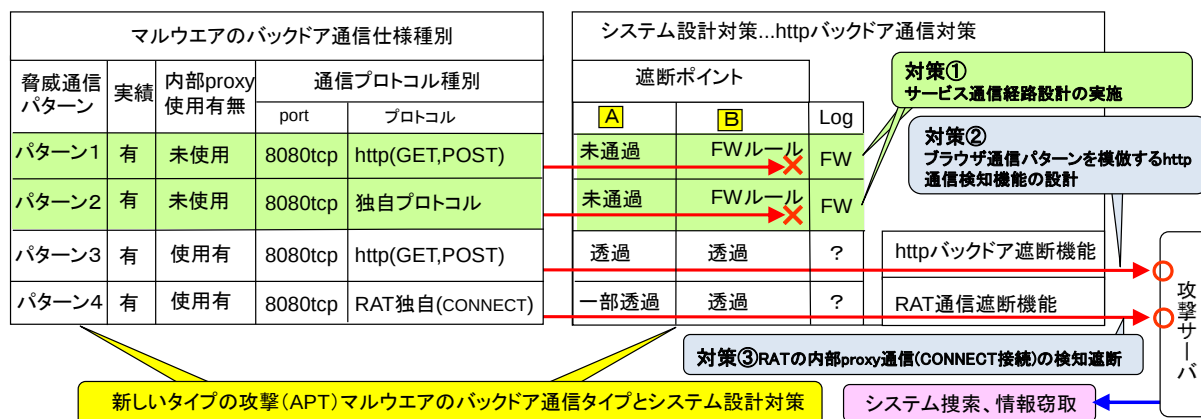


図 4-5-2: ウイルスのバックドア通信の対策イメージ(詳細)

【実装項目①:サービス通信経路設計の実施】

■通信経路の設計例

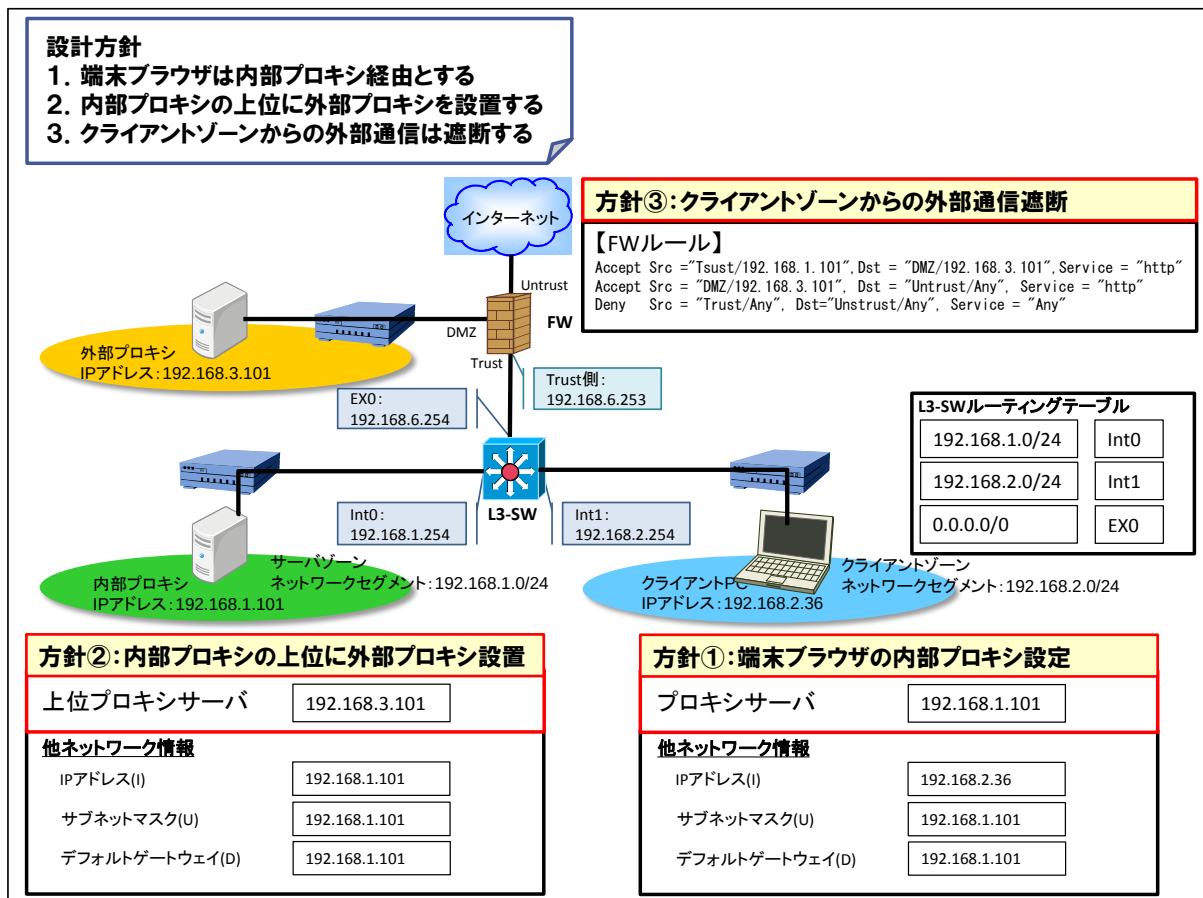


図 4-5-1-1:「実装項目①:サービス通信経路設計」例

この対策の目的は、「通信経路設計ルールから外れたウイルスの特性を基に外部 C&C サーバとのバックドア通信の遮断」です。

対策の対象は、「共通脅威6パターン」における「プロキシを介さない独自プロトコルの通信」および「プロキシを介さない HTTP プロトコルに類する通信」です。

■通信経路の実施事項

1-1

👉 FW の外向き通信遮断ルール設計(1-2 と併せて実施)

ウイルスが行う通信の内、「プロキシを介さない独自プロトコルの通信」および「プロキシを介さない HTTP プロトコルに類する通信」の特性から以下のルールを適用します。

- (1) FW では内部プロキシ(アプリケーション G/W)経由の外向け通信のみ許可、プロキシを使わない端末からの直接通信を遮断
- (2) 外部に 80,443 ポートでアクセスする以下のような各種サービスは、内部 Proxy を中継するように設計(ただし、DMZ 上に配置された機能装置を除く)

対象機能例	通信用途
Windows Server Update Services (WSUS)	Windows Update Server との通信(80,443)
System Center Configuration Manager(SCCM)	マイクロソフト製品以外のアップデート、資源管理等
IDS/IPS	シグネチャ更新
ウイルス対策ソフト関連	パターンファイル更新
検疫関連	最新のパッチやパターンファイル情報の取得
スパムメールフィルタ	ブラックリストの更新など
その他	ライセンス認証など

【注意事項】

プロキシを経由できないオンラインアップデート機能等を持つソフトウェアがある場合は、共有ファイルサーバなどを別途用意し、このサーバを経由してアップデートを行います。このとき、システム管理者が安全な PC で、社内ネットワークとは別の契約回線などを用いて入手したアップロードファイルを、共有サーバに配備する運用を行うなど検討する必要があります。

- (3) 端末から内部 Proxy を介さない外部 80 ポート通信は C&C サーバとのバックドア通信の可能性があると判断

1-2

🔍 FW の遮断ログ監視(1-1 と併せて実施)

FW の遮断ログを記録分析し、ウイルスによるバックドア通信を発見して感染端末の特定に繋がります。ログ保存期間はマルウェアのバックドア通信活動のタイミング(スリープ、キープアライブ)実績から見積ります。

■通信経路の設計例に則った通信の流れ

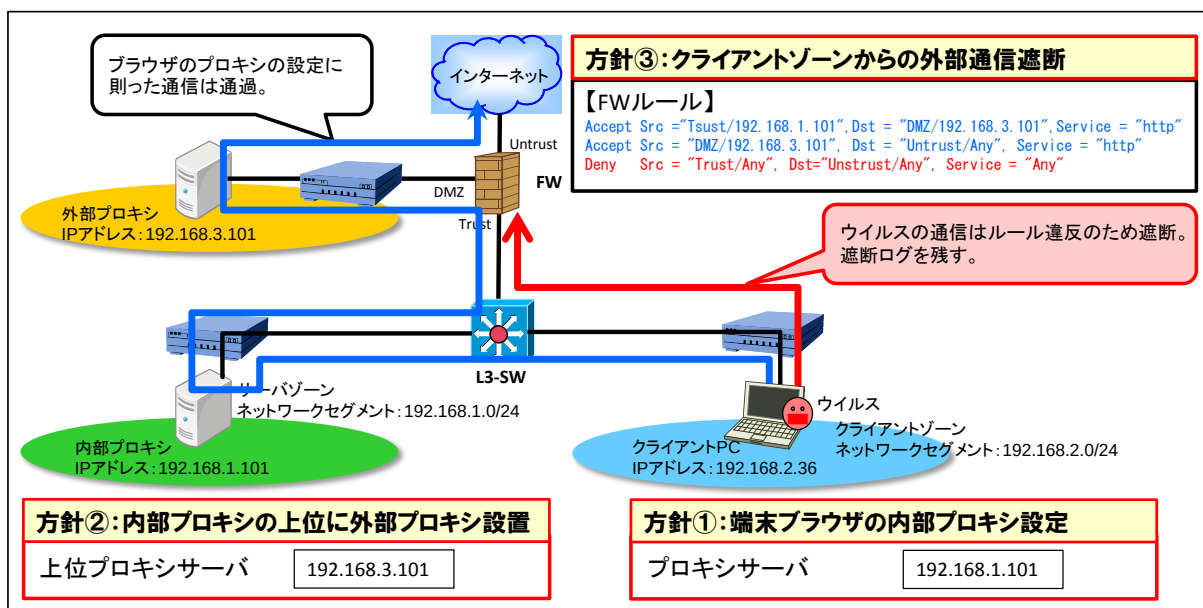


図 4-5-1-2:「対策1: サービス通信経路設計」に則った通信の流れ

このように遮断した通信のログは次の通りです。このようにログを監視することで、組織の端末がウイルスに感染しているかどうかも判明します。

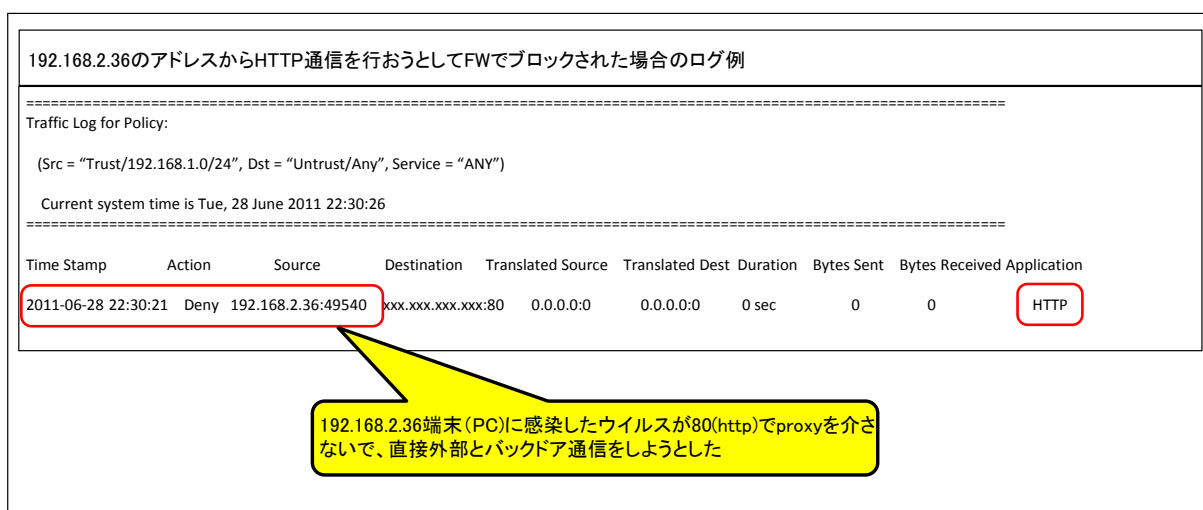


図 4-5-1-3:「対策1: サービス通信経路設計」に則った通信の流れ

【実装項目②: ブラウザ通信パターンを模倣する http 通信検知機能の設計】

■通信経路の設計例

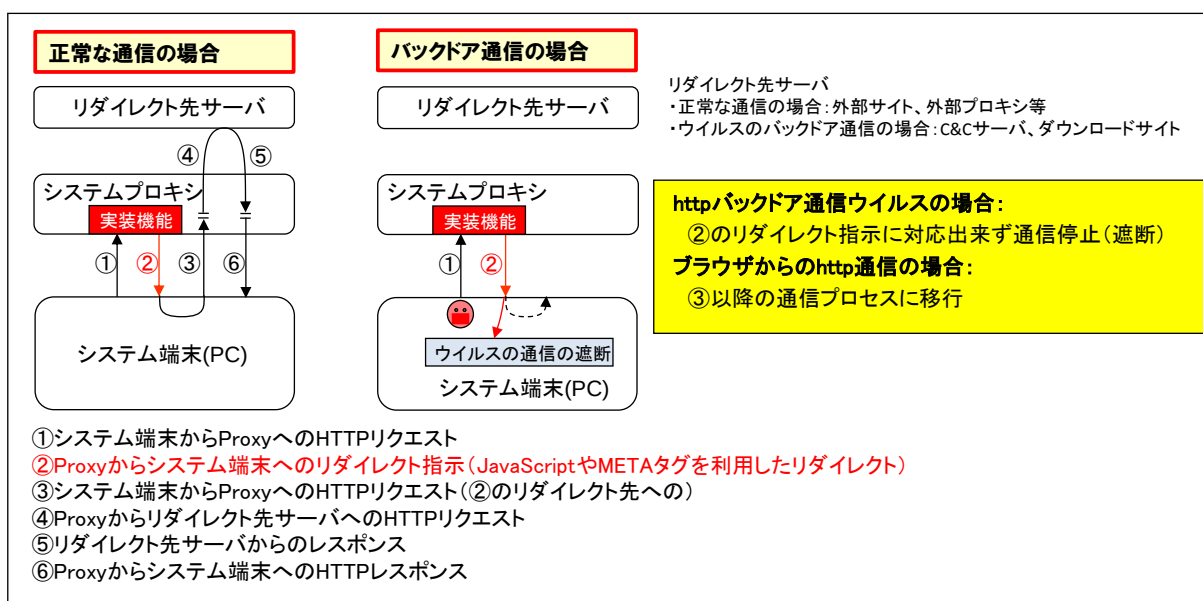


図 4-5-2-1:「対策 2-1: JavaScript や META タグを利用したリダイレクト」に則った通信の流れ

この対策の目的は、「通信経路設計に沿っており、ブラウザと同様の通信特性 (http メソッド GET, POST, CONNECT 利用通信) を持つウイルスの外部 C&C サーバとのバックドア通信を遮断」です。

対策の対象は、「共通脅威6パターン」における「プロキシを介した HTTP プロトコルに類する通信」です。

■通信経路の実施事項

2-1

🔍 JavaScript や META タグを利用したリダイレクト方式

※[注]今後、IPA において実証試験による効果確認を検討

この対策は、HTTP の応答に対してブラウザでは応答に即した対応ができて、ウイルスでは応答に即した対応ができない特性を利用した対策です。システムプロキシに JavaScript や META タグを利用したりダイレクト機能を実装し、リダイレクトに対する応答によりウイルスによるバックドア通信とブラウザ通信とを判別します。この対策には、システムプロキシ上に実装をする必要があります。

この対策ではウイルスによるバックドア通信の特徴の内、次のようなものに注目しています。

- ✓ ウイルスの通信応答は、Web ページの表示のために利用されない。
- ✓ JavaScript や META タグを利用してリダイレクトさせる方式にはウイルスは追従できない。
- ✓ システムプロキシに JavaScript や META タグを利用したリダイレクト機能を実装し、リダイレクトに対する応答によりウイルス通信とブラウザ通信とを判別する。

この特徴を利用し、ブラウザからの通信は図 4-4-3 の流れで行います。ウイルスは図中②のリダイレクトの通信に応答ができないため、通信が遮断されます。

2-2

🔍 ウイルス固有の http ヘッダ等、通信の特徴等からバックドア通信を判別

※[注]対応可能技術の調査と検証が完了次第、追加の改定記載を予定

この対策は、http バックドア通信とブラウザの正規通信の違いを基にした設計対策です。例えば、ブラウザのヘッダ情報とウイルスのヘッダ情報では差異がみられるため、このような特徴を用います。

この対策ではウイルスによるバックドア通信の特徴の内、次のようなものに注目しています。

- ✓ ウイルスのバックドア通信ヘッダはブラウザに比べ単純なヘッダの使い方をする場合がある。
- ✓ ヘッダの特徴は、ブラウザ機能に依存せずウイルスの通信仕様に依存する。
- ✓ Keep-Alive、exe ダウンロード等の周期性など、ウイルスと C&C の通信パターンが存在する。
- ✓ ウイルスの http ヘッダ拡張の User-Agent はブラウザのものとは異なる場合が多い。

ウイルスのバックドア通信ヘッダのシンプルさの例を次に示します。図 4-4-2-2 は、Internet Explorer 8 における通信のヘッダ情報です。

```
GET
/CIS/55/000/000/000/016/481.swf?fd=jp.msn.com&clickTAG=http%3A//g.msn.com/2AD0004N/13000000000044826.1%3F%3FPID%3D8722904%26amp%3
BUI%3DM%26amp%3BTargetID%3D10666778%26amp%3BAN%3D52560302%26amp%3BPG%3DJHP201%26amp%3BASID%3D2e312bb00ae2479da4bc97d
b458b894a&clickTag=http%3A//g.msn.com/2AD0004N/13000000000044826.1%3F%3FPID%3D8722904%26amp%3BUI%3DM%26amp%3BTargetID%3D106
66778%26amp%3BAN%3D52560302%26amp%3BPG%3DJHP201%26amp%3BASID%3D2e312bb00ae2479da4bc97db458b894a HTTP/1.1
Accept: */*
Accept-Language: ja-JP
Referer: http://jp.msn.com/?ocid=iefvrtx-flash-version: 10,3,181,14
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET4.0C; .NET4.0E; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR
3.0.04506.30; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Host: a.ads2.msads.net
Connection: Keep-Alive
```

図 4-5-2-2: Internet Explorer 8 におけるリクエストヘッダ情報例

ブラウザの通信ヘッダは複数の情報が記載されています。一方、ウイルスの通信は図 4-4-2-3 のようにシンプルなものです。

ウイルス例1

```
GET
http://login.51edm.net/getconf.php?m=f9c46f1f7ed5073091dd2a196cde7761&q=FamWNHTEDv¥dSvfKy=8qRnyry9fqlyqyv0qlwZqc9uqCv0a8aT0sJh¥ywfaF
XQvsJha8p4MsJfaDelHsJZKyxtWlvfOSXlOyO55 HTTP/1.1
Host: login.51edm.net
Pragma: no-cache
```

ウイルス例2

```
GET
http://pds.adncommerce.com/jmoy.php?npic= HTTP/1.1
Host: pds.adncommerce.com
```

図 4-5-2-3: ウィルスにおけるリクエストヘッダ情報例

これらの特徴を利用した対策ができる可能性のある技術は次であるとして検証を行っています。

- http ヘッダの正規 User-Agent をホワイトリスト化
- バックドアウィルスの C&C とのキープアライブ通信特性を登録
- http レスポンスデータの不自然なデータサイズを検知
- C&C への接続先が複数ある事等の動的特徴を抽出
- http ヘッダ長に基づいた検出 等

【実装項目③: RAT の内部 proxy 通信 (CONNECT 接続) の検知遮断設計】

■通信経路の設計例

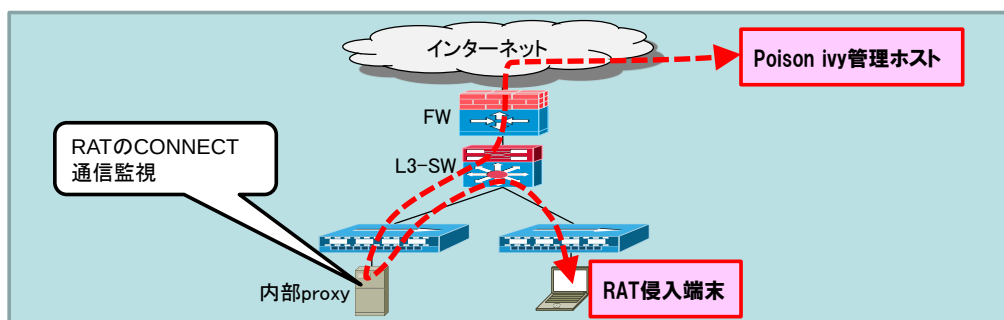


図 4-5-3-1: 内部プロキシによる CONNECT 通信監視設計例

■通信経路の実施事項

この対策の目的は、「RAT 通信の特徴を基に検知遮断対策を行うこと」です。RAT は内部 proxy に対して発行する CONNECT コマンドにより、ネットワーク設計ルールに沿って FW を通過する内部 proxy 経由の 8080 外部 RAT 通信が確立 (tcp コネクショントンネル) します。

対策の対象は、「共通脅威6パターン」における「RAT 通信」です。

3-1

内部 proxy の「**CONNECT 172.16.0.210 [**]**」において、**を特定のポート番号に限定するネットワーク設計を行い、ivy の **CONNECT** 要求通信を内部 proxy で遮断

この対策により、RAT の通信が他の端末へアクセスしようとしたときに正常ではないルールに一致しな

い通信を止めます。例えば、443/tcp のみを許す設計を行った場合、Poison ivy のデフォルト設定で使われる CONNECT 172.16.0.210:3460(ivy 通信)は遮断されます。

3-2

👁 内部 proxy のログ分析で ivy の CONNECT 通信を監視

Ivy 通信では下記ログが出力されるため、CONNECT という文字列を含む行のうち、443/tcp 以外の行を proxy ログ上で監視します(`grep CONNECT access_log | grep -v :443`)。

なお、RAT 通信の対策においては、「RAT(Poison ivy)のセッションは、張り続けられる」ことに着目した対策や「専用機等の利用を含めたシステム設計内容」も脅威と対策研究会にて検討をしています。

■RAT の仕様及び通信の特徴(Poison ivy の例)

・RAT(Remote Access Trojan / Remote Administration Tool)とは

RAT は下記の機能・特徴を備えている攻撃者が使用していると考えられるツールです。

- ✓ 侵入したシステムを遠隔から操作する。潜伏活動や窃取活動で利用されている。
- ✓ ファイアウォールを介した外部接続可能な通信環境を実現できる。
- ✓ 独自プロトコルだが、HTTP プロキシ越え(CONNECT コマンド使用)、Socks(v4 対応)越えが可能。
- ✓ 代表的な RAT: Poison ivy、Gh0st RAT など。一部は一般公開され誰でも利用可能。
- ✓ 標的型攻撃(標的型諜報攻撃)メール添付ファイルに隠れる形で攻撃に使用されるケースが増加している。
- ✓ 攻撃者は外部から以下の機能を実施可能。これにより感染端末を介したシステム内の探索や攻撃が可能

機能: ファイル/フォルダ操作、プロセス操作、コマンド実行、スクリーンキャプチャ、中継/更新機能 等

・RAT の侵入方法

標的型メールにマルウェアとして添付された形で入口対策を突破、攻撃目標とするシステム内部の一般ユーザ端末(PC)に侵入。

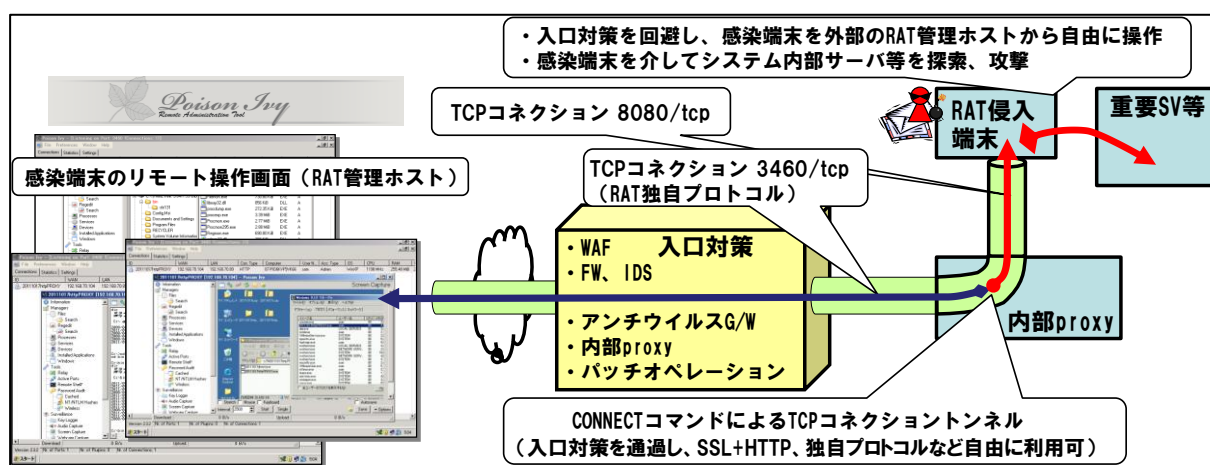


図 4-5-3-2: RAT (Poison Ivy) における侵入イメージ

■RAT の内部 proxy 通信(CONNECT 接続)の検知遮断実験

実験内容

情報システムのネットワーク構成を模擬した環境において、Poison ivy(RAT)の能力検証と Poison ivy(RAT) 機能を用いた CONNECT コマンドによる TCP コネクショントンネル接続状況下での検知遮断実験を行い、通信データ並びに内部 proxy での通信ログを取得しました。

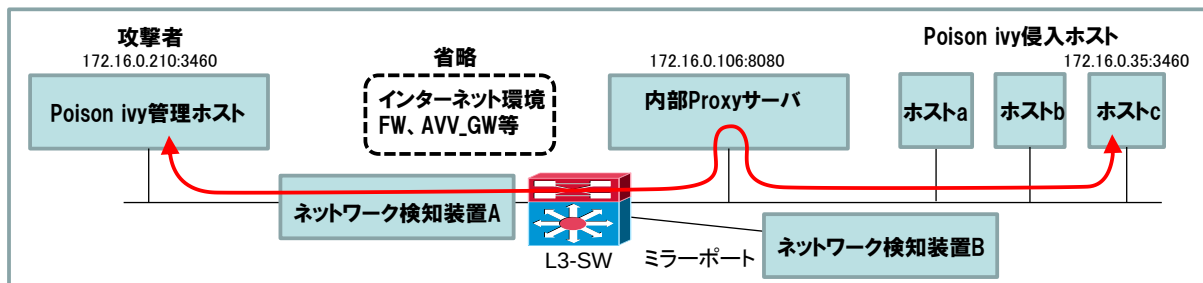
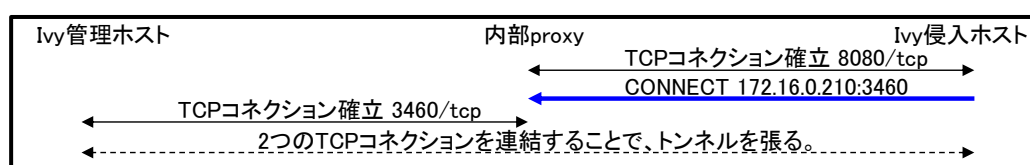


図 4-5-3-3: AT の内部 proxy 通信(CONNECT 接続)の検知遮断実験環境

Poison Ivy 通信の特徴

- ① Poison ivy のプロトコルは任意指定の独自プロトコル。(デフォルト: 3460/tcp CONNECT 発行により、proxy を介してトンネルを張れる。)



- ② ivy ホスト作成時に次のような設定と動作が可能
 - ・プロキシを明示的に指定できる。
 - ・システムに設定されているプロキシ設定値を窃取する。(この場合、IE に設定されているプロキシ設定値を利用)
 - ・管理ホスト側の待ち受け port のデフォルトは 3460/tcp だが、Ivy マルウェアを作成時に任意の待ち受け port を指定可能。
- ③ ivy は SSL を使わない(https バックドア通信(CONNECT 接続)対策は、本実験とは別に検証し対策を検討する必要がある。)
 - ・ivy の場合: CONNECT 接続した TCP コネクション上で独自プロトコルを使用
 - ・https の場合: CONNECT 接続した TCP コネクション上で SSL+HTTP プロトコルを使用
- ④ ivy は共通鍵暗号を利用した暗号通信を行う。

検知遮断実験結果

この検知遮断実験結果は次の通りです。

- ① ivy が内部 proxy と CONNECT で通信経路トンネルを作り、ネットワーク設計ルールに従った通信を行うため、proxy や FW のルール設定のみで完全に止めるのは難しいが、ivy の通信特徴から発見出来る可能性がある。
- ② ivy は、セッションが張りっぱなしなので、proxy ログは CONNECT 切断時のみ出力する。
- ③ proxy ログは(ヘッダ記録を指定しない限り)CONNECT 発行のみ記録する。


```
172.16.0.35 -- [17/Nov/2011:16:22:52 +0900]  
"CONNECT 172.16.0.210:3460 HTTP/1.0" 200
```

- ④ ivy の場合には、CONNECT のときに、HTTP ヘッダ(例えば、User-Agent など)をまったくつけないため、CONNECT 確立通信要求が CONNECT 行のみとなる。(ivy のみの特徴)

```
ivyの場合:  
CONNECT 172.16.0.210:3460 HTTP/1.0  
IEなどの場合:  
CONNECT 172.16.0.210:3460 HTTP/1.0  
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1  
Proxy-Connection: proxy-keepalive
```

- ⑤ Ivy がデフォルトポート(3460/tcp)を使用した場合は、プロキシの CONNECT 172.16.0.210 [**] において、**を特定のポート番号に限定するネットワーク設計を行った場合は遮断可能。

squidのデフォルト設定例

443以外のCONNECTは拒否する。
管理ホストの待ち受けportをデフォルト
の3460から変更されても対策可能。

【SSL_portsで設定されている443以外へのCONNECTメソッドは拒否】

```
acl SSL_ports port 443  
acl CONNECT method CONNECT  
http_access deny CONNECT !SSL_ports
```

- ⑥ プロキシのログ分析で ivy 通信を監視可能。
Ivy 通信では下記ログが出力されるため、CONNECT という文字列を含む行のうち、443/tcp 以外の行を proxy ログ上で監視。

```
「CONNECT 172.16.0.210:3460」(grep CONNECT access_log | grep -v :443)
```

【実装項目④：最重要部のインターネット直接接続の分離設計】

■通信経路の設計例

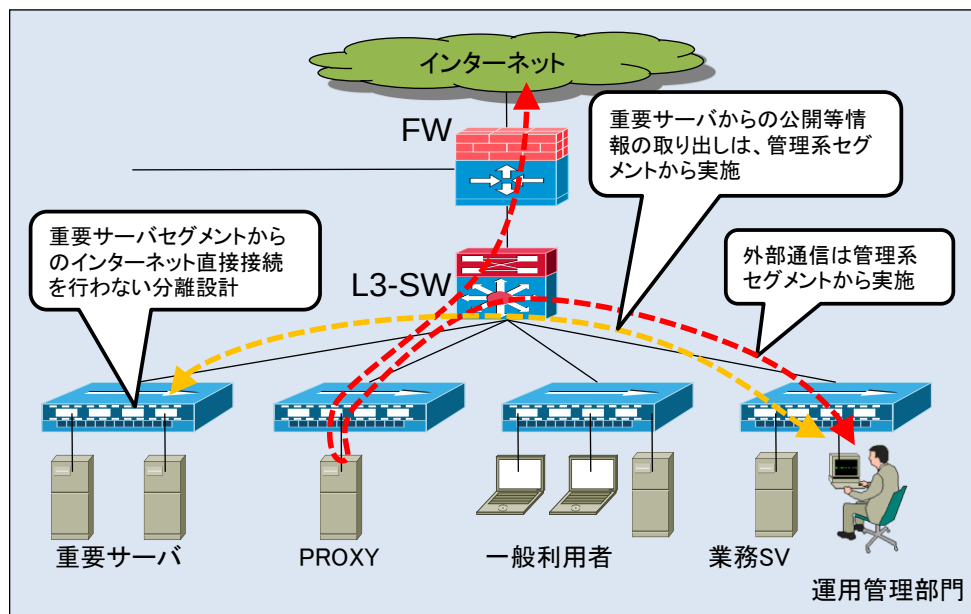


図 4-5-4-1: 重要サーバからのインターネット直接接続を行わない分離設計イメージ

この対策の目的は、「最重要部へのバックドア設置の回避」です。対策の対象は、「共通脅威6パターン」における「システム内情報の探査機能」です。この対策は、「実装項目⑧：P2P 到達範囲の限定設計」と併せて実施します。

■通信経路の実施事項

4-1

👉 VLAN による重要サーバがインターネット直接接続を行わない分離設計

最重要部(重要サーバ)の通常サービス(http, ssl)に関するインターネット直接接続を行わないように、VLAN 等により分離設計し、外部攻撃サーバからの制御シーケンスの影響を回避します。

例えば、上記の分離設計を含め次のような考えで設計を行います。

- ✓ 重要サーバからインターネットへ直接アクセスしないよう、VLAN 等による分離を行う。
- ✓ 重要サーバからの情報の取り出しを管理系セグメントのみから行う
- ✓ インターネットとのアクセスは管理系セグメントから行う

【実装項目⑤:重要攻撃目標サーバの防護】

この対策の目的は、「攻撃対象となる重要サーバの防護」です。対策の対象は、「共通脅威6パターン」における「システム内情報の探査機能」です。標的型諜報攻撃では、ユーザ端末や管理端末を攻撃後、組織配置情報等を窃取し攻撃目標を特定するケースが多いため組織配置情報等(社内の全メールアドレスや認証情報等)が一括保存されている認証サーバを攻撃対象です。このため同サーバを重要装置と位置付け、防護設計を行います。また、認証サーバにレプリカサーバがある場合は、同じ対策を取る事が必要です。

なお、この対策は、「実装項目④:最重要部のインターネット直接接続の分離設計」、「実装項目⑧:P2P 到達範囲の限定設計」と併せて実施します。

■通信経路の実施事項

5-1

👉 認証サーバ管理セグメント、認証サーバセグメントの防護

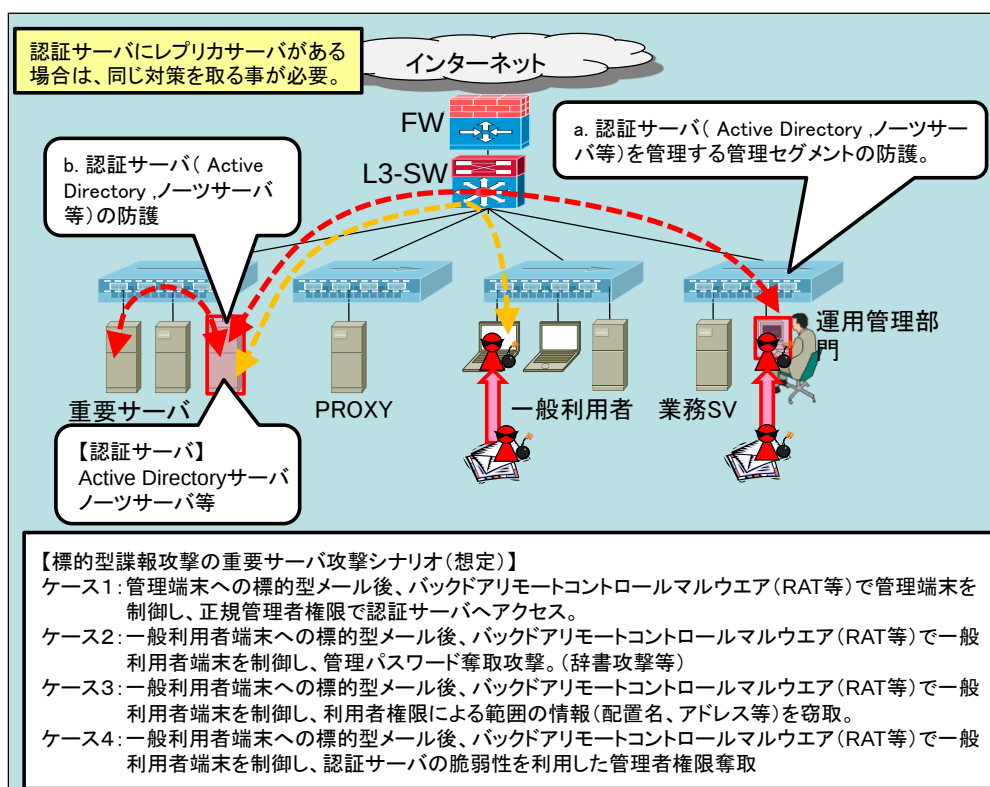


図 4-5-5-1: 認証サーバセグメント、認証サーバ管理セグメントの防護設計イメージ

この対策は、直ちに実行可能な対策です。しかし、管理端末及びユーザ端末からのバックドアリモートコントロールを用いた認証サーバアクセス対策に関しては、本対策では限界があります。

a. 認証サーバ(Active Directory, ノーツサーバ等)を管理する管理セグメントの防護

認証サーバを管理するセグメントに対しては、次のような対策を施します。

- (a) 管理セグメント以外のセグメントに対してポートを開けない。(管理セグメントからの通信とする)
- (b) 管理端末への優先的脆弱性パッチ当て。

b. 認証サーバ(Active Directory, ノーツサーバ等)の防護

認証サーバセグメントに対しては、次のような対策を施します。

- (a) 「認証サーバへのログインは管理端末のみ許可する」アクセスコントロール設計を実施。
- (b) 利用者端末から認証サーバに対する管理パスワード奪取攻撃(辞書攻撃等)対策の実施。

例: 認証サーバの連続ログイン試行回数制限を設定

参考: Active Directoryアカウント ロックアウト ポリシーのマイクロソフト推奨値
各設定値は、システム全体設計、業務設計と整合しチューニングする必要がある。

- ・ロックアウト期間 15 分
- ・アカウントのロックアウトのしきい値 10 回ログインに失敗
- ・ロックアウト カウンタのリセット 15 分

- (c) 利用者端末から見える認証サーバ各サービスに対する(サーバに対する)優先的脆弱性パッチ当て

5-2

🔍 換装等タイミングに向けての検討対象として考慮する対策

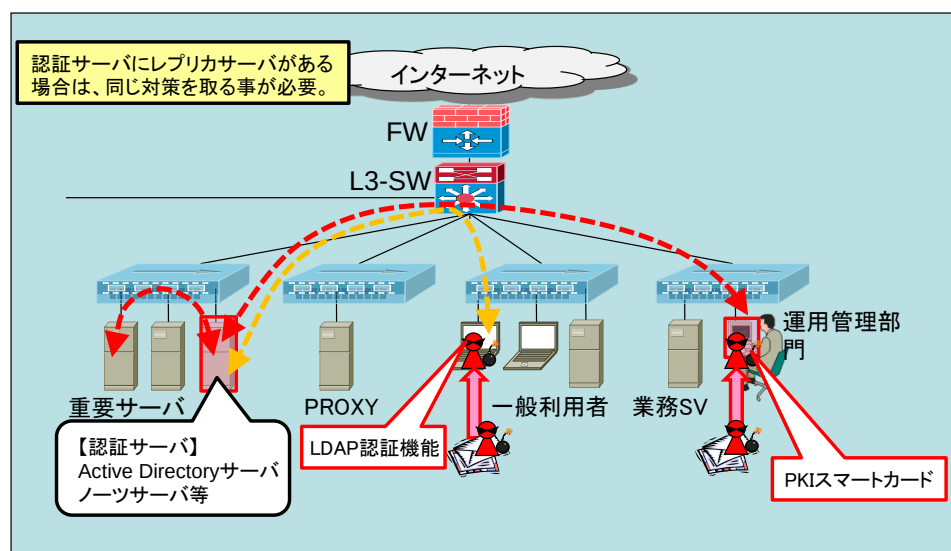


図 4-5-5-2: 認証サーバセグメント、認証サーバ管理セグメントの防護設計イメージ

a. ユーザセグメント(一般利用者)からの LDAP アクセスに認証を検討

(ただし業務運用との整合調整が必要)

b. 管理者端末と重要サーバ(AD 含む)との間に PKI 認証を行うためのスマートカードを導入し、管理者はアクセス時のみスマートカードを差し込む運用を行う

(これによりマルウェアによる AD ログインは不能)

■参考: その他の要検討設計手法案

重要セグメントにある認証サーバから、必要な情報だけを複製した参照用 LDAP サーバを一般利用者がアクセス可能な業務サーバセグメントに配置します。これにより、重要セグメントへの一般利用者のアクセスを止める設計になります(重要セグメントへの一般端末のアクセスを禁止する設計思想)。ただし、認証サーバの LDAP 機能以外(ユーザ認証)との関連や不要なユーザ情報の分類等、システム全体設計との整合を図りつつ、慎重に検証を行いながら検討する必要があります。

また、攻撃者が組織の情報やメールアドレス窃取を目的とする場合の防御効果は期待できませんが、標的型攻撃が侵入しやすい一般利用者セグメントから重要サーバセグメントへのアクセスを制限する効果は期待できます。

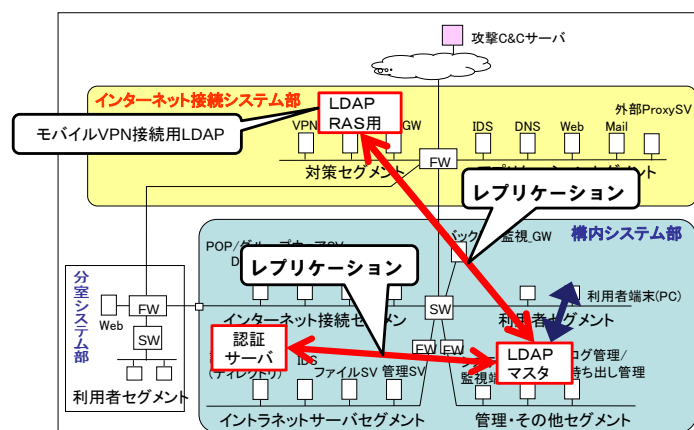


図 4-5-5-3: 重要セグメントへの一般端末のアクセスを禁止する設計イメージ

■参考: AD のネットワークポロジ設計を行う際の課題事項

Active Directory の設計を考えるうえで、現時点では次のような課題があります。

- ① AD は重要サーバが参照するため、重要サーバセグメントに配置せざるを得ない。
- ② AD は直接利用者にサービスを提供しているため、業務サーバセグメントを経由した一般利用者アクセス設計が困難。
- ③ 重要サーバセグメントは安全上、一般利用者セグメントからの全アクセスを禁止(deny)したいが、AD を重要サーバセグメントに設置する(置かざるを得ないため)ため、一般利用者セグメントからのアクセスを禁止することが出来なくなる。このため、他の重要サーバにも危険性が及ぶ場合がある。
- ④ 一般ユーザセグメントから重要サーバセグメントへのアクセス可能なポートも制限を行う場合は、業務利用ポートや AD が使用するサービスポートを全て把握する必要があるが、使用理由のブラックボックス(不明)なものが多い。
- ⑤ 一般ユーザセグメントから AD(重要サーバセグメント)へのアクセスルートを Exchange などの業務サーバ(セグメント)を経由するアクセスコントロール設計に関し、実現可能性やシステム全体設計面から再検討する必要がある。

AD の主要提供サービス

- ディレクトリサービス(LDAP)
- クライアント管理(SMB ファイル共有)
- ユーザ認証(Kerberos)
- MAPI(RPC over TCP のメッセージング API(ExchangeServer を使用する場合))

【実装項目⑦：容量負荷監視による感染動作の検出】

■通信経路の設計例

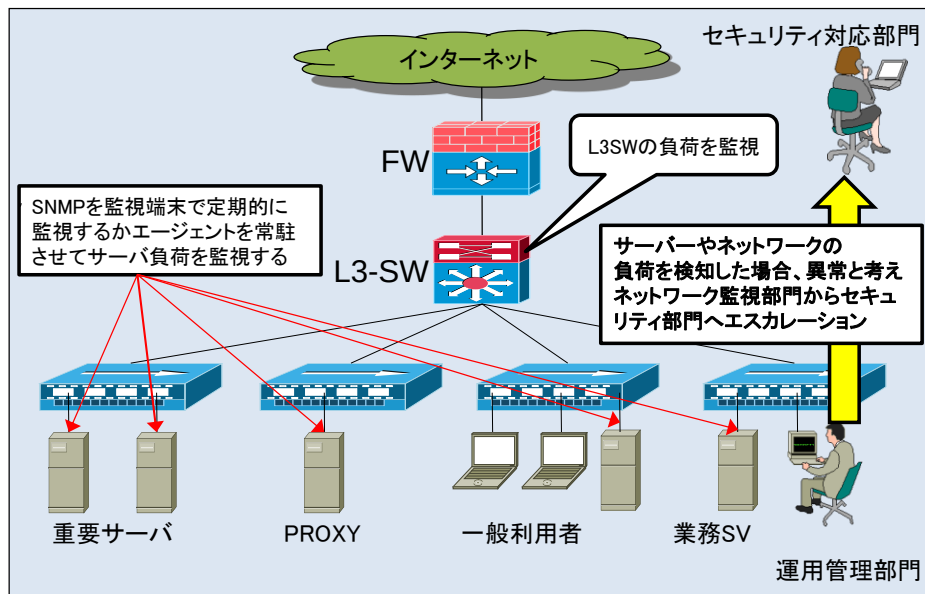


図 4-5-7-1: 負荷を監視する設計イメージ

この対策の目的は、「ウイルスの拡散範囲の限定と検知」です。対策の対象は、「共通脅威6パターン」における「侵入システム内感染拡大機能」です。この対策には、ネットワーク監視部門とセキュリティ対応部門とが連携できる体制を検討する必要があります。

■通信経路における実施事項

7-1

👁 ファイルサーバ、SW 等負荷及びログ容量等異常負荷監視機能設計

ウイルスは組織内に感染を広げる際、多くのパケットを送付するため各サーバやルータ等に負荷がかかったり、ログ容量の増加といった異常な負荷がかかったりすることがあります。ネットワーク監視部門は各サーバやルータ等に負荷がかかっている場合、セキュリティ対応部門にエスカレーションをし、ウイルスに感染している端末が存在するのか等の判断を求めます。

【実装項目⑧:P2P 到達範囲の限定設計】

■通信経路の設計例

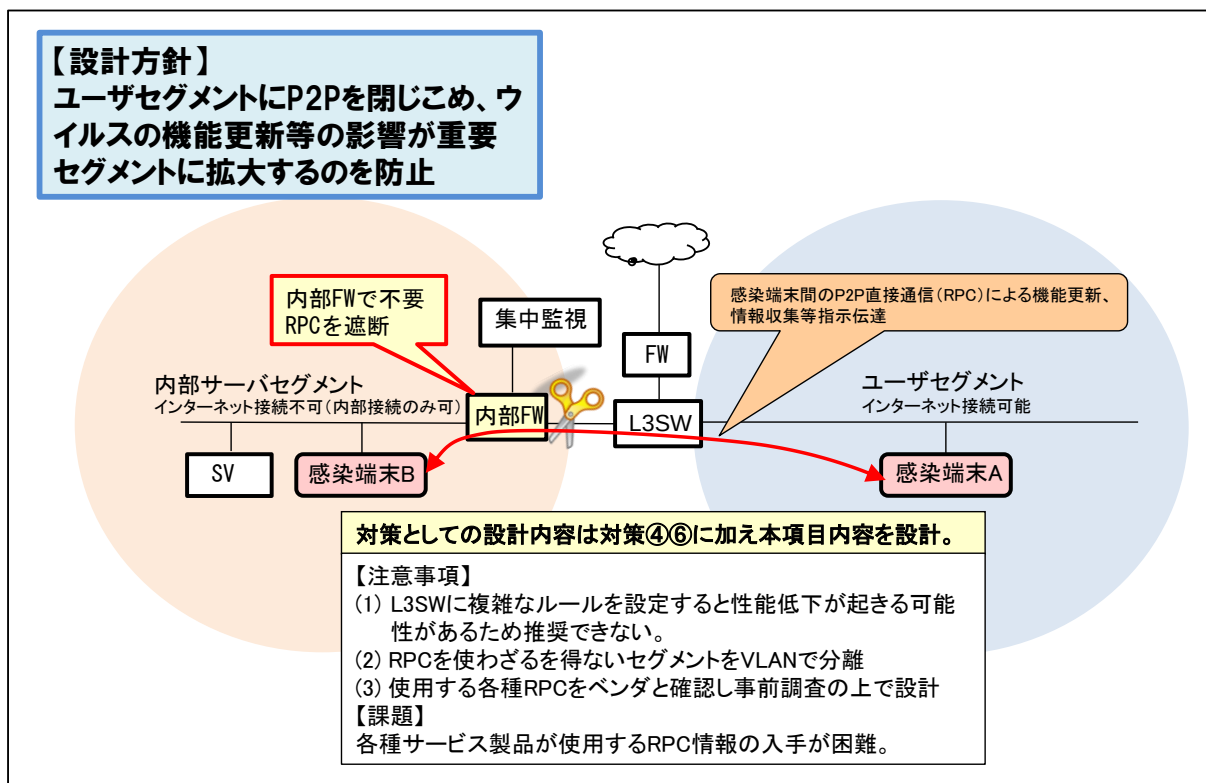


図 4-5-8-1: 負荷を監視する設計イメージ

この対策の目的は、「内部拡散済みウイルス間での更新指示等が内部で渡る脅威を抑止」です。

対策の対象は、「共通脅威6パターン」における「侵入システム内感染拡大機能」です。この対策は、「実装項目④: 最重要部のインターネット直接接続の分離設計」および「実装項目⑥: SW 等での VLAN ネットワーク分離設計」と併せて実施します。

■通信経路における実施事項

8-1

👉 不要な RPC 通信を排除したネットワーク設計

ウイルスは、内部拡散済みウイルス間での更新指示等を行います。システム内部に渡った更新指示の脅威を抑止するために、これらの通信の特徴を把握する必要があります。これらの通信の特徴は次のようなものが挙げられます。

- ✓ P2P を使用した機能更新、情報収集等の通信のやり取りを行う。

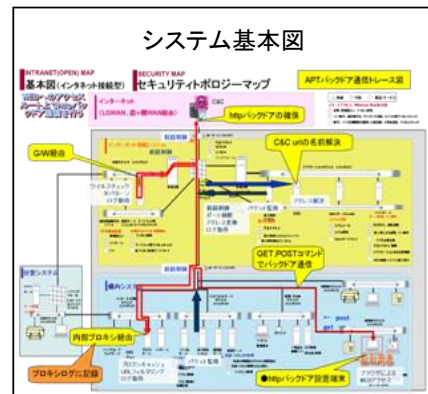
このような通信の例として Stuxnet における MS-RPC を利用したものが挙げられます。

P2P である理由は、システム内部から http 接続できないセグメント上に感染した端末に対しても機能更新、情報収集等が可能となります。

このように更新されたウイルスは特にサーバセグメントにおいては、検知・駆除が難しくなります。

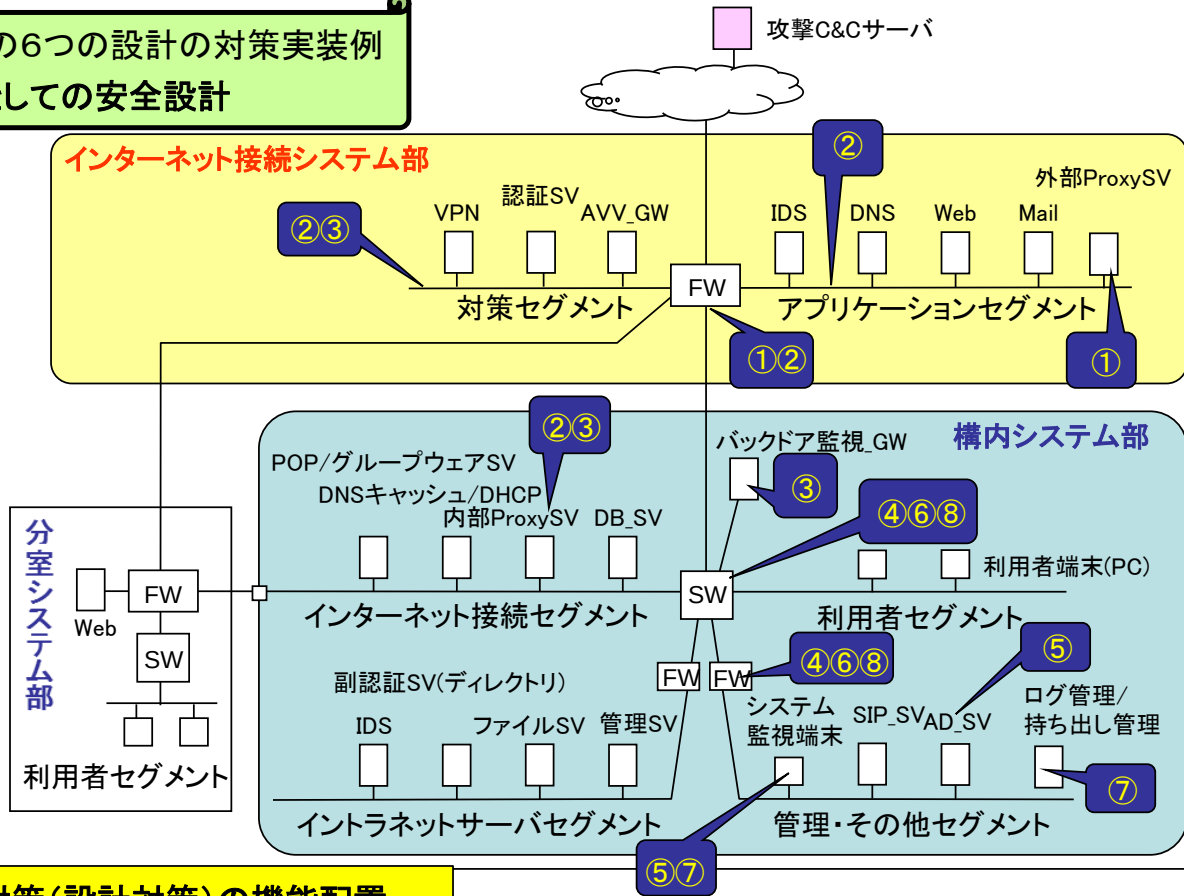
設計対策システム設計実装図例

標準的なシステム構成図上での6つの設計の対策実装例 システムの出口対策としての安全設計



システムのサービス通信フローを分析した上で、設計対策項目の実装を検討。

この際、新しいタイプの攻撃のシステム上の共通攻撃通信フローを分析



情報システムに対する8つの出口対策(設計対策)の機能配置

- ① サービス通信経路設計の実施
- ② ブラウザ通信パターンを模倣するhttp通信検知機能の設計(一部調査中)
- ③ RATの内部proxy通信(CONNECT接続)の検知遮断設計(一部調査中)
- ④ 最重要部のインターネット直接接続の分離設計
- ⑤ 重要攻撃目標サーバの防護
- ⑥ SW等でのVLANネットワーク分離設計
- ⑦ 容量負荷監視による感染動作の検出
- ⑧ P2P到達範囲の限定設計

各対策項目の設計該当箇所の実装図を参考にして、システム設計を行う。

付録 1:実装項目における実証結果

本「付録1 実証検証結果」は、4.5 実装項目「②-2 当該マルウェア固有の http ヘッダ等、通信の特徴からバックドア通信を判別」を対策として検討するための技術的可能性を調査したものです。対象とする共通脅威パターンは、攻撃サーバ(C&C)とマルウェア間の http バックドア通信が通信経路設計に沿って行われブラウザと同様な http メソッドを持っており、実装項目①「サービス通信経路設計の実施」対策を回避する通信です。

マルウェア解析から得られた通信動作の特徴分析を行った上で、検知遮断出来る技術を実際のマルウェアが行う http バックドア通信を用いて実機検証しました。また、バックドア通信上で攻撃サーバと侵入システムの間での RAT(リモートコントロール)ツールを使った通信を検知する手法についても検証を行いました。

本実証検証結果は、トレンドマイクロ社、日本 IBM 社の製品を使用して実施しました。本検証は次の4種類を実施しました。

付表 1-1:実証検証内容

No	実証検証内容	協力
1	ウイルスの http ヘッダ User-Agent を検知 (ルールベース検知実装技術での検証)	トレンドマイクロ社
2	ウイルス独自の http 拡張ヘッダを検知(IDS,IPS 実装技術での検証)	-
3	ウイルスが送信する HTTP ヘッダ長に着目したアプローチ	日本 IBM 社

検証事例1: ウイルスのhttpヘッダUser-Agentを検知(ルールベース検知実装技術での検証)

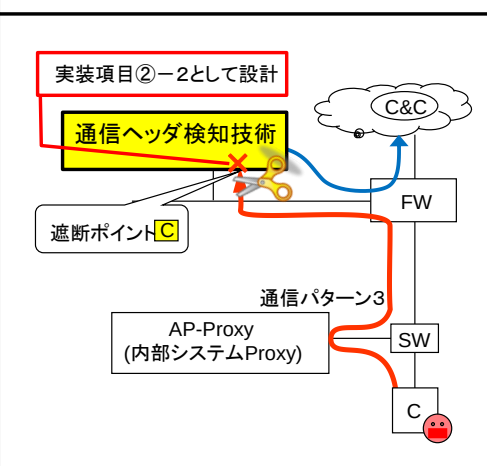
以下の特徴から検知:

ウイルスのhttpヘッダ拡張のUser-Agentはブラウザのものとは異なる場合が多い。

【検知技術】

ブラウザ等が使用するUser-Agentをホワイトリスト化し、ウイルスが使用するUser-Agent (bad user-agent) と比較検出する。

検証環境(システムへの設計使用例)



【検証結果等】

- (1) 市販の製品で実装されている検知ルールを実証実験用にカスタマイズして実施した。
- (2) ウイルスがブラウザ通信と同じUser-Agentを模倣した場合は遮断出来ないが、多くのマルウェアはブラウザとは異なる固有のUser-Agentを使用しているため、一定の効果は期待できる。
- (3) httpプロトコル(port80)は種々の目的で各種製品仕様に多用しており、かつ仕様が一部非開示なため、ホワイトリスト技術のみに頼る手法の検知精度はホワイトリストの精度と作成技術に依存する。
- (4) User-Agentホワイトリスト技術は、APT攻撃に対する一定の絞り込み対策としての位置付けとして捉えるアプローチ。
- (5) User-Agentのホワイトリストのみでなく、その他のhttpヘッダー特徴等の検知技術を組み合わせて分析する必要がある。

参考: ルールベース検知技術例

Event ID	Source	Destination	Port	Protocol	Severity	Message
2011-06-23 05:25:43 PM	172.16.71.100	203.106.85.49	80	HTTP	High	User-Agent: RookIE/1.0

User-Agent例:

■ IE8利用時→通過

User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30; .NET CLR 3.0.04506.648)

■ マルウェアが使用したUser-Agent→検知遮断

User-Agent: **RookIE/1.0**

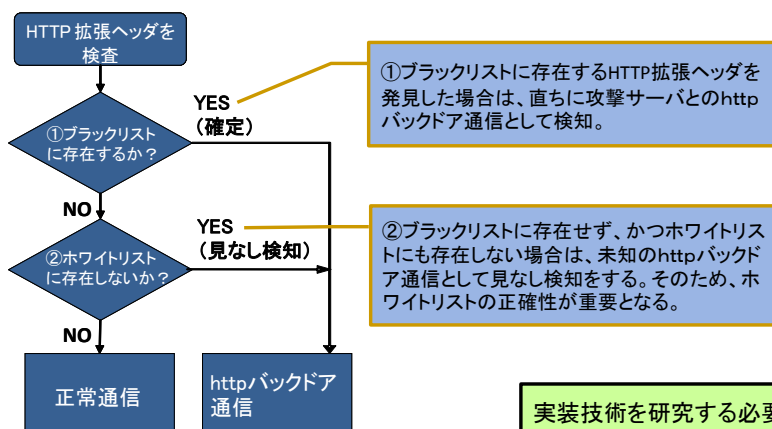
検証事例2: ウイルス独自のhttp拡張ヘッダを検知(IDS,IPS実装技術での検証)－1

以下の特徴から検知:
ウイルスのhttpヘッダ拡張のUser-Agentはブラウザのものとは異なる場合が多い。

【検知技術】

ブラウザやhttp使用アプリケーションが使用するHTTP拡張ヘッダを構文解析しホワイトリスト化。一方ウイルスが使用するHTTP拡張ヘッダのリストを維持。HTTPパケット中に見られるHTTP拡張ヘッダがこれらのリスト中に存在するかどうかで検知する。一般的なIDS/IPSでは標準機能では実装していないが、カスタミングネチャ作成することにより、対応可能である。リアルタイム性を重視しないのであれば、センサーの管理マネージャ側でログ解析により検知することも可能。

HTTP拡張ヘッダを検査するための処理概念



HTTP拡張ヘッダ情報

ブラックリスト
Malwareが生成する既知のHTTP拡張ヘッダのリスト
(攻撃情報を入手)

ホワイトリスト
Proxy等の機器やアプリが生成する拡張ヘッダのリスト(ベンダーから情報を入手)

実装技術を研究する必要があるため、実機検証は未実施。

検証事例2: ウイルス独自のhttp拡張ヘッダを検知(IDS,IPS実装技術での検証)－2

【検証結果等】

- (1) システムで使用するブラウザやhttp使用製品アプリケーションの仕様メソッドをベジアン技術等を用いた分析toolによる事前分析を行う事により、システム毎の精度の高いホワイトリストが作成出来る可能性がある。このホワイトリストを用いたIDS管理マネージャ機能による検知実装技術を研究する必要がある。
- (2) 独自にHTTPを利用する製品アプリケーションも存在する点にも注意し、事前に自システム内アプリケーションを分析する事で一定程度、検知精度を上げることが出来る。
- (3) httpプロトコル(port80)を種々の目的で製品仕様に多用しており、かつ仕様が一部非開示なため、把握が困難。また、User-Agentは、製品のバージョンアップ、パッチ適応毎に変わってしまう事があるため、ホワイトリストの維持が難しい。
- (4) User-Agentホワイトリスト技術は、APT攻撃に対する一定の絞り込み対策としての位置付けとして捉えるアプローチ。
- (5) システムに使用する製品アプリケーションが使うportやプロトコル等を設計時に調査しておく事は、サイバー攻撃に対するシステムの弱点を把握する為に重要な事項である。

検証事例3: ウイルスが送信するHTTPヘッダ長に着目したアプローチ

以下の特徴から検知:
ウイルスのhttpバックドア通信ヘッダはIEに比べ安直でシンプルなヘッダの使い方をする場合がある。

【検知技術】

バックドア通信のhttpヘッダ長一般的に短いという特徴から、閾値以下の長さのものをIDSで検知する。

【検証課題】

単純に長さのみで検出するのではFalse Positiveが懸念されるため、有効性の検証を実施。

【検証結果等】

(1) 検証準備事項:

- IDSカスタムシグネチャで検知可能。
- 一般的なブラウザ、http使用アプリケーションのヘッダーの特定部分のヘッダ長の並びにバックドアマルウェア(数十検体)の該当httpヘッダ長を調査。
- マルウェアのバックドア通信と判断可能な目安閾値を分析。

(2) 検証結果:

- デスクトップのWebブラウザ利用環境を想定するならば、httpヘッダの特定部分の長さを識別する事でバックドア通信を検出できる。

(3) 実機検証の結果得た課題等:

- Webブラウザ以外によるHTTP通信については False Positive が発生する可能性がある。

(例: アプリケーションのアップデート通信、専用クライアント、その他内製アプリなど)

(4) 本手法で有効にバックドア通信を検出するためには、httpアプリケーションの調査と管理によるIPまたはURL、HTTPヘッダなどに基づいたホワイトリストの事前準備が必要。

【注意事項】

原理上、通常のブラウザヘッダを偽装するようなバックドア通信は検知できないので他の手段で対応する必要がある。

検証結果画面: マルウェアが送信するHTTPヘッダ長による検知

IBM Proventia® Network Intrusion Prevention System

Need Help? | Logout IBM

Home Appliance Dashboard Monitor Health and Statistics Secure Protection Settings Manage System Settings Review Analysis and Diagnostics

Control: Local Management Interface
GX4002@soc-test-f43-gx4002
Clear Alerts

Security Alerts

2011-07-19 17:56:39 - 2011-07-19 16:44:41

IssueID	Event Name	Severity	Source IP	Target IP	Protocol	Protection Domain	VlanID	Status	Time
5000002	SensorStatistics	▼	0.0.0.0	0.0.0.0	0	Global		⚠	19 Jul 2011 17:56:39
5000005	CoalescerStatistics	▼	0.0.0.0	0.0.0.0	0	Global		⚠	19 Jul 2011 17:54:46
3000001	HTTP_Server_ID	▼	192.168.1.10	192.168.1.100	6 (TCP)	Global		⚠	19 Jul 2011 17:52:43
4	deploy-test-https	⚠	192.168.1.10	192.168.1.100	6 (TCP)	Global		⚠	19 Jul 2011 17:52:43
3000001	HTTP_Server_ID	▼	192.168.1.10	192.168.1.100	6 (TCP)	Global		⚠	19 Jul 2011 17:52:33
6005200	Trons_HTTP_Header_Too_Short	⚠	192.168.1.10	192.168.1.100	6 (TCP)	Global		⚠	19 Jul 2011 17:52:33

Event ID: 292891
Event Type: OpenSignature
Event Description:
Responses Executed:
DISPLAY=WithoutRaw0

Alert Details:
SourcePort:4029
DestinationPort:80
AdapterID:ExternalA
AdapterMode:Inline Protection
msg:Trons_HTTP_Header_Too_Short
offset:14
sid:5200

- IE7利用時 → 通過
ヘッダ長: 約550バイト
- マルウェアのHTTP通信 → 検知
ヘッダ長: 44バイト

※上記検証結果は、カスタムシグネチャを作成し検証した結果である。

付録 2: 対策要件定義テンプレート

本付録は、「4.5 大切な情報をサイバー攻撃により漏洩させない8つの対策」に記載された「各実装設計項目①～⑧」の内容を、自システムのネットワークポロジや通信機器等の環境に合わせて実装設計を検討する際の要領を纏めたものです。実装設計に必要な作業を、WBS(Work Breakdown Structure)の個々の作業項目に組み込んでいくためのガイドとなることを目的としています。

本付録が想定する、要件定義～実装設計までの一般的な作業項目を以下に示します。

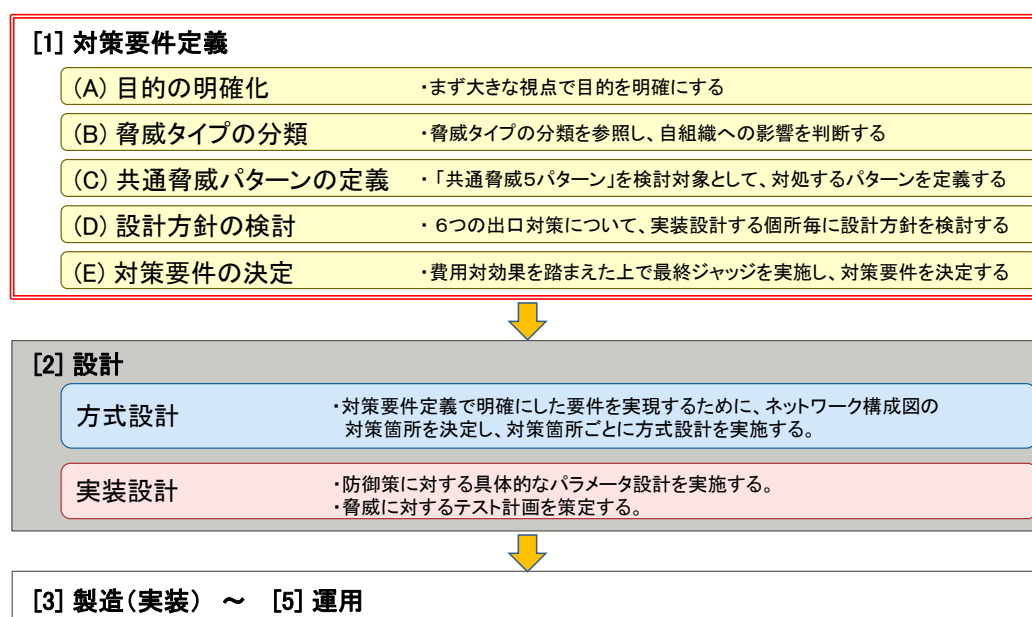
- (1) 対策要件定義の流れ
- (2) 「共通脅威6パターン」毎の対策検討
- (3) 工程毎の検討要領
- (4) 工程毎の作業項目(脅威対策 WBS)の検討

合わせて、作業項目や工程毎の成果物の事例を記載しています。これらを参考に、自システムやプロジェクトの特徴に合わせて実装設計を進めて下さい。また、工程定義は各契約形態や開発方式によって異なります。それぞれの工程定義に応じて準用して下さい。

本「対策要件テンプレート」は、共通フレーム SLCP-JCF2007 に示す各開発工程プロセス、アクティビティ、タスク等の規定内容に沿った形で作成しています。利用に際しては、各社の社内開発標準等を補うものとしてご活用下さい。

【(1) 対策要件定義の流れ】

本ガイドの各実装設計項目①～⑧の内容を実装設計するには、まずプロジェクト初期の段階で対策要件の定義を行うことが重要です。対策要件の定義を行った上で、各工程の作業項目に反映し実装設計して行きます。(本付録では、標準的な開発工程を、[1] 対策要件定義 → [2] 設計 → [3] 製造(実装) → [4] テスト → [5] 運用と想定しています。)



付図 2-1 対策要件定義の流れ

対策要件定義の流れを付表 2-1 に示します。

付表 2-1: 対策要件定義の流れ

対策要件定義の流れ	作業概要	本文の参照箇所
(A) 目的の明確化 情報を漏えいしたくない システムを破壊されたくない	・対策要件を決定する際には、まず大きな視点で目的を明確にします。明確化した目的を見失わずに実装設計を進める事が大切です。 ・左図では、以下の2点を例示しています －「情報を漏えいしたくない」 －「システムを破壊されたくない」	—
(B) 脅威タイプの分類 1. 標的型メール 2. ウェブサイトを経由した攻撃 3. 制御系破壊攻撃 4. USB感染マルウェア 5. 複合型DDoS攻撃	・次に、脅威をタイプ別の分類から自組織への影響を判断します((2)共通脅威6パターン毎の対策検討「脅威タイプ分類」をご利用ください)。 ・新しいタイプの攻撃が出現した場合は、IPA脅威と対策研究会で継続的に改訂公開していきます。	4.5 大切な情報をサイバー攻撃により漏洩させない8つの対策一覧関連図
(C) 共通脅威パターンの定義 1. バックドア通信 httpプロトコルバックドア port80、proxy未使用 2. バックドア通信 独自通信プロトコルバックドア port80、proxy未使用 3. バックドア通信 httpメソッド利用のバックドア port80、proxy使用 4. RAT通信 OCONECTコマンドによるRAT通信 port8080、内部proxy使用 5. システム内情報の搜索脅威 6. バックドアマルウェア のシステム内拡散、機能更新脅威	・セキュリティ対策を考える場合、“脅威タイプ”(例「標的型メール」)のままではどのように(How)設計すればよいか見えないため、「防御できる製品を探す」というのがこれまでの設計でした。 ・本ガイドでは、システム委託者と受託者の双方が脅威を理解し対抗する防御策を設計できるよう、新たなアプローチを追加しました。 ・IPA脅威と対策研究会で“脅威タイプ”を解析した結果、共通的な攻撃手法として左図の「共通脅威5パターン」を洗い出すことができました((2)共通脅威6パターン毎の対策検討「脅威タイプ分類」をご利用ください)。 ・これら「共通脅威6パターン」を検討対象とし、対処すべき脅威パターンを定義して下さい。 ・この工程で作成される「業務要件」と「全体ネットワーク構成図」から弱点を明確化し、対策要件定義を作成することが有効です。  「共通的脅威6パターン」を、設計に用いる対象脅威として定義します。なお共通脅威パターンは、テスト工程にも利用可能です。  (A)目的、(B)脅威タイプ、(C)共通脅威パターンを、委託者と共通認識を持ち要件定義書等に明記して下さい。	4.5 大切な情報をサイバー攻撃により漏洩させない8つの対策一覧関連図

対策要件定義の流れ	作業概要	本文の参照箇所
(D) 設計方針の検討 対策① サービス通信経路設計の実施 対策② ブラウザ通信パターンを模倣するhttp通信検知機能の設計 対策③ RATの内部proxy通(CONNECT接続)の検知遮断設計 対策④ 最重要部のインターネット直接接続の分離設計 対策⑤ 重要攻撃目標サーバの防護 対策⑥ SW等でのVLANセッetwork分離設計 対策⑦ 容量負荷監視による感染動作の検出 対策⑧ P2P到達範囲の限定設計	・設計対象となる「共通脅威6パターン」の防御設計をどのように(How)実現すればよいかを検討します。 ・IPA脅威と対策研究会の検証から、左図の6つの出口対策が、脅威がシステム深部に侵入したとしても、外部攻撃サーバとの通信の無力化として効果があるとの結果が得られました。(ガイド本文の4.5「実装項目①～実装項目⑧」をご覧ください) ・8つの出口対策について、実装設計する個所ごとの設計方針(How)を検討して行きます。検討要領を以下に示します。 ① 要件定義工程で作成した全体ネットワーク構成図(概略版)を準備する ② 全体ネットワーク構成図にゾーン(ネットワークセグメント)間の装置を記載する ③ 要件定義工程で作成した業務要件から、httpなどインターネット通信の他に業務アプリの通信経路も明記する ④ 「4. 4章 実装項目①～⑧」を参考に自システムでどのように実装設計を行うか検討する。  システム構成図にポイントを記載し、システム基盤／業務アプリなどの開発チーム間で共通認識を持ち、担当範囲(業務アプリ／通信サービス等)への影響を確認して下さい。	4.5 8つの設計対策内容の詳細(実装項目①～⑧)及び設計対策システム設計実装図例)
(E) 対策要件の決定	・(A)目的の明確化～(E) 防御対策を検討した結果、最後に設計～確認テストまでの費用を見積り、費用対効果を踏まえた上で最終ジャッジを実施して、対策要件を決定して下さい。 ・目的に対しどのような脅威が想定され、対策手法をお客様とSIerで認識を合わせることがポイントです。 ・また、設定や製品の配置で脅威対策は終わるものではなく、実運用でどのように監視／運用するのかについても検討すべきでしょう。 ・脅威に対する防御と影響の回避はシステム設計で全て決まるということを忘れずに実施してください。	2.5 予算を効果的に使う設計アプローチ

【(2) 共通脅威5パターン毎の対策検討】

共通脅威5パターン毎の対策検討は次の付表 2-2 の通りです。

付表 2-2: 共通脅威6パターン毎の対策検討

脅威タイプ分類	共通脅威6パターン	対策概要
■情報漏えい、システム破壊を目的にした5つの脅威タイプ タイプ1: 標的型メール タイプ2: ウェブサイトを経由した攻撃 タイプ3: 制御系破壊攻撃 タイプ4: USB感染マルウェア タイプ5: 複合型DDoS攻撃	共通脅威パターン1: バックドア通信 ○httpプロトコルバックドア通信 ○port80、proxy未使用	■FWの外向通信遮断ルール設定 ・内部proxy経由の外向通信のみ許可 ・端末からの直接通信の遮断 ・監視／分析タイミング及び運用方法を設計する <i>詳細は、4. 5章 対策①</i>
	共通脅威パターン2: バックドア通信 ○独自通信プロトコルバックドア通信 ○port80、proxy未使用	■FWの遮断ログ監視 ・遮断ログを記録分析し、感染端末の特定を実施 ・ログ保存装置と生データ容量の見積りを実施 ・圧縮保存する場合は装置及び媒体容量を見積もる ・監視／分析タイミング及び運用方法を設計する <i>詳細は、4. 5章 対策①</i>
	共通脅威パターン3: バックドア通信 ○httpメソッド(GET,POST,CONNECT)利用のバックドア通信 ○port80、proxy使用	■JavaScriptやMETAタグを利用したリダイレクト ・ProxyにJavaScriptやMETAタグを利用したリダイレクト機能を実装する ■通信の特徴からバックドア通信を検出 ・ログ監視から通常時と違う通信を検出する 例: Internetに当社のサーバが存在しないのに POSTメソッドで外部に通信が発生しているなど ・監視／分析タイミング及び運用方法を設計する <i>詳細は、4. 5章 対策②</i>
	共通脅威パターン4: RAT通信 ○内部proxyへのCONNECTコマンドによるRATのバックドア通信 ○port8080、内部proxy使用	■RATの内部proxy通信(CONNECT接続)を遮断 ・proxyログからRATのCONNECT通信を検出 ・専用機の使用も検討。 <i>詳細は、4. 5章 対策③</i>
■情報漏えい、システム破壊を目的にした5つの脅威タイプ タイプ1: 標的型メール タイプ2: ウェブサイトを経由した攻撃 タイプ3: 制御系破壊攻撃 タイプ4: USB感染マルウェア タイプ5: 複合型DDoS攻撃	脅威パターン5: ○システム内情報の搜索脅威	■最重要部へのバックドア設置回避 ・サーバ用途別、利用部門別、管理者など役割に応じたゾーン(セグメントで区切る)設計を実施する ・インターネットに直接接続できる環境を最重要サーバゾーンに与えない ・探索目標となる重要サーバを防護 <i>詳細は、4. 5章 対策④⑤</i> <i><対策③に合わせて最終的に修正する></i>
	脅威パターン6: ○バックドアマルウェアのシステム内拡散、機能更新脅威	■スイッチ等でのVLANネットワーク分離設計 ・サーバ用途別、利用部門別、管理者など役割に応じたゾーン(セグメントで区切る)設計を実施する ・バックドアマルウェア内部拡散の影響を最小化するために、影響範囲をネットワーク設計上分離する <i>詳細は、4. 5章 対策⑥</i> ■容量負荷監視による感染動作の検出 ・ログ容量／内容、通信量など日常と違う兆候を監視するための運用設計を実施する ・permission deniedが多発している、Reject／DropなどFWブロックログ、ネットワーク機材のルール違反ログなどの分析／解析運用設計 <i>詳細は、4. 5章 対策⑦</i>

脅威タイプ分類	共通脅威6パターン	対策概要
■情報漏えい、システム破壊を目的にした5つの脅威タイプ タイプ1: 標的型メール タイプ2: ウェブサイトを經由した攻撃 タイプ3: 制御系破壊攻撃 タイプ4: USB感染マルウェア タイプ5: 複合型DDoS攻撃	脅威パターン5: ○バックドアマルウェアのシステム内拡散、機能更新脅威	■P2P到達範囲の限定設計 ・内部Firewall(インターネット接続可能ゾーンと接続不可ゾーン間に設置)で不要RPCを遮断 ・設計内容は対策⑧(④、⑤、⑥と同じ) <i>詳細は、4. 5章 対策⑧(④⑤⑥)</i>

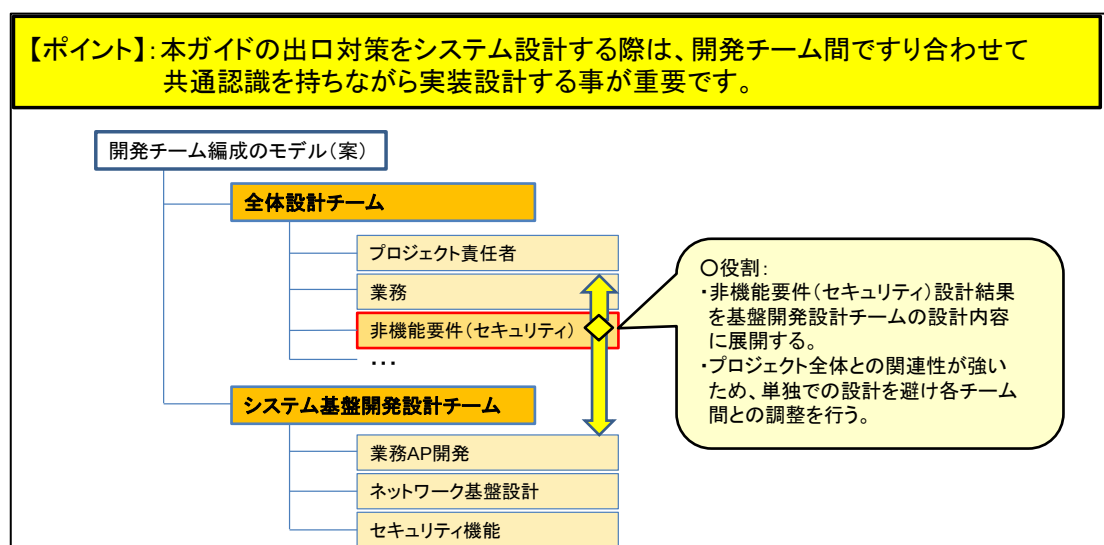
【(3) 工程毎の検討要領】

共通脅威パターンに対する具体的な設計対策を、工程毎の作業項目に反映していきます。反映する際は、開発チーム間の連携や、作業項目間の依存関係(ある作業項目の成果物が他の作業項目のインプットになる等)などを考慮すると良いでしょう。

付表 2-2 は、本ガイドにおけるシステム開発プロジェクトの開発チーム編成のモデルです。

ー 出口対策(実装項目①～⑧)をシステム設計対策手法として実装設計できるよう、全体設計チームに非機能要件(セキュリティ)チームを設定しています。

ー 従来の入口対策に相当するセキュリティ機能(アクセス制御、ウイルス対策、識別認証など)は、単独で実装設計を進めず、全体設計チームと連携して進める事が重要です。



付図 2-2 開発チーム編成モデル

		[1] 対策要件定義	[2] 設計	[3] 製造(実装)	[4] テスト	[5] 運用
全体設計チーム	経営	・投資対効果の検討 ・ステークホルダとの関係構築	・ステークホルダとの役割明確化 ・HW/SW調達の承認	・工程完了承認		
	業務	・ステークホルダから現行業務/システムをヒアリング ・業務要件の作成	・業務設計	・業務テスト計画 ・業務データの整備	・業務テスト	
	非機能要件(セキュリティ)	<1> システム全体のセキュリティ要件の定義 (A) 防御対策の目的 (B) 脅威タイプ (C) 共通脅威パターン (D) 出口対策 (E) 防御対策の設計	<2> システム全体のセキュリティ要件の仕様化(セキュリティ共通指針策定) ・方式設計及び実装設計(ログ統合、監視統合、ネットワーク分離方針)	<3> ・非機能要件(セキュリティ)のレビュー ・システム全体の防御テスト計画 ・システム全体のリスクコントロール運用の整備 出口対策: システム全体設計の一環	<4> ・システム全体の防御テスト	・リスクコントロール業務(監視、分析)
システム基盤開発チーム	業務AP開発	・アプリケーション形態の決定 ・フレームワークの調査/選定	・機能概要 ・機能方式 ・プロセス設計	・プログラム構造設計	・アプリケーション(AP)開発 ・AP単体動作 ・業務動作テスト	・業務運用サポート
	インフラ	・インフラ要件整理 ーネットワークセグメント定義 ー業務ホワイトリストの定義	・インフラ概要設計 ・インフラ方式設計 ーネットワーク設計 ・HW/SW設計 ーログ容量の見積もり	・インフラ環境設計(デザインシート作成)	・環境構築 ・インフラ動作テスト	・基盤サポート
	セキュリティ機能	・セキュリティ機能要件整理 ーセキュリティ機能の配置	・セキュリティ機能方式設計 ーファイアウォール ーウイルス対策 ースパム対策 ーアクセス制御など	・セキュリティ機能詳細設計(デザインシート作成)	・セキュリティ機能構築 ・セキュリティ機能単体テスト	・セキュリティ機能サポート
成果物		要件定義書 ・セキュリティ全体要件	全体設計書 ・セキュリティ共通指針 基本設計書 詳細設計書 (デザインシート等)	防御テストシナリオ 運用手順書	防御テスト結果確認	運用手順書

付図 2-3 工程毎の検討要領

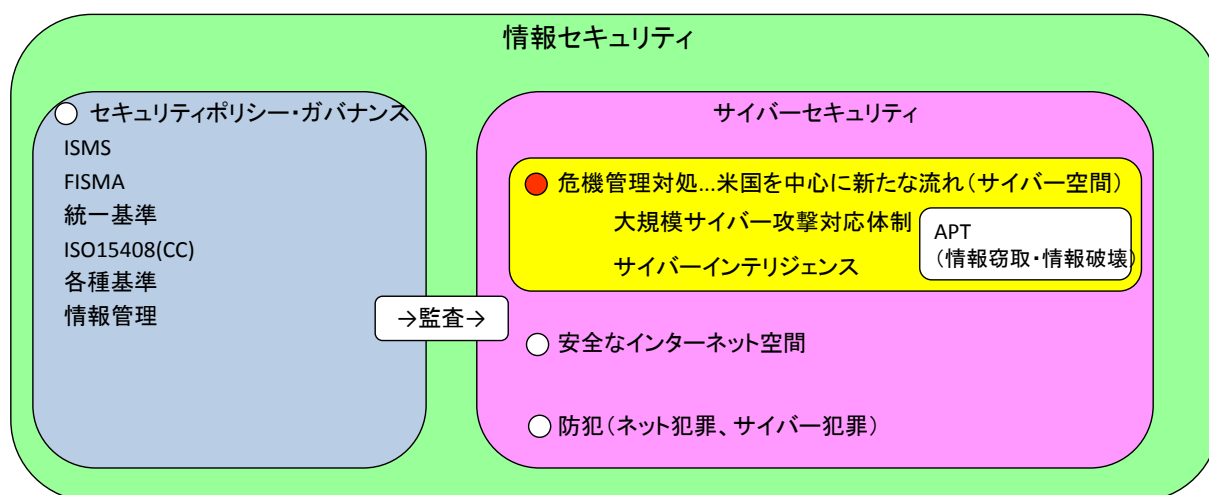
付録 3: 情報セキュリティ対策の整理

情報セキュリティ対策と一口に言っても、それぞれの対策で目的が異なります。大きく分けると、2 つ (付図 2-1)があります。

- ① 社員が内部資料を持ち出すことを防止や、コンプライアンスを遵守することなどを目的とした対策
- ② 外部からのサイバー攻撃から組織を守ることを目的とした対策

情報セキュリティ対策を検討する際に、この 2 つの目的を整理して対策を行うことが望ましいものです。それは、「何をどこから守る」ために対策を実施するのかが不明のまま対策を実施すると、その対策が有効であるかどうか不明になってしまいます。それは、せっかくの対策への投資が無駄になってしまうことを意味します。セキュリティ対策を実施する際には、内部からの情報漏えい等を防ぐためであるか、それとも外部からの攻撃を防ぐためであるかをきちんと整理して実施することが重要です。

主に内部からの情報漏えい等を防ぐ対策としては、ISMS (Information Security Management System: 情報セキュリティ マネジメントシステム) など様々な基準があります。これら基準には外部からの攻撃に対しても盛り込まれている場合があります。しかし、攻撃は日々新しくなるものです。そのため、基準に則っていれば外部からの攻撃を必ず守れるものではありません。外部からの攻撃からシステムを守るためには、「何をどこから守る」のかを明確にした上でセキュリティ対策を実施してください。



ISMS: Information Security Management System: 情報セキュリティマネジメントシステム
FISMA: Federal Information Security Management Act: 連邦情報セキュリティマネジメント法
ISO15408: 情報技術セキュリティ評価基準
CC: Common Criteria

付図 3-1: 情報セキュリティの関連図

著作・制作 独立行政法人情報処理推進機構 (IPA)

執筆者 IPA「脅威と対策研究会」

執筆協力者(敬称略):

名前	所属	名前	所属
高倉弘喜	名古屋大学	小林克巳	NRI セキュアテクノロジーズ株式会社
岡谷貢	内閣官房 情報セキュリティセンター (5/16 時点)	谷川哲司	日本電気株式会社
佳山こうせつ	富士通株式会社	前田典彦	株式会社カスペルスキーラプスジャパン
藤原靖弘	富士通株式会社	石丸傑	株式会社カスペルスキーラプスジャパン
小出洋	九州工業大学	飯田朝洋	トレンドマイクロ株式会社
高橋正和	マイクロソフト株式会社	松川博英	トレンドマイクロ株式会社
徳田敏文	日本アイ・ピー・エム株式会社	宮本久仁男	株式会社 NTT データ
渡邊浩一郎	日本アイ・ピー・エム株式会社	行木健太郎	株式会社 日立ソリューションズ
守屋英一	日本アイ・ピー・エム株式会社	松浦裕司	株式会社 日立ソリューションズ
梨和久雄	日本アイ・ピー・エム株式会社	有村浩一	Telecom-ISAC Japan
小倉秀敏	日本アイ・ピー・エム株式会社	高橋竜平	Telecom-ISAC Japan
本川祐治	株式会社日立システムズ	則武智	Telecom-ISAC Japan
折田彰	株式会社日立システムズ	寺田真敏	株式会社日立製作所
丹京真一	株式会社日立システムズ	鵜飼裕司	株式会社フォティーンフォティ技術研究所
金岡晃	筑波大学大学院	金居良治	株式会社フォティーンフォティ技術研究所
加藤雅彦	株式会社インターネットイニシアティブ	村上純一	株式会社フォティーンフォティ技術研究所

[執筆取りまとめ] 小林偉昭 金野千里 相馬基邦 大森雅司 入澤康紀

「新しいタイプの攻撃」の対策に向けた設計・運用ガイド

[発行] 2011年 8月 第1版 第1刷

2011年 11月 第2版 第1刷

[著作・制作] 独立行政法人 情報処理推進機構 セキュリティセンター

[協力] IPA「脅威と対策研究会」

このページは空白ページです。

情報セキュリティに関する届出について

IPA セキュリティセンターでは、経済産業省の告示に基づき、コンピュータウイルス・不正アクセス・脆弱性関連情報に関する発見・被害の届出を受け付けています。

ウェブフォームやメールで届出ができます。詳しくは下記のサイトを御覧ください。

URL: <http://www.ipa.go.jp/security/todoke/>

コンピュータウイルス情報

コンピュータウイルスを発見、またはコンピュータウイルスに感染した場合に届け出てください。

不正アクセス情報

ネットワーク(インターネット、LAN、WAN、パソコン通信など)に接続されたコンピュータへの不正アクセスによる被害を受けた場合に届け出てください。

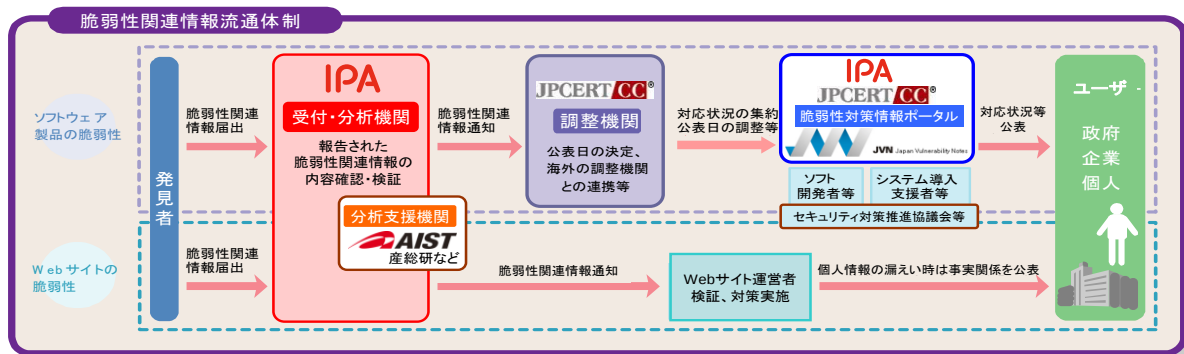
ソフトウェア製品脆弱性関連情報

OSやブラウザ等のクライアント上のソフトウェア、ウェブサーバ等のサーバ上のソフトウェア、プリンタやICカード等のソフトウェアを組み込んだハードウェア等に対する脆弱性を発見した場合に届け出てください。

ウェブアプリケーション脆弱性関連情報

インターネットのウェブサイトなどで、公衆に向けて提供するそのサイト固有のサービスを構成するシステムに対する脆弱性を発見した場合に届け出てください。

脆弱性関連情報流通の基本枠組み「情報セキュリティ早期警戒パートナーシップ」



※IPA: 独立行政法人 情報処理推進機構、JPCERT/CC: 一般社団法人 JPCERT コーディネーションセンター、産総研: 独立行政法人 産業技術総合研究所

IPA

独立行政法人 情報処理推進機構

〒113-6591

東京都文京区本駒込二丁目28番8号

文京グリーンコートセンターオフィス16階

<http://www.ipa.go.jp/>

セキュリティセンター

TEL: 03-5978-7527 FAX 03-5978-7518

<http://www.ipa.go.jp/security/>