JPCERT CC®

Japan Computer Emergency Response Team Coordination Center

高度サイバー攻撃への対処におけるログの活用と分析方法

1.0 版

一般社団法人 JPCERT コーディネーションセンター

2015 年 11 月 17 日

本書は、組織内のサーバやネットワーク機器などを管理しているシステム管理者向けに、高度サイバー攻撃の全体を見通すためのサイバーキルチェーンの区分と、それぞれの区分において、一般的に利用される機器を活用して、攻撃者の活動の痕跡をログとして残すための考え方、それらのログから痕跡を見つけ出す例をいくつか紹介し、高度サイバー攻撃への対策を検討される際の参考となるよう作成した。

目次

1. はじめに

組織を標的とした「高度サイバー攻撃」の被害が、我が国においても多くの組織で表面化しており、新しいセキュリティ脅威として、もはや対岸の火事では済まないものとなっている。高度サイバー攻撃は、標的型攻撃や APT (Advanced Persistent Threat) などとも呼ばれることがある、特定組織に対して明確な攻撃意図を持ち、組織内で情報窃取やシステム破壊などを行う、巧妙で執拗に計画された攻撃である。

高度サイバー攻撃は、従来型の攻撃に対する防御・検出だけでは完全に防ぐことができず、攻撃の全体像を正しく捉えることも難しいとされている。したがって、攻撃を受けて侵入されることも想定した上で、異常にいかに早く気づき対処できるかが成否の分かれ目となる。典型的な高度サイバー攻撃では、攻撃者が事前に対象組織について情報収集などを行い、対象組織に侵入するため継続的かつ執拗に攻撃を試みる。実際に 2015 年 5 月に独立行政法人 情報処理推進機構が公開した文書では、攻撃者が 31 か月にわたり国内の 9 組織に攻撃を行っていた例 (*1) が紹介されている。様々に試みた攻撃の中で一つでも成功したものがあれば、そこを拠点に組織内部に侵入する。侵入後は内部ネットワークなどの情報収集や攻撃用の環境を広げる活動を行い、最終的な目的を達成する。多くの高度サイバー攻撃では、攻撃者が侵入に成功した組織から長期間にわたり継続的に情報を持ち出そうとしていたと推測される。

JPCERT コーディネーションセンター (以下「JPCERT/CC」という。) では、高度サイバー攻撃の早期発見等を目標として様々な調査研究を行ってきた。その結果、高度サイバー攻撃であっても、複数の機器に、いくつかの特徴的な痕跡がログとして記録されており、適切にログを採取し分析することにより攻撃に気づき攻撃の全体像を捉えられる可能性があるとの心証を得ている。インシデント対応におけるログの重要性は多くの人が理解しており、ログの採取も多くの組織で行われている。しかし、運用の中で実際にログを分析調査している組織は稀であり、ログが広く活用されているとは言い難いのが実態であろう。また、インシデントが発生して専門家が調査に入っても、鍵を握るログが採取されていなかったために、十分な解明に到らなかった例も少なからずある。こうした状況の改善に向けた一助となるように、本書では、高度サイバー攻撃への備えと効果的な対処の観点から、典型的な組織用ネットワークを構成する各機器におけるログの採取と分析の方法について基本的な考え方をまとめている。本書の作成にあたっては、まず、セキュリティに対する意識が高く JPCERT/CC と信頼関係のある 6 組織のセキュリティ担当者の方々にヒアリングさせていただき、それをもとに、グッド・プラクティスや担当者として苦労しておられる課題を抽出した。その上で、被害組織に対する支援活動を通じて得た JPCERT/CC の知見を加味しつつ、できるだけ多くの組織で役立つように内容を整理して文書にまとめた。ヒアリングに際してご協力をいただいた組織の関係各位に対して、厚く御礼申し上げたい。

本書の構成は次のとおりである。まず、第 2 章では、高度サイバー攻撃を行う者が狙いを定めて公開情報を収集した後、組織内部への侵入を試み、そして最終的に目標を達成するまでの過程をモデル化し、典型的な組織用ネットワークにおいて、攻撃者の活動の痕跡が種々の機器にログとして記録される様子を説明する。続いて第 3 章では、メールサーバや Web プロキシサーバ、Firewall 等

の主な機器のそれぞれについて、取得すべきログの項目、ログを保存する上での注意事項などを説明する。第 4 章には、高度サイバー攻撃の痕跡を見つけるためのログの活用方法を例示する。また、その他の参考情報を付録に収録している。本書は、高度サイバー攻撃の検知と詳細調査が必要か否かを判断する初期調査までを対象とし、高度サイバー攻撃を受けたことが判明した後の詳細調査については対象外とした。最後に本書が、高度サイバー攻撃対策の参考となることを願う。

2. 高度サイバー攻撃の流れと攻撃者の活動の痕跡が記録される機器

高度サイバー攻撃では、攻撃者が様々な攻撃の手口を繰り出す。一連の高度サイバー攻撃の全体像を、いくつかの段階に区分してモデル化し、個々の攻撃の手口をその中に位置づけて考察すると、各段階での攻撃者の意図を理解でき、攻撃全体が見通しやすくなることが知られている。高度サイバー攻撃のモデルとしては、「準備 → 潜入 → 横断的侵害 → 活動」の 4 段階に区分するアプローチもあればさらに細分して、「偵察 → 武器化 → デリバリ →エクスプロイト→ インストール → Command & Control (以下「C&C」という。) → 目的の実行」の 7 段階に区分するロッキード・マーティン社のサイバーキルチェーンモデル (表 2-1) と呼ばれるものもある。いずれにしろ段階を 1 つ進むごとに攻撃は狙われた組織の深部に及ぶ。

表 2-1 サイバーキルチェーンモデル

	攻撃の段階	概要
1	偵察	インターネットなどから組織や人物を調査し、対象組織に関する情報を取得する
2	武器化	エクスプロイトやマルウエアを作成する
3	デリバリ	なりすましメール (マルウエアを添付) を送付する なりすましメール (マルウエア設置サイトに誘導) を送付し、ユーザにクリックするように誘導する
4	エクスプロイト	ユーザにマルウエア添付ファイルを実行させる ユーザをマルウエア設置サイトに誘導し、脆弱性を使用したエクスプロイトコードを実行させる
5	インストール	エクスプロイトの成功により、標的がマルウエアに感染する
6	C&C	マルウエアと C&C サーバを通信させて、感染 PC を遠隔操作する 新たなマルウエアやツールのダウンロード等により、感染拡大や内部情報の探索を試みる
7	目的の実行	探し出した内部情報を、加工 (圧縮や暗号化等) した後、情報を持ち出す

本書では、表 2-1 サイバーキルチェーンモデルに示した 7 つの段階を使って高度サイバー攻撃をモデル化し、各段階で攻撃者が残す痕跡をログとして記録できる機器を述べた上で、ログを活用して攻撃を検知する方法について解説する。次の節では、典型的な組織内ネットワークを構成する機器において記録されるログについて、サイバーキルチェーンモデルの各段階との関係を踏まえつつ説明する。

2.1. サイバーキルチェーンモデルとログ採取対象機器との関係

高度サイバー攻撃による被害を抑えるためには、自分の組織が攻撃を受けていることを、できるだけ早い段階で検知することが重要である。残念ながら高度サイバー攻撃に対抗できる万全の水際対策は無いため、組織内ネットワークまで侵入される可能性も見据えながら、正確かつ速やかに攻撃を把握し、迅速な対策を講じることが欠かせない。

ログの具体例や確認の際のポイントを解説するために、本書では、図 2-1 に挙げるような内部ネットワークと DMZ を有する、非常に単純な組織内ネットワークを仮定した。実際には、ここに挙げた以外のサーバや、IPS や IDS といったセキュリティ対策製品などが構成に加わる場合も多いだろう。本書の利用にあたっては、それらの機器を含めたデータの流れを考え、読み替えた上で、自組織に応用してもらいたい。

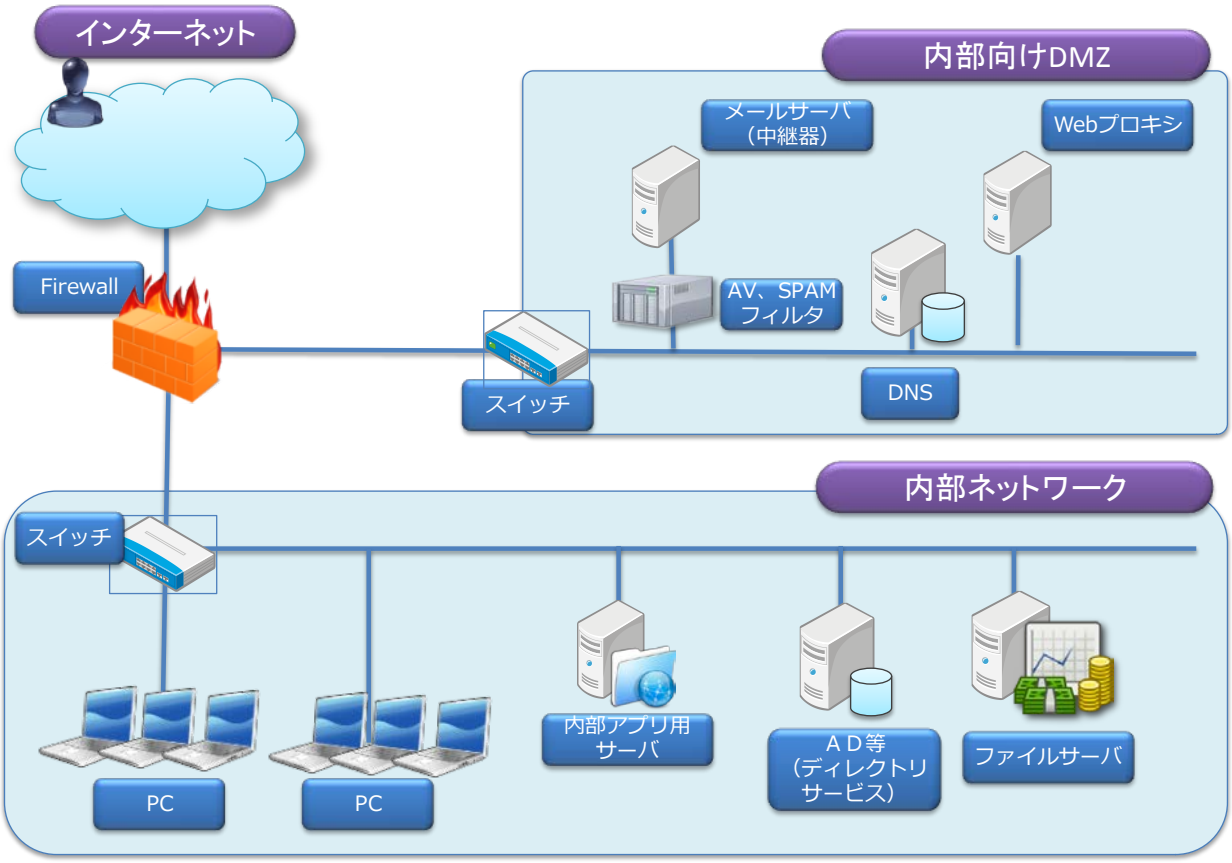

図 2-1 組織内ネットワーク構成のモデル

高度サイバー攻撃でも、表 2-1 に挙げた 1「偵察」や 2「武器化」の各段階は、攻撃者が狙った組織の外部で行う、いわゆる準備の段階であり、基本的には組織内の機器にログは記録されない。たとえ、ログが残されていたとしても、通常の通信と区別して攻撃の痕跡と判断するのは困難である。ログとして活動の痕跡が記録されるのは、組織の内部に拠点を作ろうとする 3「デリバリ」の段階から外部に機密情報を持ち出す 7「目的の実行」の段階までである。

サイバーキルチェーンの段階ごとに、典型的な攻撃の手口を表 2-2 に「A」から「H」として記載し、また、それぞれの手口の痕跡をログとして記録できる機器を書き添えた。

表 2-2 高度サイバー攻撃で使われる手口とログを記録できる機器の関係

攻撃段階		ログに記録可能な攻撃の手口		確認するログの機器
1	偵察	–	–	–
2	武器化	–	–	–
3	デリバリ	攻撃者によるマルウエア添付メールの送信	A	メールサーバ
		攻撃者によるマルウエア設置サイトへの誘導メールの送信と誘導	B	メールサーバ プロキシサーバ DNSサーバ
4	エクスプロイト	コールバック1（Webプロキシサーバを介さない外部への通信）	C	Firewall DNSサーバ
		コールバック1（HTTP, HTTPS等のプロトコルによる外部への通信）	D	プロキシサーバ DNSサーバ
5	インストール	–	–	
		–	–	
6	C&C	コールバック1（Webプロキシサーバを介さない外部への通信）	C	Firewall DNSサーバ
		コールバック1（HTTP, HTTPS等のプロトコルによる外部への通信）	D	プロキシサーバ DNSサーバ
		感染活動（脆弱なPCや内部サーバの探索など）	E	Firewall
		ファイルサーバなどへのアクセスや権限の奪取	F	AD
7	目的の実行	コールバック2（Webプロキシサーバを介さない外部への通信）	G	Firewall DNSサーバ
		コールバック2（HTTP, HTTPS等のプロトコルによる外部への通信）	H	プロキシサーバ DNSサーバ

デリバリの段階では、攻撃者が対象組織のメールアドレス宛にいわゆる標的型攻撃メールを送信することが多い。標的型攻撃メールは、送信元アドレスの詐称や事前に用意した踏み台 (取引先や関係組織に侵入し、その正規の環境を使用するなど) から送信されることが多いが、必ず組織内のメールサーバを経由する。このメールには、マルウエアが添付されていたり、本文中にマルウエア設置サイトへ誘導するリンクが含まれていたりする。

エクスプロイトの段階では、受信者に添付したマルウエアを開かせたり、マルウエア設置サイトに誘導し、ソフトウエア等の脆弱性を狙ったりする。エクスプロイトが成功すると、インストールの段階となり、PC がマルウエアに感染する。

その後の C&C の段階では、マルウエアは、攻撃者がインターネット上に用意した C&C サーバへのコールバックなどを発生させる。マルウエアは、C&C サーバを通じて攻撃者の指示を受けながら、組織内の別の PC への感染活動や、ファイルサーバへのアクセスなどを行い、最終的に、攻撃者の目的を遂行する。

デリバリから C&C の各段階では、リゾルバ (DNS) に名前解決の問合せや、Web プロキシサーバを中継するアクセスが発生し、内部ネットワークでの通信では、認証サーバへのアクセスなども発生して、ログに記録される。また、最終的に情報が外部へ持ち出される際にも、DNS や Web プロキシサーバなどを経由するため、ログに記録される。次の図 2-2 は、前述の典型的な攻撃の手口 (表 2-2) を図 2-1 に書き加えたものである (なお、このネットワーク構成において「A」から「H」

までのログが採取できない場合がある) 。

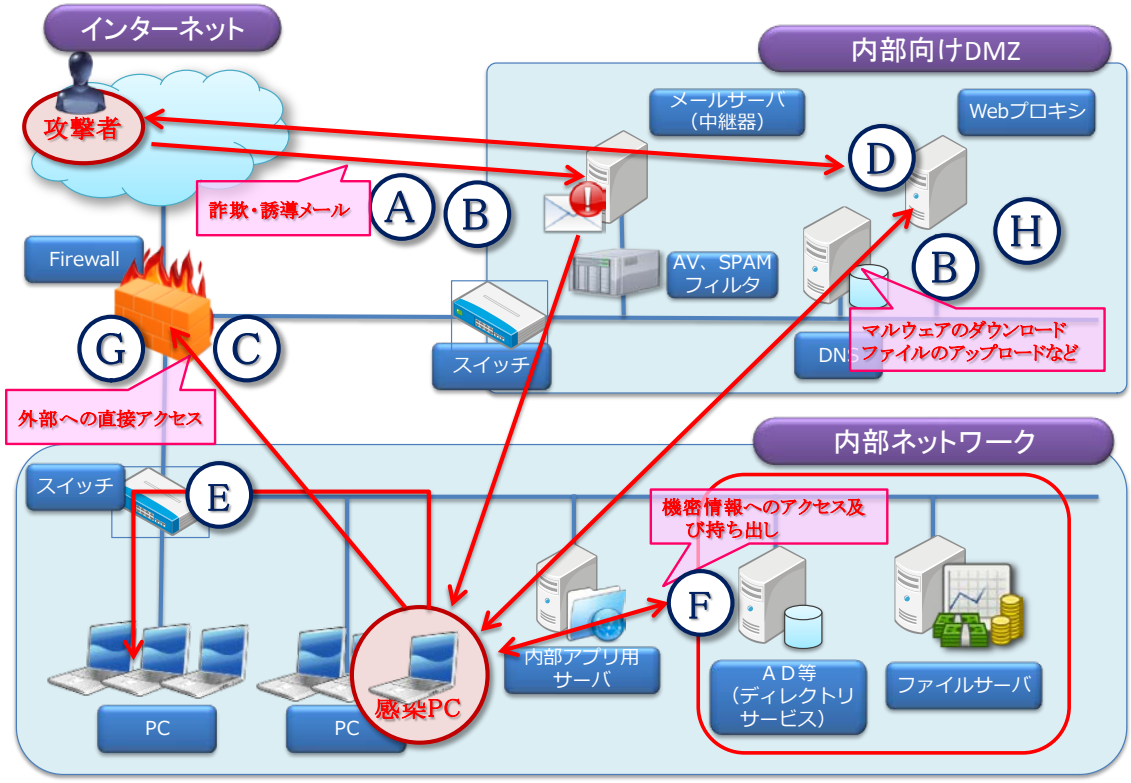

図 2-2 組織内ネットワークでの高度サイバー攻撃の流れ

表 2-3 に、攻撃の各段階でなされる典型的な不正行為の痕跡を、ログとして記録する可能性のある機器をまとめた。なお、本文書は、組織用ネットワークを構成する機器のログを対象としており、PC 内に記録される情報は対象外としている。

表 2-3 攻撃段階と取得対象機器の関係

高度サイバー攻撃の攻撃段階		メールサーバ	Firewall	プロキシサーバ	認証サーバ	DNSサーバ
1	偵察					
2	武器化					
3	デリバリ	A、B		B		B
4	エクスプロイト		C	D		C、D
5	インストール					
6	C&C		C、E	D	F	C、D
7	目的の実行		G	H		G、H

例えば、第 6 段階 (C&C) の活動が疑われる場合には、Firewall や、認証サーバ、Web プロキシサーバ、DNS サーバのログを調べるべきことを表 2-3 は示している。仮に第 6 段階の攻撃行為の痕跡が見つかれば、すでに第 3 段階から第 5 段階の攻撃行為が行われていると考えられるため、Firewall や、認証サーバ、Web プロキシサーバ、DNS サーバのログだけでなく、第 5 段階以前の攻撃行為の痕跡を調査するためメールサーバの機器のログも調査することが必要になる。すなわち、発見が遅

れて攻撃のステージが後段に進めば進むほど、攻撃者が意のままに操る機器やシステムが増える。結果として、攻撃の全体像を掌握するために調査すべき範囲が拡大することに注意が必要である。

なお、調査により攻撃の痕跡が見つかった場合には最悪の事態と影響の深刻度を勘案しつつ、速やかに専門業者へ依頼するなどして攻撃の全容を正確に掌握した上で対策を取ることが重要である。

コラム

高度サイバー攻撃への対策は入口対策だけでは不十分

従来のサイバー攻撃は、なりゆき任せの愉快犯や金銭を目的としたばら撒き型の攻撃がほとんどであった。ところが、高度サイバー攻撃では、情報窃取やシステム破壊など、明確な目的をもって特定の組織を狙う。

攻撃の手口は巧妙で、攻撃対象の組織や従業員に関する情報、組織内のシステム環境などを徹底的に調査し、周到な攻撃の準備をした上で、特別に用意した遠隔操作型のマルウエアを送り込み、C&C サーバを介して攻撃指示を出すことにより、組織内ネットワークの内側から長期間にわたり執拗に攻撃を続ける。このため、表 A に示したように、入口対策だけでは高度サイバー攻撃の被害を防ぐには不十分である。

表 A 入口対策と高度サイバー攻撃に対する効果

入口対策	高度サイバー攻撃に対する効果
ウイルス対策ソフト	標的とする組織が使っているウイルス対策製品を調査し、それが検知しないようにカスタマイズしたマルウエアを使うことが多いため、必ずしもすべてのマルウエアを検知できるわけではない。
Firewall	標的型攻撃メールは SMTP (25/ TCP) を、C&C サーバへの通信は通常の Web アクセスと同じ HTTP (80/TCP) や HTTPS (443/TCP) を使用しているので、通常の業務利用と見分けられない。
メール対策	不特定多数に送付される迷惑メールとは異なり、絞り込まれた従業員だけに宛てた業務を装った文面から、標的型攻撃メールと判断することは難しい。
Web フィルタリング	C&C サーバの URL は短期間で変化するものが多く、C&C サーバとの通信チャンネルとして Twitter や Facebook、Evernote 等のサービスを利用するマルウエアもあって、Web フィルタで C&C サーバとの通信を完全に阻止することが難しい
セキュリティ教育	手のこんだソーシャル・エンジニアリングは、IT 予防接種などで訓練を受けた利用者でも、見破ることが難しい

このように高度サイバー攻撃は、入口対策だけで完全に防ぐことは難しい。入口対策とともに、本書が提案するログ調査を通じて攻撃の兆候を早期に発見し迅速に対抗策を取ることが求められている。

3. ログの採取と取扱

本章では、ログを活用するために必要なログの採取と管理について考慮すべき事項と、各機器で採取できる、または採取すべきログ項目の概略を説明する。

3.1. ログの採取と取扱に関する一般原則

この節では、ログを採取し活用するために必要なログの保存と、ログの検索について、基本的な方法と注意すべき事項を述べる。組織内の情報システム・ネットワークの運用の一環として、ログの採取と管理のための手順を整理しておくことが肝要である。

3.1.1. ログの保存

採取したログは、何よりも適切に保存される必要がある。高度サイバー攻撃でなくとも、攻撃者がログファイルを削除、あるいは自身のアクセス記録を消すなどの事例がよく見られる。ログの保存管理においては、攻撃者のこういった妨害の可能性を忘れてはいけない。

ログを採取できる機器の中には、記憶容量の余裕がわずかで、十分な量のログを保存できないものもある。また、機器によっては、再起動するとログが消えてしまうものもある。ところが、高度サイバー攻撃の場合には、気がつかないまま、攻撃のステージが進んでしまっていることがしばしばあり、そのような場合にも攻撃の全体像を正しく分析するためには、ある程度長期間のログが保存されていなければならない。そのためには、各機器で採取したログを集約し、Syslog サーバなど長期保存に適したサーバに保存することが望ましい。SIEM (Security Information and Event Management) を導入していれば、製品によってはログの分析だけでなく、長期のログ保存機能を備えている場合もある。

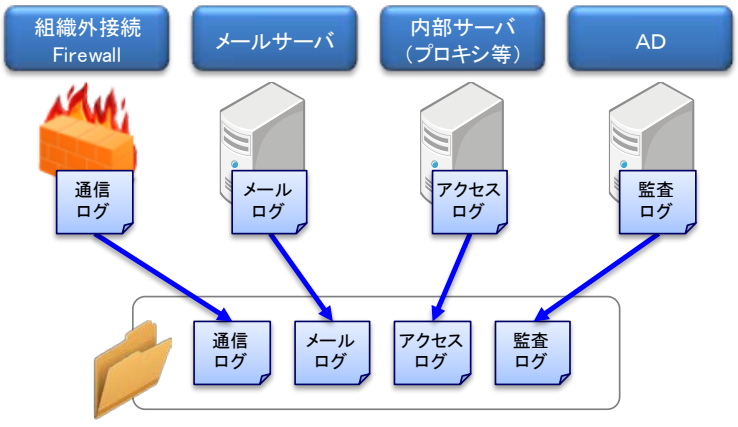

図 3-1 各機器のログの集約

Syslog サーバ等であっても、発生するログの量をあらかじめ見積っておき、運用中に記憶容量が不足しないよう計画する必要がある。記憶容量が不足すると、新規のログを保存できなくなる、または、古いログが消えてしまう可能性がある。

まず、ログの保存期間を適切に決めなければならない。決定にあたっては、表 2-2 に挙げた高度サイバー攻撃の流れを考慮すべきである。ログの保存期間が十分ではない場合は、攻撃の痕跡を一つ見つけたとしても、いつから攻撃を受けていたのか判断することが難しい。攻撃の痕跡の解析を専門業者に委託するとしても、どの程度情報が漏れたのか、進入経路はどこからか等の調査を行う上で、全容を探ることができるログが残っていると、攻撃の影響を把握する手掛かりとなる。

コラム

ログ保存期間に関する考え方

ログ保存期間は、次のように決めることが望ましい。

① ログを採取すべきシステムそれぞれのログの量を見積もる。
② 攻撃を受けていた場合には、どの程度まで過去に遡って調査する必要があるのかと、ログの長期保存に伴うコストとのトレードオフを考慮して保存期間を決定する。

JPCERT/CC では、インシデント対応支援や高度サイバー攻撃の調査等の結果から、ひとつの参考値として 1 年分のログを保存することを推奨している。しかしながら、長期間にわたる高度サイバー攻撃や、採取したログを統計的に調査して初めて検知できるマルウエアもあるため、ログを調査すべき期間は長引く傾向にある。次は、ログ保存期間について参考となる情報である。

- Mandiant 社の「APT1」のレポートによれば、標的型攻撃は平均で 1 年程度、最長では 4 年 10 ヶ月継続している。(*3)
- 内閣サイバーセキュリティセンター (NISC) は、平成 24 年にログ保存期間として 1 年以上を推奨している。 (*4)
- PCIDSS (Payment Card Industry Data Security Standard) では、即時にアクセスできるオンラインに保存で 3 か月間、オフライン保存で 1 年間を監査証跡の履歴保持に関する要件 (10.7) としている。 (*5)
- 独立行政法人情報処理推進機構 (IPA) は、標的型攻撃メールが 9 組織に対して 31 ヶ月間に渡り送られる攻撃を確認したと平成 27 年に報告している。 (*1)

ログ保存期間は 1 年以上にすることが望ましい。しかしながら、ログを長期間保存すると次の様な問題が生じる。

- 記憶媒体 (テープや光ディスクなど) が大量に必要となる
- 記憶媒体の用意と維持と管理に費用がかかる

ログの長期保存にかかる費用を抑えるために、直近 3 ヶ月のログをオンライン保存し、3 ヶ月を経過したらオフライン保存に変える方法がある。

- オンライン保存： (保存期間は 3 ヶ月程度)
  - ハードディスクなどオンラインの記憶媒体に保存する。必要な時に、すぐに調査できる。
- オフライン保存： (保存期間は残りの保存期間全て)
  - テープや光ディスクなどの記憶媒体に保存する。これらは耐久性があり大容量の保存に向いているが、調査に際してハードディスク等に展開しなければならない。

3.1.2. ログの検索

一般的に機器のログは、テキストファイルの形式で取り出すことができる。これをテキストエディタなどで開けば、基本的なログ調査が始められる。SIEM などの専用のシステムやソフトウエアを活用することで調査を効率化できる。テキストエディタでも、単純な文字列検索だけでなく、正規表現などを利用して、高度な検索を行うことのできるものもある。grep などの文字列検索コマンドを利用したログ調査で見通しを立てることも有益である。

ログ調査には、知識や技術が必要と考えられがちだが、専門家でなくても一定の手順に従って実施できる定型的な調査項目も少なからずある。そうした作業の方法を文書化しておくことで、緊急時に大量のログを、初心者を含むチームで手分けして解析することができる。そのためには、普段からログを調査する手順と体制を整備し、定期的に訓練しておくことが望ましい。

コラム

ログの時刻の重要性

ログ分析では、短単発的な事象の有無の確認だけでなく、事象が発生した時刻を確定し、複数の事象が発生したタイムラインを明らかにすることも重要である。例えば、PC の使用者が打合せや休暇などで、PC を全く操作していない時間帯に行われた、当該 PC からのアクセスは不審なものである可能性が高いと判断できる。

特に、複数機器で採取されたログを分析してタイムラインを作成する際には、各機器のタイマが正しく設定されていなければ、Web プロキシサーバ、DNS サーバ、Firewall など複数のログを付き合わせて、時間軸での攻撃の流れを正確に把握することが難しくなる。

機器のタイマは、わずかな誤差であっても累積することにより、同期を行わないとずれが生じる。正確なタイムラインを作成するため、正しい時刻でログが記録されることが望ましく、NTP を活用することが有効だ。NTP を利用する場合には、NTP サーバを適切に運用管理し、攻撃の踏み台とされないよう、アクセス制限など基本的なセキュリティ対策が必要である。

3.2. 主な機器で採取できるログ

図 2-1 に挙げたモデルネットワークに含まれる機器 (メールサーバ、Firewall、Web プロキシ、DNS サーバ、認証サーバ) のそれぞれについて、どのようなログが記録されるか説明する。機器によっては、デフォルトで設定されるログ以外の、より詳細なログを採取する設定や、ログの出力形式のカスタマイズが可能な場合もある。具体的な設定や出力の詳細は、各機器のマニュアルのログの設定と出力に関する事項を参照されたい。

3.2.1. メールサーバログについて

メール・システムが複数のメールサーバで構成されている場合には、カットセットを形成しているメールサーバを選んでログを採取する。メールサーバでは、受信メールと送信メールの双方のログを採取できる。受信メールのログでは、組織外からのなりすましメールや、実行ファイル添付メールを検知できる可能性があり、送信メールのログでは、疑わしい宛先に送信されたメールを検知できる可能性がある。 (図 3-2) 。

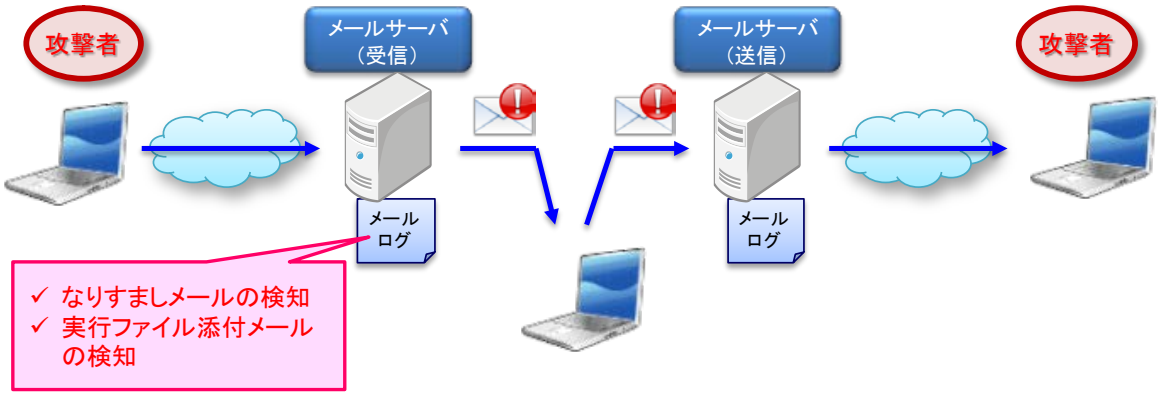

図 3-2 メールサーバに残る痕跡

表 3-1 に、本書で想定する検知方法において必要なログ項目を挙げる。

表 3-1 メールサーバログ項目

ログ項目	ログ項目の内容
From:	メールクライアントで表示される表記名、送信者アドレス、実際のメール送信者アドレス
Content-Type Content-Disposition	添付ファイル名

3.2.2. Firewall ログについて

Firewall は、ネットワークを内部と外部に隔てるために導入され、Firewall によって形成されたネットワーク境界の通過を許された、もしくは拒否した通信が Firewall のログに記録される。攻撃者が外部にいて、内部のシステムを遠隔から操作している場合には、そのための通信が Firewall を通過しており、その痕跡が Firewall のログとして記録されている可能性がある。

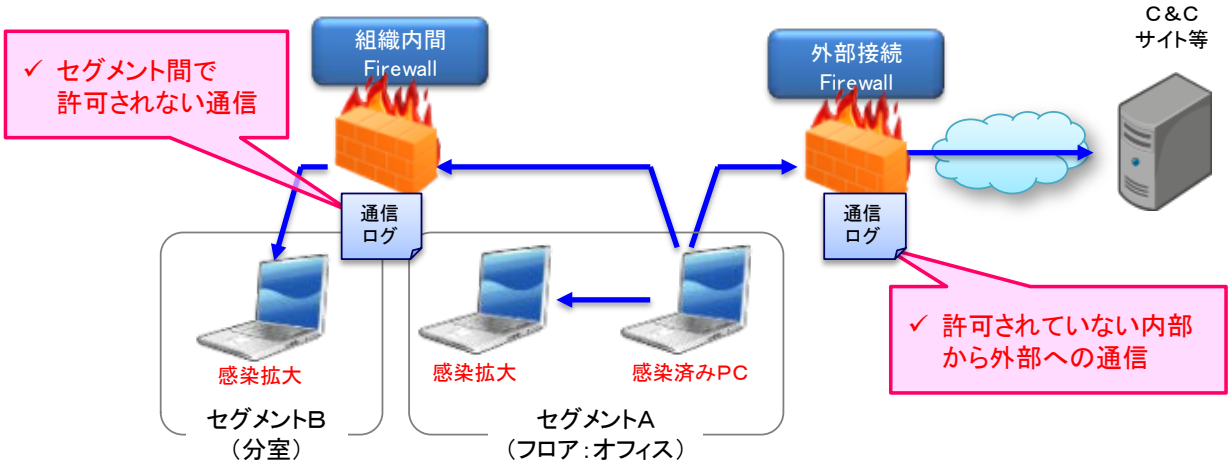

図 3-3 Firewall ログに残る痕跡

また、ネットワークの一部を他の部分から隔離してセキュリティを高めるために Firewall が利用される場合もある。例えば、重要なサーバ用ネットワークを従業員の PC を設置したネットワークから分離、あるいは、オフィスフロアや部署ごとにネットワークを分離するために Firewall を設置するのである。この場合には、マルウエアに感染した PC が、認証サーバや他の PC などにアクセスした痕跡をログ中に発見できる可能性がある。

表 3-2 に、本書で想定する検知方法において必要なログ項目を挙げる。Firewall のログは多量になるため、機器内に保存するのではなく、機器外の Syslog サーバや SIEM などに、ログを保存することが望ましい。

表 3-2 Firewall ログ項目

ログ項目	ログ項目の内容
Action	Firewall ポリシーのアクション
dst zone	送信先のゾーン設定
Src	送信元アドレス
src_port	送信元ポート
Dst	送信先アドレス

dst_port	送信先ポート

3.2.3. Web プロキシサーバログについて

Web プロキシサーバは、組織内からインターネット上の Web サイト等へアクセスするためのパケットが通過するため、そのアクセス記録をログとして採取することができる。

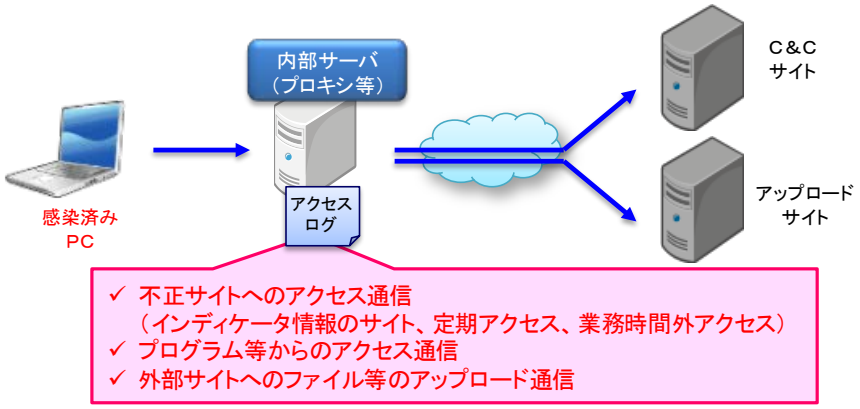

図 3-4 Web プロキシサーバに残る痕跡

Web プロキシサーバでは、PC からの Web サイトを閲覧するためのリクエストを全て記録することができる。HTTP や、HTTPS、FTP などの通信プロトコルを用いて C&C サーバと通信するマルウエアの活動の一端なども記録できる可能性がある。特に、マルウエアと C&C サーバとの通信については、Firewall のログよりも Web プロキシサーバのログの方が、より多くの情報を得られる可能性がある。

表 3-3 に、本書で想定する検知方法において必要なログ項目を挙げる。Web プロキシサーバに残されるログには、マルウエアに関する通信だけでなく、正規の通信も含まれており、さらに、利用者が強く意識していない、ソフトウエアやプラグイン等のアップデートの際の通信も含まれる。Web プロキシサーバのログの調査では、正規の通信か否かを判断できるよう、使われている端末の OS やブラウザを調べて把握しておくことが望ましい。

表 3-3 Web プロキシサーバログ項目

ログ項目	ログ項目の内容
URL	URL アドレス、送信先サイトのポート
method	メソッド
UserAgent	UserAgent
accesstime	アクセス時間

マルウエアに感染した PC は、利用者のいない時間帯でも、組織外との通信を行う場合がある。

休日や深夜にも関わらず頻繁に通信している、あるいは、特定のサイトに異常な量の通信が集中しているなど、通信の統計的な変位からもマルウエア感染の可能性を見つけ出せる場合もある。

3.2.4. DNS サーバログについて

DNS サーバでは、ホスト名の解決を行ったクエリ記録をログとして採取することができる。通常 DNS サーバは、権威サーバとキャッシュサーバの 2 つの役割があるが、痕跡の分析を行う場合は、組織内の PC やサーバからの要求に対して応答を行う、組織内部向けのキャッシュサーバのログを活用する。キャッシュサーバのログには、マルウエアに感染した PC が、C&C サーバと通信する際の、ホスト名の解決を行ったクエリ記録が残る可能性がある。組織によっては、DNS サーバを複数稼働させたり、用途によりサーバや設定を分けたりすることもあるため、その構成の場合は、キャッシュサーバの役割を持つ DNS サーバのログを採取することが望ましい。

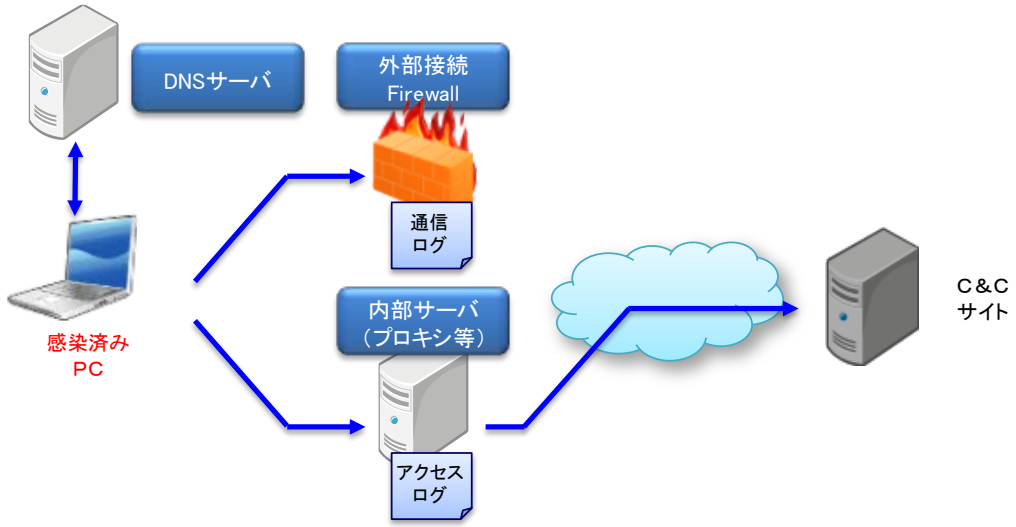

図 3-5 DNS サーバに残る痕跡

表 3-4 に、本書で想定する検知方法において必要なログ項目を挙げる。

表 3-4 キャッシュ DNS サーバログ項目

ログ項目	ログ項目の内容
clinet	名前解決を行おうとしている PC 等の IP アドレス
query	要求および応答したホストや IP アドレスの情報

3.2.5. 認証サーバログについて

組織内の認証や権限の付与を集中管理する認証サーバが設置されることもある。認証サーバは、Active Directory や LDAP、RADIUS などが用いられ、利用者が誰であるかを識別し、ユーザやコンピュータの権利と権限などを一元管理する。組織内のユーザが、ネットワークコンピュータにログオンする際やサーバの利用権の確認などが行われる際に、ログとして記録される。ここでは、認証サーバとして用いられることが多い Active Directory を例にとって説明する。

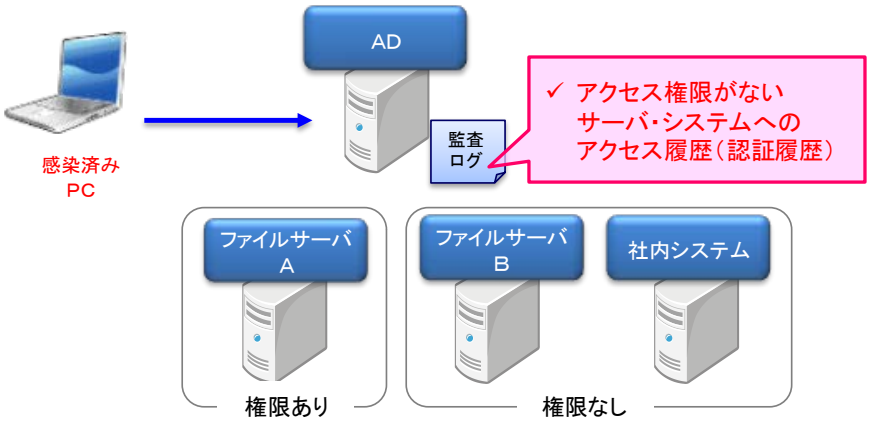

図 3-6 認証サーバに残る痕跡

マルウエアの中には、認証サーバや他のサーバにアクセスし、認証や権限昇格を行うものがある。マルウエアからのアクセスを含むユーザ認証のログや監査ログが認証サーバで記録される。ただし、そのログは、Windows イベントログとして記録されるため、他の機器やサーバのように検索を行うことはできない。そのため、Windows のイベントビューアーより、テキスト形式や、CSV ファイル形式のファイルに保存した上で検索を行う。また、Windows は、ログをエクスポートするためのインターフェースが他の機器とは異なるため、Syslog サーバなどでログを収集して保存する場合には、専用のソフトウエアの使用など工夫が必要となる。

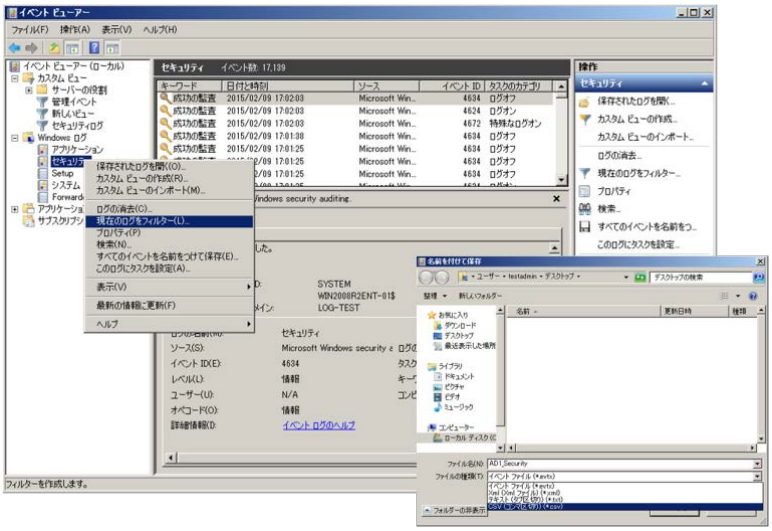

図 3-7 イベントログのエクスポート

4. 高度サイバー攻撃の痕跡を見つけるためのログの分析方法

第 2 章で、高度サイバー攻撃が段階的に進行する過程と、その中で攻撃の痕跡がログとして機器に記録される様子をモデル化して説明し、第 3 章では、ログの採取と管理について考慮すべき事項と、各機器で採取できる、または採取すべきログ項目の概略を説明した。本章では、高度サイバー攻撃にできるだけ早期に気付けるよう、ログを分析して攻撃の痕跡を見つけ出す方法を述べる。4.1 節では、異常な事象が無くとも定期的に行うべき、いわばプロアクティブなログ分析の基本について最初に述べ、その後で、異常事象の報告を受けた時に行うべき、いわばリアクティブなログ分析の基本について述べる。4.2 節では、攻撃の痕跡を発見するために鍵となるログが記録される機器について、機器毎にログの分析方法を述べる。4.3 節では、DNS サーバと認証サーバのログ分析について紹介する。これらには、膨大な量のログが記録されるため、4.2 節で述べるログ分析から得られる手掛かりなどを用いて、調査すべき範囲の絞り込みを行うのが望ましい。

4.1. 攻撃の痕跡を見つけるためのログ分析概論

攻撃の痕跡を発見するためのログの分析には、次の 2 つの文脈が考えられる。一つは、つね日ごろから異常な現象が起きていないことを確認するために定期的に行うログ分析であり、もう一つは、異常な事象について報告を受け、詳細を確認するために行うログ分析である。本節では、4.1.1.で前者について、4.1.2.で後者について、それぞれの基本的な進め方を述べる。なお、個々の機器に依存するログの分析方法の詳細については、括弧内に示した節を参照されたい。

4.1.1. 定期的に行うログ分析

定期的に行うログ分析では、各機器が普段どのようなログを出力するかを予め把握しておき、それと違うログが出力されていないかに目を凝らす。定期的に行うログ分析において、攻撃の痕跡を探し出すための着眼点を次に挙げる。

(1) Firewall で採取された通信ログ (成功・失敗) について、通信の発生時刻や、通信プロトコル、通信元、通信先は妥当か (参考：4.2.2.1 組織内から組織外への拒否通信を手掛かりとしたログ分析、4.2.2.2 異なるセグメントに収容された PC 間の不正な通信を手掛かりとしたログ分析)。

(2) Web プロキシサーバで採取されたログの中に、次のような通信を示唆するものがないか。

- 定期的な通信 (参考：4.2.3.4 定期的に発生する HTTP 通信を抽出するログ分析)
- 就業時間帯以外の時刻 (出勤前、帰宅後、打合せ中、外出中など) の外部への通信 (参考：4.2.3.5. 業務時間外に発生する HTTP 通信を抽出するログ分析)
- 外部に異常に大量のデータを送出する通信 (参考：4.2.3.6. 大量の HTTP 通信を抽出するログ分析)

4.1.2. 異常事象の報告に対応して行うログ分析

報告された異常事象により、確認すべきログやログ分析の方法が異なる。報告されることの多い異常事象ごとに基本的な考え方を述べる。

(1) 高度サイバー攻撃のデリバリ段階のメールの受信が疑われる事象が報告された場合

業務に関わる内容を模した偽のメールや、差出人として関係組織や取引組織をかたったメールは、高度サイバー攻撃におけるデリバリ段階のメールである可能性がある。そうしたメールを受け取ったとの報告を受けた場合、次のようなログ分析をしておくべきである。

- メールサーバのログを分析し、疑わしいと報告されたメールと同じ送信元や、添付ファイル名をもつメールの受信記録が他にないかを調べる (参考：4.2.1.2.実行ファイルが添付されたメールを手掛かりとしたログ分析)。

見つかった場合には、メールサーバのログを使って配送先を調べて、配送先のユーザが添付ファイルを開くなどしてマルウエア感染が起きていないかを確認しておくべきである。

(2) 組織内で遠隔操作型のマルウエア感染が疑われる場合

C&C サーバと通信する遠隔操作型のマルウエアに関する情報を受け取った場合には、次のようなログの調査を行っておくことが望ましい。

- C&C サーバの URL が分かっていれば、Web プロキシサーバのログを分析する (参考：4.2.3.1.不審な送信先への通信)

- C&C サーバの IP アドレスだけしか分かっていなければ、Web プロキシサーバのログに加えて、Firewall の内部から外部に対するログなどを分析する (参考：4.2.2.1. 組織内から組織外への拒否通信を手掛かりとしたログ分析) 。

これらの分析により、当該マルウエアの活動の有無を確認できる。また、この調査で、組織内の PC が C&C サーバにアクセスした痕跡が見つかった場合には、当該 PC 関して次の調査を行うべきである。

- 当該 PC から、組織外あるいは組織内の許可されていないセグメントなどへの不審なアクセスが無いかを Firewall のログを分析する (参考：4.2.2.1.組織内から組織外への拒否通信を手掛かりとしたログ分析、4.2.2.2. 異なるセグメントに収容された PC 間の不正な通信を手掛かりとしたログ分析)

- 組織内で利用しないブラウザなどの UserAgent や CONNECT メソッドを使ったアクセスをしていないかを Web プロキシサーバのログを分析する (参考：4.2.3.2.CONNECT メソッドで 80、443 以外ポートへの通信を抽出するログ分析、4.2.3.3. 標準利用以外の User

Agent によるアクセスを抽出するログ分析)

- アカウント認証の失敗が無いか、普段と異なるアカウントの利用が無いかを認証サーバのログを分析する (参考：4.3.2. 認証サーバ)

(3) 機密情報の組織外への持出しが疑われる場合

機密情報が組織外に持ち出された可能性が強く疑われる場合には、すでに高度サイバー攻撃が最終段階に至っていることも想定しつつ、少なくとも次のような分析をすべきである。

- 組織外に向けた著しく大量のデータの送信が行われていないか Web プロキシサーバのログを分析する (参考：4.2.3.6. 大量の HTTP 通信を抽出するログ分析)

インターネット上のオンライン・ストレージサービスや無料メールの利用を禁止するルールを設けている組織にあっては、そのルールが守られているかどうかを、ログを分析して確認しておくとよい。

コラム

システム管理者が攻撃の痕跡を見つけた時の留意点

高度サイバー攻撃の痕跡を発見した場合には、さらなる情報漏洩や、攻撃段階の進展をくい止めることが重要である。一方で、そうした対策をシステム管理者が取ったために、その後の専門業者による調査が難しくなってしまうこともある。システム管理者は、調査・対応にあたって、安易に表 B に示した行為をしないよう留意すべきである。

表 B システム管理者が留意すべき“Do Not”

	システム管理者が してはならない行為	行為による影響／行為を避ける理由
1	マルウエアを含むと疑われる不審なファイルを、聞きかじりの知識や我流で削除する	複数のファイルを使用し動作するマルウエアの場合、一部のファイルが削除されると情報が断片的となって、マルウエアの機能を特定できなくなるなど、専門家による調査が困難になる
2	手当たり次第に PC やサードパーティ製品などの設定（ログインパスワードを含む）を変更する	設定の変更がマルウエアによるものかどうかを判断できなくなり、専門家による調査が困難になる
3	感染が疑われる PC の調査のために、新たなセキュリティ対策製品（当初からインストールされていたものと異なるウイルス対策ソフトやツールなど）をインストールし実行する	マルウエアの痕跡が失われ、専門家による調査が困難になる

マルウエアの感染が疑われる PC は、被害の拡大を防止するために、直ちにネットワークから切り離すよう推奨されている。しかし、ネットワークから切断されると動かなくなるマルウエアもあり、PC をシャットダウンすれば、メモリ上に存在していたマルウエアやマルウエアが作り出したデータなどが消失する可能性もある。専門家に調査を依頼する場合は、感染が疑われる PC の取扱（PC のネットワークからの切り離しや、シャットダウンなど）についても意見を求めた方がよい。

4.2. ログに残る攻撃の痕跡を見つけるための考え方

本節では、機器ごとにログを分析するための方法について説明する。各機器における、(a) 採取すべきログ項目と設定方法、(b) 攻撃の痕跡の見つけ方、(c) 検知例、(d) 注意点を述べる。攻撃の手口は様々であり、記録されるログも一様ではないため、本書の解説は、基本的な考え方を学ぶための参考事例として読んでいただき、実践においては、個々の状況や機器に応じた対応を心がけていただきたい。

4.2.1. メールサーバのログ分析

攻撃者の活動を示す痕跡のうち、メールサーバで検知できる主なものを表 4-1 に示す。

表 4-1 攻撃の痕跡をメールサーバログから見つけ出す手掛かり

	攻撃行為	*注*	攻撃の痕跡を見つける手掛かり
From フィールドの表示名偽装	送信元を偽装したメールを送り付けて、その添付ファイルを開かせる、またはメッセージ中の URL をクリックさせる	A、B	受信メールにおける送信者情報の不自然な設定
実行ファイル添付	マルウエアである実行ファイルを添付したメールを送り付ける	A	実行ファイル形式が添付されたメール

注：表 2-2 および図 2-2 における攻撃活動の表示に対応

本節では、組織内のメールサーバとして利用されることの多い「postfix」を前提として説明する。他のメールサーバを使っている場合には、マニュアルを参照するなどして適宜読み替えて欲しい。

4.2.1.1. From フィールドの表示名偽装を手掛かりとしたログ分析

メールに含まれる送信者情報には、エンベロープの MAIL From とメールヘッダの From の 2 種類がある。このうちメールヘッダの From には、送信者メールアドレスとは別に自由に文字を入力できる display name というフィールドを追加できる (以下、「From フィールドの表示名」という)。図 4-1 の例では、sample@example.co.jp が From フィールドの表示名であり、attack@example.com が送信者メールアドレスである。From フィールドの表示名が存在する場合には、それだけを表示し送信者メールアドレスは表示しないメールソフトもあるため、攻撃者は、怪しまれないよう From フィールドの表示名に関係組織や取引組織のメールアドレスを設定して攻撃メールを送り、添付ファイルを開かせる、またはメールのメッセージ中の URL をクリックさせて、受信者が使用している PC のマルウエア感染を狙う。

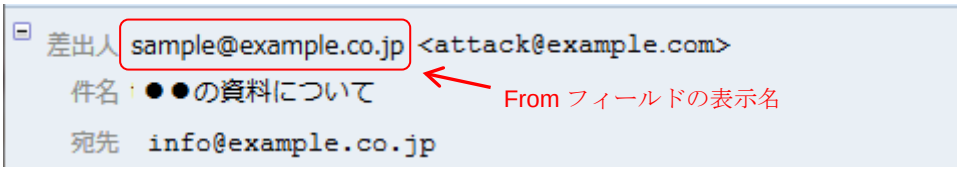

図 4-1 From フィールドの表示名

この節では、メールヘッダの From フィールドの表示名にメールアドレスが含まれており、かつ送信者メールアドレスが異なるものを見つける方法を示す。

(a) 採取すべきログ項目と設定方法

Postfix の標準設定では、メールヘッダの From フィールドの情報はログに出力されない。分析に必要なログを採取するためには、次の設定が必要である。

表 4-2 postfix のログの設定例

File: /etc/postfix/main.cf のファイルに次の内容を追記
header_checks = regexp:/etc/postfix/header_checks
File: /etc/postfix/header_checks のファイルに次の内容を追記
/^From:/ WARN

上述の設定により、攻撃の痕跡を見つけるために必要な表 4-3 に示すようなログ項目が採取される。

表 4-3 検知に必要なログ項目

ログ項目	ログ項目の内容
From:	メールヘッダの From に含まれる情報

(b) 攻撃の痕跡の見つけ方

攻撃の痕跡を見つける方法は次のとおりである。

① メールサーバのログから メールヘッダの "From:" が含まれる行を抽出する
② From フィールドの表示名に含まれているメールアドレス形式の文字列を抽出する
③ From フィールドの表示名のメールアドレスと送信者のメールアドレスを分離して、文字列を比較し、異なる場合には攻撃の痕跡である可能性ありと判定する

(c) 検知例

攻撃の痕跡として抽出されたログの例を図 4-2 に示す。

```
Feb 16 11:43:32 mail-server postfix/cleanup[29597]: B1467845E2:
warning: header From: "sample@example.co.jp" <attack@example.com> from
unknown[192.168.xxx.xxx]; from=<root@example.com>
to=<info@example.co.jp> proto=ESMTP helo=<[127.0.0.1]>
```

図 4-2 Postfix のログの例

このログの例には、表 4-4 のような内容が含まれている。

表 4-4 ログ分析の結果

メール項目	メールサーバのログの内容
From フィールドの表示名	"sample@example.co.jp"
メールヘッダの 送信者メールアドレス ※ソフトによっては非表示	attacker@example.com
MAIL From のメールアドレス	root@example.com

攻撃の痕跡が見つかった場合は、デリバリの段階が疑われるので、偽装された From フィールドの表示名が取引先や関係組織などのメールアドレスであれば、メールサーバのログからメールの宛先と配送時間の情報とともに、対象メールの扱い (不審な添付ファイルを開いたり、メッセージ内のリンクをクリックしたりしていないかなど) についてメール受信者に確認することが必要であると考えられる。

(d) 注意点

- 攻撃の痕跡である可能性ありと判定されるメールには、メーリングリストやメールマガジン等で代行業者が本来の送信者に変わって送るメールや、SPAM、迷惑メールなどが含まれている可能性がある。そのため見つかったメールが本当に攻撃の痕跡かどうかは、吟味が必要である。

4.2.1.2. 実行ファイルが添付されたメールを手掛かりとしたログ分析

攻撃者は、マルウエアである実行形式のファイルを添付した標的型攻撃メールを送り、受信者にそのファイルを実行させることで PC をマルウエアに感染させて、組織内部に攻撃の起点を作ることを狙う。この節では、拡張子が実行形式 (例として.exe としている) のファイルが添付されたメールを見つけ出す方法を示す。

(a) 採取すべきログ項目と設定方法

Postfix の標準設定では、添付ファイルに関する情報がログに出力されない。分析に必要なログを採取するためには、次の設定が必要である。

表 4-5 postfix のログ設定例

File: /etc/postfix/main.cf のファイルに次の内容を追記
`mime_header_checks = regexp:/etc/postfix/mime_header_checks`
File: /etc/postfix/mime_header_checks のファイルに次の内容を追記
`/^¥s*Content-(Disposition|Type).*name¥s*=¥s*"?(.+)"?¥s*$/ WARN`

上述のような設定により、攻撃の痕跡を見つけるために必要な表 4-6 のようなログが採取できる。

表 4-6 検知に必要なログ項目

ログ項目	ログ項目の内容
Content-Type **Content- Disposition**	添付ファイル名

(b) 攻撃の痕跡の見つけ方

痕跡を見つる方法は次のとおりである。

① メールサーバのログから "Content-Type"、 "name" が含まれる行のログを抽出する
② 添付ファイル名が含まれている箇所 (name= の後のダブルクォートで括られた部分) を抽出する
③ 添付ファイル名に実行形式の拡張子が含まれていれば攻撃の痕跡の可能性があると判定する

(c) 検知例

攻撃の痕跡である可能性ありと判定されたログの例を図 4-3 に示す。

```
Feb 16 16:17:26 mail-server postfix/cleanup[6952]: 08C08845EF: warning:
header Content-Type:
application/vnd.openxmlformats-officedocument.wordprocessingml.docume
nt;? name="=?Shift_JIS?B? gXmDfYOLlOmBeozai3GP7pXxgUkuZXhl=?=" from
unknown[192.168.xxx.xxx]; from=<attacker@example.com>
to=<sample@example.co.jp> proto=ESMTP helo=<[127.0.0.1]>
```

図 4-3 Postfix のログの例

図 4-3 のログから添付ファイルの名前を取出し、Base64 エンコードされた文字列をデコードすることで、表 4-7 のような「【マル秘】顧客情報！.exe」の実行形式のファイル名を見つけることができる。

表 4-7 ログ分析の結果

メール項目	メールサーバのログの内容
添付ファイル名	"=?Shift_JIS?B? gXmDfYOLlOmBeozai3GP7pXxgUkuZXhl?="
添付ファイル名 ※ Base64 デコード済み	【マル秘】顧客情報！.exe
添付ファイルの拡張子	.exe

デリバリの段階の攻撃の痕跡であることが疑われるが、攻撃の成否は、ログ分析だけからは判断できない。ログからメールの配送先と配送時間の情報を特定し、受信したメールの添付ファイルの扱い (開いたかどうか) について受信者にヒアリングする必要がある。また、同じ送信元メールアドレスから別の宛先に送信されたメールや、このメールアドレスに対して、内部から送信されたメールが無いことも念のため確認しておくとよい。

(d) 注意点

- メールヘッダの中では、ファイル名にマルチバイトの文字コード (日本語等) を使う場合、Base64 等を利用しエンコード処理することになっている。そのためデコード処理が必要な場合がある
- 正規のメールにも、自己解凍形式の圧縮ファイルなどで拡張子が .exe であるファイルを添付されているものがあるので、攻撃の痕跡と断定する前に、ユーザに確認する等の必要がある
- 昨今では、メールサーバやウイルス対策ソフトなどによって、実行形式のファイルが添付されたメールは自動的にブロックされる場合が増えているため、この種の攻撃手法は少なくなりつつある

- 高度サイバー攻撃では、実行ファイルを圧縮した上でメールに添付するケースもある。その場合にも、この分析法を応用すれば、実行ファイル以外 (rar や zip などの圧縮ファイル)の拡張子を確認することができる

4.2.2. Firewall のログに残る痕跡の見つけ方

攻撃者の活動のうち、Firewall で検知できる主なものをいくつかに示す。

表 4-8 攻撃の痕跡を Firewall のログから見つけ出す手掛かり

	攻撃行為	*注*	攻撃の痕跡を見つける手掛かり
組織内から組織外への不正な通信	Web プロキシサーバを経由せずに、ボットに感染した PC が C&C サーバに、または、ダウンローダに感染した PC がマルウエア設置サイトに、通信を試みる	C	Web プロキシサーバを経由せずに、直接インターネットへの通信を試みる組織内の PC 等を、Firewall の通信ログから検知する
異なるセグメントに収容された PC 間の不正な通信	マルウエアに感染した PC が、他の PC 等に対して感染を広げるための通信を行う	E、F	セグメント間で許可されていない通信を、Firewall の通信ログから検知する

注：表 2-2 および図 2-2 における攻撃活動の表示に対応

本節では、組織網の構築に際して Firewall として利用されることの多い「Juniper SSG」を前提として説明する。他の Firewall を使っている場合には、マニュアルを参照するなどして適宜読み替えて欲しい。

4.2.2.1. 組織内から組織外への拒否通信を手掛かりとしたログ分析

マルウエアに感染した PC は、指令を受け取るために C&C サーバへ通信を試みたり、マルウエア設置サイトから新たなマルウエアのダウンロードを試みたりする。この節では、高度サイバー攻撃の痕跡を見つけ出すため、マルウエアに感染した PC から行う、Web プロキシサーバを経由しない組織外への通信をログから抽出する方法を述べる。

(a) 採取すべきログ項目と設定方法

攻撃の痕跡を見つけるために必要なログ項目を表 4-9 に示す。

表 4-9 検知に必要なログ項目

ログ項目	ログ項目の内容
Action	Firewall ポリシーのアクション
dst zone	送信先のゾーン設定 ※製品依存があるため定義が必要な場合がある
Src	送信元アドレス
Dst	送信先アドレス
dst_port	送信先ポート

(b) 攻撃の痕跡の見つけ方

痕跡の見つけ方は次のとおりである。

① Firewall ログから送信元アドレスが組織内で送信先アドレスが組織外への通信を抽出する
② 業務で通信が必要となる機器 (Web プロキシサーバやメールサーバ) などから組織外への通信は除外 (通信を許可) する
③ 通信拒否 (action が Deny または Reject) を攻撃の痕跡の可能性があると判定する

(c) 検知例

攻撃の痕跡である疑いがあるとして抽出されたログの例を図 4-4 に示す。

```
2014-12-16T01:02:01.258399+09:00 192.168.xxx.xxx ns208-master:
NetScreen device_id=ns208-master
[Root]system-notification-00257(traffic): start_time="2014-12-16
00:11:15" duration=0 policy_id=36 service=http proto=6 src
zone=SHANAI dst zone=Untrust action=Deny sent=0 rcvd=0
src=192.168.100.xxx dst=23.23.xxx.xxx src_port=58461 dst_port=80
session_id=0
```

図 4-4 Juniper SSG の検知例

図 4-4 のログからは、表 4-10 が示すように、192.168.100.xxx の IP アドレスが割り当てられた PC から、IP アドレスが 23.23.xxx.xxx の 80 番ポートにアクセスしようとしていたことが分かる。

表 4-10 ログ分析の結果

通信ログ項目	通信ログの内容
Firewall ポリシー アクションステータス	Deny
送信先ゾーン ※製品依存の項目	Untrust
送信元アドレス	192.168.100.xxx
送信先アドレス	23.23.xxx.xxx
送信先ポート	80

この種の攻撃の痕跡が見つかった場合は、少なくとも高度サイバー攻撃における「インストール」の段階まで進んでいることが疑われる。当該 PC がマルウエアに感染していないか、該当 PC が定常的に通信している他の送信先がないかなどを調査する必要がある。送信元アドレスから同一の送信先アドレスに継続して通信してないか、送信元アドレスを起点に他のログの分析方法で不審な通信をしていないかなどの確認が必要である。

(d) 注意点

- ここで述べた方法が機能するためには、Firewall のポリシーやゾーンの定義が、必要最小限の通信を通過させるよう正しく設定されていること、インターネットへの通信が Web プロキシサーバ経由に制限されていることが前提である
- Web プロキシサーバ無しで構築されている組織内ネットワークでは、この手法では攻撃を検知できないし、Web プロキシサーバに対応したマルウエアに感染していた場合にも検知ができない
- マルウエアは、通信先ポートとして 25 (SMTP)、80 (HTTP)、443 (HTTPS)、8080 (Proxy) を使用することが多いため、これらのポートを中心に調査するとよい

4.2.2.2. 異なるセグメントに収容された PC 間の不正な通信を手掛かりとしたログ分析

マルウエアに感染した PC が、他の脆弱な PC や組織内のサーバに対して、感染させるための活動や、認証情報の詐取を試みる事例がしばしば見られる。その際の通信は、正規の利用とは異なった端点間で試みられることも多く、ログを分析することにより見つけ出せる可能性がある。組織内ネットワークに Firewall などが組み込まれていて、必要最小限の通信だけを許可する設定になっている場合には、発見はさらに容易である。

この節では、マルウエアに感染した PC から組織内の別の脆弱な PC や組織内部のサーバに対する許可していない通信をログ分析により見つけ出す方法を示す。

(a) 採取すべきログ項目と設定方法

攻撃の痕跡を見つけるために必要なログ項目を表 4-11 に示す。

表 4-11 検知に必要なログ項目

ログ項目	ログ項目の内容
Action	Firewall ポリシーのアクション
dst zone	送信先のゾーン設定 ※製品依存があるため定義が必要な場合がある
Src	送信元アドレス
Dst	送信先アドレス
dst_port	送信先ポート

(b) 攻撃の痕跡の見つけ方

攻撃の痕跡の見つけ方は次のとおりである。

① Firewall のログから送信元アドレスが組織内で送信先アドレスが組織内への通信を抽出する
② 拒否された通信 (action が Deny または Reject) を攻撃の痕跡の可能性があると判定する

(c) 検知例

攻撃の痕跡として抽出されたログの例を図 4-5 に示す。

```
2014-12-16T01:01:55.711749+09:00 192.168.xxx.xxx ns20x-master:
NetScreen device_id=ns20x-master
[Root]system-notification-00257(traffic): start_time="2014-12-16
00:11:10" duration=0 policy_id=38 service=- proto=17 src zone=SHANAI
dst zone=INTRA action=Deny sent=0 rcvd=0 src=192.168.100.xxx
dst=192.168.200.xxx src_port=2562 dst_port=8089 session_id=0
```

図 4-5 Juniper SSG のログの例

図 4-5 の例から表 4-12 が示すような情報を読み取ることができ、192.168.100.xxx の IP アドレスが割り当てられた PC から、192.168.200.xxx に割り当てられた PC の 8089 番ポートにアクセスしようとしていたことが分かる。

表 4-12 ログ分析の結果

通信ログ項目	通信ログの内容
Firewall ポリシー アクションステータス	Deny
送信元ゾーン ※製品依存の項目	SHANAI
送信先ゾーン ※製品依存の項目	INTRA
送信元アドレス	192.168.100.xxx
送信先アドレス	192.168.200.xxx
送信先ポート	8089

この例では、高度サイバー攻撃が「C&C」の段階まで進んでいることが疑われる。当該 PC が、組織内外と継続的に不正な通信をしていないかを確認する必要がある。

(d) 注意点

- Firewall のポリシーやゾーンの設定を正確に把握していないと、送信元と送信先の組合せが分からないため、このログ調査手法で検知することが出来ない
- 組織内のセグメント間に Firewall を設置することは少なく、設置していても、ログを採取していないことが多い。十分なログを採取するためには、自組織のネットワークの設計を見直す必要がある

4.2.3. Web プロキシサーバのログに残る痕跡の見つけ方

攻撃者の活動の痕跡のうち、Web プロキシサーバのログを分析して見つけられるものを表 4-13 に示す。

表 4-13 攻撃の痕跡を Web プロキシサーバのログから見つけ出す手掛かり

	攻撃行為	注	攻撃の痕跡を見つける手掛かり
不審な送信先への通信	マルウエアに感染した PC が C&C サーバやマルウエア設置サイトへの通信を試みる	B、D、H	高度サイバー攻撃に関連する情報として通知された IP アドレスやドメインなどで検索する
CONNECT メソッドで 80、443 以外のポートへ通信	CONNECT メソッドを使用して、組織外との通信を試みる	B、D、H	CONNECT メソッドの通信を検知する
標準利用以外の User Agent による通信	マルウエアに感染した PC が C&C サーバやマルウエア設置サイトへの通信を試みる	B、D、H	組織内で標準利用しているブラウザの User Agent と異なる User Agent による通信を検索する
定期的に発生する HTTP 通信	ボットに感染した PC は C&C サーバへの通信を定期的に行い、情報の取得やコントロールの受信を試みる	B、D、H	通信先サイトごとに通信頻度を調べ、頻度の高い通信先を抽出する
業務時間外に発生する HTTP 通信	マルウエアに感染した PC は、変則的な時間帯にも、C&C サーバ等へ通信を試みる	B、D、H	業務時間外に発生した HTTP 通信を抽出する
大量の HTTP 通信	マルウエアに感染した PC が C&C サーバやアップロードサイトへの通信を試みる	B、D、H	組織外への大量のデータ送信を Web プロキシのアクセスログから抽出する

注：表 2-2 および図 2-2 における攻撃活動の表示に対応

本節では、組織内の Web プロキシサーバとして利用されることの多い「squid」を前提として説明する。他の Web プロキシサーバを使っている場合には、マニュアルを参照するなどして適宜読み替えて欲しい。

4.2.3.1. 不審な送信先への通信を抽出するログ分析

マルウエアに感染した PC は、Web プロキシサーバ経由で C&C サイトへの通信やマルウエア設置サイトから新たなマルウエアなどのダウンロードを試みる。この節では、高度サイバー攻撃に関連する情報として提供された送信先 IP アドレスやドメインなどの情報を使用して、マルウエアに感染した PC から Web プロキシサーバを経由する、組織外への通信を見つけ出す方法を述べる。

(a) 採取すべきログ項目と設定方法

攻撃の痕跡を見つけるために必要な Web プロキシサーバのログ項目を表 4-14 に示す。

表 4-14 検知に必要なログ項目

ログ項目	ログ項目の内容
URL	URL、送信先サイトのドメイン

(b) 攻撃の痕跡の見つけ方

攻撃の痕跡の見つけ方は次のとおりである。

① Web プロキシサーバのアクセスログに、高度サイバー攻撃に関連する情報として示されていたアドレス (ドメイン、サブドメイン) が含まれていた場合に、攻撃の痕跡と判定する

(c) 検知例

攻撃の痕跡として抽出されたログの例を図 4-6 に示す。

```
1424221299.090 452 127.0.0.1 TCP_MISS/200 74769 GET
http://apt.example.com/xxx/xxx/apt.zip -
DEFAULT_PARENT/113.xxx.xxx.xxx application/ zip-compressed
```

図 4-6 squid の検知例

図 4-6 の例からは、表 4-15 のような情報を読み取ることができ example.com のドメインが含まれる URL に通信していたことが分かる。

表 4-15 ログ分析の結果

アクセスログ項目	アクセスログの内容
URL アドレス	http://apt.example.com/x.x/xxx/apt.zip
送信先サイトのドメイン	example.com

この種の攻撃の痕跡が見つかった場合は、高度サイバー攻撃の「デリバリ」、「インストール」、「C&C」、または「目的の実行」の段階にあることが疑われる。当該 PC がマルウエアに感染していないか、該当 PC が定常的に通信している他の送信先がないかなどを調査する必要がある。

(d) 注意点

- インターネットへの通信が、Web プロキシサーバを経由せずとも可能な場合には、検知漏れが生ずる可能性がある

4.2.3.2. CONNECT メソッドで 80、443 以外ポートへの通信を抽出するログ分析

マルウエアに感染した PC は、Web プロキシサーバ経由で C&C サイトへの通信や、マルウエア設置サイトから新たなマルウエアなどのダウンロードを行う際に CONNECT メソッドを使用する。この節では、マルウエアに感染した PC から Web プロキシサーバを経由する組織外への CONNECT メソッドを使用した通信を見つけ出す方法を示す。

(a) 採取すべきログ項目と設定方法

攻撃の痕跡を見つけるために必要な Web プロキシサーバのログ項目を表 4-16 に示す。

表 4-16 検知に必要なログ項目

ログ項目	ログ項目の内容
URL	URL、送信先サイトのポート
method	メソッド

(b) 攻撃の痕跡の見つけ方

攻撃の痕跡の見つけ方は次のとおりである。

① Web プロキシサーバのログから、CONNECT メソッドを抽出する
② 送信先ポートが、80 または 443 以外の場合に攻撃の痕跡と判定する

(c) 検知例

攻撃の痕跡として抽出されたログの例を図 4-7 に示す。

```
1423528142.737 0 192.168.xxx.xxx TCP_DENIED/403 3641 CONNECT
192.168.xxx.xxx:8089 - NONE/- text/html
```

図 4-7 squid の検知例

図 4-7 の例から、表 4-17 のような情報を読み取ることができ、192.168.xxx.xxx が含まれる URL に CONNECT メソッドで通信していたことが分かる。

表 4-17 ログ分析の結果

アクセスログ項目	アクセスログの内容
URL	192.168.xxx.xxx:8089
送信先のポート	8089
method	CONNECT

この攻撃の痕跡が見つかった場合は、高度サイバー攻撃が「デリバリ」、「インストール」、「C&C」、または「目的の実行」の段階に到達していることが疑われる。当該 PC から問題の送信先に継続して通信していないか、他の PC が問題の送信先と通信をしていないかなどを確認する必要がある。また、送信先についても、WHOIS の登録情報などにより、どのような素性のサイトかを調査しておくのがよい。

(d) 注意点

- インターネットへの通信が、Web プロキシサーバを経由せずとも可能な場合には、検知漏れが生ずる可能性がある
- 過去には Web プロキシサーバ経由で SMTP もしくはハイポートなどによる通信の事例がしばしば見られたが、現在は少なくなってきている

4.2.3.3. 標準利用以外の User Agent によるアクセスを抽出するログ分析

マルウエアに感染した PC は、Web プロキシサーバ経由で C&C サーバやマルウエア設置サイトへの通信を試みる。マルウエアによる通信では、組織内で利用しているブラウザとは異なった UserAgent を表示してクエリが発行されることがある。この節では、マルウエアに感染した PC から Web プロキシサーバを経由する組織外への通常利用しない UserAgent を使った通信を見つけ出す方法を述べる。

(a) 採取すべきログ項目と設定方法

攻撃の痕跡を見つけるために必要な Web プロキシサーバのログ項目を表 4-18 に示す。

表 4-18 検知に必要なログ項目

ログ項目	ログ項目の内容
UserAgent	UserAgent

squid の標準設定では、UserAgent の項目は出力されない。分析に必要なログを採取するためには、次の設定が必要である。

表 4-19 squid のログの設定例

File: /etc/squid/squid.conf のファイルに次の内容を追記
logformat combined %>a %ui %un [%tl] "%rm %ru HTTP/%rv" %>Hs %<st "%{Referer}>h" "%{User-Agent}>h" %Ss:%Sh access_log /var/log/squid/access_combined.log combined

(b) 攻撃の痕跡の見つけ方

攻撃の痕跡の見つけ方は次のとおりである。

① Web プロキシサーバのアクセスログから、UserAgent を抽出する。
② 組織内で利用している以外の UserAgent の場合を攻撃の痕跡と判定する。

(c) 検出例

攻撃の痕跡として抽出されたログの例を図 4-8 に示す。

```
192.168.xxx.xxx - - [12/Feb/2015:13:53:00 +0900] "POST
http://apt.example.com/control/apt.zip HTTP/1.1" 200 851 - "Wget/1.12
(linux-gnu)" TCP_MISS:DIRECT
```

図 4-8 squid の検知例

図 4-8 の例から、表 4-20 のような情報を読み取ることができ、組織内では使用しない Wget の UserAgent で通信していたことが分かる。

表 4-20 ログ分析の結果

アクセスログ項目	アクセスログの内容
UserAgent	"Wget/1.12 (linux-gnu)"

この攻撃の痕跡が見つかった場合には、高度サイバー攻撃の「インストール」、「C&C」、または「目的の実行」の段階にあることが疑われる。当該 PC から問題の送信先に継続して通信していないか、他の PC から問題の送信先に通信していないかなどを確認する必要がある。また、送信先についても、WHOIS の登録情報などにより、どのような素性のサイトかを調査しておくのがよい。

(d) 注意点

- インターネットへの通信が、Web プロキシサーバを経由せずとも可能な場合には、検知漏れが生ずる可能性がある
- 組織内で利用されているブラウザ以外のアプリケーション・プログラムやツールについての UserAgent も把握しておく必要がある。例えば、アップデート情報を取得する Java 等がこれに含まれる

4.2.3.4. 定期的に発生する HTTP 通信を抽出するログ分析

マルウエアに感染した PC は、C&C サイトへの通信を定期的に行い、情報の取得やコントロールの受信を試みる。この節では、マルウエアに感染した PC から Web プロキシサーバを経由し、組織外へ定期的に発生する通信を見つけ出す方法を示す。

(a) 採取すべきログ項目と設定方法

攻撃の痕跡を見つけるために必要なログ項目を表 4-21 に示す。

表 4-21 検知に必要なログ項目

ログ項目	ログ項目の内容
accesstime	アクセス時間
URL	URL、ドメイン

(b) 攻撃の痕跡の見つけ方

攻撃の痕跡の見つけ方は次のとおりである。

① Web プロキシサーバのアクセスログから、URL を含む行を抽出する
② URL からドメインを抽出する
③ 正規の利用で定常的にアクセスするドメイン (例えば、検索サイト等) を除去する
④ 各ドメインへの日ごとのアクセス回数を集計する
⑤ 複数日にわたって 1 日 1 回以上のアクセスが続いており、アクセスの妥当性が説明できないドメインがある場合には攻撃の痕跡と判定する

(c) 検知例

攻撃の痕跡として抽出されたログの例を図 4-9 に示す。

```
1424227775.972 21 192.168.xxx.xxx TCP_MISS/200 553 POST
http://apt.example.com/blog/ - HIER_DIRECT/apt.example.com text/html
1424314175.972 21 192.168.xxx.xxx TCP_MISS/200 553 POST
http://apt.example.com/blog/ - HIER_DIRECT/apt.example.com text/html
1424486975.972 21 192.168.xxx.xxx TCP_MISS/200 553 POST
http://apt.example.com/blog/ - HIER_DIRECT/apt.example.com text/html
```

図 4-9 squid の検出例

図 4-9 の例から、表 4-22 のような情報を読み取ることができ、apt.example.com が含まれる URL に定期的にアクセスしていたことが分かる。

表 4-22 ログ分析の結果

アクセスログ項目	アクセスログの内容
accesstime	1424227775.972
URL	http://apt.example.com/blog/
ドメイン	example.com

この種の攻撃の痕跡が見つかった場合は、高度サイバー攻撃の「C&C」または「目的の実行」の段階にあることが疑われる。当該 PC から問題の送信先に継続して通信してないか、他の PC から問題の送信先へ通信をしていないかなどを確認する必要がある。また、送信先についても、WHOIS の登録情報などにより、どのような素性のサイトかを調査しておくのがよい。

(d) 注意点

- インターネットへの通信が、Web プロキシサーバを経由せずとも可能な場合には、検知漏れが生ずる可能性がある
- C&C サーバとして、一般的なブログサイト等が用いられた場合には、ドメインごとでなく、URL (表 4-22 の URL で示す内容) ごとに集計するなど分析で工夫する必要がある
- 複数の C&C サーバを使用する、あるいは C&C サーバとの通信を不定期に行うなどのカモフラージュを行っているマルウエアは検知できない

4.2.3.5. 業務時間外に発生する HTTP 通信を抽出するログ分析

マルウエアに感染した PC は、定期的に繰り返し Web プロキシサーバ経由で C&C サーバやマルウエア設置サイトへの通信を試みる。この節では、マルウエアに感染した PC が、業務時間外など担当者が操作するはずのない時間帯に、Web プロキシサーバを経由して行う、組織外への通信を見つけ出す方法を述べる。

(a) 採取すべきログ項目と設定方法

攻撃の痕跡を見つけるために必要な Web プロキシサーバのログ項目を表 4-23 に示す。

表 4-23 検知に必要なログ項目

ログ項目	ログ項目の内容
accesstime	アクセス時間
URL	URL、ドメイン

(b) 攻撃の痕跡の見つけ方

攻撃の痕跡の見つけ方は次のとおりである。

① Web プロキシサーバのアクセスログから、特定の業務帯の通信ログを抽出する
② 通信先 URL を抽出し、システムメンテナンス等で利用されているサイト (例えば、Windows アップデート等) を除外する
③ 通信先 URL として説明のつかないものがあった場合には攻撃の痕跡と判定する

(c) 検出例

攻撃の痕跡として抽出されたログの例を図 4-10 に示す。

```
1424221299.090 21 192.168.xxx.xxx TCP_MISS/200 553 POST
http://apt.example.com/blog/ - HIER_DIRECT/aaa.bbb.xxx.xxx
text/html
```

図 4-10 squid の検知例

図 4-10 の例より、表 4-24 のような情報を読み取ることができ、example.com のサイトに不審な通信が発生していることが分かる。

表 4-24 ログ分析の結果

アクセスログ項目	アクセスログの内容
accesstime	1424221299.090
URL	http://apt.example.com/blog/
ドメイン	example.com

この攻撃の痕跡が見つかった場合には、高度サイバー攻撃が「デリバリ」、「インストール」、「C&C」または「目的の実行」の段階まで進んでいることが疑われる。当該 PC から問題の送信先アドレスに継続して通信していないか、他の PC から問題の送信先へ通信をしていないかなどを確認する必要がある。また、送信先についても、WHOIS の登録情報などにより、どのような素性のサイトかを調査しておくのがよい。

この方法による検知を目的として、メンテナンスなどの名目で従業員に PC 操作をさせない時間帯を意図的に作り出し、その時間帯に発生したアクセスを抽出して調査するアプローチも考えられる。

(d) 注意点

- インターネットへの通信が、Web プロキシサーバを経由せずとも可能な場合には、検知漏れが生ずる可能性がある
- マルウエアでなく利用者による通信の可能性を排除するため、抽出された通信を攻撃の痕跡と断定する前に、ユーザへのヒアリング等の調査が必要である。
- 検知されることを避けるため、 PC のタイムゾーンを取得して、C&C サーバとの通信を昼間時間帯にだけ行うマルウエアが存在する

4.2.3.6. 大量の HTTP 通信を抽出するログ分析

マルウエアに感染した PC は、Web プロキシサーバ経由で C&C サイトやアップロードサイトへ、ファイルや組織内で収集した情報のアップロードを試みる。この節では、Web プロキシサーバを経由して組織外の特定サイトに大量のデータを送信する行為 (ファイルのアップロード等) を見つけ出す方法を述べる。

(a) 採取すべきログ項目と設定方法

攻撃の痕跡を見つけるために必要なログ項目を表 4-25 に示す。

表 4-25 検知に必要なログ項目

ログ項目	ログ項目の内容
URL	URL、送信先サイトのポート
method	メソッド

(b) 攻撃の痕跡の見つけ方

攻撃の痕跡の見つけ方は次のとおりである。

① Web プロキシサーバのアクセスログから、同一の送信先に対する、POST メソッドから始まり、CONNECT メソッドが連続する通信ログのシーケンスを抽出する
② 抽出された通信ログのシーケンスのそれぞれについて、通信されたデータ量の合計値を算出する
③ 通信したデータ量の合計が閾値を超えた場合には攻撃の痕跡と判定する

(c) 検知例

省略。なお、Squid の場合には、通信量をログに記録する機能がないため、この手法は適用できない。

この種の攻撃の痕跡が見つかった場合には、高度サイバー攻撃の「C&C」または「目的の実行」の段階まで進んでいることが疑われる。当該 PC から問題の送信先に継続して通信していないか、他の PC から問題の送信先に通信をしていないかなどを確認する必要がある。また、送信先についても、WHOIS の登録情報などにより、どのような素性のサイトかを調査しておくのがよい。

(d) 注意点

- インターネットへの通信が、Web プロキシサーバを経由せずとも可能な場合には、検知漏れが生ずる可能性がある
- マルウエアでなく利用者による通信の可能性を排除するため、抽出された通信を攻撃の痕跡と断定する前に、該当 PC のユーザに、ログに記録された送信先、送信時間をもとにヒアリング等が必要である。
- この方法を適用するには、通信量がログに記録されていなければならないが、Squid はそのような機能をもっていない (商用製品やアプライアンス製品等にはこの機能を持つものがある)

4.3. DNS サーバ、認証サーバのログの分析

4.3.1. DNS サーバのログの分析

キャッシュサーバの役割を持つ DNS サーバのログには、高度サイバー攻撃の「デリバリ」や「インストール」、「C&C」、「目的の実行」の各段階で攻撃の痕跡が記録される。マルウエア設置サイトへのアクセス (表 2-2 および図 2-2 における「B」) や、マルウエアによる C&C サーバへのコールバック(表 2-2 および図 2-2 における「C」、「D」、「G」及び「H」) の際に DNS サーバにホスト名の解決を行ったクエリが記録されている可能性がある。ただし、DNS サーバのログには、正常な PC からのホスト名の解決を行ったクエリも含まれるなど膨大な量が記録されるので、その中から痕跡を見つけ出すのは困難である。Web プロキシサーバや Firewall など他のログの分析結果から、調査範囲を絞り込むことができれば、DNS サーバのログの分析が可能になる。

なお、DNS サーバのクエリのログを採取するためには、DNS サーバでクエリをログに出力する設定を有効にする必要がある。次の表 4-26 は、bind9 における設定の例である。(この例では、file で指定したファイルにログを保存し、ファイルサイズが 1GB を超えた場合、10 世代までログローテーションを行うように設定している)

表 4-26 bind9 のログの設定例

File: /etc/named.conf のファイルに次の内容を追記

logging {
channel "queries_log" {
file "/var/log/queries.log" versions 10 size 1g;
severity info;
print-time yes;
};
category queries { " queries_log"; };
};

DNS サーバのログを Firewall のログと組み合わせて分析した例を図 4-11 に示す。この例では、Firewall のログの分析により、192.168.100.xxx の IP アドレスが割り当てられた PC から 23.23.xxx.xxx への通信が Firewall で拒否された事象が見つかり、DNS サーバのログの分析により、当該 PC がアクセスしようとした Web サイトのホスト名を割り出すことができた。

(Firewall のログ)

```
2014-12-16T01:01:55.711749+09:00 192.168.xxx.xxx ns20x-master: NetScreen
device_id=ns20x-master [Root]system-notification-00257(traffic):
start_time="2014-12-16 00:11:10" duration=0 policy_id=38 service=- proto=17
src zone=SHANAI dst zone=INTRA action=Allow sent=100 rcvd=100
src=192.168.100.xxx dst=23.23.xxx.xxx src_port=2562 dst_port=22 session_id=0
```

(DNS サーバのログ)

```
16-Dec-2014 01:03:55 client 192.168.100.xxx #47197: query: apt.example.com IN
A + (192.168.1.xxx)
```

図 4-11 Firewall と DNS サーバのログの突き合わせの例

4.3.2. 認証サーバのログの分析

高度サイバー攻撃における「横断的侵害」や、「目的の実行」の段階で、マルウエアがファイルサーバ等にアクセスする際や、割り当てられた以上の権限奪取などを試みる際に、認証サーバへのリクエストが発生し、ログに記録される。これは表 2-2 および図 2-2 の「F」に相当する。認証サーバのログには、膨大な量のログが記録されるため、他の方法で得た情報を用いて、調査対象を絞り込む必要がある。本節では、組織内環境で認証サーバとして用いられていることの多い「Active Directory」を前提として説明する。

認証サーバのログを採取するためには、同サーバの監査ポリシーの設定で、次の項目を有効にしている (OS によっては初期設定で有効となっている場合もある) 必要がある。この設定を有効にすることで、Active Directory のログが、Windows のイベントログとして記録される。

- アカウントログオン
  - 資格認証の確認の監査
  - Kerberos 認証サービスの監査

- ログオン／ログオフ
  - ログオンの監査
  - その他ログオン／ログオフイベントの監査
  - 特殊なログオンの監査

また、認証サーバのログ分析に先立って、運用で利用するドメインの管理者アカウントの棚卸ができており、各アカウントの運用実態が把握・整理されていることが重要である。

認証サーバのログ調査では、通常の認証要求では発生しないような認証イベントを抽出、あるいは、管理者アカウントが関連する認証イベントを抽出した上で、抽出されたイベントを個々に吟味することにより高度サイバー攻撃の痕跡が見つかる可能性がある。ここでは、特に注意が必要なものについて、2 つ例を示す。

(1) 通常の認証要求では発生しないような認証イベントの調査

Active Directory のログには、Windows のイベント ID が付与されている。表 4-27 に記載されたイベント ID は、通常の認証要求とは異なる特殊な操作要求などを Active Directory が受け取ったことを示している。

表 4-27 Active Directory の注意すべきイベント ID　一覧

Current Windows Event ID	Potential Criticality	Event Summary
4618	High	監視対象のセキュリティイベントパターン
4649	High	リプレイ攻撃が検出されました。
4719	High	システム監査ポリシーが変更されました。
4765	High	SID の履歴をアカウントに追加されました。
4766	High	SID の履歴をアカウントに追加できませんでした。
4794	High	ディレクトリ サービス復元モードを設定しようとしました。
4897	High	役割の分離が有効になっています。
4964	High	特殊グループは、新しいログオンに割り当てられています。
5124	High	OCSP レスポンダー サービスのセキュリティ設定が更新されました。
1102	Medium to High	イベントログ消去

参考: マイクロソフト社のレポート"Best Practices for Securing Active Directory"からの抜粋(*6)

この調査の結果、これらのイベントがあれば、サイバーキルチェーンモデルの C&C の段階の可能性が懸念されるため、詳細な調査が必要と考えられる。セキュリティベンダーなどに相談することを推奨する。

(2) 管理者アカウントに関連したイベントの調査

Active Directory のログにおいて、次のような認証イベントを抽出する。

- 管理者アカウントの認証要求を発行した PC (IP アドレス) が想定外
- 特権の割り当てを要求したアカウントが想定外
- 特定の PC から認証要求イベントの回数が急激に変化する
- 特定の PC から異常に多くの認証要求イベントが存在する

この調査の結果、イベントが意図しないものであれば、サイバーキルチェーンモデルの C&C の段階の可能性が懸念されるため、詳細な調査が必要と考えられる。セキュリティベンダーなどに相談することを推奨する。

5. まとめ

高度サイバー攻撃を受けた被害組織が、攻撃に気付くまでには数か月以上の時間が経過していることが多いと言われている。被害組織が攻撃に気付くまでの期間は、スパイ活動を目論む攻撃者の意のままに、組織内の情報システムや情報資産がアクセスされ続けるわけである。また、標的となる組織は、大企業や中央官庁などばかりでなく、中小や地方の組織にも広がってきている。中小の組織では、セキュリティの知識を身に付けた運用者を配置できていない場合も多い。本書では、情報セキュリティについて基本的な知識を身に付けただけで、情報システムの運用を任されている方々をに、少しでも早い段階で高度サイバー攻撃を受けている事実に気付いていただくために、情報システムの主な機器のログを調査分析する基本的な方法と考え方を紹介した。高度サイバー攻撃による被害の軽減に向けた各組織における活動の一助となれば幸いである。

なお、組織内の情報システムの構築に用いられているコンポーネントは一様でないため、採取できるログやログの形式にも相違が生じる。本書での説明は、図 2-1 のような構成をもつ組織内情報システムを前提として書かれているので、実際にログ調査をする場合には、システム構成の相違を吸収するための読み替えをいただきたい。また、コンポーネントに機能差がある場合等には本書には書かれていない配慮が必要となる可能性もある。高度サイバー攻撃の手口は、時とともに変化していくことが予想されるため、変化した攻撃の手口に対応するように、調査時の痕跡を見つけ出す方法を最適化していくことも忘れてはならない。JPCERT/CC などから提供されるセキュリティ動向情報にも継続的に目を通していただけるようお願いする所以である。さらには、そうした公にされた情報に加えて、高度サイバー攻撃の攻撃インフラに関する情報も含め共有しているフレームワークへの参加もお勧めしたい。

コラム

高度サイバー攻撃に関する詳細情報の共有

高度サイバー攻撃といえども、すべての手口が標的組織ごとに新たに開発されるのではなく、繰り返して利用される手口も少なくない。特に、同じ業界の組織には、類似の手口と攻撃インフラ（C&C サーバやマルウエア設置サイト、マルウエアなど）を用いた攻撃がしばしば行われる。そうした場合には、攻撃の痕跡を先に発見した組織が分析した攻撃の手口を、高度サイバー攻撃の情報（主に、標的型攻撃メールや、攻撃に使用されたサイト、ドメイン、マルウエア情報を含む攻撃の手口などの情報から、可能な限り被害組織に関連する情報を除いたもの。以下、「攻撃情報」という。）として共有すると、他の組織が攻撃を調査する際や、攻撃を防ぐための対策を検討する際の参考情報として決定的な価値がある。こうした情報共有が広がれば、結果として、有効な攻撃手口の寿命を縮めて攻撃者側のコストを上げる効果を期待できる。

攻撃情報共有のフレームワーク

あらかじめ参加組織を募り、攻撃情報を共有するためのフレームワークが設けられている。高度サイバー攻撃の痕跡と疑わしい異常を発見したメンバー組織は、それに関連する攻撃情報を抽出し、そのフレームワークに提供する。フレームワークのハブ機関が、提供された攻撃情報を分析（マルウエアなどの挙動や通信先の解析、過去の事例との類似性などを調査）した上で、必要に応じて会員組織にフィードバックする。次の図 A は、JPCERT/CC の情報共有のフレームワークをイメージしたものである。

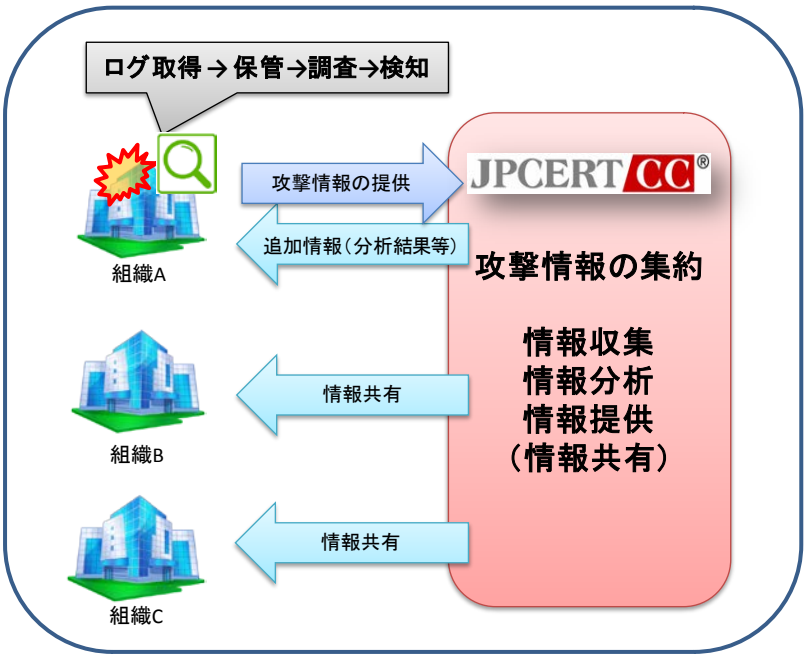

図 A 攻撃情報の共有のフレームワーク（例）

JPCERT/CC における取り組みの詳細については、「早期警戒情報の提供について」[(*7)]を参照していただきたい。

6. 付録

(1) サイバー情報共有イニシアティブ (J-CSIP) 2014 年度 活動レポート
https://www.ipa.go.jp/about/press/20150527.html

(2) LOCKHEED MATIN Cyber Kill Chain
http://www.lockheedmartin.com/us/what-we-do/information-technology/cyber-security/cyber-kill-chain.html

(3) Mandiant APT1
http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

(4) 「平成 23 年度政府機関における情報システムのログ取得・管理の在り方の検討に係る調査報告書」NISC
http://www.nisc.go.jp/inquiry/pdf/log_shutoku.pdf

(5) 「Payment Card Industry (PCI) データセキュリティ基準 V3.0」PCIDSS
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3_JA-JP.pdf

(6) Best Practices for Securing Active Directory
Appendix L: Events to Monitor
https://technet.microsoft.com/en-us/library/dn487446.aspx

(7) JPCERT/CC 早期警戒情報の提供について
https://www.jpcert.or.jp/wwinfo/

4.2 章以降に示す Postfix、squid、bind のログ出力に関する設定例については、JPCERT/CC の調査で確認した一例であり、すべてのバージョンでの動作を保証するものではありません。

本設定に関して発生したいかなる損害も JPCERT/CC は、責任を負いかねます。実際の機器に設定を行う場合は、各機器、もしくはベンダーが提供するマニュアルを参照し、十分なテストを実施の上、設定してください。