第3日目

情報セキュリティ担当者のためのインシデント対応入門

マルウェア感染対応
メール感染型マルウェア編

2014年12月

セクタンラボ勉強会

講座の全体構成

講座名称	主な学習内容
フォレンジック基礎編	・感染PCの調査に用いる基本ツールの操作方法
WEB型マルウェア編	・感染源WEBサイトの特定・遮断方法 ・感染PCに潜伏しているマルウェア検体の取得方法
メール型マルウェア編	・特定の不審メールの遮断方法 ・特定の不審メール受信者の把握方法 ・感染PCに潜伏しているマルウェア検体の取得方法
模擬訓練	・机上での模擬訓練により，マルウェア感染状況の把握，ならびに被害拡大防止対応の判断と指示を体験

本日

本章の学習内容

- メール感染型マルウェアとは，不審メールの添付ファイルの閲覧，またはメール本文に記載されたURLのクリックなどを通じて，PCへの感染を広げるマルウェアです。

- 本章では，メール感染型マルウェアの感染メカニズム，ならびに痕跡の調査方法を学習します。

本日の次第

第1章 マルウェア感染メカニズムと痕跡

- メール感染型マルウェア感染時の挙動ならびに痕跡の調査方法を学習します。

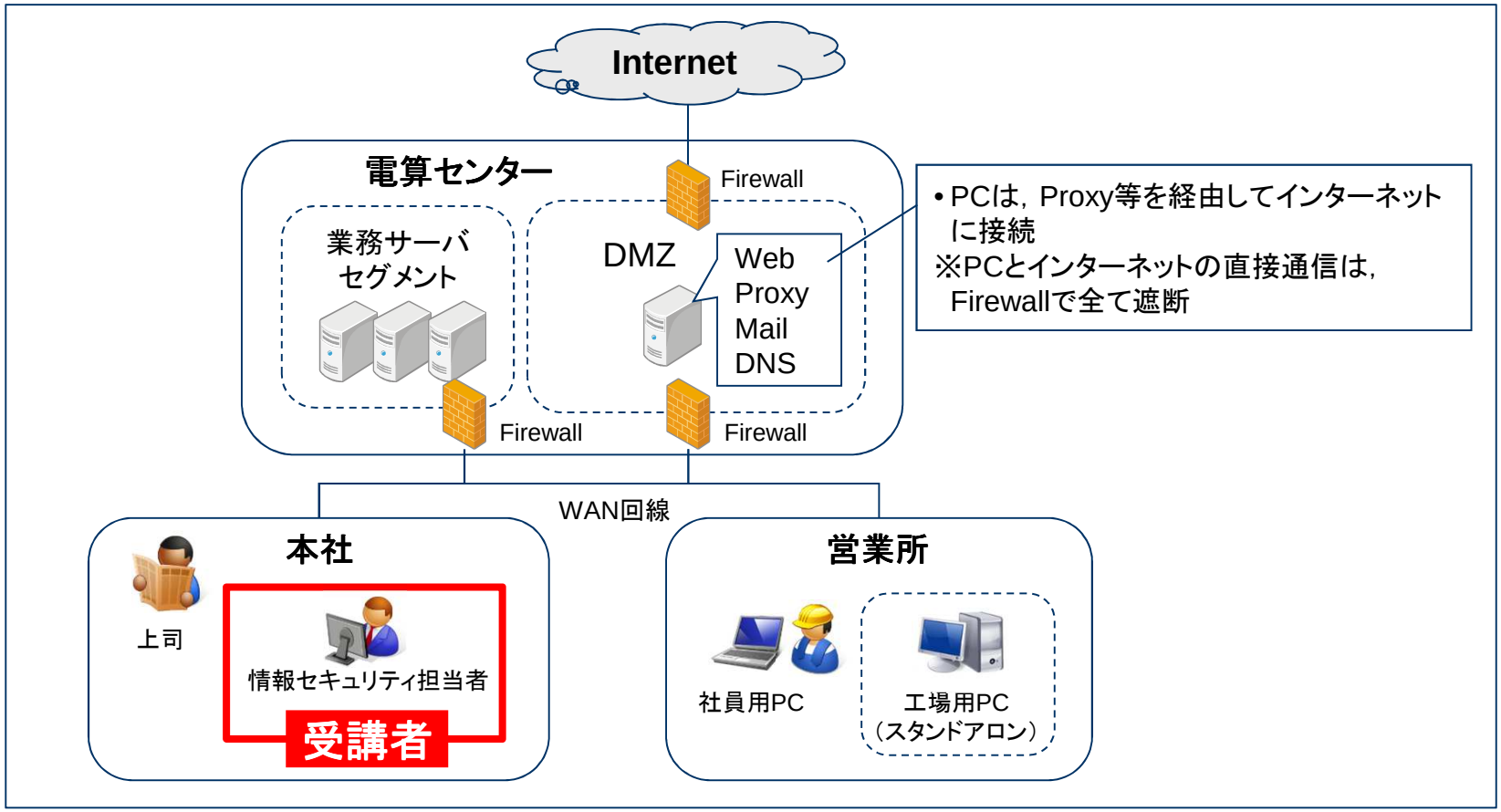
第2章 想定シナリオの対応

- 想定シナリオにおける対応を疑似体験します。

想定するシステム環境（模擬システム）

- **本講座では，次のシステム環境を想定しています。**

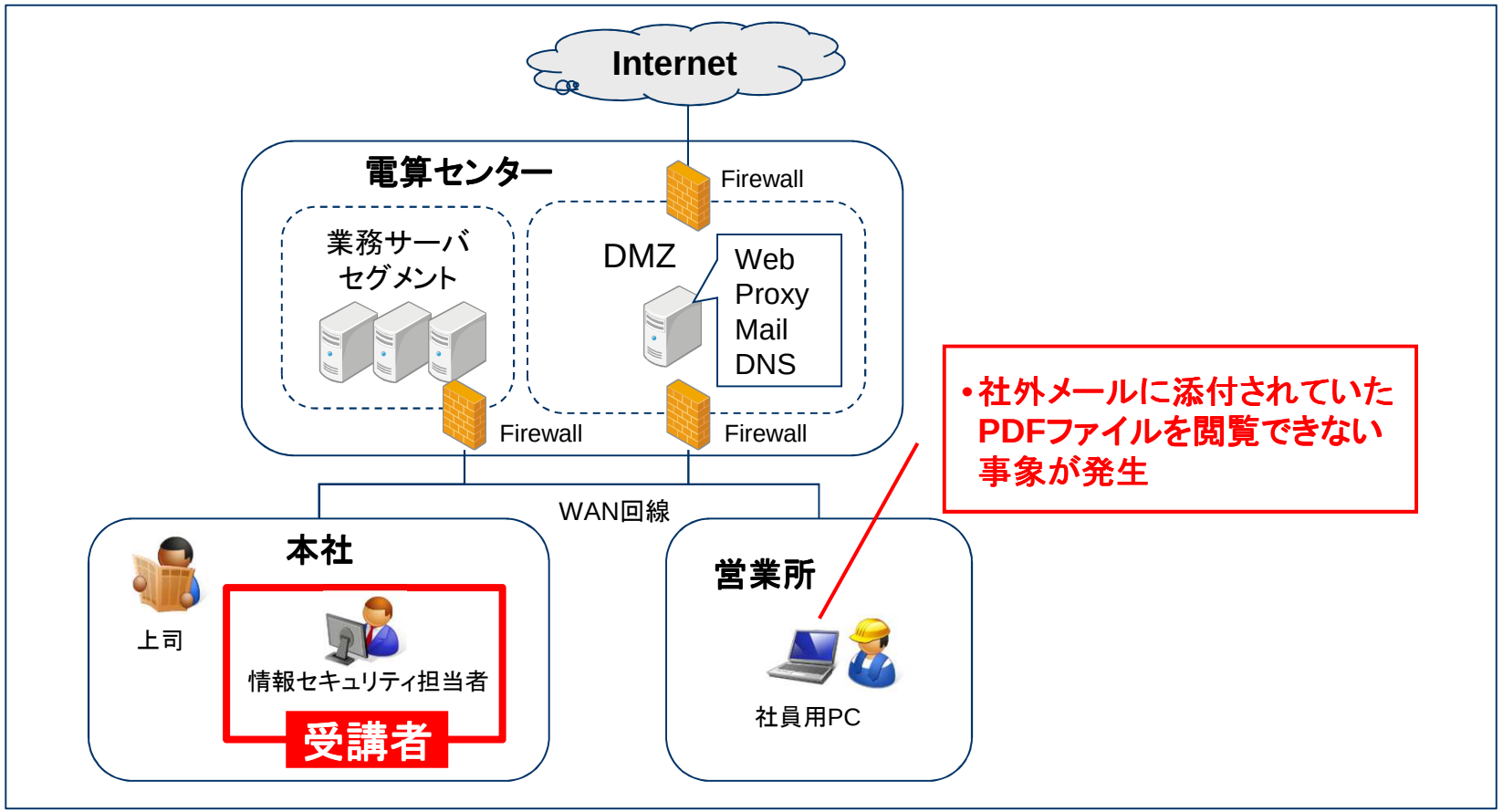
◆ **模擬システムの構成**



［注意事項］本講座では，特に指定が無い場合，Windows7のアーチファクトを説明する。WindowsXPでは一部仕様が異なるため，注意すること。

本日の想定シナリオ

- ある日，営業所の社員から，社外メールに添付されていたPDFファイルを閲覧できないとの電話連絡がありました。
- 状況を確認したところ，PCの挙動が怪しいようです。
  さて，どうしますか？

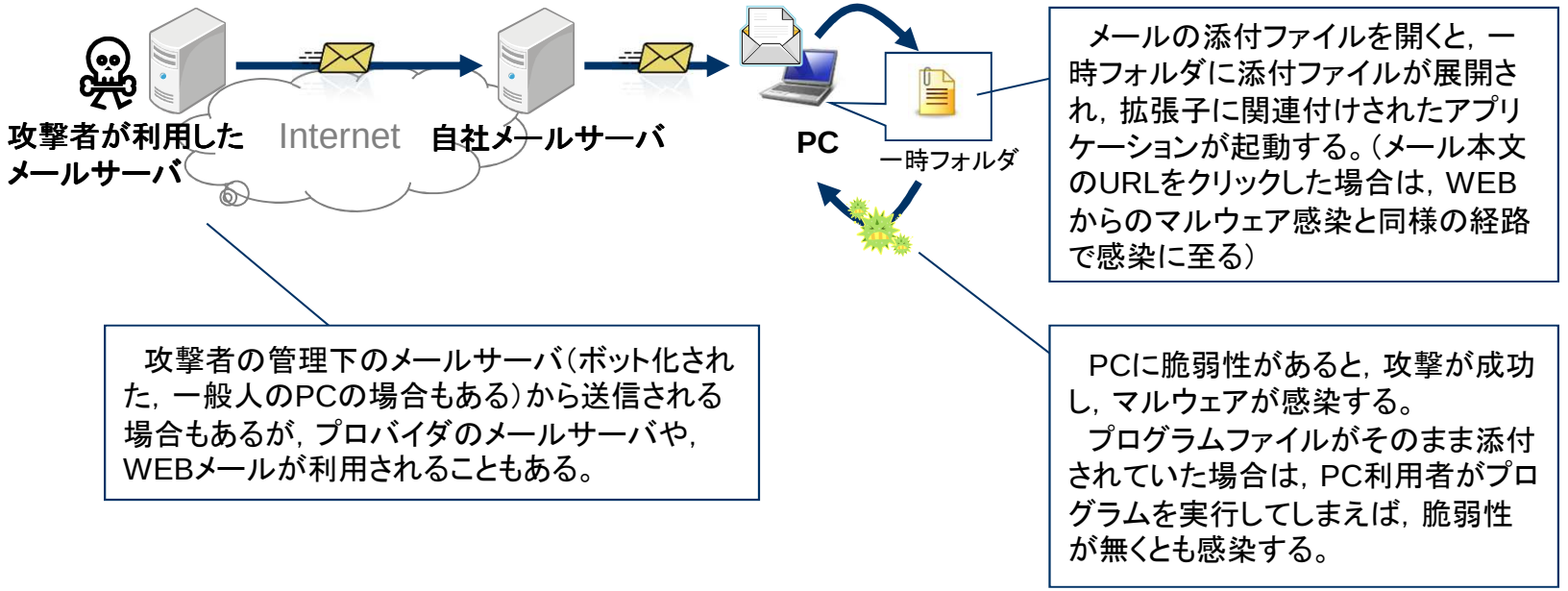


第1章 マルウェア感染メカニズムと痕跡

攻撃経路の概要

- **攻撃者は，攻撃メールをPC利用者に送信します。**
- **攻撃メールを受信したPC利用者が，添付ファイルを開いたり，本文に記載されたURLをクリックすると，PCがマルウェアに感染します。**
  - 添付ファイル　：脆弱性攻撃コードが埋め込まれたファイル，またはマルウェアのプログラムファイル
  - 本文のURL　：攻撃用WEBサイトへのリンク

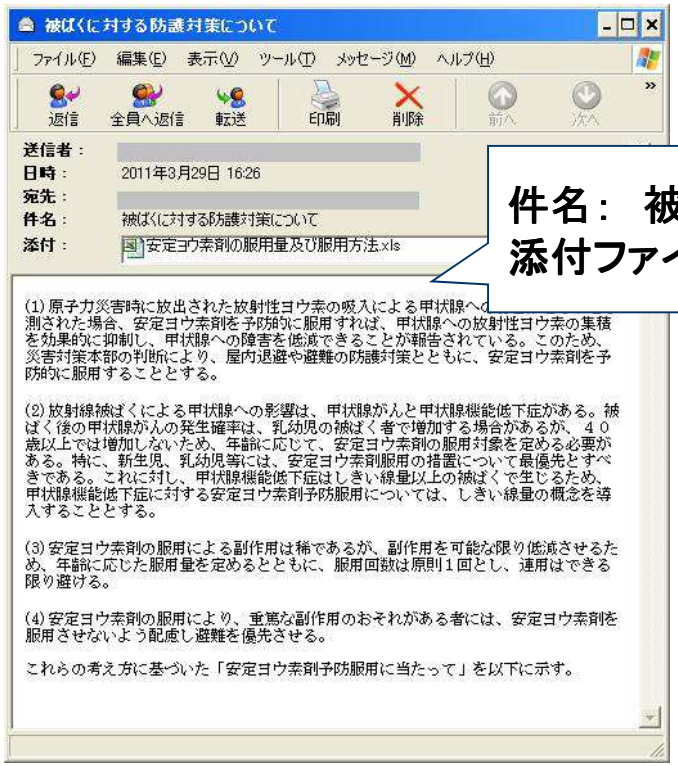
［注意］メールソフトに脆弱性があると，攻撃メールの本文を閲覧しただけで感染することもあります。



攻撃メールの事例（1/2）

- 攻撃メールは，災害情報など，受信者の興味を引く内容に工夫されています。
- 差出人メールアドレスが，フリーメールアドレスとなっている場合も多いです。

◆攻撃メールの一例（2011年の東日本大震災の直後に出回ったメール）



件名： 被ばくに対する防護対策について
添付ファイル名： 安定ヨウ素剤の服用量及び服用方法.xls

［画像の引用元］
IBM Tokyo SOC Report 原発事故に便乗した不正なメールを確認
https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/spam_jp_20110330?lang=ja

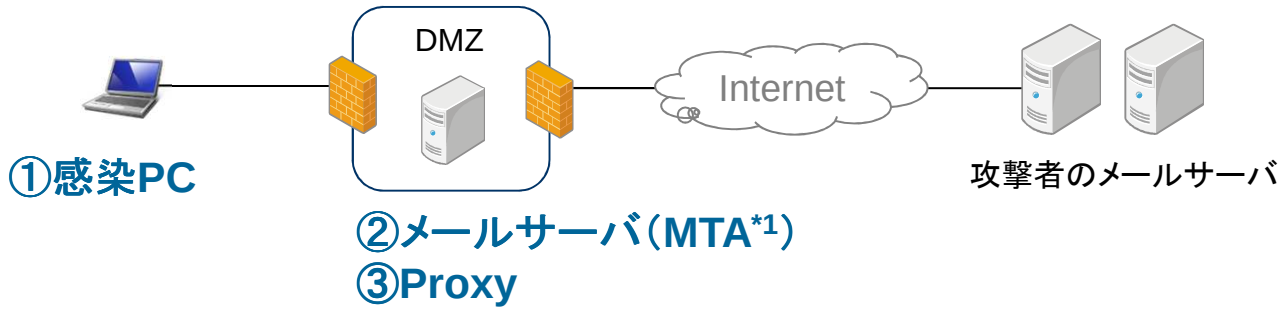
攻撃メールの事例（2/2）

- **メールプロトコルであるSMTPの仕様上，差出人（From）など，ほとんどのメールヘッダー情報は偽装できます。特定の組織に狙いを定めた巧妙な攻撃メールは，メール件名や本文を注意深く見ても，攻撃メールと判断できない可能性があります。**

- **最近は，次のような攻撃事例も報告されており，利用者の注意だけでは攻撃を完全に防止することが困難な場合もあります。**
  - 標的とする企業の取引先企業などのPCを乗っ取り，盗聴した本物の業務メールにマルウェアを添付し「再送」する攻撃
  - 問い合わせを装い，何度かメールでやりとりをしたうえで，マルウェアを添付した攻撃メールを送信してくる「やりとり型」攻撃

攻撃の痕跡が残される個所

- 攻撃の痕跡は，①感染PC，②メールサーバ，③Proxyに残されます。



個所	主な痕跡
① 感染PC	• 攻撃メール（送信元の情報，攻撃に利用された添付ファイル検体） • マルウェアの検体 • マルウェアが改変したファイル/レジストリ
② メールサーバ	• 攻撃メールの受信者
③ Proxy	• 感染PCのインターネット通信履歴

*1 MTA（Mail Transfer Agent）：メールの中継に利用されるSMTPサーバのこと。

メールサーバ

Proxy

感染時のPCの挙動

[パターン1] 実行形式の添付ファイルを開いた場合

① PCのメールソフトは，メール添付ファイルを一時フォルダに保管する。メールソフトは，一時フォルダに保管したファイルを実行する。（この時点で感染する）

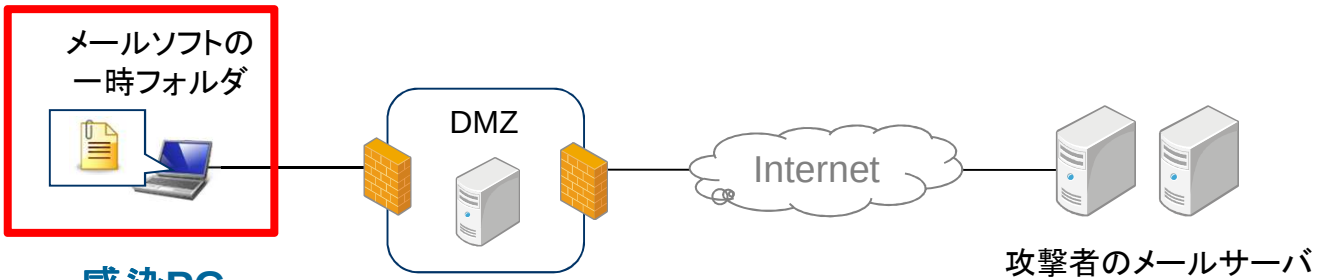
[パターン2] 文書形式の添付ファイルを開いた場合

① PCのメールソフトは，メール添付ファイルを一時フォルダに保管する。メールソフトは，一時フォルダに保管したファイルを，関連付けされたアプリケーションで開く。
PCに脆弱性が存在しない場合，ここで攻撃が失敗する。

② 脆弱性攻撃が成功すると，攻撃コードが実行される。
（攻撃者のWEBサイトから，マルウェア本体をダウンロードすることが多い）

[パターン3] メール本文のURLをクリックした場合

（WEB感染型マルウェアと挙動が同じのため，説明割愛）



感染PCの痕跡

- **感染PCには，攻撃メール*1，脆弱性攻撃コード，マルウェア検体など，さまざまな痕跡が残されます。**
  （基本的な調査方法は，WEB感染型マルウェアと同じ）

◆ **感染PCの痕跡**

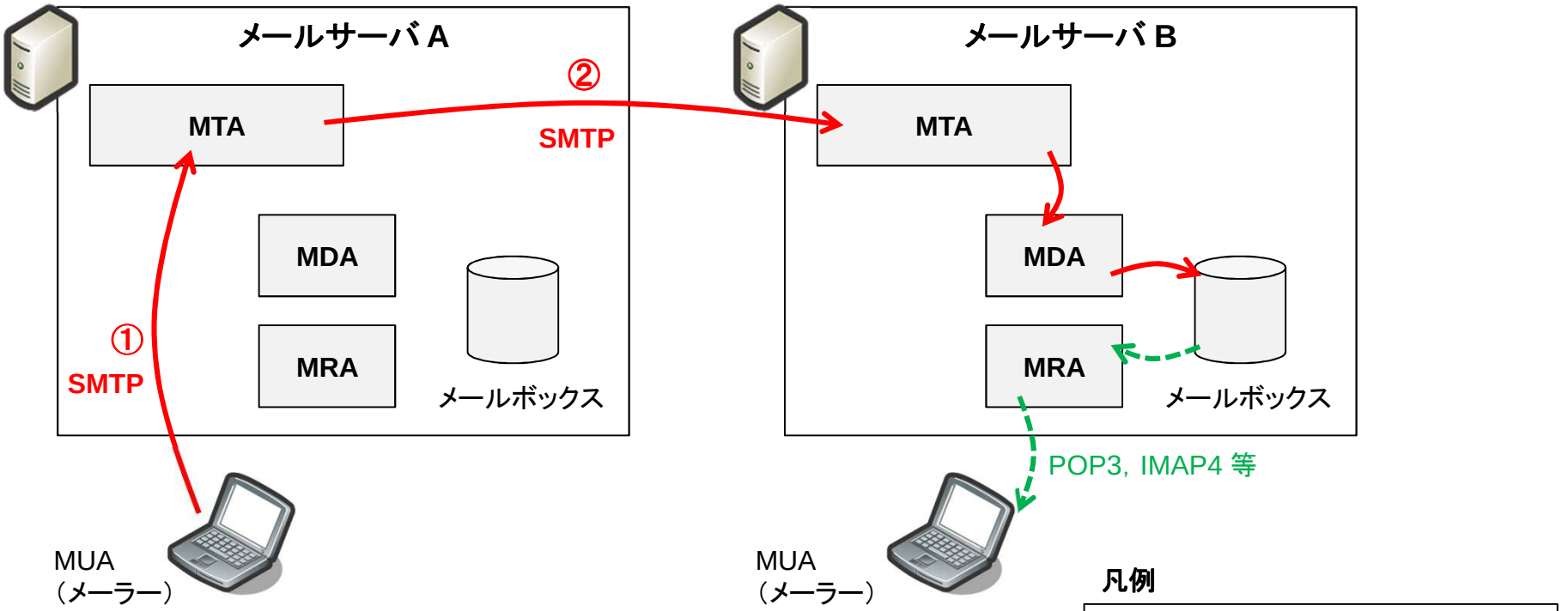
調査個所	説明
攻撃メール	• 攻撃メール本文，添付ファイルを検体として確保する。 • メールヘッダー情報から，攻撃メール送信元の手がかりを取得できる場合もある。
メールソフトの一時フォルダ	• 一時フォルダに，閲覧したコンテンツが保管されている可能性がある。
各種一時フォルダ	• ZIPファイルなどの各種一時フォルダに，ブラウザで閲覧したコンテンツが保管されている。
ファイルシステム，レジストリ	• ファイルシステム，レジストリなどに，感染により改変された痕跡が残る。

*1 WEBメールの場合は，感染PC側に攻撃メールが残らないため，サーバ側で攻撃メールを確保する必要がある。

電子メール配送の仕組み

- メールサーバは，複数の機能で構成されています。その中で，メール配送の中心的な役割を担うのが，MTAです。
- MTAは，MUA及び送受信相手のMTAと，SMTPプロトコルで通信を行います。

図．メールサーバAからメールサーバBへのメール配送の概要

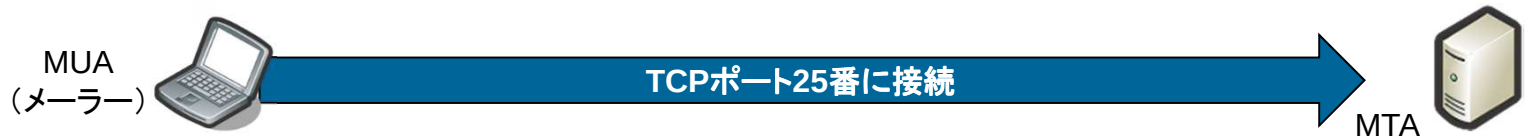


MTA(Mail Transfer Agent)：メール送信サーバ(SMTP), MUA(Mail User Agent)：メーラー
MDA(Mail Delivery Agent), MRA(Mail Retrieval Agent)：メール受信サーバ(POP3/IMAP等)

SMTPの基礎

- **SMTPは，テキスト（ASCIIコード）で通信を行うシンプルなプロトコルです。**
- **MUAがMTAにメール配送を依頼する場合は，下図のような通信を行います。**

※SMTPには，MUAから入力された内容に虚偽がないか検証する仕組みが無いため，改竄が容易です。



220 mail.exsample.com ESMTP Postfix
HELO exsample.com ・・・自ドメイン名
250 mail.exsample.com （MTAによりヘッダーに記載される）
MAIL FROM:root@exsample.com ・・・発信元アドレス（エラーメールの宛先）
250 2.1.0 Ok
RCPT TO:user01@exsample.com ・・・宛先アドレス
250 2.1.5 Ok

DATA ・・・メールデータの開始を宣言 **ヘッダー**
354 End data with <CR><LF>.<CR><LF>
FROM:root@exsample.com
TO:root@exsample.com ・・・ヘッダー情報
SUBJECT:Good Morning!
（改行）

Hello! World! ・・・メール本文 **本文**
. ・・・メールデータの終了を宣言（ピリオド）
250 2.0.0 Ok: queued as 1E14F8056D
QUIT ・・・メールサーバから切断
221 2.0.0 Bye

エンベロープ（封筒）
この情報が，実際の配送に利用されます。また，HELOコマンドを除き，ヘッダーにも記録されません。

メールデータ
ヘッダーは，本文とほぼ同等の位置づけであり，配送には利用されません。

凡例

aaa ：**MUAの入力**
bbb ：**MTAの応答**

攻撃メールの調査（1）メールヘッダーの確認

- **メールヘッダー（Receivedヘッダー）には，送信元MTAのIPアドレスが記録されているため，成りすましの有無の判断材料になります。**
  - Receivedヘッダーは，メールを受信したMTAが，上部に追記していくため，下部にいくほど，送信元に近いMTAが記載したものとなります。

（**注意**）転送したメールには，元のヘッダー情報は含まれません。攻撃メールのヘッダーを確認する際は，攻撃メールの受信者に，メールのソースを出力したものを送付してもらいます。

自社やプロバイダなど，信頼できるMTAが記録したReceivedヘッダーを確認することで，メール送信元MTAのIPアドレスを確認できる。
送信元MTAのIPアドレスが所属するドメインが，Fromのドメインと一致しない場合は，成りすましメールの可能性がある。

◆Receivedヘッダーの書式

Received: from 送信側MTAホストネーム【1】 (送信型MTAホストネーム [送信側MTAのIPアドレス]【2】)
by 受信側MTAホストネーム【3】
with プロトコル【4】 id キューID【5】
for 受信者のEメールアドレス
MTAの受信日時

Receivedヘッダーを記録したMTA

メールサーバのログに記録されるキューIDと一致する

【1】送信側MTAが自己申告したホストネーム（任意に設定可能なので，詐称されている可能性がある）
【2】送信側MTAのIPアドレスと，DNSでリバースルックアップしたホストネーム
【3】このReceivedヘッダーを記載したMTA
【4】SMTPやESMTPなどのプロトコル名
【5】受信側MTAで識別用に設定するユニークなキューID

（参考）メールヘッダーのサンプル（1/2）

◆例1.検証環境（Postfix）で，example.comから，localdomain.invalidに送信したメール

（前略）

Received: from mail.example.com (unknown [192.168.0.200])

by mail.localdomain.invalid (Postfix) with ESMTP id 9E920F005D

for <user01@localdomain.invalid>; Sun, 2 Sep 2012 22:36:00 +0900 (JST)

送信元MTAのIPアドレス

メールサーバのログに記録されるキューIDと一致

Received: from 192.168.0.200 (localhost.localdomain.invalid [127.0.0.1])

by mail.example.com (Postfix) with ESMTP id 471E7F0093

for <user01@localdomain.invalid>; Sun, 2 Sep 2012 22:36:23 +0900 (JST)

Received: from 192.168.0.2

(SquirrelMail authenticated user attacker)

by 192.168.0.200 with HTTP;

Sun, 2 Sep 2012 22:36:23 +0900 (JST)

（後略）

ここより下は，自社の管理外のMTAが記載したヘッダーのため，詐称されている可能性がある

［メール送信側の設備情報］
送信PCのIP　：192.168.0.2
送信元MTA　：mail.example.com，192.168.0.200（オープンソースのWEBメール「SquirrelMail」+「Postfix」）

［メール受信側の設備情報］
受信MTA　：mail.localdomain.invalid，192.168.100.50（Postfix）
受信アドレス　：user01@localdomain.invalid

（参考）メールヘッダーのサンプル（2/2）

◆例2．メールソフト（プロバイダAのアカウント）から，hotmailに送信したメール

（前略）
Received: from ■.■.ne.jp ([XXX.XXX.XXX.XXX]) by ■.■.hotmail.com with Microsoft SMTPSVC(6.0.3790.4900);
Sat, 1 Sep 2012 06:55:49 -0700
Received: from [127.0.0.1] (■.■.■.■.ne.jp [XXX.XXX.XXX.XXX])
by ■.■.ne.jp with ESMTP id q81DtnOV000766
for <■■■■@live.jp>; Sat, 1 Sep 2012 22:55:49 +0900
Message-ID: <504213E5.9060700@yahoo.co.jp>
Date: Sat, 01 Sep 2012 22:55:49 +0900
From: ■■■■@■■.ne.jp
（後略）

プロバイダAのMTAのIPアドレス

プロバイダAから送信元PCに割り当てられたグローバルIPアドレス（プロバイダのMTAが記録したヘッダー）

◆例3．WEBメール（Yahoo）から，hotmailに送信したメール

（前略）
Received: from ■.yahoo.co.jp ([XXX.XXX.XXX.XXX]) by COL0-MC2-F29.Col0.hotmail.com with Microsoft SMTPSVC(6.0.3790.4900);
Sat, 1 Sep 2012 07:03:47 -0700
Received: (qmail 26120 invoked by uid 60001); 1 Sep 2012 14:03:46 -0000
（中略）
Received: from [XXX.XXX.XXX.XXX] by web4009.mail.ogk.yahoo.co.jp via HTTP; Sat, 01 Sep 2012 23:03:46 JST
X-Mailer: YahooMailWebService/0.8.111_27
Date: Sat, 1 Sep 2012 23:03:46 +0900 (JST)
From: ■■■■@yahoo.co.jp
（後略）

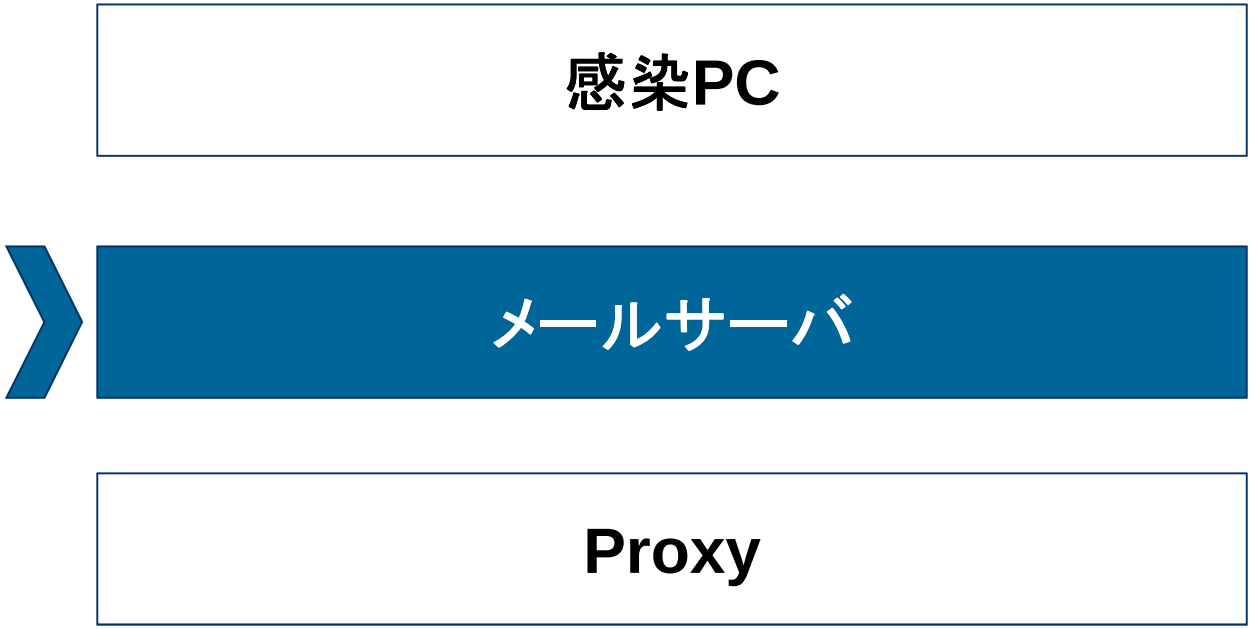
送信元PCのグローバルIPアドレス
（YahooのWEBメールサーバが記録したヘッダー）

メールソフトの一時フォルダ

- メールソフトにより一時フォルダの取扱いが異なります。
- ウィルス対策ソフトが，一時フォルダのファイルをリアルタイム検知した場合は，添付ファイルを閲覧したものの，感染を未然防止した可能性が高いと考えることができます。

◆ メールソフトの一時フォルダ

メールソフト	一時フォルダの場所
Microsoft Windows Live Mail ver.2011	①C:¥Users¥（ユーザ名）¥AppData¥Local¥Microsoft¥Windows¥Temporary Internet Files¥Content.IE5¥ランダムなフォルダ名¥ 上記に添付ファイル名と同じ名前のファイルが作成される。 （補足）一時ファイルは，Windows Live Mailの終了時に自動的に削除される。ただし，添付ファイルを開いた状態でWindows Live Mailを終了した場合は削除されない。
Mozilla Thunderbird ver.31.0	① C:¥Users¥（ユーザ名）¥AppData¥Local¥Temp 上記に添付ファイル名と同じ名前のファイルが作成される。 （補足）一時ファイルは，Thunderbirdを終了しても自動削除されない。
IBM Lotus iNotes 8.5.1(DWA)	① C:¥Users¥（ユーザ名）¥AppData¥Local¥Temp¥Domino Web Access¥ 上記に添付ファイル名と同じ名前のファイルが作成される。 ②Internet Explorerの一時フォルダと同じ場所 上記に「 $File[N] 」（Nは数字）という名前で保存される。 （補足）「ログアウト」のタイミングで一時フォルダ「Domino Web Access」が削除される。（ログアウトせずにブラウザを終了した場合は削除されない）


感染PC
メールサーバ
Proxy

メールサーバのログの調査（1/2）

- 攻撃メールのヘッダーに記載されているキューIDを検索し，攻撃メールを受信したアカウントを特定します。
- また，送信元MTAのIPアドレスが記録されているため，攻撃メールの差出人の成りすましの有無の判断材料とします。

◆Postfixのログ（/var/log/maillog）：メール受信（宛先に1アカウントを指定）

```
Sep  2 23:03:13 dmz_ns postfix/smtpd[2418]: connect from unknown[192.168.0.200]
                ・外部のMTA（192.168.0.200）からの接続（この例では，攻撃者のMTA）

                                                メールヘッダーと一致するキューID
Sep  2 23:03:13 dmz_ns postfix/smtpd[2418]: 59781F0079 : client=unknown[192.168.0.200]
Sep  2 23:03:13 dmz_ns postfix/cleanup[2422]: 59781F0079: message-id=20120902140330.BDD1DF0093@mail.example.com
                ・WEBメールから送信されたメールの場合，メッセージIDに送信元PCのIPアドレスが含まれる場合がある。
                （参考）オープンソースのsquirrel mailから送信されたメールでは，「message-id=<3615.192.168.0.2.1346592983.squirrel@192.168.0.200>」のように，送信元PCのIPアドレス（192.168.0.2）が含まれる。

Sep  2 23:03:13 dmz_ns postfix/smtpd[2418]: disconnect from unknown[192.168.0.200]
Sep  2 23:03:13 dmz_ns postfix/qmgr[2053]: 59781F0079: from=<testmail@example.com>, size=724, nrcpt=1 (queue active)
                ・エンベロープで指定された送信元（from） ヘッダー情報と一致しない場合があるため注意

Sep  2 23:03:13 dmz_ns postfix/local[2423]: 59781F0079: to=<user01@localdomain.invalid> relay=local, delay=0.09, delays=0.06/0.02/0/0.01, dsn=2.0.0, status=sent (delivered to mailbox)
                ・エンベロープで指定された宛先（rcpt to）
                                                メールを受信したアカウント
Sep  2 23:03:13 dmz_ns postfix/qmgr[2053]: 59781F0079: removed
```

メールサーバのログの調査（2/2）

- **複数宛先を指定して送信されたメールは，キューIDが同一となります。**
  - 複数宛先の指定方法が，To, CC, BCCのいずれでもキューIDが同一となります。
  - 「1回のメール送信で，1アカウントに送信する操作」を繰り返した場合は，それぞれキューIDが異なるものとなります。

◆Postfixのログ（/var/log/maillog）：メール受信（宛先に3アカウントを指定）

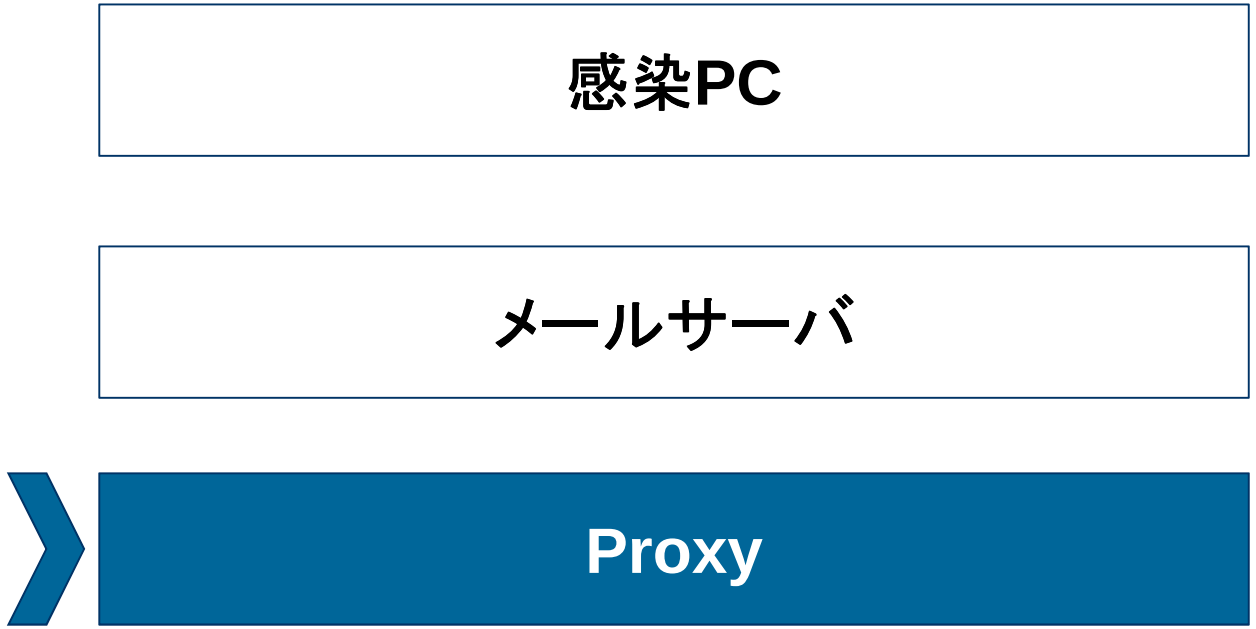
```
Sep  5 17:12:23 dmz_ns postfix/smtpd[6540]: connect from unknown[192.168.0.210]
Sep  5 17:12:23 dmz_ns postfix/smtpd[6540]: 18E2CF0088: client=unknown[192.168.0.210]
Sep  5 17:12:23 dmz_ns postfix/cleanup[6544]: 18E2CF0088: message-id=<20120905081151.99884F
                00A2@mail.example.com>
Sep  5 17:12:23 dmz_ns postfix/qmgr[2065]: 18E2CF0088: from=<yokokawa@vahoo.co.jp>, size=663
                30, nrcpt=3 (queue active)
Sep  5 17:12:23 dmz_ns postfix/smtpd[6540]: disconnect from unknown[192.168.0.210]
Sep  5 17:12:23 dmz_ns postfix/local[6545]: 18E2CF0088: to=<user01@localdomain.invalid>, relay=
                local, delay=0.28, delays=0.1/0.04/0/0.13, dsn=2.0.0, status=sent (delivered to mailbox)
Sep  5 17:12:23 dmz_ns postfix/local[6546]: 18E2CF0088: to=<user02@localdomain.invalid>, relay=
                local, delay=0.28, delays=0.1/0.06/0/0.12, dsn=2.0.0, status=sent (delivered to mailbox)
Sep  5 17:12:23 dmz_ns postfix/local[6547]: 18E2CF0088: to=<user03@localdomain.invalid>, relay=
                local, delay=0.28, delays=0.1/0.07/0/0.1, dsn=2.0.0, status=sent (delivered to mailbox)
Sep  5 17:12:23 dmz_ns postfix/qmgr[2065]: 18E2CF0088: removed
```

[実習01] メール調査

- 「Mail_User01.eml」は，社員（user01）が受信した不審メールのメールソースです。
- 「maillog.txt」は，不審メール受信時の自社メールサーバのログです。
- これらのエビデンスを解析してください。

Mission01 不審メール送信元MTAの特定

Mission02 社内の不審メール受信者の特定


感染PC
メールサーバ
Proxy

プロキシサーバにおけるマルウェアの通信の痕跡

- **次の事例におけるプロキシログを例示します。**
  ①PDFファイルの脆弱性攻撃コードが，マルウェア「Poison Ivy」をダウンロードし，PCに感染させた。
  ②その後，攻撃者は，Poison Ivyのバックドア機能を通じて，機密情報を窃取した。

◆PDFファイルからPoison Ivy感染時のProxyログのサンプル

11/Mar/2012:07:59:24 +0900.803 665 172.16.0.132 TCP_MISS/200 7614 GET http://192.168.0.50/malware.exe - DIRECT/192.168.0.50 application/x-msdos-program "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)“

脆弱性攻撃コードが，不審なプログラムをダウンロードしたログ。この例では，ファイル名を見ただけで不審と判断できるが，実際の攻撃では，拡張子はJPGなどが用いられるため，ログだけで不審なプログラムを識別することは困難である。

11/Mar/2012:08:04:12 +0900.609 128696 172.16.0.132 TCP_MISS/200 1069272 CONNECT 192.168.0.200:443 - DIRECT/192.168.0.200 - "-“

CONNECTメソッドによる通信は，セッション切断時にログに記録される。（接続時間 [ms] ）

通信サイズ[byte]

（参考）Squidログ

- オープンソースのProxyであるSquidのログを紹介します。

◆Squidのログ（/var/log/squid/access.log）の例

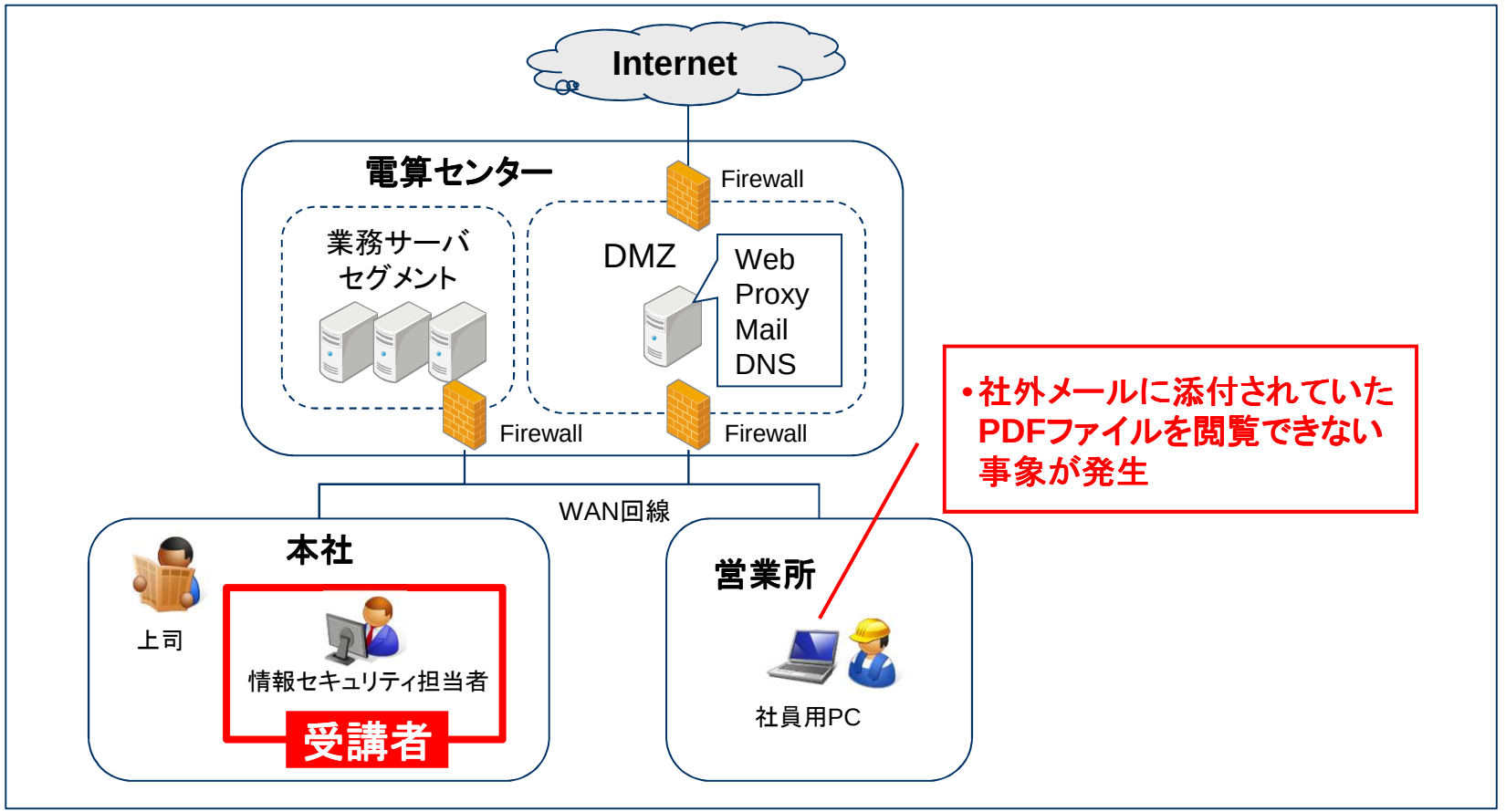
Date			転送時間(ms)	Src IP	Status	Size (byte)	URL		UN	Dst IP	MIME	User Agent
23/Aug/2012	11:13:35	+0900	181	192.168.0.10	TCP_MISS/200	112009	GET	http://www.yahoo.co.jp/	-	DIRECT/124.83.179.227	text/html	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; InfoPath.1; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
23/Aug/2012	11:13:35	+0900	162	192.168.0.10	TCP_MISS/200	101735	GET	http://www.yahoo.co.jp/javascript/fp_base_bd_ga_5.0.33.js	-	DIRECT/124.83.179.227	application/javascript	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; InfoPath.1; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
23/Aug/2012	11:13:35	+0900	54	192.168.0.10	TCP_MISS/200	2957	GET	http://k.yimg.jp/images/top/sp2/clr/1/clr-120807.css	-	DIRECT/124.83.226.246	text/css	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; InfoPath.1; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)

squid.conf: logformat squid %{%d/%b/%Y %H:%M:%S %z}tl %6tr %>a %Ss/%03>Hs %<st %rm %ru %un %Sh/%<A %mt "%{User-Agent}>h"

第2章 想定シナリオの対応

本日の想定シナリオ

- ある日，営業所の社員から，社外メールに添付されていたPDFファイルを閲覧できないとの電話連絡がありました。
- 状況を確認したところ，PCの挙動が怪しいようです。
  さて，どうしますか？



PC利用者からの電話連絡の内容

電話連絡の内容

昨晩の夜勤中（2012年9月4日 2:15頃），社外から苦情のメールが届きました。添付されていたPDFファイルを閲覧しようとすると，Adobe Readerが異常終了してしまい，閲覧できませんでした。パソコンに詳しい担当者にも確認しましたが，原因は分かりませんでした。

また，いつのまにか，デスクトップに身に覚えのないファイル「iso88591」が作成されていました。エラーログでしょうか？　この他には，特に不審な挙動はありません。

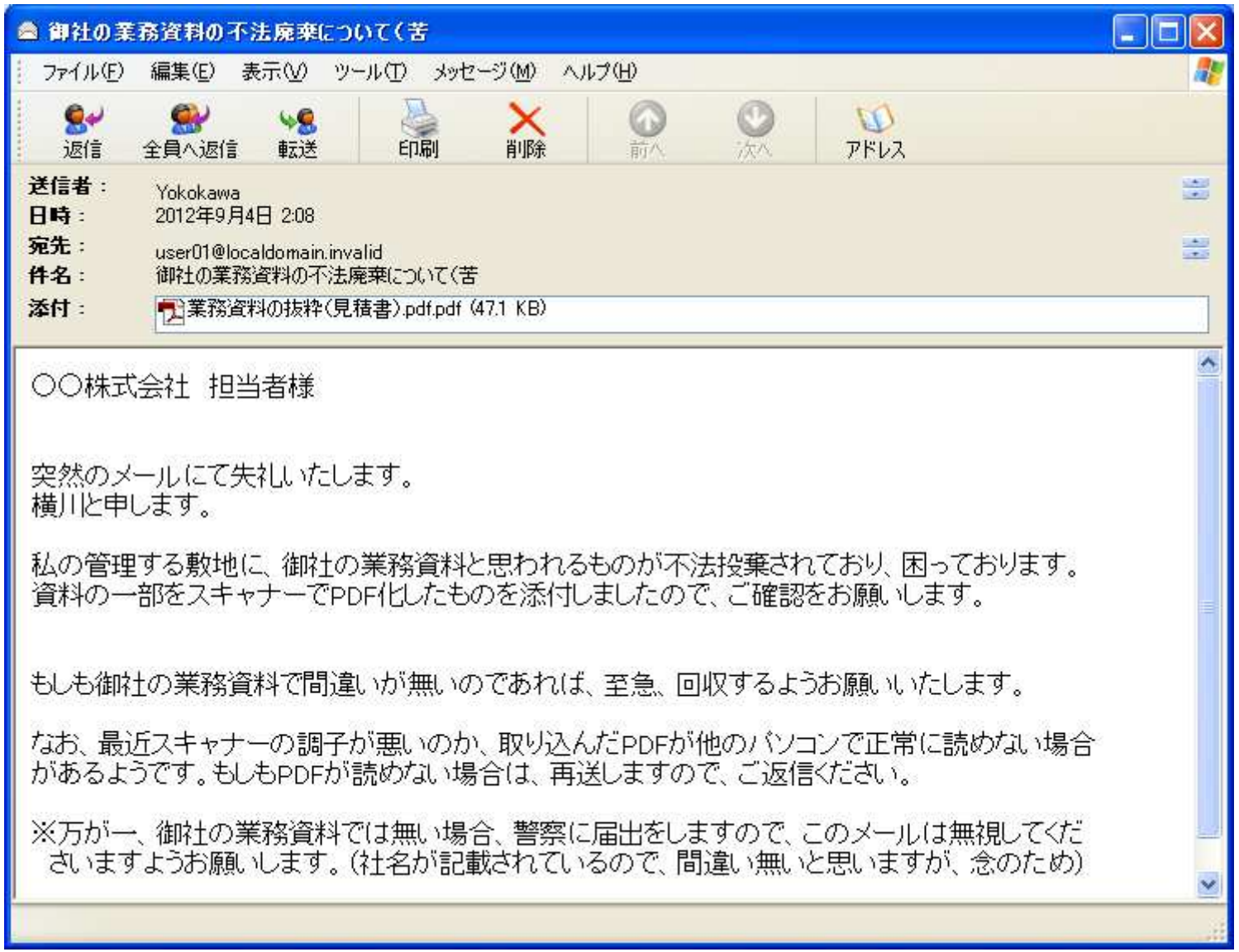
苦情には速やかに対応する必要があるため，至急，PDFファイルを閲覧したいです。

なお，苦情メールの差出人に身に覚えはなく，どうして私のメールアドレスを知っているのか分かりません。（過去に名刺を渡したことがあるのかもしれません・・・）

社員のメールアドレス：　user01@localdomain.invalid

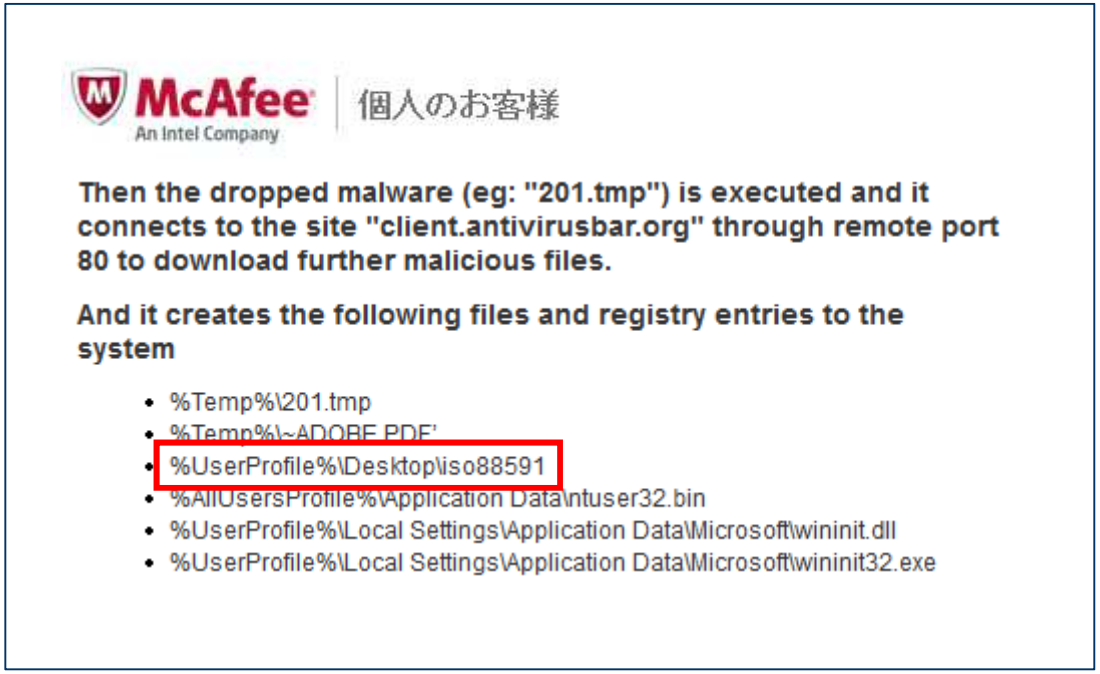
*1 実習環境準備の都合により，WindowsXP SP3における感染事案とします。

お客様からの苦情メール



「iso88591」

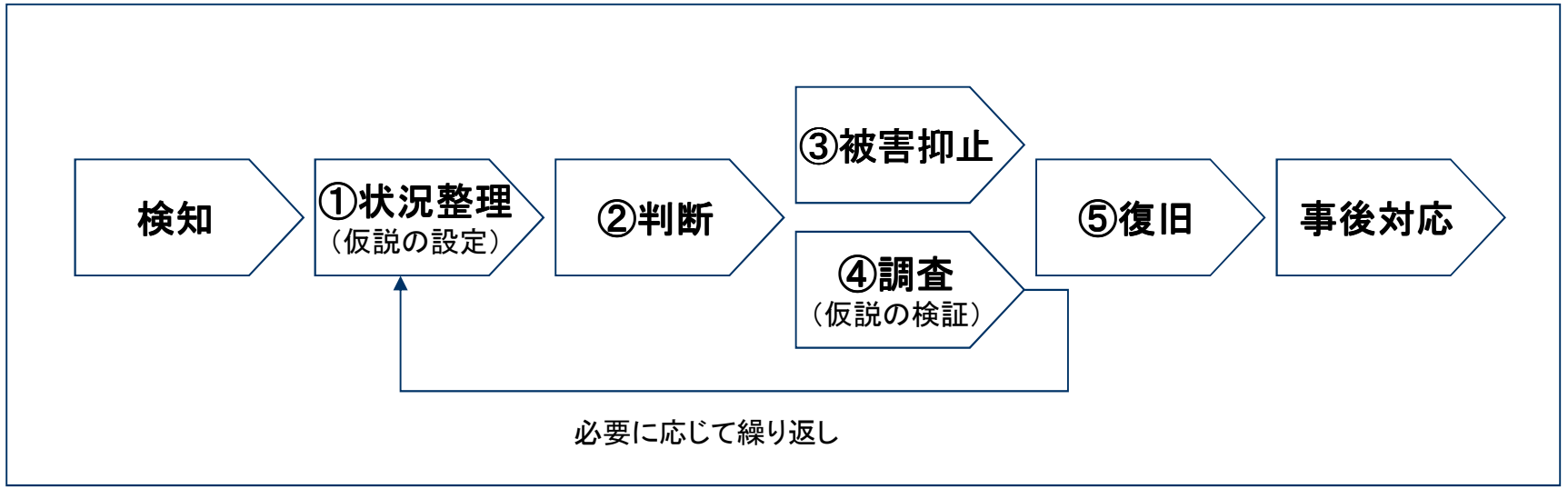
- Googleにて，「desktop¥iso88591 pdf exploit」で検索したところ，本事案のメールに添付されていたPDFファイルは，脆弱性攻撃コードを含んでいる可能性があることが判明しました。
- ただし，まだ本事案が攻撃であるとの断定はできていないため，まずはメールソース，および現地で取得した各種エビデンスを解析することとします。



インシデントレスポンスの基本手順

- インシデントレスポンスでは，状況整理フェーズで事実と推測を整理し，発生している事象とリスクの「仮説」を設定します。
- しかし，対応の初期段階では，情報の不足や輻輳が発生しやすく，仮説には，推測が含まれることが多いため，必要に応じて，フォレンジック技術や，マルウェア解析技術を活用し，仮説の検証を行います。

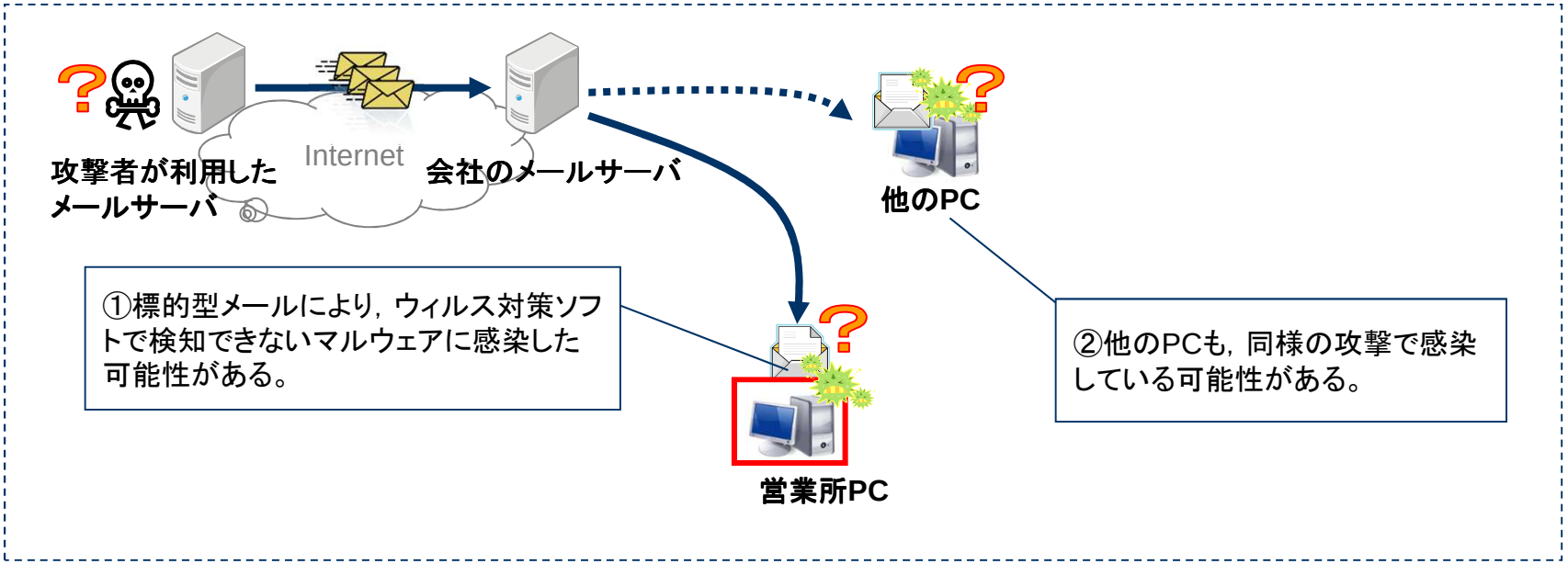
◆ インシデントレスポンスの基本手順



①状況整理（仮説の設定）

- 現時点では断定はできませんが，標的型メール攻撃により，マルウェアに感染した可能性を念頭に置き，慎重に確認作業を進めます。

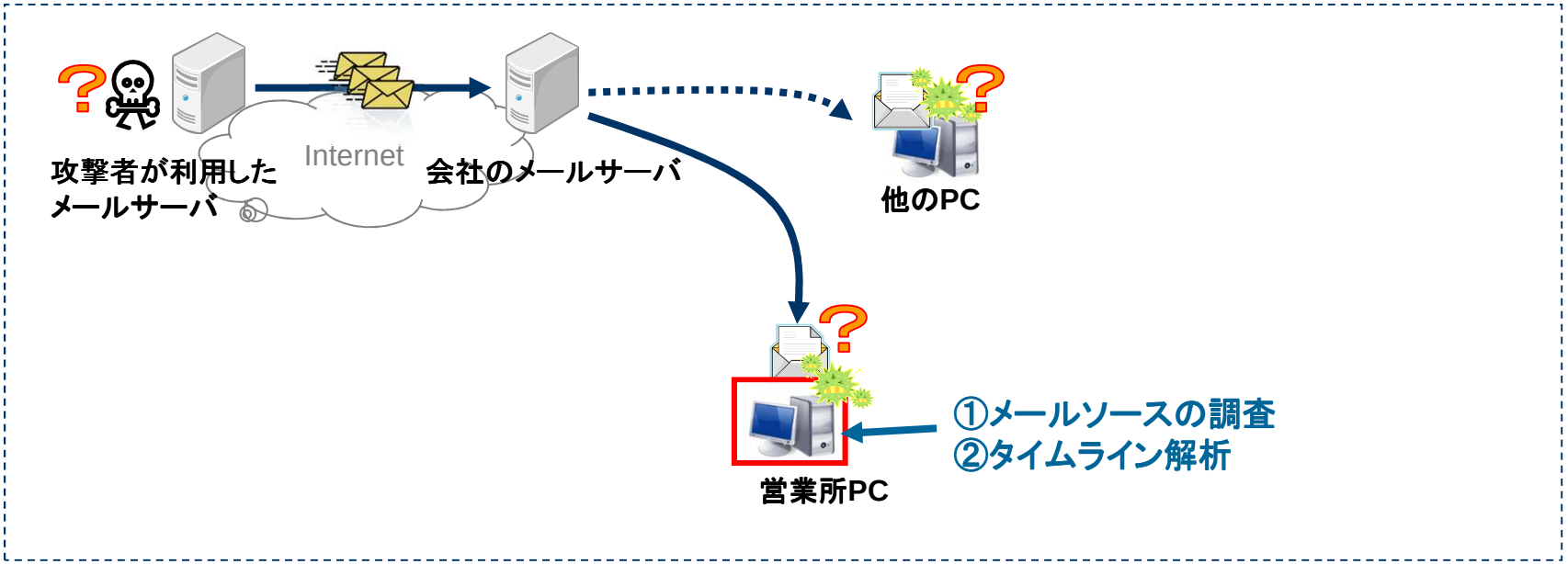
◆本事案の仮説 （最悪のシナリオの想定）



②判断

- 本事案のメールソースおよび添付ファイル（PDFファイル）を確認します。
- また，営業所PCをタイムライン解析し，不審なプログラムの起動有無を調査します
  - 現地社員に，$MFTおよびレジストリを取得するバッチファイルを起動してもらい，エビデンスを社内共用ファイルサーバに保存してもらうこととします。

◆状況整理図



③被害抑止（1）

- 現時点では情報が不足しており，被害抑止のために実施できることはありません。

④調査（1）感染PCの解析

- **メールヘッダーなどに不審な点がないか確認します。**
- **ファイルシステム，レジストリのタイムライン解析を行い，メール添付ファイルの閲覧日時に不審な点がないか確認します。**
  - なお，本シナリオはゼロデイ攻撃を想定しているため，PDF文書からは不審な点を発見できなかったものとします。

◆主な調査ポイント

項目	説明
メールヘッダー	• 送信元MTAのホスト名，IPアドレスは正規のものか • 差出人のメールアドレスなどに不審な点はないか （例：官庁を名乗っているのに，フリーメールアドレスを利用） • キューID（メールログの調査で利用）
タイムライン解析	• メール添付ファイルの閲覧直後に，不審なプログラムが起動していないか。 • 不審なプログラムの起動直後に更新されたレジストリはないか • 不審な実行形式ファイルなどが作成されていないか

[実習02] 感染PCの解析

- 不審メールのメールソース，および営業所PCから取得したエビデンスを解析し，不審な点がないか確認してください。
  - 本実習は，実習手順の説明資料はありません。これまでの学習内容を振り返り，取り組んでください。

Mission01 メールヘッダーの確認

Mission02 タイムライン解析による感染有無の確認

③被害抑止(2)

- **本事案の不審メールは，攻撃メールであると判断できたことから，被害抑止のため，次の対応を実施します。**

◆被害抑止対応

項目	説明
感染PCの隔離	• 感染PCをネットワークから隔離する。 （電源OFF，またはLANケーブル取り外し）
同様の攻撃メールの遮断	• 攻撃メールの特徴（差出人メールアドレス，送信元MTAのIPアドレスなど）の情報をもとに，MTAで攻撃メール遮断設定を実施する。
攻撃メール受信者の把握と状況確認	• メールサーバログを調査し，攻撃メールを受信した利用者のPCを調査する。 （遠隔地の場合，初動として電話連絡による聞き取り調査） • 感染が疑われる場合は，ネットワークから隔離したうえで調査を実施する。 • なお，クライアントPCの操作ログを取得している場合は，操作ログから，マルウェアが実行されたPCの有無を調査する。
ウィルス対策ソフトのパターンファイル手配	• マルウェアの検体をウィルス対策ソフト開発元に送付し，パターンファイルの作成を依頼する。

④調査（2）メールサーバログ

- 攻撃メールの特徴をもとに，メールサーバログを調査し，攻撃メールを受信した利用者を特定します。
  - 検索キーワードの例： キューID，差出人メールアドレス，送信元MTAのIPアドレス

[実習03] メールサーバログの調査

- 本事案の攻撃メールの特徴をもとに，攻撃メールを受信した利用者を特定します。
（user01の他に，攻撃メールを受信したメールアカウントが存在するか調査する）
  - 本実習は，実習手順の説明資料はありません。これまでの学習内容を振り返り，取り組んでください。

Mission01 メールログの調査

④調査（3）Proxyログ

- **感染PCのIPアドレスをキーとして，攻撃メールの添付ファイルを開いた以降のProxyログを検索し，不審な通信の有無を確認します。**

［不審な通信の例］

- 感染PCが，攻撃メールの添付ファイルを開いた直後に接続しているWEBサイト
- 感染PCで利用されているブラウザと異なるユーザーエージェント名での通信
  （マルウェアの通信の可能性がある）
- ランダムなURLのWEBサイト，ロシア（.ru），中国（.cn）などのWEBサイト
- 不明なサイトに対する長時間にわたるConnectメソッドによる接続
  （Connectメソッドは，HTTPS通信でも利用されている）

[実習04] Proxyログの調査

- Proxyログを調査し，感染PCによる不審なインターネット通信の有無を確認します。
  - 本実習は，実習手順の説明資料はありません。これまでの学習内容を振り返り，取り組んでください。

Mission01 感染PCの不審インターネット通信の調査

⑤復旧/事後対応

- **感染したPCは，データをバックアップし，クリーンインストールすることを推奨します。**
  - インターネットから他のマルウェアをダウンロードされた可能性があるため，感染したPCの安全性の確保には大きな労力がかかります。

- **再発防止対策は，セキュリティパッチ適用などの技術的な対策だけでなく，利用者に対する注意喚起の実施など，人的対策も検討します。**

まとめ

まとめ

- 適切なインシデント対応とするためには，状況を正しく把握することが重要です。
- マルウェアの感染メカニズム，ならびに感染時に残される痕跡を理解することで，状況を正しく把握することができます。

- 攻撃メールの内容などから，自社に対する標的型攻撃であると判断した場合は，さまざまな手法で攻撃を受けていた（または今後も攻撃が継続する）可能性があるため，必要に応じて外部専門企業の協力を得て，対応方針を判断します。