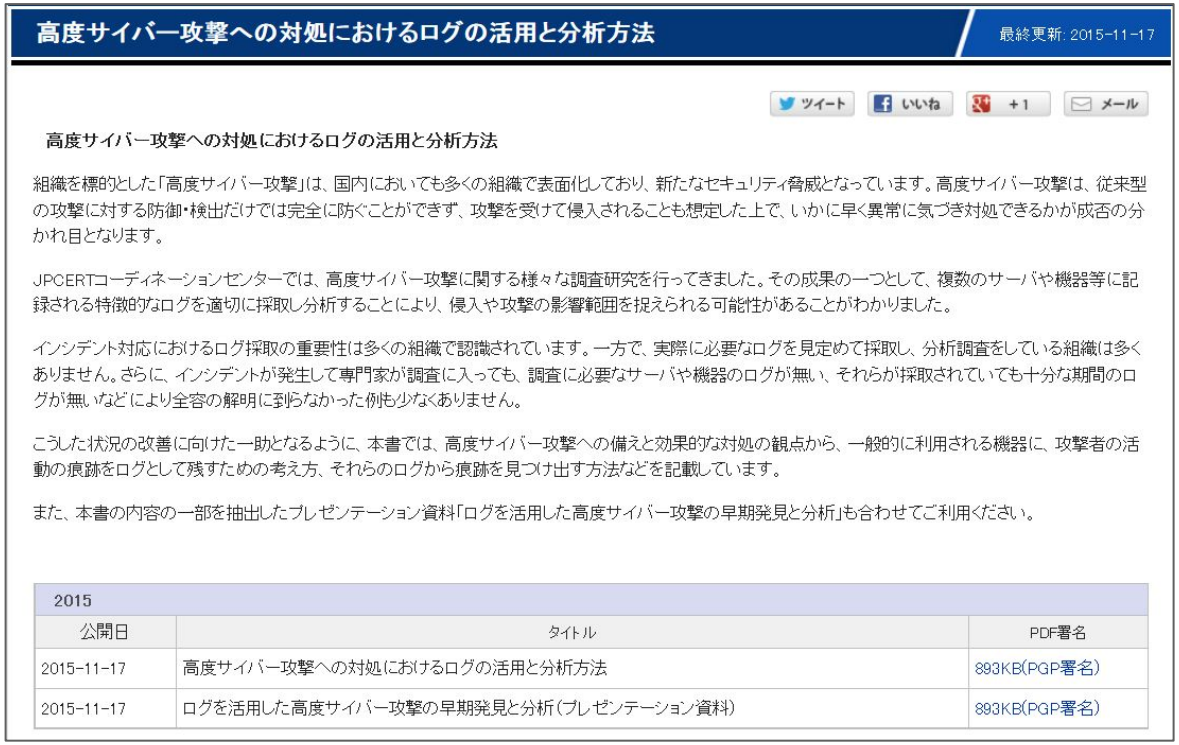
ログを活用した高度サイバー攻撃の早期発見と分析

JPCERT/CC　早期警戒グループ
技術アドバイザー
満永　拓邦

本資料の位置づけ

- 本資料は、JPCERT/CCにて作成したレポート「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」の一部を講演で紹介した際に利用したものです。本資料の「３．攻撃の痕跡が残る機器」「４．痕跡が残る機器の検知例」についての詳細な内容はレポートを参照ください。



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

最終更新: 2015-11-17

ツイート　いいね　+1　メール

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

組織を標的とした「高度サイバー攻撃」は、国内においても多くの組織で表面化しており、新たなセキュリティ脅威となっています。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、攻撃を受けて侵入されることも想定した上で、いかに早く異常に気づき対処できるかが成否の分かれ目となります。

JPCERTコーディネーションセンターでは、高度サイバー攻撃に関する様々な調査研究を行ってきました。その成果の一つとして、複数のサーバや機器等に記録される特徴的なログを適切に採取し分析することにより、侵入や攻撃の影響範囲を捉えられる可能性があることがわかりました。

インシデント対応におけるログ採取の重要性は多くの組織で認識されています。一方で、実際に必要なログを見定めて採取し、分析調査をしている組織は多くありません。さらに、インシデントが発生して専門家が調査に入っても、調査に必要なサーバや機器のログが無い、それらが採取されていても十分な期間のログが無いなどにより全容の解明に到らなかった例も少なくありません。

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、一般的に利用される機器に、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方法などを記載しています。

また、本書の内容の一部を抽出したプレゼンテーション資料「ログを活用した高度サイバー攻撃の早期発見と分析」も合わせてご利用ください。

2015

公開日	タイトル	PDF署名
2015-11-17	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	893KB(PGP署名)
2015-11-17	ログを活用した高度サイバー攻撃の早期発見と分析（プレゼンテーション資料）	893KB(PGP署名)

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
http://jpcert.or.jp/research/apt-loganalyis.html

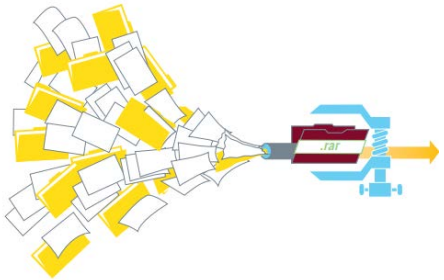
1．背景と概要

背景

- 最近、特定の組織を標的とする高度サイバー攻撃がメディアを騒がせている
- 攻撃者は長期間に渡り、組織内に潜伏し、巧みに情報を窃取し続ける
- 攻撃は巧妙化しており、境界防御のみで高度サイバー攻撃を完全に防ぐことは難しい
- 検知が遅れると被害は拡大の一途をたどるため、早期に検知し攻撃の流れを断つことが重要である

高度サイバー攻撃による攻撃の特徴

- 米セキュリティ企業 Mandiant 社のレポートによると攻撃の特徴は以下の通り、
  - 組織的かつ体系的な攻撃により、20業種141組織から数百テラバイトの情報を窃取してきた
  - 侵入を発見するきっかけは、 **94%が外部からの通知**による
  - 組織内に侵入されていた**平均期間は 356 日**であり、期間が長い場合では1764日であった
  - 組織内ネットワークに一度侵入を許すと、数カ月から数年の期間に渡って、組織内に保管されている技術文書、財務資料、経営計画、契約書など様々に渡るカテゴリーの情報、ならびにEメールアドレスなどの外部の連絡先を詐取する



(参考)
Mandiant Intelligence Center Report
http://intelreport.mandiant.com/

インシデント対応プロセス

マネージメントの積極的関与

外部との情報連携

外部からの情報で
インシデントが発覚する
ケースが多い

インディケータ

ここが
最も重要

一般的に
ここが起点になる

外部と共有

準備 | 検知・分析 | 封じ込め | 根絶 | 修復 | 教訓

平常時の備え

有事における対応

原因追及、全容把握、フィードバックのために多種のデータを利用

- ✓通信ログ（ファイアウオール、プロキシ等: 内部⇒外部や内部⇒内部）
- ✓証跡データ（IT資産管理システム等）
- ✓IT資産管理情報など

侵入後の検知と事前対策

- 組織への侵入を防ぐ事には限界がある
  - メール経由以外でも、Webサイト閲覧などにより内部に侵入するケース
  - 未修正の脆弱性を狙う攻撃の発生
  - 従業員のセキュリティ意識の不足、人的エラーの発生
  - セキュリティ対策ソフトによる検知、不審な通信の検知の限界

本日の内容

侵入された**後**の対策も重要
- 各機器でログは十分に取れているか？
- 侵入後に検知できる仕組みがあるか？
- 重要な情報資産は切り離されているか？
- インシデント発生時の対応手順は明確か？

高度サイバー攻撃への対策の一つとして

- 組織でよく利用される機器のログ（あるいは簡単な設定変更で取得できるログ）を有効に活用し、高度サイバー攻撃を早期に発見する

- 早期発見のポイント
  - ログの適切な保管（後述のログ保管の推奨期間を参照）
  - ログの定期的な確認
  - 見るべきログの把握（痕跡の見つけ方の例）

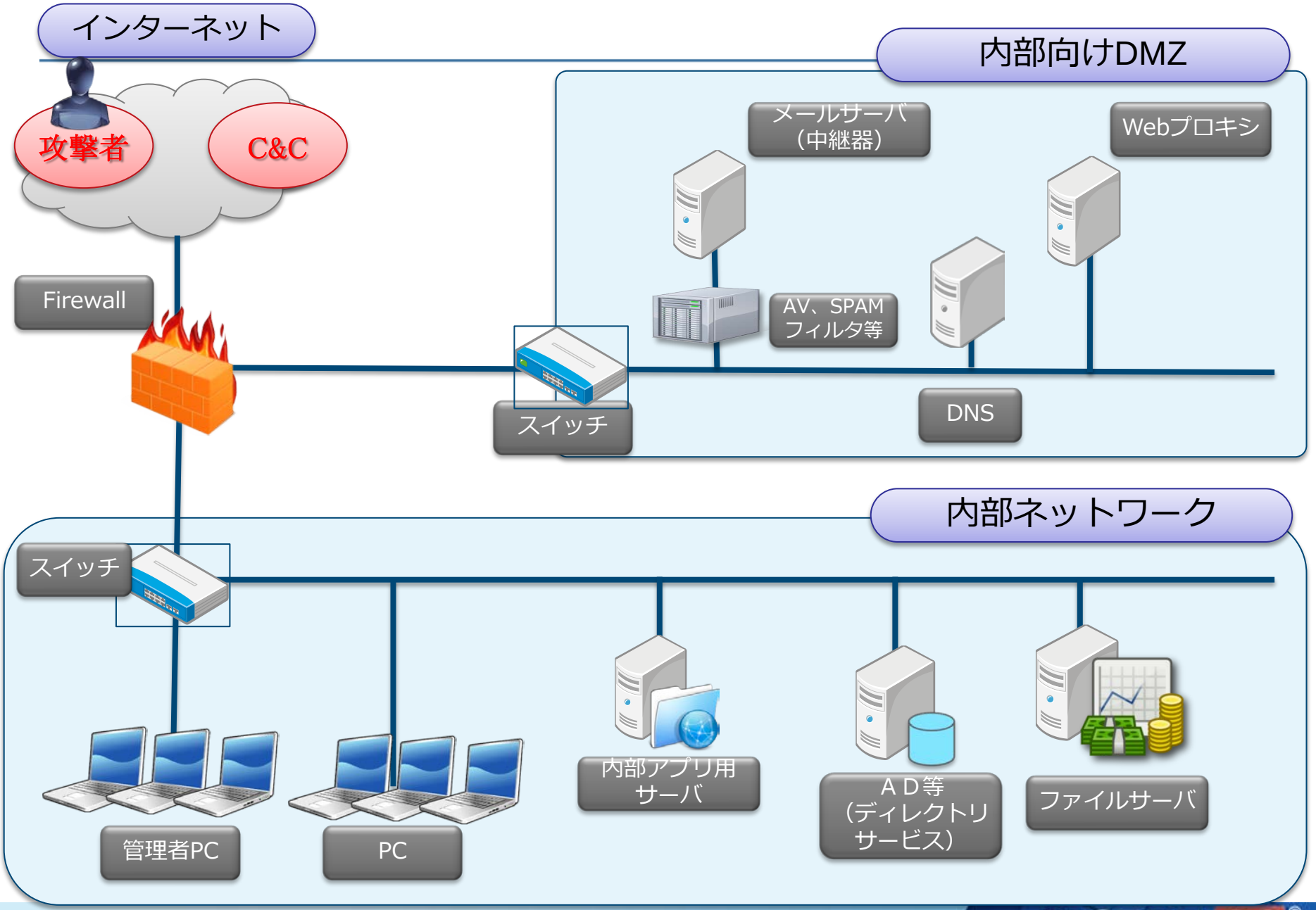
※注意事項
・紹介する構成は一例であり、自組織のネットワーク構成と照らし合わせて読み替えつつ、自組織のネットワーク構成や設定の見直しに活用ください。
・前提としてセキュリティを配慮した堅牢なネットワークの構築も必要です。

2．高度サイバー攻撃の流れ

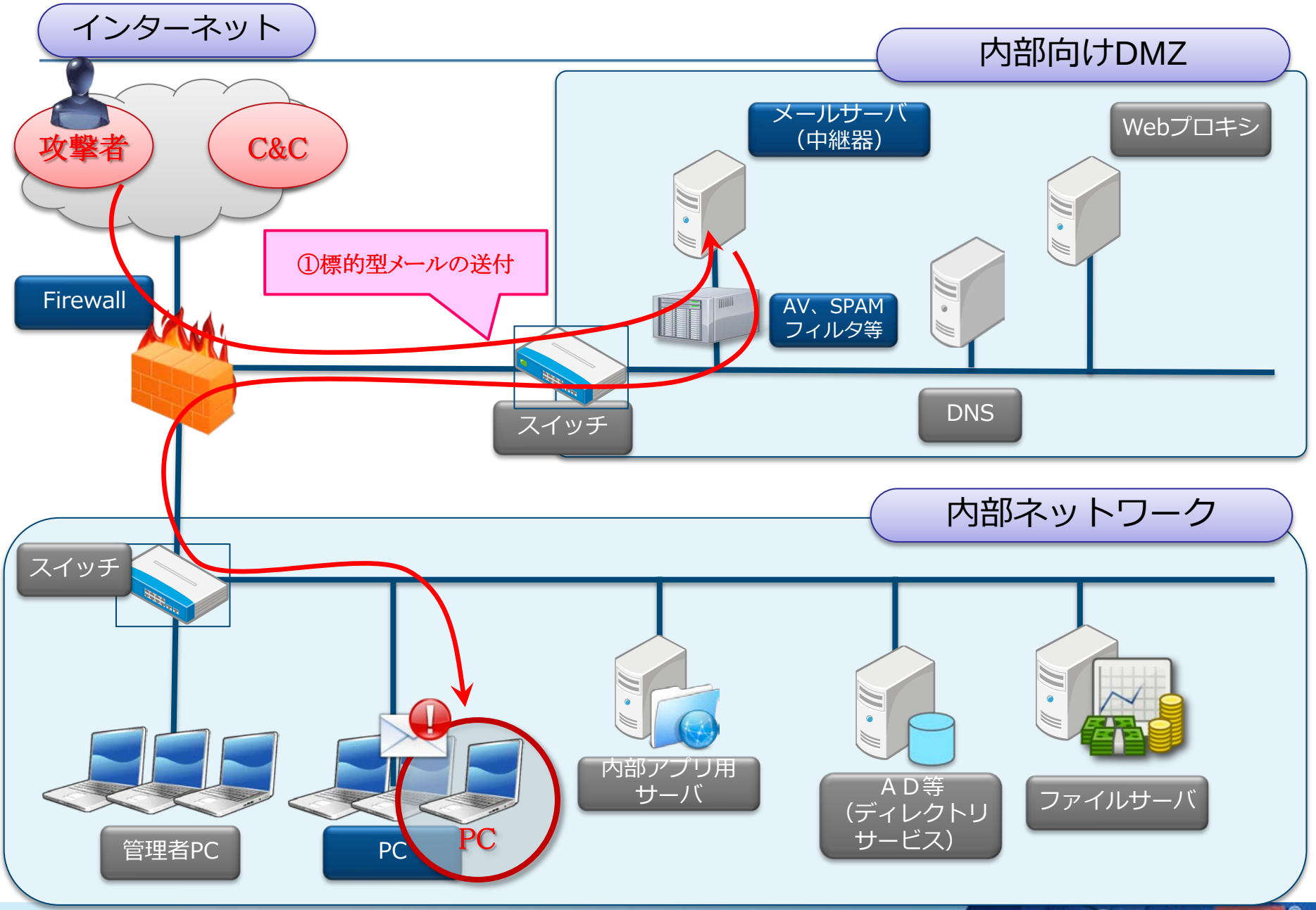
高度サイバー攻撃におけるキルチェーンモデル

	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の調査し、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、ユーザにクリックさせるように誘導する
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(PC)がマルウエアに感染する
6	C&C	・マルウエアによりC&Cサーバと通信させ、感染PC を遠隔操作し、追加のマルウエアやツールなどをダウンロードさせることで、感染を拡大する、あるいは内部情報を探索する
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

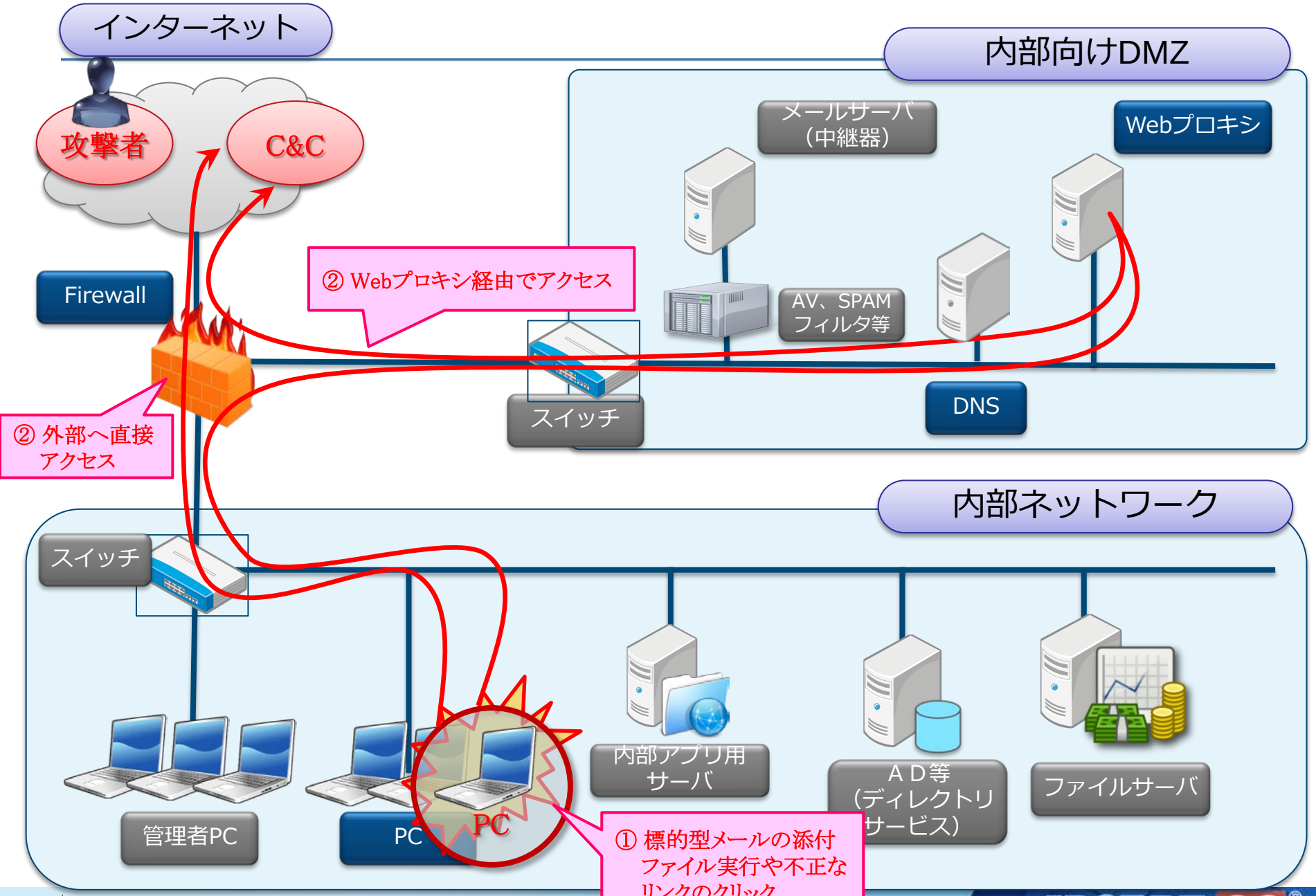
第1段階 偵察、第2段階 武器化



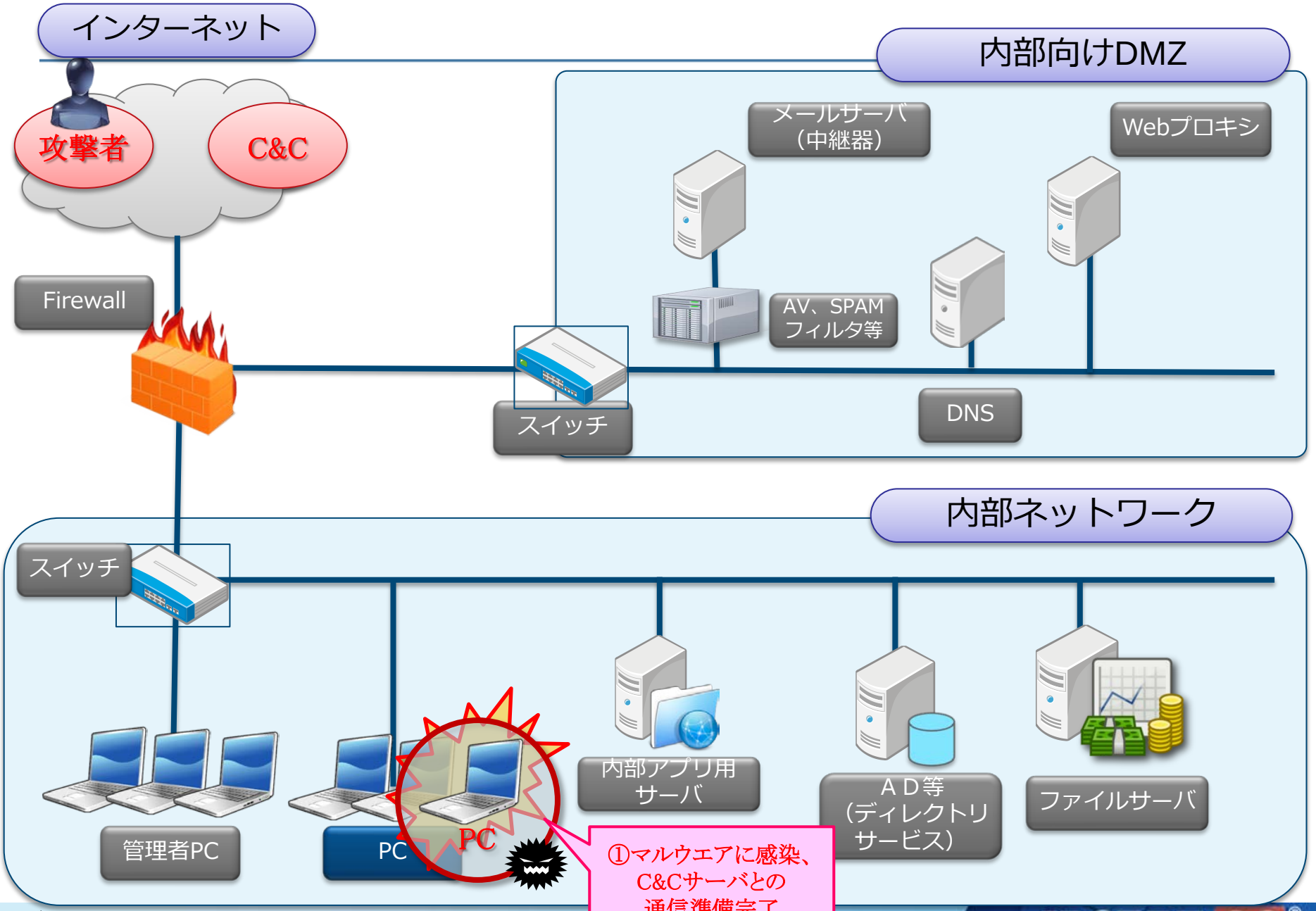
第3段階 デリバリ



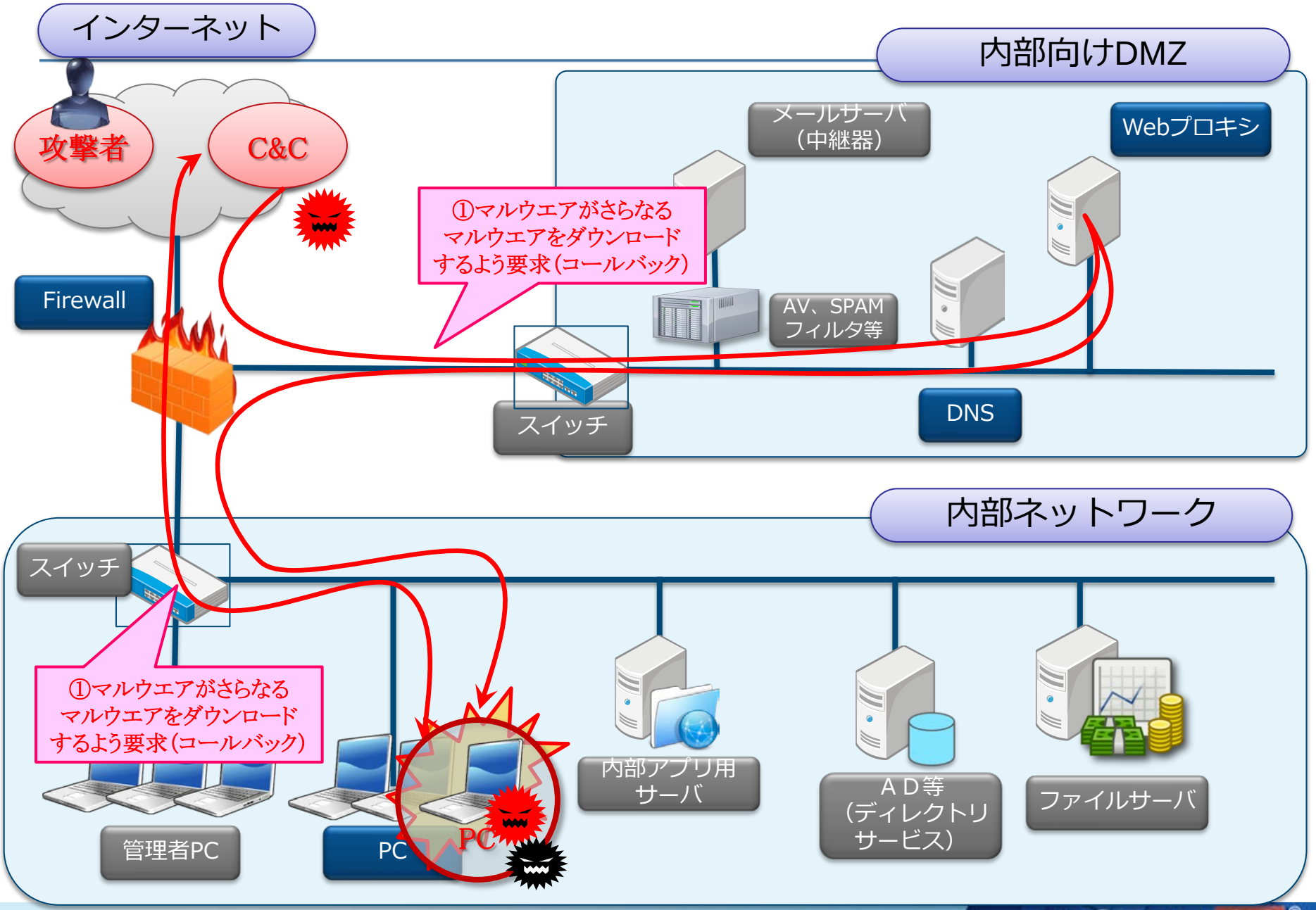
第4段階 エクスプロイト



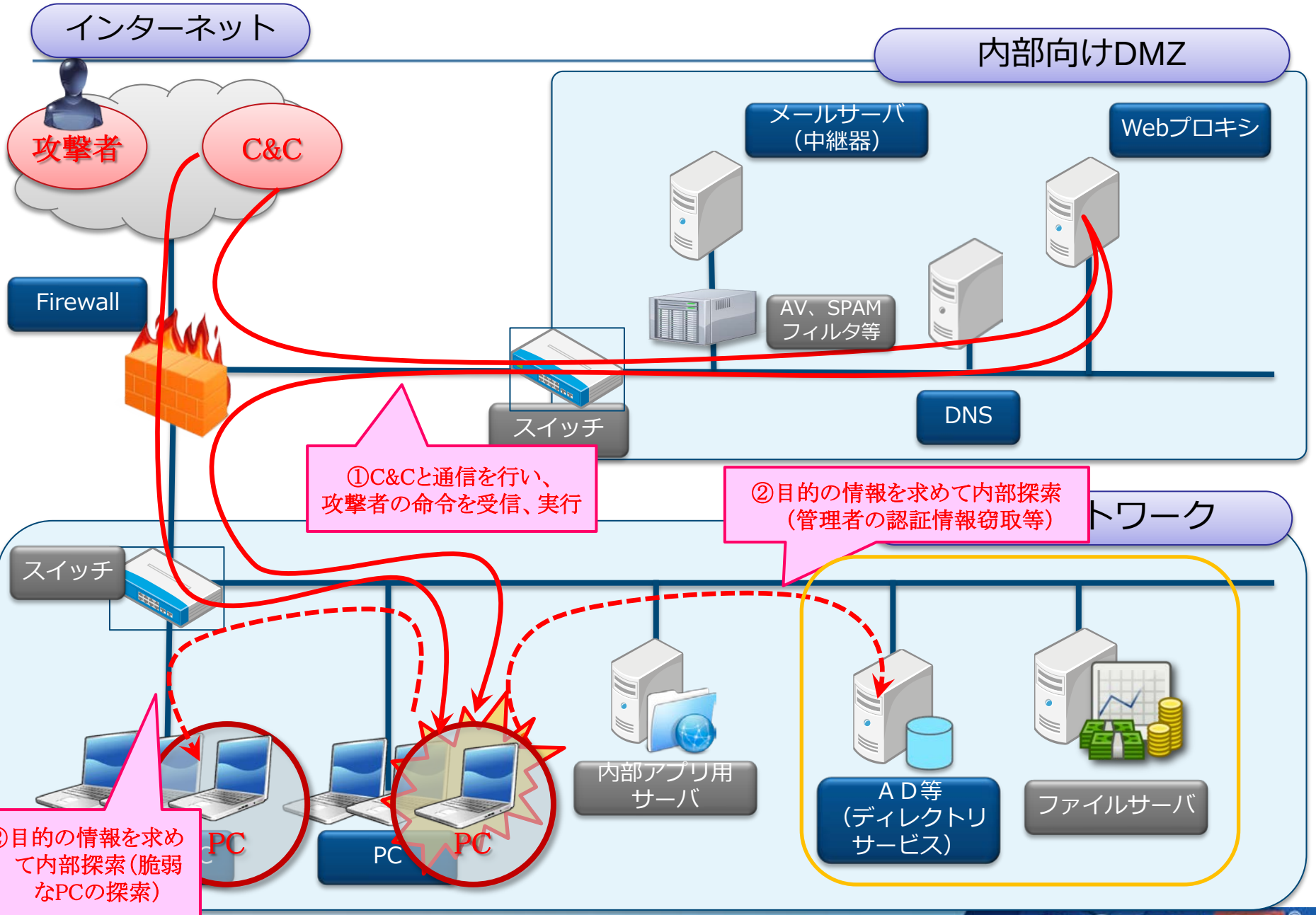
第5段階 インストール



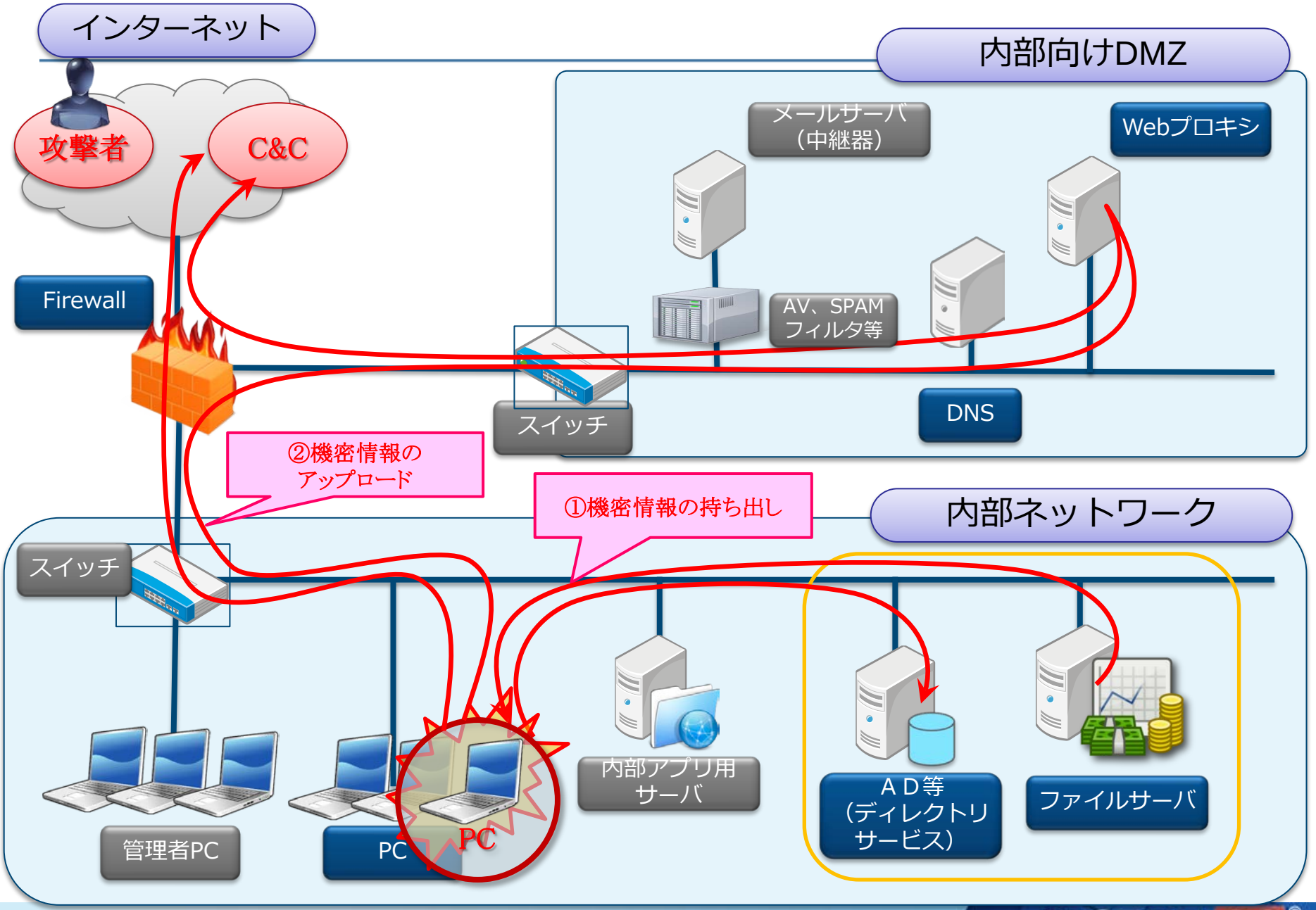
第6段階 C&C(1)



第6段階 C&C(2)



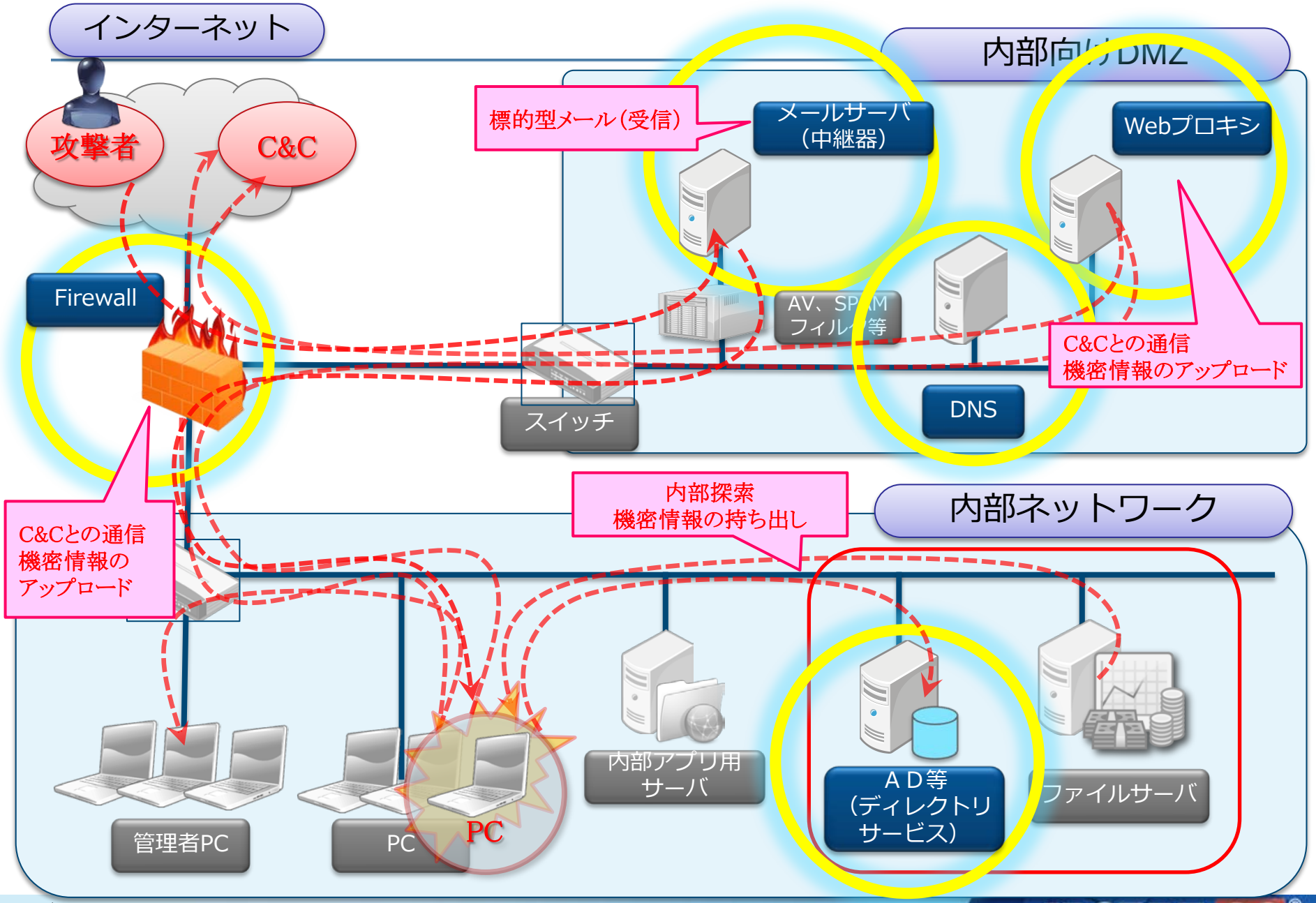
第7段階　目的の実行



３．攻撃の痕跡が残る機器

攻撃の痕跡が残る機器

※「PC」における攻撃の痕跡については別途資料を公開予定



攻撃段階および攻撃内容とログの関係

攻撃段階		ログで検知可能な攻撃内容	ログ取得対象機器
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	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	メールサーバ Web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（Webプロキシサーバを介さない外部への通信）	Firewall DNSサーバ
		コールバック（HTTP, HTTPS等のプロトコルによる外部への通信）	Web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（Webプロキシサーバを介さない外部への通信）	Firewall DNSサーバ
		コールバック（HTTP, HTTPS等のプロトコルによる外部への通信）	Web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）	Firewall
		ファイルサーバなどへのアクセスや権限の奪取	ADログ Firewall
7	目的の実行	コールバック（Webプロキシサーバを介さない外部への通信）	Firewall DNSサーバ
		コールバック（HTTP, HTTPS等のプロトコルによる外部への通信）	Webプロキシサーバ DNSサーバ
		機密情報持ち出し (メールサーバ経由)	メールサーバ DNSサーバ

ログを分析する上でのポイント

- 定期的な分析
  - 各機器のログにどのような情報があり、何が出力されるのかを事前に把握し、定常的な状態を知る
  - 定常的な状態と異なるログが出力されていないかを確認する
    - 就業時間外に外部への通信が発生していないか
    - 大量の通信が発生していないか
    - 許可されていない通信により、エラーが発生していないか（Firewallのdropログなど）
- 外部からの情報を起点とする分析
  - 提供された情報をもとに一致するログが存在しないかを確認する
    - メールヘッダ、差出人情報、添付ファイル名
    - 通信先のURL、IPアドレス、ドメイン
    - etc

４．痕跡が残る機器の検知例

メールサーバにおけるポイント

代表的なログ項目

ログ項目	ログ項目の内容	標準設定での出力
From(詳細):	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	×

攻撃とそれを発見するための手法の例

	攻撃行為	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、油断させて開かせる	受信メールの送信者情報の不自然な設定 例：エンベロープとメールヘッダのアドレスが異なるものを抽出
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	実行ファイル形式が添付されたメール 例：“Content-Type”、”name” が含まれる箇所がファイル名を示す。ファイル名の拡張子が実行形式であるものを抽出

メールサーバのログ (Postfix)

- Fromフィールドの表示名偽装のログの例

```
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]>
```

- 実行ファイル添付のログの例

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

日本語のファイル名がBase64エンコードされた状態で、ログに出力される。デコードすると「【マル秘】顧客情報！.exe」と表示

（参考）Postfixの標準設定で出力されないログ

- postfix において、次の情報をログ出力するためには設定変更が必要です
  - メールヘッダのFromフィールドの記録

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

  - 添付ファイル名の記録

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

ファイアウォールにおけるポイント

代表的なログ項目

ログ項目	ログ項目の内容	標準設定での出力
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	○
Dst	送信先アドレス	○
dst_port	送信先ポート	○

攻撃とそれを発見するための手法の例

	攻撃行為	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がダウンロードサイトに、通信を試みる	Webプロキシを経由せずに、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 例：組織内から組織外へ通信で、かつ許可されていない通信を抽出
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	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 例：組織内から組織内へ通信で、かつ許可されていない通信を抽出

Firewallのログの例 (Juniper SSG)

- 組織内から組織外への不正な通信のログの例

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

- 異なるセグメントに収容された PC 間の不正な通信のログの例

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

Webプロキシサーバにおけるポイント(1/2)

代表的なログ項目

ログ項目	ログ項目の内容	標準設定での出力
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	○

攻撃とそれを発見するための手法の例

	攻撃行為	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サーバやダウンロードサイトへの通信を試みる	高度サイバー攻撃に関連する情報（IPアドレスやドメインなど）で検索
CONNECTメソッドで80、443以外のポートへ通信	HTTPやHTTPS通信の偽装を行い、組織外との通信を試みる	80、443番ポート以外のCONNECTメソッドの通信を抽出

Webプロキシサーバのログの例 (squid)

- 不審な送信先への通信のログの例

```
1424221299.090 452 192.168.xxx.xxx TCP_MISS/200 74769 GET
http://apt.example.com/xxx/xxx/apt.zip - DEFAULT_PARENT/113.xxx.xxx.xxx
application/ zip-compressed
```

- CONNECTメソッドで80、443以外のポートへ通信のログの例

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

Webプロキシサーバにおけるポイント(2/2)

- 攻撃とそれを発見するための手法の例

	攻撃行為	攻撃の痕跡を見つける手掛かり
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サーバやダウンロードサイトへの通信を試みる	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
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	業務利用しないURLを日ごとに集計。不自然なアクセスが続いているものを抽出
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	業務時間外の時間帯でシステムメンテナンス利用を除いたものを抽出。不自然なアクセスがないか確認
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	同一の送信先に対するPOSTメソッド、それに続くCONNECTメソッドを抽出し、データ量の合計値が異常に大きなものを確認

Webプロキシサーバのログの例 (squid)

- 標準利用以外のUser Agentによる通信

```
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
```

- 定期的に発生するHTTP通信のログの例

```
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
```

- 業務時間外に発生するHTTP通信

```
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
```

（参考）Squidの標準設定で出力されないログ

- Squidにおいて、次の情報をログ出力するためには設定変更が必要
  - UserAgentの情報の記録

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

DNS(キャッシュ)サーバにおけるポイント

- 代表的なログ項目

ログ項目	ログ項目の内容	標準設定での出力
クエリログ	PCなどのクライアントがDNSサーバにホスト名の解決を行ったクエリ	×
Src	ホスト名の解決を行ったクエリが送られた送信元ホストのIP アドレス	×

- 攻撃とそれを発見するための手法の例

	攻撃行為	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サーバやダウンロードサイトへの通信を試みる	高度サイバー攻撃に関連する情報（URLやドメインなど）で検索

- ホスト名の解決を行ったクエリのログの例

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

（参考）BINDの標準設定で出力されないログ

- BIND9において、次の情報をログ出力するためには設定変更が必要

  ・PCなどのクライアントがDNSサーバにホスト名の解決を行ったクエリの記録

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"; };
};
```

認証サーバ (Active Directory)におけるポイント

代表的なログ項目

ログ項目	ログ項目の内容	標準設定での出力
セキュリティログ	資格認証、Kerberos認証、特殊なログオンの要求と結果	×

攻撃とそれを発見するための手法の例

	攻撃行為	攻撃の痕跡を見つける手掛かり
通常の認証要求では発生しないような認証イベント	マルウエアに感染した PC が感染拡大のため他のPCへのログオンを試みる	通常の認証要求とは異なる特殊な操作要求を確認
管理者アカウントに関連したイベントの調査	目的の情報を得るため、特権が必要な操作を試みる	管理者が通常使用するIPアドレスと異なるIPアドレスからの管理者権限要求など

認証サーバ (Active Directory)におけるポイント(詳細)

- 通常の認証要求では発生しないような認証イベント

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

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

認証サーバ (Active Directory)におけるポイント

- 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
    - 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
    - 特定のPCから異常に多くの認証要求イベントが存在、など

発見した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。

（参考）ADのログ出力設定

- AD サーバの監査ポリシーの設定で、次の項目を有効にする (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。
  - 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

5．インシデント対応体制

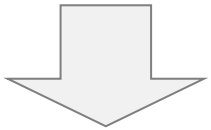
セキュリティに関する対応体制

- インシデント(*)発生時の対応体制
  - ユーザ部門、システム管理、営業、法務、広報などの関連部署間で情報の共有および対策の一元化
  - システム責任者、対応フローの明確化(ex. 誰がサーバを止めれるか？)
  - 外部組織からの通知窓口の設置

インシデント(*)・・IT システムの正常な運用または利用を阻害するウィルス感染、不正アクセス、情報漏えい、DoS 攻撃などの事案や現象の発生をいう

完全なセキュリティ予防策はない

- インシデント対応活動
  - インシデントを検知し、或いはその報告を受けることにより認知し、影響の拡大を防ぐとともに、情報を収集して分析を加え、インシデントの全体像や原因について把握し、復旧措置や再発防止のための措置を取る
- 「コンピュータセキュリティ」で思い描くイメージ
  - 「いかにしてインシデントの発生を未然に防ぐか」を主眼に置かれることが多い
- コンピュータセキュリティを取り巻く状況を見ると．．．
  - 人為的ミス（パッチの適用忘れなど）
  - 未知（公知になっていない）の脆弱性の悪用
  - 技術的な対応の限界　等



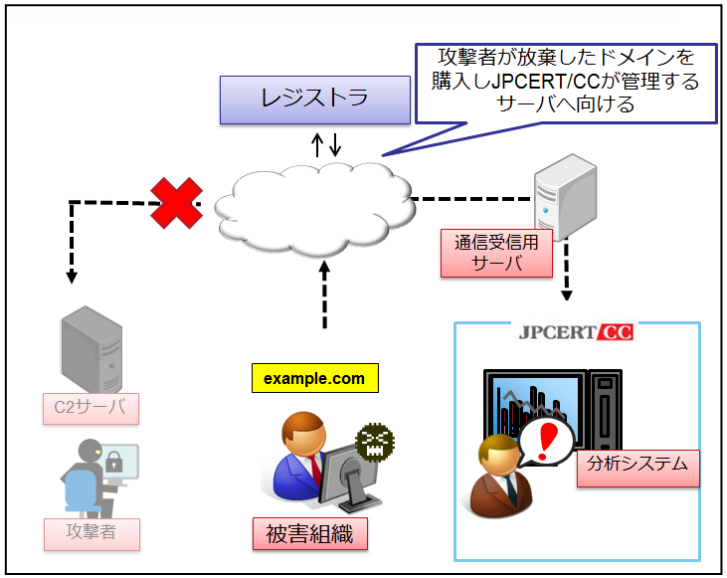
インシデントの発生を「完全に回避する」ための予防策はない
（事故前提の対応体制が必要）

（発生確率を低下させ、発生時の影響や被害を低減するための予防策はある）

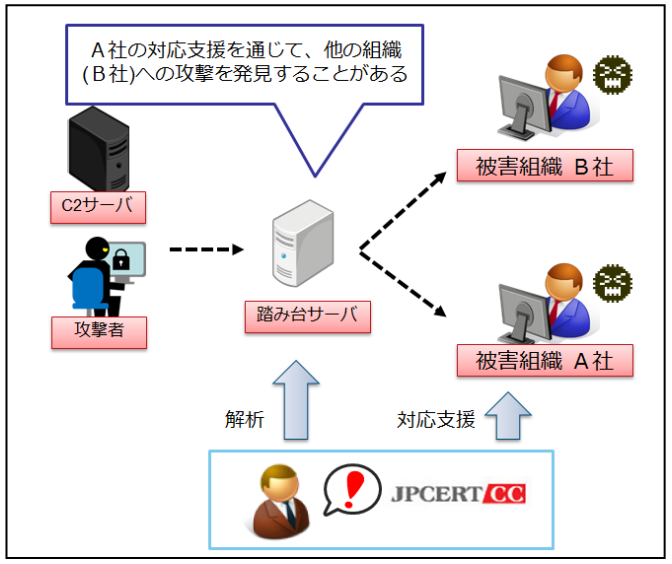
外部組織からの通知

- DNSシンクホールや、踏み台となったサーバの解析により外部組織が、被害組織より先にマルウエア感染に気づく場合がある

- JPCERT/CCが2015年4月から9月末までに実施した通知は
  133件(うち Emdivi に関連するのは96件)



DNSシンクホールの概要



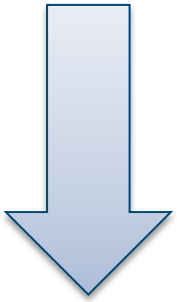
踏み台サーバ解析による攻撃の検知

「通知」におけるコミュニケーション

- 「御社は標的型攻撃の被害にあっているようだ」と外部組織から連絡を受けた際に、迅速な対応が実施できる体制を構築できているか
- リスク・コミュニケーションという観点からは、「面識がない人から突然連絡を受け、リスク(脅威)を説明されたとしても信頼や理解しづらい」とされる。むしろ疑うのが自然。

→日常的にリスクへの理解や信頼構築を行う必要性がある

1. **C**redibility(信頼確立)	価値観の共有を通じた信頼の確立
2. **A**wareness(意識)	リスクに気づき、意識する
3. **U**nderstanding(理解)	リスクについて理解を深める
4. **S**olution(解決策)	リスクに対する解決策を理解、検討する
5. **E**nactment(対処行動)	リスクへの対処行動を起こす



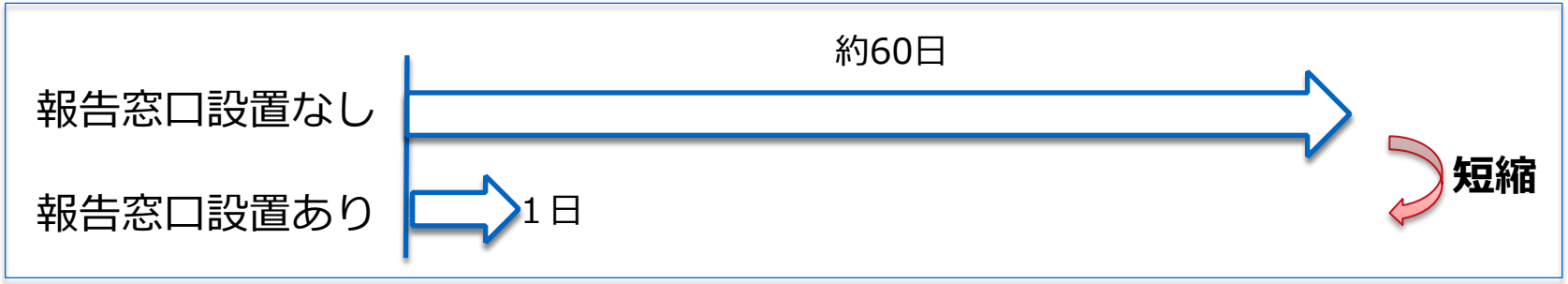
信頼醸成と
リスクへの対処

リスク・コミュニケーションにおけるCAUSEモデルの段階
(参考)KE Rowan: “Why Rules for Risk Communication Are Not Enough”

「通知」にかかる日数

- 代表電話番号や一般の問い合わせ窓口からセキュリティ担当部門までの情報伝達が、必ずしもスムーズに行われるわけではない
- そのため、セキュリティ担当部門への報告窓口を設置している組織への通知と、設置していない組織への通知は必要な日数は異なることが多い
- 報告窓口に通知できない場合、セキュリティ担当部門に届くまでに約60日を要した事例もある(設置後は即日通知が可能になった)

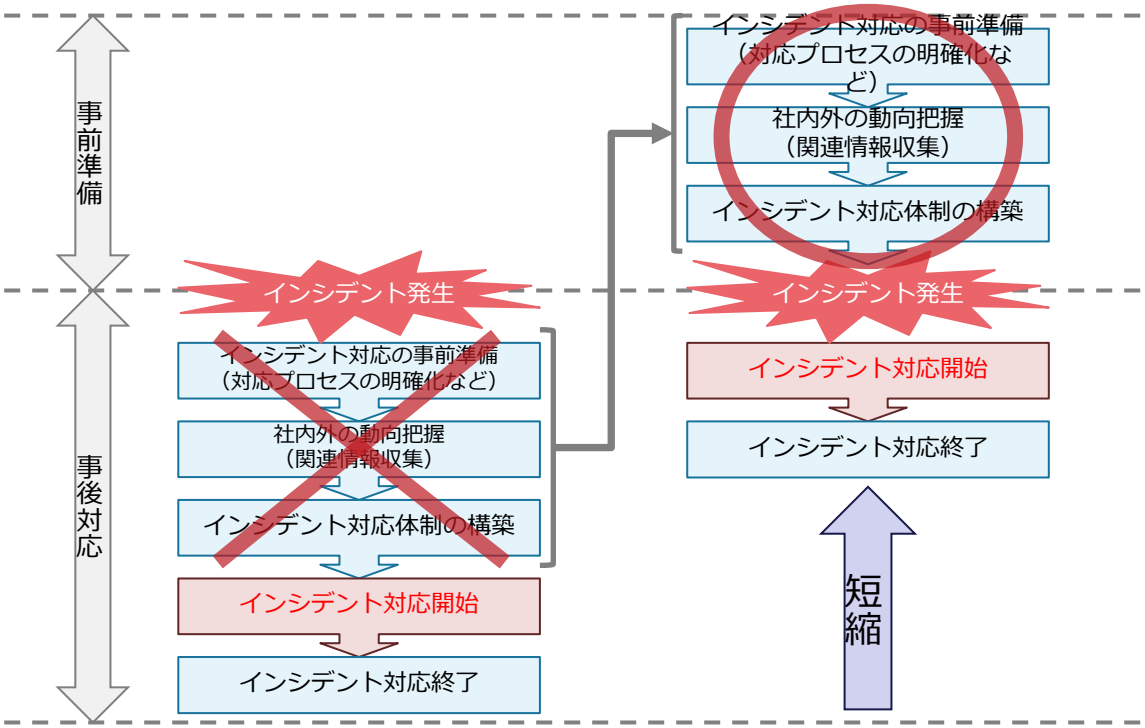
→セキュリティに関する外部組織との連絡窓口を設置し、また組織内部で実効的な調整を行える体制が必要（組織内CSIRTの必要性）



ある事例で通知に要した日数

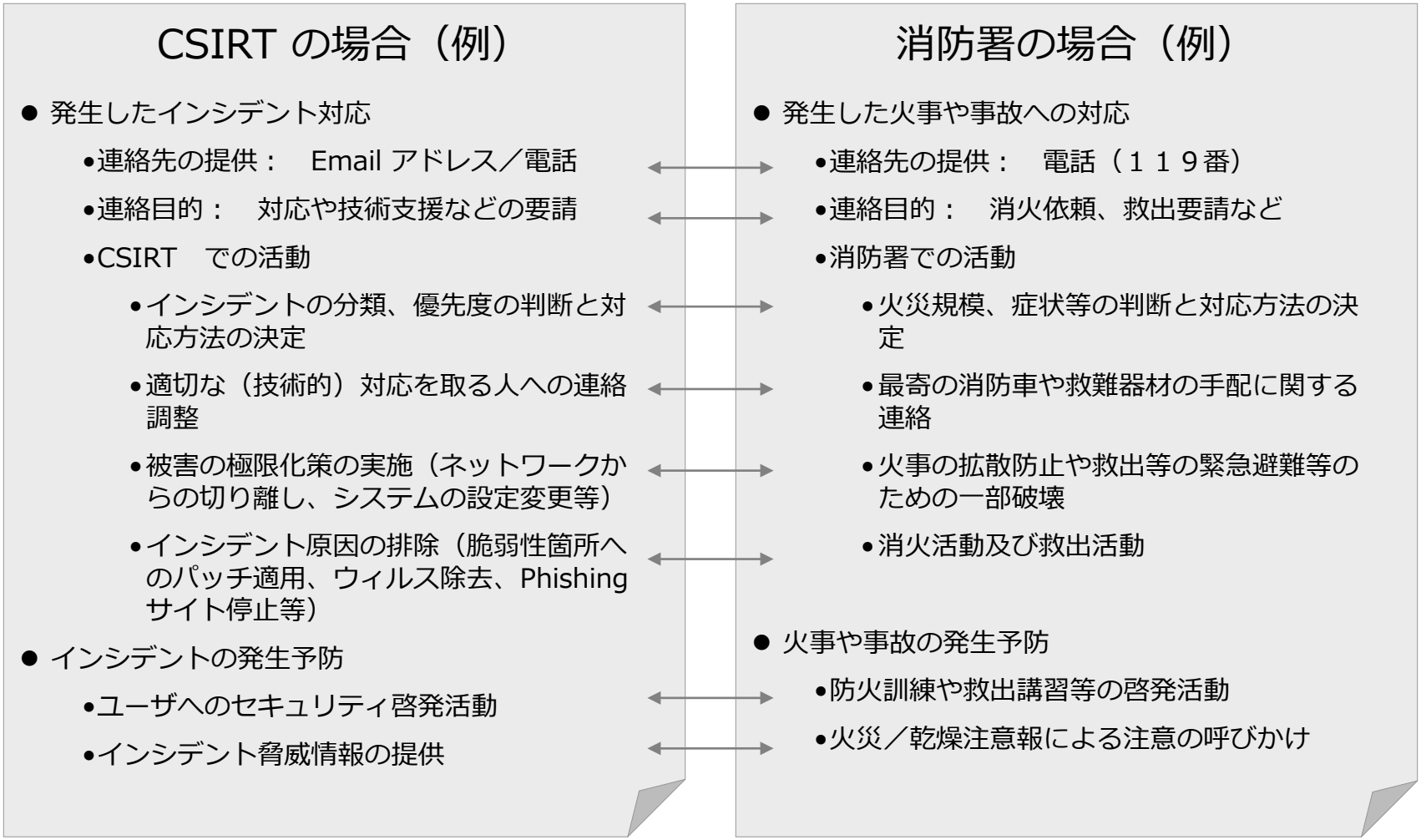
事前準備の重要性

- インシデント発生後、その対応方法を考え始め、対応体制をとるのは被害を拡大させる一因となるため、できるだけ**事前に** 対応体制等を整えておく必要がある



対応体制構築、マニュアル整備に加え、
情報セキュリティに関する”避難訓練(対応訓練)”を実施してみる

CSIRT と消防署の役割の比較例



まとめ

- 攻撃の高度化に伴い、事前の対策だけで全ての攻撃を防ぐことは困難になっている。そのため、侵入を受けたとしても被害を局所化すべく、迅速な検知と対応および事前の備えが重要である

- ログはインシデント対応時には重要な手掛かりとなるため、各機器で取得可能なログを理解したうえで、十分な期間のログを保管することが望まれる

- インシデントに備えて、日常的に情報収集を行い、リスクを理解する必要がある。また外部からの連絡を受ける可能性に鑑みてCSIRTなどの実効的な体制を構築が望まれる

(参考)ログの推奨保管期間

本章は、2013年にJPCERT/CCと米国DeltaRisk社にて作成した調査レポート”Log Data Retention Analysis Report”の内容を一部利用している。

民間セクタにおけるログ管理のベストプラクティス

- 投資対効果の評価にもとづいたデータ保管期間についてのベストプラクティスを決めるにあたり、いくつかの組織にインタビューを行った。
- 一部の組織は高度な標的型攻撃への対応プログラムを持ち、攻撃者による侵入を迅速に検知、対応するため様々なログの相関分析能力を持っていた。
- 攻撃者属性ごとの特徴を以下に示す。

攻撃者属性	主な目的	説明	脅威度
高度サイバー攻撃	攻撃対象の機密情報の取得	企業のネットワークに侵入して、企業の機密情報などを取得する	高
経済的目的の攻撃者	金銭窃取、攻撃対象の混乱	マルウエアなどを使用し、金銭窃取、業務妨害などを行う	中
愉快犯 ハクティビズム	主張	主義主張を伝えるためサイバー攻撃を行う	低

民間セクタにおけるログ管理のベストプラクティス

- 投資対効果に関するインタービューに加え、対応支援の実績をもとに攻撃者属性に対しログ保管の重要性を評価した。

- 攻撃者属性ごとのログ保管の重要性

ログ種別	高度サイバー攻撃	サイバー犯罪	ハクティビズム
DNS サーバ	Very High	High	Medium
プロキシサーバ	Very High	Very High	Medium
メールサーバ	High	High	Medium
Firewall	Medium	Medium	Medium
その他サーバ (AD等)	Medium	Medium	Medium
ホストログ(PC端末)	Low	Low	Very Low

オンライン/オフラインログの推奨保管期間

・オンラインログ(実働している機器に保管されるログ)

ログの種類	期間
DNSサーバ	1～2年
プロキシサーバ	1年
メールサーバ	N/A
Firewall	6～12カ月
その他サーバ	3～12カ月
ホストログ	1年

・オフラインログ(ファイルサーバなど別の媒体に保管されるログ)

ログの種類	期間
DNSサーバ	2年以上
プロキシサーバ	1年以上
メールサーバ	N/A
Firewall	1年以上
その他サーバ	6カ月以上
ホストログ	1年以上

Q&A、連絡・お問い合わせ先

- **その他、ご質問・ご意見などがありましたら、お知らせください。**
  - 担当 ： JPCERT/CC 早期警戒グループ
  - Mail ： ww-info@jpcert.or.jp
  - TEL ： 03-3518-4600