ログを活用した高度サイバー攻撃（標的型攻撃）の早期発見と分析

一般社団法人
JPCERTコーディネーションセンター
水野 哲也

アジェンダ

1. JPCERTコーディネーションセンターの活動
2. 高度サイバー攻撃（標的型攻撃）の背景と特徴
3. 高度サイバー攻撃の流れ
4. 攻撃の痕跡が残る機器
5. 攻撃の痕跡が残る機器における検知例
6. まとめ

1. JPCERTコーディネーションセンター（JPCERT/CC）の活動

(参考) JPCERT/CCとは

一般社団法人 JPCERTコーディネーションセンター

Japan Computer Emergency Response Team Coordination Center
ジェーピーサート コーディネーションセンター

- 日本国内のインターネット利用者や組織のセキュリティ管理担当者、ソフトウエア製品開発者等（主に、情報セキュリティ担当者）がサービス対象
- コンピュータセキュリティインシデントへの対応、国内外にセンサをおいたインターネット定点観測、ソフトウエアや情報システム・制御システム機器等の脆弱性への対応などを通じ、ITセキュリティ向上を推進
- インシデント対応をはじめとする国際連携が必要なオペレーションや情報連携に関する、我が国の窓口となるCSIRT（窓口CSIRT）

CSIRT: Computer Security Incident Response Team

※各国に同様の窓口となるCSIRTが存在する(米国のUS-CERT、CERT/CC、中国のCNCERT, 韓国のKrCERT/CC など)

- 経済産業省からの委託事業として、サイバー攻撃等国際連携対応調整事業を実施

1.1 JPCERT/CCの活動

インシデント予防 → インシデントの予測と捕捉 → 発生したインシデントへの対応

脆弱性情報ハンドリング

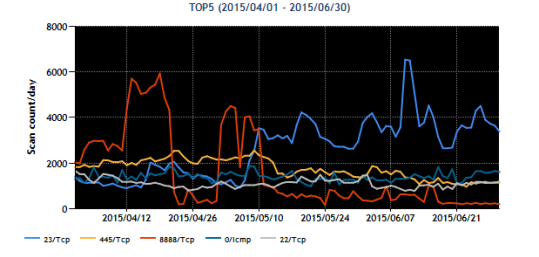
- 未公開の脆弱性関連情報を製品開発者へ提供し、対応依頼
- 関係機関と連携し、国際的に情報公開日を調整
- セキュアなコーディング手法の普及
- 制御システムに関する脆弱性関連情報の適切な流通

JVN Japan Vulnerability Notes

情報収集・分析・発信

定点観測（TSUBAME）

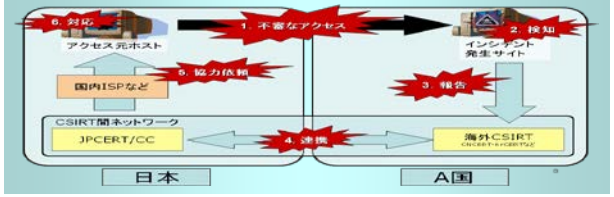
- ネットワークトラフィック情報の収集分析
- セキュリティ上の脅威情報の収集、分析、必要とする組織への提供



インシデントハンドリング

（インシデント対応調整支援）

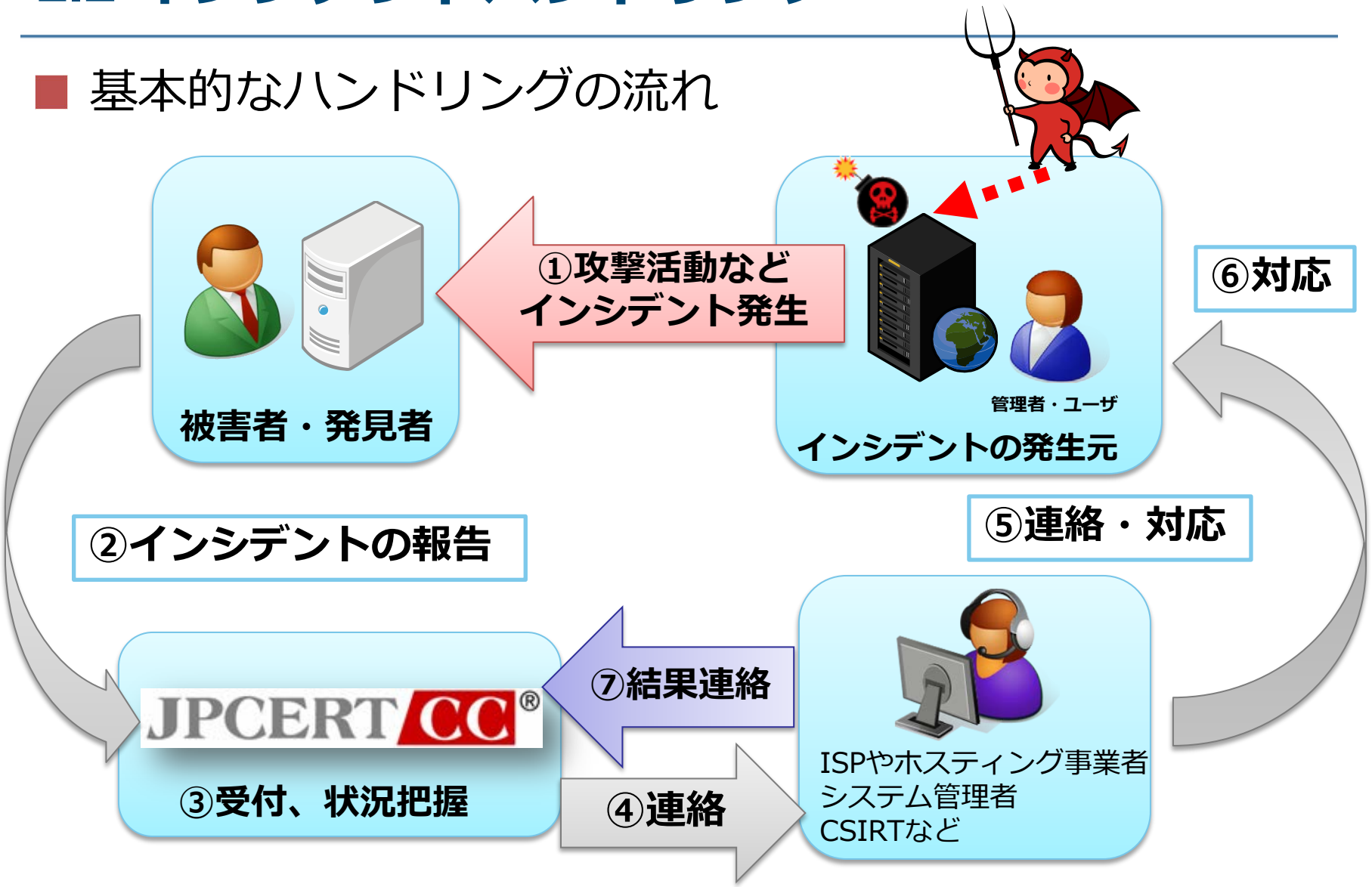
- マルウエアの接続先等の攻撃関連サイト等の閉鎖等による被害最小化
- 攻撃手法の分析支援による被害可能性の確認、拡散抑止
- 再発防止に向けた関係各関の情報交換及び情報共有



早期警戒情報	重要インフラ、重要情報インフラ事業者等の特定組織向け情報発信
CSIRT構築支援	海外のNational-CSIRTや企業内のセキュリティ対応組織の構築・運用支援
制御システムセキュリティ	制御システムに関するインシデントハンドリング、情報収集・分析発信
アーティファクト分析	マルウエア（不正プログラム）等の攻撃手法の分析、解析
国内外関係者との連携	日本シーサート協議会、フィッシング対策協議会の事務局運営等
国際連携	各種業務を円滑に行うための海外関係機関との連携

1.2 インシデントハンドリング

- 基本的なハンドリングの流れ



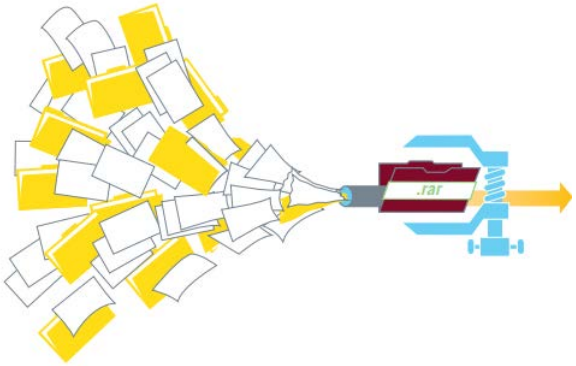
2. 高度サイバー攻撃（標的型攻撃）の背景と特徴

2.1 背景

- 最近、特定の組織を狙う高度サイバー攻撃がメディアを騒がせている
- 攻撃者は、狡猾なため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
- 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
- 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

2.2 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高度サイバー攻撃の特徴は次の通り
  - 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が窃取された
  - 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の期間は、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窃取する

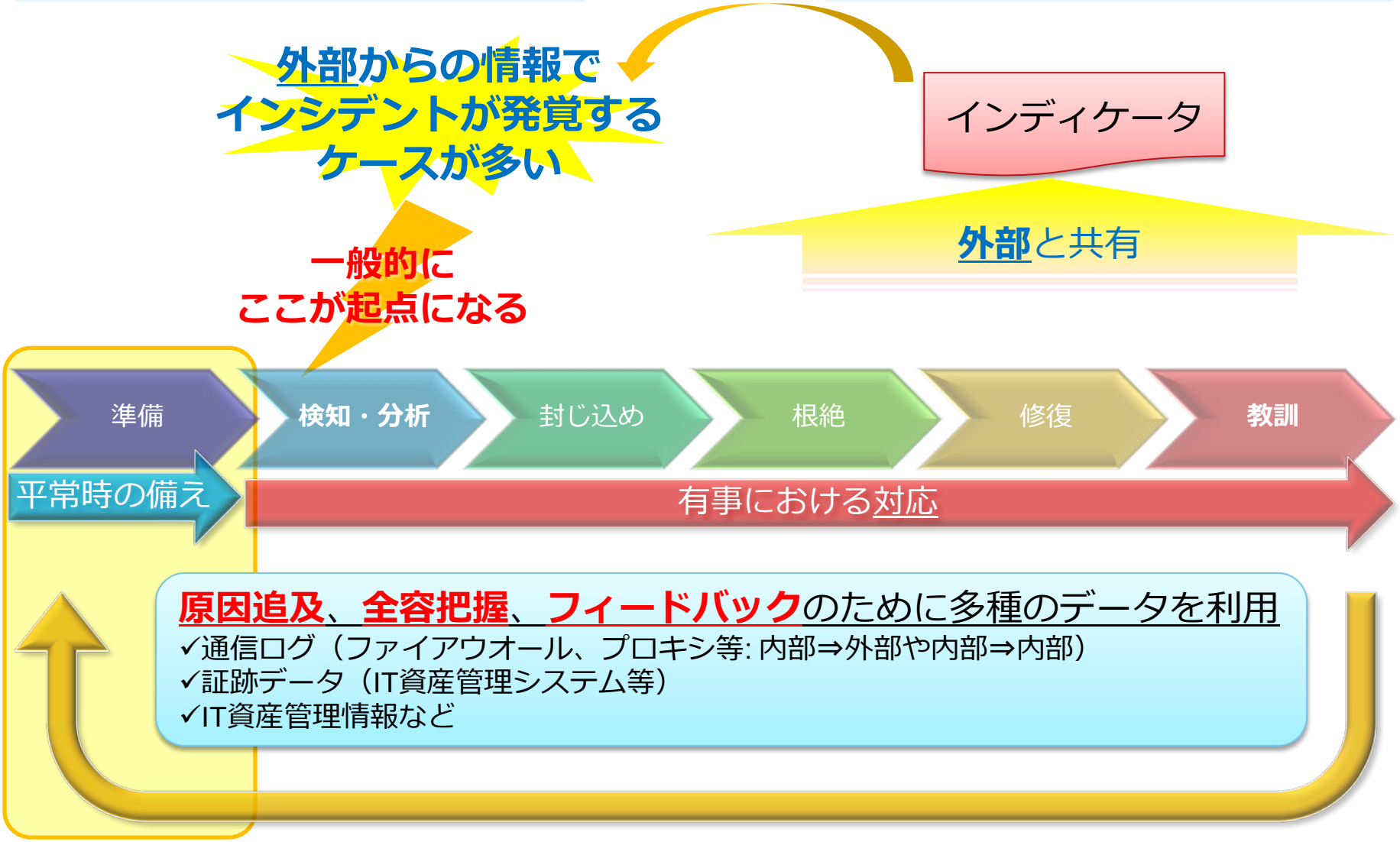


(参考)
Mandiant Intelligence Center Report
http://intelreport.mandiant.com/

2.3 各組織におけるインシデント対応のプロセス

マネージメントの積極的関与

外部との情報連携



2.4 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？

2.5 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（1年以上の保存を推奨）
  - 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。

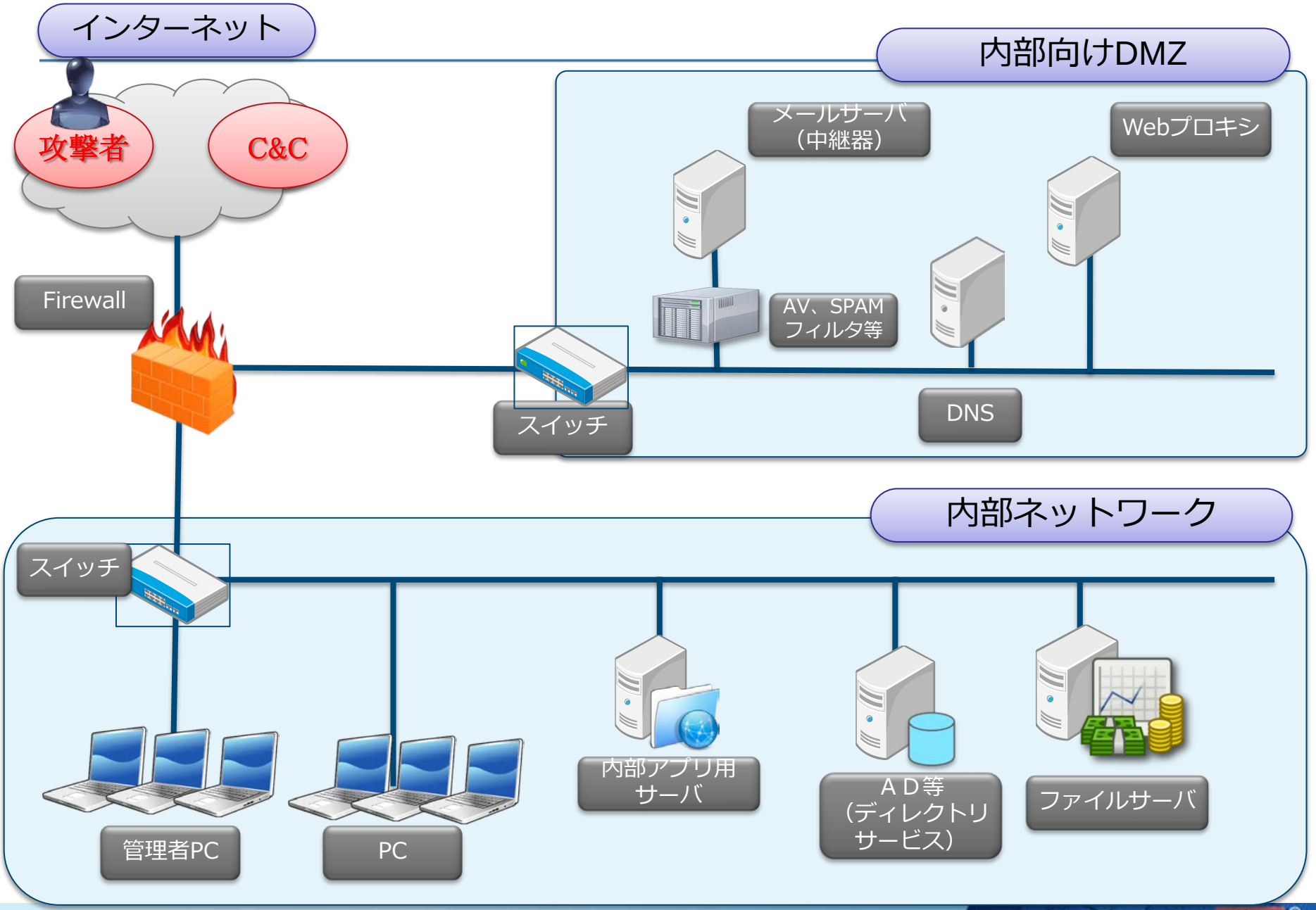
3. 高度サイバー攻撃の流れ

3.1 高度サイバー攻撃におけるキルチェーンモデル

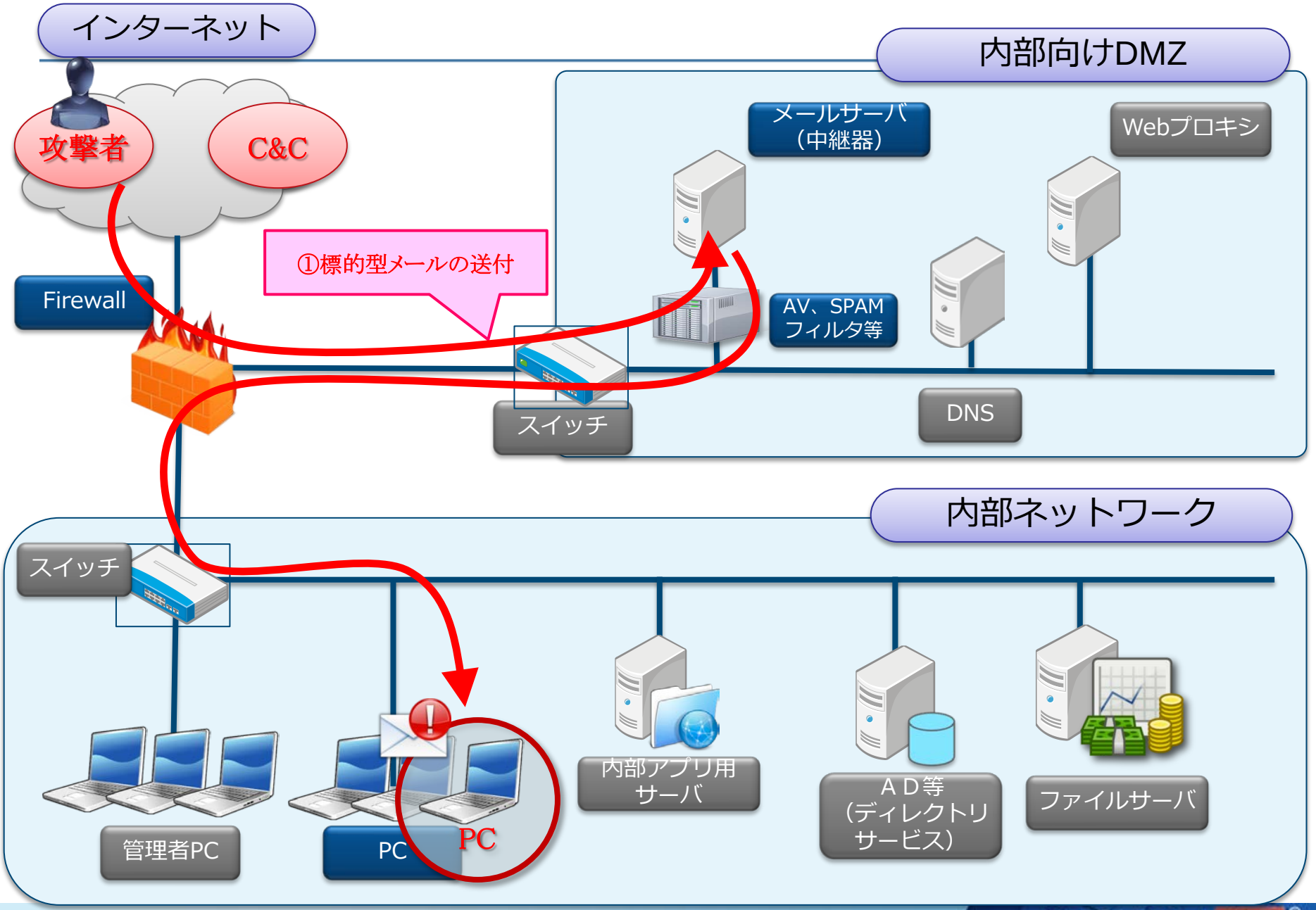
	攻撃の段階	概要
1	偵察	・インターネットなどから組織や人物の調査し、対象組織に関する情報を取得する
2	武器化	・エクスプロイトやマルウエアを作成する
3	デリバリ	・なりすましメール（マルウエアを添付）を送付する ・なりすましメール（マルウエア設置サイトに誘導）を送付し、ユーザにクリックさせるように誘導する
4	エクスプロイト	・ユーザにマルウエア添付ファイルを実行させる ・ユーザをマルウエア設置サイトに誘導し、脆弱性を使用したエクスプロイトコードを実行させる
5	インストール	・エクスプロイトの成功により、標的(PC)がマルウエアに感染する
6	C&C	・マルウエアによりC&Cサーバと通信させ、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

3.2 高度サイバー攻撃の流れ（例）

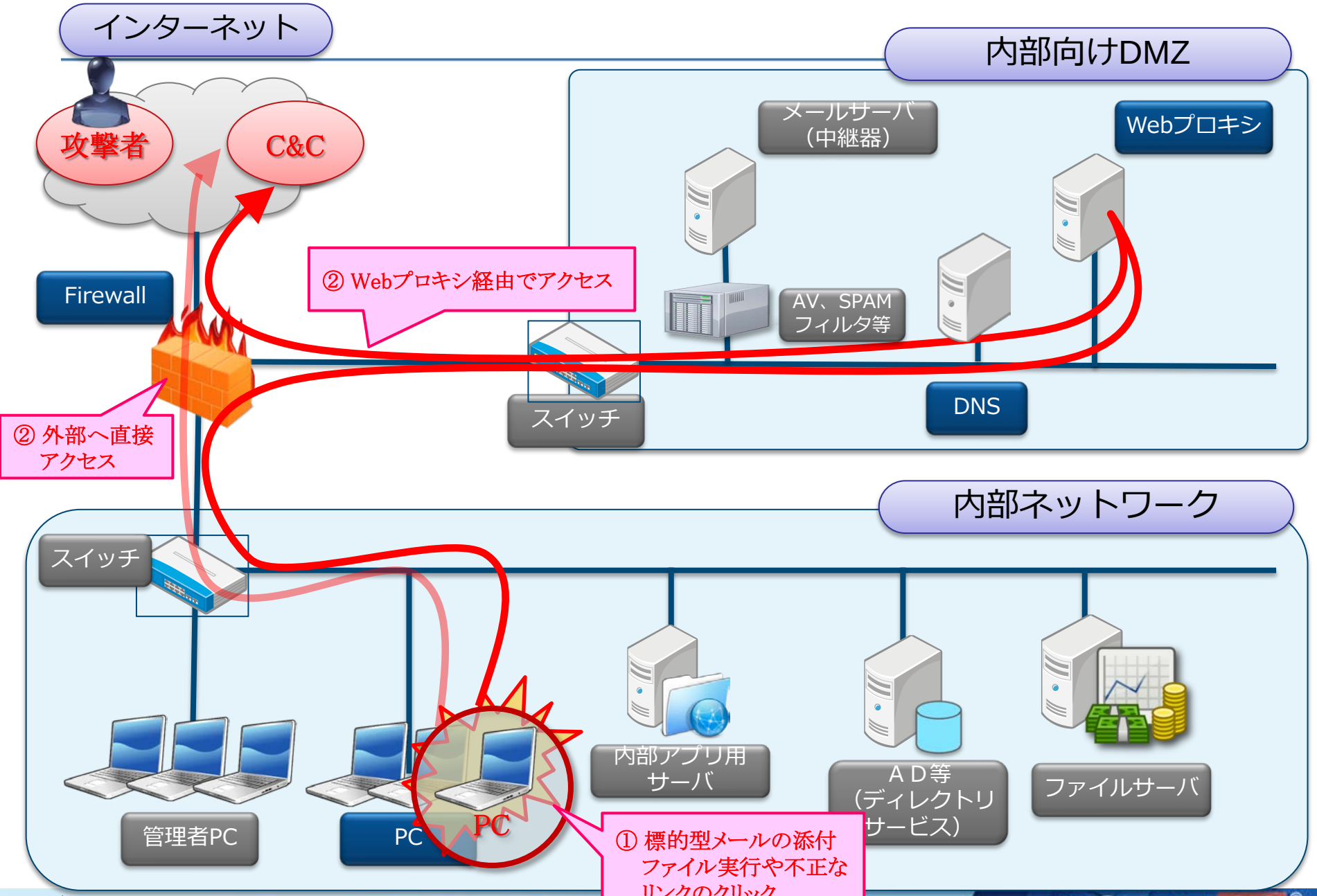
3.2.1 第1段階 偵察、第2段階 武器化



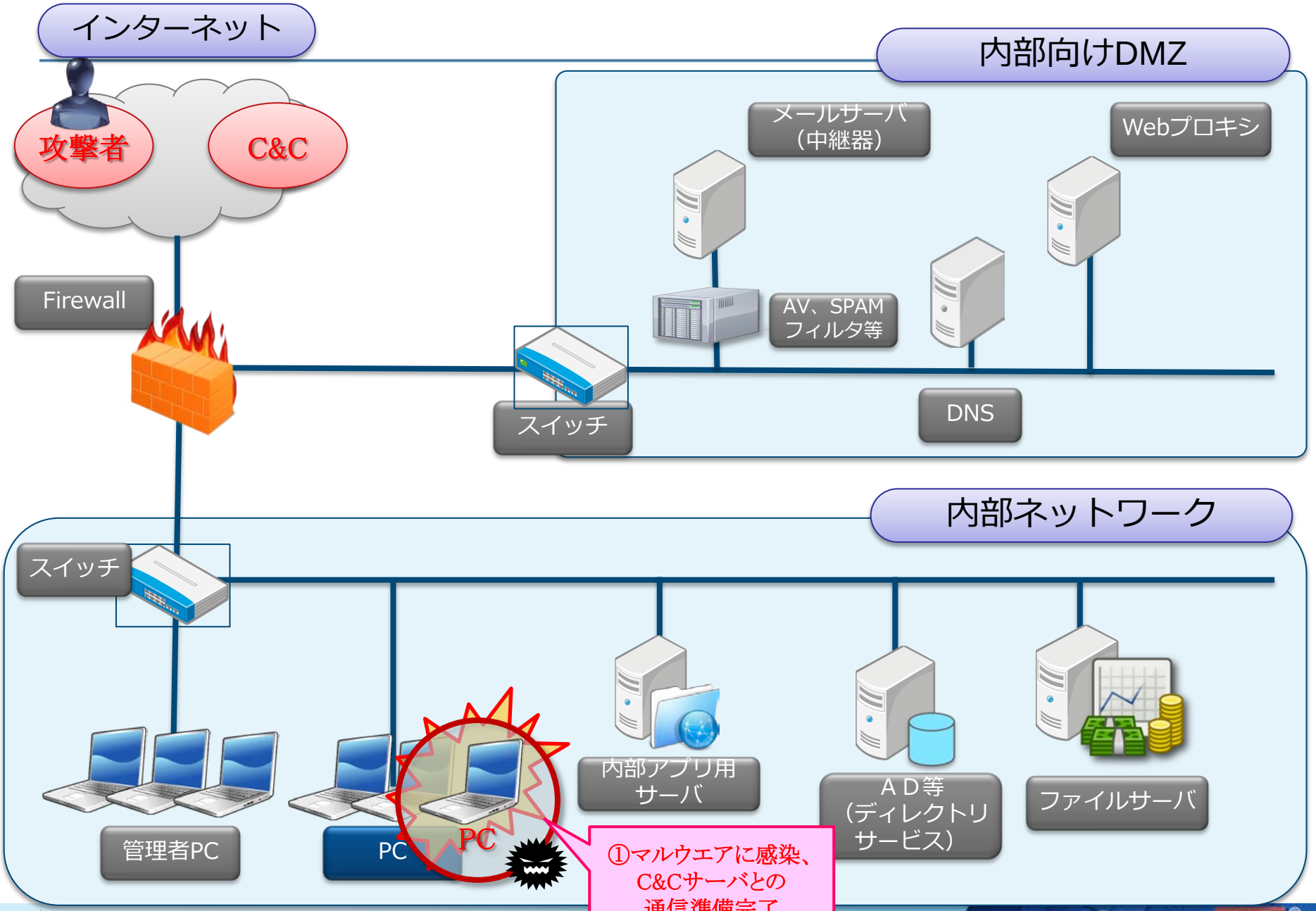
3.2.2 第3段階 デリバリ



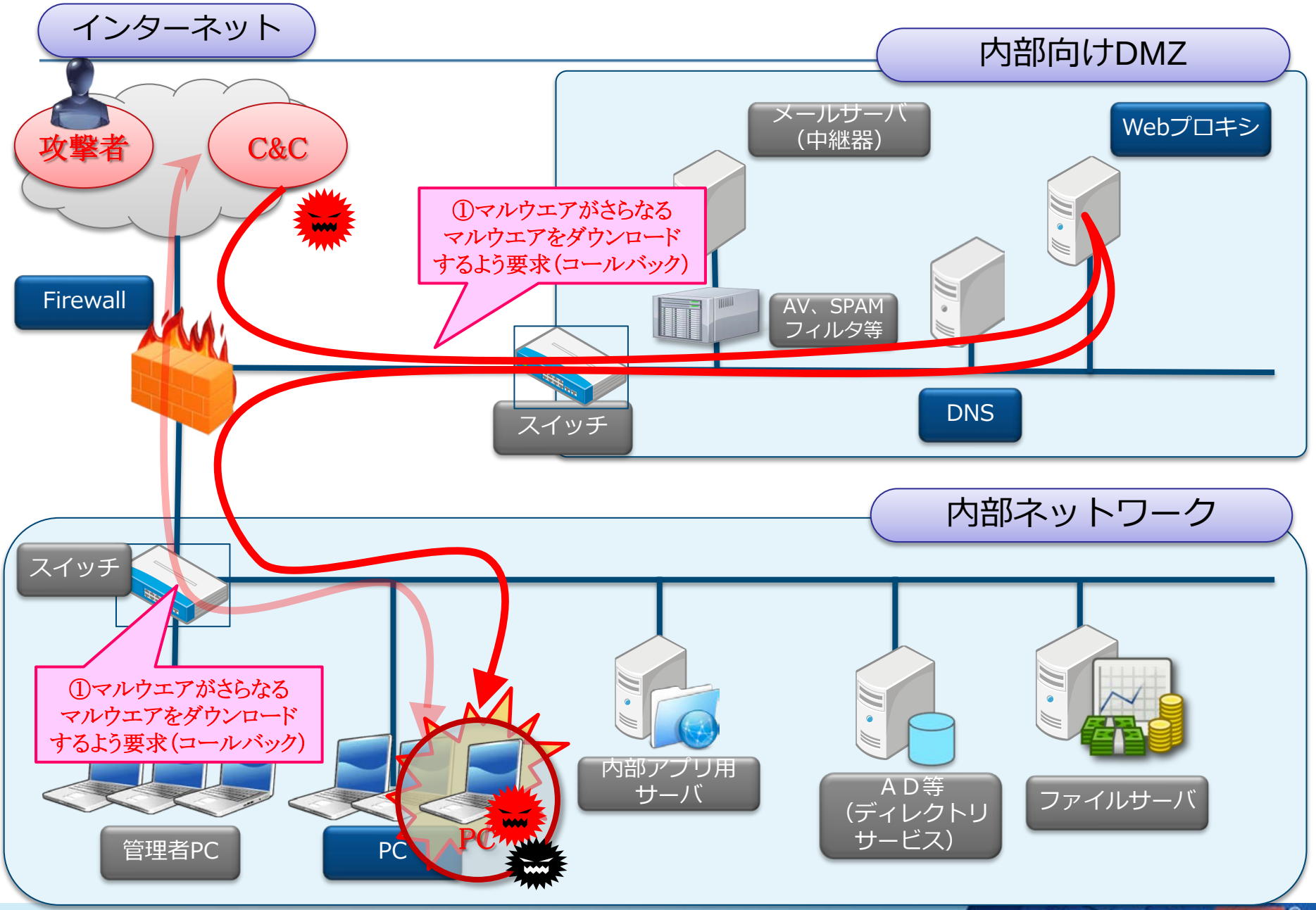
3.2.3 第4段階 エクスプロイト



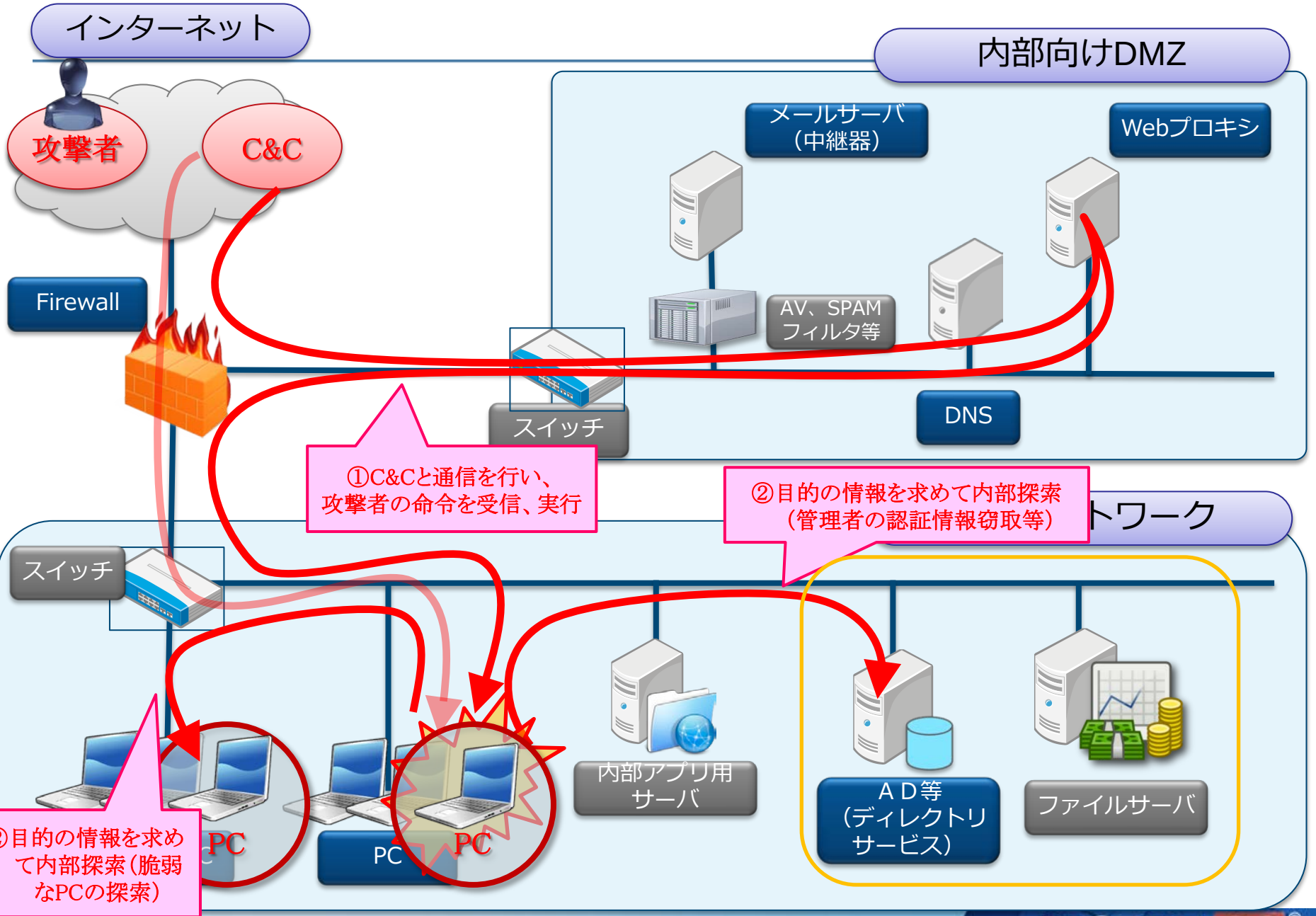
3.2.4 第5段階 インストール



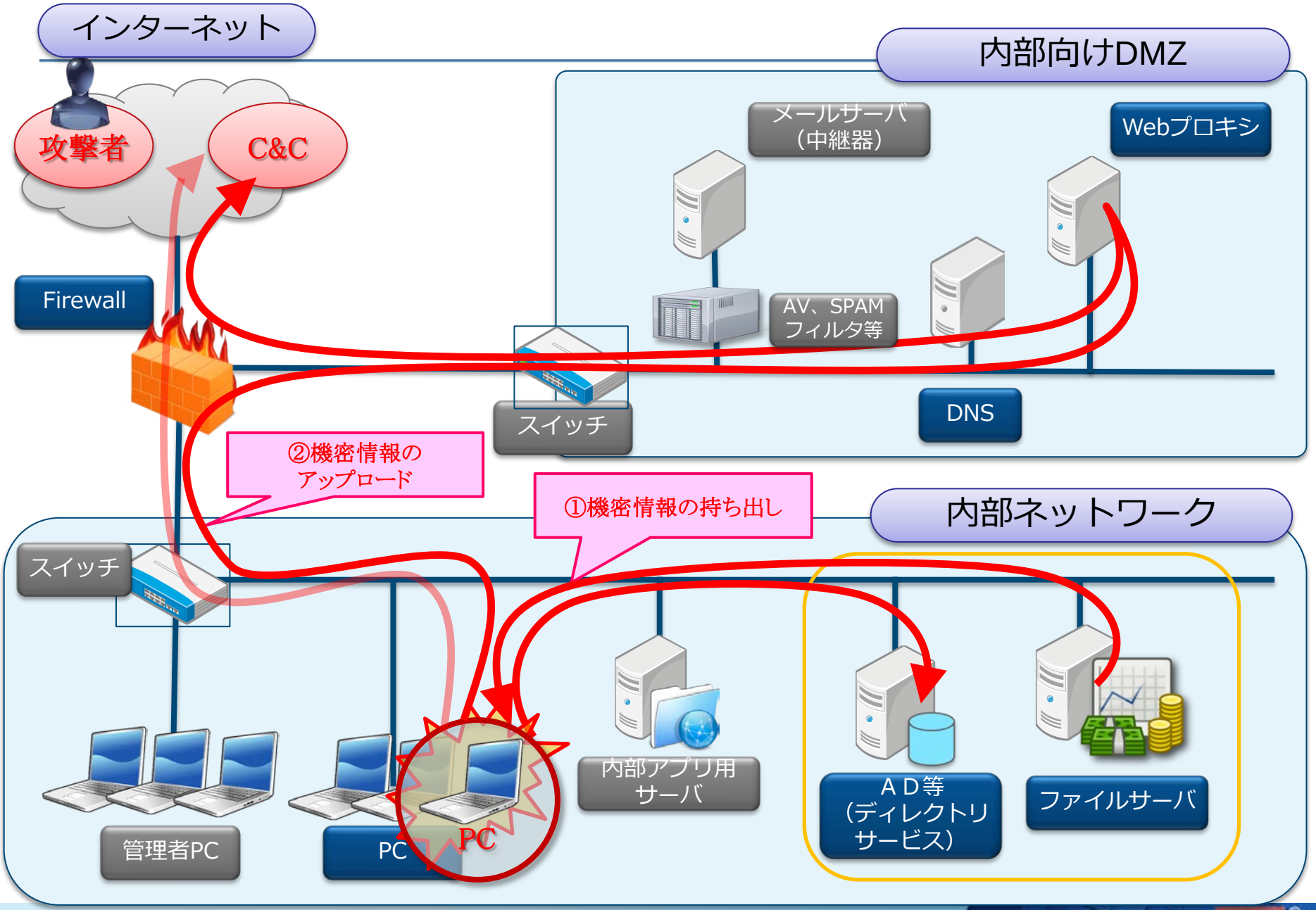
3.2.5 第6段階　C&C(1)



3.2.6 第6段階　C&C(2)

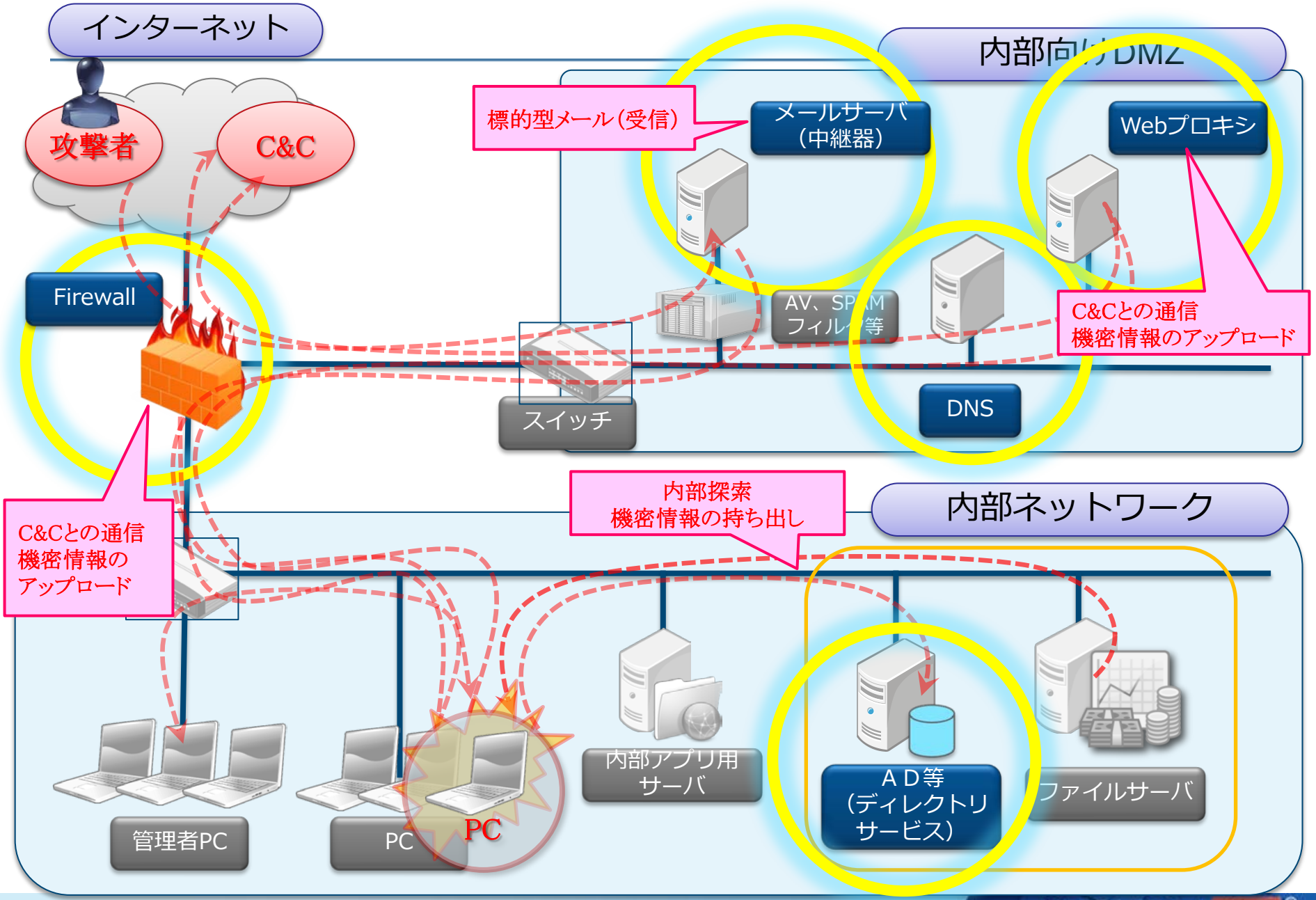


3.2.7 第7段階　目的の実行



4. 攻撃の痕跡が残る機器

4.1 攻撃の痕跡が残る機器



4.2 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

4.3 ログを分析する上でのポイント (1/2)

- 定期的なログ分析
  - 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
  - 定常的な状態とは異なるログが出力されていないかを確認
    - 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ログ分析
  - 提供された情報をもとに、その情報に一致するログが存在しないかを確認
    - メールヘッダ、差出人情報、添付ファイル名
    - 通信先（C&C、マルウエア設置サイト）のURL、IPアドレス、ドメインなど

4.4 ログを分析する上でのポイント (2/2)

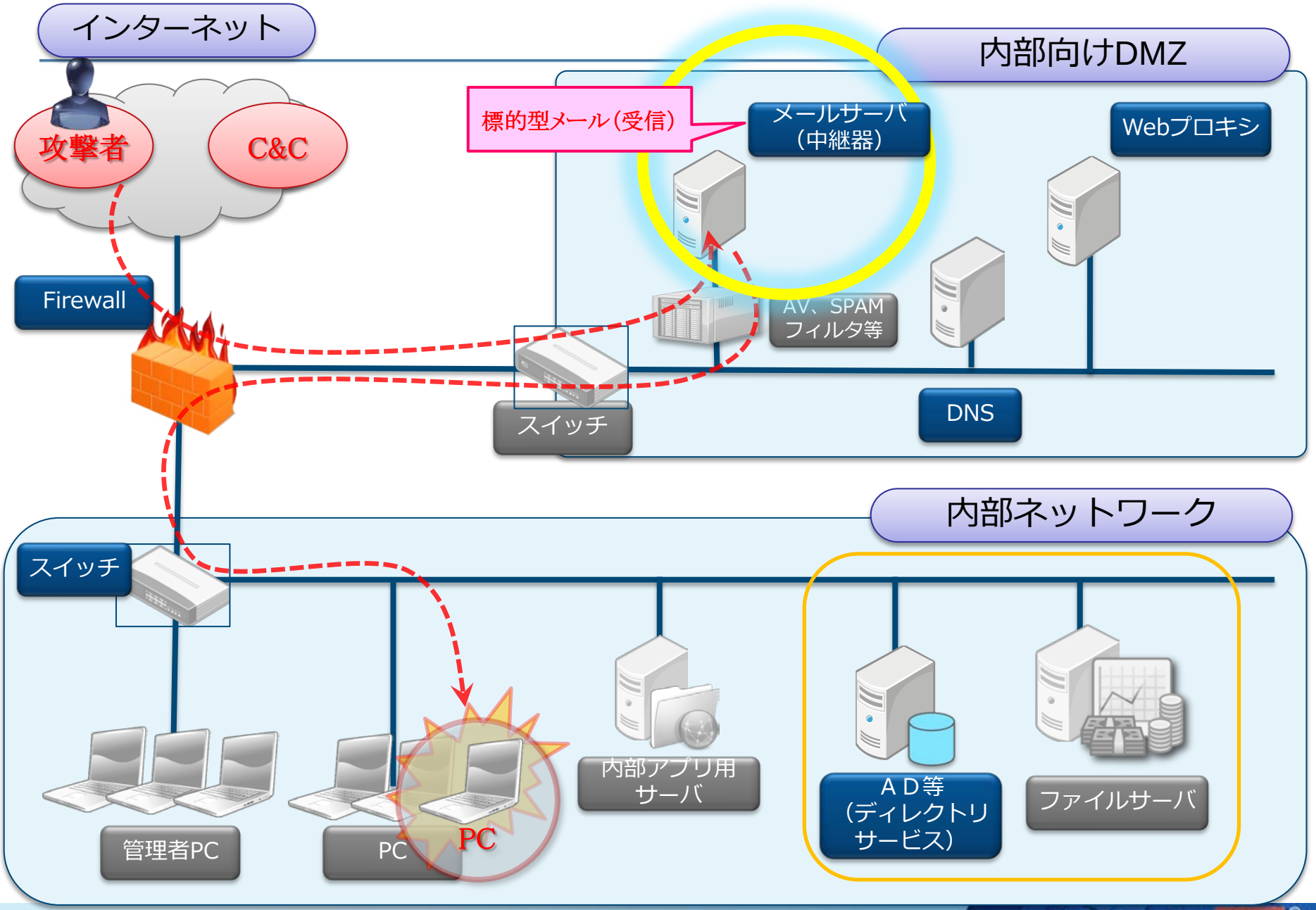
- JPCERT/CCの対応支援の経験則上、高度サイバー攻撃を考慮するログの保存期間は、最低１年以上を推奨している。

- ログを長期間保存すると次の様な課題が発生する。
  - 記憶媒体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

- 直近のログをオンラインで保存し、ある期間を経過したらオフライン保存に切り替える
  - オンライン保存 (例：保存期間は3ヶ月程度)
  - オフライン保存 (例：3ヶ月以上の期間全て)

5. 痕跡が残る機器における検知例

5.1 攻撃の痕跡が残る機器における検知例(メールサーバ)



5.1.1 メールサーバにおけるポイント

- 攻撃の発見に利用できる代表的なログ項目

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メール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

5.1.2 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

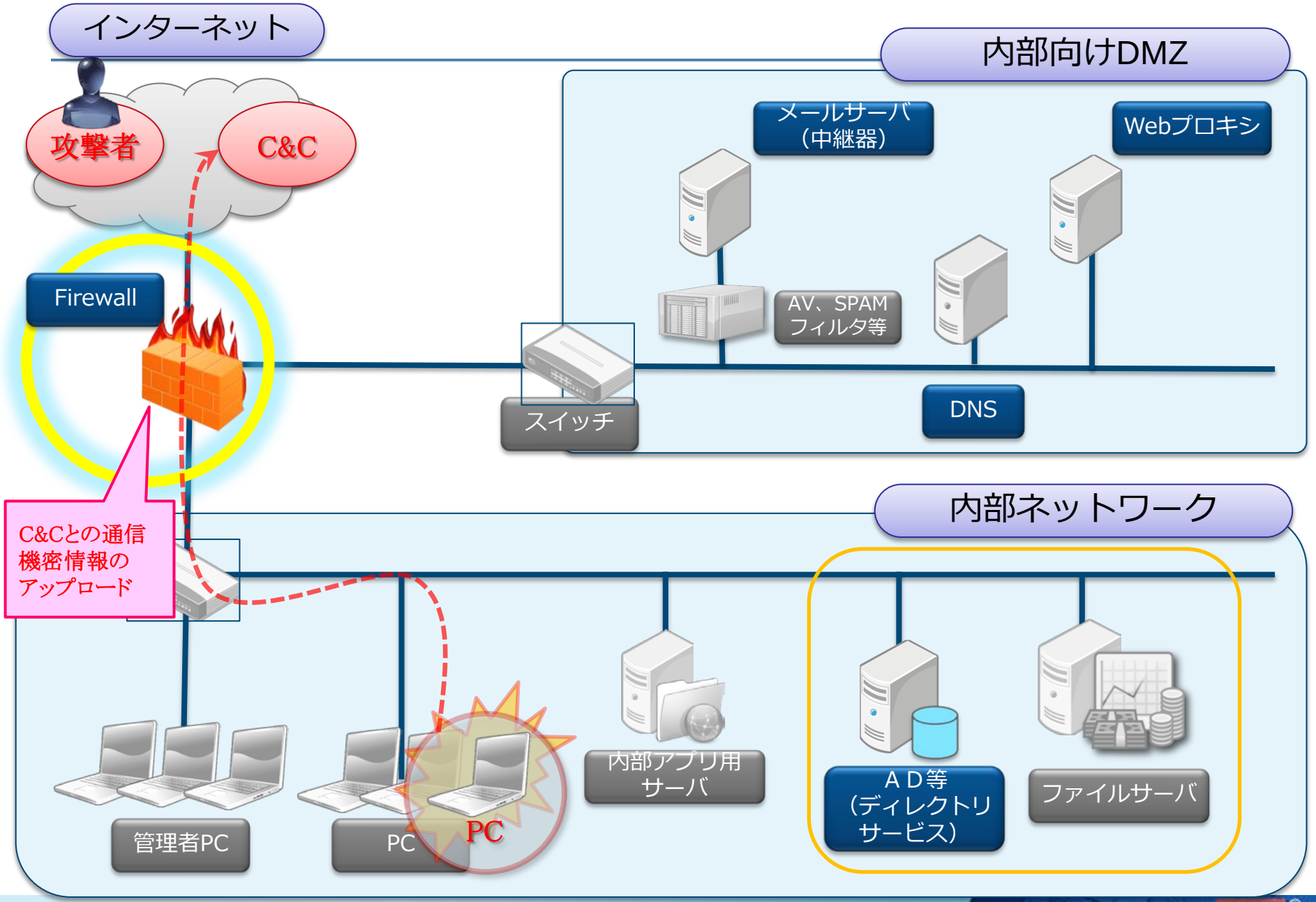
File: /etc/postfix/main.cf のファイルに次の内容を追記
header_checks = regexp:/etc/postfix/header_checks
File: /etc/postfix/header_checks のファイルに次の内容を追記
/^From:/ WARN

  - 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

* 設定の適用によるシステムへの負荷や、ログの増加量を見定めたうえで実施してください。

5.2 攻撃の痕跡が残る機器(Firewall)



5.2.1 Firewallにおけるポイント

- 攻撃の発見に利用できる代表的なログ項目

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通信をFirewallのログから検知する 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

5.2.2 Firewallのログの例(Juniper SSG)

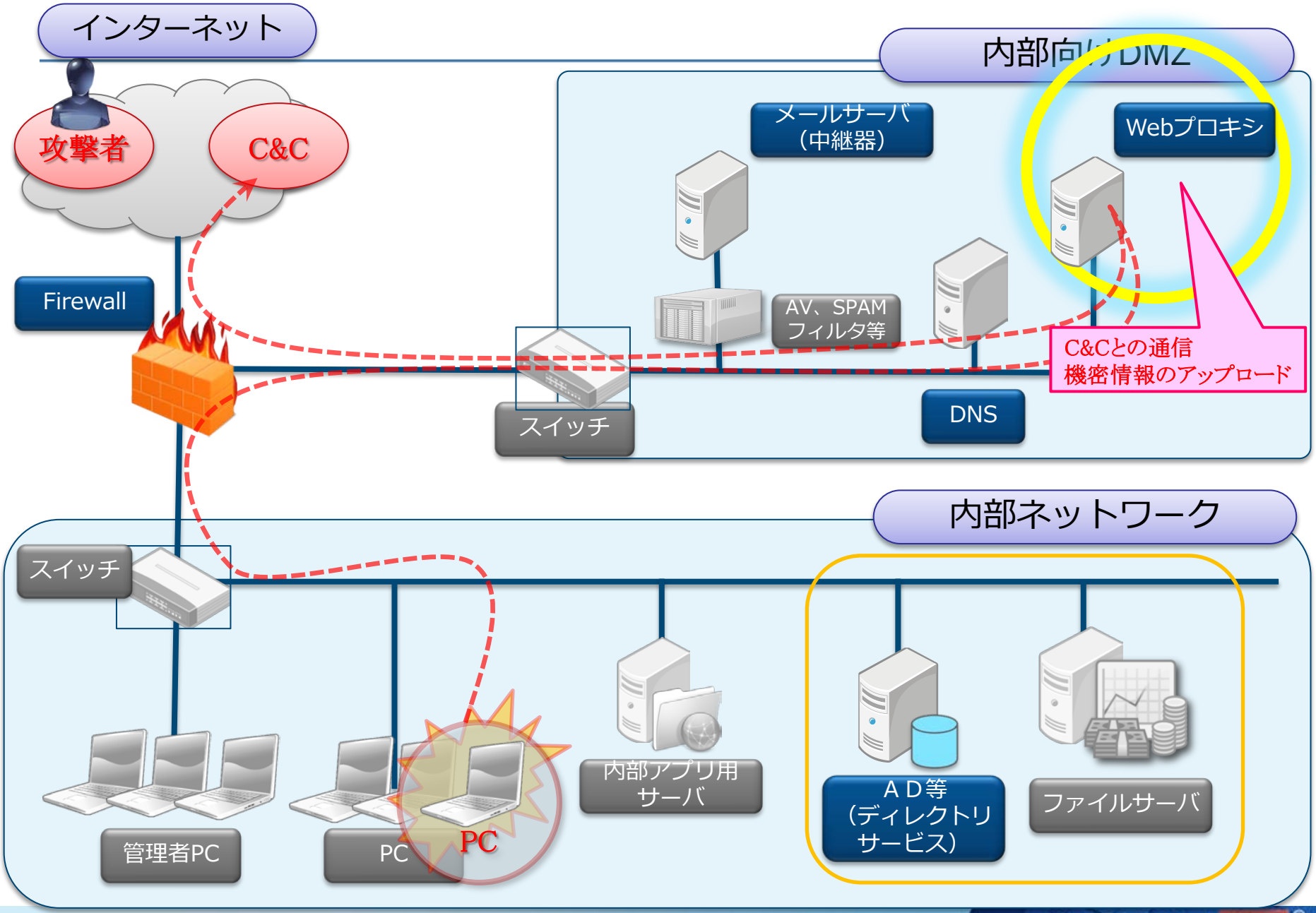
- 組織内から組織外への不正な通信ログの例

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

5.3 攻撃の痕跡が残る機器 (Webプロキシ)



5.3.1 Webプロキシサーバにおけるポイント(1/2)

- 攻撃の発見に利用できる代表的なログ項目

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

5.3.2 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

5.3.3 Webプロキシサーバのログの例(squid)(1/2)

- 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
```

5.3.4 Webプロキシサーバのログの例(squid)(2/2)

- 標準利用以外のUser Agentによる通信ログの例

```
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通信ログの例

```
1424721299.090 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

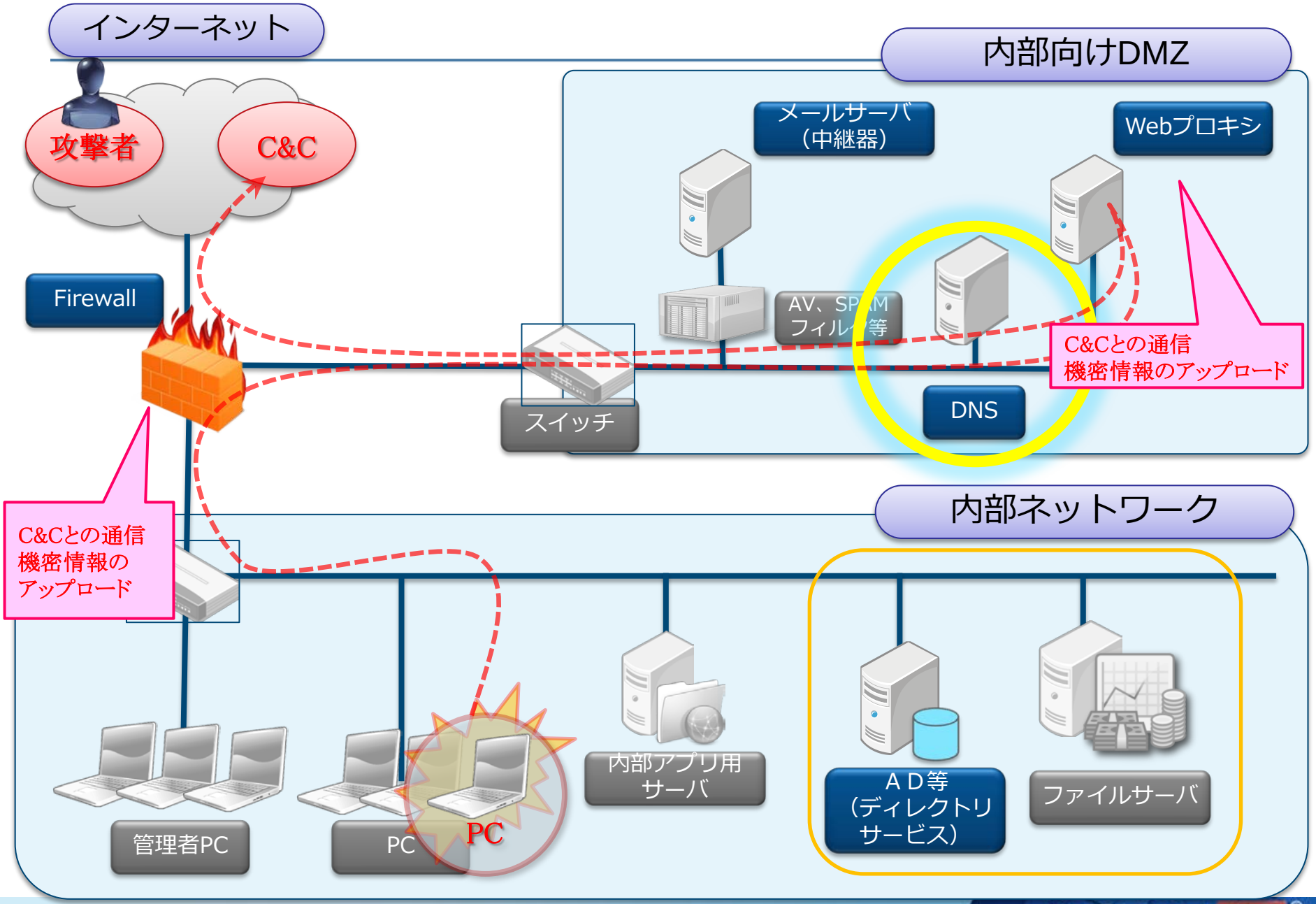
- Squidにおいて、次の情報をログ出力するためには設定変更が必要
  - UserAgentの情報の記録

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
```

* 設定の適用によるシステムへの負荷や、ログの増加量を見定めたうえで、実施してください。

5.4 攻撃の痕跡が残る機器(DNSサーバ)



5.4.1 DNS(キャッシュ)サーバにおけるポイント

- 攻撃の発見に利用できる代表的なログ項目

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

- 不審な送信先への通信ログの例

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

（参考）BINDの標準設定で出力されないログ

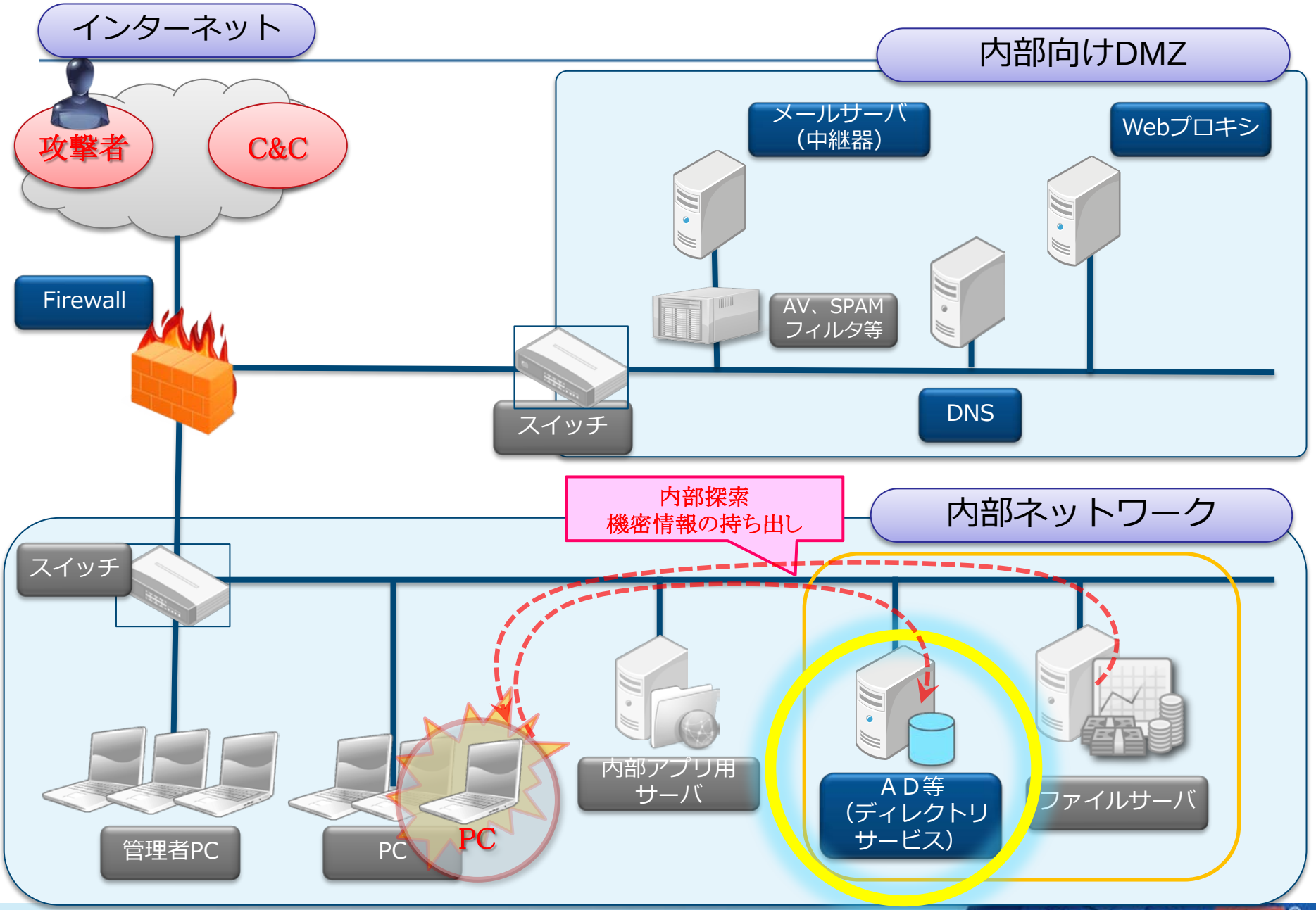
- BIND9において次の情報をログ出力するためには設定が必要
  - PCなどのクライアントがDNSサーバにホスト名の解決を行ったクエリの記録

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“;
        severity info;
        print-time yes;
        };
        category queries { " queries_log"; };
};
```

* 設定の適用によるシステムへの負荷や、ログの増加量を見定めたうえで、実施してください。

5.5 攻撃の痕跡が残る機器(認証サーバ)



5.5.1 認証サーバ (Active Directory)におけるポイント

- 攻撃の発見に利用できる代表的なログ項目

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（イベントログ）	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
管理者アカウントに関連したイベントの調査	マルウエアに感染したPCから、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
通常の運用では発生しないようなイベント	侵入の痕跡を消すために、ログを消去を試みる	通常の運用では発生しない特殊な操作要求を確認

5.5.3 認証サーバ (Active Directory)におけるポイント(1/2)

- 管理者アカウントに関連したイベントの調査
  - 調査対象とする認証イベント
    - ログインの成功　(イベント ID:4624)
    - ログインの失敗　(イベント ID:4625)
    - Kerberos 認証　(イベント ID:4768)
    - NTLM 認証　(イベント ID:4776)
    - 特権の割り当て　(イベント ID:4672)
  - 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。

5.5.2 認証サーバ (Active Directory)におけるポイント(1/2)

- 通常の運用では、発生しないようなイベントID

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る場合、サイバーキルチェーンモデルのC&Cの段階の可能性を考慮し、想定された運用によるものかどうかを確認する必要があると考えられる。

（参考） Active Directoryのログ出力設定

- Active Directoryの監査ポリシーの設定で、次の項目を有効にする必要がある（バージョンによっては初期設定で有効となっている場合もある）。
  - 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

* 設定の適用によるシステムへの負荷や、ログの増加量を見定めたうえで、適用を実施してください。

6. まとめ

6.1 まとめ

- 国内でも高度サイバー攻撃による被害は深刻になってきており、各組織でも十分な対応体制が必要とされている
- 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、十分な期間のログ保存が望まれる

6.2 Q&A、連絡・お問い合わせ先

- **11月17日公開ドキュメント**

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
https://www.jpcert.or.jp/research/apt-loganalysis.html

- **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