A-3.
標的型サイバー攻撃の調査と対応（ネットワーク編）

明治大学
服部　裕之

このセッションの目標

標的型サイバー攻撃を受けた時の
「痕跡調査」と「一時対応」手法を学び、実習にて確認する

標的型サイバー攻撃を受けた時に
ネットワークレベルでの調査・対応が行えるようになる

インシデント対応フローチャートに沿った対応

1. 外部からの指摘
2. 事実の確認・一次対応
   1. ネットワークレベルでの調査・対応
   2. PCレベルでの調査・対応

A−3

3. インシデント対応に関する体制、手順の確認
4. インシデント情報の集約
5. 被害（情報漏えい）の調査・予想
6. 対外的窓口の設置
7. インシデント情報公開の時期と公開内容の検討
8. 再発防止計画

標的型サイバー攻撃の流れ

① 計画立案
② 攻撃準備

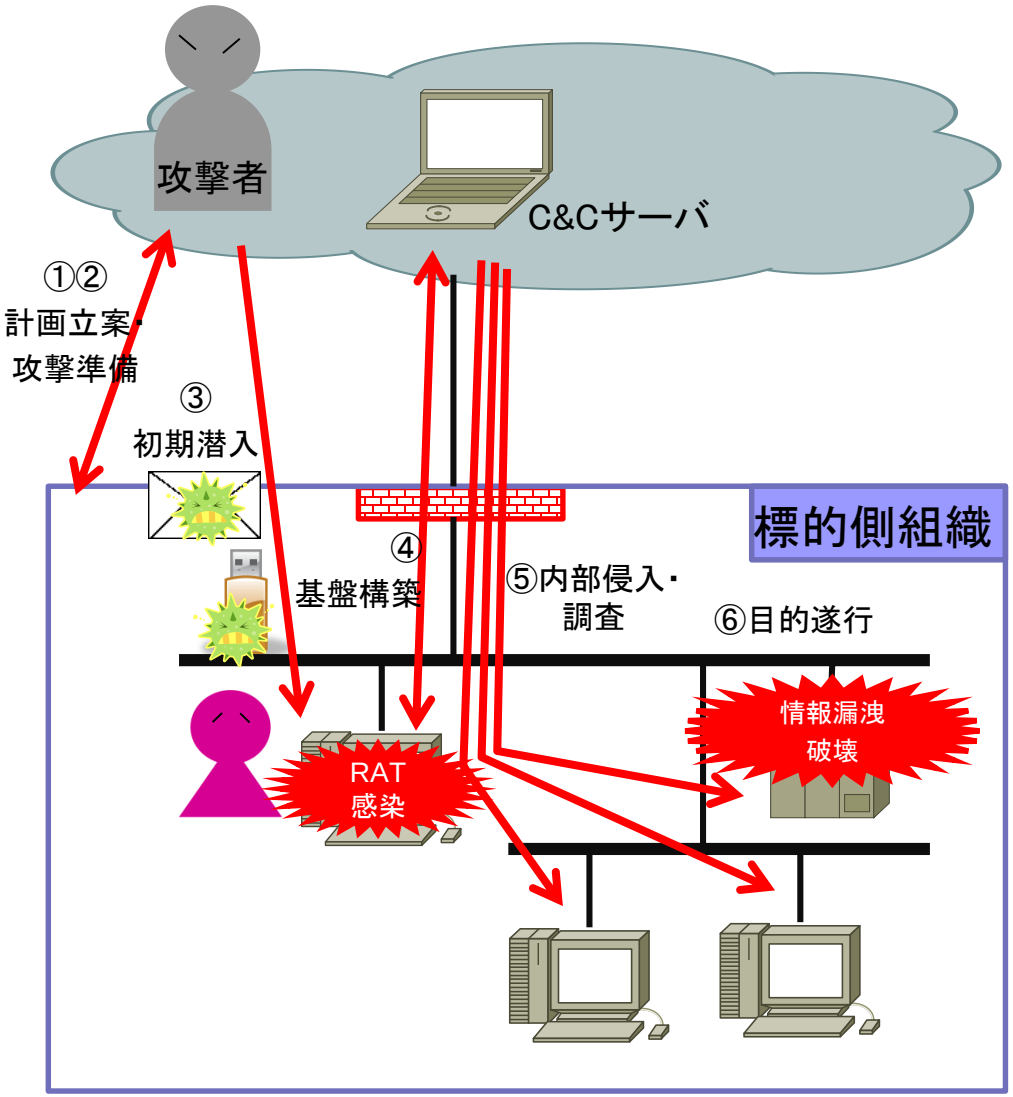
③ 初期潜入

④ 基盤構築

⑤ 内部侵入
調査

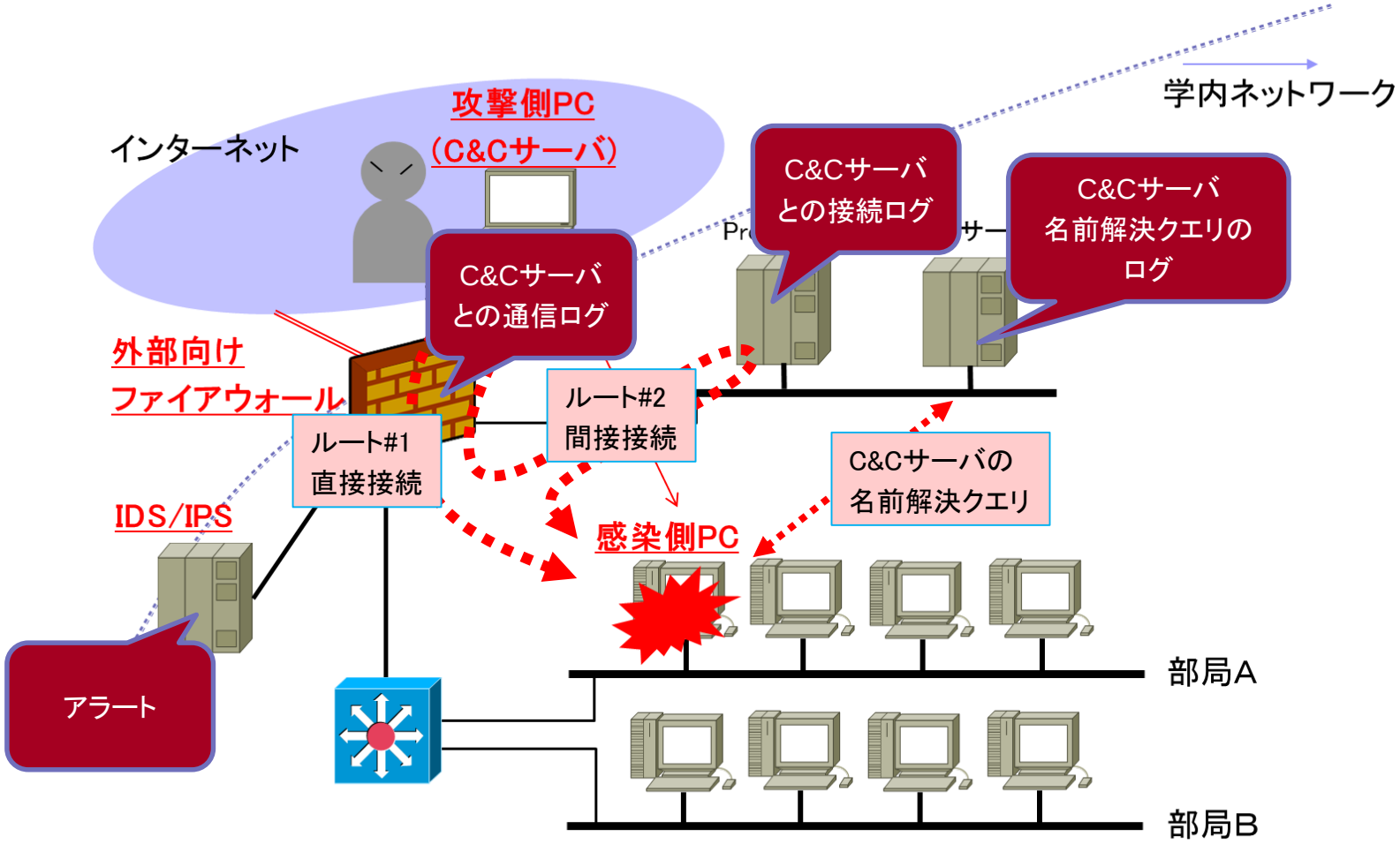
⑥ 目的遂行

A-3
ネットワーク
レベルでの
調査・対応



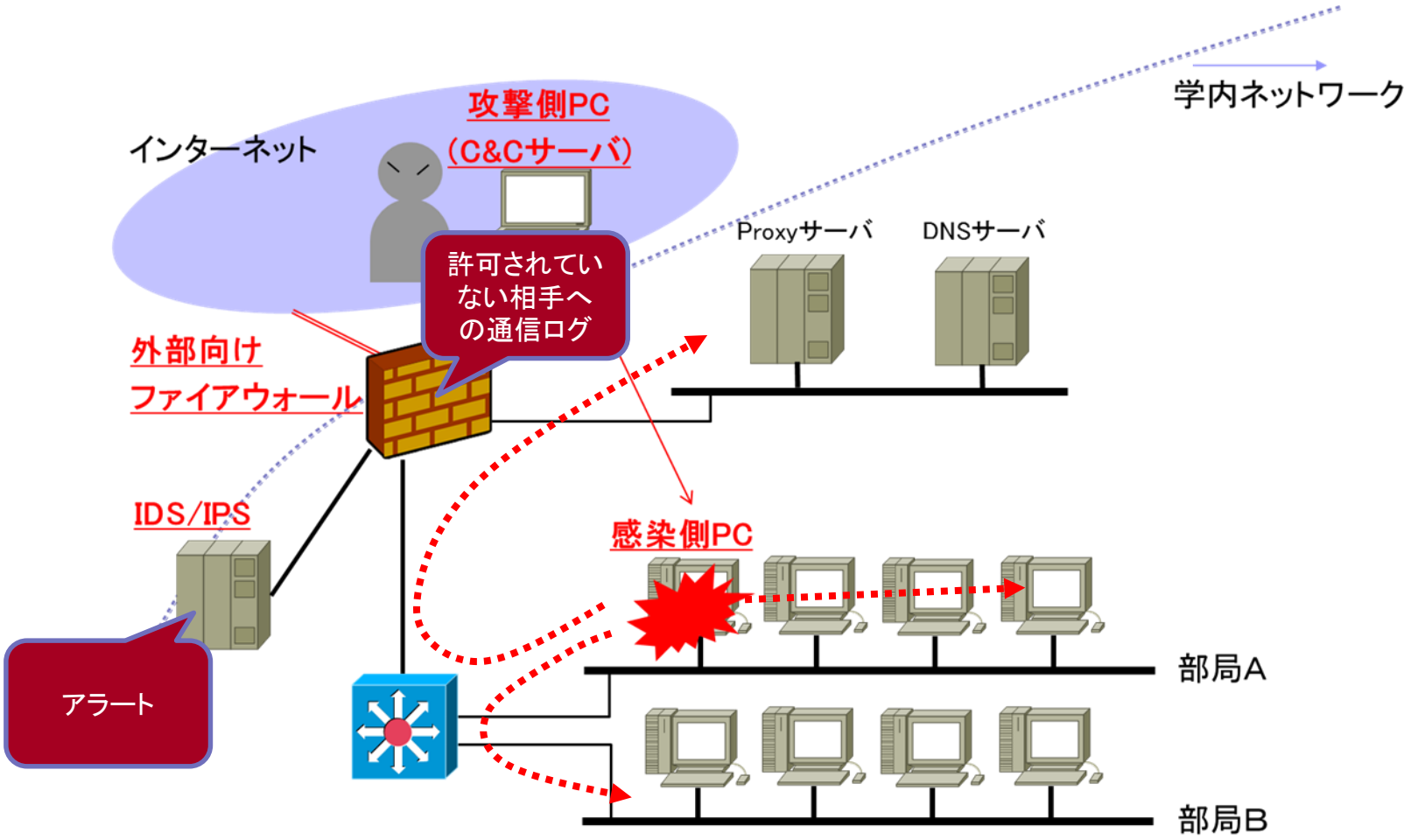
「基盤構築」とその痕跡

- 「C&Cサーバ」と「感染側PC」の通信の痕跡を探す



「内部侵入・調査」とその痕跡

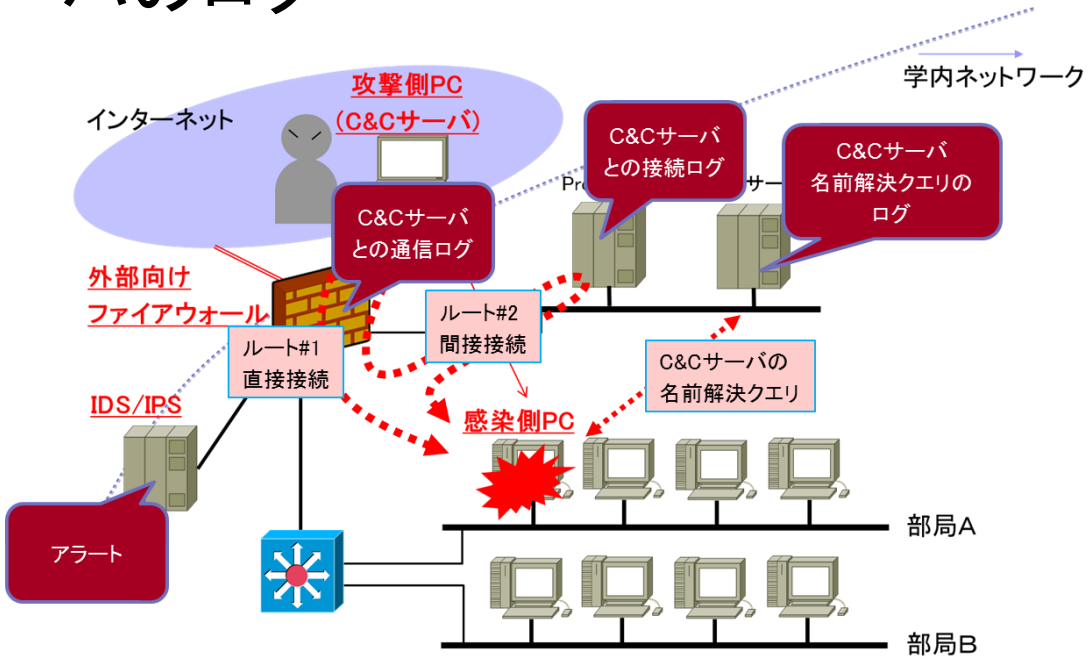
- 内部システムの不審な通信の痕跡を探す



1.「基盤構築」の痕跡調査

ネットワークレベルで行える痕跡調査

- ファイアウォール
  - マルウェアに感染したPCからC&Cサーバへの通信
  - ブラウジング中、マルウェアに感染したPCから、ダウンロードサイトへの通信
- IDS/IPSのアラート
- Proxyサーバのログ



ファイアウォールでの痕跡調査（1）

- セッションの確認
  - C＆Cサーバとのセッション
    - 現在、C&Cサーバと接続中の端末はあるか？

Output

```
pfTop: Up State 1-72/72, View: default, Order: bytes
PR    D SRC                  DEST                 STATE   AGE   EXP  PKTS BYTES
tcp   I 192.168.1.2:1048     10.10.10.2:80         4:4    720 86400  159K  104M
tcp   O 192.168.1.2:1048     10.10.10.2:80         4:4    720 86400  159K  104M
tcp   I 192.168.1.200:1232   10.10.10.2:3389       4:4    873 86400 19248   12M
tcp   O 192.168.1.200:1232   10.10.10.2:3389       4:4    873 86400 19248   12M
tcp   O 127.0.0.1:33842      127.0.0.1:6379        4:4   1148 86400 15687 1031K
tcp   I 127.0.0.1:33842      127.0.0.1:6379        4:4   1148 86400 15687 1031K
tcp   I 192.168.1.2:1046     192.168.1.1:80        9:9    758     7   419  127K
tcp   I 192.168.1.2:1047     192.168.1.1:80        9:9    748    26   406  116K
tcp   I 192.168.1.2:1049     192.168.1.1:80        4:4    658 86397   367  107K
tcp   I 192.168.1.2:1205     192.168.1.1:80        4:4     43 86400   123 47786
tcp   I 192.168.1.2:1171     192.168.1.1:3000      9:9     83     7    51 40093
tcp   I 192.168.1.2:1195     192.168.1.1:3000      9:9     61    29    46 39653
tcp   I 192.168.1.2:1149     192.168.1.1:80        4:4     98 86392    71 21523
```

ファイアウォールでの痕跡調査（2）

- 通信ログの確認
  - C&Cサーバへの接続痕跡
    - 現在あるいは過去に、C&Cサーバへの接続はあるか？

Firewall Logs

Act	Time	IF	Source	Destination
✔	Aug 8 08:45	LAN	192.168.1.2	10.10.10.2:80
✖	Aug 8 08:45	lo0	127.0.0.1	127.0.0.1:6379
✖	Aug 8 08:45	LAN	192.168.1.1	192.168.1.10:1611
✔	Aug 8 08:45	LAN	192.168.1.2	10.10.10.2:80
✖	Aug 8 08:44	lo0	127.0.0.1	127.0.0.1:6379

ファイアウォールの通信ログ（補足）

- 通常Firewallのログには、"Block"や"Reject"された通信のみを残す
  ⇒ ログの量が多くなるため、"Pass"の記録は残さない

- しかしC&Cサーバなど、特定の相手との通信を行う内部端末を洗い出したい場合は、その相手との通信のみ記録を残す設定が有効

IDS/IPSでの痕跡調査（1）

- 一部のRATによる通信については、検知可能
  - Emdivi　（Snortで検知可（ルール化済み））
  - 暗号化(https)されると検知は困難

- 次世代ファイアウォール
  - アプリケーションの識別
  - ふるまい検査

IDS/IPSでの痕跡調査（2）

Snort Alerts

Interface/Time	Src/Dst Address	Description
LAN Aug 08 09:11:24	192.168.1.200:1149 10.10.10.2:80	(http_inspect) UNESCAPED SPACE IN HTTP URI
LAN Aug 08 09:05:54	192.168.1.200:1149 10.10.10.2:80	ET ATTACK_RESPONSE Possible MS CMD Shell opened
LAN Aug 08 08:54:17	10.10.10.2:80 192.168.1.200:1149	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-
LAN Aug 08 08:54:07	192.168.1.200:1149 10.10.10.2:80	(http_inspect) BARE BYTE UNICODE ENCODING
LAN Aug 08 08:54:07	192.168.1.200:1149 10.10.10.2:80	ET TROJAN Bozok.RAT checkin

C&Cサーバから CMD shellを起動されたことを検知

遠隔操作ツール(Bozok)を用いたC&Cサーバとの接続を検知

IDS/IPSで痕跡調査を行う上での注意

- C&Cサーバとの通信は「正常なもの」とみなされる場合が多い
  - HTTP、HTTPSに偽装
  - 通信を暗号化
    ⇒　IDS/IPSで検知できないことが多い。
- 誤検知への対応
  - 運用中のチューニングが必要

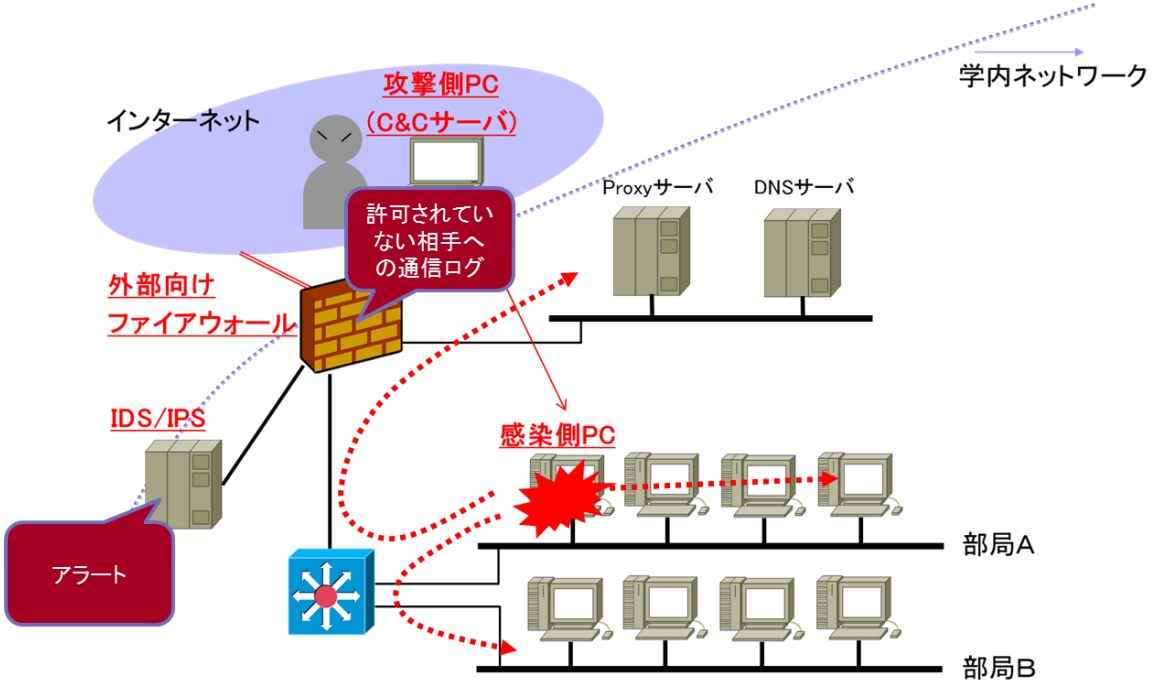
Proxyサーバでの痕跡調査

- マルウェアに感染したPCから、C&Cサーバへの通信
  - マルウェアに感染したPCがC&Cサーバやダウンロードサイトへの通信を試みている
- CONNECTメソッドで、80,443以外のポートへの通信
  - HTTPやHTTPS通信を偽装し、組織外との通信を試みている
- 標準利用以外のUser Agentによる通信。
  - マルウェアに感染したPCがC&Cサーバやダウンロードサイトへの通信を試みている
- 定期的に発生するHTTP通信
  - マルウェアに感染したPCがC&Cサーバと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ている
- 業務時間外に発生するHTTP通信
  - マルウェアに感染したPCが変則的な時間帯にC&Cサーバへの通信を試みている
- 大量のHTTP通信
  - マルウェアに感染したPCが、C&Cサーバやアップロードサイトへの通信を試みている
  - 組織内機密ファイル等が、学外へ流出している兆候

２.「内部侵入・調査」の痕跡調査

ネットワークレベルで行える痕跡調査

- ファイアウォール
  - マルウェアに感染したPCからの不審な内部通信
- IDS/IPSのアラート



ファイアウォールでの痕跡調査

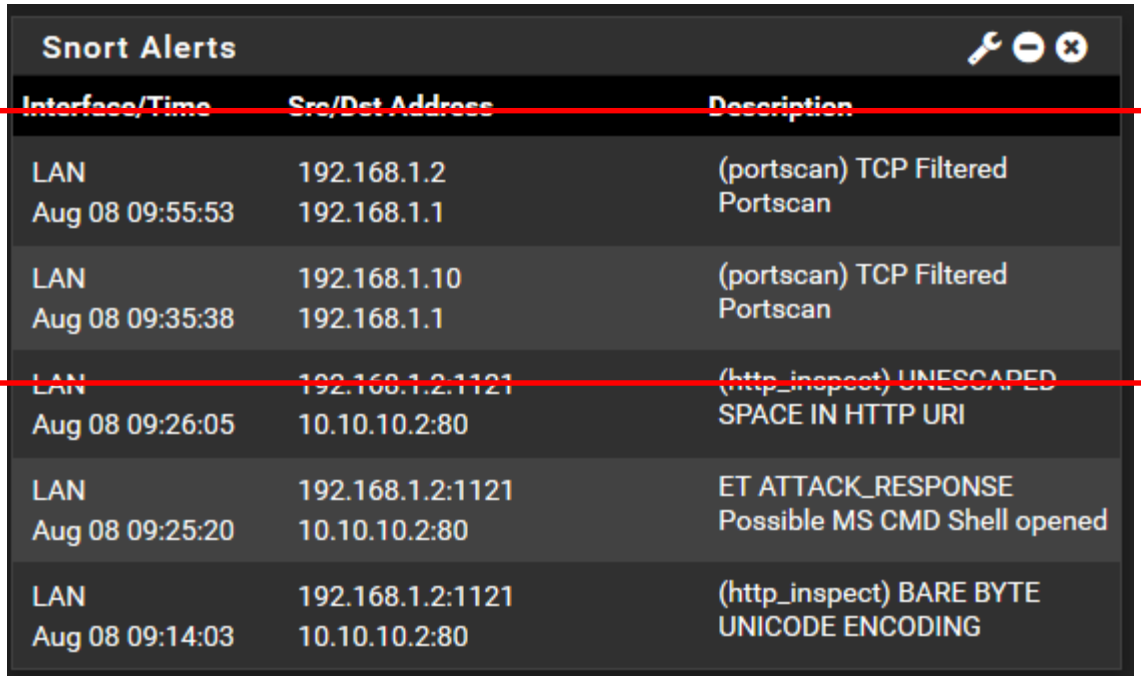
- 内部から内部への不審な通信
  - 「端末間での侵害拡大」、「サーバへの侵入」の痕跡
    - Pass the Hash等

    ⇒内部で許可されていない通信を、Firewallの通信ログから検知

IDS/IPSでの痕跡調査

- 内部から内部への不審な通信
  - 「ネットワークの調査」の痕跡
    - ポートスキャン等

    ⇒通常、内部ではありえない通信をIDS/IPSのアラートで検知



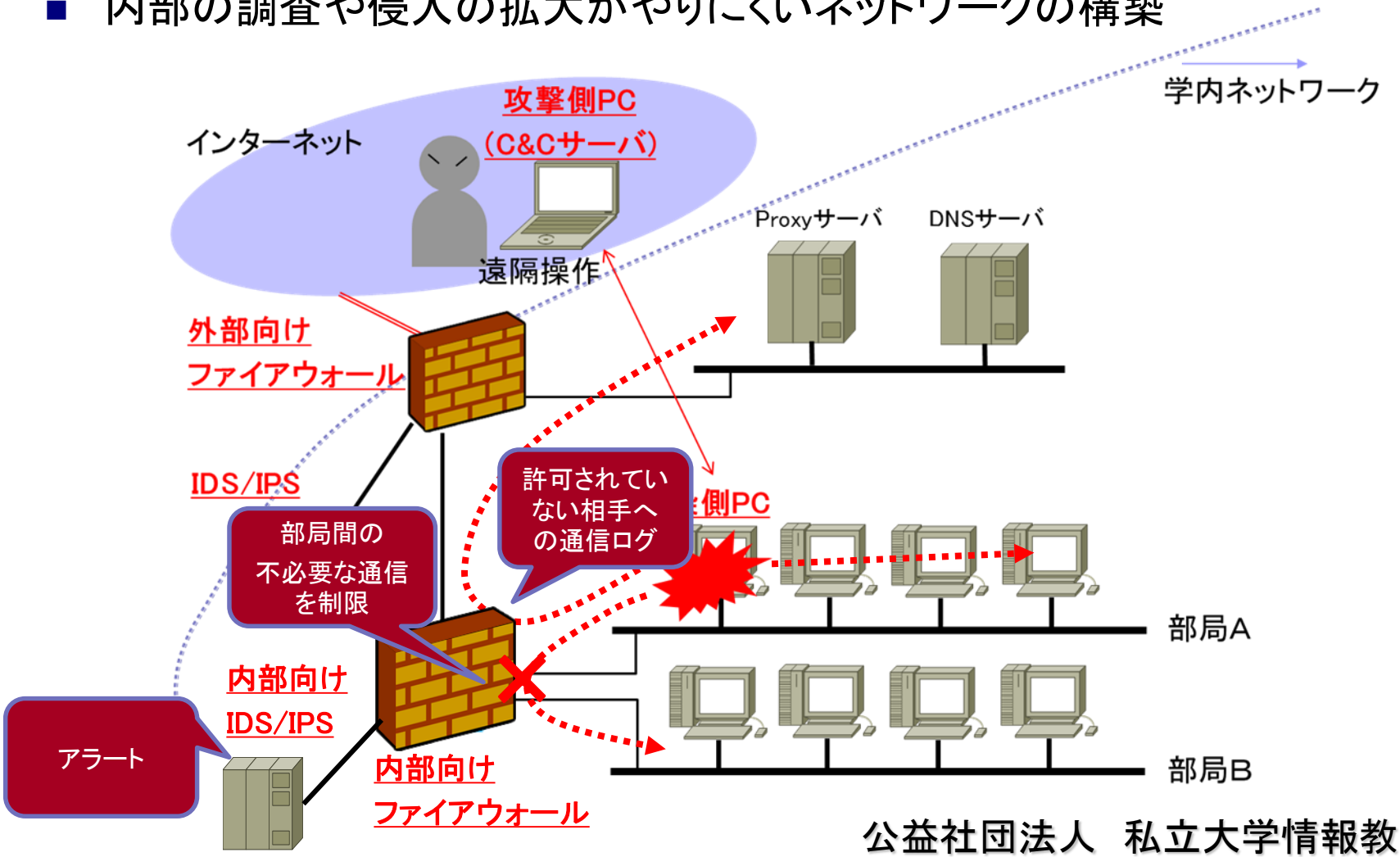
Snort Alerts

Interface/Time	Src/Dst Address	Description
LAN Aug 08 09:55:53	192.168.1.2 192.168.1.1	(portscan) TCP Filtered Portscan
LAN Aug 08 09:35:38	192.168.1.10 192.168.1.1	(portscan) TCP Filtered Portscan
LAN Aug 08 09:26:05	192.168.1.2:1121 10.10.10.2:80	(http_inspect) UNESCAPED SPACE IN HTTP URI
LAN Aug 08 09:25:20	192.168.1.2:1121 10.10.10.2:80	ET ATTACK_RESPONSE Possible MS CMD Shell opened
LAN Aug 08 09:14:03	192.168.1.2:1121 10.10.10.2:80	(http_inspect) BARE BYTE UNICODE ENCODING

内部から内部への
ポートスキャンを検知

内部用ファイアウォール、IDS/IPSの導入

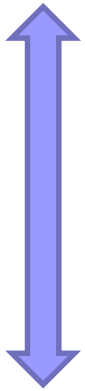
- 「内部侵入・調査」の兆候をいち早く検知
- 内部の調査や侵入の拡大がやりにくいネットワークの構築



３．ネットワークレベルでの対応

ネットワークレベルでの対応例

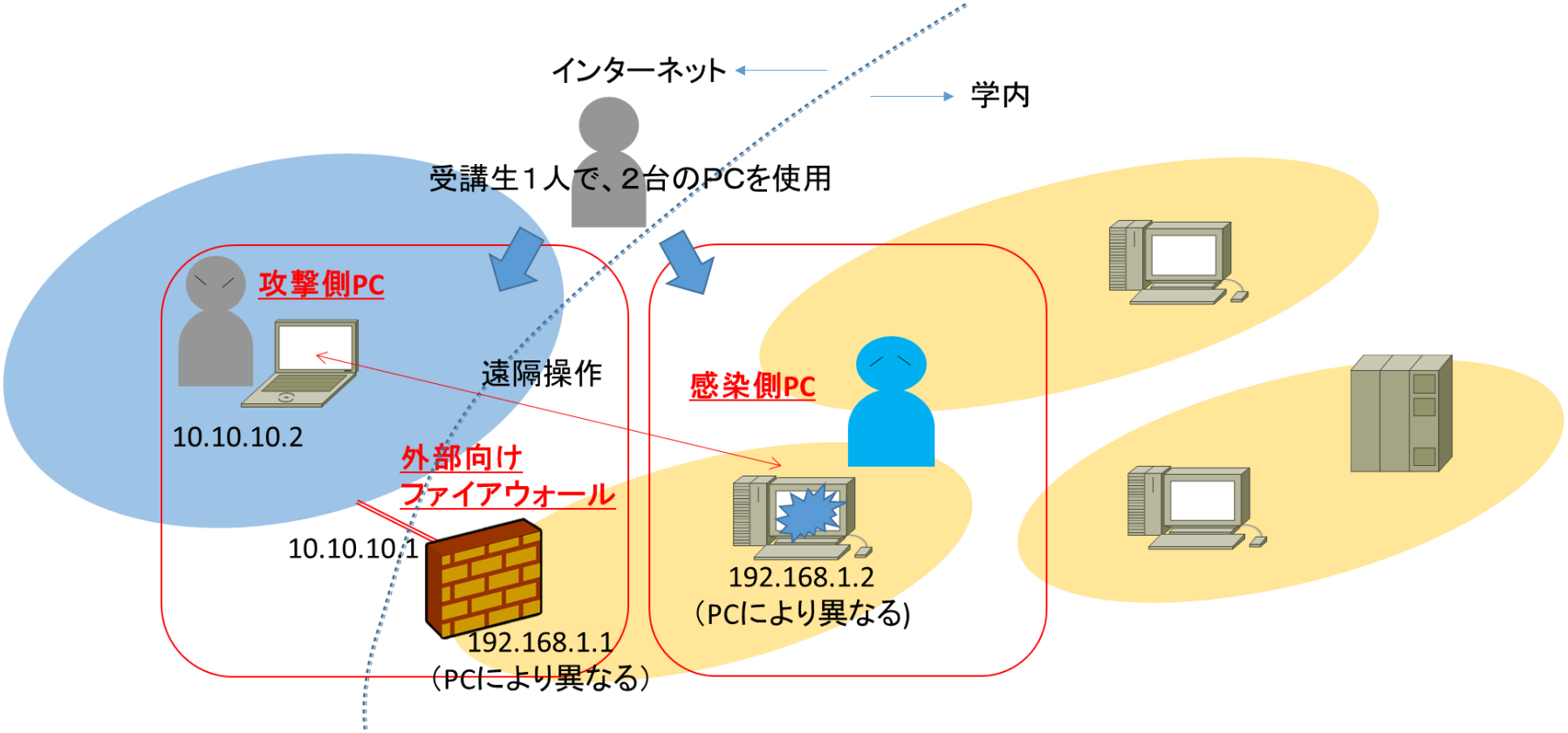
対応の
レベル感



- 外部ネット接続ケーブルの抜線
- 外部向けファイアウォール
  - 外部との接続を「すべて」遮断
  - 外部との接続を「一部のサービス（例：メール）」を除き遮断
  - C&Cサーバとの通信「のみ」を遮断
- 内部用ファイアウォール（導入済の場合）
  - 重要サーバへの通信の監視強化、通信制限
  - ネットワークの分離設計とアクセス制御の実施
    →【参考】『高度標的型攻撃』対策に向けたシステム設計ガイド（IPA）

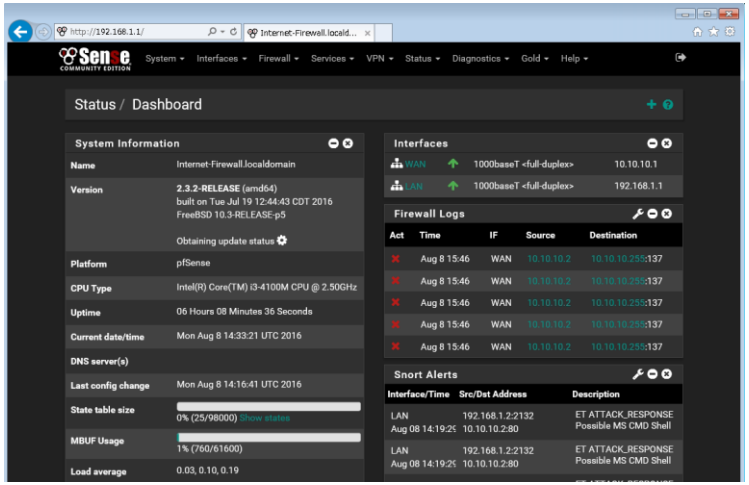
実習

実習のネットワークモデル



仮想ファイアウォールについて

- pfSense
  - オープンソースで配布されているファイアウォール（FreeBSDベース）
  - 豊富なセキュリティ機能
    - ファイアウォール、IDS/IPS(Snort)、Proxy(Squid)、ウィルス対策ソフトなどがパッケージ化
    - 機能の追加も容易
  - Webブラウザを用いて設定・管理
  - https://www.pfsense.org/



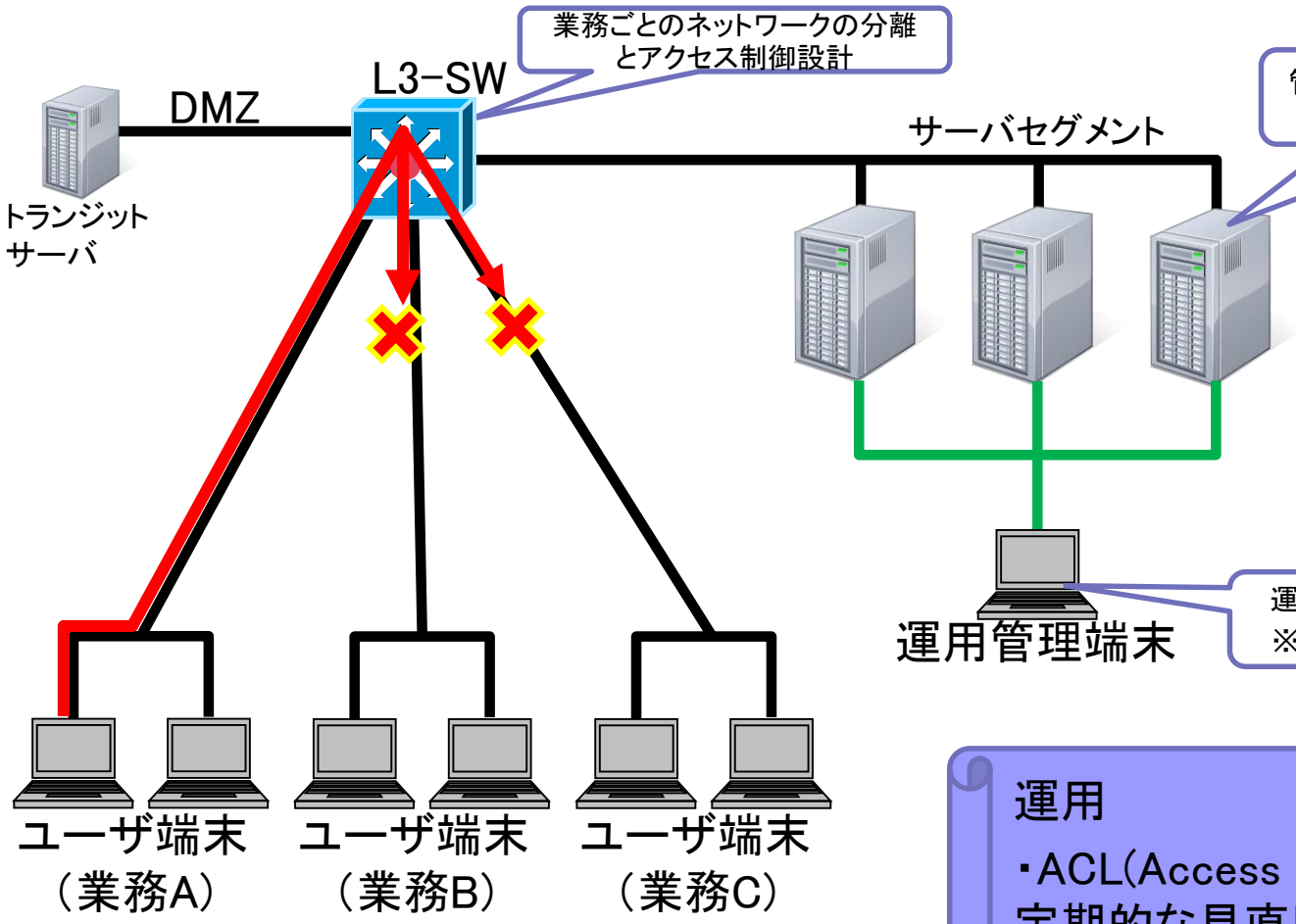
参考

「内部侵入・調査」への対策

- ネットワークレベルの対策
  - ① ネットワークの分離設計とアクセス制御
    - 業務ごとにサブネットを分割
    - ユーザ端末とシステム管理用端末の分離
- 端末レベルの対策
  - ② ユーザ端末間のファイル共有禁止
  - ③ オートコンプリートの禁止
  - ④ キッティング時に設定した共通アカウントの削除
- ドメインレベルの対策
  - ⑤ 管理者権限アカウントのキャッシュ禁止
- 監視の強化
  - ⑥ トラップアカウントによる認証ログの監視と分析

①ネットワークの分離設計とアクセス制御

- 攻撃者の侵入範囲の限定およびサーバへの侵入拡大防止が目的

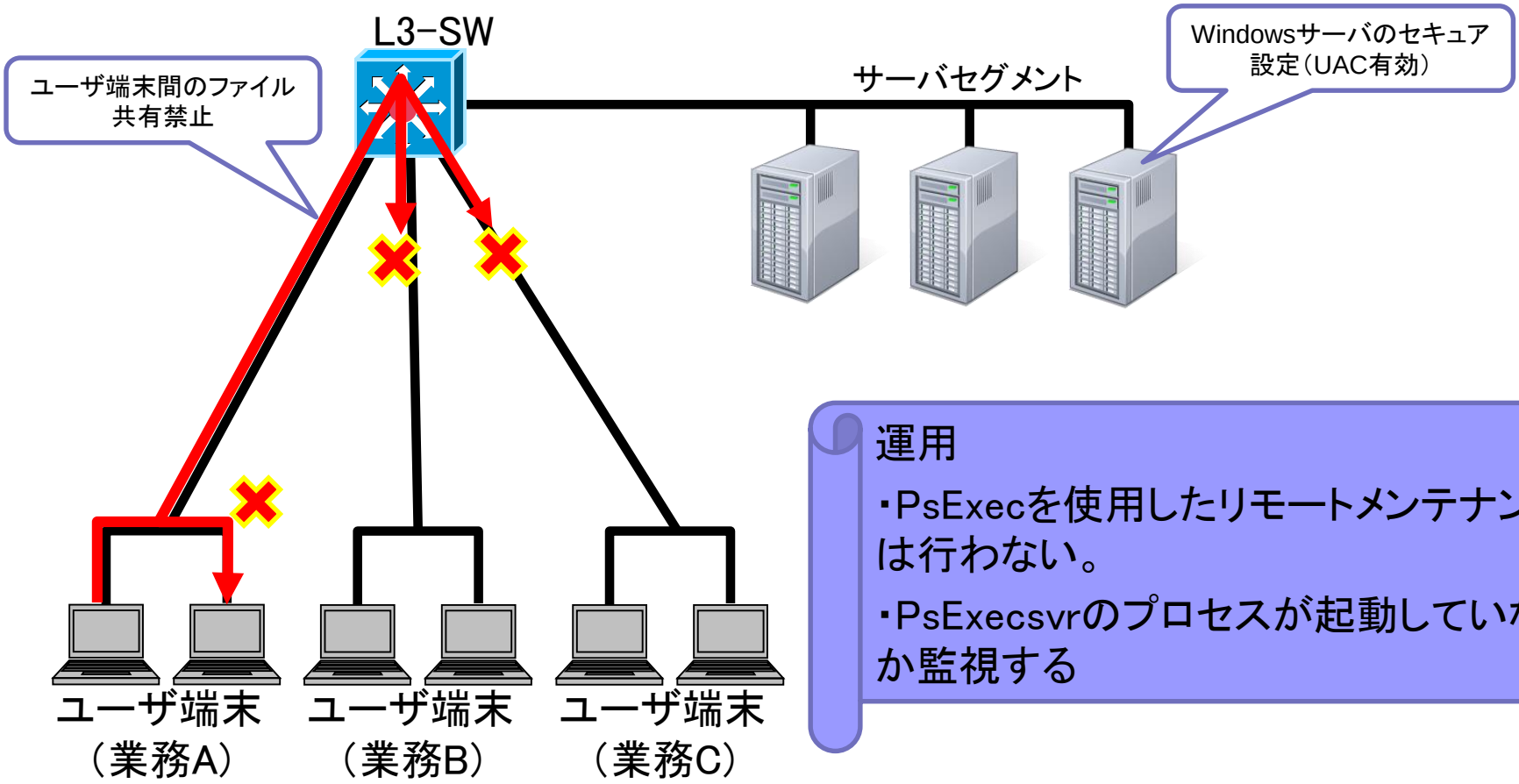


運用

・ACL(Access Control List)の設計と定期的な見直し

②ユーザ端末間のファイル共有禁止

- ユーザ端末から必要な通信先(File Serverなど)に限定したファイル共有を許可することにより、侵入拡大を防止することが目的



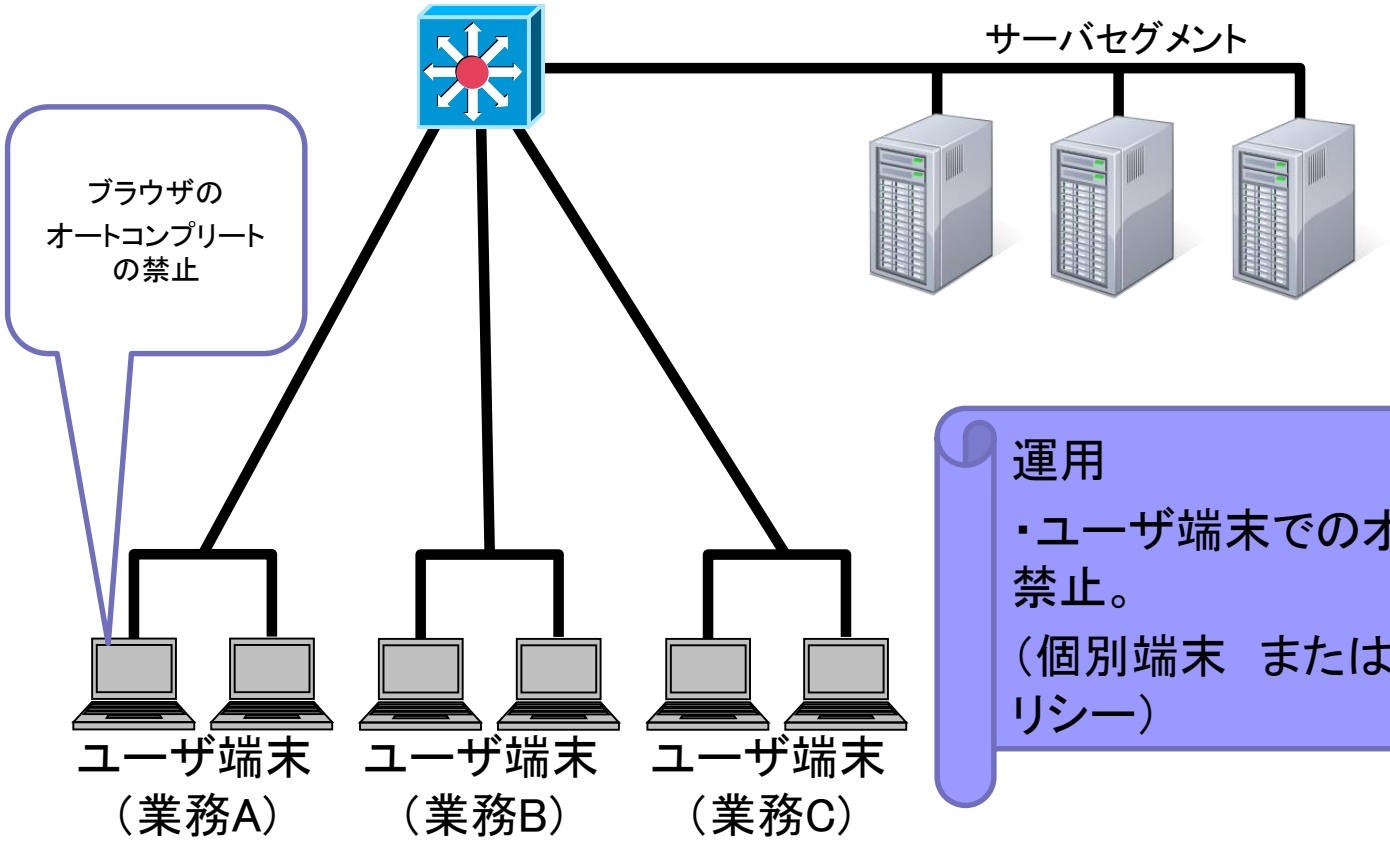
運用

・PsExecを使用したリモートメンテナンスは行わない。

・PsExecsvrのプロセスが起動していないか監視する

③オートコンプリートの禁止

- 認証情報（ID/PW）が端末上に保存されることを抑制。攻撃者に窃取され内部サービスへの侵入拡大を防ぐことを目的



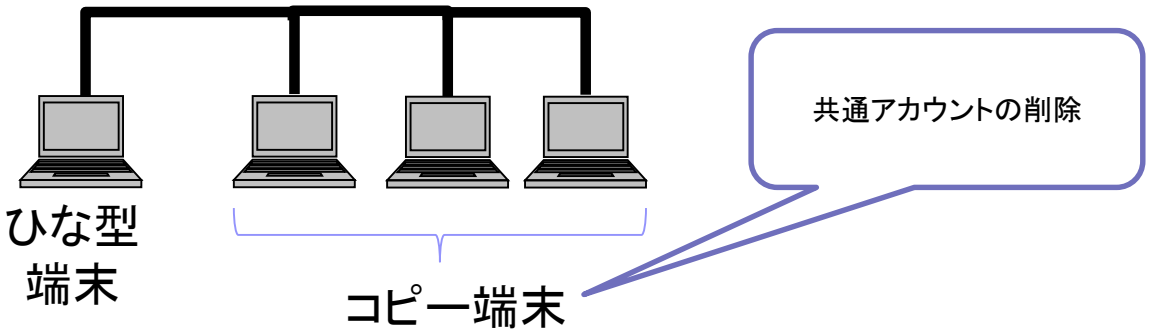
運用

・ユーザ端末でのオートコンプリートを禁止。

（個別端末　または　ADのグループポリシー）

④キッティング時に設定した共通アカウントの削除

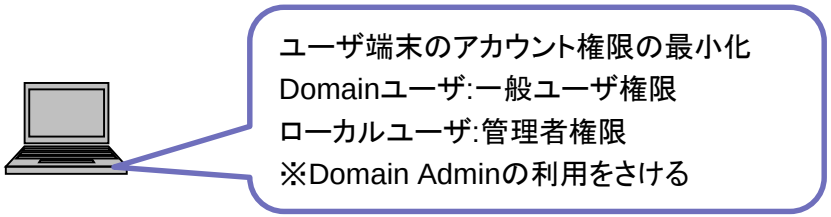
- ひな型を複数のPCに展開する際、同じアカウントがコピーされてしまう。これを削除することにより、Pass the Hash攻撃による他端末への侵入拡大を防ぐことを目的



運用
・共通アカウントを削除

⑤管理者権限アカウントのキャッシュ禁止

- リモートからのパッチ配布などの管理者権限が必要な運用を維持しつつ、各サーバに影響を与えないアカウント運用を実現することを目的



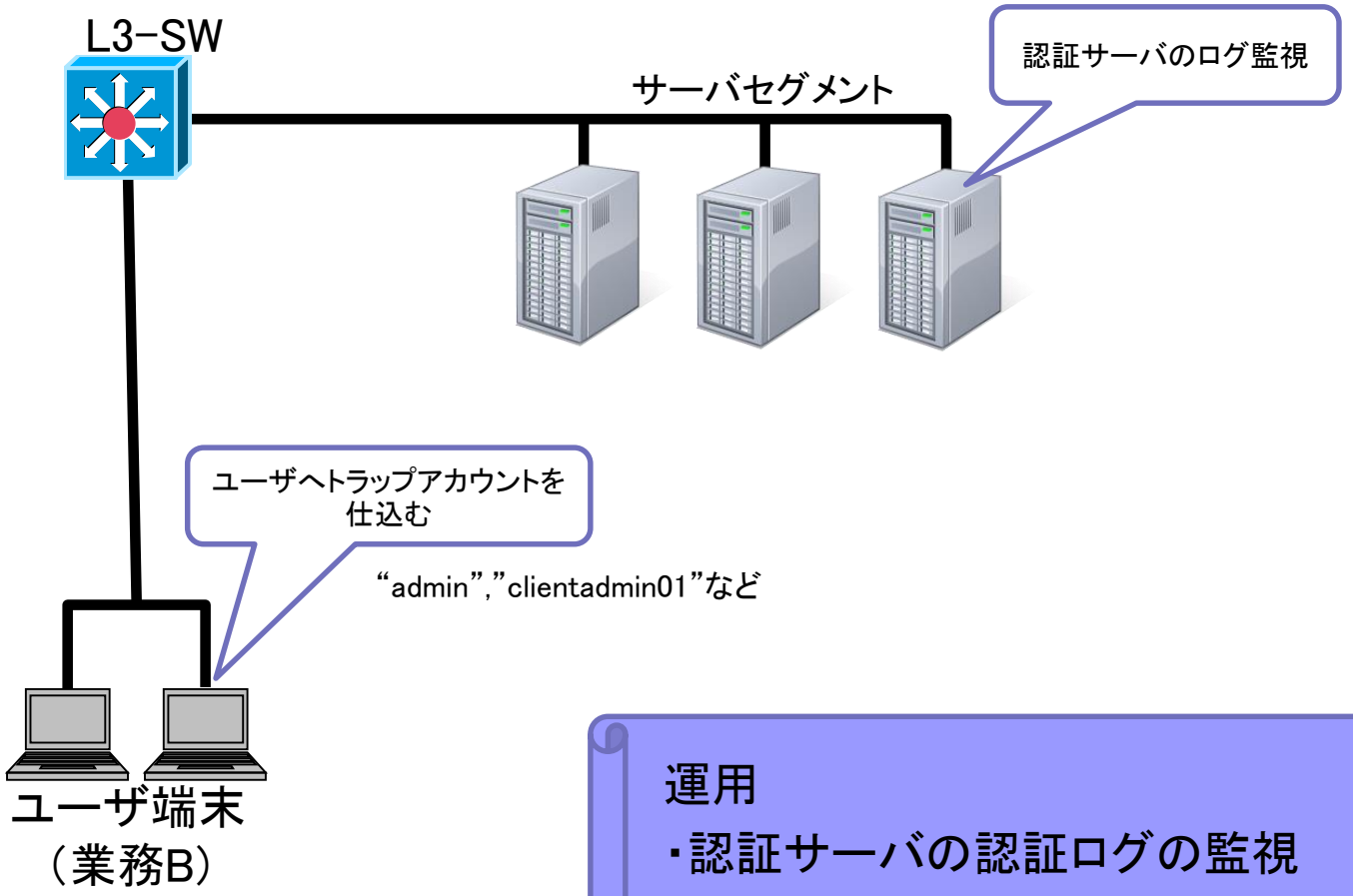
運用

・ユーザ端末でのDomain Adminでログインを禁止。

・ユーザ端末でDomain Adminグループのユーザがログインしていないか定期的に確認。

⑥トラップアカウントによる認証ログの監視と分析

- ユーザ端末上で通常業務で使用しないトラップアカウントを仕込み、重点的に監視を行うことで、不正なアクセスと正常なアクセスを見分けることが目的



運用
・認証サーバの認証ログの監視

参考資料

- JPCERT/CC
  - 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

- IPA
  - 『高度標的型攻撃』対策に向けたシステム設計ガイド
    ～入口突破されても攻略されない内部対策を施す～
    http://www.ipa.go.jp/security/vuln/newattack.html