配布用資料

CyberDefense

最近のサイバー攻撃に対する企業の自己防衛策

2012年1月

サイバーディフェンス研究所
名和 利男

アジェンダ

1. 最近のサイバー攻撃のプロセス

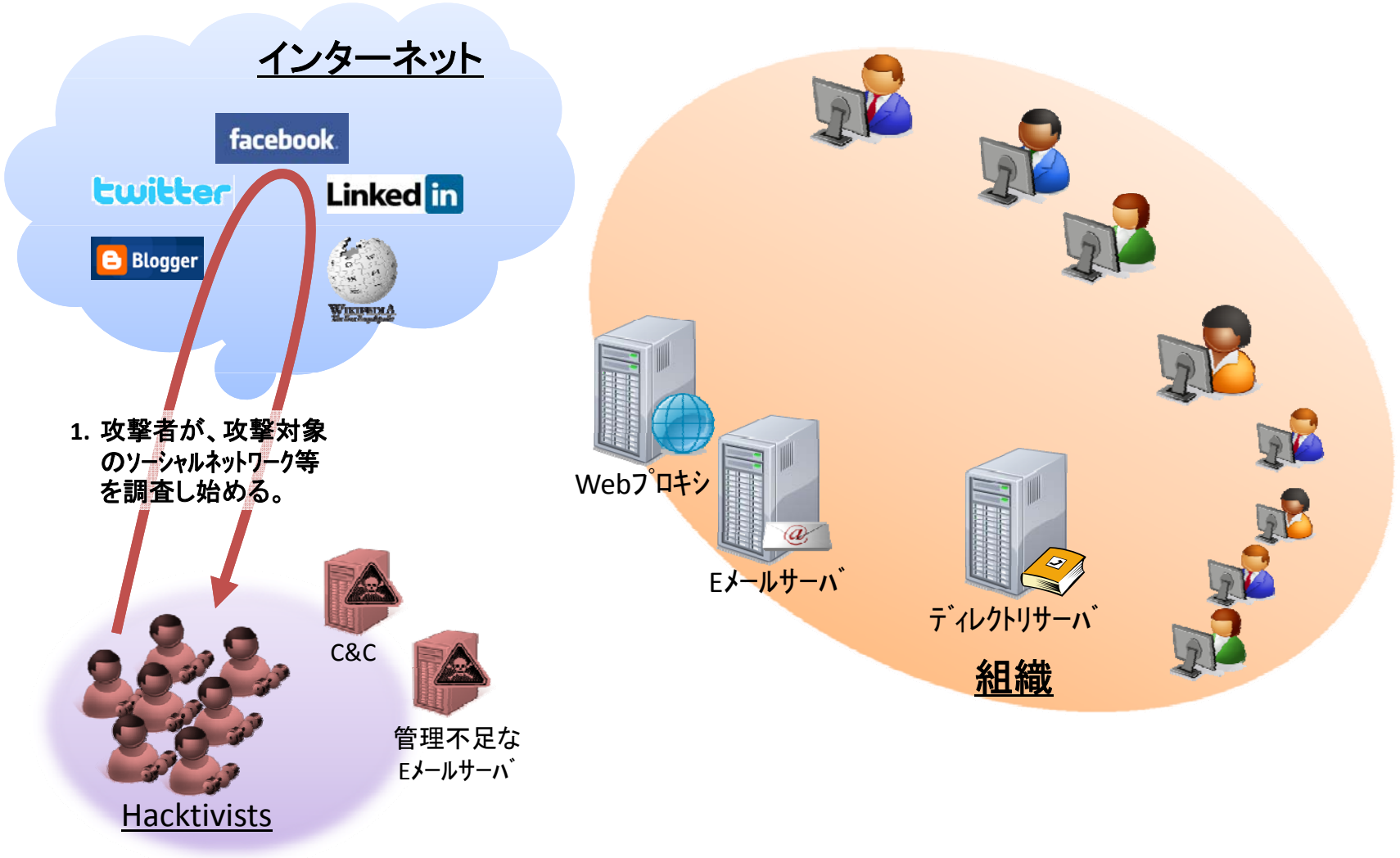
2. 注目すべき事例

3. 求められる防衛策のポイント

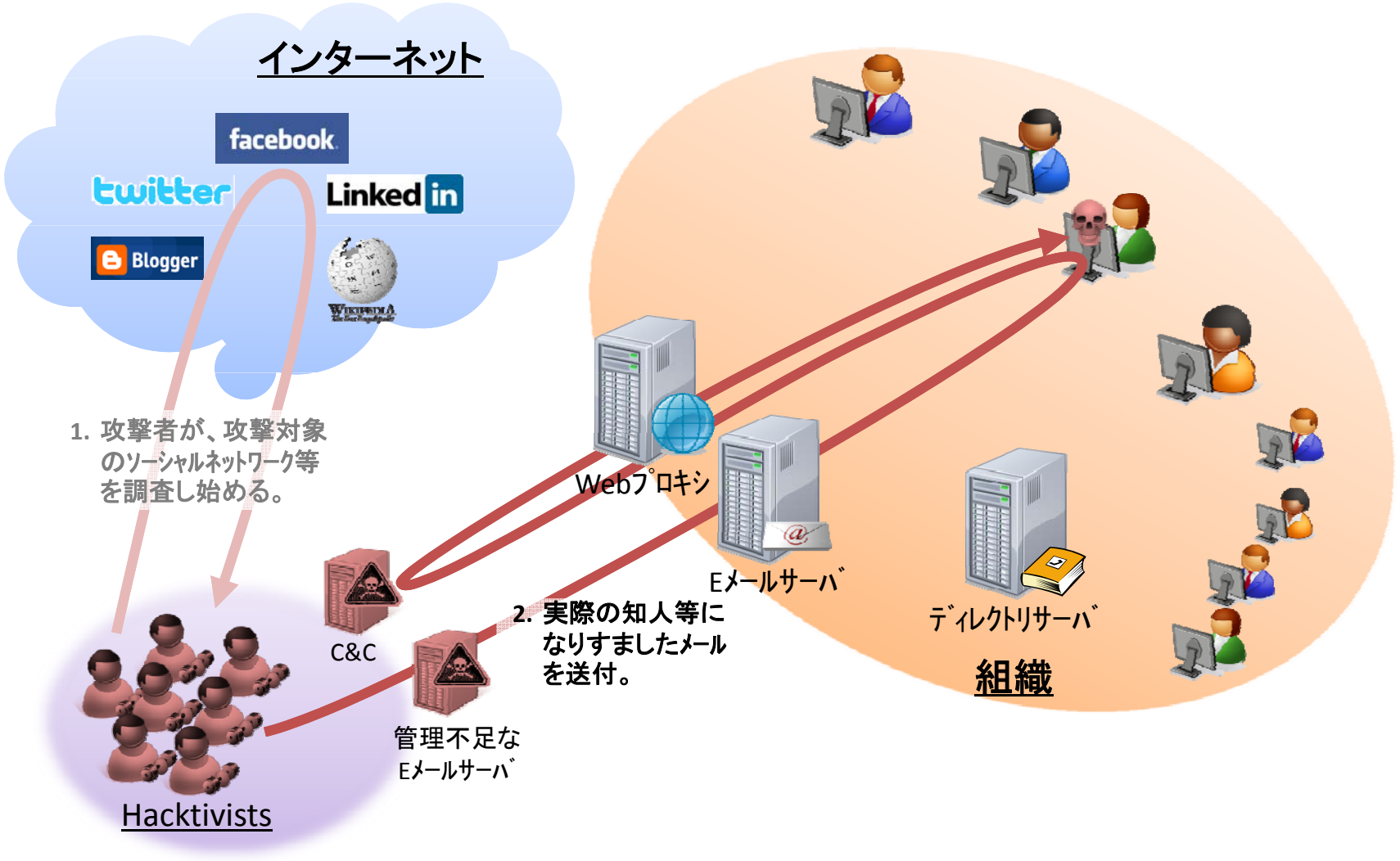
トピック 1

最近のサイバー攻撃のプロセス

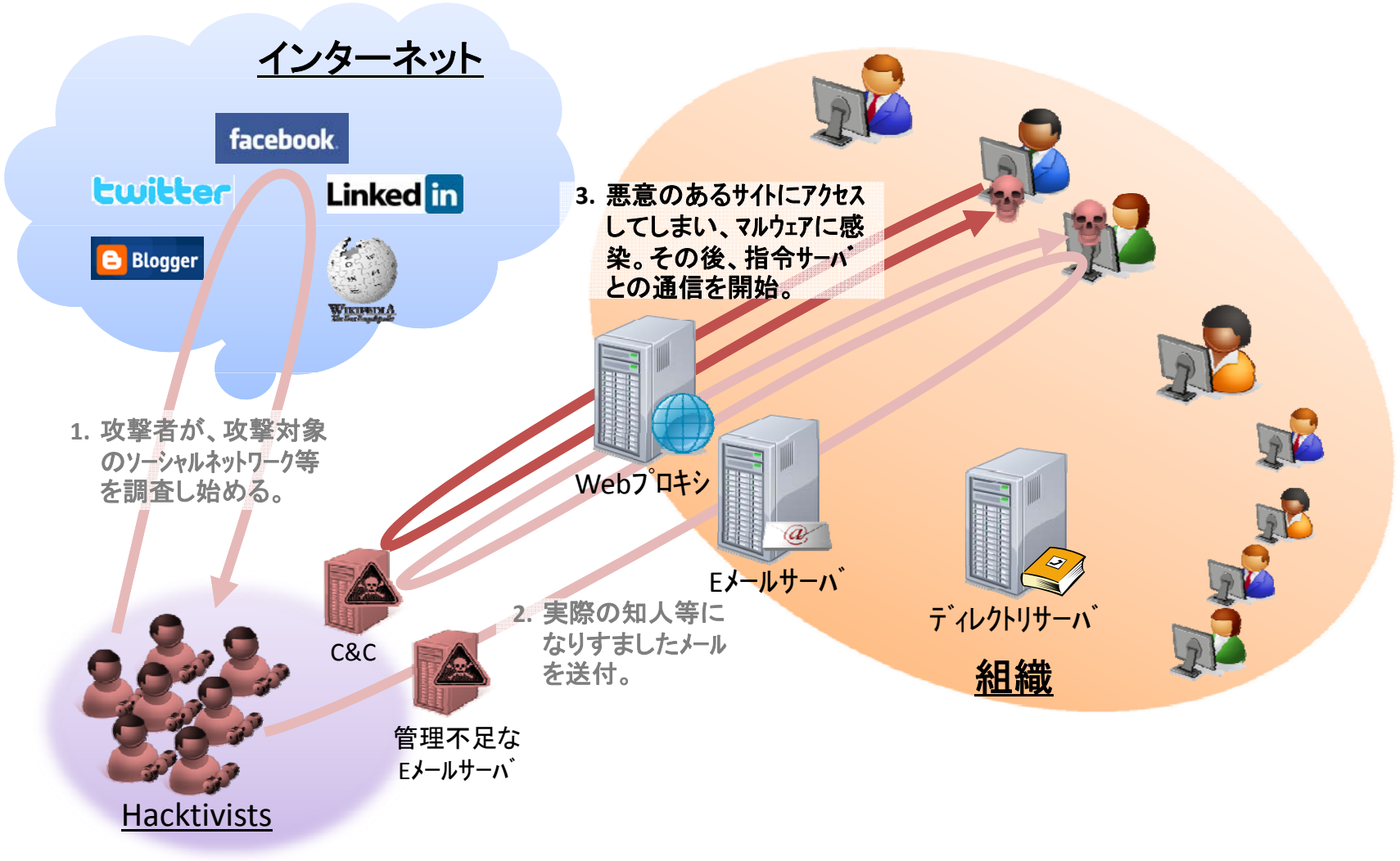
最近のサイバー攻撃のプロセス(1)



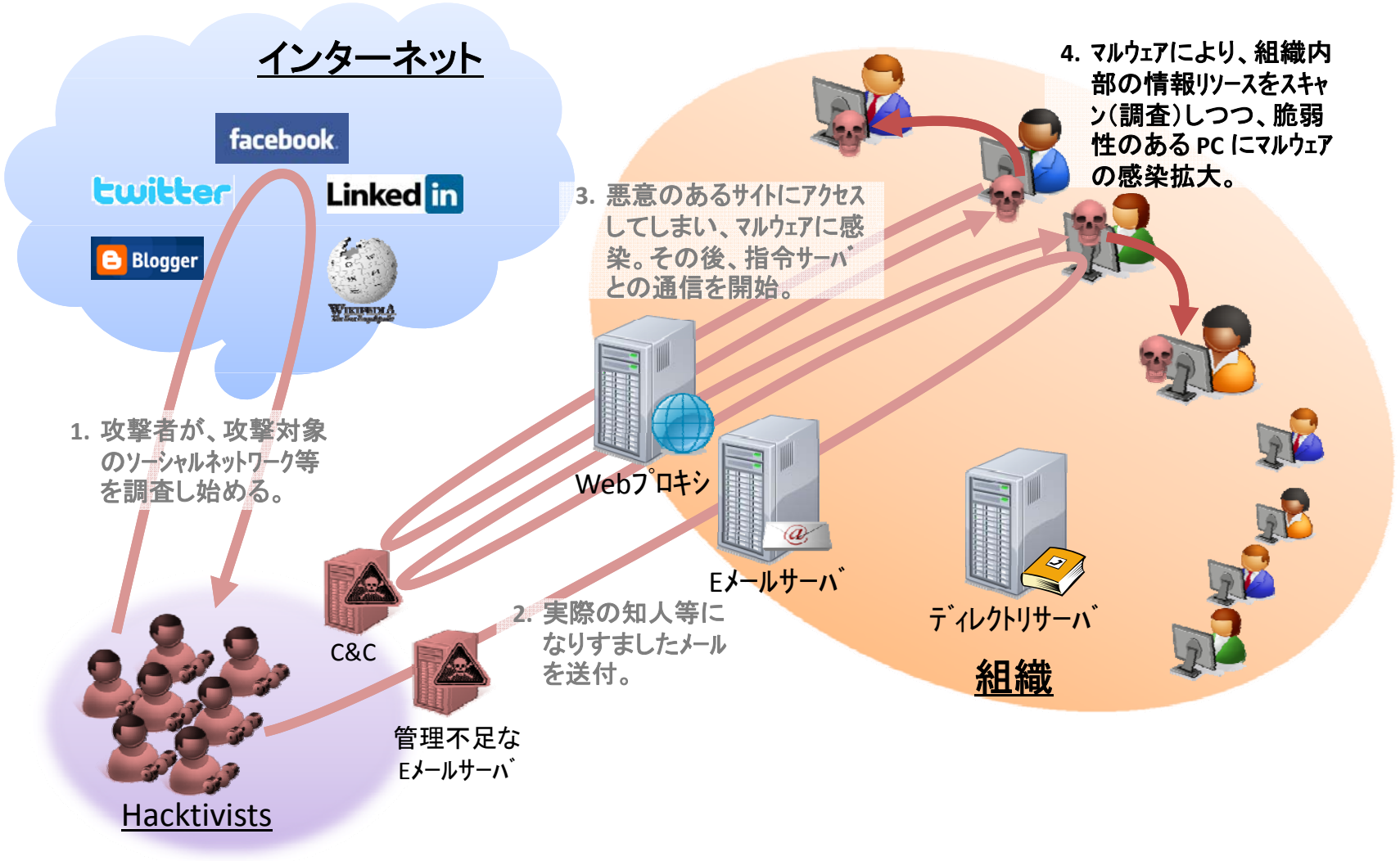
最近のサイバー攻撃のプロセス(2)



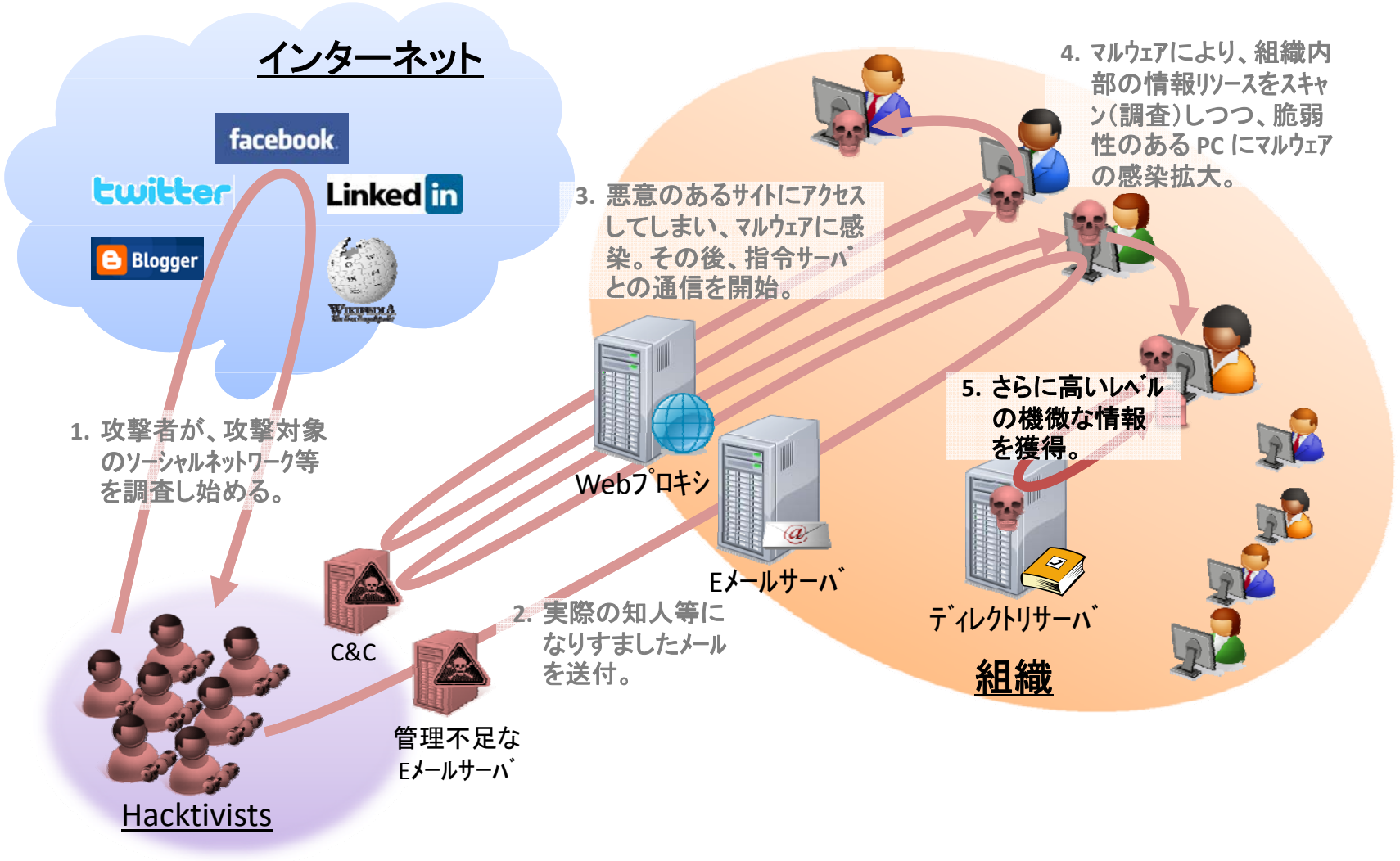
最近のサイバー攻撃のプロセス(3)



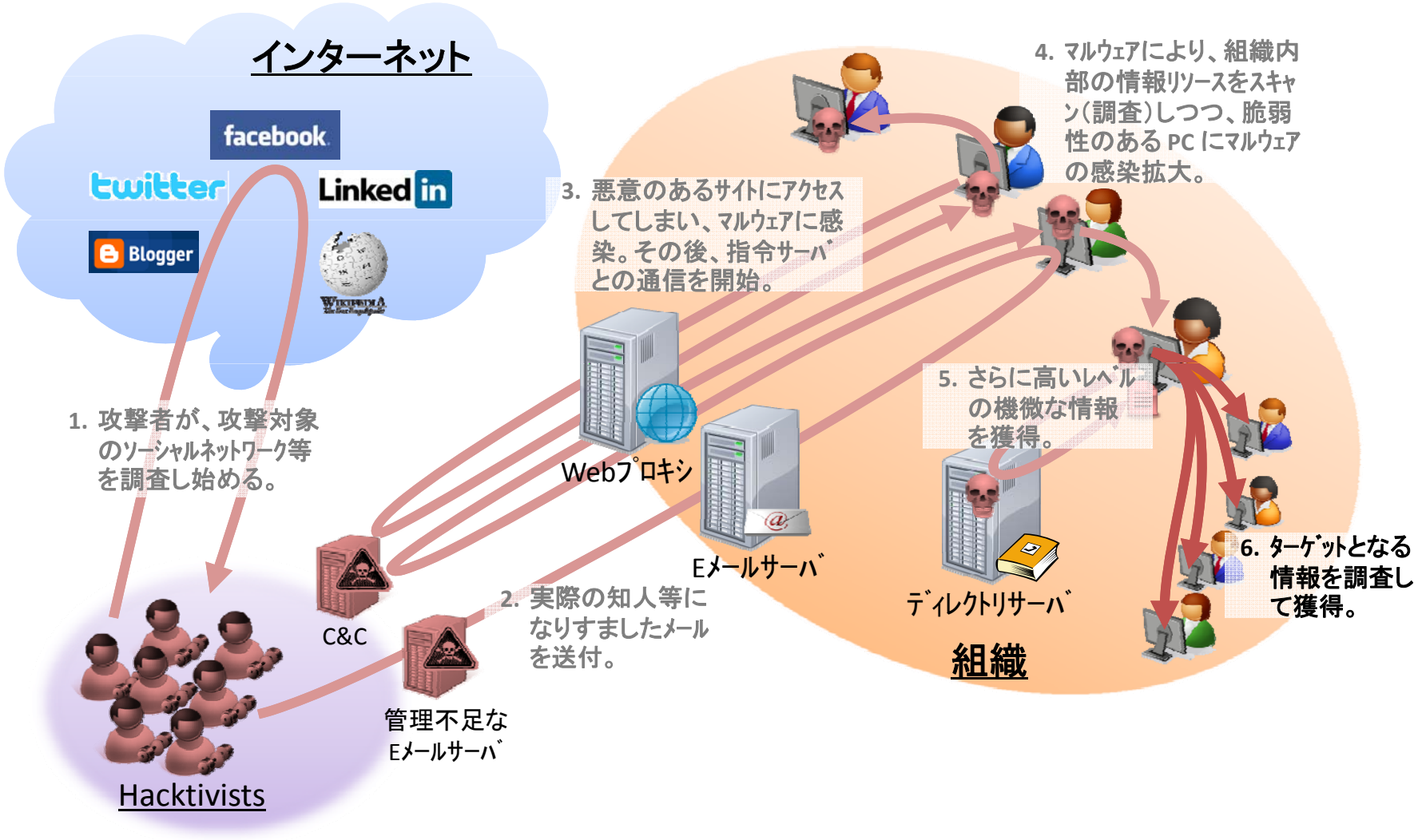
最近のサイバー攻撃のプロセス(4)



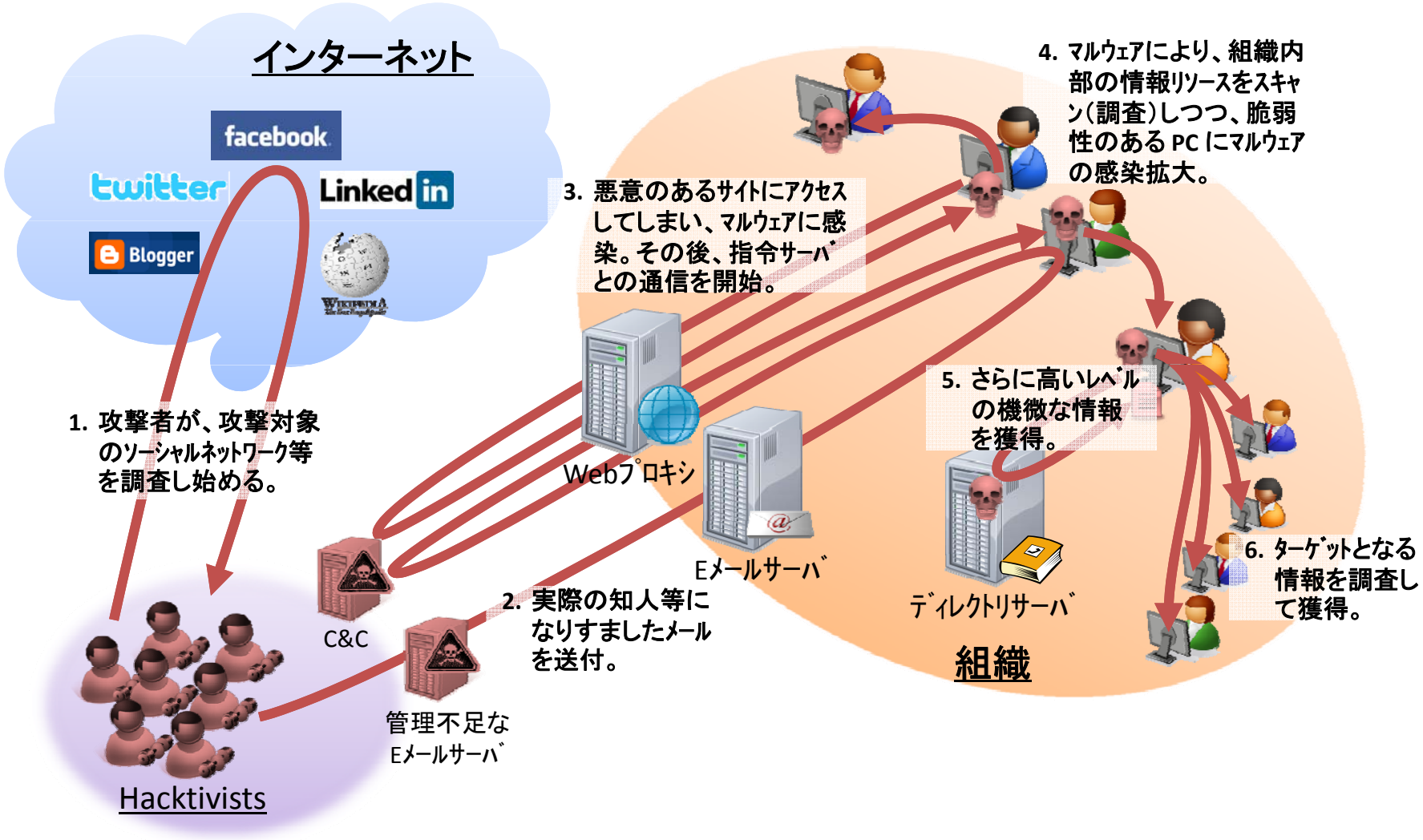
最近のサイバー攻撃のプロセス(5)



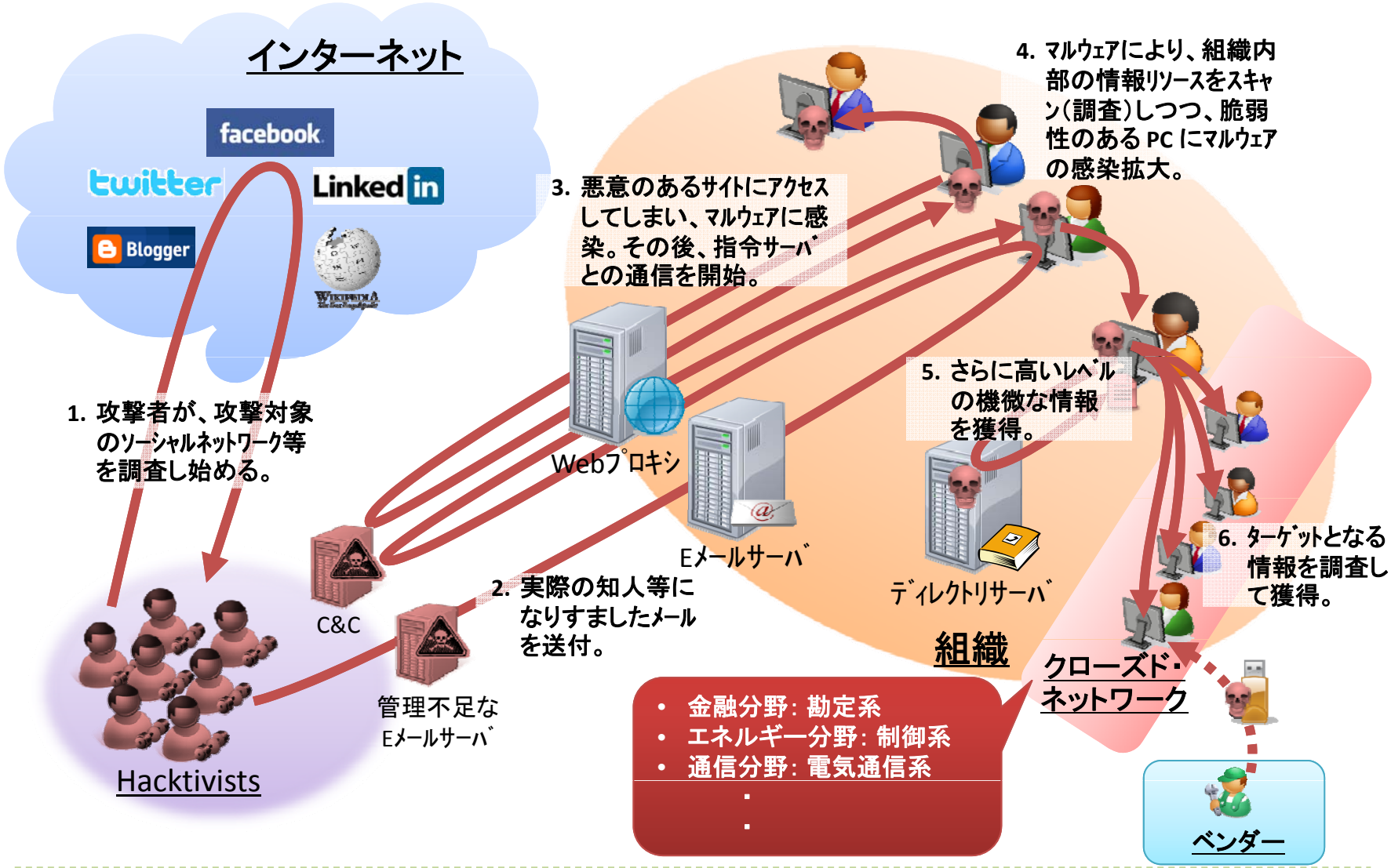
最近のサイバー攻撃のプロセス(6)



最近のサイバー攻撃のプロセス(全体)



今後のサイバー脅威のシナリオ



トピック2

注目すべき事例

配布用資料

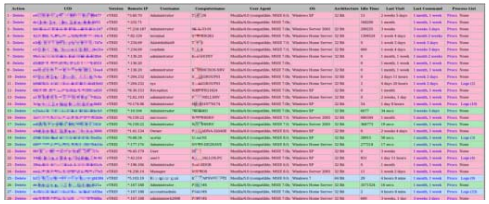
米国におけるPOS端末のマルウェア

【経緯】

- 2012年9月14日、米国書店大手 Barnes & Noble社が、9州63店舗におけるクレジットカード読み取り機（POS端末）が不正な状態にあることを発見。
- FBIは、Barnes & Noble社に対し、捜査のために顧客への連絡はしないように要請。これを受けて、Barnes & Noble社は、カード発行者のみに伝達し、顧客保護の措置を取る。
- 2012年10年23日、New York Times が報道。
  - Credit Card Data Breach at Barnes & Noble Stores
    http://www.nytimes.com/2012/10/24/business/hackers-get-credit-data-at-barnes-noble.html?_r=0
- 2012年10月24年、Barnes & Noble社がプレスリリース。
  - Barnes & Noble Detects Tampering with PIN Pad Devices at Stores
    http://www.barnesandnobleinc.com/press_releases/10_23_12_Important_Customer_Notice.html

【手口】

- 未だ発表なし
  - 専門家の間では、内部関係者がPOSにマルウェアを埋め込む、或いは従業員を騙して、マルウェアをダウンロードさせるサイトのアクセスさせる手口ではないかと推測。
  - 2012年12月12日、POSに感染して内部データを外部送信させるマルウェア Dexter の存在が公表され、本件との関連性を確認中。
    - http://blog.seculert.com/2012/12/dexter-draining-blood-out-of-point-of.html

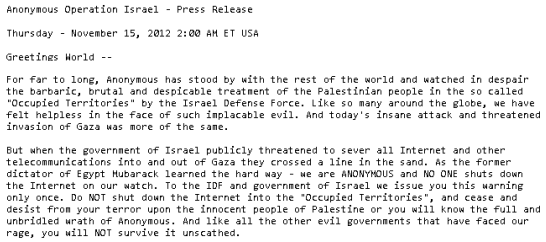


Dexter の管理パネル
（POSシステムからクレジットカードデータを不正入手したものを一覧表示、現在、世界各国で数百台の被害を確認。）

配布用資料

Anonymous によるイスラエルへのサイバー攻撃

- 2012年11月17日、Anonymous は、イスラエルによるガザ攻撃に抗議してイスラエル政府機関や主要銀行の1つの Bank of Jerusalem を含む700以上のサイトに対するサイバー攻撃を行った。
  - アノニマスの一部は、Bank of Jerusalem のデータベース内のデータを削除したと公表した。



Anonymous Operation Israel - Press Release

Thursday - November 15, 2012 2:00 AM ET USA

Greetings World --

For far to long, Anonymous has stood by with the rest of the world and watched in despair the barbaric, brutal and despicable treatment of the Palestinian people in the so called "Occupied Territories" by the Israel Defense Force. Like so many around the globe, we have felt helpless in the face of such implacable evil. And today's insane attack and threatened invasion of Gaza was more of the same.

But when the government of Israel publicly threatened to sever all Internet and other telecommunications into and out of Gaza they crossed a line in the sand. As the former dictator of Egypt Hubarack learned the hard way - we are ANONYMOUS and NO ONE shuts down the Internet on our watch. To the IDF and government of Israel we issue you this warning only once. Do NOT shut down the Internet into the "Occupied Territories", and cease and desist from your terror upon the innocent people of Palestine or you will know the full and unbridled wrath of Anonymous. And like all the other evil governments that have faced our rage, you will NOT survive it unscathed.

http://www.anonpaste.me/anonpaste2/index.php?0c3787b9e504b257#4vuPTzmEXo9+uyq78aSSgvqJgb1nV5DwOZXdau60ajQ=

https://twitter.com/YourAnonNews/status/269558244782006274

http://www.mediafire.com/?hpnne29xvx1ceuv
（OpIsrael.Care.Package.v2.0 ）

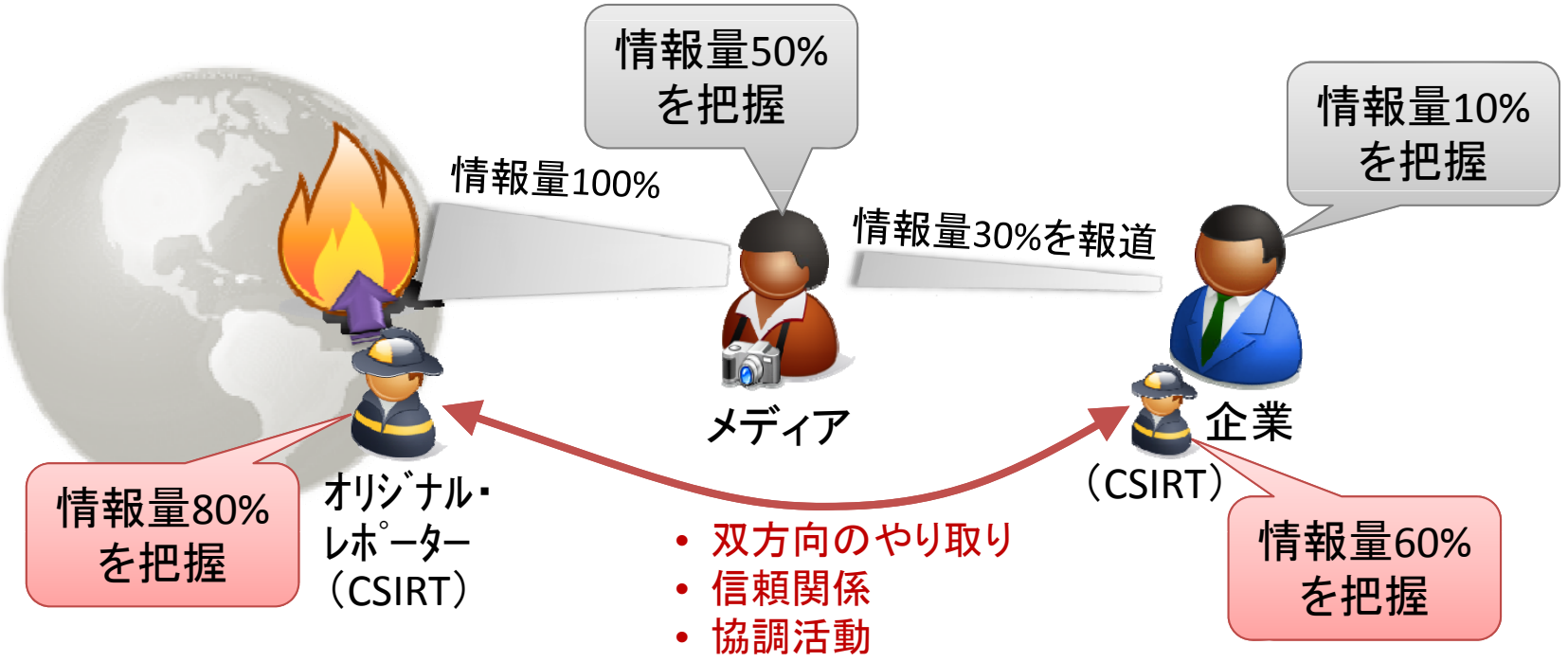
- 2012年11月18日、イスラエルのユバル・シュタイニッツ財務相は、次のように説明した。
  - 4,400万回のサイバー攻撃のうち、侵入に成功したのは1件のみだったが、10分程度で復旧した。
  - 戦時中のサイバー攻撃の標的として最もおかったのは、国防関連サイトであった。
  - 大統領府が1,000万回、外務省が700万回、首相府が300万回の攻撃を受けた。
  - 攻撃元は、イスラエル国内かパレスチナ自治区からだった。
  - ほとんどのサイバー攻撃は、防御できている。
  - 平時でも1日数百万回のさいば一攻撃がある。

トピック 3

求められる防衛策のポイント

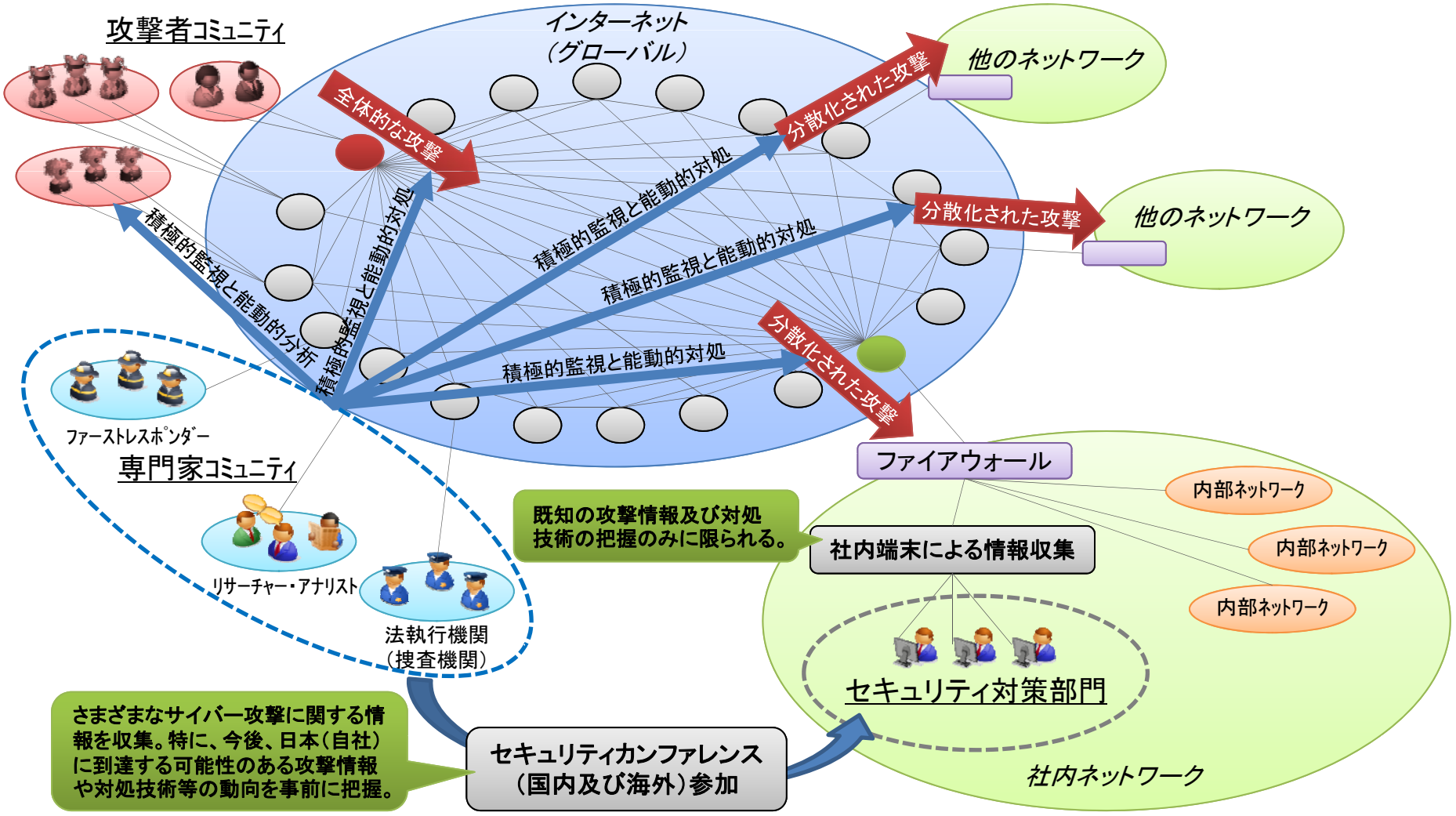
防衛策の「現実的な策定」をするためのポイント(1)

- サイバー空間における**<u>脅威を適切に把握すること</u>**
  - 一般メディア等が発信する情報を鵜呑みにしない
  - オジリナル・レポーター(Original Reporter)が発信する情報を追求する



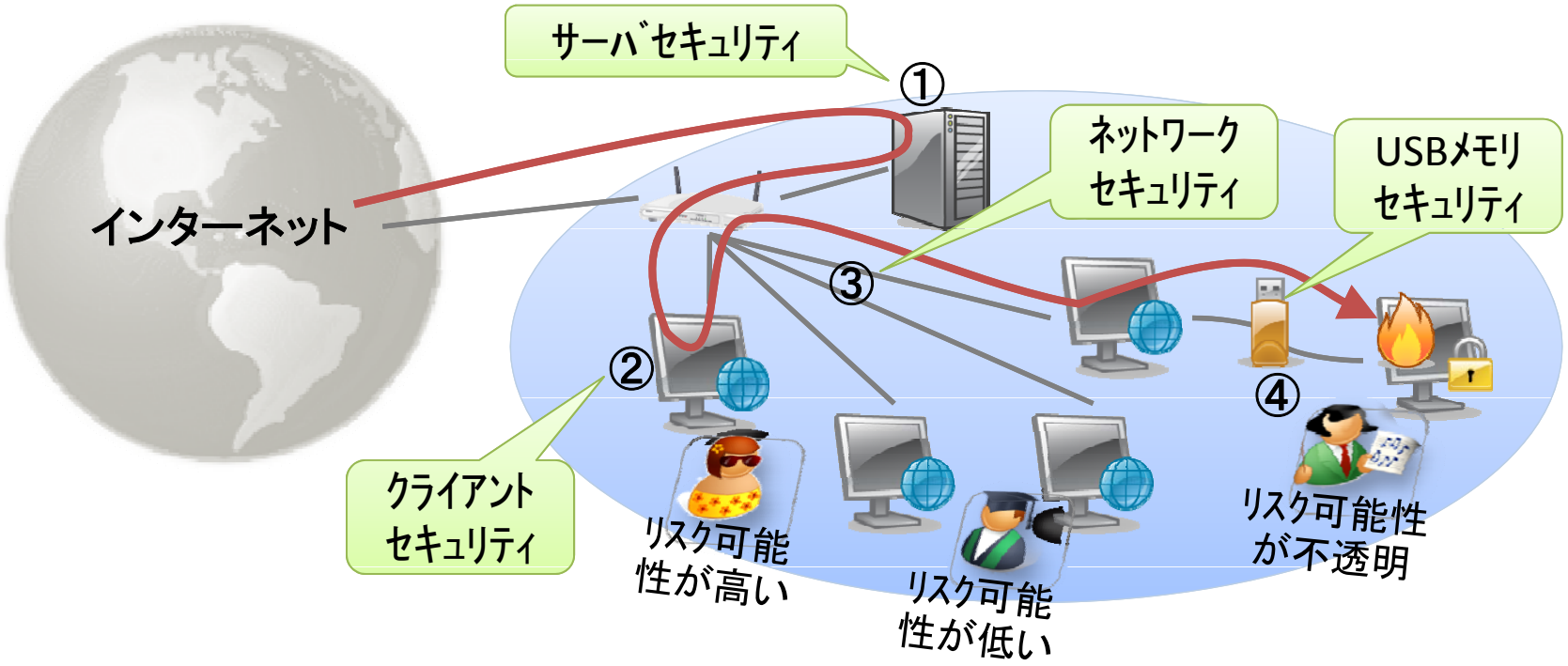
防衛策の「現実的な策定」をするためのポイント(2)

- サイバー空間における**動向情報を積極的に収集すること**



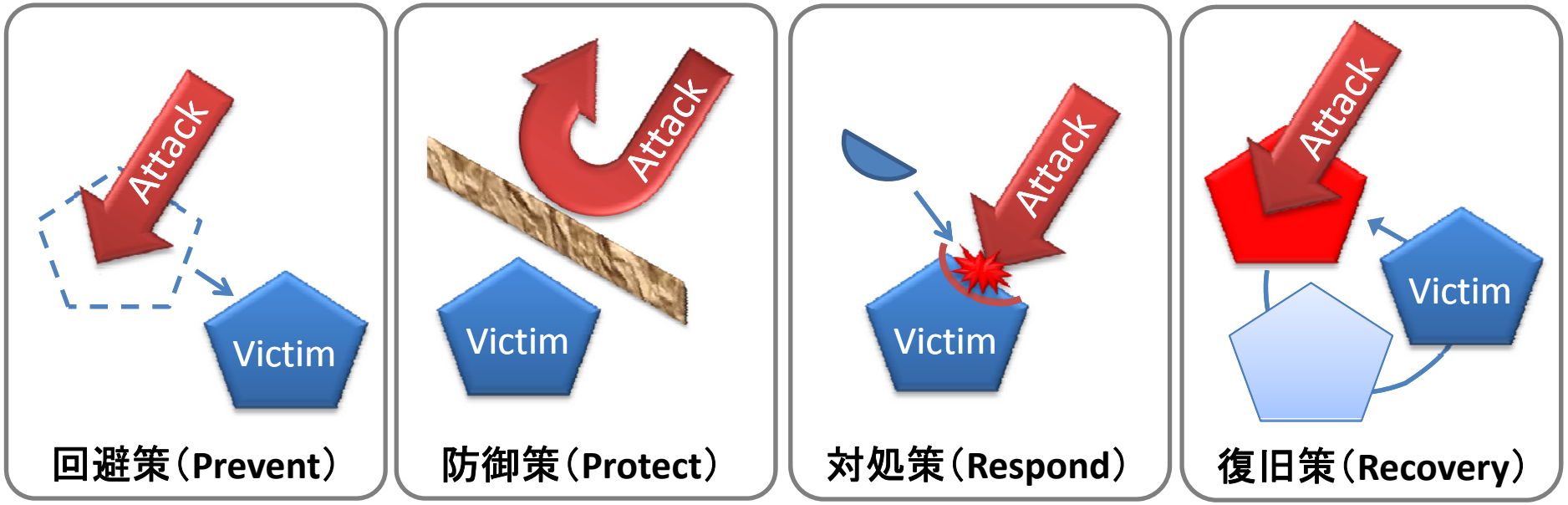
防衛策の「現実的な策定」をするためのポイント(3)

- ある程度の攻撃の仕組みを理解し、**その攻撃経路における適切なセキュリティ対策**を実装すること
  - サイバー攻撃を「静的な絵」として理解するのではなく、組織全般に渡る＆時間の流れのある「動的ストーリー」として理解することが必要
  - 主要な(攻撃)経路ポイントにおけるセキュリティ対策の要否及びレベルの設定には、業務慣習や部署風土も考慮することが必要



防衛策の「現実的な策定」をするためのポイント(4)

- サイバー脅威に対して、**メリハリのついた対策** を検討し、実装及び確実な運用をすること。
  - 日本国内の対策は、「防御策(Protect)に偏重」しているため、いたずらにコストがかかってしまう状況が見られる。
  - 最近のサイバー防衛策におけるベストプラクティス(最善策)は、対処策(Respond)である。(最低限のリスクを受容し、実質的な被害を発生させないことで、結果的に有効な防衛策となる。)
  - 基本的な対策コンセプトは、次の4つのとおり。



本資料に関する連絡先

名和 利男（Toshio NAWA）
サイバーディフェンス研究所
情報分析部／CDI-CIRT

Email: nawa@cyberdefense.jp
SNS: about.me/nawa
Tel: 03-3242-8700

Office: www.cyberdefense.jp
Response Team: www.cirt.jp