CyberDefense

# 最近のサイバー攻撃の実情

2011年12月

サイバーディフェンス研究所
名和 利男

# アジェンダ

1. 2011年9月 中国からのサイバー攻撃
2. 2011年8月 韓国LG U+ モバイルネットワークの障害
3. 2011 Japan: Cyber Attack on Mitsubishi Heavy Industry & Japanese Parliament
4. サイバー脅威の動向と既存対策の分析
5. 今後の組織に求められる防衛策

トピック 1

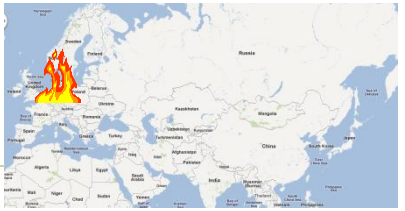
# 2011年9月 中国からのサイバー攻撃

# 2007年 エストニア vs 2010／2011年 日本

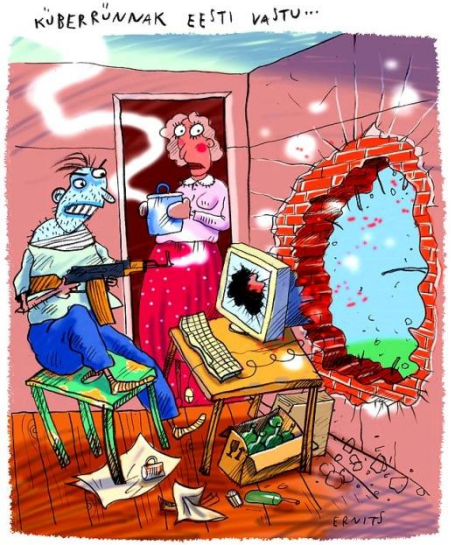
- **2007年**5月、ロシア系のインターネットユーザによる **エストニア** に対する大規模サイバー攻撃（DDoS攻撃、メールボム、Web改ざん等）
  - 発端は、2007年4月下旬、首都タリンの公園にあった旧ソ連兵士の銅像を撤去したこと
  - このサイバー攻撃（DDoS攻撃等）のピークとなった**5月9日は旧ソ連諸国における対独戦勝記念日**。つまり、旧ソ連兵士の銅像の撤去により、愛国心を傷つけられたロシア系のインターネットユーザが、強い憤りを感じて、互いに攻撃を呼びかけたものであった。

- **2010年及び2011年**9月、中国紅客連盟による **日本** に対するサイバー攻撃（DDoS攻撃、Web改ざん、不正侵入等）
  - 発端は、2010年9月7日尖閣諸島沖での中国船長の逮捕
  - 最終的な攻撃日となった**9月18日は日本にとっては満州事変が勃発した日**であるが、中国では旧日本軍から侵攻を許してしまったため、「国恥の日」とされ、反日感情と愛国心が高まる時期である。
  - 2011年は、満州事変80周年目となり、より一層の盛り上がりが見られた。

# 2007年 エストニア



## ブロゴスフィアを通じた伝播

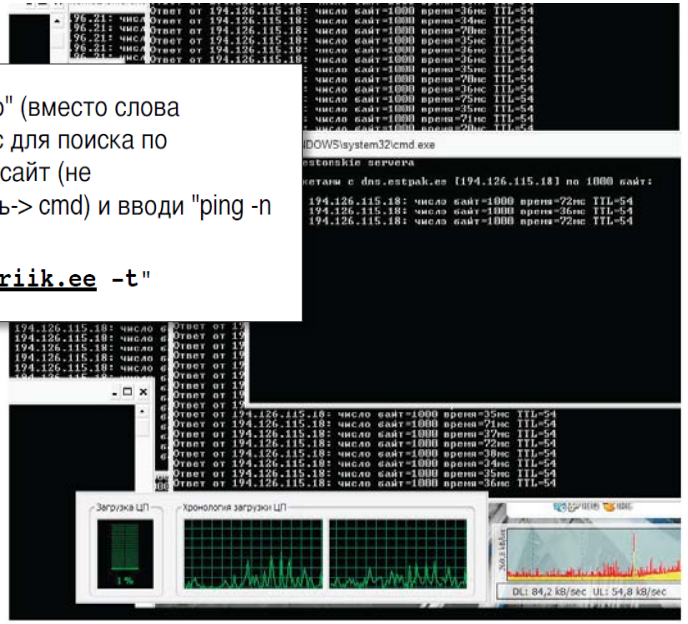



## 攻撃方法

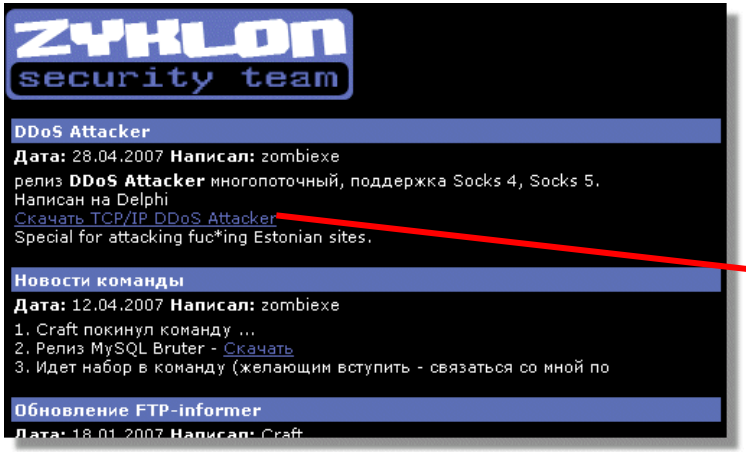
Просто введи в гугле "site:.ee правительство" (вместо слова правительство любой интересующий запрос для поиска по эстонским сайтам). Выбери понравившийся сайт (не русскоязычный!!!), нажми (пуск -> выполнить-> cmd) и вводи "ping -n 5000 -l 10000 эстонский_сайт-t". OK. ВСЕ!!!

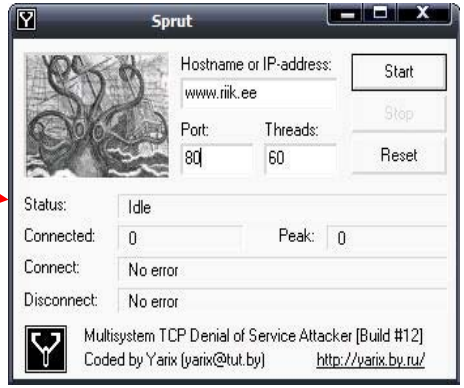
пример: " **ping -n 5000 -l 1000 www.riik.ee -t**"

## 手動による攻撃

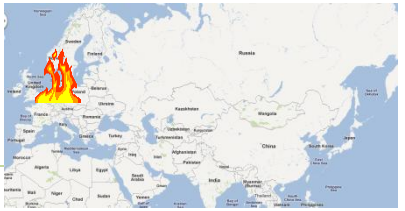


## 攻撃ツールの公開



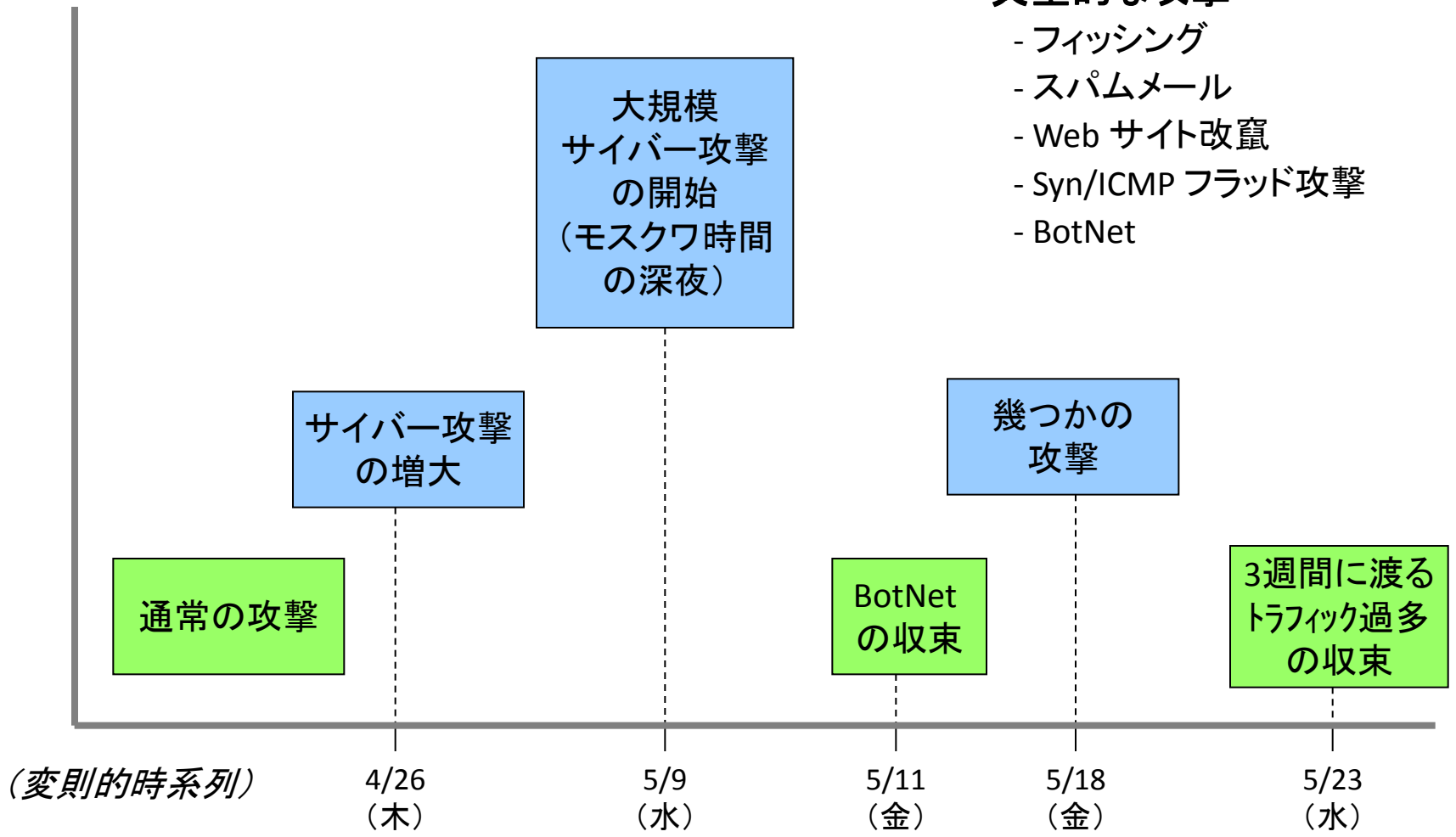



# 2007年 エストニア

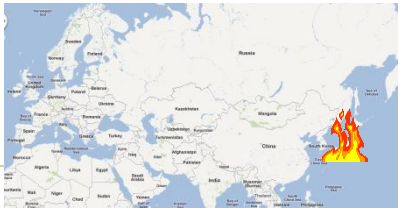


**典型的な攻撃**

- フィッシング
- スパムメール
- Web サイト改竄
- Syn/ICMP フラッド攻撃
- BotNet

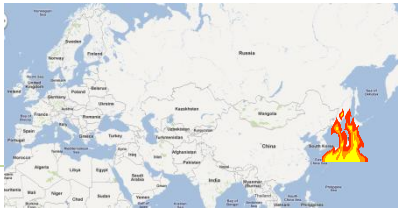


# 2010年／2011年 日本



- 2010年及び2011年、国におけるインターネットユーザーが、日本に対して実施したDDoS攻撃及び小規模なWeb改ざん攻撃した。
  - 2010年9月、尖閣諸島問題を発端にして、中国のインターネットユーザーの一部（中国紅客連盟 等）において、日本に対するサイバー攻撃を実施する予告があり、これに賛同する者によるサイバー攻撃が見られた。
  - 2011年9月、満州事変80周年という節目となり、関連する報道の影響を受けた形で、2011年と同様なサイバー攻撃が見られた。
- 攻撃賛同者の多くは、20才前後の若者と見られるが、その年代は、日本に対する偏った認識と、偏重した愛国心を持っているとされている。
- 予告された攻撃の最終日は、9月18日（満州事変の日）。
  - 中国にとっては「国恥の日」として、旧日本軍から中国の一部領域を占領された日とされており、日本に対する批判が多くなる時期。

# 2010年／2011年 日本



# 中国红客联盟

- 英語名
  - Honke Union of China
- 創設日
  - 2000年12月31日
- 創設者
  - 林勇（通称 Lion）

2011.09.22 COG信息安全论坛
@上海浦东干部学院

・・・よって本日9/22をもって「紅客連盟」の新たなる発足・組織を宣言する。新サイトは11/1に稼働予定。新・旧メンバともに歓迎。「cnhonker.com」が正しいドメイン。


http://cnhonker.com/

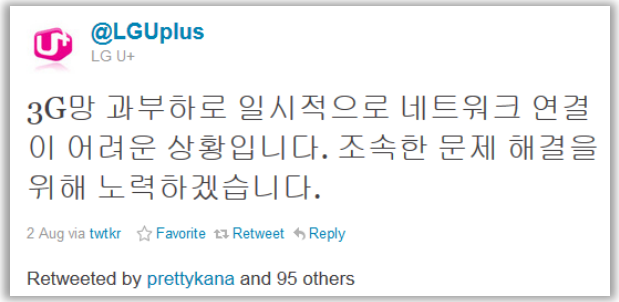
- 特記事項
  - 2004年12月に解散し、2005年に、別の者たちが後継目的で同盟組織を乱立させる。

トピック 2

# 2011年8月 韓国LG U+ モバイルネットワークの障害

# 事象発生

- 2011年8月2日、韓国 LG U+ の 3G モバイルネットワークにおいて、一時的なネットワーク障害が発生した。




https://twitter.com/#!/LGUplus/status/98200868263952384
（3G網過負荷で一時的にネットワーク接続が困難な状況です。
早急な問題解決のために努力します。）

- LG U+（旧 LG テレコム）は、韓国LGグループにおけるモバイルフォンオペレーター会社
  - 民間で 最初に3G サービスを開始したことで有名
  - モバイルバンキングサービスを提供する BankOn を推進


- 2011年4月に発生した韓国農協（金融業務）に対する大規模なサイバー攻撃に、北朝鮮が関与したと見られたため、幾つかの国の政府機関や情報機関が強い関心を示し、関連情報の提供の要請があった。

**「韓国LG U+ におけるネットワーク障害」の事象解明と安全保障上の脅威との関連性の分析要請**

# 情報収集(1)

- LGユープラス、不通にも株価は “黙々”(2011.08.02 15:18)
  - http://finance.joinsmsn.com/news_stock/article/article.asp?ctg=1103&Total_ID=5889314


  - 「LGユープラスは、・・・午前8時前後で3Gデータ網が不通になり、午後3時現在70%ほど回復したと発表した。・・・」
  - 「LGユープラスは、”サービスの不通で不便を経験した利用者の条件に応じて適切な被害補償が提供されるだろう“と明らかにした。LGユープラスの条件は、3時間以上の障害が発生した場合の補償をするようになっている。」

# 情報収集(2)

- LG U +、不通7時間 “原因不明”…再発の可能性を示唆(2011.08.02 15:42)
  - http://ddaily.co.kr/news/news_view.php?uid=80896


  - 「LGユープラスよると、午前8時からロングタームエボリューション(LTE)を除く全国の移動通信ネットワークが不通だ。」
  - 「70%の回復は、10回のデータの通信の試行中に7回は接続されている状態というのがLGユープラスの説明だ。」
  - 「LGユープラス関係者は“データのトラフィックが急に通常の5倍に増加したため、ネットワーク障害が発生した。回復は進行中だ。しかし、なぜ、データトラフィックが5倍になったのかは把握できていない"と述べた。」

# 情報収集(3)

- 焦るLGユープラス、LTEは"温い"2Gは"不通"(2011.08.02 18:22)
  - http://www.asiatoday.co.kr/news/view.asp?seq=510278


  - 「先月1日、業界1位の飛躍を叫んで商用化を開始した第4世代(4G)移動通信のロングタームエボリューション(LTE)までの市場での生ぬるい反応を得ており、大きな悩みに陥った。」
  - 「最も影響を及ぼす可能性は機器の老朽化に応じて、携帯電話網(MSC)が正常に動作しないことができなかったはずだという推測だ。LGユープラスがLTEにだけ神経を使うため2G網の設備投資不足で装置の改善に怠ったという指摘だ。」
  - 「LGユープラスは、1.8㎓帯で2Gのサービスの運用中には、計7つの周波数チャネル(FA)を使い、そのうち4つのFAは、音声用に使っていて、残りの3つのFAはデータ専用に使っている。このうち、データ専用で使っている3つのFAで寡婦化が発生し、すべてのデータサービスが中断されたという説明だ。」

# 情報収集(4)

- LGユープラス不通の事態は、トラフィックの急増比不良が原因…類似事故対策急ぐ(2011.08.03)
  - http://www.etnews.com/news/detail.html?id=201108030143


  - 「LGユユープラスは、前日のデータ通信網不通の事態は、午前8時頃、約5分間、通常20万～30万件に比べて5倍の140万～150万着信の試みが続いたためだと発表した。」
  - 「LGユープラスは、大規模なトラフィックを誘発する主要なサイトは継続的に監視するが、前日、障害発生の原因となったサイトでは管理の範囲に含まれていないため、対応していないと説明した。現在のところ、悪意のある攻撃の可能性は低いとLGユプルロスヌン明らかにした。」
  - 「これによりLGユープラスは、スマートフォンアプリが基地局と頻繁に交信して発生させるトラフィック(Keep Alive Message)を制御するための対策を用意する計画だ。」

# 情報収集(5)

- LGユープラスの不通は'グーグル'だ(2011.08.15)
  - http://news.mk.co.kr/v3/view.php?sc=30000001&cm=%C7%EC%B5%E5%B6%F3%C0%CE&year=2011&no=528806&selFlag=&relatedcode=000060051&wonNo=527583&sID=300


  - 「LGユープラスの基地局に接続され、Googleのサーバーが一時的にダウンしたため発生した。LGユープラスは、Googleに公式文書を送って抗議したが、Googleは、“事業者を差別しない”という原論的な立場を明らかにしたものが知られて論難が予想される。」
  - 「Googleのサーバは、100万台を超えるほどに多いが、この日、ダウンしたサーバーは特にLGユープラスのAndroidスマートフォンの基地局に多数の接続されていたと推定される。」

# 情報収集(6)

- LGユープラス2日のデータ不通の原因は…グーグル、地図サービス遮断措置理由(2011.08.17)
  - http://news.hankooki.com/lpage/economy/201108/h2011081702350621540.htm


  - 「状況から、Googleがこのような措置を取った背景には、独島の表記をきちんとしていない、Googleに対するネチズンの攻撃があった蓋然性が高いと思われる。」
  - 「16日、関連業界によると、LGユープラスで内部調査をした結果、GoogleのモバイルGoogleマップサービスへのアクセス遮断が不通の事態につながったことが確認された。」
  - 「グーグルコリアの関係者は"国際的に独島は紛争地域なので混乱の素地を作るために、意図的に地図サービスで削除した"とし"この問題で、ネチズンたちの世論が良くなかったことを知っていた"と説明した。」

# 事象のまとめ(1)

【発生事象】

- 2011年8月2日
  - 午前8時、韓国のLG U+ において、韓国全土のモバイル通信ネットワークが不通状態になる
    - 影響を受けたのはデータ通信のみで、音声と SMS(シートメッセージサービス)は正常
  - 午後3時、全体の70%回復
    - LG U+は「10回のデータ通信の試行中に7回接続される状態に回復」と説明
  - LG U+ 関係者は、「データのトラフィックが急に通常の5倍に増加したため、ネットワーク障害が発生した。回復は進行中である。しかし、なぜデータトラフィックが5倍になったのかについては、把握できていない」と述べた
    - LG U+ の通常対応のデータトラフィック量は公開されていない
  - 韓国の通信業界の反応
    - LG U+ のスマートフォンのユーザーは、2011年第2四半期で210万人増加したため、LG U+ のデータ処理能力に疑い
    - LG U+ のモバイル通信ネットワーク機器の老朽化と運営能力に問題があると分析
      - "データトラフィックの問題であれば、一部地域のみで障害が発生するはず"
      - "全国ネットワークに障害が発生する場合、無線通信を有線で接続させる部分で問題が生じた可能性"
      - "純粋にデータのトラフィックだけで、全国の障害が発生する確率は非常に低い"

# 事象のまとめ(2)

【技術的な背景】

- LG U+ ネットワークにアクセスしていたスマートフォンは、「一時的にダウンした Google サーバ」に対して、接続要求(Keep Alive )が継続
- そのため、通常の5倍となる 140万～150万件のリクエストが発生し、トラフィックが急増
- これに対し、LG U+ は基地局での対応をしたが、データ不通事態を防ぐことが出来なかった

【グーグルコリアからの非公式情報】

- "국제적으로 독도는 분쟁지역이어서 분란의 소지를 만들지 않기 위해 일부러 지도 서비스에서 삭제했다. 이 문제로 네티즌들 여론이 좋지 않았음을 알고 있었다"
  (国際的に独島は紛争地域なので混乱の素地を作らないために、意図的に地図サービスで削除した。この問題でネチズンや世論が良くない反応を示したのは知っていた。)

- "사고 당일 구글 내부에 문제가 있어 SK텔레콤 KT LG유플러스 모두 오전 8시부터 15분 가량 데이터통신이 불통됐다"
  (事故当日、Googleの内部に問題があり、SKテレコム、KT、LG U+ において午前8時から15分ほど、データの通信が不通になった)

- "SK텔레콤과 KT는 바로 복구했으나 LG유플러스는 그렇지 못했는데, 그 이유를 지금도 찾고 있다"
  (SKテレコムとKTはすぐに回復したが、LG U+ ではできなかった。その理由を今も探している)

# 事象のまとめ(3)

【LG U+ の公式発表】

- 2011年8月15日
  - “평소 카카오톡과 같은 앱들은 트래픽을 관리하는데 이날은 관리대상이 아닌 사이트에서 트래픽이 몰려왔다”（普段からカカオトークのようなアプリのトラフィックを管理しているが、この日は、管理対象外のサイトのトラフィックが集中した）
    - カカオトーク（www.kakao.com/talk）は、特に韓国で利用の多い無料メッセンジャーアプリで、全世界で iPhone、Android、BlackBerry 計1,000万人以上の利用者があり、Android だけでも500万以上ダウンロード
    - 1対1のチャットだけでなく、20～30人によるグループチャットが可能
    - チャット以外に写真、動画、ボイスメッセージが送信可能
  - 加入者に対して、最大3,000ウォン（約200円弱）の補償を準備
    - LG U+ の利用規約には、連続3時間以上のサービスが提供されない場合、または、1ヶ月の間、サービス障害発生が合計12時間を超える場合は、月額料金に反映する形で補償すると規定されている。

# 関連情報(1)

- 2011年7月19日、外交通商部は21日からインドネシア、バリで開かれるASEAN地域安保フォーラム(ARF)で日本の独島(ドクト、日本名:竹島)挑発問題を必ず確かめると明らかにした。

공감언론 NEWSis.( ) 국내 최대 민영 뉴스통신사 2001-2011

인쇄하기 | 닫기

## 외교부 "ARF 때 일본에 독도문제 반드시 짚겠다"

기사등록 일시 : [2011-07-19 15:09:42]

【서울=뉴시스】 이현정 기자 = 외교통상부는 21일 부터 인도네시아 발리에서 열리는 아세안지역안보포럼(ARF)에서 일본 독도 도발 문제를 반드시 짚고 넘어가겠다고 밝혔다.

조병제 외교부 대변인은 19일 정례브리핑에서 "ARF를 계기로 독도 문제와 관련한 몇가지 문제들에 대해 반드시 우리의 기존 입장에 따라 짚고 넘어갈 계획"이라고 밝혔다.

조 대변인은 "일본 국회의원들이 독도 문제를 거론할 목적으로 울릉도를 방문할 계획이라면 양국관계 발전에 전혀 도움이 되지 않는다"며 "방문을 자제하는게 좋겠다"고 말했다.

아울러 일본 외무성의 대한항공 탑승 자제조치와 관련해 "사리에도 상식에도 어긋나는 것"이라며 "효과도 목적도 불분명하고 양국관계에 부정적 영향만 미칠 뿐"이라고 지적했다.

그는 "독도 영유권 문제와 관련한 일본 정부의 어떠한 훼손 기도에도 단호하게 대처해 나가겠다"고 덧붙였다.

다만 일본 의원들이 울릉도 방문을 강행할 경우 입국금지 조치를 취할지에 대해서는 "가정을 전제로 어떠한 대응을 할 것이라는 답변을 하기에는 적절치 않다"며 "모든 가능성은 열려 있다"고 말했다.

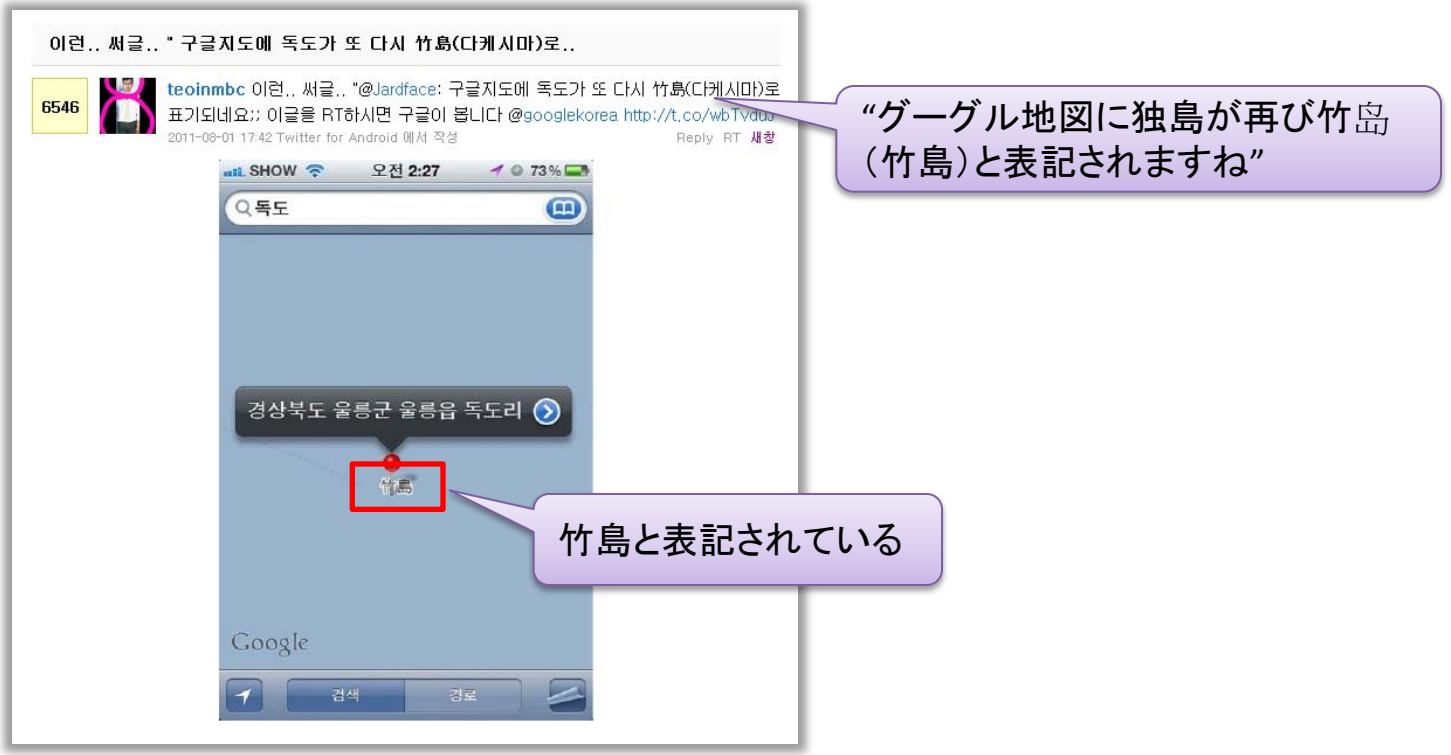
http://www.newsis.com/article/print.htm?ar_id=NISX20110719_0008714357&type=1

# 関連情報(2)

- 2011年8月1日、韓国政府は竹島(韓国名:独島)に近い韓国の鬱陵島を視察しようとした自民党の新藤義孝衆議院議員ら議員3人の入局を拒否した。新藤議員らは9時間ほど金浦空港で待機しながら韓国側の説明を求めたが、入国の目途が立たず、夜の最終便で帰国した。
(以下は、各国のメディアが報道した関連画像)


# 関連情報(3)

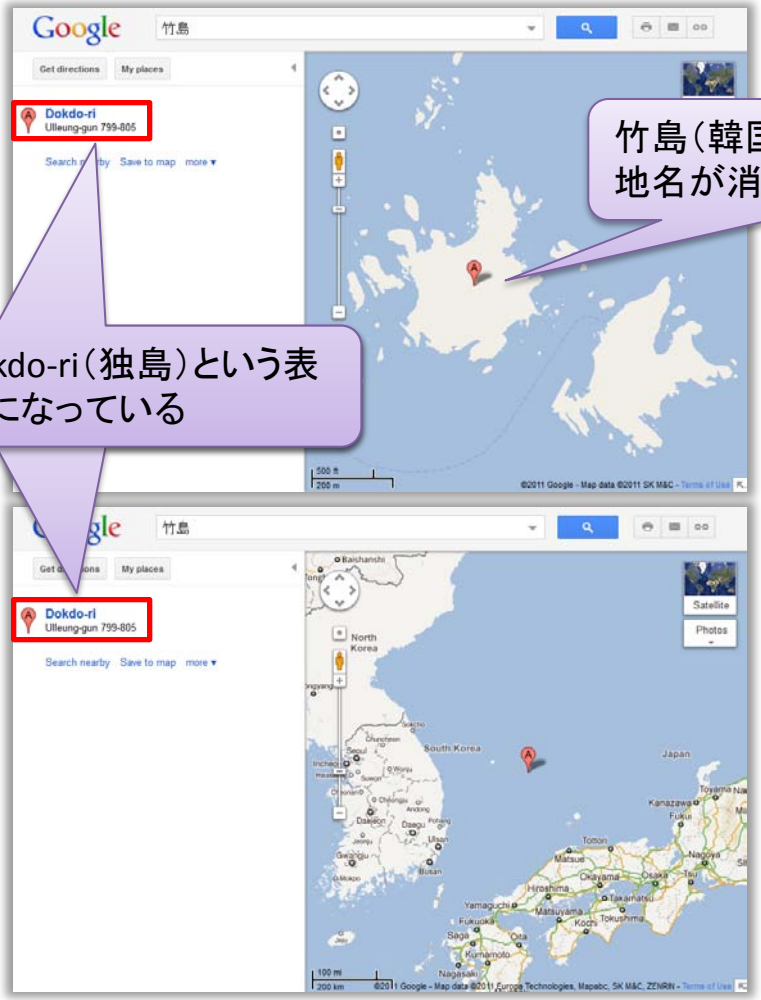
- 事象発生の前夜(2011年8月1日)、Twitter において、スマートフォンの Google Map において、独島が竹島と表記されていることを伝えるメッセージが、膨大にリツイートされる。




http://twitaddons.com/pic/detail.php?id=8268237

# 関連情報(4)

- 現在(2011年10月10日)の Google Map 検索結果を確認すると「Dokdo-ri」となっている




# 事象分析

- 関連するオープンソース情報を統合し、評価及び分析
  - 2011年7月中旬から8月1日までの間、韓国において、「日本と韓国における領土問題（日本名:竹島、韓国名:独島）の盛り上がりが、これまでにない程大規模なものとなっていった。
  - 2011年8月1日、スマートフォンの Google マップにおいて、領土問題の対象（日本名:竹島、韓国名:独島）が韓国において認められていないものになっていることに対する反感は、異常なものとなった
  - 過去に発生した韓国を発信源とする大規模なサイバー攻撃（特に、2009年7月及び2011年3月のDDoS攻撃）を鑑みると、「Google Map に対するDDoS攻撃の発生の可能性は十分に考えられ、その規模は大となる恐れがある」と評価でき、米国企業である Google はそれを予見できたと考えるのが自然である。

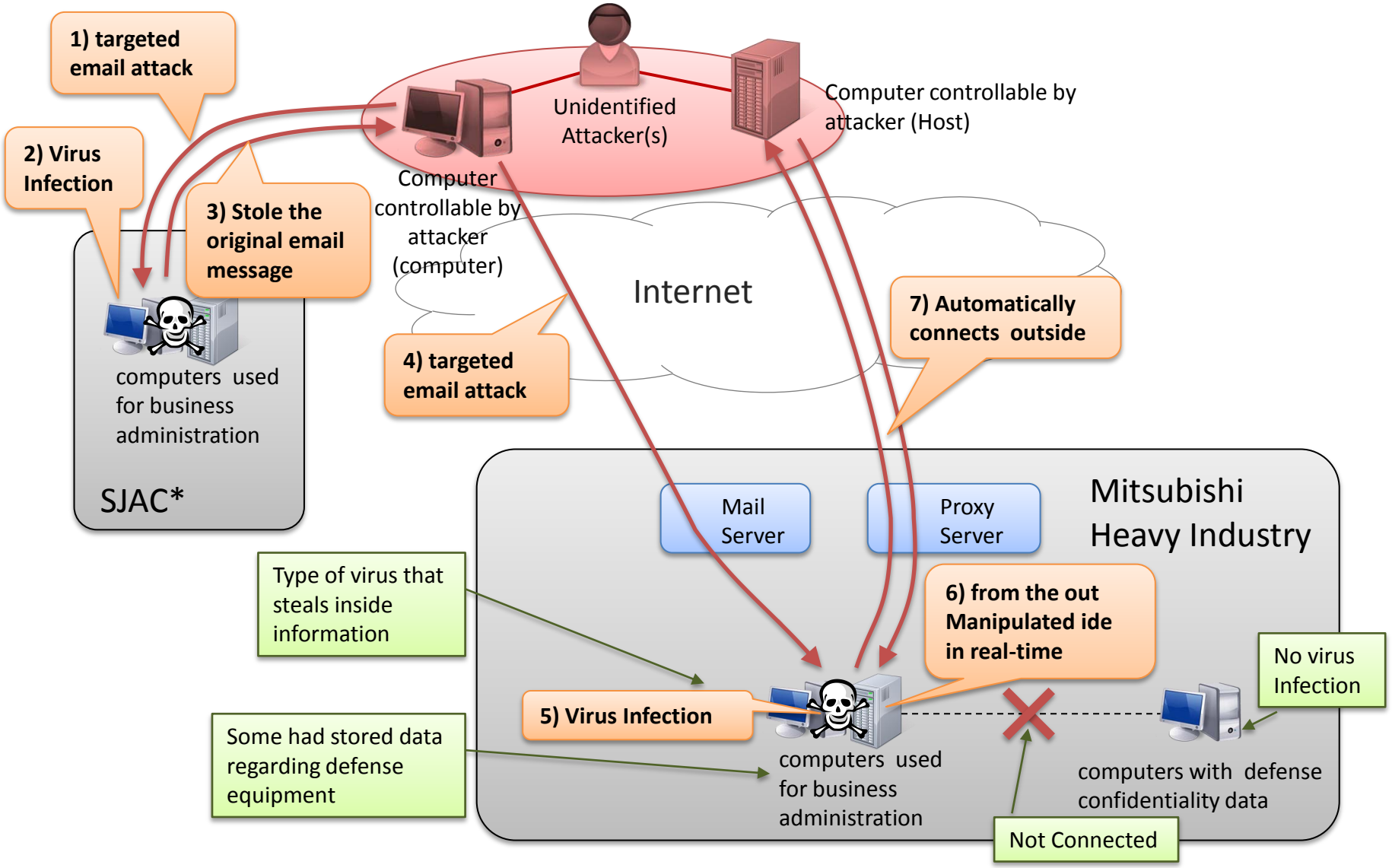
「韓国LG U+ におけるネットワーク障害」は、2011年7月中旬から8月1日までの韓国における「日本と韓国の間の領土問題」の高まりを起因とし、スマートフォンの地図サービスにおいて「竹島」と表記をしていた Google に対するサイバー攻撃の機運を予見したGoogle 社の対応が、韓国 LG U+ のネットワーク経の障害を与える結果となったと分析できる。

日本でも、韓国における領土問題の高まり時に、国内事業者のインターネットサービスのコンテンツ中に「竹島」が表記されている場合、何かしらのサイバー攻撃を受ける可能性が十分に考えられる

トピック 3

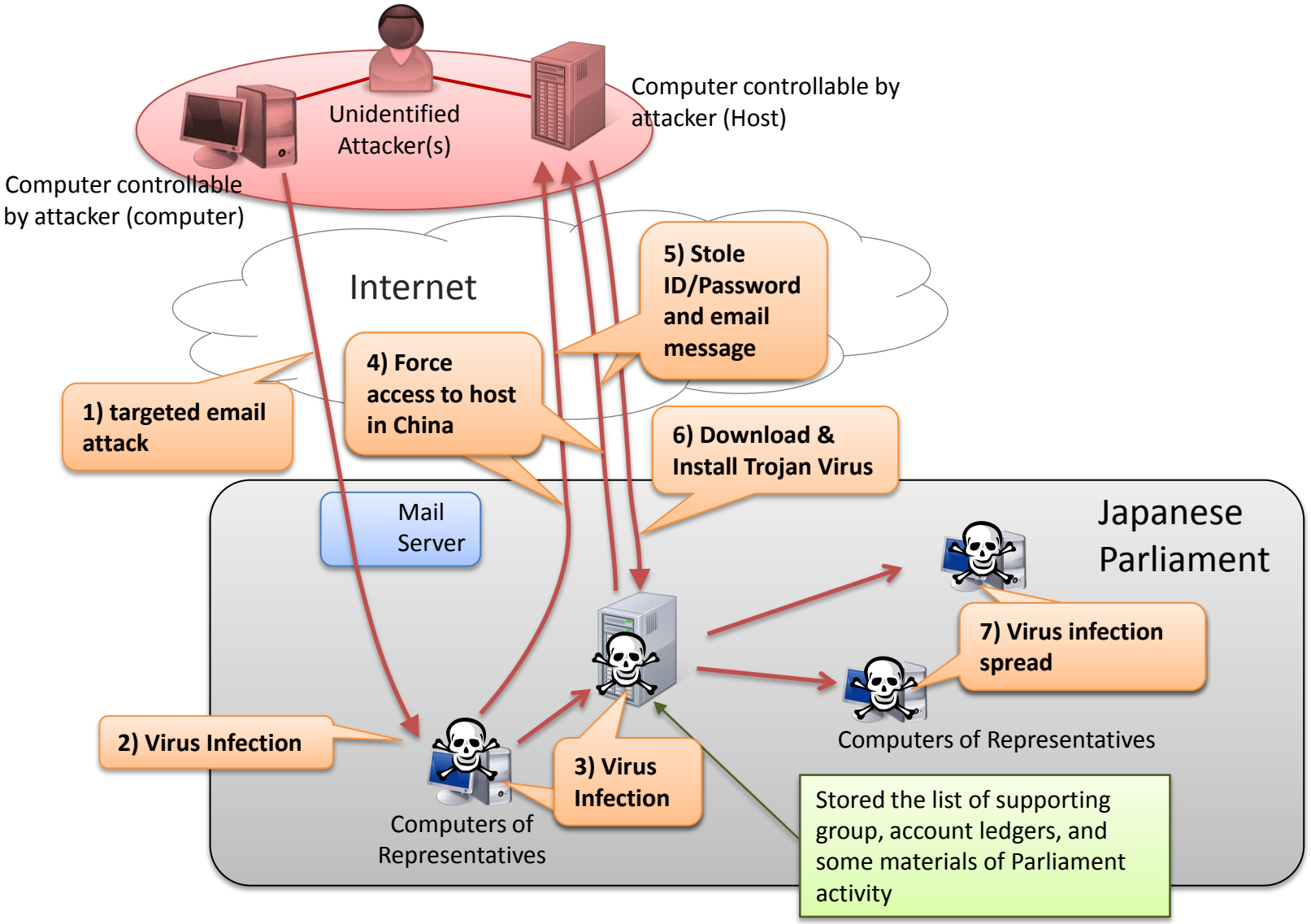
# 2011 JAPAN: CYBER ATTACK ON MITSUBISHI HEAVY INDUSTRY & JAPANESE PARLIAMENT

# Cyber Attack to Mitsubishi Heavy Industry




***SJAC** (Society of Japanese Aerospace Companies) : the sole public entity representing the interests of the Japanese aerospace industry

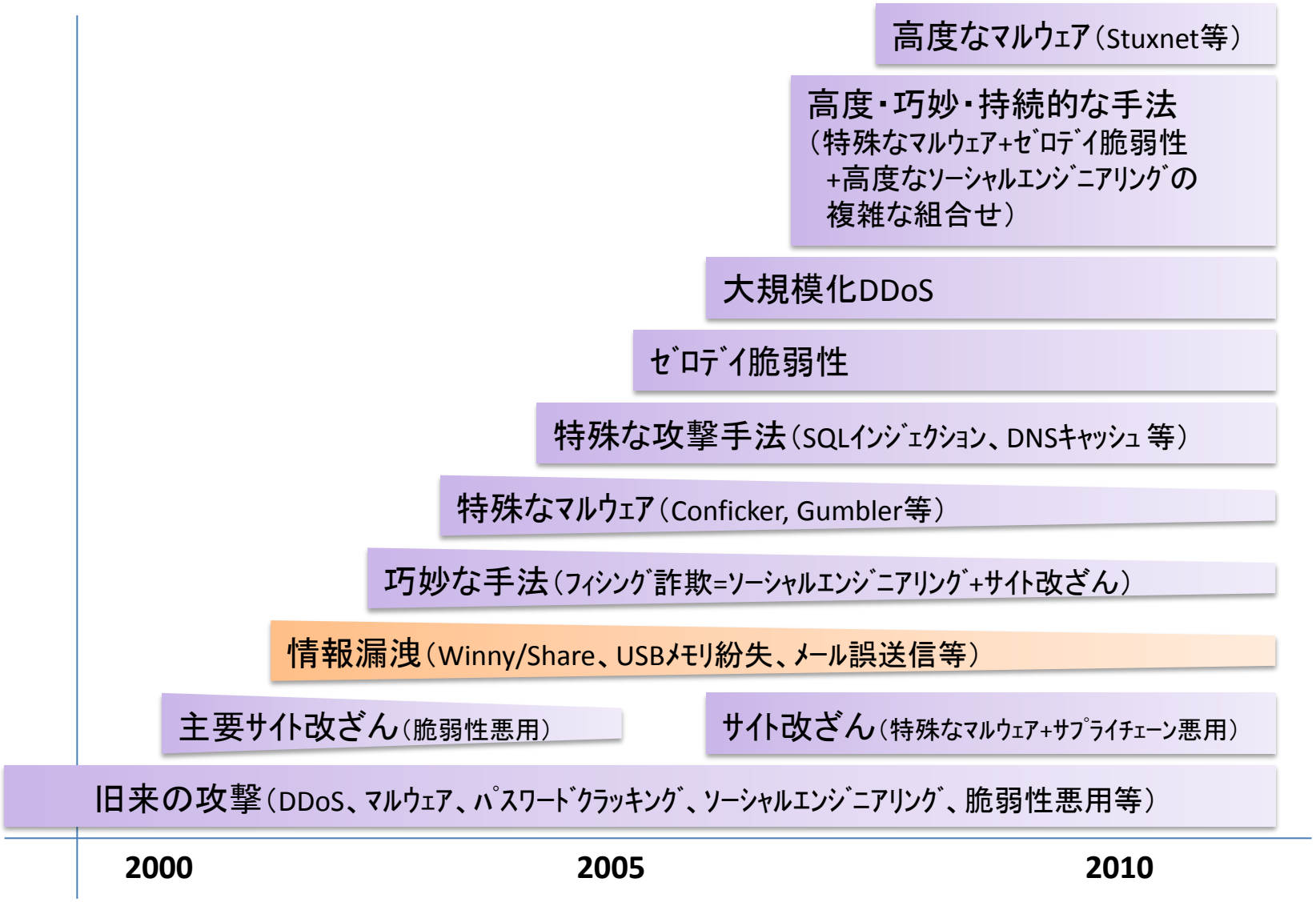
# Cyber Attack on Japanese Parliament



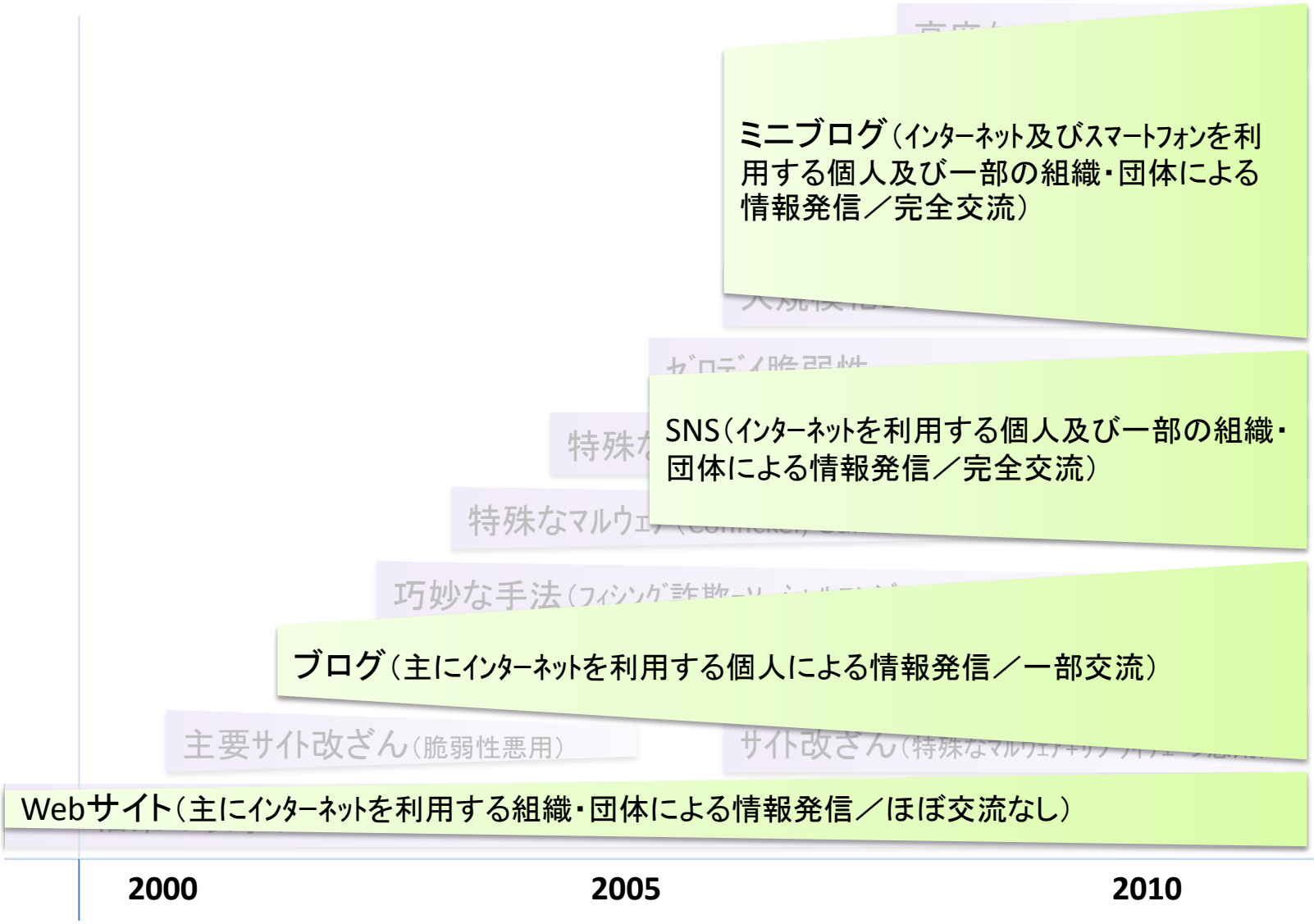
トピック 4

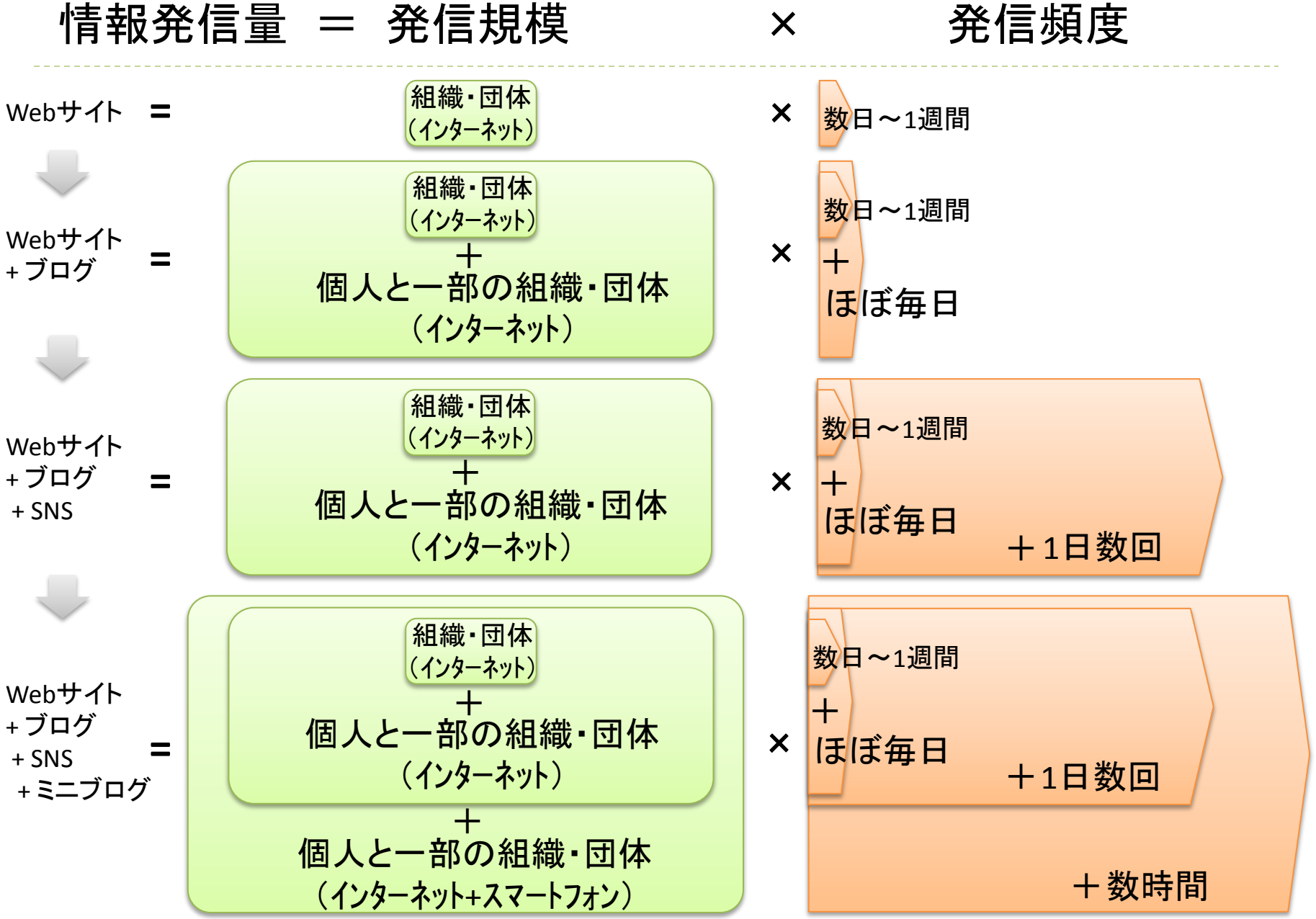
# サイバー脅威の動向と既存対策の分析

# 国内のサイバー攻撃の動向変化

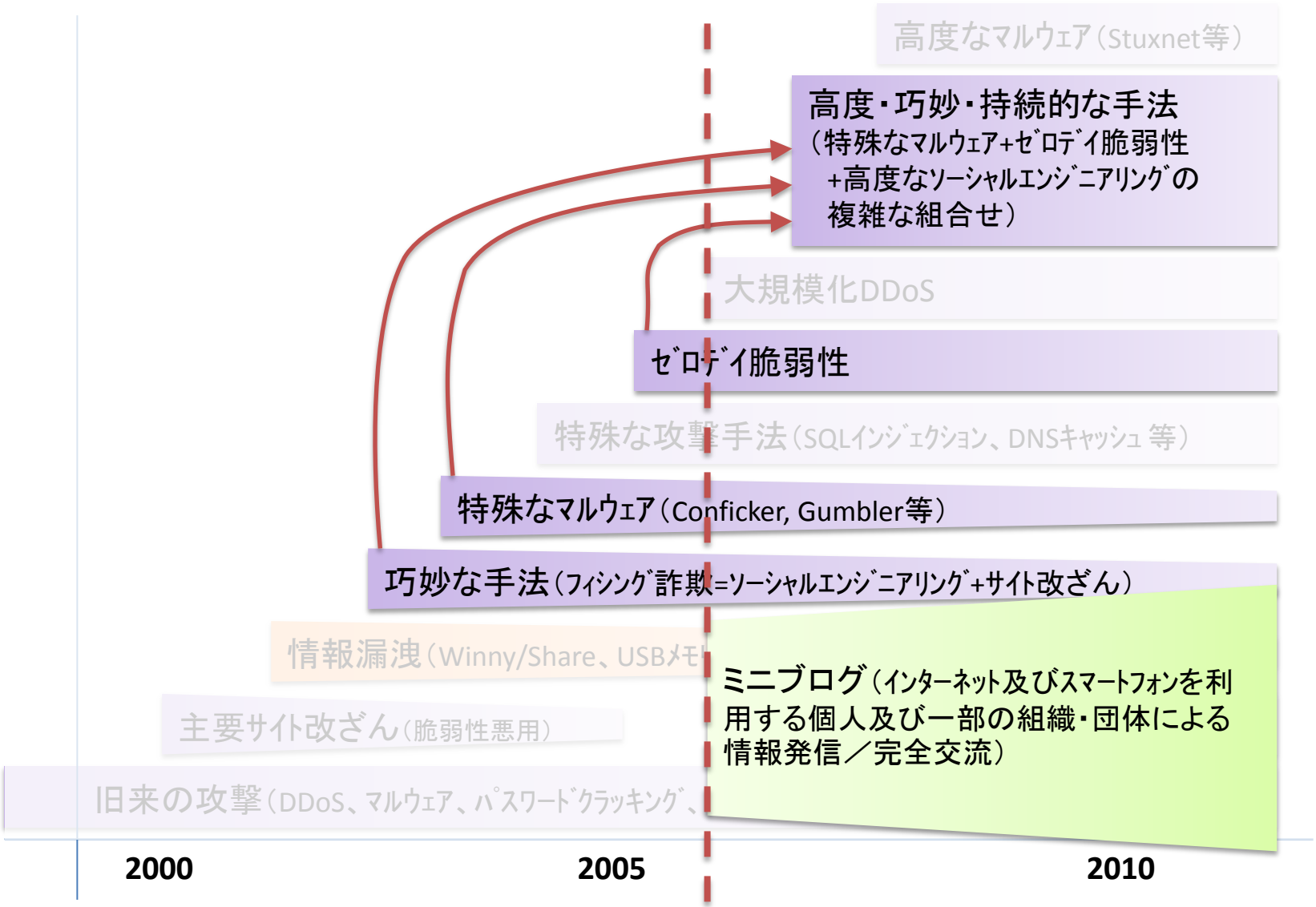


# 情報の発信／交流の変化

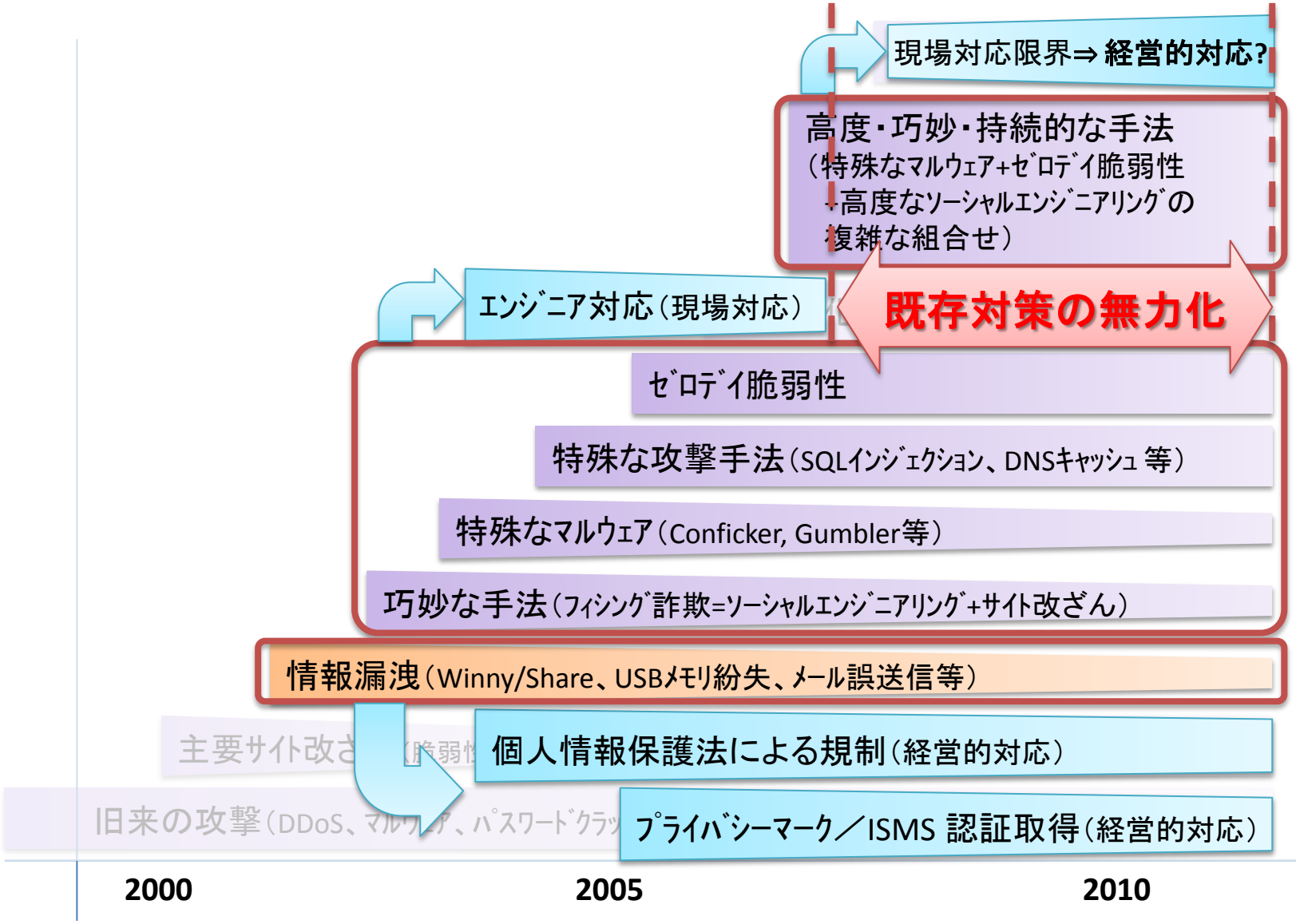




# 国内のサイバー攻撃の動向変化（ここ数年）



# 既存のセキュリティ対策の無力化



# セキュリティ対策が後追いになる要因と効果を出さない対策（例）

- 日本においてセキュリティ対策が後追いとなる要因

**通常のIT運用**

**インシデントの発生と対応**

**IT部門**

IT部門は、高いレベル業務クオーリティ（品質）が求められ、かつ、それに努力

IT部門における業務のアサイメント、内容、達成レベルが曖昧
- ✓ 欧米のIT部門は、日本に比べてジョブ（業務）アサイメントとジョブディスクリプション（業務内容）が明確化

発生インシデントへの対応に関する認識と行動
- ➢「業務及び運用上の品質の維持」と認識
- ➢ 想定業務や業務範囲外の対応活動を許容

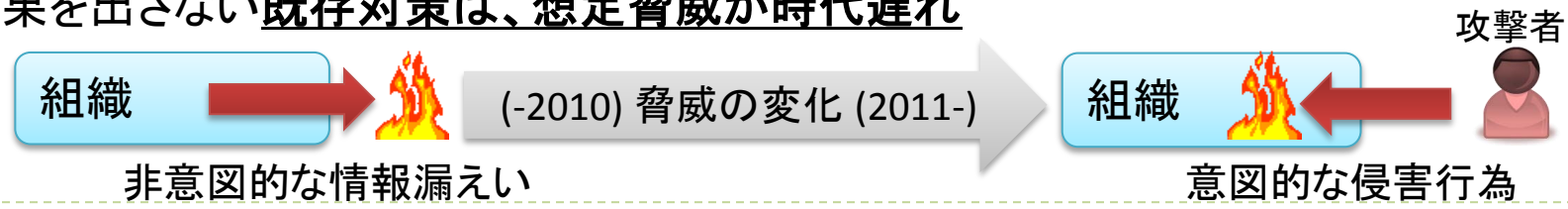
↓

**-2010年：現場で対処**
**2011年-：現場で限界**

**経営層**

発生インシデントへの認識不足と意思決定の機会喪失
- ➢ インシデントの脅威実情と動向の**変化に気付きにくい**
- ➢ 適切な対策レベルと適切な意思決定がされない

- 効果を出さない**既存対策は、想定脅威が時代遅れ**



# 今後の展開を見積もる上で重要なファクター

- **スマートフォン／タブレット端末**
  - ユーザー（利用者）の急拡大
    - 利便性の飛躍的向上（充実したアプリ、興味あるサービスが得やすい 等）
    - （PCに比較して）低コスト
  - サービス提供事業者の急拡大（IT業界唯一の成長産業）
    - 利用（活用）目的の広がり
    - ターゲット型サービスの充実化
    - 必然的なクラウドサービスの利用促進
    - （他のサービス開発に比較して）低コスト

- **スマートコミュニティ**
  - スマートグリッド
    - 再生可能エネルギー利用促進、（蓄電池を含む）分散電源の管理システム導入 等
  - スマートハウス／スマートビルディング
    - ネット型家電の普及、太陽光発電等の利用拡大、電源供給管理システム導入等
  - スマートカー
    - 電気自動車、ネット連動型サービスの普及 等

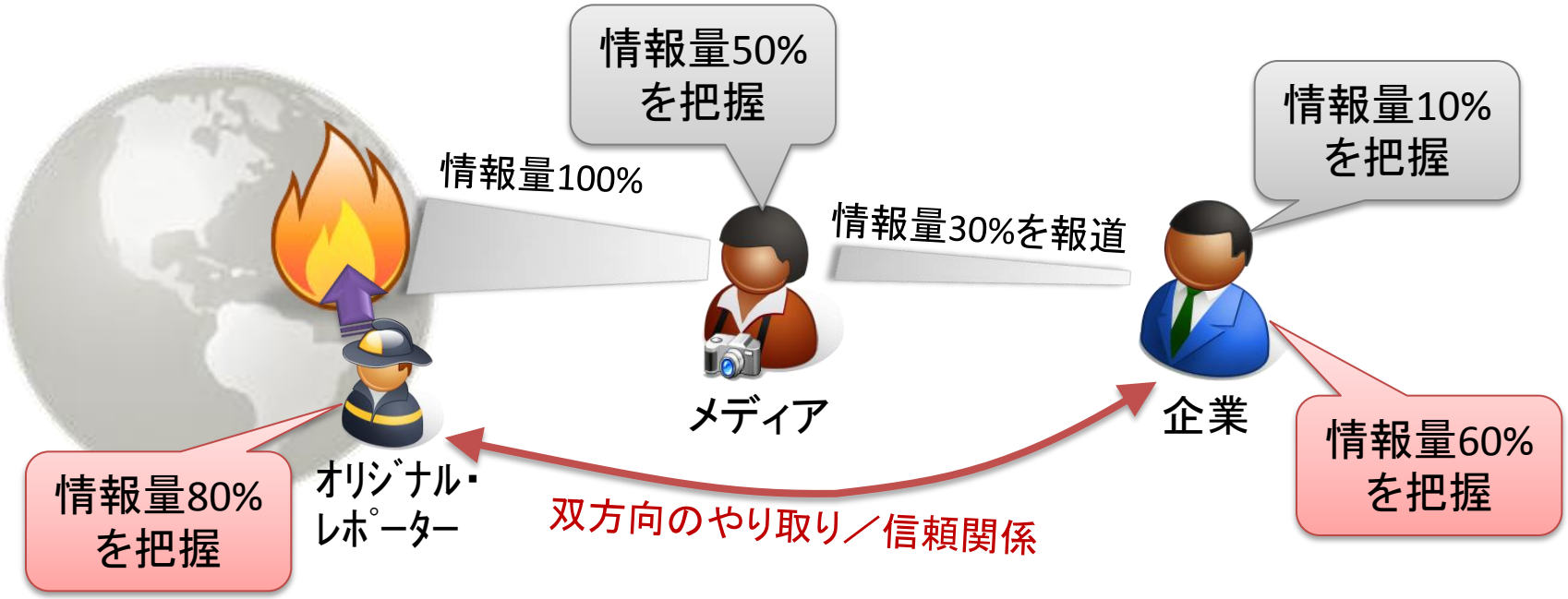
- **サイバー攻撃の活性化と対象拡大**
  - サイバー攻撃賛同者の急激な増加
    - 長引く不況により職に付けないITリテラシラーの高い若者
  - 攻撃対象に社会インフラ、政府機関及び国防産業が加わる
    - 産業用制御システム
    - 組織内の閉鎖的環境にある重要情報を扱うシステム

トピック 5

# 今後の組織に求められる防衛策

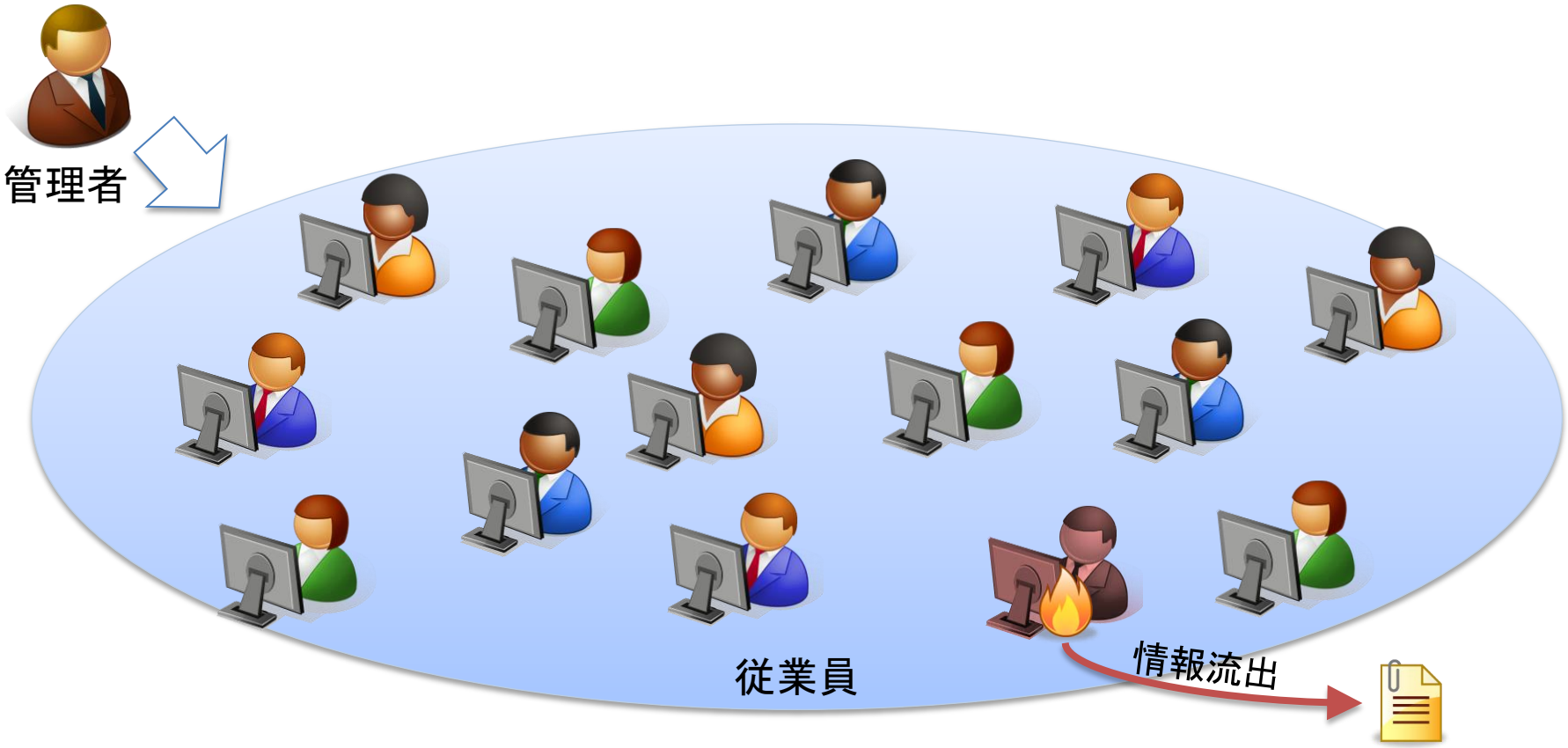
# 防衛策の「現実的な策定」をするためのポイント

- サイバー空間における**<u>脅威を把握すること</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 Report）が発信する情報を追求する



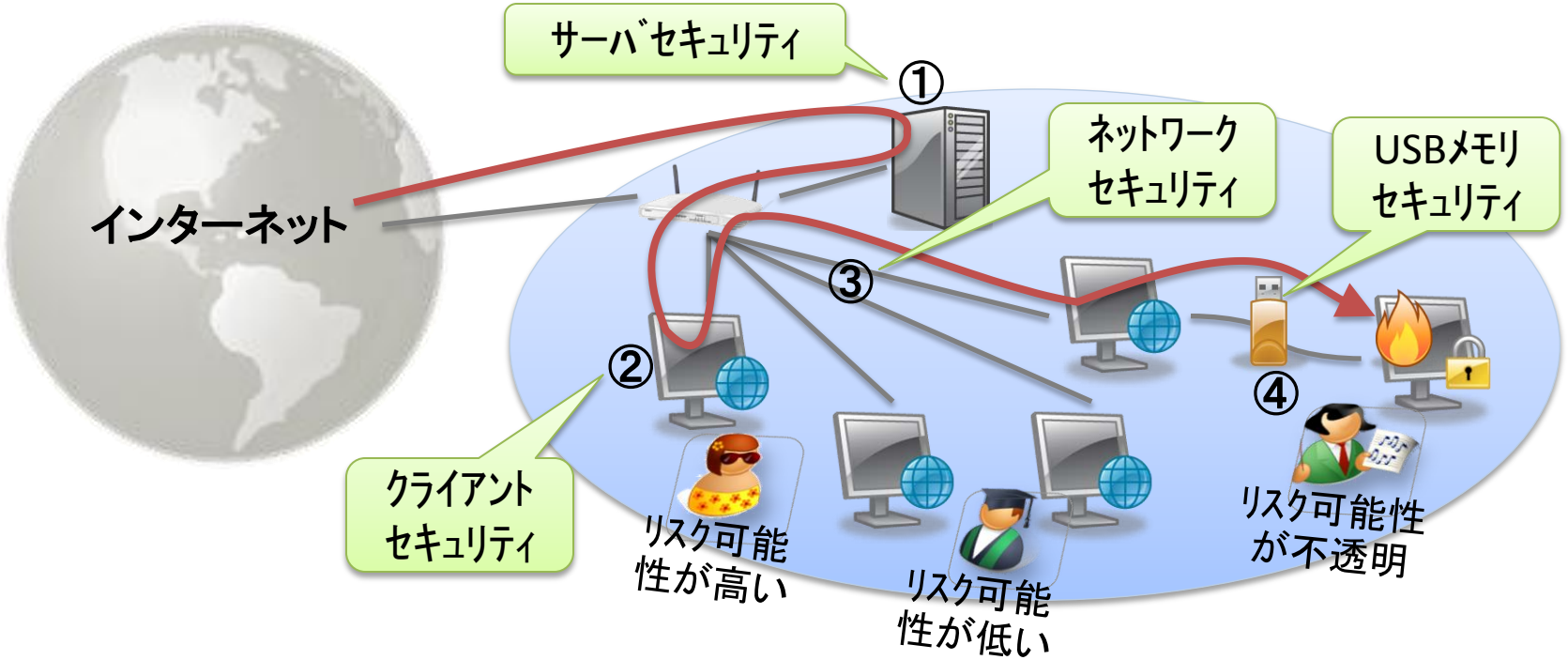
# 防衛策の「現実的な策定」をするためのポイント

- サイバー攻撃を 100% **防ぐことは不可能という前提認識**を持つこと
  - 業務等で活用する ICT（情報通信技術）は、悪用することが可能
  - セキュリティに関しては、人を信じる「性善説」ではなく、適切な「性悪説」を



# 防衛策の「現実的な策定」をするためのポイント

- 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



# 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

Email: nawa@cyberdefense.jp
SNS: about.me/nawa
Tel: 03-3424-8700

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