CyberDefense

サイバー脅威の背景と実状理解

2012年5月

サイバーディフェンス研究所
名和 利男

アジェンダ

1. 「攻撃者」と「サイバー脅威」

2. サイバー脅威の動向と既存対策の分析

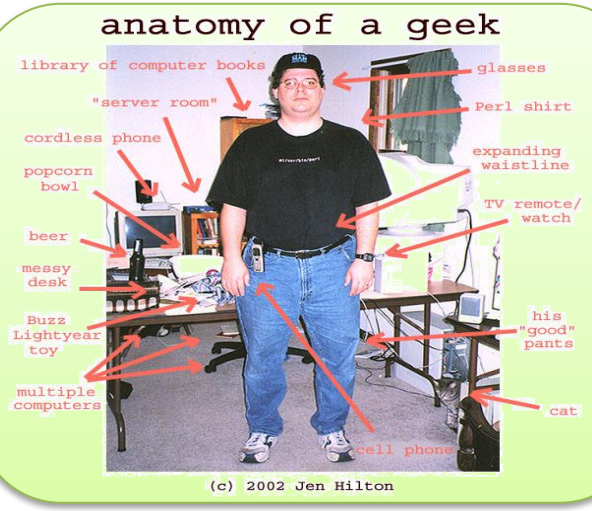
［事例解説］
- 2011年 日本における標的型攻撃（ソニーグループ、三菱重工、衆議院）
- 2011年8月 韓国LG U+ モバイルネットワークの障害
- 2011年-2012年 Android ﾓﾊﾞｲﾙ用犯罪ｱﾌﾟﾘ（ZITMO）

3. 今後の組織に求められる防衛策のポイント

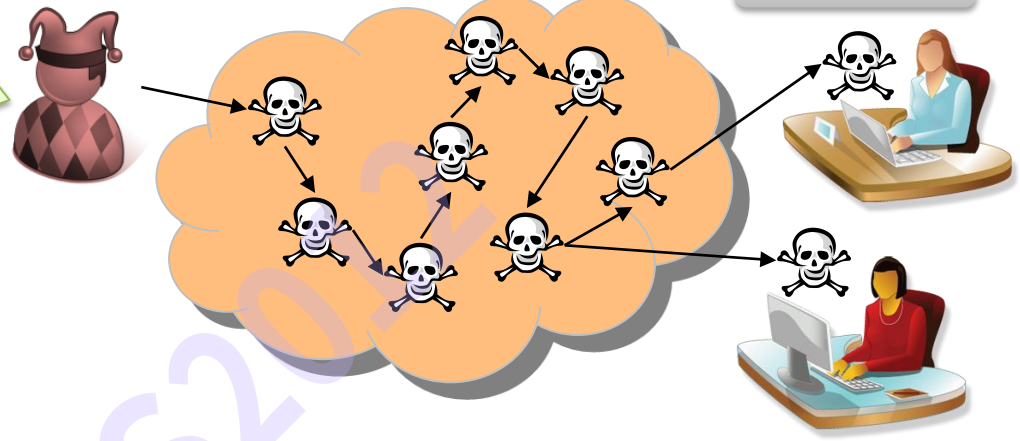
トピック 1

「攻撃者」と「サイバー脅威」

「攻撃者」と「サイバー脅威」の変化



Geeks/Hackers?



数年前まで

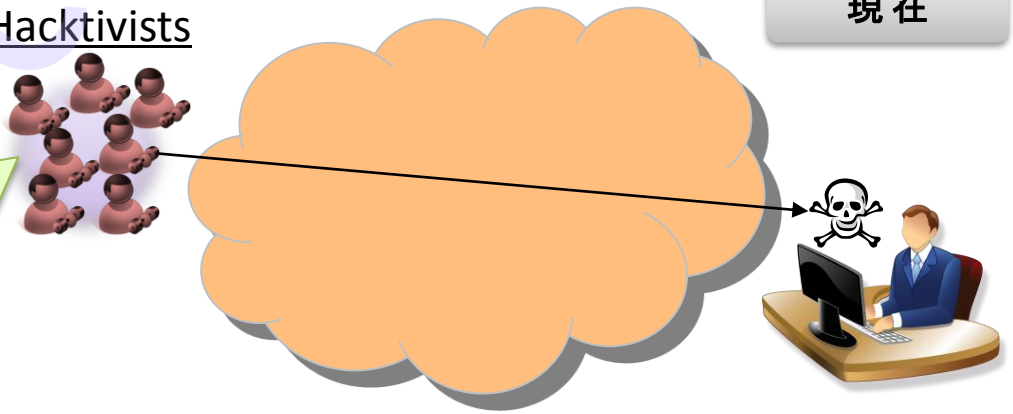
Possible Victim

Hacktivist = Hacker + Activist

「ハッキングという道具を使って抗議をし、より広い闘争に参加しようとする反乱者、フリーダム・ファイター、テロリスト、その他ディジタルな戦場で活動をする人々のこと」

1. 実行者のメッセージを極めて広汎な徴収に届けることができる。
2. 実行に際してほとんどコストが掛からない。
3. 地理や距離的制約を超えることができる。
4. 匿名で危険を伴うことなく闘争に参加出来る形態である。

Hacktivists



現 在

Targeted Victim

Source: Activists and Terrorists Turn to Cyberspace by Dorothy Denning
The Future of War, Vol. 23 (2) - Summer 2001 Issue

中国の代表的な攻撃者コミュニティ - 中国红客联盟

中国红客联盟

- 英語名
  - Honke Union of China
- 設立日
  - 2000年12月31日
- 中核メンバ
  - **lion**：連盟の創設者で Web マスター、ネットワークセキュリティを担当
  - **bkbll**：連盟の総務を担当
  - **yaya**：連盟の会計兼人事のネットワーク管理を担当
  - **Redfreedom**：米国に対するサイバー攻撃、非常勤の技術責任者を担当
  - **NikNanA**：連盟の運用及びネットワーク管理担当
- 登録者数
  - ピーク時は8万人（**約65%は大学生**）
- 概要
  1. 1998年 3月 インドネシアに対するサイバー攻撃
  2. 1999年 3月 米国に対するサイバー攻撃
  3. 1999年 8月 台湾に対するサイバー攻撃
  4. 2000年 1月~2月 日本に対するサイバー攻撃
  5. 2001年 4月 米国に対するサイバー攻撃
  6. 2004年12月　解散
  7. 2005年 4月　再編
  8. 2005年 日本に対するサイバー攻撃
  9. 2010年 8月 フィリピンに対するサイバー攻撃
  10. 2010年 9月 日本に対するサイバー攻撃

- 黒客（ヘイカー）／駭客（ハイカー）→「ハッカー」
- **紅客（ホンカー）→「愛国的なハッカー」**
- （稀に）博客（ポーカー）→「ブロガー」

http://www.cnhonkerarmy.com/

中国红客联盟の経緯(1)

863计划
(国家高技术
研究发展计划)

天安門事件

中国における科学技術の推進

中国における愛国主義教育の強化

愛国思想の強い中国人ハッカーによる活動

“红客”の確認

ユーゴ紛争
(中国大使館誤爆)

日米の
サイト改ざん

“红客联盟”の確認

海南島事件
(中国空軍パイロット行方不明)

ｺｰﾄﾞﾚｯﾄﾞ
出現

“红客联盟”の脅威

尖閣諸島問題

大規模
DDoS攻撃

1985 1990 1995 2000 2005 2010

中国红客联盟の経緯(2)

863计划(人民網による邦訳:国家863計画)
1986年3月に始まったハイテク技術の研究発展計画。王大コウ、王淦昌、楊嘉チ、陳芳允の4人のベテラン科学者が1986年3月3日、「世界の先端技術から取り残されないためにも、国内のハイテク技術を発展させていく必要がある」として、中国共産党中央に陳情書を提出したことから始まった。

問題を重視した鄧小平氏は「すぐに決めるべきで、引き延ばすべきではない」とし、計画の開始に向け自ら指示を行った。

その後の全面的な科学論証や技術論証を経て、国務院は「ハイテク技術研究発展計画概要」を批准。これが通称「国家863計画」と呼ばれる。863計画では生物、宇宙、情報、レーザー、オートメーション、エネルギー、新素材の7分野(1996年に海洋技術を追加)を重点分野に決定。

これらの重点分野で世界最先端のレベルに照準に合わせ、優れた技術力を結集、先進国との技術格差を縮小させ、関係分野の科学技術の進歩を促進、優秀な人材を育成し、将来のハイテク産業の発展に向けて条件を整備していくことを目的としている。
(http://j.people.com.cn/2003/02/13/jp20030213_26019.html)

中国の愛国主義教育に関する諸規定(一部抜粋)
中国の教育の基本法である「教育法」は1995年3月18日に制定され、同年9月1日施行された。「教育法」は、諸外国の教育基本法を比較検討し、それらを参考にしながら草案の改訂を重ね、立案以来年の歳 月を経てようやく成立した。
愛国主義教育に関する条文は次のとおりである。

「国家は教育を受ける者に愛国主義、集団主義、社会主義の教育を行い、理想、道徳、規律、法制、国防、民族団結の教育を行わなければならない。」(6条)

なお、後述するように、「教育法」成立に先立って、1994年に「愛国主義教育実施要綱」が制定された。これは中国共産党の教育政策における重要文献と位置付けられ、「教育法」の愛国主義教育規定もその方針に沿ったものであると考えられる。

「教育法」以外の教育関係法では、「教師法」(1993年10月31日制定、1994年1日1日施行)と「高等教育法」(1998年8月29日制定、1999年1月1日制定)に、愛国主義教育に関する条文がある。「教師法」では、教師の履行すべき義務を6項目定めた第8条において、その3項目目として、*「学生に対し憲法の定める基本原則の教育、愛国主義・民族団結の教育、法制教育及び思想品性・文化・科学技術教育を行い、学生を組織・引率して有益な社会活動を展開する」*と規定している。

「高等教育法」では、*「高等教育機関の学生は法律・法規を遵守し、学生行為規範と学校の各種の管理制度を遵守し、教師を敬い、勉学に励み、体質を向上させ、愛国主義と集団主義と社会主義の思想を打ち立て、マルクス・レーニン主義と毛沢東思想と小平理論の学習に努め、良好な思想品性を備え、高度な科学文化知識と専門技能を身に付けなければならない。」*(53条)として、愛国主義教育そのものではないが、学生自身が愛国主義思想の涵養に努めなければならないことを明記している。

なお、「義務教育法」(1986年4月12日制定、同年7月1日施行)には、愛国主義という言葉は条文に盛り込まれていない。これは、愛国主義教育の強化が本格的になる前に制定されたためであると考えられる。
(http://www.ndl.go.jp/jp/data/publication/refer/200412_647/064705.pdf)

中国红客联盟の最近の状況

COG信息安全论坛

（COG情報セキュリティフォーラム）

http://www.chowngroup.com/

- 日時：2011年9月22日
- 場所：上海浦东干部学院（上海市浦东新区前程路99号）
- 目的：安全なインターネットライフ、技術的な自由、共有、平等及び連帯の追求。
- 参加者：ハッカーグループリーダ、製造業、ネットセキュリティ関係者、メディア、学生 他
  （約350名、うち米国人1名／日本人1名／台湾人3名）
- 注目すべき発言：

COG信息安全论坛の閉会翌日（9月23日）、中国紅客聯盟の創始者**Lion（林勇）**が、公式Webサイトおよび自身の微博（中国版Twitter）を通じて、「**<u>10年ぶりに中国紅客聯盟の再編する</u>**」と宣言。

中国红客联盟によるサイバー攻撃（2010年/2011年、日本）

- **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。

公告： 2010-09-14 20:44:50　关闭公告　收藏

活动名称：918勿忘国耻，爱国保钓 中华魂圣战
活动口号：反击日本侵略 保卫钓鱼岛
活动时间：9.18日 晚19点集合所有战士，21点开始攻击
活动地点：YY 6969 频道
活动参与：6969圣战队员 红客联盟 转基因阻击战队员及广大爱国青年
活动任务：瘫痪各大日本贴吧及网站 发出中华民族的怒吼，钓鱼岛是中国的 神圣不可侵犯
活动意义：日本一次次侵占我国钓鱼岛，扣押我国人员。忘记历史就会挨打！！
中华民族百年耻辱，无不让热血中华儿女而愤怒。掀起一场盛大的网络反日侵略 保卫钓鱼岛的活动勿忘国耻，重新聚拢中华魂！
希望每一位流淌着中华民族血液的爱国青年，请加入我们！让我们相聚YY 6969频道共同战斗！

世界の代表的な攻撃者コミュニティ - Anonymous

- Anonymous（アノニマス）
  - 米国の画像掲示板サイト”4chan”などから派生したハッカーコミュニティ。
  - “Knowledge is Free”（知識は自由）を掲げ、ネット上の言論の自由を守るために戦う自警団を自称する集団。
  - DDoS攻撃（大量のパケットを送信してシステムダウンを引き起こすトラフィック攻撃）などのサイバー攻撃や、現実世界での抗議運動も実施する。

2ch.net

ふたば★ちゃんねる

www.2chan.net

4chan

www.4chan.org

Anonymous

驚異的な身体能力と頭脳によって、独裁政権に反旗を翻す架空の義賊を描いたSF映画「V for Vendetta」の主人公「V」の仮面を被ったAnonymousメンバ

Anonymous によるサイバー攻撃（2011年、日本）

OPERATIONGREENRIGHTS

FlyerOP: http://img69.imageshack.us/i/tepto04.jpg/

Press eng

Fukushima tragically reminded the world that the nuclear risk is unmanageable and its consequences are unacceptable. Nuclear power involves the intrinsic need to lie, to misrepresent, hide information and the size of the facts as we saw in Fukushima and informs us as **WikiLeaks** be done by the **IAEA** in relation to **TEPCO**.

• • •

Anonymous によるサイバー攻撃（2011年、米国）（1）

ターゲット	起因するイベント	攻撃者の反応		時間差
PayPal（クレジットカード決済代行会社）	PayPalがWikiLeaks のWebサイトに対するサービスを停止した。	Anonymous の一部メンバが、PayPalに対してDDoS攻撃成功させ、サービスの一時的な途絶を引き起こした。		2～3日後
HBGary（ITセキュリティサービス会社）	HBGaryのCEOが、WikiLeaks の Webサイトに対するサービスを停止した PayPalのサービスを途絶したAnonymous のリーダーを特定した。	Anonymous の一部のメンバが、HBGaryに対してSQLインジェクション攻撃とDDoS攻撃を行ない、40,000件のEメールを搾取及び公開した。また、Anonymous の一部のメンバは1テラバイトのデータを削除した。		1日後

Anonymous によるサイバー攻撃（2011年、米国）（2）

ターゲット	起因するイベント	攻撃者の反応		時間差
Sony（大手電子機器メーカー・電機メーカー）	Sony が、その会社製品のセキュリティを無効にしたハッカーを見つけ、提訴した。	Anonymous と LulzSec の一部メンバが、DDoS攻撃を行ない、Sonyの さまざまな Web サイトや各部署の社員アカウント情報を盗み出した。 LulzSec の一部メンバが、100万件の米国、ベルギー、オランダの顧客のユーザーネームとパスワードを公開した。		訴訟の和解から2日後 最初の訴訟から2～3ヶ月後
Monsanto（多国籍バイオ化学メーカー）	殺虫剤や遺伝子組み換え食品を製造する会社が、成長ホルモンを含んでいないというラベル表記した有機栽培農家に対して、訴訟を起こした。	Anonymous の一部メンバが、MonsantoのWebシステムに2日間に渡るサイバー攻撃を行ない、3つのメールサーバの機能低下、広範囲に渡る農産業を含む2,000件以上の個人情報を搾取し、公開した。		2ヶ月後

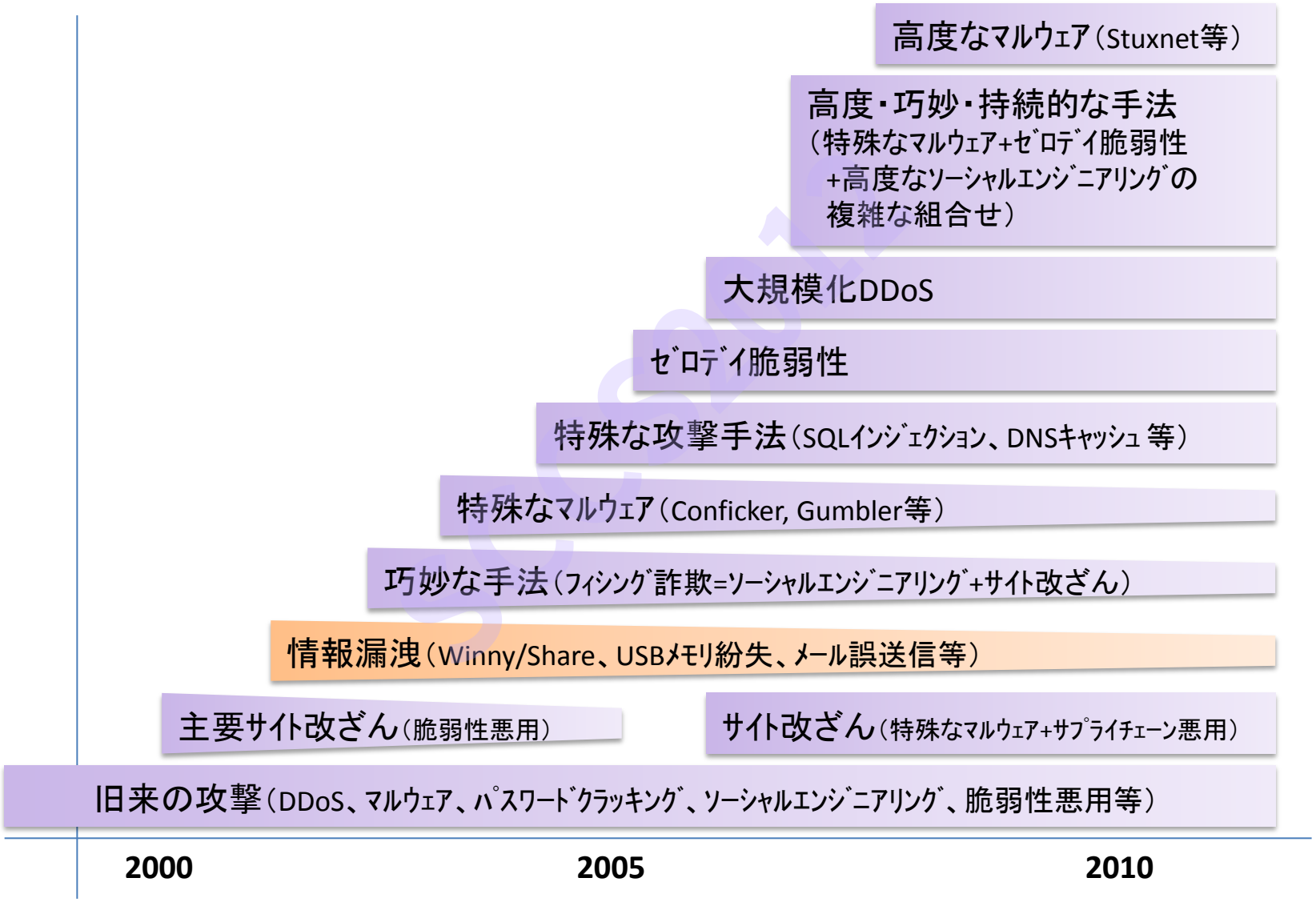
Anonymous によるサイバー攻撃（2011年、米国）（3）

ターゲット	起因するイベント	攻撃者の反応	時間差
Exxon Mobil, ConocoPhillips, Canadian Oil Sands, Imperial Oil（石油会社）	石油会社が、カナダのアルバータ州から米国テキサス州のポートアーサー間に2,100マイルの送油パイプラインの構築に取り掛かった。	Anonymous のメンバが“Operation Green Rights プロジェクト：Tarmageddon”を開始した。これは、大手石油会社にサイバー攻撃を行う意図と、環境問題に対する自分たちの位置づけを示した宣誓となる。 	パイプライン構築に伴い脅威を発生とあるが、まだ攻撃は発生していない。
法執行機関	捜査当局者が、複数の容疑で、Anonymous 攻撃者をターゲットとした全国的な活動を開始し、複数の容疑者を逮捕した。	Anonymous とLulzSec の一部メンバが、米国全土の70人以上の保安官事務所に対してサイバー攻撃を行ない、機微情報を含む10ギガバイトのデータを公開した。 	2週間後
BART（サンフランシスコの公共交通機関）管理センタ	BART 管理センターが、抗議団体の結成を抑制するために、幾つかの駅で非合法のモバイル電話サービスを遮断した。	Anonymous の一部メンバが、その公共交通機関管理センタのWebサイトに対してサイバー攻撃を行ない、その利用者の個人情報を含む 2,400人のユーザーアカウント個人情報を搾取した。 	1週間後

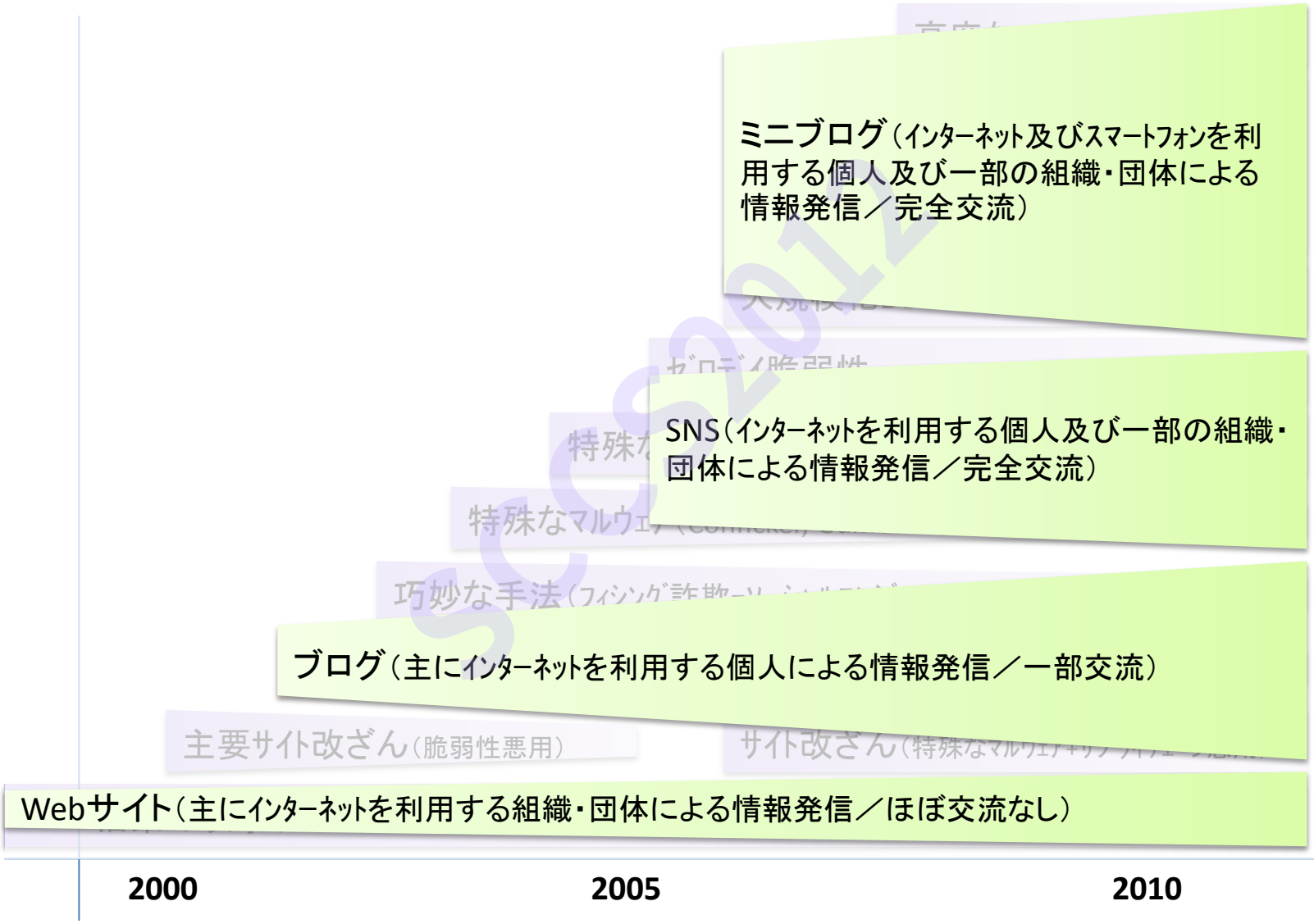
トピック 2

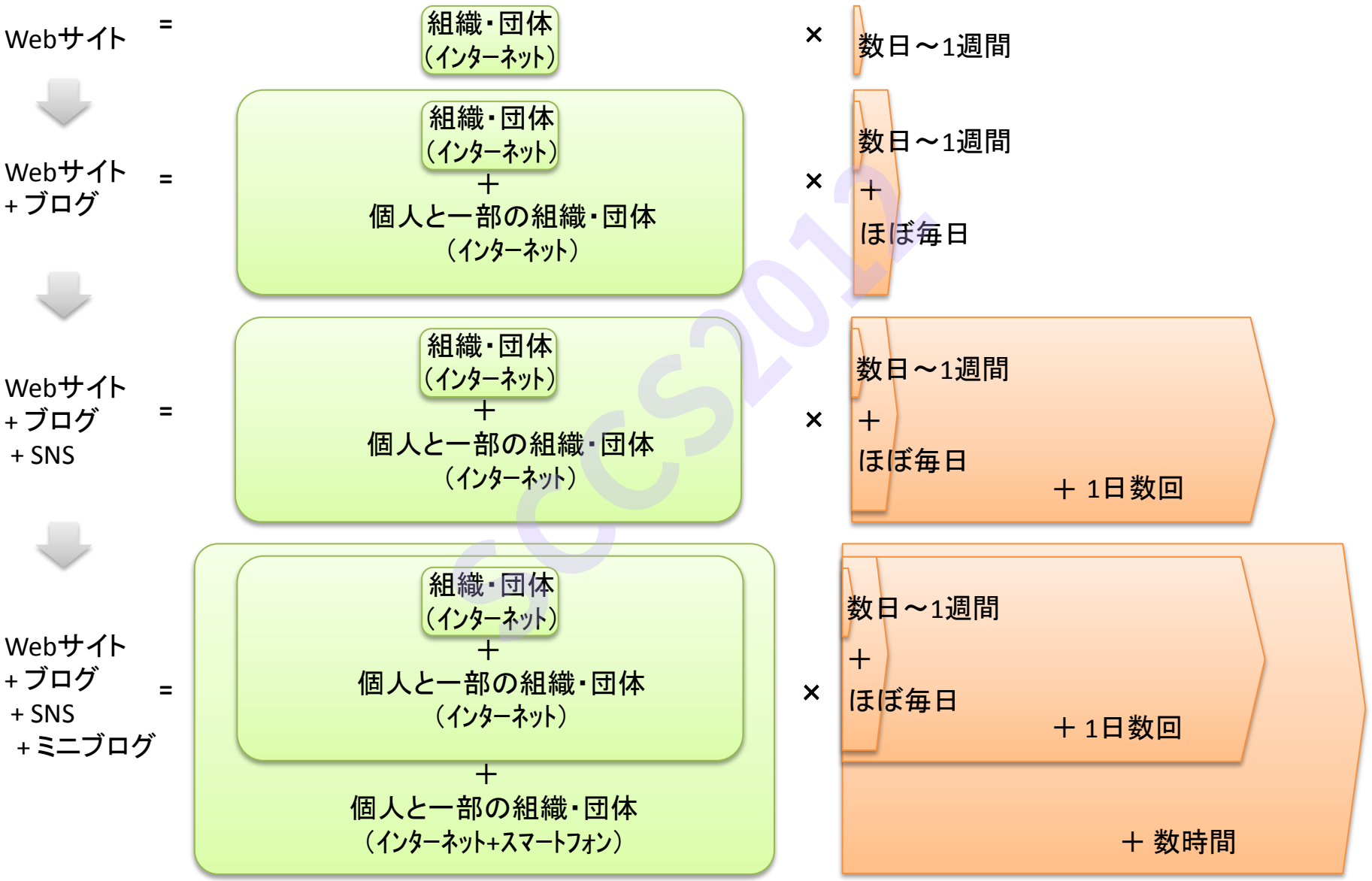
サイバー脅威の動向と既存対策の分析

国内のサイバー攻撃の動向変化

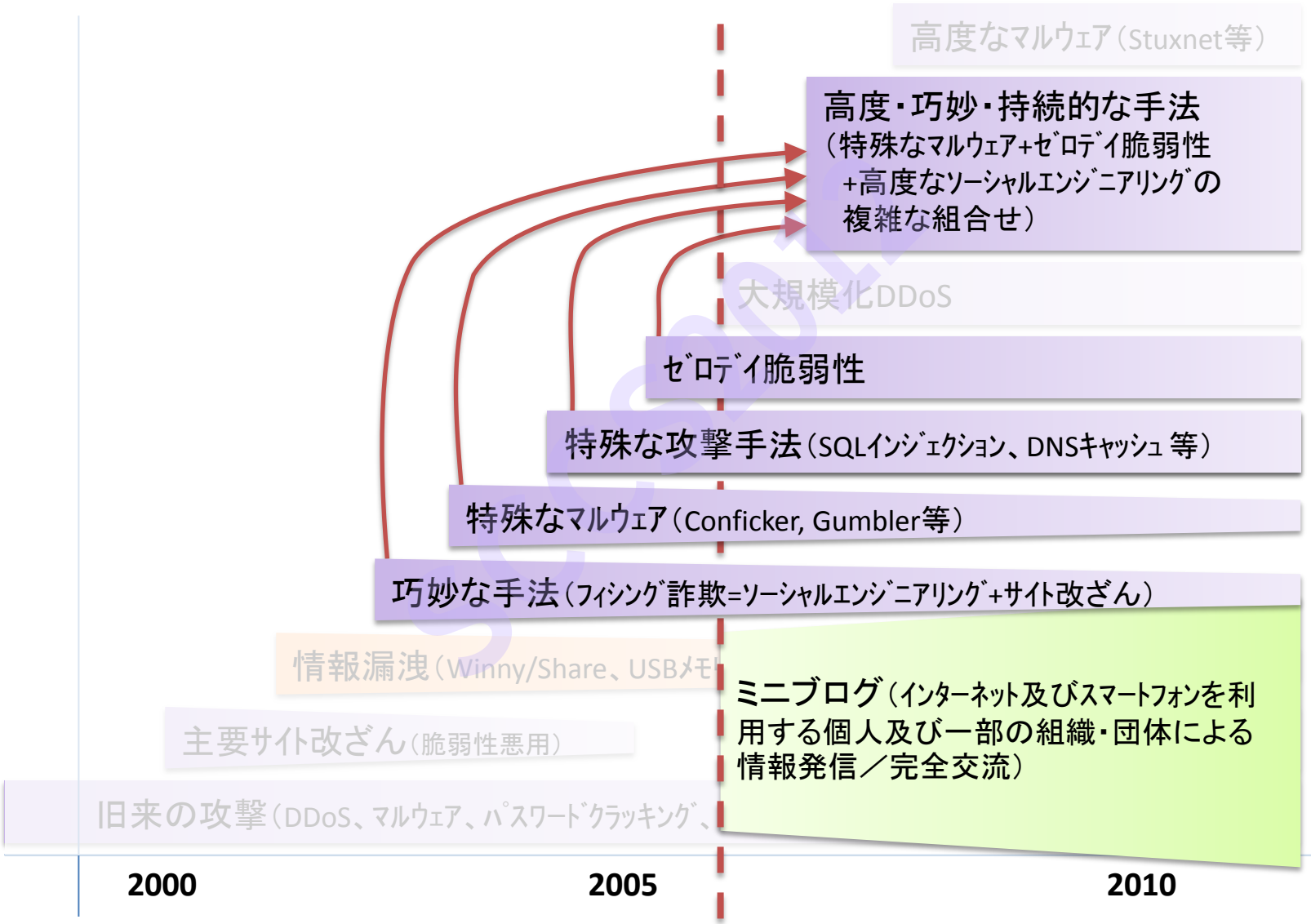


情報の発信／交流の変化

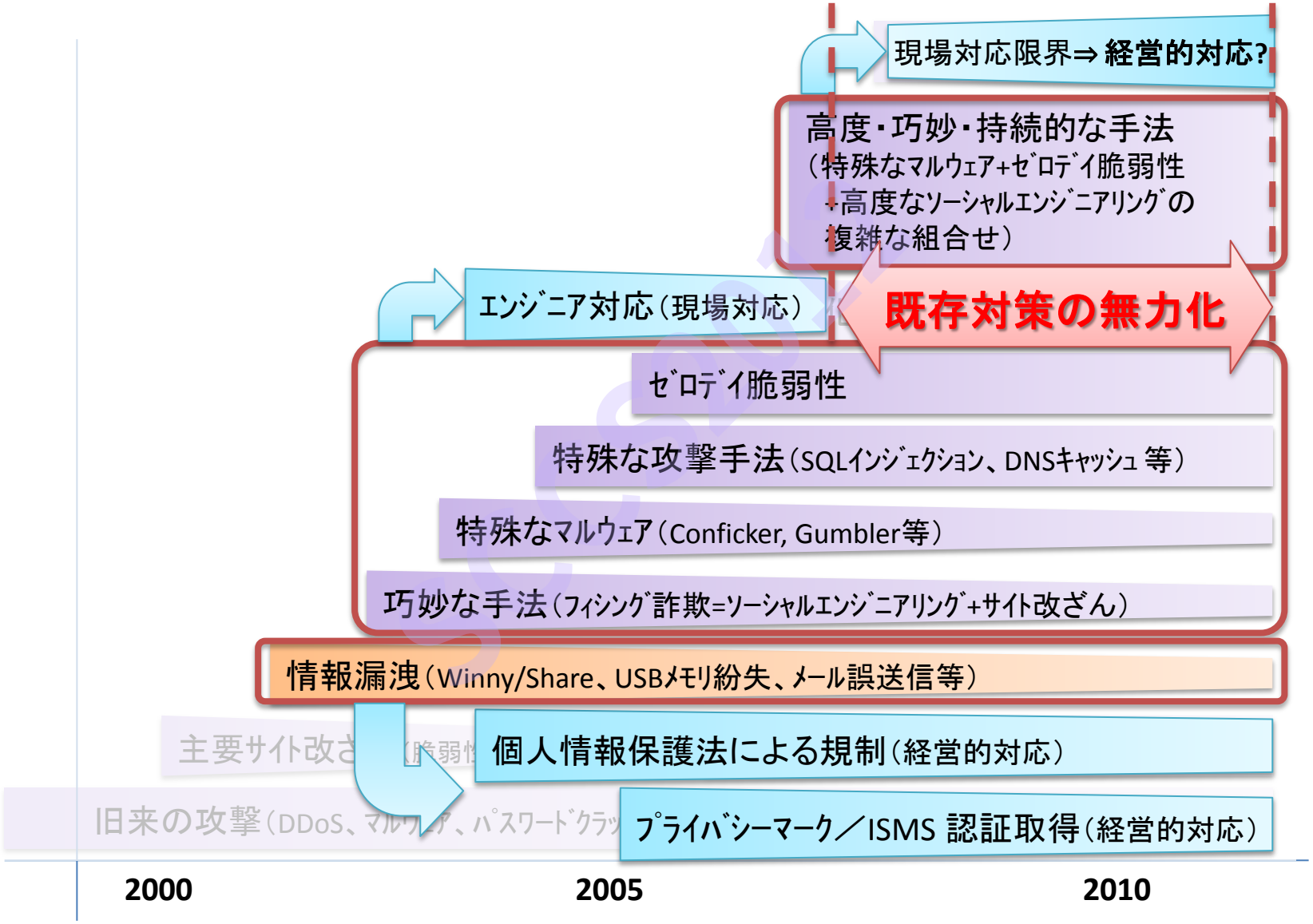




国内のサイバー攻撃の動向変化（ここ数年）



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

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アサイメント（業務割り振り）とジョブディスクリプション（業務内容）が明確

インシデントの発生と対応

IT部門

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**

事例解説

2011年 日本における標的型攻撃
ソニーグループ、三菱重工、衆議院

ソニーグループに対するサイバー攻撃（1）

	2010年	2011年 1月	2011年 2月	2011年 3月	2011年 4月	2011年 5月
事象	Hotz 氏による Playstation3 プロテクト解除	Hotz氏による PlayStation 3 改造方法 公開	ソニー技術的措置・警告	ソニーによる PlayStation 3 不正ツール 公開サイトの 閲覧IPアドレス 開示請求手続き（法的措置）	ソニーと Hotz氏の和解	ソニー記者会見
攻撃者	PlayStation3 機能削除 訴訟問題（米国）	ソニーによる Hotz氏ほか 100名に対する法的措置	ソニーによる 法的措置（ドイツ）		大規模侵害（情報搾取）攻撃	
アノニマス				#opsony Congratulations, Sony.	攻撃宣言 DDoS 攻撃 ソーシャルエンジニアリング攻撃 ソニーに対する抗議の扇動	

ソニーグループに対するサイバー攻撃（2）

	（2011年）6月	7月
ラルズセック 	ソニー・ミュージック（日本）	ソニー・ピクチャー（日本） ソニー BMG ベルギー ソニー BMG オランダ
アイダハク（レバノンのハッカー集団） 	ソニー・エリクソン カナダ	ソニー ヨーロッパ ソニーBMG ポルトガル
その他の攻撃者または特定の難しい主体	ソニー ・オンライン・エンターテイメント アメリカ ソネット（日本） ソニー タイ ソニー・ミュージック インドネシア ソニー・ミュージック ギリシャ	ソニー・ピクチャー ロシア

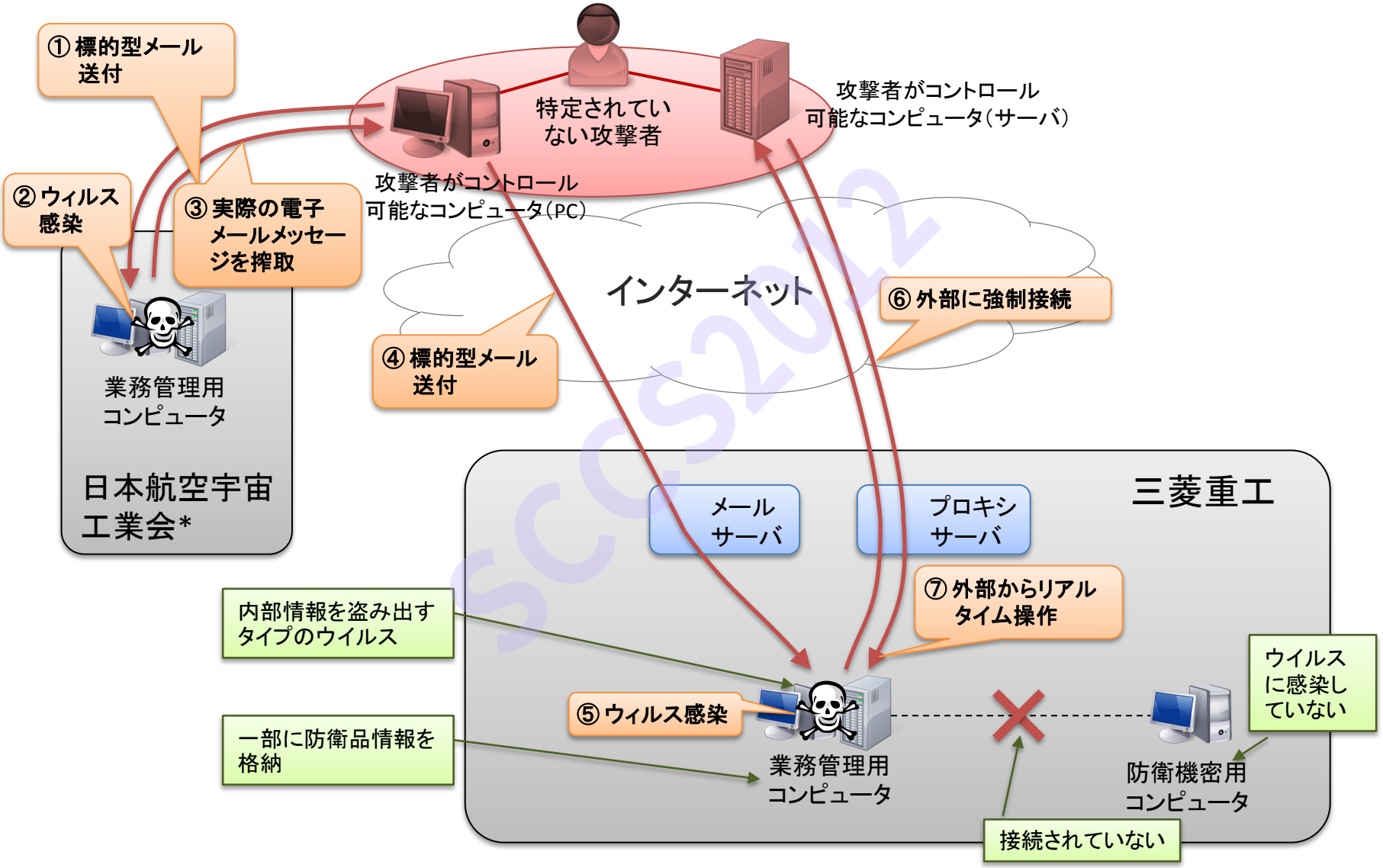
ソニーグループに対するサイバー攻撃(2)

サイバーディフェンス研究所によるアナリストコメント

- ***企業とハッカーのそれぞれの文化の違い***
  - システムの安全性を高めるため情報をブラックボックスに閉じ込めて管理したい「企業」と、技術の進化はオープンな環境から生まれると考えている「ハッカー」の間には、大きな意識の隔たりがある。
  - ソーシャルメディアの重要性が増してきているが、オンラインでコミュニティを作り、価値を生み出してきたのはハッカーである。目的は違うが、ハッカーの試行錯誤の歴史から学べる点はいろいろある。
  - 今日のインターネット技術は、ハッカーたちが産み出してきたものが多くある。その目的や考え方を学ぶことで、表層の現象だけでないレベルでインターネットを理解することができる。
  - インターネットは、もはや、ソニーという企業グループだけでなく、チュニジア等の一国の歴史を変えるほどの影響力を持ち、その影響力は相当大きなものがある。

- ***事後における社会的要請レベルの向上と単独(自社)対処可能レベルの低下(双方の乖離の拡大)***
  - サイバー空間を利用したIT関連のサービスやプロダクト(製品)と、その情報処理等の増大により、システムが複雑かつ大規模になる傾向にあり、インシデント発生時の規模が非常に大きくなる。しかし、サービス継続の観点で「インシデントを発生させない仕組み」に偏重することが多くなり、「インシデントが発生した場合の対処プロセス」に対する事前準備が不十分になりやすい。
  - ところが、世界各所で発生しているサイバーインシデントに対する懸念が高まる中、インシデント発生後における社会的な要請レベルが向上しているため、企業の経営層も、事後対応の仕組みの整備が急がれている雰囲気は感じ取っている。
  - しかしながら、企業における事後対応の仕組みや整備の実情としては、「現場任せ」のところが多く、経営層とIT管理やセキュリティ管理の部門と一体化になっていないのがほとんどである。このため、組織単独で対処可能な能力に一定の限界が出てくる。この理由は、サイバー空間で発生する事象に対する認識と判断基準が、経営層と現場のIT／セキュリティ部門では大きく異なり、解決に向けた対処プロセスに食い違いが出てくるためである。
  - 今回のソニーの不正アクセスによる情報漏洩問題に関するさまざまな公表情報を見る限りでは、規模の拡大を続けるソニーが、社会的要請レベルの十分な認識と、それに見合う「インシデント発生後の対処能力」を実現可能とする体制や対処準備がされていたとは言い難い。

三菱重工に対するサイバー攻撃(1)



*日本航空宇宙工業会: 航空宇宙工業の健全な発展を図り、世界の航空宇宙産業の健全な発展に貢献することを目的とする民間公益団体

三菱重工に対するサイバー攻撃(2)

サイバーディフェンス研究所によるアナリストコメント

- 三菱重工業に対するサイバー攻撃について、注目すべき攻撃技術分析情報は、次の3つのマルウェア分析レポートである。
  - Sophos　Troj/Derusbi-A (2011月9月21日)
    http://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj~Derusbi-A/detailed-analysis.aspx
  - Symantec　Infostealer.Derusbi (2011年9月30日)
    http://www.symantec.com/security_response/writeup.jsp?docid=2011-093012-0008-99&tabid=2
  - Dr.Web　Trojan.DownLoader4.46395（公開日不明）
    http://www.drwebhk.com/zh/virus_techinfo/Trojan.DownLoader4.46395.html
- それぞれの発見されたマルウェアが「proxy.smw.mhi.co.jp」の DNSクエリを実行しようとしているが、次のサイトで確認する限り、このドメインは存在しているようである。

Base	Record	Name		IP	Reverse	Route	AS
proxy.smw.mhi.co.jp 22 minutes old	mx	10	mx03.mhi.co.jp 7 minutes old	202.32.46.6 Japan	(none)	202.32.0.0/16 IIJ CIDR BLOCK 1 (AS2497) Jinbocho Mitsui Bldg., 1-105 Kanda Jinbo-cho, Chiyoda-ku, Tokyo 101-0051, Japan	AS2497 IIJ-AS-JP1 IIJNET
		10	mx04.mhi.co.jp 1469 days old	202.32.46.101 Japan	scm-yokohama.mhi.co.jp		
		20	mx01.mhi.co.jp 914 days old	202.32.46.101 Japan			
		20	mx02.mhi.co.jp 1168 days old	210.199.211.247 Japan	smtp-kobe.mhi.co.jp	210.199.128.0/17 POWEREDCOM	AS4716 POWEREDCOM , Garden Air Tower, 3-10-,Iidabashi,Tiyoda-ku,Tokyo, 102-8460,Japan

http://www.robtex.com/dns/proxy.smw.mhi.co.jp.html#records
（2012年3月20日11:55確認）

- このドメインは、インターネット上の Whois で公開されていなく、かつ、proxy（代理）という言葉を利用していることから、内部のローカルネットワークで利用されているものであると考えられる。
- Dr.Web の分析では、このマルウェアは「proxy.smw.mhi.co.jp:12080」に接続を試みるとされている。
  - 12080ポートは、チェコ共和国に本社を置くAVAST Software a.s. が開発、販売するウィルス対策ソフト avast! antivirus において、Webshield と呼ばれるWeb閲覧リアルタム監視で自動的に設定されるローカルプロキシとして設定されるポートである。
  - この他、Dwyco Video Conferencing, NetworkServer のアプリケーションでも使われているポートでもある。
- Sophos の報告では、12080ポートで バックドア型HTTP プロキシとして機能するマルウェアが存在する。
  - Sophos Troj/Agent-E
    http://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj~Agent-E/detailed-analysis.aspx

三菱重工に対するサイバー攻撃(3)

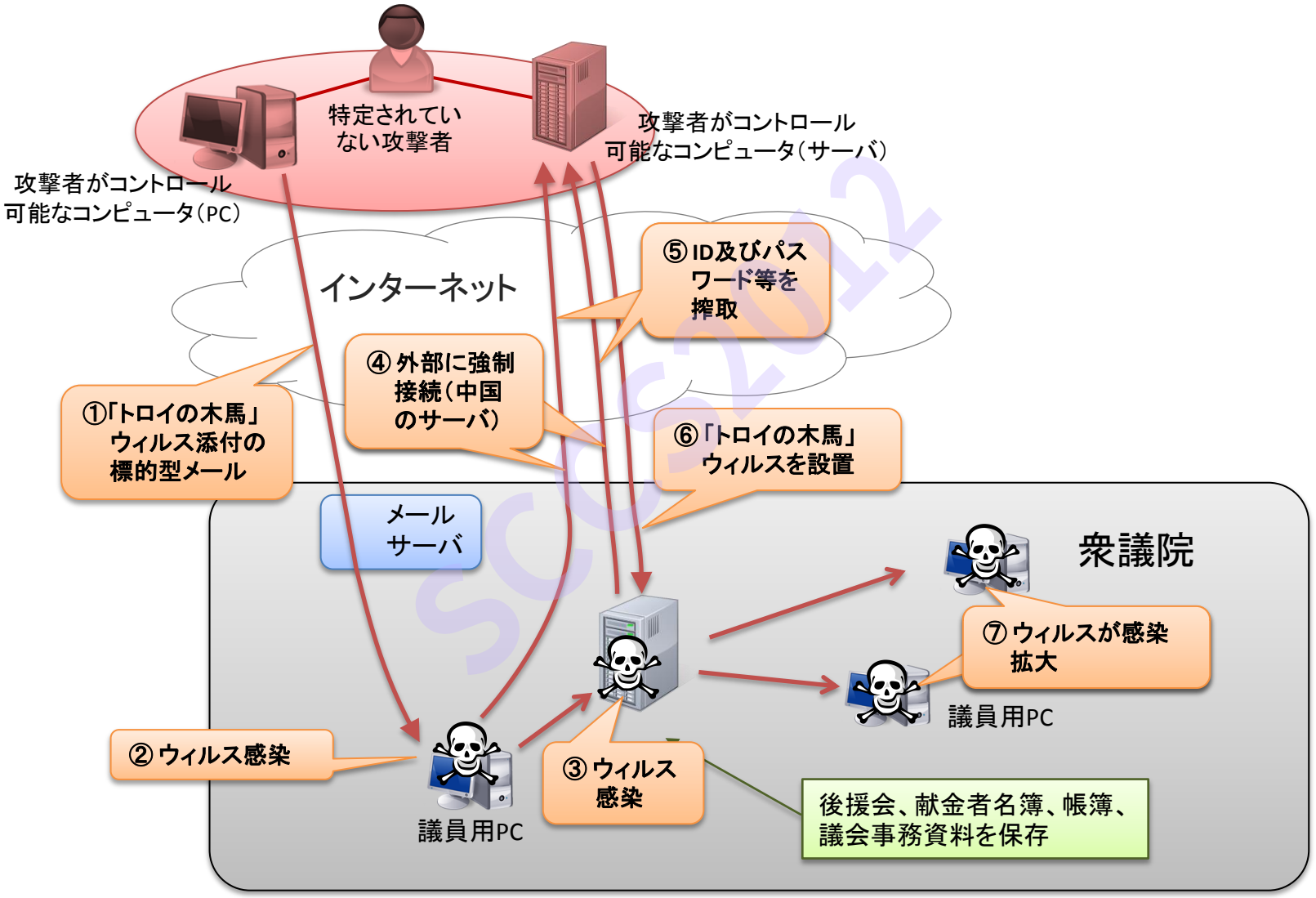
サイバーディフェンス研究所によるアナリストコメント

- ***社内の部署の有機的な連携について***
  - 三菱重工の説明では、情報セキュリティ確保は「IT推進部」と「総務部」が中心となって全社的に体制をもって取り組んでいることになっている。
  - しかし、情報通信技術は、事業プロセスに深く入り込んでいるため、インフラ及びサポートの役割を担う「IT推進部」と「総務部」がどこまで、事業推進を担う「事業関連部門」に対して、セキュリティ確保にかかる強い影響力を行使できていたかについて注目すべき。

- ***外部からの積極的なサイバー攻撃対処に関する取り組みについて***
  - 三菱重工の説明では、インシデントを発生させないという文脈の取り組みが多く見られるが、インシデントが発生した後の取り組みに関するものがほとんどみられない。
  - サイバー攻撃への取り組みとしては、従業員の不可抗力によるウィルス感染に対する対策と読み取れるものしかない状況である。
  - 最近は、攻撃者による積極的なサイバー攻撃が多発しており、従業員が意識をしていても、「不可抗力によるウィルス感染の防止策」だけでは継続的かつ巧妙に仕掛けられるサイバー攻撃に対しては無力になることがほとんどである。

- ***インシデント対応能力について***
  - 2011年5月下旬にサイバー攻撃を受けた米国軍事産業企業ロッキード・マーチンは、その直後の声明において、「社内の情報セキュリティ部門が攻撃開始とほぼ同時に、情報システムとデータを保護するための“積極的な行動”を取り、速やかに対応したため、被害はなかった」としている。つまり、ロッキード・マーチン社内の部署のインシデント対応能力は高いレベルにあったことを示唆している。
  - しかし、2011年8月の三菱重工の場合は、サイバー攻撃発生後、声明を出すことなく、外部のセキュリティ会社や警察と相談というプロセスをとったところを鑑みると、社内のインシデント対応能力は十分でなかった可能性がある。

衆議院に対するサイバー攻撃

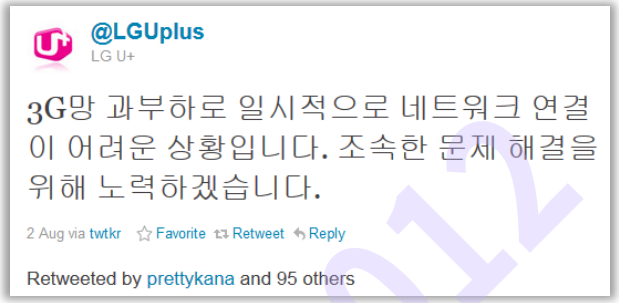


事例解説

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。」

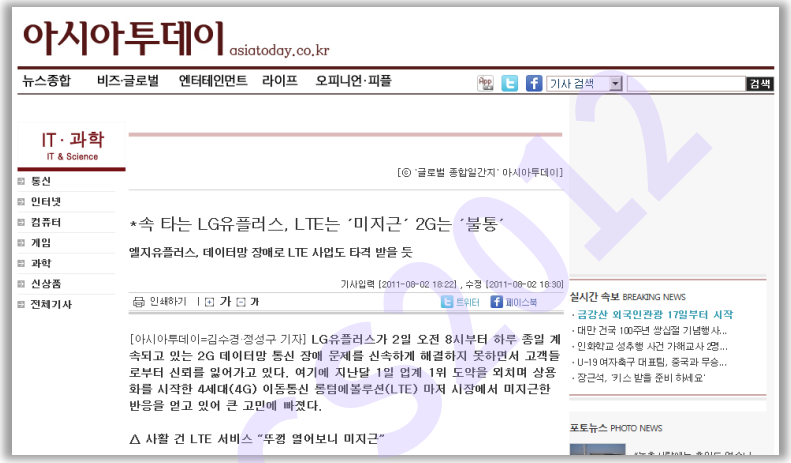
情報収集(2)

- 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で過負荷**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。」

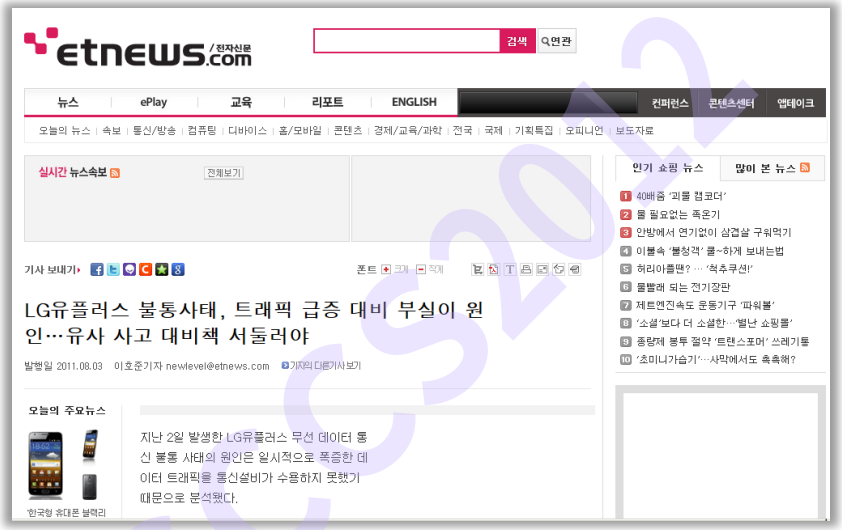
情報収集(4)

- 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ユープラスは明らかにした。」
  - 「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.

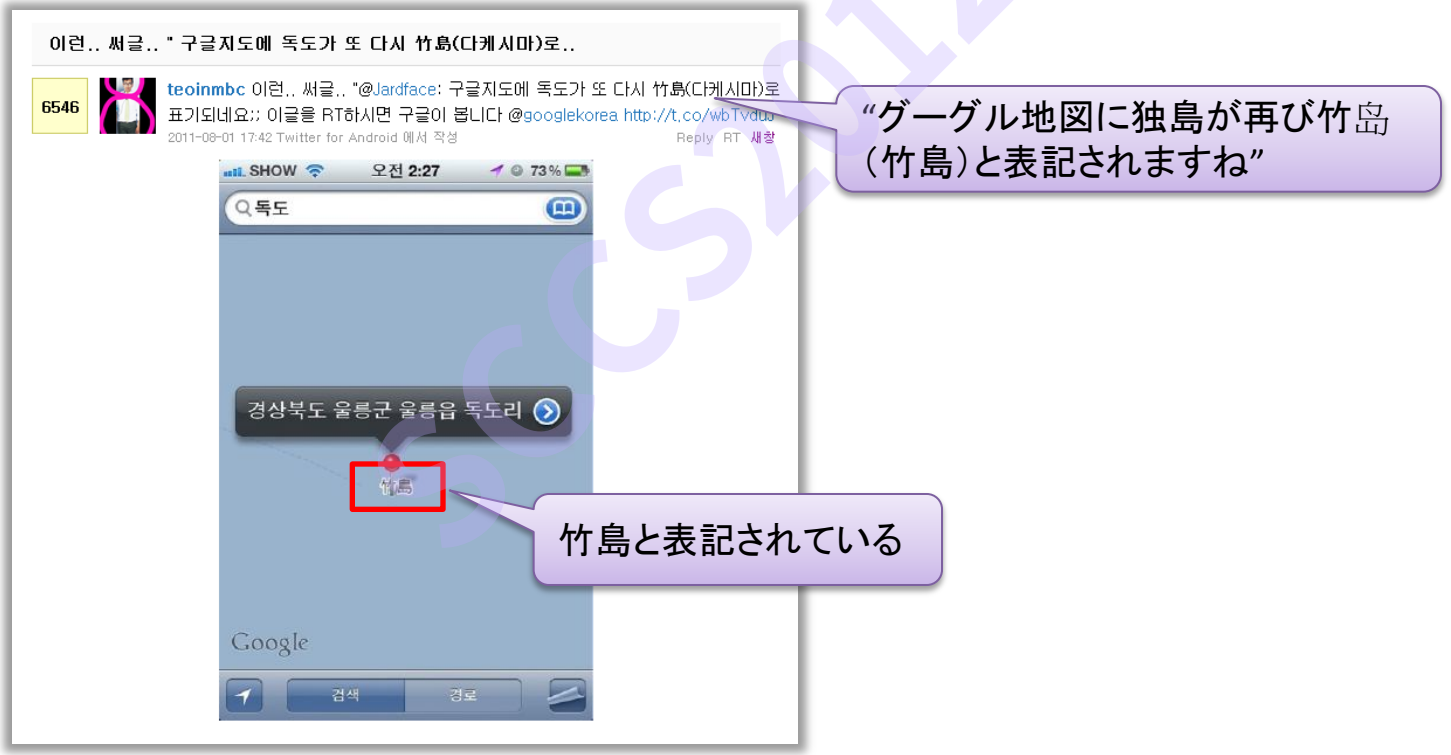
http://www.newsis.com/article/print.htm?ar_id=NISX20110719_0008714357&type=1

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、韓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+ のネットワーク系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

事例解説

2011年-2012年 ANDROID ﾓﾊﾞｲﾙ用犯罪ｱﾌﾟﾘ(ZITMO)

ZITMO とは

- ZITMO とは
  - Zeus In The MObile：Android モバイルをターゲットにした、情報搾取が目的のトロイの木馬型マルウェア
  - PCからモバイルにターゲットを広げた ZueS の亜種であり、
    - Zeusとは、主に金融機関の顧客のPCをターゲットにし、金融機関の認証情報を搾取を目的とし、結果としてインターネット上の電子取引から不正に利益を得ることを可能にしたトロイの木馬型マルウェア
  - 2011年2月、ポーランド国内銀行の Android モバイルフォンを利用した顧客に影響を与えた新しい脅威として認識される。

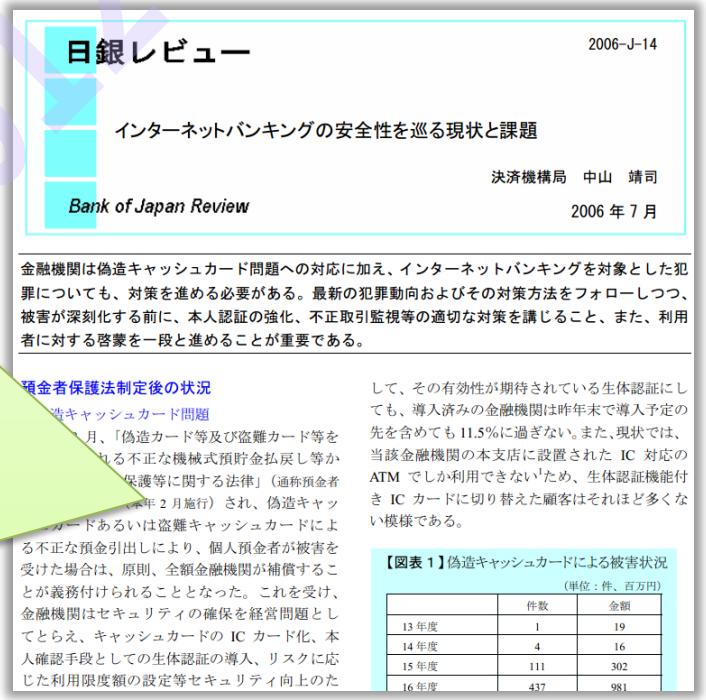
- ZITMO の目的
  - 多くの銀行が、モバイルデバイス向けの新しいセキュリティ対策として、モバイルを通じた取り引きを行う際、2要素認証として m-TAN（Mobile Transaction Authentication Number）をSMS 経由で送信している認証情報を第三者に送信させる。

- ZITMOの特性（2011年7月時点の分析）
  - すべてのSMSメッセージを傍受し、第三者に対する送信に、暗号化されず、難読化もされていない（高度なマルウェアではない）
  - SMS傍受したメッセージをフィルタしていないため、特定の銀行を狙ったものではない。（単なるSMSスパイウェアと呼ばれることもある）
  - 第三者の意図による、アドホックな SMSメッセージ盗聴やURL変更等のメカニズムがないため、（Zeusに比べると機能不十分）

m-TAN の説明

- 日本銀行による m-TAN の説明

③ 必要の都度別の通信経路で連絡するタイプ
取引の都度、インターネットとは別の通信経路で、リアルタイムにパスワードが送られてくる方法等である。**代表的なものとしては、あらかじめ登録されている携帯電話のSMS（ショートメッセージサービス）等にパスワードが送られてくるmobile-TAN等がある。**インターネット以外に別の通信経路を使っているため、「二経路認証」にもなっている。
なお、ワンタイムパスワードではないが、携帯電話を使った他のセキュリティ対策としては、携帯電話自体を認証トークンとして位置付け、取引の際に携帯電話にコールバックを行い、通常のパスワードを携帯電話経由で送信することによって認証するタイプのものや、予め携帯電話によって口座のロックを解除する連絡をしないと資金移動が出来なくするといった方法も存在する。



日銀レビュー　2006-J-14

インターネットバンキングの安全性を巡る現状と課題

決済機構局　中山　靖司

Bank of Japan Review　2006 年 7 月

金融機関は偽造キャッシュカード問題への対応に加え、インターネットバンキングを対象とした犯罪についても、対策を進める必要がある。最新の犯罪動向およびその対策方法をフォローしつつ、被害が深刻化する前に、本人認証の強化、不正取引監視等の適切な対策を講じること、また、利用者に対する啓蒙を一段と進めることが重要である。

預金者保護法制定後の状況

偽造キャッシュカード問題

…月、「偽造カード等及び盗難カード等を…る不正な機械式預貯金払戻し等か…保護等に関する法律」（通称預金者…年 2 月施行）され、偽造キャッ…カードあるいは盗難キャッシュカードによる不正な預金引出しにより、個人預金者が被害を受けた場合は、原則、全額金融機関が補償することが義務付けられることとなった。これを受け、金融機関はセキュリティの確保を経営問題としてとらえ、キャッシュカードの IC カード化、本人確認手段としての生体認証の導入、リスクに応じた利用限度額の設定等セキュリティ向上のため…

して、その有効性が期待されている生体認証にしても、導入済みの金融機関は昨年末で導入予定の先を含めても 11.5%に過ぎない。また、現状では、当該金融機関の本支店に設置された IC 対応の ATM でしか利用できない[1]ため、生体認証機能付き IC カードに切り替えた顧客はそれほど多くない模様である。

【図表 1】偽造キャッシュカードによる被害状況

（単位：件、百万円）

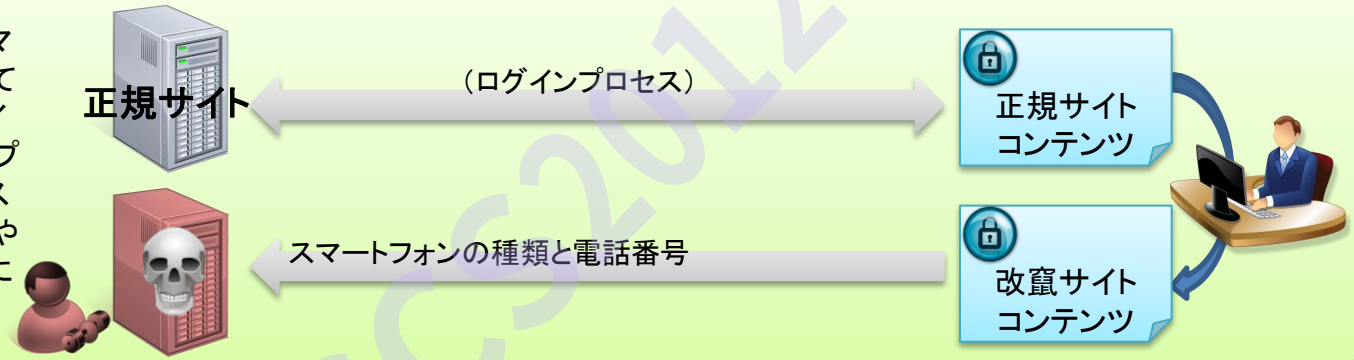
	件数	金額
13 年度	1	19
14 年度	4	16
15 年度	111	302
16 年度	437	981

インターネットバンキングの安全性を巡る現状と課題（日本銀行 2006年7月）
http://www.boj.or.jp/research/wps_rev/rev_2006/data/rev06j14.pdf

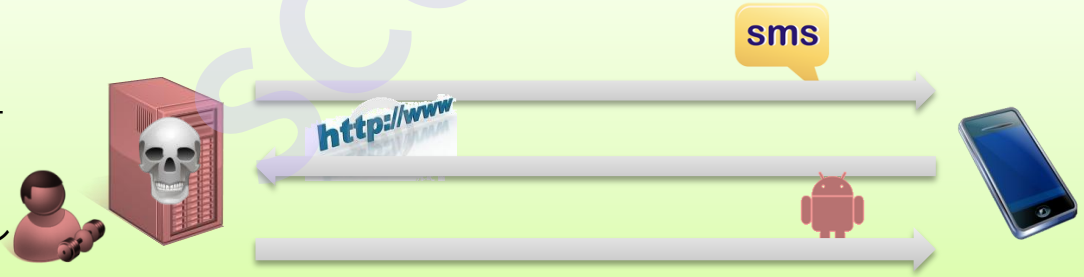
ZITMO の展開プロセス

1. 攻撃者が、ドライブバイダウンロードなどの手法によりPCにマルウェアをインストールする。

2. インストールされたマルウェアが、閲覧している正規の銀行サイトのログインの一部プロセスを改ざんし、スマートフォンの種類や電話番号を攻撃者に通知させる。



3. 攻撃者が、2. で得た情報を元に、被害者のスマートフォンに対して悪意のあるSMSメッセージを送付し、ZITMO をインストールさせる。

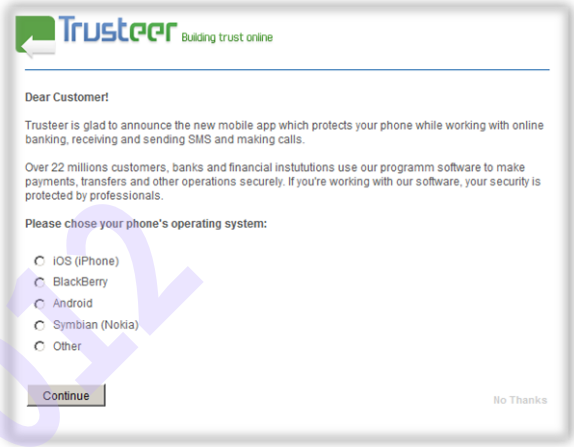


3. 攻撃者が、被害者のスマートフォンに着信したSMSメッセージを不正に入手。

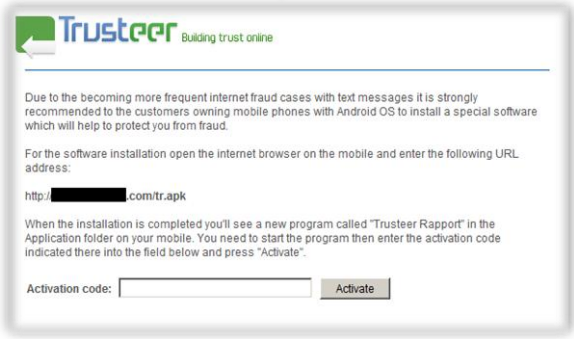
ZITMO の事例（1）

- 2011年7月、アンドロイドフォンをターゲットにした ZITMOが発見される。
  1. フィッシング詐欺目的で送付された SMS メッセージ中の URL をクリックすると、次のようなサイトにアクセスする。
  2. http://**********.com/tr.apk からセキュリティソフトと見せかけた、不正なアプリ（ZITMO）を、アンドロイドフォンにダウンロードさせる。
  3. アンドロイドフォンにインストールされた ZITMO は、受信したSMSメッセージを http://******rifty.com/security.jsp に送信する。
     - 送信フォーマットは、次のとおり。
       f0={SMS_sender_number}&b0={SMS_text}&pid={infected_device_ID}

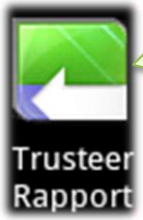
1.



2.



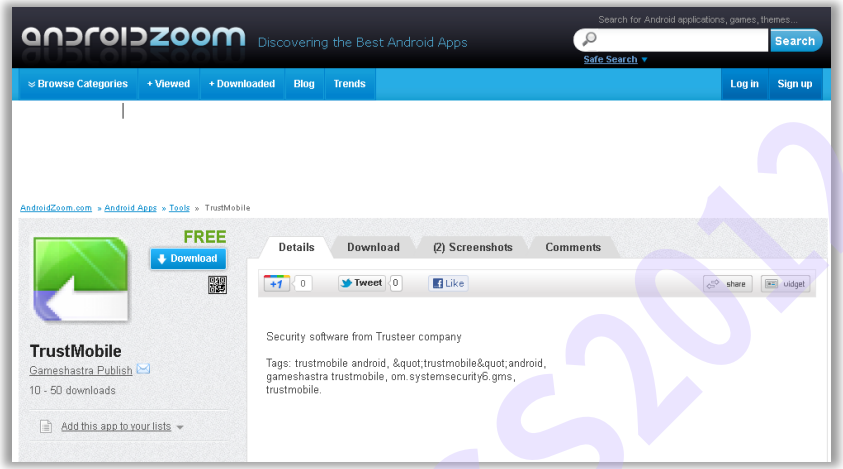
3.



- サイズ：19KB
- アンドロイドマーケットから削除されているが、他のミラーサイトで公開中。

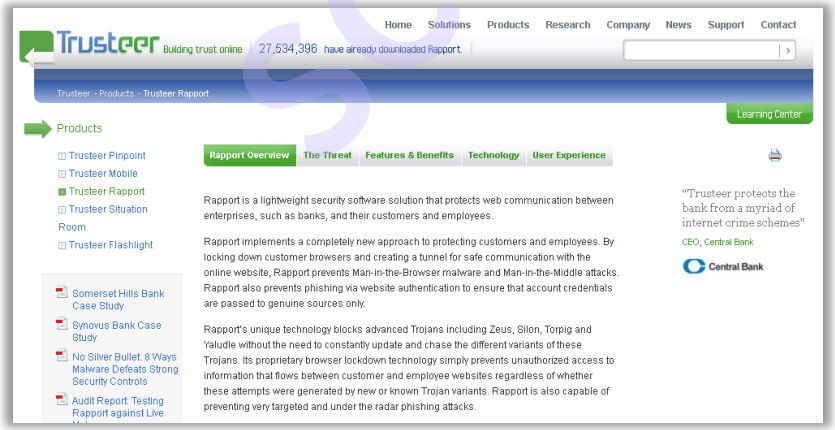
ZITMO の事例(2)

- 2011年3月11日時点で公開されている ZITMO アプリ



http://www.androidzoom.com/android_applications/tools/trustmobile_bbvkl.html

- 本物の Trusteer のサイト



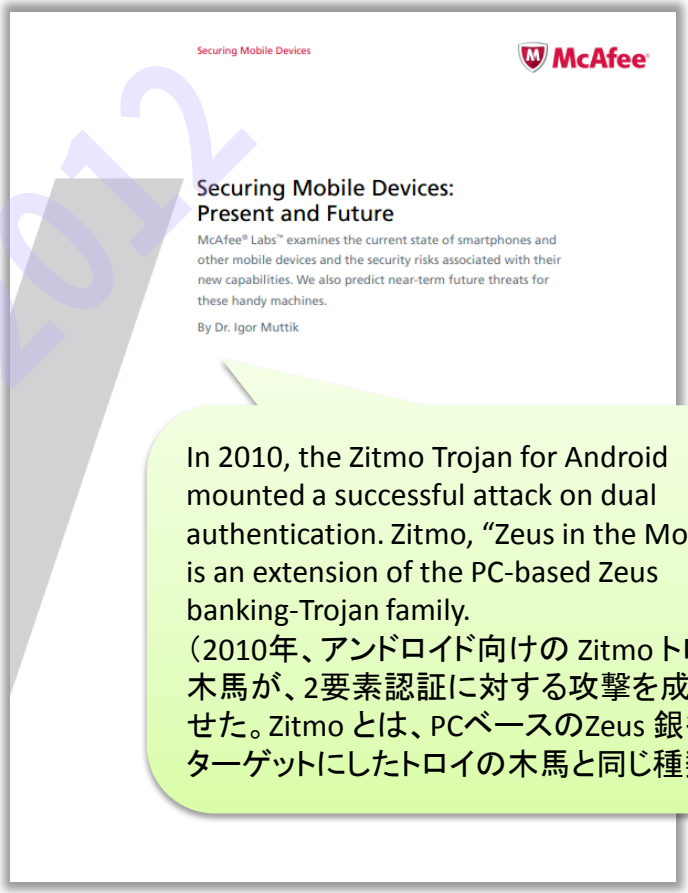
http://www.trusteer.com/product/trusteer-rapport

ZITMO に関する報告

M86 Security Lab による報告

http://www.m86security.com/documents/pdfs/security_labs/m86_security_labs_predictions_2012.pdf

McAfee による報告



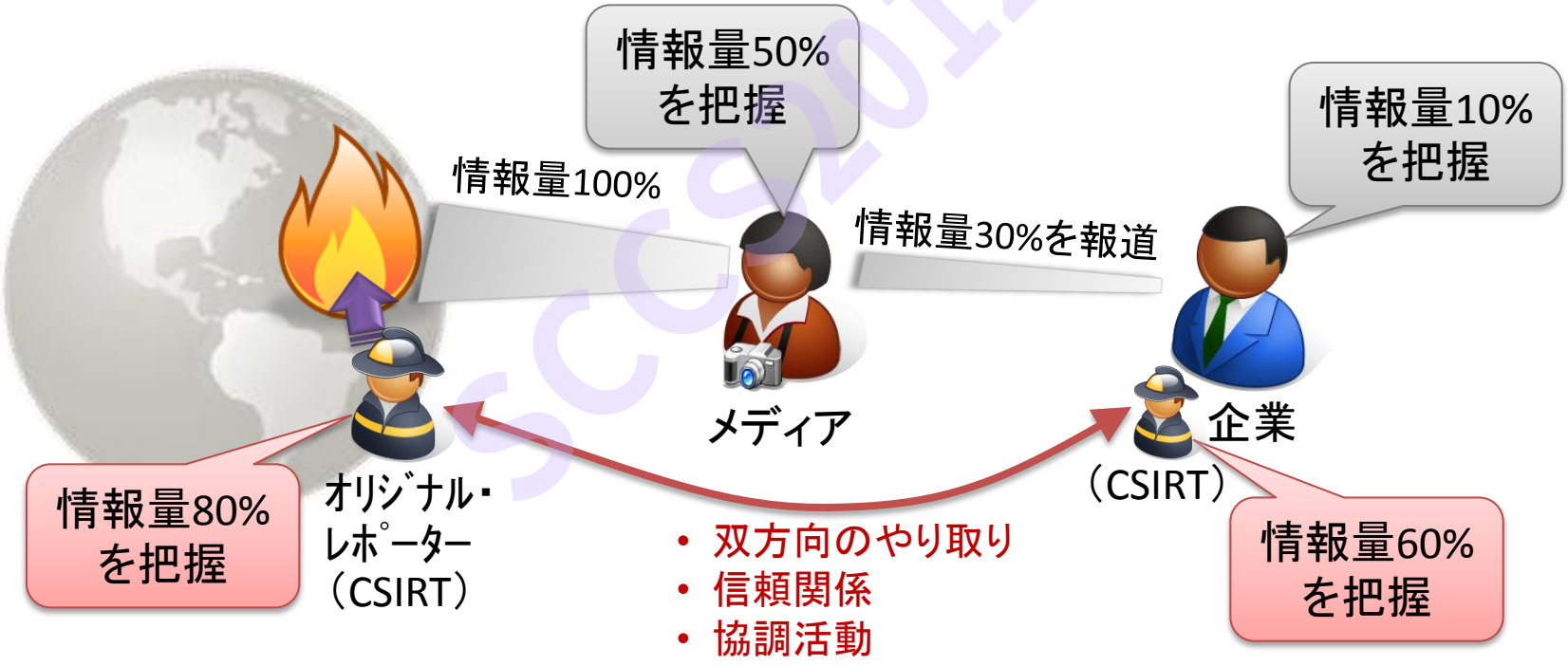
http://www.mcafee.com/us/resources/reports/rp-securing-mobile-devices.pdf

トピック 3

今後の組織に求められる防衛策のポイント

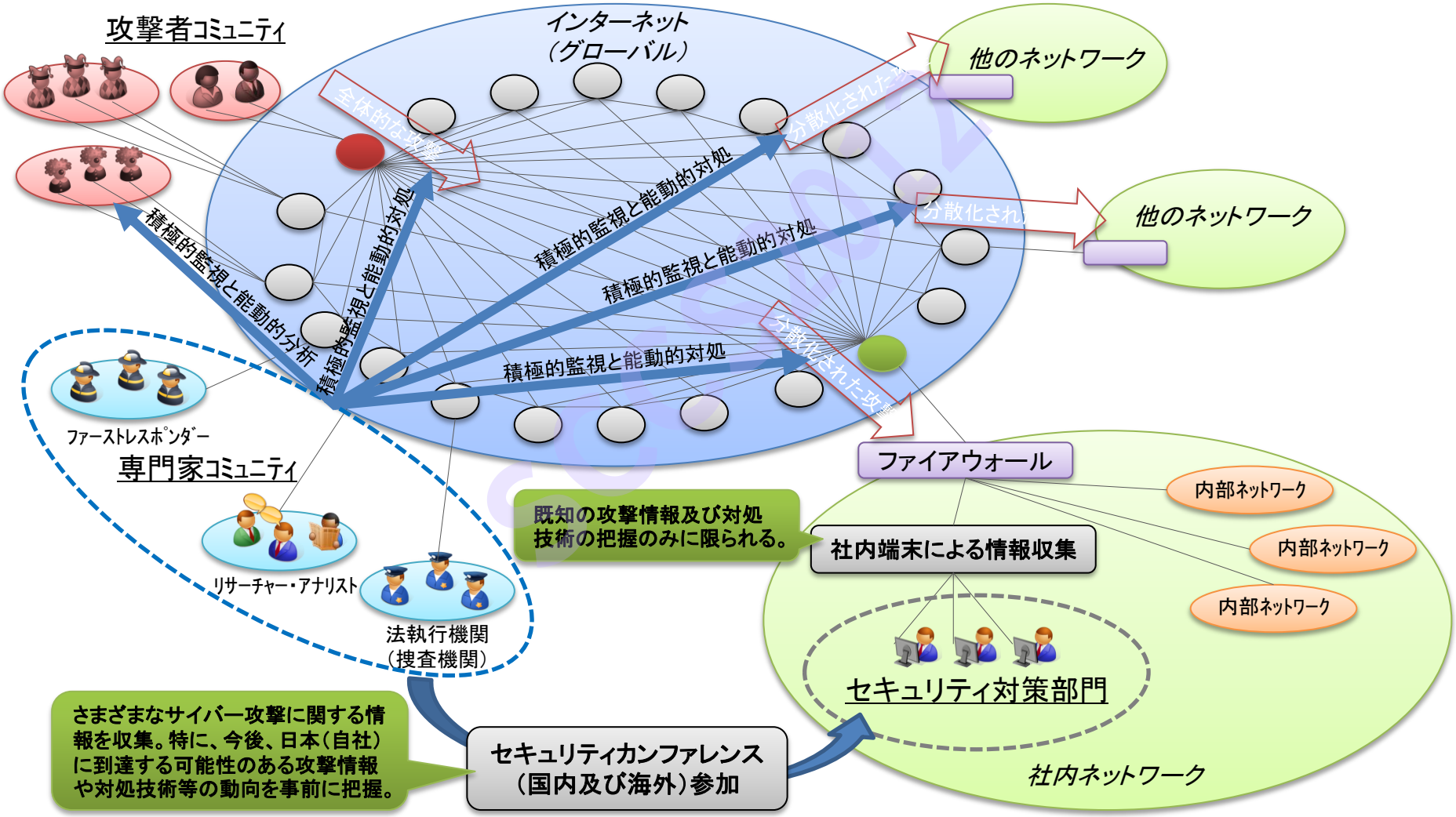
防衛策の「現実的な策定」をするためのポイント(1)

- 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



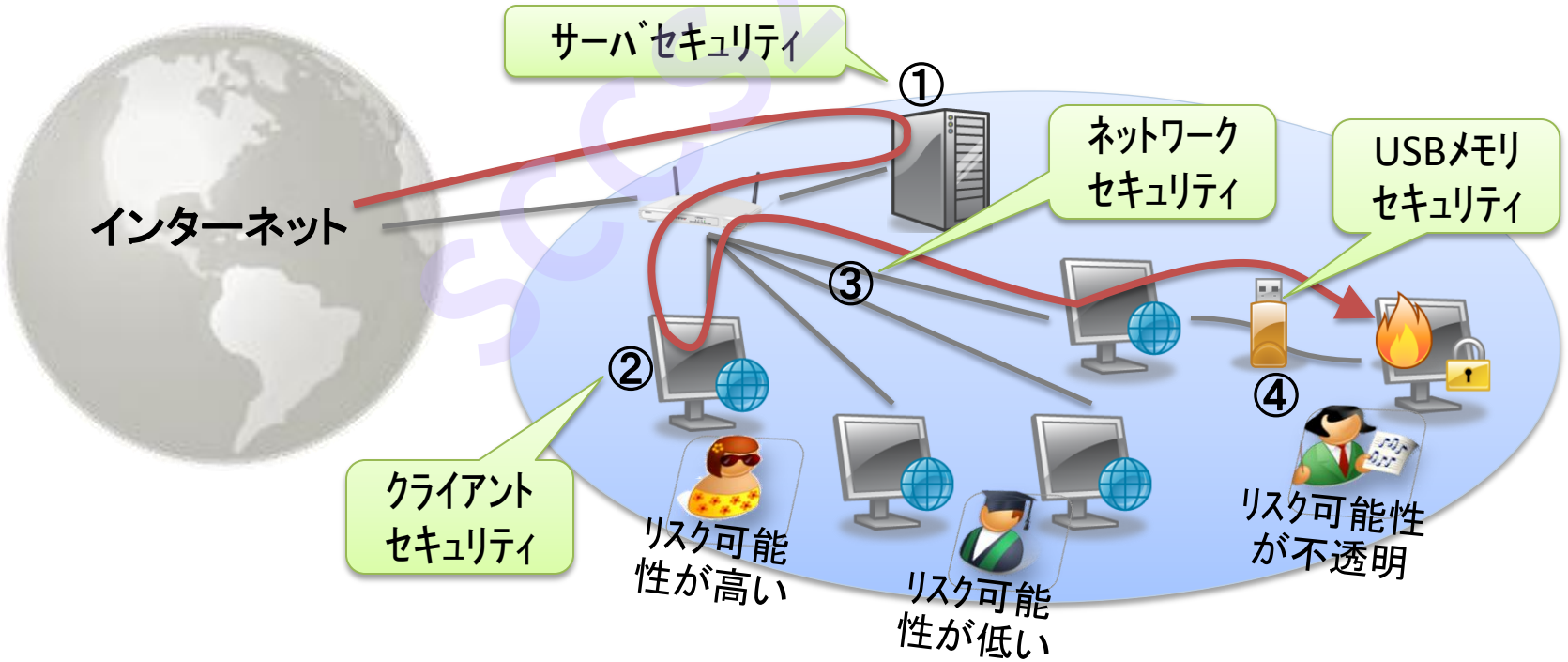
防衛策の「現実的な策定」をするためのポイント(2)

- 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**



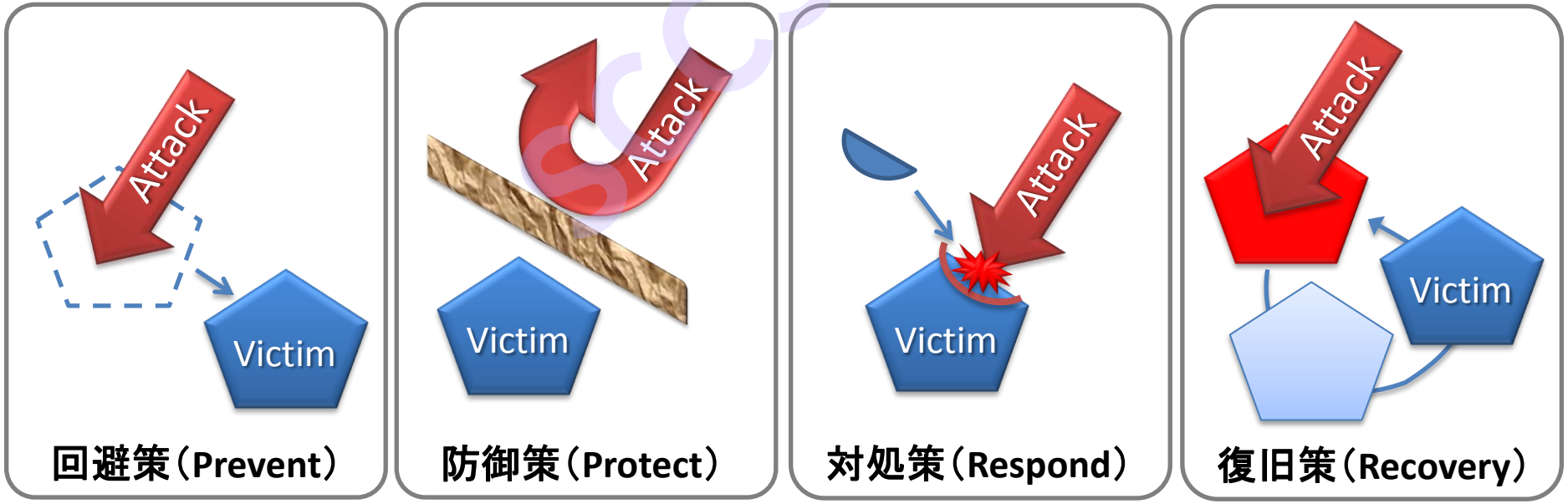
防衛策の「現実的な策定」をするためのポイント(3)

- 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: 03-3424-8700

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