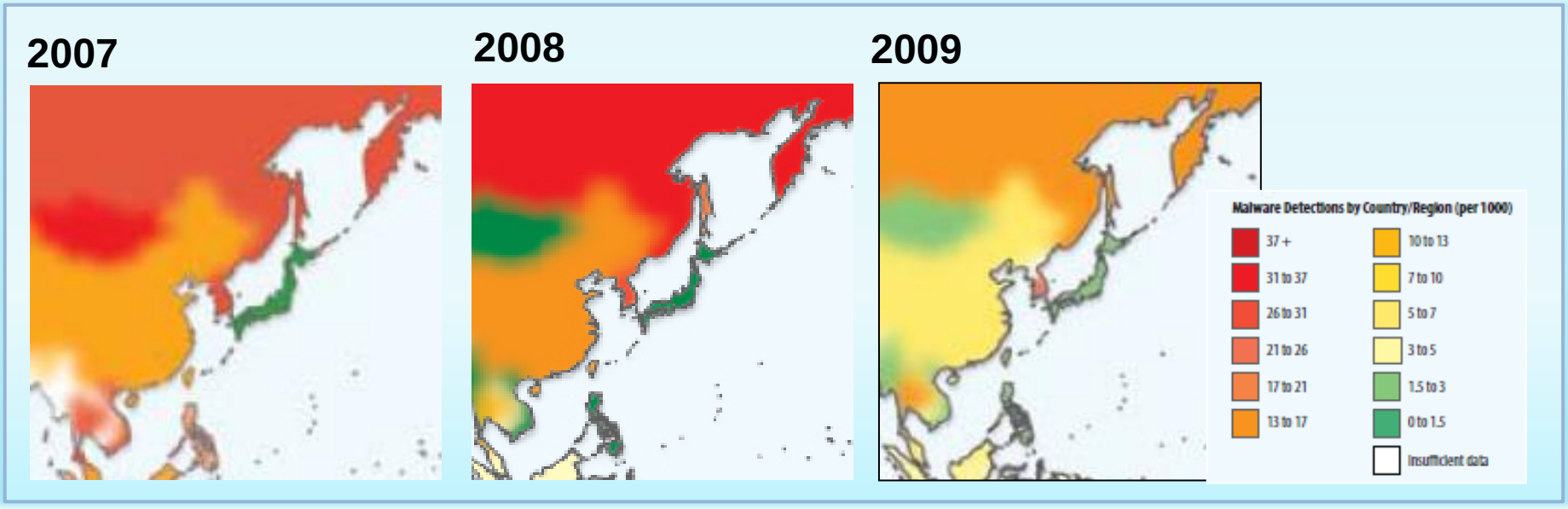
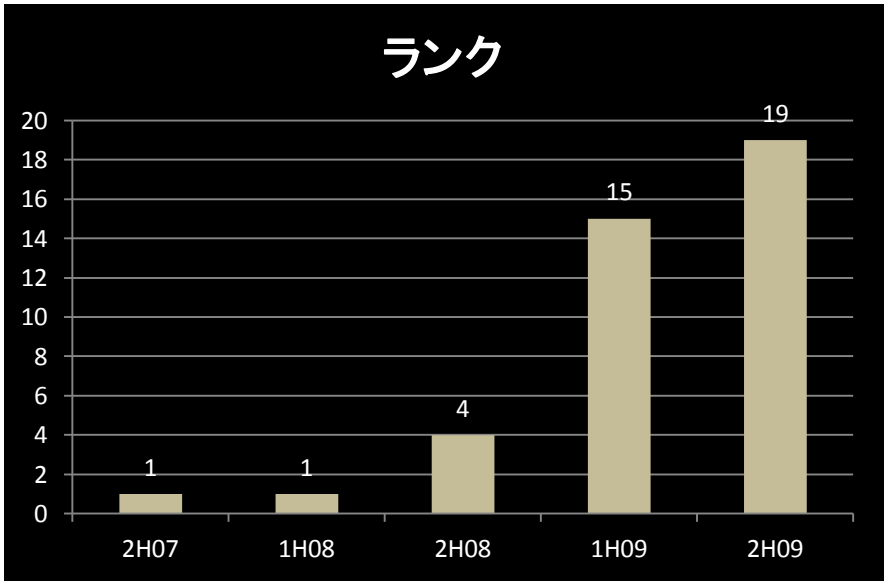
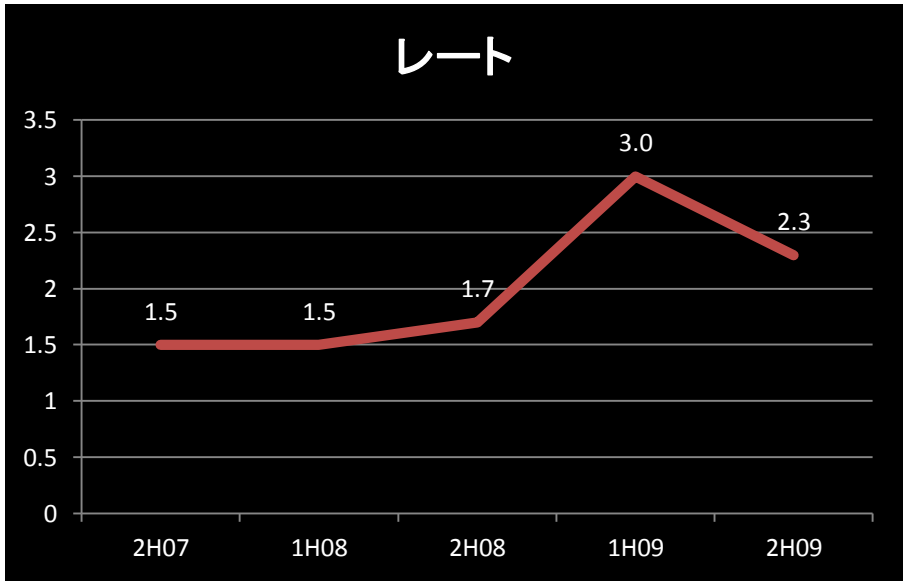
転換期を迎えた情報セキュリティ対策
～ システムとデータをいかに守るのか～

日本マイクロソフト株式会社
チーフセキュリティアドバイザー
高橋　正和

日本は安全なのか？

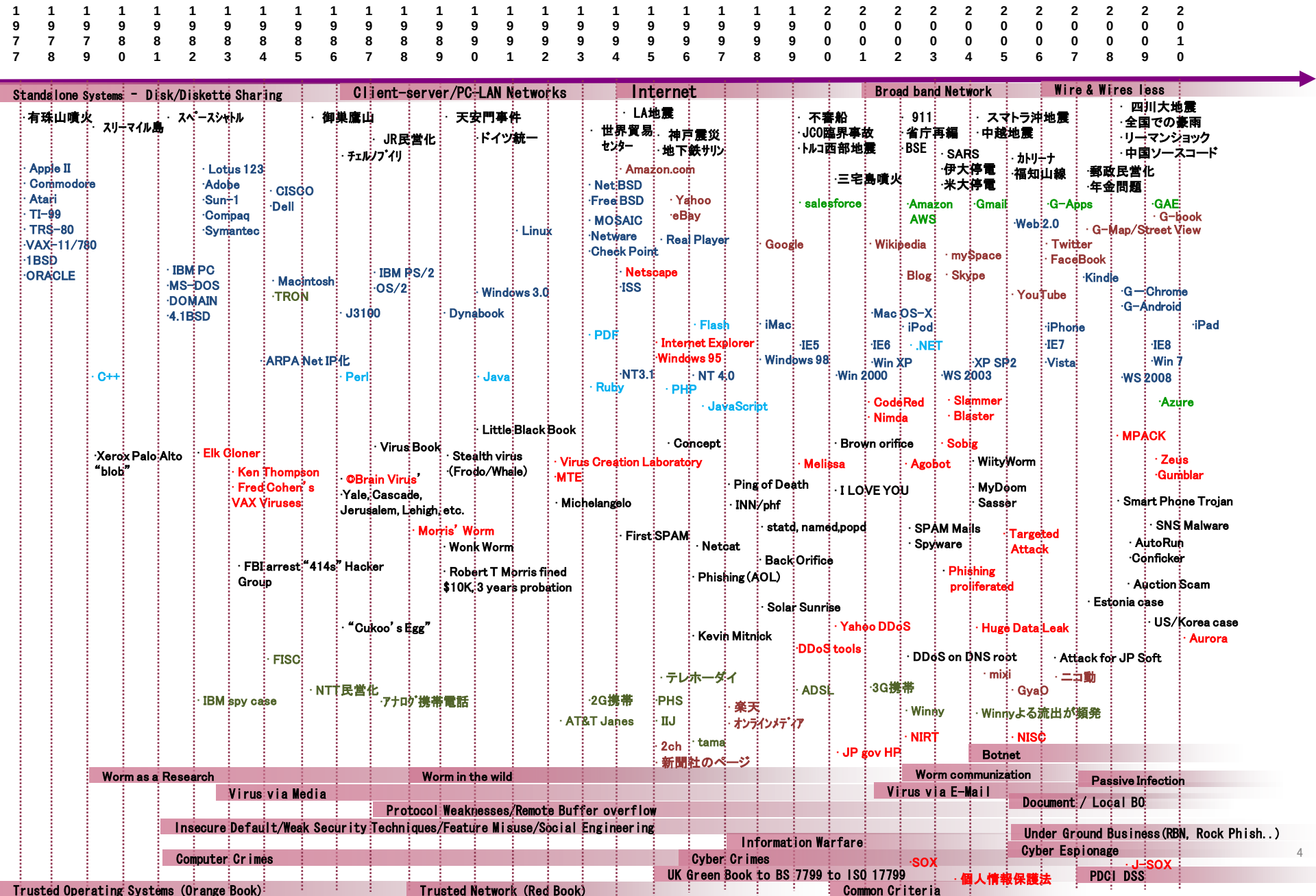

2007
2008
2009
Malware Detections by Country/Region (per 1000)
37 +
31 to 37
26 to 31
21 to 26
17 to 21
13 to 17
10 to 13
7 to 10
5 to 7
3 to 5
1.5 to 3
0 to 1.5
Insufficient data


ランク
20
18
16
14
12
10
8
6
4
2
0
1
1
4
15
19
2H07
1H08
2H08
1H09
2H09

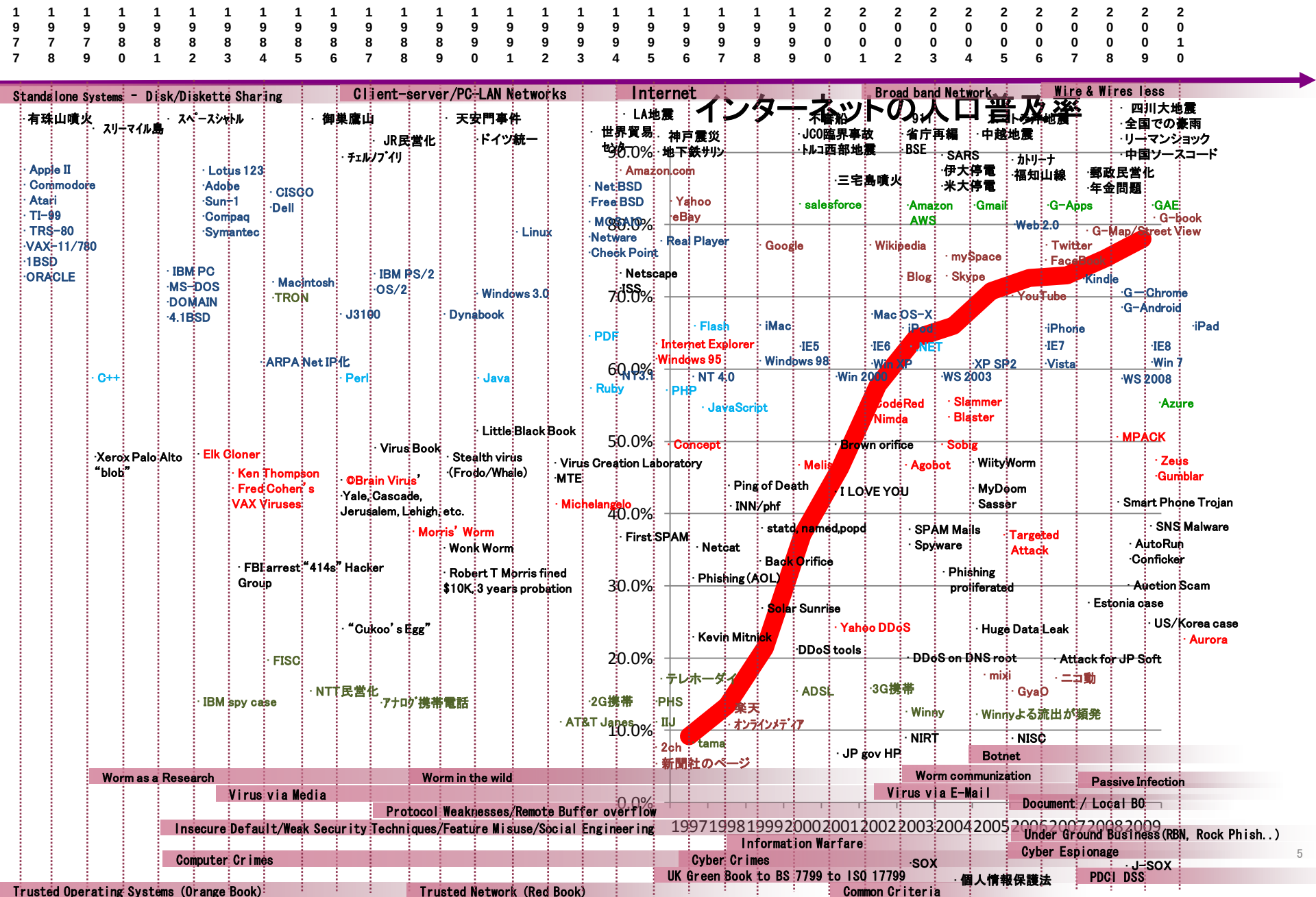

レート
3.5
3
2.5
2
1.5
1
0.5
0
1.5
1.5
1.7
3.0
2.3
2H07
1H08
2H08
1H09
2H09

セキュリティにかかわる歴史を振り返る

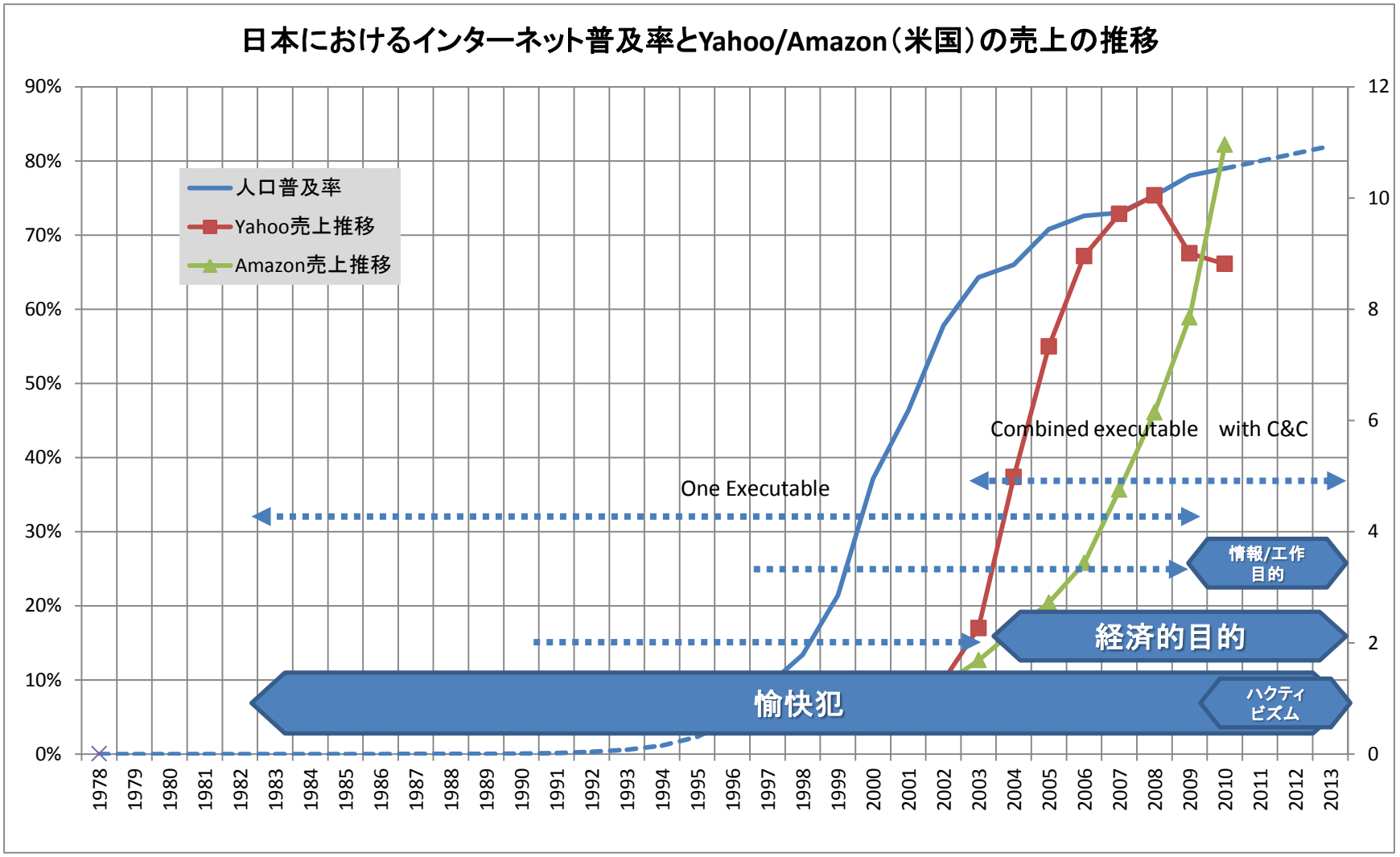
30+ years of computing & insecurity



30+ years of computing & insecurity



攻撃の傾向とインターネット経済



脅威の類型

特に目的を持たない愉快犯
従来のウィルスやワームなど、単に感染を目的としたもの。現在も存在するため無視はできないが、主たる関心は下記の3つのカテゴリーに向けられている。

サイバークライム（犯罪）

経済的な利益を目的とした攻撃
これらの事件と比較して、あまり報道されていないが、マルウエア（ウィルス）を使って、銀行口座から現金を盗み出す事件が数多く発生している。Zeus(zbot), SpyEyeなどが代表的なもので、ラテンアメリカやヨーロッパを中心に数百億円の被害が発生していると考えられている。
また、企業のWEBサイトにマルウエアを侵入させるGumblerなども、経済的な利益を目的とした攻撃の一環として実施されている。

サイバーテロ

自らの考えや主義を主張するための攻撃（Hacktivisim: ハクティビズム）
Anonymousと名乗るグループによるSONYグループへの攻撃、海外では、チェニジア政府やエジプト政府へのDDoS（サービス不能攻撃）、著名なセキュリティ企業への攻撃、LulzSecと名乗るAnonymousに関連するグループによるTV番組への侵入、英国のATM情報の公表など多数。

サイバーエスピオナージ（諜報活動）

企業や政府機関の情報を盗み出すことを目的とした攻撃
（APT: Advanced Persistence Thread:高度で執拗な攻撃,またはCyber Espionage: 電子的な諜報活動）
防衛産業、政府機関などの事例。海外では、2010年のフリーメールに対する攻撃、セキュリティ企業へ侵入し2要素認証にかかわる情報を取得後に行われた、軍事産業への攻撃など

サイバーウォーフェア（戦争）

兵器としてサイバー攻撃（APT: Advanced Persistence Thread）
国家間の戦争行為としてのサイバー兵器。Stuxnetによるイラン原子力発電所の遠心分離器への攻撃、中東での空爆が行われた際のレーダー網への関与などが疑われている

自爆型
サイトやプログラムの設計上の問題から、正常な範囲のアクセスで、サイトが停止してしまう例

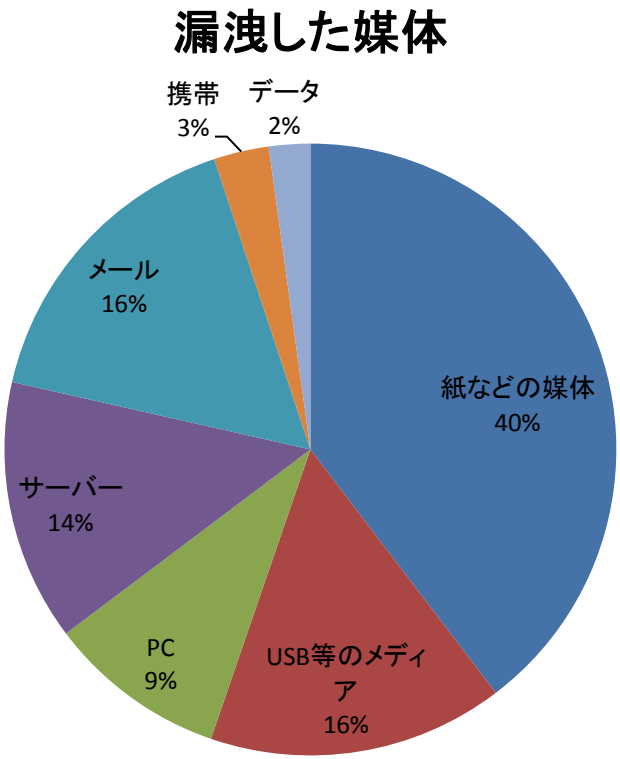
2011年の事件を振り返る

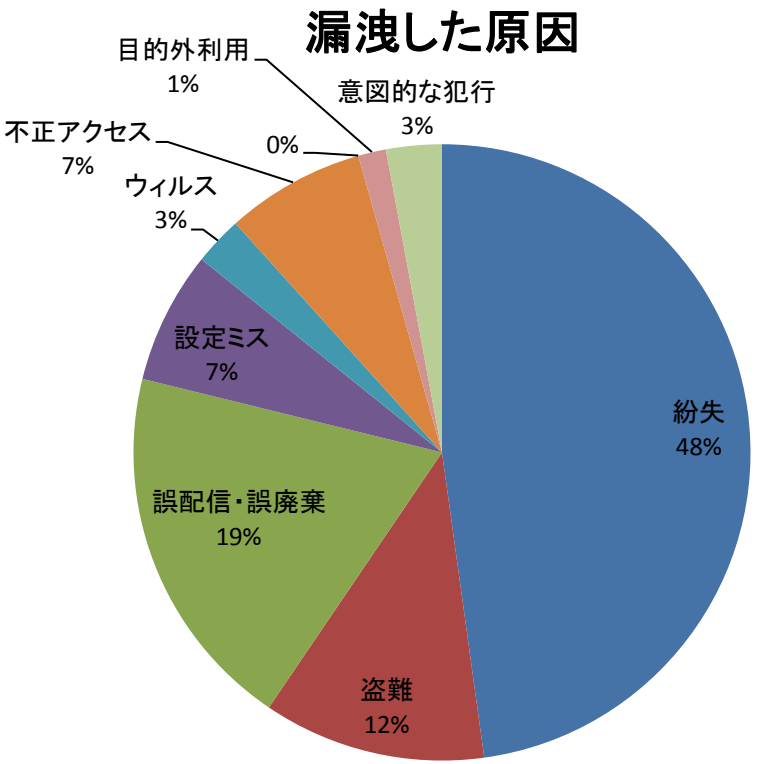
2011年に国内で発生した事件

2011/01/06	茅ヶ崎市で発生した児童の個人情報放置、年末に再び相次ぐ
2011/01/07	個人情報含む人権相談票が所在不明 - 新潟地方法務局
2011/01/14	全校生徒の成績情報含むUSBメモリを紛失 - 横浜市の中学校
2011/01/18	トークライブ参加学生のメールアドレスが流出 - 静岡市
2011/01/19	個人情報含む設計図をサイトに誤掲載 - 大阪市水道局
2011/01/21	生徒の個人情報や写真データ含むUSBメモリを紛失 - 福岡市の特別支援学校
2011/01/24	顧客情報含む書類が配送中に紛失 - パナソニック関連会社
2011/01/25	中学校教諭がひったくり被害、USBメモリなど盗難 - 北九州市
2011/02/10	滞納者情報など匿名化せずに誤って公開 - さいたま市
2011/02/10	顧客情報含む帳票を一時紛失、掲示板に貼られ判明 - 大阪市水道局
2011/02/17	児童の個人情報含む記録簿など無断で持ち出し紛失 - 大阪市の小学校
2011/02/18	石巻市で選挙人名簿が警察押収物として見つかる - 流出経路は不明
2011/02/18	メール誤送信で協議会外部委員のアドレスを流出 - 鳥取県教育委
2011/02/18	米出荷者の個人情報含むPCが事務所から盗難 - JA三重四日市
2011/02/21	車上荒らしで個人情報盗まれた臨時教員を処分 - 愛知県
2011/02/21	都営バス営業所で顧客情報含む書類を紛失 - 都交通局
2011/02/22	市政モニターのメールアドレスを誤って送信 - 鎌倉市
2011/02/23	誤送信で市掲示板登録者のメールアドレスが流出 - 東大阪市
2011/03/02	水道料金滞納者の個人情報含む書類を一時紛失 - 静岡市
2011/03/04	求職者の個人情報含むUSBメモリを紛失 - 愛知県のハローワーク
2011/03/08	アンケート依頼メールの誤送信でメールアドレスが流出 - 長野県
2011/03/09	生徒の個人情報含むUSBメモリを紛失 - 兵庫の中学校
2011/03/11	中学で生徒の試験結果などを保存したUSBメモリを紛失 - 浦安市
2011/03/24	公文書の紛失や誤送付など51件、監査で判明 - 広島県
2011/03/25	児童名簿を自転車の前かごに放置し紛失 - 平塚市の小学校
2011/03/28	県立武道館のメルマガ誤送信で氏名とアドレスが流出 - 神奈川
2011/03/29	小学校で児童や教職員の個人情報含むUSBメモリを紛失 - 大阪市
2011/03/31	保育所児童の個人情報含む書類が車上荒らし被害 - 野田市
2011/03/31	府営住宅入居者の個人情報含む書類が盗難 - 大阪府
2011/04/04	小学校児童の個人情報含むUSBメモリを学外で紛失 - 板橋区
2011/04/05	廃棄業者の収集車から個人情報含む書類が散乱 - 横浜市
2011/04/07	県立高校で生徒指導要録が紛失 - 静岡県
2011/04/12	振込依頼書の誤印字で聴講生の個人情報が流出 - 大阪市の高校
2011/04/13	事業者情報含む帳票を非常勤職員が紛失 - 大阪府
2011/04/14	誤送信でボランティア情報希望者のメールアドレスが流出 - 神奈川県
2011/04/18	児童の個人情報含むPCを駅ホームに置き忘れ紛失 - 目黒区
2011/04/18	住民の個人情報含む水道管の布設図面を紛失 - 川崎市
2011/04/19	求職者の個人情報含むファイルを誤送信 - 京都の就職サポートセンター
2011/04/20	県立高校生徒の個人情報を運搬中に紛失、一部未回収 - 群馬
2011/04/21	利用者の個人情報が車上荒らしで盗難 - 愛知の介護保険センター
2011/04/22	県立高校で中学校から送られた新入生の個人情報を紛失 - 静岡
2011/04/22	個人情報含むUSBメモリを紛失した教師に懲戒処分 - 千葉県
2011/04/28	水道局でシステム設定ミス、個人情報が一時閲覧可能に - 新潟市
2011/04/28	メール誤送信でキャッチコピー応募者のアドレス流出 - 岩手県
2011/05/12	個人情報記載のノートを路上に落として紛失 - 足立区
2011/05/12	生活保護受給者名簿を一時紛失、同日中に回収 - 大阪市
2011/05/18	利用者の個人情報を車両の屋根に置いたまま走行 - 沖縄の介護施設
2011/05/19	土地権利者の個人情報を職員が紛失 - 東京都
2011/05/23	水道局の委託検針員が個人情報を一時紛失 - 静岡市
2011/05/26	委託先がメール誤送信、アドレス484件を流出 - 福岡県
2011/05/31	労働力調査の「調査世帯一覧表」を紛失 - 長野県
2011/06/01	メール誤送信で関係企業担当者のアドレス流出 - にいがた産業創造機構
2011/06/03	私立高校の就学支援金通知を誤送付 - 長野県
2011/06/14	委託業者が市乗合タクシー利用者情報を紛失 - 相模原市
2011/06/17	消防が火災現場へ向かう途中に個人情報を紛失、同日中に回収 - 大阪市
2011/06/20	生徒の個人情報含む私物USBメモリを紛失 - 横浜市の中学校
2011/07/01	営業先担当者の電話番号など含む業務用携帯電話を紛失 - 名古屋市交通局
2011/07/05	小学校で児童の個人情報を2年半前に紛失、匿名の投書で発覚 - 横浜市
2011/07/05	高齢者の個人情報含む生活実態調査リストを紛失 - さいたま市
2011/07/05	区報配送先情報含むFDを委託業者が紛失 - 目黒区
2011/07/12	印鑑登録申請書など保存期限内の文書など約9000件誤廃棄 - 港区
2011/07/15	福岡市早良区のPRサイトが一時改ざん - 閲覧でウイルス感染のおそれ
2011/07/21	チャリティーバザー協力者の個人情報を紛失 - 杉並区社会福祉協議会
2011/07/22	メルマガ誤送信で読者のアドレス流出 - 千葉市
2011/07/25	小学校教諭の自家用車が車上荒らし、個人情報盗難 - 横浜市
2011/07/27	小学校教諭2人がパチンコ中に出席簿盗まれる - 堺市
2011/07/28	取手市のウェブサイトが不正アクセスで改ざん - ウイルス混入は確認されず
2011/07/28	PCがウイルス感染、アカウント情報や個人情報が流出の可能性 - 国交省
2011/07/29	個人情報流出で停止した「行政情報検索システム」を再開 - さいたま市
2011/07/29	再交付申請書のファックスを誤送信 - 全国健保協会
2011/08/01	横須賀市、委託先のメール転送ミスを公表
2011/08/05	委託先が公共施設に接続できるPC盗まれる - 千葉市
2011/08/08	学生の個人情報含む書類を紛失 - 岐阜大
2011/08/08	かんぽ生保の顧客情報を紛失 - 広島県の郵便局
2011/08/08	千葉市委託先のPC盗難、別の駅トイレから回収 - PCの使用形跡なし
2011/08/09	水泳教室の講師と受講者の名簿を紛失 - 岸和田市
2011/08/10	メール誤送信で地元就活学生のアドレスが流出 - 中津川市
2011/08/11	中学校で個人情報含むUSBメモリを保管忘れ紛失 - 大阪市

情報ソース：Security NEXT:個人情報漏洩事件・事故一覧
http://www.security-next.com/category/cat191/cat25

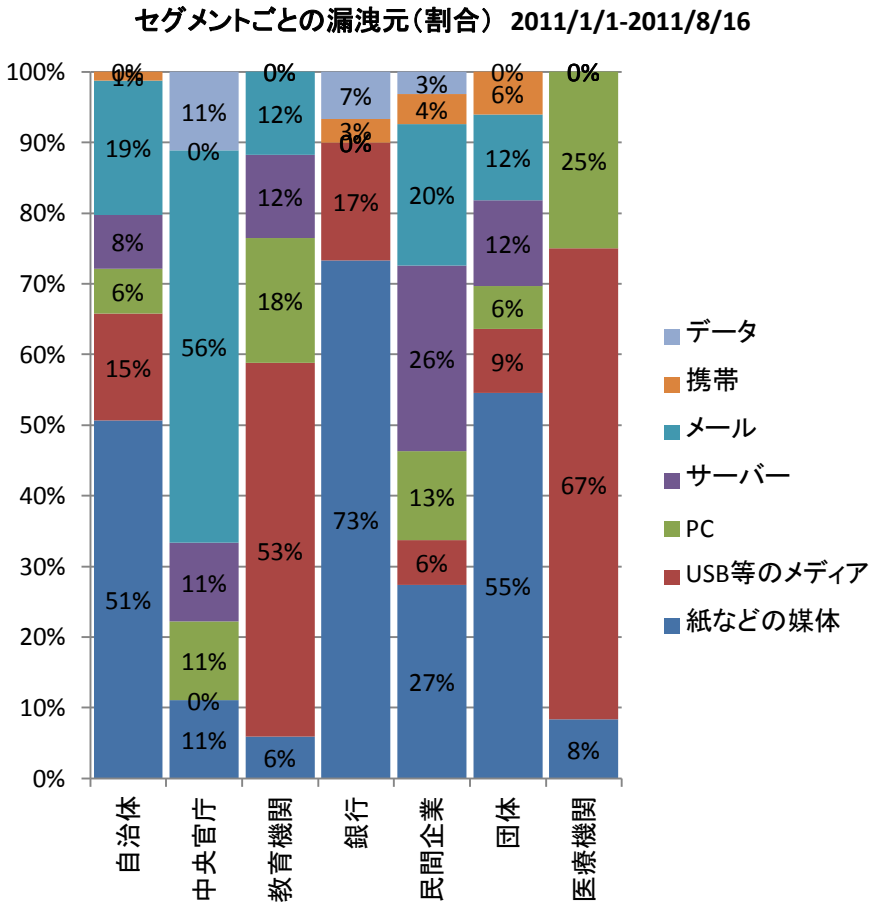
2011年に国内発生した事件の傾向

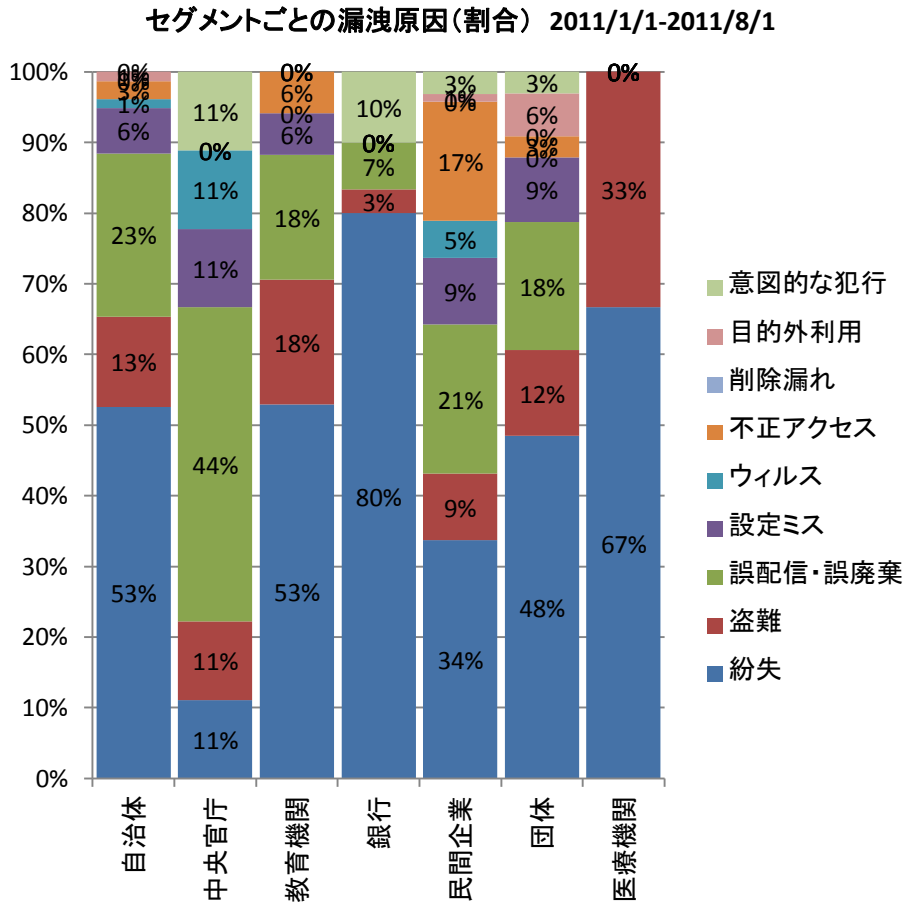




情報ソース：Security NEXT:個人情報漏洩事件・事故一覧
http://www.security-next.com/category/cat191/cat25

2011年に発生した事件の傾向





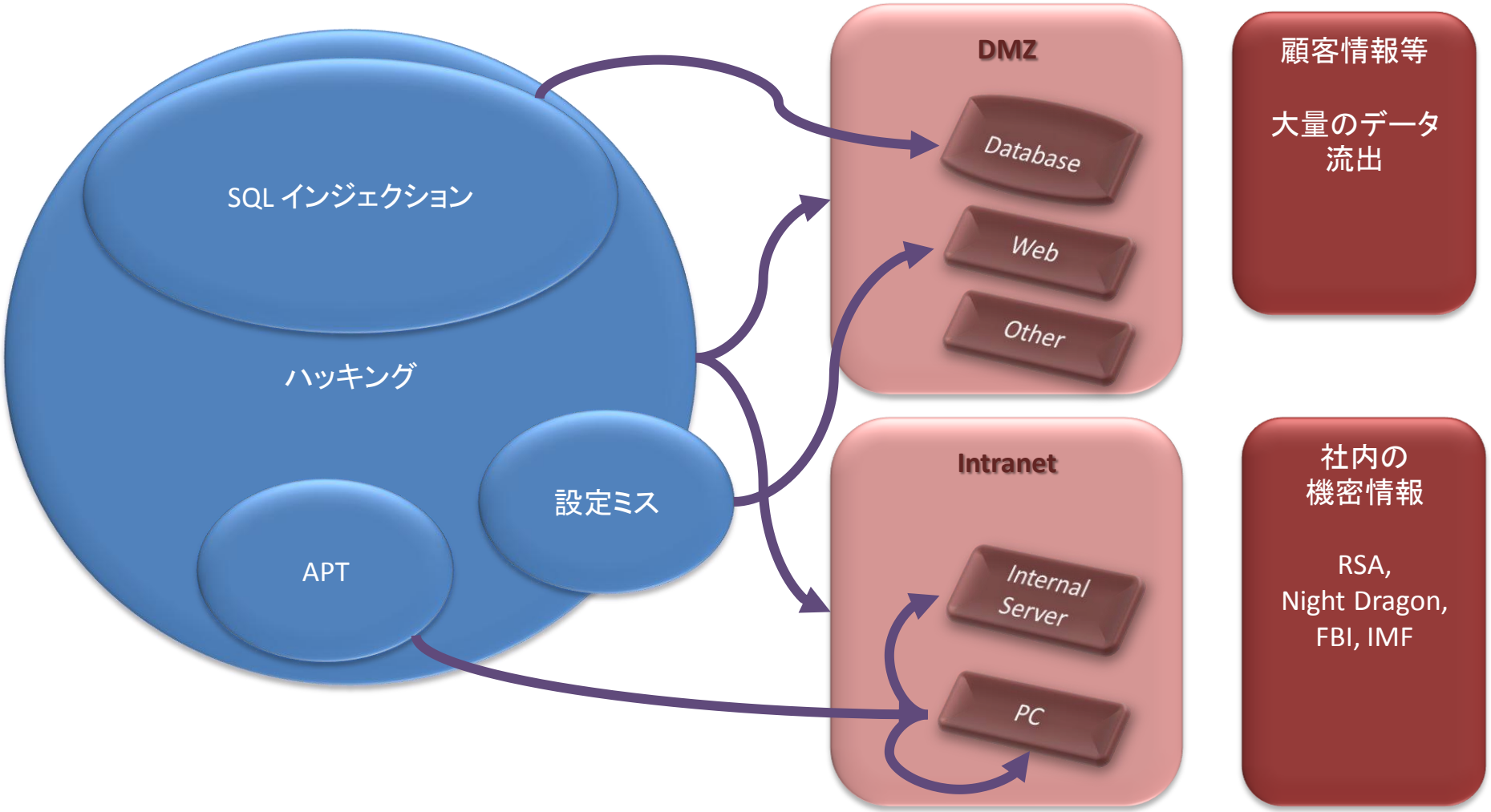
情報ソース：Security NEXT:個人情報漏洩事件・事故一覧
http://www.security-next.com/category/cat191/cat25

世界的な傾向をみる

1/4		Anonymousがチュニジア政府のWebサイトをDDoSでダウンさせる
1/10		Aonymousがアイルランドの中道右派 Fine GaelのWebサイトに侵入し、検閲を非難した。2000人以上の党員のアカウントが侵害された
1/18		グリーファーグループGoatse Securityのメンバーは、iPadユーザ情報を公開したことに関して、連邦捜査局によって起訴された
1/28		CNETが、Goast Securityのホームページが、脱会したメンバーによって侵入されたと報じた。我々はこれは、宣伝活動であると考える。グループのスポークスマンがこれを否定していることを記録する (グリーファー◆オンラインゲームなどで、ゲームの欠陥を利用して対戦相手に嫌がらせをする人。)
1/28		英国警察は、5人のAnonymousの嫌疑のかかっているメンバーを逮捕します。
2/3		Anonymousメンバーが、ムバラク大統領に対する革命の間、エジプト政府のwebsiteをDDoSでダウンさせた。
2/5	2/6	HBGaryのセキュリティコントラクターがAnonymousによって、SQL Injection、ソーシャルエンジニアリング等を使ってハックされた。68000のE-Mailが詐取され、そのうちのひとつは、Bank of AmericaがHBGaryをWililieaksへの攻撃を行うために雇ったメールも含まれていた
2/10		中国のハッカーが、”Night Dragon"の一環として、複数の石油会社から情報を盗み出した
2/10		iPhoneのJale Breaを使った攻撃により、パスワードが詐取できると ホワイトペーパーが記載
2/17		カナダ政府への"前例のない攻撃"に中国が関与
2/24		兵士出身のハクティビスト「Jester」(th3j35t3r)は、ウェストバラ・バプティスト過激派キリスト教徒カルトのウェブサイトを停止させた
2/27		Anonymousは、Koch Industries, Inc.(組合に対してロビー活動をすることに数百万人を費やして、大規模なキャンペーンにWisconsinの「組合活動妨害屋」Scott Walker知事に対する貢献を支払ったアメリカの製造複合企業)への攻撃を開始した。
3/1	3/6	マルウエアが、260,000台のAndroidフォンで構成するボットネットを構築。Google社(GOOG)は問題のあるルートキットを取り除くためのツールを提供
3/7		何者かが、マイクロソフトのポイント詐欺により、$1.2Mを盗み出した
3/14		Anonymnousは、バンクオブアメリカが、差し押さえ詐欺を犯したことを示す文章を盗み出し、公開した
3/18		セキュリティ企業RSAが、ハッキングにあったことを報告した
4/2		Anomymousは、ハッカー Geroge "GeogHot" Hotzへの起訴に抗議して、SONY CorpへのDDoS攻撃を行った
4/4		Epsilon Data Management LLC (ダイレクトメール、電子メールマーケットなどを行う企業)がハックされ、数百万ものユーザーのe-Mailとコンタクト情報が漏れた
4/17	4/19	PlayStation Networkはハックされ、7700万の記録が侵害。 Anonymousと結びつける向きもあるが、グループによる関与はないと思われる。 Sony Online Entertainmentも侵害され、2400万の記録が盗まれた。
4/19		ハッカーが米国の風力発電システムを侵害すると脅迫し、限定的なアクセス情報を公開。
4/26		SonyがPSNが侵害されたことをアナウンス
5/2		SOEが、顧客データベースが侵害を受けたことをアナウンス
5/7		Sony の懸賞サイトが単純なGoogle Searchを通じて侵害され、2500レコードが盗まれる
5/7		FOXのX-Factor TVショーの出場者データベースが、LulzSecによるSQL Injectionにより流出。
5/10		LulzSecは、FoxのWebサイトの管理者アカウント、従業員のパスワードセールスデータベースを公表
5/15		LulzSecは英国のATM情報のデータベース(所有者、配置場所等)を公表
5/17		Androidの認証トークンが安全ではないAPIにより侵害
5/20		数名のAppleの従業員が、20台に1台のMACがMacDefender に感染していると報告。Appleはこの記事を無視している
5/21		Sonyは、所有するサーバーがフィッシングに使われている事を発見した
5/21		何者かが、Sony所有のインターネット・サービス・プロバイダー(ISP)の上で、128のアカウントから仮想通貨で1,220ドルを詐取
5/21		"k4L0ng666"ハッカーが、ソニーミュージックインドネシアのWebサイトをSQL Injectionで侵害した
5/22		"b4d_vipera" ハッカーが、Sony BMGギリシャのWebをSQL Injectionで侵害し、8500レコードを詐取した
5/23		LulzSecは、Sonyの日本のWebサイトをSQL Injectionで侵害し、取得した情報を公開した(ユーザー情報は含まれない)
5/24		Sonyカナダは、レバノンのハッカーグループLdahcによるSQL Injection攻撃により、2000レコードを流出した。
5/25		Sonyは、影響を受けたカスタマーに無料の個人情報の盗難防護物の1年を約束した
5/27		カナダのホンダサイトに不正アクセス、最大28万件以上の顧客情報が流出(ホンダ)
5/29		PBSが、Wikileaksに対する報道の後LulzSecによってハックされる。ハッカーは偽の記事を送って、そのページの変更した。
5/30		RSAから流出した情報を利用して、ロッキードマーチンのサーバーが、侵害された。中国関係が疑われている
6/1		インテリアショップサイトに不正アクセス、カード情報含む個人情報が漏えい(ミサワ)
6/2		LulzSecは、SQL Injectionを使ってSony Pictures懸賞ウェブサイトから100万件の情報を詐取。Sonyは、実際には38,000アカウントと発表
6/2		何者かが、SQL Injectionを使って、Sony BMGオランダとベルギーから、100万件の情報を詐取。ユーザー名と、平文のパスワードを含む。
6/2		Gmailアカウントが侵害され、このアカウントが中国の反体制派グループのものであったことから、中国政府の関与が疑われる
6/2	6/3	特定のユーザーとの口論から、LulzSecは 大衆誌ハッカー誌2600のIRCサーバーとProxyサーバーにDDoS攻撃を行う。 メンバーと出版管理がチャット後、論争は結局解決された。 http://www.amazon.com/2600-Magazine-Hacker-Quarterly-Digital/dp/B004GB1WF6
6/3		Sony Europeデータベースへの SQL Injectionにより、120人の開発者の名前、写真と電子メール・アドレスが流出
6/3		LulzSecは、日本のゲーム・メーカーNintendo(TYO:7974)にそのオンライン・セキュリティのセキュリティ上の問題について警告。
6/3		FBIのInfragardがLulzSecにより侵害、emailなどがリークされる
6/5		Sony Picturesロシアが、SQLインジェクションによって侵害。いくつかのデータベースから収集されたユーザーレコードが、Pastebinに公開された。(pastbin.com)
6/5		Anonymousは、著名な中東の政治家数名の名前、パスワードと電子メール・アドレスを発表した。
6/6		Sony BMGが、LulzSecによって侵害され、内部のネットワーク情報と、SCE開発者のコードが盗まれた。
6/8		Sony Music ポルトガルは、SQL Injection攻撃により、更にデータが流出した。Ldahcが行ったと視聴している
6/8		LulzSecは、セキュリティ企業Black & Berg Cybersecurity Consultingが運営する、”侵入不可能”なWebサイトに侵入。侵入に成功した場合に支払われる賞金を辞退した。
6/9		閉鎖したサービスのサーバに不正アクセス、撤去時に発覚 - ゲオ
6/9		Anonymousは、検閲に抗議するため、Low Orbit Ion Cannon (LOIC) DDoS攻撃を使って、トルコに攻撃を行った。
6/10		LulzSecは、ポルノサイトから盗み出された、公務員の管理情報とアカウントをポスト
6/10		Anonymousインドと名乗るグループが、インド軍のWebサイトにDDOS攻撃を行った
6/11		IMFにサイバー攻撃 FBIが捜査へ
6/12		LulzSecは、ネットワーク侵入によるベセズダSoftworksとZeniMax Mediaのソースコード、ネットワーク・マッピング等を公開。しかし、ユーザー情報は公開しなかった。「我々は、この企業がすきだから」
6/12		米上院の、侵入されないとされるサーバーにも関わらず、LulzSecにより侵害を受けた (Webサーバーの情報を公開)
6/12		スペインの警察が、Anonymousの3人の嫌疑のかかっているメンバーを逮捕。Anonymousは、スペインの警察ウェブサイトのDDoSテークダウンで対抗。
6/14		Pastebinへの投稿によると、Anonymousは、インド政府への攻撃を非難した、彼らは詐欺師により騙された
6/14		Citiグループのカードへの侵害は、当初公開されたものよりも大きかった
6/14		"Titanic Takeover Tuesday"がLulzSecによって実行される。グループは、ゲーム誌にEscapist、EVE Onlineのサーバ、政府と契約を持つソフトウェア会社Finfisherのサイト、Minecraftのためのサーバと Legends(MMORPG)のLeagueのためのサーバに攻撃
6/14		Anonymousは彼らのサイトへのポストを通して、米国連邦準備制度理事会会長Ben Bernankeを標的とした。攻撃が実現したかどうかは不明。
6/14		トルコは、Anonymousの32人の嫌疑のかかっているメンバーを逮捕。グループは復讐を宣言

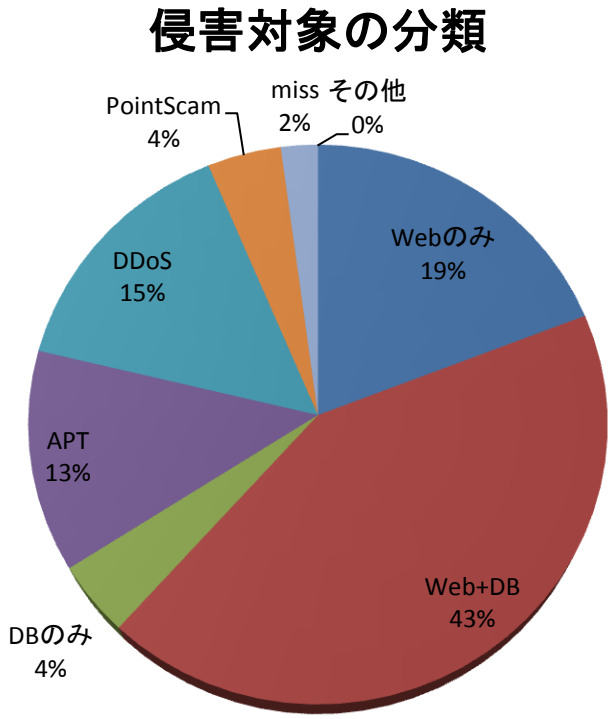
主な出典:Welcome to 2011, Year of the Hacker, Jason Mick (Blog) - June 14, 2011 9:40 PM
http://www.dailytech.com/Welcome+to+2011+Year+of+the+Hacker/article21896.htm

公開セグメントと内部セグメント



事例が示唆する必要な対策（侵害対象への着目）

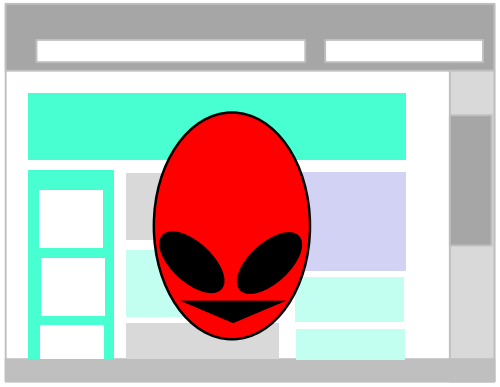
- 侵害の対象は、**WEBとデータベース**が約70%を占めている。
  - 古典的な公開サーバーに対するセキュリティの対策
- 重要な情報が侵害されているという点で、**APT（新しいタイプの攻撃）**の対策も進める必要がある。
  - APTとはなにか、何が危険なのか？
- アジテーションとして、特定の**企業グループ**への攻撃
  - 経営上のガバナンスと、ブランディングの不一致



犯罪の基盤としてのボットネット

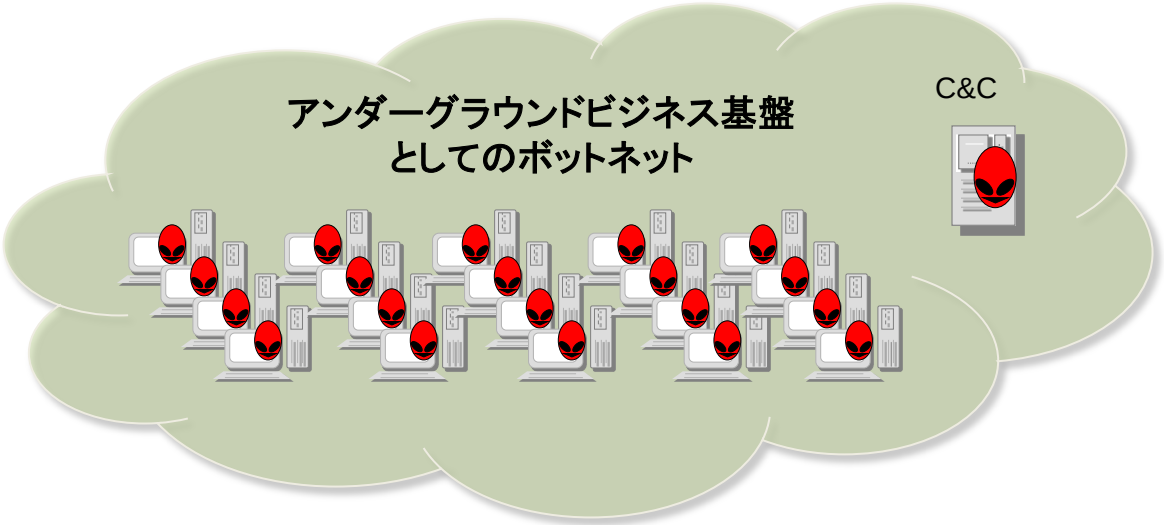
アンダーグラウンドポータルとボットネット

アンダーグラウンド ポータル



メニュー例

- **アカウント系のデータ**
  - 口座、クレジットカード、
  - オンラインアカウント
  - サーバーアカウント
- **技術情報・製品**
  - マルウエア、攻撃コード、
  - 脆弱性
  - フィッシングキット
- **物販・その他情報**
  - ブランクカード、エンボス
  - 機密・非機密情報
  - 海賊版(Wares)
- **サービス提供**
  - メール配信（スパム）
  - DDoS攻撃
  - 暗号解読サービス
  - BBS
  - ホスティング
  - ロンダリング（MULE）
  - アフェリエート

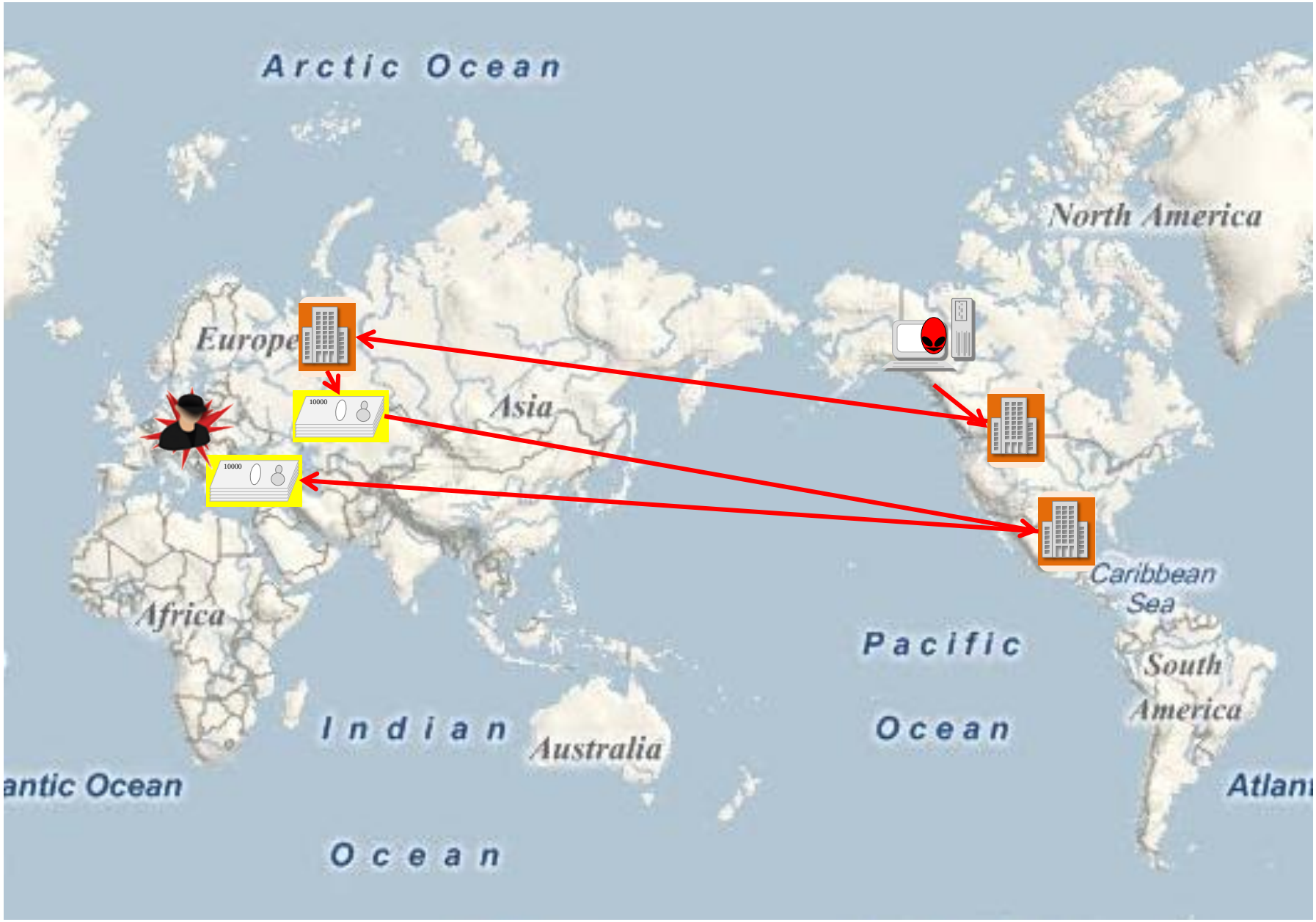


ボットネットの利用

- ボットからのデータ収集
  - ターゲットの情報
  - サーバーなどの情報
- DDoS攻撃
- スパムメールの送信
- 新たなボットを作る基盤（感染）
- 広告・アフェリエート詐欺

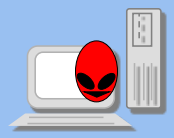
ボットネットの世界的な展開

世界的な金銭の流れ


Arctic Ocean
North America
Europe
Asia
10000
10000
Africa
Pacific
Caribbean
Sea
South
America
Indian
Ocean
Australia
Ocean
Ocean
Atlan

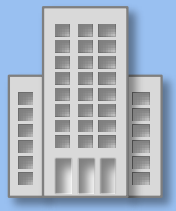
銀行口座を盗み出す

PCから口座情報を詐取



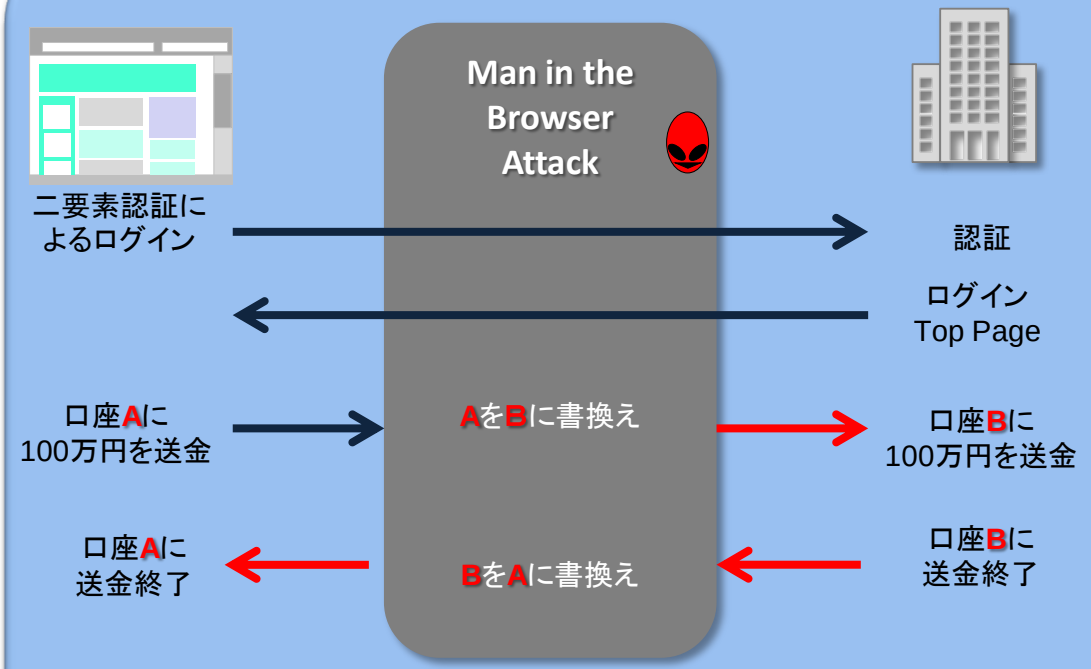
・ファイル等からの詐取
・Key loggerによる詐取

銀行などの
ID盗難の対策



・二要素認証
乱数表
ワンタイムパスワード

二要素認証を使うオンラインバンクからの金銭を詐取

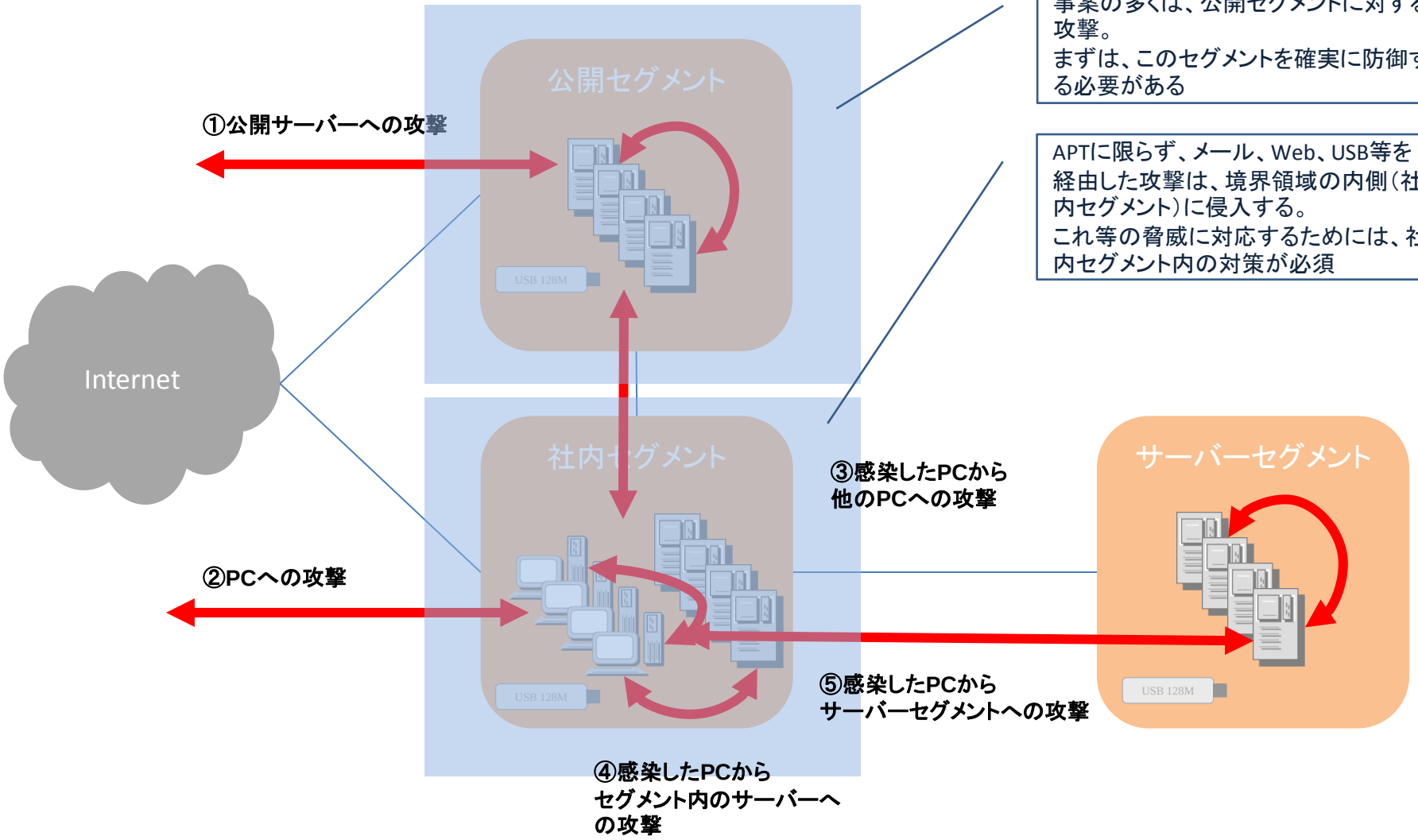


認証の確立したセッションを利用して、トランザクションを改ざんするため、二要素認証でも攻撃を防ぐことができない。また、銀行から表示されるデータも改ざんされているため、この行為に気づくことは困難。
一般に、送金先は、Money Muleと呼ばれる運び屋の口座が利用される。
Zeus/Zbot, URLZone/Bebloh 等

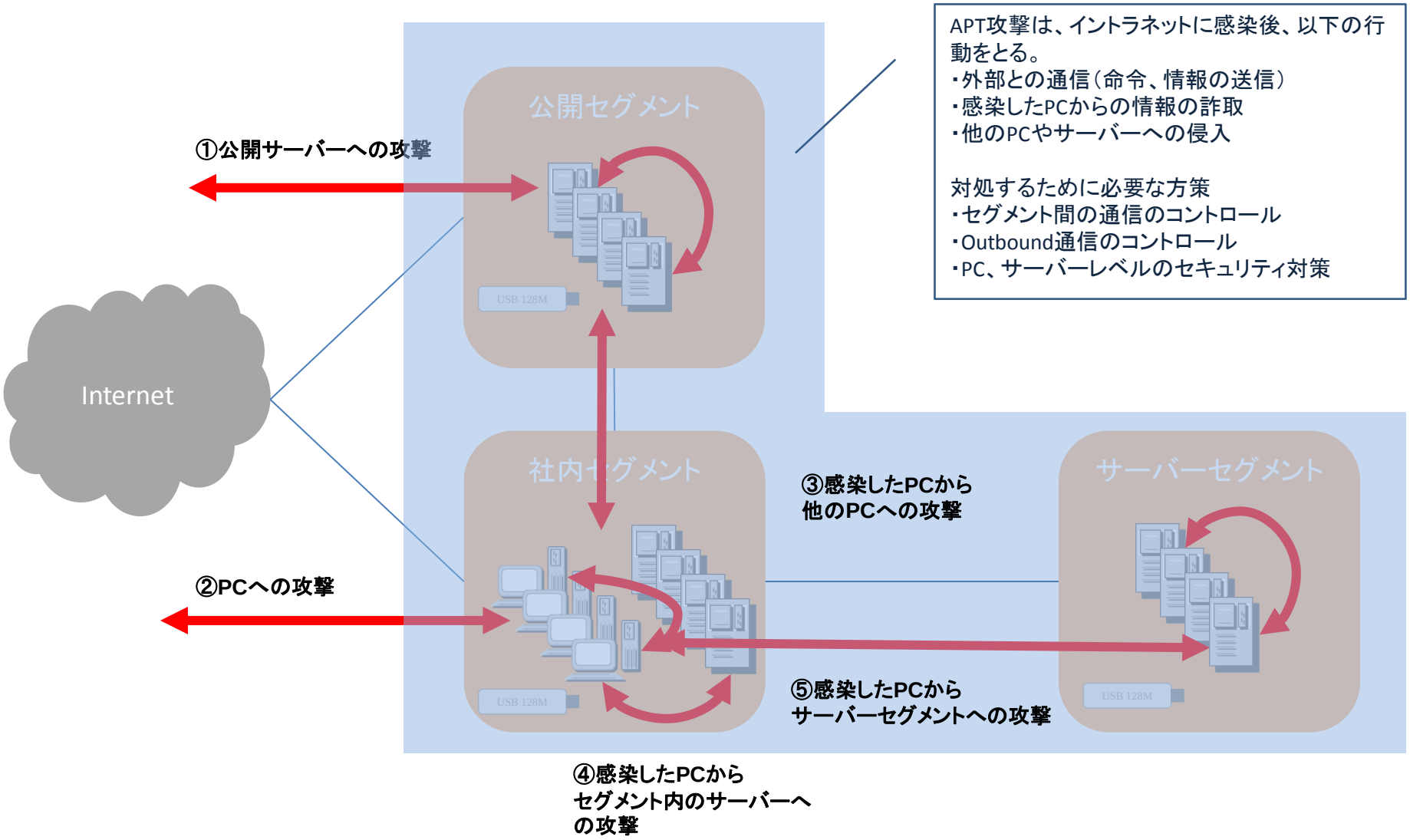
システムとデータをいかに守るのか

対策の方向性

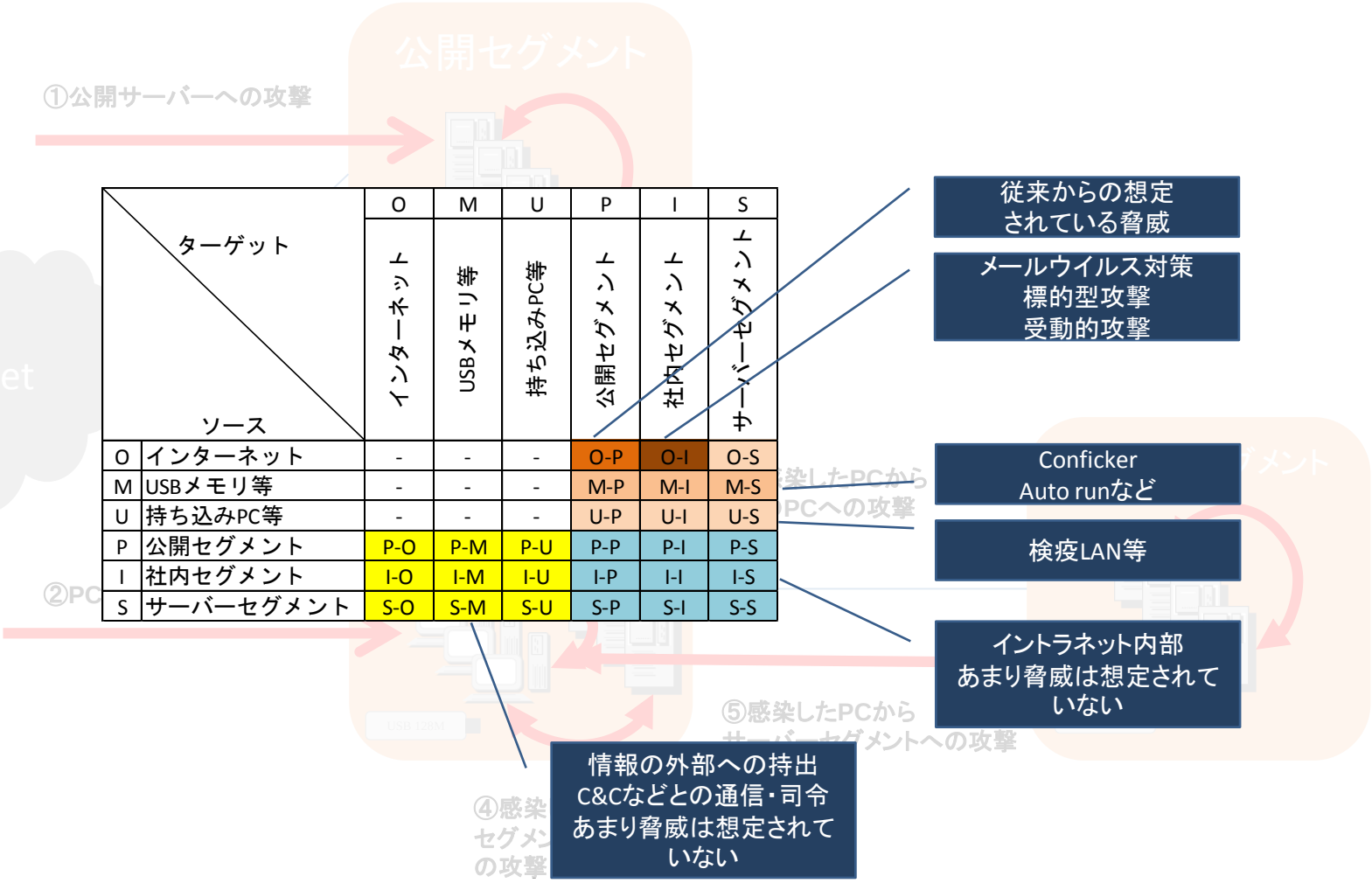
公開セグメント・社内セグメント



APT: Advanced Persistence Threat



セグメント間の通信と脅威・対策



ターゲット / ソース		O インターネット	M USBメモリ等	U 持ち込みPC等	P 公開セグメント	I 社内セグメント	S サーバーセグメント
O	インターネット	-	-	-	O-P	O-I	O-S
M	USBメモリ等	-	-	-	M-P	M-I	M-S
U	持ち込みPC等	-	-	-	U-P	U-I	U-S
P	公開セグメント	P-O	P-M	P-U	P-P	P-I	P-S
I	社内セグメント	I-O	I-M	I-U	I-P	I-I	I-S
S	サーバーセグメント	S-O	S-M	S-U	S-P	S-I	S-S

対策の方向性

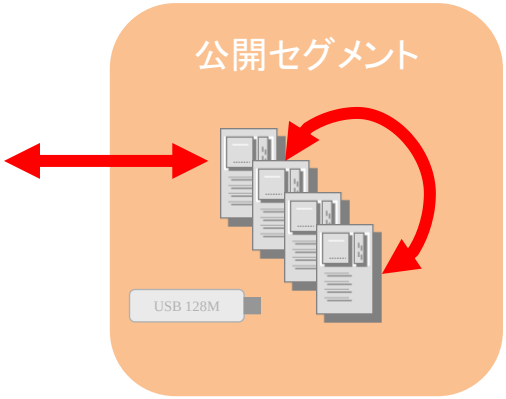
- 通達から制御へ
- 管理者権限からユーザー権限へ
- ブラックリストからホワイトリストへ
- インタビューから計測へ
- より安全性の高いシステムへ

- セグメンテーションを再考する

セグメンテーションを再考する

公開セグメント

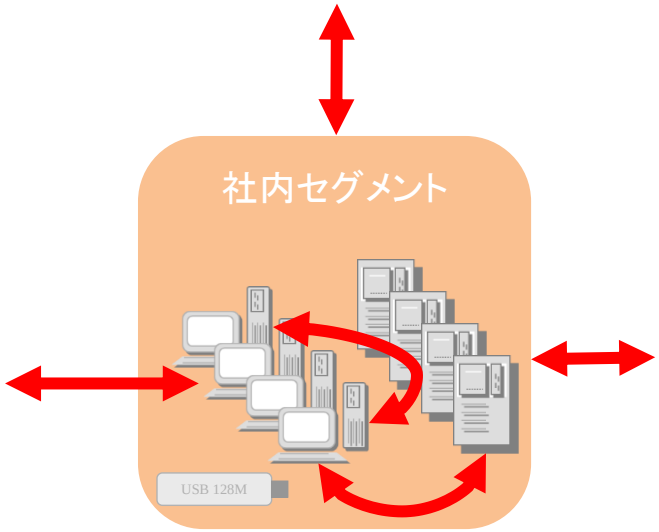
- 物理的な対応
  - 入退出制限・管理
  - 非正規デバイスの持ち込み・接続の対処
- 境界領域の対応
  - FWによるアクセスコントロール
  - IPS/WAF等による攻撃の検知・防御
- サーバーレベルの対処
  - OS・システム
    - 脆弱性パッチ、安全性の高い設定（要塞化）
  - ミドルウェア等
    - 脆弱性対策、安全性の高い設定
  - アプリケーション
    - 脆弱性対策、安全性の高い設定
- オペレーションとマネージメント
  - パッチの配信と安定した運用の両立
  - 安全性の高い設定の統制
  - ログや攻撃に関する情報のモニター
- 対策と対策レベルの確認
  - セキュリティ診断・インベントリ
  - コンテンツの確認



- 子会社・関連会社を含めたガバナンス
  - 経営の独立性から、ITガバナンスを、子会社・関連会社ごとに独立している事が多い。
  - しかし、経営上のガバナンスの範囲と、世間（社会）がイメージするブランドの範囲は異なる事が多い。
  - これまで、各社ごとのガバナンスに重点が置かれてきたが、今後は、グループ会社やブランドと言ったより大きな単位で、ガバナンスを考えていく必要が出てきている。

内部セグメント

- 物理的な対応
  - 入退出制限・管理
  - 非正規デバイスの持ち込み・接続の対処
- 境界領域の対応
  - FWによるアクセスコントロール
  - IPS等による攻撃の検知・防御
  - メールサーバー等によるウィルス対策
  - PROXY等を使ったアクセス制御
- PC・サーバーレベルの対処
  - OS・システム
    - 脆弱性パッチ、安全性の高い設定（要塞化）
    - ディスクボリュームレベルの暗号化
    - USBメモリなどの暗号の強制
  - アプリケーション
    - 脆弱性対策、安全性の高い設定
- オペレーションとマネージメント
  - パッチの配信と安定した運用の両立
  - 安全性の高い設定の統制
  - ログや攻撃に関する情報のモニター
- 対策と対策レベルの確認
  - セキュリティ診断・インベントリ
  - コンテンツの確認

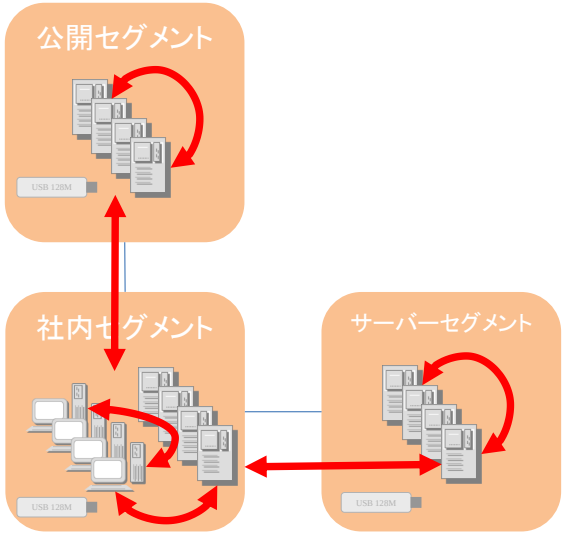


- 境界領域防御の限界
  - 2000年ごろから常識化している境界領域防御では、対策の難しい攻撃が増えている。
  - メール、Web閲覧、USBメモリの持ち込み等を使った攻撃は、境界領域を超えて、直接社内セグメントに侵入する。
- ゼロデー攻撃
  - 高度な攻撃においては、ゼロデー攻撃が利用される。
  - これ等の攻撃は適切なパッチマネージメントを行っていても防ぐことができない。
  - 対処するためには、システムレベル、セグメントレベルでの要塞化、そしてモニタリングが必要となる。

APTに対する考察

システムレベル・セグメントレベルの要塞化

- 物理的な対応
  - N/A
- 境界領域の対応
  - マルウエアの通信に対する対策
    - セグメント間のアクセスコントロール
    - Outbound通信のコントロール
- PC・サーバーレベルの対処
  - OS・システム
    - 脆弱性パッチ、安全性の高い設定（要塞化）
    - 侵入を前提とした対処
  - アプリケーション
    - 脆弱性対策、安全性の高い設定
- オペレーションとマネージメント
  - パッチの配信と安定した運用の両立
  - 安全性の高い設定の統制
  - ログや攻撃に関する情報のモニター
- 対策と対策レベルの確認
  - セキュリティ診断・インベントリ



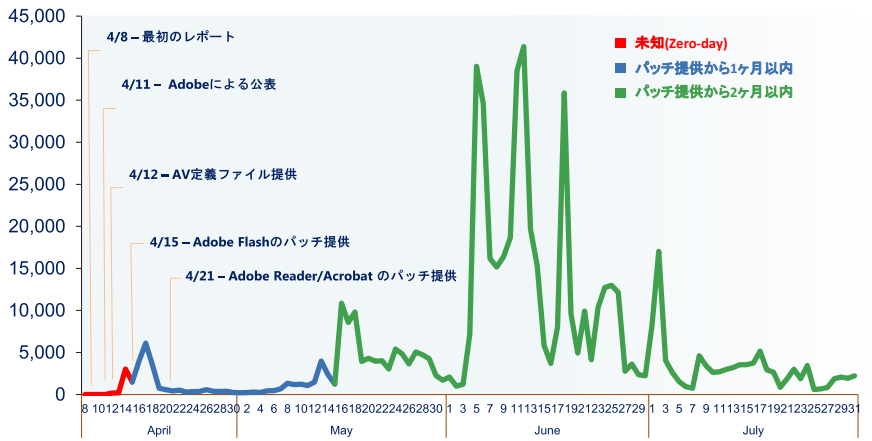
- セグメント間の通信のコントロール
  - セグメント間の通信をDefault Denyとする。
  - セグメント内の通信をDefault Denyとする。
    - PC間での通信の必要性を再考する
  - 管理用セグメントの分離。
- Outbound通信の制限

  外部への情報の詐取と、通信、司令、新しいマルウエアのダウンロードを防ぐ
  - 外部との通信を許可するプロトコルを限定する。
  - Webアクセスは、Proxyを経由を義務付ける

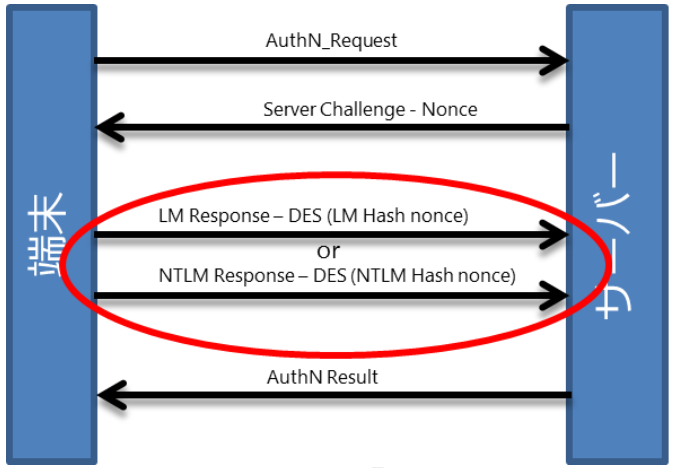
マイクロソフトのアプローチ

統制すべき具体的な問題

脆弱性の対応の必要性

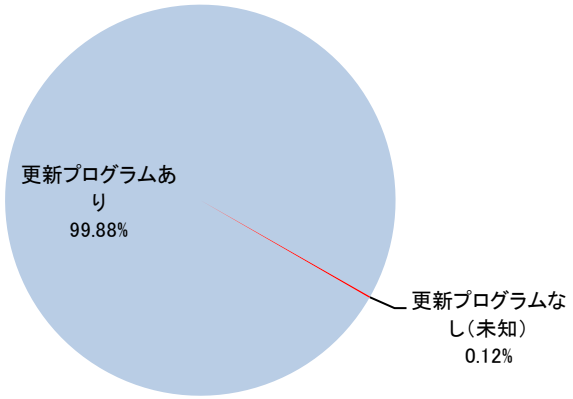


脆弱な設定を回避する



LM 認証

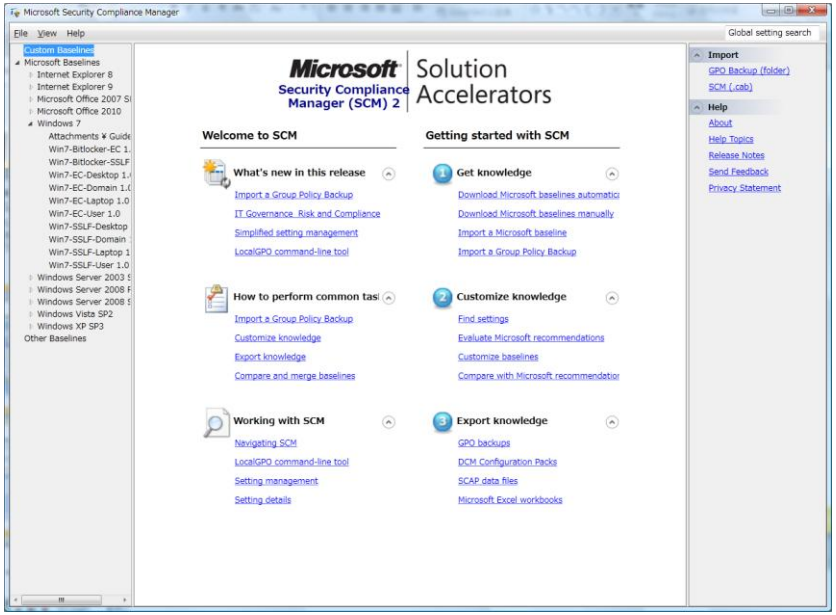
未知の攻撃の占める割合(2011年上半期)

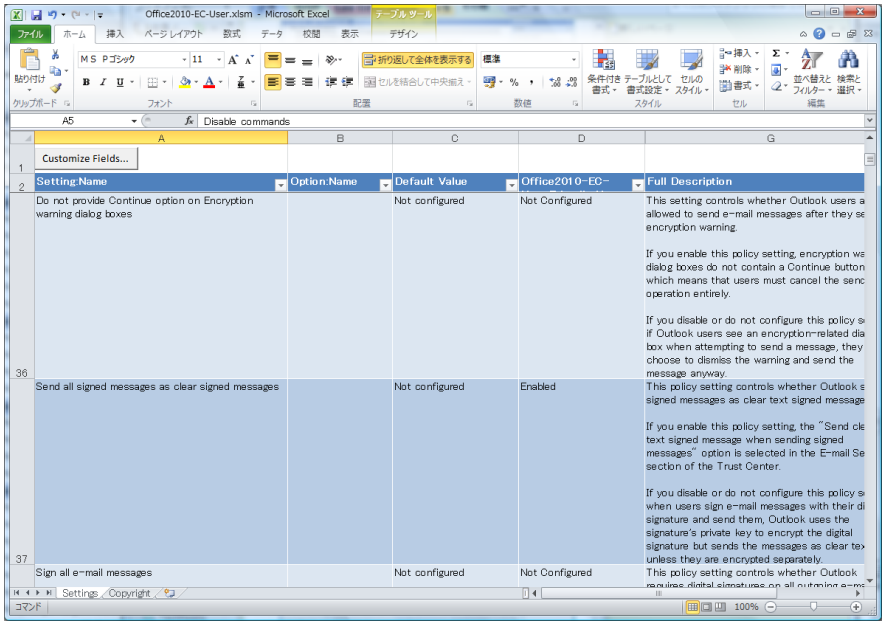


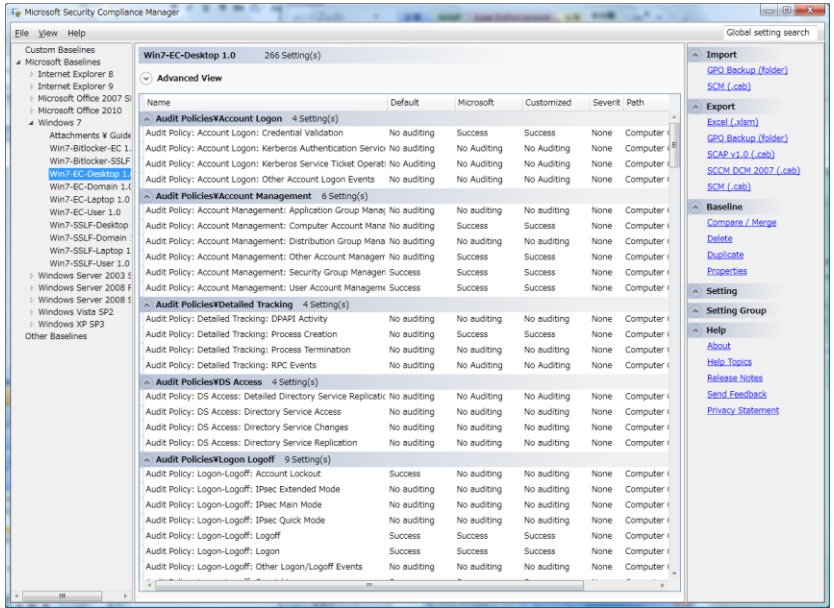
システムに対して安全な設定を行う(最低限の設定例)

項目	値
パスワードの有効期間	42日間
パスワードの変更禁止期間	1日
最小パスワード	12文字以上
パスワードは複雑さを満たす必要がある	有効
暗号化を元に戻せる状態でパスワードを保存する	無効
ロックアウト期間	1分
アカウントのロックアウトのしきい値	10回ログオンに失敗
ロックアウトカウンタのリセット	15分
ネットワーク セキュリティ: 次のパスワードの変更で LAN Manager のHashの値を保存しない	有効
ネットワーク セキュリティ: LAN Manager 認証レベル	NTLMv2 応答のみ送信する。LM と NTLM を拒否する

安全な設定と環境を強制する







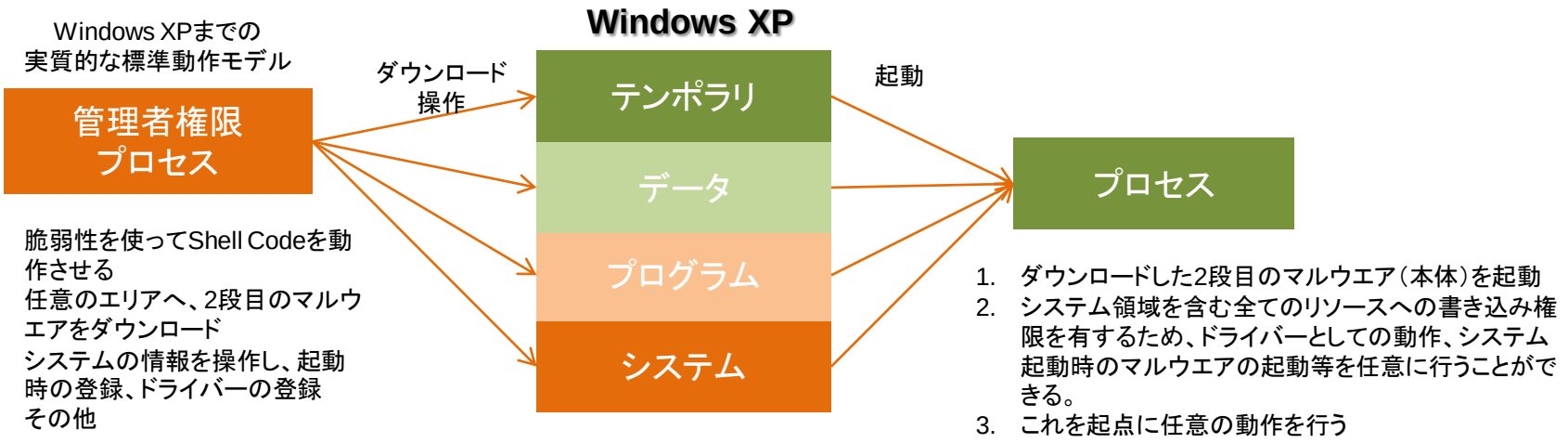
適切なグループポリシーの適用

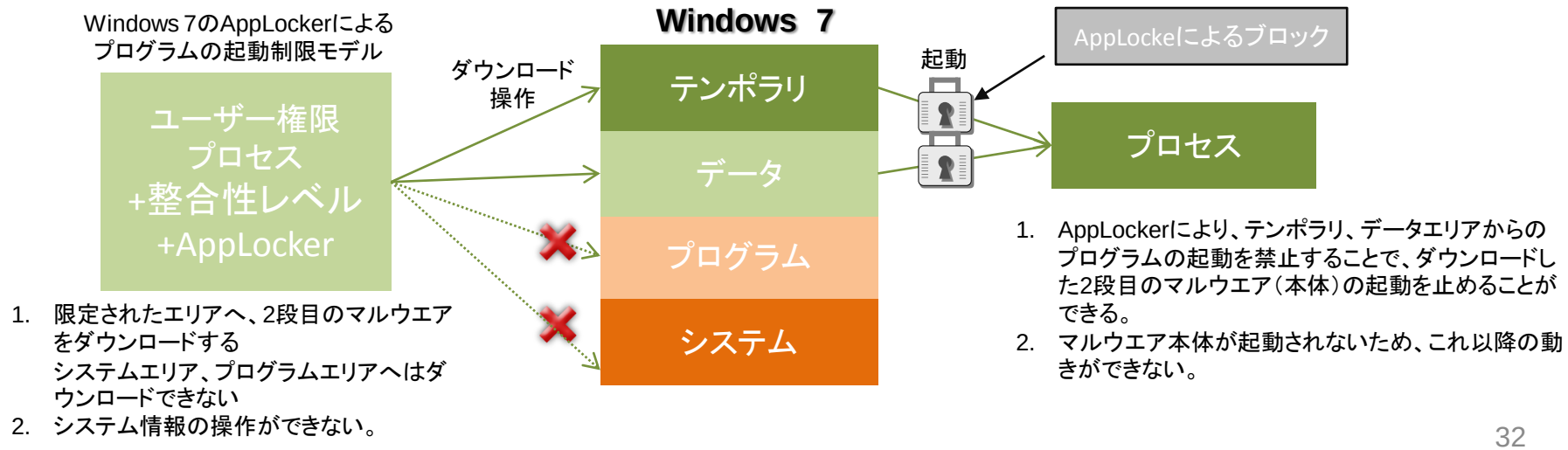
SCM (Security Compliance Manager)

- 標準化されたグループポリシー
- 現在のグループポリシーとの比較
- 作成したグループポリシーの適用

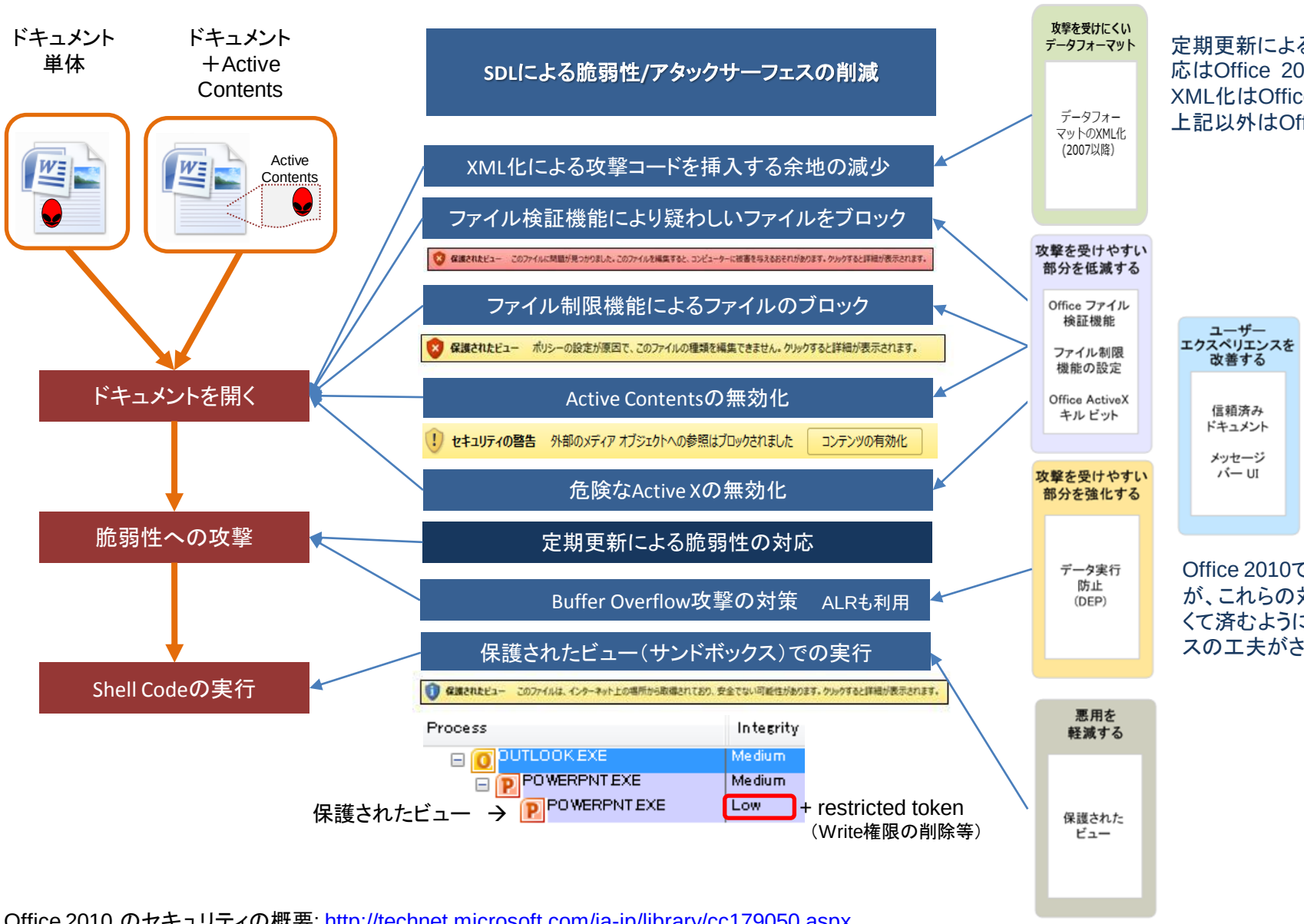
ユーザ権限の管理と多層防御

マルウエアの動作とプロセス権限





入り口の対策：Office 2010の多層防御



定期更新による脆弱性の対応はOffice 2003と共通
XML化はOffice 2007と共通
上記以外はOffice 2010から

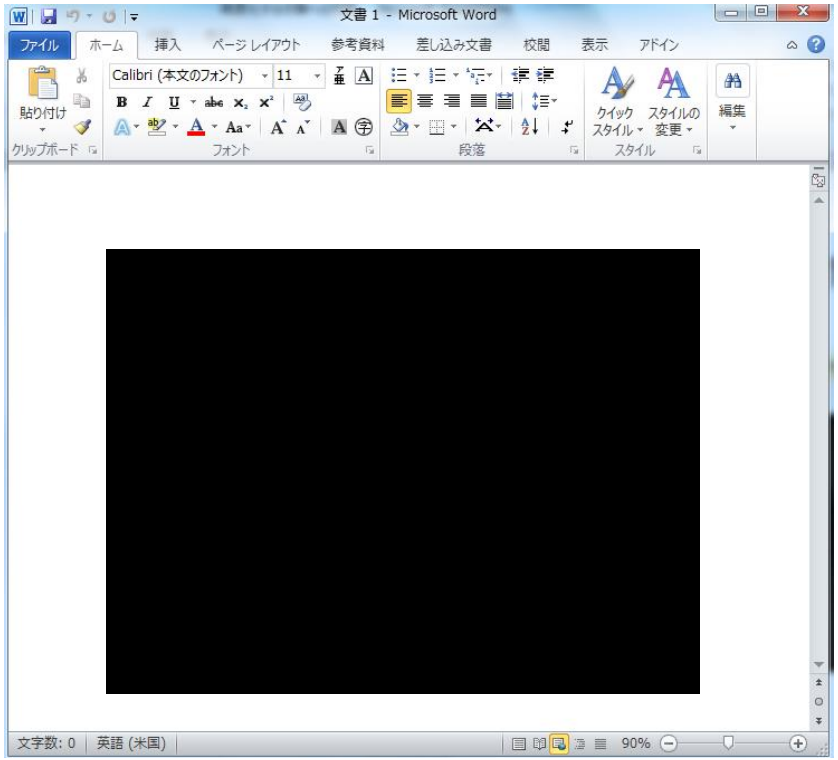
Office 2010では、ユーザーが、これらの対策を意識しなくて済むように、インタフェースの工夫がされている。

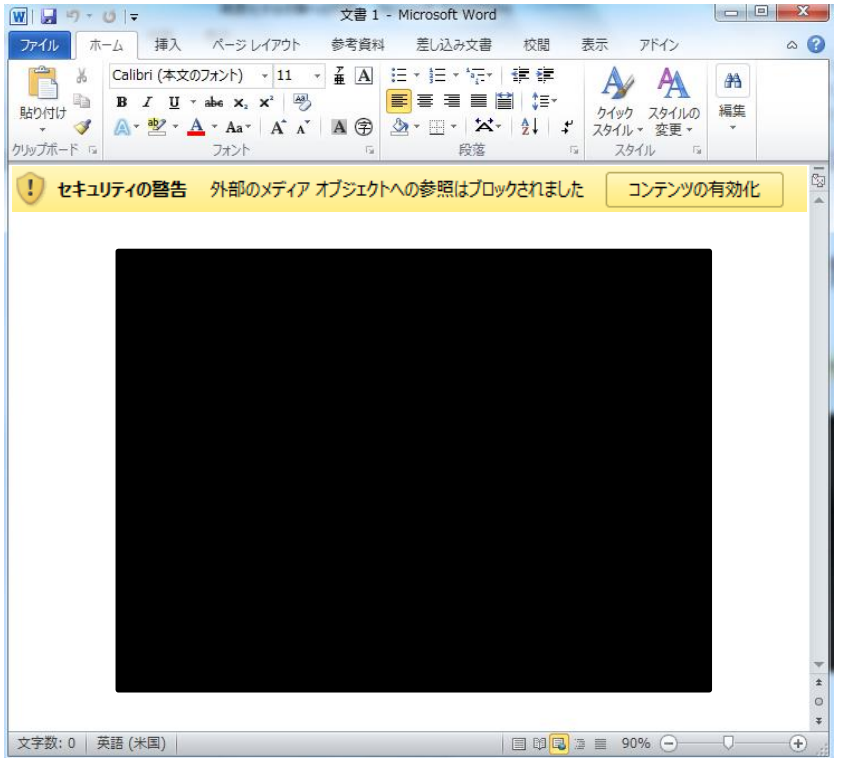
Office 2010 のセキュリティの概要: http://technet.microsoft.com/ja-jp/library/cc179050.aspx
Protected View in Office 2010: http://blogs.technet.com/b/office2010/archive/2009/08/13/protected-view-in-office-2010.aspx

入り口の対策

Office ファイル内のアクティブコンテンツ無効化

メール添付やインターネットからダウンロードされたドキュメントは、
アクティブ コンテンツ（画像、Active X）が無効化されて表示される

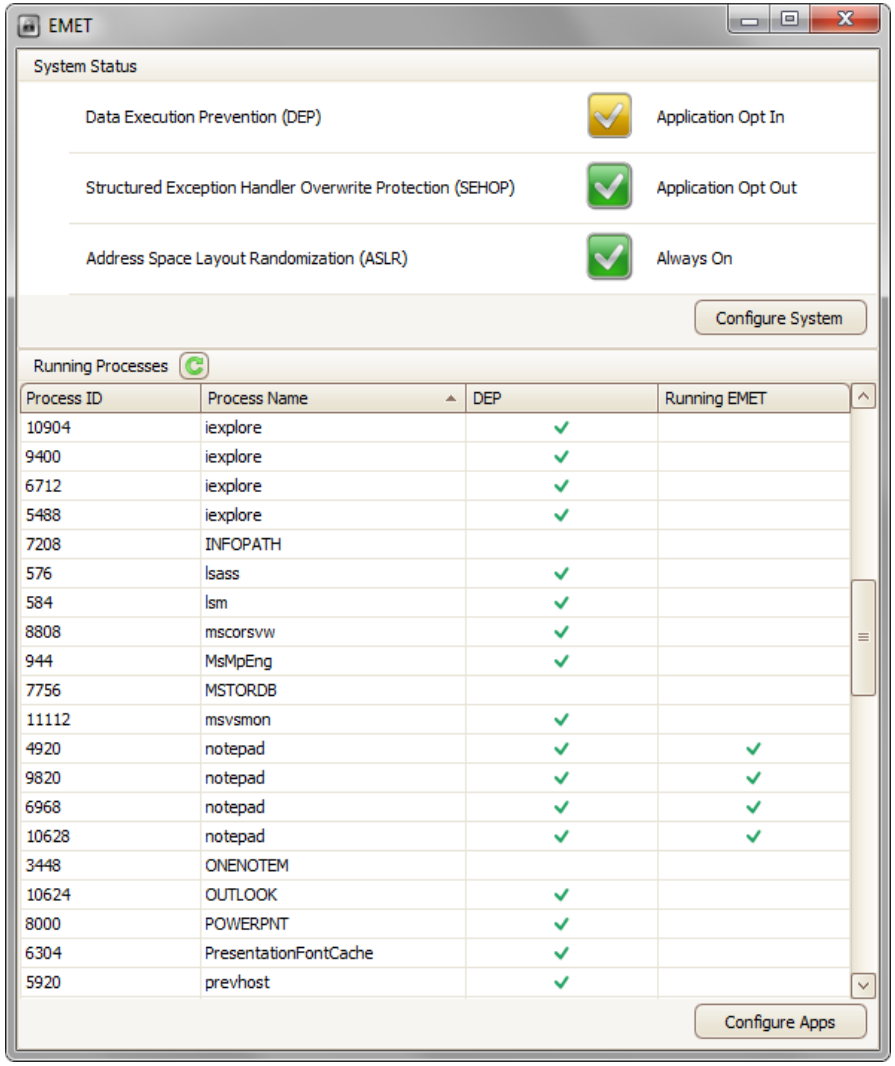




Enhanced Mitigation Experience Toolkit

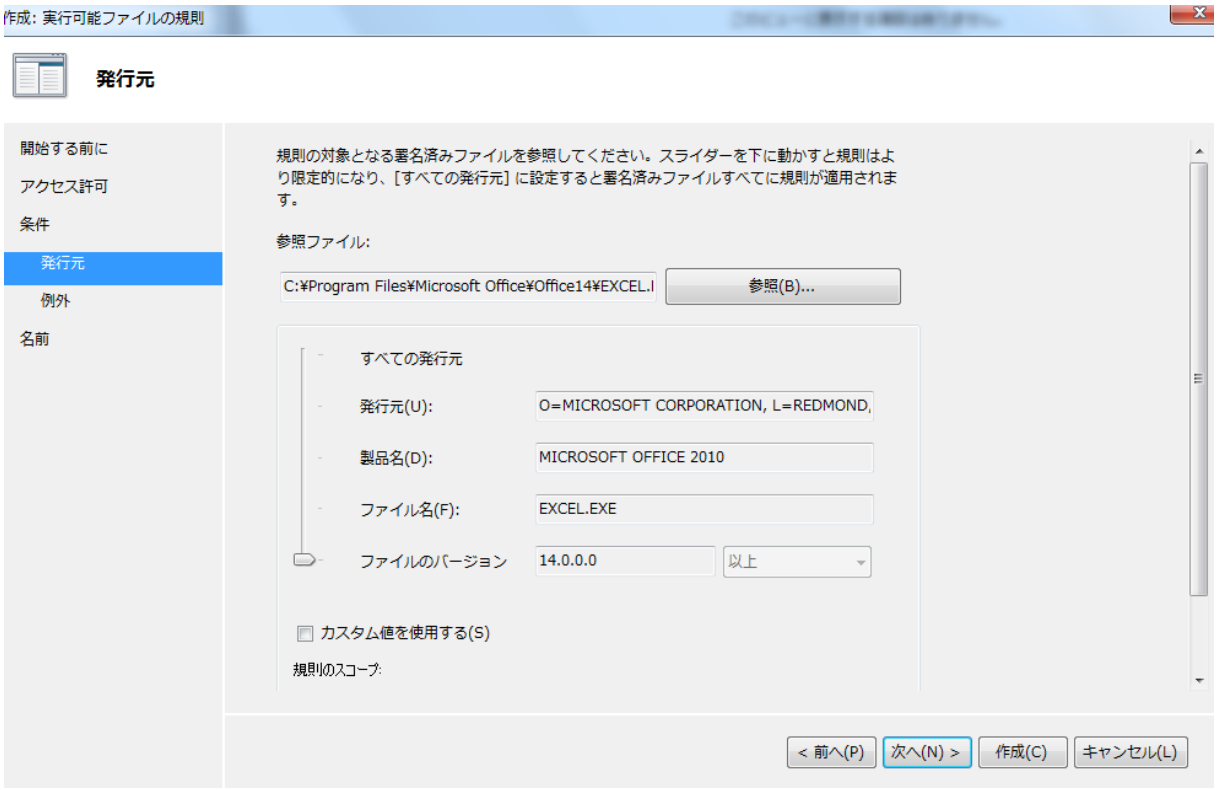
EMET =
脆弱性緩和技術導入ツール

- 6 つのセキュリティ緩和技術
- あらゆるアプリケーションに対応
  - 基幹業務アプリケーション
  - 他社アプリケーション
  - 古いアプリケーション
  - ソース コードが利用不可の アプリケーション
- プロセス単位で設定
- 更新プログラム インストール前の緩和策



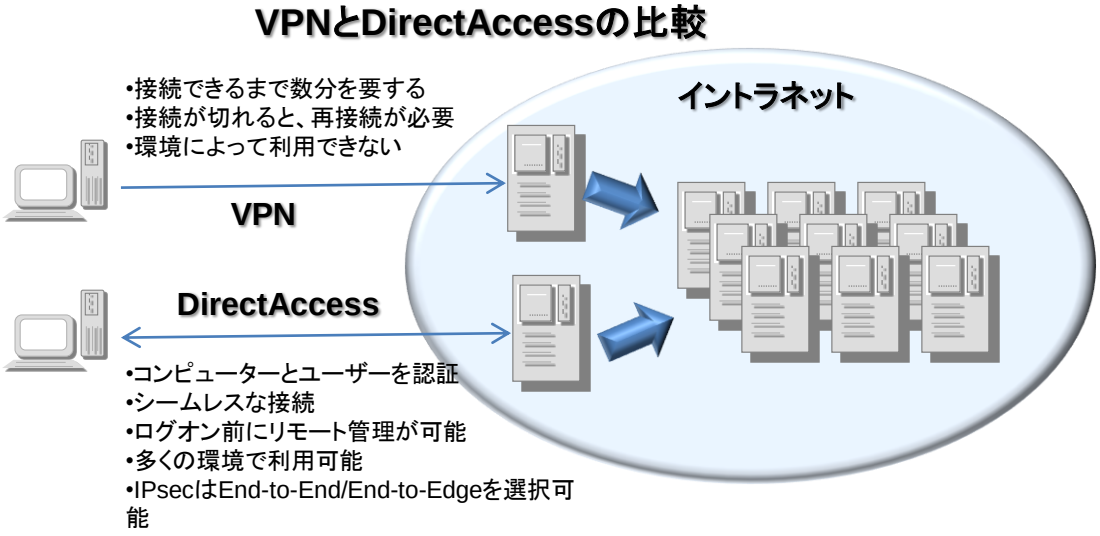
AppLocker：ホワイトリスト化

- 指定した特定のプログラムの実行を許可・拒否する
- プログラム（マルウェア）の実行・感染防止、ゼロデイ対策にも役立つ



リモート接続環境を整える:DirectAccess

- USB で情報を持ち出さなくて良いようリモート接続環境を整える
- 社外のPCを、社内と同様にドメイン管理
  - グループポリシーの適用、バージョンアップの実施など
  - ノート PC持ち運ぶPCの管理も容易に



サイバー犯罪の収益バランスを変える

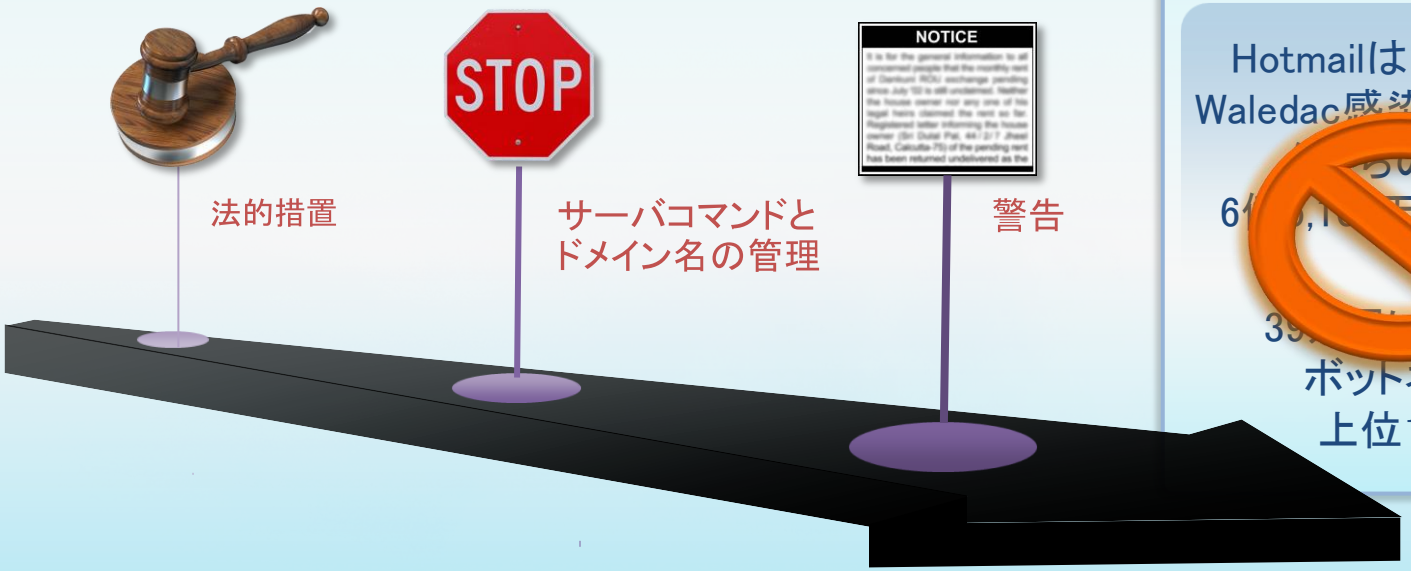
ボットネットのテイクダウン事例

日時	ボット名	推定台数	概要
2010/2/22	**Waledac**	**数十万台**	**Operation b49 1日当たり15億通以上のスパム・メール送信に悪用**
2010/10/25	Bredolab	3千万台	オランダ当局ハイテク犯罪チーム主導。ボットネットの停止の他、追加コマンドを送信し、コンピュータが感染していることを表示するプログラムをダウンロードさせてユーザーに通知
2011/4/11	Coreflood	2百万台	FBI 主導。感染したPCに対してマルウェアの停止コマンドを送信
2011/3/17	**Rustock**	**2百万台**	**Operation b107 1日当たり300億通以上のスパム・メール送信に悪用。全スパム流通量の47.5%はRustock経由で送信**
2011/9/27	**Kelihos**	**4万台**	**Operation b79 スパムの大量送信、個人情報の窃盗、DDoS攻撃など。Waledacとの類似性からWaledac 2.0とも呼ばれている。**

Waledac: Operation b49

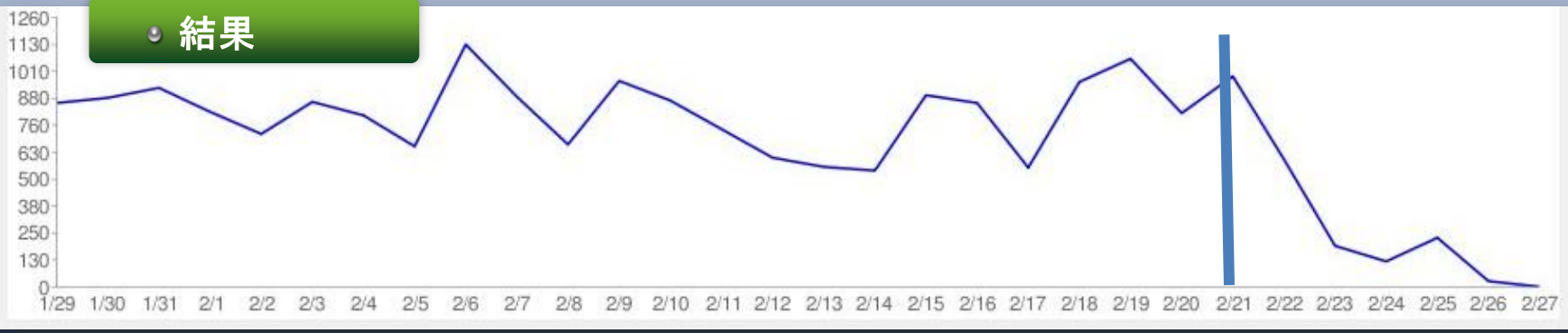
WALEDACボットネット「遮断」アプローチ

短期的 – 先例を作る



Hotmailは18日間で
Waledac感染コンピュー
[illegible]
6[illegible]件を[illegible]断
[illegible]
ボットネット
上位10位

結果



DNSの対策：ホスト名の削除

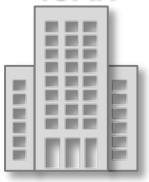
ICANNの紛争解決方針

ハーダーに動きを知られ、対応の時間を与える

犯人逮捕

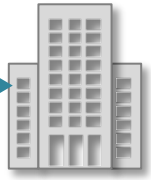
犯人不明のため、法的対策が取れない

ハーダー



ICAN

統括

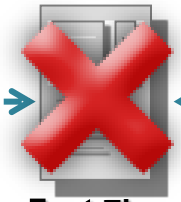


レジストラ

連邦裁判所

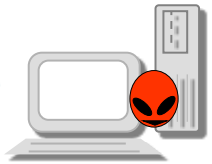
xxTLD

登録



Fast Flux DNS Server

名前解決



Waledac

一方的な仮処分 (ex parte TRO)

48時間以内のドメイン名の停止を、当事者に知らせることなく強制できる

停止依頼（非公式なレター）

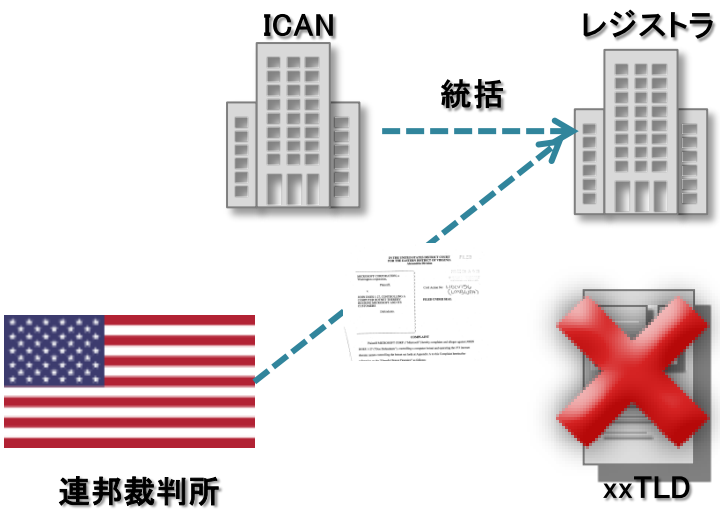
強制力がないため、必ずしも実施されない

DNS サーバーの Take Down

DNSサーバーは、ハーダーのものではない

このページは、Security Intelligence Report Vol.9（SIR9)に基づいて発表者が資料化したものであり、内容を保証するものではありません。正確な情報については、SIR9をご確認ください

DNSの対策：ホスト名の削除



一方的な仮処分
（ex parte TRO）

紛争相手への事前通史なしに、一時的（14-28日間）な対処を行うための特別な救済策、証拠隠滅や回避策の実施を阻止するために適用される。
一般に”一方的なTRO“の発行は困難で、連邦原則ルール 65に基づき、**「これを行わない場合に即座に解決できない危害が継続すること」、「相手方への通知を行い、それができない場合にはその理由を明確にすること」**を求めている。

連邦裁判所に対する一方的なTRO発行の必要性の訴求

連邦裁判所は、通知を行った場合、訴訟を避け、不法行為を続ける機会があると判断し、“一方的なTRO”を発行した。
（30年以上前に偽ブランド品に対して実施）

ドメインが乗っ取られているケースの対処

ドメイン登録者を被告とせず、27のドメイン登録者に対して被告人不詳として訴訟（John Does訴訟）。

中国のレジストラを通じて登録されたドメインの対処

起訴手続きの連邦原則、米国憲法、中国の法律を満たすことを確認し、ハーグ条約に基づいて、中国法務省に依頼

ドメイン登録者に通知

適法手続権利の維持を保証するため、ドメイン登録者に、訴状を送ると共に、電子メール、FAX、書簡による通知を行い、加えて、サイトを作成し、訴訟に関する書面をすべて掲載の上、これをメディアなどを通じて周知
www.noticeofpleadings.com

停止命令が実施されない場合の対処

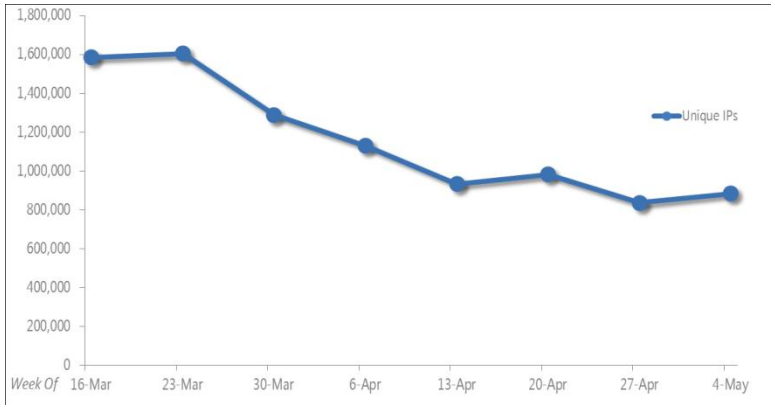
停止命令が実行され倍場合に、ドメインの所有権がマイクロソフトに移行するように申請し、認められる。

Operation b107:Rustock 解析結果

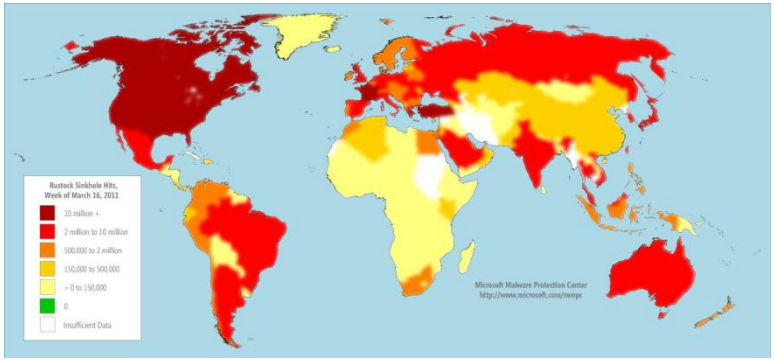
- 2011年3月16日、米国の7都市に拠点を置くホスティングプロバイダー5社からサーバーを押収
- プロバイダーの支援を受け、ボットネットを制御しているIPアドレスを分断

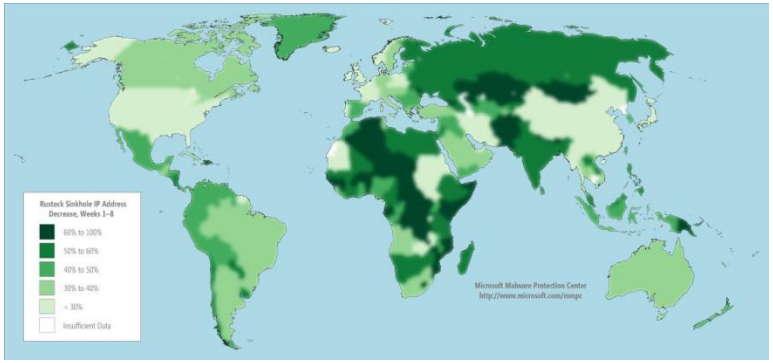
- ハードディスク20台の解析結果
  - スパムを送信するためのソフトウェアとデータ
    - 数千個の、メールアドレス、ID/パスワードの組み合わせを含んだテキストファイル
    - 42万個以上の電子メールアドレス
    - マイクロソフトや製薬会社の商標を不正に利用したテンプレート
  - ロシアのIPアドレスに対するサイバー攻撃に利用されていたことを示すデータ
  - 匿名インターネットアクセスを提供するノードとして使用
    - 電子メールテンプレート、商標、電子メールアドレスなどを保存する Rustockシステムへの匿名アクセスを提供するために使用したとみられる
- サーバーのホスティング契約を調査
  - オンライン決済サービスを利用
  - アカウントはモスクワ付近の住所が登録
  - C&Cサーバの多くは“Cosma2k”という個人によって設定
  - このニックネームは多数の異なる名前と関連
  - 法的な措置を取るために、これらの名前、電子メールアドレス、その他の証拠に対する調査を継続している

オペレーションの結果



シンクホールに接続した IP アドレス数の推移（1 週間ごと）



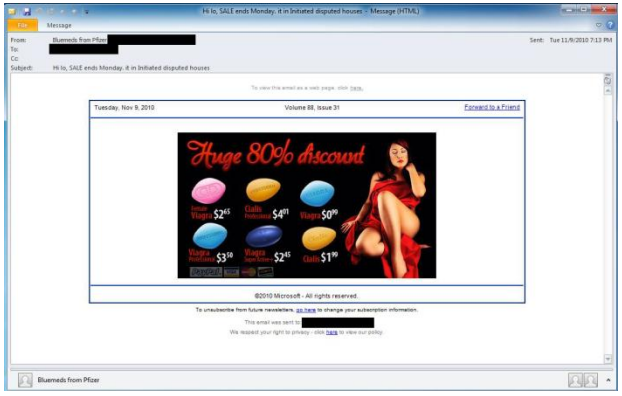


- Rustockが利用するフェールオーバー用ドメイン名を使った観測
  - アルゴリズムを解析し、該当するドメイン名をマイクロソフトが取得
  - このドメインへの通信は、シンクホールへ向けられる

- 地理的な分析

第1週（トラフィックの多い国）	
米国	5,580万
フランス	1,370万
トルコ	1,340万
カナダ	1,140万
インド	730万
ブラジル	710万

第1週（トラフィックの少ない国）	
中国	42万
チリ	50万
デンマーク	53万
ノルウエー	58万

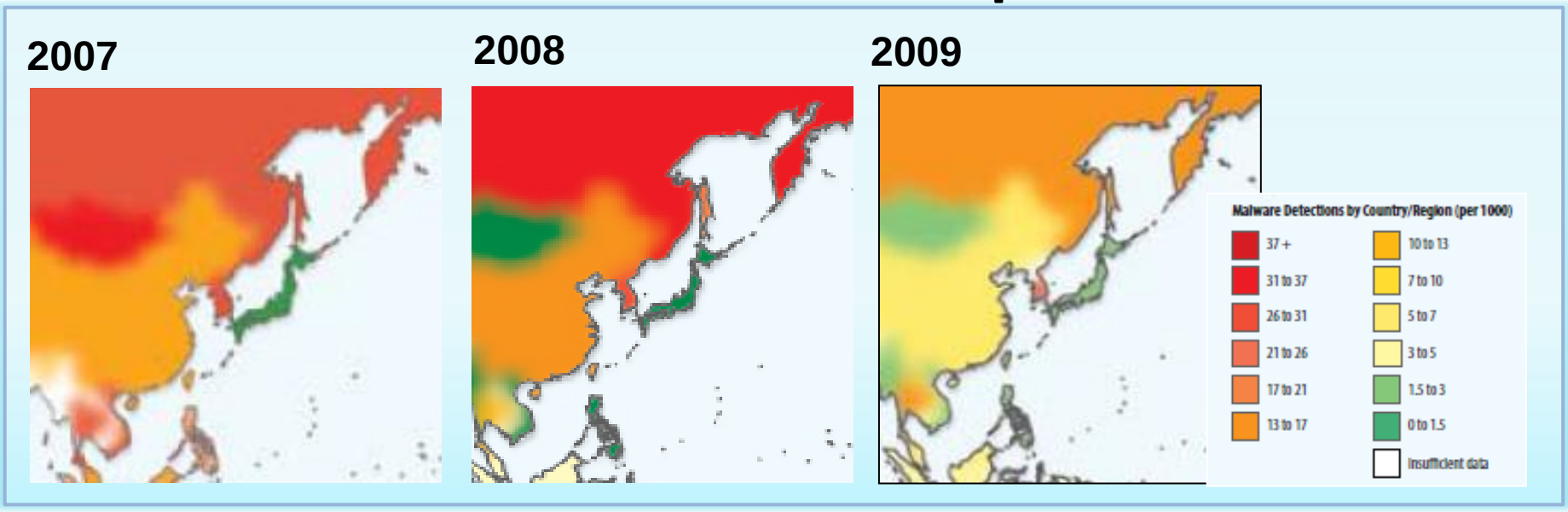


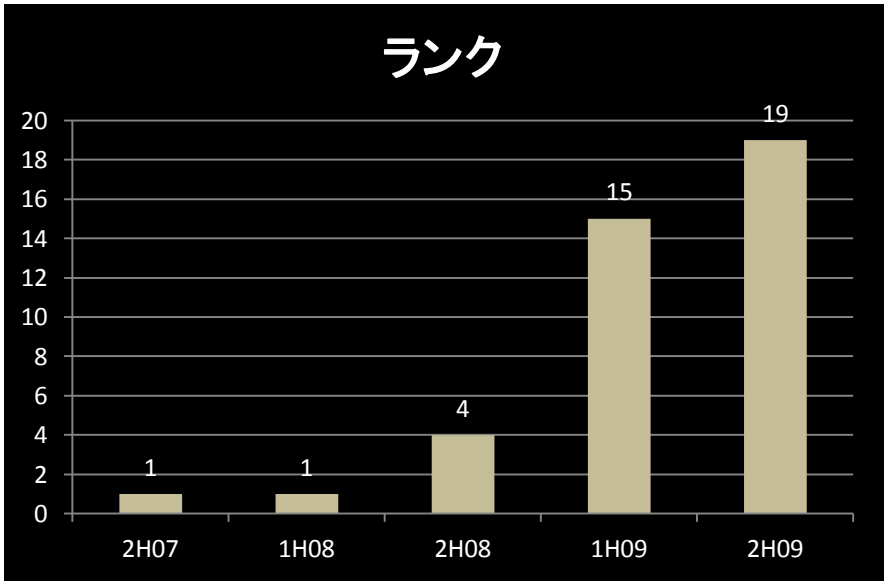
その他のアプローチ

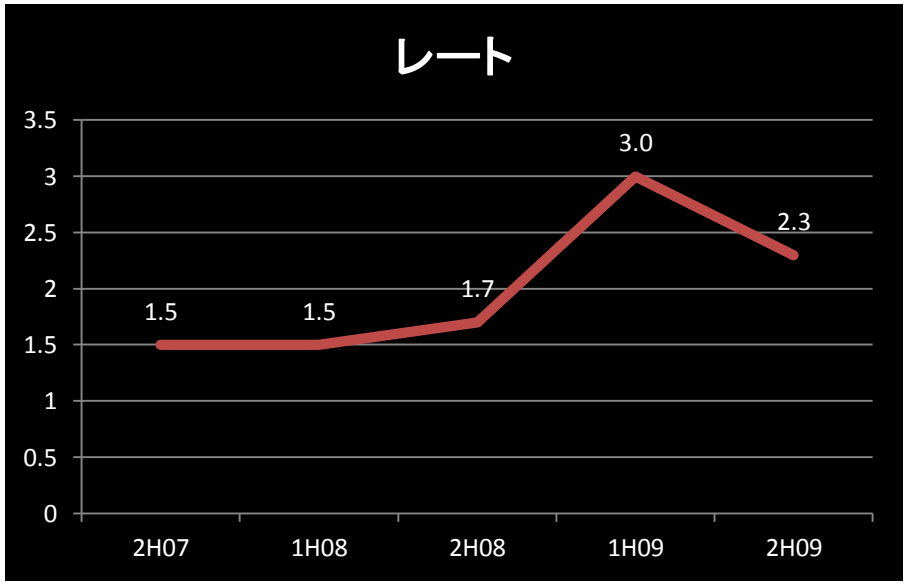
- MAPP: Microsoft Active Protection Program
  - セキュリティ更新プログラム公開前に、詳細な脆弱性情報を、セキュリティベンダーに提供
  - セキュリティ更新プログラム公開直後の集中的なアタックの対策
  - Zero-Day攻撃が発生した際にもユーザーを守る
- MSRT: Malicious Software Removable Tool
  - 月例の更新の際に、影響の大きなマルウエアを削除する
- SDL: Security Development Lifecycle
  - 安全なシステムを開発・構築するための規範
- MSRA: Microsoft Security Response Alliance
  - GAIAIS, SCP, SAFI

むすび

Malware Infection Rate in Japan







USB 経由で感染するマルウェアの減少

XP/Vista 自動実行機能（Autorun）無効化の効果

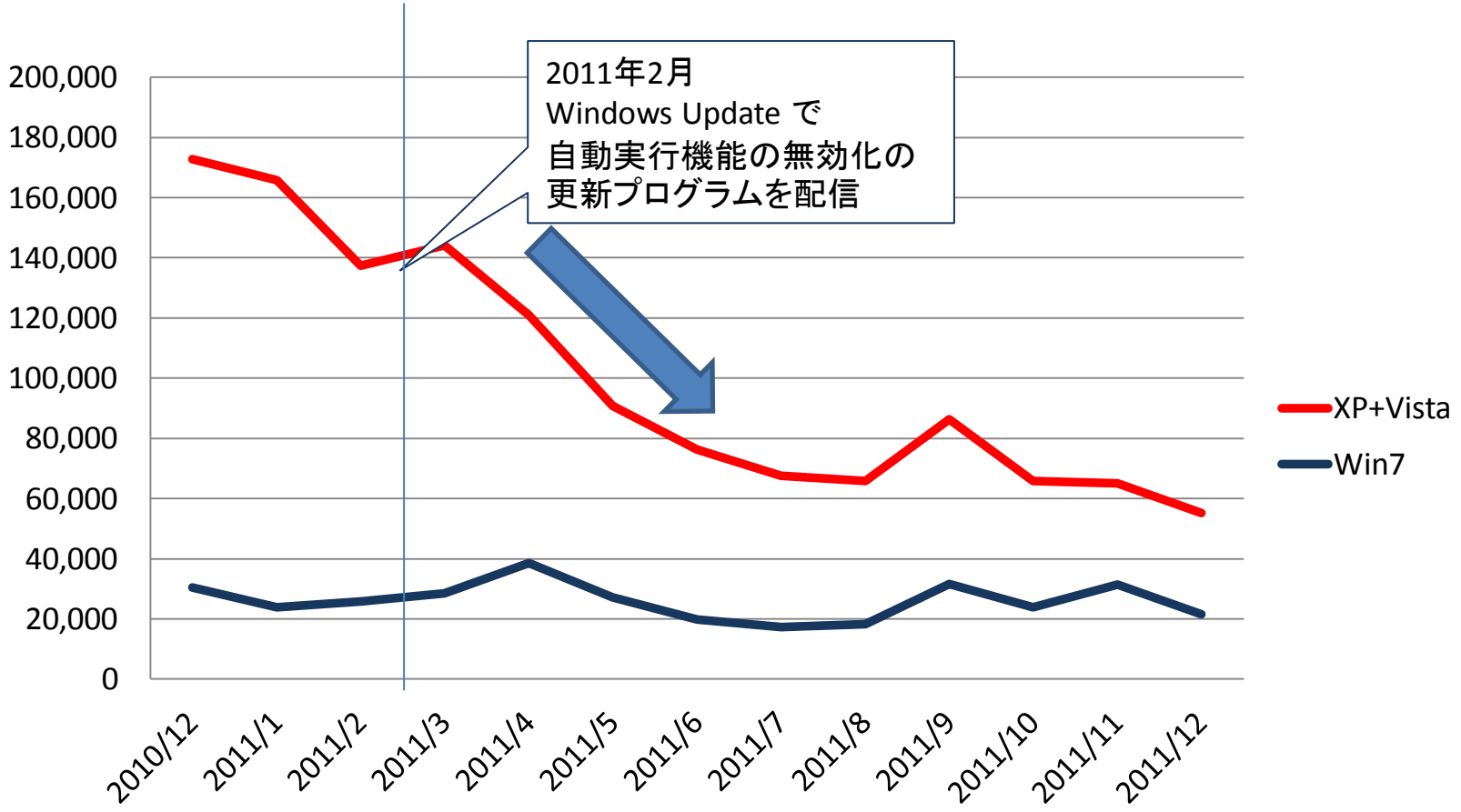


図5. 悪意のあるソフトウエア削除ツールで削除された Conficker の数 (2010/12-2011/12)

- Windows XP, Windows Vista に自動実行機能（Autorun）を無効化する更新プログラムを配信することで、約 9か月間で Conficker を半分以下に削減

結び

- 昨日とは違う今日
  - インターネットの発展・変化に伴って、攻撃の目的と方法が変わっている
  - 境界領域防御だけでは守れなくなってきている
- 対策の方向性
  - 通達から制御へ
  - 管理者権限からユーザー権限へ
  - ブラックリストからホワイトリストへ
  - インタビューから計測へ
  - より安全性の高いシステムへ
  - セグメンテーションを再考する
- 現実的に対策を進める
  - すべてを一度に対応できるのがベスト
  - しかし、何もしないのはワースト


Microsoft®
Be what's next.™