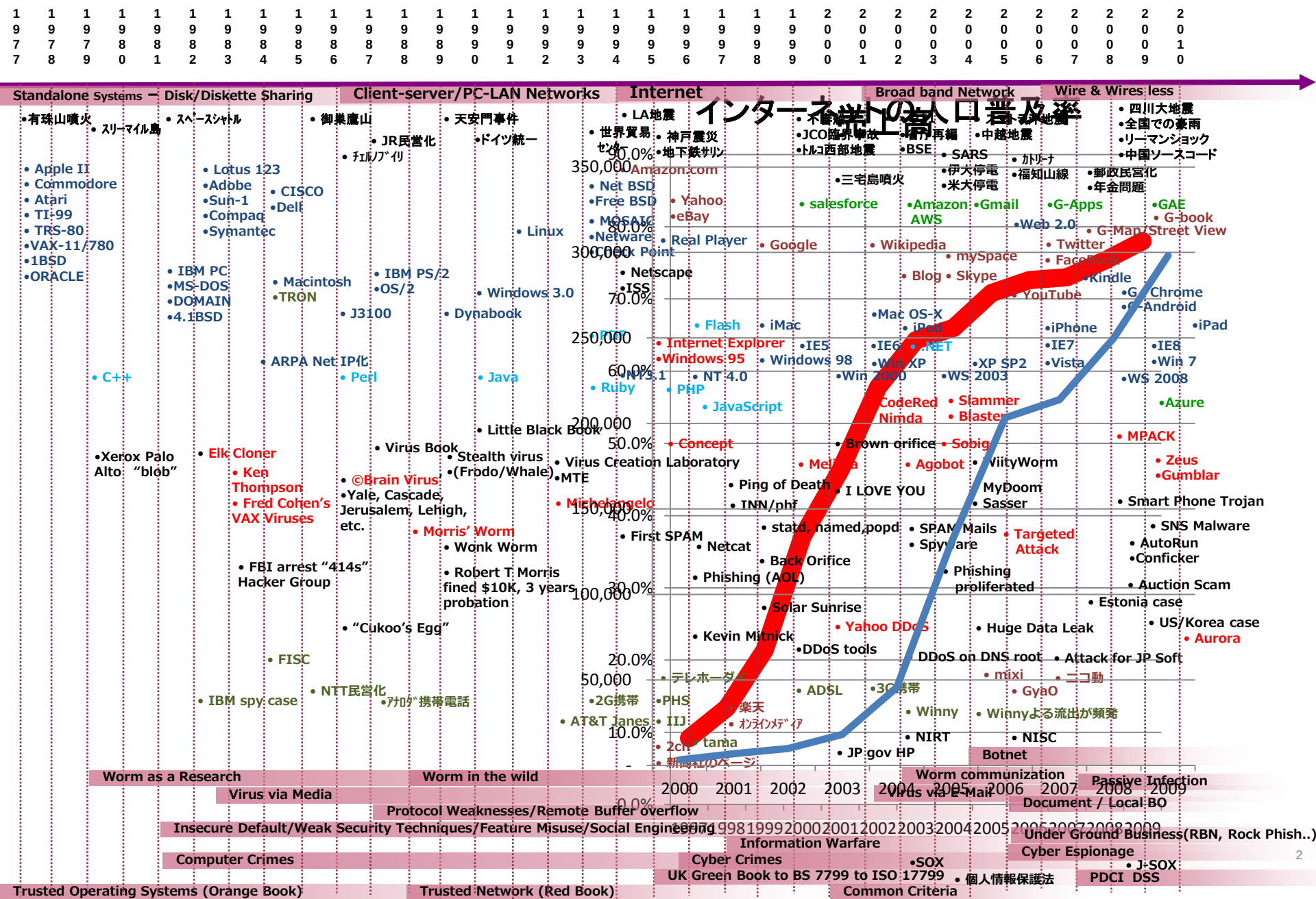
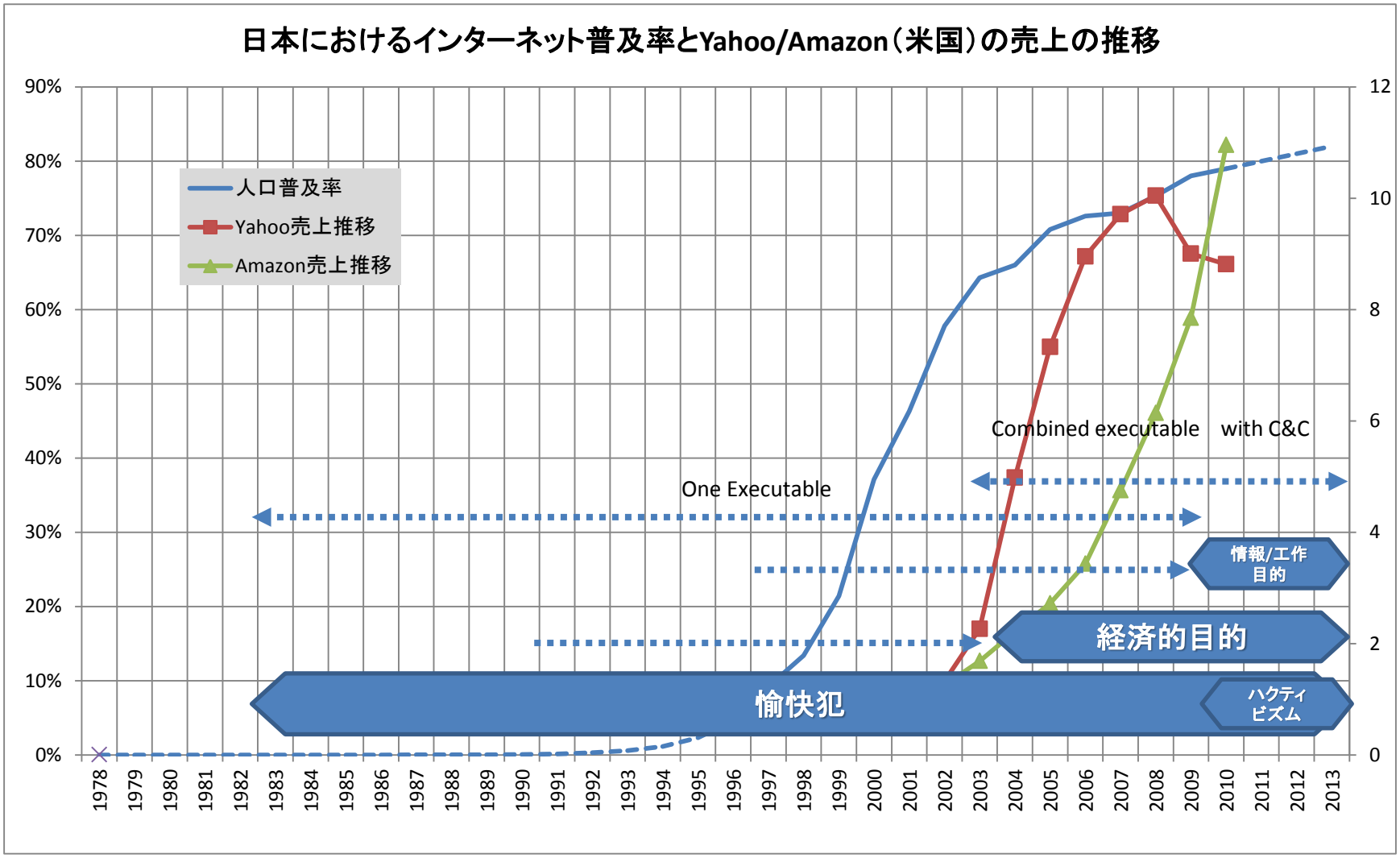
サイバー攻撃
脅威の多様化と顕在化

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

30+ years of computing & insecurity




日本におけるインターネット普及率とYahoo/Amazon（米国）の売上の推移
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
12
10
8
6
4
2
0
人口普及率
Yahoo売上推移
Amazon売上推移
Combined executable
with C&C
One Executable
情報/工作目的
経済的目的
愉快犯
ハクティビズム
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013

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HBGary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（Fox）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）

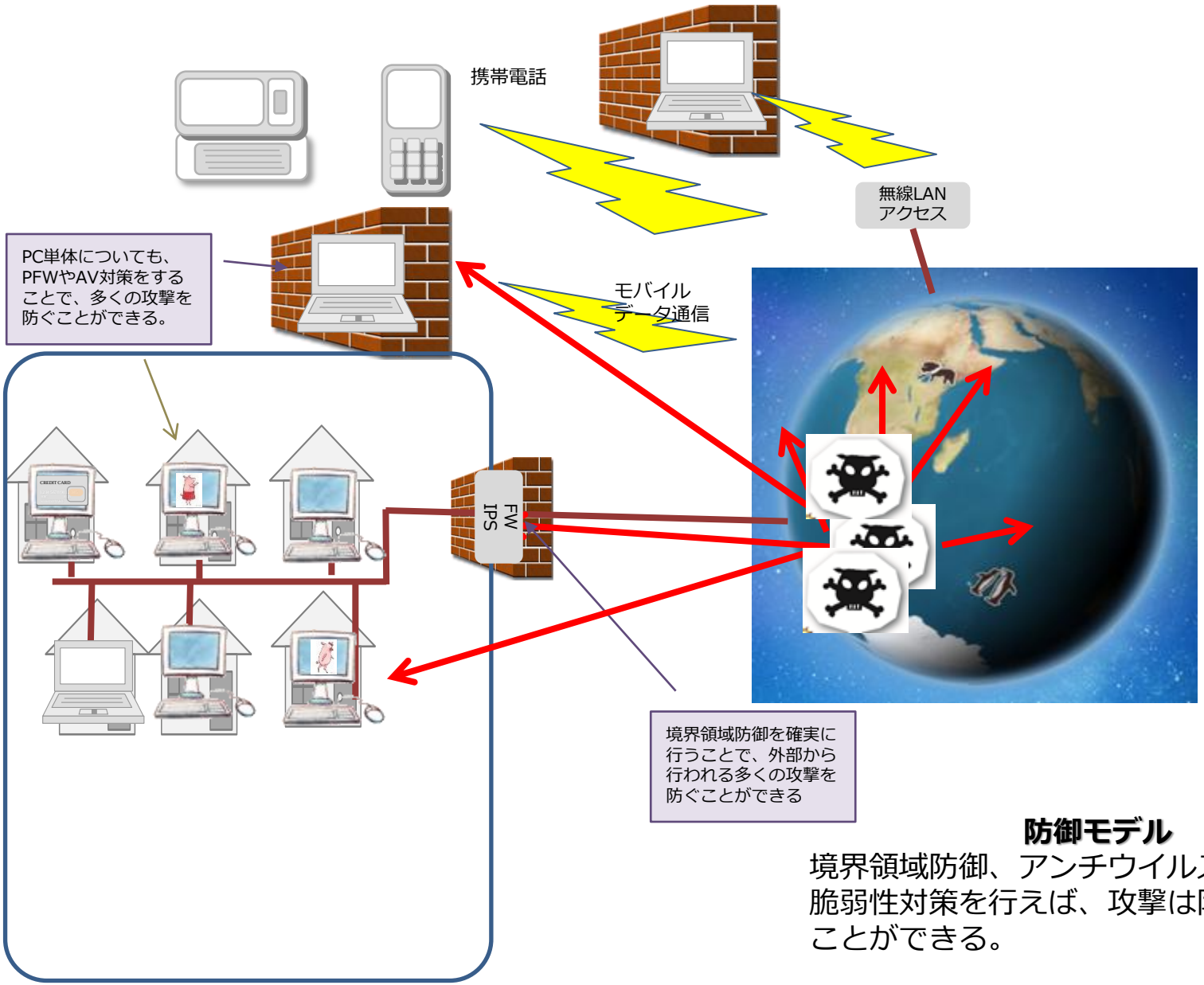
企業や政府機関の情報を盗み出すことを目的とした攻撃
（APT: Advanced Persistence Thread:高度で執拗な攻撃,またはCyber Espionage: 電子的な諜報活動）
三菱重工、衆議院議員会館などの事例。海外では、2010年のGoogleに対する攻撃、RSAセキュリティとロッキードマーチン社への攻撃など

サイバーウォー（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によるイラク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

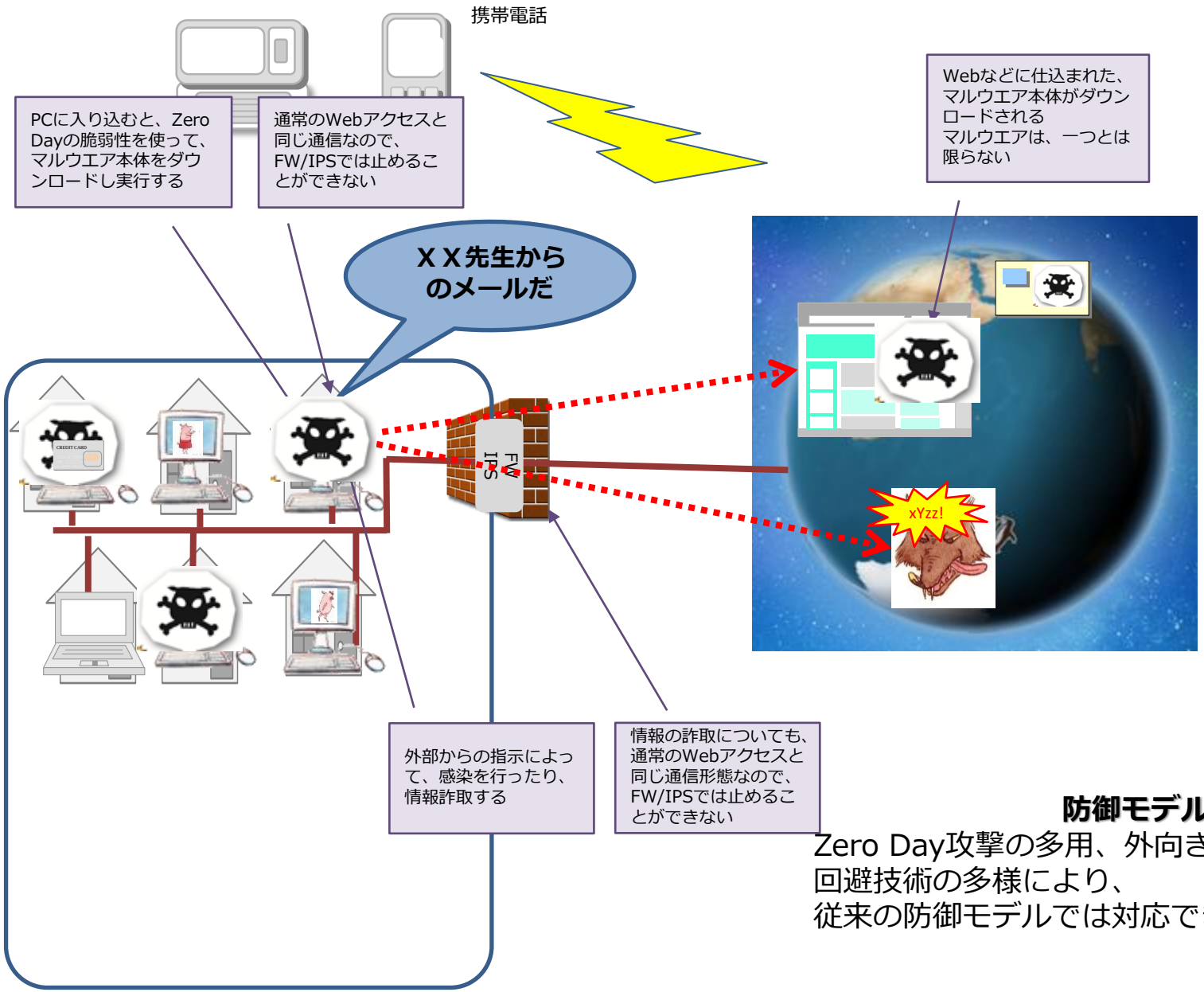
ネットワークワームや外部からの侵入行為の対策（従来の攻撃）



防御モデル

境界領域防御、アンチウイルス、脆弱性対策を行えば、攻撃は防ぐことができる。

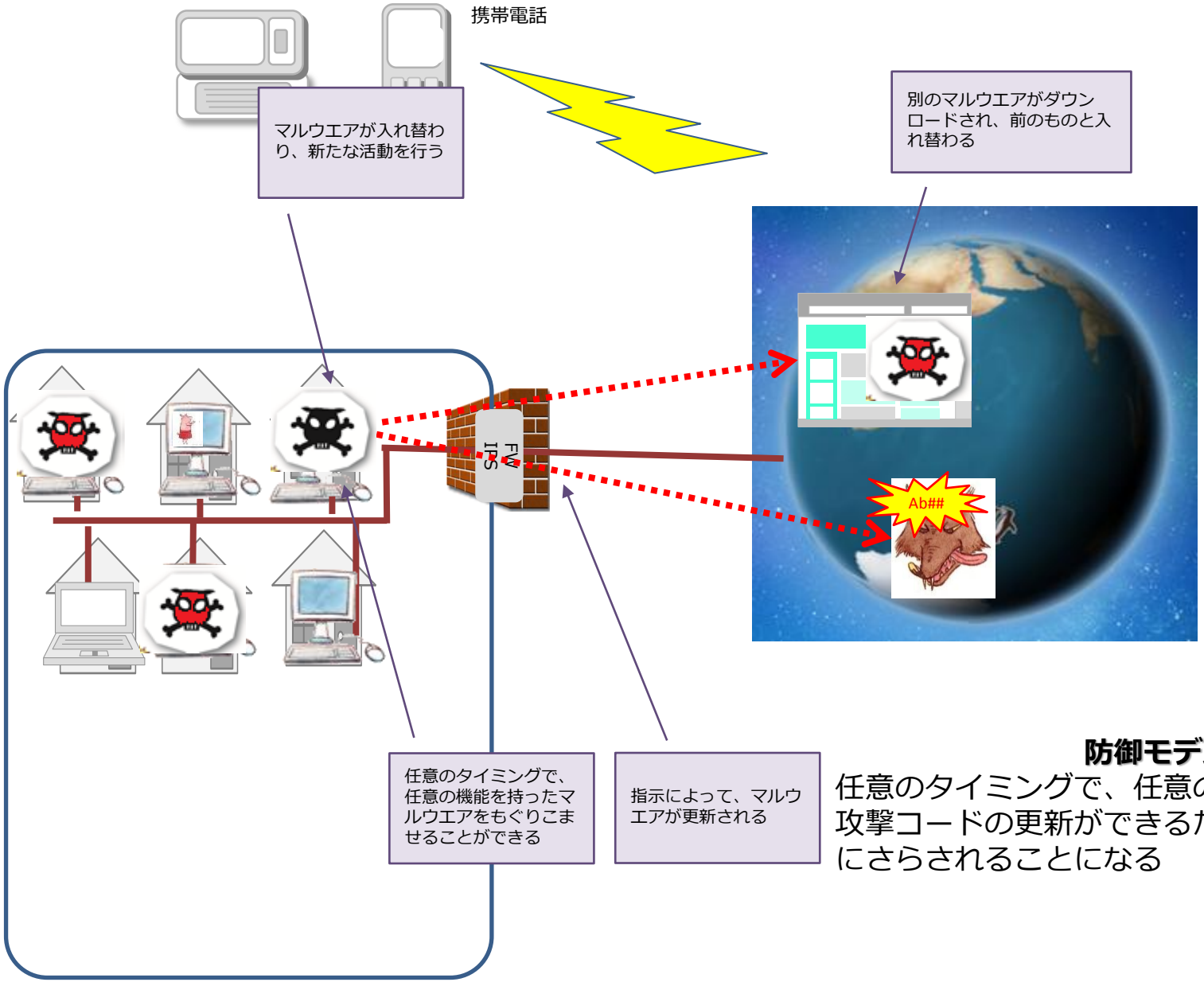
標的型攻撃とはどのような攻撃か？



防御モデル

Zero Day攻撃の多用、外向き通信の利用、AV回避技術の多様により、
従来の防御モデルでは対応できない

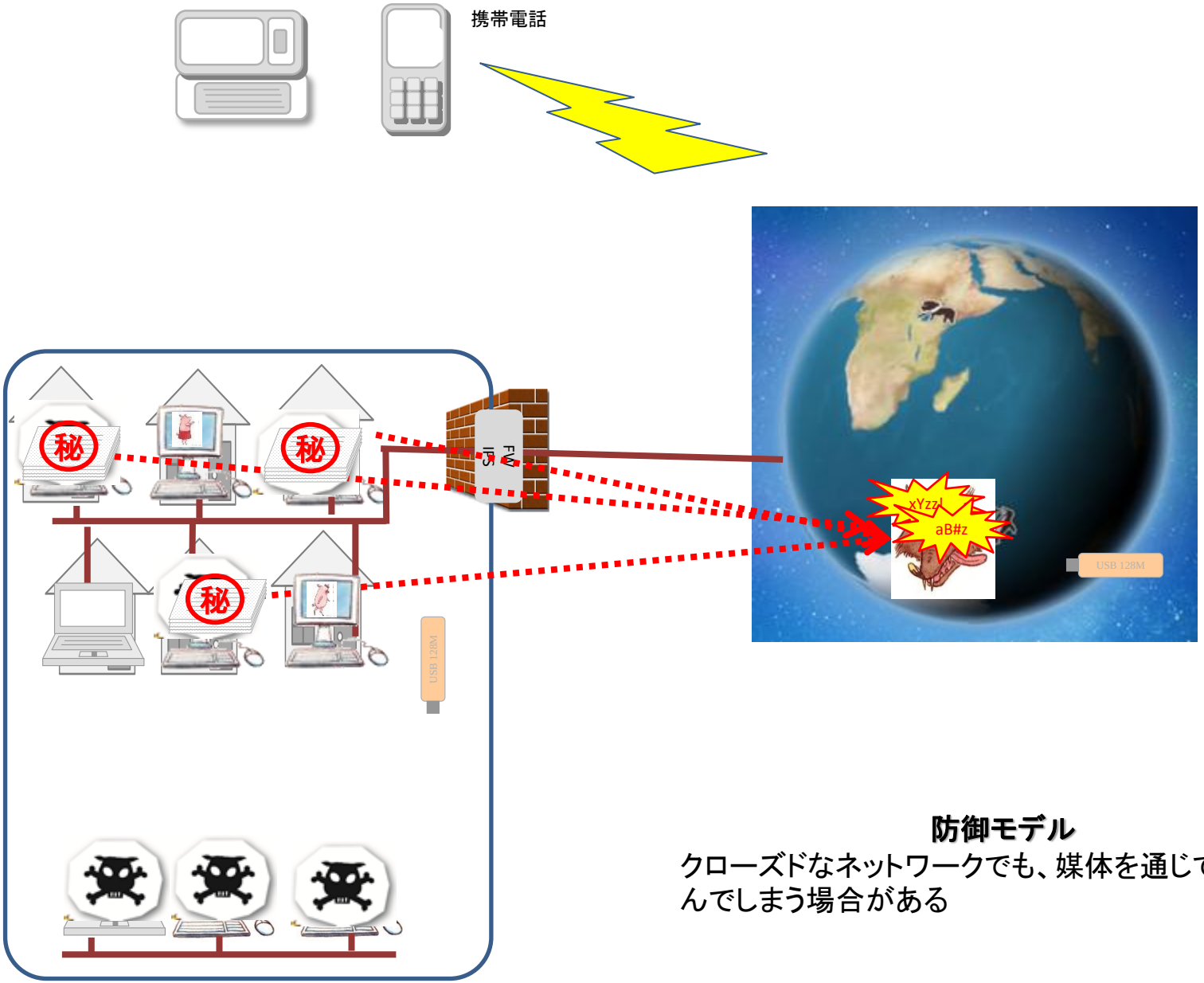
標的型攻撃は、段階的かつ継続的に行われる



防御モデル

任意のタイミングで、任意のコマンドの実行、攻撃コードの更新ができるため、継続的な脅威にさらされることになる

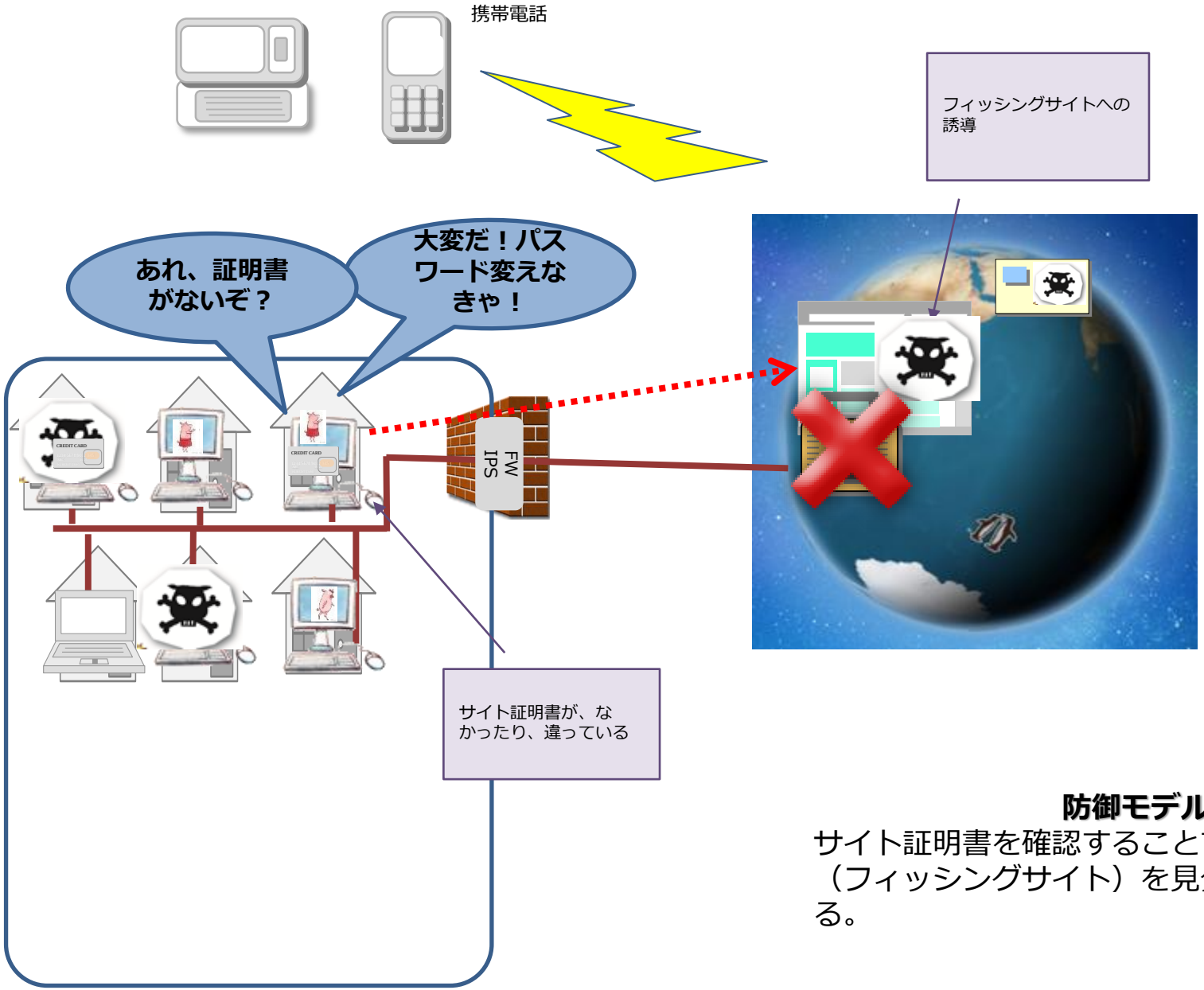
クローズドな環境であれば大丈夫なのか？（Confickerの例）



防御モデル

クローズドなネットワークでも、媒体を通じて、入り込んでしまう場合がある

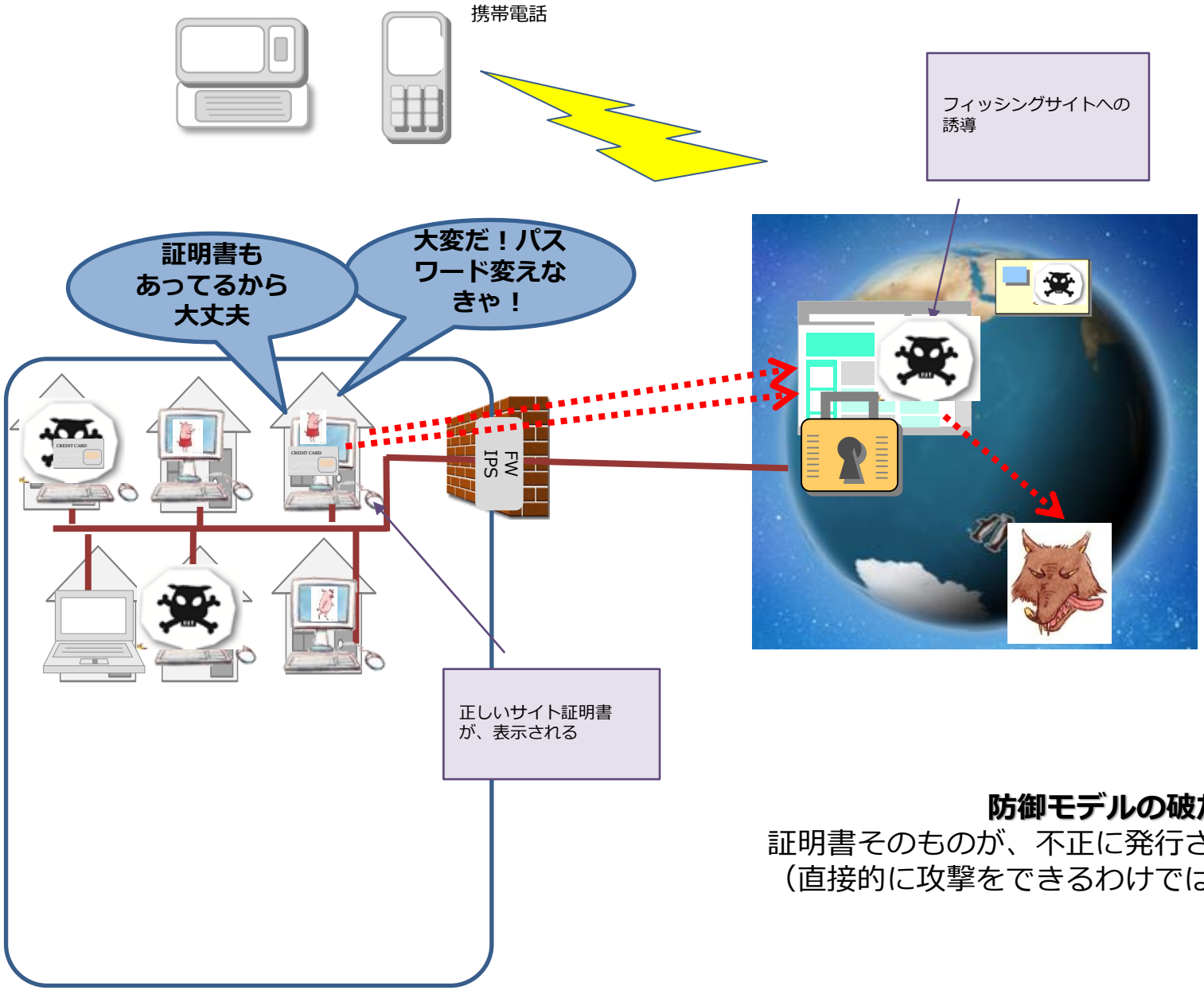
フィッシングに対するサイト証明書



防御モデル

サイト証明書を確認することで、偽サイト（フィッシングサイト）を見分けることができる。

証明書の問題？



防御モデルの破たん？

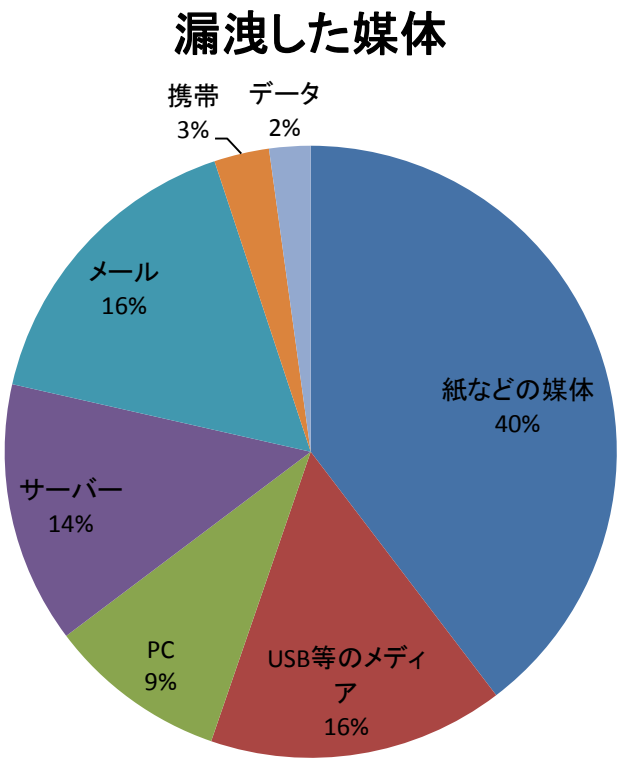
証明書そのものが、不正に発行されている。
（直接的に攻撃をできるわけではないのだが…）

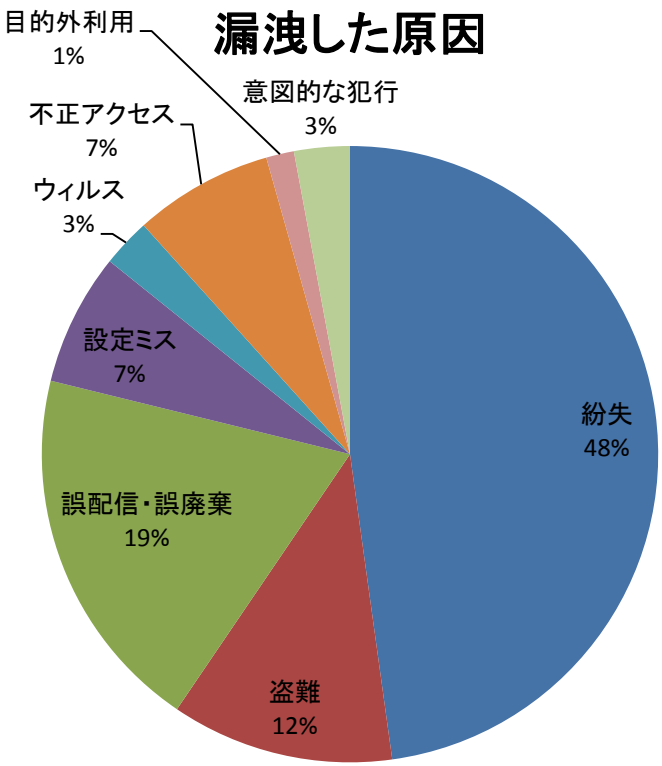
2011年に国内で発生した事件

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

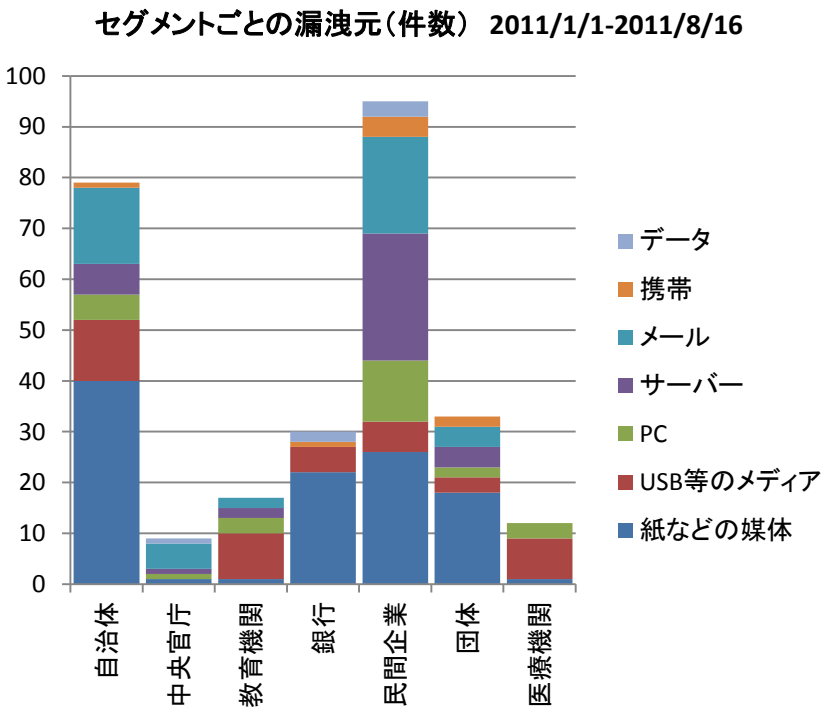
2011年に国内発生した事件の傾向

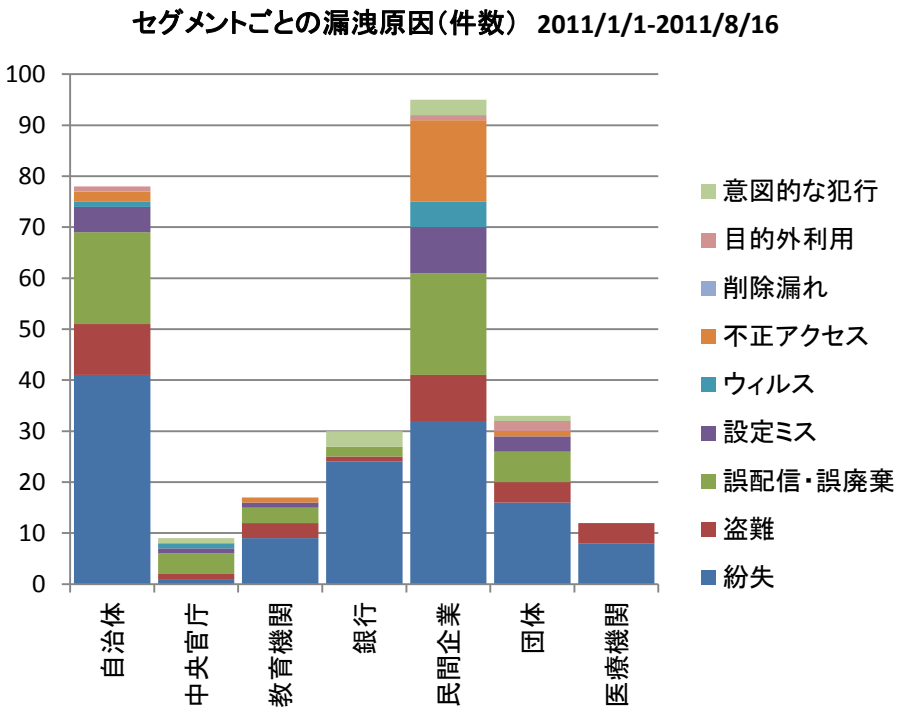




情報ソース：Security NEXT:個人情報漏洩事件・事故一覧
http://www.security-next.com/category/cat191/cat25

2011年に発生した事件の傾向





- 自治体の情報漏えい事故の割合が多い
- 内訳

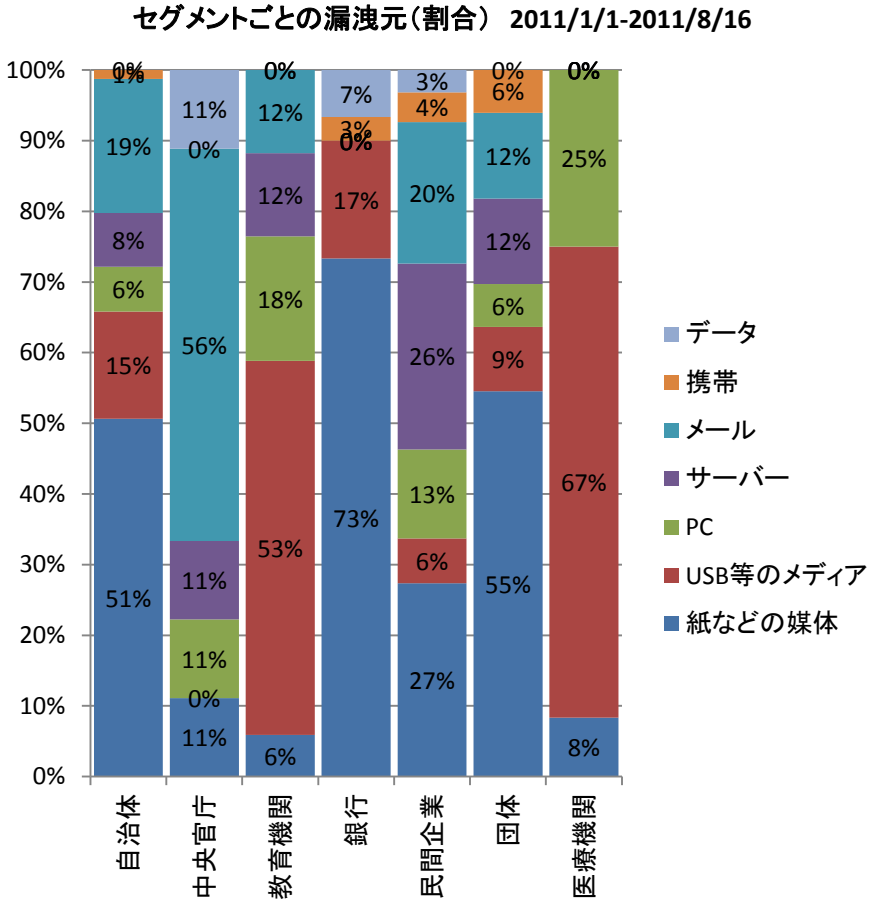
紙などの媒体	51%
メールの誤送信が	19%
USBメモリ等	15%
サーバー等	8%
PC	6%

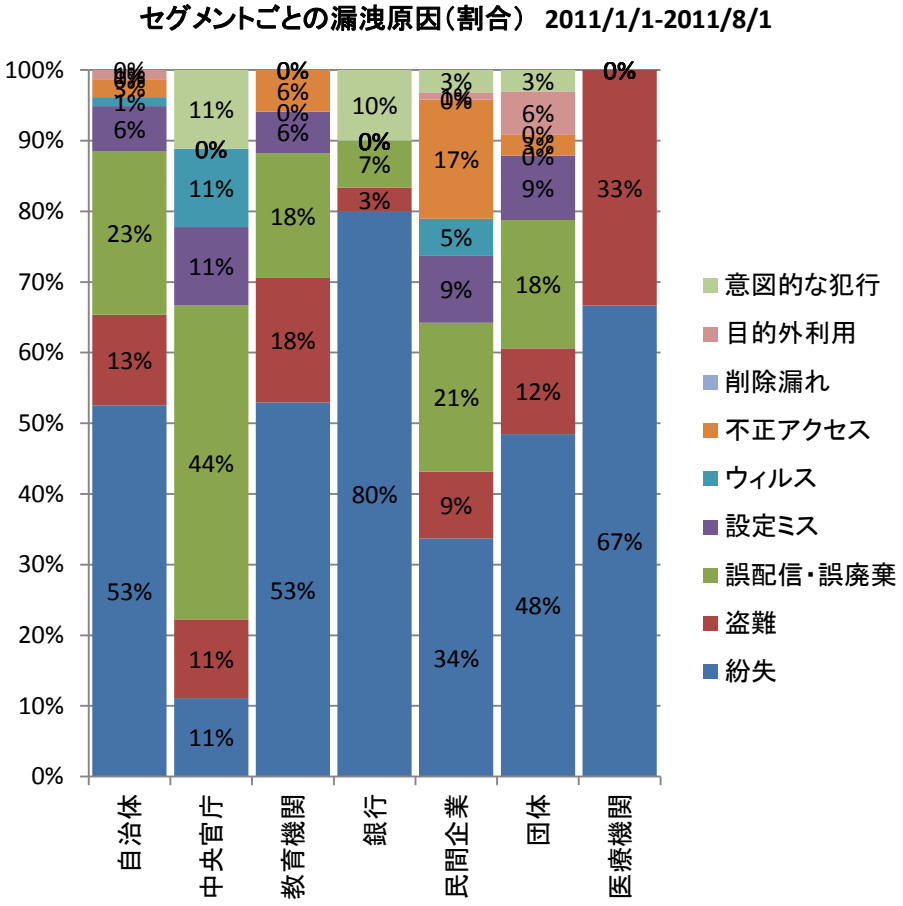
- 内訳

紛失	53%
盗難	13% (合計64%)
誤配信	23%
設定ミス	6%
不正アクセス	3%

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

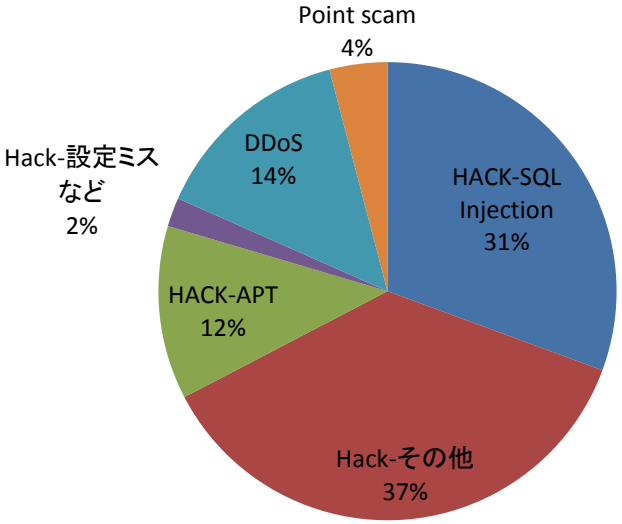
主な出典:Welcome to 2011, Year of the Hacker, Jason Mick (Blog) - June 14, 2011 9:40 PM

http://www.daily tech.com/Welcome+to+2011+Year+of+the+Hacker/article21806.htm

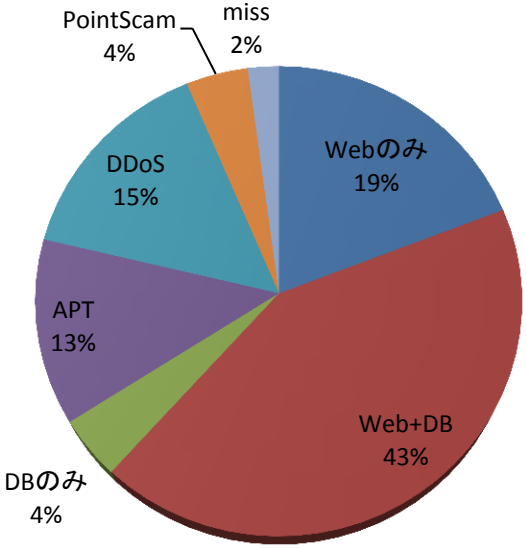
事案の内訳

- ハッキング　37(80%)
  - SQL Injection　*14(30%)*
  - APT(新しいタイプの攻撃）　*6(13%)*
  - その他　*17(37%)*
- DDoS　7(15%)
- Point scam　2(4%)

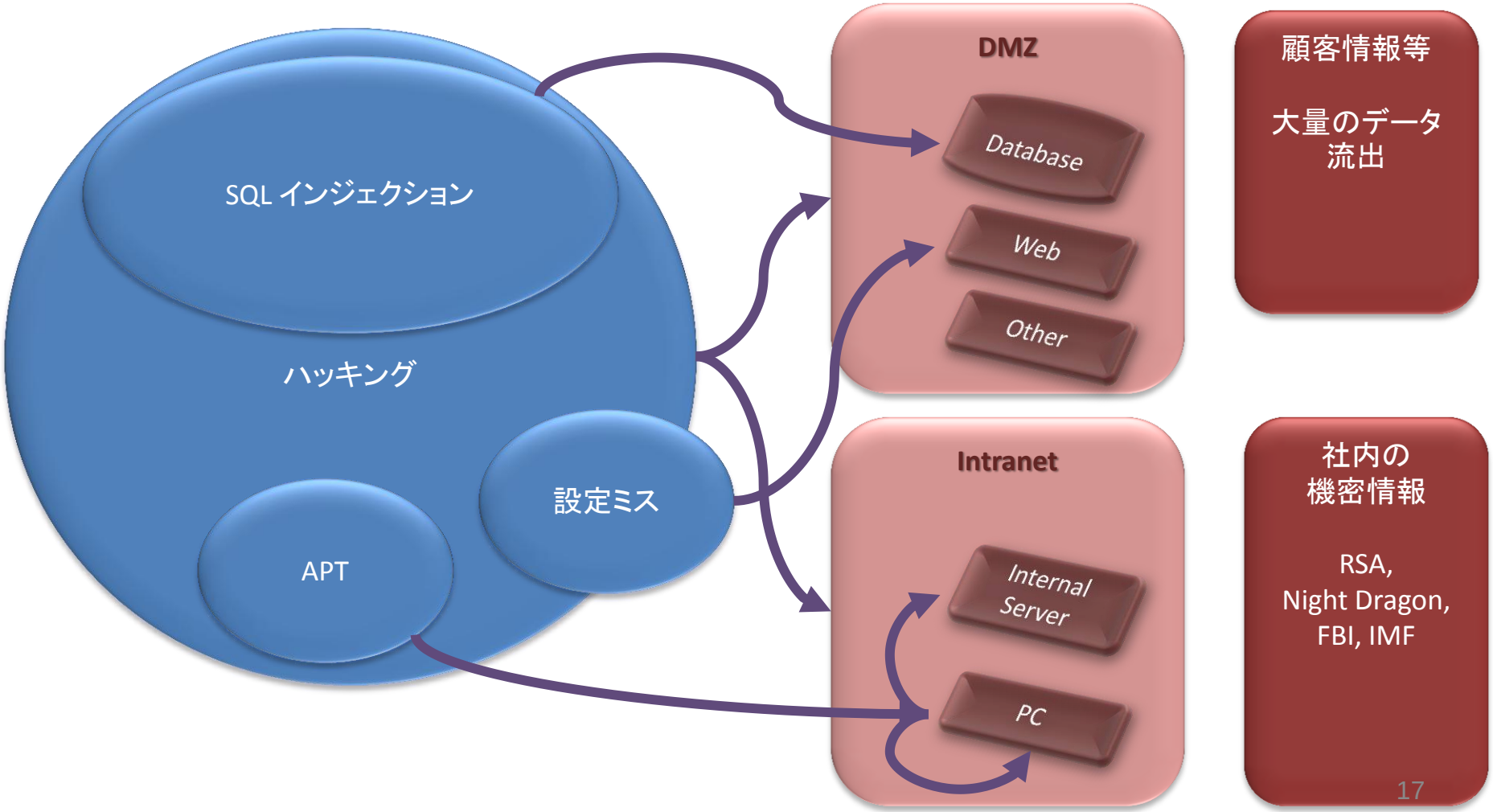
侵害手法の内訳（中分類）



侵害対象の分類



公開セグメントと内部セグメント



AGENDA

13:40	13:50	10	サイバー攻撃の現状と課題	MS 高橋
13:50	14:30	40	多発化する攻撃をハッカー目線で	IIJ 齋藤様
14:30	15:10	40	証明書は信頼できるのか	IPA 神田様
15:10	15:20	10	休憩	
15:20	16:00	40	マルウエアの最先端	FFR 金居様
16:00	16:40	40	法律面の現状と課題	高橋弁護士
16:40	17:00	20	戦う手段はあるのか？	MS高橋
17:00	17:40	40	今できる事、これから準備する事	全員