

情報セキュリティ

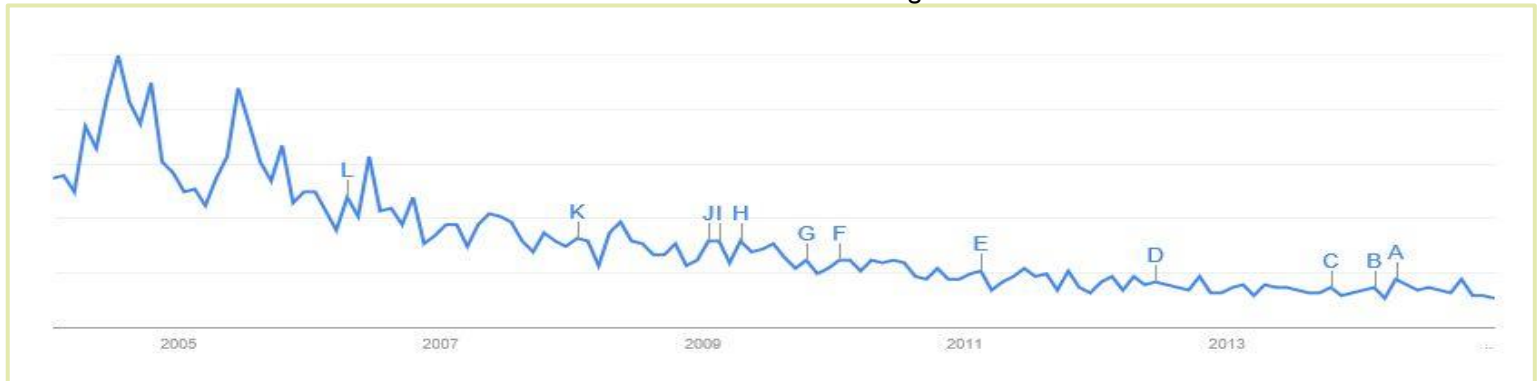
メディアから見た、そのトレンド（の一部）

田口 潤
インプレスIT Leaders編集主幹

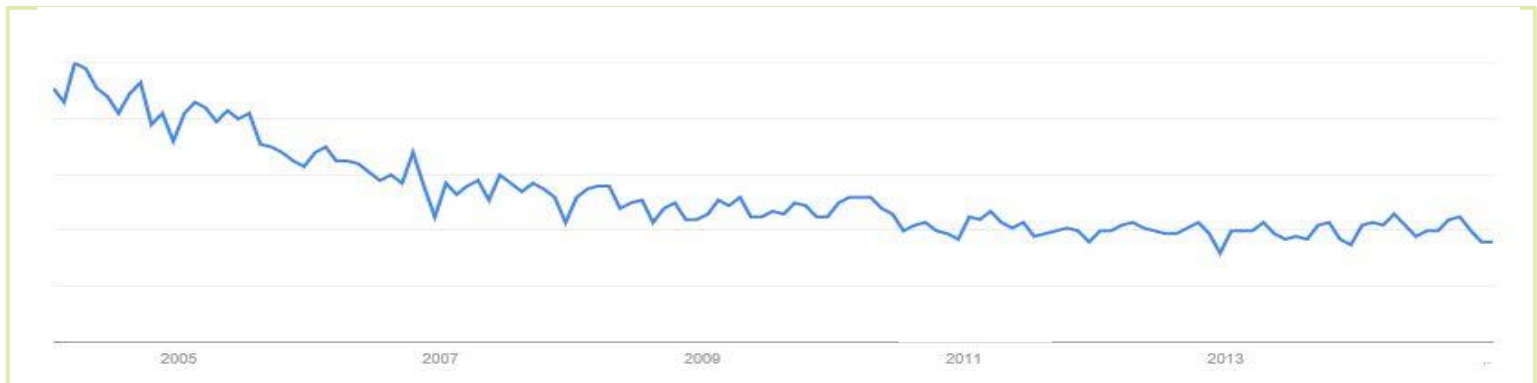
Google Trendによる動向①

Google Trendによる検索動向。ピークを100とした相対値

日本
情報
セキュリティ



米国
Information
Security



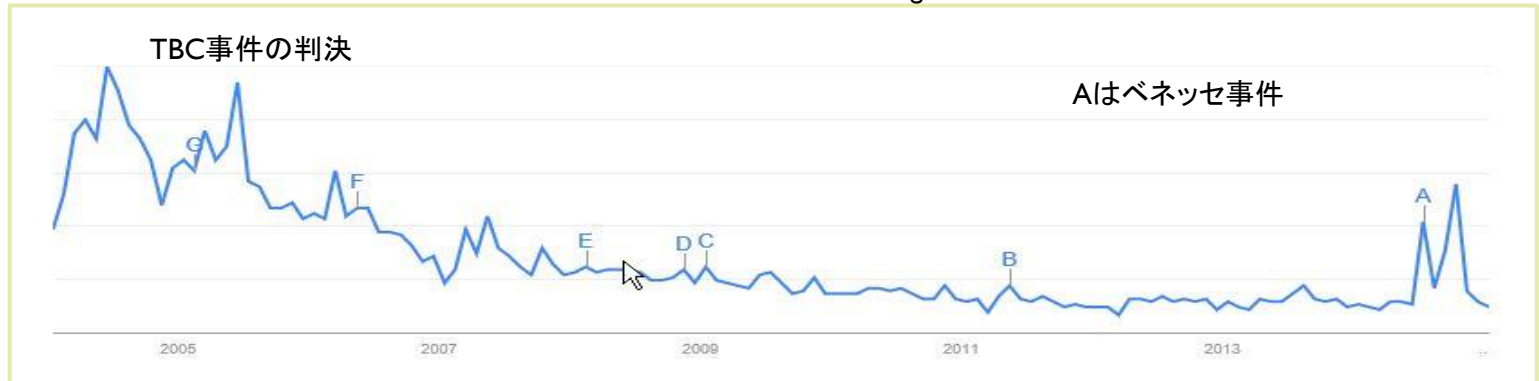
- ▶ 日本のピークは2006年前後。その後は漸減傾向
- ▶ 米国も同様だが、日本に比べると常に高水準

Google Trendによる動向②

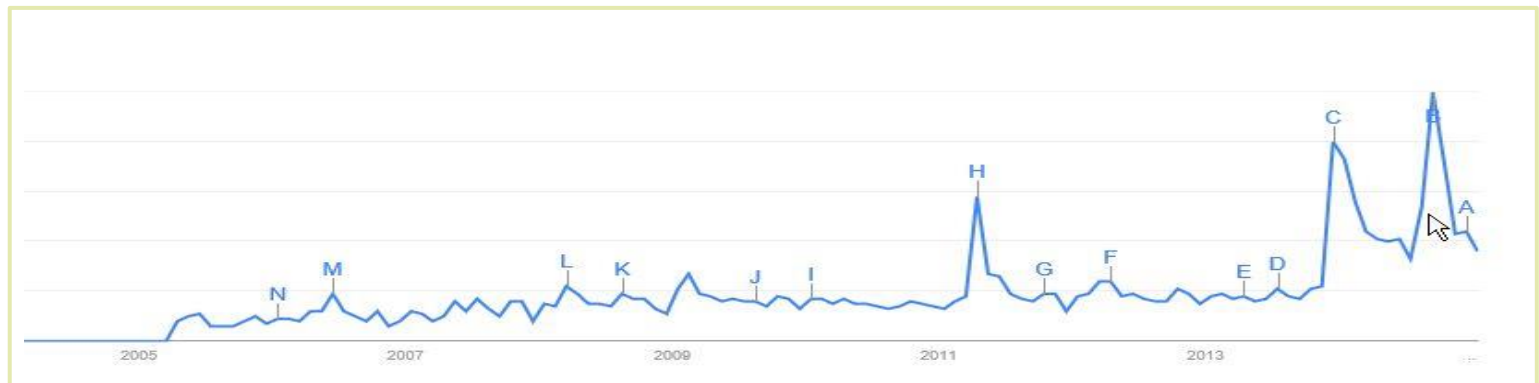


Google Trendによる検索動向。ピークを100とした相対値

日本
情報漏洩



米国
data
Breach



- ▶ 日本のピークは2006年前後。ごく最近(ベネッセ事件)までは沈静化
- ▶ 米国は最近になって大きな事件が多発

2006年の情報漏洩事件（Wikipediaより）

日付	法人・団体名	件数・人数	漏洩原因	漏洩内容・詳細・二次被害（悪用）など	出典
2006/12/22	日産自動車	538万人	不明	「旧お客さまデータベース」の顧客情報が流出した可能性。流出経路や流出件数は不明。 <u>二次被害（架空請求）</u>	[41]
2006/10/4	テレコム三洋 （NTTドコモの携帯電話販売会社）	3万8,483件	盗難（車上荒らし）	9月25日に同社新潟支店の社員が事務所移転準備の作業中に、駐車場で車上荒らしに遭い、取引先の販売代理店の顧客情報を含む経理処理用資料を保存していたUSBメモリーが盗まれる。	[42]
2006/10/06	三菱東京UFJ銀行	96万人	紛失	顧客情報86ヶ店の96万人分。ATM資料や伝票などを紛失。名義、住所、口座番号、取引金額や届印など含む。	[43]
2006/10/06	熊本市	28人	盗難	税金滞納者の個人名や納税額などを記した領収書、嘱託職員のバッグが盗難。	[44]
2006/10/03	テレビ朝日	108人		「題名のない音楽会21」の番組出演者など計108人分。インターネット上に流出。	[45]
2006/10/03	テレビ東京	47人	ウイルス感染	「出没!アド街ック天国」の取材候補先の担当者47人分。社外の制作スタッフがWinny通じ流出。	[46]
2006/09/25	東京社会保険事務所	4,708人	記録媒体の紛失	被保険者の情報を含むフロッピーディスクを紛失。	[47]
2006/09/19	甲南大学	506件	ウイルス感染	雇修者506件分。学籍番号、氏名、出欠記録や成績など。同大学院生の私物パソコンがShareウイルスに感染。	[48]
2006/09/13	NTTデータ	506件	ウイルス感染	共同プロジェクトの研究員や技術資料など506件分。社員の私物パソコンがWinnyウイルスに感染。	[49]
2006/09/07	富士ゼロックスシステムサービス	400万件	関係者の不正行為	自治体の戸籍情報400万件が流出。当該データを使い富士ゼロックスシステムサービスを恐喝未遂。 [45] 2007年1月12日第4回公判東京地方裁判所（平成18年刑（わ）第3506号 恐喝未遂）の被告人質問で、元協力会社社員は自治体から戸籍データをコピーし、40自治体分の約400万戸籍を自宅の個人PCに所持が判明。恐喝未遂は共犯者が持ち込んだPCにデータを一部コピーし使用された。2007年2月16日第5回公判では富士ゼロックスシステムサービスを恐喝したとされる共犯者は、流出した戸籍データを格納したPCを2台保持していたことが明らかになった。富士ゼロックスシステムサービスが戸籍事務のコンピュータ化を担当した自治体のうち、流出した40自治体について、どの自治体の戸籍データが流出したかは明確にはなっていないが一部はWEB上で名前が掲載されている。9月8日記事	[50]
2006/06/13	KDDI	399万6,789人		インターネット接続サービスDION（現au one net）の利用者399万6789人分。漏洩情報を持ち込み金を脅し取ろうとした男2人が恐喝未遂容疑で逮捕された。	[51] [52]

2013－14年の情報漏洩事件（同）

日付	法人・団体名	件数・人数	漏洩原因	漏洩内容・詳細・二次被害（悪用）など	出典
2014/7/9	ベネッセ	760万件 最大2070万件の可能性	外部持ち出し （詳細不明）	子供や保護者の住所や氏名、電話番号、子供の性別や生年月日など（ベネッセ個人情報流出事件）	[5]
2014/06/20	長野県須坂市の小学校	33人	記録媒体の紛失 外部持ち出し	男性教諭が、担当する児童の名前や写真、連絡網などを私物のUSBメモリに保存し、持ち帰り、紛失。	[6]
2013/10/29	寒河江市立小学校	21人	記録媒体の紛失 外部持ち出し	20代女性教諭が児童の個人情報を保存したUSBメモリを紛失。校長の許可を得ず自宅に持ち帰る。	[7]
2013/10/3	アドビシステムズ	290万人	不正アクセス	顧客名、暗号化されたクレジットカードまたはデビットカードの番号、有効期限、および顧客注文に関連するその他の情報	[8]
2013/8	N.T.Technology	約3万件	OnionちゃんねるTor板上に流出	2ちゃんねるの有料サービスである2ちゃんねるビューア会員のクレジットカード番号や名前などの個人情報 匿名で投稿した投稿者個人が書き込み内容と共に特定される内容が含まれており、実際にピンポンダッシュや無言電話などの二次被害が報告されている他、ライトノベル作家の杉井光が他の作家に対する誹謗中傷を行っていたことが発覚し、本人が謝罪する事態なども発生している。	[9] [10]
2013/05/17	Yahoo! JAPAN	最大2200万件	不正アクセス	不正アクセスによりIDが抽出されたファイルが作成され、外部に流出した可能性。うち148.6万件については、不可逆暗号化されたパスワードおよびパスワード再設定に必要な情報の一部が流出した可能性。	[11]

- ▶ Yahoo!の事件は件数が膨大だが、大半はIDのみ。ちなみに同社は2004年に内部犯行により、BBの登録者の個人情報450万人分の情報漏洩に遭った。この時、一人500円の金券を送付している
- ▶ これに倣ってベネッセはお詫びの金額を500円に設定。金券(電子マネーギフト、図書券、自社運営の財団基金への寄付のいずれか)を送付

180° 事情が異なる米国

2014年に表面化した事件のトップ5を見る

5位：CHS社

- ▶ 社名はCommunity Health Systems。全米29州で206の病院を運営する医療大手
- ▶ 被害
 - ▶ 2014年8月、中国と見られるハッカーによって450万件の患者データ(氏名、住所、生年月日、電話番号、社会保障番号)が漏洩
- ▶ 手口
 - ▶ 「高度に洗練されたマルウェアと技術が使われた」(事故を調べたMandiantがSECに提出した文書)
 - ▶ 主に社会保障番号が目的。病院は大量の情報を持つが脆弱

<http://www.healthcareinfosecurity.com/healthcare-fresh-target-for-hackers-a-7207>

4位：The Home DEPOT



- ▶ 米国最大のホームセンター。米国、カナダ、中国などに2000以上のテナポを持つ
- ▶ 被害
 - ▶ 4月から9月に書けて、合計5600万件の顧客カード情報と、5300万件の電子メールアドレスが漏洩
- ▶ 手口
 - ▶ Targetの事件(後述)と同様に外部業者のIDから侵入され、支払いシステムが感染。データの暗号化やPOSのセキュリティ対策は実施済み。しかし独自のマルウェアを利用されたため、発見できなかった。
- ▶ 事件の対策費は6200万ドル(事故調査、顧客のクレジット監視サービス、コールセンターの増員、法的な費用など)
- ▶ EMV(Europay, MasterCard、Visa)技術を全店に適用中
- ▶ <http://www.databreachtoday.com/home-depot-53-million-e-mails-stolen-a-7537>



TARGET (番外)

- ▶ 北米に2000店弱の店舗を持つ米大手小売りチェーン
- ▶ 被害
 - ▶ 2013年末のクリスマス前に、クレジットカード、デビットカードが漏洩。1億1000万人に影響。その後続く、大規模なハッキングの最初のものであり、手口の高度差、CFO、CIO(2014年3月)とCEO(同5月)の首が飛んだことなど、多くの関心を集めた
- ▶ 手口
 - ▶ 出入りの業者のIDで同社のネットワークに侵入。POSを感染させる
 - ▶ POSからは売上げデータを本部に送付するタイミングで、盗んだデータを外部に送付。送付先を5カ所に分散させる年の入れ方
 - ▶ マルウェアのコード解析から「Rescator」という、盗難クレジットカードを扱う“ダークネット”が浮上。地理的拠点をたぐると、ウクライナのオデッサに拠点がある
- ▶ 対策
 - ▶ 端セキュリティ製品「FireEye」、シマンティック社との契約、PCI-DSSの認証取得など事前に様々な手を打っていた。がFireEyeなどの一部機能をオフにしていたことが指摘されている

<http://it.impressbm.co.jp/articles/-/11538>

3位：JPMorgan Chase

- ▶ 米国最大手の銀行であり、セキュリティ対策も世界一とされる
- ▶ 被害
 - ▶ 7600万世帯、700万の中小企業の顧客情報(名前、住所、電話、メールアドレス)が漏洩。ただし銀行の中核システムではなく、Chase.com, JPMorganOnline, Chase Mobile and JPMorgan MobileといったWebとモバイルサービスから。「口座番号やパスワード、誕生日、社会保障番号が漏洩した証拠はない。顧客はパスワードを変える必要はない」(同社のSECへの報告より)。
- ▶ 手口
 - ▶ 不明
- ▶ 関連するすべてのシステムを精査して復旧。Bloombergが「ロシアのハッカーがChaseとほかの金融機関を攻撃」と報じた8月に表面化した。
- ▶ http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/?_r=0

2位：eBay

- ▶ 世界最大のオークションサイト。ECサイトも運営
- ▶ 2014年2月から3月にかけて、中枢のデータベースに侵入された。ユーザーIDやパスワード、メールアドレス、住所、電話番号、生年月日などが流出。ただしパスワードなどは暗号化されていた。またクレジットカードなどの情報は別に管理されている（PayPalの情報も同じく別管理）
- ▶ 5月初めに発覚し、eBayは即座に1億4500万人の全利用者に対し、パスワード変更を求めるメールを送付。「（その時点で）不正行為などは見つからないが、ユーザーがパスワードを使い回していると深刻な被害になりかねないため、ebayユニークなパスワードに変更して欲しい」。
- ▶ ハッカーは、ebayの社員のアカウントを使った模様。eBayは、この漏洩により（利用者が慎重になるため）、10%程度の減収を見込んでいる。

<http://www.forbes.com/sites/gordonkelly/2014/05/21/ebay-suffers-massive-security-breach-all-users-must-their-change-passwords/>

1位：Sony Pictures Entertainment



- ▶ ソニーの子会社であり、映画・映像メディア企業の大手
- ▶ 情報システムがハックされ、多様な情報(100TBと言われる)が流出した。未公開の映像コンテンツ、社員の人事情報、電子メール記録、契約する俳優などの社会保障番号、報酬など
- ▶ Guardians of Peace (GoP)が犯行声明。Lenaと呼ばれる、会社には不満を持った社員が関わったともされる
- ▶ GoPのマルウェアがかつて北朝鮮が攻撃に使ったマルウェアと似ているため、FBIは北朝鮮が背後にいることを示唆したが、専門家の間では否定的な見解が主流
- ▶ 現在進行形であり、被害の全容や犯人像など不明な点が多い。

<http://www.theverge.com/2014/12/8/7352581/sony-pictures-hacked-storystream>



--Warninig--

Wei've already warned you, and this is just a beginning.

We continue till our request be met.

Wei've obtained all your internal data including your secrets and top secrets.

If you doni't obey us, wei'll release data shown below to the world.

Determine what will you do till November the 24th, 11:00 PM(GMT).

**Post an email address and the following sentence on your twitter and facebook,
and wei'll contact the email address.**

i°Thanks a lot to Godi'sApstls contributing your great effort to peace of the world.i±

GOP



SPE事件の流れ

▶ 11月24日

- ・ 月曜の朝、通常通り始業。
- ・ しかし社員のPCには、頭蓋骨のおどろおどろしい画面
- ・ 「This is just the beginning we've obtained all your internal data」
- ・ 自らをGuardians of Peaceと名乗り、「100TBの情報をサーバーから詐取した」と宣言。

電話や電子メールが使用不能

▶ 11月25日~30日

- ・ 世界各国のメディアで一斉に報道。SPEでは依然、computers, e-mail and voice mail.が使用不能
- ・ 未公開4本を含む5本の映画がファイル共有Hubで公開。公開中だった「Fury」(ブラッドピット主演)は少なくとも100万ダウンロードされた。Annie, Mr. Turner, Still Alice and To Write Love On Her Armsも同様
- ・ 北朝鮮が関与しているとのレポートが表面化。SPEの映画「The Interview」を北朝鮮が「邪悪な挑発行為である」とWebで指摘していた。昨年の韓国政府や金融機関への攻撃と似た手段が使われていたなどから。
- ・ ただし、ハッキング元のIPアドレスを辿ると、バンコクの五つ星ホテルである、St. Regis Hotelだった
- ・ 北朝鮮は関与を否定

▶ 12月~

- ▶ ソニーの役員17人の報酬、従業員の給与がリークされる。ソニーはサイバーセキュリティ専門企業、SealMandiantを雇う。FBIも捜査を本格化
- ▶ 俳優兼脚本家アダム・サンドラーに対するソニー社員による痛烈な批判が公開。アンジェリーナ・ジョリーなどセレブのパスポートの画像、映画の予算、機密扱いの契約なども漏洩。ソニーの監査会社であるデロイトの社員のサラリーも公開される
- ▶ Guardians of Peace と名乗るハッカーが、ソニーの社員に対し、会社と縁を切る文書にサインしない者は家族を含めて攻撃するとのメールを送付。ハッカーは、「想像もできない場所からあなたたちを見ている」。ただし、本物かどうかは疑問
- ▶ Mandiant は、ソニーに対し、「この攻撃の範囲は、過去我々が対応したことがないもの。資産を破壊し、重要情報を公開する点で。少なくとも非常によく計画されており、組織化されたグループによると考えられる」と報告
- ▶ Guardians of Peaceは、ファイル共有サイトにレターをポスト。地域の平和を乱し、戦争を起こすテロ映画の上映中止を求める。同時に、先のソニー従業員への脅しへの関与を否定
- ▶ SPEの幹部によるアンジェリーナ・ジョリーを非難するメールのやりとりが公開。オバマ大統領に関するメールのやりとりも公開。人種問題に関する映画が好き、など。
- ▶ FBIは、捜査のアップデートを公開。破壊的なマルウェアを原因とし、情報が盗まれた。SPEの数千台のコンピュータを使用不能にしたなどの被害が明らかに。また北朝鮮の関与を確認した。オバマ大統領は「相応の対応をしていく」。
<http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation>

JANUARY 20TH, 2015 9PM ET

STATE OF THE UNION

SAY YOU'RE IN

the WHITE HOUSE PRESIDENT BARACK OBAMA

Contact Us ▶

Get Email Updates ▼



BRIEFING ROOM

ISSUES

THE ADMINISTRATION

PARTICIPATE

1600 PENN

Search



Foreign Policy

Cybersecurity

"America's economic prosperity, national security, and our individual liberties depend on our commitment to securing cyberspace and maintaining an open, interoperable, secure, and reliable Internet. Our critical infrastructure continues to be at risk from threats in cyberspace, and our economy is harmed by the theft of our intellectual property. Although the threats are serious and they constantly evolve, I believe that if we address them effectively, we can ensure that the Internet remains an engine for economic growth and a platform for the free exchange of ideas."

President Obama

Cybersecurity

Protect Critical Infrastructure

Improve Incident Reporting & Response

Engage Internationally

Secure Federal Networks

オバマ大統領、所信表明演説で サイバーセキュリティ対策を表明へ



- ▶ 多くは必ずしも目新しいものではない
 - ▶ federal data-breach notification law
 - ▶ リスクにさらされる人に告知する義務を定める。同時に搾取した事柄を海外に提供することを法律違反と明示
 - ▶ legislation giving companies legal protections
 - ▶ 企業が政府機関も含めて相互に情報を共有する、あるいはハッキングに遭遇した際の訴訟から、企業を保護する
- ▶ 「SPEに対する攻撃は、かつてない破壊的なもの。損失は何百万ドルにも上る。そんな状況から企業を守らなければ、経済が立ちゆかない」
- ▶ 企業団体であるthe Internet Security Allianceの代表は、「提案は素晴らしい」とする一方で、「実効あるものにするにはより多くのインセンティブが必要」と指摘

フランスの150万人デモ

