Secureworks が見た “グローバル”なサイバー攻撃

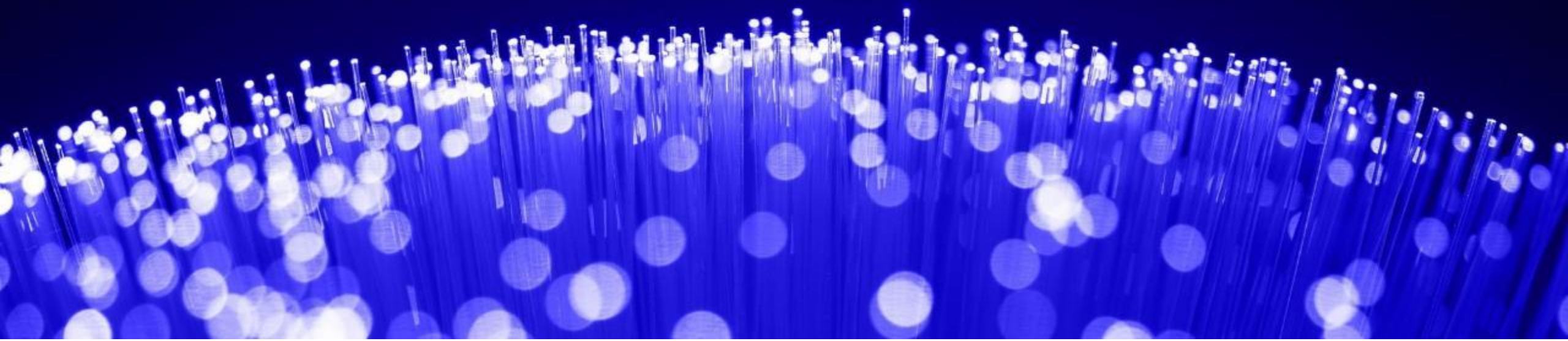
中津留 勇
Counter Threat Unit
SecureWorks Japan 株式会社

2017/11/28
Internet Week 2017
D1-1 サイバー攻撃最前線2017

Agenda

グロー バルから国内へ、その特徴的なインシデントを紹介

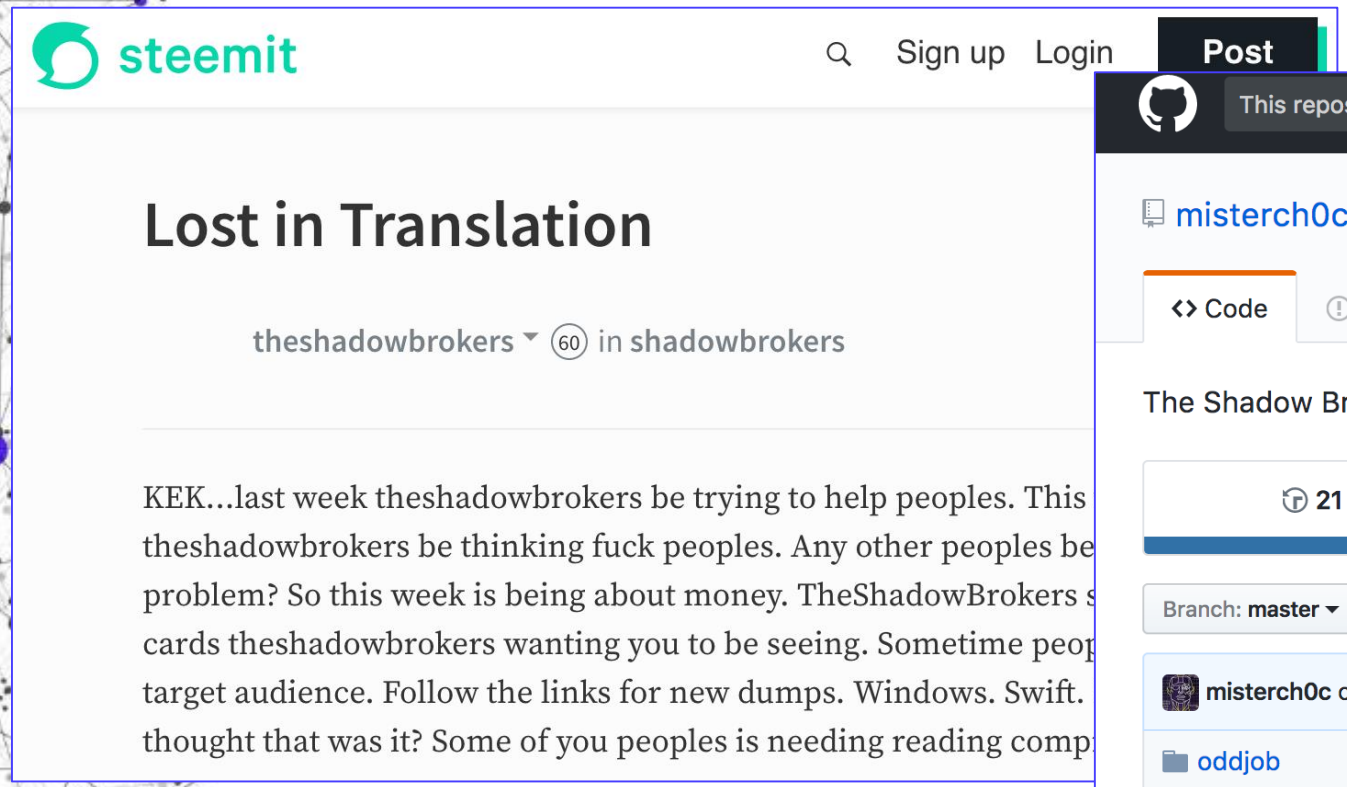
- Lost in Translation
- 例えば Struts を避ける
- この先生きのこるために



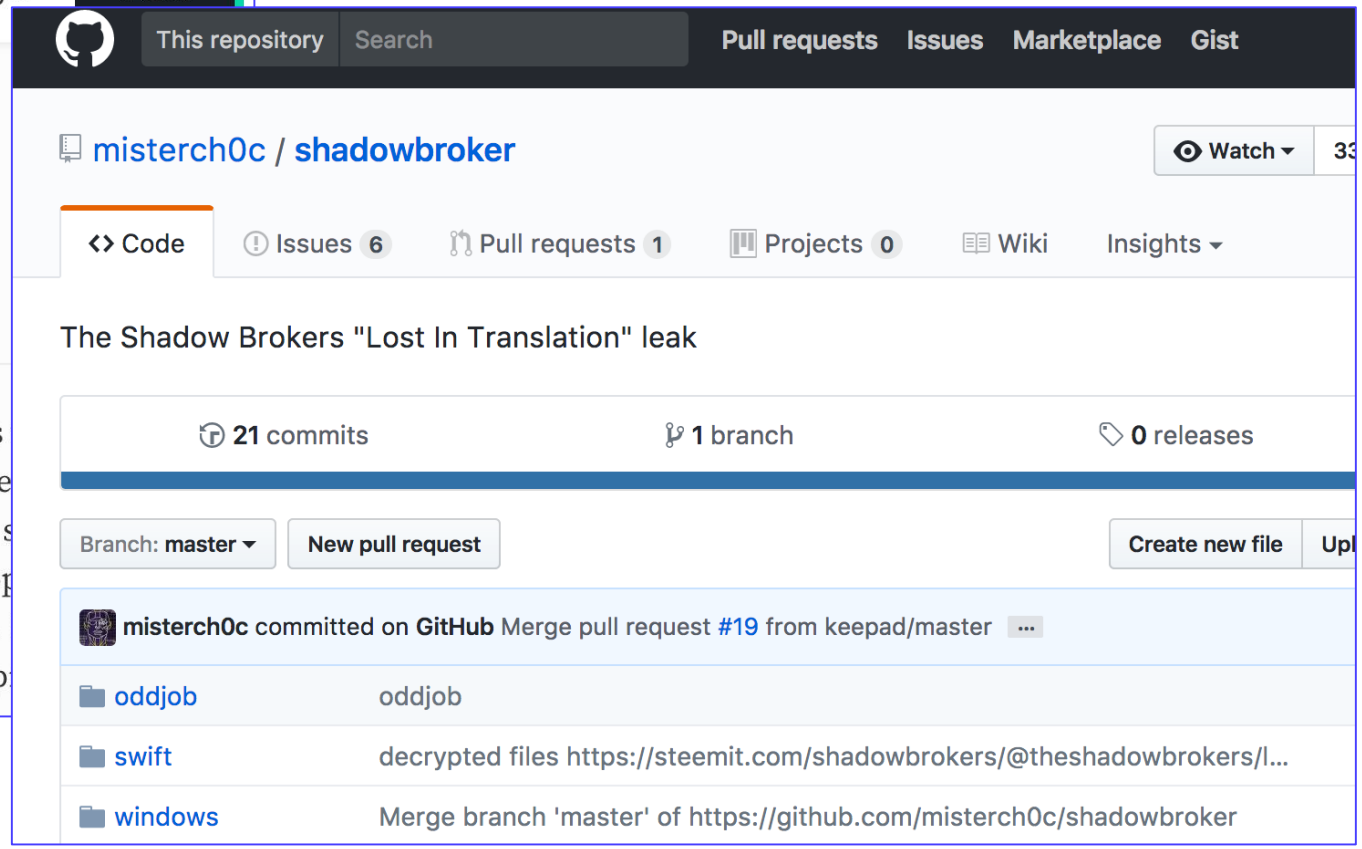
Secureworks

Lost in Translation

2017年4月に公開された、NSA関連ツール・情報群



https://steemit.com/shadowbrokers/@theshadowbrokers/lost-in-translation



https://github.com/misterchoc/shadowbroker

The Equation Group から盗み出された情報

TheShadowBrokers

- 2016年8月に The Equation Group の機密データを盗み出したとして、そのデータの公開・販売をはじめたハッカー集団
  - ロシアのグループであるという説も

The Equation Group

- カスペルスキー社が存在を明らかにした高度な標的型攻撃グループ
  - Stuxnet, Flame といったマルウェアを作成したグループ
- 活動の高度さから NSA (米国家安全保証局) またはその関連組織ではないかと考えられている
  - スノーデン氏と TheShadowBrokers それぞれ情報に共通性が見られる

Lost in Translation に含まれるもの

2017年4月に公開された、NSA 関連ツール・情報群

Windows

- Windows を標的とする攻撃ツール群
  - DoublePulsar/EternalBlue を含む

Swift

- SWIFT (Society for Worldwide Interbank Telecommunication) に関わる資料集
  - テキストや PowerPoint 資料など

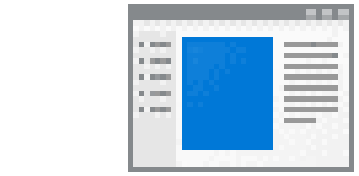
Oddjob

- Windows ベースの RAT (Remote Administration Tool)
  - Windows Server 2003 Enterprise から Windows XP Professional に対応

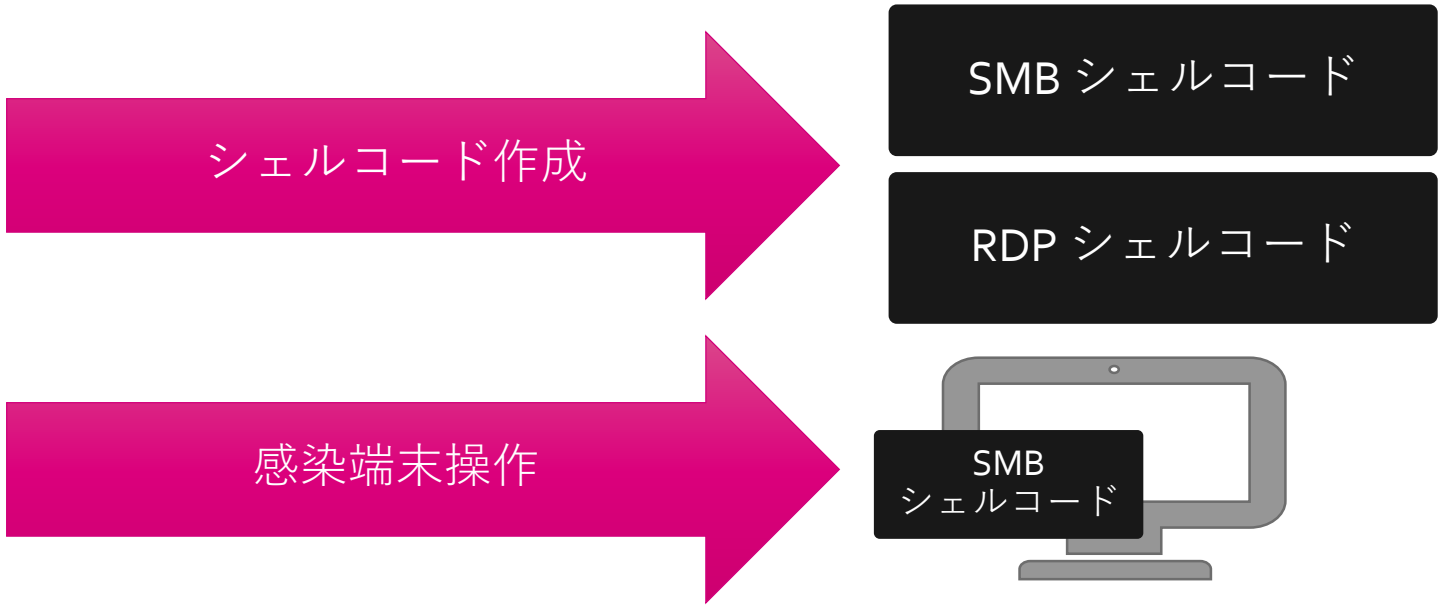
DoublePulsar

カーネルバックドア作成ツール兼コントローラ

- バックドアコードの作成と、その操作を行なうツール
  - SMB または RDP サービスを改ざんし、バックドアを埋め込む



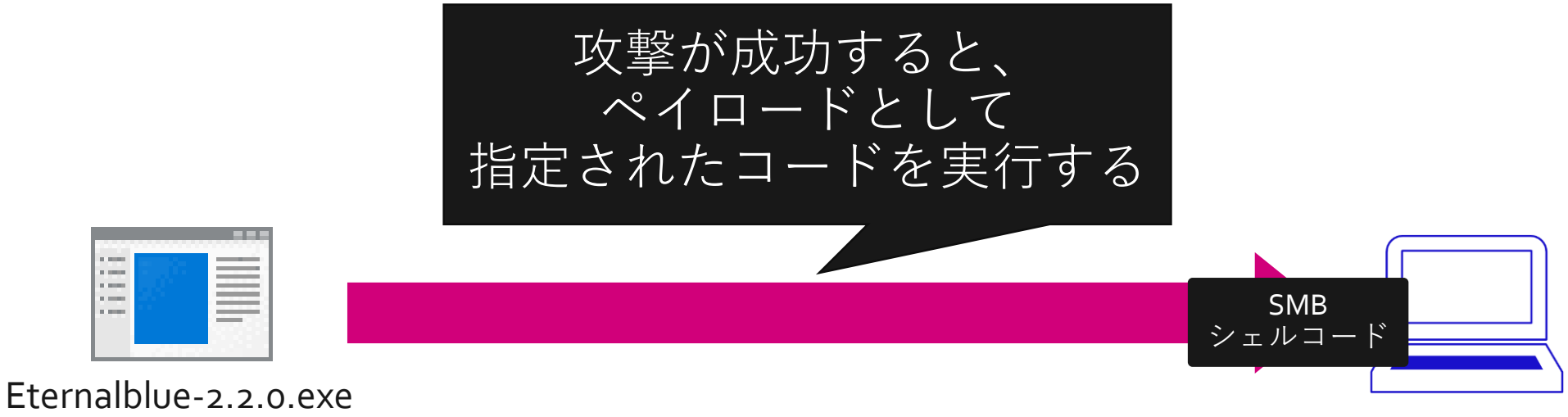
Doublepulsar-1.3.0.exe



EternalBlue

MS17-010 攻撃ツール

- 指定された IPアドレスに対し、MS17-010 の脆弱性を突く攻撃を行う
  - そのペイロードとして、デフォルトでは Doublepulsar (SMBモジュール) を使用する



その他のツール

攻撃ツールや情報収集ツールなど 50種ほどのツールが存在

- FuzzBuzz を使うことで Metasploit 感覚で使うことが可能

```
fb > use
Architouch              Englishmansdentist  Iistouch            Regwrite
Darkpulsar              Erraticgopher       Jobadd              Rpcproxy
Domaintouch             Erraticgophertouch  Jobdelete           Rpctouch
Doublepulsar            Eskimoroll          Joblist             Smbdelete
Easybee                 Esteemaudit         Mofconfig           Smblist
Easypi                  Esteemauditttouch   Namedpipetouch      Smbread
Eclipsedwing            Eternalblue         Pcdlllauncher       Smbtouch
Eclipsedwingtouch       Eternalchampion     Printjobdelete      Smbwrite
Educatedscholar         Eternalromance      Printjoblist        Webadmintouch
Educatedscholartouch    Eternalsynergy      Processlist         Worldclienttouch
Emeraldthread           Ewokfrenzy          Regdelete           Zippybeer
Emeraldthreadtouch      Explodingcan        Regenum
Emphasismine            Explodingcantouch   Regread
```

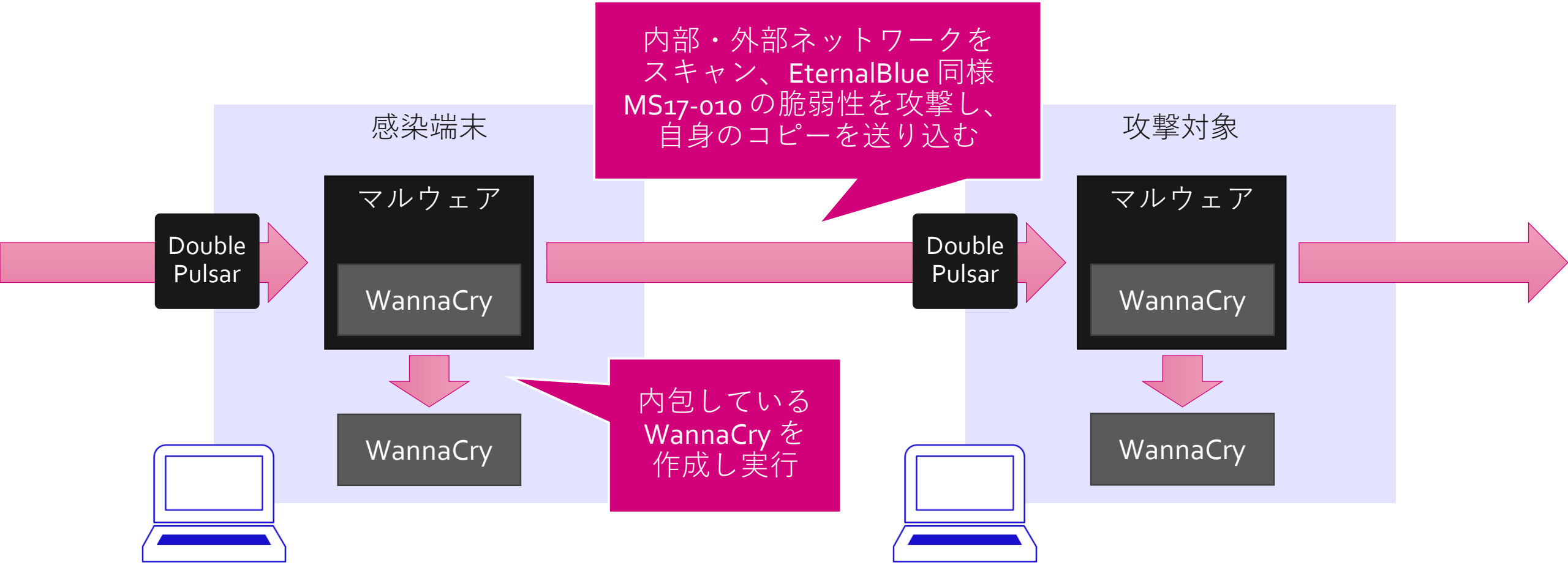
Lost in Translation の悪用事例

WannaCry だけでなく多数のインシデントが発生

- WannaCry の大規模感染、亜種の出現
- ランサムウェア Uiwix の出現
- DoublePulser 経由で仮想通貨マイニングマルウェアや RAT に感染
- 複数のツールを悪用する EternalRocks の出現
- ランサムウェア NotPetya の出現
- ランサムウェア BadRabbit の出現

WannaCry の悪用例

WannaCry 自身の機能ではなく、ドロッパーの機能



Secureworks

WannaCry の変化

バグ修正などされた複数のバージョンが存在

- 過去メールで拡散されていたバージョン（1.0）
- MS17-010 を悪用し感染を拡大するバージョン（2.0）
- ビットコイン処理のバグを修正したバージョン
- キルスイッチおよび暗号化機能を無効化されたバージョン

WannaCry の被害

暗号化だけではなく、ネットワーク障害になる場合も

関連が疑われる事例

日本国内で被害が確認された等と報じられている事例は次の通り。 *23 *24 *25

対象	発生・把握日	発生事象
JR東日本 高崎支社	5月12日頃	関東地方支社でインターネット閲覧に使用しているPC1台が感染。 PCは社内イントラネットには接続されておらず、運行等業務への影響はない。*26 インターネット閲覧中に感染を示す画像が表示された。メール機能はこの端末には存在しない。*27 15日に警察へ被害の相談。*28
近鉄エクスプレス	5月12日以降	東京都内事業所にある37台の端末が感染。感染した端末は社内ネットワークには接続されていなかった。*29
滋賀県内の個人(50代男性)	5月12日夕	自営業男性の端末1台が感染。600ドルを要求する画面が表示されていた。 インターネット閲覧中に感染を示す画像が表示。 15日に報道で被害に気づき、翌日に交番に相談。 滋賀県内で把握された2例目。*30
滋賀県内の個人(50代男性)	5月12日16時頃	オークションサイト利用後席を外し、30分後に戻ったところ感染を示す画像が表示されていた。 ウイルス対策ソフトは更新していなかった。 16日に甲賀署署員に相談。 OSはWindows 7。*31
愛知県内のコンビニ	5月12日	防犯カメラの管理端末1台が感染。インターネットには接続されていたがメールやウェブサイトの閲覧は行っていなかった。*32カメラ認されていない。*33
日立金属	12日夜	メールの送受信や添付ファイルが開けなくなるなどの障害が発生。*34
日立製作所	5月12日深夜	ランサムウェアによる被害および復旧状況について メール管理システムの一部で障害発生を確認。メールの送受信や添付ファイルの開封が出来ない事態。 海外のグループ会社でも12日から同様の障害が確認されている。*35 その後感染が多発しているランサムウェアと同じであることが確認された。*36 サーバーを切り離す等して一部は復旧している。*37また一部は電話やFAXの利用に業務を切り替えている。*38

http://d.hatena.ne.jp/Kango/20170513/1494700355

ランサムウェア以外のマルウェア

金銭目的だけでなく、研究目的のようなものも存在

仮想通貨マイニング Adylkuzz, Coinminer

- Monero コインのマイニング

ForShare RAT

- ダウンローダによって外部からダウンロードされる
- GUI で感染端末を遠隔操作可能

EternalRocks

- Lost in Translation に含まれる 7つのツールを使う、SMB 経由で感染を広げるワーム
- 暗号化機能などはない

NotPetya, BadRabbit

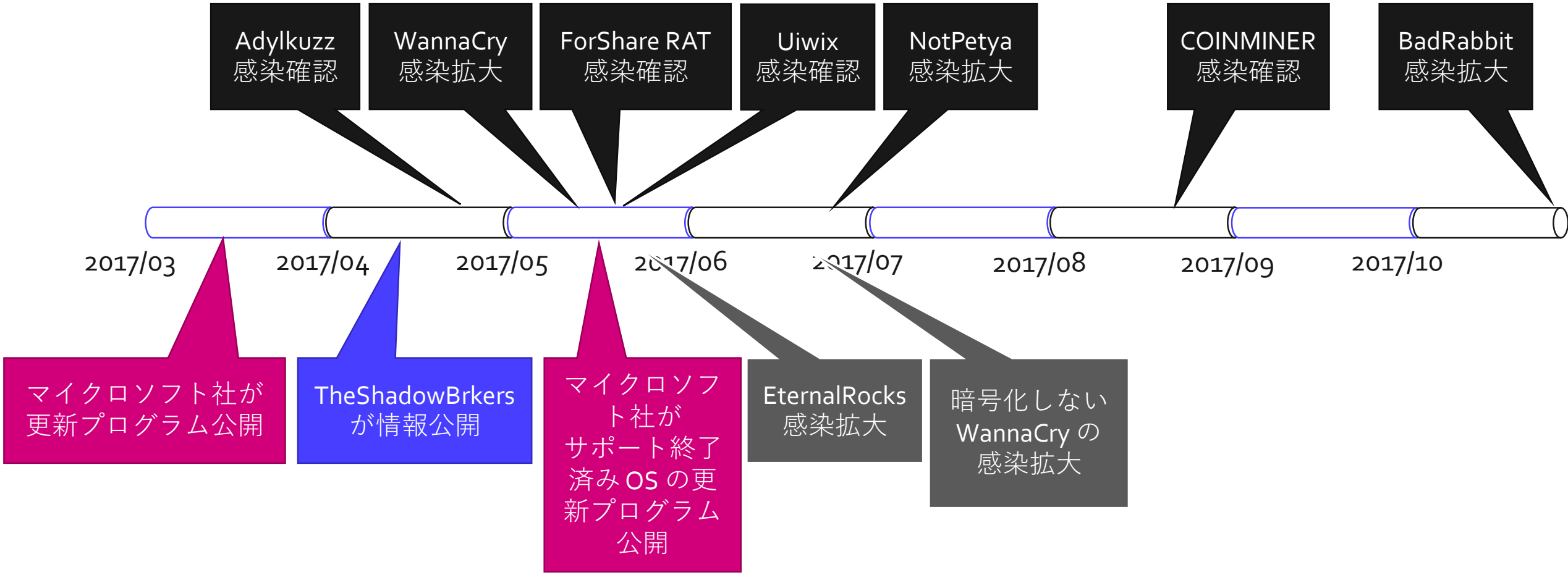
ネットワーク感染能力が強いランサムウェア

- Lost in Translation のツールだけでなく、パスワードクラックなど様々な方法を用いて感染しようとする

EternalBlue (MS17-010)	EternalRomance (MS17-010)	Mimikatz による認証情報窃取
PsExec によるファイル実行	WMI によるファイル実行	辞書攻撃によるパスワードクラック

悪用のタイムライン

パッチ適用や機能無効化までの時間はそれなりにあった



Secureworks

例えば、Struts を避ける

Secureworks

2017年に公表された脆弱性

致命的な Remote Code Execution を含む

脆弱性番号	脆弱性概要
S2-045	任意のコードを実行される脆弱性
S2-046	Jakarta Multipart パーサに関する脆弱性(S2-045と同様)
S2-047	サービス運用妨害 (DoS) の脆弱性
S2-048	任意のコードを実行される脆弱性
S2-049	サービス運用妨害 (DoS) の脆弱性
S2-050	サービス運用妨害 (DoS) の脆弱性
S2-051	サービス運用妨害 (DoS) の脆弱性
S2-052	任意のコードを実行される脆弱性
S2-053	任意のコードを実行される脆弱性

Struts2 の脆弱性への攻撃

2017年3月、Struts2の脆弱性 CVE-2017-5638 (S2-045)を悪用される事例が多発

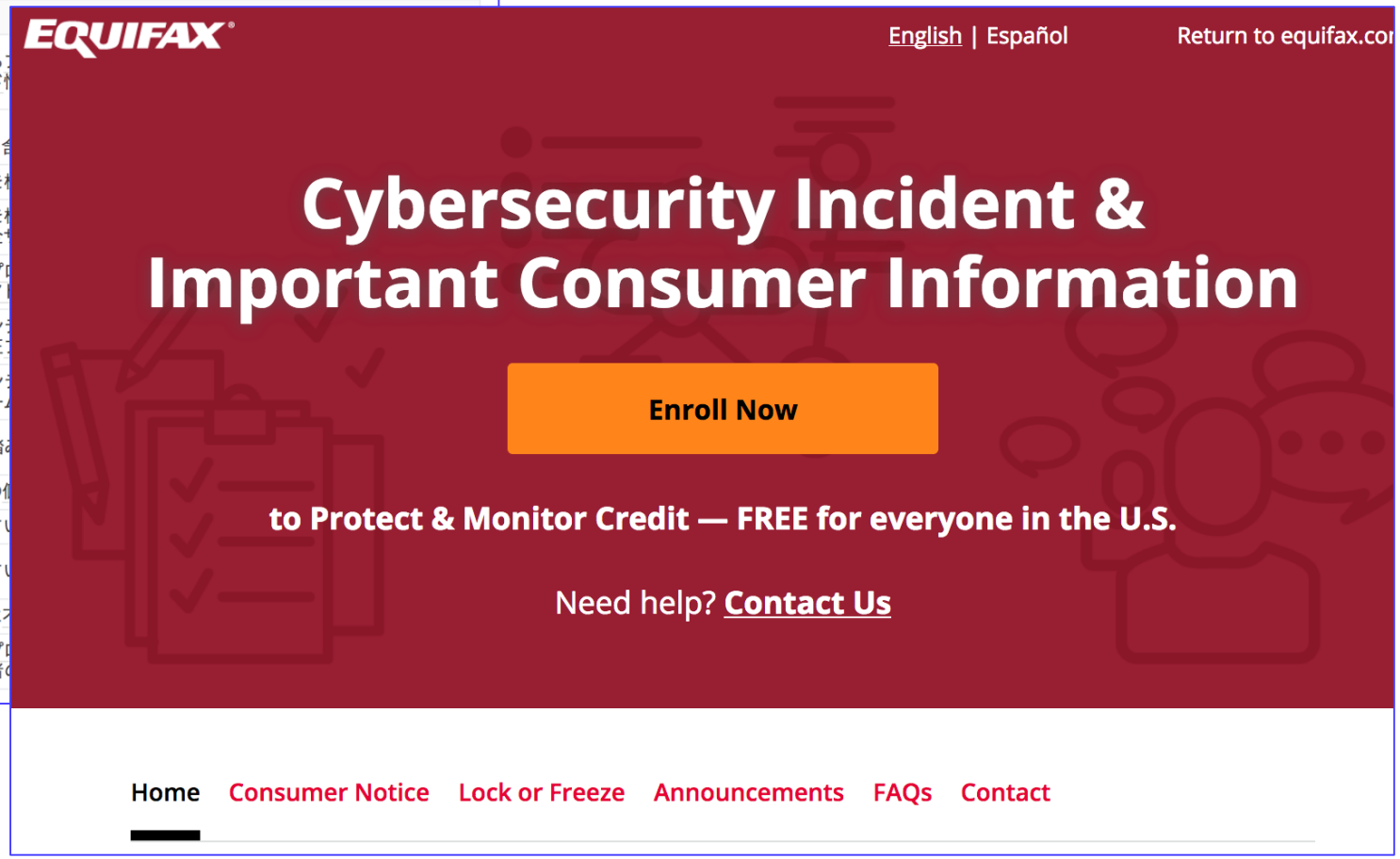
被害状況の概要

攻撃を受けたサイトやその被害概要をまとめると次の通り。

運営元	攻撃を受けたサイト	
トヨタファイナンス GMOペイメントゲートウェイ	都税クレジットカードお支払いサイト(旧) ⇒新しいドメインへ移転 機構団体信用生命保険特約料クレジットカード支払いサイト	サイトに悪意ある クレジットカード
JETRO	相談利用者登録ページ	一部情報の削除。 メールアドレスを
科学技術振興機構	科学技術情報発信・流通総合システム(J-STAGE)	外部からの攻撃を
工業所有権情報・研修館	特許情報プラットフォーム(J-PlatPat)	外部からの攻撃を 緊急措置として全
日本郵便	国際郵便マイページサービス	サイトに不正なプ 送り状やメールア
沖縄電力	停電情報公開サービス	Webサイトのコン 情報漏えいや不正
ニッポン放送	Radital	Webサイトのコン 会員情報やフォー
岡山県 県内12市町	おかやまオープンデータカタログ	外部への攻撃の踏
ジェイアイエヌ	JINSオンラインショップ	ショップサイトの
総務省	地図による小地域分析(jSTAT MAP)	利用時に登録して
ぴあ	B.LEAGUE チケットサイト B.LEAGUE ファンクラブ受付サイト	利用時に登録して
情報通信研究機構	「MCML音声インタラクションSDK」外部研究者向け提供サーバー	サーバー停止前に
国土交通省	土地総合情報システム 不動産取引価格アンケート回答（電子回答）	サイトに不正なプ アンケート回答者

http://d.hatena.ne.jp/Kango/20170311/1489253880

https://www.equifaxsecurity2017.com/



Secureworks

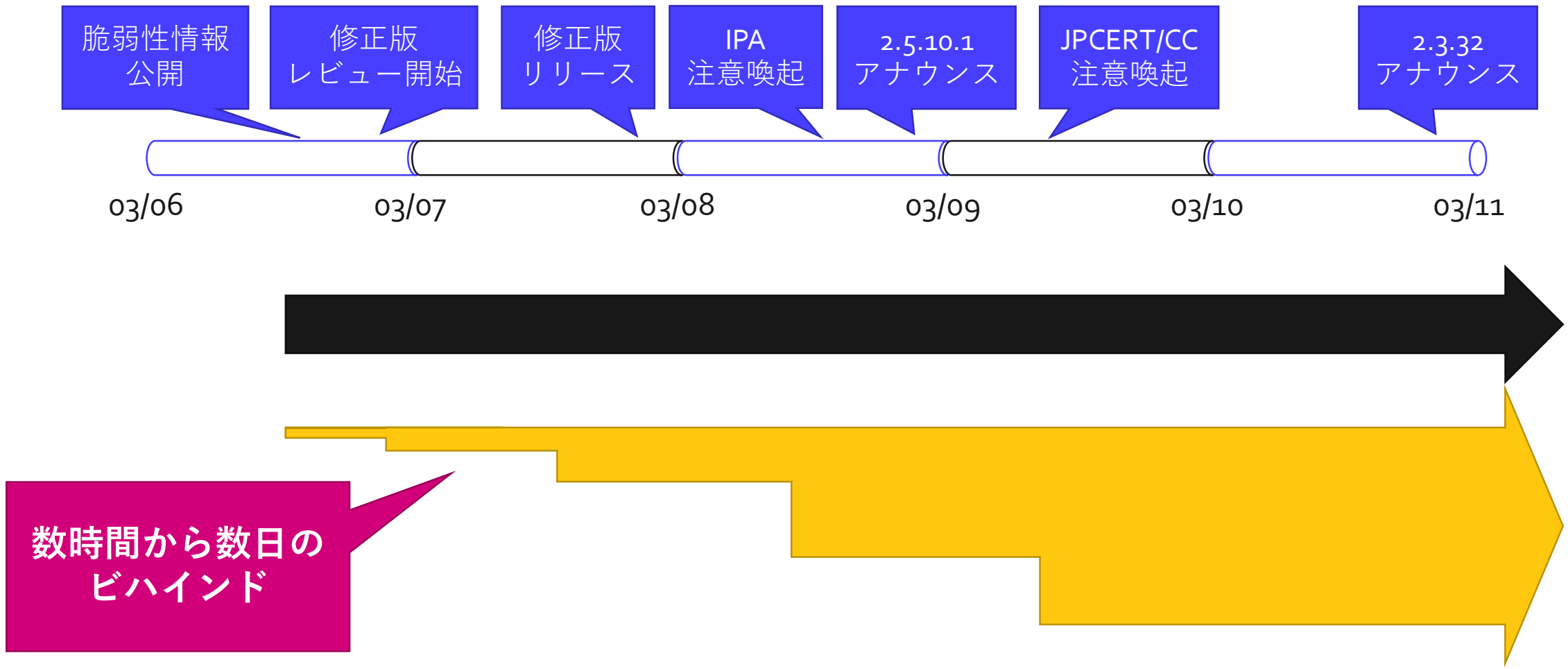
S2-045/S2-046 のタイムライン

対応に多くの問題点が窺える

日時	イベント	関連 URL
2017-03-06 18:54 JST	S2-045 のアドバイザリが公開される	https://cwiki.apache.org/confluence/display/WW/S2-045
2017-03-06 21:07 JST	修正版の test build が公開され、レビュー・投票が開始される	https://twitter.com/TheApacheStruts/status/838722669726031873, https://twitter.com/TheApacheStruts/status/838722824621674496
2017-03-07 21:03 JST	修正版がリリースされる	https://dist.apache.org/repos/dist/release/struts/2.5.10.1/, https://dist.apache.org/repos/dist/release/struts/2.3.32/
2017-03-08 00:15 JST	NTTセキュリティ・ジャパン株式会社が攻撃情報についてツイート	https://twitter.com/NTTSec_JP/status/839132398210031616
2017-03-08 21:24 JST	修正版 2.5.10.1 がメーリングリストでアナウンスされる	http://markmail.org/thread/fc5c2b7wfl6u33an
2017-03-10 21:24 JST	修正版 2.3.32 がメーリングリストでアナウンスされる	http://markmail.org/thread/b5bjmguga6mlz5ji
2017-03-19 15:54 JST	S2-046 のアドバイザリが公開される	https://cwiki.apache.org/confluence/display/WW/S2-046

攻撃者と国内ユーザの置かれた状況

攻撃者が圧倒的に有利だった3月



Secureworks

S2-052/S2-053 のタイムライン

S2-045 での反省は活かせたのか

日時	イベント	関連 URL
2017-09-05 18:16 JST	修正版 2.5.13 がリリースされる	https://dist.apache.org/repos/dist/release/struts/2.5.13/
2017-09-05 19:04 JST	S2-052 のアドバイザリが公開される	https://cwiki.apache.org/confluence/display/WW/S2-052
2017-09-05 23:17 JST	修正版 2.5.13 がメーリングリストでアナウンスされる	http://markmail.org/message/5ydeachhj2btlglw
2017-09-06 03:28 JST	修正版 2.3.34 test build が公開され、レビュー・投票が開始される	http://markmail.org/message/5xuhb2vwc7iagjjr
2017-09-06 16:52 JST	NTTセキュリティ・ジャパン株式会社が攻撃情報についてツイート	https://twitter.com/NTTSec_JP/status/905338023214161920
2017-09-07 04:36 JST	修正版 2.3.34 がリリースされる	https://dist.apache.org/repos/dist/release/struts/2.3.34/
2017-09-07 18:24 JST	修正版 2.3.34 がメーリングリストでアナウンスされる	http://markmail.org/message/ostesyu7jgfibzng
2017-09-08 15:08 JST	S2-053 のアドバイザリが公開される	https://cwiki.apache.org/confluence/display/WW/S2-053

Java の Web アプリケーションフレームワーク

自社制フレームワークのベース変更や、新規開発で Struts を排除する動きも出てきている

- Apache Struts
- Spring Framework
- JavaServer Faces (JFS)
- SAStruts
- Play Framework
- Apache Wicket
- Apache Tapestry

この先生きのこるために

Secureworks

考えなければならないこと

グローバルな時代、ワンデイな時代の生き方

海外で公開された脆弱性がすぐに悪用される

- 自分が気付くよりも
- パッチを適用するよりも先に
  - そもそも地方・海外拠点など適用したかどうか分からないケースも

関係ないはない

- 海外の、国レベルの話であっても
- 使っていないと思ってもどこかで使われていたケース

この先生きのこるために

そもそも信頼して良いのか

- アプリケーションの思想
- 過去見つかった脆弱性・その頻度、世の中の評価

それに頼らなくて済むように

- 脆弱性が出ても防げる
  - 検知・遮断する、あらかじめ機能を無効化しておく
  - 止める勇気
- 脆弱性が悪用されても被害を局所化できる
- 単体ではなく全体で考える
  - 組織体制
  - 開発から運用・保守まで