セキュリティ動静マップ 2017年まとめ

セキュリティ動静共有プロジェクト
リーダー：佳山こうせつ(富士通株式会社)
サブリーダー：小宮山功一朗(JPCERT/CC)
サブリーダー：小野和紀

このドキュメントは公開情報から集めたものであり、メンバーの所属する組織を代表する意見ではありません。
このようなボランティアベースの活動による情報の共有が、前向きなセキュリティの活性化につながってくれれば嬉しいです。

グローバル動静マップの目的

グローバルの動静情報を地図にマッピングすることで、
点と点をつなげ関係性を可視化し、単体では見えない
本質的なナニカを洗い出す。

喉元過ぎ去った情報をしっかり次に繋げるために、
一目でわかる情報共有手段を模索する。

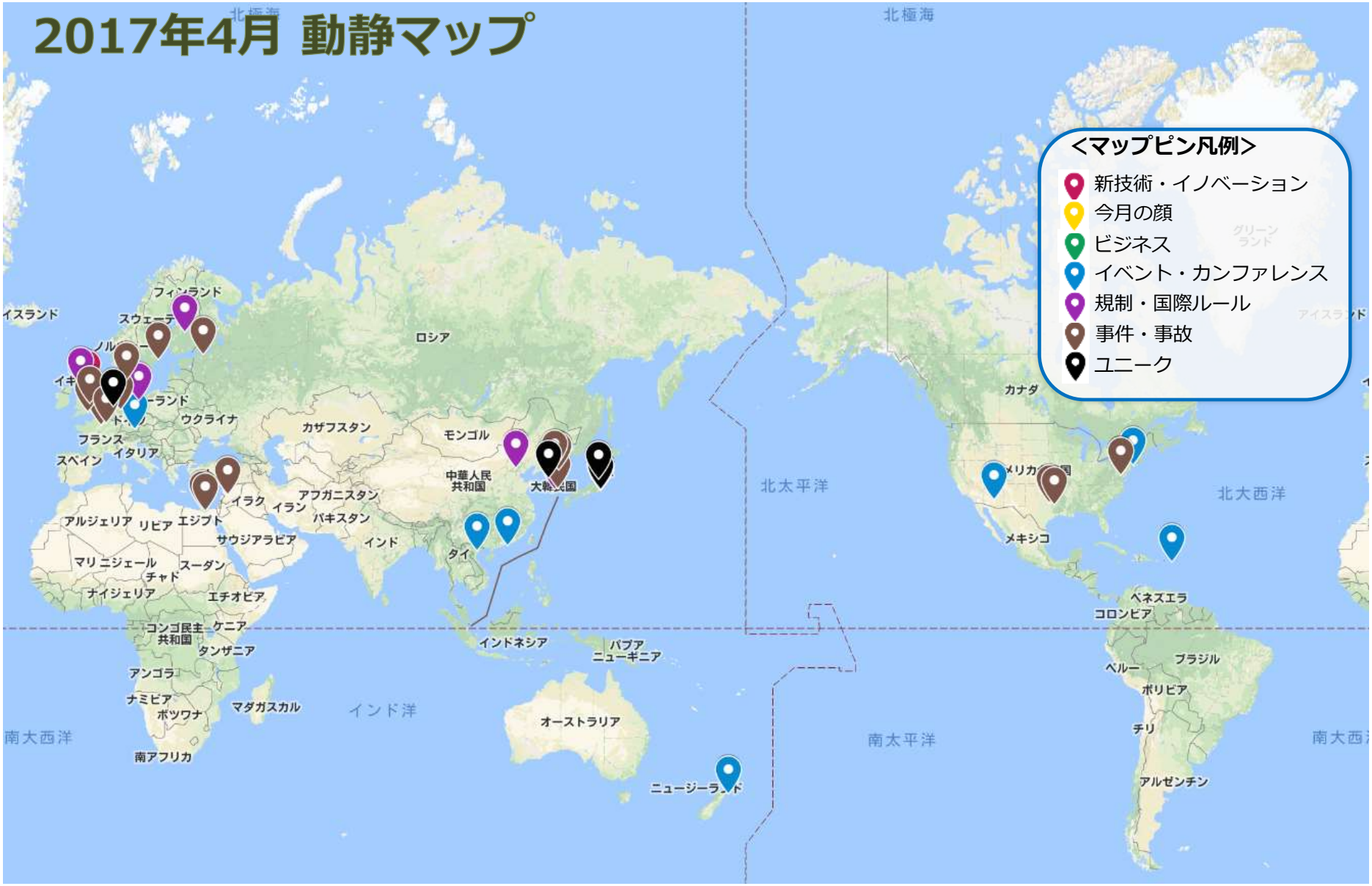
動静マップまとめ

動静マップをもとに2017年4月～12月のまとめを行う。

次の3点が軸。

- 大きな話題（点）
- 特徴的なリージョンと動静（点と点）
- アナリストコメント（本質的なナニカ）

2017年4月 動静マップ



2017年4月 動静マップ

- 大きな話題（点）

  フランス大統領選の第1回投票が、歴史的な選挙戦の末、無所属のマクロン氏と極右政党「国民戦線」党首ルペン氏の決選投票。それに乗じサイバー攻撃で選挙を妨害するという動きの報道。一方、中国ではサイバーセキュリティ法案が可決。

- 特徴的なリージョンと動静（点と点）

  地政学的な歪みがサイバーセキュリティの分野でも顕在化し、EU圏を中心とした動静がたくさん届いた。そんな中、中国では重要な法案が議論されていたがあまり日本では大きな話題にならなかった。

- アナリストコメント（本質的なナニカ）

  キー：欧米

  ドイツでは、ソーシャルメディアの運営業者などにフェイクニュース（偽記事）やヘイトスピーチ（憎悪表現）の速やかな消去を義務付け、違反した場合には法人に最大5千万ユーロ（約59億円）を科す法案が閣議決定された。フェイスブックやツイッターなどの運営者に対し、実質的な対策義務化となる。関連ビジネスを行う企業は、今後他国の動向を含めウォッチする必要性が加速した。これらもフランス大統領選挙で顕在化された動きに関連するもので、EU圏の動きは、各国で起きている話題とつながる。

  一方で、アジアでもそれら大きな話題に負けず劣らず中国での大きな法案可決もあり、日本でも大局観を見た青写真を描く陣頭指揮が求められる。

  ３月はインドやアフリカのニュースが多かったが、欧米で大きな話題が起きるとそれらリージョンの話題が入ってこなくなることも見えてきた。

2017年4月 話題一覧

	カテゴリ	話題
	新技術・イノベーション	スマホの傾きでパスワードを盗まれる危険性
		米国空軍、バグ報奨プログラム開始
	今月の顔	-
	ビジネス	改正資金決済法（仮想通貨法）施行
		Symantec Japan執行役員社長に波立行智（はりゅう ゆきのり）氏が就任
		JAL、羽田ーニューヨーク線が復活　1日1往復で運航
	イベント・カンファレンス	Kaspersky Security Analyst Summit
		APWG ecrime 2017
		VXCon2017
		故金日成（キムイルソン）国家主席生誕１０５周年
✓		第1回投票(2017年フランス大統領選挙)
		ニュージーランドでNational CSIRT （CERT NZ)が設立！
		【報告】2017 IBM X-Force Threat Intelligence Index
		【報告】F-Secure ランサム歴史まとめ
	規制・国際ルール	英・米、トルコ・中東・北アフリカからのラップトップなどの機内持ち込みを禁止
✓		独、ＩＴ大手に最大罰金59億円　偽記事対策
		韓国軍、サイバー防衛強化に５年で約２３６億円投入

2017年4月 話題一覧

カテゴリ		話題
規制・国際ルール	✓	中、サイバーセキュリティ法案、企業の海外データ送信審査へ
		盗聴の危険性ある人形(My Friend Cayla) 破棄をしない場合に25,000 euroの罰金
		米・英・EU諸国・NATO諸国が、サイバー攻撃対応センター設置に合意
事件・事故		北朝鮮が飛翔体を発射
		深夜に緊急サイレン鳴り響く--ダラス市の警報システムにハッキング
		深夜に緊急サイレンの真相と教訓
		露サンクトペテルブルク地下鉄で爆破テロ
		米韓軍の最高機密軍事作戦が流出か？
		米、シリア空軍基地をミサイル攻撃 化学兵器使用に報復
		ストックホルム中央駅近くのデパートにトラック突入。テロ。
		爆弾テロ：エジプト北部のアレクサンドリアおよびタンタの2都市
		原子力空母「カール・ビンソン」朝鮮半島近海へ移動開始
		独ドルトムント：プロサッカーチームを狙った爆発テロ
		弾道ミサイル発射直後に爆発
		パリ中心部：自動小銃で警官銃撃
	✓	英国民投票でサイバー攻撃　「中露が関与の疑い」と下院委員会報告書
		インターコンチネンタルホテルグループ(IHG)、クレカ情報漏えい
	✓	露政府寄りハッカー集団、仏大統領選候補を攻撃

2017年4月 話題一覧

カテゴリ	ニュース
事件・事故	北朝鮮 軍創設以来 最大規模の攻撃訓練
	✓デンマーク防衛大臣、ロシアからのサイバー攻撃を受けた事実語る
	Northrop Grumman不正アクセスを受け従業員情報が漏えい。同社はステルス爆撃機など米軍の主要兵器を開発／製造。
ユニーク	APCERT Annual Report 2016
	ワールドプレス騒動w
	オランダ警察はカスペルスキーとフレンズ
	北朝鮮ミサイル発射失敗は、米サイバー攻撃？

2017年5月 動静マップ

2017年5月 動静マップ

- 大きな話題（点）
  5/7にフランス大統領選、5/9に韓国大統領選と立て続けに大きな国政選挙が行われた。また5/12頃より身代金を要求するランサムウェア「WannaCry」の被害が世界各地で発生。

- 特徴的なリージョンと動静（点と点）
  アメリカが韓国にTHAAD配置など、米中韓の関係に緊張が走り、北朝鮮は5月にミサイルを何度も撃つなど日本周辺のアジア圏の軍事バランスが崩壊しそうな気配を見せる。WannaCryについても世界各国を巻き込んだ事態となった。一方、国内のワイドショーでは森友加計問題など偏った話題のみにフォーカスされていた。

- アナリストコメント（本質的なナニカ）
  ランサムウェア被害は見た目にも画面に変化があるなど、メディアに取りあげられやすい。一部の店舗の表示用パソコンが感染するなど、影響度の低い事案についても大々的に報じられ、過熱報道や誤報などが逆にパニックをもたらした。セキュリティに携わる者たちが正しい情報を提供し、その影響度合いをコンピュータに対する影響度ではなく社会に対する影響度として正しく判断する基準づくりの必要性が改めて顕在化した。

キー：WannaCry、過熱パニック

2017年5月 話題一覧

カテゴリ	話題
新技術・イノベーション ✓	日経ビジネス報道「謎のAI半導体メーカー」が話題に（5月22日）
今月の顔	秋篠宮眞子さまが結婚へ、大学時代の同級生と（5月16日）
	【訃報】与謝野馨氏が死去、享年78歳（5月24日）
ビジネス	東芝が暫定決算発表、最終赤字9,500億円、債務超過5,400億円（5月15日）
	ヤマハがJASRAC提訴、音楽教室での著作権料徴収めぐり（5月16日）
	ソフトバンクが10兆円ファンド設立（5月下旬）
	【東京五輪】小池都知事が東京都以外の整備費用について都の全額負担を明言（5月11日）
イベント・カンファレンス	OWASP AppSec EU 5/8-
	Afrinic(Kenya) 5/29-
	IFIP SEC Roma 5/29-
	THOT CON 5/4-

2017年5月 話題一覧

カテゴリ		話題
規制・国際ルール	✓	自衛隊、安保法初任務、海上自衛隊が米艦防護のため出航、朝鮮半島情勢を受け（5月1日）
		安倍首相が2020年度の憲法改正を明言、憲法9条に自衛隊を明記する加憲の方針示す（5月3日）
		プエルトリコが破産法申請、債務8兆円、米国自治体としては過去最大（5月4日）
		民法債権規定を120年ぶり改定へ、賃貸契約での敷金返還義務、修繕費負担を禁じる内容を明文（5月26日）
		国連報告者が日本の特定秘密保護法の改正勧告、メディアの独立性に懸念（5月31日）
事件・事故	✓	世界各地で同時多発サイバー攻撃、世界150ヵ国で20万件の被害（5月13日）→週明け日本でも被害が（5月15日）→北朝鮮のハッカー集団が関わった疑い（5月23日）
	✓	北朝鮮が弾道ミサイル発射、高度2,000km級、約30分飛行し着水（5月14日）
		北朝鮮が中距離弾道ミサイル発射、北朝鮮国営通信は成功協調（5月21日）
		アリアナ・グランテのコンサート会場でテロ、22人死亡、59人けが（5月23日）
		金塊密輸の疑いで韓国人4人を再逮捕、4月の現金持ち出し騒動で逮捕されたグループ（5月24日）
		築地市場の土壌調査、豊洲に続き基準値上回る有害物質検出（5月25日）
		北朝鮮が短距離ミサイル発射、日本EEZ内に着水、日本政府は抗議（5月29日）
ユニーク	✓	スナック菓子「カール」が販売縮小、東日本からは完全撤退、西日本でも2種類以外廃止へ（5月25日）
		宮崎駿が引退撤回、4年ぶり数度目（5月19日）
		文科省・前川前次官が記者会見、「総理のご意向」文書について本物と主張、ガールズバー通いは「貧困女性の調査のため」と説明（5月25日）

2017年6月 動静マップ

2017年6月 動静マップ

- 大きな話題（点）

  6月末に欧州各国にてNotPetyaによるランサムウェアの感染被害が確認された。
  ※小さなセキュリティインシデントが散見した。

- 特徴的なリージョンと動静（点と点）

  5月のWannaCryによる喧騒からはうって変わり、月初から中旬にかけては世界的に大きな事件は報告されていなかった。月末の6月27日頃から欧州各国でNotPetyaによる攻撃検知が見られた月であった。

キー：台風一過

- アナリストコメント（本質的なナニカ）

  6月は何といっても月末に舞い込んできたNotPetyaの被害発生である。ただウクライナ、ロシアなどの欧州各国での被害は見られるものの、日本での感染は報道など外に出てくるものとしては確認されていない。日本国内では5月に発生したWannaCryに比べると全体的に落ち着いた、事象を静観する形の対応になったと思われる。これはWannaCryの際の過熱報道によって右往左往した経験が冷静な判断を促したのでは無いかと考えられる。
  「Oni」という日本をターゲットにしたマルウェアが出現するなど攻撃者はターゲットを明確において攻撃を仕掛けてきているということが改めて感じられた。

2017年6月 話題一覧

カテゴリ	話題
新技術・イノベーション	日本版GPS衛星みちびき打ち上げ成功
	豊島区役所、自前でマルウェア解析ができる対策システムを構築
	Yahoo! Japan「kukai」を開発
今月の顔	James B. Comey 前FBI長官の上院公聴会
	コール元首相死去
ビジネス	ソフトバンク、Boston Dynamicsを子会社化
	NYC10ヶ年計画： will invest heavily in technology, particularly cybersecurity (30,000 jobs) etc.
	Amazonが高級スーパーのWhole Foodsを137億ドルで買収
	ソフトバンク、Cyberreasonに1億USD追加出資
	Microsoft社は中国版のWindows10を公表
イベント・カンファレンス	FIRST Annual Conference
	Apple WWDC 2017
	RECON2017
	Interop 2017
	Google主催CTF開催(20170617-18)、予選の上位10チームは秘密の会場に招待され賞金を巡って争う
規制・国際ルール	中、新サイバーセキュリティ法導入、企業にデータ監視と国内保管求める
	EUがGoogleに制裁金3000億円　独占禁止法違反で過去最高額

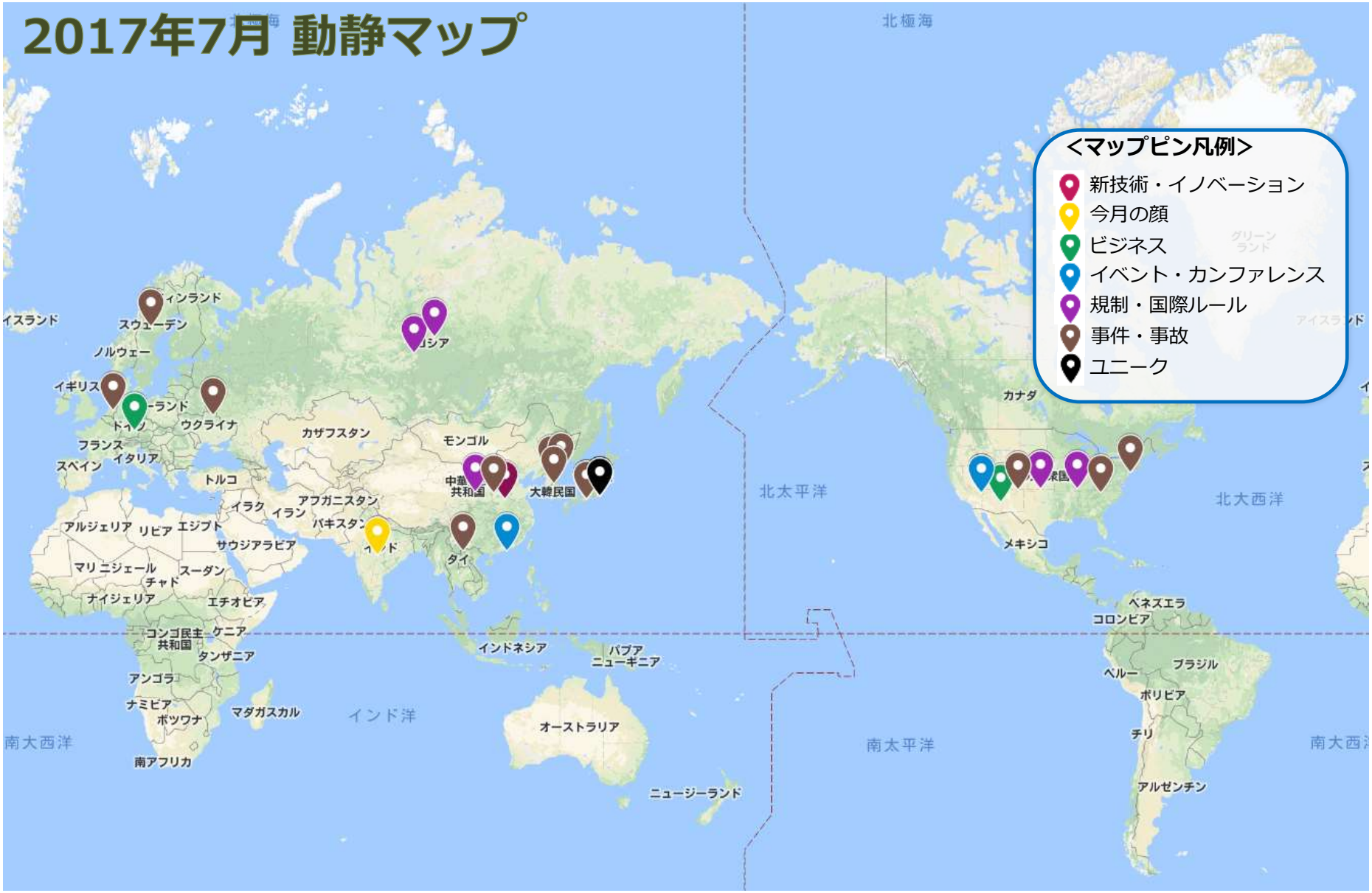
2017年6月 話題一覧

カテゴリ	話題
事件・事故	Skytrak Travel情報漏洩
	ウクライナとフランスをターゲットにしたPetyaの活動が盛んに
	TrendMicro 警察を偽装したネット詐欺を国内で新たに確認
	外務大臣のTwitterアカウントが乗っ取られる
	中国発のFireballマルウェアが2億5000万台に感染
	ロンドンでテロ ISが犯行声明
	国交省：「土地総合情報システム」における不正アクセスおよび情報流出の可能性について
	テヘラン 国会議事堂とイマーム・ホメイニ廟が襲撃 12人死亡
	浙江省蒼南県でApple従業員ら２２人拘束　窃取ＩＤ売却
	British Parliament hit by cyber attack
	約２億人分の米国有権者の個人情報へアクセス可能な状態に
	報道機関アルジャジーラが、ハッキング攻撃を組織的かつ継続的に受けていることを明かす
	ブリトニー・スピアーズの公式Instagramページに水飲み場攻撃が仕掛けられた
	シリア国内全域でインターネット障害、5時間以上に渡り通信できない状況となった
	米国機密データ約28GBが、AWSで公開状態で格納されているのが発見された

2017年6月 話題一覧

カテゴリ		話題
事件・事故		国内からの 22/TCP ポートへのアクセスの増加
	✓	ランサムウェア「Oni」出現、日本が標的の可能性
		ニュース - カブドットコム証券にDDoS攻撃、検知から約38分後にブロック
		ロシアで大規模反政権デモ　野党指導者ナワリヌイ氏は30日間拘束に
	✓	ホンダ、狭山工場の操業を一時停止　サイバー攻撃で
ユニーク		サウジアラビア、バーレーン、アラブ首長国連邦（ＵＡＥ）、エジプトの中東４カ国は５日、ペルシャ湾岸のカタールと国交を断絶するとの声明を発表
		天安門事件28年

2017年7月 動静マップ



2017年7月 動静マップ

- 大きな話題（点）

  7月22日～31日　ラスベガスでBlackHat/DEF CONが開催される。カンファレンスで、数々の新しい攻撃手法の詳細が発表された。また、北朝鮮から弾道ミサイルが発射される、ロシアで次期戦闘機が公開される、といった軍事的な動きもあった。

  ちょうど東京オリンピック(2020年7月24日～)が開催される3年前という節目であり、警察庁やSymantecでオリンピックを見据えた新規サービスが開始された点も特徴的。

- 特徴的なリージョンと動静（点と点）

  BlackHat/DEF CONの開催にあわせて、特にアメリカで政府機関が規制や注意喚起を行っていた。北朝鮮で軍事的な動きがあったためか、北朝鮮をターゲットとしてKONNI RATを感染させようとするAPT攻撃が確認された。また、中国で新しいマルウェアが確認されたり、マルウェア作成者が逮捕される、中国から日本に対する攻撃が活発化するなど、北朝鮮を中心とした近隣諸国でのセキュリティ関連での動きも活発だった。

- アナリストコメント（本質的なナニカ）　キー：大規模イベント

  軍事関連の出来事があると、それに対して抗議の意味をこめたサイバー攻撃が発生していることが分かる。また、近隣諸国においても攻撃が発生したりとセキュリティ情勢が不安定になる。
  大きなイベント（BlackHatやオリンピック)を成功させるために、政府機関・民間企業が対策に乗り出すという風潮がみえてきた。

2017年7月 話題一覧

カテゴリ	話題
新技術・イノベーション	中国で新しいマルウェアGreen Hatが確認される
	新しいマルウェアCowerSnailが確認される
	Black HatとDEF CONでハッキング手法が続々と発表される
今月の顔	旧被差別階層（ダリット）出身ラム・ナス・コビンドがインド大統領に就任
ビジネス	Audi　レベル3自動運転量産化を発表
	✓ Adobe 2020年にFlash Player提供終了を発表
	東京都議選の投開票が行なわれ、小池都知事が率いる都民ファーストの会が大勝
	警察庁、東京オリンピック警備へ「情報センター」設置
	✓ Symantec　東京オリンピックを視野にいれSOC拡張
イベント・カンファレンス	香港返還20年
	✓ ラスベガスでBlackHat/DEF CON開催
規制・国際ルール	中国当局通信会社大手3社に対してVPN接続を止め要請
	米政府、カスペルスキーの製品調達禁止　安全保障上の懸念指摘
	FBIがinternetに接続されている子供向けおもちゃについて注意喚起
	ロシアの次期主力戦闘機 MiG-35 が公開(7月18日)
	MicrosoftがFancy BearのC&Cサーバドメインを訴訟により取得

2017年7月 話題一覧

	カテゴリ	話題
	事件・事故	Apache Struts2複数の脆弱性公開
		中国でマルウェアFireball開発者逮捕
		中国の「APT10」、日本の官公庁や製造業、メディアなどを狙う攻撃が活発化
✓		北朝鮮 午前９時３９分 弾道ミサイル発射
		AlphaBayとHansaがテイクダウンされる
		Microsoft社から漏洩したとみられるファイルがhive.comで公開
		北朝鮮をターゲットとしたKONNI RATを感染させる攻撃キャンペーン
		Verizon社の1400万人分の顧客データがクラウドストレージ上で公開状態に
		「スマート水槽」がハッカーの侵入口に、北米のカジノで被害
		スウェーデン政府、ほぼ全国民分の個人情報＆軍の機密情報を流出
✓		AlphaBay経営者のアレキサンダー・カーゼスがタイの拘置所で死亡
		旧バージョンのPetyaへのDecryptorが公開される
	ユニーク	ヒアリ発見

2017年8月 動静マップ

2017年8月 動静マップ

- 大きな話題（点）
  USENIX Security Symposiumにおいて、米ジョージア工科大学などの学術機関やAkamai、 Google などの研究者が、大規模な DDoS 攻撃を発生させたIoTマルウェア「Mirai」の手口や、踏み台にされた IoT 機器の現状について包括的に分析した報告書を発表した。
  25日(金)に大規模ネット障害が発生。GoogleのBGP経路情報の誤りが世界に影響。180万人の有権者情報が露呈する事案の原因がAWSの設定ミス。

- 特徴的なリージョンと動静（点と点）
  運用上のミスが連鎖的に発生し、通信障害にまつわる話題も多いつきであった。

- アナリストコメント（本質的なナニカ）
  キー：人的ミス
  運用上のミスによる大規模な通信障害や情報漏洩が目立つ月であった。サーバ設定の不備、リニューアルする作業の不備などから、情報漏洩が発生した。ルーティング情報の設定ミスによる大規模通信障害は、日本を中心に様々なサービスを一時的な停止へと追い込み、人的ミスや内部不正の対策に一石を投じることとなった。

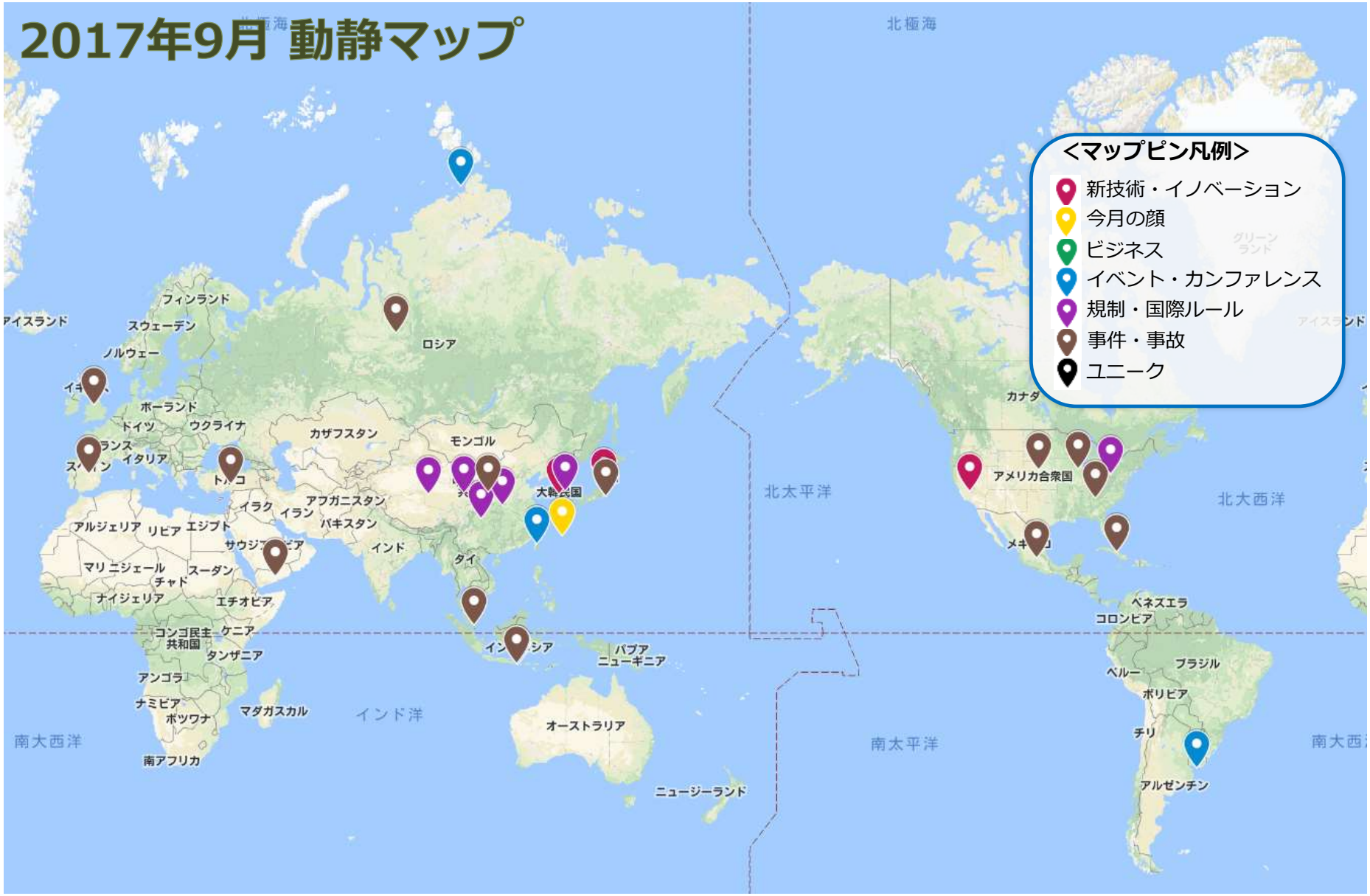
2017年8月 話題一覧

カテゴリ	話題
新技術・イノベーション	中国のUSB充電アダプター型盗聴器が先進的すぎて怖い
	エストニア世界各地のミラーリング拠点でサイバー攻撃に備える
	エストニア、独自の仮想通貨「エストコイン」発行を検討
	Kasperskyのリサーチャー、個人開発のリモートフォレンジックツール無償公開
	Facebook Messengerを介したマルウェア拡散が観測される
今月の顔	-
ビジネス	監視カメラ映像、中国では一大コンテンツに
	DeNAと小学館が共同出資会社「MERY」を設立 女性向けデジタルメディアを運営
	アリババ、日本で中国発スマホ決済　ＱＲコード使用
イベント・カンファレンス	HITCON2017
✓	USENIX Security Symposium
	日印サイバー協議
規制・国際ルール	米政府、IoTに求めるセキュリティ基準に関する法案
	DHSのサイバーオペレーションを明確化する法案可決
	インドネシア政府、サイバー犯罪に関わった153名の中国人を国外退去処分に
事件・事故	Bitcoinが分裂
	WannaCryの身代金約14万ドル相当引き出される
	WannaCryキルスイッチ発見した研究者Marcus Hutchins氏、マルウェアKronosに関与で起訴される

2017年8月 話題一覧

	カテゴリ	話題
	事件・事故	2012年韓国総選挙において、ネットを使い諜報機関NISが民意を扇動していた
		不正が発覚した中国の認証局、Microsoftも無効化を通告
✓		GPSを狙ったサイバー攻撃増加
		北朝鮮２９日午前６時前、日本上空を通過する弾道ミサイルを発射
		ベネズエラで同時サイバー攻撃、大統領府など標的 反乱集団を支持
		複数の衆院議員事務所に大量の中国語スパムメール　自民議員には１３日夕から５万超
		NetSarang社、正規のソフトウェアアップデートにマルウェア、法人顧客に配信
		HBO social media hacked in latest cyber security breach
		北朝鮮関連サイトを踏み台とした水飲み場型攻撃解析レポート
✓		25日（金）のネット障害、原因は経路情報の誤り、世界に影響
		ＡＩが「共産党は無能」と批判＝中国ネット大手、サービスを停止-香港紙
		人気YouTuberが「VALU」で売り抜けか--運営会社が対策発表、買い戻しの事態に
		スペイン・バルセロナ繁華街でISテロ、14人死亡、100人以上けが
✓		180万人の有権者情報が露呈、AWSの設定ミスに警鐘
✓		HISで情報漏洩、バスツアー客の予約情報が流出
		ブータンを挟んで対峙する中国とインド：「幸せの国」は戦場になるか
	ユニーク	-

2017年9月 動静マップ



2017年9月 動静マップ

- 大きな話題（点）
  CCleaner5.3にマルウェアが含まれていた。中国におけるWeChatの通信監視、米国DHSにおけるKaspersky社製品の削除指示が話題に。

- 特徴的なリージョンと動静（点と点）

  中国サイバーセキュリティ法施行後、9月ではWeChatの通信監視、2000万台のカメラ網SkyNetによる人民監視、10億人が利用するメッセージアプリWhatsAppの遮断などが行われセキュリティ強化(統制？)をアピールする月となった。一方米国でのKaspersky社製品の削除など、スパイ活動に関する連鎖が大きな動きとして見て取れた。

- アナリストコメント（本質的なナニカ）　キー：諜報

  情報の監視、情報を読み取るためのマルウェアの観戦活動、国家間の牽制など、スパイ活動に関する動きが同時期に顕在化するなど、単体のニュースだけでは読み取れない米中露の情報戦が見え隠れする月となった。

2017年9月 話題一覧

カテゴリ		話題
新技術・イノベーション		宇宙船であらゆる都市間を約３０分で移動 米企業が計画
		SAMSUNG社バグ報奨金制度を新設
		「KSKロールオーバー」が始まる
今月の顔		-
ビジネス		-
イベント・カンファレンス		CODE BALI 2017
		APNIC / FIRST TC Taichung
		LACNIC 28 LACNOG 2017
規制・国際ルール	✓	中国政府がメッセージングアプリWeChat全ユーザ情報にアクセス可能となる
	✓	中国にて、2,000万台の監視カメラシステムSky Netは、人工知能(AI)、顔認識技術、GPSトラッキングが使われリアルタイム監視をしている
		中国、仮想通貨を通じた資金調達を禁止
	✓	中国、10億ユーザ以上が利用するメッセージングアプリ「WhatsApp」を遮断
		中国がBitcoin取引所を閉鎖
	✓	米政府機関からKaspersky社製品の削除するようDHSが指示

2017年9月 話題一覧

	カテゴリ	話題
	事件・事故	キューバの米大使館に音響攻撃か 人員を大幅縮小へ
		イエメン コレラ感染１００万人に達するおそれ
		バリ島 火山噴火の警戒１週間 避難者は１４万人超
		ロシアとトルコ 両大統領が会談 関係強化を強調
		Kaspersky社AVソフトを侵害して、ロシア政府がNSAの機密情報を窃取
		シンガポールがサイバー攻撃の起点国のトップに
		中国製Androidキーボードアプリ GO Keyboardがユーザ情報を収集
✓		CCleaner 5.33にマルウェア
		米Equifax社(消費者信用情報会社)が1億4300万件の信用情報を漏えい
		米国の35州の有権者情報全てが入手可能、情報書き換えも可能と判明
		米、税金還付企業MoneyBack、300GB以上のパスポートやクレジットカード情報を漏洩
✓		米TigerSwan 社が、 保有する米軍と諜報機関への求職に関する情報が公開状態に
		ネット金融狙うDDoS攻撃が続く、脅迫型による被害も明らかに
		空の便に世界的な乱れ、国際予約システムに障害－復旧までに３時間半

2017年10月 動静マップ

2017年10月 動静マップ

- 大きな話題（点）

  ヨーロッパやウクライナ、ロシアを中心に、ランサムウェア「Bad Rabbit」が確認され、国内のサーバではアイカ工業が拡散に使われていた。ラスベガスで開催されたBlackHatの会場近辺で銃乱射事件が発生した。「パナマ文書」報道に加わった女性記者が車を運転中に爆弾が爆発し死亡する事件が発生した。スウェーデンの交通局に対してDDoS攻撃が仕掛けられシステムがダウンしたことにより、列車予約不能や遅延情報受信不可等の影響が発生した。

- 特徴的なリージョンと動静（点と点）

  ヨーロッパを中心に、マルウェア感染の拡散や交通機関へ影響のある被害、テロ事件など、何らかの意図とその連鎖が見え隠れする。

- アナリストコメント（本質的なナニカ）

  キー：EU

  サイバー空間における攻撃が、目に見える形で被害が発生させたことが目立つ一か月であった。特にヨーロッパを中心とした話題が多く挙がったが、Bad Rabbitによるランサムウェアの感染においては、日本のアイカ工業が拡散元に利用されてしまうなどの被害があった。また、被害規模の大きい攻撃や事件が発生しており、今後の再発防止策について議論が過熱する話題が見受けられた。

2017年10月 話題一覧

カテゴリ	話題
新技術・イノベーション	-
今月の顔	ノーベル文学賞にカズオ・イシグロ氏
ビジネス	欧州 モナーク航空が運航取りやめ混乱 １１万人の帰国便なくなる
	トヨタ 豪での車生産を終了 通貨高などで採算悪化
	インテル、ビッグデータ関連15社に68億円　日本企業も
	グーグル、ウーバーからリフトに乗り換え　出資を主導
	googleに対抗のためMSとamazonがAI分野で提携
✓	「サイボウズLive」終了へ　200万ユーザ超えも……「有料サービスに集中」
イベント・カンファレンス	タイ前国王葬儀を前に王宮立ち入り制限 追悼ムード
	APWG.EU eCrime Cyber-Security Symposium

2017年10月 話題一覧

カテゴリ	話題
事件・事故	ラスベガス銃乱射事件 59人死亡 527人けが 「過去最悪」
	パリ出発後エンジン損傷 Ａ３８０旅客機が緊急着陸
	パレスチナ ガザ ハマスが暫定自治政府の統治受け入れ
	米空母が香港に寄港 指揮官が北朝鮮をけん制
	ジョンナム氏殺害事件で初公判 無罪主張
	Yahoo30億件のアカウント全てがハッキングされていた
	神戸製鋼所　アルミ製品データ改ざん
	ロシアの工作、「ポケモンＧＯ」悪用＝昨年の米大統領選介入疑惑
✓	スウェーデン交通機関を標的にしたDDoS
	新型ウイルスで不正送金　被害２億円超、初摘発
	タイ銀行協会、サイバー攻撃対処で新組織
✓	アイカ工業 WebサーバーがマルウエアBad Rabbitの拡散に使われた可能性
✓	ウイルス保管容疑でセキュリティ企業ディアイティの社員逮捕、同社は反論
	マレーシアで4,600万件の携帯電話加入者の顧客情報が漏洩
	エストニア、国民が利用する電子認証のセキュリティ強化

2017年10月 話題一覧

カテゴリ	話題
事件・事故	ユネスコ脱退、アメリカとイスラエルが表明　パレスチナ問題で抗議
	オーストリア総選挙　世界最年少の31歳首相誕生へ
	「イスラム国」壊滅へ　拠点都市ラッカ陥落
✓	記者爆殺、揺れるマルタ　「パナマ文書」報道、疑惑追及
	中国共産党大会が１８日開幕
	ＮＹでトラック突っ込む、８人死亡
	Twitter、ロシア主要2メディアの広告締め出し
✓	ランサムウェア「BadRabbit」が猛威、交通機関やメディアに被害
ユニーク	「ドラゴンフォース、帰ってきたウルトラマン」１日から中国国内で公開
	衆議院議員選挙2017

2017年11月 動静マップ

2017年11月 動静マップ

- 大きな話題（点）

  10月に比べると、アジアの話題が目立った。トランプ大統領のアジア5か国歴訪に始まり、米国による北朝鮮のテロ支援国家の再指定があった。またアフリカにおいても、長年独裁政治が行われてきたジンバブエで大統領が交代したことが取り上げられるなど、政治の話題が多く報じられた。サイバー攻撃の観点からは、世界規模で影響の出た事象はなかったものの、月末にMac OSにおける脆弱性が明るみになり、懸念が広がった。また、角界ではモンゴル出身の横綱・日馬富士による暴行問題で引退に追い込まれる事態となり、報道が過熱した。

- 特徴的なリージョンと動静（点と点）

  アジアでは日本企業の新たなビジネス進出が相次ぎ明らかになったり、日本の誇るスーパーコンピューターやロボットの再開発についても話題になった一方で、東芝のテレビ事業の売却が決まるという、残念なニュースもあった。ヨーロッパではENISA（欧州ネットワーク・情報セキュリティ機関）がIoTセキュリティベースラインの推奨事項をまとめた文書を公開したり、Interpolがシスコとの連携を表明したりと、規制・ルール面での動きが浮き彫りとなった。さらにオペレーショナルなレイヤーでは、CSIRT関連・技術者コミュニティのカンファレンスが数件開催される動きがあった。

- アナリストコメント（本質的なナニカ）

  キー：アジア

  サイバーセキュリティインシデントの観点からは、過去数か月に比べて比較的落ち着いた月であったように感じられるが、その分政治や国際問題・技術開発など、その他の分野での動きが目立った。ニュースの分散という点では、特定の地域の動きというより、各地で違うレイヤーに、独立した様々な動きがみられたといえる。

2017年11月 話題一覧

カテゴリ	話題
新技術・イノベーション	人型ロボット「ソフィア」、サウジで市民権を獲得
	✓ 6期連続でスーパーコンピュータ「京」がGraph500で世界第1位を獲得
	ソニー、アイボ予約受け付け開始　初回は約３０分で完売
	iPhone X 発売開始
今月の顔	✓ 横綱日馬富士が引退　暴行問題で
	✓ トランプ大統領、アジア歴訪
	ジンバブエのムガベ大統領が辞任　37年の政権に幕
ビジネス	ブラジルにもフィンテック投資の波が到来
	【ミャンマー】丸紅、ヤンゴンの火力発電所改修を受注
	【タイ】電力バンプー、山形県のメガソーラーに出資
	【インドネシア】三菱日立パワー、ＰＬＮにガスタービン納入
	トレビの泉の小銭、市収入へ＝ローマ、財政難で検討
	【シンガポール】ＵＯＢ、スマートウオッチでの決済可能に
	✓ 東芝、中国家電大手にテレビ事業を売却　ＰＣ撤退も現実味
イベント・カンファレンス	APCERT Annual Conference 2017
	Global Conference on Cyber Security
	CODEBLUE 2017
	OIC-CERT Conference 2017
	PacSec 2017

2017年11月 話題一覧

	カテゴリ	話題
	規制・国際ルール	エアーズロック登山禁止＝2年後、先住民の聖地―豪
		Cisco、インターポールと脅威情報を共有 - サイバー犯罪対策で
✓		ENISA: Baseline Security Recommendations for IoT
		メキシコ、サイバーセキュリティ戦略発表
	事件・事故	ニューヨークで車暴走、8人死亡 「テロ」と断定
		＜インド＞火力発電所で爆発事故　１６人死亡１００人負傷
		ISが都市を再占拠＝撤退装い猛反撃―シリア東部
		北朝鮮がミサイル発射、高度4000キロ超　ＩＣＢＭ級と推定
		札幌管制部で管制システムに不具合、新千歳空港など離発着できず
✓		海外の研究者により macOS High Sierra の設定に関する問題が公開
		Qihoo 360 report: A New Mirai Variant is Spreading Quickly on Port 23 and 2323
✓		米、北朝鮮をテロ支援国再指定＝「最大限の圧力」－大規模追加制裁も実施へ
	ユニーク	“ＩＴ犯罪に不安” 過去最多の60%余 内閣府調査
		祈る間、実は居眠り＝ローマ法王が告白
		ソシャゲ不具合の原因、ソースコード開示して説明　「詫びソースコードとは斬新」と話題に

2017年12月 動静マップ

2017年12月 動静マップ

- 大きな話題（点）
  中東での対立の激化が目立った。トランプ米大統領がエルサレムをイスラエルの首都と認定したことから、中東の各地で抗議デモが発生した。また、イエメンでの内戦はサウジアラビアによる封鎖のため、約800万人が飢餓に瀕する事態となった。

- 特徴的なリージョンと動静（点と点）
  中東では、トランプ米大統領によるエルサエムの首都認定に対し、抗議デモに加え、ハッカー集団Anonymousが米国およびイスラエルに対するサイバー攻撃を警告するに至った。イエメンの内戦やサウジアラビアでの汚職摘発などと合わせて、地域の緊張が高まっている。
  仮想通貨の不正な取得に関する動きも確認された。欧州や韓国の仮想通貨取引所に対するサイバー攻撃に関する調査結果が公表された。また、webサイトの閲覧者に無断で仮想通貨のマイニングを行わせる手法が悪質化し、webブラウザを終了してもマイニングを行い続けるスクリプトが確認された。

- アナリストコメント（本質的なナニカ）
  キー：仮想通貨
  ビットコインの価格が高騰し、取引の参加者が増えるなか、仮想通貨を窃取するサイバー攻撃が更に増える恐れがある。特に、資金調達のためこれまで以上に仮想通貨を狙うことが考えられる。また、サイバー犯罪者が金銭や決済カード情報に加えて仮想通貨も標的とする恐れがある。ウォレットや取引所のセキュリティ対策が不透明な点もリスクを高めている。

2017年12月 話題一覧

カテゴリ	話題
新技術・イノベーション	-
今月の顔	-
ビジネス	ビットコインの取引高で日本円がシェア1位に
	米国でビットコインの先物取引が開始
	ビットコインの価格が200万円を超える
イベント・カンファレンス	-
規制・国際ルール	米FCC、ネット中立性の原則撤廃を決定
事件・事故	イエメン内戦800万人飢餓
	サウジアラビア、汚職により拘束されたエリート層の大半が資産没収で合意
	レバノン首相辞意撤回
	✓ 国際オリンピック委員会、ロシアの平昌五輪参加認めず
	✓ イスラエル首都にエルサレム　トランプ大統領認める
	グーグルを騙るフィッシングメールの犯人逮捕
	StorageCrypt Ransomwareの観測
	英警察、爆破物によるメイ首相暗殺計画を阻止
	ニューヨーク中心部で爆発　バングラデシュ出身の容疑者を逮捕
	大阪大で８万人の個人情報漏洩の恐れ　教員ＩＤ使い海外から不正アクセス

2017年12月 話題一覧

カテゴリ	話題
事件・事故	Anonymous、米国のエルサレム首都認定に抗議しOpUSA、OpIsraelを実施と警告
	米政府、国家安全保障戦略を発表。中国・ロシアを「競合勢力」と位置づけ
	✓ 米政府、WannaCryの大規模感染に北朝鮮が関与との見方を示す
	北朝鮮系ハッカーが欧州のビットコイン取引所を攻撃
	✓ 韓国のビットコイン取引所に対するサイバー攻撃が北朝鮮によるものと韓国政府が発表
	ブラウザを終了しても仮想通貨のマイニングを続けるマルウェアが出現
	JAL、ビジネスメール詐欺で約3億8千万円の被害
ユニーク	-

作成者一覧

- 阿部 慎司　NTTセキュリティ・ジャパン株式会社
- 石井 中　日本電信電話株式会社
- 上野 宣　株式会社トライコーダ
- 内田 有香子　JPCERT/CC
- 亀田 勇歩　SCSK株式会社
- 川口 洋　株式会社ラック
- 河島 君知　NTTデータ先端技術株式会社
- 寺島 崇幸　株式会社ディアイティ
- 中西 克彦　NECネクサソリューションズ株式会社
- 早川 敦史　NECソリューションイノベータ株式会社
- ももい やすなり　株式会社インターネットイニシアティブ
- 柳 優　日本アイ・ビー・エム株式会社
- 塩田 修一　株式会社富士通エフサス
- 芋川 泰子　富士通株式会社
- 小野 和紀
- 佳山 こうせつ　富士通株式会社

今年も一年お疲れ様でした。

グローバル動静共有プロジェクト(いまグロ) 一同
リーダー 佳山
2017.12.18