

サイバー攻撃 最前線 -広島版-

中津留 勇

Counter Threat Unit

SecureWorks Japan 株式会社

2018/06/01

Internet Week ショーケース in 広島
サイバー攻撃に耐える組織と運用

Secureworks®

Agenda

2017年から2018年における特徴的なインシデントを紹介

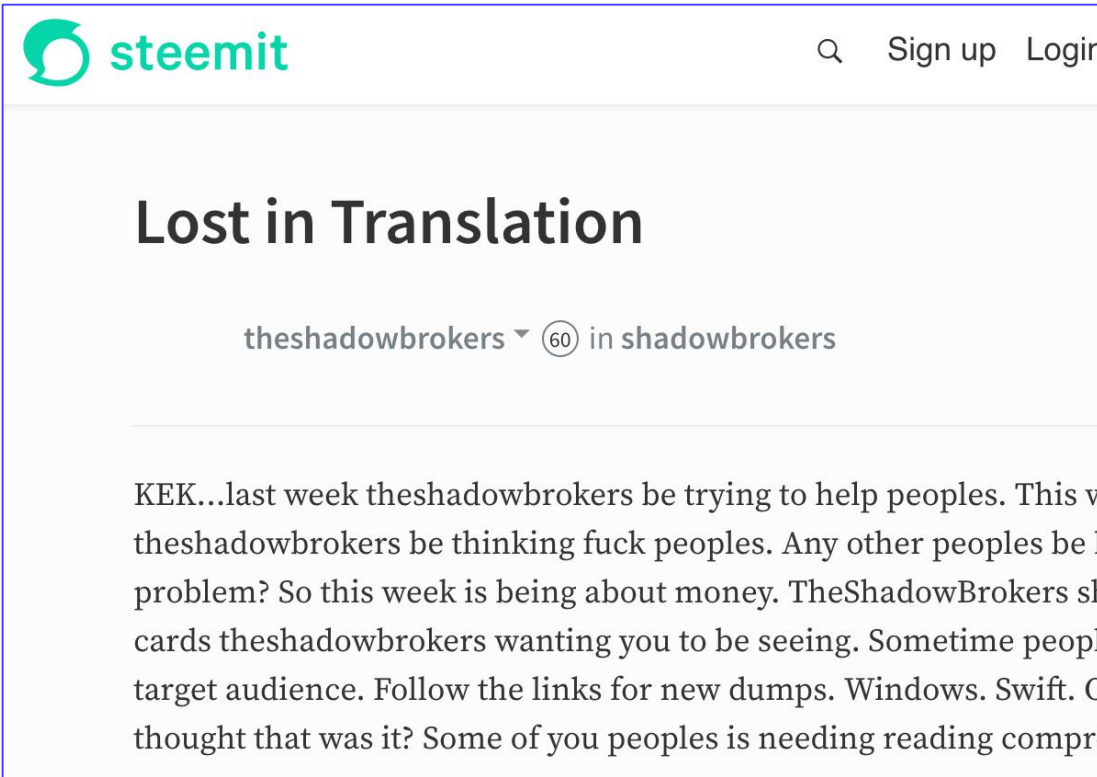
- Lost in Translation
- 例えば Struts を避ける
- 金銭をめぐるサイバー攻撃の変化
- この先生きのこるために



Lost in Translation

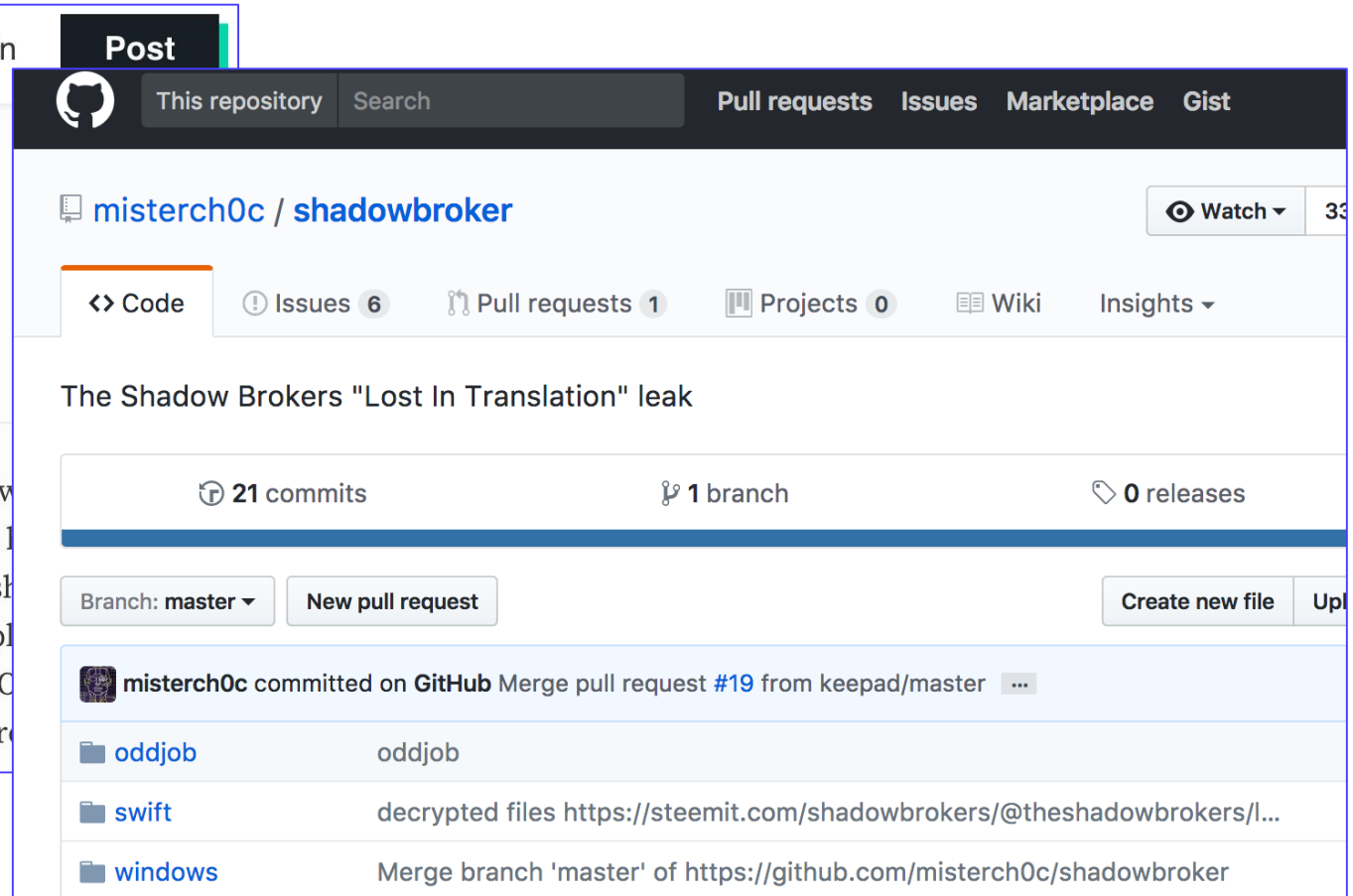
Lost in Translation

2017年4月に公開された、NSA 関連ツール・情報群



The screenshot shows a Steemit post. The title is "Lost in Translation" and it is by the user "theshadowbrokers" (60 followers). The text of the post is partially visible and reads: "KEK...last week theshadowbrokers be trying to help peoples. This v theshadowbrokers be thinking fuck peoples. Any other peoples be I problem? So this week is being about money. TheShadowBrokers sh cards theshadowbrokers wanting you to be seeing. Sometime peopl target audience. Follow the links for new dumps. Windows. Swift. C thought that was it? Some of you peoples is needing reading compr".

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



The screenshot shows a GitHub repository page for "misterch0c / shadowbroker". The repository has 21 commits, 1 branch, and 0 releases. A recent commit by "misterch0c" is shown, which merged pull request #19 from the "keepad/master" branch. The commit includes three files: "oddjob", "swift", and "windows". The "swift" file is described as "decrypted files" with a link to the Steemit post. The "windows" file is described as "Merge branch 'master' of https://github.com/misterch0c/shadowbroker".

<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

- 国際銀行間金融通信協会 (Society for Worldwide Interbank Telecommunication: SWIFT) に関わる資料集
- テキストや PowerPoint 資料など

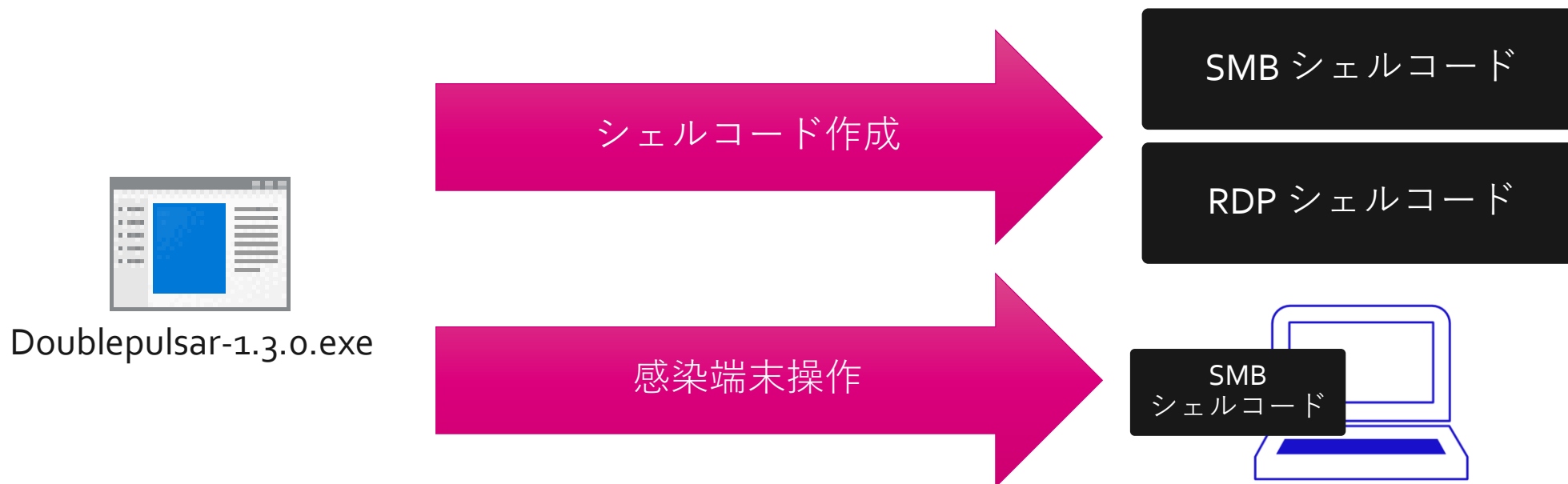
Oddjob

- Windows 用の 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



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

攻撃が成功すると、
ペイロードとして指定された
コードを実行する



Eternalblue-2.2.0.exe

SMB
シェルコード



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
 - 同梱されている FuzzBuzz を使うことで Metasploit 感覚で使うことが可能

```
fb > use
```

Architouch

Darkpulsar

Domaintouch

Doublepulsar

Easybee

Easypi

Eclipsedwing

Eclipsedwingtouch

Educatedscholar

Educatedscholartouch

Emeraldthread

Emeraldthreadtouch

Emphasismine

Englishmansdentist

Erraticgopher

Erraticgophertouch

Eskimoroll

Esteemaudit

Esteemaudittouch

Eternalblue

Eternalchampion

Eternalromance

Eternalsynergy

Ewokfrenzy

Explodingcan

Explodingcantouch

Iistouch

Jobadd

Jobdelete

Joblist

Mofconfig

Namedpipetouch

Pcdlllauncher

Printjobdelete

Printjoblist

Processlist

Regdelete

Regenum

Regread

Regwrite

Rpcproxy

Rpctouch

Smbdelete

Smblist

Smbread

Smbtouch

Smbwrite

Webadmintouch

Worldclienttouch

Zippybeer

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

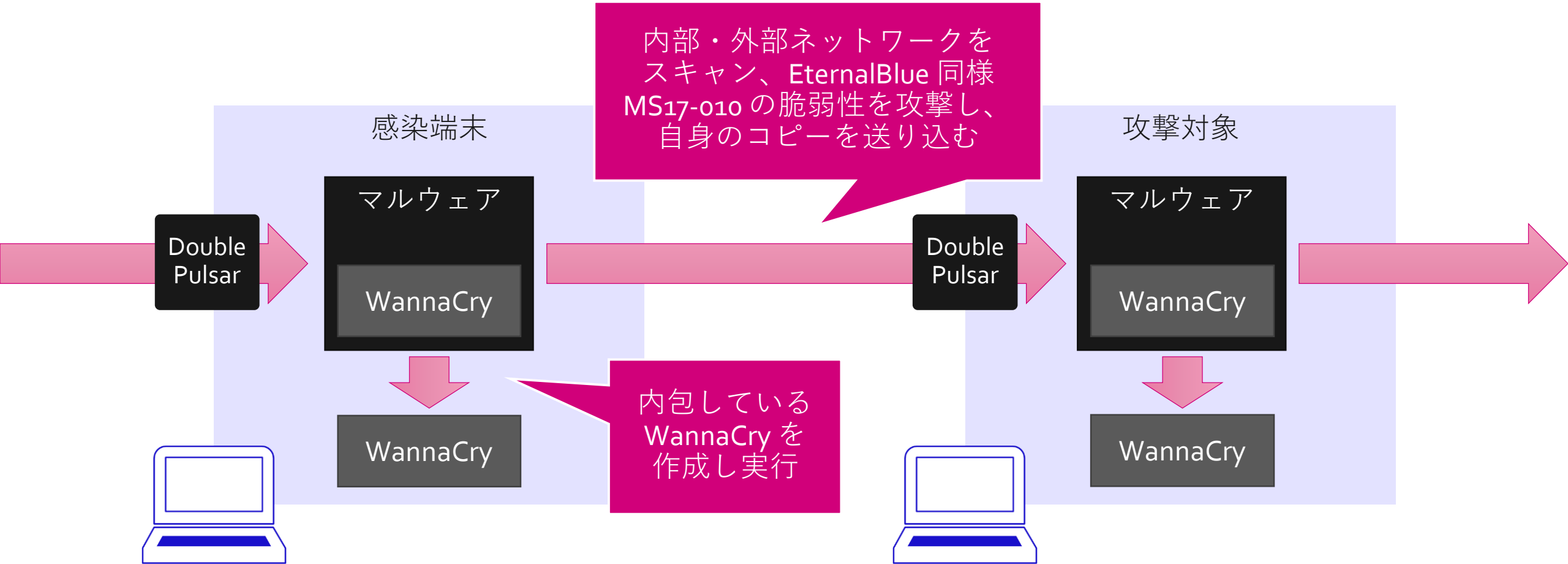
複数のツールを悪用する EternalRocks の出現

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、ドロップターの機能



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カメラの映像が漏えいする被害などは確認されていない。*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 家電量販店等と取引をする受発注システムにも影響が及び障害が発生。*39 ドイツのグループ会社事業所にある電子顕微鏡の操作装置からネットワークを通じて世界中の事業所に拡散した可能性がある。*40
富士・富士宮市消防指令センター	5月12日	指揮車3台に配備されていたタブレットの内、1台が感染。 火災・救急等の現場から動画をリアルタイムに送信するための専用機。 作業には支障がなかったことからそのまま継続して使用していた。 報道等を受けて15日に署員が報告。*41 ウイルス対策ソフト、OSの更新は動作不安定となることから実施しない設計となっていた。*42
墨田区の樹脂メーカー	12日昼	出社した際にマシンがブルースクリーンとなっていた。再起動後にランサムウェア感染を示す画面が表示。夕方にはもう1台別の端末でも同じ症状が発生。

<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

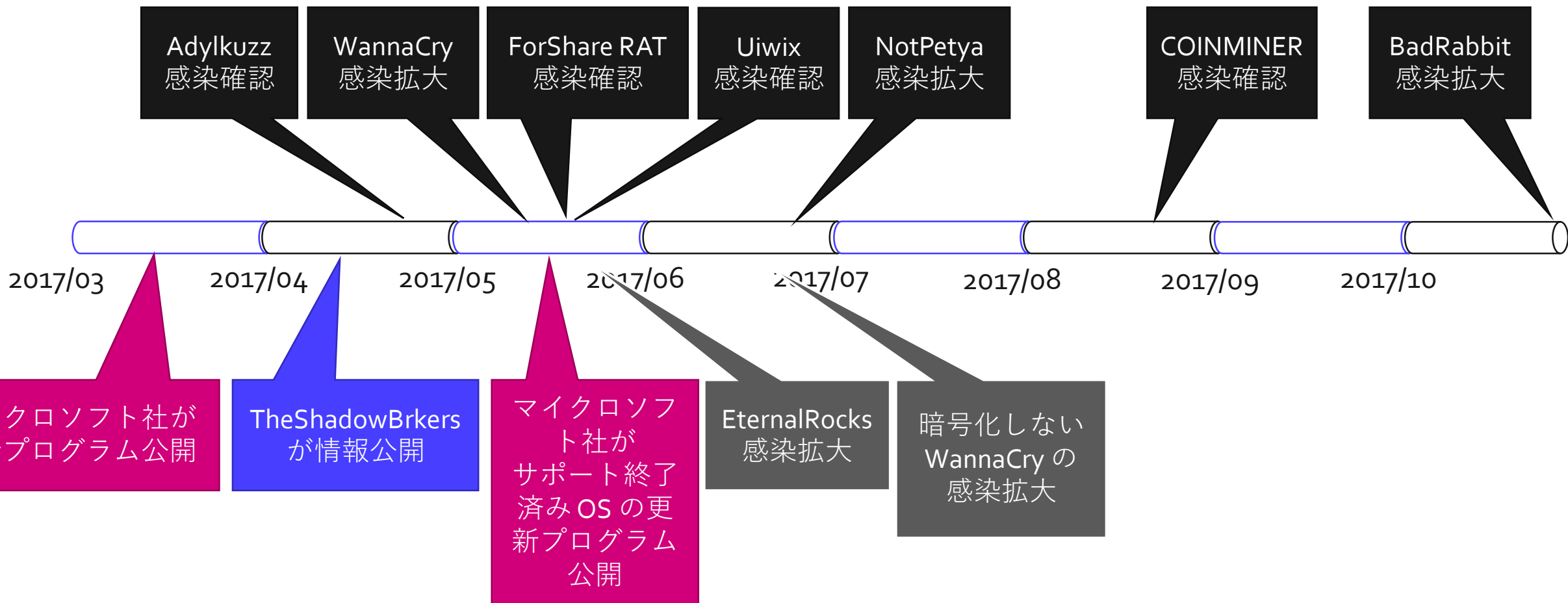
PsExec による
ファイル実行

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



例えば、**Struts** を避ける

2017 - 2018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	任意のコードを実行される脆弱性 (Jakarta Multipart パーサ)
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
S2-054	サービス運用妨害 (DoS) の脆弱性
S2-055	任意のコードを実行される脆弱性 (Jackson ライブラリ)
S2-056	サービス運用妨害 (DoS) の脆弱性

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	ショップサイトの信
総務省	地図による小地域分析(ISTAT 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/>

EQUIFAX English | Español Return to equifax.com

Cybersecurity Incident & Important Consumer Information

Enroll Now

to Protect & Monitor Credit — FREE for everyone in the U.S.

Need help? [Contact Us](#)

Home Consumer Notice Lock or Freeze Announcements FAQs Contact

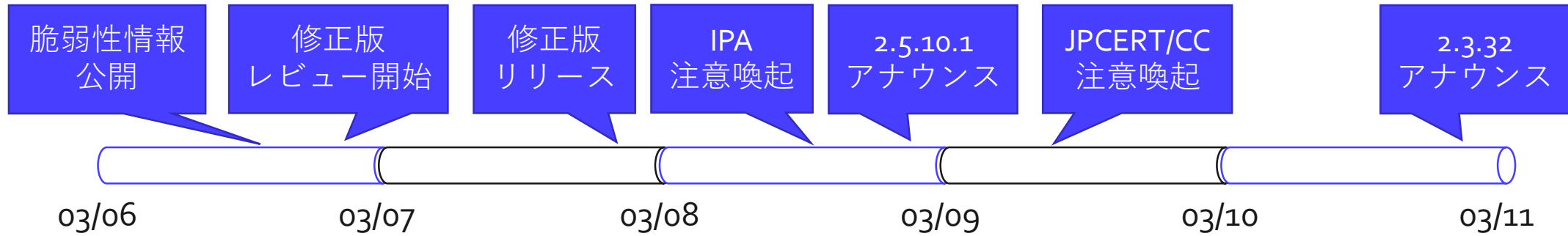
S2-045/S2-046 のタイムライン

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



数時間から数日の
ビハインド

S2-052/S2-053 のタイムライン

S2-045 での反省は活かされたのか

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、脆弱性情報も公開される	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/5ydeachhj2btglw
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/5xuhb2vwc7iagjir
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/ostesyujgfibzng
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

Struts 以外の脆弱性

2018年4月に Spring Framework の複数の脆弱性が公表

<https://spring.io/blog/2018/04/05/multiple-cve-reports-published-for-the-spring-framework>

Multiple CVE reports published for the Spring Framework

ENGINEERING ROSEN STOYANCHEV

UPDATE 2018-04-09: see follow-up [announcement](#)

Spring Framework 5.0.5 and 4.3.15 (superseded by [earlier](#) this week, include fixes for the following vuln

- [CVE-2018-1270](#) -> [CVE-2018-1275](#)
- [CVE-2018-1271](#)
- [CVE-2018-1272](#)

Spring Boot 2.0.1 and 1.5.11 (superseded by 1.5.12 above Spring Framework versions, were [released too](#)

Spring Framework の脆弱性に関する注意喚起

最終更新: 2018-04-10

ツイート メール

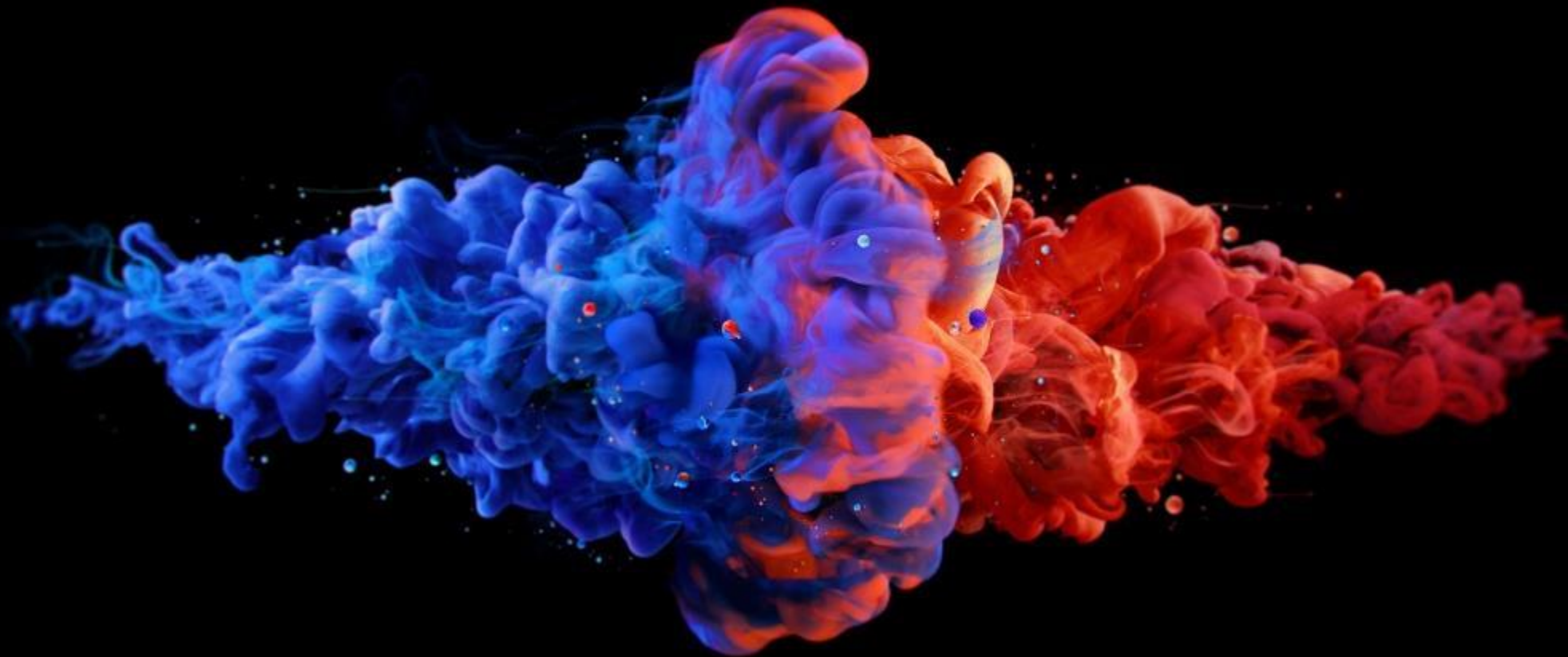
JPCERT-AT-2018-0014
JPCERT/CC
2018-04-10

I. 概要

Pivotal Software は、2018年4月3日、5日、9日 (現地時間) に、Spring Frameworkに関する複数の脆弱性情報を公開しました。Spring Framework は、Java の Webアプリ開発を行うためのフレームワークの 1 つです。公開された情報によると、Spring Framework には複数の脆弱性があり、脆弱性を悪用されると、実行しているアプリケーションサーバの実行権限で、リモートから任意の OS コマンドが実行されるなどの可能性があります。詳細は、Pivotal Software からの情報を参照してください。

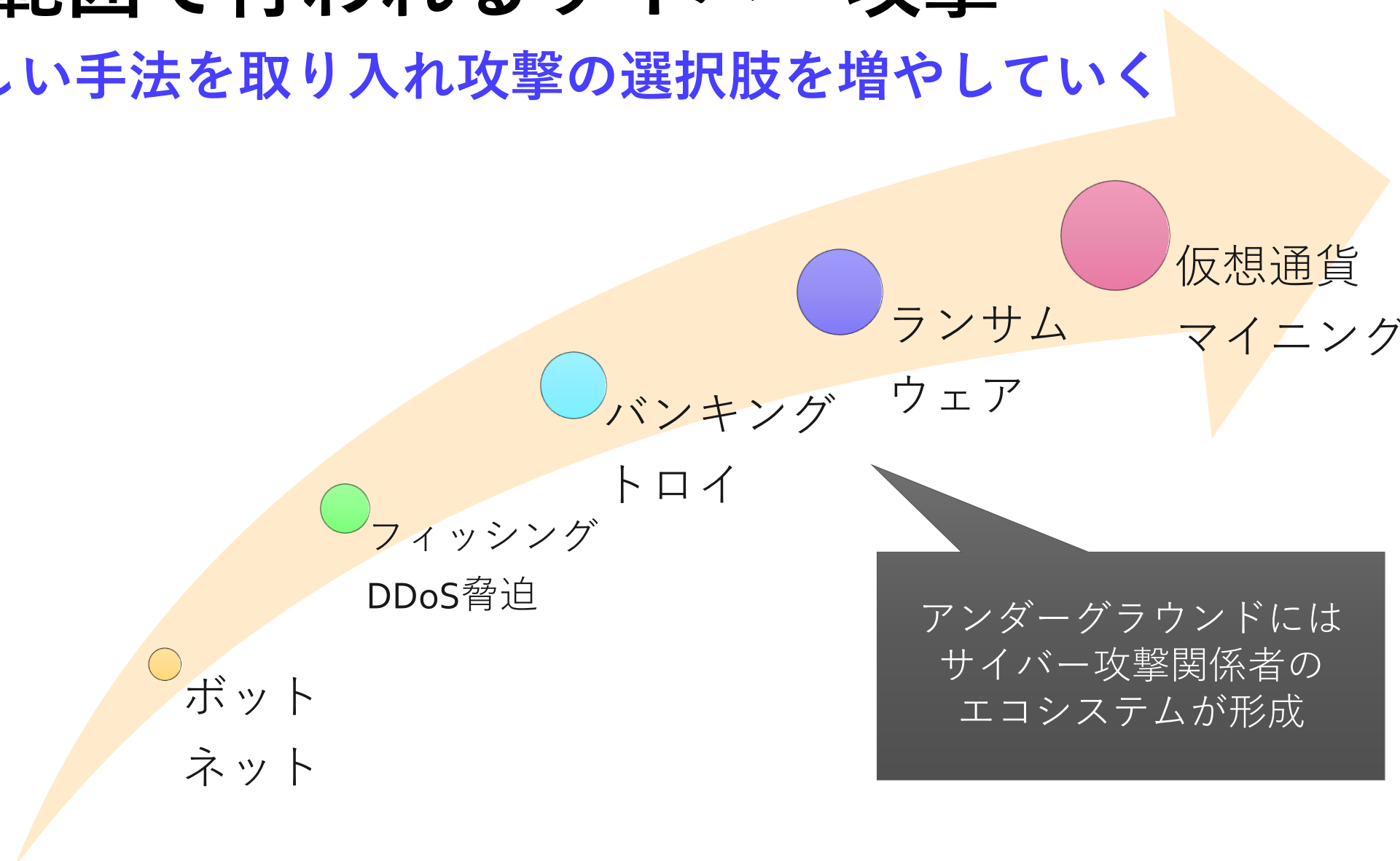
<https://www.jpccert.or.jp/at/2018/at180014.html>

金銭をめぐるサイバー攻撃の変化



広範囲で行われるサイバー攻撃

新しい手法を取り入れ攻撃の選択肢を増やしていく

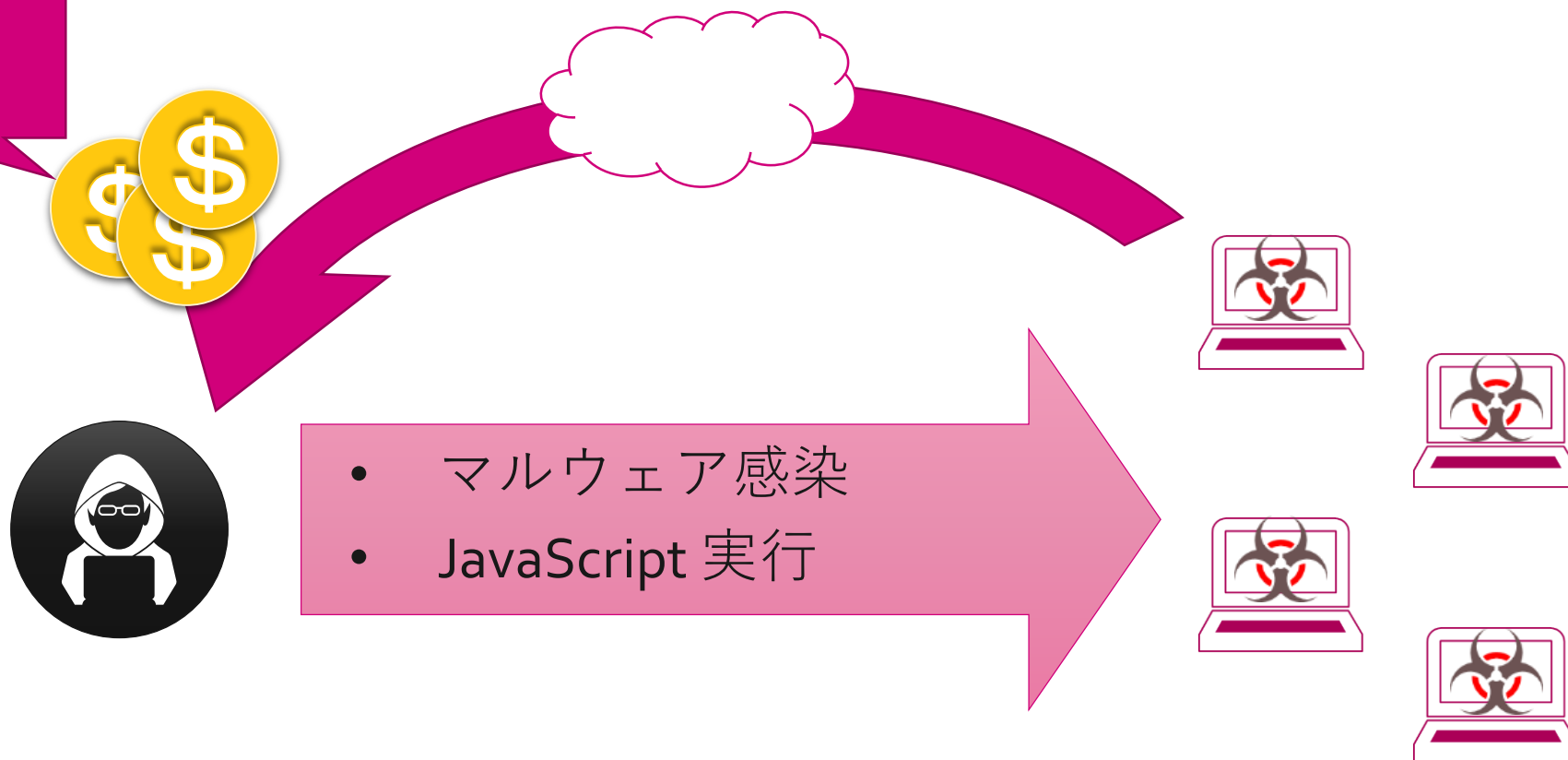


アンダーグラウンドにはサイバー攻撃関係者のエコシステムが形成

仮想通貨マイニング

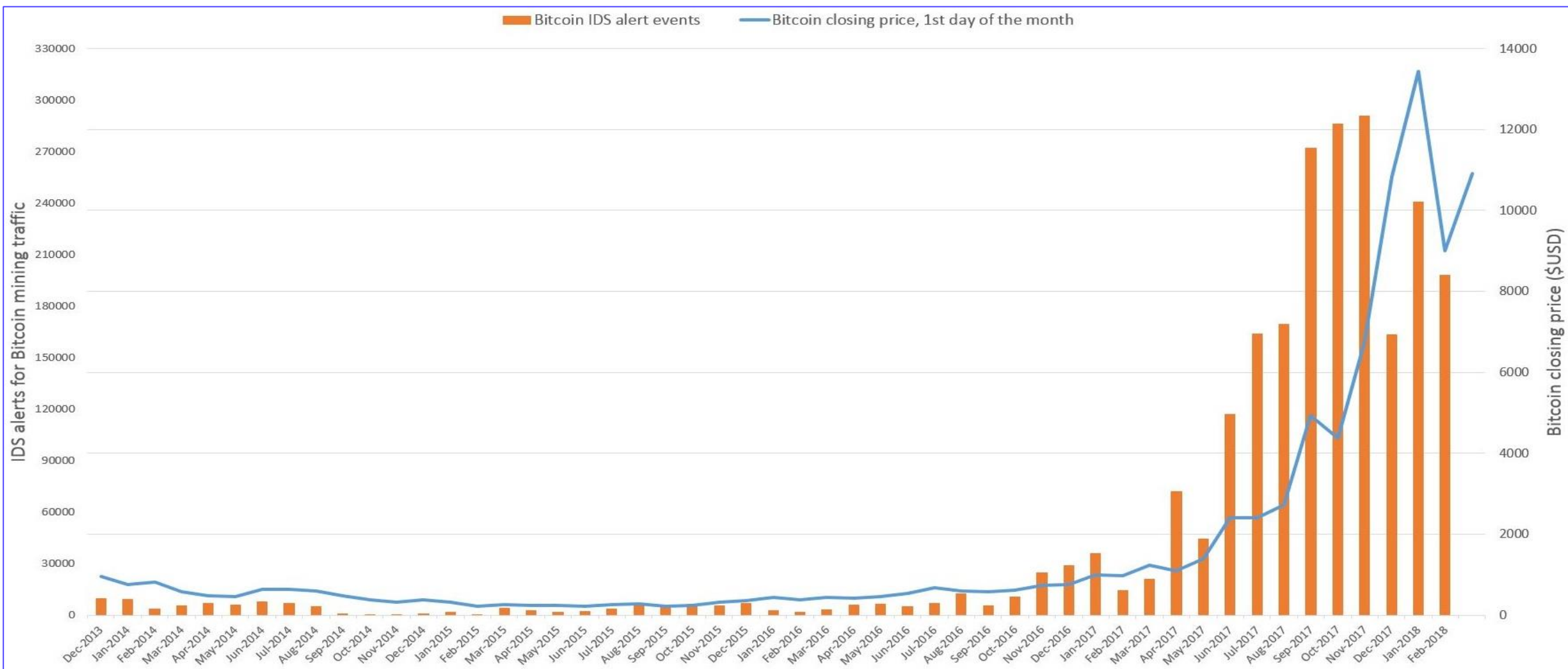
- マイニング (採掘) 処理をマルウェア感染端末、または Web サイト訪問者のブラウザを用いて行う

マイニング
成功報酬



仮想通貨マイニングブーム

ビットコインの価格高騰に合わせてマイニング活動が増加



“金銭を目的とした” 標的型攻撃

より金銭を奪える方向に？

情報売買

- 組織内に侵入し、窃取した機密情報を売買

ビジネスメール詐欺

- 経営者などになりすまし金銭を振り込ませる

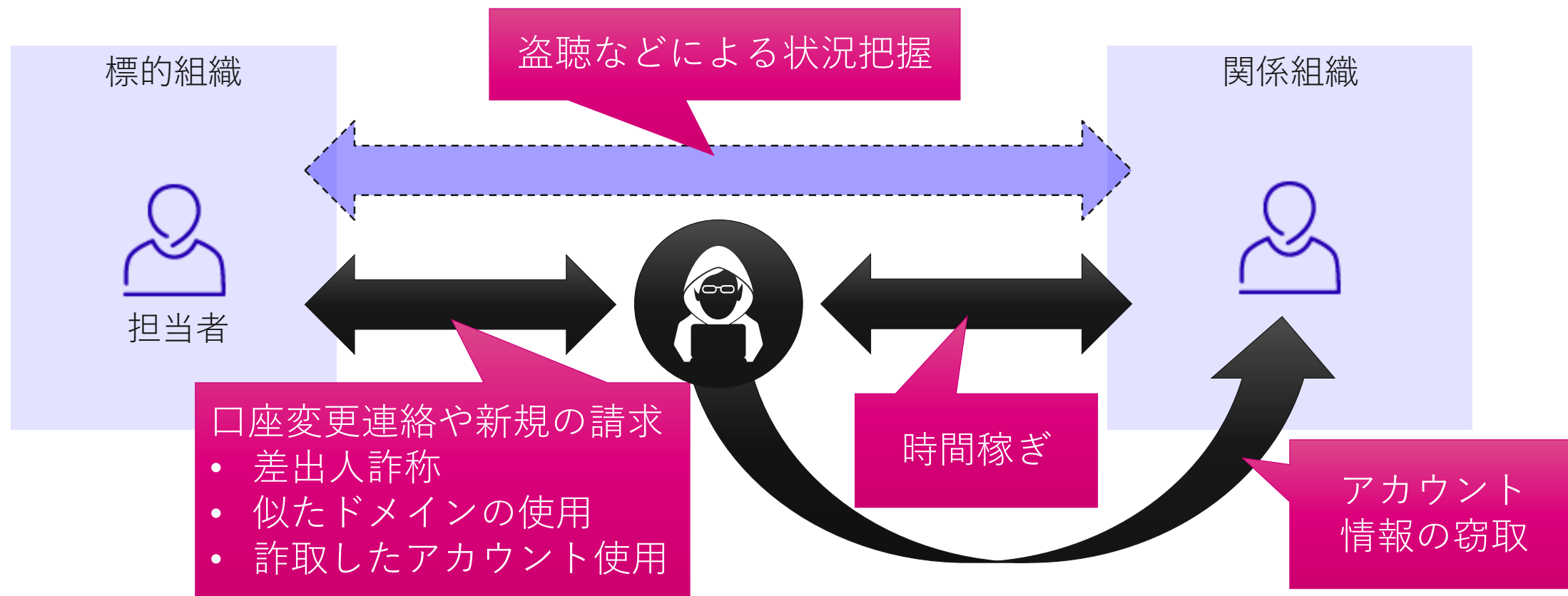
仮想通貨強奪？

- マイニングなどではなく直接的に奪う

ビジネスメール詐欺

Business Email Compromise: BEC

- 関係組織になりすまして金銭または機密情報を詐取するサイバー攻撃



ビジネスメール詐欺被害

海外での被害が主だが、日本国内でも大規模な被害が発生している

STATISTICAL DATA

The BEC/EAC scam continues to grow, evolve, and target small, medium, and large businesses. Between January 2015 and December 2016, there was a 2,370% increase in identified exposed losses³. The scam has been reported in all 50 states and in 131 countries. Victim complaints filed with the IC3 and financial sources indicate fraudulent transfers have been sent to 103 countries.

Based on the financial data, Asian banks located in China and Hong Kong remain the primary destinations of fraudulent funds; however, financial institutions in other regions are also identified as primary destinations.

2013年10月から2016年12月までで
約5800億円の被害

The IC3 and are...
complaint data and filings from financial institutions between **October 2013 and December 2016:**

Domestic and international incidents:	40,203
Domestic and international exposed dollar loss:	\$5,302,890,400

<https://www.ic3.gov/media/2017/170504.aspx>

<https://www.nikkei.com/article/DGXMZO24979150S7A221C1EA5000/>

日本経済新聞

2018年5月25日 (金)

トップ 経済・政治 ビジネス マーケット テクノロジー 国際・アジア スポーツ 社会

朝刊・夕刊

アドレス1字違い見逃す 日航3.8億円メール詐欺被害

2017/12/22 20:51 | 日本経済新聞 電子版

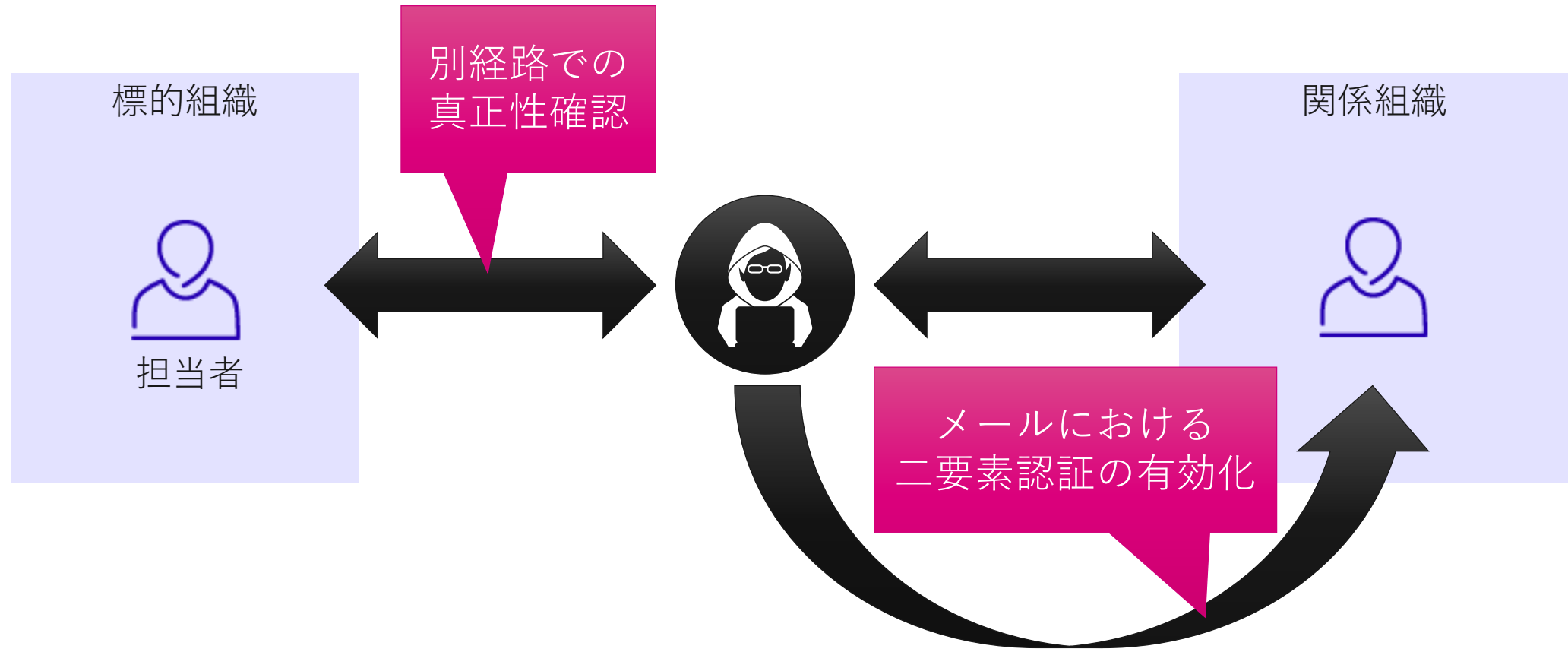
保存 共有 印刷 CO ME Twitter Facebook その他

かねて国内で小規模な被害が報告されてきたビジネスメール詐欺で、ついに大規模被害が発生した。日本航空の被害額は計3億8400万円。詐欺師は取引先とのメールをハッキングし、支払い手順を学んだうえで犯行に及ぶ。取引先を含むサプライチェーン全体での対策が求められている。

二要素認証による保護

ソーシャルエンジニアリングを見抜くことの難しさ

- 技術面だけでなく、手続き面でも「ダブルチェック」





この先生きのこるために

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
- 過去見つけた脆弱性・その頻度、世の中の評価
- 目に見える情報

それに頼らなくて済むように

- 攻撃されても防げる
 - 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
- 攻撃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



The logo features a large, stylized letter 'S' composed of two overlapping shapes: a solid black circle on the right and a blue shape on the left that resembles a speech bubble or a stylized 'S' segment. The word 'Secureworks' is written in white, sans-serif font across the center of the 'S'.

Secureworks®