TLP:GREEN

参考資料3

2018年「深刻な影響を発生させたサイバー攻撃」及び現実的な対策(事態対処態勢)

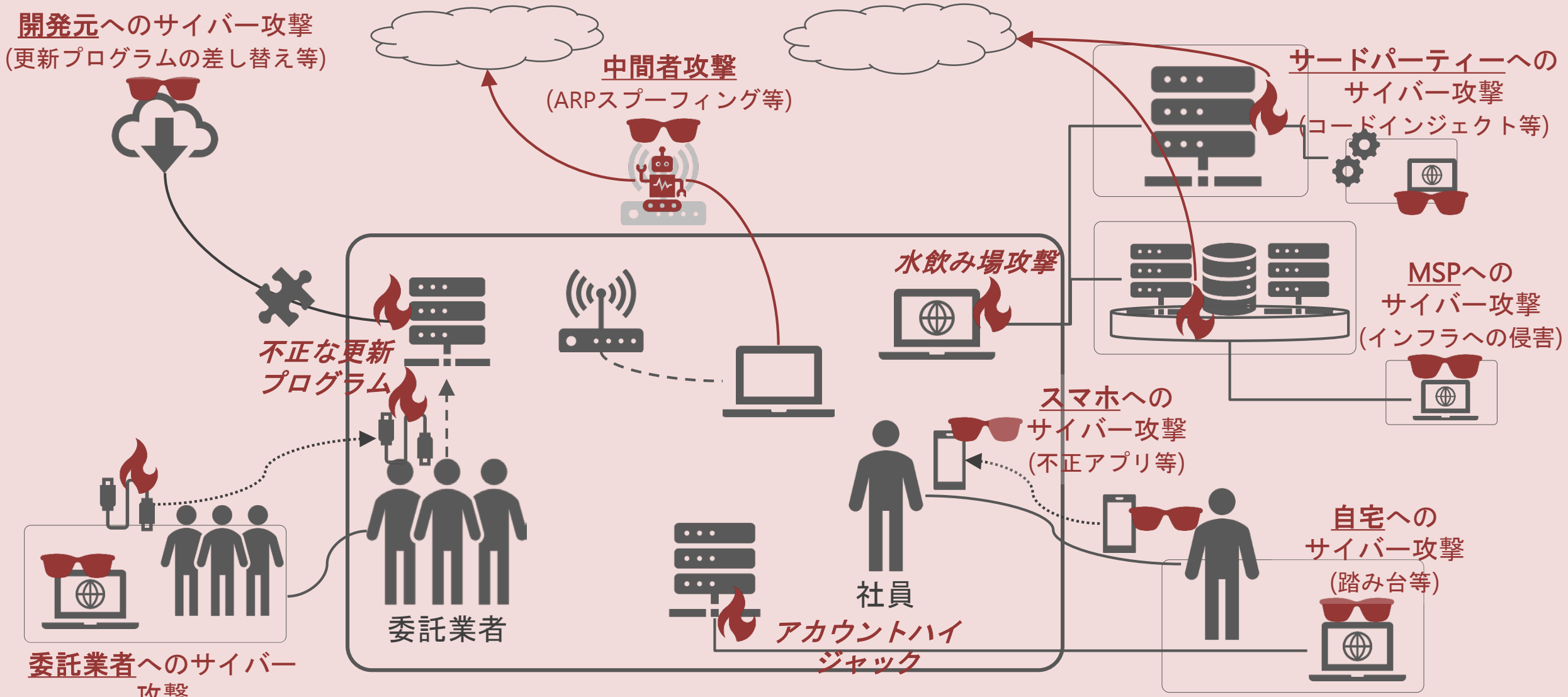
2019年3月

名和 利男

トピック１

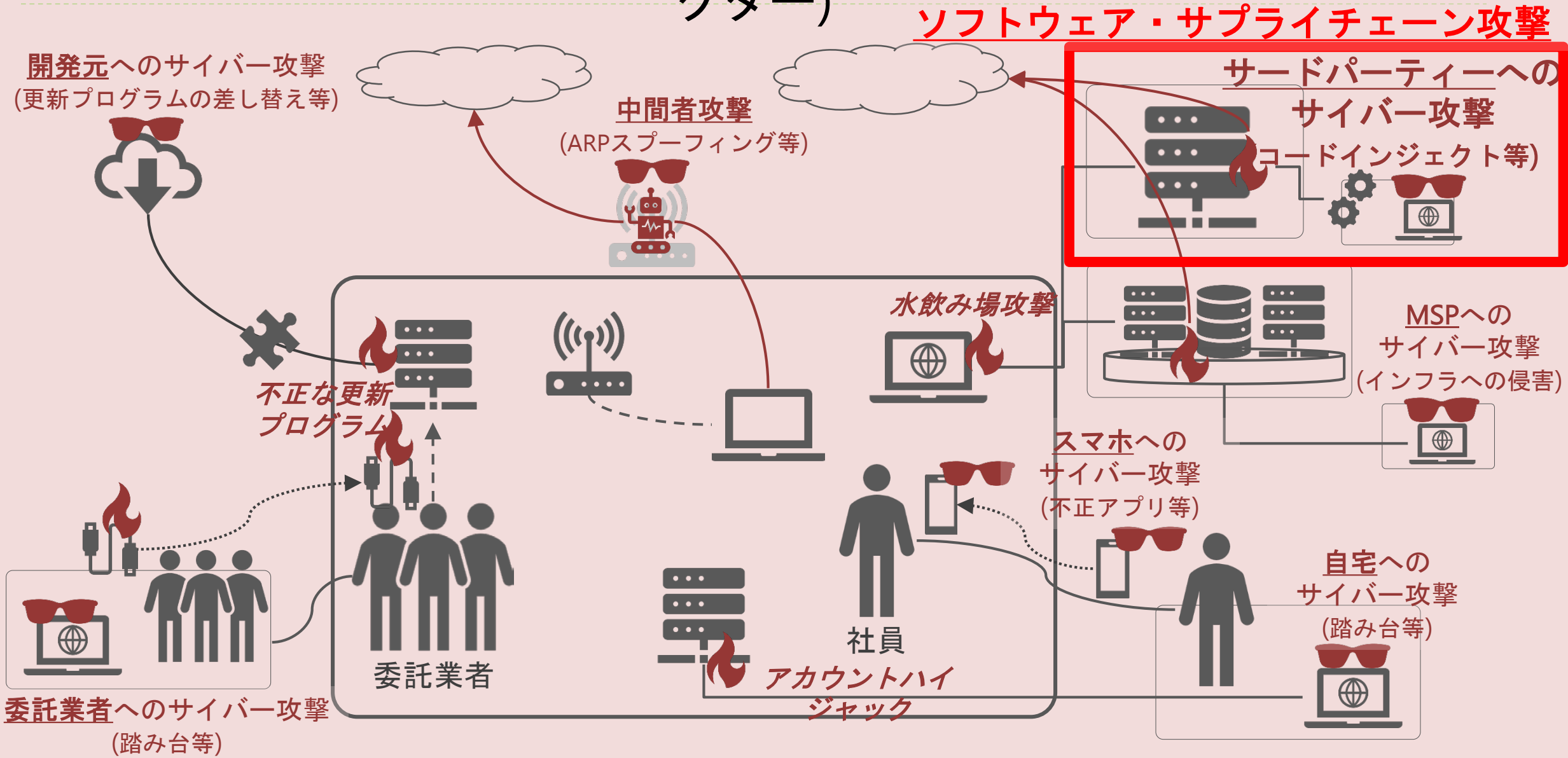
2018年「深刻な影響を発生させたサイバー攻撃」の外観（特に、ソフトウェア・サプライチェーン攻撃）

2018年 「深刻な影響を発生させたサイバー攻撃」の外観 (攻撃ベクター)



TLP:GREEN

2018年 「深刻な影響を発生させたサイバー攻撃」の外観 (攻撃ベクター)



TLP:GREEN

「ソフトウェア・サプライチェーン」の背景

- ソフトウェア開発は、さまざまな領域で推進されている**イノベーションに起因**する形、次の要求事項が強く求められています。
  - 開発スピード（プロセスの短縮）
  - 設計、開発、運用保守のコスト圧縮（低予算）
  - 高い安定性とスケーラビリティ
  - 高機能・多機能

- このような要求事項を満たすためには、**多種多様なオープンソースとして利用できるコンポーネントやツール**を利用する必要がある。
  - 無償でありながら、高い安定性のあるコンポーネント
  - 開発サイクル全体を自動化・最適化するツール

- オープンソースのコンポーネントやツールを利用する形態は、**それぞれの開発及び保守する主体が異なる**ため、ソフトウェアの開発及び運用におけるサプライチェーンであると見されている。

「ソフトウェア・サプライチェーン」のリスク

The 2018 State of the Software Supply Chain Report is here!

by Derek Weeks on September 25, 2018

Tags: 2018 State of the Software Supply Chain, ssc, State of the Software Supply Chain, devops, devsecops

Two months after we launched our 2017 report, we all learned that Equifax had been breached. The hackers attack vector was a known vulnerable open source component from the Apache Struts project.

The world changed, the conversations changed, but did we all change?

A series of high profile and devastating cyber attacks demonstrated that adversaries have the intent and ability to exploit, and in some cases plant, security vulnerabilities in the software supply chain. While Equifax was breached due to a Struts vulnerability, we also documented eight other Struts breaches this year. We also detailed a new battlefront of attacks on open source releases that impacted tens of thousands of developers.

https://blog.sonatype.com/2018-state-of-the-software-supply-chain-report

世間から注目を浴びた致命的なサイバー攻撃は、**敵対者がソフトウェアサプライチェーンのセキュリティ上の脆弱性を悪用**する意思と能力を持っていることを示した。

数万人の開発者に影響を与えた**オープンソースに対する攻撃**に対する新しい戦いを詳しく説明する。

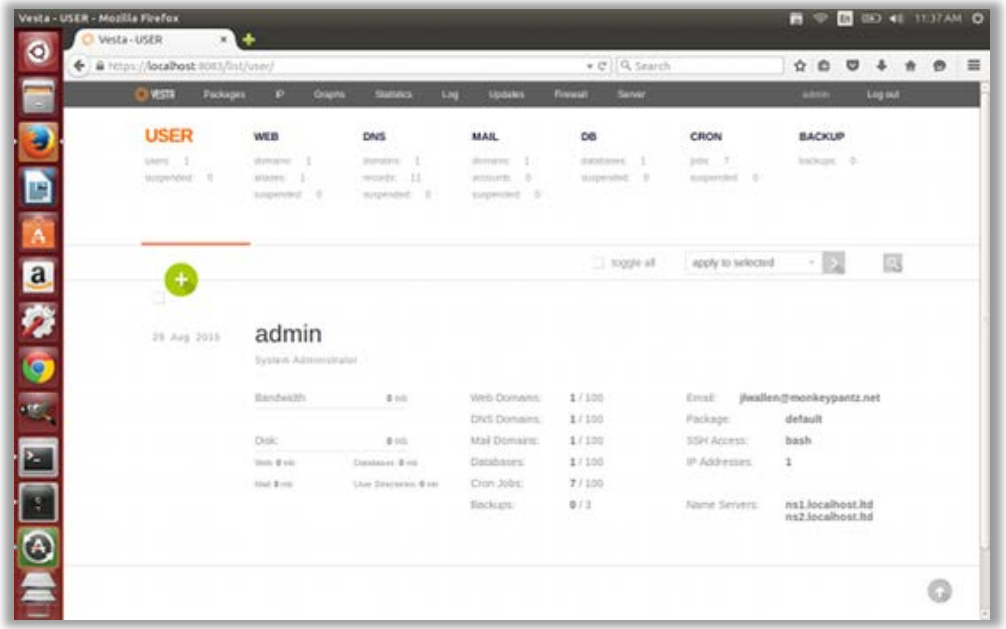
TLP:GREEN

2018年5月 サーバ用コントロールパネル「VestaCP」のスクリプト改ざん

- 2018年5月、サーバ用コントロールパネル「VestaCP (Vesta Control Panel)」の配布サーバに攻撃者が侵入してインストールスクリプトを改ざんし、ユーザがインストール時に作成した管理者(admin)の認証情報を攻撃者に通知する仕組みを構築していた。
- VestaCPの開発者Serghey Rodin氏は、「*この問題がいつ起きたのか正確には分かっていないが、修正されたインストールスクリプトは、5月31日から6月13日までGitHubのソースコード管理に表示されていた*」と証言。

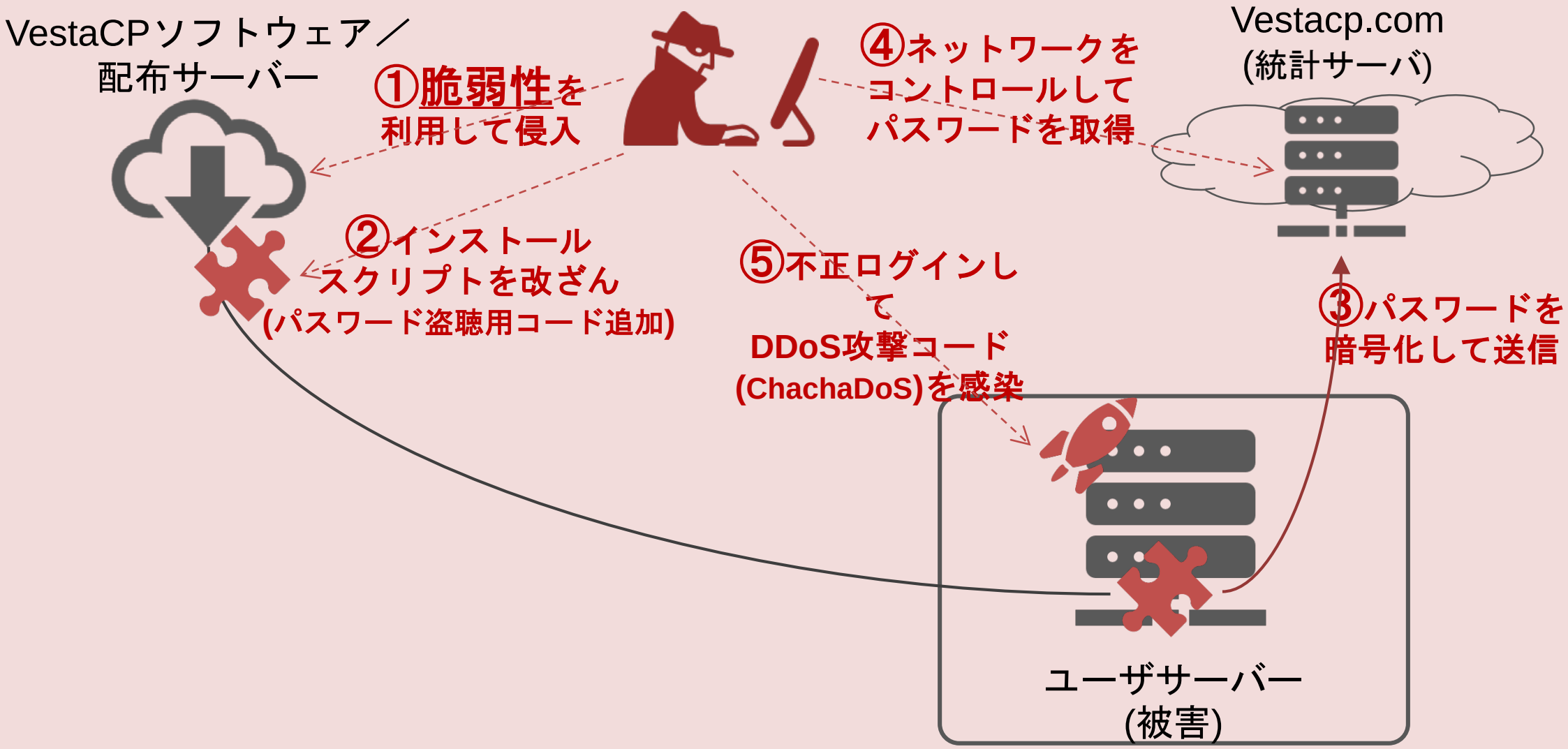
VestaCPとは：
- インストールが簡単なサーバ用コントロールパネル。
- インストーラーが、Apache と MySQLを個別にコンパイル。
- Web、DNS、データベース、メール、FTP、Nginx、SSL 認証、構成テンプレート、バックアップ、アップデート、監視、スパム監視、ウィルス監視、WHMCS(クライアント管理、課金システム) などを管理。

https://github.com/serghey-rodin



TLP:GREEN

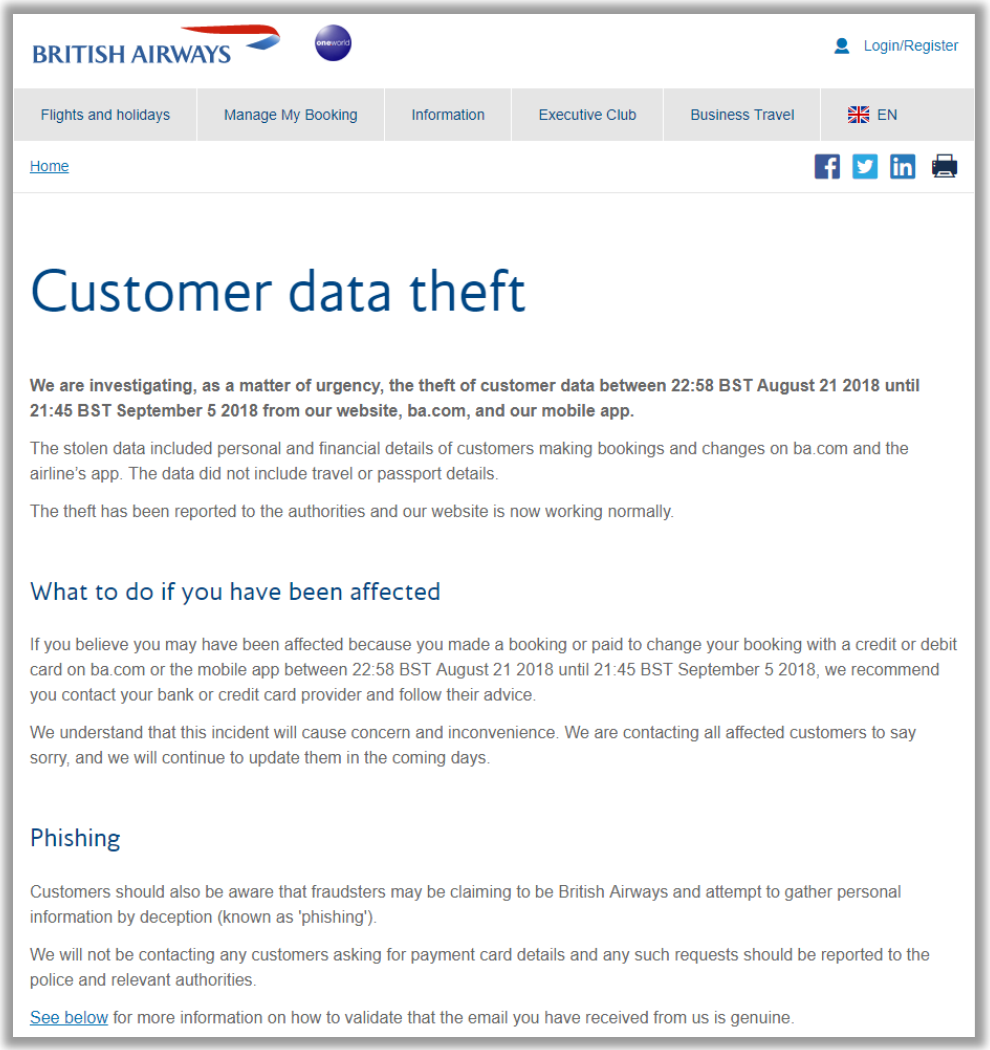
2018年5月 サーバ用コントロールパネル「VestaCP」のスクリプト改ざん



TLP:GREEN

2018年9月 不正スクリプトの埋め込みによる英国航空の顧客情報流出

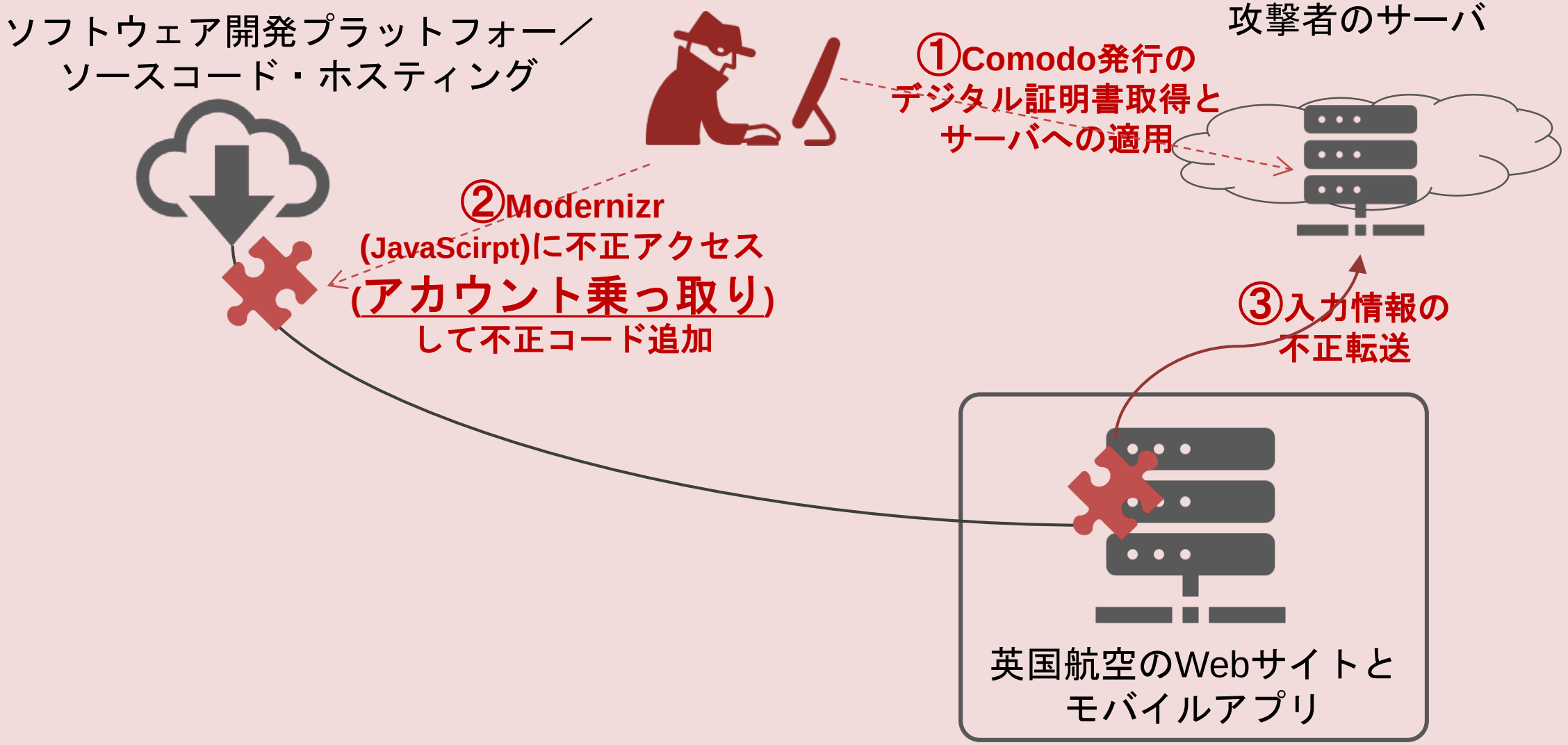
- 2018年9月6日、英航空会社ブリティッシュ・エアウェイズ(British Airways)が、同社の**ウェブサイトと携帯電話向けアプリで予約手続きをした顧客の個人情報と金融情報**が盗まれたと発表した。
  - 流出したデータは2018年8月21日から9月5日までに予約手続きをした顧客のもので、支払いに使われた銀行カードまたはクレジットカード38万件の情報を含む。
- この流出は、攻撃グループ「Magecart」によるものである可能性が高い。
  - Megecartグループは、オンラインストアをハッキングして、サイトにJavaScriptのコードを埋め込み、支払いフォームに入力されるあらゆる情報(クレジット番号、名前、住所など)を盗むことが得意。以前、Ticketmasterの決済カード情報流出にも関与したとされている。



https://www.britishairways.com/en-gb/information/incident/data-theft/latest-information

TLP:GREEN

2018年9月 不正スクリプトの埋め込みによる英国航空の顧客情報流出



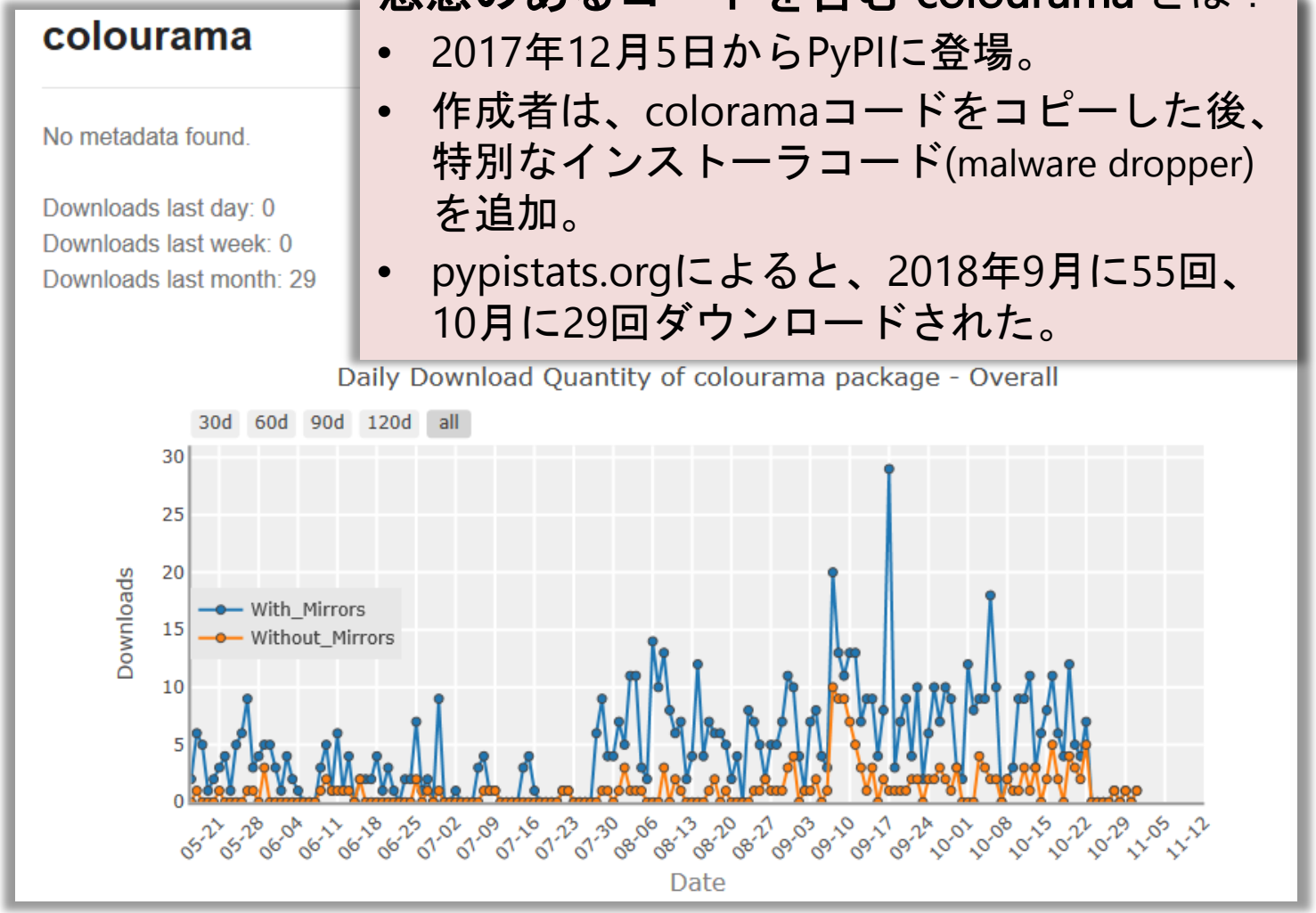
TLP:GREEN

2018年10月 仮想通貨を狙う悪質なPythonライブラリ (Colourama)

- 2018年10月、PythonのPyPIリポジトリに置かれていた悪意のあるコードを含むパッケージColouramaが発見された。
  - PyPIで人気のある正規パッケージColoramaのタイプミスのような名称であり、その正規パッケージのほとんどの正規機能を有していた。
- 主な機能は、ユーザがWindowsサーバにインストールするとVBSスクリプトを仕込み、仮想通貨の支払いを監視し、支払が発生するとウォレットアドレスを改ざんして仮想通貨を窃取する。

悪意のあるコードを含む colourama とは：

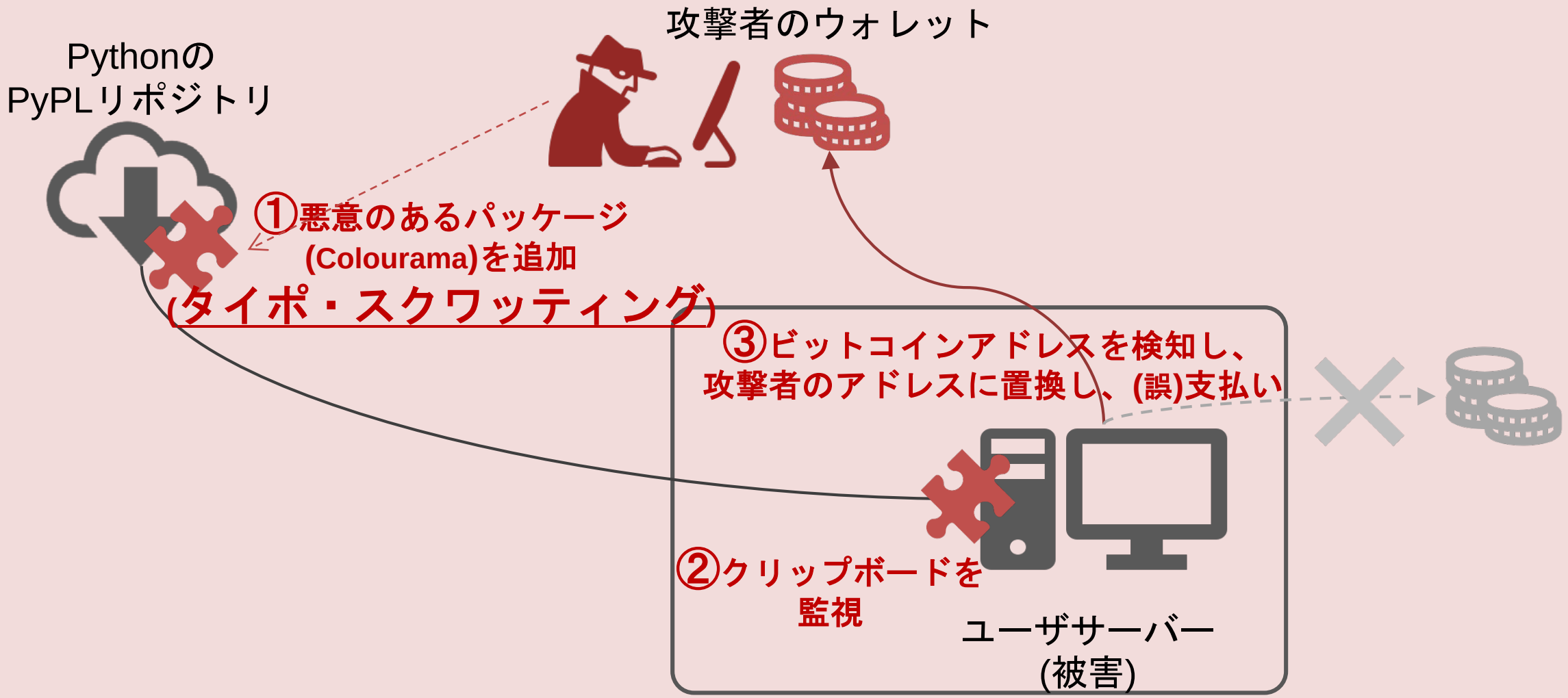
- 2017年12月5日からPyPIに登場。
- 作成者は、coloramaコードをコピーした後、特別なインストーラコード(malware dropper)を追加。
- pypistats.orgによると、2018年9月に55回、10月に29回ダウンロードされた。



https://pypistats.org/packages/colourama

TLP:GREEN

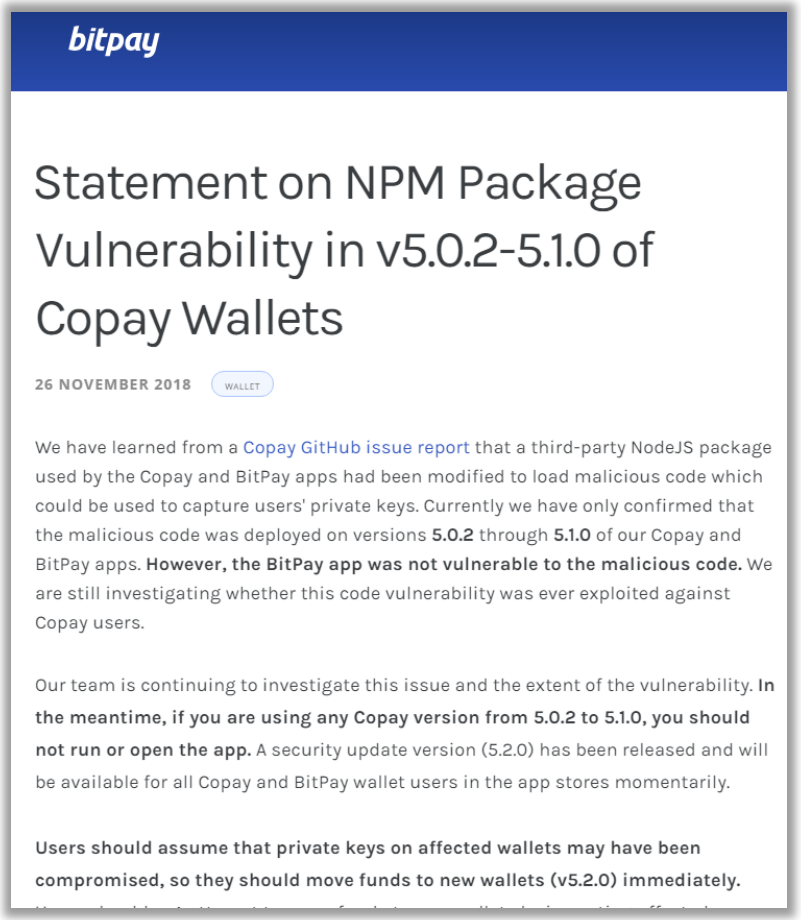
2018年10月 仮想通貨を狙う悪質なPythonライブラリ (Colourama)



TLP:GREEN

2018年11月 ビットコインの秘密鍵を狙う Node.js ライブラリ

- 2018年11月26日、ビットコインウォレットアプリを提供する米BitPayが、同社のアプリに使われているサードパーティーのNode.jsパッケージが改ざんされて不正なコードが仕込まれ、ユーザーの秘密鍵が流出した可能性があることが分かったと発表した。
  - 不正なコードは「Copay」「BitPay」のバージョン5.0.2～5.1.0で確認。
  - 不正なコードが仕込まれていたのは「Event-Stream」というNode.jsライブラリ。（npmリポジトリから1週間に200万以上もダウンロード）
- 2018年9月から10月にかけて、Event-Streamのメンテナンスを作者から引き継いだユーザーが、コードに手を加え、悪質なコードが仕込んだ。
  - 不正なコードは、仮想通貨ウォレットから暗号鍵を盗み出す機能。



bitpay

Statement on NPM Package Vulnerability in v5.0.2-5.1.0 of Copay Wallets

26 NOVEMBER 2018 WALLET

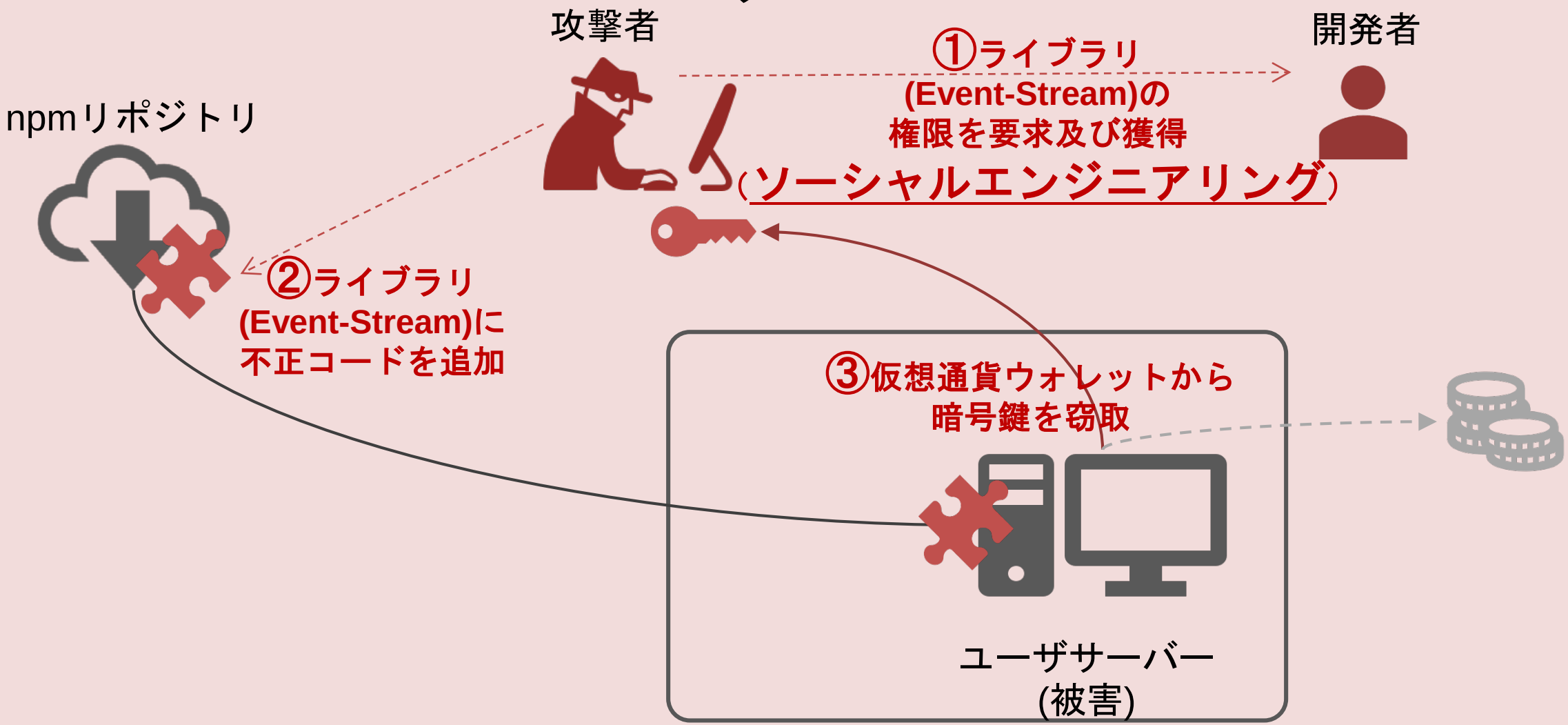
We have learned from a Copay GitHub issue report that a third-party NodeJS package used by the Copay and BitPay apps had been modified to load malicious code which could be used to capture users' private keys. Currently we have only confirmed that the malicious code was deployed on versions **5.0.2** through **5.1.0** of our Copay and BitPay apps. **However, the BitPay app was not vulnerable to the malicious code.** We are still investigating whether this code vulnerability was ever exploited against Copay users.

Our team is continuing to investigate this issue and the extent of the vulnerability. **In the meantime, if you are using any Copay version from 5.0.2 to 5.1.0, you should not run or open the app.** A security update version (5.2.0) has been released and will be available for all Copay and BitPay wallet users in the app stores momentarily.

Users should assume that private keys on affected wallets may have been compromised, so they should move funds to new wallets (v5.2.0) immediately.

https://blog.bitpay.com/npm-package-vulnerability-copay/

2018年11月 ビットコインの秘密鍵を狙う Node.js ライブラリ



TLP:GREEN

トピック２

現実的な対策(事態対処態勢)

現実的な対策

- サイバーセキュリティ事案に対する現実的な対策は、"情報(資産)"を対象とする「情報セキュリティ体制」ではなく、**"設備とプロセス"を対象とする「(サイバーセキュリティ)事案対処態勢」**を構築する必要がある。

	制御システム	情報(業務)システム
セキュリティの考え方	情報の機密性、完全性、可用性が侵害されても**設備**の健全性は維持	設備の健全性が侵害されても、**情報**の機密性、完全性、可用性は維持
価値創出資産	**設備**	**情報**
設備の位置づけ	主要資産	**情報**を保護するための支援資産
情報の位置づけ	**設備**を活用するための支援資産	主要資産

「情報セキュリティ体制」と「事案対処態勢」の違い

- 「情報セキュリティ体制」は管理策(Security Control)に基づいた各担当者の役割分担を重要視するが、**「事案対処態勢」は想定事案に相応する対処行動及びその能力維持を重要視**する。

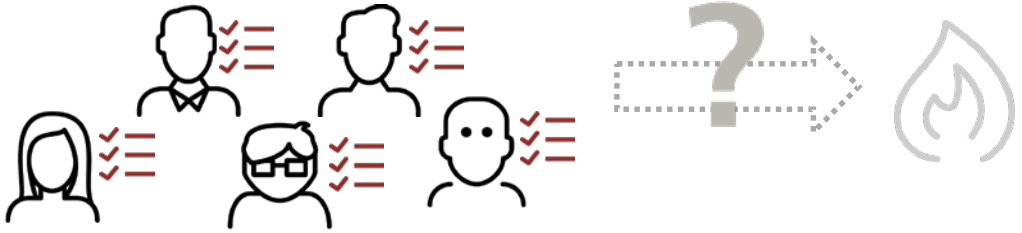
❖ 「態勢」と「体制」は、***取るべき準備行動***が大きく異なる。

– 態勢: 事態に対処するための準備ができている状態のこと。（前もっての身構え）

本当に事態対処できるかどうかが重要

– 体制: 基本原理・方針によって秩序づけられている組織のこと。（政治支配の様式）

組織内の役割分担（責任所在）が重要



「事案対処態勢」の構築のための重要ポイント（1）

- 全ての関係者が、**徹底的な状況認識(Situation Awareness)**を行うこと。

- インシデント発生時においてやり取りする**相手の顔**が見える
- やり取りにおいて必要となる**認識・教養の統一化**を図ることができる
- インシデントハンドリングの流れや**規定等の改善**を図ることができる
- **上層部の考え方**を把握することができる
- **発生した事例**を把握することができる

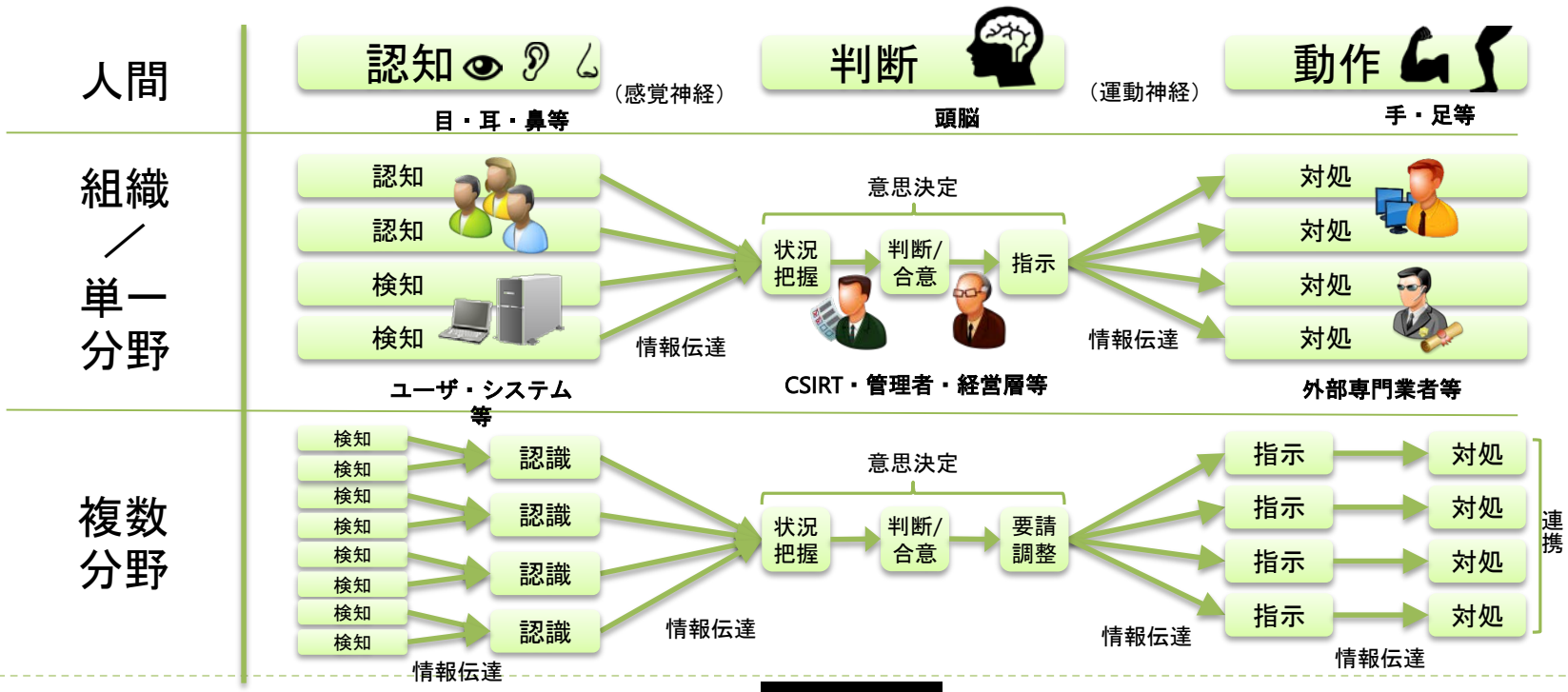
- 連絡先の**疎通確認**をすることができる(異動等による疎通不能の回避)
- サイバー脅威の**変動状況**に(ある程度)追いつくことができる
- メンバー間の**一体感**を感じることができる
- 潜在化した可能性のあるイベント(事象)を検知する**トリガー**となる
- **教養不足を補う**ことができる

TLP:GREEN

「事案対処態勢」の構築のための重要ポイント（2）

- 専任されたチームが、**検知(Detect)⇒トリアージ(Triage)⇒対処行動(Respond)**の各プロセスを確立及び実務能力の構築を行うこと。

  - 「人間の行動原理(認知⇒判断⇒動作)」をベースにして、「組織／単一分野」及び「複数分野」における**各フェーズ(認知検知⇒意思決定⇒対処)で実施される行動**を特定した上で、それを実現可能にする**能力スキルや情報・知見(ノウハウ)等**を見出し、実施可能な状況にしておくこと。



TLP:GREEN

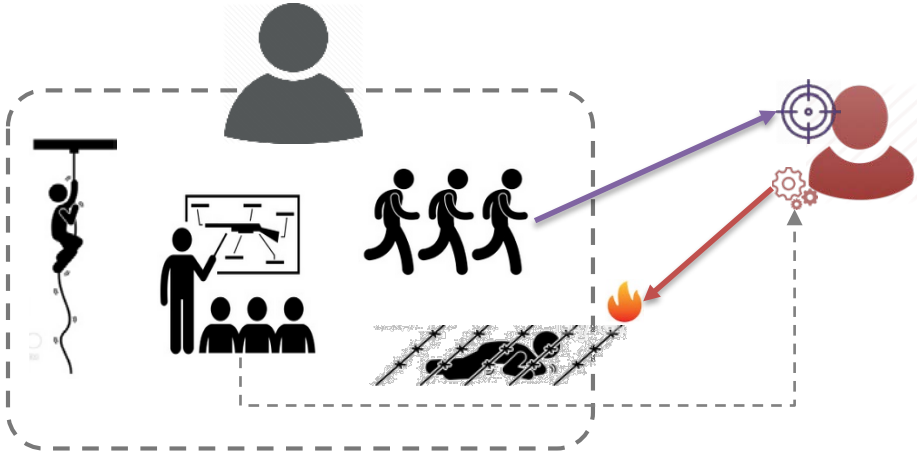
「事案対処態勢」の継続強化のためのアクションアイテム

- 状況認識(Situation Awareness)の共有や向上のために、サイバーセキュリティ事案への対処態勢関係者による定例会及び外部の専門家を招聘した**勉強会**を実施。

- 連絡体制の維持のために、定期的な**疎通確認訓練**(Communication Check Drill)或いは**電話会議**(Teleconference)を実施。

- 意思決定能力の向上及び最新の脅威動向の把握のために、脅威シナリオをベースにした**TTX**(Table Top Exercise; **机上演習**)を実施。

- メンバー間の**関係性強化**を図ることができる
- 教養に加え、**(擬似)経験**を積み上げることができる
- メンバー間で流通する情報に対する**関心が向上**する
- インシデントハンドリングや規定等の**具体的な改善点**を見出せる
- 全般的なインシデント対応に係る**時間を短縮**できる



TLP:GREEN

本資料に関する連絡先

名和 利男（Toshio NAWA）

SITE: https://www.nawa.to

PGP: 0xE38B4E01

TLP:GREEN