NTT DATA
Trusted Global Innovator

注目されているセキュリティ事故・事件に関する情報＜2019年3月版 (第28号)＞(選り抜き版)

2019年3月28日
ＮＴＴデータ先端技術株式会社
セキュリティ事業部

今回のサマリー

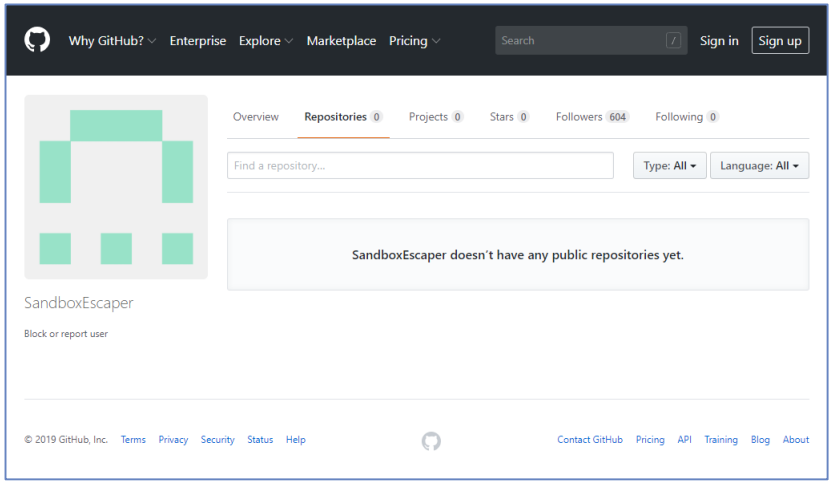
ゼロデイ脆弱性公開時の対策と脆弱性の取り扱いポリシーについて
2018年10月23日にSandboxEscaperと名乗る人物がWindows 10のゼロデイ脆弱性を公開しました。2019年3月時点で本脆弱性の対応方法は公開されていないため、ユーザは本脆弱性を悪用した攻撃によって被害を受ける可能性があります。本記事では、対応方法が公開されていない脆弱性情報を公開するリスクと、日本国内の脆弱性の取り扱いについて紹介するとともに、ゼロデイ脆弱性が公開されたときの対応方法についてご紹介します。

ゼロデイ脆弱性公開時の対策と脆弱性の取り扱いポリシーについて

1. SandboxEscaperによるゼロデイ脆弱性情報の公開

2018年10月23日に「SandboxEscaper」と名乗る人物が、TwitterとGitHubへWindows 10のゼロデイ脆弱性情報を公開しました。

2018/10/23 17:39の
@SandboxEscaperによるツイート
(2019年3月時点で削除されている)



SandboxEscaperのGitHub
(2019年3月時点でリポジトリが閲覧できなくなっている)
https://github.com/SandboxEscaper

本脆弱性は「MsiAdvertiseProductにおける権限昇格の脆弱性」としてJVNに登録・公開されています。2019年3月時点で、マイクロソフトからは本脆弱性を修正したアップデートや、本脆弱性を悪用した攻撃を受けた場合に被害を軽減する方法は公開されていません。そのため、**Windows 10 ユーザは本脆弱性への対応ができず、本脆弱性を悪用した攻撃によって被害によって被害を受ける可能性があります**。

2. ゼロデイ脆弱性情報の公開によるリスク (1/2)

脆弱性の発見者が対応方法が公開されていない(ゼロデイ)脆弱性の情報が公開した場合、攻撃者もその情報を知ることができるため、ユーザは攻撃者によるゼロデイ脆弱性を悪用したサイバー攻撃によって被害を受ける可能性があります。そのため、**アップデートなどの対応方法が公開された後に脆弱性情報が公開されるのがユーザにとって安全な順番といえます**。

OpenSSLのように、事前にアップデートの公開を予告することによって、ユーザが対応の準備を行うことができるようにしている例もあります。

2017年2月13日にOpenSSLのメーリングリストへ、重要度「High」の脆弱性を修正したバージョン1.1.0eを、3日後の2017年2月16日にリリースする予告が公開されました。予告通り、2017年2月16日に公開されたバージョン1.1.0eの更新情報には修正された脆弱性情報が掲載されています。

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Forthcoming OpenSSL release
===========================

The OpenSSL project team would like to announce the forthcoming release of
OpenSSL version 1.1.0e

This release will be made available on 18th February 2017 between 1200-1600
UTC, and will include a fix for a security defect classified as severity "High".
This issue does not affect OpenSSL versions prior to 1.1.0.

Please see the following page for further details of severity levels:
https://www.openssl.org/policies/secpolicy.html

Yours

The OpenSSL Project Team
```

OpenSSLメーリングリストのリリース予告
https://mta.openssl.org/pipermail/openssl-announce/2017-February/000095.html

CVE-2017-3733 (OpenSSL advisory) [High severity] 16 February 2017:

During a renegotiation handshake if the Encrypt-Then-Mac extension is negotiated where it was not in the original handshake (or vice-versa) then this can cause OpenSSL to crash (dependent on ciphersuite). Both clients and servers are affected. Reported by Joe Orton (Red Hat).

- Fixed in OpenSSL 1.1.0e (git commit) (Affected 1.1.0-1.1.0d)

バージョン1.1.0eで修正された脆弱性情報(CVE-2017-3733)
https://www.openssl.org/news/vulnerabilities.html#CVE-2017-3733

2. ゼロデイ脆弱性情報の公開によるリスク (2/2)

一方で、脆弱性の発見者がベンダや調整機関へ脆弱性情報を報告してから一定期間が経過しても対応方法が公開されない場合は、**脆弱性情報を公開するほうが社会全体の利益になるという考え方もあります**。これによって、ユーザは別のソフトウェアを使用するなどの対応を行なうことができます。

日本では、脆弱性の発見者が「脆弱性関連情報の非開示依頼の取り下げ」を申請することによって脆弱性情報を公開できます。

また、世界には発見や確認がされているものの、ベンダや調整機関に提供されておらず、一般に公開されていない脆弱性情報が存在します。これらの脆弱性は**ダークウェブ上での金銭取り引きや国家レベルのサイバー攻撃に用いられている可能性があります**。非公開の脆弱性を用いた攻撃による被害を防ぐため、HackerOneなどによるバグバウンティプログラム(脆弱性報奨金制度)によって、脆弱性情報を買い上げる施策も行われています。

3. 情報セキュリティ早期警戒パートナーシップガイドライン (1/3)

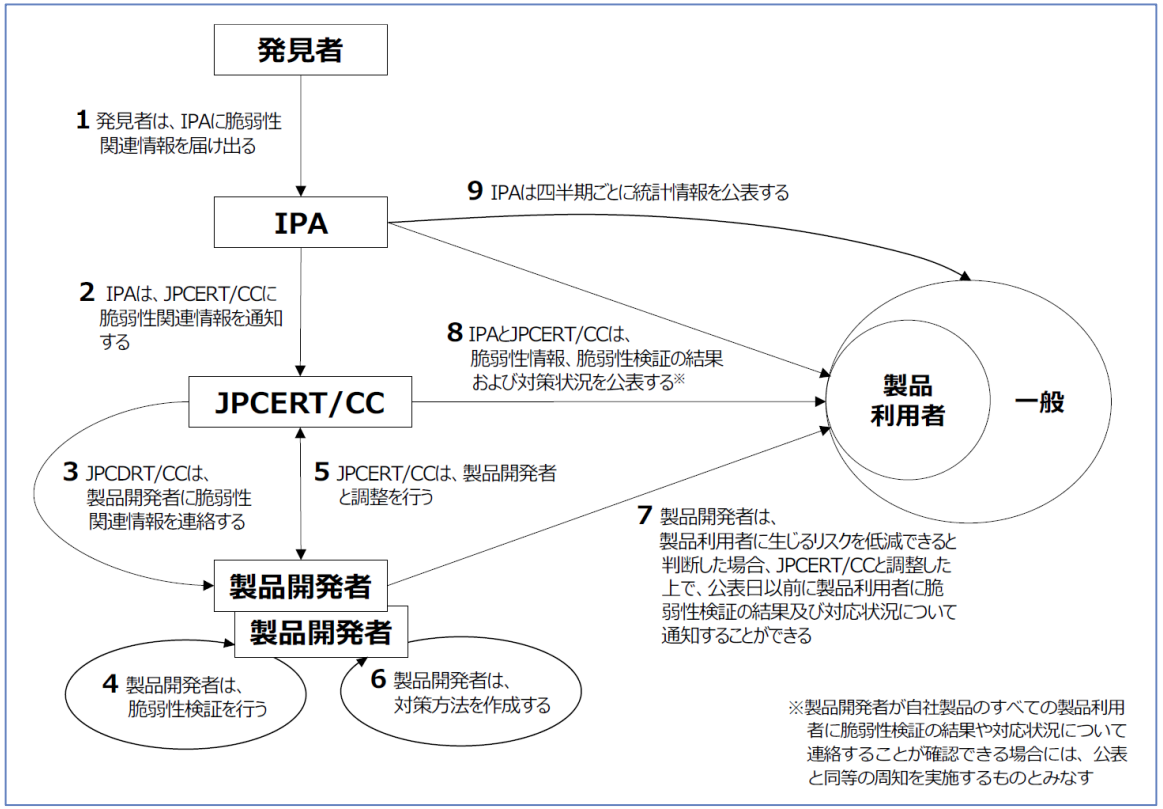
日本では、脆弱性情報を適切に流通させ、脆弱性の修正を促すための制度としてIPAから「情報セキュリティ早期警戒パートナーシップガイドライン」(以降「本ガイドライン」)が公開されています。

本ガイドラインはIPAによる「情報システム等の脆弱性情報の取扱いに関する研究会」が2004年に提言した「ソフトウエア等脆弱性関連情報取扱ガイドラインモデル案」をもとにしています。

情報セキュリティ早期警戒パートナーシップガイドライン
https://www.ipa.go.jp/security/ciadr/partnership_guide.html

3. 情報セキュリティ早期警戒パートナーシップガイドライン (2/3)

本ガイドラインの対象は、日本国内で利用されているソフトウェアとウェブアプリケーションの脆弱性情報です。脆弱性の発見者がIPAへ届け出ることで、IPAとJPCERT/CCが開発者へ脆弱性情報の提供を行い、ユーザへの対応方法の公開までを調整します。



ソフトウエア製品に係る脆弱性関連情報取扱の概要
(情報セキュリティ早期警戒パートナーシップガイドラインより)

3. 情報セキュリティ早期警戒パートナーシップガイドライン (3/3)

本ガイドラインは脆弱性を発見した者に対して、脆弱性情報をIPAへ指定の様式で届け出るとともに脆弱性情報を適切に管理することを要求しています。また、本ガイドラインは法的な論点として、脆弱性関連情報の管理および開示に際しての法的な問題についても触れています。

a) 脆弱性関連情報の公表は、その情報の内容が真実と異なることを知っていた場合、あるいは，真実である場合であっても、特定人の名誉を毀損する意図で公表がなされ、かつ、公共の利益と無関係である場合には、刑法の名誉毀損罪に触れる可能性があります。
b) 特定人の信用を毀損する意図で事実と異なる脆弱性関連情報を、事実と異なると認識して公表がなされる場合には、刑法の信用毀損罪に触れる可能性があります。
c) 通常人に求められる程度の相当の注意をもって調査・検証したりしたのではなしに脆弱性関連情報であるとして公表し、かつ、脆弱性関連情報の開示に起因して損害が発生した場合、損害賠償責任等の民事責任を追及される可能性があります。

脆弱性関連情報の管理および開示に際しての法的な問題
(情報セキュリティ早期警戒パートナーシップガイドライン 付録3より)

4. 脆弱性の取扱いに関する海外動向

ソフトウェアの脆弱性の取扱いについて、米国ではNIST(国立標準技術研究所)がSP800-40 「Guide to Enterprise Patch Management Technologies」を公開しています。また、国際標準としてISO/IEC 29147:2014とISO/IEC 30111:2013が規格化されています。

規格名	SP800-40 Guide to Enterprise Patch Management Technologies	ISO/IEC 29147:2014 Vulnerability disclosure	ISO/IEC 30111:2013 Vulnerability handling processes
対象	ITシステムを運用するすべての組織 • 脆弱性管理プログラムの設計と実施を担当するセキュリティ管理者 • パッチの適用やソリューションの導入を担当するシステム管理者や運用担当者	ソフトウェア製品に係わる者 • 製品開発者 • オンラインサービス事業者 (ウェブサイト運営者、クラウド事業者、ECモール事業者など) • 中間ベンダ(SIerやリセラーなど)	ソフトウェアを開発している者 • 製品開発者 • オンラインサービス事業者
規程範囲	パッチおよび脆弱性管理プロセス • パッチおよび脆弱性グループの設置 • システム管理者の責務 • システムインベントリの作成 • 脆弱性、修正措置、および脅威の監視 • 脆弱性に対する修正措置導入の優先順位付け • 組織固有の修正措置データベースの作成 • 修正措置のテスト • 脆弱性に対する修正措置の導入 • 管理者への脆弱性および修正措置の情報の配布 • 修正措置の検証 • 脆弱性に対する修正措置のトレーニング パッチおよび脆弱性管理のセキュリティメトリクス策定と実施 • NIST SP 800-55 を使ったセキュリティメトリクスの実施 • メトリクスの策定 • メトリクスプログラムの実施	脆弱性公開ポリシーの策定 • 最低限のポリシー要件 脆弱性情報の受信 • 脆弱性情報の安全な受信 • 脆弱性情報の受領確認 • 報告者とのコミュニケーション • コーディネーターからの支援 アドバイザリの公開 • アドバイザリ公開のタイミング • アドバイザリの項目 • アドバイザリの信頼性 (このほか、ISO/IEC 30111との関係も解説されている)	脆弱性ハンドリングのポリシー策定 • 脆弱性ハンドリングのポリシー • ベンダーのCSIRTとPSIRT • 製品開発部門の責務 • カスタマーサポート部門の責務 • 法律相談 脆弱性ハンドリングのプロセス策定 • 脆弱性ハンドリングのプロセス • プロセスのモニタリング • 脆弱性情報の機密性

SP800-40 と ISO/IEC 29147:2014 と ISO/IEC 30111:2013の概要

5. ゼロデイ脆弱性が公開されたときの対応 (1/4)

ゼロデイ脆弱性が公開されたとき、または公開され得る状況に備えて、脆弱性対応を行う組織が実施するべき対応の例をご紹介します。

1．事前の備え

多くのユーザに使われているソフトウェアの中でも**脆弱性情報の公開が頻繁または定期的に行われるソフトウェアは攻撃・被害を受けるリスクが高くなります**。使用しないソフトウェアはアンインストールする、無効化する、または最初からインストールしないなどの対策が必要です。

インターネット上の攻撃動向は、システムが攻撃を受けるリスクの度合いを測り、インシデント発生時の対応の緊急性を検討する際に役立ちます。警察庁はインターネット定点観測や特定の攻撃に関する統計情報を公開しています。これらの統計情報はポート番号やプロトコル別となっていますが、これらのプロトコルに対応しているソフトウェアを使用している際にはシステムは攻撃を受けるという前提でリスクを評価できます。

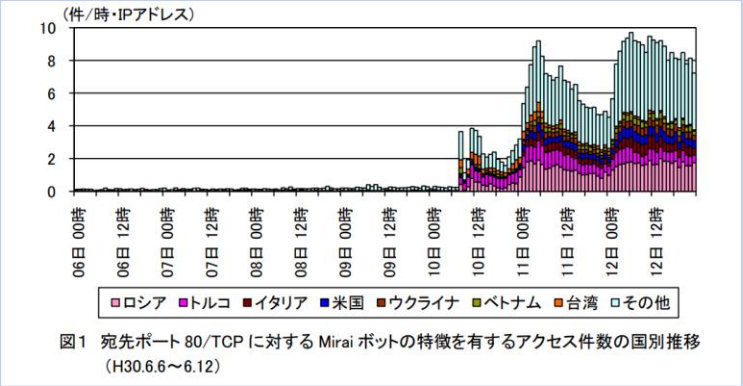


図1　宛先ポート 80/TCP に対する Mirai ボットの特徴を有するアクセス件数の国別推移
（H30.6.6～6.12）

警察庁@Police 宛先ポート80/TCPに対するMiraiボットの特徴を有するアクセスの増加について より
https://www.npa.go.jp/cyberpolice/detect/pdf/20180613.pdf

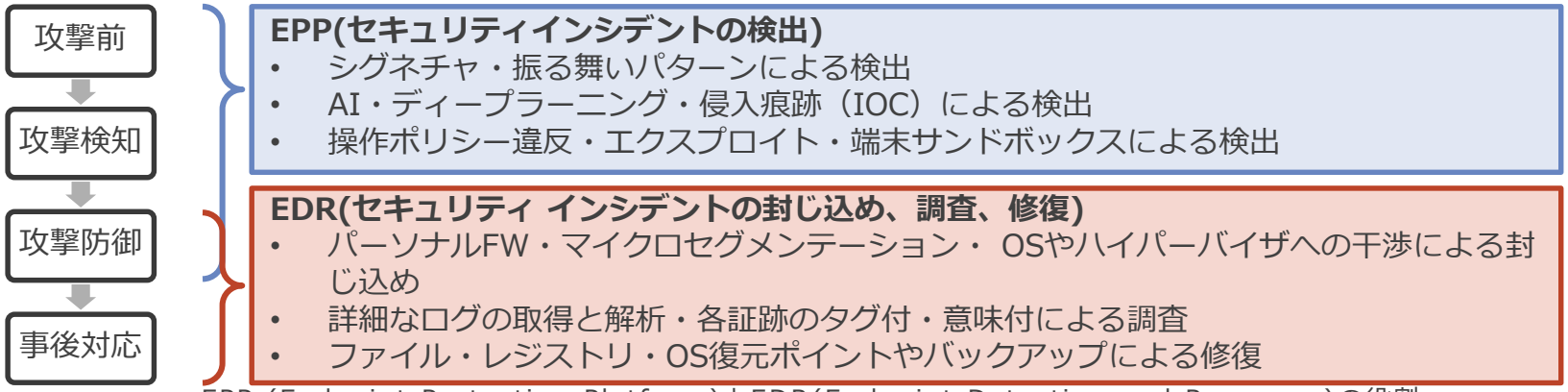
5. ゼロデイ脆弱性が公開されたときの対応 (2/4)

1．事前の備え(続き)

また、資産管理を行い、システムに導入されている製品を掌握しておくことが重要です。脆弱性情報が公開されたときに、システムへの対応の必要有無を迅速に判断できます。

さらに、EPP (Endpoint Detection and Response)の導入によるインシデントの検出に加えて、EDR (Endpoint Protection Platform)を導入し被害範囲の封じ込め、攻撃・被害調査や修復をできるようにしておきます。

EDR製品の中には資産管理の機能を持つものもあります。



EPP (Endpoint Protection Platform)とEDR(Endpoint Detection and Response)の役割

5. ゼロデイ脆弱性が公開されたときの対応 (3/4)

2. 継続的な情報収集と迅速な対応判断

脆弱性情報は公開された後も状況によって内容が更新されることがあります。例えば、脆弱性の発見時は深刻度が低いため対応が不要であったとしても、深刻度が高くなり対応が必要になる可能性があります。このため、継続的な情報収集によって対応の要否を柔軟に判断することが重要です。特にゼロデイ脆弱性は初出の情報が少なく信頼性が低い傾向にあり、更新が行われる前提で対応する必要があります。

対応判断のために入手するべき情報の例

- 脆弱性情報
  - 製品名称
  - バージョン
  - 脆弱性によって想定される影響
  - 脆弱性の深刻度評価(CVSS)
  - 脆弱性の影響を軽減する方法
- 製品ベンダやセキュリティベンダの技術情報
  - 製品ベンダによる脆弱性の一次情報
  - セキュリティ製品の定義ファイルやシグネチャの公開有無
  - 脆弱性を悪用した攻撃の発生状況

5. ゼロデイ脆弱性が公開されたときの対応 (4/4)

3．組織内への注意喚起

ユーザが対応できるように、入手した情報をもとに組織内のユーザへ注意喚起の周知をします。

注意喚起に記載する対応方法の例

- 組織としての対応方法や対応予定期日
  - 集中管理による自動アップデートの有無
    (ユーザによる手動アップデートの必要有無)
  - 集中管理をしているクライアントへの対応予定日
  - 未対応クライアントへの検疫ネットワーク隔離開始日
  - 公開サーバへの対応報告有無
- 対象となるソフトウェアの情報
  - 製品名称
  - バージョン
  - 脆弱性の影響を受ける設定
- 対応方法
  - 脆弱性の影響を軽減する方法
  - ソフトウェアの使用停止や代替ソフトウェアの使用
- 攻撃を受けた際の確認方法

6. まとめ

ゼロデイ脆弱性情報は発見者、調整機関やベンダなどが適切に管理しないと、脆弱性を悪用した攻撃が発生するリスクがあります。
SandboxEscaperによるゼロデイ脆弱性の公開は、発見者がゼロデイ脆弱性情報を適切に管理していない行為であると言えます。

日本では、情報セキュリティ早期警戒パートナーシップガイドラインによって脆弱性情報の取り扱いが定められています。ソフトウェアの脆弱性の取扱いはISO規格にもなっています。
さらに、HackerOneなどのバグバウンティプログラムによって脆弱性情報の発見やベンダへの通知を促進する活動が行われています。

一方、ソフトウェアの利用者側は、ゼロデイ脆弱性情報が公開された際には攻撃を受ける可能性を踏まえて対応する必要があります。
資産管理による所有製品の掌握や、継続的な情報収集と対応判断だけでなく、EDR導入などの事前の備えが必要です。対応方法が分かり次第、ユーザへの注意喚起し、被害を軽減できるようにすることが重要です。

7. 参考URL

- JVNVU#92357871 MsiAdvertiseProduct における権限昇格の脆弱性
  https://jvn.jp/vu/JVNVU92357871/index.html
- 情報セキュリティ早期警戒パートナーシップ
  https://www.ipa.go.jp/security/ciadr/partnership_guide.html
- 情報システム等の脆弱性情報の取扱いに関する研究会 報告書
  https://www.ipa.go.jp/security/fy15/reports/vuln_handling/index.html
- NIST SP 800-40 Rev. 3 Guide to Enterprise Patch Management Technologies
  https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final
- パッチおよび脆弱性管理プログラムの策定(NIST SP 800-40 Version 2.0の翻訳)
  https://www.ipa.go.jp/files/000025330.pdf
- ISO/IEC 29147:2014 Vulnerability disclosure
  https://www.iso.org/obp/ui/#iso:std:iso-iec:29147:ed-1:v1:en
- ISO/IEC 30111:2013 Vulnerability handling processes
  https://www.iso.org/obp/ui/#iso:std:iso-iec:30111:ed-1:v1:en
- HackerOne
  https://www.hackerone.com/
- 警察庁 @police インターネット情勢
  https://www.npa.go.jp/cyberpolice/detect/index_top.html
- 修正プログラム提供前の脆弱性を悪用したゼロデイ攻撃について
  https://www.ipa.go.jp/security/virus/zda.html

NTT DATA

Trusted Global Innovator