

注目されているセキュリティ事故・事件に関する情報 ＜2021年12月版（第39号）＞（選り抜き版）

2021年12月23日
NTTデータ先端技術株式会社
セキュリティ事業本部

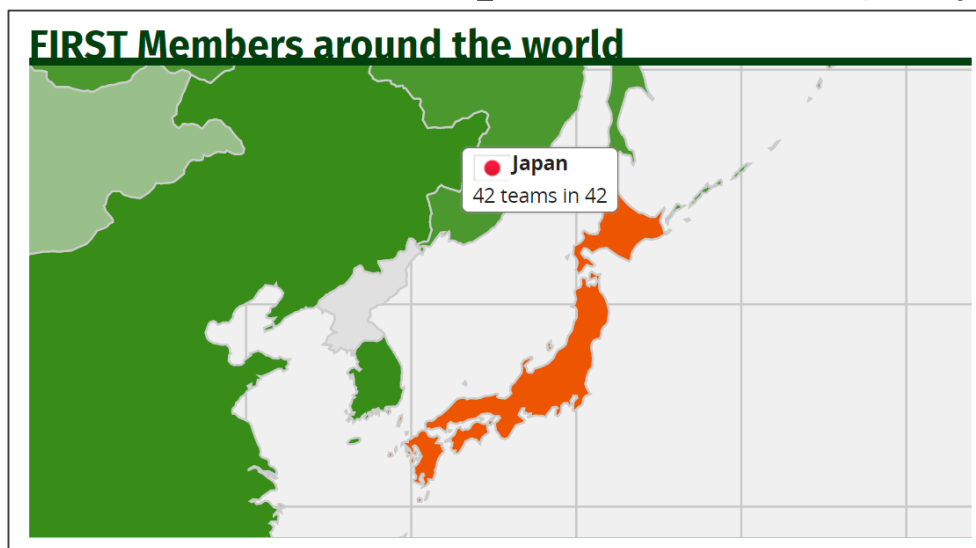
CSIRTなどのセキュリティ対応チームの倫理規範「EthicsfIRST」

日本シーサート協議会は、FIRSTが公開した文書EthicsfIRST(インシデント対応およびセキュリティチームのための倫理規範)の日本語版を公開しました。本記事では、CSIRTなどのセキュリティ対応チームを対象とした倫理ガイドラインであるEthicsfIRSTを解説します。

CSIRTなどのセキュリティ対応チームの 倫理規範「EthicsfIRST」

1. FIRSTについて

FIRST(Forum of Incident Response and Security Teams)は、**世界中のセキュリティ対応チーム(CSIRTやPSIRT、セキュリティ研究者)が集まるコミュニティ**です。セキュリティに関する情報交換やインシデントレスポンスに関する協力関係を構築する目的で、1990年に米国CERT/CCなどが中心となって設立されました。加盟チーム数は世界で604チームあり、そのうち**日本のチームは42チーム加盟しています**(2021年12月5日時点)。FIRSTは、目的に応じて特定のテーマを議論するSIG(Special Interest Groups)の活動や、年次カンファレンス「FIRST Conference」などのイベントを開催しています。



出展 : FIRST Members around the world

<https://www.first.org/members/map#country%3AJP>

(世界地図で日本をクリックすると日本のチーム数とチーム名の一覧が表示される)

2. EthicsfIRST概要



出展 : EthicsfIRST: Ethics for Incident Response and Security Teams

<https://ethicsfirst.org/>

EthicsfIRST(Ethics for Incident Response and Security Teams)はFIRSTのEthics SIGが作成した文書であり、2020年10月21日に公開されました。EthicsfIRSTは、**セキュリティ対応チームがインシデント対応をするにあたって、チームのメンバ全員の倫理的な行動を奨励するガイドライン**となる内容が記載されています。

日本のCSIRTコミュニティである日本シーサート協議会は、2021年8月27日に有志のチームが翻訳し、JPCERT/CCとNTT-CERTがレビューしたEthicsfIRSTの日本語訳を公開しました。**EthicsfIRSTの日本語訳はFIRSTのWebサイトで公開されています。**

3. EthicsfIRSTの「義務」(1/2)

EthicsfIRSTは、以下の12項目の「義務(Duty) ※¹」で構成されています。これらの項目は**ICTが信頼されるためにも重要であり、セキュリティ対応チームのメンバだけでなく、技術者に対しても広く当てはまる**倫理規範であると言えます。

#	義務	概要
1	信頼性の義務	信頼はチーム間の多くの関係の基礎であり、有意義な情報交換が行われるために必要とされる。
2	協調的な脆弱性開示の義務	利害関係者と協力してセキュリティ脆弱性を修正し、開示に伴う損害を最小限に抑える必要がある。脆弱性に対して、ユーザがリスクを評価して防御策をとれるような十分な詳細情報を提供すべきである。
3	機密保持の義務	情報に指定されているTLP※ ² などの情報の共有範囲を守ることによって機密性を保持する必要がある。
4	受領確認を返信する義務	外部の機関から情報を受け取った際に、受領確認だけでもよいのでタイムリーに返答する必要がある。
5	認可についての義務	責任範囲を理解し、アクセスを許可されたシステムでのみ行動する正当な必要性和権利がある。

※¹ 「必須事項」ではなくRFC2119が定義している「SHOULD」や「RECOMMENDED」と同じレベルの「推奨事項」であると注釈されています。

※² Traffic Light Protocol 機微情報の共有範囲を定めた基準

3. EthicsFIRSTの「義務」 (2/2)

#	義務	概要
6	情報を提供する義務	セキュリティ上の脅威やリスクについてコンスティチュエンシーに情報を提供し続けることを義務と認識する。
7	人権を尊重する義務	インシデント対応の過程で個人の機微情報にアクセスすることになるため、自分たちの行動が他者の人権に影響を与える可能性があることを認識すべきである。
8	チームの健康に対する義務	チームはメンバの身体的・精神的な健康を支え、健康的で安全かつ前向きな職場環境を維持するよう努めるべきである。
9	チームの能力に対する義務	チームはメンバが技術的かつ科学的知識を学んで発展させるためのリソースを提供すべきである。
10	責任ある収集の義務	インシデント対応の目的とデータの利害関係者を尊重し、収集および抽出したデータは適用される法律に従い、プライバシーを尊重して取り扱わなければならない。
11	管轄区域の境界を認識する義務	管轄区域の境界は国や居住地などの物理的な場所などによって決定される場合がある。メンバはプライバシー規則などの要件をはじめ、関係する管轄区域に影響を与える重要な問題を認識しておくべきである。
12	根拠のある推論の義務	チームは検証可能な事実に基づいて活動すべきである。

4. 「ジレンマ」への対処

EthicsFIRSTには、前述の12項目の「義務」を守ると何も行動できなくなってしまう場合において、セキュリティ対応チームのメンバーが考慮すべき点を解説した「ジレンマへの対処」が付録として記載されています。

12項目の義務のいずれかを守れない場合でも、**インシデント対応を前に進めるためには影響を考慮しながら行動をする事が重要**であるとしています。

チームメンバーは**倫理原則の全てを満たすような行動が何もない状況に陥**ることがよくある。そのような状況では、どの原則を優先すべきかを選択しなければならない。この状況において、インシデントハンドラーには、**自分たちの行動によってどの利害関係者がどのような影響を受けるか**について、できれば同僚との話し合いの中で検討することが望まれる。原則として、**この倫理規範のフレームワークに反するものを最小限に抑える解決策を選択すべき**である。時には、外部からの圧力などによって、それが不可能な場合もあるかもしれない。そのような状況では、**倫理的ジレンマに注意しながら、不承不承でも前に進める**ことが推奨される。

出展：インシデント対応およびセキュリティチームのための倫理規範

https://ethicsfirst.org/FIRST_EthicsFIRST_jp.pdf

(赤太字は解説のために修飾)

5. 義務を守らない場合の影響 (1/3)

12項目の義務のうち、いずれかの項目が守られなかった場合には重大なセキュリティインシデントが発生すると考えられます。本項では義務を守らなかった事が原因と考えられる、実際に発生したセキュリティインシデントを紹介します。

#	義務	概要
2	協調的な脆弱性開示の義務	利害関係者と協力してセキュリティ脆弱性を修正し、開示に伴う損害を最小限に抑える必要がある。脆弱性に対して、ユーザがリスクを評価して防御策をとれるような十分な詳細情報を提供すべきである。

脆弱性の発見者が「協調的な脆弱性開示の義務」を守らずに、脆弱性情報を開示する行為は、**脆弱性の対象となる製品のベンダの対応が取られるまでの間はゼロデイ脆弱性となり、攻撃者によって製品への攻撃行われ、被害が発生する**と考えられます。

実際に、Windowsインストーラのローカル昇格特権の脆弱性「CVE-2021-41379」の発見者がPoCコードを2021年11月21日に公開し、この脆弱性を悪用するマルウェアがセキュリティベンダによって確認されています※。

※参考：Windows 10、11などのゼロデイ脆弱性、パッチ公開前に報告者が概念実証コード公開
<https://www.itmedia.co.jp/news/articles/2111/25/news089.html>

5. 義務を守らない場合の影響 (2/3)

#	義務	概要
1	信頼性の義務	信頼はチーム間の多くの関係の基礎であり、有意義な情報交換が行われるために必要とされる。
4	受領確認を返信する義務	外部の機関から情報を受け取った際に、受領確認だけでもよいのでタイムリーに返答する必要がある。

あるプロダクトのベンダが外部から脆弱性情報を受け取った際に「受領確認を返信する義務」を守らない場合、その対応はベンダの信頼に関わり、**脆弱性に対する対応が十分に行われなくなる**可能性があります。

実際に、AppleのiOSのゼロデイ脆弱性が、こっそりと修正されていたと脆弱性を報告したセキュリティ研究者が暴露する事態となりました※。Appleはバグ報奨金プログラムを実施していますが、セキュリティ研究者はバグ報奨金の支払いはなく、放置されたとしています。

※参考：Appleが「iOS 15.0.1」でロック画面をバイパスできてしまう脆弱性を修正、しかしバグ報奨金を支払っていないとの指摘
<https://gigazine.net/news/20211002-apple-patched-ios-lock-screen-bypass/>

5. 義務を守らない場合の影響 (3/3)

#	義務	概要
6	情報を提供する義務	セキュリティ上の脅威やリスクについてコンスティチュエンシーに情報を提供し続けることを義務と認識する。

コンスティチュエンシー※に対してセキュリティ上の脅威やリスクの提供されない場合、**セキュリティインシデント発生時の対応が遅れ、被害が発生・拡大する**可能性があります。

#	義務	概要
9	チームの能力に対する義務	チームはメンバが技術的かつ科学的知識を学んで発展させるためのリソースを提供すべきである。

インシデント対応体制や対応能力が十分ではなく、**CSIRTが十分に機能しない**場合、インシデント発生時の対処・対応が遅れることで被害が発生・拡大し、更に終息に長い期間を要すると考えられます。

※ constituency 「活動範囲」と訳され、CSIRTがサービスを提供する対象(守る対象である人やシステムなど)を指します。

6. まとめ

EthicsfIRSTは世界中のセキュリティ対応チームのコミュニティであるFIRSTが作成し、インシデント対応に際してチームメンバ全員の倫理的な行動を奨励するガイドラインとなるように設計されています。

ひとつのチームやひとりのメンバのみがEthicsfIRSTを遵守すればよいものではなく、世界中のセキュリティ対応チームがEthicsfIRSTをもとに行動指針を定めることで、コミュニティで協働してインシデント対応を行えることがセキュリティの向上や発展に繋がります。

EthicsfIRSTの内容はICTが信頼されるためにも重要であり、セキュリティ対応チームのメンバだけではなく技術者に対しても広く当てはまる倫理規範であると言えるため、職業倫理の観点で一読をお勧めします。

7. 参考URL

- EthicsfIRST: Ethics for Incident Response and Security Teams
<https://ethicsfirst.org/>
- EthicsfIRST インシデント対応およびセキュリティチームのための倫理規範
https://ethicsfirst.org/FIRST_EthicsfIRST_jp.pdf
- FIRST launches new code of ethics for incident response and security teams on Global Ethics Day
<https://www.first.org/newsroom/releases/20201021>
- FIRST Members around the world
<https://www.first.org/members/map#country%3AJP>
- 活動内容 | CSIRT - 日本シーサート協議会
<https://www.nca.gr.jp/ttc/ethicsfIRST.html>
- ITmedia NEWS : Windows 10、11などのゼロデイ脆弱性、パッチ公開前に報告者が概念実証コード公開
<https://www.itmedia.co.jp/news/articles/2111/25/news089.html>
- Gigazine : Appleが「iOS 15.0.1」でロック画面をバイパスできてしまう脆弱性を修正、しかしバグ報奨金を支払っていないとの指摘
<https://gigazine.net/news/20211002-apple-patched-ios-lock-screen-bypass/>

