

OWASP Nagoya Chapterミーティング第33回  
OWASP 758 Day



# 脆弱性対応におけるデータソースと検討方法

(公開用修正版)



2024年02月10日  
フューチャー株式会社  
CyberSecurityInnovationGroup  
井上圭

「未知の情報セキュリティ脅威に備えるために」というテーマを頂いたので、企業等の脆弱性管理における「未知の脅威に備えるために」という視点で話します。

学生の方は、システムや企業のサービスはどのように脅威に備えているのか、という視点で見ていただければと思います。

## 1. そもそも脅威とは何か

- 脅威に関する理解を深める

## 2. 脅威に対する対応

- 認識されていない脆弱性による脅威への備え
  - ✓ ASM, SBOMなどでの備え
- 脆弱性は認識されたが、自組織への影響が未知の脅威
  - ✓ CVSS, EPSS, KEV Catalog等、使えるデータと使い方

## 3. まとめ



本資料は Creative Commons CC BY-NC-SA 4.0 DEEDの範囲で利用してください。

- 原作者のクレジット（氏名、作品タイトルなど）を表示し、かつ非営利目的に限り、また改変を行った際には元の作品と同じ組み合わせのCCライセンスで公開することを主な条件に、改変したり再配布したりすることができるCCライセンス。
- 資料の独り歩き防止の処置です
- <https://creativecommons.jp/licenses/>

！覚えておこう！

右下のTLPとは

- TRAFFIC LIGHT PROTOCOL
- [https://www.first.org/tlp/docs/v2/tlp-v2\\_ja.pdf](https://www.first.org/tlp/docs/v2/tlp-v2_ja.pdf)
- 情報受信者に適用される情報共有の境界を示します。

# (about TLP)

- a. **TLP:RED** = 受信者個人の目と耳に向けた共有に限られ、その先の公開はない。対象となる情報は関係組織のプライバシー、評判、または業務に重大なリスクを生み、第三者の手に渡ることによって効果的に作用しない場合には、情報の発信者は TLP:RED を使用してよい。そのため、情報の受信者は、TLP:RED 情報を他の誰にも共有してはならない。例えば会議を想定すると、TLP:RED 情報は、その会議に出席した者に限られる。
- b. **TLP:AMBER** = 限定公開、情報の受信者は Need to know の原則に基づき、組織内やそのクライアントにのみ共有できる。**TLP:AMBER+STRICT** は、ある組織のみに共有を限定する。対象となる情報は第三者の手に渡り効果的に作用することが求められるが、同時に関係組織外に共有されるとプライバシー、評判、または業務に対するリスクが生じる場合には、情報の発信者は TLP:AMBER を使用してよい。情報の受信者は、自組織とその組織のクライアントを保護し、更なる被害を防ぐためなら、Need to know の原則に基づき、自組織の構成員とその組織のクライアントに TLP:AMBER 情報を共有してもよい。備考：情報の発信者が共有範囲を一組織のみに限定したいのであれば、TLP:AMBER+STRICT を指定しなければならない。
- c. **TLP:GREEN** = 限定公開、情報の受信者はコミュニティ内に情報を共有できる。対象となる情報が、より広いコミュニティで認知度が上がることが有用な場合には、情報の発信者は TLP:GREEN を使用してよい。情報の受信者は、コミュニティ内の仲間とパートナー組織に TLP:GREEN 情報を共有してもよいが、公にアクセス可能な手段を介してはならない。TLP:GREEN 情報は、コミュニティ外には共有してはならない。備考：「コミュニティ」が定義されていない場合は、サイバーセキュリティや防衛のコミュニティを指すと想定すること。

- d. **TLP:CLEAR** = 情報の受信者は、全世界に向けて情報を共有できる。公開に制限はない。情報の発信者は、対象となる情報が誤用されるリスクが最小限または想定されない場合に、一般公開に適用される規定と手順に従って TLP:CLEAR を使用してよい。標準的な著作権保護の規定に則り、TLP:CLEAR 情報は制限なく共有してよい。

## 2. 自己紹介

井上圭

### ■ フューチャー株式会社

- サイバーセキュリティイノベーショングループ (CSIG)
  - ✓ シニアコンサルタント

### ■ 業務概要

- セキュリティコンサルタント
- 脆弱性管理製品FutureVuls 営業、サポート、トレーニング
- JNSA, ISOG-J, NCA 加盟
- 講演等：脆弱性管理や運用についての話
  - ✓ NICT サイバーコロッセオ, CodeBlue OpenTalks, Janog52, InternetWeek2023, OWASP Capter, NCA AnnualConference etc
- 勉強会主催
  - ✓ 脆弱性対応勉強会、Vuls祭り etc

### ■ 経歴

- (本資料では割愛)





…と、その前に。

# 長野日報ランサムウェア被害の話

2023-12-19にランサムウェアに感染し、21日紙面から大幅にページ数削減がされていました。  
2023-01-25に、02月中旬目途で復旧する見込みが立ったようです。

- 市民に目に見える形で被害が出た
  - 21日はページ数が半減し、8ページしか提供されなかったようだ。
- 業務再開にあたり、同業他社との連携で紙面は作られているようです
- 一般市民に目に見える被害が出た事例、といえるかもしれません

これも「未知の情報セキュリティ脅威」といえるかもしれません。

- （自分にとっての）未知の脅威
- （IT業界にとっての）既知の脅威

The screenshot shows the Nagano Nippo Web homepage. At the top, there's a navigation bar with categories like 社会 (Society), 地域 (Local), 経済 (Economy), 行政・政治 (Administration & Politics), 文化 (Culture), スポーツ (Sports), 八面観 (Eight Views), and 御柱祭 (Gojushiki Festival). Below the navigation bar, there's a main content area with a headline: 「おわび（サーバーウイルス感染のため特別紙面）」 (Apology (Special Paper Due to Server Virus Infection)). The text below the headline states that on December 19th, the company's server was infected with a ransomware (ransomware), leading to a significant reduction in the number of pages published on December 21st. It also mentions that the company is working on restoring the service and that the number of pages will be gradually increased. To the right of the main content area, there's a sidebar with various links and information, including 「長野日報社からのお知らせ」 (Notice from Nagano Nippo Shisha), 「フォトサービス」 (Photo Service), 「諏訪湖マラソン」 (Suwa Lake Marathon), 「第35回諏訪湖マラソン記録」 (35th Suwa Lake Marathon Record), 「長野日報ご購入」 (Purchase Nagano Nippo), 「長野日報就職研究会」 (Nagano Nippo Job Research Association), 「長野日報社員募集」 (Nagano Nippo Employee Recruitment), 「アクセスランキング」 (Access Ranking), and a list of recommended articles.

<http://www.nagano-np.co.jp/articles/119535>

本題へ…



# 3. 「脅威」とは何か

「未知の情報セキュリティ脅威に備えるために」というテーマでお話します。  
何かの話をする場合、言葉の定義を再確認しておいたほうが良いことが多いです。



…そもそも「脅威」とは何でしょうか。

- 今回の話題の範囲では、事業継続に対するリスク（事業リスク）、といえると思います。
  - リスクは、目的に対する不確かさの影響をいう。ある事象の結果とその発生の起こりやすさとの組み合わせとして表現されることが多い
    - ✓ ref: 政府機関等の対策基準策定のためのガイドライン 令和3年度版
    - ✓ 事業継続という目的に対する、不確かさへの影響度合い（継続を困難にする影響）

- リスク、とは
  - 脅威と脆弱性と資産価値のかけ合わせで評価されます。

リスク

=

脅威

×

脆弱性

×

資産価値

今回はから「未知の事業リスクに備える」という方向で話をします。

<https://www.nisc.go.jp/policy/group/general/kijun.html>

表 3-2 事業リスクの種類

#	事業リスクの種類 Impacts per Category
①	利用者に不便、苦痛を与える、又は事業を所管する機関等が信頼を失う Potential impact of inconvenience, distress, or damage to standing or reputation:
②	利用者に金銭的被害を与える、機関等に賠償責任が生じるなど財務上の影響を与える Potential impact of financial loss:
③	機関等の活動計画や公共の利益に対して影響を与える Potential impact of harm to agency programs or public interests:
④	利用者の個人情報などの機微な情報が漏洩する Potential impact of unauthorized release of sensitive information:
⑤	利用者の身の安全に影響を与える Potential impact to personal safety:
⑥	法律に違反する The potential impact of civil or criminal violations is:

(出典) NIST SP 800-63-3 「Digital Identity Guidelines (電子的認証に関するガイドライン)」より作成



## 4. 「未知の脅威」とは何か

同様に、「未知の脅威」について定義を考えてみましょう。

「未知」がどこにあるのか、という点が重要だと思われます。

今回は情報セキュリティの脅威という話なので、「脆弱性とその影響」ということを考えてみようと思います。

その場合は、以下が「未知」になるかと思います。

- 脆弱性それ自体が「未知」
- 脆弱性が自組織のどの部分に影響するのか、影響範囲が「未知」

この2つについてもう少し考えます



## 4.a. 未知の脆弱性

いわゆる「0day」など、ある日突然発見される脆弱性が該当します。

- 発見されるまでは、その脆弱性にはだれも気が付かないので、安全とされている
- 発見されることで、突然「脆弱性がある状況」になる

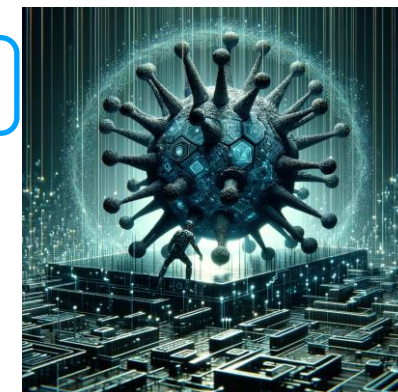
そもそも、脆弱性はCVE-IDが付くものだけとは限らず、更新するだけで修正されるものでもない場合があります。

- パッケージの脆弱性は、ベンダの更新プログラム/パッチで改善できることが多い
  - アップデートのチェックと適用が対策になる
- WEB系の脆弱性の場合、作り込みにより発生するため、更新では改善できない
  - WEB診断をし、自分で作ったプログラム/WEBアプリ部分を改修する必要がある

備えが重要です

対策は攻撃可能面を減らすことで、リスクを減らすことになります。

- ASM, 攻撃者の情報, MitreATT&CKを考慮したリスク低減



## 4.a.i. ASM (Attack Surface Management)

攻撃者視点で、攻撃を受ける面（Attack Surface）を考え、露出を最小限に抑えることでリスクを減らします。

- 守るべき資産へのアクセス経路などを整理し、管理していく
  - インターネットから直接アクセスできる機器は、どの程度あるのか
    - ✓ すべて管理できているのか、管理外でインターネットに接続されていないか
  - クラウドの設定は適切なのか
    - ✓ アカウントや多要素認証などの保護設定、公開設定ミスや過大な権限付与など
    - ✓ = CSPM (Cloud Security Posture Management; クラウドセキュリティ態勢管理)



ネットワークスキャンを行う、DNSによる追跡を行う、Shodanのようなスキャナを使う、などがあります。

- 考え方
  - 攻撃を受ける面積を減らし、そもそも攻撃を受けにくくする/管理できる状況にする
- どのように使えるか
  - 資産管理（アカウントやホストなど）、監視対象の明確化

## 4.a.ii. 攻撃者の情報

既に知られている攻撃者グループの攻撃手法を活用することで、同じような攻撃を防ぐことができる可能性があります。

- 例えば、MITRE ATT&CK®のCTIやTechniquesなどを参照する
- とはいえ検討するのは難しいので、あまり活用されていない

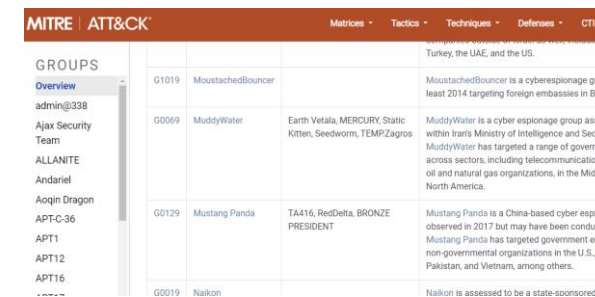
未知の攻撃を、既知の攻撃の知見で防ごうという考え方です。

- 考え方

- 攻撃者グループごとによく利用する手法があるので、それらへの対策をする（検出等の準備）

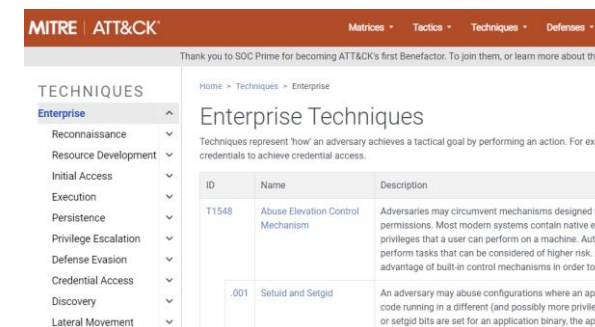
- どのように使えるか

- 既に行われた攻撃手法を基に、検出や防御の方針を決め、同じ手法で攻撃されても影響が発生しないようにする



The screenshot shows the MITRE ATT&CK Groups page. On the left, there is a sidebar with a list of groups including admin@338, Ajax Security Team, ALLANITE, Andarief, Aqin Dragon, APT-C-36, APT1, APT12, and APT16. The main content area displays a table of groups with columns for ID, Name, Aliases, and Description. The table lists groups like MoustachedBouncer, MuddyWater, Mustang Panda, and Naikon, each with a brief description of their activities and targets.

ID	Name	Aliases	Description
G0109	MoustachedBouncer		MoustachedBouncer is a cyberespionage group least 2014 targeting foreign embassies in Belarus, the UAE, and the US.
G0069	MuddyWater	Earth Vetal, MERCURY, Static Kitten, Seedworm, TEMPZagros	MuddyWater is a cyber espionage group active within Iran's Ministry of Intelligence and Security. MuddyWater has targeted a range of government and non-governmental organizations, including telecommunications, oil and natural gas organizations, in the Middle East and North America.
G0129	Mustang Panda	TA416, RedDelta, BRONZE PRESIDENT	Mustang Panda is a China-based cyber espionage group observed in 2017 but may have been conducting operations since 2010. Mustang Panda has targeted government entities, non-governmental organizations in the U.S., Europe, Pakistan, and Vietnam, among others.
G0019	Naikon		Naikon is assessed to be a state-sponsored cyber espionage group.



The screenshot shows the MITRE ATT&CK Techniques page. On the left, there is a sidebar with a list of technique categories including Enterprise, Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, and Lateral Movement. The main content area displays a table of techniques with columns for ID, Name, and Description. The table lists techniques like T1548 (Abuse Elevation Control Mechanism) and T1001 (Setuid and Setgid), each with a brief description of the technique.

ID	Name	Description
T1548	Abuse Elevation Control Mechanism	Adversaries may circumvent mechanisms designed to control permissions. Most modern systems contain native elevation control mechanisms that a user can perform on a machine. Adversaries may perform tasks that can be considered of higher risk. An advantage of built-in control mechanisms is that they are often not easily bypassed.
T1001	Setuid and Setgid	An adversary may abuse configurations where an application code running in a different (and possibly more privileged) context can perform actions that the application binary is not intended to perform.

MITRE ATT&CK: <https://attack.mitre.org/>

## 4.a.iii. CYBER KILL CHAIN

攻撃者が目的を達成するためのフェーズを7段階で分類したものです。  
この攻撃段階の途中で止めることで、目的を達成させないことを意図しています。

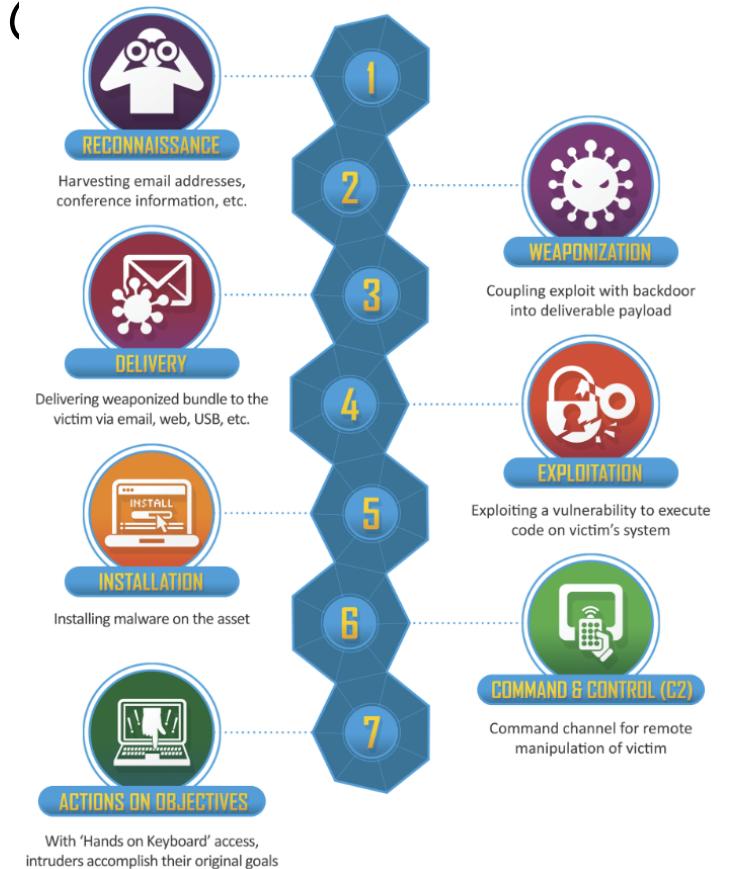
- 同じような思想、これをさらに進めたものもあるが、まずは基礎として Lockheed Martin Cyber Kill Chain®から始めるのが良い
- MITRE ATT&CK®でも同様に、TACTICSで実装されている

- 考え方

- 攻撃のフェーズを理解し、最終目的に達成させない戦略を考える

- どのように使えるか

- 現状で実装しているセキュリティ対策の過不足の確認をし、リスクに対しどこまで費用をかけるか、リスクを許容するかを検討する



<https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>



# MITRE | ATT&CK®

## TACTICS

### Enterprise

- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

Mobile

ICS

## Techniques

ID	Name	De
T1659	Content Injection	Ad sys we col col an
T1189	Drive-by Compromise	Ad Wi col
T1190	Exploit Public- Facing Application	Ad Th
T1133	External Remote Services	Ad Re ne/ cre usi
T1200	Hardware Additions	Ad or rer int
T1566	Phishing	Ad ele spi

## Cyber Kill Chain

1. RECONNAISSANCE
2. WEAPONIZATION
3. DELIVERY
4. EXPLOITATION
5. INSTALLATION
6. COMMAND & CONTROL(C2)
7. ACTIONS ON OBJECTIVE



v.s.

こちらでは、詳細なtechniques等の記載はないため、考え方を示しているのみといえる。



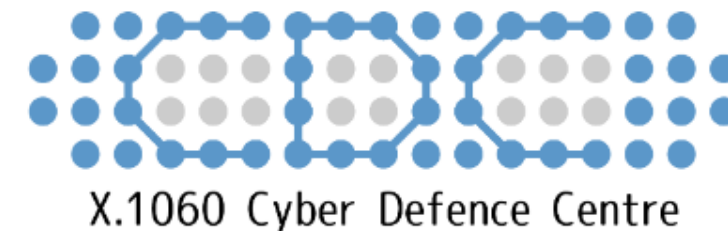
## 4.a.iv. 組織組成

そもそもの、未知の脅威による攻撃によるインシデントが発生したとして、迅速に回復できる組織を作り被害低減を目指すことも必要です。



ITU-Tの勧告として提供されている

X.1060 Framework for the creation and operation of a cyber defence centre



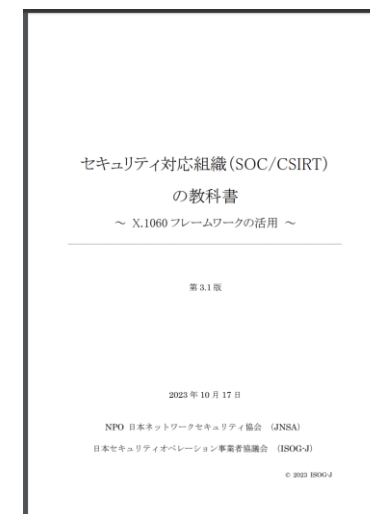
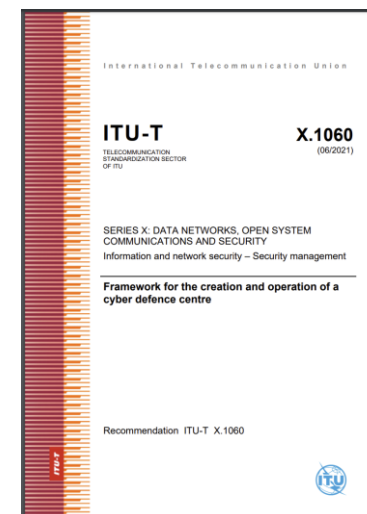
で、組織の現状を確認し、レジリエンスを高めることで脅威に対応することも重要です。

- 考え方

- 攻撃のフェーズを理解し、最終目的に達成させない戦略を考える

- どのように使えるか

- 現状で実装しているセキュリティ対策の過不足の確認をし、リスクに対しどこまで費用をかけるか、リスクを許容するかを検討する



<https://www.itu.int/rec/T-REC-X.1060-202106-I>

[https://www.ttc.or.jp/document\\_db/information/view\\_express\\_entity/1423](https://www.ttc.or.jp/document_db/information/view_express_entity/1423)

## X.1060概要

- ISOG-Jセキュリティ対応組織の教科書をITU-Tで議論し、X.1060として採用された
- 日本語版として、一般社団法人 情報通信技術委員会（TTC）から“JT-X1060 サイバーディフェンスセンターを構築・運用するためのフレームワーク”として日本語版が出ている
- X.1060で採用される際に、各国の状況に合うように一部変更された。それを取り入れた同教科書の3.0/3.1版が出ている。近日、3.2版を出す予定。
- SOC/CSIRTがどのような活動をすべきか、をサービスリストという形で示している。
- 各機能の詳細は、各国により異なる環境なので、X.1060の方では定義されていない。

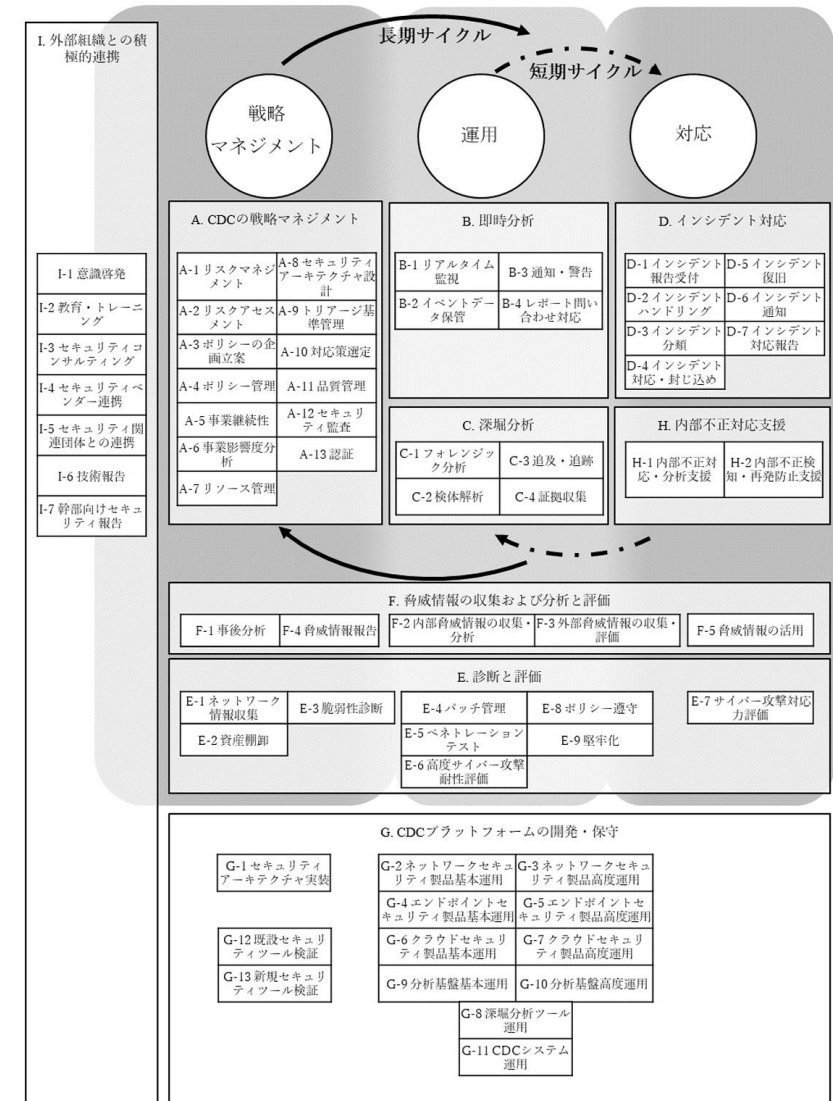


図 8 CDC サービスカテゴリー

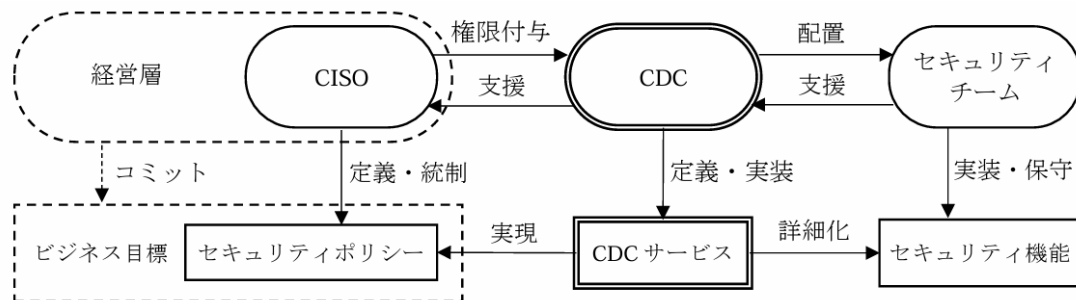


図 1 CDC の運営における関係者とその役割

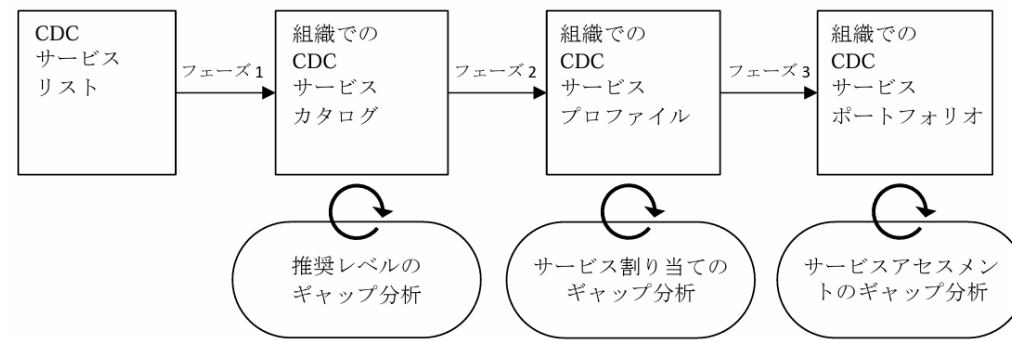


図 7 CDC 評価プロセス

### セキュリティ専門スキルの必要性

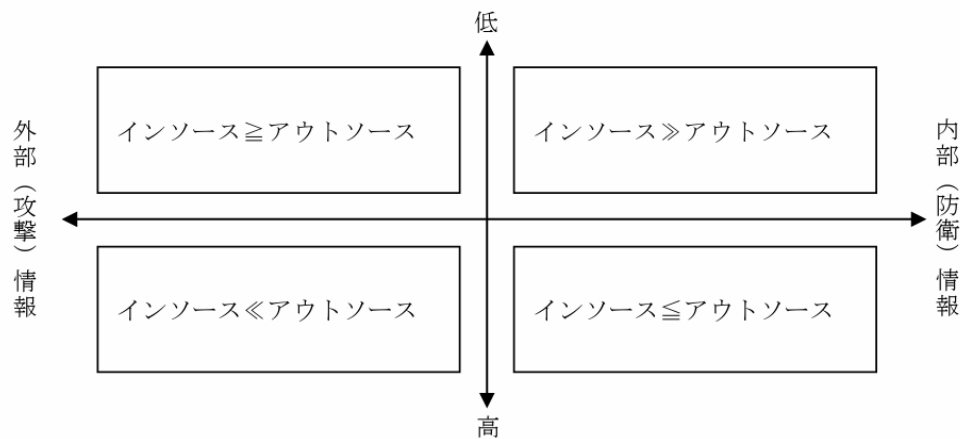


図 5 調達の象限

表 4 CDC サービスリスト

A	CDC の戦略マネジメント	F	脅威情報の収集および分析と評価
A-1	リスクマネジメント	F-1	事後分析
A-2	リスクアセスメント	F-2	内部脅威情報の収集・分析
A-3	ポリシーの企画立案	F-3	外部脅威情報の収集・評価
A-4	ポリシー管理	F-4	脅威情報報告
A-5	事業継続性	F-5	脅威情報の活用
A-6	事業影響度分析	G	CDC プラットフォームの開発・保守
A-7	リソース管理	G-1	セキュリティアーキテクチャ実装
A-8	セキュリティアーキテクチャ設計	G-2	ネットワークセキュリティ製品基本運用
A-9	トリアージ基準管理	G-3	ネットワークセキュリティ製品高度運用
A-10	対応策策定	G-4	エンドポイントセキュリティ製品基本運用
A-11	品質管理	G-5	エンドポイントセキュリティ製品高度運用
A-12	セキュリティ監視	G-6	クラウドセキュリティ製品基本運用
A-13	評価	G-7	クラウドセキュリティ製品高度運用
B	即時分析	G-8	環境分析ツール運用
B-1	リアルタイム監視	G-9	分析基盤基本運用
B-2	イベントデータ保管	G-10	分析基盤高度運用
B-3	通知・警告	G-11	CDC システム運用
B-4	レポート問い合わせ対応	G-12	既設セキュリティツール検証
C	情報分析	G-13	新規セキュリティツール検証
C-1	フォレンジック分析	H	内部不正対応支援
C-2	検体解析	H-1	内部不正対応・分析支援
C-3	追及・追跡	H-2	内部不正検知・再発防止支援
C-4	証拠収集	I	外部組織との連携的連携
D	インシデント対応	I-1	意思伝達
D-1	インシデント報告受付	I-2	教育・トレーニング
D-2	インシデントハンドリング	I-3	セキュリティコンプライアンス
D-3	インシデント分類	I-4	セキュリティベンダー連携
D-4	インシデント対応・対応済み	I-5	セキュリティ関連関係との連携
D-5	インシデント復旧	I-6	技術報告
D-6	インシデント通知	I-7	幹部向けセキュリティ報告
D-7	インシデント対応報告		
E	動向と評価		
E-1	ネットワーク情報収集		
E-2	資産情報		
E-3	脆弱性診断		
E-4	パッチ管理		
E-5	ペネトレーションテスト		
E-6	高度サイバー攻撃的性評価		
E-7	サイバー攻撃対応力評価		
E-8	ポリシー遵守		
E-9	電率化		

## このセクションのまとめ

### ■ 脆弱性それ自体が「未知」 今までの話は、ここ

- ASM : 攻撃される対象を減らす
- 攻撃者の情報 : 攻撃方法の認識
- CYBER KILL CHAIN : 守り方の検討
- 組織構成 : レジリエンスを高める

### ■ 脆弱性が自組織のどの部分に影響するのか、影響範囲が「未知」

- これからお話しします

あと、  
VDP(Vulnerability  
Disclosure Program)  
も重要です。  
善意の報告者を味方に  
つけましょう。

VDPの参考資料として、脆弱性対応勉強会のVDP回を置いておきます。

<https://zeijyakuseitaioukenkyukai.connpass.com/event/305932/>

<https://github.com/hogehuga/vulnRespStudyGroup/tree/master/studySession/vulnStudyExp07-vdp>

## 4.b. 未知の影響範囲

未知の脆弱性に対する対応の対として、脆弱性自体は認識できたが自組織の影響が未知である、という状況について考えます。

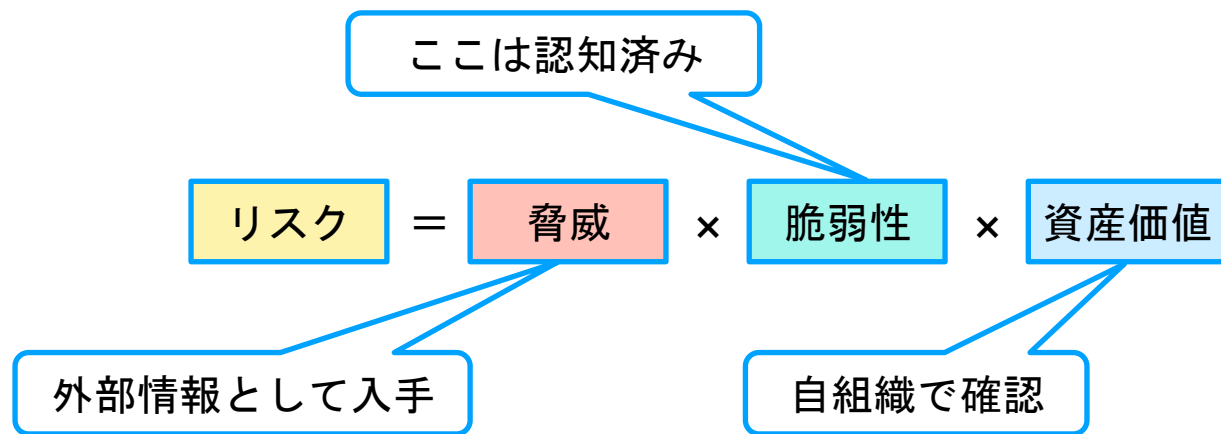
この場合必要な情報は、脆弱性に対する情報と、システムに対する情報、です。

### ■ システムに対する情報

- 対象システムの保有資産価値
- SBOMによるソフトウェア資産一覧

### ■ 脅威（攻撃可能性）に関する情報

- CVSS
- EPSS
- KEV Catalog(Known Exploited Vulnerability Catalog)
- Exploit情報




## 4.b.i. システムの価値

リスク定義の、資産価値に該当します。

システムの価値を定義することで、どの程度リスクに対して対策を行うか判断ができます。

- 個人情報などの「資産価値」のある情報を取り扱う場合、同じ 脅威/脆弱性 でもリスクが高まります。
- 公開情報を保有し、停止も許されるシステムであれば、侵害された場合のリスクは低く、備えが警備でも構わない、という事業判断は会えます。

$$\text{リスク} = \text{脅威} \times \text{脆弱性} \times \text{資産価値}$$


### • 考え方

- 攻撃のフェーズを理解し、最終目的に達成させない戦略を考える

### • どのように使えるか

- 現状で実装しているセキュリティ対策の過不足の確認をし、リスクに対しどこまで費用をかけるか、リスクを許容するかを検討する



表3-2 事業リスクの種類

#	事業リスクの種類 Impacts per Category
①	利用者に不便、苦痛を与える、又は事業を所管する機関等が信頼を失う Potential impact of inconvenience, distress, or damage to standing or reputation:
②	利用者に金銭的被害を与える、機関等に賠償責任が生じるなど財務上の影響を与える Potential impact of financial loss:
③	機関等の活動計画や公共の利益に対して影響を与える Potential impact of harm to agency programs or public interests:
④	利用者の個人情報などの機微な情報が漏洩する Potential impact of unauthorized release of sensitive information:
⑤	利用者の身の安全に影響を与える Potential impact to personal safety:
⑥	法律に違反する The potential impact of civil or criminal violations is:

(出典) NIST SP 800-63-3「Digital Identity Guidelines (電子的認証に関するガイドライン)」より作成

表3-3. 事業への影響度の定義

影響度	内容
高位 (High)	当該リスクの影響による損失が、組織の運営、組織の資産、又は個人に致命的又は壊滅的な悪影響を及ぼすと予想される

12

中位 (Moderate)	当該リスクの影響による損失が、組織の運営、組織の資産、又は個人に重大な悪影響を及ぼすと予想される
低位 (Low)	当該リスクの影響による損失が、組織の運営、組織の資産、又は個人に限定的な悪影響を及ぼすと予想される
非該当 (NA)	該当しない または 当該リスクによる影響がないと予想される

(出典)「連邦政府の情報および情報システムに対するセキュリティ分類規格 (連邦情報処理規格 FIPS 199)」より作成

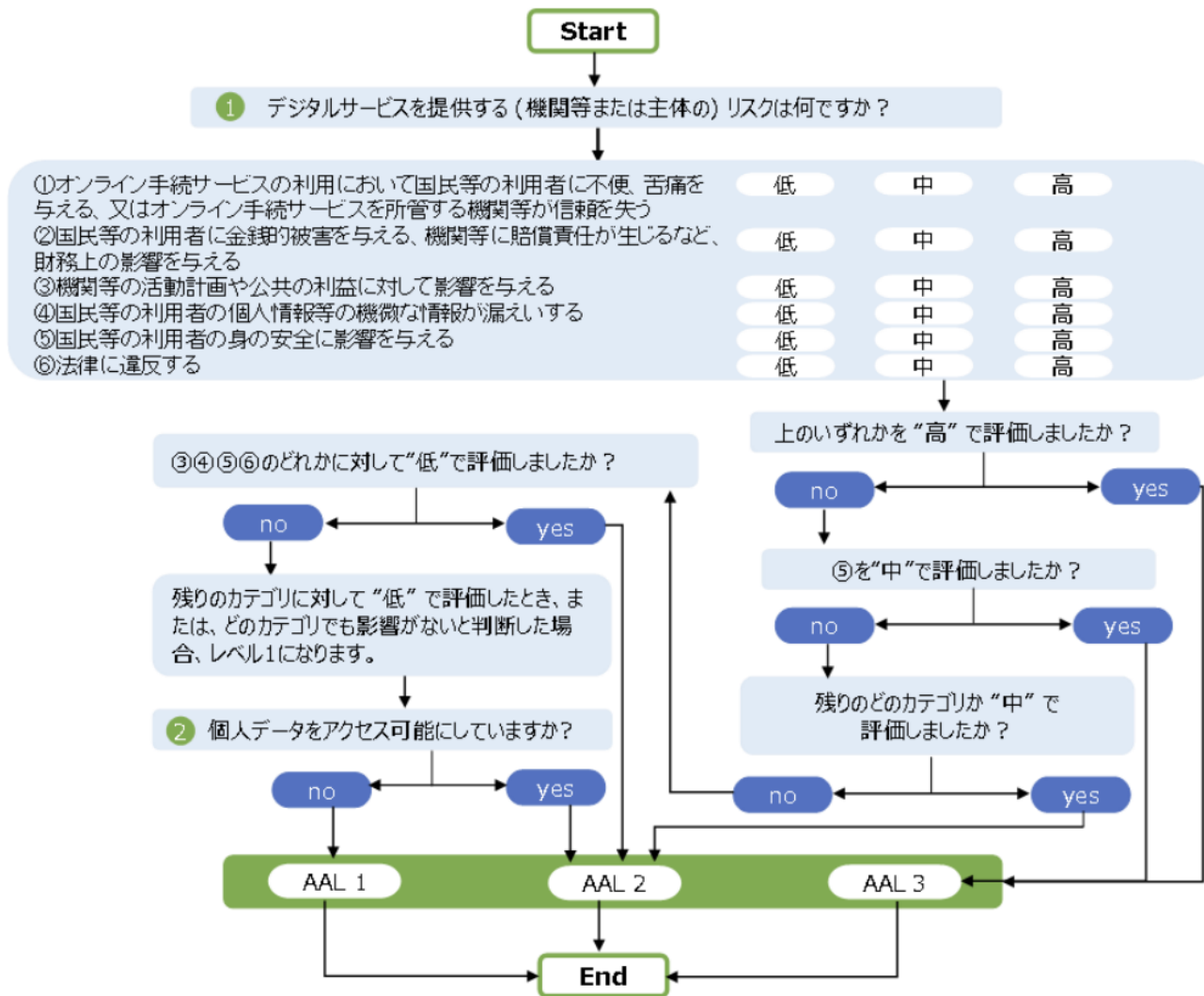



図3-2 システムの保証レベルのデシジョンフロー

## 4.b.ii. SBOM

SBOM (Software Bill Of Materials) は、製品に含むソフトウェアを構成するコンポーネントや依存関係、ライセンス情報などをリスト化した一覧表で、「ソフトウェアの構成部品一覧表」となる物です。

- ホストで利用しているソフトウェアのバージョンやライセンス情報などを、特定のフォーマットに沿って記載するもの
- どこまでSBOMを用意するか、どのタイミングで更新するか、などが運用の肝になる

$$\text{リスク} = \text{脅威} \times \text{脆弱性} \times \text{資産価値}$$


- 考え方

- 保有するソフトウェア一覧を用意することで、脆弱性を確認すべき対象がわかるようにする

- どのように使えるか

- 保有ソフトウェアのバージョン情報等から、残存する脆弱性を特定できる
  - アップデートを確認すべき対象を認識できる



CESER Partners with CISA to Release New Framework for Software Bill of Materials Sharing

<https://www.cisa.gov/sbom>

```

"copyrightText" : "Copyright 2008-2010 John Smith",
"description" : "The GNU C Library defines functions that are specified by the ISO C standard, as well as additional features specific to P
"downloadLocation" : "http://ftp.gnu.org/gnu/glibc/glibc-ports-2.15.tar.gz",
"externalRefs" : [ {
  "referenceCategory" : "SECURITY",
  "referenceLocator" : "cpe:2.3:a:pivotal_software:spring_framework:4.1.0:*:*:*:*:*:*:*",
  "referenceType" : "cpe23Type"
}, {
  "comment" : "This is the external ref for Acme",
  "referenceCategory" : "OTHER",
  "referenceLocator" : "acmecorp/acmenator/4.1.3-alpha",
  "referenceType" : "http://spdx.org/spdxdocs/spdx-example-444504E0-4F89-41D3-9A0C-0305E82C3301#LocationRef-acmeforge"
} ],
"filesAnalyzed" : true,
"homepage" : "http://ftp.gnu.org/gnu/glibc",
"licenseComments" : "The license for this project changed with the release of version x.y. The version of the project included here post-d
"licenseConcluded" : "(LGPL-2.0-only OR LicenseRef-3)",
"licenseDeclared" : "(LGPL-2.0-only AND LicenseRef-3)",
"licenseInfoFromFiles" : [ "GPL-2.0-only", "LicenseRef-2", "LicenseRef-1" ],

```

<https://github.com/spdx/spdx-spec/blob/development/v2.3.1/examples/SPDXJSONExample-v2.3.spdx.json>

## 4.b.iii. CVSS (Common Vulnerability Scoring System)

おそらく、脆弱性の管理といえばCVSSを想像されることが多いと思います。

CVSSは「脆弱性それ自体」の影響度を示すものです。

- 現時点ではCVSS v3を使っていますが、近い将来CVSS v4を使うことになる
- 脆弱性それ自体の影響度であるため、脅威が少ない（攻撃確率が低い）場合はリスクは低く見積もる等の判断ができる
  - 脆弱性をすべて修復するのは難しいことが多い（コスト的に）
  - 他の影響する要因でリスクを軽減する
  - 脆弱性の原因を見ることで、自組織では影響が少ない等の判断もできる

### • 考え方

- そのものの脆弱性の特徴を理解し、対応方法を検討する

### • どのように使えるか

- 脆弱性が発動する要件を読み取ることで、自組織で影響があるのかどうかを判断することができる

$$\text{リスク} = \text{脅威} \times \text{脆弱性} \times \text{資産価値}$$



Common Vulnerability Scoring System version 4.0:  
Specification Document

<https://www.first.org/cvss/>

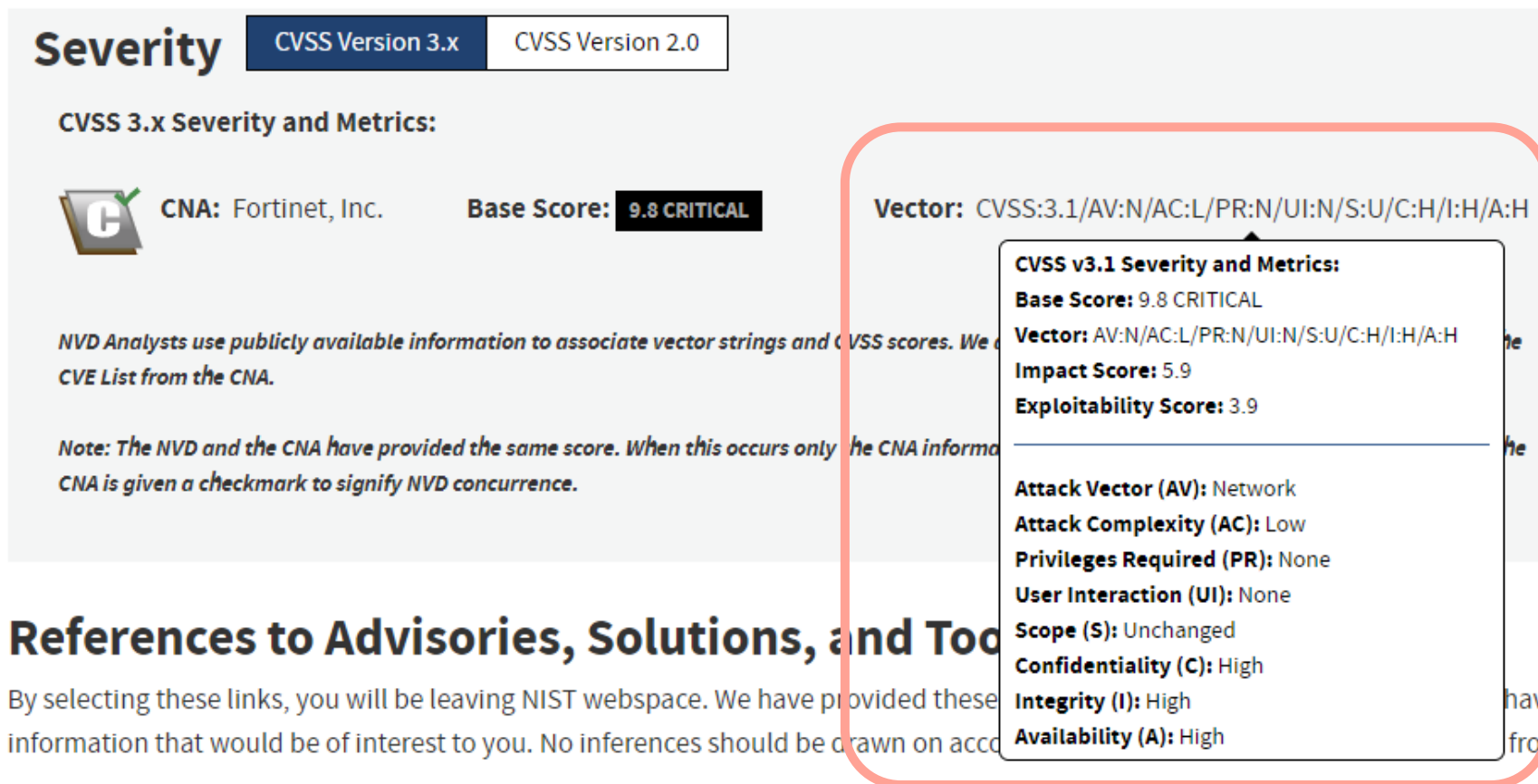
## CVSS v3

### ■ BaseScoreは、攻撃情報インパクトなどで算出されている

- 元データとなる Vector は読めるようになっていたほうがよい


- ✓ 例 CVE-2023-27997

- CVSS v4で多少変わるが、BaseScoreだけを見ていると対応ができない



**Severity** CVSS Version 3.x CVSS Version 2.0

**CVSS 3.x Severity and Metrics:**

 **CNA:** Fortinet, Inc. **Base Score:** 9.8 CRITICAL

*NVD Analysts use publicly available information to associate vector strings and CVSS scores. We do not guarantee the accuracy of the information provided in the CVE List from the CNA.*

*Note: The NVD and the CNA have provided the same score. When this occurs only the CNA information is given a checkmark to signify NVD concurrence.*

**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**CVSS v3.1 Severity and Metrics:**

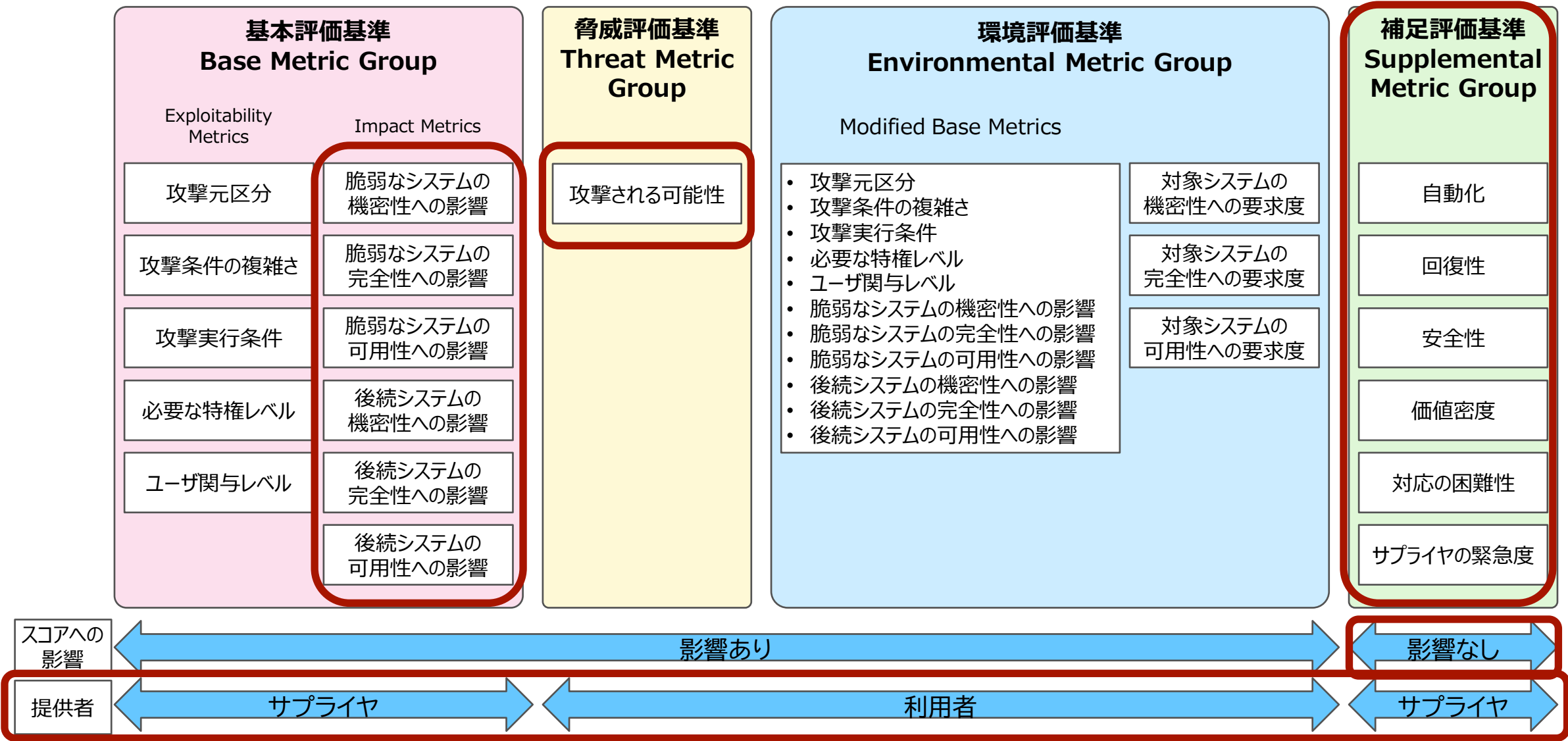
- Base Score:** 9.8 CRITICAL
- Vector:** AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- Impact Score:** 5.9
- Exploitability Score:** 3.9

---

**Attack Vector (AV):** Network  
**Attack Complexity (AC):** Low  
**Privileges Required (PR):** None  
**User Interaction (UI):** None  
**Scope (S):** Unchanged  
**Confidentiality (C):** High  
**Integrity (I):** High  
**Availability (A):** High

**References to Advisories, Solutions, and Tools**

By selecting these links, you will be leaving NIST webspace. We have provided these links to help you find more information that would be of interest to you. No inferences should be drawn on account of the information provided.





FIRSTがメンテナンスをしている、CVE-ID毎の今後30日以内に脆弱性が悪用される確率を示したものです。


- 確率論であり、Scoreが10%だと全体の87.6%に該当する、というようなデータになる
- Scoreが幾つ以上なら対応すべき、のような論文はあるが...
- EPSSは「脅威」に関する情報であり、その点は有用
  - 私達はリスクに対応したい
  - どれだけ脆弱性が危険でも、悪用される確率が低ければ許容できる場合もある

### • 考え方

- 実際に悪用される確率を把握することで、備えの優先度を判断できる

### • どのように使えるか

- リスクへの対応判断基準として利用する

$$\text{リスク} = \text{脅威} \times \text{脆弱性} \times \text{資産価値}$$




<https://www.first.org/epss/>

## EPSSは2つの軸がある

### ■ Probability

- 30日以内に悪用される確率
- 元データでは、0.0-1.0で提供される
- スコア、と呼ばれることも多い

### ■ Percentile

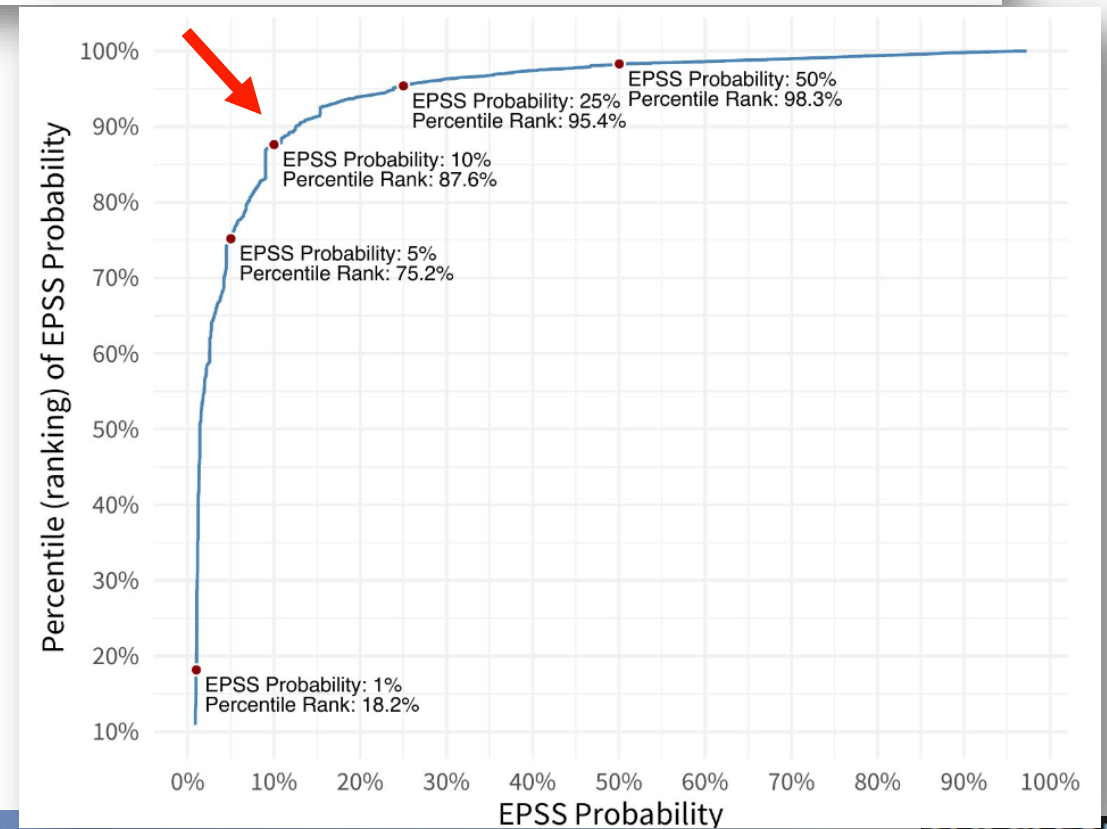
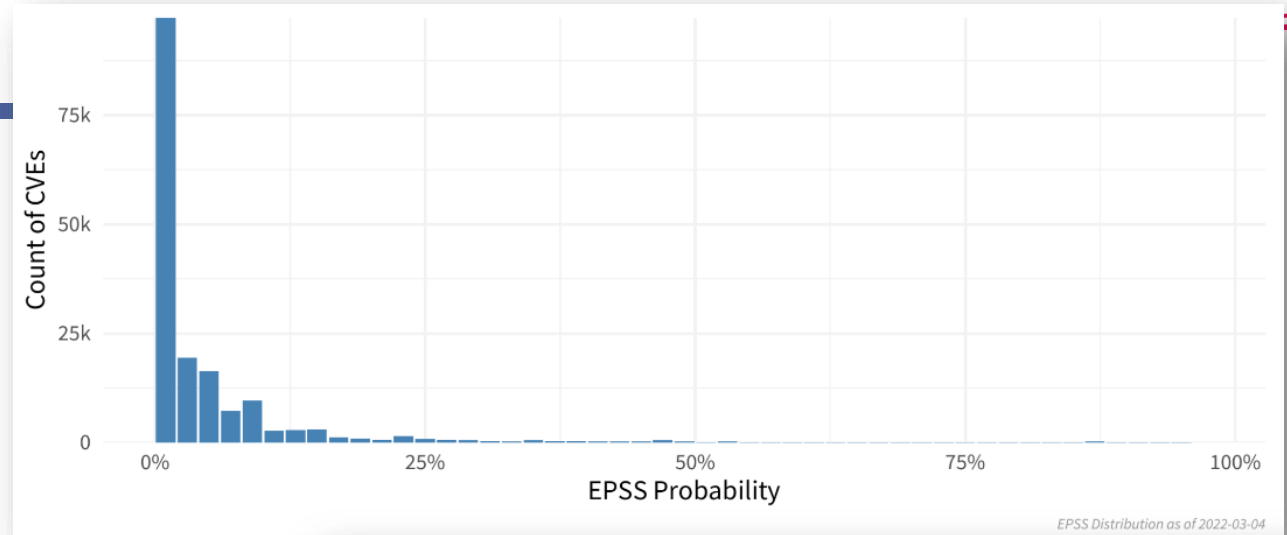
- 全体のどのランクにあるかを相対的に示す
- 例えばProbabilityが10%の場合
  - ✓ Percentile Rankが87.6%
  - ✓ これは、EPSSでスコア化されている脆弱性全体の87.6%の脆弱性より悪用される可能性が高いことを意味している  
(危険なもの上位12.4%にいる、といういい方でもよいかもしれません)

上記のように、単純に「閾値以上なら危険」という安易な判断には使えないので、どのように取り扱うかは事前に検討が必要です。

詳しく検討したい方は

[github.com/hogehuga/epss-db](https://github.com/hogehuga/epss-db)

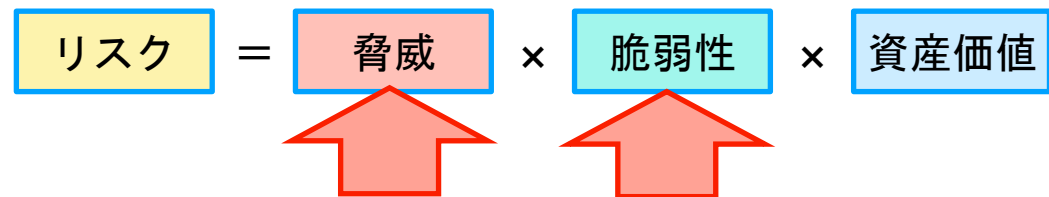
辺りを使うとよいでしょう。



## 4.b.v. Known Exploited Vulnerability Catalog(KEV)

CISAが提供する、「悪用が確認された脆弱性のカタログ」です。

- 米国において既に悪用がされている、早急に対応すべき脆弱性の一覧として利用されている
- 米連邦機関においては、BOD 22-01(拘束力のある運用指令)において、KEV Catalog登録後2週間以内に対応することが必要とされる
- リスクの観点では、脅威と脆弱性を示している
  - 悪用の機会が高いことと、脆弱性それ自体が危険なものが登録されるため



### • 考え方

- 悪用される確率が非常に高いものであり、基本的には対応すべきもの

### • どのように使えるか

- KEV Catalogに記載されたものは悪用される前提として対応を考えられる

## +

■ **Date Added:** 2024-01-31

**TLP: CLEAR**

## 4.b.vi. Exploit情報

実際のExploit情報があるかを調べることで、今後攻撃が行われる可能性が高いかを確認することができる。

- データソースとしては、SNSや商用情報、公開情報などがある
  - SNSやgithubなどは、信ぴょう性が低いものも多々あるので確認が必要
- まずは、ExploitDBを使ってみるのが良い

例えば、metasploitで使うexploitdbなどが確実性が高い

- 例えばserchsploitコマンド

- 考え方
  - すぐに使える攻撃コードがすでに広まっている場合、攻撃をされる機会が増え、リスクが高くなると考えられる
- どのように使えるか
  - 既にCVE-IDが降られている脆弱性に関して、攻撃コード有無でリスクを評価する

## 例) searchsploitでのExploit有無の調査

searchsploitは、ExploitDBのコマンドライン検索ツールです。

■ <https://www.exploit-db.com/searchsploit>

- ExploitDB : OffSec社 (旧Offensive Security社) が維持管理している、非営利の脆弱性Exploitのデータベース

```

:~$ searchsploit nginx
-----
Exploit Title | Path
-----
Nginx (Debian Based Distros + Gentoo) - 'logrotate' Local Privilege Escalation | linux/local/40768.sh
Nginx 0.6.36 - Directory Traversal | multiple/remote/12804.txt
Nginx 0.6.38 - Heap Corruption | linux/local/14830.py
Nginx 0.6.x - Arbitrary Code Execution NullByte Injection | multiple/webapps/24967.txt
Nginx 0.7.0 < 0.7.61 / 0.6.0 < 0.6.38 / 0.5.0 < 0.5.37 / 0.4.0 < 0.4.14 - Denial of S | linux/dos/9901.txt
Nginx 0.7.61 - WebDAV Directory Traversal | multiple/remote/9829.txt
Nginx 0.7.64 - Terminal Escape Sequence in Logs Command Injection | multiple/remote/33490.txt
Nginx 0.7.65/0.8.39 (dev) - Source Disclosure / Download | windows/remote/13822.txt
Nginx 0.8.36 - Source Disclosure / Denial of Service | windows/remote/13818.txt
Nginx 1.1.17 - URI Processing SecURity Bypass | multiple/remote/38846.txt
Nginx 1.20.0 - Denial of Service (DOS) | multiple/remote/50973.py
Nginx 1.3.9 < 1.4.0 - Chunked Encoding Stack Buffer Overflow (Metasploit) | linux/remote/25775.rb
Nginx 1.3.9 < 1.4.0 - Denial of Service (PoC) | linux/dos/25499.py
Nginx 1.3.9/1.4.0 (x86) - Brute Force | linux_x86/remote/26737.pl
Nginx 1.4.0 (Generic Linux x64) - Remote Overflow | linux_x86-64/remote/32277.txt
PHP-FPM + Nginx - Remote Code Execution | php/webapps/47553.md
-----
Shellcodes: No Results
:~$

```



未知の情報セキュリティの脅威に備える、というテーマから、脆弱性との関係話を話しました。  
若干当初のテーマからずれた気がしますが、何等かの知見の足しになれば幸いです。

### ■ 未知の情報セキュリティ脅威に備える

- 現状を把握し、準備をすることで、脅威に対抗できる
- 脅威の影響が未知の場合は、脅威となる脆弱性を理解することで対抗できる

### ■ デジタル庁の「デジタル社会推進標準ガイドライン」は読んでおいたほうがいい

- [https://www.digital.go.jp/resources/standard\\_guidelines](https://www.digital.go.jp/resources/standard_guidelines)
- 個人的には「DS-201 政府情報システムにおけるセキュリティリスク分析ガイドライン ～ベースラインと事業被害の組み合わせアプローチ～」辺りはおすすめ。

ご質問、ご相談、ディスカッション等は、[k.inoue.xz@future.co.jp](mailto:k.inoue.xz@future.co.jp) までご連絡ください。



**FUTURE**