
# Cracker Probing-Eyes®

## Proposal of ASP type external vulnerability diagnosis service

ICMS-SR0032B / JIS Q 27001

018-0038-20

10470048

株式会社ブロードバンドセキュリティ

BroadBand Security, Inc.

# Incidents and vulnerabilities on the rise

**All kinds of companies in Japan are being victimized one after another (according to recent cases).**

More than 230 cases **of unauthorized use of electronic payment services Leakage of information Total damage of more than 29 million yen**

**Cybercriminal groups attack game companies Fear of leakage of up to 390,000 pieces of personal information**

**Two attacks on a general electronics manufacturer Leakage of defense information Leakage of 8,000 customer account information**

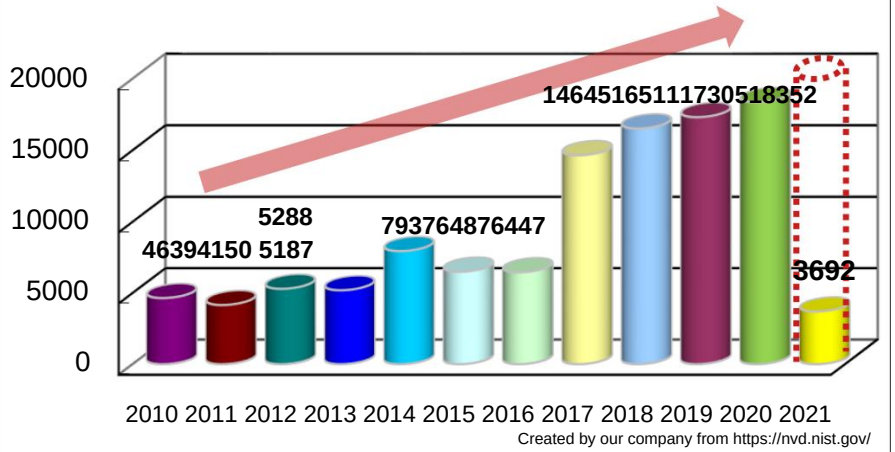
**It is important to obtain the latest vulnerability information and take countermeasures!**

**Continued rapid increase from 2017**

**Increasing complexity of software, increasing number of connected hosts and IoT**

National Vulnerability Database

Number of vulnerabilities registered in (NVD)

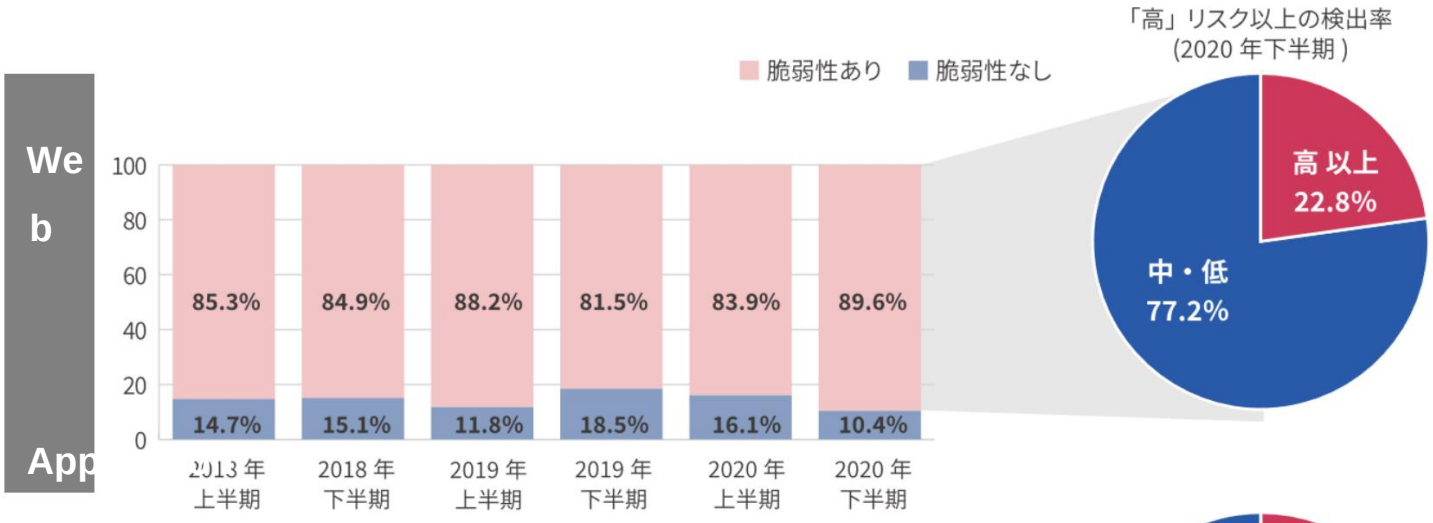



Created by our company from https://nvd.nist.gov/

NVD (National Vulnerability Database): Vulnerability information database managed by NIST (National Institute of Standards and Technology)

# Over 80% of systems have vulnerabilities! *

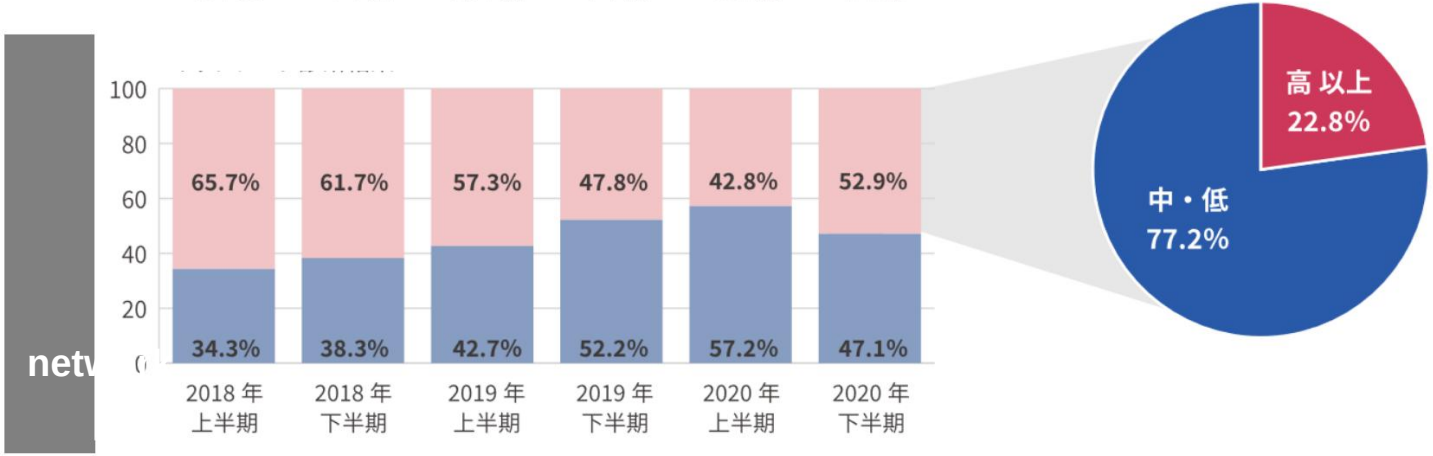
*Based on our diagnostic results




**Major Vulnerabilities of High Risk Level and above:**

- **SQL injection**
- cross-site scripting
- HTML tag injection
- Allowing Weak Passwords

There is a vulnerability that may lead to damage such as leakage of confidential information or guidance to unauthorized sites.




**Major Vulnerabilities of High Risk Level and above:**

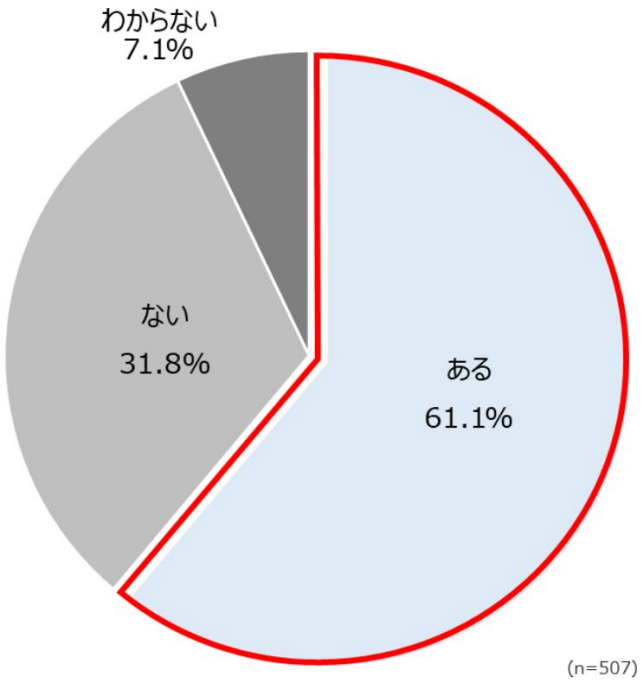
- **End of support/older version Use of OS/middleware**
- **Continued use of factory ID/passwor**
- **Use of vulnerable network services**

You may be targeted by attackers, and you need to upgrade your version or update your platform .

# The reality of patch management

**More than 60% of systems have not been patched!**

The application rate of `` security patches'' to fill the holes of ``vulnerability'' is not high

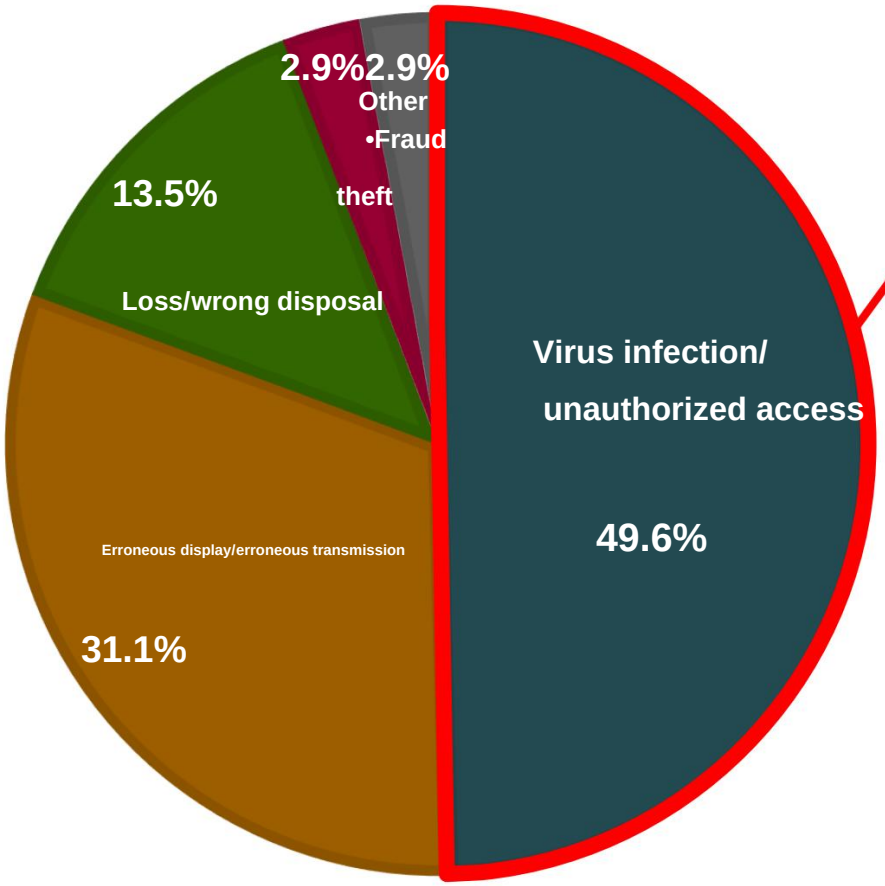



**The reason why there are patches that have not been applied…**

The main reasons are “lack of asset management/confirmation,” “lack of understanding/coordination,” and “lack of resources/environment.”


Broadband Security Co., Ltd. × IID Co., Ltd. (survey conducted in August 2020) “We asked 500 people, ‘Is your company doing vulnerability management and patch management well?’”

# Cause of information leakage




Tokyo Shoko Research Co., Ltd.
"Personal Information Leakage/Loss Accidents of Listed Companies" Survey (2020)

**About 50% of information leaks are caused by cyberattacks**

- Targeted attacks • Ransomware • Spear phishing • Improper security settings • Leakage/theft of authentication information • Component vul

# Recent cyber attacks - how to deal with them?

Increasingly sophisticated and sophisticated attack methods

Vulnerability increasing day by day

**Anyone can be a target**

How can I always know the security status of my system?

**Know the state of your system and take necessary measures!**

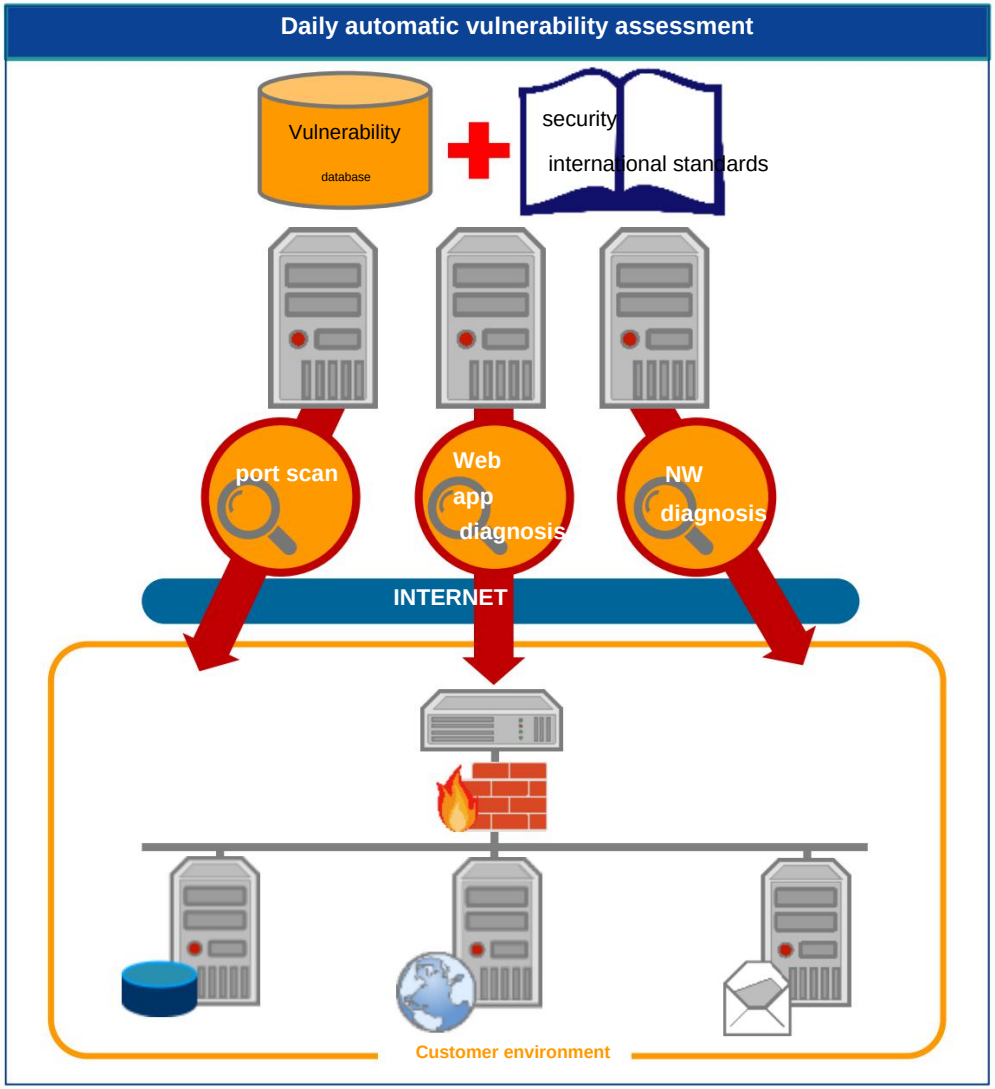
"Ignorance is the greatest vulnerability", and "knowing" is important for information security

**Vulnerability diagnosis allows you to check the security status of your system against threats that change daily, so you can implement timely and appropriate counterm**

# Cracker Probing-Eyes® (CPE)

ASP type external vulnerability diagnosis service

# About CPEs




**Diagnosis is performed daily, so new vulnerabilities can be discovered quickly**

**diagnosis result Can be checked at any time on the web**

**The report output for each diagnosis is color-coded by risk level, allowing you to check the diagnosis results and the importance of countermeasures at a glance.**

# Overview of CPE service ÿ

## Automatic diagnosis service from outside (daily diagnosis)

### Diagnosis target

ÿ Global IP address: 5

ÿ URL address (FQDN): 1

ÿ Diagnosis targets are devices with global IP addresses

### Basic service

Basic scan : Annual service

ÿ Full scan : Annual service

*Provided with a one-year service license Consumption tax is not included

### point

**Points 1** network all port scan

•Port scan of all TCP and UDP ports •Investigation of possible denial of service (DoS) •Identification of operating system

**Points 2** letwork vulnerability diagnosis

•Backdoor investigation •Default password investigation •DNS investigation FTP probe General firewall probe Simple Mail Transfer Protocol (SMTP) probe NFS probe Remote Procedure Call (RPC) Server Message Block (SMB)/NetBIOS probe Simple Network Management Protocol (SNMP) probe•Database (DB) server inspection •UNIX/LINUX vulnerability investigation

•Windows vulnerability research, etc.

**Points 3** Veb application vulnerability diagnosis

•Cross-site scripting •Directory traversal •OS command injection •iframe injection•Link injection •Improper exception handling •Passive Scan

•Problems related to SQL injection, session management, etc.

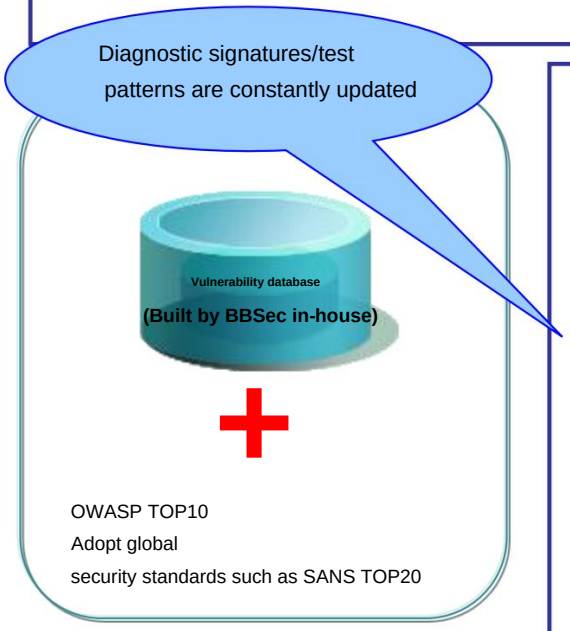
# Overview of CPE serviceÿ

**Inspection method and service overview**

•Diagnosis method: Tool diagnosis •Diagnosis location: Diagnosis performed from outside (BBSec) •Diagnosis time: Either 6:00 to 18:00 or 18:00 to 6:00 the next day •Contents provided: Diagnosis results from the portal site Reference /Support: (Paid option) Up to 5 inquiries.

Customer benefits

- ASP-type tool diagnosis does not require the customer to purchase equipment or install software.
- Daily diagnosis results can be immediately checked on the web, enabling countermeasures to be taken before threats become a reality.




**Superiority of this method**

•Daily diagnosis is possible.

•Web Application Diagnosis -

Diagnosis service for vulnerabilities such as cross-site scripting and SQL injection, which account for more than 80% of current attacks. - In manual diagnosis, the estimate is usually based on the dynamic page transition unit.

This service can be used at a low cost because the fee is set per URL (FQDN).•Network diagnosis

- Inspection signatures are updated once a week, so new known vulnerabilities can be detected.
- In the manual diagnosis, the estimate is based on the premise of the penetration test. Since this service is based on diagnostics using tools, it can be used inexpensively for a large number of servers.

# Strengths of CPE

## easy-to-understand reports

Since it is a purely Japanese tool, the details of vulnerabilities and countermeasures in the report are clear.

BBSec security engineers perform

over-detection checks on the diagnostic results of the **highly accurate detection result** tool, so unnecessary findings that tend to occur in diagnostic tools are not posted.

**Easy** diagnosis No

preparations such as system changes are required for diagnosis.

Vulnerability scores are

standardized because **standardized result** CVSS values are output . The security level can be easily grasped even when the results are reported to upper management or outside, or when the person in charge is changed .

## Extensive support

In response to inquiries from customers ,

BBSec security professionals are available directly via email and phone.

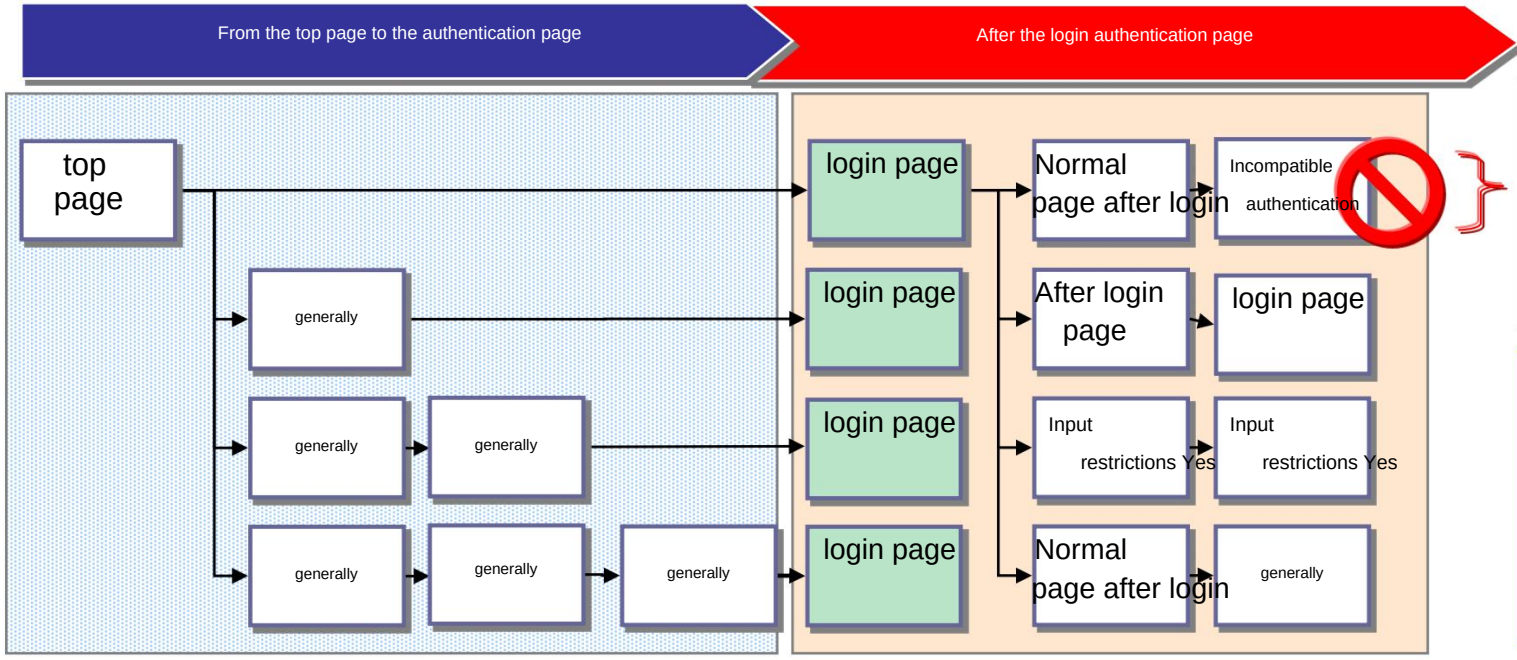
# Difference between Basic Scan/Full Scan

## Basic service

The difference is due to the "diagnosis target range" of the Web application diagnosis.

ÿ Basic scan — Vulnerability diagnosis before authentication page

ÿ Full scan — Automatically diagnose pages after login authentication




However, some pages cannot be scanned depending on the authentication method or page generation method. Please refer to the next page to see if the site is compatible .

Automatic diagnosis by the system is limited. If you need a complicated page or a full-fledged investigation, please use the separate manual diagnosis .

# CPE restrictions

ÿ Authentication methods supported by CPE

| Authentication method | Authentication method (details) | availability |
|---|---|---|
| Basic authentication | | • |
| Form authentication | ID/PASS | • |
| | ID/PASS + device-specific information | • |
| | ID/PASS + user agent (screen for mobile phones) | • |
| | ID/PASS + user agent + terminal identification number (screen for mobile phones) | • |
| | ID/PASS + one-time token | × |
| | Combined authentication with CAPTCHA | × |
| DIGEST certification | | × |
| CLIENT-CERT authentication (SSL certificate) | | × |

ÿ Other configurations that cannot be supported by CPE (page)

| Unsupported configuration (page) | availability |
|---|---|
| Page transitions that require JavaScript processing | ÿ |
| Ajax generated page | ÿ |
| Page transitions that require processing in JSON format requests | × |
| Pages that control transitions with tokens, etc. | × |
| Pages generated by Flash, Java applets | × |

# CPE restrictions

ÿ Targets that cannot be diagnosed

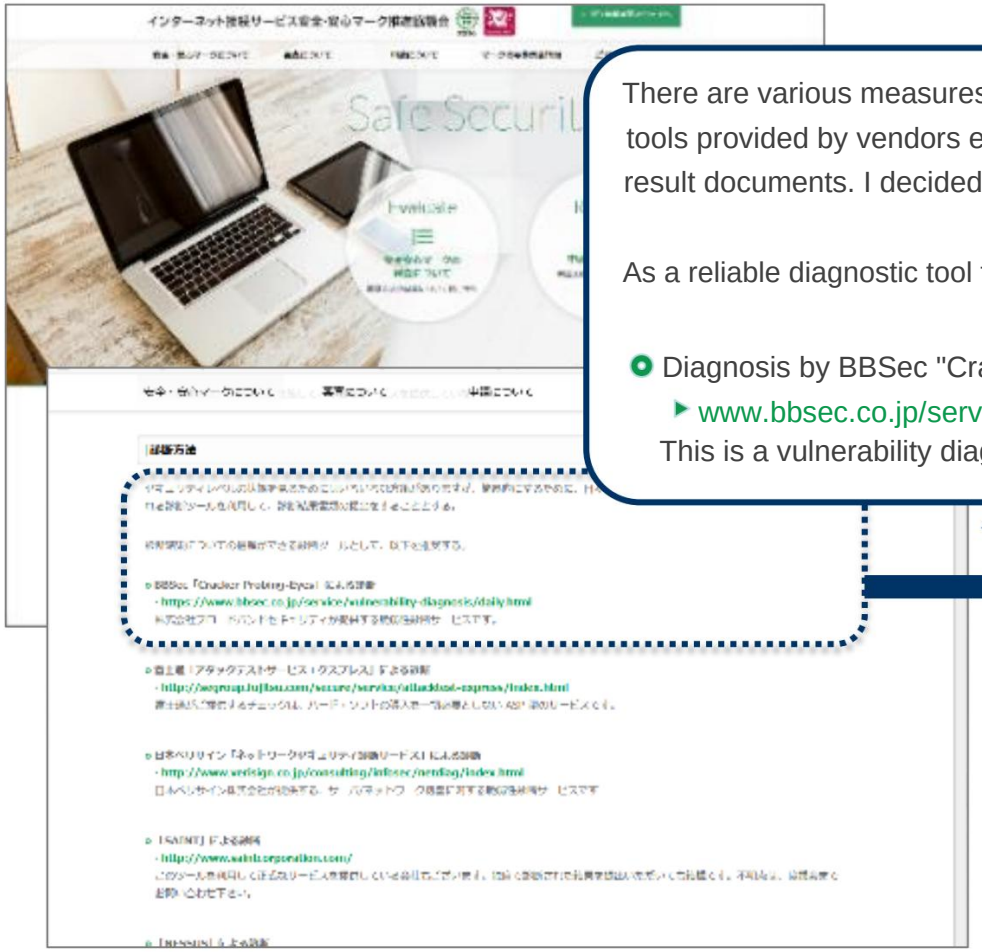
| composition | detail | example |
|---|---|---|
| Functions that cannot be executed multiple times | Diagnosis is not possible because multiple patterns are inspected for the same request. | • Withdrawal<br>• Deletion of data •<br>Functions with processing limits |
| It is necessary to take over the session with<br>an FQDN that is different from the diagnosis target | Diagnosis is not possible because it is not possible to transition across different FQDNs. | • FQDN of diagnosis target and login site different<br>• The FQDN of the diagnosis target and the site issuing the session are different |

ÿ Targets requiring attention in diagnosis

| composition | detail | example |
|---|---|---|
| Data registration, update | Since multiple patterns of inspection are performed for the same request, a large number of registrations and updates are performed , which may affect the target system and the customer's business. | • Send inquiry • Register new<br>data • Update existing data |

# Tools recommended by the Safety and Security Mark Promotion Council

"Cracker Probing-Eyes®" is a vulnerability diagnosis tool recommended by the Internet Connection Service Safety and Security Mark Promotion Council .



There are various measures to check the security level status, but to make it simple, use diagnostic tools provided by vendors etc. for diagnostic items that are updated daily, and submit diagnostic result documents. I decided to.

As a reliable diagnostic tool for diagnostic results, we recommend the following:

- Diagnosis by BBSec "Cracker Probing-Eyes" https://
  - www.bbsec.co.jp/service/vulnerability-diagnosis/daily.html

  This is a vulnerability diagnosis service provided by Broadband Security Co., Ltd.

### Safety and security mark

An Internet connection service provider that has met the licensing screening criteria of the screening committee of the Internet Connection Service Safety and Security Mark Promotion Council, with the aim of providing a guideline for users to be able to use the Internet with peace of mind. mark given to The expiration date of the mark is one year from the date of issue, and it is necessary to pass the renewal examination for continued use .

Website of the Internet Connection Service Safety and Security Mark Promotion Council https://www.isp-ss.jp/ | https://www.isp-ss.jp/examination/item/

# Manual diagnostics and tool diagnostics – your needs

The Manual Diagnostics Service and the Tool Diagnostics Service each have specific usage needs. Many of our customers use both services depending on their circumstances.

| manual diagnosis | | tool diagnostic |
|---|---|---|
| A dynamic and highly functional website equipped with an authentication mechanism, DB linkage, etc. | Features of Sites to be Diagnosed | A static website displaying boilerplate content |
| EC site<br>Financial transaction site | Examples of sites to be diagnosed | Corporate site information distribution site |
| Before a new release or during a refurbishment | Example of diagnostic timing | Maintenance period after release |
| Spot implementation only when necessary | Example of diagnostic frequency | Conducted on a regular basis, such as daily and weekly |
| Comprehensive vulnerability detection results and risk analysis according to system characteristics | Desired reporting quality | Detected presence or absence of major vulnerabilities and general risk assessment results |

*This table is for reference only and does not apply to all cases.

# Differences between CPE and manual diagnosis (WEB)

| Item number | item | explanation | Service comparison | | | | |
|---|---|---|---|---|---|---|---|
| | | | Diagnostic range | diagnostic category | False positive over-positive | Risk determination | diagnostic report |
| 1 | manual diagnosis | This is a diagnosis performed by our diagnostic engineers. We have the widest range of diagnosis and diagnosis categories , and we will submit the diagnosis report in the same format and appearance as before. | • It is possible to cover diagnosis targets under all kinds of conditions . | • All possibilities are examined and reported at the time of diagnosis . | • We will check whether there is false detection or over-detection of the problem area . | • We will report the overall results of the tool judgment results and the diagnosis engineer 's judgment. | ÿ We will provide you with a report prepared by our diagnostic engineers . |
| 2 | CPEs | We will conduct a diagnosis using a commercial tool that we use for vulnerability diagnosis and report the results. Our diagnostic engineers will set up and operate the tool , and check for over-detection and false detection. We do not examine the risk judgment based on the system characteristics. Inspection results will be submitted in a report generated by the tool (in BBSec specifications). | ÿ Due to the characteristics of tool diagnostics, there may be diagnostic screens that cannot be covered by tool diagnostics, such as screens that cannot be moved unless under specific conditions. | ÿ Although it discovers major vulnerabilities, it is advantageous to manually respond to the latest techniques , and it is not good at diagnosing session management (see the following pages). | • False detection of problem parts We will check whether there is false detection. | ÿ We will present the judgment result of the tool as it is . | • We will submit a report generated by the tool (format customized to BBSec specifications ). |

# Overview of Inspection Items (WEB)

## ÿ Response to OWASP TOP10 2017

*Specific examples of each survey item are only major examples and are not intended to limit the content of the diagnosis. In addition, there is a part where the accuracy of tool diagnosis is inferior to that of manual diagnosis.

| OWASP TOP 10 | Example | Manual | Tool diagnosis |
|---|---|---|---|
| A1 – Injection | SQL injection | diagnosis • | • |
| | command injection | ● | ● |
| | HTML injection Email | ● | ● |
| | header injection | ● | × |
| | HTTP header injection Inspection | ● | × |
| A2 – Poor Authentication and Session Management | of authentication method Handling | ● | ● |
| | of user IDs, passwords, and session information Display of information | ● | ● |
| A3 – Sensitive data exposure | that should not be disclosed Detection of application paths that should not | ● | ● |
| | be disclosed Detection of platform paths that should not be disclosed | ● | ● |
| | | ● | ● |
| A4 – XML External Entity Reference (XXE) | XML external entity | ● | Verifying signature |
| A5 – Poor Access Control | reference (XXE) file | ● | × |
| | inclusion Path traversal | ● | ● |
| | Forced browsing Privilege | ● | × |
| | escalation Robots.txt | ● | × |
| | detection | ● | Supported by NW diagnosis |
| A6 – Mistakes in security settings | Publish admin page | ● | ● |
| | Directory listing | ● | ● |
| | Allow deprecated | ● | Supported by NW diagnosis |
| | methods Unrestricted file upload | ● | × |
| A7 – Cross Site Scripting (XSS) | capabilities Cross-site scripting (XSS) | ● | ● |
| A8 – Insecure deserialization | Object and data structure related attacks Typical | ● | × |
| | data tampering Use of components with known vulnerabilities | ● | × |
| A9 – Use of components with known vulnerabilities | such as access control related attacks | ● | Supported by NW diagnosis<br>Supported by CPECore |
| A10 – Poor Logging and Monitoring | Check log files | Supported by GlassBox | Supported by CPECore |
| | Log monitoring | × | × |

# Difference between CPE and manual diagnosis (NW)

| Item number | item | explanation | Service comparison | | | | |
|---|---|---|---|---|---|---|---|
| | | | Diagnostic range | diagnostic category | False positive over-positive | Risk determination | diagnostic report |
| 1 | manual diagnosis | This is a diagnosis performed by our diagnostic engineers. We have the widest range of diagnosis and diagnosis categories , and we will submit the diagnosis report in the same format and appearance as before. | • It is possible to cover diagnosis targets under all kinds of conditions . | • All possibilities are examined and reported at the time of diagnosis . | • We will check whether there is false detection or over-detection of the problem area . | • We will report the overall results of the tool judgment results and the diagnosis engineer 's judgment. | ÿ We will provide you with a report prepared by our diagnostic engineers . |
| 2 | CPEs | Diagnosis is performed using a tool equipped with an engine developed independently by our company, and the results are reported. Our diagnostic engineers will set up and operate the tool , and check for over-detection and false detection. We do not examine the risk judgment based on the system characteristics. Inspection results will be submitted in a report generated by the tool (in BBSec specifications). | • Port scan and network vulnerability diagnosis are performed in the same way as manual diagnosis . | ÿ Some items that can lead to server stoppages that cannot be verified by tool diagnosis have lower accuracy than manual diagnosis. | • False detection of problem parts We will check whether there is false detection. | ÿ We will present the judgment result of the tool as it is . | • We will submit a report generated by the tool (format customized to BBSec specifications ). |

# Overview of Inspection Items (Network)

ÿOverview of inspection items for [Network Diagnosis]

*Specific examples of each survey item are only major examples and are not intended to limit the content of the diagnosis. In addition, there is a part where the accuracy of tool diagnosis is inferior to that of manual diagnosis.

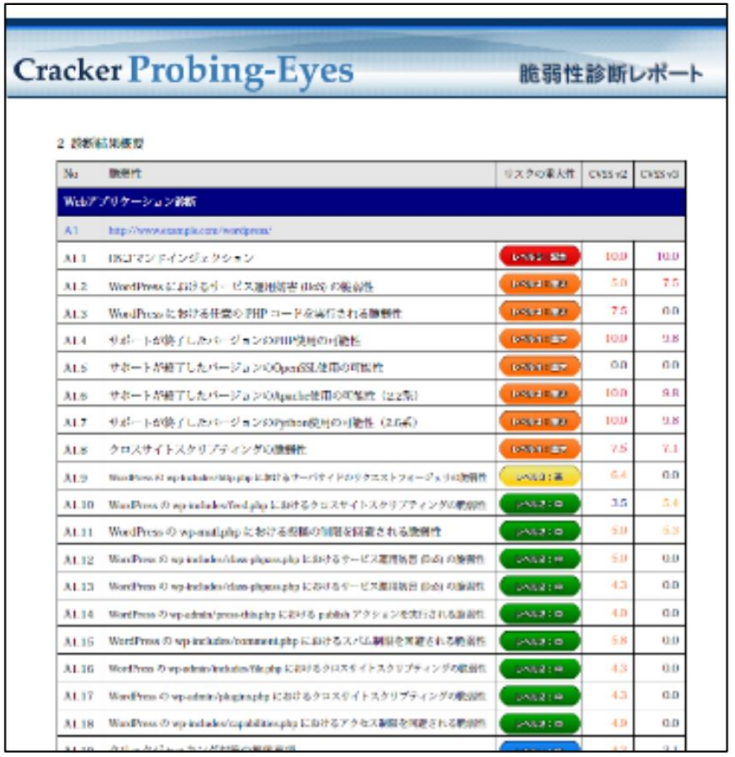
| category | Action Item | Example of implementation | Manual diagnosis Tool |
|---|---|---|---|
| Host scan | TCP, UDP, ICMP port scanning | TCP: Perform full port scan | diagnosis • • • • ▪▪▪▪▪▪▪ |
| | | UDP: Performs TOP1000 port scan with high detection frequency (full port if necessary) Response | • • • • • • • • • • • • ▪▪▪▪▪▪▪▪▪▪ |
| | Discover running services | confirmation for various protocols (HTTP, SMTP, FTP, etc.) Response confirmation for custom | • • • • • • • • • • • • ▪▪▪▪▪▪▪▪▪▪ |
| | | packets (SNMP, NTP, etc.) | • • • • • • • • • • • • Not |
| network service vulnerabilities | Research on DNS | Verification of DNS recursive query behavior | implemented Not |
| | | Extracting information from DNS cache | implemented Not |
| | Research on mail servers | Verification of relay control in SMTP service | implemented Not |
| | | Account investigation using EXPN/VRFY commands | implemented Not |
| | Survey on FTP | Verification of AnonymousFTP | implemented Not |
| | | Version identification of vsFTPD ~ Verification of known vulnerabilities | implemented Not |
| | RPC research | Execution service identification by RPC service | implemented Not |
| | | Extracting information from DCE/RPC services | implemented |
| | File sharing research | Verification of access control on SMB services | |
| | | Validating Null Session Issues | |
| | Survey on SNMP | Verify default settings in SNMP service | |
| | | Information extraction using SNMP | |
| | Survey on SSH server | Validation of acceptable encryption methods and MAC algorithms | |
| | | Verification of plaintext recovery attack in | |
| | Research on database servers | SSH Default account investigation | |
| | | Identification of database server and version by fingerprinting | |
| | Research on other services | Disclosure of system information by NTPD | |
| | | Validating ICMP Timestamp Responses | |
| Web server vulnerabilities | Web server vulnerabilities | Verification of cross-site scripting, etc. in ApacheKiller and Expect headers | |
| | | Validation of encryption in SSL/TLS (heartbleed, RC4 algorithm acceptance, etc.) | |
| | Web application server vulnerabilities | Validating Arbitrary Command Execution in ApacheStruts | |
| | | Detecting EasterEgg information in PHP | |
| | Allowed HTTP methods | Validating deprecated methods (TRACE, DELETE, PUT, etc.) Checking usage of | |
| Various OS vulnerabilities | Windows Known Vulnerabilities | Windows after vendor support ends | |
| | | Information extraction via NetBIOS | |
| | Known vulnerabilities of | Patch level verification via fingerprinting | |
| | Solaris Known vulnerabilities of various Linux distributions Verification of us | age status of old kernels Known | |
| | vulnerabilities of other various OS | VMware ESXi version identification to known vulnerability verification | |
| malicious software | Investigating backdoors | Detection of unintended services and applications (TCP Port 0 release, etc.) Matching with | |
| | | backdoor program databases Matching with P2P application databases such as gnutella | |
| | Investigation of P2P software | | |
| Vulnerability of network equipment | Known vulnerabilities of various router | Problems related to DNS settings (DNS poisoning) | |
| | devices Known vulnerabilities of various firewall | Problems caused by default settings (internal web server disclosure) | |
| | devices Known vulnerabilities of various other network | Checking for known vulnerabilities by fingerprinting Detecting various logins | |
| others | devices Investigation of other entire hosts | and management screens | |
| Unusual surveys | Denial of Service (DoS) attacks | ClassLoader operations on ApacheStruts | |
| | | SYN flood attack | |
| | Brute force attack | Brute Force Attack on SSH, FTP | |
| | | Brute Force Attack on Web Login Screen | |

# WordPress diagnostic check summary

## ÿVulnerability check for WordPress is possible

* Please contact us for details, as each option item will be quoted separately.

| Inspection item | detail |
|---|---|
| WordPress vulnerability scan | Check if you are using a vulnerable version of WordPress |
| Vulnerability check for WordPress plugins | Installed plugins are checked for vulnerabilities* |
| Vulnerability check for WordPress theme | Checks for vulnerabilities in installed themes* |




* Detailed inspection cannot be performed if the content/plugin directory cannot be accessed from the CPE diagnosis source IP address due to access permissions, etc. Please set permission in advance.

# Signature update frequency

**ÿ [Platform (network) diagnosis] signature update frequency** (normal time)

regular work: once a week

• Updating platform signatures after release validation. • High frequency due to frequent occurrence of vulnerabilities related to middleware.

**ÿ [Web Application Diagnosis] signature update frequency**

(Normal time) Periodic work: once a month (addition of new diagnostic items once a quarter)

• Reviewing valid signatures at signature review meetings and updating signatures.
• Vulnerabilities related to Web applications rarely generate new diagnostic items.

**ÿ Emergency (Temporary) Signature Update** (Emergency)

Temporary work: Implemented each time it occurs (approximately one week after signature analysis and verification)

# Report screen image

## 1. Login screen ÿ

Customers from the dedicated portal site
You can use it by logging in with your ID/PW.


## 2. Diagnosis report viewing screen ÿ Vulnerabilities found in drill-down format for each IP address and URL are ranked,

You can see reports of risks and countermeasures.


## 3. Vulnerability statistics viewing screen ÿ Daily

vulnerability reports can be managed for one year. You can also view vulnerability statistics, such as the extent to which previously discovered vulnerabilities have been fixed and how often new vulnerabilities are discovered .

*Screen specifications are subject to change without notice.

# Notes ÿ

ÿ Frequency of access to target systems (approximate)

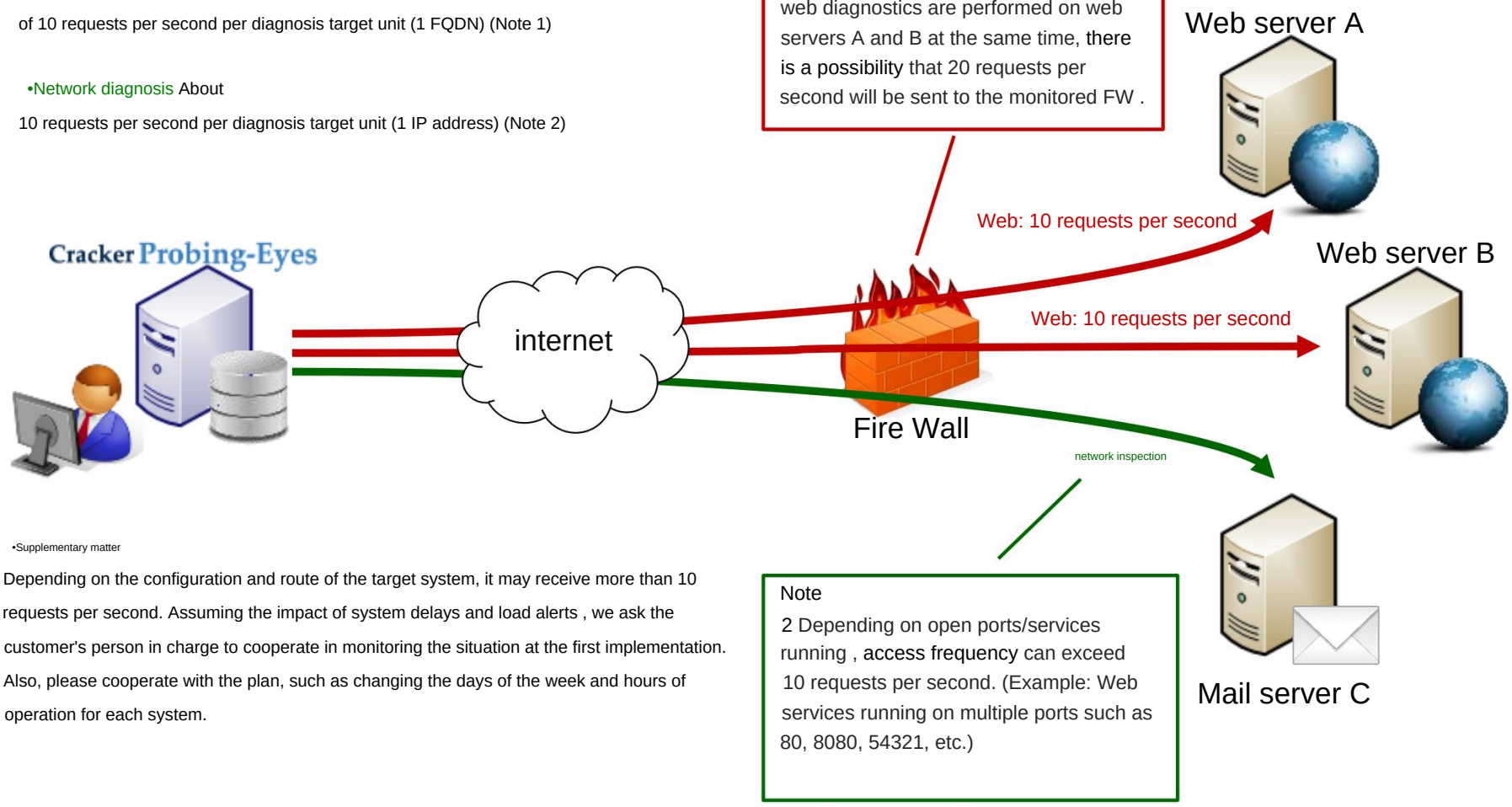
•Web application diagnosis A maximum

of 10 requests per second per diagnosis target unit (1 FQDN) (Note 1)

•Network diagnosis About

10 requests per second per diagnosis target unit (1 IP address) (Note 2)

*1 If
web diagnostics are performed on web servers A and B at the same time, there is a possibility that 20 requests per second will be sent to the monitored FW .




•Supplementary matter

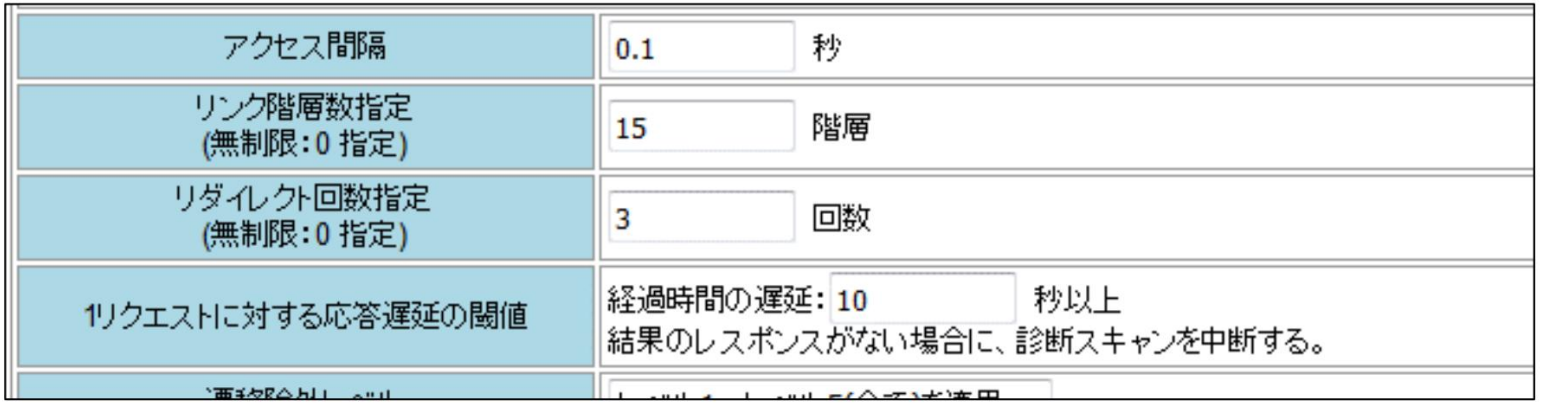
Depending on the configuration and route of the target system, it may receive more than 10 requests per second. Assuming the impact of system delays and load alerts , we ask the customer's person in charge to cooperate in monitoring the situation at the first implementation. Also, please cooperate with the plan, such as changing the days of the week and hours of operation for each system.

Note
2 Depending on open ports/services running , access frequency can exceed 10 requests per second. (Example: Web services running on multiple ports such as 80, 8080, 54321, etc.)

# Notes ÿ

## ÿ About access interval

In Web application diagnostics, access intervals can be set as follows. (Set value: 0.1 second interval) In the case of the following settings, after confirming the response of the target server, sleep for 0.1 seconds and send the next request, so it will not exceed 10 accesses per second.



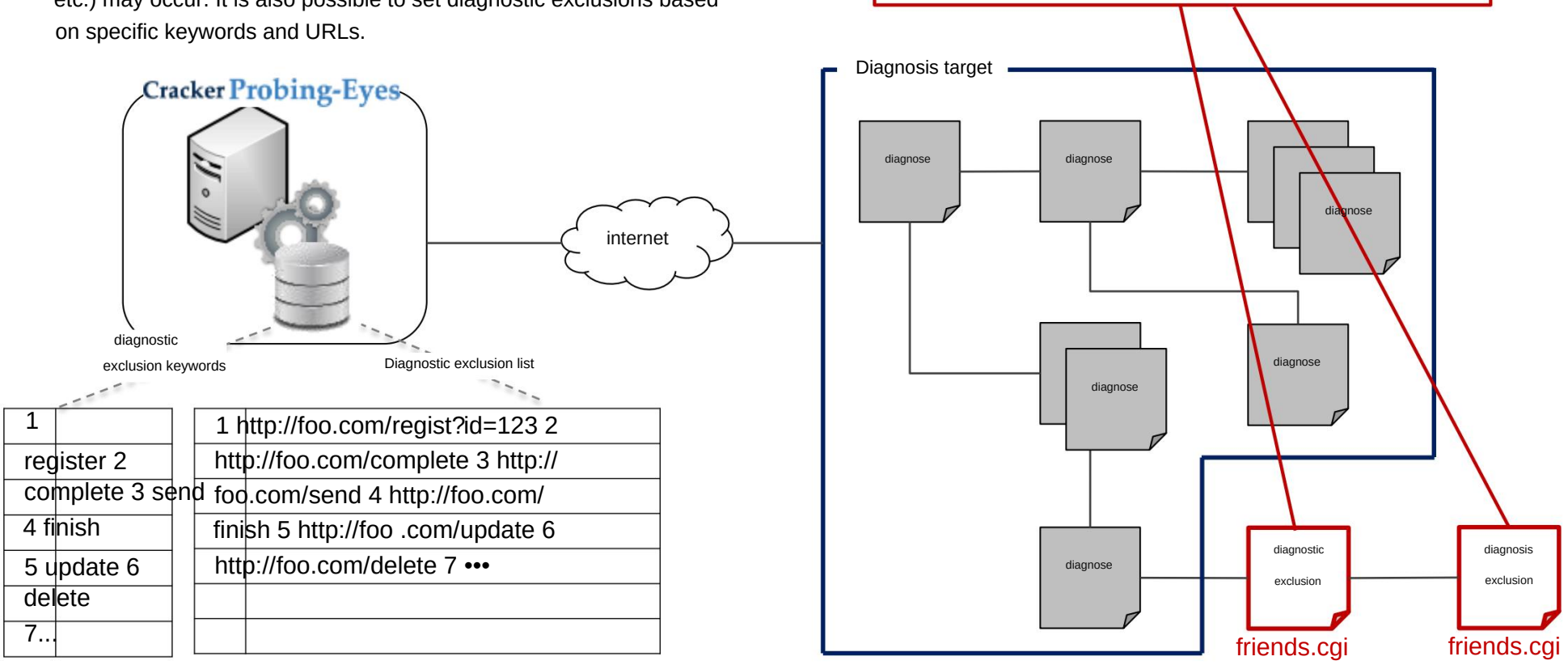
| | |
|---|---|
| アクセス間隔 | 0.1 秒 |
| リンク階層数指定<br>(無制限:0 指定) | 15 階層 |
| リダイレクト回数指定<br>(無制限:0 指定) | 3 回数 |
| 1リクエストに対する応答遅延の閾値 | 経過時間の遅延: 10 秒以上<br>結果のレスポンスがない場合に、診断スキャンを中断する。 |

# Note ÿ

## ÿ Access control (diagnosis/crawling)

In Web application diagnosis, the system automatically explores and accesses the screen to be diagnosed . Therefore, unintended data registration (sending from the inquiry form, updating user information, etc.) may occur. It is also possible to set diagnostic exclusions based on specific keywords and URLs.

In order to exclude from the system (blacklist registration) the targets and screens that you do not want to access, please provide the characteristics of the function and URL information. (Example: If you use the •• function, other users can view it, so exclude it. URL is http://example.com/friends.cgi etc.)




| |
|---|
| 1 |
| register 2 |
| complete 3 send |
| 4 finish |
| 5 update 6 |
| delete |
| 7... |

| |
|---|
| 1 http://foo.com/regist?id=123 2 |
| http://foo.com/complete 3 http:// |
| foo.com/send 4 http://foo.com/ |
| finish 5 http://foo .com/update 6 |
| http://foo.com/delete 7 ••• |
| |
| |

# Preparations on the customer side

The following preparations are mainly required on the customer side between ordering and scanning.

ÿ CPE diagnosis confirmation work (before ordering)

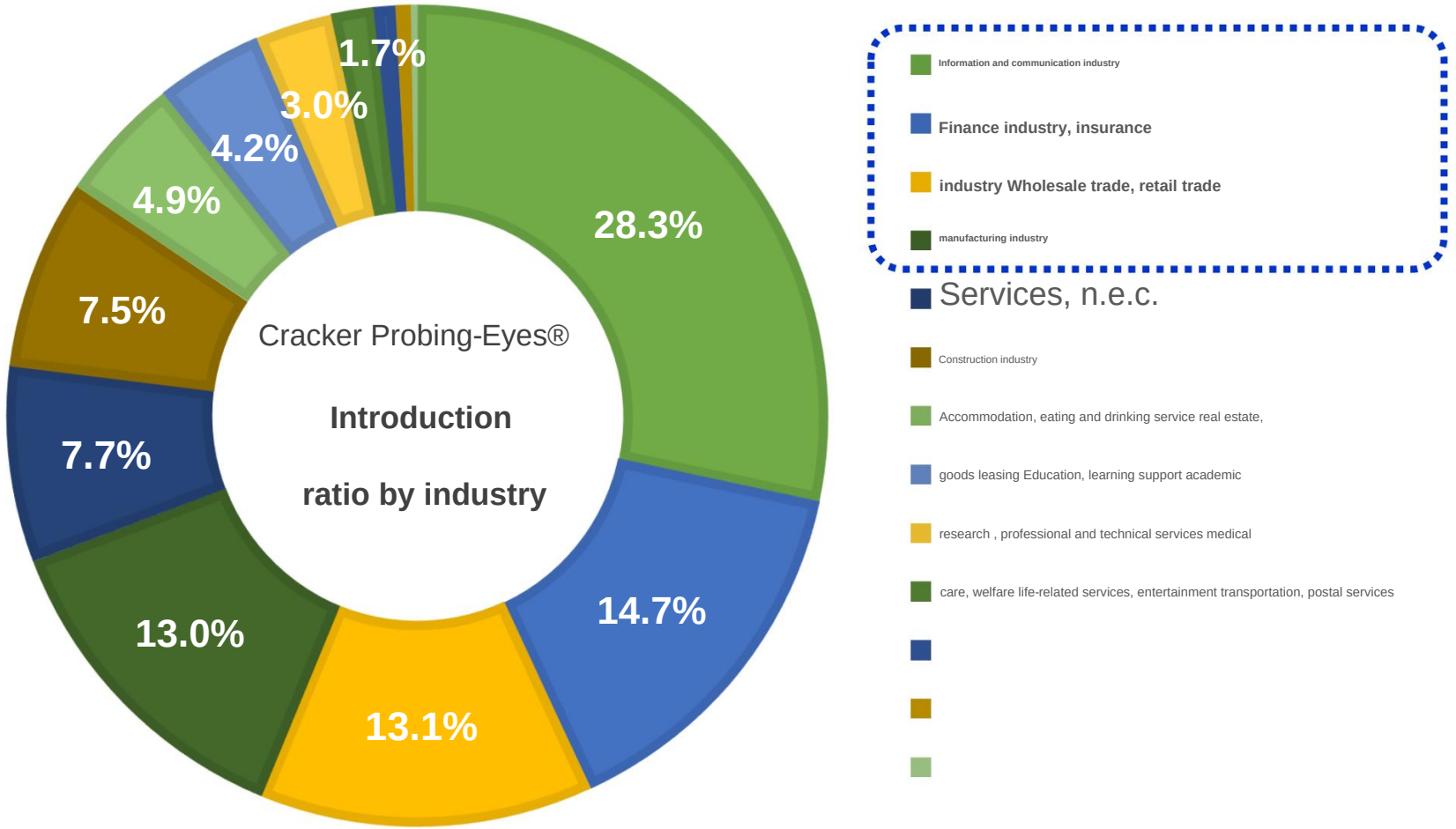
•If you wish to perform a web diagnosis, it may not be possible depending on the target HTML structure and request content, so our engineers will confirm the feasibility in advance. (It takes about 2-3 business days per URL.) ÿAccess preparation (after placing an order)•Access permission to CPE diagnosis source IP address •Authentication information •Account preparation (if you want a full scan) ÿApplication Fill out and send the form (after ordering)•Select the desired time for diagnosis The following is only for annual contracts•Confirm the email address to be notified of diagnosis completion, suspension, failure, and maintenance emails •To log in to the CPE portal Confirmation of e-mail address for account (ML not available) •Confirmation of desired diagnosis cycle Response to various inquiries (during crawling period)•Questions and confirmation from CPE support (continued during diagnosis period)•Details of crawling results Confirmation and response to whether or not scanning can be executed

# Cracker Probing-Eyes®

## Case study

# Implementation results by industry

It is mainly used for regular diagnostics on Web application development and provision, company product / service introduction sites, EC / community sites, etc.



# Introduction case list

| Industry | Company Name | scale | use case |
|---|---|---|---|
| wholesale, retail | A certain EC site operating company: Company S | about 20 sites | It is used for regular scanning after manual diagnosis for online shopping sites . |
| Professional and technical services | Certain IT solution company: Company F | about 10 sites | It is used for prior confirmation of the developed website before providing this service . |
| manufacturing industry | Certain steel company: Company J | about 30 sites | It is used for simple scanning of corporate websites that introduce steel-related products and product information. |
| entertainment industry | Certain game company: Company S | about 30 sites | It is used to regularly scan the platform for community sites for game-related content. |
| Insurance business | Certain insurance company: Company A | about 5 sites | It is used for regular scanning of members' sites for insurance-related information . |
| real estate business | Certain real estate company: Company T | about 20 sites | It is used for simple scanning of corporate websites with real estate-related information. |
| entertainment industry | Certain entertainment company: Company A | about 20 sites | It is used for regular scanning of community sites that distribute entertainment information. |

There are many other examples.