BioResource Now !

Issue Number 12 (2) 2016

National BioResource Project Information Center

The newsletter of this month introduces the portal site of the National BioResource Project (NBRP). The NBRP was inaugurated in 2002 and it has entered the final year of its third term in April 2016 (five years a term). The NBRP conducts the following four programs:

(1) Core Facility Updating Program
(2) Information Center Updating Program
(3) Genome Information Updating Program
(4) Fundamental Technologies Updating Program

The Core Facility Updating Program, a central program of the NBRP, has been promoted by 29 resource groups to "establish and improve systems for collecting, preserving, and providing bioresources as materials used for research and development." The NBRP Information Center is in charge of the second program, and its two major missions are to "manage the NBRP portal site (www.nbrp.jp)" and to "support the disclosure of information contained in the Core Facility Updating Program (presently, the disclosure of information on 20 out of 29 bioresources is supported)."

All information about the NBRP is publicly available at the NBRP portal site (Fig.1). Each of the 29 resource groups can be accessed on the webpage shown in Fig. 1-A, and the latest information on each center of the NBRP and its representative can be obtained from the webpage shown in Fig. 1-B.

Fig.1. NBRP portal site

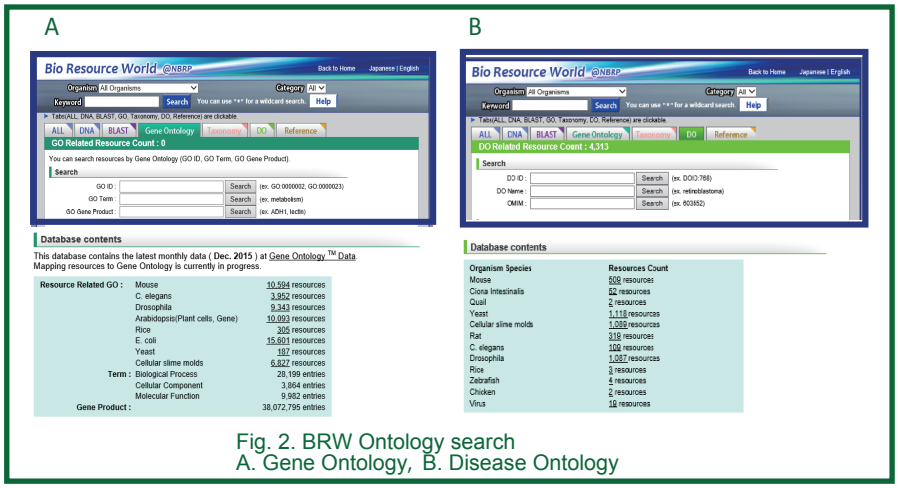

Fig. 2. BRW Ontology search
A. Gene Ontology, B. Disease Ontology

The contents and achievements of programs (3) and (4) are publicly available at the webpage shown in Fig.1-C and Fig.1-D, respectively. The activities of the three divisions responsible for the tasks of the Information Center Updating Program, "the Great Ape Information Network (GAIN)," "the Japan Node of Global Biodiversity Information Facility (GBIF)," and "the Access and Benefit Sharing (Nagoya Protocol) Task Force Team for Academia," are publicly available at the webpage as shown in Fig.s 1-E,1-F,1-G, respectively. Information on research papers using NBRP resources (Resource Research Circulation [RRC]) can be obtained from the webpage shown in Fig. 1-H. Research papers can also be registered on the RRC website. A liaison between the RRC and each resource database has been established so that information on research papers fed back from the users can be immediately reflected in the information on resources.

PubMed is a database of information on research papers that has been used by researchers across the world. PubMed provides a service known as LinkOut, which links information from each research paper to external databases. RRC uses this service and links more than 9000 research papers to the information sites of NBRP resources.Similar to the RRC, the main resource institutions of other countries too, such as Addgene, ATCC, CCR, GCM, JAXMice, PCC, and GRIN, are registered on LinkOut, with the number of institutions registered increasing with each year. Therefore, any information on a research material used for a research paper can be obtained with the guarantee of quality from a resource center through a formal procedure instead of obtaining the information directly from the author.

Another characteristic of the NBRP portal site is that all the resources provided by the 29 resource groups (6.5 million resources as of February 2016) can be searched for in the block (Bio Resource World [BRW]).

There are plans in the pipeline to develop a portal site in which if a user wants to access information about a specific resource, the site will systematically direct the user to the resource that meets the user's research purpose requirements.

The first stage of development is that besides keyword search and DNA sequence homology search, resources can be searched in the block using gene ontology, disease ontology, etc. (Fig. 2 A).

↳To the next page

These ontologies are uniquely added by the NBRP Information Center using external databases such as PubMed MeSH, Homologene, OMIM, dictyBase, WormBase, and ZFIN. Although the ontologies for the resources have not been sufficiently developed, there has been a significant increase in the number of resources with ontologies (Fig. 2 B). Presently, a majority of the researchers search for a resource after specifying the species, but at times it is quite possible that a resource of a different species may be suitable for the research purpose.

However, researchers find it difficult to use a new resource. For the convenience of such users, many resource institutions in the NBRP have held seminars for beginners on how to handle resources. The NBRP Information Center is also planning to improve information on resources further to establish a scheme by which researchers can select the most suitable research material from many options.

(responsibility for the wording: Yukiko Yamazaki).

Detecting Unauthorized Changes to Websites

It is essential to take sufficient countermeasures to prevent unauthorized changes from being made to websites. In the worst case that a website is found to have been modified fraudulently, a rapid response is required to prevent further damage. To achieve this objective, a framework for detecting unauthorized changes must be implemented.

While many commercial products are already available, in this article, I introduce an open source file integrity monitoring software for Linux. The intended audience for this article is server managers.

AIDE(Advanced Intrusion Detection Environment)

AIDE is an intrusion detection and file integrity verification tool that has been made available starting with Red Hat Enterprise Linux version 5 (RHEL5). AIDE saves the state of the files and directories to be monitored in a database (referred to as the baseline state), and it performs a periodical comparison between the current state and the baseline state to detect changes. AIDE can also be used with CentOS. It can be installed simply by running yum as follows:

```
#yum install aide
```

This completes the installation. The tool works using its default configuration; however, it is more effective if you limit the scope of the files and directories that are monitored. You can change this configuration by editing the configuration file "/etc/aide.conf" .

Standard detection rules defined in the default configuration file

NORMAL: Detects attribute changes such as file permissions and file size
DIR: Detects changes to directory permissions, extended file attributes, etc.
PERMS: Only detects file and directory permission changes
LOG: Detects increase in log file sizes
LSPP: Similar to NORMAL, but uses MD5 and SHA256 hash for recording the current state
DATAONLY: Only detects changes to file data

The files and directories to be monitored are specified after the detection rules are defined. The syntax is as follows. Use the "!" prefix to exclude objects from being monitored.

AIDE Configuration File Format

Target File or Directory: [Path] [Detection Rule]
Example: /home/hoge NORMAL
Exclusion List: ![Path]
Example: !/home/hoge/tmp

The next step after configuring the rules and the list of files and directories to be monitored is the initialization of the AIDE database. After creating the baseline, changes are detected by comparing the current state against this baseline. To update the baseline, run the command # aide --update. Once the initialization is successfully completed, the message shown in Fig.1 will be displayed.

```
#aide --init
```

```
AIDE, version 0.13.1

### AIDE database at /ver/lib/aide/aide.db.new.gz initialized.
```

Fig. 1. Initializing the file integrity monitoring database

Ongoing Column [No.102]

The name of the initialized database is not the default database that AIDE references, so it must be renamed as follows.

```
#mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
```

To compare the current state against the baseline, the following command is used. If no changes are detected, then the message shown in Fig.2 will be displayed.

```
#aide --check
```

```
AIDE, version 0.13.1

### All files match AIDE database. Looks okey!
```

Fig. 2. Result of integrity check

On the other hand, if changes are detected, then a report such as that shown below in Fig.3 will be displayed.

```
AIDE found differences between database and filesystem!!
Atart timestamp: 2016-01-28 11:46:48

Summary:
  Total number of files:       5
  Added files:                 0
  Removed files:               1
  Changed files:               2


---------------------------------------------------
Removed files:
---------------------------------------------------

removed: /home/hoge/hoge2.txt

---------------------------------------------------
Changed files:
---------------------------------------------------

changed: /home/hoge
changed: /home/hoge/hoge.txt

---------------------------------------------------
Detailed information about changes:
---------------------------------------------------


Directory: /home/hoge
  Mtime    : 2016-01-28 11:44:30          , 2016-01-28 11:46:34
```

Fig. 3. An example report showing detected changes.

After validation, if all changes turn out to be legitimate, then a new baseline must be established and the old baseline must be overwritten. This will make the state after modification the new baseline. The baseline is updated as follows.

```
#aide --update
#mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
```

Strengths and weaknesses of AIDE

The strengths of AIDE over other integrity checking tools are that it has all the required functionality and can be implemented for free. At the same time, its weaknesses are the lack of additional features such as user notification, auto-repair, and approval workflow. These functions must be programmed by yourself. If you require features that AIDE lacks, then you should consider buying commercial integrity checking products. The prices vary, but all commercial tools will have a notification function built-in by default. However, the price will increase with the number of features. The pricing models differ from product to product, making a direct comparison difficult; relatively inexpensive products start for less than $100, but high-end products can be as expensive as several tens of thousands of dollars. Therefore, you should carefully determine your requirements first and then choose the optimal intrusion detection and file integrity monitoring tool to meet your needs.

The AIDE tool introduced in this article can be used with RHEL 5 or CentOS 5 or later. Because both the implementation and the configuration are easy, you should definitely implement it if you would like to try out a file integrity monitoring tool.

(Tohru Watanabe)

Contact Address

Genetic Resource Center, National Institute of Genetics
1111 Yata, Mishima-shi, Shizuoka 411-8540, Japan
Tel.: 055-981-6885 (Yamazaki)
E-mail： brnews@shigen.info

BioResource Information

(NBRP) www.nbrp.jp/
(SHIGEN) www.shigen.nig.ac.jp/
(WGR) www.shigen.nig.ac.jp/wgr/
(JGR) www.shigen.nig.ac.jp/wgr/jgr/jgrUrlList.jsp

Editor's Note

The recent updates from the NBRP Information Center have been introduced by the publisher of this newsletter for the first time in many years. Previously, the Introduction to the Resource Center was published in the October 2011 issue. It was slightly depressing to realize that only a small part of the vigorous "plans" I had written five years ago could be achieved. However, all I can do is just keep going! (Y. Y.).

BioResource Now !
Issue Number 12 (2) 2016
"translated by ASL translation service"