Design and development of vulnerability management portal for DMZ admins powered by DBPowder

Tadashi Murakami   High energy accelerator research organization (KEK)

Security management in DMZ network

- Especially in public servers (**DMZ servers**), server admins have to spend a lot of effort to maintain the security
- It may be efficient for the security to be managed in **command-hierarchical** manner, however, it may **reduce variety and flexibility**
- In some of research institute, like KEK, DMZ servers are operated like below:

various usage
- experiment
- login shells
- public relations
- etc

various kind of research

various users

various kind of groups (e.g. num of members are 10 - 1000)

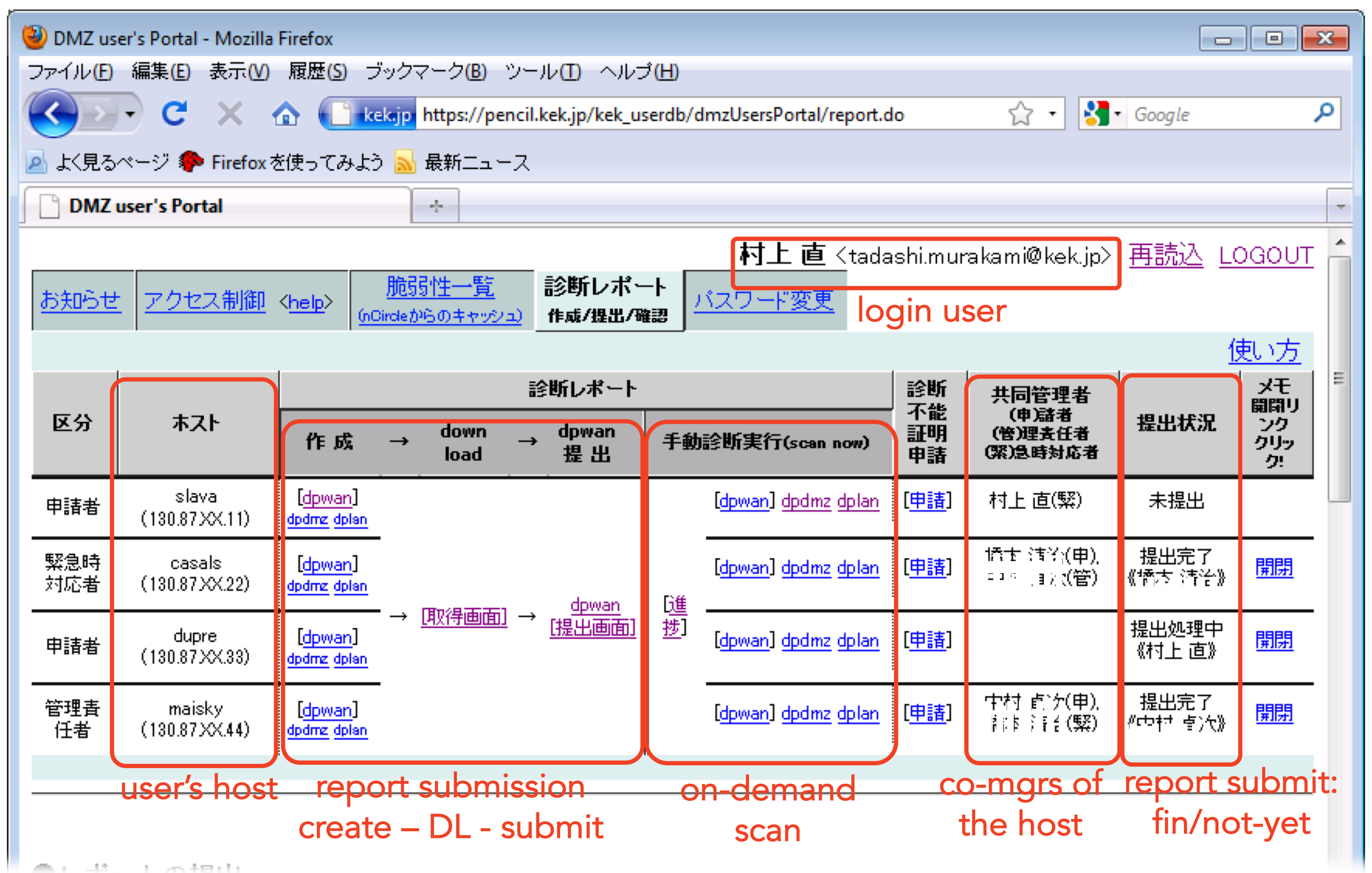
login shell with **hundreds** of accounts in **various** countries

various level of management skill

- **Command-hierarchical manner is not suitable in research institutes**
  - It is difficult to cover various circumstances
  - In research institutes, variety and flexibility are crucially important

DMZ User's Portal

to maintain security with keeping variety and flexibility of DMZ hosts



DMZ user's Portal - Mozilla Firefox

https://pencil.kek.jp/kek_userdb/dmzUsersPortal/report.do

村上 直 <tadashi.murakami@kek.jp> 再読込 LOGOUT

お知らせ アクセス制御 <help> 脆弱性一覧 (nCircleからのキャッシュ) 診断レポート 作成/提出/確認 パスワード変更

login user

使い方

区分	ホスト	診断レポート 作成 → down load → dpwan 提出	手動診断実行(scan now)	診断不能証明申請	共同管理者 (申)請者 (管)理責任者 (緊)急時対応者	提出状況	メモ開閉リンククリック!
申請者	slava (130.87.XX.11)	[dpwan] dpdmz dplan	[dpwan] dpdmz dplan	[申請]	村上 直(緊)	未提出	
緊急時対応者	casals (130.87.XX.22)	[dpwan] dpdmz dplan → [取得画面] → dpwan [提出画面]	[進捗] [dpwan] dpdmz dplan	[申請]	[illegible](申), [illegible](管)	提出完了 《[illegible]》	開閉
申請者	dupre (130.87.XX.33)	[dpwan] dpdmz dplan	[dpwan] dpdmz dplan	[申請]		提出処理中 《村上 直》	開閉
管理責任者	maisky (130.87.XX.44)	[dpwan] dpdmz dplan	[dpwan] dpdmz dplan	[申請]	中村 [illegible](申), [illegible](緊)	提出完了 《中村 [illegible]》	開閉

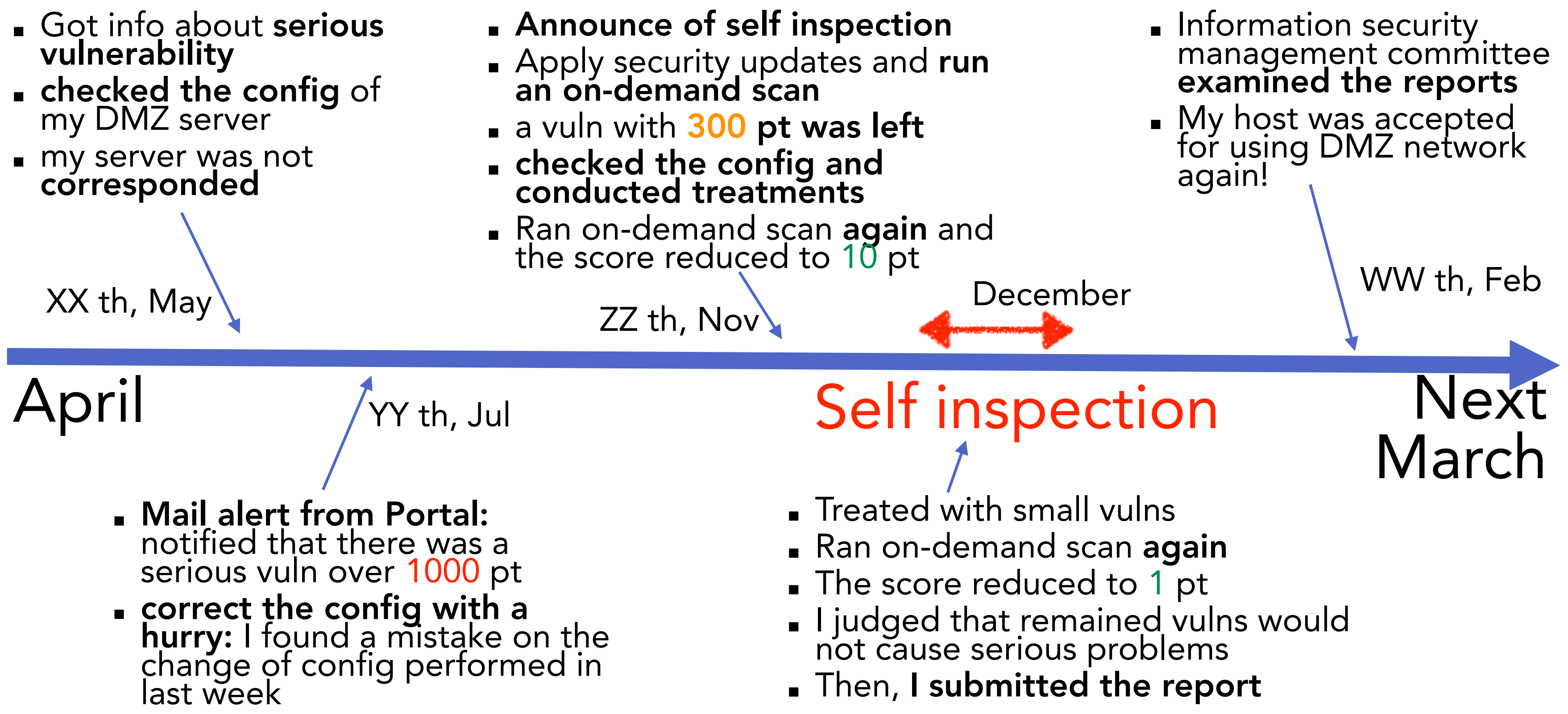
- We introduced and operate a vulnerability scanner for DMZ server admins
- Because of rich functions themselves, the vuln scanner is intricate to use
- To simplify, we develop **DMZ User's Portal** that wraps the functions and promotes self security management for DMZ admins, as the points below:

POINT1: provide easy-operation user-interface to manage and handle the vulns by DMZ admins themselves

POINT2: with **harmony** of **support** and **command-hierarchy**
- **support:** DMZ admins can conduct the vulnerability scan by their own
- **support:** The portal collect and aggregate the info to maintain the security
- **command-hierarchy:** the portal helps the duty for DMZ admins to self-inspect their hosts annually, by providing the management interface

POINT3: feedback the vuln info of their host in **multi** and **continuous way**
- Three scanners are set in WAN, DMZ, LAN, which assume attacks from the locations
- regular scan per week by the portal / on-demand scan by DMZ admin
- The vulnerability list can be browsed together / downloaded in each host
- When serious vulnerabilities are found on a DMZ host, the portal notifies the info per week by email
- Various feedback ways shown above help to determine the priority to measure

Self inspection ~ a story of admin task in one year (April to March)



- Got info about **serious vulnerability**
- **checked the config** of my DMZ server
- my server was not **corresponded**

XX th, May

- **Mail alert from Portal:** notified that there was a serious vuln over 1000 pt
- **correct the config with a hurry:** I found a mistake on the change of config performed in last week

YY th, Jul

- **Announce of self inspection**
- Apply security updates and **run an on-demand scan**
- a vuln with **300 pt was left**
- **checked the config and conducted treatments**
- Ran on-demand scan **again** and the score reduced to 10 pt

ZZ th, Nov

December

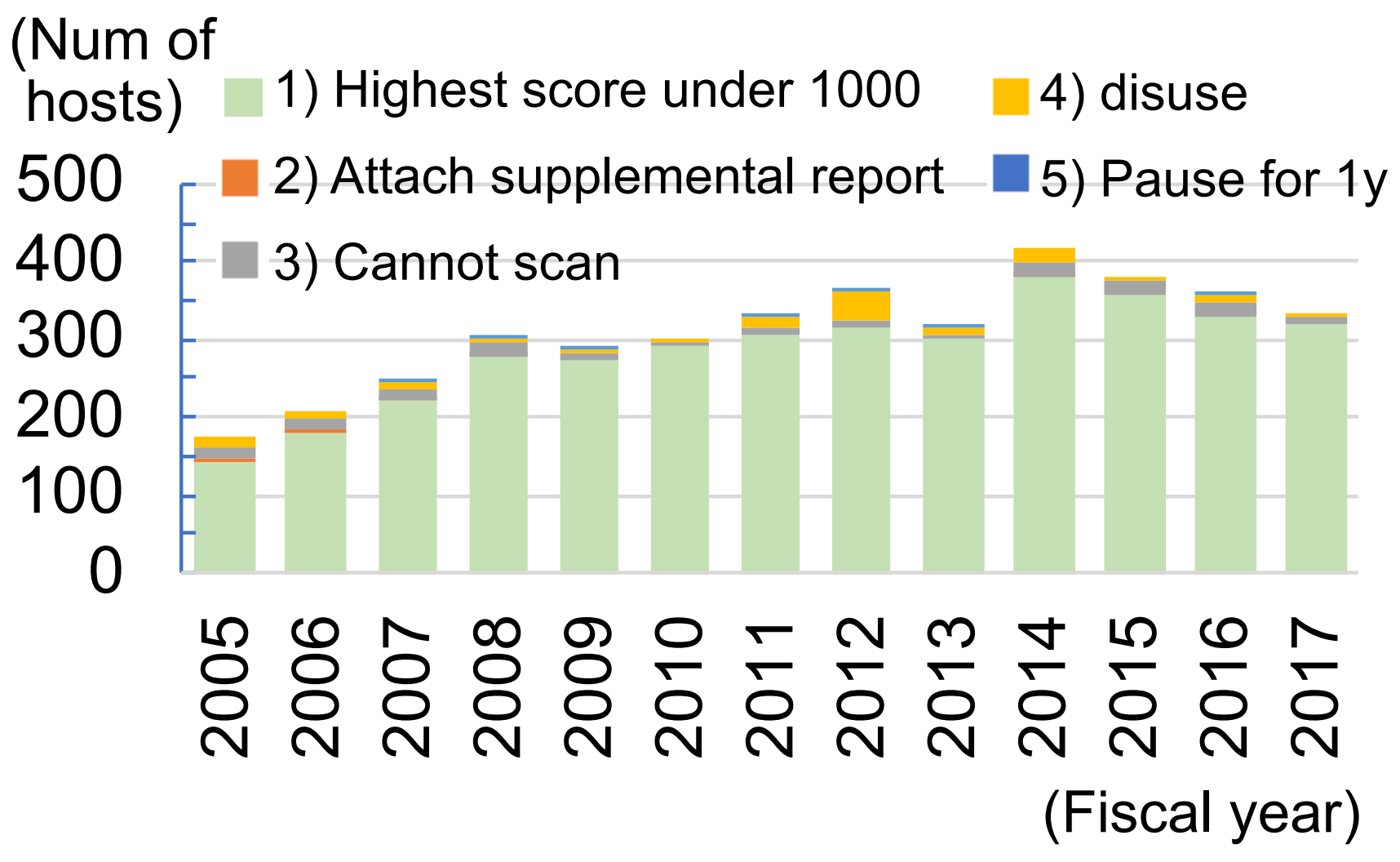
Self inspection

- Treated with small vulns
- Ran on-demand scan **again**
- The score reduced to 1 pt
- I judged that remained vulns would not cause serious problems
- Then, **I submitted the report**

- Information security management committee **examined the reports**
- My host was accepted for using DMZ network again!

WW th, Feb

Statistics of the self inspection: submit a report

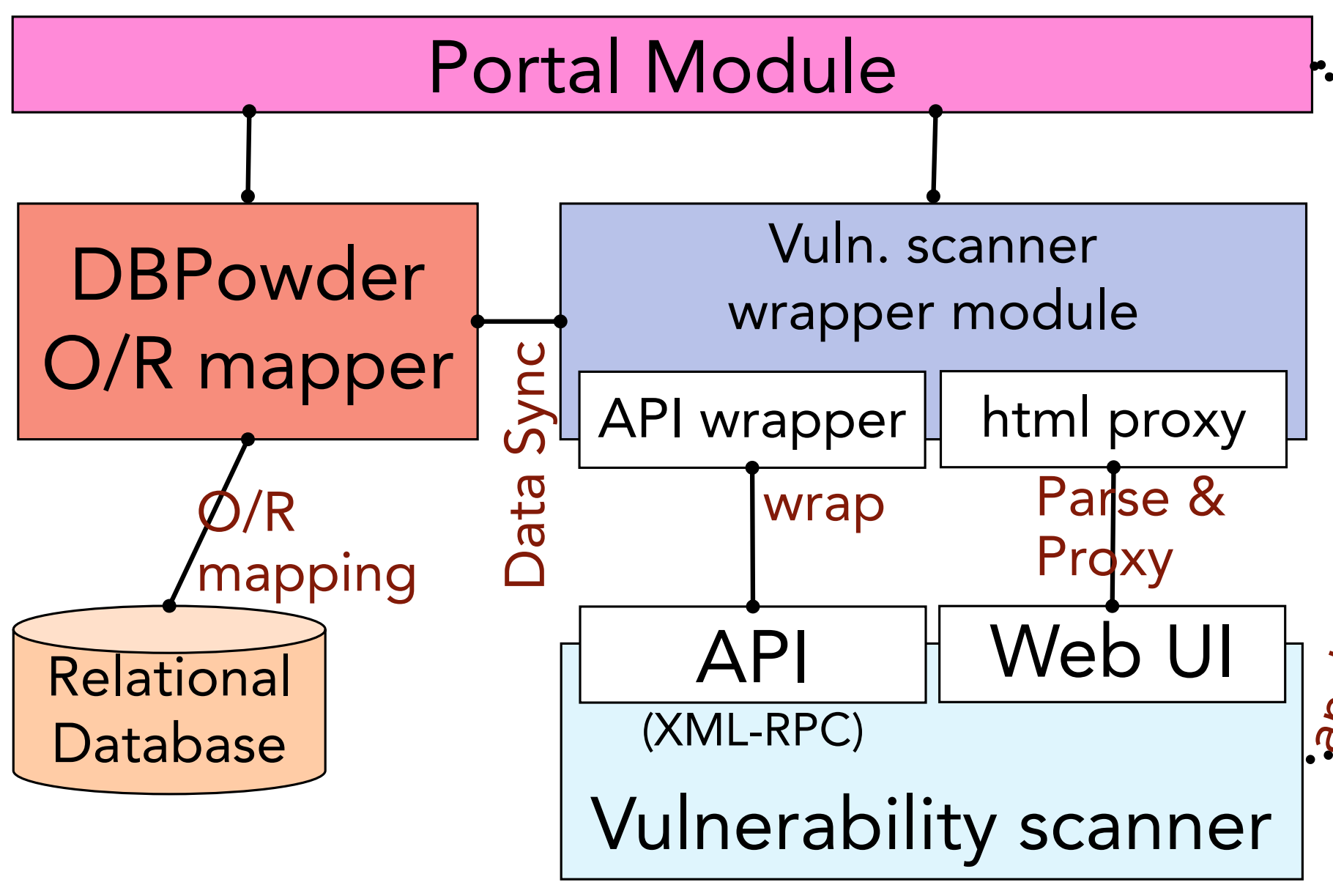


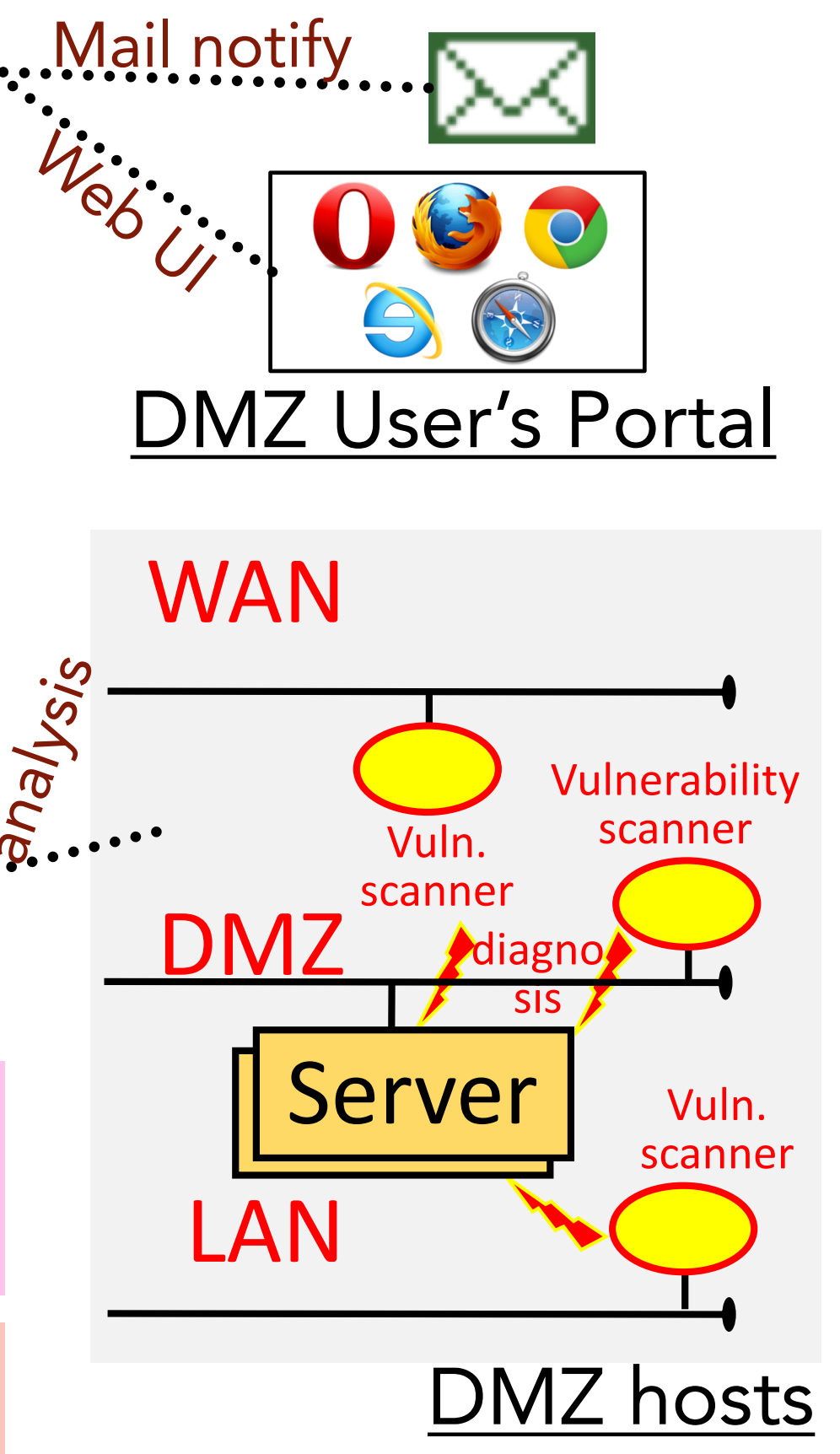
- Started in 2005 (Fiscal year)
  - Security managers in divisions help the operation a lot
- Num of hosts increases every year
- Most of hosts end in 1) or 2): submission is completed

1) under 1000 pt
- There are no vulns with red score left

2) supplemental report
- a report that explains of false-positives

System design of DMZ User's Portal





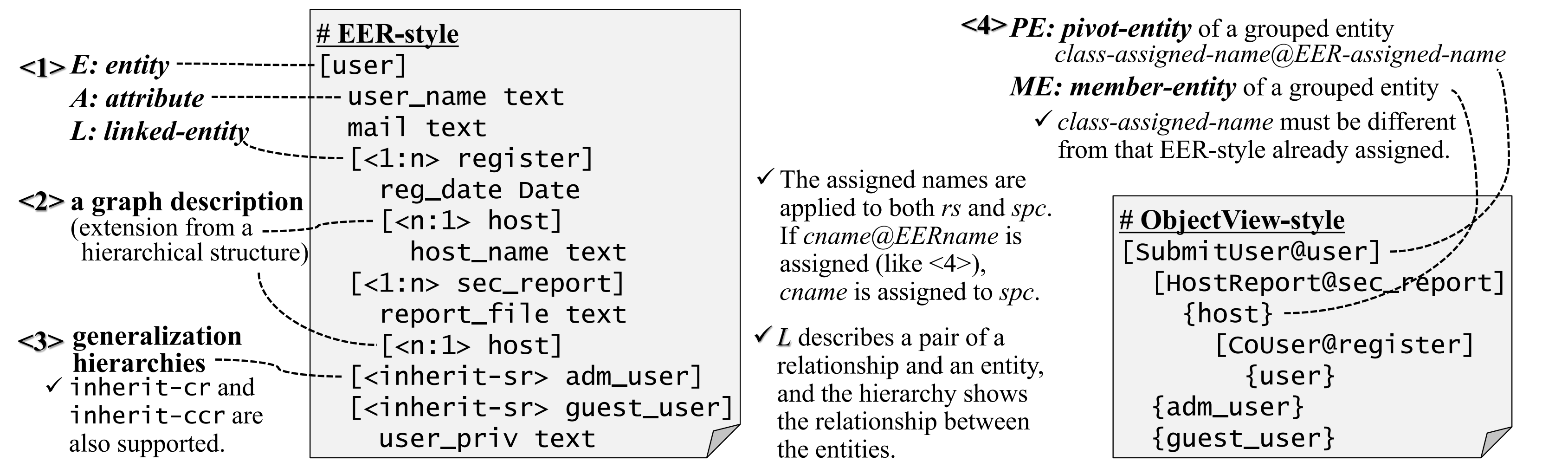
Vuln. scanner is always called via wrapper module
- to reduce the module dependency to the vuln. scanner
- to endure the change of specification in vuln. scanner

- **Portal Module:** to provide functions of portal site using DBPowder and wrapper module
- **DBPowder** (O/R mapper): to bridge database (MySQL) to Portal Module
  - Using MySQL via Object-Relational Mapping Module
- **Wrapper module:** to call vuln. scanner
  - **API** in vuln scanner does not support some important functions such as pdf-report download
  - **Html proxy module** supports such essential functions for portal module
  - Html proxy module parses and interprets html generated by vulnerability scanner

[1] Murakami, T., Amagasa, T. and Kitagawa, H.: DBPowder: A Flexible Object-Relational Mapping Framework Based on a Conceptual Model, IEEE-COMPSAC, 2013.

[2] Murakami, T. DBPowder-mdl: EoD Featured and Much Descriptive Domain Specific Language for O/R Mapping IPSJ-TOD, 2010.

DBPowder-mdl [1]: schema description language



```
# EER-style
[user]
  user_name text
  mail text
  [<1:n> register]
    reg_date Date
    [<n:1> host]
      host_name text
  [<1:n> sec_report]
    report_file text
    [<n:1> host]
  [<inherit-sr> adm_user]
  [<inherit-sr> guest_user]
    user_priv text
```

```
# ObjectView-style
[SubmitUser@user]
  [HostReport@sec_report]
    {host}
      [CoUser@register]
        {user}
  {adm_user}
  {guest_user}
```

<1> *E: entity*
A: attribute
L: linked-entity

<2> **a graph description** (extension from a hierarchical structure)

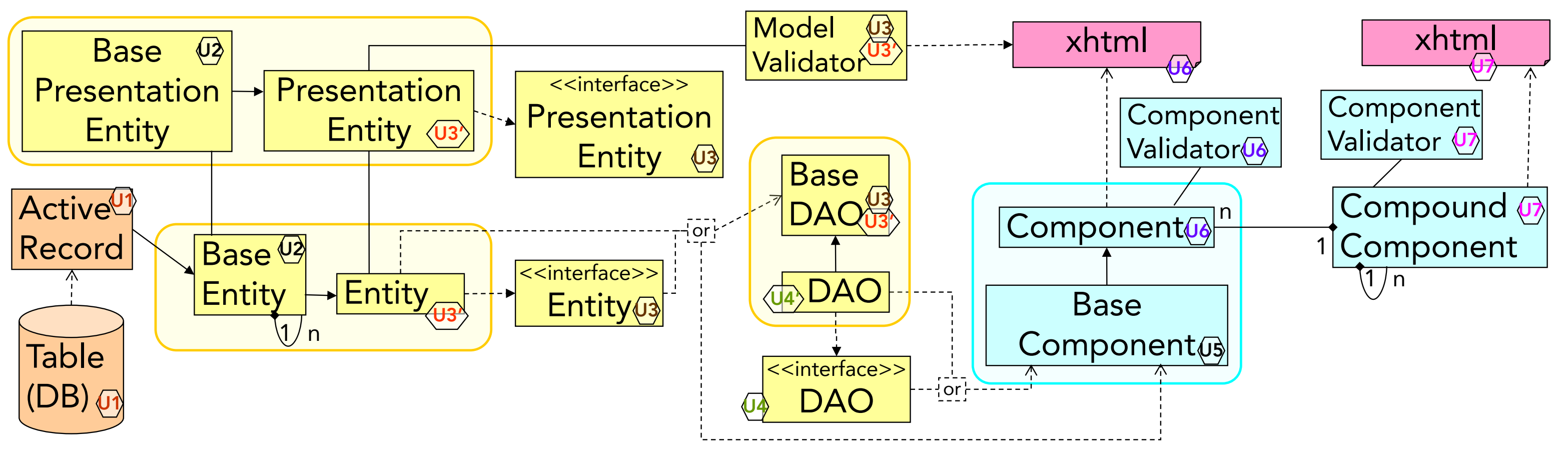
<3> **generalization hierarchies**
✓ inherit-cr and inherit-ccr are also supported.

✓ The assigned names are applied to both *rs* and *spc*. If *cname@EERname* is assigned (like <4>), *cname* is assigned to *spc*.

✓ *L* describes a pair of a relationship and an entity, and the hierarchy shows the relationship between the entities.

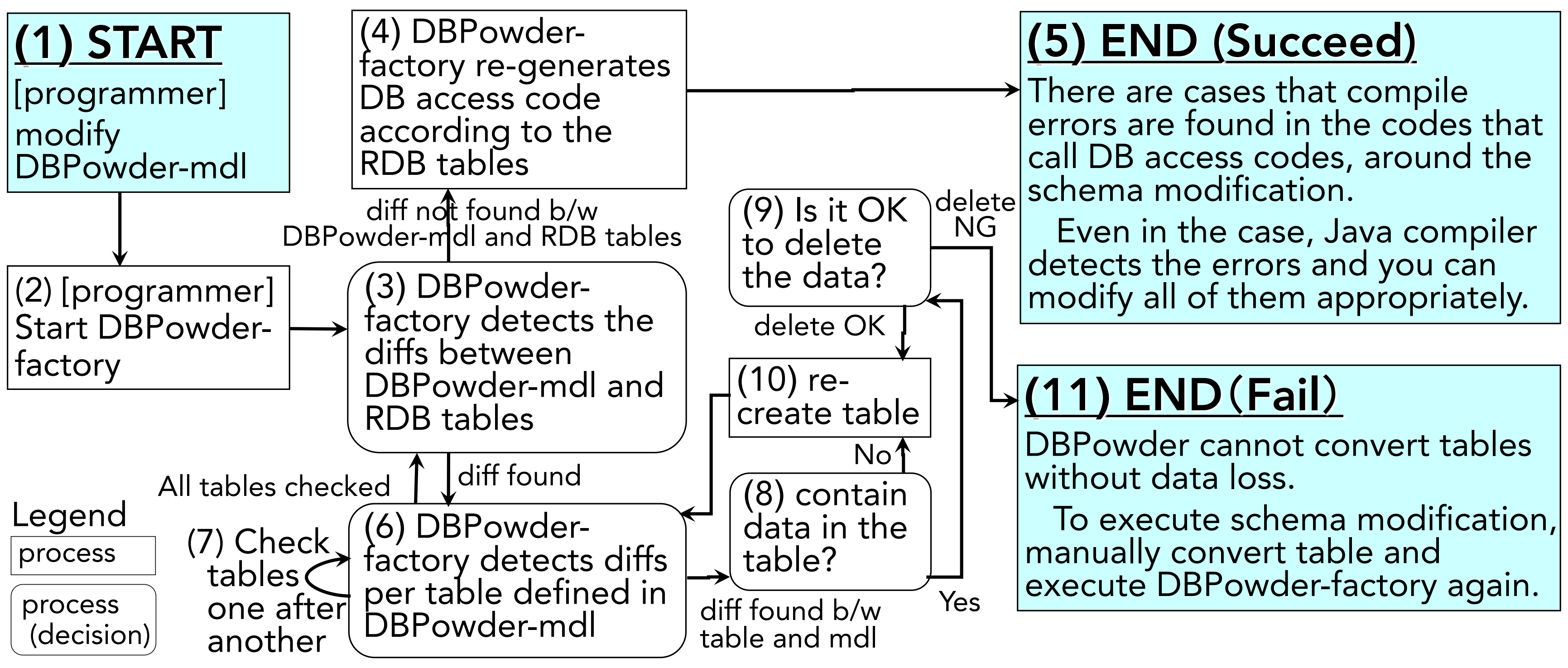
<4> ***PE: pivot-entity*** of a grouped entity
class-assigned-name@EER-assigned-name
ME: member-entity of a grouped entity
✓ *class-assigned-name* must be different from that EER-style already assigned.

Class structure of DBPowder (O/R mapping)



- Except for base classes, code generator generates all of codes
- Entities can have a relationship between them

Helper for database schema modification in DBPowder



(1) START
[programmer] modify DBPowder-mdl

(2) [programmer] Start DBPowder-factory

(3) DBPowder-factory detects the diffs between DBPowder-mdl and RDB tables

(4) DBPowder-factory re-generates DB access code according to the RDB tables

(5) END (Succeed)
There are cases that compile errors are found in the codes that call DB access codes, around the schema modification.
Even in the case, Java compiler detects the errors and you can modify all of them appropriately.

(6) DBPowder-factory detects diffs per table defined in DBPowder-mdl

(7) Check tables one after another

(8) contain data in the table?

(9) Is it OK to delete the data?

(10) re-create table

(11) END（Fail）
DBPowder cannot convert tables without data loss.
To execute schema modification, manually convert table and execute DBPowder-factory again.

Extended DMZ User's portal to other networks

- DMZ User's portal is implemented in a flexible manner. It enabled to extend the portal to other two sites in 2011 and 2016 (J-PARC, HEPnet-J)

Conclusions

- In research institutes, variety and flexibility are crucially important --- also in DMZ network
- We developed and operate DMZ User's Portal
  - with harmony of support and command-hierarchy
  - feedback the vulnerability information of their host in multiple and continuous way
- Operation over 10 years shows the validity
- Flexible implementation enables to expand DMZ User's Portal to other sites