

laCスクリプトの欠陥を分類

Gang of Eight: A Defect Taxonomy for Infrastructure as Code Scripts

Akond Rahman, Effat Farhana, Chris Parnin, Laurie Williams

ICSE 2020

背景 (1/2)

- IT分野では, puppetやchefなどのツールを用いて
IaCの実践が行われている
 - General Motor:デプロイ頻度が21倍 [20]
 - CERN:15000台を管理し, 毎日2000テラバイトのデータを処理 [7]
- 深刻な問題を伴う欠陥が現れることがある
 - AWS:1億5000万のビジネス損失 [23]
 - Githubの停止 [19]
 - Wikimedia commonsのユーザディレクトリの削除 [12]

背景 (2/2)

- 欠陥分類の重要性
 - verification & validation活動に集中するのに役立つ[39]
 - バグトリアージのプロセスにおいて重要なステップ[6]
- 特殊なソフトウェアの欠陥分類は複数研究行われている
 - Android, ディープラーニング, ブロックチェーンなど

laCの分野では行われていない

リサーチクエストション

RQ1：カテゴリ化

OpenStack

- IaCにはどのようなカテゴリの欠陥が現れるのか？

RQ2：認識

66人

- カテゴリ化されたIaCの欠陥を実務者はどのように認識しているのか？

RQ3：頻度

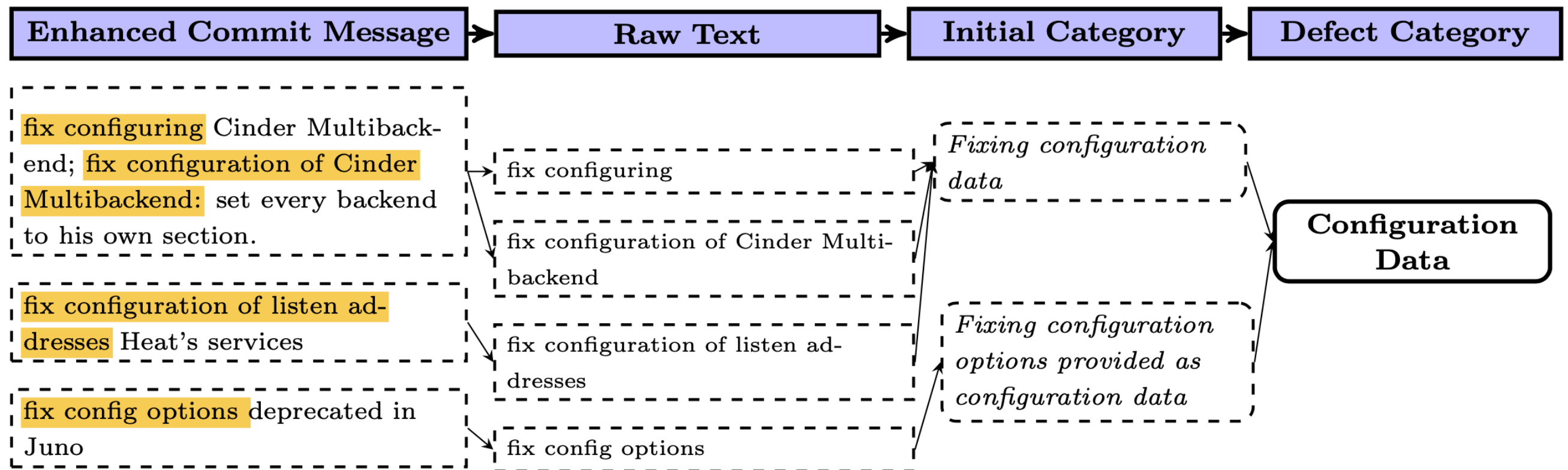
自動識別ツールACIDを開発し、
4プロジェクトを分析

- 同定された欠陥カテゴリはIaCにどの程度の頻度で出現するのか？

RQ1 IaCにはどのような欠陥があるのか？

ECM(Enhanced Commit Message)を用いて定性分析を行う

- コミットメッセージと既存バグレポート記述の組み合わせ



2つの初期カテゴリを組み合わせると

両方とも設定データの欠陥を修正する内容であることがわかる

RQ1 IaCにはどのような欠陥があるのか？

Idempotency	IaCスクリプトのIdempotencyプロパティに違反する欠陥
Config. Data	IaCスクリプトに存在する誤った設定データが 原因で発生する欠陥
Dependency	依存関係による欠陥
Security	ログでの機密の公開, パスワードなどの秘密のハードコーディングなど
Syntax	IaCスクリプトの構文に関する欠陥
Conditional	条件分岐による欠陥
Documentation	IaCスクリプトに関する誤った情報が 指定された場合に発生する欠陥
Service	不適切なプロビジョンや可用性に関連する欠陥

RQ1 IaCにはどのような欠陥があるのか？

Idempotency

IaCスクリプトのIdempotencyプロパティに違反する欠陥

Config. Data

Idempotency

る誤った設定データが
生ずる欠陥

1回目の実行結果とN ($n > 1$) 回目の実行結果
全く同じであることを保証するプロパティ
→ IaCスクリプトならではの欠陥であると言える

Conditional

条件分岐による欠陥

Documentation

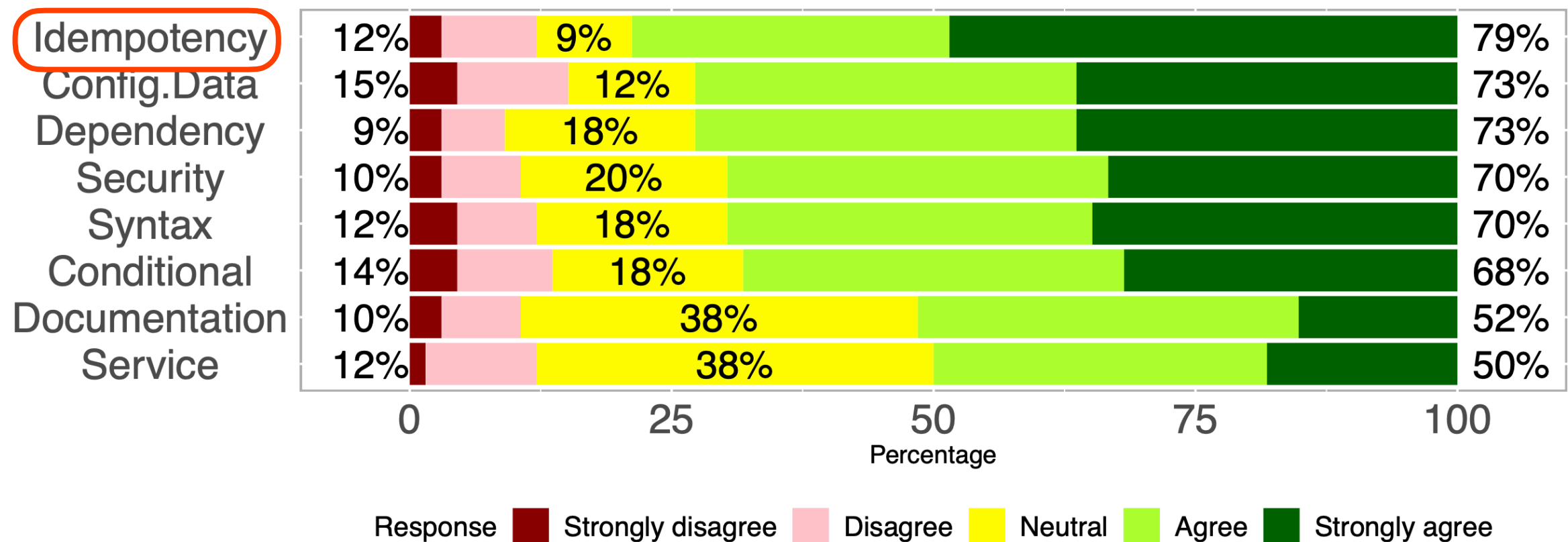
IaCスクリプトに関する誤った情報が
指定された場合に発生する欠陥

Service

不適切なプロビジョンや可用性に関連する欠陥

RQ2 分類された欠陥を実務者はどう認識しているのか？

- 66名/750名 (8.8%) が回答
 - ソフトウェア工学の研究では決して珍しいことではない [69]



- idempotencyに遭遇したことがないという意見も
- 頻繁な依存関係の欠陥発生はIaCの限界かも

RQ3 同定された欠陥カテゴリはIaCにどの程度の頻度で出現するのか？

自動識別手法ACIDの手順

ECMをトークン化 テキスト前処理 依存関係解析[32] ルールマッチング

Step #1	Step #2	Step #3	Step #4
Update incorrect comment about nova-network status	updat incorrect comment about nova network statu	HEAD:[updat], DEPE:[comment]	Rule matched for documentation defect as per Table 2
The network manifest contained a comment that said that nova-network was no longer receiving any patches.	network manifest contain comment that said that nova network was no longer receiv ani patch	HEAD:[contain], DEPE:[comment]	No match
That's not actually the case; so replace the comment with a new description that describes the current state.	that not actual case so replac comment with new descript that describ current state	HEAD:[replac], DEPE:[comment]	No match

具体例

- ECM

Update **incorrect comment** about nova-network status

Category	Rule	Function	String Pattern
Conditional	$hasDefect(x.sen) \wedge hasCond(x.sen.dep)$	$hasDefect()$	'error', 'bug', 'fix', 'issu', 'mistake', incorrect , 'fault', 'defect', 'flaw'
Configuration Data	$hasDefect(x.sen) \wedge ((hasStorConf(x.sen.dep) \vee hasFileConf(x.sen.dep) \vee hasNetConf(x.sen.dep) \vee hasUserConf(x.sen.dep) \vee hasCachConf(x.sen.dep)) \vee dataChanged(x.diff))$	$hasCond()$	'logic', 'condit', 'boolean'
		$hasStorConf()$	'sql', 'db', 'databas'
		$hasFileConf()$	'file', 'permiss'
		$hasNetConf()$	'network', 'ip', 'address', 'port', 'tcp', 'dhcp'
		$hasUserConf()$	'user', 'usernam', 'password'
Dependency	$hasDefect(x.sen) \wedge (hasDepe(x.sen.dep) \vee changedInclude(x.diff))$	$hasCachConf()$	'cach'
		$hasDepe()$	'requir', 'depend', 'relat', 'order', 'sync', 'compat', 'ensur', 'inherit'
Documentation	$hasDefect(x.sen) \wedge (hasDoc(x.sen.dep) \vee changedComment(x.diff))$	$hasDoc()$	'doc', comment , 'spec', 'licens', 'copyright', 'notic', 'header', 'readm'
Idempotency	$hasDefect(x.sen) \wedge hasIdem(x.sen.dep)$	$hasIdem()$	'idempot'
Security	$hasDefect(x.sen) \wedge hasSecu(x.sen.dep)$	$hasSecu()$	'vulner', 'ssl', 'secur', 'authent', 'password', 'secur', 'cve'
Service	$hasDefect(x.sen) \wedge (hasServ(x.sen.dep) \vee changedService(x.diff))$	$hasServ()$	'servic', 'server'
		$hasSynt()$	'compil', 'lint', 'warn', 'typo', 'spell', 'indent', 'regex', 'variabl', 'whitespac'
Syntax	$hasDefect(x.sen) \wedge hasSynt(x.sen.dep)$		

```
# [*enabled*]
# (optional) Whether the network service should be enabled.
-# Defaults to false
+# Defaults to true
```

RQ3 同定された欠陥カテゴリはIaCにどの程度の頻度で出現するのか？

自動識別手法ACIDの評価

- 22人の大学院生レベルの学生で評価用データセットを構築
- 各ECMが2人以上にレビューされるように132個をレビュー

Category	Occurr.	Precision	Recall
Conditional	6	0.75	1.00
Configuration Data	29	0.91	1.00
Dependency	3	0.75	1.00
Documentation	6	0.75	1.00
Idempotency	3	0.75	1.00
Security	1	1.00	1.00
Service	13	0.85	0.85
Syntax	6	0.86	1.00
No defect	65	0.96	0.82
Average		0.84	0.96

全てのデータセットとACIDのソースコードは公開されている

- <https://hub.docker.com/r/akondrahman/acid-puppet>

RQ3 同定された欠陥カテゴリはlaCにどの程度の頻度で出現するのか？

データセット

- リポジトリに属するファイルの11%以上がlaCスクリプトであること
- リポジトリの他のリポジトリのコピーでないこと
- リポジトリのコミット数が月に2回以上であること
- リポジトリには少なくとも貢献者が10人はいること

Table 7: Attributes of the Four Datasets

Attribute	GHB	MOZ	OST	WIK
Repo. Type	Git	Mercurial	Git	Git
Tot. Repos	218	2	61	10
Tot. Commits	434,234	14,449	44,469	71,795
Tot. Puppet Scripts	10,025	1,596	2,845	3,143
Tot. Puppet-related Commits	40,286	6,836	12,227	21,066
Time Period	01/2005- 04/2019	05/2011- 04/2019	09/2011- 04/2019	01/2006- 04/2019

RQ3 同定された欠陥カテゴリはlaCにどの程度の頻度で出現するのか？

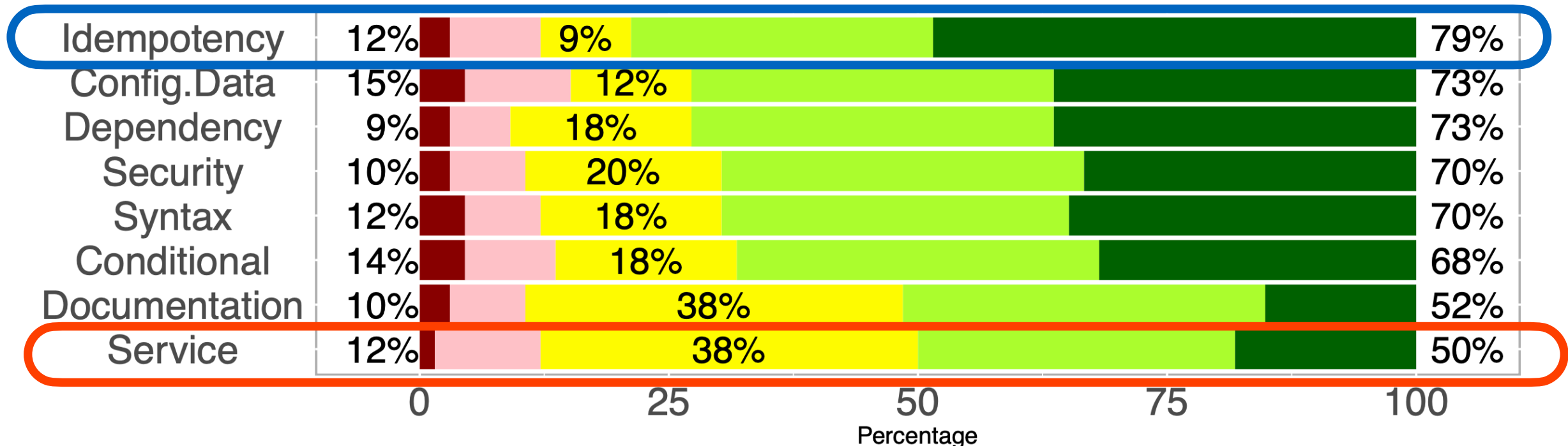
少なくとも1つのカテゴリの欠陥を含むコミットで修正されたスクリプトの割合

Categ.	Defect Prop. (%)				Script Prop. (%)			
	GHB	MOZ	OST	WIK	GHB	MOZ	OST	WIK
Cond.	0.3	0.04	0.3	0.1	1.9	0.3	1.8	1.4
Conf.Data	9.5	3.8	11.5	7.2	29.2	23.5	33.9	29.6
Depe.	1.8	1.3	2.4	1.7	10.6	12.4	16.3	17.1
Docu.	1.7	0.8	1.6	1.5	13.7	7.2	14.0	13.6
Idem.	0.1	0.01	0.3	0.01	1.0	1.6	3.5	0.1
Secu.	0.1	0.5	0.5	0.1	0.9	5.5	2.8	1.1
Serv.	1.4	2.6	1.8	3.0	4.9	23.1	9.3	12.4
Synt.	2.8	1.7	2.3	2.4	16.3	9.2	19.2	17.4
Total	16.6	10.9	18.7	15.2	43.6	47.4	48.6	49.2

少なくとも1つのカテゴリの欠陥を含むコミット

- コミットの11~19%がいずれかの欠陥を含む
- 全laCスクリプトのうち40~50%が欠陥カテゴリを含む

議論 ～ 特定されたカテゴリと実務者の認識の相違 ～



Categ.	Defect Prop. (%)				Script Prop. (%)			
	GHB	MOZ	OST	WIK	GHB	MOZ	OST	WIK
Cond.	0.3	0.04	0.3	0.1	1.9	0.3	1.8	1.4
Conf.Data	9.5	3.8	11.5	7.2	29.2	23.5	33.9	29.6
Depe.	1.8	1.3	2.4	1.7	10.6	12.4	16.3	17.1
Docu.	1.7	0.8	1.6	1.5	13.7	7.2	14.0	13.6
Idem.	0.1	0.01	0.3	0.01	1.0	1.6	3.5	0.1
Secu.	0.1	0.5	0.5	0.1	0.9	5.5	2.8	1.1
Serv.	1.4	2.6	1.8	3.0	4.9	23.1	9.3	12.4
Synt.	2.8	1.7	2.3	2.4	16.3	9.2	19.2	17.4
Total	16.6	10.9	18.7	15.2	43.6	47.4	48.6	49.2

議論とまとめ

議論

- 特定されたカテゴリと実務者の認識が異なる
- Serviceの欠陥は最も同意が得られなかったが、
頻度で言えばidempotencyよりも大きい

まとめ

- IaCスクリプトの欠陥を8つに分類した
- 実務者が分類した8つのカテゴリに同意しているかを評価した
- ACIDと呼ばれるツールを構築し、
IaCスクリプトの欠陥カテゴリを自動的に特定した

付録

注釈付きpuppetスクリプト

```
[#An example Puppet script]
[include server]
class sample($service_flag)
{
    [$service_flag = true]

    [if $service_flag] {
        $path_var = '/var/www/html/'
    } else {
        $path_var = '/var/www/html/pages/'
    }

    [service {'apache2':
        ensure => running,
        enable => true,
        path   => $path_var
    ]
}
```

Comment

Refer dependent class 'server'

Variable 'service_flag'

If-else block

Specifying 'apache2' service

Attribute 'enable' of 'apache2' service

具体例

- ログに利用者のパスワードが公開されている
セキュリティ上の欠陥を示す.

```
glance_cache_config{  
  'DEFAULT/auth_url' : value=>$auth_url;  
  'DEFAULT/admin_tenant_name' : value=>$keystone_tenant;  
  'DEFAULT/admin_user' : value=>$keystone_user;  
- 'DEFAULT/admin_password' : value=>$keystone_password;  
+ 'DEFAULT/admin_password' : value=>$keystone_password, secret=>true;  
}
```

- secret => trueを追加することで緩和される

8つの欠陥カテゴリを検出するためのルール

Category	Rule
Conditional	$hasDefect(x.sen) \wedge hasCond(x.sen.dep)$
Configuration Data	$hasDefect(x.sen) \wedge ((hasStorConf(x.sen.dep)$ $\vee hasFileConf(x.sen.dep)$ $\vee hasNetConf(x.sen.dep) \vee$ $hasUserConf(x.sen.dep) \vee$ $hasCachConf(x.sen.dep)) \vee$ $dataChanged(x.diff))$
Dependency	$hasDefect(x.sen) \wedge (hasDepe(x.sen.dep) \vee$ $changedInclude(x.diff))$
Documentation	$hasDefect(x.sen) \wedge (hasDoc(x.sen.dep) \vee$ $changedComment(x.diff))$
Idempotency	$hasDefect(x.sen) \wedge hasIdem(x.sen.dep)$
Security	$hasDefect(x.sen) \wedge hasSecu(x.sen.dep)$
Service	$hasDefect(x.sen) \wedge (hasServ(x.sen.dep) \vee$ $changedService(x.diff))$
Syntax	$hasDefect(x.sen) \wedge hasSynt(x.sen.dep)$

関数とステム処理された文字列パターン

Function	String Pattern
<i>hasDefect()</i>	'error', 'bug', 'fix', 'issu', 'mistake', 'incorrect', 'fault', 'defect', 'flaw'
<i>hasCond()</i>	'logic', 'condit', 'boolean'
<i>hasStorConf()</i>	'sql', 'db', 'databas'
<i>hasFileConf()</i>	'file', 'permiss'
<i>hasNetConf()</i>	'network', 'ip', 'address', 'port', 'tcp', 'dhcp'
<i>hasUserConf()</i>	'user', 'usernam', 'password'
<i>hasCachConf()</i>	'cach'
<i>hasDepe()</i>	'requir', 'depend', 'relat', 'order', 'sync', 'compat', 'ensur', 'inherit'
<i>hasDoc()</i>	'doc', 'comment', 'spec', 'licens', 'copyright', 'notic', 'header', 'readm'
<i>hasIdem()</i>	'idempot'
<i>hasSecu()</i>	'vulner', 'ssl', 'secur', 'authent', 'password', 'secur', 'cve'
<i>hasServ()</i>	'servic', 'server'
<i>hasSynt()</i>	'compil', 'lint', 'warn', 'typo', 'spell', 'indent', 'regex', 'variabl', 'whitespac'

先行研究[62,63]

ECM	Dependent
fix catalog compilation when not configuring endpoint	compilation
fix spurious warning in pipeline check	warning
fix puppet lint 140 characters	lint
typo fix	typo

```
- $network_scheme = hiera('network_scheme')
- $cidr = $settings['contrail_private_cidr']
- $netmask=cidr_to_netmask($cidr)
- $netmask_short=netmask_to_cidr($netmask)
+ $network_scheme = hiera_hash('network_scheme',{})
+ $cidr = pick(get_network_role_property('neutron/mesh','cidr'),
    ↪ get_network_role_property('contrail/vhost0','cidr'))
+ $netmask = pick(get_network_role_property('neutron/mesh','
    ↪ netmask'),get_network_role_property('contrail/vhost0','
    ↪ netmask'))
+ $netmask_short = netmask_to_cidr($netmask)
```

Sanity check

- ごく簡単で基本的な動作の確認を行うこと
- 明らかな不具合がないかの確認のために行う

Table 8: Sanity Checking ACID's Accuracy

Category	Occurr.	Precision	Recall
Conditional	15	0.88	0.93
Configuration Data	99	0.90	0.96
Dependency	59	0.86	0.93
Documentation	32	0.91	0.94
Security	23	0.88	0.91
Service	54	0.85	0.93
Syntax	74	0.93	0.93
No defect	1644	0.99	0.98
Average		0.90	0.94