2013年度

慶應義塾大学入学試験問題

環境情報学部

英語

注意事項

1. 試験開始の合図があるまで、この問題冊子を開かないでください。
2. 受験番号と氏名は、解答用紙の所定の欄に必ず記入してください。
3. 解答用紙の「注意事項」を必ず読んでください。
4. この問題冊子は、表紙を含めて16ページあります（問題は２ページから13ページ）。試験開始の合図とともに、全てのページが揃っているか確認してください。ページの欠落・重複があった場合には、直ちに監督者に申し出てください。
5. 問題冊子は、試験終了後に必ず持ち帰ってください。

I. 次の文章に関して、空所補充問題と読解問題の二つがあります。まず、[1]から[20]の空欄を埋めるのに、文脈的に最も適切な語を１から３の中から選び、その番号を解答欄（1）から（20）にマークしなさい。次に、内容に関する[21]から[30]の設問には、１から４の選択肢が付されています。そのうち、文章の内容からみて最も適切なものを選び、その番号を解答欄（21）から（30）にマークしなさい。

1 Google and Facebook are leading the development of "personalization"—the process through which the type of information offered is adjusted to users' demands. The way that personalization shapes identity is still becoming clear—especially because most of us spend more time consuming broadcast media than personalized content streams on the Internet. But by looking at how those two major players on the web conceive of identity, it's becoming possible to predict what these changes might look like. Personalization requires a theory of what makes a person;—of what bits of data are most important to ascertain who someone is, and the two web giants have quite different ways of approaching the problem.

2 Google's personalization system relies heavily on web history and what you click on to [1](1. infer 2. defer 3. prefer) what you like and dislike. These clicks often happen in an entirely private context: The assumption is that searches for "intestinal gas" and celebrity gossip are between you and your browser. You might behave differently if you thought other people were going to see your searches. But it's that behavior that determines what content you see in Google News, what ads Google displays—that determines, in other words, Google's theory of you.

3 The basis for Facebook's personalization is entirely different. [2](1. Unless 2. While 3. Since) Facebook undoubtedly tracks clicks, its primary way of thinking about your identity is to look at what you share and with whom you interact. That's a whole different kettle of data from Google's: There are plenty of odd and embarrassing things we click on that we'd be [3](1. ready 2. reluctant 3. flattered) to share with all of our friends in a status update. And the reverse is true, too. I'll admit to sometimes sharing links I've barely read—the long investigative piece on the reconstruction of Haiti, the bold political headline—because I like the way it makes me [4](1. turn 2. stick 3. look) to others. The Google self and the Facebook self, in other words, are radically different people. There's a big difference between "you are what you click" and "you are what you share."

4 Both ways of thinking have their benefits and drawbacks. With Google's click-based self, the gay teenager who hasn't [5](1. run up 2. come out 3. looked up) to his parents can still get a personalized Google News feed with pieces from the broader gay community that affirm that

he's not alone. But at the same time, a self built on clicks will tend to draw us even more toward the items we're [6](1. predisposed 2. entitled 3. embarrassed) to look at already. Your perusal of an article on a celebrity gossip site is [7](1. filed 2. thrown 3. given) away and the next time you're looking at the news, you are more likely to find salacious details about an actor's infidelity on the screen.

5 Facebook's share-based self is more aspirational: Facebook takes you more at your word, presenting you as you'd like to be seen by others. Your Facebook self is more of a performance, less of a metaphorical black box, and ultimately it may be more prosocial than the bundle of signals Google tracks. But the Facebook approach has its downsides as well—to the extent that Facebook draws on the more public self, it necessarily has [8](1. no rooms 2. less room 3. a tiny room) for private interests and concerns. The same closeted gay teenager's information environment on Facebook remains [9](1. inhuman 2. incomplete 3. indifferent).

6 Both are pretty poor representations of who we are, in part because there is no one set of data that substantively describes who we are. "Information about our property, our professions, our purchases, our finances, and our medical history does not tell the whole story," writes privacy expert Daniel Solove. "We are more than the bits of data we [10](1. put 2. take 3. give) off as we go about our lives."

7 Robotics engineers frequently run [11](1. down 2. into 3. over) problems when attempting to create realistic reflections of life. There can actually be an uncomfortable sense of disconnect that one feels when looking at imperfectly animated humans or plastic-looking, human-faced robots—the so-called "uncanny valley." The problem is that the data do not necessarily represent reality. We can say that Facebook and Google are in fact experiencing similar problems in their efforts to capture individual personalities. With Facebook, users are actually creating a mask to show the world, but at the moment it is an imperfect and unconvincing one. With the Google paradigm, the personality sketch created of users is also flawed, albeit differently. This is due to misinterpreting aspects of a given customer's online behavior as being indicative of his or her identity. It could be said that rather than a good representation of self, right now the Internet can only provide a shoddy doppelganger.*

8 Mark Zuckerberg, the founder of Facebook, claims that we have "one identity", a claim that has become the foundation of the Facebook personalization model. Psychologists, however, warn us against this misconception. We tend to explain people's behavior in terms of their unchanging inner traits rather than the situations in which they're placed. Even in situations

where the context clearly plays a major role, we find it hard to separate [12](1. how 2. when 3. where) someone behaves from who she is.

9 Our personalities are fluid. Someone who's gregarious and outgoing when happy may be introverted when [13](1. stressed 2. excited 3. joyful). We may think that our personalities are set, and our behaviors are predictable, but this is not necessarily the case. Even people who think themselves to be gentle and mild-mannered may act brutally under certain conditions. This was demonstrated by psychologist Stanley Milgram in his oft-cited experiment at Yale in the 1960's where he got decent ordinary people to apparently electrocute other subjects upon the instruction of a researcher in a white lab coat, a symbol of authority.

10 There is a reason that we act this way: The personality traits that serve us well when we're at dinner with our family might get [14](1. on 2. along 3. in) the way when we're in a dispute with a passenger on the train or trying to finish a report at work. The [15](1. platitude 2. plasticity 3. profusion) of the self allows for social situations that would be impossible or intolerable if we always behaved exactly the same way. Advertisers have understood this phenomenon for a long time. It's no accident that you don't hear many beer ads as you're driving to work in the morning. People have different needs and aspirations at eight a.m. than they do at eight p.m. [16](1. By contrast 2. On the contrary 3. By the same token), billboards in the night-life district promote different products than billboards in the residential neighborhoods the same partiers go home to.

11 The one-identity problem illustrates one of the dangers of [17](1. running 2. turning 3. getting) over your most personal details to companies who have a skewed view of what identity is. And when we're aware that everything we do enters a permanent, pervasive online record, another problem emerges: The knowledge that what we do affects what we see and how companies see us can create a chilling effect. Genetic privacy expert Mark Rothstein describes how lax regulations around genetic data can actually reduce the number of people willing to be tested for certain diseases: If you might be discriminated against or denied insurance for having a gene linked to Parkinson's disease, it's not unreasonable just to skip the test and the troubling knowledge that might result.

12 However, the one-identity problem isn't a fundamental flaw. It's more of a [18](1. bug 2. bit 3. virus): Because Facebook thinks you have one identity and you don't, it will do a worse job of personalizing your information environment. As a friend of mine told me, "We're so far away from the nuances of what it means to be human, as reflected in the nuances of the technology." People don't have a single, tidy identity in all contexts, and every [19](1.

increasing 2. dropping 3. passing) fancy is not demonstrative of some core desire or interest. In theory, however, the one-identity, context-blind problem isn't impossible to fix. Personalization will undoubtedly get better at sensing context, and, in fact, people in the field are working on it. They might even be able to better balance long-term and short-term interests. But when they do—when they are able to accurately [20](1. dial 2. gauge 3. switch) the workings of your psyche—things will get even more uncomfortable.

Note:

* : doppelganger: someone who looks exactly like you, but is not you

–Adapted from Eli Pariser (2011). *The Filter Bubble.* Penguin Press.

[21] Which of the following is closest to the description of Google's personalization system mentioned in the 2nd paragraph?

1. Providing users with information by filtering it through their self-reported data on likes and dislikes.
2. Letting users adjust their clicking history in case their families, friends and other users gain access to it.
3. Keeping your online identity just between you and Google, beyond the reach of other users.
4. Adjusting the type of information they provide based on each user's browsing record on the web.

[22] In the 4th paragraph, the author mentions the case of a gay teenager in order to illustrate

1. how seriously Google is committed to basic human rights and liberalism.
2. what a narrow range of personal interests can be maintained by using Google.
3. how you can get information you want without revealing yourself to the public.
4. how your information environment can be jeopardized by Google's click-based self.

[23] Which of the following would be closest in meaning to the phrase "more of a performance, less of a metaphorical black box" as mentioned in the 5th paragraph?

1. Facebook is concerned with what you show, rather than what you click.
2. You are more of what you do than what you feel.
3. Treat others as you would like to be treated.
4. You hide what people want to see rather than what you want to show.

[24] Which of the following is claimed by the 7th paragraph?

1. Facebook encourages users to put up a façade to hide their true identities on the Internet.
2. Neither robotics engineering nor social networking has solved the problem of the "uncanny valley."
3. With Google's personality profile method, you show the world an imperfect version of yourself.
4. Internet services can learn from other technological fields to overcome the problems of online identity.

[25] In order to avoid the misconception discussed in the 8th paragraph, it would be necessary to

1. take into consideration people's psychological factors as well as behavioral patterns.
2. regard people's personality based on various behaviors in different situations.
3. distinguish behaviors visible from the outside from feelings buried inside the heart.
4. realize there is no consistency to be found when you observe someone's behaviors.

[26] The purpose of the experiment conducted by Stanley Milgram as mentioned in the 9th paragraph was to show that

1. humans hide a natural inborn drive to harm others though it is rarely put into action.
2. people's willingness to harm others is affected by what type of context they are in.
3. people's cruelty is typically the result of overbearing authority figures.
4. people's personality traits have a strong effect on how they act in a given situation.

[27] Which of the following is another example of a "chilling effect" as it is used in the 11th paragraph?

1. If regulations are not strict enough, personal records of diseases may leak out to the public causing distrust in authority.
2. When a large number of people skip medical tests, there will be an increased chance of infectious diseases going rampant.
3. Once people know you have a gene linked to a specific disease, there will be no way to avoid their discrimination against you.
4. If you work in a hospital with an incompetent doctor, you do not report him because you are afraid you will be fired.

[28] The statement "people in the field are working on it" in the 12th paragraph means that they are trying to

1. strike a balance between leaving users unknown to each other and requiring them to maintain a single identity.
2. incorporate Facebook's sharing functions into Google search functions.
3. better personalize search results by making personalization more context-sensitive.
4. help Facebook improve the way they personalize the type of information users access on the Internet.

[29] Which of the following phrases from the article best corresponds to the phrase "a single, tidy identity" as used in the 12th paragraph?

1. unchanging inner traits
2. a mask
3. the public self
4. a shoddy doppelganger

[30] Which of the following can be inferred from this article?

1. Personalization on the web makes you look multi-dimensional, although in reality your full personality is hard to pinpoint.
2. Invisible filtering of web content via personalization may threaten to limit your exposure to different thoughts and ideas.
3. As a Facebook user, you might feel like sharing any kind of news with your friends, whether it is favorable or unfavorable to your self-image.
4. Two people in different regions with different interests will receive identical Google results when typing in the same search phrase.

II. 次の文章に関して、空欄補充問題と読解問題の二つがあります。まず、[31]から[50]の空所を埋めるのに、文脈的に最も適切な語を1から3の中から選び、その番号を解答欄（31）から（50）にマークしなさい。次に、内容に関する[51]から[60]の設問には、1から4の選択肢が付されています。そのうち、文章の内容からみて最も適切なものを選び、その番号を解答欄（51）から（60）にマークしなさい。

1 Medical devices are a wonder of the modern age. "Smart" infusion pumps deliver drugs perfectly dosed for individual patients. Easy-to-use AEDs (Automatic Electronic Defibrillators) can bring heart-attack victims back from the brink of death. Pacemakers and artificial hearts keep people alive by ensuring that blood is pumped smoothly around their bodies.

2 However, as these devices have become more [31](1. capable 2. collectable 3. compatible), they have also become more complex. More than half of the medical devices sold in America (the world's largest health-care market) rely on software, and often lots of it. The software in a pacemaker may require over 80,000 lines of code, a drug-infusion pump 170,000 lines, and an MRI (Magnetic Resonance Imaging) scanner more than 7 million lines.

3 This growing reliance on software causes problems that are [32](1. familiar 2. famous 3. simple) to anyone who has ever used a computer: bugs, crashes, and vulnerability to digital attacks. One in three of all software-based medical devices sold in America between 1999 and 2005 were recalled for software failure. Dr. Kevin Fu, a computer science professor at the University of Massachusetts, calculates that such recalls have affected over 1.5 million individual devices since 2002. In 2012, researchers at McAfee, a computer-security firm, said they had found a way to get an implanted insulin pump to deliver 45 days' worth of insulin in one go. And in 2008, Dr. Fu and his colleagues published a paper detailing the remote, wireless reprogramming of an implantable defibrillator.

4 When software in a medical device malfunctions, the consequences can be far more serious than just having to reboot your PC. During the 1980s, a bug in the software of Therac-25 radiotherapy machines caused massive overdoses of radiation to be [33](1. delivered 2. dragged 3. driven) to several patients, killing at least five. America's Food and Drug Administration (FDA) has linked problems with drug-infusion pumps to nearly 20,000 serious injuries and over 700 deaths between 2005 and 2009. Software errors were the most frequently cited problem.

5 [34](1. As regards 2. Despite 3. In addition to) accidental malfunctions, wireless and networked medical devices are also vulnerable to attacks by malicious hackers. Dr. Fu and his colleagues showed how an implantable cardioverter defibrillator could be remotely reprogrammed either to withhold therapy when it is needed or, [35](1. as if 2. even worse 3. if

so), to deliver unnecessary shocks. Dr. Fu says that when it comes to testing their software, device manufacturers lack the safety culture found in other high-risk industries such as aviation, and are failing to keep up with the latest advances in software engineering. Insup Lee, professor of computer science at the University of Pennsylvania, agrees: “Many manufacturers do not have the expertise or the willingness to utilize new tools being developed in computer science,” he says.

6 Just how bad it is, though, no one knows for sure. The software used in the vast majority of medical devices is closed and [36](1. primary 2. probationary 3. proprietary). This prevents rivals from copying each other’s code or checking for patent infringements. It also makes it harder to [37](1. expose 2. produce 3. protect) flaws. The FDA, which could demand to see the source code for every device it approves, does not routinely do so, but instead leaves it to manufacturers to validate their own software.

7 Frustrated by the lack of co-operation from manufacturers, some academics now want to reinvent the medical-device industry from the [38](1. belly 2. seat 3. ground) up, using open-source techniques. In open-source systems, the source code is freely shared and can be viewed and modified by anyone who wants to see how it works or build an improved version of it. Exposing a design to many hands and [39](1. ears 2. eyes 3. feet), the theory goes, results in safer products.

8 The Generic Infusion Pump project, a joint effort between the University of Pennsylvania and the FDA, is taking these [40](1. meddlesome 2. quarrelsome 3. troublesome) devices back to basics. The researchers began not by building a device or writing code but by imagining everything that could possibly go wrong with a drug-infusion pump.

9 Mathematical models of existing and new pump designs were tested against the possible risks, and the best-performing models were used to [41](1. encase 2. generate 3. invigorate) code, which was installed on a second-hand infusion pump bought online for $20.

10 Equally ambitious is the Open Source Medical Device initiative at the University of Wisconsin-Madison. Two medical physicists, Rock Mackie and Surendra Prajapati, are designing a machine to combine radiotherapy with high resolution CT (computed tomography) and PET (positron-emission tomography) scanning. Their [42](1. aim 2. sight 3. stock) is to supply, at zero cost, everything necessary to build the device from scratch, including hardware specifications, source code, assembly instructions, suggested parts—and even recommendations [43](1. by 2. on 3. over) where to buy them and how much to pay. The machine should cost

about a quarter as much as a commercial scanner, making it attractive in the developing world, says Dr. Prajapati. "Existing devices are expensive both to buy and maintain," he says, whereas the open-source model is more sustainable. "If you can build it yourself, you can fix it yourself when something breaks."

11 Open-source devices are also to be found [44](1. generously 2. laterally 3. literally) at the cutting edge of medical science. An open-source surgical robot called Raven, designed at the University of Washington in Seattle, provides an affordable platform for researchers around the world to experiment with new techniques and technologies for robotic surgery.

12 All these open-source systems address very different problems in medical science, but they have one thing in common: all are currently prohibited for use on live human patients. To be used in a clinical setting, open-source devices must first [45](1. undergo 2. underlie 3. understand) the same expensive and lengthy FDA approval processes as any other medical device. FDA regulations do not yet require software to be analyzed for bugs, but they do insist on a rigorous paper trail detailing its development. This is not always a good fit with the collaborative and often informal nature of open-source coding.

13 The high cost of navigating the regulatory [46](1. regime 2. regiment 3. reproduction) has forced some not-for-profit, open-source projects to alter their business models. "In the 1990s we developed an excellent radiation-therapy treatment-planning system and tried to give it away to other clinics," says Dr. Mackie. "But when we were told by the FDA that we should get our software approved, the hospital wasn't willing to fund it." He formed a spin-off firm specifically to get FDA approval. It took four years and cost millions of dollars. The software was subsequently sold as a traditional, closed-source product.

14 Others are skirting America's regulatory system altogether. The Raven surgical robot is intended for research use on animals, while the Open Source Medical Device scanner will be large enough only to [47](1. accommodate 2. eradicate 3. relocate) rats and rabbits. However, says Dr. Mackie, there is nothing to stop anyone taking the design and putting it through a regulatory process in another country. "It may even happen that the device will be used on humans in parts of the world where strict regulation does not exist," he says. "We would hope that if it is used in such a way, it will be well-enough-designed not to hurt anybody."

15 The FDA is gradually embracing openness. The Medical Device Plug-and-Play (MD PnP) Program, a 10-million-dollar initiative funded by the National Institutes of Health with the support of the FDA, is working to set open standards for interconnecting devices from different

manufacturers. This would mean that, say, a blood-pressure cuff could instruct a drug pump to stop delivering medication if it sensed that a patient was suffering an [48](1. admitted 2. advantageous 3. adverse) reaction.

16 [49](1. Eventually 2. Inádvertently 3. Ironically) medical devices might evolve into collections of specialized (and possibly proprietary) accessories, with the primary computing and safety features managed by an open-source hub.

17 In the meantime, there are moves afoot to improve the overall security and reliability of software in medical devices. America's National Institute of Standards and Technology has just recommended that a single agency, probably the FDA, should be responsible for approving and [50](1. racking 2. stacking 3. tracking) cybersecurity in medical devices, and the FDA is re-evaluating its ability to cope with the growing use of software.

18 Such changes cannot happen too soon. "When a plane falls out of the sky, people notice," says Dr. Fu. "But when one or two people are hurt by a medical device, or even if hundreds are hurt in different parts of the country, nobody notices." With ever more complex devices, opening up the hidden heart of medical technology makes a great deal of sense.

—Based on "When code can cure or kill". (2012, June 2). *The Economist.*

[51] In the 5th paragraph, what does "safety culture" refer to?

1. National training for dangerous situations.
2. A culture in which medical safety laws are especially strong.
3. Countries with low levels of crime, like Denmark and Canada.
4. An organizational situation in which safety is of first importance.

[52] According to the 8th paragraph, the Generic Infusion Pump project developed their product by first

1. considering potential problems.
2. studying all of the competing products.
3. surveying medical professionals about their needs.
4. creating open-source equivalents from proprietary rivals.

[53] What does the quotation in the last two sentences of the 14th paragraph indicate?

1. The belief of the speaker that the regulations for open-source medical equipment should be less strict.
2. An admission that if not used correctly, the technology could be dangerous.
3. The possibility that foreign countries are more advanced in the design of open-source devices.
4. Only through internationalization can open-source technologies become readily available.

[54] Which of the following is ***NOT*** a problem with using open source software for medical devices?

1. It is expensive to pass government regulations.
2. Medical companies have not accepted open-source methods.
3. The informality of open-source programing makes documentation more difficult.
4. Academics disapprove of open-source software because of buggy code and hackers.

[55] What ultimately happened to Dr. Mackie's radiation-therapy treatment-planning system?

1. It could not successfully compete in the marketplace.
2. It was released as closed-source software.
3. It failed due to poor open-source coding.
4. It was too expensive to build.

[56] In the last paragraph, Dr. Fu's comment, "When a plane falls out of the sky, people notice," can be taken to mean that

1. the dramatic nature of airplane failures bring more attention and faster change than medical software failures.
2. people are more likely to notice very dramatic events, so only when someone dies from medical software, will change occur.
3. the medical industry has nothing to learn from the aviation industry.
4. aviation disasters are more important than medical disasters.

[57] Which of the following is an implication of the article?

1. Open-source medical software is impractical because of the lack of organization of open-source programmers.
2. The FDA approval process has ruined any chance of future success for open-source in the field of medicine.
3. Open-source software has the potential to make medical devices safer.
4. A closed-source system is necessary to ensure patient safety.

[58] According to the article, what is currently true about ***ALL*** open-source medical devices?

1. They have been approved by the FDA.
2. They are restricted to non-human testing.
3. They are more costly than similar proprietary versions.
4. They are considerably more popular in the developing world.

[59] Which of the following is ***NOT*** a theme explored in this article?

1. Doctor liability
2. Medical law
3. Patient safety
4. Wireless security

[60] Which of the following is an argument made by the article with reference to the widespread use of open-source software in the medical industry?

1. The use of open software prevents cyber-security breaches.
2. The wider use of open-source would lessen the influence of closed-source companies.
3. Open-source allows for more error checking, which could prevent medical emergencies.
4. Closed-source software has superior design and safety to that of its open-source counterparts.

（下書き用）

（下書き用）

（下書き用）