翻訳トライアル実践講座　第 2 回

＜問題 1＞　全文を訳して提出してください。

11 Hard Truths About HTML5

HTML5 heralds some nifty new features and the potential for sparking a Web programming paradigm shift, and as everyone who has read the tech press knows, there is nothing like HTML5 for fixing the Internet. Sprinkle some HTML5 into your code, and your websites will be faster and fancier -- it'll make your teeth white, too. But the reality of what HTML5 can do for those seeking native-app performance on the Web falls short of the hype.

After several years of enjoying HTML5's sophisticated new tags and APIs, the time is ripe to admit that there are serious limitations with the model. Not only are there reasons to grouse about HTML5 failing to fulfill our Web nirvana dreams, there are even reasons to steer away from HTML5 in some cases.

The truth is, despite its powerful capabilities, HTML5 isn't the solution for every problem. Its additional features are compelling and will help make Web apps formidable competitors for native apps, but security issues, limitations of local data storage, synchonization challenges, and politics should have us all scaling back our expectations for the spec. After all, every technology has its limitations.

What follows is a list of 11 hard truths Web developers must accept in making the most of HTML5.

HTML5 hard truth No. 1: Security is a nightmare

The fundamental problem with client-side computing is that the user ultimately has control over the code running on the machine. In the case of Web apps, when your browser comes with a great debugging tool, this control is easier than ever to abuse.

With a JavaScript debugger like Firebug, anyone who is curious about what Facebook, Google, or any other website is doing can just start inserting breakpoints and watch the code. This is great for debugging and learning how websites operate, but it's a nightmare for security.

Suppose there's a variable that holds a value you'd like to change; well, Firebug or any of the other browser debuggers is happy to help you tweak the data to be anything you desire. Do you want to trick your friends into thinking you're in another geographic location? It's easy to edit the variables that hold latitude and longitude to place your browser anywhere in the world. All the neat features of your Web app can be modified, and the browser environment makes it easier than it would be normally with native code.

There are limits to the security problems that can be incurred. Some JavaScript tools such as Google Web Toolkit are nearly as complicated as standard compilers. Their output can be fairly inscrutible. Luckily tools like the JavaScript Deminifier can help.

The danger depends, of course, on the nature of the application. It's one thing when someone edits their latitude and longitude to play tricks on their friends by checking into a website while pretending to be halfway around the world. The trouble begins when someone qualifies for all of the rights, privileges, and free beers accorded by being crowned the mayor of some location. When money gets involved, the games can only get worse. All of this means that client-based HTML5 apps can't be trusted with serious data collection, and it's better for everyone to be aware of their capabilities.

＜問題2＞　全文を訳して提出してください。

A Tempting Target for Cybercrime

Cybercrime's effects are felt throughout the Internet, and cloud computing offers a tempting target for many reasons. As previously discussed, startups typically have limited resources; to alleviate the expense of developing a secure computing environment, they might turn to cloud computing to deflect cybersecurity concerns. To support their clouds' integrity, large providers typically require that users place 100 percent of their data within the providers cloud. Providers such as Google and Amazon have the existing infrastructure to deflect and survive a cyberattack, but not every cloud has such capability. Clouds can comprise multiple entities, and in such a configuration, no cloud can be more secure than its weakest link. If a cybereriminal can identify the provider whose vulnerabilities are the easiest to exploit, then this entity becomes a highly visibile target. The lack of security associated with this single entity threatens the entire cloud in which it resides. If not all cloud providers supply adequate security measures, then these clouds will become high-priority targets for cybercriminals. By their architecture's inherent nature, clouds offer the opportunity for simultaneous attacks to numerous sites, and without proper security, hundreds of sites could be comprised through a single malicious activity.

Security and Technology

To advance cloud computing, the community must take proactive measures to ensure security. A movement exists to adopt universal standards (for example, open source) to ensure interoperability among service providers. Incluced in this effort are attempts to develop security standards to ensure data's CIA. Even though the community at large is aware of the need for security and is attempting to initiate robust measures, a realm of security concerns transcends these efforts. As with most technological advances, regulators are typically in a "catch-up" mode to identify policy, governance, and law. Cloud computing presents an extension of problems heretofore experienced with the internet.

以上