第 14 回 IT ソフトウェア翻訳士認定試験

＜1次試験＞　4月15日（日）10：00～15：00

問題 1・2 の両方について解答のこと。選択ではありません。

＜問題 1＞　全文を訳して提出してください（固有名詞、社名は変更してあります)。

Consumerization of IT: The Social Networking Problem

Social tools debuting at the enterprise level face many pitfalls that can derail even the best laid plans. A few IT leaders speaking at the Consumerization of IT in the Enterprise Conference and Expo in San Francisco last week revealed some of these social danger zones

Look Who's Talking

Once people start using social tools, you're still not out of the woods.

IT leaders warn that some older workers might view the new social tools with a skeptical eye. Social networking in the enterprise has been billed as a way to recruit and retain the younger generation. Older workers may feel social networking keeps them out of the conversation and undermines their careers.

Though this is a common fear, Thomas denies that social networking has generational gap consequences. "That's absolutely balderdash," he says.

Another problem is workers who will try to take over the conversation.

Enterprise social networking experts need to be wary of these potential pitfalls, but this doesn't mean that they should stop people from making critical comments about the company. At ABES, Hikita worried that

management would take a tough stance against an employee who posted critical comments.

As it happened, the critical comment received 88 replies. The issue quickly rose up the command chain to the vice president of human resources. Within four weeks, ABES responded positively to the issue. "It's the value of working out loud," Hikita says.

The flip side, of course, is the handful of employees who constantly complain, vent and bicker, usually on micro-blogging platforms. IT leaders advice: Let them do it. If you staunch their voice, then you destroy trust.

How do you avoid social networking problems? The trick is knowing how people interact, not necessarily the intricacies of the technology. For instance, social networking is self-regulating and self-outing so that peer pressure will often correct behavior without corporate intervention.

"You have a social reputation," Tanaka says. "When you have more eyes, there will be less complaining because [nobody] wants to appear as a whiner."

＜問題 2＞　下線部分のみを訳して提出してください（固有名詞、社名は変更してあります)。
訳に下線はつけなくて結構です。

Hackers Target IPv6

If your IPv6 strategy is to delay implementation as long as you can, you still must address IPv6 security concerns right now.

If you plan to deploy IPv6 in a dual-stack configuration with IPv4, you're still not off the hook when it comes to security. And if you think you can simply turn off IPv6, that's not going to fly either.

The biggest looming security threat lies in the fact that enterprise networks already have tons of IPv6 enabled devices, including every device running Windows Vista or Windows 7, Mac OS/X, all Linux devices and BSD.

And unlike its predecessor, DHCP for IPv4, IPv6 doesn't require manual configuration. This stateless auto-configuration feature means that "IPv6-enabled devices are just waiting for a single router advertisement to identify themselves on the network," says Jun Abe, Distinguished Systems Engineer at Cisco and co-author of the book "IPv6 Security."

He cautions that "IPv4-only routers and switches don't recognize or respond to IPv6 device announcements, but a rogue IPv6 router could send and interpret this traffic."

Stateless auto-configuration allows any IPv6-enabled device to communicate with other IPv6 network devices and services on the same LAN. To do this, the device advertises its presence and is located via the IPv6 Neighbor Discovery Protocol (NDP).

But left unmanaged, NDP may be a bit too neighborly, possibly exposing devices to attackers anxious to glean information about what's going on inside the network, or even allowing the device itself to be taken over and turned into a "zombie."

Abe says the threat is real. "We have observed worldwide that bots are increasing their use of IPv6 as a covert channel to communicate with their botmaster." Among its many disguises, IPv6-enabled malware can take the form of a malicious payload encapsulated in one or more IPv4 messages. Without IPv6-specific security measures such as deep packet inspection, this type of payload may pass through the IPv4 perimeter and DMZ defenses undetected.

SEND (SEcure Neighbor Discovery) is the IETF solution to Layer-2 IPv6 threats such as rogue RA and NDP spoofing, which equate to IPv4 threats named rogue DHCP and ARP spoofing. Some OS vendors support SEND, while others, notably Microsoft and Apple, do not.

Cisco and the IETF are in the process of implementing the same security mechanisms for IPv6 that are currently used to protect IPv4 against these threats.

The IETF has a working group SAVI (Source Address Validation) and Cisco is implementing a three-phase plan to upgrade its IOS that started in 2010 and will be fully implemented by sometime in 2012, depending upon the switch type.

Abe notes that some of the more common IPv6 security risks are accidentally created by an improperly configured end-user device on the network, and that proper configuration and IPv6 security measures would eliminate many of these risks.

"The answer to this type of problem is to deploy native IPv6, and to protect IPv6 traffic at the same level and against the same kinds of threats you already defend in IPv4," Abe explains.

以上