第 6 回ソフトウェア翻訳士認定試験

＜一次試験＞　3 月 5（日）10：00～15：00

問題 1～3 のすべてについて解答のこと。選択ではありません。

＜問題 1＞　下線部を訳してください。

Small and midsize businesses (SMBs) face a world of threats that can impact productivity, compromise customer privacy, and even put the survival of the business at risk. Years ago, building backup systems and maintaining a firewall was protection enough. But threats continue to evolve, increasing in sophistication and frequency. If you're not keeping up, your outdated hardware and software could leave your company vulnerable. How?

10 WAYS TO PROTECT YOUR BUSINESS

So how do you protect your business in a cost-effective, sustainable way? Here are some tips to get you started.

1.Develop a backup and recovery strategy.

Many SMBs have not determined the value of their data. Most who have are surprised at the high value --- and the high cost of recovery. A winning backup and recovery strategy is tested regularly and includes full and incremental backups. Store backups offsite, in case disaster strikes at the office. Also: schedule automated backups to occur during non-peak times so they won't disrupt work.

2.Embrace remote server management.

Cut operating costs by managing servers from one location. Solve problems before they happen, even with servers far away. Make sure your solutions support this capability if you have servers in multiple locations.

3.Enable remote client management.

Establish a solution for managing systems and data centrally, including software updates and data backup and restore. The solution should include remote-control software that enables support staff to access employee PCs.

4.Protect against hacker attacks.

When hackers poke around on a network, they do so in predictable patterns. An intrusion detection system can notify you of this activity, allowing you to stop the attack and figure out how to prevent similar attacks in the future.

5.Prtotect against natural disasters.

A disaster can't be prevented, but unnecessary harm to your business as a result of disasters can be minimized. Formulate --- then communicate --- a disaster plan that assumes multiple scenarios. For example, what should the company do in the event of a 12-hour power failure? A 72-hour system outage? The total destruction of all servers and storage? Such a plan would include how staff would communicate with each other; how remote backups would be restored; where employees would work; and other actions needed to minimize damage.

6.Use antivirus wisely.

It's important to deploy antivirus software on all systems and enforce an antivirus policy that ensures automated signature updates. It's common for some employees to turn off antivirus protection and/or automated updates. These systems become the doorways through which malware enters your company.

7. Set up virtual private network (VPN) capability.

One of the most reliable ways to establish a secure connection between mobile workers and the office is through a VPN. VPNs enable access behind the firewall through any public Internet connection with the use of authentication and encryption technology. To establish VPN capability, you need a VPN router on your central network, and VPN client software on employee systems.

8.Deploy a firewall.

A firewall --- hardware or software --- is an indispensable component of your business protection program. Companies with DSL modems can use the DSL router as a firewall. Most companies, however, will want to deploy a firewall server or an integrated firewall, VPN and cache server to save time and money.

9.Use strong passwords.

The chain of business protection is only as strong as its weakest link. Often, that weakest link is bad password management. That's why it's important to enforce a good password policy (see "Tips for Creating Good Passwords").

10.Use the latest WLAN standard.

There are big differences between older and newer wireless LAN standards. Make sure your network and PCs support the 802.11g standard for maximum performance and compatibility.

＜問題2＞　下線部を訳してください。

Visionary Signaling

IP Telephony Solution (IPTS) customers have been successfully deploying global SS7/C7 solutions since 1997. Now IPTS' excellence continues with the IPTS MSS (Multipoint Signaling Server), a highly scalable a flexible solution. IPTS MSS can be connected in both associated and quasi-associated modes, operating directly connected to signaling end points or signaling transfer points. The SS7/C7 MSS can grow hand in hand with IPTS' customers, from the most basic networking configurations to highly robust networks.

IPTS Delivers for Carriers

IPTS' next generation network signaling product, the SS7/C7 IPTS MSS delivers the attributes demanded by today's carrier market; redundancy, high reliability and capacity. The distributed SS7 software architecture is the corner stone for IPTS' Multipoint Signaling Server's immense reliability and availability. The possibility of a single point of failure is eliminated with the IPTS' MSS configurations that can be designed with several clusters that are configured in a geographically dispersed manner. Thereby providing reliability comparable to fault-tolerant "5-nines" systems.

System or network failures can be handled with no switchover delay because each unit, when necessary, can control and load balance the entire configuration.

The IPTS' MSS caters to the carrier's needs with a few crucial features. MSS is available on a Compact PCI bus (cPCI), NEBS compliant model with hot-swappable T/E cards. Every cPCI I/O card is hot swappable and can be replaced while the system is running, without disrupting operations. SS7 Link load sharing is possible across platform units. Point codes can be conserved by deploying multiple units in a cluster configuration to act as a single point code. IPTS MSS supports IN (Intelligent Network) services such as Local Number Portability (LNP) and other CLASS features like Calling Name and Automatic Call Back through Transaction Capabilities Application Part (TCAP) protocol.

＜問題 3＞　下線部を訳してください。

Security in IE7

The security history of Internet Explorer is not a happy one. Microsoft's combination of naive and sloppy programming has led to an infamous string of vulnerabilities and patches over many years. But with the upcoming Internet Explorer 7, Microsoft may finally be biting all the bullets necessary to do browser security right.

To use IE7, currently in a limited beta test only for MSDN subscribers, you'll need to be running Microsoft Windows XP SP2 or Windows Vista. The most important security precautions are supported only on Vista.

We'll stop short of taking Microsoft at its word, but the company has said that security supersedes compatibility as the top priority in IE7, and several key modifications seem to bear this out. The most significant is Protected Mode, which runs the browser in a special limited-privilege context, regardless of the privileges of the user running the system.

In reports on malware you'll often see a statement that the attack code will run in the context of the user. This means that the attack program essentially becomes part of the compromised program the user was running and therefore runs with the privileges the user has. If the user has limited privileges, so does the attack code. If the user is an administrator, the system is utterly compromised.

Protected Mode, available only in Windows Vista, means that even if the browser is compromised, the system is largely protected. IE can't install software without explicit user consent, and it can't write files outside of the Temporary Internet Files directory.

Protected Mode is not fully implemented in Beta1, and Microsoft hasn't revealed the interface for situations where elevated privileges are needed. IE could ask the user for credentials when privileged operations are necessary, though this may be no more secure than with IE6. Both are equally vulnerable to social engineering and credulous users, for which there's no technological solution.

Security is also improved with UIPI(User Interface Privilege Isolation), another mechanism for combating unauthorized permissions escalation, also available only with Vista. UIPI prevents "shatter attacks" in which window messages from processes with fewer permissions are sent to higher-level windows, tricking them into performing privileged activities. New APIs are available for third-party programs, such as the Adobe Acrobat ActiveX control, to perform such activities with the user's explicit consent.

Microsoft is adding an antiphishing filter to IE7, composed mainly of whitelists of known safe sites and blacklists of known phishing sites. The phishing blacklist's performance needs sound daunting, considering the potential number of IE7 users, but Microsoft says that IE7 will look up unknown sites in real time rather than periodically downloading updates to a list, and that this will result in less traffic. The whitelist will be downloaded periodically.

To allay concerns that Microsoft could track sites users are visiting, the company has tried to construct the service to minimize the possibility of abuse and has updated its privacy policy (www.microsoft.com/windowsvista/privacy/ieprivacy_pr7.mspx). For instance, IE7 won't send the query-string portion of a URL(beyond the "?") to the lookup, and it won't send cookies or form submissions; only the address portions of the URL will be sent. If even this makes you uncomfortable, you can disable the feature.

Finally, IE7 will require secure Web sites to use newer cryptographic techniques, specifically SSLv3 (Secure Sockets Layer Version3) and TLS (Transport Layer Security), blocking older ones.

Clearly, Microsoft doesn't get the benefit of the doubt. It is good to see the company aiming high and putting its priorities where they need to be, but we'll reserve judgment until the bad guys have some time to beat on IE7.

以上