Global Information Assurance Certification Paper

Challenges to Effective Management of Observance of Security Policy for client PCs

Mar 15,2004

Masato Kagotani
kagotani@nri-secure.co.jp

Table of Contents

Index of Figures

Index of Tables

1 Abstract

Management of security of client PC is more difficult than that of s erver. [1][2] But the security management of c lient PC is becoming a big subject on the security of co mpanies or individuals in recent years. Therefore in this paper I have researched the trends of security of client PCs and I would like to present one solution to manage security of client PCs and security policy.

The system introduced in this paper has client PCs security diagnosis function, security management function of client PCs and function of managing security policy. These functions had implemented the function of effective management of observance of security policy of client PCs that has been insufficient.

I was one of the development member s of that system.

2 Introduction

2.1 Summary of the security of client PCs

In recent years, worms and viruses using the secu rity hole of operating systems and applications ha ve spread. And inadequate settings of application and Operating Systems raise up threat of spreads of worms and viruses. For such fact backgrounds, the voice which desires solution in order to manage securi ty of client PC is mounting from many company and other organizations which have a lot of client PCs. On the ot her hand, many companies have troubles in managing security of clien t PCs because of its difficulty. [2]

Unlike a server, neither users nor use p urposes are being specified at many of clients PC. And there is no case in which software and hardw are i n one company are unified. Therefore patching software on client PCs is more difficult than that of servers , becaus e there is so me situation that there are users who use application without patches because of its troublesome and because patching sometimes broken the software which is indispensable for their business. And so, software without patching is continuing being used.

One of the reasons why the se curity level of client PCs is lower than that of servers is that management of client PCs is almost left to ordinary users who have not adequate knowledge of security. It can be said generally that ordinary users of client PCs have only a few consciousness toward security matter co mpared with administrators of servers. And it can be also said that the PC users ' consciousness toward security matter greatly contributes security level of client PCs. However, at case of such a co mpany, which has so many ordinar y users the cost and time to educate the users is heavy subject of business administration. So in many cases, promotion of users' consciousness has been failed.

The impacts and threats, which are caused by dangerous client PCs is growing up year by year wi th evolutions of worms and virus. For example, just one fragile client PC is infected with worm using security hole via the Internet and then the worm will be searching a new target on LAN and be contaminating that. Like this, all fragile PCs connected to the LAN will be infected. And the traffic of that LAN will overflow. In the worst case, the business of that company may be stopped because of just one fragile client PC. In recent days, the worst cases described previously became less new.

In general, the number of c lient PCs that the company ha s is in proportion of the number of the members of that company. And so the number of fragile client PCs will be in proportion of the scale of t hat company. And its impacts and t hreats by worm and virus will

be in the same. In short word, it is very necessar y and important for large co mpany to find out and eliminate the fragile client PCs because the impact caused by that fragile client PCs is so big. To cope with the problem like this, audit of client PCs, auto patc hing tool and tool to carry out the security policy collectively have been available ever before. However, in some case the scale of the company too large to adopt that so lution.

I said again that users' high consciousness to the security of client PCs are necessary and important to cope with the threat , which is increasing day by day. In other words, client PCs users need to observe the security policy actively by t hemselves. But those tools , which were described previously is not much effective to do so. And promoting the ordinary user's consciousness to security is difficult in short terms.

2.2 Importance of the security of client PCs

2.2.1 Security holes of client PCs

All of the Operating System of almost client PCs is Microsoft's Windows series. T herefore in this report I describe about only client PCs, which are using windows.

Not only in Windows but also in software have so me bugs surely. And the b ugs in software often cause security problems. The s oftware used on server is maintained by server administrator who is expert in operating servers. And the security levels of servers are generally kept. And settings of server software can be set up as having no security problems in case that administrator of server has common sense about server operating. On the oth er hand, the software used at client PCs also has bugs. But the security problems of client PCs are hardly modified. Because users of client PCs are indifferent to security problems or/and users' skill is not enough. However, attacks to the fragile client PCs such as described before is increasing. In order to defense the attacks, these counter measures showed in below are available.

- Parching security holes
- Using software under safe se ttings
- Promoting users' consciousness of client PCs security

However it is difficult to practice all the counter measures described above because of the characteristics of client PCs.

2.2.2 The trend of patches of Windows OS in recent years

In 2003 the number of patches (Security Bulletin) released by Microsoft was over 50. The numbers of patch release from 1999 to 2003 ar e showed below. And until the end of Feb. 2004 , 7 patches have already been released. If this trend continues, the number of patch release in 2004 will be almost same as recent year. [3]

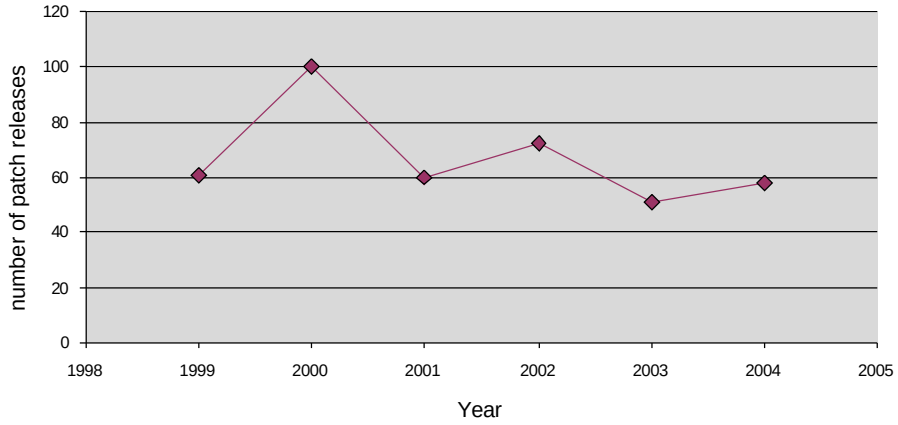
Year	Patch Releases
1999	61
2000	100
2001	60
2002	72
2003	51

Table 1: Number of Patch Release

The graph below shows that the trend of the number of the patch release by Microsoft has been decreasing , excepting the number in 2000. The number in 2000 was extremely large.

The reason is that the releases of Windows 2 000 and Windows ME had caused patch release rush. However the average of the number of the patch release is 61(standard deviation is 8.6 pt.) , excepting the number of 2000. And the number has been still high.

If about 60 patches are released in one year an d the number is simply divided by 12 month, it can be said that users of client PCs need to patch their PCs 5 times in a month. Even if Windows Update is available, it can be troublesome operation for ordinary users. At the same time, checking that all cli ent PCs in company have been patched is difficult for system administrators and security administrators.



Graph 1: Transition of the number of patch release

Notice: The number of 2004 in the graph is being forecasted by Re gression analysis.

Microsof t has released the solutions for these difficulties. These solutions are showed below. [4][5][6]

- SUS (Software Update Service)
- SMS (System Management Server)
- MBSA (Microsoft Baseline Security Analyzer)

The specifications of each tool will be described in other chapter.

2.2.3 Worm and Virus using the security holes

In recent year, worm and virus using security holes is extremely increasing. The examples of the worm and virus are shown below. [7] Their means are continuously evolving year by year. And the damages by them are also becoming large with their evolution. For example Nimda had damaged not only one organization but also entire Internet.

Name	Charactaristics	Security hole of
CodeRED	Spreading by using security hole of IIS	IIS
Nimda	Spreading with various means: not only file copy, via e-mail and via a network drive but also embedded script to homepage on ISS' web server invaded by using the security hole. And very strong infection power.	Internet Explorer IIS
WORM_ALIZ	Mail body is "Peace."	Internet Explorer
WORM_BADTRANS	Not only Mailing to other users but also inject a keylogger to the victim client PC. And sending the log to the Internet. Spreading for long terms.	Internet Explorer
WORM_KLEZ	Because subject, body and attached file of the infected mail is randomized it is difficult to specify the actual infected victim client PC. And some kind of subspecies destroys files of the victim PC.	Internet Explorer
WORM_FRETHEM	Because the mail subject name which becomes that it is likely to perform carelessly "Re: Your password" was used. worm spread mainly by the company for a short period of time. It sends harmless text file besides the virus file "password.txt".	Internet Explorer
WORM_BUGBEAR	A back door is devised and the worm stops security software.	Internet Explorer
WORM_MSBLAST	It invades into the computer on a network using the security hole of Windows called "RPC DCOM buffer overflow." And the DoS tool which devises a network attack to "windowsupdate.com"	RPC DCOM

Table 2: worm and virus using security holes to infect

The characteristic of worm and virus using security hole is that when at once they infected a fragile computer, they find other fragile computer on the LAN which the infected computer is connected to and infect the computer they find. There are a lot of reports about MSBLAST. The characteristics of the damage by MSBLAST have been reported that mobile PCs infected by MSBLAST had been connected to the LAN and then the MSBLAST had spread into the LAN and finally stopped the LAN.

The reason why MSBLAST had spread so widely was that MSBALST had been using the security hole of the low level API of OS. And unfortunately almost all the ordinary user had not realized that the damage was very large, when malicious code was exploited with the security hole. As the results so many fragile client PCs had continued connecting to LAN and Internet though the patch for the security hole had been released. The appearance of MSBLAST was the turning point of changing ordinary users' consciousness to the patching and to security of client PCs.

2.2.4 Secure setting of client PCs for applications

Patching client PCs is not enough to assure safety of client PC. The reason is that worm and virus have been wisely using the inadequate software settings, which helped them to trick users. For example some worms have a technique that tricks user to click himself with the fact that registered file extension is not displayed. To avoid this trick, users need to select the option ("registered file extensions shall be displayed") of explorer of windows. However, many users are continuing using Windows without selecting that option.

And it is hard for ordinary users to set the settings of JavaScript and ActiveX of browser in order to be able to surf Internet safely and easily because it needs knowledge of security to do so. Needless to say using ActiveX downloaded from Internet is dangerous. And inadequate JavaScript settings sometimes cause users to be stolen Cookies by malicious web site. But many web sites on the Internet require that their users turn on JavaScript of users' browser. And so a lot of users are continuing using browser with convenience, which

do not need for almost users. [2]

And a lot of products of Microsoft have macro functions. Worm and virus have been continuing using macro functions since the function implemented on Microsoft Office. To protect user from worm and virus, Microsoft office have function to inquire users whether they permit office to use macro or not if the office files to be opened include macro. However this function is not enough to protect users from worm and virus. And some users turn this function off. The reason is that what office inquire users every time when users is opening the file that may include macro worms make user feeling uncomfortable. Worm and virus attack the users like this.

2.3 The necessity and importance of management tool of security polices

2.3.1 The security polices of client PCs

In the organization that so many types of user are in it is very hard to manage patching the client PCs and setting of software installed in the client PCs. However, if this management is inadequate, so large damage will be caused.

And then organizations establish security policies in order to request users that they should patch their client PCs and set up their application safety according to the security policies. But in so many cases, skill and consciousness of ordinary users are not enough to realize the security policy.

In other case, the security policy is violated intentionally. When the security policy is violated, penalty is given to who violated the security policy. But it is not realistic that penalty is given to users whenever they forget to patch their client PCs by so many released patches.

And audits are needed in order to give penalty to users who are suspected to be violating the security policy. But it is not realistic that system administrator check every client PCs in the organization.

2.3.2 Types of users in organization

The types of client PCs users are classified as 3 classes and their subtypes. This classification is shown below. [1][2]

A. Users who observe security policy
   - i) Users who observes independently
   - ii) Users who observes but not independently

B. Users who do not observe security policy
   - i) Users whose consciousness to security is not enough
   - ii) Users whose knowledge and skill of security is not enough

C. Users who protest the security policy

Type-A users are good user from the point of view of security administration. Especially Sub type A-i users is good users. Because subtype A-ii users are cooperative with security administrator and system administrator, they do not trouble with security administrator and system administrator.

Type-B users so metimes trouble with security administrator and system administrator. The reason is that they have some trouble with themselves. The security administrators and system administrators must educate these type -B users. Needless to say this process should be done in the limited budget and schedules , which are divided by the manag ement of the organization.

Subtype B-i users are the users who sometimes violate the sec urity policy because they have little consciousness to security. However, i f they have no malice, the security administrator can educate them and make them be type -A us ers. On the other hand, type B-ii users are the users who have little skill and knowledge about security. And the security administrator can educate them or distribute security utility software and make them to be type-A users.

Type-C users are rebellious to the security administrators and the system administrators. In other words, they are terrorists in the co mpany. They complain to the rules and vio late them intentionally. They set u p their client PCs as they like. Sometimes their settings are very danger and their client PCs are very fragile. This type of user is already an enemy for a security administrator and a system administrator. And so administrators must fight against the terrorists in the co mpany. However the terror ists often trick administrators cleverly. So they are hard to be found.

Almost users could be c lassified into Type A and Type B a lthough it is dependent on the degree of maturity of an orga nization. However, who m administrators truly have to correspond to is a user with the strong tende ncy of Type B, and especially Type C user. Type C user should be punished according to security policy of the entire organization. So the administrators should find out type -C users and collect evidences. It's an audit.

2.3.3 The necessity for a management sol ution of police management

Some solution s, which support administrators to manage client PCs and users are released by Microsoft . Example solutions are described below again. [4][5][6]

- SUS (Software Update Service)
- SMS (System Management Server)
- MBSA (Microsof t Baseline Security An alyzer)

Detailed explanations about these tools are omitted i n this paper. The cor respondence table of a solution, the characteristic of the function which a security management person needs, and an effective user is shown belo w.

Microsoft Solutions			Tool	Description	Type-A	Type-B	Type-C
MBSA	SUS	SMS					
*	*	*	Patch tool	This tool supports users to patch security holes without complexity by theirselves.	Available	Available	Not available
	*	*	Integrated management tool	This tool supports system manager to manage users.	Available	Available	Not available
*			Client security check utility	PC users can check the security level of their PCs easily with this tool.	Available	Needed	Not available
			Secure setting supporting tool	PC users can set up their PCs as a secure PC easily with this tool.	Available	Needed	Not available
			User education tool	This tool supports system manager to educate PC users to promote their consciousness to security.	Not Needed	Needed	Needed
			Penalty Tool	This tool can find out the users who break the security policy and give some punishment.	Not Needed	Needed	Needed

* means that the solution can be used as the tool

Table 3: correspondence table of a solution

The 3 solutions released by Microsoft can mitigate a system administrators' works. However these solutions cannot cover all tools, which administrators need, as shown in a table. Secure setting supporting tool, User education tool and Penalty tool are necessary for security administrator to correspond to type-B users and type-C users. Client PC Security Check System described in next chapter can supply and cover these tools.

3 Client PC Security Check System

3.1 Summary of Client PC Security Check System

Client PC Security Check System aims to supply tools that former solutions could not provide to administrators. These tools are being described below. [8]

- Secure setting supporting tool
- User education tool
- Penalty tool

The figure shown below describes the abstract of Client PC Security Check System.

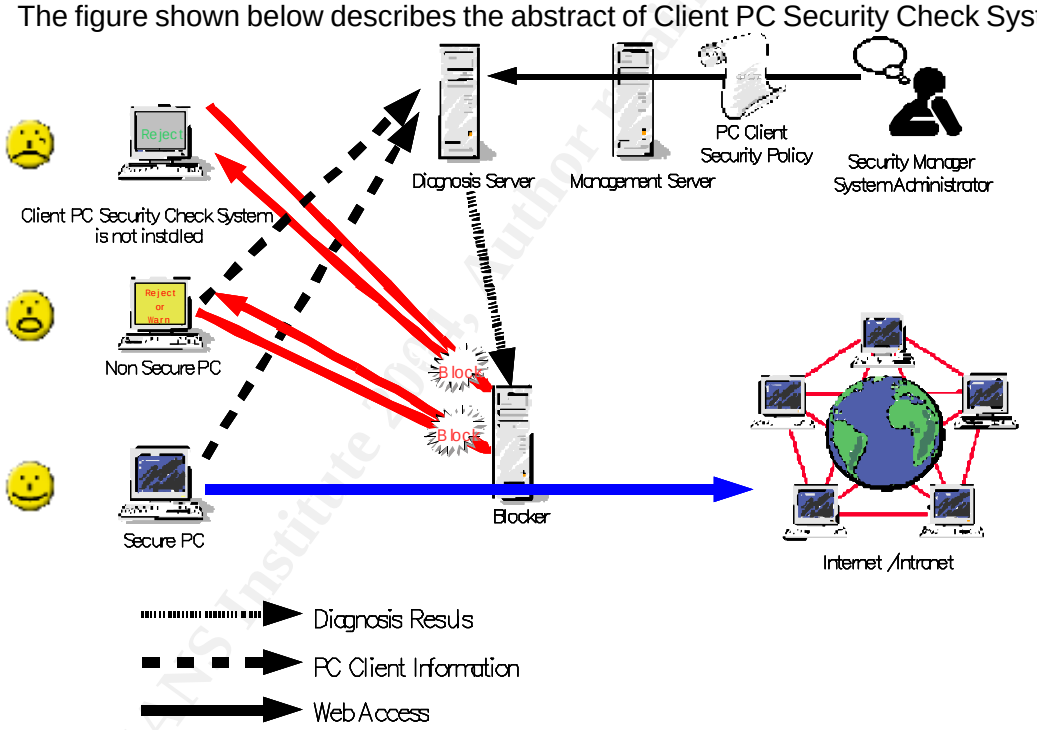


Figure 1: Abstract of Client PC Security Check System

The Agent, which is called "Check Agent" is installed into client PCs by administrator or client PC user. Check Agent gathers information of client PCs. Diagnosis Server receives client PC information by Check Agent and notifies status of the client PC to Blocker. Blocker restricts or permits web access from the client PC by the status of client PC.

Because browser is the most indispensable and important tool for client PC users, restricting browser using and notifying the message claiming that users have to observe security policy are effective to promote the consciousness to security.

Check Agent compares the information of the client PCs to the information registered in the Management Server such as information of patches and software settings and so on.

And then Check Agent displays the difference between the client PC state and the ideal state registered in Management server by administrators to client PC users. Client PC users are able to understand the difference very easily by using the information displayed by Check Agent.

After diagnosis server receives information of client PCs, the results of diagnosis are sent to blocker. Blocker acts on the web access from the client as described below.

- Accept If nothing dangerous exists in client PC, the web access from the client PC would be accepted.
- Warn If something dangerous but not so dangerous exists in client PC, blocker warns via browser the user that the client PC of the user may be dangerous. Once this warning is displayed on user's browser, the warning is not displayed until the warning interval will reach. This warning is replayed every 30 min.
- Reject If something dangerous exists in client PC, the web access from the client PC is rejected by blocker and Blocker warns via browser the user that the client PC of the user is dangerous and that the user should observe the security policy.

Blocker is aiming at promoting the users' consciousness of the security by blocking the web access from the client PCs that are managed by the user who violate the security policy. On the other hand, if client PC user dose not run Check Agent, Blocker denies the web access from his/her client PC. Therefore, Blocker can give penalty to user who dose not run Check Agent intentionally. In this way, Blocker saves resources to educate ordinary client PC users.

And Check Agent has a function to modify the settings that are different from the settings recommended by administrators. And the users can modify the inadequate settings easily with one click of "Modify Button". The "Modify Button" is activated automatically if something wrong exists in the client PC. By using this function, the user who is too busy or not enough skillful to set up his/her client PC correct can observe the security policy.

3.2 Introduction of each function of Client PC Security Check System

3.2.1 Diagnosis

Diagnosis function is the most important of the Client PC Security Check System. The screen shot shown below is the diagnosis results on the user screen. System and security administrators can view the result via the management interface. The management interface is being explained in other chapter: Management of users. And diagnostic items are also explained in other chapter: diagnostic items.

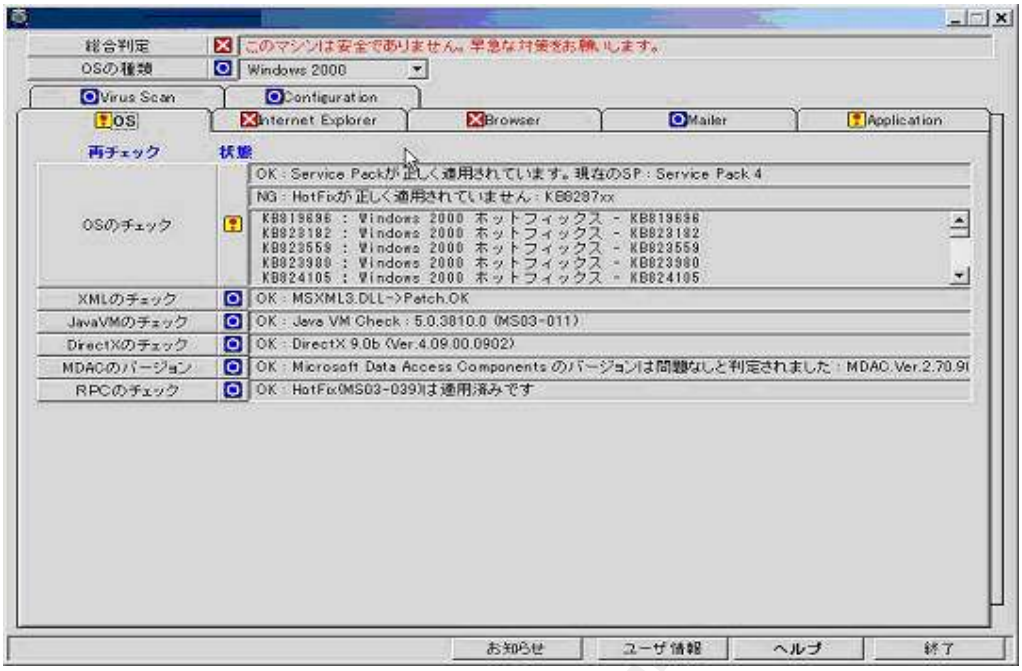


Figure 2: Diagnostics Interface 1

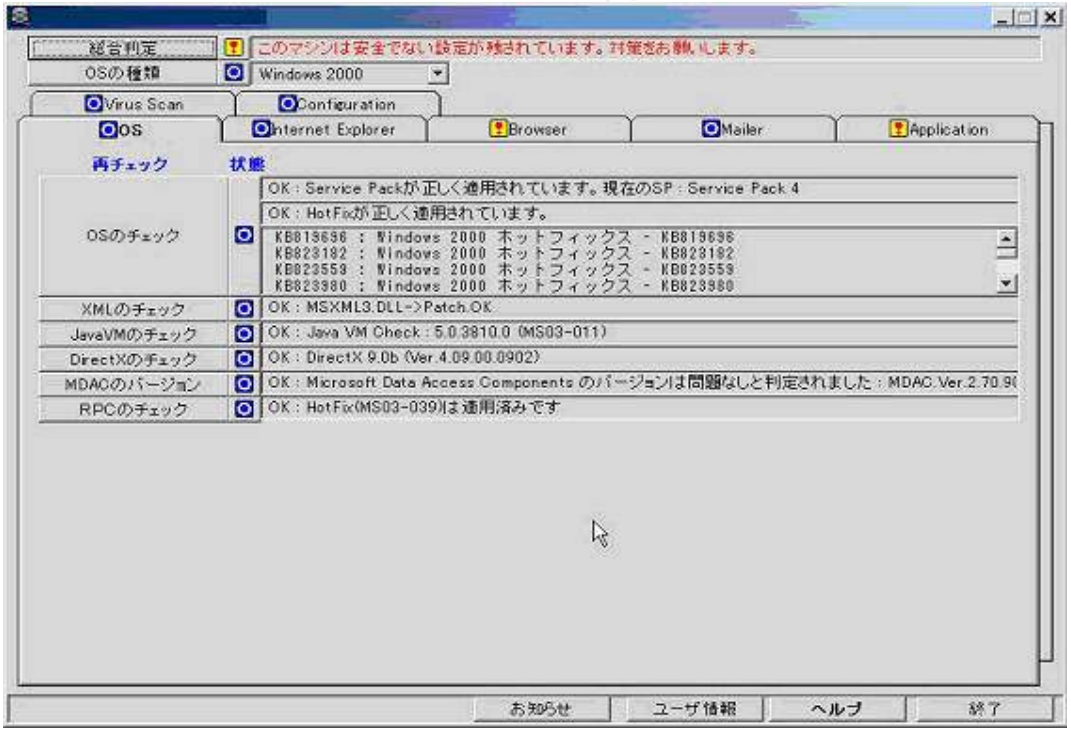


Figure 3: Diagnostics Interface 2

The user interface of Check Agent can display the difference between the settings of the client PC and the ideal settings recommended by the administrators. And the display is very easy to understand what is wrong. The i nterface has function which can lead the users to the security portal site created by the administrators on intranet or internet The users can acquire information about the latest security affair. And it can promote users' consciousness of security. On the other hand, the users can retrieve the information about how to patch their client PC and so the site can be help desk when the users patch their client PCs by themselves.

Unfortunately, this system has been released in only Japan. So screen shots are not in English. However, each tabs on the application's window correspond to each diagnosis items. Each diagnosis items written in English are described in proceeding chapters.

3.2.2 Adjustment of Settings of PC

As described for mer chapter, Check Agent has a function to modify the settings that are different from the settings recommended by administrators. And the users can modify the inadequate settings easily with one click. Check Agent modifies the registries and the setting files directly in order to modify incorrect settings. But users do not needs to understand which registry or file should be modified. And the users do not need to understand even where the setting menu is. This function can help busy user and skillless user to correct their client PCs by themselves. Therefore this function is useful to educate Type-B users to be Type-A users.

3.2.3 Block of Web Access

This function restricts the web access from the client PCs that have dangerous settings. In recent years, web access is indispensable tool for office works. And so if users were restricted to use browser for web access on the Internet or the Intranet, user would feel it so inconvenient. Therefore to block web access must be one of the best penalty for the users who violate the security policy. By this penalty, the function is aiming to force the users to observe the security policy. In other words, blocking web access can promote the users' consciousness of security.

And some kind of browsers such as Internet Explorer which is not newest have dangerous bugs allowing malicious web site to inject virus and worm into client PC. If the user accesses the malicious web site via the fragile browser, the fragile client PC will be infected. And so restricting use of the browser for accessing to the Internet can mitigate the risk.

The screen shot shown below is the block messages. This message will be displayed if the user intends to access the Internet from fragile client PC. The fragile client PC has serious violation of security policy.

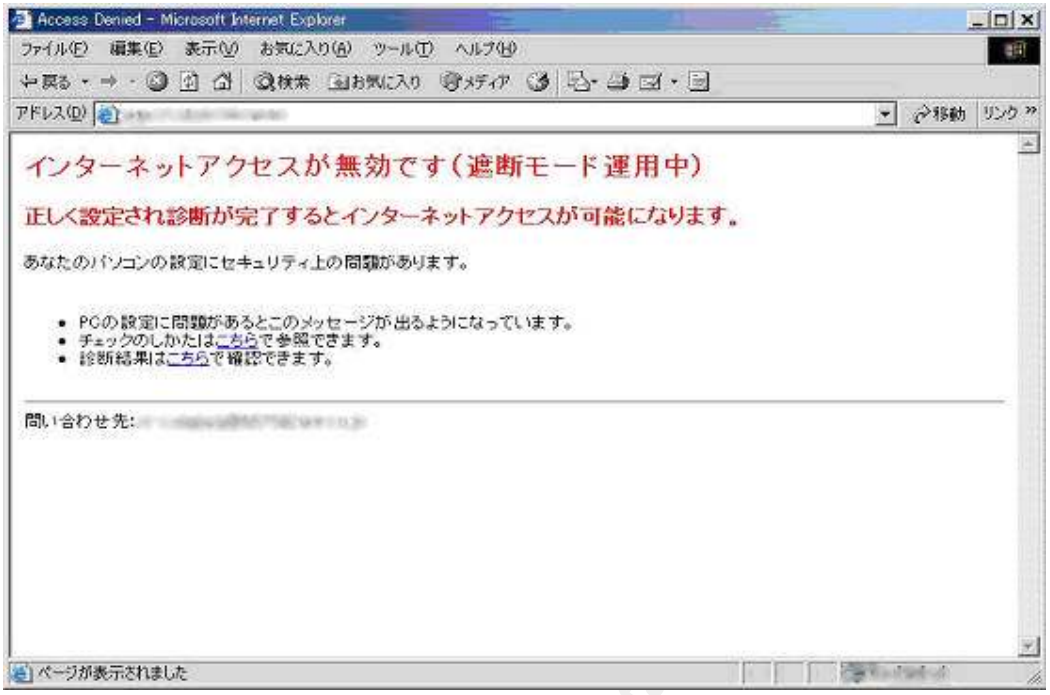


Figure 4: Rejecting web access because the client PC is v ery fragile

And the screen shot shown below is the block message that will be displayed if the user s do not run Check Agent intentionally or not i ntentionally.

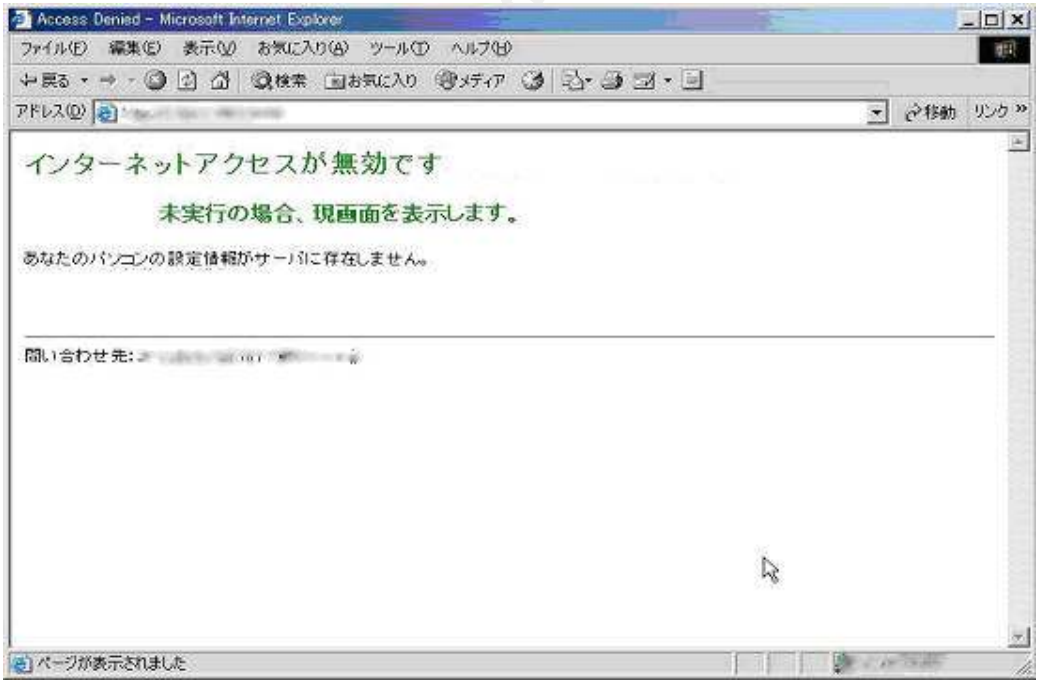


Figure 5: Intercepting web access because the client PC did not run Check Agent

And the next screen shot shown below is the warning message that will be displayed if the user access es the Internet from not so fragile client PC . This warning is aiming promoting the user's consciousness of security.

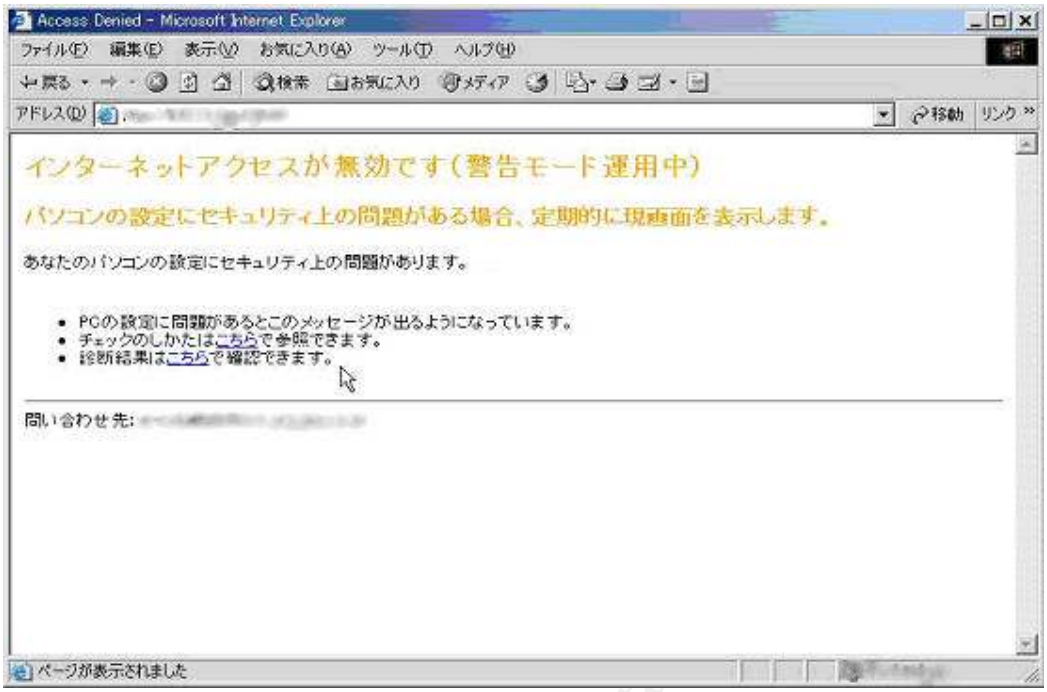


Figure 6: Warning the client PC user who violate security policy

3.2.4 Notification form Administrators

Notification function notifies the latest information registered by administrators to the users when Check Agent runs. By using this function, the administrators exactly can notify urgent information about security to the users. The message is emphasized and displayed according to urgency. Client PC Security Check System emphasizes the critical message about security by displaying the message on the top of dialog and changing the color of the title of the message. By pushing the display button that is beside the title, the user can see the contents of the messages.

Figure 7: Title dialog

The screen shot shown below is the dialog of the content of a message.

Figure 8: Message from administrators

3.2.5 Management of Users

System and security managers can manage the users via the web interface of Management Server of Client PC Security Check System. They can search and select user by using the user's attributes. The screen shot shown below is the user searching int erface.

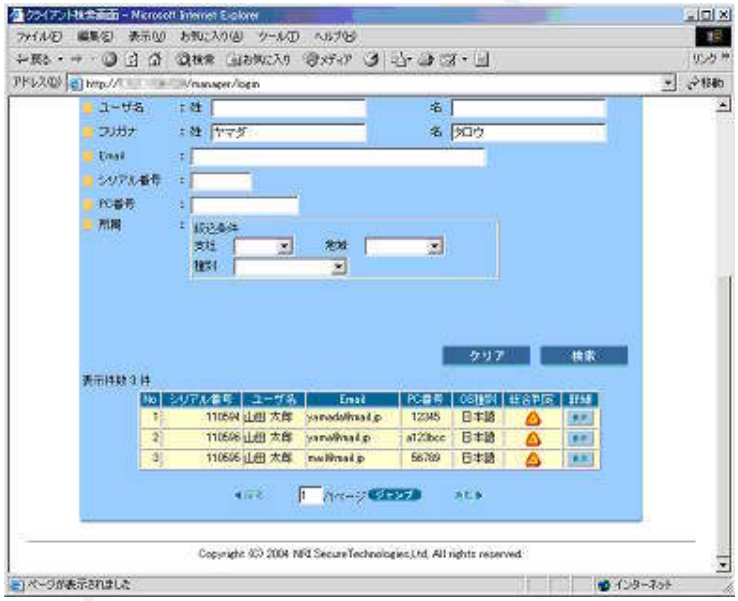


Figure 9: Web interface to search users

This information about users can be exported as CVS fi le. Administrators can total the data uniquely.

And administrators can view detailed data of the users who se arched by the user searching interface and can grasp the state of user client PC state. These detailed data is including client PC settings, patch information and difference between them and security policy.

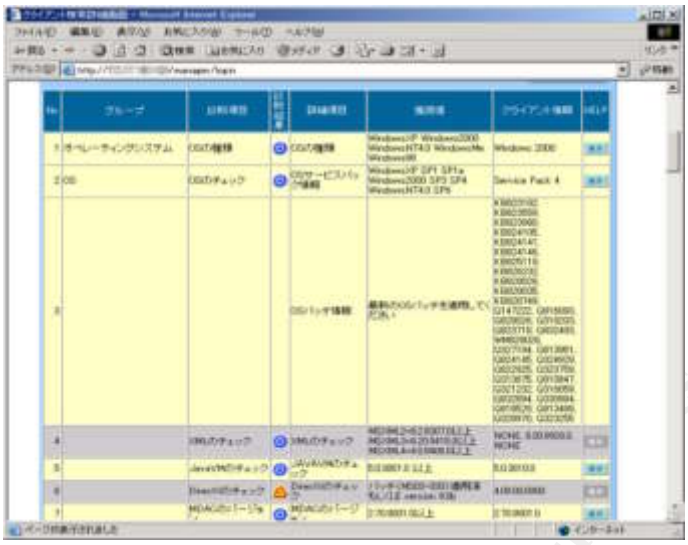


Figure 10: Details of client PC state

And Client PC Security Check System has function to grasp easily the state of client PCs which are being administrated now. The administrators of Client PC Security Check System can estimate how much risks their or ganization have. The func tion provides these parameters describe below.

- Number of client PCs which are being accepted web access tod ay
- Number of client PCs which are being warned today
- Number of client PCs which are being rejected web access today
- Number of client PCs which are not being diagnosed today
- Total Number of c lient PCs which are being mana ged today

And Client PC Security Check System has function to grasp easily the state of client PCs which are being administrated now. The administrators of Client PC Security Check System can estimate how much risks their organizations have. The screen shot shown under below is the summary of states of client PCs.

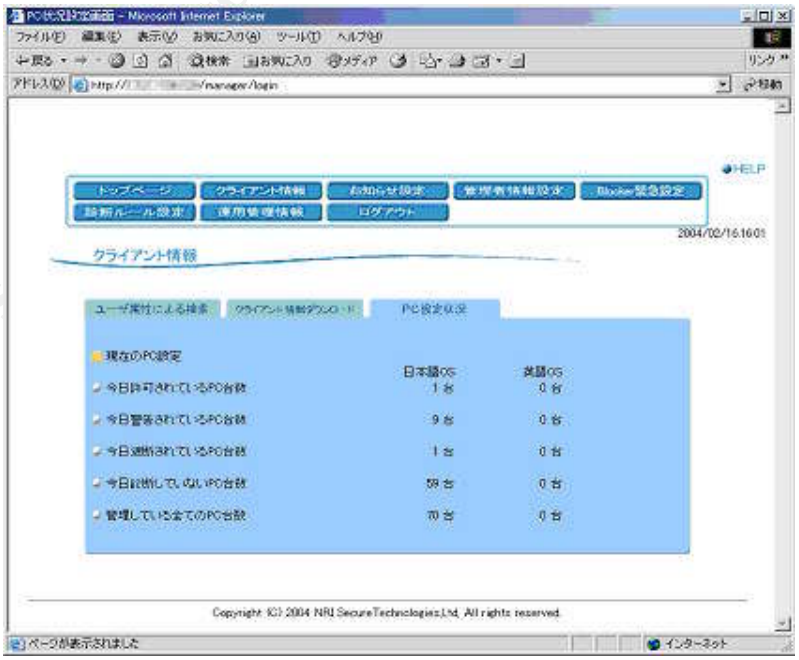


Figure 11: Summary of state of client PCs

3.3 Diagnostic Items

Samples of d iagnostic items are described in chapters to the next. The selected diagnostic items are the results that many specialists engaged in security have shared each knowledge and experience and have argued about them.

3.3.1 Operating Systems

This diagnostic item ch ecks client PC state of patches and Hotfixes including API version.

Target name for PC User	Diagnosis Target	Criteria of Judgement
OS	Name of OS	Windows 2000 SP4 or later Windows XP SP1 or later
	Service Pack	latest
	HotFix	OS must be patched with the latest HotFix.
XML	Version of XML parser	The version must be the latest.
JavaVM	Version of Java VM	The version must be the latest.
DirectX	Version of DirectX	The version must be the latest.
MDAC	Version of MDAC	The version must be the latest.
RPC	Version of RPC	The version must be the latest.

Table 4: Diagnostic Items for Operating System

3.3.2 Internet Explorer

This diagnostic item checks the version of Internet Explore and its s ettings. The settings must be proper to use Outlook Express safety.

Target name for PC User	Diagnosis Target	Criteria of Judgement
IE	Version of IE	The version must be the latest.
Settings of Security	Settings of ActiveX and Plug-ins for each security zones	Refere to the another table.
	Settings of script for each security zones	Refere to the another table.
	Setting of password auto complete	Password must not be memorized by IE.
Patch level of VB Script	Version of VB Script	The version must be the latest.

Table 5: Diagnostics Items for Internet Explorer

Diagnosi Target	Internet	Intranet	Authenticated Site	Restriced Site
Execution of ActiveX and Plug-ins	disable	enable	enable	disable
Initialization and execution of ActiveX with marking which claims that execution of script is safe.	disable	enable	enable	disable
Initialization and execution of ActiveX without marking which claims that execution of script is safe.	disable	disable	Display dialog	disable
Download of ActiveX with authenticated signature.	disable	enable	enable	disable
Download of ActiveX without authenticated signature.	disable	disable	disable	disable
Permission for Java	Safety Lebel-HIGH	Safety Lebel-HIGH	Safety Lebel-HIGH	Safety Lebel-HIGH
Active Script	enable	enable	enable	disable
Java Applet Script	disable	disable	enable	disable
Paste Function of Script	disable	disable	enable	disable

Table 6: Diagnostics Items for zone settings of Internet Explorer

3.3.3 Netscape

This diagnostic item checks the v ersion of Netscape and its settings if Netscape has been installed in client PC.

Target name for PC User	Diagnosis Target	Criteria of Judgement
Version of Netscape	Version of Netscape	The version must be the latest.
Settings of Java	Whether the settings of Java is avaliable or not.	The setting must be as not avaliable.
	Whether the settings of Java in e-mails is avaliable or not.	The setting must be as not avaliable.

Table 7: Diagnostics Items for of Netscape

3.3.4 Outlook Express

This diagnostic item checks the version of Outlook Express and its settings if Outlook Express has been installed. The settings must be proper to use Ou tlook Express safety.

Target name for PC User	Diagnosis Target	Criteria of Judgement
Version of Outlook Express	Version of Outlook Express	The version must be the latest.
Configurations of Outlook Express	Preview	Preview must not be used.
	Auto Download of messages	Message mut not be downloaded automaticaly.
	Security Zone	The Security Zone must be set as Restricted Zone.
	HTML message	HTML message must not be used.
	The mail is replyed in the same form as the message which received.	The mail must not be replyed in the same form as the message which received.
	It will warn, if other applications tend to transmit mail in the name of user.	It must be warn.
	The attached file which may be a virus is not opened and saved.	The attached file must not be opend and saved.

Table 8 : Diagnostics Items for of Outlook Express

3.3.5 Other applications

This diagnostic item checks the version of Microsoft Office series and their versions if they have been installed.

Target name for PC User	Diagnosis Target	Criteria of Judgement
Office2000	Version of Office2000	The version must be the latest.
	Level of Security for VBA	The level must be High.
Office XP	Version of Office XP	The version must be the latest.
	Level of Security for VBA	The level must be High.
Flash	Version of Flash	The version must be the latest.
MediaPlayer	Version of MediaPlayer	The version must be the latest.
VBA	Version of VBA	The version must be the latest.

Table 9: Diagnostics Items for of other applications

3.3.6 Virus Scan

This diagnostic item checks that at least one security scanner product is installed and it is being used properly.

Target name for PC User	Diagnosis Target	Criteria of Judgement
Configurations	Version of the serach engine	The version must be the latest.
	Realtime protection	It must be setted as on.
Virus pattern	Date of Pattern update	The date of pattern update must be in 10 days before.
Scan	Date of the last scan	The date of the last scan must be in 10 days before.

Table 10: Diagnostics Items for of Virus Scan

3.3.7 Configurations of Windows OS

This diagnostic item checks that Windows OS installed on client PC is being used properly and configured to be secure.

Target name for PC User	Diagnosis Target	Criteria of Judgement
Shutdown	Check of PC shutdown	The PC must be shutdonwed evryday.
File System	Format type of HDD	The format of the file system must be NTFS.
Explorer	Display of File extension	The registerd file extension must be displayed.
	Display of hidden file	The hidden file must bet displayed.
ActiveDesktop	Setting of active desktop	The conventional Windows desktop must be used.
	Display of Web	Display of Web must not be used.
	Mouse click	Single click must be as select and double click is as open.
File Sharing	Security setting of the shared folder	The folder which is evryone full control must not be shared.

Table 11: Diagnostics Items for of configurations of Windows OS

4 Conclusions

Client PC Security Check System project has just started. Therefore, it is impossible to measure the users' changes of the consciousness to the security which had been changed by Client PC Security Check System. However, when an example is taken in the fact that the number of the patch released dose not decrease and that the new security holes continue being discovered, the necessity for Client PC Security Check System has no room of doubt.

And just security scanners have been usable from old days. But such a security tool which ordinary users could use easily and which administrators could grasp the situation of client PC users with have not been available. So Client PC Security Check System is better than former security solutions because Client PC Security Check System realized the functions. It's a strength point of the system I described in this report.

5 Next Challenges

5.1 Subjects on Operating Client PC Security Check System

New virus and worm are increasing while the number of patch release and of discovery of security holes is not decreasing. And so the subject on maintenance and operation of Client PC Security Check System is that Check Agent must be updated when the new security risk is likely to occur. For example, Microsoft releases new patches every month. And so Check Agent must update the diagnosis items for new patches every month. And the time between when patch is released and Check Agent update the diagnosis items must be as short as possible. To avoid this problem, it is required that Check Agent commissions the function for checking patches to other tool such as MSBA.

And also when new application and new version of application are released, Check Agent

needs to be updated.

5.2 Coping with new threats

The appearance of the application, which causes the problem on security according to diversification of how to use PC client, is increasing.

For example, one of such applications is SoftEther [9] which emulates Ethernet LAN on TCP/IP network. This application is very useful as VPN. However, this software has the danger of exposing PC, which is protected by the firewall in the company, to the dangerous Internet, while the administrator of LAN in the company does not know. And sessions of SoftEther are encrypted by SSL. So administrators cannot exactly recognize difference between the session and HTTPS. Therefore administrators need to check all client PCs in their company one by one in order to check exactly whether SoftEther is used or not. In such case, administrators' burden can be reduced by checking existence of this application by Client PC Security Check System which has been modified to check the existence of SoftEther.

However, It is thought that the same software such as SoftEther is developed one after another and used. Therefore, the accumulation of know-how which perceives the trend of a world quickly and is made into the target of management is required.

Acknowledgement

I am thankful to members of NRI Secure Technologies, Inc. that obtained me great cooperation in writing this paper. Moreover, it is thankful to members of the development team of Client PC Security Check System who offered the subject matter.

Bibliography

[1] "Article about importance of Windows update for non client PCs without guard", http://itpro.nikkeibp.co.jp/members/ITPro/SEC_CHECK/20040302/1/
[2] "Special Issue: Advice to manage your client PC to be strong against Virus and Worms such as Blaster", Nikkei Windows Pro Magazine Nov., pp76-89, Nikkei BP
[3] "Security Bulletin Search", http://www.microsoft.com/technet/security/CurrentDL.aspx
[4] "Official Site of MBSA", http://www.microsoft.com/technet/security/tools/mbsahome.mspx
[5] "Official Site of SMS", http://www.microsoft.com/smserver/default.asp
[6] "Official Site of SUS", http://www.microsoft.com/japan/windowsserversystem/sus/default.mspx
[7] "Virus and worm Information of vender", http://securityresponse.symantec.com/avcenter/vinfodb.html
[8] "Official Site of Secure Cube", http://www.nri-secure.co.jp/service/cube.html#pc-check
[9] "Abstract of SoftEther", http://www.softether.com/jp/overview/

Last Updated: September 20th, 2017

Upcoming Training

SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS New York SEC401*	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session - SEC401	Minneapolis, MN	Oct 03, 2017 - Nov 14, 2017	Mentor
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
Community SANS Omaha SEC401	Omaha, NE	Oct 23, 2017 - Oct 28, 2017	Community SANS
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401*	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401**	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event