JPNIC・JPCERT/CC
Security Seminar2004

ホストレベル、セグメントレベル、企業レベル、グローバルレベルでの不正侵入の発見手法とは？(Windows版)

インターネットセキュリティシステムズ株式会社
セキュリティオペレーションセンター　スーパーバイザー
シニアセキュリティエンジニア
守屋　英一

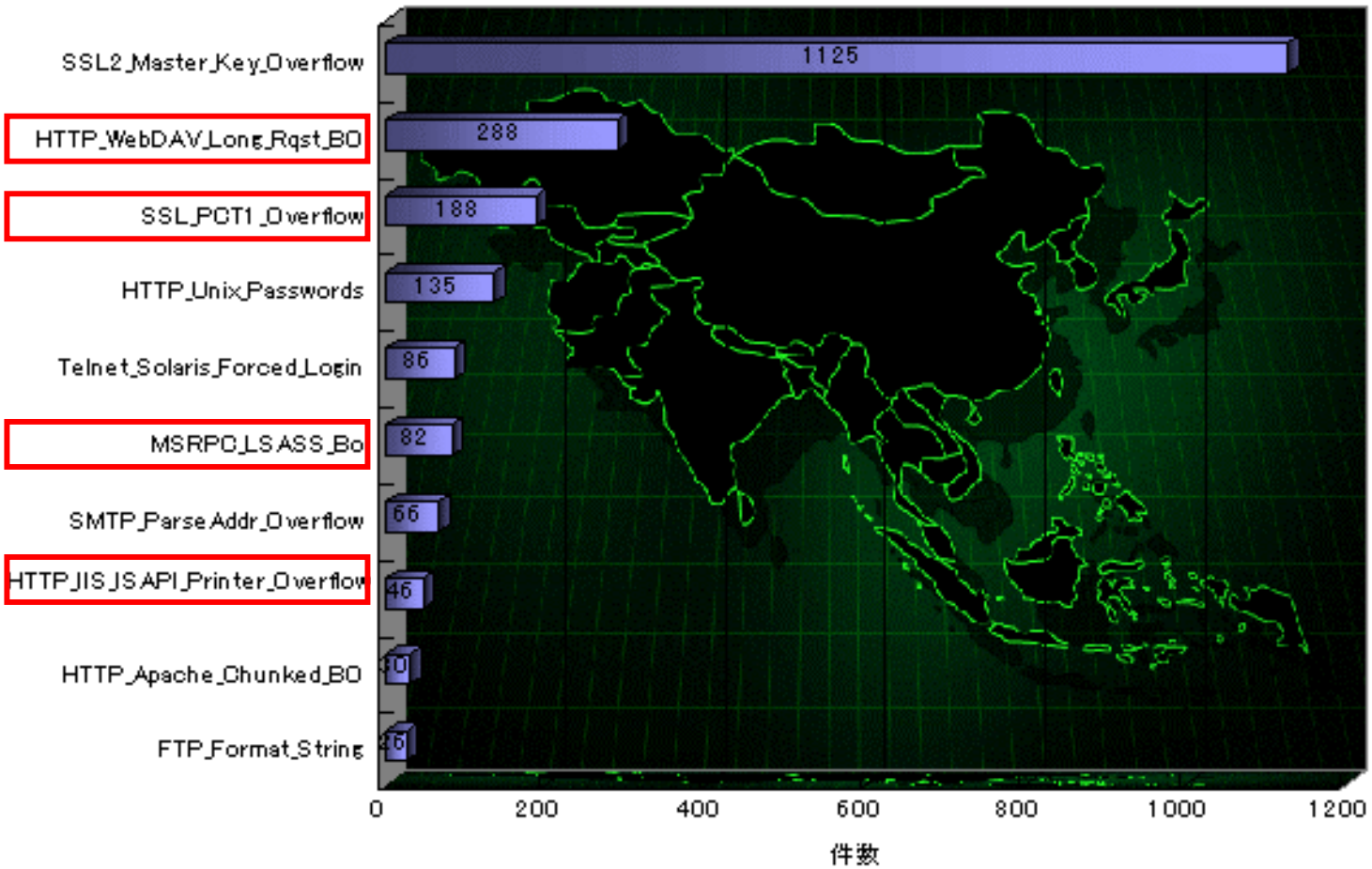
INTERNET SECURITY SYSTEMS®

2005年02月04日

目次

- はじめに
  - 不正侵入の現状
- 不正侵入の発見手法
  - ホストレベル
  - セグメントレベル
  - 企業レベル
  - グローバルレベル

トップ１０(2004年)
～はじめに～



INTERNET | SECURITY | SYSTEMS®

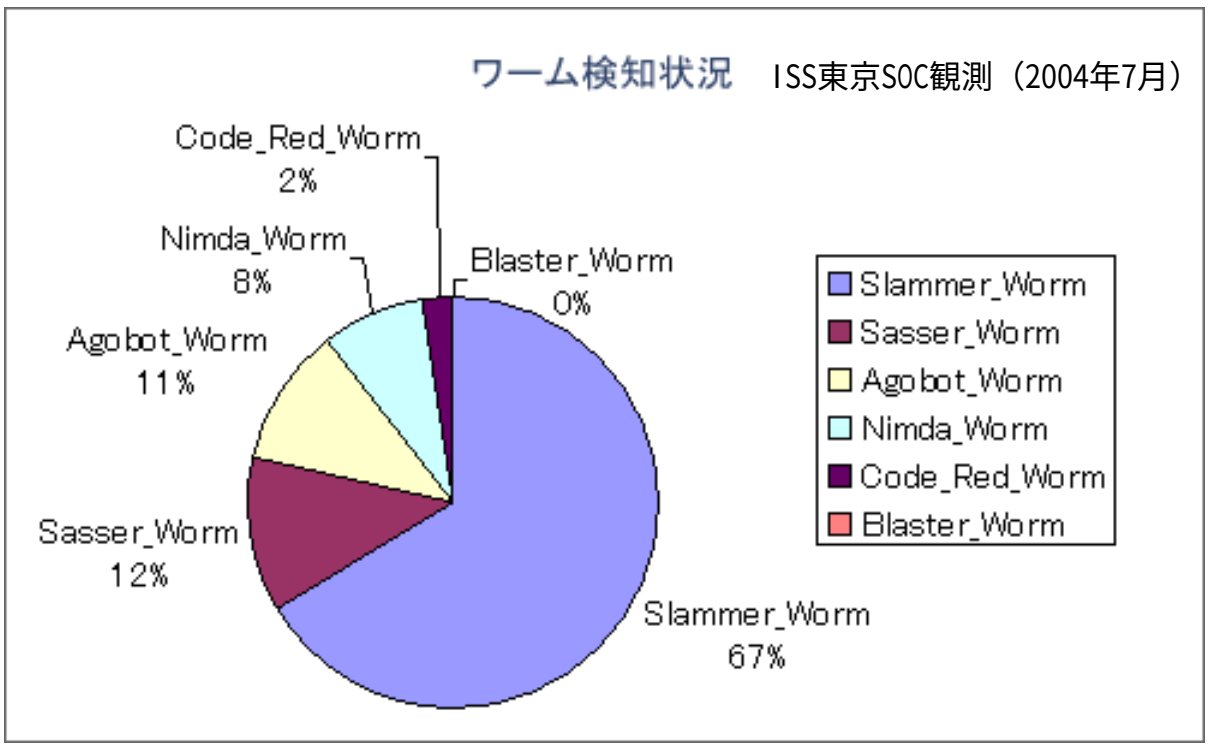
現在も観測されるワーム
～はじめに～

想定される原因のひとつ

未管理サーバの存在
感染に気が付いていない

→

不正侵入検知・防御（IDS/IPS）などセキュリティ対策がとられていない

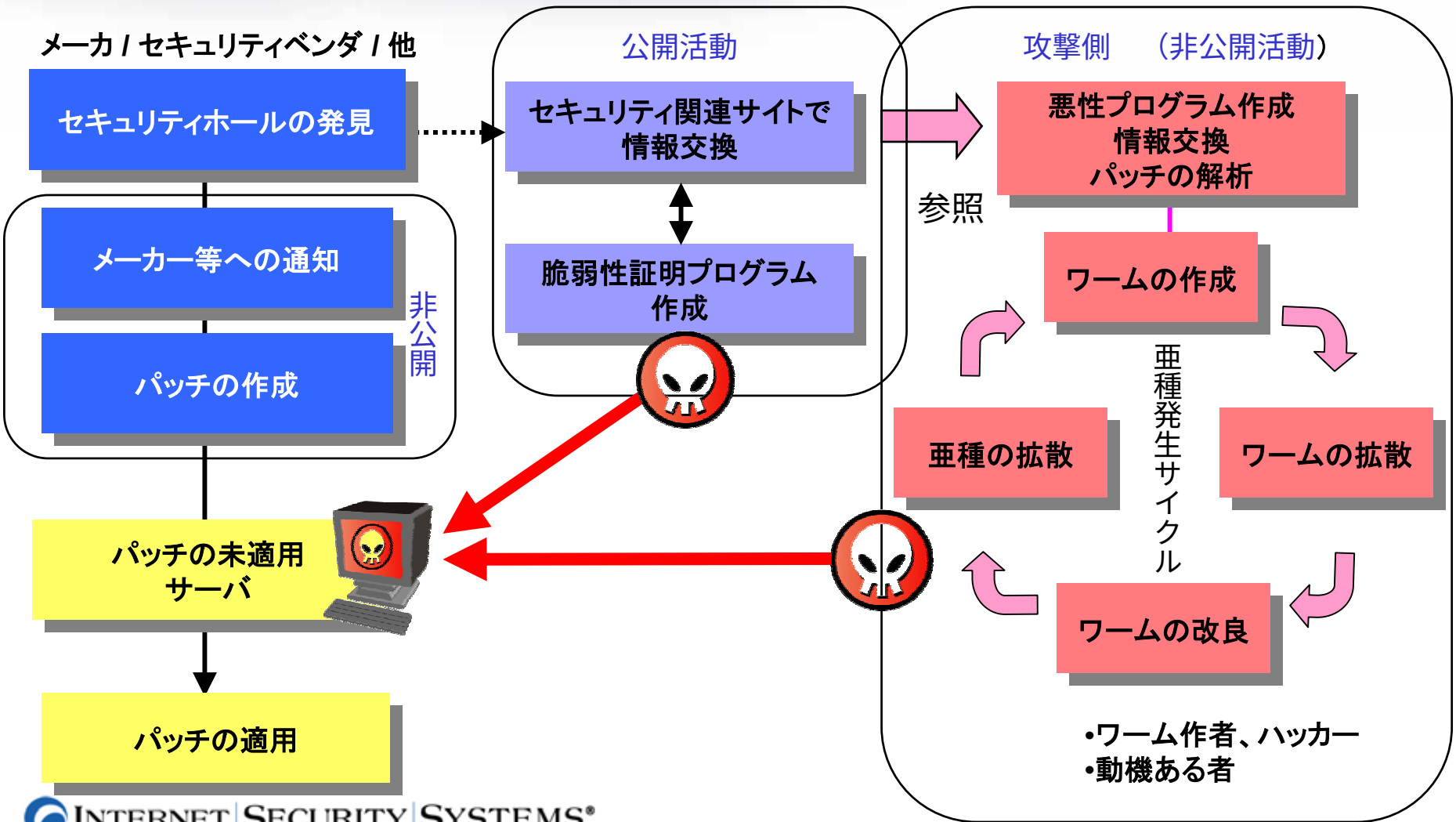


ワーム発生日時

2004/5/01 Sasser_Worm
2003/8/22 Agobot_Worm
2003/8/11 Blaster_Worm
2003/1/25 Slammer_Worm
2001/9/18 Nimda_Worm
2001/8/04 Code_Rad II
2001/7/19 Code_Rad v2
2001/7/12 Code_Red v1

INTERNET SECURITY SYSTEMS®

脆弱性の発見からワーム発生まで
～はじめに～



INTERNET | SECURITY | SYSTEMS®

攻撃のサイクル
～はじめに～

メーカ / セキュリティベンダ / 他

セキュリティホールの発見

メーカー等への通知

パッチの作成

非公開

パッチの未適用
サーバ

パッチの適用

攻撃側

悪性プログラム作成
情報交換
パッチの解析

侵入行為

悪性プログラムの
ダウロード

レジストリ修正
バックドア作成

スキャン行為
次のターゲットへ

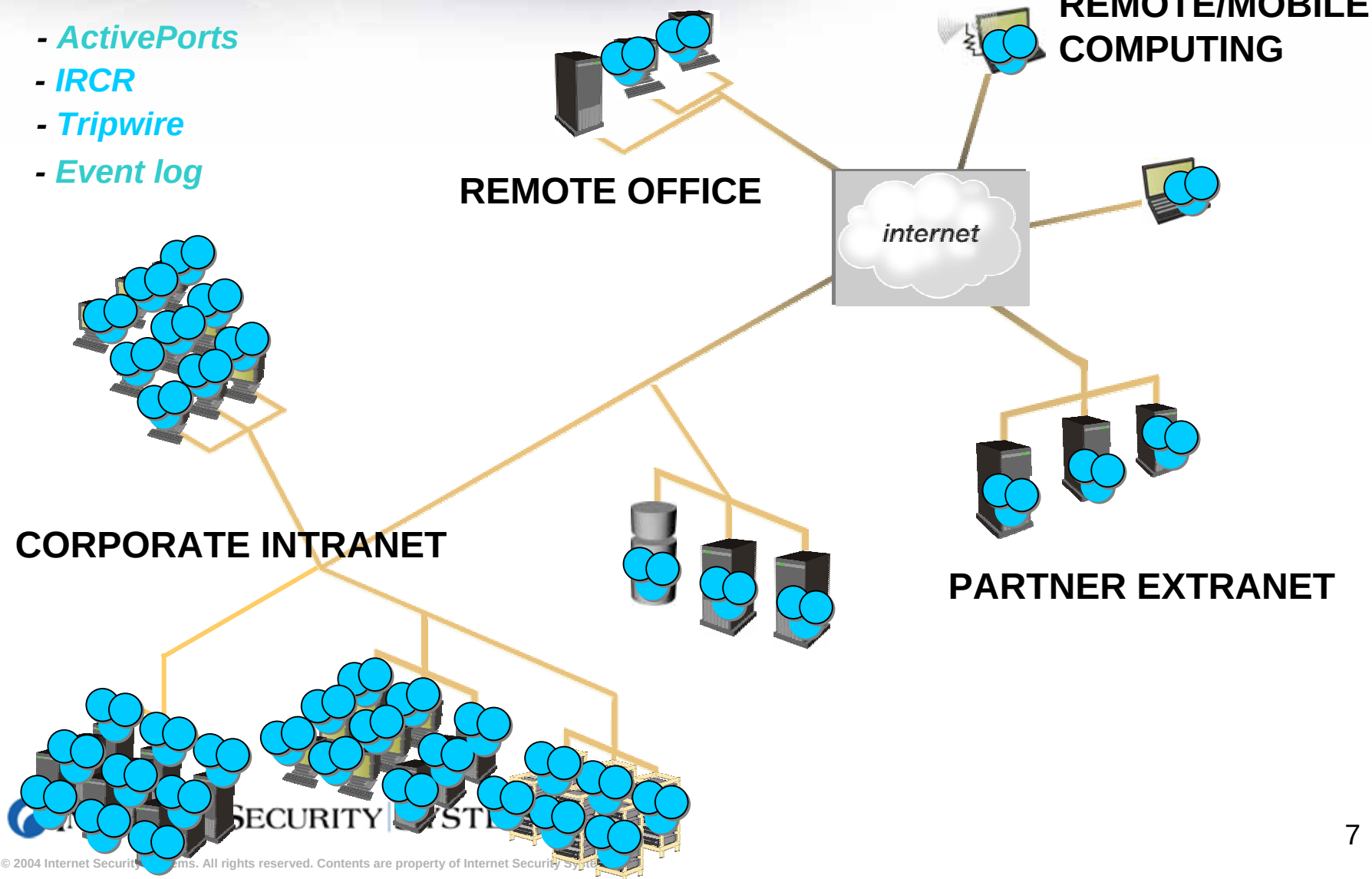
攻撃サイクル

•ワーム作者、ハッカー
•動機ある者

INTERNET | SECURITY | SYSTEMS®

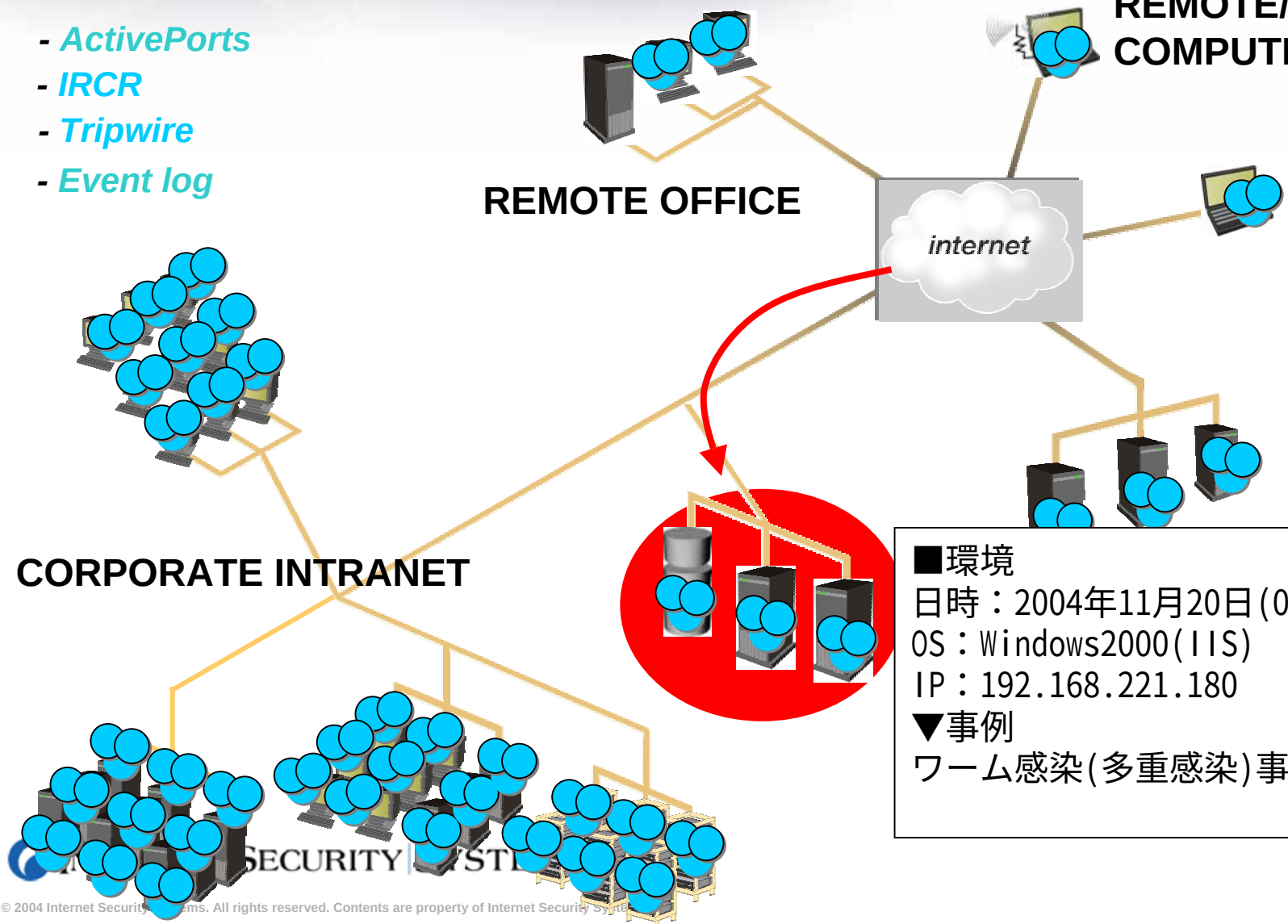
監視範囲
～ホストレベル～

- *ActivePorts*
- *IRCR*
- *Tripwire*
- *Event log*



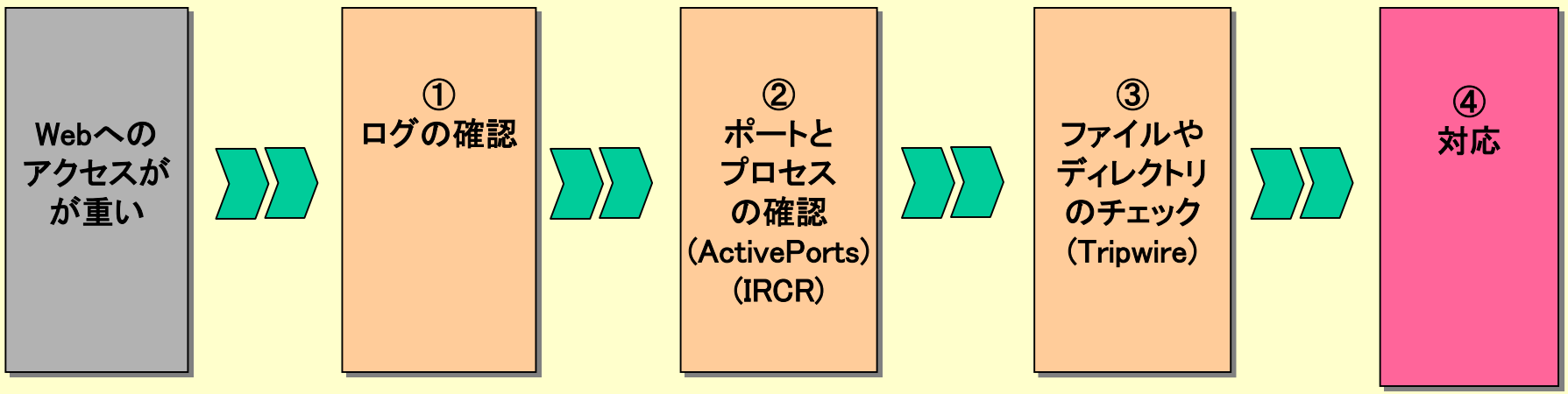
発見事例
～ホストレベル～

- *ActivePorts*
- *IRCR*
- *Tripwire*
- *Event log*



■環境
日時：2004年11月20日(0:00～8:30)
OS：Windows2000(IIS)
IP：192.168.221.180
▼事例
ワーム感染(多重感染)事例

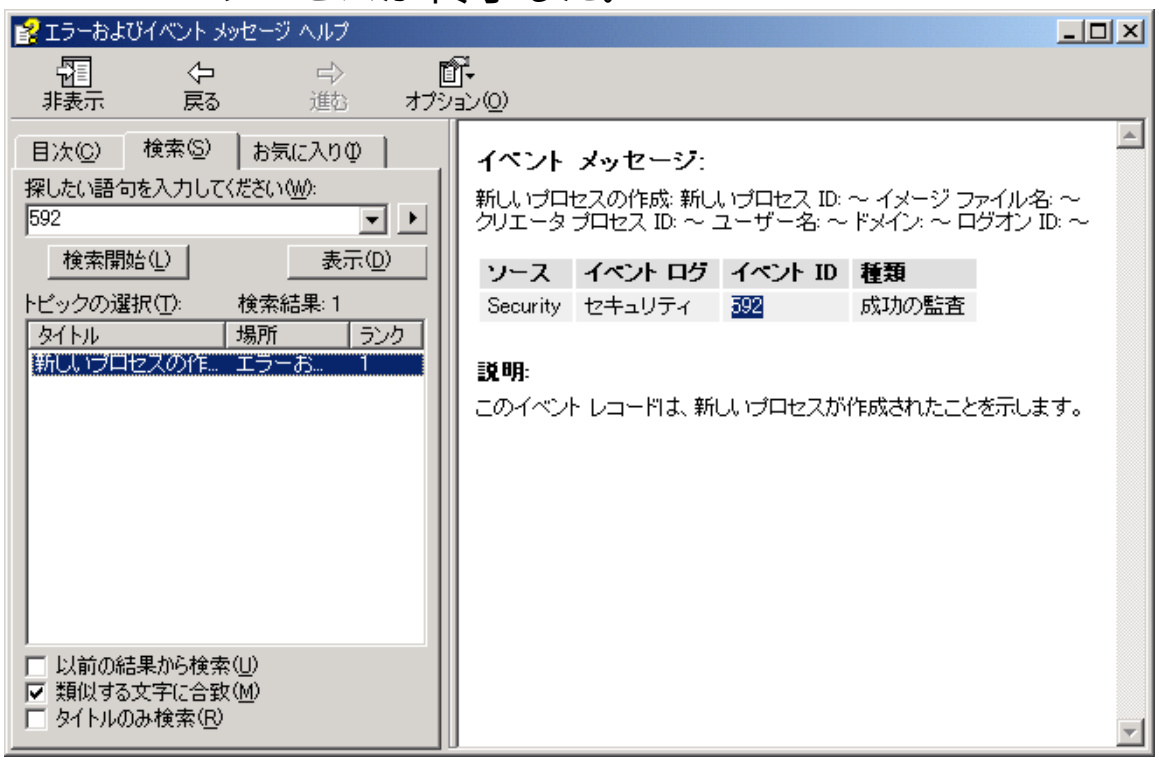
時系列
～ホストレベル～



INTERNET | SECURITY | SYSTEMS®

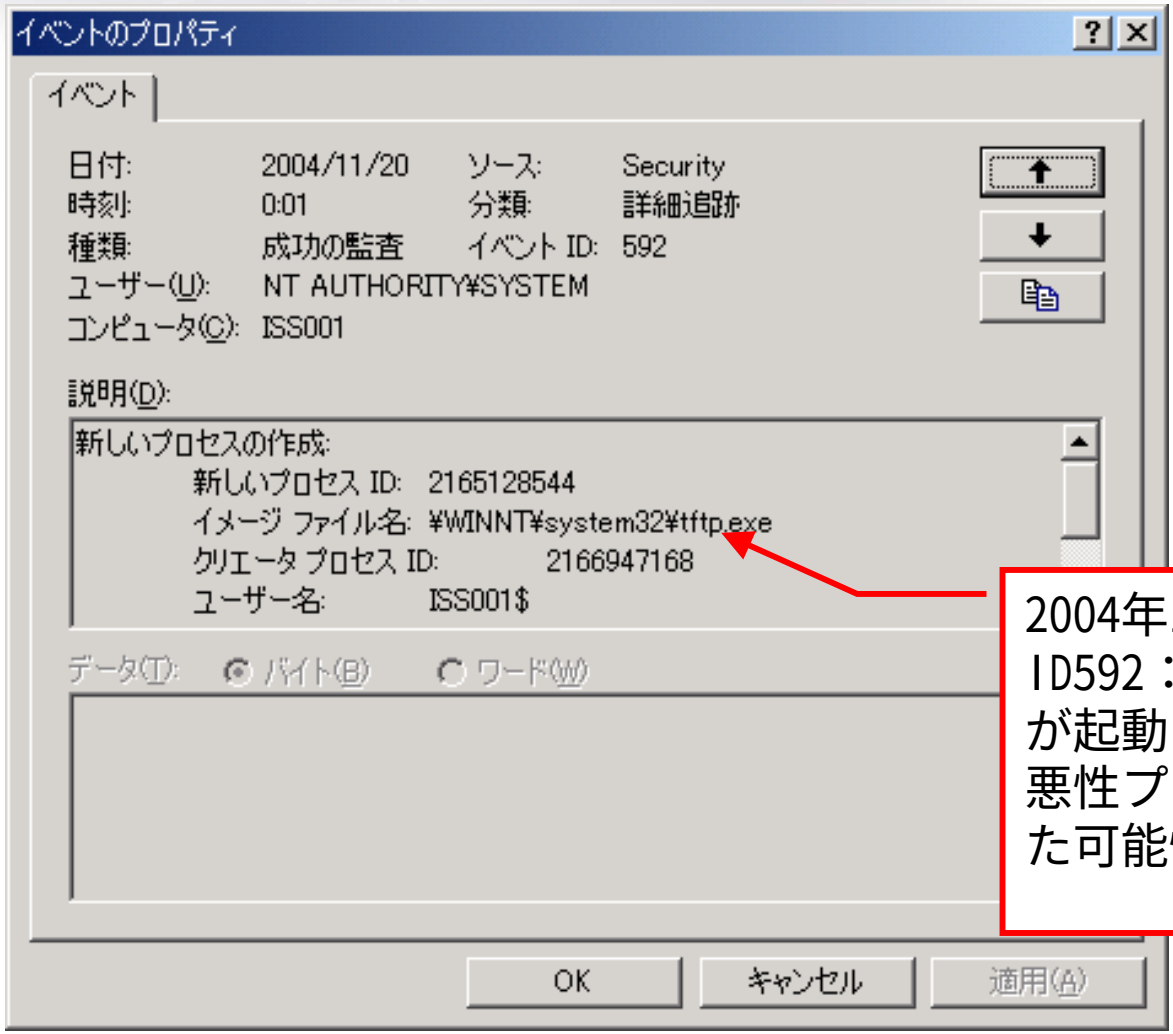
①セキュリティログでの確認
～ホストレベル～

- セキュリティログのイベントID
  - ID592：新規プロセスが作成された。
  - ID593：プロセスが終了した。



  - 詳細：http://download.microsoft.com/download/technetpluscd/Update/100/NT5/JA/w2000msgs.exe(日本語)

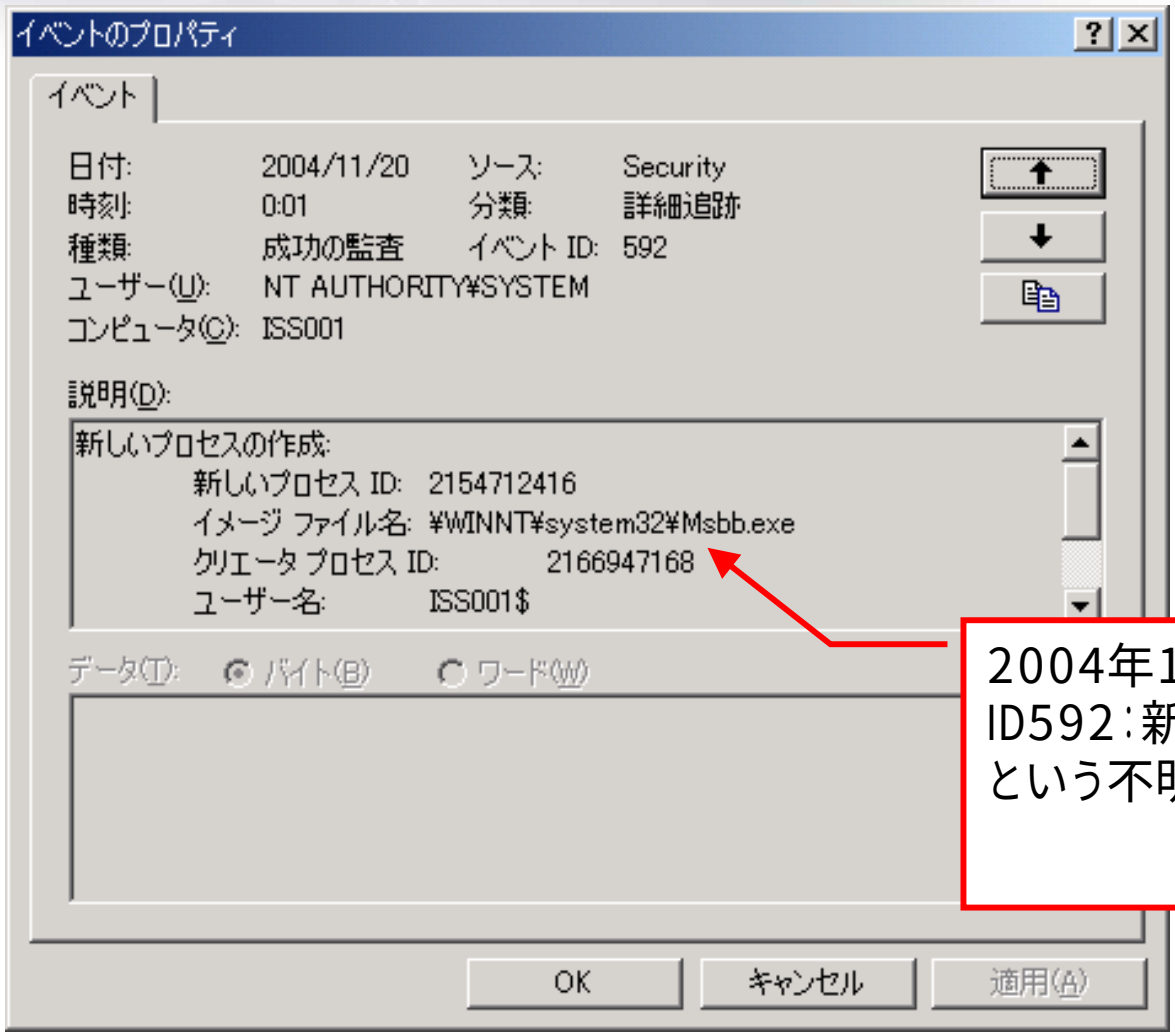
①セキュリティログでの確認
～ホストレベル～



2004年11月20日　0:01
ID592：新規プロセスとしてTFTPが起動されている。
悪性プログラムがダウロードされた可能性がある。

INTERNET SECURITY SYSTEMS®

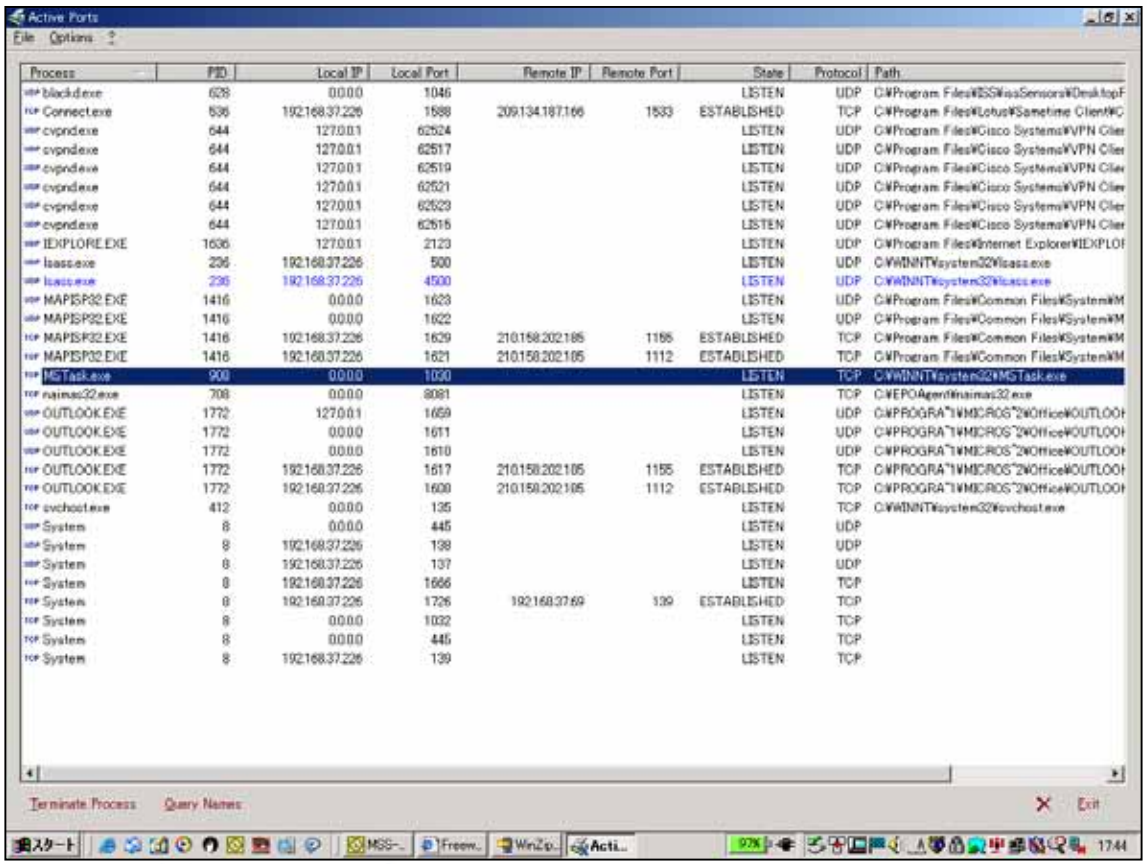
①セキュリティログでの確認
～ホストレベル～



2004年11月20日　0:01
ID592：新規プロセスとして、Msbb.exe
という不明なプロセスが起動されている。

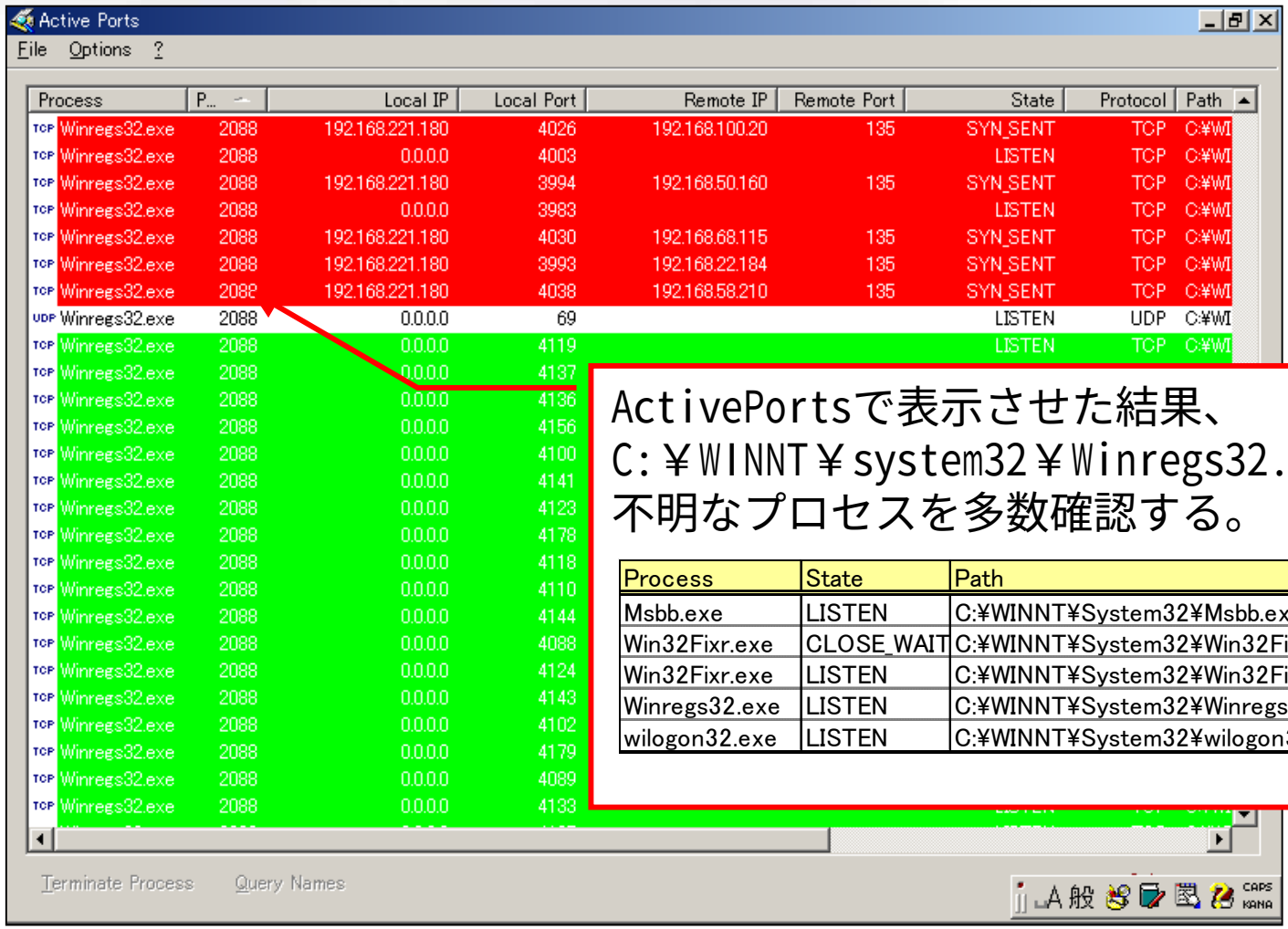
ActivePortsによる解析
～ホストレベル～

- ActivePorts (http://www.protect-me.com/)
  - ポートとプロセス関連付けて表示する



INTERNET SECURITY SYSTEMS®

②ActivePortsでの確認
～ホストレベル～

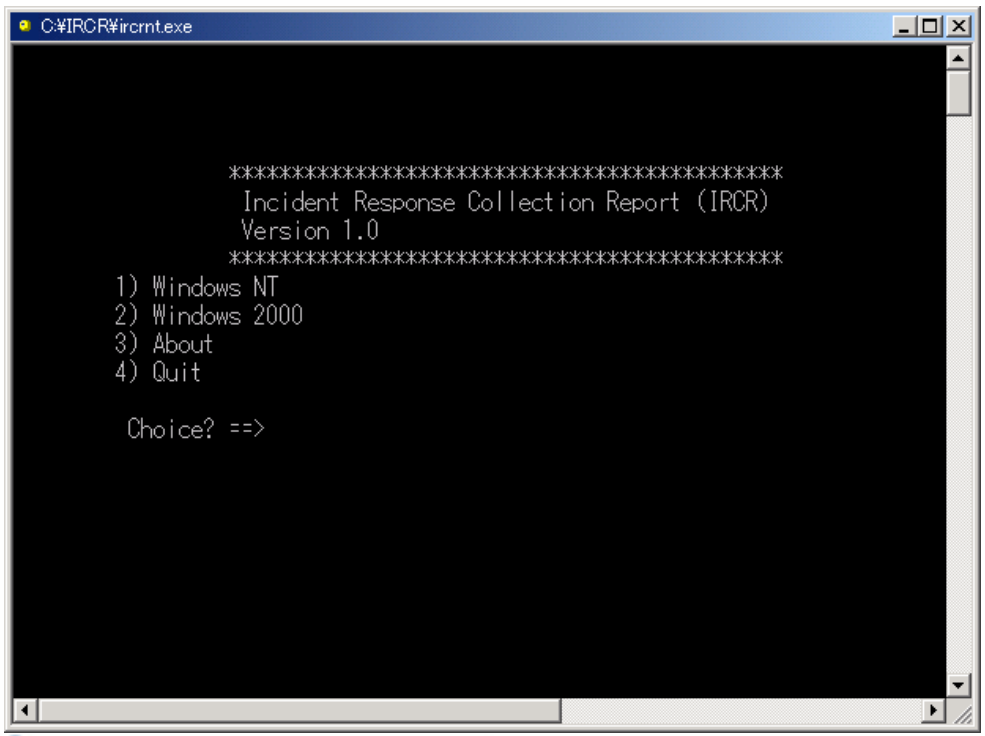


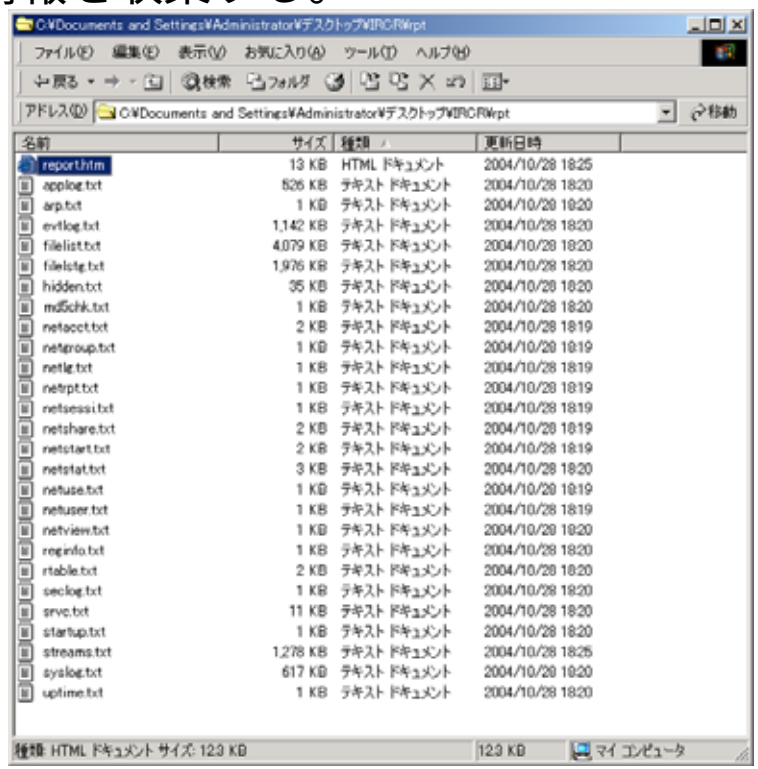
ActivePortsで表示させた結果、
C:￥WINNT￥system32￥Winregs32.exeという
不明なプロセスを多数確認する。

Process	State	Path
Msbb.exe	LISTEN	C:¥WINNT¥System32¥Msbb.exe
Win32Fixr.exe	CLOSE_WAIT	C:¥WINNT¥System32¥Win32Fixr.exe
Win32Fixr.exe	LISTEN	C:¥WINNT¥System32¥Win32Fixr.exe
Winregs32.exe	LISTEN	C:¥WINNT¥System32¥Winregs32.exe
wilogon32.exe	LISTEN	C:¥WINNT¥System32¥wilogon32.exe

②IRCRによる解析
～ホストレベル～

- IRCR(http://www.Incident-reponse.org/IRCR.html)
  - TCT(The Coroner's Toolkit)に類似した機能がある。
  - NETコマンド,ARPテーブルなどの各種情報を収集する。





INTERNET SECURITY SYSTEMS®

②IRCRによる解析
～ホストレベル～

```
TCP    192.168.221.180:3079   192.168.130.231:135    SYN_SENT
TCP    192.168.221.180:3080   192.168.131.105:135    SYN_SENT
TCP    192.168.221.180:3081   192.168.91.100:135     SYN_SENT
TCP    192.168.221.180:3082   192.168.248.26:135     SYN_SENT
TCP    192.168.221.180:3083   192.168.255.35:135     SYN_SENT
TCP    192.168.221.180:3084   192.168.112.178:135    SYN_SENT
TCP    192.168.221.180:3085   192.168.57.236:135     SYN_SENT
TCP    192.168.221.180:3086   218.18.21.232:135      SYN_SENT
TCP    192.168.221.180:3087   218.221.53.234:135     SYN_SENT
TCP    192.168.221.180:3088   192.168.139.85:135     SYN_SENT
TCP    192.168.221.180:3089   218.63.86.146:135      SYN_SENT
TCP    192.168.221.180:3090   192.168.126.37:445     SYN_SENT
TCP    192.168.221.180:3091   192.168.62.73:445      SYN_SENT
TCP    192.168.221.180:3092   192.168.222.141:445    SYN_SENT
TCP    192.168.221.180:3093   192.168.84.67:445      SYN_SENT
TCP    192.168.221.180:3094   192.168.108.118:445    SYN_SENT
TCP    192.168.221.180:3095   192.168.224.10:445     SYN_SENT
TCP    192.168.221.180:3096   192.168.122.46:135     SYN_SENT
TCP    192.168.221.180:3097   192.168.169.113:135    SYN_SENT
```

対象ホストから複数のホストに対して、Port135,445へのアクセスを確認する。

INTERNET SECURITY SYSTEMS®

③Tripwireによる解析 ～ホストレベル～

- Tripwire(http://www.tripwire.co.jp/)
  - ファイルやディレクトリの改竄を検知する

```
Tripwire 整合性チェックレポート バージョン 4.0.0
Tripwire(R) for Servers バージョン 4.5.0.178

レポート生成者：            Administrator
レポート作成日付：          2004年11月20日 08:01:15
データベース最終更新日付：  未更新

================================================================================
レポート要約：
================================================================================

ホスト名：                  ISS001
ホスト IP アドレス：        192.168.221.180
ホスト ID：                 S-1-5-21-1390067357-362288127-839522115
使用ポリシーファイル：      C:¥Program Files¥Tripwire¥TFS¥policy¥tw.pol
使用設定ファイル：          C:¥Program Files¥Tripwire¥TFS¥bin¥tw.cfg
使用データベースファイル：  C:¥Program Files¥Tripwire¥TFS¥db¥database.twd
使用コマンドライン：        tripwire -m c
```

INTERNET SECURITY SYSTEMS®

③Tripwireでの確認
～ホストレベル～

```
  ------------------------------------------------------------------------
  セクション : Windows File System
------------------------------------------------------------------------

  ルール名                          重要度レベル      追加     削除     変更
  ---------                         --------------    -----    -------  --------
* Critical System Startup files     1000              0        0        1
  (C:\)
* OS Support Files                  35                0        0        1
* System32 Folder                   100               15       0        15
* Network Configuration Files       100               0        0        2
  Critical Drivers                  35                0        0        0
  System Folder                     35                0        0        0
  (C:\WINNT\System)
  Program Files Folder              35                0        0        0
  (C:\Program Files)
* Tripwire for Servers Configuration Files
                                    1000              1        0        0
  Tripwire for Servers Executables
                                    1000              0        0        0
  Tripwire for Servers Log and Support Files
                                    1000              0        0        0
  Temporary Files Folder            15                0        0        0

スキャン済みオブジェクト総数 :  6,408
発見された総侵害箇所 :  35
```

System32 Folderの
下に新規に追加された
15個のファイルを確認

③Tripwireでの確認 ～ホストレベル～

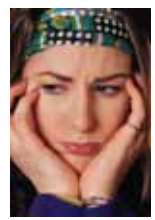
```
  ---------------------------------------------------------------------------
  セクション : Windows Registry
---------------------------------------------------------------------------

  ルール名                          重要度レベル      追加      削除      変更
  ---------                         --------------    -----     -------   -----
  Hardware keys                     35                0         0         0
* Service Registry Keys             100               25        0         10
  Critical Tripwire Registry keys   1000              0         0         0
* Critical Security Account Keys    1000              0         0         1
* Security Information keys         100               0         0         1
  Local Admin Activity              1000              0         0         0
  (HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000001F4)
* Local Admin Login                 1000              0         0         1
  (HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000001F4|F)
  Local Admin Password Change       1000              0         0         0
  (HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000001F4|V)
* Guest Account Activity            1000              0         0         1
  (HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000001F5)
* System Startup Executables        1000              11        0         0
  Critical System Registry Keys     100               0         0         0
  Software keys                     35                0         0         0
  Current User Registry keys        15                0         0         0
  Class keys                        35                0         0         0

スキャン済みオブジェクト総数 :  27,467
発見された総侵害箇所 :  50
```

Service Registry
25個の追加を確認

System Startup
11個の追加を確認

まとめ
～ホストレベル～

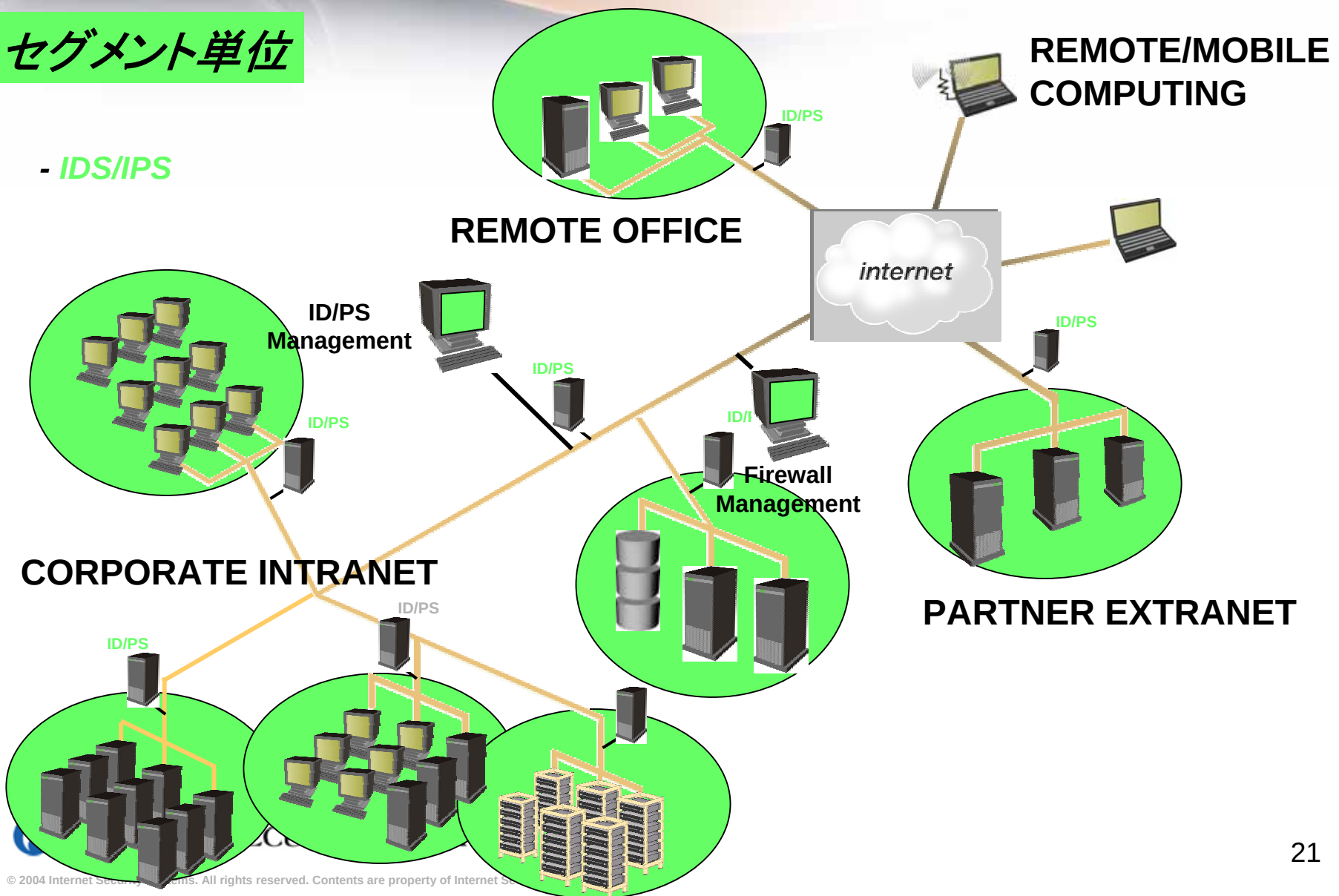
- ホストレベルの場合は、影響が表面化した段階で発見される。
- 攻撃手法がわからない



監視範囲
～セグメントレベル～

セグメント単位

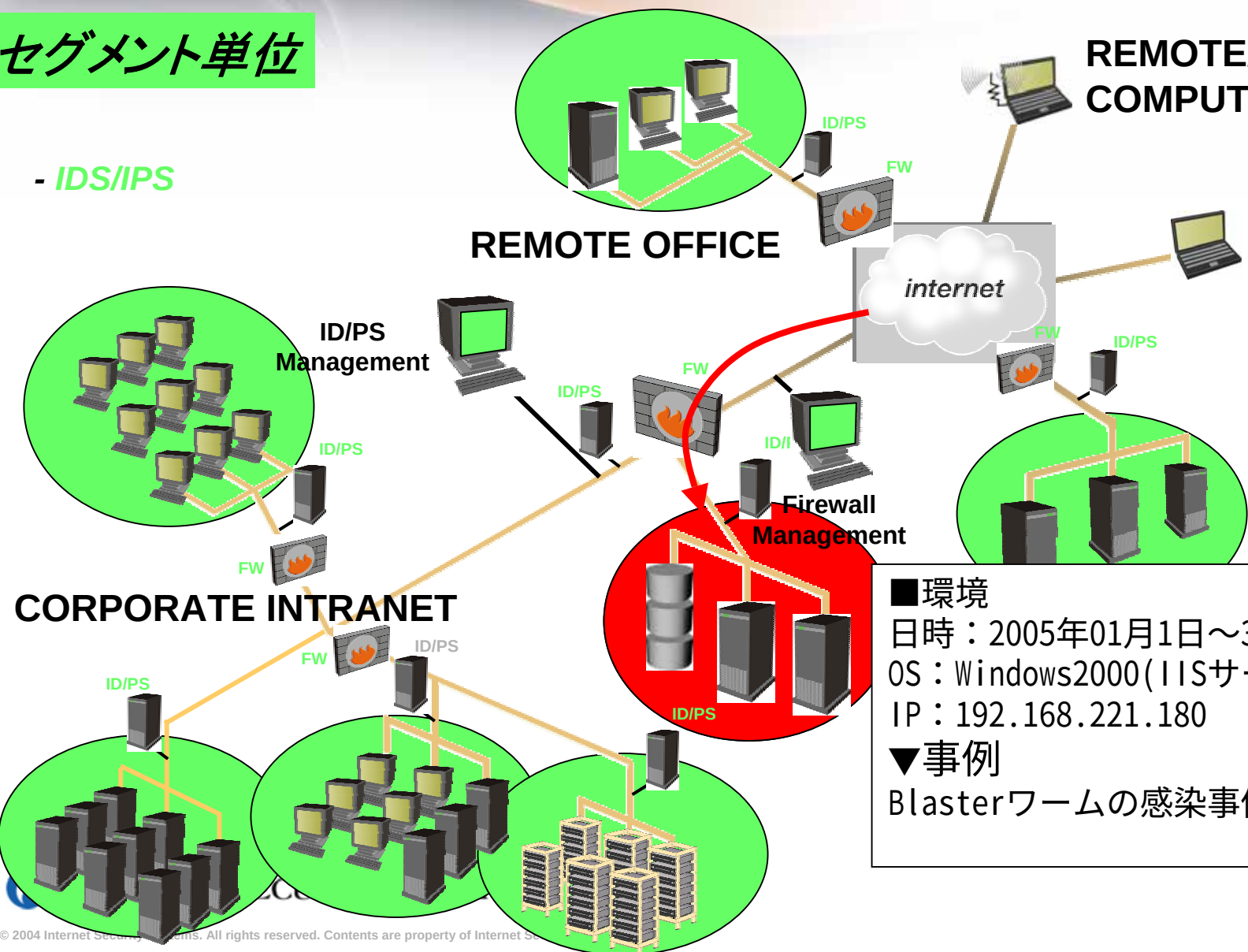
- *IDS/IPS*



発見事例
～セグメントレベル～

セグメント単位

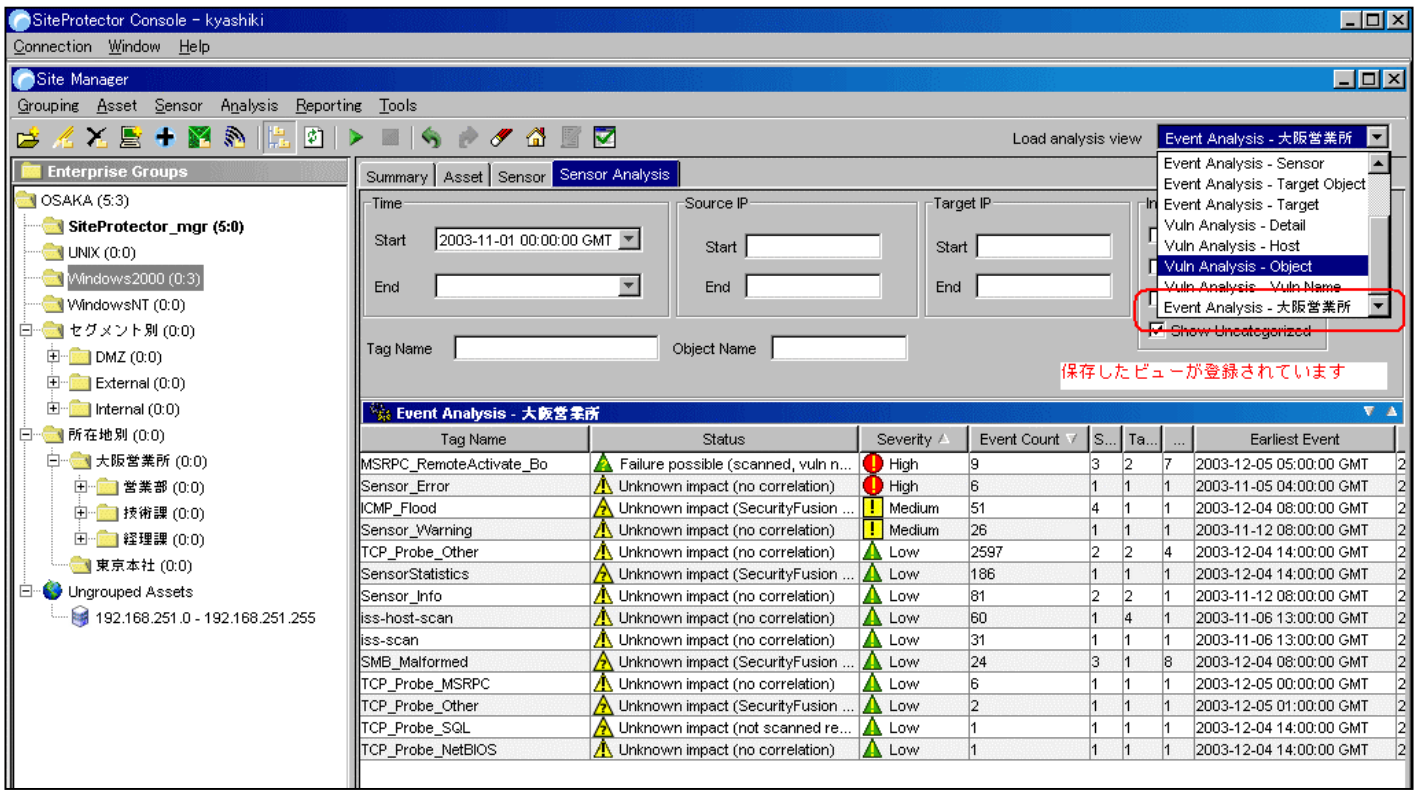
- *IDS/IPS*



■環境
日時：2005年01月1日～3日
OS：Windows2000(IISサーバ)
IP：192.168.221.180
▼事例
Blasterワームの感染事例

IDS/IPS
～セグメントレベル～

- SiteProtector(http://www.isskk.co.jp/product/SiteProtector.html)
  - ネットワーク、サーバ、デスクトップそれぞれに導入されている防御システムの管理を一元化し、セキュリティ管理作業にすばやく優先順位をつけ、危険度が高く、実際に影響があるイベント対応を最優先させることが可能な統合管理ツール



侵入検知システムによる確認
～セグメントレベル～

Summary | Asset | Sensor | Sensor Analysis | Reporting

Event Analysis - Event Name

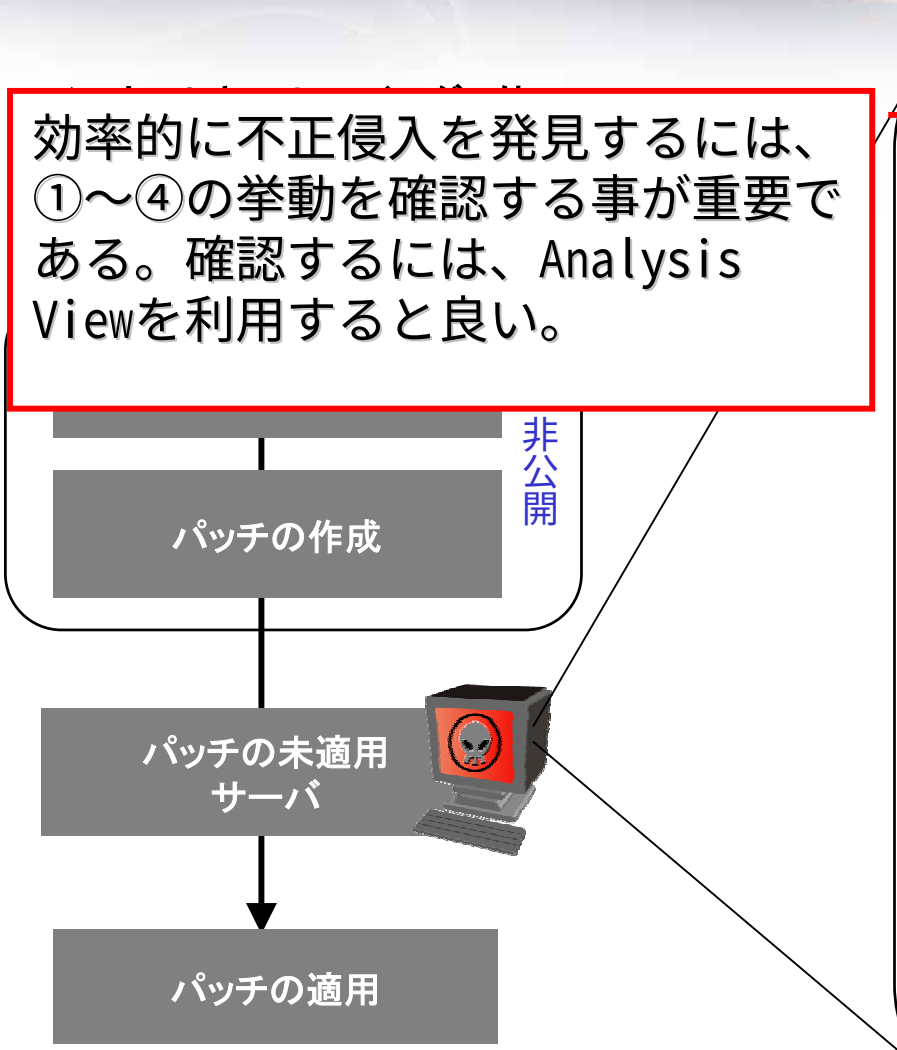
Severity	Tag Name	Event Count	Source Count	Target Count	Object Count	Earliest Event	Latest Event
High	SMB_Empty_Password_Failed	1236	8	3	2	2005-01-02 11:00:00 JST	2005-01-03 11:00:00 JST
High	HTTP_Head	71	4	14	1	2005-01-01 08:00:00 JST	2005-01-03 09:00:00 JST
High	SQL_SSRP_Slammer_Worm	21	18	1	1	2005-01-01 02:00:00 JST	2005-01-03 10:00:00 JST
High	MSRPC_RemoteActivate_Bo	10	6	5	1	2005-01-02 11:00:00 JST	2005-01-03 02:00:00 JST
High	MSRPC_LSASS_Bo	10	5	1	1	2005-01-02 12:00:00 JST	2005-01-03 02:00:00 JST
High	HTTP_WebDAV_Long_Rqst_BO	2	2	1	1	2005-01-02 13:00:00 JST	2005-01-03 10:00:00 JST
High	EventCollector_Error	2	1	1	1	2005-01-02 10:00:00 JST	2005-01-02 10:00:00 JST
High	FTP_Args_Overflow	2	2	2	2	2005-01-01 05:00:00 JST	2005-01-01 05:00:00 JST
High	HTTP_ActiveX	1	1	1	1	2005-01-02 12:00:00 JST	2005-01-02 12:00:00 JST
High	HTTP_Unix_Passwords	1	1	1	1	2005-01-02 11:00:00 JST	2005-01-02 11:00:00 JST
Medium	IM_Activity	104	1	10	3	2005-01-02 11:00:00 JST	2005-01-03 00:00:00 JST
Medium	HTTP_Gator_Installed	68	1	19	1	2005-01-01 00:00:00 JST	2005-01-03 11:00:00 JST
Medium	MSRPC_Domaindump	29	27	1	1	2005-01-01 00:00:00 JST	2005-01-02 07:00:00 JST
Medium	HTTP_URL_Name_Very_Long	10	10	1	1	2005-01-01 13:00:00 JST	2005-01-03 10:00:00 JST
Medium	TFTP_Get	9	1	2	1	2005-01-02 13:00:00 JST	2005-01-03 02:00:00 JST
Medium	Audit_TFTP_Get_Filename	9	1	2			
Medium	HTTP_Connect_Proxy_Bypass_SMTP	3	2	1			
Medium	HTTP_Connect	3	2	1			
Medium	ICMP_Redirect	3	1	1			
Medium	TFTP_Exe_Transfer	1	1	1			
Medium	HTTP_IE_Status_Spoof	1	1	1			
Medium	MSRPC_Share_Dump	1	1	1			
Low	TCP_Probe_MSRPC	105835	42	3			
Low	TCP_Service_Sweep	16552	1	2			
Low	TCP_Probe_Other	3676	87	6			
Low	Windows_Access_Error	1278	16	3			
Low	HTTP_User_Agent	937	4	88	2	2005-01-01 00:00:00 JST	2005-01-03 12:00:00 JST
Low	HTTP_Get	838	3	77	2	2005-01-01 00:00:00 JST	2005-01-03 12:00:00 JST
Low	HTTP_Server_ID	760	15	74	3	2005-01-01 00:00:00 JST	2005-01-03 11:00:00 JST
Low	SensorStatistics_Cumulative	708	1	1	1	2005-01-01 00:00:00 JST	2005-01-03 12:00:00 JST
Low	SensorStatistics	708	1	1	1	2005-01-01 00:00:00 JST	2005-01-03 12:00:00 JST
Low	HTTP_Cookie	668	3	63	1	2005-01-01 00:00:00 JST	2005-01-03 11:00:00 JST

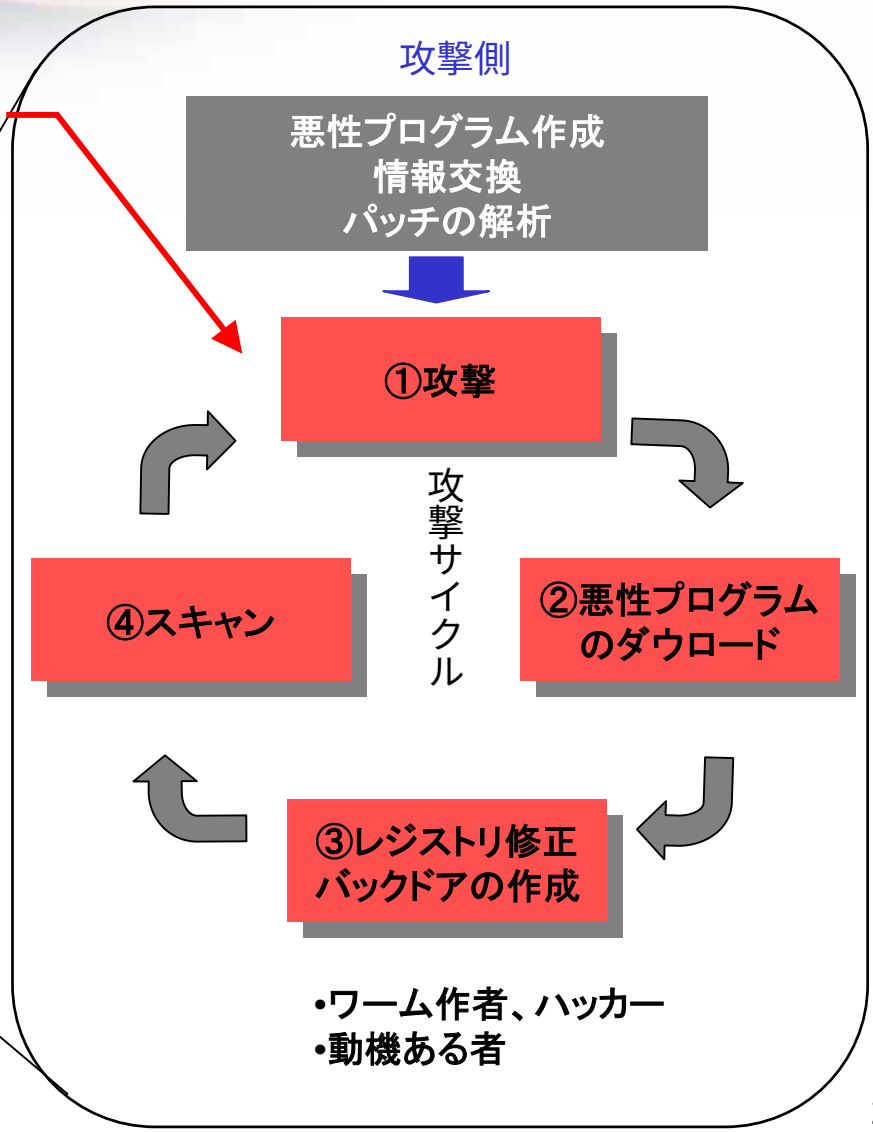
2005年1月1日～3日間の侵入検知システムよる検知状況である。
不正侵入を発見するには、検知件数が多く、判別が困難である。

INTERNET SECURITY SYSTEMS®

不正侵入を発見するポイント
～セグメントレベル～

効率的に不正侵入を発見するには、①～④の挙動を確認する事が重要である。確認するには、Analysis Viewを利用すると良い。



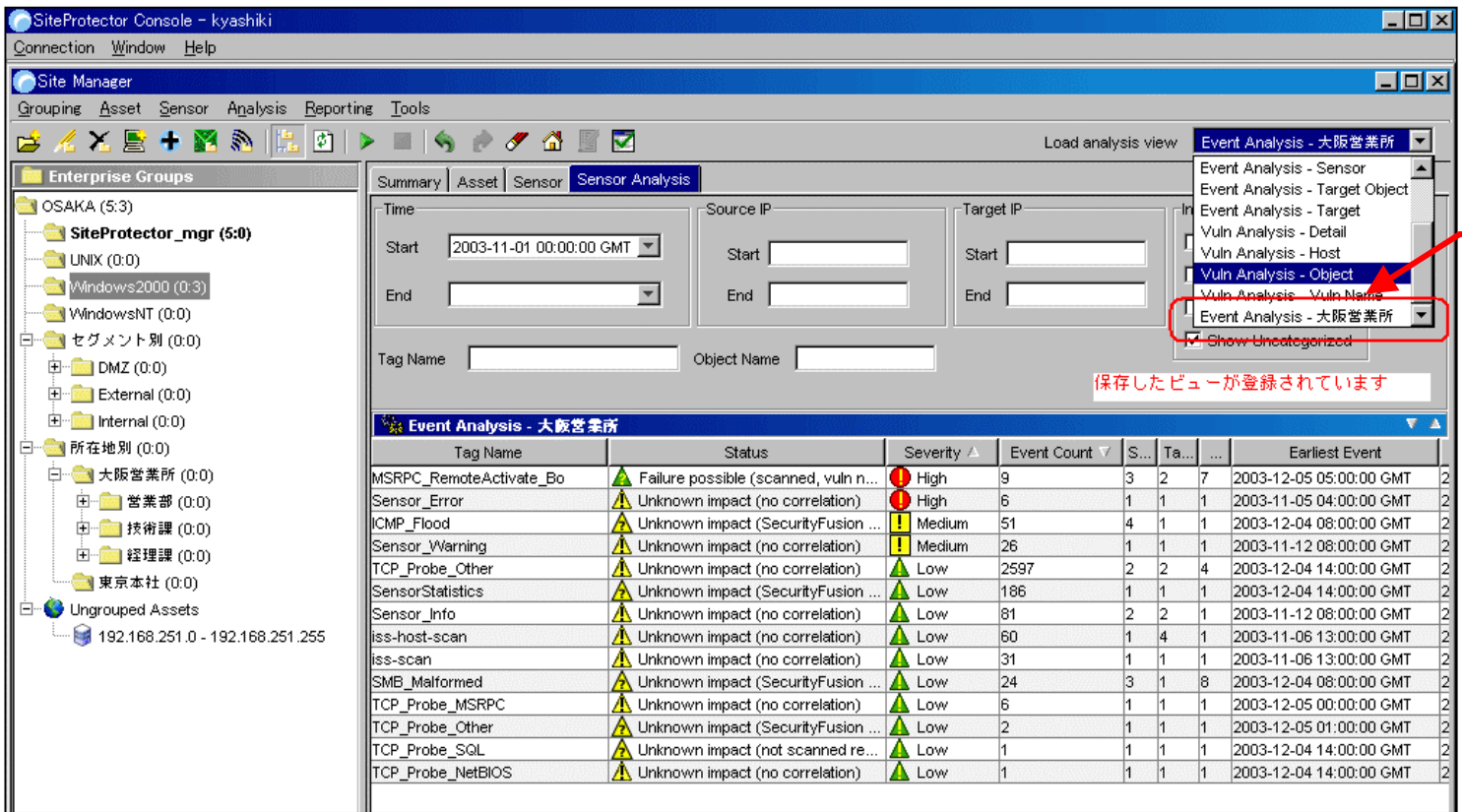


INTERNET | SECURITY | SYSTEMS®

Analysis Viewの活用
～セグメントレベル～

「Advanced Filter」の項目で、フィルタすべき条件項目を指定することをAnalysis Viewという。

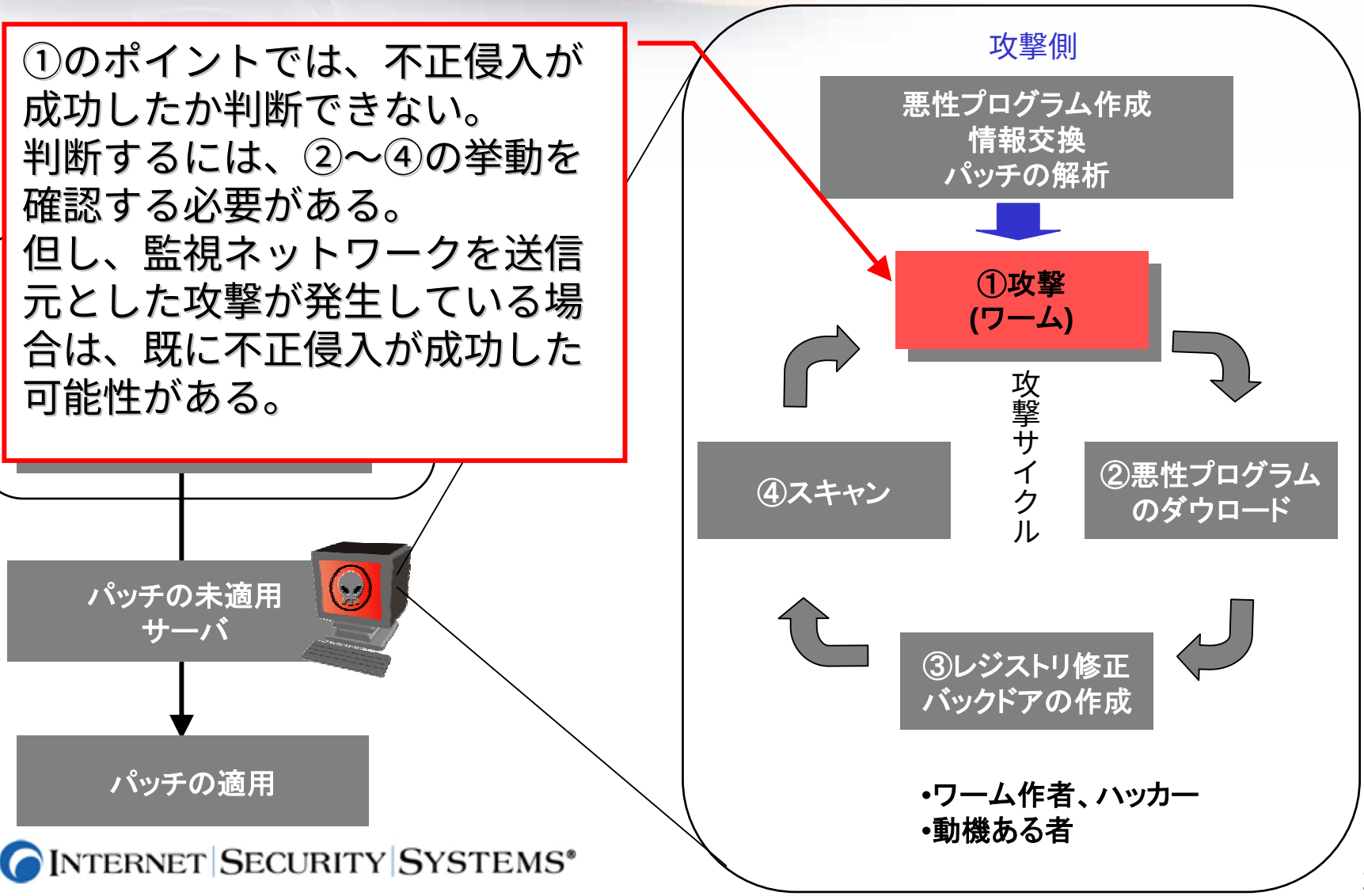
カスタマイズの方法としてはSite Managerのメニューから[Analysis] --> [Add / Remove Data Columns...] を選択します。
表示している項目を更に追加／削除したり、フィルタイリングの条件を指定することができる。



Analysis View

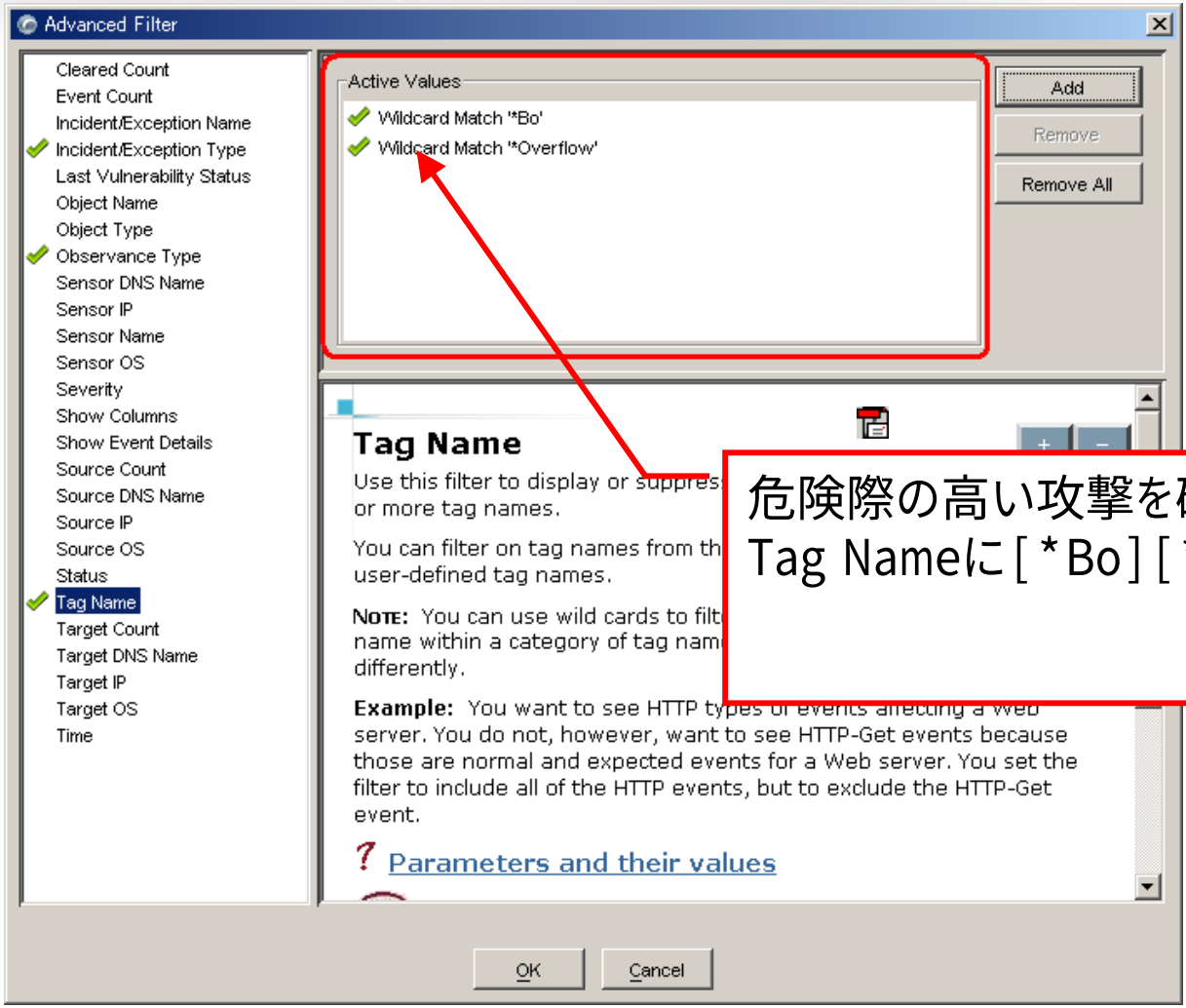
①攻撃(Analysis View)
～セグメントレベル～

①のポイントでは、不正侵入が成功したか判断できない。
判断するには、②～④の挙動を確認する必要がある。
但し、監視ネットワークを送信元とした攻撃が発生している場合は、既に不正侵入が成功した可能性がある。



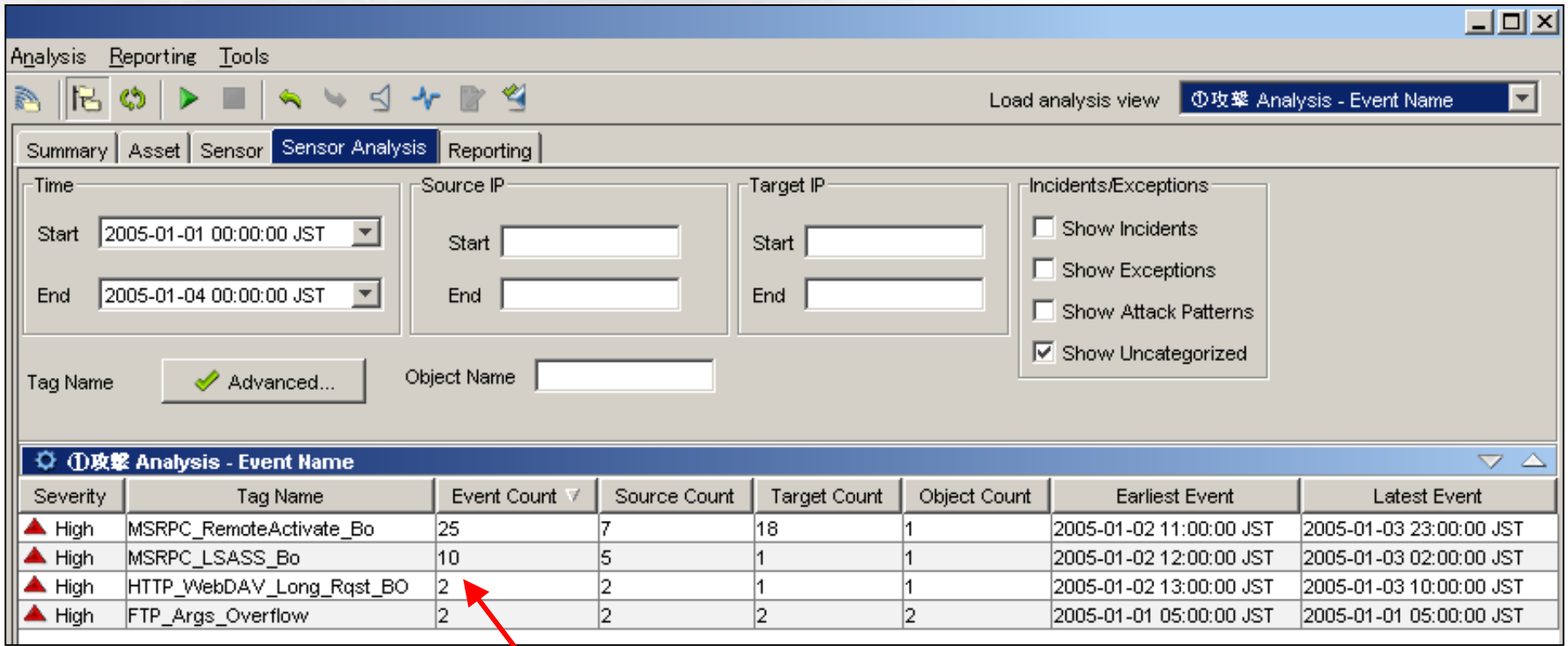
INTERNET | SECURITY | SYSTEMS®

①攻撃(Analysis View)
～セグメントレベル～



危険際の高い攻撃を確認するには、
Tag Nameに[*Bo][*Overflow]を追加する。

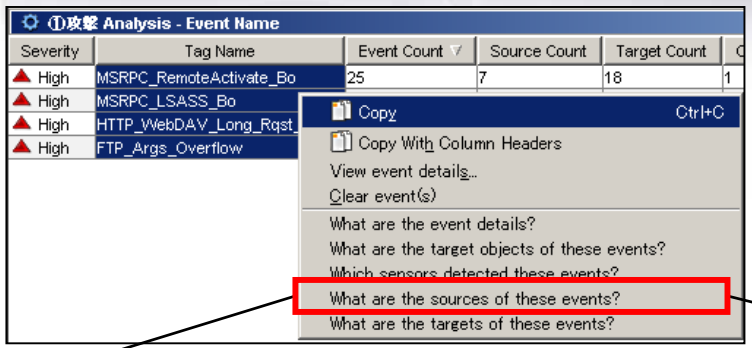
Analysis Viewによる表示
～セグメントレベル～



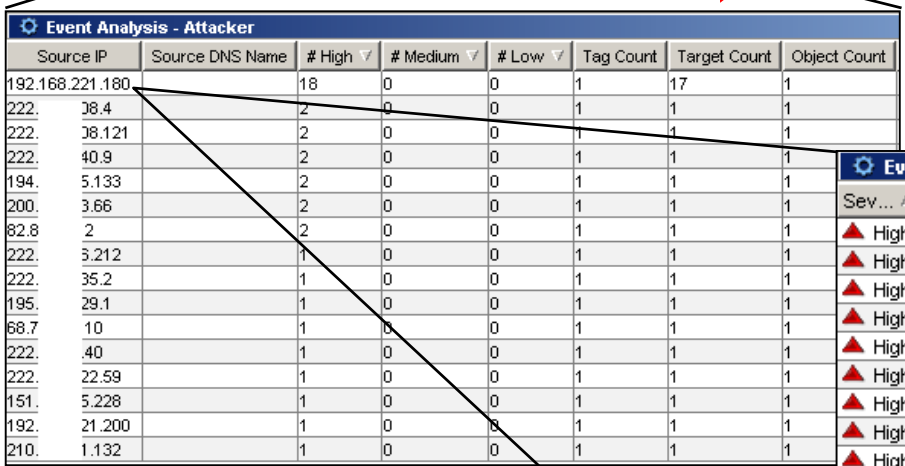
危険性の高い攻撃のみをレポートする事ができる。

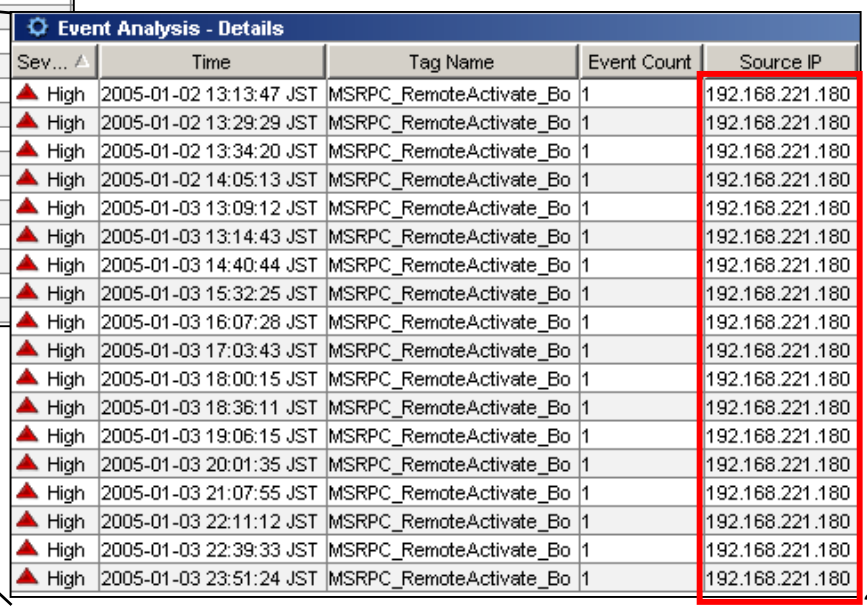
INTERNET SECURITY SYSTEMS®

Analysis Viewによる表示
～セグメントレベル～



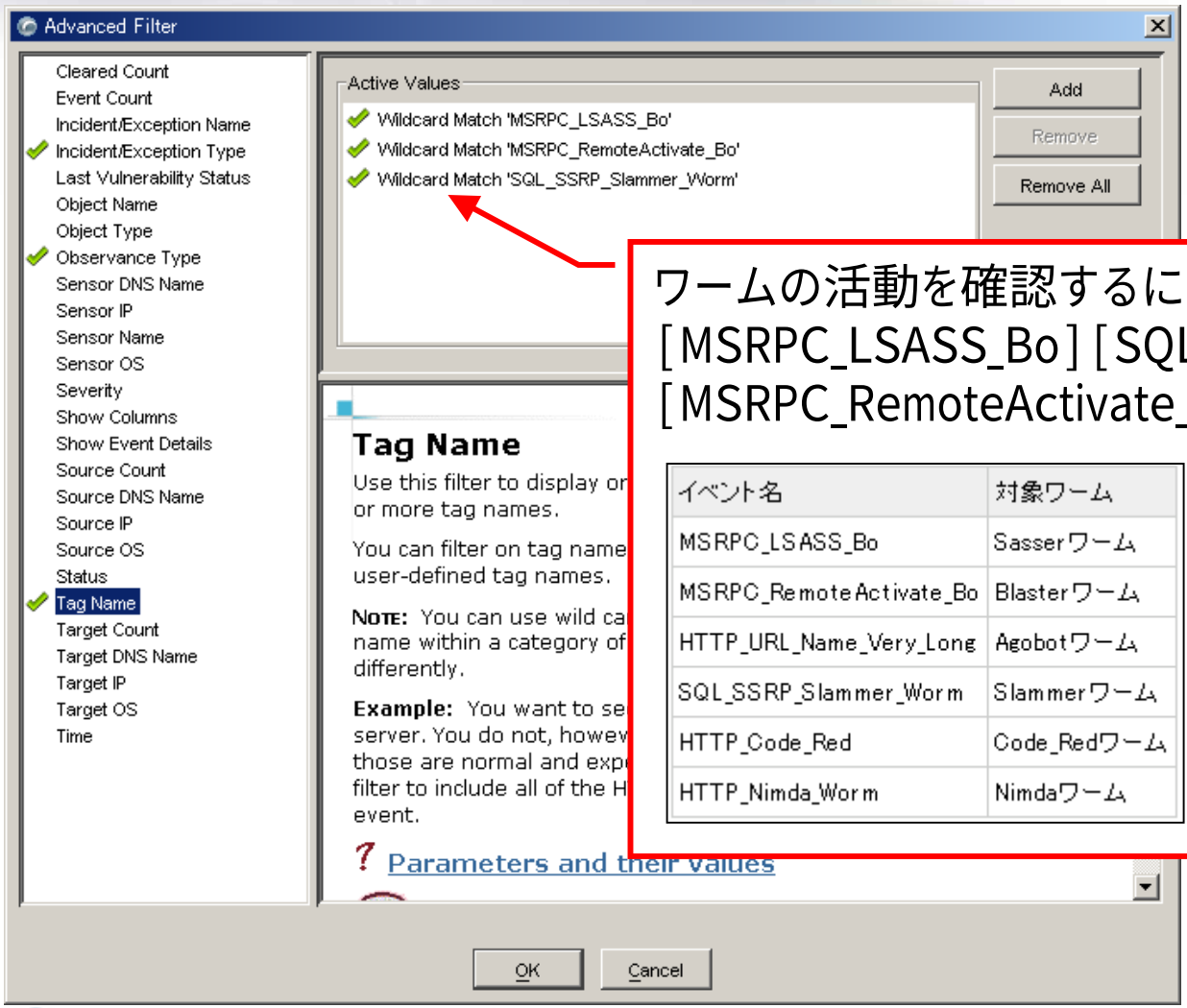
監視セグメントが明確な場合は、
SourceIPの一覧を表示させる。
そして、リストの中に監視セグメントの
IPアドレスが含まれていないか確認を
行う。





INTERNET SECURITY SYSTEMS®

ワーム(Analysis View)
～セグメントレベル～

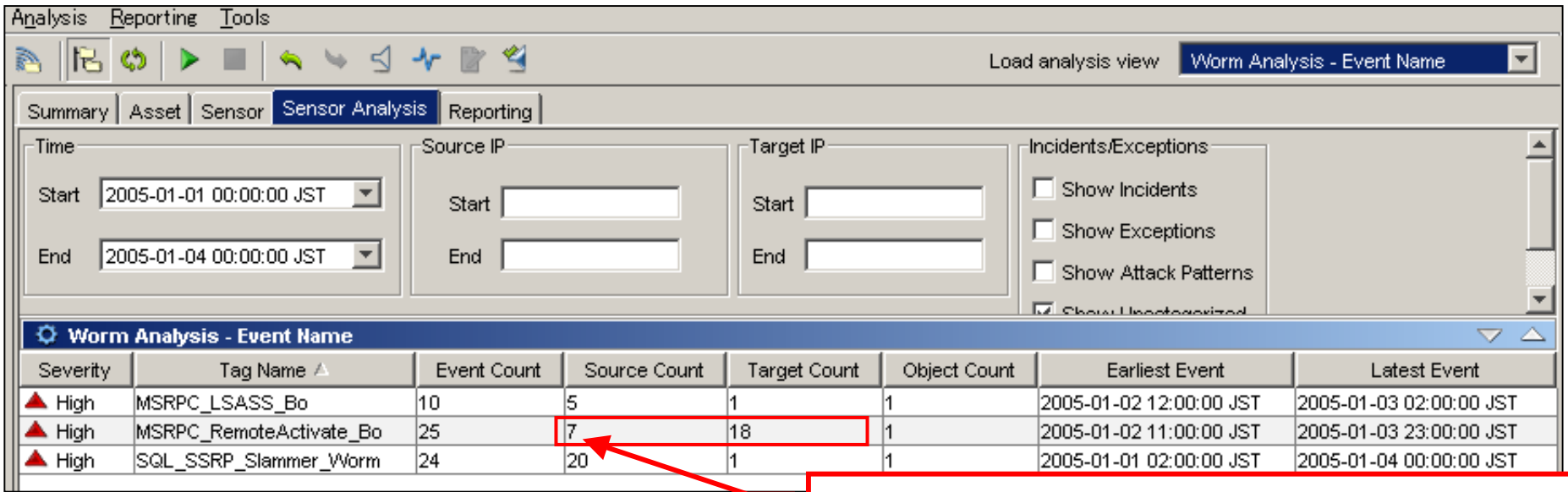


ワームの活動を確認するには、Tag Nameに
[MSRPC_LSASS_Bo] [SQL_SSRP_Slammer_Worm]
[MSRPC_RemoteActivate_Bo]などを追加する。

イベント名	対象ワーム
MSRPC_LSASS_Bo	Sasserワーム
MSRPC_RemoteActivate_Bo	Blasterワーム
HTTP_URL_Name_Very_Long	Agobotワーム
SQL_SSRP_Slammer_Worm	Slammerワーム
HTTP_Code_Red	Code_Redワーム
HTTP_Nimda_Worm	Nimdaワーム

INTERNET SECURITY SYSTEMS®

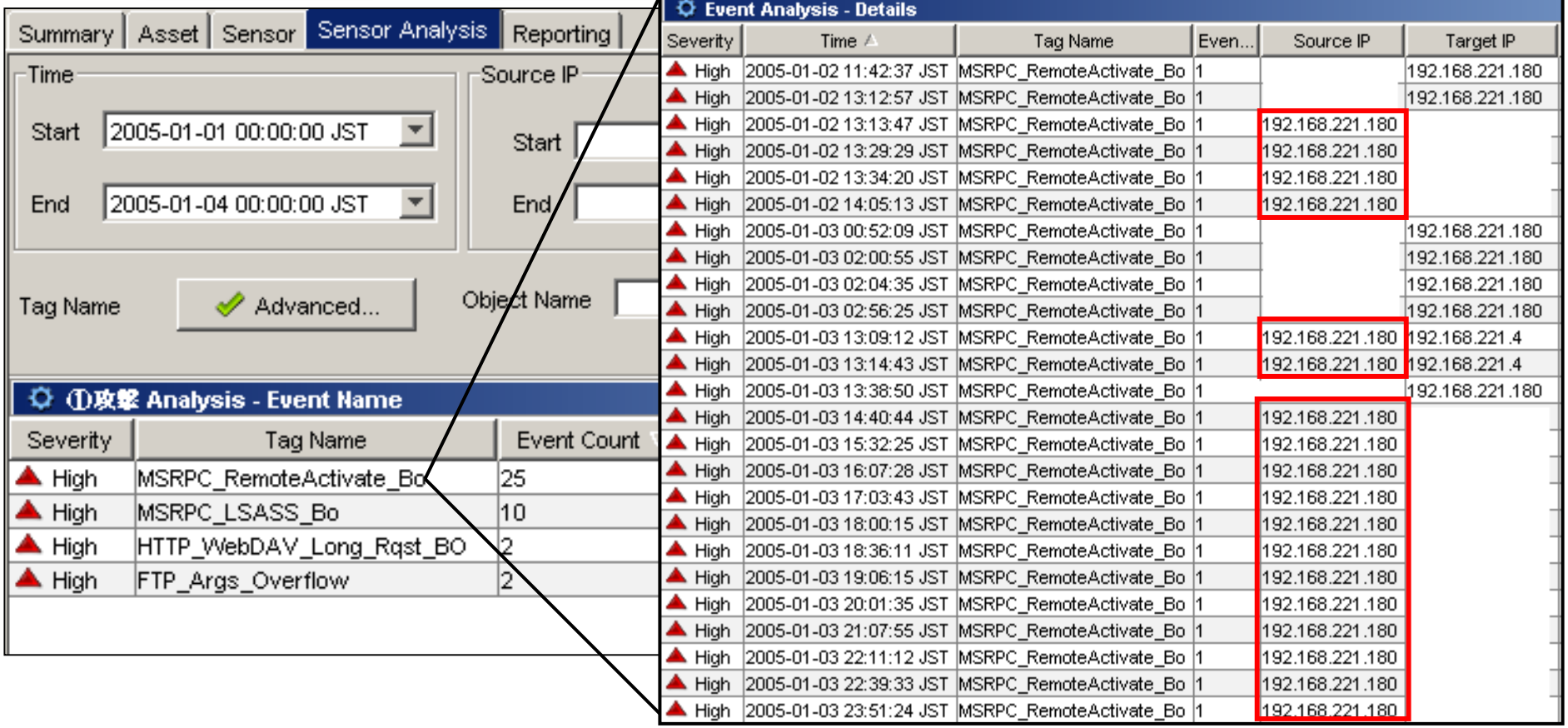
Analysis Viewによる表示
～セグメントレベル～



Source Countより、Target Countの方が多く検知されている場合は、ワームなどに感染した可能性がある。
その為、管理者がホストレベルでの調査を行う必要がある。

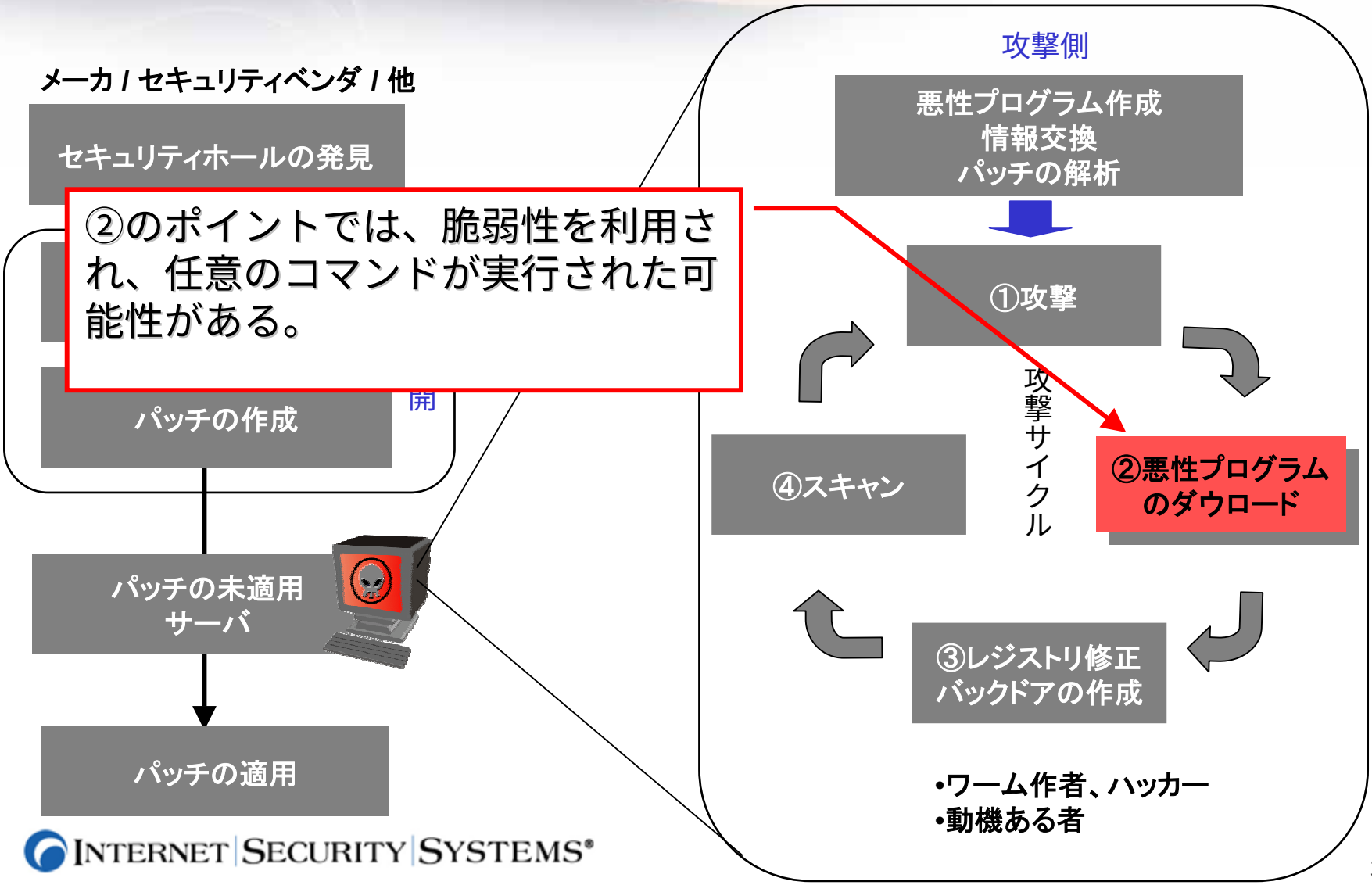
INTERNET SECURITY SYSTEMS®

Analysis Viewによる表示
～セグメントレベル～



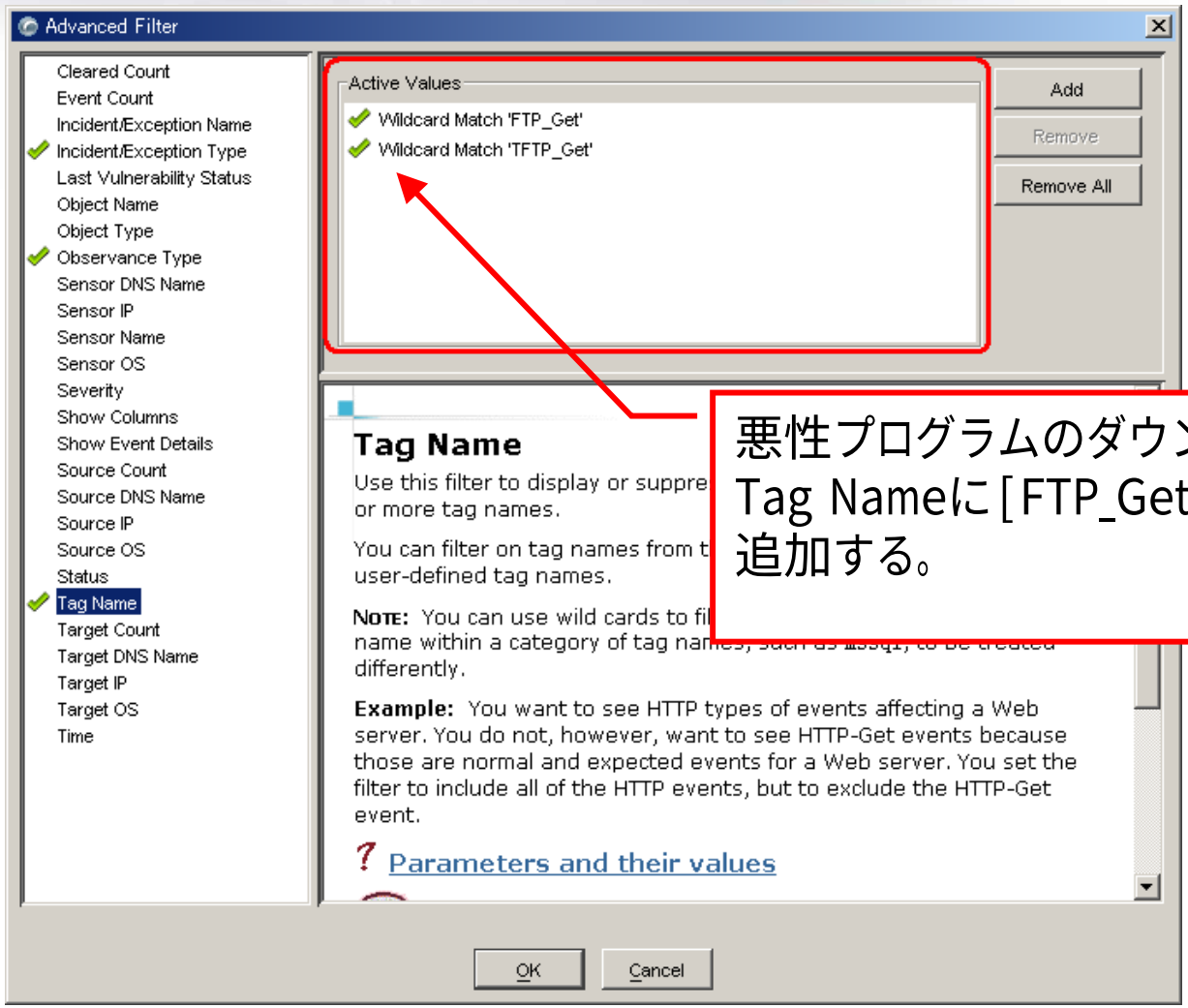
INTERNET SECURITY SYSTEMS®

不正侵入を発見するポイント
～セグメントレベル～



INTERNET | SECURITY | SYSTEMS®

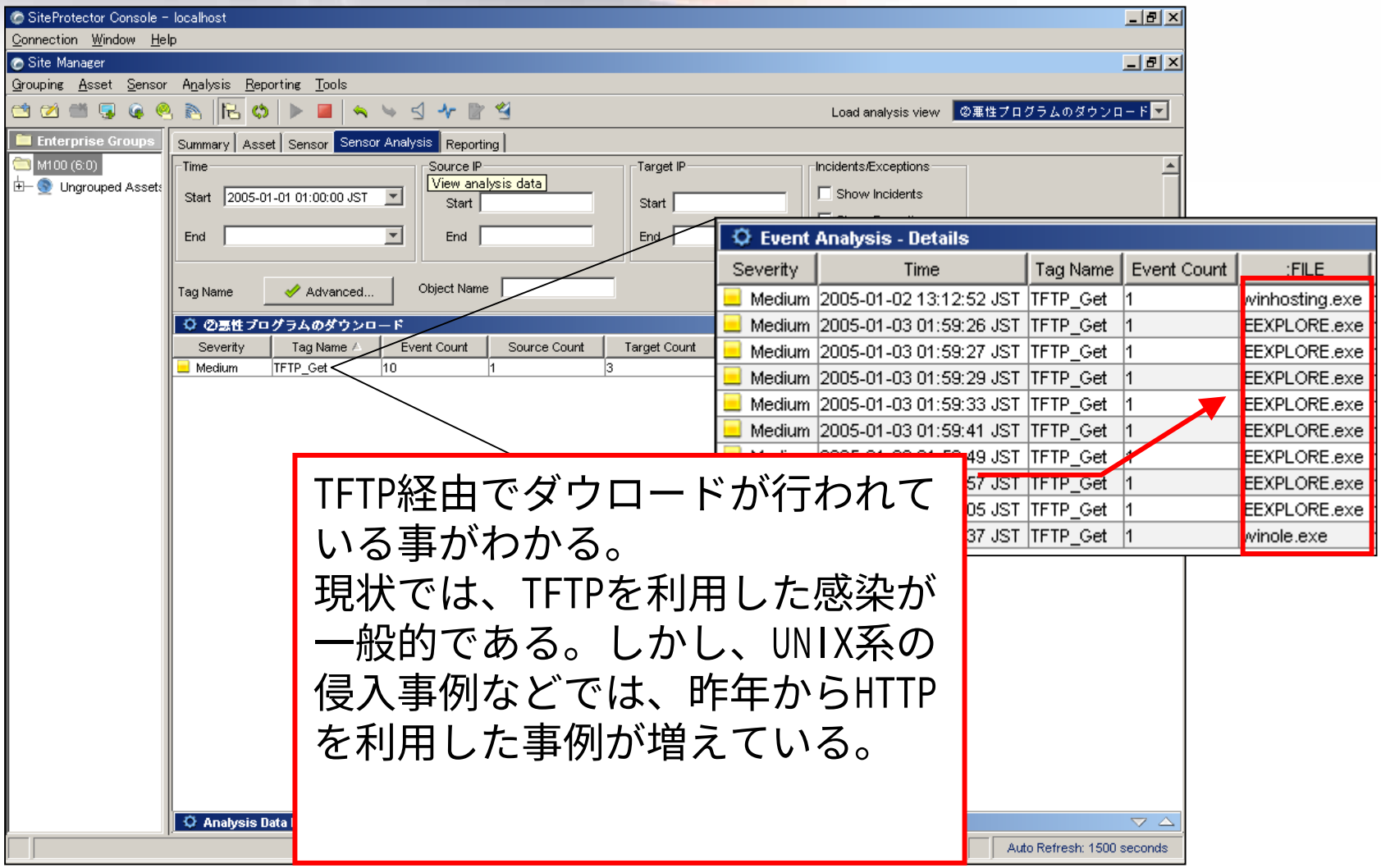
②ダウロード(Analysis View)
～セグメントレベル～



悪性プログラムのダウンロードを確認するには、
Tag Nameに[FTP_Get][TFTP_Get]などを
追加する。

INTERNET SECURITY SYSTEMS®

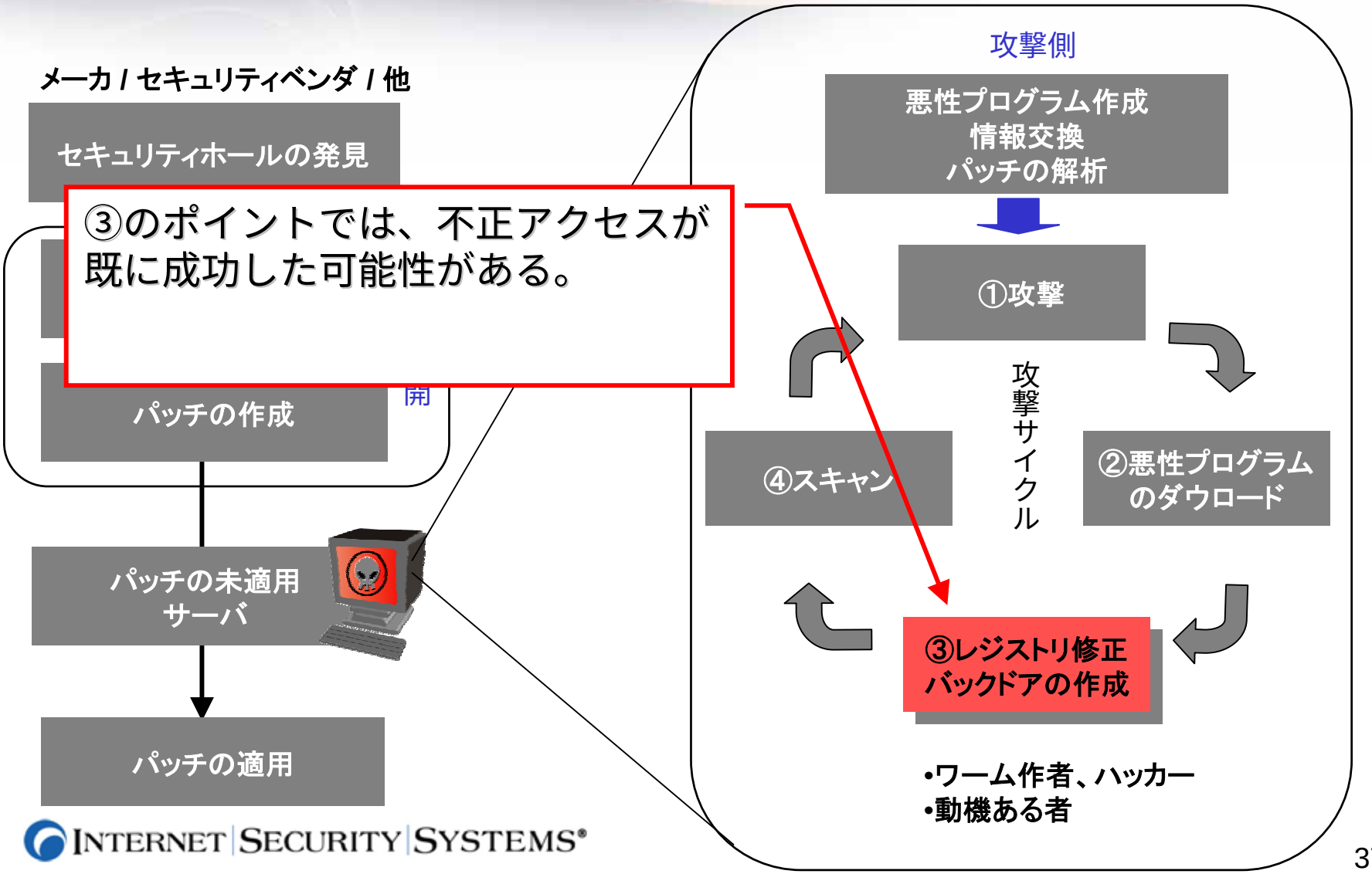
Analysis Viewによる表示
～セグメントレベル～



TFTP経由でダウロードが行われている事がわかる。
現状では、TFTPを利用した感染が一般的である。しかし、UNIX系の侵入事例などでは、昨年からHTTPを利用した事例が増えている。

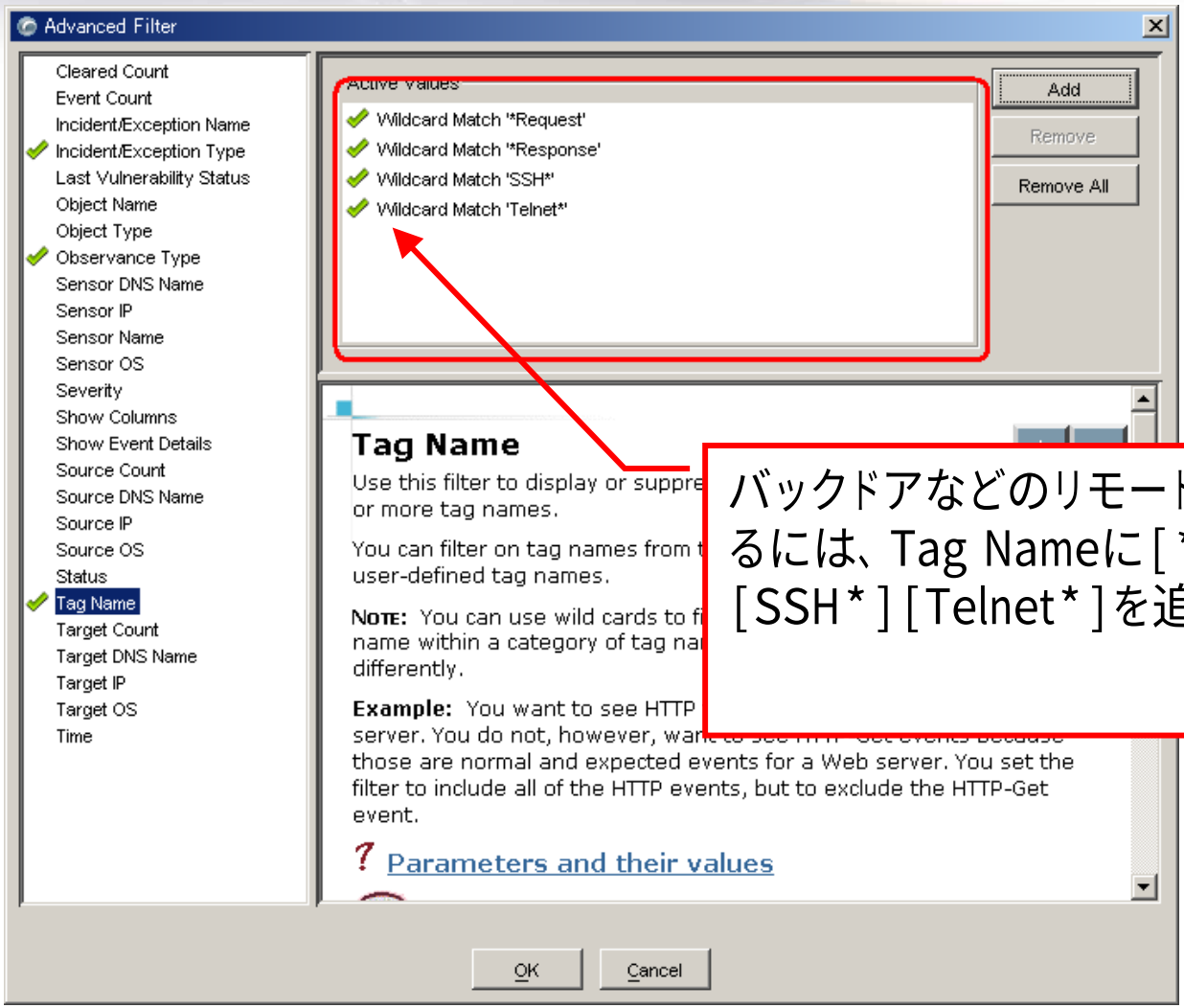
INTERNET SECURITY SYSTEMS®

不正侵入を発見するポイント
～セグメントレベル～



INTERNET | SECURITY | SYSTEMS®

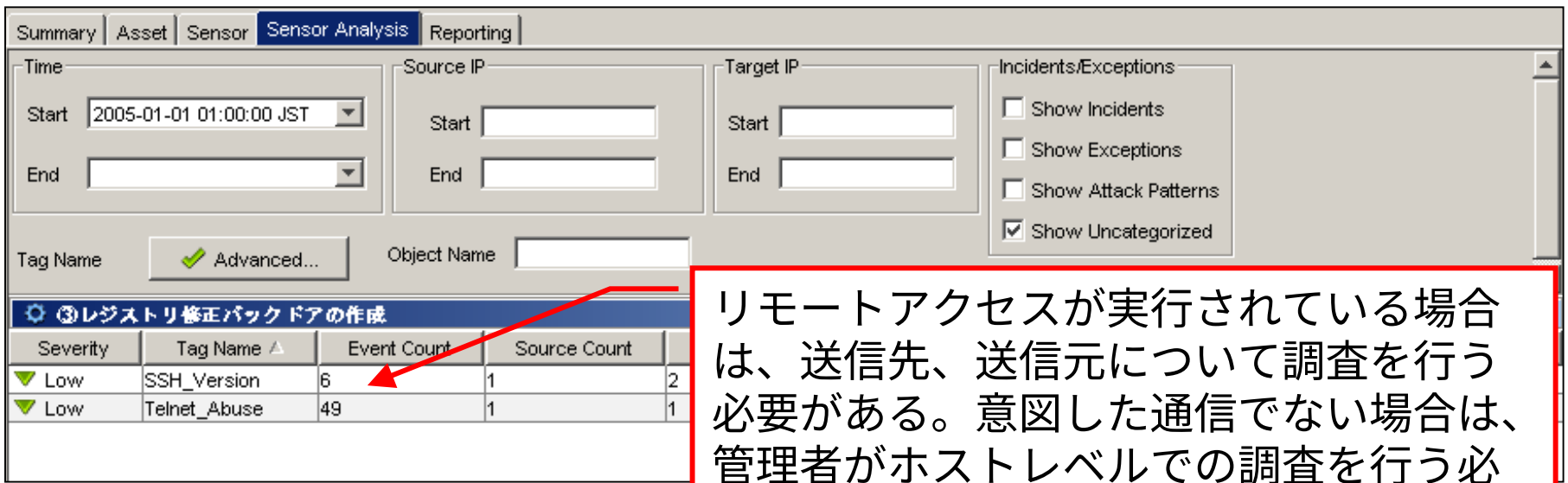
③バックドア(Analysis View)
～セグメントレベル～



バックドアなどのリモートからのアクセスを確認するには、Tag Nameに[*Request][*Response][SSH*][Telnet*]を追加する。

INTERNET SECURITY SYSTEMS®

③バックドア(Analysis View)
～セグメントレベル～



リモートアクセスが実行されている場合は、送信先、送信元について調査を行う必要がある。意図した通信でない場合は、管理者がホストレベルでの調査を行う必要がある。但し、一般的に管理者がすべての通信を把握している事は稀である為、発見は難しい。

不正侵入を発見するポイント
～セグメントレベル～

メーカ / セキュリティベンダ / 他

セキュリティホールの発見

④のポイントでは、被害者から加害者になる。ネットワーク回線が重いなど、影響が表面化する。

パッチの未適用サーバ

パッチの適用

攻撃側

悪性プログラム作成
情報交換
パッチの解析

①攻撃

②悪性プログラムのダウロード

③レジストリ修正
バックドアの作成

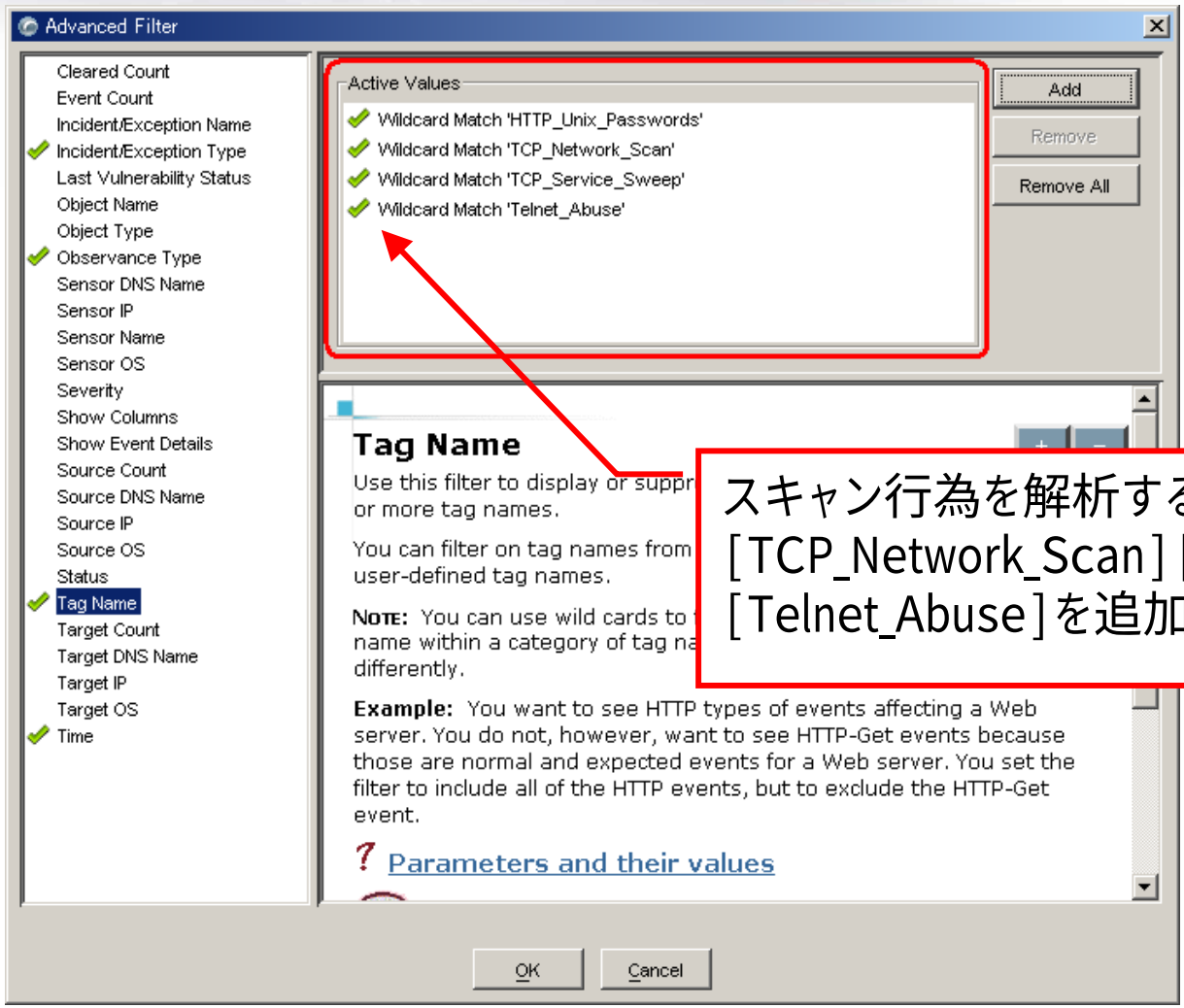
④スキャン

攻撃サイクル

•ワーム作者、ハッカー
•動機ある者

INTERNET | SECURITY | SYSTEMS®

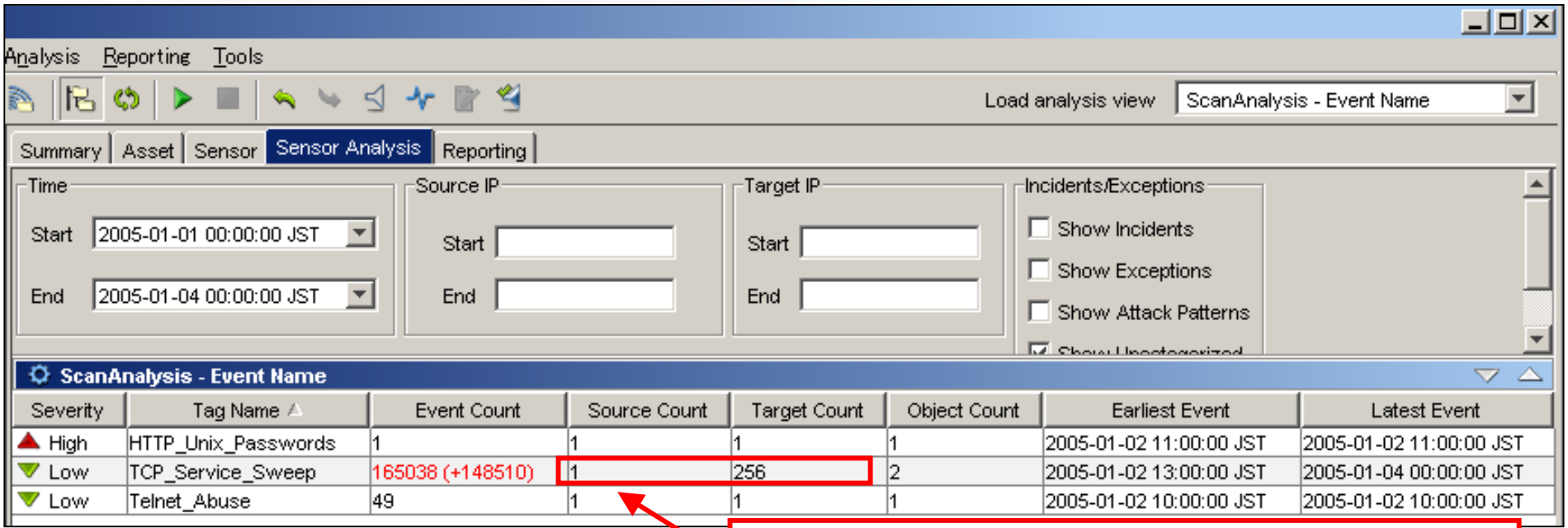
④スキャン(Analysis View)
～セグメントレベル～



スキャン行為を解析するには、Tag Nameに
[TCP_Network_Scan] [TCP_Service_Sweep]
[Telnet_Abuse]を追加する。

INTERNET SECURITY SYSTEMS®

④スキャン(Analysis View)
～セグメントレベル～



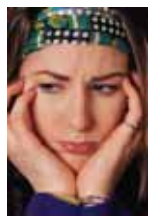
Severity	Tag Name	Event Count	Source Count	Target Count	Object Count	Earliest Event	Latest Event
High	HTTP_Unix_Passwords	1	1	1	1	2005-01-02 11:00:00 JST	2005-01-02 11:00:00 JST
Low	TCP_Service_Sweep	165038 (+148510)	1	256	2	2005-01-02 13:00:00 JST	2005-01-04 00:00:00 JST
Low	Telnet_Abuse	49	1	1	1	2005-01-02 10:00:00 JST	2005-01-02 10:00:00 JST

Source Countより、Target Countの方が多く検知されている場合は、送信元ホストでワームなどに感染した可能性がある。その為、管理者がホストレベルでの調査を行う必要がある。スキャンは、検知件数にピークが発生する為、安易に発見できる。

INTERNET SECURITY SYSTEMS®

疑問
～セグメントレベル～

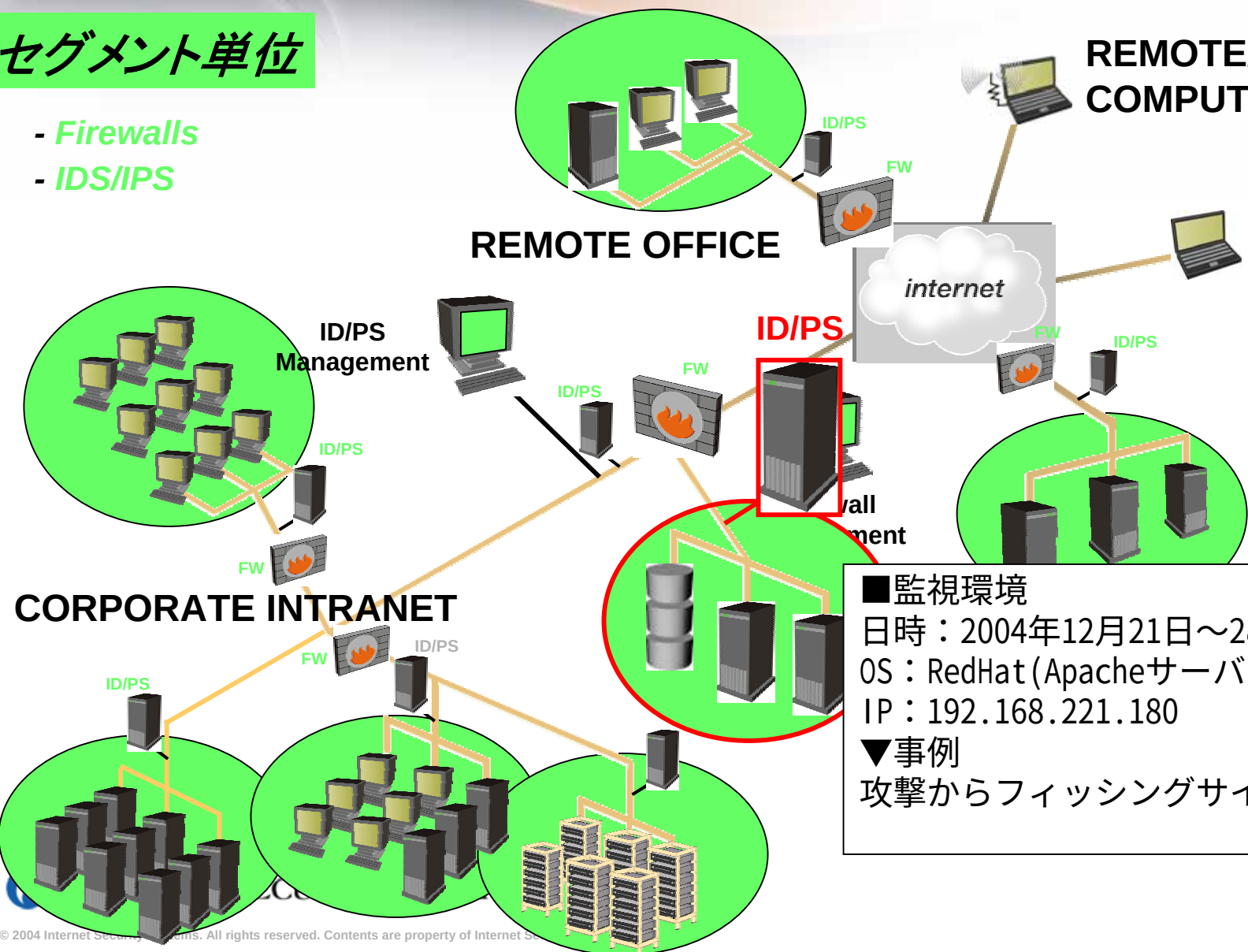
- UNIXの場合はどうなの？
- ワーム以外の攻撃は？



Case Study1
～セグメントレベル～

セグメント単位

- *Firewalls*
- *IDS/IPS*



■監視環境
日時：2004年12月21日～28日
OS：RedHat(Apacheサーバ)
IP：192.168.221.180
▼事例
攻撃からフィッシングサイト構築まで

Case Study1
～セグメントレベル～

Summary | Asset | Sensor | Sensor Analysis | Reporting

Event Analysis - Event Name

Tag Name	Status	Severity	Event Count	Source Count	Target Count	Object Count
SQL_SSRP_Slammer_Worm	Unknown impact (SecurityFusion not enabled)	High	48	35	1	1
Ident_Error	Unknown impact (SecurityFusion not enabled)	High	39	24	1	1
HTTP_Head	Unknown impact (SecurityFusion not enabled)	High	36	2	10	1
SMB_Admin_Sneak	Unknown impact (SecurityFusion not enabled)	High	7	3	1	1
FTP_Glob_TildeBrace_Vulns	Unknown impact (SecurityFusion not enabled)	High	6	2	2	4
HTTP_WebDAV_Long_Rqst_BO	Unknown impact (SecurityFusion not enabled)	High	3	3	1	1
FTP_Generic_Intel_Overflow	Unknown impact (SecurityFusion not enabled)	High	3	1	1	1
FTP_Cwd_Overflow	Unknown impact (SecurityFusion not enabled)	High	3	1	1	1
HTTP_ActiveX	Unknown impact (SecurityFusion not enabled)	High	2	2	2	1
DNS_Windows_SMTP_Overflow	Unknown impact (SecurityFusion not enabled)	High	1	1	1	1
DNS_Query_All	Unknown impact (SecurityFusion not enabled)	Medium	46380	1	2	1
ICMP_Redirect	Unknown impact (SecurityFusion not enabled)	Medium	15721	1	1	1
HTTP_Gator_Installed	Unknown impact (SecurityFusion not enabled)	Medium	392	1	36	1
ICMP_Flood	Unknown impact (SecurityFusion not enabled)	Medium	134	1	1	1
HTTP_URL_Name_Very_Long	Unknown impact (SecurityFusion not enabled)	Medium	25	25	1	1
MSRPC_Domaindump	Unknown impact (SecurityFusion not enabled)	Medium	17	16	1	1
FTP_Pass	Unknown impact (SecurityFusion not enabled)	Medium	13	2	5	1
FTP_Pasv	Unknown impact (SecurityFusion not enabled)	Medium	11	1	3	1
TCP_Port_Scan	Unknown impact (SecurityFusion not enabled)	Medium	7	3	1	1
HTTP_Connect_Proxy_Bypass_SMTP	Unknown impact (SecurityFusion not enabled)	Medium	4	2	1	1
HTTP_Connect	Unknown impact (SecurityFusion not enabled)	Medium	4	2	1	
Email_Relay_Spam	Unknown impact (SecurityFusion not enabled)	Medium	3	1	1	
FTP_dotdotdot	Unknown impact (SecurityFusion not enabled)	Medium	2	2	2	
Email_ServerID	Unknown impact (SecurityFusion not enabled)	Low	24255	2272	4	
Email_Ehlo	Unknown impact (SecurityFusion not enabled)	Low	23163	2	22	
Email_From	Unknown impact (SecurityFusion not enabled)	Low	23012	3	22	
Email_To	Unknown impact (SecurityFusion not enabled)	Low	19998	3	17	
Email_Data	Unknown impact (SecurityFusion not enabled)	Low	13559	1	10	
Email_Subject	Unknown impact (SecurityFusion not enabled)	Low	13555	1	10	
TCP_Probe_SMTP	Unknown impact (SecurityFusion not enabled)	Low	4933	1	24	
HTTP_Server_ID	Unknown impact (SecurityFusion not enabled)	Low	2315	41	12	
HTTP_User_Agent	Unknown impact (SecurityFusion not enabled)	Low	2304	13	13	
HTTP_Get	Unknown impact (SecurityFusion not enabled)	Low	2173	14	112	1
SensorStatistics_Cumulative	Unknown impact (SecurityFusion not enabled)	Low	1959	1	1	1

2004年12月21日～28日の侵入検知システムによる検知状況である。

INTERNET SECURITY SYSTEMS®

Case Study1(時系列１)
～セグメントレベル～

Summary | Asset | Sensor | Sensor Analysis | Reporting

Event Analysis - Details

Severity	Time	Tag Name	Event Count	Source IP	Target IP	Sensor DNS Name	Object Type	Object Name
Low	2004-12-23 00:06:06 JST	TCP_Probe_Other	2	220 .231	192.168.221.180		Target Port	4899
Low	2004-12-23 00:11:43 JST	FTP_User	1	203. .114	192.168.221.180		Target Port	21
Medium	2004-12-23 00:11:43 JST	FTP_Pass	1	203. .114	192.168.221.180			
Low	2004-12-23 00:11:43 JST	FTP_Server_Identity	1	203. .114	192.168.221.180			
Low	2004-12-23 00:11:43 JST	FTP_Server_Identity	1	203. .114	192.168.221.180			
Low	2004-12-23 00:11:53 JST	FTP_Commands_With_Binary	1	203. .114	192.168.221.180			
High	2004-12-23 00:11:53 JST	FTP_Generic_Intel_Overflow	1	203. .114	192.168.221.180			
High	2004-12-23 00:11:53 JST	FTP_Cwd_Overflow	1	203. .114	192.168.221.180			
High	2004-12-23 00:13:23 JST	FTP_Glob_TildeBrace_Vulns	1	203. .114	192.168.221.180		Target Port	21
Low	2004-12-23 00:14:16 JST	FTP_Server_Identity	1	192.168.221.180	193. .143		Target Port	21
Low	2004-12-23 00:14:24 JST	FTP_User	1	192.168.221.180	193. .143			
Medium	2004-12-23 00:14:28 JST	FTP_Pass	1	192.168.221.180	193. .143			
Low	2004-12-23 00:14:28 JST	FTP_Syst	1	192.168.221.180	193. .143			
Medium	2004-12-23 00:14:32 JST	FTP_Pasv	1	192.168.221.180	193. .143			
Low	2004-12-23 00:14:33 JST	FTP_Filename	1	192.168.221.180	193. .143			
Low	2004-12-23 00:14:33 JST	FTP_Get	1	192.168.221.180	193. .143			
Low	2004-12-23 00:15:04 JST	TCP_Probe_Other	1	222. .61	192.168.221.180			
Low	2004-12-23 00:15:04 JST	TCP_Probe_NetBIOS	1	222. .61	192.168.221.180		Target Port	139
Low	2004-12-23 00:15:04 JST	TCP_Probe_SQL	1	222. .61	192.168.221.180		Target Port	1433
Low	2004-12-23 00:15:05 JST	HTTP_Server_ID	1	222. .61	192.168.221.180		Target Port	80
Low	2004-12-23 00:16:08 JST	TCP_Probe_SQL	2	222. .61	192.168.221.180		Target Port	1433
Low	2004-12-23 00:16:08 JST	TCP_Probe_NetBIOS	2	222. .61	192.168.221.180		Target Port	139
Low	2004-12-23 00:16:08 JST	TCP_Probe_Other	11	222. .61	192.168.221.180		Target Port	1025
Medium	2004-12-23 00:16:08 JST	HTTP_URL_Name_Very_Long	1	222. .61	192.168.221.180		Target Port	80
Medium	2004-12-23 00:16:24 JST	FTP_dotdotdot	1	203. .114	192.168.221.180		Target Port	21
Low	2004-12-23 00:16:42 JST	UDP_Probe_Other	1	222. 32	192.168.221.180		Target Port	1434
Low	2004-12-23 00:17:33 JST	TCP_Probe_Ftp	1	192.168.221.180	206. .88		Target Port	21
High	2004-12-23 00:18:03 JST	SQL_SSRP_Slammer_Worm	1	222. 2	192.168.221.180		Target Port	1434
High	2004-12-23 00:20:39 JST	FTP_Glob_TildeBrace_Vulns	1	192.168.221.180	203 .114		Target Port	3817
Medium	2004-12-23 00:20:39 JST	FTP_dotdotdot	1	192.168.221.180	203 .114		Target Port	3817

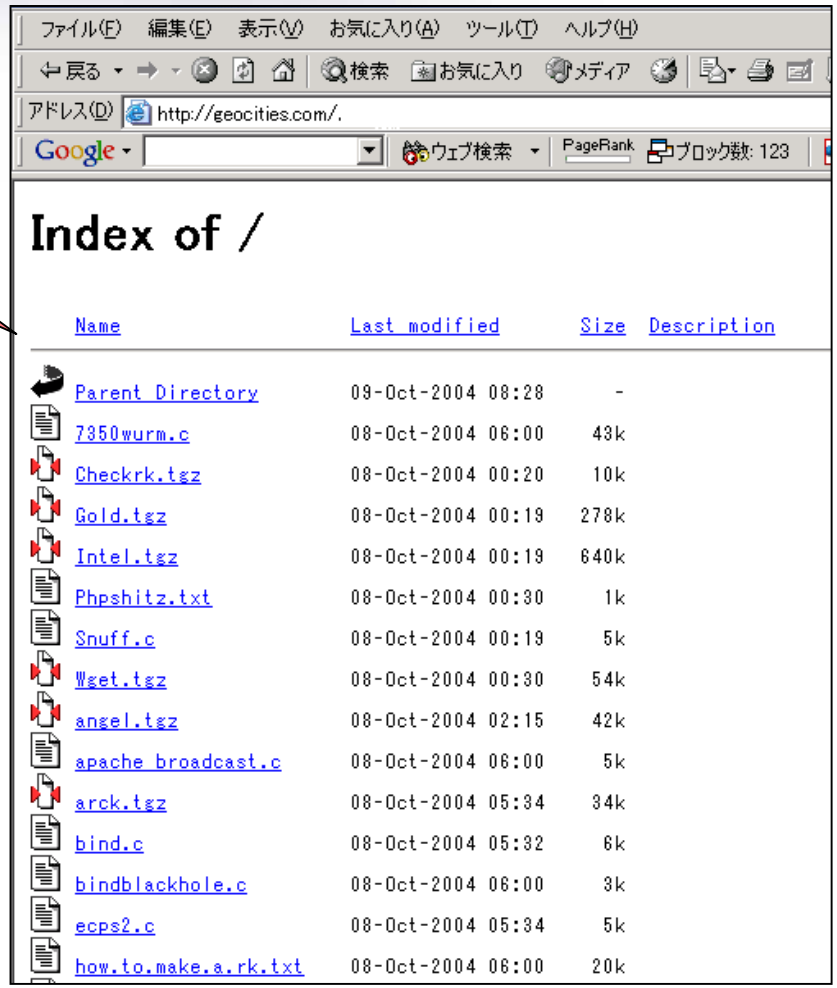
①攻撃
12/23 0:11～0:13
経過時間　2分

②ダウンロード
12/23 0:14～0:14
経過時間　3分

INTERNET SECURITY SYSTEMS®

Case Study1(時系列１)
～セグメントレベル～

悪性プログラムが
保存されている
サイト



INTERNET SECURITY SYSTEMS®

Case Study1(時系列２)
～セグメントレベル～

③バックドア
12/23 0:25～
経過時間 14分

Summary | Asset | Sensor | Sensor Analysis | Reporting

Event Analysis - Details

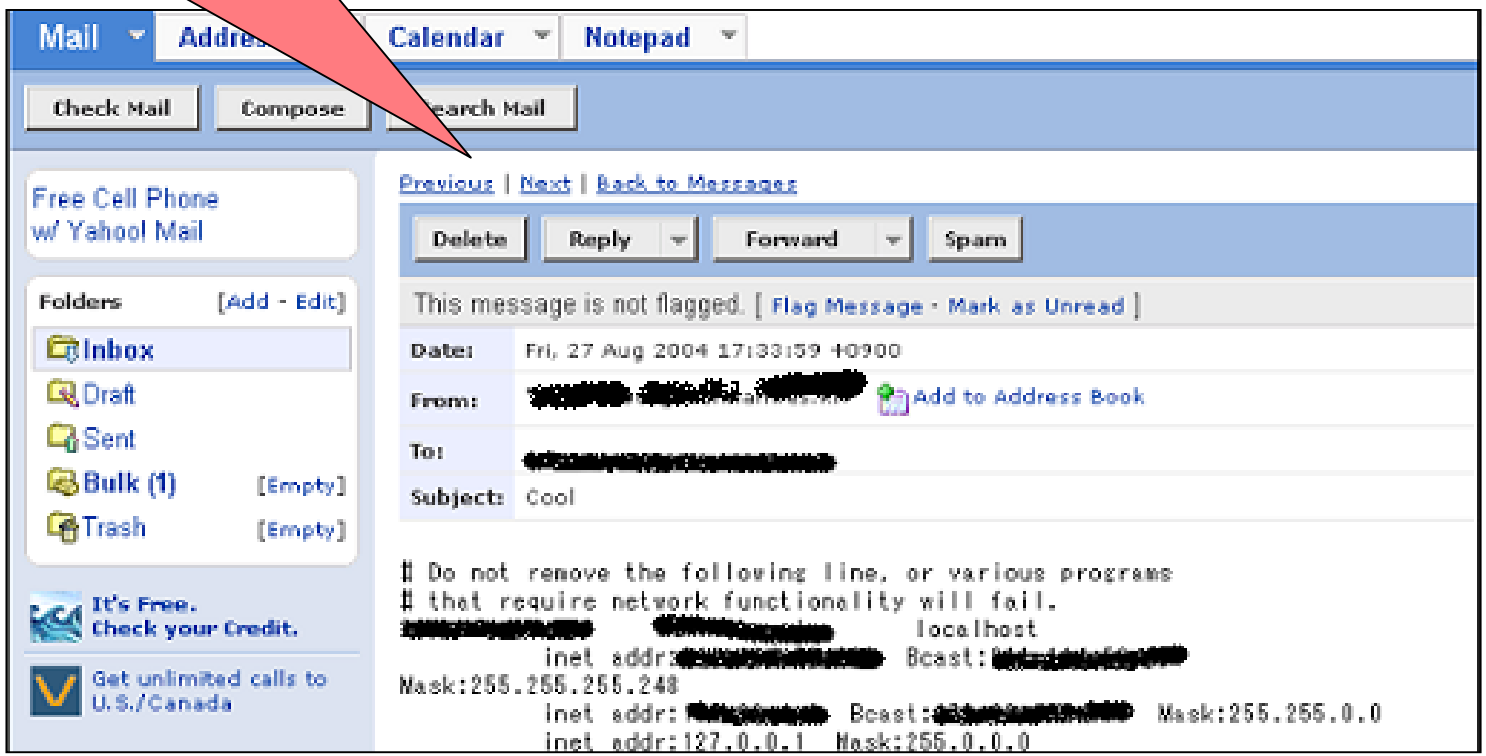
Severity	Time	Tag Name	Event C...	Source IP	Source Port	Target IP	Object Name	:recipient
Low	2004-12-23 00:25:39 JST	SSH_Version	1	82. .179	2192	192.168.221.180	121	
Low	2004-12-23 00:25:40 JST	SSH_Version	1	82. .179	2192	192.168.221.180	121	
Medium	2004-12-23 00:25:47 JST	DNS_Query_All	1	192.168.221.180	1026	202 .1	53	
Low	2004-12-23 00:26:03 JST	Email_Ehlo	1	192.168.221.180	1043	64. 18	25	
Low	2004-12-23 00:26:03 JST	Email_ServerID	1	64. .18	25	192.168.221.180	1043	
Low	2004-12-23 00:26:11 JST	Email_To	1	192.168.221.180	1043	64. .18	25	root_kyt@ .com
Low	2004-12-23 00:26:11 JST	Email_From	1	192.168.221.180	1043	64. .18	25	
Low	2004-12-23 00:26:12 JST	Email_Data	1	192.168.221.180	1043	64. .18	25	
Low	2004-12-23 00:26:12 JST	Email_Subject	1	192.168.221.180	1043	64. .18	25	
Low	2004-12-23 00:26:48 JST	FTP_Server_Identity	1	203. .114	2769	192.168.221.180	21	
Low	2004-12-23 00:26:49 JST	FTP_Server_Identity	1	203. .114	3422	192.168.221.180	21	
Medium	2004-12-23 00:26:49 JST	FTP_Pass	1	203. .114	3422	192.168.221.180	21	
Low	2004-12-23 00:26:49 JST	FTP_User	1	203. .114	3422	192.168.221.180	21	
High	2004-12-23 00:27:04 JST	FTP_Glob_TildeBrace_Vuln				203. .111	4060	
Low	2004-12-23 00:28:28 JST	TCP_Probe_Ftp				206. .88	21	
Low	2004-12-23 00:35:02 JST	TCP_Probe_NetBIOS				192.168.221.180	139	
Low	2004-12-23 00:36:15 JST	TCP_Probe_NetBIOS				192.168.221.180	139	
Low	2004-12-23 00:52:32 JST	TCP_Probe_NetBIOS				192.168.221.180	139	
Low	2004-12-23 00:53:55 JST	TCP_Probe_NetBIOS				192.168.221.180	139	

メール送信を確認
12/23 0:26～0:26
経過時間 15分

INTERNET SECURITY SYSTEMS®

Case Study1(時系列２)
～セグメントレベル～

ユーザのパスワード情報
などをフリーメールへ転送



INTERNET | SECURITY | SYSTEMS®

Case Study1(時系列３)
～セグメントレベル～

Summary | Asset | Sensor | Sensor Analysis | Reporting

Event Analysis - Details

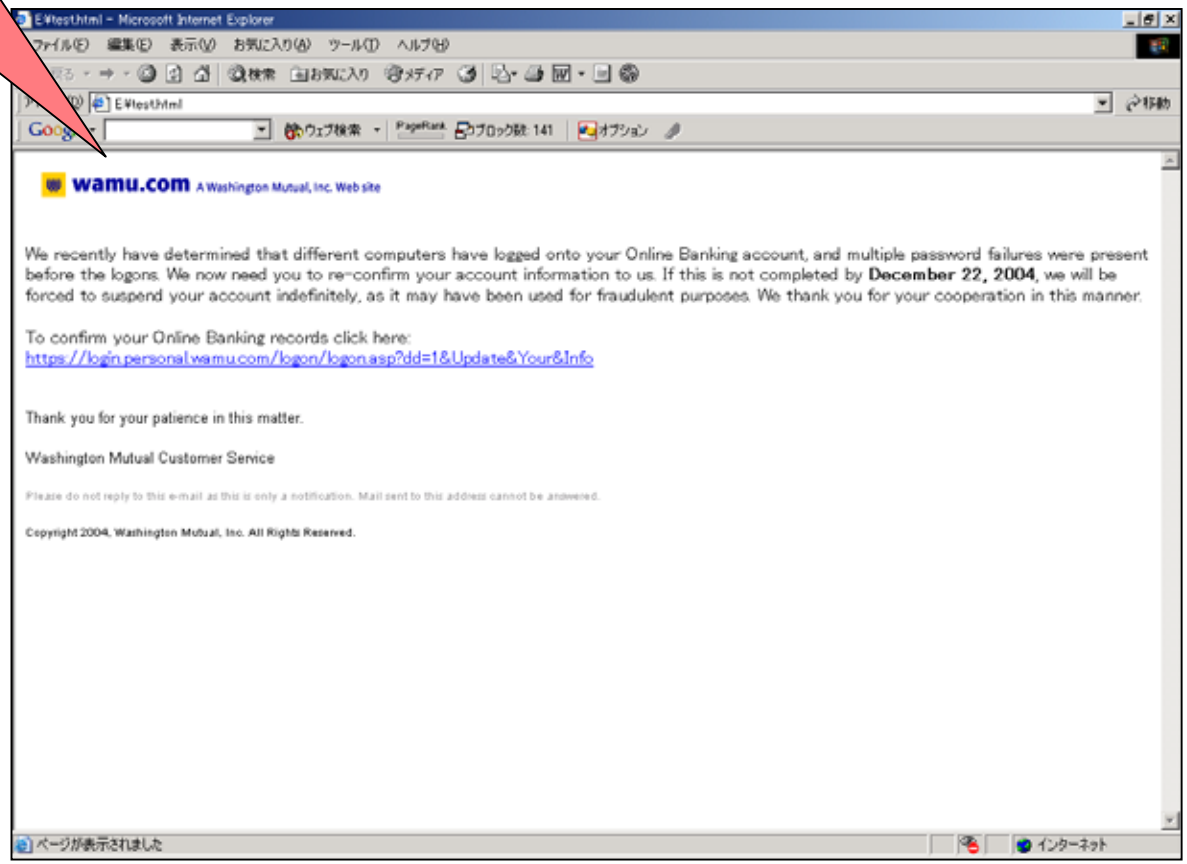
Severity	Time	Tag Name	Event C...	Source IP	Target IP	Object Name	Source Port	:serve
Low	2004-12-24 21:31:05 JST	HTTP_Server_ID	1	192.168.221.180	62. .246	80	1056	Apache/1.3.28 (Unix) mod_ssl/2.8.12 OpenS
Low	2004-12-24 21:31:55 JST	TCP_Probe_DNS	1	192.168.221.180	218 3.4	53	1058	
Low	2004-12-24 21:31:55 JST	TCP_Probe_Other	1	192.168.221.180	218 3.4	220	1061	
Low	2004-12-24 21:31:55 JST	TCP_Probe_Finger	1	192.168.221.180	218 3.4	79		
Low	2004-12-24 21:31:55 JST	TCP_Probe_POP3	1	192.168.221.180	218 3.4	110		
Low	2004-12-24 21:36:55 JST	HTTP_Get	1	192.168.221.180	62. .246	80		
Low	2004-12-24 21:36:55 JST	HTTP_User_Agent	1	192.168.221.180	62. .246	80		
Low	2004-12-24 21:36:55 JST	HTTP_Server_ID	1	192.168.221.180	62. .246	80		mod_ssl/2.8.12 OpenS
Low	2004-12-24 21:40:06 JST	TCP_Probe_Ftp	1	192.168.221.180	218 3.4	21		
Low	2004-12-24 21:43:42 JST	TCP_Probe_MSRPC	1	211. 194	192.168.221.180	135		
Low	2004-12-24 21:44:24 JST	HTTP_User_Agent	1	192.168.221.180	62.2 .246	80		
Low	2004-12-24 21:44:24 JST	HTTP_Get	1	192.168.221.180	62.2 .246	80	1064	
Low	2004-12-24 21:44:25 JST	HTTP_Server_ID	1	192.168.221.180	62.2 .246	80	1064	Apache/1.3.28 (Unix) mod_ssl/2.8.12 OpenS
Low	2004-12-24 21:44:43 JST	TCP_Probe_MSRPC	2	211.1 194	192.168.221.180	135	63943	
Low	2004-12-24 21:45:06 JST	Email_Ehlo	1	192.168.221.180	64.1 8	25	1065	
Low	2004-12-24 21:45:06 JST	Email_Ehlo	1	192.168.221.180	67.2 .11	25	1066	
Low	2004-12-24 21:45:06 JST	Email_From	1	192.168.221.180	67.2 .11	25	1066	
Low	2004-12-24 21:45:06 JST	Email_ServerID	1	64.1 '8	192.168.221.180	1065	25	YSmtp mta107.mail.sc5.yahoo.com ESMTP s
Low	2004-12-24 21:45:06 JST	Email_ServerID	1	67.2 .11	192.168.221.180	1066	25	YSmtp mta179.mail.re2.yahoo.com ESMTP se
Low	2004-12-24 21:45:07 JST	Email_Data	1	192.168.221.180	64.1	25	1065	
Low	2004-12-24 21:45:07 JST	Email_Data	1	192.168.221.180	67.2 1	25	1066	
Low	2004-12-24 21:45:07 JST	Email_From	1	192.168.221.180	64.1	25	1065	
Low	2004-12-24 21:45:07 JST	Email_Subject	1	192.168.221.180	64.1	25	1065	
Low	2004-12-24 21:45:07 JST	Email_Subject	1	192.168.221.180	67.2 1	25	1066	
Low	2004-12-24 21:45:07 JST	Email_To	1	192.168.221.180	64.1	25	1065	
Low	2004-12-24 21:45:07 JST	Email_To	1	192.168.221.180	67.2 1	25	1066	
Low	2004-12-24 21:46:43 JST	UDP_Probe_Other	1	206.1 .177	192.168.221.180	1434	1277	
Low	2004-12-24 21:57:16 JST	SSH_Version	1	81.19 .47	192.168.221.180	121	3240	
Low	2004-12-24 21:57:18 JST	SSH_Version	1	81.19 .47	192.168.221.180	121	3240	

④スパムメール
12/24 21:45～
経過時間 45:34

INTERNET SECURITY SYSTEMS®

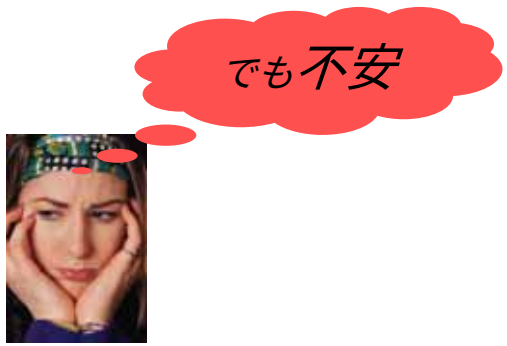
Case Study1(時系列３)
～セグメントレベル～

フィッシングメール



実践偏
～セグメントレベル～

- とりあえず発見手法を試してみよう



Case Study1(①攻撃)
～セグメントレベル～

①攻撃 Analysis - Event Name

Severity	Tag Name	Event Count	Source Count	Target Count	Object Count	Earliest Event	Latest Event
High	HTTP_WebDAV_Long_Rqst_BO	3	3	1	1	2004-12-26 16:00:00 JST	2004-12-27 18:00:00 JST
High	FTP_Cwd_Overflow	3	1	1	1	2004-12-22 22:00:00 JST	2004-12-23 00:00:00 JST
High	FTP_Generic_Intel_Overflow	3	1	1	1	2004-12-22 22:00:00 JST	2004-12-23 00:00:00 JST
High	DNS_Windows_SMTP_Overflow	1	1	1	1	2004-12-24 23:00:00 JST	2004-12-24 23:00:00 JST

Summary | Asset | Sensor | Sensor Analysis | Reporting

Event Analysis - Attacker

Source IP	Source DNS Name	# High	# Medium	# Low	Tag Count	Target Count	Object Count	Earliest Event	Latest Event
203.198.215.114		6	0	0	2	1	1	2004-12-22 22:00:00 JST	2004-12-23 00:00:00 JST
222.65.63.138		1	0	0	1	1	1	2004-12-27 18:00:00 JST	2004-12-27 18:00:00 JST
222.136.199.225		1	0	0	1	1	1	2004-12-26 23:00:00 JST	2004-12-26 23:00:00 JST
222.50.14.209		1	0	0	1	1	1	2004-12-26 16:00:00 JST	2004-12-26 16:00:00 JST
202.224.32.1		1	0	0	1	1	1	2004-12-24 23:00:00 JST	2004-12-24 23:00:00 JST

検知した攻撃は、監視セグメントの
IPアドレスは含まれていなかった。

INTERNET SECURITY SYSTEMS®

Case Study1(②ダウロード)
～セグメントレベル～

悪性プログラムのダウロードを確認

Summary | Asset | Sensor | Sensor Analysis | Reporting

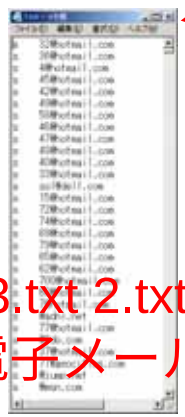
②悪性プログラムのダウンロード

Severity	Tag Name	Event Count	Source Count	Target Count	Object Count	Earliest Event	Latest Event
Low	FTP_Get	6	1	3	1	2004-12-23 00:00:00 JST	2004-12-24 22:00:00 JST

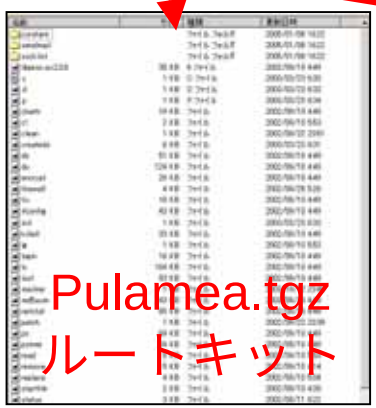
Summary | Asset | Sensor | Sensor Analysis | Reporting

Event Analysis - Details

Severity	Time	Tag Name	Event Count	:file	:intruder-ip-addr	:intruder-...	:victim-ip-addr	:victim-port	Object Name	Source Port
Low	2004-12-23 00:14:33 JST	FTP_Get	1	inst	192.168.221.180	1033	153.143	21	21	1033
Low	2004-12-23 00:24:11 JST	FTP_Get	1	Armand.tgz	192.168.221.180	1040	.20.134	21	21	1040
Low	2004-12-23 04:46:12 JST	FTP_Get	1	pulamea.tgz	192.168.221.180	1047	153.143	21	21	1047
Low	2004-12-23 05:08:13 JST	FTP_Get	1	pulamea.tgz	192.168.221.180	1050	.153.143	21	21	1050
Low	2004-12-24 22:00:47 JST	FTP_Get	1	3.txt	192.168.221.180	1068	.71.246	21	21	1068
Low	2004-12-24 22:03:51 JST	FTP_Get	1	2.txt	192.168.221.180	1068	71.246	21	21	1068



3.txt 2.txt
電子メール



Pulamea.tgz
ルートキット

Armand.tgz
フィッシングサイト

INTERNET SECURITY SYSTEMS®

Case Study1(③バックドア)
～セグメントレベル～

Summary | Asset | Sensor | Sensor Analysis | Reporting

③レジストリ修正バックドアの作成

Severity	Tag Name	Event Count	Source Count	Target Count	Object Count	Earliest Event	Latest Event
Low	SSH_Version	79	9	3	2	2004-12-22 07:00:00 JST	2004-12-27 02:00:00 JST

Summary | Asset | Sensor | Sensor Analysis | Reporting

Event Analysis - Details

Severity	Time	Tag Name	Event Count	:victim-ip-addr	:victim-port	:intruder-ip-addr	:intruder-port	:software
Low	2004-12-23 00:25:35 JST	SSH_Version	1	192.168.221.180	121	81. 3.86	3421	1.2.27
Low	2004-12-23 00:25:35 JST	SSH_Version	1	192.168.221.180	121	81. 3.86	3421	PuTTY-Release-0.56
Low	2004-12-23 00:25:39 JST	SSH_Version	1	192.168.221.180	121	82. .179	2192	1.2.27
Low	2004-12-23 00:25:40 JST	SSH_Version	1	192.168.221.180	121	82. .179	2192	PuTTY-Release-0.56
Low	2004-12-23 03:21:16 JST	SSH_Version	1	192.168.221.180	121	81. 81	3209	1.2.27
Low	2004-12-23 03:21:17 JST	SSH_Version	1	192.168.221.180	121	81. 81	3209	PuTTY-Release-0.56
Low	2004-12-23 03:41:10 JST	SSH_Version	1	192.168.221.180	121	81. 81	3280	PuTTY-Release-0.56
Low	2004-12-23 03:41:10 JST	SSH_Version	1	192.168.221.180	121	81. 81	328	
Low	2004-12-23 04:10:53 JST	SSH_Version	1	192.168.221.180	121	81. 81	330	
Low	2004-12-23 04:10:53 JST	SSH_Version	1	192.168.221.180	121	81. 81	330	
Low	2004-12-23 04:19:59 JST	SSH_Version	1	192.168.221.180	121	81. 81	331	
Low	2004-12-23 04:19:59 JST	SSH_Version	1	192.168.221.180	121	81. 81	331	
Low	2004-12-23 04:20:11 JST	SSH_Version	1	192.168.221.180	121	81. 81	331	
Low	2004-12-23 04:20:11 JST	SSH_Version	1	192.168.221.180	121	81. 81	331	
Low	2004-12-23 04:32:04 JST	SSH_Version	1	192.168.221.180	121	81. 81	33	
Low	2004-12-23 04:32:05 JST	SSH_Version	1	192.168.221.180	121	81. 81	33	
Low	2004-12-23 04:44:58 JST	SSH_Version	1	192.168.221.180	121	81. 81	33	
Low	2004-12-23 04:44:58 JST	SSH_Version	1	192.168.221.180	121	81. 81	33	
Low	2004-12-23 05:07:07 JST	SSH_Version	1	192.168.221.180	121	81. 81	3415	PuTTY-Release-0.56
Low	2004-12-23 05:07:07 JST	SSH_Version	1	192.168.221.180	121	81. 81	3415	1.2.27

このアクセスは、攻撃者がバックドア(SSH)へ接続している様子である。Port121は、攻撃者によって作成されたバックドアである。

INTERNET SECURITY SYSTEMS®

Case Study1(④スキャン)
～セグメントレベル～

Summary | Asset | Sensor | **Sensor Analysis** | Reporting

ScanAnalysis - Event Name

Severity	Tag Name	Event Count	Source Count	Target Count	Object Count	Earliest Event	Latest Event
Medium	Email_Relay_Spam	3	1	1	1	2004-12-24 23:00:00 JST	2004-12-24 23:00:00 JST
Low	Email_Data	13559	1	1080	1	2004-12-23 00:00:00 JST	2004-12-25 10:00:00 JST
Low	Email_Ehlo	23163	2	2272	1	2004-12-23 00:00:00 JST	2004-12-25 10:00:00 JST
Low	Email_Error	794	2	243	1	2004-12-24 22:00:00 JST	2004-12-25 00:00:00 JST
Low	Email_From	23012	3	2269	1	2004-12-22 11:00:00 JST	2004-12-25 10:00:00 JST
Low	Email_ServerID	24255	2272	4	3975	20	
Low	Email_Subject	13555	1	1079	1	20	
Low	Email_To	19998	3	1793	1	20	
Low	TCP_Service_Sweep	64	1	4	3	20	

Summary | Asset | Sensor | **Sensor Analysis** | Reporting

Event Analysis - Details

Severity	Time	Tag Name	E...	:subject	:intr
Low	2004-12-24 23:07:32 JST	Email_Subject	1	WARNING: CONFIRM YOUR ONLINE BANKING RECORDS	92
Low	2004-12-24 23:07:33 JST	Email_Subject	1	WARNING: CONFIRM YOUR ONLINE BANKING RECORDS	92
Low	2004-12-24 23:07:33 JST	Email_Subject	1	WARNING: CONFIRM YOUR ONLINE BANKING RECORDS	92
Low	2004-12-24 23:07:33 JST	Email_Subject	1	WARNING: CONFIRM YOUR ONLINE BANKING RECORDS	92
Low	2004-12-24 23:07:33 JST	Email_Subject	1	WARNING: CONFIRM YOUR ONLINE BANKING RECORDS	92
Low	2004-12-24 23:07:33 JST	Email_Subject	1	WARNING: CONFIRM YOUR ONLINE BANKING RECORDS	92
Low	2004-12-24 23:07:34 JST	Email_Subject	1	WARNING: CONFIRM YOUR ONLINE BANKING RECORDS	92
Low	2004-12-24 23:07:34 JST	Email_Subject	1	WARNING: CONFIRM YOUR ONLINE BANKING RECORDS	92
Low	2004-12-24 23:07:37 JST	Email_Subject	1	WARNING: CONFIRM YOUR ONLINE BANKING RECORDS	92
Low	2004-12-24 23:07:37 JST	Email_Subject	1	WARNING: CONFIRM YOUR ONLINE BANKING RECORDS	92
Low	2004-12-24 23:07:38 JST	Email_Subject	1	WARNING: CONFIRM YOUR ONLINE BANKING RECORDS	92

このアクセスは、攻撃者が複数のアドレスに対して、メールを送信している様子である。

INTERNET SECURITY SYSTEMS®

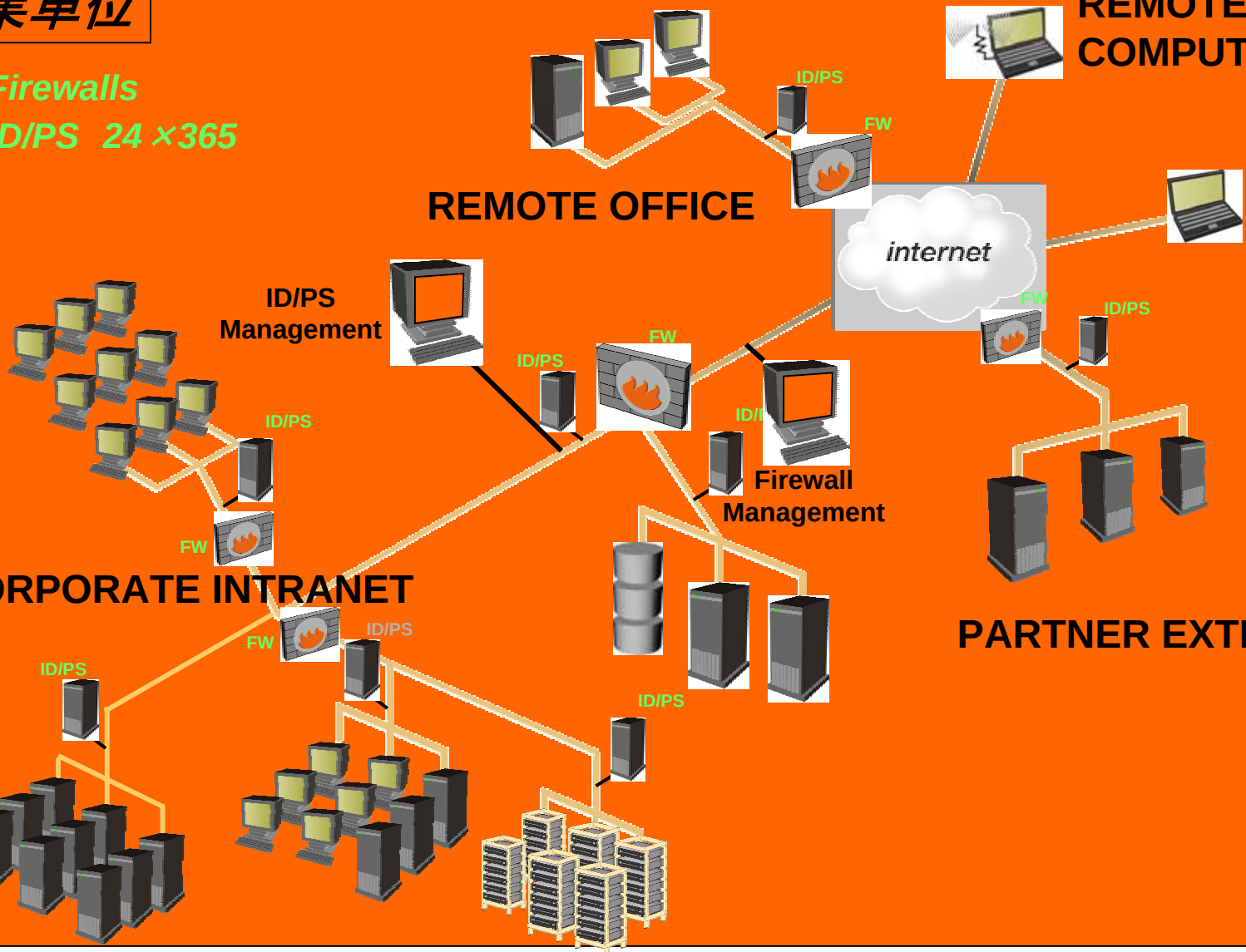
まとめ
～セグメントレベル～

- セグメントレベルの場合は、攻撃の初期段階から発見することができる。

監視範囲
～企業レベル～

企業単位

- *Firewalls*
- *ID/PS 24 ×365*

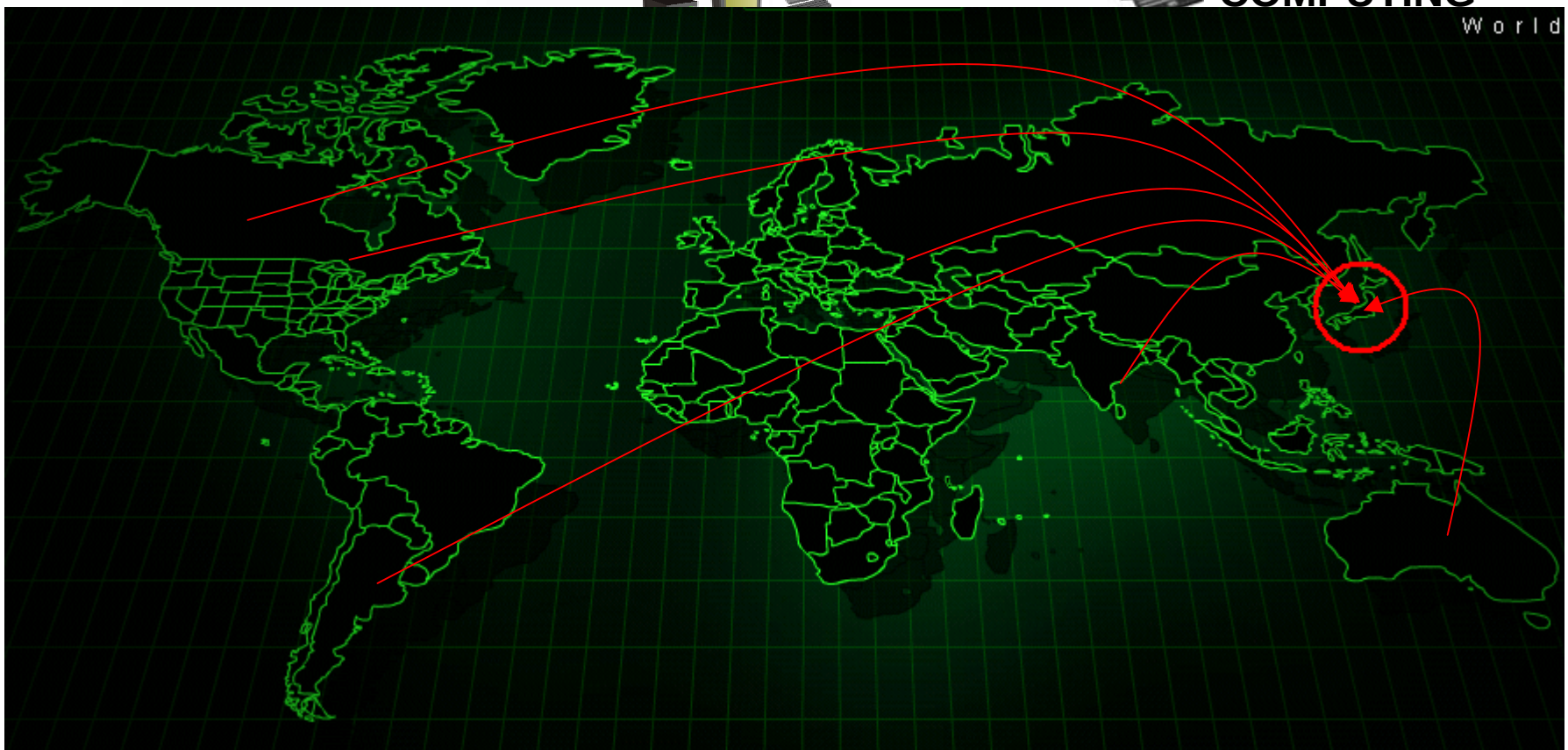


まとめ
～企業レベル～

- 脆弱性情報やワーム情報などの情報収集が必要である。
- 攻撃の初期段階で迅速に対応する必要がある。
- 24時間365日の対応が必要である。

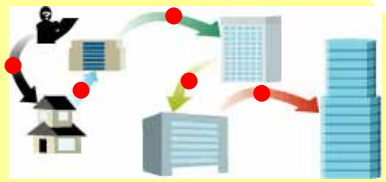
監視範囲
～グローバルレベル～

REMOTE/MOBILE
COMPUTING



インターネット上の脅威分析
～グローバルレベル～

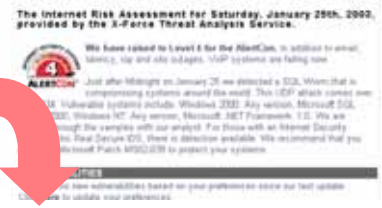
宣伝です



社会動性
テロや紛争など

US SOC

総合分析



インターネットリスクレベル

GTOC X-Force Global Threat Analysis Center

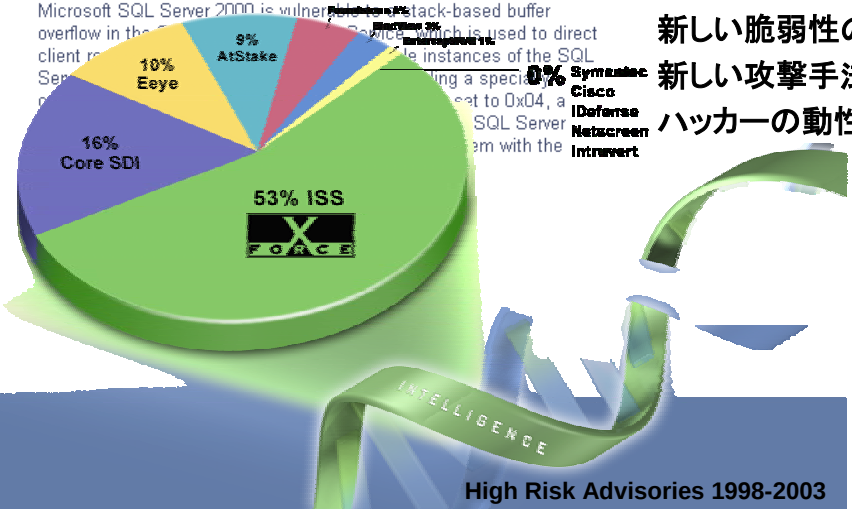
分析情報配信

mssql-resolution-service-bo2 (10031) High Risk

Microsoft SQL Server Resolution Service stack buffer overflow

Description:

Microsoft SQL Server 2000 is vulner... stack-based buffer overflow in the ... which is used to direct client r... instances of the SQL Ser... a speci... set to 0x04, a ... SQL Server ... with the ...



High Risk Advisories 1998-2003

X-Force
監視・防御シグネチャを提供
新しい脆弱性の発見
新しい攻撃手法、ツール
ハッカーの動性

SOC
世界 5 箇所のSOCで検知されたイベント状況により連動
X-FORCEは常に最新のシグネチャをリアルタイムに提供
日本語・英語によるオペレータ対応ー海外拠点を持つ企業

各国のSOC

Case Study2
～グローバルレベル～

監視側　（非公開情報）

メーカ / セキュリティベンダ / 他

セキュリティホールの発見

メーカー等への通知

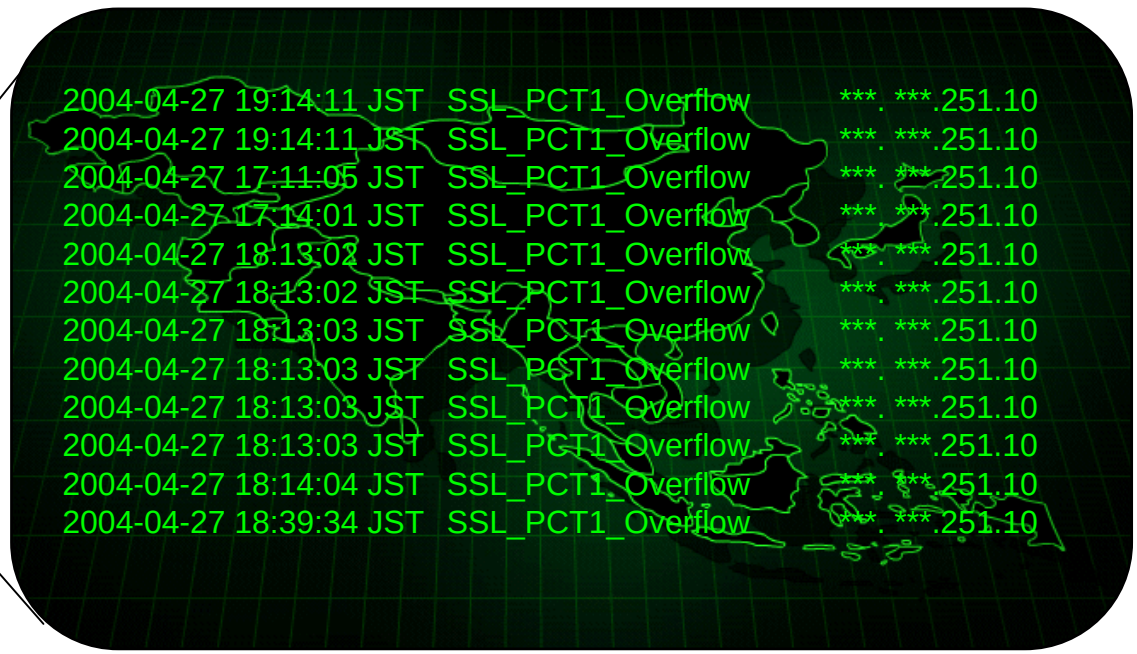
パッチの作成

非公開

パッチの未適用サーバ

パッチの適用

日時：2004年4月27日（火曜日）
各拠点に設置されたセンサーからアラートが発生する。



INTERNET SECURITY SYSTEMS®

Case Study2
～グローバルレベル～

監視側　（非公開情報）

メーカ / セキュリティベンダ / 他

セキュリティホールの発見

メーカー等への通知

パッチの作成

非公開

パッチの未適用サーバ

パッチの適用

送信元は、中華人民共和国に割り当てられたIPからであると判明する

INTERNET SECURITY SYSTEMS®

Case Study2
～グローバルレベル～

メーカ / セキュリティベンダ / 他

セキュリティホールの発見

メーカー等への通知

パッチの作成

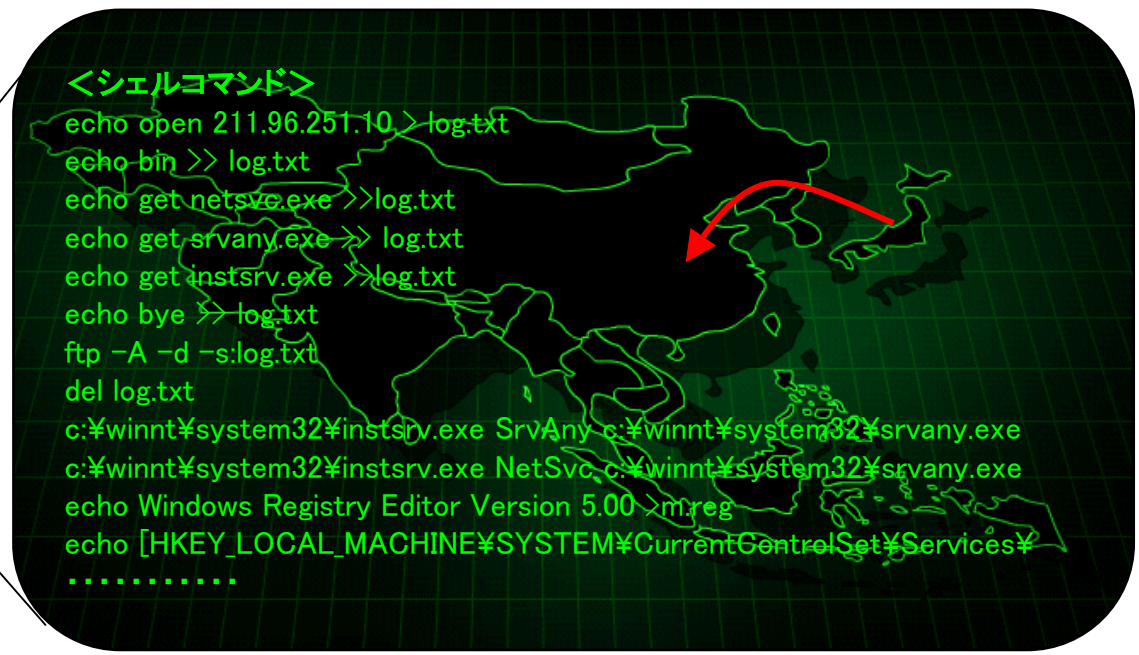
非公開

パッチの未適用サーバ

パッチの適用

監視側　（非公開情報）

攻撃を受けた後の挙動
①攻撃を受けたマシンから***.***.251.10の443/tcpへ
②シェルスクリプトが実行される。
③FTPを利用して3つのファイルがダウロードされる。
④netsvc.exe がサービスとして起動される。
⑤リモートから操作が可能になる。



INTERNET SECURITY SYSTEMS®

まとめ
～グローバルレベル～

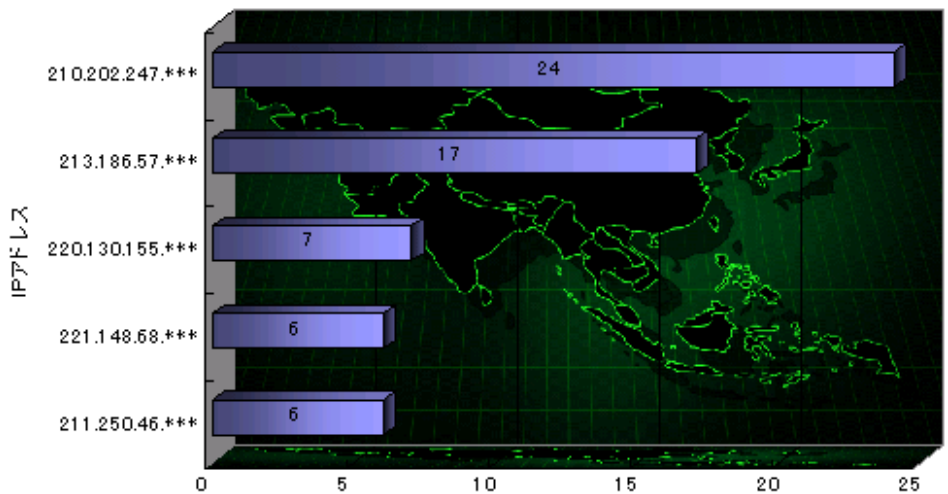
- グローバルレベルの攻撃は、企業レベルでの発見は難しい。
- グローバルレベルの情報の収集および迅速な対応を必要とする場合は、アウトソーシングなどを利用するのも一つの手段である。

Weekly SOC Reportについて
～グローバルレベル～

宣伝です

ブラックリストIP（要注意IPアドレス）

IPアドレス	不正アクセスの種類	国コード	件数
210.202.247.***	侵入行為	TW（台湾）	24
213.186.57.***	侵入行為	FR（フランス）	17
220.130.155.***	侵入行為	TW（台湾）	7
221.148.68.***	侵入行為	KR（韓国）	6
211.250.46.***	侵入行為	KR（韓国）	6



http://www.isskk.co.jp/SOC_report.html（毎週火曜日更新）

INTERNET SECURITY SYSTEMS®

全体のまとめ

- 発見手法については、その時々の攻撃手法の変化にあわせて改善して行く必要がある。その為、常に情報収集と解析をおこなう必要がある。

付録

FTP_Glob_TildeBrace_Vulns
～付録～

FTP glob() vulnerabilities using tilde and left brace (FTP_Glob_TildeBrace_Vulns)

このシグネチャまたは脆弱点について
RealSecure Network Sensor: このシグネチャは、チルダ（~）で始まり左中括弧（{）で終わる FTP コマンド引数を検出します。 このようなコマンドは、影響を受ける FTP サーバーの脆弱点を悪用しようとする攻撃者の試みを示す場合があります。

影響を受けるシステム
Linux kernel、Unix、FTP

タイプ
不正アクセスの試み

脆弱点の説明
Glob 関数を使うことによってプログラムは、シェルが使用するルールに従って特定パターンに一致するパス名を検索することができます。 複数の FTP サーバーの実装は、チルダ（~）で始まり左中括弧（{）で終わるコマンド引数を使用している攻撃に対して脆弱です。 特定の脆弱性は、FTP サーバー間で異なる場合があります。

この脆弱点の解決方法
このイベントは、ワシントン大学の FTP デーモン（WU-FTPD）または多数の Linux ディストリビューションに収録されている glibc パッケージにある脆弱点を示す可能性があります。 アップグレード情報またはパッチ情報については、各特定の脆弱点に関連する X-Force データベースの記録を参照してください。

SSL2_Master_Key_Overflow ～付録～

OpenSSL SSL2 master key buffer overflow (SSL2_Master_Key_Overflow)
このシグネチャまたは脆弱点について
RealSecure Network Sensor: このシグネチャは、メジャー バージョン番号が 2 である SSL サーバーに対する SSL ネゴシエーション ハンドシェイクを検出します。具体的には、クライアント マスター キー パケットのキー引数の長さが設定可能なパラメータ「ssl.v2masterkey.arglenthreshold」の値を超える場合に、このデコードがトリガされます。 デフォルトのしきい値は 8 です。

影響を受けるシステム
OpenSSL: 0.9.6d 以前、OpenSSL: 0.9.7-b2 以前、Red Hat Linux: 7.x、OpenVMS: すべてのバージョン、Red Hat Linux: 7.3、Debian Linux: 3.0、OpenPKG: 1.0、EnGarde Secure Linux: Community Edition、Tru64 UNIX: すべてのバージョン、Red Hat Linux: 7.0、Trustix Secure Linux: 1.1、Red Hat Linux: 6.2、Debian Linux: 2.2、Red Hat Linux: 7.2、Trustix Secure Linux: 1.5、Red Hat Linux: 7.1、Trustix Secure Linux: 1.2

タイプ
不正アクセスの試み

脆弱点の説明
OpenSSL は、SSL (Secure Sockets Layer) プロトコルおよび TLS (Transport Layer Security) プロトコルのオープン ソース実装であり、多くの Linux ディストリビューションに付属しています。 OpenSSL バージョン 0.9.6d 以前、0.9.7 beta1 以前、および現在の開発スナップショット 0.9.7 は、SSL2 クライアント マスター キーの処理が不適切なために発生するバッファ オーバーフローに対して脆弱です。 リモートの攻撃者は、長すぎる SSL2 クライアント マスター キーを送信することによってバッファをオーバーフローさせ、上位の権限を使って任意のコードを実行したり、システムをクラッシュさせたりする可能性があります。

この脆弱点の解決方法
OpenSSL Project の Web サイトから OpenSSL の最新バージョン (0.9.6e 以降) を入手してアップグレードします。

MSRPC_RemoteActivate_Bo
～付録～

RPC DCOM インターフェースのバッファ オーバーフロー (MSRPC_RemoteActivate_Bo)
このシグネチャまたは脆弱点について
RealSecure Server Sensor:

このシグネチャは、バッファ オーバーフローを引き起こすために使用される、特殊な形式の MSRPC Remote ActivationRequest を検出します。

影響を受けるシステム
Windows NT: 4.0 TSE、Windows 2000: 任意のバージョン、Windows NT: 4.0、Windows 2003: Server、Windows: XP

タイプ
不正アクセスの試み

脆弱点の説明
Microsoft Windows 2000、Windows NT 4.0、Windows XP、および Windows Server 2003 は、RPC (Remote Procedure Call) サービスの Distributed Component Object Model (DCOM) インターフェースにおけるバッファ オーバーフローに対して脆弱です。リモートからの攻撃者は、TCP ポート 135 で待機している RPC サービスに不正なメッセージを送信することで、バッファをオーバーフローさせ、ローカル システムの権限を使ってシステム上で任意のコードを実行する可能性があります。

この脆弱点の解決方法
Microsoft Security Bulletin MS03-026 を参照して、システムに適切なパッチを適用します。

MSRPC_LSASS_Bo
～付録～

Microsoft Windows LSASS buffer overflow (MSRPC_LSASS_Bo)
このシグネチャまたは脆弱点について
RealSecure Network Sensor、RealSecure Server Sensor:

このシグネチャは、Microsoft Local Security Authority Subsystem Service プロトコルをデコードした後、LSASS 要求に関連するフィールドをデコードします。さらに、これらフィールドのいずれかの長さがしきい値を超えた場合に、このシグネチャがトリガされます。

影響を受けるシステム
Windows Server 2003: すべてのバージョン、Windows XP: 64-bit Edition 2003、Windows XP: 任意のバージョン、Windows 2000: 任意のバージョン

脆弱点の説明
Microsoft Windows 2000、XP、Windows Server 2003、および Windows XP 64-Bit Edition 2003 では、不適切な境界チェックによって発生する Local Security Authority Subsystem Service (LSASS) のバッファ オーバーフローに対して脆弱です LSASS は、ローカル セキュリティ、デーモン認証、および Active Directory 操作のための管理インターフェースです。リモートの攻撃者は、特殊な形式のメッセージを影響を受けるシステムに送信することでバッファをオーバーフローさせ、システム上で任意のコードを実行する可能性があります。

注記: この脆弱点を悪用できるのは、Microfsoft Windows Server 2003 および Windows XP 64-Bit Edition 2003 のローカル管理者だけです。

この脆弱点の解決方法
Microsoft Security Bulletin を参照して、システムに適切なパッチを適用します。

INTERNET | SECURITY | SYSTEMS®

SSL_PCT1_Overflow ～付録～

SSL PCT1 でのバッファ オーバーフロー (SSL_PCT1_Overflow)
このシグネチャまたは脆弱点について
RealSecure Network Sensor、RealSecure Server Sensor:

このシグネチャは、PCT1 SSL のオーバーフローを引き起こす試みを検出します。

影響を受けるシステム
任意のアプリケーション: 任意のバージョン

タイプ
不正アクセスの試み

脆弱点の説明
Secure Sockets Layer (SSL) プロトコルは、2 つの通信アプリケーション間でプライバシを提供します。SSL PCT1 Private Communication Technology (PCT) プロトコル ライブラリはバッファ オーバーフローを含んでいます。

この脆弱点の解決方法
この問題がネットワーク上で検出された場合は、スウィープの発信元アドレスに基づいてアクティビティの性質を確認してください。

SQL_SSRP_Slammer_Worm
～付録～

SQL Slammer worm propagation (SQL_SSRP_Slammer_Worm)
このシグネチャまたは脆弱点について
RealSecure Network Sensor、RealSecure Server Sensor:

このイベントは、宛先ポート 1434 と SQL Slammer Worm のリターン アドレスにおける UDP パケットのオーバーフローを検出します

影響を受けるシステム
Microsoft MSDE: 2000、Microsoft SQL Server: 2000、Cisco CallManager: 3.3.x、Cisco Unity: 4.x、Backup Exec: 9.0、ExecView: 3.1、Cisco Unity: 3.x、Windows NT: すべてのバージョン、Cisco BBSM: 5.1、Cisco BBSM: 5.0、Windows 2000: すべてのバージョン

脆弱点の説明
SQL Slammer ワームは W32/SQLSlam-A、Sapphire、New SQL、Worm.SQL、および Helkern としても知られており、Microsoft SQL Server 2000 または Microsoft Desktop Engine (MSDE) 2000 の Resolution Service におけるバッファ オーバーフロー脆弱点を悪用することによって増殖します。 Slammer ワームの主な機能は、増殖し続けることです。 このワームには、分散型サービス不能 (DDoS) やバックドアの機能は組み込まれていません。 適切な防御をしなくても、再起動することで感染を除去できますが、サーバーが脆弱な場合は再感染する可能性があります。

Slammer ワームは Kernel32.dll と WS2_32.dll をロードし、GetTickCount を呼び出します。これは、ランダムな IP アドレス ルーチンのシードとして使用されます。 このルーチンは、悪用と増殖を行う 376 バイトのコードを SQL Server プロセスがシャット ダウンするまで UDP ポート 1434 に連続して送信します。 Slammer ワームは、Nimda ワームのようにローカル サブネット アドレスをスキャンすることを好みません。 このことは、ローカル ネットワークでの感染速度を制限しますが、このスキャン方法はネットワークに障害を引き起こすことが可能な大量のトラフィックを生成します。

この脆弱点の解決方法
管理者は、Microsoft Security Bulletin MS02-061 を参照して SQL Server の最新の累積パッチを適用し、さらなる感染に対して防御するためにシステムを再起動する必要があります。

INTERNET SECURITY SYSTEMS®

HTTP_Unix_Passwords
～付録～

passwd file accessed through Web server (HTTP_Unix_Passwords)
このシグネチャまたは脆弱点について
RealSecure Network Sensor: このシグネチャは、「passwd」または「shadow」パスワード ファイルに対する HTTP GET 要求を検出します。
RealSecure Server Sensor: このシグネチャは、Web(HTTP) サーバーを介した、UNIXシステム上の /etc/passwd ファイルへのアクセス試行を検出します。
影響を受けるシステム
HTTP、Unix

タイプ
不正アクセスの試み

脆弱点の説明
Unix システムの /etc/passwd ファイルには、パスワード情報が含まれています。 攻撃者は etc/passwd ファイルにアクセスして、システム上のすべてのパスワードに対してブルート フォース攻撃を試みている可能性があります。

攻撃者は、Web(HTTP) サーバーを経由して etc/passwd ファイルへのアクセス権を得る可能性があります。 これは通常サーバーにインストールされている CGI スクリプトの 1 つを介して行われます。

この脆弱点の解決方法
アクセスされた ＵＲＬ を調べて、アクセス試行が成功したかどうかを確認します。 成功している場合は、システムのセキュリティ侵害とすべてのパスワードが盗まれた可能性について検討してください。 このイベントは特定の脆弱点の結果起こるものですが、Web サーバーと CGI スクリプトに /etc/passwd ファイルへのリモート アクセスが可能な脆弱点がないか、よく確認する必要があります。

TCP_Network_Scan
～付録～

Portscan attack (TCP_Network_Scan)
このシグネチャまたは脆弱点について
RealSecure Network Sensor、RealSecure Server Sensor:

この異常シグネチャは、一人の侵入者からの、ネットワーク全体の頻繁な TCP 調査アクティビティを検出します。これは、TCP_Port_Scan シグネチャのしきい値を（場合によっては故意に）下げる可能性がある特定の種類のスキャンニング アクティビティを検出します。pam.tcp.network.scan.count および pam.tcp.network.scan.interval 調整パラメータを設定して、このシグネチャの調査の頻度のしきい値を制御します。

影響を受けるシステム
任意のアプリケーション:任意のバージョン

タイプ
攻撃準備調査

脆弱点の説明
ポートスキャンは、各ポートを調査して応答の有無を調べることにより、マシン上で実行されているサービスを判別する攻撃者の試みのことです。攻撃者はポートスキャンを利用して、その後の攻撃に役立つ情報を収集できます。

この脆弱点の解決方法
ポートスキャンの発信元を特定します。この発信元と、ターゲット ホストで実行されているサービスを関連付けてください。スキャンの送信元とその意図を確認してください。さらにいくつかの対策を講じて、スキャン対象のデバイスを保護することもできます。また、アクセス ログでも、不正アクセスの兆候がないかを確認してください。不正アクセスの可能性がある場合は、システムのセキュリティの侵害を考慮して、適切な措置をとってください。

TCP_Network_Sweep ～付録～

Service scanner attempting to connect to same port on multiple computers (TCP_Network_Sweep)
このシグネチャまたは脆弱点について
RealSecure Server Sensor、RealSecure Network Sensor:

この異常シグネチャは、複数の侵入者からの、ネットワーク全体の任意の 1 つのポートに対する頻繁な TCP 調査アクティビティを検出します。これは、マルウェアが一般的に知られるようになる前でも、ネットワーク上のトロイの木馬やワームのアクティビティを検出できる場合があります。これらのプログラムのスキャン アクティビティは、TCP_Service_Sweep および TCP_Port_Scan のしきい値を下げることがあります。しかし、これらのプログラムのアクティビティが集まると、このシグネチャのトリガがさらに容易になります。pam.tcp.network.sweep.count および pam.tcp.network.sweep.interval 調整パラメータを設定して、このシグネチャの調査の頻度のしきい値を制御します。

影響を受けるシステム
任意のアプリケーション:任意のバージョン

タイプ
攻撃準備調査

脆弱点の説明
攻撃者は、ネットワーク内で特定のサービスを実行しているコンピュータを見つけるため、さまざまなコンピュータの同じポートに接続しようとします。この情報は、攻撃者が攻撃を仕掛ける際に役立つ可能性があります。

攻撃者は、この種のスキャンを実行する際、検出されないように接続速度を遅くすることがあります。

この脆弱点の解決方法
このイベントの発信元を調べ、侵入者である可能性がないかどうか確認します。その発信元ネットワークから発信されたパケットをすべてブロックすることを検討してください。