情報窃取型サイバー攻撃対策に
ネットワークフォレンジック活用の試み

2014年4月21日
株式会社パイオリンク

本日のアジェンダ

（第一部）

実証プロジェクトの概要

株式会社パイオリンク
朴 昶昱（バク チャンウク）

（第二部）

プロトタイプ開発の概要、実機デモ

日本ダイレックス株式会社
松尾 義司

（第三部）

質疑応答

実証プロジェクトメンバー

（第一部）

実証プロジェクトの概要

1. PIOLINKのご紹介
2. 実証プロジェクトのご紹介
3. 標的型サイバー攻撃の理解
4. 実証プロジェクトの推進結果
5. 実証プロジェクトを通して

PIOLINKのご紹介

- 会社名 ： 株式会社 パイオリンク （PIOLINK, Inc.）
- 代表取締役 ： チョ ヨンチョル（YC.Cho）
- 設立日 ： 2000年7月26日
  （2004年7月に日本支社を開設）
- 所在地 ： 韓国 ソウル市
  （海外拠点：日本、中国、台湾、東南アジア）
- 資本金 ： 2億4,000万円
- 従業員数 ： 130名
- 株式公開（IPO）：2013年8月 韓国KOSDAQ市場（証券コード：70790）
- 事業分野 ： アプリケーション･ネットワーキング（AN）を実現する製品の
  開発 / 製造 / 販売 / 保守サービス
- 主力製品 ： ADC製品、WAF製品、セキュリティスイッチ、SDNスイッチ
- 販売実績 ： 約 30,000 台 （約 5,000 サイトで稼働中）

KOSDAQ LISTED COMPANY

PIOLINK

実証プロジェクトのご紹介

実証プロジェクトのご紹介

■ 実証プロジェクトを始めたきっかけ

– **サイバー攻撃の現場対応のセキュリティ専門家から**

・発生可能性のあるサイバー攻撃を想定したログ取得を行う必要がある。

・痕跡を残さない攻撃に実態解明のためには攻撃者の意図を意識したネットワーク挙動の監視が必要である。

– **サイバー攻撃対策に必要なネットワーク挙動監視の有効な方法を検討する**

・セキュリティ専門家・開発ベンダー・インテグレータが、それぞれの知見・知識を持ち寄って検討し実証してみる。

■ 実証プロジェクトメンバーの紹介

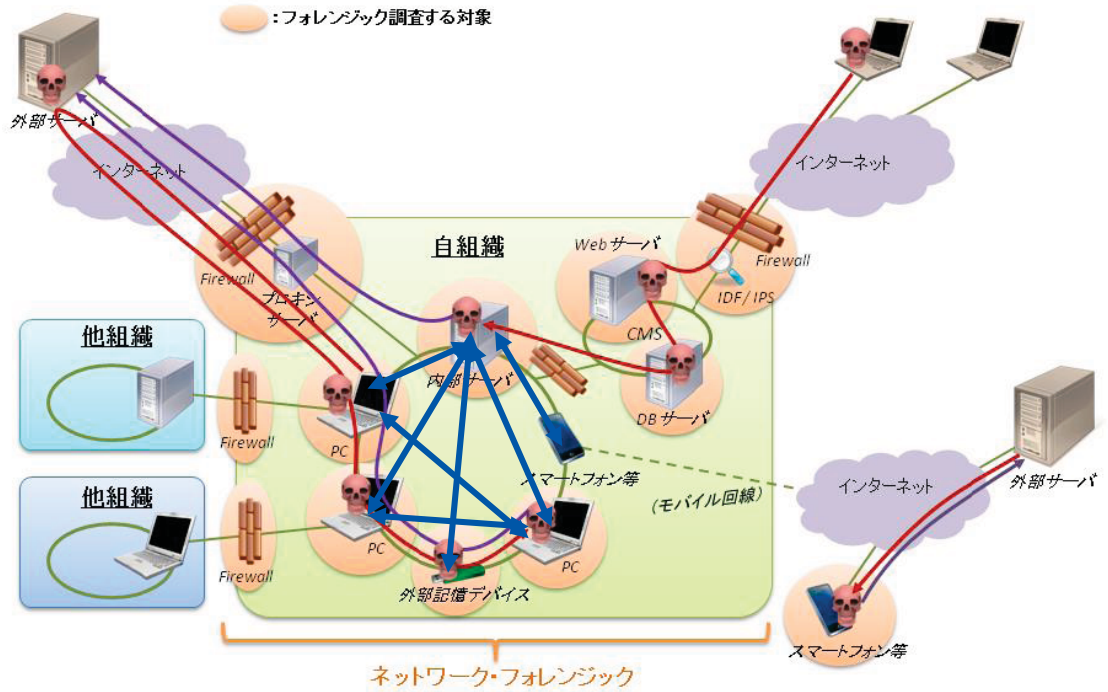
– 株式会社サイバーディフェンス研究所 理事 上級分析官 名和 利男 氏
– マクニカネットワークス株式会社 セキュリティ研究センター センター長 政本 憲蔵 氏
– 日本ダイレックス株式会社 ネットワーク技術グループ 取締役 松尾 義司 氏
– 株式会社パイオリンク 日本支社 支社長　朴 昶昱

■ 実証プロジェクト推進経緯

– 2013年7月　実証プロジェクトの立ち上げ
– 2013年9月　攻撃手法のリサーチ等
– 2014年1月　プロトタイプの開発、検証
– 2014年3月　実環境においての実証実験の推進中

IDF 設立１０周年記念表彰式・シンポジウム（2013年8月23日）資料より

最近のデジタル・フォレンジックの調査対象



IDF 設立１０周年記念表彰式・シンポジウム（2013年8月23日）資料より

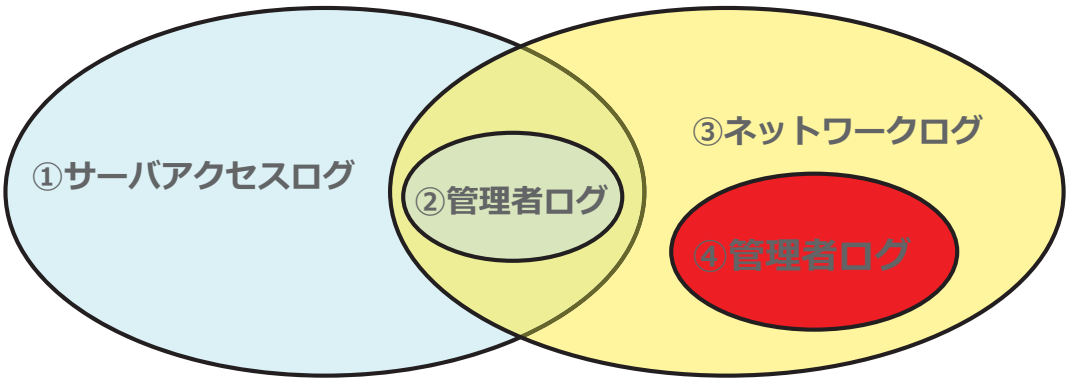
今後のネットワーク・フォレンジックの課題

- ネットワーク化されたシステムを設計する際には、**発生可能性のあるサイバー攻撃を想定したログ取得**を行うようにしなければならない。
  - 製品やシステム開発者、設計者、インテグレーター、運用者等が、最近のサイバー攻撃ロジックの直接的な習得と理解をする必要があるが、その仕組みが見当たらない。（実施しても相当のコストになるため、そのコストを回収する仕組みを作れない状況）
- ログ等の情報の分析からサイバー攻撃の実態解明をするに至るまでの基本的な**学術的な理論や手法を確立**しなければならない。
  - これを確立するには、徹底的なサイバー攻撃の分析に加え、既存製品による実際の検証を繰り返す必要がある。（製品仕様の記述情報のみでは、期待する情報の過不足を特定することは難しい。）
  - すべて経験に裏打ちされたものでなければ、実際の現場で活用することは難しい。
- 今後もネットワーク化されたシステムが発展していくため、**大規模なログ等の情報の解析技術・手法**を作り出していく必要がある。
  - いわゆる「ログ等の情報に特化したデータ・サイエンス」の分野を作り出していくことが考えられる。

内部ネットワークにおけるログ取得（仮説）

■ 内部ネットワークから取得する区分

① サーバ機器から取得するログ
② 通常業務のための管理者権限によるアクセスログ
③ ネットワークトラフィックの監視によって取得するログ
④ サーバのアクセスログに無い管理者権限のログ



■ ログの相関関係分析

ネットワークログの中で、サーバアクセスログから正規の管理者ログを除いた後に残る「管理者権限のログ」については疑いを持って対応する。

実証プロジェクトの試み

1．標的型サイバー攻撃に対する理解

標的型サイバー攻撃の侵入後に内部ネットワークでの攻撃実態が解明されつつあるので、この段階の攻撃手法について理解及び検証を行う。

2．内部ネットワークでのログ取得

侵入後に行われる内部ネットワークでの内部侵入・調査段階においてサイバー攻撃の兆候として判断できるログ取得について検討する。

3．リアルタイムのサイバー攻撃対策

内部ネットワークにおけるログ監視から、サイバー攻撃の兆候と判断できる事象に対する対応を検討する。

攻撃手法を理解し、ログ収集を実証してみよう ！

標的型サイバー攻撃の理解

標的型サイバー攻撃

[事前調査]

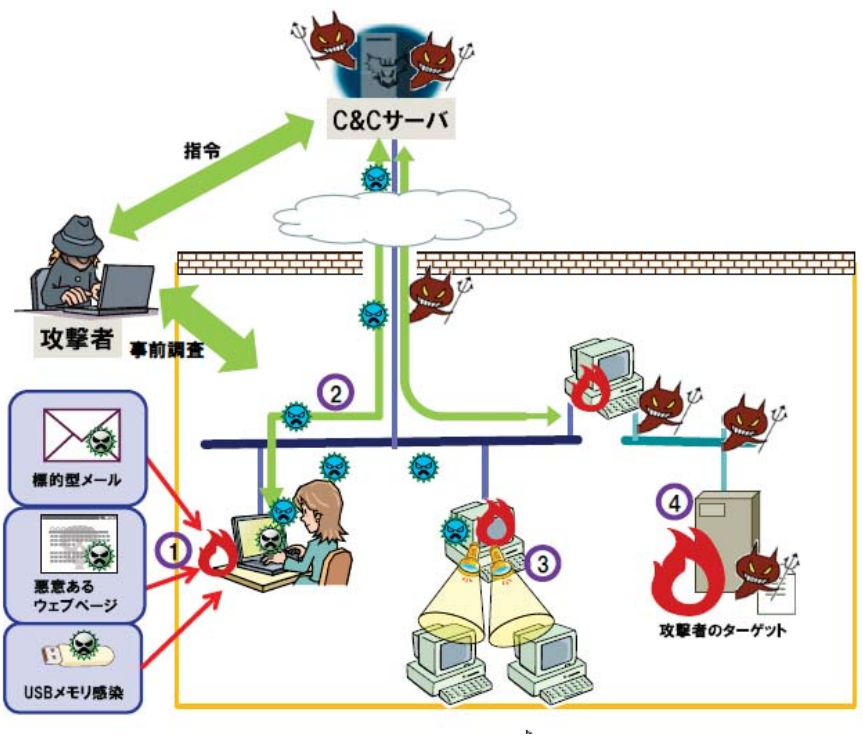
[初期潜入]

[攻撃基盤構築]

[内部侵入・調査]

[攻撃最終目的の遂行]

[目的実行]
（情報搾取・破壊）



※参照元：独立行政法人情報処理推進機構（IPA）「標的型サイバー攻撃の実態と対策」

実証プロジェクトとして着目したポイント

[事前調査]

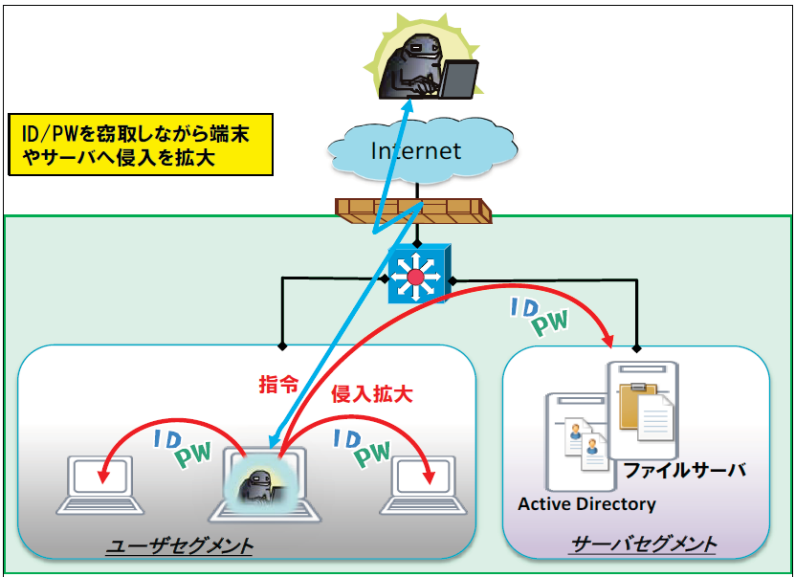
[初期潜入]

[攻撃基盤構築]

[内部侵入・調査]

[攻撃最終目的の遂行]

[目的実行]
（情報窃取・破壊）



■ 内部侵入・調査段階での主な手法として
・管理者権限の窃取に利用される **Pass-the-Hash攻撃**
・ファイル転送に利用される **SMB通信**
・リモート実行に利用される **PsExec**

※参照元：独立行政法人情報処理推進機構（IPA）「標的型サイバー攻撃の実態と対策」

Pass-the-Hash

ID:NAKAMURA
PWD:zTosk91!2p

通常のログイン

Hash化されたデータ送信

ログイン成功

サーバ

実際保存されているNAKAMURAさんのパスワードのHash
NAKAMURA:1001:NO PASSWORD**********:611BC9FF08C0113832E03C47E49F55F:::

Pwdump、Cachedump、lsIsass
などを利用してHash取得

Pass-the-Hashによるログイン

Hash化されたデータ送信

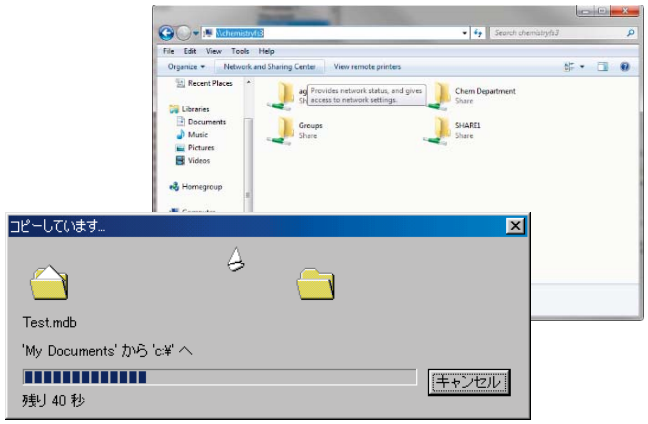
ログイン成功

パスワードを
知らなくても
ログインが出
来てしまう。

※参考元：http://www.microsoft.com/en-us/download/details.aspx?id=36036

SMBによる実行ファイル転送

SMBは、Windowsネットワーク上でリソース（フォルダやプリンタなど）を共有するために用いられるプロトコル。SMBによるファイル転送とはWindows環境で一般的なネットワークドライブへファイルをコピーすることを言う。



SMB通信のログ

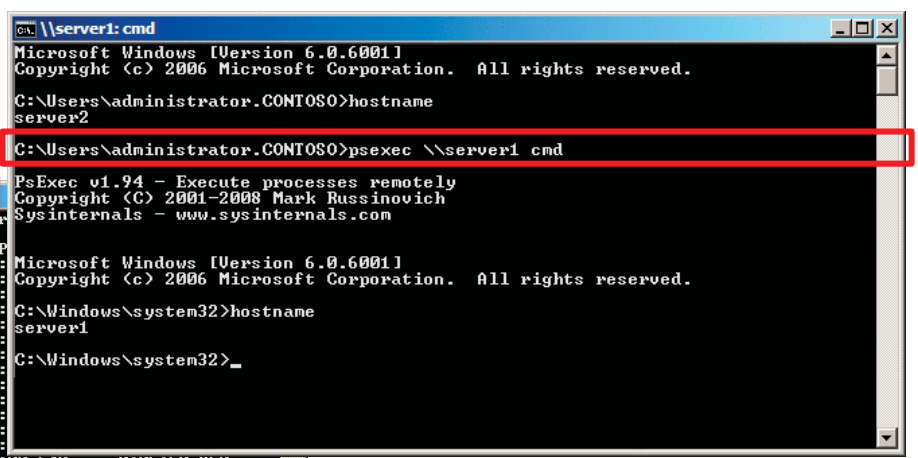
```
Protocol","Length","Info"
"192.168.50.45","192.168.50.55","SMB","142","Negotiate Protocol Request"
"192.168.50.55","192.168.50.45","SMB","143","Negotiate Protocol Response"
"192.168.50.45","192.168.50.55","SMB","243","Session Setup AndX Request, NTLMSSP_NEGOTIATE"
"192.168.50.55","192.168.50.45","SMB","395","Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_
"192.168.50.45","192.168.50.55","SMB","555","Session Setup AndX Request, NTLMSSP_AUTH, User: WORKGROUP\\test"
"192.168.50.55","192.168.50.45","SMB","147","Session Setup AndX Response"
"192.168.50.45","192.168.50.55","SMB","129","Tree Connect AndX Request, Path: \\\\192.168.50.55\\IPC$"
"192.168.50.55","192.168.50.45","SMB","104","Tree Connect AndX Response"
"192.168.50.45","192.168.50.55","SMB","131","Tree Connect AndX Request, Path: \\\\192.168.50.55\\ADMIN$"
"192.168.50.55","192.168.50.45","SMB","107","Tree Connect AndX Response"
"192.168.50.45","192.168.50.55","SMB","137","Open AndX Request, FID: 0x8000, Path: \\KZxdQWuo.exe"
"192.168.50.55","192.168.50.45","SMB","123","Open AndX Response, FID: 0x8000"
"192.168.50.45","192.168.50.55","SMB","621","Write AndX Request, FID: 0x8000, 500 bytes at offset 0"
"192.168.50.55","192.168.50.45","SMB","105","Write AndX Response, FID: 0x8000, 500 bytes"
"192.168.50.45","192.168.50.55","SMB","621","Write AndX Request, FID: 0x8000, 500 bytes at offset 500"
"192.168.50.55","192.168.50.45","SMB","105","Write AndX Response, FID: 0x8000, 500 bytes"
"192.168.50.45","192.168.50.55","SMB","621","Write AndX Request, FID: 0x8000, 500 bytes at offset 1000"
"192.168.50.55","192.168.50.45","SMB","105","Write AndX Response, FID: 0x8000, 500 bytes"
"192.168.50.45","192.168.50.55","SMB","621","Write AndX Request, FID: 0x8000, 500 bytes at offset 1500"
```

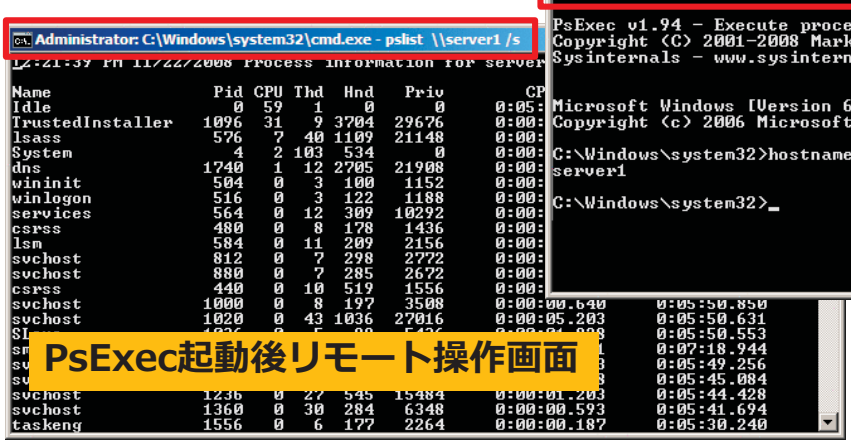
SMB通信のログをみると実行ファイルがリモートへ転送される。

PsExec実行

PsExec は、
ローカル システムとリモート システムの管理をサポートするツールである PsToolに入っているツールの一つ。
Windows標準ではないがマイクロソフト純正の無償ツールであり、インストールの手間もほとんど要らず、事前の設定も最小限で済む。GUIベースのプログラムには適さないが、コマンドライン・プログラムであれば、ローカルで実行するのとほとんど変わらない感覚で利用できる。

PsExec起動画面





PsExec起動後リモート操作画面

実証プロジェクトの推進結果

検証から得られたSMB通信のログ取得ポイント

内容	SMBコマンド	一般ファイル/フォルダー共有	PsExec単体の実行	Metasploit のPsExec実行時
SMB認証	Negotiate Protocol Request/Response	◎	◎	◎
SMBセッション確立	Session Setup AndX RequestResponse	◎	◎	◎
共有リソース接続１	Tree Connect AndX Request/Response Path: ¥¥¥¥server ip¥¥IPC$	◎	◎	◎
共有リソース接続２	Tree Connect AndX Request/Response Path: ¥¥¥¥server ip¥¥ADMIN$	×	◎	◎
PsExecファイル転送時のファイル名	NT Create AndX Request, FID: 0xc000, Path: ¥¥...	-	PSEXESVC.EXE	ランダムファイル名.EXE
PsExecの保存場所		-	C:¥windows	C:¥windows
サービス制御マネージャとの接続	SVCCTL OpenSCManagerW, CreateServiceW, StartServiceW, CloseServiceHandle request/response ¥¥¥¥server_ip	×	◎	◎
PsExec終了時		-	◎ PsExecファイルの削除	× （smb通信なし）PsExecファイルの削除
ターゲットPCでの痕跡			PSEXESVC.EXE-35EFACCF.pf	左記と同様のファイル

プロタイプ開発、実証実験の結果

■ **プロトタイプ開発**

検証から得られらたSMB通信のログ取得ポイント

- ADMIN$の共有
- 実行ファイルの転送（「*.exe」ファイル）

– 詳細は、第二部 「プロトタイプ開発の概要、実機デモ」にてご紹介

■ **実ネットワーク環境における実証実験**

– モニタリング実施中（3-4月）

区分	モニタリング時の運用状況	結果
A社、B社	端末数は、20-50台 ファイルサーバ運用	*.exe ファイル転送時にログ取得
C社	端末数は、50-100台 ファイルサーバ運用	ログ取得無し
D社	端末数は、20台以下 ファイルサーバ無し	ログ取得無し

実証プロジェクトを通して

実証プロジェクト推進を通して

■ 結果

内部ネットワークにおいて、ネットワークトラフィックを監視し、
一定条件下でネットワーク上の通信ログを取得することができた。
（リアルタイムのモニタリングによるアラート及び対応は未実施）

■ 課題

・実ネットワーク環境でのモニタリング数が少ない。
・攻撃手法の変化に対するネットワークログ取得の仕組み
・有志による実証プロジェクト推進における課題

■ 意義

・攻撃の兆候を事前に検知するために、ネットワークログの活用
・自組織のネットワークトラフィックの正常時の特性を確認する方法
・防御側の意思を反映したネットワークのモニタリング、挙動監視
・リアルタイムのアラートと対応の自動化の可能性

ありがとうございました。

本資料に関する連絡先：

朴 昶昱（バク チャンウク）
株式会社パイオリンク
〒160-0022　東京都新宿区新宿1-34-14
TEL： 03-5367-2547
URL： www.piolink.co.jp
Mail： cwpark@piolink.co.jp