Internet Week 2012
CSIRTの今とこれから
CSIRTの運用に役立つツールの紹介

CSIRT エヴァンジェリスト
NCA 運営委員
NTT-CERT
杉浦芳樹

2012年11月19日

ツールの分類

分析ツール

- Forensics
- Malware
- Log Analysis

情報収集/共有

- Public Monitoring
- Social Media

案件管理

- チケッティングシステム
- DBシステム

分析

Forensics

EnCase

- 実質的な標準ツール
- 様々なベンダーが取り扱い

FTK 3

- もう一つのフォレンジックツール

Sleuthkit

- Open Source
- http://www.sleuthkit.org/

Malware分析

IDA Pro

- 逆アセンブル
- デバッガーも付属

Ollydbg

- デバッガー

libemu

- シェルコードの実行をエミュレーション

Log analysis （ログ分析）

各種ログの記録

- Syslog(Web、Mail、DNS)、snmp
- Firewall、IDS、IPS、Anti Virus
- Event Log、Audit

分析ツール

- AWStats (apacheのログ解析)
- Log Parser (IIS、各種ログ)、Kiwi Syslog Server
- grep, awk, perl, 各種自作スクリプト,目grep

SIEM （Security Information and Event Management）

- 複数の異なる製品からログを収集・解析、統計解析・相関分析
- 代表的製品 (RSA enVison, ArcSight, splunk)

その他の重要なツール

HDD Duplicator

・元のHDDを触らないようにする

HDD

・様々なタイプの様々なサイズ

ロックワイヤー付きカバン

・HDD等の運搬に必要

情報収集/共有

情報収集の目的

1. ・脅威・リスクを見つける
2. ・欲しい人に情報を届ける
3. ・見る目を養う

ソース

Dragon New Bite

- https://lists.cymru.com/mailman/listinfo/ians_dragon_newsbytes

セキュリティホールメモ

- http://www.st.ryukoku.ac.jp/~kjm/security/memo/

F-Secureブログ

- http://blog.f-secure.jp/

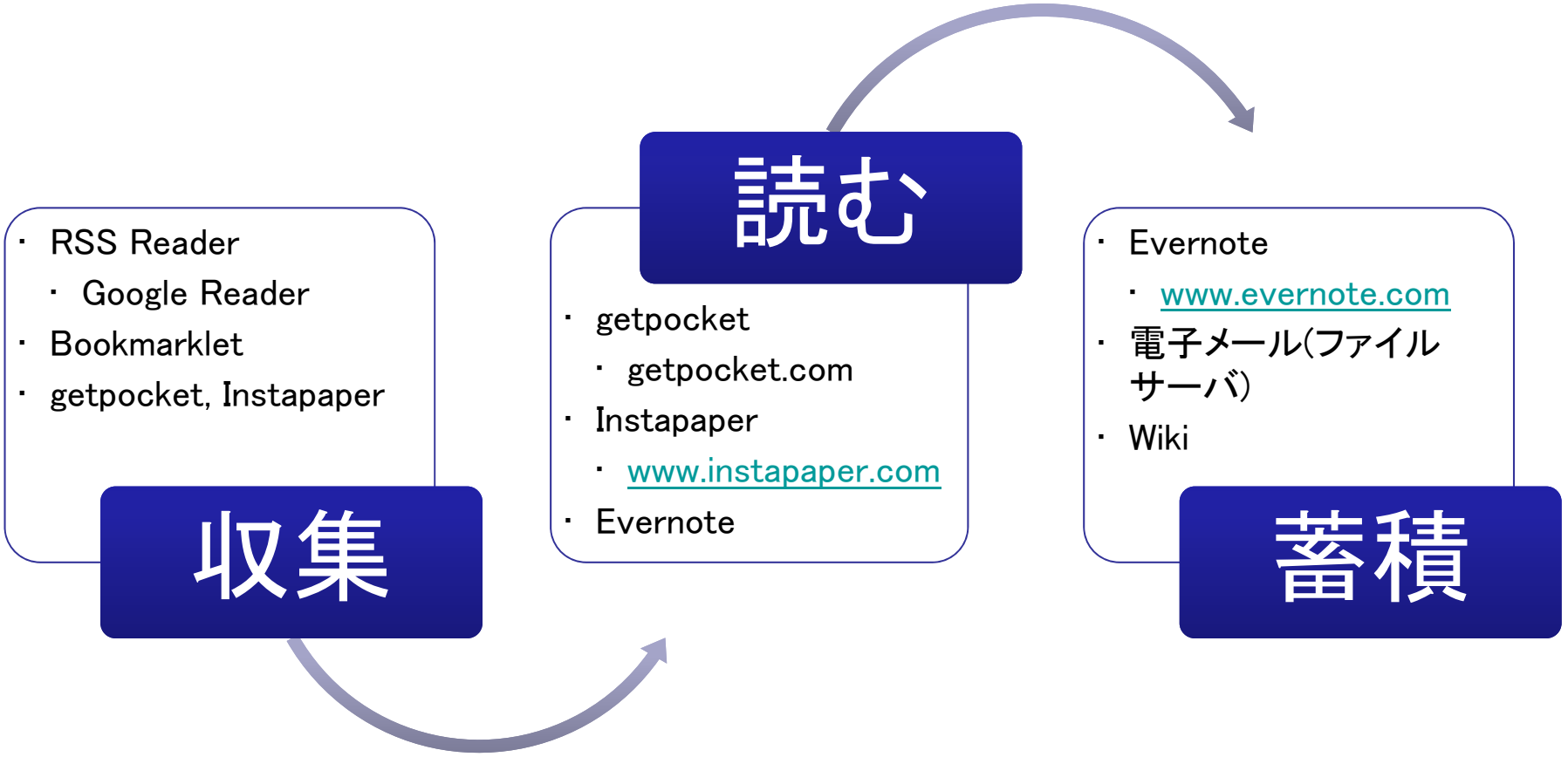
日本のセキュリティチーム

- http://blogs.technet.com/b/jpsecurity/

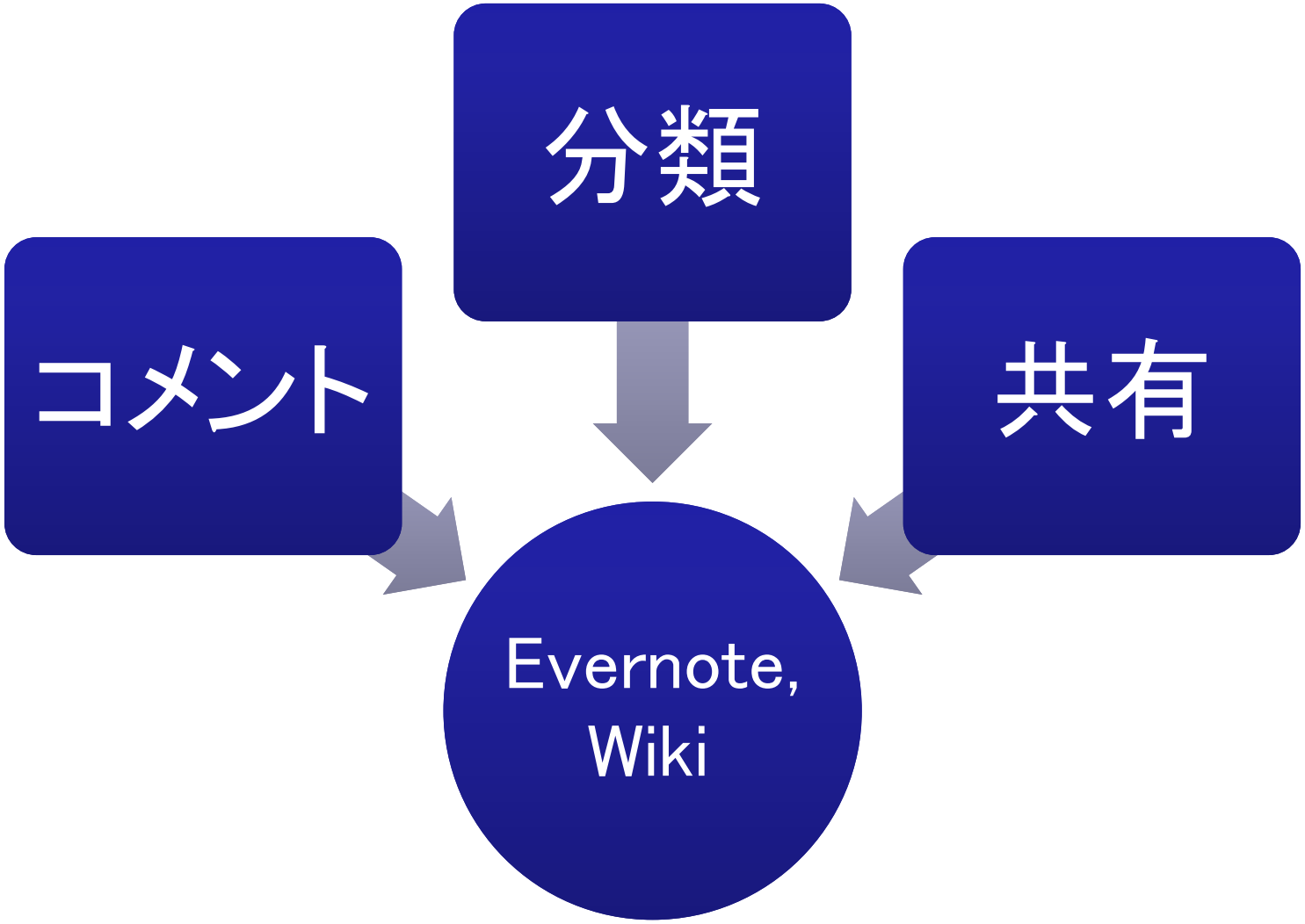
SANS

- http://www.sans.org/

流れ



情報分析



共有

SNS

- Facebook
- Twitter
- Yammar

社内

- メーリングリスト
- 社内Wiki
- ファイルサーバー

案件管理

チケッティングシステム

Remedy

- http://www.bmc.com/ja-JP/products/remedy-itsm
- カスタマイズ可能なサービスマネージメントシステム

RTIR

- ヨーロッパのCSIRTで開発されたCSIRTのためのチケット管理システム
- http://www.bestpractical.com/rtir/index.html

Bugzilla

- http://www.bugzilla.org/

エクセルやimap等のシステムを使用するのも一案
PostgrsqlやMySQLで自作

どのような項目が必要か

基本情報

- チケット番号、案件ID
- タイトル、対応者
- 状態(Open, close, Wait)

付加情報

- 対応履歴、リファレンス
- 重要性、緊急度
- クローズ理由、必要になったスキル

どのような項目が必要か

カテゴリー

- インシデント
- 脆弱性
- 技術問い合わせ

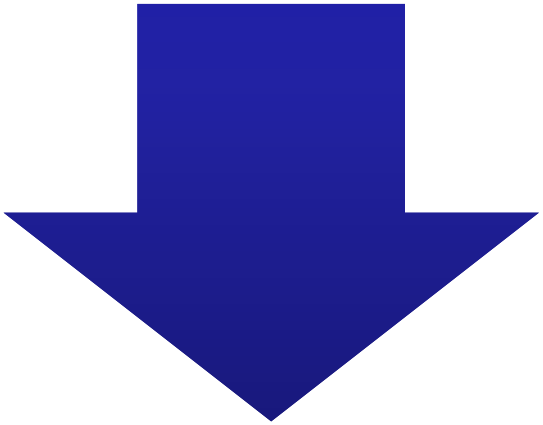
サブカテゴリ

- Malware感染
- Phishing
- 情報漏えい

検索

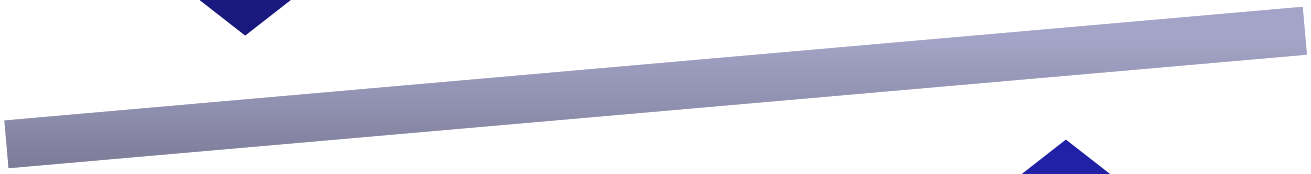
- カテゴリー
- ハンドラー
- 状態
- 案件登録日(期間)
- 最終対応日

統計分析



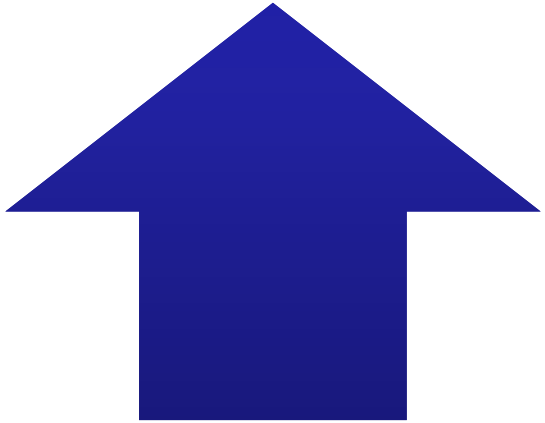
案件数の推移

- 月単位
- 案件の種別



全体の稼働

- メール数
- 稼働時間



その他のツール

コミュニケーション

- PGP(GnuPG)
- メーリングリスト、チャット、Wiki、SNS
- ファックス、電話

物理

- 金庫、専用ルーム
- ホワイトボード
- 付箋紙、大きな紙(A0)

システム

- 専用システム(IR、分析、実験)
- 専用ネットワーク

メンバーでなくても参加できる会合などもあります。
(構築を検討されている皆さんと既存のメンバーの意見交換の場)

CSIRTに関する相談:　　csirt-pr@nca.gr.jp
NCAおよび加盟に関して:　nca-sec@nca.gr.jp

CSIRT
日本シーサート協議会

http://www.nca.gr.jp/