

第18回 サイバー犯罪に関する白浜シンポジウム

平成26年5月23日(金)

情報通信研究機構における ネットワークセキュリティの研究開発



独立行政法人 情報通信研究機構(NICT)
ネットワークセキュリティ研究所

平 和昌



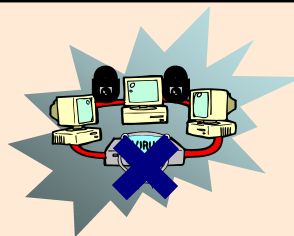
独立行政法人情報通信研究機構(NICT)

- 役職員： 理事長 坂内正夫（前 国立情報学研究所長）
職員 937名（非常勤職員を含む 平成26年4月1日現在）
- 平成26年度予算： 一般会計 280.7億円（運営費交付金）
- 所在地： 本部 東京都小金井市
研究所 神奈川県横須賀市、兵庫県神戸市、
京都府相楽郡精華町（けいはんな）
技術センター 茨城県鹿嶋市、石川県能美市 等
- 主な業務：
 - ・情報通信分野の研究開発及び成果の普及
 - ・日本標準時の決定、標準電波の送信
 - ・電波の伝わり方の予報・警報
 - ・民間、大学等が行う情報通信分野の研究開発の支援 等

NICTが取り組む研究開発(第3期中期計画)

ネットワーク基盤技術

情報量の増大、消費電力の低減等の要請に応える
安心・安全なネットワークを実現する



インターネットの次のNW(新世代NW)の研究開発
・光通信・ネットワーク技術、無線通信技術、**情報セキュリティ技術**

ユニバーサルコミュニケーション基盤技術

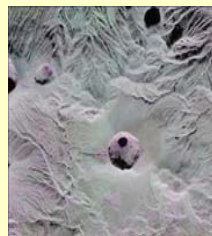
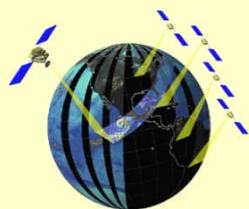
様々な壁を超えて人に優しい
コミュニケーションを実現する



多言語間通訳技術、情報から知識に結びつける情報処理技術、
立体映像等の臨場感あふれるコミュニケーション技術

電磁波センシング基盤技術

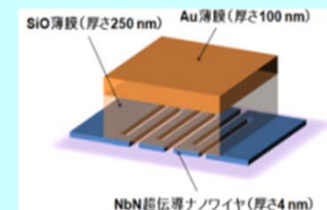
高精度な時刻情報や環境情報を
容易に安全に利用できるようにする




日本標準時・電波時計電波発射、レーダ等の地球センシング
技術、宇宙天気技術、EMC電磁波影響評価技術

未来ICT基盤技術

未来の情報通信にパラダイムシフトをもたらす



脳情報融合技術、ナノ情報通信技術。量子通信技術、
テラヘルツ帯利用技術

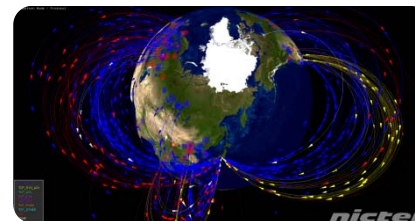


NICTERと そのスピンオフ技術

NICTERとそのスピノフ技術たち

1. インシデント分析センタ


NICTER



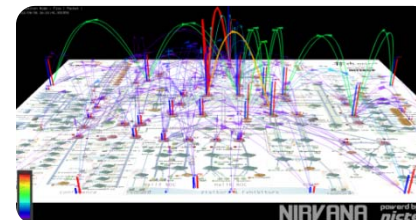
2. 対サイバー攻撃アラートシステム

DAEDALUS



3. ネットワークリアルタイム可視化システム


NIRVANA



4. サイバー攻撃統合分析プラットフォーム

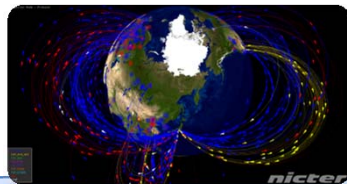

NIRVANA改



ダークネット観測

ライブネット観測

鳥の目/虫の目

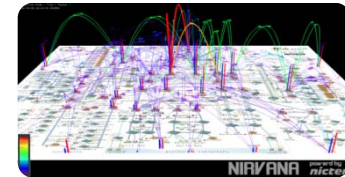


NICTER

グローバル観測
(ダークネット)



DAEDALUS



NIRLVANA
NIRLVANA改

ローカル観測
(ライブネット)

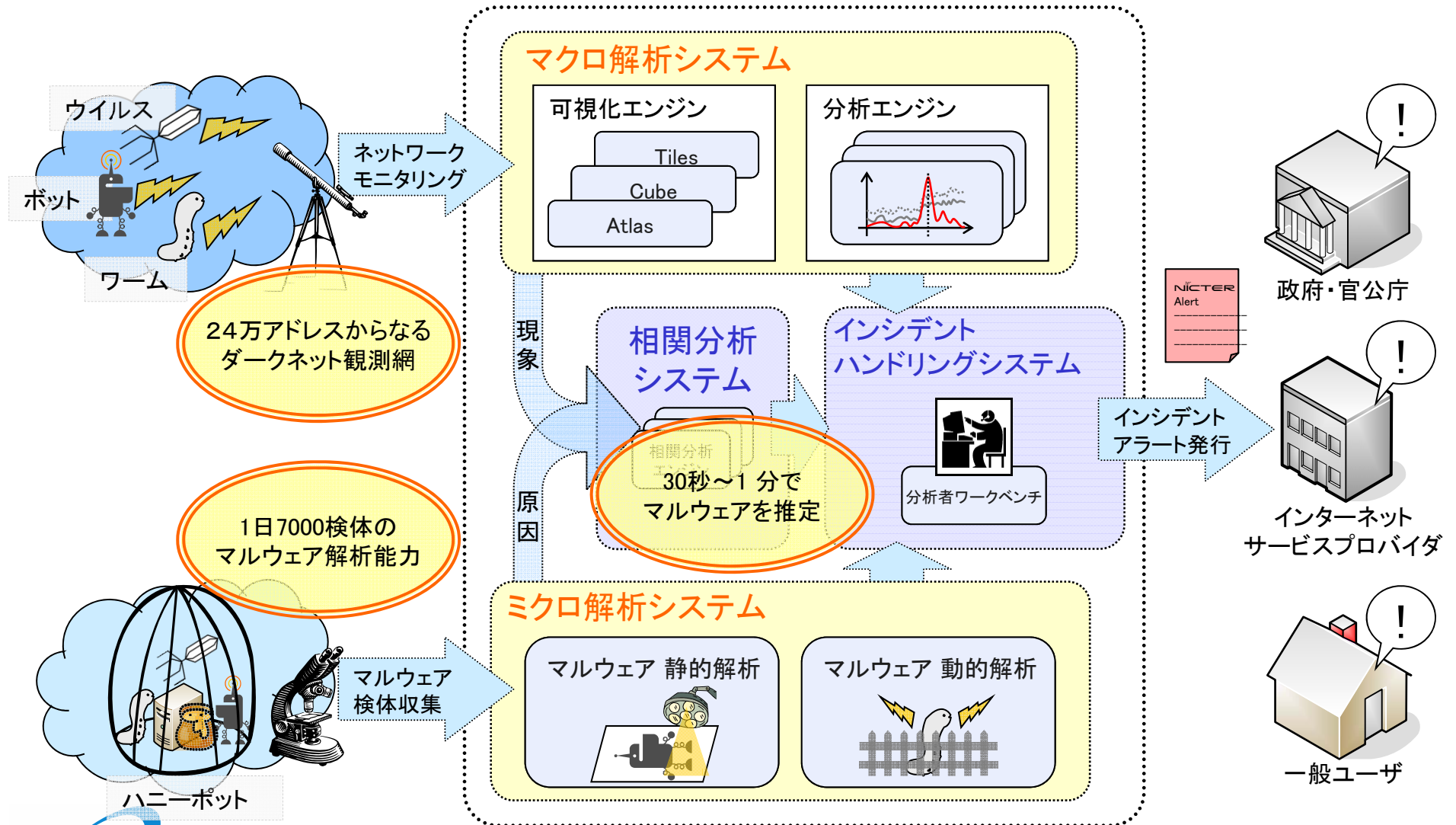


インシデント分析センター

NICTER

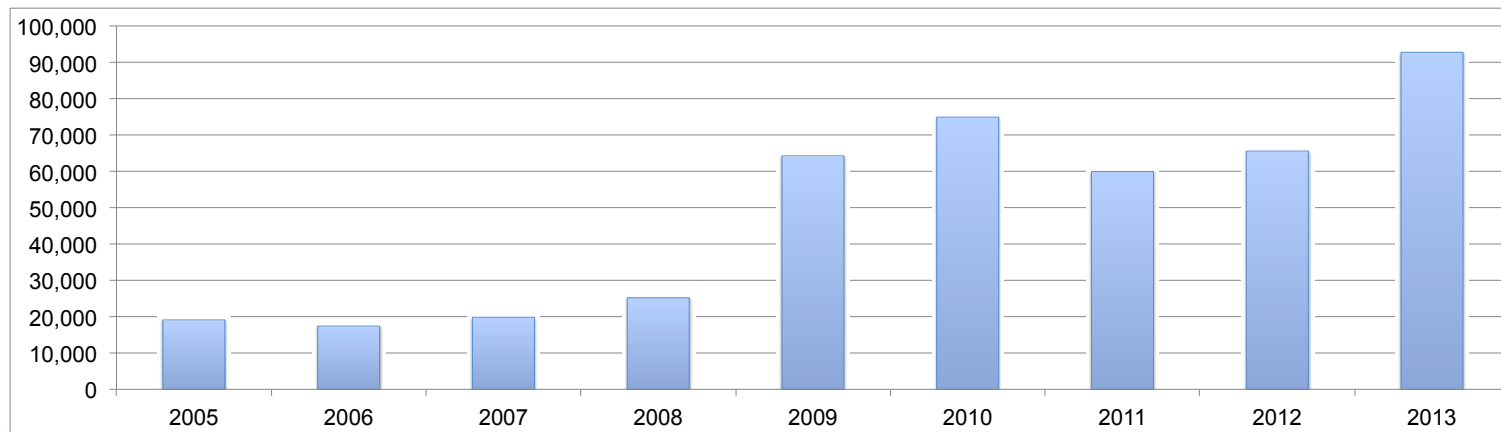
(**N**etwork **I**ncident analysis **C**enter
for **T**actical **E**mergency **R**esponse)

NICTERの全体像



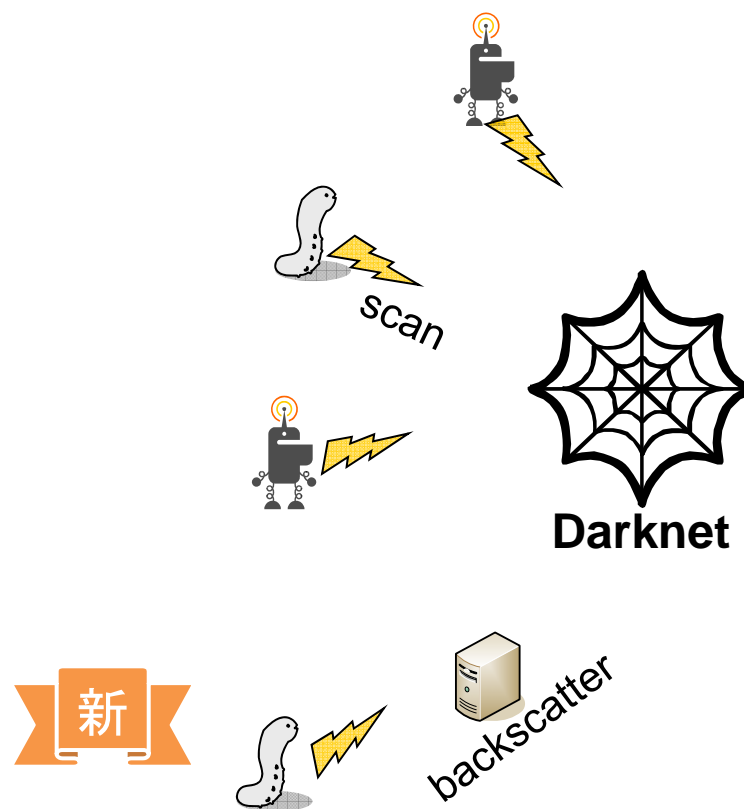
NICTERダークネット観測統計

年	年間 総観測パケット数	観測IPアドレス数	1IPアドレス当たりの 年間総観測パケット数
2005	約 3.1億	約1.6万	約19,066
2006	約 8.1億	約10万	約17,404
2007	約 19.9億	約10万	約19,855
2008	約 22.9億	約12万	約25,242
2009	約 35.7億	約12万	約64,304
2010	約 56.5億	約12万	約74,952
2011	約 45.4億	約12万	約59,987
2012	約 77.9億	約19万	約65,614
2013	約128.8億	約21万	約92,835



ダークネットで何が見えているのか？

- **マルウェアによるスキャン**
 - ✓ ワーム型マルウェアの探索活動
 - ✓ マルウェア感染の大局的傾向
 - ✓ 感染爆発の前兆
- **DDoS攻撃の跳ね返り**
 - ✓ 送信元IPアドレス偽装されたSYN Flood
 - ✓ 被攻撃サーバからの応答(SYN-ACK)
 - ✓ DDoS攻撃の早期検知(1パケット目から)
- **設定ミス**
 - ✓ 組織内ダークネット
- **リフレクション攻撃の準備活動**
 - ✓ DNS Open Resolver探索
 - ✓ NTP探索 etc.



対サイバー攻撃アラートシステム
DAEDALUS

(Direct Alert Environment for
Darknet And Livenet Unified Security)

境界防御技術とDAEDALUS

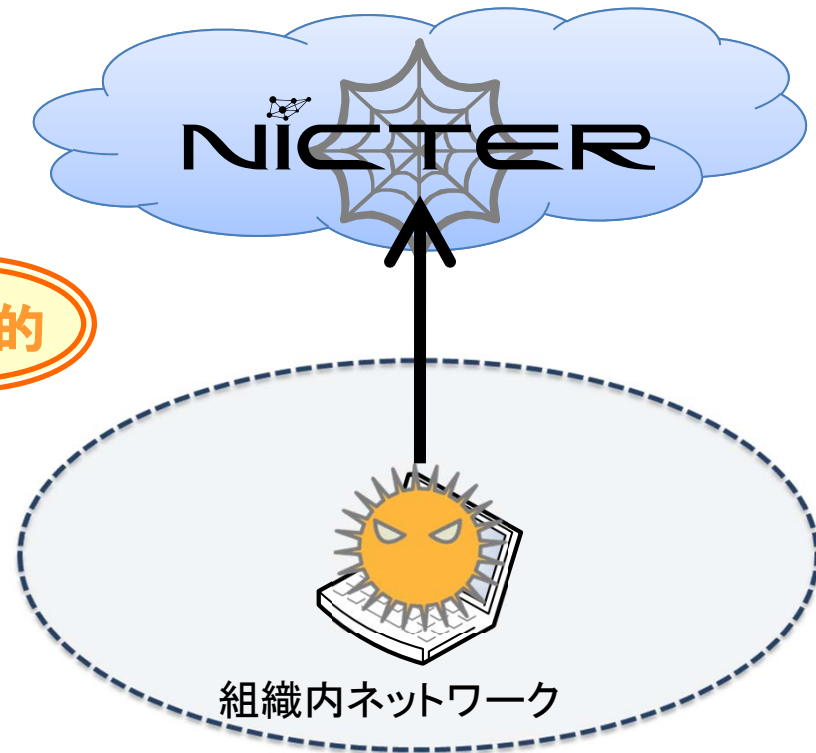
境界防御技術

組織外からの攻撃をネットワーク境界で検出



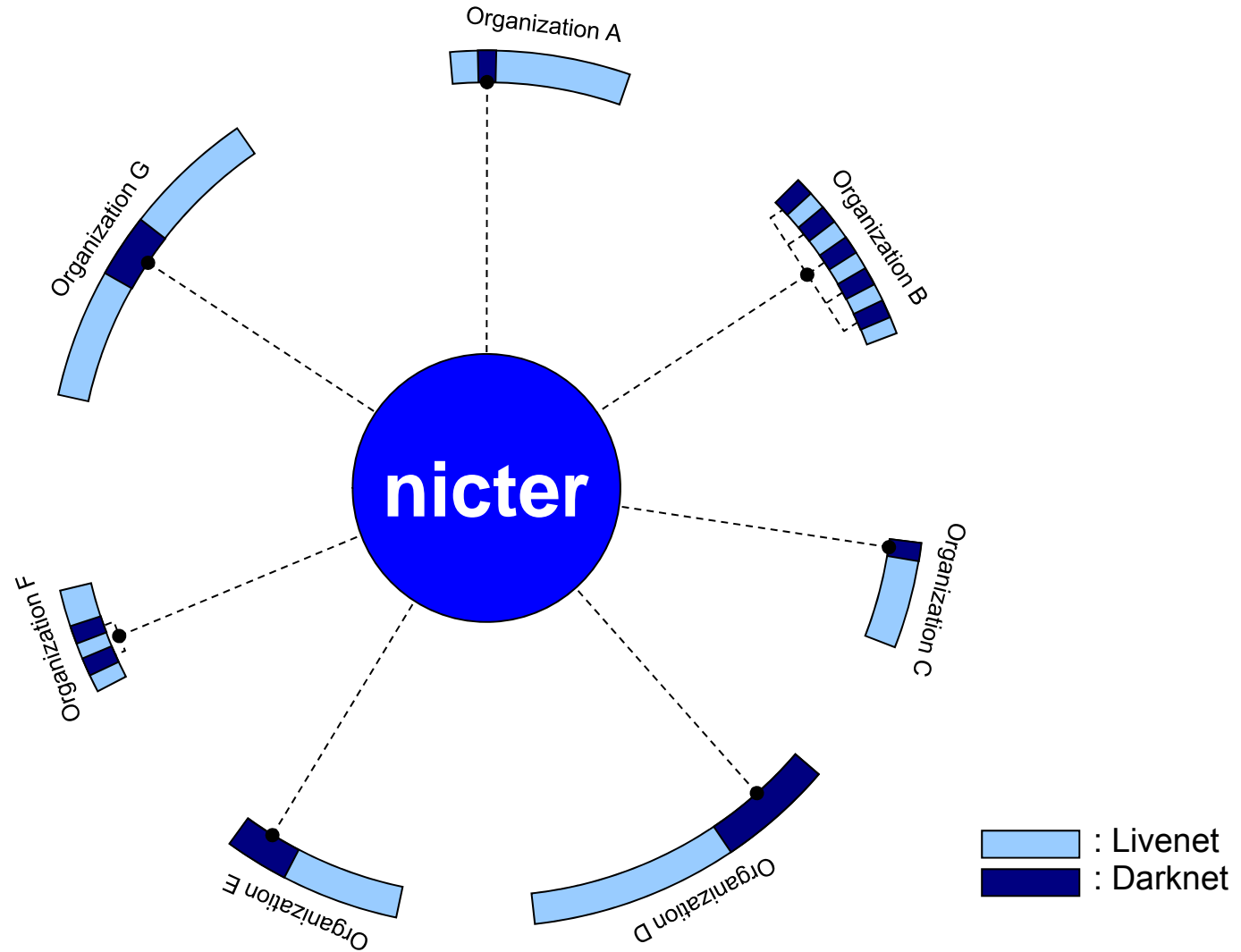
DAEDALUS

組織内からの攻撃をネットワーク広域で検出



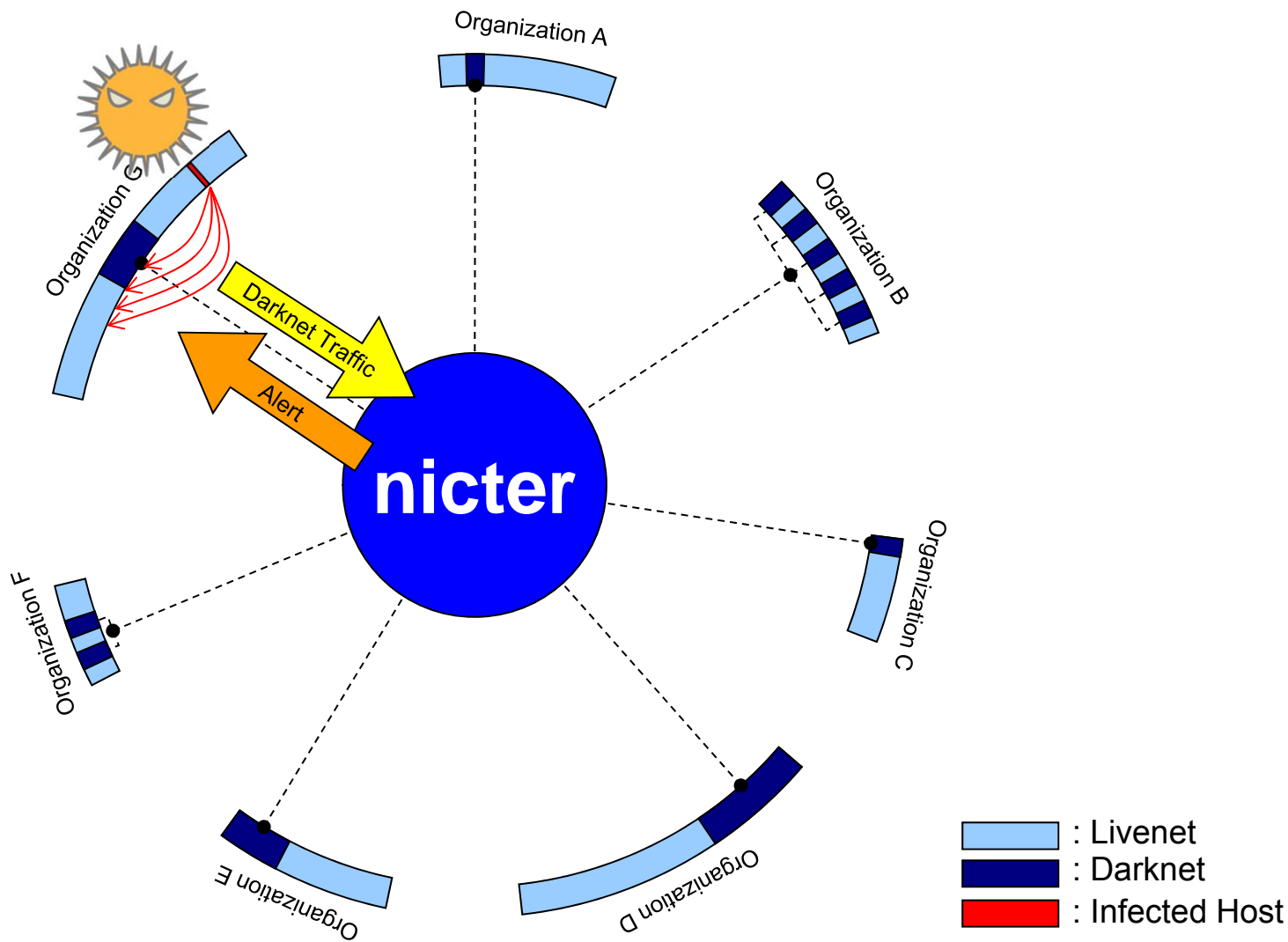
相補的

想定環境



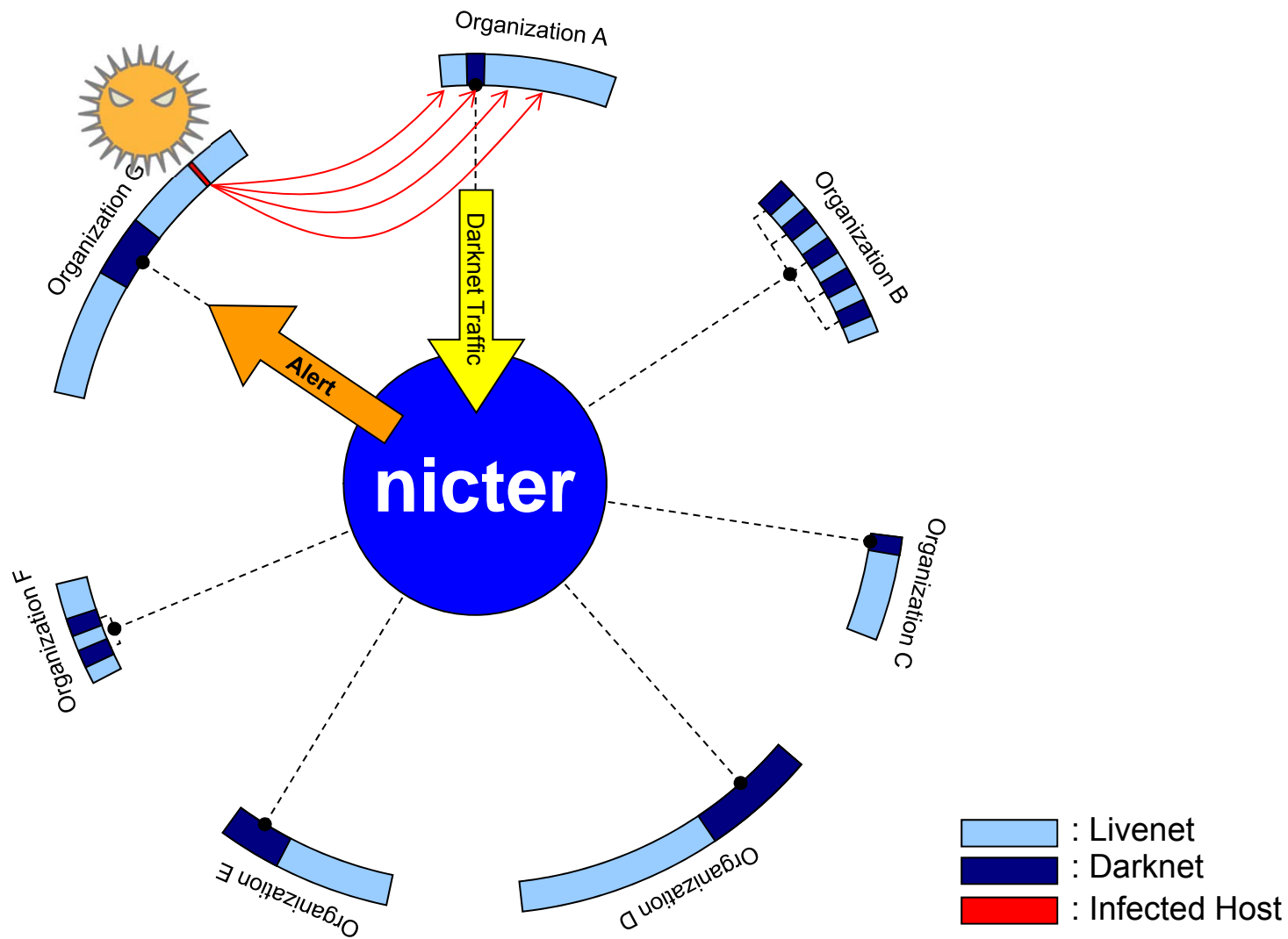
ケース1

組織内感染(内部アラート)



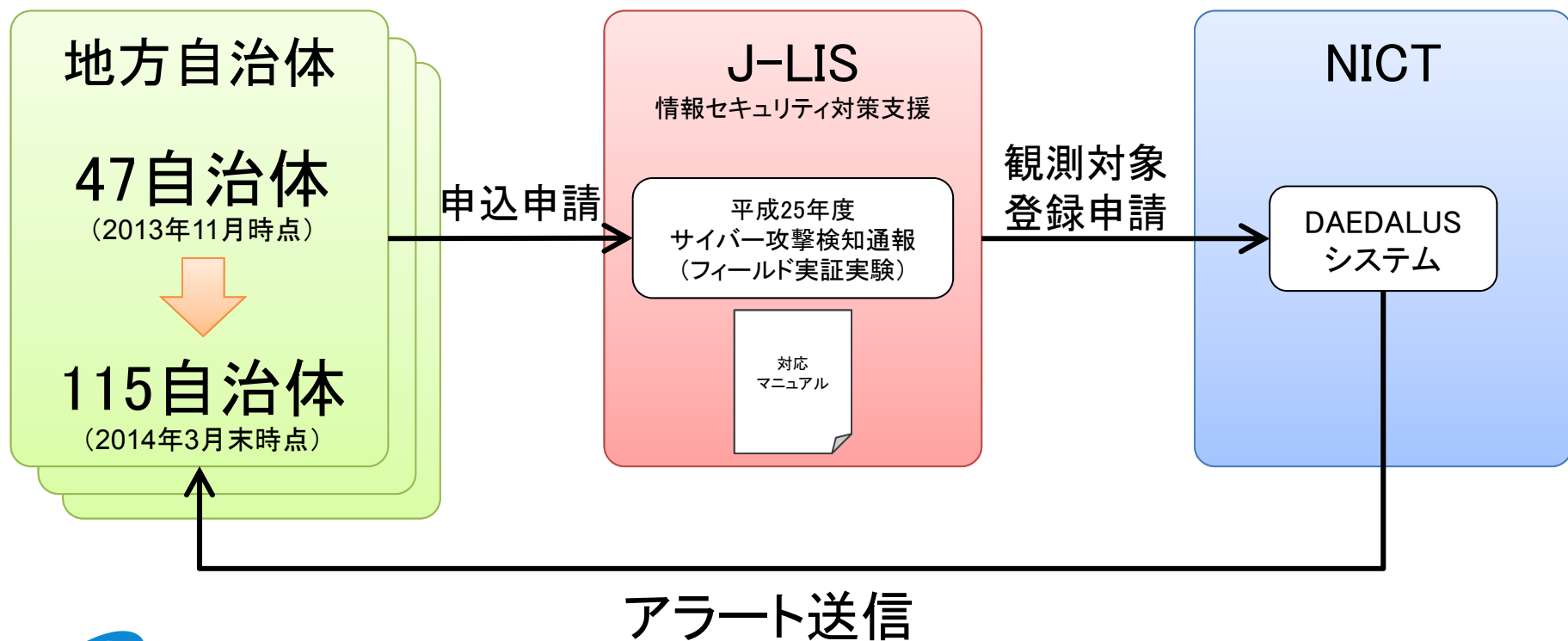
ケース2

組織外への攻撃(外部アラート)



DAEDALUSの成果展開:国内展開 地方自治体へのアラート提供

- 2013年11月1日より、地方自治体に向けてアラート送信開始
 - 地方公共団体情報システム機構(J-LIS)を窓口として自治体より申込受付
 - アラート発生時の対応マニュアルをNICTとJ-LISで整備



ネットワークリアルタイム可視化システム


NIRLVANA

(nicter real-network visual analyzer)

サイバー攻撃統合分析プラットフォーム

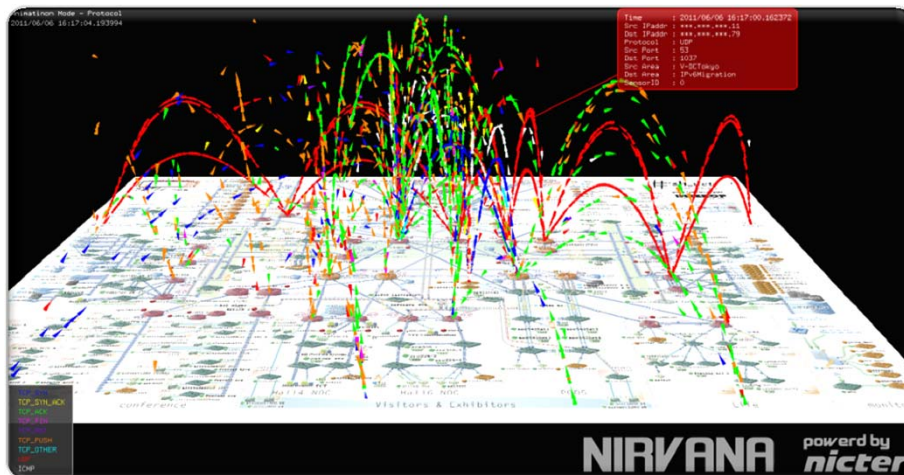

NIRLVANA 改

NIRVANA

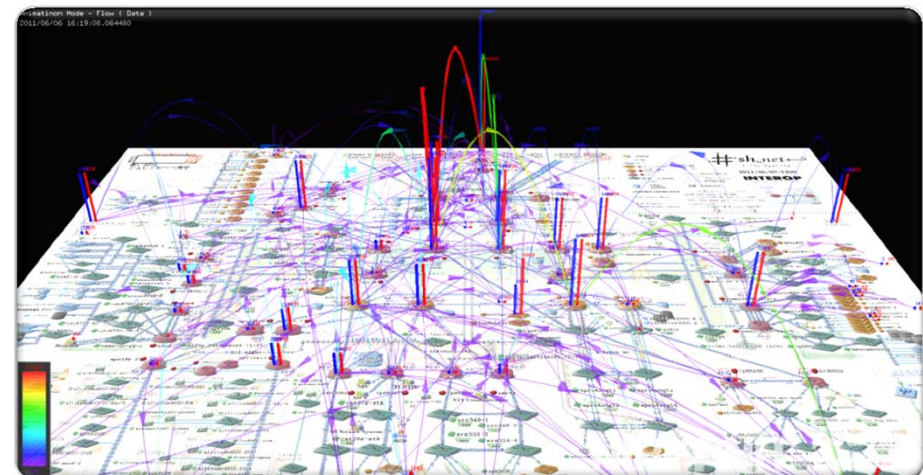
ライブネット
トを
見える化

ネットワーク管理者
の負荷を軽減
(輻輳・切断等の障害、
設定ミス等を瞬時に発見可能)

管理コスト
の軽減
(管理の迅速化
・効率化)



パケットモード



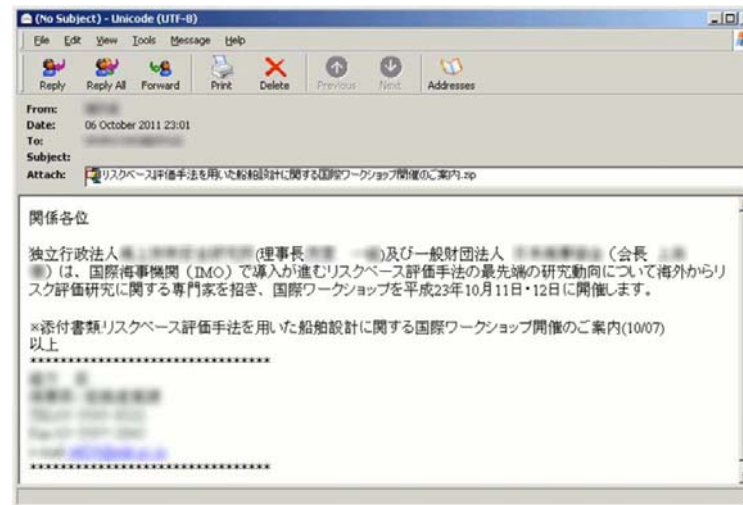
フローモード

標的型攻撃

- 特定組織を標的にした長期に渡る執拗なサイバー攻撃
- 周到な内容のメールに添付されたマルウェアで組織に侵攻
- 組織内ネットワークに潜伏・浸透し重要情報を収奪

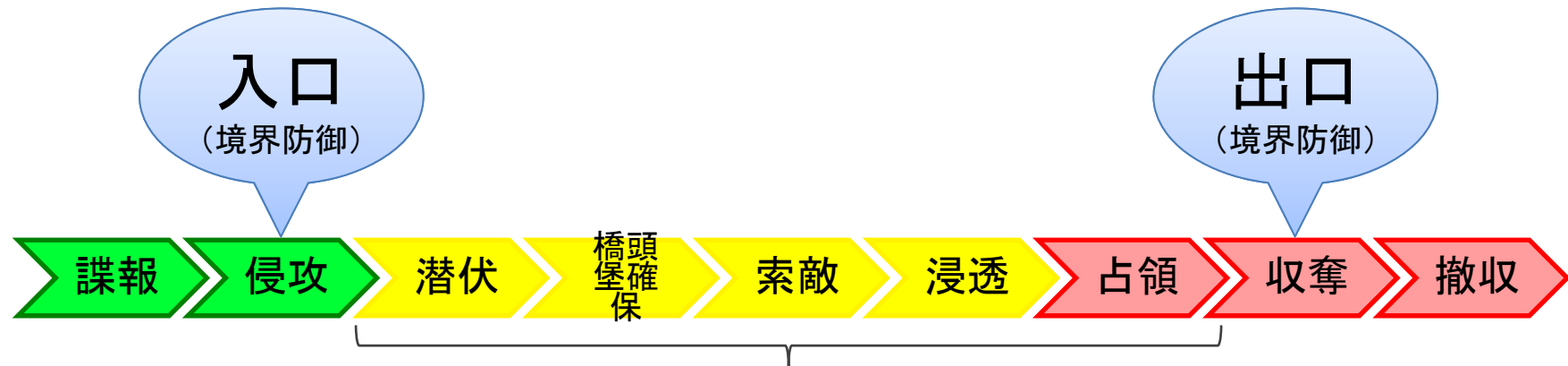


標的型攻撃のKill Chain

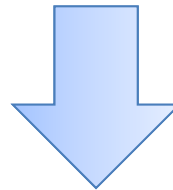


TECH.ASCII.jp「9.5社に1社が対象に！シマンテックが明かす日本の標的型攻撃」
<http://ascii.jp/elem/000/000/652/652712/> (2011-11-30)

入口対策/出口対策



ネットワークの内側でも対策を！
(組織内ネットワークのリアルタイム観測・分析)



NIVANA 改

= NIVANA + セキュリティ分析機能

まとめ

- **ダークネット**: 広がる応用・高まる効用
 - ✓ ワーム型マルウェアの傾向把握・大規模感染検知
 - ✓ DDoS攻撃の早期検知
 - ✓ リフレクション攻撃の準備活動検知
 - ✓ 外部へのアラート提供
- **ライブネット**: 入口/出口、次の一手
 - ✓ 組織内ネットワークのリアルタイム観測・分析
 - ✓ 新規&既存対策技術を統合したメタ分析
 - ✓ Kill Chainの進行途中で攻撃検知
 - ✓ ビッグデータへの挑戦

SSL/TLSサーバ認証における RSA公開鍵の安全性について

公開鍵認証基盤(PKI)

PKI: Public Key Infrastructure

認証局
(CA: Certificate
Authority)



信頼している

公開鍵証明書を
発行

A



提示



B

Bだと分かる

認証局CAの公開鍵を
用いてCAの署名を検証

Bの公開鍵証明書

認証局CA
による署名

公開鍵暗号(RSAなど)
が使われている

X.509公開鍵証明書

```
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 1 (0x1)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
OU=Certification Services Division,
CN=Thawte Server CA/emailAddress=server-certs@thawte.com
Validity
Not Before: Aug 1 00:00:00 1996 GMT
Not After : Dec 31 23:59:59 2020 GMT
Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
OU=Certification Services Division,
CN=Thawte Server CA/emailAddress=server-certs@thawte.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
00:d3:a4:50:6e:c8:ff:56:6b:e6:cf:5d:b6:ea:0c:
68:75:47:a2:aa:c2:da:84:25:fc:a8:f4:47:51:da:
85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:06:
6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2:
6a:0c:44:38:cd:fe:be:e3:64:09:70:c5:fe:b1:6b:
29:b6:2f:49:c8:3b:d4:27:04:25:10:97:2f:e7:90:
6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f:
5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36:
3a:c2:b5:66:22:12:d6:87:0d
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints: critical
CA: TRUE
Signature Algorithm: md5WithRSAEncryption
07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8e:ca:d9:
a8:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c8:48:
3e:59:43:7d:4f:95:3d:a1:8b:b7:0b:62:98:7a:75:8a:dd:88:
4e:4e:9e:40:db:a8:cc:32:74:b9:6f:0d:c6:e3:b3:44:0b:d9:
8a:6f:9a:29:9b:99:18:28:3b:d1:e3:40:28:9a:5a:3c:d5:b5:
e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9:
b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:89:bc:a3:ff:8a:23:2e:
70:47
```

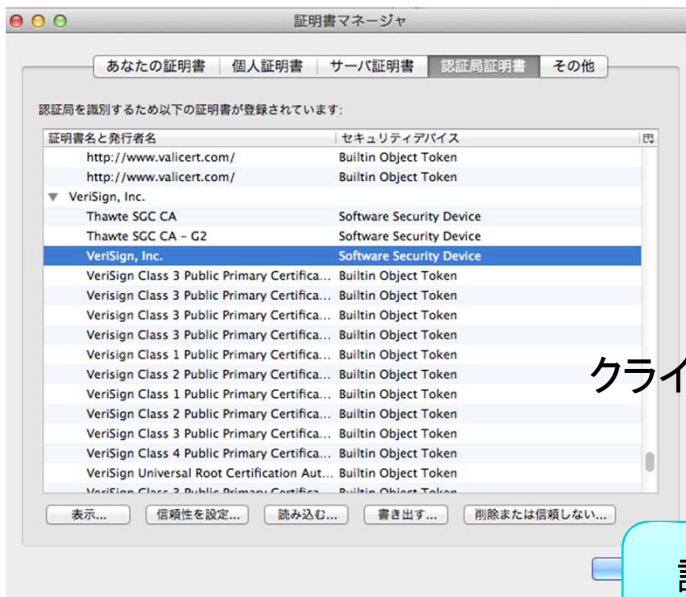
署名対象
データ

- 発行者
- 有効期間
- 主体者
- 主体者の公開鍵情報
公開鍵アルゴリズム
主体者の公開鍵

CAによる署名データ

TLS/SSLにおけるサーバ認証

認証局
(CA: Certificate
Authority)



信頼している

公開鍵証明書を
発行

提示

クライアント

サーバの身元
が確認できる

サーバ

認証局CAの公開鍵を
用いてCAの署名を検証

サーバの公開鍵証明書
(サーバ証明書)

認証局CA
による署名

主要な認証局の公開鍵証明書は
あらかじめブラウザに
組み込まれている

RSA公開鍵への新たな脅威

RSA



Rivest, Shamir, Adleman

- 1977年に発明され、最も利用されている公開鍵暗号
- 大きな合成数の素因数分解が困難であることを安全性の根拠としている
- 公開鍵 (n, e) と秘密鍵 d の鍵ペアを作成し、公開鍵を公開

大きな2つの素数 p, q を生成

公開鍵: $n = p \times q$, e を選択 ($65537 = 2^{16} + 1$ がよく使われる)

秘密鍵: $d = e^{-1} \pmod{(p-1)(q-1)}$

暗号化(平文 m から暗号文 c を作成): $c = m^e \pmod{n}$

復号(暗号文 c からもとの平文 m を得る): $m = c^d \pmod{n}$

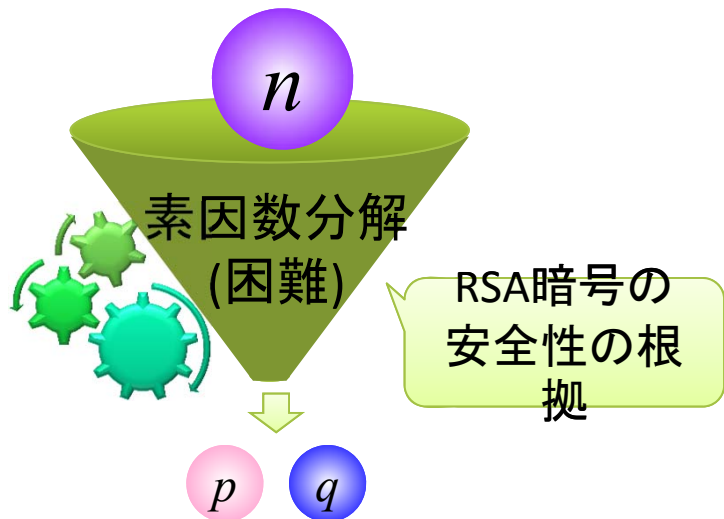
RSA公開鍵への新たな脅威

- 同じ素数を因子として含む公開鍵が多数生成され、公開鍵証明書等に組み込まれて利用されていることが明らかに。
 - Heninger et.al., “Mining your Ps and Qs: Detection of widespread weak keys in network devices”, Usenix Security 2012.
 - TLS scan (約585万, 2011/10)
 - SSH scan (約661万, 2012/2-4)
 - Lenstra et.al., “Public Keys”, CRYPTO 2012.
 - The Electronic Frontier Foundation (EFF)
SSL Observatory (約619万, 2011/11)
 - <https://www.eff.org/observatory>

同じ素因子を含むと、何が起きるのか

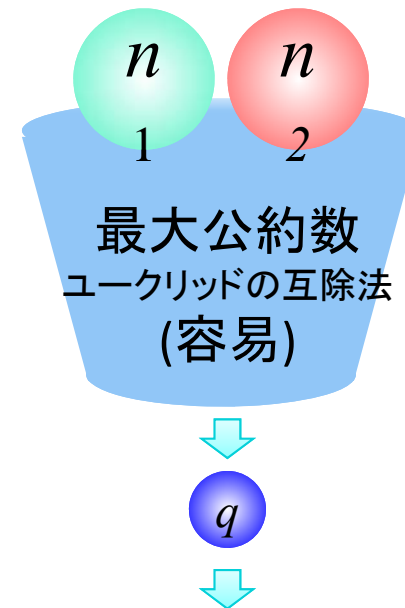
2つの大きな素数: p, q

RSAの公開鍵: $n = p \times q$



2つの公開鍵: n_1, n_2

$n_1 (= p_1 \times q)$ $n_2 (= p_2 \times q)$



2つの公開鍵 n_1, n_2 が
容易に素因数分解できてしまう

$$n_1 \Rightarrow p_1 \times q \quad n_2 \Rightarrow p_2 \times q$$

p_1 q p_2 q

RSA公開鍵への新たな脅威

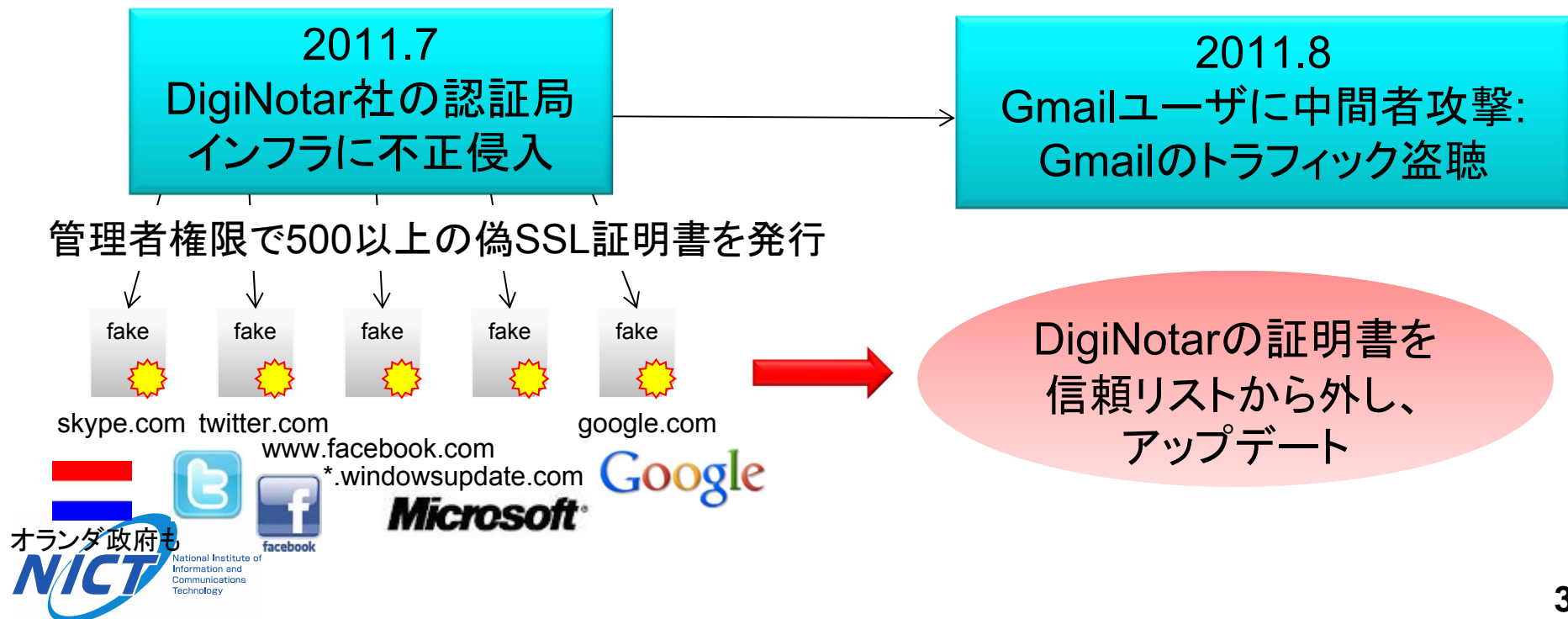
- RSAの安全性は大きな数の素因数分解が難しいことで支えられている。
 - ⇒これまで長い鍵長(2048ビット等)のRSAを使っていれば安全とされてきた。
- 大きな数の素因数分解は難しいが、2つの大きな数の最大公約数を求めることは容易
- もし、2つのRSAの公開鍵に同じ素数が含まれていた場合、最大公約数を求めることで簡単にその素数が分かり、素因数分解でき秘密鍵が暴かれてしまう。

脅威の原因

- RSA鍵生成時に同じ素数が生成されている
 - 素数生成時の乱数生成のseedがランダムでない
 - 特にルーター、ファイアウォールや組み込みデバイス等（物理乱数源を取得する手段が乏しい）
 - RSAの鍵生成時の疑似乱数生成モジュールに脆弱性
 - そもそも9個の素数しか生成しないモジュールも
 - 出荷時のデフォルト鍵がそのまま利用されている

RSA秘密鍵が暴かれると？

- 認証局の秘密鍵が暴かれた場合、認証局になりすまして署名が可能になり、不正SSL証明書などが発行できる → 偽サイトへの誘導など
- [参考事例] DigiNotarの不正証明書問題 (2011年)



課題

- この新たな脅威の実態が把握されていない
 - 発表されたのは過去のある時点での統計情報
 - 現在の状況は不明、個々の実態も不明
 - 日本国内の実態は？
 - 多くのユーザが利用しているサイトは安全なのか



XPIA構築の目的: 実態の把握

公開鍵検証・可視化システム XPIA (エクスピア)

X.509 certificate Public-key
Investigation and Analysis system

XPIAのシステム概要

公開鍵証明書の収集
(クローリング)



RSAの公開鍵を抽出



公開鍵の解析

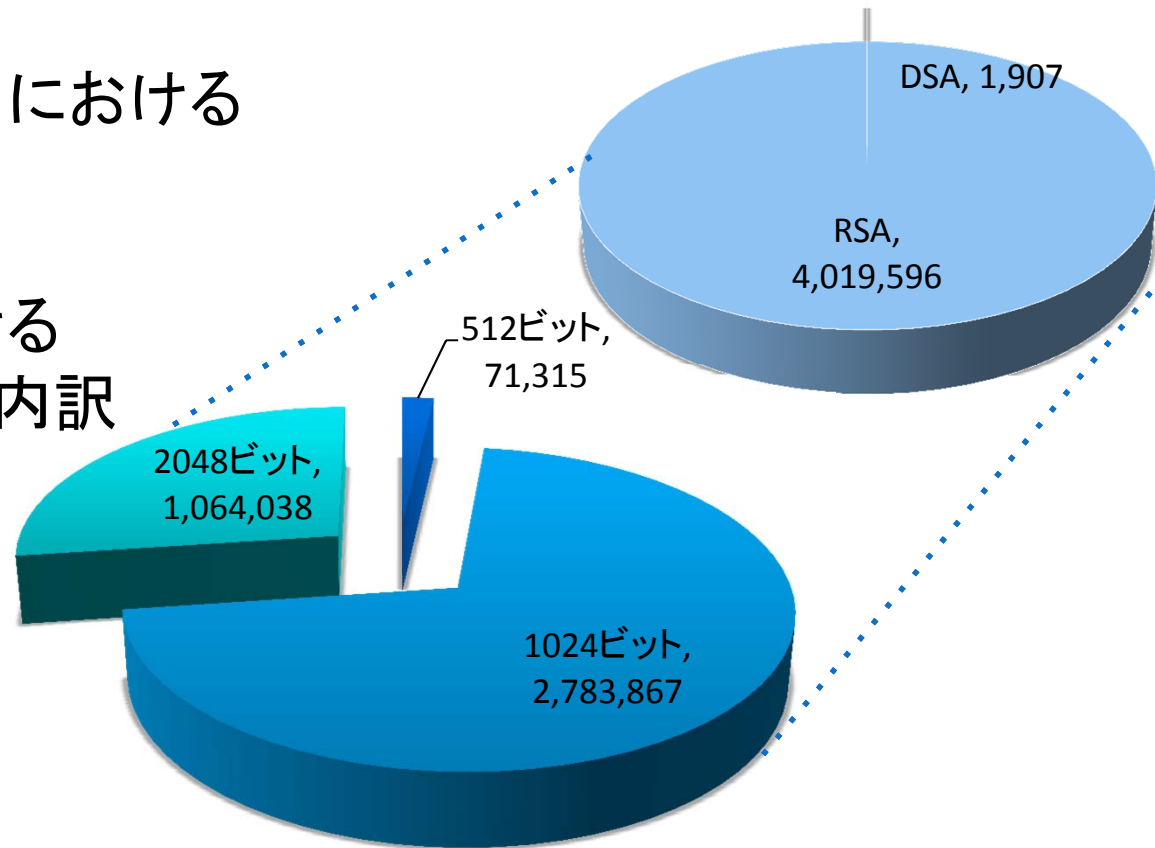


可視化

解析対象のSSL公開鍵証明書

SSL Observatory (2010) における
RSA と DSA の内訳

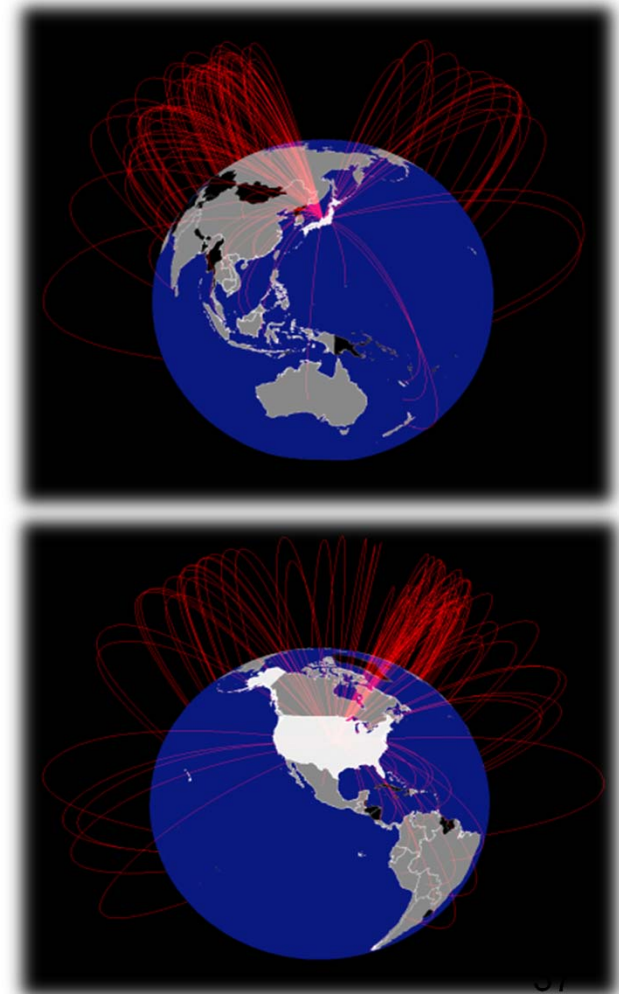
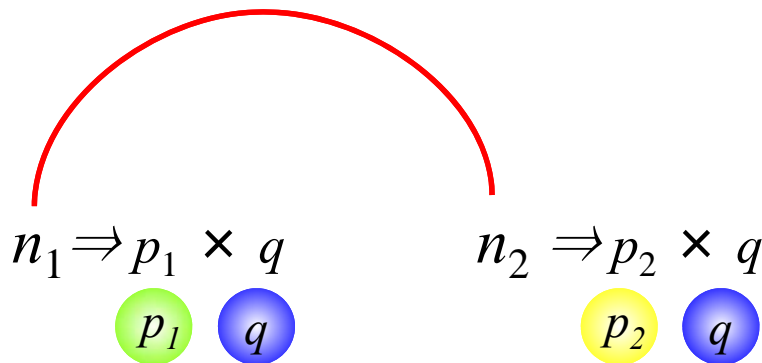
SSL Observatory における
RSA公開鍵のサイズ別内訳



8,703個の異なるRSA公開鍵が素数を共有
⇒ 8,703台のSSLサーバが危険な状態

可視化

公開鍵証明書が素因子を共有している
2つのSSLサーバ間を赤い線で結ぶ
(サーバ位置情報は国情報のみ)



XPIAでの解析結果 (2013.8)

8,703 (171) 個:SSL Observatory に含まれる
RSA 公開鍵で素因数分解できるもの

括弧内は日本

3,260 (104) 個:公開鍵を
ダウンロード可能

5,443 (67) 個:公開鍵を
ダウンロード不可能

ほとんどがタイムアウト

2,611 (90) 個:いまだ
に脆弱な公開鍵を利用

649 (14) 個:異なる
公開鍵に更新

危険な状態にある2,611サイトを発見

まとめ

- 公開鍵検証・可視化システムXPIAを開発、SSL/TLSサーバ認証で最も利用されているRSA暗号に関する脆弱性の実態を把握
- 今後の展開
 - わが国の電子政府等において、暗号技術を安全に利用するために活用
 - 本システムをSSLに対する他の攻撃 (BEAST攻撃, RC4の統計的偏りを利用した攻撃) にも対応できるよう拡張

今後に向けて

誰もが安心・安全にコミュニケーションできる社会を実現するために、理論と実践の両側面からネットワークセキュリティ技術の研究開発を推進し、NICTの中立性を最大限に活用することにより、世界的な研究開発拠点となることを目指します。