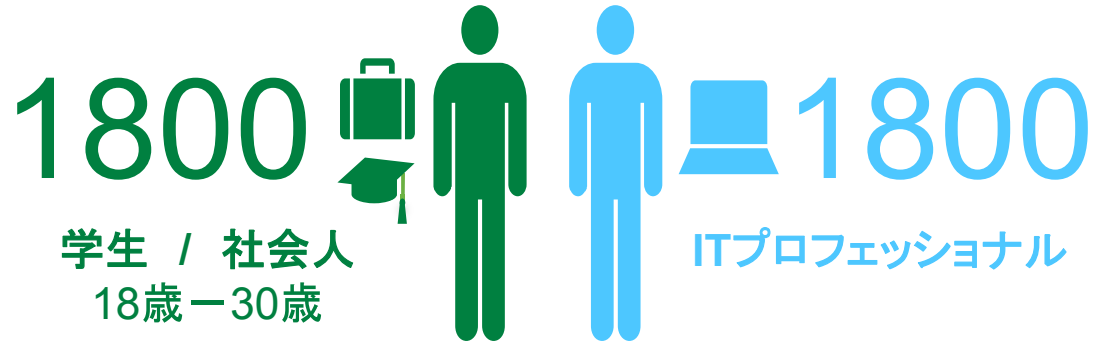
資　料　編

企業から見た日本版NCFTA

2013年7月5日
シスコシステムズ合同会社
石井　延幸

shharada@cisco.com

Cisco Connected World Technology Report



実施日　：2012年8月

対象人数：各国カテゴリーごとに100名づつ

対象国　：米国、カナダ、メキシコ、ブラジル、アルゼンチン、英国、フランス、ドイツ、オランダ、ロシア、ポーランド、トルコ、南アフリカ、韓国、インド、中国、日本、オーストラリア

shharada@cisco.com

“Generation Y” の生態

毎日利用するデバイス数

1 device	2 devices	3 devices	4 devices	5 or more
17%	46%	29%	6%	2%

オンライン利用

36%	22%	20%	13%
サーチエンジン	オンラインビデオ	SNS	広告

パスワード

25+%	10%
5~9つのパスワード	管理できず

プライバシー

58% は、プライバシーの時代は終わったと考えている

90% は、オンラインショッピングを利用している

57% は、割引やセールのお知らせを得るためにメールアドレスを登録している

60% は、口コミに頼っている

75% は、多くのサイトで個人情報を安全に保つことを信用していない

81% は、オンラインとオフラインのアイデンティティが違うと信じている

33% は、ほとんどの人はオンラインとオフラインのアイデンティティが完全に違うと思っている

50% は、私は同じと思っている

shharada@cisco.com

会社支給デバイスでの私的なネットサーフィンを企業がトラックすることについて

私用目的のブラウジングについても、プライベートは厳格に保たれるべきであり、誰も追跡および利用すべきではない	40%
まず、自分が許可すればトラックされてもいい	38%
会社がトラックしていることを知らなかった	12%
気にしません	5%
分かりません	5%

従業員は業務とソーシャの区別がない

40% は、「企業ポリシーは支給端末での私的利用を禁じている」と認識している

71% は、企業ポリシーに従っていません

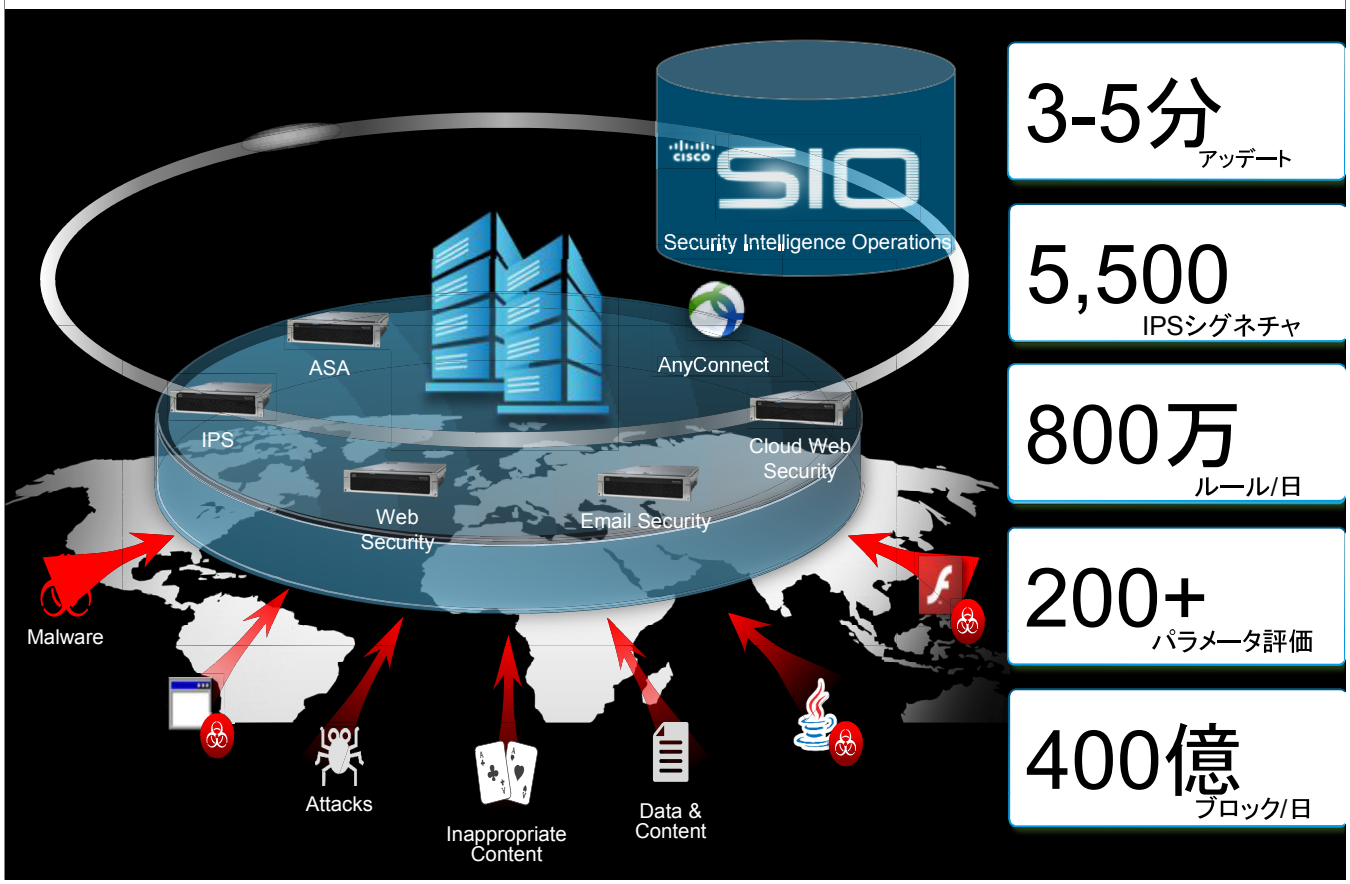
50% のIT管理者は、従業員が私的利用に関するポリシーに従っていると信じている

shharada@cisco.com

シスコセキュリティレポート2013

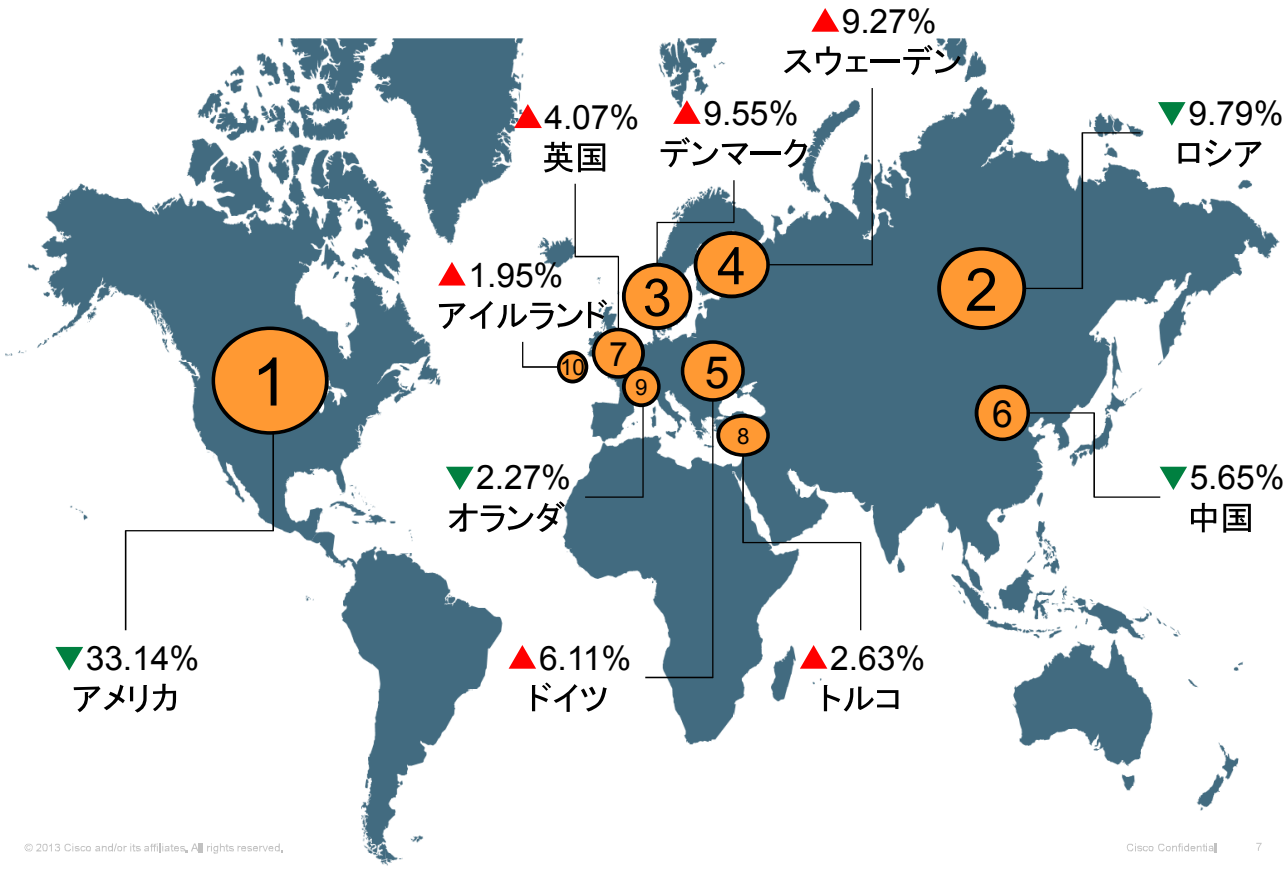
http://www.cisco.com/en/US/prod/vpndevc/annual_security_report.html

グローバルセキュリティネットワーク

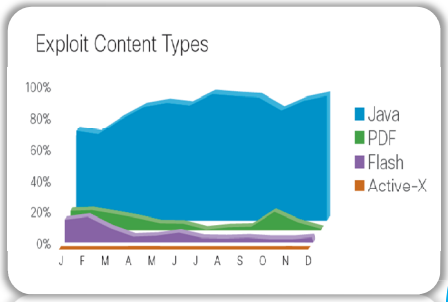


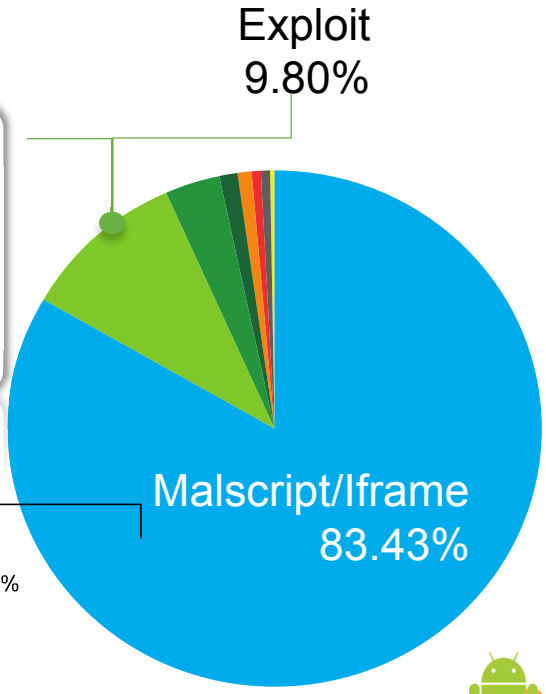
国別ウェブマルウェア出現率

▲2011年より上昇
▼2011年より減少



タイプ別ウェブマルウェアランキング



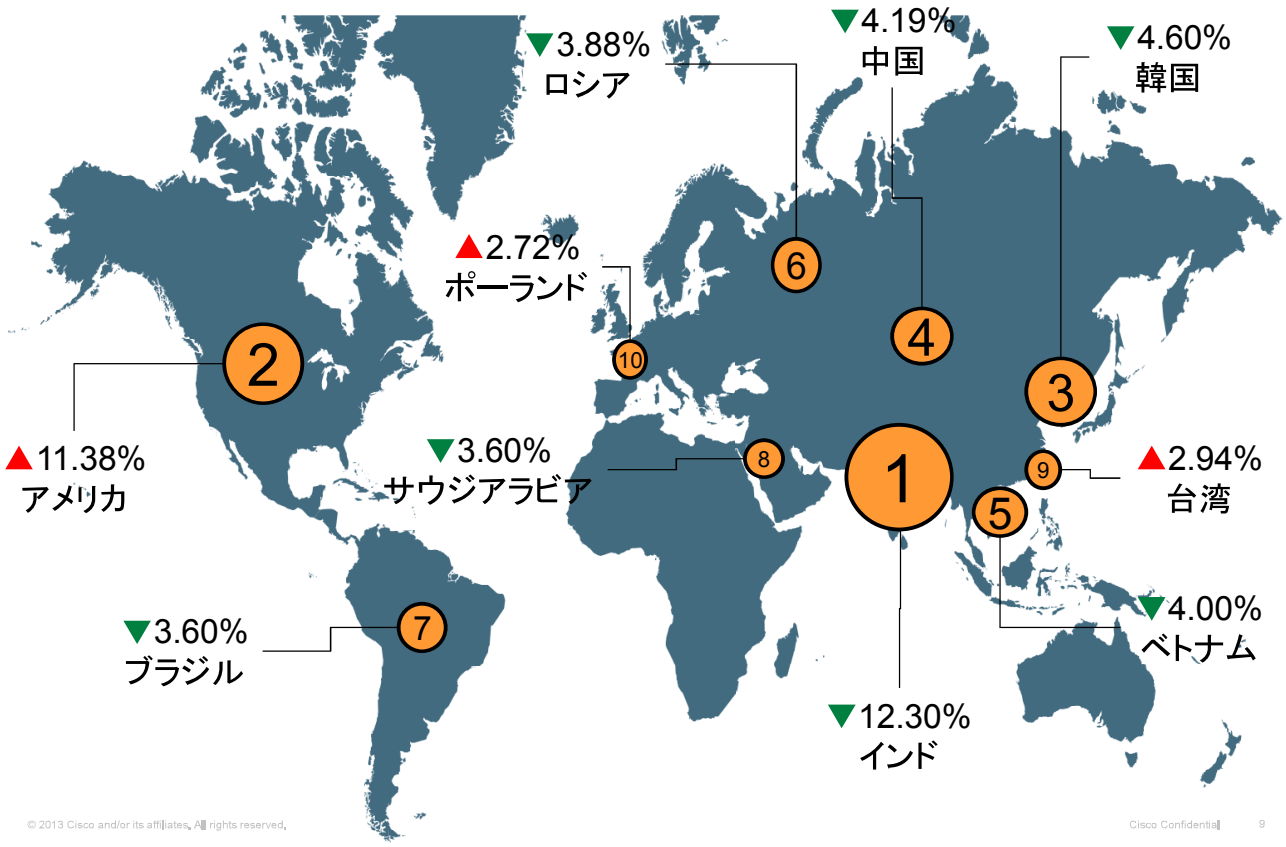


Infostealer 3.50%
Downloader 1.12%
Worm 0.90%
Virus 0.48%
Mobile 0.42%
Scareware 0.16%
Ransomware 0.06%

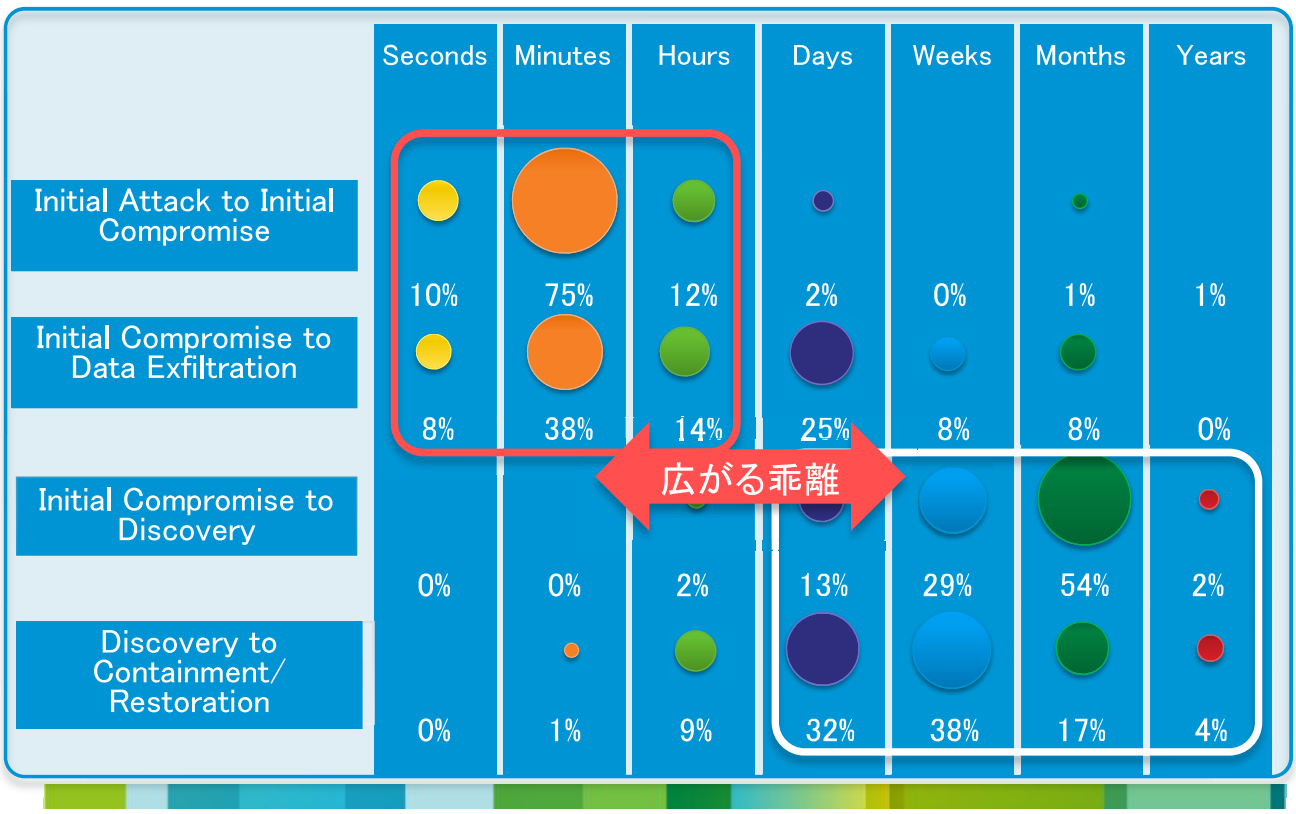
Online Communities 2.66%
Entertainment 2.57%
Online Storage & Backup 2.27%
News 2.18%
Sports & Recreations 2.10%
File Transfer Services 1.50%
SaaS & B2B 1.40%
Web-Based Email 1.37%
Education 1.17%
Transportation 1.11%
Health & Nutrition 0,97%

国別スパムメール状況

▲2011年より上昇
▼2011年より減少

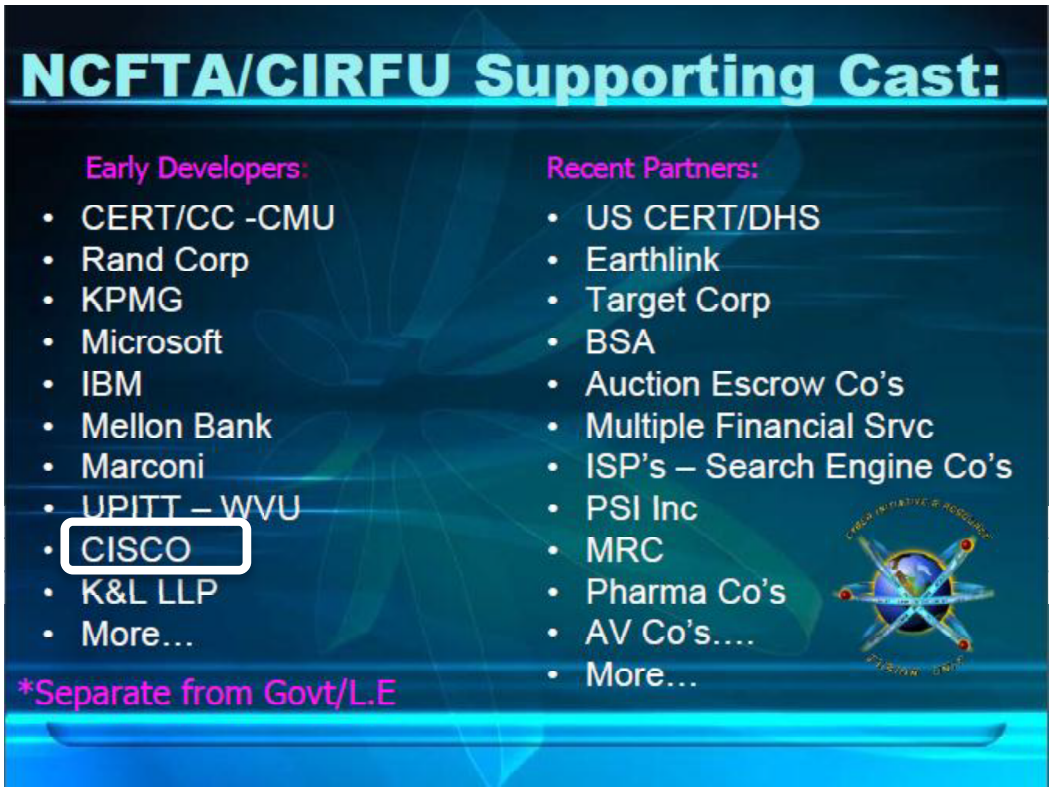


昨今のプロアクティブなサイバー攻撃と既存の防御スピードの差分解析(Powered by Cisco SIO)



shharada@cisco.com

ご参考



shharada@cisco.com

ディスカッション・ポイント

企業から見た産官学連携（問題提起）（1/3）

①想定される保護対象、情報共有する対象をどこまで想定するか？

一般個人 （Individual）	一般法人、 組織 (Organization)	重要インフラ企業 (Critical Infrastructure)
・Smart Meter/HEMS の導入が脆弱性ポイント を幾何級数的に増大	・IT要員、セキュリティ要員 の限られる中小規模以下の 企業をどのように守れるか	・CEPTOAR/NISCとの情報連携

CEPTOARに相当する米国ISACでは次頁に示す情報項目を業界内で共有化する仕組みが出来ているが、参加者のQualificationが不十分なためさほど機能していない。

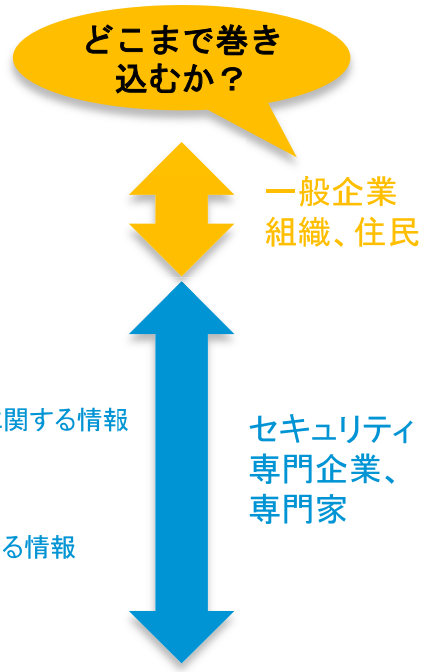
如何に情報シェアを行う参加者と信頼関係が構築できるかが要
- Qualification の基準、Processの確立
- Small Startが重要なポイント

企業から見た産官学連携（問題提起）（2/3）

②どのような情報項目の共有化を目指すか？
想定される課題（共有化するDBの観点から）

情報項目

- 事態・事件情報 (Incident Information)
  ー企業、組織、または個人の被害に関する情報
  ・ウィルス、不正アクセス、情報改ざん、等
  ・予兆情報→発生情報
- 脅威情報 (Thread Information)
  ー脅威（マルウェア）及び脅威になるグループ、個人（ハクティビスト）の情報
  ・一時的に群れとなって襲ってくる脅威
- 脆弱性情報 (Vulnerability information)
  ー製品、システム、ソフトウェア等の技術的脆弱性に関する情報
  ・汎用製品のセキュリティホール
  ・特定業界向け製品のセキュリティホール
- 解決策情報 (Solution Information)
  ー事態・事件、脅威、及び脆弱性への解決策に関する情報
  ・汎用製品のセキュリティホール
  ・特定業界向け製品のセキュリティホール



企業から見た産官学連携（問題提起）（3/3）

③その他、

-日本版NCFTAは、どの様な機能を提供し（範囲）、どの部分で産官学連携を行うか？

事例：Cisco Cyber Security Analyst Specialist Training (CSA)

Table 1 Service Features

Infrastructure	Attack	Defense
• Wired, wireless, and remote access • Network and routing • Client simulator • Server simulator • Application simulator • Traffic generation	• DDoS • Network attacks • Application attacks • Computer malware • Mobile device malware • Evasion techniques • Botnet simulation • Open source attack tools	• Client endpoint security • Firewall • IDS/IPS • Web & email proxy • Telemetry analysis • Identity & access management • Security and event management • Investigation tools • Open source defense tools

shharada@cisco.com

Thank you.

CISCO

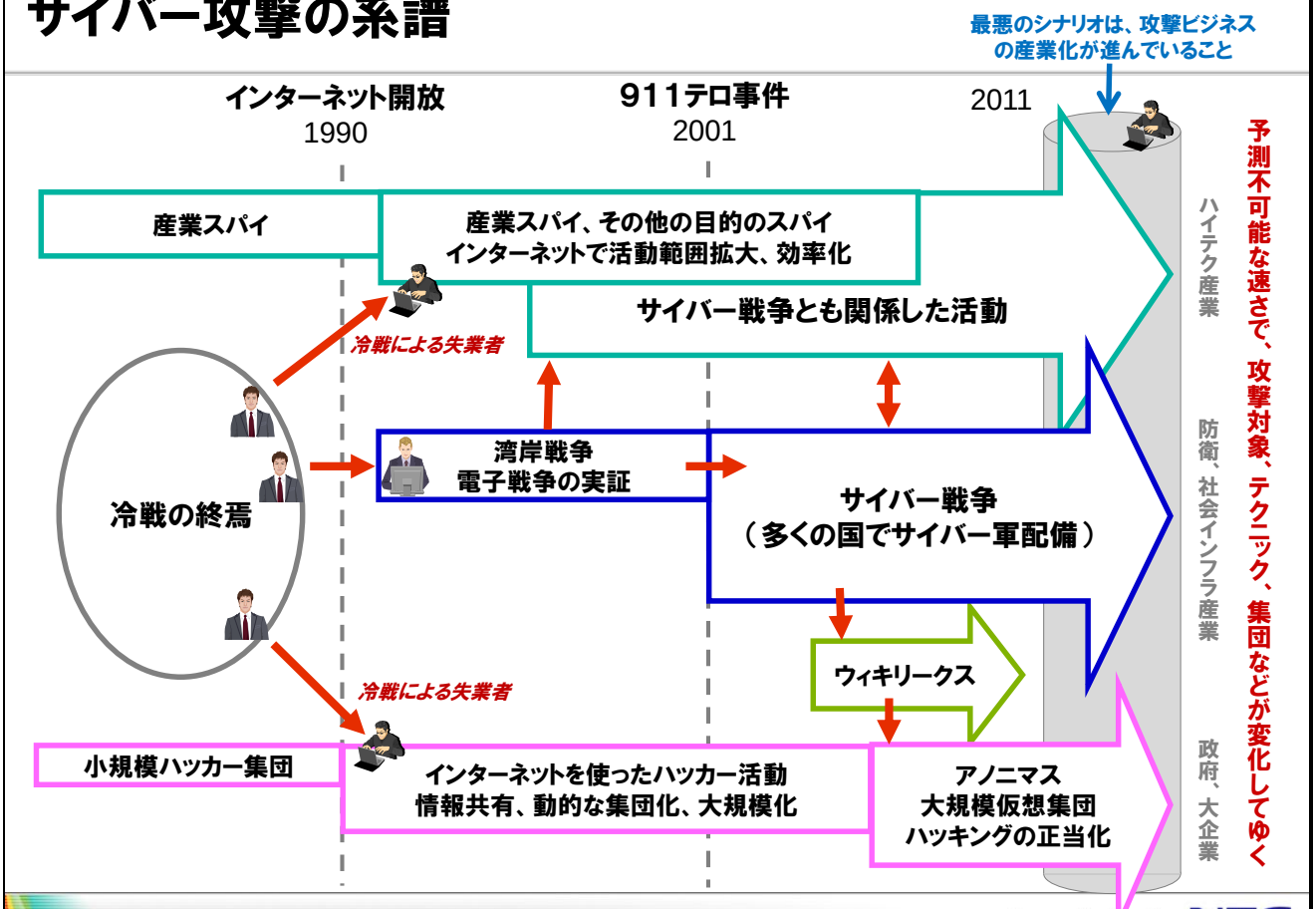
Empowered by Innovation NEC

総合セキュリティ対策会議2013 第一回

サイバー空間のセキュリティ
いつかは攻撃を受ける企業の立場で

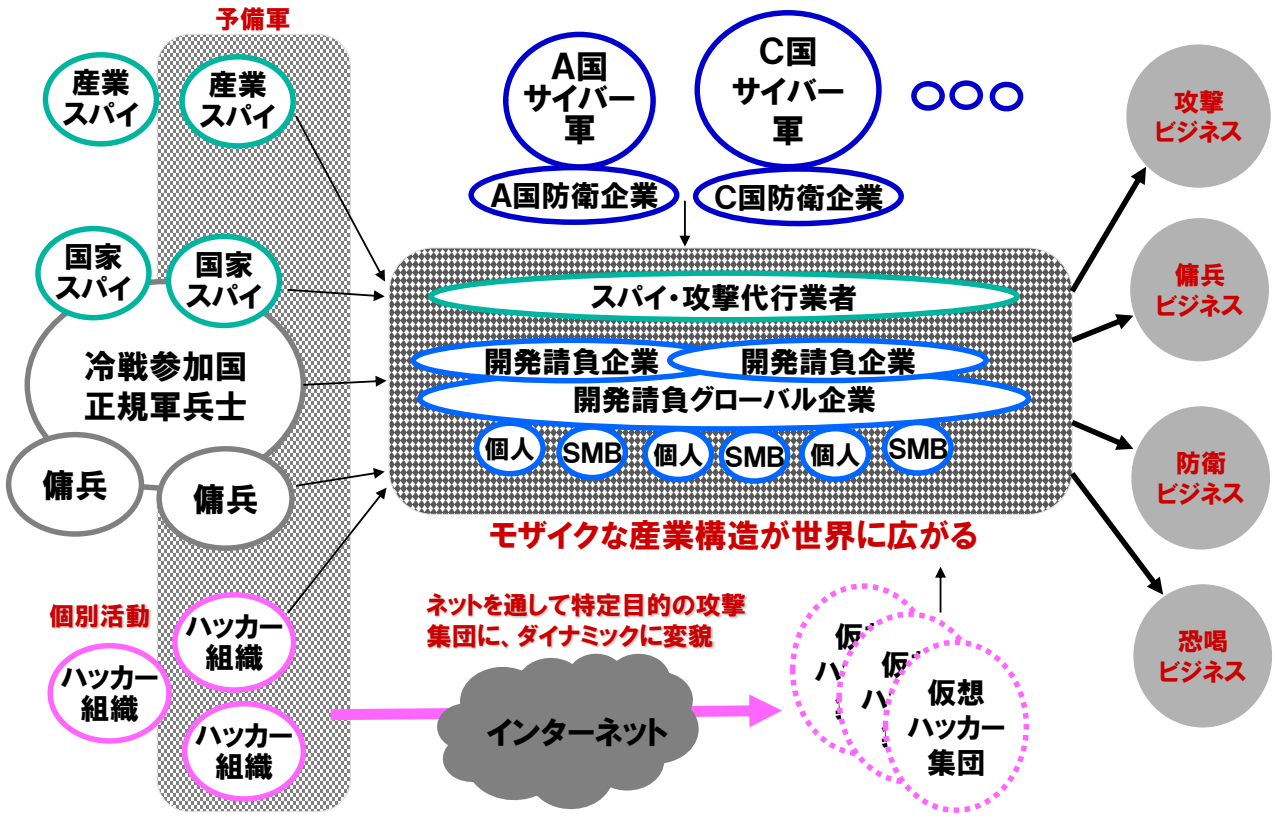
2013/7/5
日本電気
ナショナルセキュリティ・ソリューション事業部
則房雅也, CISSP

サイバー攻撃の系譜



Empowered by Innovation NEC

攻撃者のキャリアパス



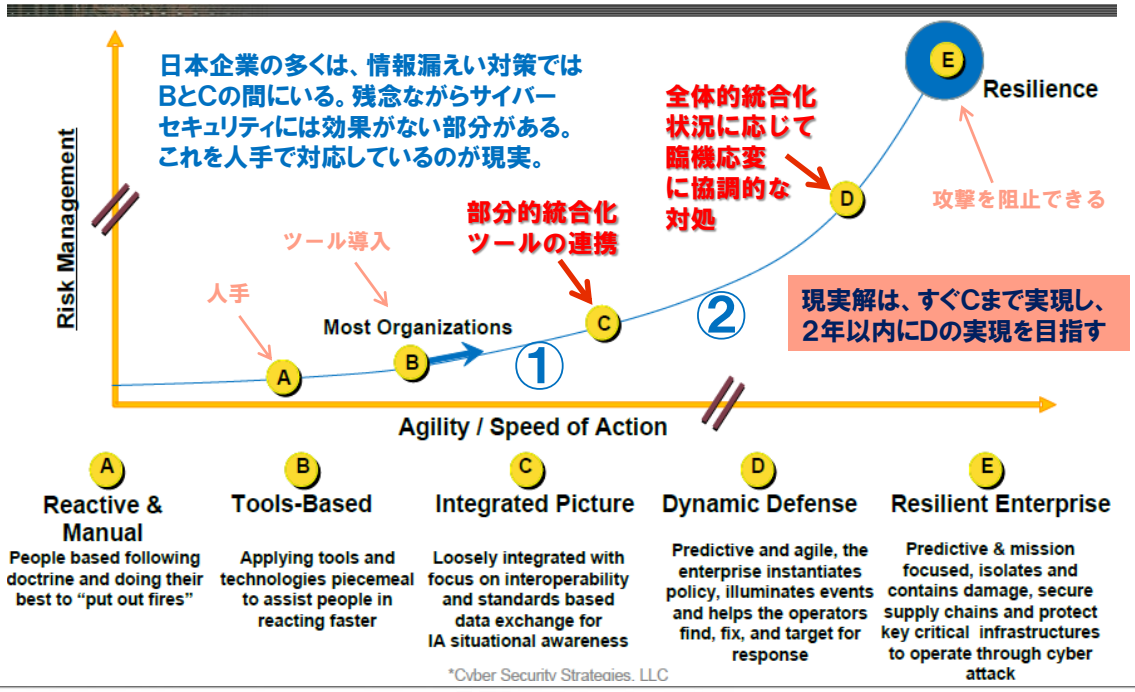
「これまで vs. これから」のセキュリティ

	これまで	これから
課題	個人情報漏えい対策	標的型サイバー攻撃対策
犯行者	社員（アマチュア）	外部の専門家（プロ）
特長	知識・技術力は低い	知識・技術力は高い
動機	不注意、不平・不満	国家、組織的ビジネス
発見	社員からの申告	何か月も発見されない
頻度	一回きり	成功するまで、何度でも
結果	謝罪、弁済	企業活動停止

サイバーセキュリティ成熟度モデル

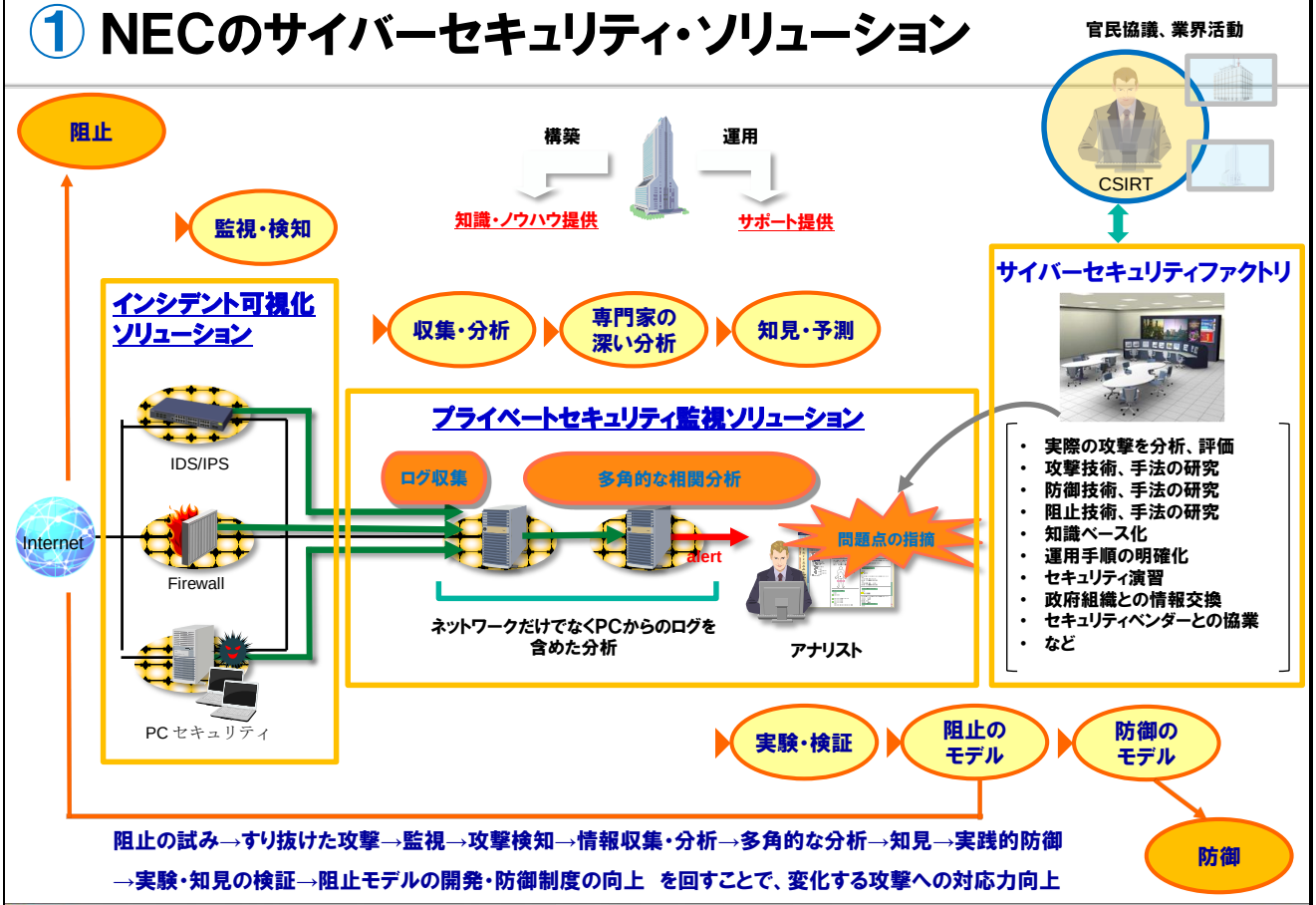
Cyber Security Maturity Model*

Robust Information & Communications Technologies for Mission Success



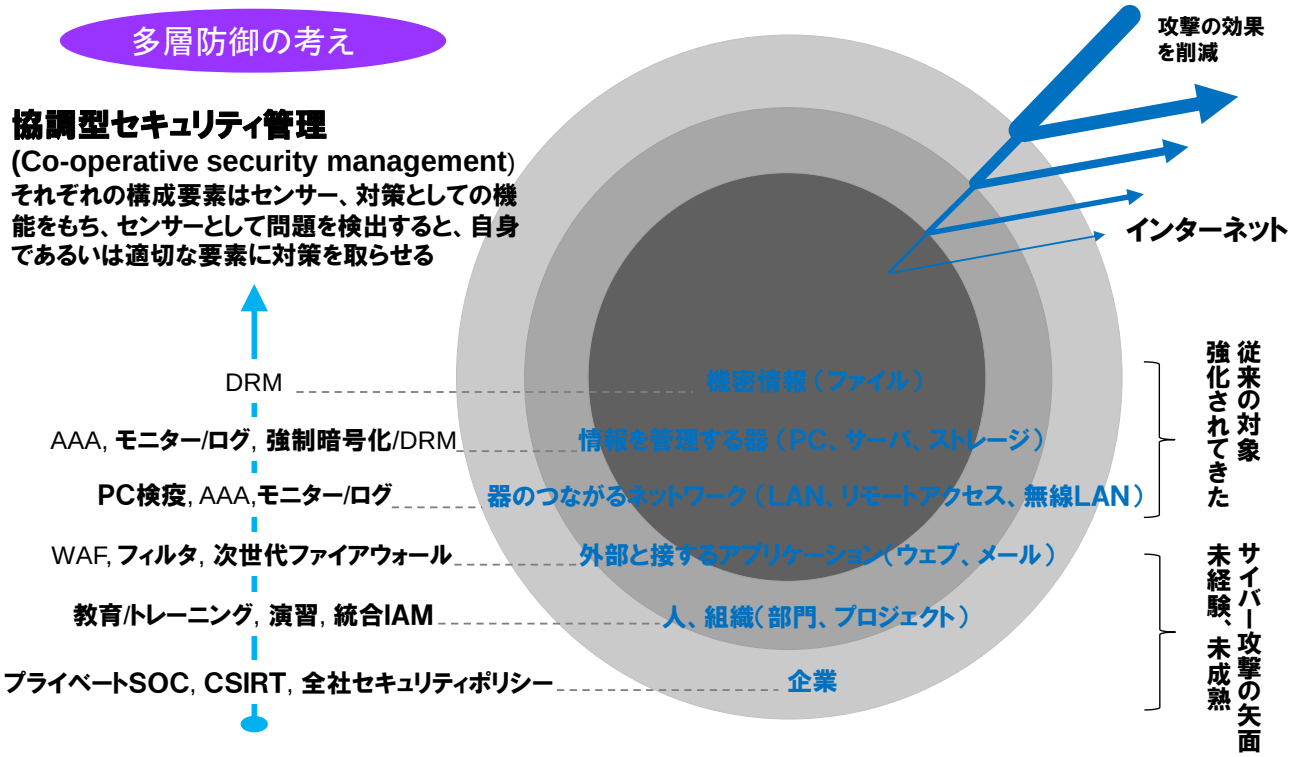
*Cyber Security Strategies, LLC

① NECのサイバーセキュリティ・ソリューション

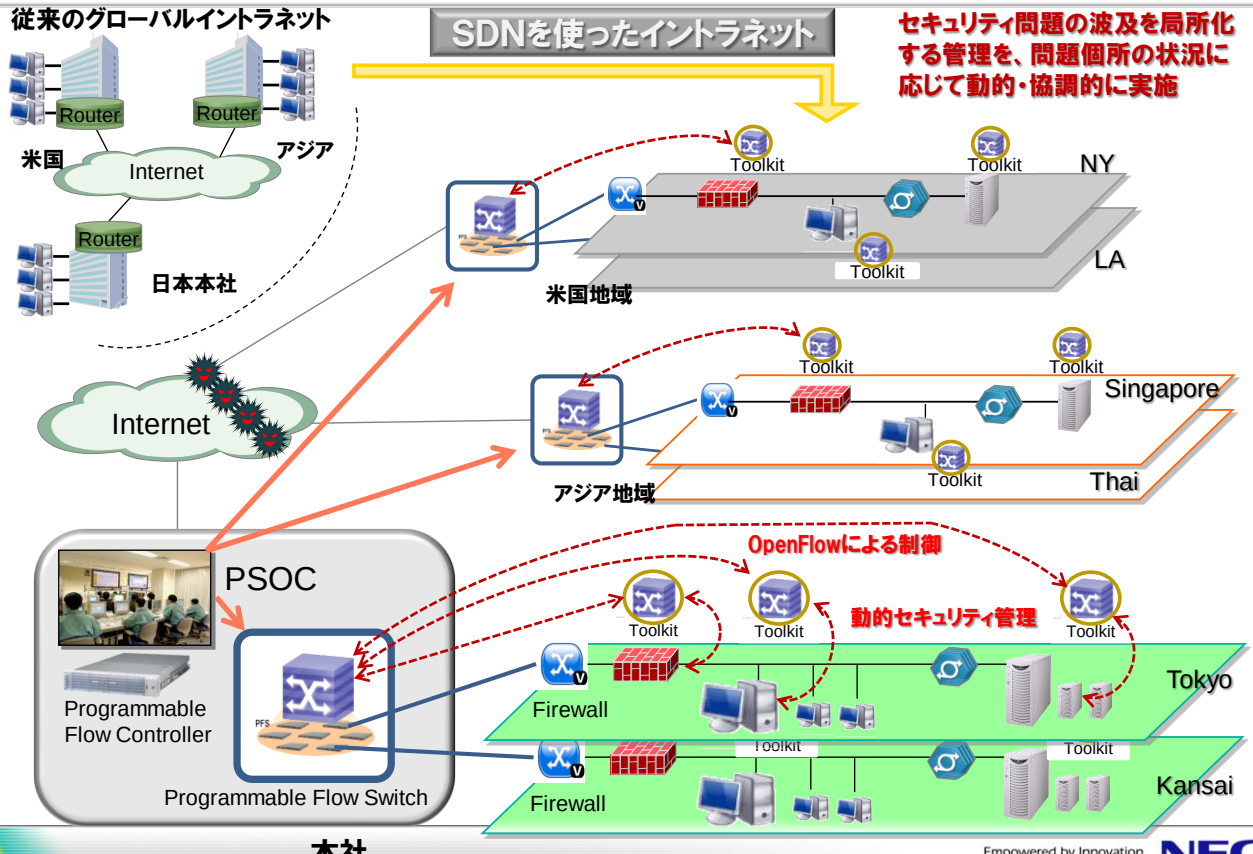


阻止の試み→すり抜けた攻撃→監視→攻撃検知→情報収集・分析→多角的な分析→知見→実践的防御
→実験・知見の検証→阻止モデルの開発・防御制度の向上　を回すことで、変化する攻撃への対応力向上

② 新しい脅威からの影響を減らす考え方



② 協調型サイバーセキュリティマネージメント



まとめ：認識を共有したいこと（課題）

さまざまな協調連携が必要

- ツール間：ベンダーを超えた製品連係、「機能の協調」
- 人と人：　運用者、アナリスト、開発者、研究者の連携、「視点の協調」
- 企業間：　特に同業種、「意識の協調」
- 官民：　「タイミングの協調」
- 国際間：「時差の協調」「知見の協調」
- 相手は見えなくて巨大、単機能、単製品、一握りの人材では対応できない

情報交換は必須

- ただし、情報ソース(Information)の交換ではなく、情報分析して知見の入った情報(Intelligence)の交換が必要

サイバーセキュリティ人材の育成

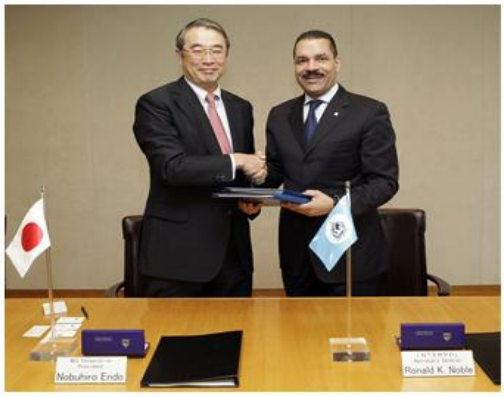
- 企業内で再配置は困難。高度専門職、安定雇用がカギ。
  - 全国大学で1000名／年、上場企業が1～2名雇用（CSIRT、分析官などの専門職）、他はセキュリティベンダー、中長期視点での技術開発・研究機関

Press Releases on 12/18/2012

INTERPOL and NEC sign partnership agreement to enhance cyber security
Partnership will develop digital crime centre

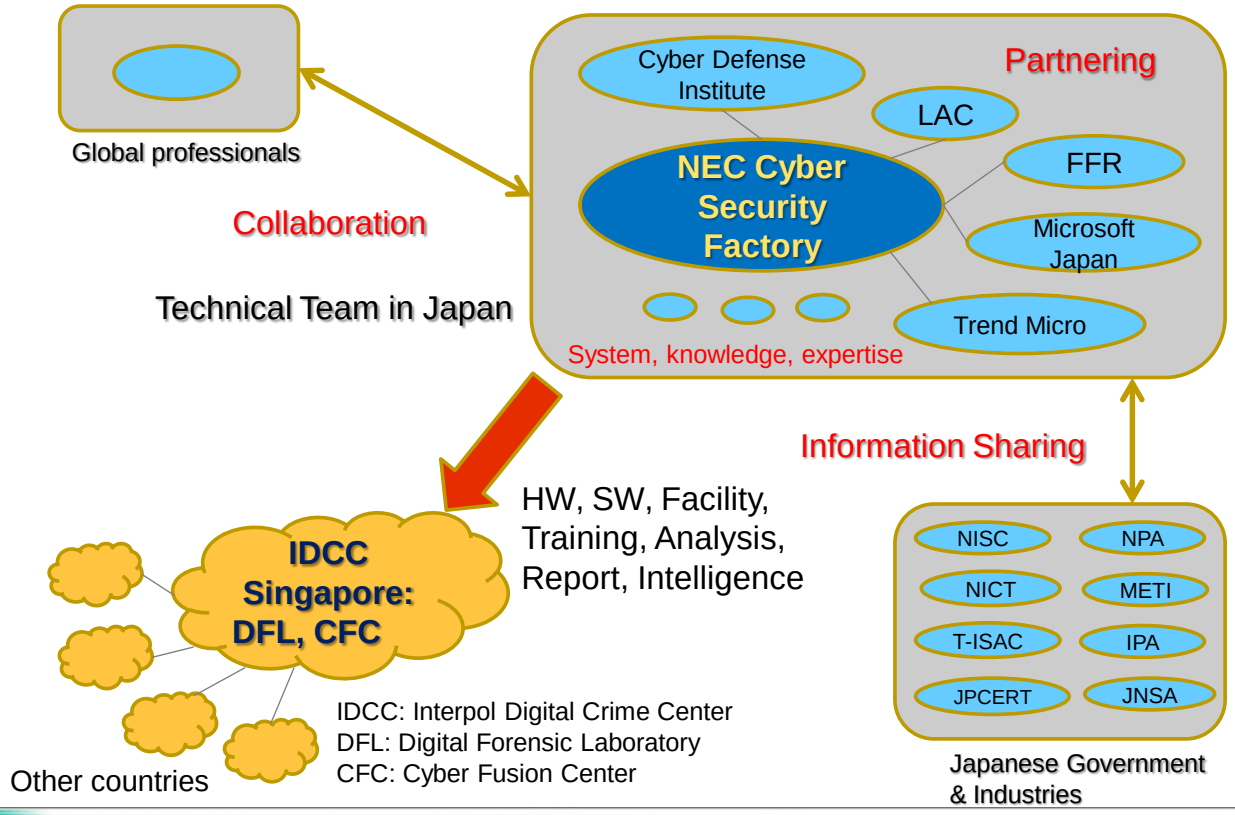
*** For immediate use December 18, 2012

Share:
Recommend 77
Tweet



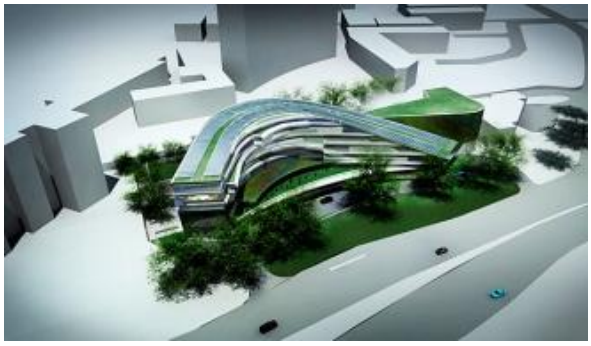
Tokyo, December 18, 2012 - In a bid to strengthen the global fight against cybercrime, INTERPOL and Japan's NEC Corporation today signed a partnership agreement which will see NEC provide the world police body with vital assistance in developing core elements of the Digital Crime Centre being established within the INTERPOL Global Complex for Innovation in Singapore.

Integration of IT, Human, Knowledge, & Time



The INTERPOL Global Complex for Innovation (IGCI)

- New facility at Singapore to focus on Cyber Crimes. Operation will start in 2014.



- The INTERPOL Digital Crime Centre (IDCC)
  - Digital Forensic Lab(DFL)
  - Cyber Fusion Centre(CFC)
  - Capacity Building and Training
- NEC partners with
  - Security vendors in Japan as well as other countries

まとめ（期待）

- サイバーセキュリティ情報の多くは組織の外、日本の外にある
  - さまざまな地域性、文化、環境に基づいた知見がある
  - 視点の異なる知見の中で、問題を解決する手法を発見できるのではないか
- 情報を収集する仕組み、知見を収集する仕組みの構築
- 人材ネットワークの構築
- 必要なこと
  - 今出来ることは今始める ← サイバーに関してはできていない！
  - ぶれない目的の設定 ← やはり攻撃から守れるようになること
  - 対応プロセスの自動化、ITシステム化が理想、しかし、当面は高度人材（分析官、研究者、意思決定者など）を中心に据えた対応システムの構築
  - 出来るところからの連携

Empowered by Innovation

NEC

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

学術機関から見た産学官連携

2013年7月5日

林　紘一郎、Ph.D.,LL.D.
情報セキュリティ大学院大学

1

私の職歴と研究暦

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

研究と実務の融合

ビジネス（33年）＋ 研究者（16年）

文理融合

文系職場　17年 ＋ 理系職場　9年*

＋ マネジメント　7年

法と経済学

経済学　5年 ＋ 法学　11年

官民融合

電電公社（官）22年 ＋ NTT（民）11年

国内　27年 ＋ 海外　6年

この間経験したこと
シンクタンクの顧問　2件
ベンチャーの監査役等 4件
NPOの理事長等　4件

異文化融合

NTT America社長　3年
Nextel Communications 1年
（Now Sprint-Nextel）

実務感覚の維持

委員会設置会社

*データ通信本部（NTTデータの前身）4年 + 計画局総括課長等3.5年
パケット通信部長　1.5年

2

情報セキュリティ大学院大学

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 2004年開学＝本年度末で10周年
- 9.11を見た理事長の決断
- 当初から、①実学、②文理融合（理系7：文系3程度を想定）、③産学協調を目指す
- 教員も、①～③のバランスを重視
- しかし、大学による院生の囲い込みを打破できず、社会人院生が中心（80%弱）
- 女性と外国人は少ない（今後の課題）
- 昨年度末までの修了生：修士226名、博士21名
- 同、ISS Square サーティフィケート取得者67名

3

情報セキュリティ人材の不足（民間）

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

従業員規模	現従事者数（推計）	不足人材数（推計）
100≤ X <300	約85,000	約8,500
300≤ X <1,000	約63,000	約6,200
1,000 ≤ X	約81,000	約7,700
合計	約23万人*	約2.2万人

＊ただし、うち14万人は何らかのトレーニングを要す。

供給する人材	定義	概数
専門的教育受講者	体系的コース修了者（大学院・大学・高専・専門学校）	130人/年
	セキュリティをテーマにした研究経験者（大学・大学院）	1,000人弱/年
選択可能者	セキュリティ科目を選択・受講することが可能な者（大学院・大学・高専・専門学校）	2万人弱/年

出典：2012年4月27日　IPA報告書

4

人材育成の基本

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

情報セキュリティ人材育成に係る基本的な考え方

1．「ハイブリッド型人材」、「問題発見・解決型人材」の育成・確保
① **「ハイブリッド型人材」**：急速に高度化・多様化する中、ダイナミックな情報セキュリティリスクの変化に対応することができるよう、様々な専門分野の知見を融合できる人材。
② **「問題発見・解決型人材」**：情報セキュリティリスクを、他のリスクと比較考慮しながら最適な解を模索するなど、鳥瞰的な視点から情報セキュリティリスクに対応した問題発見・解決能力を有する人材。

2．情報セキュリティ人材育成環境の整備
① **企業のトップの意識改革**：「係長セキュリティ」から「社長セキュリティ」へ
② **情報セキュリティ人材の価値や効果の可視化**：必要とされる人材の明確化、求められる知識や技能の体系化・共通化、資格制度・処遇・キャリアパスの関係の明確化、インセンティブ付与等の検討

3．産学連携の強化
- 教育機関及び産業界がそれぞれ求める人材像のギャップの解消
- 産学連携を含めた大学教育の充実

4．先導的研究開発、情報セキュリティ産業の活性化を通じた人材の育成
先導的技術開発、高度情報セキュリティ人材育成、情報セキュリティ産業の活性化の好循環構造の構築を目指す。

5．グローバル化に対応できる人材の育成
情報セキュリティ脅威への対応や、諸外国との関係機関との情報連絡・情報共有を含めた国際連携を構築するためにも、グローバル化に対応できる人材を育成する。

出典：情報セキュリティ政策会議、普及啓発・人材育成専門委員会報告書を踏まえたNISC指針（2012年5月31日）

5

人材育成のキャリア・パス

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

前出のIPA報告書から：

(3) 情報セキュリティ人材のキャリアパスに関する調査

現在、国内の情報セキュリティ分野で活躍している合計61名に、個人の業務経験とキャリアアップの経緯、スキルアップの方法等についてインタビュー調査し、キャリアパスのモデル化を行いました。

セキュリティ人材を、①セキュリティ戦略／統括、②企画／設計、③開発／構築、④運用／管理、⑤監査／検査、⑥コンサルティング／教育の6職種に分類して調査した結果、職種毎に一定の特徴は見られるものの、全体的には高いスキルを確立するには必ずしも特定のキャリアパスに依存していないという傾向が見られました。

また、転職とキャリアアップとに相関関係は見られず、転職することが必ずしもキャリアアップにつながるわけではないと考えられます。

一方で、現在ハイレベルにある人材では、ミドルレベルからステップアップする際に、社外のコミュニティ活動への参加、マネージメント業務の経験、国際業務の経験などが自己を成長させるきっかけになったとの意見が多く見られました。

6

産と学の意識のズレ

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

産業界の高度IT人材に関する現状認識

◆平成18年以降のIT国家戦略など、今後のIT政策の焦点は「ITの利活用の推進」。
◆なかでも、ITを活用し高い付加価値を創造できる高度情報通信人材の育成は重要課題。
◆ソフトウェア（組み込みソフトを含む）は、我が国の中核技術として産業全体の競争力の一翼を担う。しかし、現在ソフトウェア開発・利用に携わる人材の質・量の不足が深刻化。

■高度情報通信人材の現状

（我が国）	（海外）
○外国人技術者の活用、海外への業務委託が進展 ○大学教育は学術的な教育研究が中心で、実務教育は企業内のIT研修で対応。	○米国では産学連携の下、大学で高度なIT実践教育を実施。 ○中国、韓国、インド等では、国策として高度情報通信人材育成に対する重点的取り組み強化し、世界的人材供給基地として発展。

■企業が新卒者に求める理想と現実のギャップ

（理想）	（現実）
情報関連専攻者を中心に、企業内の実践教育・業務に耐えうる、ITの高度な専門知識・スキルを備えた新卒者を採用したい。	新卒者のうち、即戦力たる人材はわずか1割。新卒者のうちIT研修を受けても、業務に従事できない人材が約2割いる。（日本経団連調査）

実践性を備えた世界レベルの先進的IT拠点を、大学・大学院から選抜、もしくは新設し、
産学官連携による重点的な資源投資の下、トップレベルの高度IT人材を育成する必要がある。

【出展：日本経済団体連合　提言「産学官連携による高度な情報通信人材の育成強化に向けて」(H17.6)】

7

ISS Square（2008～2012年度）

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 経団連提案等を受けて、文科省が予算化した「先導的ITスペシャリスト育成推進プログラム」に応募し認められたもの
  http://www.mext.go.jp/a_menu/koutou/it/index.htm
- 内容はソフトウエア人材育成と高度セキュリティ人材育成に分かれ、セキュリティについては、東拠点（当大学院、中大、東大）と西拠点（奈良先端大、京大、阪大、北陸先端大）が競争と協調の中で実施
- 終了後の評価では「当初の目的を、良く達成できている。」と認められている
- 受講者は、通常の修士課程を修了するとともに、特定の付加条件（選択必修とサブへの参加など）をクリアすれば、サーティフィケートを授与
- サーティフィケート累計取得者数：当大学院67名、他の3大学78名。東拠点の合計145名（西拠点は、これより少ない ）

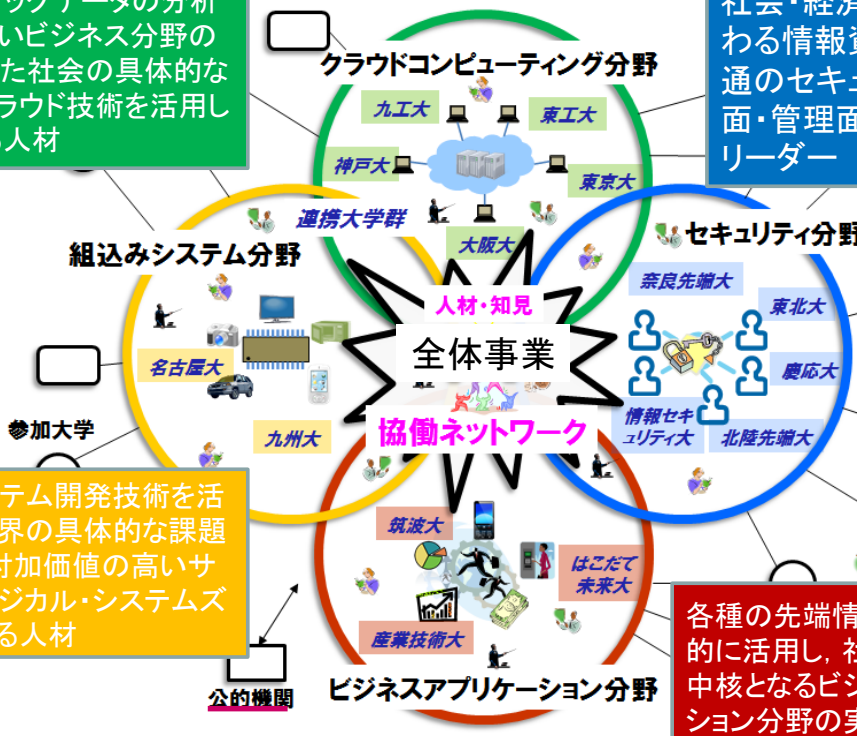
8

enPiT（2012～2016年度）

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

いわゆるビッグデータの分析手法，新しいビジネス分野の創出といった社会の具体的な課題を，クラウド技術を活用し解決できる人材

社会・経済活動の根幹にかかわる情報資産および情報流通のセキュリティ対策を，技術面・管理面で牽引できる実践リーダー



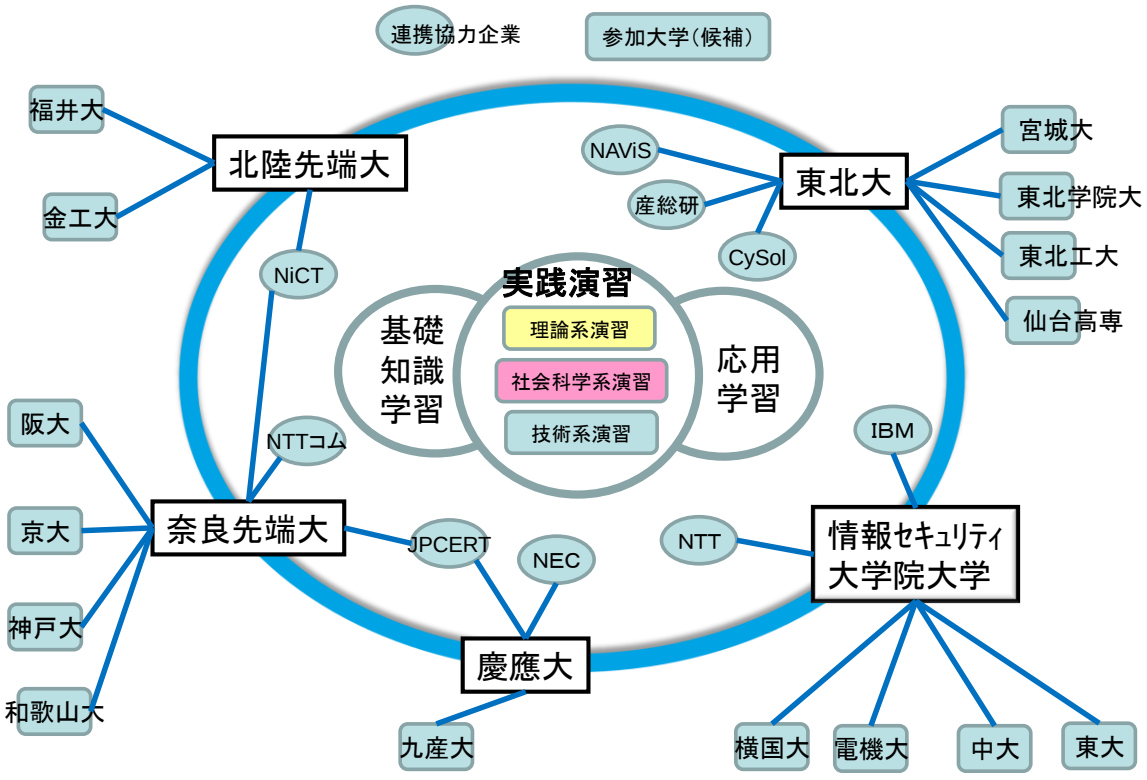
組込みシステム開発技術を活用して産業界の具体的な課題を解決し，付加価値の高いサイバー・フィジカル・システムズを構築できる人材

各種の先端情報技術を有機的に活用し，社会情報基盤の中核となるビジネスアプリケーション分野の実践的問題解決ができる人材

9

enPIT-Security

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



10

産学官連携の肝

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 三者間の相互理解が不可欠
- 3つの分野をすべて経験した人が居ればよいが、そうは行かないのが現状。せめて2つの分野を経験した人が欲しい
- それも望み得ない場合の次善の策としては、① お互いに天動説（自己チュー）を採らないことを明確にし、② 中立的なカタリストを活用すること
- NPO等を経験して苦労した人は、カタリストにふさわしいメンタリティを備えている
- 「命令する」とか、「指示があるまで待つ」という態度は、連携には不向き

11

蛇足：セキュリティ分野での連携

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- それぞれが情報を囲い込んだら、十分な対策が講じられない（ISACにおける経験）
- IISECからIPAに「一定時間が経過したインシデントを匿名化して教育目的だけに利用させて欲しい」と申し出たが、断られた（目的外利用なのでIPAを非難できない）
- NATOのNational Cyber Security Framework Manual（2012年12月）でも、5つのジレンマの中に挙げられている。
  ① Stimulate the Economy vs. Improve National Security
  ②Infrastructure Modernization vs. Critical Infra. Protection ③ Private Sector vs. Public Sector ④ Data Protection vs. Information Sharing ⑤ Freedom of Expression vs. Political Stability
- この報告書の作成者等、NATOの関係者は double-hatted や triple-hatted が当たり前

12