Empowered by Innovation NEC

シンポジウム
「サイバーセキュリティ産業化：日本の課題とイスラエルの動向」

企業IT産業における課題
～人材育成が急務～

２０１５年２月２日
日本電気株式会社
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

サイバーセキュリティに於ける課題

日本の課題、企業ITの課題

有効な情報の不足、実践的人材の不足

- 2011年、ようやく日本のサイバーセキュリティ元年
- 海外の情報はすぐ流通するが表層的
- トップ技術者は極少、中級技術者を指導できる人がいない
- 初級技術者を育成するところはどこにもない（授業は無い、即戦力重視）

ITの延長でしか考えられない管理者層

- 個人情報漏えい対策（保護法）→内部統制（J－SOX）→サイバーセキュリティ
- 感心を引くのは結局「情報漏えい」
- IT予算の１０％程度がセキュリティ予算。その半分は既存セキュリティシステムの保守、維持費。残りの予算の優先的使い方がサイバーセキュリティ。既存セキュリティシステム、製品を捨てられるわけではない。

誤解、認識不足

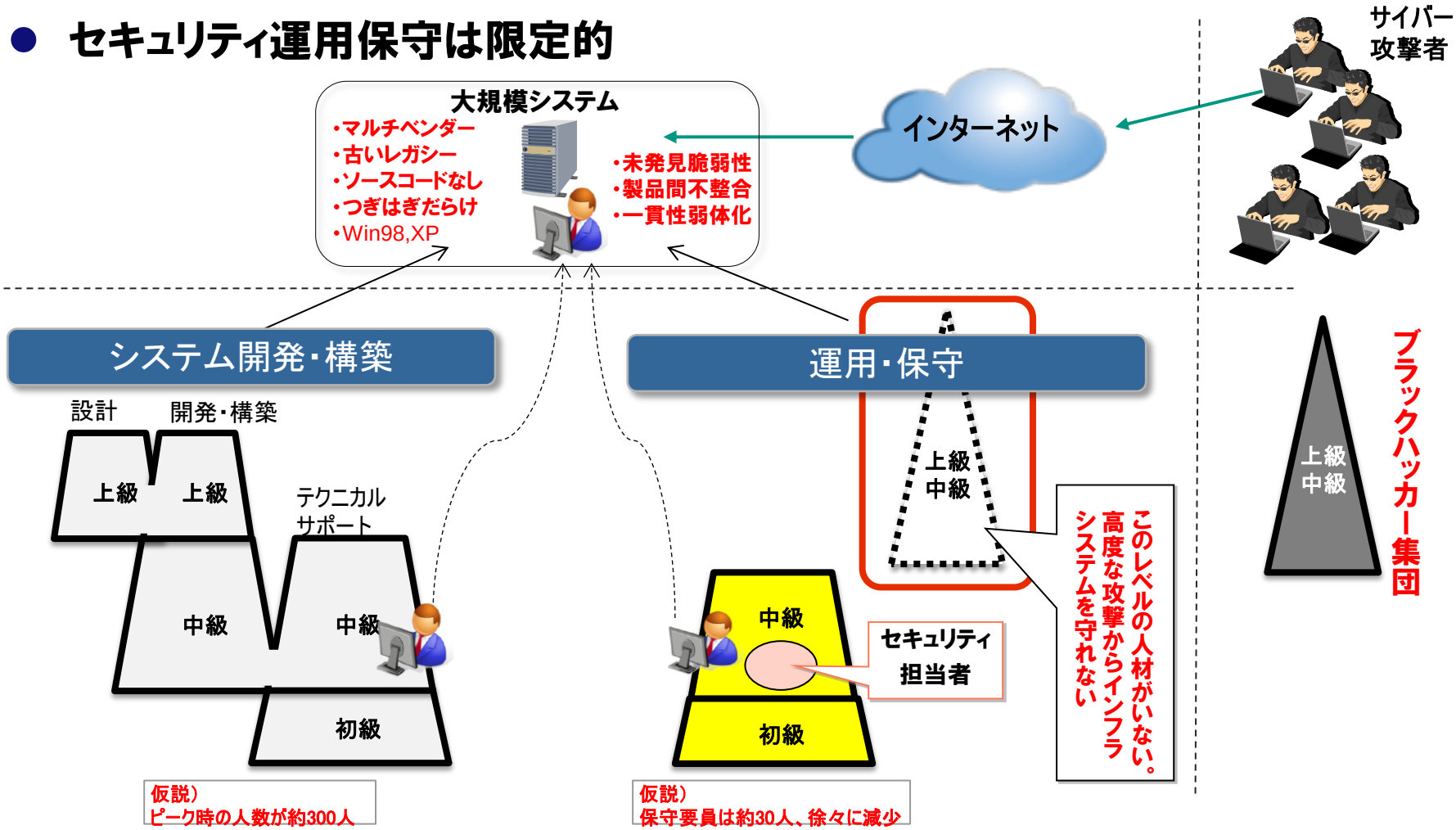
- あふれるIT技術者をサイバーセキュリティ技術者に配置転換できる
- セキュリティ製品、システム開発者はセキュリティを熟知している
- 何とかなる

構造的に攻撃に弱い

攻撃されるシステム

セキュリティ管理が切実なのは、運用・保守フェーズ

- 大規模インフラシステムほどサイバー攻撃の対象になりやすい
- セキュリティ運用保守は限定的



2011年からの3年間を振り返る

- 2011年、防衛企業に対するサイバー攻撃ショック
- 3年間で「サイバーセキュリティ」を口にする社内の人は劇的に増加（今では知らない人はいない）

- **しかし、サイバー攻撃を実際に受けて対応できる技術者が多くなった気はしない**
- **3年たっても増えていないのに、今後急に増える気はしない**

- 課題は単純ではなさそう

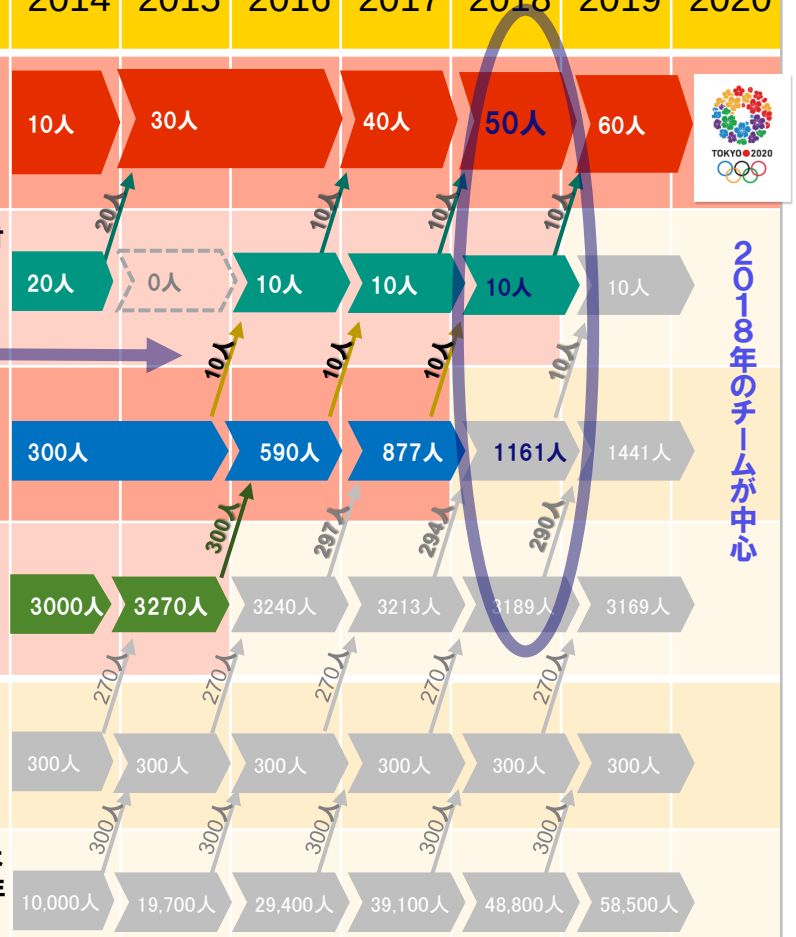
- **問題を見える化** するために、簡単なシミュレーションをしてみました

参考：サイバーセキュリティ人材像（７階層）と想定スキル

1	トップガン	サイバー攻撃を未然に防ぐ事ができるスキルを有し、サイバー攻撃に対して的確な「チームの指揮」を執ることができる。 確たる倫理観念を持っている。
2	トップガン補佐	サイバー攻撃を食い止めるスキルを有し、攻撃が内部に到達したときには、被害の拡大を防ぎ、問題個所を突き止めて除去できる。
3	中間層エリート （トップガン候補）	サイバーセキュリティの専門知識はあるが、臨機応変にいろいろな攻撃を防ぐ事ができるわけではない。
4	中間層 （2－3年以上の実務経験者）	担当業務システムの範囲内で、セキュリティ専門知識と知られた攻撃への対処スキルを有する。
5	中間層の卵 （実務経験１年未満）	基本的な教育は終え、適性があることも確認後、セキュリティ関連業務を行う部署へ配属されて間もない担当者。
6	基礎教育修了者	大学、大学院で2年間以上のセキュリティ教育を修めた者。
7	卵	高専、大学教養課程までの人材。体系だったセキュリティの知識は持っていない。

東京オリンピックをターゲットとした育成シミュレーション

スキルレベル	現状での人材数（想定人数の算定方法）	上位スキルレベルへの昇格イメージ
トップガン	現在10人以下 （セキュリティベンダーの中でも突出した専門スキルを有するスーパー人材。各社0人～2人）	―
トップガン補佐 （トップガンへの研修）	現在20人 （セキュリティに強いITベンダー10数社に在籍する人材。各社1～2人程度存在すると仮定）	トップガン補佐になった人材は100%トップガンに育成
中間層エリート	現在300人 （ITベンダーTOP50社、1社当たり6人程度存在すると仮定）	中間層エリートから有望な人材を毎年10人程度トップガン補佐として選抜
中間層	現在3000人 （従業員数3000人規模の上場企業トップ100社において、従業員の1%が中間層のセキュリティ運用者と仮定）	10%程度が中間層エリートに昇格
中間層の卵 （セキュリティ技術者として採用）	（300人採用／年） （ITベンダーTOP50社の中間層エリートが部下1名を雇用し、OJT指導すると仮定）	90%程度が中間層に昇格 10%は職種変更
基礎教育修了者 （大学、大学院卒）	（10,000人輩出／年） （理工系学部の上位200学部に在籍する学生、1学部50名程度育成と仮定）	中間層の卵に昇格するかは企業の採用数に依存。毎年300人と仮置き
卵（高専、大学）		

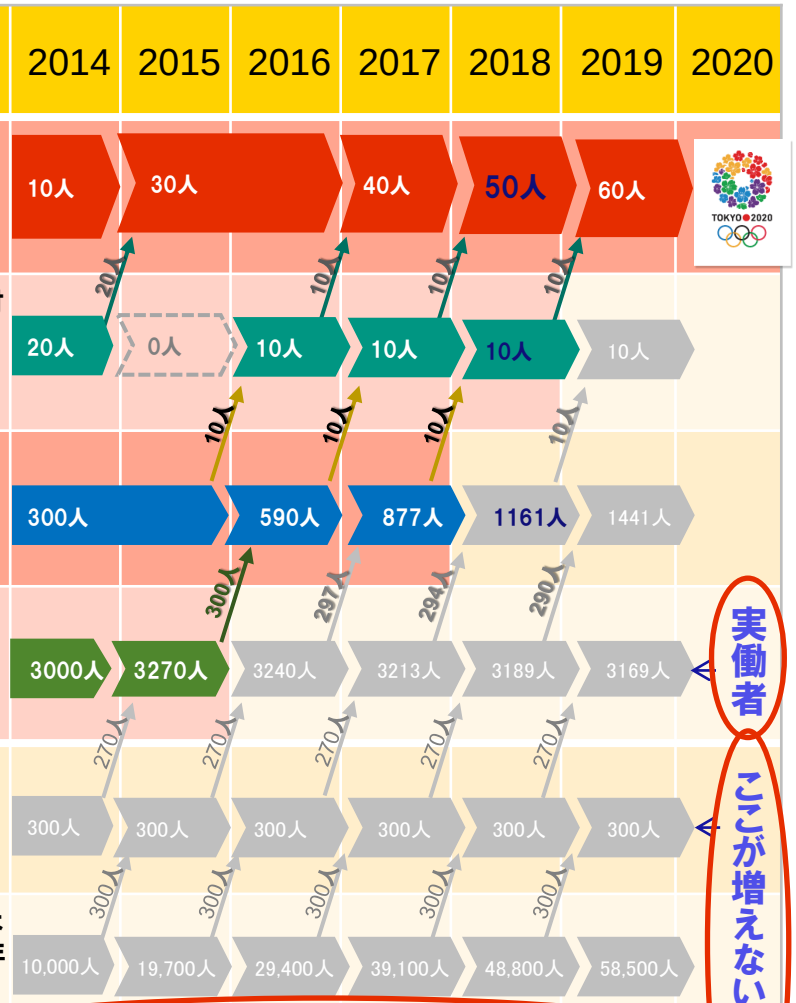


大学から人材育成していては間に合わないので市場の現役を活用！
ただし、市場の現役数は年を経てもさほど増えない！

シミュレーションでわかった課題

トップガンの獲得シナリオはよく見えない

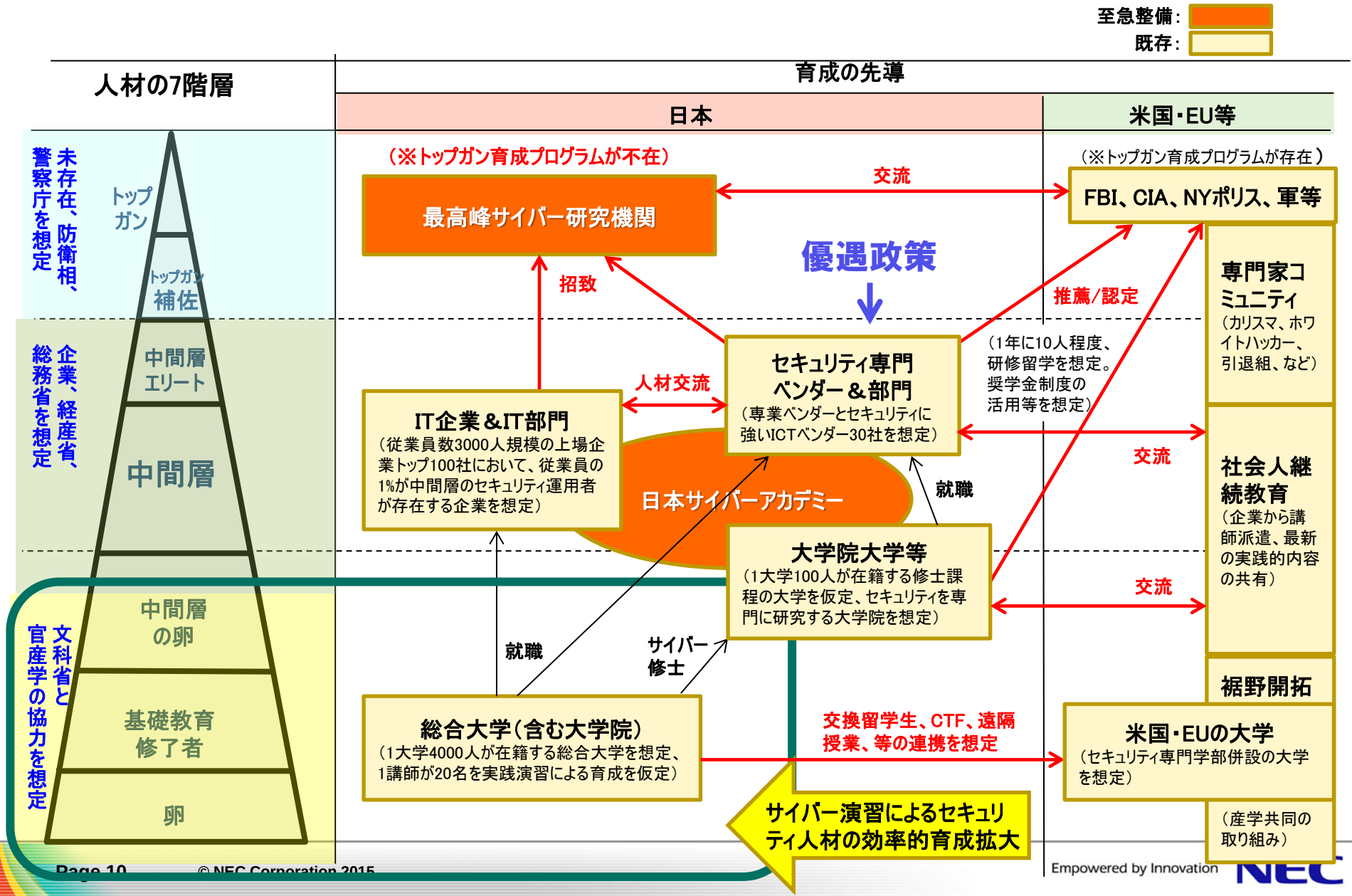
スキルレベル	現状での人材数（想定人数の算定方法）	上位スキルレベルへの昇格イメージ
トップガン	現在10人以下（セキュリティベンダーの中でも突出した専門スキルを有するスーパー人材。各社0人～2人）	―
トップガン補佐（トップガンへの研修）	現在20人（セキュリティに強いITベンダー10数社に在籍する人材。各社1～2人程度存在すると仮定）	トップガン補佐になった人材は100%トップガンに育成
中間層エリート	現在300人（ITベンダーTOP50社、1社当たり6人程度存在すると仮定）	中間層エリートから有望な人材を毎年10人程度トップガン補佐として選抜
中間層	現在3000人（従業員数3000人規模の上場企業トップ100社において、従業員の1%が中間層のセキュリティ運用者と仮定）	10%程度が中間層エリートに昇格
中間層の卵（セキュリティ技術者として採用）	（300人採用／年）（ITベンダーTOP50社の中間層エリートが部下1名を雇用し、OJT指導すると仮定）	90%程度が中間層に昇格 10%は職種変更
基礎教育修了者（大学、大学院卒）	（10,000人輩出／年）（理工系学部の上位200学部に在籍する学生、1学部50名程度育成と仮定）	中間層の卵に昇格するかは企業の採用数に依存。毎年300人と仮置き
卵（高専、大学）		



日本市場に潜在するセキュリティ教育修了者

すそ野を中間層に変換できないと現状は長く変わらない

セキュリティ人材の育成促進とキャリアパス



最高峰サイバー研究機関の目指すところ

至急整備：
既存：

最高峰サイバー研究機関

- 高度サイバー攻撃に対する実践的演習の場
- 攻撃手法の研究
- ダイナミックディフェンスのための研究
- ベンダーから買えないインテリジェンスの入手
- ホワイトハッカーを抱える場
- サイバーセキュリティ技術者のキャリアパスの最終目標

結果の活用

共同研究
人材交流

国内

・日本サイバー犯罪対策センター（JC3）
・制御システムセキュリティセンター（CSSC）
・Telecom-ISAC Japan
・IPA 独立行政法人 情報処理推進機構
・日本シーサート協議会
・日本セキュリティオペレーション事業者協議会
・不正通信防止協議会
・JPCERT/CC
・J-CSIP

海外

・IGCI（The INTERPOL Global Complex for Innovation）
・NCFTA（National Cyber-Forensics and Training Alliance）

日本サイバーアカデミーの目指すところ

至急整備：
既存：

日本サイバーアカデミー

- ワーキンググループを立ち上げ最新情報を分析
- 最高峰サイバー研究機関からの作業委託
- 三者で持ち出せるものを持ち寄り活動する場
- 全国で活動する
- セミナー/シンポジウム等の活動を行う
- 最先端情報共有のクラス

講師 etc.

IT企業＆IT部門

（従業員数3000人規模の上場企業トップ100社において、従業員の1%が中間層のセキュリティ運用者が存在する企業を想定）

知見 etc.

セキュリティ専門ベンダー＆部門

（専業ベンダーとセキュリティに強いICTベンダー30社を想定

場所 etc.

大学院大学等

（1大学100人が在籍する修士課程の大学を仮定、セキュリティを専門に研究する大学院を想定）

今やれることはやる！

サイバー人材育成への貢献

実践的サイバー防御演習　CYDER

総務省「サイバー攻撃解析・防御モデル実践演習の実証実験」プロジェクトを2013年度から受託。
NECが演習プログラムを作成・運用。（写真：2014年10月実施）

大学連携　寄付講座・共同研究

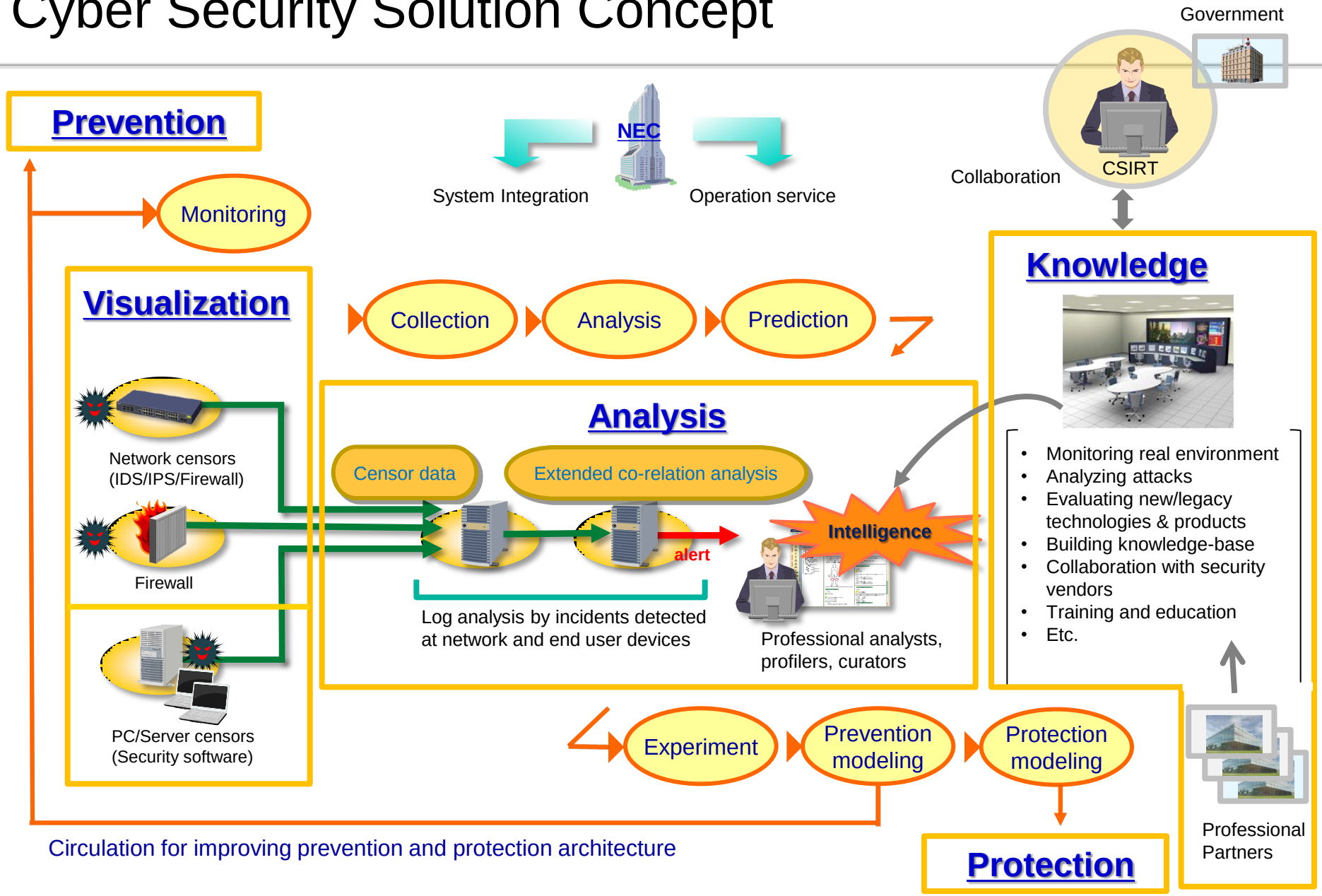
北陸先端科学技術大学院大学など各大学との寄附講座、インターン、共同研究の取組を推進。サイバーレンジを構築するため知見の研究、トップガン人材の輩出

ハッキングコンテストへの参加・協賛

若い年代、女性が参加する大会づくり、地方開催を支援するため、複数のコンテストに参加・協賛。セキュリティ人材の発掘、日本のセキュリティレベルを向上

サイバーセキュリティソリューションへの取り組み

Cyber Security Solution Concept



Cyber Security Factory

Cyber Security Factory

Knowledge, Operation Know-How, Monitoring Model accumulated and shared at Cyber Security Factory are feed backed to Human Asset and Technology Development

Partnership with Japan vendors

- ✓ Cyber Defense Institute
- ✓ Infosec
- ✓ LAC
- ✓ FFRI
- ✓ TrendMicro
- ✓ NRI Secure Technologies
- ✓ S&J Consulting

Partnership with oversea vendors

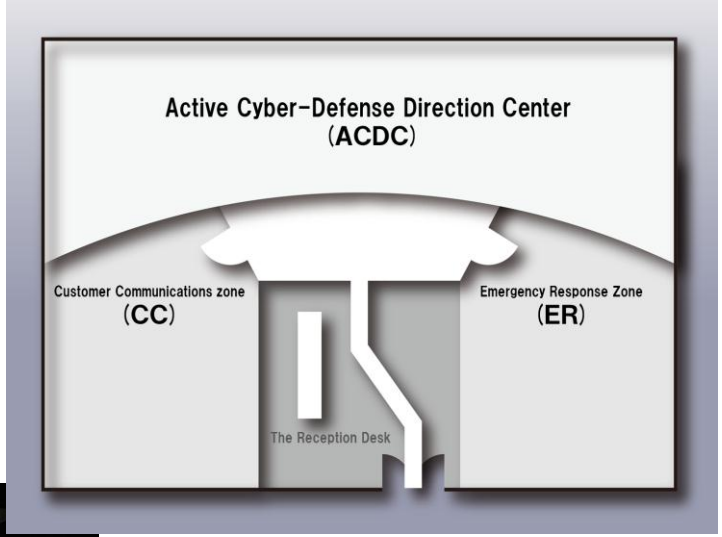
- ✓ On-going

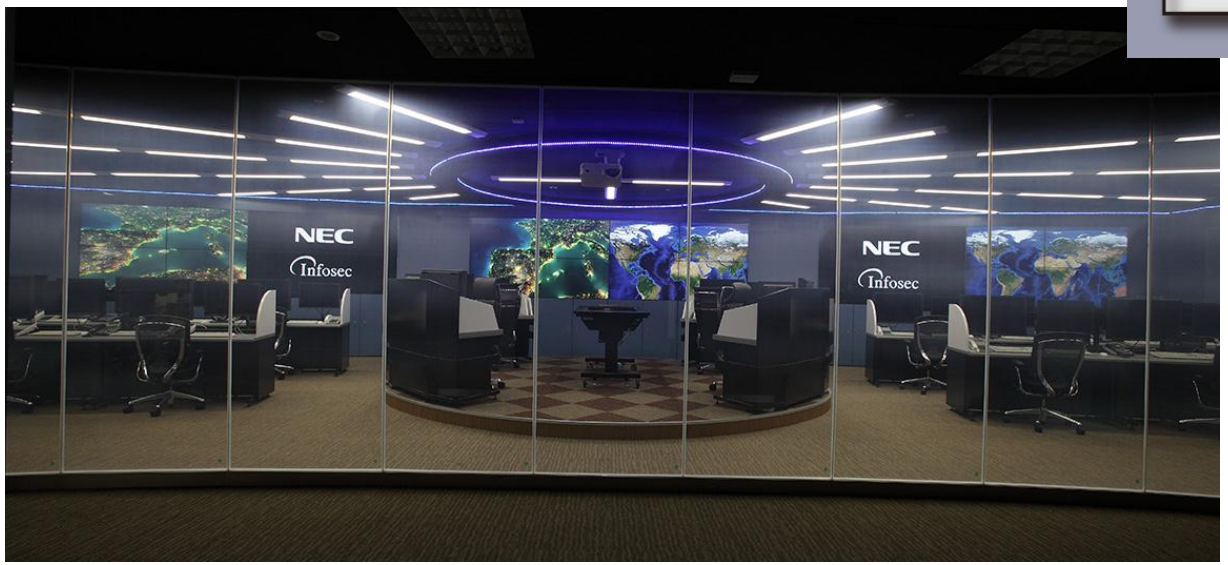
Cyber Security Operation

Cyber Security Operation Center

Cyber Security Factory consists of :

- *Active Cyber Defense Direction Centre (ACDC)*
  - ✓ *Security log monitoring,*
  - ✓ Incident response instructions
- *Emergency Response (ER) Room*
  - ✓ *Digital forensics*
  - ✓ *New products evaluation*
  - ✓ *Cyber exercise*
- *Customer Communication (CC) Zone*
  - ✓ Customer communication for incident response





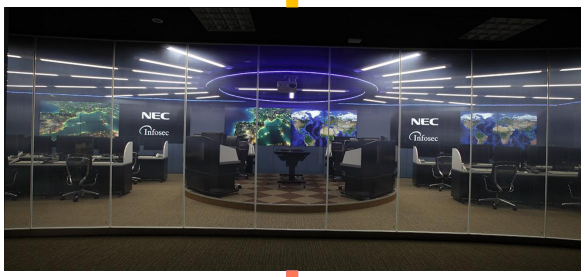
Active Cyber Defense Direction Center

Evolutional Cyber Security Operation

Cyber Security Operation

Yesterday's service

- Traditional SOC service
- Incident response



Today's service

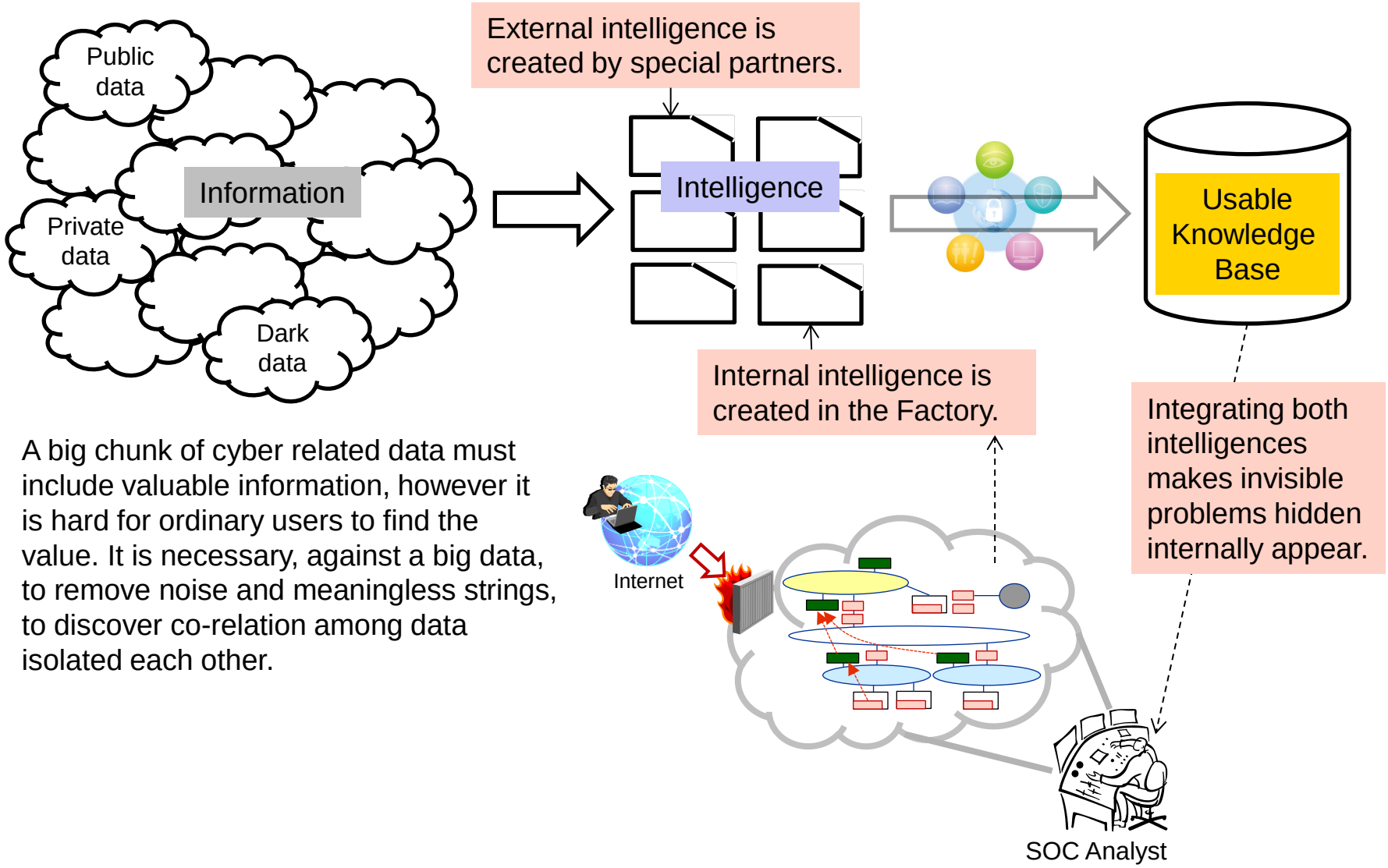
- Value-added SOC service
  - Intelligence added, still analyst-oriented problem solving
- Incident response & forensics service
- Protection semi-automated

Targeted service

- Next generation SOC service
  - Intelligence-dependent, internal monitoring integrated, knowledge-based problem solving
- Multi-layer protection integrated
- Dynamic prevention

Cyber Intelligence

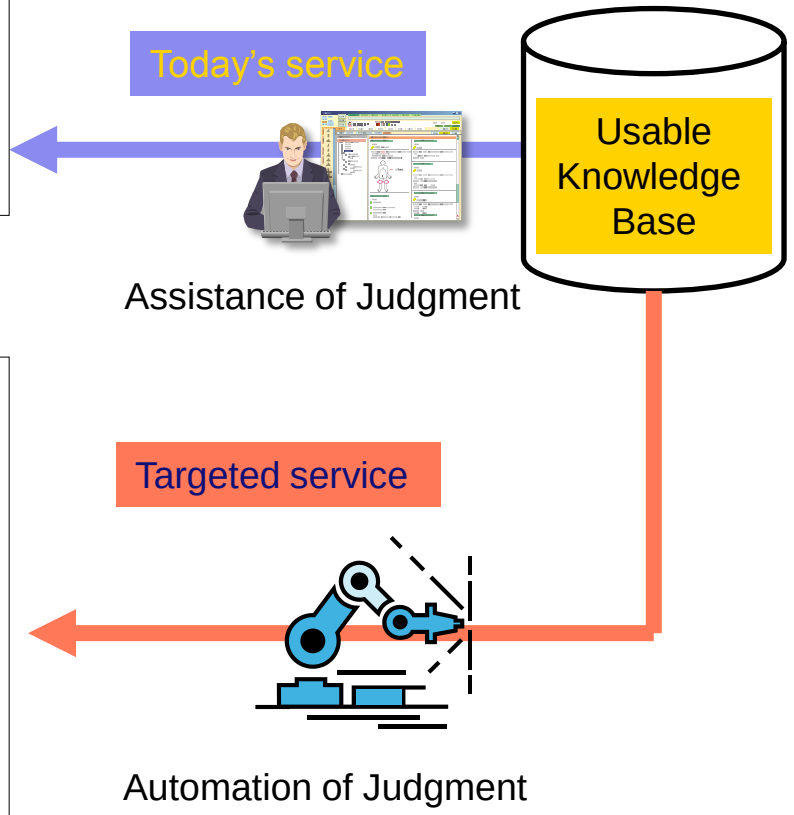
Making Information Usable



A big chunk of cyber related data must include valuable information, however it is hard for ordinary users to find the value. It is necessary, against a big data, to remove noise and meaningless strings, to discover co-relation among data isolated each other.

Value Proposition of Knowledge

- SOC analysts
- Forensics specialists
- IT security managers



- Effective operation
  - Easy-profiling by average engineers
- Speedy forensics
  - Narrowing analysis range by example
- Security policy update
- Intelligence-based prediction

Orchestrating a brighter world

世界の想いを、未来へつなげる。

未来に向かい、人が生きる、豊かに生きるために欠かせないもの。
それは「安全」「安心」「効率」「公平」という価値が実現された社会です。

NECは、ネットワーク技術とコンピューティング技術をあわせ持つ
類のないインテグレーターとしてリーダーシップを発揮し、
卓越した技術とさまざまな知見やアイデアを融合することで、
世界の国々や地域の人々と協奏しながら、
明るく希望に満ちた暮らしと社会を実現し、未来につなげていきます。

Empowered by Innovation

NEC