# 韓国の知識情報セキュリティ事情及び最近のイシュー

Jan 25, 2011

崔 正濬（チェ ジョンジュン）

KISIA
（株）イグルーセキュリティ

# Agenda

## 自己紹介

## Part Ⅰ　韓国の知識情報セキュリティ事情

- 韓国の知識情報セキュリティ関連組織、団体等紹介
- 韓国及び世界の知識情報セキュリティ市場
- サイバー侵害事故動向

## Part Ⅱ　最近の知識情報セキュリティ・イシュー

- 知識情報セキュリティ関連法制度の整備
- 融合セキュリティ
  - IT融合パラダイムと融合セキュリティ
  - スマートグリッド・セキュリティ
  - 融合セキュリティ管理・監視


# 自己紹介

# Profile

崔　正濬（チェ　ジョンジュン）

株式会社イグルーセキュリティ日本支社

IGLOO SECURITY

World-Class
Integrated Security Management
Solution & Service Provider

**ESM分野でのリーディング・カンパニー**

**最上位のセキュリティ基準を要求する政府機関及び大企業に製品提供**

**ESM分野卓越な技術力**

- （株）イグルーセキュリティ
- 設立：1999年
- 本社所在地：韓国ソウル
- 支社所在地：米国カリフォルニア、日本東京
- 社員数：230名. 売上： 310億ウォン（2010年）
- KOSDAQ上場（2010年）

- **事業分野**
  - Enterprise Security Management (ESM)
  - Converged Security Management (CSM)
  - Managed Security Service (MSS)
- **顧客社**
  - 250+ in Government, Public Services, Education, Telecom, Finance, etc.
  - Managed Security Service on 500+ sites

- **韓国で8年連続、ESM分野の市場占有率70%以上のリーディング・カンパニー**

# KISIA 紹介

**設立根拠**

- 情報通信産業振興法

**設立目的**

- 知識情報セキュリティ産業の健全な発展及び産業全般における知識情報セキュリティレベルと意識を高める。
  知識情報セキュリティ産業の事業環境造成及び会員相互協力を図ることにより、安全な知識情報化社会と国家経済に寄与する。

**沿　革**

- 1997. 8　情報セキュリティ産業協議会としてスタート
- 1998. 7.　韓国情報セキュリティ産業協会創立総会
- 2004. 9.　法定法人設立認可
- 2009. 9.　知識情報セキュリティ産業協会として再出帆
- 2010. 2.　第10代　李　得春　会長就任

# KISIA紹介

## 運 営 目 標

- 経済危機克服の為の雇用創出活性化
- 新規需要創出による知識情報セキュリティ市場拡散
- 業界代表団体としてのポジション強化

## 主な活動内容

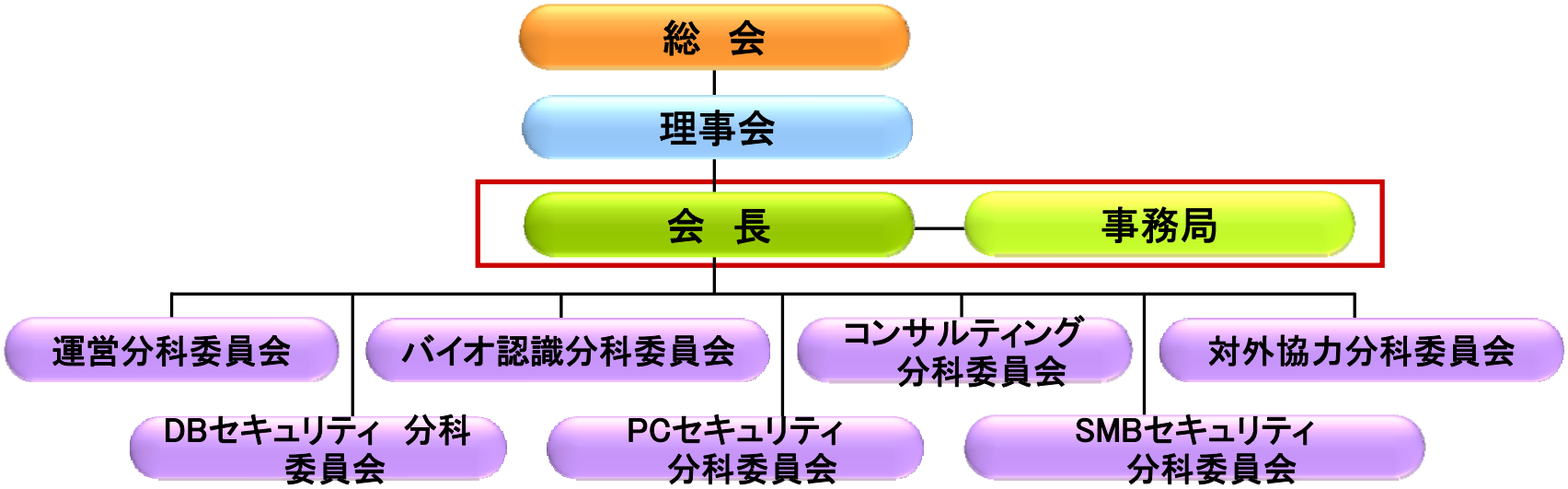
- 知識情報セキュリティ産業の活性化戦略樹立及び支援
- 業界としてのマーケティング活動及び会員社の海外進出支援
- 知識情報セキュリティ専門人材養成の支援

# KISIA紹介

## 会員社現況及び事務局

- 会　員　社　：　149社 (2010. 12.)
- 事　務　局　：　常勤副会長外 7名
- Homepage　：　www.kisia.or.kr　/ Tel : (02) 2142-0900 / Fax : (02) 2142-0909

## 組　　織



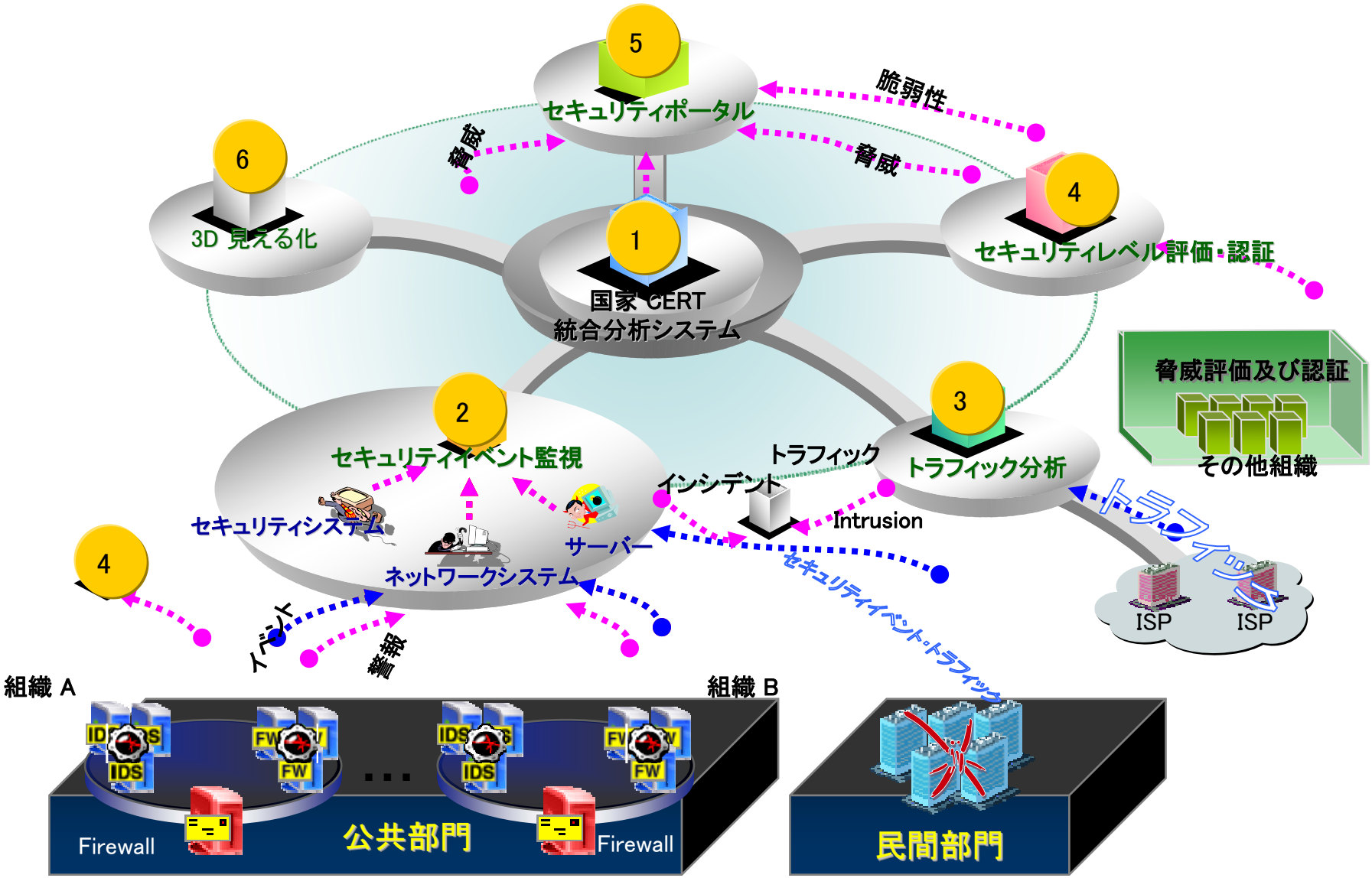
# Part I

# 韓国の知識情報セキュリティ事情

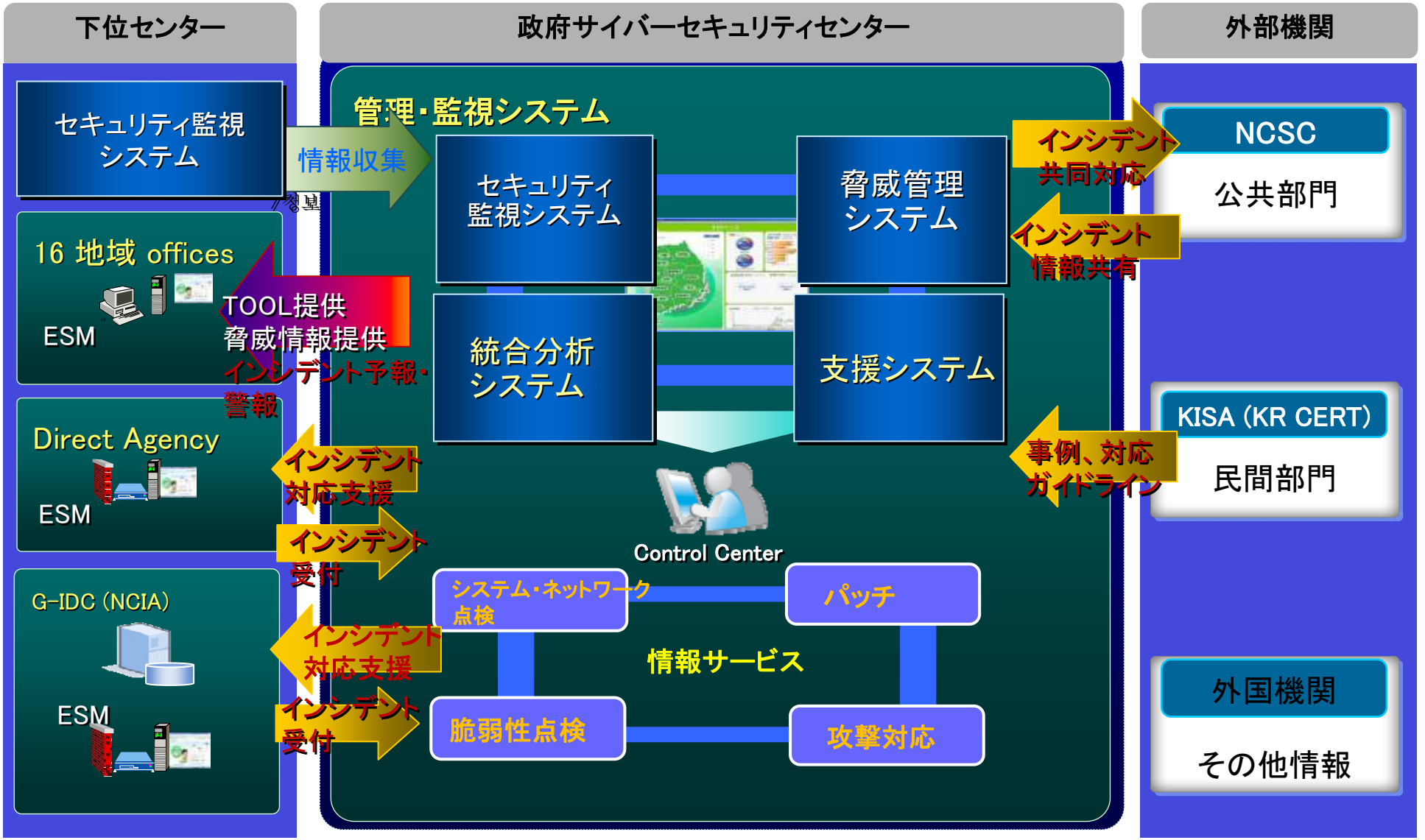
- 韓国の知識情報セキュリティ関連組織、団体等紹介
- 韓国及び世界の知識情報セキュリティ市場
- サイバー侵害事故動向

# 韓国の知識情報セキュリティ関連組織・団体

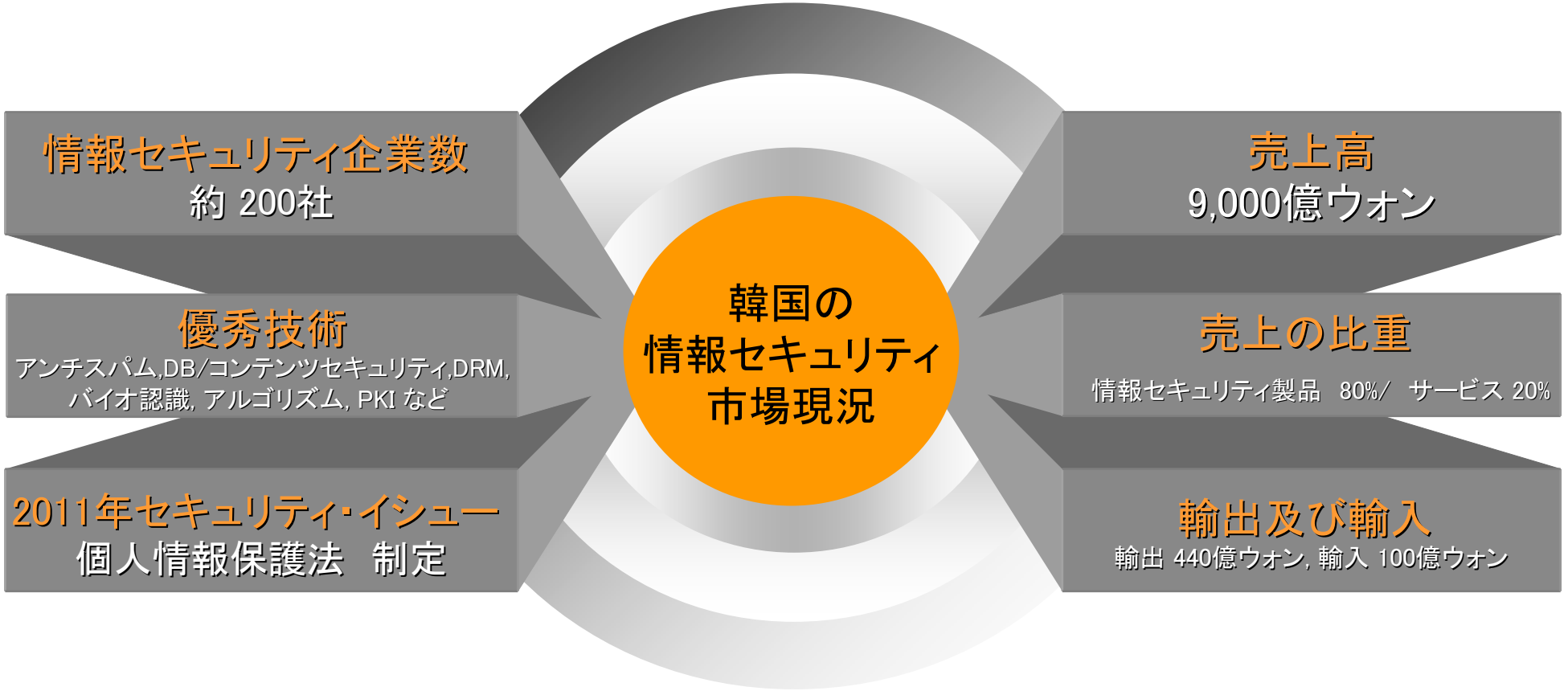
# 韓国の国家CERT セキュリティ管理・監視構造



# 韓国政府のCERTモデル



# 韓国の知識情報セキュリティ市場現況

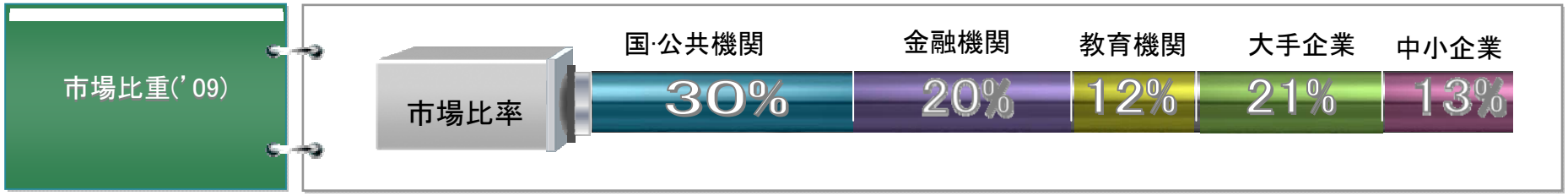



2009 国内 知識情報セキュリティ産業市場及び動向調査. 2009. KISA

# 分野別シェア

- 韓国は情報セキュリティサービス市場が比較的に小さい
- 公共市場の比重が大きく, 政府予算の増減に敏感に反応


＊世界分野別の市場規模('08) : SW(44%, 240億ドル), HW(13%, 71億ドル) ,サービス(43%, 231億ドル)
＊日本分野別の市場規模('09) : SW(42.5%, 2,927億円), HW(10.3%, 708億円), サービス(47.1%, 3,237億円)



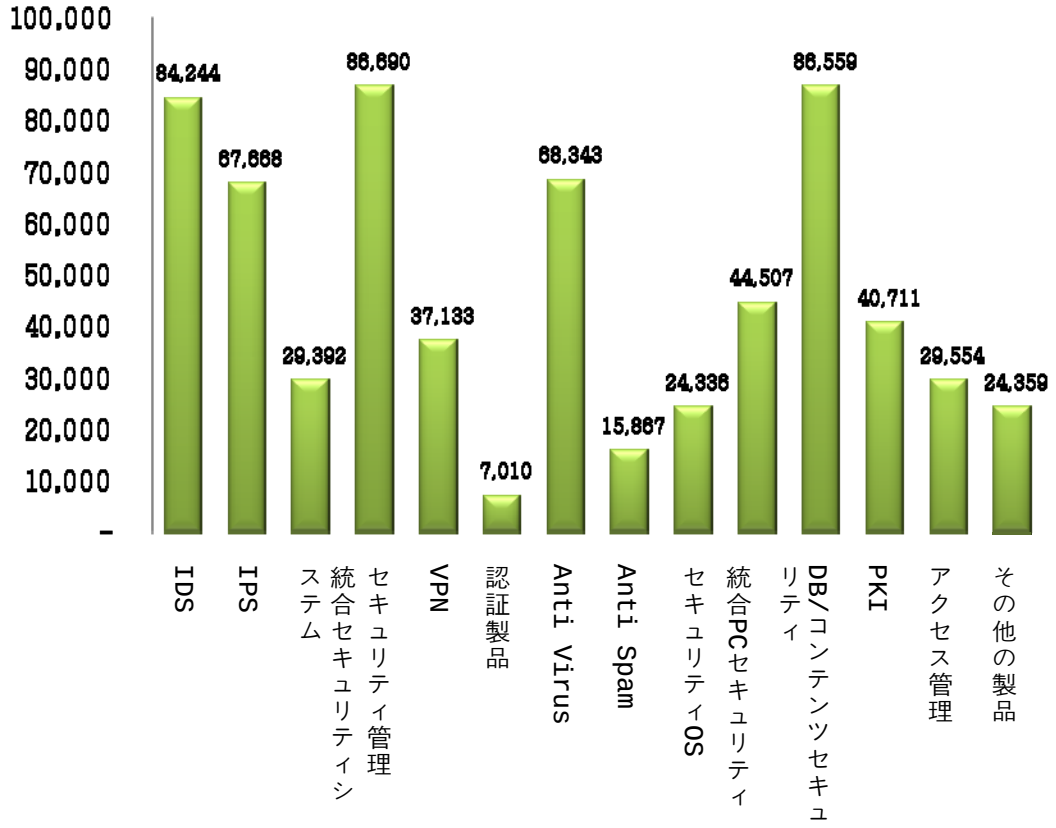

2009 国内 知識情報セキュリティ産業市場及び動向調査. 2009. KISA

# 製品及びサービス区分別売上

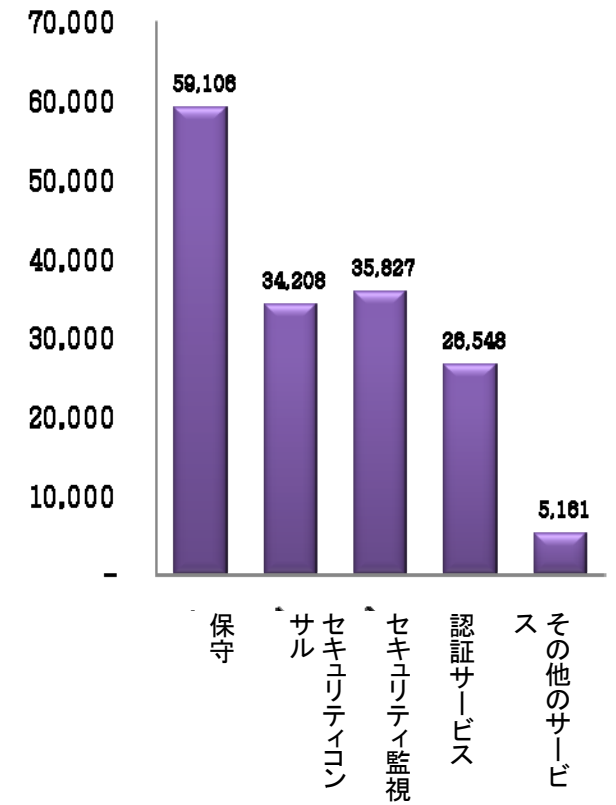
## ‘09年度情報セキュリティ市場の製品及びサービス区分別売上

### 情報セキュリティ製品

[ 単位 : 百万ウォン ]



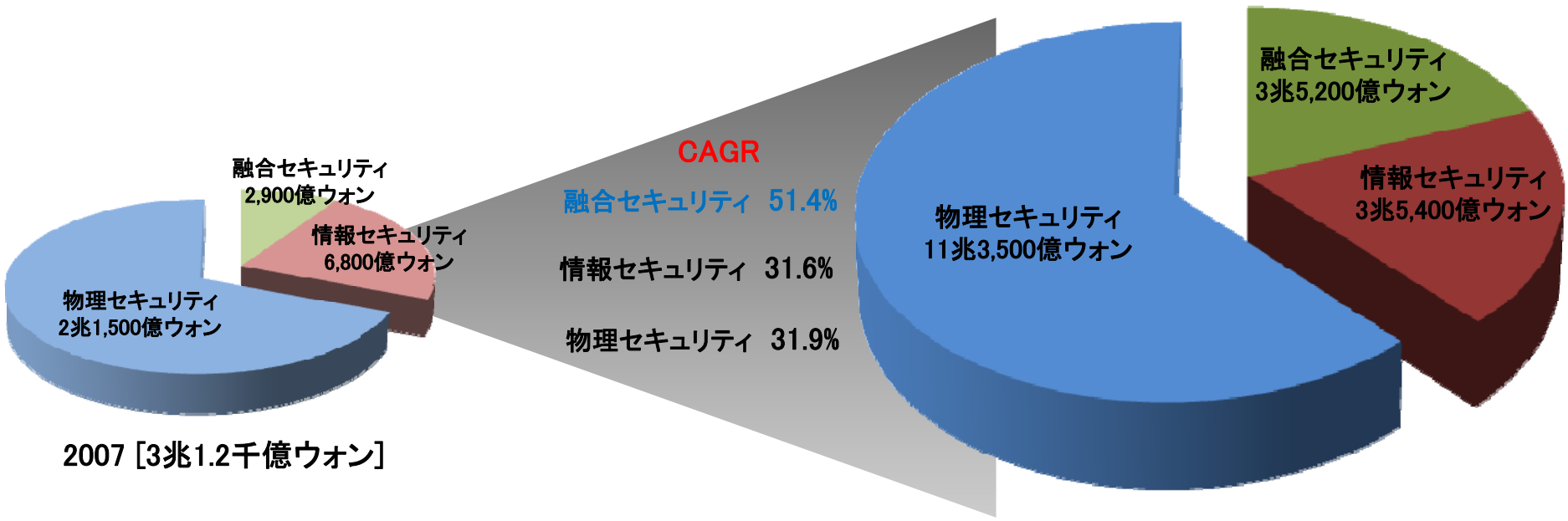

### 情報セキュリティサービス




2009 国内 知識情報セキュリティ産業市場及び動向調査. 2009. KISA

# 韓国の知識情報セキュリティ市場展望

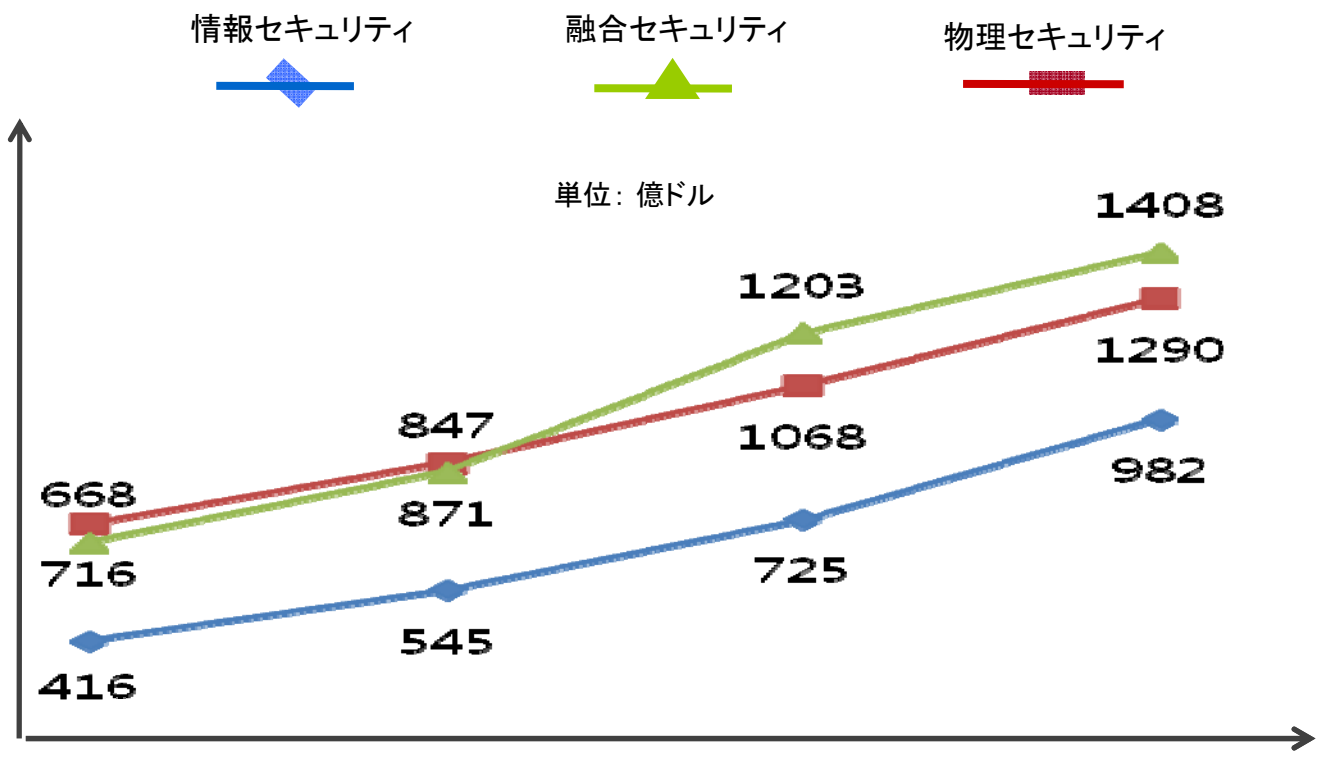
## 2013年まで知識情報セキュリティ産業は18兆ウォン規模の市場に拡大




出典：2009年、国内の知識情報保安の産業市場及び動向調査、KISA

# 世界の知識情報セキュリティ産業展望

## 2013年、世界市場規模は3,680億ドルに増加する展望




| 区分 | 2007 | 2009(E) | 2011(E) | 2013(E) | CAGR |
|---|---|---|---|---|---|
| 総額 | 1,800 | 2,263 | 2,995 | 3,680 | 12.7% |

出典：IDC 2008

# サイバー侵害事故動向

1. 2009.7.7 DDoS 侵害事故の発生
2. ソーシャル・メッセージング基盤のフィッシング多発
3. 偽セキュリティ製品の登場
4. オンライン・ゲームにて、ハッキング急増
5. 成績偽造のために、大学電算網ハッキング
6. 個人情報漏洩の被害者集団訴訟の判決
7. ホームページへの隠匿不正コードの持続的な脅威
8. 社会的イシュー、イベントを悪用した不正コードの流布
9. 応用プログラムのZero Day 攻撃増加

[出典: 放送通信委員会/行政安全部/知経部　2010 国家情報保護白書]

# 2009年、サイバー侵害事故の発生現況

- 総ハッキングの処理件数：21,230件．　前年15,940件、前年比33.2%増加．
- 発生分布：スパム・リレー（47.8%）＞ホームページ改ざん(20.3%）＞その他のハッキング（14.3%）＞単純侵入の試み(12.9%)

| 区分 | 2008年総計 | 2009年 | | | | | | | | | | | | 2009年総計 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | |
| ● ワーム・ウイルス | 8,469 | 460 | 641 | 695 | 925 | 941 | 837 | 886 | 879 | 1,591 | 844 | 1,002 | 694 | 10,395 |
| ● ハッキングの申告処理 | 15,940 | 1,579 | 1,119 | 1,285 | 1,582 | 1,863 | 2,319 | 2,200 | 2,704 | 2,676 | 1,748 | 1,011 | 1,144 | 21,230 |
| - スペム・リレー | 6,490 | 617 | 495 | 599 | 764 | 1,134 | 1,290 | 1,392 | 1,108 | 1,002 | 1,012 | 409 | 326 | 10,148 |
| -フィッシングの経由地 | 1,163 | 65 | 72 | 86 | 51 | 88 | 100 | 68 | 104 | 103 | 105 | 73 | 73 | 988 |
| -単純侵入の試み | 3,175 | 194 | 230 | 219 | 162 | 210 | 282 | 244 | 231 | 285 | 232 | 215 | 239 | 2,743 |
| -その他のハッキング | 2,908 | 277 | 225 | 291 | 299 | 238 | 261 | 245 | 241 | 247 | 252 | 199 | 256 | 3031 |
| -ホームページ改ざん | 2,204 | 426 | 97 | 90 | 306 | 193 | 386 | 251 | 1,020 | 1,039 | 147 | 115 | 250 | 4320 |

[出典: 韓国インターネット振興院（KISA）インターネット侵害事故の動向および分析　月報 2009年12月]

# Part II

# 最近の知識情報セキュリティ・イシュー

- 知識情報セキュリティ関連法制度の整備
- 融合セキュリティ
  - 融合産業と融合セキュリティ
  - スマートグリッドセキュリティ
  - 融合セキュリティ管理・監視


# 知識情報セキュリティ関連法制度の整備

# 個人情報保護法の制定

## 個人情報保護法

→ 官公庁のコンピューター、CCTVなど情報処理または送受信機能を持つ装備によって処理される 個人情報の保護の為に個人情報の扱いに必要な事項を定める。それによって公共事務の適切な遂行を図るとともに国民権益を保護する事を目的とし制定される。(1994年最初制定 -> 2010年3月改定)

### ▫ 個人情報流出事故多発、国民と企業の不安感が広がる

◎ '08年から大量の個人情報流出

| 2,234万人 | 600万人 | 2,650万人 |
|---|---|---|
| 2008年<br>大手ポータルD社、<br>ショッピングA社、<br>ガソリンスタンドG社など | 2009年<br>SNS大手S社など | 2010年<br>大手デパートS社など |

◎ 盗まれた個人情報はボイスフィッシング、金融取引詐欺名儀盗用などに悪用される。

- 住民番号、氏名、口座番号、ID,、PW、電話番号など

情報セキュリティ強化方針により
民間分野を含む
『個人情報保護法』立法推進

→ 2010年9月国会法案審査委員会通過
2011年、国会通過予定

# 『セキュリティ管理・監視センター』設置の義務化

## 国家サイバー安全管理規定(大統領訓令)

→ 国家サイバー安全の為の組織体系及び運営に関する事項を規定し、サイバー安全業務を行う各機関間協力を強化することにより、国家安保を脅かすサイバーテロから国家情報通信網を保護することを目的として <国家サイバー安全管理規定> 発令 (2005. 1. 31)

→ 2009年発生した ‘7.7DDos サイバーテロ’ 以降, セキュリティの重要性が社会全般に台頭
国民認識も高まる。

### 国家サイバー危機総合対策 (2009年 8月)

ハッキング、DDoS 攻撃、個人情報漏洩など国民の不安が広がり、政府は
『サイバー危機総合対策』(09年8月大統領に報告)を樹立し、国家的な対応体制を作った。

### 国家サイバー安全管理規定改定 (2010年 4月)
### 『セキュリティ管理・監視センター』義務化

- 全ての公共機関はサイバーテロを検知、分析して即時対応できるように『セキュリティ管理・監視センター』常設運営義務化
- 自前設立が不可能な場合はMSS専門企業からサービスを受けなければならない。

# 『セキュリティ管理・監視センター』設置の義務化

## トータルなセキュリティ管理・監視のためのソリューションが必要

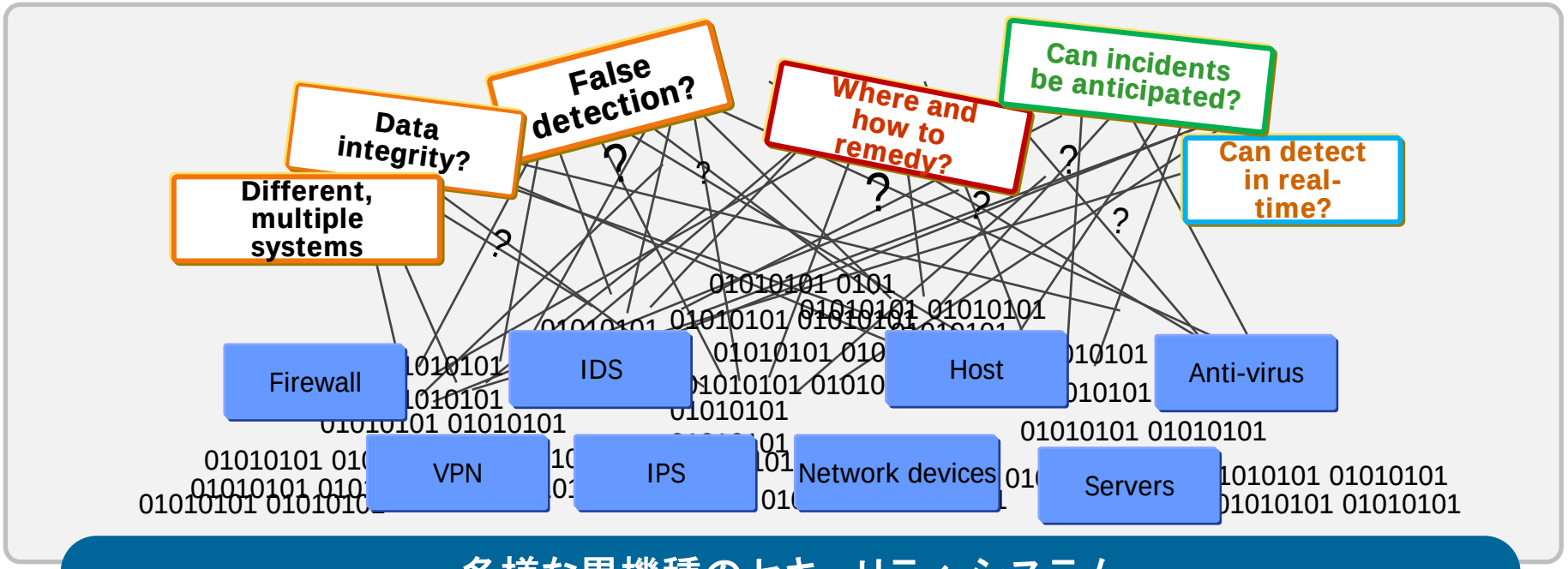
## 個別的管理・断片的情報による従来の管理方式

多数の異機種デバイスから発生する大量のイベントログを個別的に管理

多様なの技術に関して各々の専門知識を持っている多数の管理人材が必要

効率的管理及び運用不可能。

投入時間と人件費に比べて情報セキュリティは脆弱




多様な異機種のセキュリティ・システム

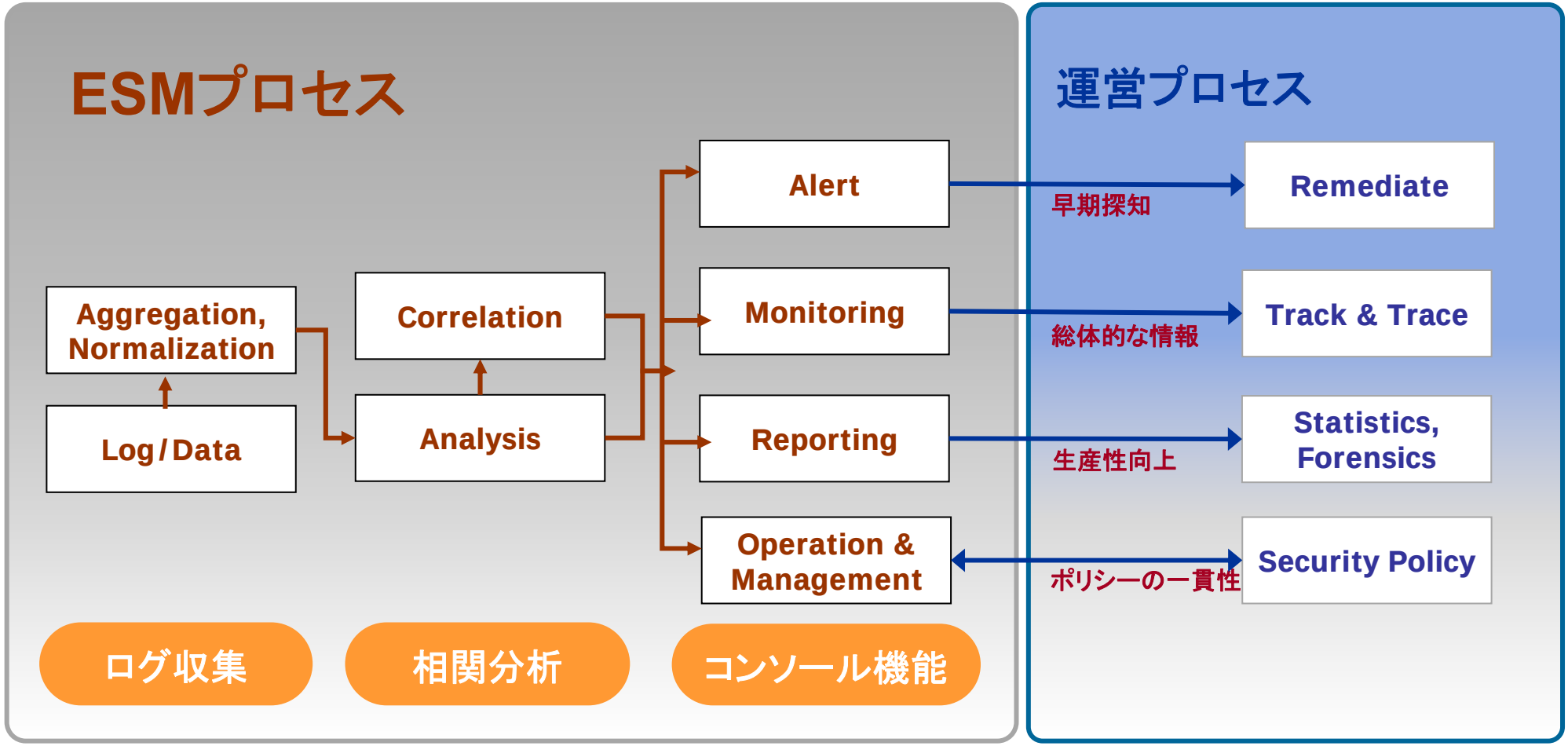
# 『セキュリティ管理・監視センター』設置の義務化

## 新しいアプローチ ： トータルなセキュリティ管理・監視（ESM）

全てのシステムとデバイスの統合管理　→ セキュリティ運用の効率性向上
深層的な相関分析を通じて早期探知及び予防措置が可能
システム、プロセス、ポリシー、組織の統合的運用のためのフレームワーク提供

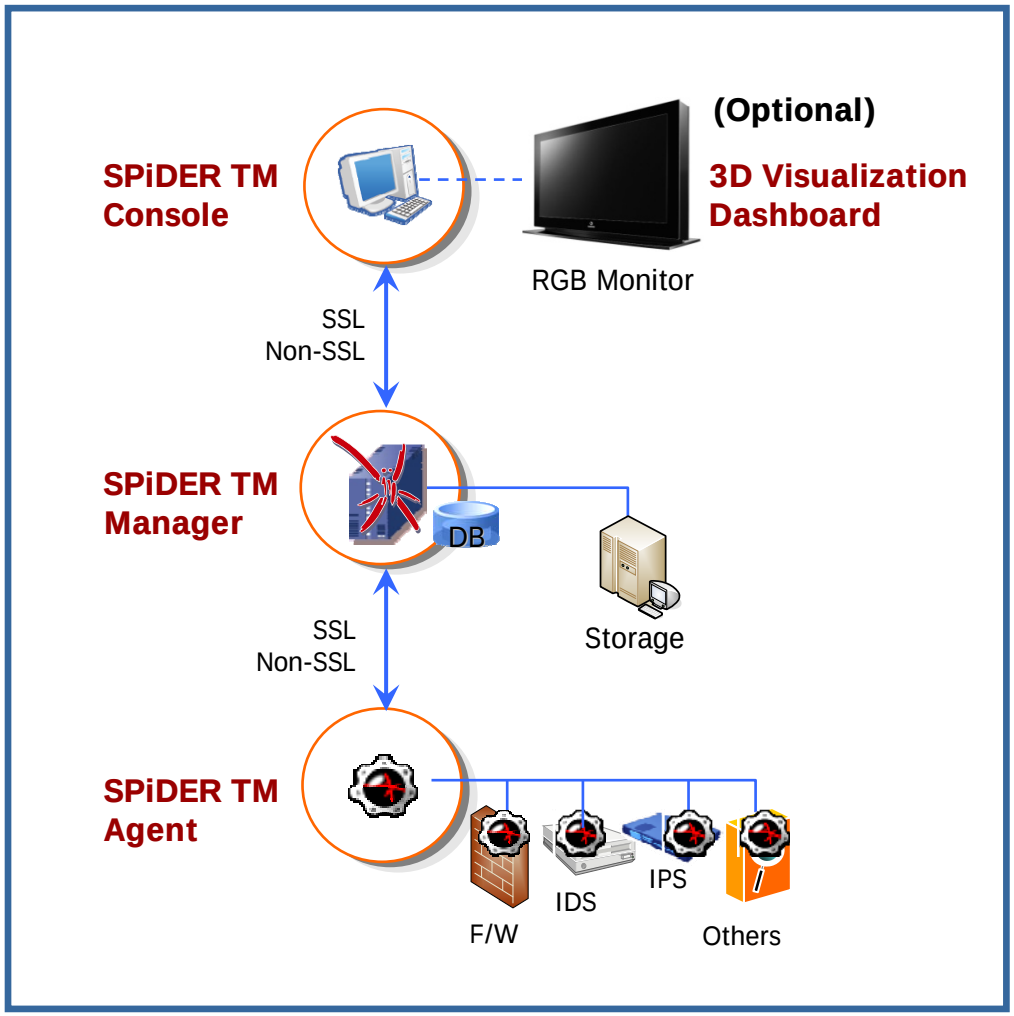
# 『セキュリティ管理・監視センター』設置の義務化

## ESMシステムの主要機能



# 『セキュリティ管理・監視センター』設置の義務化

## ESMの構造（例）




### Console

- 管理Console
- マネージャー及びエージェントの制御
- マネージャーとは、暗号化/非暗号化で通信
- ポリシー設定、モニタリング、分析/警報、データ検索、報告書作成など

### Manager

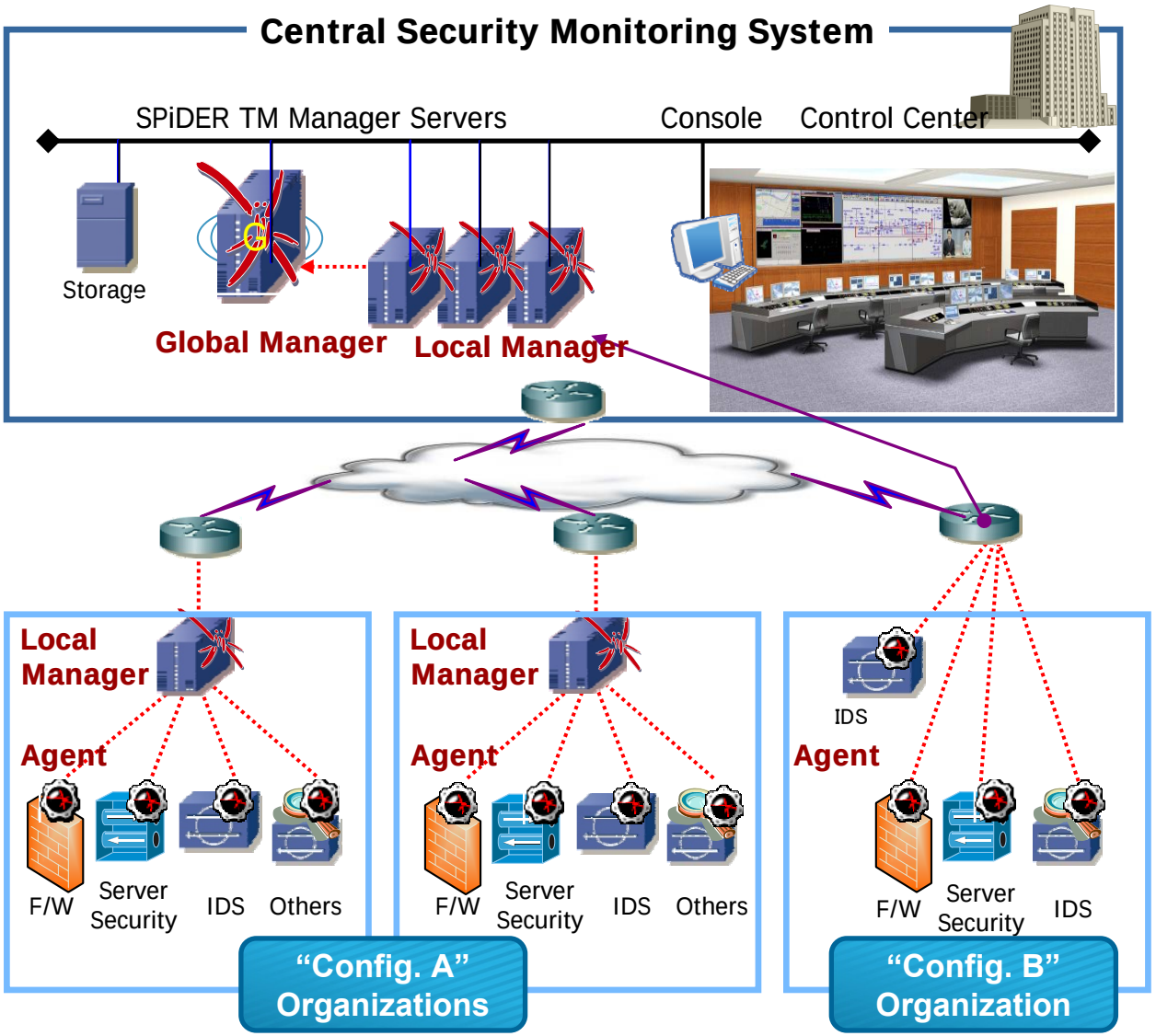
- 中央統制モジュールとしてDB使用
- データ保存(サーバーDiskの容量の超過時、外装ストレージ活用)
- ミドルウェアーを用いてコンソールと通信
- 警報およびセキュリティ・ポリシーの適用
- データの集合/保存、統計、相互関連分析など

### Agent

- 管理対象システム(セキュリティデバイス、サーバーなど)に搭載
- マネージャー収集ポリシーによって統制される
- セキュリティ・システムのログ、システムのアクセスログ、システム・リソース・データの収集
- 管理対象ファイルの無欠性点検
- Open Port、Backdoor、DoS検知

# 『セキュリティ管理・監視センター』設置の義務化

## ESMの構成（例）




## Overview

- 全てのセキュリティ・システムを統合管理
- 多様な異機種のセキュリティ・ システムからデータを収集・分析してトータル的に管理・監視を行う
- 脅威要素およびセキュリティ侵害事故に備えてセキュリティ運用の実効性と対応能力を向上

## System Configuration

- 3段階構造
  - SPiDER TM コンソール
  - SPiDER TM マネージャー (Global/Local)
  - SPiDER TM エージェント
- サイト内にエージェントとマネージャー設置および運用を通じて独自のセキュリティ監視遂行可能(A形態の構成)
- 状況によって、サイトにはエージェントのみ設置し、外部に存在するマネージャーによって監視遂行(B形態構成)


# 融合セキュリティ

- IT融合パラダイムと融合セキュリティ
- スマートグリッドセキュリティ
- 融合セキュリティ管理・監視

# IT融合パラダイムと融合セキュリティ

## 次世代の新成長動力の育成のため、『10大IT融合戦略産業』選定

成熟期に入り込んだIT産業の持続的な成長と伝統産業の競争力確保のため、IT融合パラダイム台頭

=> ITと他の産業間の融合は産業間の均衡成長と生産性向上,新製品開発及び新しいサービスの創出に寄与

韓国の未来企画委員会 : IT Korea未来戦略発表(2009. 09)

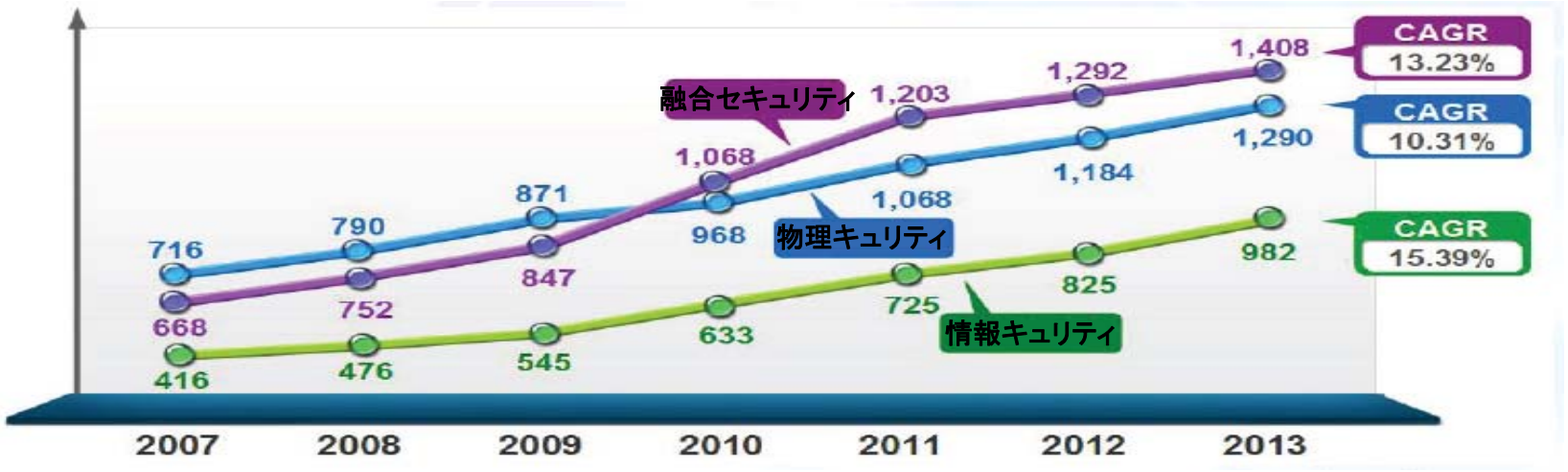
・波及効果の大きい１０大IT融合戦略産業の育成に注力
・IT融合技術へのR&D投資拡大 、IT融合拠点の構築 、グリーンIT国家戦略樹立等

# IT融合パラダイムと融合セキュリティ

## 融合セキュリティ

- 技術間融合,産業間融合時に発生するセキュリティ脆弱性を解決することにより、融合産業と製品に対する信頼性を提供して ， 製品の競争力強化に寄与
- 情報セキュリティと物理セキュリティの融合で、より安全安心なセキュリティを提供
- 融合セキュリティは知識情報セキュリティ産業の新たな成長の軸として浮上

[ ※世界知識情報セキュリティ産業市場展望]




[出処:IDC(2008) ]

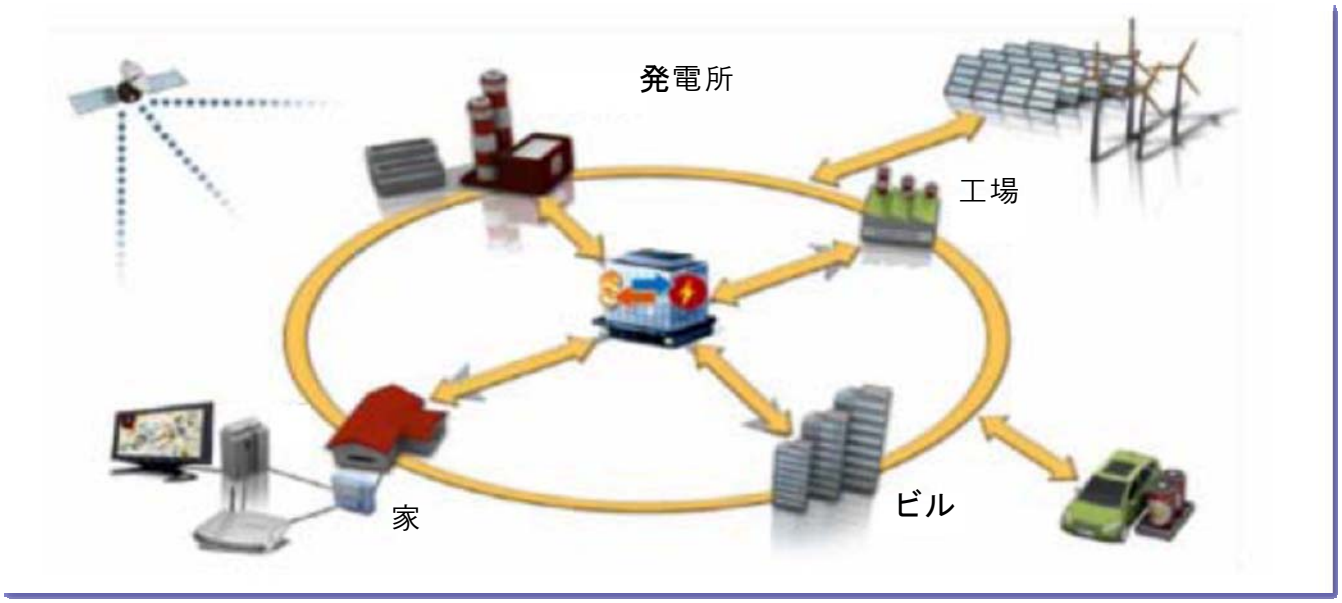
# スマートグリッド・セキュリティ

## スマートグリッド ： ITと電力産業の融合

- スマート グリッド(Smart Grid)とは、既存の電力網(発電->送電->配電->消費者)にITを活用して、供給者と消費者が両方向でリアルタイムの情報を交換することによって、エネルギー効率を最適化して、新しい付加価値を創り出す電力網のスマート化を意味する。

- スマート グリッド(Smart Grid)は多数の電力生産者と消費者との間の相互作用に基づいて、消費者にリアルタイムでの価格情報を提供して、消費者の合理的なエネルギー消費を誘導し、エネルギー効率性の向上に寄与する。

**< ※ スマート グリッドの基本構造>**




*資料:知識経済部(2010) / ‘スマート グリッド国家ロードマップ’

# スマートグリッド・セキュリティ

## 韓国のスマートグリッド推進状況

### 2030年まで世界初国家単位スマート グリッド構築

| 2010 ~ 2012 | 2013 ~ 2020 | 2021 ~ 2030 |
|---|---|---|
| ・リアルタイム需要反応システム構築<br>–リアルタイム料金制設計及び実証<br>・スマートグリッド拠点都市選定 | ・ 知能型電力取引システム構築<br>–電力取引ポータルの構築<br>–電力の卸売取引システム | ・統合電力システム構築<br>–国家連係電力取り引き統合サービス運営システム |

＊資料:知識経済部(2010) / ‘スマート グリッド国家ロードマップ’

**[※韓国のスマートグリッド構築目標]**

電力需要分散及びリアルタイム料金管理などにより、電気エネルギーの節約(6%,1.8兆ウォン/年)

CO2排出低減(2,700万トン/年、国家排出量の4.6%)

電力送配電の損失低減(損失率4% → 3%、年200億ウォン)

# スマートグリッド・セキュリティ

## スマートグリッドのセキュリティ脅威と対応準備の動向

- 両方向通信サービス(2way system)
- 商用ハードウェアとソフトウェア使用増加
- スマートグリッド システム接点増加
- スマートグリッド構成装備間の相互連結性増加
- 広範囲な地域に散在するスマートグリッド装備

**サイバー攻撃に対する**
**脆弱点及び運営危険増加**

### 関連法令内にセキュリティと関連した規定を含む

スマートグリッド活性化のための促進法にセキュリティ関連内容を含む予定　=>“知能型電力網構築及び利用促進に関する法律”制定推進

### スマートグリッド・ロードマップにセキュリティ対策を含む

2010年1月スマートグリッド国家ロードマップ確定(2010年～ 2030年)
-安全なスマートグリッドの為、‘セキュリティ・ガイドライン’用意
-国家単位スマートグリッドに適合したセキュリティ体系構築の支援
-スマートグリッドのセキュリティ標準用意及びセキュリティ認証制度運営

### スマートグリッド実証団地内にセキュリティ対策を用意

-スマートグリッド技術の試験・評価のため、実証団地を済州島に構築
-スマートグリッド実証団地でセキュリティ問題の解決努力

# 別紙

# ありがとうございました。

崔　正濬（チェ　ジョンジュン）
株式会社イグルーセキュリティ日本支社
Email: jjchoi@igloosec.com
Phone:03-3459-6323 , 080-3080-5469