KYUSHU UNIVERSITY 2011
100th Anniversary

サイバーセキュリティと社会情報基盤

国立大学法人九州大学
理事•副学長
安浦寛人

KYUSHU UNIVERSITY

現状

サイバーセキュリティは社会問題[2]

最近の事件

＊マウントゴックスのビットコイン取引停止。2014年2月
- 16億円相当のビットコインが不正に引き出し。
- 取引停止により、48億円相当が失われたとも言われる。

＊ベネッセの個人情報漏洩。2014年7月
- 3500万件の会員情報の漏洩で、経営危機に。
- システム担当の子会社の派遣社員が容疑者。

＊日本年金機構の個人情報漏洩。2015年5月
- 125万件の個人情報の漏洩。
- 標的型攻撃とずさんな内部セキュリティ管理による。

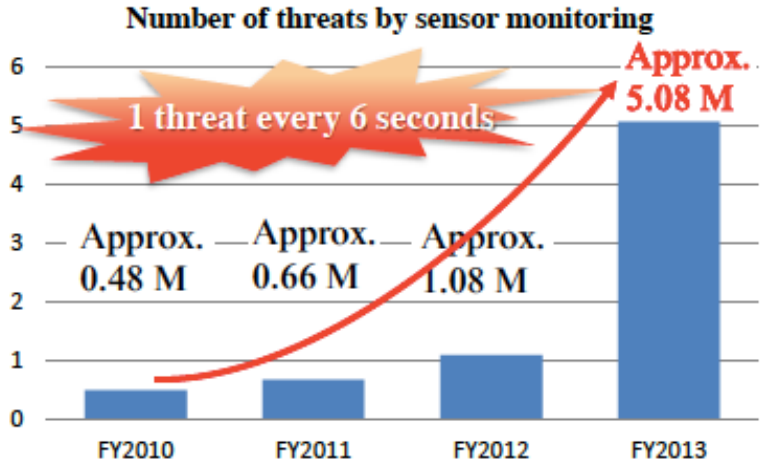
＊東京商工会議所の会員情報流出。2015年6月
- 1万2000件の会員情報。
- 標的型攻撃と見られる。

サイバーセキュリティを取り巻く状況

急激に増加するサイバー犯罪

- サイバー犯罪の損失額は全世界で年間59兆円（2014年）
- 日本の政府機関を標的にしたH25年度のサイバー攻撃は約508万件（→前年度に比べ5倍に急増）
- 手口も巧妙化→サイバー攻撃の脅威は急速に拡大
  - 毎秒1個のペースでウィルスやワームが新しく作られている
- サイバーセキュリティの被害者の6割強が18歳から31歳
  - 被害者が間接的な加害者になるリスク

- 状況の変化は極めて急速、問題は拡散し、グローバル化
  - 「国家安全保障」や「危機管理」上の最重要課題
  - 重要インフラの防護に最善の措置の導入が不可欠
  - 情報の自由な流通を確保し、常に深刻化するリスクに対し新たな対応の強化が必要



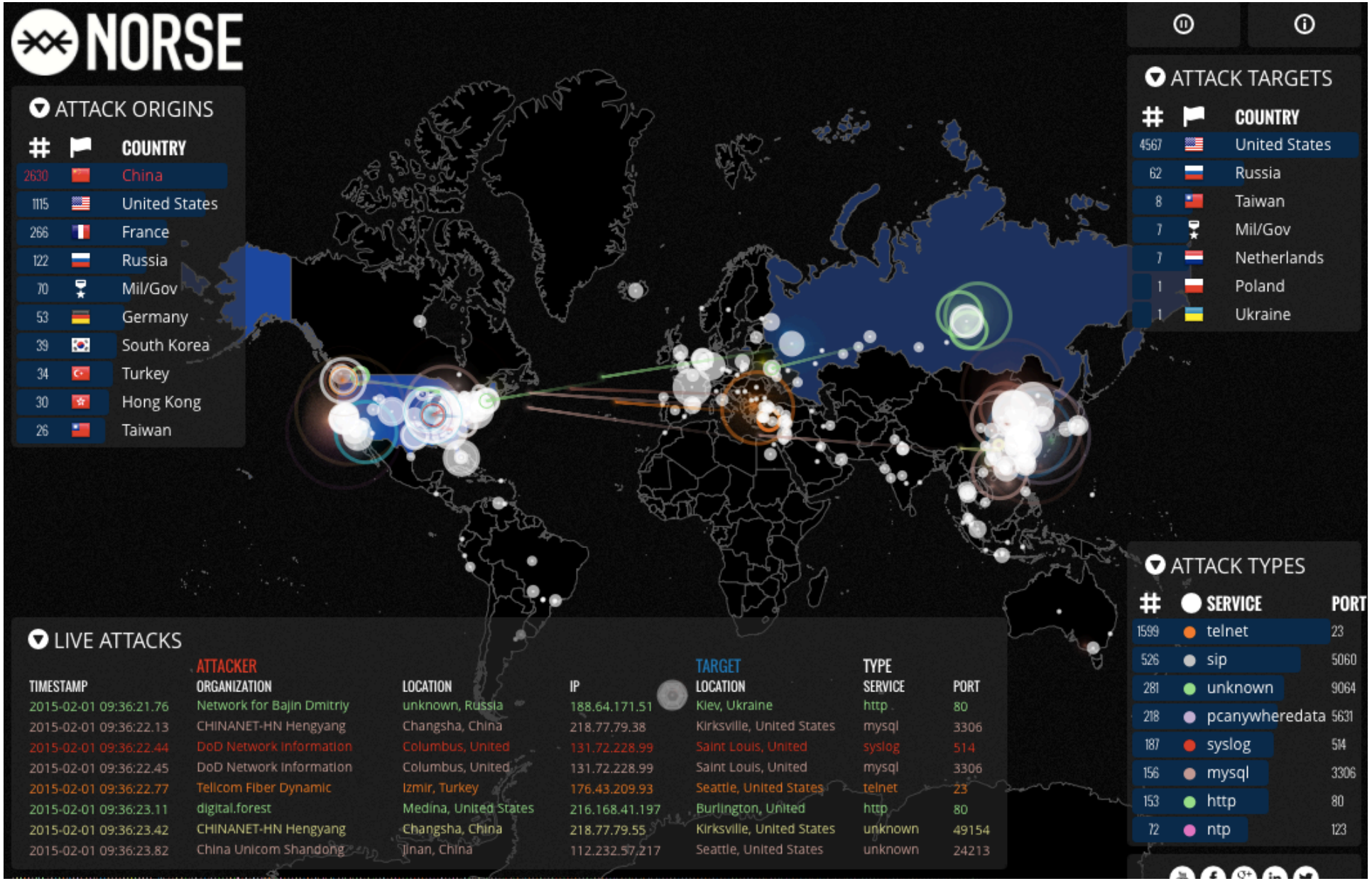
ウィルスやワームの増加

マルウェア:Malware(Virus and Warm)
毎日10万種類の新型が作られる
毎秒1個のペース

Source: McAfee

サイバー空間は戦場

http://map.ipviking.com



新たな国防問題

The Price of Progress…

UMBC
AN HONORS UNIVERSITY IN MARYLAND

兵力の侵攻なき破壊

Kevin “KAL” Kallaugher, The Economist – Jun 9, 2012

サイバー戦争

* 2010年、イランの核施設の機器破壊。
  - Stuxnetと呼ばれるウィルスによってイラン国内のネットワークを破壊。
  - イスラエルの諜報機関が行った？
* 2012年、サウジアラムコの30,000台のコンピュータがダウン。
  - Shamoon攻撃と呼ばれる。石油産業が停止。
* 2014年、ソニーエンターテイメントへの攻撃。
  - 社員情報や映画作品の漏洩。新作の発表の遅延。
  - 北朝鮮からの攻撃と推定。
* 2014年、Sony PlaystationとX boxのサーバーへの攻撃。
  - DDoS攻撃

サイバー攻撃の技術

* 暗号解読：暗号化された通信情報を解読して秘匿情報を読み取る。パスワード等の取得にも利用。
* DoS攻撃／DDoS攻撃：一斉にアクセスをかけて、ウェブサイトに大きな負荷をかけて、利用不能にする。
* SQLインジェクション：DBを改ざんする。
* クロスサイトスクリプティング：ページを閲覧したユーザーに不正プログラムを送りつける。
* ルートキット攻撃：他人のコンピュータに不正侵入して、その痕跡をわからないようにする。
* ウィルス／ワーム：送り込まれる不正プログラム。メールや不正ページのアクセスで感染する。
* フィッシング、トロイの木馬、標的型攻撃。
* ゼロディ攻撃：脆弱性を公表以前に攻撃する。

何が狙われるか？

＊愉快犯から窃盗、詐取、破壊活動へ

＊組織や個人の重要情報の詐取
- 個人情報や個人資産
- 企業の秘密情報や情報化資産
- 電子的資産（電子マネーや電子化証券）
- 国家機密

＊情報システムや社会システムの破壊
- ホームページの破壊や改ざん
- 企業の基幹システムの破壊
- ライフラインの破壊（電力網、水道、ガス、交通信号など）
- 社会システムの破壊（金融システム、行政システムなど）
- 防衛システムの破壊（軍事ネットワーク）

対策

サイバーセキュリティ基本法の概要

別添１

第Ⅰ章．総則

■目的（第1条）

■定義（第2条）

⇒「サイバーセキュリティ」について定義

■基本理念（第3条）

⇒ サイバーセキュリティに関する施策の推進にあたっての基本理念について次を規定

① 情報の自由な流通の確保を基本として、官民の連携により積極的に対応

② 国民1人1人の認識を深め、自発的な対応の促進等、強靱な体制の構築

③ 高度情報通信ネットワークの整備及びITの活用による活力ある経済社会の構築

④ 国際的な秩序の形成等のために先導的な役割を担い、国際的協調の下に実施

⑤ IT基本法の基本理念に配慮して実施

⑥ 国民の権利を不当に侵害しないよう留意

■関係者の責務等（第4条～第9条）

⇒ 国、地方公共団体、重要社会基盤事業者（重要インフラ事業者）、サイバー関連事業者、教育研究機関等の責務等について規定

■法制上の措置等（第10条）

■行政組織の整備等（第11条）

第Ⅱ章．サイバーセキュリティ戦略

■サイバーセキュリティ戦略（第12条）

⇒ 次の事項を規定

① サイバーセキュリティに関する施策の基本的な方針

② 国の行政機関等におけるサイバーセキュリティの確保

③ 重要インフラ事業者等におけるサイバーセキュリティの確保の促進

④ その他、必要な事項

⇒ その他、総理は、本戦略の案につき閣議決定を求めなければならないこと等を規定

第Ⅲ章．基本的施策

■国の行政機関等におけるサイバーセキュリティの確保（第13条）

■重要インフラ事業者等におけるサイバーセキュリティの確保の促進（第14条）

■民間事業者及び教育研究機関等の自発的な取組の促進（第15条）

■多様な主体の連携等（第16条）

■犯罪の取締り及び被害の拡大の防止（第17条）

■我が国の安全に重大な影響を及ぼすおそれのある事象への対応（第18条）

■産業の振興及び国際競争力の強化（第19条）

■研究開発の推進等（第20条）

■人材の確保等（第21条）

第Ⅲ章．基本的施策（つづき）

■教育及び学習の振興、普及啓発等（第22条）

■国際協力の推進等（第23条）

第Ⅳ章．サイバーセキュリティ戦略本部

■設置等（第24条～第35条）

⇒ 内閣に、サイバーセキュリティ戦略本部を置くこと等について規定

附則

■施行期日（第1条）

⇒ 公布の日から施行（ただし、第Ⅱ章及び第Ⅳ章は公布日から起算して1年を超えない範囲で政令で定める日）する旨を規定

■本部に関する事務の処理を適切に内閣官房に行わせるために必要な法制の整備等（第2条）

⇒ 情報セキュリティセンター（NISC）の法制化、任期付任用、国の行政機関の情報システムに対する不正な活動の監視・分析、国内外の関係機関との連絡調整に必要な法制上・財政上の措置等の検討等を規定

■検討（第３条）

⇒ 緊急事態に相当するサイバーセキュリティ事象等から重要インフラ等を防御する能力の一層の強化を図るための施策の検討を規定

■IT基本法の一部改正（第４条）

⇒ IT戦略本部の事務からサイバーセキュリティに関する重要施策の実施推進を除く旨規定

大学の構成員数(2014年度)

身分	人数
学部生	11,859
修士課程学生	3,912
博士課程学生	2,758
専門職大学院	317
学生の小計	(18,846)
教員	2,106
事務･医療･技術職員	1,999
その他職員	3,831
職員の小計	(7,936)
総計	26,782

KYUSHU UNIVERSITY 学生のPC必携化

- BYOD(Bring Your Own Device)
- パソコンなしでは済まない教育•研究環境
  - パソコン用教室が12部屋では全く不足
- 何時でも、何処でも、自分のペースで、自由に学習できる環境の構築
  - Web学習システム
  - オンライン教材やe-portfolio
  - MOOCs
- ガラパゴス大学にならないために
  - ソフトウェア（Office、ウイルス対策）
  - 無線LANの整備
  - ファイアウォールの整備（著作権侵害防止）
  - 事前の講習会を実施
- 情報セキュリティとしては大きなリスク

情報セキュリティポリシー

特徴

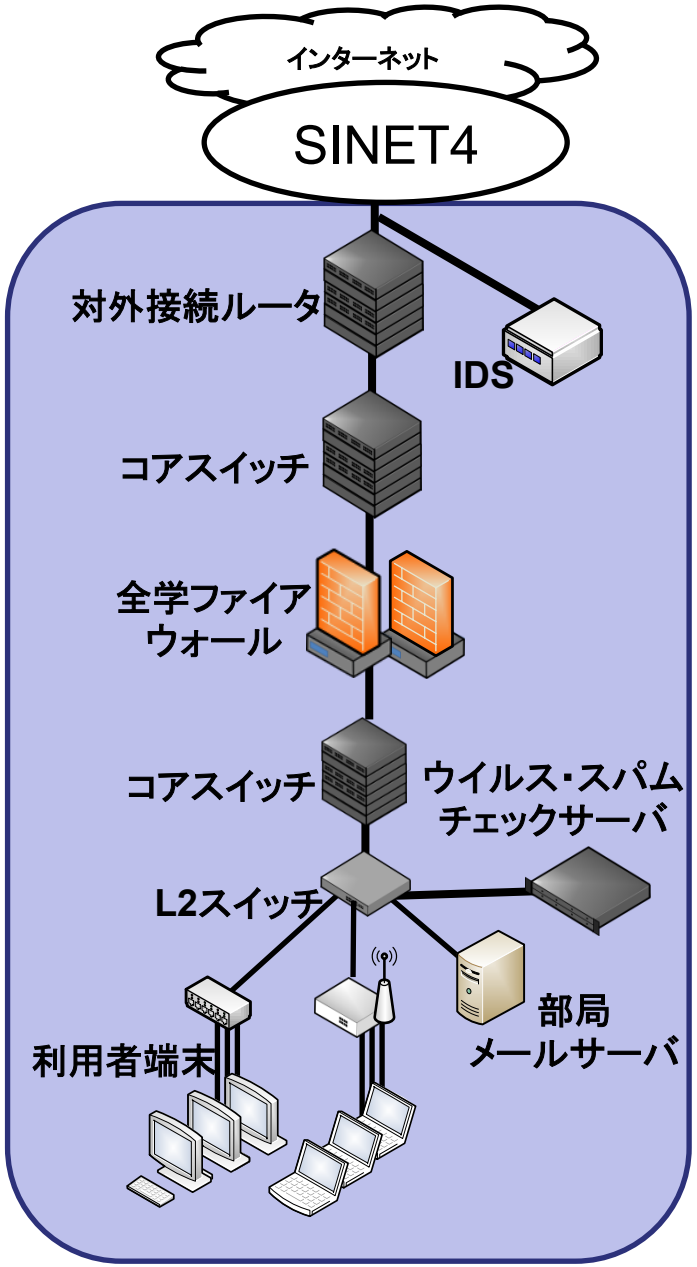
- 基本方針を説明するだけでなく、ガイドラインを含む
- 医療系のセキュリティポリシーは一般よりも厳しくあるべきである との考えから別立て
- 部局長会議等での審議、情報統括本部の広報を通じて学内に浸透
- 平成14年度に策定され、平成22年度に第二版を策定、現在では 第三版となっている。

ポリシーの概要

- 前文
- 1. 情報システム運用基本方針
- 2. 定義等
- 3. 組織・体制
- 4.情報の格付け、分類と管理
- 5.物理的セキュリティ保護の方針
- 6.情報システムを取り扱う者の留意事項
- 7.セキュリティポリシーの実施、評価及び見直し

KYUSHU UNIVERSITY

情報セキュリティ対策への取り組み



対外接続のポート制限

危険性の高いポートをフィルタリングで遮断

侵入検知システム（IDS）

ウイルス感染，脆弱性への外部からの攻撃等の検知

全学ファイアウォールシステム

・URLフィルタリング，脆弱性防御機能
・アクセス規制（HTTP/HTTPS通信，動画・音楽ファイルのダウンロード等）

ウイルス・スパムメールチェックサービス

ウイルスメールの検出，スパムメールの判定

ウイルス対策ソフト提供サービス

SymantecEndPoint を本学構成員に提供（インストール対象は，大学所有PC，本学学生，職員，名誉教授が所有する個人PC（1人1台））

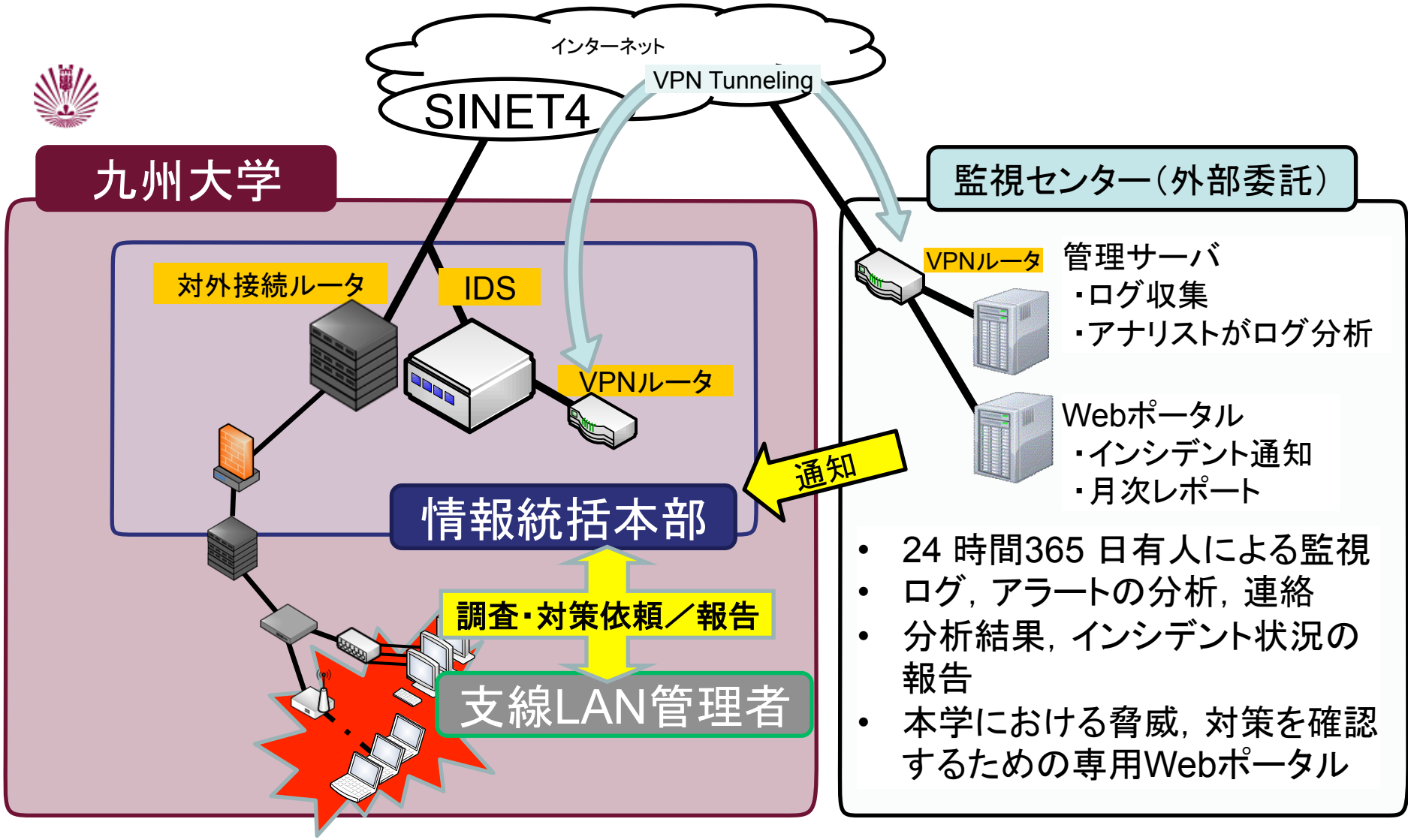
情報インシデント対策に関する情報提供

脆弱性の注意喚起，対策の情報提供

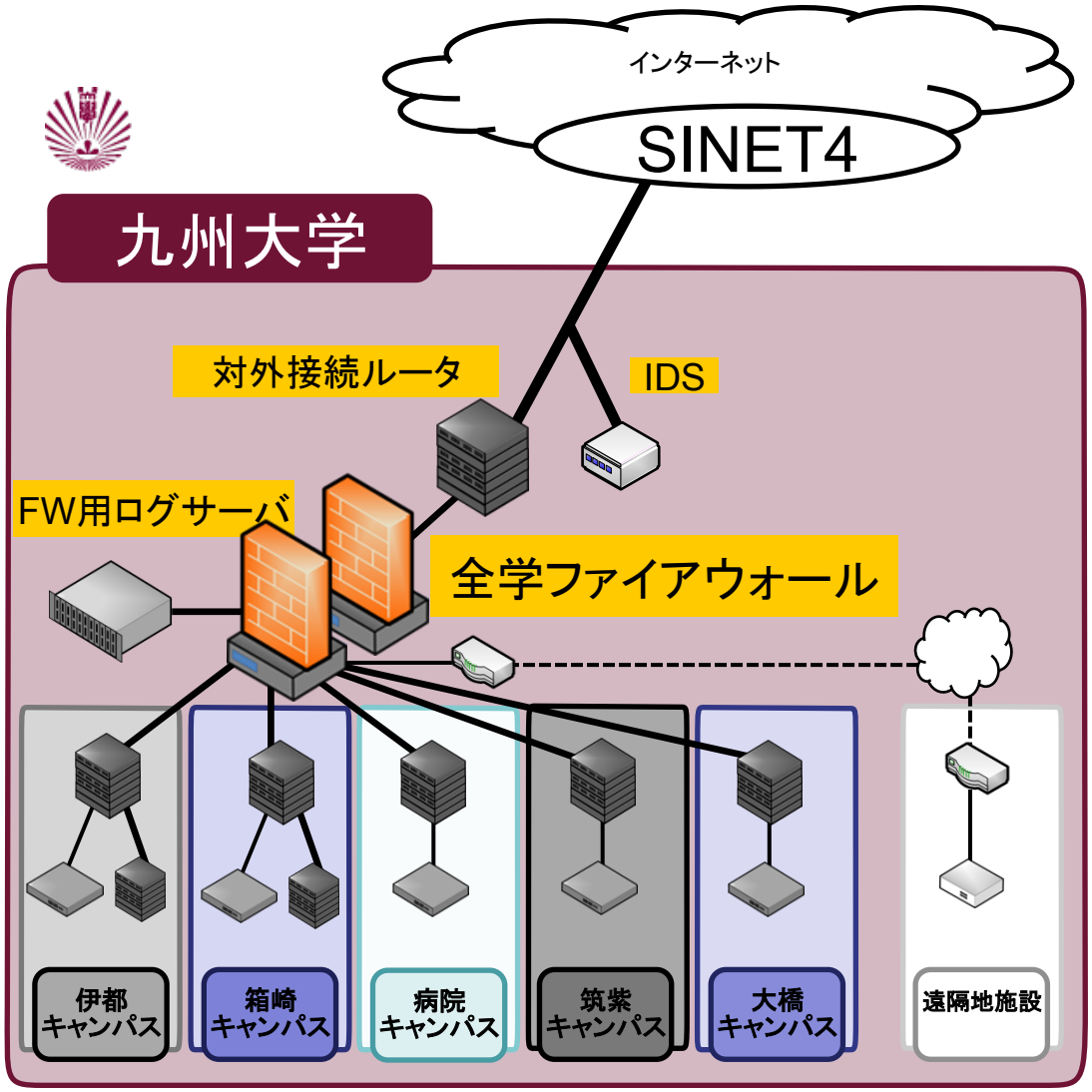
KYUSHU UNIVERSITY

侵入検知システム（IDS）

ウイルス感染，脆弱性への外部からの攻撃等の検知

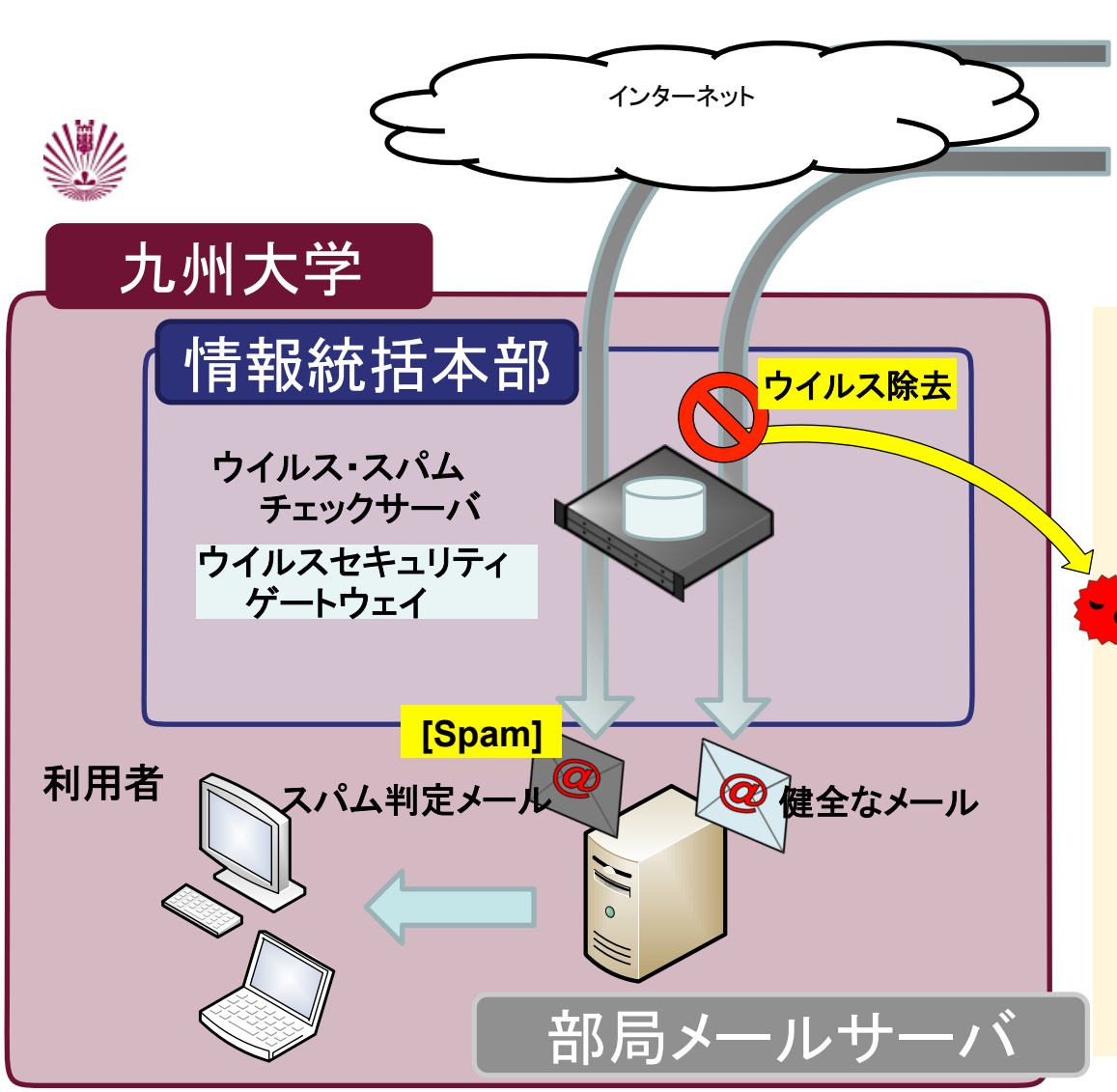


KYUSHU UNIVERSITY 全学ファイアウォールシステム



- URLフィルタリング，脆弱性防御機能
- アンチウィルス，アンチスパム
- ファイル交換ソフトの通信を遮断
- 特定カテゴリのウェブサイトのアクセスを規制
- 学外から学内への動画・音楽ファイルのダウンロードを規制
- DoS攻撃プロテクション
- 学外から学内へのhttp/https通信を規制
- 学外から学内へのntp通信を規制
- VPN通信を規制
- アクティブ/スタンバイ構成（冗長化）

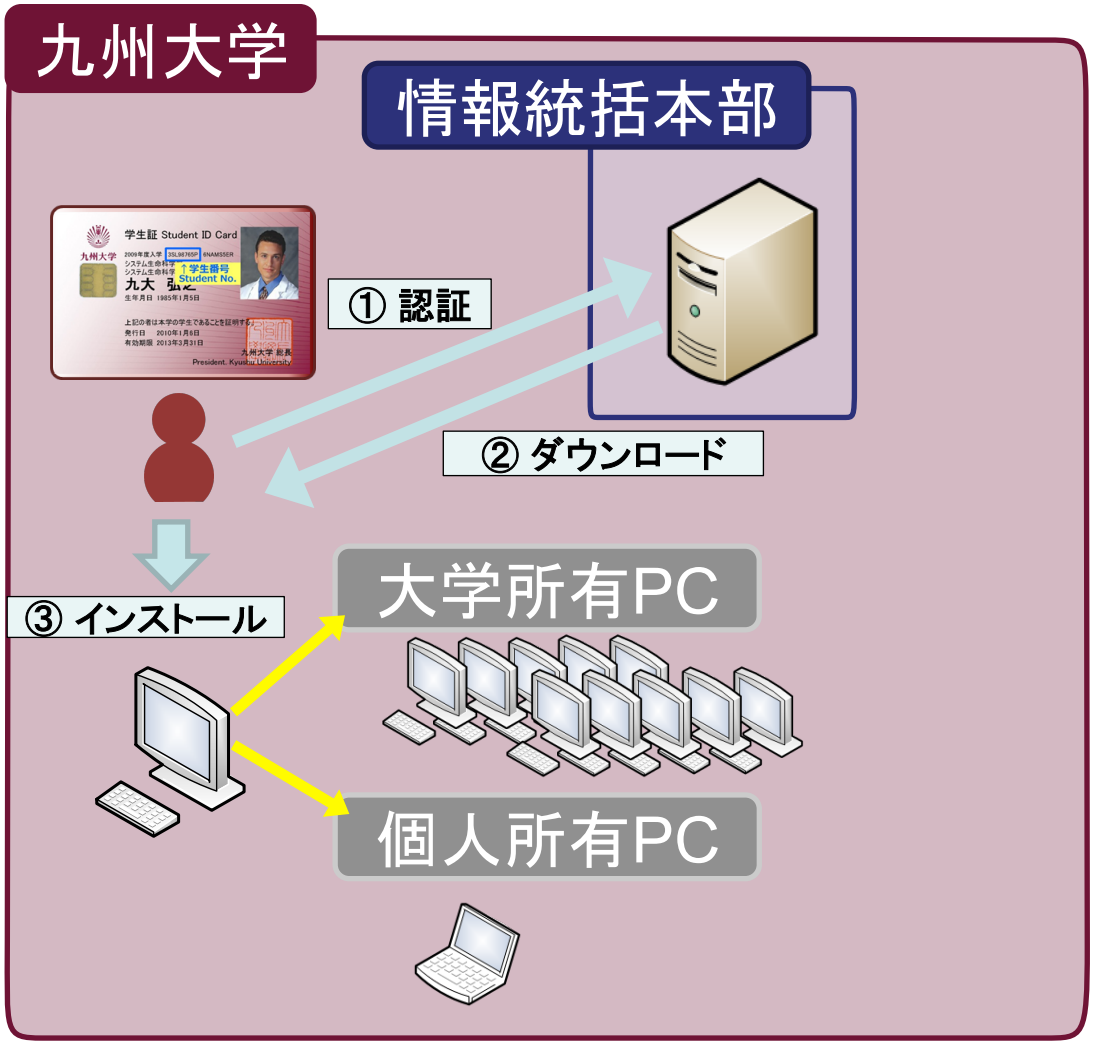
KYUSHU UNIVERSITY ウイルス・スパムメールチェックサービス



◆ スパムメールと判定した場合，以下の処理を行った後，メールを配送
- ヘッダ部に「X-Spam-check-kite: Spam」を挿入
- タイトル（Subject）の先頭に「[Spam]」を挿入

◆ ウイルスを検出した場合、受信者にのみ警告メールを送信
（メールアドレスは詐称されている場合が多く，その場合，送信者への警告メールは，スパムメールになる恐れがあるため，受信者にのみ送信）

ウイルス対策ソフト提供サービス



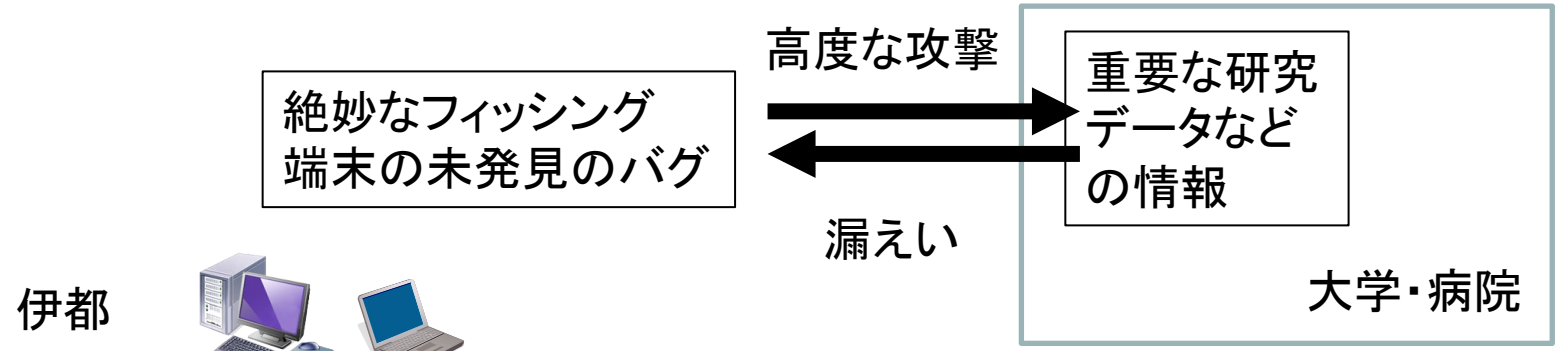
- 大学所有PCへのインストール
  - 台数無制限でインストール可能
  - 全学共通ID（SSO-KID）を持つ教職員に限りインストール可能
- 個人所有PCへのインストール
  - 1人に対し1台までインストール可能
  - 教職員，学生，名誉教授がインストール可能
- ダウンロード時に全学共通ID(SSO-KID，学生ID)で認証

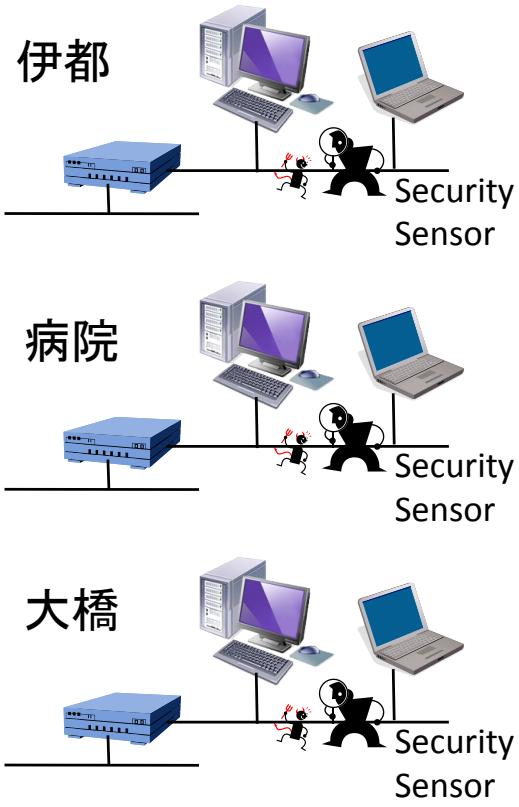
KYUSHU UNIVERSITY 情報インシデント対策に関する情報提供

http://www.sec.kyushu-u.ac.jp

- 脆弱性の注意喚起
  - マイクロソフトワードの脆弱性について
  - IE の未修正の脆弱性について
  - Adobe Flash Playerの脆弱性について
  - EmEditorの更新機能を悪用したウイルス感染に関する注意喚起
  - GNU bashの脆弱性に関する注意喚起
  - Kerberos KDC の脆弱性に関する注意喚起
- 対策の情報提供
  - 九州大学の不特定多数の者に送信されていると思われるメールに対する注意喚起について
  - OpenSSLにおける修正版ソフトウェアの公開について
  - Java実行環境における修正版ソフトウェアの公開について
- マニュアル，印刷物の配布
  - 情報漏洩対策マニュアル
  - 情報セキュリティ安全対策 あなたの情報はねらわれている（個人マニュアル）

セキュリティ対策の課題：標的型攻撃への対応





- 標的型攻撃は、数年前からアメリカでの被害が始まり、現在では日本の主要な企業の被害も出始めている。
  - 年金機構もその一例
- 日本国内の大学にも被害が出ることは自明
- アンチウイルスなどと違い、対処できるシステムは存在しない

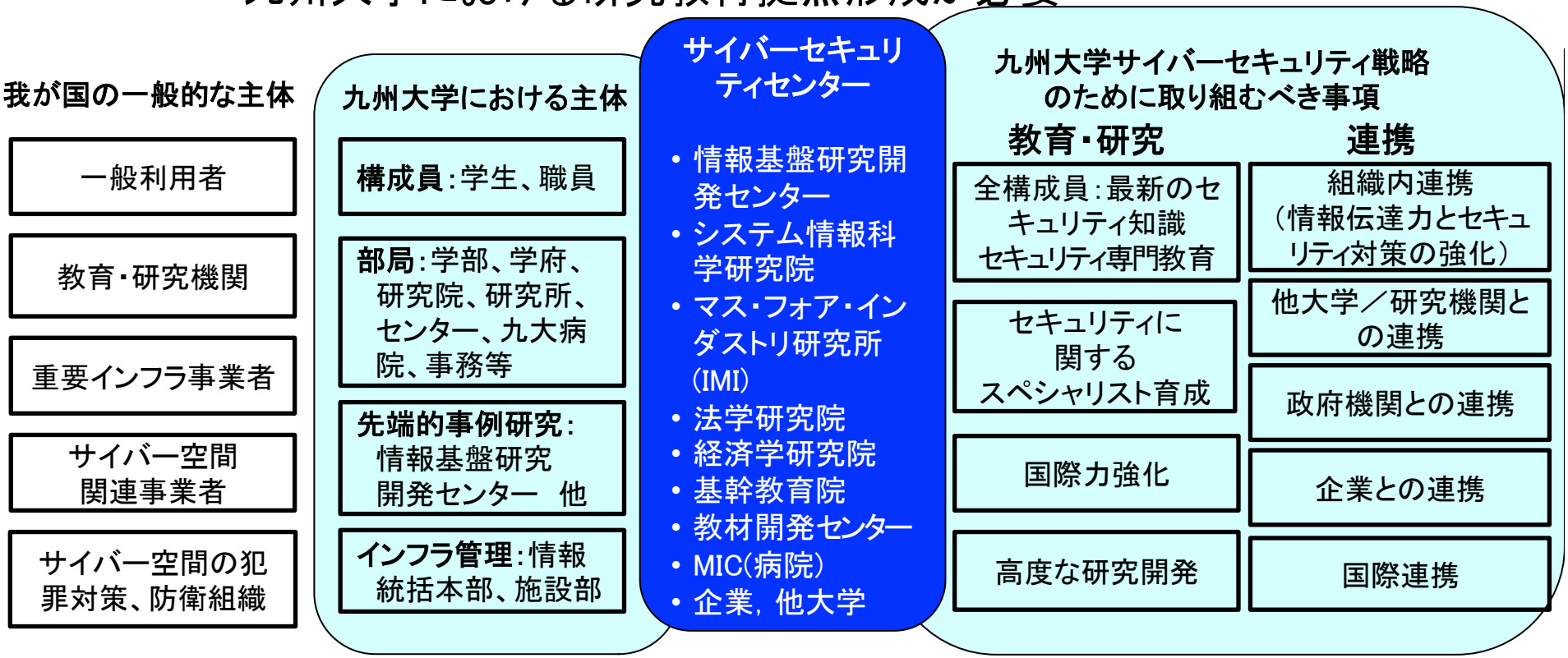
- 全学・全支線にセキュリティセンサーを設置
- リアルタイム処理
- 外部との連携、情報収集が必須
  - 企業、国内外研究機関との共同研究
  - 基礎研究　＋　運用能力 が必要
  - 戦略的セキュリティ対策研究
- 構成員（学生、教職員）の基本的なスキル向上

KYUSHU UNIVERSITY

サイバーセキュリティセンターの構成

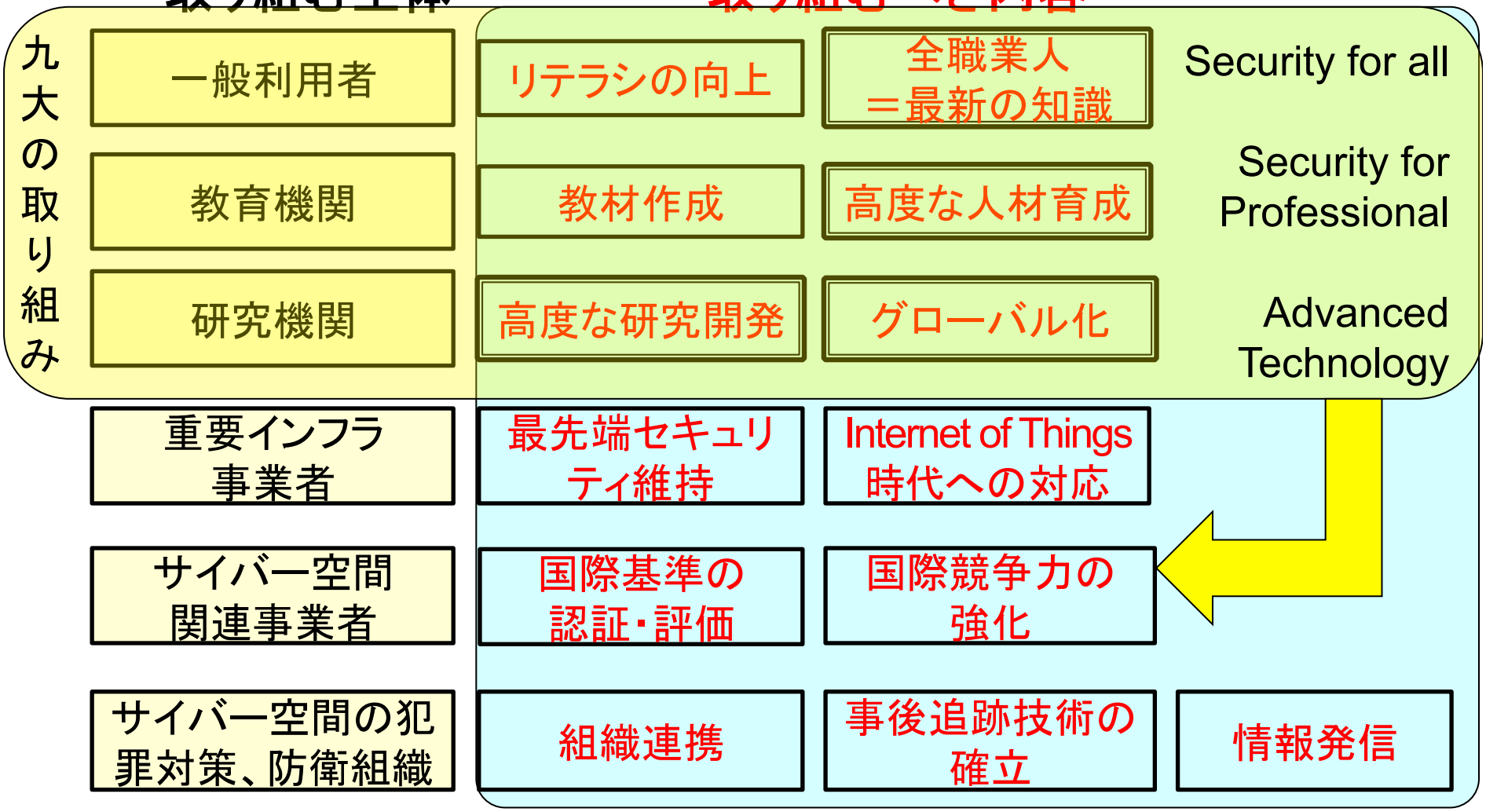
情報科学＋数学＋社会科学＋病院＋基幹教育院の連携

- 九州大学は世界最先端の大学を目指す
  - それにふさわしい安全なサイバー空間の実現が必要
- 世界的セキュリティ研究教育展開のための国際的大学間連携進行
  - 九州大学における研究教育拠点形成が必要



KYUSHU UNIVERSITY 九州大学サイバーセキュリティセンター

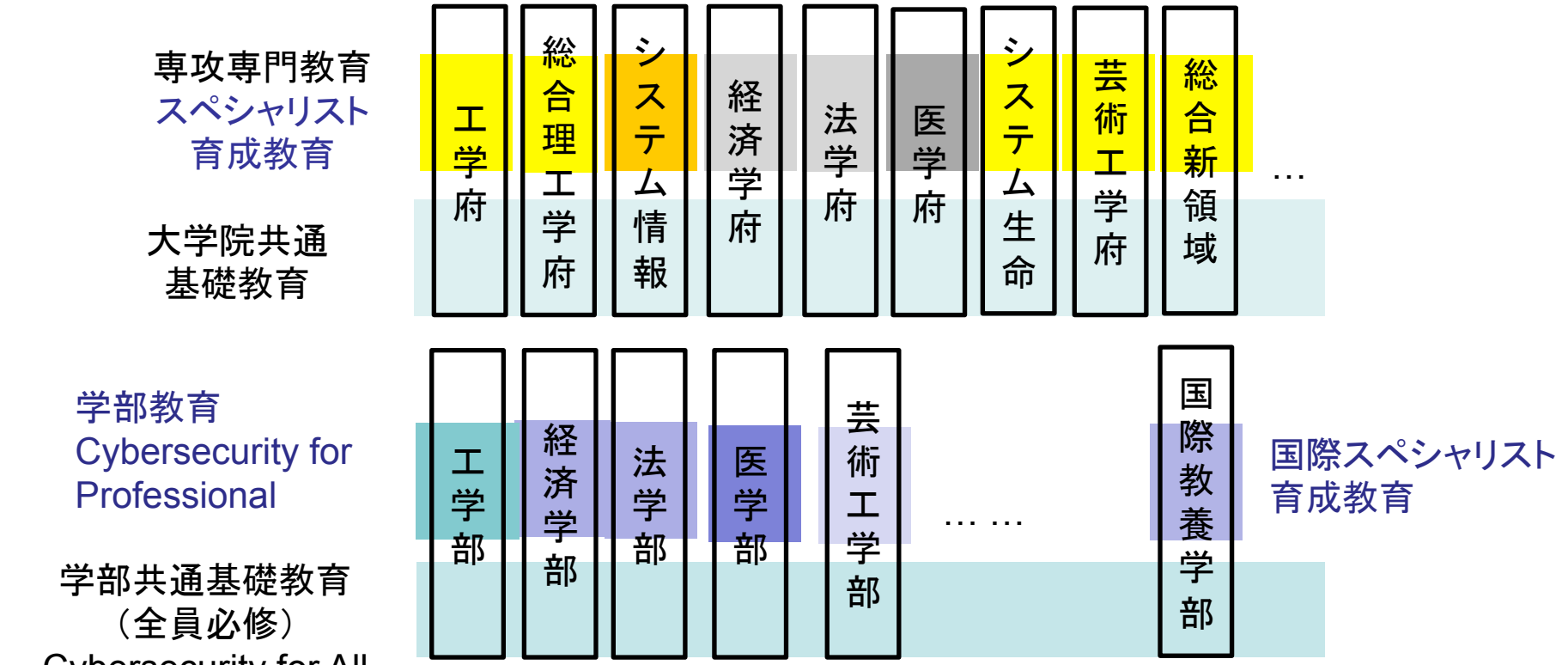
H26年12月1日設置



米国メリーランド大学(UMBC)との連携

KYUSHU UNIVERSITY

サイバーセキュリティ総合教育



- シラバス
- 教育レベルの選択
- 教材

サイバーセキュリティに関する専門知識
教育の質の保証（世界標準）
学部・専攻別に必要になる知識の分類
スペシャリスト育成に必要な要件

情報技術レイヤ
横断的レイヤ
社会科学レイヤ
多角的な視野が必要
グローバルレイヤ

世界標準となる学部～大学院
サイバーセキュリティ総合教育プログラムの研究開発

UMBC 連携

KYUSHU UNIVERSITY

教育・研究開発スケジュール

2014年度	2015年度	2016年度	2017年度	2018年度

基礎教育プログラムの開発・基幹教育の実施

- 基礎教育用プログラムの開発
  - 基幹教育での実施
  - 全ての学生が受講できるようカリキュラムの調整
    Cyber Security for All

先端教育プログラムの開発・プロフェッショナル育成

- 先端教育プログラムの開発
  - 様々な専門で必要となるサイバーセキュリティ教育プログラムの開発
  - UMBCとの連携に基づくEducation Share
- 先端プログラムによるプロフェッショナル育成
  - サイバーセキュリティ演習
  - 企業と共同実施，社会への成果フィードバック

教育研究開発拠点の整備，競争的資金，概算要求

- プロジェクト申請（大型科研費，CREST，SCOPE他）
- 企業等との共同研究検討
  →複数企業参画による共同研究部門（COOPプログラム）

先端／連携研究の推進

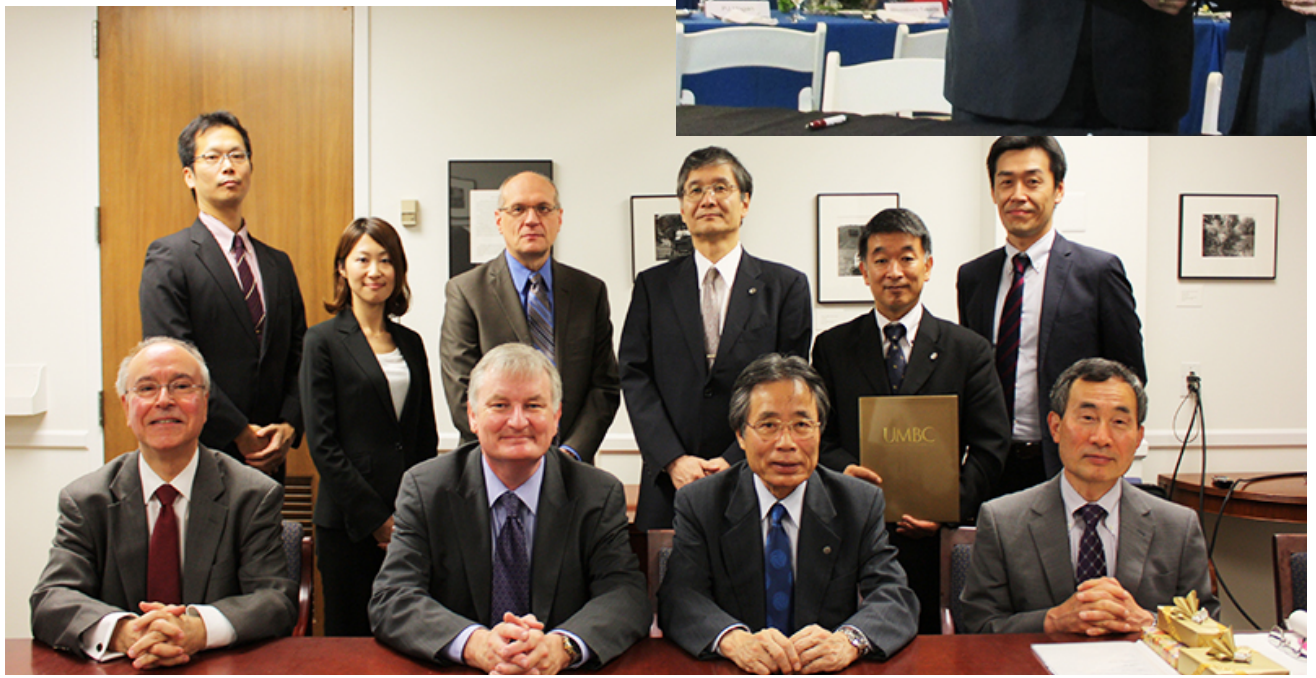
- サイバービッグデータから未知の脅威を発見する技術の開発
- サイバーセキュリティにまつわる法制度や社会現象の研究
- プライバシー保護，サイバー犯罪抑止技術の開発

センター組織の拡充

- 情報基盤研究開発センター，システム情報科学研究院，その他サイバーセキュリティに関連する部局等で全学的に，拡充計画を検討し，実施

UMBCとの連携

2014年7月
メリーランド大学
ボルチモアカウンティ校
との連携協定



2015年1月
合同シンポジウム

今後

何を守るか

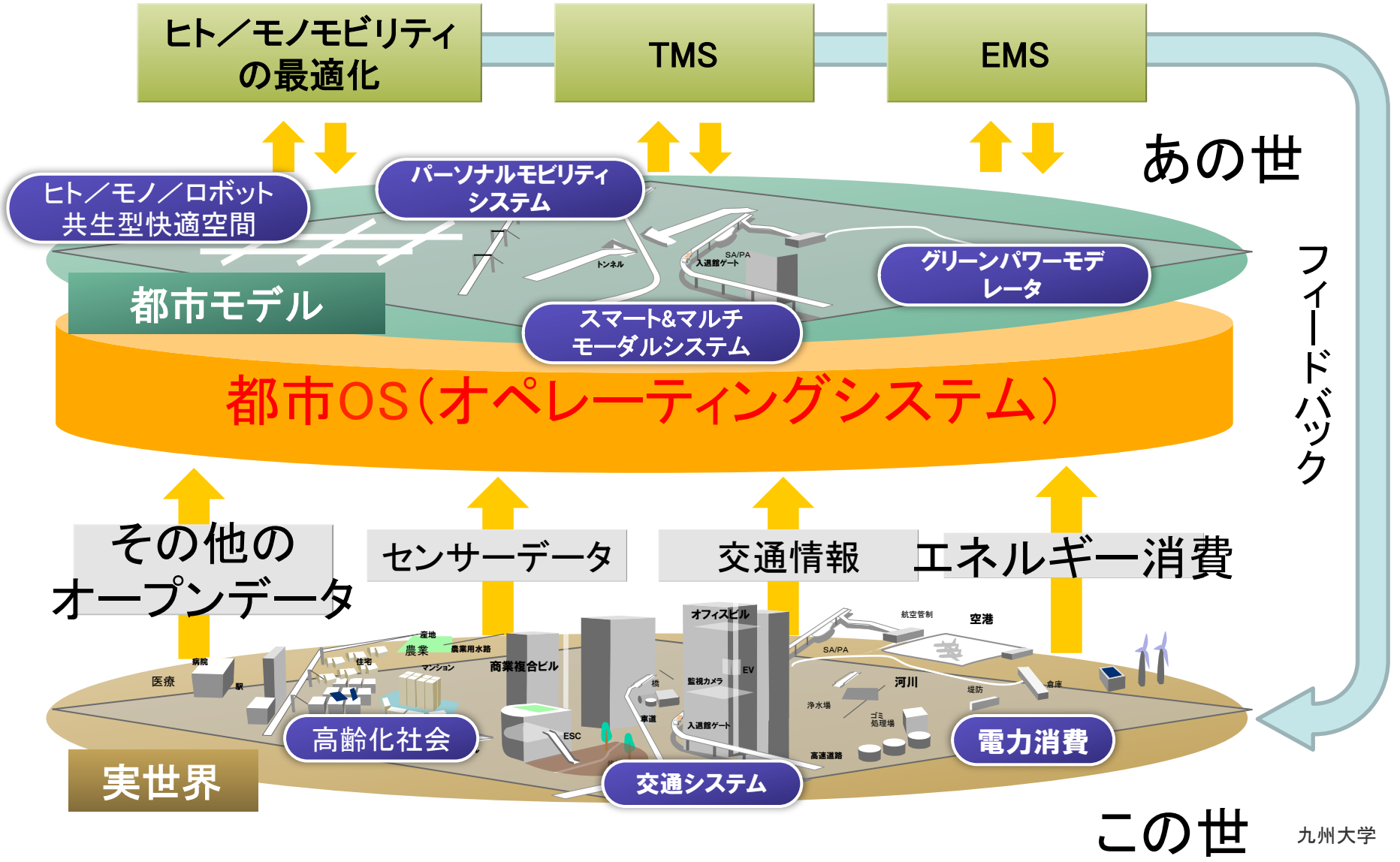
* 個人や組織の名誉や信頼と生命の安全
  – 被害者にも加害者にもならない
* 個人や組織の財産
  – 情報は重要な財産（個人情報、情報化資産）
* 社会の秩序と安定
  – 社会情報基盤の混乱は社会の混乱に直結
* 社会や国家の存立基盤
  – 行政、外交、治安維持、防衛など

サイバーセキュリティの難しさ

- 情報はコピーが容易で直接見えない
  - 盗まれても気づかない
  - 盗まれた痕跡が残りにくい
- 情報は改ざんが容易
  - 情報の改ざんが、生命、財産、プライバシーに影響
- 命かプライバシーか？
  - 相反する社会的な要求
- 個人のリテラシーの不足
  - 「おれおれ詐欺」の高度化
  - 被害者が加害者にもなる
- 社会のあらゆる場面で情報化が進む
  - IoT(Internet of Things)やCPS(Cyber Physical System)

超サイバー社会ーあの世とこの世ー

IoT(Internet of Things)とCPS（Cyber Physical System)



次の社会変革は？

Data税

- 税の基本は、最も重要なものに課税する
  - データの蓄積、データの移動、データの加工
  - セキュリティの徹底的な保障ー＞新しい国富の源
- Data税の活用による国際的な産業集積
- そのためには「安全性」の保障が必要

個人情報の管理 （情報Bank）

- マイナンバー制度とプライバシー保護
- 個人情報および保有する権利や価値の管理•運用
- 高齢者の個人情報の管理と資産管理の連携

人間の反応時間と整合した社会制度•法体系

- プログラム取引は妥当か？
- 人間が関与する時間の確保は必要か？
- 新しい技術による社会変化へ対応した法整備

→安全で安心なサイバー空間の構築は都市や国の基盤

世界のデータが集まる都市へ

- 世界のデータが集まる安全な都市の構築：３つの脅威からの安全保障
  - 自然災害からのセキュリティ
  - 戦争やテロからのセキュリティ
  - サイバーセキュリティ
- データ税が課税できるだけの安全性を保障する都市
  - データの蓄積への課税
  - データの移動への課税
  - データの処理への課税
- 世界のデータの集積拠点＝世界のビジネスセンター

サイバーセキュリティの研究

暗号：Cryptography
- 公開暗号系：Public key system (RSA, Elliptic Curve etc.)
- 設計と解析の技術
- 標準化と利用技術

安全な情報システム：Secure Information System
- 攻撃からの防御法 (Fire walls, Network 構造)

通信の安全性：Security in Communication
- 安全な通信プロトコル：Secure Protocols
- 量子通信

ソフトウェアの安全性：Security for Software
- ウィルスやワームの検出／無力化

ハードウェアの安全性：Security for Hardware
- 分解攻撃からの防御（Anti-tampering）
- 外部攻撃からの防御(Protection from Side Channel Attack)

幅広い分野の協力

- 大学や研究機関：Academic Sectors
- 政府や自治体：Governments
- 企業やビジネス界：Business and Industrial Sectors
- インフラ事業者：Social Infrastructure Operators
- 法律家：Lawyers
- 公安や警察：Public Security Sectors
- 教育界：Educational Sectors
- 国際機関：International Organizations
- 防衛機関：Military

安全・安心なサイバー空間

- 安全なサイバー空間の維持は、行政や企業、さらには国家など現代組織の基本的使命であり、社会の安定に直結する。

- サイバー空間の安全性は、自由や民主主義の維持とも関係する。セキュリティとプライバシーのバランスについて社会的なコンセンサス形成が必要である。

- サイバー空間を含む社会の安全は、個人一人一人の倫理観と責任において担保される。新しい哲学と倫理、そしてその教育が求められている。

ご清聴ありがとうございました。

http://www.kyushu-u.ac.jp