韓国におけるサイバー攻撃対応

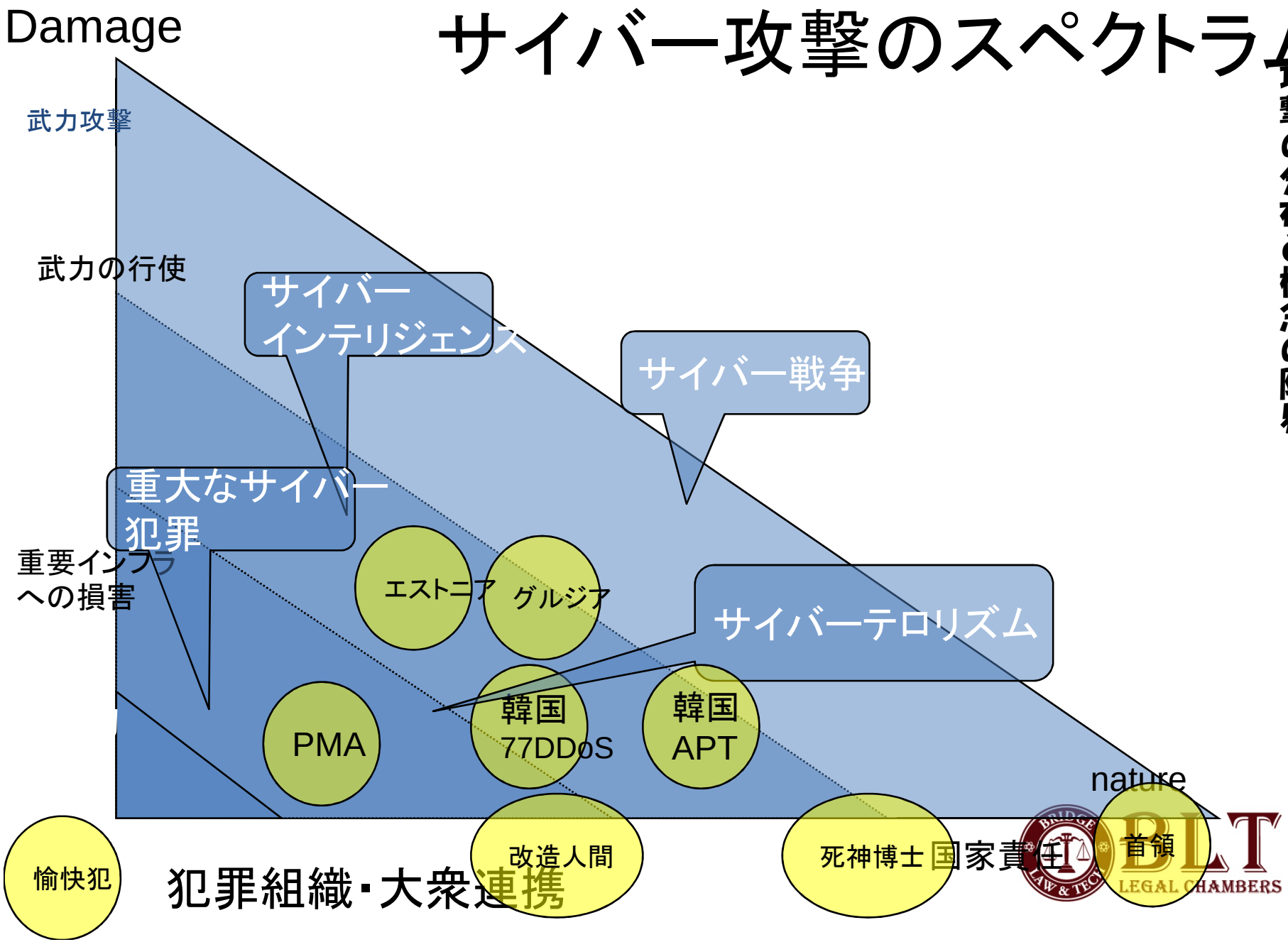
高橋郁夫
弁護士-BLT法律事務所

国際的ケーススタディ

- 総務省「情報システムにおけるセキュリティインシデントに関する調査研究の請負」応募
- チーム構成
  - 佐々木良一先生、高倉弘喜先生、島田秋雄さん、Eli Jellencさん
- 制度変革の概要のみのフォローに終わってしまう懸念
  - 例「情報共有が大事です」
    - どうすれば、共有できるのですか？という問題設定に
    - まずは、見学にいってみよう。

BLT LEGAL CHAMBERS

サイバー攻撃のスペクトラム



攻撃の分布と概念の限界

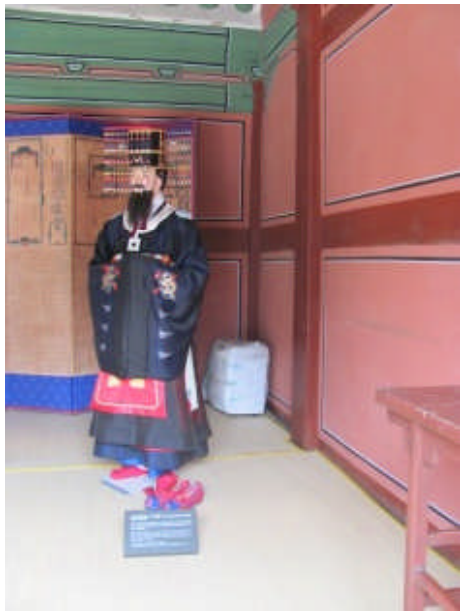
BLT
LEGAL CHAMBERS

APTを仮面ライダーで分析してみる

- 首領率いるショッカーのリソースを用いれば、一見、非効率にみえる攻撃でも、実は効率的であったりする
- 日本支部長も、いろいろな作戦を考えて、長期的な視点で日本征服を考えるだろう
- これらの動きから考えるとき、改造人間をつくるよりも、サイバーのほうが効率的であれば、日本支部長は、APTをしていたかもしれない
- ショッカーの壊滅のためには、ライダーを中心に協力体制を整える必要
- サイバーの新しい手法ではなく、攻撃(もしくは諜報)の最新手法ととらえるほうが解決策を見つけやすいだろう

BRIDGE LAW & TECH BLT LEGAL CHAMBERS

ソウル訪問



BRIDGE LAW & TECH BLT LEGAL CHAMBERS

1 韓国におけるDDoS対応

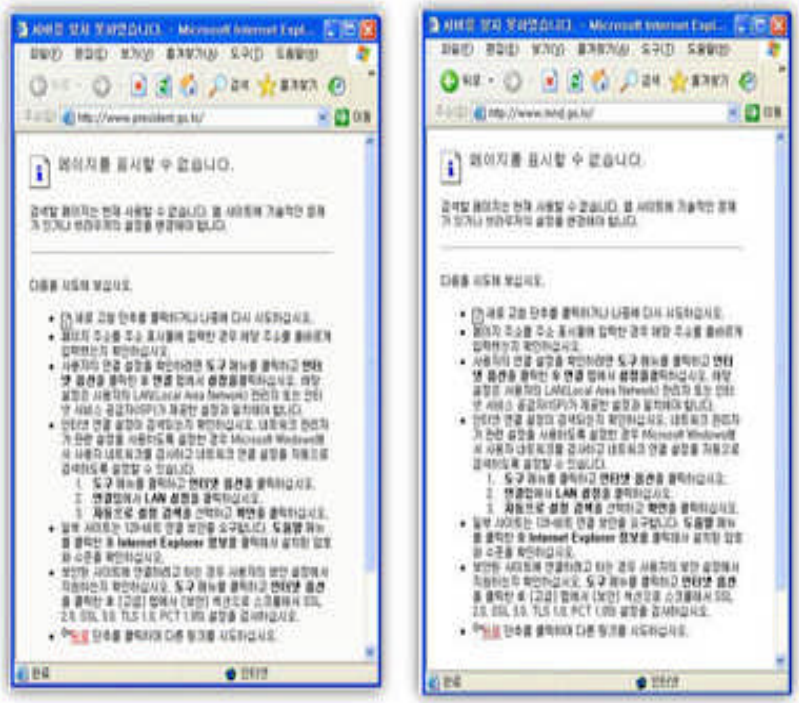
77DDoSから34DDosに

BRIDGE LAW & TECH BLT LEGAL CHAMBERS

2009年韓国攻撃

- 7月5日ころ
  - 米国のホワイトハウス（whitehouse.gov）、www.faa.gov、faa.gov、evisaforms.state.govなどに対して攻撃
- 7月7日
  - 韓国の青瓦台（大統領官邸）、政党、銀行、その他主要なポータルサイト

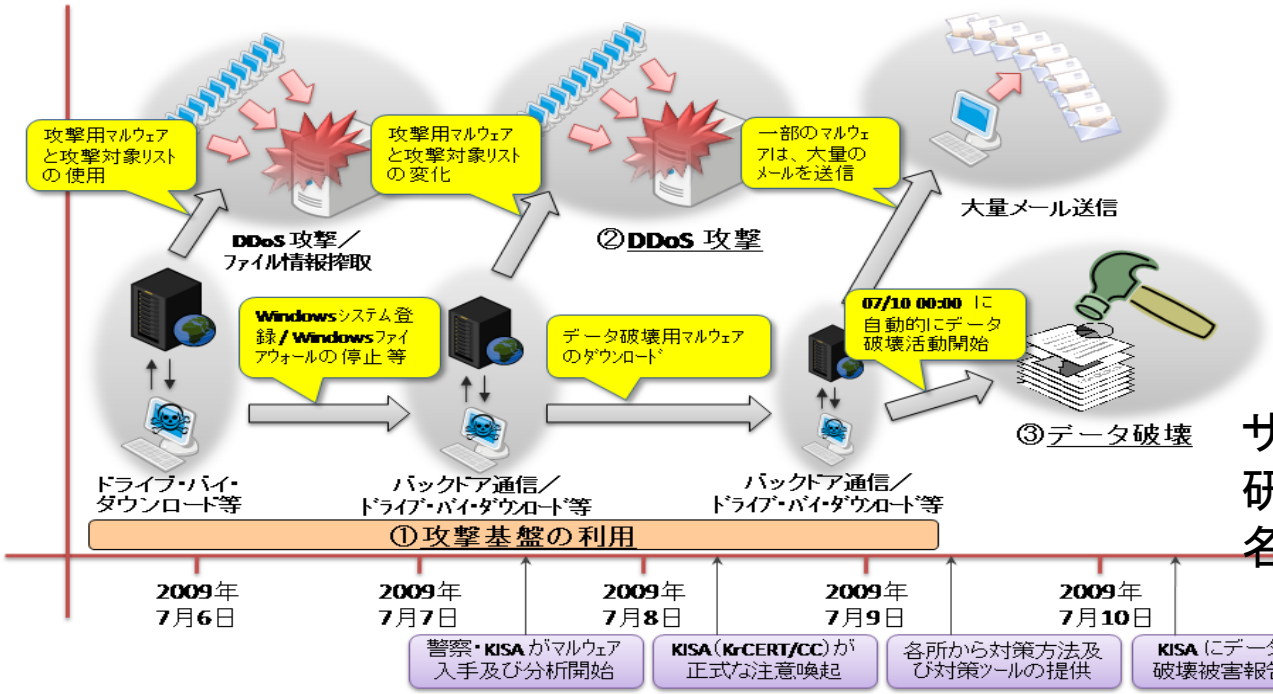
閲覧できなくなった大統領府と国防部のサイト



攻撃の詳細

- DDoS攻撃、スパムメール、自己破壊プログラムの実行-三波の攻撃
- 伝統的な C&C サーバを利用するものではない
- 前の段階
  - マルウエアが、海賊版ソフトウエアを配布するサイトなどから、ダウンロードされていた。
- 攻撃の時間が到達するとともに、このマルウエアが実行

- 各PCのウインドウズファイアウォールを停止
- 攻撃対象リストが生成
- 生成されたリストに従って、感染PCが、一斉に攻撃を開始
- 大統領府・国防部のサイトなどが閲覧不能
- システム情報とファイルリスト情報等を窃取



サイバーディフェンス研究所
名和さんの資料より

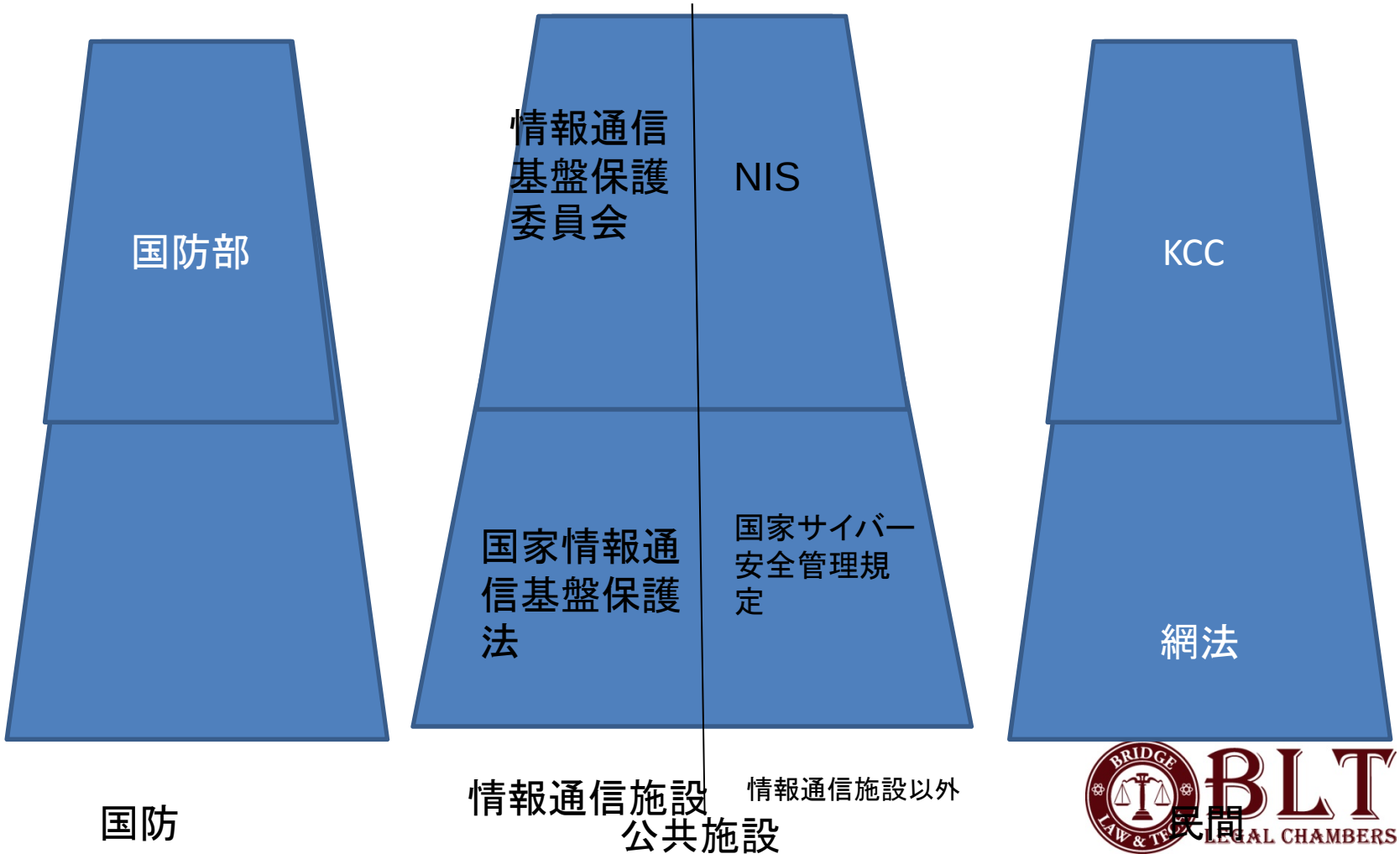
BLT LEGAL CHAMBERS

反省点

- (1) 情報保護ポリシー機能の分散による中央統制機関の不在
- (2) サイバー攻撃の知能化・組織化
- (3) サイバー攻撃に対する訓練および国際協調の不足
- (4) インターネット利用増加に伴う情報保護対象の急増
- (5) マルウェア分析のための装備・専門人材の不足
- (6) サイバー脅威に対するインターネットユーザーのリテラシーの不足
  - 韓国国会立法調査署 作成「『7.7DDoS事故』対応の問題点と再発防止法案」レポート

BRIDGE LAW & TECH BLT LEGAL CHAMBERS

「7.7大乱」発生当時の
サイバー危機対応体制

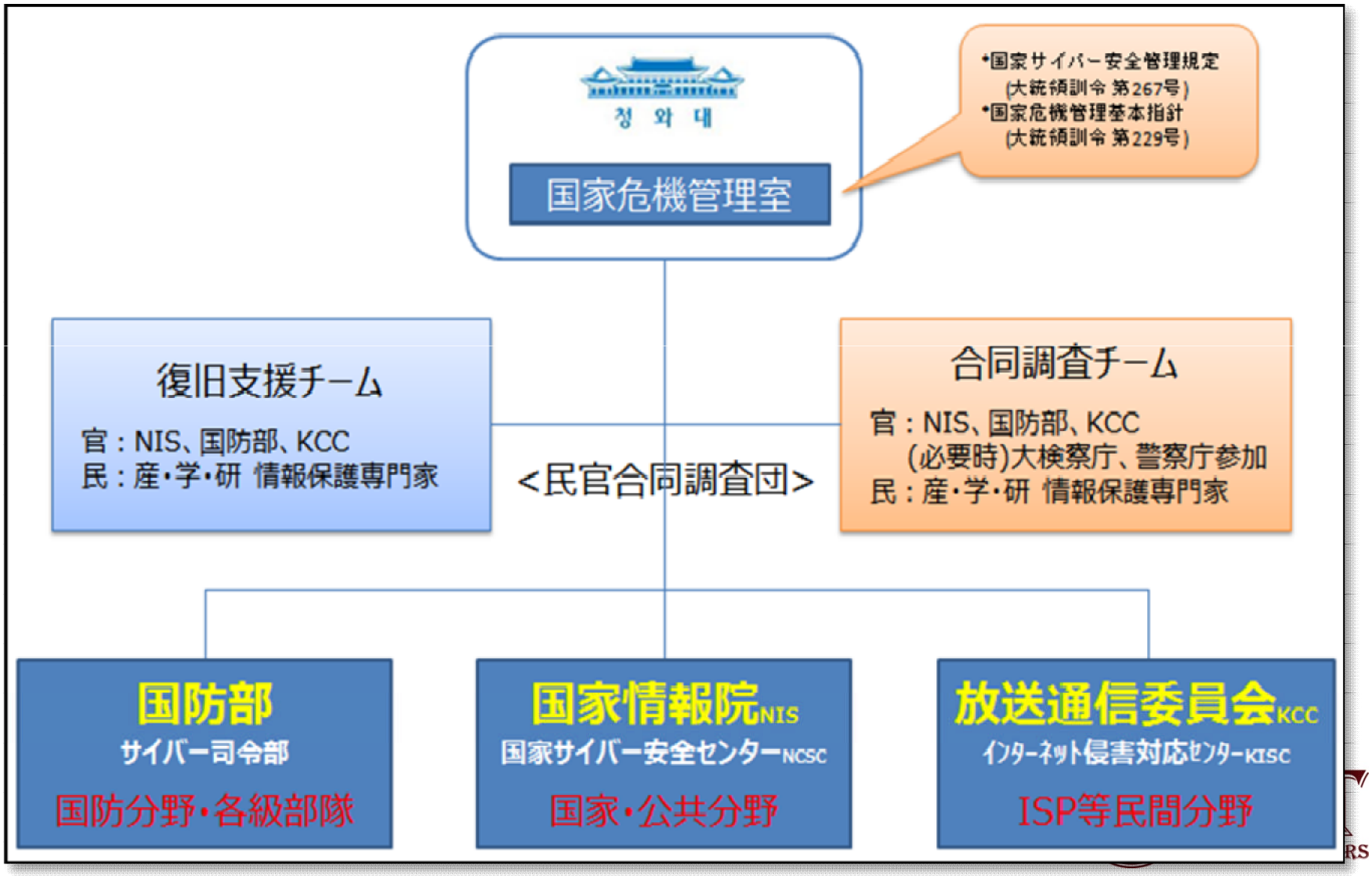


2009年8月以降の効果的な政策

- 予算の増加
- 「コントロールタワーの構築」
- 「サイバー駆除体系の整備」
- 「DDoSサイバー避難所」

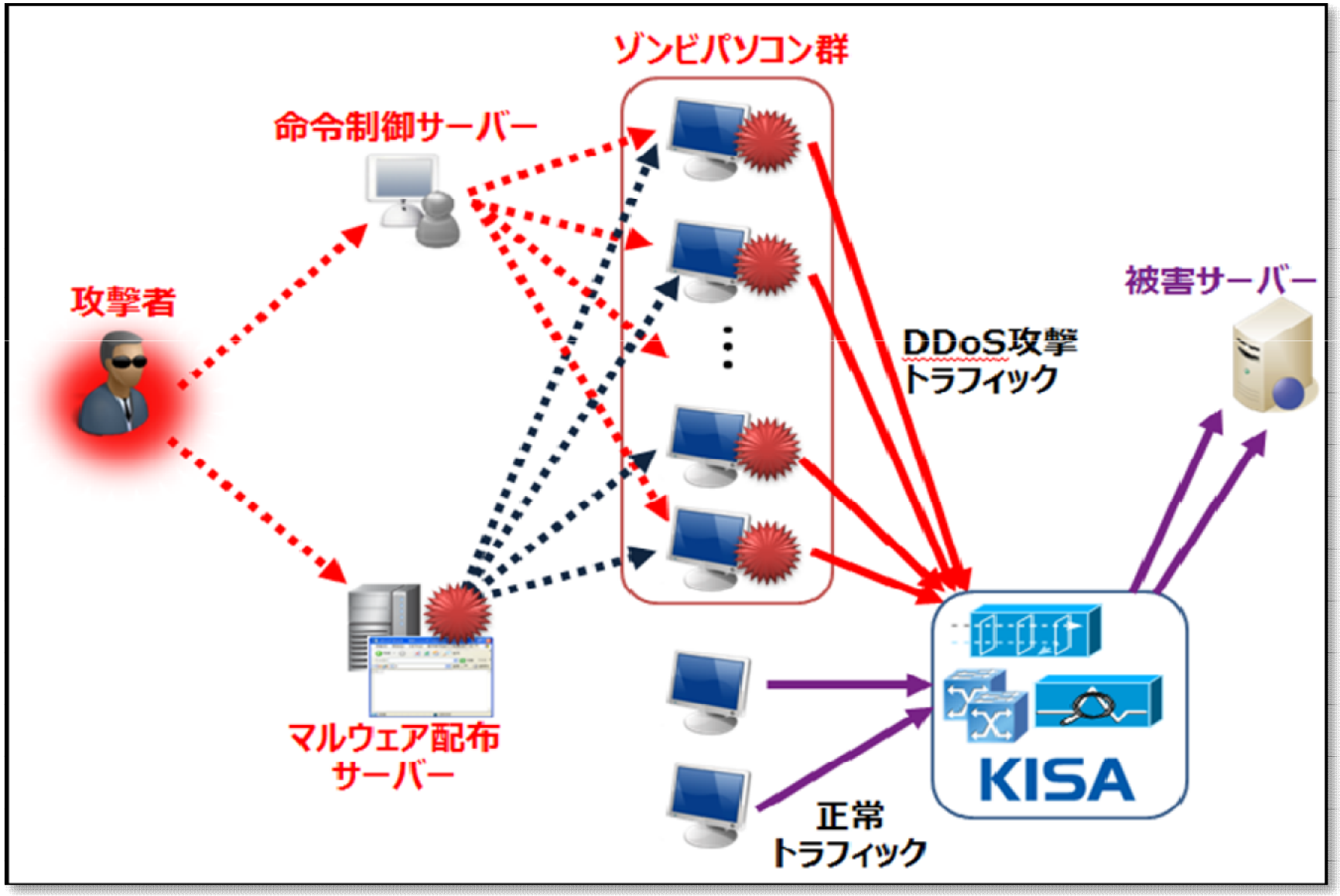
BRIDGE LAW & TECH BLT LEGAL CHAMBERS

コントロールタワー


청 와 대
国家危機管理室
•国家サイバー安全管理規定
(大統領訓令 第267号)
•国家危機管理基本指針
(大統領訓令 第229号)
復旧支援チーム
官：NIS、国防部、KCC
民：産・学・研 情報保護専門家
<民官合同調査団>
合同調査チーム
官：NIS、国防部、KCC
(必要時)大検察庁、警察庁参加
民：産・学・研 情報保護専門家
国防部
サイバー司令部
国防分野・各級部隊
国家情報院NIS
国家サイバー安全センターNCSC
国家・公共分野
放送通信委員会KCC
インターネット侵害対応センターKISC
ISP等民間分野

「感染パソコンサイバー駆除体系」

「D-DOSサイバー待避所」



「マルウェア拡散防止等に関する法律案」(ゾンビパソコン防止法)

- 2011年4月18日、韓国国会に上程
- 反対が強く、まだ、国会を通過していない
  - (1)サイバーテロ発生時-サーバーのドメインやIPアドレス、クライアントコンピュータのIPアドレスの遮断も可能
  - (2)感染マルウェアを強制駆除/削除 (セキュリティソフトウェアのインストール命令)
  - (3)セキュリティソフトウェアに欠陥がある場合、そのソフトウェアの販売を禁止できる
  - (4)マルウェアを含む掲示物の強制削除

BRIDGE LAW & TECH BLT LEGAL CHAMBERS

3.4 DDoS攻撃

- 韓国で2011年3月4日10時および18時30分の2度にわたり、韓国の主要な政府機関および韓国内の各国サイト40サイトに対しDDoS攻撃が試みられた事件
- サイバー駆除体系などが有効に働いて被害を最小限に押さえることに成功した
- 詳しくは、NC-18「同時多発的DDoS攻撃への対応と即応態勢の整備」に

BRIDGE LAW & TECH BLT LEGAL CHAMBERS

評価

- 「3.4 DDoS攻撃」
  - 「7.7大乱」との比較-多くの面で進化
    - マルウェアの難読化、配布手法の巧妙さ、攻撃対象・時間の変化、ハードディスクの即時破壊命令など
- 「3.4 DDoS攻撃」-被害を最小化-スピーディな対応
  - 「国家サイバー危機総合対策」、「コントロールタワーの整備」、「感染パソコンサイバー駆除体系」
  - ゾンビパソコン対策に集中的にリソースを投下

BRIDGE LAW & TECH BLT LEGAL CHAMBERS

2 韓国におけるAPT攻撃とその対応

BRIDGE LAW & TECH
BLT
LEGAL CHAMBERS

農協に対するAPT攻撃

- 2011年4月12日16:50ごろ
- 韓国農協の電算ネットワークのデータが大量に破壊され、数日にわたって(4月30日に取引が完全復旧)サービス利用ができなくなった事件
  - 農協の電算ネットワークをメンテナンスする外部委託業者(韓国IBM) の社員がウェブハードサイト利用中マルウェアに感染
  - キーロガーを仕込まれバックドアを開けられた
  - 電算ネットワークのデータファイル削除を実行された。

BLT LEGAL CHAMBERS

APT攻撃のインパクト

- きわめて大きい
  - 農協 韓国最大規模の金融機関
  - 緻密に準備された標的型攻撃
  - 農協のバックアップされたデータも同時に削除
  - 一部のデータは復旧不可能
  - サービス復旧まで相当な時間
  - 3,000万名の大規模ユーザーが被害
  - 検察がこの事件を「北朝鮮が関与する前代未聞のサイバーテロ」であると結論づけたこと

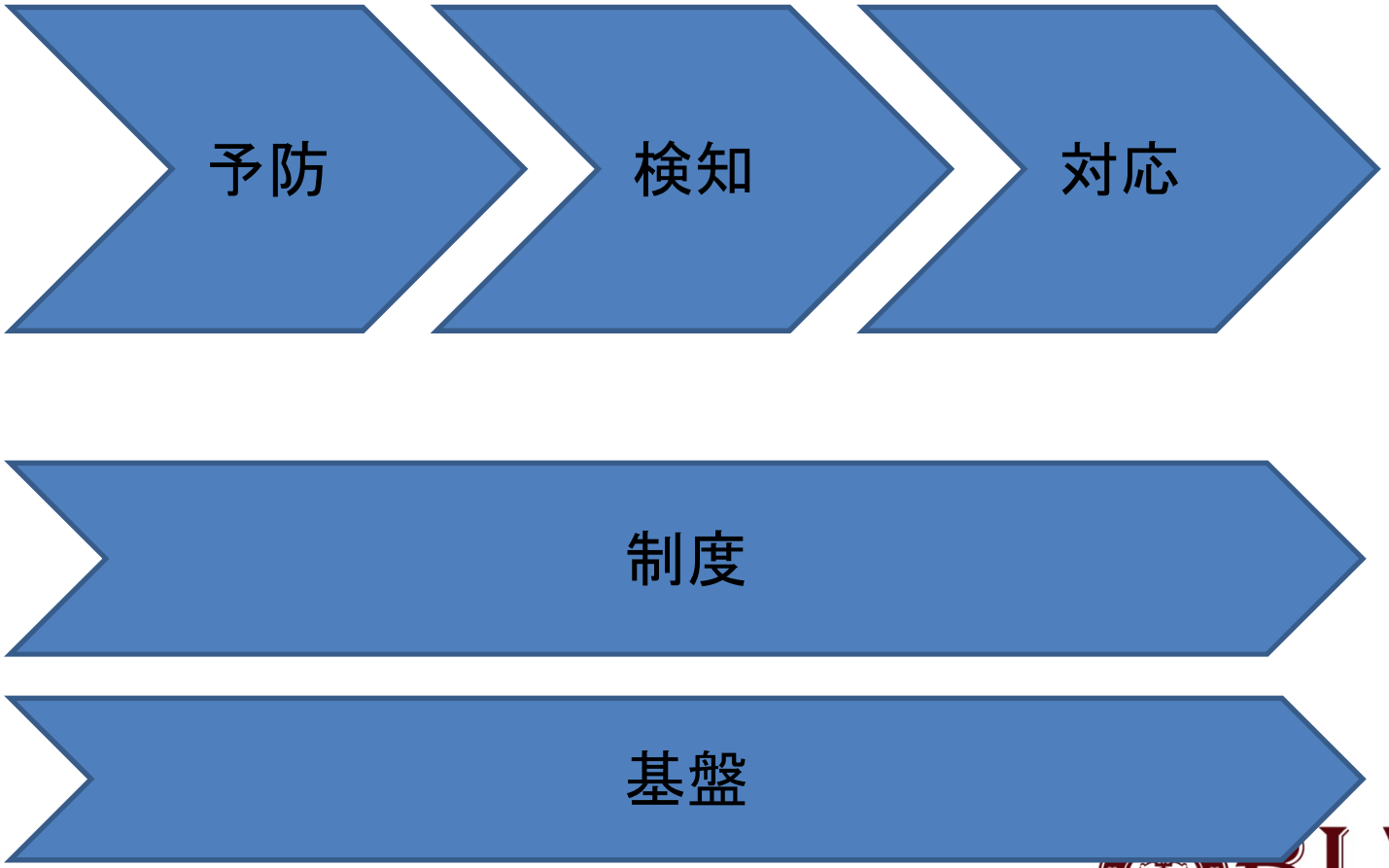
BRIDGE LAW & TECH BLT LEGAL CHAMBERS

国家サイバー安保マスタープラン

- 2011年8月8日「国家サイバー安保マスタープラン」を施行すると発表
  - 「国家サイバー安全実務会議」と外部の専門家の諮問を経て決定した
  - 国務総理室、KCC、国防部、行政安全部、金融委員会、企画財政部、教育科学技術部、外交通商部、統一部、法務部、知識経済部、保健福祉部、国土海洋部、警察庁、NISの15の政府関係部署が参加

BRIDGE LAW & TECH BLT LEGAL CHAMBERS

マスタープランの概要



BLT LEGAL CHAMBERS

予防

- 戦略、金融、医療など基盤システム運営機関と企業の保護措置強化
- 主要システムに対するバックアップセンターと災害復旧システム拡大構築
- 政府ソフトウェア開発段階でのセキュリティ脆弱性の事前診断制度を義務化
- 国際協調強化を通じたサイバー挑発抑止力の確保

BRIDGE LAW & TECH BLT LEGAL CHAMBERS

検知

- サイバー攻撃に対応するための3ライン防御体制の導入（IGW/インターネット連動網↔ISP↔企業/個人）を通じた攻撃トラフィック段階別検知・遮断
- 地方自治体の情報システムサイバー攻撃検知実施
- 保険・カード会社等第2金融機関の電算ネットワークセキュリティ監視拡大
- 北朝鮮初の不法ソフトウェア流通監視・遮断活動の強化
- 金融・通信等民間主要システムに対し、専門ベンダを活用したセキュリティ点検年1回義務化

BRIDGE LAW & TECH BLT LEGAL CHAMBERS

対応

- 民・官合同対応チーム運営で組織的ハッカー攻撃に対応
- 主要国家と国際機構との協力強化を通じて高度化するハッキングに総力対応

BRIDGE LAW & TECH BLT LEGAL CHAMBERS

制度

- 国家・公共機関対象情報セキュリティ評価制度改善、ISMS 認証活性化、金融分野「IT部門評価」対象機関拡大など推進
- 民間企業ハッキングインシデント発生時、経営者の責任、委託業者による発生時民・刑事上の責任を同時に問えるようにする等委託事業および民間分野セキュリティ管理を強化
- 「サイバーセキュリティの日」制定・施行と「クリーンインターネット運動」活性化などを通じた社会全般のサイバーセキュリティに対する意識向上に注力

BRIDGE LAW & TECH BLT LEGAL CHAMBERS

電子金融監督規定

- ５．５．７とは？
  - 人材の5 パーセントがIT 関連の人材
  - 5 パーセントがセキュリティ人材
  - 予算の7 パーセントが、セキュリティ関連
- 2011年11月より施行

BRIDGE LAW & TECH BLT LEGAL CHAMBERS

基盤

- 各政府機関の情報セキュリティ人材増員と金融委員会セキュリティ業務専門組織新設
- KISAの情報セキュリティ正規職比率増加
- 原発など国家インフラ運営機関のセキュリティ専門人材確保を推進
- 情報保護学科増設および契約型修士課程の拡大
- ソフトウェア分離発注の定着
- 韓国内情報保護製品の海外輸出サポートと情報保護開発拡大など関連産業および研究活性化サポート強化

BRIDGE LAW & TECH BLT LEGAL CHAMBERS

韓国対応からの示唆

- 国際的なケーススタディの重要性
- 国家や制度の役割の重要性
- 技術のみでの対応の限界
  - APT攻撃をあらたな「手法」と考えているのでは限界がある
- 早期検知・早期対応の重要性

BRIDGE LAW & TECH BLT LEGAL CHAMBERS

一般論として

- サイバー攻撃についての属性・被害からの分析が重要
- サイバーインテリジェンスとしての位置づけ
  - 法と政策の重要課題としての位置づけ
- 情報共有体制の詳細な検討
  - 使われないことを前提としない
  - 情報のクラス分けと分析組織の重要性
  - インセンティブ設計

BRIDGE LAW & TECH BLT LEGAL CHAMBERS