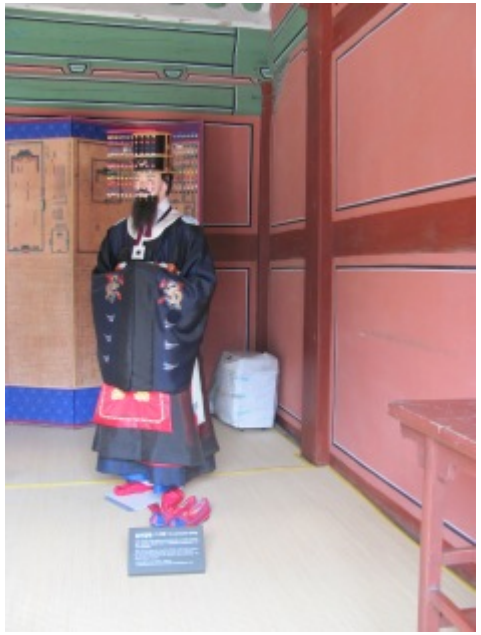
韓国における情報セキュリティのケーススタディ

弁護士 高橋郁夫

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。

ソウル訪問

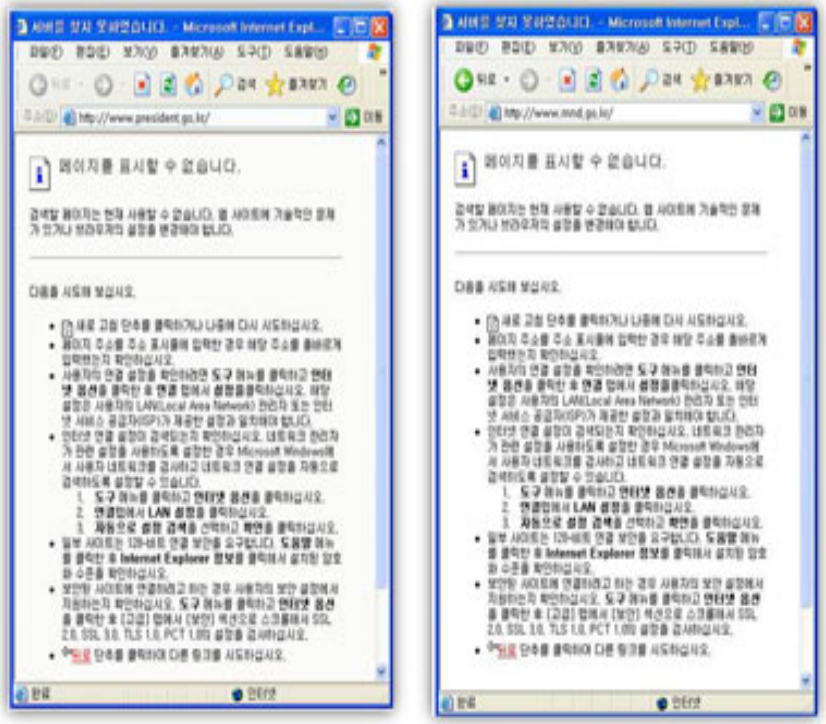


1　2009年7月7日 DDoS

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

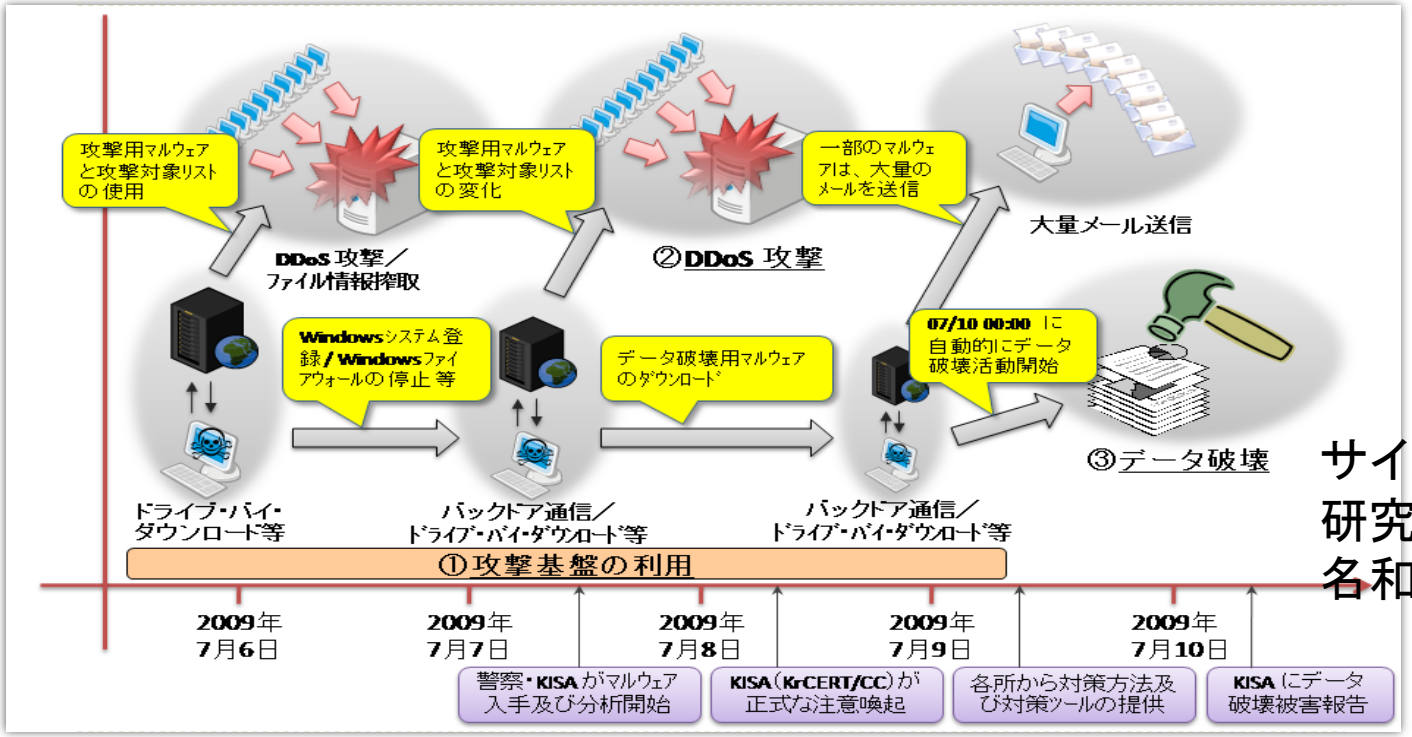
閲覧できなくなった大統領府と国防部のサイト



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

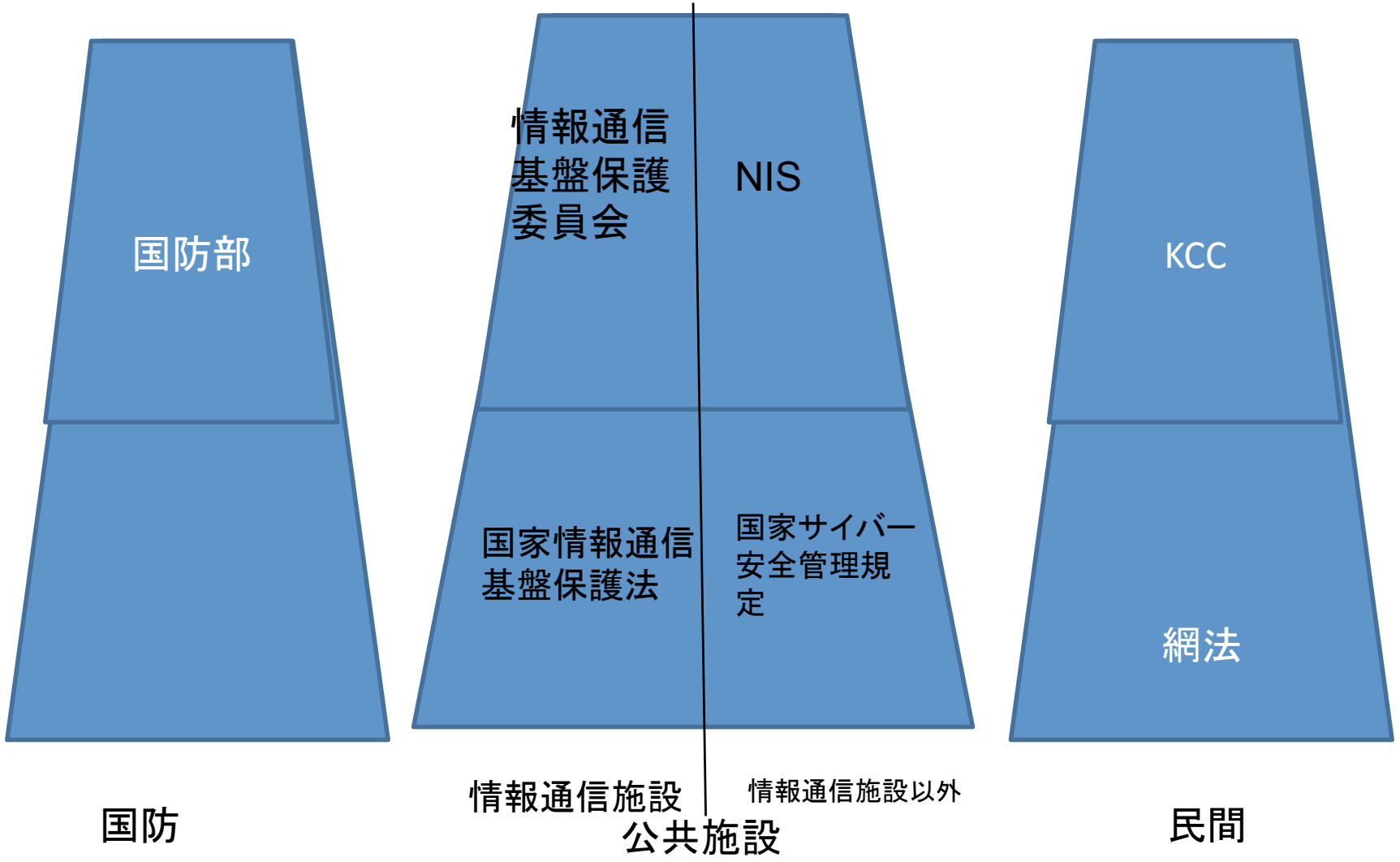


サイバーディフェンス研究所
名和さんの資料より

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

「7.7大乱」発生当時のサイバー危機対応体制



「『7.7DDoS事故』対応の問題点と再発防止法案」レポート

- (1) 政府各部署に分散した情報保護機能を効率的に調律できるようサイバー危機管理のための求心点の確立
- (2) インターネットインシデント対応のための韓国内外の民・官が協調できるリアルタイム協調体制の確立 (主要国家のCERT/ISP、韓国インターネットインシデント対応センター、韓国内ISP、ポータル、セキュリティベンダ、
- インターネット取引企業など)
- (3) 法的な不足を補う「(仮称) マルウェア拡散防止等に関する法律 (案)」制定
- (4) 企業および個人の情報保護認識を引き上げる必要性
- (5) 情報保護レベルの引き上げのための予算投入
- (6) 民間部門のサイバーインシデント対応専門人材の育成

「国家サイバー危機総合対策」(2009年8月)

分野	詳細
国家機関役割分担	NIS：サイバー危機対応総括担当 KCC：「ゾンビパソコン」除去および国民広報 国防部：サイバー部隊編成
法・制度の整備	-マルウェア削除要請権およびシステムアクセス要請権の法的根拠整備 -国家危機管理基本指針など政府規制改定
人材育成	-大学内に情報保護特化課程を新設 -「サイバー保安官」3,000 名育成
民間分野	-企業のサイバーセキュリティ教育の拡大 -産業別セキュリティ監視セン(ISAC) 設立
サイバー危機発生時対応	-民・官合同汎政府対策機構の構成 -KCCにマスコミ対応一元化
その他	-中央政府のネットワーク分離作業進行、地方自治体の分離作業も政府が -情報化予算に占める情報セキュリティ予算の段階的拡大 -国家インフラセキュリティ体制の高度化

韓国の通信の秘密

- 基本的な二つの法律
  - 「通信秘密保護法 (法律第9752号)」
  - 「情報通信網利用促進及び情報保護等に関する法律 (法律第9637号)」

通信秘密保護法

- 3条(通信と対話秘密の保護)
  - ①何人も、この法律刑事訴訟法または軍事裁判所法の規定によらないで郵便の検閲•電気通信の傍受や通信事実確認資料の提供をしたり、公開されていない他人との間の会話を録音または聴取できない。
- 第7条（国家安全保障のための通信制限措置(=通信傍受のこと)）
  - ①大統領令が定める情報捜査機関の長（以下 “情報捜査機関の長”という。）は、国家安全保障に対する重大なリスクが予想される場合に限り、その危害を防ぐために、これに関する情報収集が特に必要があるときは、次の各号の区分に応じて通信制限措置を行うことができる。<改正2001.12.29>(略)

「情報通信網利用促進及び情報保護等に関する法律 」

- 通称「網法」
- 日本ならば通信の秘密に関連する条項
- 第44条の7（不法情報の流通禁止など）
  - 1項
    - 「4 正当な事由なく、情報通信システム、データまたはプログラムなどを毀損·滅失·変更·改ざんしたり、その運用を妨害する内容の情報」
    - 「7 法令に基づいて分類された秘密など、国家機密を漏洩する内容の情報
    - 「8 “国家保安法”で禁止する行為を行う内容の情報」
  - 2項
    - 放送通信委員会は、(略) 審議委員会の審議を経て、情報通信サービス提供者または掲示板管理運営者に扱いを拒否・停止または制限するように命じることができる。

網法 続き

- 第46条の2（集積情報通信施設事業者の緊急対応）
  - (略)そのサービスの全部または一部の提供を中断することができる。 <改正2009.4.22>
  - 1 (略) 情報システムで発生した異常現象で、他の施設利用者の情報ネットワークや集積された情報通信施設の情報ネットワークに深刻な障害が発生するおそれがあると判断される場合
  - 2 外部で発生した侵害事故に集積された情報通信設備の重大な障害が発生するおそれがあると判断した場合
  - 3 重大な侵害事故が発生してバンソントンシンウィウォンフェナ韓国インターネット振興院が要求した場合

2 2009年8月以降の対応

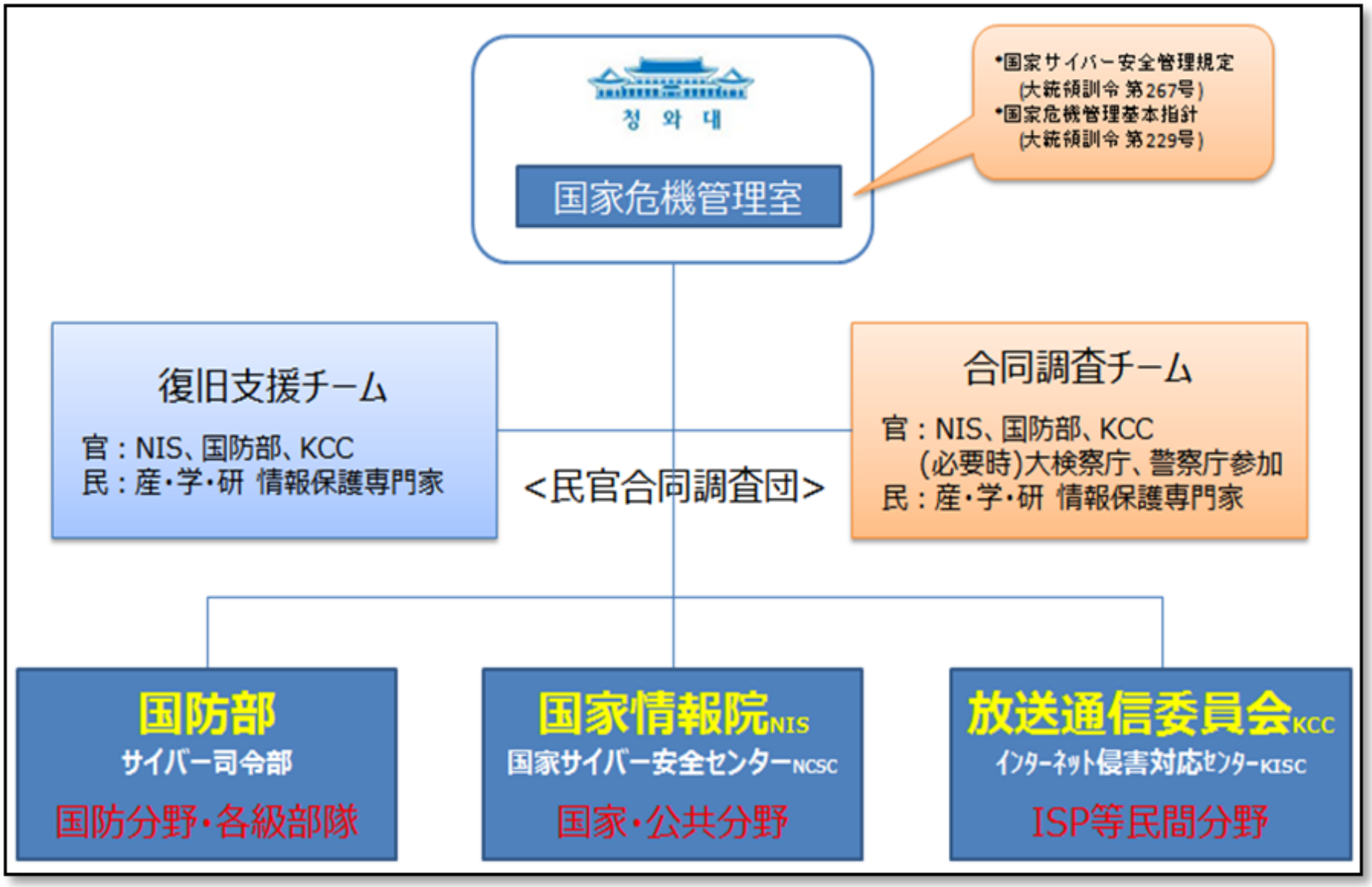
情報セキュリティ関連予算の増加

年度	情報化予算 (単位：億ウォン)	情報保護予算の比率
2007年	34,104	2.9%
2008年	34,062	4.7%
2009年	31,278	5.6%
2010年	32,867	8.2%
2011年 (案)	33,023	6.2%

効果的な政策

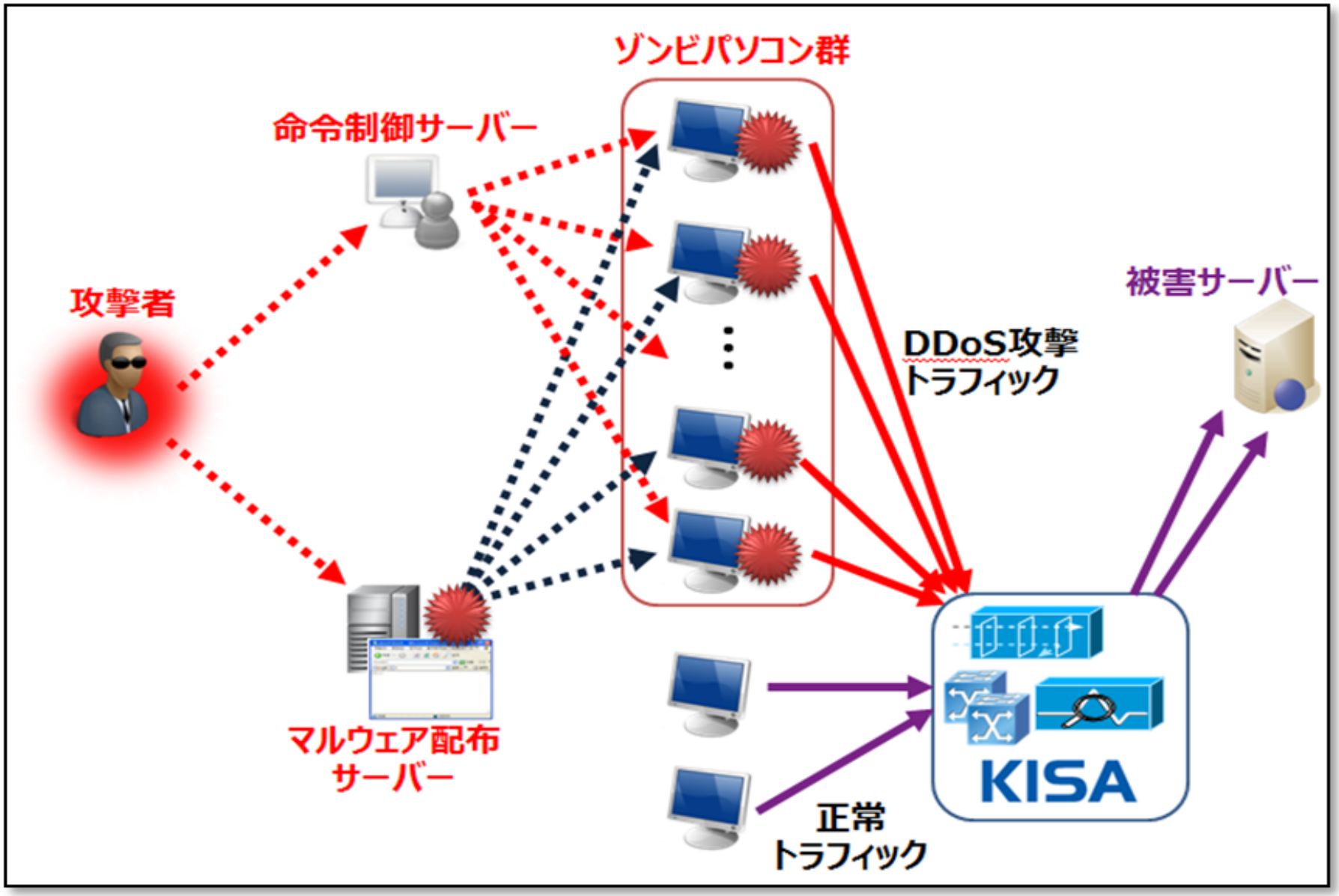
- 「コントロールタワーの構築」
- 「サイバー駆除体系の整備」
- 「DDOSサイバー避難所」

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

3 2011年3月4日 DDoS

防衛策の成功

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
- (対応の詳細は、省略
- 情報の早期取得・対応が功を奏した事件)

77DDoSとの比較

	7.7 大乱 (2009 年)	3.4 DDoS (2011 年)
攻撃対象	大統領府など韓国主要 23 サイト	大統領府など政府サイト、ネイバーなど国内主要国家トおよび駐韓米軍など 40 サイト
ダウンしたサイト	攻撃対象の多くのサイトが一時的にダウン	なし
攻撃持続時間	7~9 の 3 日間、18 時~ 翌日 6 時まで	4 日 10 時、18 時 30 分に開始、終了時点不明確
破壊 OS	MS Windows 2000/XP/2003	すべての Windows OS
ファイル構成	同一ファイル構成で複数回の攻撃	攻撃ごとにファイル構成が変化
駆除妨害	なし	ホスト改ざんでセキュリティソフトアップデートおよびアクセス妨害
HDD/ファイル破壊時点	最後の DDoS 攻撃日である 10 日正午に破壊。セキュリティソフトがない場合、システムをバックデートすれば防げた	システム時間を変更したり、感染時刻を記録した noise03.dat ファイルを削除すると感染後、4 日だったものが 5 日夜 9 時以降は即時破壊に変更
ゾンビパソコン数 (KCC 発表)	115,044 台	116,299 台
対応方式	備えがない状態で攻撃され、混乱を招いた	7.7 大乱以降、企業/機関の備えがあり、セキュリティと各機関との協調で被害最小化

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

４ 国家サイバー安保マスタープラン について

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。

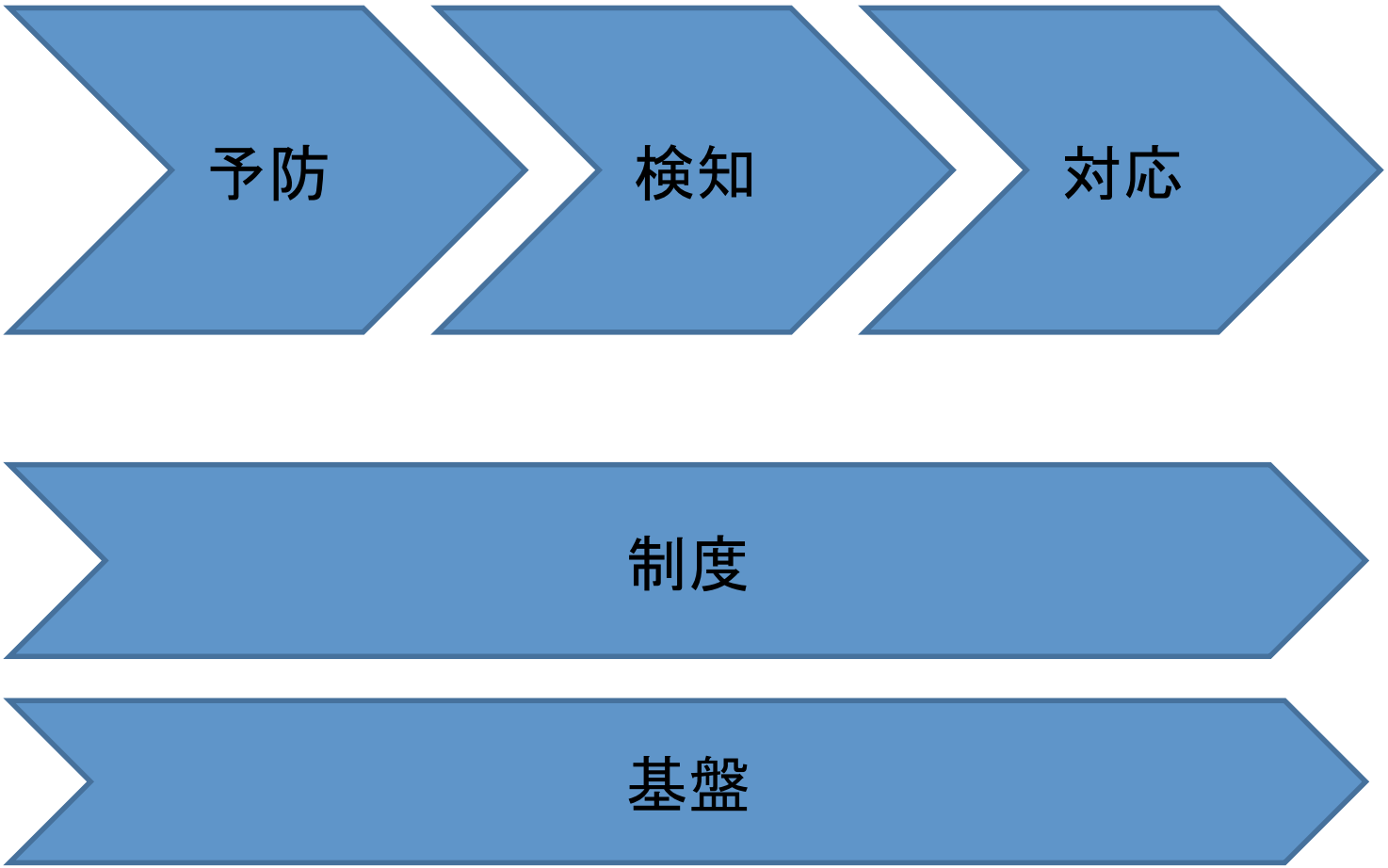
APT攻撃のインパクト

- 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

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

マスタープランの概要



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

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

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

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

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

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

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

まとめ

- 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
- 早期検知・早期対応の重要性