情報戦争の中での情報セキュリティ
―見えない敵とどう戦うか―

Black Hat Briefings

2004.10.14

宮脇磊介

目次

２１世紀の新しい「国力」
― Net War Capabilitiesの向上 ―

１　一人ひとりが「国際競争力」を高めること：自分は世界で何番目に位置するかを常日頃念頭に置くこと

２　国内法に抵触するような不始末はしないこと：海外のハイレベルを相手に腕だめしをすること

３　海外の仲間から尊敬される技量とモラルを示すこと：新しい世界（Cyberspace）に通用する説得力ある価値観を求めること

世界の流れに関する基礎認識
― 新たなステージ ―

１　Attrition Mirrored Sitesの閉鎖（2001.5.21）＝ Cyber Attacksの大衆化・日常化 ＝ プロ・エキスパートの時代

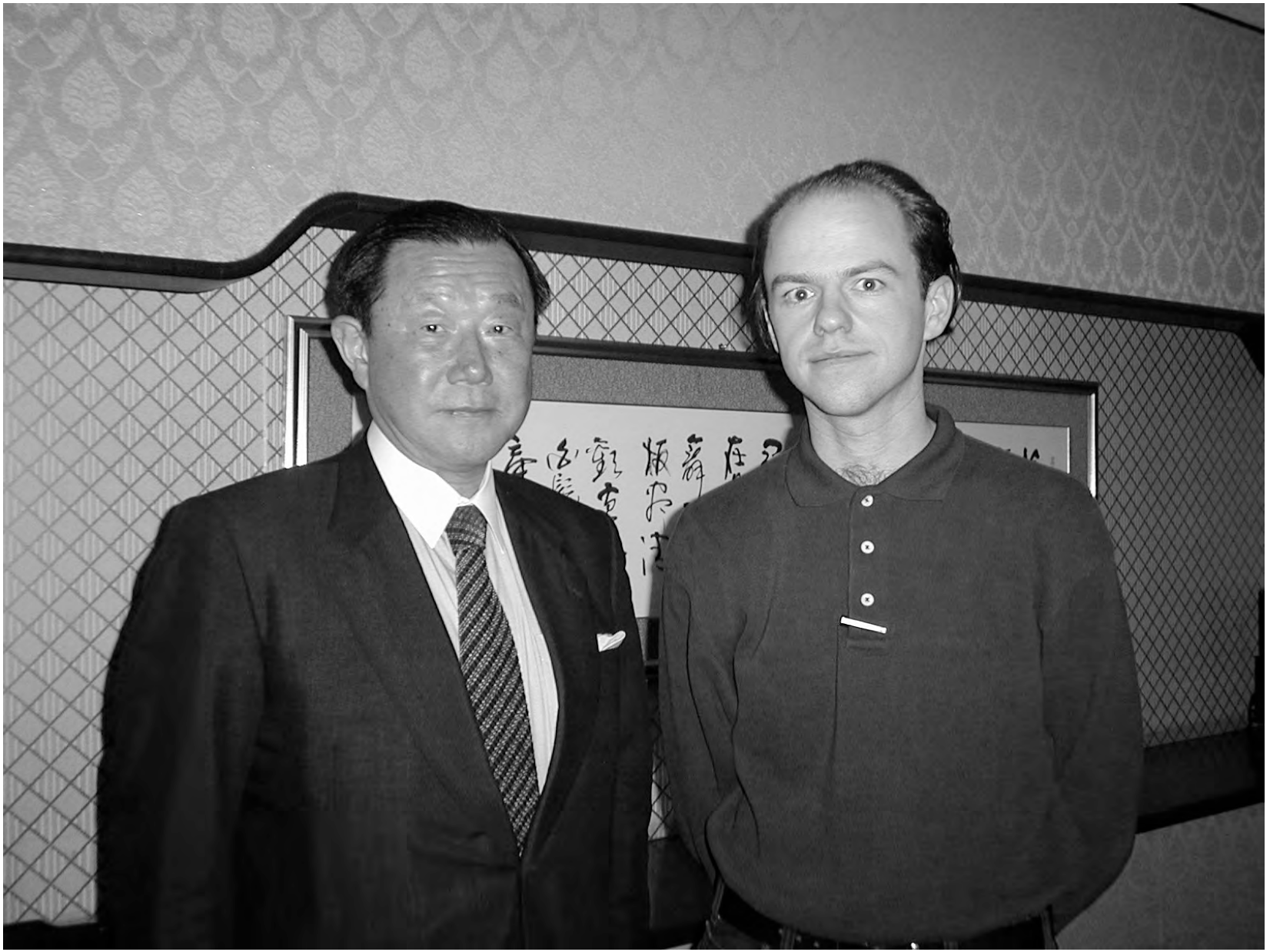
２　サイバーテロ・サイバー戦争の主役

・Cyber Rogue States（サイバーならず者国家）とその Patriotic Hackers

・Terrorist Groups

・Foreign Intelligence（海外情報機関）＝ 国営の組織犯罪

３　米国の卓越したサーベイランス（監視）機能がテロに対する強力な抑止力：「エシュロン」



ハッカーの順位（洗練度による）

Raymond　Parks

５　Naive　Novice

４　Advanced　Novice

３　Professional　Hacker

２　Organized　Crime／Terrorist　Group

１　Foreign　Intelligence

日本で起きていながら、実体が報道されないサイバー攻撃

１　中国の「HUC(Honker Union of China)」「CEU(China Eagle Union)と韓国のグループによる「予告を伴うサイバー攻撃」にさらされた日本

２　自民党本部のサイトがシャットダウンしたのを知らない自民党国会議員たち

○　深刻な事態に反応できない日本のリーダー層とジャーナリズム　＝　旧来の情報チャンネルの陳腐化

平成１３年２月２３日

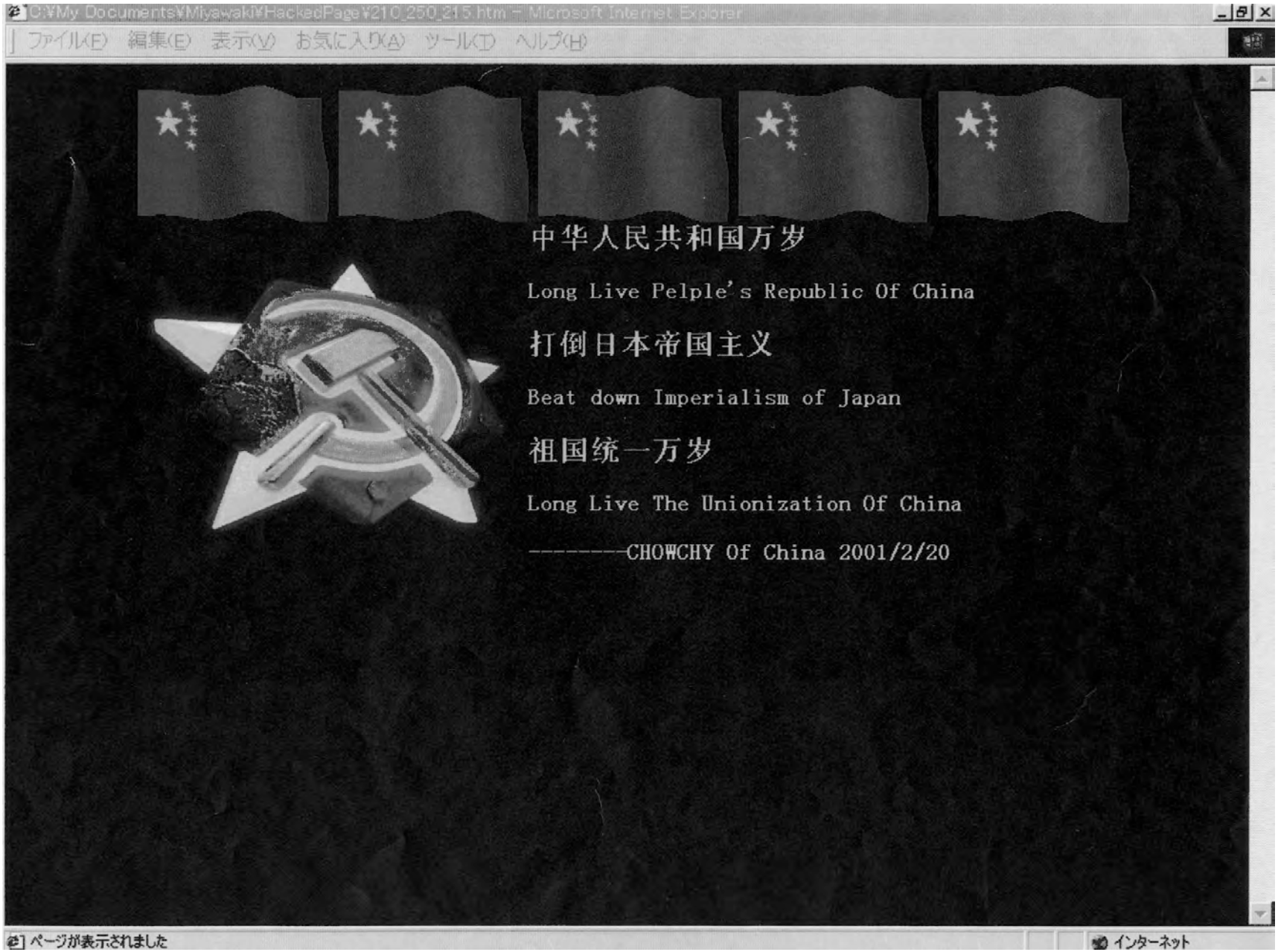
警察庁

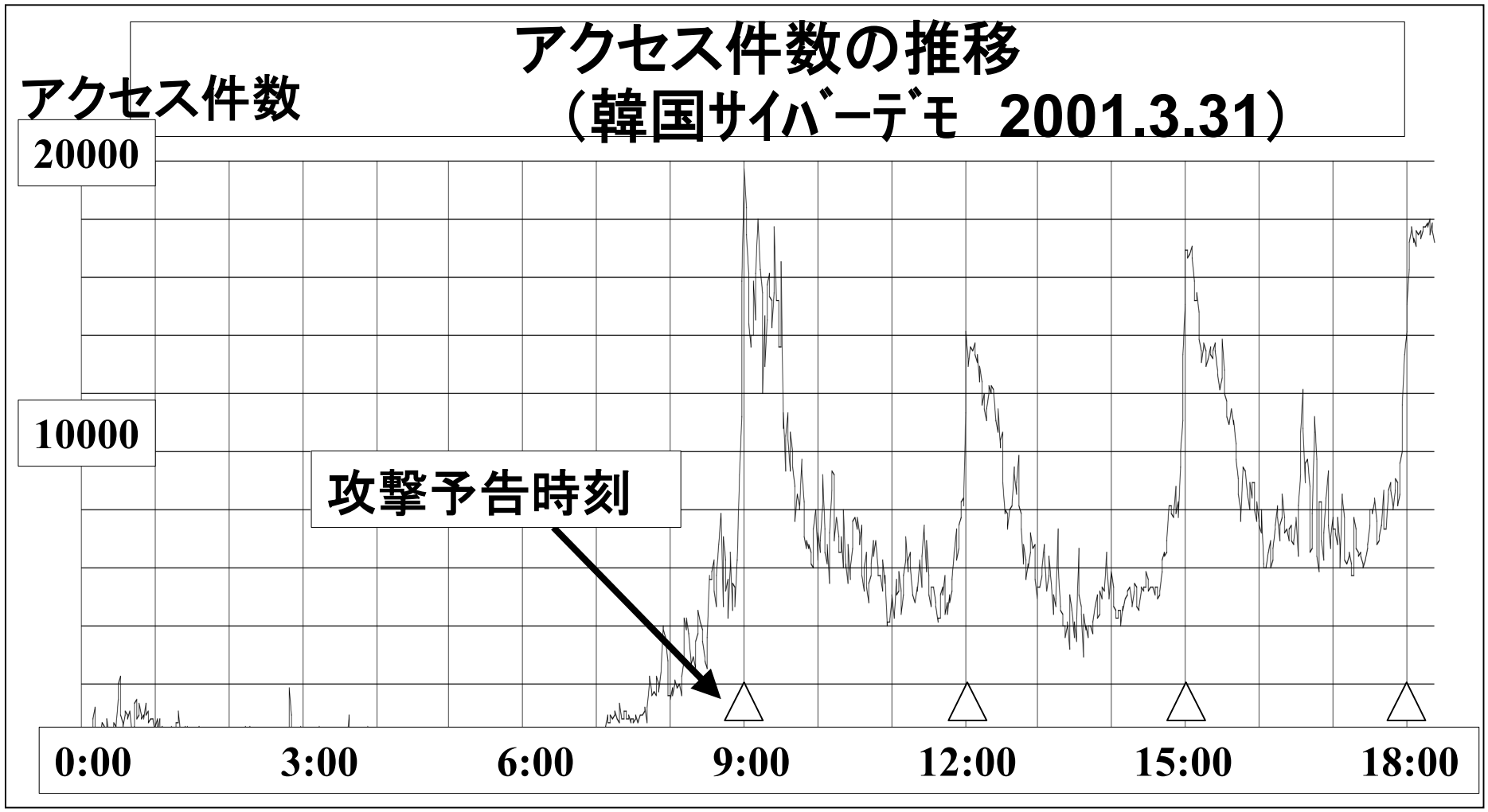
ホームページ書き換え事案に関する対策について

平成１３年２月１９日に、海外のサイトに我が国のサイトに対する攻撃を予告する内容が掲載されているとの情報を入手しましたが、これに関係すると思われる日本企業等に対するホームページ書き換え事案が発生しています。

２月２３日午前０時現在、約７０件の書き換えが行われたとの情報があります。今後の被害防止のための当面の対応策ついて確認することが重要です。

（以下略）





ログの解析からわかること

- アクセス状況
- 発信元
- その他の不正行為

日本の指導者層にみられる「リーダーシップの空洞化」現象

１「文系支配構造」：製造業の社長も法学部・経済学部出身者が主流だった

２「軍事／インテリジェンス無知構造」：日本特有の戦後の言論環境

３ リーダー層の「横並び意識」と「不勉強」：「政官業の鉄のトライアングル」の既得権益権護構造化

日本の情報セキュリティに見られる根本的問題点

ネットワークの正面玄関からの侵入対策を「情報セキュリティ」と考えていること

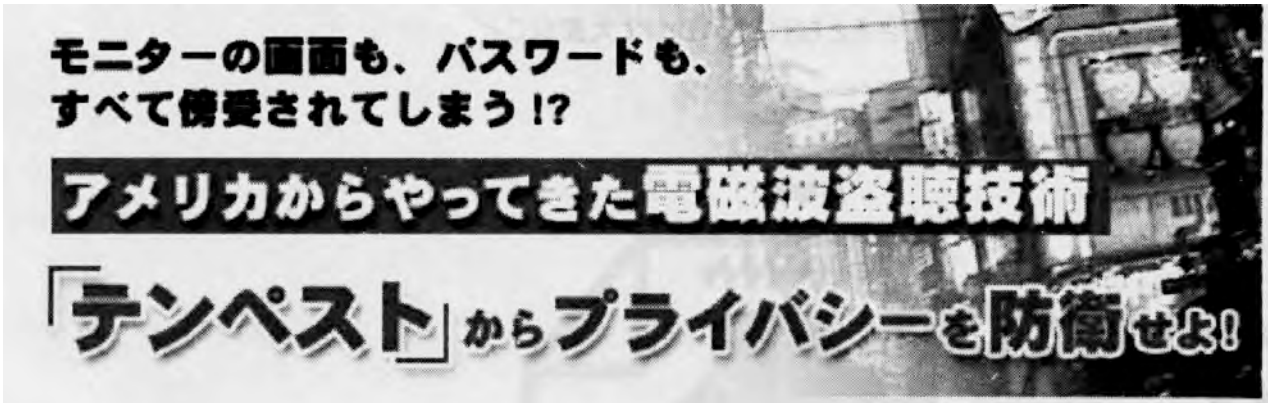
・・・・・・それ以外の手法がいっぱい

○ なぜでしょうか

ネットワークの技術者がネットワークを守れない！

（例）TEMPEST（テンペスト：The Electoro – Magnetic Pulse Emination Standardの略）

- コンピュータから漏れる電磁波をアンテナでキャッチして作動の内容・IDパスワード等を現示
- 秋葉原で部品を購入して容易に作成可能
- マニアは日常的に活動



モニターの画面も、パスワードも、すべて傍受されてしまう!?

アメリカからやってきた電磁波盗聴技術

「テンペスト」からプライバシーを防衛せよ!

2001/3/14 update

「テンペスト」という言葉をご存知だろうか。
我々がいかにセキュリティに気を配ってネットに接続しようとも、まったく関係なくパソコンの中身を覗き込めてしまう技術のことである。
パソコンに電源を入れている限り、接続されているさまざまな機器からは電磁波が漏れている。
それを傍受することで、モニターに表示される画像はおろか、表示されないパスワードまでが、離れた場所から盗まれてしまうというのだ！
果たしてそのようなことが起こり得るのか、もしそうならば我々はどのように対応すればよいのか。言葉だけが一人歩きし、パソコンユーザーの間に恐怖を撒き散らす「テンペスト」の実態を徹底検証する。

日中韓共同によるOS開発

朝日新聞 2003年(平成15年)8月31日 日曜日 42

携帯電話・カーナビ…

脱ウィンドウズ 日中韓が連携

日中韓3カ国と、そのコンピューターソフトや電機業界は、次世代型の携帯電話など情報家電やサーバーに組み込む基本ソフト(OS)を連携して開発することで大筋合意した。リナックスなど、製品に応じ自由に改造できる「オープンソース・ソフトウエア」(OSS)をベースに開発する。数年内にも実用化を目指す。世界で圧倒的シェアを握る米マイクロソフトのOS「ウィンドウズ」に依存して製品を作っていては、独自の開発力が伸びず、自国の関連産業の衰退につながるとの共通の危機感が背景にある。

来月3日にカンボジアで開かれる日中韓経済貿易大臣会合で、平沼経済産業相が3カ国間の協力を正式に提案、中旬に開く局長級会談で合意する。合意を受けて日本からはNTTデータ、松下電器産業、日立製作所、NEC、富士通などの大手が参加して、秋をめどに「日中韓OSS推進フォーラム」を設立する。

経産省によると、3カ国が連携してソフト開発を進めるのは初めて。

連携するのは、携帯電話やデジタルカメラ、カーナビゲーションなどの情報家電のほか、サーバー向けOSやソフトの開発。今後、リナックスなどをベースにOSを開発するなど、国境を超えた連携が進んでいる。ただ、今後の市場の拡大に備えたり、開発力の強化を図ったりするには、世界の工場・中国の参加が不可欠で、かねて国内ソフト会社でつくる情報サービス産業協会や経産省が働きかけてきた。

官公庁や自治体では、独自の安全対策が講じられることやコストの安さなどを理由に、コンピューターのOSにリナックスを採用する動きが加速している。

基本ソフト(OS)開発での日中韓の連携

キーワード

リナックス　コンピューターを動かす基本ソフト(OS＝オペレーティング・システム)の一つ。ウィンドウズと違って無料で、プログラムの設計図である「ソースコード」も公開されており、自由に改造できる。このため製品コストを安くしたいメーカーが製品に組み込む動きを加速させている。フィンランド・ヘルシンキ大学の学生だったリーナス・トーバルズ氏が開発し、世界中の個人が改良に参加するうち、動作が軽快で安定したソフトに成長した。

官民で基本ソフト開発

情報家電のOSは、リナックスとマイクロソフトのOSが主導権争いを繰り広げている。特にアジアで急速に普及する携帯電話のOSの行方は、国内のソフト開発業界にも大きな影響を与える。

「携帯電話のOSがマイクロソフトに独占されれば、日本のIT(情報技術)産業の拡大の余地はなくなる」(ソフト業界関係者)との懸念もあった。

今回の動きに先行して、ソニー、松下など日韓欧の大手電機8社が7月、開発したOSの性能強化を目指す「CE・リナックス・フォーラム」を設立するなど、各国政府の研究データを共有したりする。

不正侵入を防護するツールが危ない

１　ファイアーウォール

２　侵入検知装置（IDS）

〇海外メーカーと海外情報機関：「バックドア」

「情報セキュリティ」（案）

2003.12.16

内閣官房情報セキュリティ対策室
経済産業省情報セキュリティ政策
宮脇磊介

１　「情報セキュリティ」とは

　情報セキュリティとは、電子的に構築されているシステムおよびそのシステムに関わる情報を、物理的、技術的、欺計的な外部および内部からの破壊活動から、そのシステムが本来期待されている機能を安定的に確保（システムの安全、情報の安全な流通、保存、活用）するべく、防護し、保全すること

「情報セキュリティ」（案）

２ 「情報セキュリティ」の内容

（１）システムの出入口から侵入する外部者およびシステムに関する内部者によるシステムの損壊および情報の窃視・窃取・損壊の防止

（２）システムから漏洩する電磁波の採集（TEMPEST）やケーブルへの器材敷設（wire tapping）などによる情報傍受の防止

（３）システムを構築する基本ソフト（OS）やファイアーウォール（FW）、侵入検知装置（IDS）の情報保全

（４）システムへの電磁波照射によるシステムの誤作動・破壊および情報の損壊の防止

（５）システムの関係者（設計者、設定者、運用者等）による破壊活動・情報漏洩の防止

（６）その他脆弱点の発見および保全対策

情報セキュリティに対する日米の相違点

- 情報セキュリティを考えるスタート
  米: 「国家安全保障（National Security）」
  ＝高い視点・総合的な対策
  日: 「ネットワーク・セキュリティ」

- 情報セキュリティをリードする中心人物
  米: 軍／情報機関関係者
  テロ・組織犯罪専門家
  日: ネットワーク技術者
  暗号技術の学者

日米の相違点（続き）

- 情報セキュリティにおける「脅威」
  - 米：海外情報機関、テロリスト、組織犯罪、海外軍・情報機関の意向を体したハッカー、etc.
  - 日：DoS攻撃、スパムメール、トロイの木馬、etc.

- 情報セキュリティ対策の主眼
  - 米：重要インフラ防護（CIP）に向けた諸対策
  - 日：「セキュリティ・ポリシー」「ISMS」

1999.6　米国CSISでの講演

CYBERCRIME...
CYBERTERRORISM...
CYBERWARFARE...

AVERTING AN ELECTRONIC WATERLOO

Project Membership

Global Organized Crime Steering Committee Membership

Chair

William H. Webster
Former Director, Central Intelligence Agency
Former Director, Federal Bureau of Investigation

Director

Arnaud de Borchgrave
Senior Adviser, CSIS

Deputy Director

Frank J. Cilluffo
Senior Analyst, CSIS

Members

Duane Andrews
Former Assistant Secretary of Defense (Director C^3I)

Zoe Baird
Yale Law School

Robert Bonner
Former Administrator
Drug Enforcement Agency

William S. Cohen
Former U.S. Senator
(currently serving as Secretary of Defense)

Charles Connolly
Merrill Lynch & Co., Inc.

John Deutch
Former Director
Central Intelligence Agency

Robert Gates
Former Director
Central Intelligence Agency

Carol Hallett
Former Commissioner
U.S. Customs Service

Admiral James R. Hogg
U.S. Navy (Ret.)

Fred C. Iklé
Former Under Secretary of Defense

Stuart Knight
Former Director
U.S. Secret Service

Jon Kyl
U.S. Senator

Walter Laqueur
Cochair, International Research Council
CSIS

Patrick J. Leahy
U.S. Senator

Bill McCollum
U.S. Representative

General Edward C. Meyer
U.S. Army (Ret.)

Sam Nunn
Former U.S. Senator

Oliver Revell
Former Associate Deputy Director
Federal Bureau of Investigation

William V. Roth Jr.
U.S. Senator

Donald Rumsfeld
Former U.S. Representative
Former Secretary of Defense

James R. Schlesinger
Former Secretary of Defense
Former Secretary of Energy
Former Director, Central Intelligence Agency

William Sessions
Former Director
Federal Bureau of Investigation

Admiral William Smith
U.S. Navy (Ret.)

Lieutenant General Edward Soyster
Former Director
Defense Intelligence Agency

J. Chips Stewart
Booz-Allen & Hamilton Inc.

Richard Thornburgh
Former U.S. Attorney General

Curt Weldon
U.S. Representative

R. James Woolsey
Former Director
Central Intelligence Agency

William Zeiner
MITRE Corporation

高度情報通信ネットワーク社会推進戦略本部　名簿

本部長	小泉純一郎	内閣総理大臣
副本部長	竹中平蔵	情報通信技術（IT）担当大臣・経済財政政策担当大臣
	福田康夫	内閣官房長官・男女共同参画担当大臣
	片山虎之助	総務大臣
	平沼赳夫	経済産業大臣
本部員	森山眞弓	法務大臣　他各省庁大臣
有識者	秋草直之	富士通株式会社社長
	出井伸之	ソニー株式会社会長兼CEO
	奥山雄材	KDDI株式会社社長
	梶原　拓	岐阜県知事
	岸　暁	株式会社東京三菱銀行会長
	鈴木幸一	株式会社インターネットイニシアティブ社長
	松永真理	エディター
	宮津純一郎	日本電信電話株式会社社長
	村井　純	慶応義塾大学環境情報学部教授

情報セキュリティ専門家調査会委員名簿

石井　威望	東京大学工学部名誉教授
今井　秀樹	東京大学生産技術研究所教授
江畑　謙介	軍事評論家
春日　正好	（社）情報サービス産業協会副会長
菅野　明	全国銀行協会副会長・専務理事
久和野　泰之	（社）テレコムサービス協会事務局長
合田　宏四郎	（社）日本ガス協会副会長・専務理事
酒井　昭	（社）日本民間放送連盟専務理事
鈴木　賢	小田急電鉄（株）常務取締役運輸事業本部長
高橋　利彦	日本電気（株）NECソリューションズ執行役員常務
辻井　重男	中央大学理工学部教授
殿塚　猷一	電気事業連合会専務理事
前田　雅英	東京都立大学法学部教授
宮原　英明	（社）電気通信事業者協会専務理事
横山　善太	日本航空（株）副社長

（五十音順：敬称略）

国土安全対策委員会（重要インフラ対策委員会の発展的解消）

委員長	： 樋口廣太郎	アサヒビール㈱相談役
委員長代理	： 石原　信雄	地方自治研究機構　理事長（元内閣官房副長官）
委員	： 相原　宏徳	宇宙通信㈱会長
	荒木　浩	東京電力㈱顧問
	大堀　文男	東京ガス㈱副社長
	火災　敬之	東海旅客鉄道（JR東海）㈱社長
	佐藤　謙	都市基盤整備公団副総裁（元防衛次官）
	谷　公士	マルチメディア復興センター理事長（元郵政次官）
	谷野　剛	㈱三菱総合研究所社長
	西岡　喬	三菱重工業㈱会長
	浜口　友一	NTTデータ㈱社長
	御手洗冨士夫	キャノン㈱社長（経団連副会長）
特別参与	： 宮脇　磊介	宮脇磊介事務所代表（初代内閣広報官）
技術顧問	： 舟橋　信	前警察庁技術審議官

事務局を（財）未来工学研究所におく。

（事務局長　：　稗田浩雄　　（財）未来工学研究所　技術・国際関係センター長）

情報セキュリティをめぐる環境の変化

１　冷戦の終結

（１）軍事から経済へ：「エシュロン」を活用した経済情報戦略（１９８０年代後半から日本企業がターゲット）

（２）グローバリゼーションによる企業の国際競争激化：「コンペティティブ・インテリジェンス（競合企業間情報活動）

（３）国際テロの激化に対する監視（サーベイランス）の強化：「ジミー・カーター」

２　IT革命の進展

（１）インターネット／コンピュータシステムの普及による新たな脆弱性の増大

（２）通信傍受等情報収集技術の高度化・大衆化

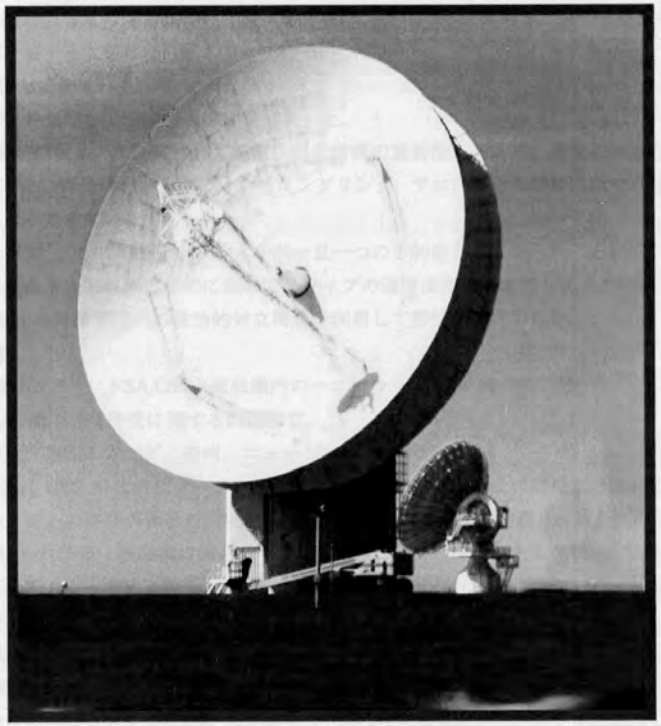
３　企業への従業員の帰属意識の希薄化：内部者が最も危険

○国家も企業も個人も「情報戦争」の当事者

エシュロン

Interception Capabilities 2000

盗聴能力２０００



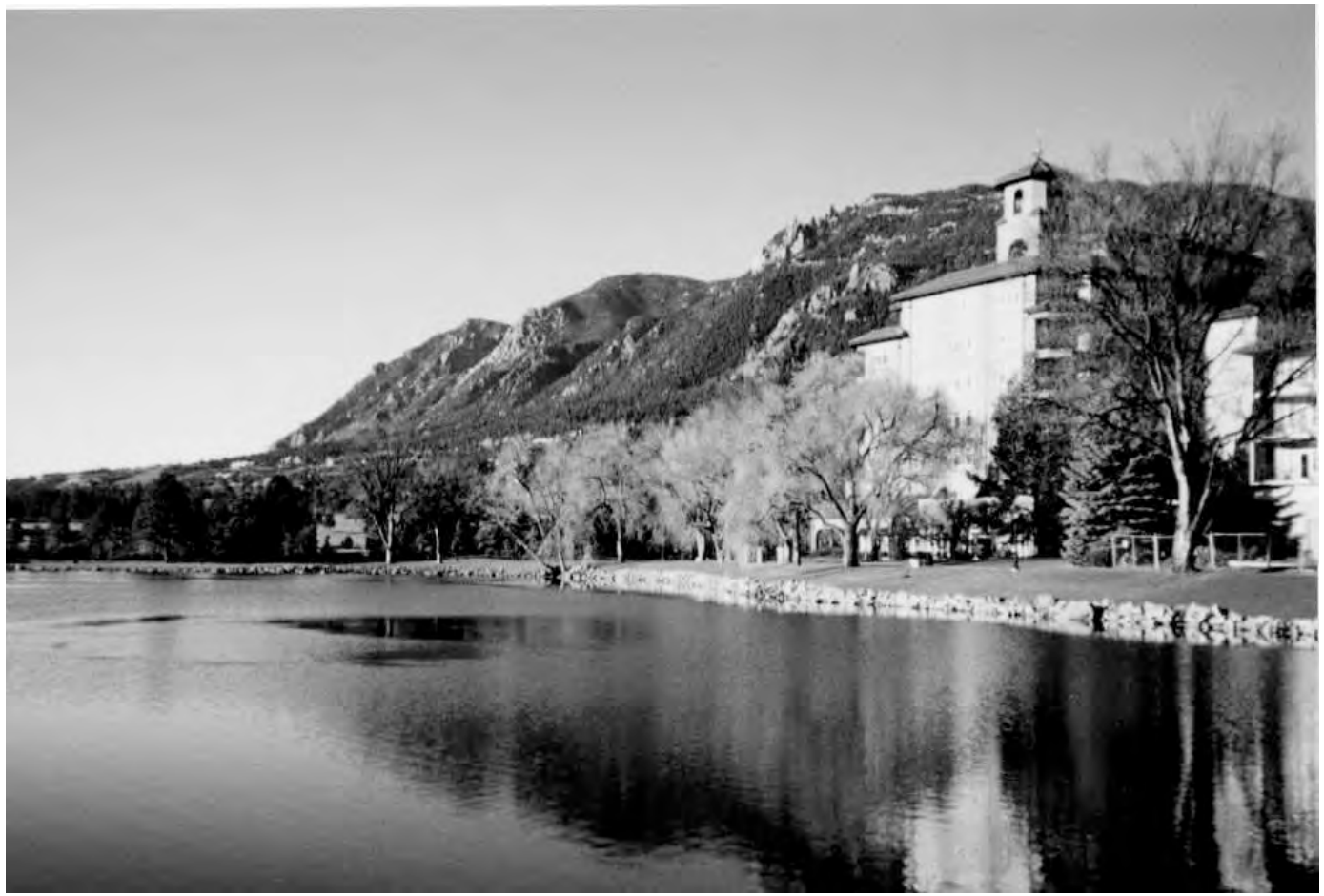
Report to : Director General for Research of the European Parliament
(Scientific and Technical Options Assessment Program Office)
By Duncan Campbell, IPTV LTD, Scotland

情報コミュニティの経済情報戦略

Fourth,we are assessing how some governments violate the rules of the game international trade. This does not mean that the CIA is in the business of economic espionage--for example, trying to learn the business plans of foreign companies in order to give such information to America firms. It does mean, however,that we are paying careful attention to those countries or businesses who are spying on our firms, to the disadvantage of American businesses and American workers, and to those governments and foreign companies that try to bribe their way into obtaining contracts that they cannot win on the merits. Frequently we are able to help the U.S. government obtain quick redress when such companies never realize that they have received our assistance and even state publicly that they do not need it. This is fine with us. It is the nature of the intelligence business.

（1995.1 CIA長官証言）

シャイアンマウンテン



シャイアンマウンテン（Cheyenne Mtn）の地下大要塞
―何をあなたに語りかけているか―

・NORAD（北米防空軍総司令部）＝米国宇宙軍と総令官が兼務

・コロラドスプリングス（ロッキー山脈最南端）

・岩山の下に4階建て15棟

地球上の衛星・航空機・艦船（潜水艦は特に重要）の運航状況

地球上の更新状況その他電波の動きを掌握

・核攻撃に対して攻撃してくる国家意思を特定できるシステムと連結

米国宇宙軍次いで米国戦略空軍が
サイバー戦争を統括することになった　なぜ？

１　核戦争を抑止するには、どこの国が核ミサイルを発射したのかを瞬時に特定できる能力が必要
＝そのために、シャイアンマウンテン（CMOC）に全情報が集約されるシステムが構築されてきた

２　核戦争と同様、サイバー戦争を仕掛けられた場合、どこの国の国家意思に基づくものか、いかなるテログループによる仕業かを瞬時に特定する必要あり ＝ 卓越した米国のサーベイランス能力

〇このシステムが、テロ対策に威力

国際関係の本質
―「表のゲーム」と「裏のゲーム」―

１　国際関係は、「ルールのある表のゲーム」と「ルールのない裏のゲーム」とで成り立っている

２　「ルールのある表のゲーム」は、外交や戦争（従来型）である

３　「ルールの無い裏のゲーム」の主役は、海外情報機関である。国益を実現し、国益を守るために完全犯罪を追求する（＝「国営の組織犯罪」）。テロや革命をも誘発させる

４　日本は、「ルールの無い裏のゲーム」に参加していない、やられる一方の国である

「情報活動」の手法

1　ヒューミント（HUMINT）：スパイなど人的情報源からの情報活動

2　シギント(SIGINT)：

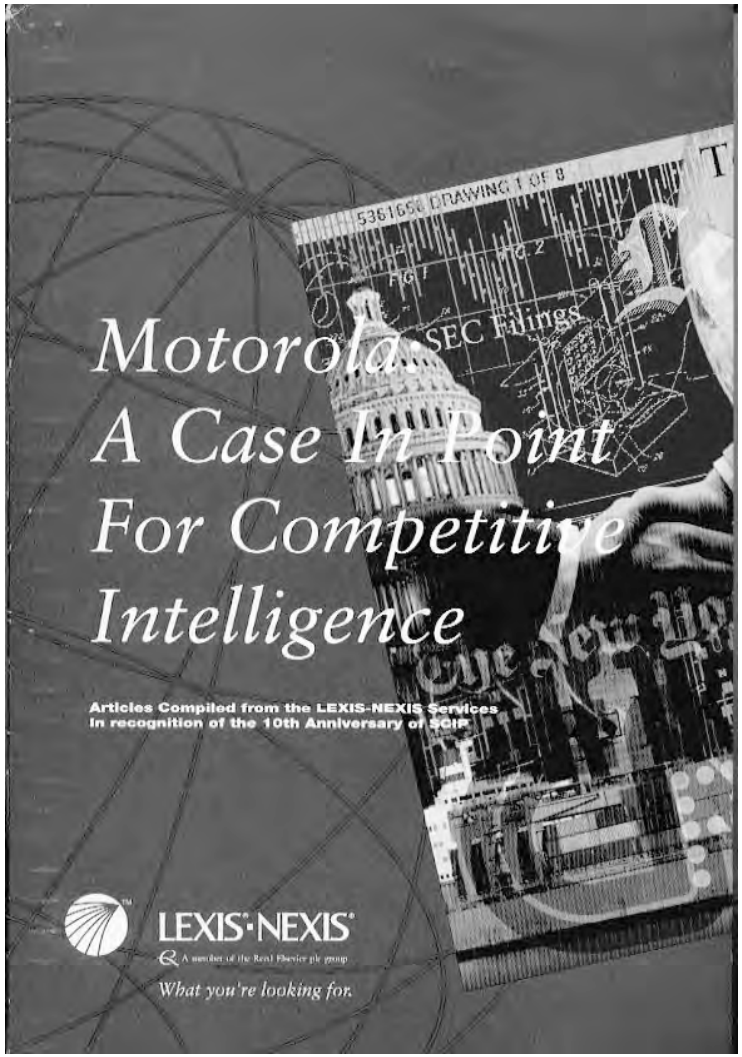
コミント（COMINT）：通信傍受による情報活動
・地上回路（電話線・通信ケーブル）による通信
・無線電波による通信

エリント(ELINT)：電子的に収集する情報活動
・コンピューター侵入
・人工衛星による偵察・捜査通信
・トラヒック分析（２者間で電子的通信が行われている事実だけをもとにして、実際にその通信内容を知ることなく結論を引き出す手法）

サイビント(CYBINT)
・e-mail傍受
・コンピューター侵入

コンペティティブ・インテリジェンス

— 1997.1 日本に上陸 —



①誰が

②いかなる意図・目的で

③いかなる手法をもって

あなたの企業を狙ってくるか

その全体像と対策を共有すること

あなたの企業を狙う者は何者か、
狙いは何か（＝脅威の主体と目的）

- **外国政府機関（軍・情報機関）**
  国家戦略
  技術入手
  自国企業支援（＝経済情報戦略／「経済安全保障」）
- **外国企業（ Competitive Intelligence／産業スパイ）**
  技術入手
  海外企業の買収等企業戦略
- **組織犯罪・テロリスト集団**
  サイバーテロその他の破壊活動
- 個人
  インサイダー
  職業的犯罪者
  愉快犯罪者

◎日本企業は「情報戦争＝見えない敵による戦争」の当事者である

狙われている企業情報

１　企業戦略（合併、海外展開、etc.）

２　技術

３　特許出願／研究開発

４　個人情報／顧客情報／個人情報分析データ

５　その他企業として盗まれると大きなダメージを受ける情報

２つのキーワード

「イマジネーション（想像力を働かせること）」
―見えない敵が見えてくる

「インテリジェンス（チエを働かせること）」
―勝ち方（よりスキの無い対策）が見えてくる

むすび

BROADER PERSPECTIVE!!

より広い視野で隙（すき）の無い対策を

天然資源に乏しい日本の国是は

①科学技術立国

②情報（インテリジェンス）立国

あなたはそれを達成するための貴重な資源です

Thank you very much!