レポート

サイバー防衛報告書
「サイバーセキュリティ:世界ルールの主たる争点」 概要

※本冊子は 2012 年 1 月 30 日に米国マカフィー社と SDA により発表された
「Cyber-security : The vexed question of global rules」の一部をまとめたものです。

目次

エグゼクティブ サマリー

このレポートは世界のサイバー防衛状態に関する報告書です。本レポートは、SDA (Security & Defence Agenda) のサイバー セキュリティ プログラムの一環として発表するもので、2012 年に SDA で行われる議論と調査の基礎となるものです。SDA はブリュッセルに本部を置くセキュリティ分野のシンクタンクです。

本レポートは、2011 年の終わりから 2012 年の初めにかけて政府機関、企業、国際組織、学術機関に所属する 80 人のサイバー セキュリティ専門家に行ったインタビューを基に作成されています。本レポートにより、世界の専門家が現在のサイバー脅威とその防衛対策をどのように見ているのか概観することができます。

誰が規則を定めるべきか、また、軍の優位性はどの程度まで許されるのかについても議論しています。サイバー空間には国境がないため、セキュリティは最も脆弱なリンクと同じレベルになります。規制のない国に対して何の対策も講じなければ、サイバー犯罪者を取り締まることはできません。

本レポートは 2 部構成になっています。最初の部分では、サイバー戦争またはサイバー攻撃という用語の意味が定義されていない理由を主題にしています。同じ言葉を使っていても、軍関係者と技術的な専門家とでは表す意味が異なります。

本レポートにより、早急に対応を要するいくつかの課題が浮き彫りになりました。一例をあげてみましょう。

- 軍と民間企業の間でどの程度の情報共有を事前に行うべきか
- 国際的な協力関係を強化する必要性
- インターネットに対して、より強固なセキュリティ アーキテクチャを導入すること
- 国際協定の代わりとなるサイバー空間の信頼基準を構築すること

本レポートの後半部分では、21 か国に対するストレス テストの結果をまとめています。この評価システムは、Robert Lentz 元米国防次官補代理 (サイバー情報保障担当) の方法論を採用しています。攻撃からの耐性を 5 段階で表し、サイバー防衛状態とサイバー攻撃の阻止能力を評価しました。

この国別のストレス テストは、2011 年の秋に SDA が 35 か国 250 人のサイバー セキュリティ専門家に行った調査結果を補完するものです。この調査は、政府閣僚、国際組織のスタッフ、第一線で活躍する学者、シンクタンク研究員、IT 専門家を対象に行いました。サイバー空間での国際協力の強化については様々な意見が出されましたが、調査対象の半数以上はサイバー空間を海や宇宙と同様にグローバルな領域と考えています。

推奨事項

1. 透明性については多くの課題が残るが、セキュリティ機構とプロセスの利用において民間企業と政府機関の信頼関係を構築する必要がある。
2. CAMM (Common Assurance Maturity Model) や CSA (Cloud Security Alliance) のように、情報とベスト プラクティスを共有する組織を設立し、業界の利害関係者の間での信頼関係を構築する。
3. インターネット データの保護に対するユーザーの意識を高める。
4. 新しい技術だけでなく、標準規格や規則にも投資し、攻撃者の識別を可能にする。
5. 人権を侵害せずに匿名性を排除し、識別能力を向上させる。
6. 官民の協力体制を強化するため、第三者を介したオランダのモデルを参考にする。
7. 今後の環境を予測し、スマートフォンやクラウド コンピューティングがもたらす新たな問題を分析する。最適なセキュリティ レベルを実現するには、クラウド コンピューティングに適切なアーキテクチャが必要です。
8. 情報の保護に優先順位を付ける。1 つのもので全てをまかなうことはできません。達成すべき目標は、状況に応じて機密性、統合性、可用性を維持することです。
9. 国際協定に代わるものとして、暫定的であってもサイバー空間の信頼基準を構築することを検討する。米国などは協定を検証不能で、法的拘束力がない非現実的なものと見ています。
10. サイバー空間と既存のプロセスや体系への統合を検討する。サイバー空間は現実の世界を表します。政府の意思も反映されます。

世界的な調査

SDA が 2011 年の終わりに行った世界的な調査では、サイバー攻撃に対する準備が最も整備されている国はどこか回答者に質問しました (自国は除く)。この結果、米国、英国、エストニアが上位 3 か国になり、最も評価が低かったのがアルバニア、メキシコ、ルーマニアでした。

SDA は 250 人のセキュリティ専門家にサイバー空間での国際協力を強化する最も簡単な方法を質問しました。回答者には EU、国際刑事警察機構、欧州警察組織、国連、NATO、OSCE などの職員も含まれています。多くの回答者が、情報共有の促進、サイバー空間での訓練の増加、共通する標準規格の策定などを挙げています。

主な調査結果

- 回答者の 26% は、サイバー戦争という用語を不正確なもの、または不安を煽るものと答えています。適切な用語だと答えたのは 45% です。
- 回答者の 38% は、サイバー防衛をミサイル防衛と同等に重要だと答えています。サイバー セキュリティの方が重要だと答えた回答者もほぼ同数でした (36%)。
- また、回答者の 45% は、サイバー セキュリティを国境警備と同等に重要だと答えています。国境警備よりも重要性が低いと答えたのは 35% で、意見が分かれています。
- 回答者の 63% は、サイバー セキュリティを予算削減の対象にすべきではないと答えています。予算削減の例外にすべきではないと答えたのは 8% に過ぎません。
- ほぼ同数の回答者 (62%) がサイバー空間を海や宇宙空間と同様にグローバルな存在と見ています。
- 半数以上の回答者 (57%) は、サイバー空間で軍拡が起きていると考えています。大半の回答者 (84%) は、サイバー攻撃を国家、国際安全保障、貿易に対する脅威と感じています。
- 大半の回答者がサイバー セキュリティの訓練が重要だと考えていますが、民間企業の回答者でこのように答えたのは調査対象全体の 5 分の 1 に過ぎません (21% は国際的な訓練、22% は国内での訓練が重要と回答)。
- 3 分の 2 以上 (67.6%) の回答者は、民間企業に対する政府の規制を強化すべきと答えています。
- 民間企業と公営企業の両方で、回答者の半数以上 (56%) が技術不足を指摘しています。
- サイバー攻撃による重大な脅威として重要インフラの損傷や破壊が挙げられていますが、サイバー攻撃が広範囲に経済的な影響を及ぼす国家的な脅威だと答えたのは 43% です。
- 最大の脅威として、個人情報や知的財産を盗み出すサイバー上のスパイ活動だと答えたのは 15% です。

セクション I. サイバー セキュリティにおける難題の解消

専門家や政府関係者の間で用語が統一されていない状況では、サイバー空間を規制することは至難の業でしょう。同じ言葉でも防衛関係者とセキュリティ専門家の間で解釈が異なっています。サイバー セキュリティについて国際的な議論を進めるには、まず言葉の定義を行う必要がありますが、このような動きはまだ見られません。

用語：サイバー戦争とサイバー攻撃という用語は様々な意味で使われています。一つの意味に固定するべきでしょう。米国のサイバー セキュリティ責任者だった Richard Clarke 氏は『Cyber War』の中で航空機を墜落させて地下鉄を破壊するシナリオについて言及しています。このようなシナリオの現実性については懐疑的な見方もありますが、多くの人がサイバー空間で大量破壊兵器が使われる可能性を否定していません。

Stewart Baker 氏はサイバー戦争の定義を明確に述べています。Steptoe & Johnson のパートナーであり、ジョージ W. ブッシュ政権下で国土安全保障省次官補を務めた同氏は「サイバー戦争を軽視する人物は、サイバー空間に限定された戦争は起きていないと主張するが、これは空中戦は空中に限定されるというのと同じだ。実際の空中戦はより大きな戦闘の一部として行われている」と述べています。

Baker 氏は、単独かどうかは別として、21 世紀の戦争ではサイバー兵器が最初に配備される可能性があるとし、「これは空軍力とは異なる。サイバー兵器は様々なことが実行できるし、このような武器を実際に使っても戦争状態と言えるかどうかは微妙だ。飛行禁止区域を設けても戦争行為とは言えないだろう。効果的かどうかは別として、2008 年に発生したグルジアに対する攻撃はサイバー戦争に他ならない」と述べています。

stratsec の CEO で、BAE Systems Australia のサイバー セキュリティ責任者である Tim Scully 氏は「サイバー戦争という言葉を使いすぎると、サイバー セキュリティの問題を政府や防衛関係者に押しつけることになる。民間企業に対するサイバー脅威の影響が無視され、政府の予算配分に支障をきたす可能性もある。サイバー空間の軍事化を招く結果にもなりかねないので、サイバー戦争という言葉は使用を控えるべきだ」と述べています。

ワシントン DC にある戦略・国際問題研究所 (CSIS) で Technology and Public Policy プログラムを担当する James Lewis 氏は、現実に発生している事象をよく検討するべきだと指摘し、「現行の国際法と戦略の枠組みにサイバー紛争を組み込むことを検討するべきだ。エストニアに対する攻撃は攻撃ではなかった。NATO 条約第 5 条 * は適用されず、軍事行為とは見なされなかった」と述べています。NATO 条約第 5 条では、NATO 加盟国に対する攻撃を全加盟国に対する攻撃と見なし、集団的自衛権を行使すると定義されています。

未知の領域に突入：サイバー犯罪は儲かるだけでなく、リスクが低く、匿名で実行することが可能です。核の脅威やそれ以前の脅威と異なり、サイバー上の脅威は知らないうちに襲ってきます。猛威を振うまでにそれほど時間はかかりません。毎年、100 万もの新しいウイルスやワーム、論理爆弾が出現し、この数字は年々増えています。

McAfee の公共事業担当 CTO の Phyllis Schneck は次のように述べています。「サイバー犯罪者は動きが迅速で、資金も豊富にある。情報共有に対する法的な制限もなく、非常に組織的な攻撃を実行することも可能だ。このような犯罪者に対抗する側は、わざわざ会議に参加してレポートを出して、わずかな敵の情報を共有するだけだ。十分なデータを蓄積し、適切な情報を得た人材と機器を確保するまでは、半分のピースでチェスをせざるを得ない。」

サイバー空間で国境がなくなった現在では各国の協力体制が不可欠です。政府や諜報機関だけでなく、自宅でコンピューターやスマートフォンを利用しているユーザーも例外ではありません。

サイバー攻撃では、攻撃対象はほぼ無制限です。核の時代に入ってから軍縮が推進されるまで 20 年から 30 年ほどかかりましたが、サイバー空間において国際的な法体系が整備されるまでに同程度の時間が必要になるでしょう。

Accenture のグローバル マネージング ディレクターで、グローバル セキュリティの実践を推進する Alastair MacWillson 氏は「我々は未知の領域に足を踏み入れている。サイバー環境の変化は非常に激しい。コンテンツだけでなく、次々と新たな使い方が出てくる。ビジネス モデルも多岐にわたる。実際に何が起きていて、我々が何をすべきか誰も把握していない」と述べています。

犯罪者を誰が裁くか明確でないこともあると、カナダの専門家である Rafal Rohozinski 氏は指摘しています。同氏は「サイバー攻撃はより段階的に定義する必要がある。この定義がなければ普遍的な議論はできないし、過失についても様々な定義を許すことになる。担当の管轄区域が分かれば良いようにしたいものだ」と述べています。

信頼は定義の難しい概念です。インターネットは信頼に基づいて構築されていますが、これが弱点でもあります。良く知られているように、インターネットは性善説に基づいて構築されたため、保護対策は殆ど実装されていませんでした。初期のハッカーは、自らの技術力を試すためにシステムを攻撃していましたが、今では金もうけや知的財産、軍事的な機密事項、企業秘密を盗み出すことが目的になっています。しかし、信頼は現在でも有効な言葉です。これを「保証」という人もいます。

毎日使用しているシステムを信頼するには、どのような対策を講じるべきでしょうか。ソフトウェア ベンダーが製品に対する責任を負うのか、インターネット サービス プロバイダーの責任になるのか。IT チェーン全体のコンポーネントを信頼するにはどうすべきか。クラウド コンピューティングによって管轄区域が判断できない場合はないのか。サイバー空間の責任者を設定するために国際的な協定が必要か。このような問題を解決するため、世界の優秀な頭脳が努力しています。すべての問題で見解が一致することはないでしょうが、大半の研究者は、世界中に普及しているインターネットの問題は一国で解決できるものではなく、国際的な問題であることを認識しています。

セクション II. サイバー空間の変革：新しい脅威と変化する倫理観

考え方を変える時期に来ているのかもしれません。私たちが以前よりも脆弱であることに異を唱える人は殆どいないでしょう。インターネットに接続するシステム数は急増し、技術への依存度は日増しに強くなっています。インターネットの父と言われる Vint Cerf 氏は昨年、現状のシステムを一旦止めて規制の整備された環境で最初からやり直すべきだと提言しましたが、これは現時的ではないというのが大方の見方です。

英国で情報セキュリティを教える Christopher Richardson 氏は「私たちは本当に無秩序な情報革命の中にいるのだろうか」と疑問を投げかけています。一部の見方に反し、「誇張が過ぎるのではないか。私たちは事実を知らされていない」と考えています。同氏は、セキュリティに対する関心を煽るため、政府や民間企業で発生した事件について正しい情報が与えられていないのでないかと見ています。毎年多くの受講生にサイバー攻撃の被害を受けたかどうか調査しても、実際に被害を受けたものは殆どいない、と同氏は述べています。

誇張かどうかはともかく、サイバー犯罪が増えれば、インターネットの利用に対して法規制や規則、制限が増えるのはやむを得ないでしょう。40 年前は紳士的なユーザーが利用する場所だったかもしれませんが、今ではサイバー犯罪者が簡単に金を稼げる天国と化しています。

McAfee の Phyllis Schneck は次のように述べています。「インターネットは誰でも利用でき、何でもどこにでも情報を送信できる。不正なデータのルーティング、配信、実行に対する制限を強化して犯罪者の利点を破壊し、脅威を阻止しなければならない。プールに水質維持のフィルターがあるように、ネットワークやコンピューターにも情報フィルターを装備し、攻撃者が標的を探せないようにする必要がある。」

米ロードアイランド州ニューポート市にある米国海軍大学の Richard Crowell 教授らは、新しいリスクを理解するにはサイバー脅威が存在する新たな領域について冷静に分析する必要があると考えています。同教授は「我々は両大戦間と同じ状況にある。第一次大戦のガリポリの戦いで連合国は大敗を喫し、水陸両面での戦闘を二度と行ってはならないという教訓を得た。この戦いでは海から陸に戦場を移すべきだった。1930 年代から 40 年代にかけてはこの教えが徹底された。現在また当時と同じ状況だ」と述べています。

考え方を変えるべきか

今回インタビューを行った専門家はみな、サイバー空間の急激な変化はシステムの成熟を意味しないと考えています。CSIS の専門家である James Lewis 氏は「これらの変化はまだ終わっていない。支配領域の拡大やガバナンスの変化も起きるだろう。インターネットに対する自由なアプローチは見直しが必要かもしれない」と述べています。

石油メジャーの BP でセキュリティ情報最高責任者を務める John Meakin 氏は「我々のような組織の場合、新しい技術が出現すればセキュリティモデルの変更が必要になる。以前のネットワーク セキュリティの古いモデルは、クローズであれば安全、という考え方だった。しかし、完全に管理できないインターネットでは、どのように安全性を維持すればよいのか。データは管理できても、インターネットは完全に制御できない。

データの入れ物が手元にない以上、何が起きてもおかしくはない。考え方を変える必要がある」と述べています。

保証とは、保護対策が信頼できるかどうかを判断するための基準と測定方法を確立することです。Luna 氏は「たとえば、利用しているインターネット サービス プロバイダー (ISP) のセキュリティ対策がマルウェアなどのサイバー脅威を完全に阻止する保証はあるのか。ISP が適切な保証レベルを提供していることを確認する方法があるのか」と疑問を呈しています。

スマートフォンによる新たな問題

スマートフォンやクラウド コンピューティングの普及により、接続性と領域に関連する新たな問題が発生しています。これらの問題を解決するには、新しい規制や考え方が必要になります。

カナダの専門家である Rafal Rohozinski 氏は「モバイルの普及で状況が変わった。今後 20 億のユーザーがモバイル端末からインターネットに接続するだろう。また、モバイル端末の多くは発展途上国で使用されている。この状況はフラッシュ・モブのように社会的な影響をもたらす可能性がある。サイバー空間で行われる紛争が多くなり、サイバー空間の規制を求める声が増えている。全体としてのインターネット ガバナンスにはサイバー空間を規制する複数の国家が関係する」と述べています。

クラウド コンピューティング : ネットワークとコンテンツの分離における課題

データ保管の外部委託は 40 年も前から行われています。クラウド コンピューティングの違いはストレージが地理的に分散している点です。クラウド コンピューティングの問題点としては、処理能力と接続コスト、ネットの中立性に関連する問題がありますが、Luna 氏はこの新しいストレージ施設がセキュリティの問題と司法権の問題を引き起こす可能性があると述べ、「問題が起きた場合、どこに訴えればよいのか」と疑問を呈しています。

「クラウド コンピューティングは、これまでにない方法でネットワークとコンテンツを分離している。現行の著作権法と国内法では対処できない」と Rohozinski 氏は指摘しています。

たとえば、Google の場合、クラウド ストレージの 3 分の 1 がカナダにあります。Rohozinski は、この情報には米国の法律が適用されるのか、カナダの法律が適用されるのか分からないと指摘しています。法的責任はどうなるのか、データ保存期間やプライバシーに関する法律が異なる場合はどうなるのか、データの保存場所が移動した場合にはどうなるのか、最終的な管轄区域は誰が判断するのか、など法律家にとって新たな問題が発生しています。

セクション III. サイバー防衛戦略：最も重要な課題と成功の条件

では、サイバー空間の防衛戦略で最も重要な課題は何でしょうか。インタビューの結果、次の 20 のテーマが明らかになりました。

1. 攻撃態勢の確立
2. 国の攻撃能力の評価
3. 統合が進むグローバル システムの保護
4. SCADA システムの保護対策
5. セキュリティとプライバシー
6. ネットの中立性
7. 国際的なルールの確立
8. より強固なサイバー アーキテクチャの構築
9. 最も脆弱な国々への対処
10. インターネット サプライチェーンの保護
11. 問題に関する認識を高める
12. 全体的なアプローチ
13. 技術者と組織トップと対話を増やす
14. 政府の役割の定義
15. 国際レベルでの情報共有
16. サイバー セキュリティに対する考え方を変える
17. 一般市民の認識を高める
18. 秘密主義を緩和する
19. 各国の刑法と法律の調和を図る
20. サイバー空間における先制攻撃の定義

セクション IV. サイバー空間を統治する規則と規制に関する探求

米国、EU、アジアの一部の諸国では、サイバー攻撃の急増に伴い、政府関係者がサイバー攻撃の重大性を認識し、攻撃による影響を調査するようになりました。

BP の情報セキュリティ最高責任者の John Meakin 氏は「コンピューター セキュリティの分野に 23 年従事しているが、政府関係者がこの問題を重視し始めたのは 2、3 年前のことだ」と述べています。

Accenture のグローバル マネージング パートナーの Alastair MacWillson 氏は「初期段階からセキュリティと制御が考慮されていたらインターネットはここまで発展しなかっただろう。インターネットの強みは規制のないことであり、規制は誰も望まない」と述べています。

コーポレート ガバナンスを強化すれば多くの問題が解決するかもしれません。英国の DCCIS (Defence College of Communications and Information Systems) で講師を務める Christopher Richardson 氏は、多くの企業が必要のないデータを抱えているため、厳しい内部監査を実施してこの状況を改善すべきだと考えています。

他に状況を改善する方法はあるでしょうか。まず、実践的で低コストのベスト プラクティスを市場で構築し、迅速に実装するのがよい方法でしょう。EU では、ENISA (European Network and Information Security Agency) のミッションに、この種の情報を 27 の加盟国間で共有することを定義しています。

サイバー空間での規範と共通のセキュリティ基準

ENISA では標準規格の定義という困難な作業も行っています。「EU の加盟国は国ごとに状況が異なる。まず各国の状況を把握し、共通の基準を定義しなければならない」と技術部門の責任者である Steve Purser 氏は述べています。

このような標準を遵守するにはどうしたらよいでしょうか。標準を強制的に実施するだけでなく、市場に規制させる方法もあります。多くの企業は ISO 9000 を遵守していますが、この認定マークがあれば企業の信頼性は向上します。セキュリティ市場でも同様なことが可能でしょう。

グローバル化の問題点

国家の主権は一つだけですが、サイバー空間では共同責任にならざるを得ません。世界の多くの国が自国で CERT を設立しているか、その準備を進めています。また、大企業や公的機関も、緊急事態に対処し、コンピューター セキュリティに関する情報を提供するために独自の緊急対策チームを組織しています。このような組織の多くが CERT のグローバル ネットワークに参加しています。

Purser 氏は「ボットネットを閉鎖する場合、ボットネットが自国内に限定されていれば幸運だが、実際には国際的な協力が必要になる。国境内だけのセキュリティは意味をなさない。すべてがグローバルに接続している。国際的な協力関係を構築できなければ、ヨーロッパのアプローチも効果はない」と述べています。

しかし、法律の制定方法については様々な意見があります。インターネットの変化が速いため、法規制が追いつかないという主張や、法規制で創造性が損なわれるという意見がある一方、コンテンツに対する規制を強化したいと考えている国もあります。サイバー セキュリティやサイバー プライバシーに対してグローバルな規制を行うことは現実的ではないのでしょうか。

現行の法規制の適用

専門家の多くは、現行の法規制を適用可能と考えているのでしょうか。一部の専門家はそのように考えています。刑法を一から作り直し、新しい法体系を整備するよりも、現行法の適用範囲を拡張した方が簡単かもしれません。

BP の John Meakin 氏は「サイバー犯罪者に対して有効な対策を講じるために、現行の刑法の多くは適用できないだろう。警察、検察、裁判官がコンピューター システムの仕組みを知らないことが問題だ」と述べています。

ジュネーブ条約などの国際協定を見ると、戦争に関わる現行法もサイバー空間に適用できるかもしれません。サイバー セキュリティの専門家である Tim Scully 氏は「サイバー空間を 5 つ目の戦場とする見方もある。この点を考えると、法律家が現行の法律を調査すれば、国際的なレベルでサイバー空間に適用できる法律が見つかるかもしれない」と述べています。

国際的な機構の欠如

当面の間、情報収集を含む各国のサイバー防衛を調整する国際的な機構は生まれないでしょう。カナダの専門家である Rafal Rohozinski 氏によると、調整と情報共有が最も進んでいるのは、カナダ、米国、英国、オーストラリア、ニュージーランドの 5 か国間の協力関係です。「NATO、欧州評議会、集団安全保障条約機構 (CSTO) などの協力関係は希薄だ」と同氏は述べています。

国際協定は実現不可能か

2010 年、国連の国際電気通信連合 (ITU) の会議がメキシコで開催される前に、ITU の Hamadoun Touré 事務総局長がサイバー空間での平和条約の必要性について言及しました。共通ルールの構築については賛同を得たものの、世界的な組織の構築には大きな障壁があります。

米国の法律家の Stewart Baker 氏などのタカ派の人物は、国際協定を時間の無駄だと考えています。最悪の場合、西諸国側は、調印国が一方的に協定を放棄した場合も、ある程度、保護されるかもしれないと誤解をする可能性があります。

サイバー セキュリティを安全な国々のネットワークとすると、セキュリティを担保できない国々を排除するような大まかな合意を考慮する必要があると Baker 氏は指摘しています。「この問題は銀行取引で経験済みだ。資金洗浄を行う犯罪組織の多くは資金洗浄を取り締まる法律が施行されていない国を経由しようとした。グローバルな金融システムが成長するにつれ、このような国は効果的に排除され、資金を隠匿できる場所が減少した。同じようなメカニズムで、調査依頼に応答しない国を隔離することも可能だろう」と同氏は述べています。

平和条約に代わる現実的な方策 : サイバー空間の信頼基準

CSIS の James Lewis 氏、University of Bath で情報セキュリティを担当する Paul Cornish 教授、国連軍縮研究所の Theresa Hitchens 所長など、多くの学者がサイバー空間の信頼基準の設計に取り組んでいます。Lewis 氏は「条約は機能しない。検証事項が多すぎる。コンプライアンスや定義の問題も多い」と述べています。

サイバー空間の信頼基準には、期待される国家行動の基準に同意することも含まれると、Lewis 氏は述べています。また、「特に、軍事的な目的でサイバー攻撃を行う場合の原則については透明性が求められる。大半の国はこのような方針を定めているが、議論はされていない」とも述べています。

サイバー空間の支配権を巡る争い

インターネットは組織の継ぎ接ぎで運用されている厄介な存在です。誰が責任を持つのか国によって考え方が異なります。政府による規制を厳しくした方がいいのでしょうか。あるいは、政府の規制は是が非でも回避すべきでしょうか。政府に何らかの対策を求めるべきなのか。我々は状況の変化にどのように対応すればよいのでしょうか。

毎年、国連のインターネット ガバナンス フォーラム (IGF) が開催され、利害関係者が参加して活発な議論を展開しています。様々な利害が対立する中で、インド、ブラジル、南アフリカがインターネットを管理する世界的な組織の設立を求めました。中国とロシアは、両国が提唱している情報セキュリティ実施の国際規約の採択を国連総会で求めました。この規約では、政府に様々な権限を認め、コンテンツに対する制限を強化できるようにしています。これらの国は、国際電気通信連合 (ITU) などの国連機関に監督権限を持たせようとしていますが、米国や西側諸国はこの提案に強く反対しています。

EU の外交機関である欧州対外行動庁の Frank Asbeck 氏は、国連は討論の場であって決定機関としては適切ではない、と指摘しています。「今は、実際的で社会的に容認される解決策を迅速に行うことが求められている。結論が出るまでに何十年もかかる交渉を行っている余裕はない」と同氏は述べています。

リソース管理

より事態を複雑にしているのは、西側諸国がインターネット アドレス システムである ICANN (Internet Corporation for Assigned Names and Numbers) に対して一定の影響力を維持したいと考えている点です。ICANN はインターネットにおいて世界的な影響を及ぼす数少ない組織の一つです。ドメイン名の管理を ITU が行うべきだと考える国もあります。ITU にも複数の利害関係者が関係していますが、多くのインターネット コミュニティはこの組織に対する政府の影響を懸念しています。

米国の民間団体である ICANN にはネット ユーザー、民間企業、政府機関が参加し、IP アドレスの管理、アドレスの割り振り、ドメイン名の登録と管理を行っています。

イタリア国家研究委員会の Stefano Trumpy 氏は「ICANN と ITU の問題は複数の利害関係者が関与していることだ。この点を多くの人が問題だと考えている。2011 年 9 月にナイロビで開催された IGF で、インド、ブラジル、南アフリカは国連で臨時委員会を開催し、標準規格を含むインターネット関連の公共政策を議論するべきだと主張した。しかし、これは難題だ。標準規格は民間の組織が策定している。政府がコントロールするべきものではない」と述べています。

標準化

サイバー セキュリティのガバナンスで次に問題になるのが技術な標準化です。この問題は現在、IETF (Internet Engineering Task Force) で ITU と業界が協力して取り組んでいます。奈良先端科学技術大学院大学教授で、元内閣官房情報セキュリティ対策推進室情報セキュリティ補佐官の山口英氏は「オープンなプロセスが必要だ。民間企業や公共企業が自由に参加できるようにすべきだ」と述べています。

捜査当局

3 つ目の要素は捜査当局です。国際刑事警察機構は強力な法的枠組みを構築し、他の国際的な枠組みも準備しています。この枠組みは、サイバー犯罪に対する法的枠組みがない国で発生したサイバー犯罪に対処するためのものです。

情報共有

4 つ目の要素は情報共有です。グローバルな情報共有は国際的な問題ですが、インターネットを健全に運営するには重要な要素です。FIRST という国際的なコンピューター緊急事態対策チーム (CERT) のフォーラムは、非常に効果的に機能していますが、まだ十分とは言えません。グローバルな情報共有を推進するにはより一層の連携が必要と山口氏は指摘しています。

ITU は、マレーシアでの IMPACT (電気通信コミュニティの早期警戒システム) の設立に資金援助をしましたが、Accenture の Alastair MacWillson 氏は「米国に問題を通知するには非常に優れているが、電気通信業界は何をすれば良いのか分からない」と述べています。

国家による攻撃の危険性が情報共有の障害になることも少なくありません。各地域でも特別な会議が開催されています。たとえば、アジアでは、ASEAN+6 が ARF (ASEAN Regional Forum) を開催し、朝鮮半島の緊張緩和のための協議を重ねています。

「一部の国家間では基本的な信頼関係が欠如している。緊張緩和のためには率直な話し合いが必要だ。産業界は期待が持てる。多くの企業がグローバルに事業を展開しているため、情報共有に関して前向きな姿勢が見られる。このようなグローバル企業がきっかけとなり、各国政府が話し合う機会が増えることを期待する」と山口氏は述べています。

スマートフォンに対する ITU の対応

ジュネーブを拠点にする国際電気通信連合 (ITU) の Hamadoun Touré 事務総局長は「固定電話の利用者が 10 億人に達するまでに 125 年かかったが、携帯電話はわずか 11 年で同じ数字に達した」と述べています。同氏が指摘しているように、光ファイバー ネットワークの登場で私たちの世界は想像よりもはるかに速く接続されるようになりました。2010 年、この急速な成長に伴う問題を解決するために Broadband Commission が設立されました。Touré 事務総局長は、ミレニアム開発目標の達成に高速で大容量のインターネットが不可欠であることを強調し、「ブロードバンドは医療、教育、エネルギー効率を改善している。これは世界的な現象であり、その安全性を維持するには、世界的な協力の枠組みを構築して対応する必要がある」と述べています。

セクション V. サイバー セキュリティ間に存在する壁の解体

サイバー空間を統治する有効な国際ルールを策定するには、業界、国、世代の間に存在する壁を取り除く必要があります。サイバー空間には蜂の巣のように多くの壁が存在します。世代間の壁や国家間の壁だけではなく、専門分野の間にも壁が存在します。問題は、これらの壁が硬い地盤の上にあるわけではなく、殆ど意味がないという点です。グローバルで抜け穴の多いサイバー空間で法的な枠組みを構築するには、国や見解を超えて専門家が協力する必要があります。

サイバー セキュリティの提唱者であるTim Scully氏は「政府の対応は一般的に遅い。しかし、サイバー セキュリティに対しては迅速な対応が求められる。サイバー セキュリティは軍事的な問題にとどまらず、社会的な問題でもある。国家のセキュリティについて語る場合、国家の利益に沿って考える必要がある」と述べています。また、他の分野以上に政府、業界、学会のトップが信頼関係を構築し、協力していく必要性を強く主張しています。この方向に沿った流れとして、2012 年にオーストラリアで初めてサイバー空間白書が発表される予定です。

世代間の隔たり

最も原始的な障壁は世代間の壁です。多くの専門家は、自分の子供たちの世代とインターネット プライバシーに対する考え方が全く違うと感じています。特に、ソーシャル ネットワークに対する見方は大きく異なります。

「子供たちの世代はコンピューターを怖がらないし、プライバシーも気にしない」と英国のサイバー セキュリティ専門家の Peter Sommer 氏は述べています。2011 年にソニーで 7,700 万人分の顧客情報が流出したときに、同社は PlayStation ネットワークを 2 週間閉鎖しましたが、若い世代のユーザーはプライバシー侵害ではなくネットワークの閉鎖に怒っていました。

業界関係者間での信頼関係の改善

民間企業の多くは自社の情報が政府や競合他社に悪用されることを恐れています。世界各地で信頼関係を構築する試みが行われていますが、これは競争相手と協力することになることも少なくありません。詐欺事件の増加に伴い、米国の金融機関は金融システムに対する攻撃手口やサイバー脅威に関する情報を共有するため FS-ISAC (Financial Services Information Sharing and Analysis Center) を設立しました。規模の点では及ばないものの (238 社)、ベルギー金融業界協会 (Febelfin) もフリーの専門家と契約して同様の仕事を行っています。

競争相手との協力

PwC のセキュリティ責任者である William Beer 氏は、専門グループ間のコミュニケーションを促進するにはまとめ役が必要だと考えています。「行動的な人物と仕事をすると、軍関係者やビジネスマンの考え方を把握し、情報共有の仕方を考えることができる。我々は長い間、非常に限られたスキルしか持たないセキュリティ担当者に依存してきた。業界でも専門的な話しか行われていなかった」と同氏は述べています。

サイバー犯罪とサイバー セキュリティ

犯罪は撲滅しなければなりません。境界のない世界では、サイバー犯罪とサイバー セキュリティの区別は意味がないかもしれません。欧州警察組織でサイバー犯罪の戦略的アドバイザーを務める Victoria Baines 氏は、民間企業、政府機関、学術機関を巻き込み、地域の脅威や世界的な脅威に協力して対応することが重要だと述べています。

同氏は、2009 年に学術機関、軍、警察、民間企業、第三国の協力でスペインの Mariposa ボットネットの解体に成功した例を挙げ、「欧州警察組織と国際刑事警察機構に欠けていたものはサイバー犯罪に対する国際的な協力関係だ。犯罪サイトと異なり、サイバー犯罪は国内の捜査機関だけでは摘発できない」と述べています。

グローバルな情報共有に向けて

西側と東側の国々でサイバー脅威に関する情報を共有するための一つのステップとして、国連機関の国際電気通信連合 (ITU) の部門で、マレーシアに設立された Impact の例が挙げられます。

Mohd Noor Amin 議長は、複数の利害関係者が関わるプラットフォーム構築の積極的な提唱者です。同議長は「最終的なユーザーは責任のある行動を行うように教育する必要がある。民間企業と政府は、

資金不足であっても、セキュリティに対する投資を行うべきだ」と述べています。Impact の参加国は 137 か国ほどですが、英国や米国などの非参加国にも積極的な取り組みが見られます。「これらの国々も他の国々と接続していることは認識している。すべての国が参加するのも時間の問題だろう」と Amin 議長は述べています。

セクション VI. 民間企業が直面するプライバシーの問題

サイバー空間に投資する企業にとって秘密主義は非常に重要な要素なります。しかし、サイバー セキュリティの面では、これが様々な問題と脅威を招く原因となります。多くの人が認めるように、サイバー セキュリティのプラットフォームで官民の協力が最も成功しているのはオランダでしょう。Accenture の Alastair MacWillson 氏は「問題について議論し、自発的であろうが義務的であろうが、何らかの形でアクションを起こすことは素晴らしい方法だ。これは世界的に行われるべきだ」と述べています。

米国にも良い事例があります。しかし、世界的にみると、官民の協力関係は遅々として進んでいません。フランスなど、官民の緊密な関係について疑念を持つ国もあります。

民間企業に情報共有が推奨される理由は何でしょうか。民間企業は営利目的でサイバー空間を利用しています。BP のサイバー セキュリティ責任者である John Meakin 氏は、リスクを取らなければ利益は得られない、と指摘しています。

民間企業もサイバー攻撃に対して貴重な経験をしています。問題は、企業がサイバー攻撃について情報を公開したがらないという点です。各企業でデータ プライバシーに関する規則が定められていますが、競合他社や顧客に脆弱性を開示したくはないでしょう。

すべての関係者に意味のある規則を設定することが重要です。学者やセキュリティ製品の販売者は「最適なセキュリティ対策と保証レベルを提供するので安心してデータを任せてほしい」と主張し、政府関係者は「より安全な環境にするために規則や規制を考えよう」と呼びかけます。規制はすぐに時代遅れになってしまうかもしれませんが、サイバー セキュリティの提唱者である Tim Scully 氏は「多くの国でシートベルトの着用を義務付けているが、これによって死亡事故がなくなるわけではない。しかし、多くの人命が救われていることは確かだ」と述べています。

Accenture の Alastair MacWillson 氏は「規制や標準を策定している人物はビジネス戦略やニーズに詳しいわけではない。政府は、規制の草案作りの段階で民間企業を参画させ、意見を求めるべきだ。オランダの事例が良いお手本だ」と述べています。

大半の政府は、知識の共有を促進するために様々なことができることを理解しています。また、攻撃の手口や手法を理解するためには企業秘密に触れる場合があることも認識しています。「ハッキングされた組織やデータを消失した組織に対する罰則はなくすべきだ。このような罰則があれば、攻撃の発生を申告しなくなる。情報共有の推進には邪魔になるだけだ」と MacWillson 氏は述べています。

ソフトウェア ベンダーからサービス プロバイダーへの責任転嫁：誰が何に対して責任を負うのか。100%完全なセキュリティは実現不可能です。システムがサイバー攻撃を受ける原因には、不適切なセキュリティ ポリシーやユーザーの誤使用など、様々な要因があります。MacWillson 氏は「更新を怠っていても、多くのユーザーはすぐにソフトウェア ベンダーに責任を求める。元凶を突き止めるにも、関係者が多すぎる」と述べています。

セクション VII. サイバー空間が安全でない場合の負担

サイバー セキュリティに多大な費用がかかるようでは問題です。では、企業や政府が費用の大半を負担すべきなのでしょうか。EU の新しい外交機関である欧州対外行動庁の Frank Asbeck 氏は、経済的な危機を回避するにはインターネットの安全性が鍵になると見ています。「サイバー空間とインターネットが重要な役割を果たしている経済領域がある。サイバー セキュリティへの投資はサイバー空間の信頼性を高めることを意味する。金融、情報産業、エネルギー利用の最適化やスマート グリッドのように、情報技術の利用で他の分野の資源が節約できる」と同氏は述べています。
計量経済学モデルで個々のサイバー攻撃のコストを計算しても、結果はすぐに出ないでしょう。情報収集や統計の対象にする人物が多岐にわたり、企業もこの種の情報を公開しようとしません。

セクション VIII. 一般市民：自由と保護の問題

サイバー セキュリティに関する厄介な問題に、セキュリティとプライバシーの関係があります。この 2 つは相反するものでしょうか。それとも共存が可能でしょうか。Accenture グローバルセキュリティ部門マネージング ディレクターの Alastair MacWillson 氏は次のように述べています。「現時点では非常に難しい問題だ。セキュリティに対する考え方は年齢によって異なる。若いユーザーほどプライバシーに対する意識が低く、完全なアクセスを求める。プライバシーに対する意識は国によっても異なる。」

たとえば、中国やロシアは、宣伝活動や反政府的な活動もサイバー脅威とみなし、コンテンツの検閲にも肯定的です。アラブの春では、エジプト政府がインターネットを切断すると民衆を脅しました。ヨーロッパでは、共産主義を経験した国の方がプライバシーに対する問題意識が強いようです。ドイツの場合には、これにナチスの記憶も加わります。しかし、国内では様々な意見が存在しています。

インターネットの責任は個人のユーザーではなく大企業に

Gaycken 氏は、ユーザーの平均的な意識を高めるのがシステムを保護する効果的な方法だと考えています。「ユーザーは犯罪者の手口をもっと知るべきだ。セキュリティに対する全般的な意識を向上させる必要がある」と述べています。また、インターネットから切り離してクローズド システム モデルを利用すれば、サービス拒否攻撃や他の洗練された攻撃からも守ることができるとし、「ホストのセキュリティでネットワークを制御すべきでない」と述べています。

フランスでサイバー セキュリティに関するコンサルタントを行う Devoteam の Olivier Caleff 氏は、サイバー脅威に打ち勝つには教育と研修が重要だと考えています。「解決できるのは 80% だろう。多くのユーザーが携帯端末を使用し、読んだことをすべて信じてしまう。どんなにくだらないメッセージでも例外ではない」と述べています。

非常に多くのユーザーがインターネット上に個人情報を無警戒に投稿しています。実際には非常にオープンなセッションにいても、非常に限られたユーザー グループにいると思うかもしれません。彼らは自分のデータが他の会社に送信される可能性があることに気付いていません。Caleff 氏も、学校で教育を行うべきであり、規模の大小を問わず、どの企業も従業員の教育を行うべきだと考えています。

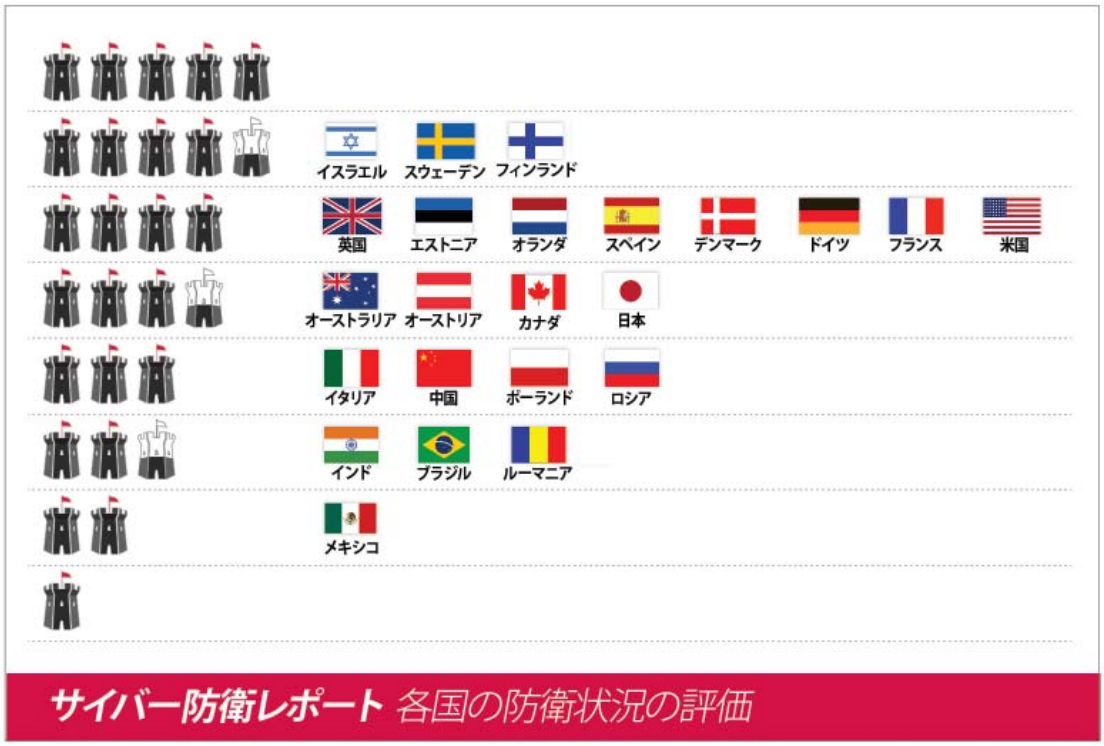
サイバー セキュリティのスキル格差

教育という点でみると、多くの国でサイバー セキュリティに従事する人材を必要としています。全国的な競争で優秀な人材を採用している Cyber Security Challenge UK の Judy Baker 氏は人材不足を指摘しています。米国でも同じ採用方法が行われています。戦略・国際問題研究所 (CSIS) はオバマ米大統領に対し、1 万から 1 万 5 千人以上のサイバー セキュリティの専門家が必要だと助言し、競争を通じて優秀な人材を確保しています。Baker 氏は、考えれば方法はいくらでもある、と述べています。

米国の調査教育機関である SANS Institute の調査によると、企業の 90% はサイバー セキュリティに必要な要員を確保していません。これらの企業では、技術的な分野から戦略的な分野まで 8 種類の職種を募集しています。

国別の評価表

各国のサイバー防衛状況を評価する方法は、Robert Lentz 氏 (Cyber Security Strategies 代表、元国防次官補代理サイバー情報保障担当) が作成したモデルを採用しています。同氏のサイバー セキュリティ成熟度モデルは攻撃からの耐性を表すもので、高度なサイバー攻撃を受けた場合でも効果的な運営の持続が必要な政府機関や企業の究極の目標となります。このモデルでは、経済的および国家的な危機を回避するために、ポリシー、プロセス、改善、人材、技術を統合する能力を測ることができます。



出典: SDA サイバー防衛レポート (McAfee の支援により作成)。このレポートは、www.mcafee.com/japan/ からダウンロードできます。

日本

日本には CERT(JPCERT/CC) があり、非公式の CERT コミュニティに参加しています。日本のサイバー セキュリティ センターは、内閣官房に設置された内閣官房情報セキュリティセンターです。アジア太平洋地域において、JPCERT/CC は APCERT (Asia Pacific Computer Emergency Response Team) で中心的な役割を果たしています。また、FIRST (Forum of Incident Response and Security Teams) にも参加しています。

評価 : 3.5

2011 年 3 月 11 日の東日本大震災からの復興が最重要課題となっていますが、サイバー セキュリティは検討課題の上位に置かれています。2011 年の夏に三菱重工業 (MHI) の情報システムがハッキングされました。防衛省の納入業者が攻撃を受けたことで、政府は緊急課題としてサイバー セキュリティの強化に取り組み、現在、重要インフラと主要産業に対する数多くの保護対策が実行されています。

現在でも災害復興に多くの費用が必要とされています。奈良先端科学技術大学院大学教授で、元内閣官房情報セキュリティ対策推進室情報セキュリティ補佐官の山口英氏は「現在は自然災害対策に多くの資金が必要とされている。防衛予算は削減され、サイバー セキュリティも防衛力強化の 5 か年計画でも最優先事項から外れている」と述べています。また、法的には、自衛隊以外の情報システムの保護は自衛隊の任務ではありません。

「世論の喚起は、サイバー セキュリティ政策を後押しするまでには至っていない。国民はサイバー犯罪取り締まりと警察庁の捜査能力の強化に期待している。防衛省のサイバー防衛計画に対する関心は低い」と山口氏は述べています。

日本はネット普及率の高い国です。家庭では 70% が、事務所では 95% 以上がインターネットに接続し、携帯電話世帯普及率は 93% を超えました。2010 年の B2C 電子商取引の市場規模は約 8 兆円 (1,000 億ドル) でした。ソニー、パナソニック、トヨタ、ホンダ、三菱重工業などのグローバル企業を狙った産業スパイが重大な問題となっています。

サイバー防衛における官民パートナーシップ (PPP) の枠組みは、サイバー セキュリティの基本計画の一部として 2006 年に構築され、これまでに 10 の重要インフラの整備が行われています。「日本の PPP は非常に良好だ。情報交換には改善の余地があるが、政府は計画を定期的に更新し、民間企業は積極的に参加して意見交換を行っている」と山口氏は述べています。

政府機関と業界の良好な協力関係により、インターネットの状態を改善するための様々な対策が講じられています。2006 年、ISP と政府機関の協力でマルウェアの駆除を促進するサイバークリーンセンター (CCC) が設立されました。それ以降、同センターはマルウェアに感染した PC の特定とウイルスの駆除を行っています。

日本では、サイバー防衛における自衛隊の位置付けについて活発な議論が行われています。この議論は米国で行われている議論と似ています。勿論、軍需産業を除いて、自衛隊が他の政府機関や民間企業と活動を共にすることはありません。「法体系の面でも、自衛隊の任務とその長期計画を定義する点でも、これは非常に難しい議論である」と山口氏は述べています。

この他にも、2013 年から 2015 年までの間に高度な ID システムを導入する計画についても議論が行われています。「国内外からサイバー攻撃を受ける恐れがある中で国民のプライバシーを保護するために何をすべきか」と山口氏は問題を提起しています。すべての住民にデジタル ID を発行する計画に対しては、活動家、専門家、政府関係者、議員を交えた国民的な議論が展開されています。

また、APT (Advanced Persistent Threat) や国家の支援を受けた攻撃に対する情報機関の役割についても議論が行われています。「第二次大戦以降、日本の情報機関は単独で活動を行ってきた。多くの政府関係者は他の政府機関との連携が必要ではないかと感じているが、これらの機関の協力関係は円滑に機能している。サイバー セキュリティの調査予算も毎年増加している」と同氏は述べています。

国際的には日米同盟が効力を発揮しています。日本と ASEAN 諸国は毎年情報セキュリティ会議を開催しています。また、日本、中国、韓国の 3 国間でのサイバー政策の調整を行っています。

引用 :

「現在は自然災害対策に多くの資金が必要とされている。防衛予算は削減され、サイバー セキュリティも防衛力強化の 5 か年計画でも最優先事項から外れている。」-- 山口英。奈良先端科学技術大学院大学教授、元内閣官房情報セキュリティ対策推進室情報セキュリティ補佐官。

「世論の喚起は、サイバー セキュリティ政策を後押しするまでには至っていない。国民はサイバー犯罪取り締まりと警察庁の捜査能力の強化に期待している。防衛省のサイバー防衛計画に対する関心は低い。」-- 山口英。奈良先端科学技術大学院大学教授、元内閣官房情報セキュリティ対策推進室情報セキュリティ補佐官。

「法体系の面でも、自衛隊の任務とその長期計画を定義する点でも、これは非常に難しい議論である。」-- 山口英。奈良先端科学技術大学院大学教授、元内閣官房情報セキュリティ対策推進室情報セキュリティ補佐官。

「国内外からサイバー攻撃を受ける恐れがある中で国民のプライバシーを保護するために何をすべきか。」-- 山口英。奈良先端科学技術大学院大学教授、元内閣官房情報セキュリティ対策推進室情報セキュリティ補佐官。

「第二次大戦以降、日本の情報機関は単独で活動を行ってきた。多くの政府関係者は他の政府機関との連携が必要ではないかと感じているが、これらの機関の協力関係は円滑に機能している。サイバー セキュリティの調査予算も毎年増加している。」-- 山口英。奈良先端科学技術大学院大学教授、元内閣官房情報セキュリティ対策推進室情報セキュリティ補佐官。

このセクションの寄稿者 (日本):

山口英氏。奈良先端科学技術大学院大学教授。元内閣官房情報セキュリティ対策推進室情報セキュリティ補佐官。

レポート全体の寄稿者 (日本):

井上淳氏。欧州連合日本政府代表部一等書記官、テレコム アタッシェ。

吉田丈夫氏。総務省情報流通行政局情報セキュリティ対策室係長。日本のサイバー防衛とサイバー セキュリティに関する助言と政策及び戦略立案を担当。

McAfee®
An Intel Company

マカフィー株式会社
www.mcafee.com/jp

●製品、サービスに関するお問い合わせは下記へ

東京本社　〒150-0043 東京都渋谷区道玄坂1-12-1 渋谷マークシティウエスト20F
TEL:03-5428-1100(代) FAX:03-5428-1480

西日本支店　〒530-0003 大阪府大阪市北区堂島2-2-2 近鉄堂島ビル18F
TEL:06-6344-1511(代) FAX:06-6344-1517

名古屋営業所　〒460-0002 愛知県名古屋市中区丸の内3-20-17 中外東京海上ビルディング3F
TEL:052-954-9551(代) FAX:052-954-9552

福岡営業所　〒810-0801 福岡県福岡市博多区中洲5-3-8 アクア博多5F
TEL:092-287-9674(代) FAX:092-287-9675

MCARPT-SDA-1204-MC