

通商産業省委託事業

「重要インフラにおけるセキュリティ対策の事例調査」
報告書（追補版）

平成 12 年 1 月

情報処理振興事業協会

目次

はじめに.....	2
大統領決定指令 63 - 重要インフラ防衛指令の位置づけ.....	3
推奨.....	3
米国政府は2003年までに、攻撃に対して不安定なあらゆる重要セクターないし重要インフラのために、関連民間セクターと調整して攻撃を警戒、牽制、阻止する計画の策定に当たる主幹機関を任命する。.....	3
結果.....	3
攻撃を警戒し、攻撃に対応する国家センターの早急な設立.....	4
結果.....	4
米国政府、民間セクターに対する情報共有分析センター（ISAC）設立の奨励.....	5
結果.....	5
インフラ防衛の達成法に関し、連邦政府が他国の模範となるための必要事項.....	5
結果.....	5
米国の重要システム防衛という共通目標を官民一体となって達成するための、民間セクターの自発的参加を要望.....	6
結果.....	6
個人の権利の保護および市場の力の活用。これは、米国の経済力を強化し、防衛するためであり、抑制するためではない。.....	6
結果.....	6
議会の全面的参加と関与を要望.....	7
結果.....	7

はじめに

「コンピュータやインターネット、その他の新しい情報技術は、ビジネス、研究開発、個人間のコミュニケーション、および教育や娯楽の実践において不可欠な要素である。しかしながら、社会のネット化につれ、犯罪も同様になった。コンピュータやインターネットの利用により助長された犯罪には、高齢者に対する詐欺、幼児ポルノの氾濫、クレジットカード番号の盗難、マネー・ロンダリング、保険詐欺、株式市場の不正操作、および銀行資金の窃盗などがある。ネット上の窃盗は、インターネットの広範な利用の可能性と電子商取引の人気の増大により儲かるビジネスになった」 - 1999年、FBI長官ルイス・フリーチ

全体的には、サイバー攻撃は1999年に増加した。法務省の現在の統計によると、サイバー犯罪は1997年以後43%増加した。CSI、FBI、SARC、CERT、SANS、その他の民間の調査研究所のほか、グローバル・インテグリティ・コーポレーション（GIC）が行った報告と分析は、コンピュータ関連の事件やサイバー攻撃の増加を裏付けている。

大統領決定指令 63 - 重要インフラ防衛指令 の位置づけ

大統領決定指令（PDD）63 により、PCCIP の推奨を利用して重要インフラ防衛の枠組みの概要が規定され、本枠組みに従って関連政府機関が任命された。同機関は、民間セクターと協力して 2005 年までに米国が指定された重要インフラに悪影響を与える恐れのあるあらゆる事象に確実に対応できるようにする。PDD63 は、2003 年までに、信頼性が高く、相互に連結された、安全な情報システム・インフラを構築し、2000 年までに政府のシステムの安全性を極めて高度に引き上げるという目標を設定している。

推奨

米国政府は 2003 年までに、攻撃に対して不安定なあらゆる重要セクターないし重要インフラのために、関連民間セクターと調整して攻撃を警戒、牽制、阻止する計画の策定に当たる主幹機関を任命する。

結果

インフラ	機関	計画の策定
電力システム	エネルギー省	未策定
ガス・石油製造	エネルギー省	未策定
銀行および金融	財務省	策定済み
通信	FCC	策定済み
運輸	運輸省	未策定
給水システム	商務省	未策定
緊急サービス	FEMA	未策定
公共サービスの継続性	CIAO	未策定

通信業界は、既にプロジェクト・チームを編成した。全米戦略通信行動委員会（NSTAC）が 10 年前に設立され、通信能力の維持という重大なニーズに取り組んでいる。通信は、国防総省が重要と判断した分野であり、この判断に基づき、通信を防衛し、国防に対する支援能力を強化するには何が必要かを特定するために、NSTAC が設立された。

金融サービス業界は、財務省と協力して 1998 年 10 月に共同会議を開催した。本会議では、民間業界が先導して計画を策定し、反応を探る、あるいは必然的で新しい法律や規制の問題に対応する必要があるという結論に達した。同省を防衛する計画は、1999 年 3 月に完成した。

そのほかの重要インフラに責任を有する省庁は調整が終了しておらず、PDD63 の要求に対する反応を示すに至っていない。同省庁の主要な問題は、CIP の要求に対応する必要性を民間業界に説明することである。

攻撃を警戒し、攻撃に対応する国家センターの早急な設立

結果

NIPC は、36 の政府諸機関の支援を得て設立された。NIPC は FBI 内に設立され、法執行力の特質という分野を担当した。NIPC は、いかなる機関がデータを供給しようとするすべての情報に対する権利を要求し、すべての情報を法執行力に分類して、ほとんどの諸機関が自らが支援する業界と同情報を共有できないようにした。PCCIP の責任者でさえ、FBI の特別許可がなければ同データを閲覧することはできなかった。

これは議論の紛糾を招き、その結果、ほとんどの情報がすべての関連諸機関と共有できなくなった。

2000 年 2 月時点で、6 機関を除くすべての機関が NIPC に対する支援を中止した。これは、役割と責任の衝突という直接的問題であった。

政府諸機関は、最新の情報を関連業界に提供するために非公式な同盟を結び、NIPC/FBI を経由せずに情報交換を行っている。この非公式な機構の主要参加機関は、シークレット・サービス、CIA、NSA および DIA である。

米国政府、民間セクターに対する情報共有分析センター（ISAC）設立の奨励

結果

財務省と金融サービス業界は 1999 年 10 月 1 日、グローバル・インテグリティ・コーポレーションの支援を得て最初の ISAC を設立した。グローバル・インテグリティは、同業界と緊密に協力して、金融サービス ISAC（FS/ISAC）起ち上げのための企画、立案、資金提供を行った。

FCC は、NSTAC を通して議論データベースを転換し、通信 ISAC として操作するようにしたが、ISP など通信に特化していないメンバーを容認、あるいは受け入れていない。

アメリカ鉄道協会（AAR）はグローバル・インテグリティと共に、運輸省と協力して運輸 ISAC を開発中である。しかしながら、これは初期段階で、AAR が会員の支援を得るまで実用化されないと思われる。

アメリカ情報技術協会（ITAA）は、ヤフー、エキサイト、Eベイなどが Distriuted Denial of Service（DDOS）の攻撃を受けたため、検討と会員のニーズの特定に着手したばかりである。DDOS の攻撃は、すべてのビジネスが直面し、対策を講じる必要がある弱点を指摘した。

インフラ防衛の達成法に関し、連邦政府が他国の模範となるための必要事項

結果

連邦政府は、大幅に遅れている。現在まで、政府内ではインフラ防衛のために、実際にインフラを変革する対策がほとんど講じられていない。最も積極的な省庁は、国防総省である。政府は、内部機構の改善のために巨額の資金（30 億ドル）を予算計上している。しかしながら、指導や調整がなく、必要な変革は何年も遅れることになるだろう。

直近の政府 CIP 会議では、様々な政府機関が先を競って基準を設定し、大幅な予算獲得に動いた。この継続的駆

け引きが、CIP の要求を満たす計画の策定に必要な行動を遅らせている。

米国の重要システム防衛という共通目標を官民一体となって達成するための、民間セクターの自発的参加を要望

結果

官民の提携は、金融および通信業界では進展しており、成果を上げている。しかしながら、これは他のセクターにはあてはまらない。当該セクターでは、CIP の必要性が未だ確立されておらず、また強力な支持者も特定されていない。

エネルギー省、運輸省、FEMA は、どの省庁が先になるかに関して「雌雄を決する」のは業界の協会にかかっているというアプローチを取った。

個人の権利の保護および市場の力の活用。これは、米国の経済力を強化し、防衛するためであり、抑制するためではない。

結果

この要求を掲げているの唯一のセクターは、金融サービス業界である。業界の代表は新たなプロセスに同意しており、要求事項は消費者の個人的期待を満たす必要がある。

医療業界の本問題への取り組みは新 HIPPA 法によって主導されているが、要求事項を満たすための対応は調整されていない。

議会の全面的参加と関与を要望

結果

1999年2月22日、ベネット上院議員はCIP会議において、「クリントン政権は、議会と協議する、あるいは議会に持ちかけるのに適した機会を得ていない」と述べた。

この発言がすべてを表している。議会は、CIPはどうあるべきで、変革を実施する最良の方法は何かということに関し、独自のヒアリングを始めている。