米国の「20 の重要なセキュリティ対策」及びオーストラリアの「35 の標的型サイバー侵入に対する軽減戦略」の概要

客員主任研究員　横山恭三

はじめに

ほぼ時を同じくして、2009 年と 2010 年に、米国とオーストラリアの政府機関から、優先度を付けたサイバー攻撃を阻止する対策リストが考案・公開された。

1 つは、米国・国家安全保障局（NSA）から公開された「The Critical Security Controls（20 の重要なセキュリティ対策）」であり、もう 1 つは、オーストラリア・国防信号局（Defense Australian Signals Directorate ：DSD）（現、オーストラリア電子通信局 Australian Signals Directorate ：ASD）から公開された「The Strategies to Mitigate Targeted Cyber Intrusions（35 の標的型サイバー侵入に対する軽減戦略）」である。

サイバーセキュリティに関して責任を有する国家安全保障局（NSA）と国防信号局（DSD）は、それぞれ独立して、どの攻撃が最も有効で、そして最も頻度が高いかについて回数を数え始めた。それから、彼らは、何故、最も頻度の高い攻撃が成功するのか、について分析した。他の調査と同じように、彼らは、大部分の成功した攻撃が、基本的な脆弱性を利用していることを発見した。そして、利用された脆弱性を攻撃の頻度と攻撃の成功率によってランク付けした。つまるところ、国家安全保障局（NSA）と国防信号局（DSD）の両者は、これらの脆弱性を軽減することが、攻撃者の成功を劇的に減少させることを発見したのである。

国防信号局（DSD）は、その分析結果を使って、35 項目の戦略リストを開発した。一方国家安全保障局（NSA）は、民間企業や政府機関と協力して、国防信号局（DSD）のリストに類似した 20 項目（米国の対策は複数の要素を持っているので、米国の方が戦略の数が少ない。）の対策リストを開発した。

国防信号局（DSD）と国家安全保障局（NSA）のアプローチの強さの 1 つは、測定結果と反復可能なデータに基づいているということである。もう 1 つの強さは、これらの対策が、標的型サイバー侵入の 3 つの段階の 1 つ以上で侵入を妨害することにより、他のリア

クティブなアプローチと比較して、既知又未知の攻撃を効果的に阻止することができるということである。3 番目の強さは、既存の対策と比較して、実際に経費を節約することができることを示唆していることである[1]。

いずれの対策リストも、その後のサイバー攻撃の変化や新しい対策などを取り込んで、改訂が行われ、「20 の重要なセキュリティ対策」は第 5 版（2014 年 2 月）に至り、一方、「35 の標的型サイバー侵入に対する軽減戦略」は 2014 年 2 月に第 2 版が公表されている。現在、「20 の重要なセキュリティ対策」は、米国のセキュリティ研究組織 SANS Institute が公開しており、「35 の標的型サイバー侵入に対する軽減戦略」はオーストラリア通信電子局（ASD）が公開している。

本稿は、これらの対策等の概要を紹介することを目的とするものである。

なお、「20 の重要なセキュリティ対策」について、米国 CIS（Center For Internet Security）のサイトにて、NRI セキュアテクノロジーズの翻訳による全訳版が、また、「35 の標的型サイバー侵入に対する軽減戦略」については当協会のサイトに抄訳版が公開されているので、詳細については、そちらを参照されたい。

１．「The Critical Security Controls（20 の重要なセキュリティ対策）」

（１）全般[2]

長年にわたり、多くのセキュリティ基準や要件のフレームワークが、システムと重要データへのリスクに対処するために開発されてきた。しかし、それらの努力のほとんどは、コンプライアンス事項に関する報告に多くの時間を費やすもので、常に進化する攻撃に対して実効的な対策になっているとは言い難いものであった。これが 2008 年に、国家安全保障局（NSA）によって重要な課題であると認識され、実際の脅威に対するセキュリティの向上に大きな影響力を与えるであろう対策（Controls）を順位付けするために、「攻撃とその防御対策」を結びつけるアプローチによる取組みを開始した。その後、SANS Institute のコーディネーションの下に、政府機関、民間企業から数多くの専門家が参加し、この取組みはコンソーシアムとして急速に成長していった。こうしてまとめられた推奨対策は、2013 年に、その管理と維持をグローバルな非営利団体である「Council on CyberSecurity（the Council）」に移管された。

「20 の重要なセキュリティ対策」は、情報セキュリティ対策と対策が優先付けされたベースラインを示したコンセンサスドキュメントである。APT などの高度な攻撃を含めて現在までに認識されている攻撃と、近い将来に発生が懸念される攻撃を阻む上で、有効であると考えられる技術的なセキュリティ対策に焦点をあてている。

各対策で定義されたアクションは、米国立標準技術研究所（NIST）の SP800-53 で総合的に定義されている事項のサブセットで、行政命令（Executive Order）13636 に対応した「サイバーセキュリティフレームワーク」を含む米国立標準技術研究所（NIST）の取組みに代わるものではない。あくまで「最初に最低限行わなければならない」ことに注力し、シンプルにすることを理念として作成されているものである。 上位の対策を実践することによって、情報セキュリティにかけるコストを大幅に削減でき、かつ効果が目に見えて改善されるであろう。

因みに、「20 の重要なセキュリティ対策」は「コンセンサス監査ガイドライン（Consensus Audit Guidelines：CAG）」とも称される。

(2)「20 の重要なセキュリティ対策（以下、CSC という。）」が必要な理由[3]

現在、いわゆるサイバー防御の発展段階において、我々は非常に興味深い時期を迎えている。大規模なデータ損失、知的財産の盗用、クレジットカードの悪用、個人情報の漏洩、プライバシー侵害、サービス拒否など、サイバースペースでは日常的な事象となった。

皮肉にも、防御する側として利用できるセキュリティツールやテクノロジー、セキュリティ標準、トレーニング／研修、認定資格、脆弱性データベース、ガイダンス、ベストプラクティス、セキュリティコントロールのカタログ、無数のセキュリティチェックリスト、ベンチマーク、推奨事項／勧告は膨大な数に上っている。直面する脅威の理解を促進する目的で、脅威情報フィード、レポート、ツール、アラートサービス、規格、脅威共有スキームなどが登場した。これらをすべてまとめるために、セキュリティ要件、リスク管理フレームワーク、コンプライアンス体制、規定が存在する。セキュリティ担当者を対象とした、インフラストラクチャの保護に関する情報があふれている。

このようなテクノロジー、情報、監督／監視などから、「選択肢が多すぎることによる混沌（Fog of More）」が生じた。競合するオプション、優先事項、意見、要求などは、企業を麻痺させ、重要な活動を妨げる可能性がある。脅威は進化し、攻撃側も防御側もますます高度化し、さらにユーザのモバイル化が進んでいる。データは複数の場所に分散されているが、その多くは組織のインフラの外部にある。クラウドへの依存度が高まるにつれ、データとア

プリケーションの分散がさらに進んでいる。組織ネットワークは、ユーザがアプリケーションとデータにアクセスするさまざまな場所の 1 つにすぎなくなっている。相互に接続した複雑な環境では、セキュリティを 1 つの独立した問題としてとらえることはできなくなっている。そこで、1 つのコミュニティとして（業界、セクター、提携、連合などにおいて）団結し、優先する処置を決定し、相互にサポートし、急速に変化する問題とそれに対する膨大な数の解決策に直面しながら、常に最新の知識とテクノロジーを維持するにはどうしたらよいか。取り組むべき最も重要な領域はどれか。企業はリスク管理プログラムの充実に向けてどのように第一歩を踏み出したらよいか。原則を怠ることなく新たに発生する特殊な脅威をすべて追跡し、原則事項のロードマップに沿って、評価と改善の方向性を得るにはどうしたらよいか。 最も効果的な防御対策とはどのようなものか。このような課題から CSC が開発され、現在推進されている。

当初は「Fog of More」を切り開く草の根活動として始まり、あらゆる企業がとるべき最も基本的かつ重要な処置を中心としていた。ここでは、知識とデータによって価値が決まる。この場合の価値とは、すなわち現在企業を悩ます攻撃を防止し、このような攻撃についてアラートを発し、対処できることである。CSC は、それを開発、採用、サポートする国際的なコミュニティ活動へと発展してきた。 コミュニティを構成する各個人と機関は以下の活動を行う。

▲攻撃と攻撃者に関する情報／識見を共有し、根本的な原因を洗い出し、これらの情報から各種防御対策を策定する。

▲導入事例と問題解決ツールの使用について文書化する。

▲脅威の変化、攻撃者の能力、現在の不正侵入経路を追跡する。

▲法規制フレームワークに対策を対応させ、全体的な優先事項を特定して集中的に取り組む。

▲ツール、作業支援機能、翻訳を共有する。

▲共通する課題（初期アセスメント、実装ロードマップの策定など）を特定し、個人／個々の組織としてではなくコミュニティとして解決に取り組む。

上記によって、CSC は単なる推奨対策の一覧ではなく、優先的で非常に焦点が絞られた活動として確立されている。CSC にはコミュニティ全体でのサポートネットワークがある

ため、実装、使用、拡張可能であり、業界や政府のあらゆるセキュリティ要件に準拠している。

(3) CSC が効果的である理由[4]

CSC は、実際の攻撃に関する知識と、専門家による効果的な防御対策に関する知識の両方を反映している。これには、エコシステム（複数の組織がパートナーシップを組み、組織の垣根を越えて共存共栄していく仕組み）のあらゆる構成要素（企業、政府機関、個人ユーザ)、すべての役割（脅威対応担当者、脅威分析担当者、技術者、脆弱性特定担当者、ツール開発者、ソリューション提供者、防御者、ユーザ、ポリシー決定者、監査担当者など)、多くのセクター（政府、電力、防衛、金融、運輸、学術、コンサルティング、セキュリティ、IT）が連携して、対策の開発、採用、サポートにあたっている。 あらゆる組織のトップ専門技術者は、実際のサイバー攻撃に対する防御経験から得られた幅広い知識を蓄積し、攻撃を防止または追跡するための最良の防御テクニックをまとめた合意リストを作成する。 これにより、CSC は、最も一般的な攻撃から最も高度な攻撃まで、さまざまな攻撃を検知し、防止し、対応し、このような攻撃による被害を緩和する上で最も効果的かつ具体的な技術対策をまとめたものとなったのである。

これらの対策は、システムの初期のセキュリティ侵害をブロックするだけではなく、すでにセキュリティ侵害されたマシンを検知し、攻撃者によるその後の活動を防止または中断することについても対処している。

これらの対策で特定された防御対策は、最初に攻撃される側面を低減するために装置の構成を強化し、組織のネットワーク内の長期的な脅威に対処するためにセキュリティ侵害されたマシンを特定し、攻撃者によって埋め込まれた悪意のあるコードによるコマンド&コントロール通信を中断し、維持／改善が可能で適応性があり継続的な防御対応機能を確立する。

(4) 各対策項目の概要[5]

①CSC 1 : 許可された装置と無許可の装置のインベントリ ; ネットワーク上のすべてのハードウェアデバイスをアクティブに管理（イベントリ作成、追跡、訂正）する。これにより、無許可の装置や管理されていない装置が検出され、このような装置によるアクセス権限の取得が防止される。

②CSC 2 : 許可されたソフトウェアおよび無許可のソフトウェアのインベントリ ; ネットワーク上のすべてのソフトウェアをアクティブに管理（イベントリ作成、追跡、訂正）

する。これにより、許可されたソフトウェアのみがインストールされ実行可能になり、無許可のソフトウェアや管理されていないソフトウェアが検出され、不正なソフトウェアのインストールと実行を防止する。

③CSC 3：モバイル装置、ラップトップ、ワークステーション、およびサーバのハードウェアおよびソフトウェアのためのセキュアな構成；攻撃者が脆弱なサービスや設定を悪用できないようにするため、厳格な構成管理および変更管理プロセスを使用して、ラップトップ、サーバ、およびワークステーションのセキュリティ構成を確立、実装し、アクティブに管理（追跡、報告、訂正）する。

④CSC 4：継続的な脆弱性評価および修復；脆弱性を特定して修復し、攻撃者が攻撃できるチャンスを最小限に抑えるため、継続的に新しい情報を取得、評価し、この情報に基づいて措置を講じる。

⑤CSC 5：マルウェアの防御；常に最新のアンチウイルスシグネチャを維持するため、組織は自動化機能を使用する。組織は自動化されたアセスメントを毎日実行して結果を確認し、保護が有効になっていないシステム、および最新のマルウェア定義がないシステムを見つけ、リスクを低減する。

⑥CSC 6：アプリケーションソフトウェアのセキュリティ；ソフトウェアにおけるセキュリティ上の脆弱性を防止、検出、訂正するため、社内で開発したソフトウェアと取得したソフトウェアのすべてのセキュリティライフサイクルを管理する。

⑦CSC 7：無線 LAN に関するアクセスコントロール；無線装置は、攻撃者が標的とする環境への長期のアクセスを維持する上で便利な攻撃手段となる。組織は、市販の無線侵入検知システムとともに、市販の無線スキャン、探知、および発見ツールを使用する。

⑧CSC 8：データ復旧能力；攻撃者がマシンを侵害する際、多くの場合、構成とソフトウェアを大きく変更する。場合によっては、データをわずかに変更して、組織の有効性を危険にさらすこともある。四半期ごとに 1 回（および新規バックアップ装置の購入時）、テストチームは、テストベッド環境でシステムバックアップの復元を試行・評価する。

⑨CSC 9：要員のスキル不足を補うためのセキュリティスキル評価および適切なトレーニング；サイバーセキュリティはしばしば技術上の課題だけだと考えられがちであるが、関係者である人間の行動が成否を左右する場合が多くある。全体計画に基づき、セキュリティポリシーの作成、教育計画の作成、トレーニングの実施、セキュリティリテラシー教育の実施し改善を進める。この計画はすべての職務を対象に含める。その際に、事

業の重要性とその事業をすすめる上で不可欠なセキュリティの職務を優先して計画を策定する。

⑩CSC 10：ファイアウォール、ルーター、スイッチなどのネットワーク機器のためのセキュアな構成；製造業者や再販業者から納品されたネットワークインフラ機器は、デフォルト設定ですぐに使用できるようになっているが、セキュリティの考慮がなされていない。攻撃者が脆弱なサービスや設定を悪用できないようにするため、厳格な構成管理および変更管理プロセスを適用してネットワークインフラの機器構成を確立、実装し、アクティブに管理（追跡、報告、訂正）する。

⑪CSC 11：ネットワークポート、プロトコル、およびサービスの制限および監視；攻撃者は、悪用されやすい、リモート側でアクセス可能なネットワークサービスを探している。このため、攻撃者に対して脆弱性が利用可能である期間を最小限に抑えるため、ネットワーク接続装置でのポート、プロトコル、およびサービスの継続的な運用を管理（追跡／コントロール／訂正）する。

⑫CSC 12：管理特権の制限；管理特権の誤用は、攻撃者が標的とする企業内に侵入するための主な手段となる。このため、コンピュータ、ネットワーク、アプリケーションの管理特権の使用、割り当て、構成を追跡／管理／防止／訂正する。

⑬CSC 13：境界防御；内部ネットワークと外部ネットワーク間の境界線が曖昧になりつつあることに注意する必要がある。DMZ システムだけでなく、ワークステーションやノートＰＣなどインターネットからコンテンツを取得できるシステムは全て攻撃者によって、インターネットを介して攻撃される可能性がある。このため、異なるトラストレベルのネットワーク間を流れる情報の中からセキュリティ上問題となるデータを検出／防止／訂正する。

⑭CSC 14：監査ログのメンテナンス、モニタリングおよび分析；セキュリティロギング機能と分析が欠如している場合、攻撃者は、所在地、悪意のあるソフトウェア、および被害者のマシンでの不正活動を隠ぺいできる。しっかりとした監査ログがないと、攻撃は無期限に気づかれないままになり、行われた特定の損害は取り消すことができないことがある。場合によっては、ロギングレコードは、成功した攻撃の唯一の証拠である。このためイベント監査ログを収集、管理、分析する。

⑮CSC 15：「Need to Know」に基づくアクセス制御；承認された分類に基づき、どのユーザ、コンピュータ、アプリケーションが重要な資産（情報、リソース、システムなど）

へのアクセスを必要とし、アクセス権限を持つべきであるかに関する正式な決定内容に基づいて、このような資産へのアクセスを追跡／制御／防止／訂正する。

⑯CSC 16：アカウントの適正な管理と監視；攻撃者がシステムアカウントおよびアプリケーションアカウントを利用できる機会を最小限に抑えるため、このようなアカウントのライフサイクル（アカウントの作成、使用、休止、削除）をアクティブに管理する。

⑰CSC 17：データの保護； データの不正持ち出しを防止し、不正に持ち出されたデータの影響を低減し、機密情報の機密性と完全性を確保するため、暗号化（暗号鍵の管理を含む）と DLP（データ損失防止）技術を組み合わせて使用する。これによりデータを最も適切に保護できる。

⑱CSC 18：インシデント対応とその管理；組織の情報と信頼を保護するため、攻撃を迅速に検知し、損害を効果的に最小限に抑え、攻撃者の存在を根絶させ、ネットワークとシステムの完全性を復元するためのインシデント対応基盤（計画、定義されている役割、訓練、コミュニケーション、管理／監督）を策定、実装する。

⑲CSC 19：セキュアなネットワークエンジニアリング；信頼性の高いシステム運用を可能にし、攻撃者に攻撃の機会を与えないか、もしくは攻撃を最小限に抑える機能を特定して設計し、組み込むことで、セキュリティをその組織の属性に適合するようにする。

⑳CSC 20：ペネトレーションテストおよびレッドチームの訓練；攻撃者の目的と活動をシミュレーションして、組織の防御対策（テクノロジー、プロセス、担当員）の全体的な強度をテストする。ペネトレーションテストでは、社内で特定可能な脆弱性の特定と評価を最初に行う。独立したレッドチームは、脆弱性の存在、すでに実施されている防御対策および低減コントロール、さらには将来の実装のために計画されている防御対策および低減コントロールの有効性に関する価値のある客観的な見識を提供することができる。

2.「The Strategies to Mitigate Targeted Cyber Intrusions （35 の標的型サイバー侵入に対する軽減戦略）」

（1）概要[6]

オーストラリアのコンピュータ・ネットワークは、機密情報へのアクセスを求める敵対者の標的とされている。一般的に用いられるテクニックはソーシャル・エンジニアリングであ

る。そして、悪意のある「スピアフィッシング」電子メールは、読者をそそのかして開封するよう工夫されている。ユーザは、悪意のある電子メールの添付ファイルを開封するか、埋め込まれた「悪意のあるウェブサイト」へリンクするかもしれない。どちらの行動でも、ネットワークを危殆化することができ、機密情報を漏えいすることがきる。

通信電子局（ASD）は、標的型サイバー侵入を軽減する戦略のリストを開発した。このリストは、オーストラリア通信電子局の、重大なサイバー侵入への対応、オーストラリア政府機関に対する脆弱評価と侵入テストの実施を含むサイバーセキュリティに関する運用上の経験に基づいている。

2010 年 2 月に最初に公開された軽減戦略のリストは、オーストラリア政府全体へのごく最近のサイバー侵入の分析に基づいて、2014 年に改訂された。

（2）標的型サイバー侵入の 3 段階[7]

標的型サイバー侵入は 3 段階で行われることを考えれば、組織は、サイバー侵入のすべての 3 つの段階で対処できる戦略を選択しなければならない。

ア．第 1 段階―コード実行（Code Execution）

サイバー空間の敵対者は、標的とするユーザを選定するために偵察を実行する、そして、悪意のあるウェブサイトを設置するか、あるいはユーザがアクセスする合法的なウェブサイトを危殆化する。この技術は、「ドライブ・バイ・ダウンロード攻撃」又は「水飲み場型攻撃」といわれる。また、サイバー空間の敵対者は、悪意のある「スピアフィッシング」電子メールを送信する。その電子メールには、悪意のあるコンテンツを持ったウェブサイトへのハイパーリンクが貼り付けられているか、あるいは PDF ファイル若しくはマイクロオフィス文書が RAR/ZIP（データ圧縮形式：訳者注）のアーカイブ・ファイルとして添付してある。

イ．第 2 段階―ネットワーク・プロパゲーション（Network Propagation）

敵対者は、機微な情報を見つけてアクセスするために、ネットワークのあらゆる場所をプロパゲーション（横方向に移動）するために、一般に、危殆化された認証情報または組織の他のワークステーションとサーバの利用可能な脆弱性を使用する。そのようなネットワーク・プロパゲーションは、ネットワークが十分に分割及び分離されていなければ、特に複数のワークステーション又はサーバが同じ管理者パスワードを共有している場合、急速に拡大することがあり得る。しばしば、アクセスされる情報には、データベースに保管されてい

るデータのみならず、Microsoft Office ファイル、Outlook 電子メールの PST ファイル、PDF ファイルならびに情報が含まれる。敵対者は、一般的に、以下にアクセスする。

▲遠隔アクセス認証情報、組織階層、ユーザ名とパスワードなどのユーザについての詳細

▲ワークステーション、サーバ及びネットワークの設定の詳細を含むシステム情報

ウ．第 3 段階―データの密かな抜き取り（Data Exfiltration）

敵対者は、組織の機微な情報のコピーを、圧縮・暗号化するために、通常、RAR/ZIP アーカイブ・ツール・ファイルを使用する。

敵対者は、この情報をネットワークから密かに抜き取る。しばしば、組織のネットワークの上の一つの「ステージング（動作や表示などの最終確認を行う段階化：訳者注）にある」ワークステーション又はサーバからこの情報を密かに抜き取る。

敵対者は、HTTPS/SSL、HTTP、又は場合によっては DNS 若しくは電子メールなどの組織のゲートウェイ・ファイアウォールで許可された使用可能なネットワークプロトコル及びポート番号を使用する。

敵対者は、VPN 又は他の遠隔アクセスの認証情報を入手するかもしれない。そして、情報を密かに抜き取るために、ネットワーク・ベースのモニタリングを打破する目的を持って、この暗号化されたネットワーク接続を使用するかもしれない。

一般に、敵対者は、危殆化された VPN 又は他の遠隔アクセス・アカウントのみならず、組織のネットワーク上にいくつかの危殆化されたワークステーション又はサーバを所有している。そして、将来における情報の更なる収集と密かな抜き取りを容易にするバックドアとして維持する。

（3）軽減戦略を実装することの合理性[8]

センシティブ情報へアクセスする政府機関を含むオーストラリアの組織のセキュリティ態勢が不十分であるならば、それらの組織は、洗練されていないサイバー侵入によっても危殆化される高い可能性がある。オーストラリアの経済的繁栄にもたらされる損害、その結果により引き起こされるオーストラリアの市民に対する損害に加えて、危殆化された組織の評判は傷つき、オーストラリア政府に対する市民の信頼は徐々に失われ、さらに、洗練されていないサイバー侵入を絶えずクリーンアップするために、希少な財源と人的資源が必要以上に消費される。

多くの組織の資金とスタッフは、有限である。そして、組織のセンシティブ情報を保護することの重要性に全力を尽くす経営陣を必要としている。軽減戦略の上位 4 項目（以下、軽減戦略トップ 4 という。）は、パッケージとして実装された時、サイバー侵入の 3 段階すべてのサイバー侵入に対処し、比較的少ない時間と努力とお金で、セキュリティ態勢を大きく強化することができる。

組織は、最初に、最も標的にされそうなユーザのワークステーションに、次にすべてのワークステーションとサーバに、軽減戦略トップ 4 を実装し、それが終了したならば、残存リスクが許容できるレベルに達するまで、セキュリティ・ギャップに対処するための追加の軽減戦略を選択することができる。

（4）各戦略項目の概要[9]

①軽減戦略#1：アプリケーションのホワイトリスト化；少なくとも、最も標的にされやすいユーザが使用しているワークステーションに実装されているダイナミック・リンク・ライブラリ（Dynamic Link Library：DLL）ファイル、スクリプト、及びインストーラーなどの悪意のある又は承認されていないプログラムの実行を防止するために、許可／信頼されたプログラムをホワイトリスト化する。

②軽減戦略#2：アプリケーションへのパッチ適用；アプリケーション、特に Java、PDF ビューア、Flash Player、Microsoft Office、ウェブ・ブラウザ及び ActiveX を含むウェブ・ブラウザ・プラグインに対してパッチを適用する。また、インターネットでアクセスできるウェブサーバ・ソフトウェアと同様に機密情報を格納するデータベースなどのサーバ・アプリケーションにもパッチを適用する。

③軽減戦略#3：オペレーティングシステムの脆弱性に対するパッチの適用；「非常に危険」な脆弱性にさらされているシステムに対しては、2 日以内に、パッチを適用するか又は軽減する。組織のビジネス要件を満たすオペレーティングシステムの最新バージョンを使用する。何故なら、より新しいオペレーティングシステムは、一般的に、エクスプロイテーション対策能力を含む追加のセキュリティ技術を取り入れているからである。

④軽減戦略#4：管理者権限の制限；管理者権限を、ユーザの役割に基づき、オペレーティングシステムとアプリケーションに制限する。そのようなユーザは、電子メールを読むこと、ウェブを閲覧すること（ウェブ・ブラウジング）、例えばインスタントメッセージングなどのインターネット・サービスを経由してファイルを取得することなどの管理業務でない活動又は危険な活動のためには、別の非特権アカウントを使用し、できるなら

ば物理的にも別のワークステーションを使用しなければならない。そのようなユーザは、少なくとも軽減戦略トップ 4 が実装されたワークステーションを使用して管理業務を行わなければならない。

⑤軽減戦略＃5：ユーザ・アプリケーション設定（configuration）の堅牢化；ユーザ・アプリケーション設定の堅牢化により、インターネット・ベースの Java コード、信頼できない Microsoft Office マクロ、並びに必要とされない／望ましくないウェブ・ブラウザ及び PDF ビューアの機能を無効化する。

⑥軽減戦略＃6：自動化された動的解析；ネットワーク・トラフィック、新しい若しくは修正されたファイル又は他の構成変更を含む疑わしいふるまいを探知するために、電子メールとウェブ・コンテンツをサンドボックス内で動作させる自動化した動的解析を実施する。

⑦軽減戦略＃7：オペレーティングシステム（OS）に対する一般のエクスプロイトの脅威の軽減；データ実行防止（Data Execution Prevention：DEP)、アドレス空間配置のランダム化（Address space layout randomization：ASLR）及び脆弱性軽減ツールキット（Enhanced Mitigation Experience Toolkit : EMET)などの一般的な脅威軽減技術を OS に適用する。

⑧軽減戦略＃8：ホスト型の侵入探知／防止システム（IDS／IPS）；例えばプロセス・インジェクション、キーロガー、ドライバーローディング及びコールフッキングなどのプログラムの実行の間の異常なふるまいを特定するためにホスト基盤の侵入探知／防止システム（IDS/IPS）を実装する。

⑨軽減戦略＃9：ローカル管理者権限の無効化；サイバー空間の敵対者が、いくつかのワークステーションで共有されている危殆化されたローカル管理者証明書を使用して、組織のネットワーク全体に、簡単に拡大することを防止するために、ローカル管理者権限を無効にする。

⑩軽減戦略＃10：ネットワークの分割及び分離；センシティブな情報及び例えば、マイクロソフト・アクティブディレクトリ・サービスによるユーザ認証などの重要なサービスを保護するために、ネットワークをセキュリティゾーン毎に分割及び分離する。

⑪軽減戦略＃11：複数要素認証；複数要素認証を、特に、最も狙われやすい標的のため、リモートアクセスのため及びユーザが特権的な行動（システム管理を含む）を行うか又はセンシティブ情報のリポジトリ（格納庫）にアクセスしようとする時のために、実装する。

⑫軽減戦略＃12：外部から入ってくるネットワーク・トラフィックを遮断するソフトウェア型のアプリケーション・ファイアウォール；ソフトウェア型のアプリケーション・ファイアウォールを実装する。そして、それは、悪意がある又はさもなければ未許可である外部から入ってくるネットワーク・トラフィックを遮断するよう標準設定する。

⑬軽減戦略＃13：外部へ出ていくネットワーク・トラフィックを遮断するソフトウェア型のアプリケーション・ファイアウォール；ソフトウェア型のアプリケーション・ファイアウォールを実装する。それは、ホワイトリストに登録されたアプリケーションによって生成されたものでない、外部に出ていくネットワーク・トラフィックを、標準設定で遮断する。

⑭軽減戦略＃14：一時的に利用可能な仮想化かつサンドボックス化された信頼できる運用環境；ウェブ・ブラウジングのような危険な活動のために、組織の内部のネットワークの外側に、一時的に利用可能な仮想化かつサンドボックス化された信頼できる運用環境を実装する。

⑮軽減戦略＃15：成功又は失敗したコンピュータ・イベントの一元化かつ同期されたログの取得；自動化したリアルタイムのログ分析と共に、成功又は失敗したコンピュータ・イベントの一元化かつ同期されたログの取得を実行する。そして、ログは少なくとも 18 ヵ月、保存する。重要なログには、アクティブディレクトリ・イベント・ログ並びに VPN 及び他のリモートアクセス接続を含むユーザ認証に関連したログだけでなく、セキュリティ製品により出力されたログが含まれる。

⑯軽減戦略＃16：許可された又は遮断されたネットワーク活動の一元化かつ同期されたログの取得；自動化したリアルタイムのログ分析と共に、成功又は失敗したコンピュータ・イベントの一元化かつ同期されたログの取得を実行する。そして、ログを少なくとも 18 ヵ月に保存する。重要なログには、DNS サーバ、Web ユーザーエージェントのヘッダー値を含む接続の詳細を含む Web プロキシ・ログ、DHCP の割り当て情報、組織のネットワークに出入りするトラフィックの詳細を記録したファイアウォール・ログ、及びネットワークフロー・データなどのメタデータが含まれる。

⑰軽減戦略＃17：電子メール・コンテンツ・フィルタリング；ビジネス機能のために必要とされるファイルタイプとファイル拡張子でホワイトリスト化された添付ファイルだけを許可する電子メール・コンテンツ・フィルタリングを実装する。

⑱軽減戦略＃18：ウェブ・コンテンツ・フィルタリング；許可された種類のウェブ・コンテンツをホワイトリスト化するウェブ・コンテンツ・フィルタリングを実装する。そし

て、ふるまい分析、インターネット型のレピュテーション・レーティング、ヒューリスティック及びシグネチャを使用する。

⑲軽減戦略＃19：ウェブ・ドメインのホワイトリスト化；ウェブ・ドメインのホワイトリスト化を実装する。何故ならば、悪意のあるドメインのうちの小さな割合をブラックリスト化するより、この方法の方がより積極的かつ徹底的である。

⑳軽減戦略＃20：なりすまし電子メールのブロック；入ってくる電子メールをチェックするために、センダーID（Sender ID）又はセンダー・ポリシー・フレームワーク（Sender Policy Framework：SPF）を用いて、なりすまし電子メールをブロックする。さらに、SPF レコードを厳しく制御することは、自己組織のドメインのなりすましを防止する手助けとなる。

㉑軽減戦略＃21：ワークステーション及びサーバの設定管理（configuration management）；厳格な標準運用環境（Standard Operating Environment：SOE)に基づくワークステーション及びサーバの設定管理を実行する。それは、例えば、使用していない IPv6、自動再生（autorun）及び LM ハッシュ（LAN Manager ハッシュ）などの不必要／望まれていない機能を無効にする。

㉒軽減戦略＃22：ヒューリスティックな手法と自動化したインターネット型のレピュテーション・レーティングを用いたアンチウイルスソフト；プログラムを実行する前に、プログラムの普及率とデジタル署名の信頼性をチェックするために、自動化したインターネット上のレピュテーション・レーティングを用いたアンチウイルスソフトを実装する。

㉓軽減戦略＃23：ワークステーションからインターネットへの直接接続の拒否；DNS サーバ、電子メールサーバ、又は認証されたウェブ・プロキシサーバを通過させる IPv6 対応のファイアウォールを使用することにより、ワークステーションから直接インターネット接続するのを拒否する。

㉔軽減戦略＃24：サーバ・アプリケーション設定（configuration）の堅牢化；例えばデータベース、ウェブ・アプリケーション、顧客管理（customer relationship management：CRM)、財務、人事及び他のデータ記憶装置システムなどのサーバ・アプリケーション設定の堅牢化を実行する

㉕軽減戦略＃25：強固なパスワードポリシーの履行；パスワードが複雑で、長くて、暗号によって強いアルゴリズムでハッシュされるならば、サイバー空間の敵対者がパスワ

ード・ハッシュを解いて、サイバー侵入の第 2 のステージの一部として、組織のネットワーク全体に拡大することはより困難となる。

㉖軽減戦略＃26：可搬型及び携帯型メディアの管理；情報漏えい防止（Data Loss Prevention : DLP）戦略の一部として、可搬型及び携帯型メディアを管理する。それには、保管、取扱、ホワイトリスト化、USB 機器の許可制、暗号化及び廃棄が含まれる。

㉗軽減戦略＃27：Server Message Block （SMB）及び NetBIOS へのアクセス制限；ワークステーション上で、さらに可能であればサーバで稼働している SMB 及び NetBIOS へのアクセスを制限する。

㉘軽減戦略＃28：ユーザ教育；ユーザ、特に最も狙われやすい標的に対して、ソーシャル・エンジニアリングを利用したスピアフィッシング電子メール又は思いもよらない複製メールを特定し、IT セキュリティ・チームに報告するなどのインターネット脅威について教育を実施する。

㉙軽減戦略＃29：ワークステーション上のマイクロソフト・オフィス・ファイルの点検；ワークステーション上で潜在的に悪意のあるマイクロソフト・オフィス・ファイルの点検を実施する。

㉚軽減戦略＃30：シグネチャ型のアンチウイルスソフト；マルウェアを特定するために主に最新のシグネチャに依存するシグネチャ型のアンチウイルスソフトを使用する。その際、異なるベンダーから提供されるゲートウェイ及びデスクトップに実装されたアンチウイルスソフトを使用する。

㉛軽減戦略＃31：電子メールサーバ間のトランスポート・レイヤー・セキュリティ（Transport Layer Security : TLS）暗号化；電子メールサーバの間の TLS 暗号化を使用する。送信及び受信電子メールサーバ双方の TLS 暗号化は、合法的な電子メールが送信中に盗聴され、その後ソーシャル・エンジニアリングに利用されるのを防止するのを助ける。

㉜軽減戦略＃32：IP アドレスによってウェブサイトにアクセスする試みのブロック；ドメイン名の代わりに IP アドレスによってウェブサイトにアクセスする試みをブロックする。

㉝軽減戦略＃33：ネットワーク型の探知／防止システム（IDS／IPS）：軽減戦略#16 で記録された異常を特定するために、シグネチャ及びヒューリスティックスを使用したネットワーク型の探知／防止システム（IDS/IPS）を実装する。

㉞軽減戦略＃34：ゲートウェイのブラックリスト化；既知の悪意のあるドメイン及びIPアドレスへのアクセスをブロックするためにゲートウェイのブラックリスト化を実装する。

㉟軽減戦略＃35：ネットワーク・トラフィックのキャプチャ；侵入後の分析を行うために、ネットワーク周辺装置を行き来するトラフィックだけでなく、内部の重要資産であるワークステーション及びサーバを出入りするネットワーク・トラフィックをキャプチャする。

おわりに

これまで多くのセキュリティ基準がシステムと重要データへのリスクに対処するために開発されてきたが、常に進化する攻撃に対して実効的な対策になっているとは言い難く、かつ「選択肢が多すぎることによる混沌（Fog of More）」が生じていた。例えば、米・国家標準技術院（NIST）のガイダンスは、数千ページに達し、どれを実装するかが問題となる。

上記の 2 つの対策リストの新しいところは、最も一般的に用いられている攻撃と、国家標準技術院（NIST）や他の組織によって特定された防御策とを相互に関連付け、効果によって戦略に優先順位を付与したことである。そして、「最初に最低限行わなければならない」ことに注力し、シンプルにすることを理念として作成されている。その上位の対策を実践することによって、コストを大幅に削減でき、かつ効果が目に見えて改善されることである。この 2 つの対策リストは既に各国の政府機関で広く採用されている。

特に、ホワイトリスト化（whitelisting）の概念は、「35 の標的型サイバー侵入に対する軽減戦略」の主要なテーマである。それによって、ネットワーク・コミュニケーション又はプログラム実行のような活動は、初期設定により拒否される。そして、システム及びネットワーク管理者によって明白に許可された業務上の要求に合致した活動だけが許される。他方、伝統的なブラックリスト化の方法は、好ましくないと知られた少しの活動を妨害するだけである。そして、ブラックリスト化は、状況の変化に対応し、多大な時間を必要する方法で、僅かなセキュリティしか提供しない。

筆者は、「上位 4 つの対策を一括して実装することにより、攻撃の 85%を防止又は軽減することができた[10]」という実績を有するオーストラリア通信電子局（ASD）が推奨する「軽

減戦略トップ 4」を実装することを推奨する。これにより、各組織は、比較的小さな時間・努力・経費で組織のセキュリティ能力を強化することができるであろう。

[1] CSIS「Raising the Bar for Cybersecurity」 http://csis.org/publication/raising-bar-cybersecurity
[2] sans-japan 「The Critical Security Controls ver5.1 http://www.sans-japan.jp/resources/CriticalSecurityControls.html
[3] Center for Internet Security (CIS) 「Critical Security Controls Now at CIS!」 https://www.cisecurity.org/documents/TheCriticalSecurityControls_ver5.1_Japanese_final_000.pdf
[4] 同上
[5] 同上
[6] オーストラリア・通信電子局「Strategies to Mitigate Targeted Cyber Intrusions」 http://www.asd.gov.au/publications/Mitigation_Strategies_2014.pdf
[7] 防衛基盤整備協会「標的型サイバー侵入に対する軽減戦略―軽減戦略の詳細」BSK 第 27－2 号 p－34
[8] 防衛基盤整備協会「標的型サイバー侵入に対する軽減戦略―軽減戦略の詳細」BSK 第 27－2 号 P－39
[9] 防衛基盤整備協会「標的型サイバー侵入に対する軽減戦略―軽減戦略の詳細」BSK 第 27－2 号 P－41 ～65
[10] オーストラリア・通信電子局「Top 4 Mitigation Strategies to Protect Your ICT System」 http://www.asd.gov.au/publications/protect/top_4_mitigations.htm