情報サービス産業の管理体制強化に向けたセキュリティ技術検討委員会（第 2 回）
議事要旨

日時 ： 2021 年 2 月 15 日（月） 13 時 00 分～15 時 00 分
場所 ： web 会議（Zoom）

参加者 （敬称略・五十音順）

（委員）

鵜飼 裕司	株式会社 FFRI セキュリティ 代表取締役社長
岡部 寿男 座長	京都大学学術情報メディアセンター センター長
林 達也	株式会社パロンゴ CTO
平山 敏弘	情報経営イノベーション専門職大学 教授

（オブザーバー）

田辺 雄史	情報技術利用促進課 課長／ 情報産業課 ソフトウェア・情報サービス戦略室長
高野 了成	情報産業課 課長補佐
飛世 昌昭	情報産業課 課長補佐
月岡 航一	情報産業課

（事務局）

ソフトバンク株式会社

配布資料

（資料1）：議事次第
（資料2）：委員等名簿
（資料3）：情報サービス産業の管理体制強化に向けたセキュリティ技術動向等に関する調査報告書

議事進行順序

1. 開会
2. 議題
   - 調査報告書について
     - （a）阻害要因の事例調査
     - （b）改善案と求められる機能の提案
     - （c）技術開発に関する論点の整理
3. 閉会

議事要旨

上記議事進行順序に従って進行。委員・オブザーバーからの主な質問・意見は以下に記す。

1. 開会
2. 議題
   - 調査報告書について

（資料3）に基づき、事務局より説明。

(a) 阻害要因の事例調査

- 調査報告書は技術的課題を中心にまとめると理解した。様々な要因に対して実質的な対策が打てないために、リモートワークの阻害要因となっている。それらを外部脅威と内部脅威に分けた時に、内部脅威の方が影響は大きいと考えている。そのうえ、内部脅威は対策するのが困難である。例えば、内部脅威への対策として、USB メモリやプリンタの使用を禁止することがあるが、画面をビデオカメラ等で撮影するといった行為を防ぐのは非常に難しい。それゆえ、内部脅威に関しては、阻害要因として解決できない部分が課題として残ることを結論に記載した方がよい。
- コロナ禍でリモートワークを実施するための喫緊の表層的な対応と、本質的な対応を分けてまとめるべきである。特に、Wi-Fi 設定については、前回の委員会でも議題に上がった通り強要するのが難しい。また、昨今の情勢を踏まえ、社員にテザリング用のモバイル端末を配布した企業もあった。内部不正といった難しい問題に対しても、オフィスに出社すれば安全なのかといった観点を踏まえ、物事を表層的に捉えるのではなく、本質的に整理することが必要。そうすることで、技術的に解決すべき本質的な課題と、今回対象としない心理的な課題を分割してまとめていけるのではないか。
- 調査報告書の中で、リモートワークの阻害要因をまとめて、これらを解決することでリモートワークを安全に実施することを推奨すると理解している。しかし逆に、リモートワークを導入できない理由にされてしまうのではないかと危惧している。リモートワークのメリットを示し、推進していくような内容を調査報告書の前段に盛り込めないか。
- 今年度は緊急事態宣言が出て、各社やむにやまれず緊急にリモートワーク対応をしたということもあり、そのうちいくつかは解除後に元に戻したという。今回の調査研究事業は、新型コロナウィルスへの対応としてではなく、ポストコロナの時代に向けて日本が変わっていくうえで、リモートワークが当たり前になるという方向で考えるべきであるので、阻害要因だけが表に出ないように注意すべきである。
- 今年度に関しては、今までの仕事のやり方を変えずに、端末を持ち帰って、ビデオ会議を活用するのみに留まってしまったが、仕事のやり方そのものを変えていかねばならない。今回の調査研究の対象外ではあるが、仕事のやり方もリモートワークに合わせて変える必要があるといった技術的要因以外の事項も追記しておいた方が誤解は少ない。
- 内部不正に関しては、従来のオフィス中心の勤務形態であっても、悪意を持つ者は実行できた。リモートワークに移行し、障壁が下がっているだけである。また技術的な話のみに留まらない要素もあり、他のリモートワーク阻害要因と同列に並べてしまうと最後まで解

決できないネガティブな要因になり兼ねないため注意が必要。

(b) 改善案と求められる機能の提案

- 近年、複数の企業がゼロトラスト実現に向けて、情報収集及び検討を行っているが、一斉にゼロトラストへ移行することは困難であるという。その理由としては、レガシーシステムを抱えていることや、コスト・時間がかかりすぎるということが挙げられる。一方で、従来の境界型モデルは新型コロナウィルスによるリモートワーク対応のみならず、マルウェア対策等を考えたときにも限界がある。そのため、将来的なアーキテクチャとしてはゼロトラストアークテクチャの方へ向かっていくことが重要である。これらを踏まえて、一斉に移行するのは困難だが、段階的な移行を推進するようなメッセージが込められるとよい。
- 内部不正対策に関しては、国家安全保障に関わる業務や、機密性の高い業務を行う場合には、従業員のプライバシーに配慮して個人情報の抽象化等をしながら、画面収録などの各種対策を実施する必要はあると考えている。しかしながら、大半の企業が調査報告書に記載の対策を実施するのは現実ではなく、どこまで対策が必要か悩んでしまうのではないか。その点を踏まえて、現場の担当者が納得できるような現実的なロードマップや方針を調査報告書内に記述するのが好ましい。
- 海外事例について、それぞれの企業が持つ技術的な強みから整理するとよいのではないか。私見を含むのだが、Google 社は、公開鍵基盤（PKI：Public Key Infrastructure）の仕組みを活用しており、特に HTTPS 通信を行うブラウザを持っているという自社の強みを生かしてシステムを構築しているという技術的な側面がある。Microsoft 社は、Active Directory や Office, OS, Intune といった OS 寄りのアプローチから全体像をカバーしているというような、技術的な構成要素・コンポーネントがある。このように技術的な強みという観点から整理を行うと、事例として反映しやすくなり、例えば、ブラウザを中心に業務を行っている場合は Google 社的なアプローチで、専用アプリケーションを利用している場合は Microsoft 社的なアプローチで考えることができる。
- 内部不正対策の事例については、従業員のプライバシーインパクトがありそうであるので、どのように解消したのかを伺いたい。また、調査報告書としても、日本国の政府機関ドメイン（go.jp）で一般公開されるものであるので、いかにしてプライバシーの侵害とならないようにうまくソリューションを作ったのか記載して欲しい。
- リモートワーク阻害要因がレイヤ等に基づいて分類・マッピングされていると対策が考えやすい。例えば、ネットワークレイヤで考えたときに、どのレイヤに対する対策なのか、もしくは、レイヤではなくゾーン・セグメントで考えたときに、エッジ・PC、クラウド、ネットワーク、サーバーどの対策なのか、という観点で整理して考えることで対策がしやすくなる。また、リスクアセスメント・脆弱性診断を実施する際においても、阻害要因がレイヤ分けされていると参照しやすい。
- 調査報告書内で示した事例については、先進的な事例であり、これを標準とするわけではない。この事例で示した対策を全て行わないとリモートワークができないという論調にならないように留意すべき。

・ 阻害要因を分類・マッピングするのは非常に重要な観点である。ゼロトラストアーキテクチャやゼロトラストネットワークアーキテクチャにおいては、レイヤを跨る、あるいは、違うレイヤに移るなどして分類が難しいものもあるので、注記するとよい。

(c) 技術開発に関する論点の整理

・ 調査対象技術を使用したサービスやシステムを提供する国内企業が現時点では業界の主要プレイヤーではないことが懸念であり、それが経済安全保障上のリスクであると調査報告書の中で結論付けられている。しかしこれでは、一般の読者がどうするべきか迷ってしまうので、指針等の説明を加えるべきではないか。
・ Google 社, Microsoft 社といった米国企業が主流の状況下で、我が国としてどのように経済安全保障を実現する安全なデジタル社会を作るべきかという点で、PKI は重要であると考えている。
・ システムを構成するコンポーネントの評価には課題が残ると考えている。我が国では、クラウド・バイ・デフォルト原則に基づいて、Amazon 社, Google 社, Microsoft 社の提供するクラウドサービスの上にシステムを構築していくことが考えられる。そういった中で、安全保障上のチョークポイントがどこに潜んでいるのか評価することが重要である。
・ 調査報告書に記載がある対策を五割から八割程度賄えるサービスが提示できるとよいのではないか。
・ 地政学的リスクに対して注意が必要であるということが理解しやすくするために、各国の状況に関して具体的に過去の経緯も交えながら、注釈や説明が加えられるとよい。
・ 地政学的リスクについては、中国が米国に対して感じているところであると考えられる。昨今では、オープンソースを用いた開発も主流のため、どこの国が技術開発しているかだけではなく、どこまでオープンな技術であるかということも重要。

総括

・ ZTA と内部不正対策の融合は今後極めて重要になってくると感じたが、今回の調査で先行事例を見つけることはできたか。
・ ポリシーエンジンに内部不正対策も織り込まれているべきである。さらに、過度な監視をしないという制約の下、必要な時には位置情報を取得するといった具体的な方法も調査報告書に追記すると現実味を帯び、実行に移しやすくなる。
・ 機密度を考える上でトラストという概念の理解が必要であるので、読者への説明を追記すべき。
・ 高機密データを取り扱う業務のリモートワークを推進するには、現在市場にあるセキュリティ対策では不十分であるとまとめられているが、調査報告書の結論として不適切ではないか。
・ 多様化は重要である。できることとできないことが常にあり、例えば、自宅であっても個室が用意できる時間帯とできない時間帯がある。このように細かく区別し、状況に応じた実施可能な作業を決めていかねばならない。一方で監視に関しては、従業員のプライバシ

ーを侵害しないようにすべき。また、調査報告書に記載されている内容が経産省からのメッセージだと誤解されないように表現には留意すべき。

- オフィス勤務でも、リモートワークでも、同じように働けるように、仕事そのものの切り分けが必要であることを前向きな文言として記載すべき。

3. 閉会

座長、及び経産省から総括のコメントを拝受。

- 2 回に渡る委員会の中で、活発な議論ができ、調査報告書も世の中のためになるものになることを期待する。尚、調査報告書についての文責は事務局とする。
- 本調査事業は、経済安全保障におけるセキュリティのチョークポイントという難しいテーマだったが、うまくまとめられた。委員からの指摘の通り、前向きな表現となるように修正を依頼する。リモートワークやゼロトラストアーキテクチャ導入のハードルを上げすぎないよう、納得できるステップを示すことが現実的であり、重要である。

以上