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1回）
議事要旨

日時 ： 2021 年 1 月 19 日（火） 16 時 00 分～18 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）：議事の運営について（案）
（資料4）：本事業の概要について（提案書抜粋版）
（資料5－1）：「(a) 阻害要因の事例調査」の実施方法
（資料5－2）：「(b) 改善案と求められる機能の提案」の調査方法
（資料5－3）：「(c) 技術開発に関する論点の整理」の実施方法

議事進行順序

1. 開会
   - 議事の運営について
2. 座長の選任
3. 議題
   - 本調査事業の概要説明

- 各調査研究の実施方法について
  - 「(a) 阻害要因の事例調査」の実施方法について
  - 「(b) 改善案と求められる機能の提案」の調査方法について
  - 「(c) 技術開発に関する論点の整理」の実施方法について

4. 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。
(補足:議事要旨中の記号使用例は次の通り。[・]:委員・オブザーバーからの質問・意見等、[→]:事務局・オブザーバーからの返答)

1. 開会
   - 議事の運営について
     (資料3)に基づき、事務局より議事の運営について説明。委員会承認。

2. 座長の選任
     事務局より岡部委員を座長として推薦。委員会承認。

3. 議題
   - 本調査次長の概要説明
     (資料4)に基づき、事務局より説明。

   - 各調査研究の実施方法について

「(a) 阻害要因の事例調査」の実施方法について

(資料5－1)に基づき、事務局より説明。

- 事務局から提示された阻害要因の存在は認めるものの、必ずしもリモートワークが原因で、内部犯行による事件が起きやすくなるとはいえない。阻害要因の一つとして、技術的要素以外にも「漠然とした不安」のような心理的ハードルもあるのでは。心理的ハードルについても数値化することが理想だが、現実的には難しい。定量調査のチェックシートで×の項目があってもリモートワークを導入している企業や、全て○でも非推奨とする企業もあるだろう。
- → 今回のヒアリング調査の結果、未実施項目があってもリモートワークを導入している企業は存在し、経営者の判断によって実施しているようだった。また、昨年の緊急事態宣言が後押しとなり、リモートワークが推進された企業もあった。【事務局】
- チェックシート項目の「無線 LAN に対して業務用と個人用を分離しているか」については、リモートワークに関わらず、通常のオフィスでも実施できていない企業もある。達成困難な項目もあるため、チェックシートが独り歩きしないよう留意すること。
- チェックシートについては、「満点をとるべきであり、未実施項目があるのにリモートワーク

を導入すべきでない」という論調は避けること。各企業が、未実施項目を踏まえ適切な対策を行い、リモートワークを導入するのが理想。

- 阻害要因としては、会社の文化や仕組みも大きい。どうすればリモートワークを導入できるのか、内部不正に対する従業員の意識も考慮しながら、必要な仕組みを作っていくことが重要。昨今のニューノーマルの風潮は、変容のチャンスと捉えられる。例えば、Wi-Fi の暗号化ではなくそもそものソフトウェアの安全性をチェックすることや、TLS 通信ならばパブリック Wi-Fi でも安全であること、アイデンティティー管理とアクセスコントロールを適切に行うこと等がテクニカルな観点で必要だ。
- 前回の緊急事態宣言の際、セキュリティの懸念によりリモートワークを導入できない企業の話をよく耳にした。今回の調査で、セキュリティ上のクリアすべき観点が明確になれば、リモートワークを導入できる企業が増える。そのような報告書を期待する。

「(b) 改善案と求められる機能の提案」の調査方法について

（資料5－2）に基づき、事務局より説明。

- Microsoft や Google の事例は、コスト・時間の面で負荷が高い。もう少しライトなモデルとしてソフトバンクでの内部不正対策もマッピングできると良い。
- Microsoft と Google の事例は先進的であり、今後様々な研究開発を行っていく上で、当然視野に入れるべきだが、模倣を推奨するものではない。報告書においては、先進的な事例の一部で網羅的ではないこと、またこれを推奨するものではないことを注記すべき。
- ゼロトラストと内部不正は整理した方が良い。ゼロトラストは、ある程度は内部不正に効果が発揮できる点もあるが、内部不正対策用ではないため、画面を撮影されるなど対策できないところで揚げ足を取られないよう留意する。
- Google における BeyondCorp の概念と、Google が提供しているクラウド製品の BeyondCorp Remote Access はかなり温度差があるため、混同しないよう留意すること。
- ゼロトラストは、幅が広く抽象度の高い話であるため、常時 VPN がゼロトラストというアプローチであることと混同しないよう留意すること。
- 快適なリモートワーク環境を目指すという話と、内部不正対策は混ぜて語らない方が良い。監査と監視は別物であり、監視社会的抑圧の環境は、働きやすくはならない。監査するためにゼロトラスト・ネットワークないしゼロトラスト・アーキテクチャの一部が有効に作用するのは、アクセス管理やリソースのアクセスコントロールのログなど。
- G Suite(Google Workspace)だけで仕事をしているような会社の方が、安全なリモートワークができるという状況もあり、クラウドベースで設立したスタートアップ企業など、中小企業の方が導入しやすい側面もある。
- ゼロトラストはバズワード化しており、人によって認識が異なるため注意が必要。Microsoft の事例が正しい方向性かと思うが、きちんと理解している方は少ないため、本報告書におけるゼロトラストの考え方・定義を記載するべき。

→ ゼロトラストについては、多種多様なホワイトペーパーが公開されており定義は難しいが、本報告書中では、昨年 8 月に公開されたアメリカ国立標準技術研究所（NIST）の「Special

Publication（SP）800-207 ゼロトラスト・アーキテクチャ」を最も基本的なものとして定義としたい。次回委員会でドラフト版を提示し、委員にも助言を頂く。【事務局】

- 経済産業省の報告書となるため、経済産業省がゼロトラストをそのように定義したと誤解を招かないよう留意する。
- ゼロトラストに関しては、政府 CIO 補佐官からディスカッションペーパーが出ており、政策的にはそちらを参照するのもわかりやすい指標となる。

「(c) 技術開発に関する論点の整理」の実施方法について

（資料5－3）に基づき、事務局より説明。

- 証明書管理は非常に重要。鍵管理は難しい技術であり、パスワード、クレデンシャル、トークンの管理等の調査は非常に重要になる。特に昨今では、多要素認証といった技術もある。PKI においても様々な課題が出ている中で、現状の課題の切り取りはあまりされていないので、興味深い。
- バイタル認証はプライバシーの問題もあるため考慮するべき。
- 国内のソフトウェアのサプライチェーンにおけるチョークポイントをいかに整理するかが、本調査の命題であると認識している。その中で、PKI、さらにはブラウザ、Web PKI の管理は、経済安全保障という単語が出ている中では重要。これに関して大きく広げる必要はないが、Google など海外企業に依拠しているものの危険性についても触れると、どこにリスクがあるのかを整理できるのでは。
- 調査結果として、海外企業の製品だけになる懸念がある。例えば、リモートワーク関連製品は海外企業が中心となってしまう。経済産業省の報告書として、国内企業が製造できないという形でも致し方ないのか。

→ チョークポイントを明らかにすることが目標。加えて、今後検討すべき技術課題が見つかれば、大きなアウトプットであると考えている。したがって、必ずしも日本の製品だけをリストアップするということではない。【経産省】

- 最終的なアウトプットとして、現時点では日本製品として存在しない、新しい技術開発要素が列挙される。これは今後、経済産業省を中心に日本製品の新しい開発案件として出てくる課題である。そのため、今ある技術をどう使うかではなく、今後我が国として今の技術動向を踏まえ、どういう研究開発に投資すべきか、つまり、来年の話ではなくもう少し先の話を見据えた調査案件と認識している。

→ ご認識の通り。この報告書で課題を取り上げ、来年度以降の政策に繋げたい。【経産省】

4. 閉会

各委員、及び経産省から総括のコメントを拝受。

- リモートワークの阻害要因について、様々な会社経営者と話すと「事故が起きないか」、「勤勉に励むことができるか」の二つの要因に集約される。「事故が起きないか」についてはサイバーセキュリティの問題がほとんどだが、経営者が、実際のリスクや現状を理解できず、腹落ちできないところが大きい。また、「勤勉に励むことができるか」については、従

来は会社に出てくれば一定の評価が貰えたが、これは評価を含めた人事的な根本の問題。評価の仕組み・制度には大きな改善の余地がある。リモートワークの阻害要因を大局的に見るのであれば、この二つの要因のような根本に立ち返ったコメントが結びに入れられると、経営者も腹落ちするのではないか。

・ IT だから危険という話は、単純に慣れによるところもある。物理的な建物にチェックなしで入れる企業があるように、IT の問題ではなく、我々がリスクの判断を IT の世界でできるまでに成熟しきれていないのではないか。先ほど述べられたように、出社していればいいのではなく、仕事をこなしているかという点に指標を移せるか。このような生理的・物理的でない課題に慣れ、組織の文化的な課題をクリアしていかなければならない。セキュリティはあくまで手段であるため、テクノロジーとセキュリティをそれに合わせて使えるようになっていくというのが、本調査の先を見据えた最終的に目指すところではないか。

・ 調査報告書について、対象読者の想定はあるか。

→ 経済産業省ホームページにて公開されるため、誰でも参照できる。その中でも特に、IT エンジニアを対象と考えている。報告書の中では、IT について多少の知見がないと理解が難しい専門用語を使用するが、セキュリティに関する高度な知識がなくても読めるように留意してまとめる。本報告書が日本として足りない技術を開発しようとする技術者のアイデアとなり、システムやソリューション、サービスを製造してくれることを期待する。【事務局】

→ 想定読者は IT エンジニアで間違いないだろう。少なくとも、技術に明るくない経営者が直に読むものではなく、CIO 補佐の立場の方が読み、経営者に伝えるための参考にはなり得る。もちろん、経済産業省を含め、今後の技術開発を考える企業の方にも役立つものになることを期待している。

・ 日本企業におけるリモートワークの阻害要因に、勤怠管理の古い考え方があるのはご指摘の通り。それを技術でカバーして、出社時のように常に見ている環境を目指すのは誤った技術の使い方で、働き方改革とあわせて実施すべき。そのうえで、内部不正防止も含め、技術で解決できる課題を示し、これを前提とした新しい働き方設計を、という提言になると思う。社会に対して広くインパクトのある報告書を期待する。

・ 調査の方向性としては概ね合意が取れたと考えている。内部不正を一つの柱としてフォーカスするという事務局の仮説と、報告書の読者定義については引き続き議論したい。様々な意見があったが、まとめ方や説明に関して取り込めるところが多いと感じたため、事務局には対応を依頼したい。報告書の次のステップとしては、政府の予算・制度の見直しにフィードバックしていきたい。政府が間違ったメッセージを発信しないよう、有識者各位にも引き続きご意見をいただきたい。【経産省】

以上