Bird & Bird

サイバーセキュリティの新たな夜明け

香港における新たな重要インフラ法制に備える

2024 年 12 月

はじめに

待望の重要インフラ（コンピューターシステム）保護法案（**ビル**）がついに公布された。法案の公表は、今年初めに行われた一連の公開協議の集大成である。この法案は、香港の重要インフラとコンピュータ・システムがどのように規制されるべきかについて、大いに必要とされる明確性と確実性を提供するものである。前回の「*香港のサイバーセキュリティ法への備えは万全か」（英語版のみ）に*続き、今回の更新では法案の主要な側面に焦点を当てるとともに、中国本土における現在のサイバーセキュリティ規制の状況と法案を比較する。

タイムライン

対象

重要インフラ（CI）	• **香港の特定セクター**（電気通信・放送、エネルギー、IT、銀行・金融サービス、航空・陸上・海上輸送、ヘルスケアサービス）における基幹インフラ、または • **侵害された場合、**香港の重要な社会・経済活動に実質的な影響を及ぼすインフラ

クリティカル・コンピュータ・システム（CCS）	香港内または香港からアクセス可能で、CIO による CI の**中核機能**に不可欠な指定コンピュータシステム（運営者の管理下にあるか否かを問わない）。 つまり、重要インフラ（コンピュータ・システム・セキュリティ）長官が明示的に指定したシステムのみが、この法案によって規制されることになる。
重要インフラ事業者（CIO）	**特定 CI を**運用する指定事業者。

法案では、**特定重要インフラ（特定 CI）**という概念が導入されている。

簡単に言えば、

CI は、以下の場合に特定 CI となる：

1. *特定分野内の指定官庁の下で特定 CI として**規定されている**。*
2. *その他、法案に従い、コミッショナーの特定 CI であると**判断された場合**。*

これは重要なことで、長官が、その危殆化が香港の重要な社会活動や経済活動に実質的な影響を及ぼす可能性があると納得する限り、現在法案に規定されている特定分野以外のインフラを重要インフラとして指定する裁量権を持つことを意味する。

香港と中国のポジションの比較

注目すべきは、法案が他の法域の関連するサイバーセキュリティおよび重要インフラ法制を参考にしている点である。以下に、法案と中国本土の制度《サイバーセキュリティ法（2016 年）、および、重要情報インフラの安全保護に関する規則（2021 年）、以下「**中国の立場**」》、適用範囲、義務、違反に対する罰則を含む基本的な側面を俯瞰的に比較する。

香港	PRC	備考
CI の定義		
• 香港の**特定分野**（通信・放送、エネルギー、IT、銀行・金融サービス、航空・陸運・海運、医療サービス）における重要インフラ • 侵害された場合、香港の重要な社会・経済活動に**実質的な影響**を及ぼすインフラ	• **重要な産業**（公共通信、エネルギー、運輸など）の重要なネットワーク施設や情報システムで、侵害された場合、国家の安全保障や経済、人々の生活や公共の福祉に**深刻な危険が及ぶ**もの	*主な類似点：*両定義は、**特定の**セクターと、そのような CI が侵害された場合の**悪影響**（損害、機能喪失、データ漏洩など）を強調しており、その範囲は非常に類似している
規制対象		
CI、CIO、CCS	CI と CIO	*主な類似点：*どちらの法律も CIO に第一義的な義務を課している *注目すべき相違点：*PRC の見解には、CCS のための独立したカテゴリーがなく、管轄区域内または管轄区域からアクセス可能なシステムに関する明示的な言及もない
担当規制当局		
重要な権限： 重要インフラ（コンピュータ・システム・セキュリティ）（**長官**） 現在指定されているその他の当局は、**香港管理局**（HKMA）と **CA** である	**主要機関**：中国サイバースペース管理局（**CAC**） その他の当局には、公安部門や各重要産業の関連部門が含まれる	*主な共通点：*どちらの法律も、中央の主要規制機関が他の規制機関の支援を受けるという規制メカニズムを確立している *弊所コメント：*大多数の回答者の意見に沿って、HKMA と CA は、それぞれの部門におけるカテゴリー1 および

CIO および CCS を指定する主な権限はコミッショナーにあるが、指定された当局は、組織上および予防上の義務（以下のカテゴリー1 および 2 を参照）の遂行を監視する		２の義務について、熟知しており能力もあることから、CIO を規制するよう指定されている。カテゴリー3 の義務については、コミッショナーがすべてのセクターを規制する
組織の義務（カテゴリー1 の義務）		
• 香港におけるオフィスを維持 • オペレーターが変更した場合は通知する • コンピュータシステムのセキュリティ管理部門を維持する（「*十分な知識*」を有する従業員を含む）	• 事業者の合併・分割・解散の届出 • 独立した専門の安全保障管理機関を維持し、責任者を指名する	*主な共通点*：どちらの法律も、ネットワーク・セキュリティを監督する専門部署と担当者の設置を義務付けているほか、特定の種類のオペレーター変更に関する通知要件も定めている
予防義務（カテゴリー2 の義務）		
コンピュータシステムとの関連で： • 重要な変更の通知 • セキュリティ管理計画の実施 • セキュリティリスク評価を少なくとも年に 1 回実施する（これには脆弱性評価と侵入テストが含まれる）	• 重要な変更の通知 • 社内セキュリティ管理体制の構築 • 少なくとも年 1 回、サイバーセキュリティの検知とリスク評価を実施する	*主な共通点*：どちらの法律も、社内のサイバーセキュリティ計画やポリシーの策定、定期的なサイバーセキュリティ保護策の実施（その結果を規制当局に提出しなければならない）を求めている *注目すべき違い*：法案とは対照的に、PRC の見解は監査要件を特に規定していない

<table>
<tr><td>

- **少なくとも2年に1回はセキュリティ監査を実施する**

</td><td></td><td></td></tr>
<tr><td colspan="3">インシデント報告および対応の義務（カテゴリー3の義務）</td></tr>
<tr><td>

- セキュリティ・インシデントトレーニングに参加
- 緊急時対応計画の提出と実施
- セキュリティ・インシデントをできるだけ早く通知：
  - 中核機能に支障がある場合、または支障が生じる可能性がある場合、（認知から）12 時間以内
  - その他の場合は 48 時間以内（認知から）

</td><td>

- 定期的なトレーニングの実施
- サイバーセキュリティ・インシデントに対する緊急対応計画を策定
- ネットワークセキュリティインシデントや重大な脅威を迅速に報告

</td><td>

主な類似点：どちらの法律にも、同様の事故報告と対応義務が含まれている

注目すべき違い：香港法案は、事故報告の時期についてより規定的

弊所コメント：規制の目的と回答者の懸念とのバランスをとるため、法案は重大インシデントの報告タイミング（2 時間から 12 時間へ）とその他のインシデントの報告タイミング（24 時間から 48 時間へ）を緩和している

</td></tr>
<tr><td colspan="3">コンプライアンス違反に対する罰則</td></tr>
<tr><td>

一般的には：

Cat 1*	30 万～50 万香港ドル
Cat 2	30 万～50 万香港ドル

</td><td>問題となる犯罪にもよるが、罰則は通常 100,000～1,000,000 人民元</td><td>*弊所コメント*：罰金額が過大であるとの回答者の懸念にもかかわらず、法案に示された最高罰金額は、2024 年 7 月の政府による当初の提案とほぼ一致</td></tr>
</table>

Cat 3	300 万～500 万香港ドル *事業者変更の届出を怠った場合、300 万～500 万香港ドルの罰金が科される*		

実務ではどうすればいいのか？

もし貴社が CIO なら、あるいは CI を運営しているなら

政府が公表した協議報告書によると、CIO と CCS は段階的かつ漸進的に指定される見込みである。アクションポイントとして、既存の情報セキュリティとサイバーセキュリティの枠組みは、既存の運用と対応手順を統合して構成することにより、組織が３つのカテゴリーの義務へのコンプライアンスを確保するための良い出発点となるだろう。

法案に基づく第一義的な責任は CIO が様々な義務を遵守することにあるが、CIO は香港内または香港からアクセス可能なコンピュータ・システム（事業者の管理下にあるか否かを問わない）が法案に基づく要件に準拠していることも保証しなければならないことに留意すべきである。実際には、CIO および CI の顧客は、法案に照らして既存のサプライヤーとの契約関係を見直し、補償、監査、解約権、サービスレベルの保証など、十分かつ強固な契約上の権利が提供されるようにすることが期待される。これは、香港個人データ（プライバシー）条例（Cap.486）に基づくデータ利用者とデータ処理者の関係（データ利用者がデータ処理者の作為・不作為に対してどのように責任を負うかなど）と同様である。

CIO または CI にコンピュータ・システム・サービスを提供する場合

他方、第三者サービス・プロバイダー（IT、クラウド、アウトソーシング・サービス・プロバイダーなど）は、CIO や CI の顧客が法案に基づく法定義務の「フロー・ダウン」を求める場合、ある程度の「間接的規制」を期待する必要がある。公開協議では、CIO が第三者のサービスプロバイダー（特に外国のサービスプロバイダー）に対して負う責任について懸念を表明する回答者が何人かいたが、この立場は法案でも維持され、「デューディリジェンス」の履行と「合理的な努力」についてのさらなる規定とガイドラインが、その後の実施規範に盛り込まれることになっている。このような観点から、CIO または CI 顧客に対し、法域を超えたサービス取り決めを提供す

る供給者について、法案と中国の見解が類似していることを考慮すると、これら２つの法域にまたがる供給者の重要インフラ義務を調和させる市場慣行が現れるかどうかは、まだ分からない。

結論

結論として、この法案は CI と CCS を明確に定義し、CIO の責任を概説することで、香港のサイバーセキュリティの枠組みを強化する重要な一歩となる。この法案はまた、香港を世界のサイバーセキュリティのトレンドに合致させ、相互の結びつきが強まる世界において重要なインフラを保護するという香港のコミットメントを強化するものである。コンプライアンスの観点からは、この点に関する香港と中国の立場の類似性は、調和の取れたアプローチの有用なケースとなり得るが、いずれにせよ、事業者もサービス・プロバイダーも、近い将来、さらなる明確化、将来のガイドラインや慣行規範に目を光らせておく必要がある。

著者＆翻訳

Wilfred Ng

Partner

+85222486116
wilfred.ng@twobirds.com

Danny Leung

Partner

+85222486067
danny.leung@twobirds.com

James Gong

Legal Director

+861059335699
james.gong@twobirds.com

Hwee Yong Neo

Senior Managing Associate

+85222486054
hweeyong.neo@twobirds.com

Olivia Cheng

Associate

+85222486121
olivia.cheng@twobirds.com

Ying Zhong

Associate

+861059335511
ying.zhong@twobirds.com

音琴涼子

日本グループ部長

+852 2248 6126
Ryoko.nekoto@twobirds.com

twobirds.com

Abu Dhabi ● Amsterdam ● Beijing ● Bratislava ● Brussels ● Budapest ● Casablanca ● Copenhagen ● Dubai ● Dublin ● Dusseldorf ● Frankfurt ● The Hague ● Hamburg ● Helsinki ● Hong Kong ● London ● Lyon ● Madrid ● Milan ● Munich ● Paris ● Prague ● Rome ● San Francisco ● Shanghai ● Shenzhen ● Singapore ● Stockholm ● Sydney ● Tokyo ● Warsaw