台湾のサイバーセキュリティ法 の概要

著者：ジョン・イーストウッド、ネイサン・スナイダー、ウエンディー・チュー、
デービッド・ローゼンタール、ロイド・Ｇ・ロバーツⅢ

１．管理のための法律や規則

台湾には、情報セキュリティに関する 2 つの主要な法律があります。一つはサイバーセキュリティに関する法律、もう一つは個人データを保護する法律です。

個人データ保護法（主に PDPA）の情報セキュリティの部分は、個人データの収集、保存、処理にのみに適用される一方で、サイバーセキュリティ法（主にサイバーセキュリティ管理法（CSMA））の要件は、データを管理する法人のステータスに応じて適用されます。金融セクターを管理する規制など、特定のセクター固有の規制はより広範囲に適用されます。

1.1　法律

一般的な法律

- 2018 年 6 月に発表されたサイバーセキュリティ管理法（CSMA）は、台湾のサイバーセキュリティに関する法律の中核を成すものです。そして 2019 年 1 月 1 日に施行された以下の規則及び規制によりさらに特定されています：
  - サイバーセキュリティ管理法施行規則（CSMA 施行規則）
  - 特定の非政府機関のサイバーセキュリティメンテナンス計画実施の監査に関する規則（監査規則）
  - サイバーセキュリティ事件の通知と対応に関する規則（事件に関する規則）
  - サイバーセキュリティ情報共有規則
  - サイバーセキュリティ責任レベルの分類に関する規則（分類規則）

- 2015 年 12 月に改正された個人データ保護法（PDPA）には、個人データに関する情報セキュリティ関連の規制が含まれています。すなわち、そのようなデータは、データのセキュリティの確保のために"適切なセキュリティ対策"が取られていることを前提としてのみ、収集、処理、使用することが許可されています。PDPA（個人データ保護法）の施行規則は解釈のための重要なガイダンスを提供しており、2016 年 3 月に公布されました。
- 刑法
- 通信セキュリティおよび監視法
- 国家安全保障法
- マネーロンダリング規制法
- テロ対策融資法

セクター別の法律

- 中華民国の銀行法
- 電子プリペイドカードの発行管理法
- 電子決済ビジネスの管理を規制する規則
- クリアリングハウスの個人情報ファイルのためのセキュリティ対策プランを管理する規制
- 銀行間のファンド送金や決済に従事する金融情報サービス企業の承認や管理に関する規定
- 金融機関業務のアウトソーシングのための内部オペレーティングシステムや手続きを管理する規定
- 金融持株会社および銀行の内部監査や内部制御システムの施行規定

● 保険代理店、保険会社、および保険ブローカー会社のオンライン保険事業やオンライン保険サービスを管理する規制
● モバイルブロードバンドビジネスの管理に関する規制
● 戦略的ハイテク商品の輸出入管理規制
● ツーリスト（観光）ホテル企業プランにおける個人情報ファイルのセキュリティ維持管理に関する規制
● 人事リクルート業界における個人情報ファイルセキュリティメンテナンス計画と処理方法に関する規制
● 旅行代理店による個人情報ファイルのセキュリティ保護プランと処理に関する管理規定

1.2.監督当局

- 金融監督管理委員会 ("FSC")
- 国家通信委員会 ("NCC")
- 国家安全保障局
- 内務省
- 外務省
- 国防省
- 経済省
- 中央銀行
- 特定の産業セクターを担当するその他の規制機関

1.3 規制当局ガイダンス

- CSMA(サイバーセキュリティ管理法)に基づく一般的なガイドラインには、サイバーセキュリティ責任の分類に関する規則、サイバーセキュリティ事件の報告と対応に関する規則、特定の非政府機関のサイバーセキュリティメンテナンスプログラムの実行状況の検査に関する規則、サイバーセキュリティ情報共有規則があります。
- また、CSMA(サイバーセキュリティ管理法)によると、多くの特定の業界セクターの規制当局は独自のサイバーセキュリティ管理ガイドラインを発行しています。

2.適用範囲

A. サイバーセキュリティ管理法

CSMA（サイバーセキュリティ管理法）の下では、軍事、インテリジェンス機関 （諜報・情報機関）を除く政府機関やいわゆる"特定非政府機関 "のための、サイバーセキュリティ要件を規定しています。これらの非政府機関とは重要不可欠なインフラストラクチャプロバイダー、国営企業、政府からの寄付を受けた財団であります。さらに、CSMA（サイバーセキュリティ管

理法）はアウトソーシングの要件を定めています。 そのため、CSMA（サイバーセキュリティ管理法）は、軍事請負業者またはインテリジェンス機関（諜報）請負業者（または下請け業者）には、これらの請負業者自身が特定の非政府機関として区分されていない限り、適用されません。

CSMA（サイバーセキュリティ管理法）によって課される義務とは下記の 3 つの大きな段階に分かれます：

1. 年次報告を含むサイバーセキュリティメンテナンス計画の実施
2. サイバーセキュリティメンテナンス計画の施行が不十分な場合の改善要件を含む、同メンテナンス計画の実施に関する年次監査
3. サイバーセキュリティ事件の対応処理と報告

民間セクターに関しては、CSMA（サイバーセキュリティ管理法）は、重要不可欠なインフラストラクチャプロバイダー（そしてサイバーセキュリティシステムのセットアップまたは維持管理が外部へ委託されている当事者またはサイバーセキュリティサービスを CSMA の対象となる機関に提供している当事者）のみに適用されます。重要不可欠なインフラストラクチャプロバイダーとは「関連業界を担当する中央当局により指命され、重要不可欠なインフラストラクチャの全体または一部を維持管理するまたは提供する」会社または個人です。重要不可欠なインフラストラクチャとは、CSMA（サイバーセキュリティ管理法）第３条７項において、「いったんその運用が中止されるまたは効果が低下すると、国家安全保障、公益、市民の生活水準および経済活動に重大な悪影響をもたらすことになる物理的または仮想の資産、システム、ネットワーク」であると定義されています。

これまでに、CSMA（サイバーセキュリティ管理法）を起草する際には、以下のインフラストラクチャ分野が重要不可欠なものであるとみなされています。

- エネルギー
- 水資源
- コミュニケーション（通信）
- 輸送
- ファイナンス
- 救急医療
- 中央および地方政府機関
- サイエンスパーク

2.1. ネットワークと情報システム

CSMA（サイバーセキュリティ管理法）

CSMA（サイバーセキュリティ管理法）第 3 条1項では、情報通信システムやサービスを、「情報の収集、制御、送信、保存、流通、削除のために使用する、またはその他のプロセスをパフォームする、そのような情報を使用するまたは共有するために使用する」システムまたはサービスとして定義しています。

2.2.重要不可欠な情報インフラストラクチャ事業者

CSMA（サイバーセキュリティ管理法）

通信インフラストラクチャは重要不可欠とみなされています。それゆえ、管轄当局により重要不可欠なインフラストラクチャプロバイダーとして指定されている限り、これらの事業者に対して CSMA（サイバーセキュリティ管理法）が適用されます。

さらに、重要不可欠な情報インフラストラクチャ事業者が政府機関または特定の非政府機関に対して外部委託サービスを提供する場合、CSMA（サイバーセキュリティ管理法）および関連規則が重要不可欠な情報インフラストラクチャ事業者に間接的に適用される場合があります。

2.3.　必須サービス事業者

CSMA（サイバーセキュリティ管理法）

エネルギー、水、輸送、救急医療のインフラストラクチャは重要不可欠であると見なされています。従って、これらの事業者は管轄当局により重要不可欠なインフラストラクチャプロバイダーとして指定されている限り、CSMA（サイバーセキュリティ管理法）がこれらの事業者に適用されます。

2.4　クラウドコンピューティングサービス

CSMA（サイバーセキュリティ管理法）

通信インフラストラクチャは重要不可欠であると見なされています。従って、これらのサービスプロバイダーは、これまで管轄当局により重要不可欠なインフラストラクチャプロバイダーとして指定されている限り、CSMA（サイバーセキュリティ管理法）がこれらのサービスプロバイダーに適用されます。

さらに、クラウドコンピューティングサービスプロバイダーが政府機関または特定の非政府機関に対してアウトソーシングサービスを提供する場合、CSMA（サイバーセキュリティ管理法）および関連規則がクラウドコンピューティングサービスプロバイダーに間接的に適用される場合があります。

金融機関では、クラウドサービスの使用と国境を越えたデータ転送も特に規制されています。金融機関の顧客データは、台湾でローカルに保存されたバックアップコピーが必要です。

2.5. デジタルサービスプロバイダー

A. CSMA（サイバーセキュリティ管理法）

通信インフラストラクチャは重要不可欠であると見なされています。従って、これらの事業者が、管轄当局により重要不可欠なインフラストラクチャプロバイダーとして指定されている限り、CSMA（サイバーセキュリティ管理法）がこれらの事業者に適用されます。

さらに、デジタルサービスプロバイダーが政府機関または特定の非政府機関に対してアウトソーシングサービスを提供する場合、CSMA（サイバーセキュリティ管理法）および関連規則がデジタルサービスプロバイダーに間接的に適用される場合があります。

2.6. その他

CSMA（サイバーセキュリティ管理法）に基づくアウトソーシング

CSMA（サイバーセキュリティ管理法）第 9 条によると、CSMA の規制対象となる機関は、情報または通信システムのセットアップまたは維持管理、あるいは情報および通信サービスの提供を外部委託することが出来ます。アウトソーシングの際、代理店は提供されるサイバーセキュリティ維持管理サービスを監督する責任を依然として負うことになり、そしてそれゆえ、CSMA（サイバーセキュリティ管理法）および関連規則により提供される債務の遵守にも責任を負うことになります。即ち、CSMA（サイバーセキュリティ管理法）施行規則第 4 条は選択基準とアウトソーシング要件を特定しています。サービスプロバイダーは、サイバーセキュリティ管理対策を実施したこと、および有資格のサイバーセキュリティの人材を確保していることを示す必要があります。さらに、国家安全保障情報に関する場合は、安全保障の身元調査を実施する必要があり、カスタマイズされたソフトウエア開発はセキュリティテストを行う必要があり、サービスプロバイダーはアウトソーシング機関に対し、いかなるサイバーセキュリティ事件をもそれが発覚された時点において、通知する義務があります。アウトソーシング機関はさらに、そのサイバーセキュリティ対策の実施状況についてサービスプロバイダーを監査することが可能でなければなりません。

3. 要件

3.1. セキュリティ対策

A. CSMA（サイバーセキュリティ管理法）

CSMA（**サイバーセキュリティ管理法**）第 16 条は、サイバーセキュリティ責任レベルの分類に関する規則と同規則に付随する 10 つの付則規定に記載されているように、重要不可欠なインフラストラクチャプロバイダーに対しサイバーセキュリティ責任レベルの要件を満たすことを課しています。これらの規則は、A から E までの５段階のサイバーセキュリティ責任を規定しており、またこの責任を果たすために実行する必要のあるセキュリティ対策を規定しています。 重要不可欠なインフラストラクチャプロバイダーのサイバーセキュリティ責任レベルは、その規

模、分野、その事業の代替可能性、および事業が中断された場合に発生する潜在的影響に基づいて決定されます。（分類規則第 4 条から第 10 条）。

プロバイダーは、責任レベルに基づき、管理、テクノロジー、認識、トレーニングを通じて、様々な度合いの制御を実行しなければなりません。制御対策には、CNS27001 や ISO27001 などの国際的に認められた標準の適用、専任のサイバーセキュリティ人材の採用、年 2 回の内部サイバーセキュリティ監査の実施、特定の第三者製品使用に対する制限、コアシステムの定期的なテスト、サイバーセキュリティ防御ソフトウエアとメカニズムのインストール、およびすべての情報担当者のサイバーセキュリティに対する認識を確証することが含まれるかもしれません。（分類規則付則 1～8）。

サイバーセキュリティの責任レベルとは関係なく、プロバイダーのサイバーシステム防御レベル（高、中、一般）は、プロバイダーの機密性、整合性、可用性、または規制コンプライアンスのうちの少なくとも 1 つに関連して最も高いレベルの要件に見合ったものでなければなりません。（分類規制付則 9）。この防御レベルに基づいて、プロバイダーは、数あるなかでも特に、アクセス制御、ビジネス継続性、ユーザーの身元　（ID）とその確証、システムと情報の整合性などに関して、そのサイバーシステムのための最小要件を決定します。（分類規則付則 10）業界によっては、その業界を担当する中央当局により発行されたサイバーシステムの追加のあるいはその他の防衛基準が存在する場合があります。

B.　個人データ保護法

PDPA（個人データ保護法）　は、個人情報の機密性を保持し、個人のプライバシーを保護するための特定のセキュリティ基準を設定していません。しかしながら、PDPA（個人データ保護法）の施行規則において、個人データを取り扱うエンティティが採用できるメカニズムの種類がより明確になっています。その上、ビジネスの本質　（金融業界、旅行および観光、電気通信、人事機関など）に応じて、より厳格な基準を提供するいくつかのセクターに対して、業界固有のガイドラインが発行されています。

PDPA（個人データ保護法）の施行規則第 12 条には、個人データの収集者または処理者が採用したセキュリティ対策が適切かどうかを評価するための 11 要素が記載されています。以下が 11 要素です：

１．経営管理者と合理的なリソースの割り当て
２．個人データの範囲を定義する
３．個人データのリスク評価と管理のメカニズムを確立する
４．データ侵害を防止する、通知する、侵害に対応するメカニズムを確立する
５．個人データの収集、処理、使用のための内部制御手順を確立する
６．データセキュリティと人員の管理
７．意識向上、教育、トレーニングを促進する
８．施設のセキュリティを管理する
９．データセキュリティの監査メカニズム確立する
１０．記録、ログファイル、および関連する証拠を保持する

１１．個人データのセキュリティとメンテナンスに関する統括された持続的改善を実行する

3.2. サイバーセキュリティ事件の通知

A. CSMA（サイバーセキュリティ管理法）

CSMA（**サイバーセキュリティ管理法**）第 18 条では、サイバーセキュリティ事件が発生した場合、事件に気付いてから 1 時間以内に規制当局に通知する義務を重要不可欠なインフラストラクチャプロバイダーに課しています（事件規制第11条ではさらに詳細が規定されています。）このような事件は、システム、サービス、またはネットワークの状態がサイバーセキュリティポリシーを違反している、またはセキュリティ対策の失敗を示している場合が多く、それが情報通信システムに悪影響を及ぼし、それゆえサイバーセキュリティへの脅威となるイベントであると広く理解されています。この通知には、事件発生時刻、状況の説明、事件に対する対応策、事件のレベルの評価などの詳細を含めなければなりません。 サイバーセキュリティ事件の通知と対応に関する規則によると、事件には４つのレベルがあり、事件が発生した場合の責任は様々です。これらのレベルは、事件の影響を受けたビジネス、事件の重症度、および特に重要不可欠なインフラストラクチャへの潜在的な影響に基づいて決定されます。（事件規則第 2 条）

プロバイダーは、事件のレベルに応じて、事件に気付いてから 36 時間または 72 時間以内に損害の制御または回復を完了しなければなりません。以上が完了したら、プロバイダーは事件をさらに調査、管理し、その関連業界を担当する中央当局に対しその報告書を提出する必要があります。この報告書には事件に対応して講じられた改善対策が記載されます。（事件規則第 13 条）。この調査、管理、改善のレポートは 1 か月以内に提出する必要があり、事件の時間枠、損害評価、事件の原因分析、および同様事件の再発防止のために講じられた対策の詳細などの様々な詳細が記載されたものでなければなりません。 （CSMA（**サイバーセキュリティ管理法**）施行規則第 8 条）

B. 個人データ保護法

PDPA（個人データ保護法）の下では、個人データの侵害が発生した場合、規制当局に通知する義務はありません。これは第12条で、「個人データが盗まれた、開示された、変更された、さもなければPDPA違反により個人データが侵害された」いかなる場合であるものと定義されています。しかしながら、個人データの保有者は、「関連事実が明らかにされた後」影響を受けたデータ主体に対して通知しなければなりません。要件が満たされた通知には、「データ侵害に関連する事実と、そのような侵害に対処するためにすでに採用された対応措置」が記載されていなければなりません。（PDPA（個人データ保護法）施行規則第 22 条）

3.3 規制当局への登録

CSMA（サイバーセキュリティ管理法）の直接の適用対象となる民間セクター、つまり重要不可欠なインフラストラクチャプロバイダーは、関連業界を担当する中央当局によって指定されます。そのため、規制当局に登録することは要求されていません。ただし、その指定が正式に決定される前に、プロバイダーは当件について意見を申し立てる権利があります。（CSMA（サイバーセキュリティ管理法）施行規則第 9 条）

3.4 セキュリティ・オフィサーの任命

A. CSMA（サイバーセキュリティ管理法）

CSMA（サイバーセキュリティ管理法）の下では、政府機関のみがサイバーセキュリティオフィサーを指名することが要求されており、企業にはその義務はありません。ただし、サイバーセキュリティの責任レベルによっては、重要不可欠なインフラストラクチャプロバイダーは、関連する専門資格およびビジネス経験を有する専任のサイバーセキュリティ人材を雇用することを法的に義務付けられる場合があります。

B. 個人データ保護法

同様に、PDPA（個人データ保護法）の下では、政府機関のみが個人情報セキュリティオフィサーを任命することを明示的に義務付けられています。 （第 18 条）ただし、PDPA（個人データ保護法）施行規則によると、セキュリティ管理職の任命は、適切なプライバシー保護計画で推奨される要素の一つとなっています。さらに、業界固有の規制の下では、登録または報告の要件に準拠するために、専門家を雇用することが要求されることがあります。

3.5 その他

サイバーセキュリティ・メンテナンス計画

CSMA（サイバーセキュリティ管理法）第 16 条の下では、重要不可欠なインフラストラクチャプロバイダーは、サイバーセキュリティメンテナンス計画を実行することが要求されています。これには、プロバイダーのサイバーセキュリティ関連のポリシーとメカニズム、コアビジネスの特定、情報とシステムのインベントリー、アウトソーシングされたシステムとサービスに対して設置された大規模なリスク評価と管理措置などの項目が含まれることが義務付けられています。 （CSMA（サイバーセキュリティ管理法）施行規則第 6 条）このサイバーセキュリティメンテナンス計画は、プロバイダーがサイバーセキュリティ債務を履行するための基盤を構築するものであり、監査プロセスを通じて当局が管理するための基盤としても機能しています。さらに、重要不可欠なインフラストラクチャプロバイダーは、サイバーセキュリティメンテナンス計画の実行状況について毎年報告しなければなりません。

重要不可欠なインフラストラクチャプロバイダーは、彼らのサイバーセキュリティメンテナンス計画の実行に関する年次監査に協力することが義務付けられています。これらの監査は日程が立てられており、不可抗力の場合を除いて、監査プログラムの通知を受けてから 5 日以内に書面による通知によって 1 回のみ延期することができます。（監査規則第 4 条） このような監

査を行う中で、所管当局はサイバーセキュリティメンテナンス計画の実施状況をレビューし、当該監査の対象者に対して、監査前のインタビューおよびオンサイトで行う物理的監査に協力するように、ならびに説明、関連文書や補足情報を提供するよう要求する場合があります。（監査規則第５条）

サイバーセキュリティメンテナンス計画の実施において、その監査結果が要件を満たしていない、または欠陥を示している場合、重要不可欠なインフラストラクチャプロバイダーは、監査結果を受け取ってから１か月以内に改善レポートを提出することを要求されるでしょう。（監査規則第 8 条）。この改善報告書には、改善すべき欠陥または項目、その欠陥の発生原因、講じられる具体的な改善措置、これらの措置のための推定タイムライン、および実行の進捗状況を追跡するためのメカニズムが記載されている必要があります。　（CSMA（サイバーセキュリティ管理法）施行規則第 3 条）

サイバーセキュリティ演習

監査と同様に、重要不可欠なインフラストラクチャプロバイダーは、サイバー攻撃やサイバー防御などのサイバーセキュリティ演習、またはシナリオ演習を実施することも要求されています。（事件規則第 19 条）これは、特定の非政府機関によつて実施されなければならない、サイバーセキュリティ責任レベル A,B,C に分かれた、隔年ごとに行われるシステムペネトレーションのテストに関連しています。（分類規則、付則 2、4、および 6）しかしながら、これはサイバーセキュリティ責任レベルに関係なく、すべての重要不可欠なインフラストラクチャプロバイダーに対してサイバーセキュリティの演習が義務付けられます。

モバイルブロードバンド事業者は、モバイルブロードバンド事業管理規則　（第 83 条 1 項）に基づき、システムの弱点を定期的に調査するためのペネトレーションテストを実施することが義務付けられています。

4.　セクター固有の要件

ヘルスセクターにおけるサイバーセキュリティ

ヘルス産業を担当する中央当局は厚生省です。2019 年 4 月 24 日に厚生省により発行された行政規則によると、厚生省が担当するすべての重要不可欠なインフラストラクチャプロバイダーは毎年 1 月 31 日までにサイバーセキュリティメンテナンス計画を提供し、毎年 12 月 31 日までに、サイバーセキュリティメンテナンス計画の実施を報告する義務があります。厚生省はまた、CSMA（サイバーセキュリティ管理法）に従い重要不可欠なインフラストラクチャプロバイダーを監査します。

金融セクターにおけるサイバーセキュリティ

金融機関、電子プリペイドカードの発行者、および電子決済を取り扱う企業は、中央銀行そして共同信用情報センター（JCIC）と彼らの情報セキュリティ対策を標準化するために連携し、また定期的な監査の際、または違反事件が発生した場合は、中央預金保険会社や金融監督管理委員会（FSC）に対して追加で報告または登録しなければなりません。

オンラインでビジネスを行う保険会社は、ビジネスを行うためのライセンスを取得するために、ISO 27001 認定を受け、分散型ドス攻撃（DDOS）に対するトラフィッククリーニングメカニズムを確立しなければなりません。

従業員のためのサイバーセキュリティプラクティス

雇用者／従業員の関係に関して適用される特定のサイバーセキュリティ規制はありません。台湾の労働基準法では、雇用者が雇用関係の終了後 5 年間は従業員の記録を保持することを義務付けています。雇用者は、PDPA（個人データ保護法）の一般的な要件に従い、これらの記録の機密性の安全を確保する必要があります。

教育セクターにおけるサイバーセキュリティ

教育産業を担当する中央当局は文部省です。文部省は、2016 年に 「教育のための個人データとサイバーセキュリティ管理ガイドライン」と呼ばれるサイバーセキュリティおよび個人データの保護を規制する管理規則を発行しました。 この行政規則では、すべての学校がグレード A（例：医科大学）、B（例：大学）、または C（例：小学校／高校）に分類されています。そして、同省はサイバーセキュリティや個人データを管理するための「個人情報管理システム」または「情報セキュリティ管理システム」を構築し、そのシステムを定期的に維持・改善するための適切なリソースとスタッフを配置しています。

5. ペナルティー

A. CSMA（サイバーセキュリティ管理法）

CSMA（**サイバーセキュリティ管理法）第 20 条は、その業界を担当する中央当局により指定された期限内に是正措置を完了しなかった企業に対して、10 万台湾ドルから 100 万台湾ドルの行政罰金を規定しています。**企業がサイバーセキュリティ事件の報告を怠わった場合、CSMA（**サイバーセキュリティ管理法）第 21 条に基づき、関連中央当局は当該企業に対して 30 万台湾ドルから 500 万台湾ドルの範囲における行政罰金を課すこと、そしてその改善を命令することが可能であります。そしてもしその企業が期限内にその改善を完了しなかった場合は、追加の罰金を課される可能性があります。**

6. その他の関心分野

● 例：トラスト、注目すべき事件とサイバー攻撃、5G ネットワークのサイバーセキュリティ、IoT/AI ベースのシステムのサイバーセキュリティ、リスク管理。

NCC（国家通信委員会）は 2019 年に電気通信事業者に対し 5G ライセンスをリリースし、現在、同事業者に対して、サイバーセキュリティメンテナンス計画を提供すること、そしてモバイルブロードバンドビジネス管理規則に関連する厳格なサイバーセキュリティ規則に遵守することを要求しています。

中央政府は、新型コロナウイルス感染症　（Covid-19）のパンデミックの間は、サイバーセキュリティの懸念に基づいて、すべての政府機関に対して、人気のあるビデオ会議サービスを使用することを禁止しました。

台湾における一般的なサイバーセキュリティ法の斬新性により、このような全面的な禁止が発令されたのはこれまでに初めてのことであったでしょう。

著者：

ジョン・イーストウッド
john.eastwood@eiger.law

ウエンディー・チュー
wendy.chu@eiger.law

ネイサン・スナイダー
nathan.snyder@eiger.law

デービッド・ローゼンタール
david.rosenthal@eiger.law

ロイド・G・ロバーツ III
lloyd.roberts@eiger.law