企業のDXにおける新たなサイバーセキュリティ

新規事業／顧客向けサービスにおけるセキュリティ
リーンセキュリティ 後編

PwCコンサルティング合同会社　ディレクター　小林 公樹

前編では、リーンスタートアップの考え方の登場とビジネスのアジャイル化の背景と共に、従来型コーポレートセキュリティとデジタルビジネスのセキュリティの特性の違いから事業スピードを重視するデジタルビジネスの事業部門と安全を重視するセキュリティ部門の対立が発生すること、これを解消し得る、スピードと安全を両立してセキュリティを検討するための新しい方法論「リーンセキュリティ」の必要性を説明しました。第2回では「リーンセキュリティ」を導入するにあたっての主要な検討ポイントを説明します。

リーンセキュリティを導入するには？

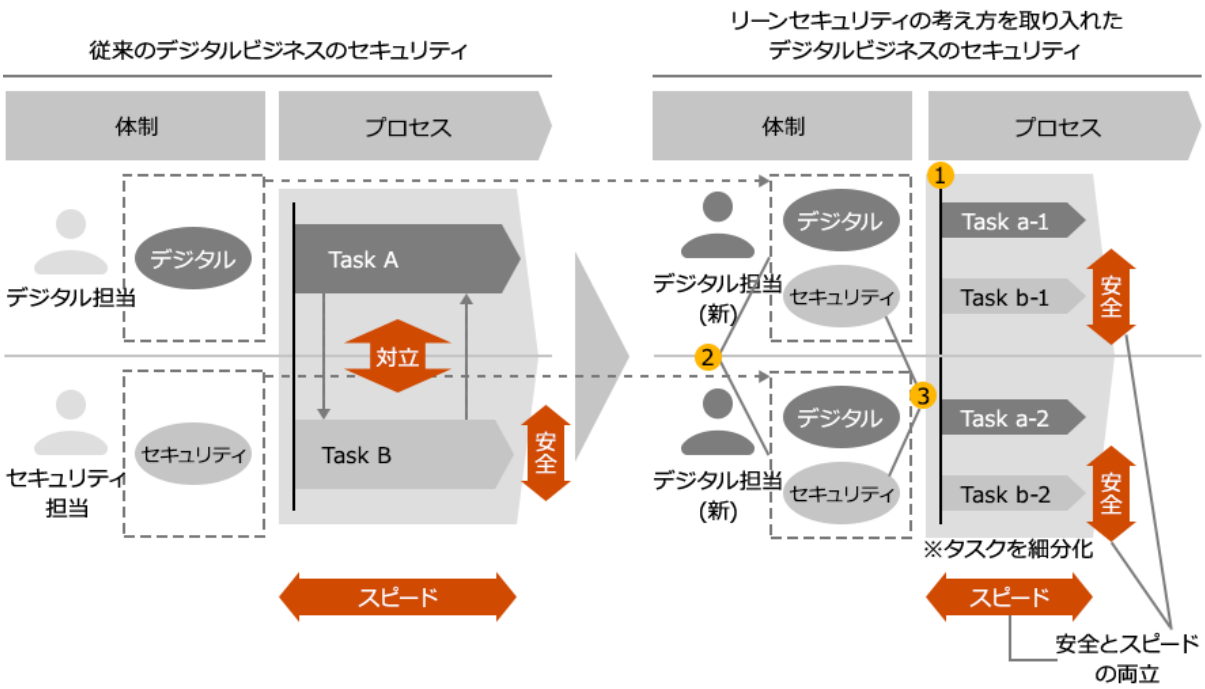
ポイントを3点説明します。

1. デジタルビジネスのサービス企画段階でのセキュリティの検討
2. デジタルビジネス担当者のデジタル＋セキュリティのスキルセット所持
3. ビジネス部門のセキュリティに関する説明責任の明確化

それぞれについて、セキュリティ対策の各ステップで検討および実施すべき内容と共に紹介します。

リーンセキュリティの考え方

・リーンセキュリティの考え方を取り入れることで担当者間の対立をなくし、スピードを落とさずセキュリティを検討できる。



リーンセキュリティの考え方	① デジタルビジネスのサービス企画段階でのセキュリティの検討
	② デジタルビジネス担当者はデジタル＋セキュリティのスキルセット所持
	③ ビジネス部門のセキュリティに関する説明責任の明確化

1. デジタルビジネスのサービス企画段階でのセキュリティの検討

デジタルビジネスの構想や予算化などのサービス企画の初期段階からセキュリティの検討を開始すべきです。これにより安全性や、信頼性、プライバシーやデータ倫理に関連するリスクを予防的に管理することができるようになります。また、同様に業務要件定義、システム要件定義段階においても、セキュリティの検討を漏れなく実施すべきです。結果としてデータセキュリティ、プライバシーなどの要件漏れによる手戻りを抑制し、セキュリティ対策の高速化を実現することができます。

検討ステップ:

- デジタルビジネス推進のプロセスとタスクを検討する。構想、予算化、業務要件定義、システム要件定義のビジネス企画段階のプロセスにセキュリティを検討するタスクが含まれているかを確認する。

構築ステップ:

- デジタルビジネス推進のプロセスとタスクを定義する。構想、予算化、業務要件定義、システム要件定義のビジネス企画段階のプロセスにセキュリティを検討するタスクが含まれていることを確認する。

計測ステップ:

- デジタルビジネスのサービス企画段階でセキュリティの検討が十分だったかを計測する。
- 計測結果を評価する。

学習／再配備ステップ:

- 検討不十分の原因を究明し、プロセスおよびタスクを見直す。

検討ステップ	構築ステップ	計測ステップ	学習／再配備ステップ
デジタルビジネス推進のプロセスとタスクを検討する。構想、予算化、業務要件定義、システム要件定義のビジネス企画段階のプロセスにセキュリティを検討するタスクが含まれているかを確認する。	デジタルビジネス推進のプロセスとタスクを定義する。構想、予算化、業務要件定義、システム要件定義のビジネス企画段階のプロセスにセキュリティを検討するタスクが含まれていることを確認する。	・デジタルビジネスのサービス企画段階でセキュリティの検討が十分だったかを計測する。 ・計測結果を評価する。	・検討不十分の原因を究明し、プロセスおよびタスクを見直す。

2. デジタルビジネス担当者のデジタル＋セキュリティのスキルセット所持

デジタルビジネスの担当者は「デジタル＋セキュリティ」のスキルセットを所持しておくべきです。デジタルビジネスでは、アイデア創出、サービス立案、概念実証（PoC）といったビジネス企画の段階でサイバーセキュリティ、データプライバシー、データ倫理に関する課題を含めた検討が必要となります。そのため、デジタルに関する知見のみならず、セキュリティのスキルセットも求められます。

デジタル＋セキュリティのスキルセットを所持することで、組織として意思統一されたポリシー／ガイドラインの下でコンプライアンスやベースラインを遵守しつつ、個人の裁量でセキュリティを検討し、関連するリスクを予防的に管理し俊敏性を損なわずにプロジェクトを推進することができるようになります。デジタルビジネスに未着手もしくは初期段階ではビジネス部門の担当者のスキルが成熟していないため、従来のセキュリティ部門からの支援や外部専門家の活用も含めて、ビジネスへの影響を極小化しつつ、段階的なスキル向上計画の推進が求められます。

検討ステップ:

- ビジネス部門が必要なセキュリティスキルセットを検討する。
- ビジネス部門は社内／社外専門家含めセキュリティスキルセットを持つ人材の確保および配置方法の検討を行う。
- セキュリティ部門はデジタルビジネスのセキュリティ評価のための基準、プロセス、システムを検討する。
- セキュリティ部門はセキュリティスキルの評価の基準、プロセス、システムを検討する。

構築ステップ:

- 必要なスキルセットを持つ人材を配置する。
- セキュリティ部門はデジタルビジネスのセキュリティ評価のための基準、プロセス、システムを構築する。
- セキュリティ部門はセキュリティスキルの評価の基準、プロセス、システムを構築する。

計測ステップ:

- ビジネス部門はデジタルビジネスのセキュリティレベルを計測、評価する。
- セキュリティ部門はデジタルビジネスのセキュリティレベルを監査する。
- ビジネス部門は担当者のセキュリティスキルを評価する。

学習／再配備ステップ:

- ビジネス部門の担当者に不足しているセキュリティスキルセットを向上する。
- 必要なスキルセットを持つ人材をデジタルビジネスに再配置する。

検討ステップ	構築ステップ	計測ステップ	学習／再配備ステップ
・ビジネス部門が必要なセキュリティスキルセットを検討する。 ・ビジネス部門は社内／社外専門家含めセキュリティスキルセットを持つ人材の確保および配置方法の検討を行う。 ・セキュリティ部門はデジタルビジネスのセキュリティ評価のための基準、プロセス、システムを検討する。 ・セキュリティ部門はセキュリティスキルの評価の基準、プロセス、システムを検討する。	・必要なスキルセットを持つ人材を配置する。 ・セキュリティ部門はデジタルビジネスのセキュリティ評価のための基準、プロセス、システムを構築する。 ・セキュリティ部門はセキュリティスキルの評価の基準、プロセス、システムを構築する。	・ビジネス部門はデジタルビジネスのセキュリティレベルを計測、評価する。 ・セキュリティ部門はデジタルビジネスのセキュリティレベルを監査する。 ・ビジネス部門は担当者のセキュリティスキルを評価する。	・ビジネス部門の担当者に不足しているセキュリティスキルセットを向上する。 ・必要なスキルセットを持つ人材をデジタルビジネスに再配置する。

3. ビジネス部門のセキュリティに関する説明責任の明確化

デジタルビジネスの担当者は、サイバーセキュリティ、データプライバシー、データ利用ガバナンスといった最新および今後発生するコンプライアンスなどの要求事項の説明責任の所在を明確化すべきです。セキュリティの考慮の不足を抑制し、スピード感を持ったセキュリティの検討を強制するからには、ビジネス部門はビジネスリスクと共にセキュリティリスクも負うべきでしょう。例えば、ビジネス部門がセキュリティリスク対応（リスク特定、分析、対策）を実施し、セキュリティ部門はセキュリティポリシーやガイドラインを提示するといった企業組織のセキュリティ全体を統括するなど、企業ごとに適したセキュリティ領域における役割を検討し、役割に応じた責任を負うよう検討すべきです。その結果、必要に応じて組織編成の見直しや最高責任者といった役職者設置などの対応を継続的かつ柔軟に進めていくこととなります。

検討ステップ:

- ビジネス部門とセキュリティ部門におけるセキュリティ業務の洗い出しを実施する。
- ビジネス部門とセキュリティ部門におけるセキュリティ業務に対する役割（業務責任を負う、業務責任者支援、業務実施、業務実施支援など）の分担を定義する。

構築ステップ:

- 役割分担に応じた業務を遂行する。

計測ステップ:

- 役割分担が適切に実施できたかを計測する。

学習／再配備ステップ:

- デジタルビジネスにおけるセキュリティ業務に対する役割（業務責任を負う、業務責任者支援、業務実施、業務実施支援など）の分担を見直す。
- 見直した役割分担で業務を遂行する。

検討ステップ	構築ステップ	計測ステップ	学習／再配備ステップ
・ビジネス部門とセキュリティ部門におけるセキュリティ業務の洗い出しを実施する。 ・ビジネス部門とセキュリティ部門におけるセキュリティ業務に対する役割（業務責任を負う、業務責任者支援、業務実施、業務実施支援など）の分担を定義する。	・役割分担に応じた業務を遂行する。	・役割分担が適切に実施できたかを計測する。	・デジタルビジネスにおけるセキュリティ業務に対する役割（業務責任を負う、業務責任者支援、業務実施、業務実施支援など）の分担を見直す。 ・見直した役割分担で業務を遂行する。

お問い合わせ
PwCコンサルティング合同会社
〒100-6921　東京都千代田区丸の内2-6-1 丸の内パークビルディング
Tel : 03-6250-1200（代表）　Mail : jp_cyber_inquiry@pwc.com