The Institute of Financial Risk management and Audit
金融高度化ウェビナー・イブニング

ＤＸの推進と
サイバーセキュリティ

～岩手銀行の取り組み～

株式会社岩手銀行
システム部

講演概要

- デジタル化のキーワード
- サイバーセキュリティとＤＸ
- モバイルワーキング
- 境界型サイバーセキュリティ
- ローンＷｅｂ完結
- 経営支援サイト
- 電子交付サービス
- 地域eKYC
- 知財管理

岩手銀行について


鬼剣舞


岩手山


めがね橋

創立年月日	1932年5月2日
本店所在地	岩手県盛岡市
預金等	3兆4,245億円
貸出金	1兆9,043億円
自己資本比率	単体：11.44% 連結：11.83%
従業員数	1,430名
店舗数	109ヵ店
発行体格付	Ａ－（㈱格付投資情報センター）


浄土ヶ浜

講師紹介

岩手銀行 執行役員システム部長　関村淳哉（54歳）

略歴

- ✓ 1990年　岩手銀行入行
- ✓ 2009年　人事部長代理
- ✓ 2013年　システム部長代理（情報セキュリティ）
- ✓ 2015年　北東北三行共同ＣＳＩＲＴ　設立
- ✓ 2017年　システム部副部長（システム企画）
- ✓ 2019年　株式会社フィッティング・ハブ　設立
- ✓ 2020年　システム部長
- ✓ 2021年　株式会社フィッティング・ハブ　代表取締役社長（兼任）
  　　執行役員システム部長

地方銀行のビジネスモデル

- 地域密着
- 堅実経営

➡ 多くの銀行の原点

- 地域企業への与信
- 預かり資産

➡ 重要性は変わらない

地方銀行に新たなビジネスモデルが求められているのも事実

デジタル化のキーワード

クラウドへの移行

レガシー業務のデジタル化

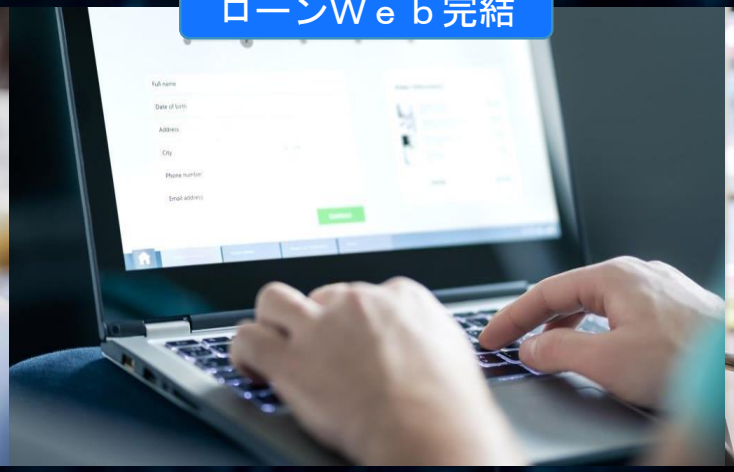
新たなビジネスの創造

非対面ビジネスの推進

弊行の主なＤＸへの取り組み

モバイルワーキング

ローンＷｅｂ完結



経営支援サイト

電子交付

地域ｅＫＹＣ

アプリの活用

ＤＸ推進のジレンマ

- 二重投資　レガシー ＋ デジタル
  - 費用対効果が出ない
  - 短期収益を追求する経営と意識にズレ
- 手段の目的化　あいまいな目的 × ＫＰＩの矮小化
  - 目的を見失い迷走
  - ＰｏＣ止まり
  - 費用対効果を軽視
- 人材不足　社内での調達難 ― 高い業務難易度
  - フリーズ
  - ベンダー丸投げ
- 横並び　他社追随 ＋ 安全志向
  - 期待先行の経営と意識にズレ

ＤＸ推進のポイント

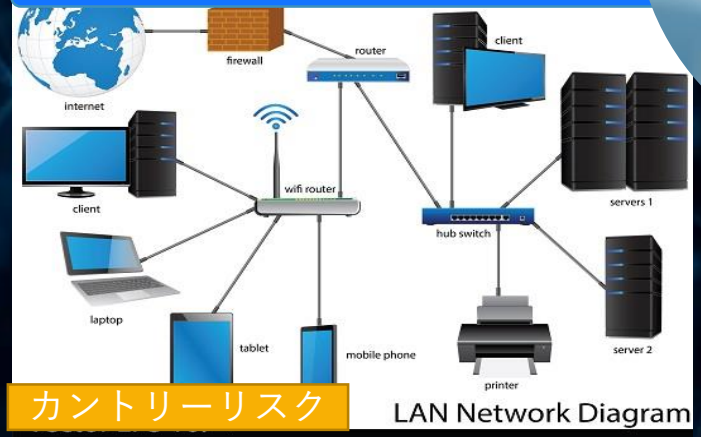
1. ＤＸというキーワードからいったん距離を置く
2. 自分が所属する組織のパーパスを具体化してみる
3. 具体化した目的を実現するための手段を考える
4. 手段選択の際、費用対効果、法令対応、サイバーセキュリティ、知財管理を常に一体で考慮する
5. ＫＰＩはパーパスに沿った指標を設定する

サイバーセキュリティのポイント

業務の重要度（詐取、脅迫のリスク）

認証、閲覧権限の設定

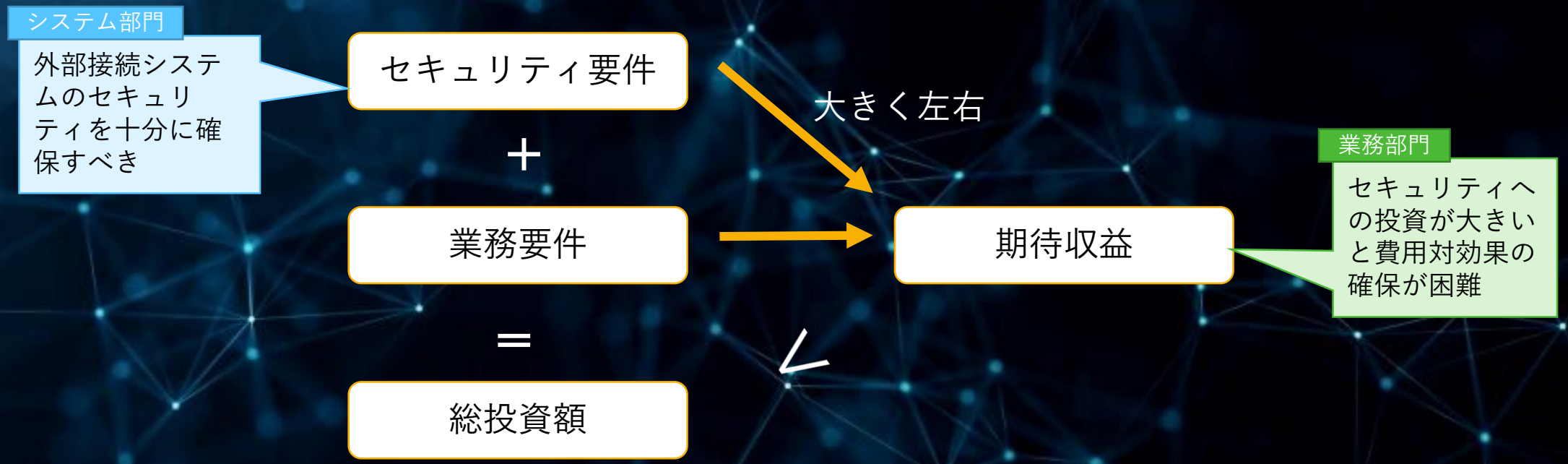
情報の保管場所と経路（ＮＷ）



カントリーリスク

継続的リスク管理、脆弱性検証

サイバーセキュリティへの投資上限

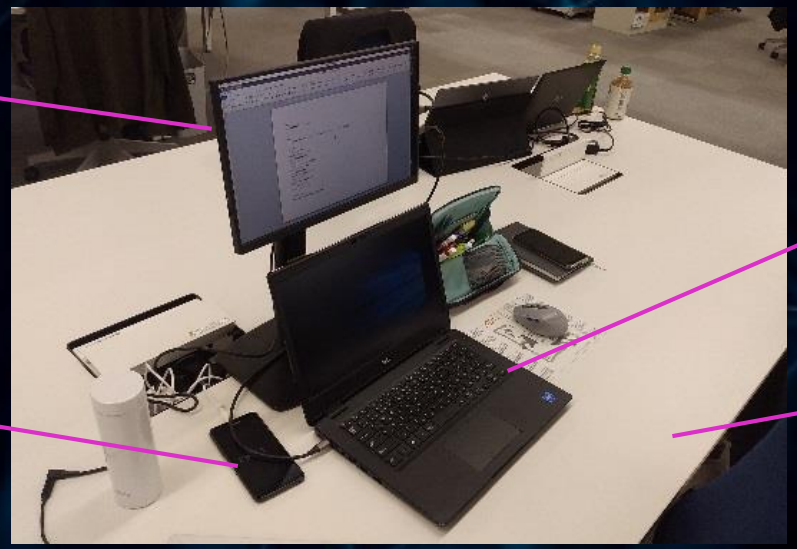


- サイバーセキュリティ単独ではなく、業務要件や期待収益（コスト削減含む）との調整でビジネスモデル全体を成立させる工夫が必要

モバイルワーキング

2020年3月

- 全職員にシンクラＰＣ＋業務用スマートフォンを配付
- ノートＰＣの半数をＬＴＥ接続
- 全店に無線ＬＡＮ環境を整備



拡張ディスプレイ

シンクラＰＣ

スマホ

フラットテーブル

- ペーパーを排除
- 引出やキャビネットを廃棄

モバイルワーキング導入の経緯

- 紙が様々なコストを生む

オフィス、机、キャビネット、倉庫	収納
コピー機、ＦＡＸ、文房具、ファイリング	編集
鍵管理、持出管理、現物管理、廃棄作業	管理
郵送、メールカー、メールセンター	移送
事務帳票システム、書類管理システム	システム

紙さえ
なければ不要

- 紙を効率よく管理できる仕組みがかえって仇に（集中管理、集中保管）
- ここまで大量の紙が事務に残っている業態は・・・
- 紙を使わないモバイルワーキングの徹底により、ファシリティコストを削減

モバイルワーキングの改善

業務フローの継続的なデジタル化

固定電話の廃止

座席の割当廃止（オフィスの有効活用）

スマホの内線電話連携

クラウド電話帳（スマホにデータを保存しない）

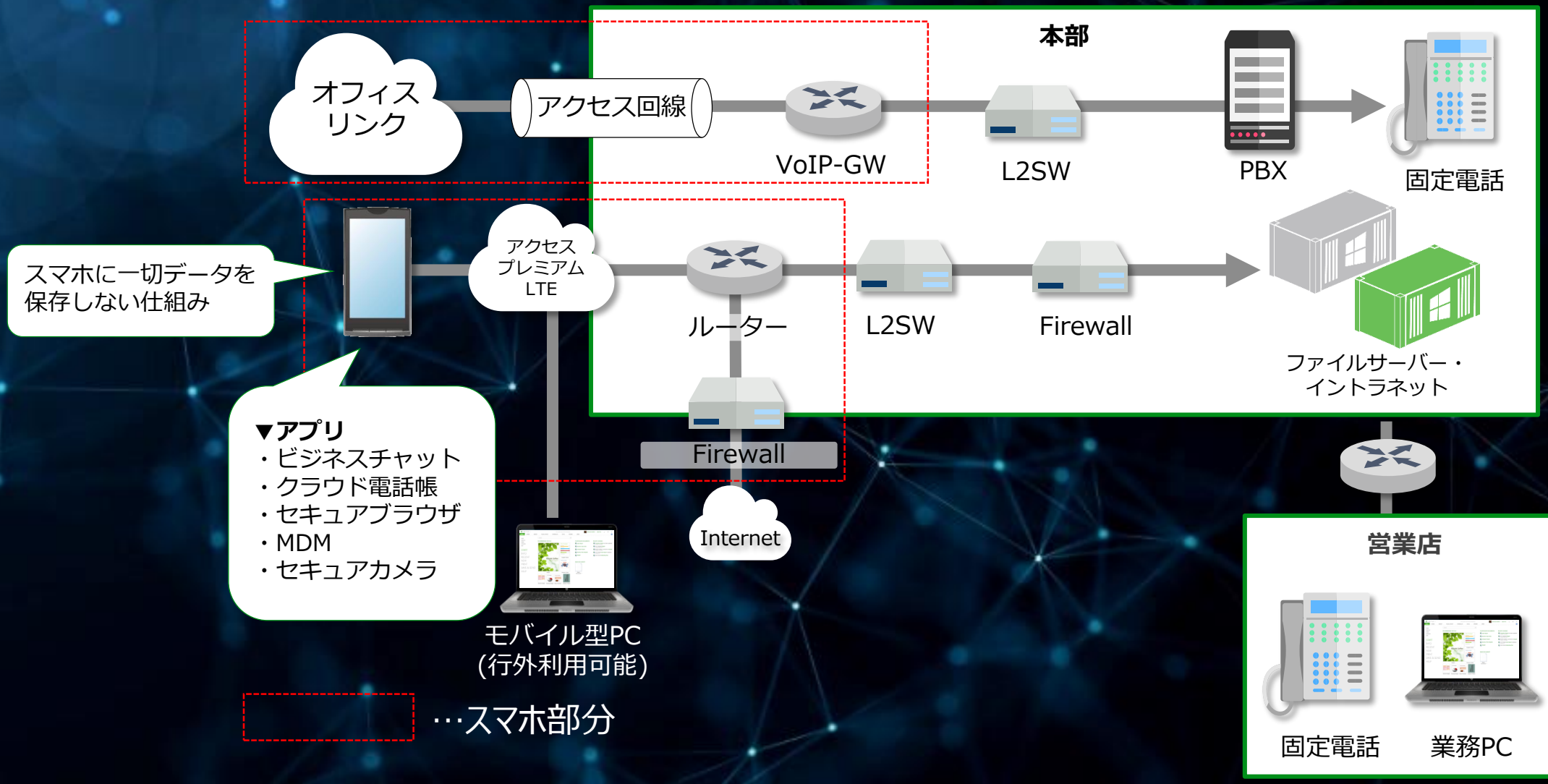
スマホでＺｏｏｍ会議

スマホで名刺管理

スマホからイントラネット利用

スマホの撮影画像を社内サーバーへ自動転送

スマートフォンのサイバーセキュリティ



スマートフォンアプリのリスク評価

リスクチェックシート抜粋

チェック項目	情報の重要度			
	高換金性 （暗証番号等）	最重要 （顧客情報）	重　要 （内部情報）	一　般 （公開情報）
業務用スマートフォンでの取扱いを禁止	○			
分散システムに準じたリスク評価		○		
分散システムに準じた外部委託先管理		○		
スマートフォンにデータを保存しない		○	○	
データの経路を全て暗号化		○	○	
情報が第三者に対して非公開		○	○	○

レギュレーションの見直し

- モバイルワーキングの課題と対応

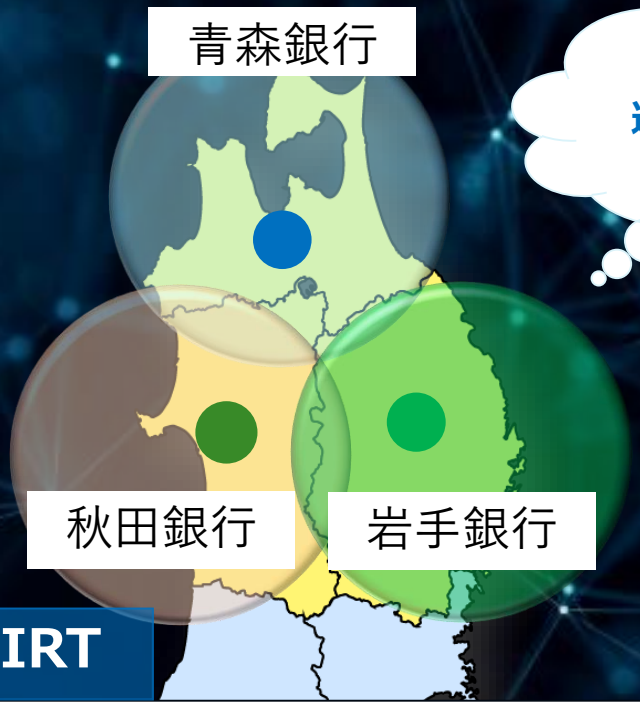
項目	課題	対応
テレワーク	• 仕事を怠けていないか、監視する仕組みが必要ではないか	• 監視ではなく、成果を評価する仕組みが必要 • テレワークと関係なく、成果主義に基づく業務設計と、単純事務の削減が必要
	• 見えていないところで情報漏洩を起こされるのではないか	• 社内であっても常に監視できるわけではない • 監視ではなく、規定の整備と教育、啓蒙が重要
	• 自宅でシステム部の行員が運用端末を操作して不正を行うのではないか	• 同上 • すでにシステムを監視する仕組みが存在
	• ＦＩＳＣの安全対策基準など、自宅勤務を想定していない規則に対応していない • 様々な規則への整理をしたうえで、実施すべきではないか	• システムと環境の変化が激しい現在において、各種規則が追随しきれないケースも多い • 規則が想定していないからダメではなく、規則の趣旨を逸脱しないことをまず考えるべき • 個々にしっかり確認して対応
	・・・・などなど	

今の時代、全てのリスクに完ぺきに対応するのは不可能

全てのリスクを考慮し、その中からリスクベースで優先順位をつける

保有リスクは定期的にチェック

共同インターネットシステム



自行単独でのCSIRT運営には限界が・・・

悪質かつ巧妙化する攻撃の最新情報の入手や個別対策が困難

セキュリティ人材の絶対的な不足

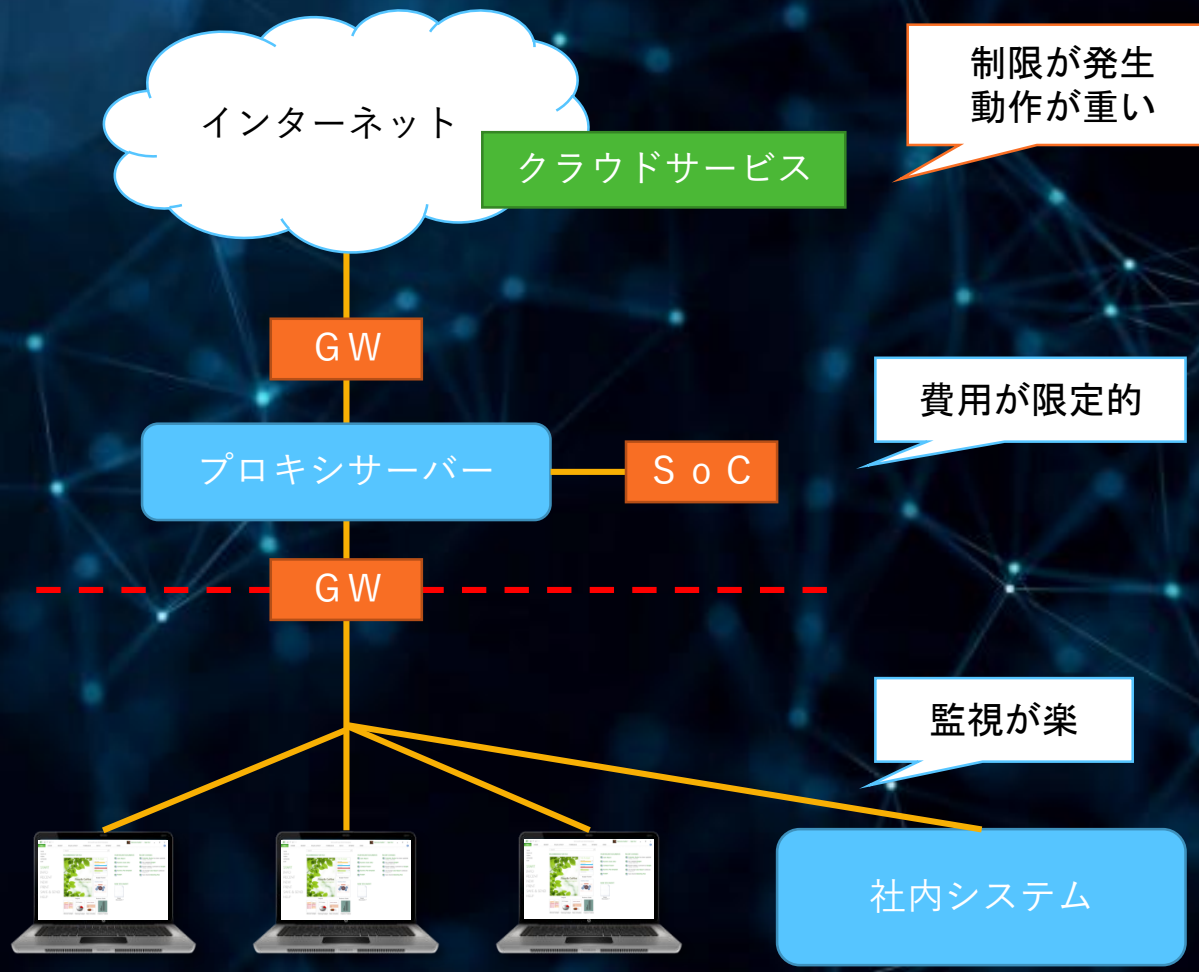
北東北三行共同CSIRT

- 2015年8月1日に『北東北三行共同CSIRT』を設立
  - ✓ インターネット接続システムの共同化
  - ✓ サイバーセキュリティ関連情報の共有
  - ✓ 相互協力体制の構築

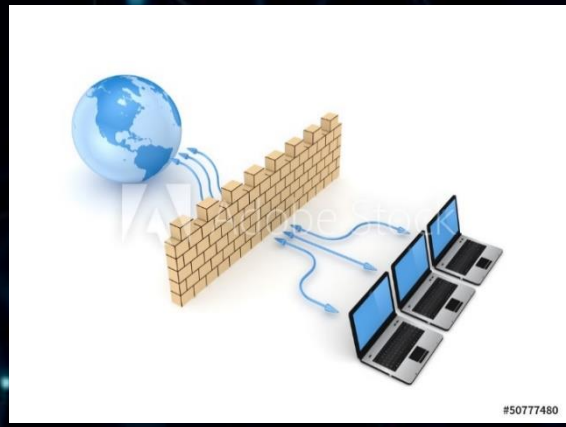
三行のサイバーセキュリティ対策レベルの底上げを実現

- 3カ月毎に幹事行のセンターで共同CSIRT定例会議を開催

境界型サイバーセキュリティ



- 境界型防御は、必ずしもゼロトラストの対義語ではない
- 一口に境界型防御といっても、様々なパターンがある
- 従来の境界型防御は境界より内部を守らないケースも多かったが、現在は、様々な監視システムや防御システムを導入しているケースも



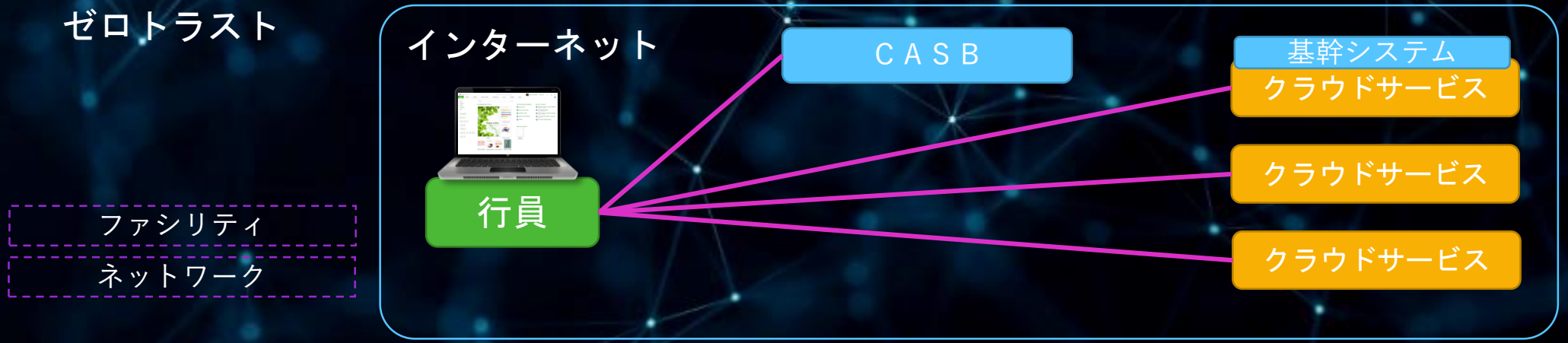
境界型防御の課題

- クラウドの積極活用には、ＣＡＳＢがほぼ必須
  Cloud Access Security Broker
- 境界型＋ＣＡＳＢは不可能ではないが、多くの場合、二重投資の恐れも
- ネットで新たな金融サービスを主体的に創造するかどうかが活用の決め手
- 境界型防御の課題でもあるが、むしろビジネスモデルや、クラウドを活用する人材の問題
- ネットリテラシーと社員教育が重要

サイバーセキュリティのモデル選択

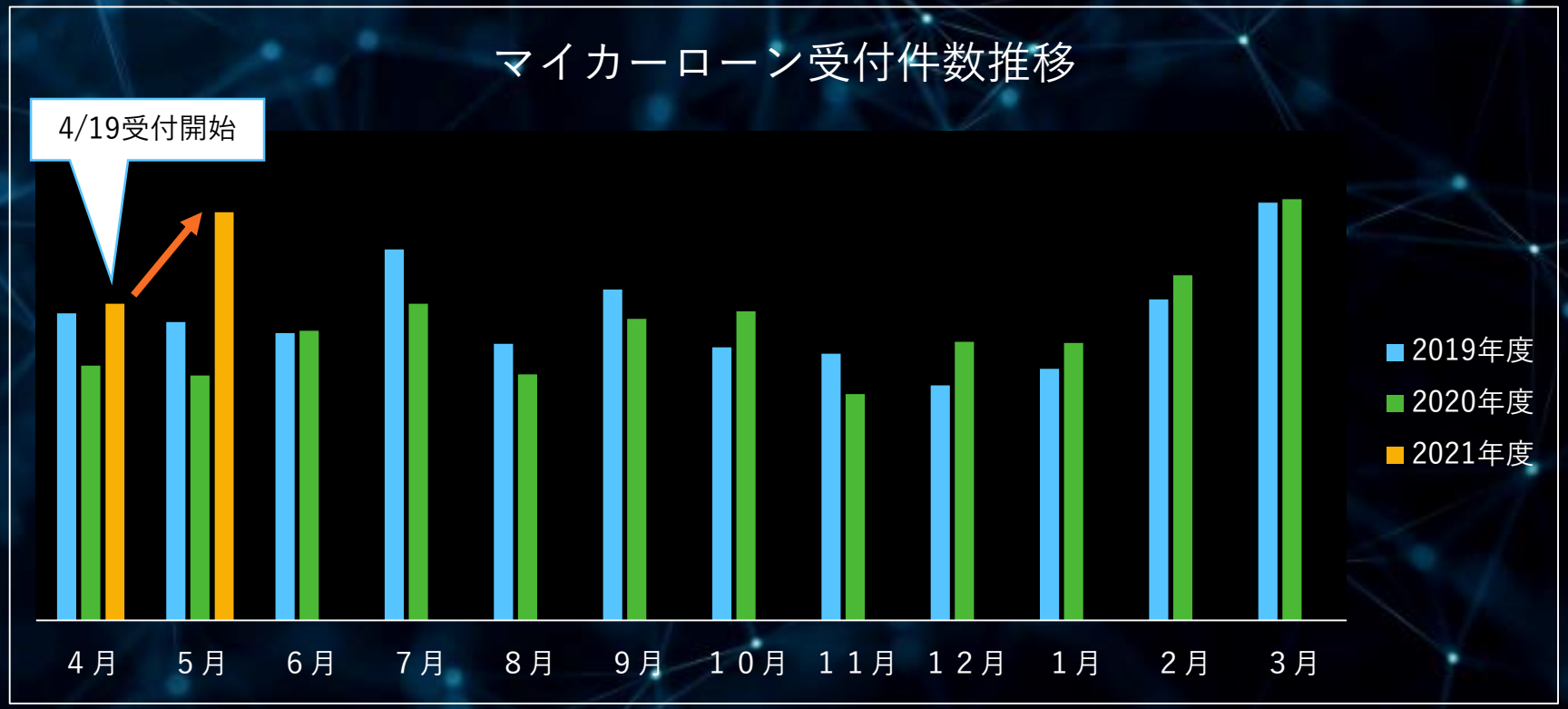
境界型セキュリティ

ゼロトラスト



事例１：ローンＷｅｂ完結

- ４月下旬にマイカーローンのＷｅｂ完結スキームを導入
- 申込から契約までＷｅｂ上で完結　⇒　非常に好調



事例１：ローンＷｅｂ完結

- クラウドサービスにおけるインシデント（他社事例）
  - ✓ 機密情報へのアクセス権限設定を誤り、情報漏洩
  - ✓ 認証設定を適切に行わず、パスワード総当たりによる侵入を許した結果、情報資産を喪失
  - ✓ 開発環境のテスト時に実データを使用し、その後消去を失念して情報漏洩
  - ✓ ＷＡＦの誤設定により情報漏洩
  - ✓ セキュリティパッチの適用漏れによりランサムウェアによる暗号化被害

事例１：ローンＷｅｂ完結

- セキュリティに関する弊行の取り組み

クラウドサービス事業者の適切な選定（信頼性）

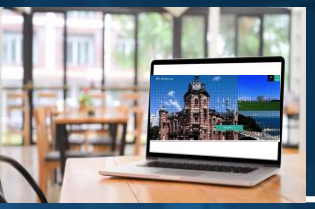
導入時の脆弱性診断

ユーザー設定の集中管理、ワークフロー管理

脆弱性に関する広範な情報収集

収集した脆弱性情報に関する影響確認

収集情報への対応に関するワークフロー管理



事例２：経営支援サイト

ビジネス
マッチング

チャット

6/1サービス開始

補助金情報等
の取得

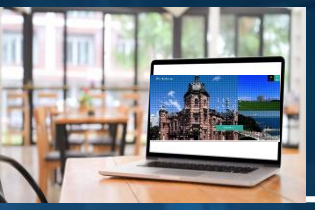
士業相談

行員は業務用スマート
フォンで利用

割引クーポン

安否確認

お客様とスマホで
チャットが可能



事例２：経営支援サイト

- 弊行のセキュリティへの取り組み

ＩＤの絞り込み（必要なユーザーのみに限定）

情報の機密性を監視、管理

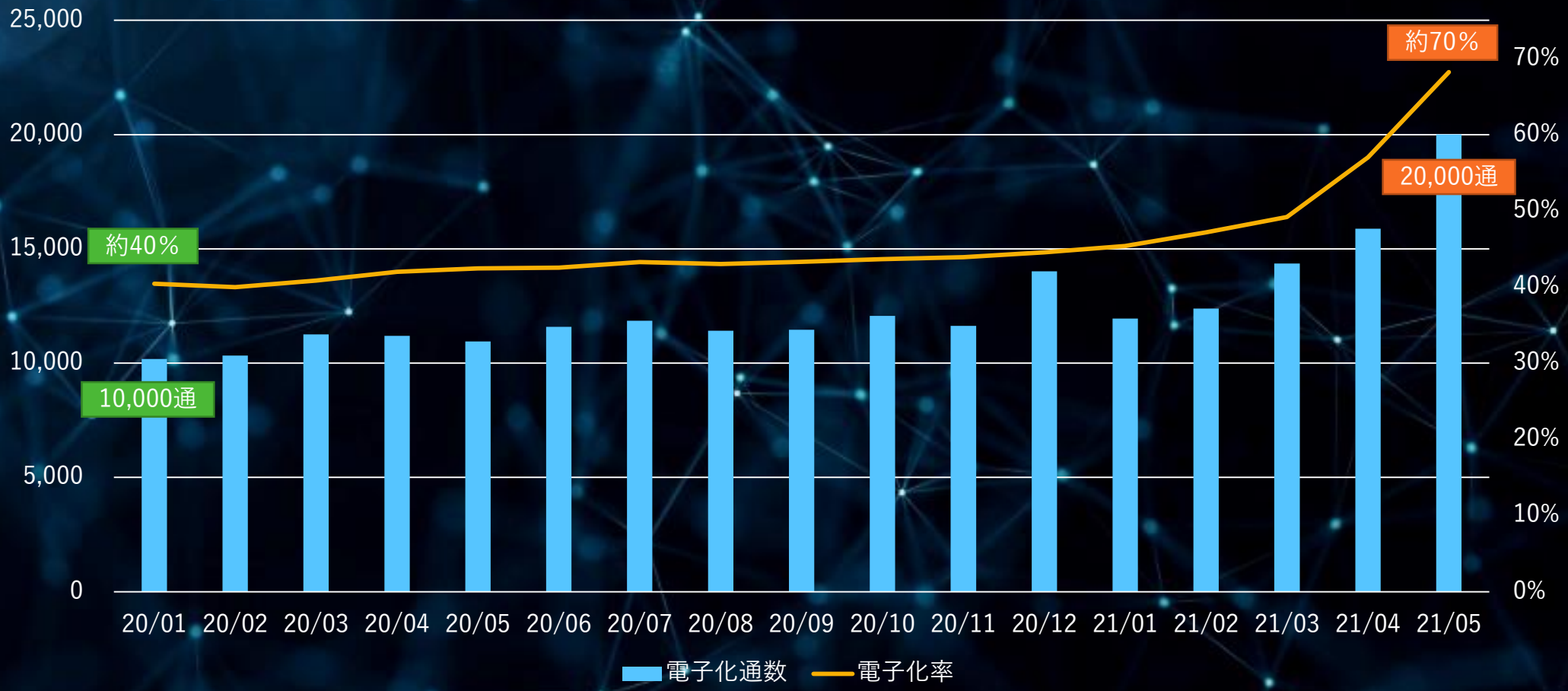
ファイルの授受に関する権限設定

運用ルールの徹底

サイト管理者（グループ）を営業部門に設置

事例３：電子交付サービス

✓ 法人向郵送物の電子化（岩手銀行）



事例３：電子交付サービス

帳票一覧

帳票表示

Financial Service Platform　○○○○○ 電子帳票利用

帳票一覧

対象期間： 2019年1月9日 ～ 2019年2月9日　銀行・期間　絞込み　検索

発行日時	発行機関	企業番号	カテゴリー	帳票名	説明
2019年01月10日 13時29分	0123 岩手銀行	ibk0141421356	振込	振込受付書	総合振込 31-01-09
2019年01月09日 19時56分	0123 岩手銀行	ibk0141421356	振込	振込受付書	給与振込 31-01-08
2019年01月09日 19時53分	0123 岩手銀行	ibk0141421356	預金	当座勘定照合票	001-9999999-310105

Items per page: 10　1 - 3 of 3

戻る

Financial Service Platform　○○○○○ 電子帳票利用

1 /2ページ

預金払戻請求書・預金口座振替による振込受付書　1ページ

依頼人 ｶ)------　殿

振込指定　31年 01月 09日　株式会社岩手銀行
総合振込　依頼人コード FB----------

	被仕向銀行（上段） 支店（下段）	科目	口座番号	受取人	金額	手数料（税込） 本支店	手数料（税込） 他行
1	ｲﾜﾃ ------	7	1000000	------	1940		
2	ｲﾜﾃ ------	7	2000000	------	15700		
	ｲﾜﾃ			------			

REST APIで様々なシステムと接続可能

簡単なスクリプトで帳票デザインが可能

事例３：電子交付サービス

＜インターネットバンキング＞

× 煩雑なログイン手続
× 限定的なサービス

お客さま

A銀行 Web　B銀行 Web　C銀行 Web

A銀行　B銀行　C銀行

× 費用は単独負担
× 銀行間の連携はない

＜金融サービスプラットフォーム＞

○ 簡単なログイン
○ 豊富なサービス

お客さま

情報集約と分析

高度なサービス

AI分析

取引情報

プラットフォーム　電子交付　アプリ

プラットフォームを金融機関が共同で提供

FinTech企業　A銀行　B銀行　C銀行

○ 共同で負担軽減
○ 連携サービス可能

事例３：電子交付サービス

- ブロックチェーンとプラットフォームの親和性

貿易取引の例

国内企業　　海外企業

信頼関係が疎

ブロックチェーン　有効

信頼性を補完　⇒
耐改ざん性が有効

プラットフォーム

ユーザー

ユーザー相互の信頼関係が疎

ユーザーと事業者の信頼関係も疎

ブロックチェーン　有効

事業者相互の信頼関係も疎

事業者

信頼が疎な関係者の集合体

プラットフォームは信頼関係が疎な多くの関係者が利用するため、信頼性の補完効果は大きい

事例３：電子交付サービス

- 運営主体は「フィッティング・ハブ」
- ベンダーと金融機関が協力して地域デジタル基盤の構築に取組む

項　目	内　　容	備　　考
商号	㈱Fitting Hub（フィッティング・ハブ）	「出会いの結節点」の意
設立日	2019年2月12日	
事業目的	システム資産管理、利用料管理、プロジェクト支援	
資本金	1億4410万円	
株主構成	青森銀行、秋田銀行、岩手銀行、山梨中央銀行 日本ＩＢＭ、ＡＩＴ、ＮＥＣ	
役員	代表取締役　　弊行システム部長 取締役　　秋田銀行、日本ＩＢＭ、日本電気 監査役　　ＡＩＴ	

事例３：電子交付サービス

- 電子交付サービスのセキュリティ

秘密鍵の保護

ネットワーク設計とＩＤ管理の連携

ログイン状況の日次モニタリング

事例３：電子交付サービス

- 改正個人情報保護法への対応
  - ✓ 来年４月施行を控え、本システムは対応が必要
  - ✓ ブロックチェーンは、データを消去できないのが強み
  - ✓ 消去が必要となるデータについて、チェーンへの書き込みを行わない対応をせざるをえない
  - ✓ ブロックチェーンに限らず、今後のシステム構築では、個人情報を分別管理し、適切に消去可能な仕組みを入れていく必要がある
  - ✓ 本システムについては、対応にめど

事例４：地域ｅＫＹＣ

- ｅＫＹＣ ＝ 犯罪収益移転防止法
- 金融取引、不動産取引などにおける特定取引で活用
- 免許証の厚みを撮影し、対象者の顔画像を解析する、など
- しかし、それ以外にも社会的ニーズはあるのではないか

なりすましは困る…

デジタル化はコストが…

申込がいまだに紙で…

決済サービスはコストが…

地域ｅＫＹＣ

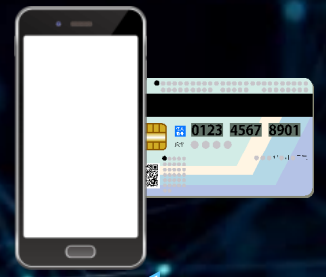
事例４：地域ｅＫＹＣ

アプリを開いて

＋

パンフやＷｅｂの
ＱＲを撮影して

＋



電子署名すれば

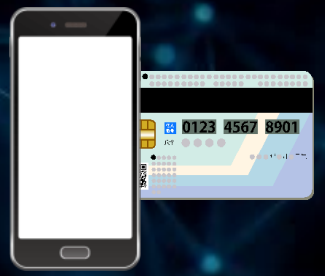
＝

- ✓ 本人確認
- ✓ 申込手続
- ✓ 口座振替申込

手続きが一括完了！

さらに・・・

ＱＲを３つ
まとめて撮影して



電子署名すれば

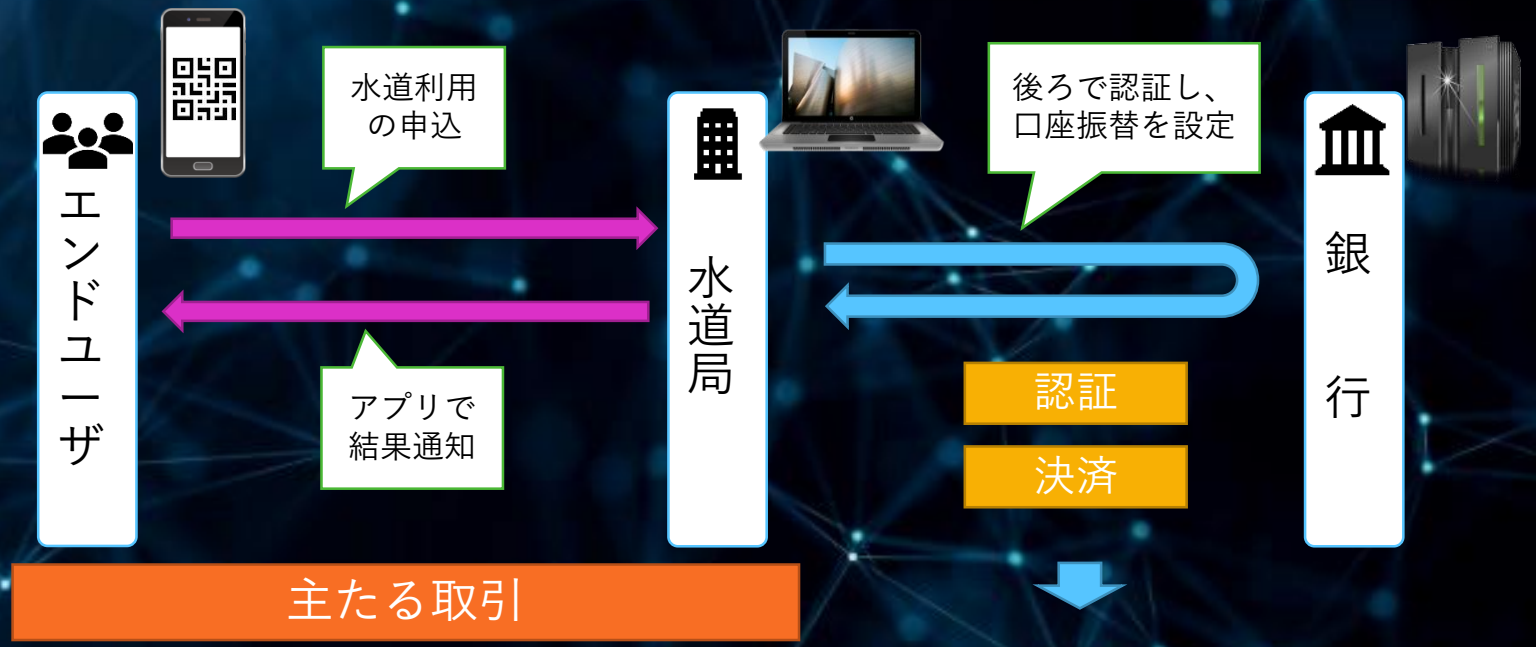
- ✓ 水道利用申込
- ✓ 電気利用申込
- ✓ ガス利用申込

複数の利用申込も
まとめて処理可能

事例４：地域ｅＫＹＣ

基礎となる電子契約の実証実験を実施中

事例４：地域ｅＫＹＣ ＜銀行機能の仮想化＞



銀行機能をデジタルで仮想化

事業者様のデジタルサービスのパーツとして銀行機能を提供

- ✓ 地域のデジタル化推進
- ✓ 地域の決済基盤掌握
- ✓ 低原価率と安定した収益
- ✓ 容易な獲得推進

事例４：地域ｅＫＹＣのセキュリティ

- 弊行のセキュリティへの取り組み

認証をマイナンバーカード寄せ

情報を極力まとめずに分散保管

重要データは電子証明書で暗号化して保管

重要データは電子証明書でのみ復号可

アプリ上には最小限のデータを保管

事例４：地域ｅＫＹＣ

1. 岩手銀行のパーパスは、「地域貢献」＋「健全経営」
2. つまり、地域経済の活性化と、銀行の収益強化ができればよい
3. 地域経済活性化において、キャッシュレス以外に何かないか
4. 経済取引の入り口をデジタルで簡単にすることで、活性化できないか
5. BtoB、BtoCを活性化するのはよいが、銀行の収益はどうする
6. 後ろに口座振替をセットすることで、クレジットカードに押されがちな手数料収益を強化
7. 口座振替申込の9割以上は未だに紙であり、預金者、委託先、銀行、全てにとって非効率
8. デジタル化で口座振替が一定数増加すれば、銀行はリスクレス、経費レスで収益が増加
9. これをただデジタル化するのではなく、付加機能をつけられないか
10. マイナンバーカードによる本人確認をつければ、銀行、委託先の全てが預金者の最新住所を共有可能に（預金者同意が前提）
11. 委託先の申込業務の受託は、銀行法上、明らかに対象外であり、高度化会社でも微妙
12. 似たようなスキーム、転用可能なスキームはないか・・・なければ自前でやるしかない

・・・・・

＜参考＞リスク対応

1. リーガル対応
   - ① 最終的に当局の理解を得られても、専業銀行ではフロントランナーは大きなリスク
   - ② 新たなビジネスモデルを立ち上げる際には、業法のリーガルチェックが必須
   - ③ 専門家と協議を行い、法的課題を事前に整理
2. 費用対効果
   - ① 自組織が収益を上げられないスキームは持続しない
   - ② 収益モデルの実現可能性と、実現に向けた施策を組織内で共有
   - ③ パーパスに沿ったＫＰＩを設定し、収益に関するＫＰＩをセットで設定
3. 知財管理
   - ① 先例のないスキームについては、事前に関連特許を広範囲に確認することが必須
   - ② 先例のないスキームについては、安全のため、基本的に特許出願検討を推奨
   - ③ 先例のあるスキームを模倣する場合は、特許侵害リスクを十分に確認
   - ④ ベンダーは銀行のスキームに関する知財管理は一切やってくれないので注意

＜参考＞知財管理

岩手銀行が出願した特許申請の例（抜粋）

難解だが、先例確認を専門家に依頼すれば数百万～数千万円かかるため、自分で行うしかない

【書類名】　特許請求の範囲
【請求項１】
　外部装置と通信する情報処理装置において各工程が実行される情報処理方法であって、
　前記外部装置において共通鍵を用いてトランザクションのデータを暗号化することで生成された第１データと、前記共通鍵とを、前記外部装置から受信する受信工程と、
　前記受信工程において受信された前記共通鍵を用いて、前記第１データから前記トランザクションのデータを復号化する復号化工程と、
　前記第１データから復号化された前記トランザクションのデータに対して所定のビジネスロジックを実行して、前記所定のビジネスロジックの実行結果を出力する処理工程と、
　前記共通鍵を用いて前記所定のビジネスロジックの実行結果を暗号化する暗号化工程と、
　前記暗号化された実行結果を、ブロックチェーンに記録する記録工程と、を有する、ことを特徴とする情報処理方法。
【請求項２】
　前記受信工程では、更に、前記トランザクションのデータを参照可能なエンティティに関連付けられた公開鍵を用いて、前記外部装置において前記共通鍵を暗号化することで生成された第２データを、前記外部装置から受信し、
　前記記録工程では、更に、前記第２データを前記ブロックチェーンに記録する、ことを特徴とする請求項１に記載の情報処理方法。
【請求項３】
　前記受信工程では、前記共通鍵を、前記ブロックチェーンに記録されないように区別されたフィールドを用いて受信する、ことを特徴とする請求項１または２に記載の情報処理方法。
【請求項４】
　前記共通鍵は、前記情報処理装置に関連付けられた公開鍵を用いて、前記外部装置において暗号化され、
　前記受信工程では、前記情報処理装置に関連付けられた公開鍵を用いて暗号化された状態の前記共通鍵を、前記ブロックチェーンに記録されるフィールドを用いて受信する、ことを特徴とする請求項１または２に記載の情報処理方法。

＜参考＞知財管理

留意事項

- ✓ システム構築に関する知財管理は、明示的に契約している場合や、パッケージ提供される場合を除き、原則、発注者に確認責任があります。
- ✓ 先例のないビジネスモデルを構築する場合は、防御的特許出願の検討が推奨されます。
- ✓ 特許出願に関しては、たとえ防御目的であったとしても、十分な能力を備えた信頼できる専門家の助言が必要です。
- ✓ 知財管理については、主に以下のようなリスクがあります。

訴訟対応	損害賠償	システム改修費用	風評被害

- ✓ 新たなビジネスモデルが必要である以上、組織的知財管理は不可欠です。
- ✓ 知財管理は、就業規則（報奨制度など）も絡むため、十分な準備が必要です。
- ✓ 上記はあくまで一般論であり、個別の助言については、業法による制限があります。

サイバーセキュリティがＤＸ対応力を定義

- どこまでサイバーセキュリティに対応できるかで、ＤＸの対応範囲が定義される
- サイバーセキュリティで対応すべき項目は、特にも重点的に対応すべき項目は、システムごとに大きく異なる

情報の機密性に応じたセキュリティの設計（データの分散保管、暗号化）

ＩＤ管理の主体的設計と、重要度に応じたアクセスログのモニタリング

定期的（導入時含む）な脆弱性診断と許容リスクの管理

留意事項

パネルディスカッション、および資料は、岩手銀行独自の見解を反映したものです。それらは情報提供の目的のみで提供されており、いかなる参加者に対しても法律的またはその他の指導や助言を意図したものではなく、またそのような結果を生むものでもありません。本講演資料に含まれている情報については、完全性と正確性を期するよう努力しましたが、「現状のまま」提供され、明示または暗示にかかわらずいかなる保証も伴わないものとします。本講演資料またはその他の資料の使用によって、あるいはその他の関連によって、いかなる損害が生じた場合も、岩手銀行は責任を負わないものとします。

本講演資料で岩手銀行のサービスに言及していても、岩手銀行が営業活動を行っているすべての地域でそれらが使用可能であることを暗示するものではありません。本講演資料で言及しているサービスのリリース予定やサービスの機能は、市場機会またはその他の要因に基づいて岩手銀行独自の決定権をもっていつでも変更できるものとし、いかなる方法においても将来のサービスまたは機能が使用可能になると確約することを意図したものではありません。本講演資料に含まれている内容は、岩手銀行が開始する活動によって特定の販売、売上高の向上、またはその他の結果が生じると述べる、または暗示することを意図したものでも、またそのような結果を生むものでもありません。 サービスのパフォーマンスは、管理された環境において標準的なベンチマークを使用した測定と予測に基づいています。ユーザーが経験する実際のスループットやパフォーマンスは、ユーザーのジョブ・ストリームにおけるマルチプログラミングの量、入出力構成、ストレージ構成、および処理されるワークロードなどの考慮事項を含む、数多くの要因に応じて変化します。したがって、個々のユーザーがここで述べられているものと同様の結果を得られると確約するものではありません。