

JPAAWG 7th General Meeting

[B2-5]NTTドコモにおけるドメイン名管理

JPAAWG 7th General Meeting
2024/11/12 (火)

株式会社NTTドコモ 情報セキュリティ部 CSIRT
三浦 未来

ドコモ情報セキュリティ部CSIRTについて

情報セキュリティ部

セキュリティガバナンス

サービス企画組織

システム開発組織

NW系開発組織

営業系組織

コーポレート系組織

私の所属するチーム

- ・インシデントハンドリングなどいわゆるCSIRT領域を担当
- ・インシデントから見えてきた各種課題への対応も実施
- ・セキュリティの何でも屋な一面も

本日は話したいこと

ドコモにおけるドメイン名管理方法の改善

きっかけ

ドメイン名廃止に関する社内ルールが守られておらず、ドメインドロップキャッチに関する問題が発生した

⇒ドメイン名の管理方法について抜本的に見直しをかけることとなった

(参考)ドメイン名の管理はなぜ大切なのか

企業がドメイン名を不用意に手放すリスクは、以下が考えられる

- ①手放したドメイン名が第3者に取得され、元所有者になりすました悪意ある行為を実行され、**企業の顧客が被害にあう**(フィッシング・コピーサイト等)
- ②手放したドメイン名が第3者に取得され、アダルトサイトやカジノサイト等を立ち上げられ、**企業のブランドイメージが毀損**されてしまう。
- ③重要なドメイン名を手放したことが外部で判明すると、①や②のリスクを考慮できていない企業とみなされ、**企業への批判で炎上する**可能性がある。
- ④ドメイン名を再取得しようとした場合に、**高額な費用が必要となる**可能性がある

当時のドコモにおけるドメイン名管理の状況【before】

ドメイン名取得/維持

- ・ドメイン名利用組織にて任意のレジストラから取得/維持管理
- ・全体を**管理する組織は存在しない**ため、利用組織の判断で手放すことも可能



当時のドコモにおけるドメイン名管理の状況【before】

ドメイン名廃止

- ・社内ルールに従って、情報セキュリティ部にドメイン名を移管
- ・**ルールが浸透しきっておらず**、情セキ部の**知らない間にドメイン名が手放される**ケースもあり。今回はこのパターン。



事件を通して見えてきた課題

課題① 管理が各組織に委ねられている

課題② ルールが浸透していない

課題③ ドメイン名は“重要な資産である”という意識の欠如

まずドメイン名管理方針を見直さなくては、、、

全ての課題の前提として、そもそも今のドコモのドメイン名管理方針を見直すべきではないか。ドメイン名は重要な資産である！

誰かがきちんと管理しなくてはいけない。

誰がやる？俺でしょ！ いつやるの？今でしょ！



「ドメイン名は全て情報セキュリティ部にて一元管理する」

「情報セキュリティ部ではドメイン名を永続的に保有する」

方針を宣言

【課題①への対応】利用組織にはドメイン名を持たせない

課題① 管理が各組織に委ねられている



既存ドメイン名を
情セキ部へ移管

- ・緊急ヒアリングにより社内保有ドメイン名を棚卸
- ・地道にひとつずつ移管

新規ドメイン名は
サブドメインを利用

- ・ドメイン名が必要な際は既存ドメイン名のサブドメインを利用
- ・サービス横断で使われている共通的なドメイン名を活用

サブドメ利用が難しい場合
は情セキ部で取得

- ・利用組織からの申請に従って、情セキ部にて取得
- ・ネームサーバやSSL証明書は利用組織にて準備し管理

【課題②への対応】ドキュメント整備とルール違反の監視

課題② **ルールが浸透していない**



ドメイン名管理に関する
専用マニュアルを制定

- ・ドメイン名利用開始、終了時の手続きを規定
- ・eラーニングなどを活用し徹底的に周知

ルール違反の監視※

- ・情セキ部で認知していないドメイン名を定期監視
- ・ドメイン名やWhois情報から、ドコモ取得を推定

※完璧な調査は難しいため、まずはルールを守ってもらうことが何より重要

【課題③への対応】ドメイン名を気軽にとらせない

課題③ ドメイン名は“重要な資産である”という意識の欠如



ドメイン名を気軽に
取得する文化を是正

- ・リスクの低い社内検証用のドメイン名も情セキ部で取得
- ・「ドメイン名をとる⇒情セキ部に相談」の意識を醸成

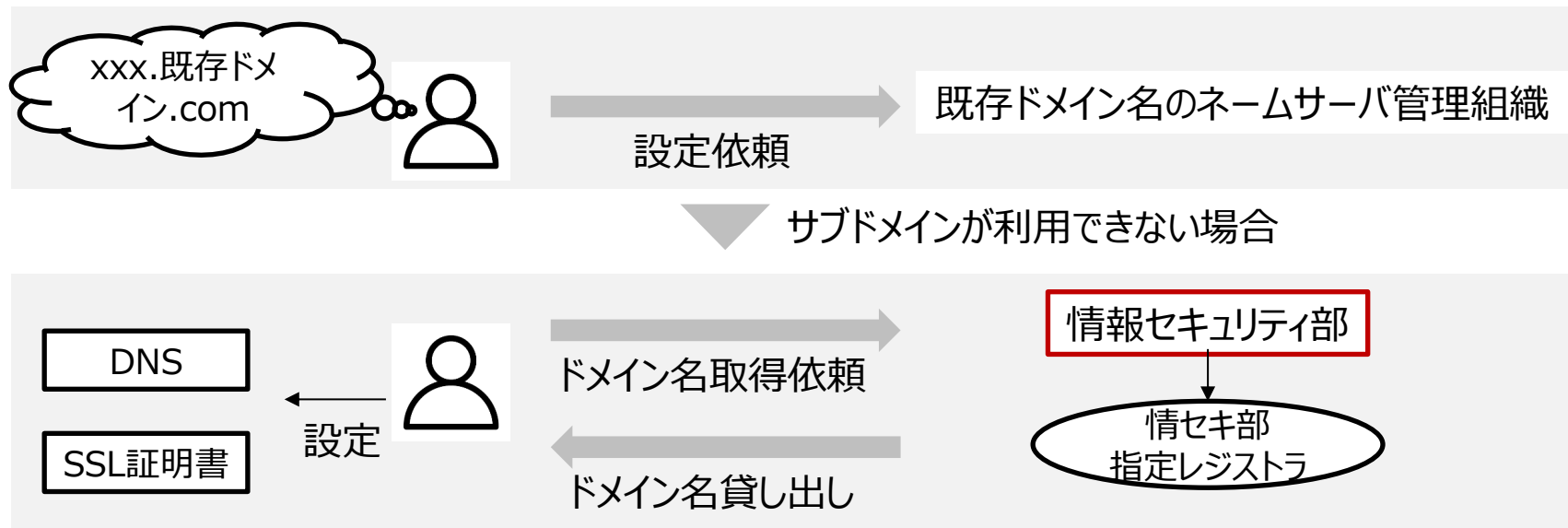
意識醸成のための
啓蒙活動

- ・eラーニングの活用
- ・各種社内会議にてドメイン名管理の取り組みをインプット

現在のドコモにおけるドメイン名管理の状況【after】

ドメイン名取得/維持

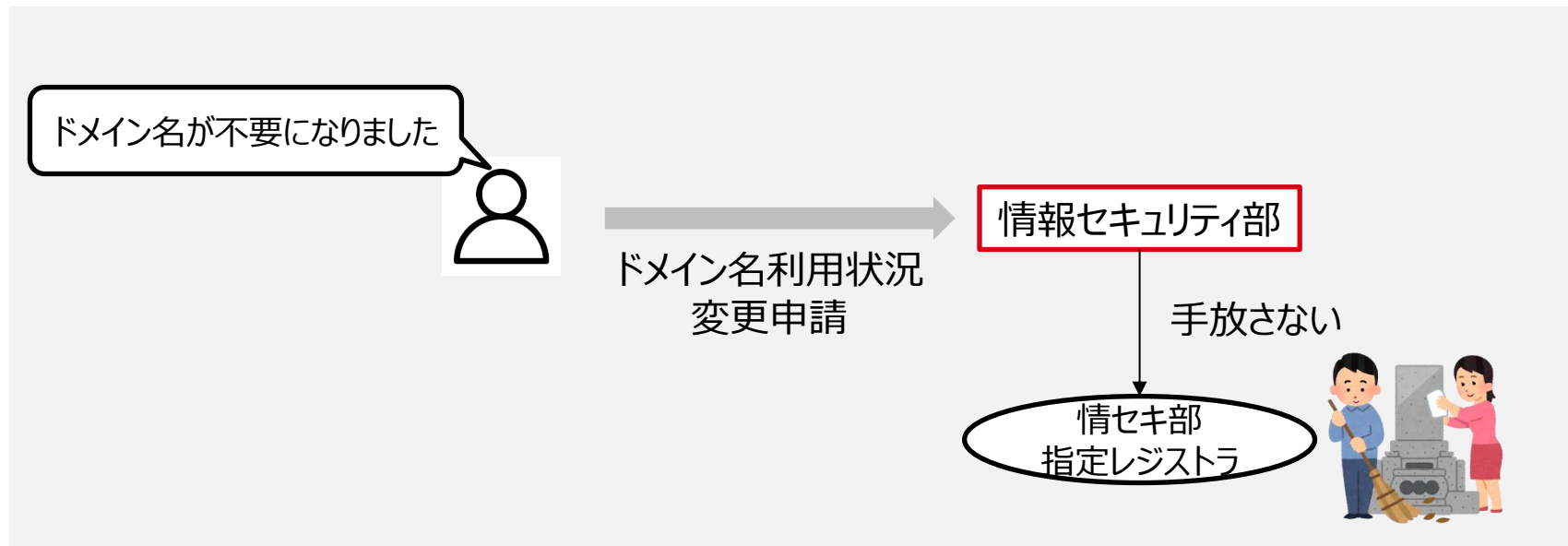
原則サブドメインを利用。利用不可の場合は情報セキュリティ部にてドメイン名を取得/維持し、利用組織に貸し出す



現在のドコモにおけるドメイン名管理の状況【after】

ドメイン名廃止

情報セキュリティ部にて永続的にドメイン名を保持(廃止しない)



課題へ対応した結果

課題① 管理が各組織に委ねられている

結果

- ・1.5年かけてほぼ全てのドメイン名を情セキ部の管理下に

課題② ルールが浸透していない

結果

- ・ドメイン名の新規取得相談が多数
- ・既存ドメイン名棚卸時の未申告ドメイン名を自ら申告する人が続々と

課題③ ドメイン名は“重要な資産である”という意識の欠如

結果

- ・ドメイン名リスクに関する相談多数
- ・情セキ部で把握していなかった各種個別ドキュメントにもいつの間にかドメイン名管理についてのルールが追記

苦勞

既存ドメイン名の移管が最も大変であった、、、。

ドメイン名を移管するためには、**現契約者の作業が必要。**

大量のドメイン名移管を実現するために

ドメイン名保有者全員の実施内容理解、協力が必要。



**愚直に丁寧に寄り添って一つずつ対応
をしていくしかない**

- ・全社向け説明会の複数回開催
- ・問い合わせ対応(十件以上/日)
- ・システム個別の事情に応じた調整 etc.

1.5年余りでほぼすべてのドメイン名移管が完了

今後の検討課題

ドメイン名廃止ルールの策定

あらゆるドメイン名を永続に保持し続けることは、コスト効果が良いとは言えない。
ドメイン名を廃止してもよい条件を検討したい。

リスクの低いドメイン名の管理方法見直し

現在はあらゆる利用用途のドメイン名を管理対象とすることで、ドメイン名の重要性を利用者に認知してもらっている。

社内の意識醸成が図れたのちは、リスクの低いドメイン名は現行の管理方法からレベルを落としてもよいのではないかな。

最後に

ドメイン名という資産の価値を甘く見ると、とても痛い目を見ます。

我々の失敗の二の舞とならないように、ぜひ日頃から注意を払ってご参考にしていただければと思います。