統合管理システム「Logstorage」による制御システムセキュリティ対策

インフォサイエンス株式会社
プロダクト事業部

Infoscience Corporation
www.infoscience.co.jp info@logstorage.com
Tel: 03-5427-3503 Fax: 03-5427-3889

1. 制御システムセキュリティとは

制御システムにセキュリティ対策が求められる背景

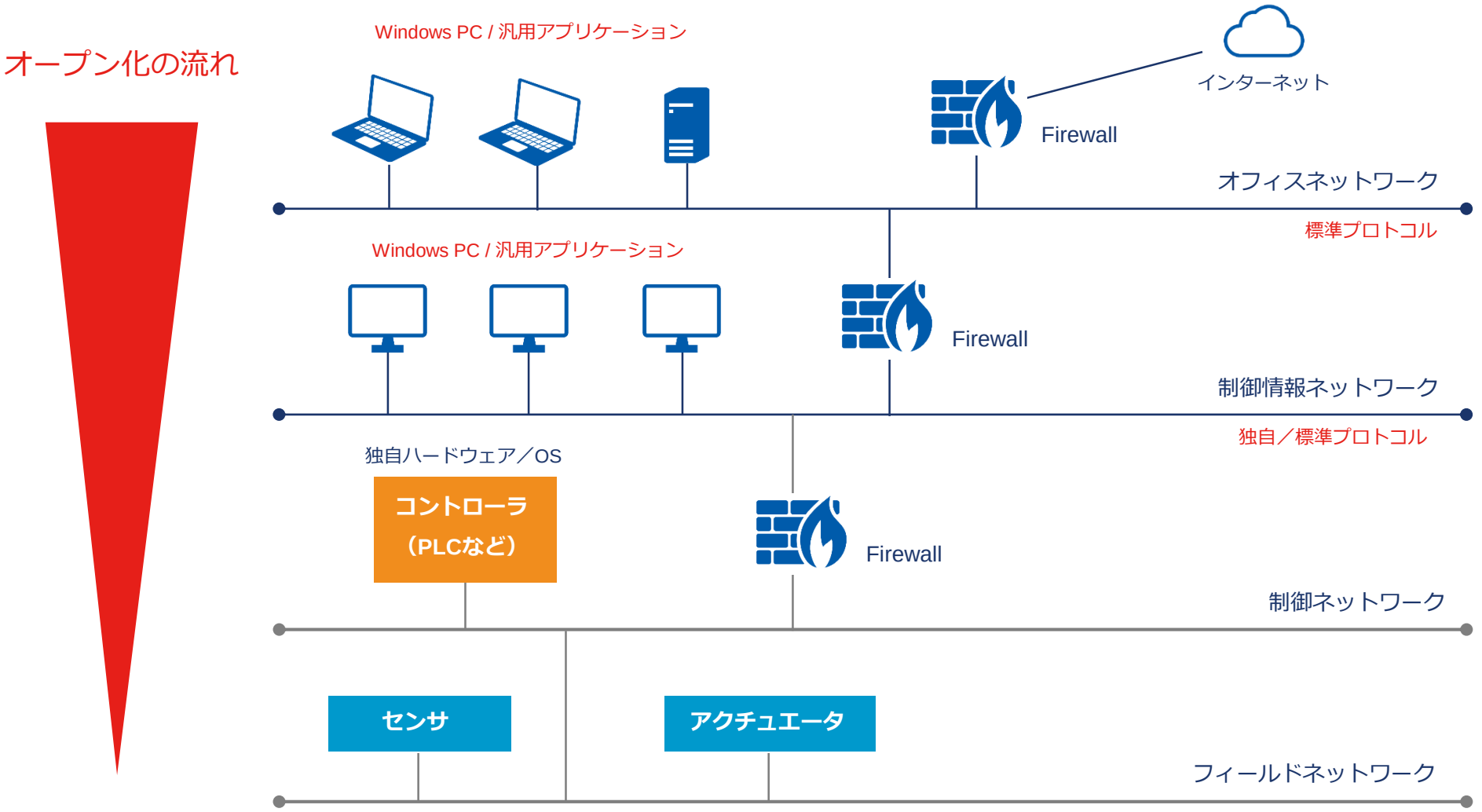
以前まで制御システムは、独自OSや独自プロトコルにより構成されており、外部のネットワークからも隔絶されていたため、外部からのサイバー攻撃に対するリスクは極めて低いと考えられてきました。

しかし昨今、低コスト化や、他のシステムとのデータ共有のニーズから、制御システムに於いても汎用OS・汎用プロトコルが用いられ、外部システムと接続されるなど、オープン化が進んできています。

その結果として、サイバー攻撃を受けるリスクが高まり、2010年には**「Stuxnet」**というマルウェアがイランの核施設を乗っ取り、遠心分離機を実際に停止に追い込むという、極めて深刻な事態も発生しています。

この**「Stuxnet」**の事例は、制御システムのセキュリティに対する従来の考え方を大きく変える契機となり、現在、様々な形でセキュリティ対策が進められています。

制御システムのオープン化



制御システムを狙うマルウェア

Stuxnet / Duqu / Flame

Stuxnet :

2010年にイランを中心とする中東地域で影響が報告されているマルウェア。
シーメンス社の産業用機器の制御システムを攻撃対象とし、イランの核施設の遠心分離機を停止させた。

Duqu :

制御システムメーカーなど、特定の組織から機密データを収集することを目的としたマルウェア。Stuxnet 2.0 とも呼ばれ一部コードが酷似していることから作成者が同じとされる。

Flame (Skywiper) :

2012年に中東地域を中心に影響が報告されているマルウェア。
Stuxnetの20倍ものコードの分量を持ち、これまで発見されたマルウェアの中でも最も複雑・高度であるといわれている。

これらマルウェアの開発には国家が関与しているとも言われており、
「サイバー戦争」への備えも求められている

情報システムと制御システムのセキュリティに対する考えの違い

情報システム

機密性 > 完全性 > 可用性

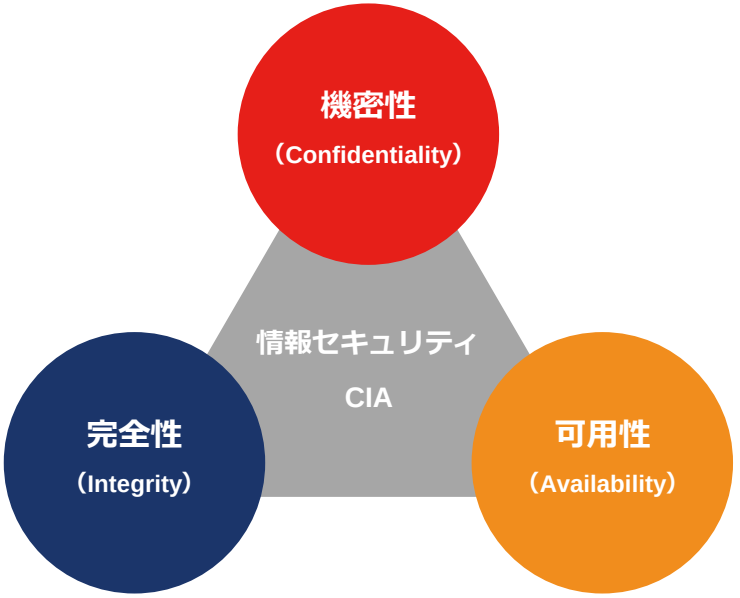
・個人情報、機密情報の漏洩防止
⇒ 情報が漏れるくらいならシステムを止める

制御システム

可用性 >= 完全性 > 機密性

・運転を開始すると止められない
⇒ セキュリティ・パッチの適用も容易ではない

・ライフサイクルが長い
⇒ レガシーなOSが使われ続ける



【 情報セキュリティに於けるC.I.A 】

制御システムの可用性・完全性を重視したセキュリティ対策が必要

2. ログ監視によるセキュリティ対策

制御システムの特徴を利用した攻撃への対処

・制御システムには高い可用性が求められるため、システムに影響・負荷を与えない、
ログ監視によって**マルウェアの感染、攻撃の兆候を早期に発見**する対策の有効性が高い。

・監視対象のシステムで、**通常のルールと異なる通信を検出**することで、システムに被害が生じる前に
その兆候を見つけ、早期に対策する。

制御システム向けのログ監視の流れ

収集 → **意味付け** → **保管** → **分析**

各所のシステムから
ログデータを収集

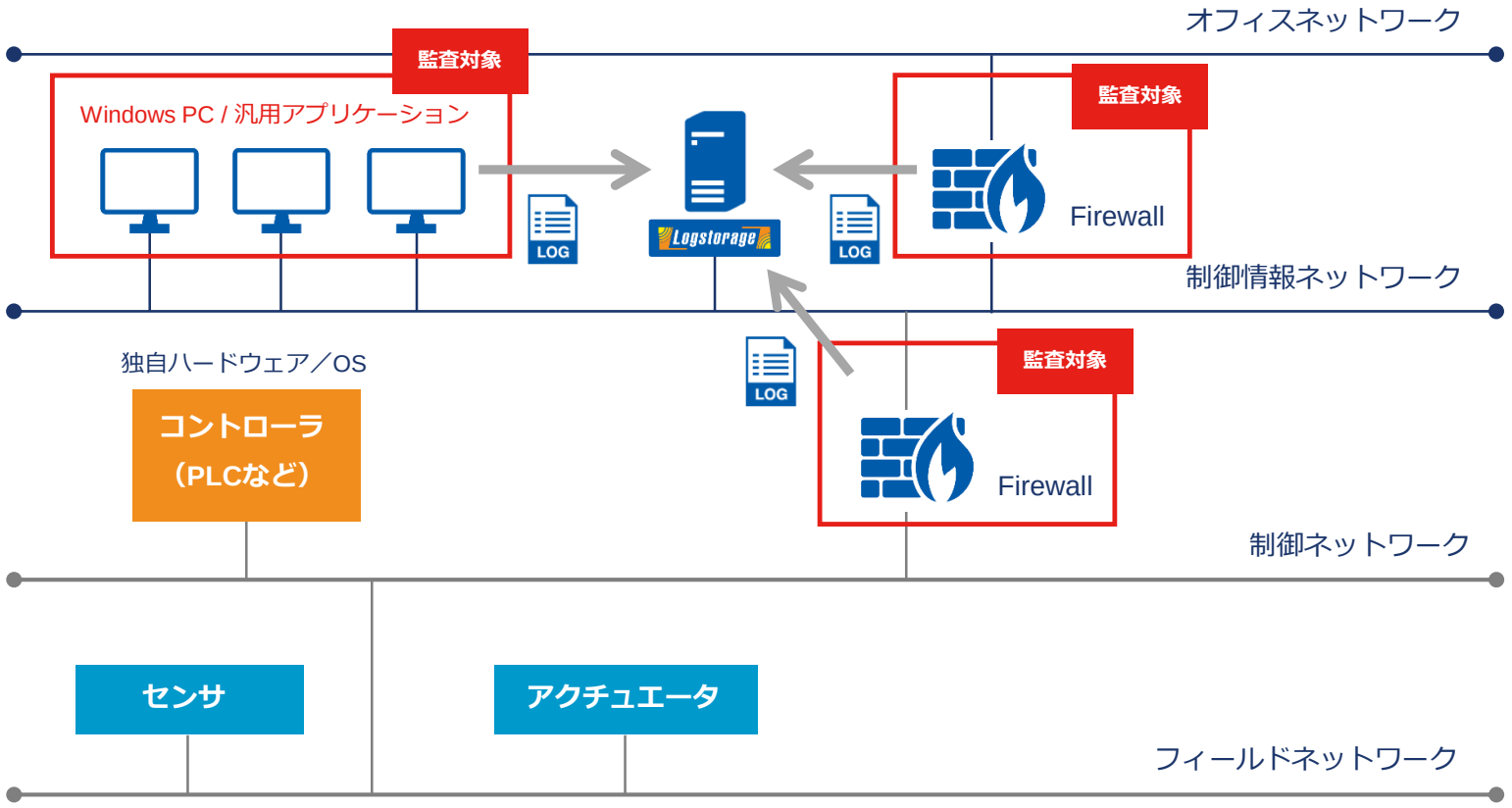
異なるログの
形式を吸収

意味付けした
ログを保管

制御システム向け
分析ルール

Timestamp,ip_address message ….
Timestamp,src_ip,src_port,dest_ip,…
Security[514]: username, ip address.…

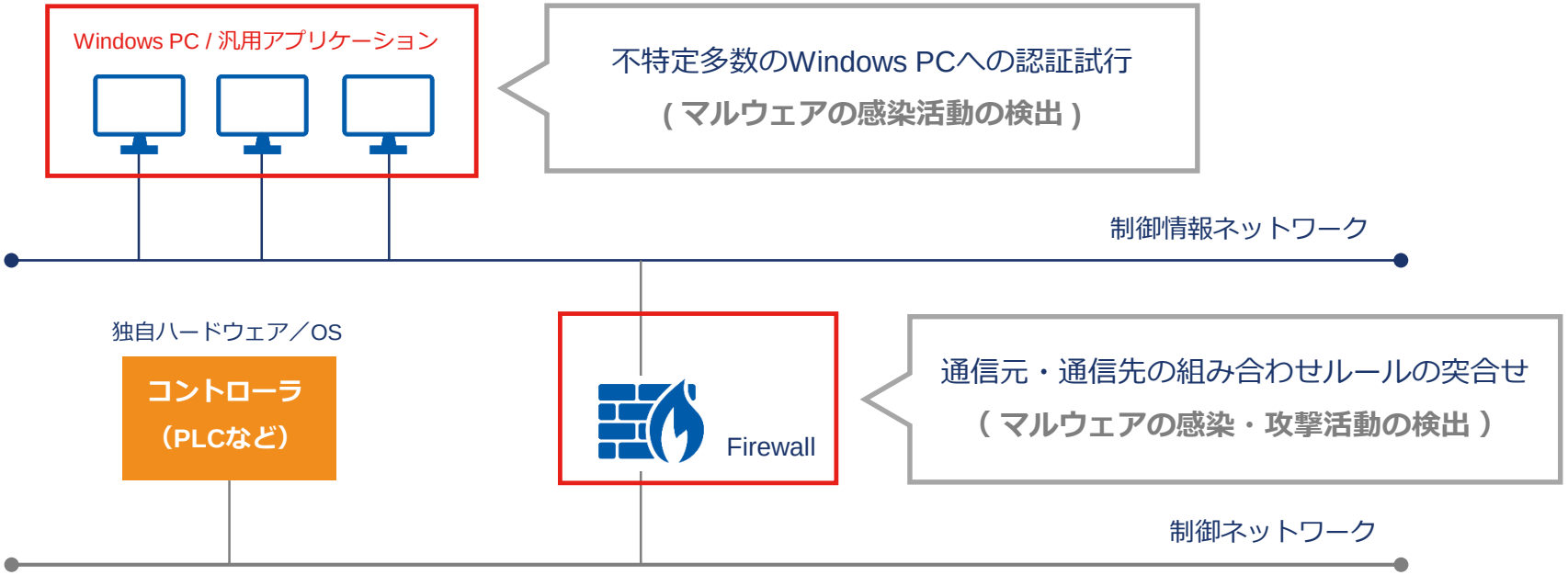
Logstorage によるログの統合管理・監視



Logstorage に各システムのログを収集・意味付け・保管し、制御システム用の分析ルールに基づいたレポートを自動出力する事により、攻撃の兆候を早期に検出する。

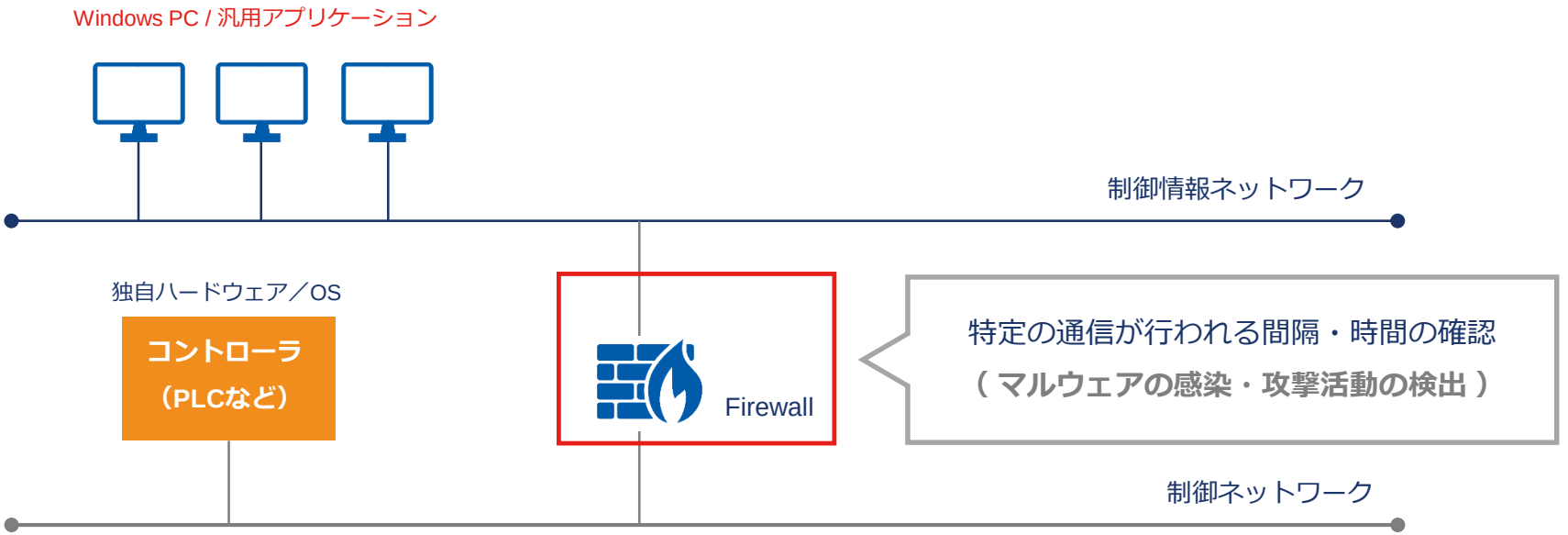
通信の宛先による異常検出

制御システムでは定型的な通信が多いため、どの機器とどの機器が通信を行うか、そのルールを限定することは比較的容易に行える。このルールを外れた通信が発生した場合、異常として検出する。



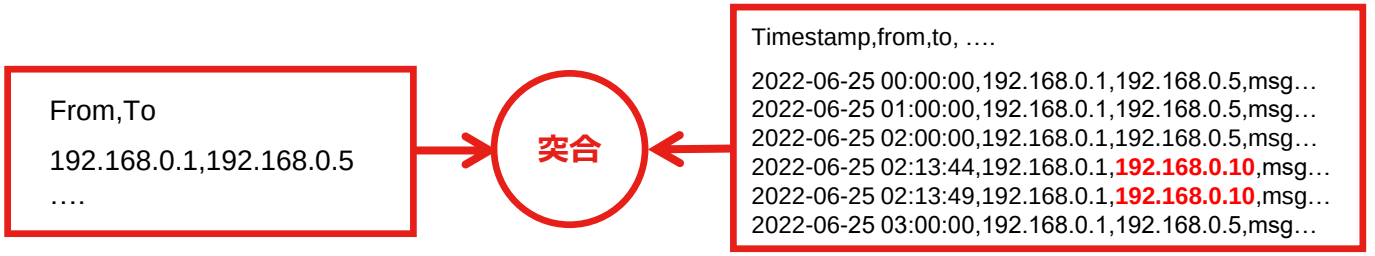
通信間隔による異常検出

制御システムでは、機器の状態を確認するために定期的に行われる通信が存在する。
この定期間隔から外れる通信が発生した場合に、異常として検出する。

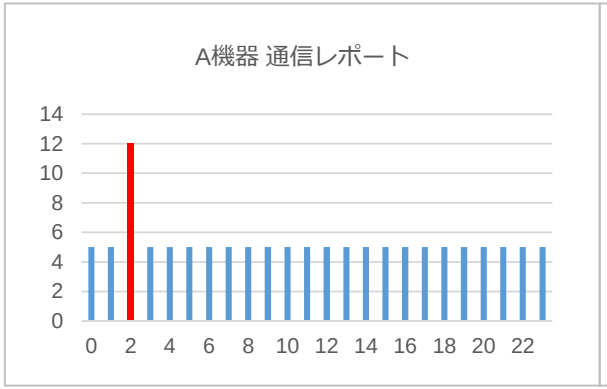


レポート例

レポートを自動生成する事で、日々の通信状況を容易に確認する事ができ、マルウェアの感染、攻撃の兆候を早期に発見し対策を取る事が可能になる。



【 通信ルール 】　　【 Firewall 通信ログ 】



【 レポート：分析ルール／通信の周期】

タイムスタンプ	送信元	送信先	メッセージ
2022-06-25 02:13:44	192.168.0.1	192.168.0.10	msg…
2022-06-25 02:13:49	192.168.0.1	192.168.0.10	msg…

【 レポート：分析ルール／通信の宛先 】

開発元

インフォサイエンス株式会社
〒108-0023
東京都港区芝浦2-4-1 インフォサイエンスビル
https://www.infoscience.co.jp/

お問い合わせ先

インフォサイエンス株式会社
プロダクト事業部
TEL 03-5427-3503　　FAX 03-5427-3889
https://logstorage.com/
mail : info@logstorage.com